User Manual

F18 Pro

Date: December 2025

Doc Version: 1.0

English

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

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

Trademark

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

Disclaimer

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

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

It is an essential pre-requisite for the satisfactory operation and maintenance that the operating and maintenance personnel are fully familiar with the design and that the said personnel have received thorough training in operating and maintaining the machine/unit/equipment. It is further essential for the safe operation of the machine/unit/equipment that personnel 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 Pro**.

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

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

Document Conventions

Conventions used in this manual are listed below:

GUI Conventions

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

Symbols

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

Table of Contents

1 Safety Measures

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

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

1. **Read, follow, and retain instructions** - All safety and operational instructions must be properly read and followed before bringing the device into service.
2. **Do not ignore warnings** - Adhere to all warnings on the unit and in the operating instructions.
3. **Accessories** - Use only manufacturer-recommended or product-sold accessories. Please do not use any other components other than manufacturer suggested materials.
4. **Precautions for the installation** – Do not place this device on an unstable stand or frame. It may fall and cause serious injury to persons and damage to the device.
5. **Service** - Do not try to service this unit yourself. Opening or removing covers may expose you to hazardous voltages or other hazards.
6. **Damage requiring service** - Disconnect the system from the Mains AC or DC power source and refer service personnel under the following conditions:
   - When cord or connection control is affected.
   - When the liquid spilled, or an item dropped into the system.
   - If the system is exposed to water or inclement weather conditions (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 required, service technicians must only use replacement parts provided by the supplier. Unauthorized substitutes can result in a burn, shock, or other hazards.
8. **Safety check** - On completion of service or repair work on the unit, ask the service technician to perform safety checks to ensure proper operation of the device.
9. **Power sources** - Operate the system only from the label's power source form. If the sort of power supply to use is unclear, call your dealer.
10. **Lightning** - Can install external lightning conductors to protect against electrical storms. It stops power-ups from destroying the system.

    Recommended installing the devices in areas with limited access.

2 Electrical Safety

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

3 Operation Safety

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

Note:

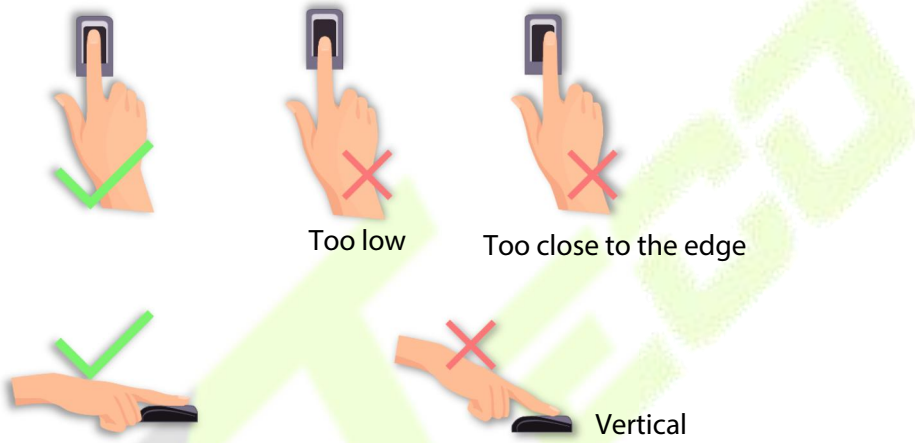
- Make sure whether the positive polarity and negative polarity of the DC 12V power supply is connected correctly. A reverse connection may damage the device. It is not advisable to connect the AC 24V power supply to the DC 12V input port.
- Make sure to connect the wires following the positive polarity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

4 Instruction for Use

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

4.1 Finger Positioning

Recommended fingers: The index, middle, or ring finger and avoid using the thumb or pinky fingers, as they are difficult to accurately press onto the fingerprint reader.



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

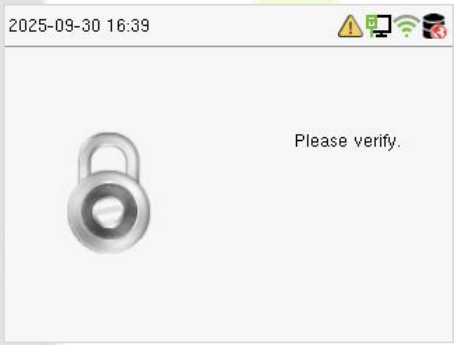
4.2 Standby Interface

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

- Enter any number to access the User ID input interface.

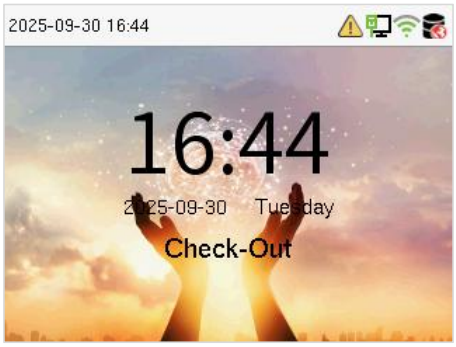
- When there is no Super Administrator set in the device, tap [**M/OK**] to go to the menu.

- 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.

- On the standby interface, the punch state options can also be shown and used directly. The black bold shortcut key mappings will be displayed on the screen if you tap the relevant shortcut key on the hidden touch keypad, as shown in the picture below. For the specific operation method, please see "Shortcut Key Mappings."



Note: The punch state options are enabled by default when the device type is set as an attendance terminal.

4.3 Verification Mode

4.3.1 Fingerprint Verification

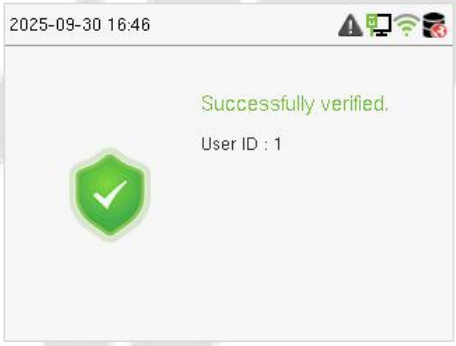
➢ **1: N Fingerprint Verification Mode**

The device compares the current fingerprint with the available fingerprint data stored in its database.

Fingerprint authentication mode is activated when a user places their finger onto the fingerprint scanner.

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

Verification is successful:



Verification is failed:

➢ **1:1 Fingerprint Verification Mode**

The device compares the current fingerprint with the fingerprints linked to the entered User ID through the virtual keyboard.

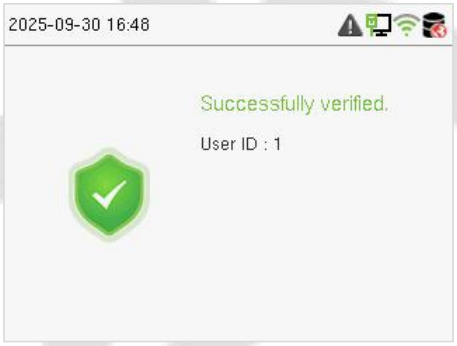
In case users are unable to gain access using the 1:N authentication method, they can attempt to verify their identity using the 1:1 verification mode.

Enter the user ID and tap [**M/OK**] to enter the 1:1 fingerprint verification mode.

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

Press the fingerprint to verify.

Verification is successful:



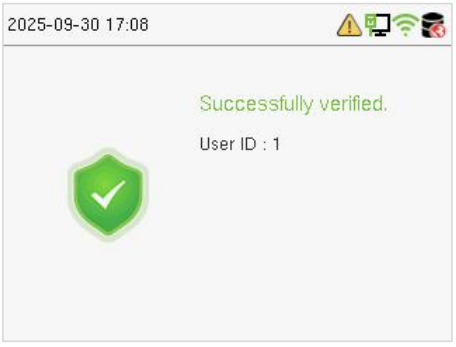
Verification is failed:

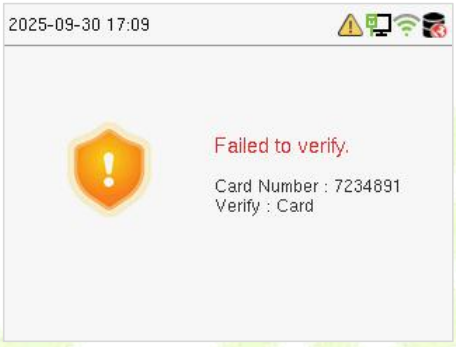
4.3.2 Card Verification

➢ **1: N Card Verification Mode**

The 1: N Card Verification Mode compares the card number in the card induction area with all the card number data registered in the device. The following screen displays on the card verification screen.

Verification is successful: Verification is failed:



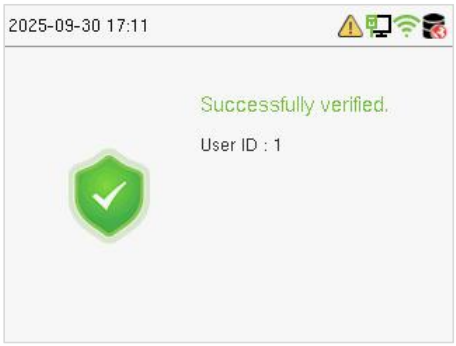


➢ **1:1 Card Verification Mode**

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

Enter the user ID and tap [**M/OK**] to enter the 1:1 card verification mode.

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

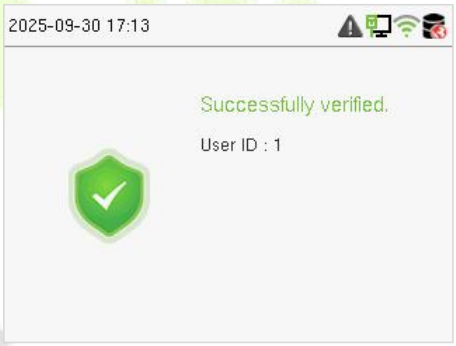


4.3.3 Password Verification

The device compares the entered password with the registered password and User ID.

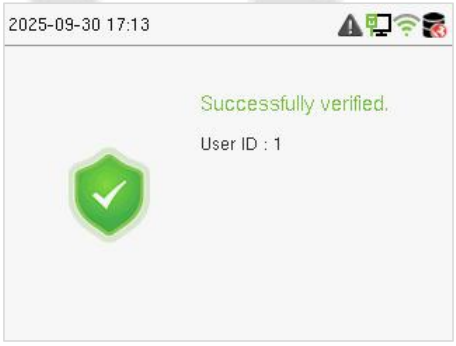
Enter the user ID and tap [**M/OK**] to enter the 1:1 password verification mode. Then, input the user ID and tap [**M/OK**].

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

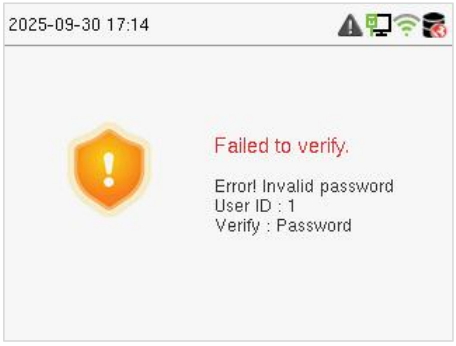


Below are the display screens after entering a correct password and a wrong password, respectively.

Verification is successful:



Verification is failed:

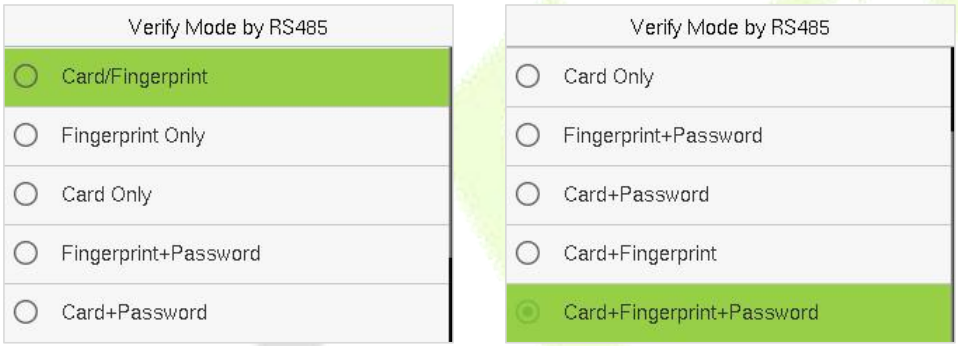


4.3.4 Combined Verification

This device allows you to use different types of verification methods to increase security. There are a total of 7 different verification combinations that can be implemented, as listed below:

Combined Verification Symbol Definition

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



Combined Verification Mode set up procedure:

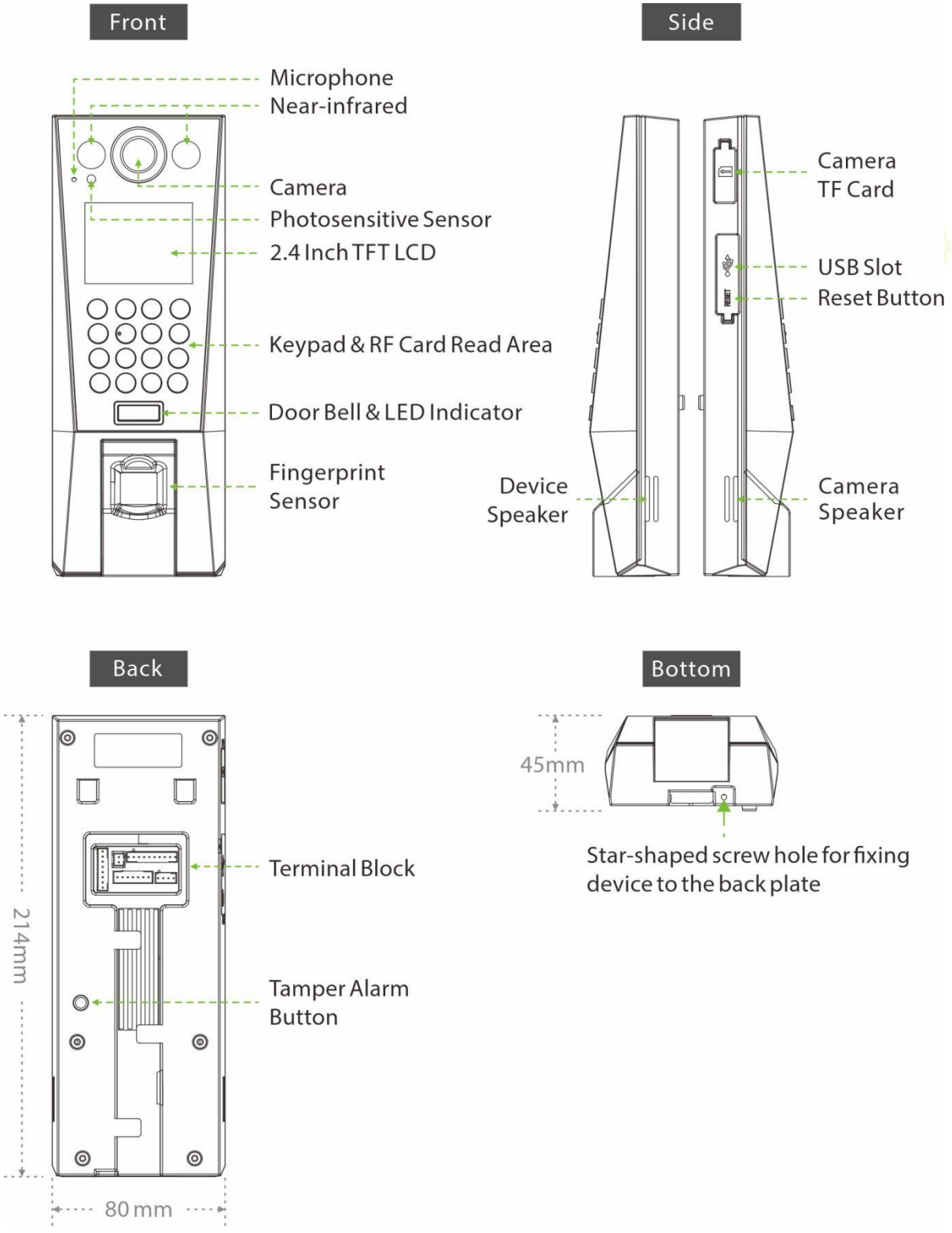
- Combined verification requires personnel to register all the different verification methods. Otherwise, employees will not be able to successfully verify the combined verification process.
- For example, if an employee has only registered for password data but the Device verification mode is set to "Password + Card", the employee will not be able to successfully complete the verification procedure.

Reason:

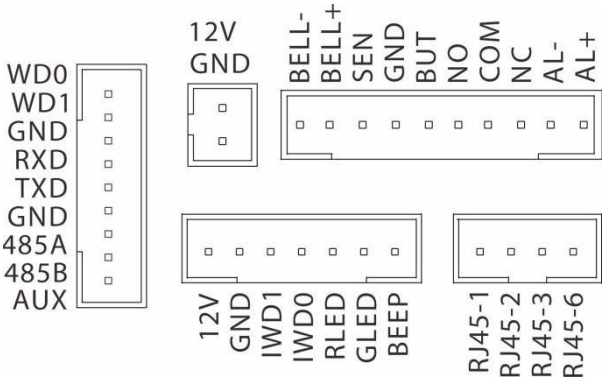
- This is because the Device compares the password template of the person with the registered verification template (both the Card and the Password) previously stored to that Personnel ID in the Device.
- But, since the employee has only registered their password and not their card, the verification process will not be successful, and the device will display the "Verification Failed."

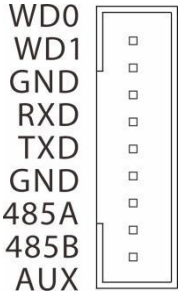
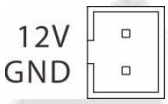
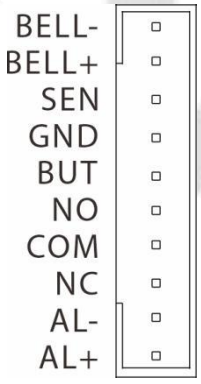
5 Overview

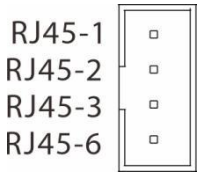
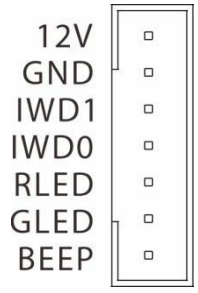
5.1 Appearance



5.2 Terminal Description



Interface	Description	
	WD0	Wiegand Out
	WD1	
	GND	
	RXD	RS232
	TXD	
	GND	
	485A	RS485
	485B	
	AUX	Auxiliary Input
	12V	12V Power in
	GND	
	BELL-	Bell
	BELL+	
	SEN	Door Sensor
	GND	
	BUT	Exit Button
	NO	Lock
	COM	
	NC	
	AL-	Alarm
	AL+	

	RJ45-1	Ethernet
	RJ45-2	
	RJ45-3	
	RJ45-6	
	12V	Power Out
	GND	
	IWD1	Wiegand In
	IWD0	
	RLED	Output
	GLED	
	BEEP	

5.3 Specifications

Model	F18 Pro
Display	2.4"@TFT Color LCD Screen(720*1280)
Camera	4MP CMOS
Operation System	Linux
Hardware	CPU: 1GHz Dual Core RAM: 128MB; ROM: 256MB Speaker *2 8Ω 1W Microphone: *1 (Sensitivity: 42dB ±3dB) Fingerprint Sensor: ZK Optical Sensor TF Card: Max 256GB
Authentication method	Fingerprint / Card / Password(Physical Keypad)
Fingerprint Template Capacity	3,000 (1: N)
Card Capacity	5,000 (1: N)
User Capacity	5,000 (1: N)
Transaction Capacity	100,000
Max. User Password Length	6 to 8 Digits
Fingerprint Verification Speed	less than 0.3 sec

False Acceptance Rate(FAR)%	FAR ≤ 0.0001%
False Rejection Rate (FRR)%	FRR ≤ 0.01%
Biometric Algorithm	ZKFingerprint V10.0/V13.0(Default)
Card Type	ID &IC Card @125kHz & 13.56MHz(Standard)
Communication	TCP/IP*1 Wi-Fi (IEEE 802.11 b/g/n) @ 2.4 GHz Wiegand (Input & Output)*1 RS485: ZKTeco RS485 *1 RS232: only for Printer*1(Optional) USB Host*1 Aux Inputs *1, Electric Lock*1, Door Sensor*1, Exit Button*1, Alarm*1, Doorbell*1
Standard Functions	ADMS, DST, Up to 14-digit User ID, Access Levels, Groups, Holidays, Anti-Passback, Record Query, Tamper Switch Alarm, Multiple Verification Methods, Video Intercom(Yoosee), AC Push and TA Pusch Protocol Switch, HTTPS / SSH Backend Access, T9 Keyboard (Input)
Infrared Supplement Light	Auto infrared light ON: < 2 lux (B/W image) Auto infrared light OFF: > 6 lux Visible light mode: ≥ 6 lx (Color image)
FOV	Diagonal: 154.8°, Horizontal: 134.7°, Vertical: 77.6°
Video Intercom and Video Cloud Storage	
Video Intercom	Support Yoosee Mobile App Communication: Yoosee private protocol Functions: live view, bi-directional talk, remote unlock
Cloud Service	Gwell cloud for video storage and analytics notifications
Video Storage	Gwell Cloud Service; Local storage with the SD Card (up to 256GB)
Video Compression	H.265,15fps
Visible Range	Up to 5m (Day & Night; Infrared)
Video Resolution	2560*1440
Video Viewing Angle	154.8(Diagonal), 77.6°(vertical), 134.7° (horizontal)
Infrared Supplement Light	Auto infrared light ON: < 2 lux (low light environment; B/W image) Auto infrared light OFF: > 6 lux Visible light mode: ≥ 6 lux (Day light; Color image)

Intelligent Video Analytics (IVA)	
IVA Camera	Human Detection/ Motion Detection / Vehicle Detection / Flame Detection
IVA Video	Intelligent retrieval, online surveillance Maximum 10 mins, playback and backup. (Video Storage: Gwell cloud; local TF card up to 256 GB)
Intelligent IVA Alarm	Human Detection / Motion Detection/ Vehicle Detection / Flame Detection
Alarm Delay	less than 3 sec
Minimum Detection Area	50x50 pixels
False Alarm Suppression	N/A
Sensitivity Adjustable	N/A
Networking &Interfaces	Wireless: Dual-band WiFi 6 (IEEE 802.11 a/b/g/n/ac/ax), 2.4/5GHz; Ethernet*1 Bluetooth 5.0
Power Supply	DC 12V 3A
Operating Temperature	-10C to 45C (14 F to 113 F)
Operating Humidity	10% to 90% RH (Non-condensing)
Dimensions	214 mm*80 mm*45 mm (L*W*H)
Gross Weight	0.75 Kg
Net Weight	0.38 Kg
Supported Software	Software: ZKBio CVAccess / ZKBio Time Mobile App: Yoosee Cloud Storage: Gwell
Installation	Wall-mount (Compatible with Asian Gang-box / Single Gang-Box / European Gang-Box)
Housing Material	ABS (black)
Ingress Protection Rating	N/A
Certifications	ISO14001, ISO9001, CE, FCC, RoHS
Factory ID	AC01-F28H-12

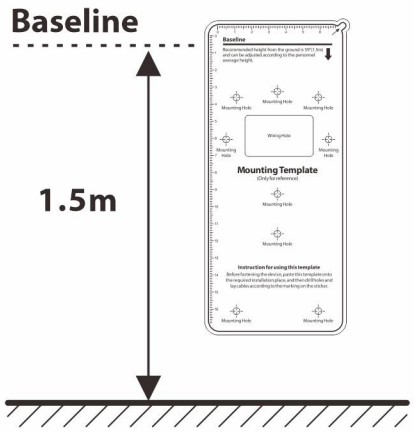
6 Installation and Wiring

6.1 Installation of Wall-mount

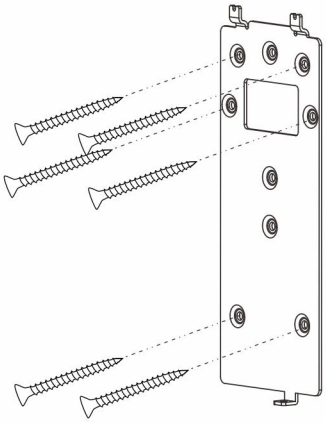
Before the installation, please connect the cables to the connectors.

1. Attach the mounting template to the wall and drill holes accordingly.
2. Fix the back plate on the wall using the provided mounting screws.
3. Mount the device on the back plate.
4. Secure the device and back plate.

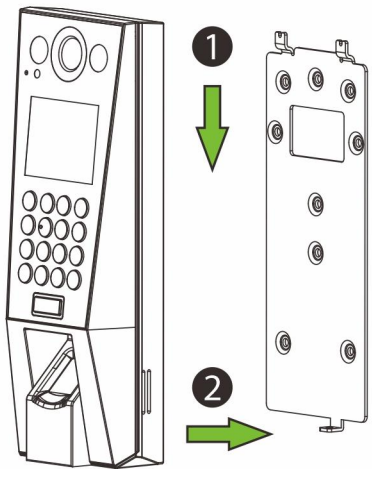
1



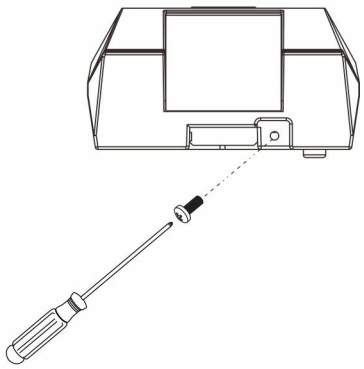
2



3

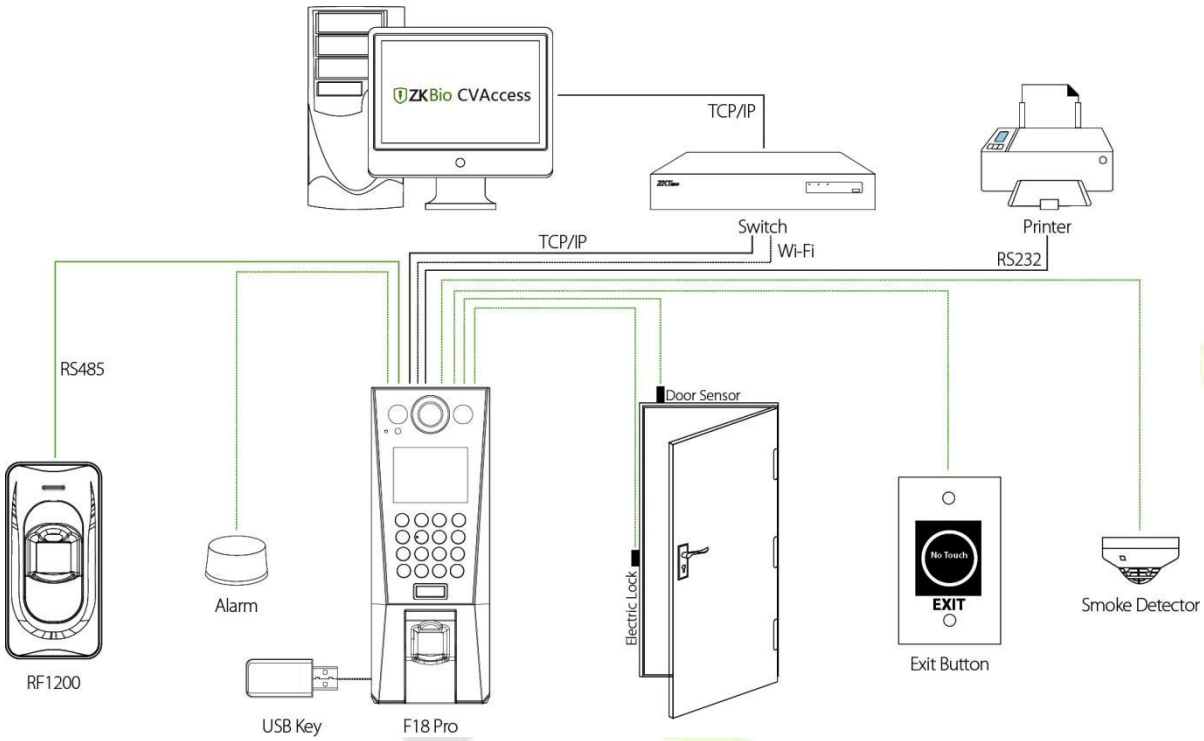


4

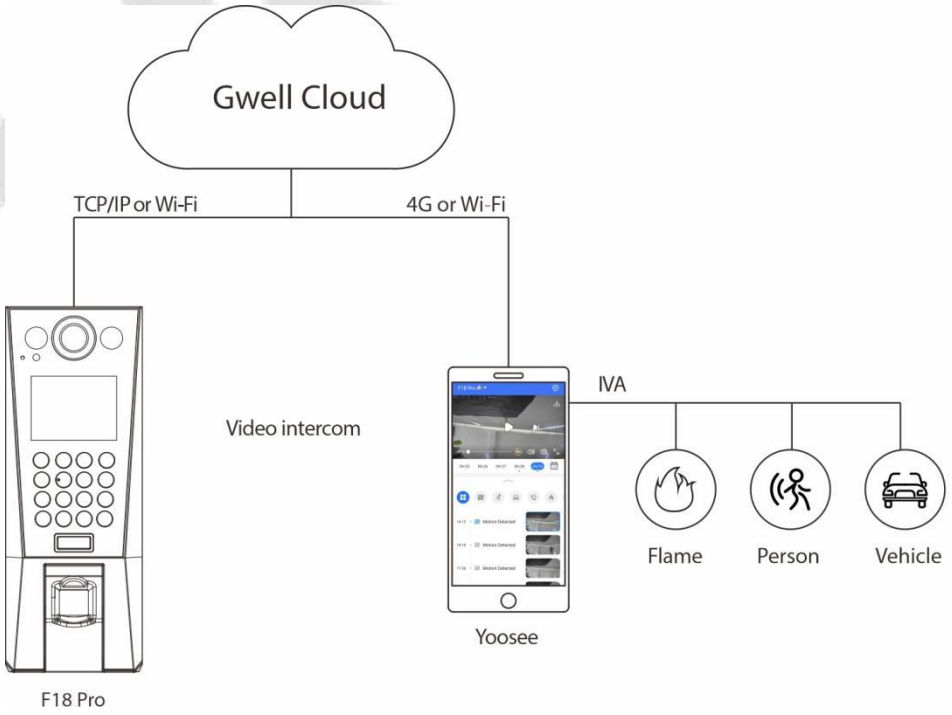


6.2 Wiring Diagram

Access Control:



IVA & Video Intercom:



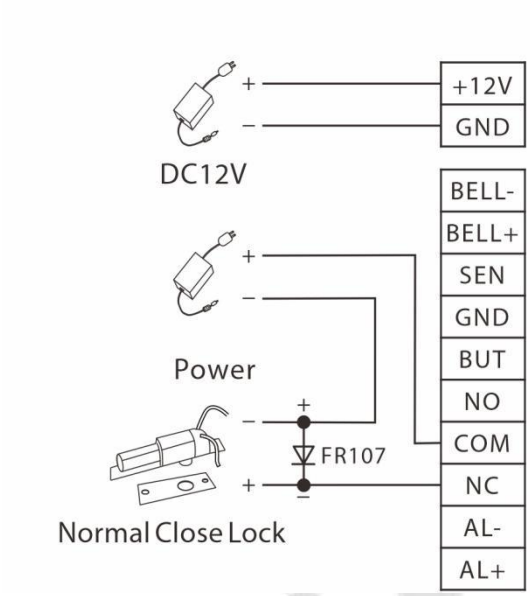
6.2.1 Lock Connection

The system supports Normally Opened Lock and Normally Closed Lock.

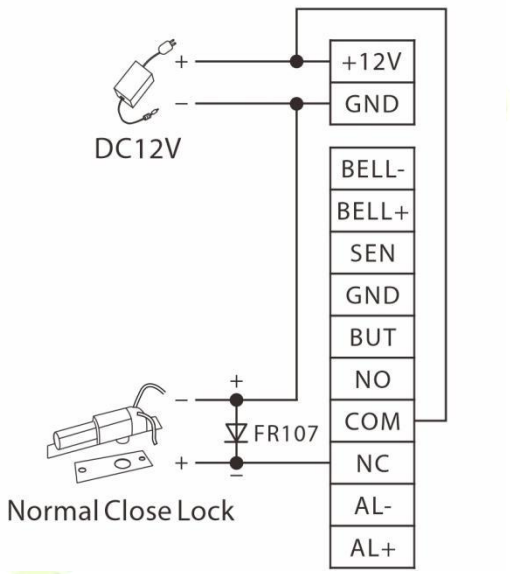
The NO LOCK (normally opened at power on) is connected with 'NO' and 'COM' terminals, and the NC LOCK (normally closed at power on) is connected with 'NC' and 'COM' terminals.

Take NC Lock as an example below:

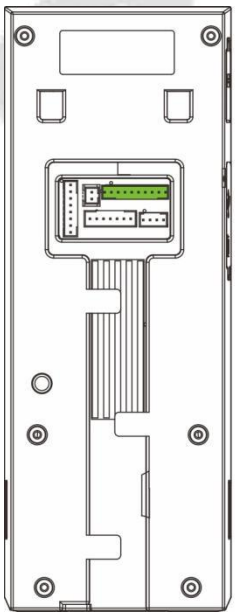
1) Device not sharing power with the lock:

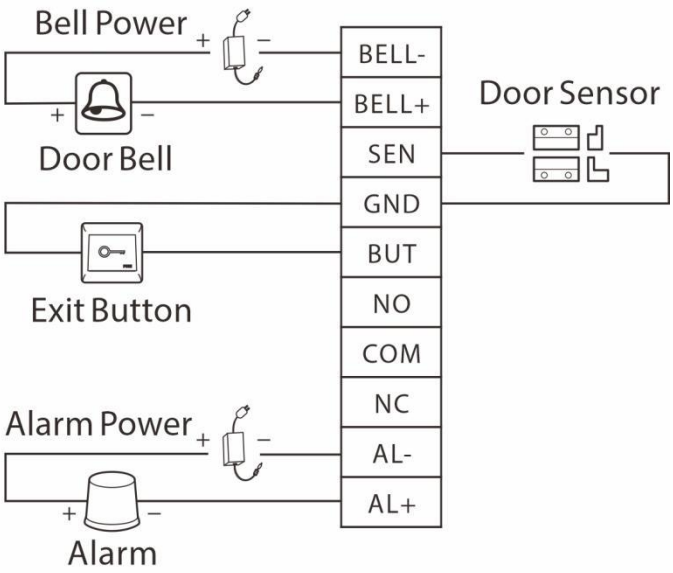


2) Device sharing power with the lock:

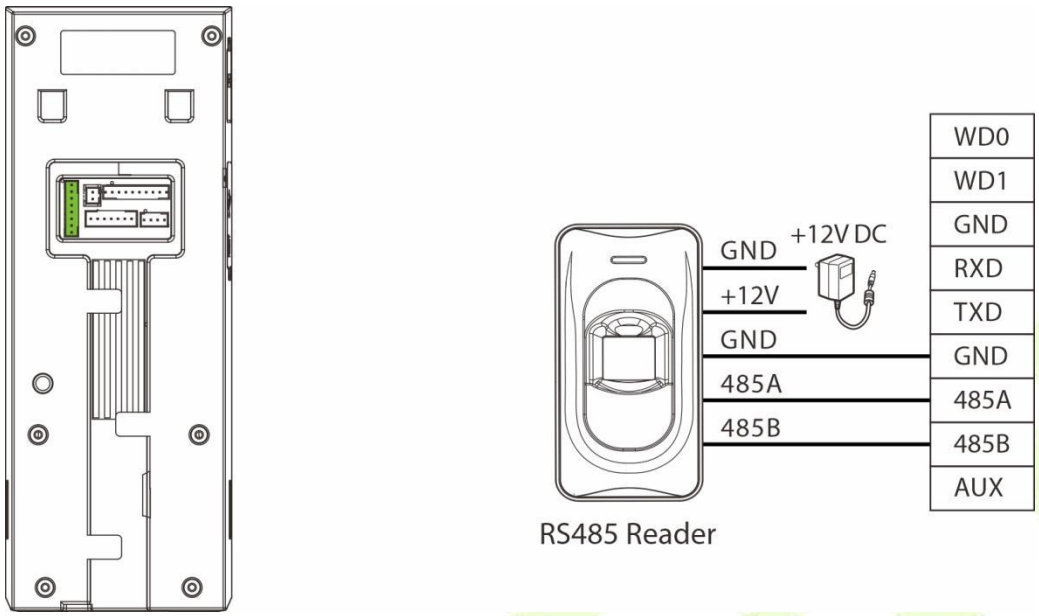


6.2.2 Door Bell & Door Sensor & Exit Button & Alarm Connection



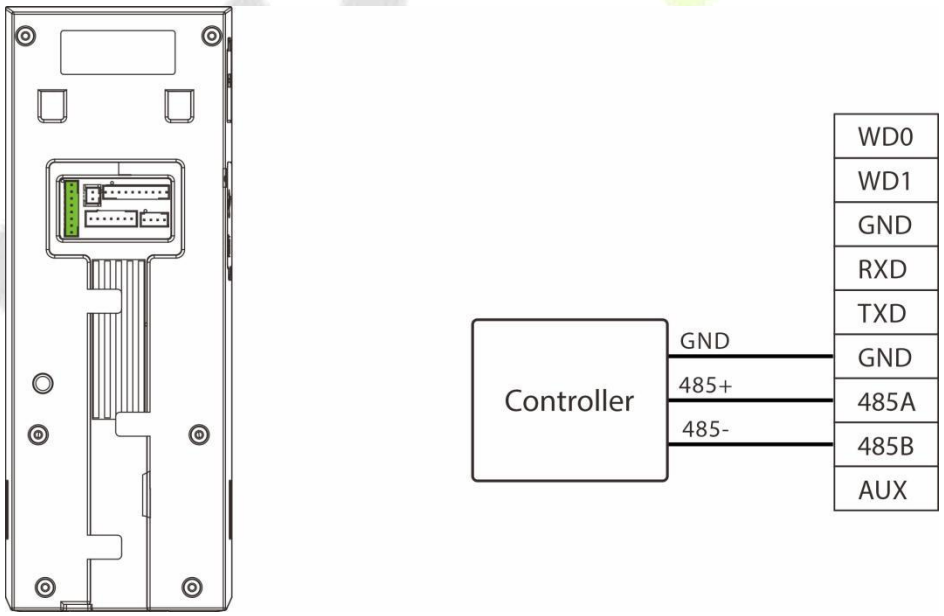


6.2.3 RS485 Reader Connection



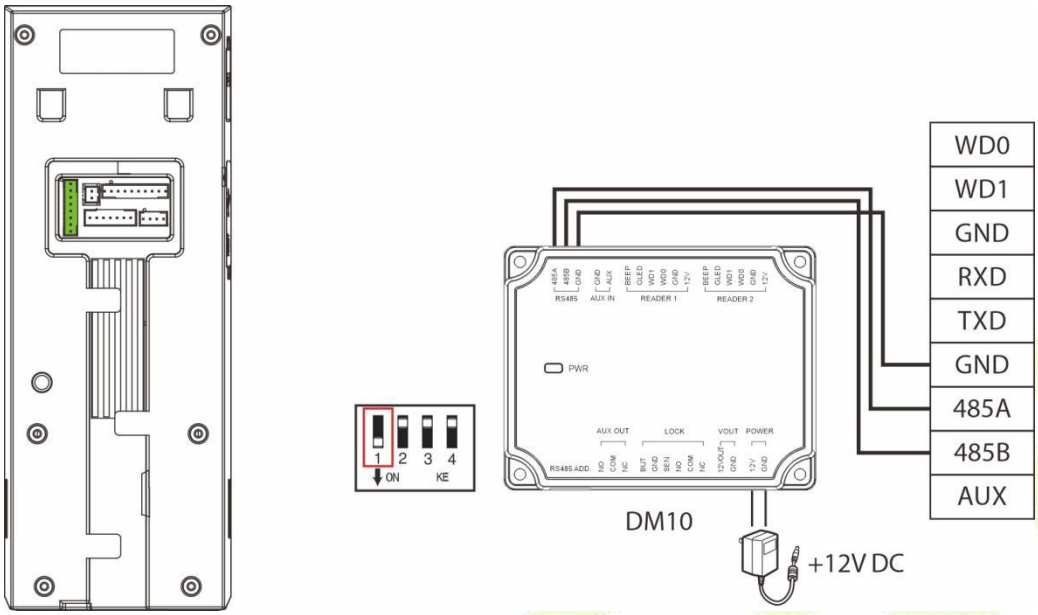
Note: Press **M/OK** on the initial interface. Select **COMM.** > **Serial Comm** > **Serial Port**, then set the serial port to **Primary Unit**.

6.2.4 Controller Connection



Note: Press **M/OK** on the initial interface. Select **COMM.** > **Serial Comm** > **Serial Port**, then set the serial port to **OSDP Secondary Unit**. The device will be used as a sub device.

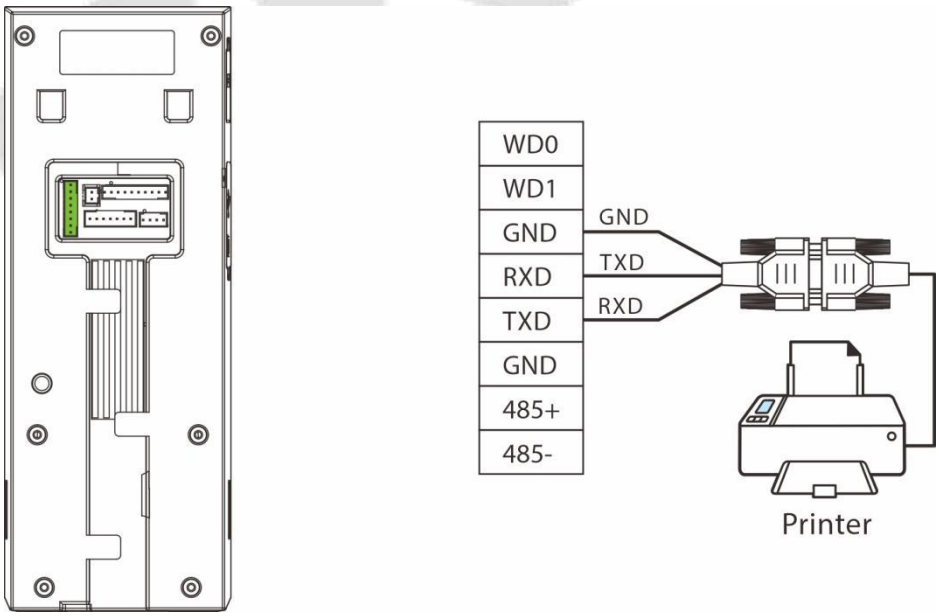
6.2.5 DM10 Connection



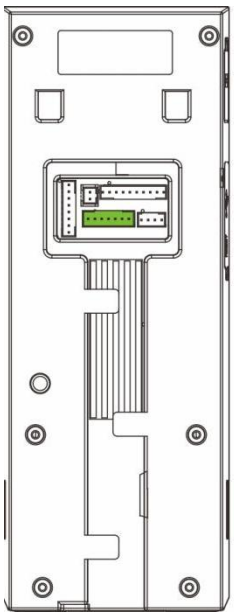
Notes:

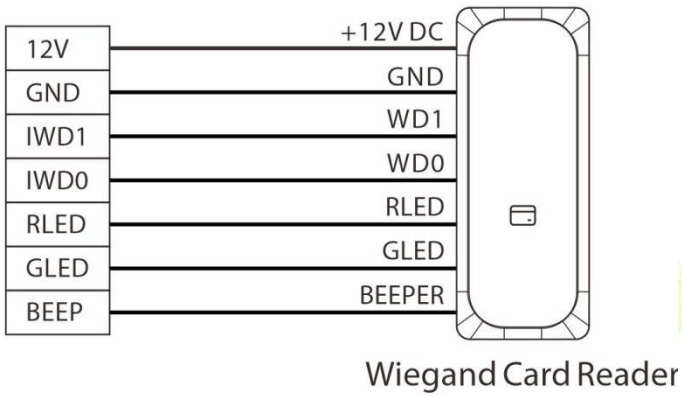
1. Press **M/OK** on the initial interface. Select **COMM.** > **Serial Comm** > **Serial Port**, then set the serial port to **DM10**.
2. When connecting to DM10, slide the DIP switch position **1** to the **ON** position.
3. DM10 requires a separate power supply.

6.2.6 RS232 Connection

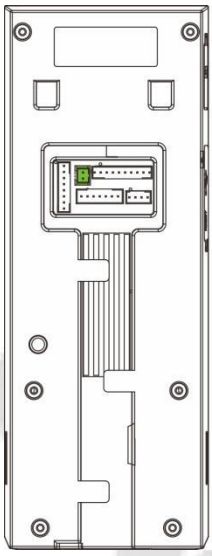


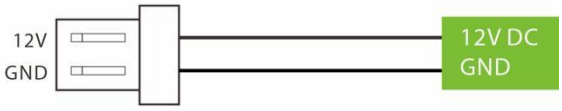
6.2.7 Wiegand Reader Connection





6.2.8 Power Connection

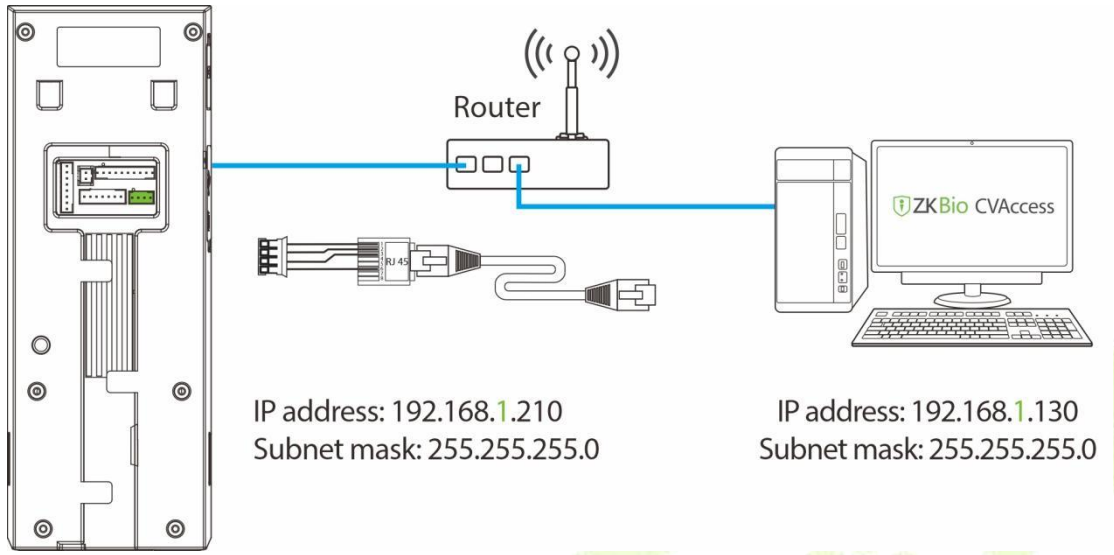




Recommended power supply:

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

6.2.9 Ethernet Connection

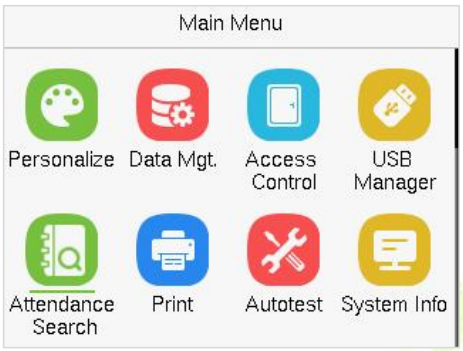


The device defaults to enabling DHCP functionality and does not support disabling DHCP. It can only obtain an IP address and connect to the network by connecting to a router.

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

7 Main Menu

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



Function Description

Menu	Description
User Mgt.	To Add, Edit, View, and Delete information of a User.
User Role	To set the permission scope of the custom role, for example the system's operating rights.
COMM.	To set the relevant parameters of Network, Serial Comm., PC Connection, Wi-Fi, Cloud Server, Wiegand and Network Diagnosis.
System	To set parameters related to the system, including Date Time, Attendance/ Access Logs Settings, Fingerprint, Video Intercom Parameters, Device Type Settings, Security Settings, USB Upgrade, Update Firmware Online and resetting to factory settings.
Personalize	To customize settings of User Interface, Voice, Bell Schedules, Punch State Options and Shortcut Key Mappings settings.
Data Mgt.	To delete all relevant data in the device.
Access Control	To set the parameters of the lock and the relevant access control device including options like Time Rule Settings/Time schedule, Holiday Settings, Access groups, Combine verification, Anti-Passback Setup, and Duress Option Settings.
USB Manager	To upload or download the specific data by a USB drive.
Attendance Search	To query the specified event logs.
Print	To set printing information and functions. Only used in TA push.
Autotest	To automatically test whether each module functions properly, including the LCD Screen, Voice, Keyboard, fingerprint sensor and Real-Time Clock.
System Info	To view Privacy Policy, Data Capacity and Device and Firmware information of the current device.

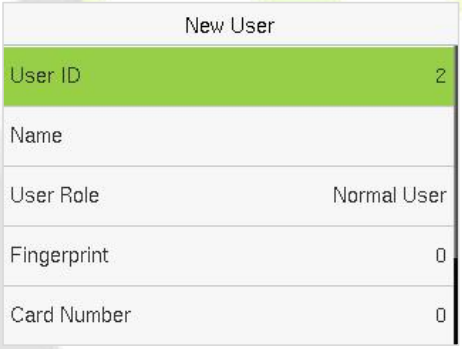
8 User Management

8.1 New User Registration

When the device is on the initial interface, press [**M/OK**] button > **User Mgt.** > **New User**.

8.1.1 Register a User ID and Name

Enter the **User ID** and **Name**.



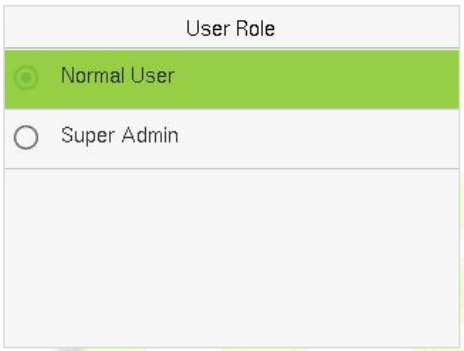
Notes:

1. A name can be taken up to 36 characters long.
2. The user ID may contain 1 to 14 digits by default, supporting both numbers and alphabetic characters.
3. During the initial registration, you can modify your ID, but not after registration.
4. If the message "**Duplicated!**" appears, you must choose a different User ID because the one you entered already exists.

8.1.2 User Role

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

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

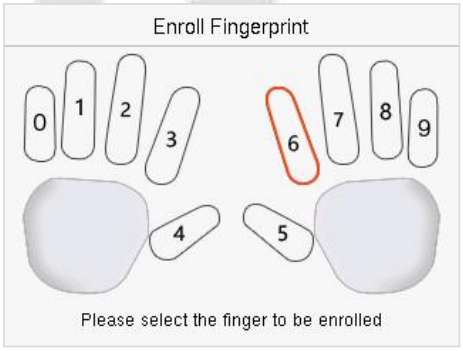


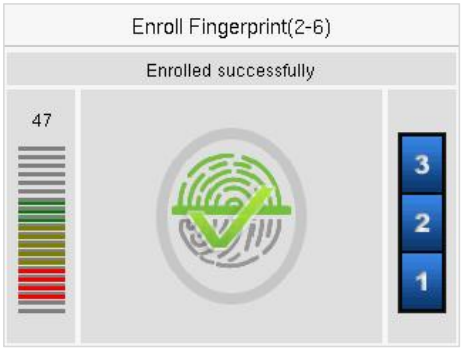
Note: If the selected user role is the Super Admin, then the user must pass the identity authentication to access the main menu. The authentication is based on the authentication method(s) that the super administrator has registered.

8.1.3 Register Fingerprint

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

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

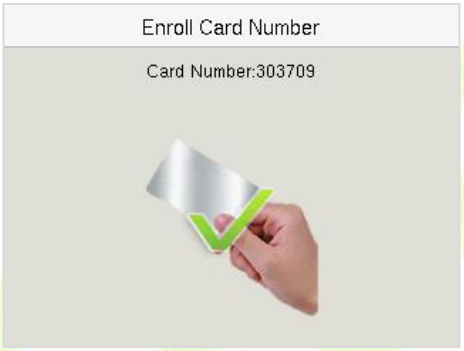




8.1.4 Card Number

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

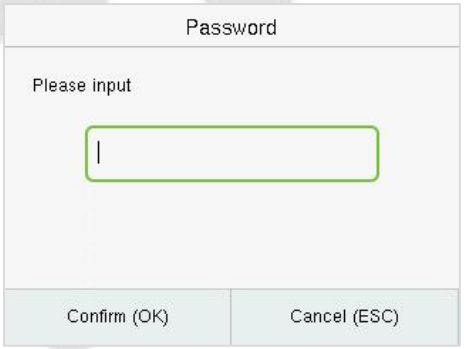
- On the card interface, swipe the card under the card reading area. The registration of the card will be successful.
- If the card has already been registered, the message "**Error! Card already enrolled**" appears. The registration interface appears as follows:

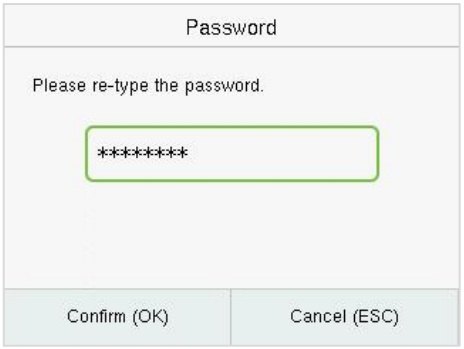


8.1.5 Password

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

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





8.1.6 Access Control Role

The **Access Control Role** sets the door access privilege for each user. It includes the access group, time period and duress fingerprint.

- Tap **Access Control Role** > **Access Group** to assign the registered users to different groups for better management. New users belong to Group 1 by default and can be reassigned to other groups. The device supports up to 99 Access Control groups.
- By selecting the **Verification 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.
- The user may specify one or more fingerprints that have been registered as a duress fingerprint(s). When press the finger corresponding to the duress fingerprint on the sensor and pass the verification, the system will immediately generate a duress alarm.
- Tap **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.

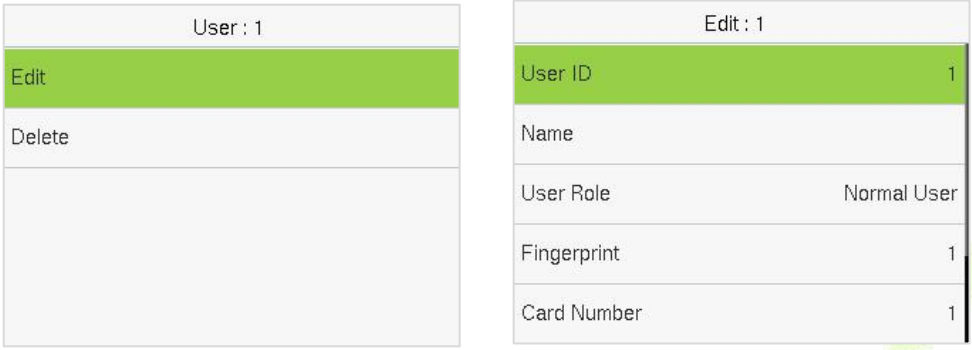
8.2 All Users

When the device is on the initial interface, press [**M/OK**] button > **User Mgt.** > **All Users**.

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

8.2.1 Edit User

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



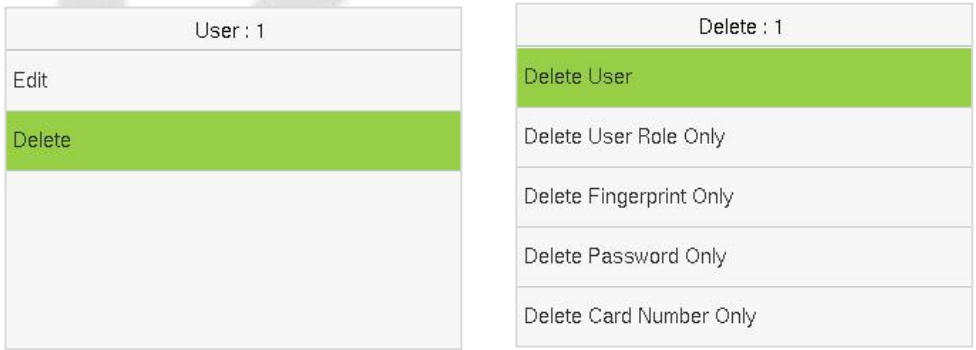
Note: The process of editing the user information is the same as adding a new user, except that the User ID cannot be modified while editing a user. The process in detail refers to "User Registration".

8.2.2 Delete User

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

Delete Operations:

- **Delete User:** Deletes all the user information (deletes the selected User as a whole) from the Device.
- **Delete User Role Only:** Deletes the user's administrator privileges and make the user a normal user.
- **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 information of the selected user.

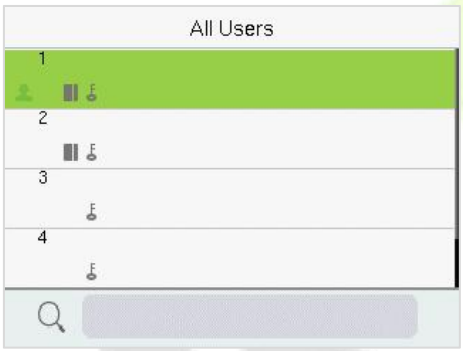


8.3 Display Style

When the device is on the initial interface, press [**M/OK**] button > **User Mgt.** > **Display Style**.

All the Display Styles are shown as below:

Multiple Line:

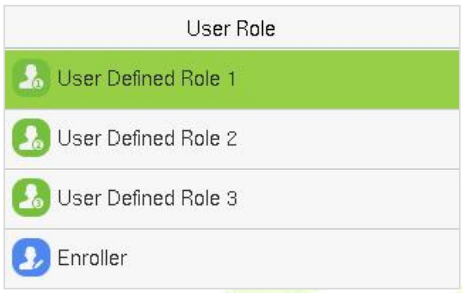


Mixed Line:

9 User Role

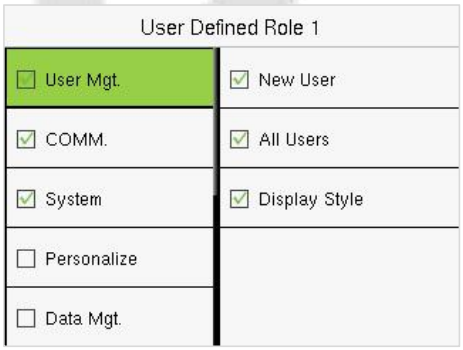
User Role allows you to assign specific permissions to certain users based on their requirements.

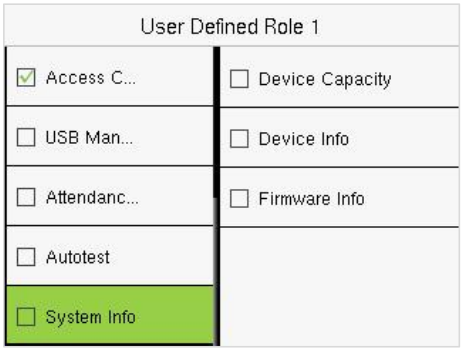
- When the device is on the initial interface, press [**M/OK**] button > **User Role** > **User Defined Role** to set the user defined permissions.
- The permission scope of the custom role can be set up into 3 roles, that is, the custom operating scope of the menu functions of the user.



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

- Then, by selecting on Define User Role, select the required privileges for the new role, and then tap the [**M/OK**] button.
- When assigning privileges, the main menu function names will be displayed on the left and its sub-menus will be listed on the right.
- First tap on the required **Main Menu** function name, and then select its required sub-menus from the list.



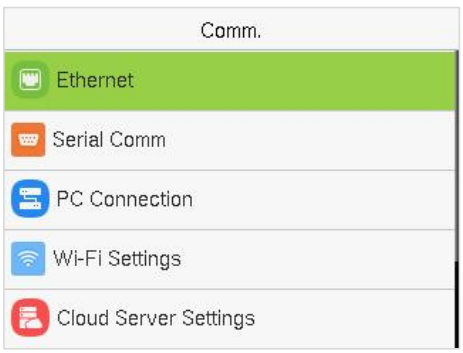


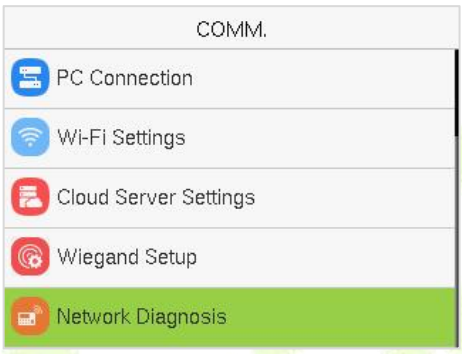
Note: If the User Role is enabled for the Device, tap on **User Mgt. > New User > User Role** to assign the created roles to the required users. But if there is no super administrator registered in the Device, then the device will prompt "**Please enroll super admin first!**" when enabling the User Role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

10 Communication

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

When the device is on the initial interface, press [**M/OK**] button > **COMM.**



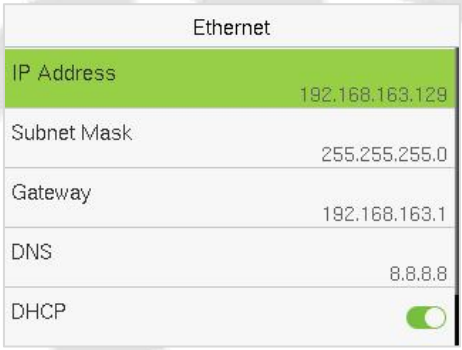


Notes: The F18 Pro can only use DHCP to obtain dynamic IP address; static IP configuration is not supported. The dynamic IP address assigned via DHCP (over Ethernet or 2.4 GHz Wi-Fi) must have direct access to the public Internet. Without Internet access, the device cannot communicate with Gwell Cloud.

10.1 Ethernet

The device defaults to enabling DHCP functionality and does not support disabling DHCP. It can only obtain an IP address and connect to the network by connecting to a router.

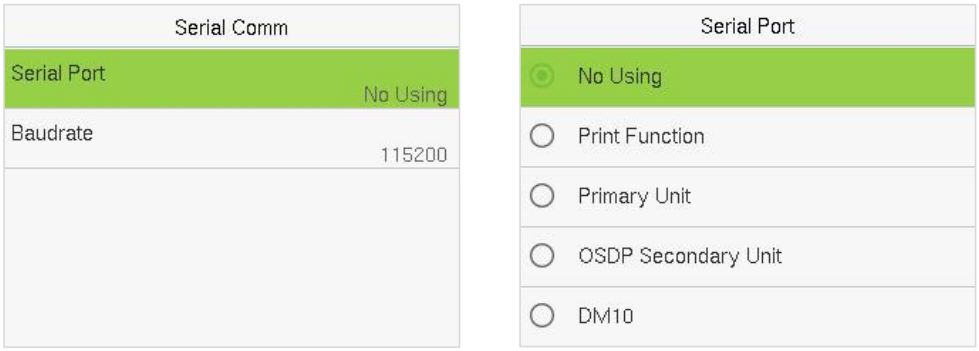
Tap **Ethernet** on the **COMM.** Settings interface to enter the settings interface.



10.2 Serial Comm

Serial Comm function establishes communication with the device through a serial port (Primary Unit/ OSDP Secondary Unit/DM10).

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



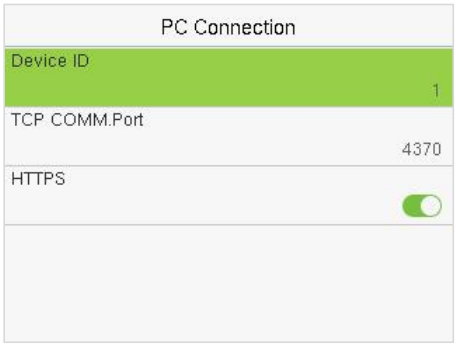
Function Description

Function Name	Description
Serial Port	**No Using:** No communication with the device through the serial port. **Print Function:** The device can be connected to the printer when RS232 enables the print function. **Primary Unit:** When RS485 is used as the function of "**Primary Unit**", it can be connected to a reader. **OSDP Secondary Unit:** When RS485 is used as the function of "**OSDP Secondary Unit**", it can be connected to a controller. **DM10:** When RS485 is used as the function of "**DM10**", it can be connected to DM10 to control the lock relay. (**Note:** When selecting DM10 or switching from DM10 to other option, the device will restart to take effect.)
Baudrate	When the serial port is set as **Primary Unit** or **DM10**, the baudrate is 115200 by default and cannot be modified. When the serial port is set as **OSDP Secondary Unit**, there are 5 baudrate options. They are: 115200 (default), 57600, 38400, 19200 and 9600. When the serial port is set as **Print Function**, there are 5 baudrate options. They are: 115200 (default), 57600, 38400, 19200 and 9600. The higher the baudrate, the faster is the communication speed, but also less reliable. Hence, a higher baudrate can be used when the communication distance is short; when the communication distance is long, choosing a lower baudrate is more reliable.

10.3 PC Connection

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

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



Function Description

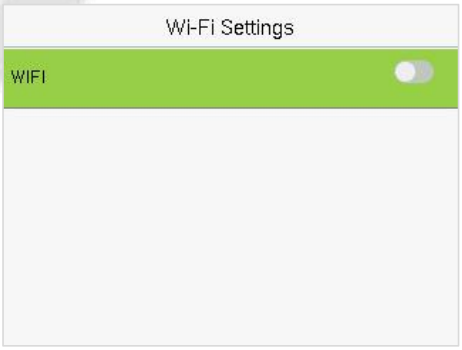
Function Name	Description
Device ID	It is the identification number of the device, which ranges between 1 and 254.
TCP COMM.Port	The default TCP COMM Port value is 4370. It can be modified according to the network availability.
HTTPS	Based on HTTP, transmission encryption and identity authentication ensure the security of the transmission process.

10.4 Wi-Fi Settings

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

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

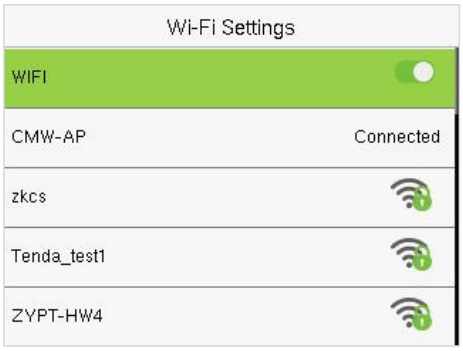
Tap **Wi-Fi Settings** on the **COMM.** Settings interface to configure the Wi-Fi settings.



➢ **Searching the Wi-Fi Network**

- Wi-Fi is enabled in the device by default. Toggle the button to enable or disable Wi-Fi.
- Once the Wi-Fi is turned on, the device will search for the available Wi-Fi within the network range.

- Tap on the required Wi-Fi name from the available list and input the correct password in the password interface, and then tap [**M/OK**].



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

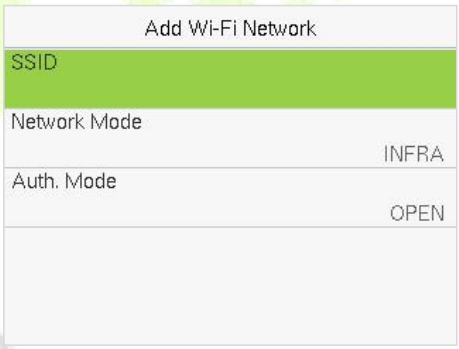
Tap on the password field to enter the password and tap [**M/OK**].

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

➢ **Adding Wi-Fi Network Manually**

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

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



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

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

➢ **Advanced Setting**

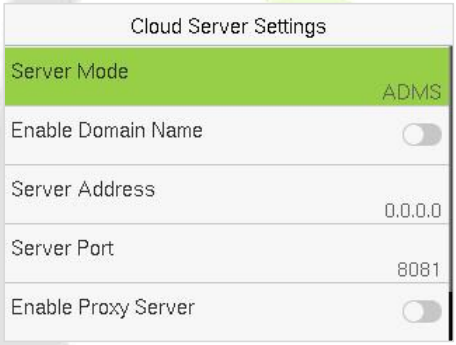
On the **Wi-Fi Settings** interface, tap on **Advanced** to set the relevant parameters as required.

Function Description

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

10.5 Cloud Server Settings

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



Function Description

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

10.6 Wiegand Setup

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

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

10.6.1 Wiegand Input

Function Description

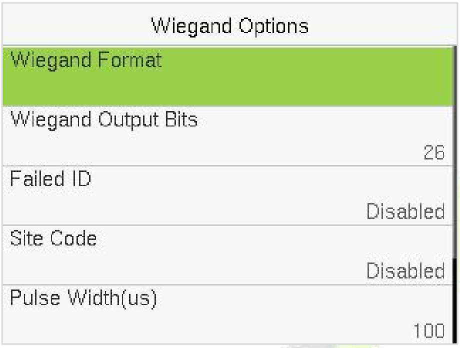
Function Name	Description
Wiegand Format	Its value can be 26 bits, 34 bits, 36 bits, 37 bits, 50 bits and 64 bits.
Wiegand Bits	The number of bits of the Wiegand data.
Pulse Width(us)	The value of the pulse width sent by Wiegand is 100 microseconds by default, which can be adjusted within the range of 20 to 400 microseconds.
Pulse Interval(us)	The default value is 1000 microseconds and can be adjusted within the range of 200 to 20000 microseconds.
ID Type	Select between the User ID and card number.

Various Common Wiegand Format Description:

Wiegand Format	Description
Wiegand26	ECCCCCCCCCCCCCCCCCCCCCCCCO It consists of 26 bits of binary code. The 1st bit is the even parity bit of the 2nd to 13th bits, while the 26th bit is the odd parity bit of the 14th to 25th bits. The 2nd to 25th bits 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	EFFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCO It consists of 36 bits of binary code. The 1st bit is the even parity bit of the 2nd to 18th bits, while the 36th bit is the odd parity bit of the 19th to 35th bits. The 2nd to 19th bits is the device codes, and the 20th to 35th bits are the card numbers.
Wiegand37	OMMMMSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCE It consists of 37 bits of binary code. The 1st bit is the odd parity bit of the 2nd to 18th bits, while the 37th bit is the even parity bit of the 19th to 36th bits. The 2nd to 4th bits is the manufacturer codes. The 5th to 16th bits is the site codes, and the 21st to 36th bits are the card numbers.
Wiegand37a	EMMMFFFFFFFFFSSSSSSCCCCCCCCCCCCCCCCO It consists of 37 bits of binary code. The 1st bit is the even parity bit of the 2nd to 18th bits, while the 37th bit is the odd parity bit of the 19th to 36th bits. The 2nd to 4th bits is the manufacturer codes. The 5th to 14th bits is the device codes, and15th to 20th bits are the site codes, and the 21st to 36th bits are the card numbers.
Wiegand50	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.

Wiegand64	ECCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC CCCCCO It consists of 64 bits of binary code. The 1st bit is the even parity bit of the 2nd to 32nd bits, while the 64th bit is the odd parity bit of the 33rd to 63rd bits. The 2nd to 63rd bits are the card numbers.
"C" denotes the card number; **"E"** denotes the even parity bit; **"O"** denotes the odd parity bit. **"F"** denotes the facility code; **"M"** denotes the manufacturer code; **"P"** denotes the parity bit; and **"S"** denotes the site code.	

10.6.2 Wiegand Output



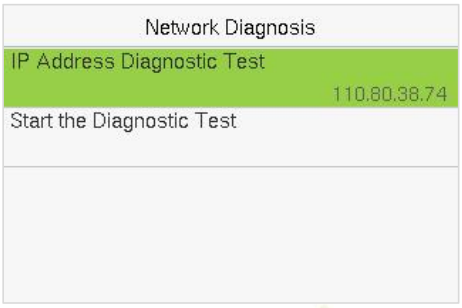
Function Description

Function Name	Description
Wiegand Format	Its value can be 26 bits, 34 bits, 36 bits, 37 bits, 50 bits and 64 bits.
Wiegand Output Bits	After selecting the required Wiegand format, select the corresponding output bit digits from the Wiegand format.
Failed ID	If the verification fails, the system will send the failed ID to the device and replace the card number or personnel ID with the new one.
Site Code	It is similar to the device ID. The difference is that a site code can be set manually and is repeatable on a different device. The valid value ranges from 0 to 256 by default.
Pulse Width(us)	The time width represents the changes in the quantity of electric charge with regular high-frequency capacitance within a specified time.
Pulse Interval(us)	The time interval between pulses.
ID Type	Select the ID types as either User ID or card number.

10.7 Network Diagnosis

It helps to set the network diagnosis parameters.

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

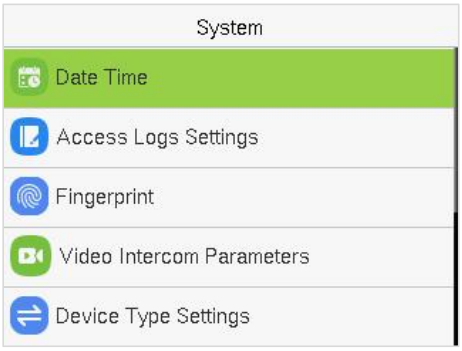


11 System Settings

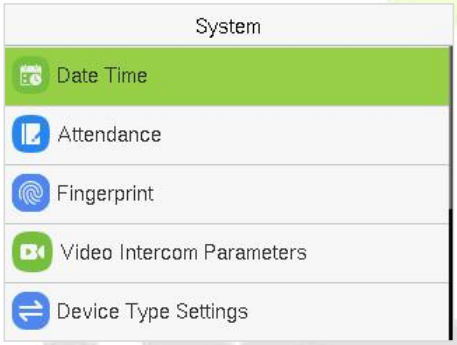
It helps to set related system parameters to optimize the accessibility of the device.

When the device is on the initial interface, press [**M/OK**] button > **System.**

Access Control Terminal:

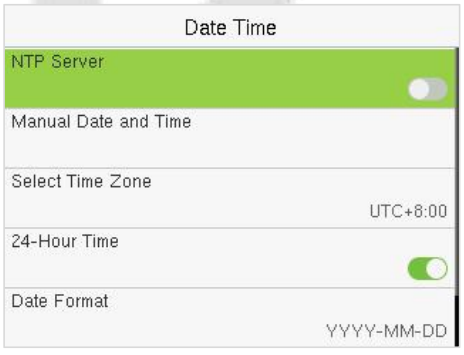


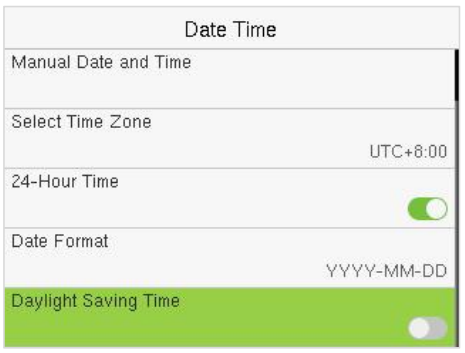
Time Attendance Terminal:



11.1 Date and Time

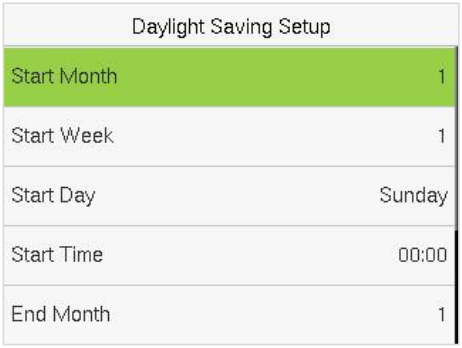
Tap **Date Time** on the **System** interface to set the date and time.





- Tap **NTP Server** to enable automatic time synchronization based on the service address you enter.
- Tap **Manual Date and Time** to manually set the date and time and then tap **Confirm** and save.

- Tap **Select Time Zone** to manually select the time zone where the device is located.
- Enable or disable this format by tapping 24-Hour Time. If enabled, then select the **Date Format** to set the date.
- Tap **Daylight Saving Time** to enable or disable the function. If enabled, tap **Daylight Saving Mode** to select a daylight-saving mode and then tap **Daylight Saving Setup** to set the switch time.



Week Mode

Date Mode

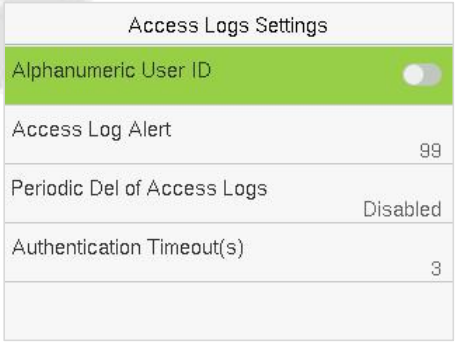
- When restoring the factory settings, the time (24-hour) and date format (YYYY-MM-DD) can be restored, but the device date and time cannot be restored.

Note: For example, if a user sets the time of the device from 18:35 on March 15, 2024 to 18:30 on January 1, 2025. After restoring the factory settings, the time of the device will remain at 18:30 on January 1, 2025.

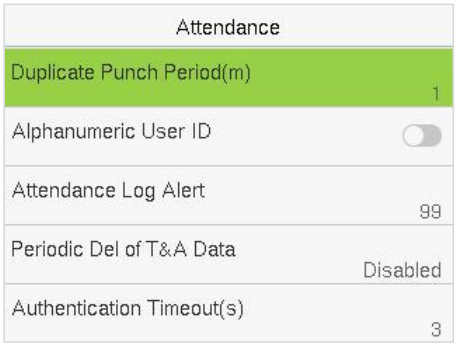
11.2 Access Logs Settings / Attendance

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

Access Control Terminal:



Time Attendance Terminal:



Function Description of Access Control Terminal:

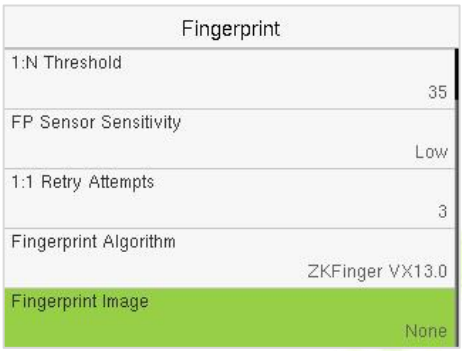
Function Name	Description
Alphanumeric User ID	Enable/Disable the alphanumeric as User ID.
Access Log Alert	When the record space of the attendance access reaches the maximum threshold value, the device automatically displays the memory space warning. Users may disable the function or set a valid value between 1 and 9999.
Periodic Del of Access Logs	When access logs reach its maximum capacity, the device automatically deletes a set of old access logs. Users may disable the function or set a valid value between 1 and 999.
Authentication Timeout(s)	The amount of time taken to display a successful verification message. Valid value: 1 to 9 seconds.

Function Description of Time Attendance Terminal:

Function Name	Description
Duplicate Punch Period(m)	Within a set time period (unit: minutes), the duplicated attendance record will not be reserved (value ranges from 1 to 999999 minutes).
Alphanumeric User ID	Enable/Disable the alphanumeric as User ID.
Attendance Log Alert	When the record space of the attendance reaches the maximum threshold value, the device automatically displays the memory space warning. Users may disable the function or set a valid value between 1 and 9999.
Periodic Del of T&A Data	When attendance records reach its maximum storage capacity, the device automatically deletes a set of old attendance records. Users may disable the function or set a valid value between 1 and 999.
Authentication Timeout(s)	The amount of time taken to display a successful verification message. Valid value: 1 to 9 seconds.

11.3 Fingerprint

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

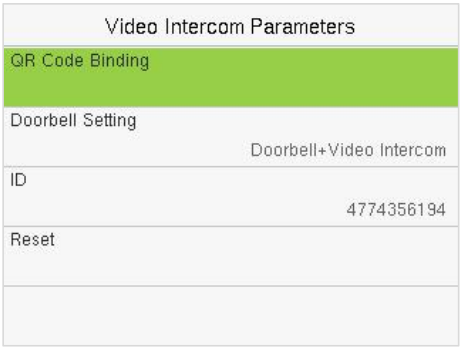


Function Description

Function Name	Description
1:1 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 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 Attempts	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	Fingerprint algorithm version. Default support ZKFinger VX13.0, can change to ZKFinger VX10.0. Switching fingerprint algorithms will clear the data.
Fingerprint Image	To set whether to display the fingerprint image on the screen during fingerprint enrollment or verification. Four choices are available: **Show for Enroll:** to display the fingerprint image on the screen only during enrollment. **Show for Match:** to display the fingerprint image on the screen only during verification. **Always Show:** to display the fingerprint image on screen during enrollment and verification. **None:** not to display the fingerprint image.

11.4 Video Intercom Parameters

Tap **Video Intercom Parameters** on the **System** interface.

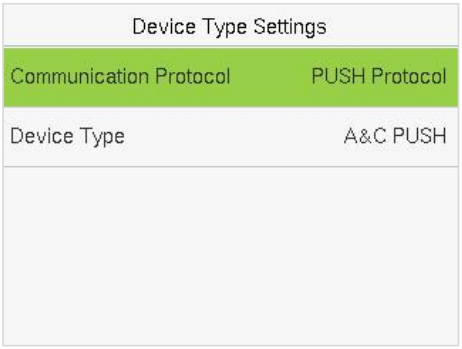


Function Description

Function Name	Description
QR Code Binding	Use the Yoosee App client to scan the QR code to connect and bind the device.
Doorbell Setting	Used to configure the doorbell button function on the device. **Doorbell Only:** Press the doorbell button on the device while on the standby interface, and the doorbell will ring. **Video Intercom Only:** Press the doorbell button on the device while on the standby interface to initiate a video intercom call to the mobile app side. **Doorbell + Video Intercom:** Press the doorbell button on the device while on the standby interface, and the doorbell will ring while initiating a video intercom call to the mobile app.
ID	Corresponding to the camera ID on the Yoosee app.
Reset	Reset the intercom module. ***Notes:*** 1) When User A has bound a device and needs to switch to User B binding that device, this reset function can unbind User A's device, allowing User B to rebind it. 2) When User A's device remains unbound, if User B attempts to scan the device's QR code to bind it directly, the app interface will display the prompt: "This device has not been reset. Please reset it and try again." Users must press the reset button to reset the video intercom module before re-binding the device.

11.5 Device Type Settings

Tap **Device Type Setting** on the **System** interface to configure the Device Type Settings.



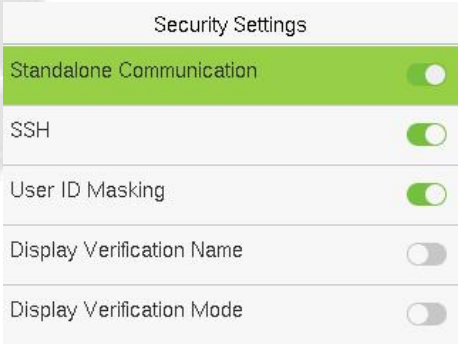
Function Description

Function Name	Description
Communication Protocol	Set the PUSH protocol.
Device Type	Set the device as an access control terminal or attendance terminal.

Note: After changing the device type, the device will delete all the data and restart, and some functions will be adjusted accordingly.

11.6 Security Settings

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



Function Description

Function Name	Description
Standalone Communication	To avoid being unable to use when the device is offline, you can download the C/S software (such as ZKAccess 3.5) on your computer in advance for offline use.

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

11.7 USB Upgrade

Tap **USB Upgrade** on the **System** interface.

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

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

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

11.8 Update Firmware Online

Tap **Update Firmware Online** on the System interface.

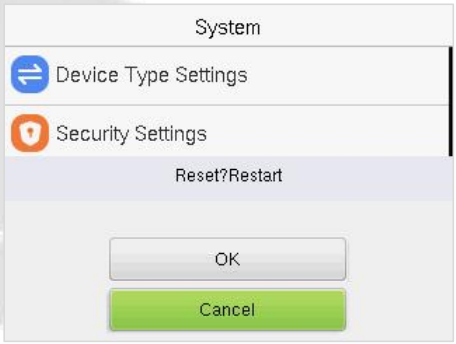
The Firmware Update Online function is enabled by default. Tap **Check for Updates** it may have the following 3 scenarios:

- If the query fails, the interface will prompt "Query failed".
- If the firmware version of the device is latest, it will prompt that the current firmware version is already the latest.
- If the firmware version of the device is not the latest, the version number and change log of the latest version will be displayed. Users can choose whether to update to the latest firmware version.

11.9 Factory Reset

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

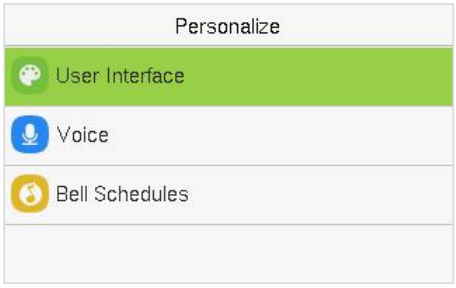
Tap **Reset** on the **System** interface and then tap **OK** to restore the default factory settings.



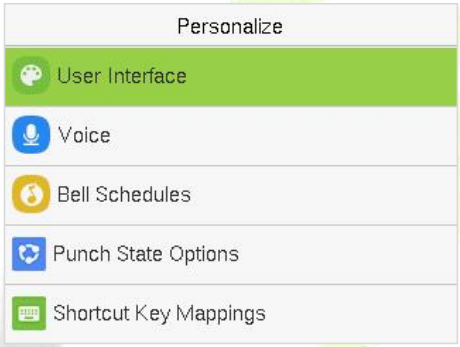
12 Personalize Settings

When the device is on the initial interface, press [**M/OK**] button > **Personalize** to customize the interface settings, voice, bell, punch state options, and shortcut key mappings.

Access Control Terminal:

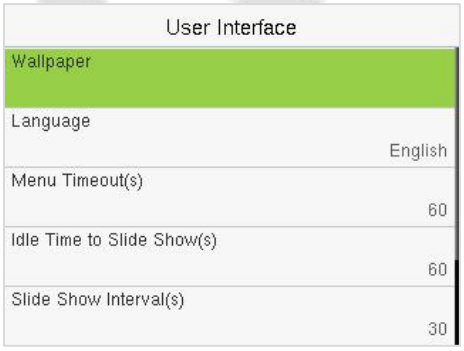


Time Attendance Terminal:



12.1 User Interface

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



Function Description

Function Name	Description
Wallpaper	It helps to select the main screen wallpaper according to the user preference.

Language	It helps to select the language of the device.
Menu 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 to 999 minutes.
Main Screen Style	The style of the main screen can be selected according to the user preference.

12.2 Voice

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

Function Description

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

12.3 Bell Schedules

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

- **New Bell Schedule:**

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

Function Description

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

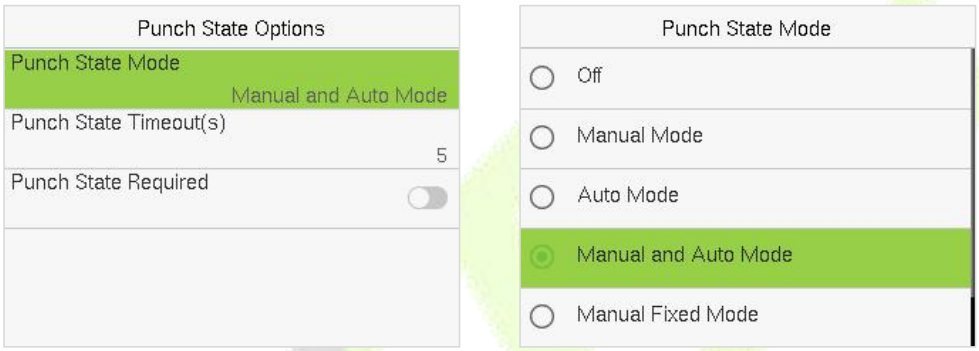
- **All Bell Schedules:**

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

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

12.4 Punch States Options

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



Function Description

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

Punch State Timeout(s)	It is the time for which the punch state displays. The value ranges from 5 to 999 seconds.
Punch State Required	Select whether an attendance state needs to be selected after verification. **ON:** Attendance state needs to be selected after verification. **OFF:** Attendance state need not requires to be selected after verification.

12.5 Shortcut Key Mappings

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

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

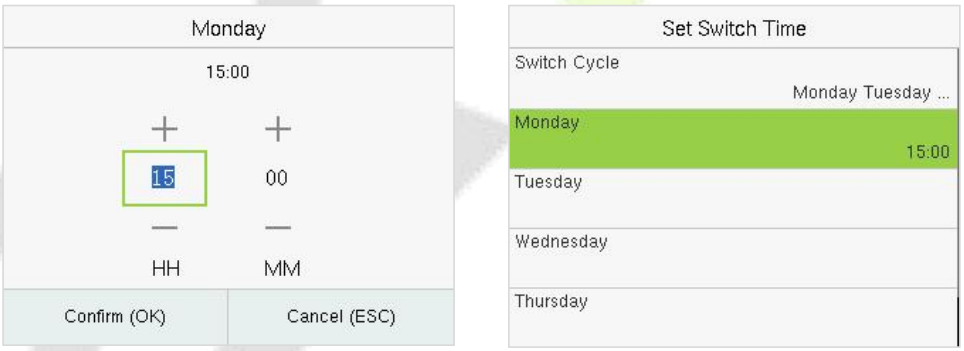
- On the **Shortcut Key Mappings** interface, tap on the required shortcut key to configure the shortcut key settings.
- On the **Shortcut Key (example, "Up Key") interface,** tap **function** to set the functional process of the shortcut key either as punch state key or function key.
- If the Shortcut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

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

➢ **Set the Switch Time**

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

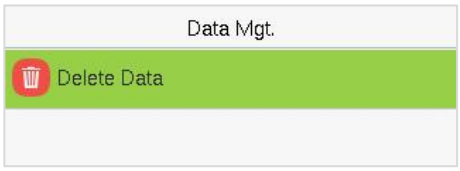
- Once the Switch cycle is selected, set the switch time for each day, and tap **OK** to confirm, as shown in the image below.



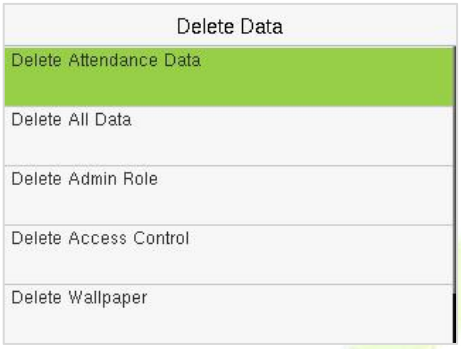
Note: When the function is set to Undefined, the device will not enable the punch state key.

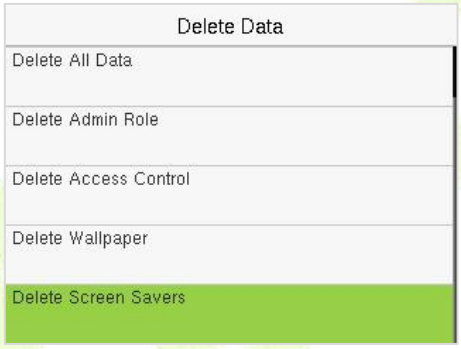
13 Data Management

When the device is on the initial interface, press [**M/OK**] button > **Data Mgt.** to manage the relevant data in the device.



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

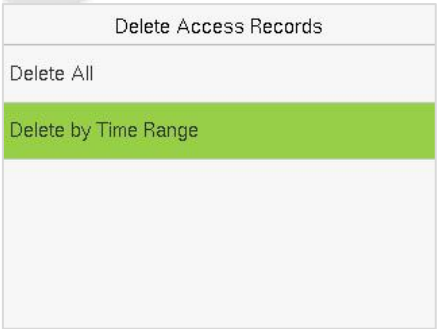




Function Description

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

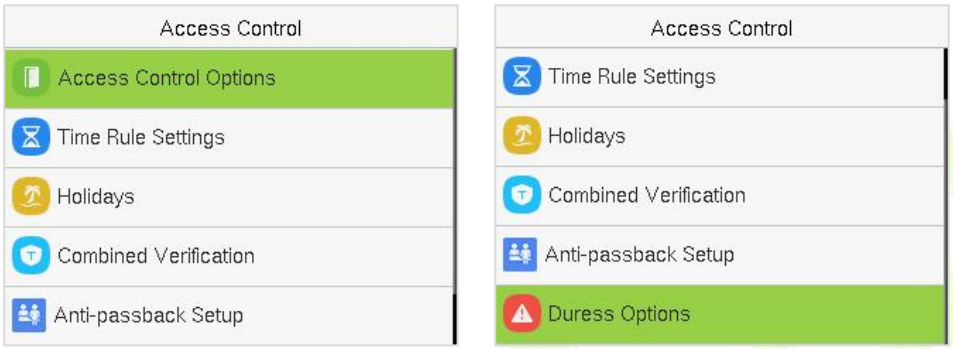
The user may select **Delete All** or **Delete by Time Range** when deleting the access records / attendance data, to **Delete by Time Range**, you need to set a specific time range to delete all data within a specific period.



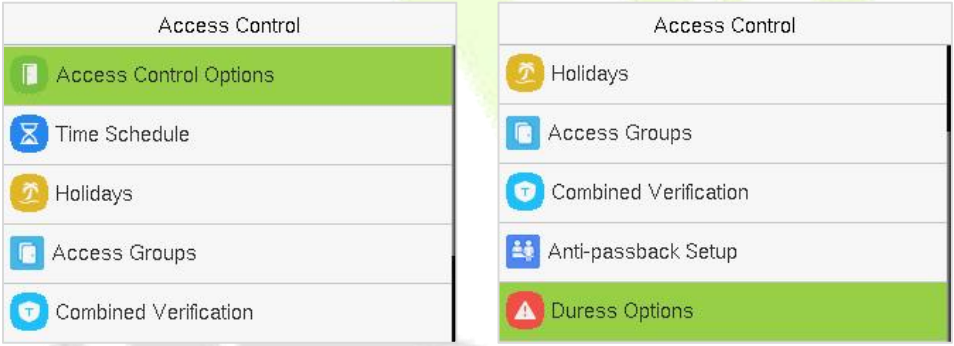
14 Access Control

When the device is on the initial interface, press [**M/OK**] button > **Access Control** to set the schedule of the door opening, locks control and to configure other parameters settings related to access control.

Access Control Terminal:



Time Attendance Terminal:



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

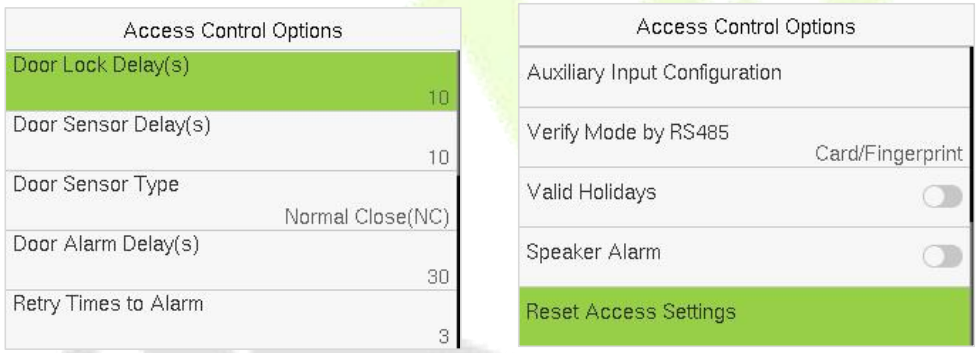
1. The relevant door's current unlock time should be within any valid time zone of the user's time period.
2. The corresponding user's group must be already set in the door unlock combination (and if there are other groups, being set in the same access combo, then the verification of those group's members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

14.1 Access Control Options

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

Access Control Terminal:

Time Attendance Terminal:



Function Description of Access Control Terminal:

Function Name	Description
Gate Control Mode	It toggles between **ON** or **OFF** switch to get into gate control mode or not. When set to **ON**, the interface removes the Door Lock Delay, Door Sensor Delay, and Door Sensor Type options.
Door Lock Delay (s)	The length of time that the device controls the electric lock to be in unlock state. Valid value: 1~99 seconds.
Door Sensor Delay (s)	If the door is not locked and is left open for a certain duration (Door Sensor Delay), an alarm will be triggered. The valid value of Door Sensor Delay ranges from 1 to 255 seconds.

Door Sensor Type	There are three Sensor types: **None**, **Normal Open**, and **Normal Closed**. **None:** It means the door sensor is not in use. **Normally Open:** It means the door is always left open when electric power is on. **Normally Closed:** It means the door is always left closed when electric power is on.
Verification Mode	The supported verification mode includes Card/Fingerprint, Fingerprint Only, Card Only, Fingerprint + Password, Card + Password, Card + Fingerprint, Card + Fingerprint + Password.
Door Available Time Period	It sets the timing for the door so that the door is accessible only during that period.
Normal Open Time Period	It is the scheduled time-period for "Normal Open" mode so that the door is always open during this period.
Primary Device	While configuring the primary and secondary devices, you may set the state of the primary as **Out** or **In**. **Out:** A record of verification on the primary device is a check-out record. **In:** A record of verification on the primary device is a check-in record.
Secondary Device	While configuring the primary and secondary devices, you may set the state of the secondary as **Out** or **In**. **Out:** A record of verification on the secondary device is a check-out record. **In:** A record of verification on the secondary device is a check-in record.
Auxiliary Input Configuration	Sets the door unlock time period and auxiliary output type of the auxiliary terminal device. Auxiliary output types include None, Trigger door open, Trigger Alarm, Trigger door open and Alarm.
Verify Mode by RS485	When the RS485 reader function is turned on, the verification method is used when the device is used as a primary or a secondary.
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, primary device, and alarm. However, erased access control data in Data Mgt. is excluded.

Function Description of Time Attendance Terminal:

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: 0 to 10 seconds.
Door Sensor Delay (s)	If the door is not locked and is left open for a certain duration (Door Sensor Delay), an alarm will be triggered. The valid value of Door Sensor Delay ranges from 1 to 255 seconds.
Door Sensor Type	There are three Sensor types: **None**, **Normal Open**, and **Normal Closed**. **None:** It means the door sensor is not in use. **Normally Open (NO):** It means the door is always left open when electric power is on. **Normally Closed (NC):** 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 verifications reach 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 the scheduled time-period for "Normal Close" mode so that the door is always closed during this period.
Normal Open Time Period	It is the scheduled time-period for "Normal Open" mode so that the door is always open during this period.
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	When the RS485 reader function is turned on, the verification method is used when the device is used as a primary or a secondary.

Valid Holidays	To set if **Normal Close Time Period** or **Normal Open 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, door alarm delay, normal close time period, normal open time period, and alarm. However, erased access control data in Data Mgt. is excluded.

14.2 Time Rule Settings / Time Schedule

Tap **Time Rule Settings / Time Schedule** on the **Access Control** interface to configure the time settings.

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

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

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

Specify the start and the end time, and then tap [**M/OK**].

Note:

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

14.3 Holidays

When there is a holiday, you may need a different access time; however, altering everyone's access time one by one is extremely time-consuming. Thus, a holiday access time that applies to all workers can be set, and the user will be able to open the door during the holidays.

Tap **Holidays** on the **Access Control** interface to set the holiday access.

➢ **Add a New Holiday:**

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

Access Control Terminal:

Time Attendance Terminal:

- **Edit a Holiday:**

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

- **Delete a Holiday:**

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

14.4 Access Groups

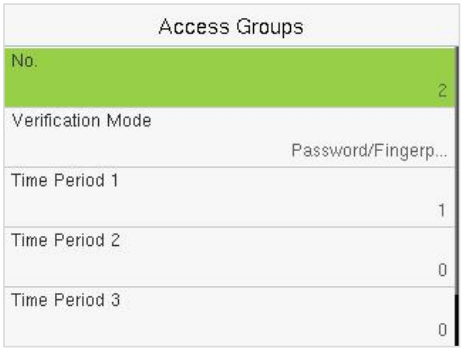
Grouping is to manage users in groups, only for time attendance terminal.

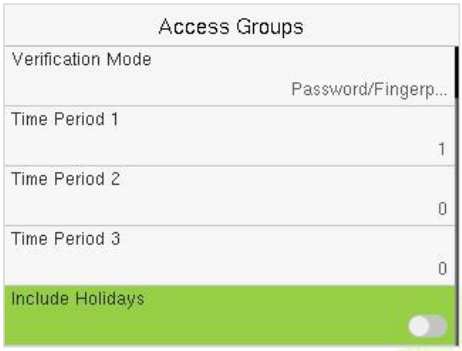
The default time zone for group members is the group time zone, while users can set their personal time zone. When the group verification mode and the user verification mode overlap, the user verification mode takes priority. Each group can set a maximum of 3 time zones; as long as one of them is valid, the group can be successfully verified. The newly enrolled user is assigned to Access Group 1 by default, but can be assigned to another access group.

Tap **Access Groups** on the **Access Control** interface.

➢ **Add a New Holiday:**

Tap **New Group** on the **Access Group** interface.





Note:

1. The system has a default access group numbered 1, which cannot be deleted but can be modified.
2. A number cannot be modified again after being set.
3. When the holiday is set to be valid, the personnel in a group can open the door only when group time period overlaps with the holiday time period.
4. When the holiday is set to be invalid, the access control time of the personnel in this group is not affected by holidays.

➢ **Edit Group:**

On the **All Group** interface, tap to select the access group item to be modified. Tap **Edit** to modify group parameters.

➢ **Delete a Group:**

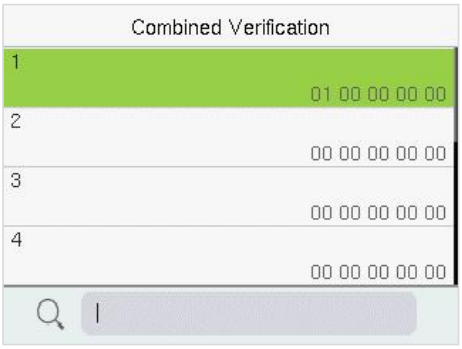
On the **All Group** interface, select an access group item to be deleted and tap **Delete**. Tap [**M/OK**] to confirm the deletion. After deletion, this group does not display on the **All Group** interface.

14.5 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.

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



On the combined verification interface, tap the Door-unlock combination to be set, and tap the **up** and **down** arrows to input the combination number, and then tap [**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.

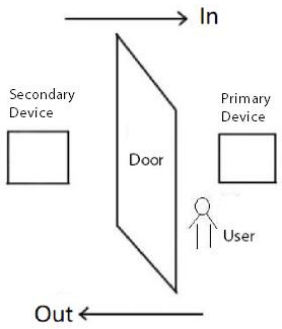
Note: To delete the door-unlock combination, set all Door-unlock combinations to 0.

14.6 Anti-passback Setup

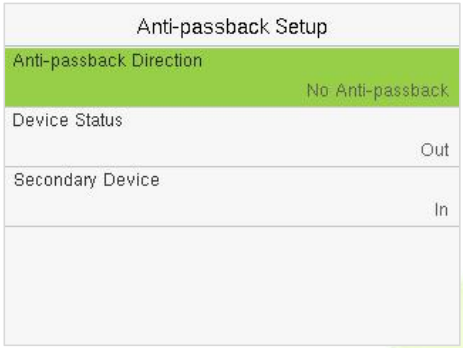
A user may be followed by some person(s) to enter the door without verification, resulting in a security breach. So, to avoid such situations, the Anti-Passback option was developed. Once it is enabled, the check-in and check-out record must occur alternatively to open the door to represent a consistent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

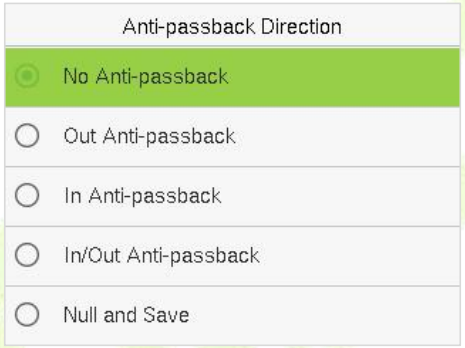
This function requires two devices to work together:

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



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





Function Description:

Function Name	Description
Anti-passback Direction	**No Anti-passback:** The Anti-Passback function is disabled, which means successful verification through either the primary device or secondary 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:** The Anti-Passback function is disabled, which means successful verification through either the primary device or secondary device can unlock the door. And can save attendance status.
Device Status	While configuring the primary and secondary devices, you may set the state of the primary as **Out** or **In**. **Out:** A record of verification on the primary device is a check-out record. **In:** A record of verification on the primary device is a check-in record.

Secondary Device	While configuring the primary and secondary devices, you may set the state of the secondary as **Out** or **In**. **Out:** A record of verification on the secondary device is a check-out record. **In:** A record of verification on the secondary device is a check-in record.

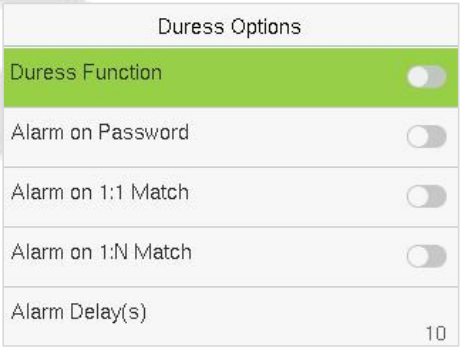
14.7 Duress Options Settings

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 activate the alarm as well.

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

Access Control Terminal:

Time Attendance Terminal:



Function Description of Access Control Terminal:

Function Name	Description
Alarm on Password	When a user uses the password verification method, an alarm signal will be generated, otherwise there will be no alarm signal.

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

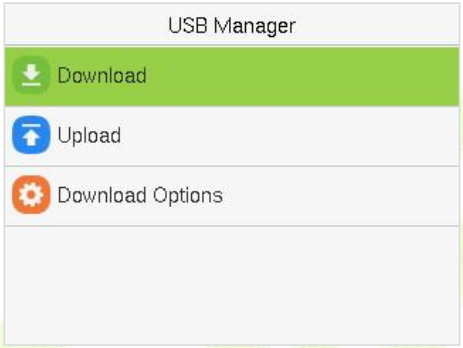
Function Description of Time Attendance Terminal:

Function Name	Description
Duress Function	Enable/Disable the duress function.
Alarm on Password	In [**ON**] state, when a user uses password verification method, alarm will be triggered. In [**OFF**] state, no alarm signal will be triggered.
Alarm on 1:1 Match	When a user uses the 1:1 verification method, an alarm signal will be generated, otherwise there will be no alarm signal.
Alarm on 1:N Match	When a user uses the 1:N verification method, an alarm signal will be generated, otherwise there will be no alarm signal.
Alarm Delay (s)	Alarm signal will not be transmitted until the alarm delay time is elapsed. The value ranges from 1 to 999 seconds.

15 USB Manager

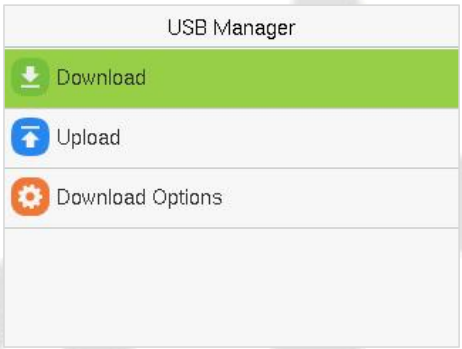
Press [**M/OK**] on the initial interface. Select **USB Manager** and press [**M/OK**] to Upload or download data between device and the corresponding software through a USB disk.

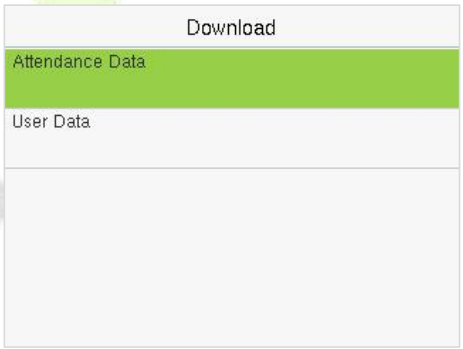
Note: Before uploading/downloading data from/to the USB disk, insert the USB disk into the USB slot first.



15.1 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.

15.2 USB Upload

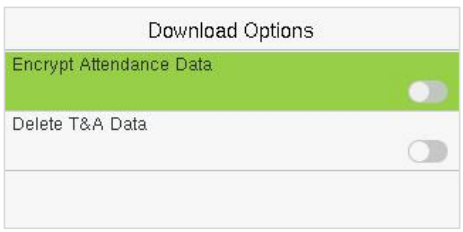
On the **USB Manager** interface, select **Upload** and press [**M/OK**].

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. **Note:** 1) Create a folder named "**Wallpaper**" in the root directory of your USB drive. Place the wallpapers you wish to upload into this folder. 2) Name each image as "Wallpaper+number,"such as Wallpaper8. The number must not exceed **Wallpaper45**. 3) Acceptable image formats are **.jpg, .bmp, .png, or .jpeg**. Each image must not exceed **2MB** in size. 4) The USB drive's file system must be **FAT32**; otherwise, the device will be unable to recognize its contents.
User Data	To upload all the user's information and fingerprints from USB disk to the device.

15.3 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**].

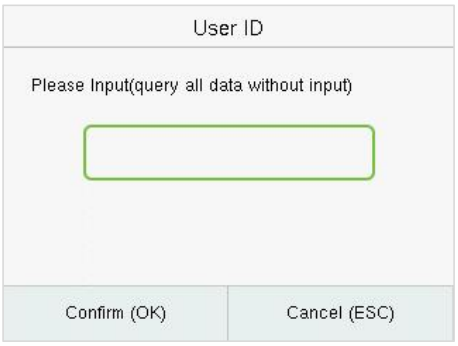


Press [**M/OK**] to enable or disable the **Encrypt Attendance Data** and **Delete T&A Data** options.

16 Attendance Search

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

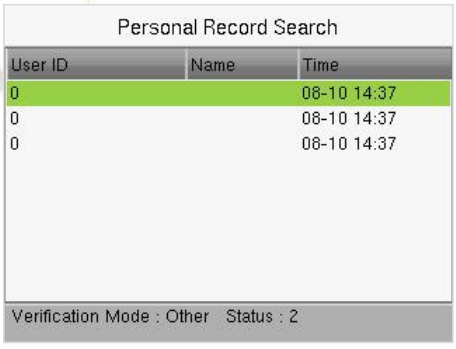
When the device is on the initial interface, press [**M/OK**] button > **Attendance Search** to search for the required event Logs.



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

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

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

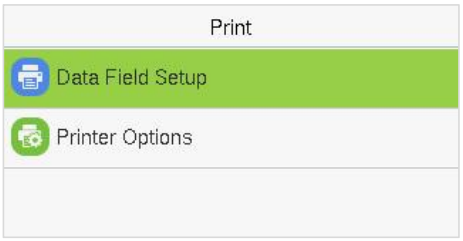


4. The figure shows the details of the selected record.

17 Print Settings

Devices with printing function can print attendance records out when a printer is connected.

When the device is on the initial interface, press [**M/OK**] button > **Print** to set printing information and functions.



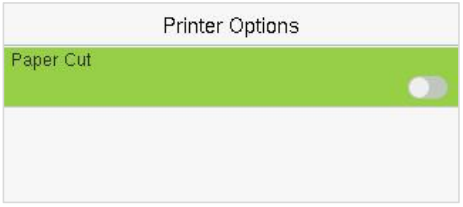
17.1 Print Data Field Settings

Select **Data Field Setup** on the Print interface. Press [**M/OK**] to turn on / off the fields needing to be printed.

Remarks: In printing, the fields position of the information can be adjusted by the left / right key: press left key to move to the previous item, and press right key to move to the next item.

17.2 Print Options Settings

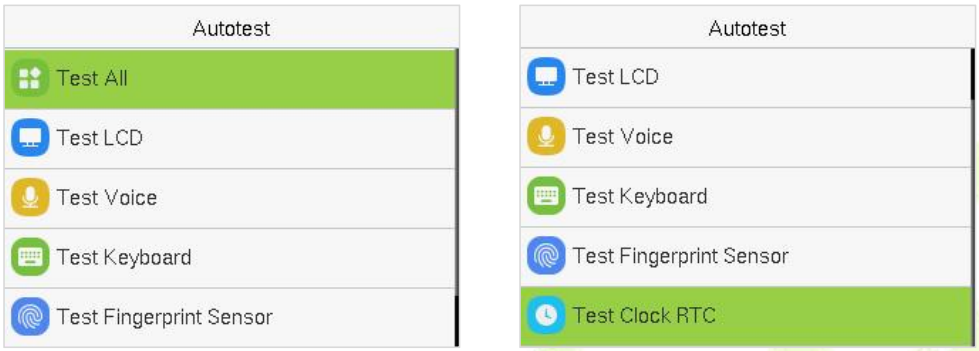
Select **Printer Options** on the Print interface. Press [**M/OK**] to turn on / off the **Paper Cut** function.



Remarks: To turn on the **Paper Cut** function, it is required to connect the device with a printer with paper cutting function, so that the printer will cut papers according to the selected printing information when printing.

18 Autotest

When the device is on the initial interface, press [**M/OK**] button > **Autotest**, it enables the system to automatically test whether the functions of various modules are working normally, including the LCD, Voice, Keyboard, Fingerprint and Real-Time Clock (RTC).

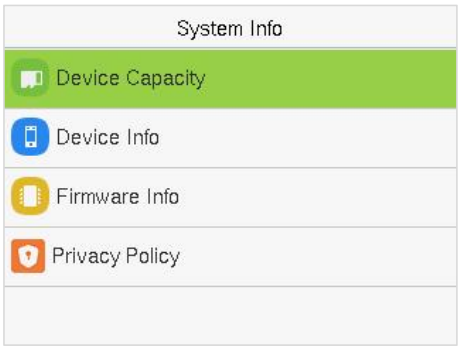


Function Description

Function Name	Description
Test All	To automatically test whether the LCD, Voice, Keyboard, Fingerprint and Real-Time Clock (RTC) are normal.
Test LCD	To automatically test the display effect of LCD screen by displaying full-color, pure white, and pure black to check whether the screen displays colors normally.
Test Voice	To automatically test whether the audio files stored in the device are complete and the voice quality is good.
Test Keyboard	The terminal tests whether every key on the keyboard works normally. Tap any key on the **Test Keyboard** interface to check whether the tapped key matches the key displayed on the screen. The keys are displayed as dark grey before and turn blue after tapped. Tap **ESC** to exit the test.
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 tap it again to stop counting.

19 System Information

When the device is on the initial interface, press [**M/OK**] button > **System Info** to view the storage status, version information of the device, firmware information and privacy policy.



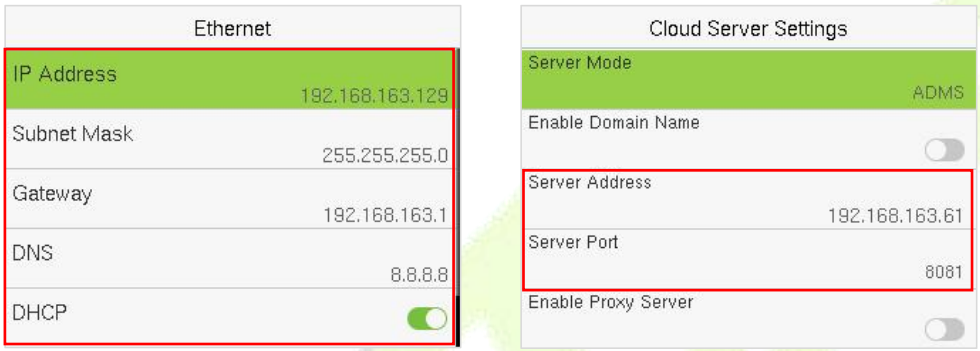
Function Description

Function Name	Description
Device Capacity	Displays the current device's user storage, fingerprint, card and password storage, administrators and records.
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.
Privacy Policy	Display the device's privacy policy.

20 Connect to ZKBio CVAccess Software

20.1 Set the Communication Address

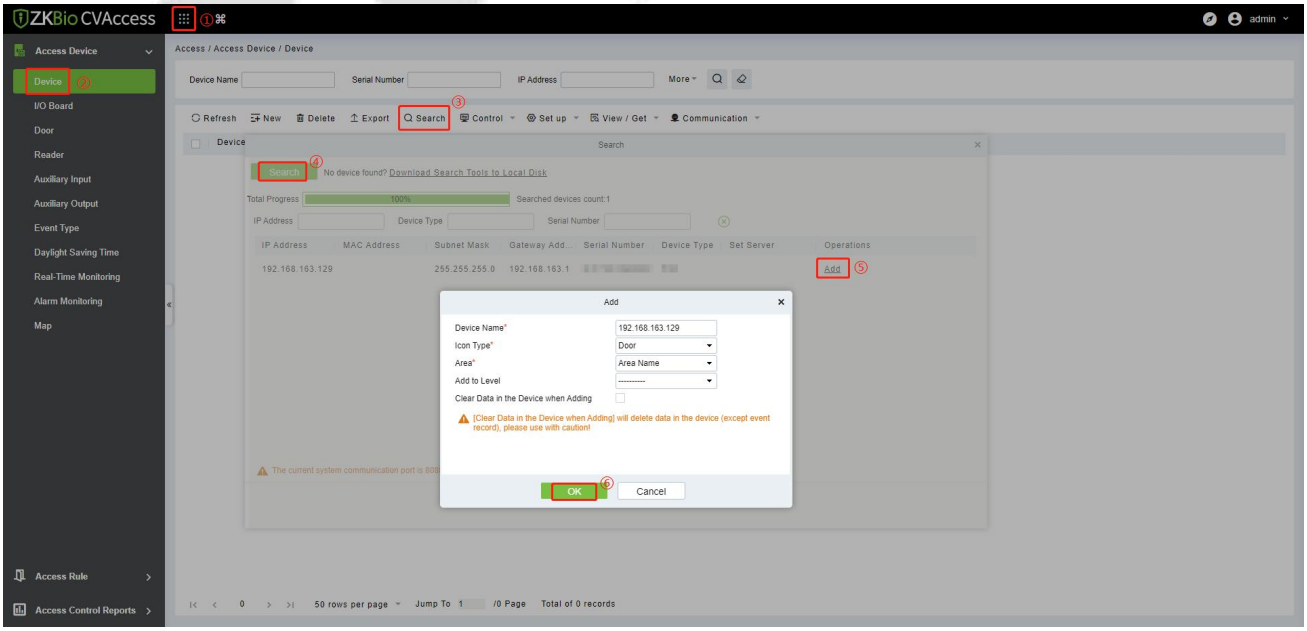
1. The device defaults to enabling DHCP functionality and does not support disabling DHCP. It can only obtain an IP address and connect to the network by connecting to a router.
2. In the main menu, click **COMM.** > **Cloud Server Setting** to set the server address and server port.
   Server address: Set the IP address as of ZKBio CVAccess server.
   Server port: Set the server port as of ZKBio CVAccess.



20.2 Add Device on the Software

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

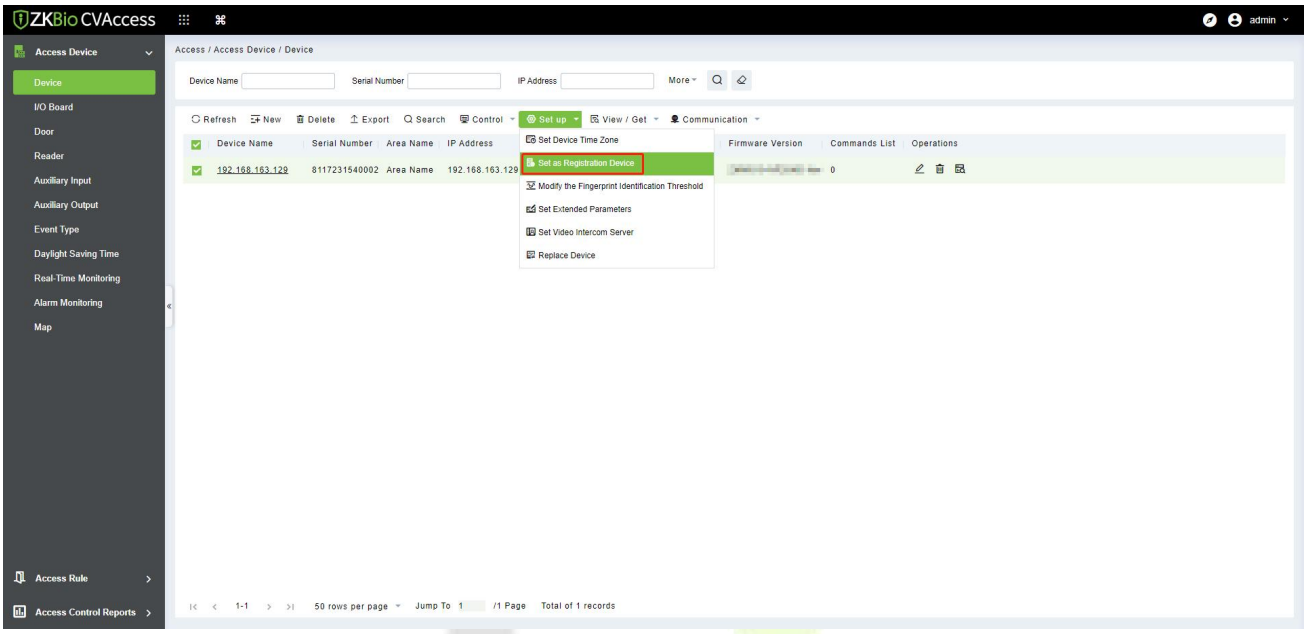
1. Click **Access** > **Device** > **Search** > **Search**, to open the Search interface in the software.
2. Click **Search**, and it will prompt [**Searching……**].
3. After searching, the list and total number of access controllers will be displayed.



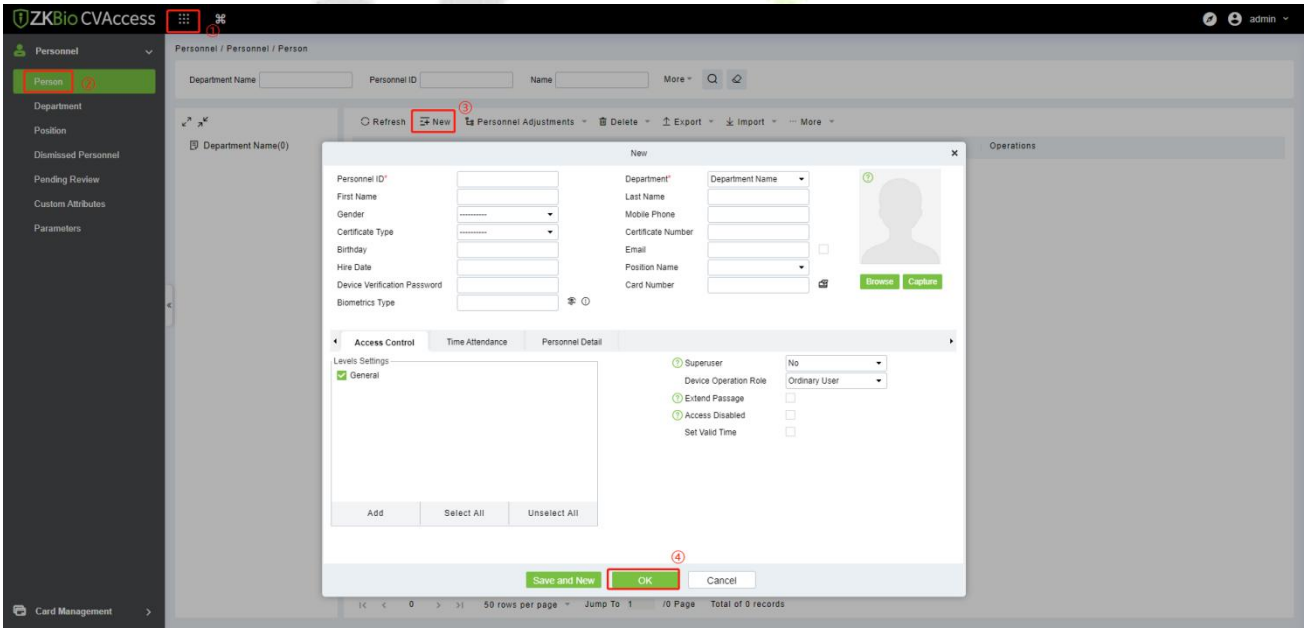
4. Click **Add** in operation column, a new window will pop-up. Select Icon type, Area, and Add to Level from each dropdown and click **OK** to add the device.
5. After the addition is successful, the device will be displayed in the device list.

20.3 Add Personnel on the Software and Online Fingerprint Registration

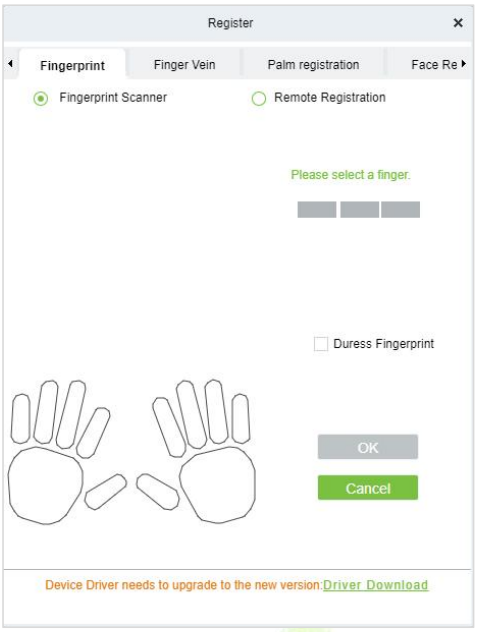
1. In the device list, select the device and click **Set up > Set as Registration Device.**



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



3. Fill in all the required fields of the user and click  to enter the online fingerprint registration interface.



4. Click **Driver Download** to install the driver first.
5. Select **Remote Registration**, then select the IP address of the device and click **Confirm**.

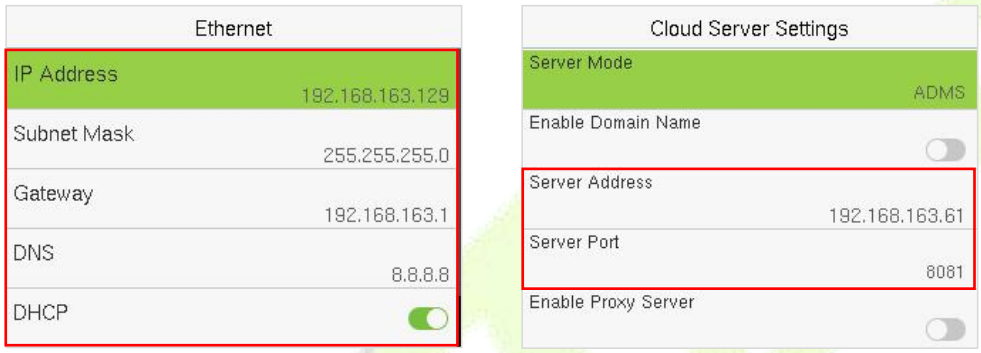
6. Select the finger you want to register and press your finger on the fingerprint sensor of the device three times. If the fingerprint is successfully registered, the device will prompt "Enrolled successfully".
7. If you want to register a duress fingerprint, you can click **Duress Fingerprint** before registering the fingerprint.
   - **Duress fingerprint:** In any case, a duress alarm is generated when a fingerprint matches a duress fingerprint.
8. Click **OK** to save the user.
9. Click **Access > Device > Control > Synchronize All Data to Devices** to synchronize all the data to the device including the new users.

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

21 Connect to ZKBioTime 8.0 Software

21.1 Set the Communication Address

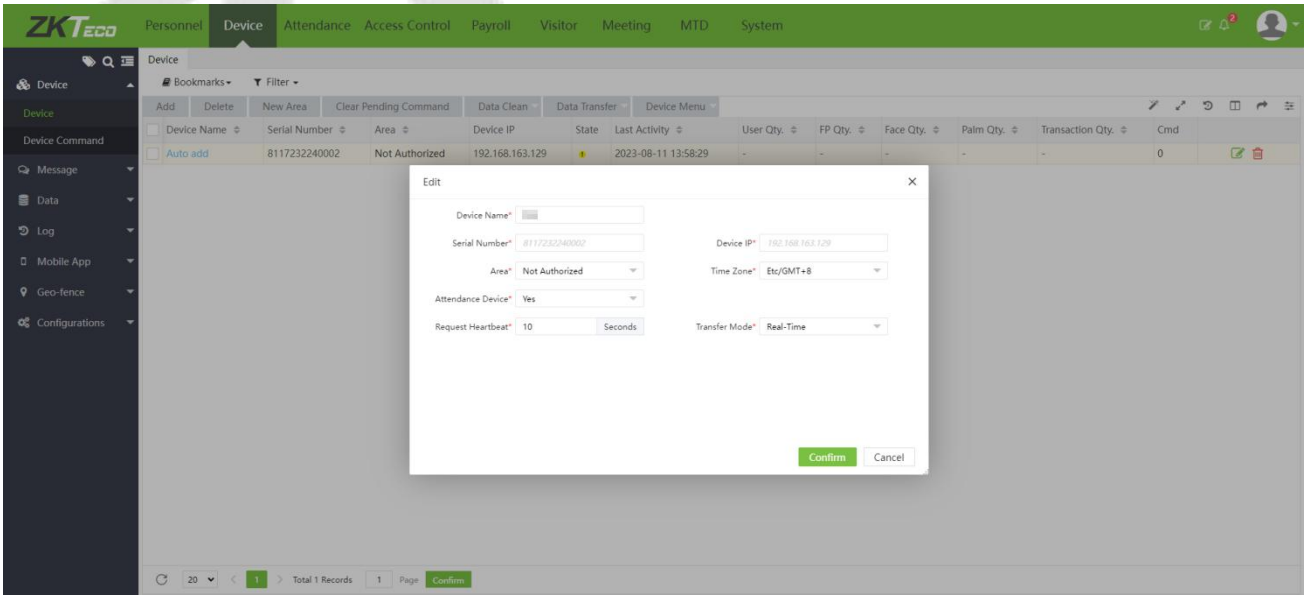
1. The device defaults to enabling DHCP functionality and does not support disabling DHCP. It can only obtain an IP address and connect to the network by connecting to a router.
2. In the main menu, click **COMM.** > **Cloud Server Setting** to set the server address and server port.
   Server address: Set the IP address as of ZKBioTime 8.0 server.
   Server port: Set the server port as of ZKBioTime 8.0 server.



21.2 Add Device on the Software

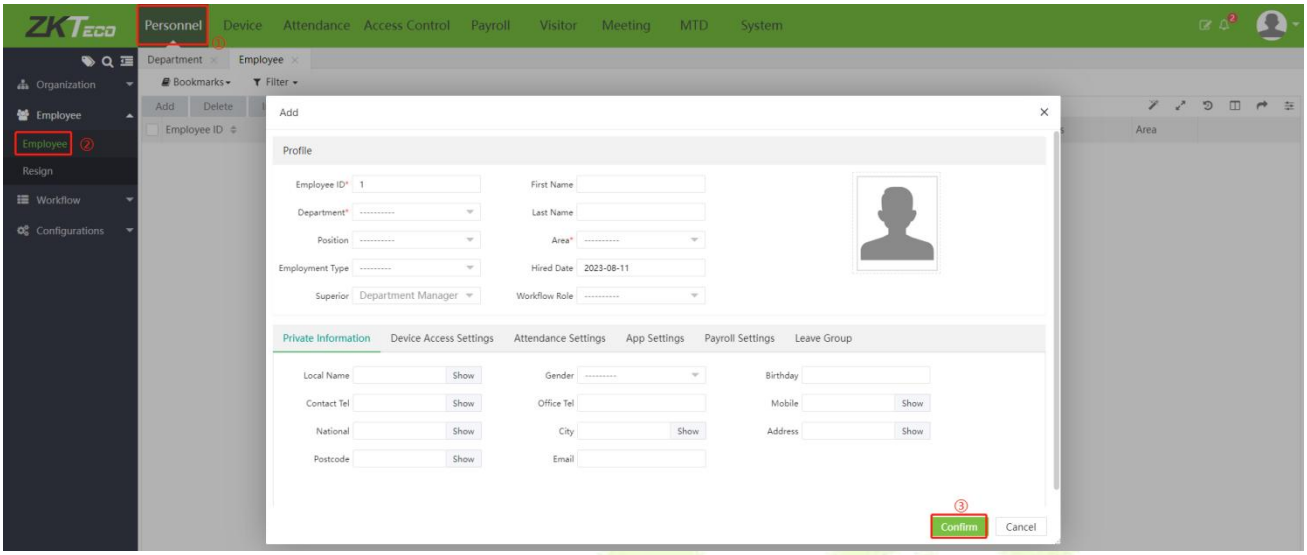
After setting on the device, the device will be automatically added to the software. Open the ZKBioTime software then select **Device Module** > **Device** > **Device**, click the device in the list, change the Device Name and Area.

Note: The devices added automatically must be assigned to custom areas to communicate with the software.

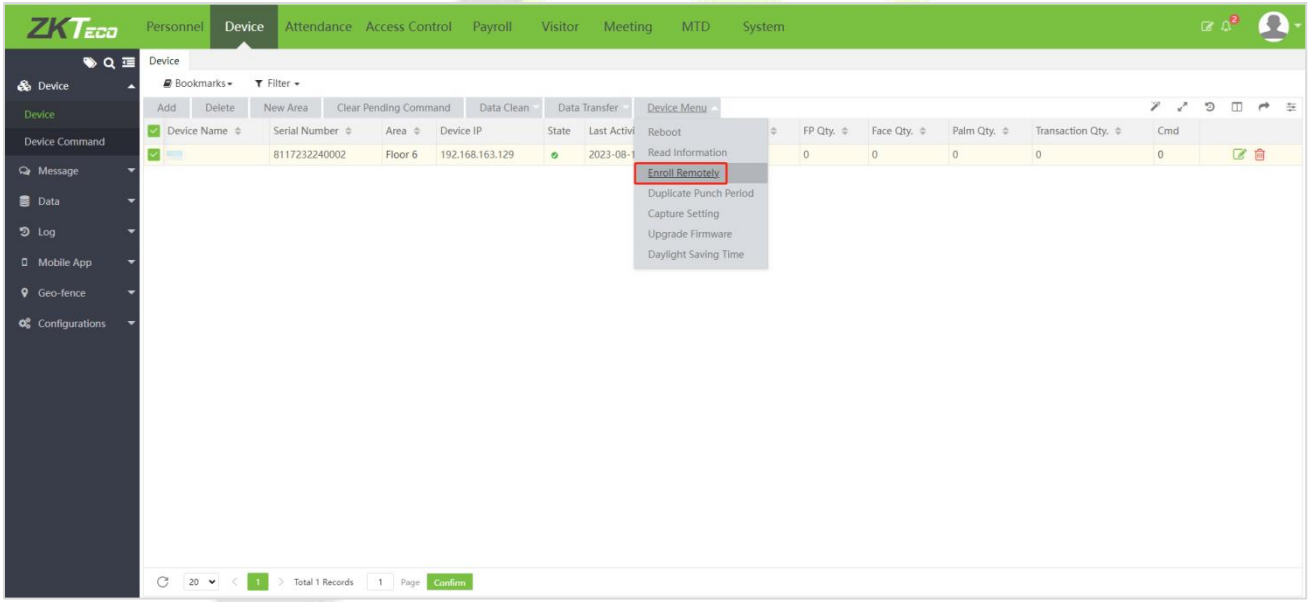


21.3 Add Personnel on the Software and Online Fingerprint Registration

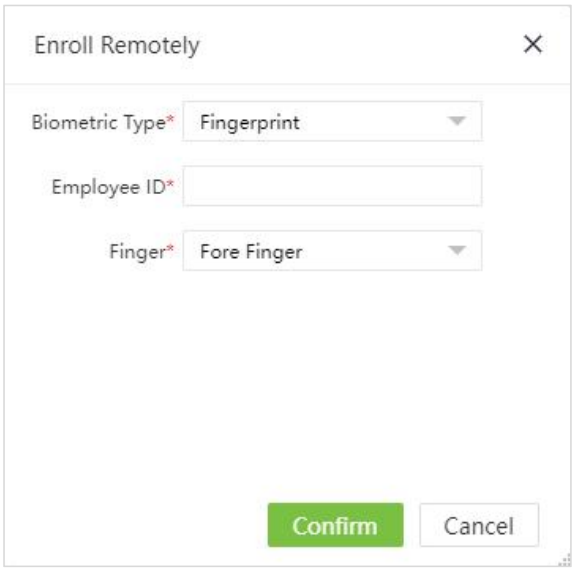
1. Click **Personnel** > **Employee** > **Add**:



2. Fill in all the required fields and click **Confirm** to register a new user.
3. Click **Device** > **Device**, select the device and click **Device Menu** > **Enroll Remotely**.



4. Enter the Employee ID and select the finger you want to register and press your finger on the fingerprint sensor of the device three times. If the fingerprint is successfully registered, the device will prompt "Enrolled successfully".



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

Note: For other specific operations, please refer the *ZKBioTime 8.0 User Manual*.

22 Connecting to the Yoosee App

The App pages may vary depending on the version, and the document is for reference only.

22.1 Download the Yoosee App

Method 1: Search for 'Yoosee' in your app store.

Method 2: Scan QR code to download Yoosee App.

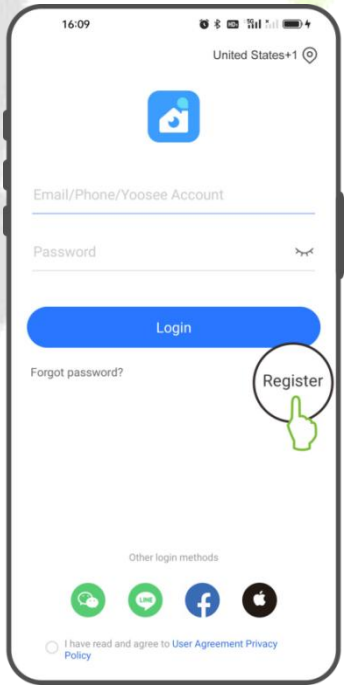
Download on the App Store

GET IT ON Google Play

22.2 Register Account and Login to the App

Method 1: Click '**Register**', enter phone/email, follow app instructions to complete registration and click **Login**.

Method 2: Choose a supported provider (e.g., WeChat / Line / Facebook / Apple Account). Then, authorize the request and complete registration. Tap **Login** if prompted.



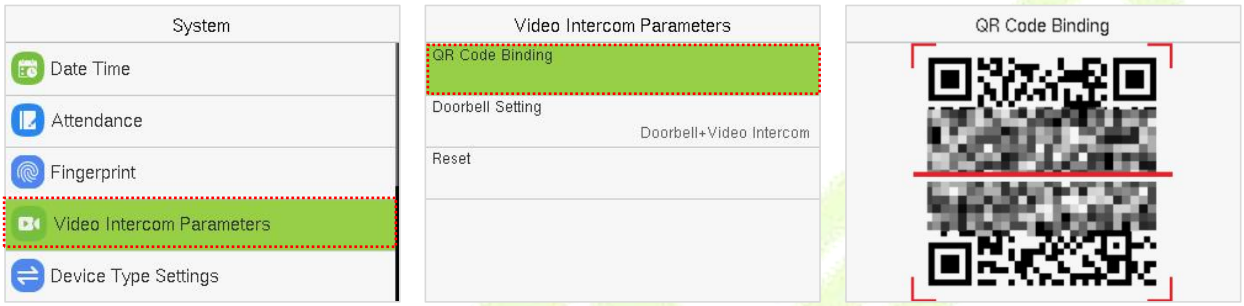
Notes:

1) When mobile number registration is unavailable in your selected country/region, only email registration is supported;

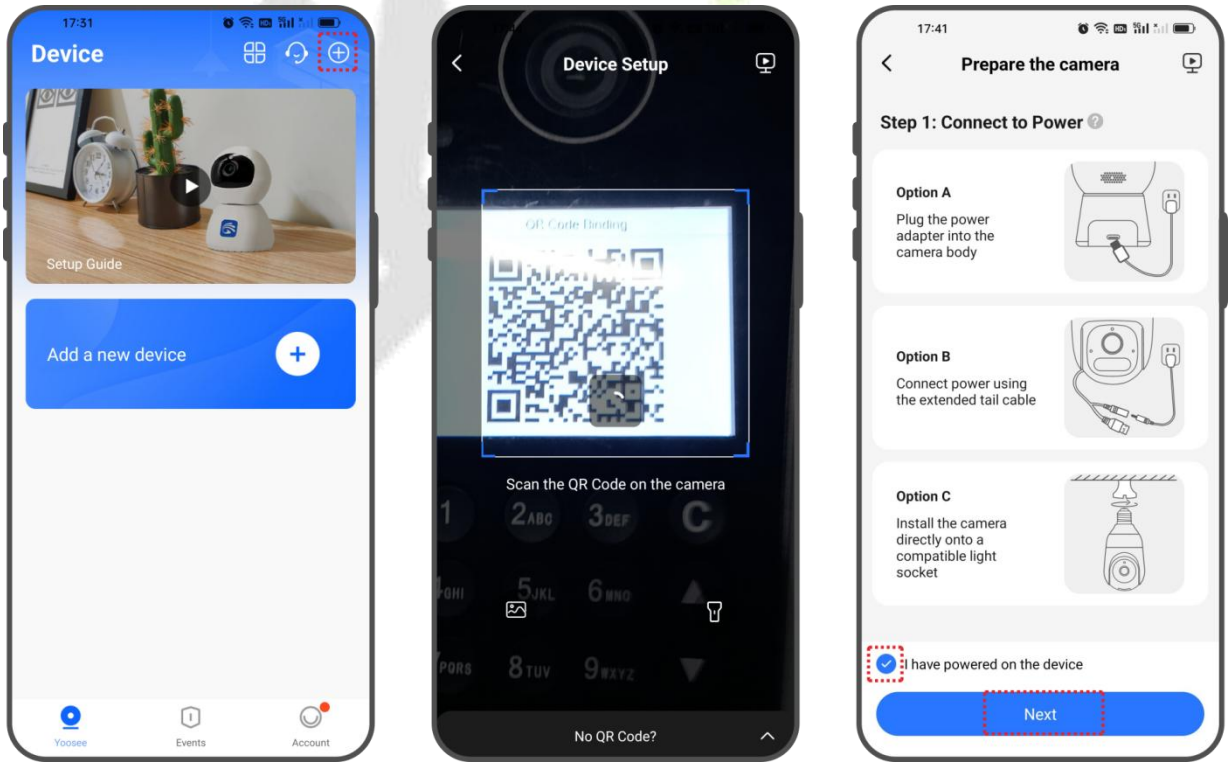
2) Data services are not interconnected across different registration regions. Please select the correct region for registration.

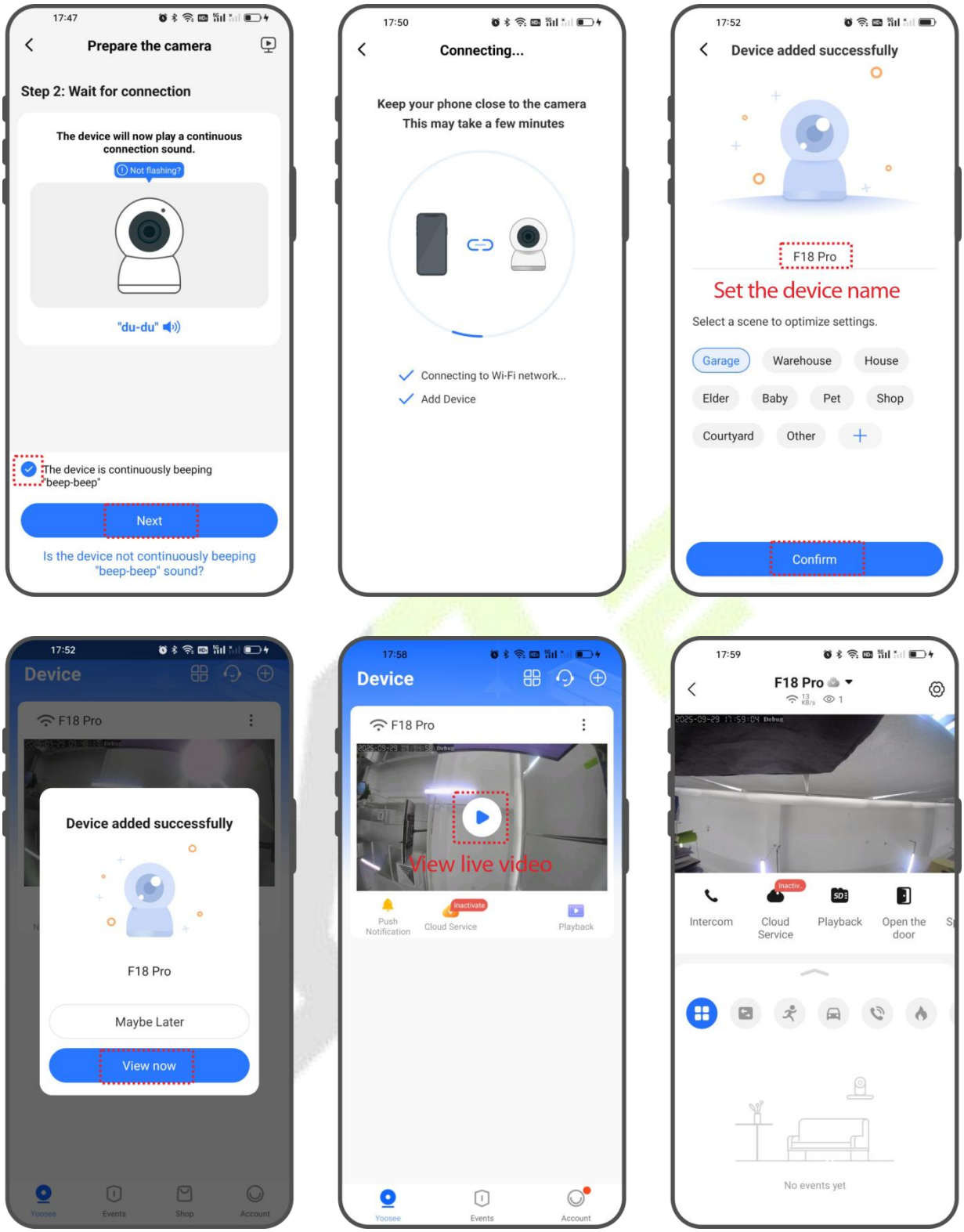
22.3 Add the Device to the App

1. Power on the device. Wait about 30 seconds until the startup tone plays.
2. Ensure that both the device and your phone connect to Wi-Fi. You can configure Wi-Fi for the device by pressing the [**M/OK**] button to enter the **Main Menu** > **COMM.** > **Wi-Fi Settings**.
3. Then press [**M/OK**] button to enter the **Main Menu** > **System** > **Video Intercom Parameters** > **QR Code Binding** to display the device QR code. As shown in the figure below.



4. Open the Yoosee app, tap the icon in the upper-right corner, and scan the device's QR code.
5. Follow the prompts on the app interface to add the device until you hear the device voice prompt stating "Device added successfully".



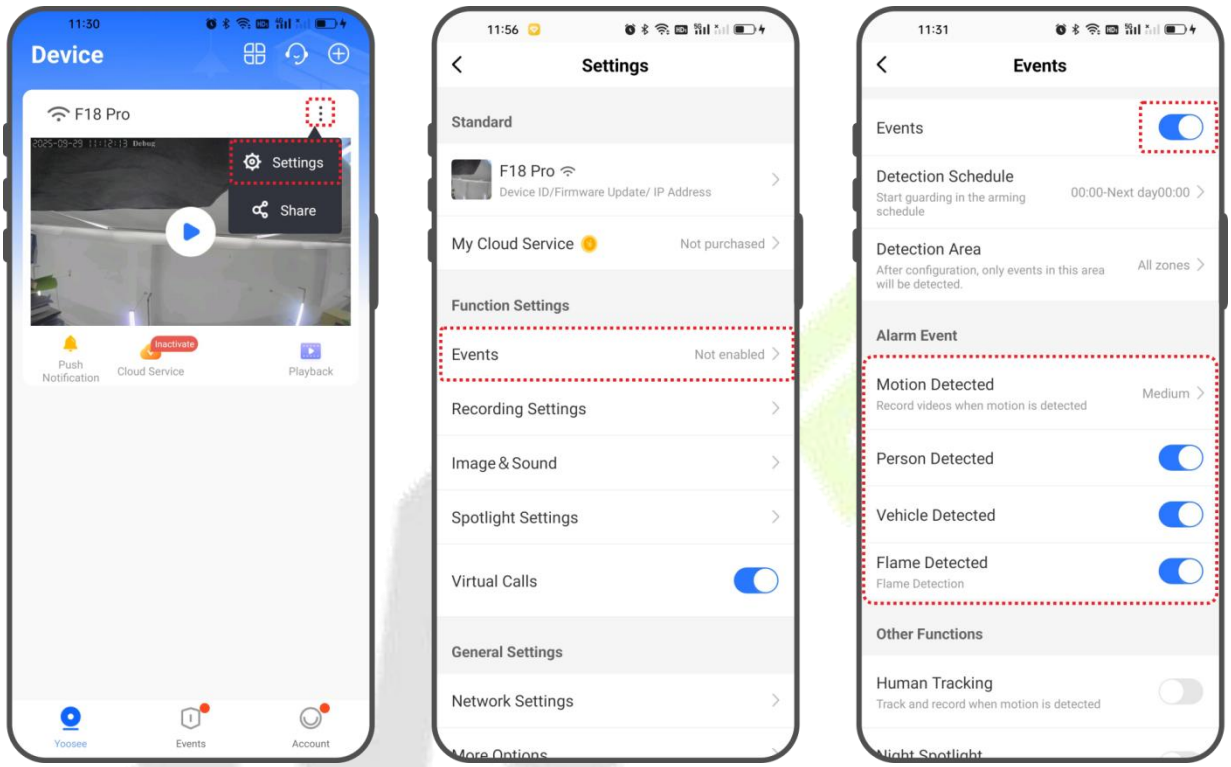


Notes:

1. Using this device as an example, one account can bind up to 300 devices.
2. Shared devices can be shared with up to 10 users.
3. Online video preview for devices supports up to 2 simultaneous viewers.

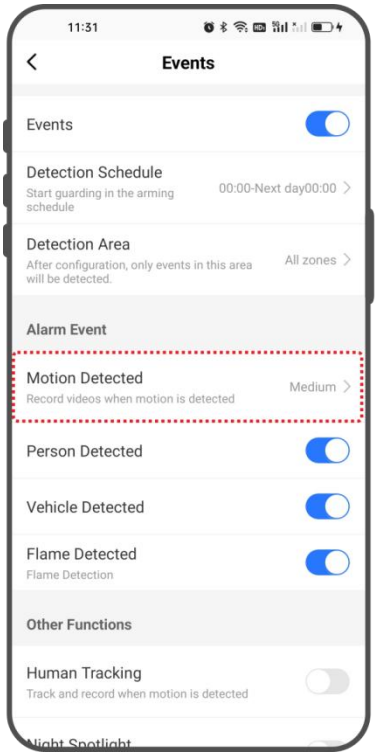
22.4 Enable Events

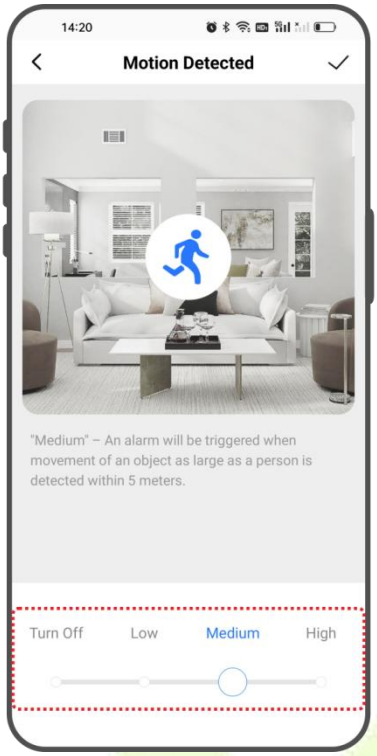
1. Click the icon in the upper-right corner and select **Settings** from the dropdown menu.
2. In the Settings interface, locate the Function Settings section and tap **Events**.
3. Click the icon to enable event functions. By default, motion detection, person detection, vehicle detection, and flame detection are enabled.

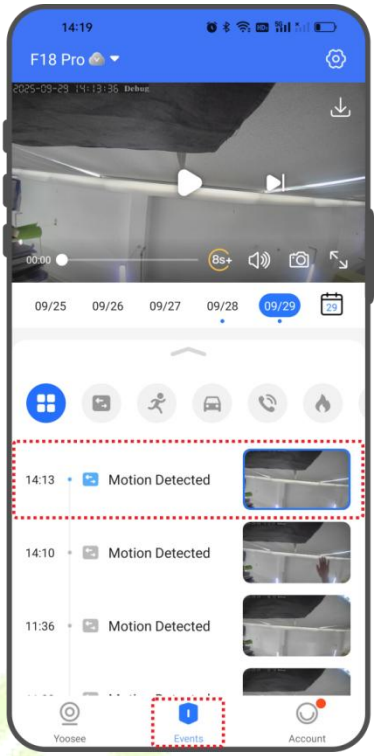


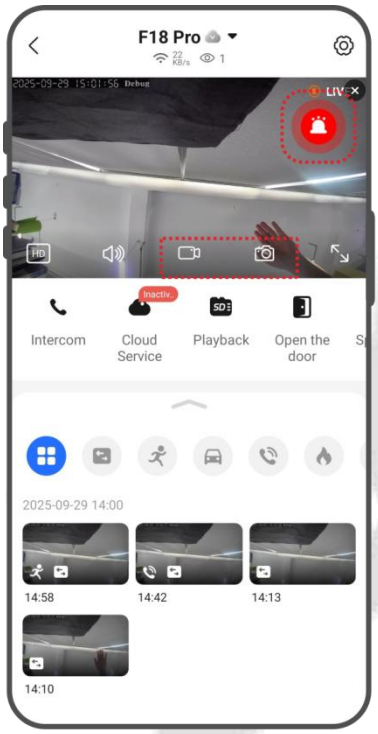
22.4.1 Motion Detected

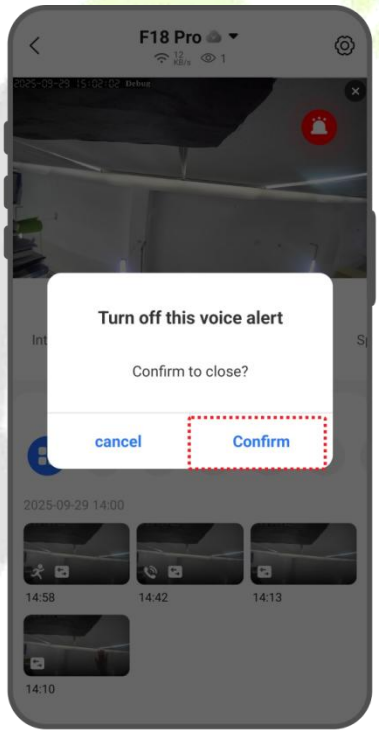
1. Record video when motion is detected in the frame; detection range can be customized.
2. There are three options available. Includes Turn Off, Low, Medium, and High. Select "**Turn Off**" to disable this feature.
3. Click the **Event** menu at the bottom to view related recorded videos. As shown below.
4. After enabling the motion detection feature, is triggered when a large target - such as a person - moves within the configured detection area.
5. As shown below, an alert icon will appear on the video interface. You can also click the or icons below the video interface to record or take a snapshot.
6. Click the red alarm icon to dismiss this alert notification.



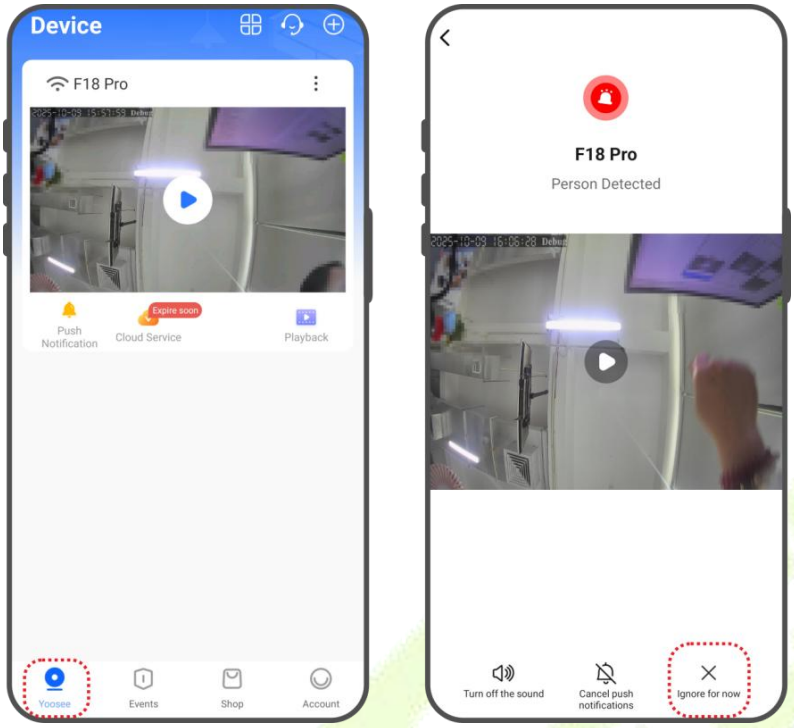






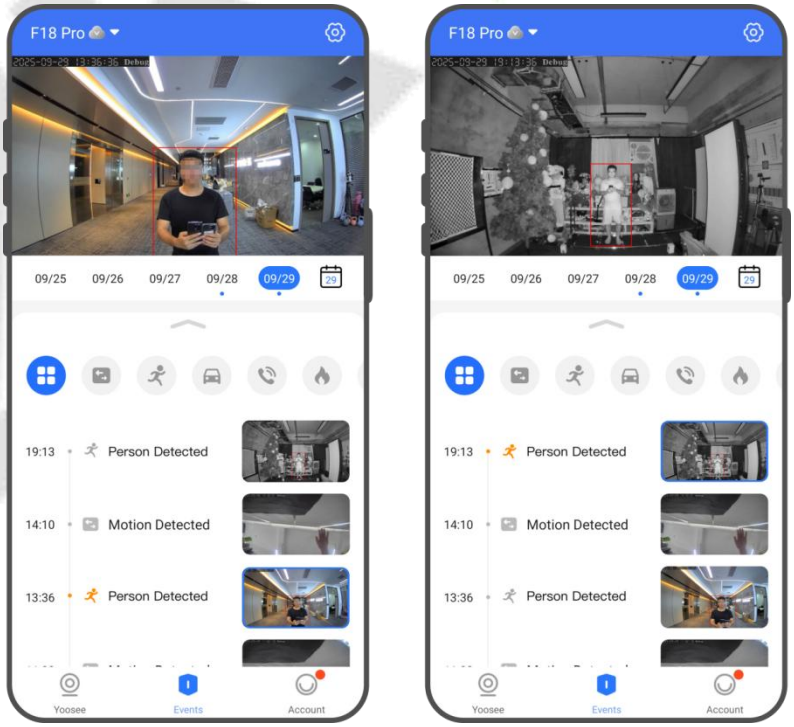


Note: When the app runs in the background or is in the Yoosee menu interface, if the device detects human activity, the following alarm interface will pop up. Click the bottom icon to perform the corresponding action. As shown in the figure below.



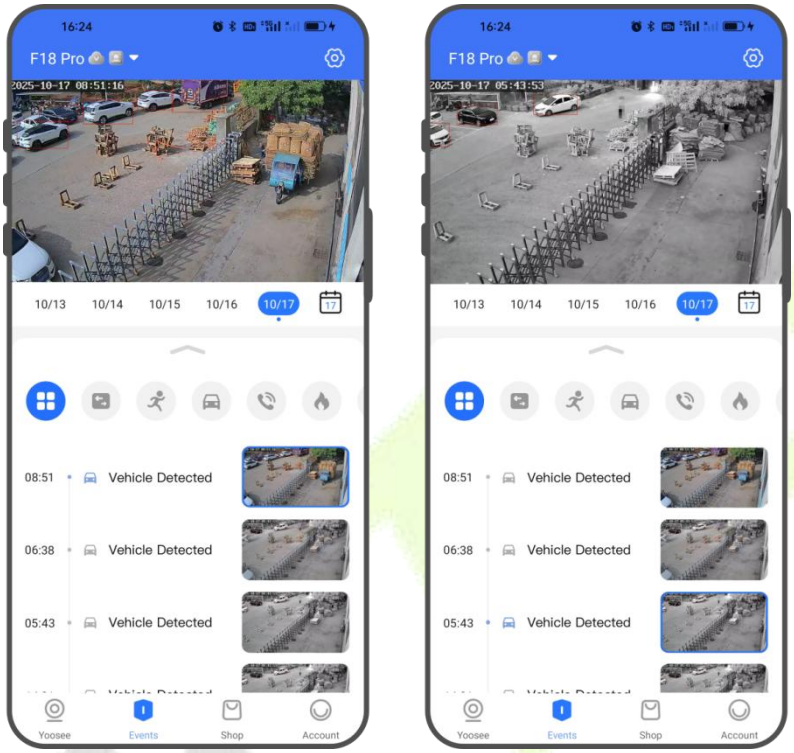
22.4.2 Person Detected

Detects and highlights people in real time with on-screen bounding boxes. Actual detection range varies with lens FOV and mounting; confirm performance on-site in both day and IR night modes.



22.4.3 Vehicle Detected

An intelligent algorithm capable of automatically identifying cars and trucks within video footage, then labeling and analyzing them. Recognition detection distance is highly dependent on camera angle, requiring field testing of night vision and daytime performance.



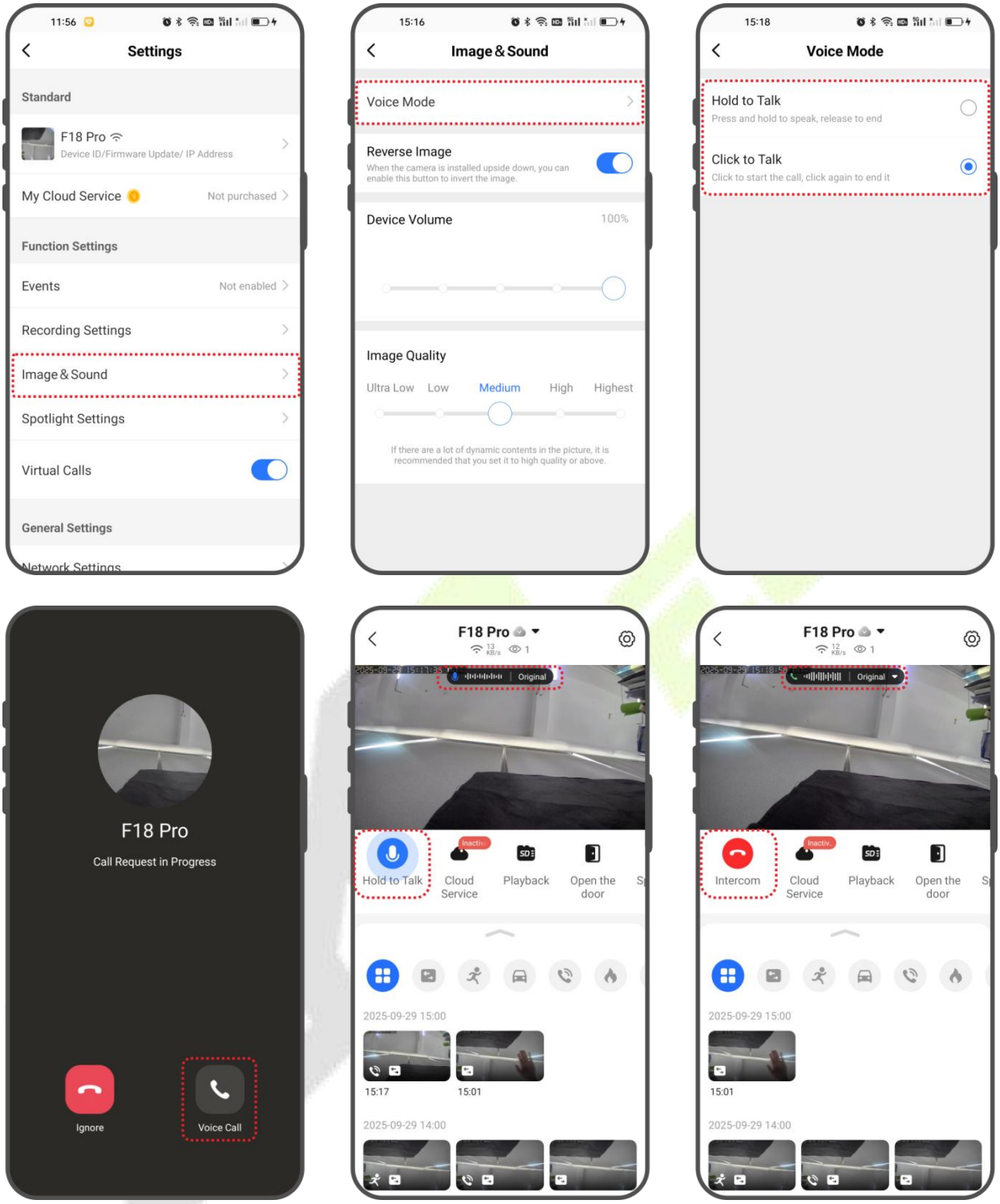
22.4.4 Flame Detected

Flame detection: Uses color, flicker frequency, and shape variation to flag suspected flames. Adjustable sensitivity and minimum area; triggers event/notification.

Disclaimer: For supplementary use only; not a replacement for code - compliant fire detection.

22.5 Video Intercom

1. In Settings, go to **Image & Sound** > **Voice Mode**, and select a voice mode.
2. When someone presses the F18 Pro doorbell, the app shows the call screen.
3. If the app is in the foreground on the Home screen, the call screen opens directly; otherwise, you'll receive a push notification - tap it to open the call screen.
4. The call screen layout varies by voice mode. See the examples below.

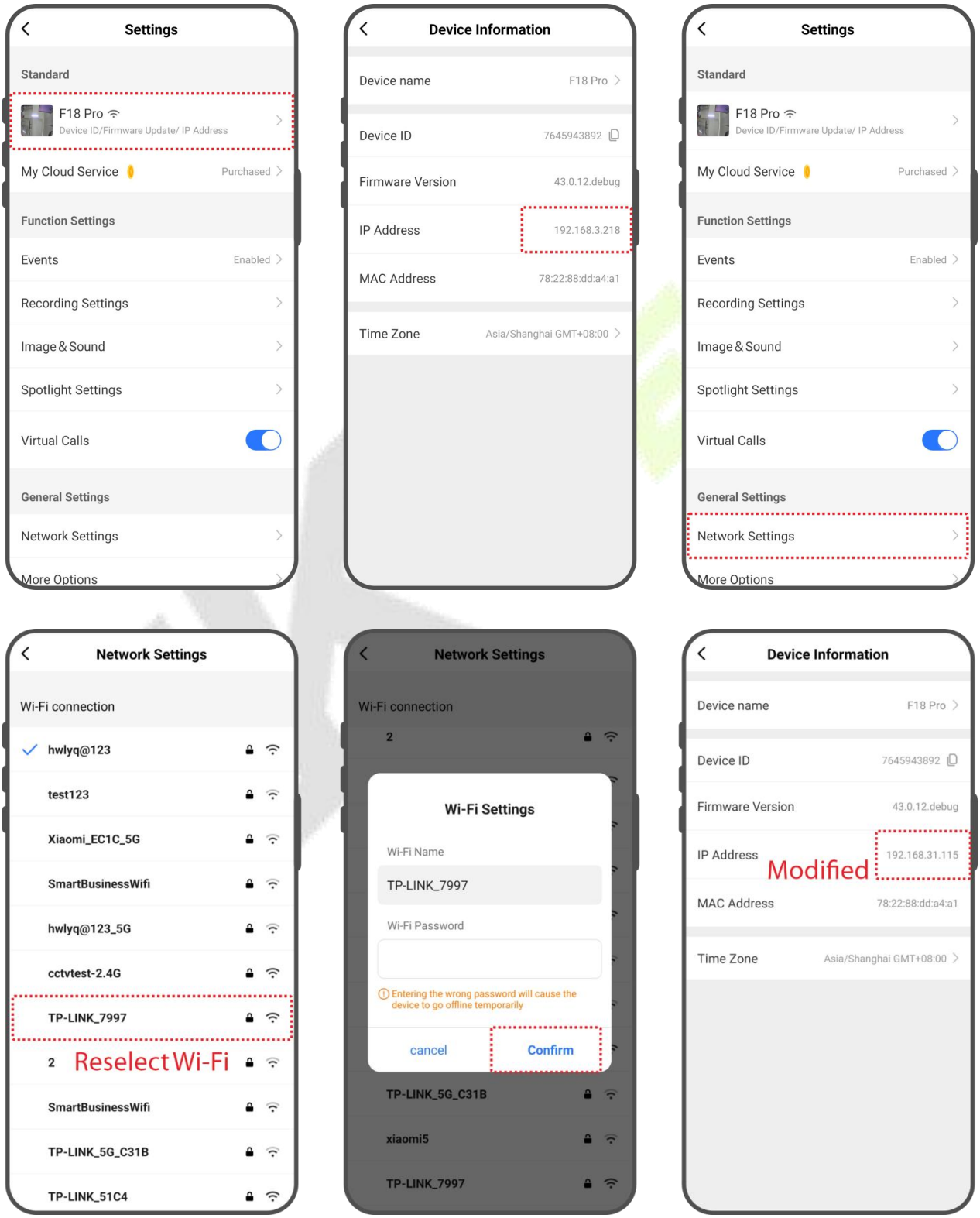


22.6 Reconfigure the intercom module's Wi-Fi

Note: This process only configures the Wi-Fi for the intercom module and does not configure the Wi-Fi for the F18 Pro machine.

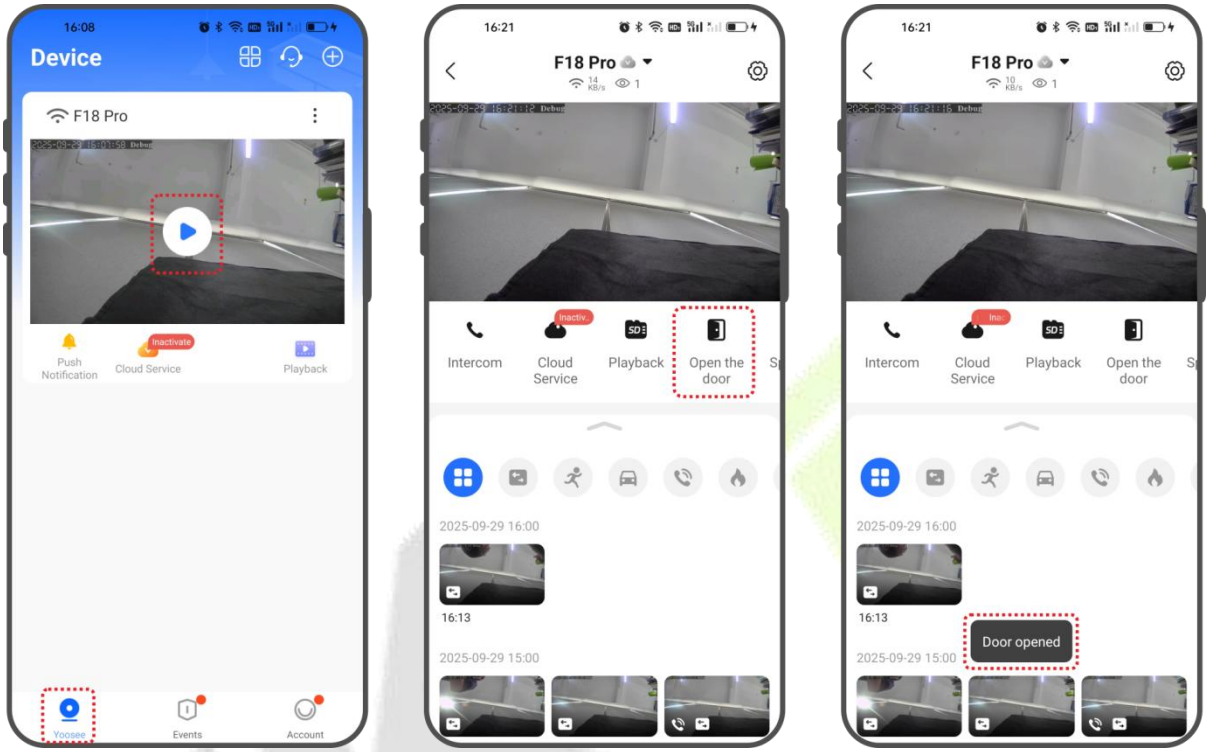
1. Click the ⋮ icon in the upper-right corner and select **Settings** from the dropdown menu.

2. Click the **device name** to enter the **Device Information** interface. You can view the device's IP address.
3. You can modify the Wi-Fi settings for the intercom module by tapping **Network Settings** in the settings interface.
4. Reselect the Wi-Fi network you wish to connect to, enter the password, and click **Confirm**.
5. Once connected, the IP address on the device information screen will update to the new address.



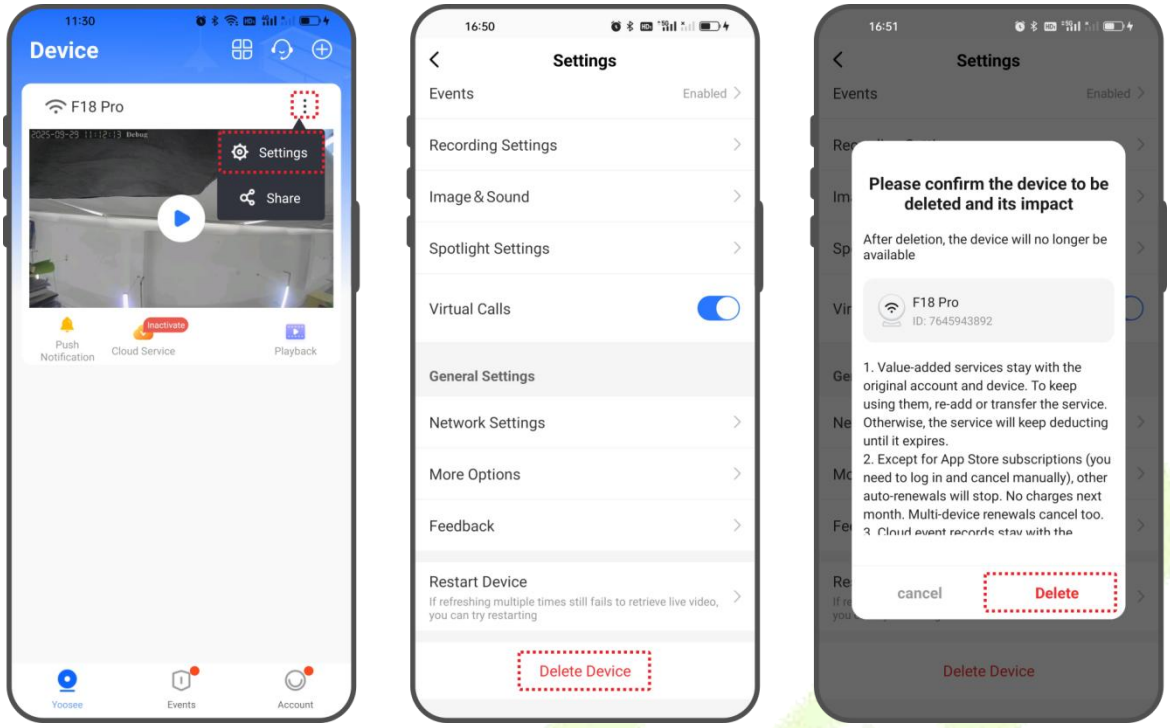
22.7 Remote Door Unlocking

1. Tap button on the app's main interface to enter the live video interface.
2. Then tap the icon to remotely unlock the door. The device will voice prompt "**Door opened**" and the app will display a notification.



22.8 Delete Device

1. Click the icon in the upper-right corner and select **Settings** from the dropdown menu.
2. In the Settings interface, scroll to the very bottom and tap **Delete Device**.
3. Then click **Delete** in the pop-up window.



When removing a device:

1) Remove the device from the app. The intercom module will beep once.
2) Wait for the module to restart. It will beep three times (beep-beep-beep).
3) After the three beeps, disconnect the device's power.

To re-add the device:

1) On the device, navigate to **System** > **Video Intercom Parameters** > **Reset**.
2) Wait for the reset to complete.
3) Scan the device's QR code in the app to bind it again.

Important: Do not disconnect power before hearing the three-beep restart tone, or the module may not reset properly.

Appendix 1

Privacy Policy

Notice:

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

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

I. Collected Information

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

1. **User Registration Information: At your first registration, the feature template (Fingerprint template/Face template/Palm template**) will be saved on the device according to the device type you have selected to verify the unique similarity between you and the User ID you have registered. You can optionally enter your Name and Code. The above information is necessary for you to use our products. If you do not provide such information, you cannot use some features of the product regularly.

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

II. Product Security and Management

1. When you use our products for the first time, you shall set the Administrator privilege before performing specific operations. Otherwise, you will be frequently reminded to set the

Administrator privilege when you enter the main menu interface. **If you still do not set the Administrator privilege after receiving the system prompt, you should be aware of the possible security risk (for example, the data may be manually modified).**

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

3. Only your user ID is displayed by default. You can set whether to display other user verification information (such as Name, Department, Photo, etc.) under the Administrator privilege. **If you choose to display such information, we assume that you are aware of the potential security risks (for example, your photo will be displayed on the device interface).**

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

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

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

III. How we handle personal information of minors

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

We will only use or disclose personal information of minors collected with their parents' or guardians' consent if and to the extent that such use or disclosure is permitted by law or we have obtained their parents' or guardians' explicit consent, and such use or disclosure is for the purpose of protecting minors.

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

IV. Others

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

Eco-friendly Operation

The product's "eco-friendly operational period" refers to the time 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	○	○	○	×	○	○

This table is prepared in accordance with the provisions of SJ/T 11364.

○ indicates that the total amount of toxic content in all the homogeneous materials is below the limit as specified in GB/T 26572.

× indicates that the total amount of toxic content in all the homogeneous materials exceeds the limit as specified in GB/T 26572.

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