User Manual

SpeedFace M4 (ZAM210)

Date: September 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 manufacturers of RFID and Biometric (Fingerprint, Facial, and 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 **SpeedFace M4 (ZAM210)**.

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

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

Document Conventions

Conventions used in this manual are listed below:

GUI Conventions

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

Symbols

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

Table of Contents

Data Security Statement

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

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

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

Safety Measures

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

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

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

   Just change controls defined in operating instructions. Improper adjustment of the controls may

result in damage and involve a qualified technician to return the device to normal operation.

And do not connect multiple devices to one power adapter as adapter overload can cause overheat or fire hazard.

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

    Recommended installing the devices in areas with limited access.

Electrical Safety

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

Operation Safety

- If smoke, odour, or noise rise from the device, turn off the power at once and unplug the power cable, and then please contact the service centre.
- Transportation and other unpredictable causes may damage the device hardware. Check whether the device has any intense damage before installation.
- If the device has major defects that you cannot solve, contact your dealer as soon as possible.

- Dust, moisture, and abrupt temperature changes can affect the device's service life. You are advised not to keep the device under such conditions.
- Do not keep the device in a place that vibrates. Handle the device with care. Do not place heavy objects on top of the device.
- Do not apply rosin, alcohol, benzene, pesticides, and other volatile substances that may damage the device enclosure. Clean the device accessories with a piece of soft cloth or a small amount of cleaning agent.
- If you have any technical questions regarding usage, contact certified or experienced technical personnel.

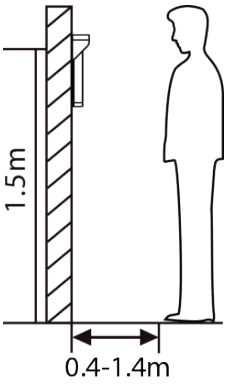
Note:

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

1 Instructions to use

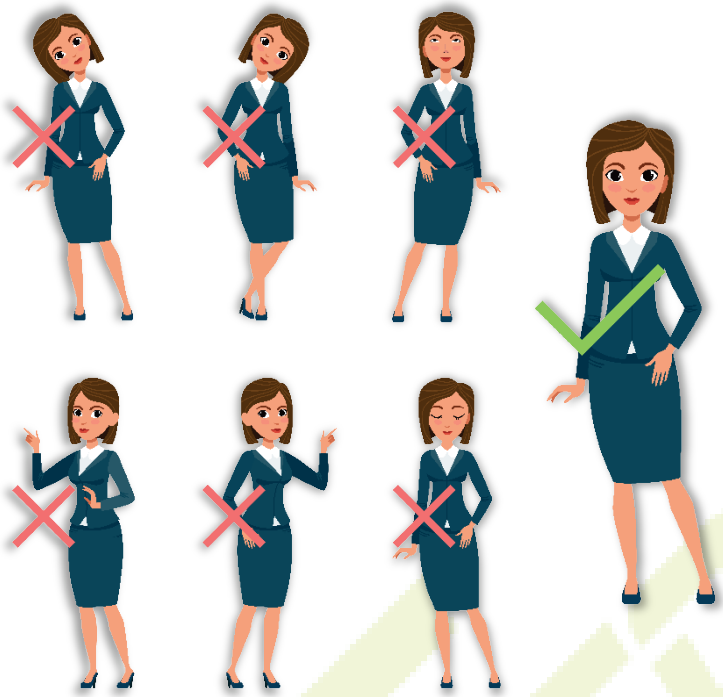
1.1 Standing Position, Facial Expression and Standing Posture

Recommended Distance



The distance between the device and a user whose height is within 1.55m to 1.85m is recommended to be 0.4 to 1.4m. Users may slightly move forwards and backwards to improve the quality of facial images captured.

Facial Expression and Standing Posture

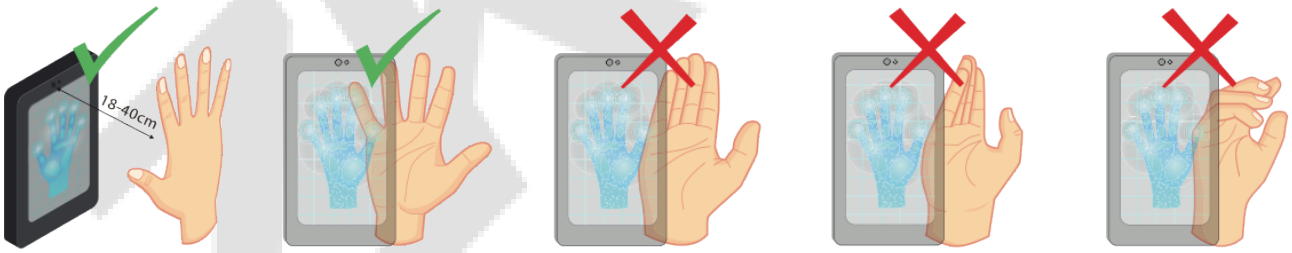


Note: During enrollment and verification, please keep natural facial expression and standing posture.

1.2 Palm Registration★

Place your palm in the palm multi-mode collection area, such that the palm is placed parallel to the device.

Make sure to keep space between your fingers.



Note:

1) Place your palm within 18 to 40 cm of the device.

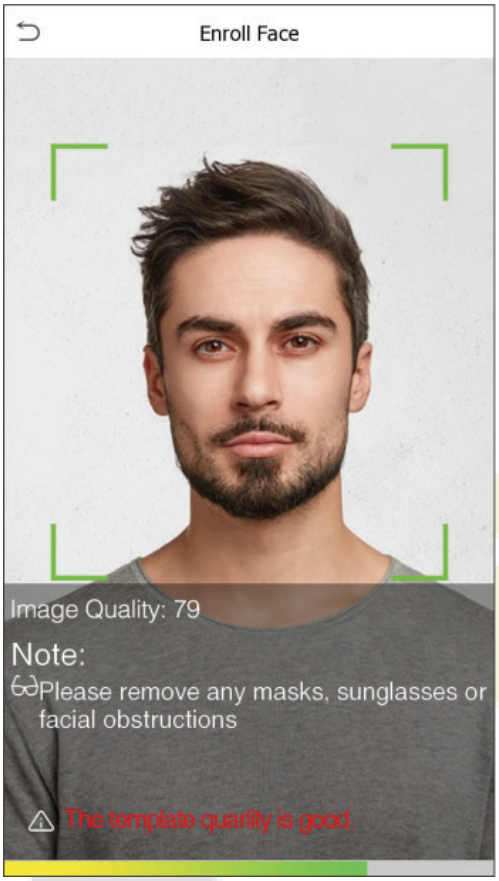
2) Place your palm in the palm collection area, such that the palm is placed parallel to the device.

3) Make sure to keep space between your fingers.

4) Please avoid direct sunlight when using the palm function outdoors. According to laboratory test, the palm recognition effect is best when the light intensity is not more than 10,000 lux.

1.3 Face Registration

Try to keep the face in the center of the screen during registration. Please face the camera and stay still during face registration. The page looks like shown below:



Face registration and authentication methods

Instructions to Register a Face

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

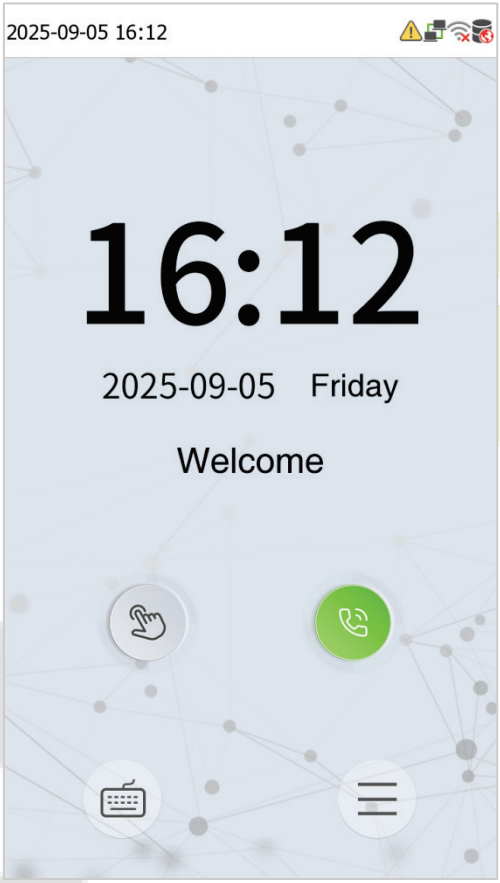
Instructions to Authenticate a Face

- Ensure that the face appears inside the detection area displayed on the device screen.

- If eyeglasses have been changed, authentication may fail. If the face without glasses has been registered, authenticate the face without glasses. If only the face with glasses has been registered, authenticate the face with the previously worn glasses again.
- 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 Standby Interface

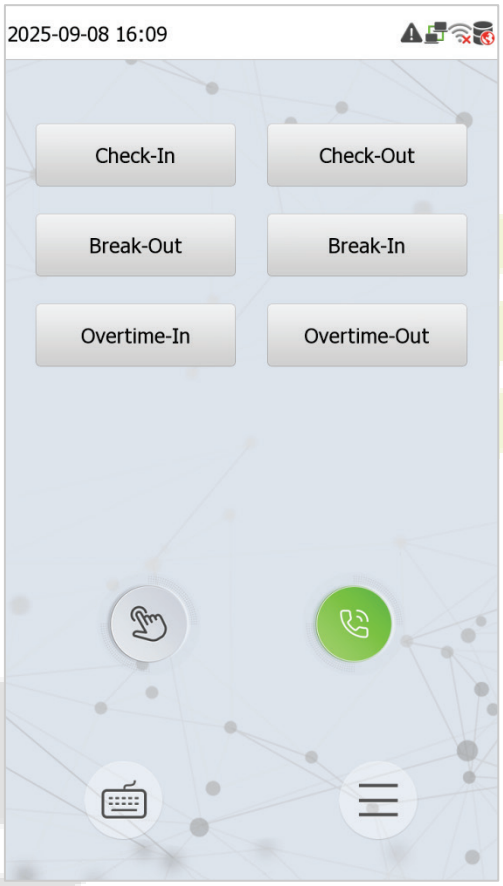
After connecting the power supply, the interface appears as shown below:



Note:

- Click to open the interface to enter the User ID.
- When there is no super administrator registered in the device, click to enter the menu. After setting the super administrator, it requires the super administrator's verification before entering the menu operation. For the security of the device, it is recommended to register a super administrator the first time you use the device.

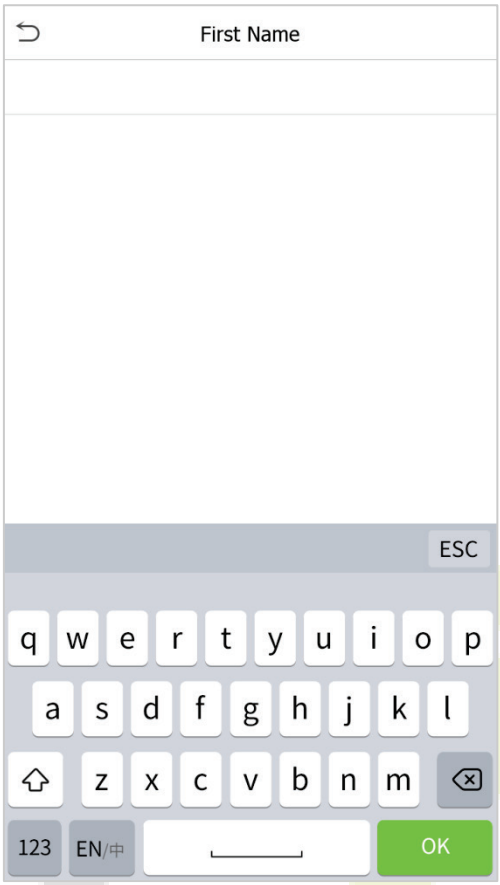
- The device defaults to disabling the camera's automatic recognition sensing function. Click icon can wake up the device's camera to automatically recognize. Please refer to section 6.2 Tap-To-Unlock for the function settings.
- Click icon to enter the video intercom call page.
- On the standby interface, the punch state options can also be shown and used directly. Click anywhere on the screen apart from the icons, and six shortcut keys appears on the screen, as shown in the figure below:



- Press the corresponding punch state key to select your current punch state, which is displayed in green.

Note: *The punch state options are off by default and need to be changed to other option in the "7.4 Punch States Options" to get the punch state options on the standby screen.*

1.5 Virtual Keyboard



Note: The device supports the input of Chinese and English characters, numbers, and symbols. Click [**En**] to switch to the English keyboard. Press [**123**] to switch to the numeric and special character keyboard, and click [**ABC**] to return to the alphabetic keyboard. Click the input box, and the virtual keyboard appears. Click [**ESC**] to exit the keyboard screen.

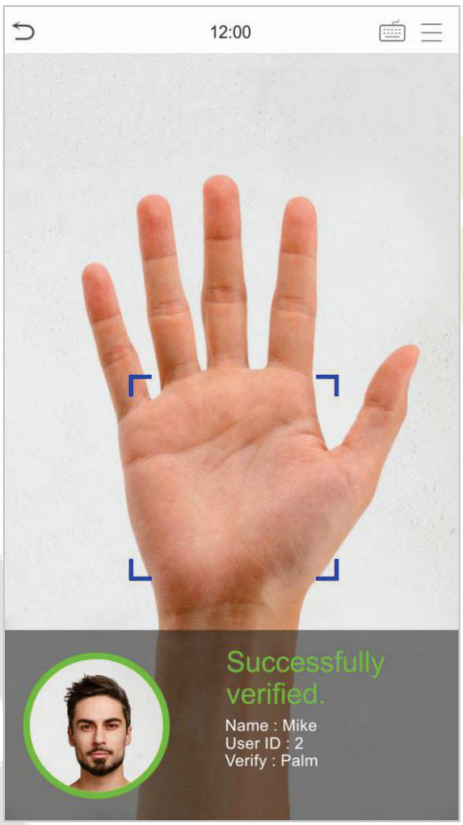
1.6 Verification Mode

1.6.1 Palm Verification★

1:N Palm Verification Mode

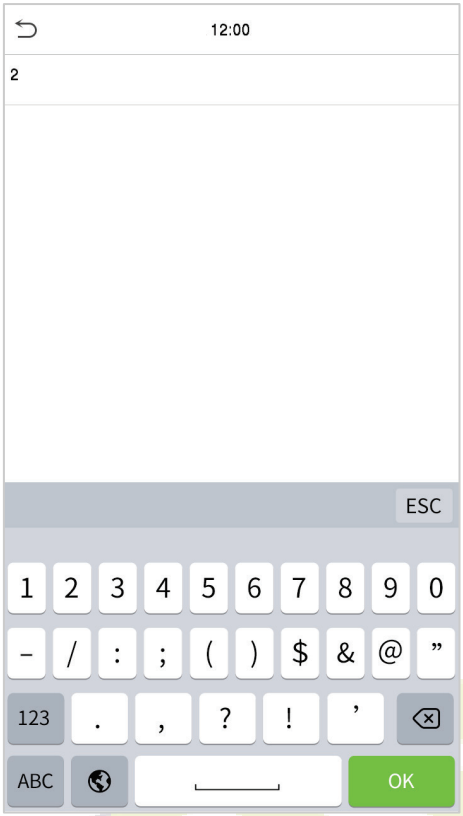
This verification mode compares the palm image collected by the palm module with all the palm data template in the device.

The device will automatically distinguish between the palm and face verification mode. 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.

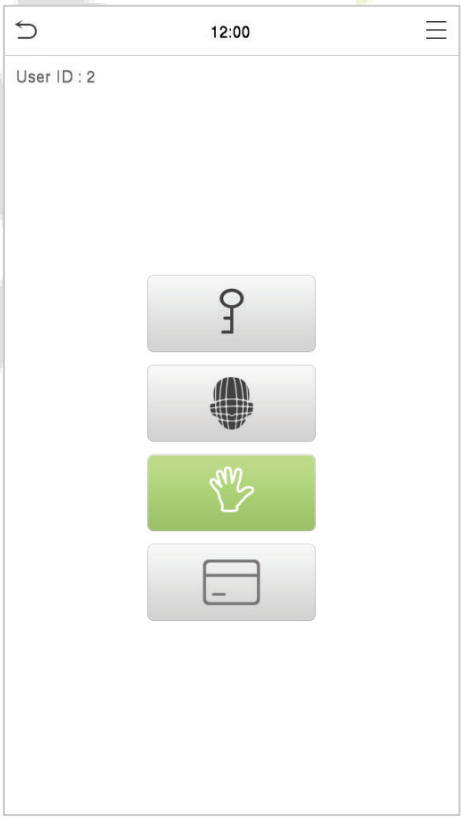


1:1 Palm Verification Mode

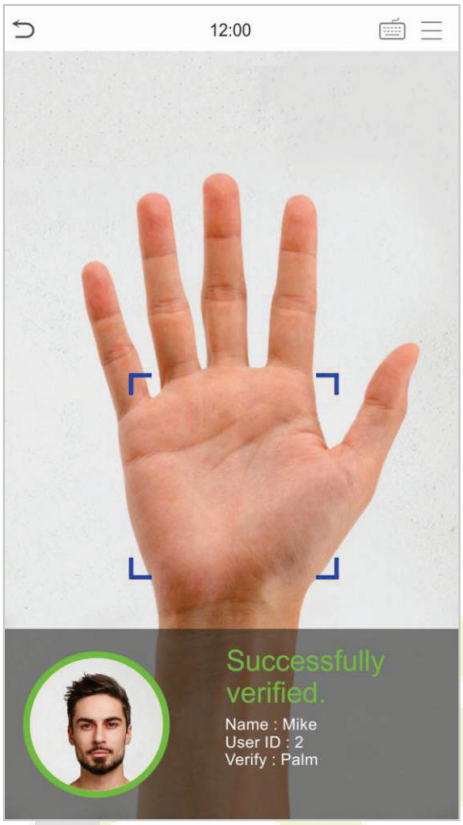
Click the button on the main screen to open the 1:1 palm verification mode. Input the user ID and press [**OK**].



If the user has registered the card, face and password in addition to palm, and the verification method is set to Password/Card/Face/Palm★, the following screen will appear. Select the palm icon to enter palm verification mode.



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



1.6.2 Facial Verification

1:N Facial Verification

1. **Conventional verification**

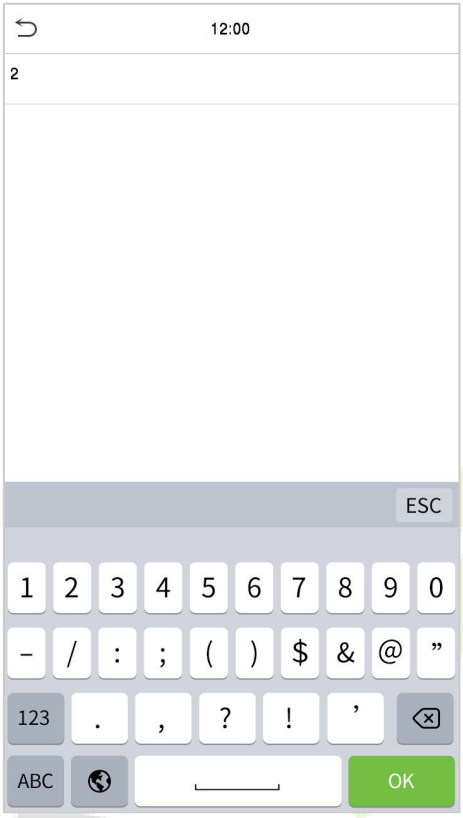
In this verification mode, the device compares the collected facial images with all face data registered in the device. The following is the pop-up prompt of a successful comparison result.

2. Enable mask detection

When the user enables the **Mask Detection** function, the device identifies whether the user is wearing a mask while verification or not. The following are the popups of the comparison result prompt interface.

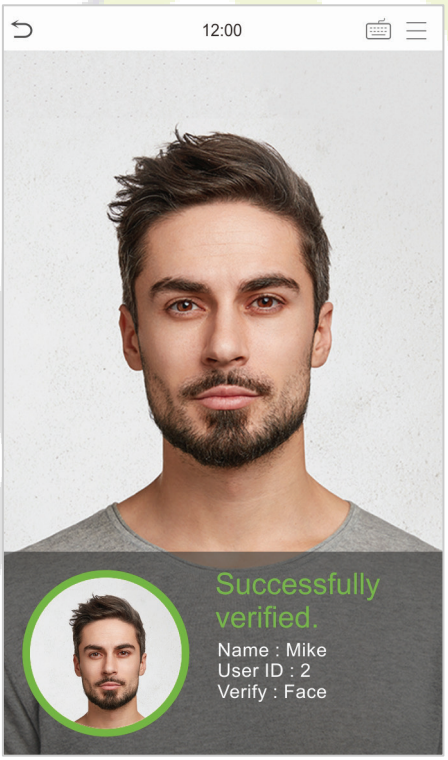
1:1 Facial Verification

In this verification mode, the device compares the face captured by the camera with the facial template related to the entered user ID. Press on the main interface and enter the 1:1 facial verification mode and enter the user ID and click [**OK**].



If the user has registered password, card and palm in addition to the face, and the verification method is set to Password/Card/Face/Palm★ verification, the following screen will appear. Select the icon to enter the face verification mode.

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



1.6.3 Multi-face Verification★

1. Conventional verification

In this verification mode, the device compares the obtained multi-person facial images with all the face data stored in it. At the same time, the device can verify up to four people. The number of verification results displayed on the right side, can be customized. The image below depicts the pop-up prompt for a successful comparison result.

Tap **System** > **Face** > **Recognition Settings** > **Multi-face Identifying** > **Count to Display** to set the number of the verification results to be displayed.

Note: The **Count to Display** can be set between 1 to 4.

2. Enable Mask Detection

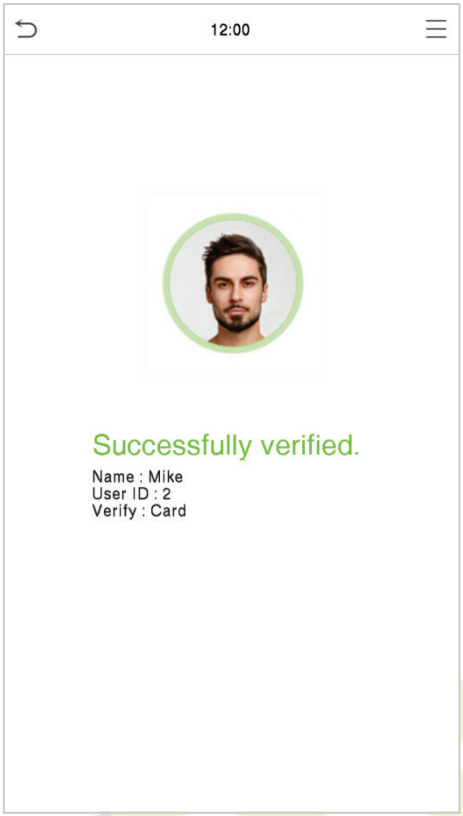
When the user enables the **Mask Detection** function, the device identifies whether the user is wearing a mask while verification or not. The following are the pop-ups of the comparison result prompt interface.

Note: Not wearing a mask is displayed as orange frame.

1.6.4 Card Verification

1:N Card Verification

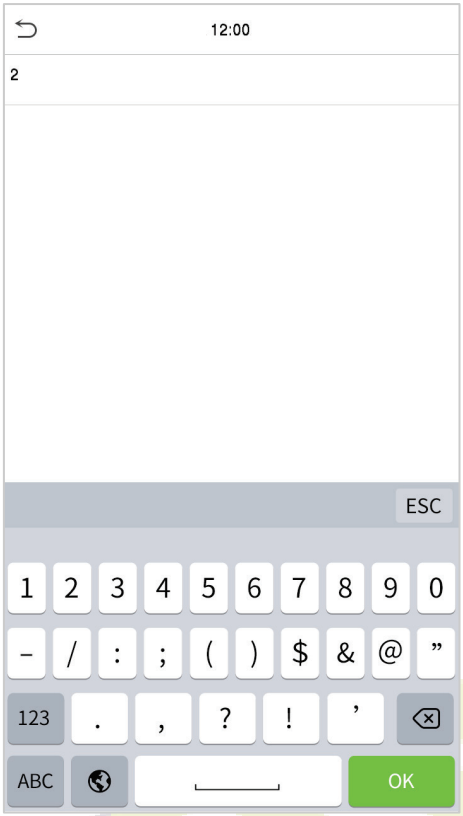
This verification mode compares the card number in the Card induction area with all the card number data registered in the device; the following is the card verification screen.



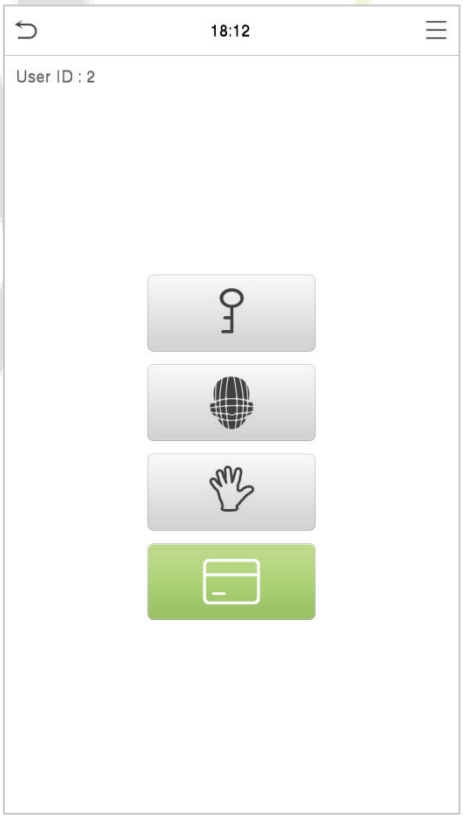
1:1 Card Verification

Click the button on the main screen to open the 1:1 Card verification mode.

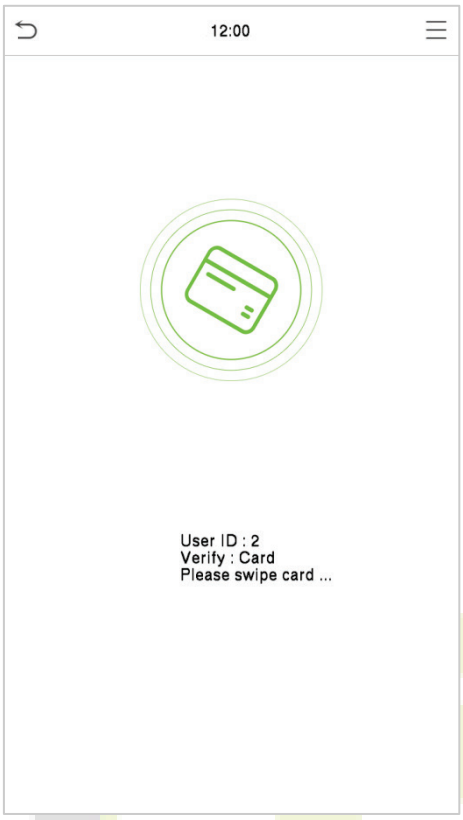
1. Input the user ID and press [**OK**].



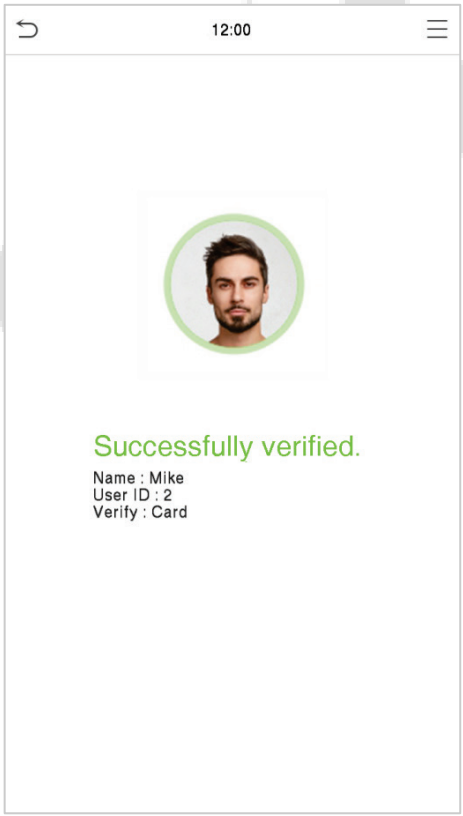
If an employee registers palm, face and password in addition to card, and the verification method is set to Password/Card/Face/Palm★, the following screen will appear. Select the icon to enter the card verification mode.



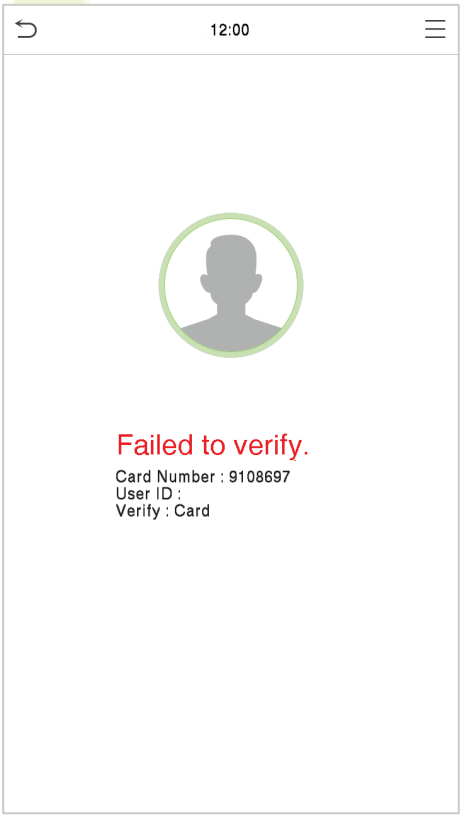
2. Swipe the card above the card area (the card must be registered first).



Successful Verification:



Failed Verification:

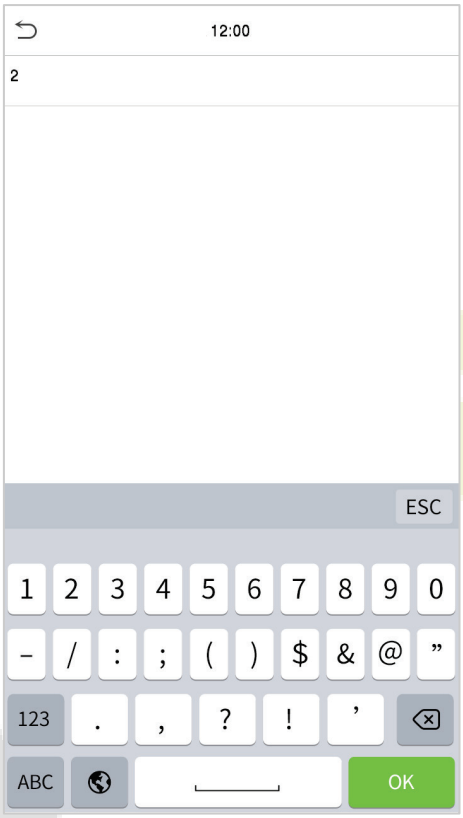


1.6.5 Password Verification

The Password Verification mode compares the entered password with the registered User ID and Password.

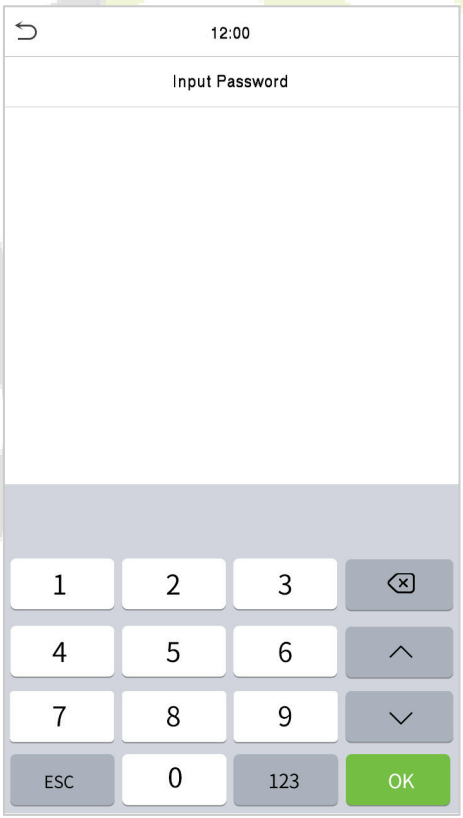
Click the button on the main screen to open the 1:1 password verification mode.

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

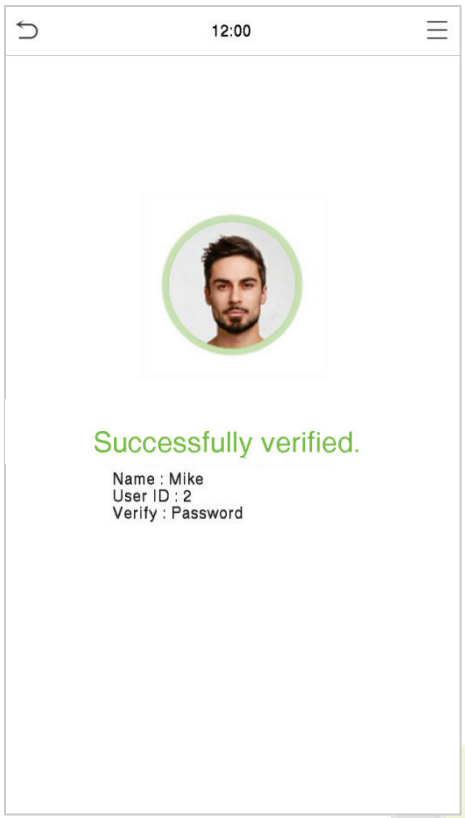


If an employee registers palm, card and face in addition to password, and the verification method is set to Password/Card/Face/Palm★, the following screen will appear. Select the icon to enter the password verification mode.

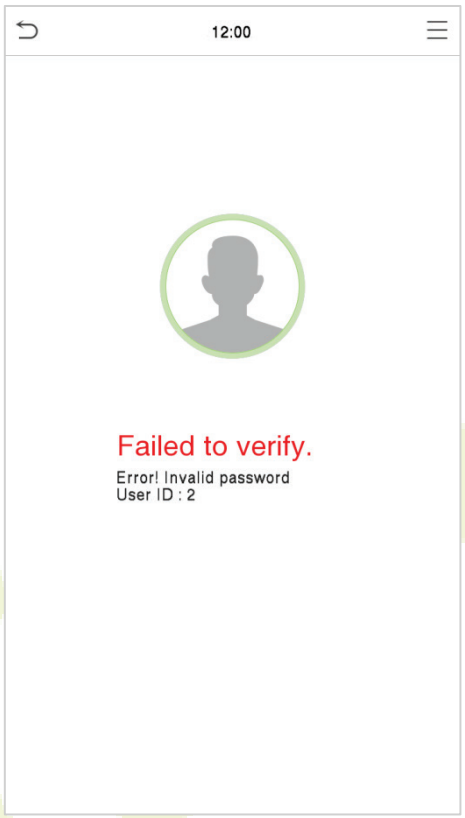
2. Input the password and press [**OK**].



Successful Verification:

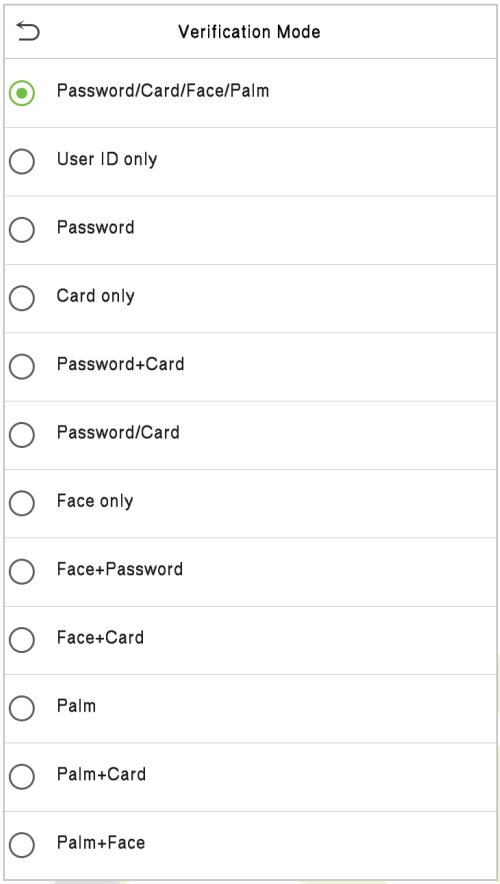


Failed Verification:



1.6.6 Multi-factor Authentication

To increase the security, this device offers the option of using multiple forms of verification methods. A total of 12 different verification combinations can be used, as shown below:



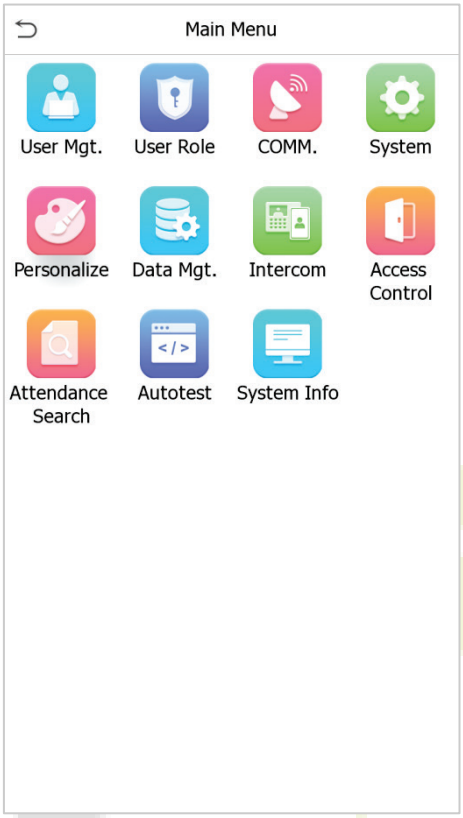
Note:

1) "/" means "or", and "+" means "and".

2) You must register the required verification information before using the combination verification mode, otherwise, the verification may fail. For example, if a user uses Face Registration but the verification mode is Face + Password, this user will never pass verification.

2 Main Menu

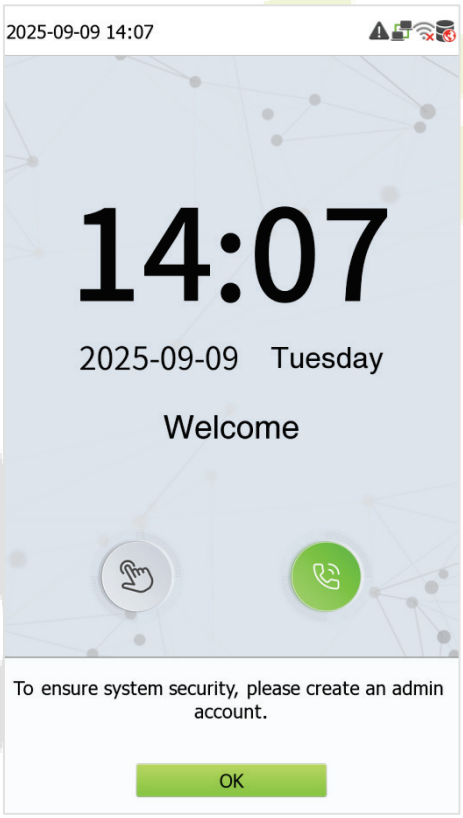
Press on the initial interface to enter the main menu, as shown below:



Menu	Description
User Mgt.	To add, edit, view, and delete the basic information about a user.
User Role	To set the permission scope of the custom role and enroller, that is, the rights to operate the system.
COMM.	To set the relevant parameters of the network, Serial comm, PC connection, Wireless network★, Cloud server, Wiegand and Network diagnosis.
System	To set the parameters related to the system, including date & time, tap-to-unlock, access logs settings/attendance, face, palm parameters★, health protection, device type settings, security settings, update firmware online and restore to factory.
Personalize	This includes user interface, voice, bell schedules, punch state options and shortcut key mappings settings.
Data Mgt.	To delete all the relevant data in the device.
Intercom★	To set the parameters related to the SIP and NVR.
Work Code★	Set different type of work. (Only for T&A PUSH)

Access Control	To set the parameters of the lock and the relevant access control device including options like Time Rule Settings, Holiday Settings, Combined verification, Anti-Passback Setup and Duress Option Settings.
Attendance Search	To query the specified Event Logs/Attendance Records, check Attendance Photos and Blocklist attendance photos.
Autotest	To automatically test whether each module functions properly, including the LCD screen, audio, microphone, camera, and real-time clock.
System Info	To view the data capacity, device and firmware information and privacy policy of the device.

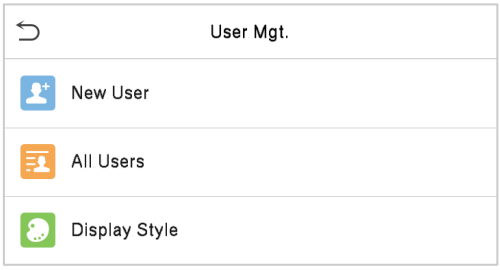
Note: When users use the product for the first time, they should operate it after setting administrator privileges. Tap **User Mgt.** to add an administrator or edit user permissions as a super administrator. If the product does not have an administrator setting, the system will show an administrator setting command prompt every time you enter the device menu.



3 User Management

3.1 Add Users

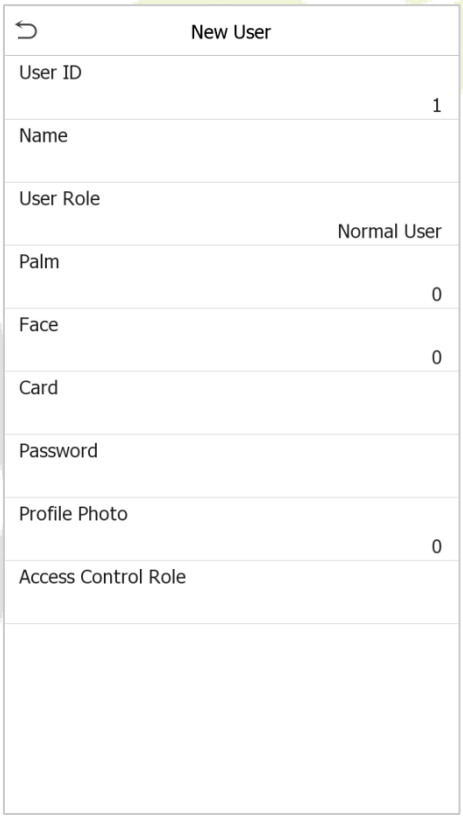
Click **User Mgt.** on the main menu.



Click **New User.**

Register a User ID and Name

Enter the User ID and Name.



Note:

1) A username may contain 34 characters.
2) The user ID may contain 1 to 14 digits by default.

3) During the initial registration, you can modify your ID, which cannot be modified after registration.

4) If a message "Duplicated ID" pops up, you must choose another ID.

Setting the User Role

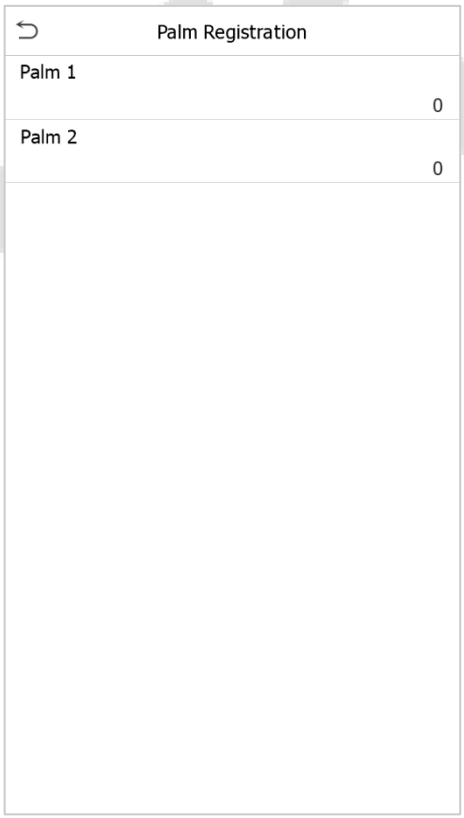
There are two types of user accounts: **Normal User** and **Super Admin**. If there is already a registered administrator, the normal users have no rights to manage the system and may only access authentication verifications. The Administrator owns all the management privileges. If a custom role is set,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

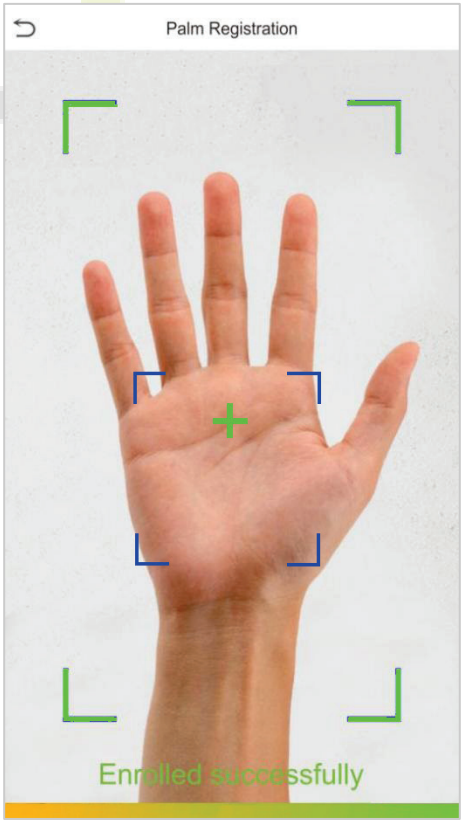
Click **User Role** to select Normal User or Super Admin.

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

Register Palm★

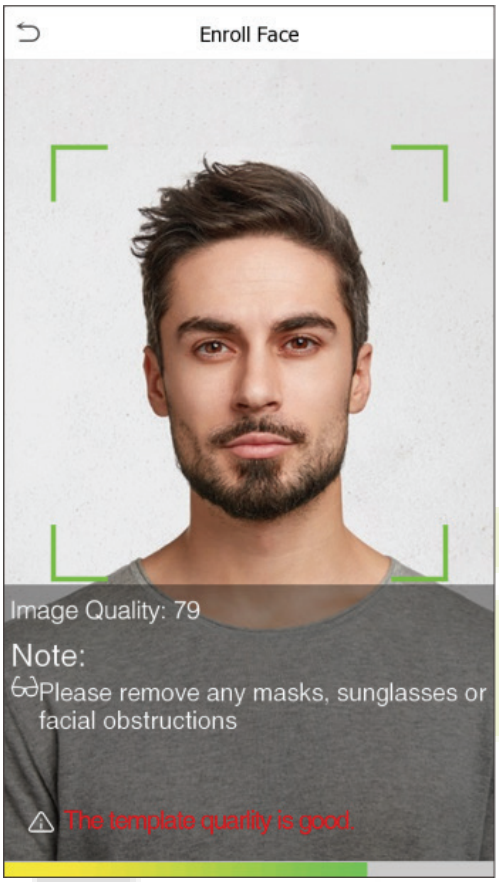
Click **Palm** to open the palm registration page. Select the hand to be enrolled.





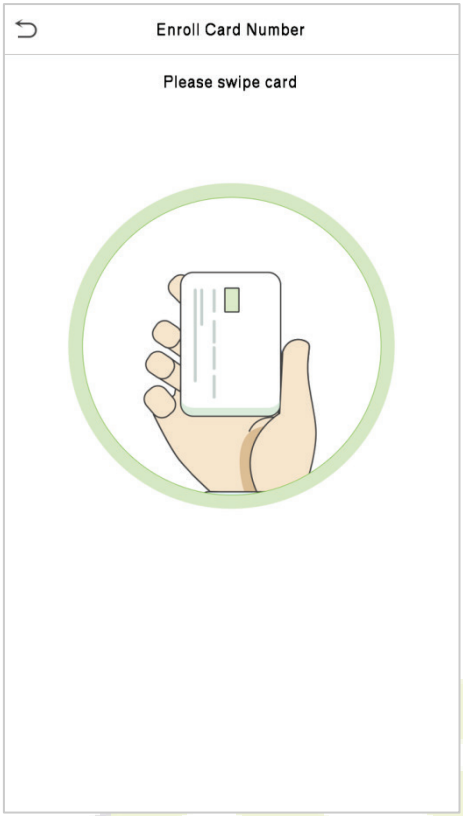
Register Face

Click **Face** to enter the face registration page. Please face the camera and stay still during face registration. The registration interface is as follows:



Register Card

Press your card above the card area. The card number registration will be successful.



Register Password

Click **Password** to open the password registration page. Enter a password and re-enter it. Click **OK**. If the two entered passwords are different, the prompt "Password not match" will appear.

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

Register Profile Photo

When a user registered with a photo passes the authentication, the registered photo will be displayed (enter **[System] > [Access Logs Settings/Attendance]** to enable **Display User Photo**).

Click **Profile Photo**; click the camera icon to take a photo. The system will return to the New User interface after taking a photo.

Note: While registering a face, the system will automatically capture a picture as the profile photo. If you do not want to register a profile photo, the system will automatically set the picture captured as the default photo.

Access Control Role

Tap **Access Control Role** > **Access Group**, to assign the registered users to different groups for better management. New users belong to Group 1 by default and can be reassigned to other groups. The device supports up to 99 Access Control groups.

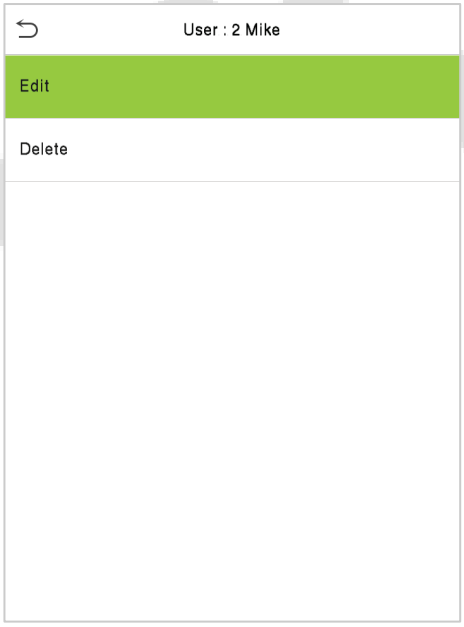
Tap **Time Period**, to select the time period to use.

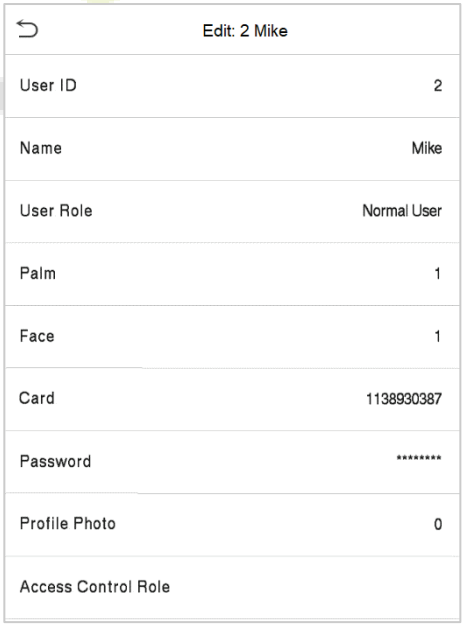
3.2 Search for Users

Click the search bar on the user list and enter the retrieval keyword (The keyword may be an ID or full name).The system will search for the users related to the information.

3.3 Edit Users

Select a user from the list and click **Edit** to enter the edit user interface.



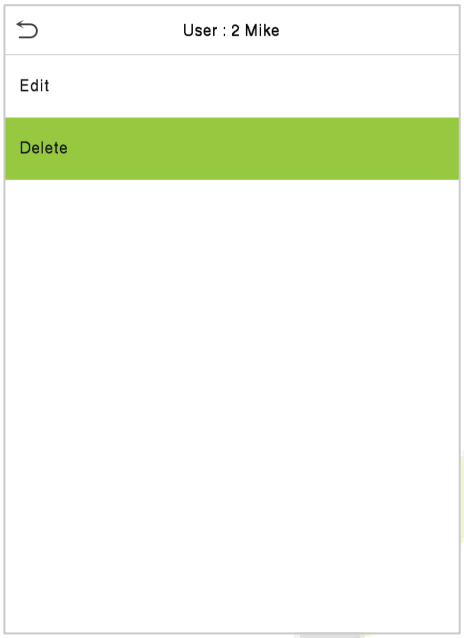


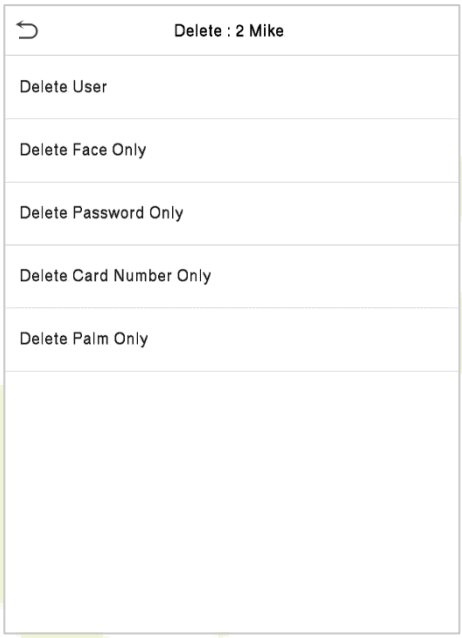
Note: The operation of editing a user is the same as that of adding a user, except that the user ID cannot be modified when editing a user. For further details, refers "3.1 Add Users".

3.4 Delete Users

Select a user from the list and click **Delete** to enter the delete user interface. Select the user information to be deleted and click **OK**.

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



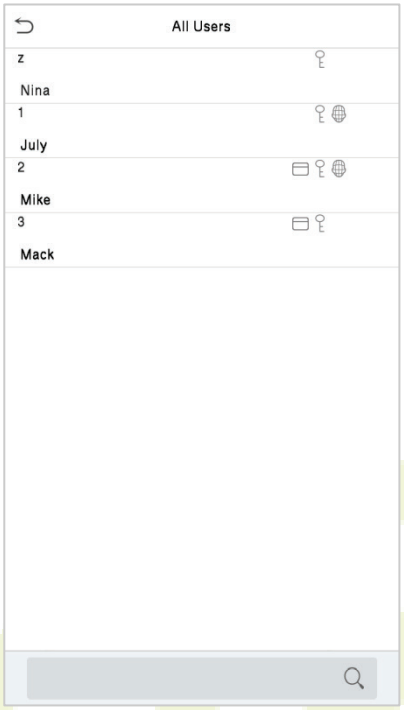


3.5 Display Style

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

All the Display Styles are shown as below:

Multiple Line



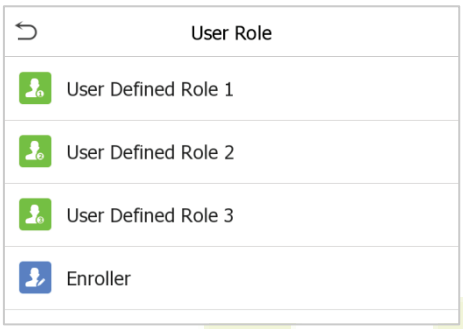
Mixed Line

4 User Role

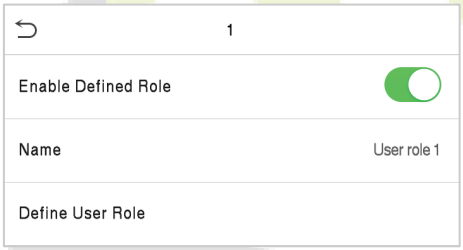
If you need to assign some specific permissions to certain users, you may edit the "User Defined Role" under the **User Role** menu.

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

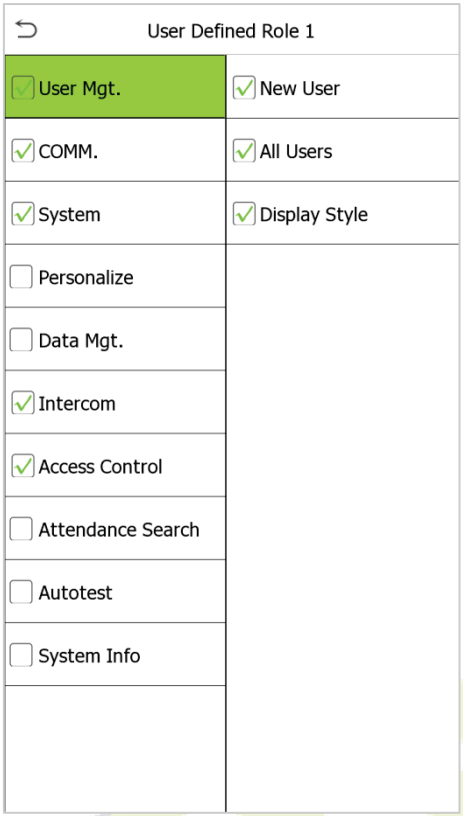
Click **User Role** on the main menu interface.



1. Click any user role to set a defined role. Toggle the **Enable Defined Role** button to enable this defined role. Click **Name** and enter the name of the role.

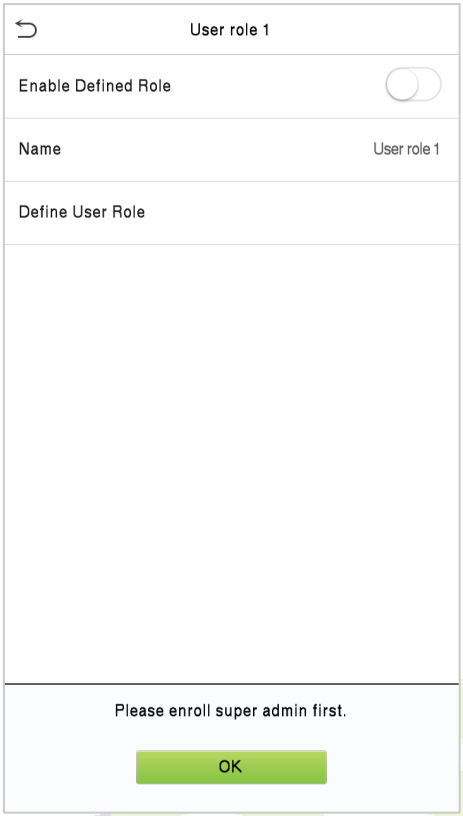


2. Click **Define User Role** to assign privileges to the role. Once the privilege assignment is completed, click **Return**.



Note: During the privilege assignment, the main menu is on the left and its sub-menus are on the right. You only need to select the features in sub-menus. If the device has a role enabled, you may assign the roles you set to users by clicking **User Mgt. > New User> User Role**.

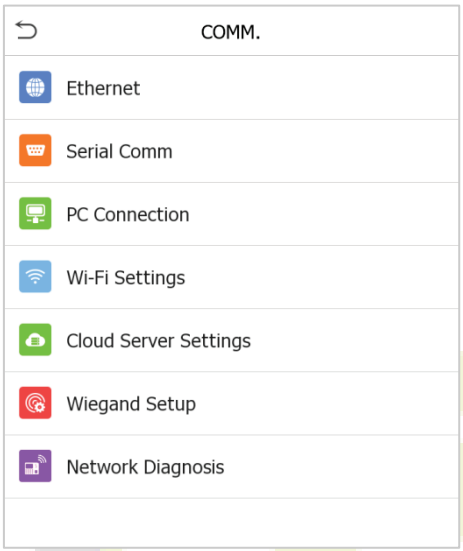
If no super administrator is registered, the device will prompt "Please enroll super admin first!" after clicking the enable bar, as shown below.



5 Communication Settings

Communication Settings are used to set the parameters of the Network, Serial Comm, PC connection, Wireless Network★, Cloud server, and Wiegand, Network Diagnosis.

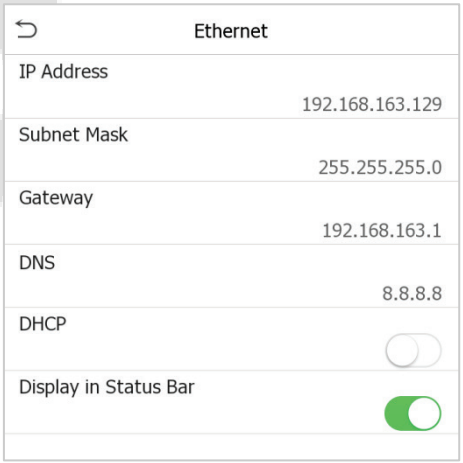
Click **COMM.** on the main menu.



5.1 Network Settings

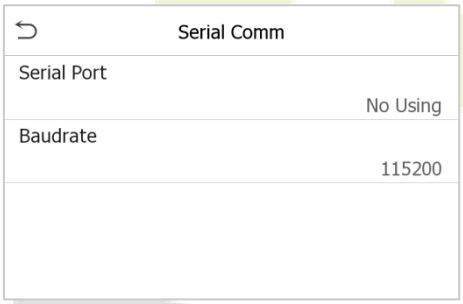
When the device needs to communicate with a PC over the Ethernet, you need to configure network settings and ensure that the device and the PC are connecting to the same network segment.

Click **Ethernet** on the Comm. Settings interface.



Menu	Description
IP Address	The factory default value is 192.168.1.201. Please set the IP Address as per the requirements.
Subnet Mask	The factory default value is 255.255.255.0. Please set the value as per the requirements.
Gateway	The factory default address is 0.0.0.0. Please set the value as per the requirements.
DNS	The factory default address is 0.0.0.0. Please set the value as per the requirements.
DHCP	Dynamic Host Configuration Protocol, which is to dynamically allocate IP addresses for clients via server.
Display in Status Bar	To set whether to display the network icon on the status bar.

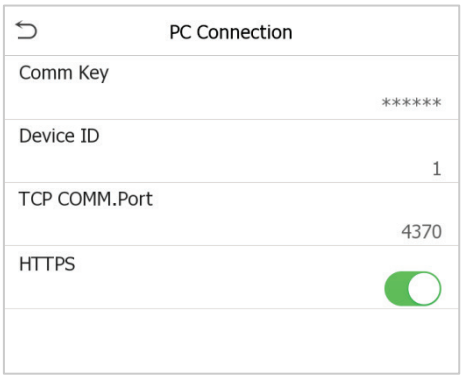
5.2 Serial Comm



Menu	Description
Serial Port	**No Using:** Do not communicate with the device through the serial port. **RS485(PC):** Communicates with the PC through RS485 serial port. **Master Unit:** When RS485 is used as the function of "**Master Unit**", the device will act as a master unit, and it can be connected to RS485 reader.
Baudrate	When the serial port is set as **Master Unit**, the baudrate is 115200 by default and cannot be modified. When the serial port is set as **RS485(PC)**, there are 4 baudrate options. They are: 115200 (default), 57600, 38400 and 19200. The higher is the baud rate, the faster is the communication speed, but also the less reliable. Hence, a higher baud rate can be used when the communication distance is short; when the communication distance is long, choosing a lower baud rate would be more reliable.

5.3 PC Connection

Click **PC Connection** on the Comm. Settings interface.

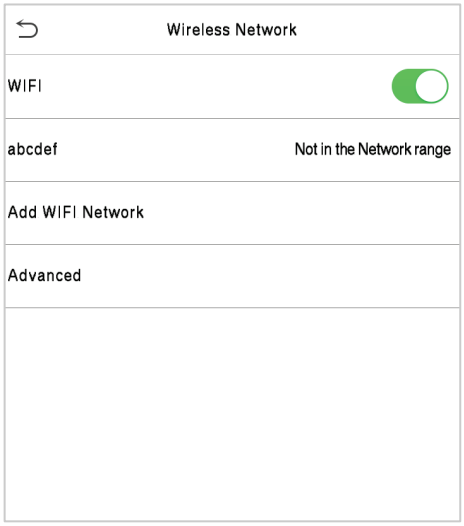


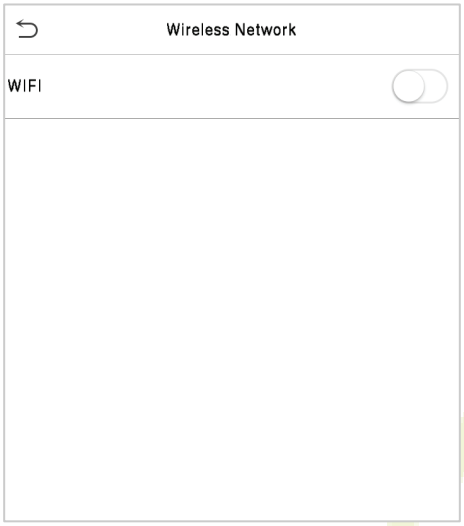
Menu	Description
Comm Key	This menu only appears after enabling **Standalone Communication** function in **System> Security Settings**. To improve the security of data, the Comm Key needs to be entered before the device can be connected to the C/S software. It can be changed as needed.
Device ID	The identity number of the device, which ranges between 1 and 254. If the communication method is RS232/RS485, you need to input this device ID in the software communication interface.
TCP COMM. Port	The default TCP COMM Port value is 4370. It can be modified according to the network availability.
HTTPS	To increase the security of software access, users can enable the HTTPS protocol to create a secure and encrypted network transmission and assure the security of sent data through identity authentication and encrypted communication. This function is enabled by default. This function can be enabled or disabled through the menu interface, and when changing the HTTPS status, the device will pop up a security prompt, and restart after confirmation.

5.4 Wireless Network★

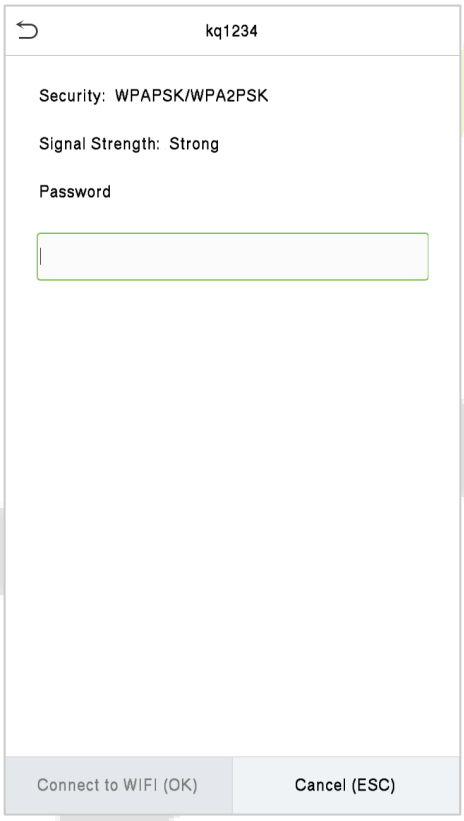
Wi-Fi is short for Wireless Fidelity. The device provides a Wi-Fi module, which can be built in the device mould, to enable data transmission via Wi-Fi and establish a wireless network environment.

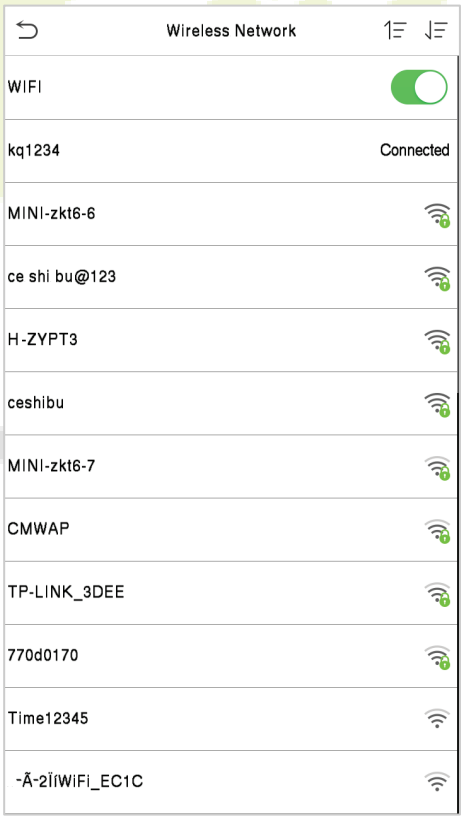
Wi-Fi is enabled in the system by default. If the Wi-Fi network does not need to be used, you can click the button to disable Wi-Fi.





When Wi-Fi is enabled, click the searched network. Click the password entry text box to enter the password, and click **Connect to Wi-Fi (OK)**.



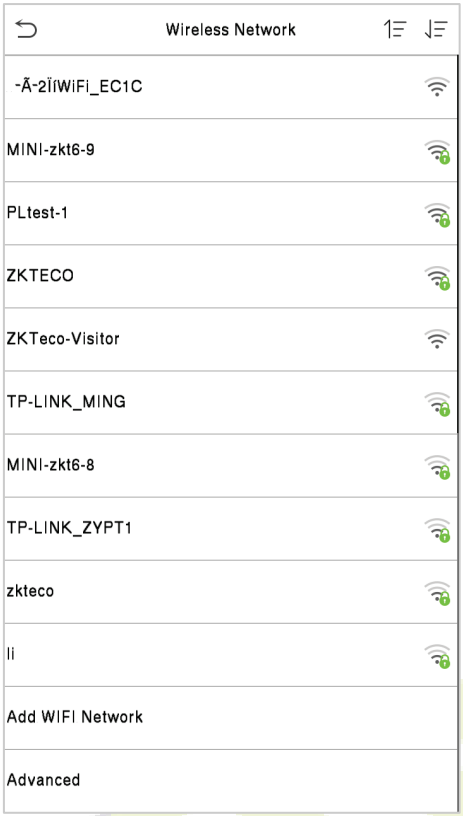


The connection succeeds, with status displayed on the icon bar.

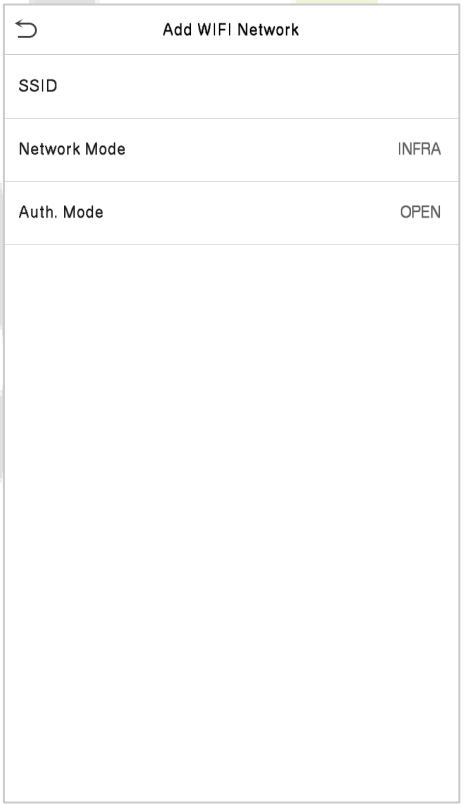
Adding Wi-Fi Network

If the desired Wi-Fi network is not in the list, you can add the Wi-Fi network manually.

Click **Page Down** and **Add Wi-Fi Network**.



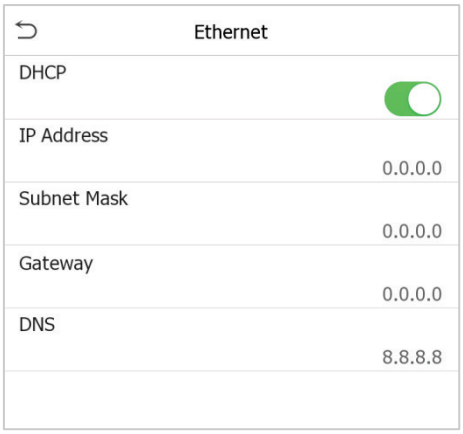
Enter the parameters of Wi-Fi network. (The added network must exist.)



After adding, find the added Wi-Fi network in list and connect to the network in the above way.

Advanced Options

This is used to set Wi-Fi network parameters.

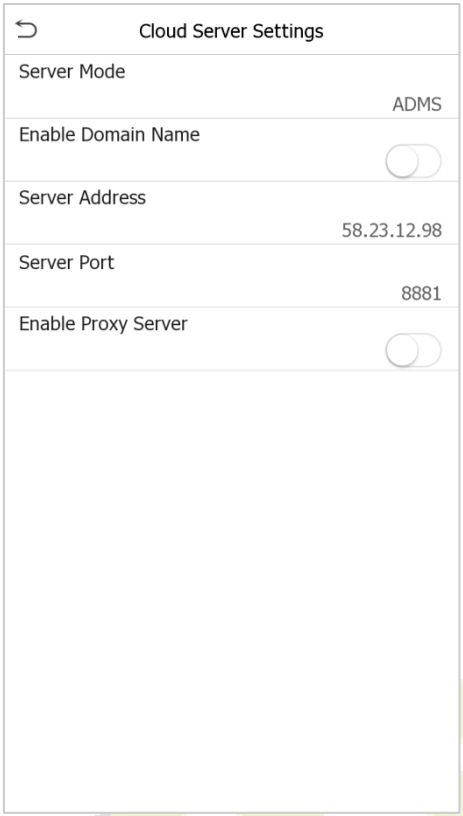


Menu	Descriptions
DHCP	Short for Dynamic Host Configuration Protocol, which involves allocating dynamic IP addresses to network clients.
IP Address	IP address of the Wi-Fi network.
Subnet Mask	Subnet mask of the Wi-Fi network.
Gateway	Gateway address of the Wi-Fi network.
DNS	DNS of the Wi-Fi network.

5.5 Cloud Server Settings

This represents the settings used for connecting the ADMS server.

Click **Cloud Server Settings** on the Comm. Settings interface.

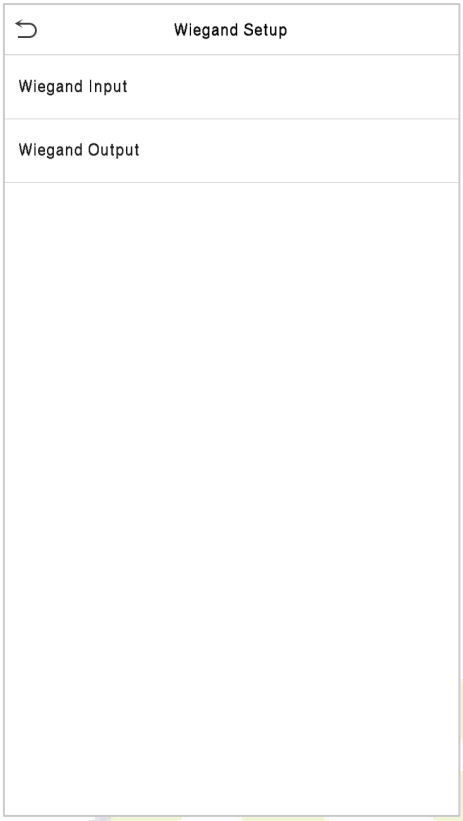


Menu		Description
Enable Domain Name	**Server Address**	When this function is enabled, the domain name mode "http://... "will be used, such as http://www.XYZ.com, while "XYZ" denotes the domain name when this mode is turned ON.
Disable Domain Name	**Server Address**	IP address of the ADMS server.
	Server Port	Port used by the ADMS server.
Enable Proxy Server		When you choose to enable the proxy, you need to set the IP address and port number of the proxy server.

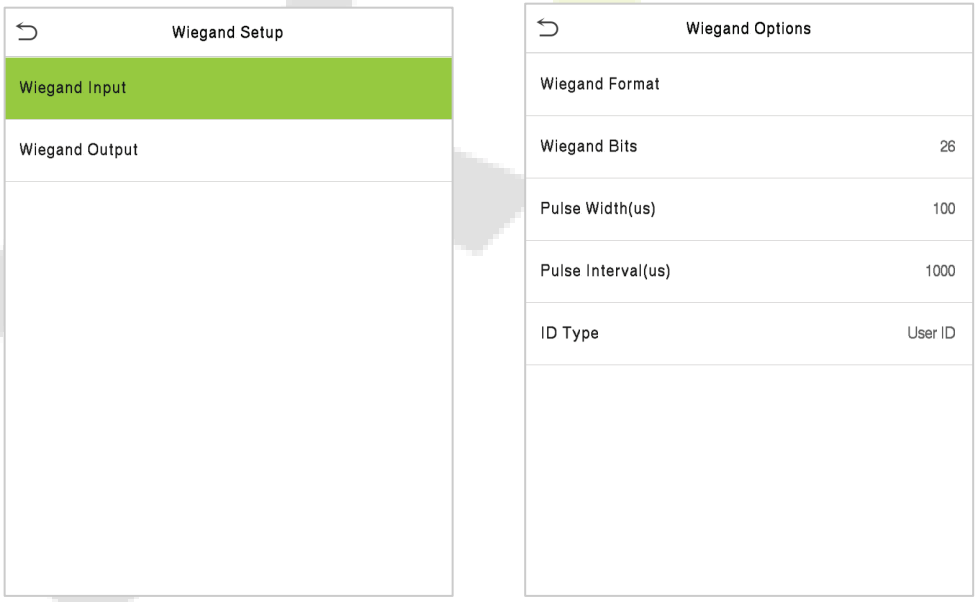
5.6 Wiegand Setup

The menu is used to set the Wiegand Input & Output parameters.

Click **Wiegand Setup** on the Comm. Settings interface.



Wiegand Input



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

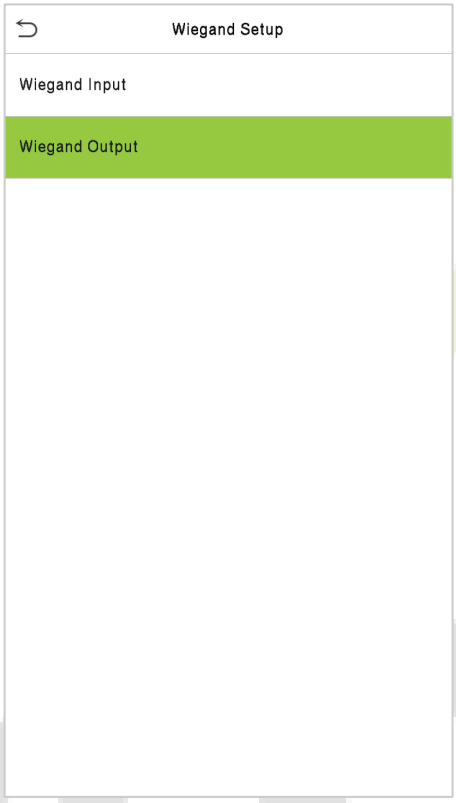
Pulse Interval(us)	The default value is 1000 microseconds, which can be adjusted within the range of 200 to 20000 microseconds.
ID Type	Select between the User ID and Card number.

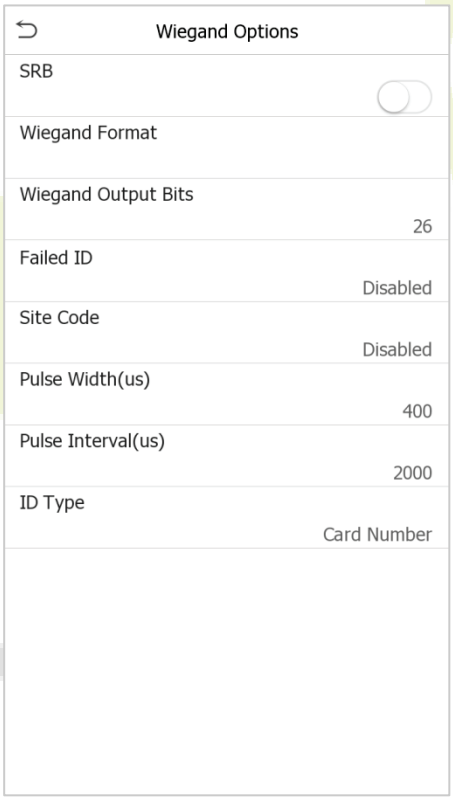
Definitions of various common Wiegand formats:

Wiegand Format	Description
Wiegand26	ECCCCCCCCCCCCCCCCCCCCCCCCO It consists of 26 bits of binary code. The 1st bit is the even parity bit of the 2nd to 13th bits, while the 26th bit is the odd parity bit of the 14th to 25th bits. The 2nd to 25th bits is the card numbers.
Wiegand26a	ESSSSSSSSCCCCCCCCCCCCCCCCO It consists of 26 bits of binary code. The 1st bit is the even parity bit of the 2nd to 13th bits, while the 26th bit is the odd parity bit of the 14th to 25th bits. The 2nd to 9th bits is the site codes, while the 10th to 25th bits are the card numbers.
Wiegand34	ECCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO It consists of 34 bits of binary code. The 1st bit is the even parity bit of the 2nd to 17th bits, while the 34th bit is the odd parity bit of the 18th to 33rd bits. The 2nd to 25th bits is the card numbers.
Wiegand34a	ESSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCO It consists of 34 bits of binary code. The 1st bit is the even parity bit of the 2nd to 17th bits, while the 34th bit is the odd parity bit of the 18th to 33rd bits. The 2nd to 9th bits is the site codes, while the 10th to 25th bits are the card numbers.
Wiegand36	OFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCMME It consists of 36 bits of binary code. The 1st bit is the odd parity bit of the 2nd to 18th bits, while the 36th bit is the even parity bit of the 19th to 35th bits. The 2nd to 17th bits is the device codes. The 18th to 33rd bits is the card numbers, and the 34th to 35th bits are the manufacturer codes.
Wiegand36a	EFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCO It consists of 36 bits of binary code. The 1st bit is the even parity bit of the 2nd to 18th bits, while the 36th bit is the odd parity bit of the 19th to 35th bits. The 2nd to 19th bits is the device codes, and the 20th to 35th bits are the card numbers.
Wiegand37	OMMMMSSSSSSSSSSSCCCCCCCCCCCCCCCCCCE It consists of 37 bits of binary code. The 1st bit is the odd parity bit of the 2nd to 18th bits, while the 37th bit is the even parity bit of the 19th to 36th bits. The 2nd to 4th bits is the manufacturer codes. The 5th to 16th bits is the site codes, and the 21st to 36th bits are the card numbers.
Wiegand37a	EMMMFFFFFFFFFSSSSSSCCCCCCCCCCCCCCCCO It consists of 37 bits of binary code. The 1st bit is the even parity bit of the 2nd to 18th bits, while the 37th bit is the odd parity bit of the 19th to 36th bits. The 2nd to 4th bits is the manufacturer codes. The 5th to 14th bits is the device codes, and15th to 20th bits are the site codes, and the 21st to 36th bits are the card numbers.

Wiegand50	ESSSSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO It consists of 50 bits of binary code. The 1st bit is the even parity bit of the 2nd to 25th bits, while the 50th bit is the odd parity bit of the 26th to 49th bits. The 2nd to 17th bits is the site codes, and the 18th to 49th bits are the card numbers.
"C" denotes the card number; **"E"** denotes the even parity bit; **"O"** denotes the odd parity bit; **"F"** denotes the facility code; **"M"** denotes the manufacturer code; **"P"** denotes the parity bit; and **"S"** denotes the site code.	

Wiegand Output

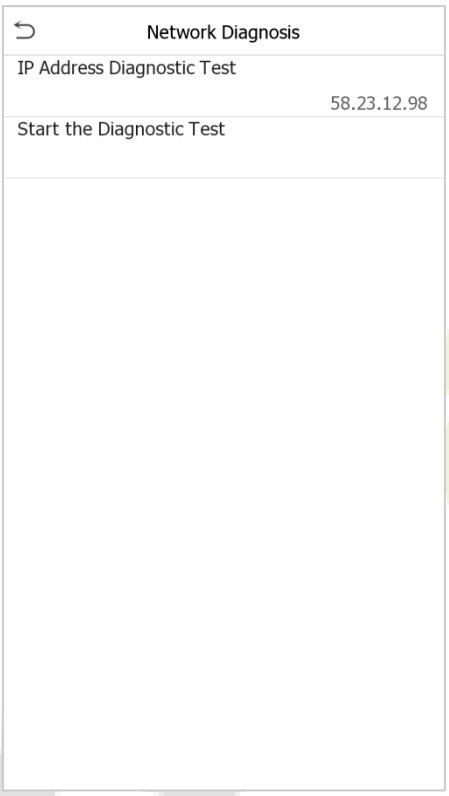




Menu	Descriptions
SRB★	When SRB is enabled, the lock is controlled by the SRB to prevent the lock from being opened due to device removal.
Wiegand Format	Values range from 26 bits, 34 bits, 36 bits, 37 bits, and 50 bits.
Wiegand Output Bits	After choosing the Wiegand format, you can select one of the corresponding output digits in the Wiegand format.
Failed ID	If the verification is failed, the system will send the failed ID to the device and replace the card number or personnel ID with the new ones.
Site Code	It is similar to the Device ID. The difference is that a site code can be set manually, and is repeatable in a different device. The valid value ranges from 0 to 256 by default.

Pulse Width(us)	The pulse width represents the changes in the quantity of electric charge with high-frequency capacitance regularly within a specified time.
Pulse Interval(us)	The time interval between pulses.
ID Type	Select between the User ID and Card number.

5.7 Network Diagnosis

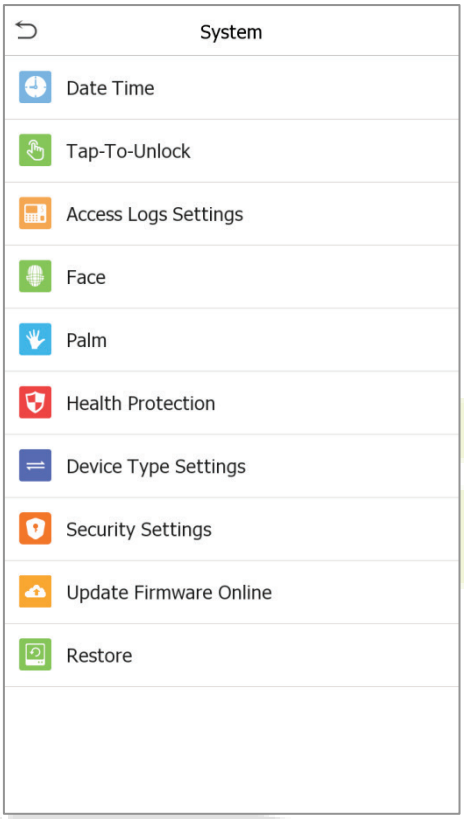


Menu	Description
IP Address Diagnostic Test	The factory default address is 0.0.0.0. Please set the value as per the requirements.
Start the Diagnostic Test	Click start to automatically diagnose the network.

6 System Settings

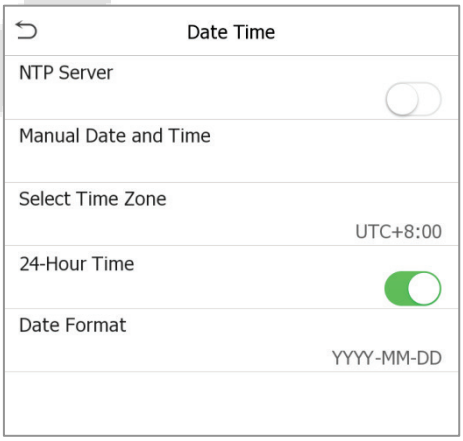
The System Settings is used to set the related system parameters to optimize the performance of the device.

Click **System** on the main menu interface.



6.1 Date and Time

Click **Date Time** on the System interface.



1. The product supports the NTP synchronization time system by default. This function takes effect after **NTP Server** is enabled and the corresponding NTP server address link is set.

2. If users need to set date and time manually, disable **NTP Server** first, and then tap **Manual Data and Time** to set date and time and tap Confirm to save.

3. Click **24-Hour Time** to enable or disable this format and select the date format.

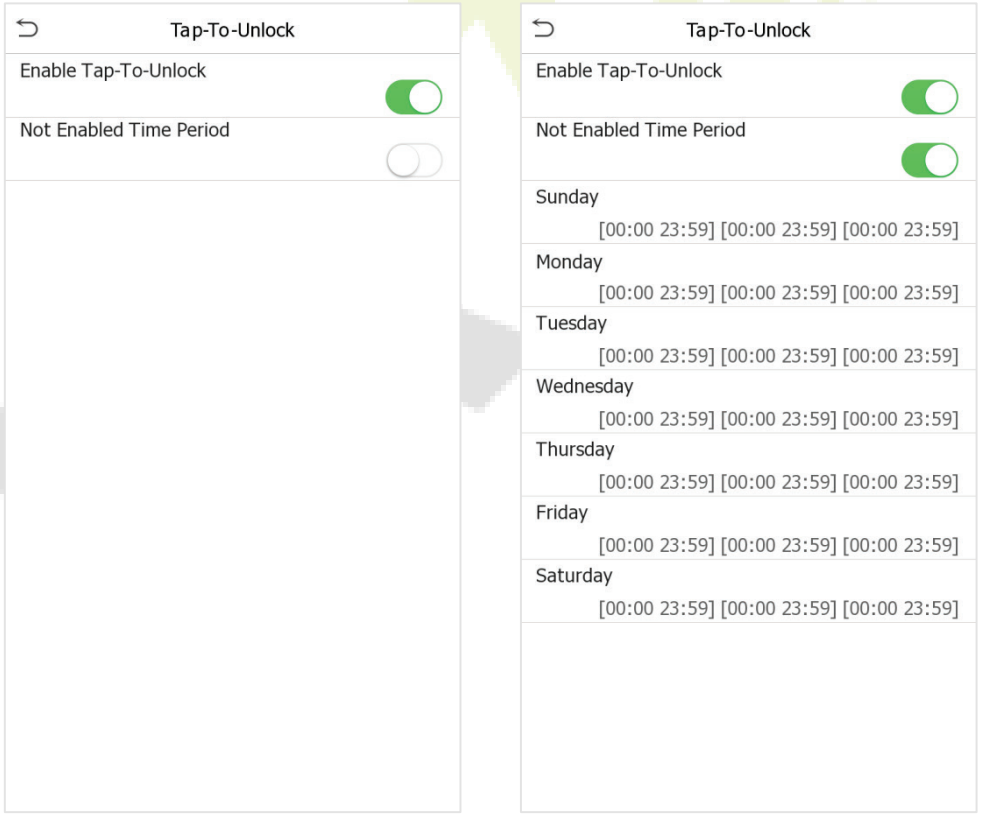
When restoring the factory settings, the time (24-hour) and date format (YYYY-MM-DD) can be restored, but the device date and time cannot be restored.

Note: For example, the user sets the time of the device (18:35 on March 15, 2020) to 18:30 on January 1, 2021. After restoring the factory settings, the time of the device will change to 18:30, January 1, 2021.

6.2 Tap-To-Unlock

Tap **Tap-To-Unlock** on the **System** interface.

After enabling Tap-To-Unlock, the device will turn off the sensing function of camera automatic recognition. Only by clicking the  icon on the screen can the device's camera automatic recognition be awakened.

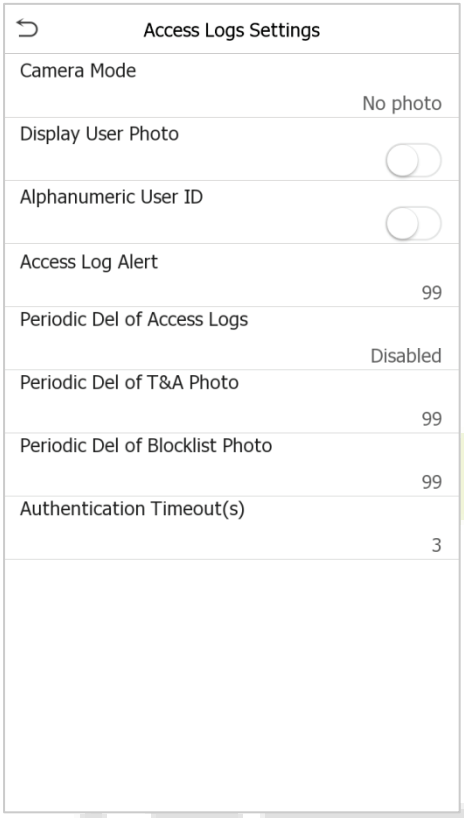


Function Name	Description
Enable Tap-To-Unlock	Select whether to enable the Tap-To-Unlock function.
Not Enabled Time	After enabled, you can set the time period for not enabling Tap-To-Unlock on

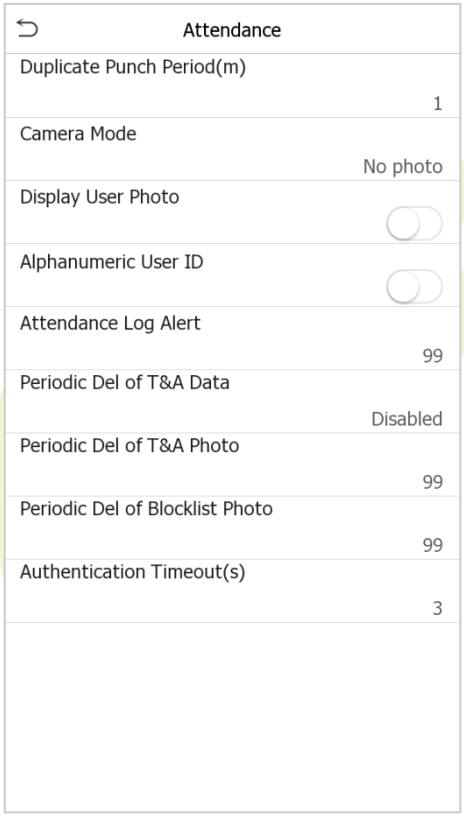
Period	the device.

6.3 Access Log Setting/Attendance

Click **Access Logs Setting/Attendance** on the System interface.



A&C Terminal



T&A Terminal

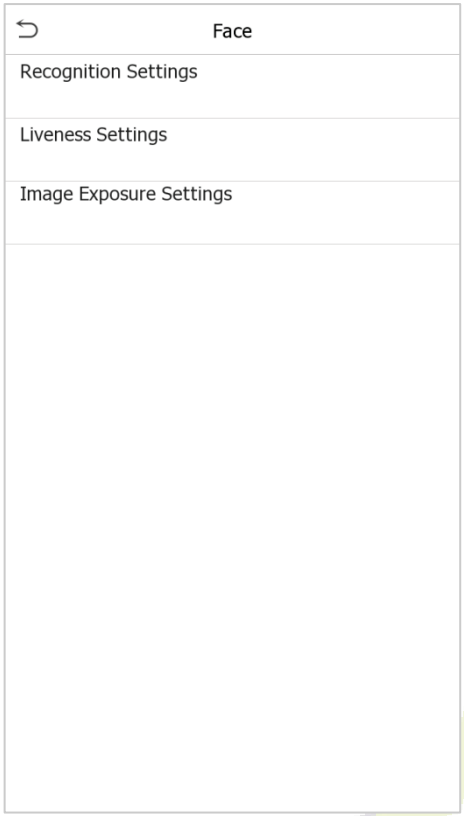
Function Description:

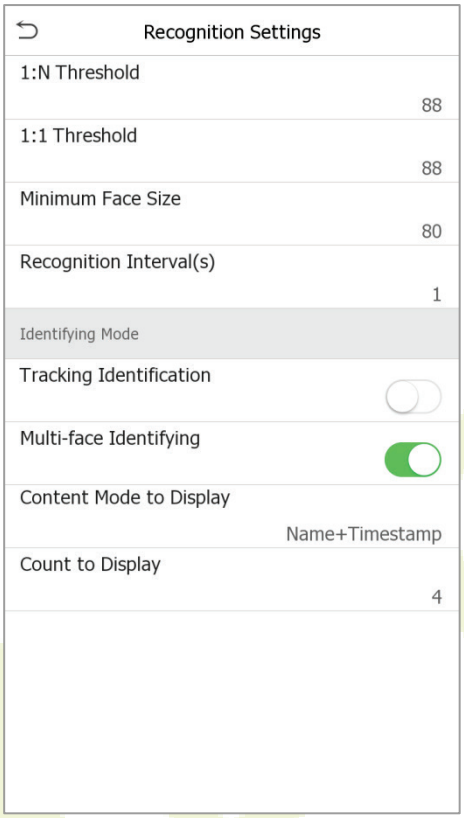
Function Name	Description
Duplicate Punch Period(m)	Within a set time period (unit: minutes), the duplicated attendance record will not be reserved (value ranges from 1 to 999999 minutes).

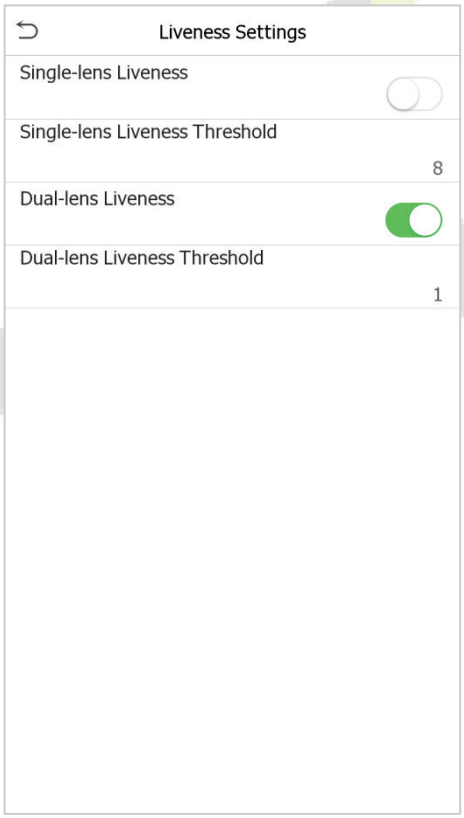
Camera Mode	This function is disabled by default. When enabled, a security prompt will pop-up and the sound of shutter in the camera will turn on mandatorily. There are 5 modes: **No Photo:** No photo is taken during user verification. **Take photo, no save:** Photo is taken but not saved during verification. **Take photo and save:** All the photos taken during verification is saved. **Save on successful verification:** Photo is taken and saved for each successful verification. **Save on failed verification:** Photo is taken and saved only for each failed verification.
Display User Photo	This function is disabled by default. When enabled, a security prompt will pop-up.
Alphanumeric User ID	Whether to support letters in employee ID.
Access/Attendance Log Alert	When the record space of the attendance/access reaches the maximum threshold value, the device automatically displays the memory space warning. Users may disable the function or set a valid value between 1 and 9999.
Periodic Del of Access Logs/T&A Data	When access/attendance logs reach its maximum capacity, the device automatically deletes a set of old access/attendance logs. Users may disable the function or set a valid value between 1 and 999.
Periodic Del of T&A Photo	When attendance photos reach its maximum capacity, the device automatically deletes a set of old attendance photos. Users may disable the function or set a valid value between 1 and 99.
Periodic Del of Blocklist Photo	When block listed photos reach its maximum capacity, the device automatically deletes a set of old block listed photos. Users may disable the function or set a valid value between 1 and 99.
Authentication Timeout(s)	The amount of time taken to display a successful verification message. Valid value: 1 to 9 seconds.

6.4 Face Parameters

Click **Face** on the System interface.







Function Name	Description	
Recognition Settings	**1: N Threshold:** The verification will be successful only if the similarity between the acquired facial image and all registered facial templates is greater than the set value in the 1: N verification mode. The valid value ranges from 0 to 100. The higher the thresholds, the lower the misjudgement rate and higher is the rejection rate, and vice versa. It is recommended to set the default value of 88.	
	1:1 Threshold: 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 misjudgement rate and the higher is the rejection rate, and vice versa. It is recommended to set the default value of 88.	
	Minimum Face Size: It sets the minimum face size required for facial registration and comparison. If the minimum size of the captured image is smaller than the set value, then it will be filtered off and not recognized as a face. This value can also be interpreted as the face comparison distance. The farther the individual is, the smaller the face, and the smaller number of pixels of the face obtained by the algorithm. Therefore, adjusting this parameter can adjust the farthest comparison of distance of faces. When the value is 0, the face comparison distance is not limited.	
	Recognition Interval(s): If the recognition interval is set to 5 seconds, then the face recognition will verify the face every 5 seconds. Valid value: 0 to 9 seconds. 0 means continuous identifying, 1 to 9 means identifying at intervals.	
	Identifying Mode	**Tracking Identification:** The same face can only be recognized once. To recognize it again, you must leave the face recognition area and re-enter it before it can be recognized again.

		Multi-face Identifying★: When it is toggled on, the device can identify multiple faces at once. The **Content Mode to Display**, and **Count to Display** can be configured only if it is toggled on. **Content Mode to Display:** You can select the content displayed below the user photo in the interface after the face verification is successful. Such as only display the **User ID**, display the **Name**, display the **User ID + Name**, display **Timestamp**, display **User ID + Timestamp**, display **Name + Timestamp**. **Count to Display:** You can choose the number of face verification results to be displayed in the interface at once, e.g., if set to 3, the interface displays up to 3 successful user verifications at once. **Note:** The **Count to Display** can be set from 1 to 4 users.
Liveness Settings		**Single-lens Liveness:** It uses visible light images to detect spoofing attempts and assess whether the biometric source sample provided is of a real person (a live human being) or a false representation. **Single-lens Liveness Threshold:** It facilitates judging whether the captured visible image is of a real person (a live human being). The larger the value, the better the anti-spoofing performance using visible light. **Dual-lens Liveness:** It uses near-infrared spectra imaging to identify and prevent fake photos and video attacks. **Dual-lens Liveness Threshold:** It is convenient to judge whether the near-infrared spectral imaging is a fake photo and video. The larger the value, the better the anti-spoofing performance of near-infrared spectral imaging. **Note:** Single-lens Liveness and Dual-lens Liveness are mutually exclusive options. Enabling Single-lens Liveness will automatically disable Dual-lens Liveness, and vice versa. When the option is turned on or off, the device reboots automatically to execute the function.
Image Exposure Settings		**Face AE:** When the face is in front of the camera in Face AE mode, the brightness of the face area increases, while other areas become darker. **WDR:** 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. **Anti-flicker Mode:** It is used when WDR is turned off. It helps to reduce flicker when the device's screen flashes at the same frequency as the light.

Note:

1) 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.

2) Face AE and Multi-face identifying are mutually exclusive options. When the Multi-face identifying feature switch is turned on, the Face AE switch will be automatically turned off. If you turn on Face AE at this time, the recognition mode will change to single face recognition mode.

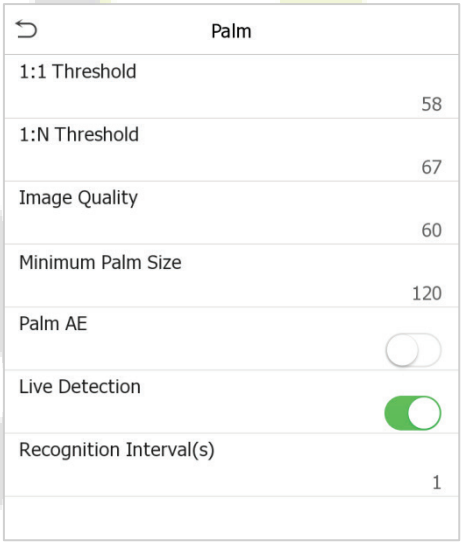
3) The Recognition interval and Tracking identification are mutually exclusive options. If the Tracking identification switch is turned on, the Recognition interval function in the Recognition Settings will be disabled, and vice versa.

Process to modify the Facial Recognition Accuracy

- On the **System** interface, tap on **Face > Liveness Settings** and then toggle to enable **Single-lens Liveness** or **Dual-lens Liveness**.
- Then, on the **Main Menu**, tap **Autotest > Test Face** and perform the face test.
- Tap three times for the scores on the left upper corner of the screen, and the red rectangular box appears to start adjusting the mode.
- Keep one arm distance between the device and the face. It is recommended not to move the face in a wide range.

6.5 Palm Parameters★

Click **Palm** on the System interface.

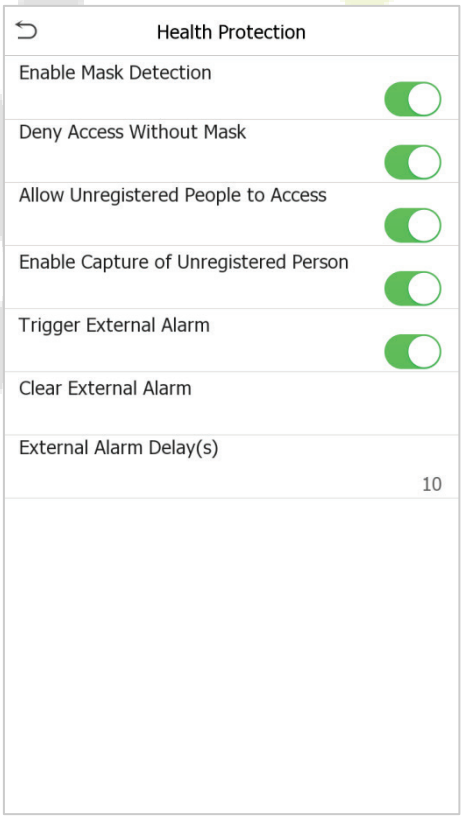


Menu	Description
1:1 Threshold	Under 1:1 Verification Method, only when the similarity between the verifying palm and the user's registered palm is greater than this value, the verification succeeds.
1:N Threshold	Under 1:N Verification Method, only when the similarity between the verifying palm and all registered palm is greater than this value, the verification succeeds.
Image Quality	Image quality for palm registration and comparison. The higher the value, the

	clearer the image requires.
Minimum Palm Size	The minimum palm size is used to limit the palm size recognized by the device, thereby eliminating background interference or misjudgment. This parameter is usually related to the distance from the camera to the palm. This value can be understood as the palm comparison distance. The farther the person is, the smaller the palm is, and the smaller the palm pixel will be obtained by the algorithm. Therefore, adjusting this parameter can adjust the furthest comparison distance of palms. When the value is 0, the palm comparison distance is not limited.
Palm AE	Palm Auto Exposure, when the palm is in front of the camera in Palm AE mode, the brightness of the palm area increases, while other areas become darker.
Live Detection	It detects the spoof attempt using visible light images to determine if the provided biometric source sample is of a real person (a live human being) or a false representation.
Recognition Interval(s)	If the comparison interval is set to 5 seconds, then the palm recognition will verify the palm every 5 seconds. Valid value: 0 to 9 seconds. 0 means continuous identifying, 1 to 9 means identifying at intervals.

6.6 Health Protection

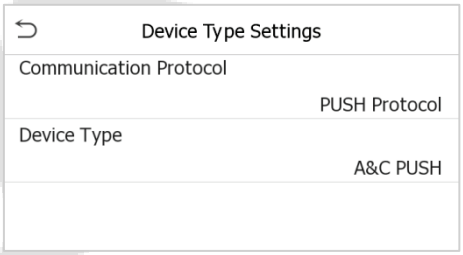
Click **Health Protection** on the System interface.



Function Name	Description
Enable Mask Detection	It enables or disables the mask detection function. When enabled, the device identifies whether the user is wearing a mask or not during verification.
Deny Access Without Mask	It enables or disables the access of a person without mask. When enabled, the device denies access of a person, if not wearing a mask.
Allow Unregistered People to Access	It enables or disables the access of unregistered person. When enabled, the device allows the person to enter without registration.
Enable Capture of Unregistered Person	To enable or disable capturing the unregistered person. When enabled, the device will automatically capture the photo of the unregistered person, enabling this feature requires to enable **Allow Unregistered People to Access**.
Trigger External Alarm	When enabled, if the user is not wearing a mask, the system will trigger an alarm.
Clear External Alarm	It clears the triggered alarm records of the device.
External Alarm Delay(s)	It is the delay(s) time for triggering an external alarm. It can be set in seconds. Users may disable the function or set a value between1 to 255.

6.7 Device Type Settings

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

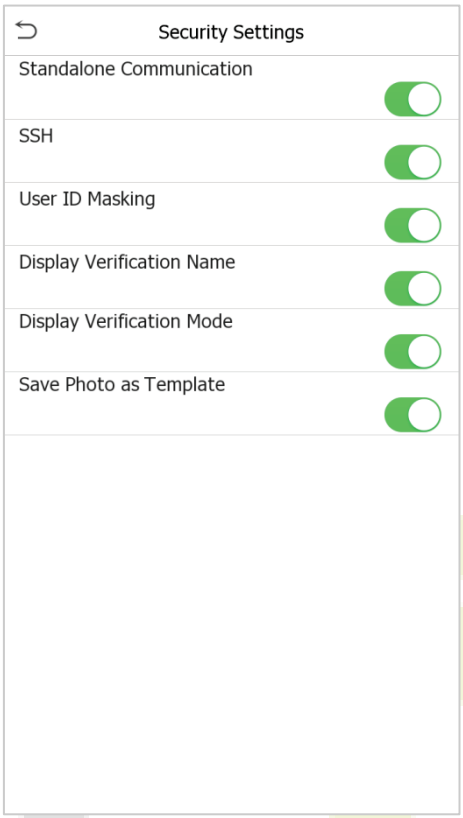


Function Name	Description
Communication Protocol	Set the device communication protocol, PUSH Protocol or BEST protocol. (BEST protocol is managed by ZKBio Zlink, please refer to 17 Connecting to ZKBio Zlink Mobile App and 18 Connecting to ZKBio Zlink Web Portal.)
Device Type	When the communication protocol is PUSH Protocol, you can set the device as time attendance terminal (T&A PUSH) or access control terminal (A&C PUSH).

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

6.8 Security Settings

Tap **Security Settings** on the **System** interface.

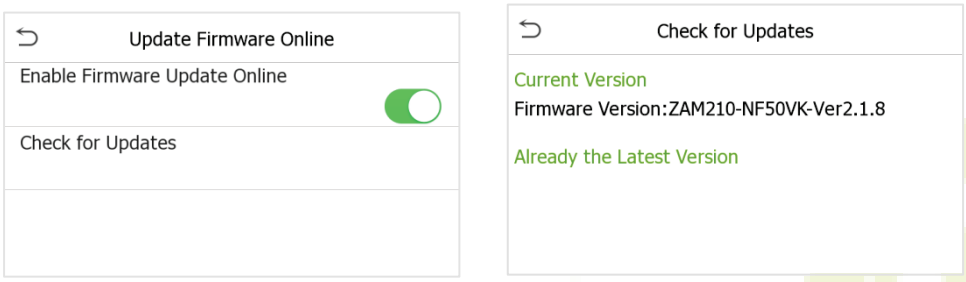


Function Name	Description
Standalone Communication	By default, this function is disabled. This function can be enabled or disabled via the menu interface. It is used to connect the C/S software. When it is switched on, a security prompt appears, and the device will restart after you confirm.
SSH	The device does not support the Telnet feature, hence SSH is typically used for remote debugging. By default, SSH is enabled. The menu interface allows you to enable and disable SSH. When enabled, there will be a security prompt, but the device will not need to be restarted after confirmation.
User ID Masking	After enabled, the User ID will be partially displayed after the personnel verification result (only the User ID with more than 2 digits supports the masking display), and it is enabled by default.
Display Verification Name	After enabled, the user's name will be displayed after the personnel verification result. The verification result will not show the name after disabling it.
Display Verification Mode	After enabled, the personnel verification result will show the user's verification mode. The verification result will not show the verification mode after you disable it.
Save Photo as Template	After disabling this function, face template re-registration is required after an algorithm upgrade.

6.9 Update Firmware Online

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

Click **Enable Firmware Update Online** function, the device will prompt that the update may bring some data security risks, which requires manual confirmation by the user (If the security setting function is turned off, the risk warning will not be displayed when the online update is turned on).



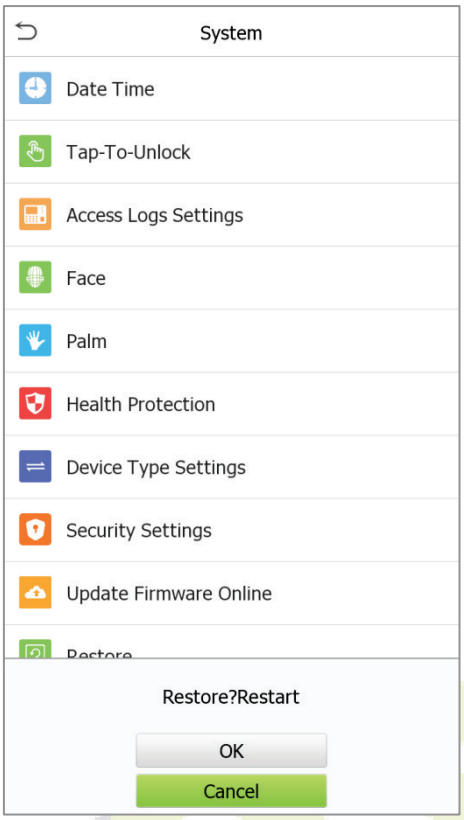
Click **Check for Updates** it may have the following 3 scenarios:

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

6.10 Factory Restore

This option restores the device, such as communication settings and system settings, to factory settings (does not clear registered user data).

Click **Restore** on the System interface.

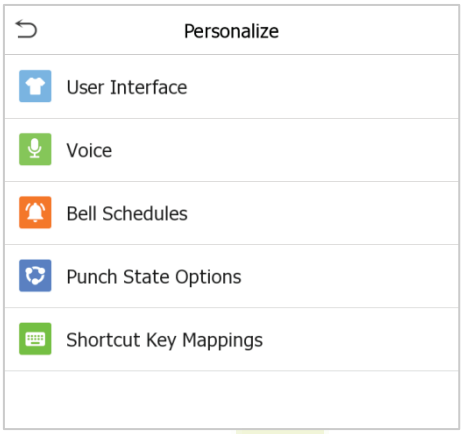


Click **OK** to restore.

7 Personalize Settings

You may customize the interface settings, audio, bell, punch state options and shortcut key mappings.

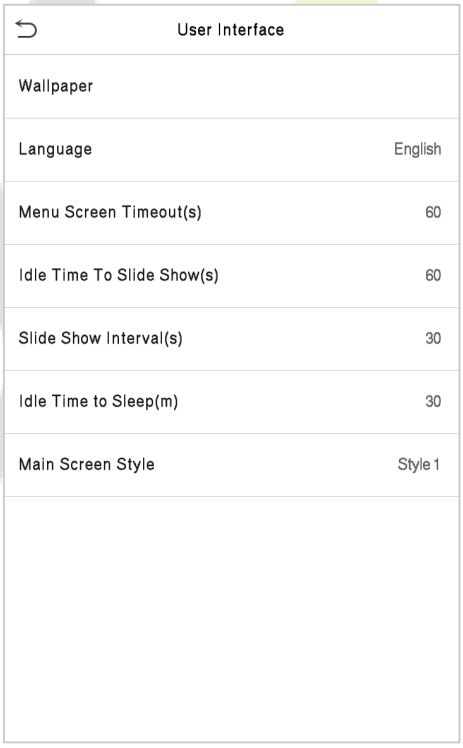
Click **Personalize** on the main menu interface.



7.1 Interface Settings

You can customize the display style of the main interface.

Click **User Interface** on the Personalize interface.

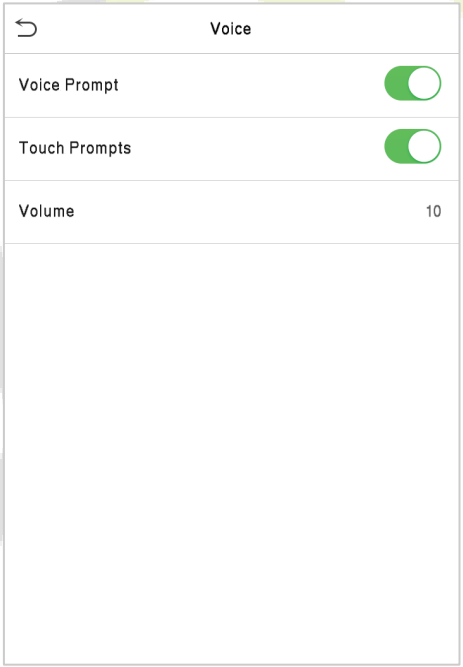


Menu	Description
Wallpaper	To select the main screen wallpaper according to your personal preference.

Language	To select the language of the device.
Menu Screen Timeout (s)	When there is no operation, and the time exceeds the set value, the device will automatically go back to the initial interface. You can disable the function or set the value between 60 and 99999 seconds.
Idle Time To Slide Show (s)	When there is no operation, and the time exceeds the set value, a slide show will be played. It can be disabled, or you may set the value between 3 and 999 seconds.
Slide Show Interval (s)	This refers to the time interval switching different slide show pictures. The function can be disabled, or you may set the interval between 3 and 999 seconds.
Idle Time To Sleep (m)	If you have activated the sleep mode, when there is no operation, the device will enter the standby mode. You can disable this function or set a value within 1-999 minutes.
Main Screen Style	To select the main screen style according to your personal preference.

7.2 Voice Settings

Click **Voice** on the Personalize interface.



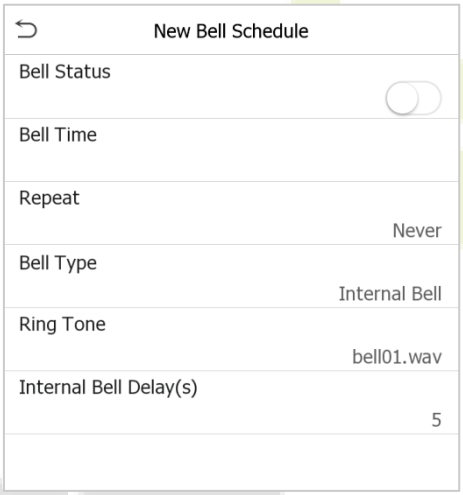
Menu	Description
Voice Prompt	Select whether to enable voice prompts during operation.
Touch Prompt	Select whether to enable keypad sounds.
Volume	Adjust the volume of the device; valid value: 0 to 100.

7.3 Bell Schedules

Click **Bell Schedules** on the Personalize interface.

Add a Bell

1. Click **New Bell Schedule** to enter the adding interface:



Menu	Description
Bell Status	Set whether to enable the bell status.
Bell Time	At this time of day, the device automatically rings the bell.
Repeat	Set the repetition cycle of the bell.
Bell Type★	Select the bell type: Internal Bell, External Bell or Internal and External Bell.
Ring Tone	Select a ring tone.
Internal bell delay(s)	Set the duration of the internal bell. Valid values range from 1 to 999 seconds.

2. Back to the Bell Schedules interface; click **All Bell Schedules** to view the newly added bell.

Edit a Bell

On the All Bell Schedules interface, click the bell to be edited.

Click **Edit**, the editing method is the same as the operations of adding a bell.

Delete a Bell

On the All Bell Schedules interface, click the bell to be deleted.

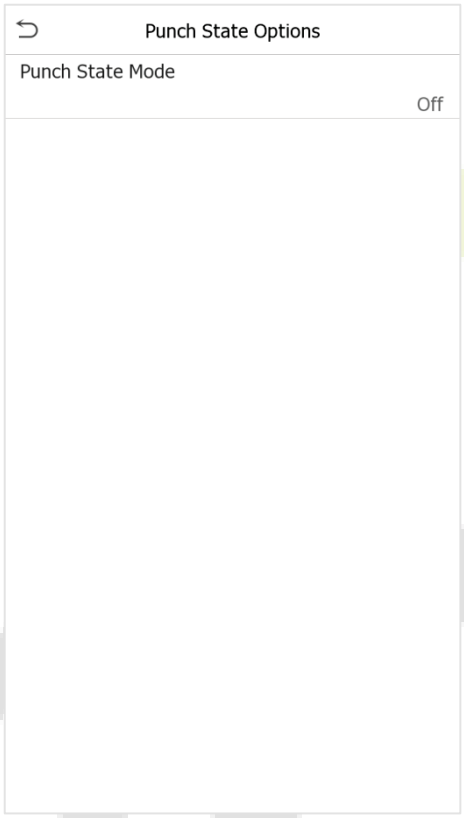
Click **Delete** and select [**Yes**] to delete the bell.

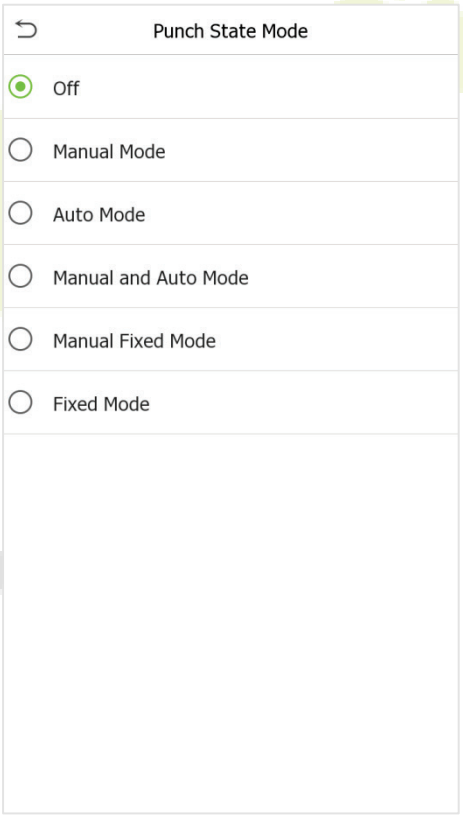
Options★

Tap **Options** on the Bell Schedule interface to set the external bell output terminal NC1 or NC2, which can be disabled.

7.4 Punch States Options

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





Function Description

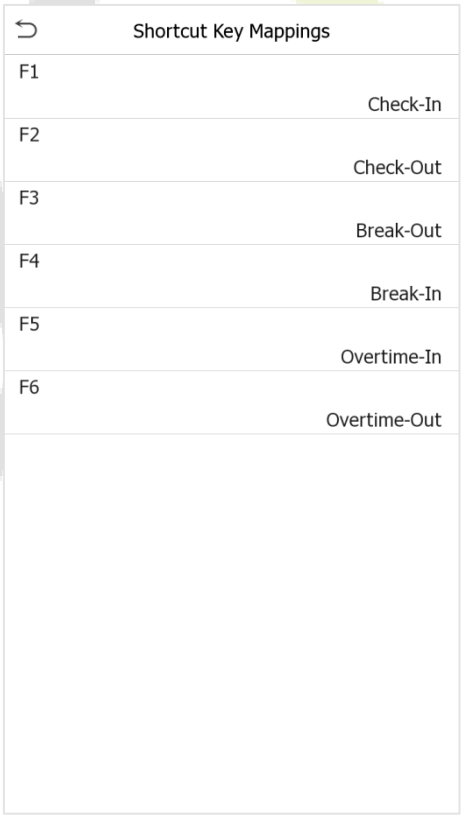
Function Name	Description
Punch State Mode	**Off:** Disable the punch state function. Therefore, the punch state key set under **Shortcut Key Mappings** menu will become invalid. **Manual Mode:** Switch the punch state key manually, and the punch state key will disappear after **Punch State Timeout**. **Auto Mode:** The punch state key will automatically switch to a specific punch status according to the predefined time schedule which can be set in the Shortcut Key Mappings. **Manual and Auto Mode:** The main interface will display the auto-switch

	punch state key. However, the users will still be able to select alternative that is the manual attendance status. After timeout, the manual switching punch state key will become auto-switch punch state key. **Manual Fixed Mode:** After the punch state key is set manually to a particular punch status, the function will remain unchanged until being manually switched again. **Fixed Mode:** Only the manually fixed punch state key will be shown. Users cannot change the status by pressing any other keys.
Punch State Timeout(s)	It is the time for which the punch state displays. The value ranges from 5 to 999 seconds.
Punch State Required	Select whether an attendance state needs to be selected after verification. **ON:** Attendance state needs to be selected after verification. **OFF:** Attendance state need not requires to be selected after verification.

7.5 Shortcut Key Mappings

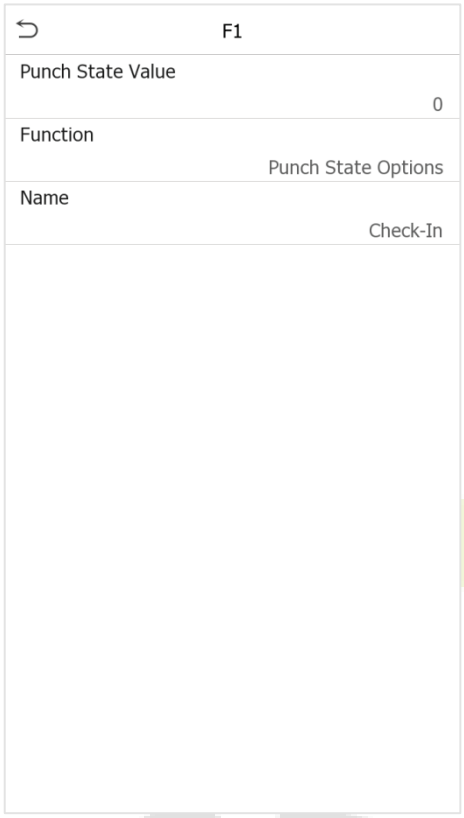
Users may define shortcut keys for attendance status and for functional keys which will be defined on the main interface. So, on the main interface, when the shortcut keys are pressed, the corresponding attendance status or the function interface will be displayed directly.

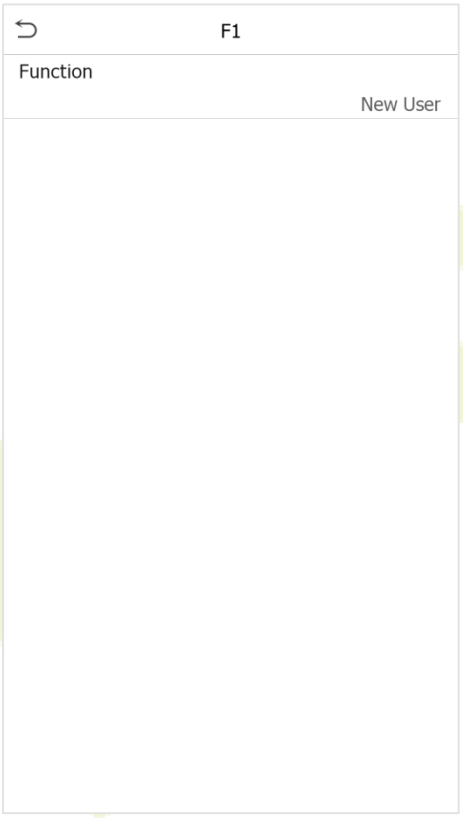
Tap **Shortcut Key Mappings** on the **Personalize** interface to set the required shortcut keys.



- On the **Shortcut Key Mappings** interface, tap on the required shortcut key to configure the shortcut key settings.

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



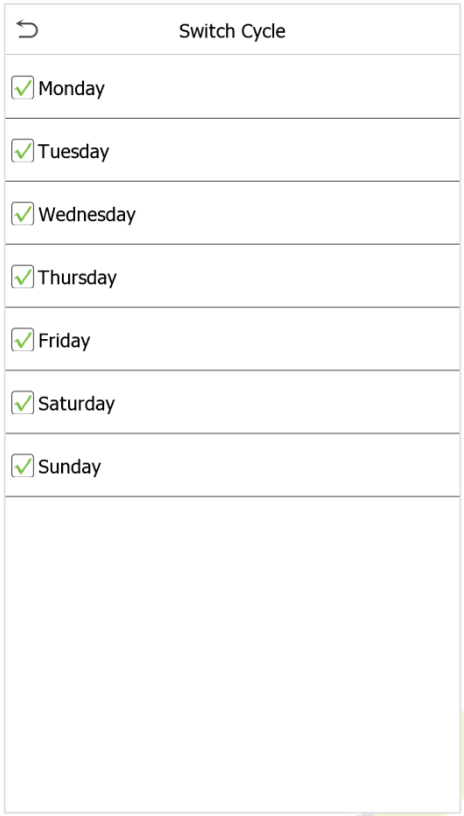


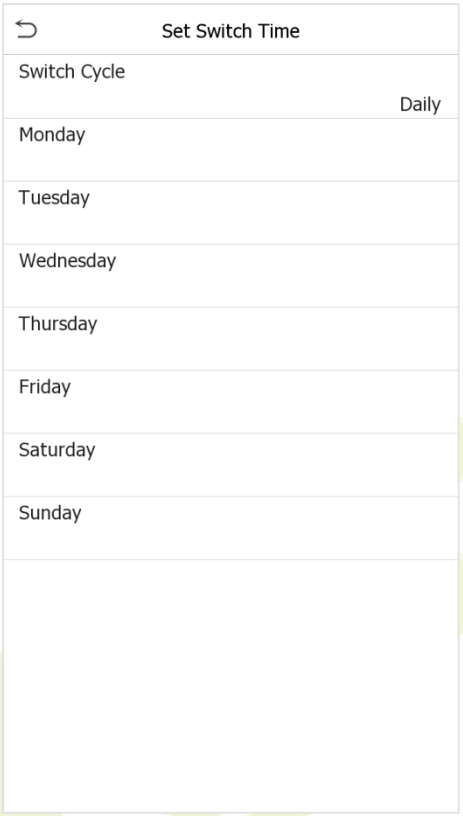
- If the Shortcut key is set as a punch state key (such as check in, check out, etc.), then it is required to set the punch state value (valid value 0~250), name.

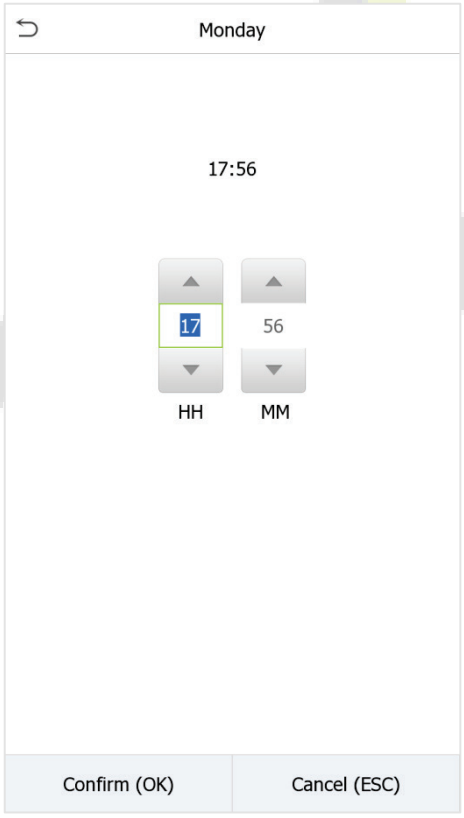
Note: *When the function is set to Undefined, the device will not enable the punch state key.*

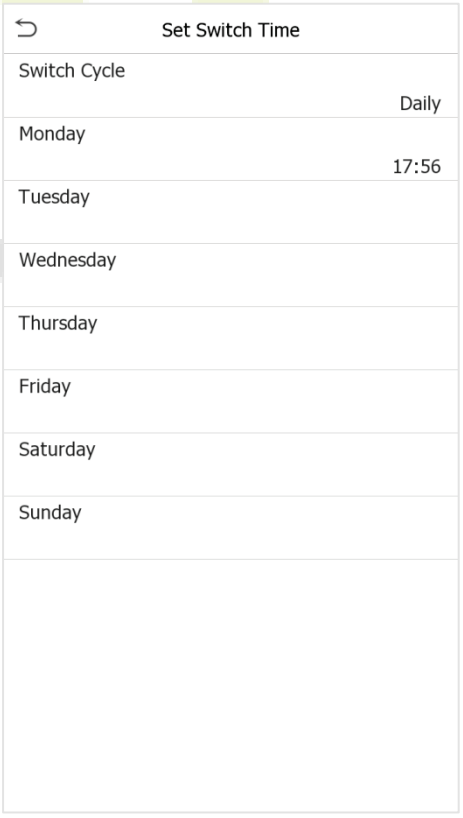
➢ **Set the Switch Time**

- The switch time is set in accordance with the punch state options.
- On the **Punch States Options** interface, when the **punch state mode** is set to **auto mode**, the switch time should be set.
- On the **Shortcut Key** interface, tap **Set Switch Time** to set the switch time.
- On the **Switch Cycle** interface, select the switch cycle (Monday, Tuesday etc.) as shown in the image below.
- Once the Switch cycle is selected, set the switch time for each day and tap **OK** to confirm, as shown in the image below.





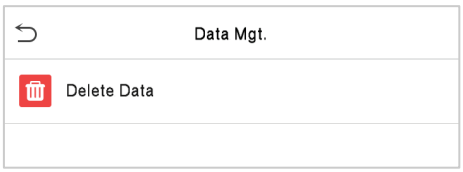




8 Data Management

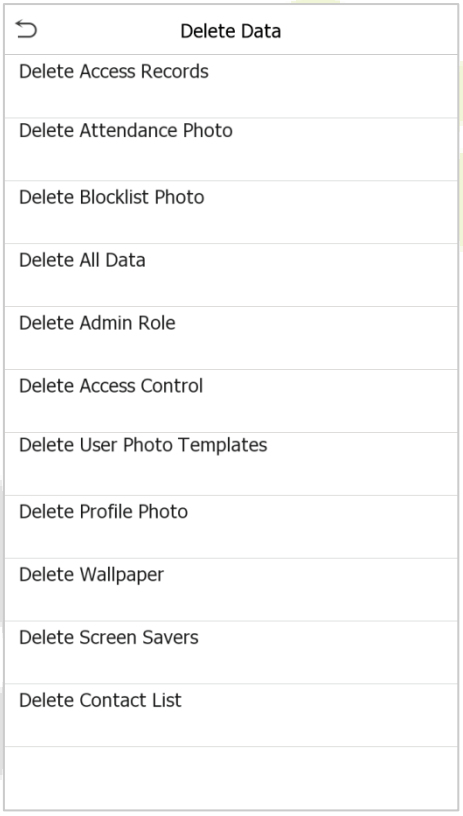
The Data Management is used to delete the relevant data in the device.

Click **Data Mgt.** on the main menu interface.



8.1 Delete Data

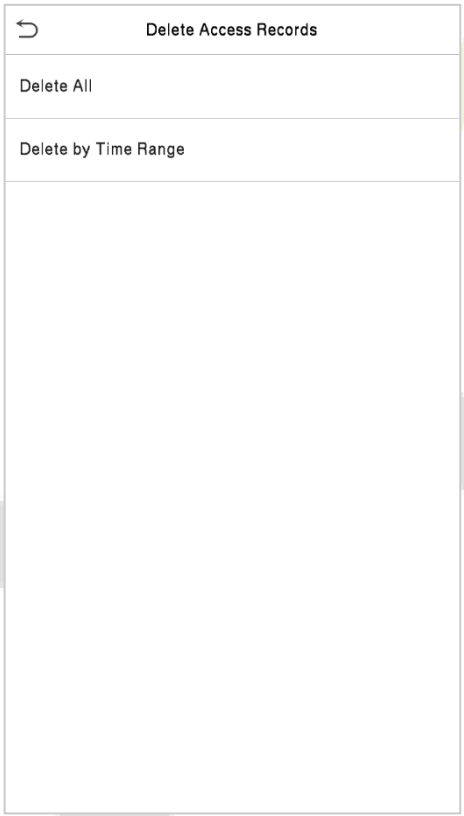
Click **Delete Data** on the Data Mgt. interface.



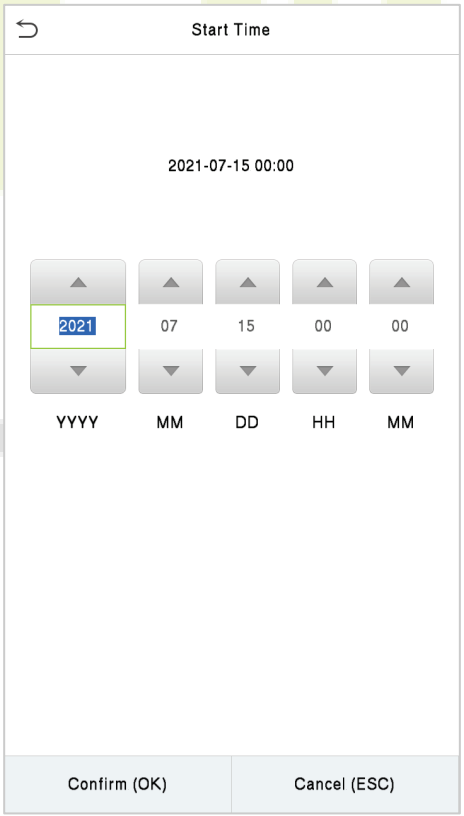
Function Name	Description
Delete Access Records/Attendance Data	To delete attendance data/access records conditionally.
Delete Attendance Photo	To delete attendance photos of designated personnel.
Delete Blocklist Photo	To delete the photos taken during failed verifications.
Delete All Data	To delete information and attendance logs/access records of all registered users.

Delete Admin Role	To remove all administrator privileges.
Delete Access Control	To delete all access data.
Delete User Photo Templates	To delete user photo templates in the device. When deleting template photos, there is a risk reminder: "**Face re-registration is required after an algorithm upgrade.**"
Delete Profile Photo	To delete all user photos on the device.
Delete Wallpaper	To delete all wallpapers in the device.
Delete Screen Savers	To delete the screen savers in the device.
Delete Contact List★	To delete all contact list of video intercom in the device.

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



Select **Delete by Time Range**.



Set the time range and click **OK**.

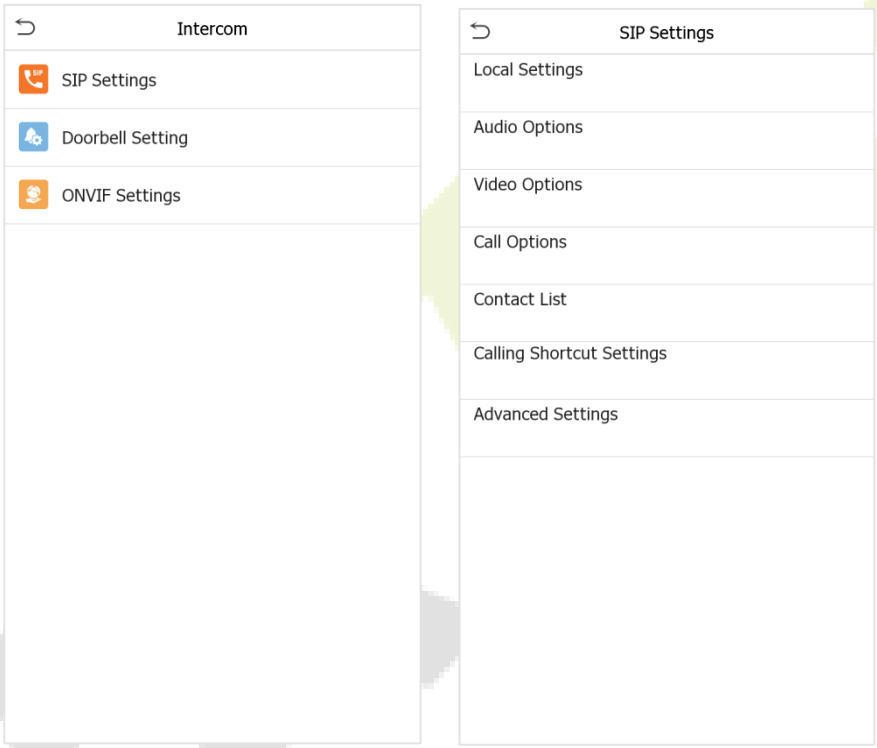
9 Intercom★

On the **Main Menu**, tap **Intercom** to set relevant parameters of intercom, including SIP, Doorbell and ONVIF Settings.

The device achieves video intercom there are two modes, respectively, the LAN and SIP server. For more details, please refer to 16 SIP Video Intercom.

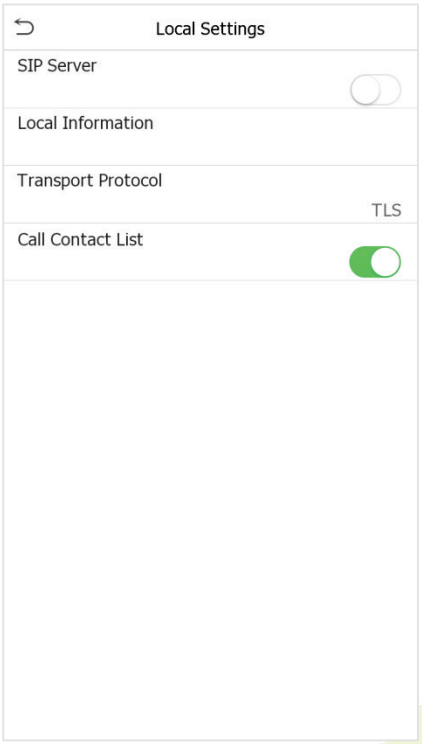
9.1 SIP Settings

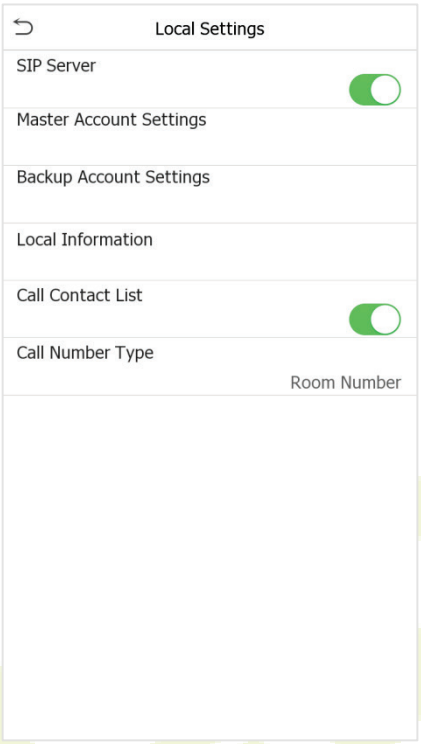
Tap **SIP Settings** on the **Intercom** interface to configure the settings.



9.1.1 Local Settings

Tap **Local Settings** on the **SIP Settings** interface.





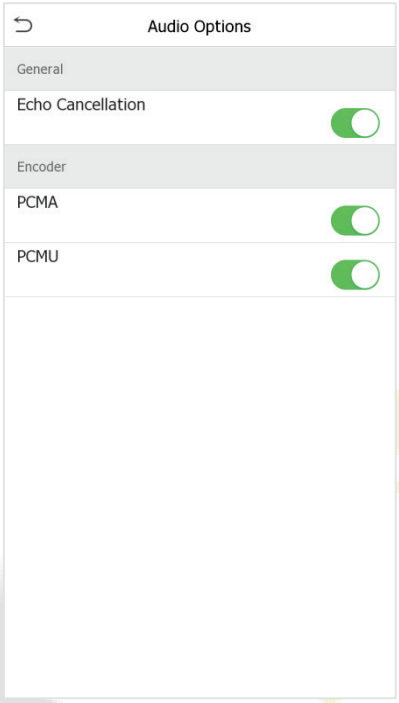
Function Description

Function Name	Description
SIP Server	Select whether to enable the SIP server. When it is enabled, the SIP account needs to be set. **Note:** Every time this feature is turned on or off, the contact list will be reset.
Master Account Settings	After assigning the SIP account to the device on the ZKBio CVAccess, the account information will be automatically synchronized to the device. You don't need to configure it manually.
Backup Account Settings	Select whether to enable the backup account settings.
Local Information	**Device Type:** Set the device type as **Entrance Station** or **Fence Terminal**. And set the specific location information of the device, including the block, unit (can be disabled), and room number. When it is set as Fence Terminal, the call page will display block, unit and room number. **Note:** The contact list will be cleared after changing the device type.
Transport Protocol	Set the transport protocol between the device and indoor monitor.
Call Contact List	Select whether to enable the contact list on the call page. When it is enabled, you can click the  icon to open the contact list on the call page.

Call Number Type	**Room Number:** The device can call the extension number (short number) or room number. **SIP Account Number:** The device can only call the SIP account.

9.1.2 Audio Options

Tap **Audio Options** on the **SIP Settings** interface.

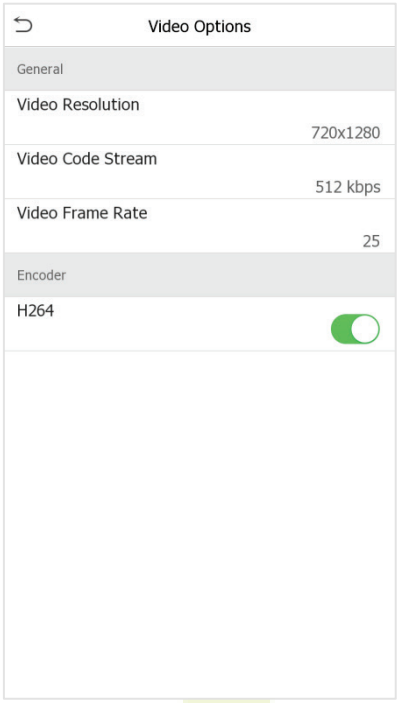


Echo Cancellation: Select whether to enable the echo cancellation. It is used to eliminate echoes caused by sound returning from the speaker to the microphone during a call.

Encoder: Select the audio encoder for intercom. Both PCMU and PCMA provide better voice quality, but they take up more bandwidth, requiring 64kbps.

9.1.3 Video Options

Tap **Video Options** on the **SIP Settings** interface.

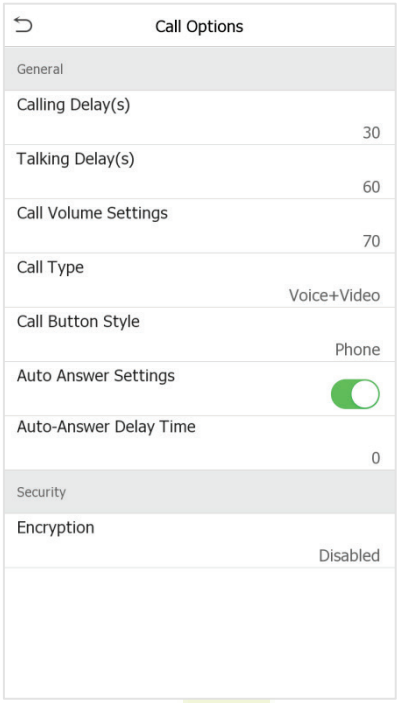


Function Description

Function Name	Description
Video Resolution	Select the video resolution of the intercom, 720 x 1280 or 600 x 600. It is 720 x 1280 by default..
Video Code Stream	Select the video code stream of the intercom, the larger the value, the higher the picture and sound quality of the video, and the greater the network requirements.
Video Frame Rate	Refers to the number of frames per second of the intercom video display, the larger the value the smoother, the device defaults to 25Hz, does not support modification.
Encoder	Whether to enable H264 Encoder.

9.1.4 Call Options

Tap **Call Options** on the **SIP Settings** interface.



Function Description

Function Name	Description
Calling Delay(s)	Set the time of call, valid value 30 to 60 seconds.
Talking Delay(s)	Set the time of intercom, valid value 60 to 120 seconds. It is suggested to set as 60s.
Call Volume Settings	Set the volume of the call, with valid value ranging from 0 to 100.
Call Type	Set the call type to Voice only or Voice+Video.
Call Button Style	Change the visual intercom call button on the standby interface of the device, optional doorbell label or phone label .
Auto Answer Settings	Select whether to enable the auto answer function. When it is enabled, the device will automatically answer if the indoor monitor calls.
Auto-Answer Delay Time	The device will automatically answer after the set delay time if the indoor monitor calls, valid value 0 to 10 seconds.

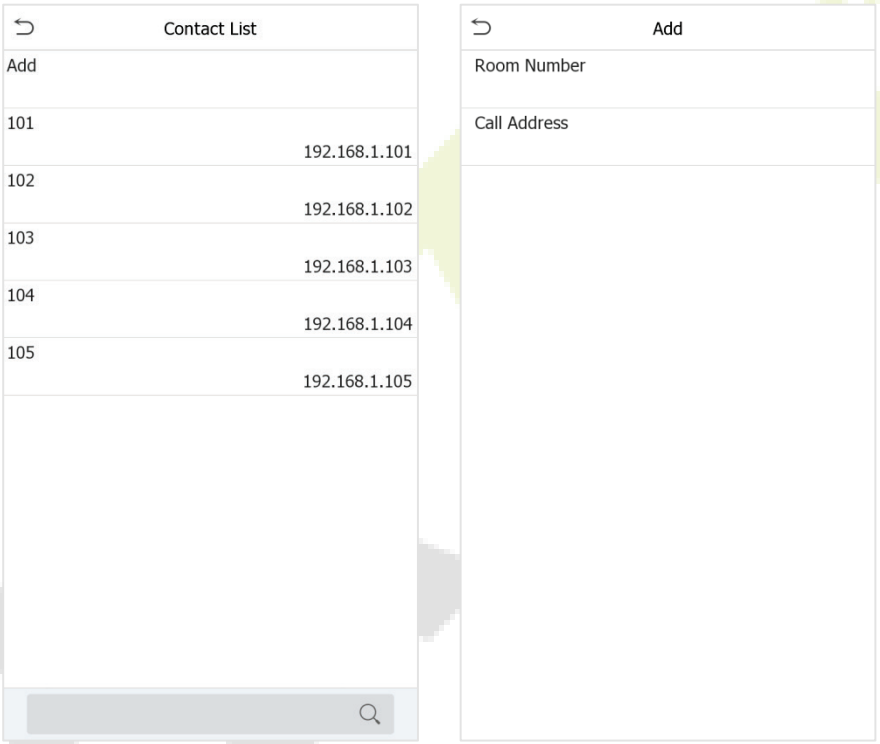
Encryption	It is disabled by default.

9.1.5 Contact List

Tap **Contact List** on the **SIP Settings** interface.

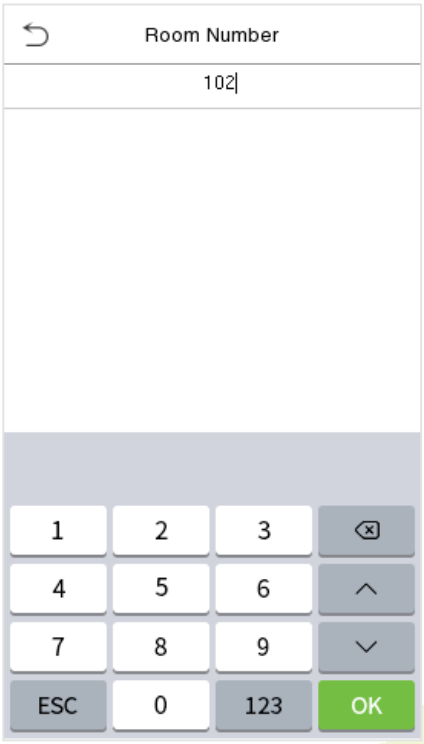
In SIP Server mode, the contact list is synchronized by the ZKBio CVAccess Server to the device. The contact list can only be viewed, cannot be edited. When the SIP server is disabled, the room number and call address of the indoor monitors can be added here.

Click **Add** to enter the Add Contact List interface.



- **Room Number:** Customize the number of the indoor monitor.

When the device type is set as **Entrance Station**, the room number can be 1~ 4 digits. When the device type is set as **Fence Terminal**, you need to input the block, unit and room number. For example, if the indoor monitor is in Block 3, Unit 2, Room 2601, then input "03.02.2601".



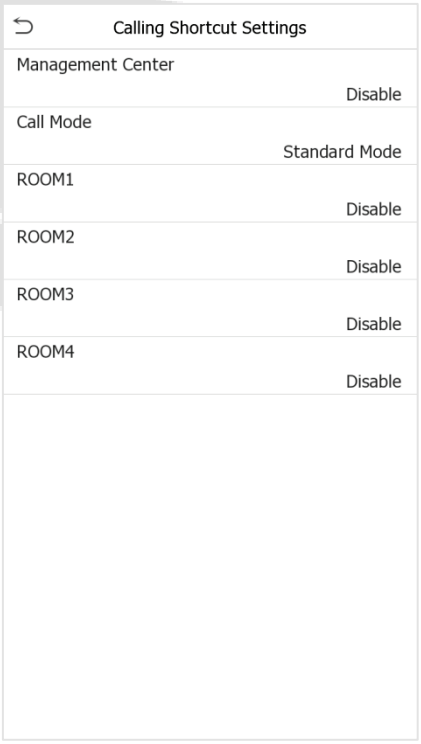
Entrance Station

Fence Terminal

- **Call Address:** It is the IP Address of the indoor monitor.

9.1.6 Calling Shortcut Settings

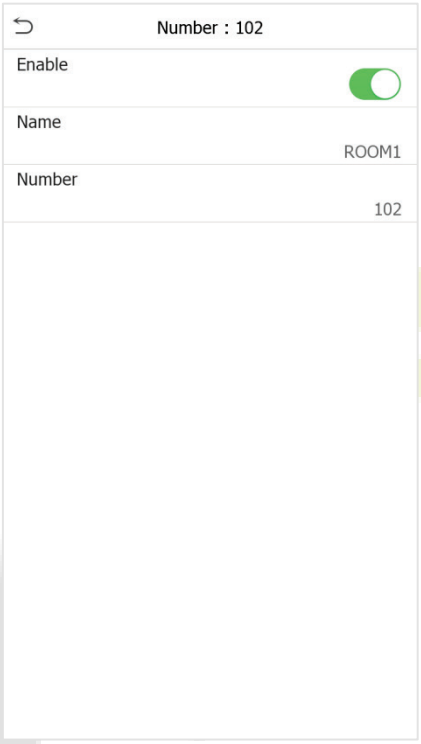
Tap **Calling Shortcut Settings** on the **SIP Settings** interface.



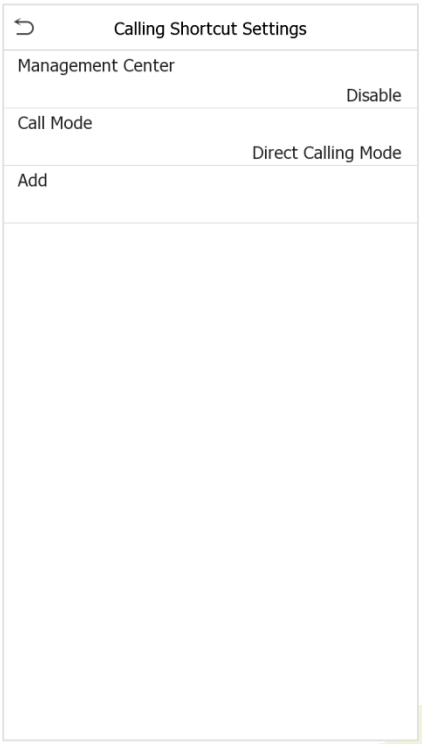
Management Center: Select whether to enable the Management Center and set its number. After enabling, you can click the  icon to directly call the admin on the call page.

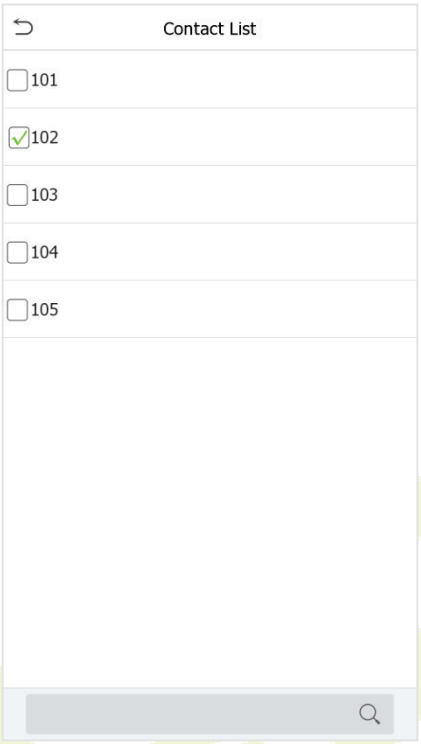
Call Mode: It can be set as **Standard Mode** or **Direct Calling Mode**.

- In Standard mode, there are **4** shortcut keys that can be enabled and defined in the device: **ROOM1**, **ROOM2, ROOM3** and **ROOM4**. You can set a shortcut key to call the indoor monitor quickly without entering the number of the indoor monitor each time.
  Name: Customize the name of the shortcut keys.
  Number: Select the room number that set in the **Contact List** Menu.



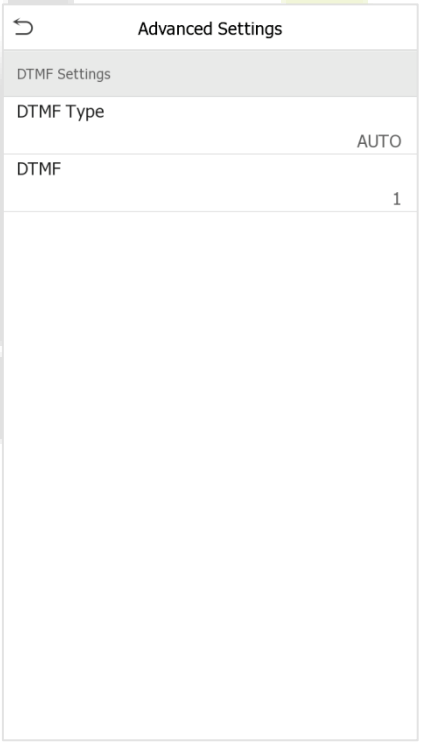
- In Direct Calling mode, the user can call multiple indoor monitors directly.
  Click **Call Mode > Direct Calling Mode> Add**, select the indoor monitors that you want to call, then the indoor monitors will be displayed in the list.





9.1.7 Advanced Settings

Tap **Advanced Settings** on the **SIP Settings** interface.

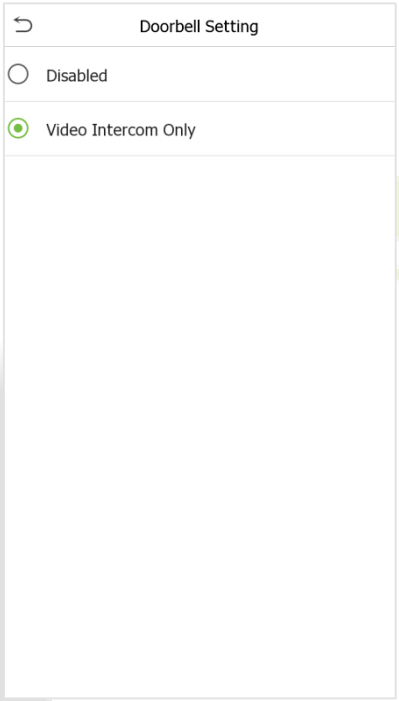


Function Description

Function Name	Description
DTMF Type	Set the DTMF type as AUTO, SIP INFO or RFC2833.
DTMF	The value should be set as same as the value of DTMF in the indoor monitor.

9.2 Doorbell Setting

Tap **Doorbell Setting** on the **Intercom** interface to set the doorbell.



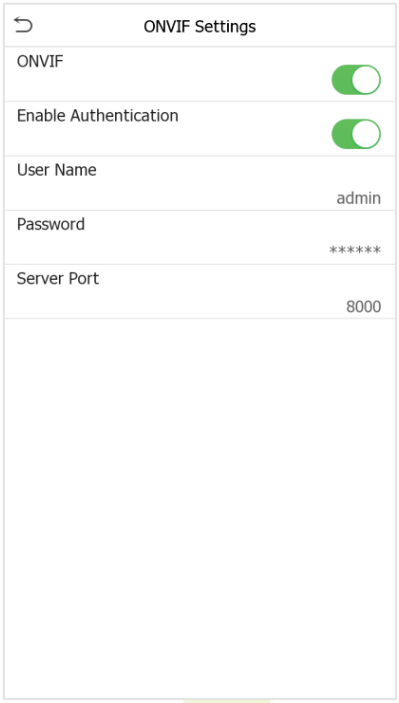
Function Description

Function Name	Description
Disabled	The doorbell button is disabled.
Video Intercom Only	Tap icon on standby interface of the device to make a call.

9.3 ONVIF Settings

Note: *This function needs to be used with the network video recorder (NVR).*

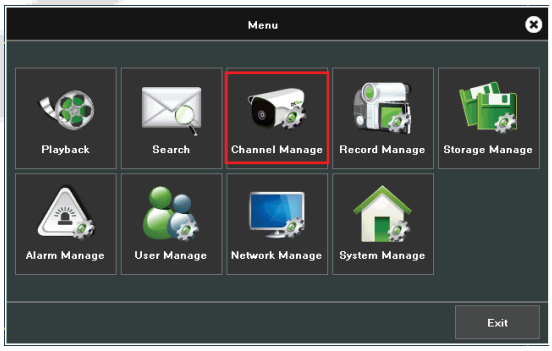
1. Set the device to the same network segment as the NVR.
2. Tap **ONVIF Settings** on the **Intercom** interface.



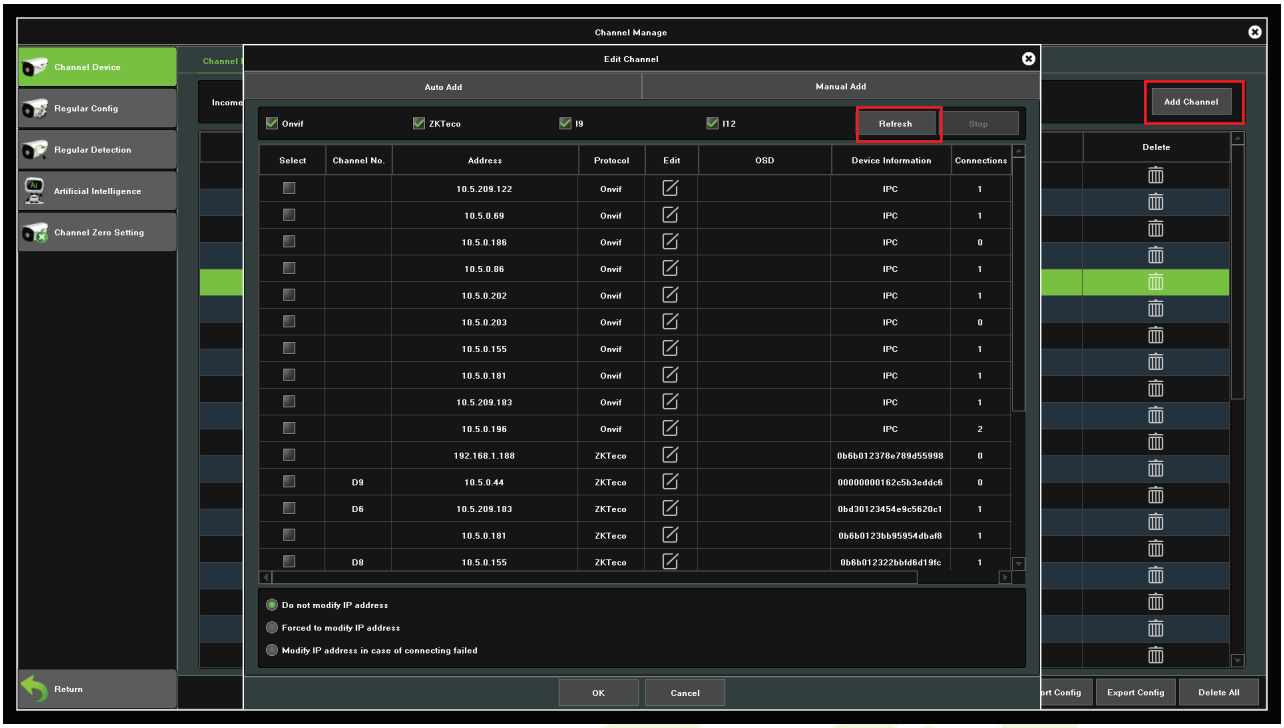
Function Description

Function Name	Description
ONVIF	Select whether to enable the ONVIF function.
Enable Authentication	Enable/Disable the Authentication Function. When it is disabled, there is no need to input the User Name and Password when adding the device to the NVR.
User Name	Set the User Name. The default is admin.
Password	Set the password. The default is admin@123.
Server Port	The default is 8000, and cannot be modified.

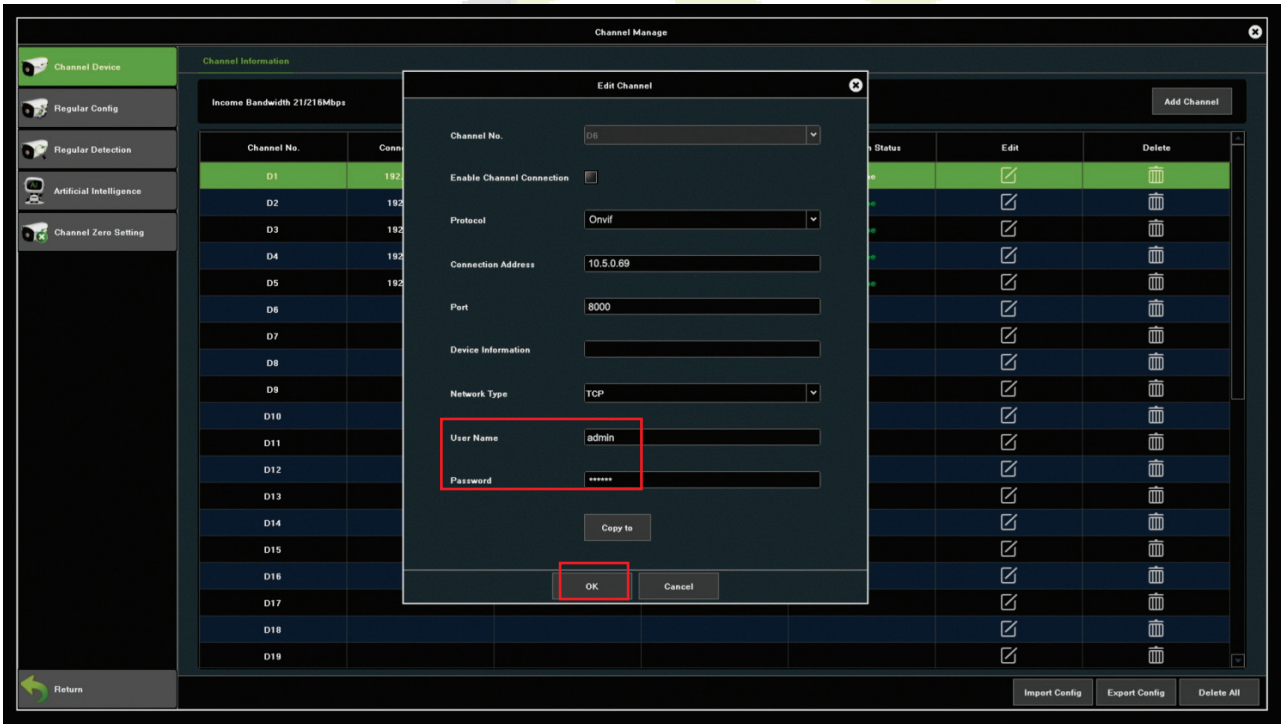
3. On the NVR system, click on [**Start**] > [**Menu**], then the main menu will pop up.



4. Click [**Channel Manage**] > [**Add Channel**] > [**Refresh**] to search for the device.

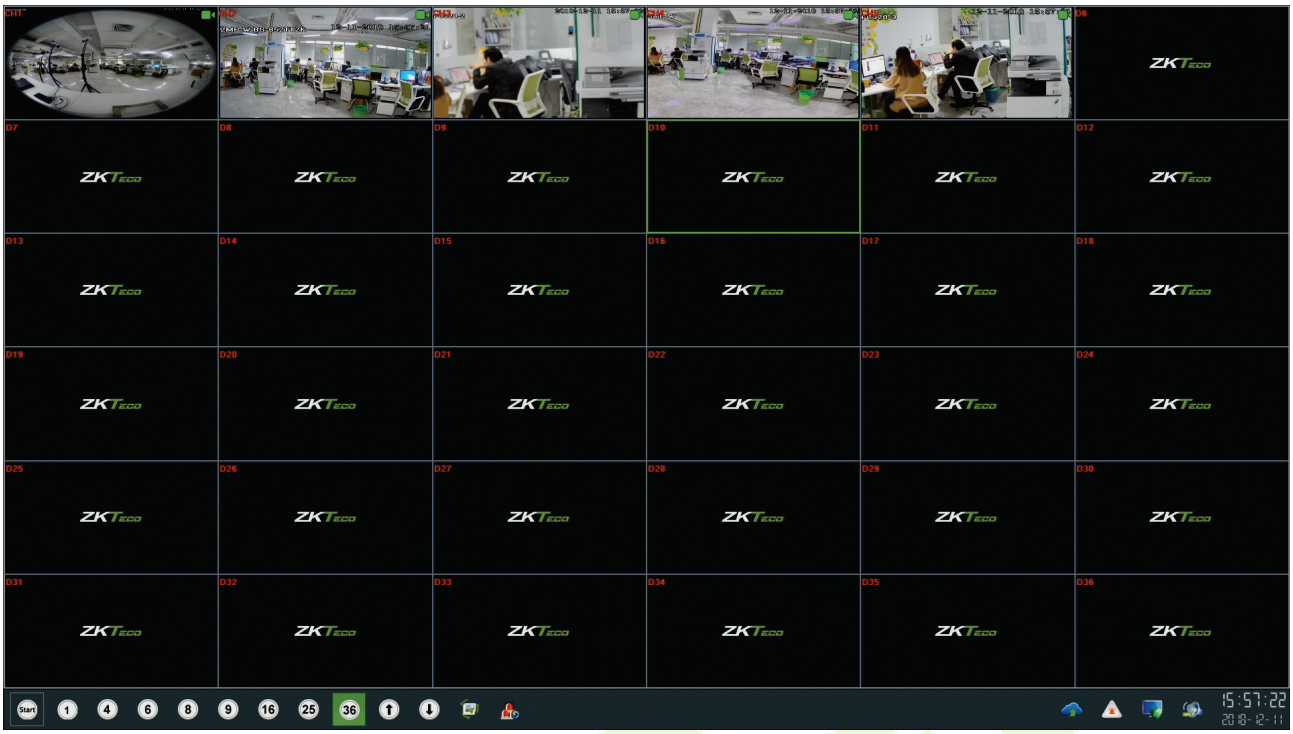


5. Select the checkbox for the device you want to add and edit the parameters in the corresponding text field, then click on [**OK**] to add it to the connection list.



Note: *The User Name and Password is set in the* ***ONVIF Settings*** *of the device.*

6. After adding successfully, the video image obtaining from the device can be viewed in real-time.



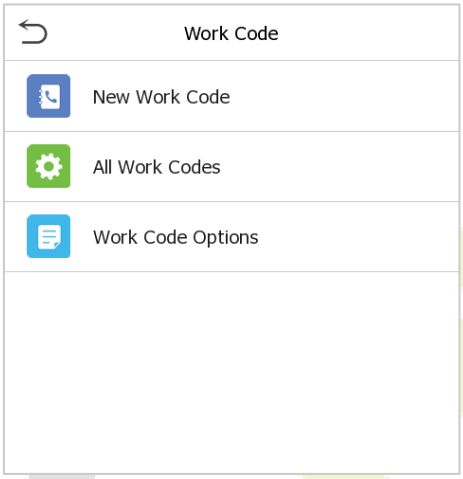
For more details, please refer to the *NVR User Manual*.

10 Work Code★

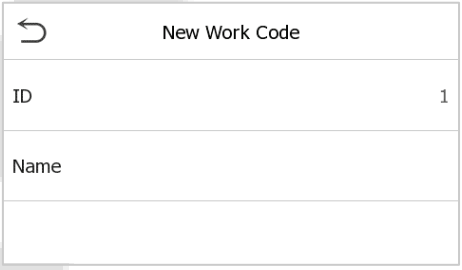
Employees' salaries are subject to their attendance records. An employee can be engaged in more than one type of work which may vary with time. As the pay varies according to the work types, the terminal provides a parameter to indicate the corresponding work type for every attendance record to facilitate rapid understanding of different attendance situations during the handling of attendance data.

Note: Only can use in the T&A PUSH, please refer to 6.7 Device Type Setting.

Tap **Work Code** on the **Main Menu** interface.



10.1 Add a Work Code



Function Description

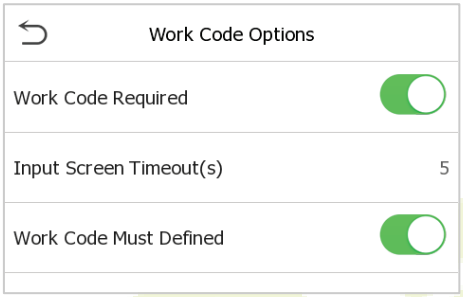
Function Name	Description
ID	It is the digital code of the work code. Users may set a valid value between 1 and 99999999.
Name	It is the naming of the work code.

10.2 All Work Codes

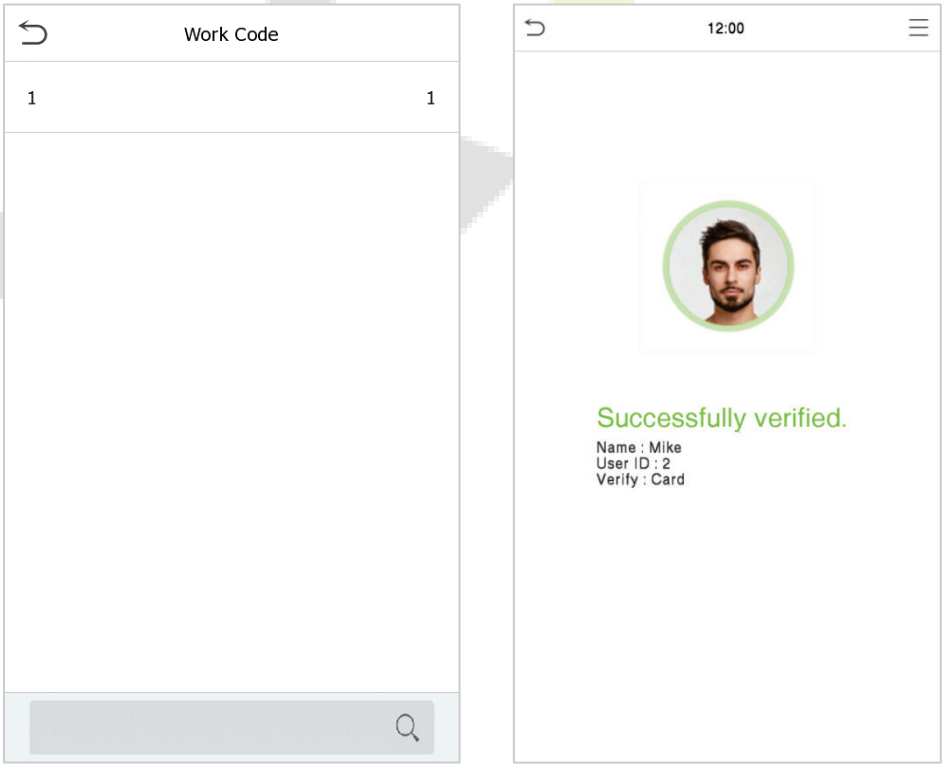
You can view, edit and delete work codes in All Work Codes. The process of editing a work code is the same as adding a work code, except that the ID is not allowed to be modified.

10.3 Work Code Options

To set whether entering the work code is a must and whether the entered work code must exist during authentication.



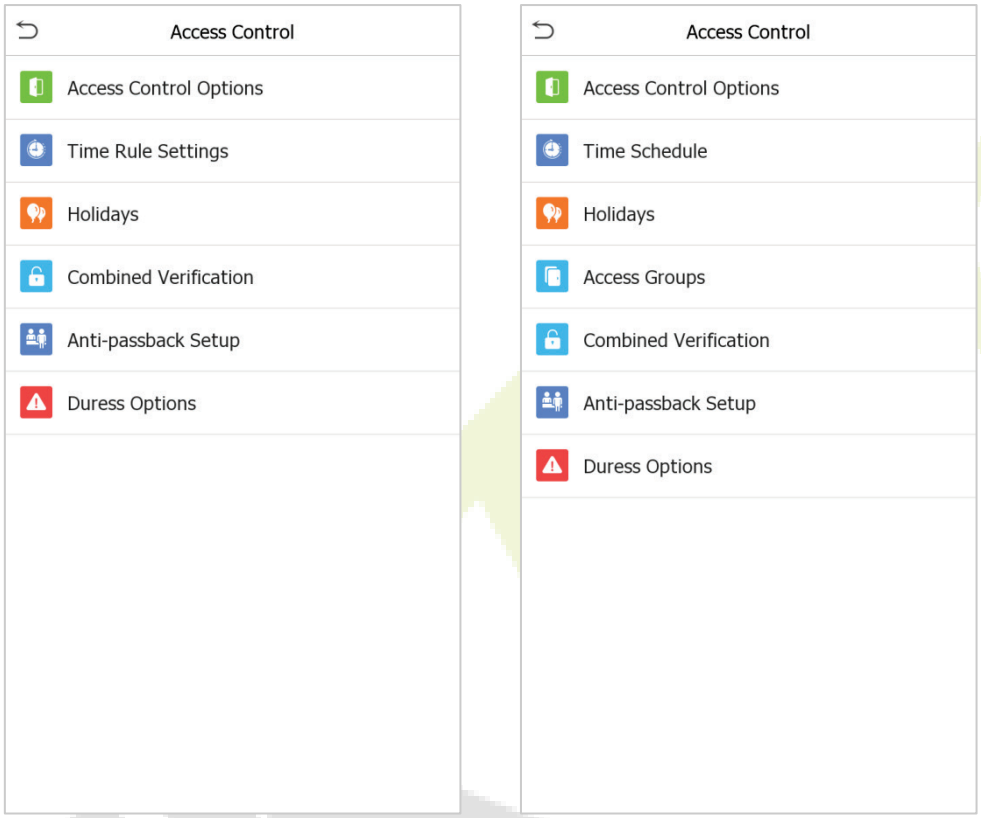
In 1: N or 1:1 verification, the system will automatically pop up in the following window. Select the corresponding Word Code manually to verify successfully.



11 Access Control

Access Control is used to set the schedule of a door opening, locks control and other parameter settings related to access control.

Click **Access Control** on the main menu interface.



A&C Terminal T&A Terminal

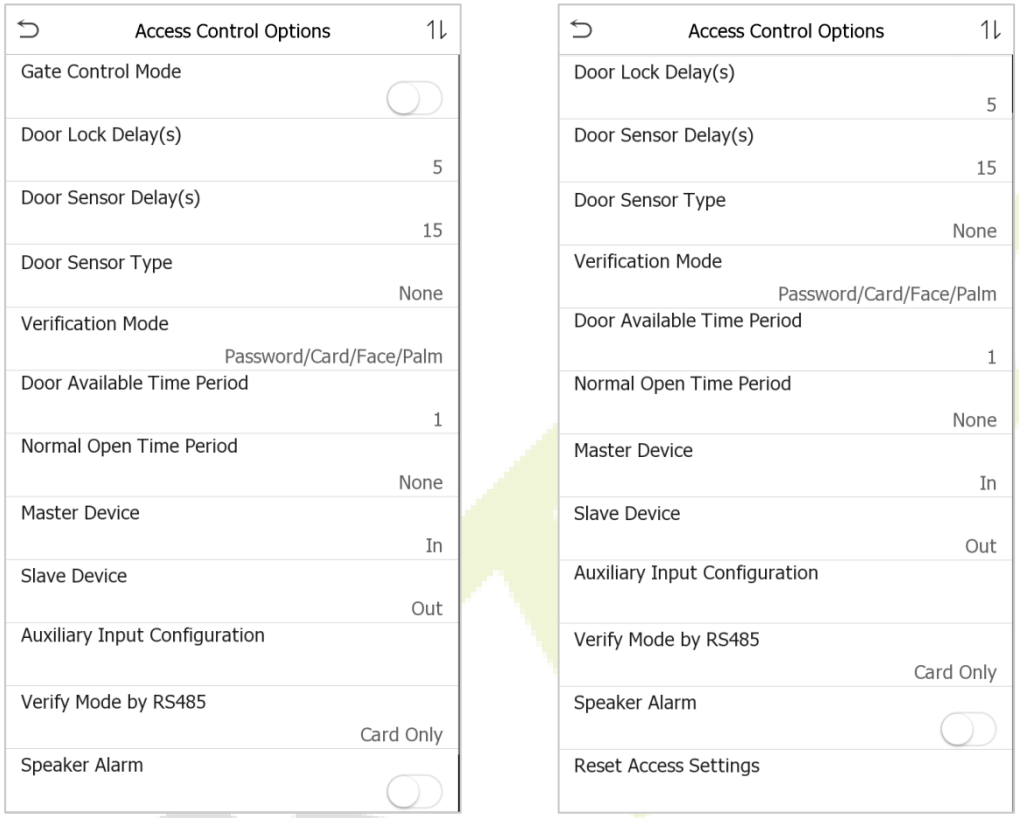
To gain access, the registered user must meet the following conditions:

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

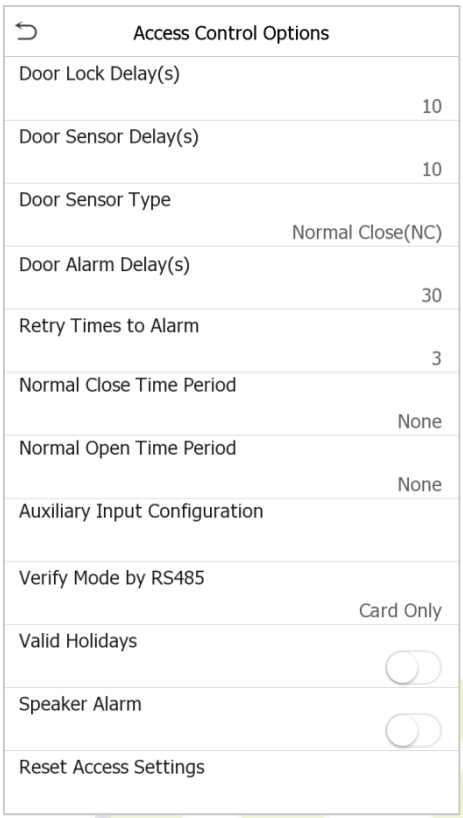
11.1 Access Control Options

This option is used to set the parameters of the control lock of the device and the related parameters.

Click **Access Control Options** on the Access Control interface.



A&C Terminal



T&A Terminal

Function Description of A&C Terminal:

Function Name	Description
Gate Control Mode	It toggles between **ON** or **OFF** switch to get into gate control mode or not. When set to **ON**, the interface removes the Door lock relay, Door sensor relay, and Door sensor type options.
Door Lock Delay (s)	The length of time that the device controls the electric lock to be in unlock state. Valid value: 1 to 10 seconds; 0 seconds represents disabling the function.
Door Sensor Delay (s)	If the door is not locked and is left open for a certain duration (Door Sensor Delay), an alarm will be triggered. The valid value of Door Sensor Delay ranges from 1 to 255 seconds.
Door Sensor Type	There are three Sensor types: **None, Normal Open,** and **Normal Closed**. **None:** It means the door sensor is not in use. **Normally Open:** It means the door is always left open when electric power is on. **Normally Closed:** It means the door is always left closed when electric power is on.
Verification Mode	The supported verification mode includes Password/Card/Face/Palm, User ID Only, Password, Card Only, and so on.
Door Available Time Period	It sets the timing for the door so that the door is accessible only during that period.

Normal Open Time Period	It is the scheduled time-period for "Normal Open" mode so that the door is always open during this period.
Master Device	While configuring the master and slave devices, you may set the state of the master as **Out** or **In**. **Out**: A record of verification on the master device is a check-out record. **In**: A record of verification on the master device is a check-in record.
Slave Device	While configuring the master and slave devices, you may set the state of the slave as **Out** or **In**. **Out**: A record of verification on the slave device is a check-out record. **In**: A record of verification on the slave device is a check-in record.
Auxiliary Input Configuration	Sets the door unlock time period and auxiliary output type of the auxiliary terminal device. Auxiliary output types include None, Trigger door open, Trigger Alarm, Trigger door open and Alarm.
Verify Mode by RS485	The verification mode is used when the device is used either as a host or slave. The supported verification mode includes Card only, and Card + Password.
Speaker Alarm	It transmits a sound alarm or disassembly alarm from the local. When the door is closed or the verification is successful, the system cancels the alarm from the local.
Reset Access Setting	The access control reset parameters include door lock delay, door sensor delay, door sensor type, verification mode, door available time period, normal open time period, master device, and alarm. However, erased access control data in Data Mgt. is excluded.

Function Description of T&A Terminal:

Function Name	Description
Door Lock Delay (s)	The length of time that the device controls the electric lock to be in unlock state. Valid value: 0 to 10 seconds.
Door Sensor Delay (s)	If the door is not locked and is left open for a certain duration (Door Sensor Delay), an alarm will be triggered. The valid value of Door Sensor Delay ranges from 1 to 255 seconds.

Door Sensor Type	There are three Sensor types: **None**, **Normal Open**, and **Normal Close**. **None:** It means the door sensor is not in use. **Normal Open (NO):** It means the door is always left open when electric power is on. **Normal Close (NC):** It means the door is always left closed when electric power is on.
Door Alarm Delay(s)	When the state of the door sensor is inconsistent with that of the door sensor type, alarm will be triggered after a time period; this time period is the Door Alarm Delay (the value ranges from 1 to 999 seconds).
Retry Times to Alarm	When the number of failed verifications reach the set value (value ranges from 1 to 9 times), the alarm will be triggered. If the set value is None, the alarm will not be triggered after failed verification.
Normal Close Time Period	It is the scheduled time-period for "Normal Close" mode so that the door is always closed during this period.
Normal Open Time Period	It is the scheduled time-period for "Normal Open" mode so that the door is always open during this period.
Auxiliary Input Configuration	Sets the door unlock time period and auxiliary output type of the auxiliary terminal device. Auxiliary output types include None, Trigger door open, Trigger Alarm, Trigger door open and Alarm.
Verify Mode by RS485	When the RS485 reader function is turned on, the verification method is used when the device is used as a master or a slave. The supported verification mode includes Card only, and Card + Password.
Valid Holidays	To set if **Normal Close Time Period** or **Normal Open Time Period** settings are valid in set holiday time period. Choose [**ON**] to enable the set **NC** or **NO** time period in holiday.
Speaker Alarm	It transmits a sound alarm or disassembly alarm from the local. When the door is closed or the verification is successful, the system cancels the alarm from the local.
Reset Access Setting	The access control reset parameters include door lock delay, door sensor delay, door sensor type, door alarm delay, normal close time period, normal open time period, and alarm. However, erased access control data in Data Mgt. is excluded.

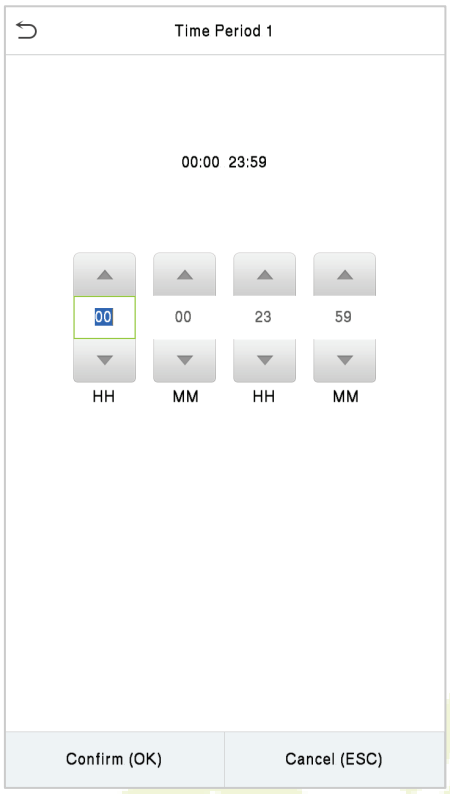
11.2 Time Rule Settings/Time Schedule

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

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

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

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



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

Note:

1) The door is inaccessible for the whole day when the End Time occurs before the Start Time (such as **23:57~23:56**).

2) It is the time interval for valid access when the End Time occurs after the Start Time (such as **08:00~23:59**).

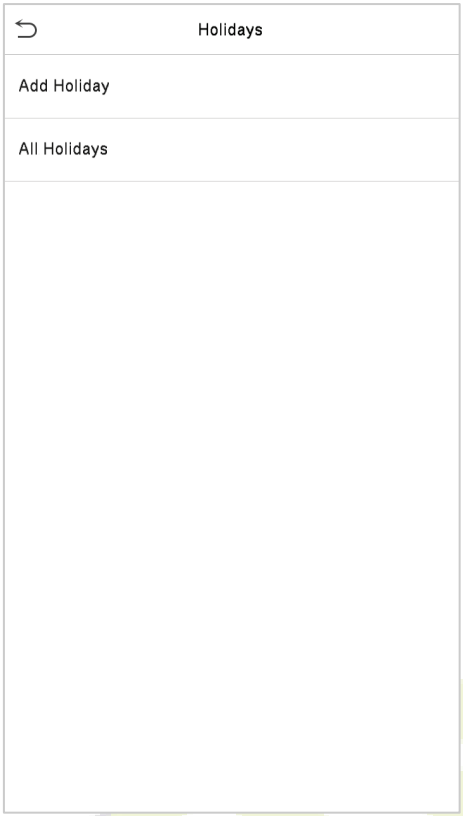
3) The door is accessible for the whole day when the End Time occurs after the Start Time (such that Start Time is **00:00** and End Time is **23:59**).

4) The default Time Zone 1 indicates that the door is open all day long.

11.3 Holiday Settings

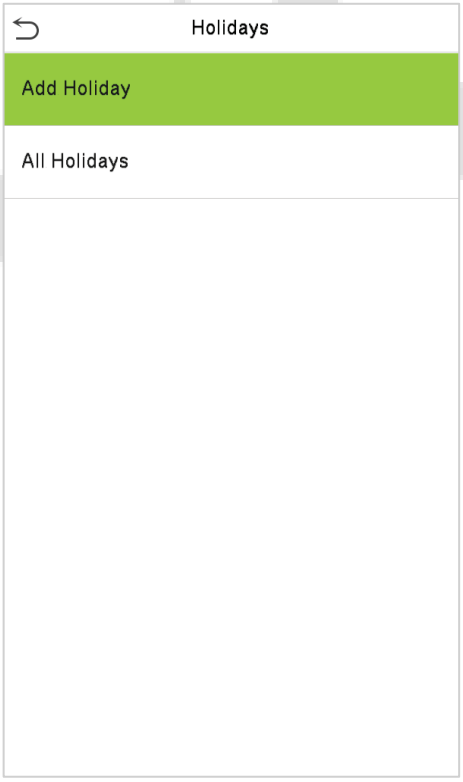
Whenever there is a holiday, you may need a special access time; but changing everyone's access time one by one is extremely cumbersome, so you can set a holiday access time which applies to all the employees, and the user will be able to open the door during the holidays.

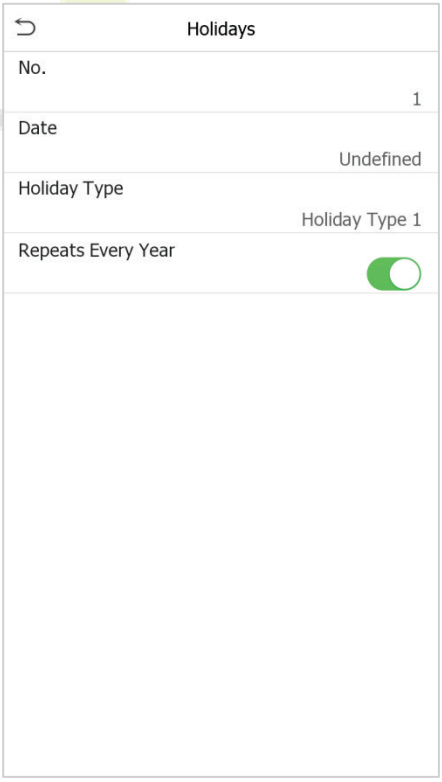
Click **Holidays** on the Access Control interface.



Add a New Holiday

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





Edit a Holiday

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

Delete a Holiday

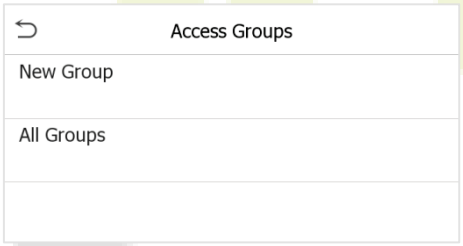
On the Holidays interface, select a holiday item to be deleted and click **Delete**. Click **OK** to confirm the deletion. After deletion, this holiday is no longer displayed on All Holidays interface.

11.4 Access Groups

***Note**: This function is only available for T&A PUSH.*

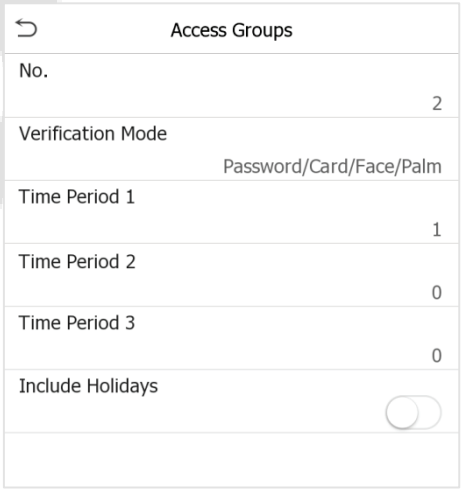
This is to easily manage groupings and users in different access groups. Settings of an access group such as access time zones are applicable to all members in the group by default. However, users may manually set the time zones as needed. User authentication takes precedence over group authentication when group authentication modes overlap with the individual authentication methods. Each group can set a maximum of three time zones. By default, newly enrolled users are assigned to Access Group 1; they can be assigned to other access groups.

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



➢ **Add a New Group**

Click **New Group** on the Access Groups interface and set access group parameters.



Notes:

- There is a default access group numbered 1, which cannot be deleted, but can be modified.

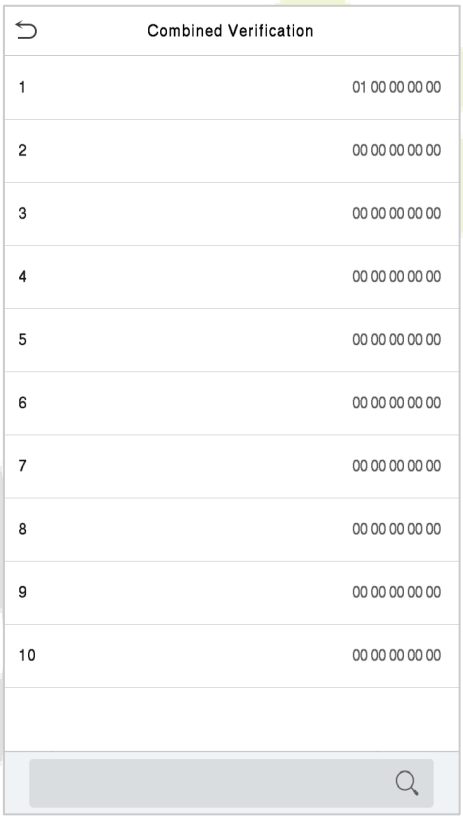
- A number cannot be modified after being set.
- When the holiday is set to be valid, personnel in a group may only open the door when the group time zone overlaps with the holiday time period.
- When the holiday is set to be invalid, the access control time of the personnel in a group is not affected during holidays.

11.5 Combined Verification Settings

Access groups are arranged into different door-unlocking combinations to achieve multiple verifications and strengthen security.

In a door-unlocking combination, the range of the combined number N is $0 \leq N \leq 5$, and the number of members N may all belong to one access group or may belong to five different access groups.

Click **Combined Verification** on the Access Control interface.



Click the door-unlocking combination to be set. Click the up and down arrows to input the combination number, then press OK.

Examples:

The door-unlocking combination 1 is set as (01 03 05 06 08), indicating that the unlocking combination 1 consists of 5 people, and the 5 individuals are from 5 groups, namely, access control group 1 (AC group 1), AC group 3, AC group 5, AC group 6, and AC group 8, respectively.

The door-unlocking combination 2 is set as (02 02 04 04 07), indicating that the unlocking combination 2 consists of 5 people; the first two are from AC group 2, the next two are from AC group 4, and the last person is from AC group 7.

The door-unlocking combination 3 is set as (09 09 09 09 09), indicating that there are 5 people in this combination; all of which are from AC group 9.

The door-unlocking combination 4 is set as (03 05 08 00 00), indicating that the unlocking combination 4 consists of three people. The first person is from AC group 3, the second person is from AC group 5, and the third person is from AC group 8.

Delete a Door-unlocking Combination

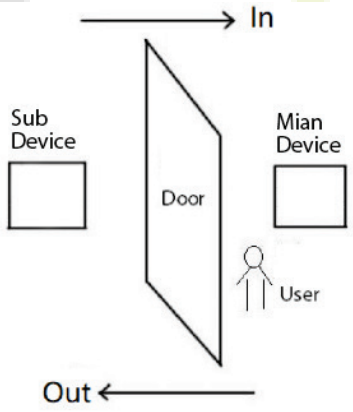
Set all the group numbers as 0 if you want to delete door-unlocking combinations.

11.6 Anti-Passback Setup

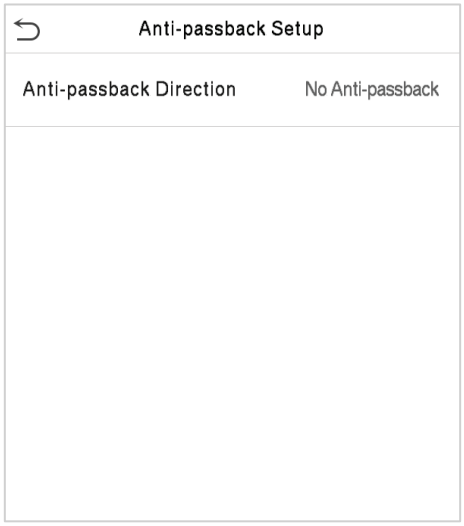
A user may be followed by some person(s) to enter the door without verification, resulting in a security breach. So, to avoid such situations, the Anti-Passback option was developed. Once it is enabled, the check-in and check-out record must occur alternatively to open the door to represent a consistent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

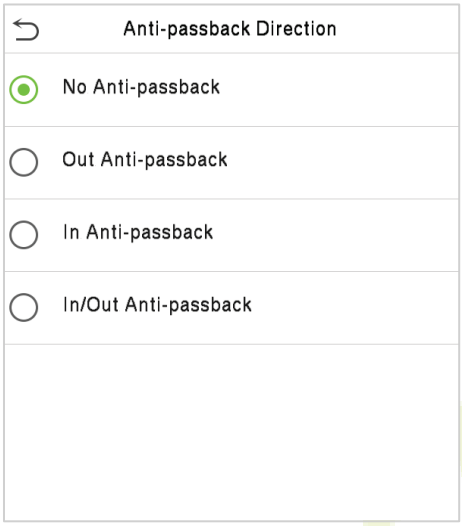
This function requires two devices to work together:

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



Click **Anti-Passback Setup** on the **Access Control** interface.



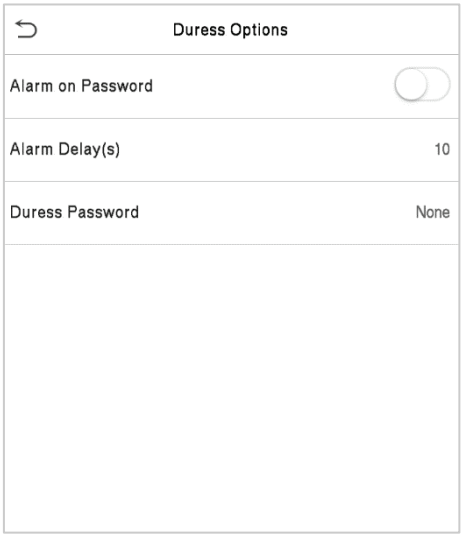


Function Name	Description
Anti-Passback Direction	**No Anti-Passback:** The Anti-Passback function is disabled, which means successful verification through either the master device or slave device can unlock the door. The attendance state is not saved in this option. **Out Anti-Passback:** The user can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

11.7 Duress Options Settings

If a user activated the duress verification function with specific authentication method(s), when he/she is under coercion during authentication with such method, the device will unlock the door as usual, but at the same time a signal will be sent to trigger the alarm.

Click **Duress Options** on the Access Control interface.

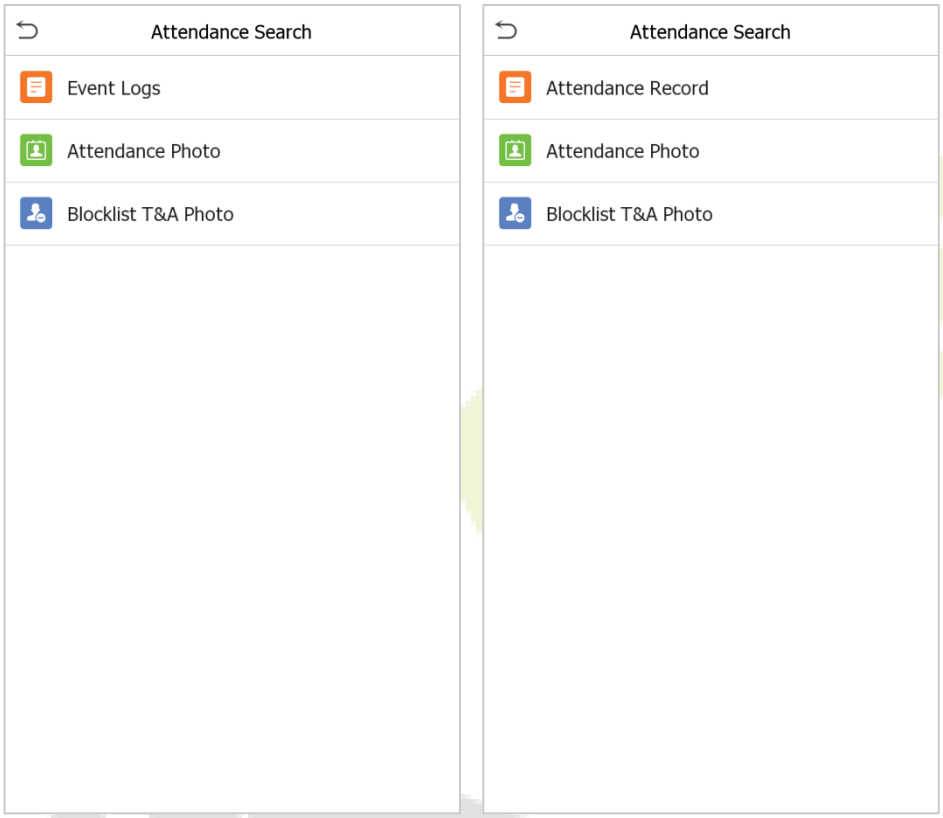


Function Name	Description
Alarm on Password	When a user uses the password verification method, an alarm signal is generated only when the password verification is successful otherwise there is no alarm signal.
Alarm Delay (s)	The alarm signal does not transmit until the alarm delay time elapses. The value ranges from 1 to 999 seconds.
Duress Password	Set the 6-digit duress password. When the user enters this duress password for verification, an alarm signal is generated.

12 Attendance Search

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

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

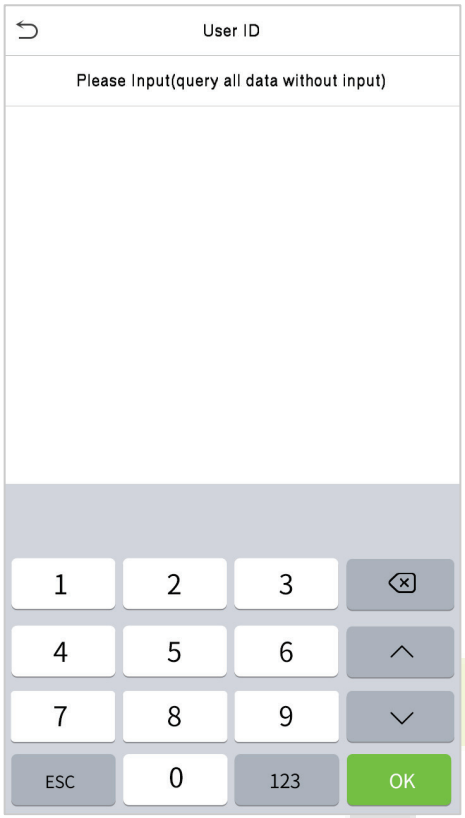


A&C PUSH T&A PUSH

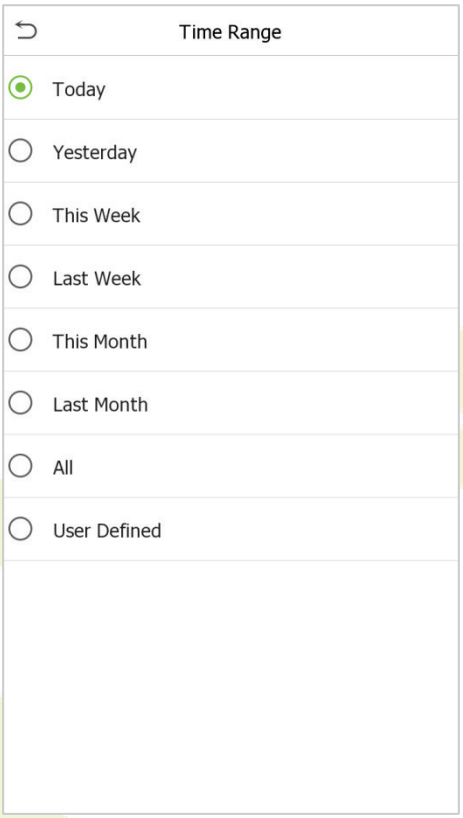
The process of searching for attendance and blocklist photos is similar to that of searching for event logs. The following is an example of searching for event logs.

On the **Attendance Search** interface, click **Event Logs/Attendance Record** to search for the required record.

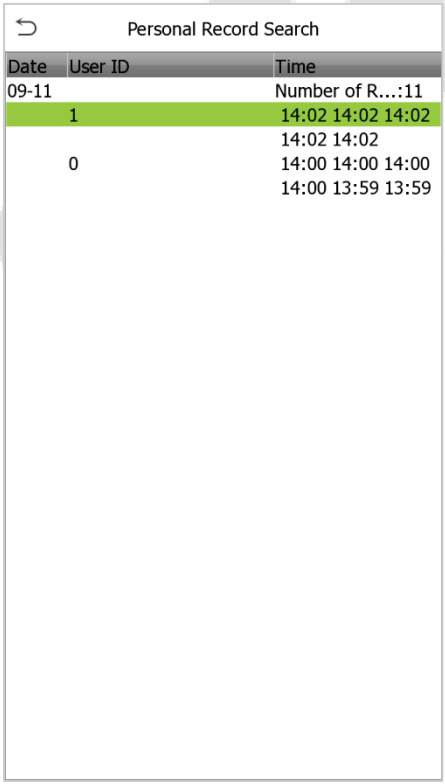
1. Enter the user ID to be searched and click OK. If you want to search for records of all users, click OK without entering any user ID.



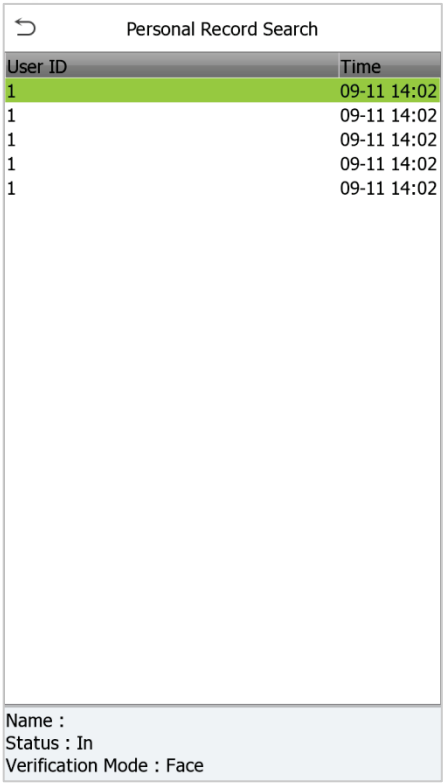
2. Select the time range in which the records you want to search for.



3. The record search succeeds. Click the record in green to view its details.



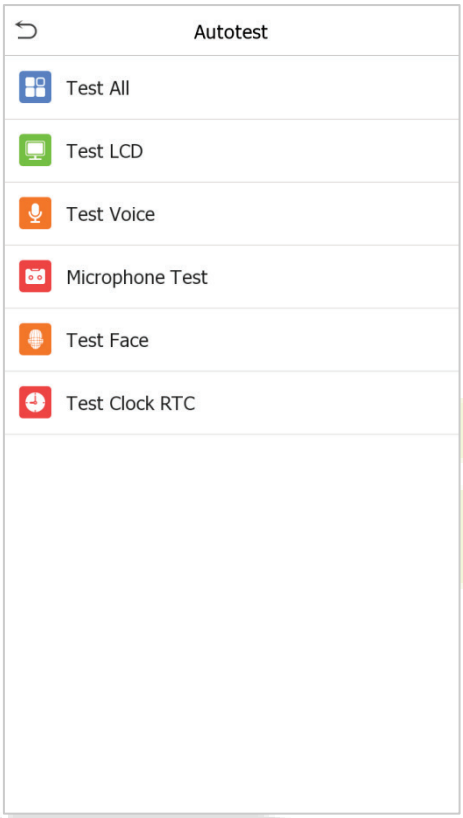
4. The below figure shows the details of the selected record.



13 Autotest

To automatically test whether all modules in the device function properly, which include the LCD, Audio, Microphone, Camera and real-time clock (RTC).

Click **Autotest** on the main menu interface.

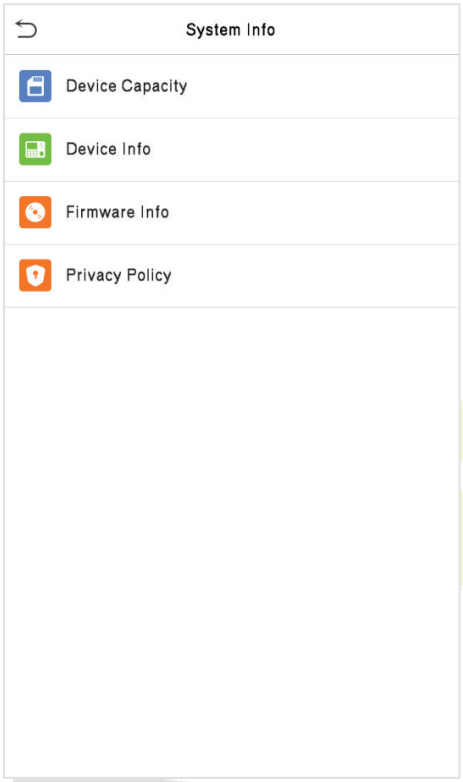


Menu	Description
Test All	To automatically test whether the LCD, audio, microphone, camera and RTC are normal.
Test LCD	To automatically test the display effect of LCD screen by displaying full-color, pure white, and pure black to check whether the screen displays the colors normally.
Test Voice	To automatically test whether the audio files stored in the device are complete and the voice quality is good.
Microphone Test	Check whether the microphone is working by speaking to microphone and playing the microphone recording.
Test Face	To test if the camera functions properly by checking the pictures taken to see if they are clear enough.
Test Clock RTC	To test the RTC. The device tests whether the clock works normally and accurately with a stopwatch. Touch the screen to start counting and press it again to stop counting.

14 System Information

With the system information option, you can view the storage status, the version information of the device, and privacy policy.

Click **System Info** on the main menu interface.



Menu	Description
Device Capacity	Displays the current device's user storage, password, palm★, face and card storage, administrators, records, attendance and blocklist photos, and Profile photos.
Device Info	Displays the Device's name, Serial number, MAC Address, Face and Palm algorithm★ version information, platform information, MCU Version and manufacturer.
Firmware Info	Displays the Firmware version and other version information of the device.
Privacy Policy	The privacy policy control will appear when the gadget turns on for the first time. After clicking "**I have read it**," the customer can use the product regularly. Click **System Info** -> **Privacy Policy** to view the content of the privacy policy. The privacy policy's content does not allow for U disc export. **Note:** The current privacy policy's text is only available in Simplified Chinese/ English. However, translation of other multi-language content is underway, with more iterations.

15 Connect to ZKBio CVAccess Software

15.1 Set the Communication Address

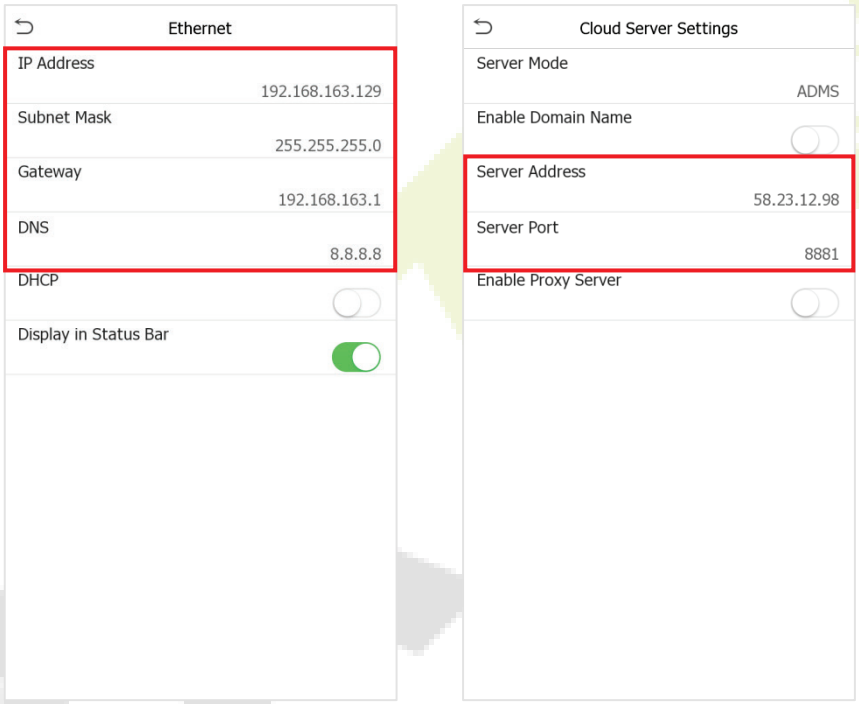
1. Tap **COMM.** > **Ethernet** in the main menu to set the IP address and gateway of the device.

   Note: *Please ensure that the IP address can communicate with the ZKBio CVAccess server.*

2. In the main menu, click **COMM.** > **Cloud Server Setting** to set the server address and server port.

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

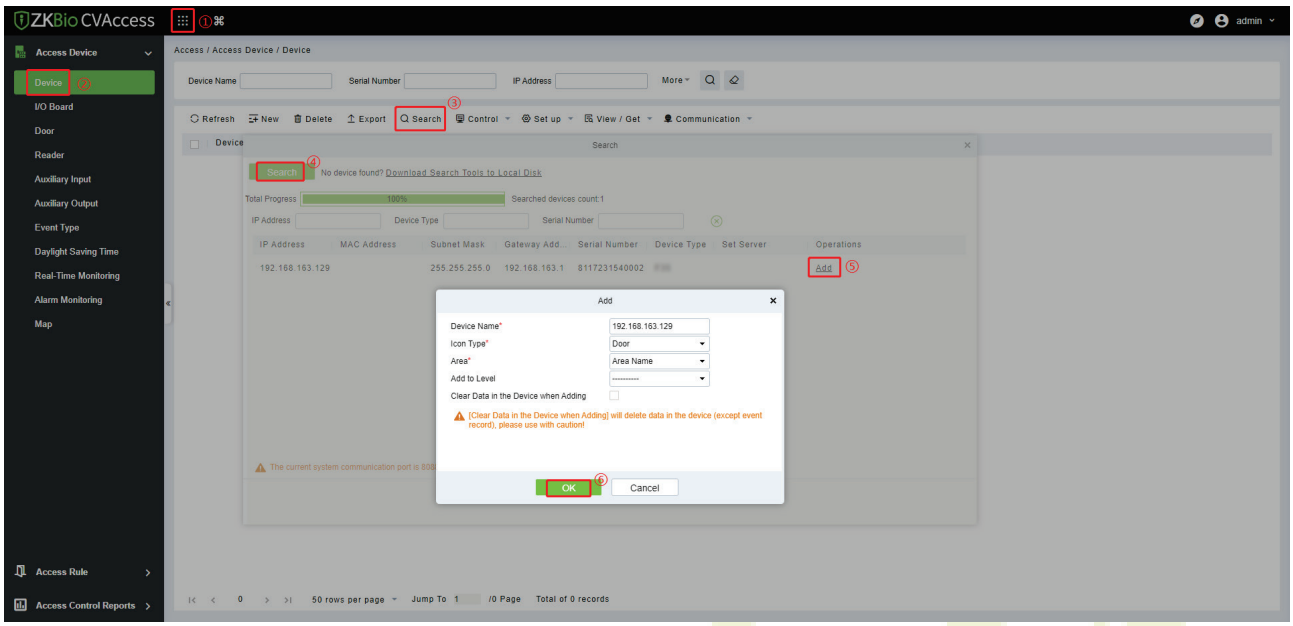
   Server port: Set the server port as of ZKBio CVAccess.



15.2 Add Device on the Software

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

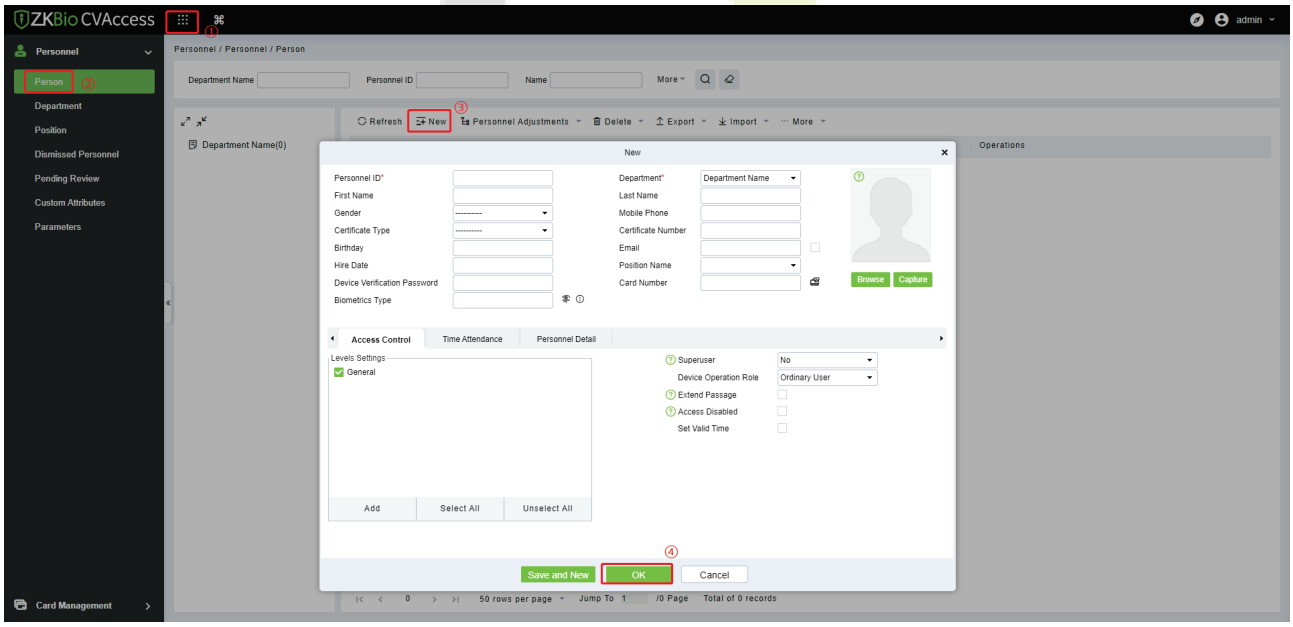
1. Click **Access** > **Device** > > **Search** > **Search**, to open the Search interface in the software.
2. Click **Search**, and it will prompt **Searching**…….
3. After searching, the list and total number of access controllers will be displayed.



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

15.3 Add Personnel on the Software

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



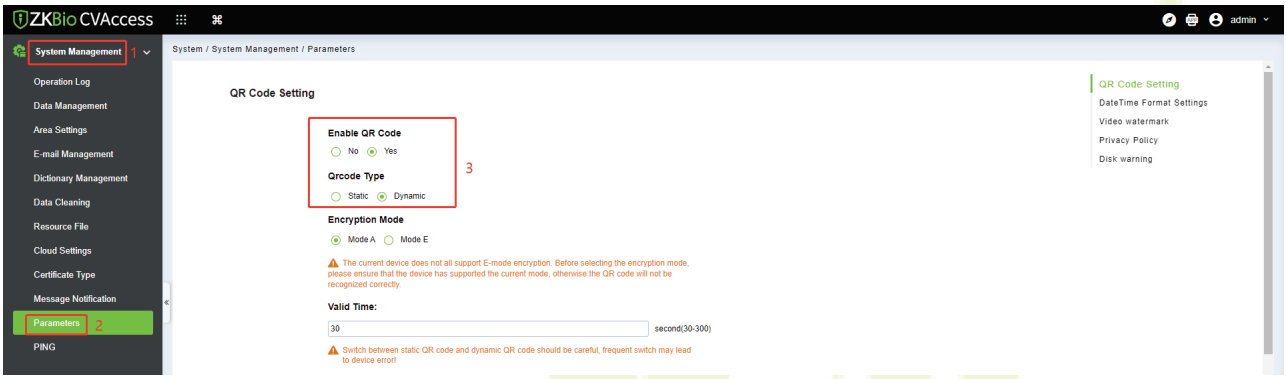
2. Fill in all the required fields and click **OK** to register a new user.
3. Click **Access > Device > Control > Synchronize All Data to Devices** to synchronize all the data to the device including the new users.

15.4 Mobile Credential★

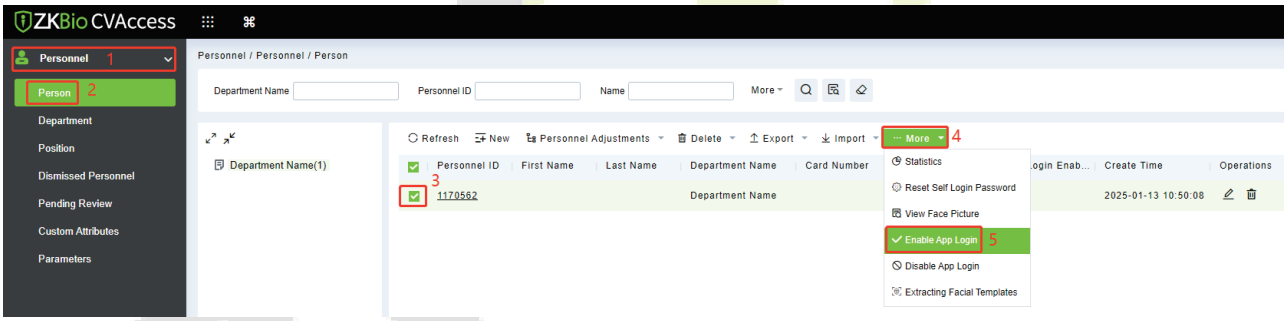
Note: To use this function, it is suggested to disable the Mask Detection function on the device (enter **System-Health Protection**).

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

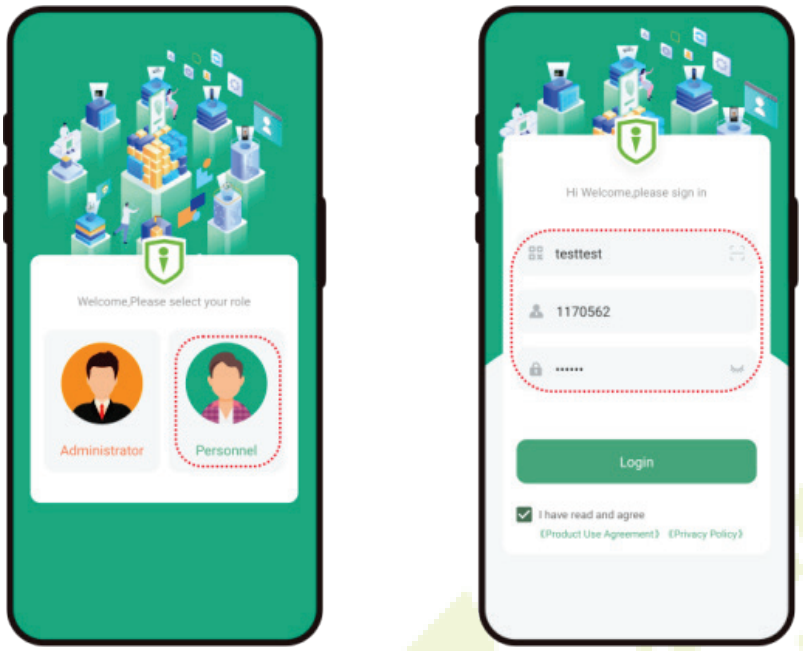
1. In ZKBio CVAccess, click **System** > **System Management** > **Parameters**, set **Enable QR Code** to "Yes", and select the Qrcode Type as **Dynamic**, the valid time of the QR code can be set.

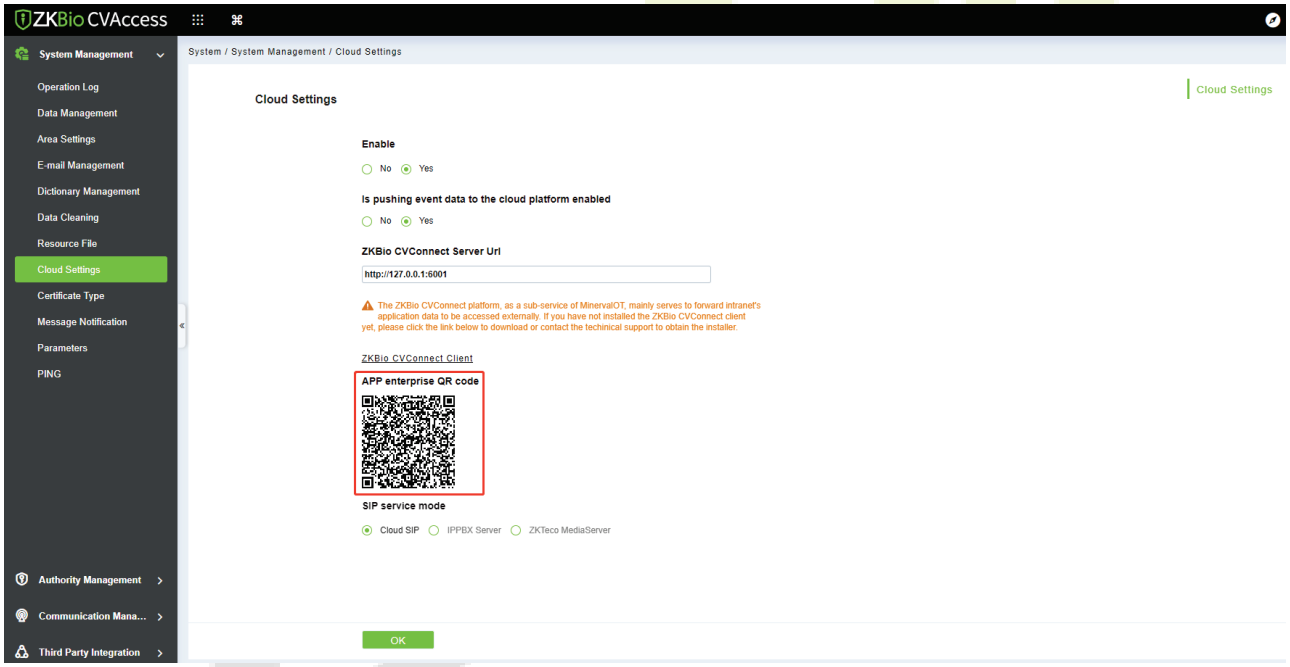


2. Click **Personnel** > **Personnel** > **Person**, select the personnel and click **More** > **Enable APP Login**.

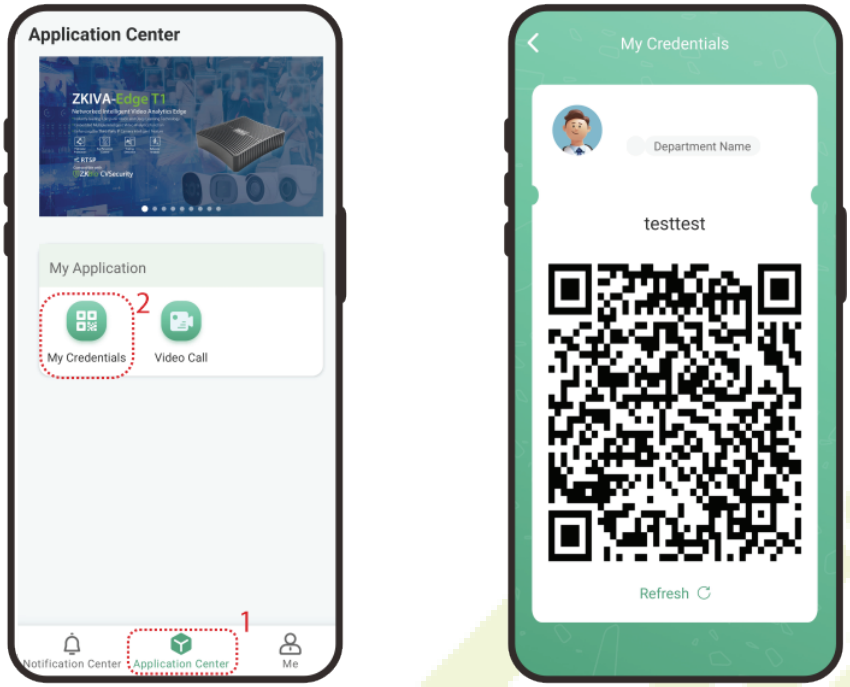


3. Open the App on the Smartphone. On the login screen, select the role-**Personnel**, enter the account information, and click **Login**.
   Organization Name: Scan the organization code you get before. (Enter **System > System Management >Cloud Setting >APP enterprise QR Code**)
   Account & Password: The personnel ID & password (default: 123456).





4. Click **Application Center** > **Mobile Credential** on the App, and a QR code will appear, which includes employee ID and card number information.



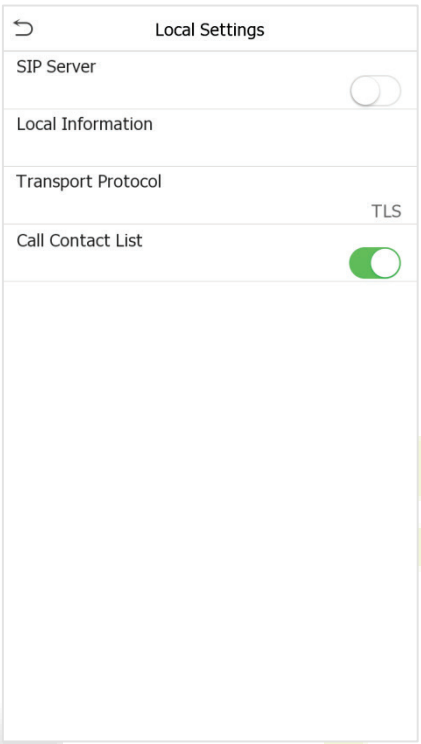
5. The QR code can replace a physical card on a specific device to achieve contactless authentication to open the door.
6. The QR code refreshes automatically for every 30s and supports manual refresh.

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

16 SIP Video Intercom★

16.1 Local Area Network Use

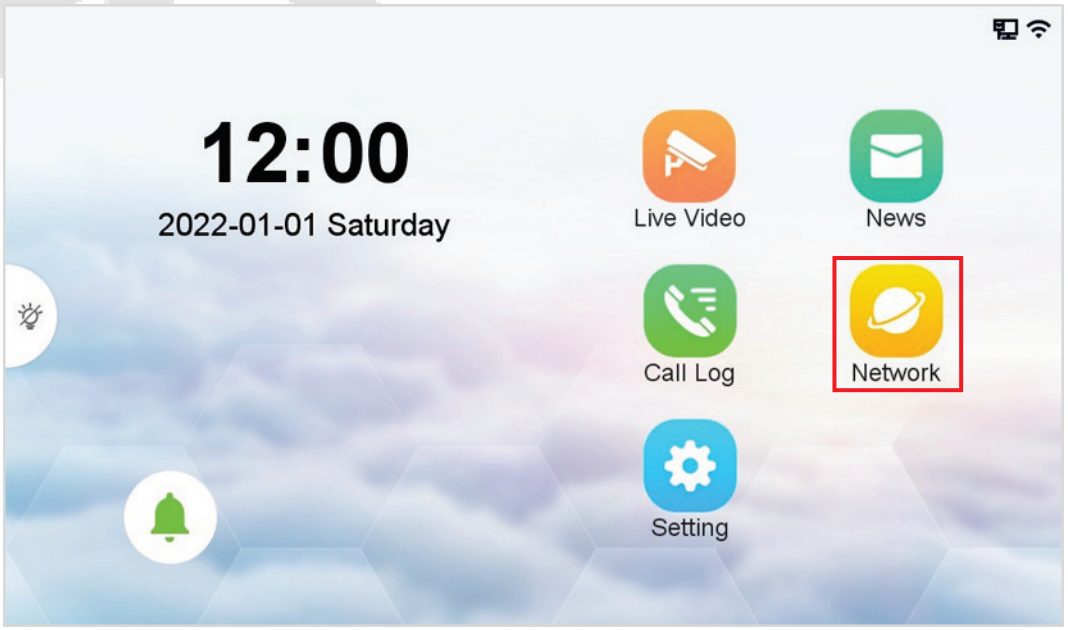
In this mode, please make sure that the SIP Server of the device is disabled.



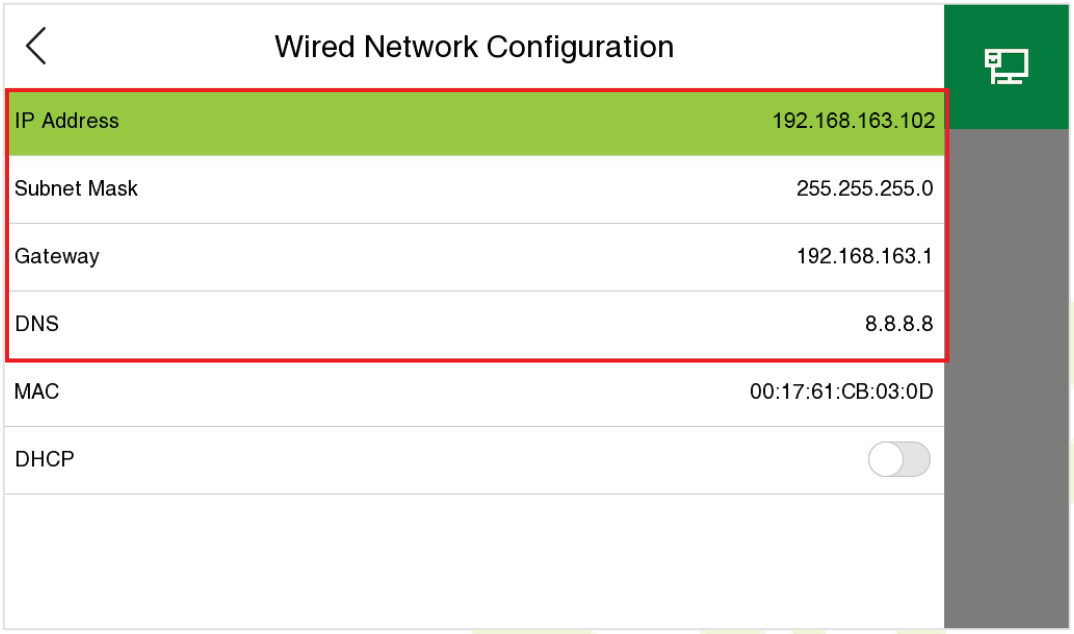
This function needs to be used with the indoor monitor VT07-B01.

- **On the Indoor Monitor:**

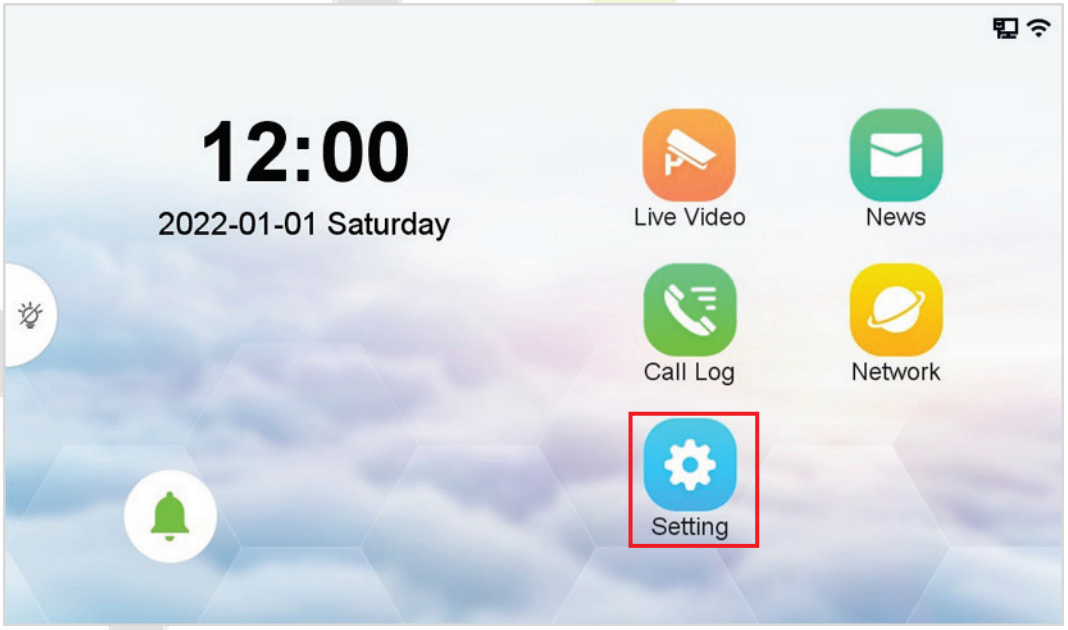
1. Tap **Network** > to enter the wired network setting interface. (Default password: **123456**)

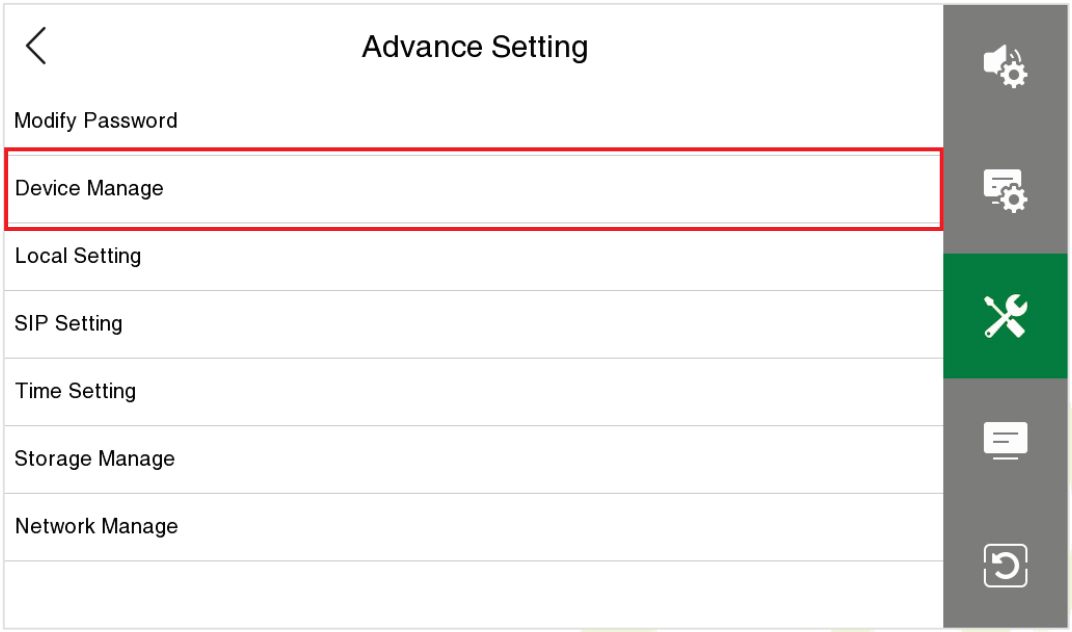


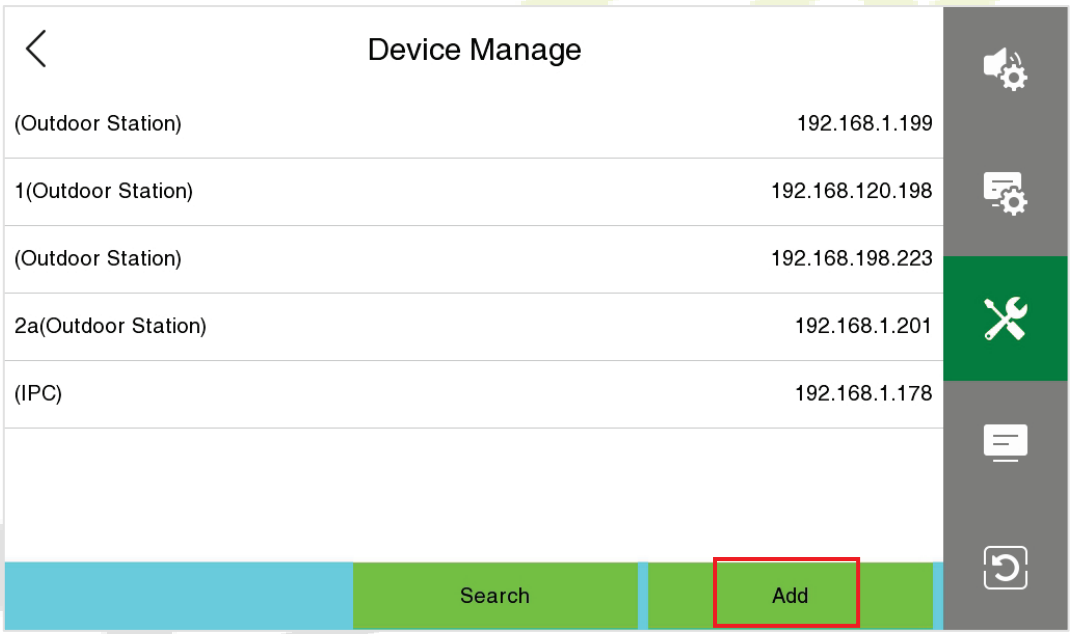
2. Set the IP Address and Gateway of the indoor monitor. (**Note:** The IP address should be in the same network segment as the device.)



3. Tap **Setting** > **Advance Setting** > **Device Manage** > **Add** to add the device.

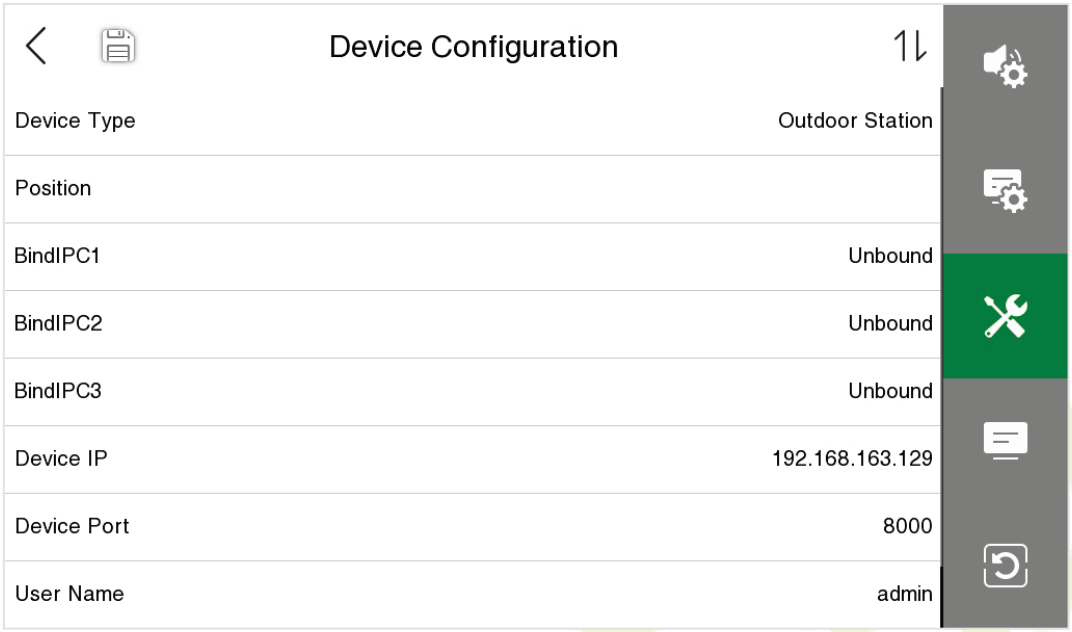






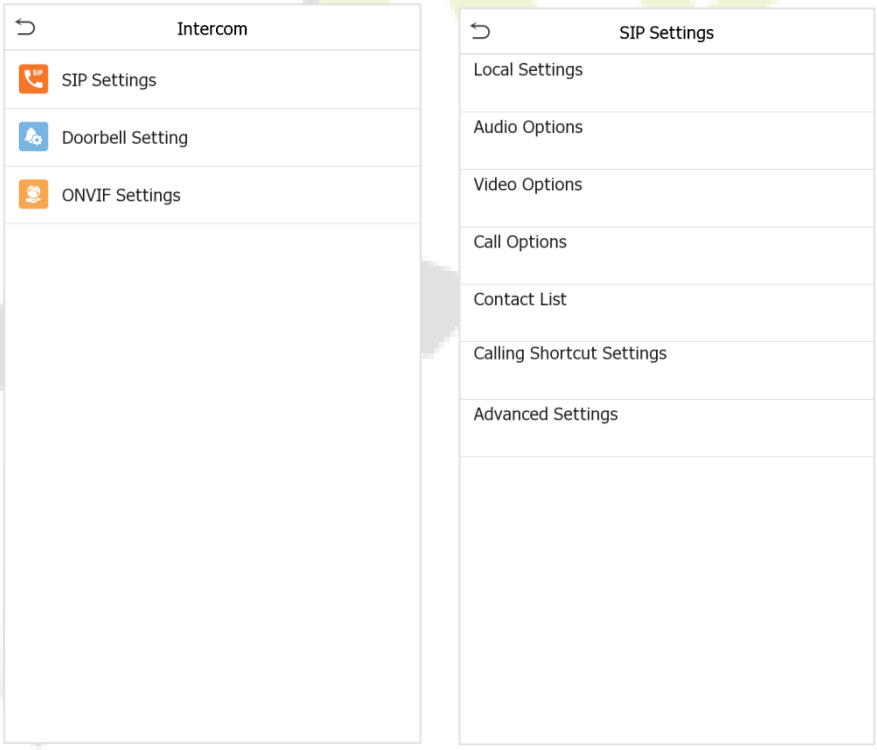
4. Set the related information of the device, then click **Save**.
   Device Type: Set as Outdoor Station.
   Device IP: Enter the IP address of the device.
   Device Port: 8000.
   User Name: admin.
   Password: 123456.

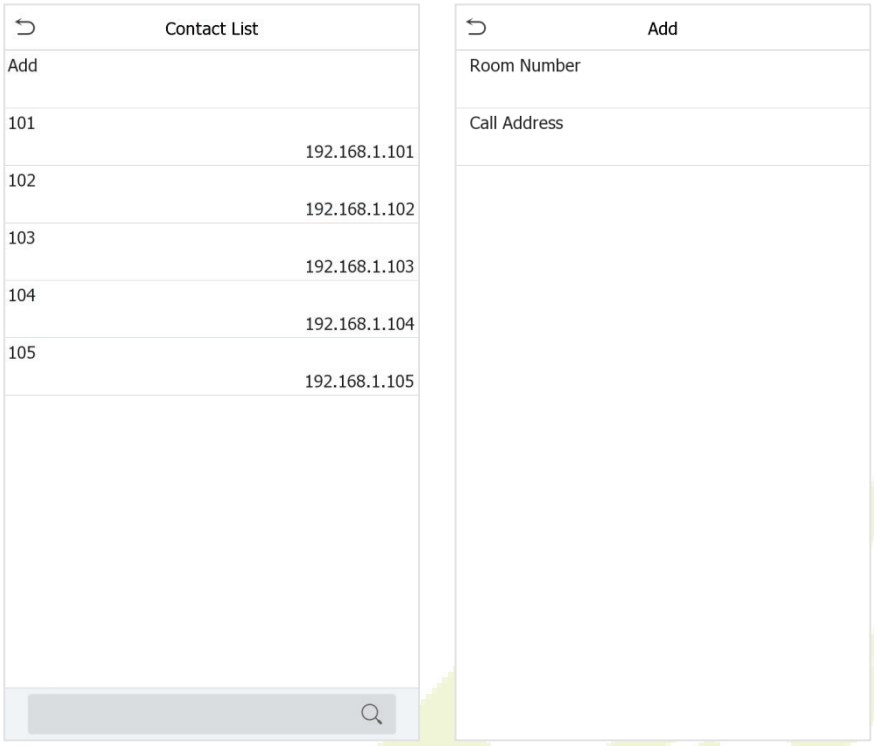
Note: When binding the device with an indoor monitor for ONVIF real-time video streaming, it is essential to synchronize and ensure that the ONVIF passwords of both the device and the indoor monitor are identical.



- **On the Device:**

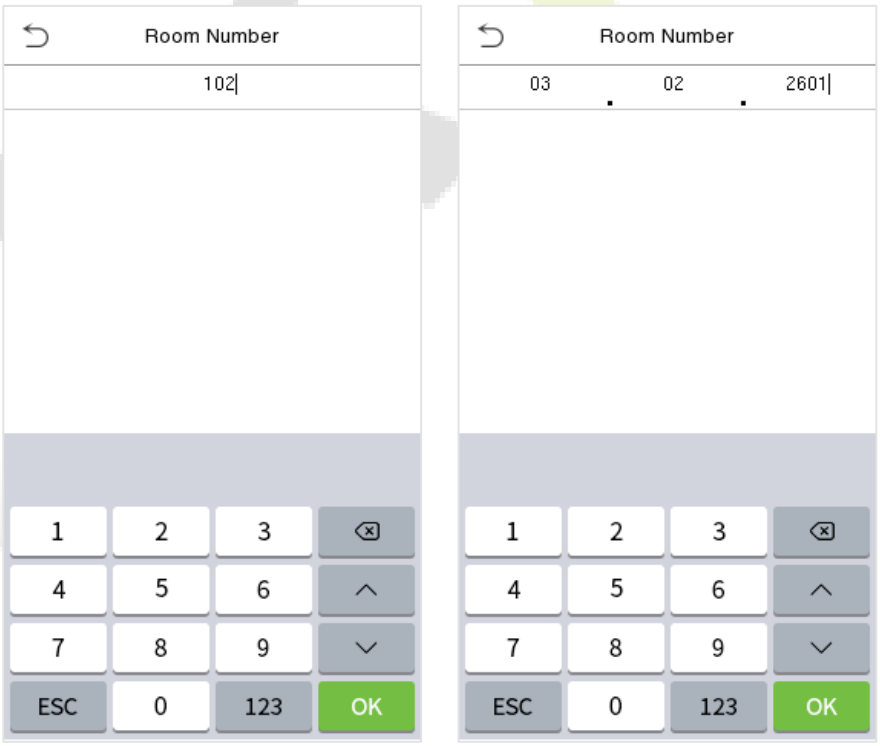
1. On the Main Menu, Click **Intercom > SIP Settings > Contact List > Add** to add the connected indoor monitors.





Room Number: Customize the number of the indoor monitor.

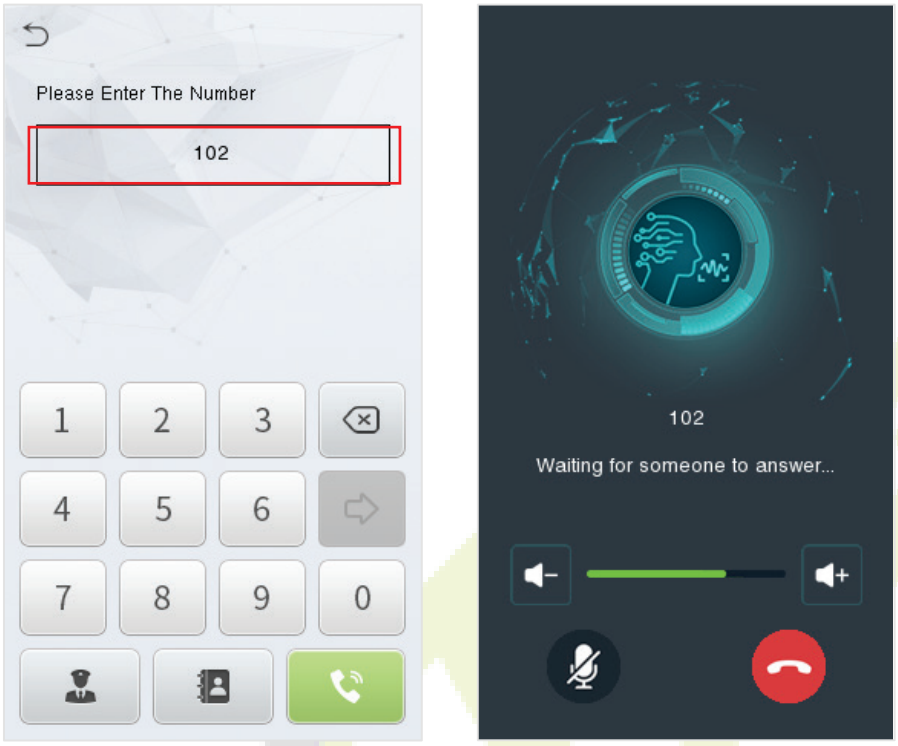
When the device type is set as **Entrance Station**, the room number can be 1~ 4 digits. When the device type is set as **Fence Terminal**, you need to input the block, unit and room number. For example, if the indoor monitor is in Block 3, Unit 2, Room 2601, then input "03.02.2601".



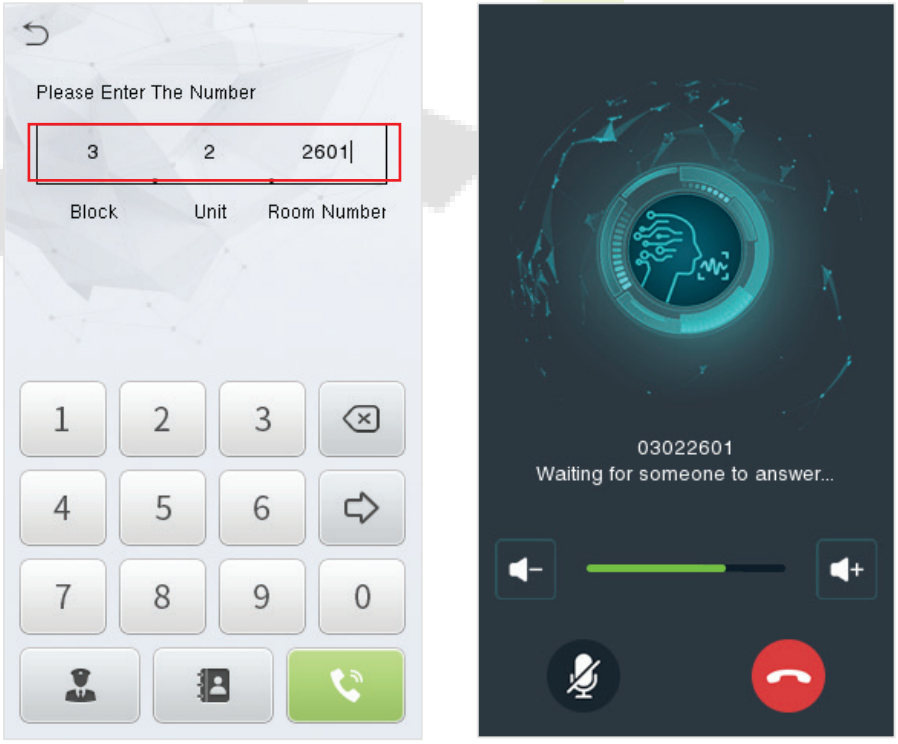
Entrance Station Fence Terminal

Call Address: It is the IP Address of the indoor monitor.

2. To enable the video intercom function, click the icon on the device and enter the number or IP address of the indoor monitor in the provided interface.



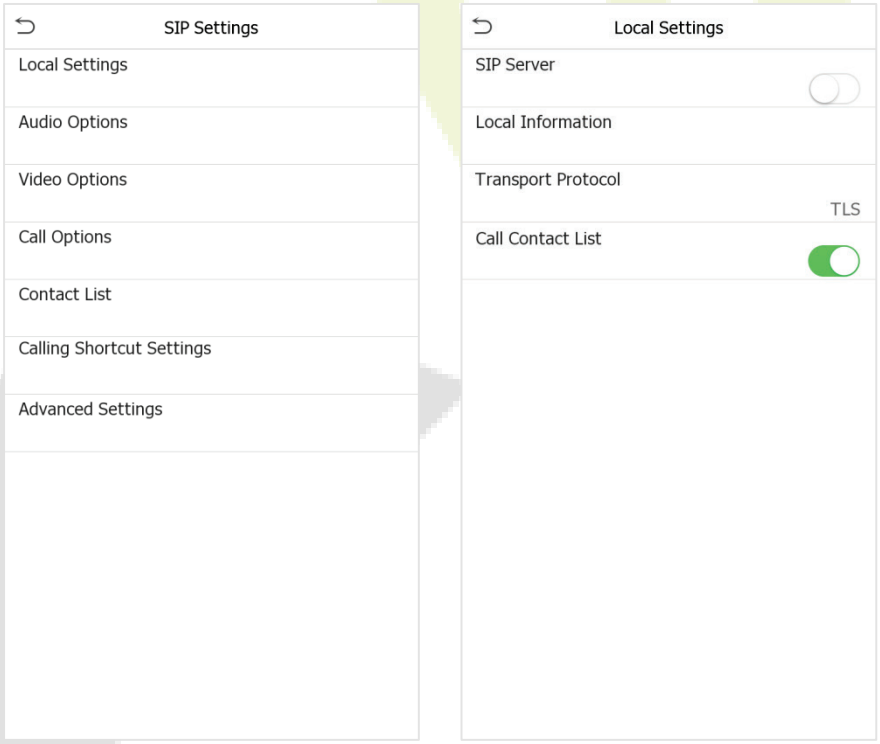
Entrance Station



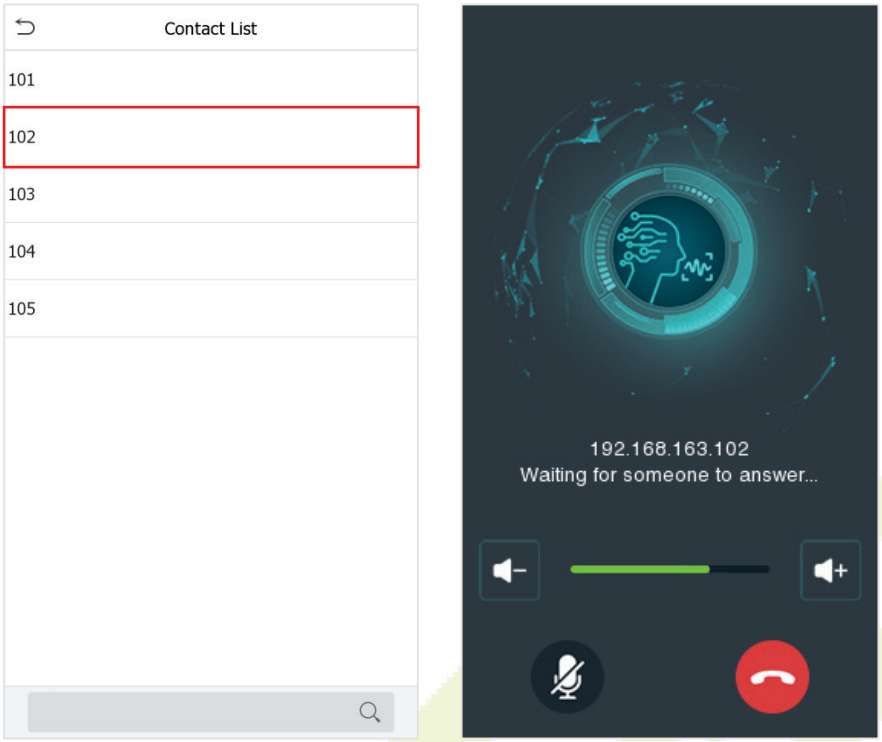
Fence Terminal

16.1.1 Call Contact List

1. On the **SIP Settings** interface, tap **Local Settings** > **Call Contact List** to enable the call contact list.

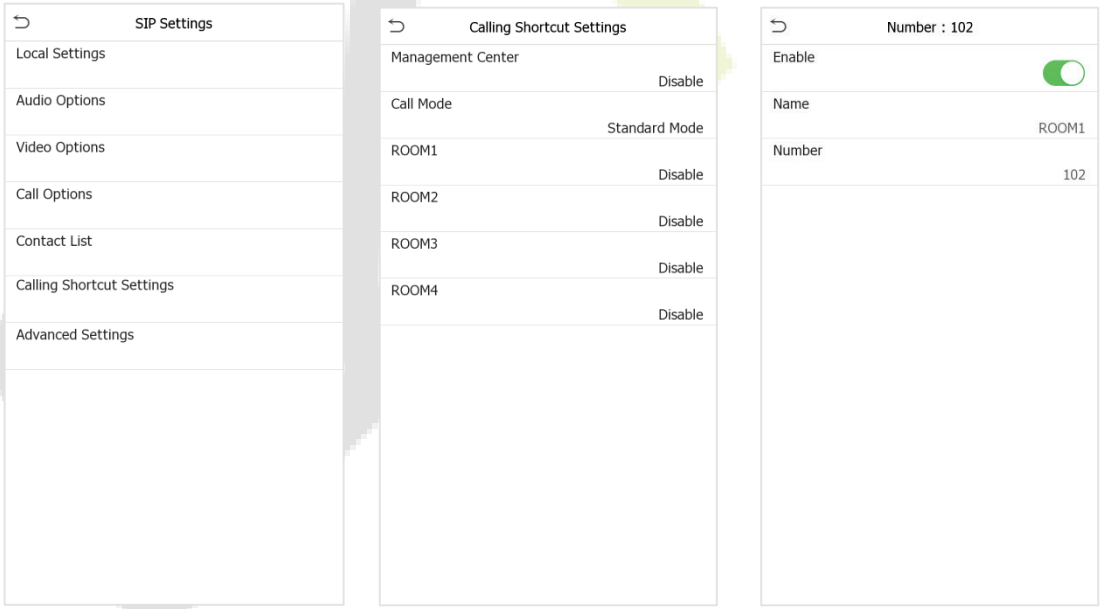


2. Click the icon on the device to enter the call page, then you can click the icon to open the contact list, select the number of the indoor monitor you want to call.



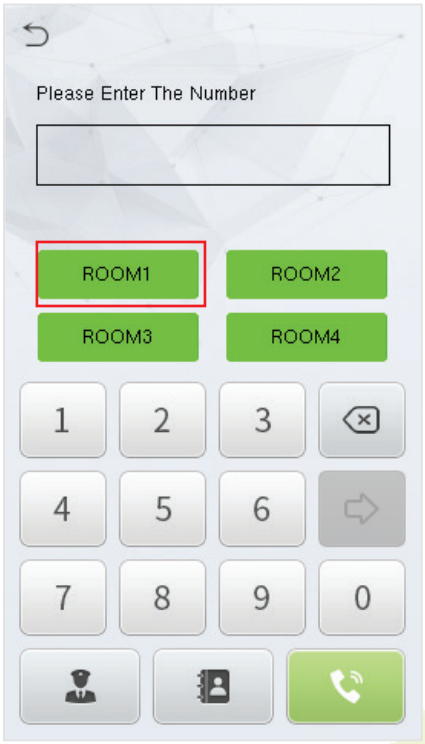
16.1.2 Custom the Calling Shortcut Keys

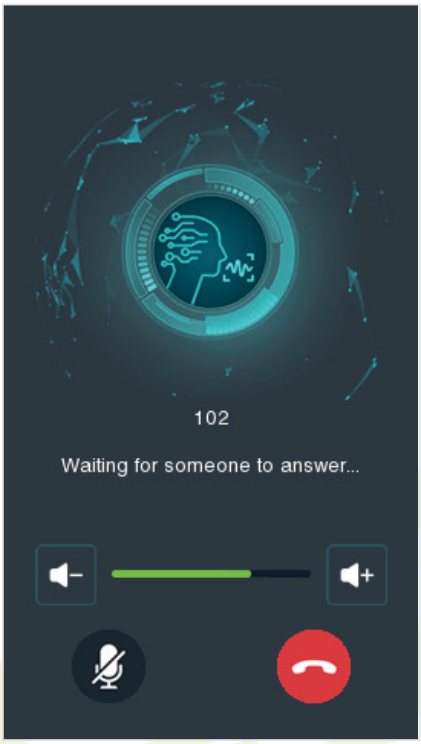
1. On the **SIP Settings** interface, tap **Calling Shortcut Settings** to enable and define the shortcut keys.



Name: Customize the name of the shortcut keys.
Number: It is the room number that set in the **Contact List** Menu.

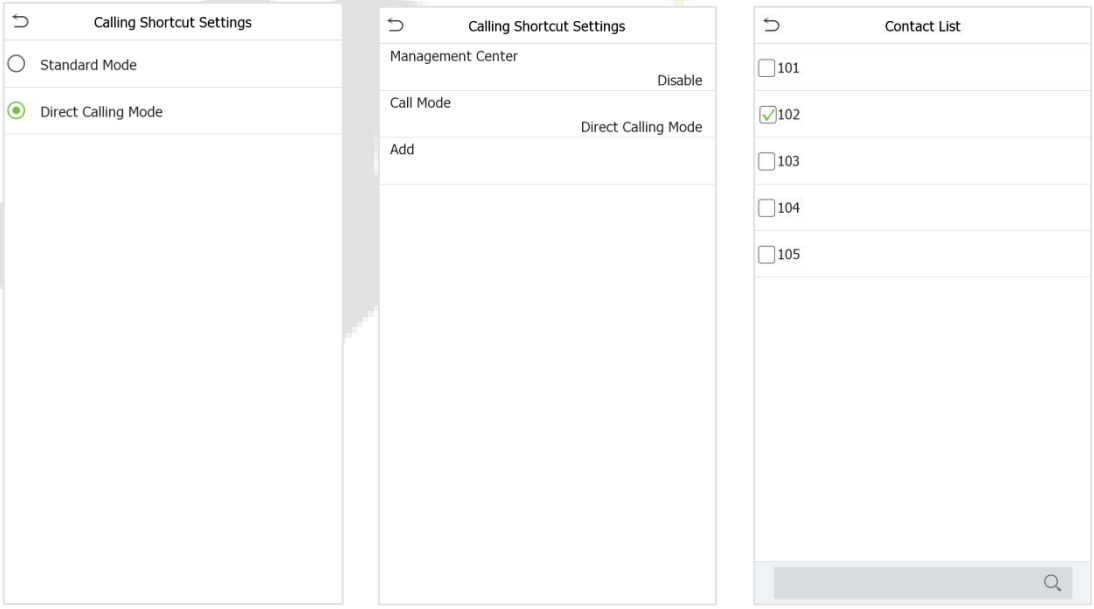
2. Then you can click the icon on the device and select the calling shortcut keys to call the indoor monitor.



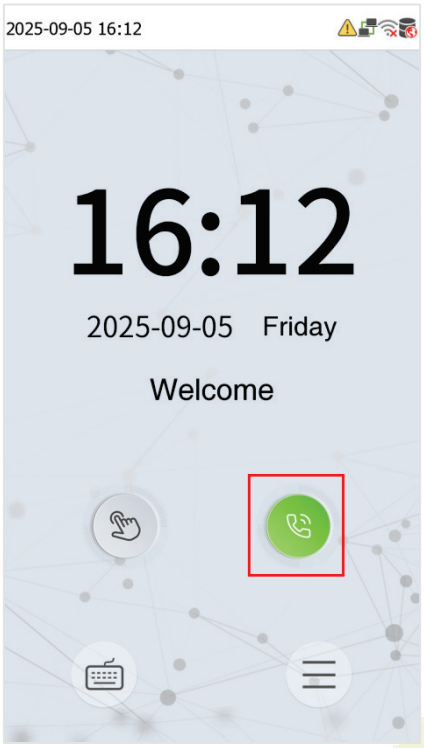


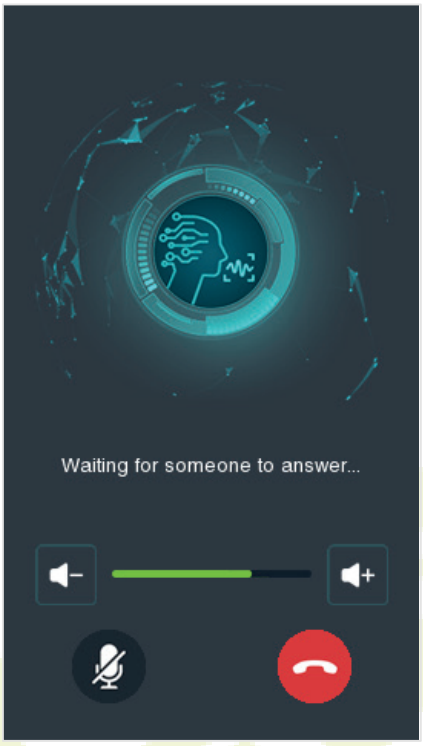
16.1.3 Direct Calling

1. On the **SIP Settings** interface, click **Calling Shortcut Settings** > **Call Mode** > **Direct Calling Mode** > **Add**. Select the IP address of the indoor monitors that you want to call, then the indoor monitors will be displayed in the list.



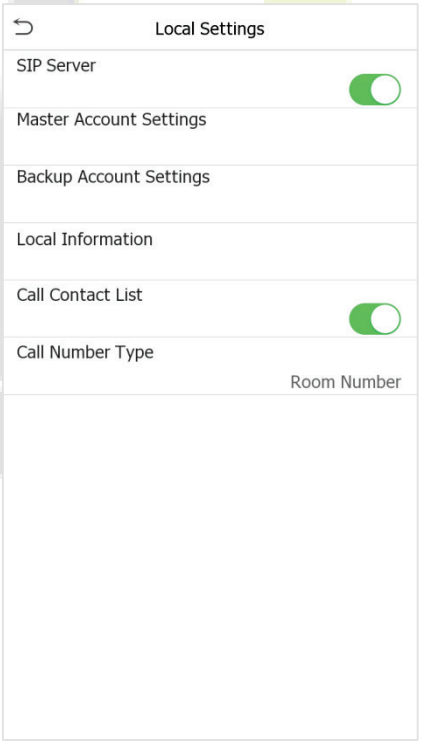
2. Then you can click the icon on the device to call the indoor monitors directly.





16.2 SIP Server

In this mode, please make sure that the SIP Server of the device is enabled.



This function needs to be used with the ZKBio CVAccess server, ZKBio Zexus Mobile App, indoor monitor VT07-B26L-W / VT07-B22L and PC Client BioTalk Pro.

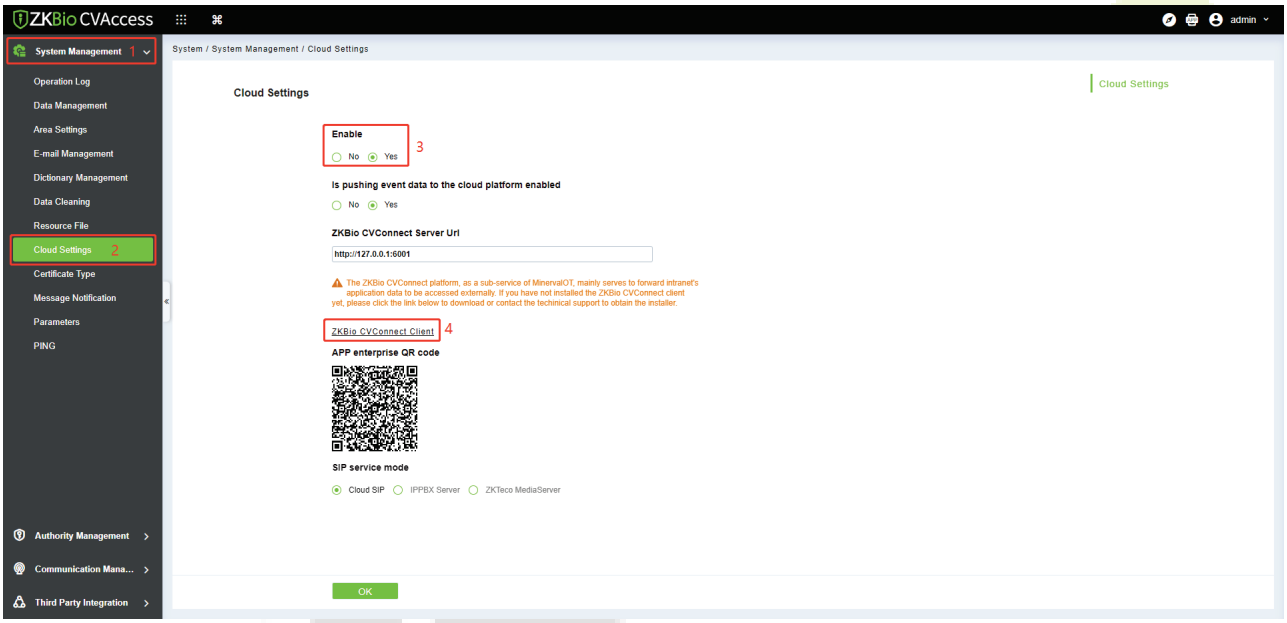
ZKBio CVAccess supports 2 kinds of SIP server: **cloud SIP** and **PBX server**, users can choose one according to the actual situation.

- **Cloud SIP mode:** Users do not need to purchase additional SIP server, only need to purchase SIP account permission.
- **PBX server:** You need to purchase a PBX server for local deployment. You do not need to purchase an additional SIP account.

The following text mainly introduces the Cloud SIP mode.

16.2.1 SIP Server Configuration

1. On the ZKBio CVAccess software, click **System** > **System Management** > **Cloud Settings** to enable the Cloud SIP service.
2. Click **ZKBio CVConnect Client** to download and install it.



Note:

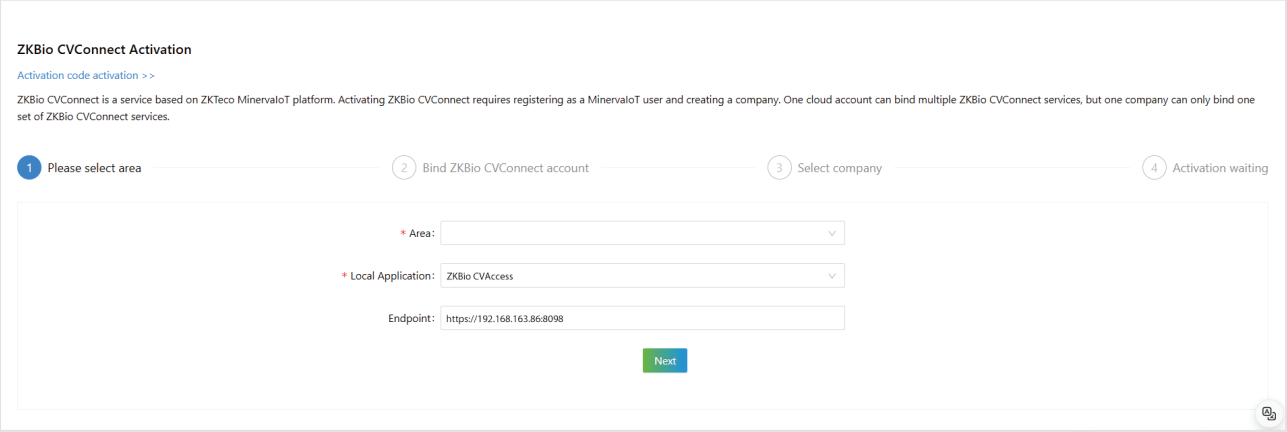
1) Ensure the ZKBio CVConnect client is installed if Cloud SIP is activated.
2) After cloud SIP is enabled, the device network needs to be able to connect to the external network before it can be used.

➢ **ZKBio CVConnect Client Activation Steps**

Step 1: Double-click the desktop shortcut key. Jump to browser page.

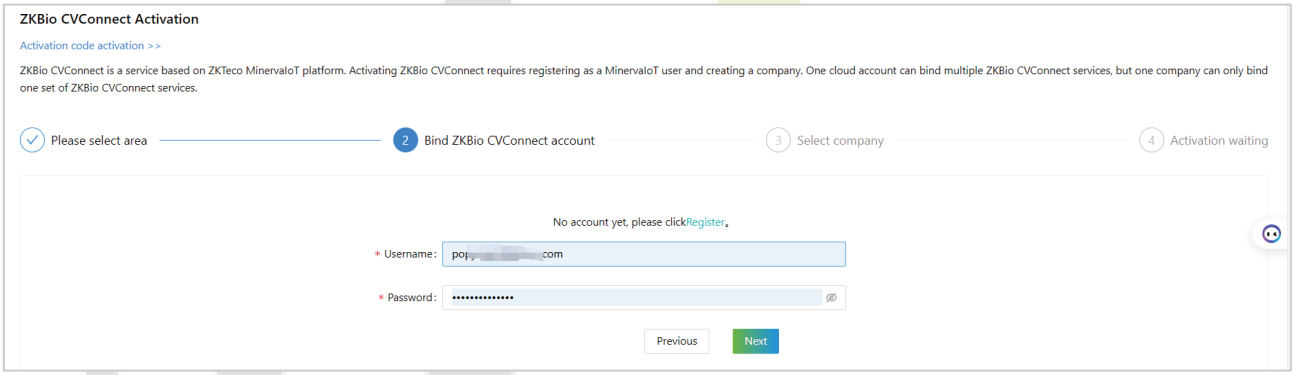
Step 2: Follow the steps on the page to complete activation.

1. Select Area



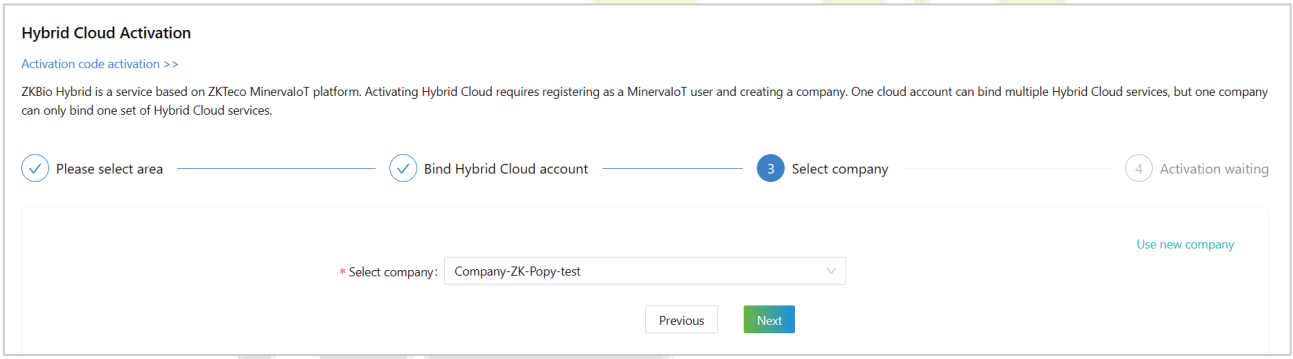
- **Area:** Select the area of the cloud server, currently only China, Singapore and America are available, other areas will be added later.
- **Local Application:** Set as ZKBio CVAccess.
- **EndPoint:** The server address of your local application. For example, if your local application is ZKBio CVAccess with a server address of https://192.168.163.86:8098, enter this server address here so that ZKBio CVConnect can correctly forward the data from your local server for access by the Mobile APP.

2. Bind ZKBio CVConnect Account

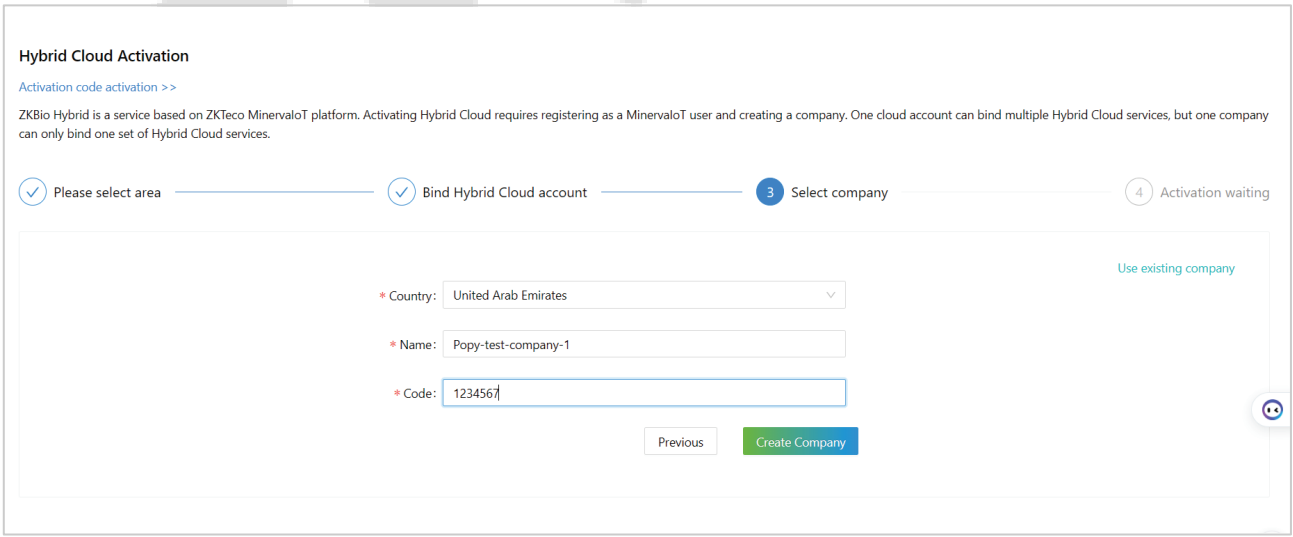


If you already have a Minerva IoT account, you can use it and log in; otherwise click on **Register**, then jump to Minerva IoT registration page and register your account.

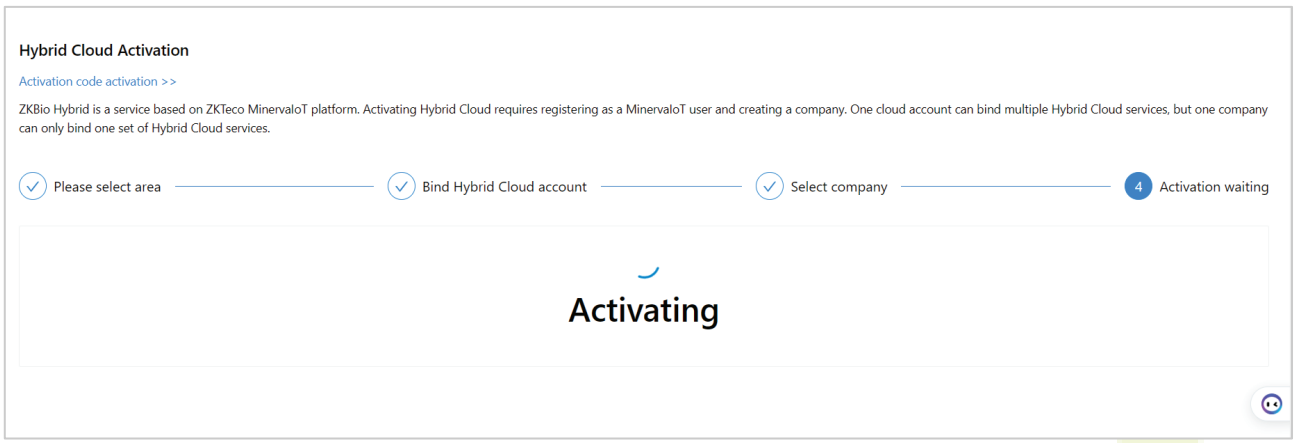
3. Select Company



If you don't currently have a company, you can choose to create one by clicking **Use New Company.**



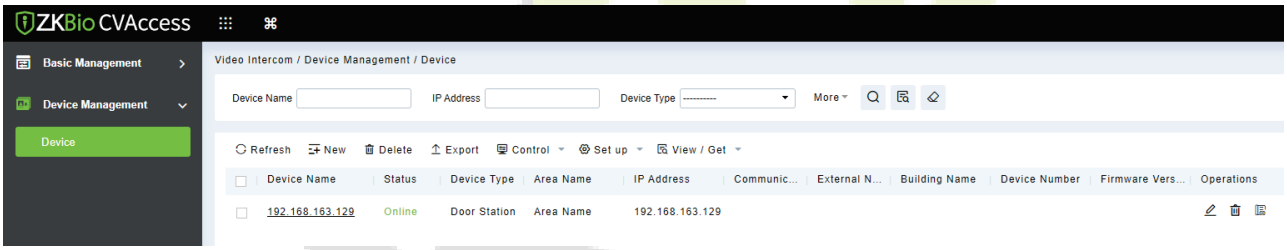
Start Activating and wait for 1-2 minutes until the Activation completely.



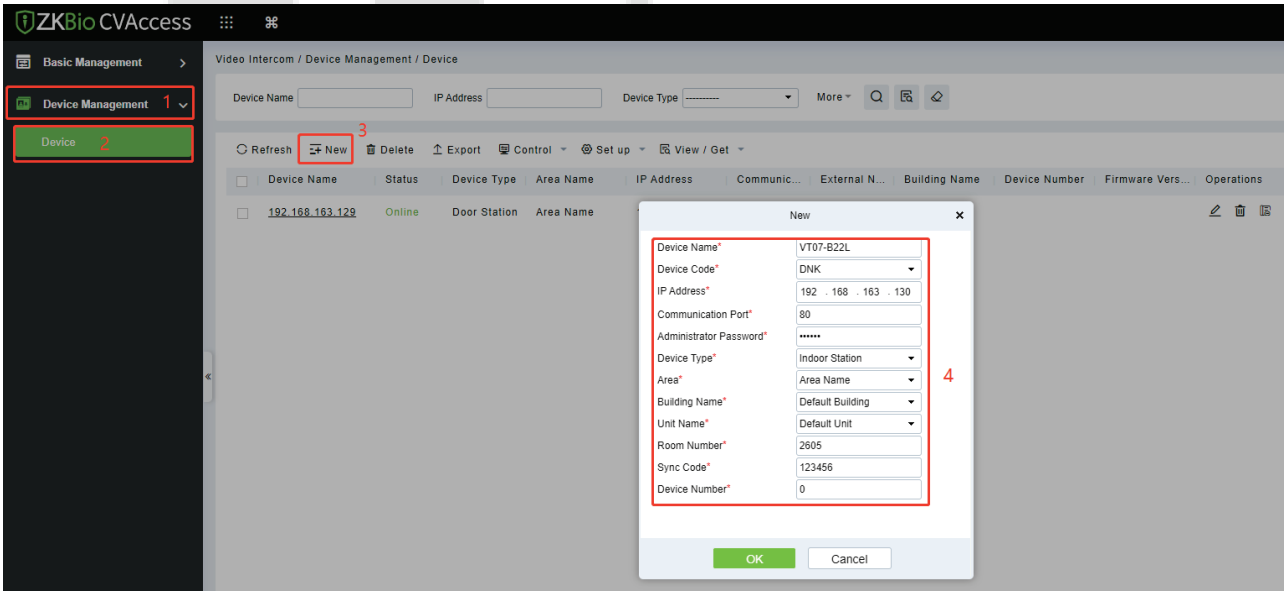
The specific installation and activation steps of the ZKBio CVConnect client can refer to ZKBio Zexus Mobile App User Manual.

16.2.2 Add Device

1. Add the device to the **Access** Module of the software. Then the device will be automatically synchronized to the **Video Intercom** module. (The adding method can refer to 15 Connect to ZKBio CVAccess Software)



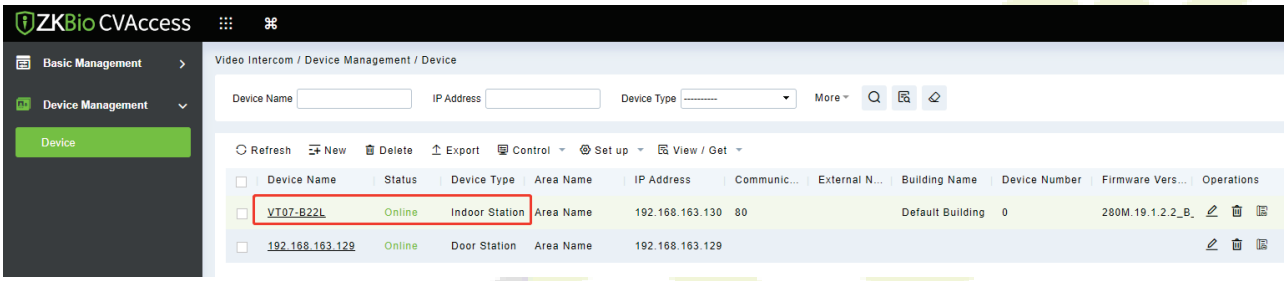
2. Click **Video Intercom > Device Management > Device > New** to add the indoor monitor.



- **Device Name:** Enter the name of the indoor monitor.

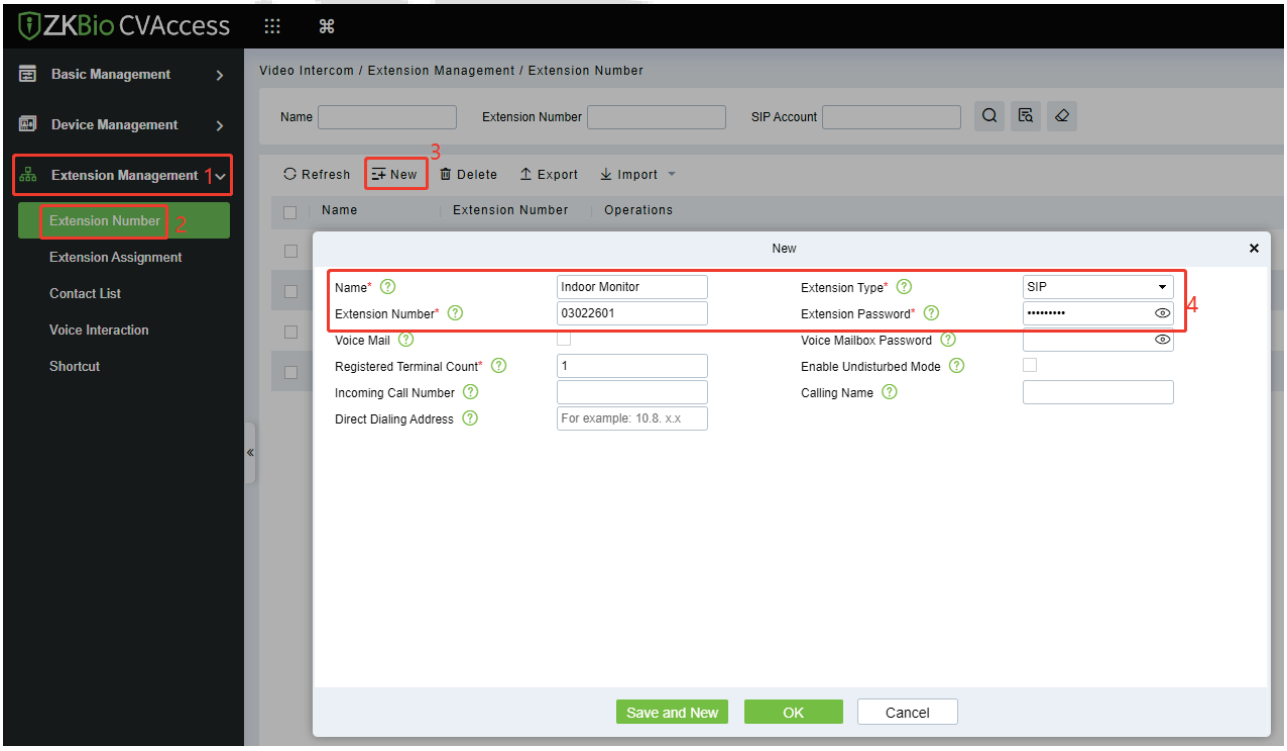
- **Device Code:** Set as DNK.
- **IP Address:** Enter the IP address of the indoor monitor.
- **Communication Port:** 80 by default.
- **Administrator Password:** 123456 by default.
- **Device Type:** Set as Indoor Station.
- **Area/ Building Name/Unit Name:** Select from the drop-down list.
- **Room Number:** Customize the number of the indoor monitor.
- **Sync Code:** Can be customized by the user. (It is used when a resident has multiple indoor monitors. The indoor monitors which have the same Sync Code will be called at the same time.)
- **Device Number:** The setting range is 0-9. For example, if there is only one indoor monitor in the room, the device number will be 0. If there are two units, one will be 0 and the other will be 1, and so on.

3. After the addition is successful, the indoor monitor will be displayed in the device list.



16.2.3 Create Extension Numbers

Click **Video Intercom > Extension Management > Extension Number > New** to create extension numbers.

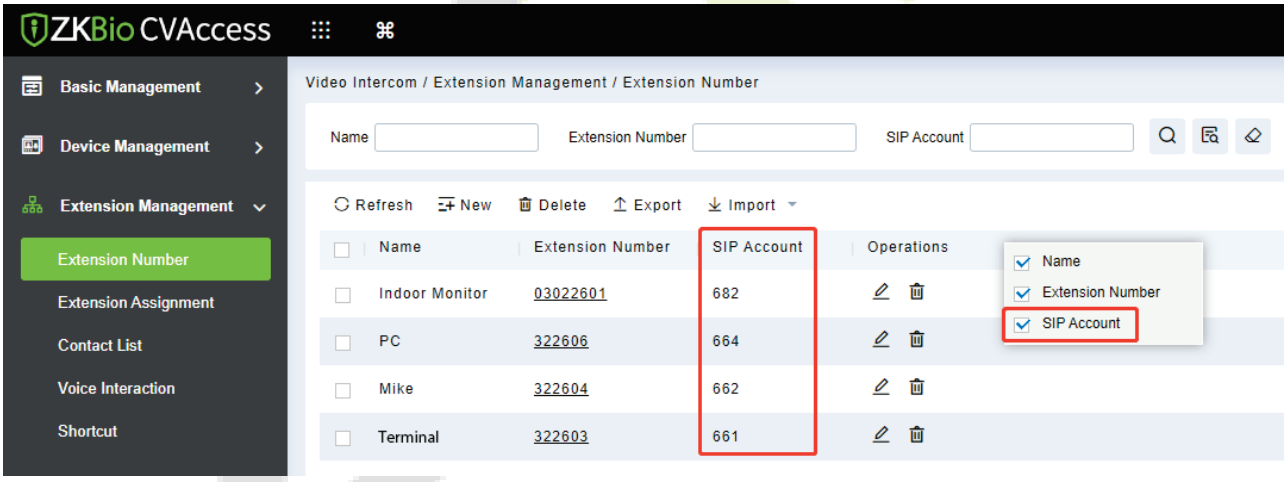


- **Name:** Customize the extension name. If it is a residential scene, the name can be set to the room number; if it is an office scene, the name can be set to the work number and name information.
- **Extension Type:** SIP by default.
- **Extension number:** Customize the extension number, it can be up to 8-digit; for example, the number of Room 401, Unit 2, Building 1 can be defined as 01020401 for quick internal identification.
- **Extension Password:** User's SIP account password, which can be used to request account registration from the SIP service.
- **Registered Terminal Count:** The maximum number of terminals that a user can register to the same number. When the number of concurrent registrations is 1, it means that new registrations are allowed to preempt the registration address. When the number of concurrent registrations is 2 or more, new registrations will be automatically blocked once the number of registrations reaches the limit.

After the user creates the extension number, the system will automatically generate a SIP account. For example, assuming the user has created the extension number 322603, the system automatically generates the SIP account as 661, so the SIP User Name used on the terminal is 661.

Note:

1) The SIP Account column is hidden by default. You can right-click the row which Operations is in and check the SIP Account to display it.

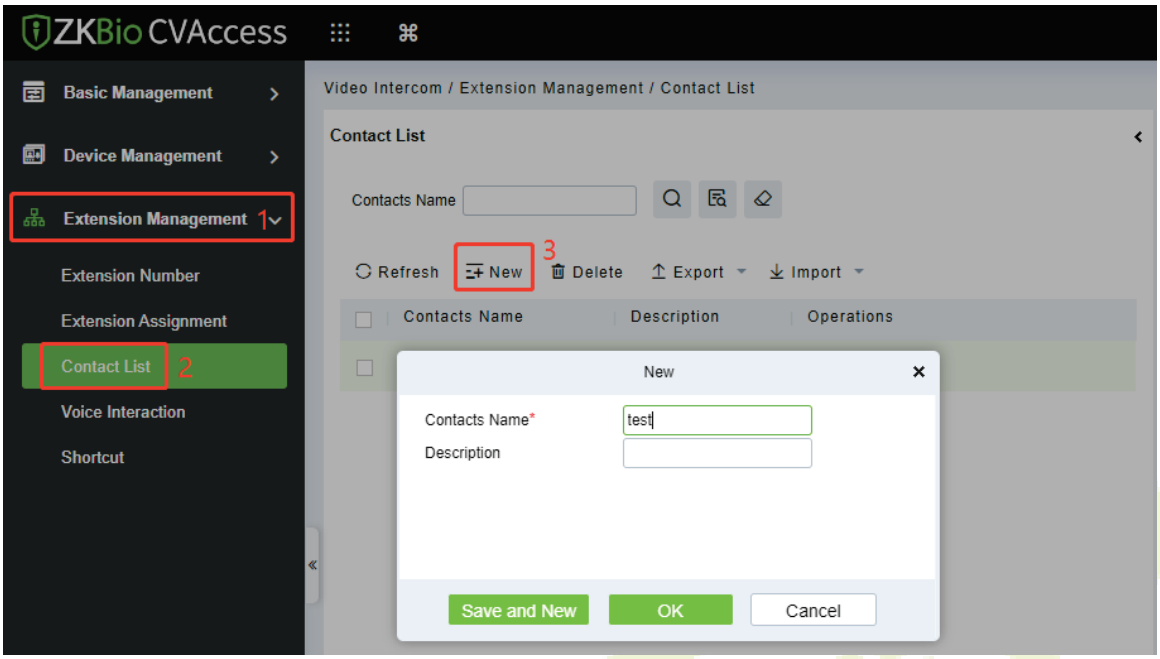


2) If you use a PBX, the extension number will be directly used, and the SIP account list will be empty.

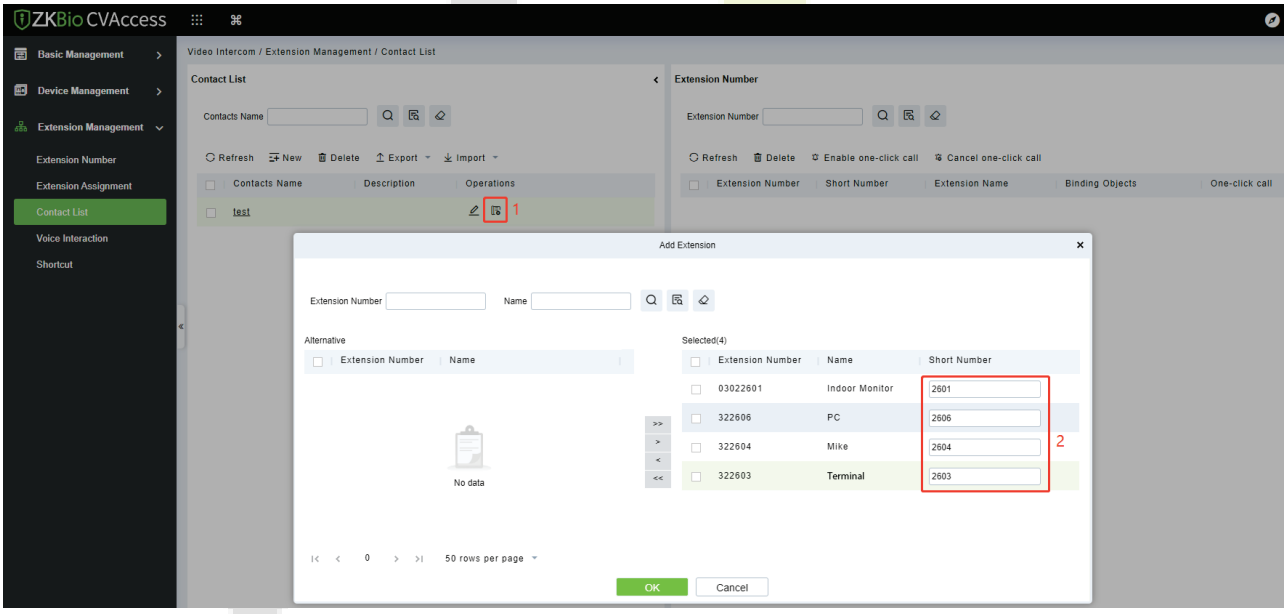
16.2.4 Contact List

If you need to enable different devices or personnel to view a limited number of contacts, you can configure the contact list.

1. Click **Extension Management > Contact List > New** to create a contact list.



2. Click the icon to add extension numbers to the contact list. During the process of adding extension numbers, you can define a short number for the extension on the right, for example, if the number for Room 1101 is defined as 101. After defining and synchronizing the short number to the device, the device can then dial the short number 101 to call that room.



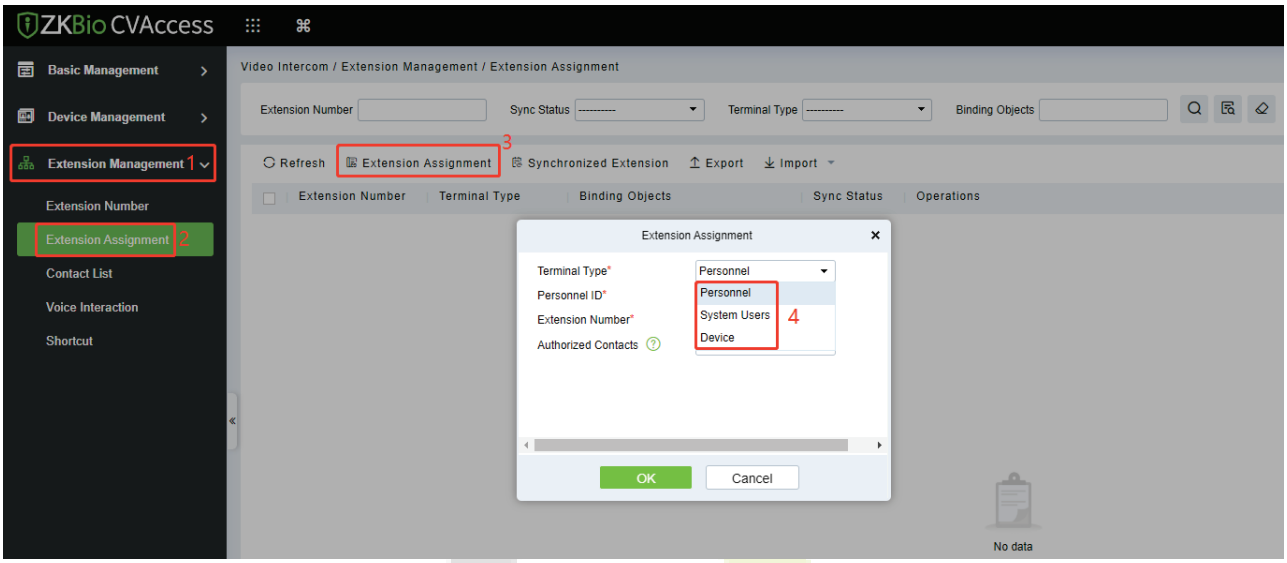
Note:

1) If you add an extension number to the contact list without editing the short number, and you wish to edit it later, you will need to delete the extension number from that contacts and then edit it when re-adding, or delete it and use the import function afterward.
2) If the device is set to be a fence terminal, please do not define the short number of the indoor monitors. You just need to input the block, unit and room number to call the indoor monitor.

16.2.5 Assignment of Extension Numbers and SIP Accounts

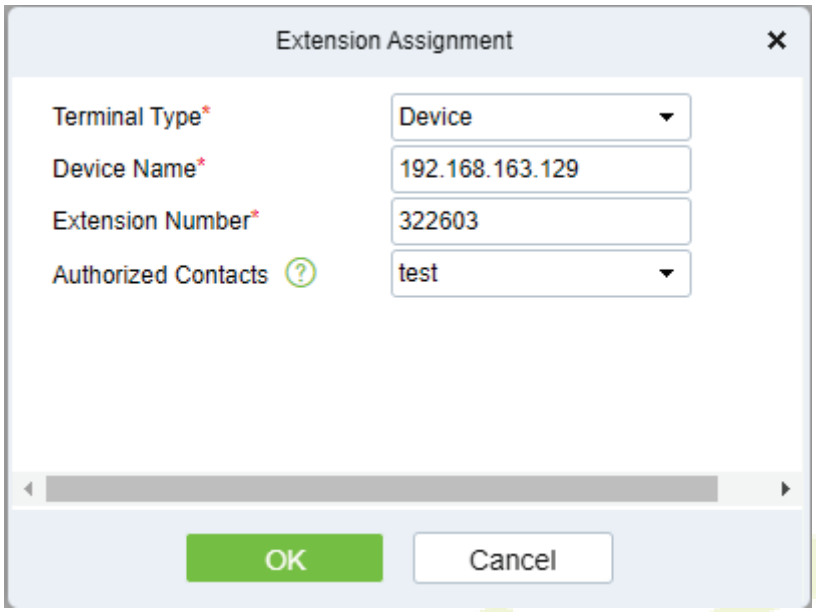
The extension number or SIP account can be assigned to personnel, devices or system users. After allocation, personnel and users' APP will be able to directly use video intercom for communication. The device can also be used directly without manual additional configuration.

Click **Extension Management > Extension Assignment > Extension Assignment**, select the Terminal Type.

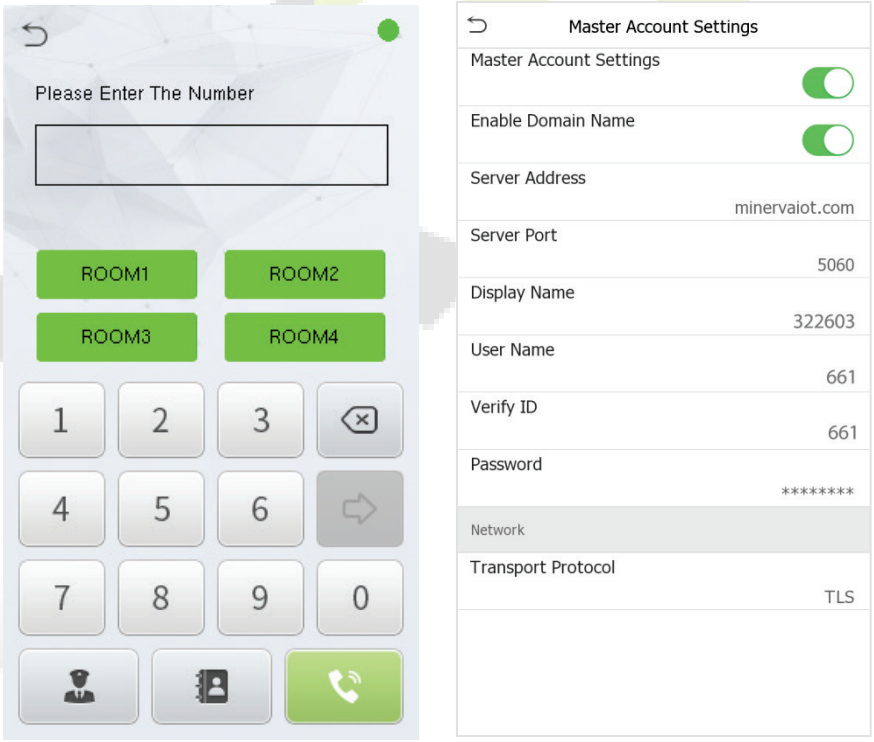


- **Device Account Assignment**

1. Select the Terminal Type as **Device**.
2. Select the device need to be bound (device or indoor monitor) and the extension number. The account information will be automatically synchronized to the device. Select the Authorized Contacts to assign the contact list to the device; only after the assignment can the device call room numbers/short numbers or make calls through the contact list search.

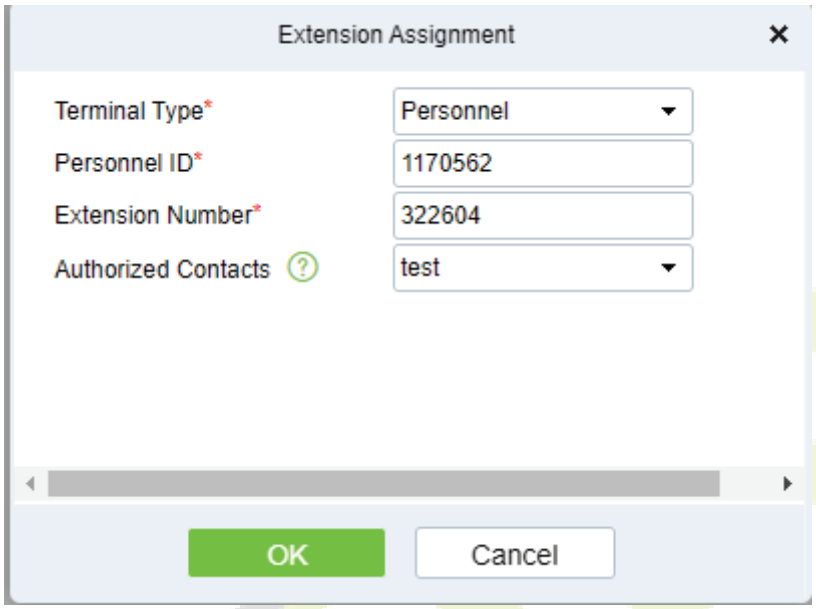


3. After successful assignment, a green dot will appear in the upper right corner of the call page, indicates that the device is connected to the server. You can also click **Intercom > SIP Settings > Local Settings > Master Account Settings** to see that SIP server and account information have been automatically written, as shown in the following figure.



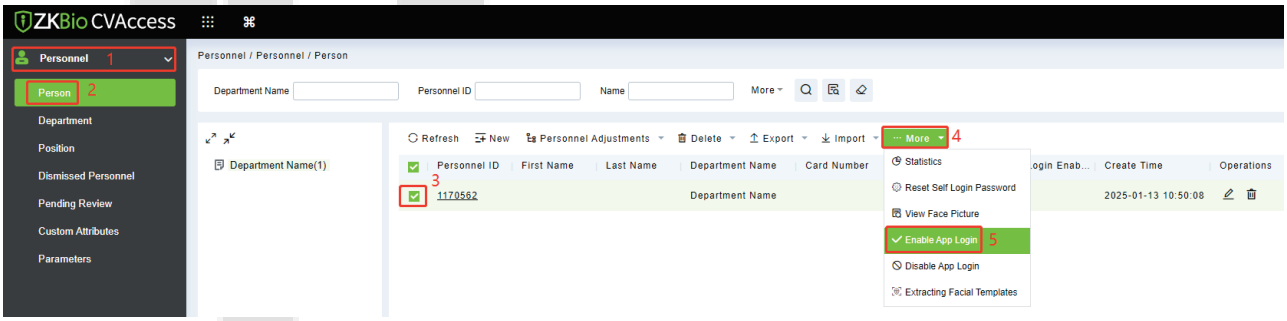
- **Personnel Account Assignment (ZKBio Zexus App)**

1. Select the Terminal Type as **Personnel**.
2. Select the person to be assigned an account and the extension number. Select the Authorized Contacts to assign the contact list to the individual, and after the assignment, the individual can view the contacts in the contact list upon logging into the ZKBio Zexus App.

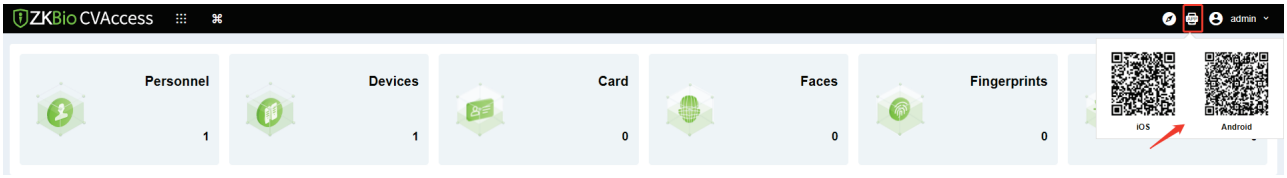


Note:

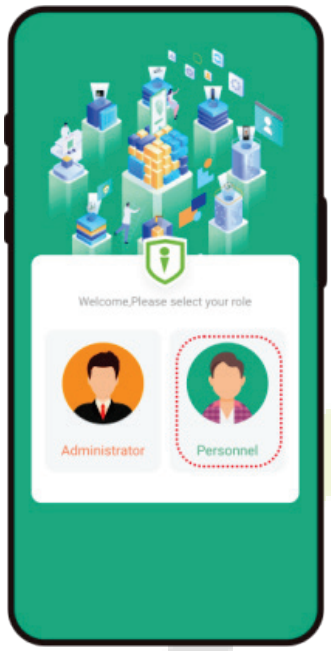
1) Before assign account to the personnel, you need first add personnel in ZKBio CVAccess. The adding method can refer to 15 Connect to ZKBio CVAccess Software.
2) The personnel need to enable APP Login. (Click **Personnel > Personnel > Person > More > Enable APP Login**.) Once a person has enabled APP login, they can directly access the Video Intercom feature upon logging into the App.

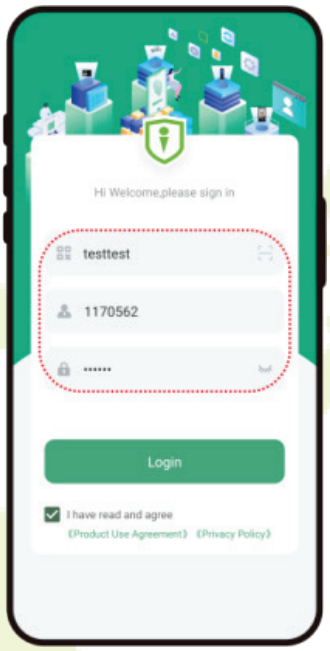


3) You can click the icon at the right top corner of the ZKBio CVAccess interface to scan the QR code to install the ZKBio Zexus App.

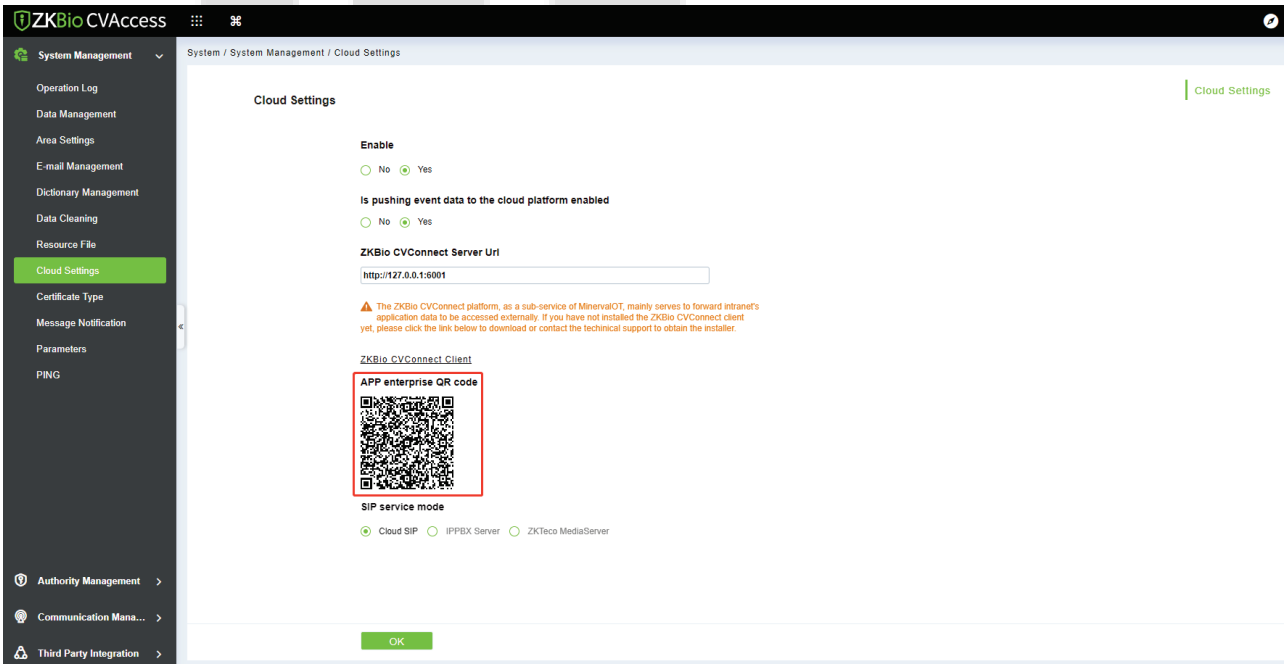


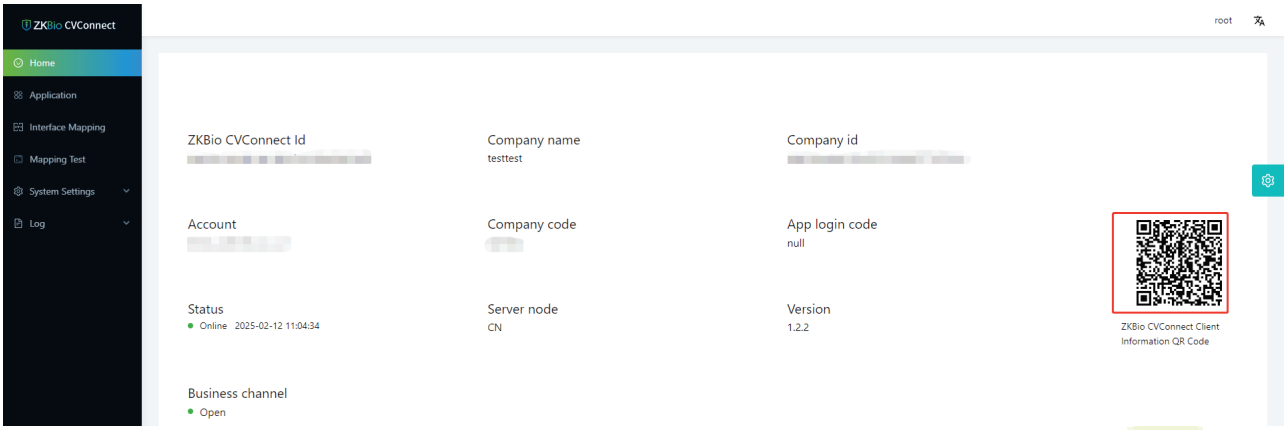
3. After successful assignment, the personnel can login to the App. Select the role-**Personnel**, enter the account information, and click **Login**.





Organization Name: Scan the organization code you get before. (Go to ZKBio CVAccess web, enter **System > System Management >Cloud Setting >APP enterprise QR Code**, or go to ZKBio CVConnect client, scan the ZKBio CVConnect Client Information QR Code.)



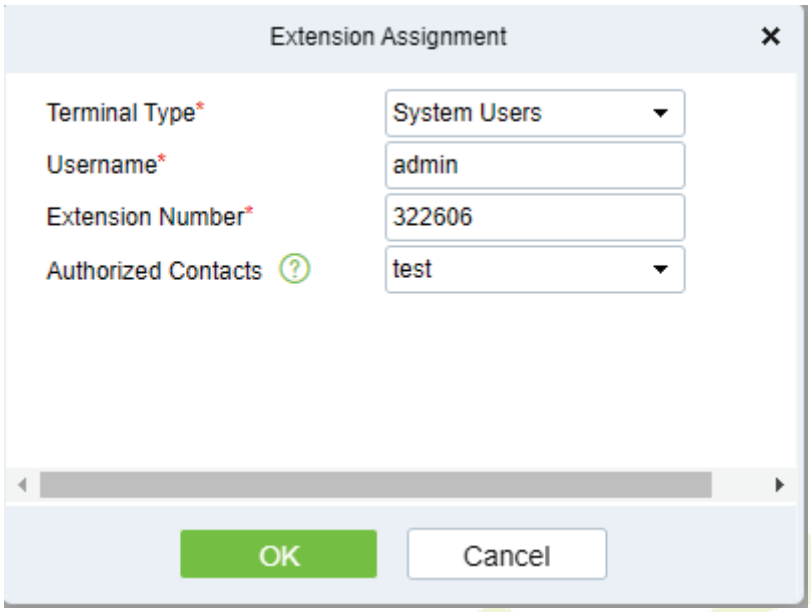


Account & Password: The personnel ID & password (default: 123456).

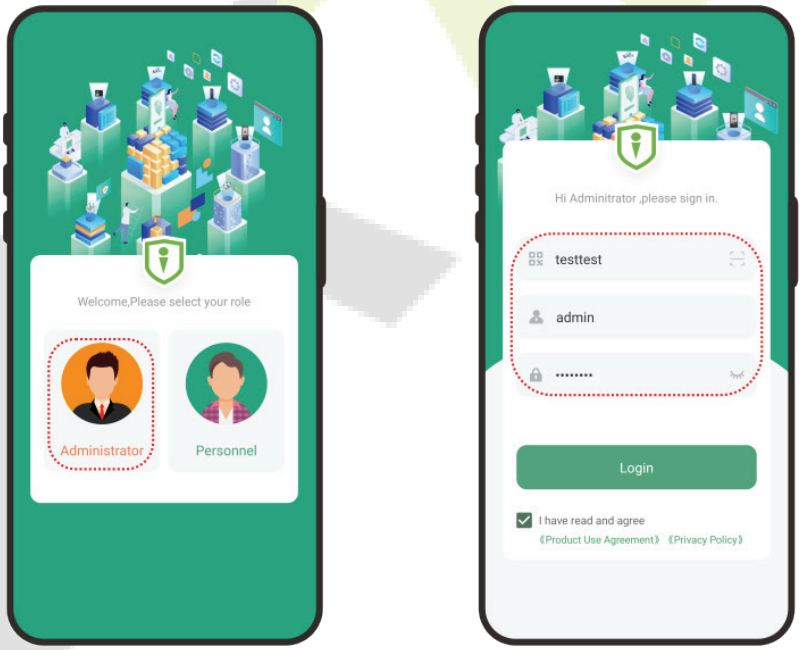
4. Click **Application Center** > **Video Call** to enter the video call application, and the status will be displayed as **Connected**. If the person has not assigned an extension number, entering the application will prompt "you have not assigned an extension number, please contact the administrator". Then you can directly enter the extension number of the device or click the icon to search for the device and call it.

- **System User Account Assignment (ZKBio Zexus App)**

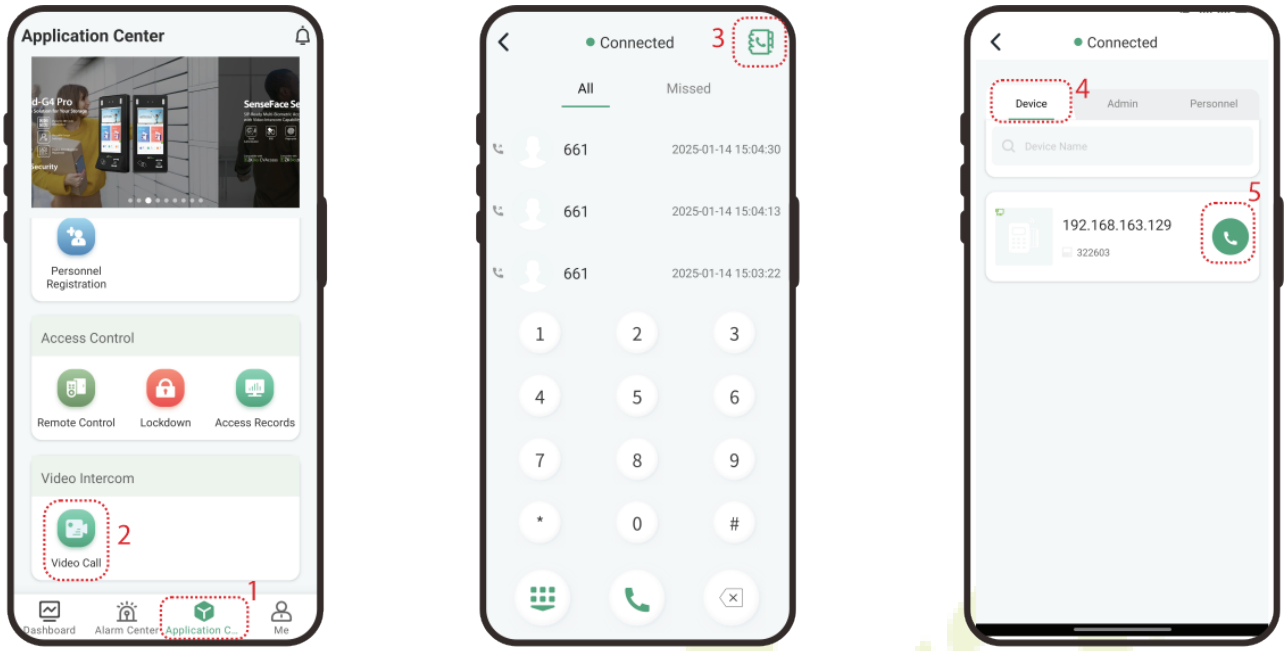
1. Select the Terminal Type as **System Users**.
2. Select the system user to be assigned an account and the extension number. Select the Authorized Contacts to assign the contact list to the admin, and after the assignment, the admin can view the contacts in the contact list upon logging into the ZKBio Zexus App.



3. After successful assignment, the admin can login to the App. Select the role-**Administrator**, enter the account information, and click **Login**.
Organization Name: Scan the organization code you get before.
Account & Password: The administrator account; Same account & password as ZKBio CVAccess.



4. Click **Application Center** > **Video Call** to enter the video call application, and the status will be displayed as **Connected**. Then you can directly enter the extension number of the device or click the icon to search for the device and call it.



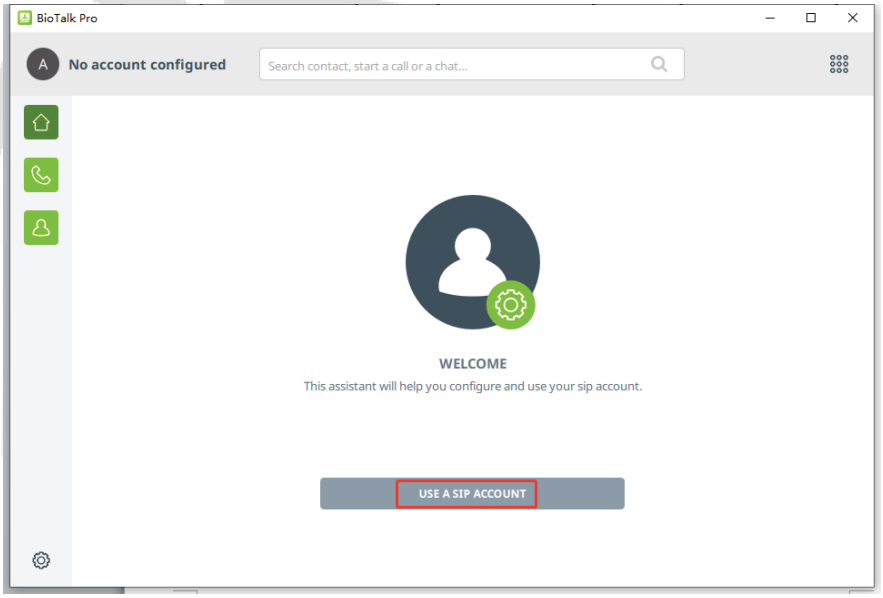
The App complete operation steps please refer to the ZKBio Zexus Mobile App User Manual.

16.2.6 PC Client Functionality

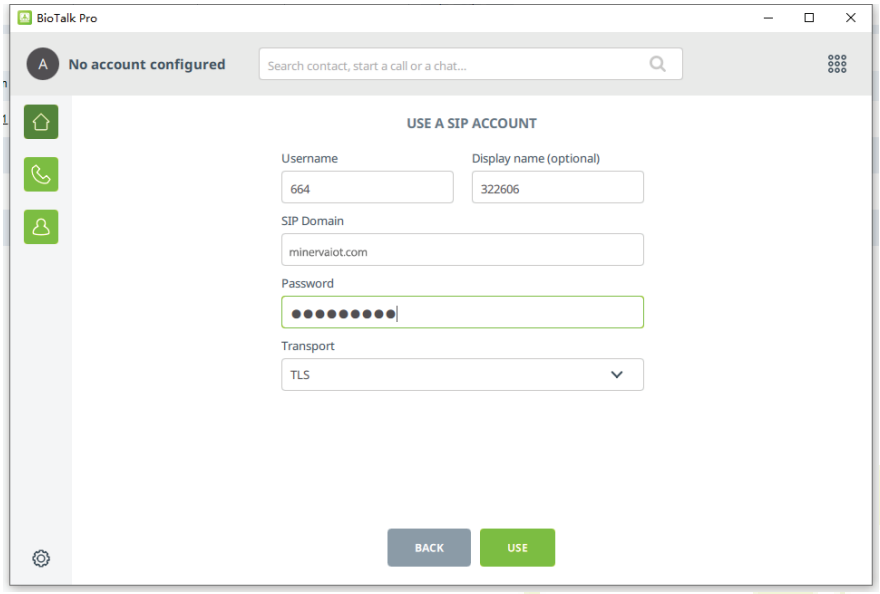
To use the BioTalk Pro PC client, please contact the appropriate person for an installation package.

Operation Guide

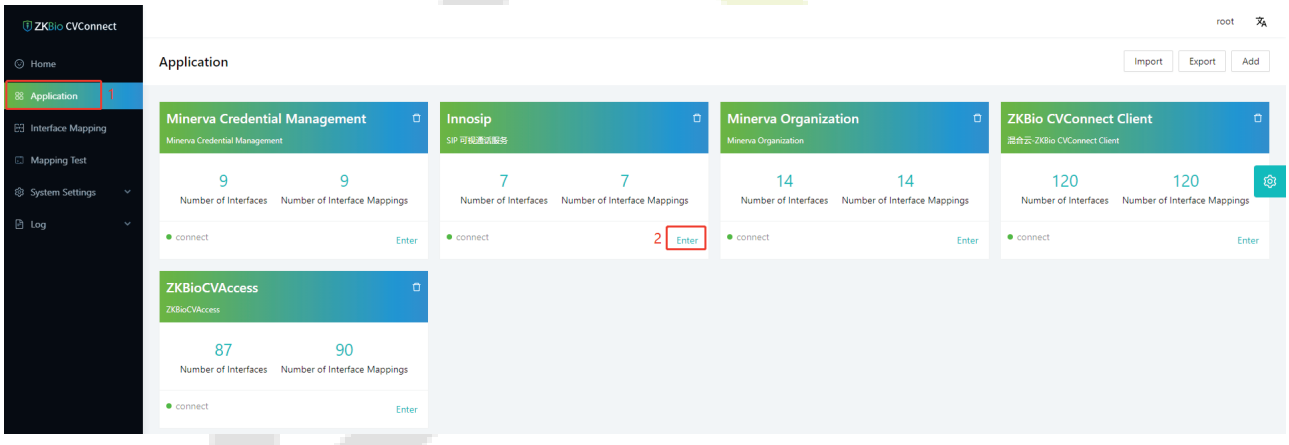
Step 1: Configure the SIP account: Click **USE A SIP ACCOUNT** button.

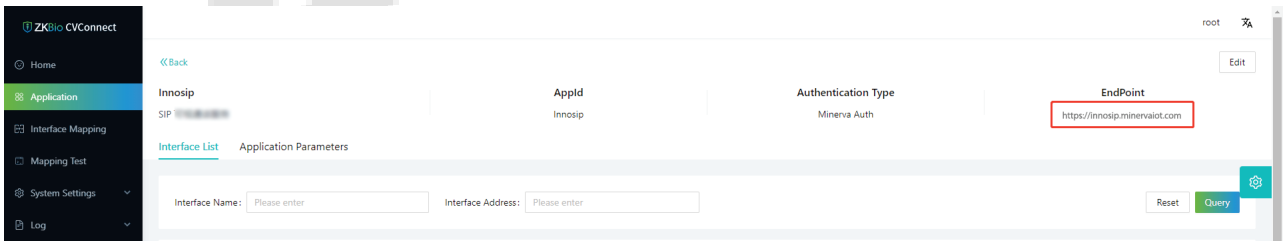


Step 2: Fill in the SIP account information in order and click **USE**.



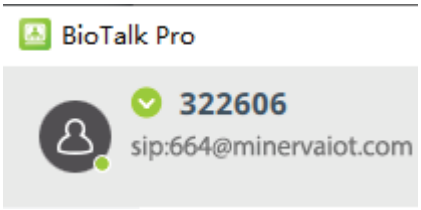
- **Username:** Enter the SIP account. (**Note:** You need to create a new SIP account for the PC client in ZKBio CVAccess, then you can use the account to login to the PC client.)
- **Display Name:** It is the extension number.
- **SIP Domain:** The SIP Server Domain. (Go to ZKBio CVConnect client, click **Application > Innosip > Enter**, the EndPoint address is "https://innosip.minervaiot.com". Then 'minervaiot.com' is the actual SIP server domain you need to enter on the PC Client.)





- **Password:** The extension password of the SIP account for PC client.
- **Transport:** Transportation Protocol, TLS by default.

Wait 1 minute until the status shows Connected, as shown below:

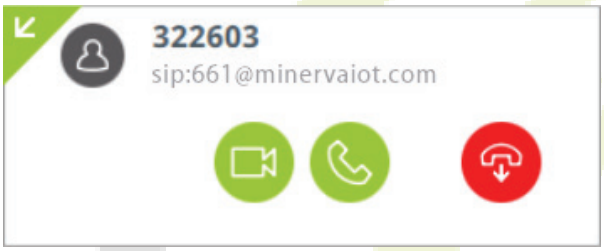


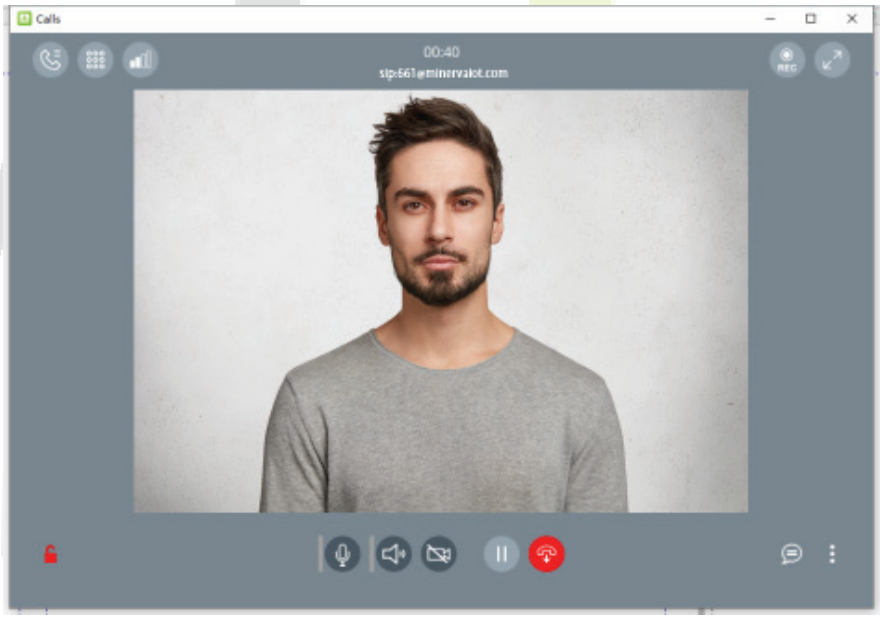
Note: In the Cloud SIP mode, if dialing is required, the PC Client should dial directly to the target SIP account. For example, if the extension number created on ZKBio CVAccess is 322603, the corresponding generated SIP account is 661, then the PC Client should dial 661 when making a call. Therefore, it is recommended to directly create a contact in the address book with the number 661.

At this point you can start to use it normally, the PC client, the device and the App can call and answer each other.

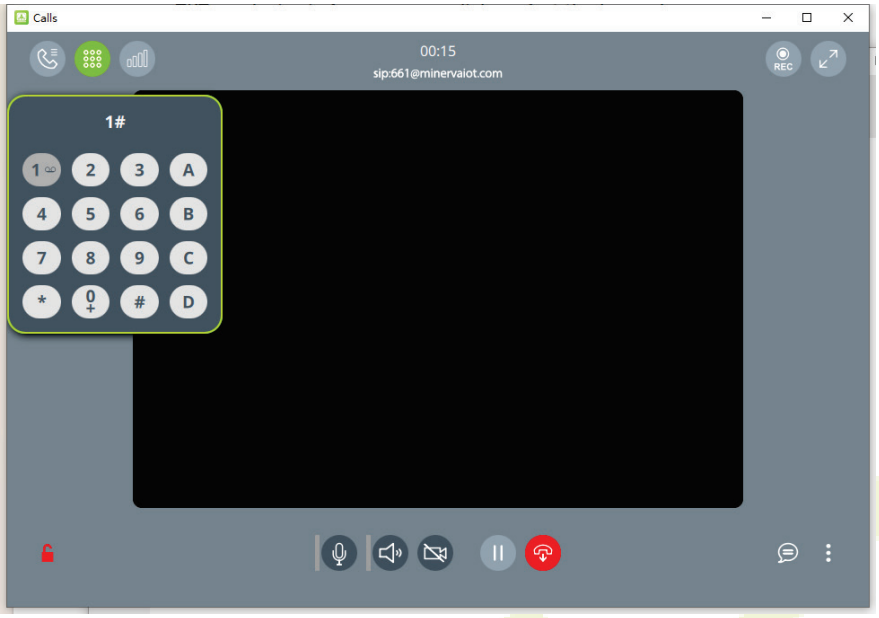
When the PC Client receives a call, a window alert will pop up in the lower right corner of the desktop.

Click the icon to accept it.





You can open the door by clicking on the keypad and entering the DTMF value of the device, e.g. the default value of ZKTeco device is 1, so you can click on 1 at the keypad.

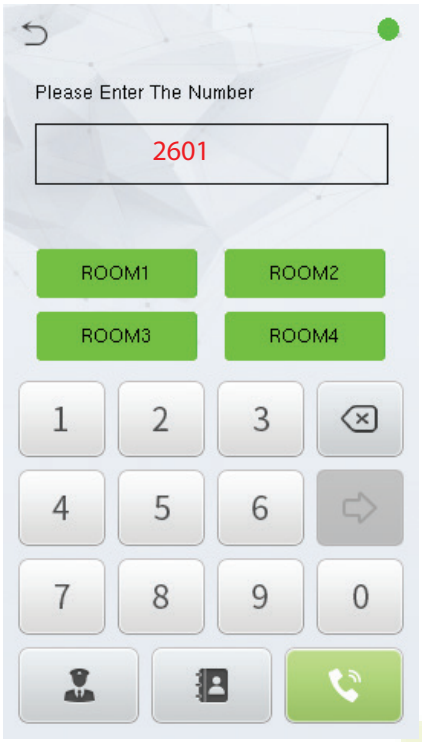


16.2.7 Make a Call

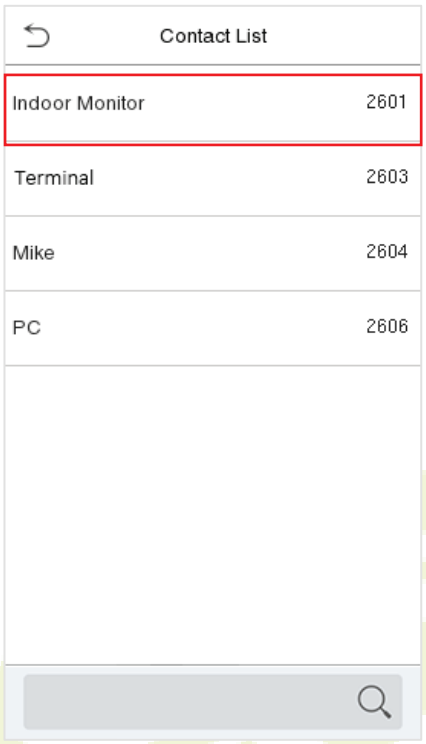
Two-way calls can be made between the device, indoor monitor, ZKBio Zexus App, and PC client (BioTalk Pro).

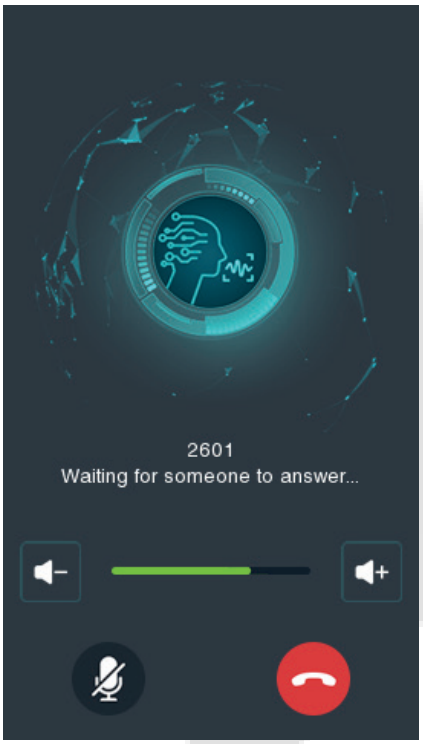
- **Device Call the Indoor Monitor (VT07-B26L-W / VT07-B22L)**

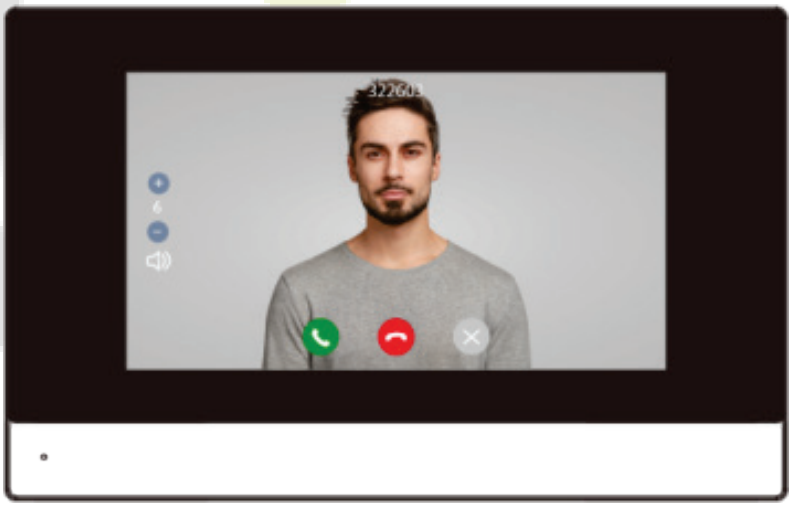
1. Add the indoor monitor on the ZKBio CVAccess software, then assign an extension number to the indoor monitor. (The operations steps can refer to 16.2.2 Add Device and 16.2.5 Assignment of Extension Numbers and SIP Accounts)
2. Click the icon on the device and enter the Short Number of the indoor monitor in the pop-up interface of the device. Or click the icon on the call page to open the contact list and search for the indoor monitor to call it.



or

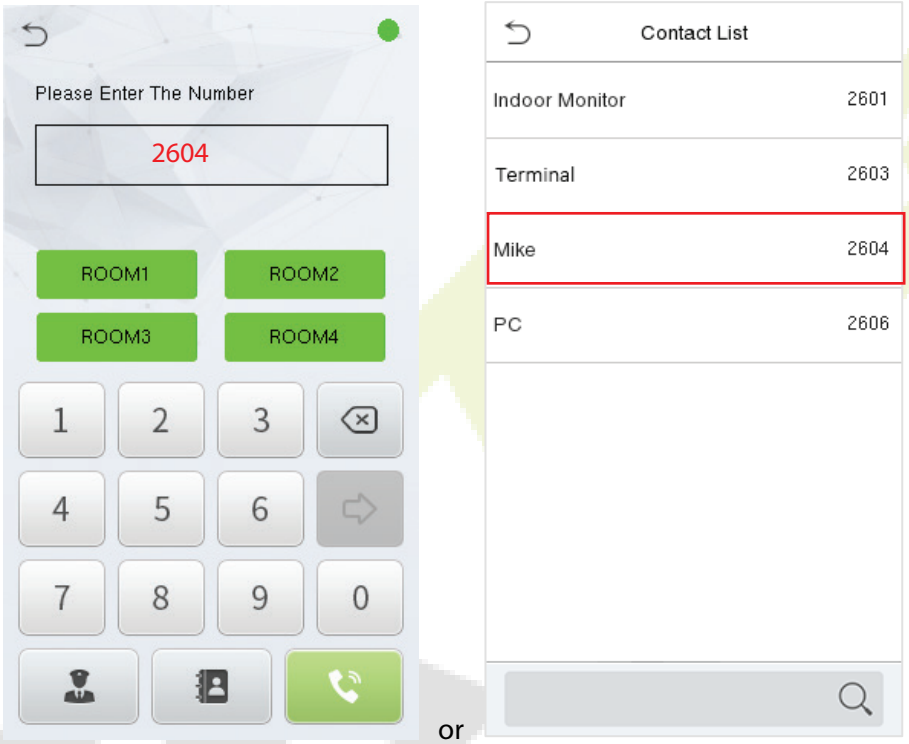


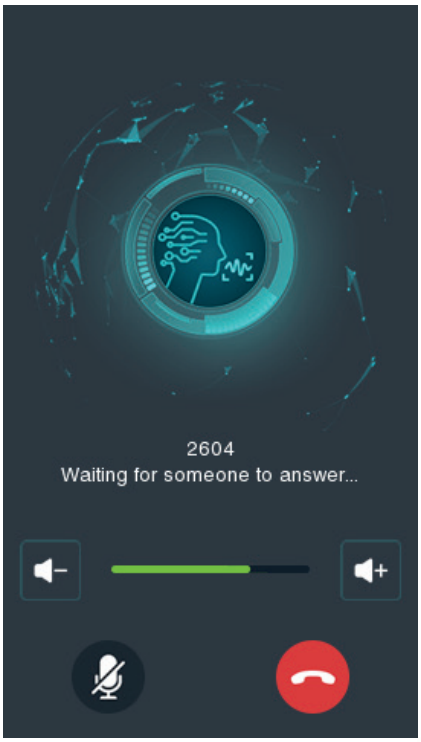


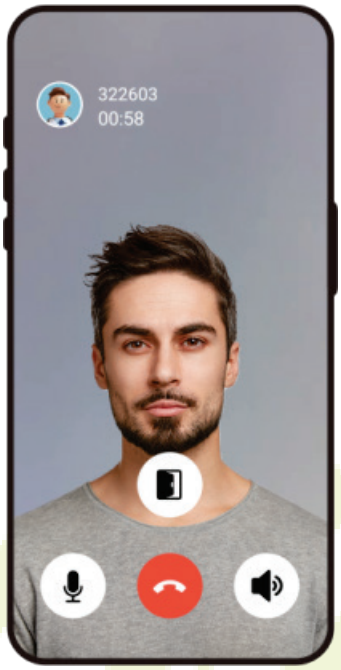


- **Device Call the Phone (ZKBio Zexus App)**

1. On the ZKBio CVAccess software, assign an extension number to the personnel. (The operations steps can refer to 16.2.5 Assignment of Extension Numbers and SIP Accounts)
2. Click the icon on the device and enter the Short Number of the personnel in the pop-up interface of the device. Or click the icon on the call page to open the contact list and search for the personnel to call him/her.

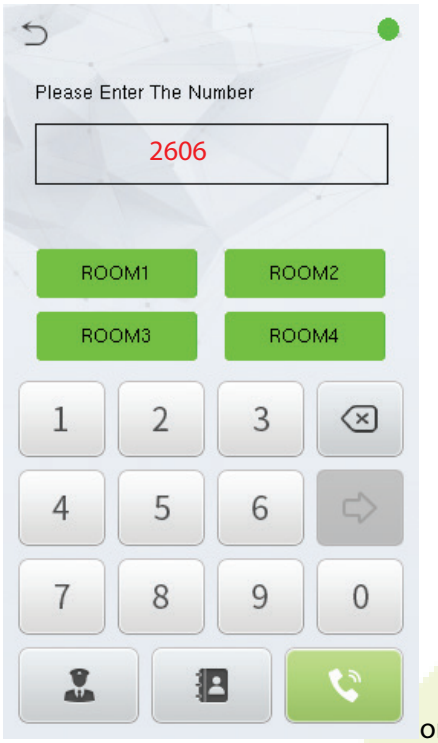




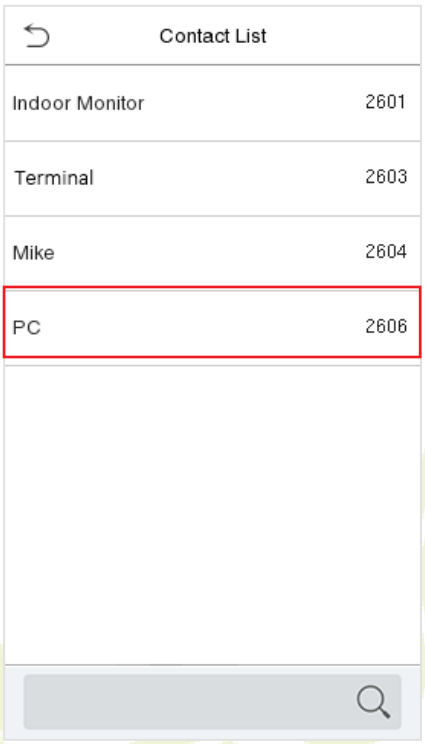


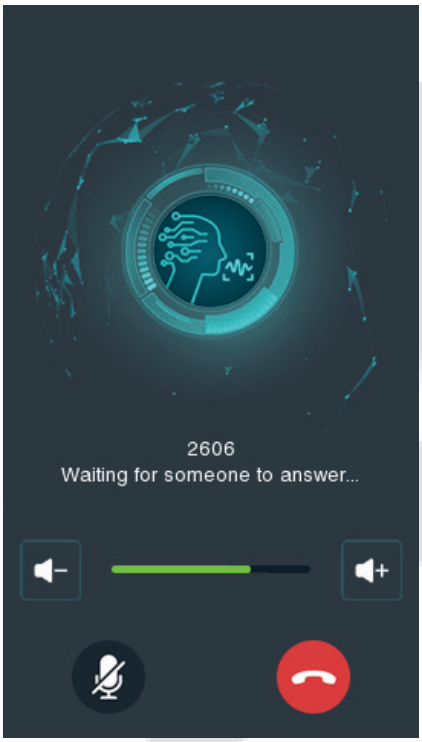
- **Device Call the PC Client (BioTalk Pro)**

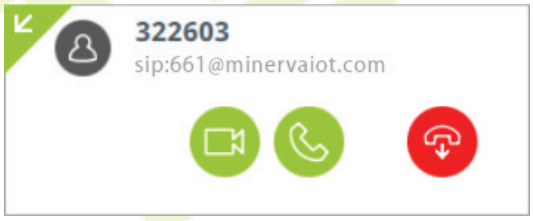
1. Install the BioTalk Pro software and configure the SIP account. (The operations steps can refer to 16.2.6 PC Client Functionality)
2. Click the icon on the device and enter the Short Number of the PC client in the pop-up interface of the device. Or click the icon on the call page to open the contact list and search for the PC client to call it.

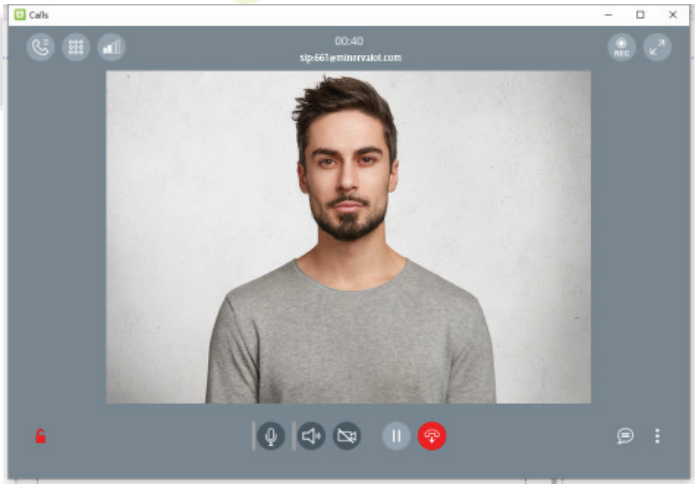


or



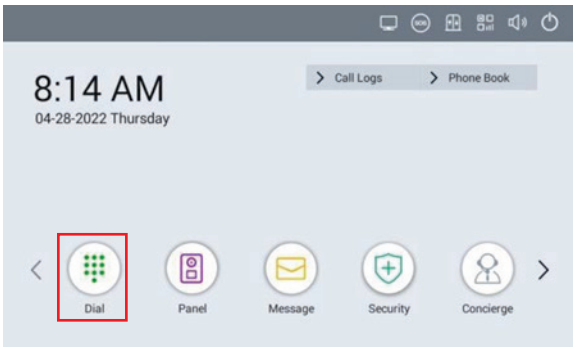


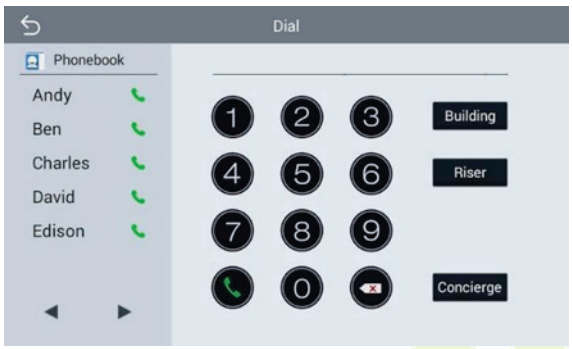




- **Indoor Monitor Call**

Click the **Dial** icon, then enter the SIP Account to make a call.





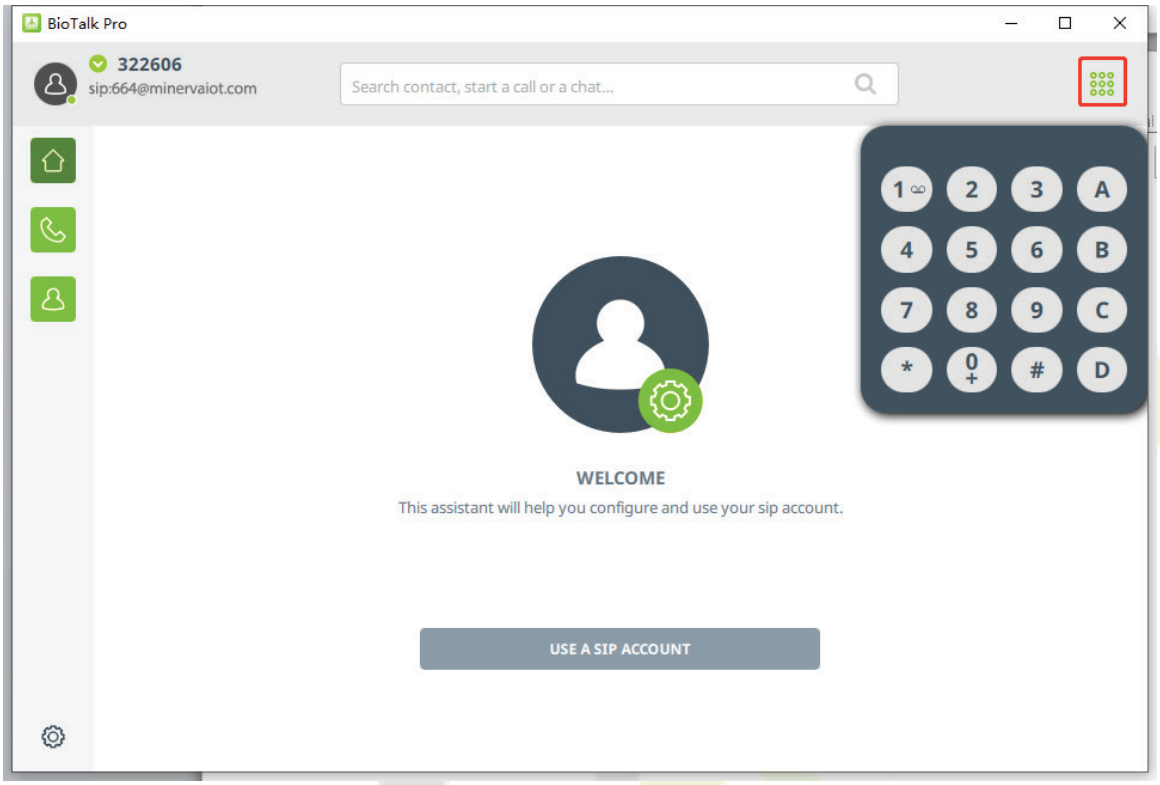
Note: The indoor monitor is not supported the assignment of the contact list in ZKBio CVAccess.

- **Phone Call**

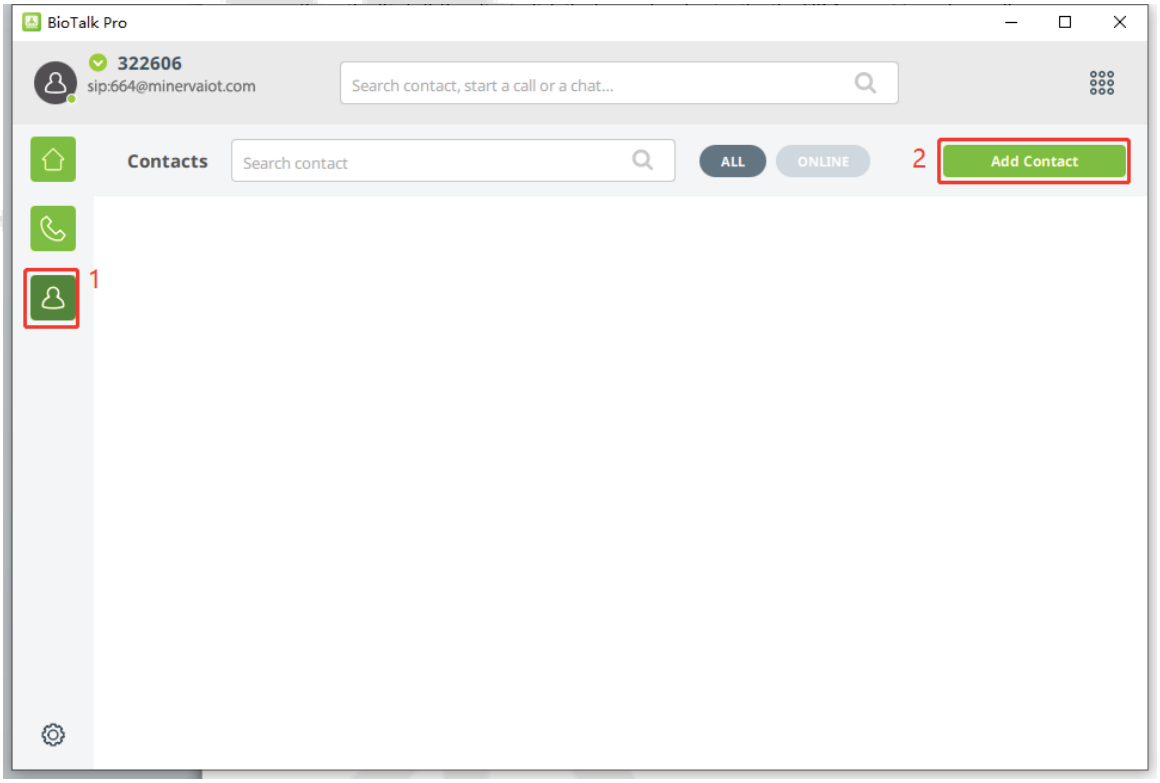
Login to the ZKBio Zexus App, click **Application Center > Video Call** to enter the video call application, Then you can directly enter the extension number or click the icon to search for the one you want to call.

- **PC Client (BioTalk Pro) Call**

Open the BioTalk Pro client, click the keypad and enter the the SIP Account to make a call.



You can click the icon > **Add Contact** to add the contact list manually.



17 Connecting to ZKBio Zlink Mobile App

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

Change the device communication protocol to BEST protocol, then the device can be managed by ZKBio Zlink, please refer to 6.7 Device Type Setting.

- **Download the ZKBio Zlink Mobile App**

Search for the "ZKBio Zlink" Mobile App in the iOS App Store or Google Play Store. Or scan the QR code below to install the app.

Apple App Store

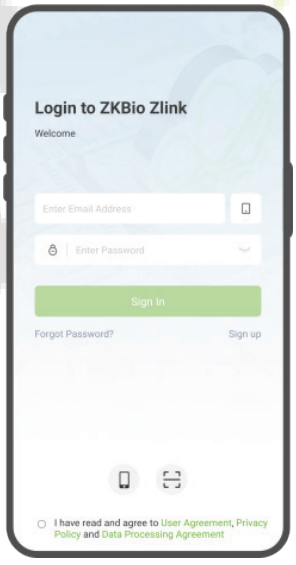
Google Play Store

Download on the App Store

GET IT ON Google Play

17.1 Login to the Mobile App

Enter your registered account and password, check “I have read and agree to User Agreement, Privacy Policy and Data Processing Agreement” and click **Sign In** to log in to the Mobile App.



Note: *For more operations, refer to the ZKBio Zlink App's user manual.*

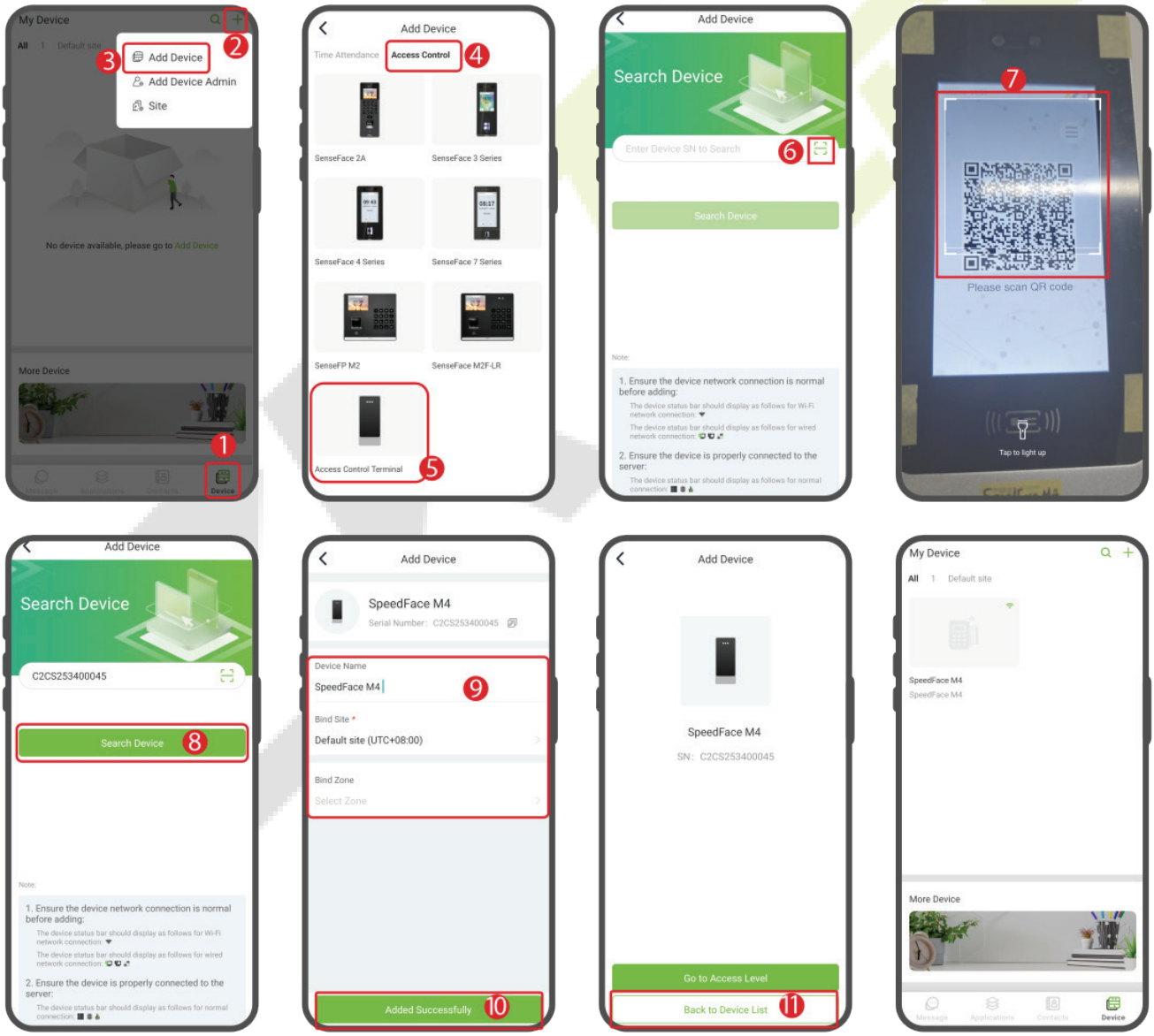
17.2 Add Device on the Mobile App

1. Access the ZKBio Zlink Mobile App and click on [**Device**] > + icon > [**Add Device**] > [**Access Control**] > [**Access Control Terminal**].

2. Click icon to scan the QR code on the device. The serial number of the device will be displayed in the bar. Then click **[Search Device]**.

3. Enter the device name and specify the device to a site and zone. Click [**Added Successfully**] to complete the addition. At the same time, the device voice prompts "**Device is added successfully**" indicating that the addition is complete.

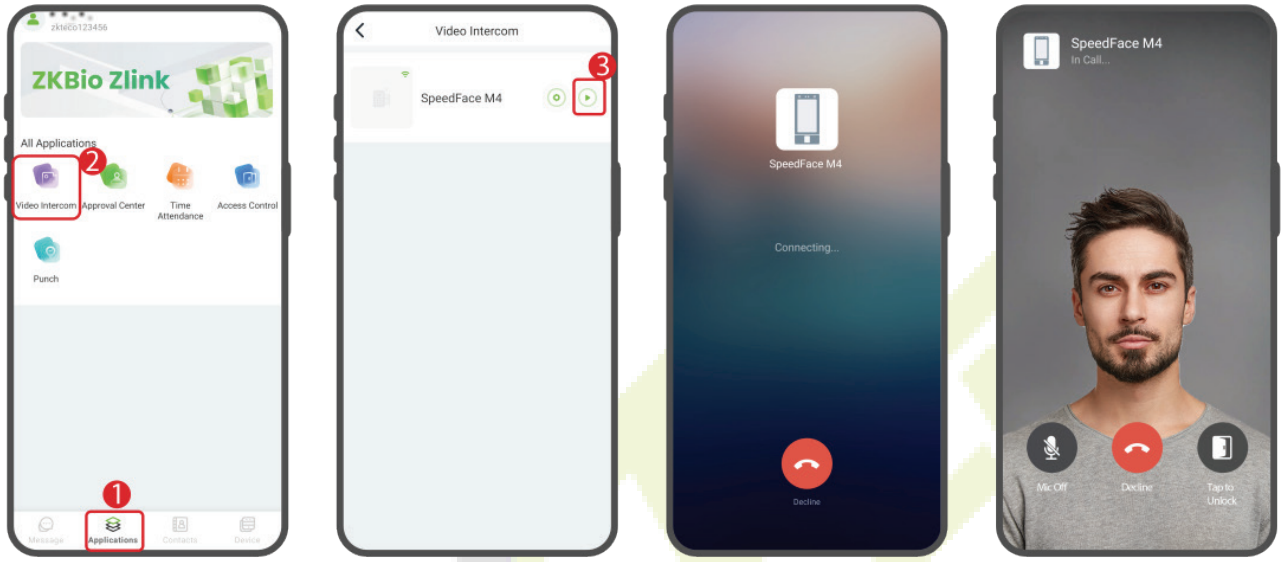
4. Once successfully added, the device is displayed in the list of the device interface. Then you can set the access levels and video intercom function as needed.



17.3 Video Intercom

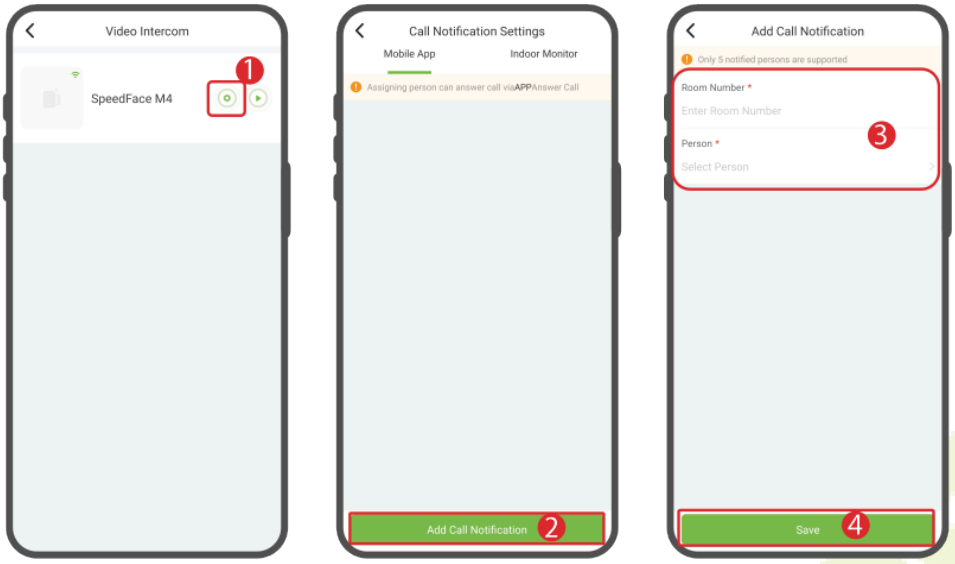
Phone Call the Device

Click [**Applications**] > [**Video Intercom**] > icon can call the device. Click **Tap to Unlock** icon can open the door remotely.



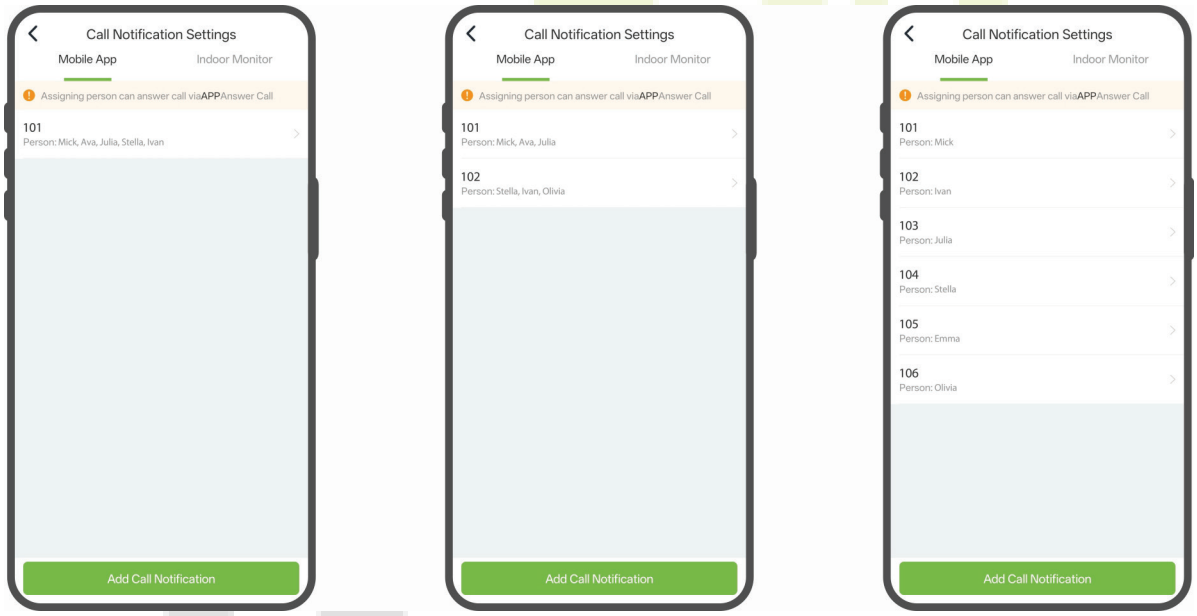
Device Call the Phone (ZKBio Zlink App)

1. Click icon > **[Add Call Notification]** to assign person that can answer call via App.
   - **Room Number:** Customize the room number.
   - **Person:** Select the personnel in the room. Up to 5 notified persons can be selected. If you select multiple people from the same room, calling the room number will notify all selected individuals in that room. If the selected people are in different rooms, only the first five people on the contact list will receive the call.



For example:

1) Suppose there are six people. We have configured the following three scenarios.



- **Scenario 1:** One room number assigned to five people. You can select up to five people.
- **Scenario 2:** Two room numbers, each with three people assigned.
- **Scenario 3:** Six room numbers, each assigned to one person.

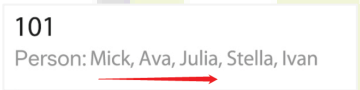
2) Enter **Intercom > SIP Settings > Calling Shortcut Settings > Call Mode** and set the call mode to **Standard Mode** or **Direct Calling Mode**, the person who receives the call will vary depending on the selected call mode and the setup in each of the above scenarios.

➢ **Standard Mode:**

- **Scenario 1:** When you call the room number, all five people in the room will be called simultaneously. Once one person answers, the calls to the others will be automatically disconnected.
- **Scenario 2:** When you call room 101, all three people in that room will be called at the same time. Once one person answers, the calls to the others will be automatically disconnected. You must hang up before calling the three people in room 102.
- **Scenario 3:** When you call a room number, only the person in that room will be called. You must hang up before dialing another room number.

➢ **Direct Calling Mode:**

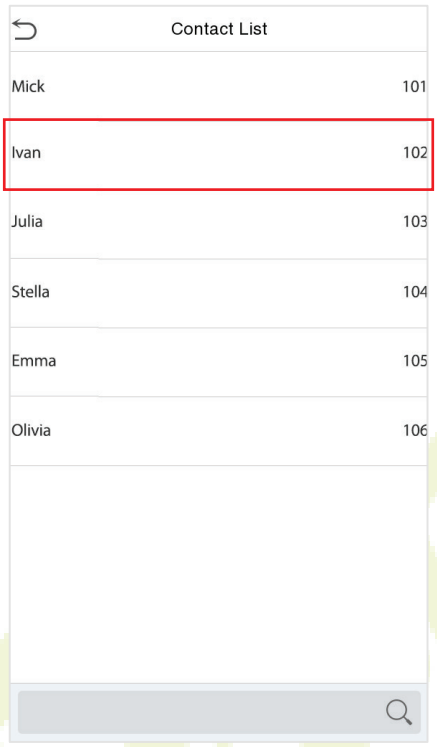
- **Scenario 1:** When you press the key, all five people in the room will be called simultaneously. Once one person answers, the calls to the others will be automatically disconnected.
- **Scenario 2:** When you press the key, you can only call the first five people listed in the app. These first five people appear on the app interface, with each room sorted from left to right, totaling five people. E.g.

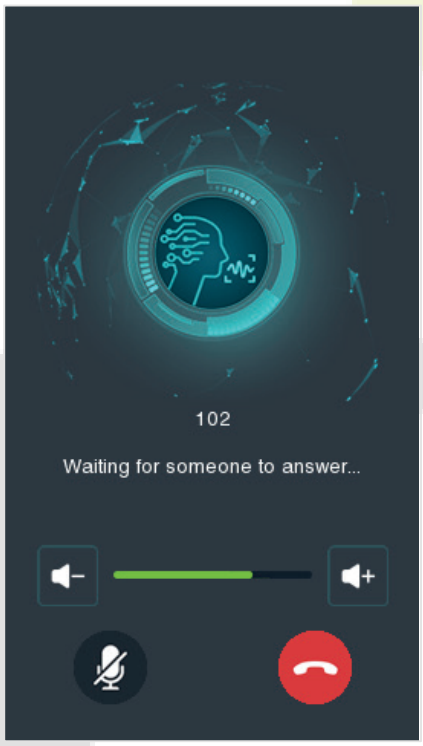


- **Scenario 3:** When you press the key, you can only call the first five people listed in the app. These first five people appear on the app interface, with each room sorted from left to right, totaling five people.

2. After the setting is successful, you can click the icon on the device and enter the Room Number in the pop-up interface of the device. Or click the icon on the call page to open the contact list and search for the person to call him/her.

or





18 Connecting to ZKBio Zlink Web Portal

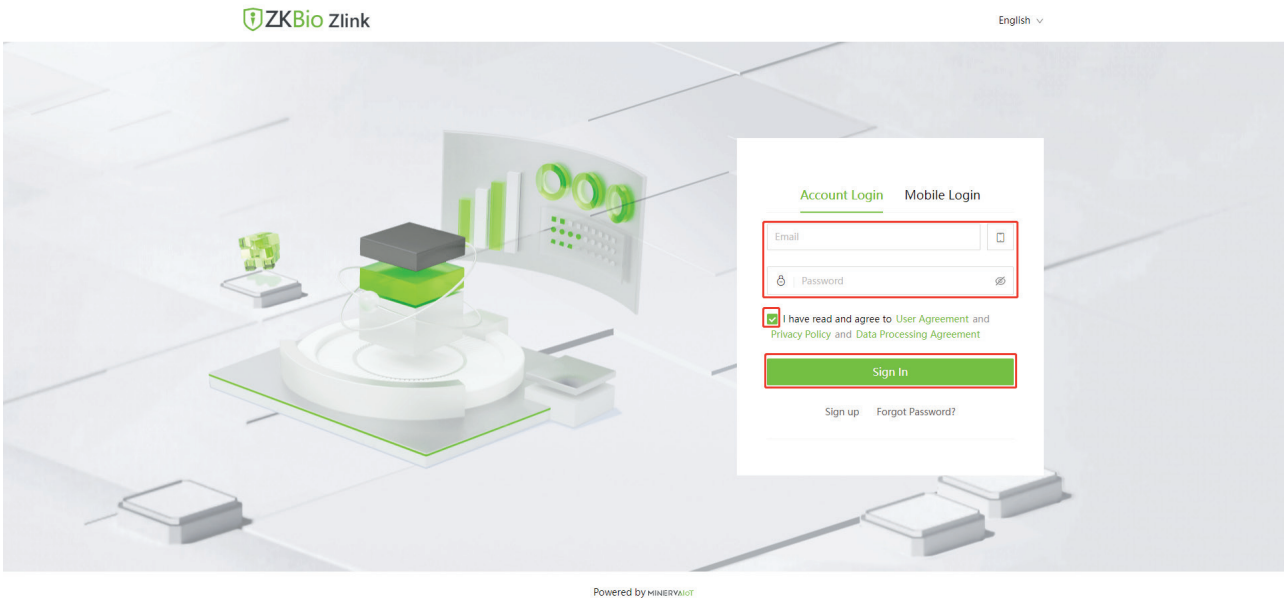
The Web Portal pages may vary depending on the version, and the document is for reference only.

Change the device communication protocol to BEST protocol, then the device can be managed by ZKBio Zlink, please refer to 6.7 Device Type Setting.

Users can use the created account to access ZKBio Zlink Web Portal to connect devices, add new personnel, register the verification method of registered personnel, synchronize personnel to devices and query records.

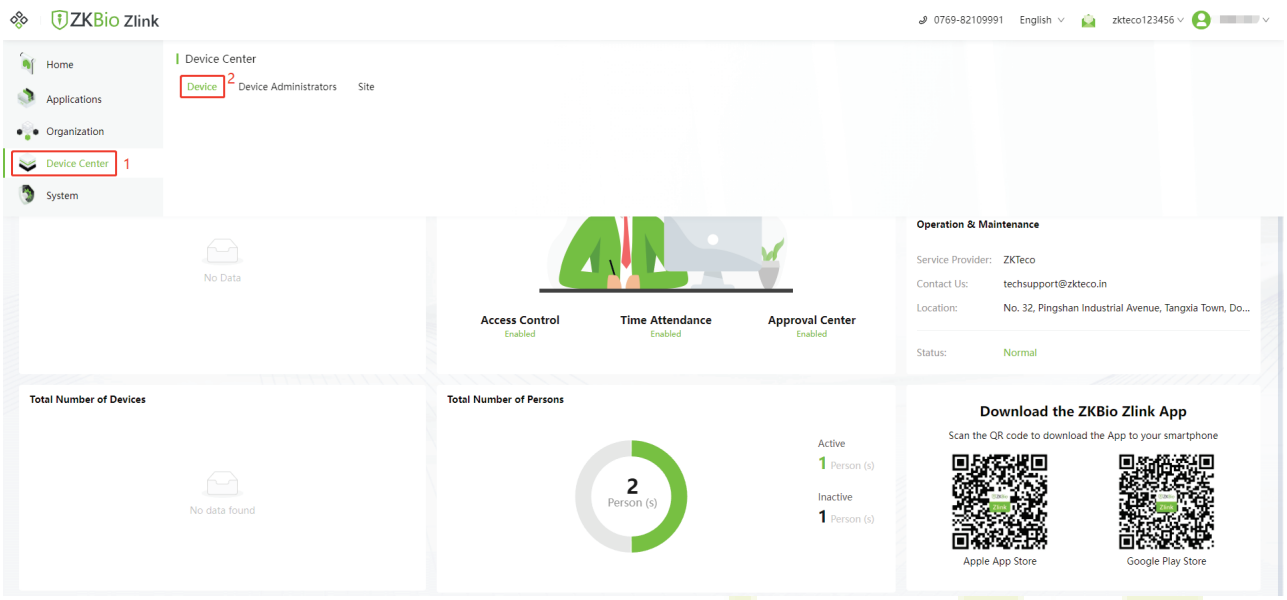
18.1 Login to the Web Portal

1. Please open the recommended browser and enter the IP address to access the ZKBio Zlink Web Portal: http://zlink.minervaiot.com.
2. Enter your registered account on the login screen, check "I have read and agree to User Agreement and Privacy Policy and Data Processing Agreement" and click [**Sign In**] to login.

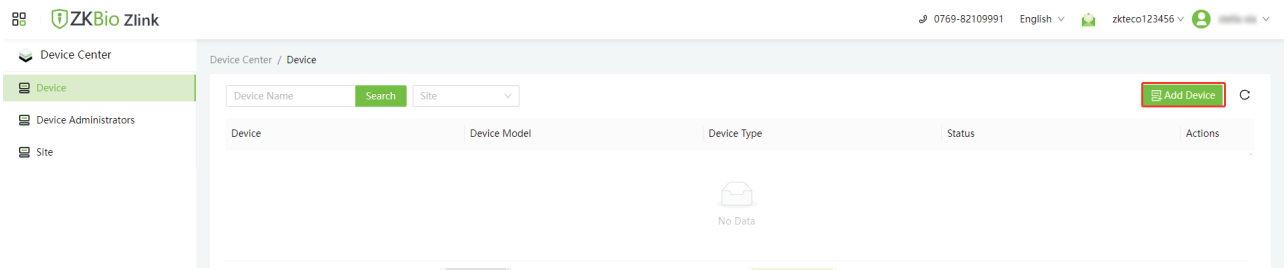


18.2 Add Device on the Web Portal

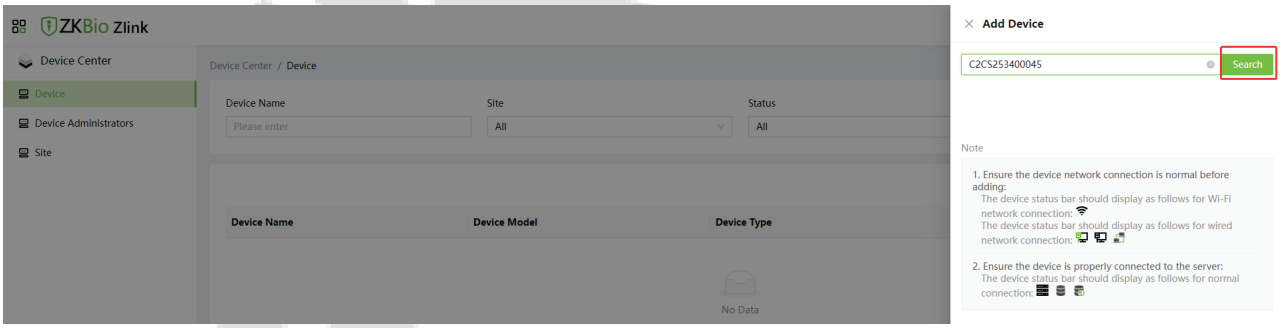
1. Click the icon on the top left corner, and click [**Device Center**] > [**Device**] to enter the device setting interface.



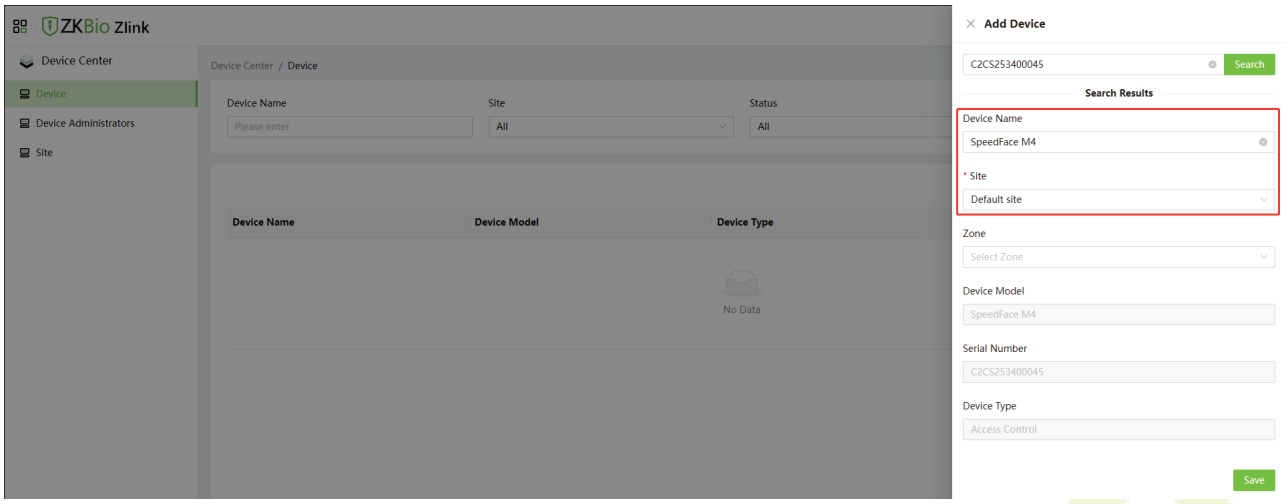
2. Then click [**Add Device**] to enter the Add Device interface.



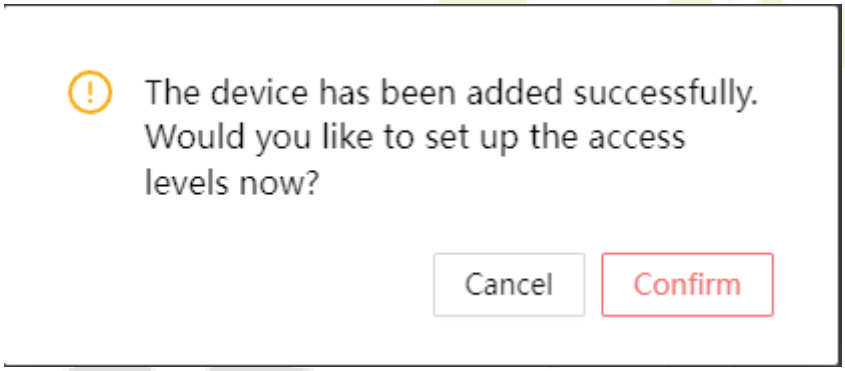
3. Enter the Serial Number and click [**Search**].

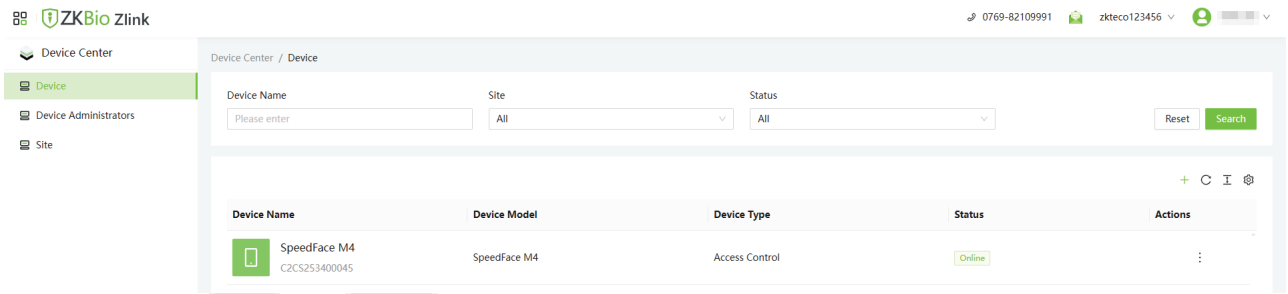


4. Then enter the device name and specify the device to a site. Select Site from the drop- down menu. Click [**Save**] to complete the addition.



5. After the device is added, it will pop up the following prompt. Click **Confirm**, it will directly enter the access level setting interface. Click **Cancel**, the device will be displayed in the device list. Then you can set the access levels as needed.





Note: *Wait a moment for the device status to change from "**Offline**" to "**Online**".*

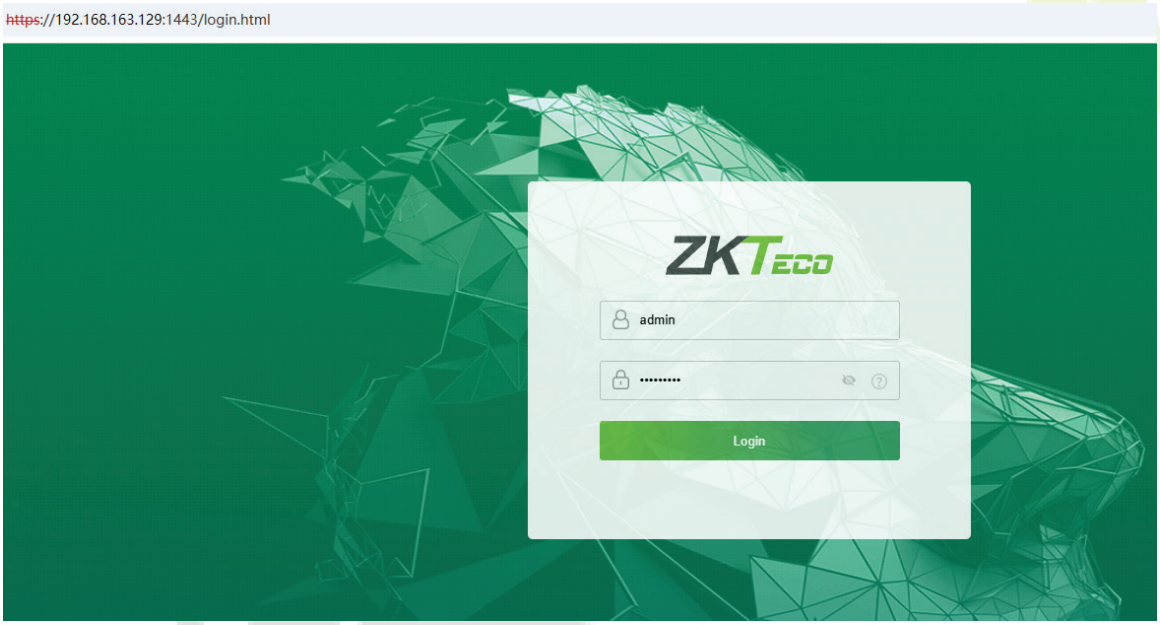
For more information, please refer to the relevant User Manual.

19 Connect to Webserver★

19.1 Login Webserver

1. Open a browser to enter the address to log in to the WebServer, the address is **https:// Serial IP Address:1443**. For example: **https://192.168.163.129:1443**.

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



Note:

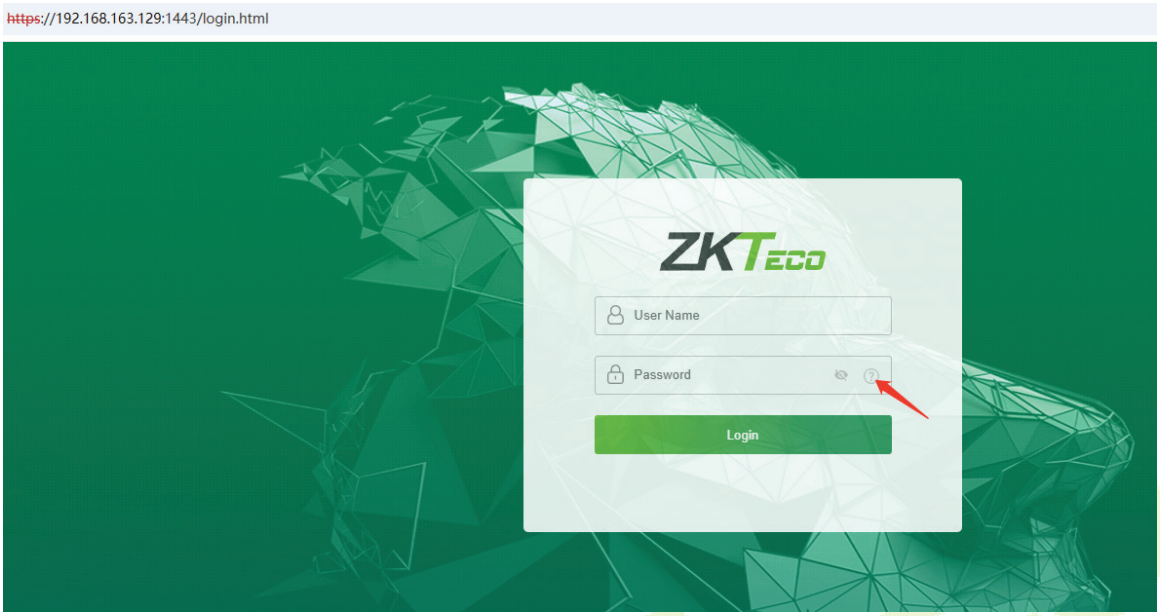
1. After logging in for the first time, it is required that the users change their original password.
2. In order to retrieve the password easily, please register a super admin first, please refer to 3.1 Add Users.

19.2 Forgot Password

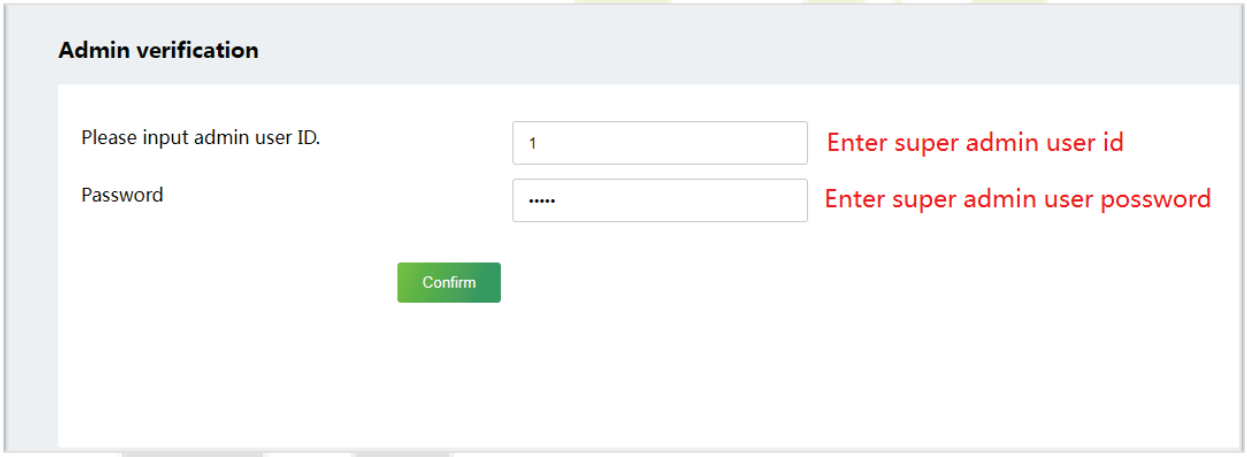
➢ **Method 1 (When there is a super admin):**

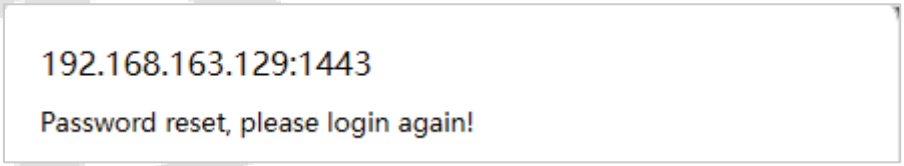
If you forgot the password of WebServer, you could reset it by the registered super admin. The detailed steps are as follows:

1. Click the icon on the login interface.

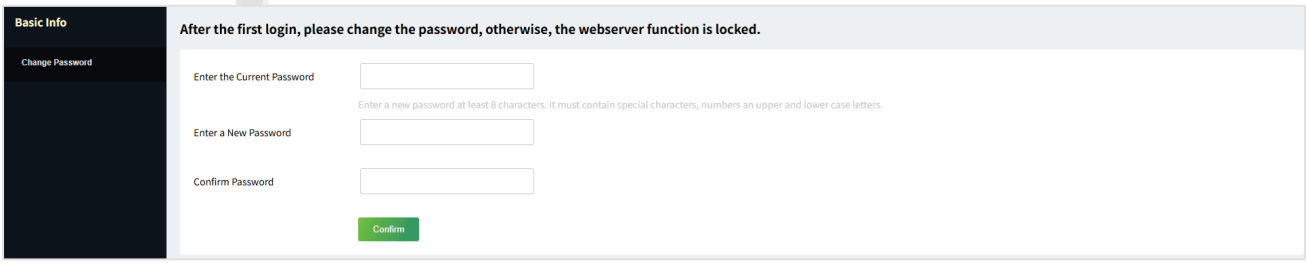


2. On the pop-up page, enter the relevant information of the super admin user as prompted.





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, it is required to change your password after successfully logging in.

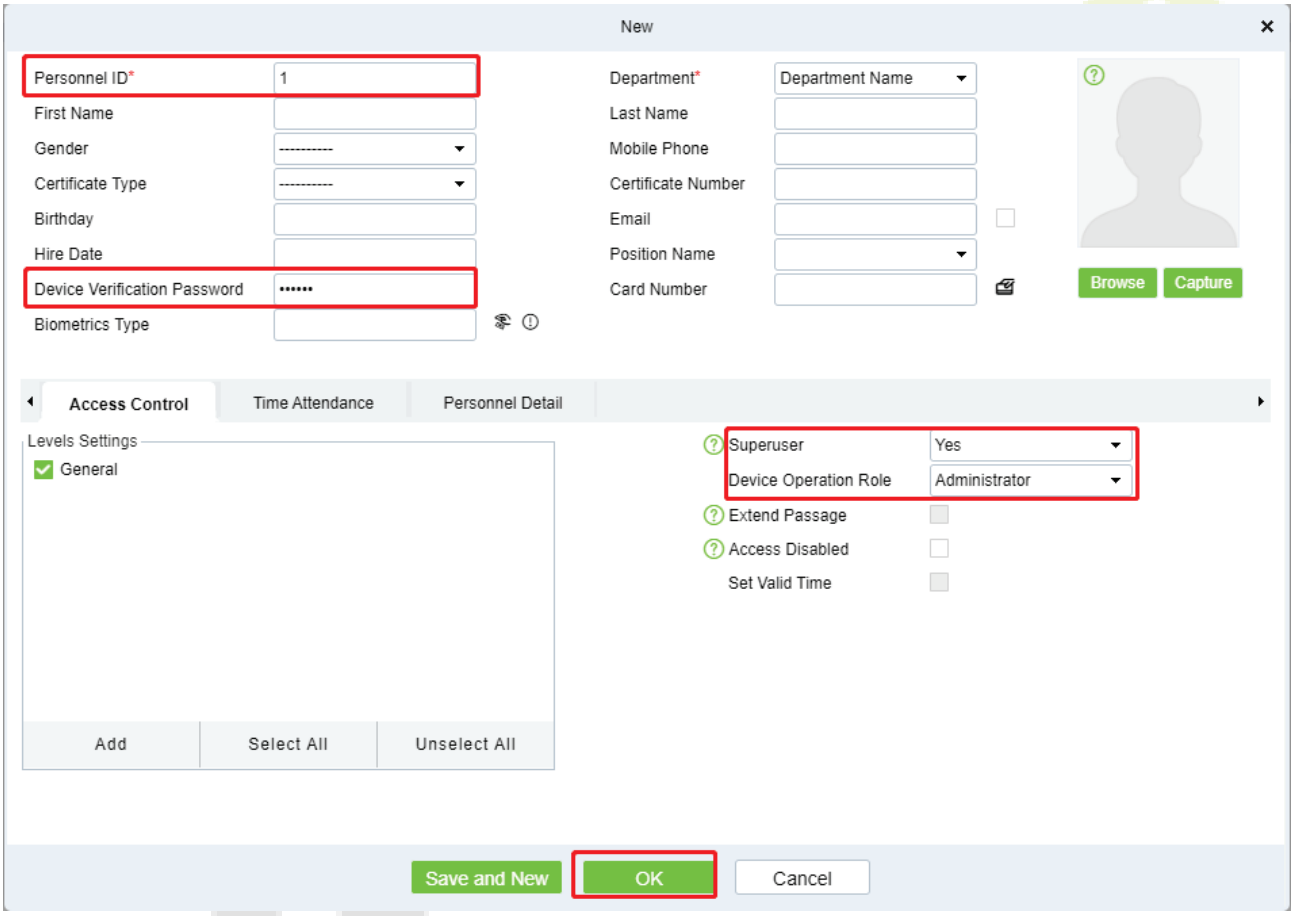


Note: The super admin must exist.

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

If the network of the device is normal and ZKBio CVAccess / ZKBio Zlink 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 CVAccess / ZKBio Zlink Cloud Server; register the super admin information and set the super admin role on the new interface as required. (Here take ZKBio CVAccess interface as an example)



2. After registering the information of the super admin, click **OK**.
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 *the relevant software 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:**

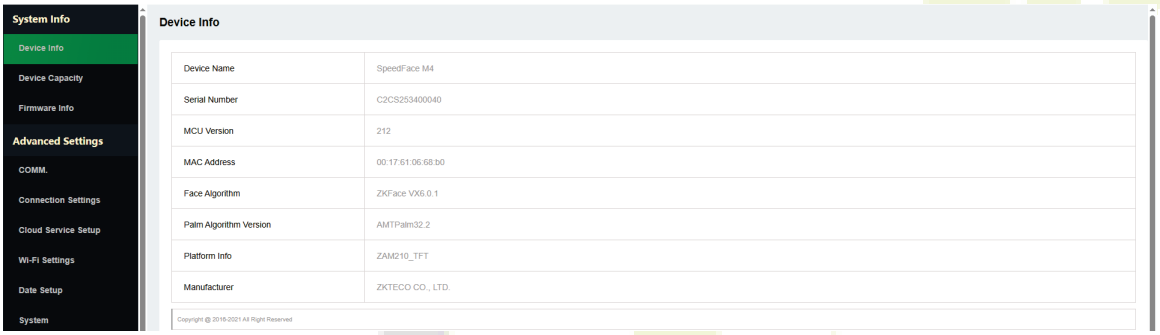
If the device has not registered a super admin and cannot connect to the server, please contact our after-sales technicians to help retrieve the password.

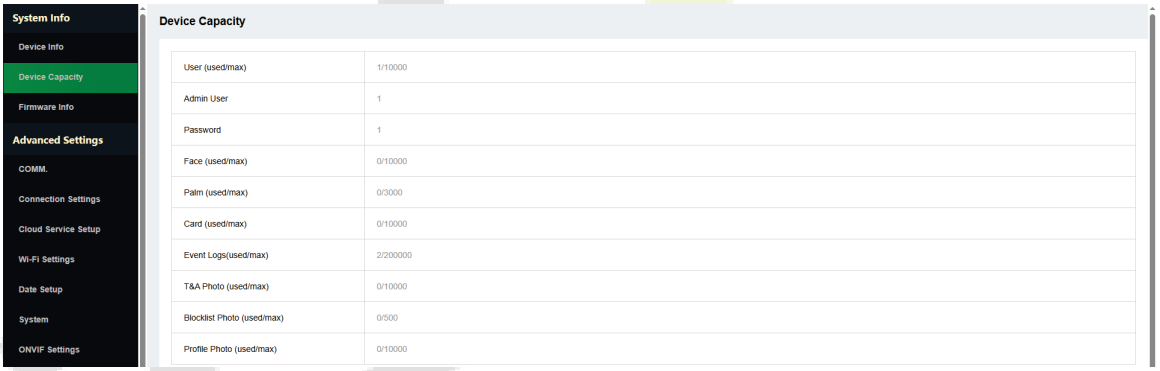
19.3 System Information

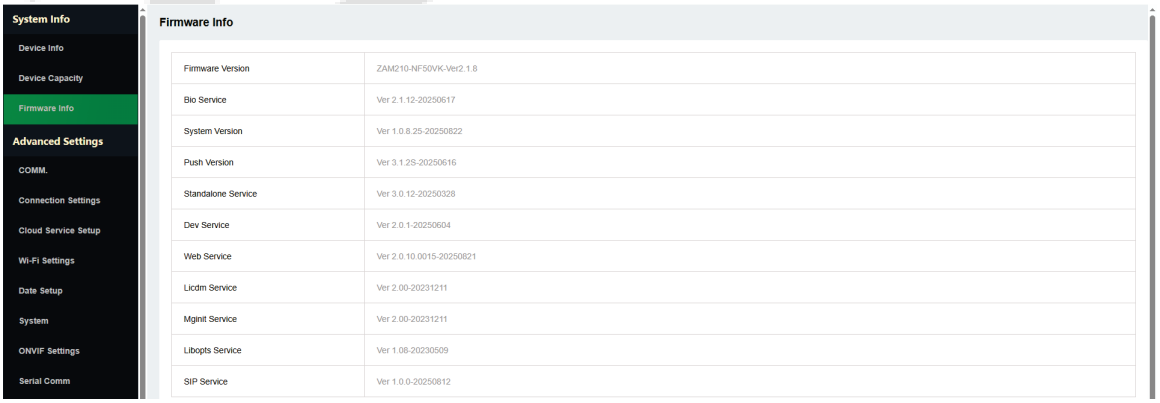
Note: The Webserver interface display may vary depending on the device type (A&C PUSH/T&A PUSH/BEST Protocol). The following text takes A&C PUSH as an example to illustrate.

Click **Device Info/Device Capacity/Firmware Info** on the WebServer.

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







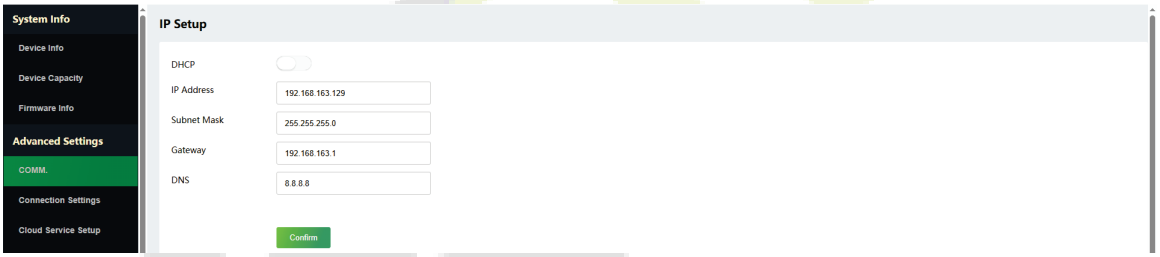
Function Name	Description
Device Info	Displays the device's name, serial number, MCU version, MAC address, face&palm★ algorithm version information, platform and manufacturer information.
Device Capacity	Displays the current device's user storage, password, face, palm★, card storage, administrators, event logs, T&A photo, blocklist photo and profile photo.
Firmware Information	Displays the firmware version and other version information of the device.

19.4 Advanced Settings

19.4.1 COMM.

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.

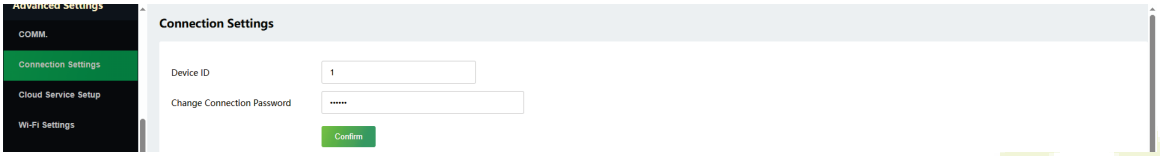


Function Name	Description
DHCP	Select whether to obtain the IP Address by automatically.
IP Address	The default IP address is 192.168.1.201. It can be modified according to network availability.
Subnet Mask	The default Subnet Mask is 255.255.255.0. It can be modified according to network availability.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

19.4.2 Connection Settings

Click **Connection Settings** on the WebServer.

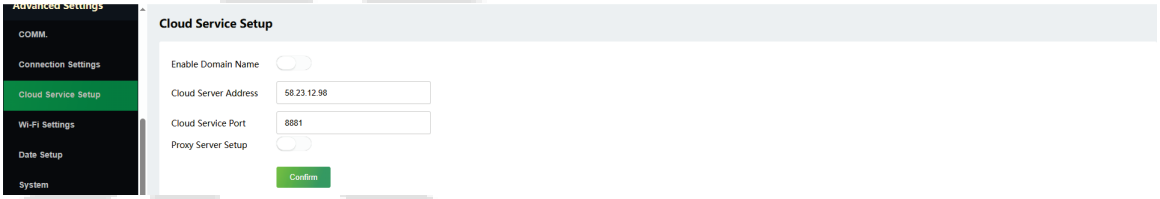


Function Name	Description
Device ID	It is the identification number of the device, which ranges between 0 and 255.
Change Connection Password	To improve the security of data, the connection password needs to be entered before the device can be connected to the C/S software. It can be changed as needed.

19.4.3 Cloud Service Setup

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

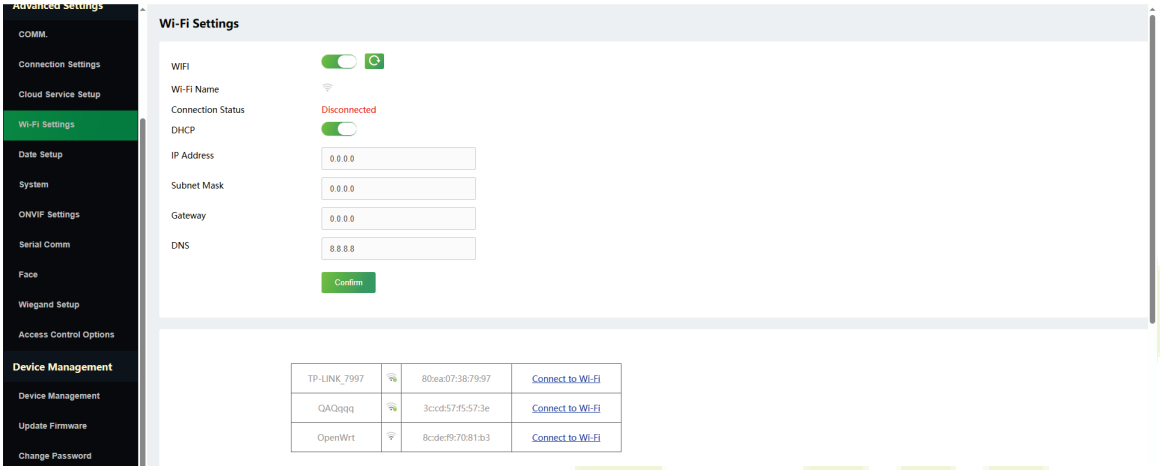
Cloud Server Setup was used to connect to the ZKBio CVAccess software, please refer to chapter 15.



Function Name		Description
Enable Domain Name	**Cloud 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	**Cloud Server Address**	IP address of the ADMS server.
	Cloud Service Port	Port used by the ADMS server.
Proxy Server Setup		When you choose to enable the proxy, you need to set the IP address and port number of the proxy server.

19.4.4 Wi-Fi Settings★

The device supports the Wi-Fi module, which is built-in within the hardware, to enable data transmission via Wi-Fi and establish a wireless network environment.

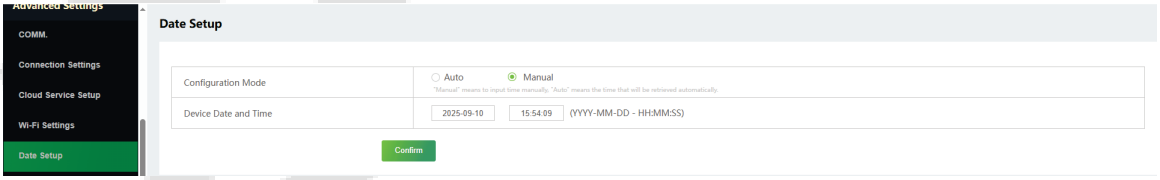


- When Wi-Fi is enabled, the device will search for the available Wi-Fi within the network range.
- Click **Connect to Wi-Fi** after the required Wi-Fi name from the available list and input the correct password, and then click [**Confirm**].
- After successful verification, the connection status will display "**Connected**".

19.4.5 Date Setup

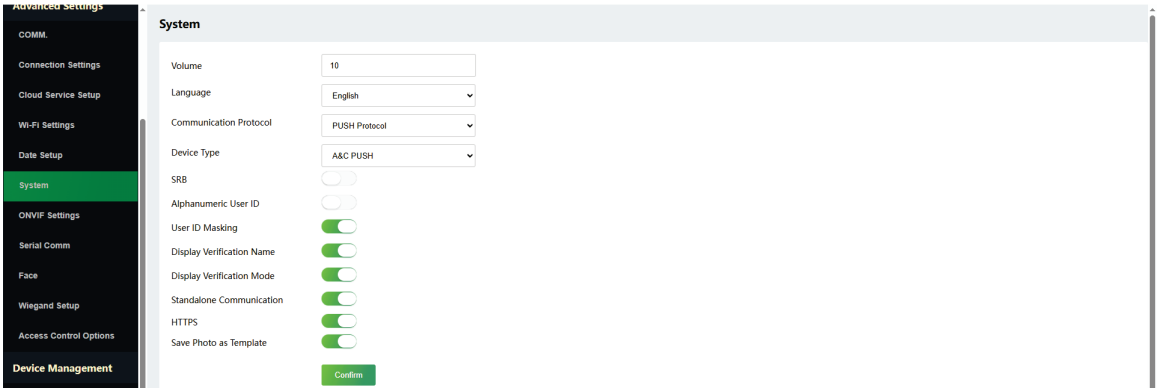
Click **Date Setup** on the WebServer.

Click **Manual** to manually set the date and time and click **Confirm** to save.



19.4.6 System

Click **System** on the WebServer.



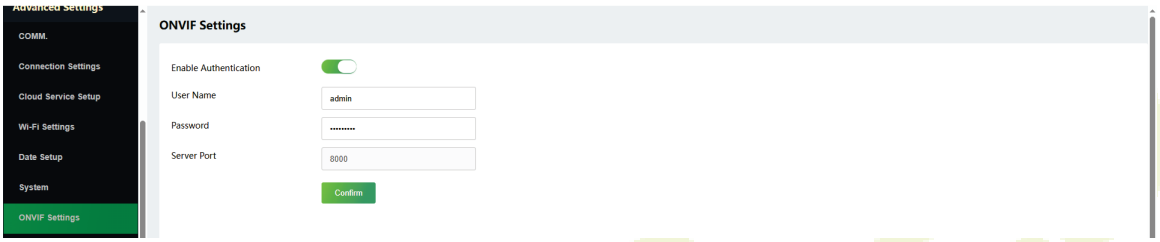
Function Name	Description
Volume	Adjust the volume of the device which can be set between 0 and 100.
Language	Select the language of the WebServer and device.
Communication Protocol	Set the communication protocol of the device.
Device Type	Set the device as an access control terminal or attendance terminal. ***Note:*** After changing the device type, the device will delete all the data and restart, and some functions will be adjusted accordingly.
SRB★	When SRB is enabled, the lock is controlled by the SRB to prevent the lock from being opened due to device removal.
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.
Standalone Communication	To avoid being unable to use when the device is offline, you can download the C/S software (such as ZKAccess 3.5) on your computer in advance for offline use.
HTTPS	Based on HTTP, transmission encryption and identity authentication ensure the security of the transmission process.

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

19.4.7 ONVIF Settings★

Note: This function needs to be used with the network video recorder (NVR).

Click **ONVIF Settings** on the WebServer.

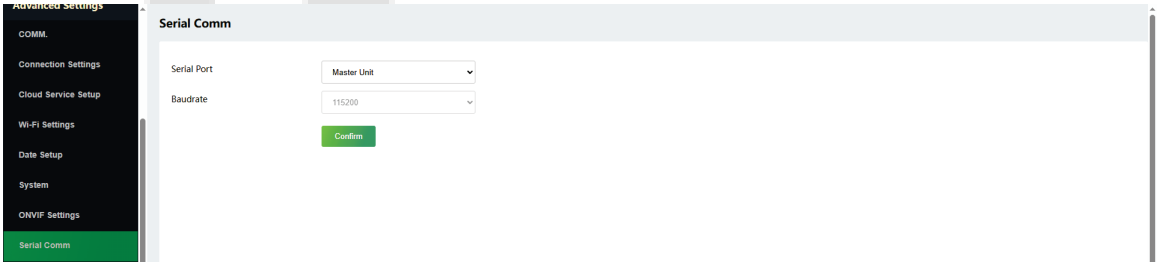


Function Name	Description
Enable Authentication	Enable/Disable the Authentication Function. When it is disabled, there is no need to input the User Name and Password when adding the device to the NVR.
User Name	Set the User Name. The default is admin.
Password	Set the password.
Server Port	The default is 8000, and cannot be modified.

For more details, please refer to 9.3 ONVIF Settings.

19.4.8 Serial Comm

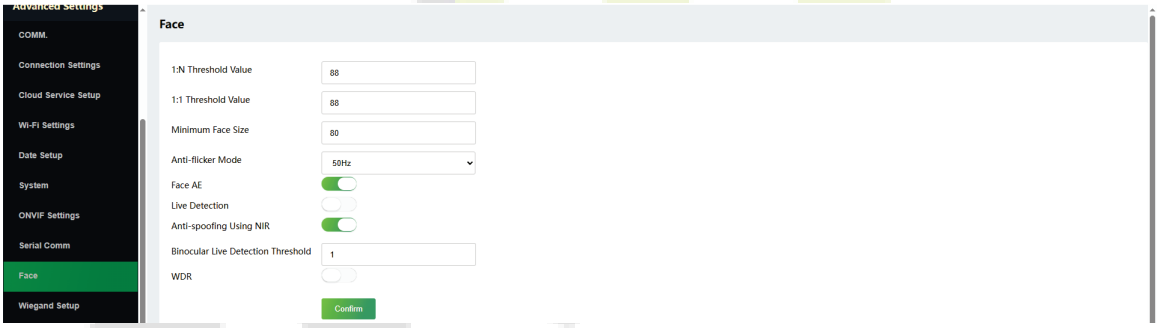
Click **Serial Comm** on the WebServer.



Function Name	Description
Serial Port	**No Using:** Do not communicate with the device through the serial port. **RS485(PC):** Communicates with the PC through RS485 serial port. **Master Unit:** When RS485 is used as the function of "**Master Unit**", the device will act as a master unit, and it can be connected to RS485 reader.
Baudrate	When the serial port is set as **Master Unit**, the baudrate is 115200 by default and cannot be modified. When the serial port is set as **RS485(PC)**, there are 4 baudrate options. They are: 115200 (default), 57600, 38400 and 19200. The higher is the baud rate, the faster is the communication speed, but also the less reliable. Hence, a higher baud rate can be used when the communication distance is short; when the communication distance is long, choosing a lower baud rate would be more reliable.

19.4.9 Face

Click **Face** on the WebServer.



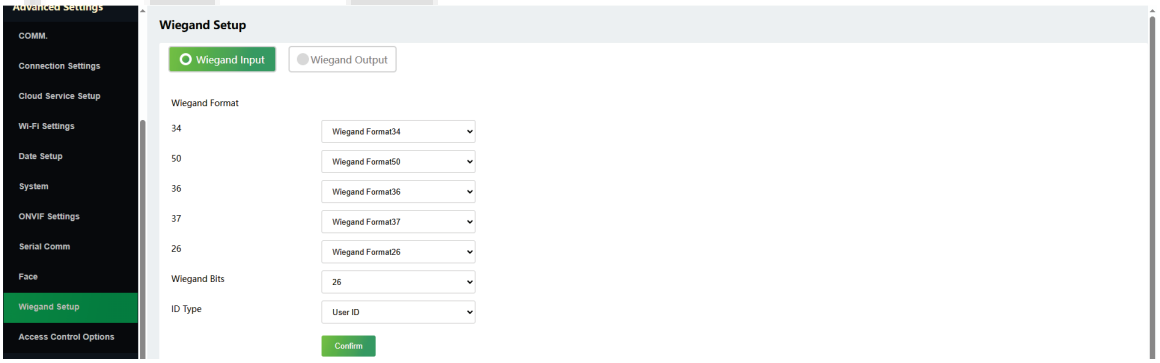
Function Name	Description
1:N Threshold	The verification will be successful only if the similarity between the acquired facial image and all registered facial templates is greater than the set value in the 1: N verification mode. The valid value ranges from 0 to 100. The higher the thresholds, the lower the misjudgement rate and higher is the rejection rate, and vice versa. It is recommended to set the default value of 88.
1:1 Threshold	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 misjudgement rate and the higher is the rejection rate, and vice versa. It is recommended to set the default value of 88.

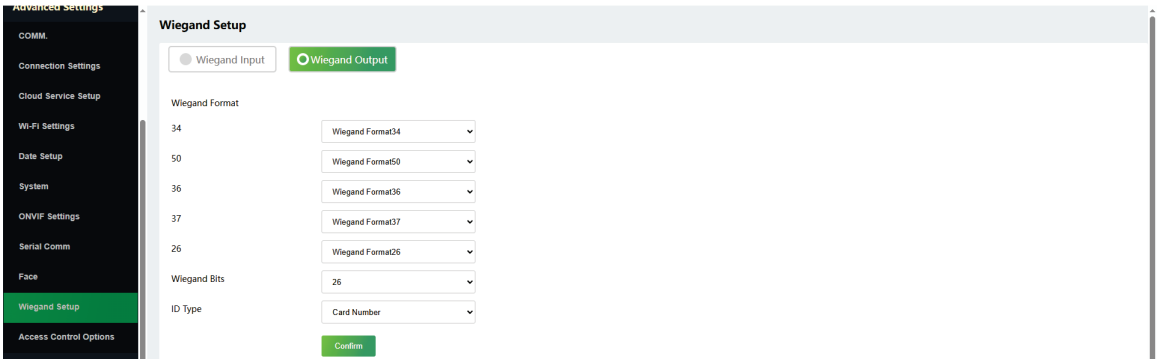
Minimum Face Size	It sets the minimum face size required for facial registration and comparison. If the minimum size of the captured image is smaller than the set value, then it will be filtered off and not recognized as a face. This value can also be interpreted as the face comparison distance. The farther the individual is, the smaller the face, and the smaller number of pixels of the face obtained by the algorithm. Therefore, adjusting this parameter can adjust the farthest comparison of distance of faces. When the value is 0, the face comparison distance is not limited.
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.
Face AE	When the face is in front of the camera in Face AE mode, the brightness of the face area increases, while other areas become darker.
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 false representation.
Anti-spoofing Using NIR	Using near-infrared spectra imaging to identify and prevent fake photos and videos attack.
Binocular Live Detection Threshold	It is convenient to judge whether the near-infrared spectral imaging is fake photo and video. The larger the value, the better the anti-spoofing performance of near-infrared spectral imaging.
WDR	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.

19.4.10 Wiegand Setup

Click **Wiegand Setup** on the WebServer.

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



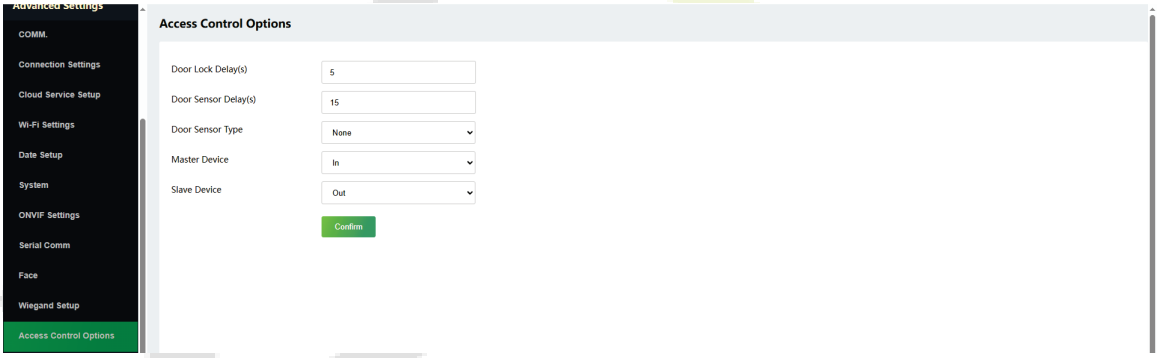


Function Name	Description
Wiegand Format	Its value can be 26 bits, 34 bits, 36 bits, 37 bits, 50 bits and 64 bits.
Wiegand Bits	The number of bits of the Wiegand data.
ID Type	Select between the User ID and card number.

19.4.11 Access Control Options

Click **Access Control Options** on the WebServer.

On the Access Control interface to set the parameters of the control lock of the terminal and related equipment.



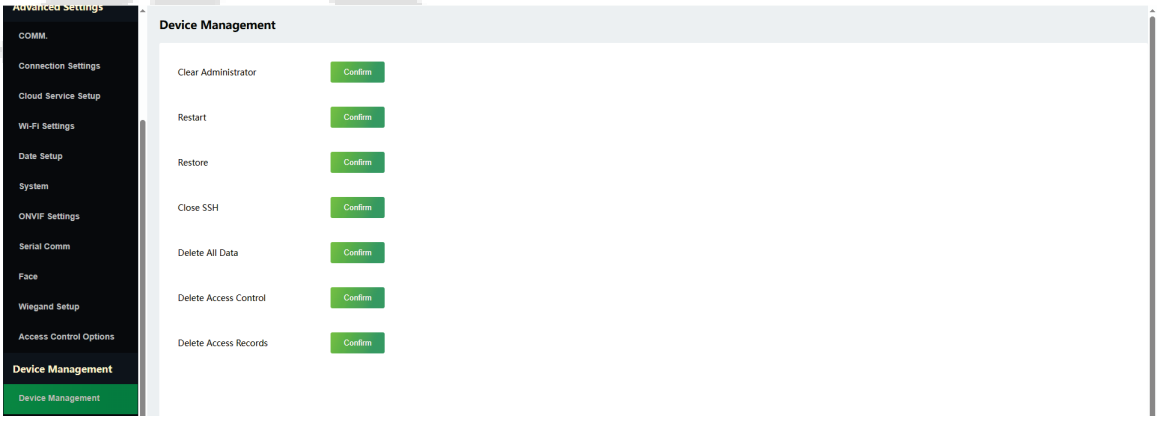
Function Name	Description
Door Lock Delay (s)	The length of time that the device controls the electric lock to be in unlock state. Valid value: 1~99 seconds.
Door Sensor Delay (s)	If the door is not locked and is left open for a certain duration (Door Sensor Delay), an alarm will be triggered. The valid value of Door Sensor Delay ranges from 1 to 255 seconds.

Door Sensor Type	There are three Sensor types: **None**, **Normal Open**, and **Normal Close**. **None:** It means the door sensor is not in use. **Normal Open:** It means the door is always left open when electric power is on. **Normal Close:** It means the door is always left closed when electric power is on.
Master Device	While configuring the master and slave devices, you may set the state of the master as **Out** or **In**. **Out:** A record of verification on the master device is a check-out record. **In:** A record of verification on the master device is a check-in record.
Slave Device	While configuring the master and slave devices, you may set the state of the slave as **Out** or **In**. **Out:** A record of verification on the slave device is a check-out record. **In:** A record of verification on the slave device is a check-in record.

19.5 Device Management

19.5.1 Device Management

Click **Device Management** on the WebServer.



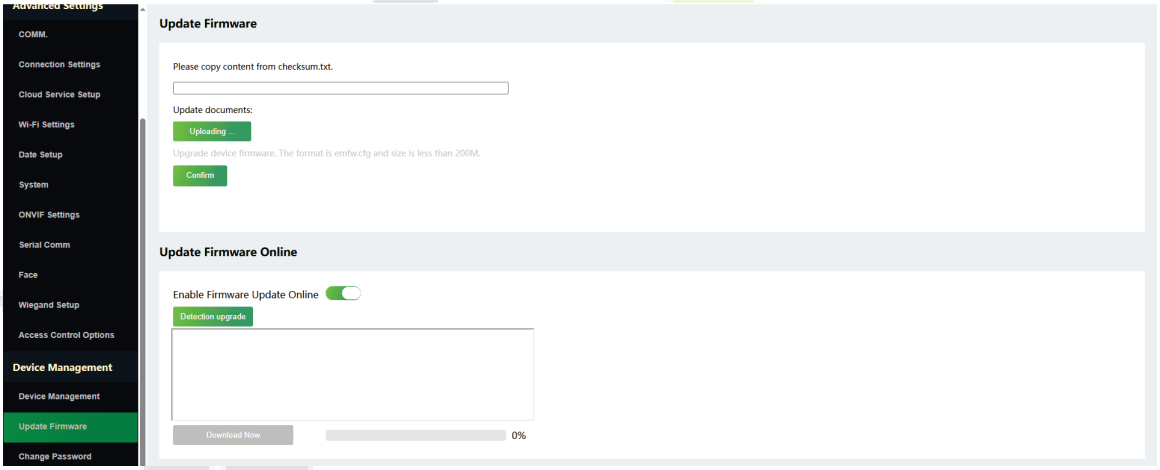
Function Name	Description
Clear Administrator	Choose whether to change the super administrator into a normal user.

Restart	Choose whether to restart the device.
Restore	The Restore 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 restore, the IP of the device is restored to the original 192.168.1.201, please refer to 19.4.1 COMM. to modify the IP.
Close SSH	SSH is used to enter the background of the device for maintenance, choose whether to close the SSH.
Delete All Data	To delete the information and attendance logs/access records of all registered users.
Delete Access Control	To delete all the access data.
Delete Access Records	To delete all the access records.

19.5.2 Update Firmware

Click **Update 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.

You can also choose to update firmware online. Click **Detection upgrade** it may have the following 3 scenarios:

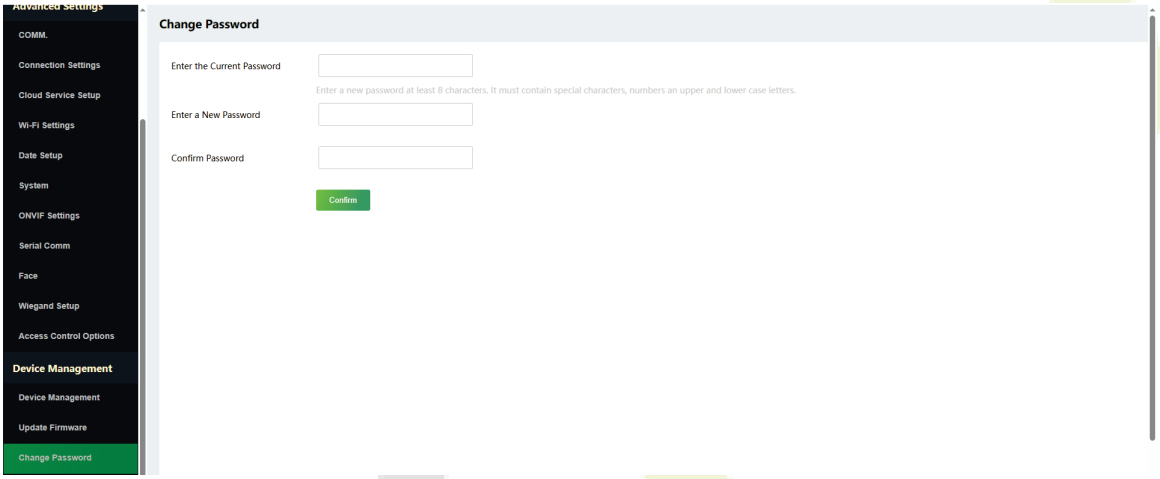
- If the query fails, the interface will prompt "Query Failed".

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

19.5.3 Change Password

Click **Change Password** on the WebServer.

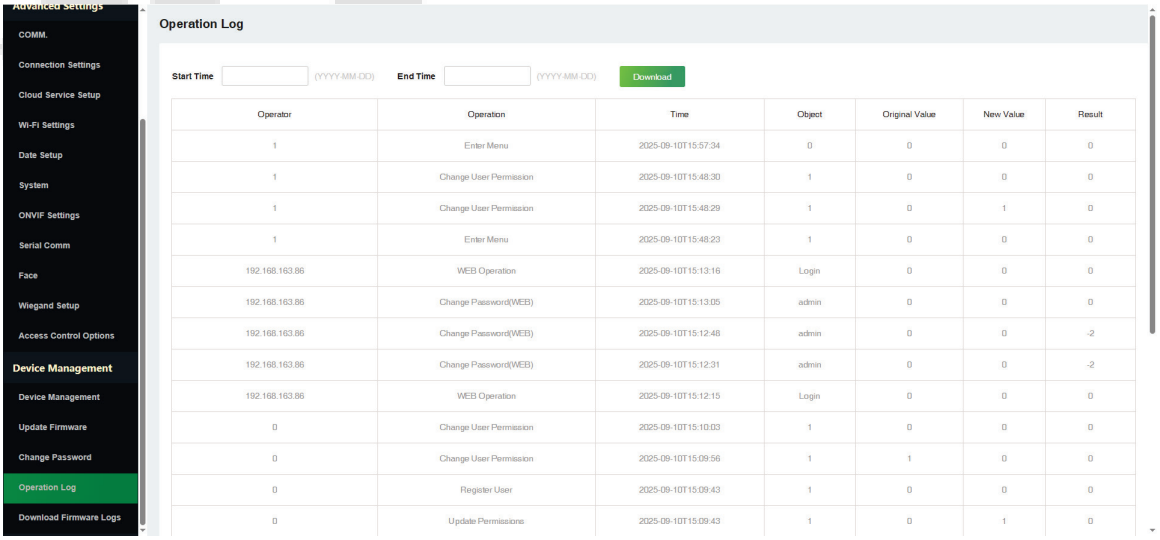
In this interface, you can change the password of WebServer.



19.5.4 Operation Log

Click **Operation Log** on the WebServer.

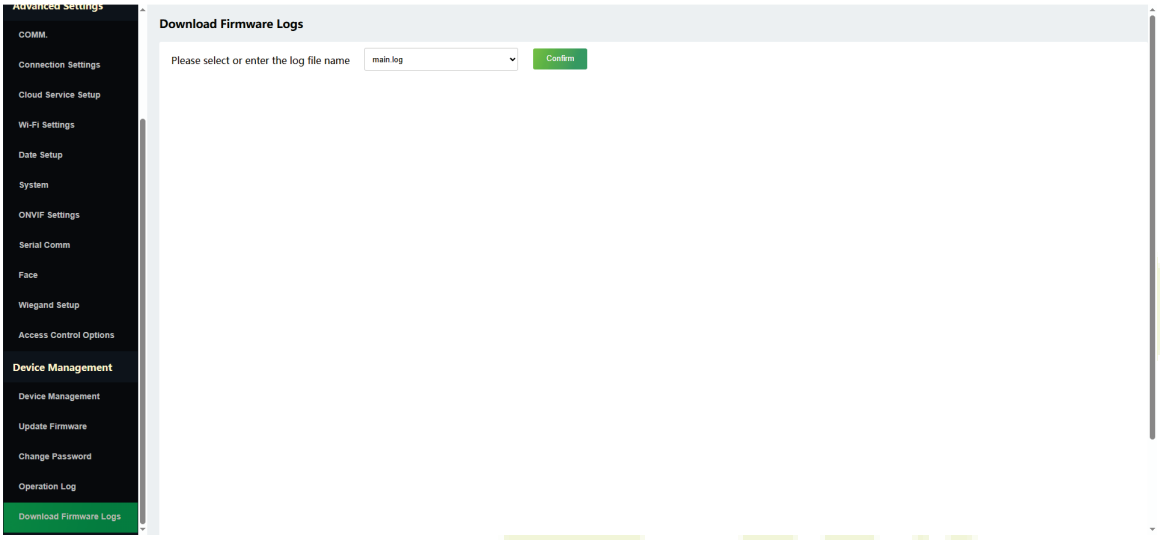
All the user's operation records on the device or WebServer are saved. Users can search and download these logs by time.



19.5.5 Download Firmware Logs

Click **Download Firmware Logs** on the WebServer.

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



Appendix 1

Requirements for Live Collection and Registration of Visible Light Face Templates

1) It is recommended to perform registration in an indoor environment with an appropriate light source without underexposure or overexposure.
2) Do not point 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) It is recommended to show a plain facial expression. Smile is acceptable, but do not close your eyes, or incline your head to any orientation. Two images are required for persons with eyeglasses, one image with eyeglasses and one other without eyeglasses.
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 to 80cm is recommended as a capturing distance, adjustable subject to body height.

Image1 Face Capture Area

Requirements for Visible Light Digital Face Template Data

The digital photo should be straight-edged, colored, half-portrayed with only one person, and the person should be uncharted and not in uniform. Persons who wear eyeglasses should remain to put on eyeglasses for photo capturing.

Eye Distance

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

Facial Expression

A plain face or smile with eyes naturally open is recommended.

Gesture and Angle

The horizontal rotating angle should not exceed ±10°, elevation should not exceed ±10°, and the depression angle should not exceed ±10°.

Accessories

Masks and colored eyeglasses are not allowed. The frame of the eyeglasses should not shield the 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 eyeglasses.

Face

The image must have 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) 24-bit true-color mode.
3) JPG format compressed image with not more than 20 KB size.
4) Definition rate between 358 x 441 to 1080 x 1920.
5) The vertical scale of the head and body should be 2:1.
6) The photo should include the captured person's shoulders at the same horizontal level.
7) The captured person should have eyes-open and with clearly seen iris.
8) A plain face or smile is preferred, showing teeth is not preferred.
9) The captured person should be clearly seen, natural in color, and without image obvious twist, no shadow, light spot or reflection in face or background, and appropriate contrast and lightness level.

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. How we handle personal information of minors

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

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

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

IV. Others

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

Eco-friendly Operation

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

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

Hazardous or Toxic substances and their quantities

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

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

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

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

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

ZKTeco Industrial Park, No. 32, Industrial Road,

Tangxia Town, Dongguan, China.

Phone : +86 769 - 82109991

Fax : +86 755 - 89602394

www.zkteco.com