User Manual

Zophon-S1000

Date: July 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 **Zophon-S1000**.

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.

Safety Instruction

These instructions are intended to ensure that user can use the product correctly to avoid danger or property loss.

The precaution measure is divided into Dangers and Cautions:
Dangers: Neglecting any of the warnings may cause serious injury or death. Cautions:
Neglecting any of the cautions may cause injury or equipment damage.

Symbols

Convention	Description
	**Dangers:** Follow these safeguards to prevent serious injury or death.
	**Cautions:** Follow these precautions to prevent potential injury or material damage.

Dangers:

- In the use of the product, you must be in strict compliance with the electrical safety regulations of the nation and region.
- The equipment must be connected to an earthed mains socket-outlet.
- Shock hazard! Disconnect all power sources before maintenance.
- Do not touch the bare metal contacts of the inlets after the circuit breaker is turned off. Electricity still exists.
- To prevent possible hearing damage, do not listen at high volume levels for long periods.
- All the electronic operation should be strictly compliance with the electrical safety regulations, fire prevention regulations and other related regulations in your local region.
- Please use the power adapter, which is provided by normal company. The power consumption cannot be less than the required value.
- Do not connect several devices to one power adapter as adapter overload may cause over-heat or fire hazard.
- Please make sure that the power has been disconnected before you wire, install or dismantle the device.
- If the top caps should be open and the device should be powered on for maintenance, make sure:
  1. Power off the fan to prevent the operator from getting injured accidentally.
  2. Do not touch bare high-voltage components.
  3. Make sure the switch's wiring sequence is correct after maintenance.
- Please make sure that the power has been disconnected before you wire, install or dismantle the device.

- If smoke, odors or noise rise from the device, turn off the power at once and unplug the power cable, and then please contact the service center.
- If the product does not work properly, please contact your dealer or the nearest service center. Never attempt to disassemble the device yourself. (We shall not assume any responsibility for problems caused by unauthorized repair or maintenance.)
- The Terminal PE of the switch should be connected to a ground wire.

Cautions:

- Instructions must be read before installation. Please follow these instructions carefully, incorrect installation could affect gate operation.
- When mounting and positioning this product please ensure the power cable is unplugged.
- The motor cover will need to be removed to mount the motor to the mounting plate. Electrical-related operation of the main unit can only be made by a licensed electrician.
- To prevent injury, this equipment must be securely attached to the floor/base of the turnstile in accordance with the installation instructions.
- Keep straight down when moving or using the equipment.
- Never place the equipment in an unstable location. The equipment may fall, causing serious personal injury or death.
- Cold-rolled SPCC steel may be corroded in some circumstances. You need to clean and care the device by using the stainless steel cleaner. It is suggested to clean the device every month.
- Do not drop the device or subject it to physical shock, and do not expose it to high electromagnetism radiation. Avoid the equipment installation on vibrations surface or places subject to shock (ignorance can cause equipment damage).
- Do not place the device in extremely hot (refer to the specification of the device for the detailed operating temperature), cold, dusty or damp locations, and do not expose it to high electromagnetic radiation.
- The device cover for indoor use shall be kept from rain and moisture.
- Exposing the equipment to direct sun light, low ventilation or heat source such as heater or radiator is forbidden (ignorance can cause fire danger).
- Do not aim the device at the sun or extra bright places. A blooming or smear may occur otherwise (which is not a malfunction however), and affecting the endurance of sensor at the same time.
- Please use the provided glove when open up the device cover, avoid direct contact with the device cover, because the acidic sweat of the fingers may erode the surface coating of the device cover.
- Please use a soft and dry cloth when clean inside and outside surfaces of the device cover, do not use alkaline detergents.
- Please keep all wrappers after unpack them for future use. In case of any failure occurred, you need to return the device to the factory with the original wrapper. Transportation without the original wrapper may result in damage on the device and lead to additional costs.

- Improper use or replacement of the battery may result in hazard of explosion. Replace with the same or equivalent type only. Dispose of used batteries according to the instructions provided by the battery manufacturer.
- Biometric authentication products are not 100% applicable to anti-spoofing environments. If you require a higher security level, use multiple authentication modes.
- Do not stay in the lane when the device is rebooting.
- RISK OF EXPLOSION IF BATTERY IS REPLACED BY AN INCORRECT TYPE. DISPOSE OF USED BATTERIES ACCORDING TO THE INSTRUCTIONS.
- SUITABLE FOR MOUNTING ON CONCRETE OR OTHER NON-COMBUSTIBLE SURFACE ONLY.
- The instructions shall require connection of the equipment protective earthing conductor to the installation protective earthing conductor.

Table of Contents

1 Overview

ZKTeco's multimodal biometric access control modules are a smart and professional access control system for pedestrian passage products. It is integrated with turnstiles. The device consists of several modules, such as the Face/RFID/QR/Palm recognition module, the LCD display, and the main/sub access control board. Based on the Android system, it supports NFC/Wi-Fi or TCP/IP communication with external devices. You can easily view and change the device's settings by connecting the device to your cell phone via NFC/Wi-Fi or connecting devices to the computer with an ethernet cable.

The module features a high degree of flexibility, allowing for diverse combinations based on the requirements of specific scenarios. Whether it involves choosing different types of authentication methods or adding display screens, it can fully meet the customers' varied and multifaceted needs. Currently, the multimodal recognition module not only supports integration into ZKTeco's mainstream products but also allows for the integration of the product module into third-party devices. For example, customers can obtain a standalone module for their own design and installation. Additionally, customized services are provided to install and fix the modules in the desired manner as an accessory kit.

When connected to the turnstile control board, whether on ZKTeco's own products or integrated with third-party systems, the module can be connected to the turnstile control board via the data communication protocol (RS485). This enables the monitoring of device status and remote control operations. The module supports communication with external devices through Near Field Communication (NFC), wireless networks (Wi-Fi), or the Transmission Control Protocol/Internet Protocol (TCP/IP). You can easily connect the device to a smartphone via NFC or Wi-Fi, or connect it to a computer using an Ethernet cable to conveniently view and modify device settings.

1.1 Key Features

- **Comprehensive Multi-Authentication Options.**

  Supports Face, Palm, RFID, QR Code for enhanced flexibility and security.

- **Advanced Biometric Authentication.**

  Offers superior biometric performance for both palm and facial recognition, ensuring accurate and reliable access control.

- **Wide-Angle Camera for Enhanced Recognition.**

  Equipped with a wide-angle camera for broader and farther facial recognition, supporting recognition distances of 0.5m to 2m and a field of view as wide as 118.9°.

- **Minimalist Design.**

  Features a sleek and unobtrusive design that seamlessly integrates with existing gate aesthetics without compromising functionality.

- **Seamless Integration.**

  Fully compatible with ZKTeco gates and third-party entrance control systems for flexible deployment.

- **Wi-Fi Enabled for easy configuration.**

  Provides Wi-Fi connectivity, allowing system configurations through a user-friendly HTML5 web interface.

- **OTA update FW**

  FW update via OTA which ensure the device using latest program.

1.2 Technical Specifications

Model	Zophon-S1000
Display	7-inch LCD Screen (1024*600 Pixels)(Optional)
Camera	2MP Binocular Camera
Operation System	Android14
Hardware	CPU: Quad-core A55, Up to 2.0GHz

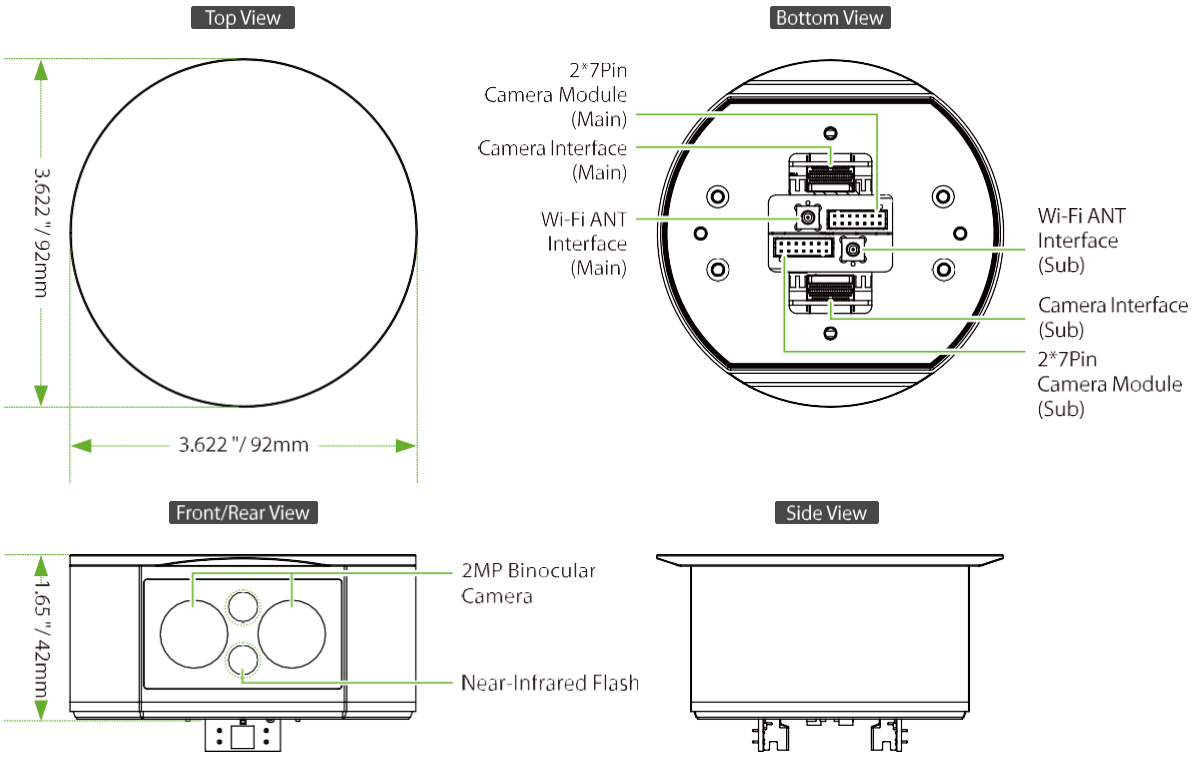
Authentication Method	Face / Palm / Card /QR
Face Template Capacity	100,000 (1:N)
Palm Template Capacity	50,000 (1:N)
Card/QR Capacity	100,000 (1:N)
Transaction Capacity	1,000,000
Biometric Authentication Speed	less than 0.5 sec (Facial Recognition) less than 0.5 sec (Palm Recognition)
Touchless Biometric Authentication Distance	50cm to 200cm (Facial Recognition) 5cm to 15cm (Palm Recognition)
False Acceptance Rate (FAR)%	FAR≤0.01% (Visible Light Facial Recognition) FAR ≤ 0.001% (Palm)
False Rejection Rate (FRR)%	FRR≤0.02% (Visible Light Facial Recognition) FRR ≤ 0.17% (Palm)
Biometric Algorithm	ZKFace V3.9 & PalmElite3.3.3
Card Type	ID Card@125 kHz (Standard) IC Card@13.56 MHz (Standard)
Communication	TCP/IP*1 NFC Wi-Fi (IEEE 802.1 a/b/g/n/ac) @2.4GHz; 5GHz Wiegand Input *1 RS485: ZKTeco RS485*1 Aux Inputs *1, Electric Lock*1, Door Sensor*1, Exit Button*1, Alarm *1
Standard Functions	Blocklist, 14-digit User ID, Access Levels, Groups, Holidays, Anti-passback, Record Query, Schedule Bell, Multiple Verification Methods
Optional Functions	Palm recognition module,QR reader module,LCD display module
Power Supply	24V DC 3A
Operating Temperature	-10°C to 55°C (Indoor application)
Operating Humidity	10% to 90% RH (Non-condensing)
Dimensions	Face recognition module(Φ3.62"*1.65"(Φ92mm*42mm)) Palm recognition module(2.44"*2.44"*0.71"(62mm*62mm*18mm)) QR reader module(2.60"*2.56"*0.86"(66mm*65.13mm*22mm)) RFID reader module(1.49"*1.96"*0.06"(37.75mm*49.80mm*1.6mm)) LCD display module(3.77"*6.40"*0.12"(95.7mm*162.5mm*3mm)) Access control module(3.44"*7.72"*1.14"(94.34mm*196mm* 29mm))

Net Weight	Facial recognition reader: 30g (single side) 40g (double side) QR code reader: 20g Palm recognition module: 80g RFID reader: 10g Display module: 80g Access control board: 250g
Supported Software	ZKBio CVSecurity
Installation	Fasten with screws
Housing Material	Mainly plastic
Ingress Protection Rating	N/A
SDK	Android LCDP PUSH SDK
Certifications	CE, FCC, ISO9001, ISO14001, ISO20000

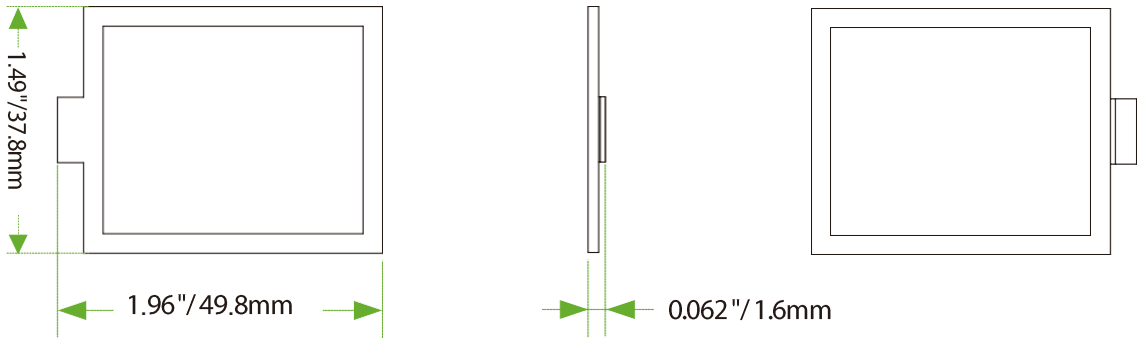
1.3 Appearance of Component Modules

1.3.1 Facial Recognition Module

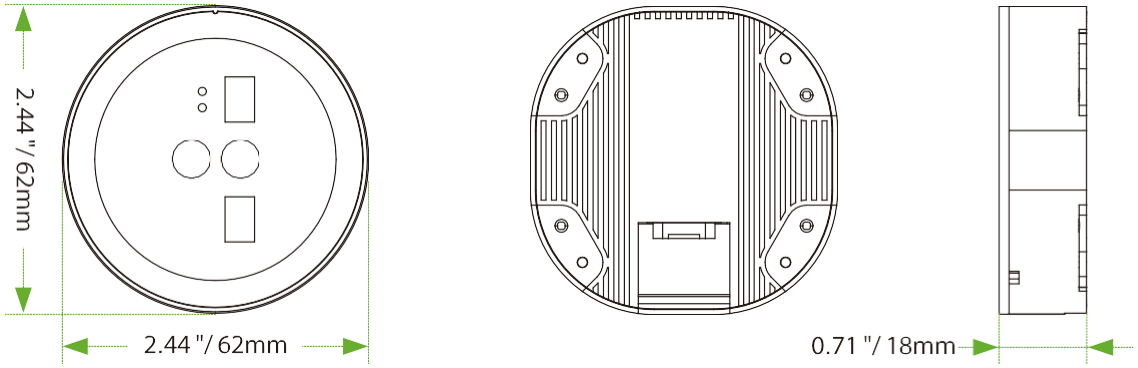
Unit: inch/mm



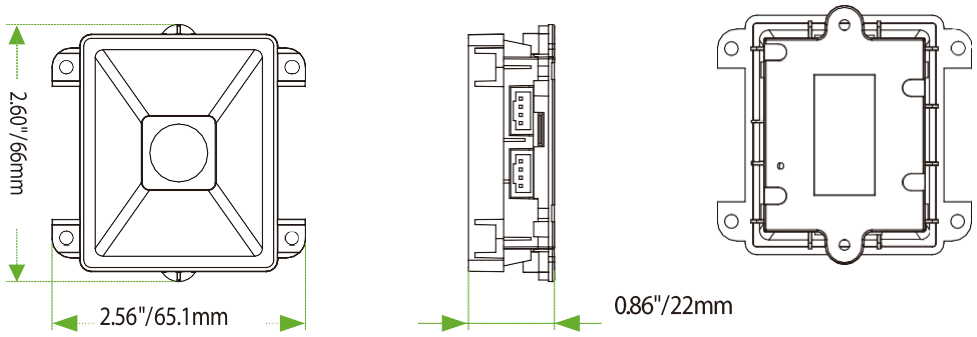
1.3.2 ID/IC Card Reader Module



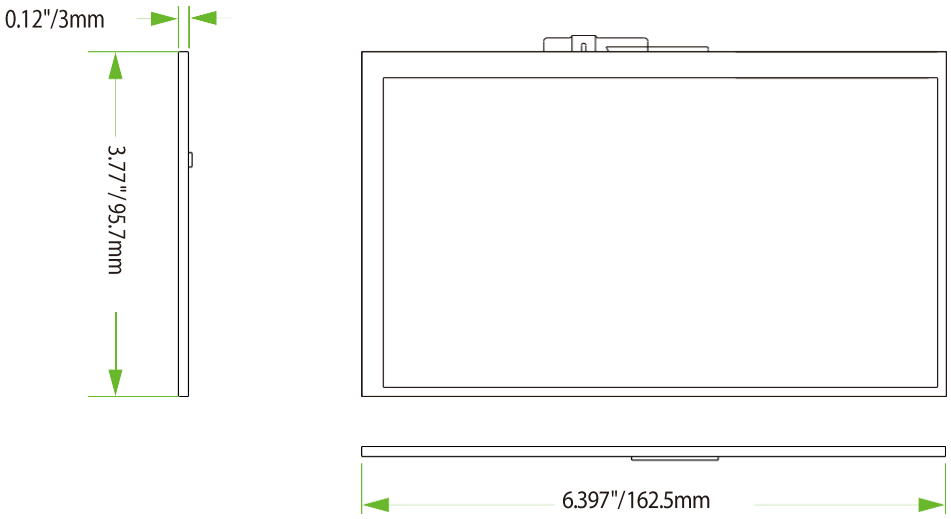
1.3.3 Palm Recognition Module★



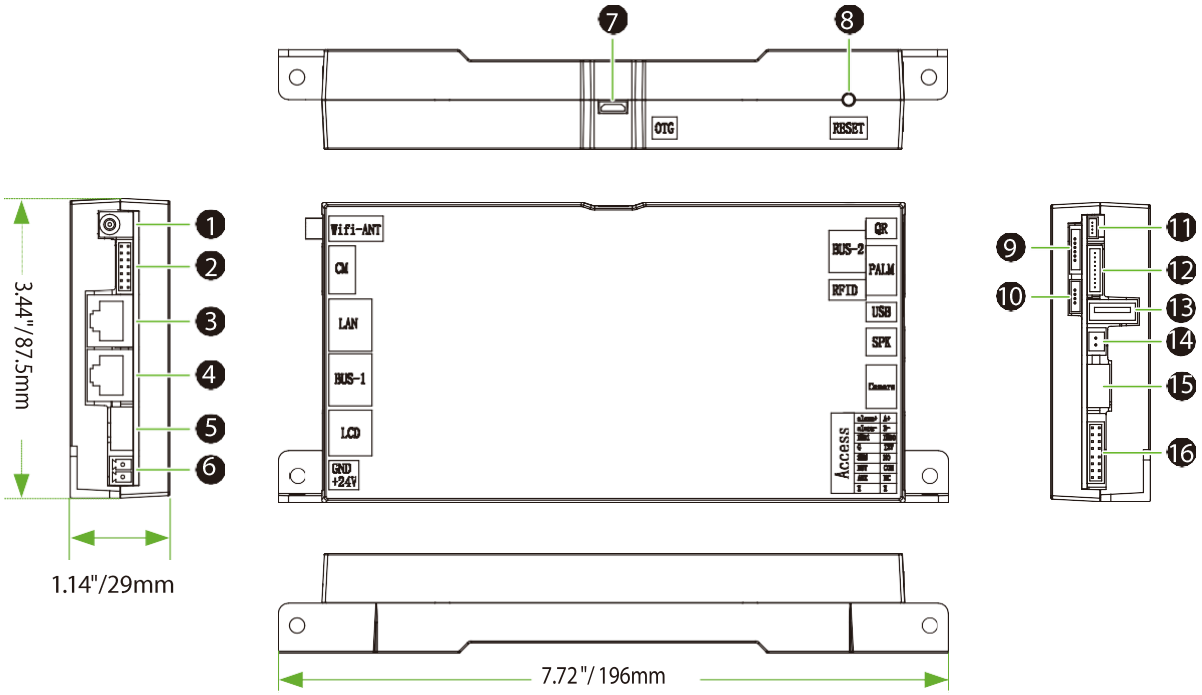
1.3.4 QR Code Reader Module★



1.3.5 LCD Display Module★



1.3.6 Access Control Module



No.	Terminals	Descriptions	Functional Description
1	Wi-Fi ANT	Wi-Fi Antenna	Connect the Wi-Fi antenna.
2	CM	Verification Tip Light	The camera connected to the facial recognition module.
		NFC	
		Camera Fill Light	

<table>
<tr><td>3</td><td>LAN</td><td>Network</td><td>RJ45, Yellow holder
The default device IP address is: 192.168.1.201 Note: In LAN, IP addresses of the server (PC) and the device must be in the same network segment when connecting to the software.</td></tr>
<tr><td>4</td><td>BUS-1</td><td>Synchronised LAN</td><td>Networking, synchronising main and sub devices
RJ45, Blue holder</td></tr>
<tr><td>5</td><td>LCD</td><td>LCD display module</td><td>Used to connect the 7” LCD display module.</td></tr>
<tr><td rowspan="2">6</td><td>GND</td><td rowspan="2">Power Input</td><td rowspan="2">24V DC power supply input</td></tr>
<tr><td>+24V</td></tr>
<tr><td>7</td><td>MicroUSB</td><td>Burn-in Port</td><td></td></tr>
<tr><td>8</td><td>RESET</td><td>Reset</td><td>For resetting account password, IP address</td></tr>
<tr><td rowspan="2">9</td><td rowspan="2">BUS-2</td><td>485-1</td><td>Connecting gate control board</td></tr>
<tr><td>485-2</td><td>Synchronous sub device</td></tr>
<tr><td>10</td><td>RFID</td><td>RFID recognition module</td><td>Used to connect the RFID recognition module.</td></tr>
<tr><td>11</td><td>QR</td><td>QR code reader module</td><td>Used to connect the QR code reader module</td></tr>
<tr><td>12</td><td>PALM</td><td>Palm recognition module</td><td>Used to connect the palm recognition module.</td></tr>
<tr><td>13</td><td>USB</td><td>USB Reservation</td><td></td></tr>
<tr><td>14</td><td>SPK</td><td>Speaker</td><td>To play alarms or alert voices.</td></tr>
<tr><td>15</td><td>Camera</td><td>Camera /
Facial recognition module</td><td>Used to connect the camera.
Can be docked to the camera of the facial recognition module. MIPI Port</td></tr>
<tr><td>16</td><td>Access</td><td>
<table>
<tr><td rowspan="8">Access</td><td>alarm+</td><td>A+</td></tr>
<tr><td>alarm-</td><td>B-</td></tr>
<tr><td>IWD1</td><td>IWD0</td></tr>
<tr><td>G</td><td>12V</td></tr>
<tr><td>SEN</td><td>NO</td></tr>
<tr><td>BUT</td><td>COM</td></tr>
<tr><td>AUX</td><td>NC</td></tr>
<tr><td>X</td><td>X</td></tr>
</table>
</td><td>Used to connect the reader, Access control all-in- one machine. And the relay can be connected directly to the gate control board.

Included:
2 pcs Relays
1 pc 485
1 pc Wiegand input
3 pcs Auxiliary inputs</td></tr>
</table>

2 Authentication Methods

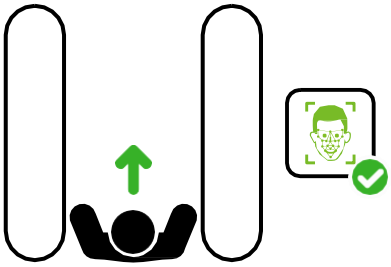
Users can freely choose to configure the authentication module according to actual needs.

2.1 Facial Verification

When the device is configured with a facial recognition module, in facial verification mode, the device compares the collected facial image with all the facial data registered in the device and sends it to the Access Controller.

During the verification process, please try to keep your face facing the camera. When registering your face, please face the camera and remain still until the entry is successful.

Verification is successful:



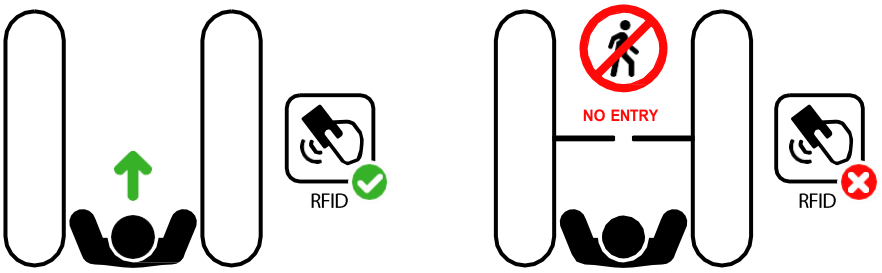
Verification is failed:

2.2 Card Verification

When the device is configured with a card reader module, the Card Verification mode compares the card number in the card induction area with all the card number data registered in the device and sends it to the Access Controller.

When a user presses his / her card on the card reading area, the device enters card authentication mode.

Verification is successful: Verification is failed:

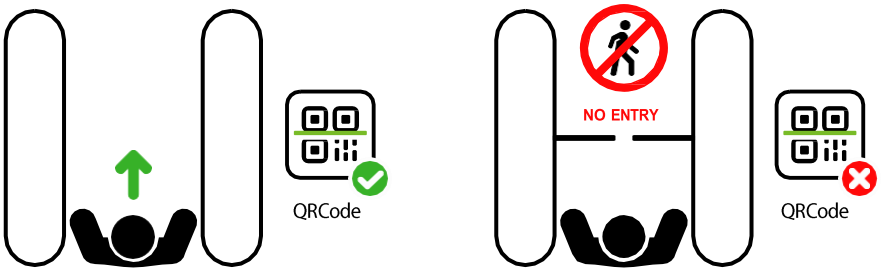


2.3 QR Code Verification★

When the device is configured with a QR code reading module, the QR code on the user's mobile phone can be scanned by a QR code scanner and the data can be compared with the registered QR code and then sent to the Access Controller.

When the user places the mobile phone displaying with the QR code on top of the QR code scanner, the device enters the QR code authentication mode.

Verification is successful: Verification is failed:

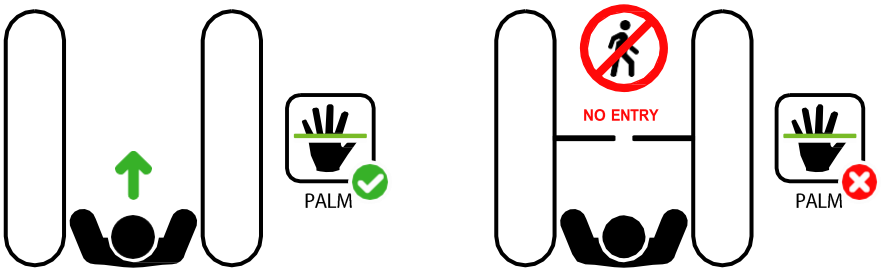


2.4 Palm Verification★

When the device is configured with a palm recognition module, this mode compares the palm image captured by the palm module with all the palm data templates in the device.

Place the palm in the area that can be collected by the palm module, so that the device will automatically switch to palm verification mode.

Verification is successful: Verification is failed:



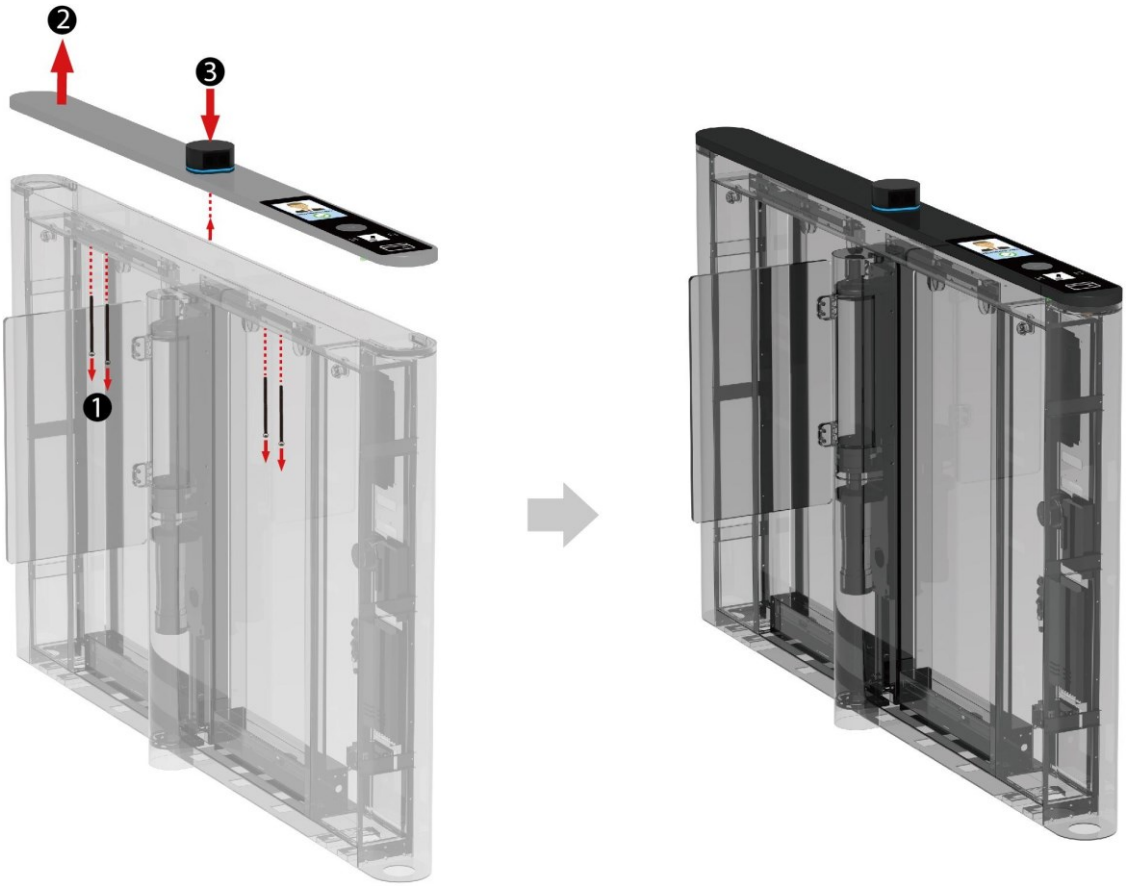
When registering and verifying your palm, please pay attention to the following points:

1. Place the palm of your hand within a distance of 7.87" to 19.69" (20 cm to 50 cm) from the device.
2. Keep the entire palm parallel to the device, ensuring that the middle finger is pointing vertically upward.
3. All five fingers must be naturally spread apart and must not be bent or pressed together.

3 Facial Recognition Module Installation

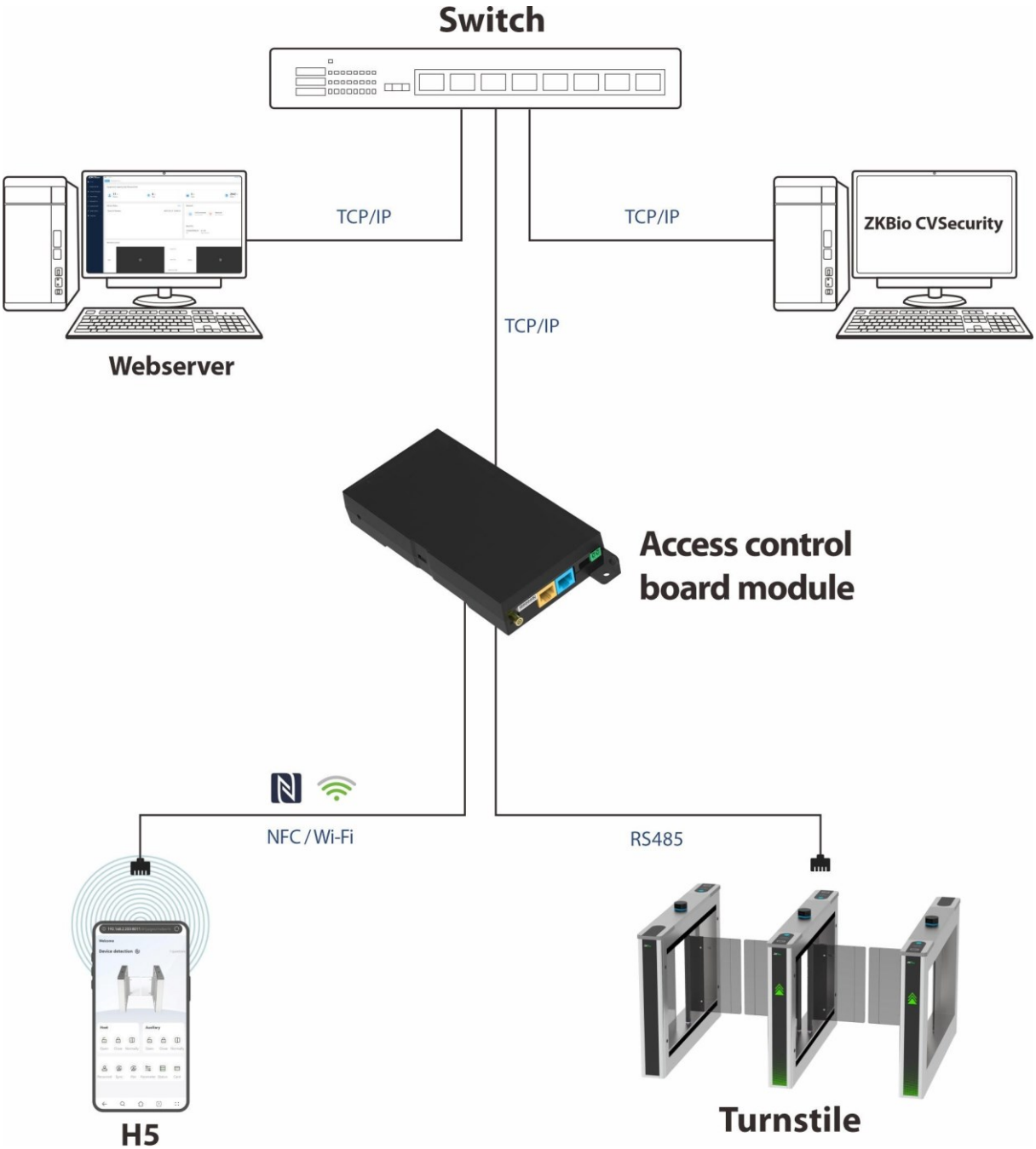
The facial recognition module is installed using screws. The images of the turnstile shown here are for illustrative installation purposes only. Please refer to the actual product purchased.

1. As shown in the figure below, loosen the fixing screws of the upper cover from the bottom and open the upper cover plate. Then, pass the facial recognition module cable through the pre-drilled installation hole.
2. Adjust the module to the appropriate angle.
3. Tighten the screws from the bottom to secure the module to the upper cover plate.
4. After the installation is complete, reinstall the upper cover and fasten the screws.
5. The effect after installation is shown in the figure on the right. The installation methods for other modules are similar and will not be described in detail here.



Note: The installation methods may vary depending on different products. Please refer to the actual product for details.

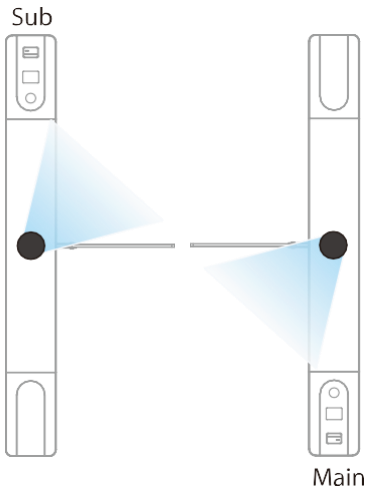
4 Configuration



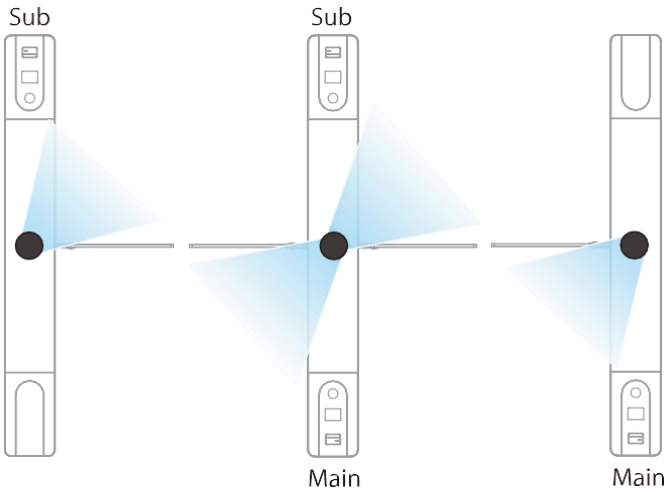
5 Wiring Instructions

5.1 Lane Composition

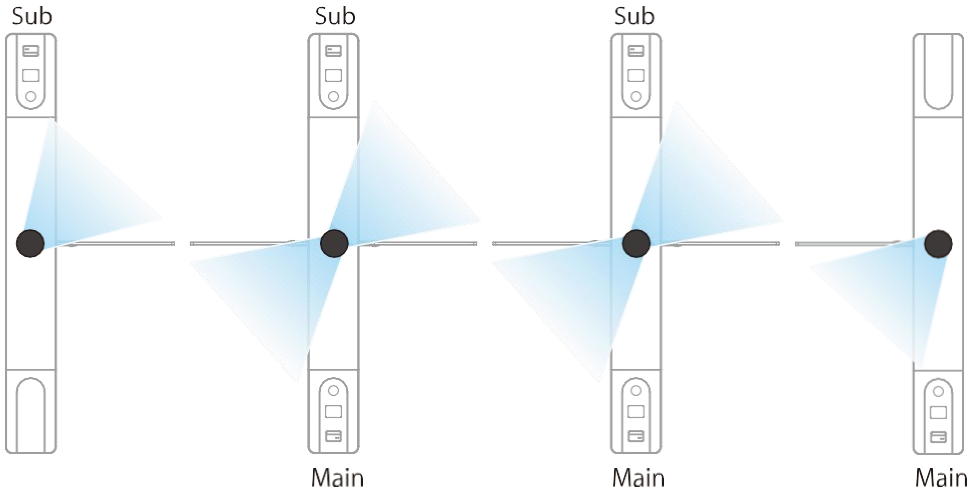
The module can be applied to single-lane, dual-lane and multi-lane with the effect as shown below.



Single-lane

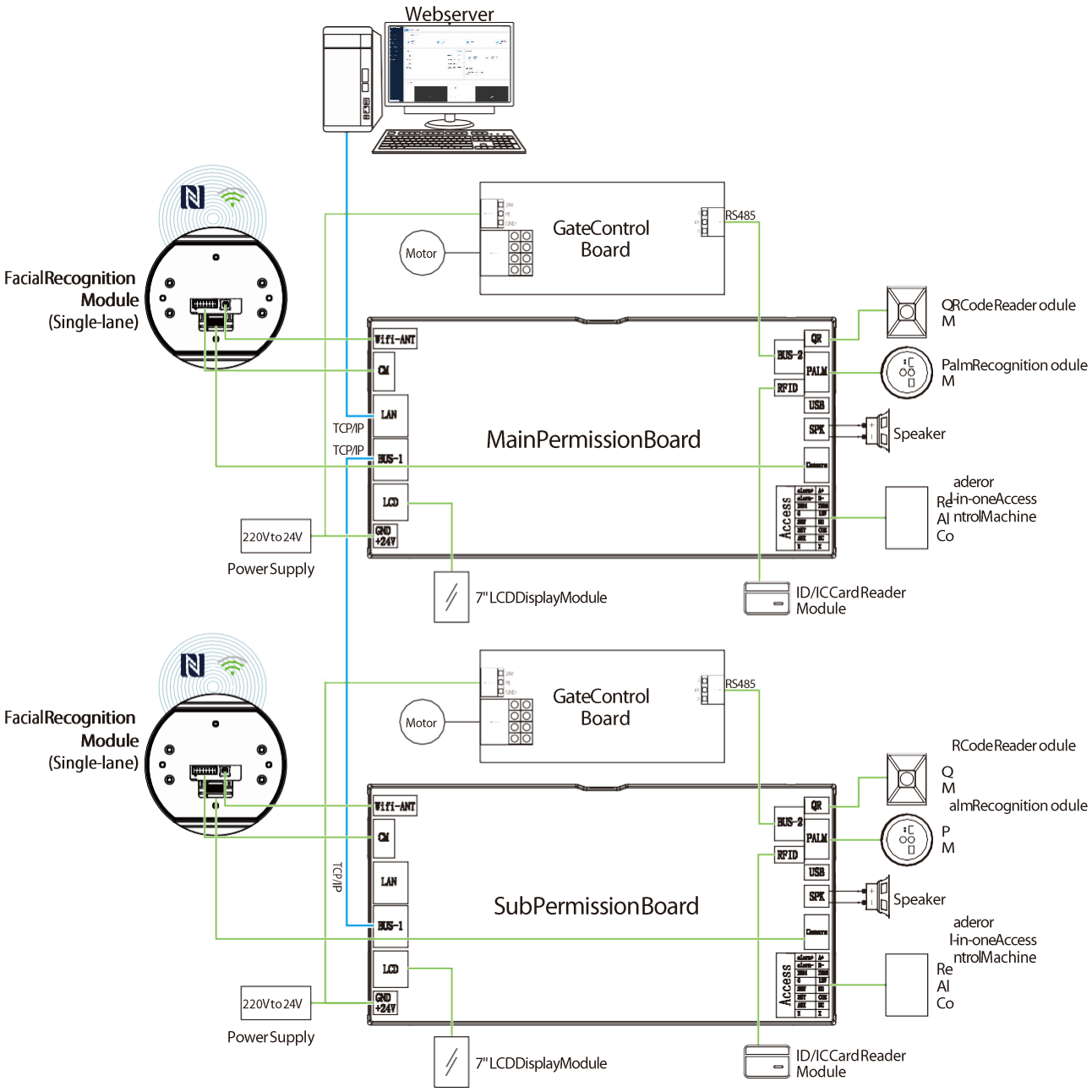


Dual-lane

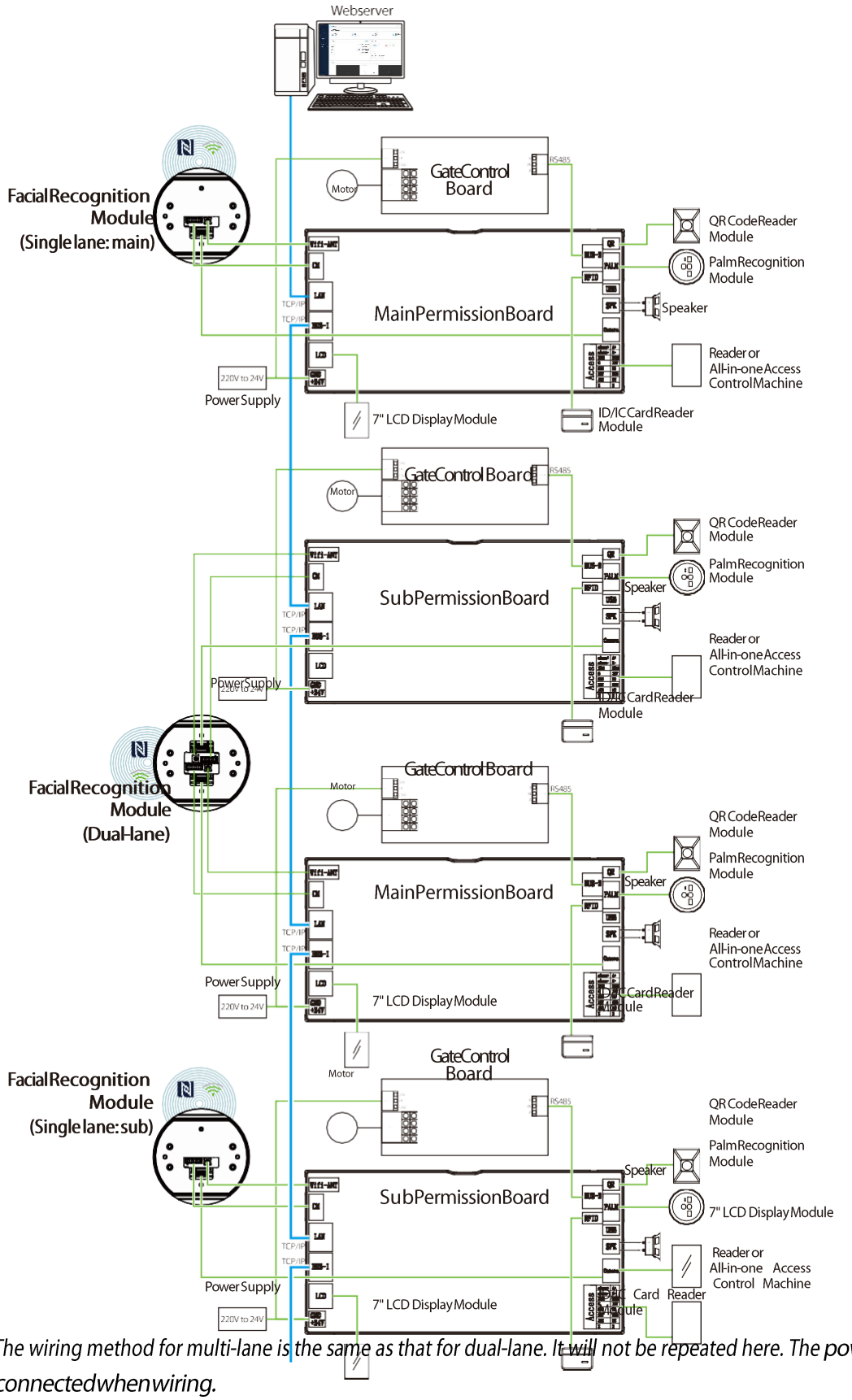


Multi-lane

5.2 Single-lane wiring instructions



5.3 Dual-lane wiring instructions



Note: *The wiring method for multi-lane is the same as that for dual-lane. It will not be repeated here. The power must be disconnected when wiring.*

6 Connect to Web server

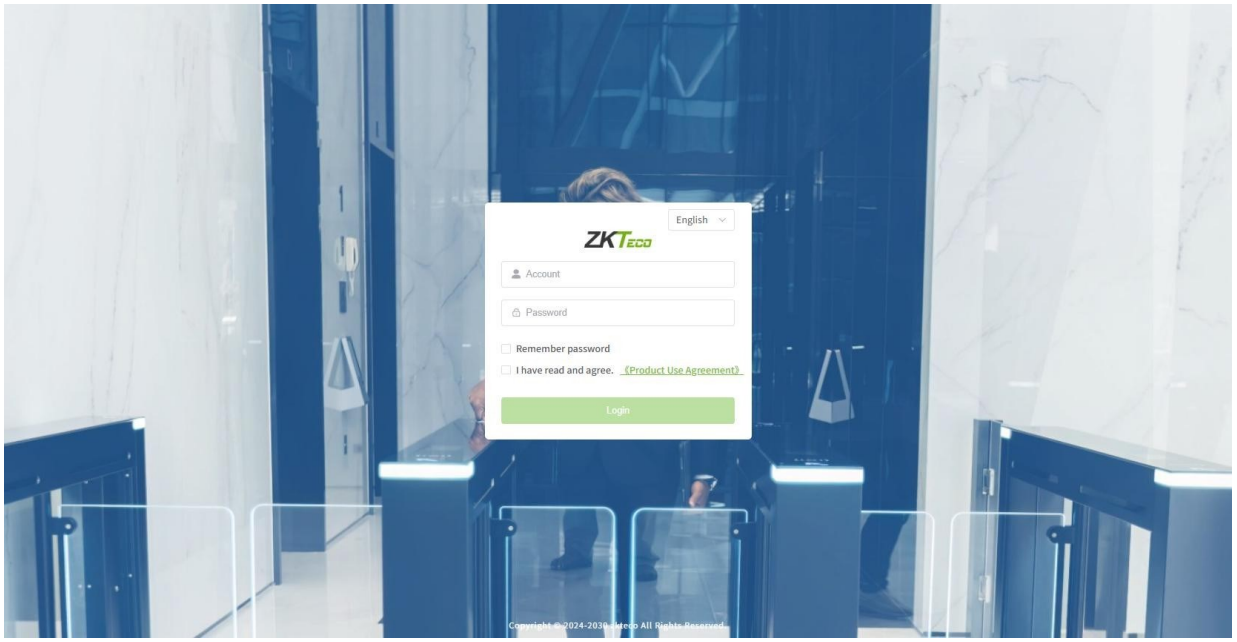
Connect the device to the network cable and power it on. After configuring the device and the computer on the same local area network and the same subnet, you can access the Web server of the device via the computer to configure various parameters.

6.1 Login to the Web server

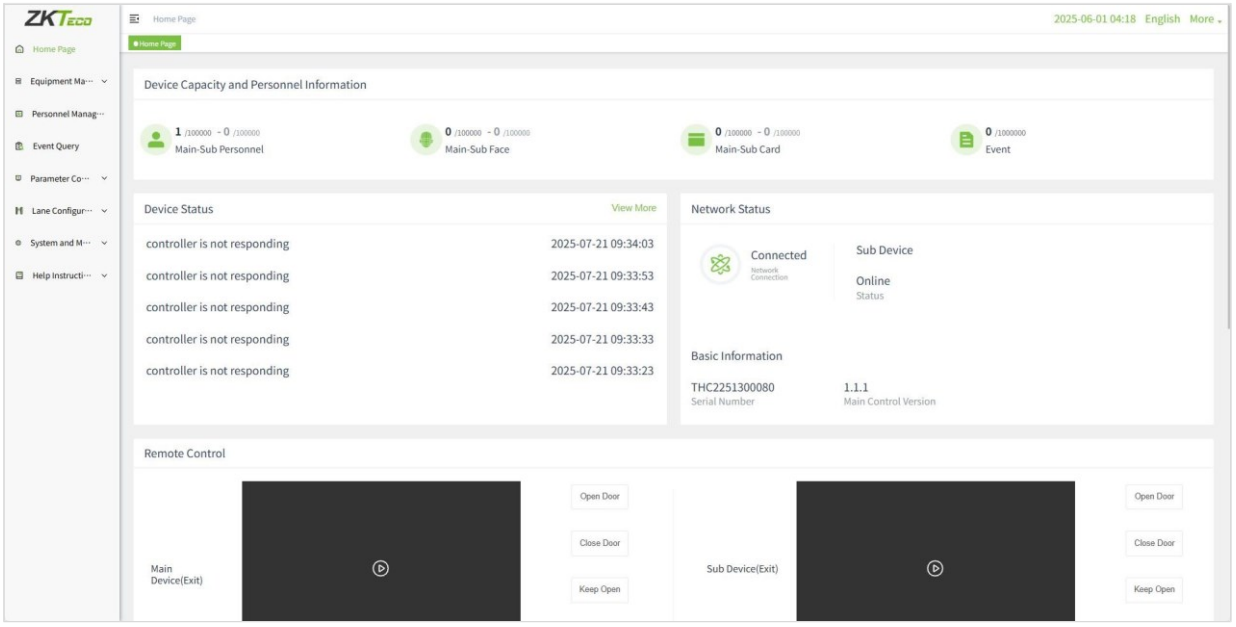
1. Enter the address in the browser to log in to the Web server. The address is: https://IP address:8011, for example, 192.168.1.201:8011.
   The default IP address of the device is **192.168.1.201**. The default port number is: **8011**.

2. When no system administrator has been added to the device, a prompt window saying "**Add a system administrator**" will pop up when logging into the Web server. Just click [**Confirm**] to enter the homepage, as shown in the figure below.

3. When a system administrator is added to the device, the administrator needs to authenticate before accessing the home page, as shown in the figure below. Enter the administrator's account and password on the login page, check the agreement, and then click [**Login**].



4. After successful login, you will enter the screen shown below.

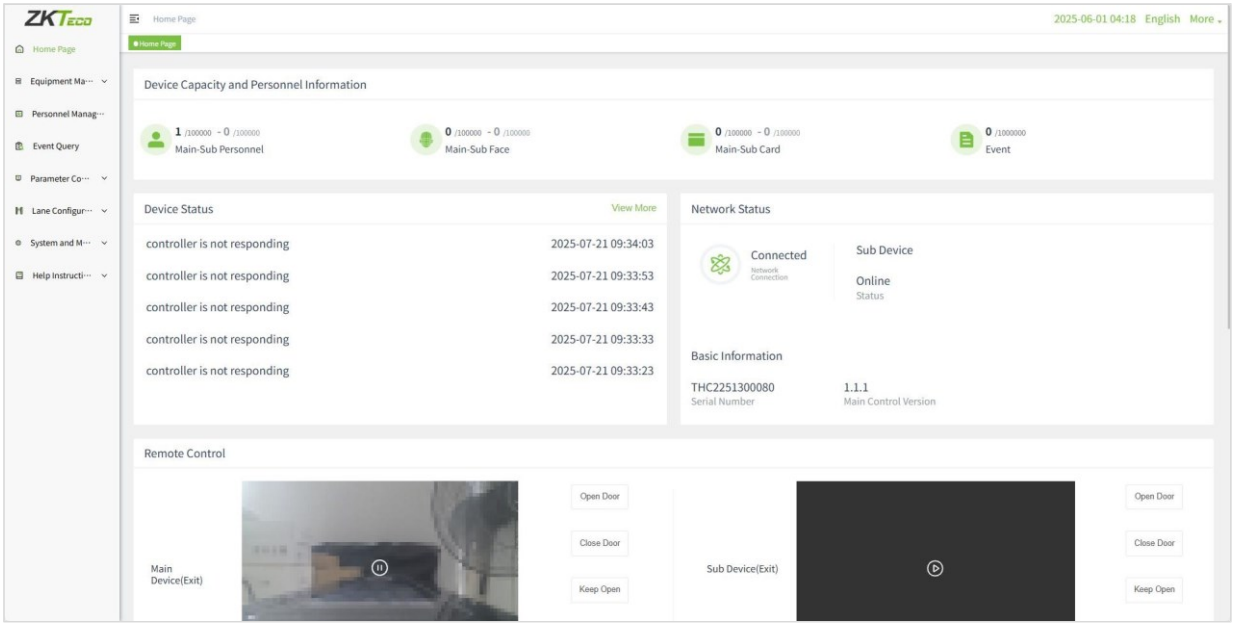


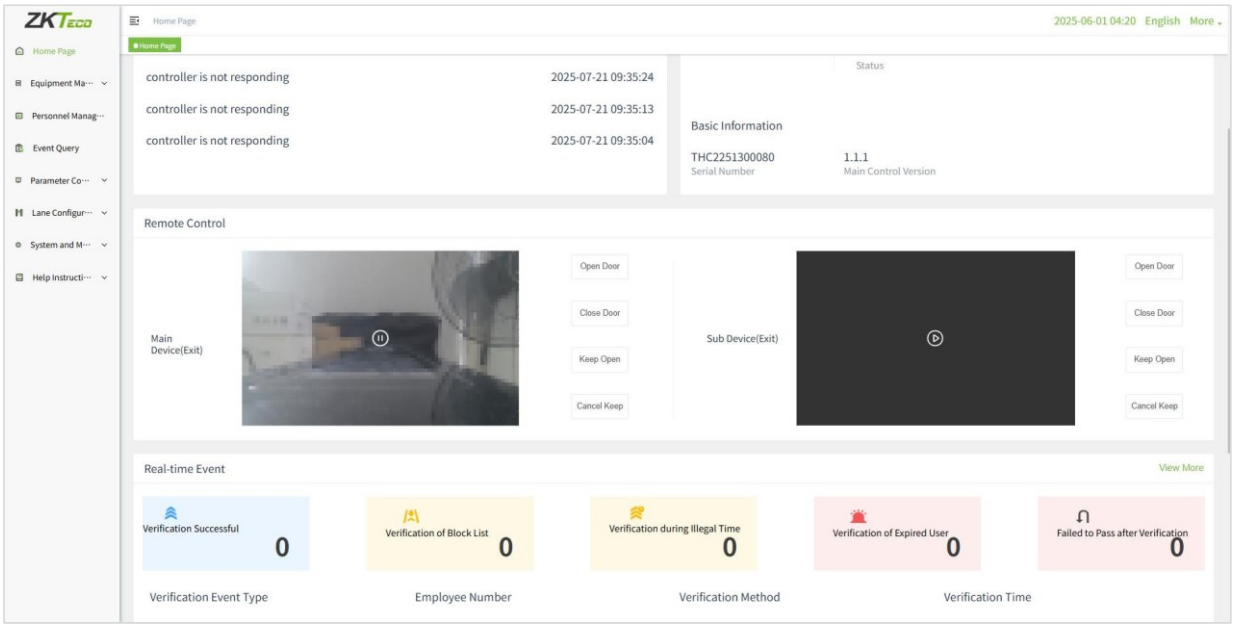
Note:

1. *For the security of the device, it is recommended to register system administrator the first time you use the device.*
2. *You can click on [**User Management**] - [**Add**] in the left-hand menu bar to add a system administrator. For details, please refer to Section 6.4 User Management.*

6.2 Home Page

On the home page users can view items such as Equipment Capacity And Personal Information, Device Status, Network status, basic equipment information, Remote Control open/close doors and Live Events.





- **Remote Control**

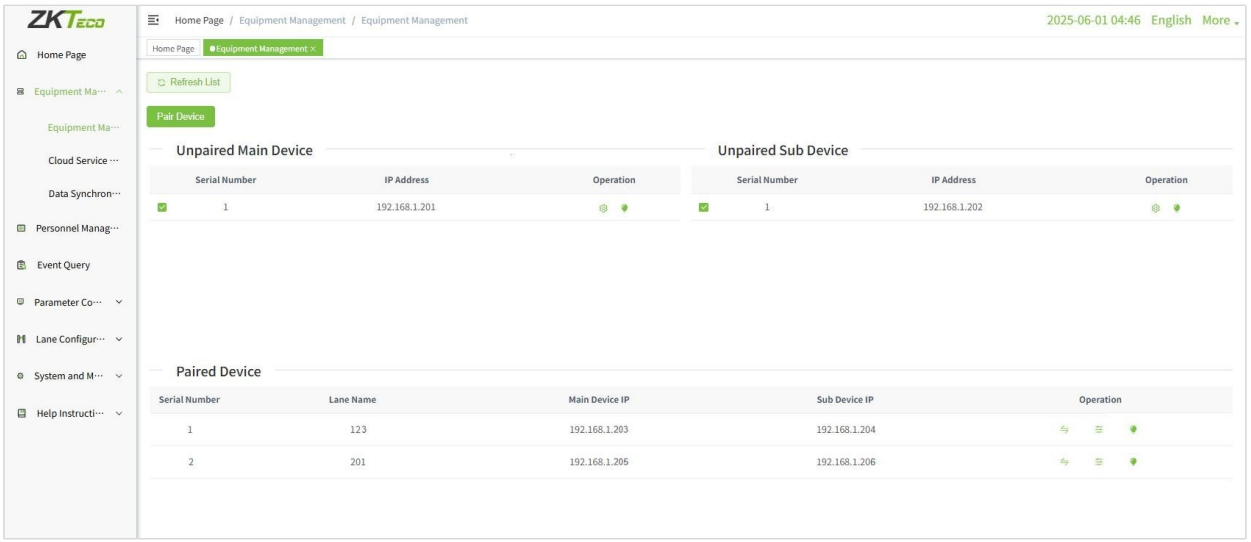
In the remote control bar, click the icon on the main/sub remote control interface to view the live video. You can also click [Close Door] / [Open Door] / [Keep Door Open] to perform remote control operations.

6.3 Equipment Management

In the Device management interface, you can configure parameters such as device management and data synchronization.

6.3.1 Equipment Management

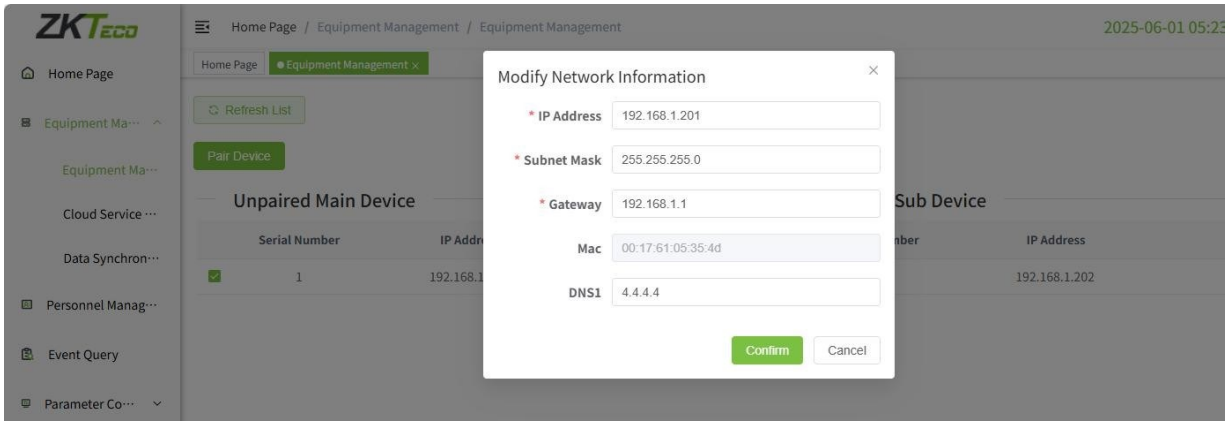
Click [**Equipment Management**] - [**Equipment Management**] in the left menu bar to enter the equipment management setting interface.



6.3.1.1 Modify device IP address

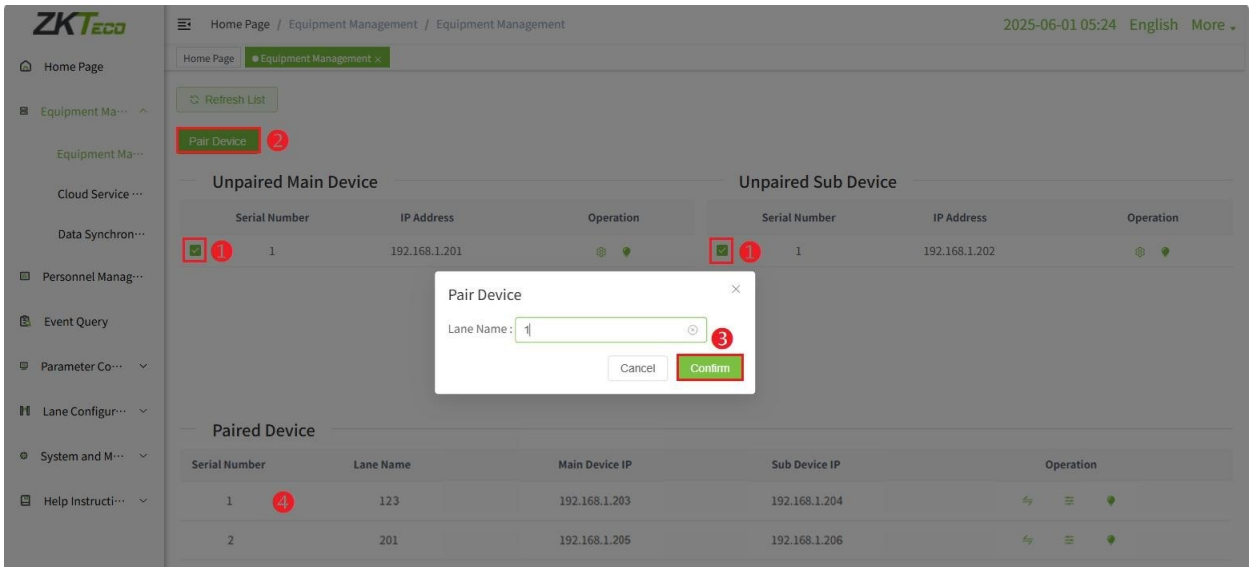
In the device management interface, select the device and click the icon next to the device to modify its IP address. Ensure that the IP addresses of the main and sub devices, as well as the computer's IP address, are within the same subnet. For example, you can modify the device IP addresses as follows:

192.168.1.201 for Main A, 192.168.1.202 for Sub A, 192.168.1.203 for Main B, 192.168.1.204 for Sub B, and so on. Click the icon next to the device to light up the device's LED, which will help you easily identify and confirm the current device.



6.3.1.2 Pairing Device

After modifying the IP address, check the main/sub devices that need to be paired, click [**Pairing Device**]. In the pop-up Pairing Device window, enter the passage name and then click [**Confirm**]. The paired devices will be displayed in the Paired Device section, as shown in the figure below.

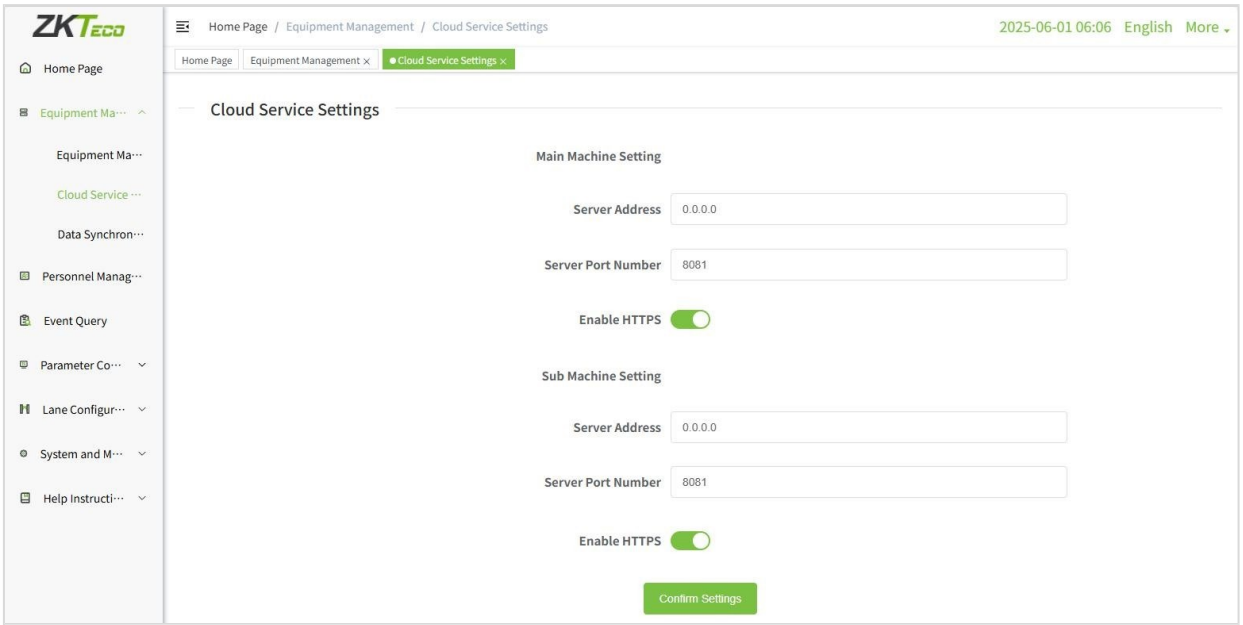


After pairing, the devices can perform operations such as synchronizing data, synchronizing parameters, and lighting up the LED lights simultaneously.

Note: *Before pairing the devices, please ensure that the connection cables between the main and sub devices are connected correctly.*

6.3.2 Cloud Service Settings

Click [**Equipment Management**] - [**Cloud Service Settings**] in the left menu bar to set the server address and server port.

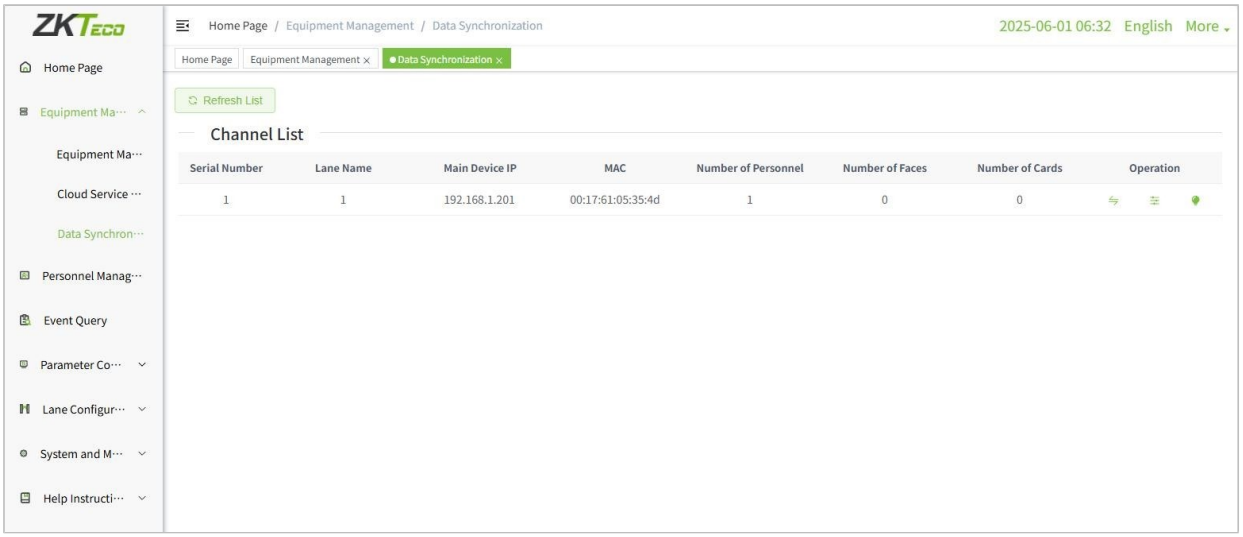


Server address: Set as the IP address of ZKBio CVSecurity server. (**Note:** The IP address of the device should be able to communicate with the ZKBio CVSecurity server, preferably in the same network segment with the server address).

Server port: Set as the service port of ZKBio CVSecurity (The default is 8088).

6.3.3 Data Synchronization

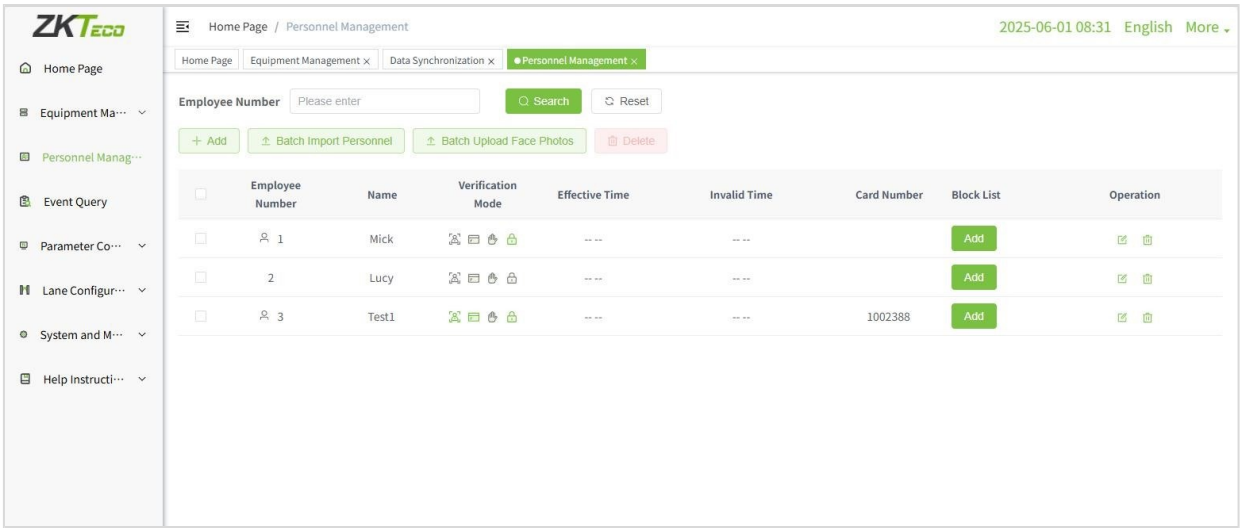
Click [**Equipment Management**] - [**Data Synchronization**] in the left menu bar to enter the data synchronization setting interface.



In the lane list, select the device to synchronize data with, click the ⇋ or ⚙ icon next to it, and then choose the target device in the pop-up window to perform data synchronization or parameter synchronization operations.

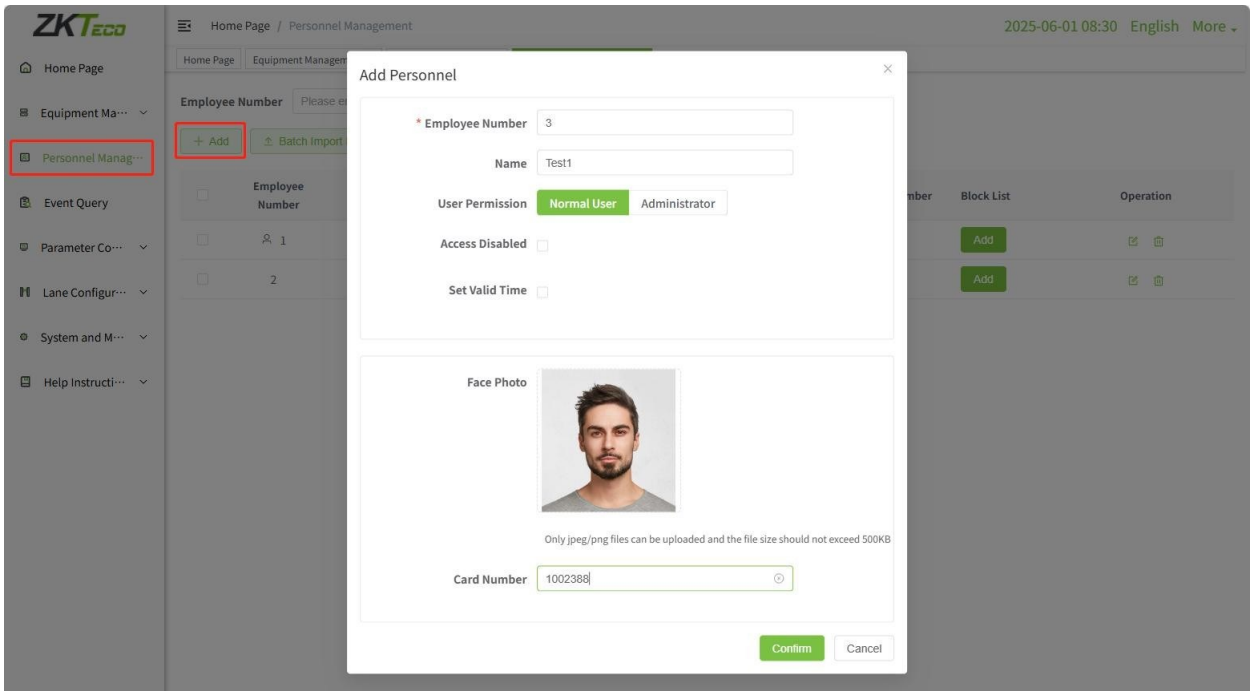
6.4 User Management

Click [**User Management**] in the left menu bar to enter the user management setting interface.

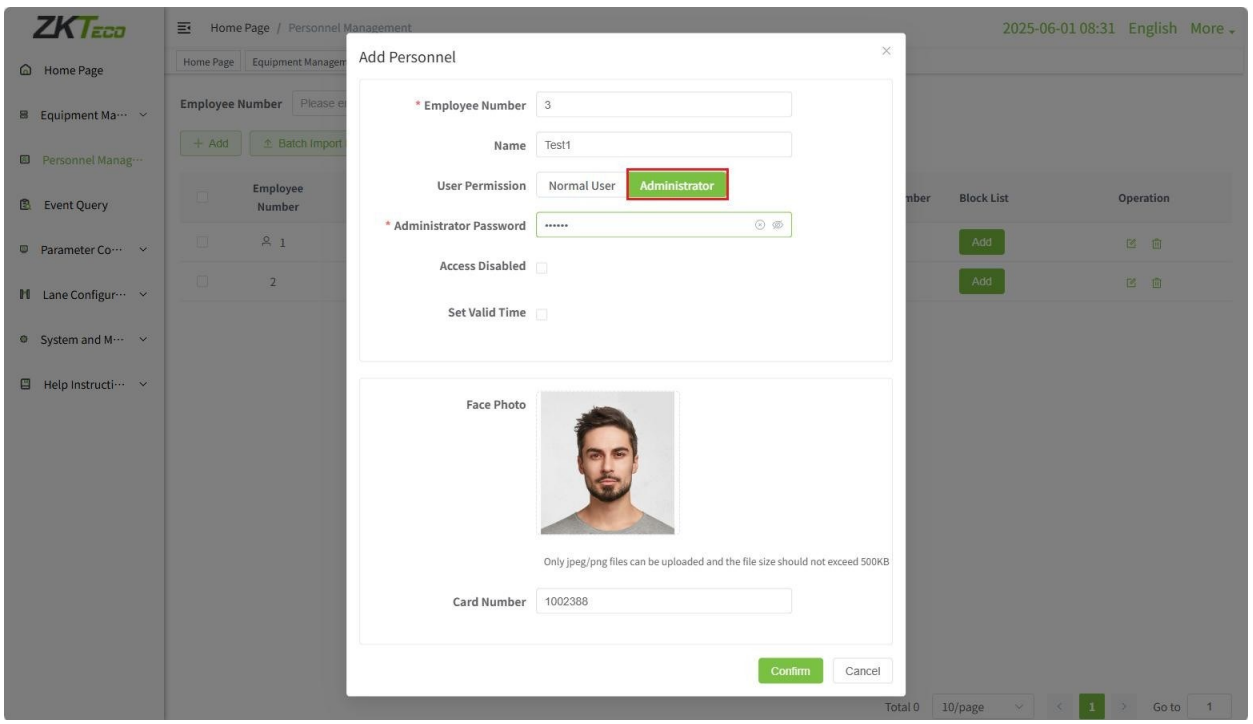


6.4.1 Adding Personnel

In the user management interface, click [**Add**]. In the pop-up Add Personnel window, enter the user pin and name, set user permission and whether it is permanently valid, upload facial photos, and enter the card number, etc. After completing these steps, click [**Confirm**].



When setting a user as an administrator, you need to set an administrator password. The administrator account and password can be used to log in to the device's Web server for device management.



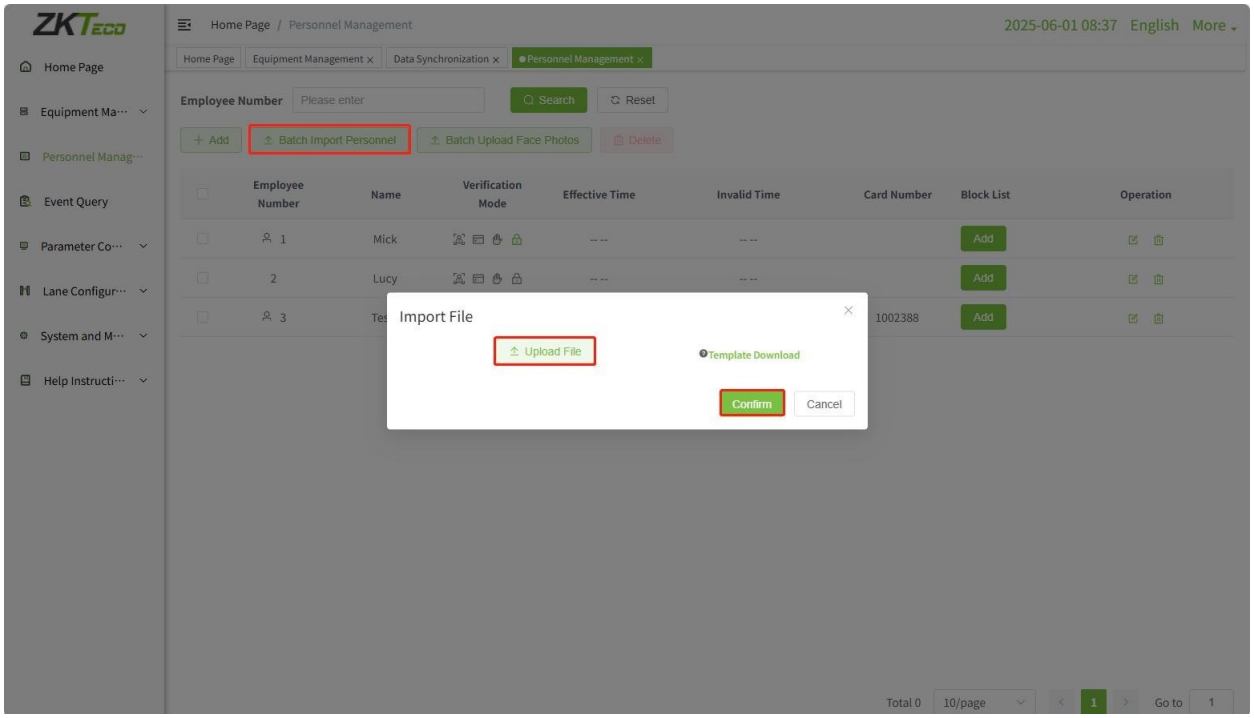
Note: *Only JPEG/PNG files can be uploaded. The size does not exceed 500KB.*

6.4.2 Edit / Delete Personnel

Select the personnel you want to modify or delete from the personnel list, and click the or icon to modify the personnel information or delete the personnel.

6.4.3 Batch Import Personnel

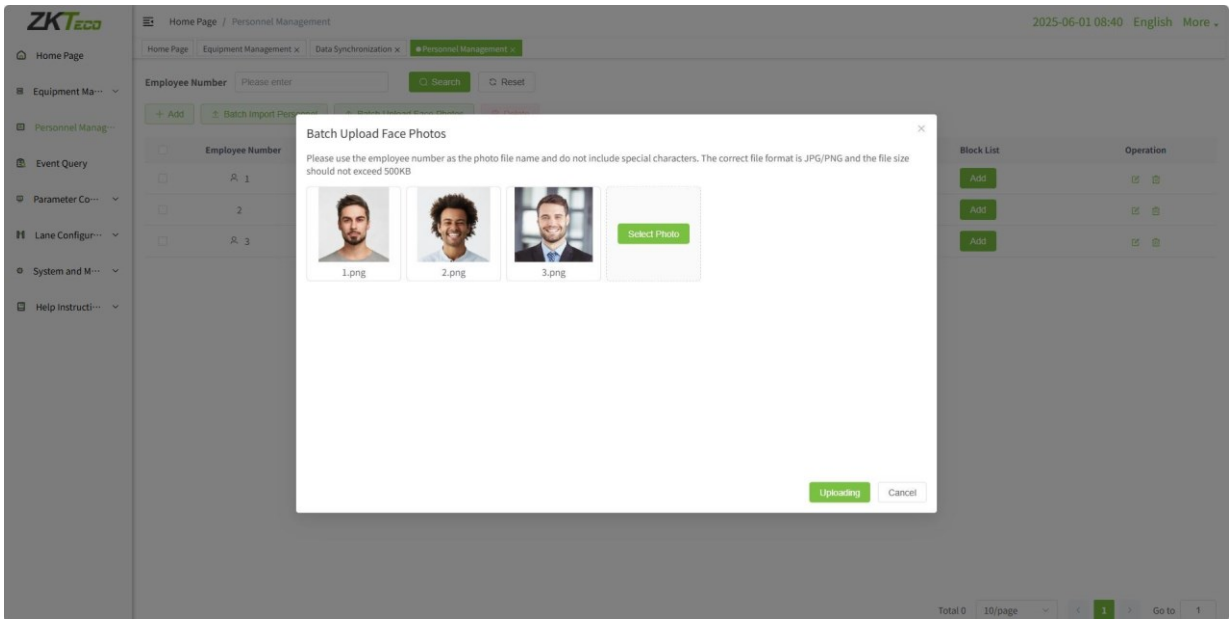
In the personnel management interface, click [**Batch Import Personnel**]. In the pop-up window, click [**Upload File**] to upload a file containing the user's employee ID, name, and card number. Click [**Confirm**] to batch upload personnel information.



	A	B	C
1	User Pin	Name	Card Number
2	5190102	Test1	5190102
3	666777888	Test2	123122314

6.4.4 Batch Upload Face Photos

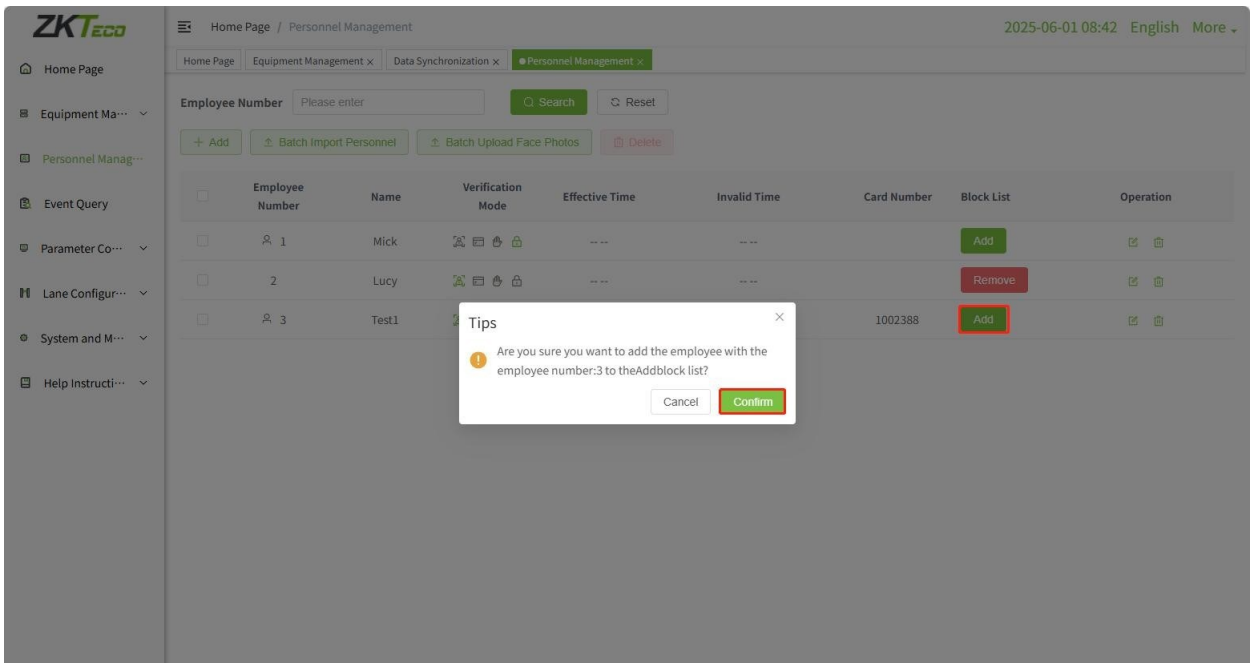
In the personnel management interface, click [**Batch Upload Face Photos**]. In the pop-up window, click [**Select Photo**] to choose the personnel photos you want to upload, and then click [**Uploading**].



Note: *Please use the employee number as the photo file name and do not contain special characters. The correct file format is JPG/PNG. The size does not exceed 500KB.*

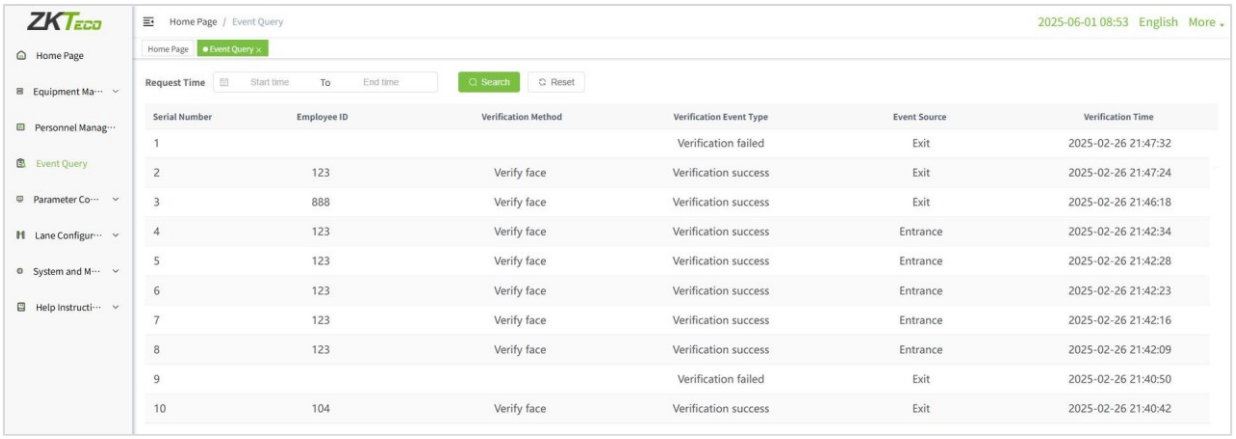
6.4.5 Block List

In the personnel list, select a person and click the [**Add**] button next to them. Then, in the pop-up prompt window, click [**Confirm**] to add the person to the block list. Click [**Remove**] to remove someone from the block list.



6.5 Event Query

Click [**Event Query**] in the left menu bar to enter the event query interface.



You can set the starting time and then click [**Search**] to search for all events within that time period.

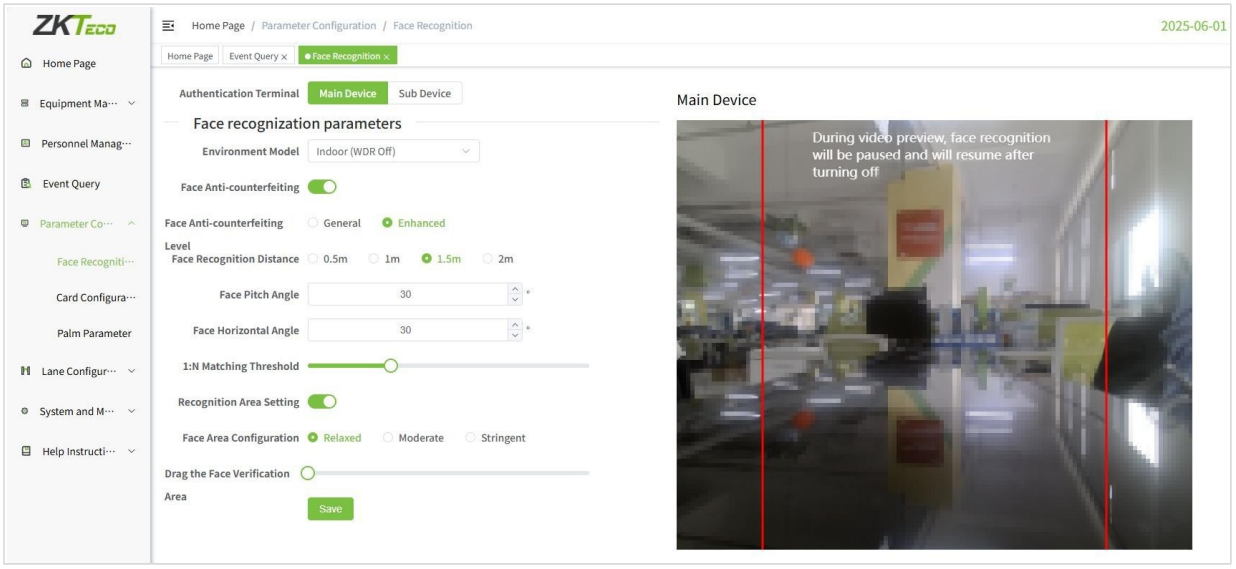
6.6 Parameter Configuration

In the parameter configuration interface, settings can be made for parameters such as facial biometric recognition, Card Configuration, and palm parameter, in order to maximize the device's ability to meet user requirements in terms of functionality and other aspects.

Click [**Parameter Configuration**] in the left menu bar to enter the setting interface.

6.6.1 Face Recognition

Click [**Parameter Configuration**] - [**Face Recognition**] in the left menu bar to enter the Face Recognition Settings interface. Set the recognition parameters for the main and sub devices according to the requirements.

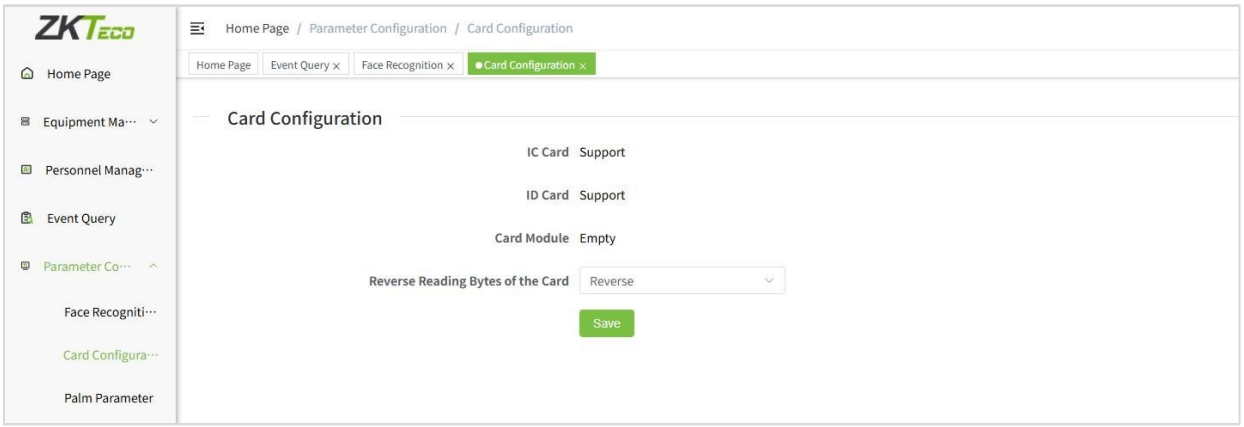


- **Authentication Terminal:** Includes the main device and sub device. Set the corresponding facial biometric parameters based on the selected terminal.

- **Environment Model:** Includes **Indoor (WDR Off)** and **Outdoors (WDR On).** Wide Dynamic Range (WDR) balances light and extends image visibility for surveillance videos under high contrast lighting scenes and improves object identification under bright and dark environments.
- **Face Anti-counterfeiting:** When enabled, it uses near-infrared images for facial anti-spoofing detection.
- **Face Anti-counterfeitingy Level:** Includes **General** and **Enhanced.**
- **Face Recognition Distance:** Includes four recognition distances: 0.5m, 1m, 1.5m, and 2m.
- **Face Pitch Angle:** The pitch angle tolerance of a face for facial registration and comparison. If a face's pitch angle exceeds this set value, it will be filtered by the algorithm, i.e. ignored by the terminal thus no registration and comparison interface will be triggered.
- **Face Horizontal Angle:** The horizontal rotation angle tolerance of a face for facial template registration and comparison. If a face's rotation angle exceeds this set value, it will be filtered by the algorithm, i.e. ignored by the terminal thus no registration and comparison interface will be triggered.
- **1:N Matching Threshold:** Under 1:N (One to Many) verification mode, the verification will only be successful when the similarity between the acquired facial image and all registered facial templates is greater than the set value. The valid value ranges from 65 to 99. The higher the thresholds, the lower the misjudgement rate, the higher the rejection rate, and vice versa.
- **Recognition Area Setting:** When enabled, a real-time video preview will appear on the right side, allowing users to set the recognition area. **Note:** Facial recognition will be disabled during adjustment and will resume after it is turned off.
  - ✧ **Face Area Configuration:** including **Relaxed**, **Moderate** and **Stringent**.
  - ✧ **Drag the Face Verification Area:** Horizontally adjust the position of the face verification area by dragging the button left or right.

6.6.2 Card Configuration

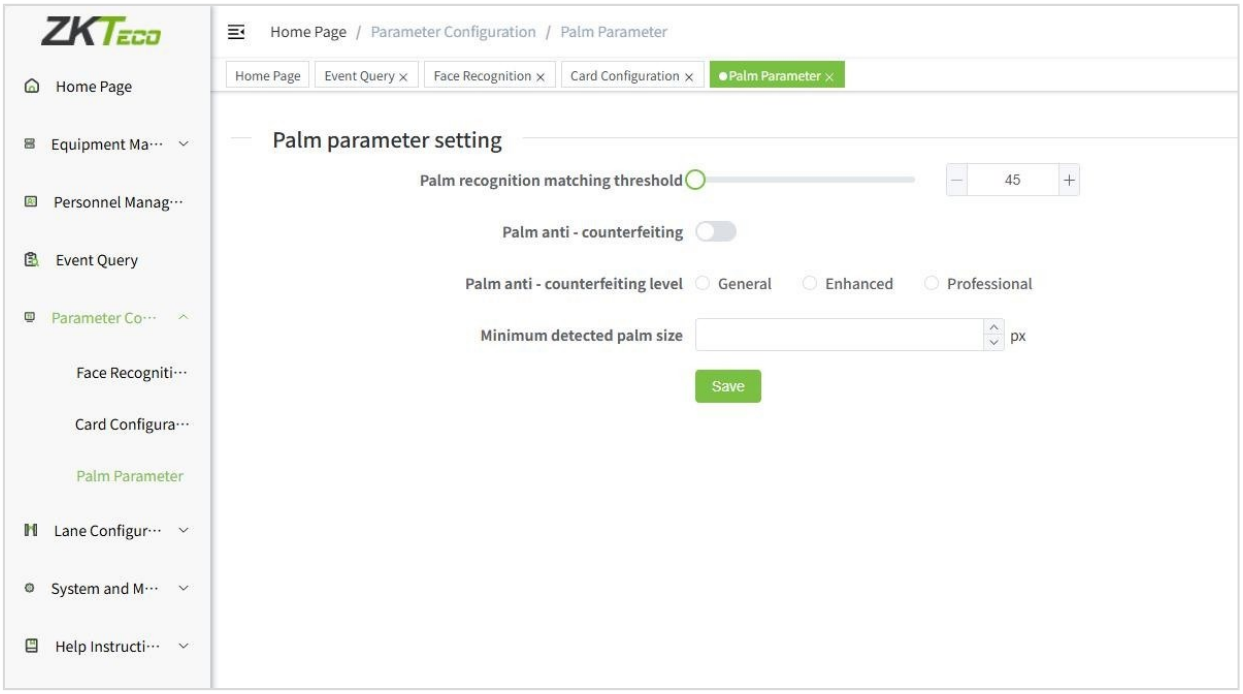
Click [**Parameter Configuration**] - [**Card Configuration**] in the left menu bar to enter the Card Configuration Settings interface.



- **Reverse Reading Bytes of the Card:** including Not Reverse and Reverse.

6.6.3 Palm Parameter

Click [**Parameter Configuration**] - [**Palm Parameter**] in the left menu bar to enter the Palm Parameter Settings interface.



- **Palm recognition matching threshold:** In the 1:N comparison mode, the device will match the current palm with the registered palm templates in the device based on similarity. If the similarity is higher than this threshold, the system will consider the palm features matched and allow access or perform the relevant operation. Conversely, if the similarity is lower than this threshold, the system will consider the palm features unmatched and deny access.
- **Palm anti-counterfeiting:** When enabled, it will perform palm anti-spoofing detection.
- **Palm anti-counterfeiting Level:** Includes **General**, **Enhanced**, and **Professional**.
- **Minimum detected palm size:** The required palm size for registration and comparison. Palms smaller than this value will be filtered out. This parameter can also be understood in terms of palm comparison distance. The farther away a person is, the smaller the palm appears, and the fewer palm pixels the algorithm captures. Therefore, adjusting this parameter can adjust the maximum comparison distance for the palm.

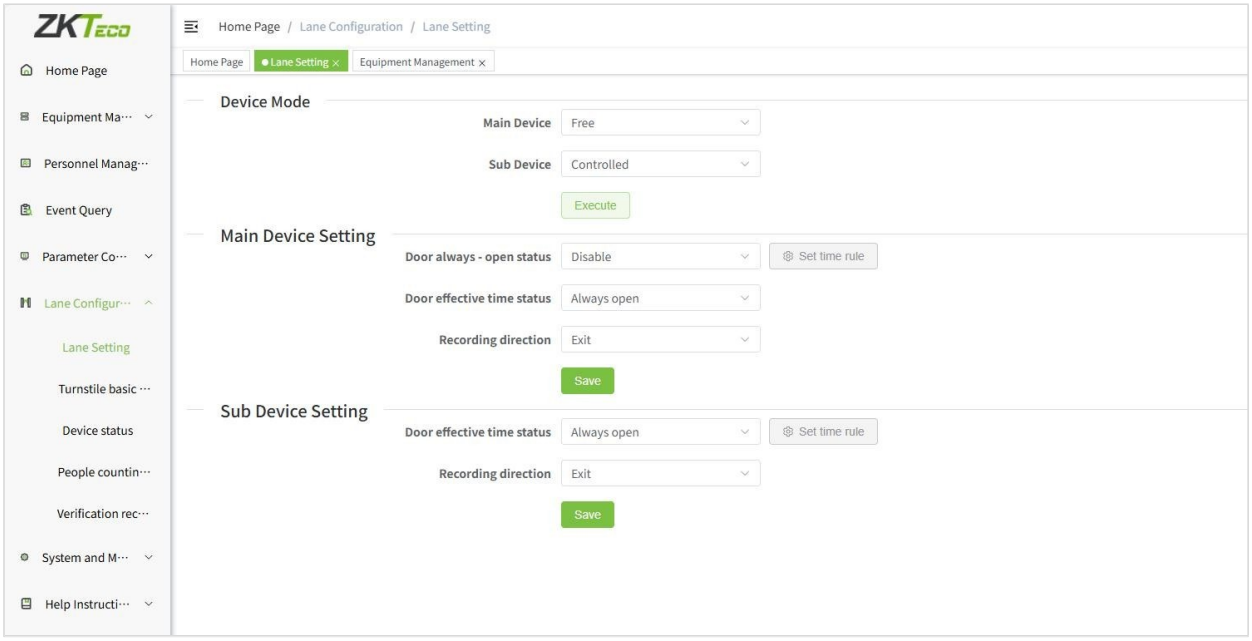
6.7 Lane Configuration

In the Lane Configuration menu, you can configure lane settings, gate parameter, equipment status, people counting configuration and verification records configuration and other parameter settings.

Click [**Lane Configuration**] in the left menu bar to enter the lane configuration interface.

6.7.1 Lane Setting

Click [**Lane Configuration**] - [**Lane Setting**] in the left menu bar to enter the lane setup settings interface.

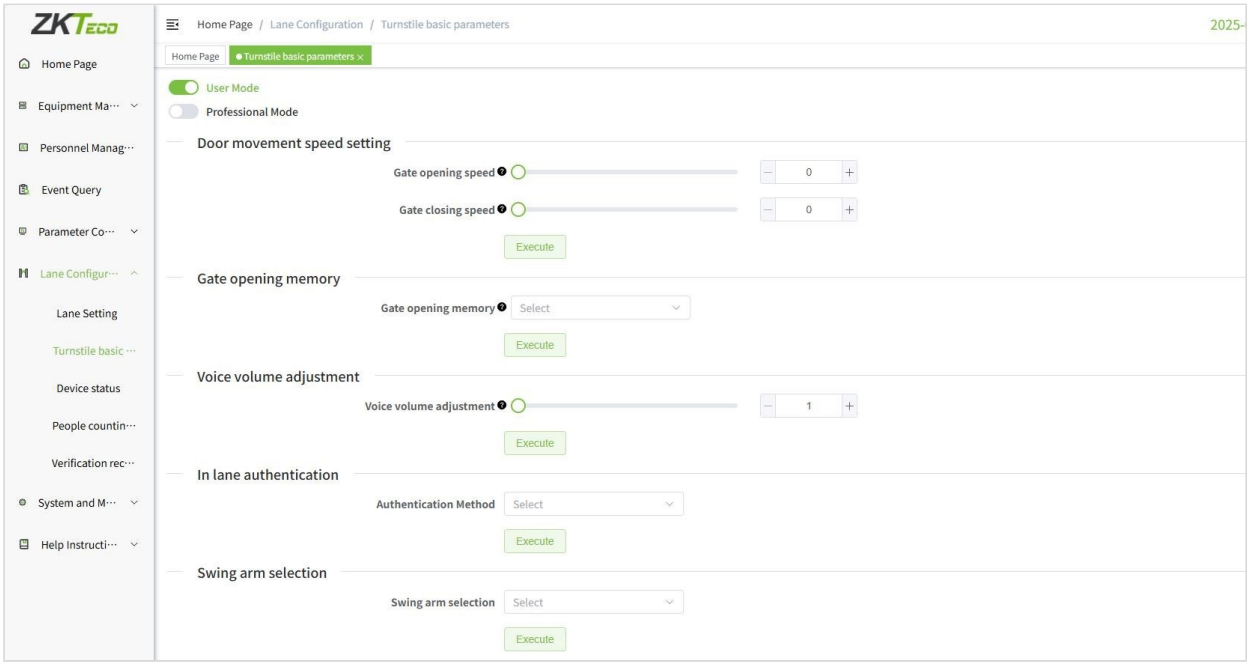


- **Device Mode:** Mode settings can be made for the main device and the sub device separately, including 3 types of device modes: controlled, free and forbidden.
- **Main Device Setting:**
  - ✧ **Door always - open status:** Used to set the normally open time period for this channel, i.e., the door remains normally open during this time period.
  - ✧ **Door effective time status:** Used to set the time period for the channel to open the door, and the verification will open the door during the set time period.
  - ✧ **Recording direction:** The status of the host can be set to Out or In. Out: The record verified on the host is the outgoing record. In: The record verified on the host computer is the incoming record.
- **Sub Device Setting:**
  - ✧ **Door effective time status:** Used to set the time period for the channel to open the door, and the verification will open the door during the set time period.
  - ✧ **Recording direction:** The status of the secondary machine can be set to Out or In. Out: The record verified on the sub is the outgoing record. In: The record verified on the sub is the entry record.

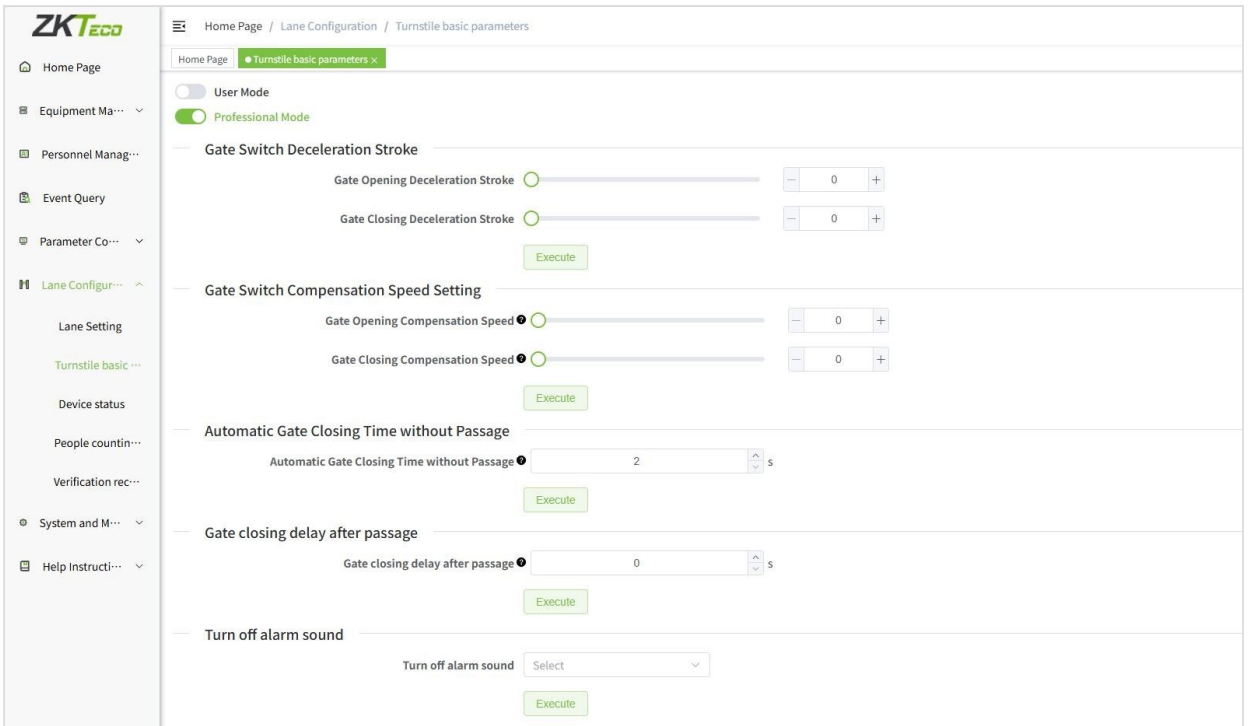
6.7.2 Turnstile basic parameters

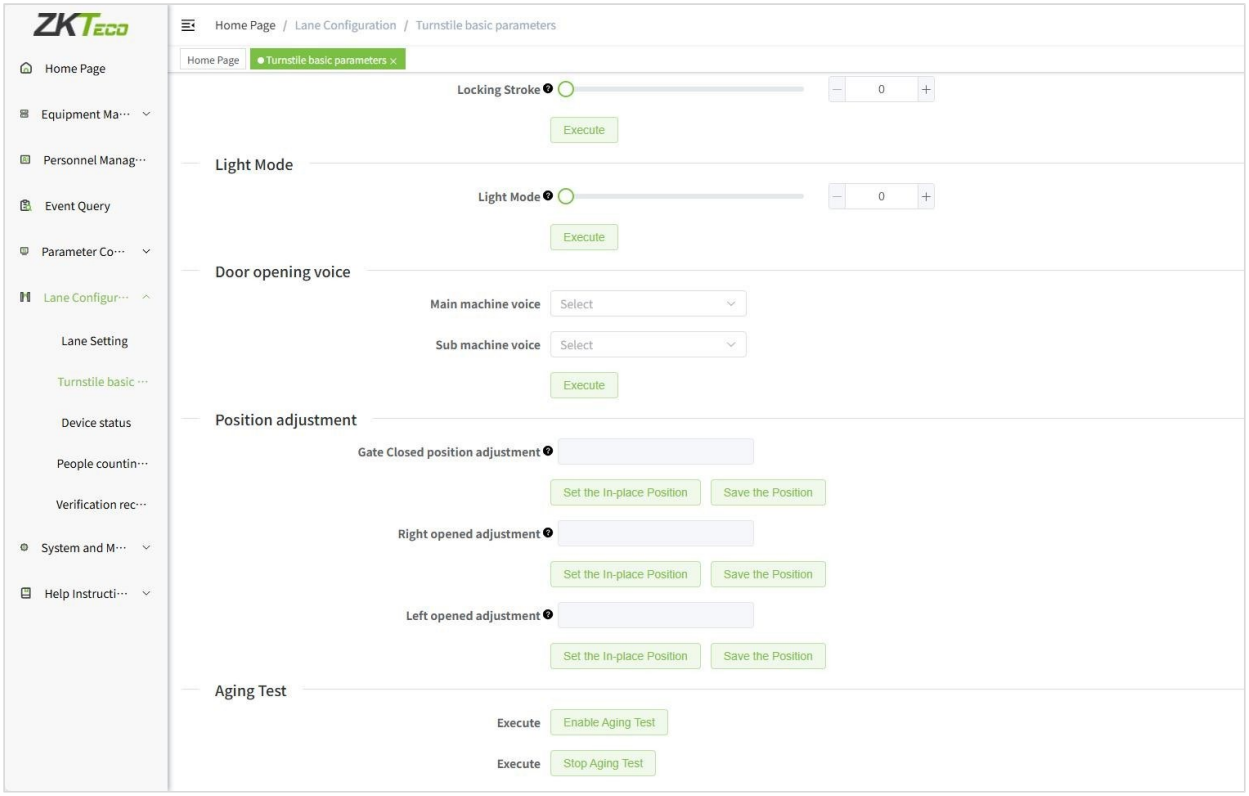
Click [**Lane Configuration**] - [**Turnstile basic parameters**] in the left menu bar to enter the settings interface. There are User Mode and Professional Mode to choose from, and set the relevant parameters according to different modes, so that the equipment in all aspects of the function and other aspects of the maximum to meet the needs of users.

- **User Mode**



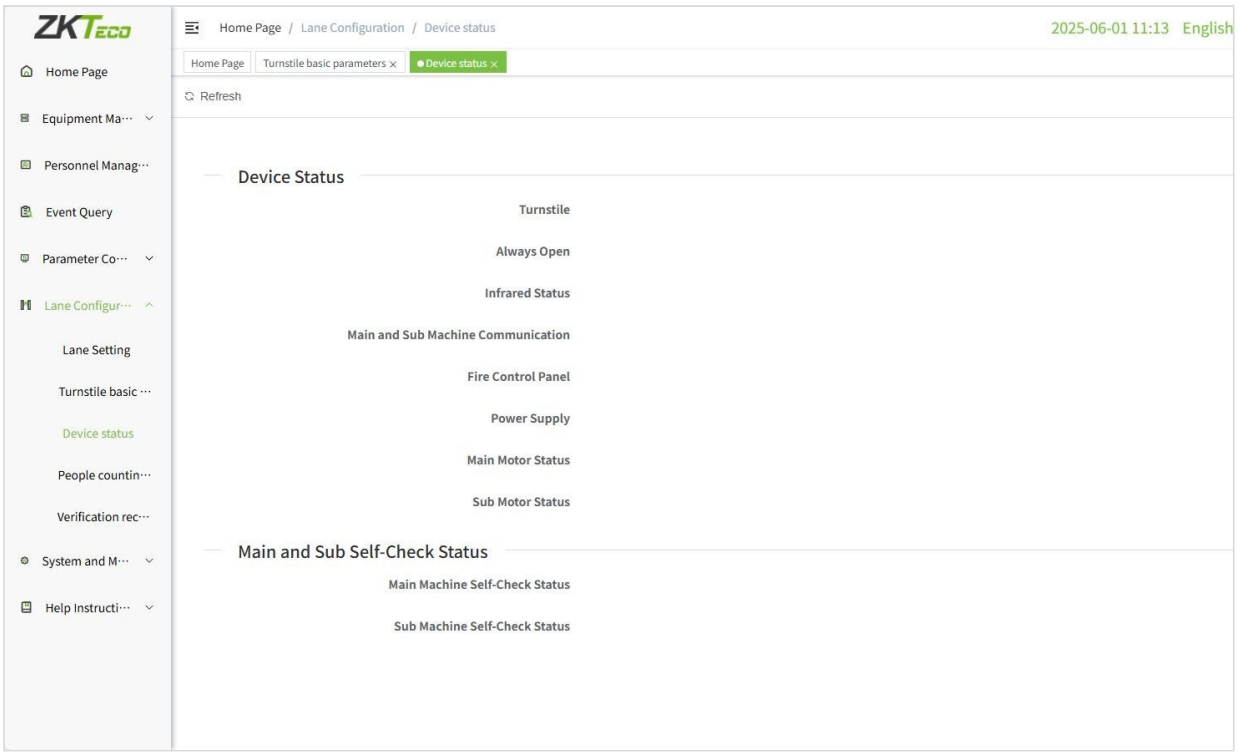
- **Professional Mode**





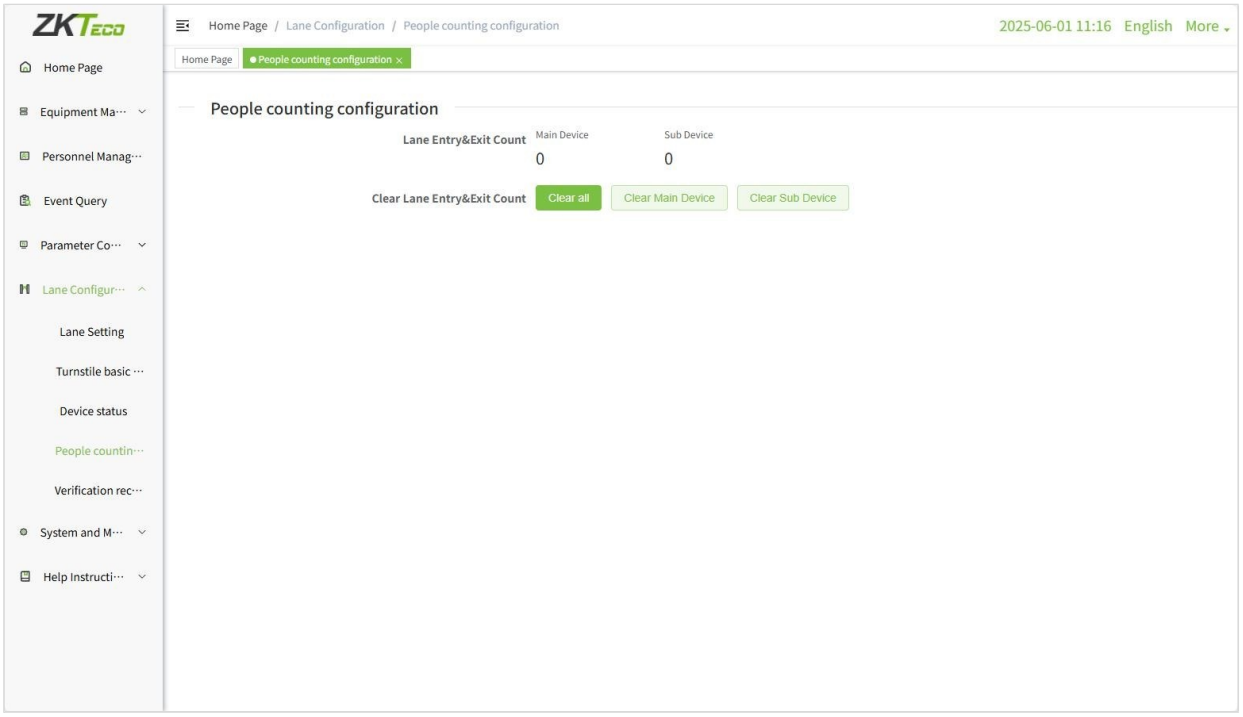
6.7.3 Device status

Click [**Lane Configuration**] - [**Device status**] in the left menu bar to enter the device status settings interface.



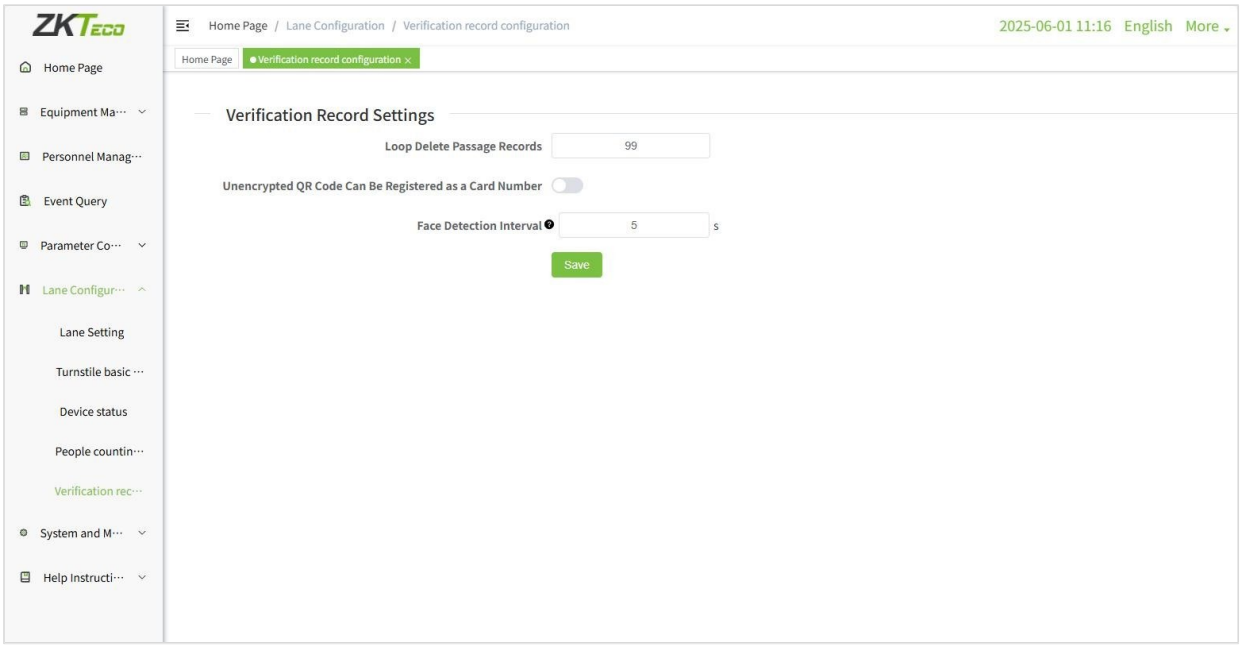
6.7.4 People Counting Configuration

Click [**Lane Configuration**] - [**People Counting Configuration**] in the left menu bar to enter the Headcount Configuration interface.



6.7.5 Verification Record Configuration

Click [**Lane Configuration**] - [**Verification Record Configuration**] in the left menu bar to enter the Verification Record Configuration interface.



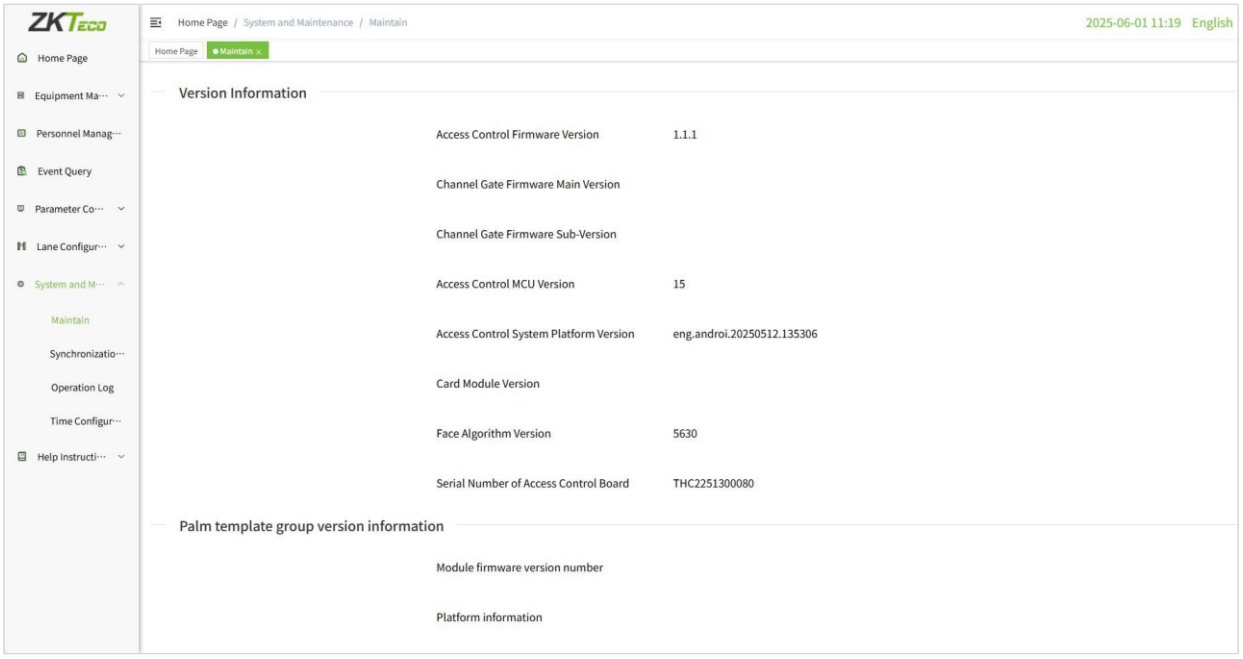
6.8 System and Maintenance

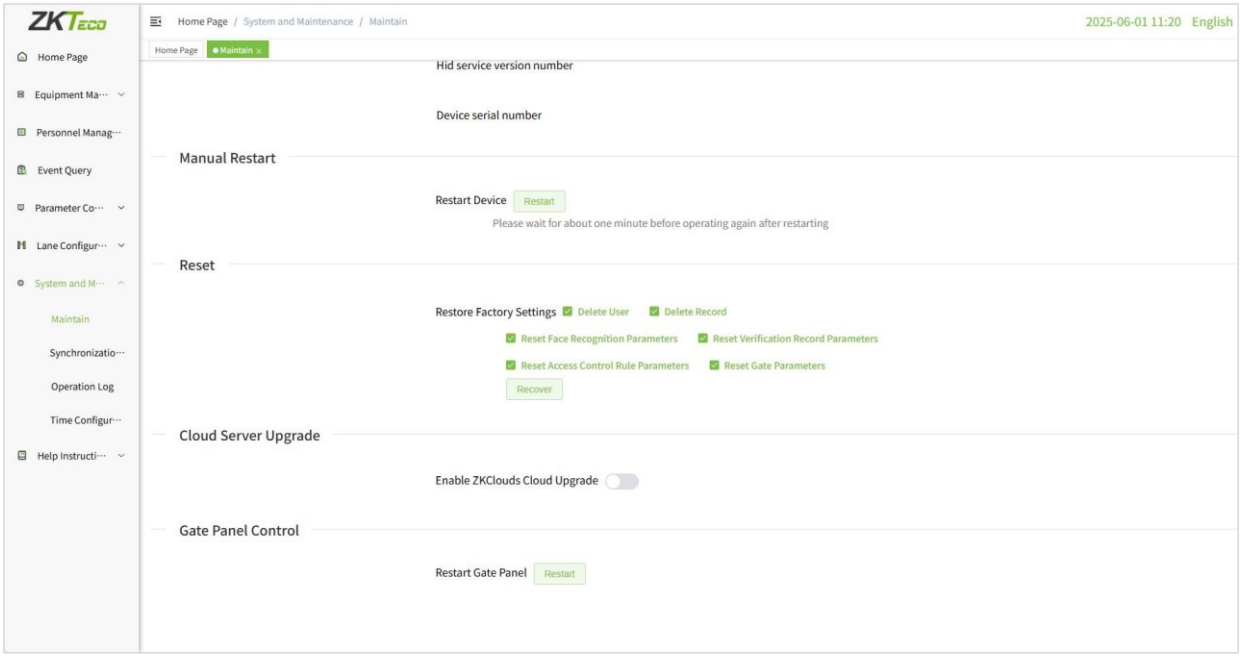
Click [**System and Maintenance**] in the left menu bar to enter the system and maintenance interface.

6.8.1 Maintain

Click [**System and Maintenance**] - [**Maintain**] in the left menu bar to enter the maintain interface.

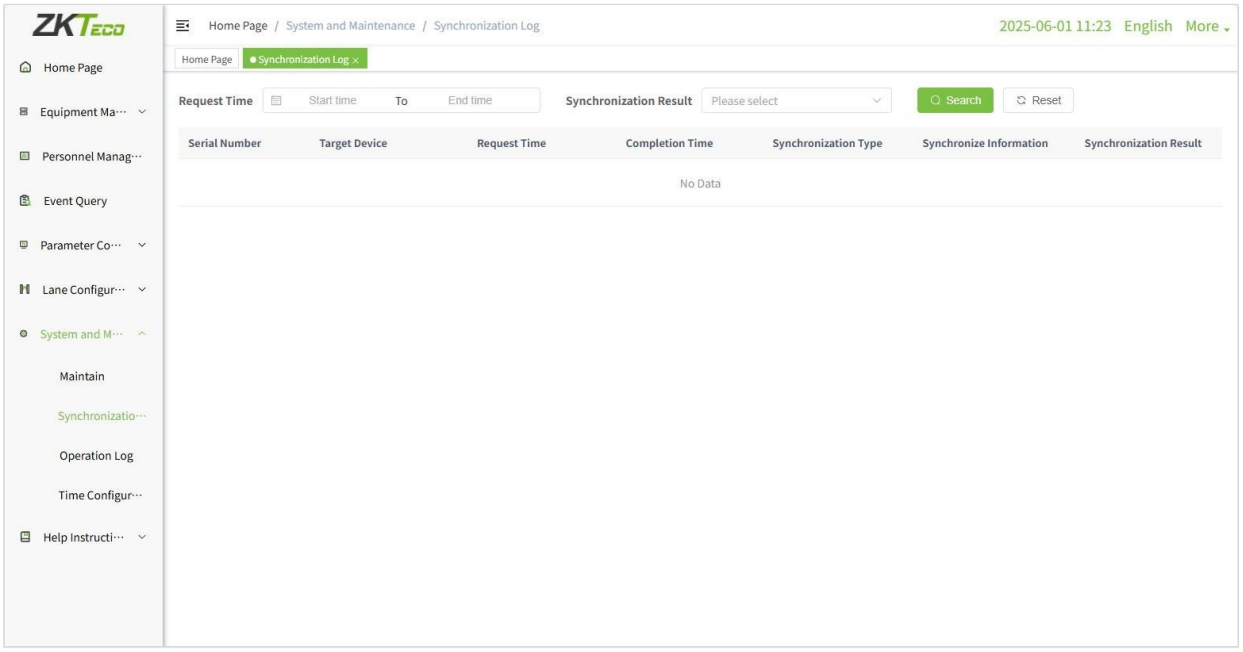
In this interface, you can view the version information, palm template group version information, manually reboot the device, restore factory settings, cloud server upgrade and restart the gate control board and other operations.





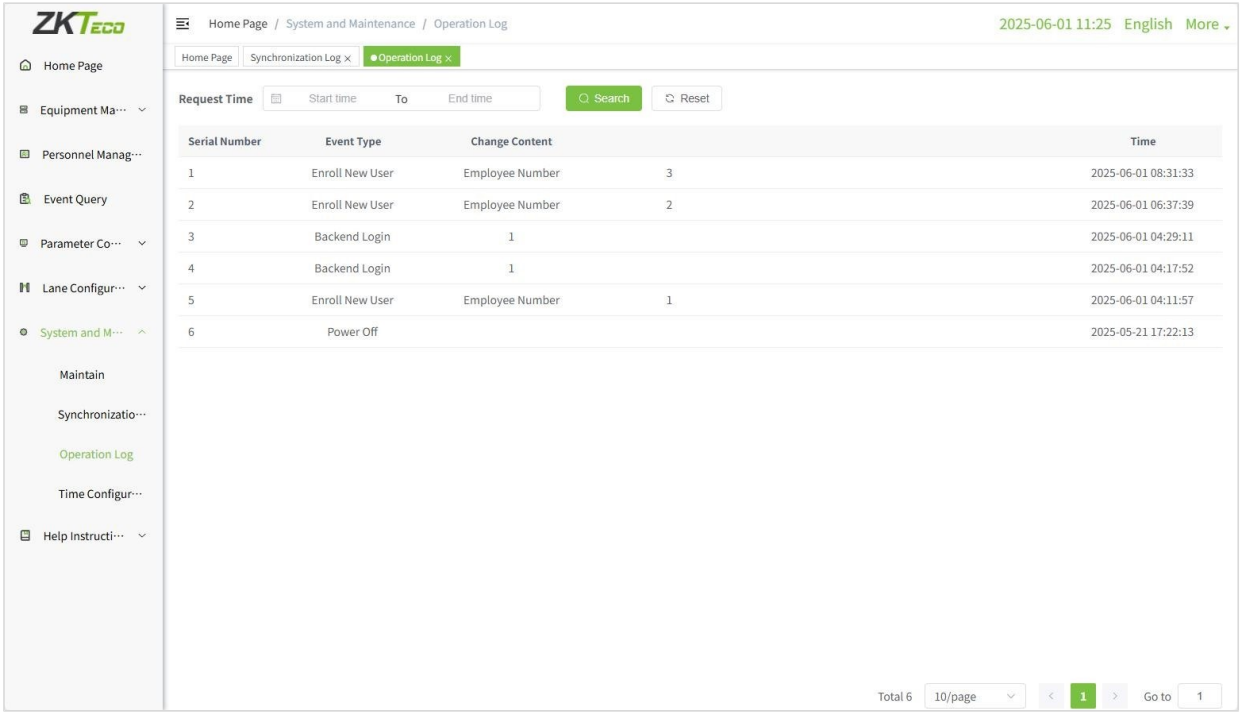
6.8.2 Synchronization Log

Click[**System and Maintenance**]-[**Synchronization Log**]intheleftmenubartoenterthe SynchronizationLog interface.



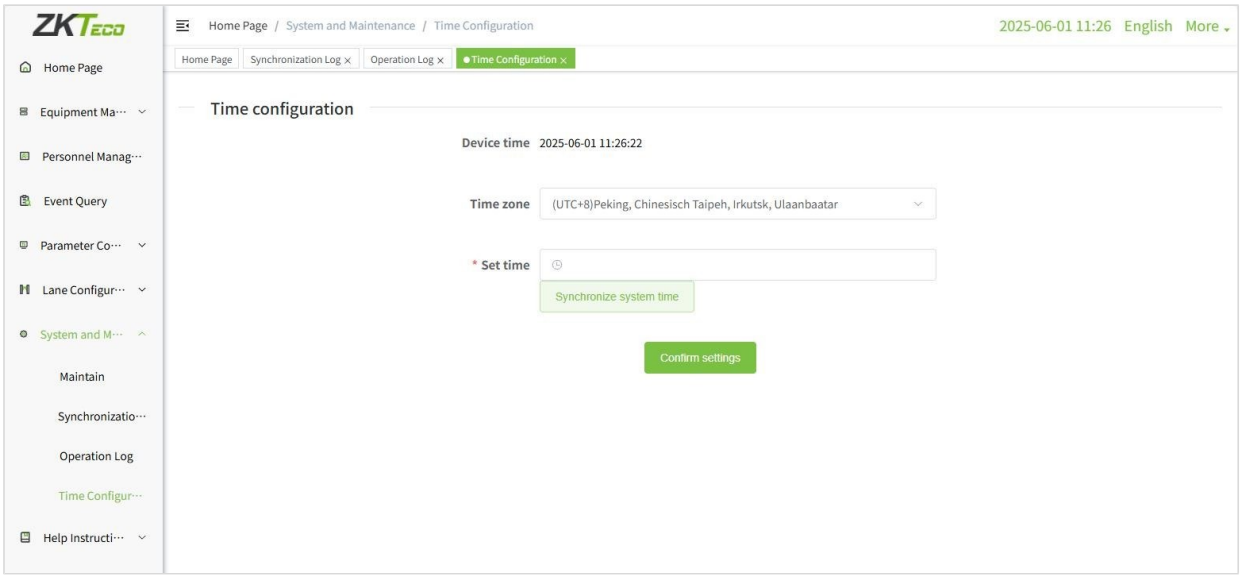
6.8.3 Operation Log

Click[**System and Maintenance**]-[**Operation Log**]intheleftmenubartoentertheOperationLog interface.



6.8.4 Time Configuration

Click [**System and Maintenance**] - [**Time Configuration**]in the left menu bar to enter the Time Configuration interface.

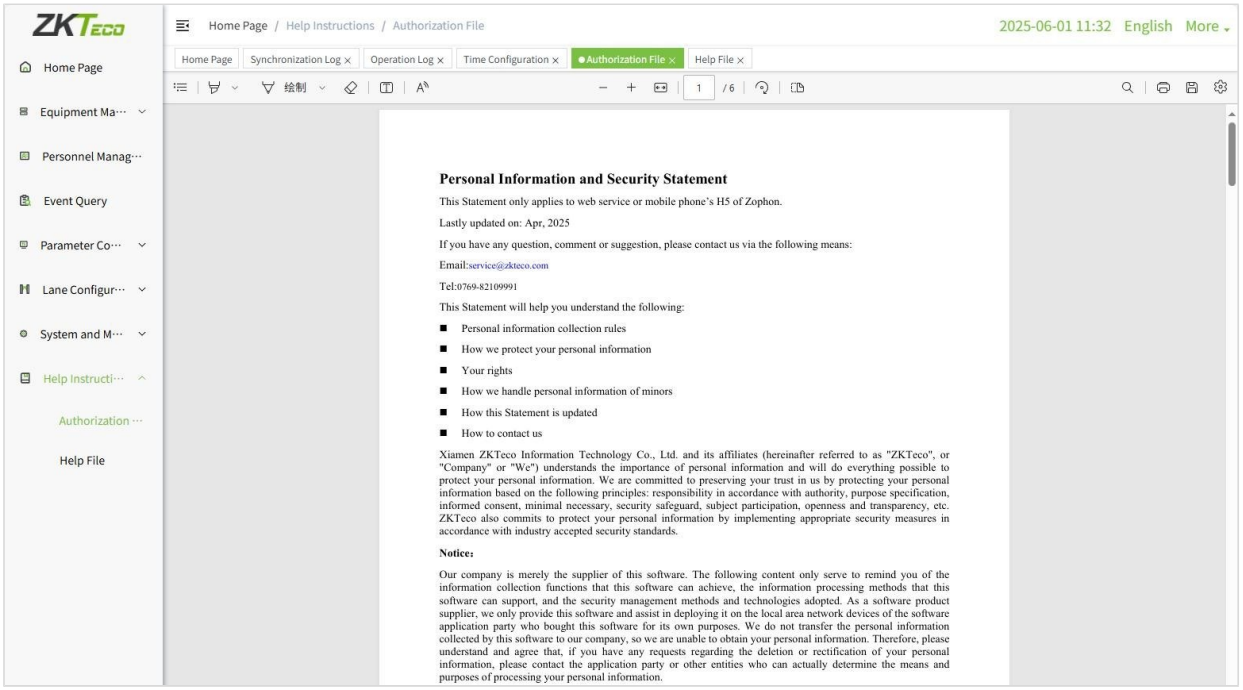


6.9 Help Instructions

Click [**Help Instructions**] in the left menu bar to enter the Help Instructions interface.

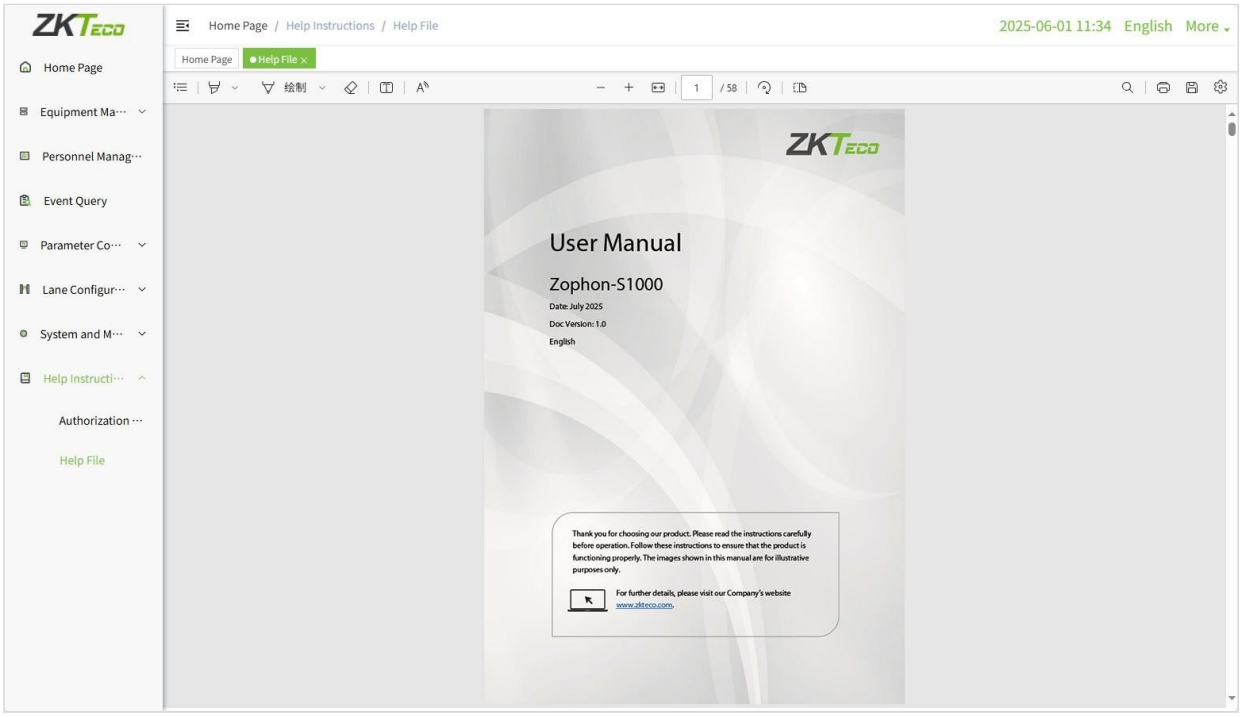
6.9.1 Authorization File

Click [**Help Instructions**] - [**Authorization File**] in the left menu bar to enter the Authorization File interface.



6.9.2 Help File

Click [**Help Instructions**] - [**Help File**] in the left menu bar to enter the Help File interface, users can view the User Manual.



7 Login to the Mobile Page

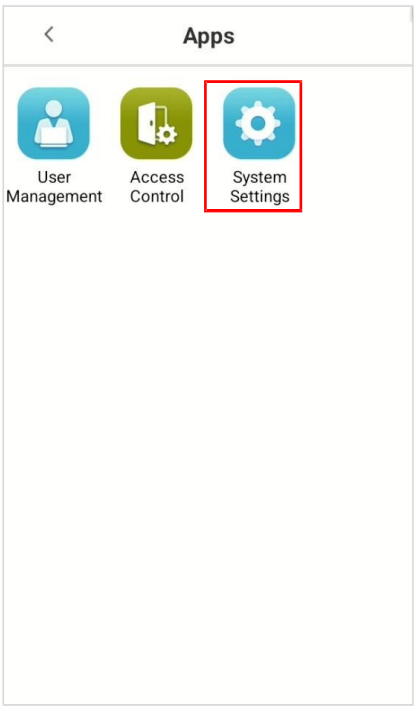
This device supports NFC / Wi-Fi communication. You can directly connect your mobile phone to the main controller's Wi-Fi for H5 access, or you can use your phone's NFC to connect to the main controller's Wi-Fi for H5 access, enabling management operations anytime and anywhere. It supports mobile H5 facial registration, allowing for quick entry of personnel information without the need for cumbersome device operations.

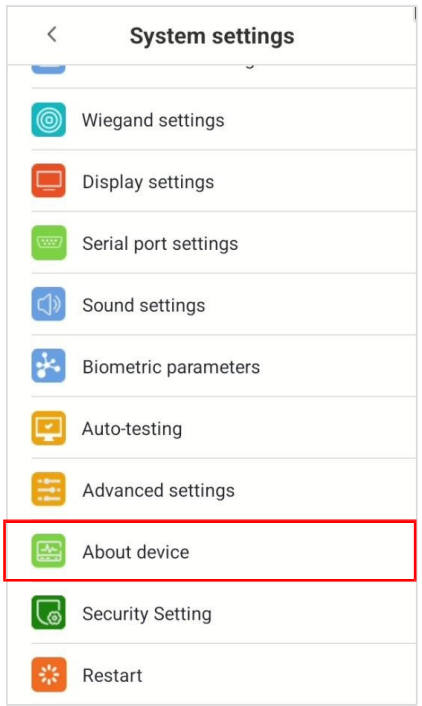
7.1 Login to the Mobile Page

7.1.1 Set the Wi-Fi password

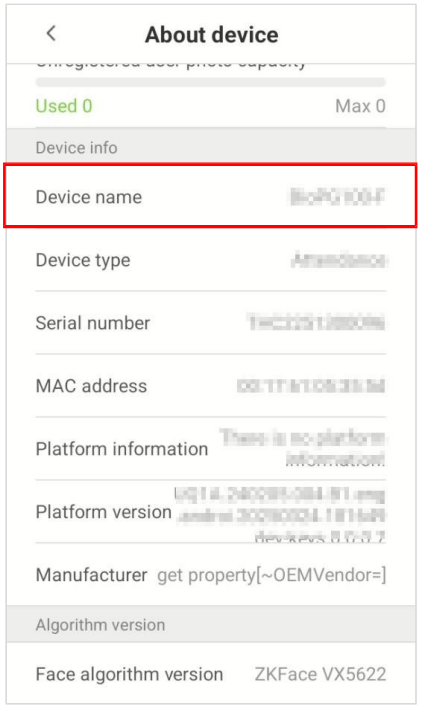
To facilitate the connection of your mobile phone to the main controller's Wi-Fi, you can advance into the main system interface to set the main's Wi-Fi password. Note: The following operations can only be performed if an LCD display Module is configured.

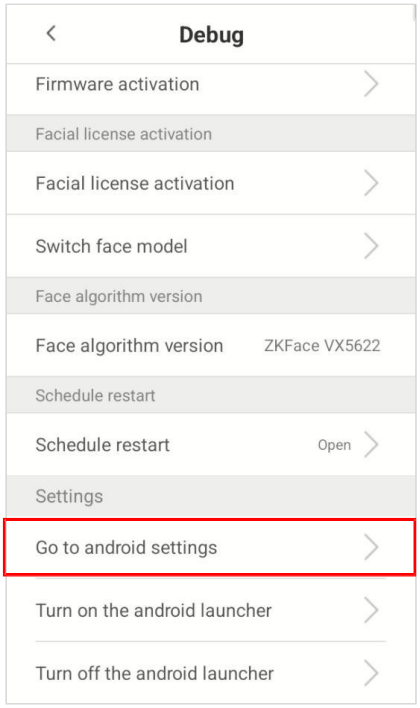
1. Insert a USB mouse into the reserved USB port on the main's permission board to operate the interface.
2. Click the icon on the display screen to enter the application menu interface, and then click [**System Settings**] - [**About Device**] to enter the About Device interface, as shown in the figure below.

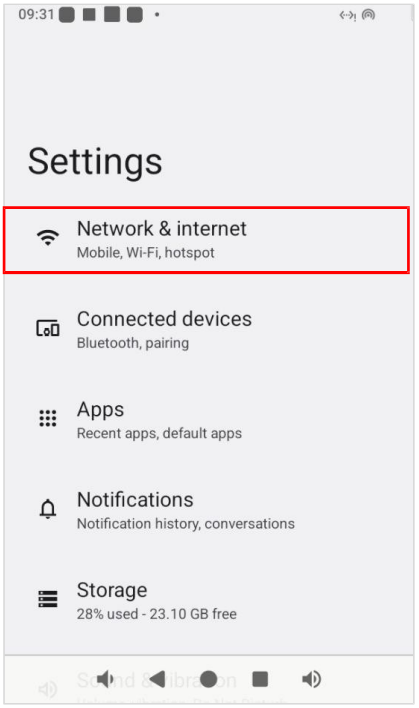




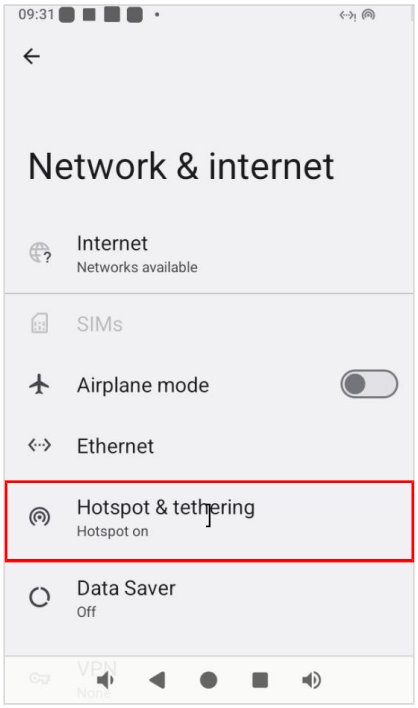
3. In the About Device interface, click [**Device Name**] five times in a row to enter the [**Debug**] interface. Then click [**Settings**] - [**Go to android settings**] - [**Network & Internet**], as shown in the figure below.

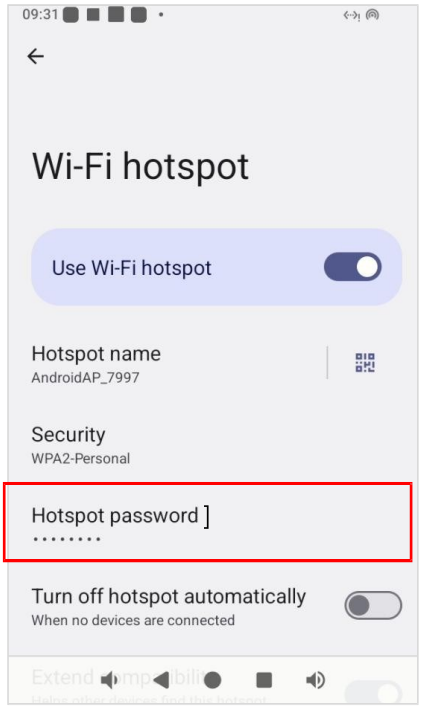






4. After entering the Network & Internet interface, click [**Hotspot & tethering**], turn on [**Wi-Fi Hotspot**], then click [**Hotspot password**]. Modify the hotspot password (e.g., 66666666) and remember this hotspot password.

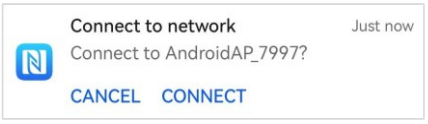




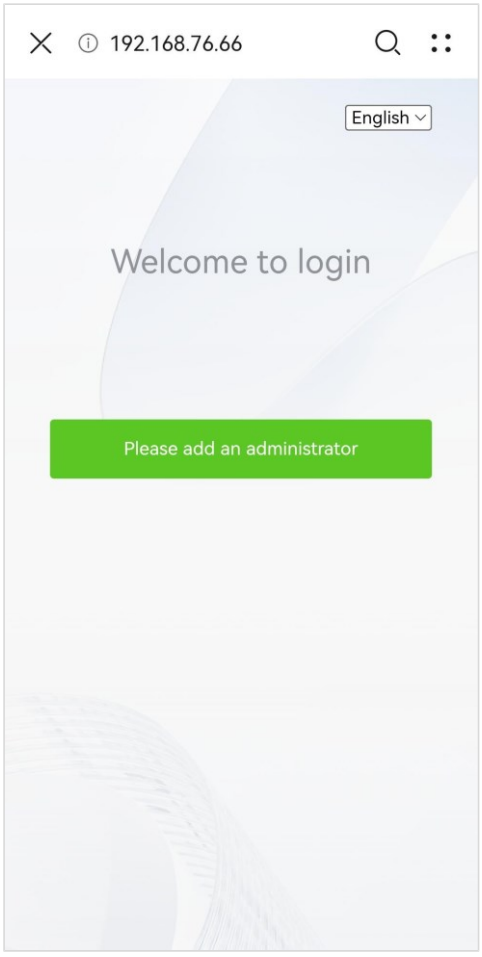
7.1.2 Login via NFC

The mobile phone can connect to the main controller's Wi-Fi via NFC for H5 access. This feature supports the **Android** system. The operating steps are as follows.

1. Enable the **NFC** function on your mobile phone, then bring the phone close to the facial recognition module. In the pop-up NFC service window, click [**Connect**] to connect to the network, as shown in the figure below.

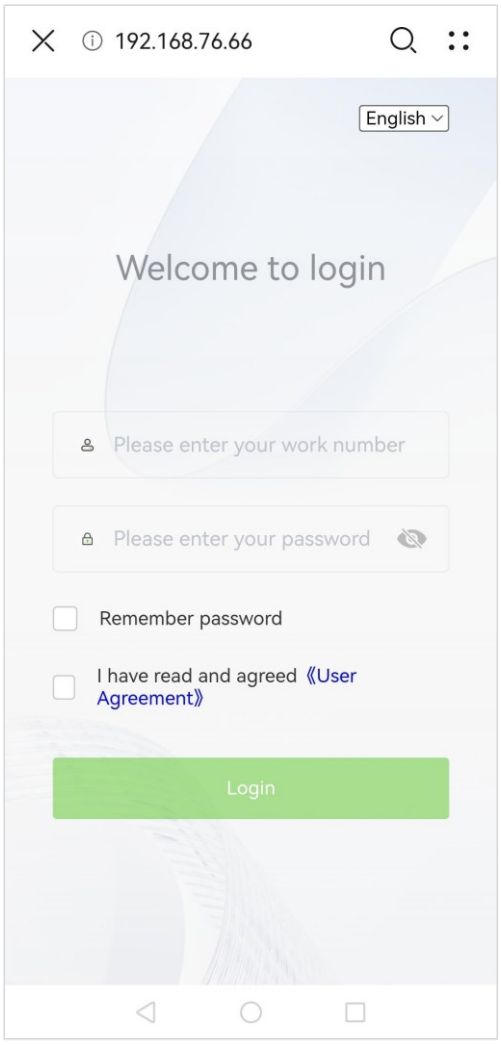


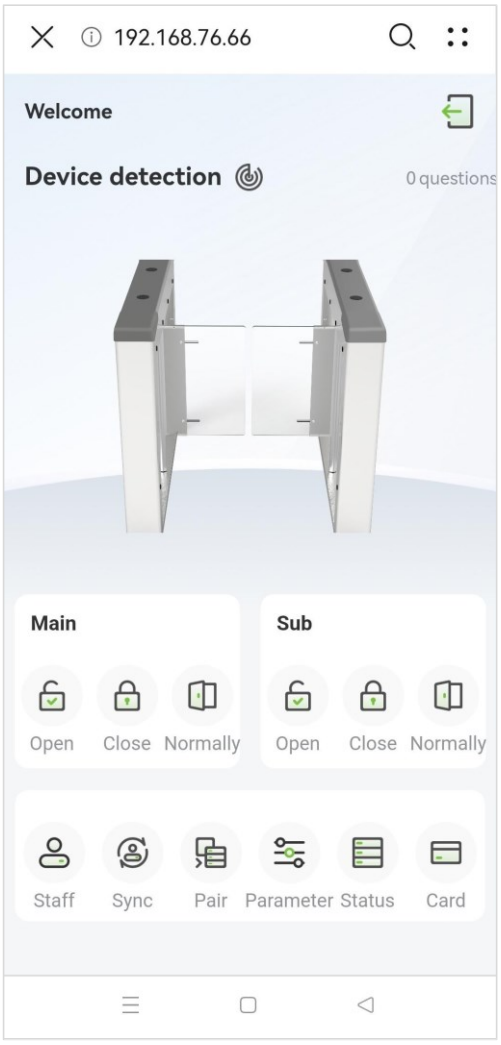
2. After a successful connection, the interface will automatically redirect to the Webserver login page. If no administrator has been added, a prompt button requesting the addition of an administrator will appear. Upon clicking this button, you will be directed to the main page, as shown in the figure below.



Note: Due to the differences in the hardware and systems of various mobile phone models and devices, there may be cases where the device cannot be connected via NFC. If you encounter such a problem, please select a suitable mobile phone device. Devices with iOS systems cannot use NFC.

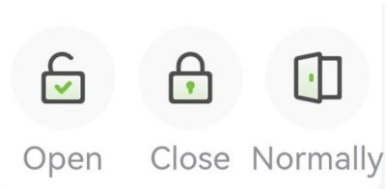
3. If an administrator has already been added, after connecting to the network, the page will redirect to the login interface. Enter the administrator's account and password, check the agreement, and then click [**Login**].





Note:

1. *For the security of the device, it is recommended to register system administrator the first time you use the device.*
2. *You can click on [**User Management**] - [**Add**] in the left-hand menu bar to add a system administrator. For details, please refer to Section 6.4 User Management.*
4. On the main interface, click the relevant icon for the host or secondary device. Within the effective range, you can perform real-time operations such as opening the door, closing the door, or setting it to always open.



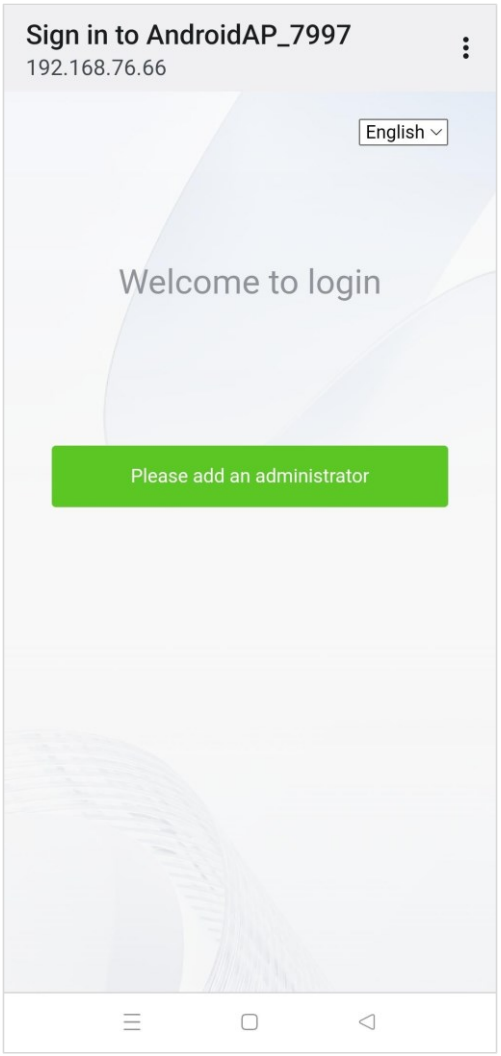
7.1.3 Login via Wi-Fi

When the mobile phone does not support NFC functionality, you can choose to connect directly to the host's Wi-Fi for H5 access. This method supports both Android and iOS systems. The operating steps are as follows.

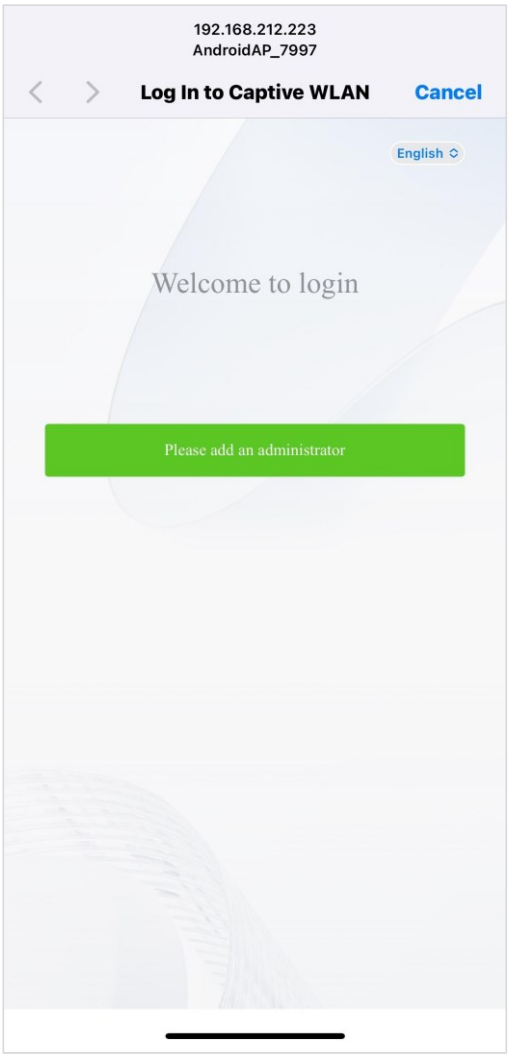
1. Enable the Wi-Fi function on your mobile phone, then locate the host's network (e.g., **AndroidAP_7997**), and click to enter the hotspot password (e.g., 66666666) to connect. After a successful connection, the interface will redirect to the Webserver login page.

2. If the device is being used for the first time or no administrator has been added, a "Please Add Administrator" prompt button will appear. Clicking this button will take you to the main page. The following figures show the prompt interfaces for the Android and iOS systems, respectively. Clicking [**Please Add Administrator**] will take you to the main interface.

Android System:

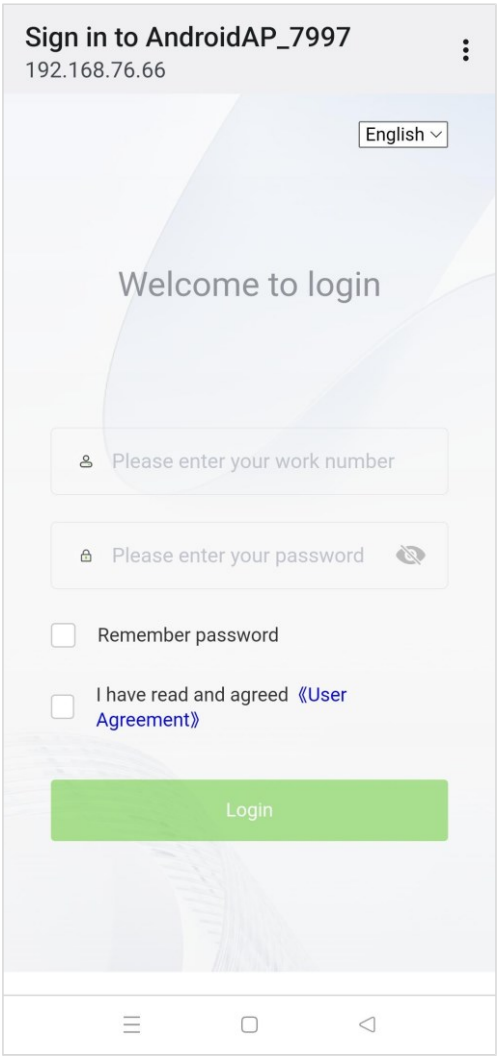


iOS System:

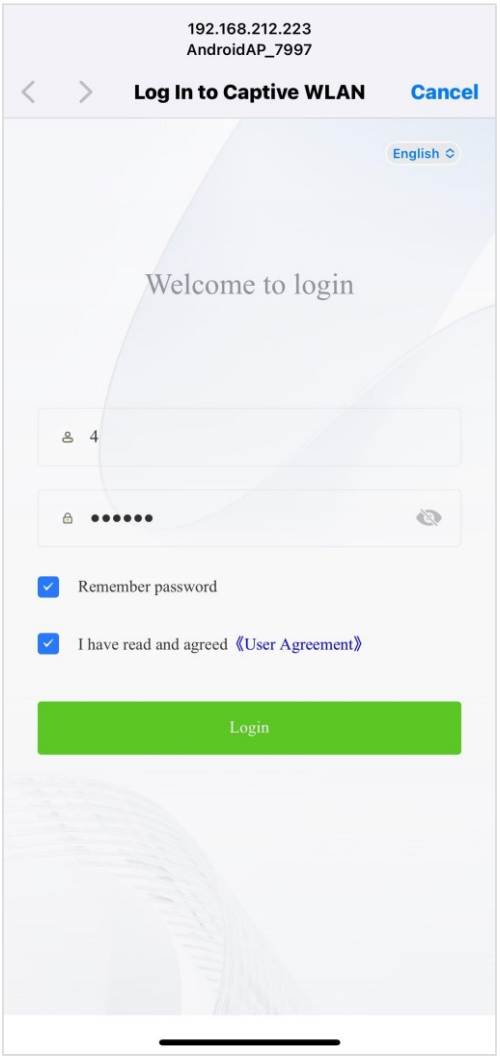


3. If the device has already added an administrator, the page will be redirected to the administrator login interface after a successful Wi-Fi connection. The following figures show the login interfaces for Android and iOS systems respectively. After entering the administrator account and password and checking the agreement, click on [**Login**] to access the main interface.

Android System:



iOS System:



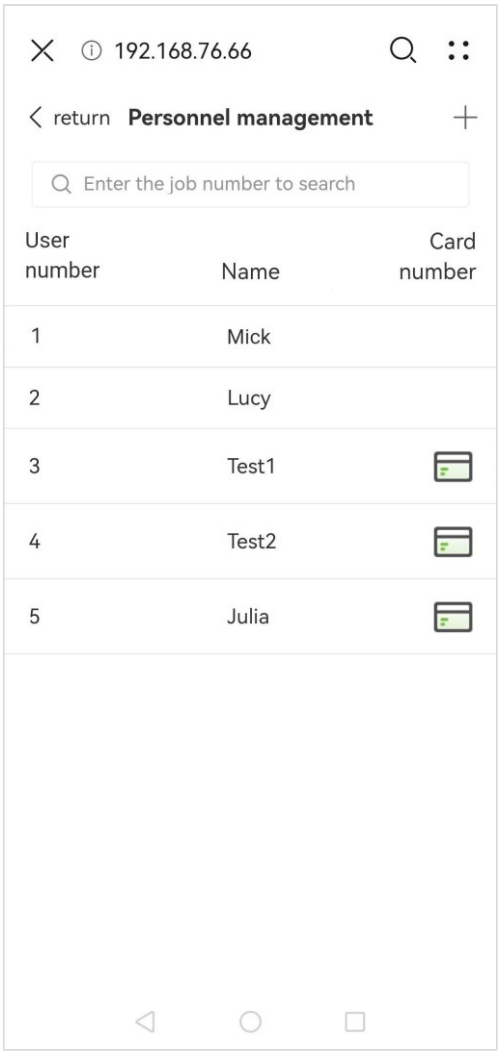
Note:

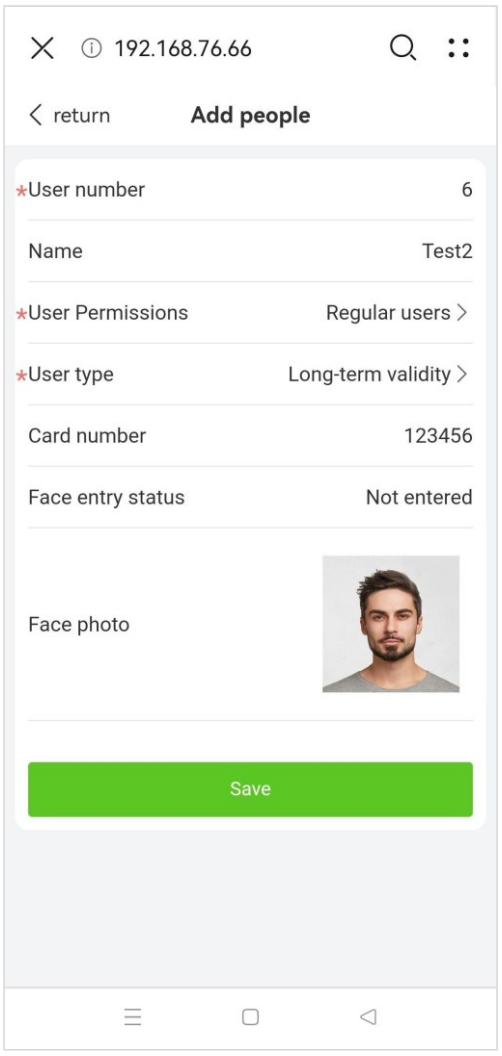
1. *For the security of the device, it is recommended to register system administrator the first time you use the device.*
2. *You can click on [**User Management**] - [**Add**] in the left-hand menu bar to add a system administrator. For details, please refer to Section 6.4 User Management.*

7.2 Personnel Management

1. Click on the [**Personnel Management**] menu on the main interface to enter the personnel management interface.

2. Click on the + icon at the top right corner of the personnel management interface to enter the interface for adding personnel and perform the operation of adding personnel.

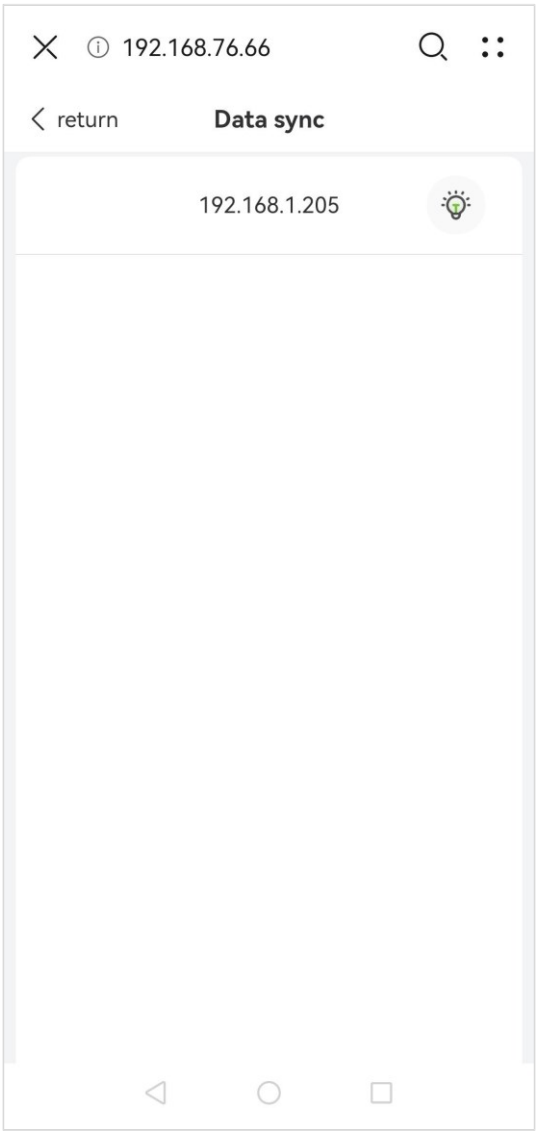




3. In the Add People interface, you can input the user number and name, set the user authority as ordinary user or administrator, enter the card number, register the face photo and so on. Click [**Save**]. The new personnel information can be instantly synchronised to the device side.

7.3 Data Synchronization

Click the [**Data Synchronization**] menu in the main interface to enter the data synchronization interface.

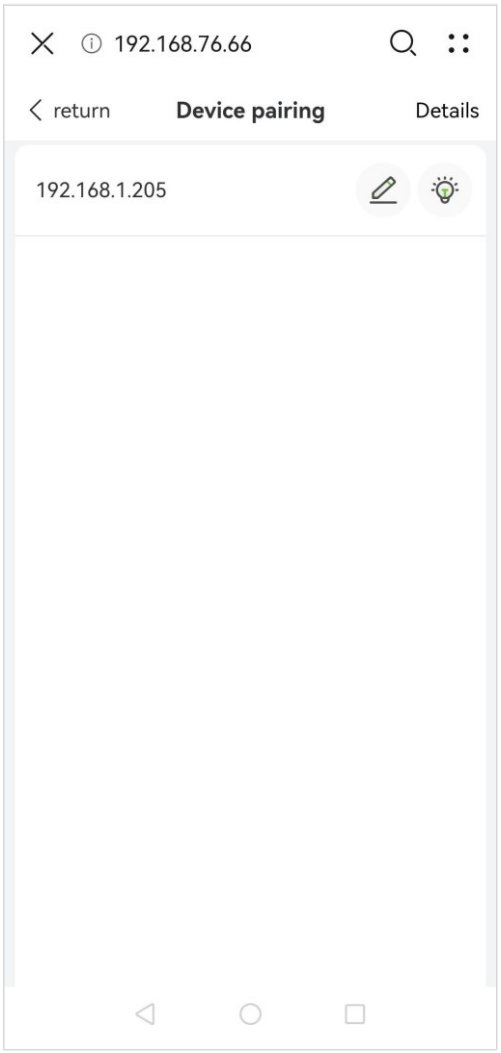


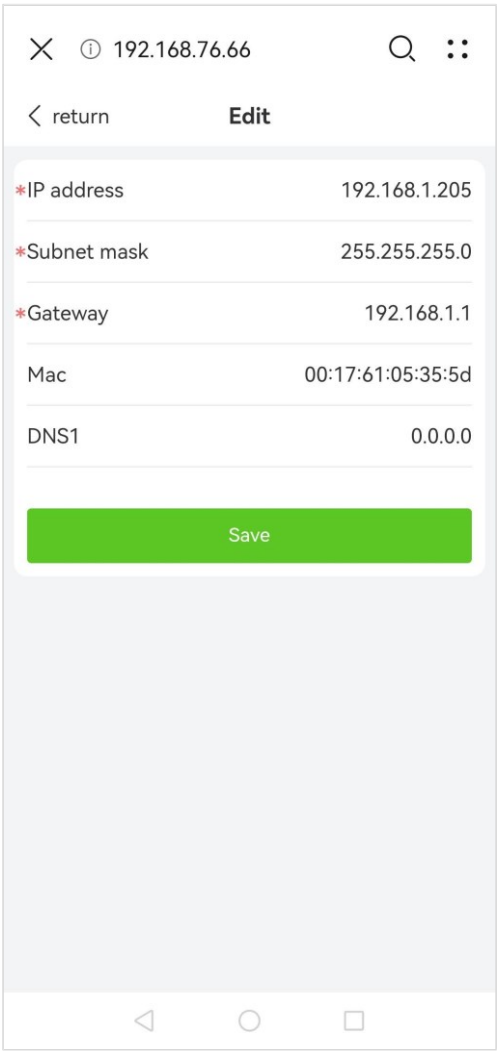
7.4 Device Pairing

Click the [**Device Pairing**] menu in the main interface to enter the device pairing interface.

7.4.1 Modify the device IP address

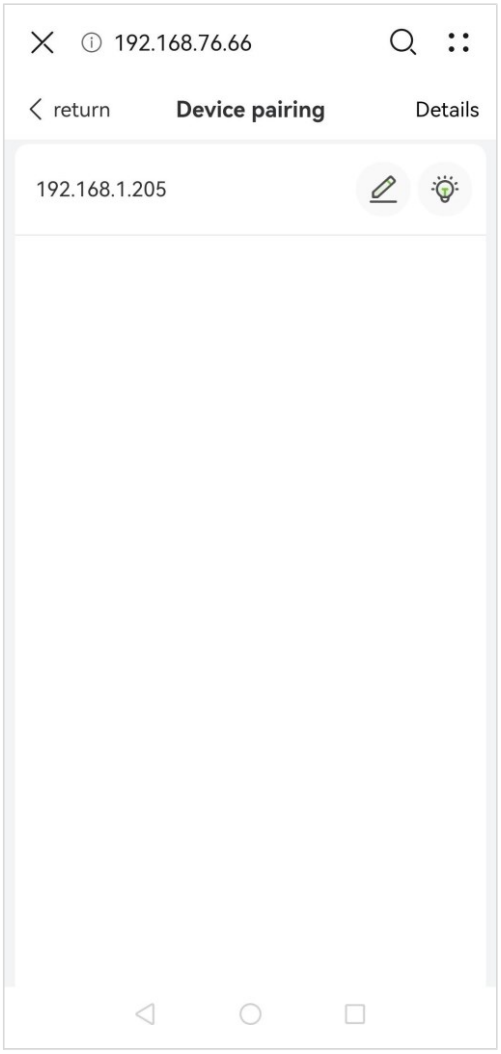
On the device pairing interface, select the device and click the icon next to it to enter the IP address editing page, where you can modify the device's IP address. Click the icon to light up the device's LED, which facilitates device identification.

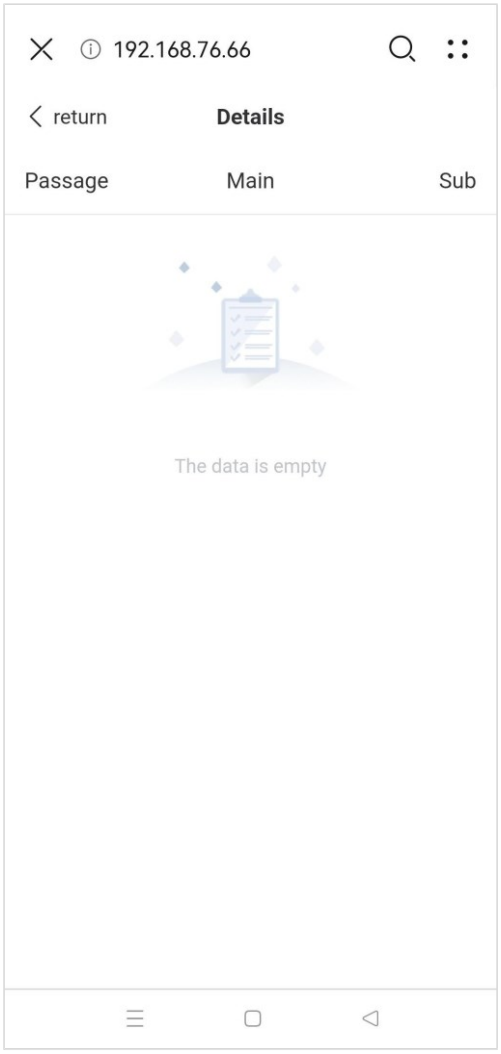




7.4.2 Device Pairing

On the device pairing interface, click on [**Details**] to enter the pairing Details page, where you can view the pairing status of the device.



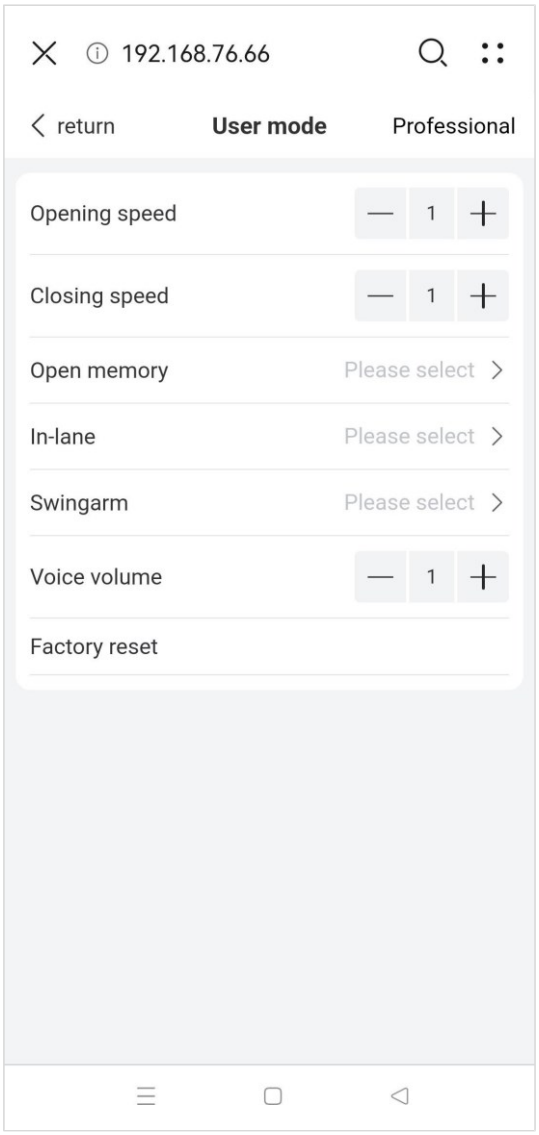


7.5 Parameter Configuration

Click [**Parameter Configuration**] menu in the main interface to enter the parameter configuration interface. You can set the parameters of user mode and professional mode.

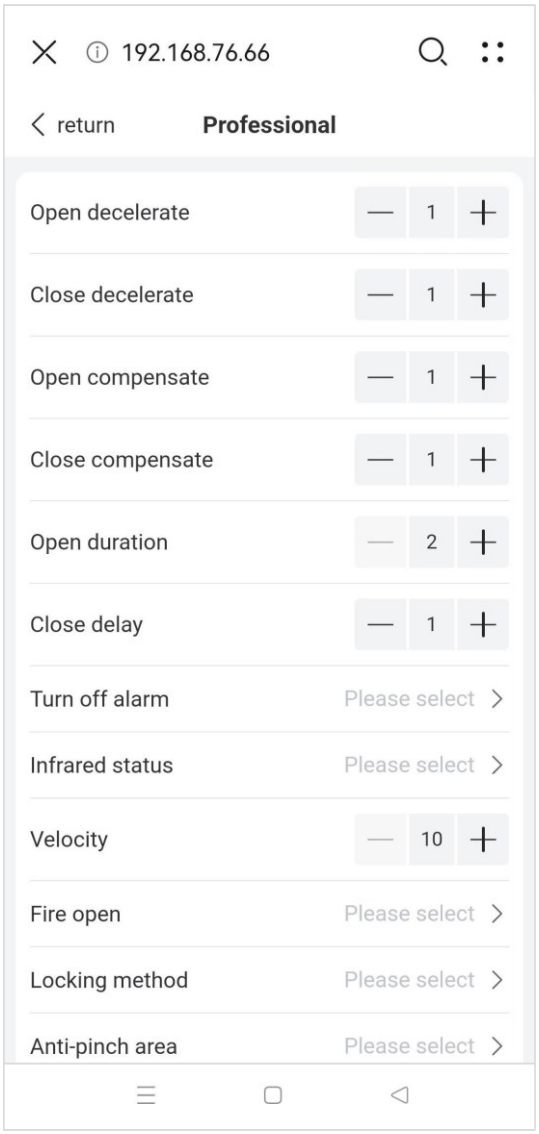
7.5.1 User Mode

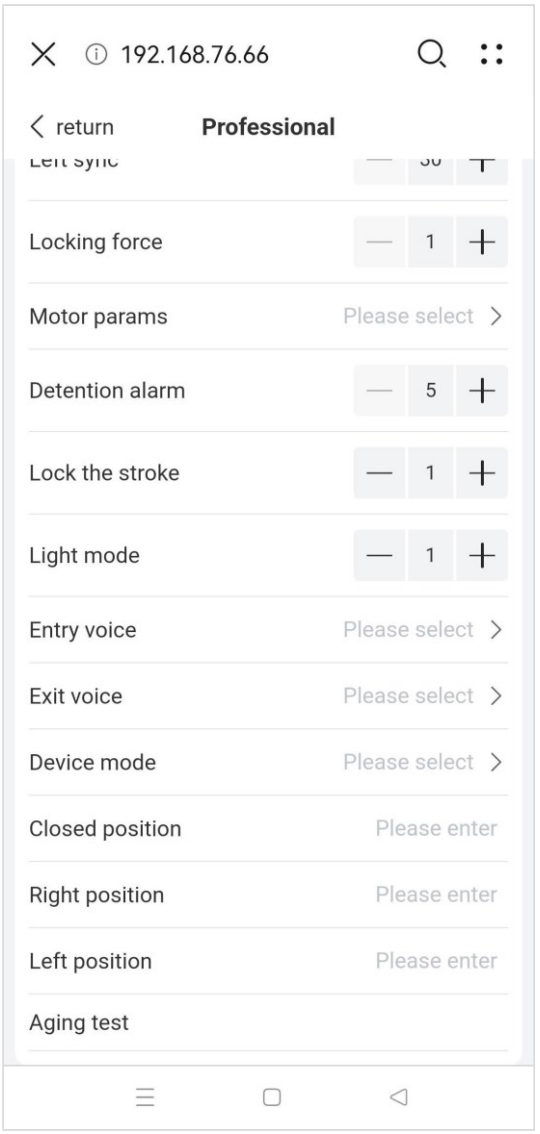
The user can modify parameters including the opening speed, closing speed, open memory, In-lane, swing arm, voice volume, and factory reset.



7.5.2 Professional Mode

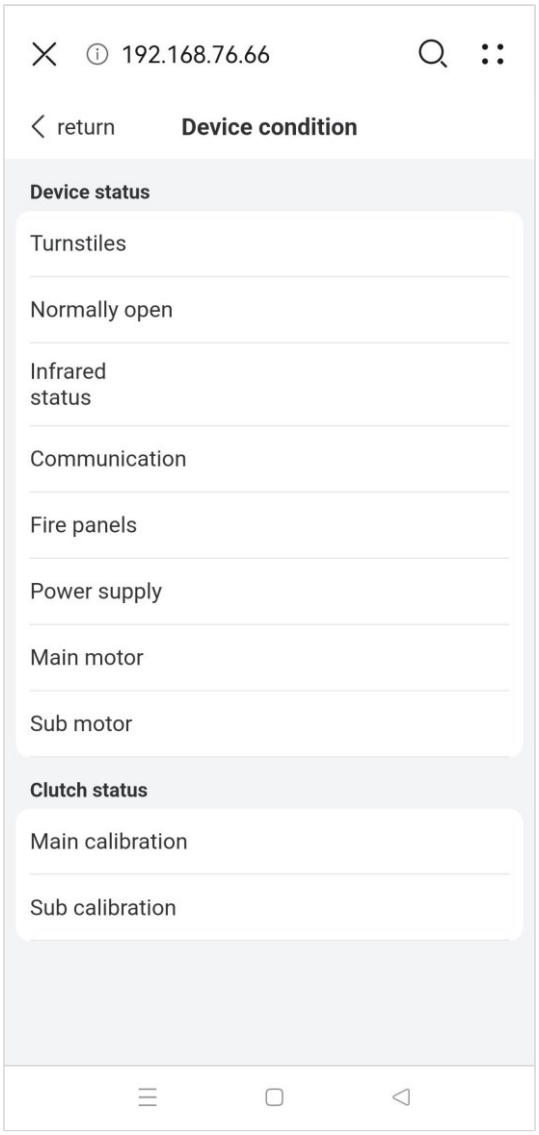
In this mode, users can modify a greater number of professional parameters to maximize the device's functionalityandmeettheirneedsineveryaspect.





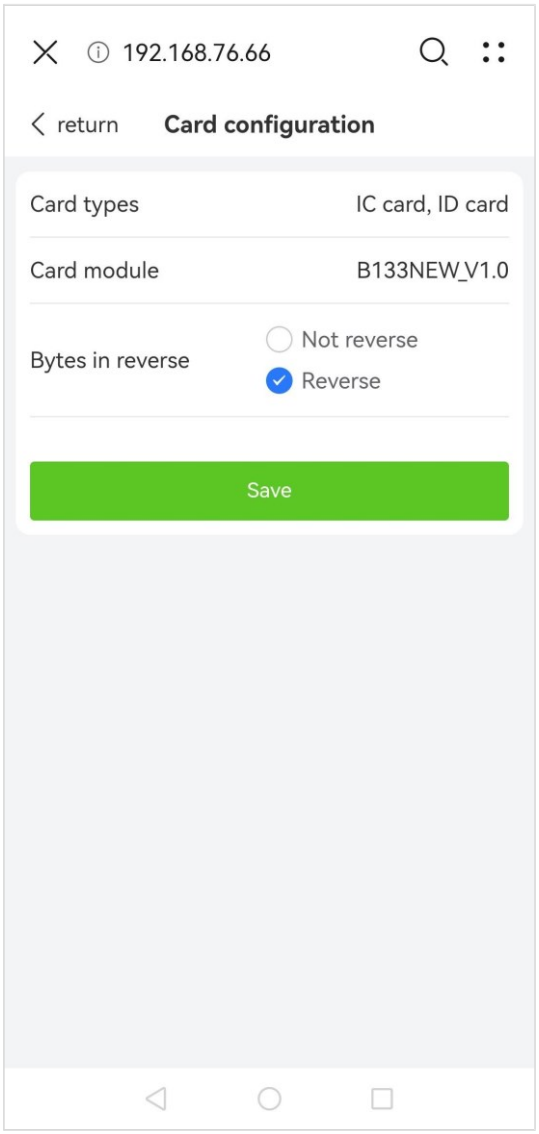
7.6 Device Status

In the device status interface, you can view the device status, and the primary and auxiliary clutch status etc. Click [**Device Status**] menu in the main interface to enter the device condition view interface.



7.7 Card Configuration

Click the [**Card Configuration**] menu in the main interface to enter the card configuration interface.

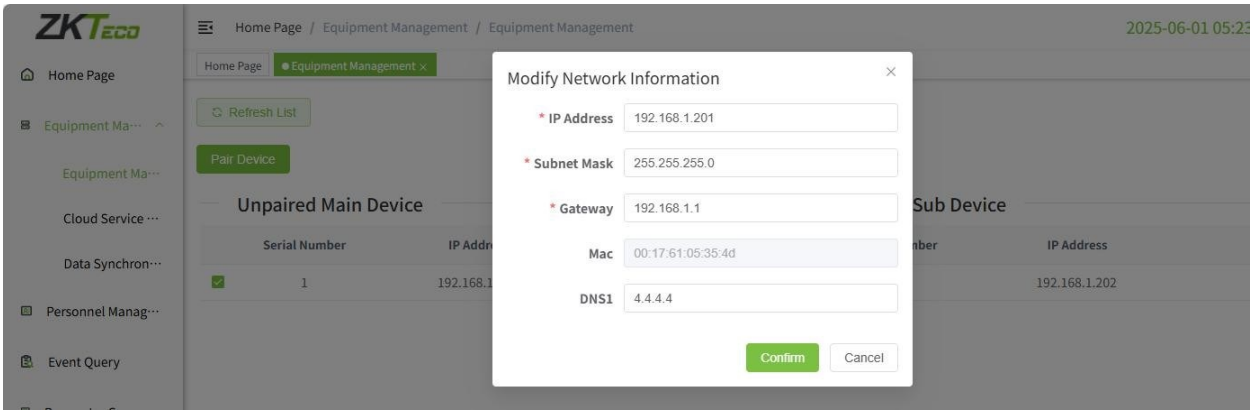


8 Connect to ZKBio CVSecurity Software

8.1 Set the Communication Address

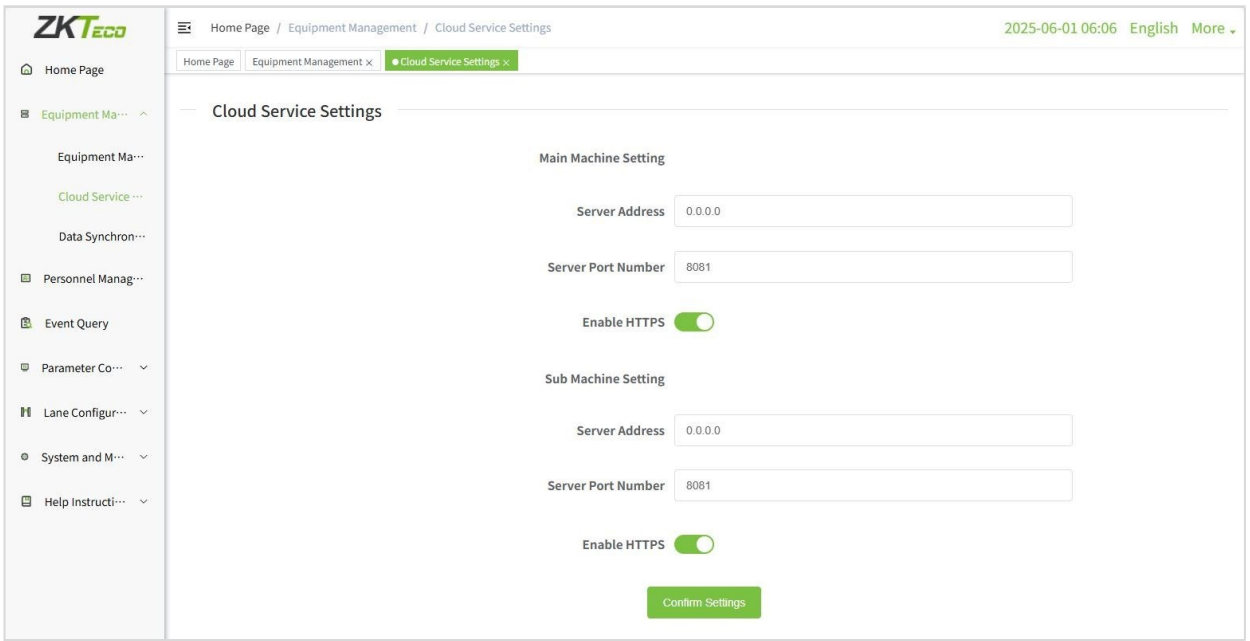
- Controller Side

1. Click [**Equipment Management**] - [**Equipment Management**] in the left menu bar to select the device and click the icon next to the device to modify its IP address.



- ***Note:*** *Please ensure that the IP address is in the same network segment as the server address and can communicate with the ZKBio CVSecurity server.*

2. Click [**Equipment Management**] - [**Cloud Service Settings**] in the left menu bar to set the server address and server port.

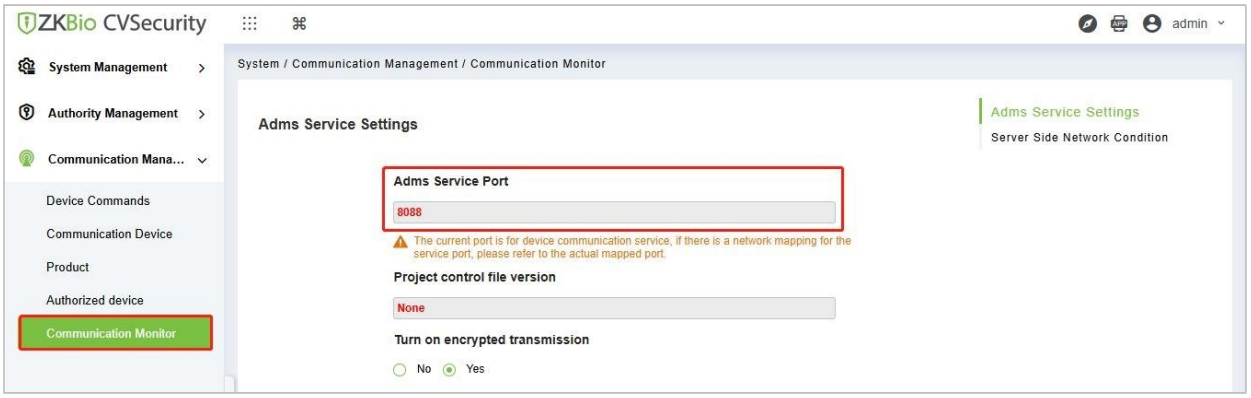


Server Address: Enter the IP address of the ZKBio CVSecurity server.

Server Port Number: Enter the service port of ZKBio CVSecurity (The default is 8088).

- **ZKBio CVSecurity Software Side**

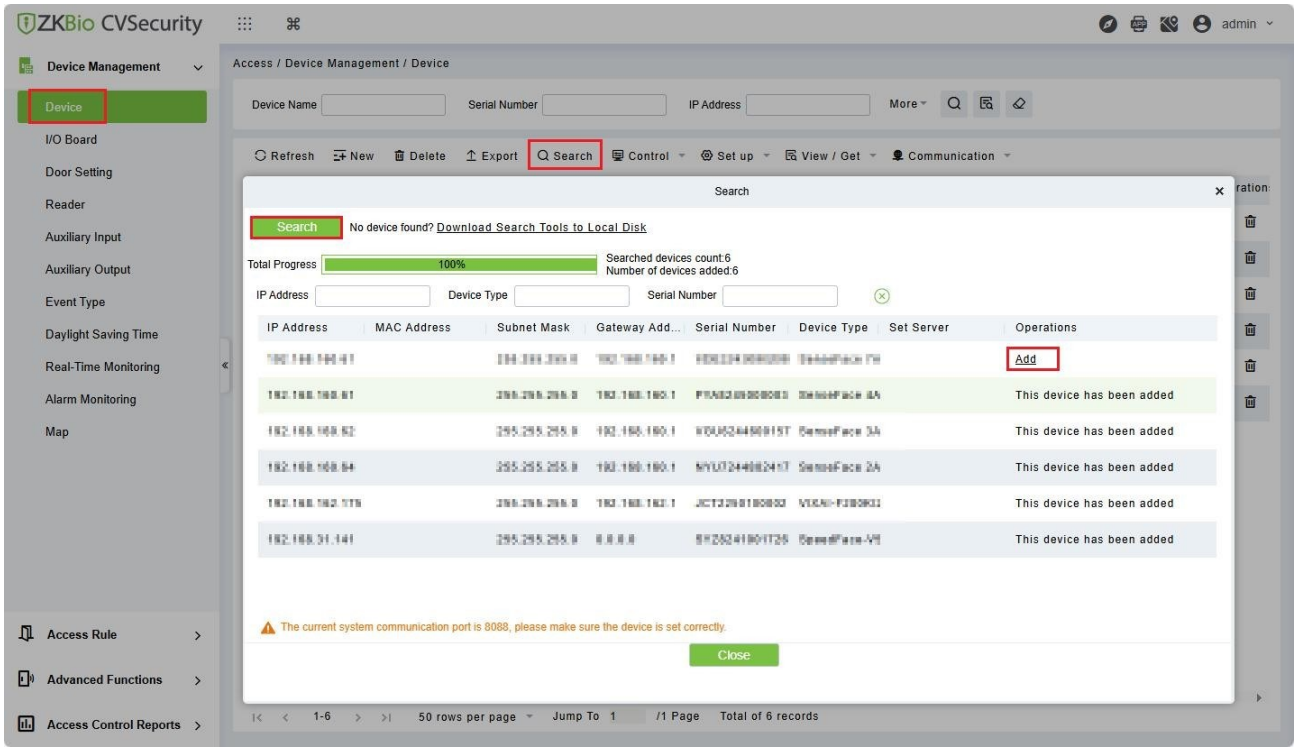
Login to ZKBio CVSecurity software, click [**System**] > [**Communication**] > [**Communication Monitor**] to set the ADMS service port, as shown in the figure below:



8.2 Add Device on the Software

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

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

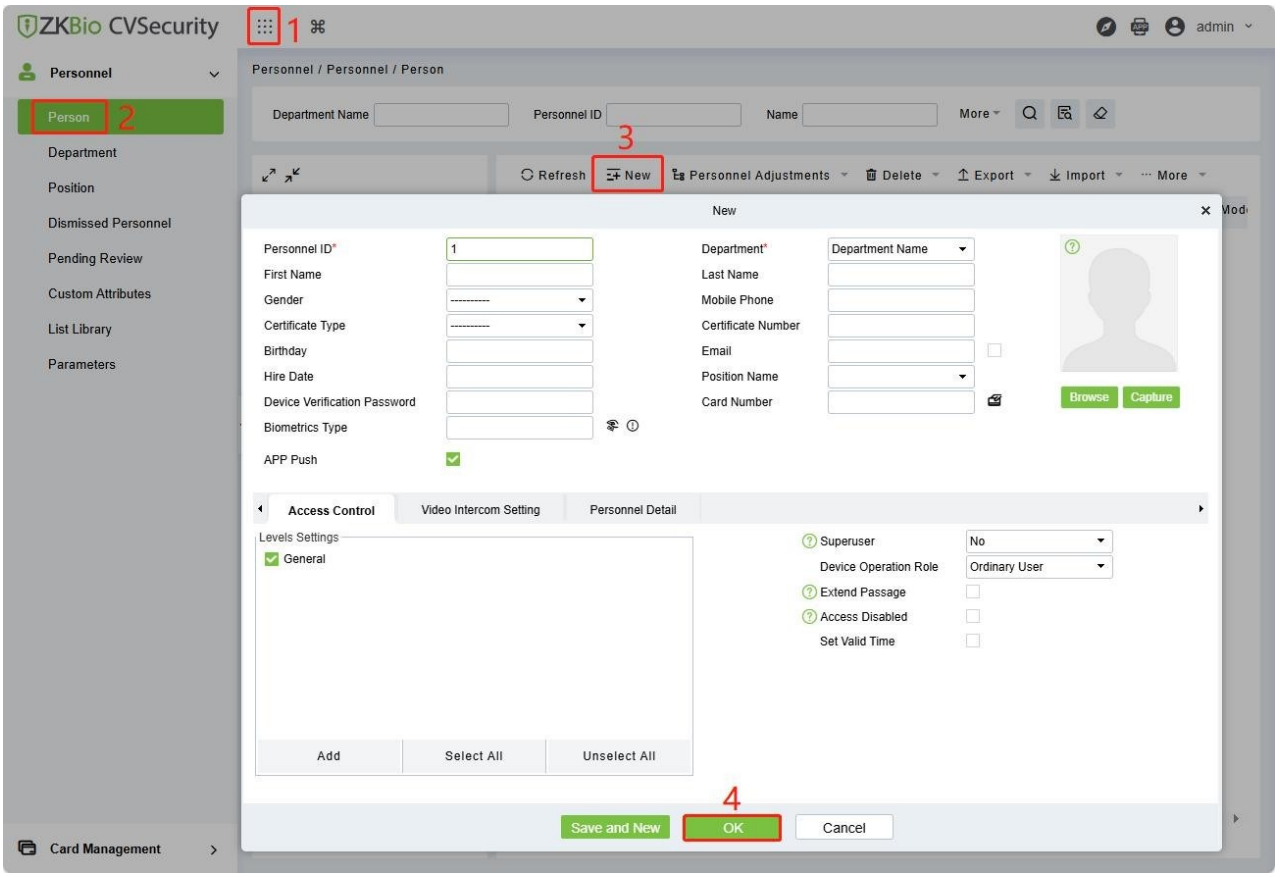


4. Click Add in operation column, a new window will pop-up. Select Icon type, Area, and Add to Level from each dropdown and click OK to add the device.

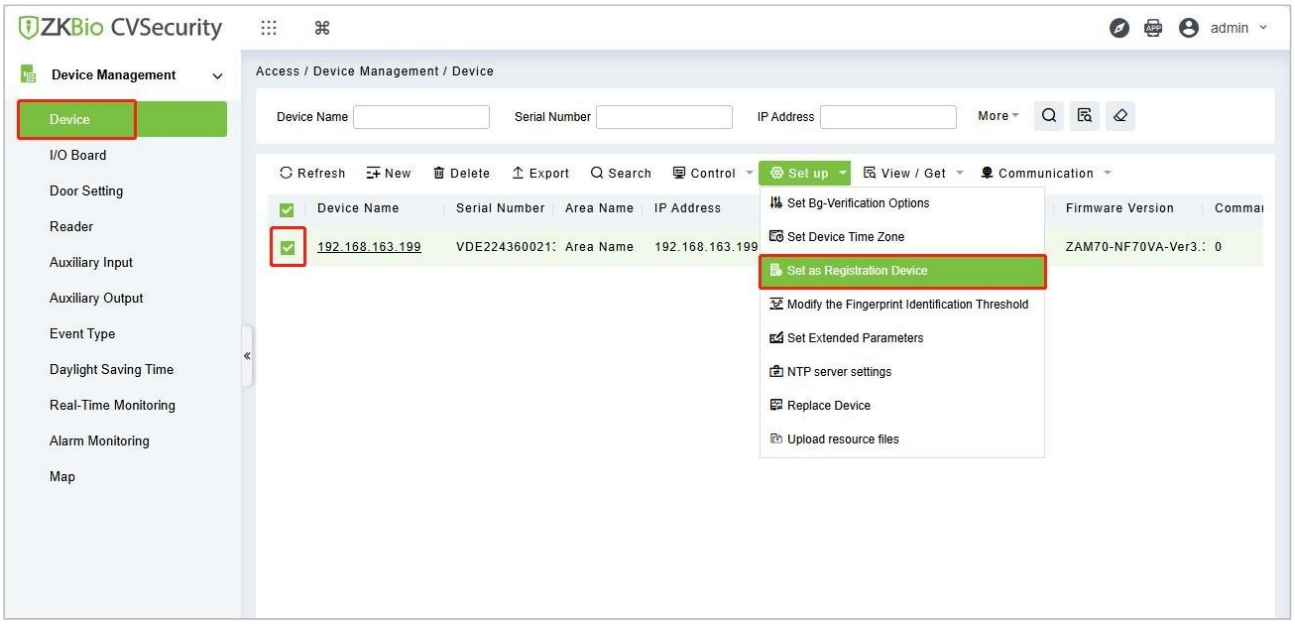
5. After the addition is successful, the device will be displayed in the device list.

8.3 Add Personnel on the Software

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



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



Revision History

Revision	Date	Author	Reviewer	Description
V1.0	07/29/2025	Julia Huang		Original Document

ZKTeco Industrial Park, No. 32, Industrial Road,

Tangxia Town, Dongguan, China.

Phone : +86 769 - 82109991

Fax : +86 755 - 89602394

www.zkteco.com