User Manual

ProMA Series

Date: May 2022

Doc Version: 1.1

English

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

For further details, please visit our Company's website

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.

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

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

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 the ProMA Series.

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 implies about the notice or pays attention to, in the manual.
	The general information which helps in performing the operations faster.
	The information which is significant.
	Care taken to avoid danger or mistakes.
	The statement or event that warns of something or that serves as a cautionary example.

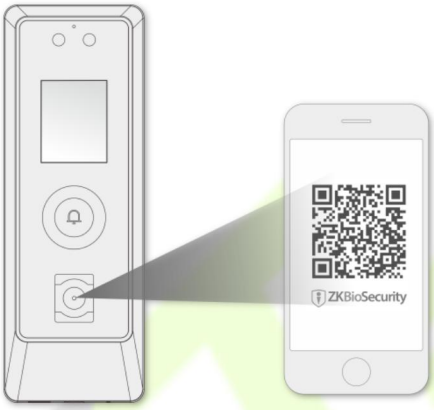
Table of Contents

1 Instruction for Use

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

1.1 How to scan the QR code?

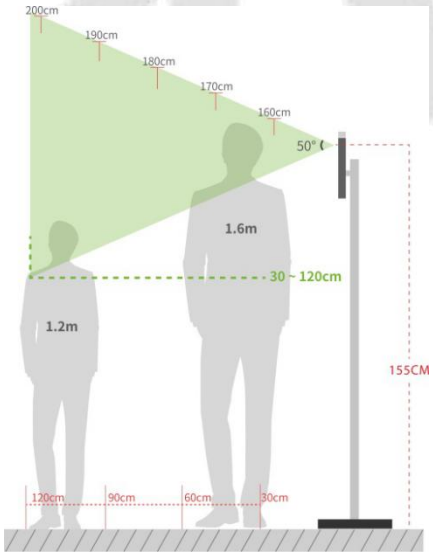
Open the Mobile Credential of ZKBioSecurity App and parallel the phone screen to the device QR code scanner.



Note: Place your phone within 15 to 50cm of the device (distance depends on the size of the phone screen), do not block the device QR code scanner and QR code in the phone screen.

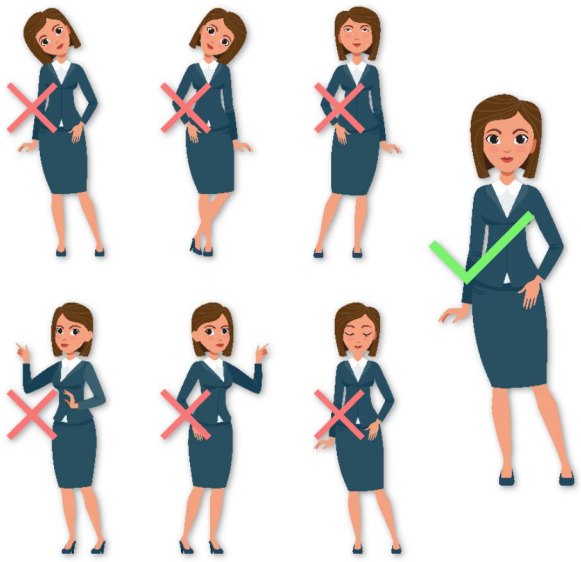
1.2 Standing Position, Posture and Facial Expression

- **The recommended distance**



The distance between the device and a user whose height is in a range of 1.55m to 1.85m is recommended to be 0.3 to 2.5m. Users may slightly move forward or backward to improve the quality of facial images captured.

- **Recommended Standing Posture and Facial Expression**



Standing Posture

Facial Expression

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

1.3 Face Registration

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

Correct face registration and authentication method

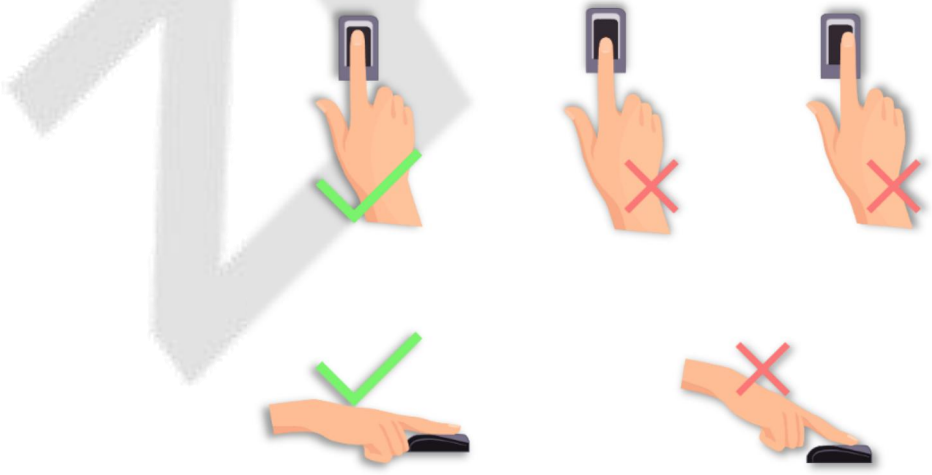
- **Recommendation for registering a face**
  - When registering a face, maintain a distance of 40cm to 80cm between the device and the face.
  - Be careful not to change your facial expression. (Smiling face, drawn face, wink, etc.)
  - If you do not follow the instructions on the screen, the face registration may take longer or may fail.
  - Be careful not to cover the eyes or eyebrows.
  - Do not wear hats, masks, sunglasses, or eyeglasses.
  - Be careful not to display two faces on the screen. Register one person at a time.
  - It is recommended for a user wearing glasses to register both faces with and without glasses.

- **Recommendation for authenticating a face**
  - Ensure that the face appears inside the guideline displayed on the screen of the device.
  - If the glasses have been changed, authentication may fail. If the face without glasses has been registered, authenticate the face without glasses further. If the face with glasses has been registered, authenticate the face with the previously worn glasses.
  - If a part of the face is covered with a hat, a mask, an eye patch, or sunglasses, authentication may fail. Do not cover the face, allow the device to recognize both the eyebrows and the face.

1.4 Finger Placement

Recommended fingers: Index, middle, or ring fingers.

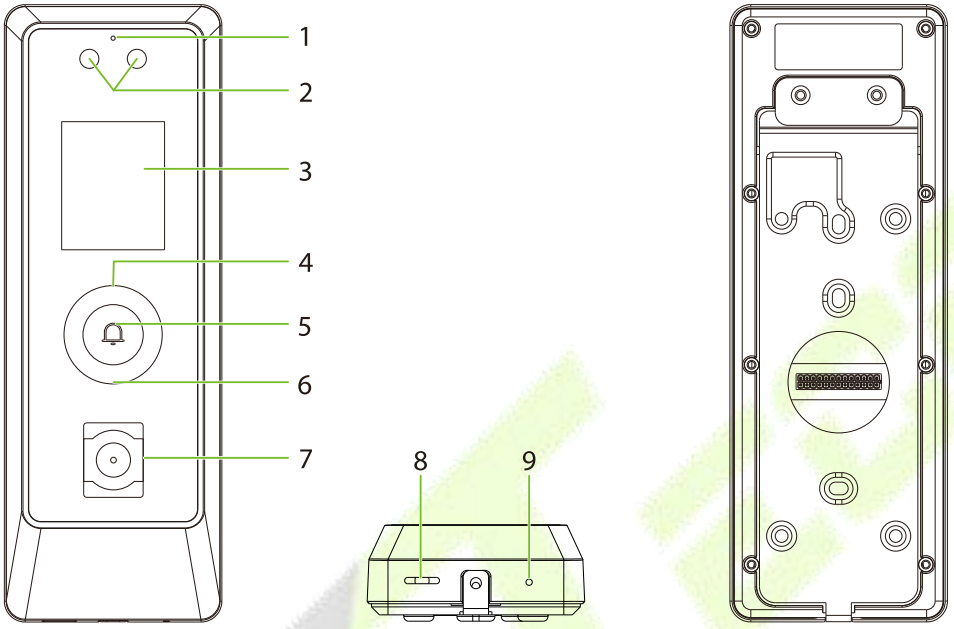
Avoid using the thumb or pinky, as they are difficult to accurately tap onto the fingerprint reader.



Note: Please use the correct method when pressing your fingers onto the fingerprint reader for registration and identification.

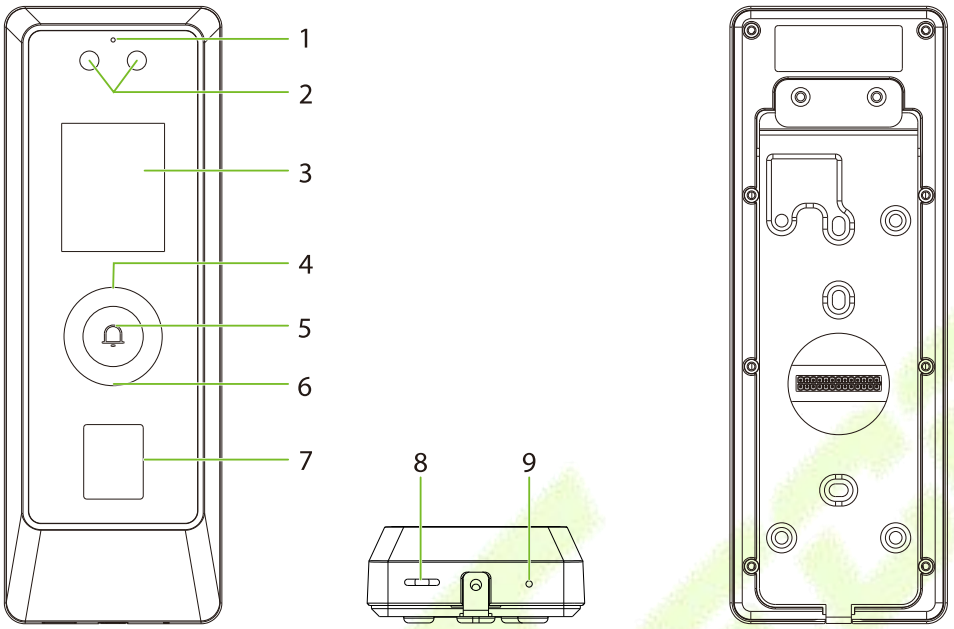
2 Appearance

2.1 ProMA-QR



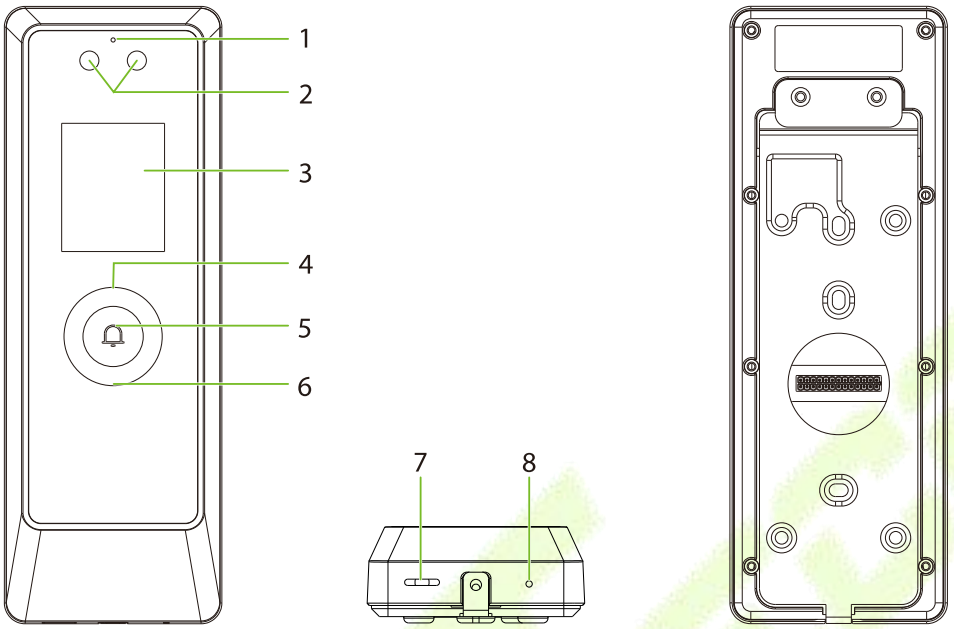
No.	Description
1	Microphone
2	Camera
3	2" Display Screen
4	Card Reading Area
5	Doorbell Button
6	Flash
7	QR Code Scanner
8	Speaker
9	Reset

2.2 ProMA



No.	Description
1	Microphone
2	Camera
3	2" Display Screen
4	Card Reading Area
5	Doorbell Button
6	Flash
7	Fingerprint Sensor
8	Speaker
9	Reset

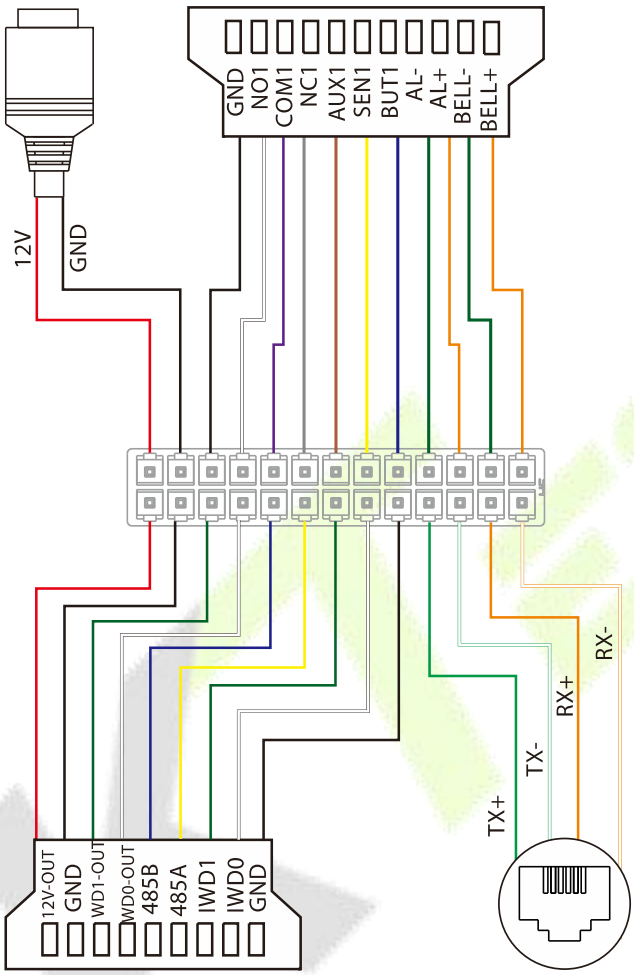
2.3 ProMA-RF



No.	Description
1	Microphone
2	Camera
3	2" Display Screen
4	Card Reading Area
5	Doorbell Button
6	Flash
7	Speaker
8	Reset

2.4 Terminal and Wiring Description

2.4.1 Terminal Description

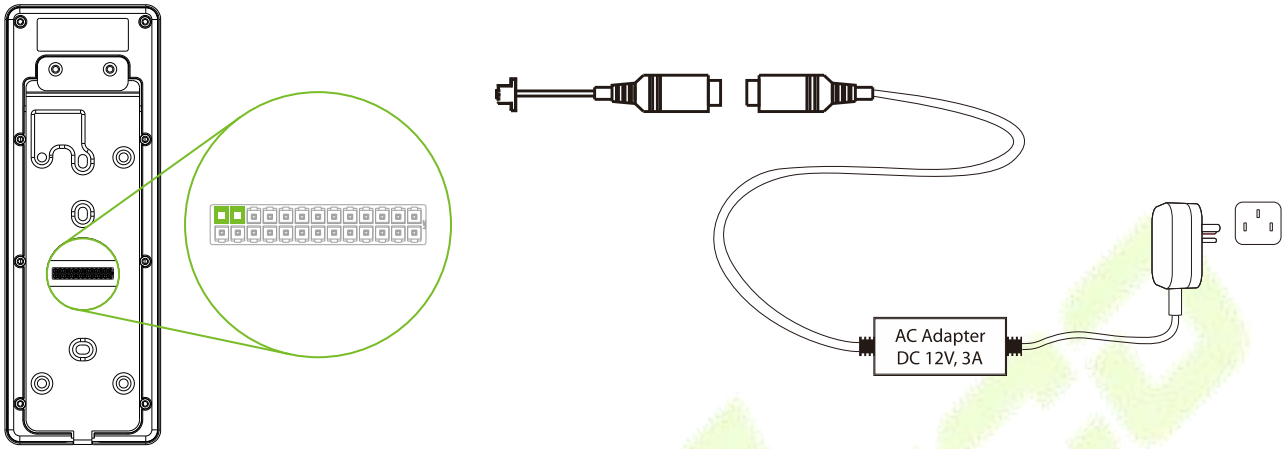


Interface	Description
12V	12V Power In
GND	
GND	
NO1	Lock
COM1	
NC1	

AUX1	Auxiliary Input
SEN1	Sensor
BUT1	Exit Button
AL-	Alarm
AL+	
BELL-	Bell
BELL+	
12V-OUT	Power Out
GND	
WD1-OUT	Wiegand Out
WD0-OUT	
485B	RS485
485A	
IWD1	Wiegand In
IWD0	
GND	
TX+	Network Interface
TX-	
RX+	
RX-	

2.5 Wiring Description

2.5.1 Power Connection



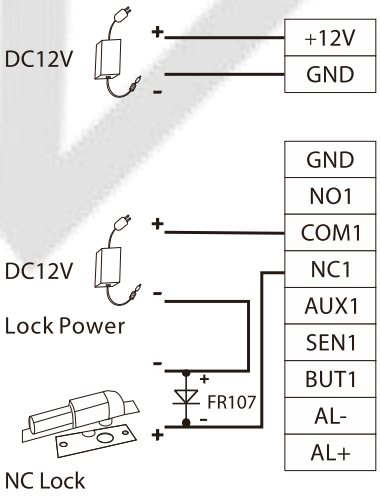
Recommended power supply

- Rating of 12V and 3A
- To share the device's power with other devices, use a power supply with higher current ratings.

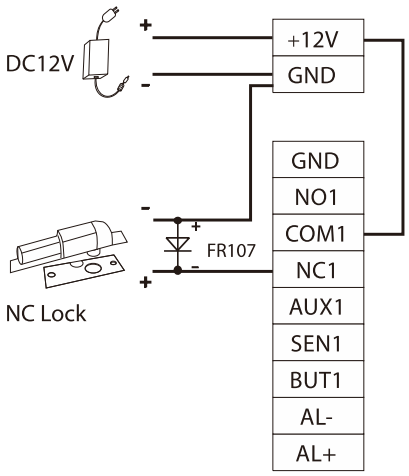
2.5.2 Lock Relay Connection

The system supports both Normally Opened Lock and Normally Closed Lock. The NO Lock (normally opened when powered) is connected with 'NO1' and 'COM1' terminals, and the NC Lock (normally closed when powered) is connected with 'NC1' and 'COM1' terminals. The power can be shared with the lock or can be used separately for the lock, as shown in the example with NC Lock below:

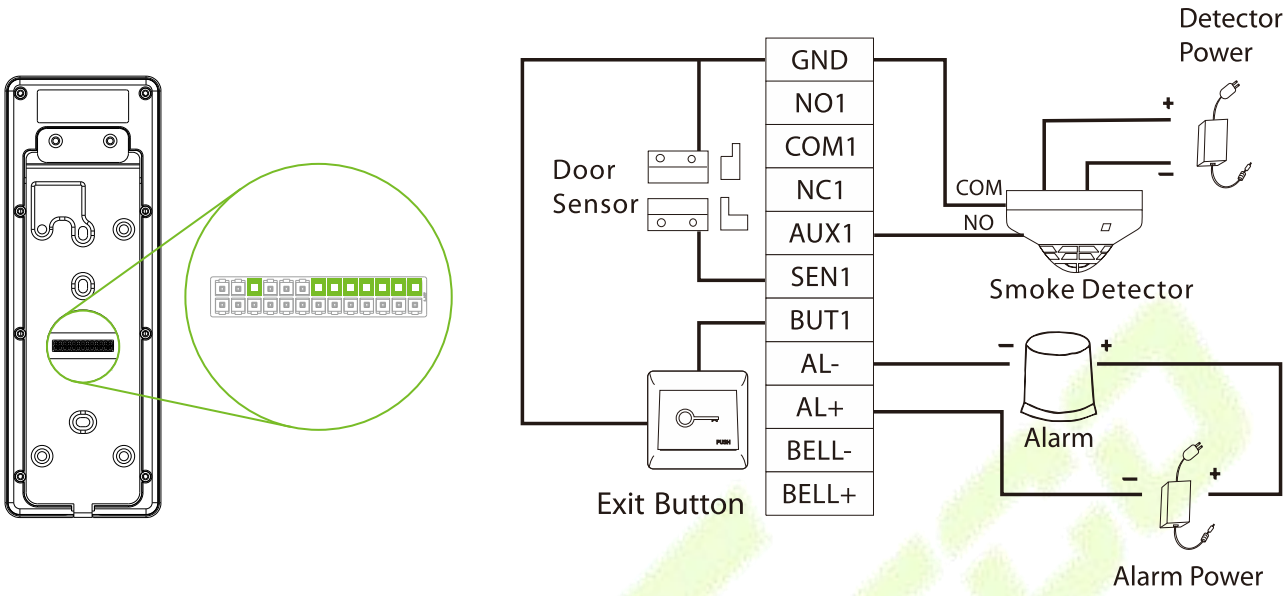
1) Device not sharing power with the lock



2) Device sharing power with the lock

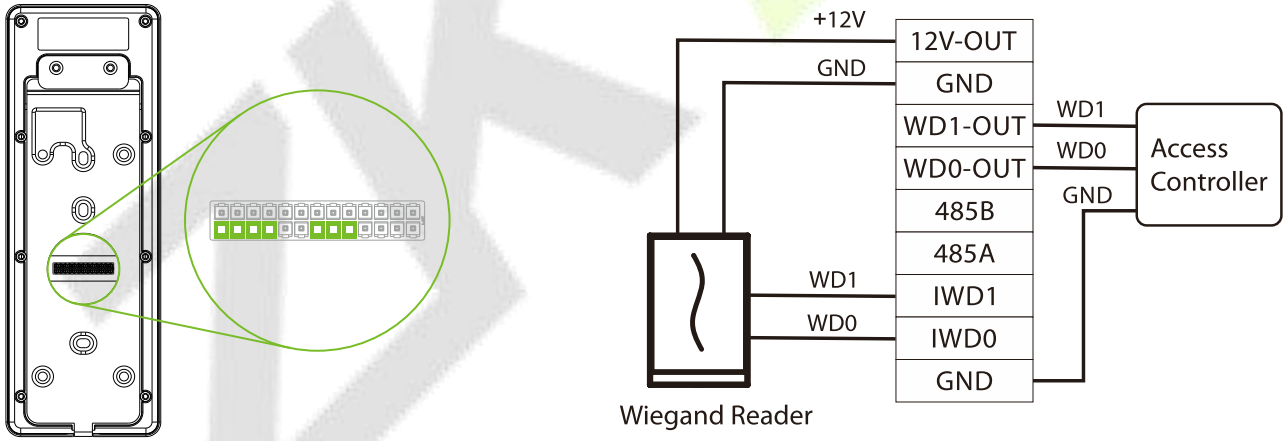


2.5.3 Door Sensor, Exit Button, Alarm and Auxiliary Connection



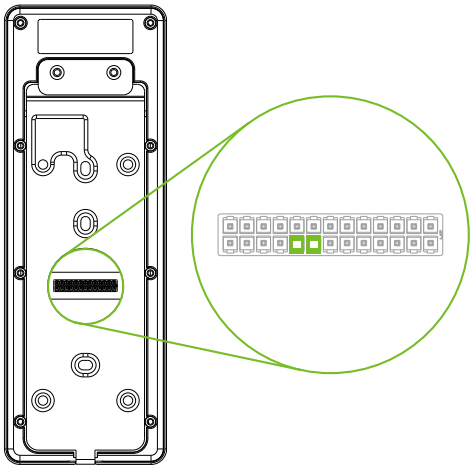
2.5.4 Wiegand Connection

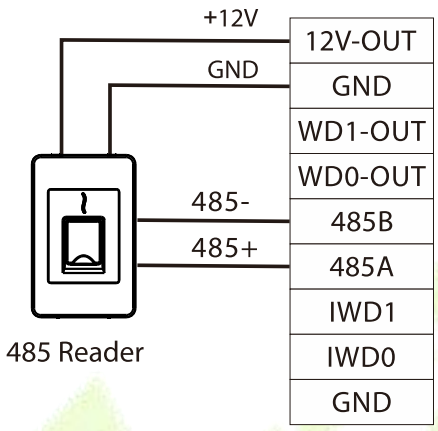
The Wiegand card reader connects to the top 4 pins of the Wiegand terminal and the last two pins are used by the Access Controller, as shown in the following figure. It sends the credentials to the device via Wiegand communication.



2.5.5 RS485 Connection

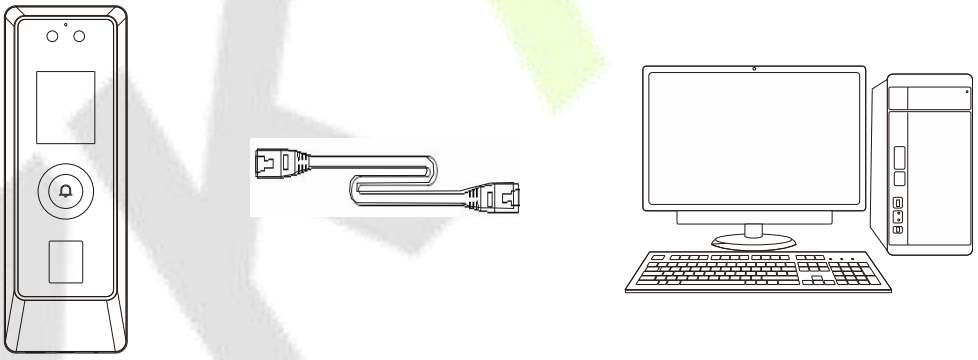
The RS485 lets users connect to multiple readers to the device. RS485 can be connected to the terminal, as shown in the figure below.





2.5.6 Ethernet Connection

Connect the device and computer software over an Ethernet cable. An example is shown below:



Default IP address: 192.168.1.201
Subnet mask: 255.255.255.0

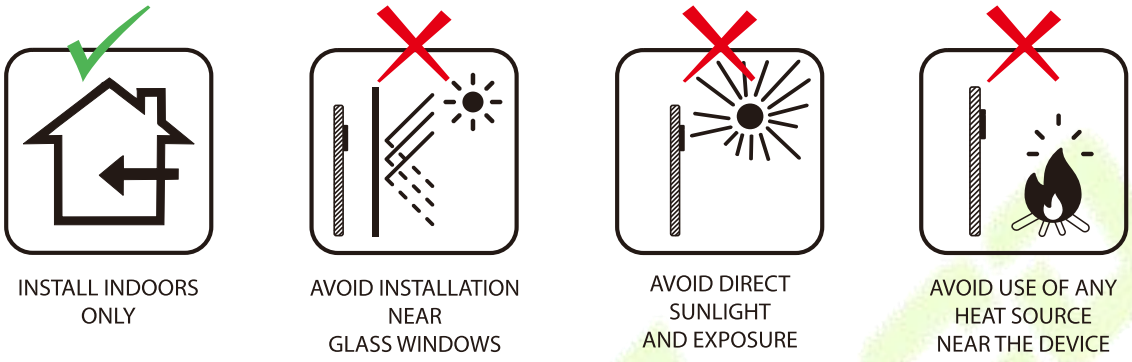
IP address: 192.168.1.130
Subnet mask: 255.255.255.0

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

3 Installation

3.1 Installation Environment

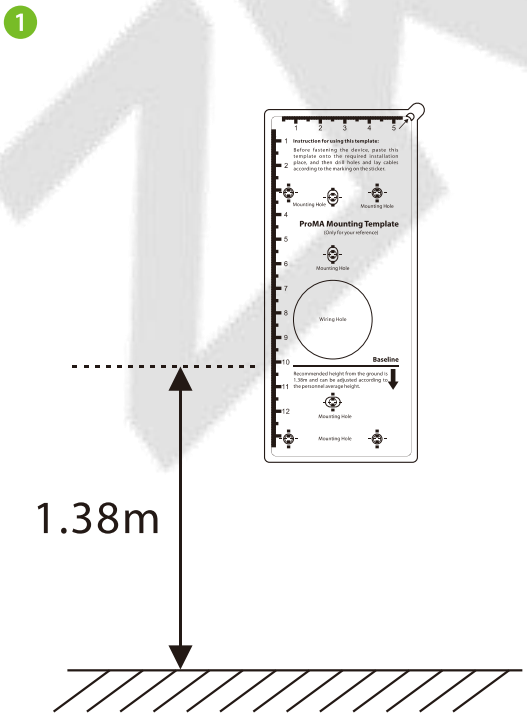
Please refer to the following recommendations for installation.

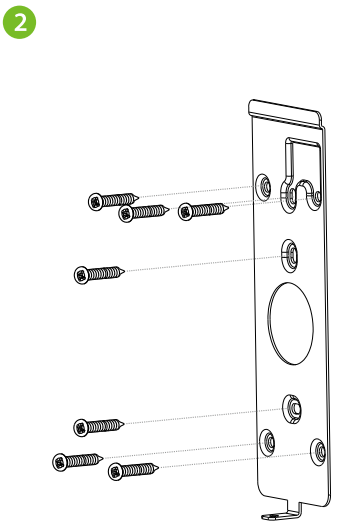


3.2 Device Installation

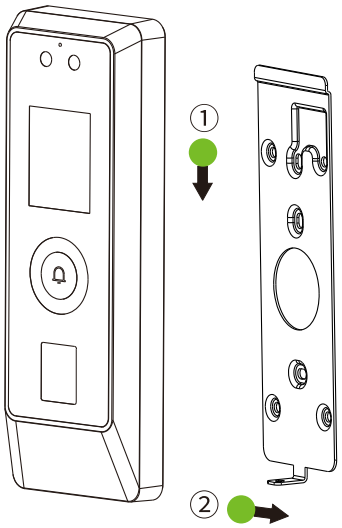
ProMA series installations are the same, the following is an example of ProMA.

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

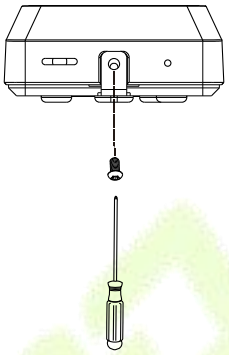




3



4



4 Standby Interface

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

The device has a built-in IP address, which can be used for device communication, connection to WebServer and ZKBio CVSecurity software, etc.

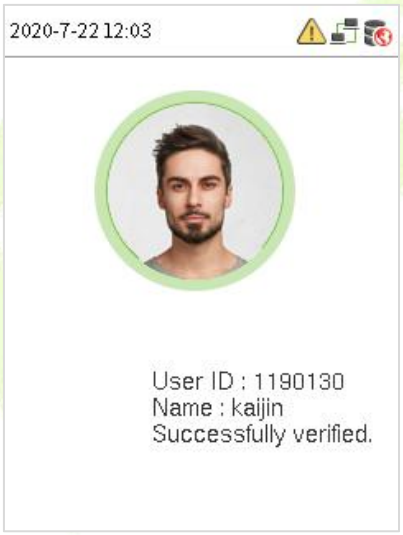
Note: The device uses a 2'' display screen, which does not support touch operation and is only used to display status and verification information. All operations such as device information, communication settings, user management and system settings are operated and set up on WebServer.

5 Verification Mode

5.1 QR Code Verification★

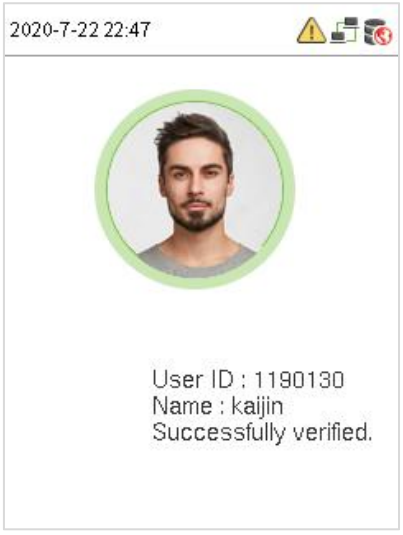
In this verification mode, the device compares the QR code image collected by the QR code collector with all the QR code data in the device.

Tap [**Mobile Credential**] on the ZKBioSecurity App, and a QR code will appear, which includes employee ID and card number (static QR code only includes card number) information. The QR code can replace a physical card on a specific device to achieve contactless authentication. Please refer to 12.4 Mobile Credential★.



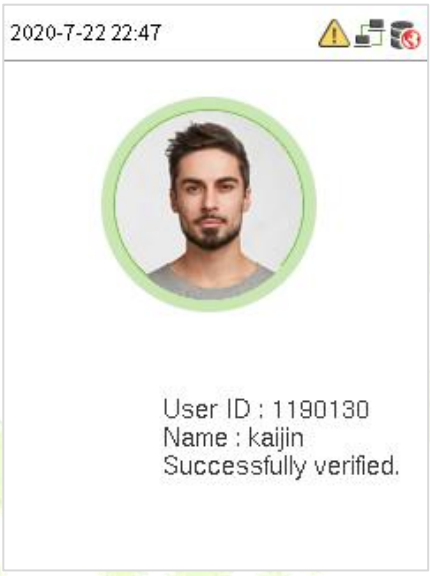
5.2 Facial Verification

In this verification mode, the device compares the collected facial images with all face data registered in the device. The following is the pop-up prompt of a successful comparison result.



5.3 Card Verification

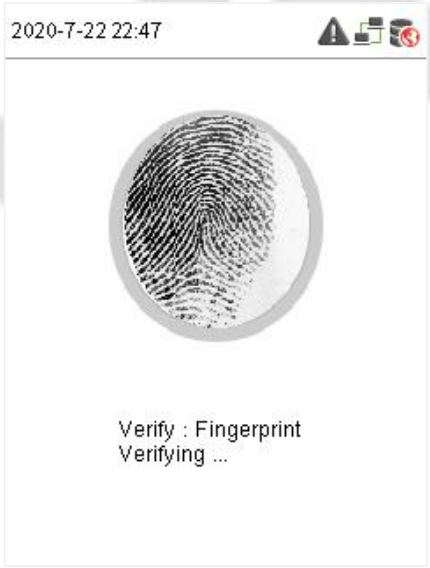
The Card Verification mode compares the card number in the card induction area with all the card number data registered in the device; The following is the card verification screen.

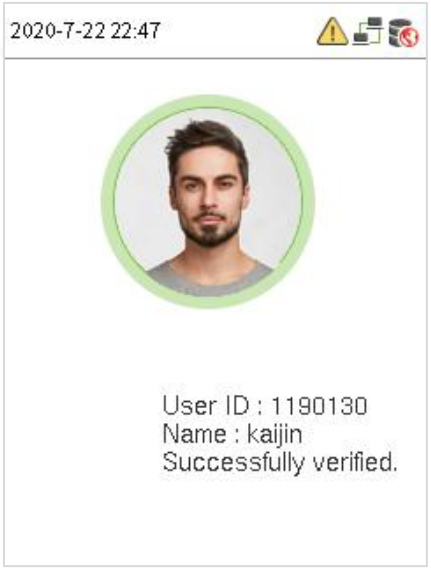


5.4 Fingerprint Verification★

This method compares the fingerprint of the user that is being pressed onto the fingerprint reader with all the fingerprint data that is pre- stored in the device.

To enter fingerprint identification mode, simply tap your finger on the fingerprint reader.

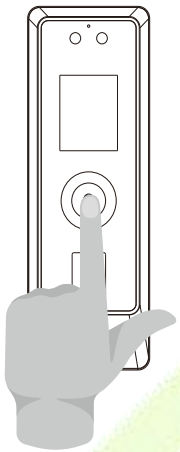




6 Login WebServer

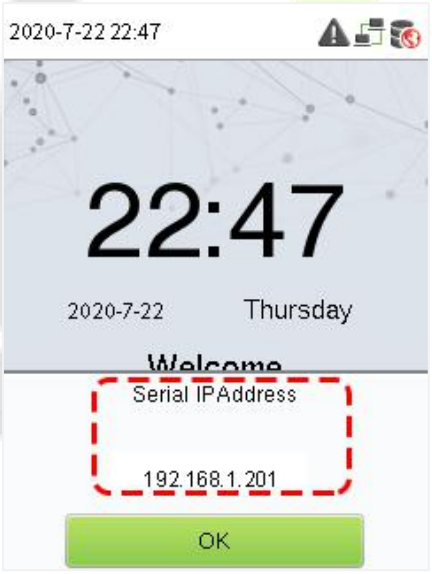
A user can open the web application to set the relevant parameters of the device.

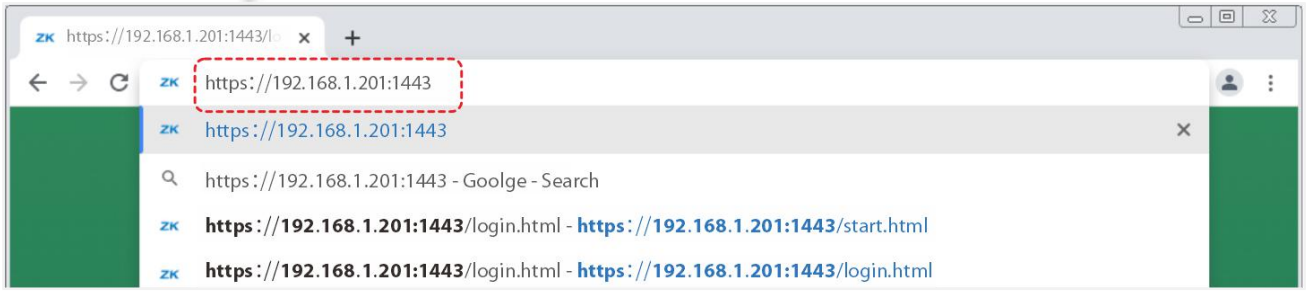
1. Press and hold the Doorbell Button of the device until the IP pops up.

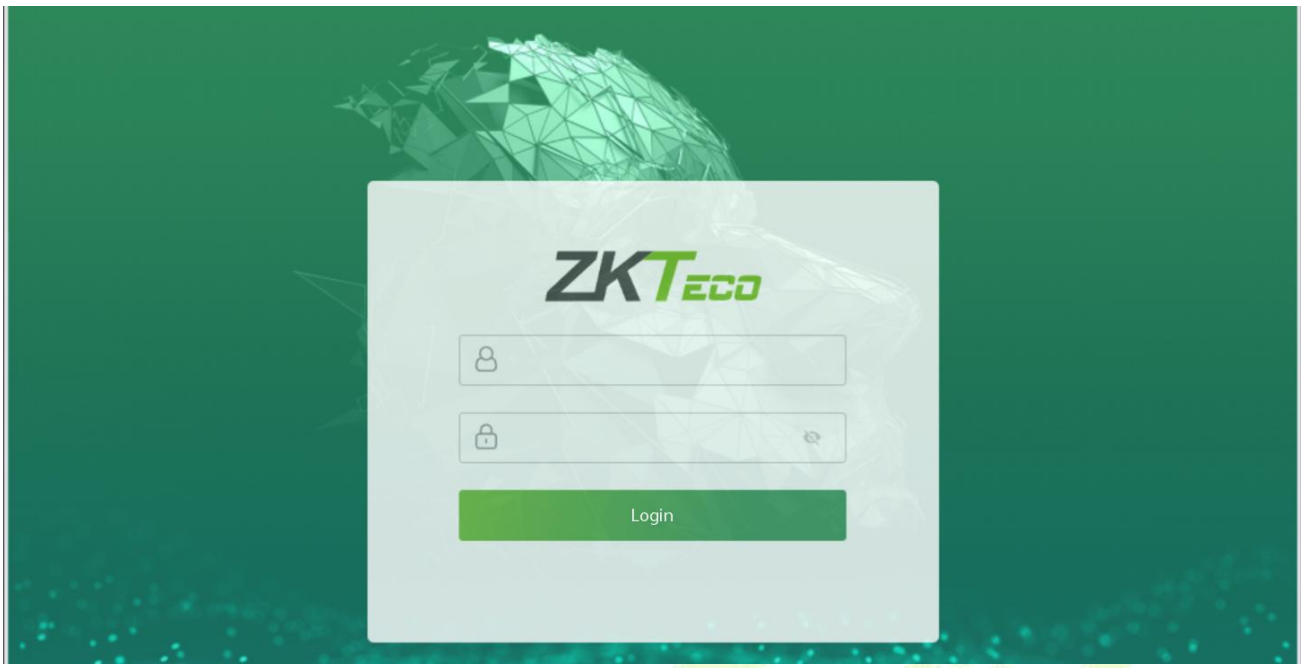


2. Open a browser to enter the address to log in to the WebServer, the address is https:// **Serial IP Address:1443**. For example: **https://192.168.1.201:1443.**

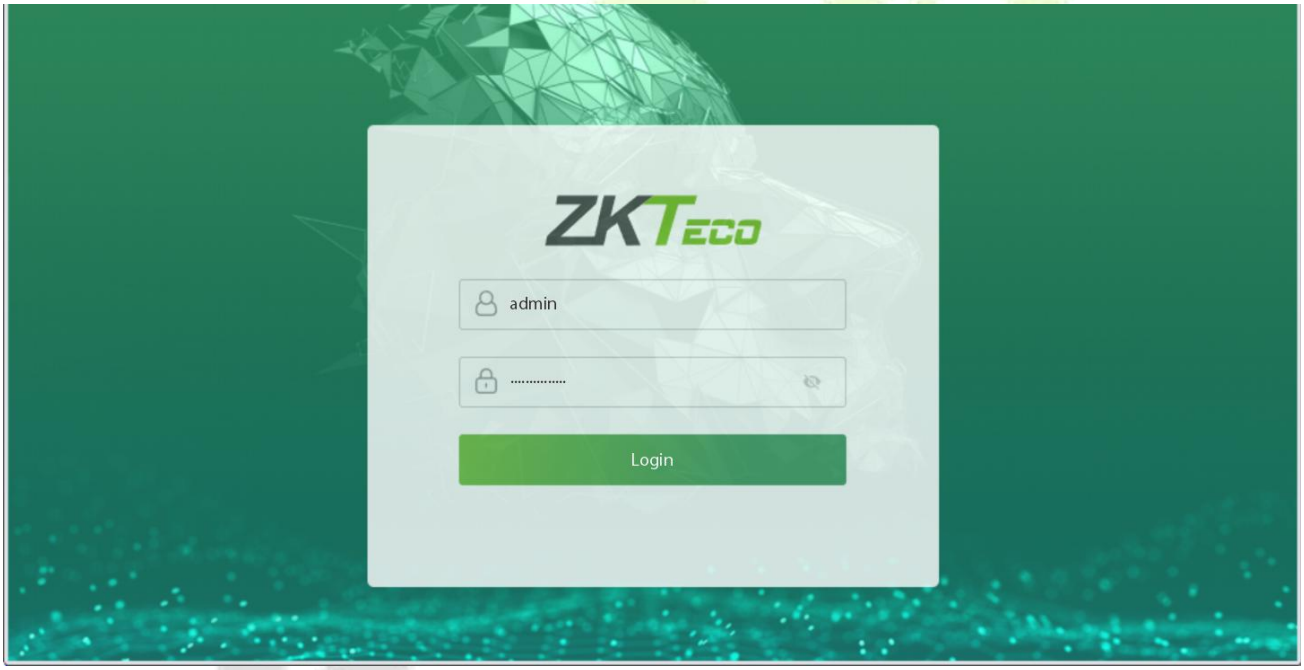
   Note: The Serial IP Address of the device for communication can be modified, for details please refer to Communication Settings.







3. Enter the WebServer account and password, the default account is: **admin**, password: **admin@123**.



Note:

1. After logging in for the first time, users need to change their original password and log in again before they can use it, please refer to 10.3 Change Password.

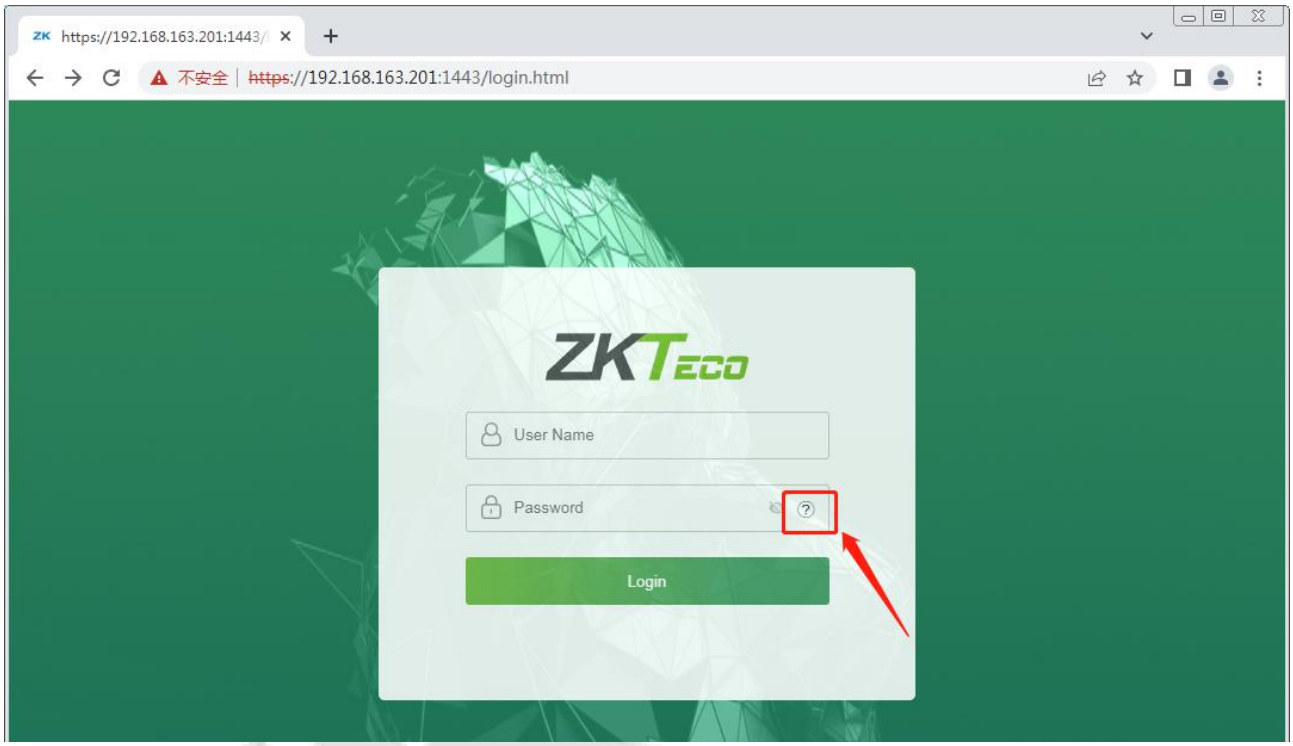
2. In order to retrieve the password easily, please register a super admin first, please refer to 8.1 User Registration.

7 Forgot Password

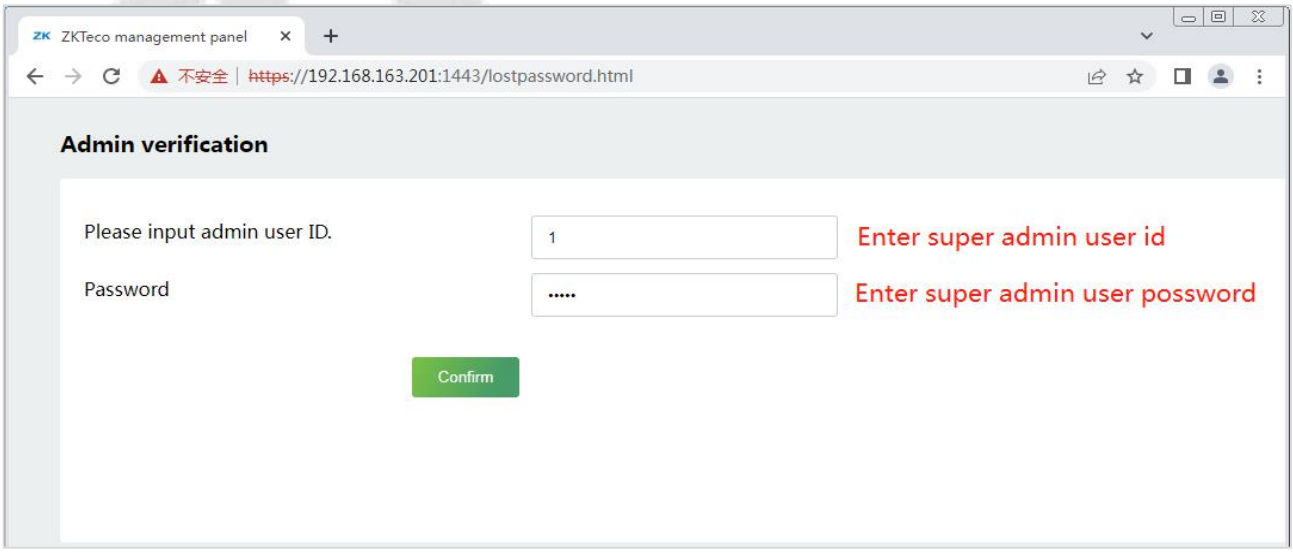
- **Method 1 (When there is a super admin):**

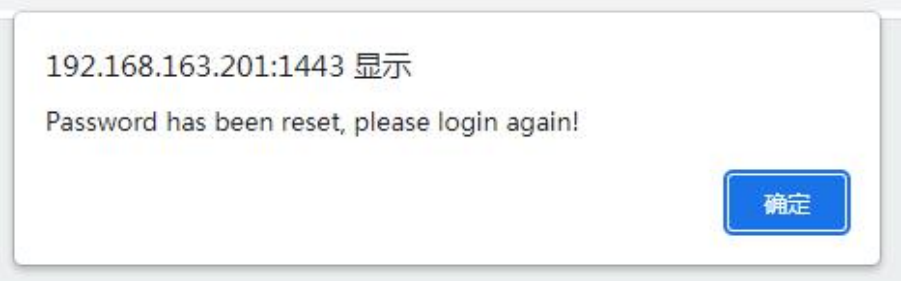
If you forgot the password of WebServer, you can reset it by the registered super admin. The detailed steps are as follows:

1. Click the icon on the login interface.



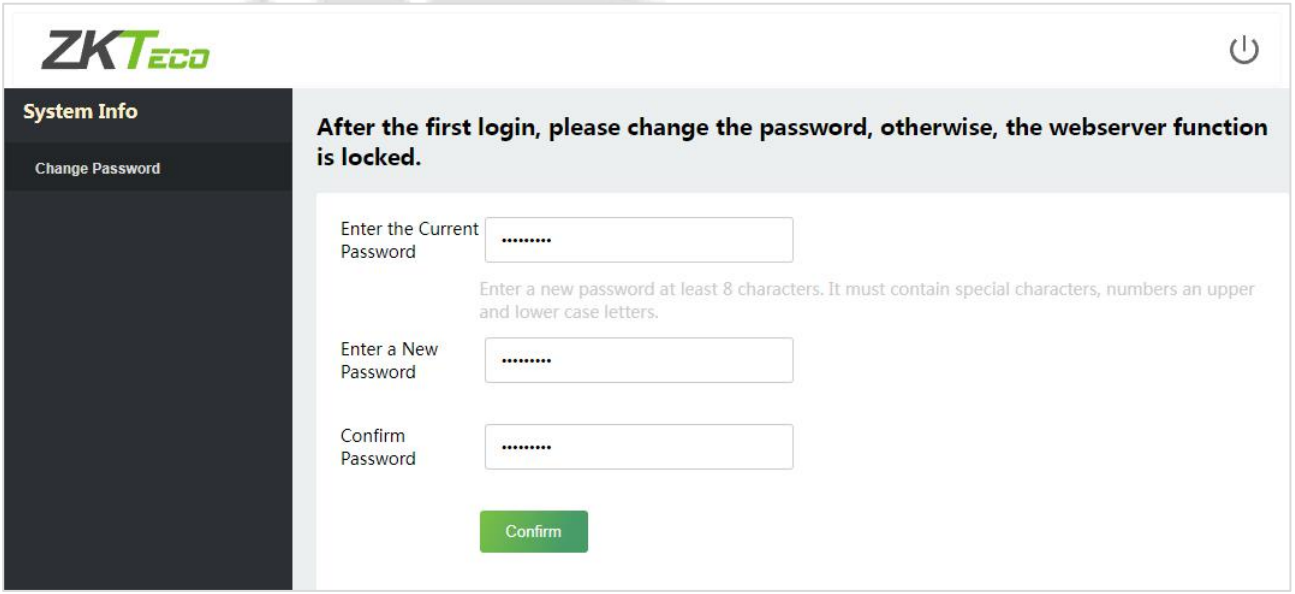
2. On the pop-up page, enter the relevant information of the super admin user as prompted.





3. After a successful reset, enter the default account and password (account: **admin**, password: **admin@123**) on the login interface to log in.

4. For security reasons, please change your password after successfully logging in.

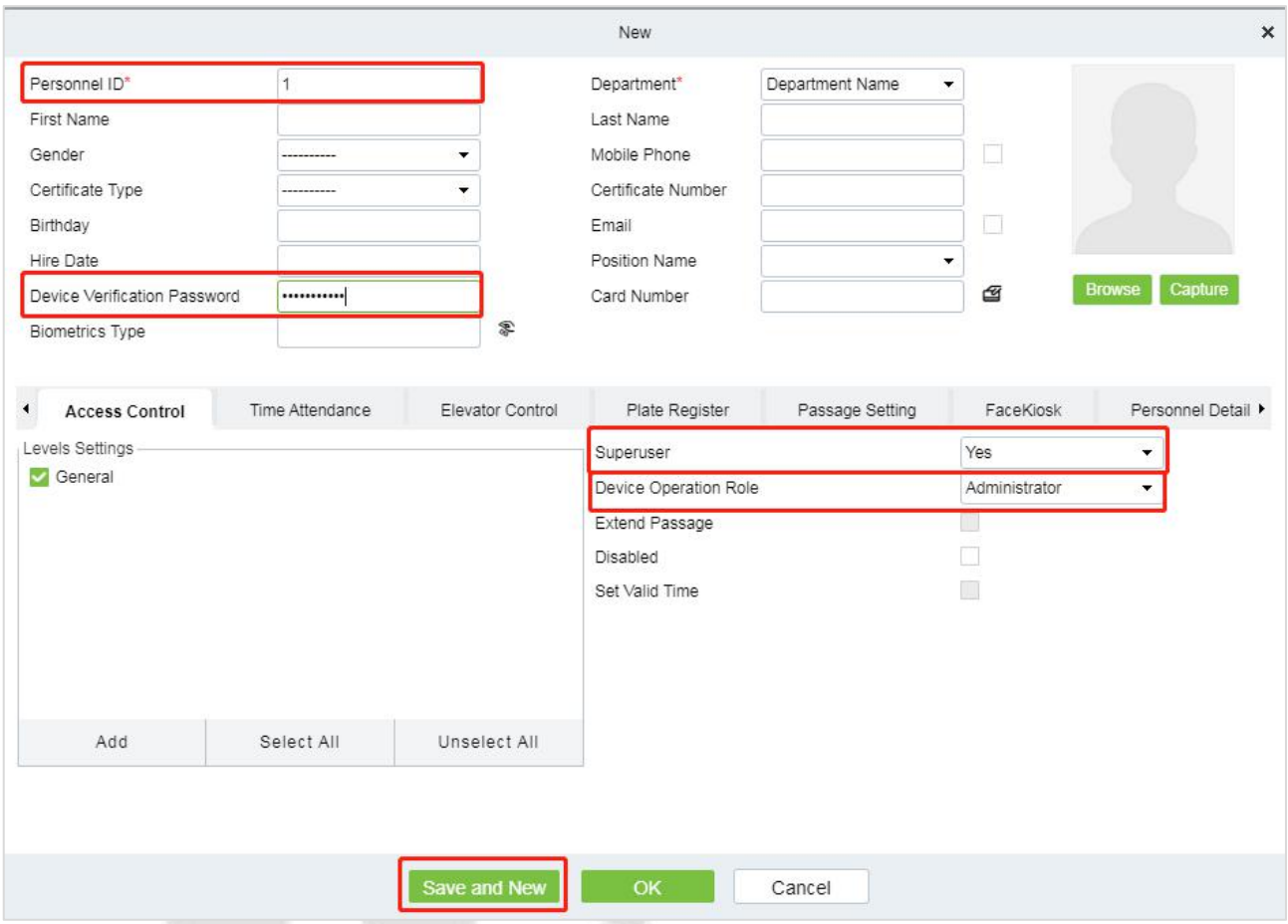


Note: The super admin must exist.

- **Method 2 (When there is not a super admin):**

If the network of the device is normal and ZKBio CVSecurity has been connected, you can reset the password by sending the super admin account and password from the server.

1. Click **Personnel** > **Person** > **New** on the ZKBio CVSecurity Server.



2. After registering the information of the super admin, click **Save and New**.
3. 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 *ZKBio CVSecurity V6600 User Manual*.

4. After the data synchronization is successful, you can reset the password with the newly registered super admin. The operation steps are the same as method 1.

- **Method 3:**

If the device has not registered a super admin and cannot connect to the server, please contact our after-sales technicians to help retrieve the password.

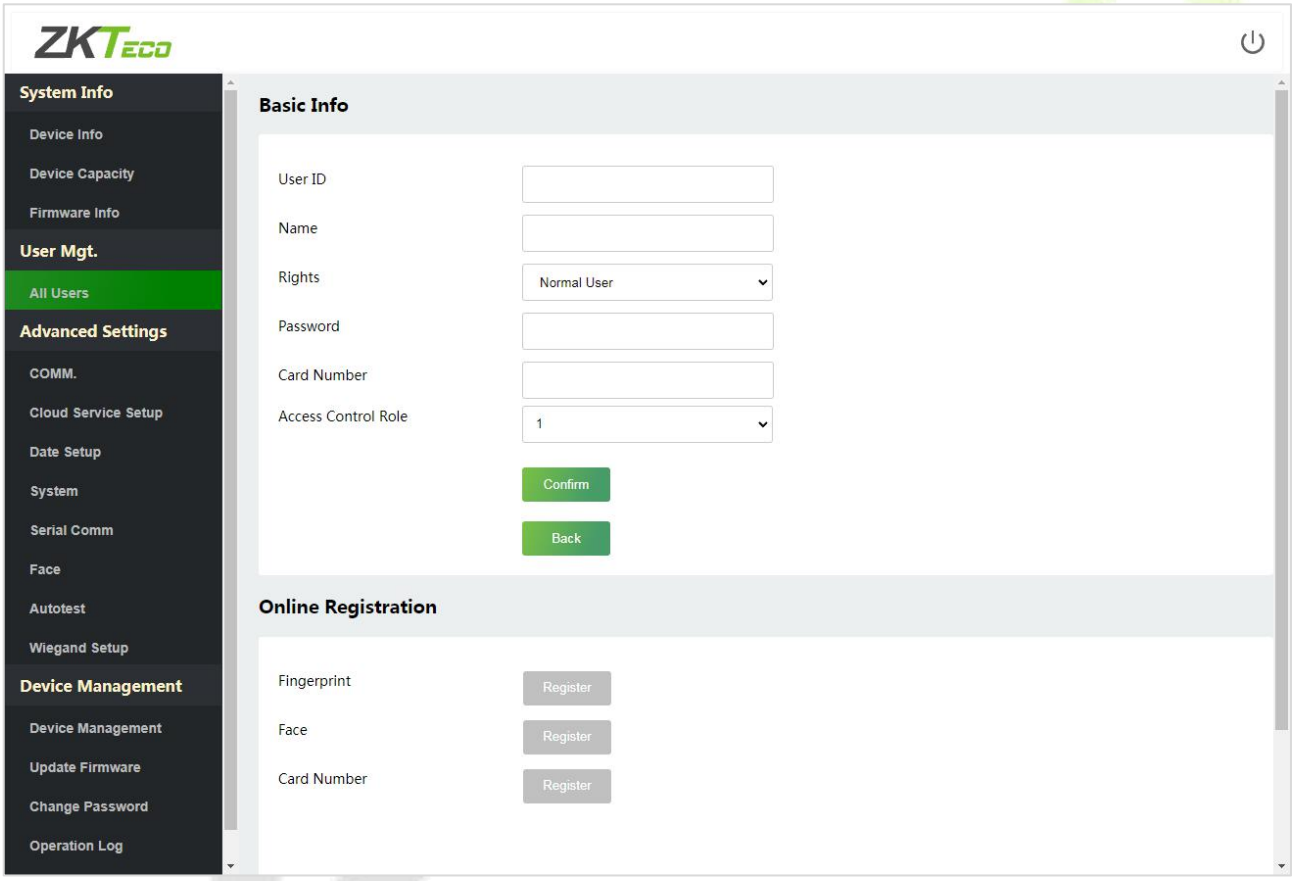
8 User Management

8.1 User Registration

8.1.1 Basic Information

Click **All Users** on the WebServer.

In this interface, you can register the User ID, Name, Rights, Password, Card Number and Access Control Role of the new user, click **Confirm** to save.



Function Name	Description
User ID	The user ID may contain 1 to 14 characters by default. It can be numbers, letters, symbols, etc.
Name	A name can be up to 63 characters.

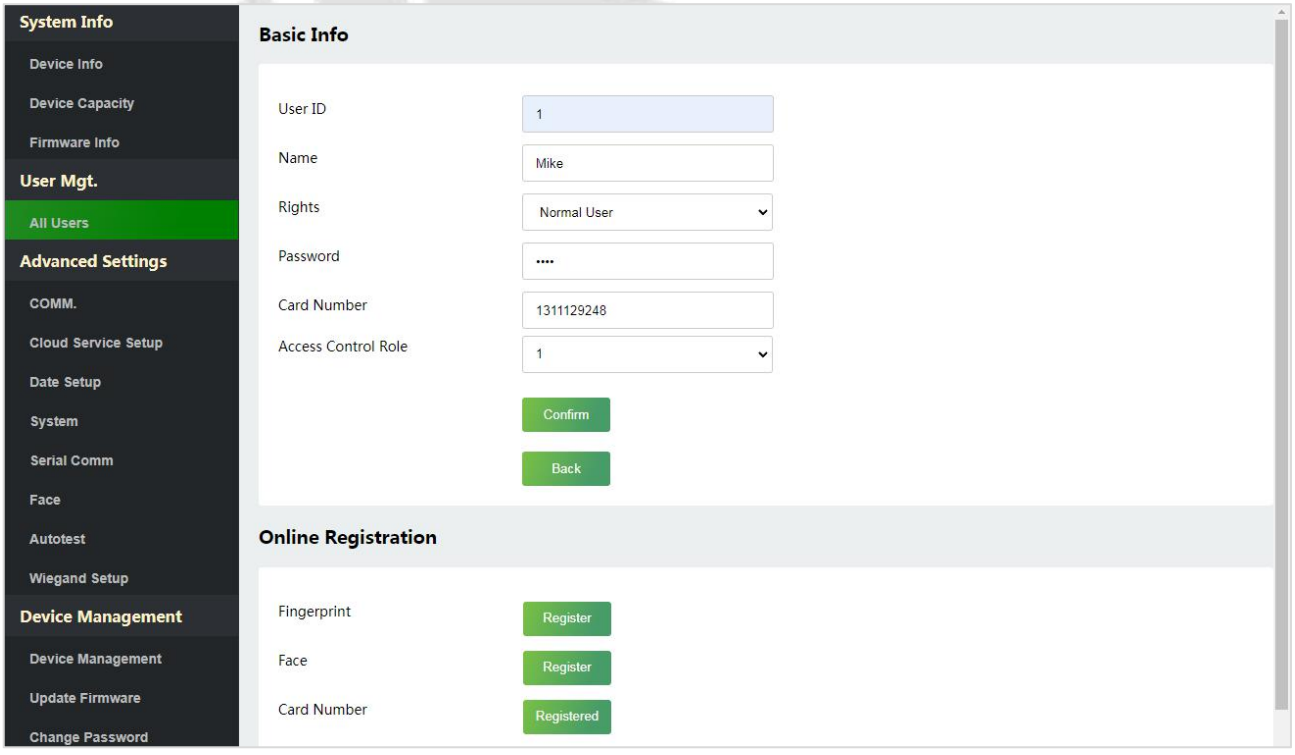
Rights	Set the role for the user as either Normal User or Super Admin. • **Super Admin:** The Super Admin owns all management privileges in the WebServer. • **Normal User:** If the Super Admin is already registered in the WebServer, then the Normal Users will not have the privileges to manage the system and can only access authentication verifications.
Password	Set the user's registration password.
Card Number	Enter the card number manually, after registering the user's card number, the user can swipe the card for verification.
Access Control Role	The Access Control Role sets the door access privilege for each user, new users will be added to Group 1 by default, which can be reassigned to other required groups. The system supports up to 10 access control groups.

Note:

1. During the initial registration, you can modify your ID; you cannot be modifying the registered ID once after the successful registration.
2. If the message **"Setup failed!"** pops up, you must choose a different User ID because the one you entered already exists.

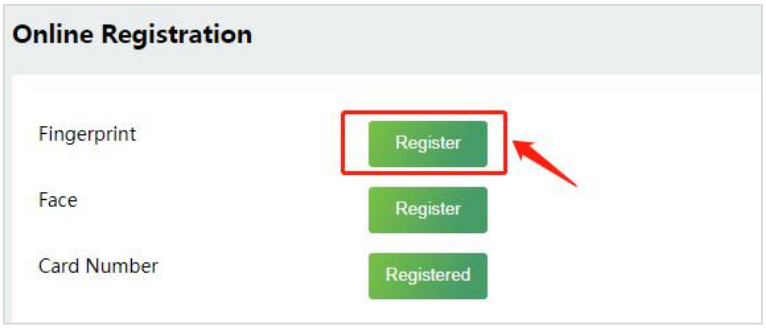
8.1.2 Online Registration

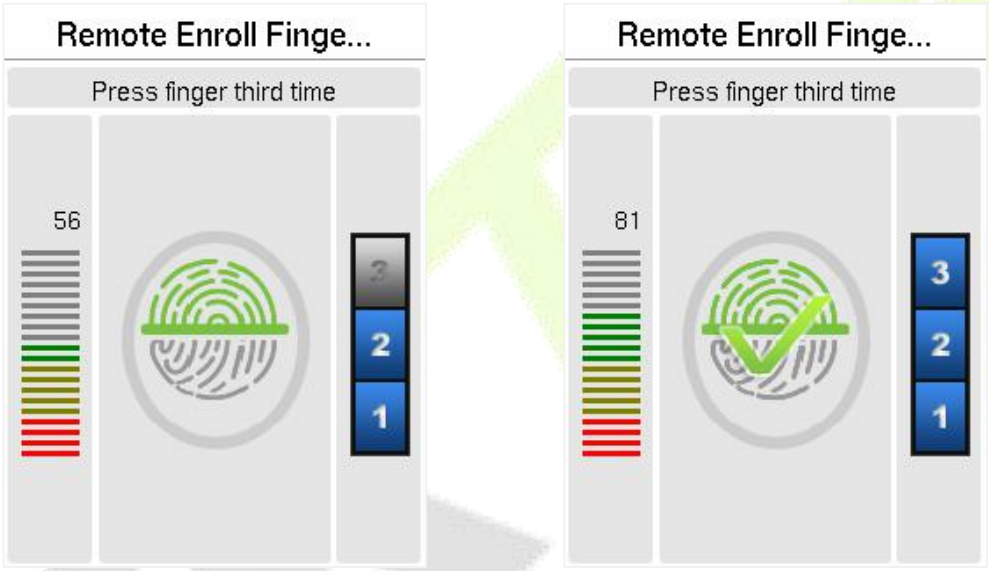
In this interface, you can register the User's Fingerprint, Face and Card Number. The verification mode can only be registered after the basic information is confirmed.



➢ Register Fingerprint

In the current interface, behind the fingerprint bar, click **Register**, and the device will display the fingerprint registration interface in real time, press your finger onto the fingerprint sensor of the device, and follow the instructions to complete the registration.

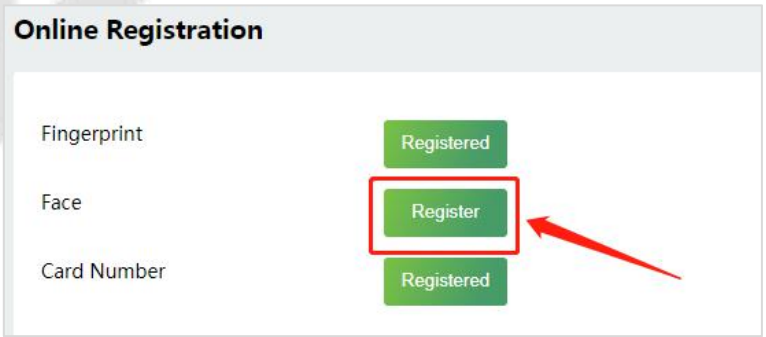




For fingerprint pressing operation, please refer to 1.4 Finger Placement.

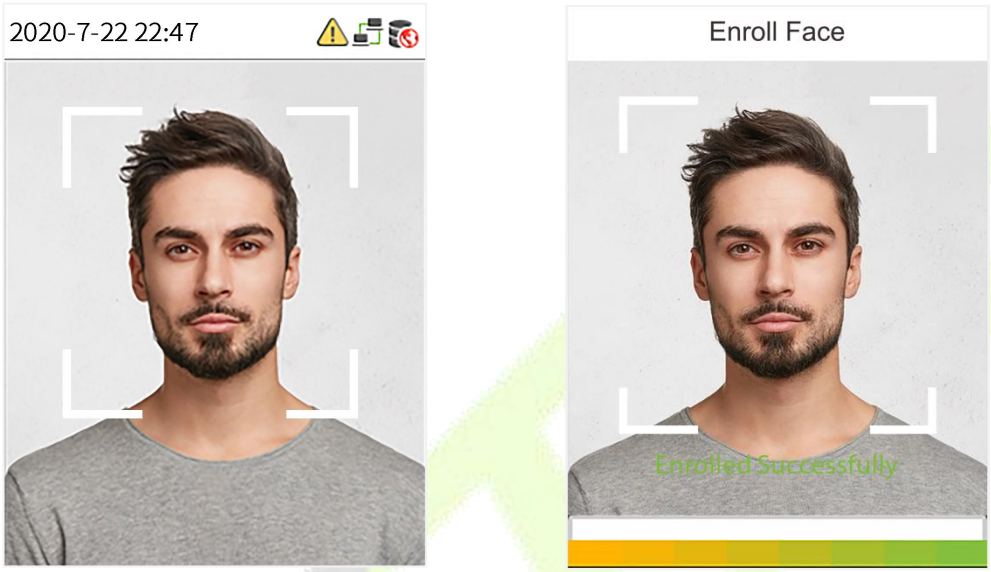
➢ Register Face

In the current interface, behind the face bar, click **Register**, and the device will display the face registration interface in real time.



- Please face towards the camera and position your face inside the white guiding box and stay still during face registration.
- A progress bar shows up while registering the face and "**Enrolled Successfully**" is displayed until the registration completes.
- If the face is registered already then, the "**Duplicated Face**" message shows up.

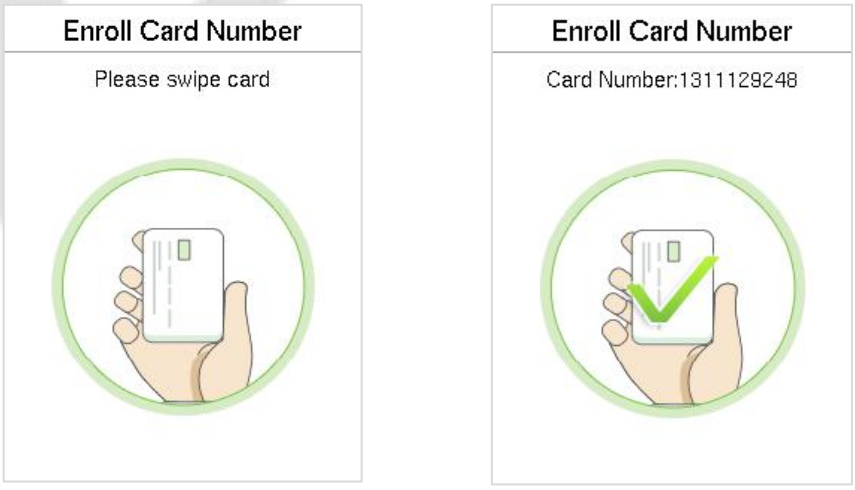
The registration interface is as follows:



Note: While registering a face, the system automatically captures a picture as the profile photo. If you do not register a profile photo, the system automatically sets the picture captured during registration as the default photo.

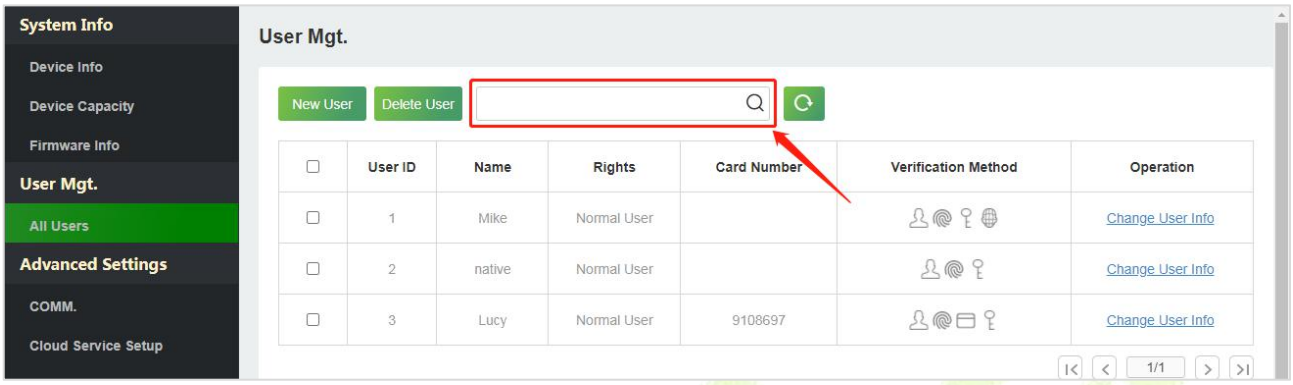
➢ Card Number

In the current interface, behind the card number, click **Register**, and the device will display the card registration interface in real time, swipe the card underneath the card reading area. The registration of the card will be successful.



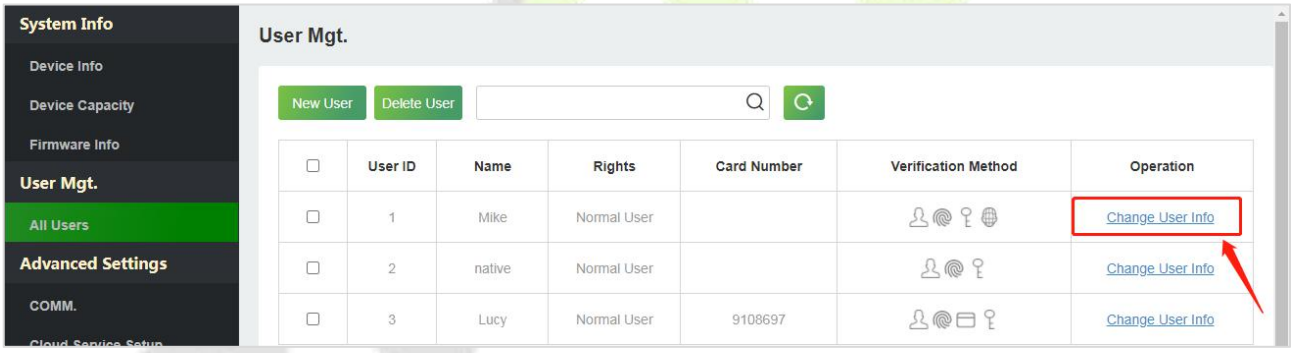
8.2 Search for Users

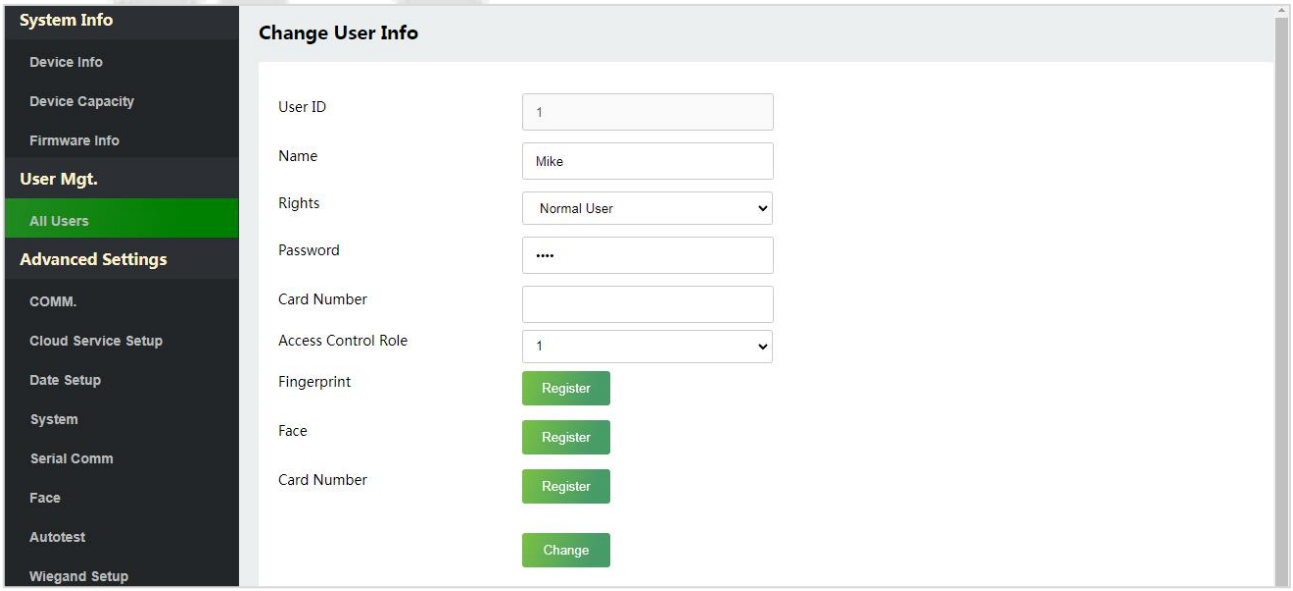
Click **All Users** on the WebServer, click the search bar to enter the required retrieval keyword (where the keyword may be the user ID, surname or full name) and the system will search for the related user information.



8.3 Edit User

On the **All Users** interface, select the required user from the list and click **Change User Info** to edit the user information.

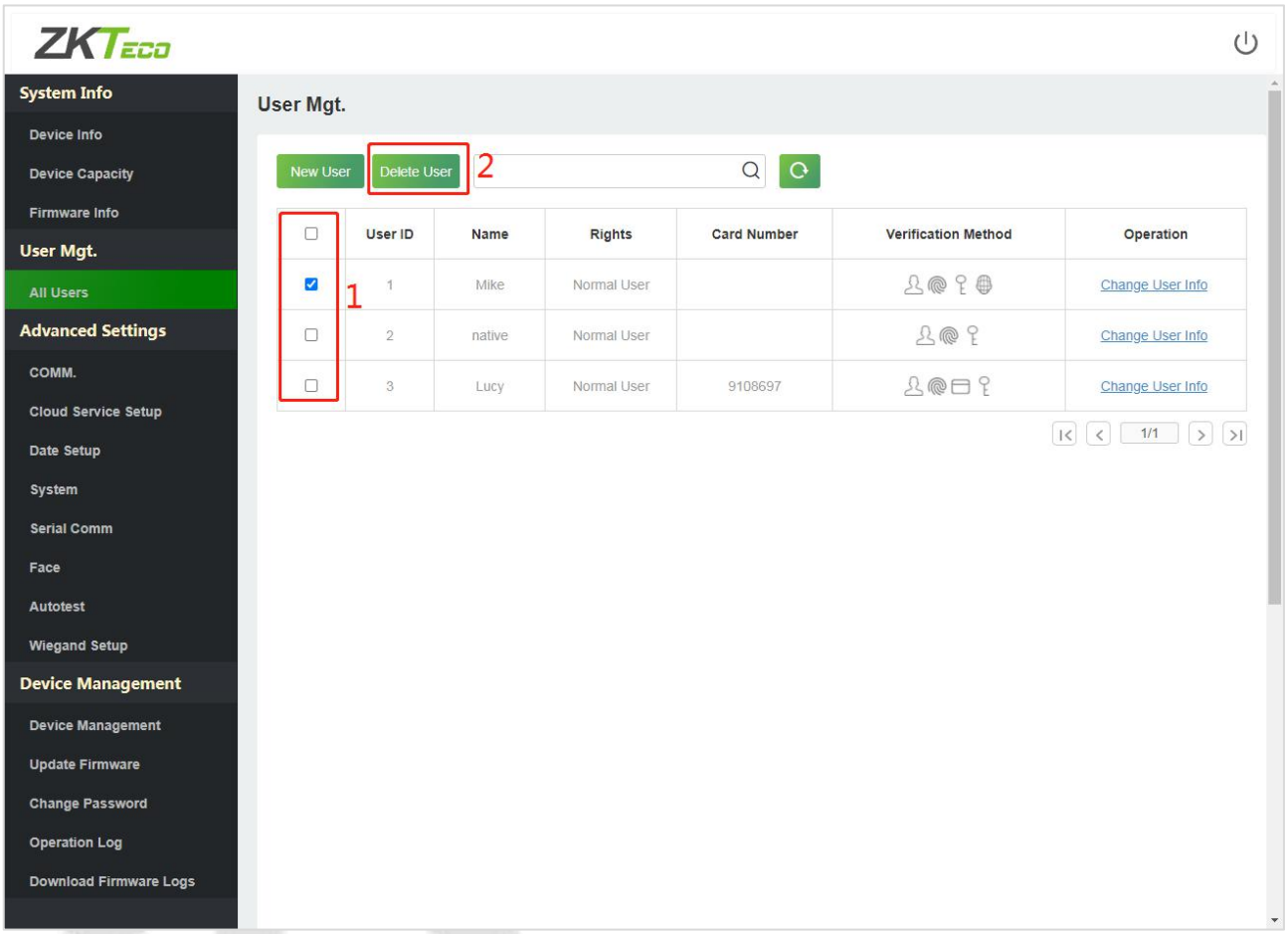




Note: The process of editing the user information is the same as that of adding a new user, except that the User ID cannot be modified. The process in detail refers to 8.1 User Registration.

8.4 Delete User

On the **All Users** interface, select the required user from the list and click **Delete User** to delete the user. Here individual deletion and batch deletion is available.

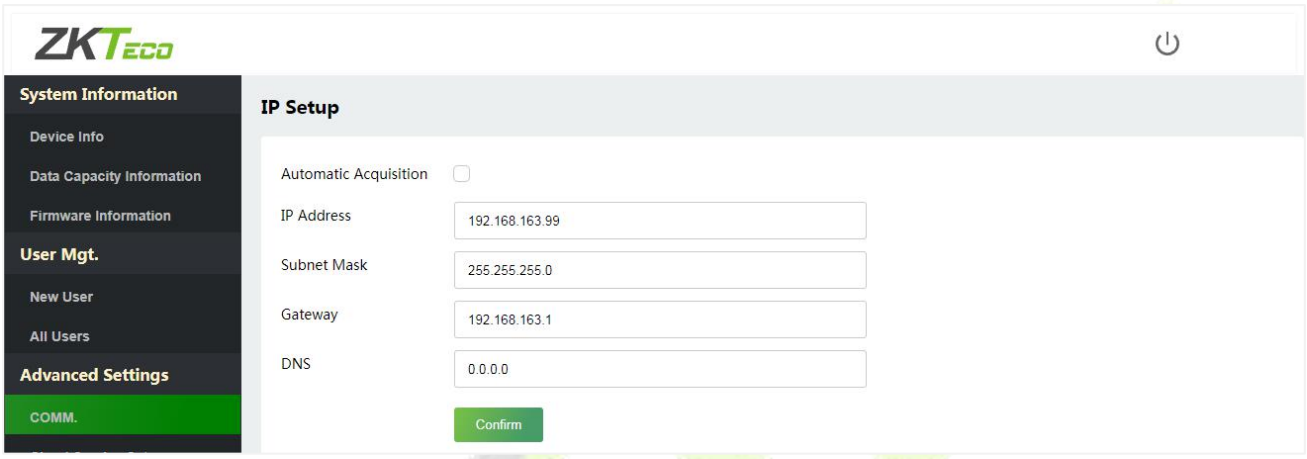


9 Advanced Settings

9.1 Communication Settings

Click **COMM.** on the WebServer.

Change the IP address of the device as needed, click **Confirm** to save, and the device will automatically synchronize the IP information.



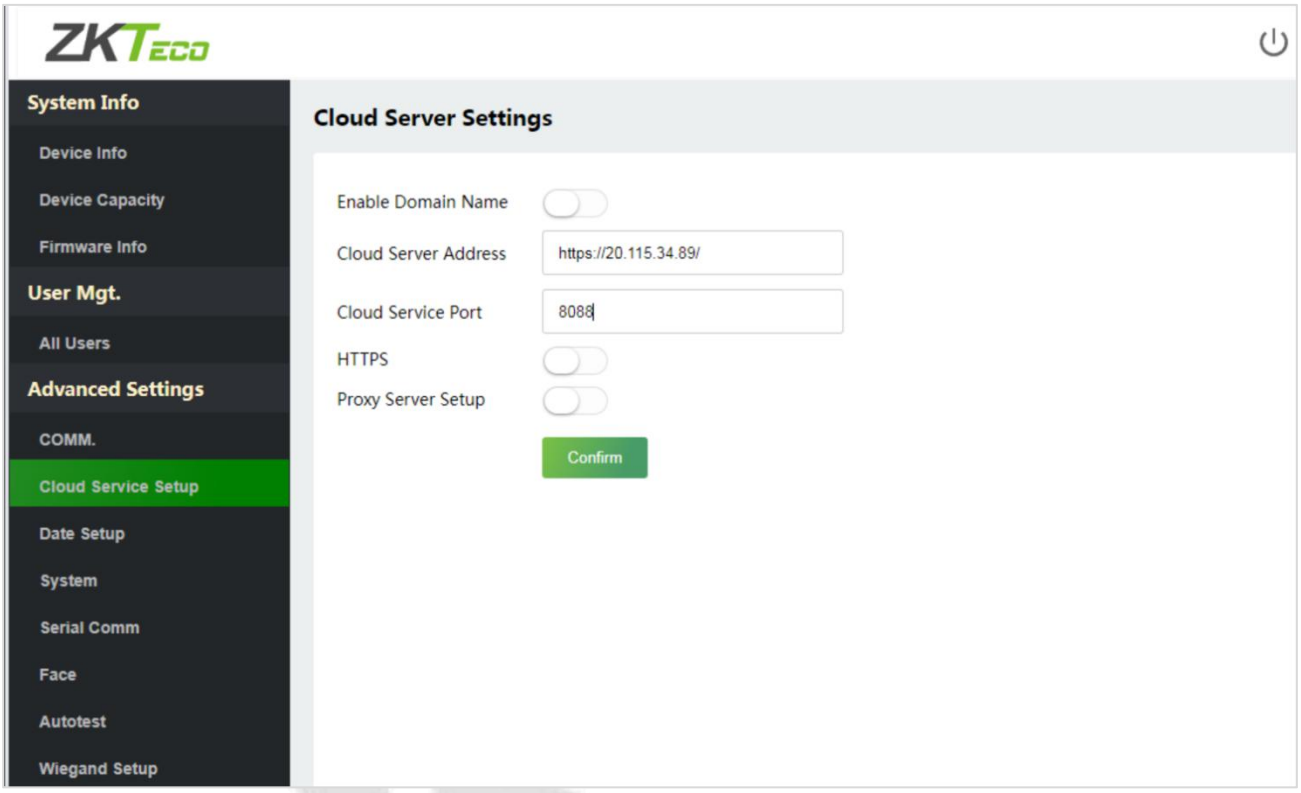
Function Name	Description
Automatic Acquisition	Select whether to obtain the IP Address by automatically.
IP Address	The default IP address is 192.168.1.201. It can be modified according to network availability.
Subnet Mask	The default Subnet Mask is 255.255.255.0. It can be modified according to network availability.
Gateway	The Default Gateway address is 0.0.0.0. It can be modified according to network availability.
DNS	The default DNS address is 0.0.0.0. It can be modified according to network availability.

Note: After the IP address of the device is changed successfully, you need to log out of the currently WebServer and log in again to the IP address you just changed to connect to the device. For WebServer login details, please refer to Login WebServer.

9.2 Cloud Server Setting

Click **Cloud Service Setup** on the WebServer.

Cloud Server Setup was used to connect to the ZKBio CVSecurity software, please refer to 12.1 Set the Communication Address.

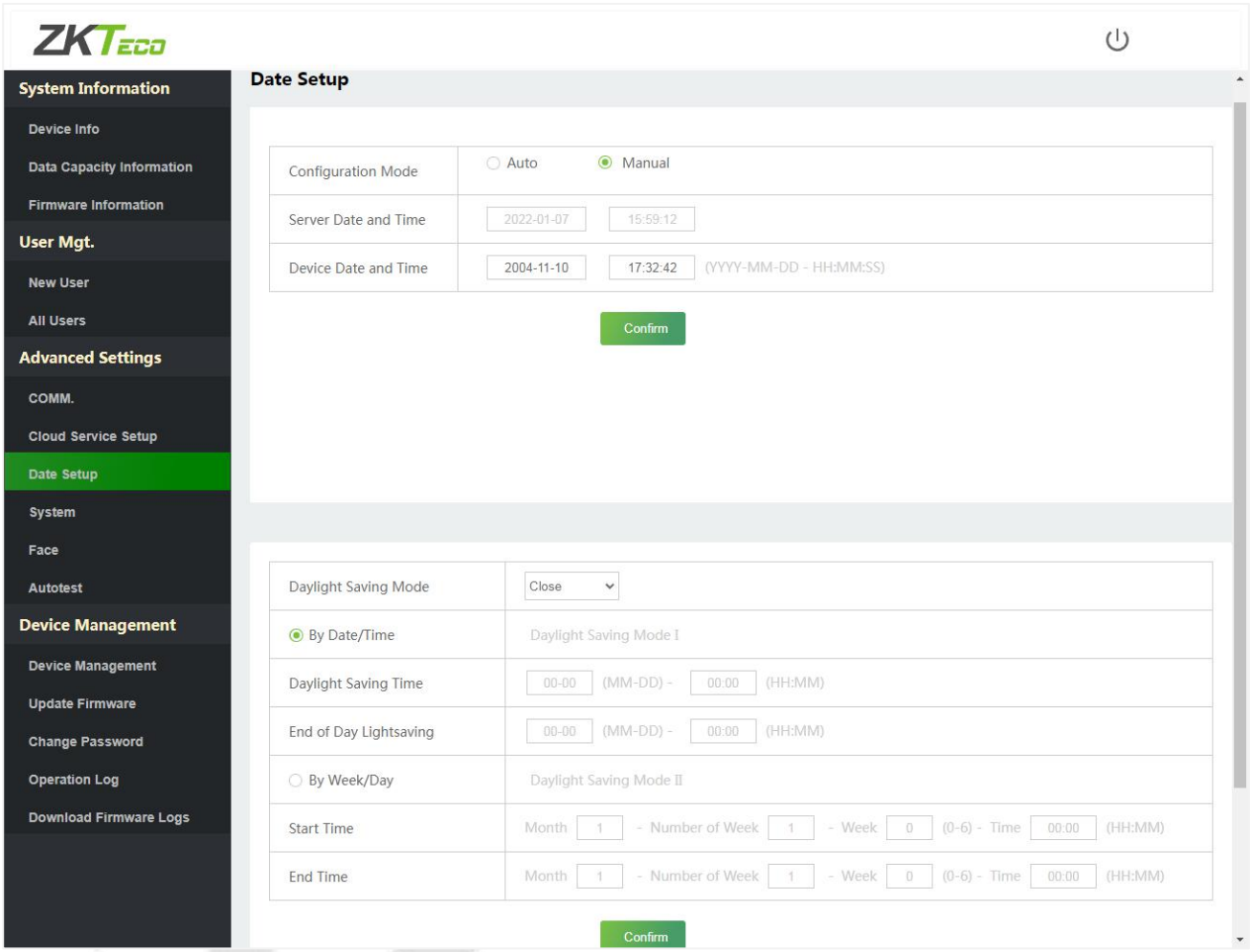


Function Name		Description
Enable Domain Name	**Server Address**	Once this function is enabled, the domain name mode "http://..." will be used, such as http://www.XYZ.com, while "XYZ" denotes the domain name (when this mode is turned **ON**).
Disable Domain Name	**Server Address**	IP address of the ADMS server.
	Server Port	Port used by the ADMS server.
HTTPS		Based on HTTP, transmission encryption and identity authentication ensure the security of the transmission process.
Enable Proxy Server Setup		When you choose to enable the proxy, you need to set the IP address and port number of the proxy server.

9.3 Date Setup

Click **Date Setup** on the WebServer.

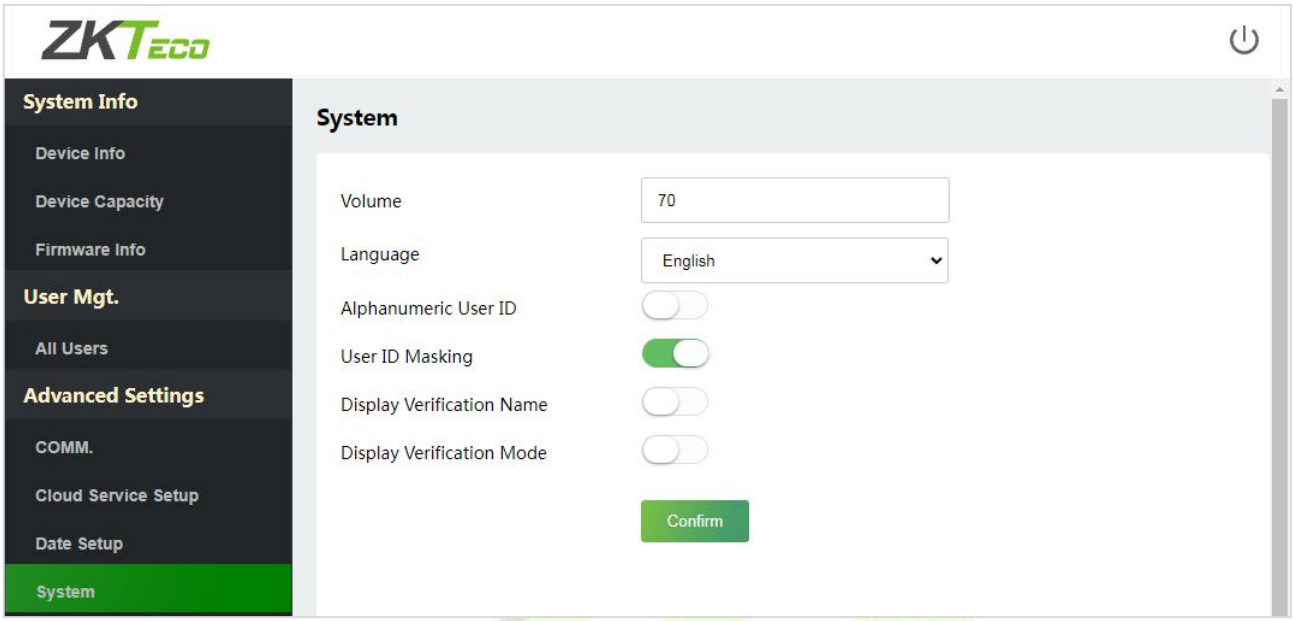
- Click **Manual** to manually set the date and time and click **Confirm** to save.
- Select Open or Close the **Daylight Saving Mode** function. If opened, set the **Daylight Saving Time** and **End of Daylight Saving**.



9.4 System Settings

Click **System** on the WebServer.

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



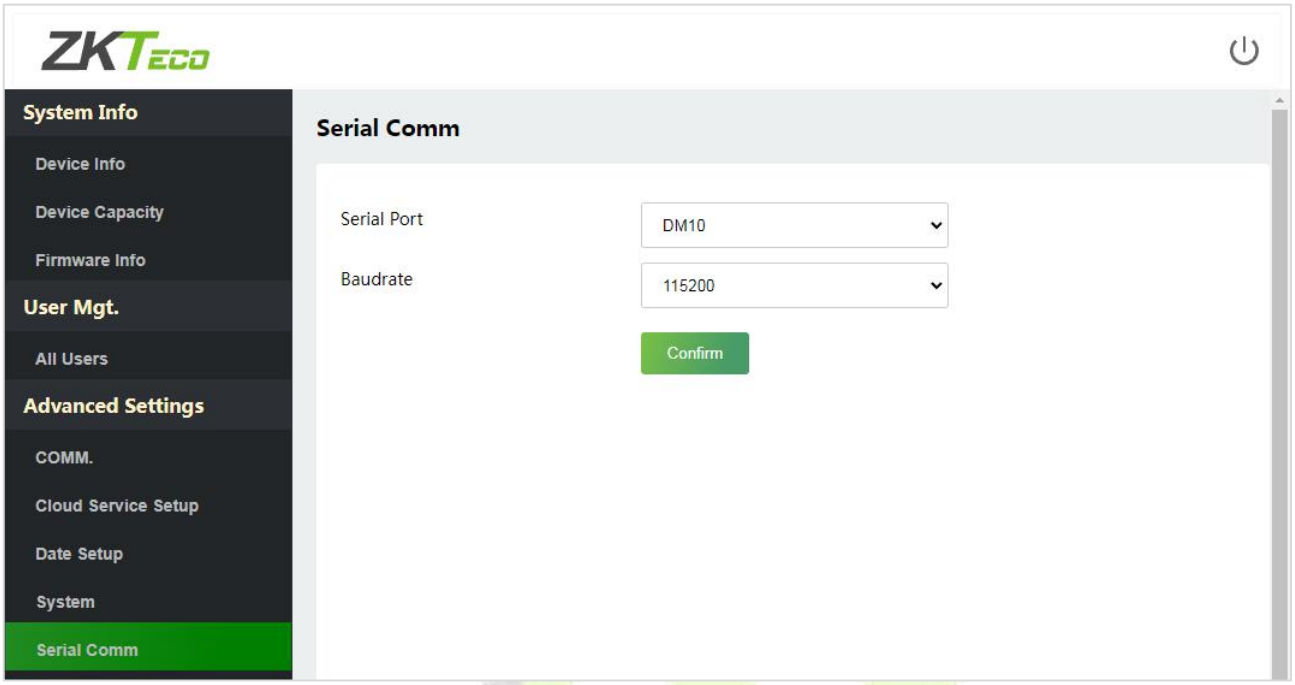
Function Name	Description
Volume	Adjust the volume of the device which can be set between 0 and 100.
Language	Select the language of the WebServer and device.
Alphanumeric User ID	Enable/Disable the alphanumeric as User ID.
User ID Masking	When enabled, and then the user is successfully compared and 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.

Note:

1. After selecting the language and clicking **Confirm**, the device will automatically reboot and display the changed language.
2. Then WebServer will not display the switched language until the device reboots and log in again.

9.5 Serial Comm

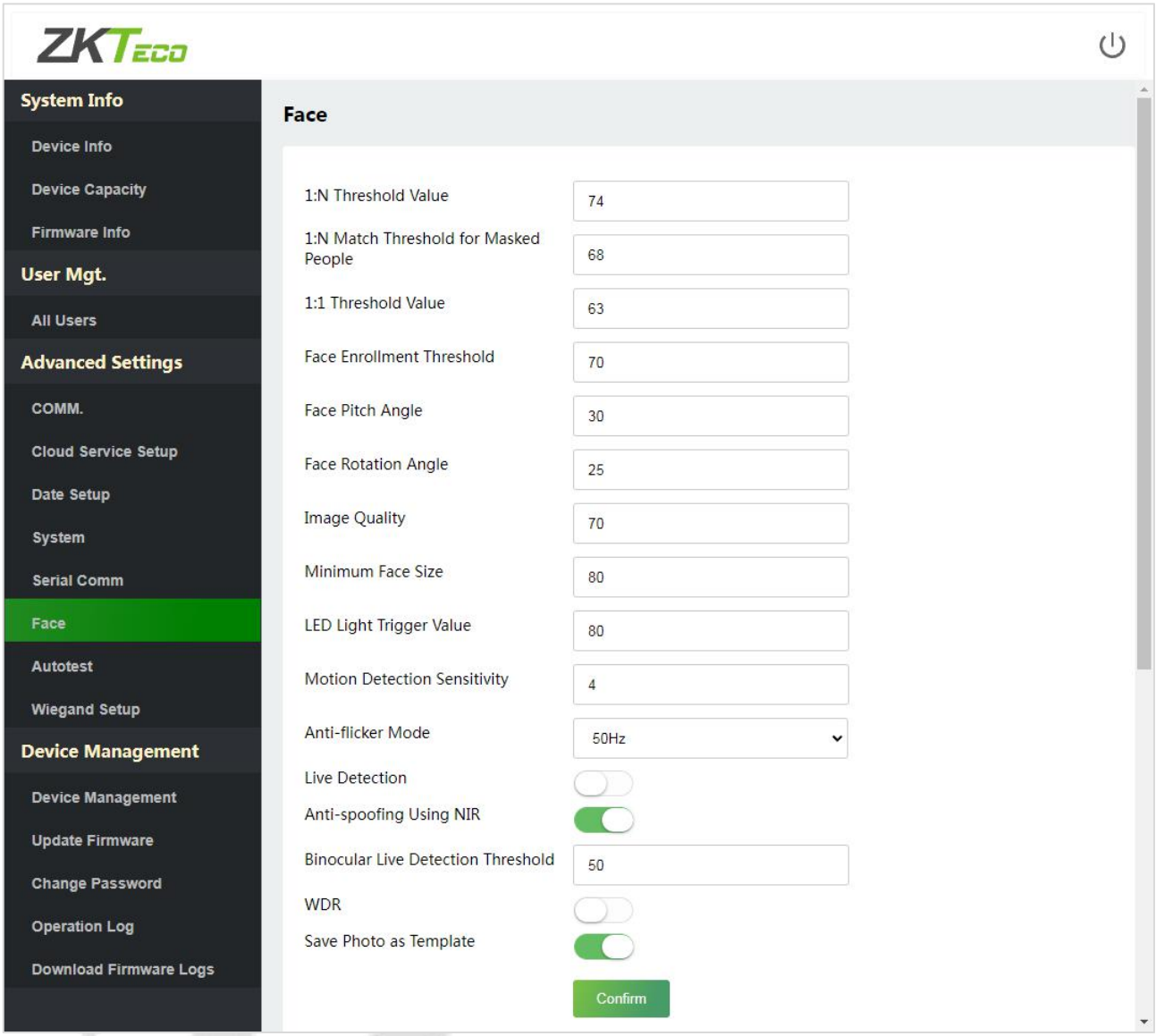
Click **Serial Comm** on the WebServer.



Function Name	Description
Serial Port	**No Using:** No communication with the device through the serial port. **RS485 (PC):** Communicate with the device through the RS485 serial port. **Master Unit:** When RS485 is used as the function of the "Master unit", it can be connected to a card reader. **DM10:** Communicate with the device through the DM10 serial port.
Baudrate	There are 5 baudrate options at which the data communicates with the PC. 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.

9.6 Face Parameters

Click **Face** on the WebServer.



Function Name	Description
1:N Threshold Value	Under face verification mode, the verification will only be successful when the similarity between the acquired facial image and all registered facial templates is greater than the set value. The valid value ranges from 0 to 100. The higher the thresholds, the lower the misjudgment rate, the higher the rejection rate, and vice versa. It is recommended to set the default value of 74.
1:N Match Threshold for Masked People	The higher the thresholds, the lower the misjudgment rate, the higher the rejection rate, and vice versa. It is recommended to set the default value of 68.

1:1 Threshold Value	Under 1:1 verification mode, the verification will only be successful when the similarity between the acquired facial image and the user's facial templates enrolled in the device is greater than the set value. The valid value ranges from 0 to 100. The higher the thresholds, the lower the misjudgment rate and the higher is the rejection rate, and vice versa. It is recommended to set the default value of 63.
Face Enrollment Threshold	During face enrolment, 1: N comparison is used to determine whether the user has already registered before. When the similarity between the acquired facial image and all registered facial templates is greater than this threshold, it indicates that the face has already been registered.
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 Rotation Angle	The 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.
Image Quality	Image quality for facial registration and comparison. The higher the value, the clearer the image requires.
Minimum Face Size	Required for facial registration and comparison. If the minimum size of the captured figure is smaller than this set value, then it will be filtered off and not recognized as a face. This value can be understood as the face comparison distance. The farther the person is, the smaller the face is, and the smaller the face pixel will be obtained by the algorithm. Therefore, adjusting this parameter can adjust the furthest comparison distance of faces. When the value is 0, the face comparison distance is not limited.
LED Light Triggered Value	This value controls the on and off of the LED light. The larger the value, the more frequently the LED light will be turned on.
Motion Detection Sensitivity	It is to set the value for the amount of change in a camera's field of view, which is known as potential motion detection that wakes up the terminal from standby to the comparison interface. The larger the value, the more sensitive the system would be, i.e. if a larger value is set, the comparison interface is much easier and the motion detection frequently triggered.

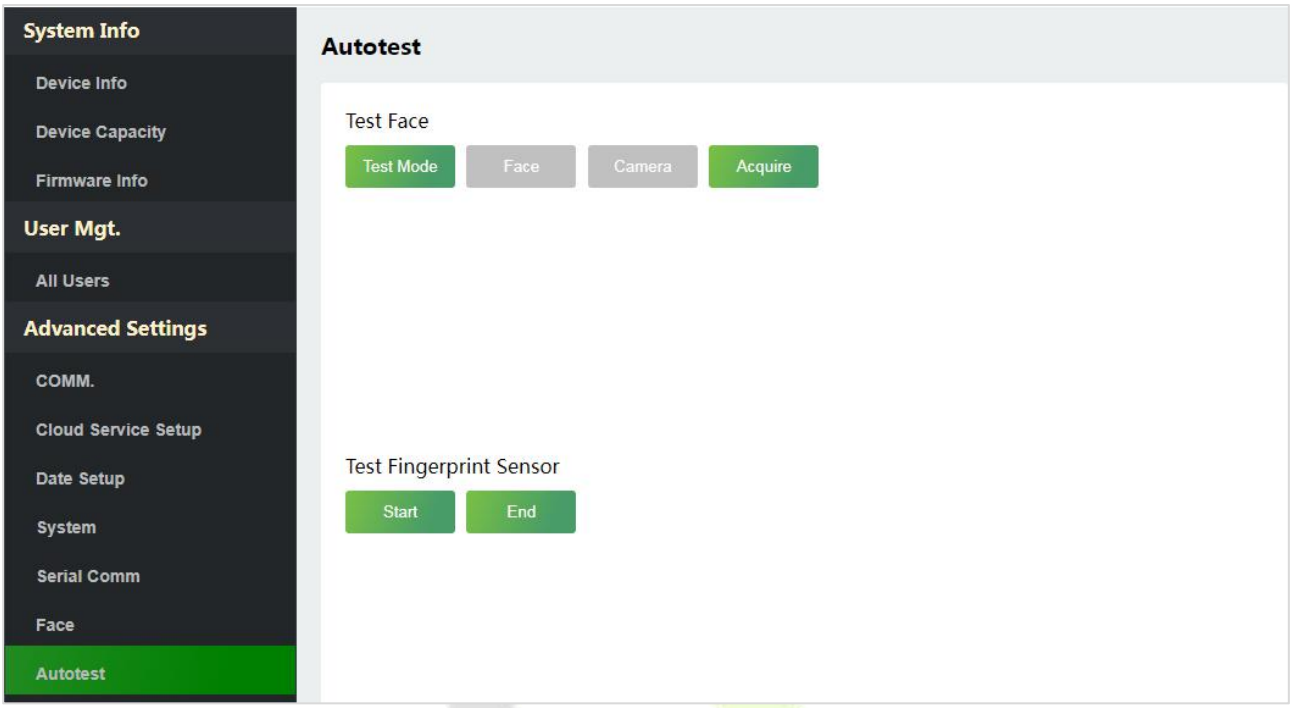
Anti-flicker Mode	Used when WDR is turned off. This helps reduce flicker when the device's screen flashes at the same frequency as the light.
Live Detection	Detecting the spoof attempt using visible light images to determine if the provided biometric source sample is really a person (a live human being) or a false representation.
Live Detection Threshold	Facilitates to judge whether the captured visible image is really a person (a live human being). The larger the value, the better the anti-spoofing performance using visible light.
Anti-spoofing Using NIR	Using near-infrared spectra imaging to identify and prevent fake photos and video attacks.
Binocular Live Detection Threshold	Facilitates to judge whether the captured visible image is really a person (a live human being). The larger the value, the better the anti-spoofing performance using visible light.
WDR	Wide Dynamic Range (WDR), which balances light and extends image visibility for surveillance videos under high contrast lighting scenes and improves object identification under bright and dark environments.
Save Photo as Template	Select whether to save the registered photo.

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

9.7 Autotest

Click **Autotest** on the WebServer.

It enables the system to automatically test whether the functions of various modules are working normally.



9.7.1 Test Face

Click **Test Mode**, the ProMA device will display the Test Face interface in real time, click **End of Testing** to exit the test.

After opening the test mode, the upper left corner of the device screen will display the value of the face in real time, the higher the value, the better quality of the face.

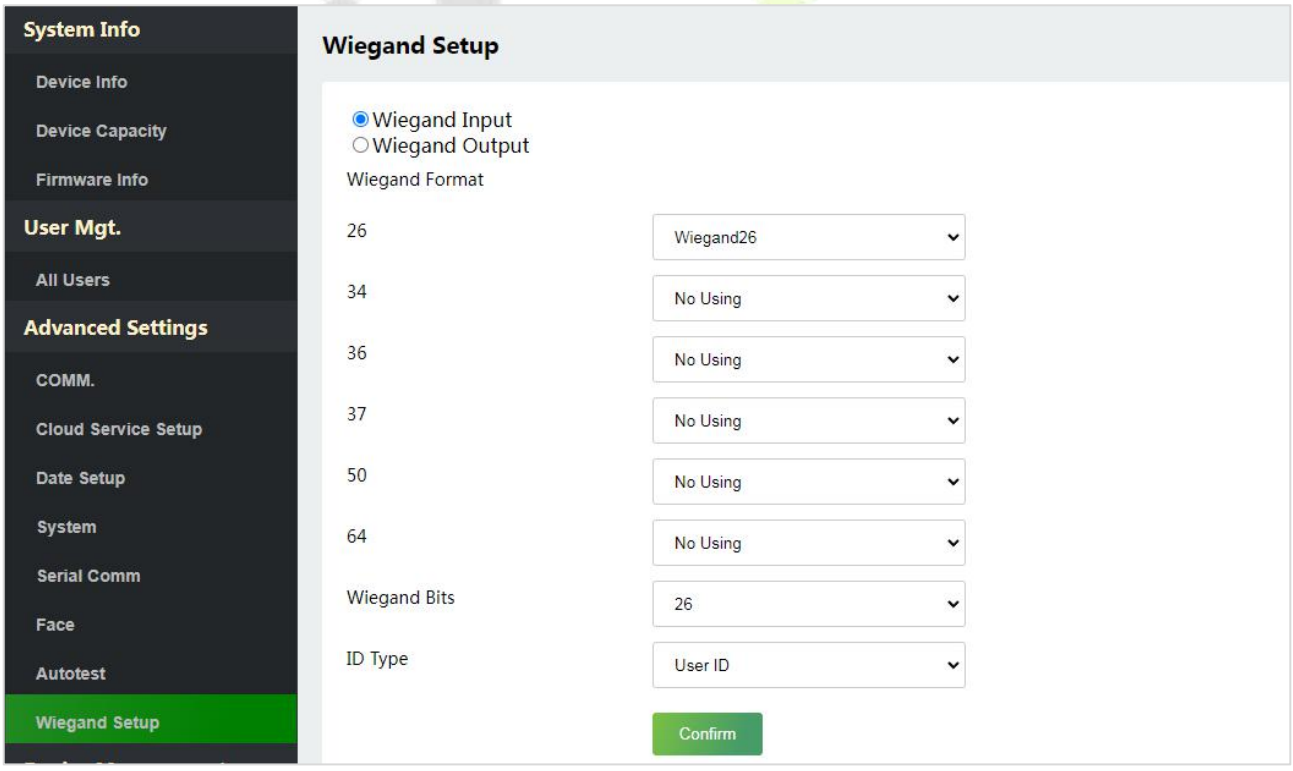
9.7.2 Test Fingerprint Sensor

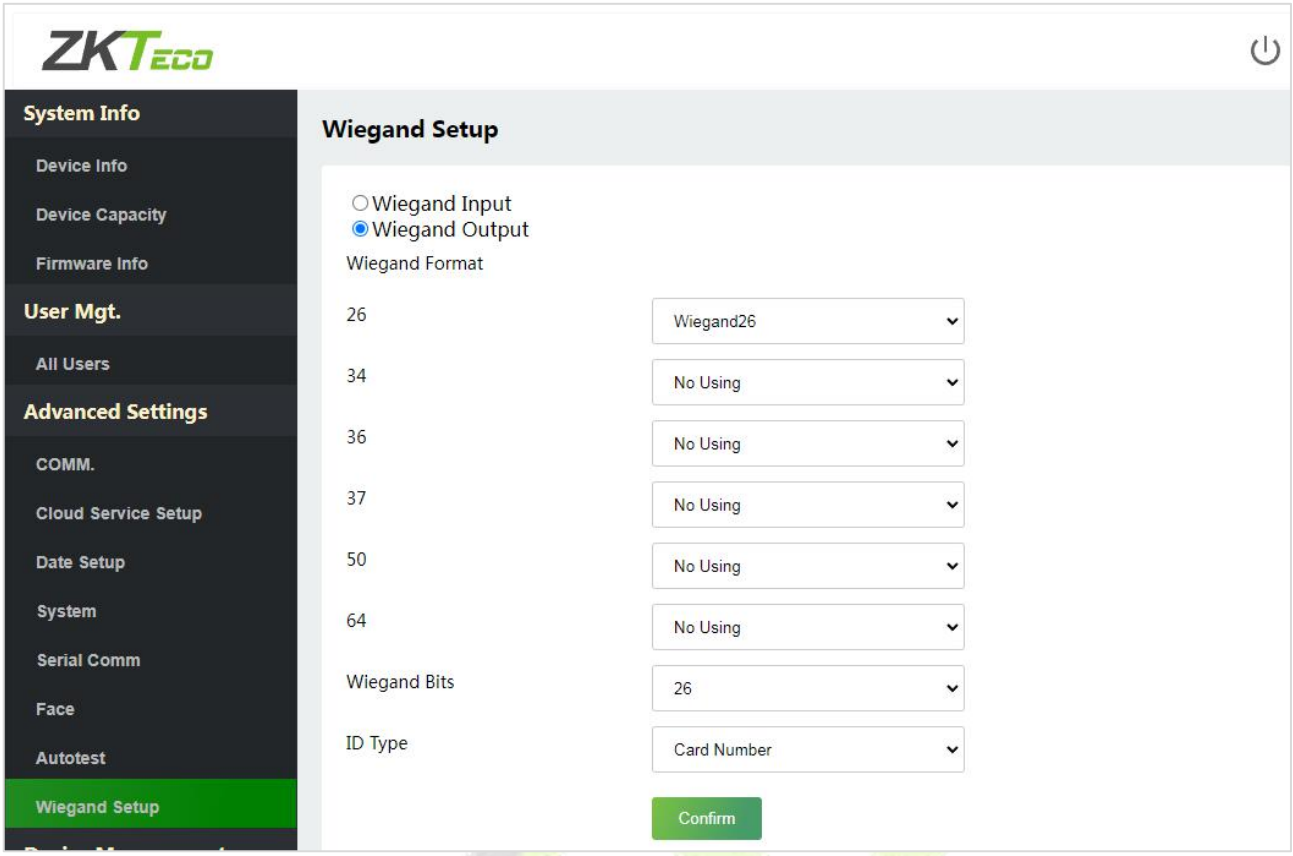
Click **Start**, the ProMA device will display the Test Fingerprint interface in real time, click **End** to exit the test.

9.8 Wiegand Setup

Click **Wiegand Setup** on the WebServer.

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



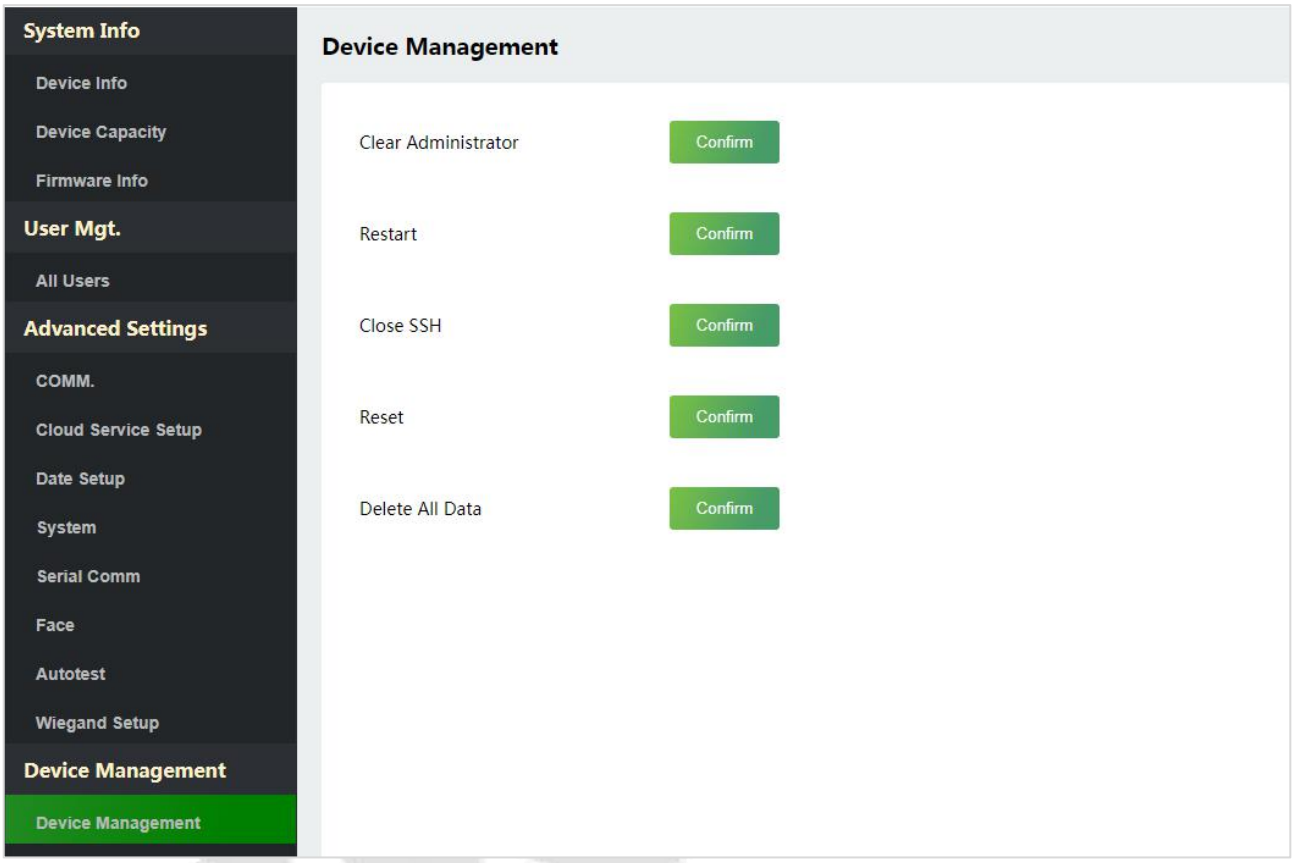


Function Name	Description
Wiegand Format	Its value can be 26 bits, 34 bits, 36 bits, 37 bits, 50 bits and 60 bits.
Wiegand Bits	The number of bits of the Wiegand data.
ID Type	Select between the User ID and card number.

10 Device Management

10.1 Device Management

Click **Device Management** on the WebServer.



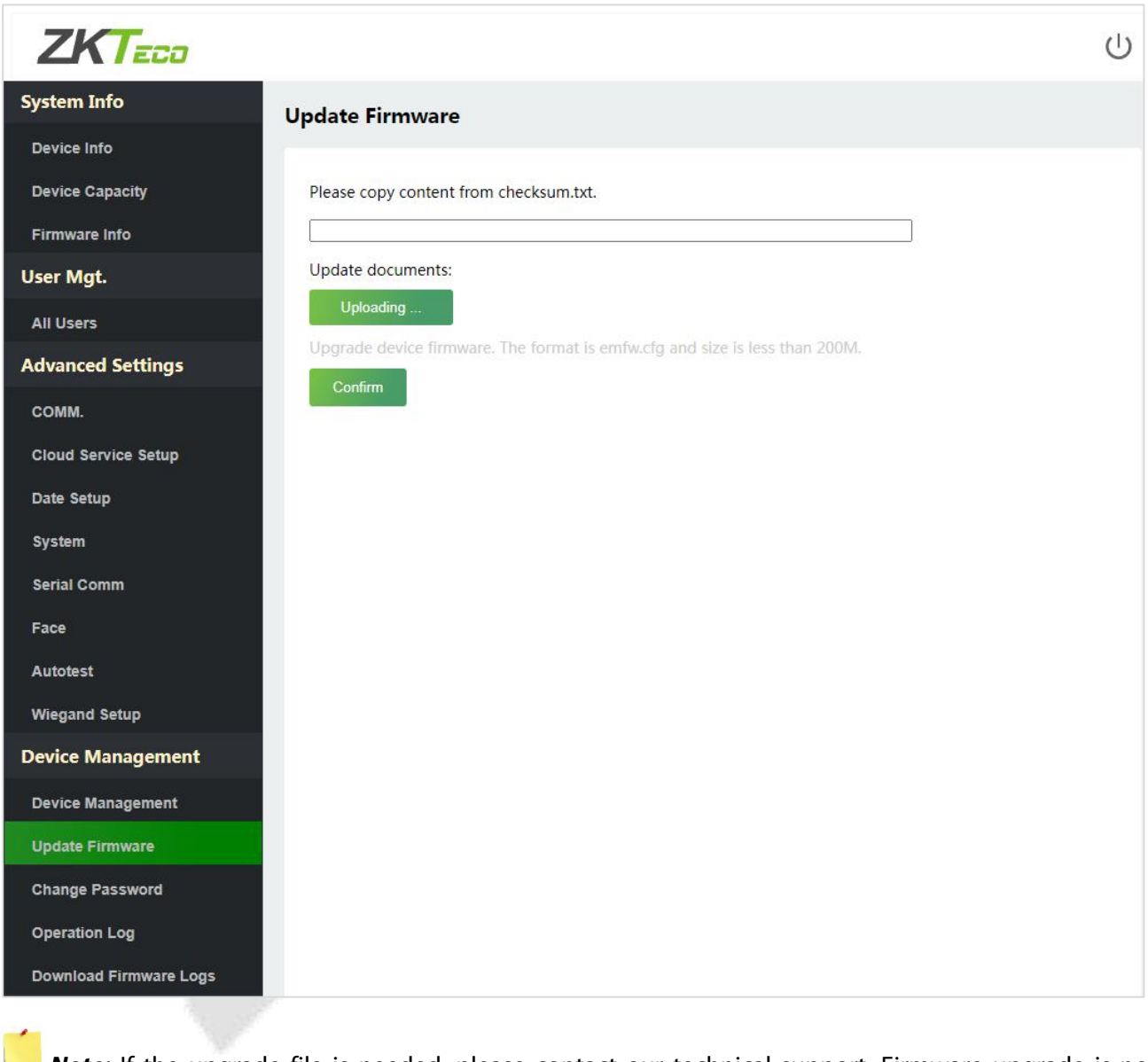
Function Name	Description
Clear Administrator	Choose whether to change the super administrator into a normal user.
Restart	Choose whether to restart the device.
Close SSH	SSH is used to enter the background of the device for maintenance, choose whether to close the SSH.
Reset	The Reset function restores the device settings such as communication and system settings to the default factory settings (this function does not clear registered user data). ***Note:*** After reset, the IP of the device is restored to the original 192.168.1.201, please refer to 9.1 Communication Settings to modify the IP.

Delete All Data	To delete the information and attendance logs/access records of all registered users.

10.2 Updata Firmware

Click **Updata Firmware** on the WebServer.

Select an upgrade file and click **Confirm** to complete firmware upgrade operation.

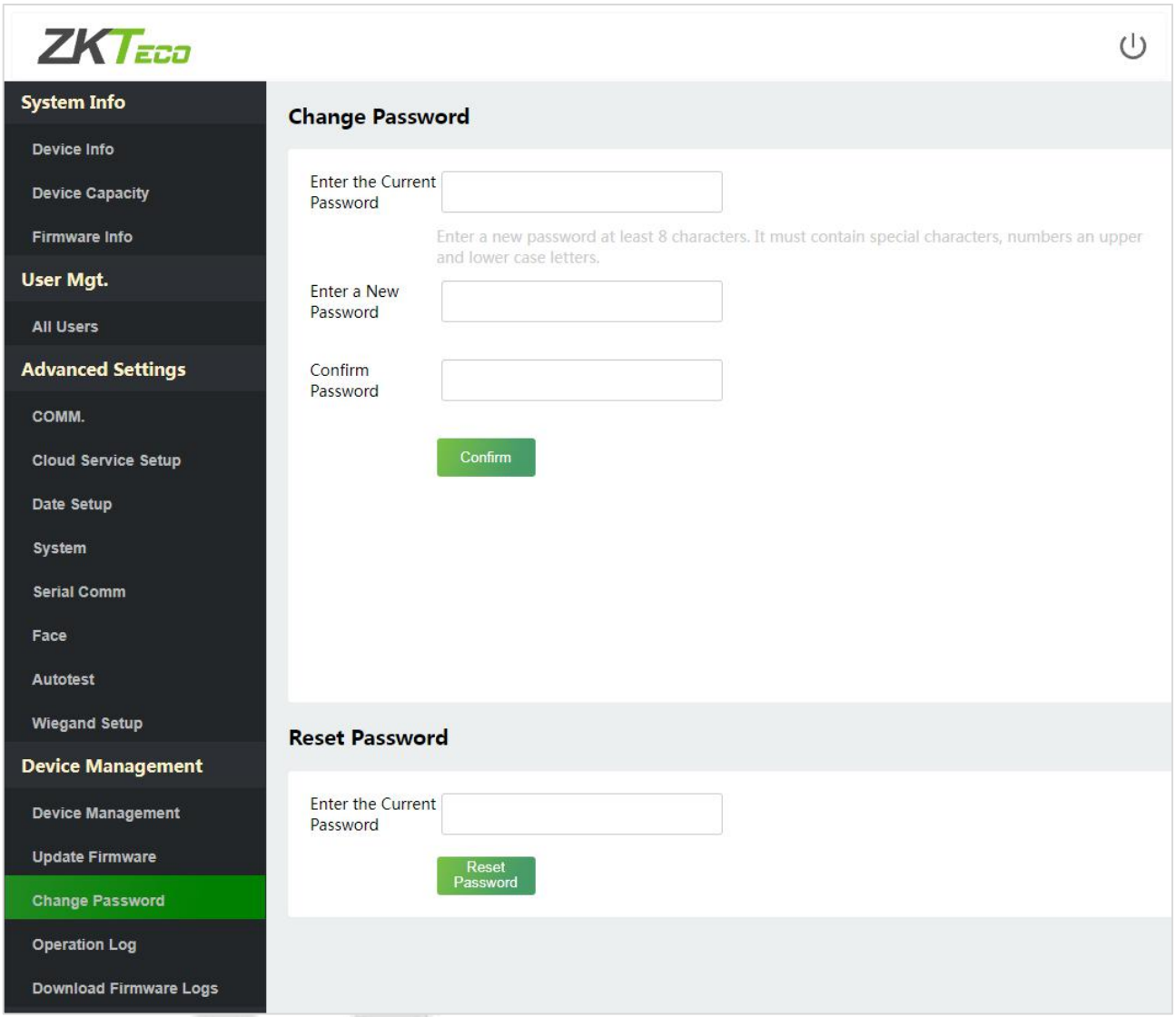


Note: If the upgrade file is needed, please contact our technical support. Firmware upgrade is not recommenced under normal circumstances.

10.3 Change Password

Click **Change Password** on the WebServer.

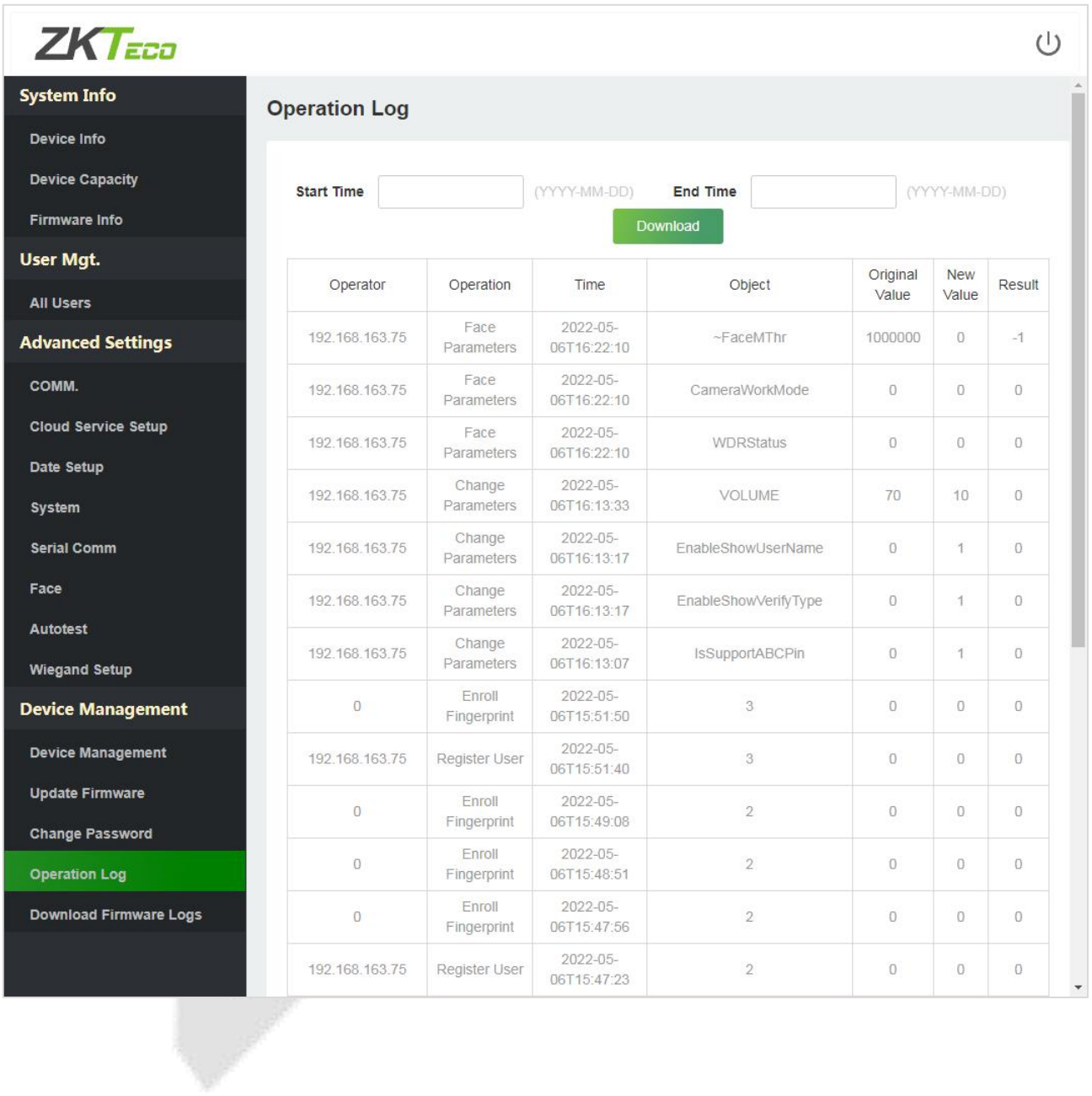
In this interface, you can change the password and reset the password of WebServer.



10.4 Operation Log

Click **Operation Log** on the WebServer.

All the user's operation records on the device or WebServer are saved. Users can search and download these logs by time.

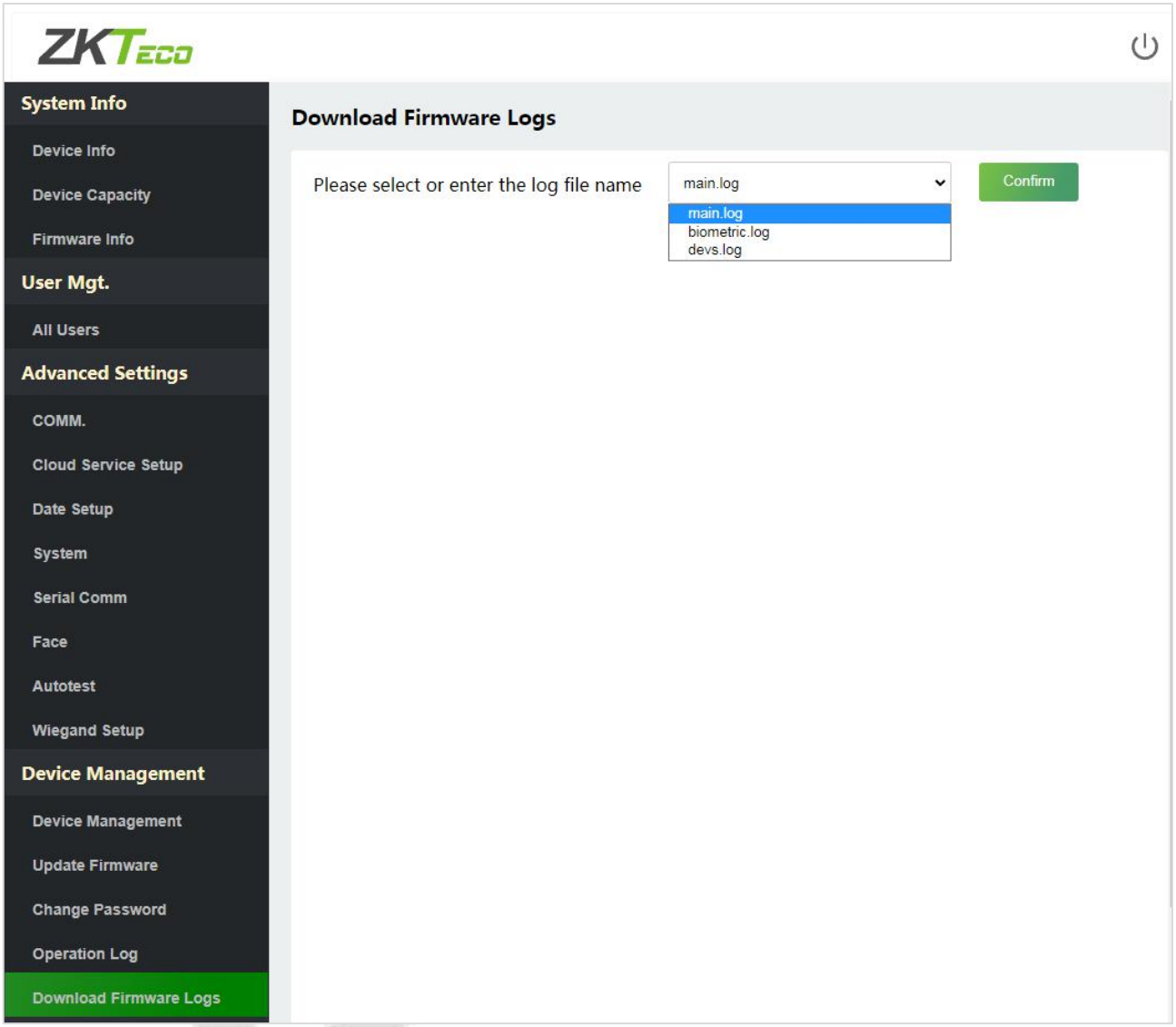


Operator	Operation	Time	Object	Original Value	New Value	Result
192.168.163.75	Face Parameters	2022-05-06T16:22:10	~FaceMThr	1000000	0	-1
192.168.163.75	Face Parameters	2022-05-06T16:22:10	CameraWorkMode	0	0	0
192.168.163.75	Face Parameters	2022-05-06T16:22:10	WDRStatus	0	0	0
192.168.163.75	Change Parameters	2022-05-06T16:13:33	VOLUME	70	10	0
192.168.163.75	Change Parameters	2022-05-06T16:13:17	EnableShowUserName	0	1	0
192.168.163.75	Change Parameters	2022-05-06T16:13:17	EnableShowVerifyType	0	1	0
192.168.163.75	Change Parameters	2022-05-06T16:13:07	IsSupportABCPin	0	1	0
0	Enroll Fingerprint	2022-05-06T15:51:50	3	0	0	0
192.168.163.75	Register User	2022-05-06T15:51:40	3	0	0	0
0	Enroll Fingerprint	2022-05-06T15:49:08	2	0	0	0
0	Enroll Fingerprint	2022-05-06T15:48:51	2	0	0	0
0	Enroll Fingerprint	2022-05-06T15:47:56	2	0	0	0
192.168.163.75	Register User	2022-05-06T15:47:23	2	0	0	0

10.5 Download Firmware Logs

Click **Operation Log** on the WebServer.

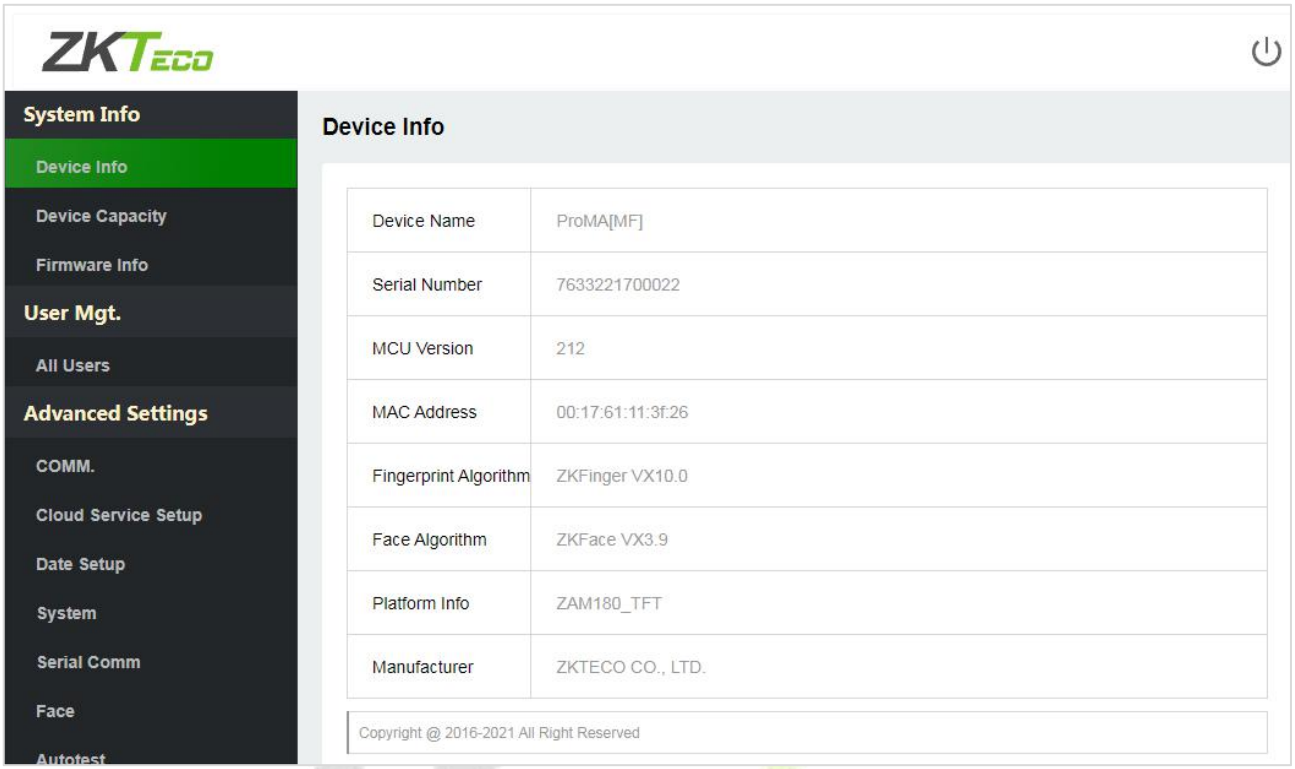
In this interface, you can select download the main, biometric, or dev.log.

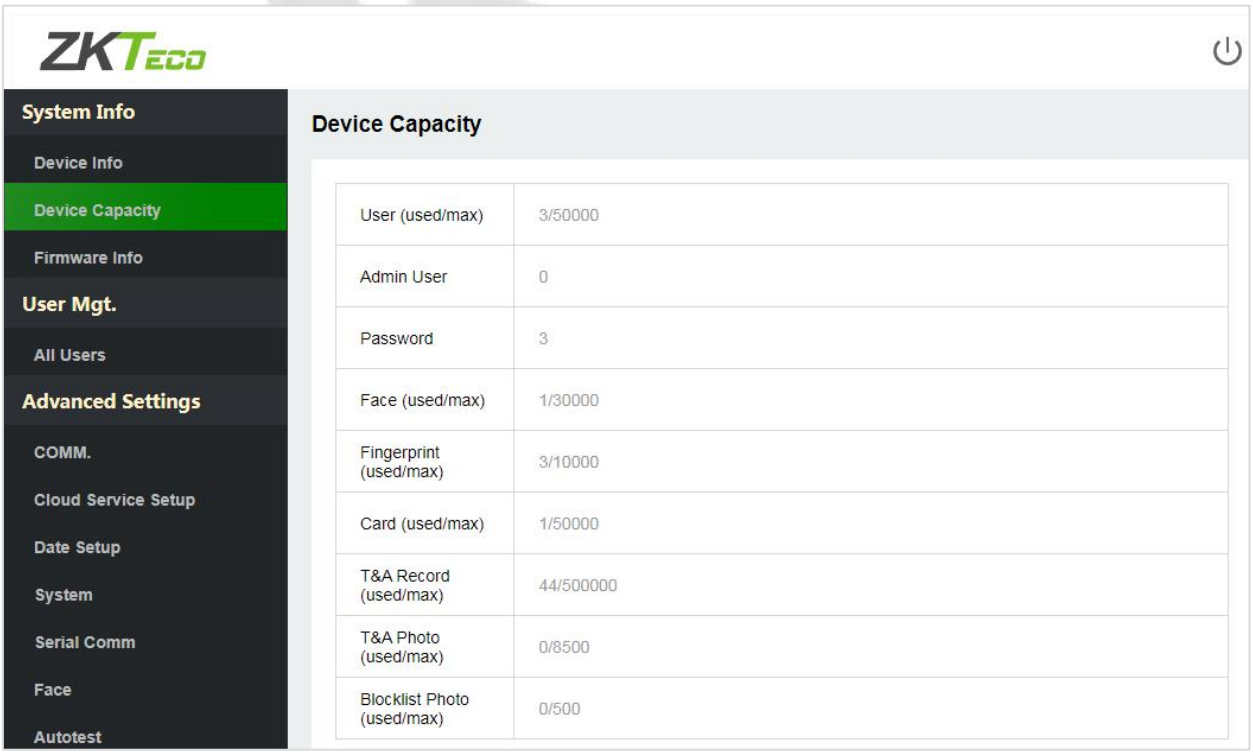


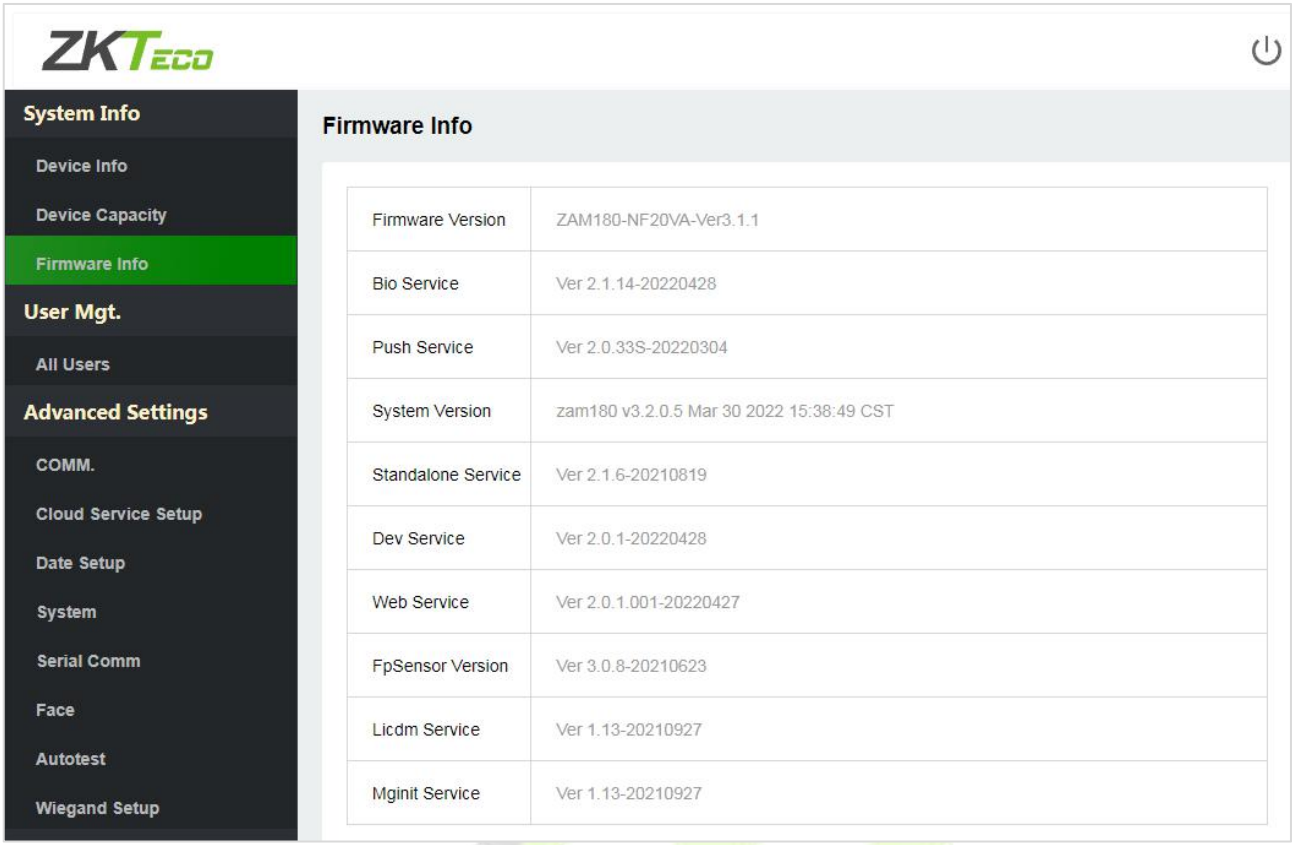
11 System Information

Click **System Information** on the WebServer.

In this interface, you can view the data capacity, device and firmware information of the current device.







Function Name	Description
Device Info	Displays the device's name, serial number, MCU version, MAC address, fingerprint and face algorithm version information, platform and manufacturer information.
Device Capacity	Displays the current device's user storage, password, fingerprint, card and face storage, administrators, attendance records, attendance and forbidden list photos.
Firmware Information	Displays the firmware version and other version information of the device.

12 Connect to ZKBio CVSecurity Software

12.1 Set the Communication Address

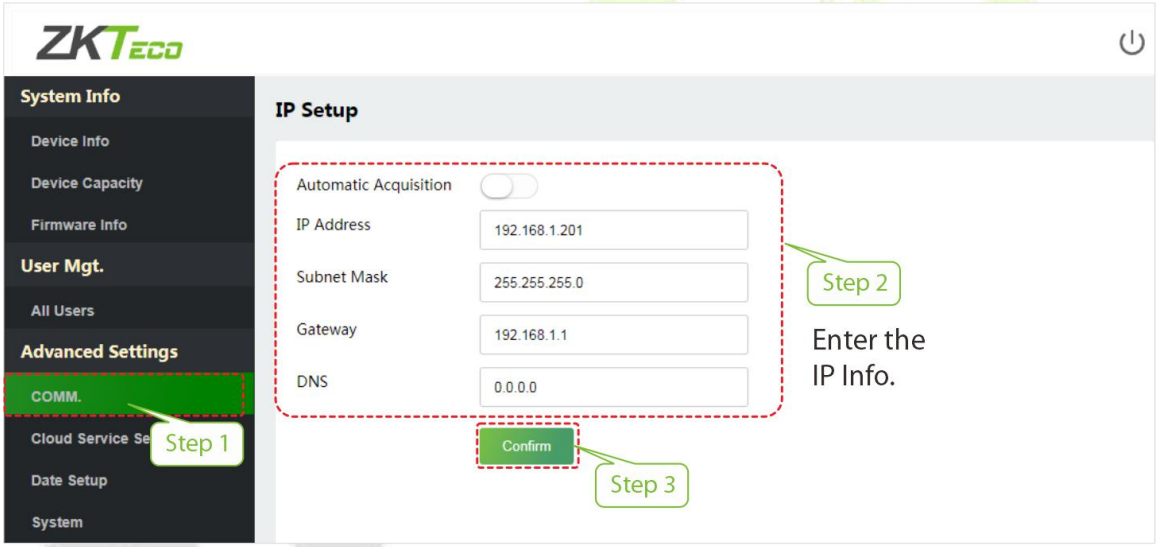
1. Click **COMM.** > **IP Setup** in the WebServer to set the IP address and gateway of the device.

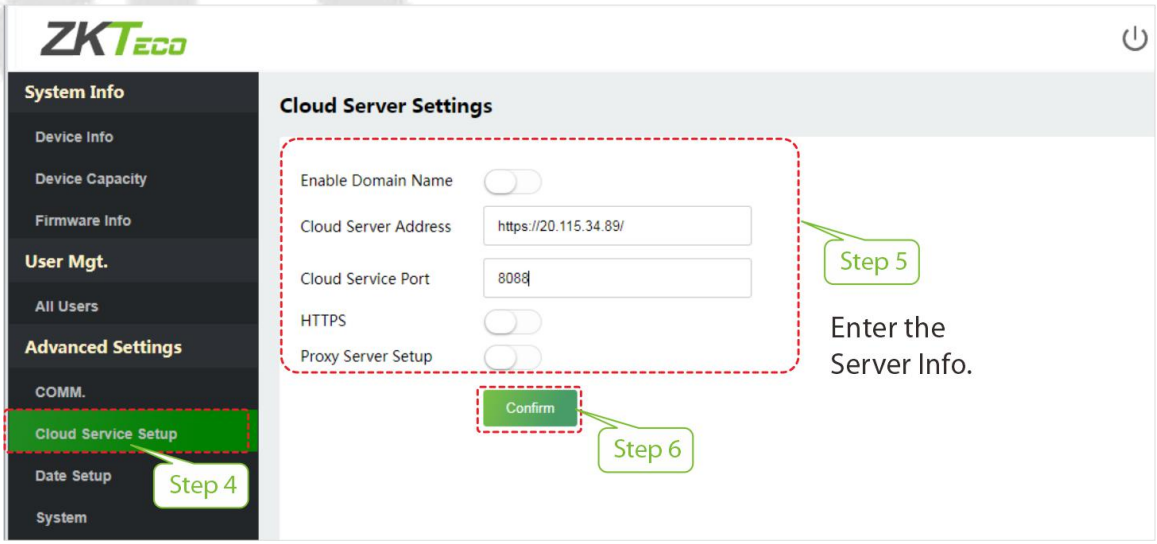
   (***Note:*** The IP address should be able to communicate with the ZKBio CVSecurity server, preferably in the same network segment with the server address)

2. In the WebServer, click **Cloud Server Setup** to set the server address and server port.

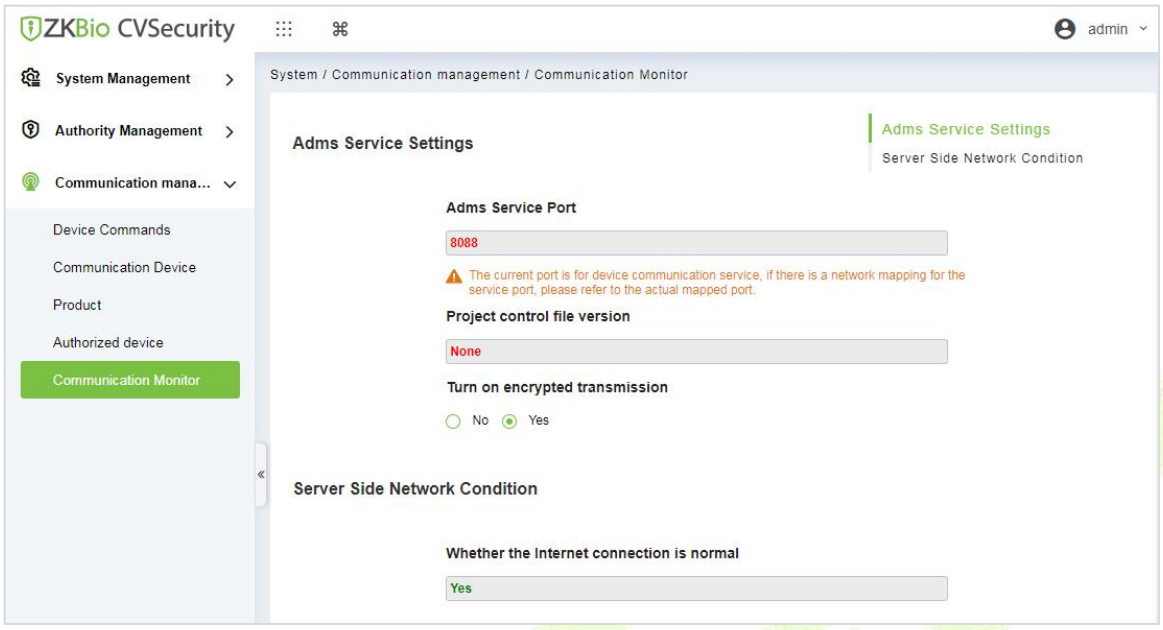
   Server address: Set the IP address as of ZKBio CVSecurity server.

   Server port: Set the server port as of ZKBio CVSecurity (The default is 8808).





3. Login to ZKBio CVSecurity software, click **System** > **Communication Management** > **Communication Monitor** to set the ADMS Service Port, as shown in the figure below:



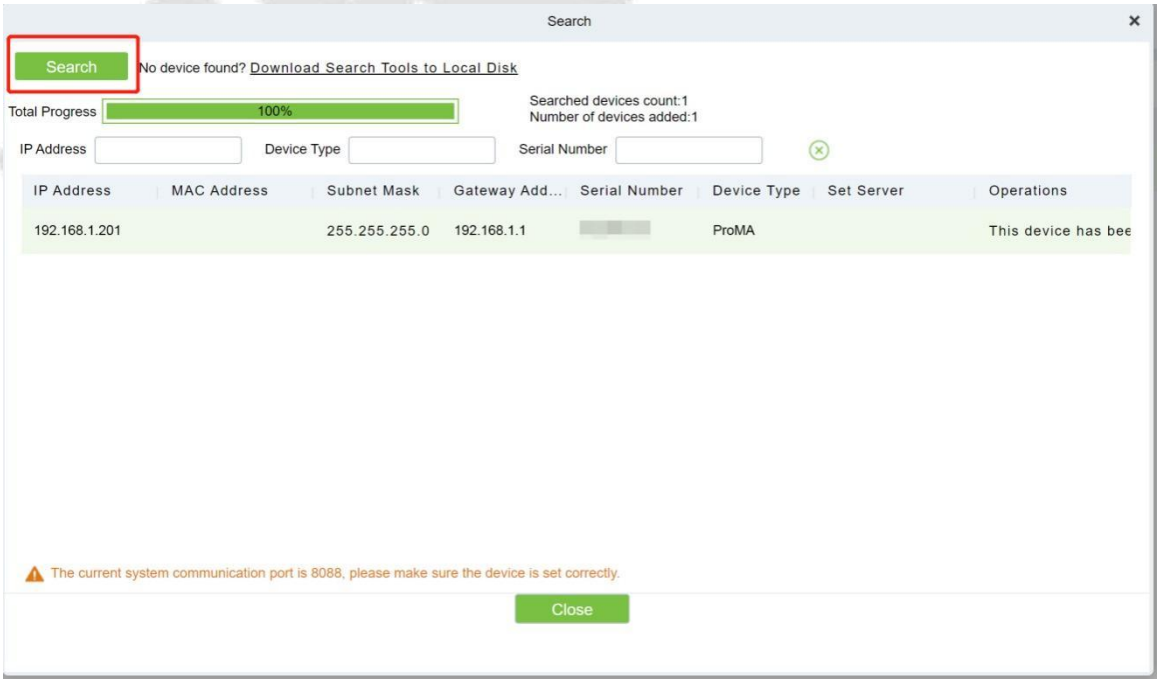
12.2 Add Device on the Software

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

1）Click **Access** > **Device** > **Search**, to open the Search interface in the software.

2）Click **Search**, and it will prompt **Searching**…….

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

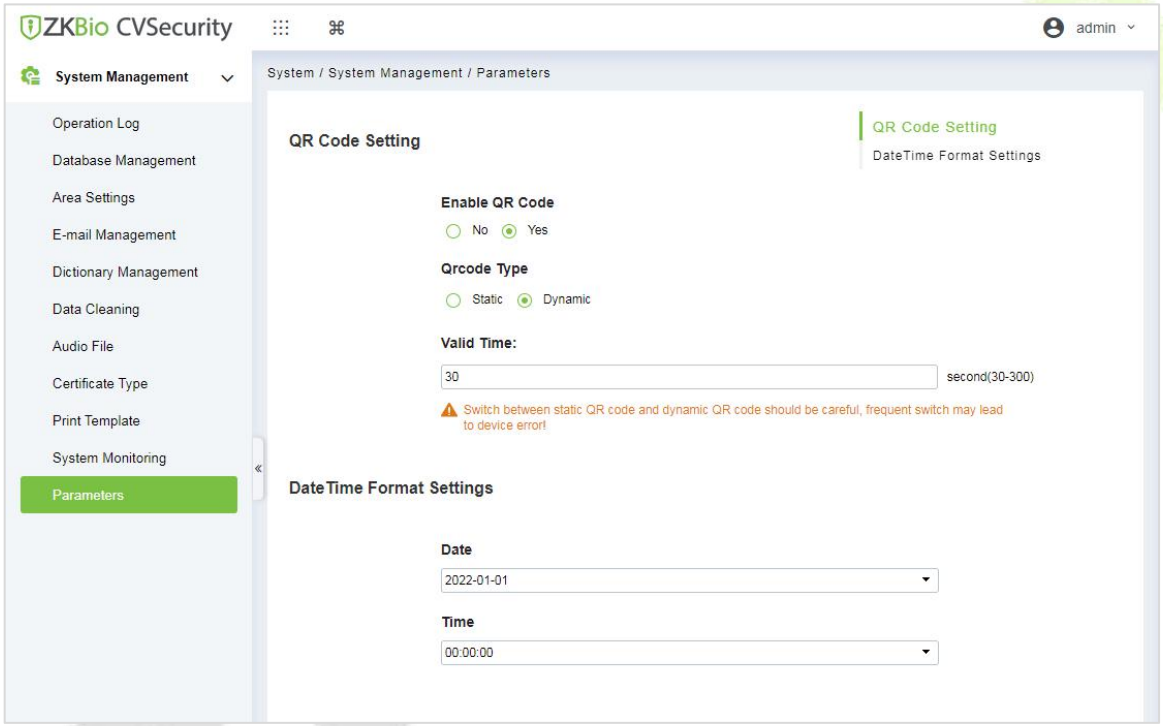


Click **Add** in operation column, a new window will pop-up. Select Icon type, Area, and Add to Level from each dropdown and click **OK** to add the device.

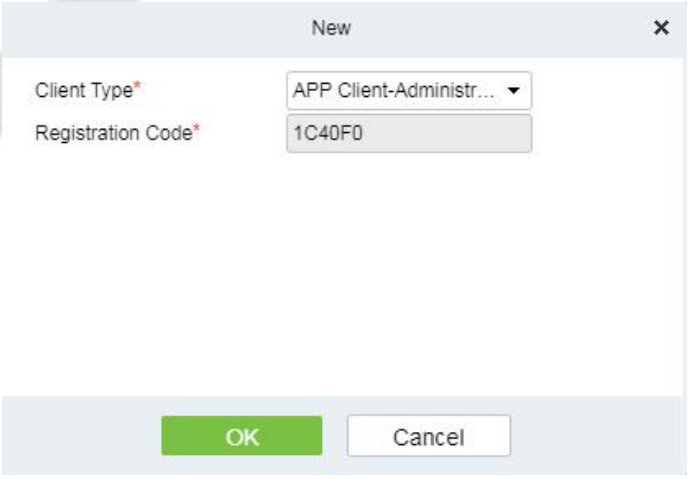
12.3 Mobile Credential ★

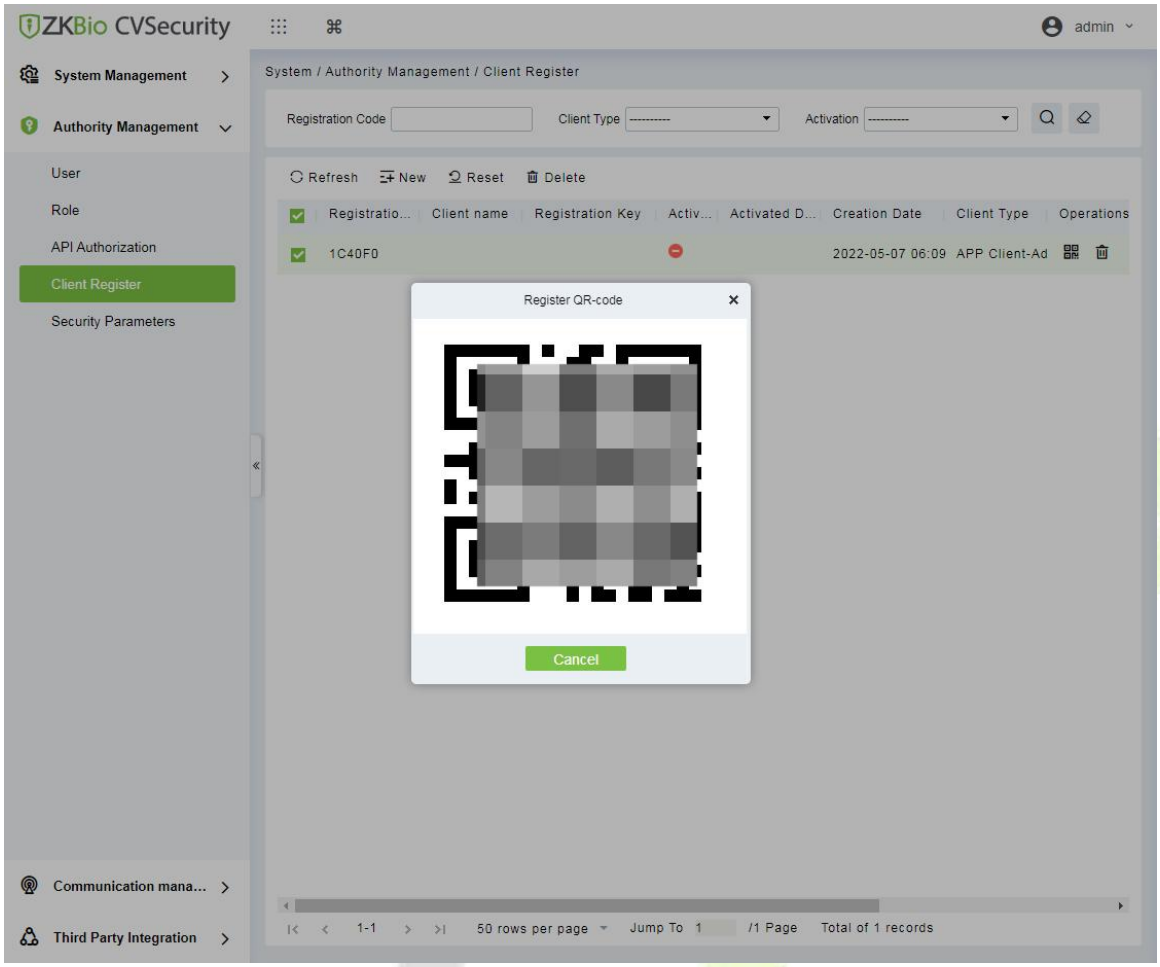
After downloading and installing the App, the user needs to set the Server before login. The steps are given below:

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

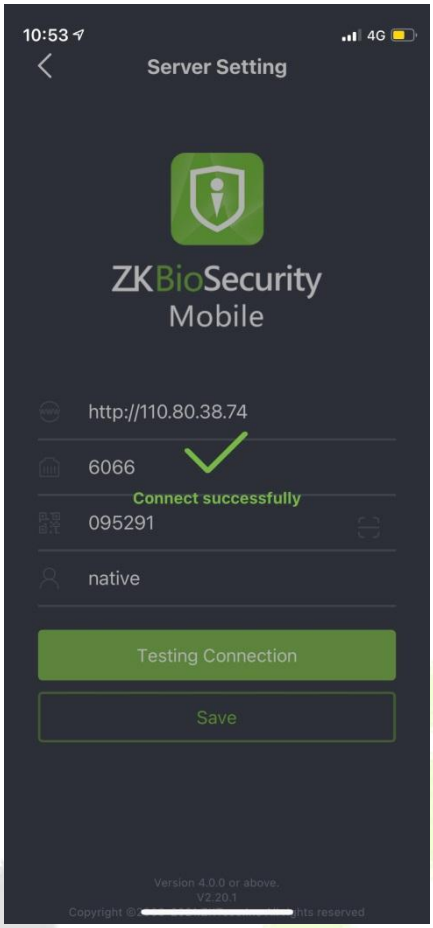


2. On the Server, choose **System** > **Authority Management** > **Client Register** to add a registered App client.





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

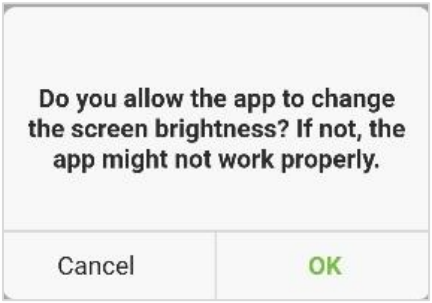


The Mobile Credential function is only valid when logging in as an employee, tap on Employee to switch to Employee Login screen. Enter the Employee ID and Password (Default: 123456) to login.

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

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

When using this function for the first time, the App will prompt to authorize the modification of screen brightness settings, as shown in the figure:



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

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

Appendix 1

Requirements of Live Collection and Registration of Visible Light Face Images

1) It is recommended to perform registration in an indoor environment with an appropriate light source without underexposure or overexposure.

2) Do not shoot towards outdoor light sources like door or window or other strong light sources.

3) Dark-color apparels which are different from the background color are recommended for registration.

4) Please show your face and forehead, and do not cover your face and eyebrows with your hair.

5) The digital photo should be straight-edged, colored, and half-portrayed with only one person, and the person should be uncharted and casual. Persons who wear eyeglasses should remain to put on eyeglasses for photo-taking.

6) Do not wear accessories like scarf or mask that may cover your mouth or chin.

7) Please face right towards the capturing device, and locate your face in the image capturing area as shown in Image 1.

8) Do not include more than one face in the capturing area.

9) 50cm - 80cm is recommended for capturing distance adjustable subject to body height.

Image1 Face Capture Area

Requirements for Visible Light Digital Face Image Data

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

- **Eye Distance**

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

- **Facial Expression**

Neutral face or smile with eyes naturally open are recommended.

- **Gesture and Angel**

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

- **Accessories**

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

- **Face**

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

- **Image Format**

Should be in BMP, JPG or JPEG.

- **Data Requirement**

Should comply with the following requirements:

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

Appendix 2

Privacy Policy

Notice:

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

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

I. Collected Information

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

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

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

II. Product Security and Management

1. When you use our products for the first time, you shall set the Administrator privilege before performing specific operations. Otherwise, you will be frequently reminded to set the Administrator privilege when you enter the main menu interface. **If you still do not set the**

Administrator privilege after receiving the system prompt, you should be aware of the possible security risk (for example, the data may be manually modified).

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

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

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

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

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

III. Others

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

Eco-friendly Operation

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

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

Hazardous or Toxic substances and their quantities

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

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

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

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

www.zkteco.eu