User Manual

5-inch VLFR Terminals (ZAM230)

Date: July 2025

Doc Version: 1.0

English

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

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

Copyright © 2025 ZKTECO CO., LTD. All rights reserved.

Without the prior written consent of ZKTeco, no portion of this manual can be copied or forwarded in any way or form. All parts of this manual belong to ZKTeco and its subsidiaries (hereinafter the "Company" or "ZKTeco").

Trademark

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

Disclaimer

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

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

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

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

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

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

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

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

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

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

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

ZKTeco Headquarters

Address	ZKTeco Industrial Park, No. 32, Industrial Road, Tangxia Town, Dongguan, China.
Phone	+86 769 - 82109991
Fax	+86 755 - 89602394

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

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

About the Company

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

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

About the Manual

This manual introduces the operations of **5-inch VLFR Terminals (ZAM230)**.

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 Overview

The SpeedFace-V5L Series employs intelligent engineering facial authentication algorithms and cutting-edge computer vision technology. It supports different versions of SpeedFace-V5L with large capacity and speedy authentication to satisfy your needs. SpeedFace-V5L[QR] comes with a QR code module to support Dynamic QR code via ZKBio CVAccess Mobile APP, while the SpeedFace-V5L-RFID standard ID card verification function.

SpeedFace-V5L Series uses touchless authentication technology and can identify individuals even when wearing masks, making it a hygienic option. Additionally, it has an advanced anti-spoofing algorithm that can detect fake photos and videos.

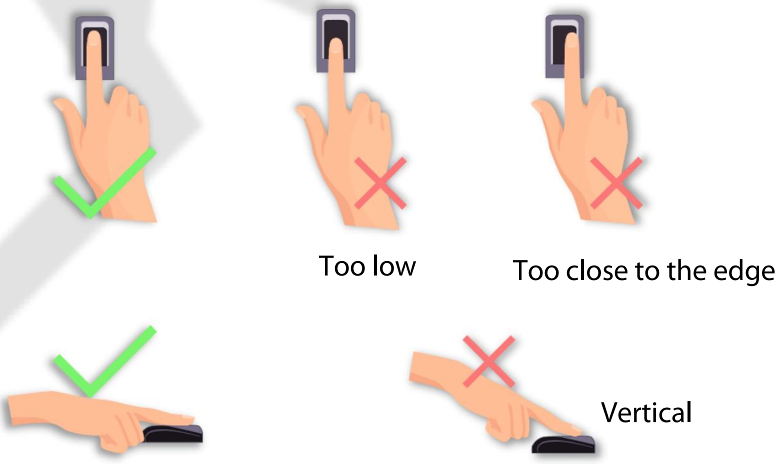
SpeedFace-V5L Series features a video intercom function with SIP protocol (Version 2.0) for compatible with video intercom indoor unit and supports ONVIF protocol to connect to ONVIF NVR for Video surveillance and recording. Moreover, it is compatible with ZKBio Zlink Mobile APP & ZKBio Zlink-Web when switching to BEST protocol.

2 Instruction for Use

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

2.1 Finger Positioning

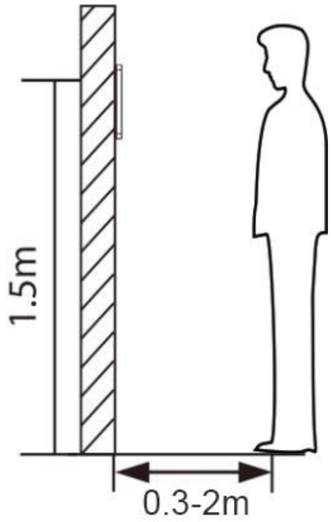
Recommended fingers: Index, middle, or ring fingers; avoid using the thumb or pinky, as they are difficult to accurately press onto the fingerprint reader.



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

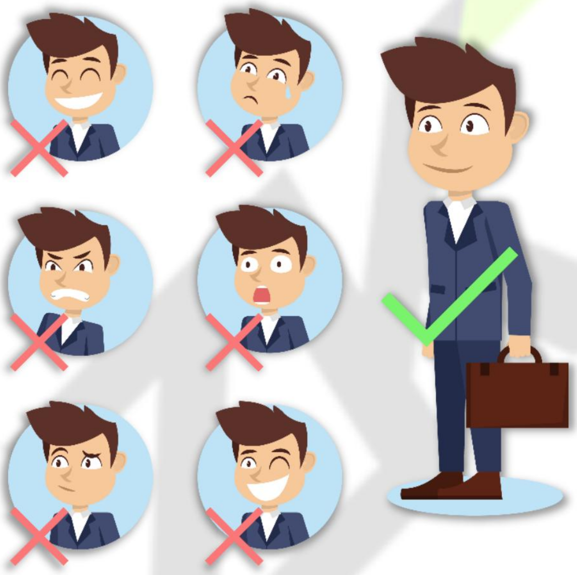
2.2 Standing Position, Facial Expression and Standing Posture

- **The Recommended Distance**

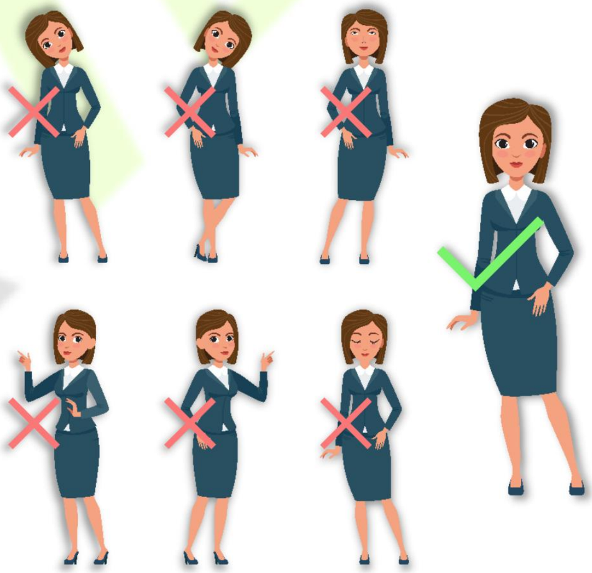


The distance between the device and a user whose height is in a range of 1.55m to 1.85m is recommended to be 0.3 to 2.5m. Users may slightly move forward or backward to improve the character of facial images captured.

- **Recommended Standing Posture and Facial Expression**



Facial Expression

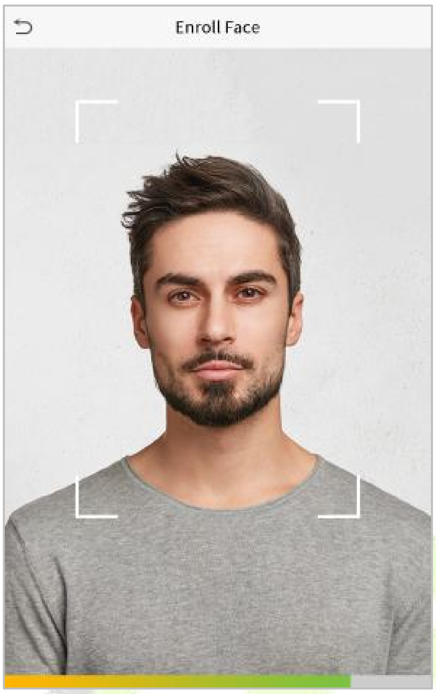


Standing Posture

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

2.3 Face Registration

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



- **Correct Face Registration and Authentication Method**

Recommendation for Registering a Face

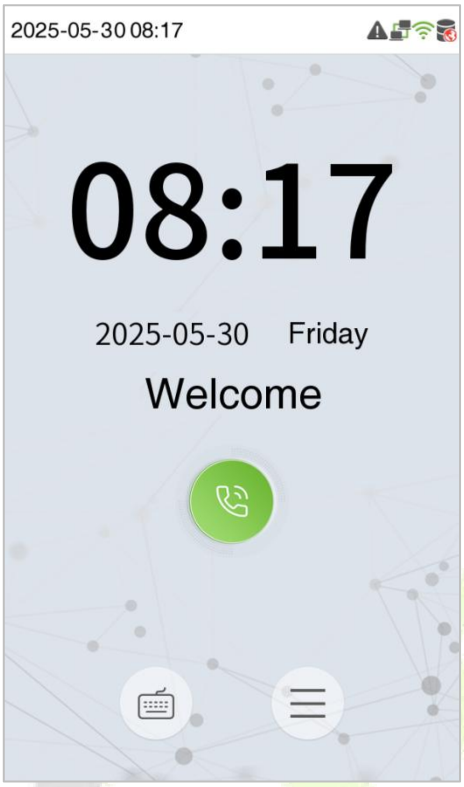
- When registering a face, maintain a distance of 40cm to 80cm between the device and the face.
- Be careful to keep your facial expression natural and not to change. (smiling face, drawn face, wink, etc.)
- If you do not follow the instructions on the screen, the face registration may take longer or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

Recommendation for Authenticating a Face

- Ensure that the face appears inside the guideline displayed on the screen of the device.
- Sometimes, authentication may fail due to the change in the wearing glasses then the one used while registration. In such a case, you may require authenticating your face with the previously worn glasses. If your face was registered without glasses, you should authenticate your face without glasses further.
- 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.

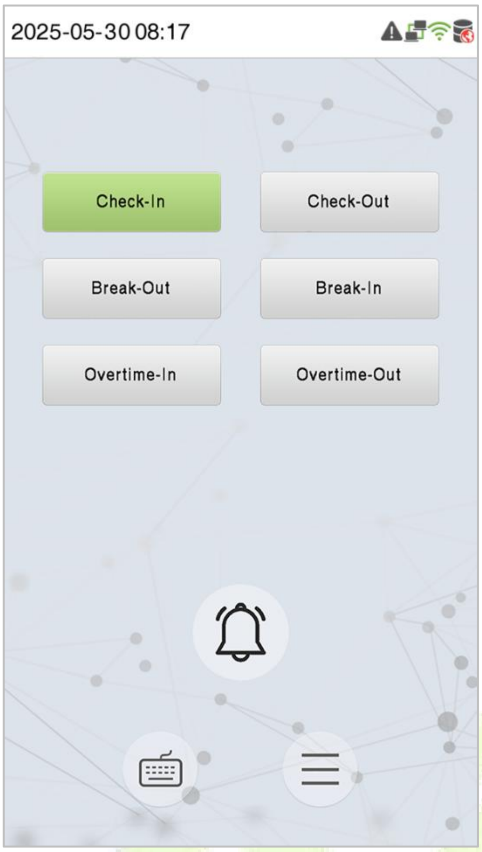
2.4 Standby Interface

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



- Tap ⌨ to enter the User ID input interface.
- When there is no Super Administrator set in the device, tap ☰ to go to the menu.
- After adding a Super Administrator on the device, it requires the Super Administrator's verification before opening the menu functions.

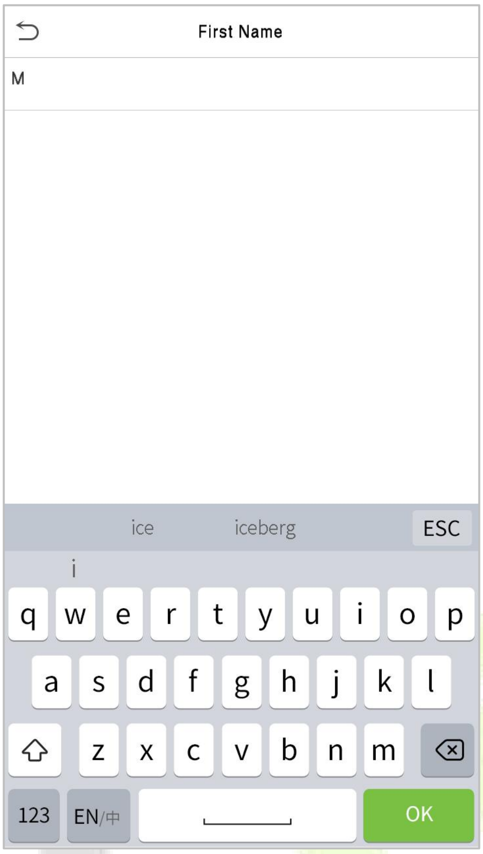
  Note: For the security of the device, it is recommended to register a super administrator the first time you use the device.
- The punch state options can also be displayed and used directly on the standby interface. Tap anywhere on the screen apart from the icons, and six shortcut keys appears on the screen, as shown in the figure below:



- Press the corresponding punch state key to select your current punch state, which is displayed in green. Please refer to "Shortcut Key Mappings" for the specific operation method.

  Note: The punch state options are off by default and need to select other mode options in the "Punch States Options" to get the punch state options on the standby screen.

2.5 Virtual Keyboard



Note: The device supports the input in Chinese language, English language, numbers, and symbols.

- Tap **En** to switch to the English keyboard.
- Press **123** to switch to the numeric and symbolic keyboard.
- Tap **ABC** to return to the alphabetic keyboard.
- Tap the input box, a virtual keyboard appears.
- Tap **ESC** to exit the virtual keyboard.

2.6 Verification Mode

2.6.1 Fingerprint Verification

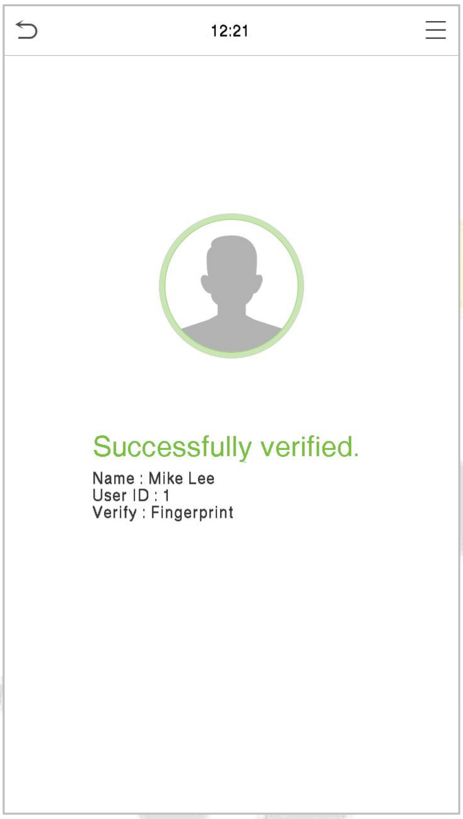
- **1: N Fingerprint Verification Mode**

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

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

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

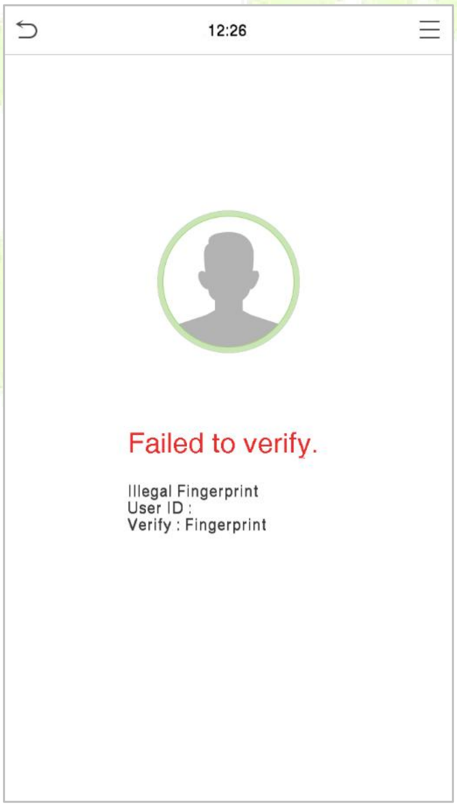
Verification is successful:



Successfully verified.

Name : Mike Lee
User ID : 1
Verify : Fingerprint

Verification is failed:



Failed to verify.

Illegal Fingerprint
User ID :
Verify : Fingerprint

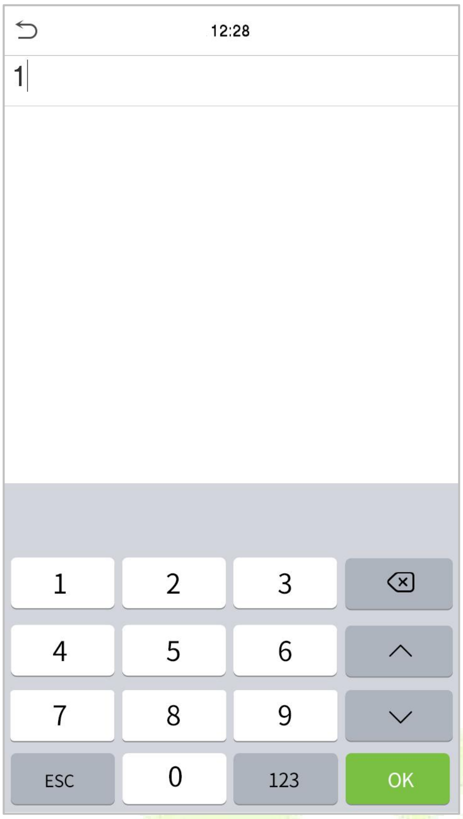
- **1: 1 Fingerprint Verification Mode**

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

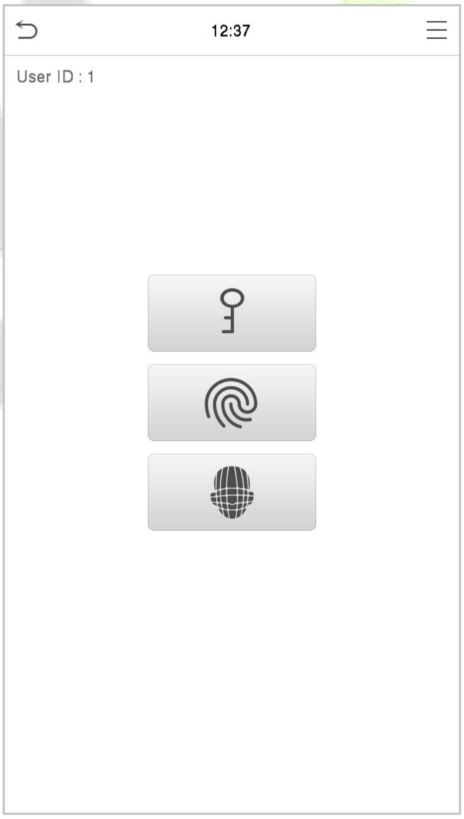
Users may verify their identities with 1:1 verification mode when they cannot gain access with 1: N authentication method.

Click the ⌨ button on the main screen to enter 1:1 fingerprint verification mode.

Input the user ID and press **OK**.

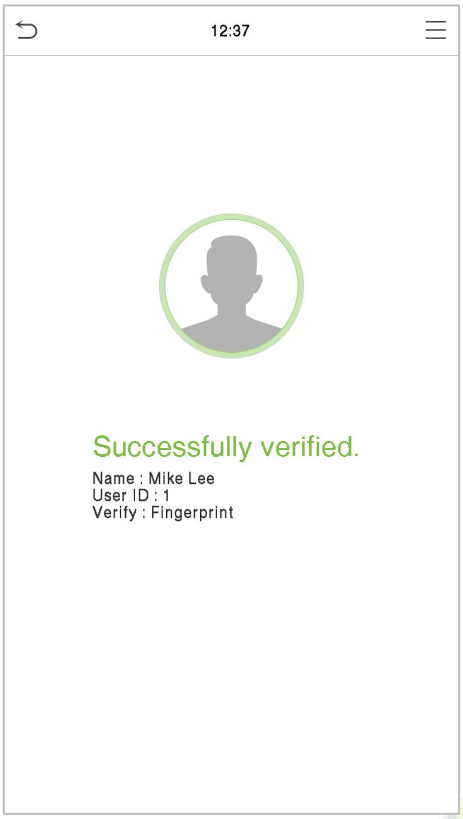


If the user has registered face and password in addition to his/her fingerprints and the verification method is set to Password/Fingerprint/Face verification, the following screen will appear. Select the fingerprint icon to enter fingerprint verification mode.



Press the fingerprint to verify.

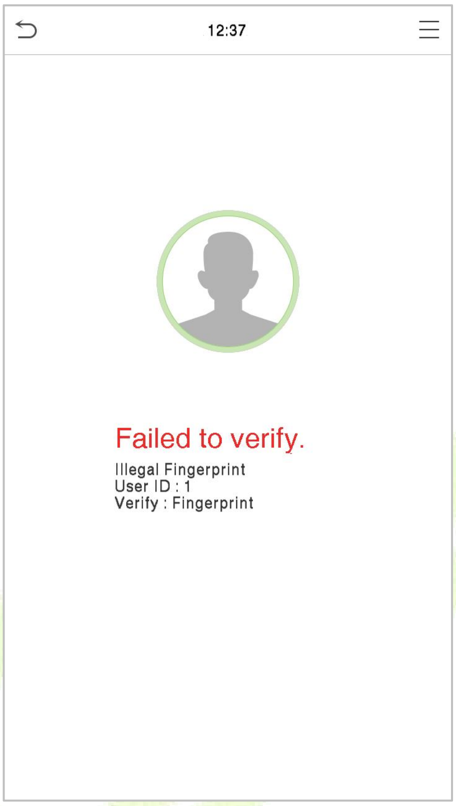
Verification is successful:



Successfully verified.

Name : Mike Lee
User ID : 1
Verify : Fingerprint

Verification is failed:



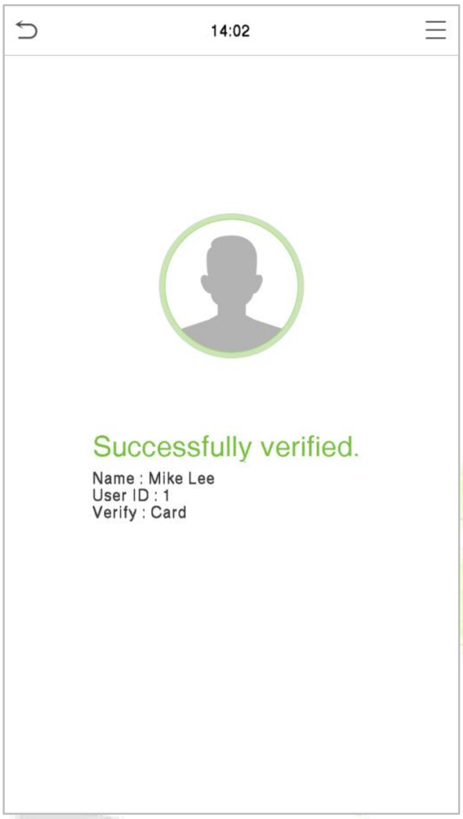
Failed to verify.

Illegal Fingerprint
User ID : 1
Verify : Fingerprint

2.6.2 Card Verification

- **1:N Card Verification**

It compares the acquired card information with all card data registered in the device. The following is the pop-up prompt box of comparison results.



Successfully verified.

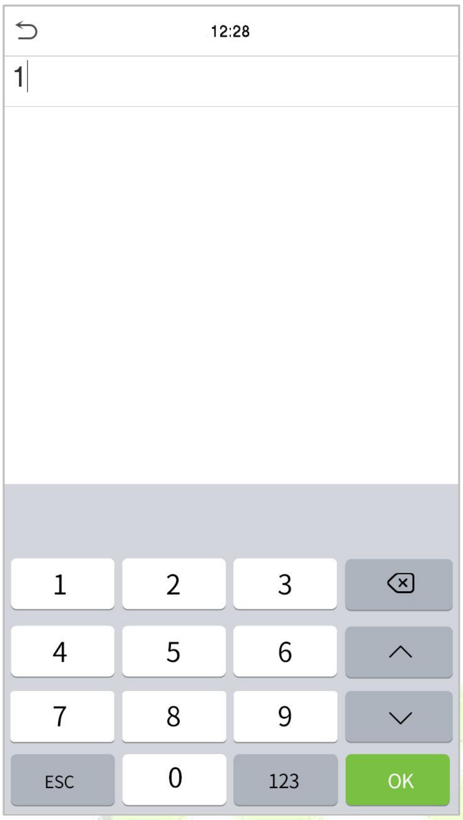
Name : Mike Lee
User ID : 1
Verify : Card

- **1:1 Card Verification**

Compares the card that is being put onto the card reader with the card data that related to the entered user ID.

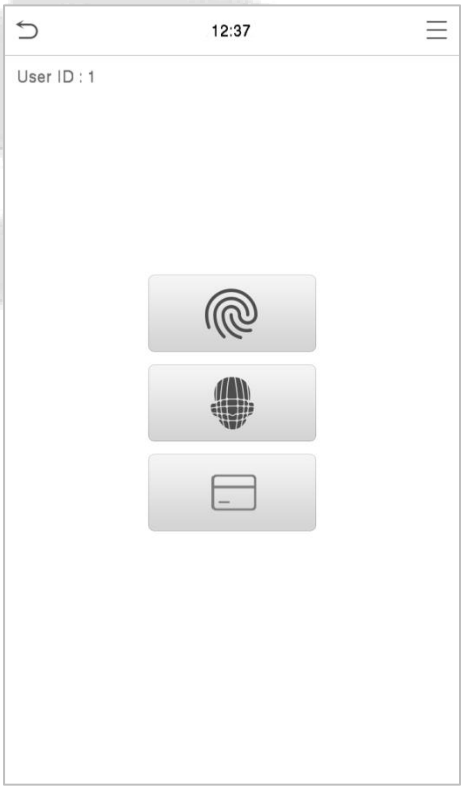
Press ⌨ on the main interface and enter the 1:1 card verification mode.

Enter the user ID and click **OK**.



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

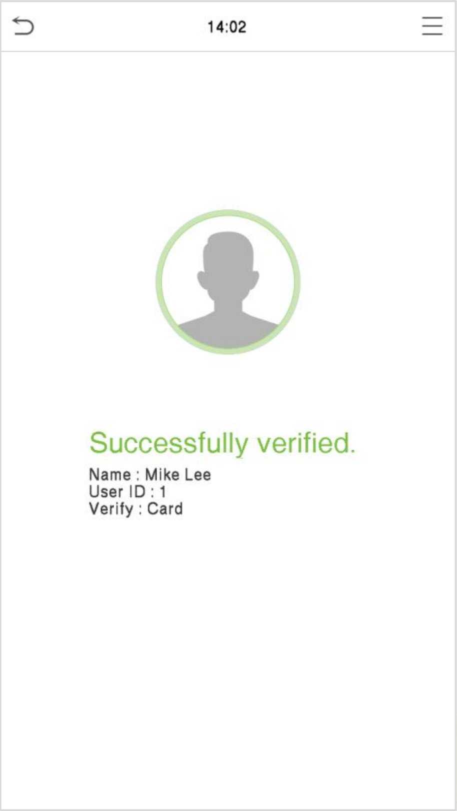
If the user has registered fingerprint and face in addition to the card and the verification method is set to Password/Fingerprint/Card/Face verification, the following screen will appear.



User ID : 1

Following are the display screen after putting a correct card and a wrong card respectively.

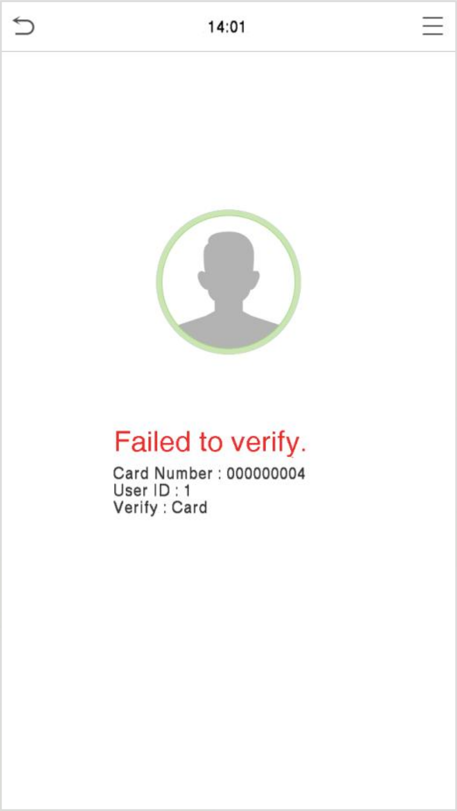
Verification is successful:



Successfully verified.

Name : Mike Lee
User ID : 1
Verify : Card

Verification is failed:



Failed to verify.

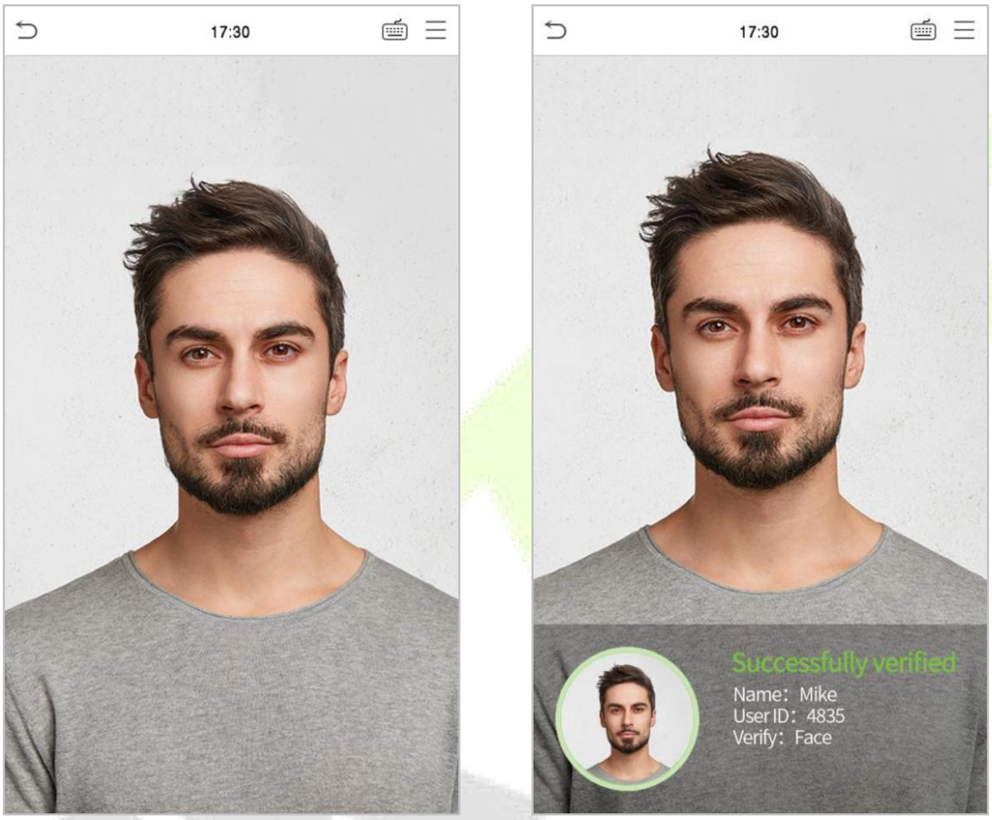
Card Number : 000000004
User ID : 1
Verify : Card

2.6.3 Facial Verification

- **1:N Facial Verification**

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.



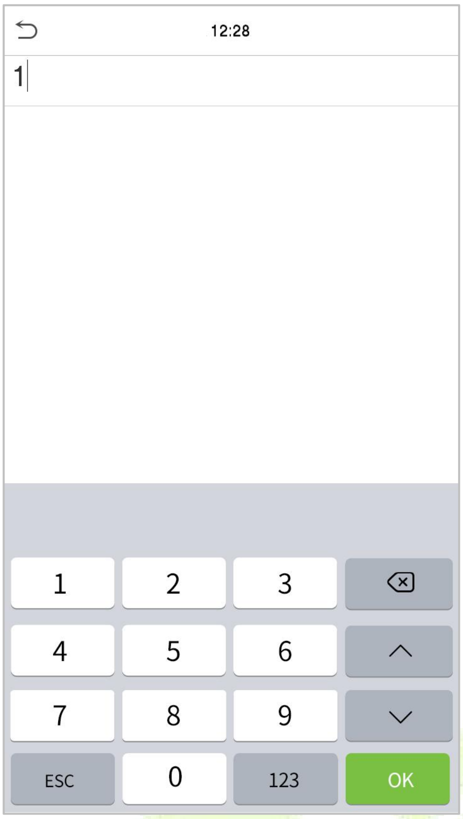
Successfully verified
Name: Mike
User ID: 4835
Verify: Face

- **1:1 Facial Verification**

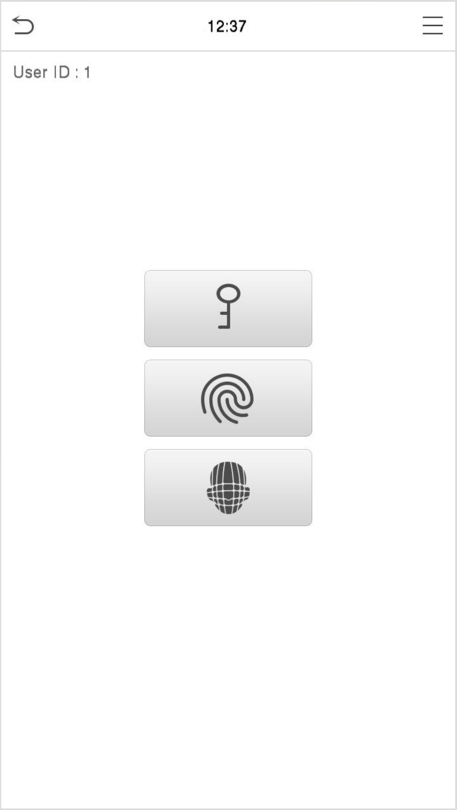
Compare the face captured by the camera with the facial template related to the entered user ID.

Press ⌨ on the main interface and enter the 1:1 facial verification mode.

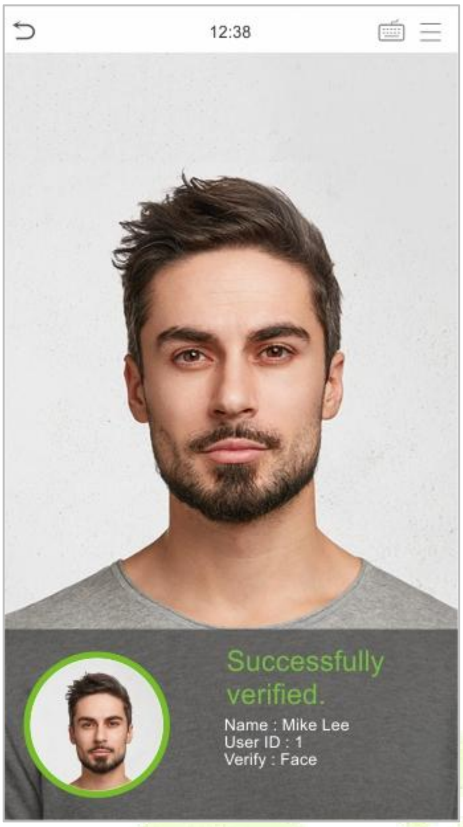
Enter the user ID and click **OK**.



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



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



Successfully verified.

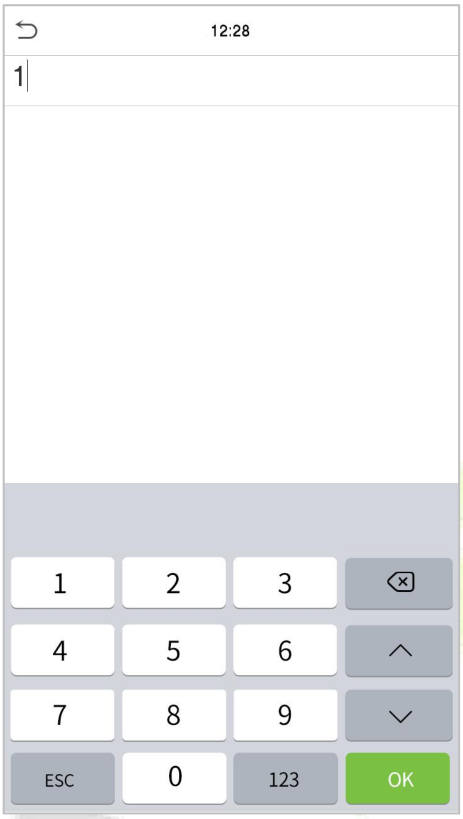
Name : Mike Lee
User ID : 1
Verify : Face

If the verification is failed, it prompts "**Please adjust your position!**".

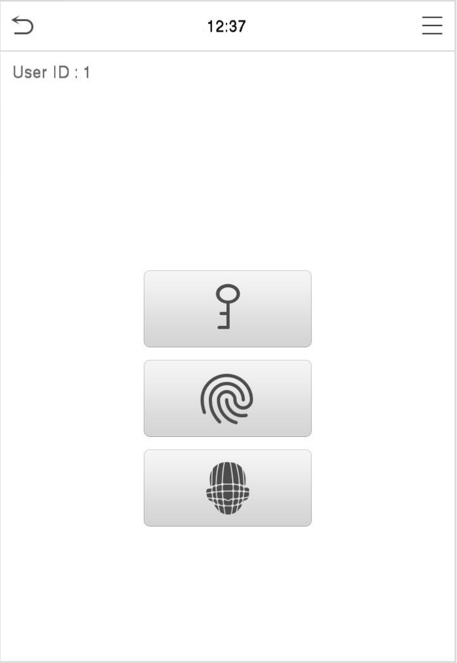
2.6.4 Password Verification

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

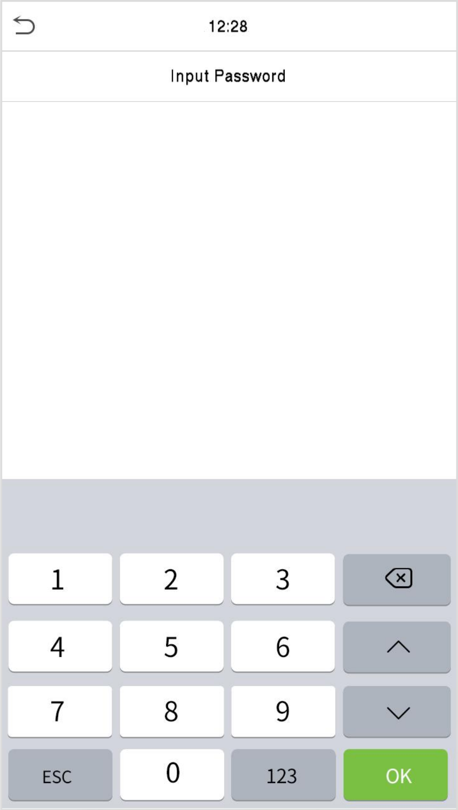
Tap the ⌨ button on the main screen to enter the 1:1 password verification mode. Then, input the user ID and press **OK**.



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

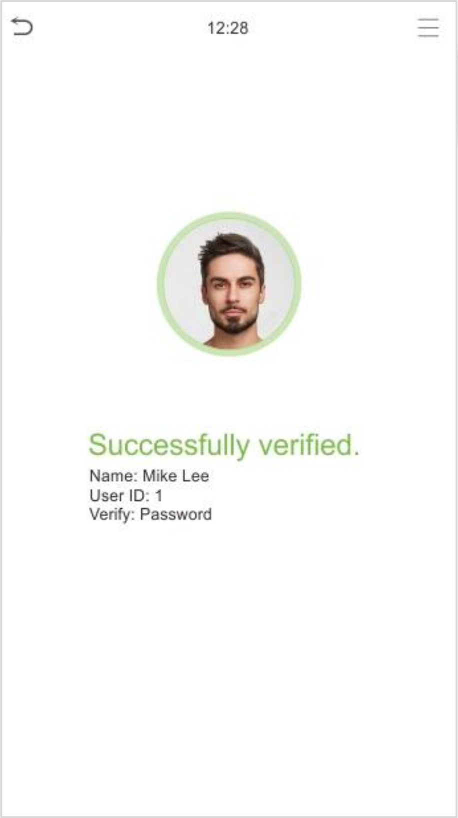


Input the password and press **OK**.



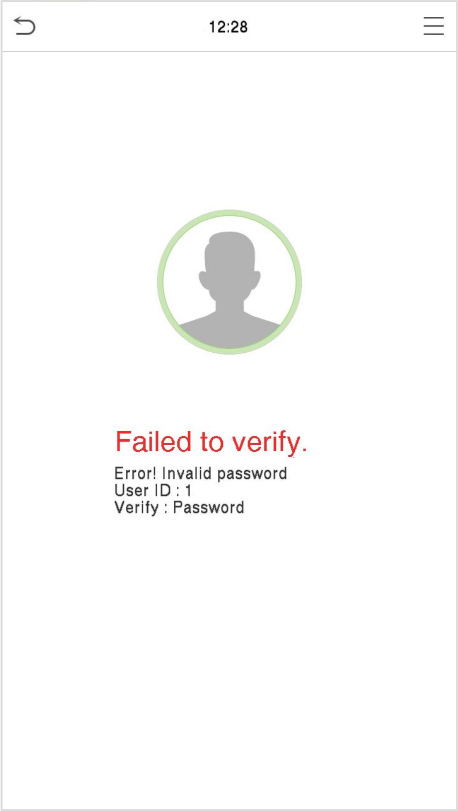
Following are the display screen after entering a correct password and a wrong password respectively.

Verification is successful:



Successfully verified.
Name: Mike Lee
User ID: 1
Verify: Password

Verification is failed:



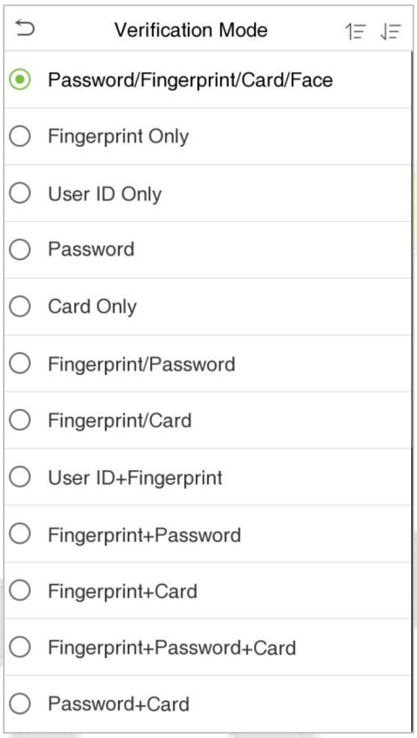
Failed to verify.
Error! Invalid password
User ID : 1
Verify : Password

2.6.5 Combined Verification

To increase security, this device offers the option of using multiple forms of verification methods. A total of 21 different verification combinations can be used, as shown below:

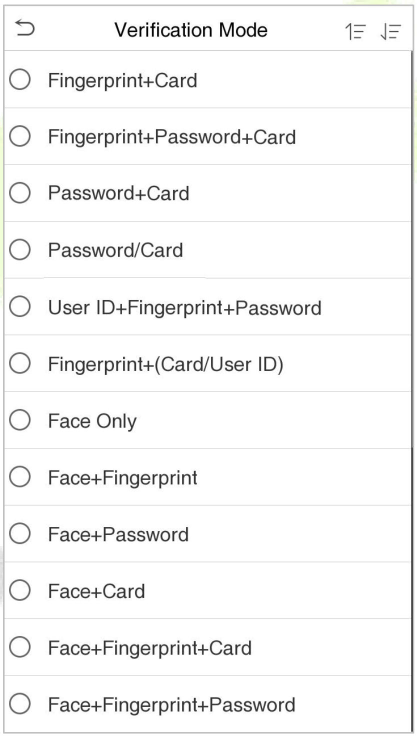
Combined Verification Symbol Definition:

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



Verification Mode

- ● Password/Fingerprint/Card/Face
- ○ Fingerprint Only
- ○ User ID Only
- ○ Password
- ○ Card Only
- ○ Fingerprint/Password
- ○ Fingerprint/Card
- ○ User ID+Fingerprint
- ○ Fingerprint+Password
- ○ Fingerprint+Card
- ○ Fingerprint+Password+Card
- ○ Password+Card



Verification Mode

- ○ Fingerprint+Card
- ○ Fingerprint+Password+Card
- ○ Password+Card
- ○ Password/Card
- ○ User ID+Fingerprint+Password
- ○ Fingerprint+(Card/User ID)
- ○ Face Only
- ○ Face+Fingerprint
- ○ Face+Password
- ○ Face+Card
- ○ Face+Fingerprint+Card
- ○ Face+Fingerprint+Password

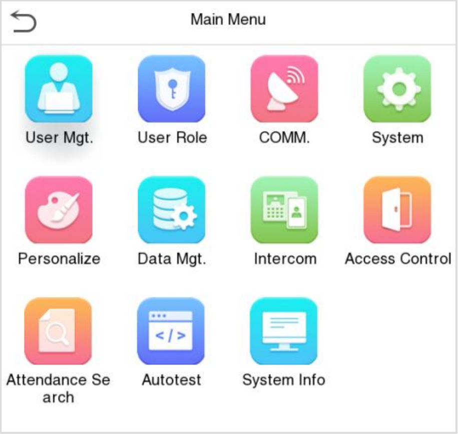
Procedure to set for Combined Verification Mode:

- Combined verification requires personnel to register all the different verification method. Otherwise, employees will not be able to successfully verify the combined verification process.
- For instance, when an employee has registered only the data, but the Device verification mode is set as "Face + Password", the employee will not be able to complete the verification process successfully.
- This is because the Device compares the scanned face template template of the person with registered verification template (both the Face template and the Password) previously stored to that Personnel ID in the Device.

- But as the employee has registered only the Face template but not the Password, the verification will not get completed and the Device displays "Verification Failed".

3 Main Menu

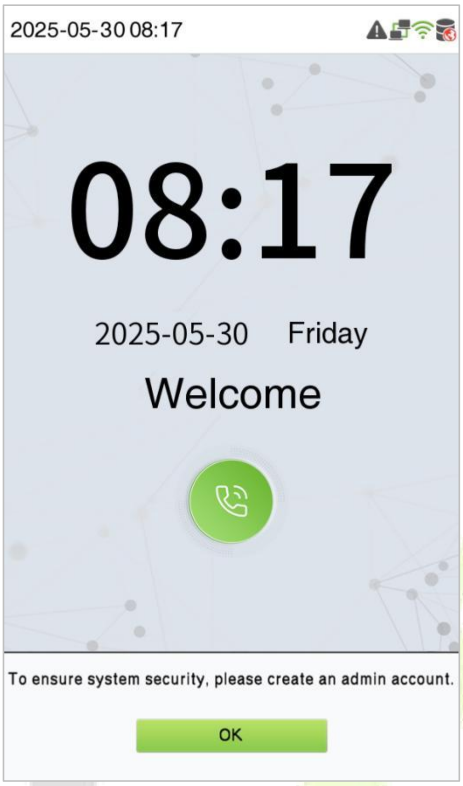
Press ☰ on the initial interface to enter the main menu, as shown below:



Function Description

Menu	Descriptions
User Mgt.	To Add, Edit, View, and Delete information of a User.
User Role	To set the permission scope of the custom role and enroller for the users, that is, the rights to operate the system.
COMM.	To set the relevant parameters of Network, Serial Comm., PC Connection, Wireless Network, Cloud Server, Wiegand and Network Diagnosis.
System	To set the parameters related to the system, including date and time, access logs settings/attendance, face template & fingerprint parameters, health protection, device type settings, advanced settings, security settings, Tap-To-Unlock, update firmware online, and reset to factory.
Personalize	To customize settings of User Interface, Voice, Bell Schedules, Punch State Options and Shortcut Key Mappings settings.
Data Mgt.	To delete all relevant data in the device.
Intercom	To set the parameters related to the SIP and NVR.
Access Control	To set the parameters of the lock and the relevant access control device including options like Time rule, Holiday Settings, Combined verification, Anti-passback Setup, and Duress Option Settings.
Attendance Search	To query the specified Event logs, check Attendance Photos and Blocklist attendance photos.
Autotest	To automatically test whether each module functions properly, including the LCD Screen, Audio, Microphone, Fingerprint sensor, Camera, and Real-Time Clock.
System Info	To view 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.

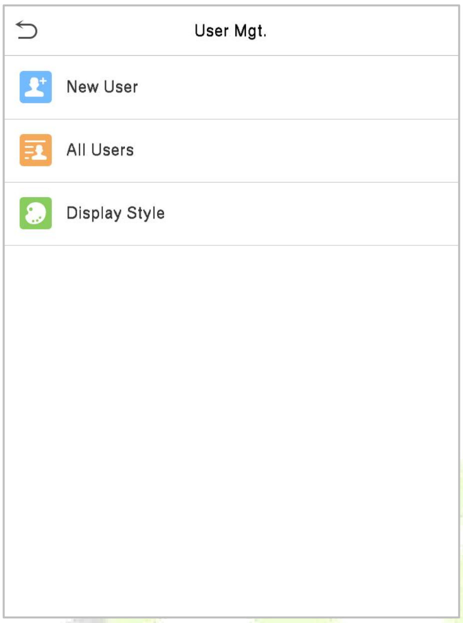


To ensure system security, please create an admin account.

4 User Management

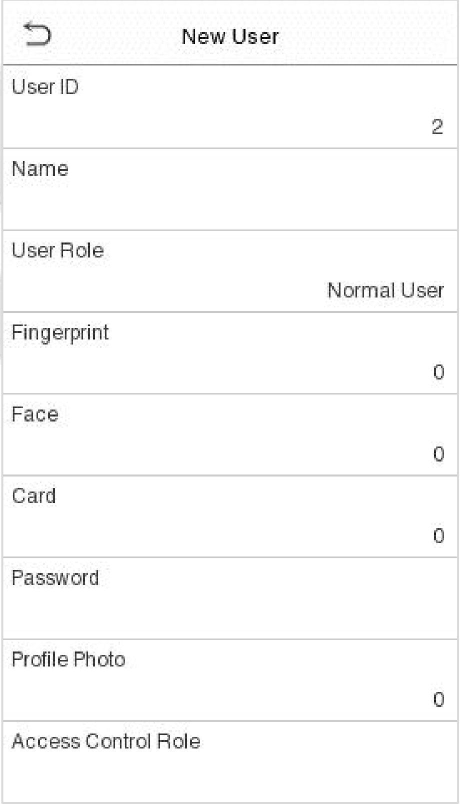
4.1 User Registration

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



4.1.1 Register a User ID and Name

Tap **New User** and enter the **User ID** and **Name**.



User ID 2

Name

User Role Normal User

Fingerprint 0

Face 0

Card 0

Password

Profile Photo 0

Access Control Role

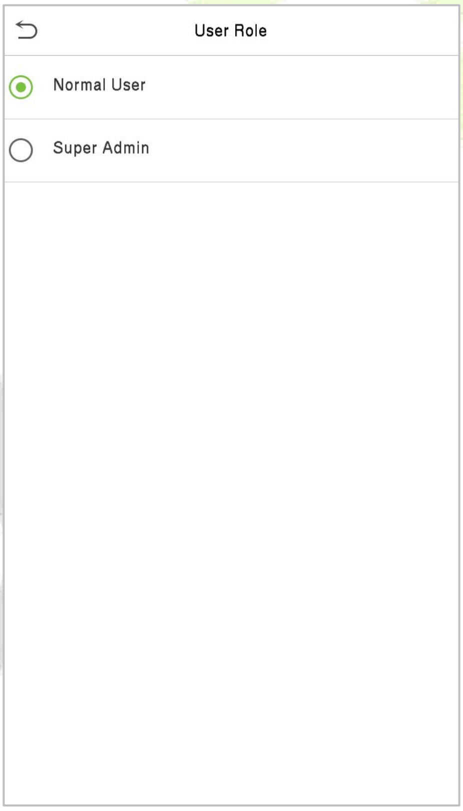
Note:

- A name can take up to 17 characters.
- The user ID may contain 1-9 digits by default.
- You can modify your ID during the initial registration but not after registration.
- If a message "**Duplicated!**" pops up, you must choose another ID as the entered User ID already exists.

4.1.2 Setting the User Role

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

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



User Role

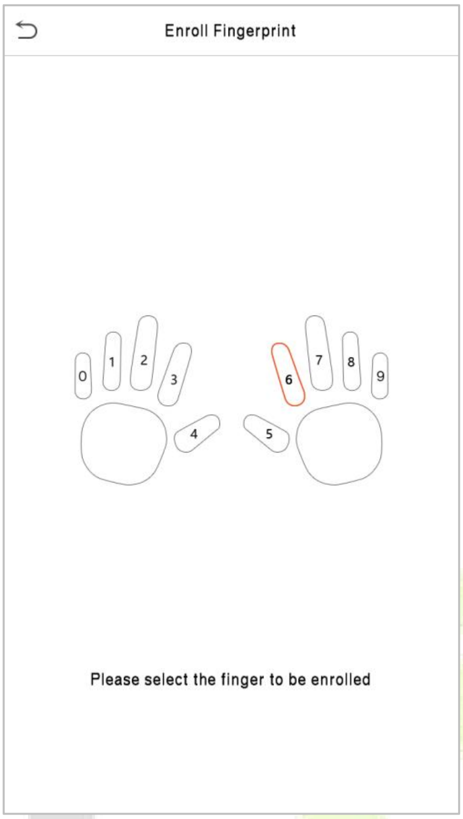
● Normal User

○ Super Admin

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

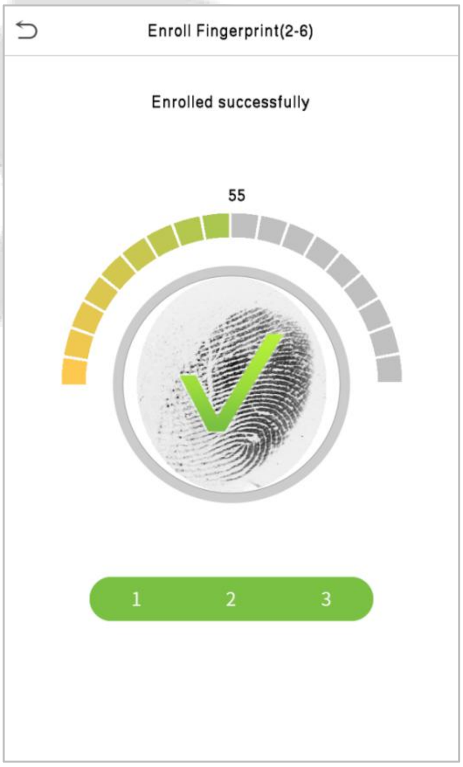
4.1.3 Register Fingerprint

Click **Fingerprint** to enter the fingerprint registration page. Select the finger to be enrolled.



Please select the finger to be enrolled

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



Enrolled successfully

4.1.4 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:

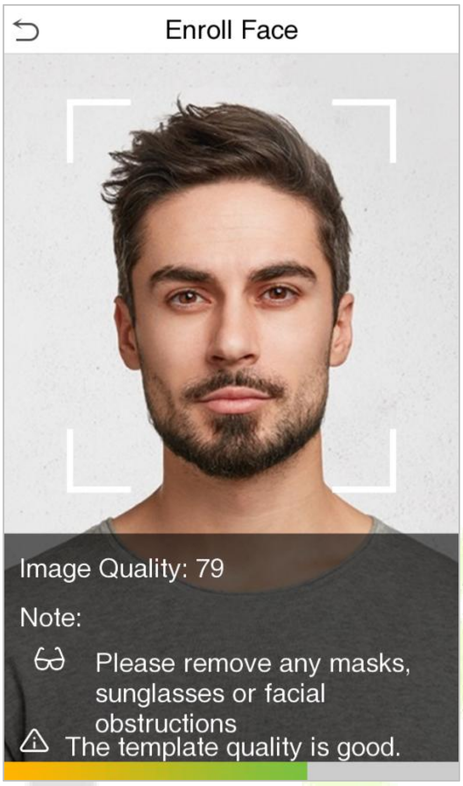


Image Quality: 79

Note:

Please remove any masks, sunglasses or facial obstructions

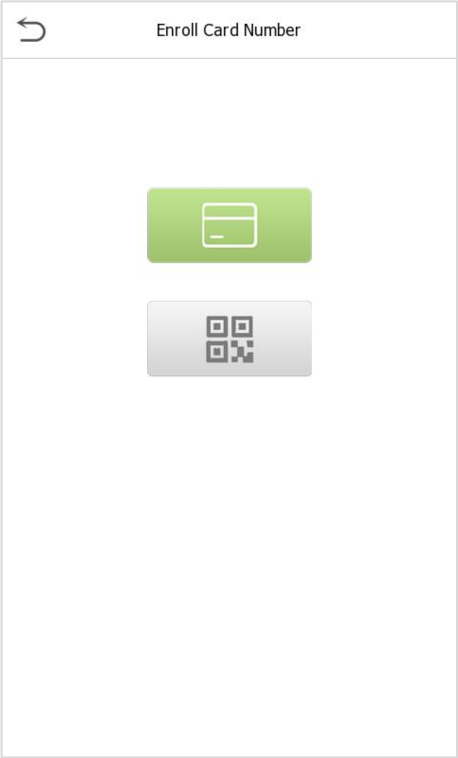
The template quality is good.

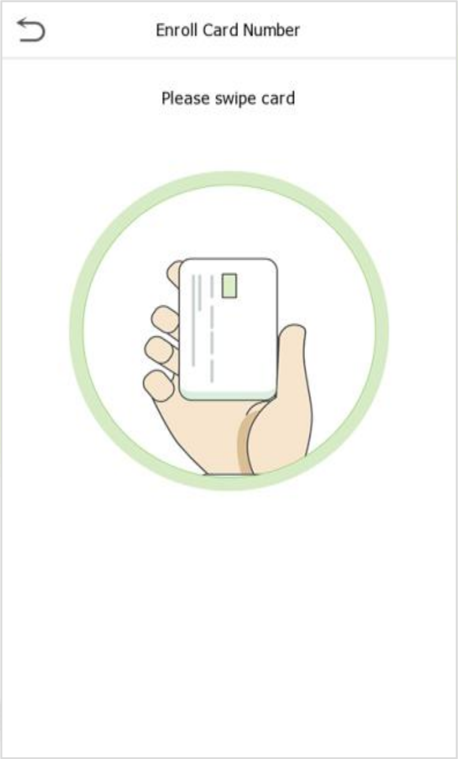
4.1.5 Register Card Number

- **Enroll Card**

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

- On the Card interface, swiping card underneath the card reading area. The card registration will be successful.
- If the card is registered already then the "**Duplicate Card**" message shows up. The registration interface is as follows:



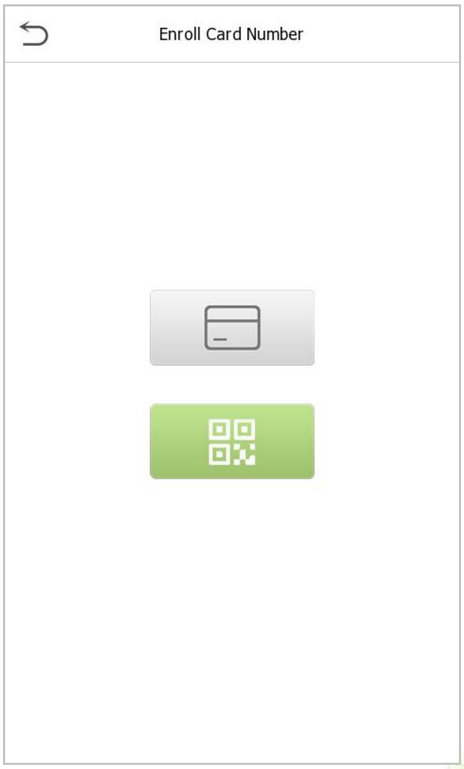


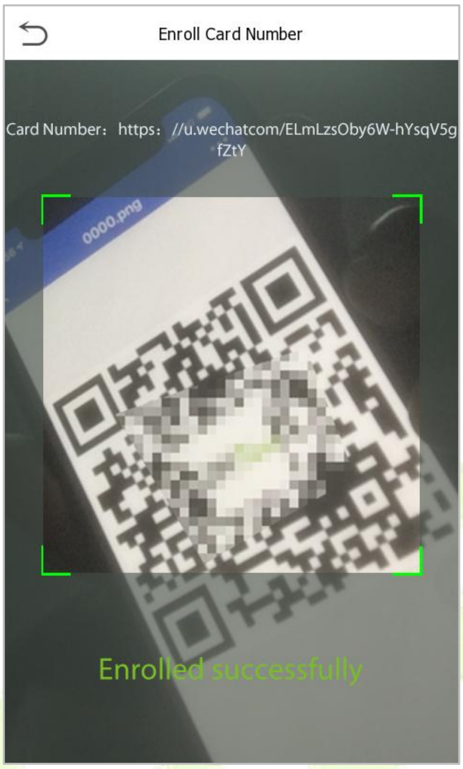
Please swipe card

- **Enroll QR Code ★**

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

- On the Card interface, show the QR code in front of the camera. The QR code registration will be successful.
- If the QR code is registered already then the "**Error! Card already enrolled.**" message shows up. The registration interface is as follows:



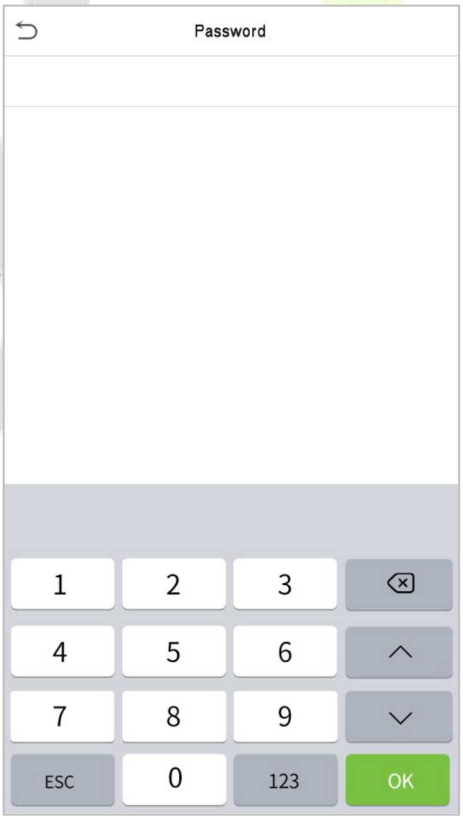


Card Number：https：//u.wechatcom/ELmLzsOby6W-hYsqV5gfZtY

Enrolled successfully

4.1.6 Register Password

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



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

4.1.7 Register User Photo

When a user registered with a photo passes the authentication, the registered photo will be displayed.

Click **User 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 user photo. If you do not want to register a user photo, the system will automatically set the picture captured as the default photo.

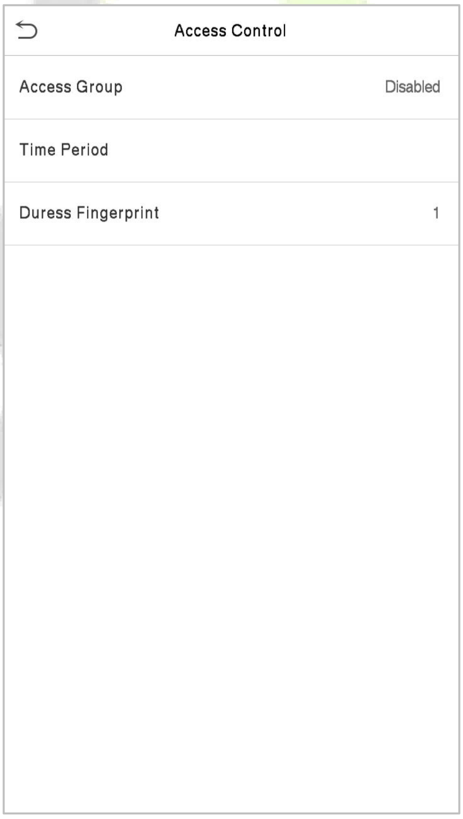
4.1.8 Access Control Role

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

Click **Access Control Role** > **Access Group**, 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.

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

Click **Duress Fingerprint**, user can choose one or more registered fingerprint(s) as Duress Fingerprint. When verifying through duress fingerprint, duress alarm will be triggered.



Access Control

Access Group Disabled

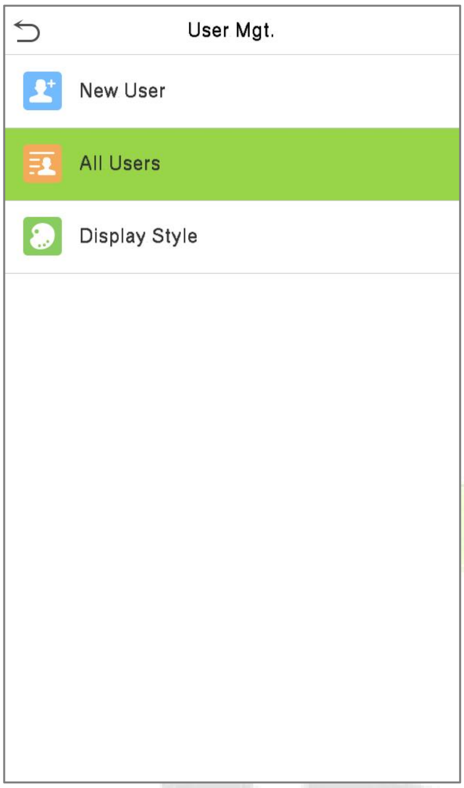
Time Period

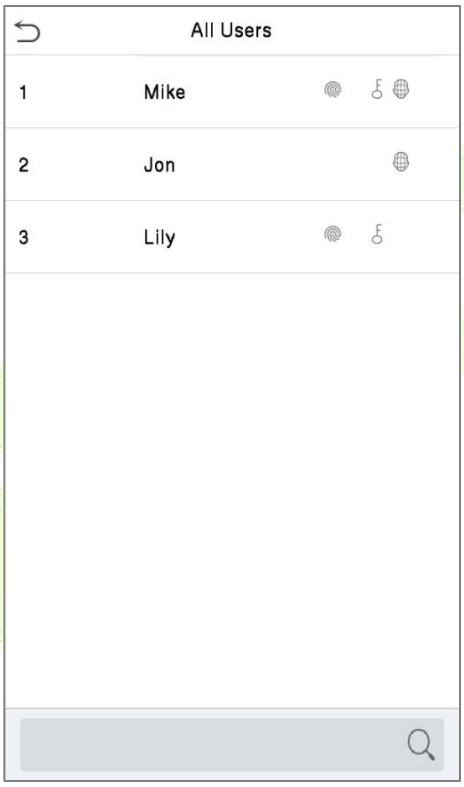
Duress Fingerprint 1

4.2 Search User

On the **Main Menu**, tap **User Mgt.,** and then tap **All Users** to search a User.

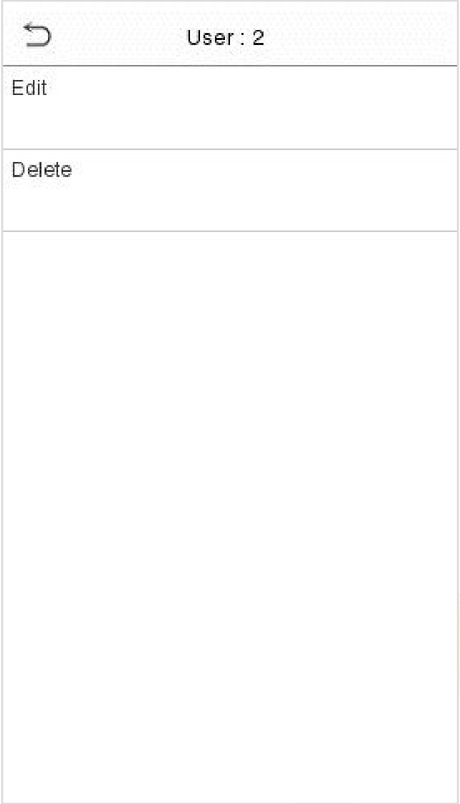
On the **All Users** interface, tap on the search bar on the user's list to enter the required retrieval keyword (where the keyword may be the user ID, surname, or full name) and the system will search for the related user information.





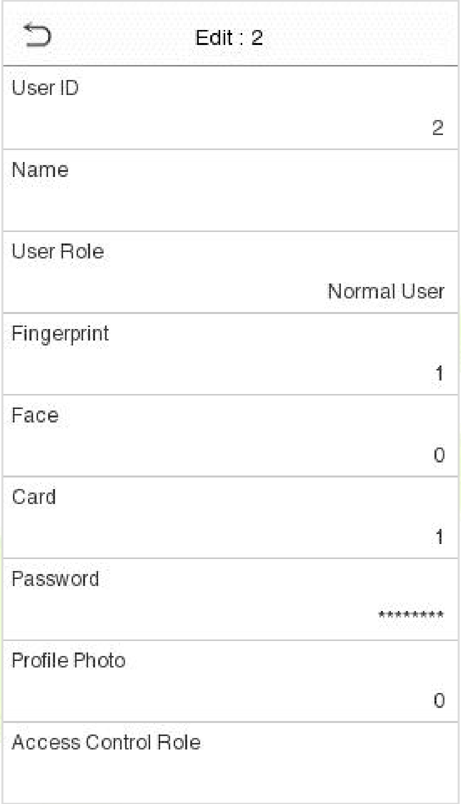
4.3 Edit User

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


User : 2

Edit

Delete


Edit : 2

User ID 2

Name

User Role Normal User

Fingerprint 1

Face 0

Card 1

Password ********

Profile Photo 0

Access Control Role

Note: The process of editing the user information is the same as adding a new user, except that the User ID cannot be modified when editing a user. The process in detail refers to "*4. User Management*".

4.4 Deleting User

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

- **Delete Operations**

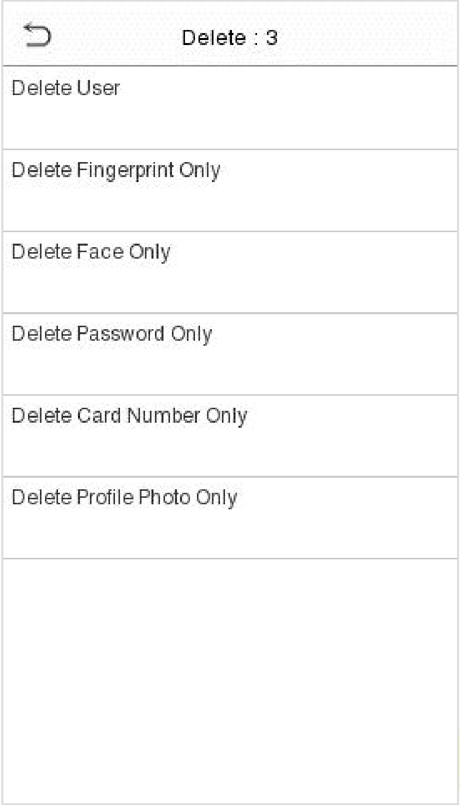
Delete User: Deletes all the user information (deletes the selected User as a whole) from the Device.

Delete Face Only: Deletes the Face information of the selected user.

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

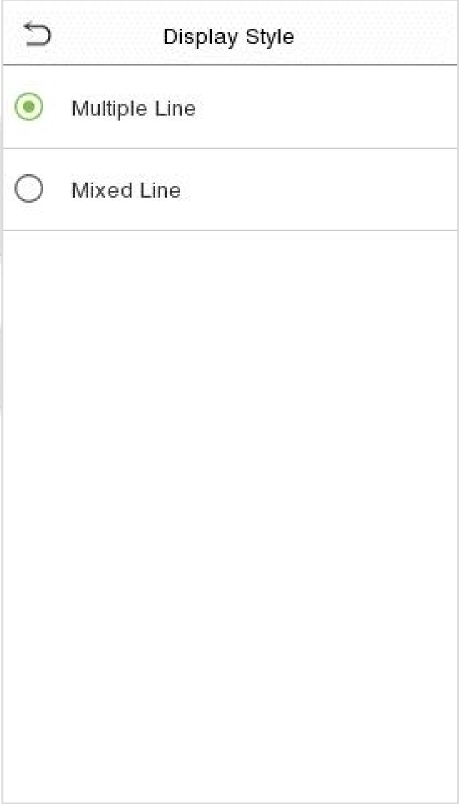
Delete Fingerprint Only: Deletes the Fingerprint information of the selected user.

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



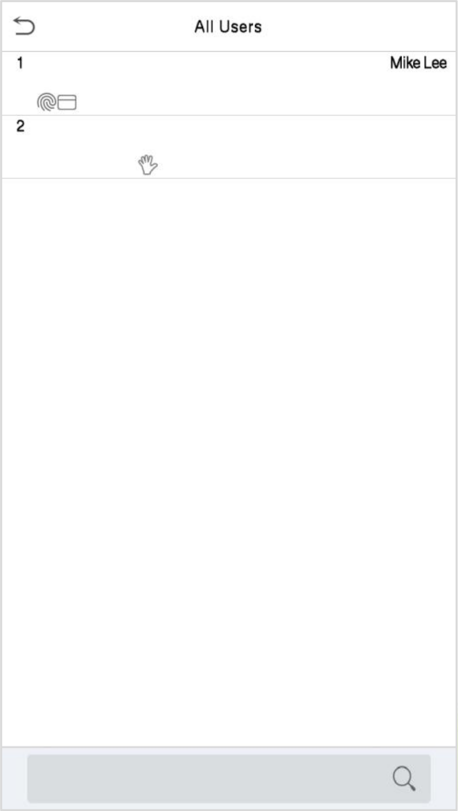
4.5 Display Style

Tap on **User Mgt.** > **Display Style** to choose the style of **All Users** interface's list.

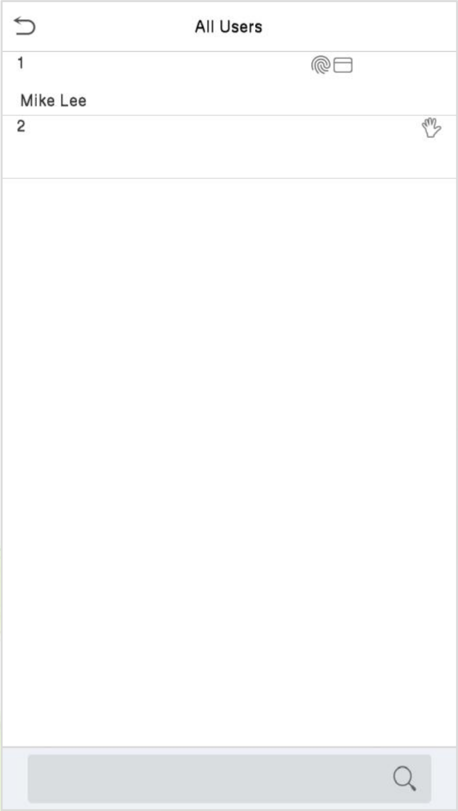


Different display styles are shown as below:

Multiple Line:



Mixed Line:

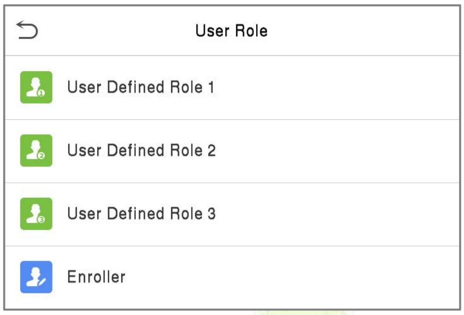


5 User Role

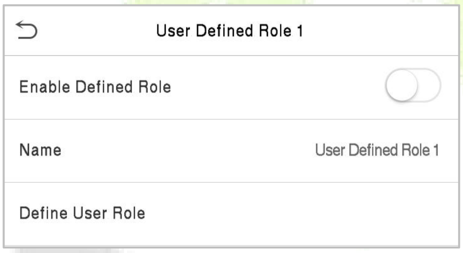
If you need to assign some specific permissions to certain users, you may edit the "User Defined Role" under the **User Role** menu.

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.



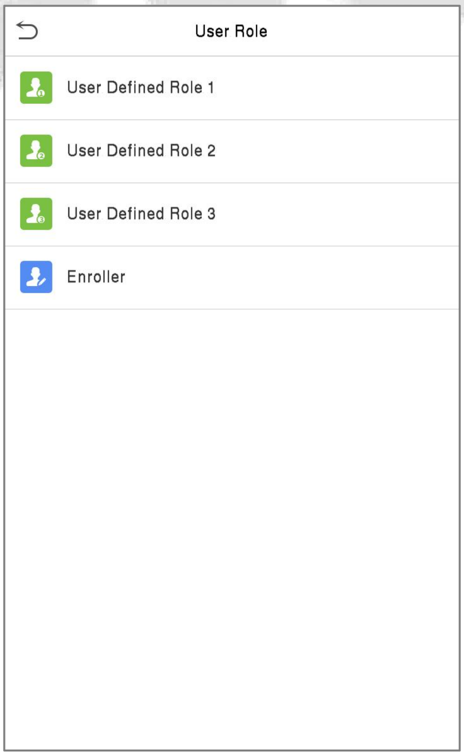
On the **User Defined Role** interface, toggle **Enable Defined Role** to enable or disable the user-defined role.

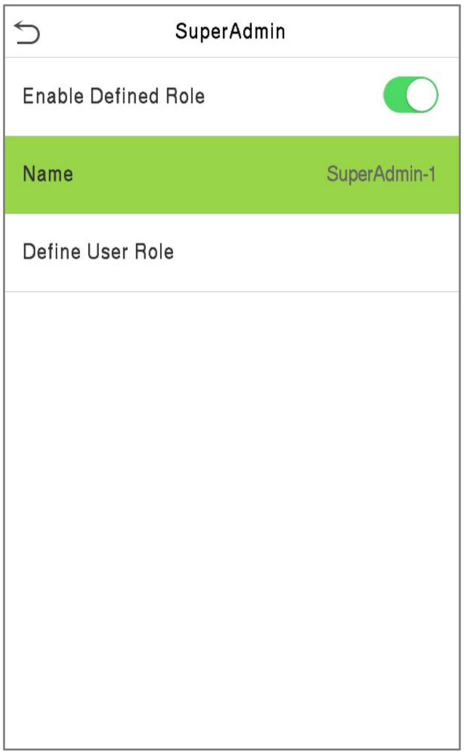


Enable Defined Role ○

Name User Defined Role 1

Tap on **Name** and enter the custom name of the role.





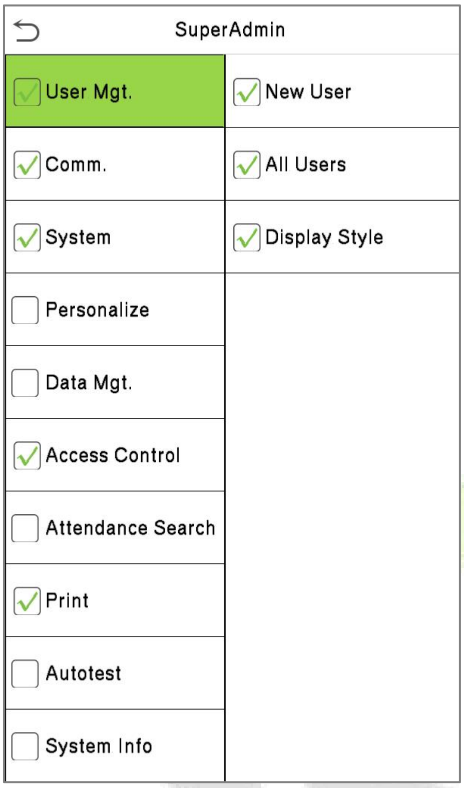
Enable Defined Role ●

Name SuperAdmin-1

Then, tap on **Define User Role** and select the required privileges to assign to the new role, and then tap on the **Return** button.

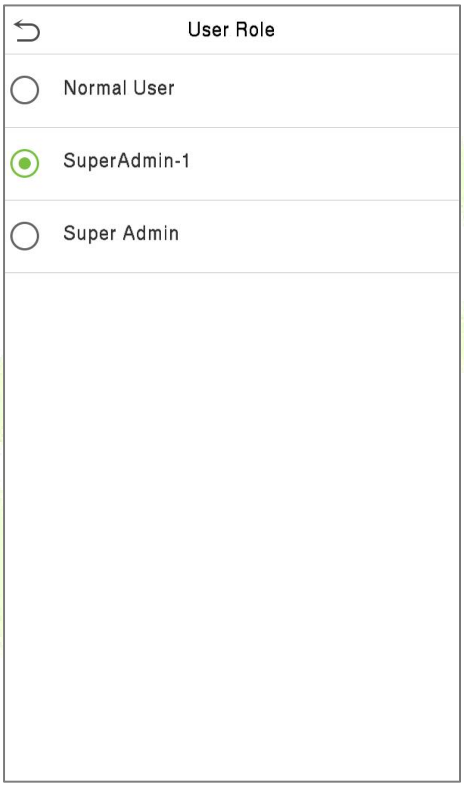
During privilege assignment, the **Main Menu** function names will be displayed on the left and its sub-menus will be listed on its right.

First, tap on the required **Main Menu** functions, and then select its required sub-menus from the list which the user can access.



SuperAdmin

☑ User Mgt.	☑ New User
☑ Comm.	☑ All Users
☑ System	☑ Display Style
☐ Personalize	
☐ Data Mgt.	
☑ Access Control	
☐ Attendance Search	
☑ Print	
☐ Autotest	
☐ System Info	



User Role

○ Normal User

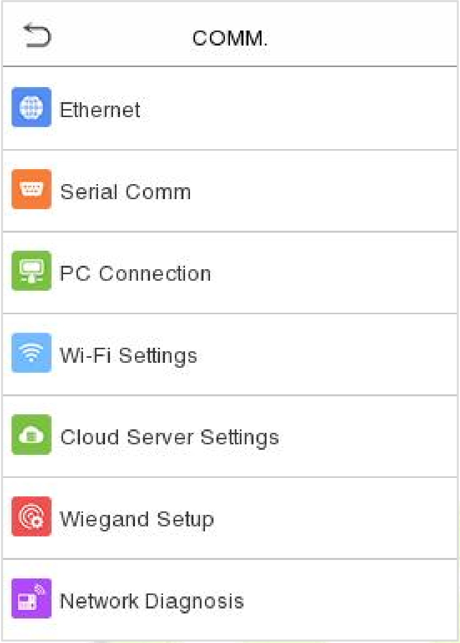
● SuperAdmin-1

○ Super Admin

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

6 Communication Settings

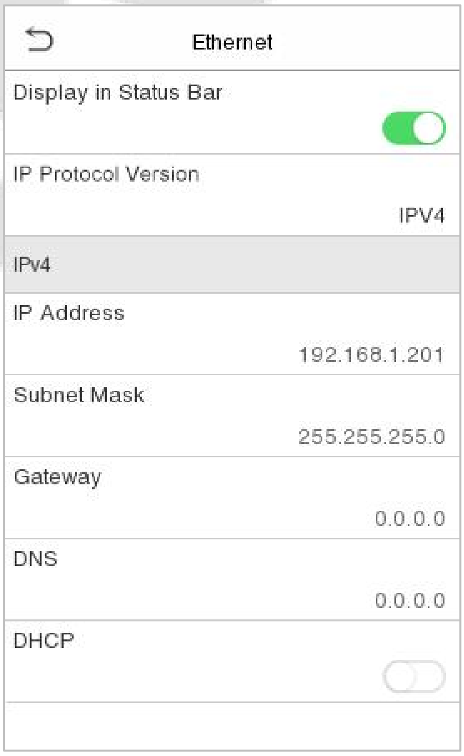
Tap **COMM.** on the **Main Menu** to set the relevant parameters of Network, Serial Comm, PC Connection, Wireless Network, Cloud Server, Wiegand and Network Diagnosis.



6.1 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 connect to the same network segment.

Tap **Ethernet** on the **Comm**. Settings interface to configure the settings.


Ethernet

Display in Status Bar: ON

IP Protocol Version: IPV4

IPv4

IP Address: 192.168.1.201

Subnet Mask: 255.255.255.0

Gateway: 0.0.0.0

DNS: 0.0.0.0

DHCP: OFF

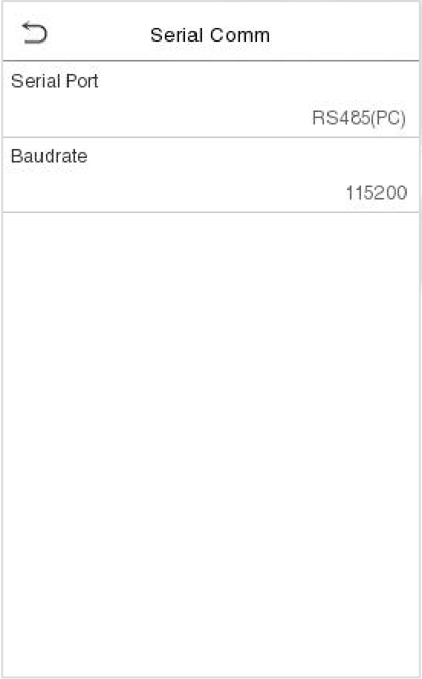
Function Description

Function Name	Descriptions
Display in Status Bar	Toggle to set whether to display the network icon on the status bar.
IP Protocol Version	Displays the IP protocol version, which defaults to IPV4.
IP Address	The default IP address is 192.168.1.201. It can be modified according to the network availability.
Subnet Mask	The default Subnet Mask is 255.255.255.0. It can be modified according to the network availability.
Gateway	The default Gateway address is 0.0.0.0. It can be modified according to the network availability.
DNS	The default DNS address is 0.0.0.0. It can be modified according to the network availability.
TCP COMM. Port	The default TCP COMM Port value is 4370. It can be modified according to the network availability.
DHCP	Dynamic Host Configuration Protocol dynamically allocates IP addresses for clients via server.

6.2 Serial Comm★

Serial Comm function facilitates to establish communication with the device through a serial port (RS232(PC)★/Print Function★/RS485/ Master Unit/DM10).

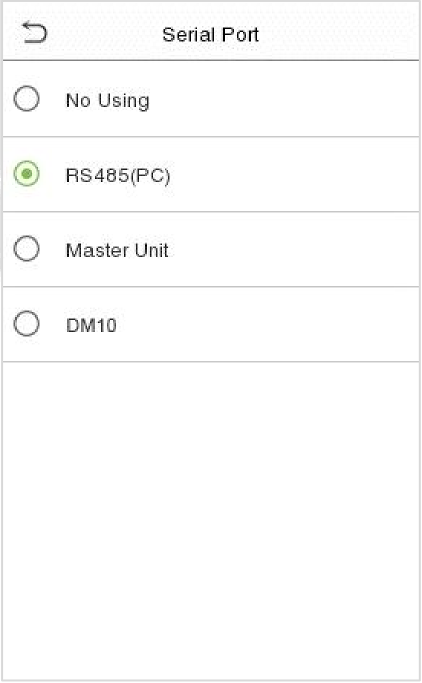
Tap **Serial Comm.** on the **Comm.** Settings interface.



Serial Comm

Serial Port
RS485(PC)

Baudrate
115200



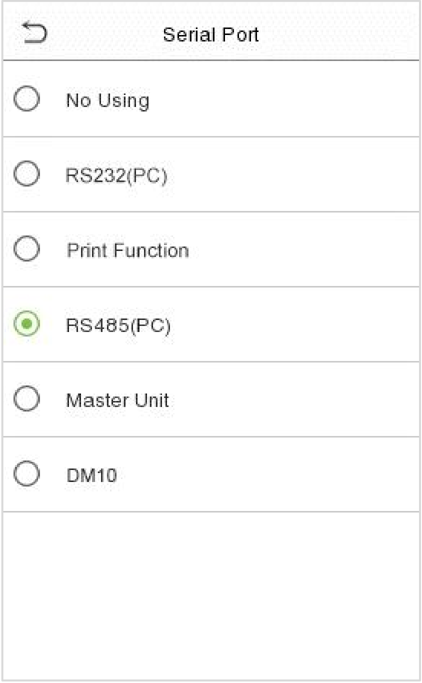
Serial Port

○ No Using

● RS485(PC)

○ Master Unit

○ DM10



Serial Port

○ No Using

○ RS232(PC)

○ Print Function

● RS485(PC)

○ Master Unit

○ DM10

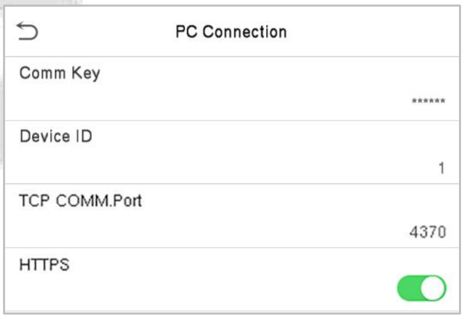
Function Description

Function Name	Descriptions
Serial Port	**No Using:** Do not communicate with the device through the serial port. **RS232(PC)★:** When RS232 is used as the function of "**RS232(PC)**", it can be connected to the PC. **Print Function★:** The device can be connected to the printer when RS232 enables the print function. **RS485(PC):** Communicates with the device through RS485 serial port. **Master Unit:** When RS485 is used as the function of "**Master unit**", the device will act as a master unit, and it can be connected to RS485 fingerprint & card reader. **DM10:** Communicates with theDM10through RS485 serial port.
Baudrate	When the serial port is set as **RS232(PC)**, there are 4 baudrate options. They are: 115200 (default), 57600, 38400 and 19200. When the serial port is set as **Print Function**, there are 5 baudrate options. They are: 115200 (default), 57600, 38400, 19200 and 9600. The higher the baudrate, the faster is the communication speed, but also less reliable. Hence, a higher baudrate can be used when the communication distance is short; when the communication distance is long, choosing a lower baudrate is more reliable.

6.3 PC Connection

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

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



PC Connection

Comm Key ******

Device ID 1

TCP COMM.Port 4370

HTTPS

Function Description

Function Name	Descriptions
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.

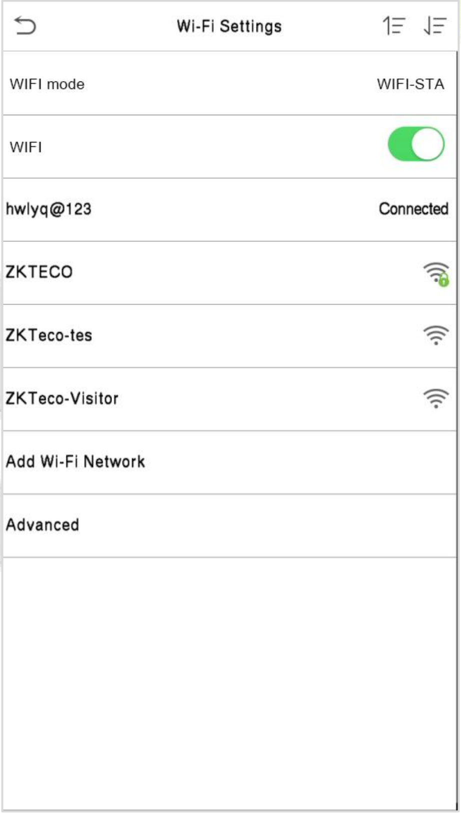
Device ID	It is the identification number of the device, which ranges between 1 and 254.
TCP COMM. Port	The default TCP COMM Port value is 4370. It can be modified according to the network availability.
HTTPS	To increase the security of software access, users can enable the HTTPS protocol to create a 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.

6.4 Wireless Network★

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

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

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



Wi-Fi Settings

WIFI mode WIFI-STA

WIFI ●

hwlyq@123 Connected

ZKTECO

ZKTeco-tes

ZKTeco-Visitor

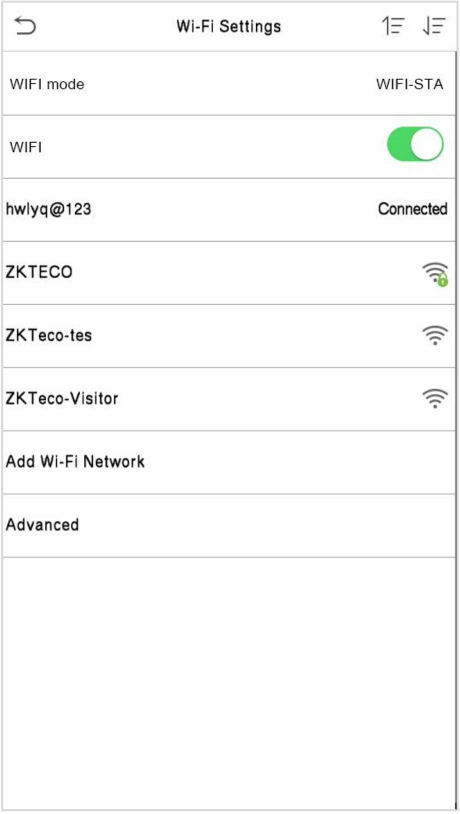
Add Wi-Fi Network

Advanced

Wi-Fi is enabled in the Device by default. Toggle on ● button to enable or disable Wi-Fi.

Once the Wi-Fi is turned on, the device will search for the available Wi-Fi within the network range.

Tap on the appropriate Wi-Fi name from the available list, and input the correct password in the password interface, and then tap **Connect to Wi-Fi (OK)**.



Wi-Fi Settings

WIFI mode WIFI-STA

WIFI

hwlyq@123 Connected

ZKTECO

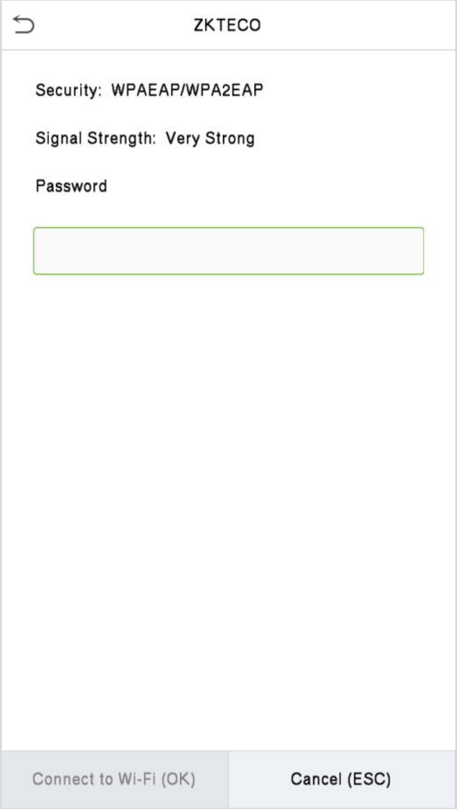
ZKTeco-tes

ZKTeco-Visitor

Add Wi-Fi Network

Advanced

Wi-Fi Enabled: Tap on the required network from the searched network list.



ZKTECO

Security: WPAEAP/WPA2EAP

Signal Strength: Very Strong

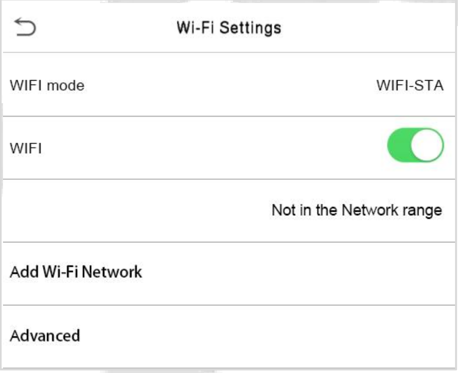
Password

Tap on the password field to enter the password, and then tap on **Connect to Wi-Fi (OK).**

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

- **Add Wi-Fi Network Manually**

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



Wi-Fi Settings

WIFI mode WIFI-STA

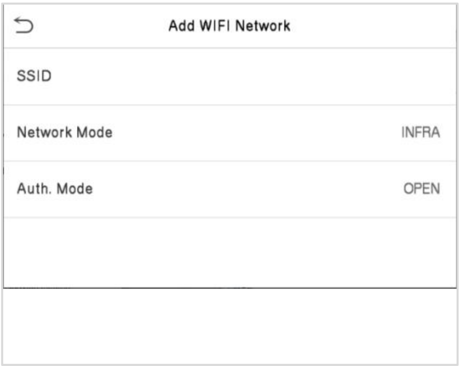
WIFI

Not in the Network range

Add Wi-Fi Network

Advanced

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



Add WIFI Network

SSID

Network Mode INFRA

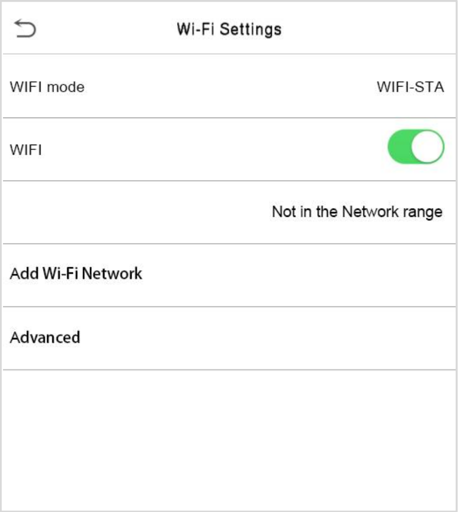
Auth. Mode OPEN

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

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

- **Advanced Setting**

On the **Wireless Network** interface, tap on **Advanced** to set the relevant parameters as required.



Wi-Fi Settings

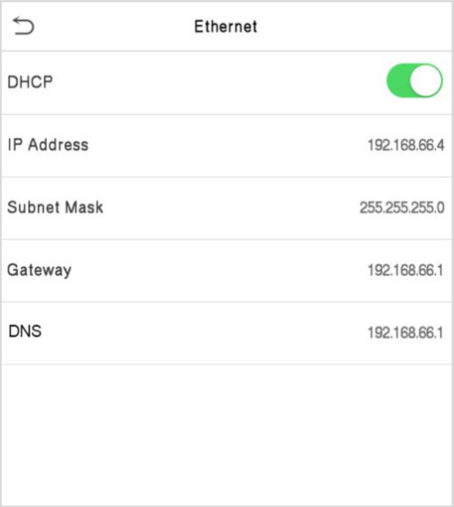
WIFI mode WIFI-STA

WIFI

Not in the Network range

Add Wi-Fi Network

Advanced



Ethernet

DHCP

IP Address 192.168.66.4

Subnet Mask 255.255.255.0

Gateway 192.168.66.1

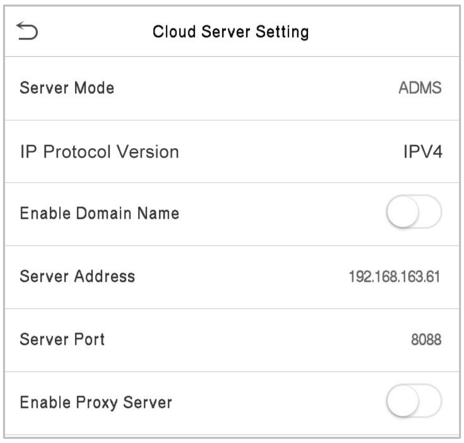
DNS 192.168.66.1

Function Description

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

6.5 Cloud Server Setting

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



Cloud Server Setting

Server Mode ADMS

IP Protocol Version IPV4

Enable Domain Name

Server Address 192.168.163.61

Server Port 8088

Enable Proxy Server

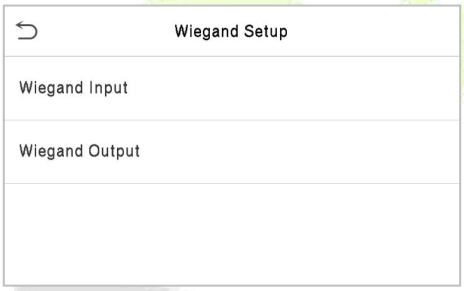
Function Description

Function Name		Description
IP Protocol Version		Displays the IP protocol version, which defaults to IPV4.
Enable Domain Name	**Server Address**	Once this mode is turned **ON**, the domain name mode "http://..." will be used, such as http://www.XYZ.com, while "XYZ" denotes the domain name.
Disable Domain Name	**Server Address**	The IP address of the ADMS server.
	Server Port	Port used by the ADMS server.
Enable Proxy Server		The IP address and the port number of the proxy server is set manually when the proxy is enabled.

6.6 Wiegand Setup

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

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

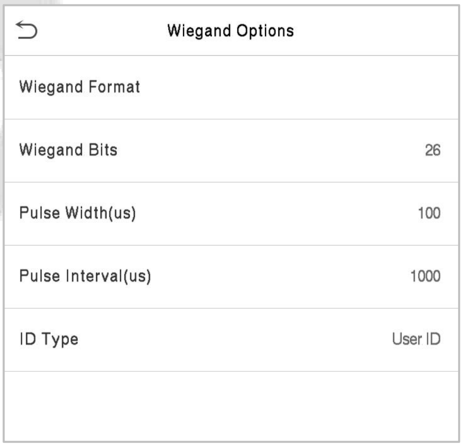


Wiegand Setup

Wiegand Input

Wiegand Output

6.6.1 Wiegand Input



Wiegand Options

Wiegand Format

Wiegand Bits 26

Pulse Width(us) 100

Pulse Interval(us) 1000

ID Type User ID

Function Description

Function Name	Descriptions
Wiegand Format	Its value can be 26 bits, 34 bits, 36 bits, 37 bits, 50 bits, and 64 bits.
Wiegand Bits	The number of bits of the Wiegand data.

Pulse Width (us)	The value of the pulse width sent by Wiegand is 100 microseconds by default, which can be adjusted within the range of 20 to 100 microseconds.
Pulse Interval (us)	The default value is 1000 microseconds and can be adjusted within the range of 200 to 20000 microseconds.
ID Type	Select between the User ID and card number.

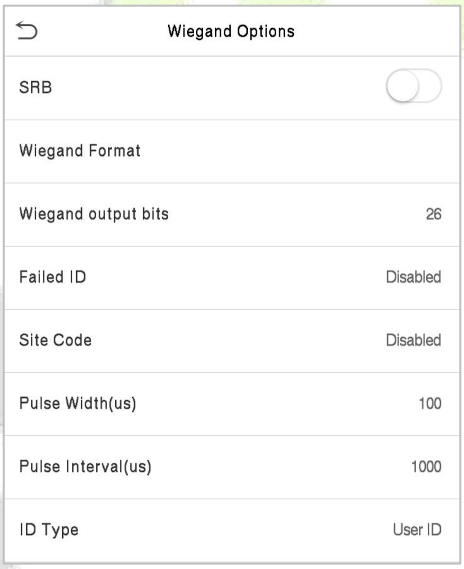
Various Common Wiegand Format Description

Wiegand Format	Description
Wiegand26	ECCCCCCCCCCCCCCCCCCCCCCCCO It consists of 26 bits of binary code. The 1st bit is the even parity bit of the 2nd to 13th bits, while the 26th bit is the odd parity bit of the 14th to 25th bits. The 2nd to 25th bits is the card numbers.
Wiegand26a	ESSSSSSSSCCCCCCCCCCCCCCCCO It consists of 26 bits of binary code. The 1st bit is the even parity bit of the 2nd to 13th bits, while the 26th bit is the odd parity bit of the 14th to 25th bits. The 2nd to 9th bits is the site codes, while the 10th to 25th bits are the card numbers.
Wiegand34	ECCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO It consists of 34 bits of binary code. The 1st bit is the even parity bit of the 2nd to 17th bits, while the 34th bit is the odd parity bit of the 18th to 33rd bits. The 2nd to 25th bits is the card numbers.
Wiegand34a	ESSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCO It consists of 34 bits of binary code. The 1st bit is the even parity bit of the 2nd to 17th bits, while the 34th bit is the odd parity bit of the 18th to 33rd bits. The 2nd to 9th bits is the site codes, while the 10th to 25th bits are the card numbers.
Wiegand36	OFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCMME 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	EFFFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCO 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	OMMMMSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCE 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	EMMMFFFFFFFFFFSSSSSSCCCCCCCCCCCCCCCCO 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	ESSSSSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO It consists of 50 bits of binary code. The 1st bit is the even parity bit of the 2nd to 25th bits, while the 50th bit is the odd parity bit of the 26th to 49th bits. The 2nd to 17th bits is the site codes, and the 18th to 49th bits are the card numbers.
Wiegand64	ECCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO It consists of 64 bits of binary code. The 1st bit is the even parity bit of the 2nd to 32nd bits, while the 64th bit is the odd parity bit of the 33rd to 63rd bits. The 2nd to 63rd bits are the card numbers.
"C" denotes the card number; **"E"** denotes the even parity bit; **"O"** denotes the odd parity bit; **"F"** denotes the facility code; **"M"** denotes the manufacturer code; **"P"** denotes the parity bit; and **"S"** denotes the site code.	

Note: This platform can support up to Wiegand66 bits format, when the device default A&C push, open the Wiegand customization function, connected to the software can be sent down through the software Wiegand66 format to the device.

6.6.2 Wiegand Output


Wiegand Options

SRB

Wiegand Format

Wiegand output bits 26

Failed ID Disabled

Site Code Disabled

Pulse Width(us) 100

Pulse Interval(us) 1000

ID Type User ID

Function Description

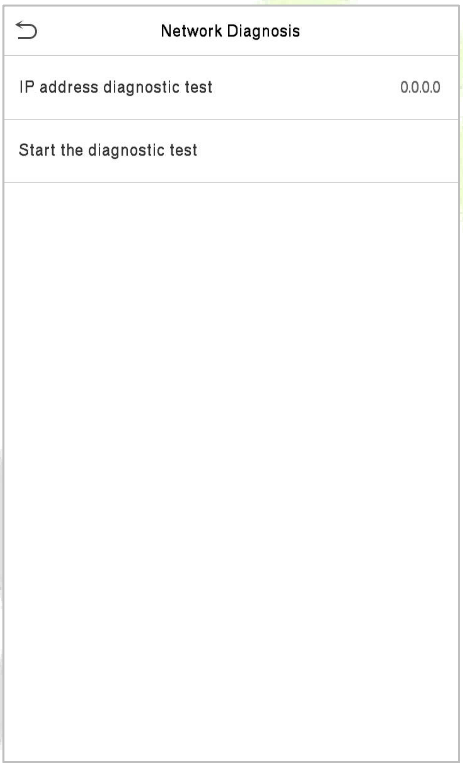
Function Name	Descriptions
SRB	When SRB is enabled, the lock is controlled by the SRB to prevent the lock from opening due to device removal.
Wiegand Format	Its value can be 26 bits, 34 bits, 36 bits, 37 bits, 50 bits, and 64 bits.
Wiegand Output Bits	After selecting the required Wiegand format, select the corresponding output bit digits of the Wiegand format.
Failed ID	If the verification fails, the system will send the failed ID to the device and replace the card number or personnel ID with the new one.

Site Code	It is similar to the device ID. The difference is that a site code can be set manually and is repeatable on a different device. The valid value ranges from 0 to 256 by default.
Pulse Width(us)	The time width represents the changes in the quantity of electric charge with regular high-frequency capacitance within a specified time.
Pulse Interval(us)	The time interval between pulses.
ID Type	Select the ID types as either User ID or card number.

6.7 Network Diagnosis

To set the network diagnosis parameters.

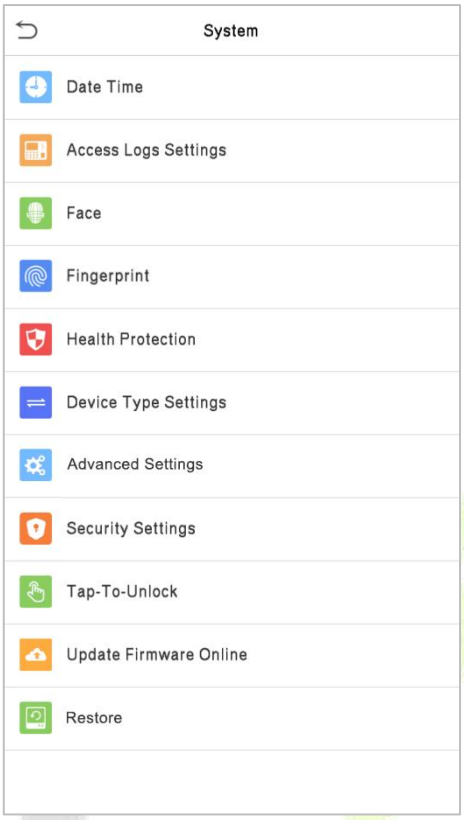
Click **Network Diagnosis** on the Comm. Settings interface. Enter the IP address that needs to be diagnosed, and click **Start the diagnostic test** to check whether the network can connect to the device.



7 System Settings

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

Tap **System** on the **Main Menu** interface to get into its menu options.



System

Date Time

Access Logs Settings

Face

Fingerprint

Health Protection

Device Type Settings

Advanced Settings

Security Settings

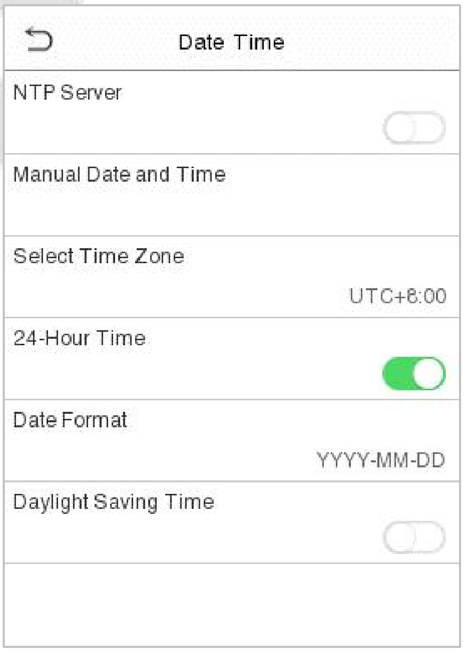
Tap-To-Unlock

Update Firmware Online

Restore

7.1 Date and Time

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



Date Time

NTP Server ○

Manual Date and Time

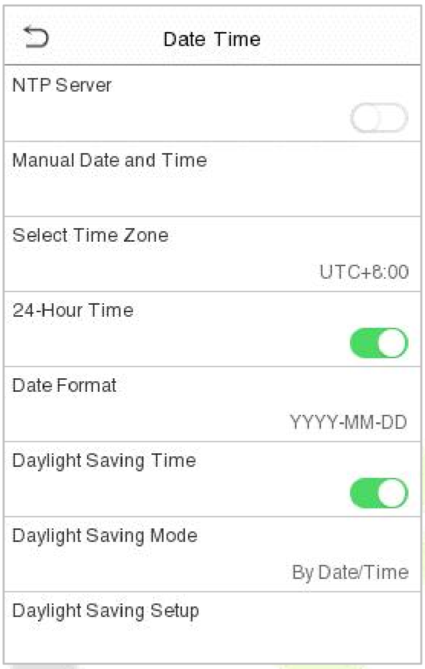
Select Time Zone UTC+8:00

24-Hour Time ●

Date Format YYYY-MM-DD

Daylight Saving Time ○

- 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.
- 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.
- Tap **24-Hour Time** to enable or disable this format. If enabled, then select the **Date Format** to set the date format.



Date Time

NTP Server ○

Manual Date and Time

Select Time Zone: UTC+8:00

24-Hour Time ●

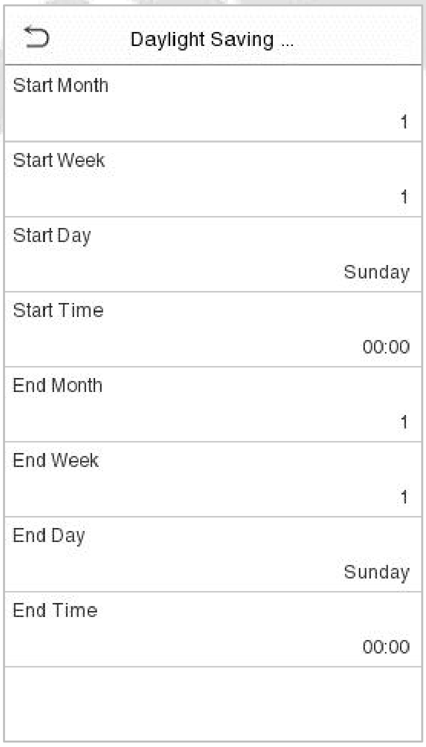
Date Format: YYYY-MM-DD

Daylight Saving Time ●

Daylight Saving Mode: By Date/Time

Daylight Saving Setup

- Tap **Daylight Saving Time** to enable or disable the function. If enabled, tap **Daylight Saving Mode** to select a daylight-saving mode and then tap **Daylight Saving Setup** to set the switch time.



Daylight Saving ...

Start Month: 1

Start Week: 1

Start Day: Sunday

Start Time: 00:00

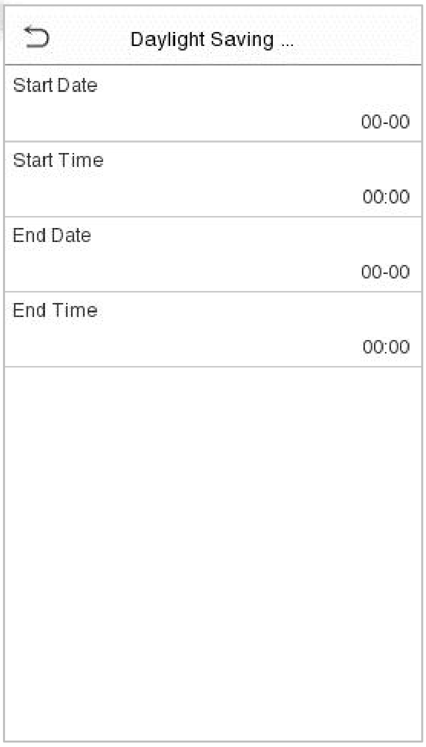
End Month: 1

End Week: 1

End Day: Sunday

End Time: 00:00

Week Mode



Daylight Saving ...

Start Date: 00-00

Start Time: 00:00

End Date: 00-00

End Time: 00:00

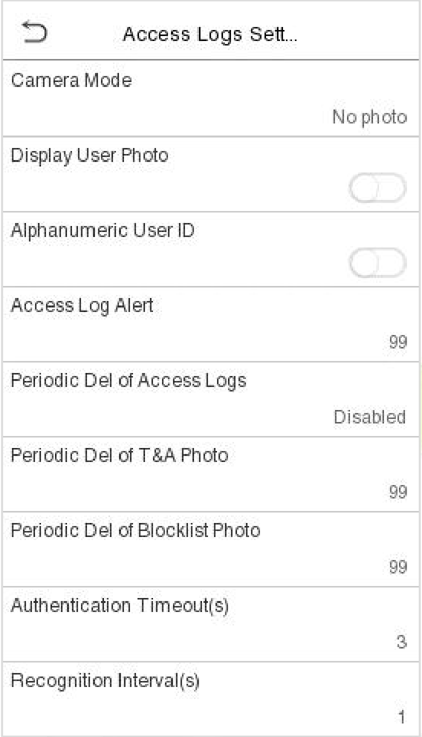
Date Mode

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

Note: *For example, the user sets the time of the device (18:35 on March 15, 2023) to 18:30 on January 1, 2024. After restoring the factory settings, the time of the equipment will remain 18:30 on January 1, 2024.*

7.2 Access Logs Settings/Attendance

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



Access Logs Sett...

Camera Mode: No photo

Display User Photo: ○

Alphanumeric User ID: ○

Access Log Alert: 99

Periodic Del of Access Logs: Disabled

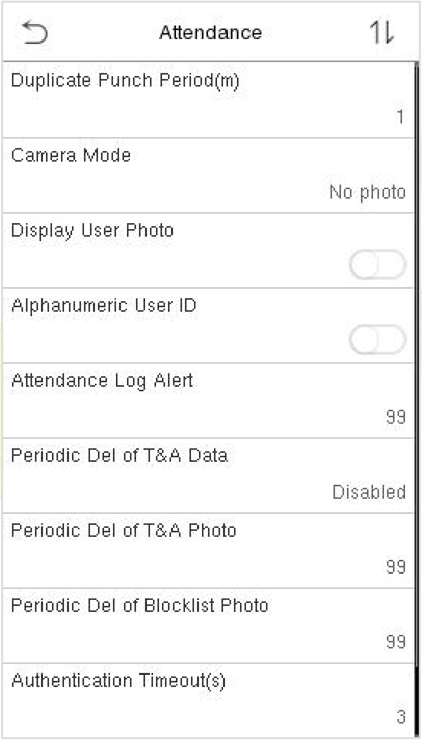
Periodic Del of T&A Photo: 99

Periodic Del of Blocklist Photo: 99

Authentication Timeout(s): 3

Recognition Interval(s): 1

A&C Terminal



Attendance

Duplicate Punch Period(m): 1

Camera Mode: No photo

Display User Photo: ○

Alphanumeric User ID: ○

Attendance Log Alert: 99

Periodic Del of T&A Data: Disabled

Periodic Del of T&A Photo: 99

Periodic Del of Blocklist Photo: 99

Authentication Timeout(s): 3

T&A Terminal

Function Description of A&C Terminal:

Function Name	Description
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 is not saved during verification. **Take photo and save:** Photo is taken and saved during verification. **Save on successful verification:** Photo is taken and saved for each successful verification. **Save on failed verification:** Photo will be taken and saved only for each failed verification.
Display User Photo	This function is disabled by default. When enabled, there will be a security prompt.
Alphanumeric User ID	Decides whether to support letters in a User ID.

Access Logs Alert	When the record space of the attendance access reaches the maximum threshold value, the device will automatically display the memory space warning. Users may disable the function or set a valid value between 1 and 9999.
Periodic Del of Access Logs	When access records have reached full capacity, the device will automatically delete a set of old access records. Users may disable the function or set a valid value between 1 and 999.
Periodic Del of T&A Photo	When attendance photos have reached full capacity, the device will automatically delete 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 have reached full capacity, the device will automatically delete 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 time length of the message of successful verification displays. Valid value: 1~9 seconds.
Recognition Interval (s)	To set the facial template matching time interval as required. Valid value: 0~9 seconds.

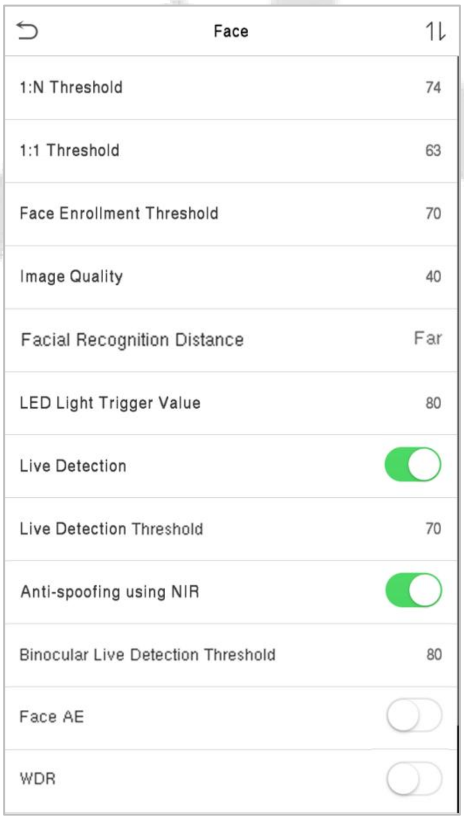
Function Description of T&A Terminal:

Function Name	Description
Duplicate Punch Period(m)	Within a set time period (unit: minutes), the duplicated attendance record will not be reserved (value ranges from 1 to 999999 minutes).
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	Whether to display the user photo when the user passes the verification.
Alphanumeric User ID	Enable/Disable the alphanumeric as User ID.
Attendance Log Alert	When the record space of the attendance reaches the maximum threshold value, the device automatically displays the memory space warning. Users may disable the function or set a valid value between 1 and 9999.

Periodic Del of T&A Data	When attendance records reach its maximum storage capacity, the device automatically deletes a set of old attendance records. Users may disable the function or set a valid value between 1 and 999.
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.
Recognition Interval(s)	After the interval identifying is clicked (selected), for example, if the comparison 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.

7.3 Face Template Parameters

Tap **Face** on the **System** interface to go to the face template parameter settings.



Face

1:N Threshold 74

1:1 Threshold 63

Face Enrollment Threshold 70

Image Quality 40

Facial Recognition Distance Far

LED Light Trigger Value 80

Live Detection ●

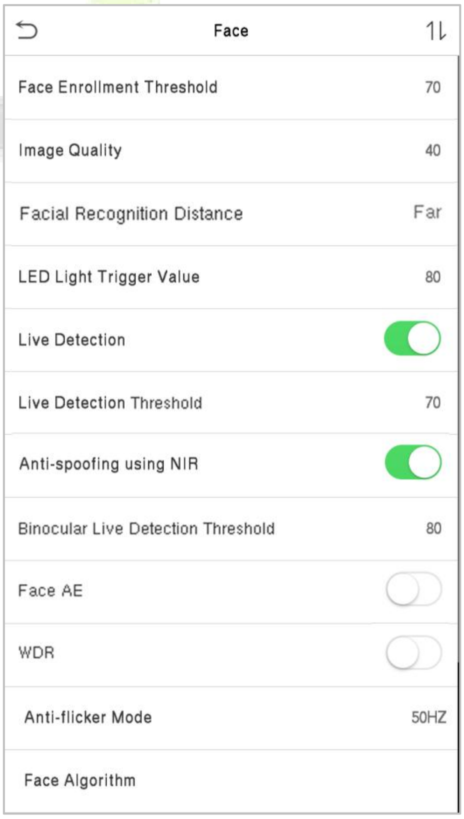
Live Detection Threshold 70

Anti-spoofing using NIR ●

Binocular Live Detection Threshold 80

Face AE ○

WDR ○



Face

Face Enrollment Threshold 70

Image Quality 40

Facial Recognition Distance Far

LED Light Trigger Value 80

Live Detection ●

Live Detection Threshold 70

Anti-spoofing using NIR ●

Binocular Live Detection Threshold 80

Face AE ○

WDR ○

Anti-flicker Mode 50HZ

Face Algorithm

FRR	FAR	Recommended Matching Thresholds	
		1:N	1:1
High	Low	85	80
Medium	Medium	82	75
Low	High	80	70

Function Description

Function Name	Description
1:N Threshold	Under 1:N verification mode, the verification will only be successful when the similarity between the acquired facial image and all registered facial templates is greater than the set value. The valid value ranges from 65 to 120. The higher the thresholds, the lower the misjudgement rate and the higher the rejection rate, and vice versa. It is recommended to set the default value of 75.
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 55 to 120. The higher the thresholds, the lower the misjudgement rate and the higher the rejection rate, and vice versa. It is recommended to set the default value of 63.
Face Enrollment Threshold	During face enrollment, 1:N comparison is used to determine whether the user has already registered before. When the similarity between the acquired facial image and all registered facial templates is greater than the set threshold, it indicates that the face has already been registered.
Image Quality	It is the image quality for facial registration and comparison. The higher the value, the clearer image is required.
Facial Recognition 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 distance of faces.
LED Light Trigger Threshold	This value controls the turning on and off of the LED light. The larger the value, the LED light will turn on or off more frequently.
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.
Live Detection Threshold	It facilitates judging whether the captured visible image is a real person (a live human being). The larger the value, the better the anti-spoofing performance using visible light.
Anti-spoofing Using NIR	Using near-infrared spectra imaging to identify and prevent fake photos and videos attack.

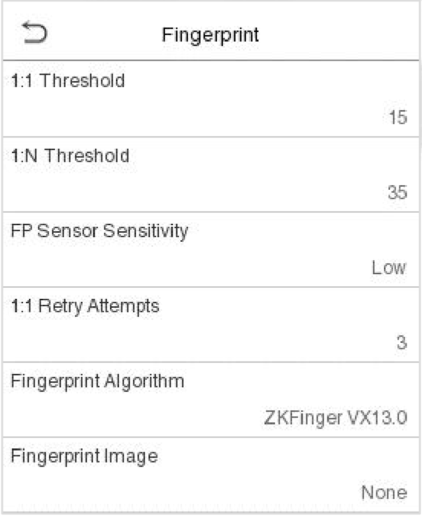
Binocular Live Detection Threshold	It is convenient to judge whether the near-infrared spectral imaging is fake photo and video. The larger the value, the better the anti-spoofing performance of near-infrared spectral imaging.
Face AE	When the face is in front of the camera in Face AE mode, the brightness 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	Used when WDR is turned off. This helps reduce flicker when the device's screen flashes at the same frequency as the light.
Face Algorithm	Facial algorithm related information and pause facial template update.

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

- **Process to modify the Face Recognition Accuracy**
- On the **System** interface, tap on **Face** and then toggle to enable Anti-Spoofing using NIR to set the anti-spoofing.
- Then, on the **Main Menu**, tap **Auto-Test > Test Face** and perform the face test.
- Tap three times for the scores on the right 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.

7.4 Fingerprint Parameters

Tap **Fingerprint** on the System interface.



1:1 Threshold: 15
1:N Threshold: 35
FP Sensor Sensitivity: Low
1:1 Retry Attempts: 3
Fingerprint Algorithm: ZKFinger VX13.0
Fingerprint Image: None

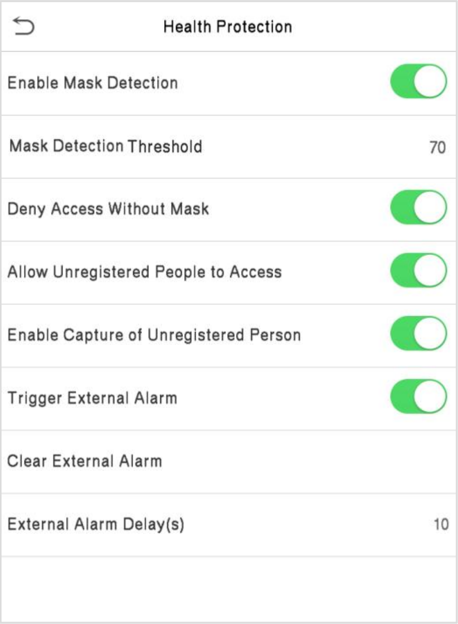
FRR	FAR	Recommended matching thresholds	
		1:N	1:1
High	Low	45	25
Medium	Medium	35	15
Low	High	25	10

Function Description

Function Name	Descriptions
1:1 Threshold	Under 1:1 verification method, the verification will only be successful when the similarity between the acquired fingerprint data and the fingerprint template associated with the entered user ID enrolled in the device is greater than the set value.
1:N Threshold	Under 1:N verification method, the verification will only be successful when the similarity between the acquired fingerprint data and the fingerprint templates enrolled in the device is greater than the set value.
FP Sensor Sensitivity	To set the sensibility of fingerprint acquisition. It is recommended to use the default level "**Medium**". When the environment is dry, resulting in slow fingerprint detection, you can set the level to "**High**" to raise the sensibility; when the environment is humid, making it hard to identify the fingerprint, you can set the level to "**Low**".
1:1 Retry Attempts	In 1:1 Verification, users might forget the registered fingerprint, or press the finger improperly. To reduce the process of re-entering user ID, retry is allowed.
Fingerprint Algorithm	Fingerprint algorithm version. Default support ZKFinger VX13.0, can change to ZKFinger VX10.0. Switching fingerprint algorithms will clear the data.
Fingerprint Image	This function is disabled by default. After disabling it, the fingerprint image will not be displayed when registering and verifying fingerprints. The menu interface allows to enable or disable this function, and there are security prompts when switching. Four choices are available: **Show for enroll**: to display the fingerprint image on the screen only during enrollment. **Show for match**: to display the fingerprint image on the screen only during verification. **Always show**: to display the fingerprint image on screen during enrollment and verification. **None**: not to display the fingerprint image.

7.5 Health Protection

Tap **Health Protection** on the System interface to configure the health protection settings.



Health Protection

Enable Mask Detection: on

Mask Detection Threshold: 70

Deny Access Without Mask: on

Allow Unregistered People to Access: on

Enable Capture of Unregistered Person: on

Trigger External Alarm: on

Clear External Alarm

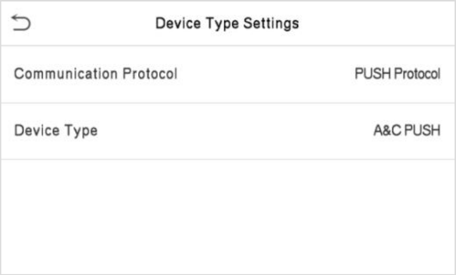
External Alarm Delay(s): 10

Function Description

Function Name	Descriptions
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.
Mask Detection Threshold	Sets the mask detection threshold. Valid values are 0 to 100.
Deny Access Without Mask	It enables or disables the access of a person without a 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 an 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 between 1 to 255.

7.6 Device Type Settings

Tap **Device Type Settings** on the System interface to set the Device Type.


Device Type Settings

Communication Protocol PUSH Protocol

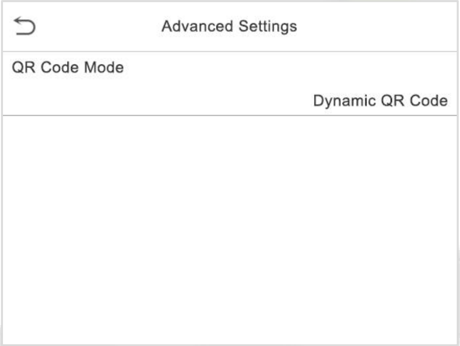
Device Type A&C PUSH

Function Description

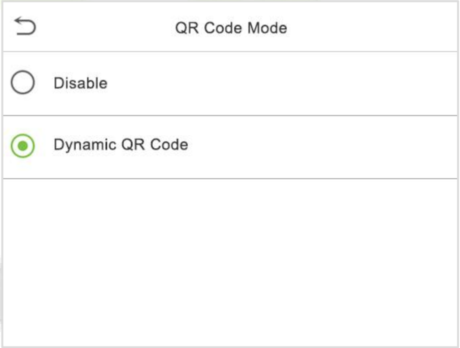
Function Name	Descriptions
Communication Protocol	Set the device communication protocol, PUSH Protocol or BEST Protocol. (BEST protocol is suitable for ZKBio Zlink, please refer to 17 Connecting to ZKBio Zlink App and 18 Connecting to ZKBio Zlink Web.)
Device Type	Set the device as an access control terminal or attendance terminal.

7.7 Advanced Settings★

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


Advanced Settings

QR Code Mode Dynamic QR Code


QR Code Mode

○ Disable

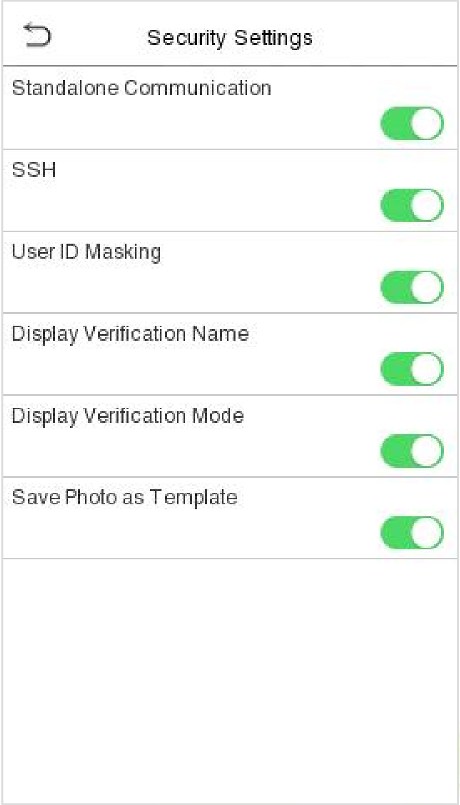
● Dynamic QR Code

Function Description

Function Name	Descriptions
QR Code Mode	**Disable:** Disable the dynamic QR code function. **Dynamic QR Code:** To enable the dynamic QR code function. And you need to use the ZKBio CVAccess software to connect the device and perform the corresponding operation to support the QR code function.

7.8 Security Settings

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



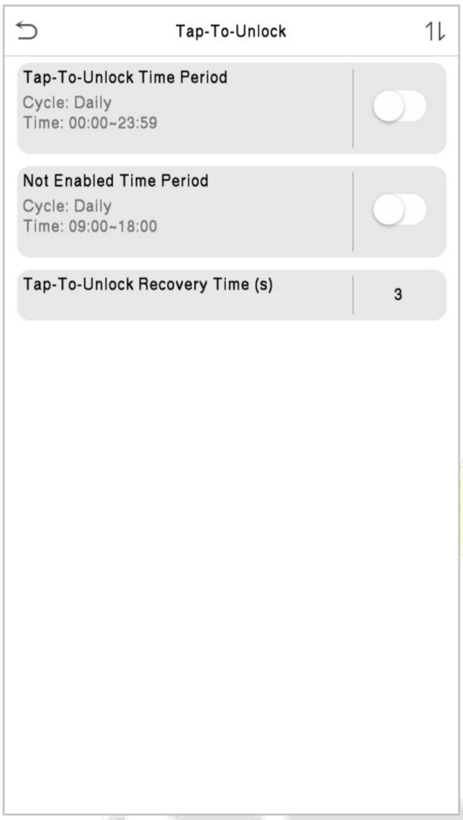
Function Description

Function Name	Description
Standalone Communication	By default, this function is disabled. It is used to connect the C/S software (like ZKTime.Net, etc.). When it is switched on, a security prompt appears, and you need to set the Comm Key, 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 disable this function, face re-registration is required after an algorithm upgrade.

7.9 Tap-To-Unlock

Enable **Tap-To-Unlock**, and it will take effect after the device restarts. Once enabled, the camera's auto-identification sensing function will be disabled. Only touching the device screen can wake up the camera for auto-identification.

Tap **Tap-To-Unlock** on the **System** interface to enable this function.

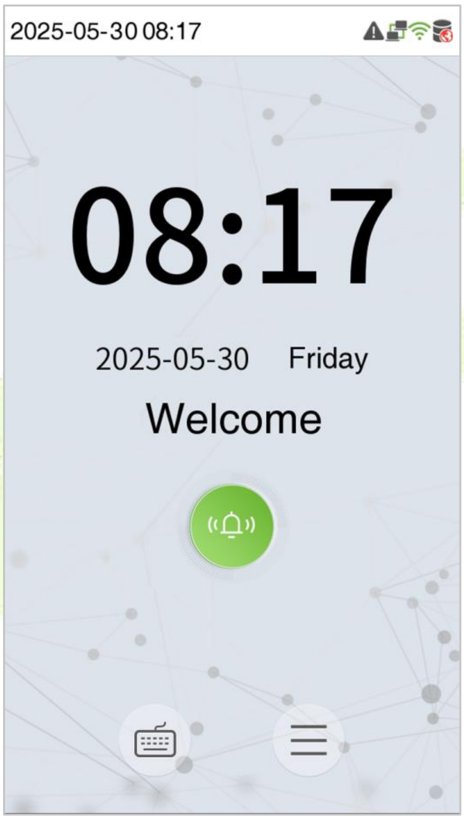


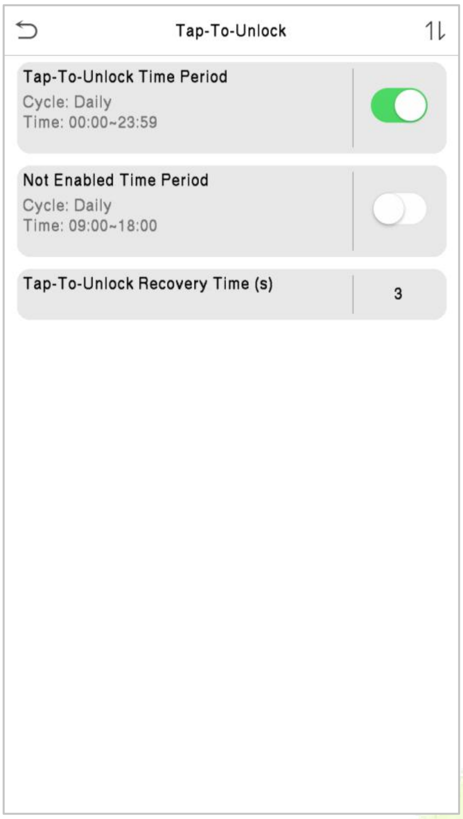
Tap-To-Unlock

Tap-To-Unlock Time Period
Cycle: Daily
Time: 00:00~23:59

Not Enabled Time Period
Cycle: Daily
Time: 09:00~18:00

Tap-To-Unlock Recovery Time (s) 3



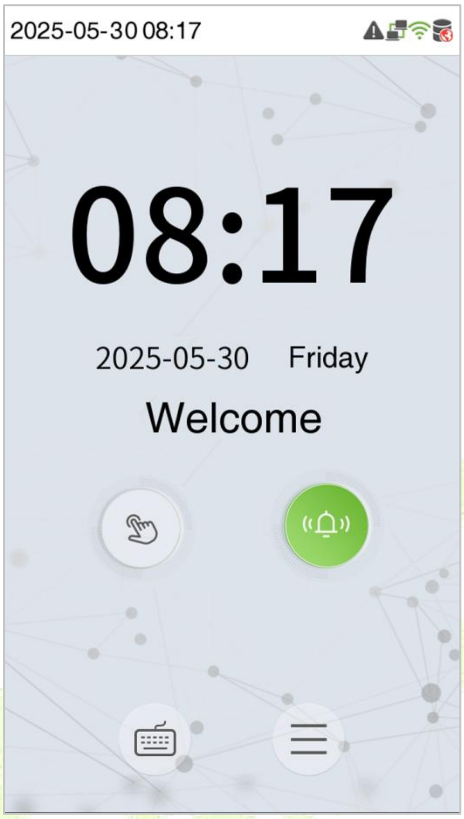


Tap-To-Unlock

Tap-To-Unlock Time Period
Cycle: Daily
Time: 00:00~23:59

Not Enabled Time Period
Cycle: Daily
Time: 09:00~18:00

Tap-To-Unlock Recovery Time (s): 3



2025-05-30 08:17

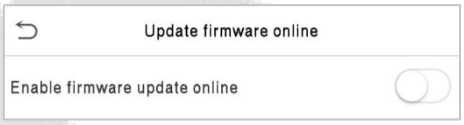
08:17

2025-05-30 Friday

Welcome

7.10 Update Firmware Online

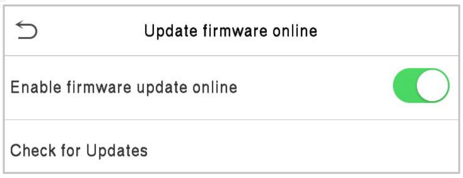
Tap **Update Firmware Online** on the **System** interface.



Update firmware online

Enable firmware update online

Tap **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).



Update firmware online

Enable firmware update online

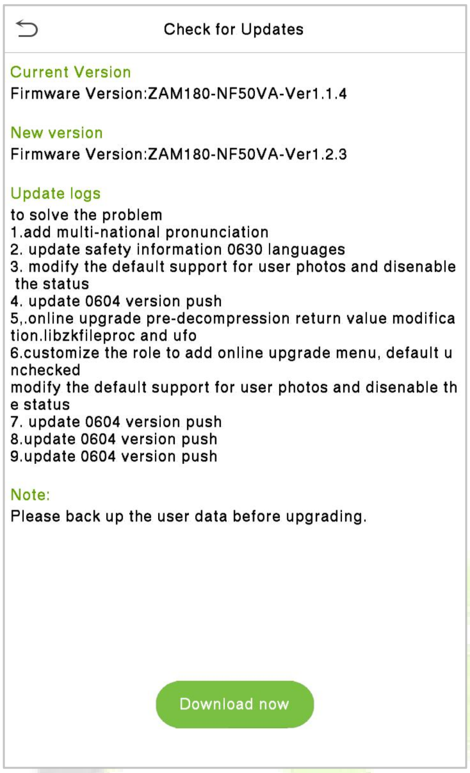
Check for Updates

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

- If the query fails, the interface will prompt "Query failed".
- If the firmware version of the device is latest, it will prompt that the current firmware version is already the latest.
- If the firmware version of the device is not the latest, the version number and change log of the latest

version will be displayed. Users can choose whether to update to the latest firmware version.

1. Tap **Download now** to start the download. After the download is complete, you can choose whether to update immediately.



Check for Updates

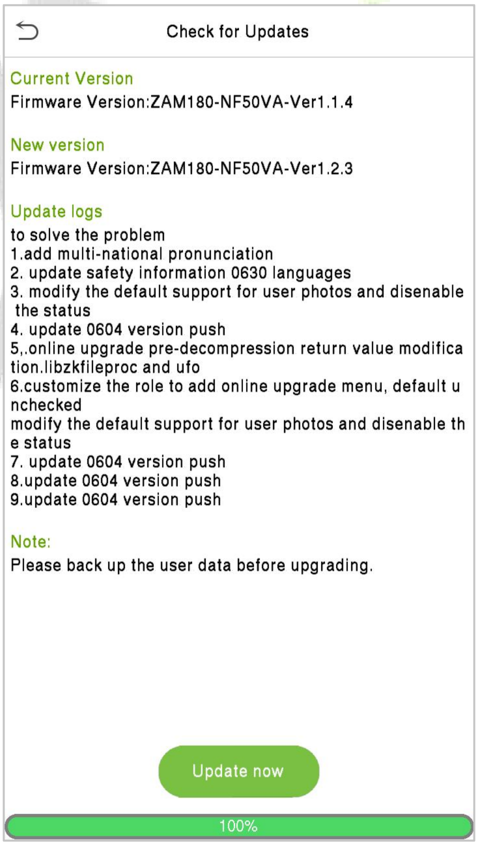
Current Version
Firmware Version:ZAM180-NF50VA-Ver1.1.4

New version
Firmware Version:ZAM180-NF50VA-Ver1.2.3

Update logs
to solve the problem
1.add multi-national pronunciation
2. update safety information 0630 languages
3. modify the default support for user photos and disenable the status
4. update 0604 version push
5,.online upgrade pre-decompression return value modification.libzkfileproc and ufo
6.customize the role to add online upgrade menu, default unchecked
modify the default support for user photos and disenable the status
7. update 0604 version push
8.update 0604 version push
9.update 0604 version push

Note:
Please back up the user data before upgrading.

2. During the download process, you can press the back button to go to other menus, and then return to this menu to update after the download is complete.



Check for Updates

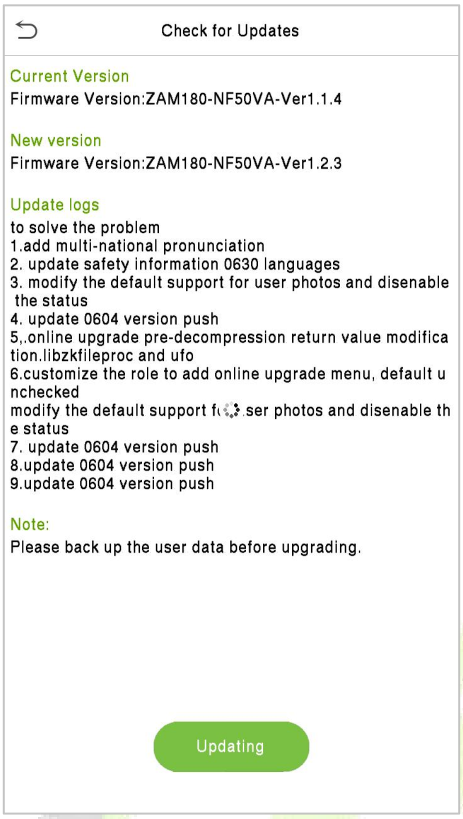
Current Version
Firmware Version:ZAM180-NF50VA-Ver1.1.4

New version
Firmware Version:ZAM180-NF50VA-Ver1.2.3

Update logs
to solve the problem
1.add multi-national pronunciation
2. update safety information 0630 languages
3. modify the default support for user photos and disenable the status
4. update 0604 version push
5,.online upgrade pre-decompression return value modification.libzkfileproc and ufo
6.customize the role to add online upgrade menu, default unchecked
modify the default support for user photos and disenable the status
7. update 0604 version push
8.update 0604 version push
9.update 0604 version push

Note:
Please back up the user data before upgrading.

3. The download speed is related to the user's network environment, and it may take about 10 minutes to complete the download. The update may take about 3 minutes.



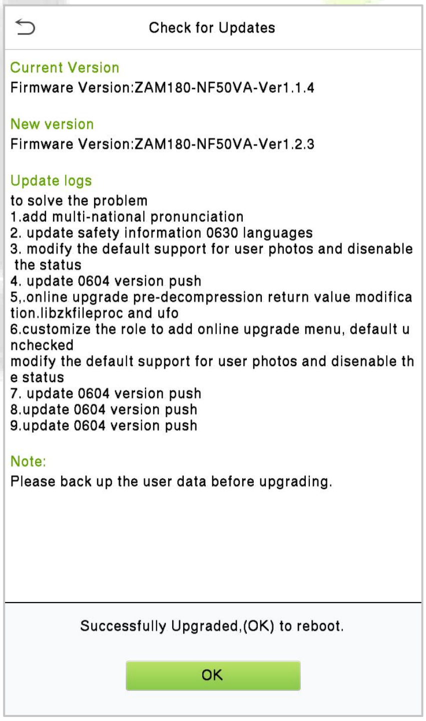
Current Version
Firmware Version:ZAM180-NF50VA-Ver1.1.4

New version
Firmware Version:ZAM180-NF50VA-Ver1.2.3

Update logs
to solve the problem
1.add multi-national pronunciation
2. update safety information 0630 languages
3. modify the default support for user photos and disenable the status
4. update 0604 version push
5,.online upgrade pre-decompression return value modification.libzkfileproc and ufo
6.customize the role to add online upgrade menu, default unchecked
modify the default support f ser photos and disenable the status
7. update 0604 version push
8.update 0604 version push
9.update 0604 version push

Note:
Please back up the user data before upgrading.

4. After the update is complete, the device will prompt to restart. After restarting, you can enter the **System Information** to view the latest firmware version after the update.



Current Version
Firmware Version:ZAM180-NF50VA-Ver1.1.4

New version
Firmware Version:ZAM180-NF50VA-Ver1.2.3

Update logs
to solve the problem
1.add multi-national pronunciation
2. update safety information 0630 languages
3. modify the default support for user photos and disenable the status
4. update 0604 version push
5,.online upgrade pre-decompression return value modification.libzkfileproc and ufo
6.customize the role to add online upgrade menu, default unchecked
modify the default support for user photos and disenable the status
7. update 0604 version push
8.update 0604 version push
9.update 0604 version push

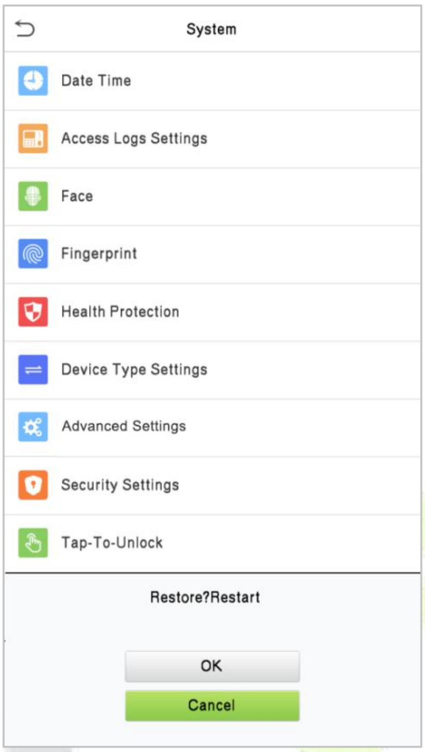
Note:
Please back up the user data before upgrading.

Successfully Upgraded,(OK) to reboot.

7.11 Factory Reset

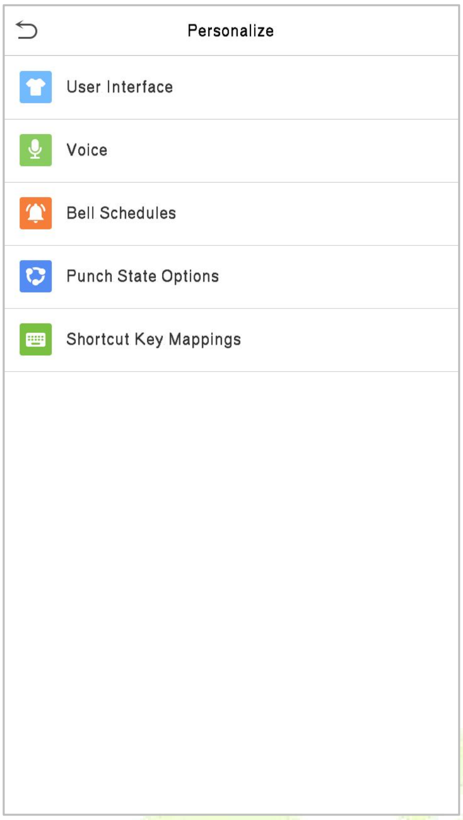
The Factory Reset function restores the device settings such as communication settings and system settings, to the default factory settings (this function does not clear registered user data).

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



8 Personalize Settings

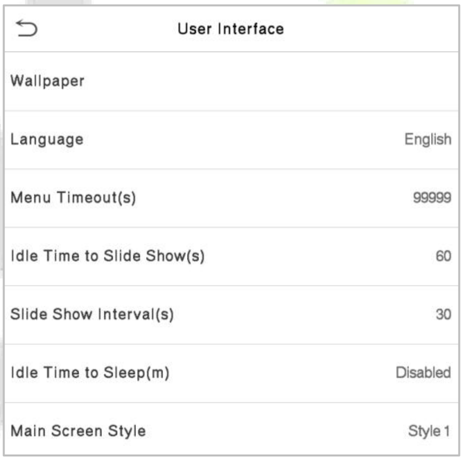
Tap **Personalize** on the **Main Menu** interface to customize interface settings, voice, bell, punch state options, and shortcut key mappings.



Personalize

8.1 Interface Settings

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



User Interface

Wallpaper

Language English

Menu Timeout(s) 99999

Idle Time to Slide Show(s) 60

Slide Show Interval(s) 30

Idle Time to Sleep(m) Disabled

Main Screen Style Style 1

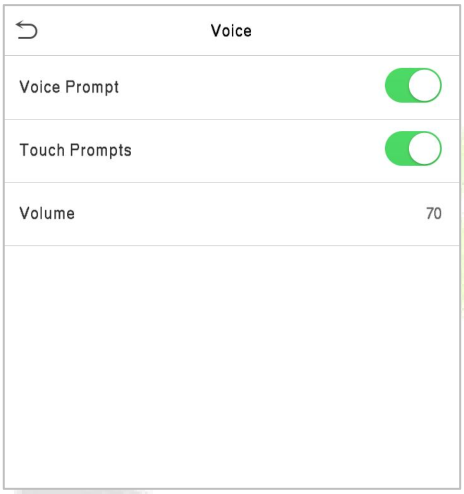
Function Description

Function Name	Description
Wallpaper	It helps to select the main screen wallpaper according to the user preference.
Language	It helps to select the language of the device.
Menu Timeout (s)	When there is no operation, and the time exceeds the set value, the device automatically goes back to the initial interface. The function can either be disabled or set the required value between 60 and 99999 seconds.
Idle Time To	When there is no operation, and the time exceeds the set value, a slide show is

Slide Show (s)	displayed. The function can be disabled, or you may set the value between 3 and 999 seconds.
Slide Show Interval (s)	It is the time interval in switching between different slide show pictures. The function can be disabled, or you may set the interval between 3 and 999 seconds.
Idle Time To Sleep (m)	If the sleep mode is activated, and when there is no operation in the device, then the device will enter standby mode. This function can be disabled or set a value within 1-999 minutes.
Main Screen Style	The style of the main screen can be selected according to the user preference.

8.2 Voice Settings

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


Voice

Voice Prompt: on

Touch Prompts: on

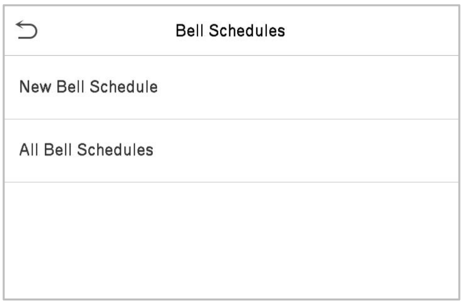
Volume: 70

Function Description

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

8.3 Bell Schedules

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

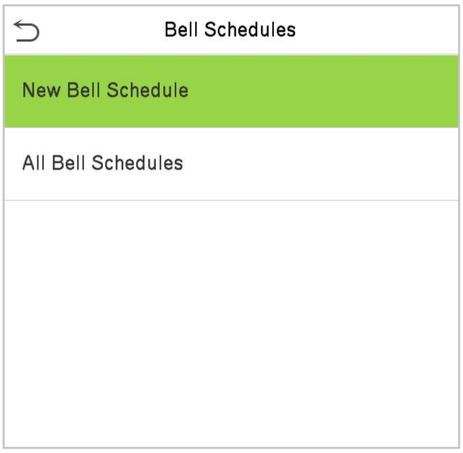

Bell Schedules

New Bell Schedule

All Bell Schedules

- **New Bell Schedule**

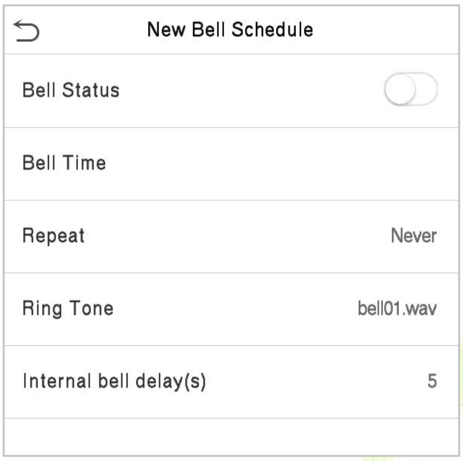
Tap **New Bell Schedule** on the **Bell Schedule** interface to add a new bell schedule.



Bell Schedules

New Bell Schedule

All Bell Schedules



New Bell Schedule

Bell Status

Bell Time

Repeat Never

Ring Tone bell01.wav

Internal bell delay(s) 5

Function Description

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

- **All Bell Schedules**

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

- **Edit the Scheduled Bell**

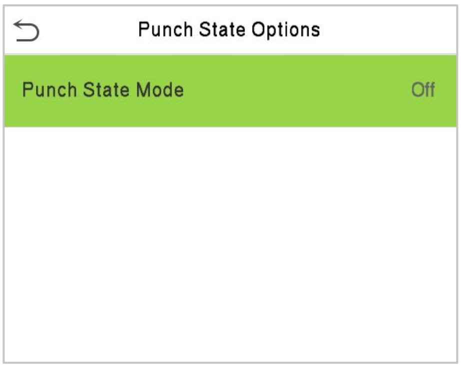
On the **All Bell Schedules** interface, tap on the required bell schedule, and tap **Edit** to edit the selected bell schedule. The editing method is the same as the operations of adding a new bell schedule.

- **Delete a Bell**

On the **All Bell Schedules** interface, tap the required bell schedule, and tap **Delete**, and then tap **Yes** to delete the selected bell.

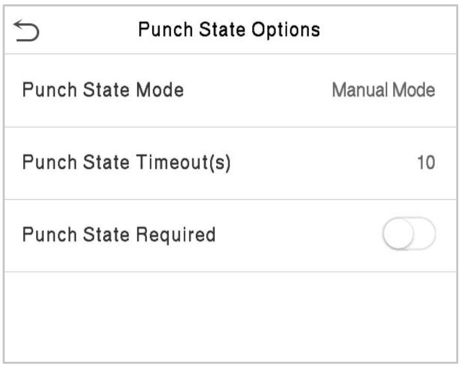
8.4 Punch States Options

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



Punch State Options

Punch State Mode	Off



Punch State Options

Punch State Mode	Manual Mode
Punch State Timeout(s)	10
Punch State Required	○

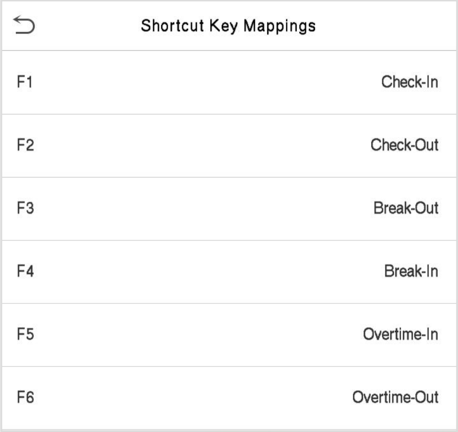
Function Description

Function Name	Description
Punch State Mode	Select a punch state mode, which can be: **Off:** It disables the punch state function. And the punch state key set under the **Shortcut Key Mappings** menu becomes invalid. **Manual Mode:** Switch the punch state key manually, and the punch state key will disappear after **Punch State Timeout**. **Auto Mode:** The punch state key will automatically switch to a specific punch status according to the predefined schedule which can be set in the Shortcut Key Mappings. **Manual and Auto Mode:** The main interface will display the auto-switch punch state key. However, the users will still be able to select an alternative that is the manual attendance status. After the timeout, the manual switching punch state key will become an auto-switch punch state key. **Manual Fixed Mode:** After the punch state key is set manually to a particular punch status, the function will remain unchanged until manually switched again. **Fixed Mode:** Only the manually fixed punch state key is shown. Users cannot change the status by pressing any other keys.
Punch State Timeout (s)	It is the amount of time for which the punch state is displayed. The value ranges from 5~999 seconds.
Punch State Required	To choose whether an attendance state needs to be selected during verification.

8.5 Shortcut Keys Mappings

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

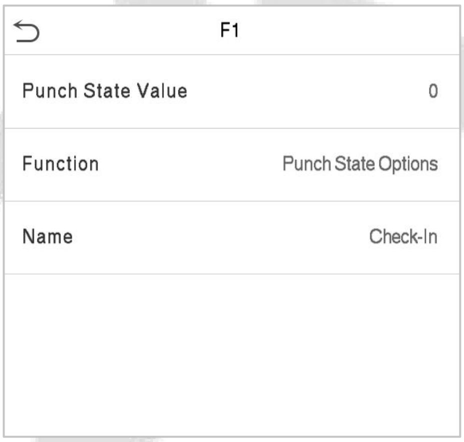
Tap **Shortcut Key Mappings** on the **Personalize** interface to set the required shortcut keys.



Shortcut Key Mappings

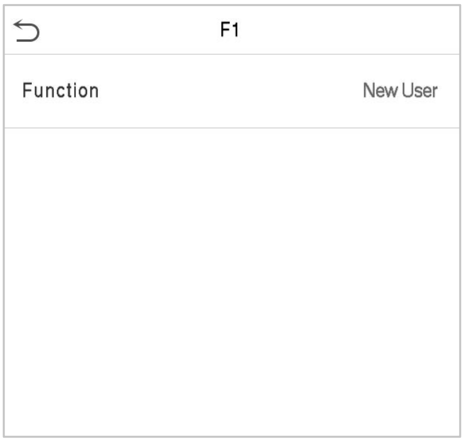
F1	Check-In
F2	Check-Out
F3	Break-Out
F4	Break-In
F5	Overtime-In
F6	Overtime-Out

- On the **Shortcut Key Mappings** interface, tap on the required shortcut key to configure the shortcut key settings.
- On the **Shortcut Key** ("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 done as shown in the image below.



F1

Punch State Value	0
Function	Punch State Options
Name	Check-In



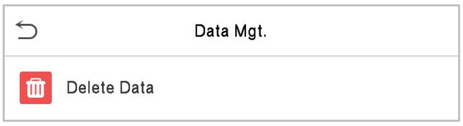
F1

Function	New User

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

9 Data Management

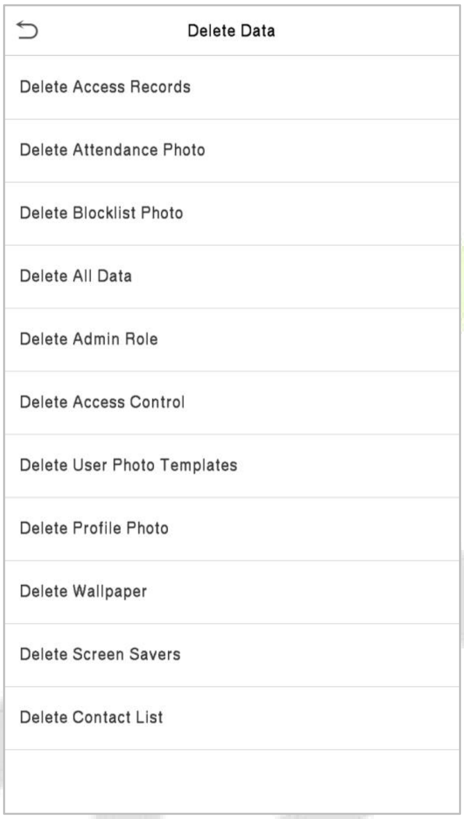
On the **Main Menu**, tap **Data Mgt.** to delete the relevant data in the device.



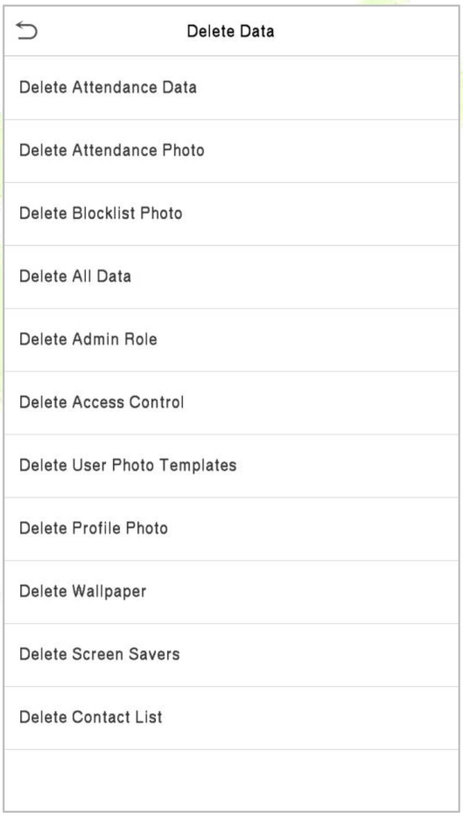
9.1 Delete Data

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

Access Control Terminal:



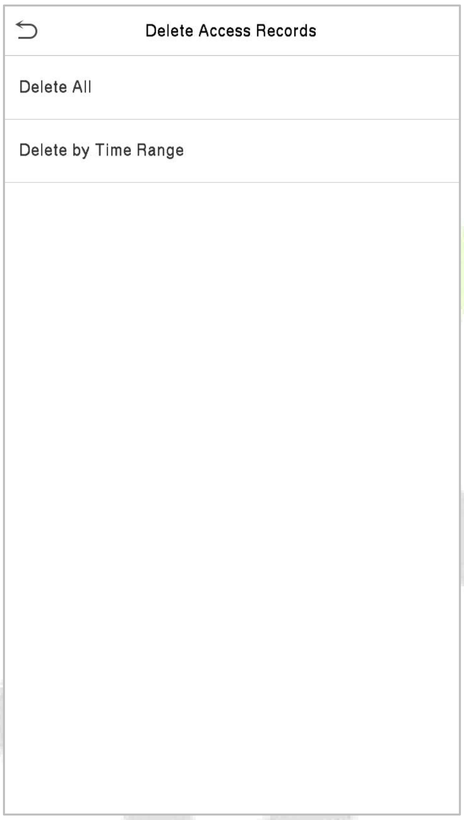
Time Attendance Terminal:



Function Name	Description
Delete Access Records / Delete 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 in 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 the contact list in the device.

The user may select **Delete All** or **Delete by Time Range** when deleting the attendance data/access records, 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.

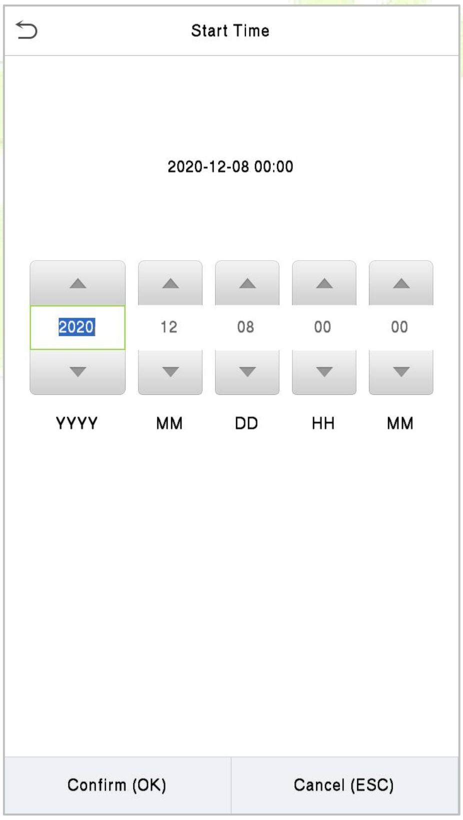


Delete Access Records

Delete All

Delete by Time Range

Select Delete by Time Range



Start Time

2020-12-08 00:00

YYYY	MM	DD	HH	MM
2020	12	08	00	00

Set the time range and tap **OK**

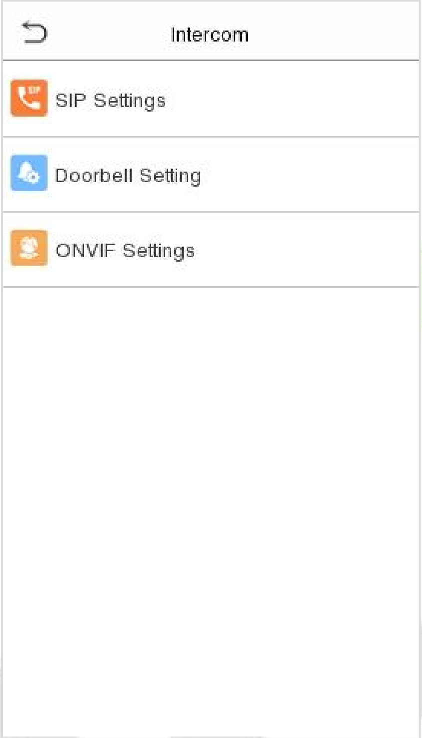
10 Intercom

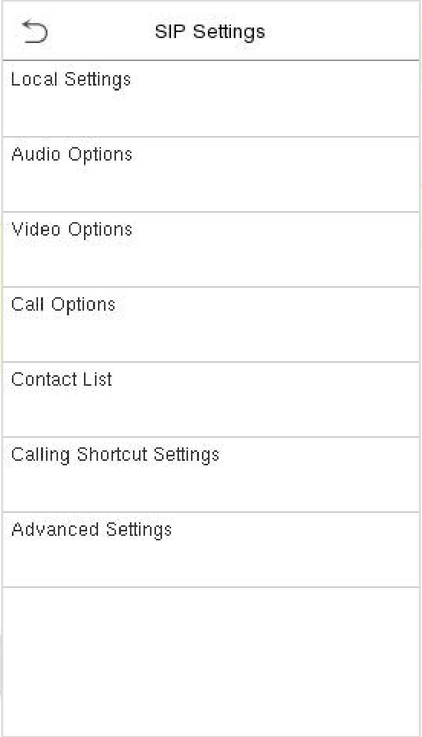
On the **Main Menu**, tap **Intercom** to set relevant parameters of intercom, including SIP, Doorbell and ONVIF Settings.

The device achieves video intercom there are two modes, respectively, the LAN and SIP server. For more details, please refer to 17 SIP Video Intercom.

10.1 SIP Settings

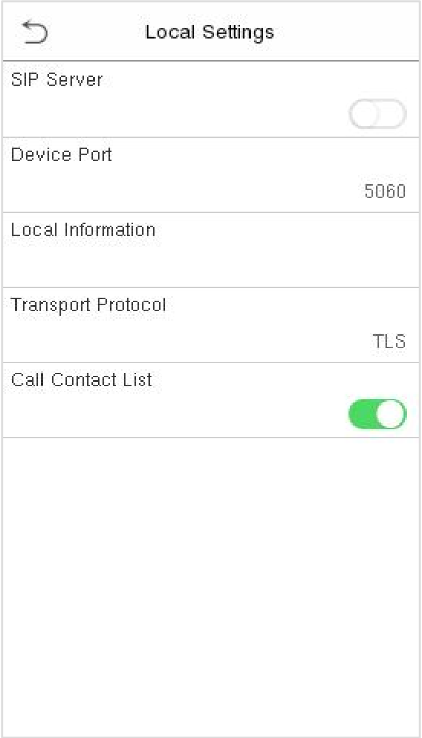
Tap **SIP Settings** on the **Intercom** interface to configure the settings.





10.1.1 Local Settings

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



Local Settings

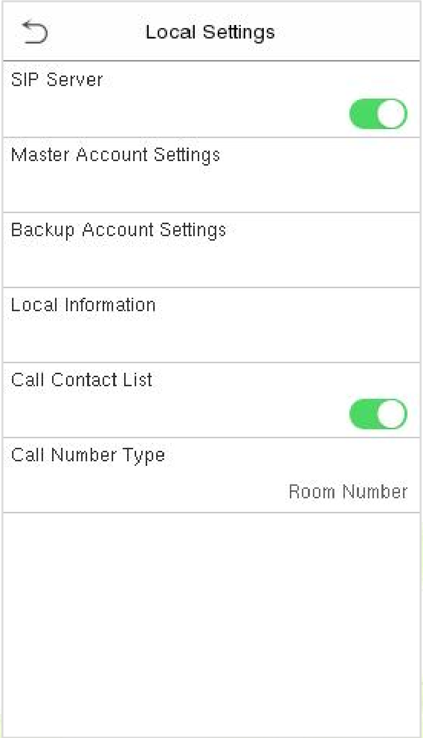
SIP Server ○

Device Port 5060

Local Information

Transport Protocol TLS

Call Contact List ●



Local Settings

SIP Server ●

Master Account Settings

Backup Account Settings

Local Information

Call Contact List ●

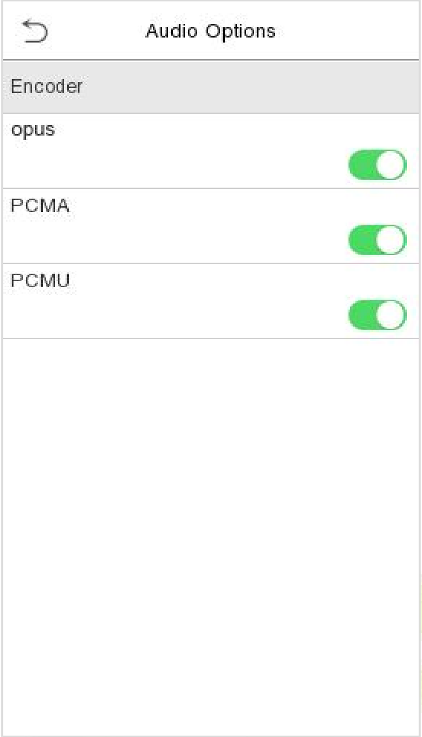
Call Number Type Room Number

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.
Device Port	When using a local area network for intercom, enter the device port number.
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.

10.1.2 Audio Options

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



Audio Options

Encoder

opus ●

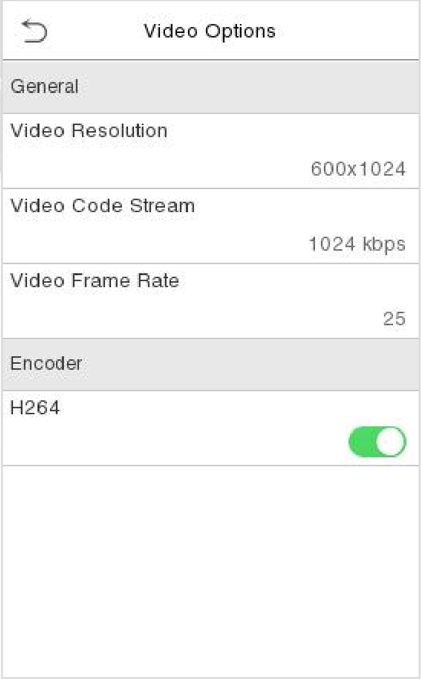
PCMA ●

PCMU ●

Select the audio encoder for intercom. Opus, PCMU and PCMA all provide better voice quality, but take up more bandwidth, requiring 64kbps of bandwidth.

10.1.3 Video Options

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



Video Options

General

Video Resolution 600x1024

Video Code Stream 1024 kbps

Video Frame Rate 25

Encoder

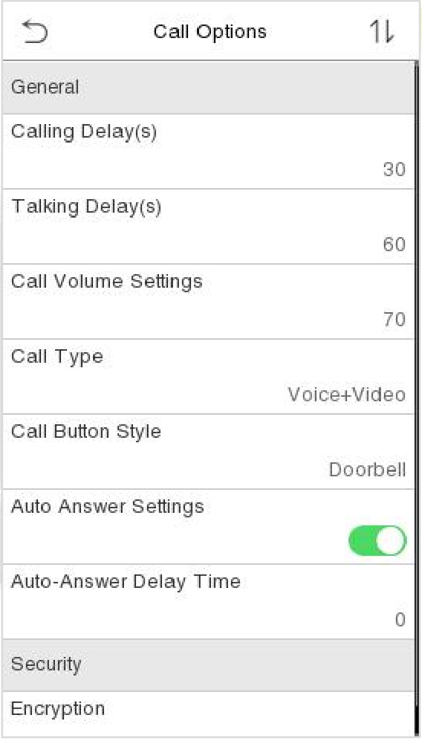
H264 ●

Function Description

Function Name	Description
Video Resolution	Select the video resolution of the intercom, 1024 x 576 (for landscape screen) or 600 x 1024 (for portrait screen). The device is suggested to set as 600 x 1024.
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.

10.1.4 Call Options

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



Calling Delay(s): 30

Talking Delay(s): 60

Call Volume Settings: 70

Call Type: Voice+Video

Call Button Style: Doorbell

Auto Answer Settings

Auto-Answer Delay Time: 0

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.

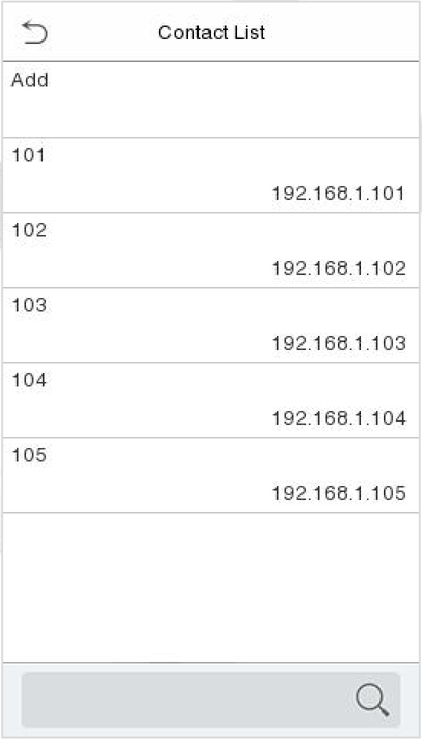
Call Volume Settings	Set the volume of the call, with valid value ranging from 0 to 100.
Call Type	Set the call type to Voice only or Voice+Video.
Call Button Style	Change the visual intercom call button on the standby interface of the device, optional doorbell label 🔔 or phone label ☎.
Auto Answer Settings	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.

10.1.5 Contact List

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

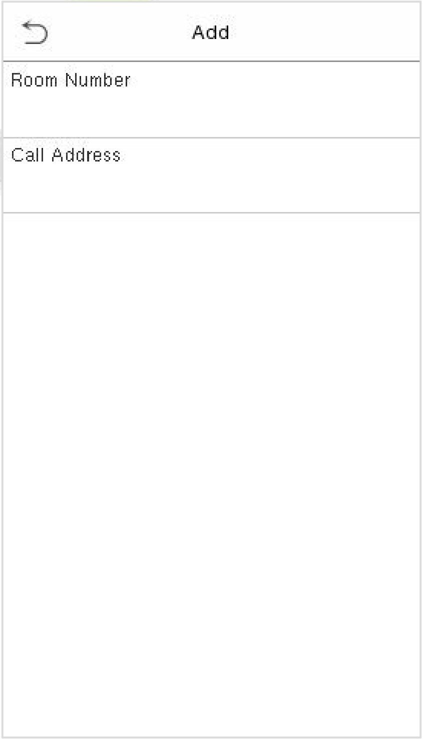
In SIP Server mode, the contact list is synchronized by the ZKBio CVAccess Server to the device. The contact list can only be viewed, cannot be edited. When the SIP server is disabled, the room number and call address of the indoor monitors can be added here.

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


Contact List

Add

101	192.168.1.101
102	192.168.1.102
103	192.168.1.103
104	192.168.1.104
105	192.168.1.105

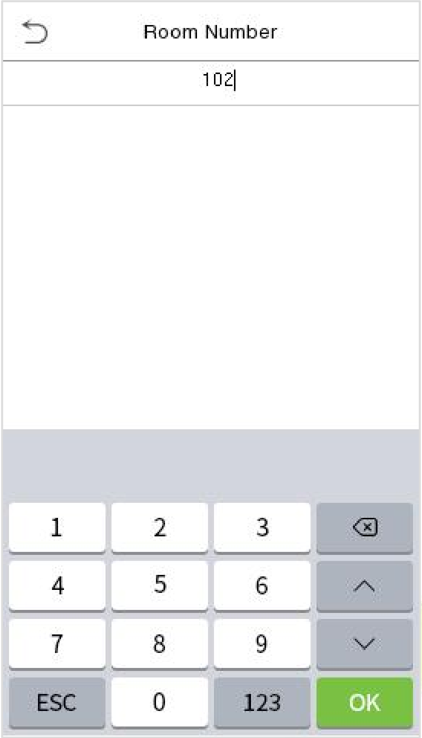

Add

Room Number

Call Address

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

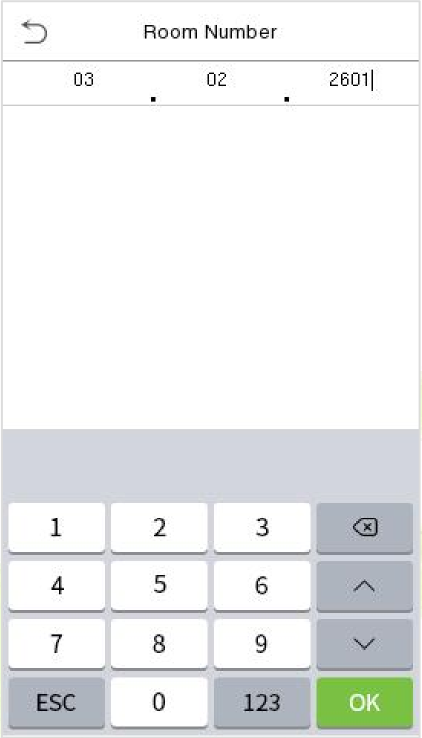
When the device type is set as **Entrance Station**, the room number can be 1~ 4 digits. When the device type is set as **Fence Terminal**, you need to input the block, unit and room number. For example, if the indoor monitor is in Block 3, Unit 2, Room 2601, then input “03.02.2601”.



Room Number

102

Entrance Station



Room Number

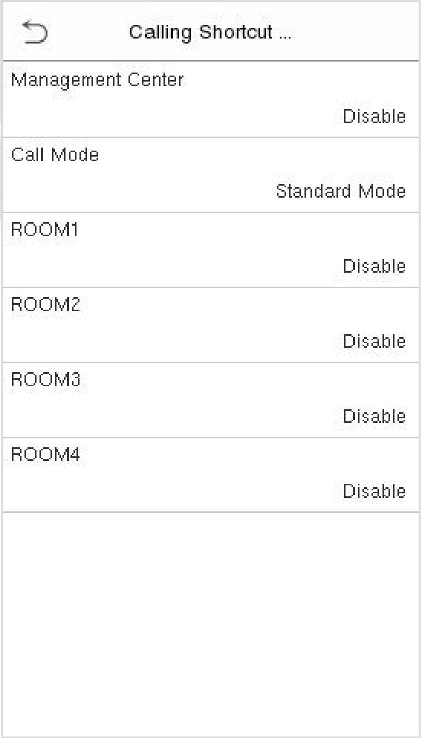
03 . 02 . 2601

Fence Terminal

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

10.1.6 Calling Shortcut Settings

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



Calling Shortcut ...

Management Center
Disable

Call Mode
Standard Mode

ROOM1
Disable

ROOM2
Disable

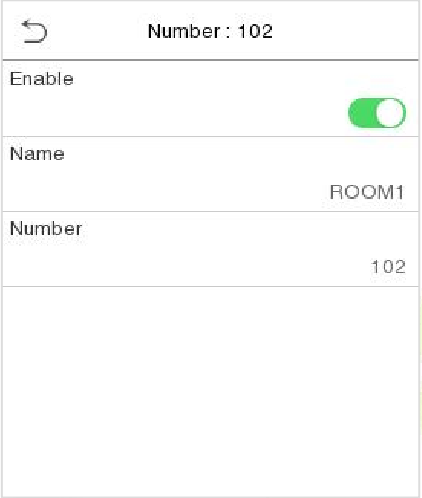
ROOM3
Disable

ROOM4
Disable

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.



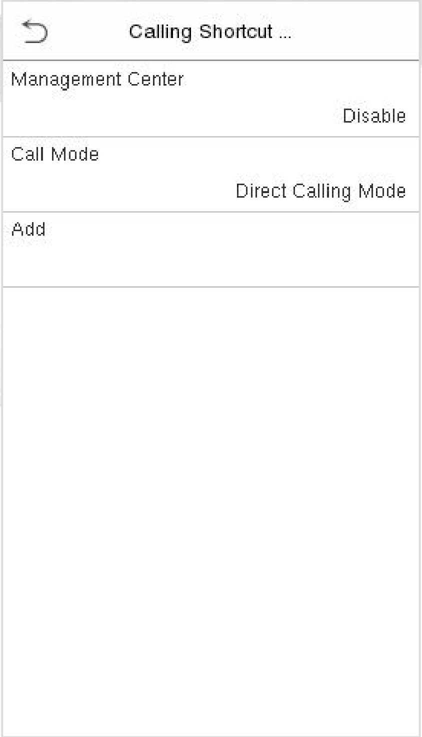
Number : 102

Enable ●

Name ROOM1

Number 102

- 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.

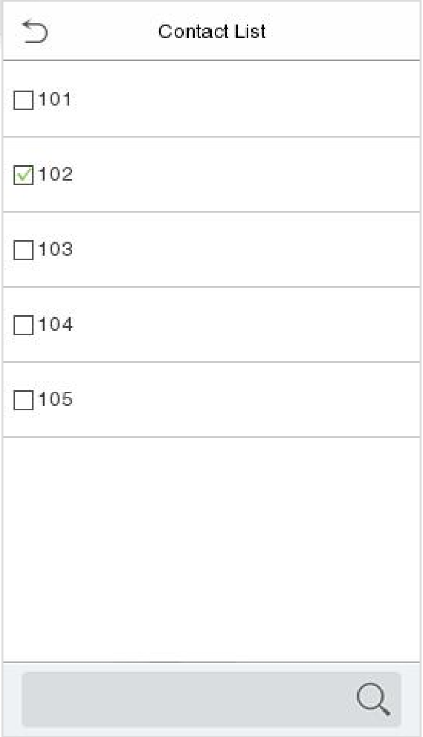


Calling Shortcut ...

Management Center Disable

Call Mode Direct Calling Mode

Add



Contact List

□101

☑102

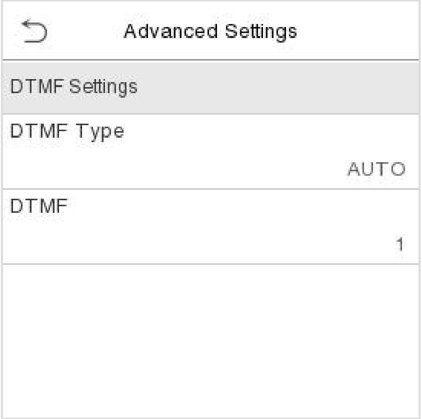
□103

□104

□105

10.1.7 Advanced Settings

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



Advanced Settings

DTMF Settings

DTMF Type: AUTO

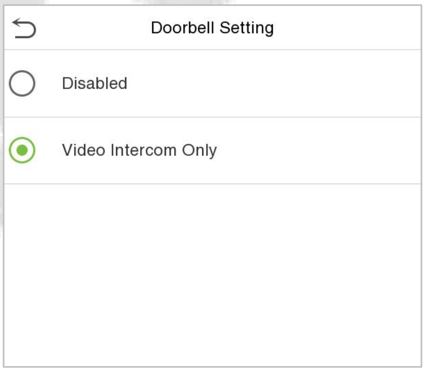
DTMF: 1

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.

10.2 Doorbell Setting

Tap **Doorbell Setting** on the **Video intercom Parameters** interface to go to the monitoring doorbell setting.



Doorbell Setting

○ Disabled

● Video Intercom Only

Function Description

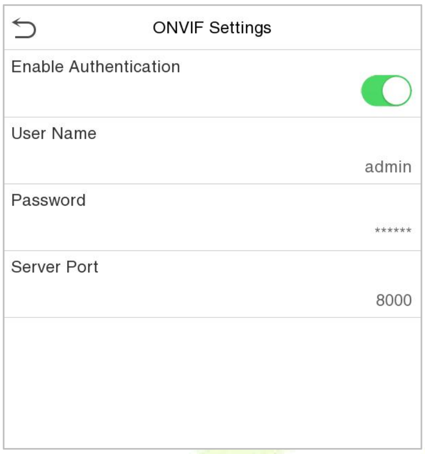
Function Name	Description
Video Intercom Only	Tap 🔔 or 📞 icon on standby interface, calling indoor unit for video intercom.

10.3 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 **Video intercom Parameters** interface.



ONVIF Settings

Enable Authentication

User Name admin

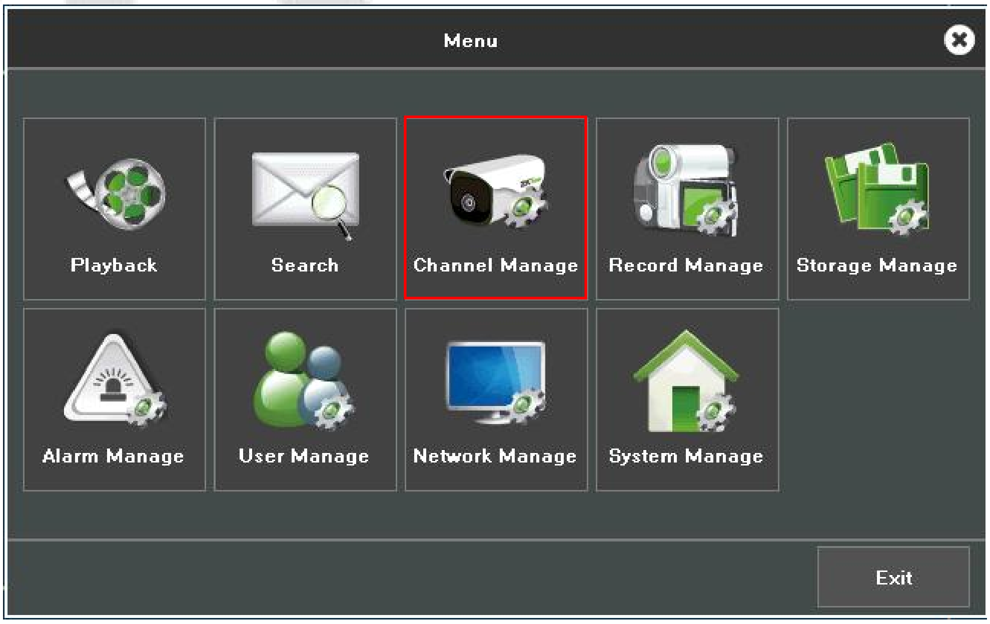
Password ******

Server Port 8000

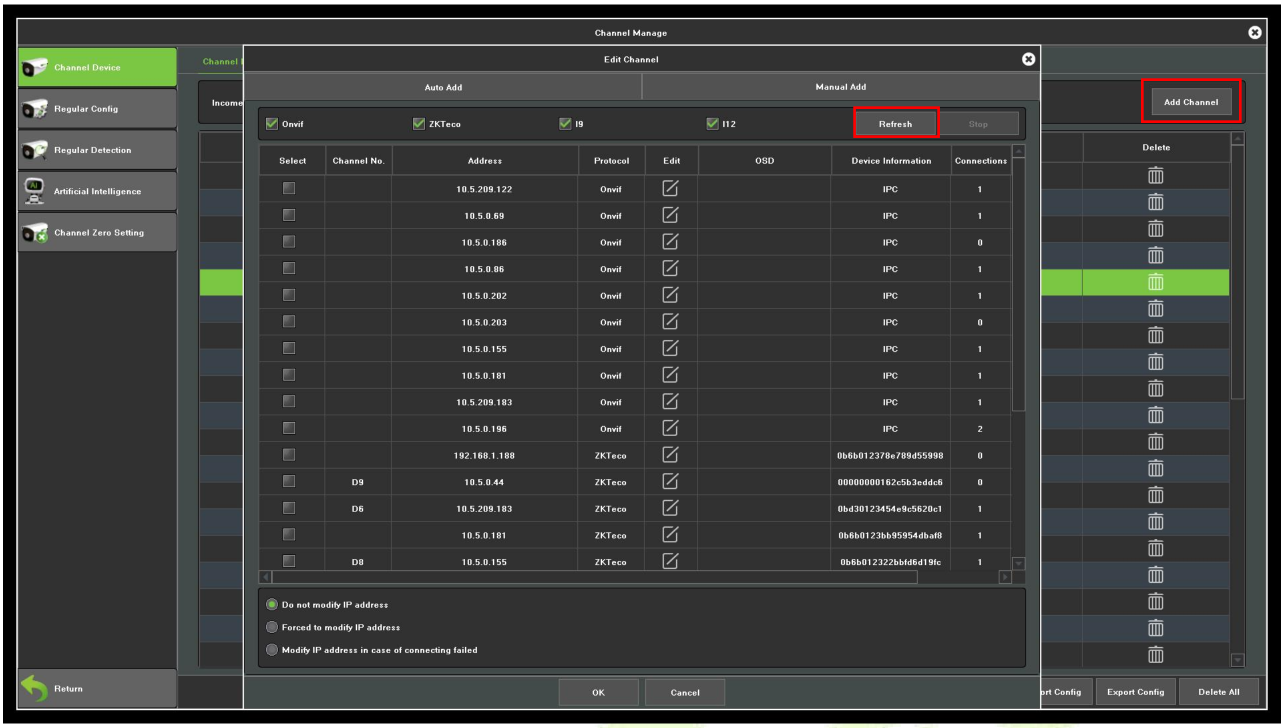
Function Description

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. The default is admin.
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.

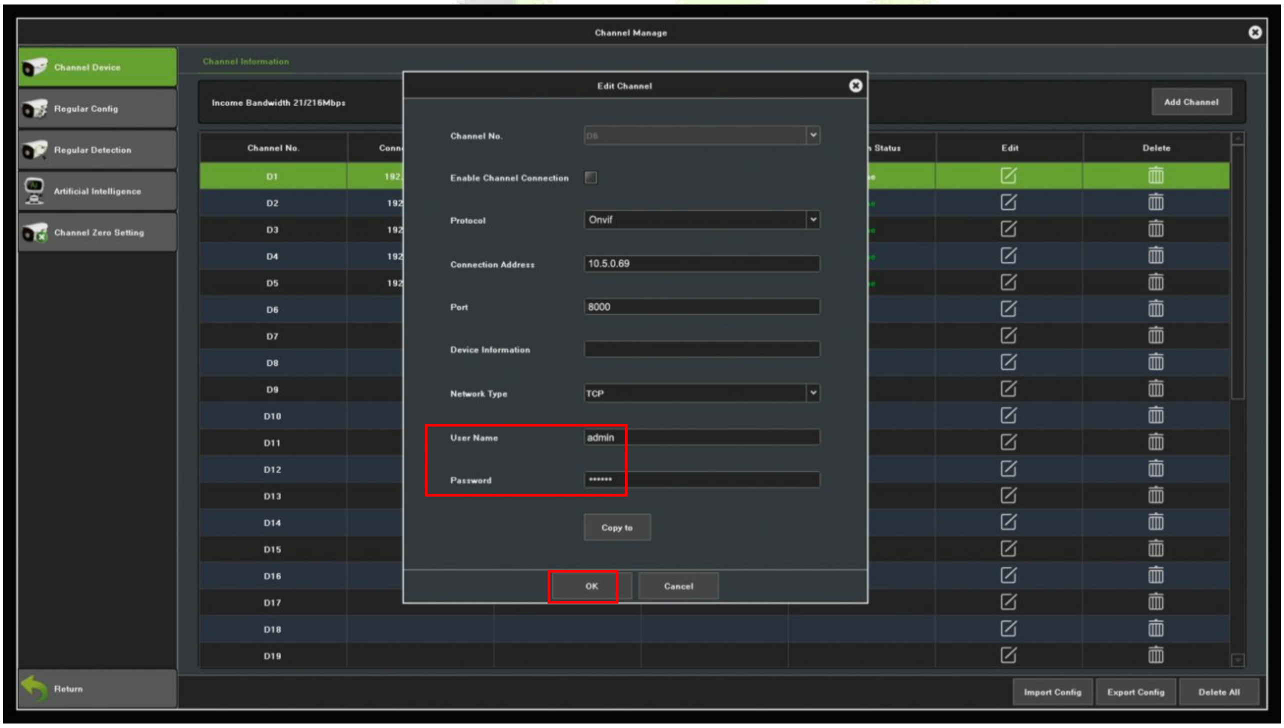


☑ Onvif ☑ ZKTeco ☑ I9 ☑ I12

Select	Channel No.	Address	Protocol	Edit	OSD	Device Information	Connections
□		10.5.209.122	Onvif			IPC	1
□		10.5.0.69	Onvif			IPC	1
□		10.5.0.186	Onvif			IPC	0
□		10.5.0.86	Onvif			IPC	1
□		10.5.0.202	Onvif			IPC	1
□		10.5.0.203	Onvif			IPC	0
□		10.5.0.155	Onvif			IPC	1
□		10.5.0.181	Onvif			IPC	1
□		10.5.209.183	Onvif			IPC	1
□		10.5.0.196	Onvif			IPC	2
□		192.168.1.188	ZKTeco			0b6b012378e789d55998	0
□	D9	10.5.0.44	ZKTeco			00000000162c5b3eddc6	0
□	D6	10.5.209.183	ZKTeco			0bd30123454e9c5620c1	1
□		10.5.0.181	ZKTeco			0b6b0123bb95954dbaf8	1
□	D8	10.5.0.155	ZKTeco			0b6b012322bbfd6d19fc	1

● Do not modify IP address
○ Forced to modify IP address
○ Modify IP address in case of connecting failed

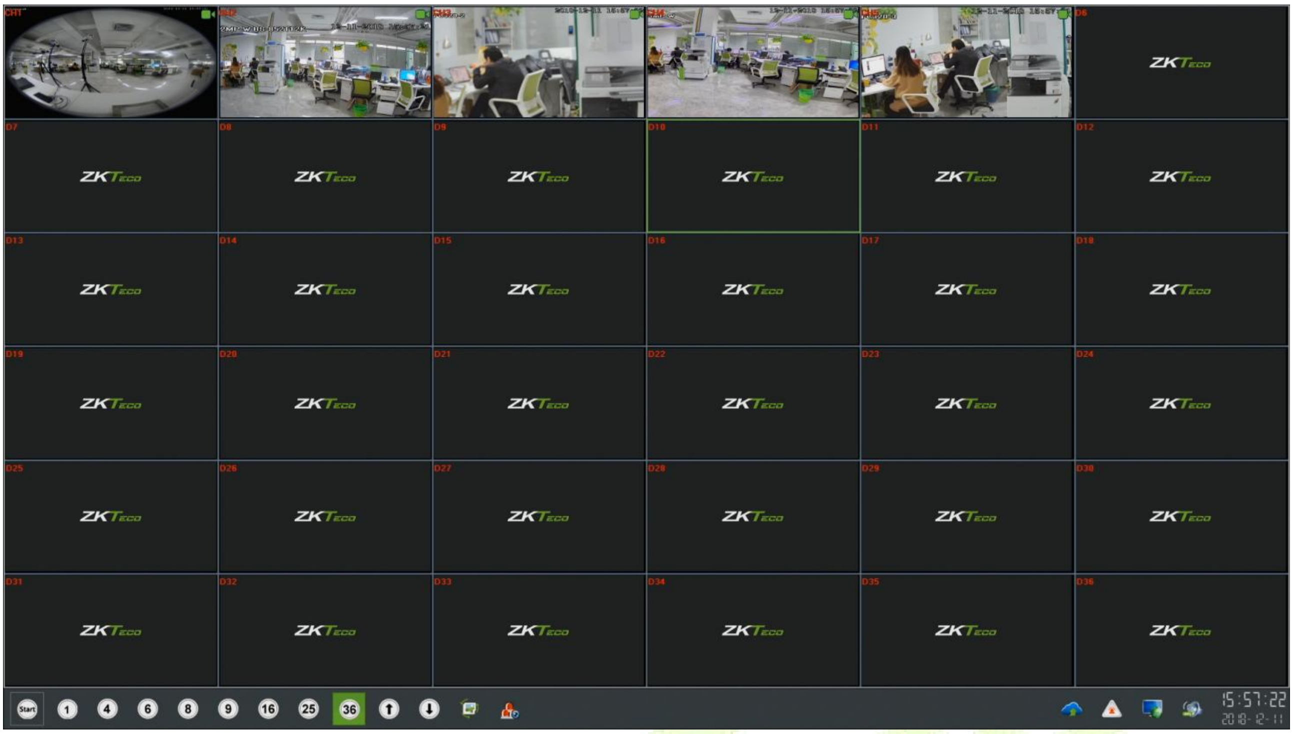
5. Select the checkbox for the device you want to add and edit the parameters in the corresponding text field, then click on [**OK**] to add it to the connection list.



Channel No.: D8
Enable Channel Connection: □
Protocol: Onvif
Connection Address: 10.5.0.69
Port: 8000
Device Information:
Network Type: TCP
User Name: admin
Password: ******

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

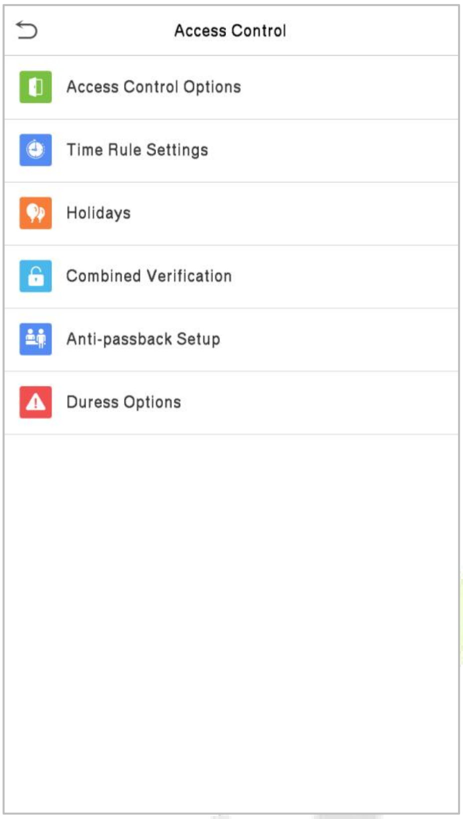
6. After adding successfully, the video image obtaining from the device can be viewed in real-time.



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

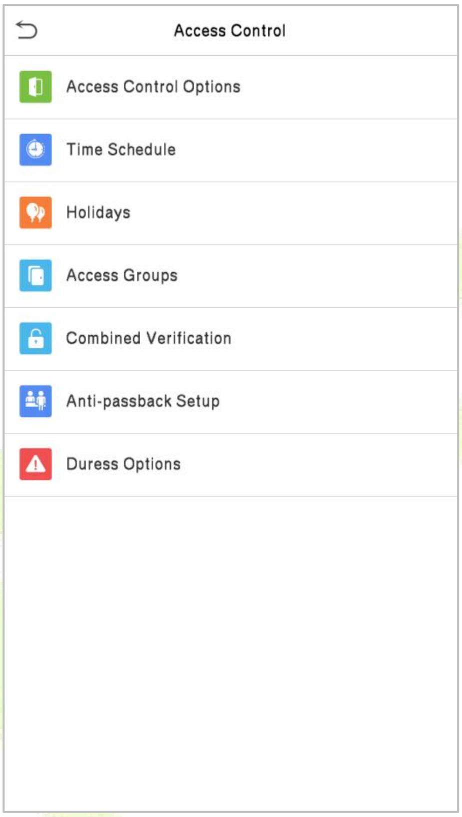
11 Access Control

On the **Main Menu**, tap **Access Control** to set the schedule of the door opening, locks control and to configure other parameters settings related to access control.



Access Control
- Access Control Options
- Time Rule Settings
- Holidays
- Combined Verification
- Anti-passback Setup
- Duress Options

A&C Terminal



Access Control
- Access Control Options
- Time Schedule
- Holidays
- Access Groups
- Combined Verification
- Anti-passback Setup
- Duress Options

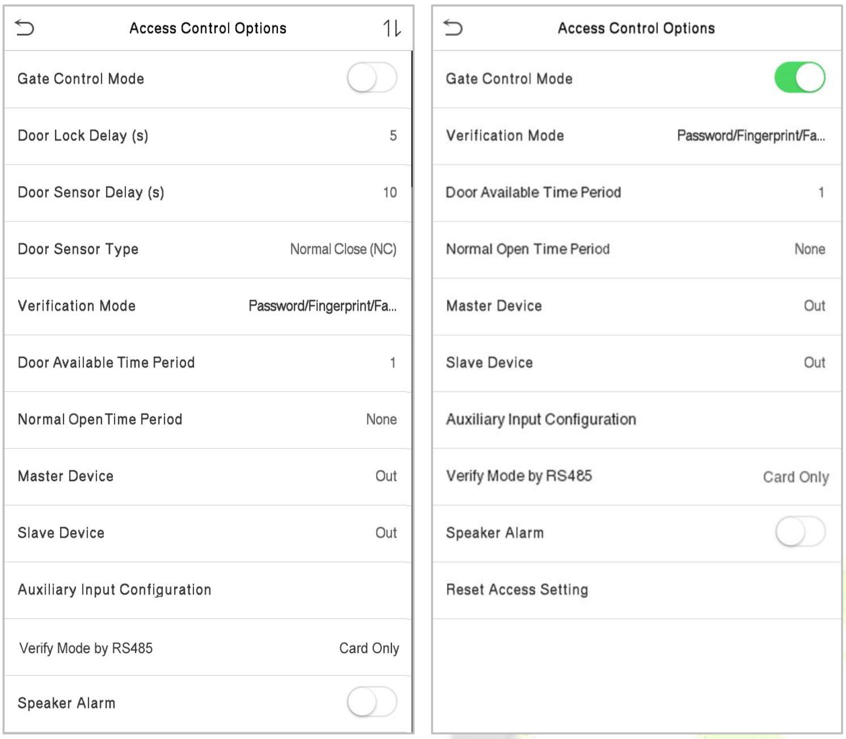
T&A Terminal

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

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

11.1 Access Control Options

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



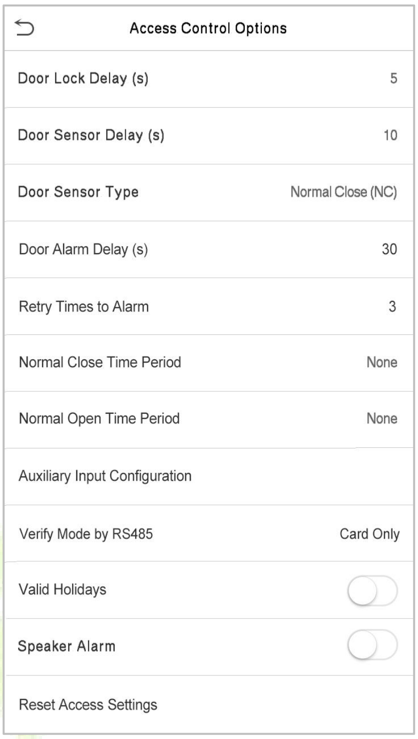
Access Control Options

Gate Control Mode	○
Door Lock Delay (s)	5
Door Sensor Delay (s)	10
Door Sensor Type	Normal Close (NC)
Verification Mode	Password/Fingerprint/Fa...
Door Available Time Period	1
Normal Open Time Period	None
Master Device	Out
Slave Device	Out
Auxiliary Input Configuration	
Verify Mode by RS485	Card Only
Speaker Alarm	○

Access Control Options

Gate Control Mode	●
Verification Mode	Password/Fingerprint/Fa...
Door Available Time Period	1
Normal Open Time Period	None
Master Device	Out
Slave Device	Out
Auxiliary Input Configuration	
Verify Mode by RS485	Card Only
Speaker Alarm	○
Reset Access Setting	

A&C Terminal



Access Control Options

Door Lock Delay (s)	5
Door Sensor Delay (s)	10
Door Sensor Type	Normal Close (NC)
Door Alarm Delay (s)	30
Retry Times to Alarm	3
Normal Close Time Period	None
Normal Open Time Period	None
Auxiliary Input Configuration	
Verify Mode by RS485	Card Only
Valid Holidays	○
Speaker Alarm	○
Reset Access Settings	

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: 1~10 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/Fingerprint/Card/Face, Fingerprint Only, User ID Only, Password, Card Only, Fingerprint/Password, Fingerprint/Card, User ID + Fingerprint, Fingerprint + Password, Fingerprint + Card, Fingerprint + Password + Card, Password + Card, Password/Card, User ID + Fingerprint + Password, Fingerprint + (Card/User ID), Face only, Face + Fingerprint, Face + Password, Face + Card, Face + Fingerprint + Card, Face + Fingerprint + Password.
Door Available Time Period	It sets the timing for the door so that the door is accessible only during that period.
Normal Open Time Period	It is the scheduled time-period for "Normal Open" mode so that the door is always open during this period.
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 Settings	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: 1~10 seconds; 0 seconds represents disabling the function.
Door Sensor Delay (s)	If the door is not locked and is left open for a certain duration (Door Sensor Delay), an alarm will be triggered. The valid value of Door Sensor Delay ranges from 1 to 255 seconds.

Door Sensor Type	There are three Sensor types: **None**, **Normal Open**, and **Normal Closed**. **None:** It means the door sensor is not in use. **Normally Open:** It means the door is always left open when electric power is on. **Normally Closed:** It means the door is always left closed when electric power is on.
Door Alarm Delay (s)	When the state of the door sensor is inconsistent with the door sensor type, an alarm will be triggered after a specified time period, i.e. the **Door Alarm Delay**. The valid value ranges from 1 to 999 seconds.
Retry Times to Alarm	When the number of failed verification reaches the set value (value ranges from 1 to 9 times), an 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 close 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	The verification mode is used when the device is used either as a host or slave. The supported verification mode includes Card Only and Card + Password.
Valid Holidays	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 Settings	The access control reset parameters include door lock delay, door sensor delay, door sensor type, verification mode, door available time period, normal open time period, master device, and alarm. However, erased access control data in Data Mgt. is excluded.

11.2 Time Rule Settings/Time Schedule

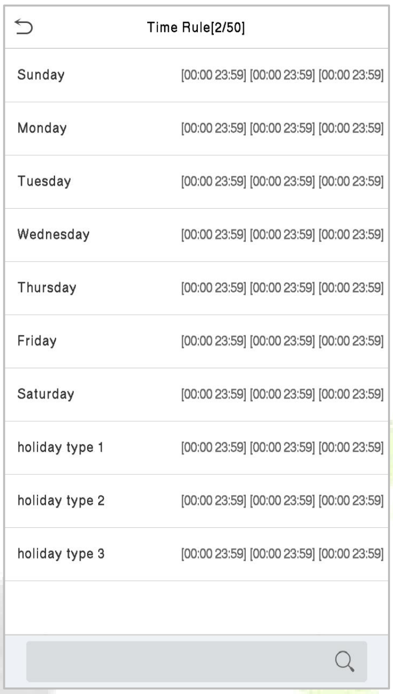
Function Description of A&C Terminal:

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

- The entire system can define up to 50 Time Periods.
- Each time-period represents **10** Time Zones, i.e., **1** week and **3** holidays, and each time zone is a standard 24 hour period per day and the user can only verify within the valid time-period.

- One can set a maximum of 3 time periods for every time zone. The relationship among these time-periods is "**OR**". Thus, when the verification time falls in any one of these time-periods, the verification is valid.
- The Time Zone format of each time-period is **HH MM-HH MM**, which is accurate to minutes according to the 24-hour clock.

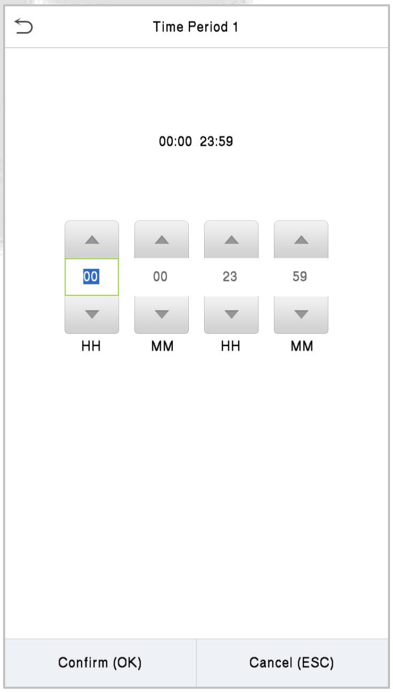
Tap the grey box to search the required Time Zone and specify the required Time Zone number (maximum up to 50 zones).



Time Rule[2/50]

Sunday	[00:00 23:59] [00:00 23:59] [00:00 23:59]
Monday	[00:00 23:59] [00:00 23:59] [00:00 23:59]
Tuesday	[00:00 23:59] [00:00 23:59] [00:00 23:59]
Wednesday	[00:00 23:59] [00:00 23:59] [00:00 23:59]
Thursday	[00:00 23:59] [00:00 23:59] [00:00 23:59]
Friday	[00:00 23:59] [00:00 23:59] [00:00 23:59]
Saturday	[00:00 23:59] [00:00 23:59] [00:00 23:59]
holiday type 1	[00:00 23:59] [00:00 23:59] [00:00 23:59]
holiday type 2	[00:00 23:59] [00:00 23:59] [00:00 23:59]
holiday type 3	[00:00 23:59] [00:00 23:59] [00:00 23:59]

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



Time Period 1

00:00 23:59

HH	MM	HH	MM
00	00	23	59

Confirm (OK) Cancel (ESC)

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

Note:

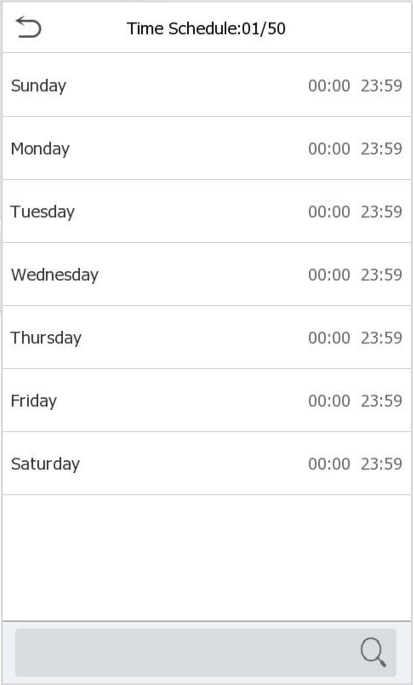
- The door is inaccessible for the whole day when the End Time occurs before the Start Time (such as **23:57~23:56**).
- It is the time interval for valid access when the End Time occurs after the Start Time (such as **08:00~23:59**).
- The door is accessible for the whole day when the End Time occurs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

Function Description of T&A Terminal★:

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

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

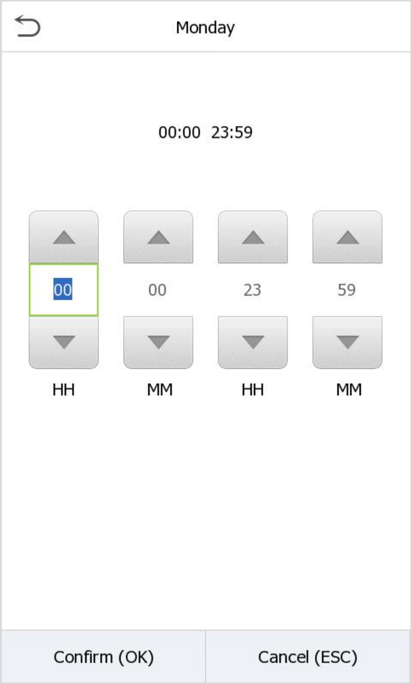
Tap the grey box to search the required Time Zone and specify the required Time Zone number (maximum up to 50 zones).



Time Schedule:01/50

Sunday	00:00 23:59
Monday	00:00 23:59
Tuesday	00:00 23:59
Wednesday	00:00 23:59
Thursday	00:00 23:59
Friday	00:00 23:59
Saturday	00:00 23:59

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



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

Notes:

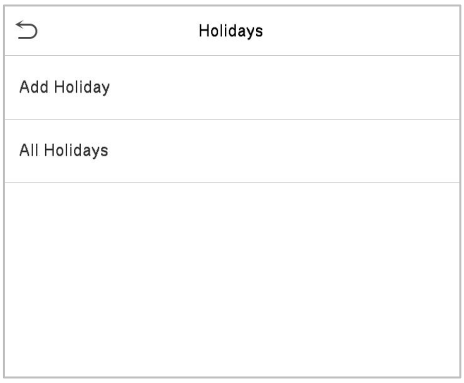
- The door is inaccessible for the entire day when the End Time occurs before the Start Time (such as **23:57 to 23:56**).
- It is the time interval for valid access when the End Time occurs after the Start Time (such as **08:00 to 23:59**).
- The door is accessible for the entire day when the End Time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

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

11.3 Holidays

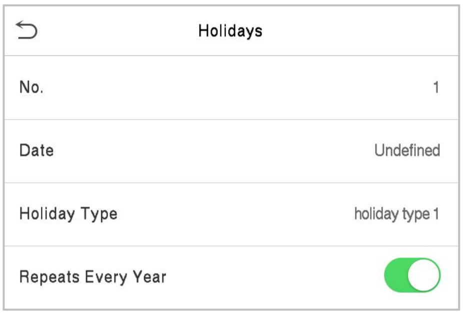
Whenever there is a holiday, you may need a distinct access time; but changing everyone's access time one by one is extremely cumbersome, so a holiday access time can be set that applies to all employees and the user will be able to open the door during the holidays.

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



- **Add a New Holiday**

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



Holidays

No. 1

Date Undefined

Holiday Type holiday type 1

Repeats Every Year

- **Edit a Holiday**

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

- **Delete a Holiday**

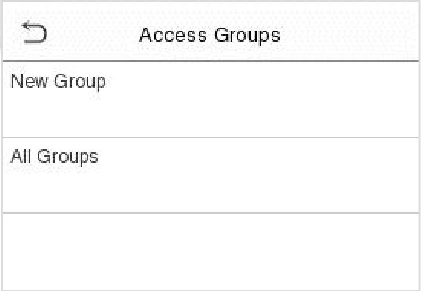
On the **Holidays** interface, select a holiday item to be deleted and tap **Delete**. Press **OK** to confirm the deletion. After deletion, this holiday does not display on the **All Holidays** interface.

11.4 Access Groups★

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

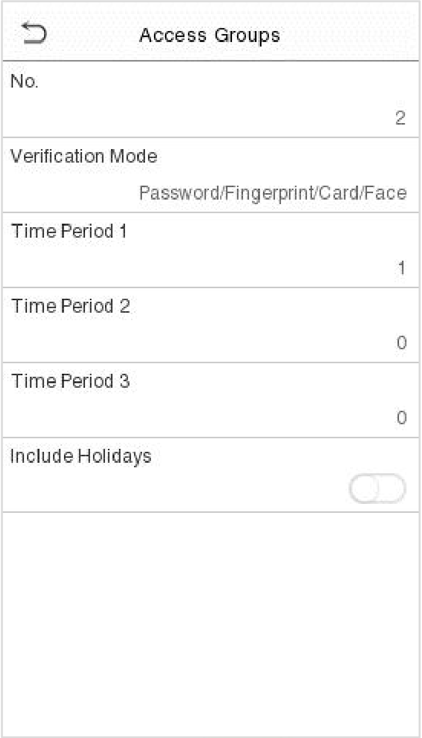
This is to easily manage groupings and users in different access groups. Settings of an access group such as access time zones are applicable to all members in the group by default. However, users may manually set the time zones as needed. User authentication takes precedence over group authentication 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.


Access Groups

No.
2

Verification Mode
Password/Fingerprint/Card/Face

Time Period 1
1

Time Period 2
0

Time Period 3
0

Include Holidays

Notes:

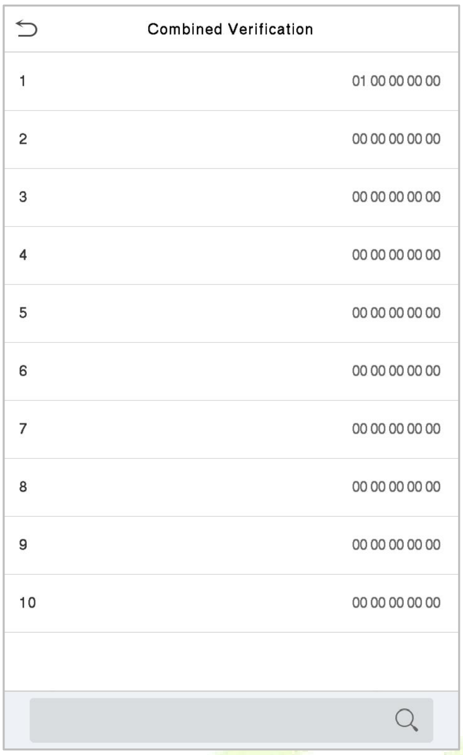
- There is a default access group numbered 1, which cannot be deleted, but can be modified.
- A number cannot be modified after being set.
- When the holiday is set to be valid, personnel in a group may only open the door when the group time zone overlaps with the holiday time period.
- When the holiday is set to be invalid, the access control time of the personnel in a group is not affected during holidays.

11.5 Combined Verification

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

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

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



Combined Verification

1	01 00 00 00 00
2	00 00 00 00 00
3	00 00 00 00 00
4	00 00 00 00 00
5	00 00 00 00 00
6	00 00 00 00 00
7	00 00 00 00 00
8	00 00 00 00 00
9	00 00 00 00 00
10	00 00 00 00 00

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

For Example:

- If the **Door-unlock combination 1** is set as **(01 03 05 06 08)**. It indicates that the unlock combination 1 consists of 5 people and all the 5 individuals are from 5 groups, namely, AC Group 1, AC Group 3, AC Group 5, AC Group 6, and AC Group 8, respectively.
- If the **Door-unlock combination 2** is set as **(02 02 04 04 07)**. It indicates that the unlock combination 2 consists of 5 people; the first two are from AC Group 2, the next two are from AC Group 4, and the last person is from AC Group 7.
- If the **Door-unlock combination 3** is set as **(09 09 09 09 09)**. It indicates that there are 5 people in this combination; all of which are from AC Group 9.
- If the **Door-unlock combination 4** is set as **(03 05 08 00 00)**. It indicates that the unlock combination 4 consists of only three people. The first person is from AC Group 3, the second person is from AC Group 5, and the third person is from AC Group 8.

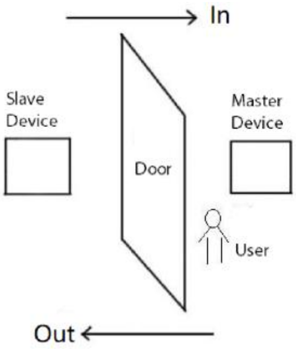
Note: To delete the door-unlock combination, set all Door-unlock combinations to 0.

11.6 Anti-passback Setup

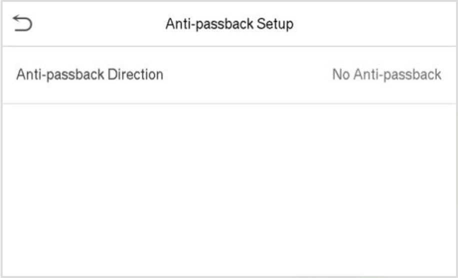
A user may be followed by some person(s) to enter the door without verification, resulting in a security breach. So, to avoid such situations, the Anti-Passback option was developed. Once it is enabled, the check-in and check-out record must occur alternatively to open the door to represent a consistent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

This function requires two devices to work together:

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

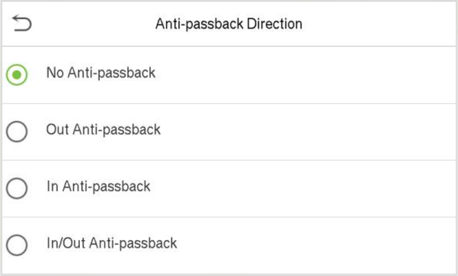


Tap **Anti-Passback Setup** on the **Access Control** interface.



Anti-passback Setup

Anti-passback Direction No Anti-passback



Anti-passback Direction

● No Anti-passback
○ Out Anti-passback
○ In Anti-passback
○ In/Out Anti-passback

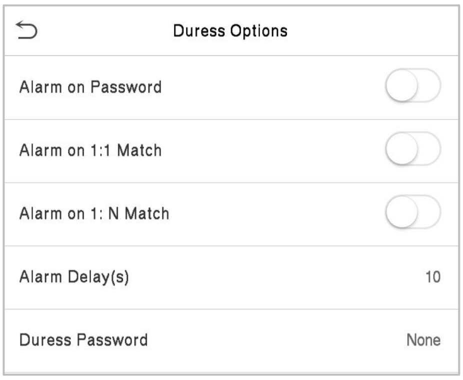
Function Description

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

11.7 Duress Options Settings

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

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



Duress Options

Alarm on Password	○
Alarm on 1:1 Match	○
Alarm on 1: N Match	○
Alarm Delay(s)	10
Duress Password	None

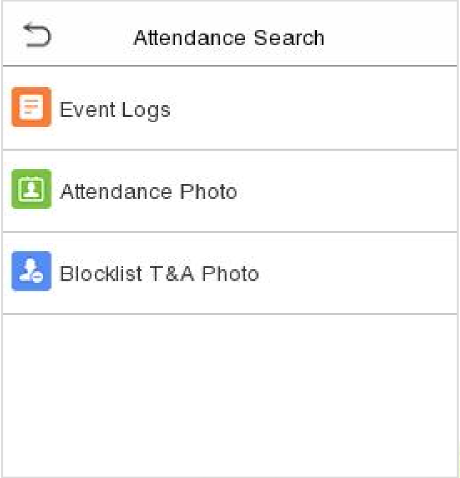
Function Description

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

12 Attendance Search

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

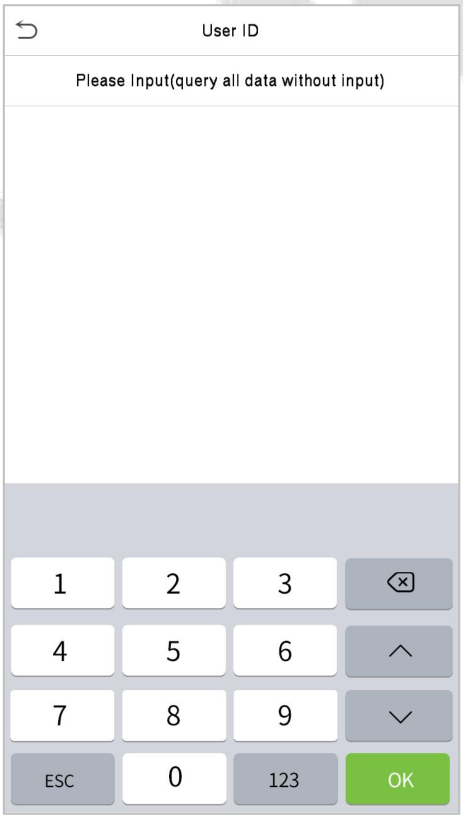
Select **Attendance Search** on the **Main Menu** interface to search for the required event Logs.



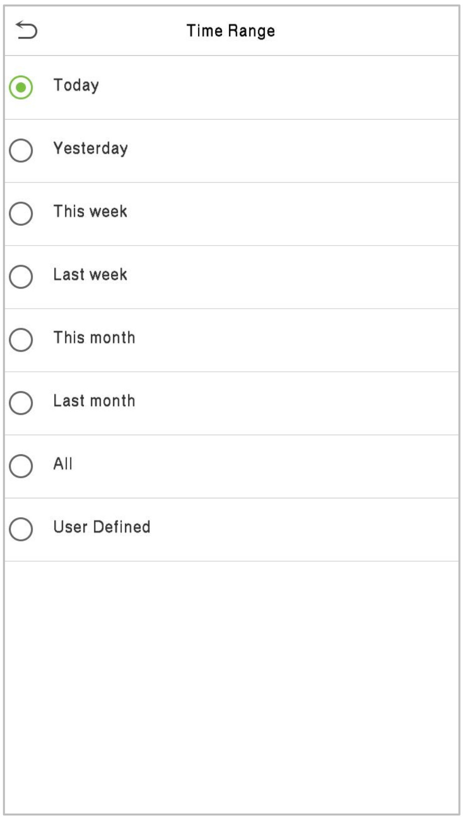
The process of searching for attendance and blocklist photos is similar to that of searching for event logs. The following is an example of searching for event logs.

On the **Attendance Search** interface, tap **Event Logs** to search for the required record.

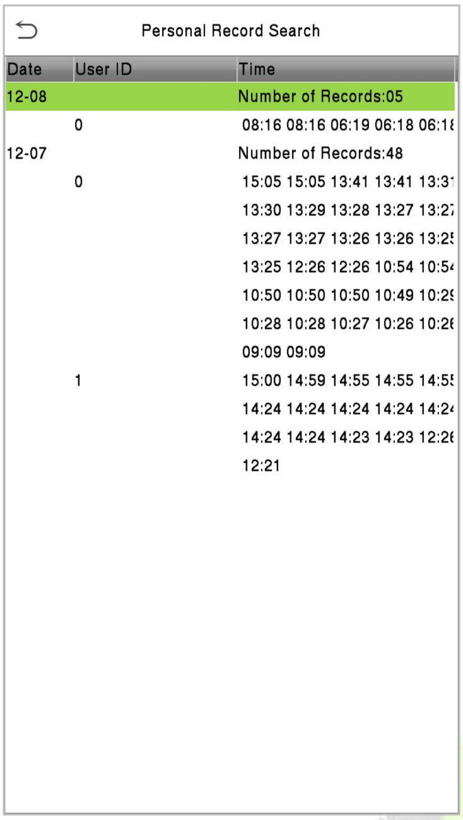
1. Enter the user ID to be searched and tap **OK**. If you want to search for records of all users, tap **OK** without entering any user ID.



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



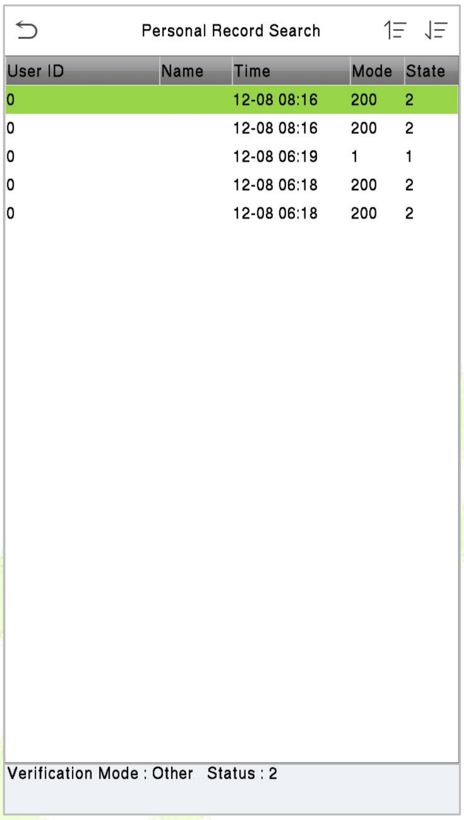
3. Once the record search completes. Tap the record highlighted in green to view its details.



Personal Record Search

Date	User ID	Time
12-08		Number of Records:05
	0	08:16 08:16 06:19 06:18 06:1
12-07		Number of Records:48
	0	15:05 15:05 13:41 13:41 13:3
		13:30 13:29 13:28 13:27 13:2
		13:27 13:27 13:26 13:26 13:2
		13:25 12:26 12:26 10:54 10:5
		10:50 10:50 10:50 10:49 10:2
		10:28 10:28 10:27 10:26 10:2
		09:09 09:09
	1	15:00 14:59 14:55 14:55 14:5
		14:24 14:24 14:24 14:24 14:2
		14:24 14:24 14:23 14:23 12:2
		12:21

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



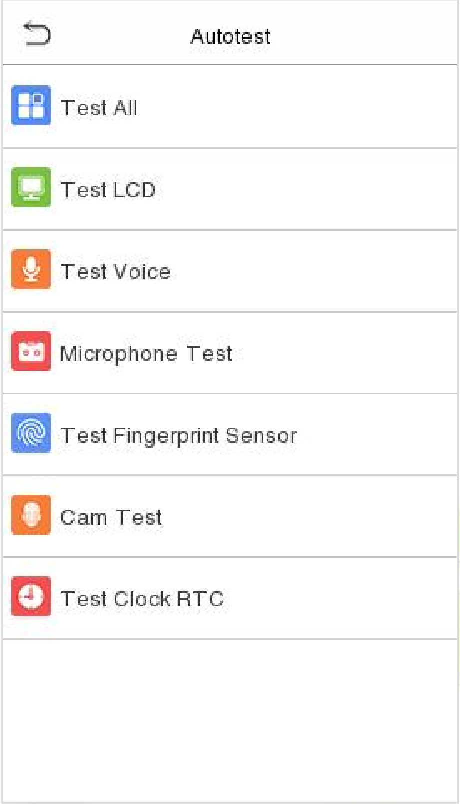
Personal Record Search

User ID	Name	Time	Mode	State
0		12-08 08:16	200	2
0		12-08 08:16	200	2
0		12-08 06:19	1	1
0		12-08 06:18	200	2
0		12-08 06:18	200	2

Verification Mode : Other Status : 2

13 Autotest

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



Autotest

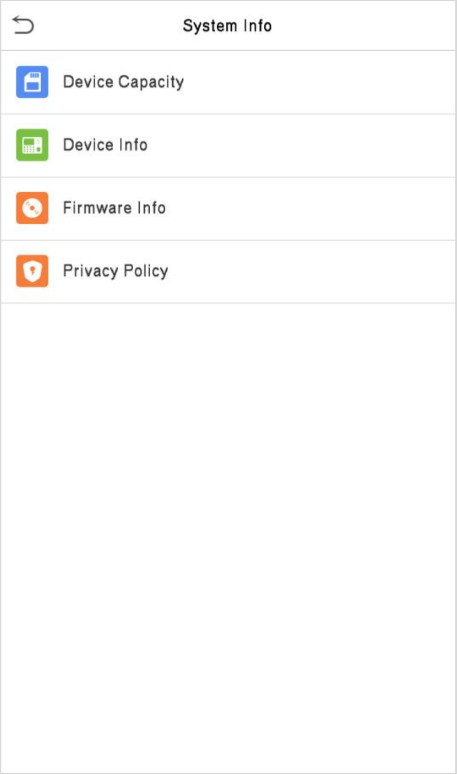
- Test All
- Test LCD
- Test Voice
- Microphone Test
- Test Fingerprint Sensor
- Cam Test
- Test Clock RTC

Function Description

Function Name	Description
Test All	To automatically test whether the LCD, Audio, Camera and RTC are normal.
Test LCD	To automatically test the display effect of LCD screen by displaying full-color, pure white, and pure black to check whether the screen displays colors normally.
Test Voice	To automatically test whether the audio files stored in the device are complete and the voice quality is good.
Microphone Test	Check whether the microphone is working by speaking to microphone and playing the microphone recording.
Test Fingerprint Sensor	To test the fingerprint sensor by pressing a finger on the scanner to check if the acquired fingerprint image is clear. When you are pressing a finger on the scanner, the fingerprint image will display on the screen.
Cam Test	To test if the camera functions properly by checking the photos taken to see if they are clear enough. (Same as "Test Face".)
Test Clock RTC	To test the RTC. The device tests whether the clock works normally and accurately with a stopwatch. Tap the screen to start counting and press it again to stop counting.

14 System Information

On the **Main Menu**, tap **System Info** to view the storage status, the version information of the device, and firmware information.



Function Description

Function Name	Description
Device Capacity	Displays the current device's user storage, password, and face storage, administrators, access records, attendance and blocklist photos, and user photos.
Device Info	Displays the device's name, serial number, MAC address, face algorithm, platform information, and manufacturer and manufacture date.
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

- **Device Side**

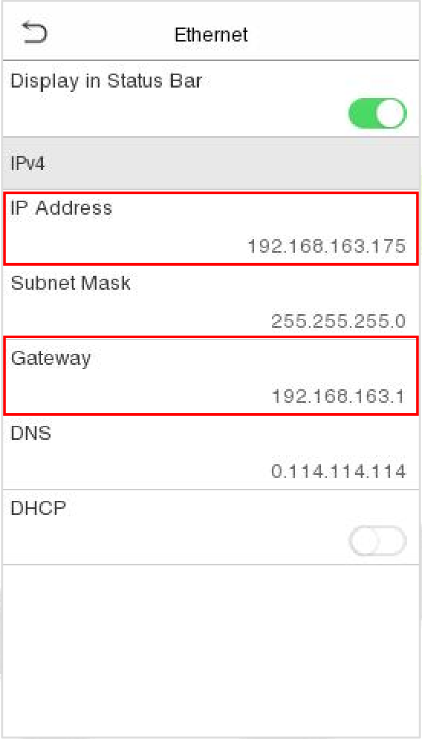
1. Tap **COMM.** > **Ethernet** in the main menu to set the IP address and gateway of the device.

   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.



Ethernet

Display in Status Bar

IPv4

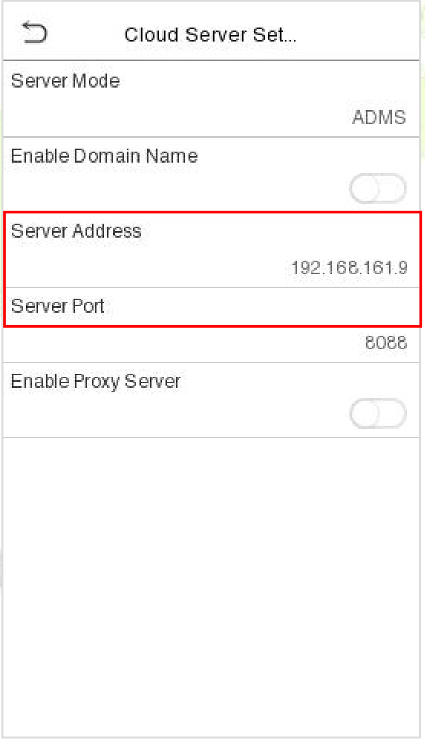
IP Address: 192.168.163.175

Subnet Mask: 255.255.255.0

Gateway: 192.168.163.1

DNS: 0.114.114.114

DHCP



Cloud Server Set...

Server Mode: ADMS

Enable Domain Name

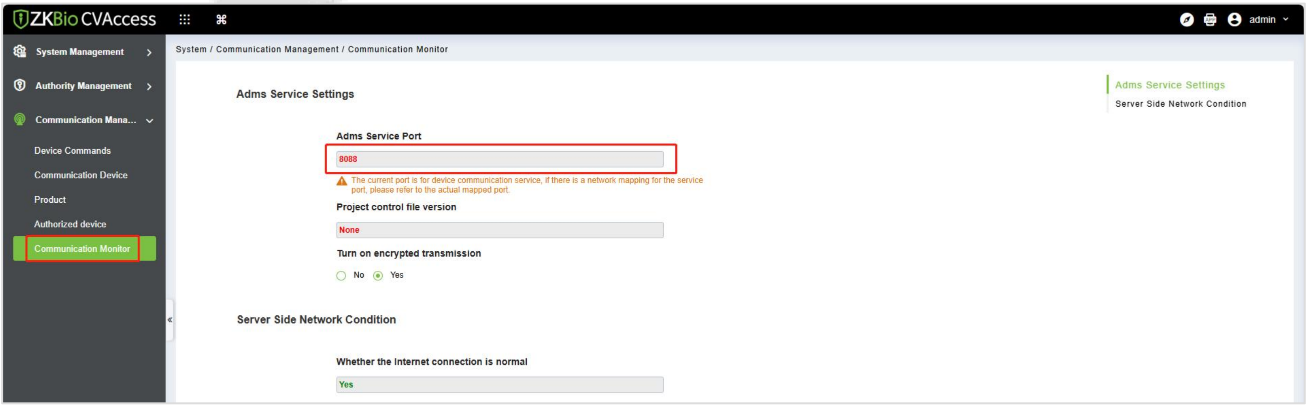
Server Address: 192.168.161.9

Server Port: 8088

Enable Proxy Server

- **Software Side**

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



System / Communication Management / Communication Monitor

Adms Service Settings

Adms Service Port: 8088

The current port is for device communication service, if there is a network mapping for the service port, please refer to the actual mapped port.

Project control file version: None

Turn on encrypted transmission: ○ No ● Yes

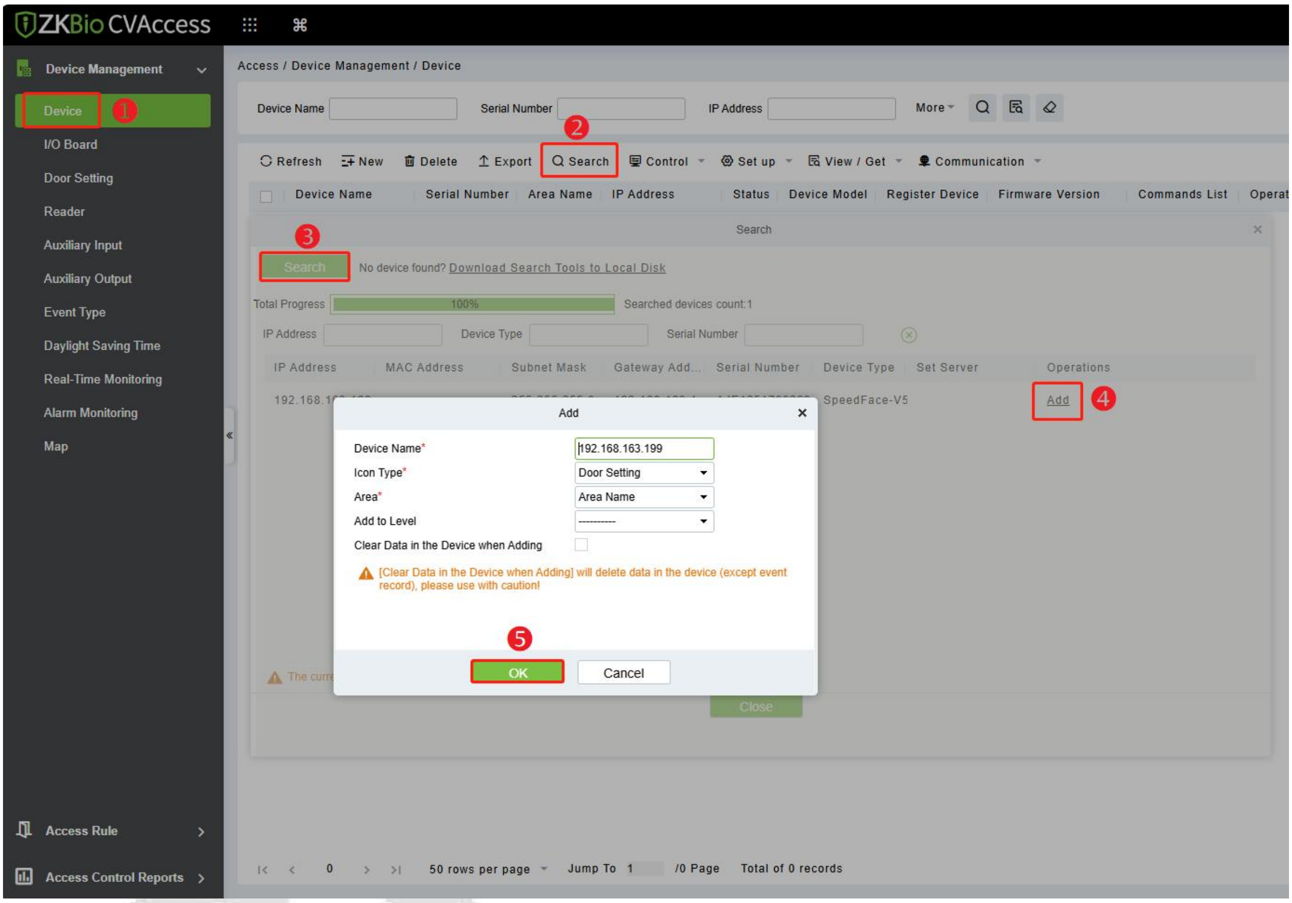
Server Side Network Condition

Whether the Internet connection is normal: Yes

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.



No device found? Download Search Tools to Local Disk

Total Progress 100% Searched devices count:1

Add

Device Name* 192.168.163.199

Icon Type* Door Setting

Area* Area Name

Add to Level ---------

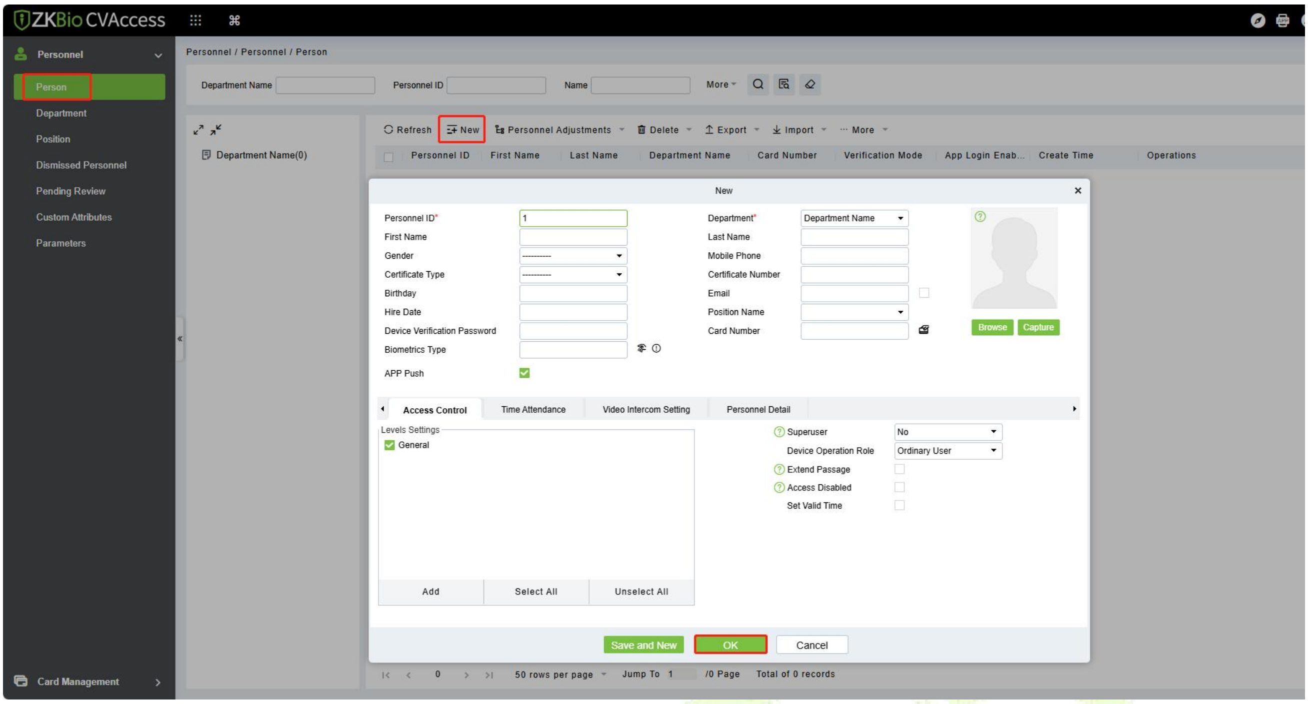
Clear Data in the Device when Adding □

[Clear Data in the Device when Adding] will delete data in the device (except event record), please use with caution!

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.



Personnel ID* 1

Department* Department Name

☑ General

Superuser No

Device Operation Role Ordinary User

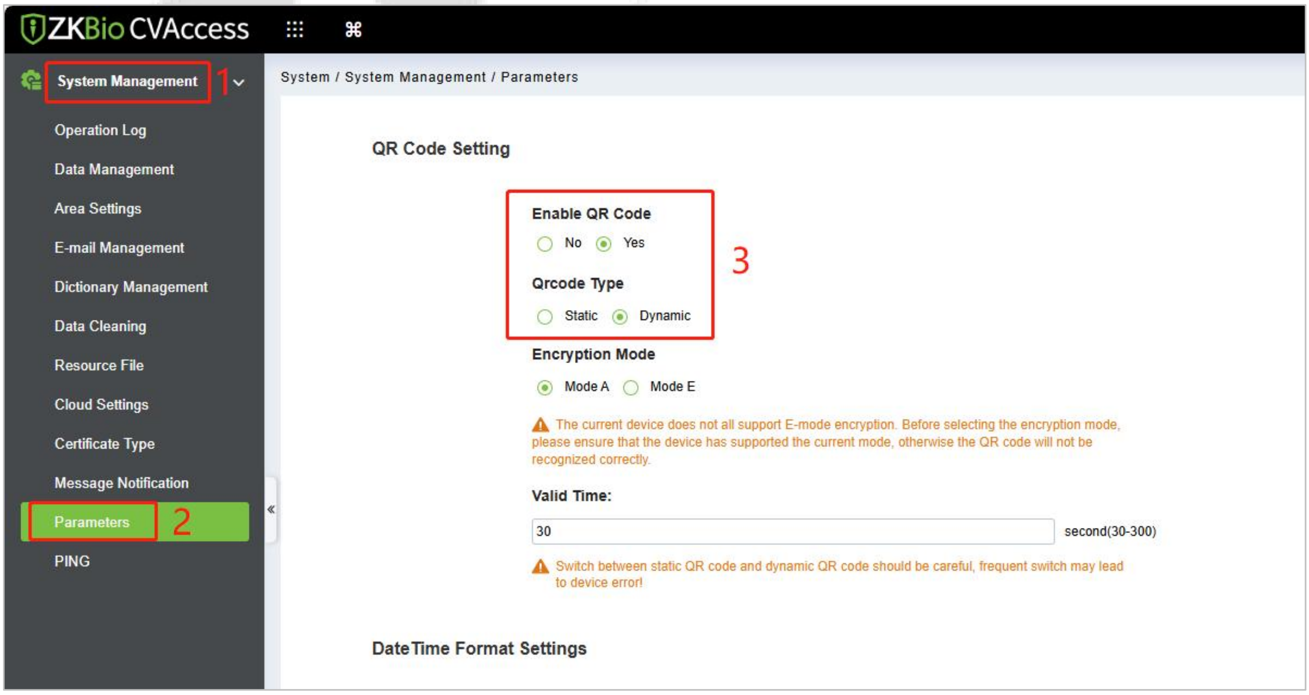
3. Click **Access** > **Device** > **Device Control** > **Synchronize All Data to Devices** to synchronize all the data to the device including the new users.

15.4 Mobile Credential★

Note: *This feature is only available for devices that support dynamic QR codes*

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 QR code Type as **Dynamic**, the valid time of the QR code can be set.



QR Code Setting

Enable QR Code
○ No ● Yes

Qrcode Type
○ Static ● Dynamic

Encryption Mode
● Mode A ○ Mode E

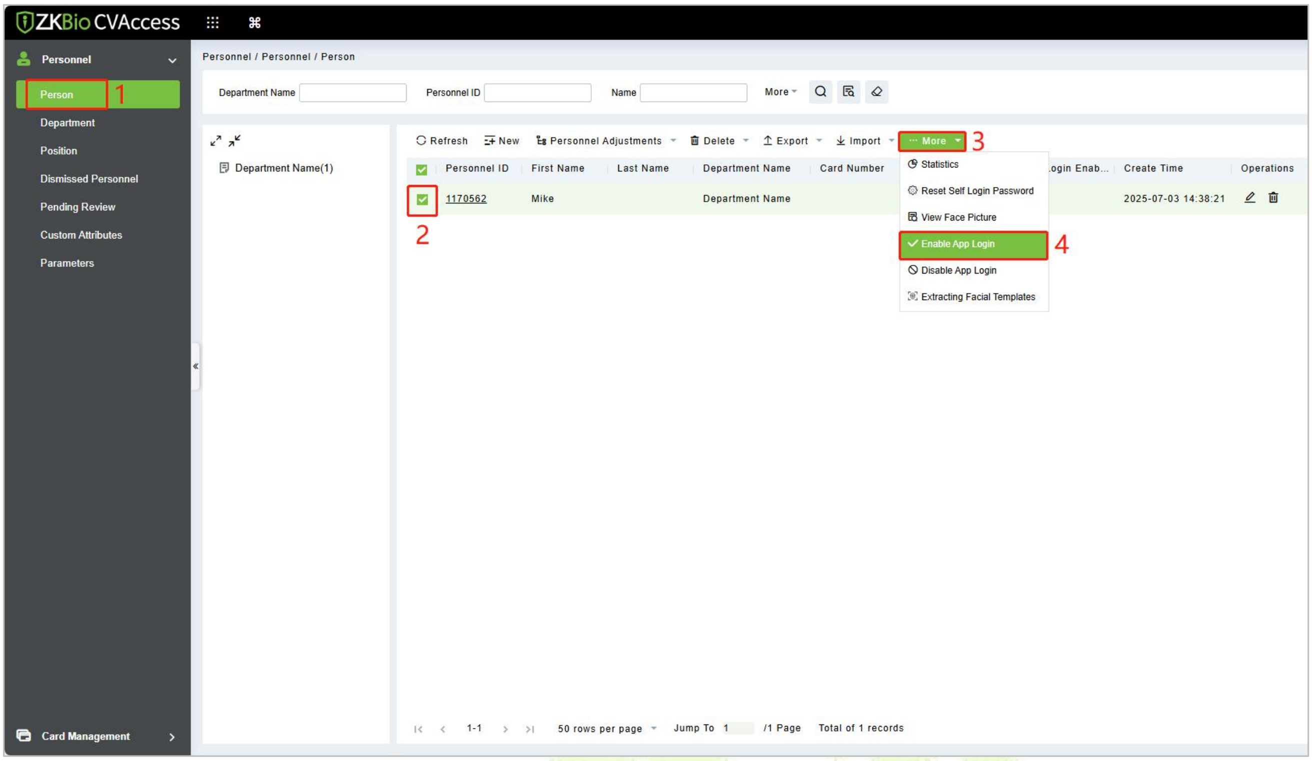
⚠ The current device does not all support E-mode encryption. Before selecting the encryption mode, please ensure that the device has supported the current mode, otherwise the QR code will not be recognized correctly.

Valid Time:
30 second(30-300)

⚠ Switch between static QR code and dynamic QR code should be careful, frequent switch may lead to device error!

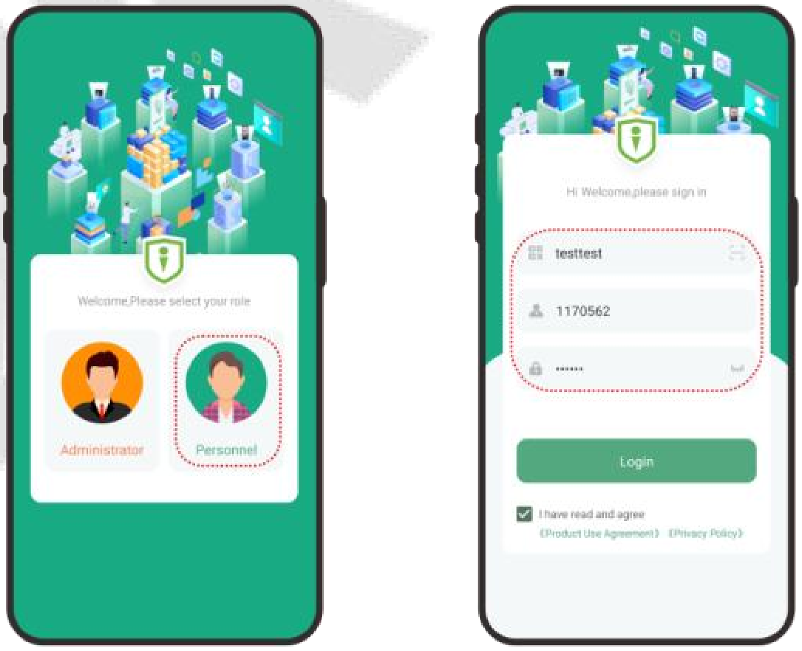
DateTime Format Settings

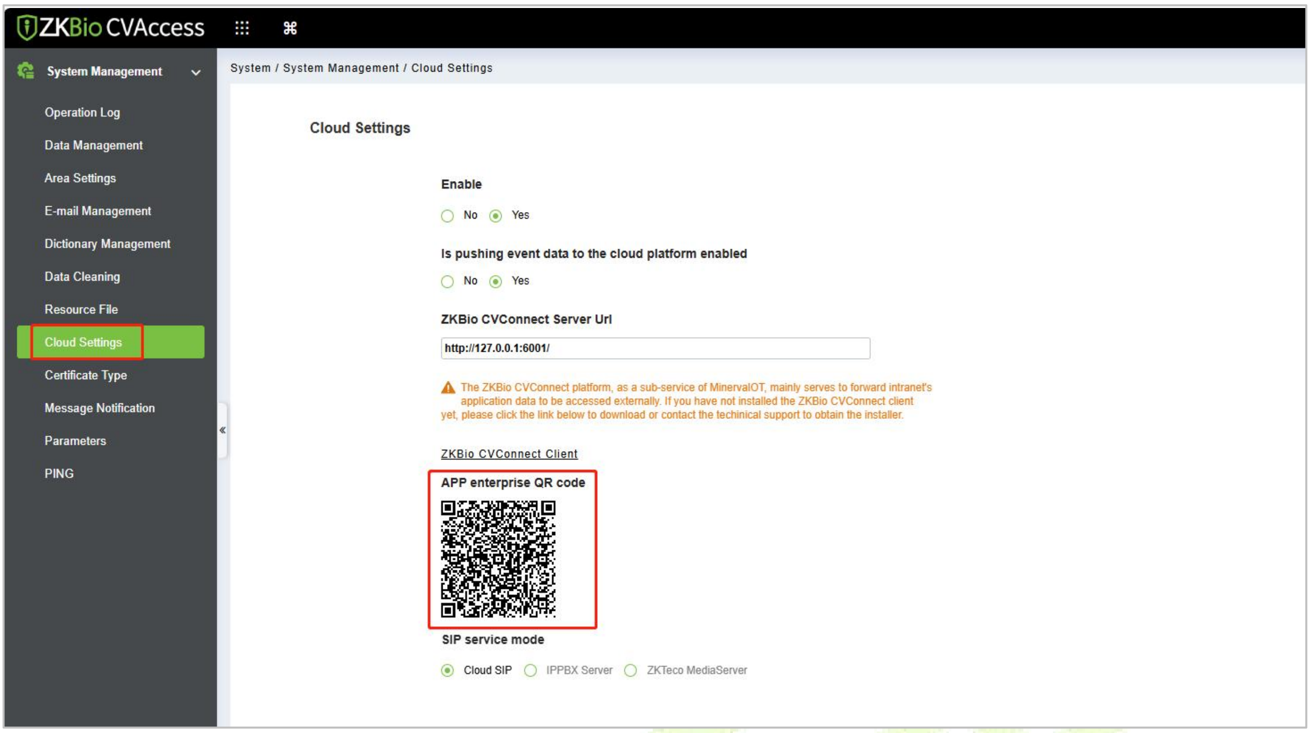
2. Click **Personnel > Personnel > Person**, select the personnel and click **More > Enable APP Login**.



☑	Personnel ID	First Name	Last Name	Department Name	Card Number	Login Enab...	Create Time	Operations
☑	1170562	Mike		Department Name			2025-07-03 14:38:21	

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**).


Welcome,Please select your role
Administrator
Personnel
Hi Welcome,please sign in
testtest
1170562
••••••
Login
I have read and agree
《Product Use Agreement》 《Privacy Policy》



System / System Management / Cloud Settings

Cloud Settings

Enable

○ No ● Yes

Is pushing event data to the cloud platform enabled

○ No ● Yes

ZKBio CVConnect Server Url

http://127.0.0.1:6001/

The ZKBio CVConnect platform, as a sub-service of MinervalOT, mainly serves to forward intranet's application data to be accessed externally. If you have not installed the ZKBio CVConnect client yet, please click the link below to download or contact the techinical support to obtain the installer.

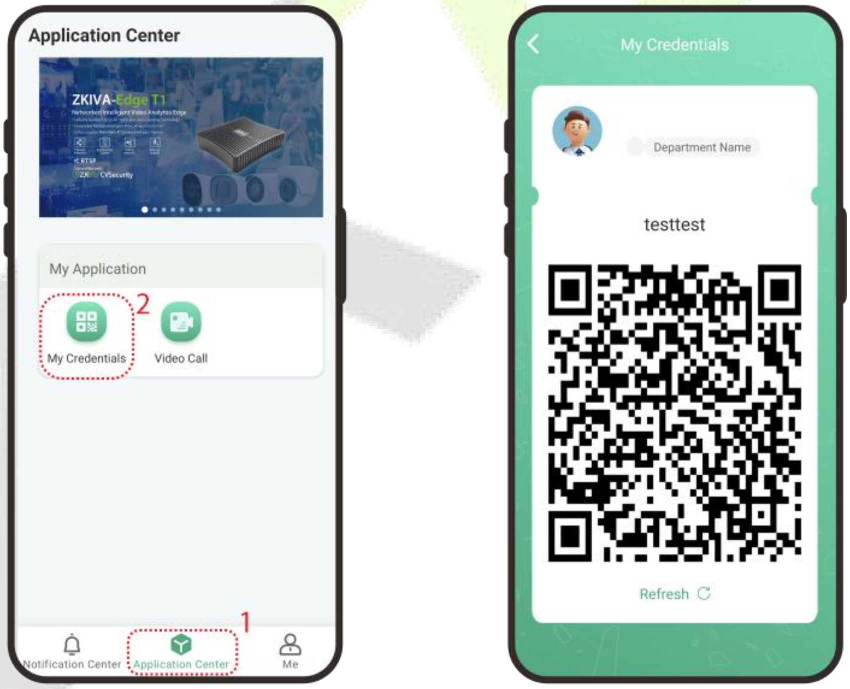
ZKBio CVConnect Client

APP enterprise QR code

SIP service mode

● Cloud SIP ○ IPPBX Server ○ ZKTeco MediaServer

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.

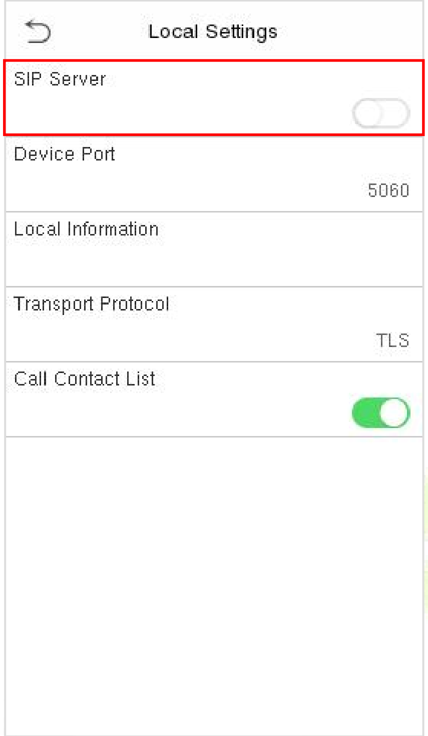
6. The QR code refreshes automatically for every 30s and supports manual refresh.

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.



Local Settings

SIP Server ○

Device Port 5060

Local Information

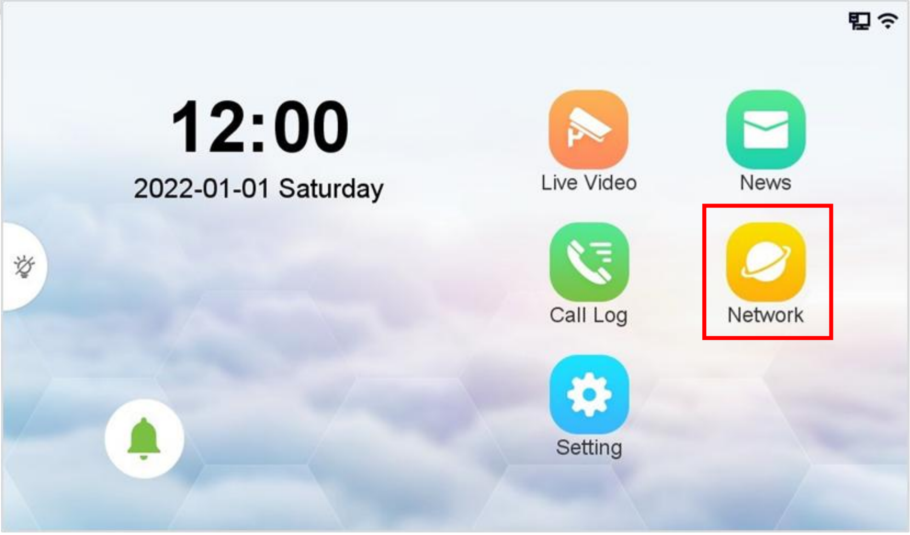
Transport Protocol TLS

Call Contact List ●

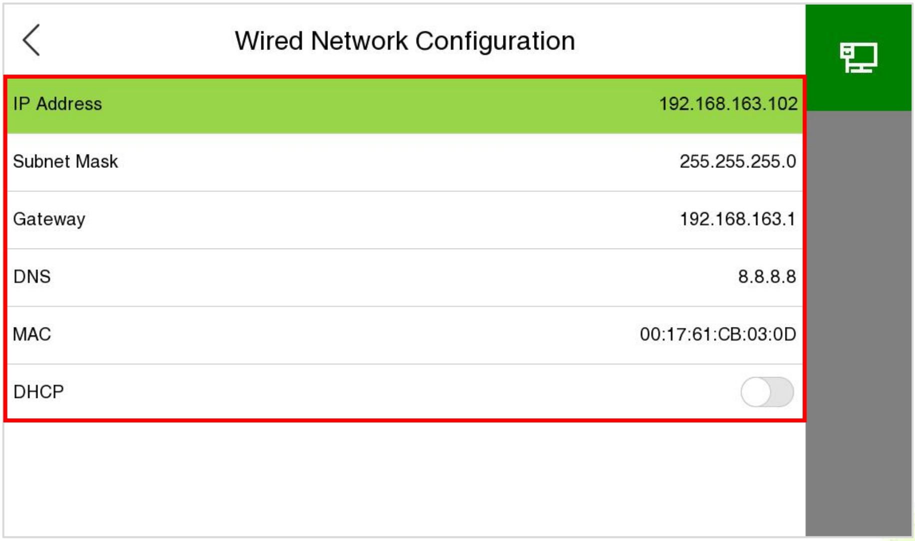
This function needs to be used with the indoor monitor VT07-B01.

- **On the Indoor Monitor:**

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



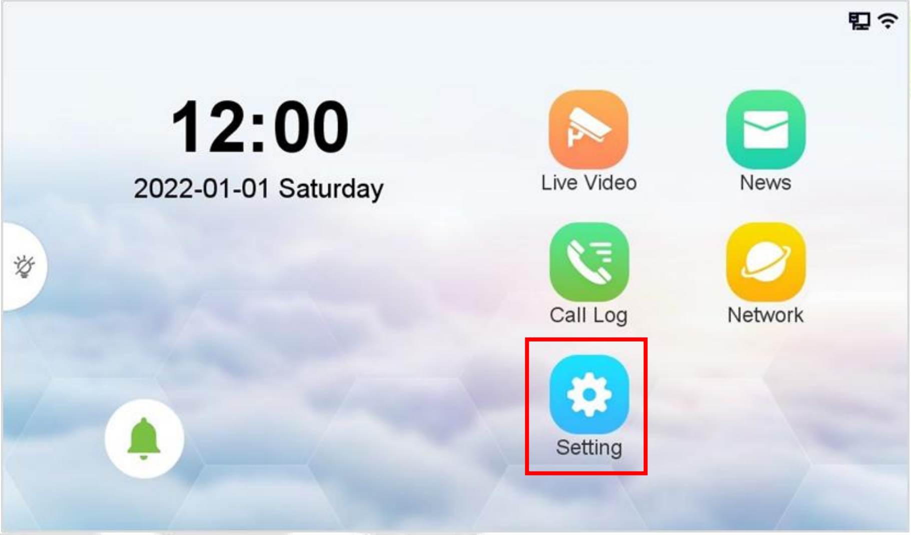
2. Set the IP Address and Gateway of the indoor monitor. (**Note:** The IP address should be in the same network segment as the device.)

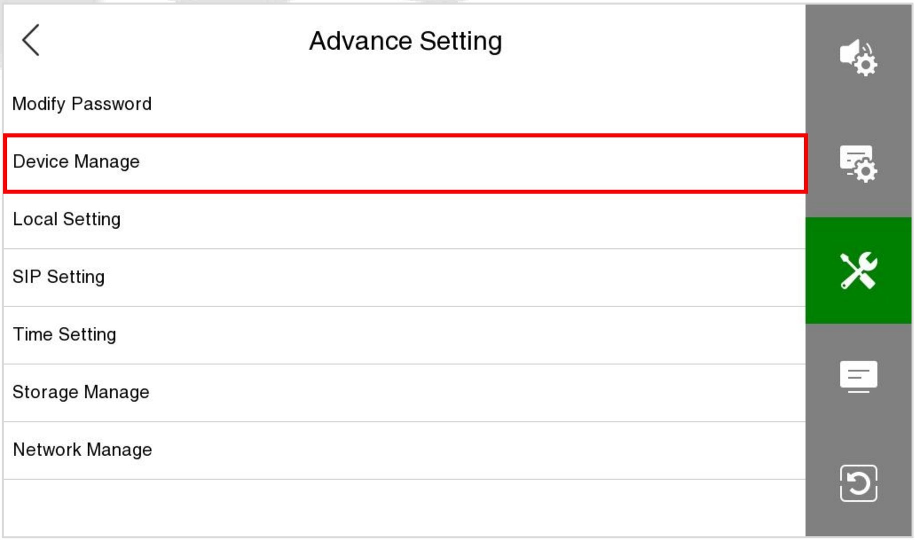


Wired Network Configuration

IP Address	192.168.163.102
Subnet Mask	255.255.255.0
Gateway	192.168.163.1
DNS	8.8.8.8
MAC	00:17:61:CB:03:0D
DHCP	○

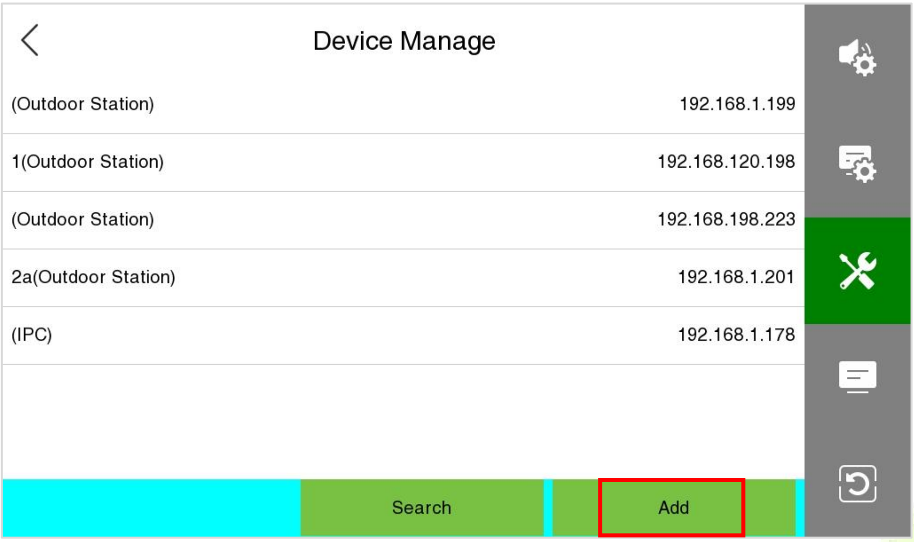
3. Tap **Setting** > 🛠 **Advance Setting** > **Device Manage** > **Add** to add the device.





Advance Setting

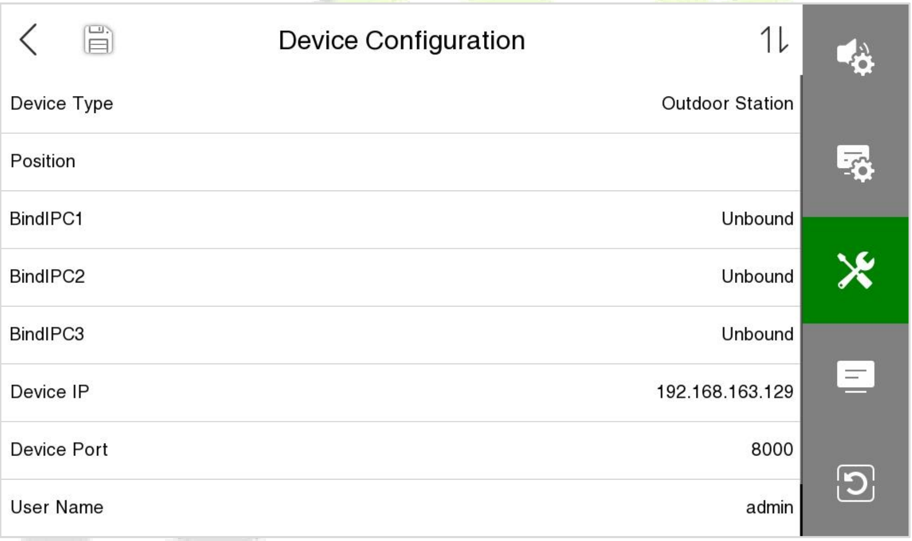
- Modify Password
- Device Manage
- Local Setting
- SIP Setting
- Time Setting
- Storage Manage
- Network Manage



Device Manage

(Outdoor Station)	192.168.1.199
1(Outdoor Station)	192.168.120.198
(Outdoor Station)	192.168.198.223
2a(Outdoor Station)	192.168.1.201
(IPC)	192.168.1.178

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.

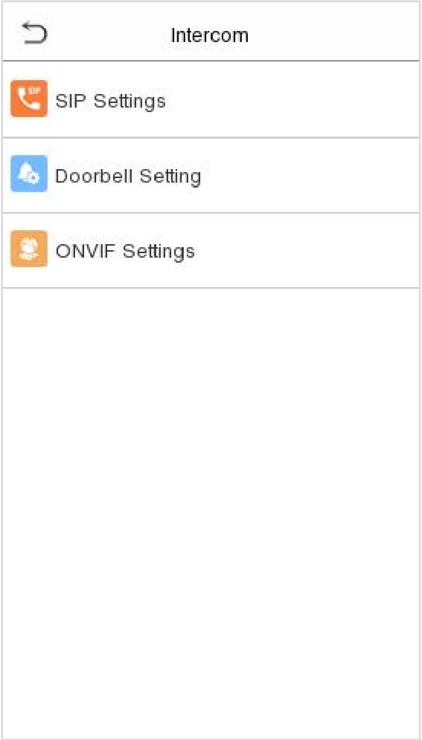


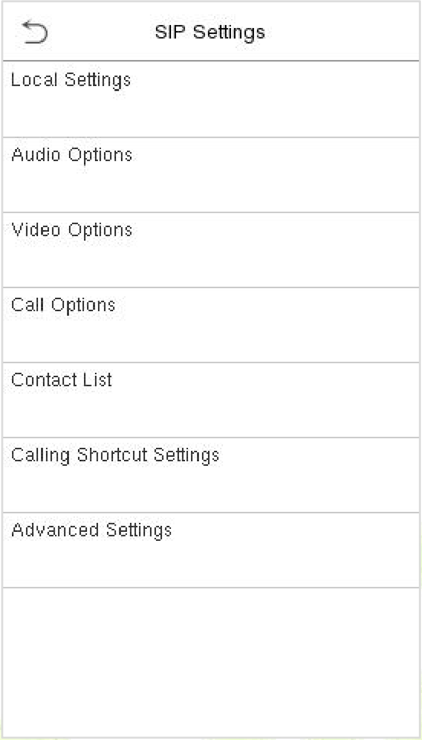
Device Configuration

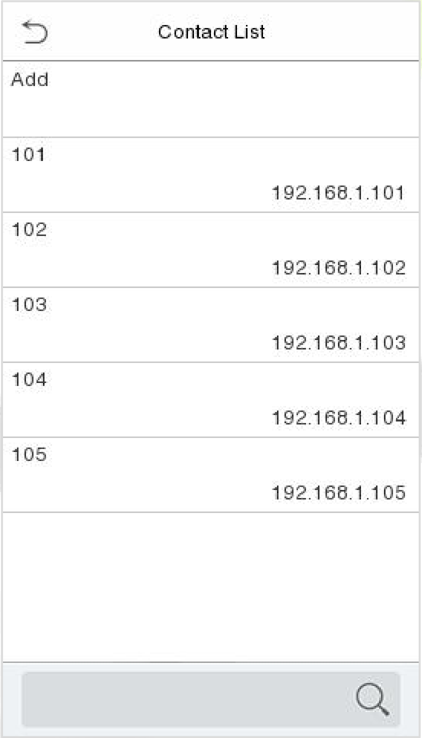
Device Type	Outdoor Station
Position	
BindIPC1	Unbound
BindIPC2	Unbound
BindIPC3	Unbound
Device IP	192.168.163.129
Device Port	8000
User Name	admin

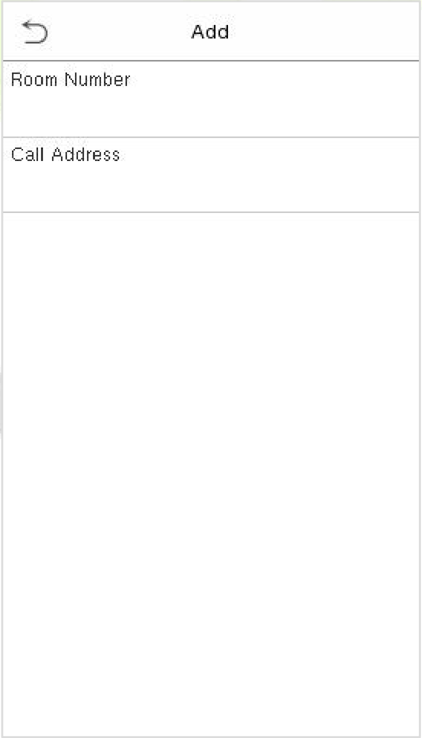
- **On the Device:**

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



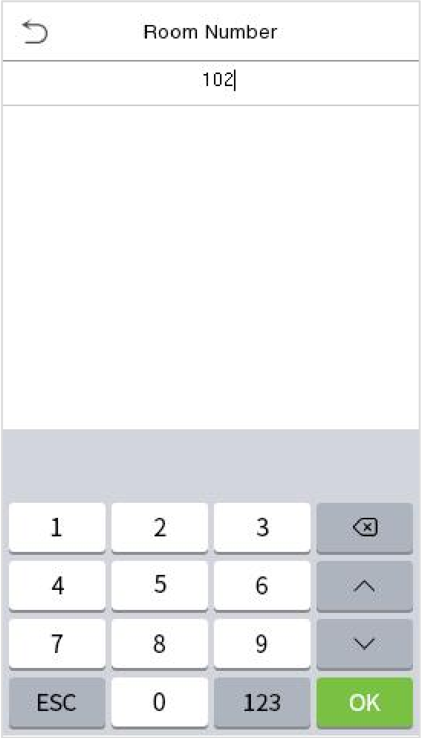




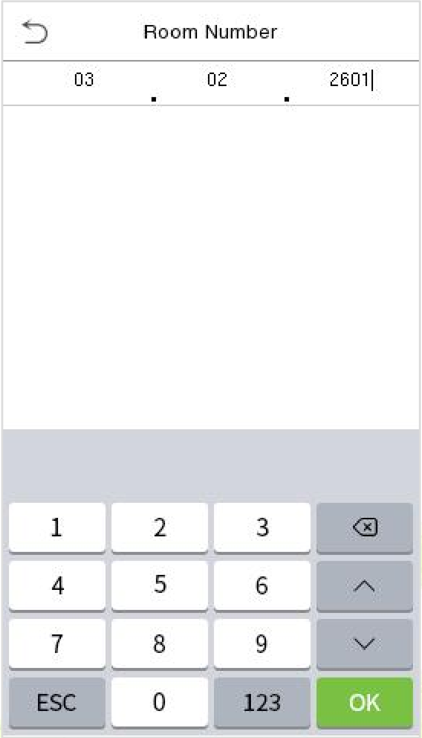


Room Number: Customize the number of the indoor monitor.

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”.



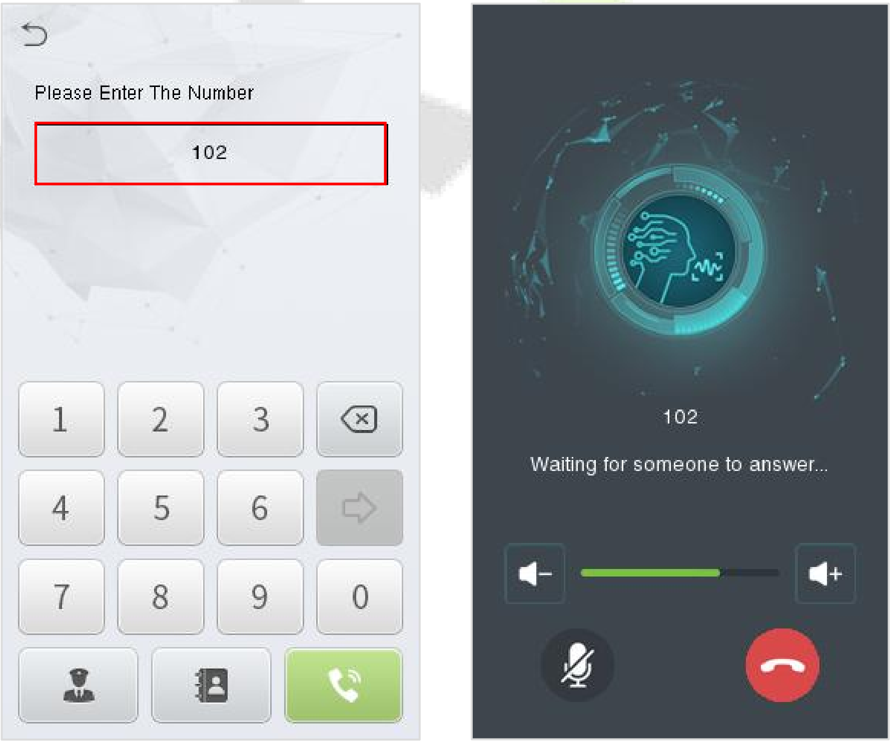
Entrance Station



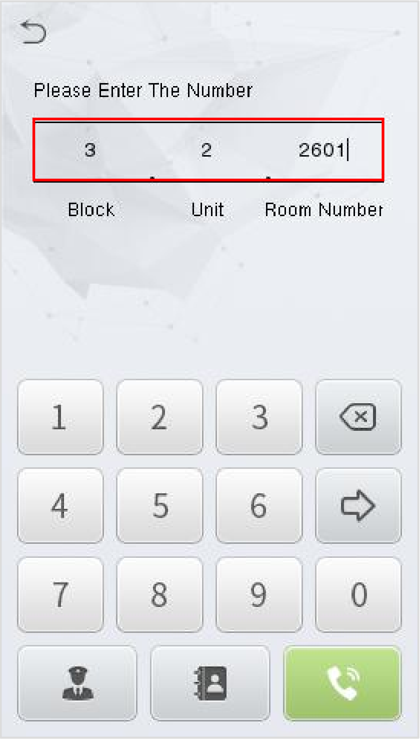
Fence Terminal

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.

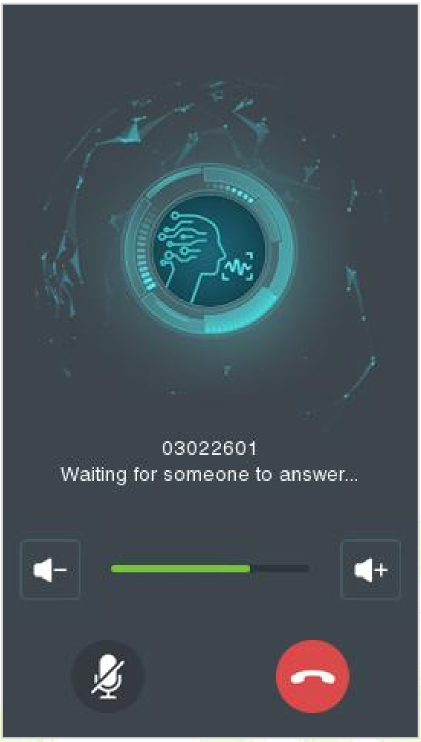


Entrance Station



Please Enter The Number

Block	Unit	Room Number
3	2	2601



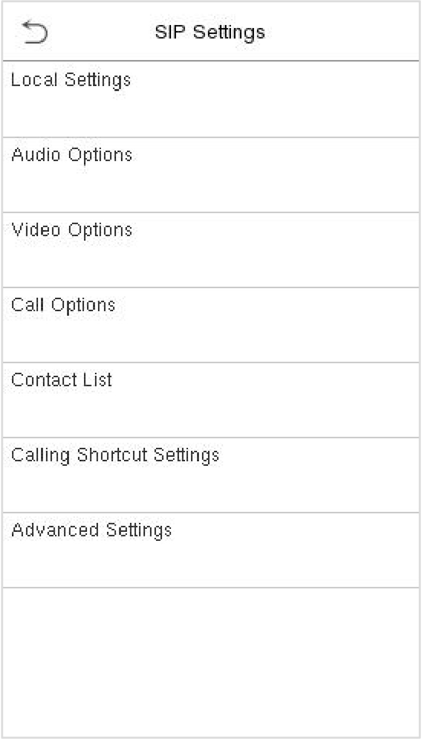
03022601

Waiting for someone to answer...

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.



SIP Settings

Local Settings

Audio Options

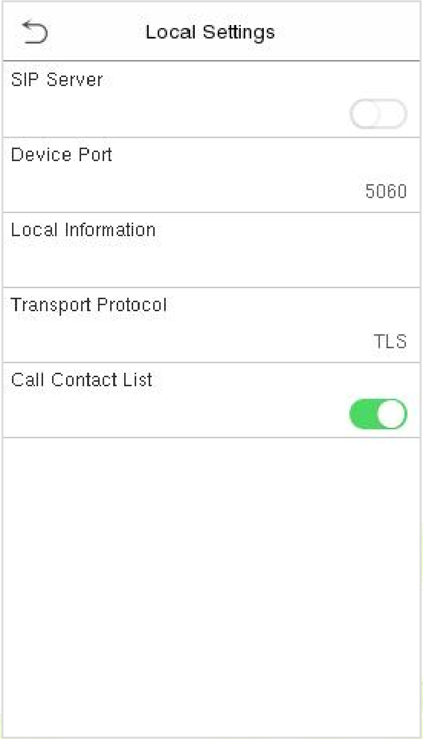
Video Options

Call Options

Contact List

Calling Shortcut Settings

Advanced Settings



Local Settings

SIP Server ○

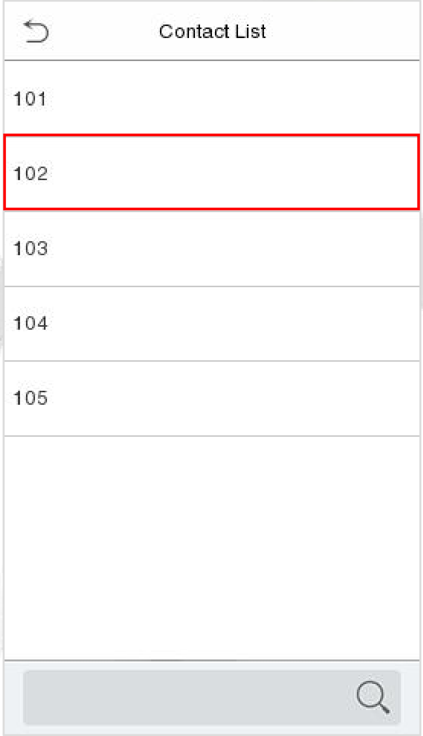
Device Port 5060

Local Information

Transport Protocol TLS

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.



Contact List

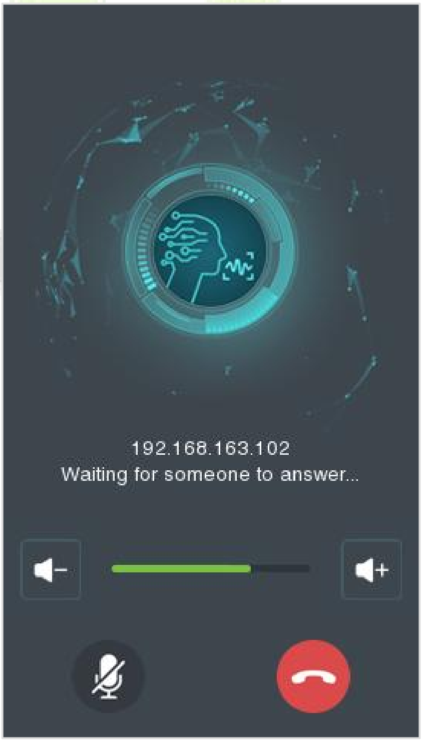
101

102

103

104

105

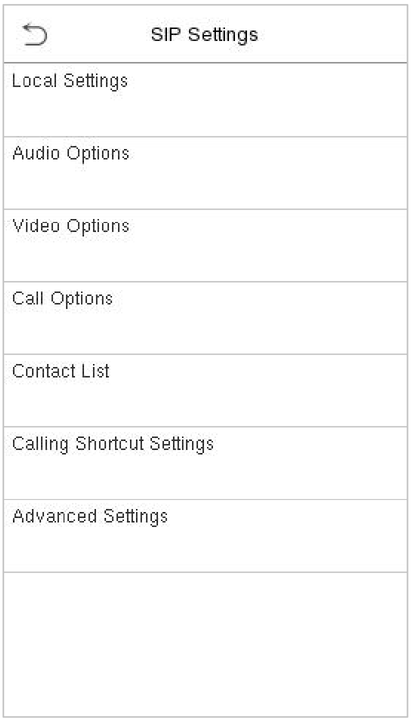


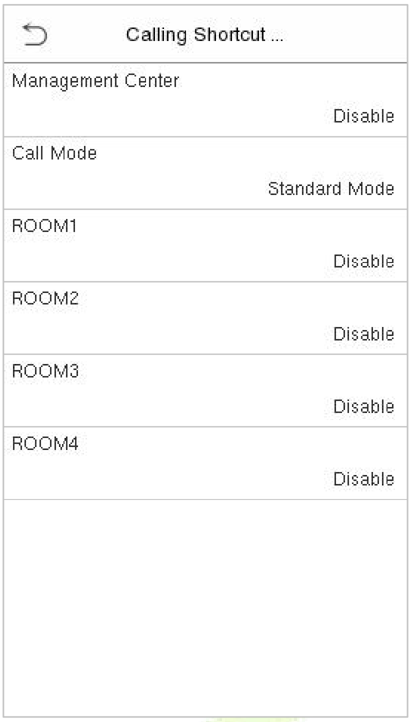
192.168.163.102

Waiting for someone to answer...

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.




Calling Shortcut ...

Management Center: Disable

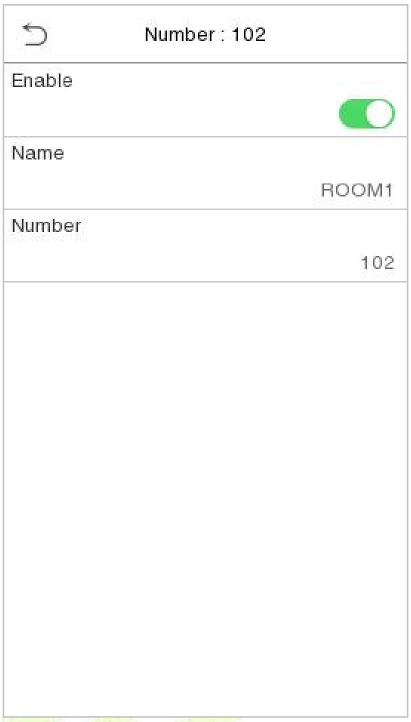
Call Mode: Standard Mode

ROOM1: Disable

ROOM2: Disable

ROOM3: Disable

ROOM4: Disable


Number : 102

Enable

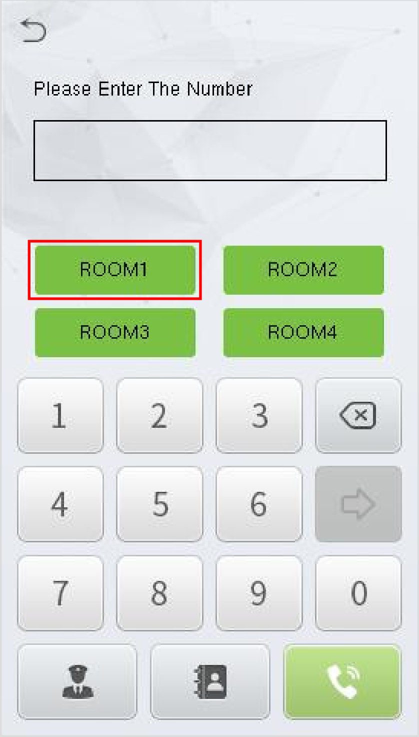
Name: ROOM1

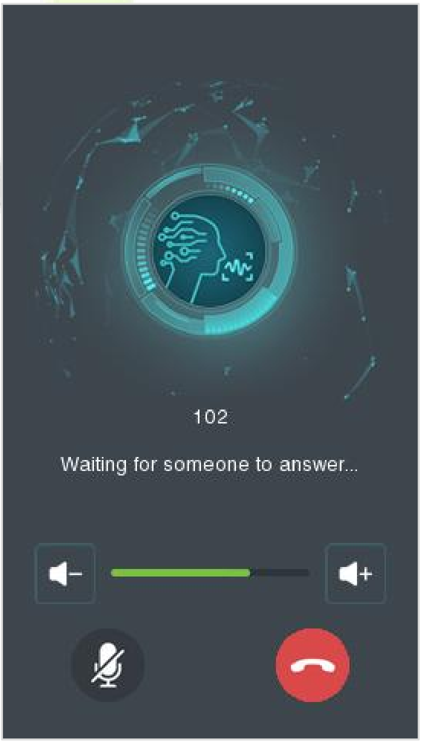
Number: 102

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.

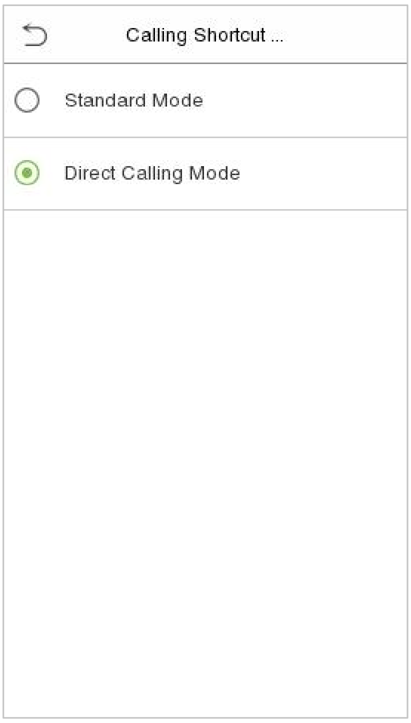



102

Waiting for someone to answer...

16.1.3 Direct Calling

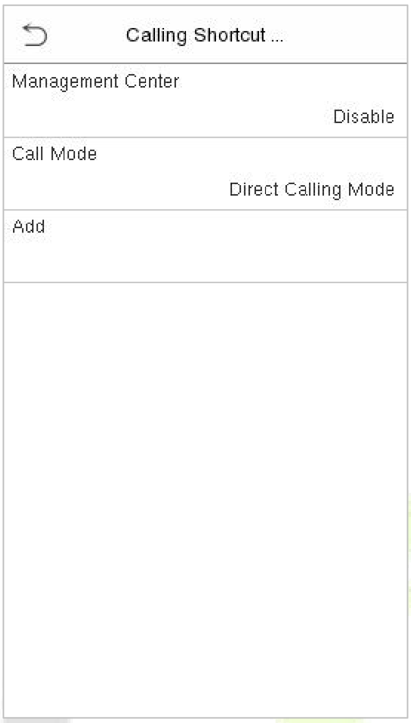
1. On the **SIP Settings** interface, click **Calling Shortcut Settings** > **Call Mode** > **Direct Calling Mode** > **Add**. Select the IP address of the indoor monitors that you want to call, then the indoor monitors will be displayed in the list.



Calling Shortcut ...

○ Standard Mode

● Direct Calling Mode

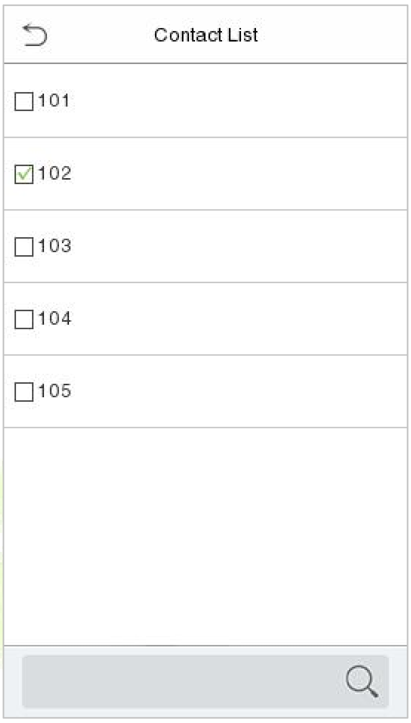


Calling Shortcut ...

Management Center
Disable

Call Mode
Direct Calling Mode

Add



Contact List

□101

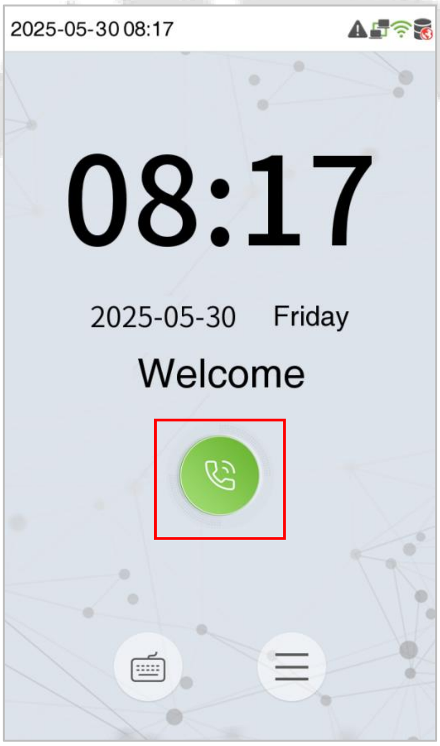
☑102

□103

□104

□105

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

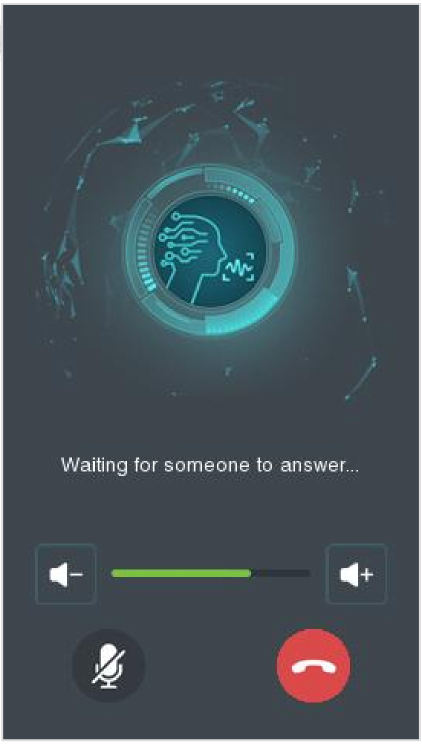


2025-05-30 08:17

08:17

2025-05-30 Friday

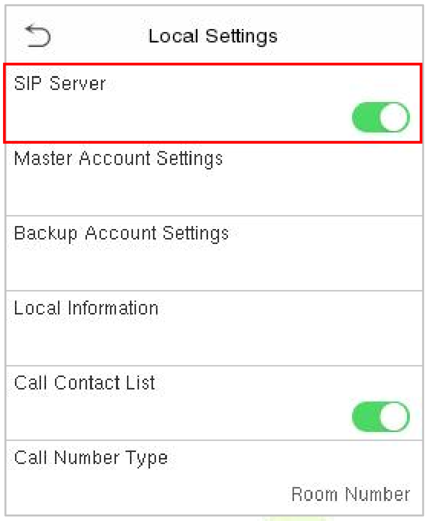
Welcome



Waiting for someone to answer...

16.2 SIP Server

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



SIP Server ●

Master Account Settings

Backup Account Settings

Local Information

Call Contact List ●

Call Number Type: Room Number

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

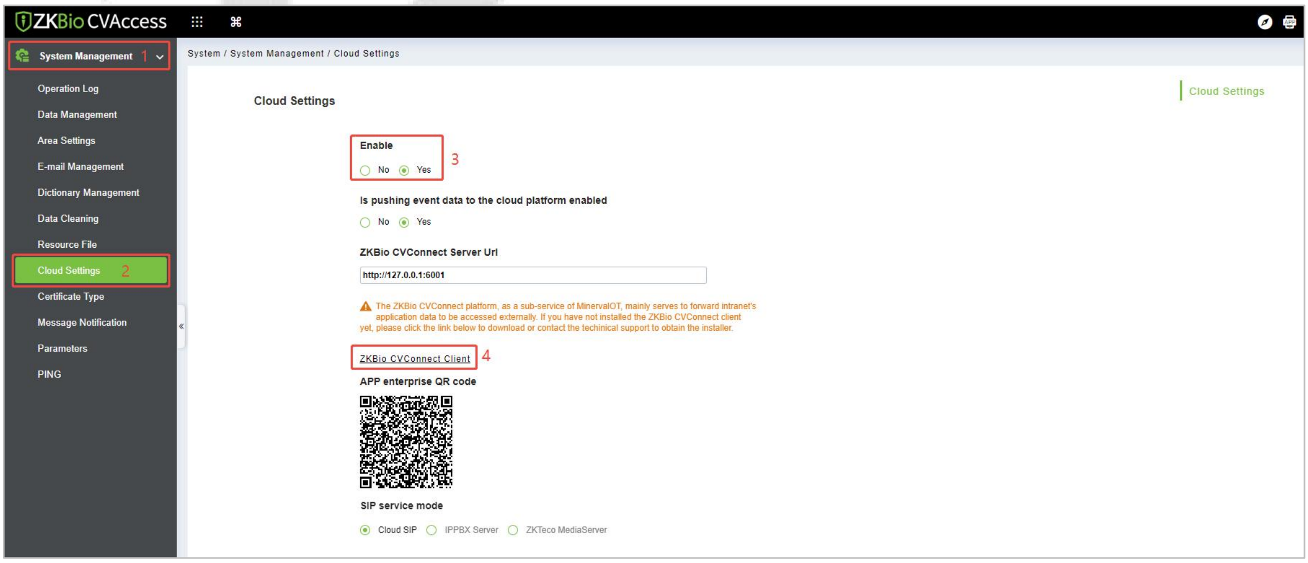
ZKBio CVAccess supports 2 kinds of SIP server: **cloud SIP** and **PBX server**, users can choose one according to the actual situation.

- **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.



Cloud Settings

Enable
○ No ● Yes

Is pushing event data to the cloud platform enabled
○ No ● Yes

ZKBio CVConnect Server Url
http://127.0.0.1:6001

⚠ The ZKBio CVConnect platform, as a sub-service of MinervalOT, mainly serves to forward intranet's application data to be accessed externally. If you have not installed the ZKBio CVConnect client yet, please click the link below to download or contact the techinical support to obtain the installer.

ZKBio CVConnect Client

APP enterprise QR code

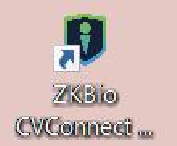
SIP service mode
● Cloud SIP ○ IPPBX Server ○ ZKTeco MediaServer

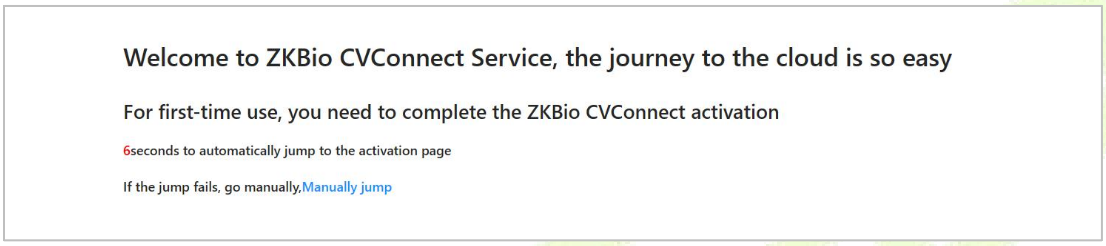
Note:

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.





Welcome to ZKBio CVConnect Service, the journey to the cloud is so easy

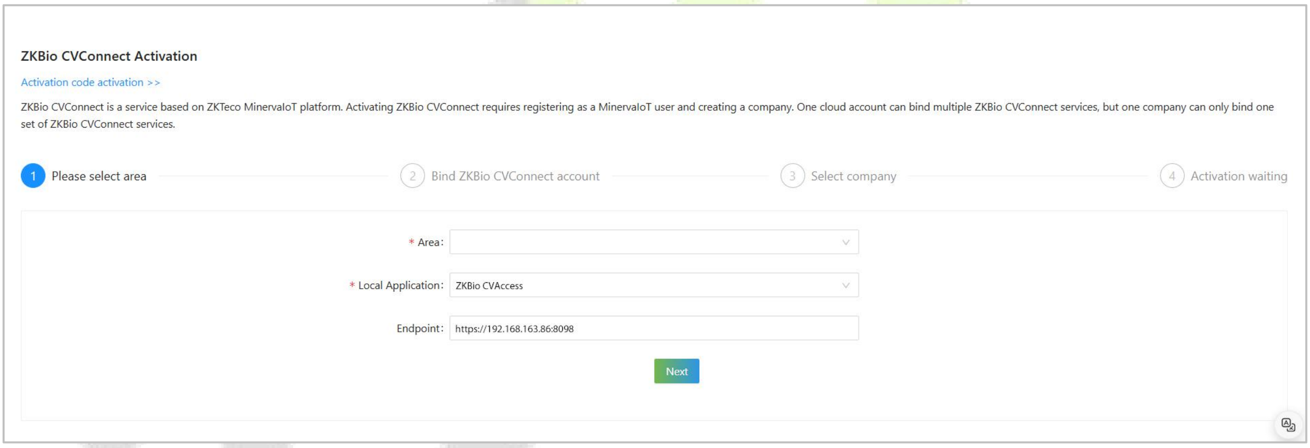
For first-time use, you need to complete the ZKBio CVConnect activation

6seconds to automatically jump to the activation page

If the jump fails, go manually,Manually jump

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

1. Select Area



ZKBio CVConnect Activation

Activation code activation >>

ZKBio CVConnect is a service based on ZKTeco MinervaIoT platform. Activating ZKBio CVConnect requires registering as a MinervaIoT user and creating a company. One cloud account can bind multiple ZKBio CVConnect services, but one company can only bind one set of ZKBio CVConnect services.

1 Please select area — 2 Bind ZKBio CVConnect account — 3 Select company — 4 Activation waiting

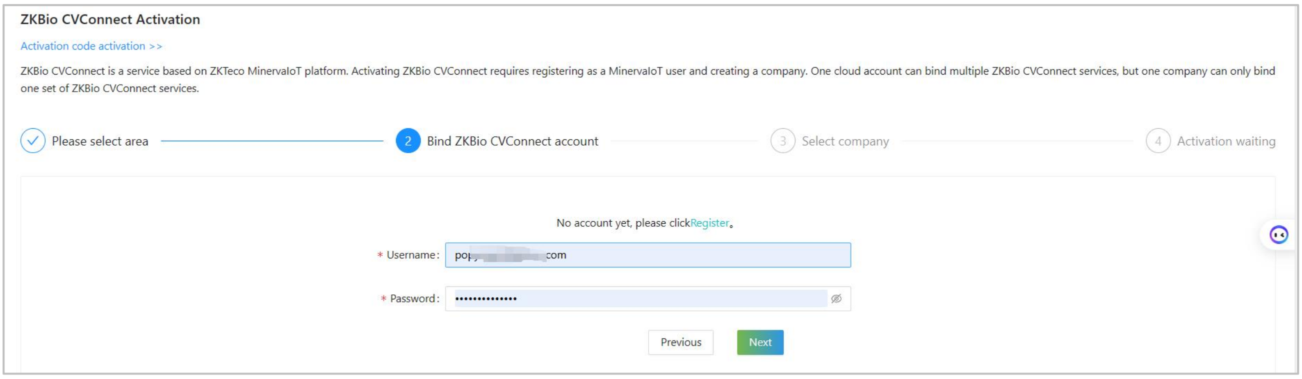
* Area:

* Local Application: ZKBio CVAccess

Endpoint: https://192.168.163.86:8098

- **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



ZKBio CVConnect Activation

Activation code activation >>

ZKBio CVConnect is a service based on ZKTeco MinervaIoT platform. Activating ZKBio CVConnect requires registering as a MinervaIoT user and creating a company. One cloud account can bind multiple ZKBio CVConnect services, but one company can only bind one set of ZKBio CVConnect services.

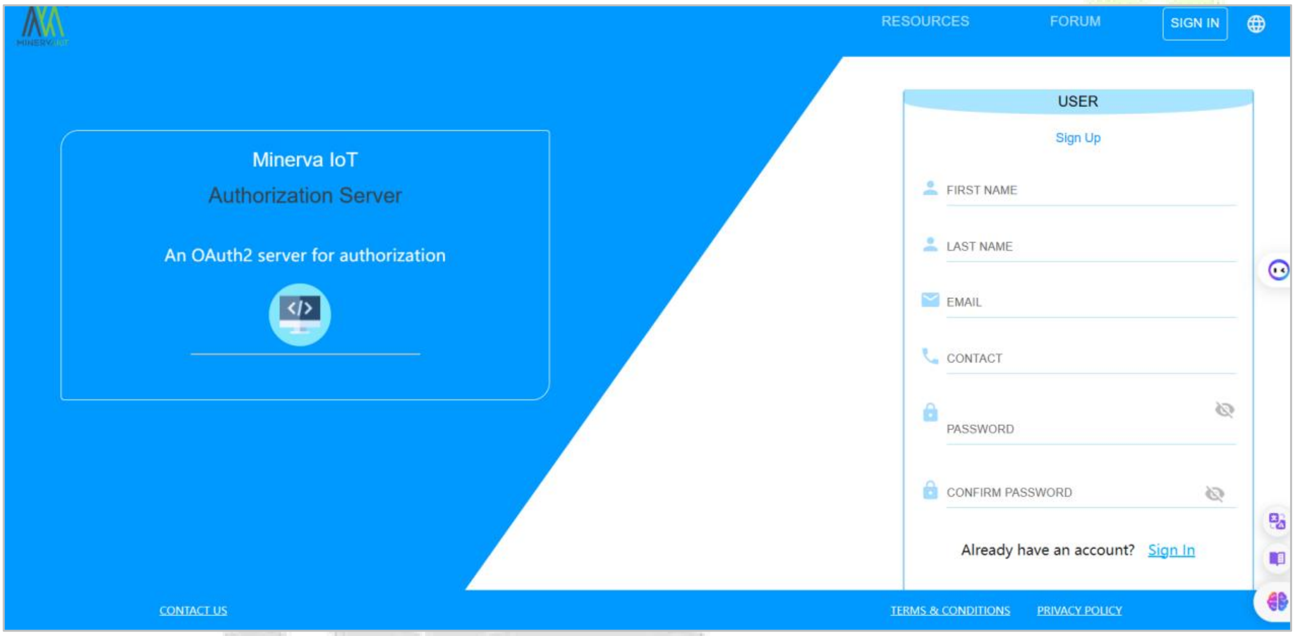
✓ Please select area — 2 Bind ZKBio CVConnect account — 3 Select company — 4 Activation waiting

No account yet, please clickRegister。

* Username: pop[redacted]com

* Password: ••••••••••••••

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.



Minerva IoT

Authorization Server

An OAuth2 server for authorization

USER

Sign Up

FIRST NAME

LAST NAME

EMAIL

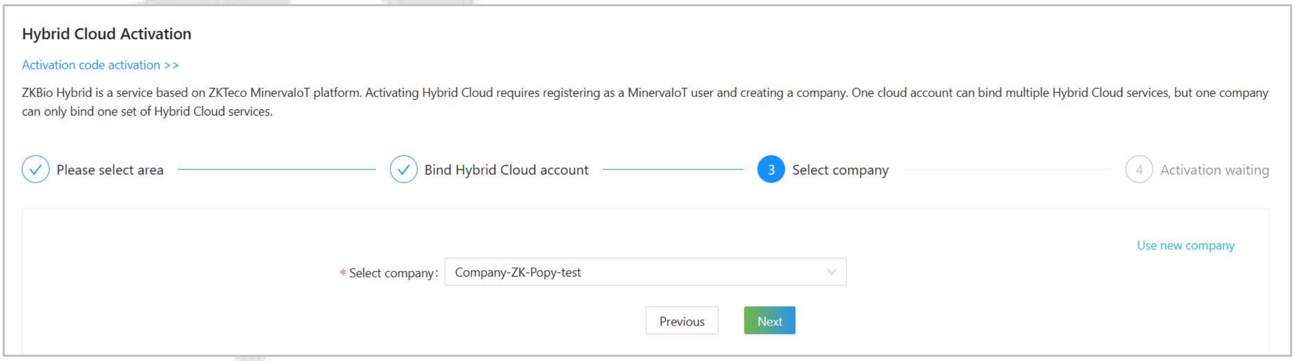
CONTACT

PASSWORD

CONFIRM PASSWORD

Already have an account? Sign In

3. Select Company



Hybrid Cloud Activation

Activation code activation >>

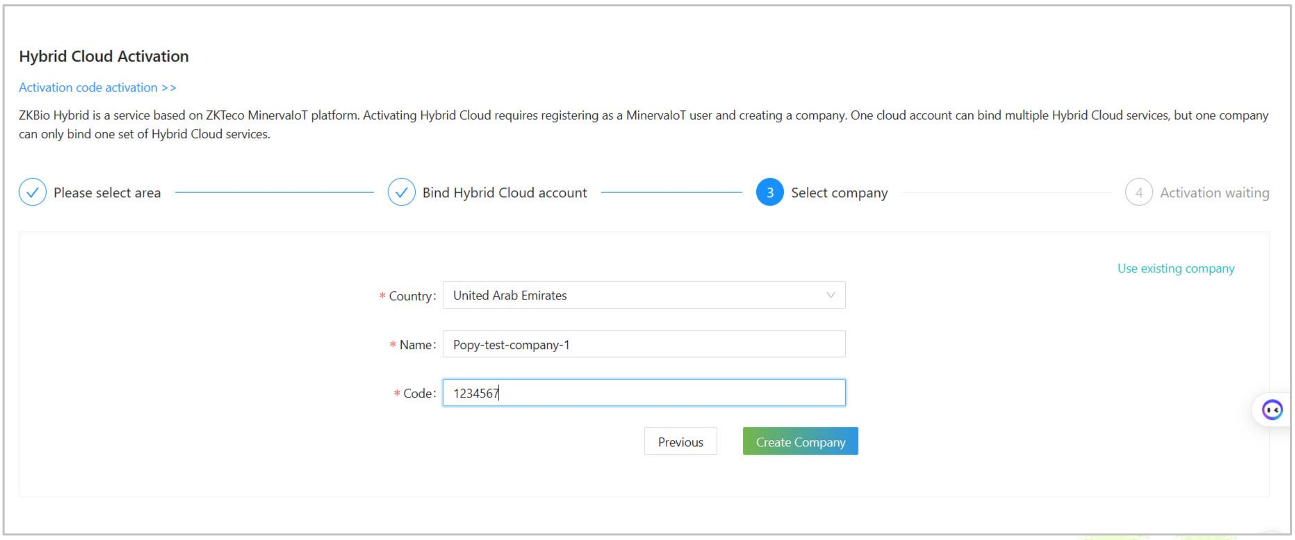
ZKBio Hybrid is a service based on ZKTeco MinervaIoT platform. Activating Hybrid Cloud requires registering as a MinervaIoT user and creating a company. One cloud account can bind multiple Hybrid Cloud services, but one company can only bind one set of Hybrid Cloud services.

✓ Please select area — ✓ Bind Hybrid Cloud account — 3 Select company — 4 Activation waiting

Use new company

* Select company: Company-ZK-Popy-test

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



Hybrid Cloud Activation

Activation code activation >>

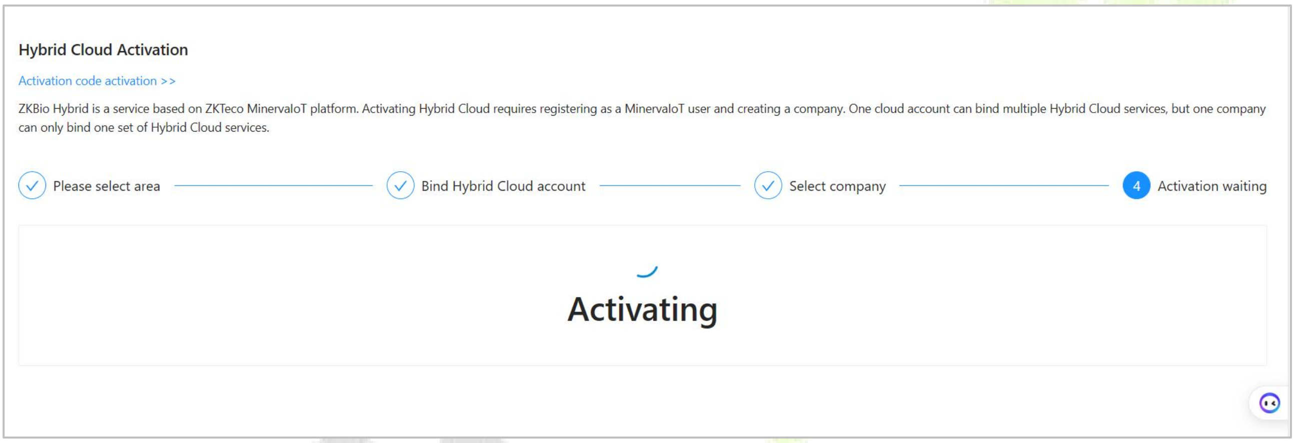
ZKBio Hybrid is a service based on ZKTeco MinervaloT platform. Activating Hybrid Cloud requires registering as a MinervaloT user and creating a company. One cloud account can bind multiple Hybrid Cloud services, but one company can only bind one set of Hybrid Cloud services.

* Country: United Arab Emirates

* Name: Popy-test-company-1

* Code: 1234567

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



Hybrid Cloud Activation

Activation code activation >>

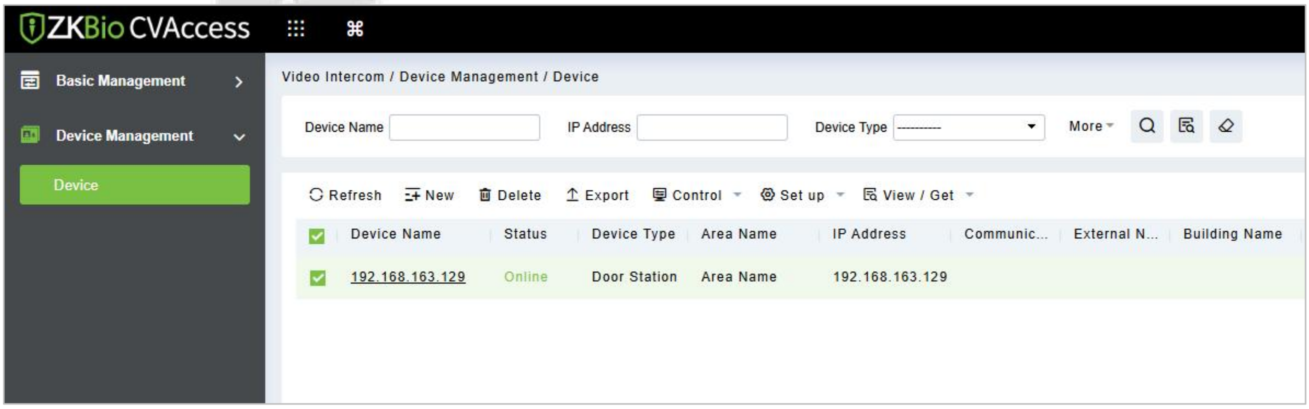
ZKBio Hybrid is a service based on ZKTeco MinervaloT platform. Activating Hybrid Cloud requires registering as a MinervaloT user and creating a company. One cloud account can bind multiple Hybrid Cloud services, but one company can only bind one set of Hybrid Cloud services.

Activating

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](#))

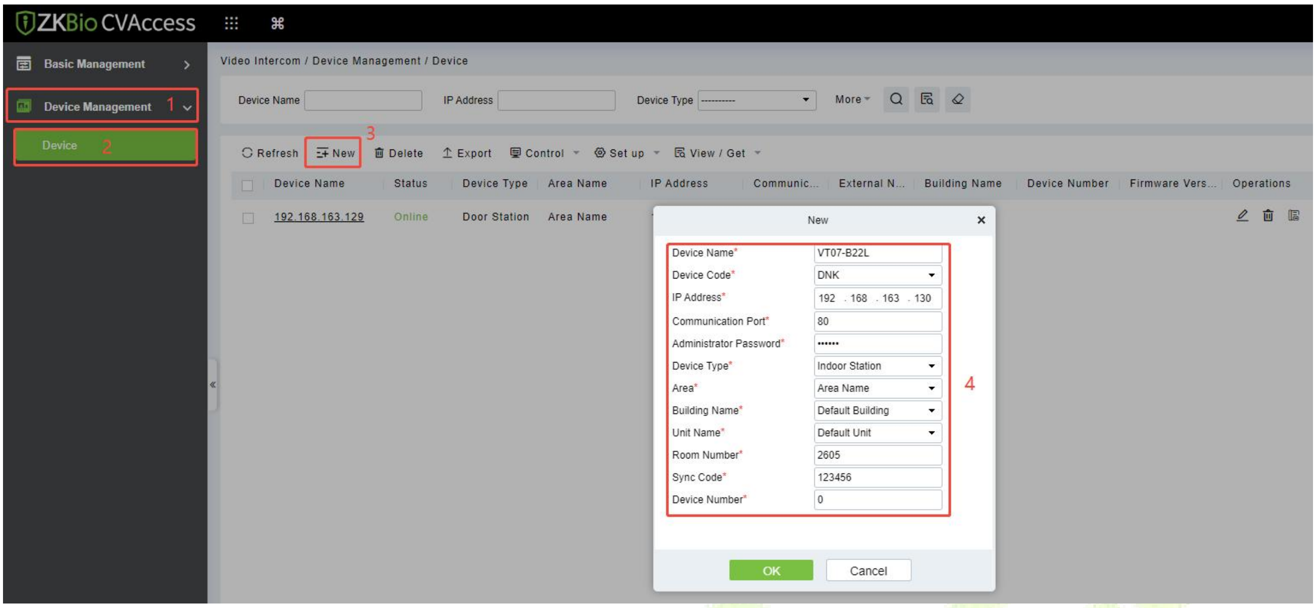


Video Intercom / Device Management / Device

Device Name | IP Address | Device Type ---------- | More

☑	Device Name	Status	Device Type	Area Name	IP Address	Communic...	External N...	Building Name
☑	192.168.163.129	Online	Door Station	Area Name	192.168.163.129			

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



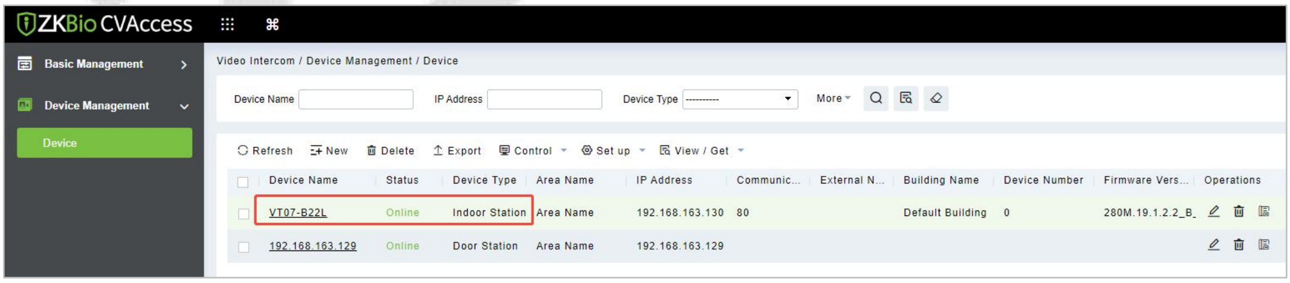
Device Name	Status	Device Type	Area Name	IP Address	Communic...	External N...	Building Name	Device Number	Firmware Vers...	Operations
192.168.163.129	Online	Door Station	Area Name							

New

Device Name*	VT07-B22L
Device Code*	DNK
IP Address*	192 . 168 . 163 . 130
Communication Port*	80
Administrator Password*	••••••
Device Type*	Indoor Station
Area*	Area Name
Building Name*	Default Building
Unit Name*	Default Unit
Room Number*	2605
Sync Code*	123456
Device Number*	0

- **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.

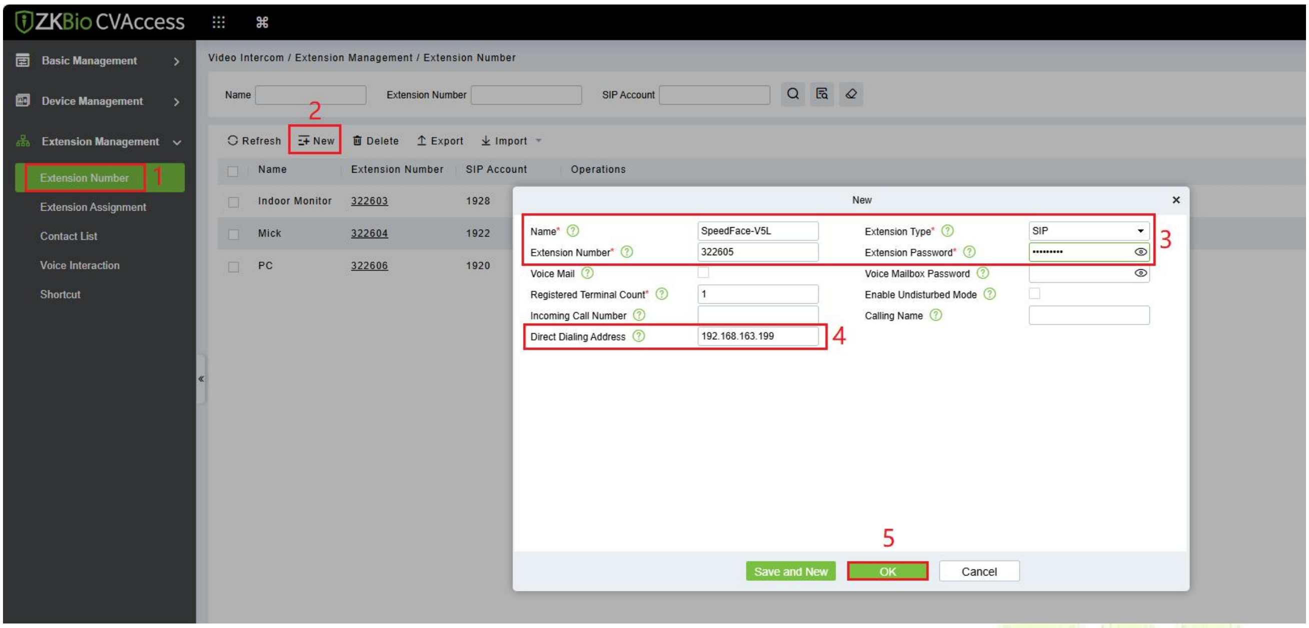
After the addition is successful, the indoor monitor will be displayed in the device list.



Device Name	Status	Device Type	Area Name	IP Address	Communic...	External N...	Building Name	Device Number	Firmware Vers...	Operations
VT07-B22L	Online	Indoor Station	Area Name	192.168.163.130	80		Default Building	0	280M.19.1.2.2_B_	
192.168.163.129	Online	Door Station	Area Name	192.168.163.129						

16.2.3 Create Extension Numbers

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



ZKBio CVAccess

Basic Management
Device Management
Extension Management
Extension Number
Extension Assignment
Contact List
Voice Interaction
Shortcut

Video Intercom / Extension Management / Extension Number

Name | Extension Number | SIP Account

Refresh | New | Delete | Export | Import

Name	Extension Number	SIP Account	Operations
Indoor Monitor	322603	1928	
Mick	322604	1922	
PC	322606	1920	

New

Name*	SpeedFace-V5L	Extension Type*	SIP
Extension Number*	322605	Extension Password*	••••••••
Voice Mail	□	Voice Mailbox Password	
Registered Terminal Count*	1	Enable Undisturbed Mode	□
Incoming Call Number		Calling Name	
Direct Dialing Address	192.168.163.199		

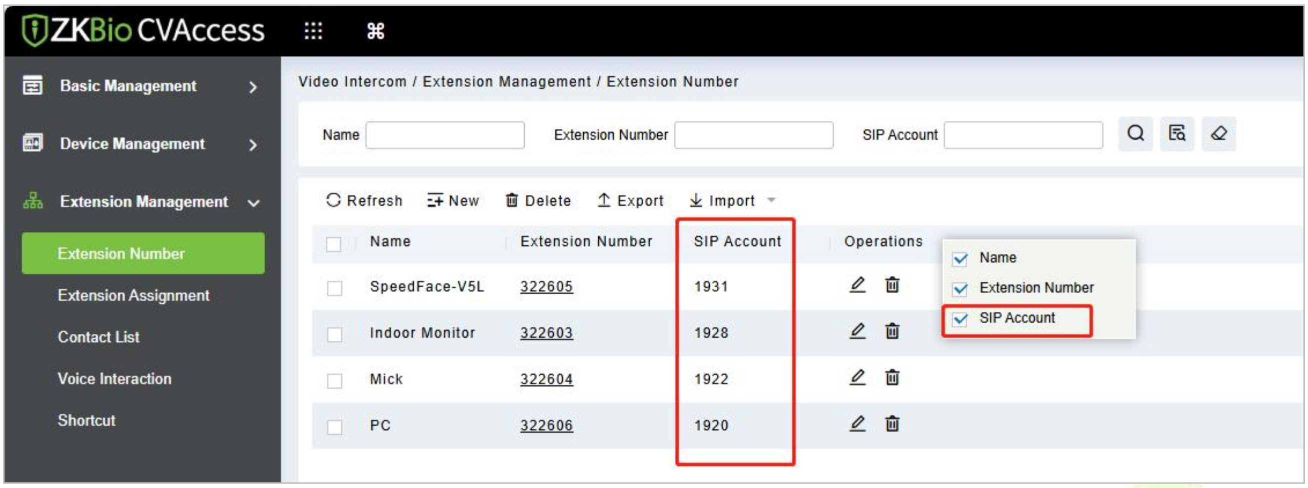
Save and New | OK | Cancel

- **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.
- **Direct Dialing Address:** Enter the IP address of the relevant device or indoor monitor. The IP address of the point-to-point calling device in the LAN; after entering the IP address here, you can directly enter the extension number to call the corresponding IP address when making a call. When there is no extension number assigned, you can make a call by entering the corresponding IP address.

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.



Video Intercom / Extension Management / Extension Number

Name | Extension Number | SIP Account

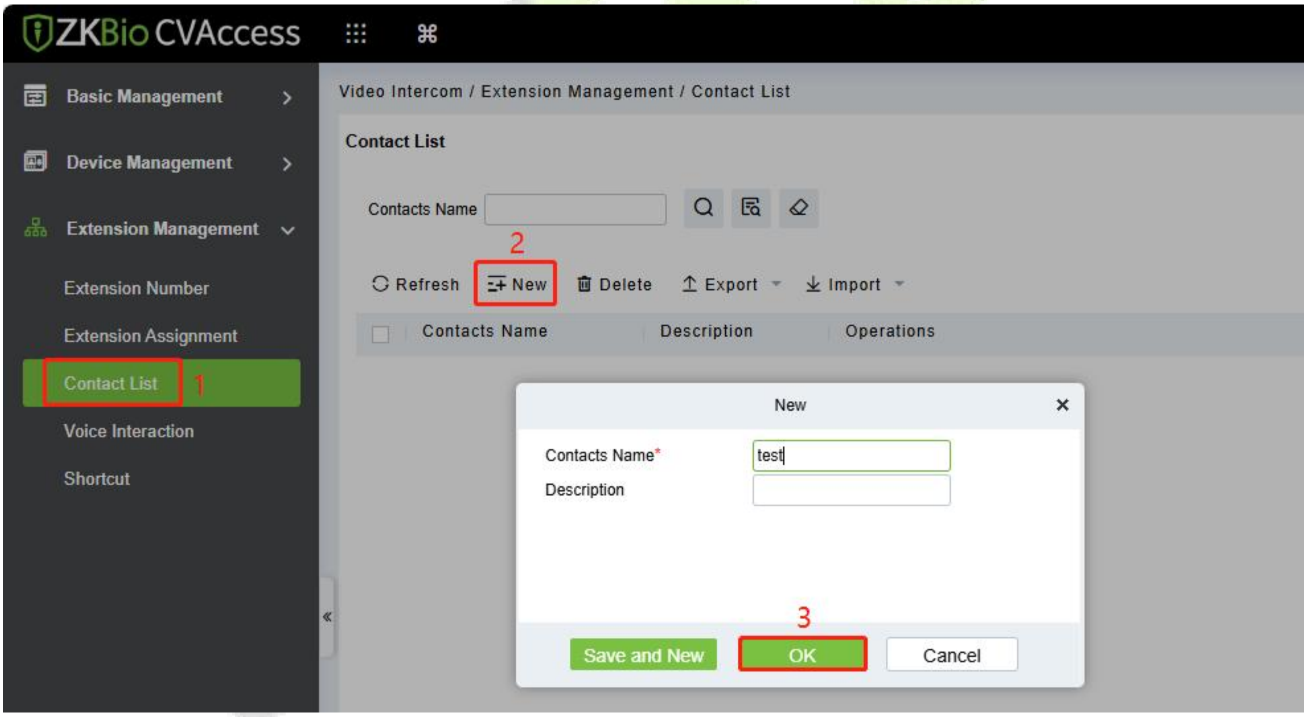
□	Name	Extension Number	SIP Account	Operations
□	SpeedFace-V5L	322605	1931	
□	Indoor Monitor	322603	1928	
□	Mick	322604	1922	
□	PC	322606	1920	

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.



Video Intercom / Extension Management / Contact List

Contact List

Contacts Name

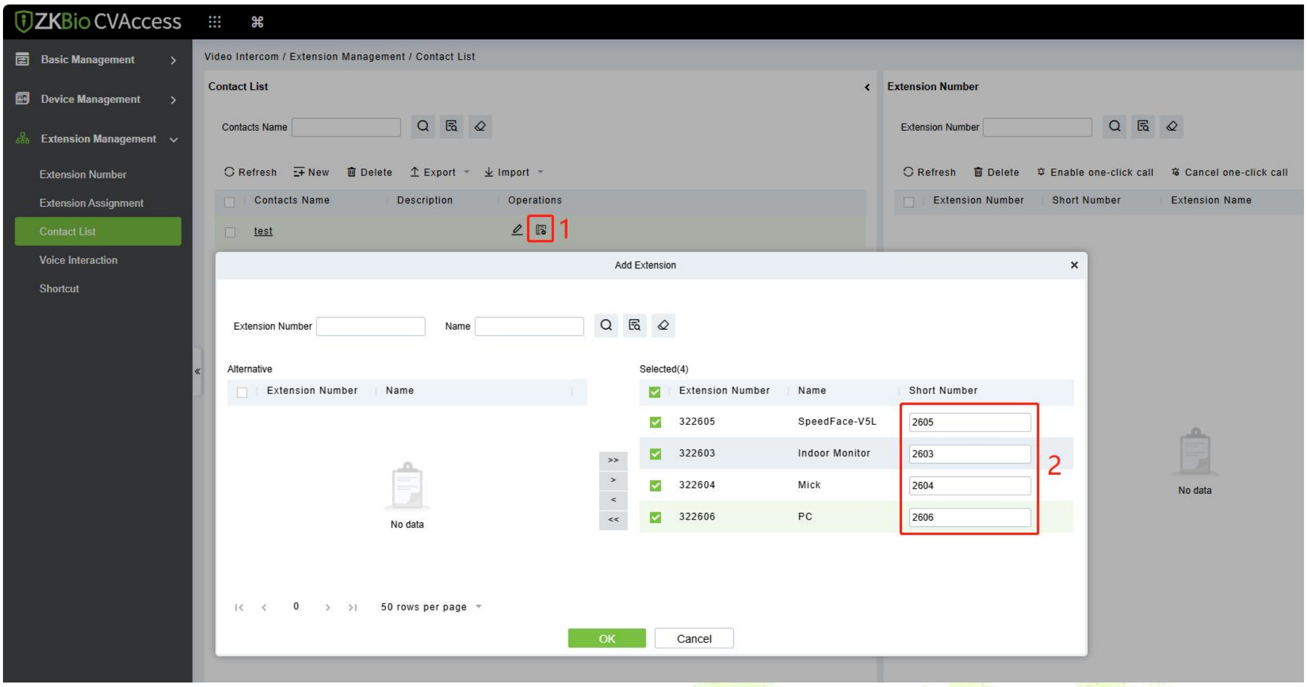
□	Contacts Name	Description	Operations

New

Contacts Name* test

Description

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.



Selected(4)

☑	Extension Number	Name	Short Number
☑	322605	SpeedFace-V5L	2605
☑	322603	Indoor Monitor	2603
☑	322604	Mick	2604
☑	322606	PC	2606

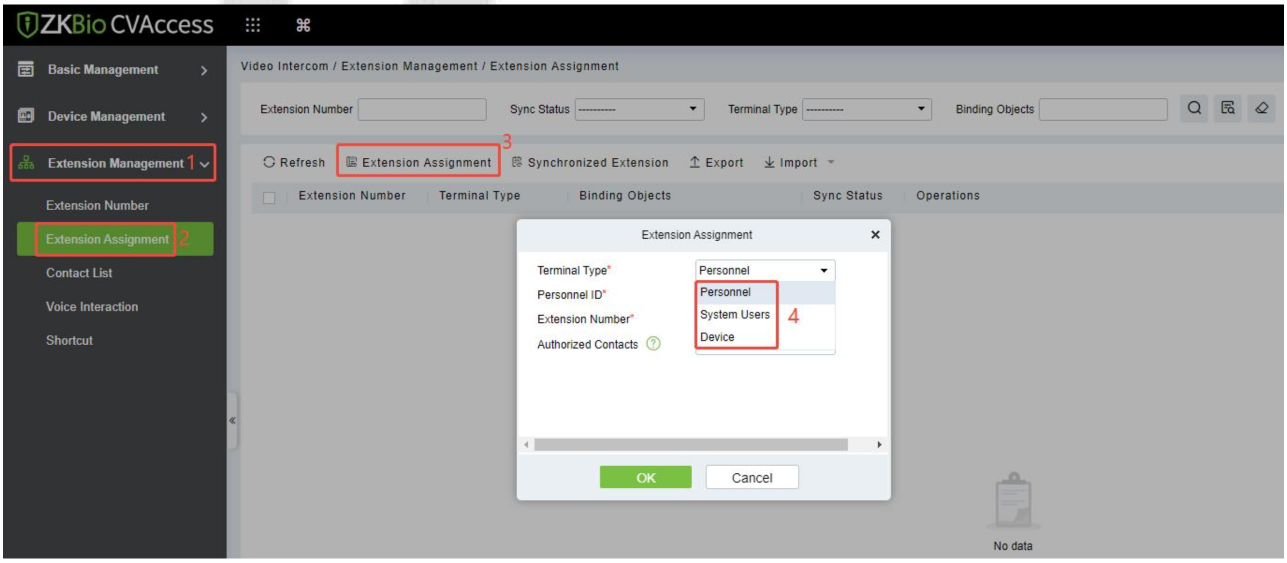
Note:

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.



Terminal Type* Personnel

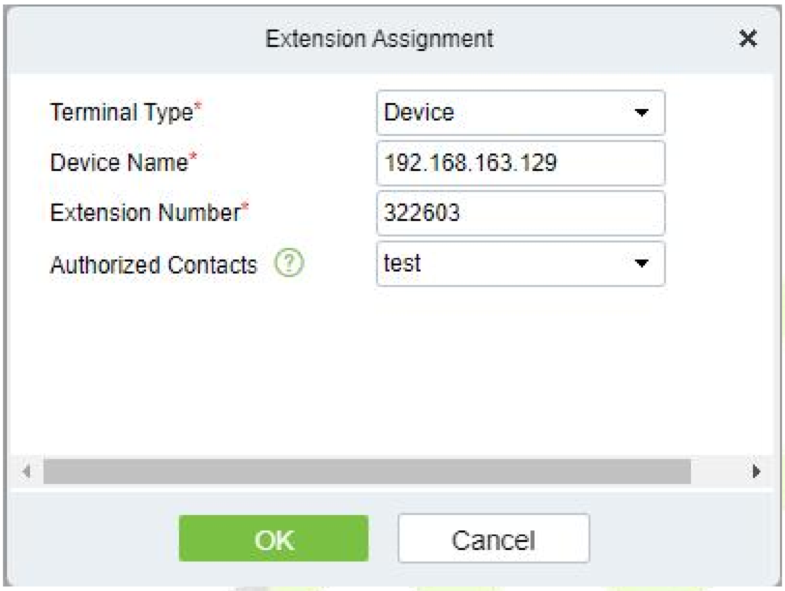
Personnel ID*

Extension Number*

Authorized Contacts

- **Device Account Assignment**

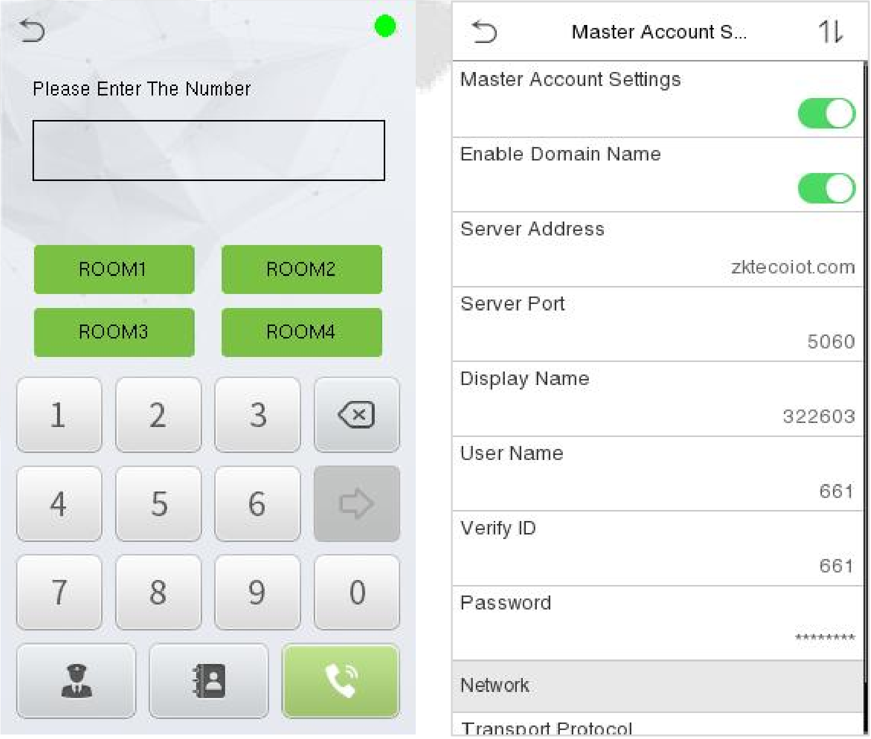
1. Select the Terminal Type as **Device**.
2. Select the device need to be bound (device or indoor monitor) and the extension number. The account information will be automatically synchronized to the device. Select the Authorized Contacts to assign the contact list to the device; only after the assignment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



Extension Assignment

Terminal Type*	Device
Device Name*	192.168.163.129
Extension Number*	322603
Authorized Contacts	test

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.

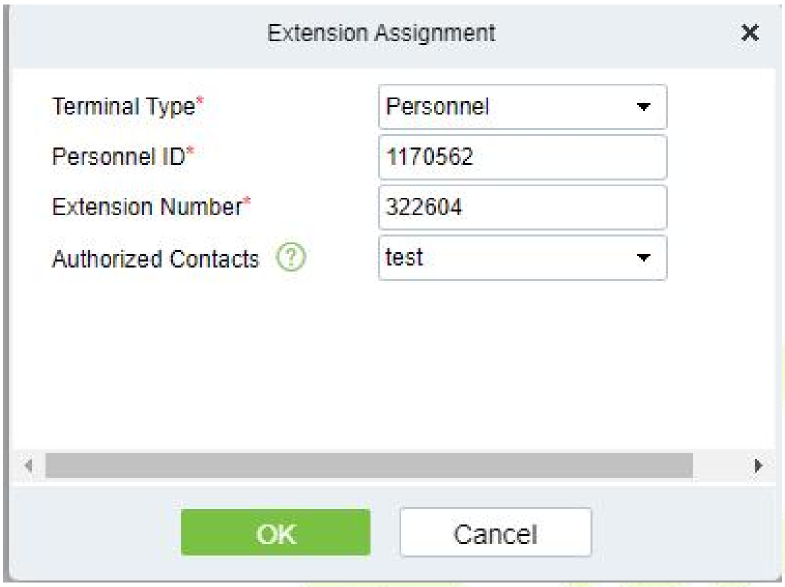


Master Account S...

Master Account Settings	On
Enable Domain Name	On
Server Address	zktecoiot.com
Server Port	5060
Display Name	322603
User Name	661
Verify ID	661
Password	********

- **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.



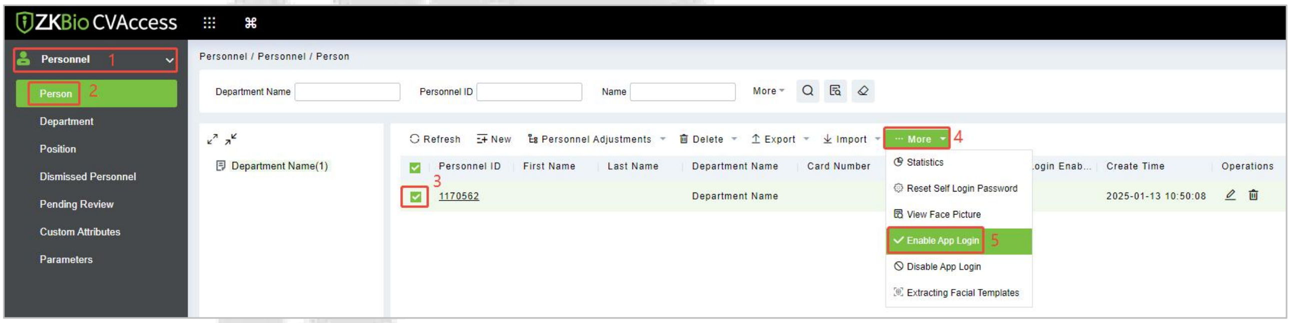
Extension Assignment

Terminal Type*	Personnel
Personnel ID*	1170562
Extension Number*	322604
Authorized Contacts	test

Note:

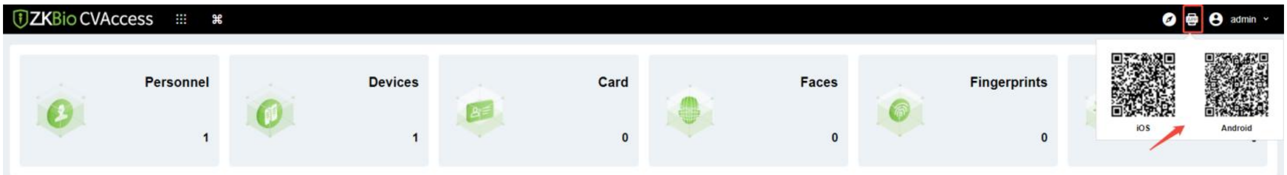
1) Before assign account to the personnel, you need first add personnel in ZKBio CVAccess. The adding method can refer to 15 Connect to ZKBio CVAccess Software.

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.

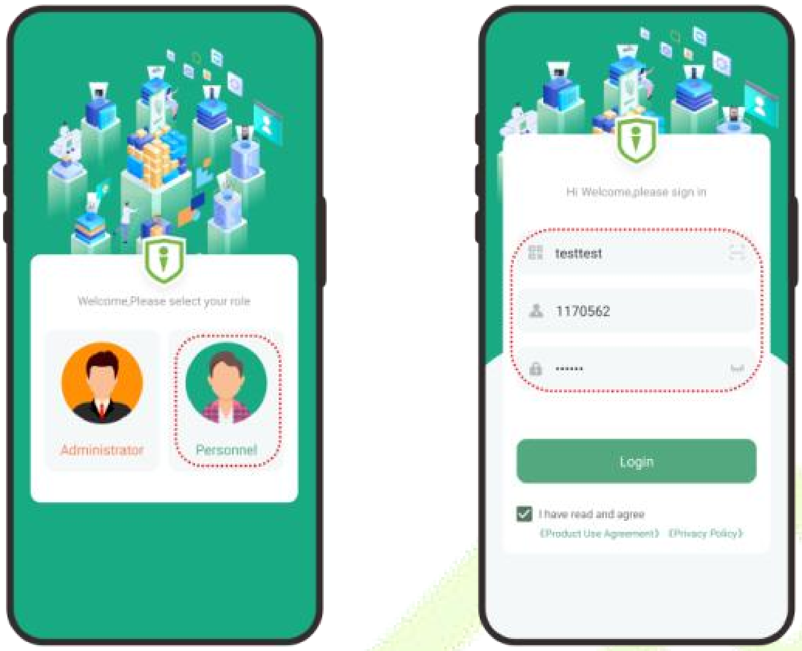


☑	Personnel ID	First Name	Last Name	Department Name	Card Number	...ogin Enab...	Create Time	Operations
☑	1170562			Department Name			2025-01-13 10:50:08	

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**.



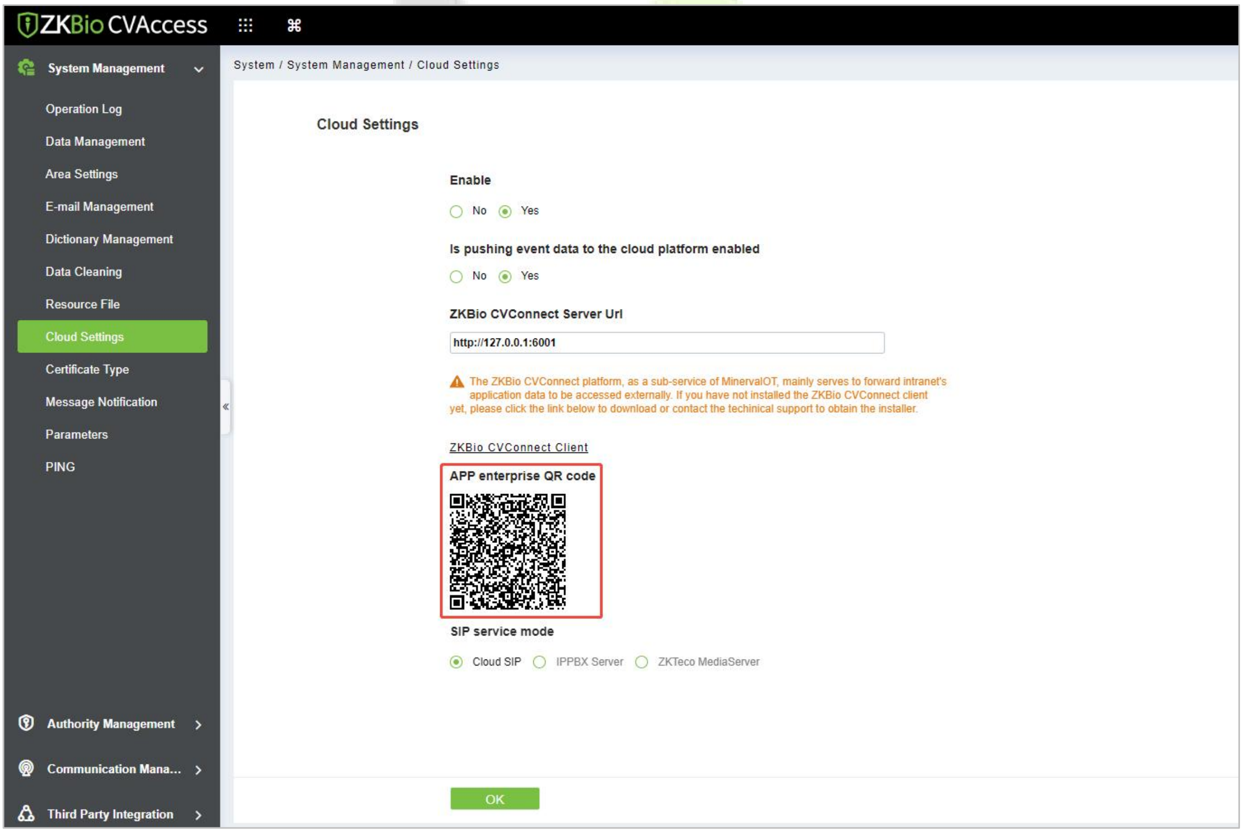
testtest

1170562

••••••

☑ I have read and agree 《Product Use Agreement》《Privacy Policy》

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.)



Cloud Settings

Enable

○ No ● Yes

Is pushing event data to the cloud platform enabled

○ No ● Yes

ZKBio CVConnect Server Url

http://127.0.0.1:6001

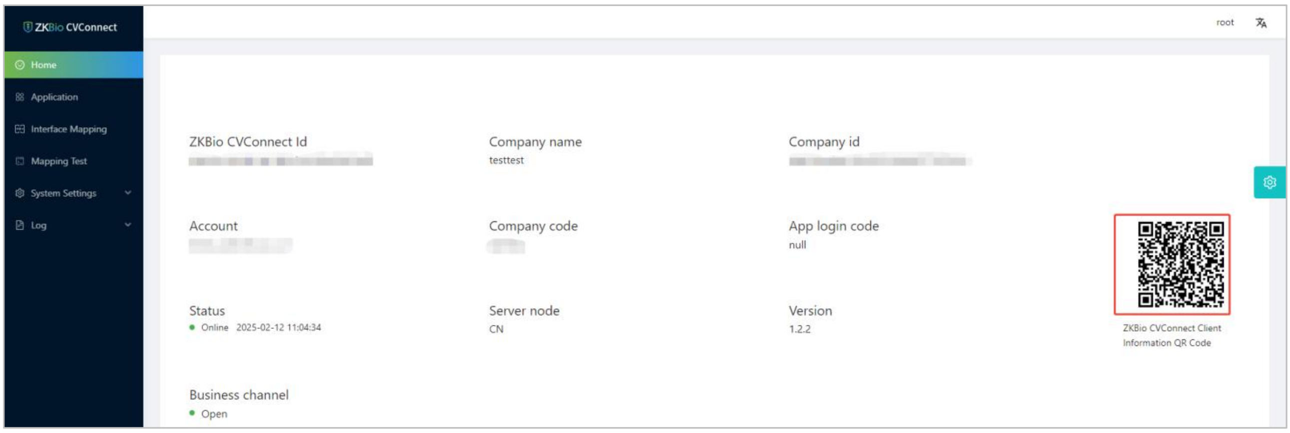
The ZKBio CVConnect platform, as a sub-service of MinervaIOT, mainly serves to forward intranet's application data to be accessed externally. If you have not installed the ZKBio CVConnect client yet, please click the link below to download or contact the technical support to obtain the installer.

ZKBio CVConnect Client

APP enterprise QR code

SIP service mode

● Cloud SIP ○ IPPBX Server ○ ZKTeco MediaServer



ZKBio CVConnect Id
[redacted]

Company name
testtest

Company id
[redacted]

Account
[redacted]

Company code
[redacted]

App login code
null

Status
● Online 2025-02-12 11:04:34

Server node
CN

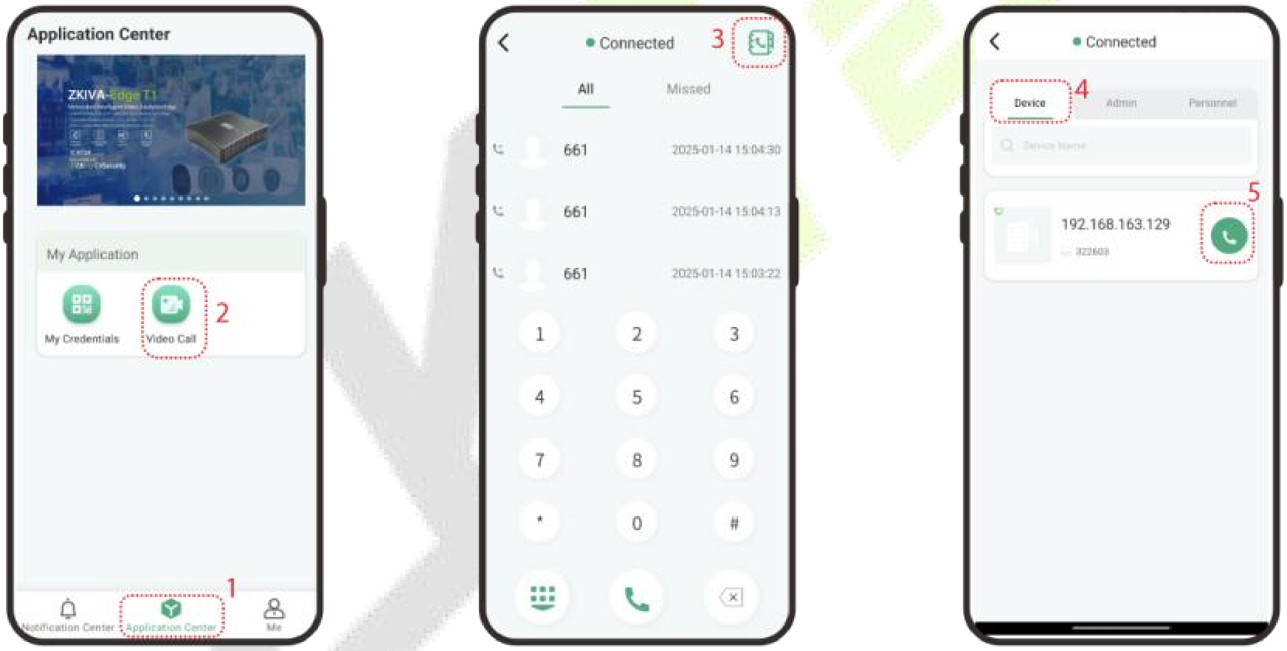
Version
1.2.2

ZKBio CVConnect Client Information QR Code

Business channel
● Open

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.

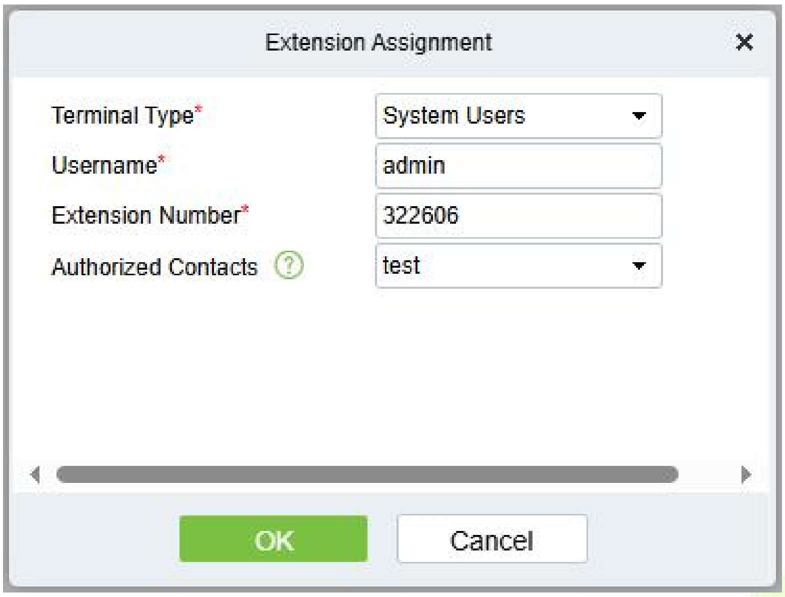


661 2025-01-14 15:04:30
661 2025-01-14 15:04:13
661 2025-01-14 15:03:22

192.168.163.129
322603

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

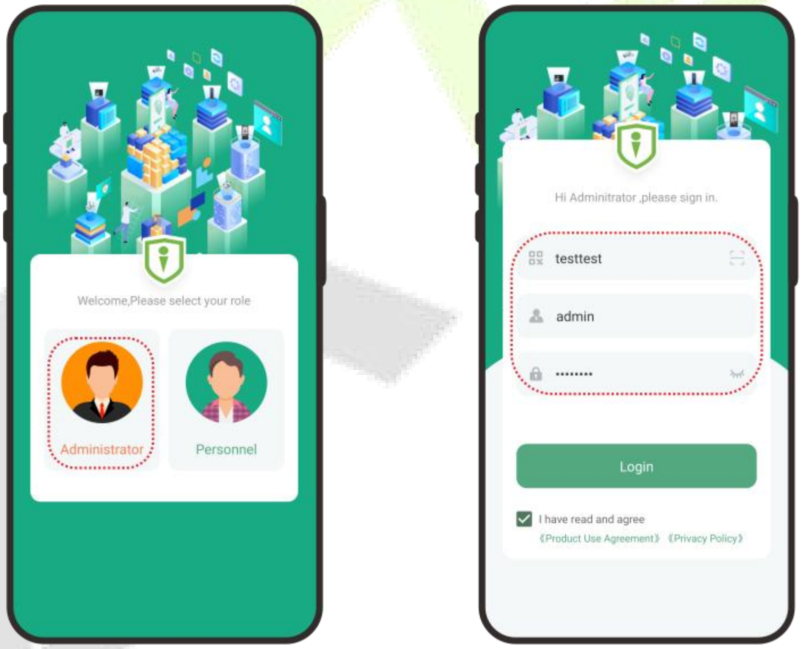
1. Select the Terminal Type as **System Users**.
2. Select the system user to be assigned an account and the extension number. Select the Authorized Contacts to assign the contact list to the admin, and after the assignment, the admin can view the contacts in the contact list upon logging into the ZKBio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



Extension Assignment

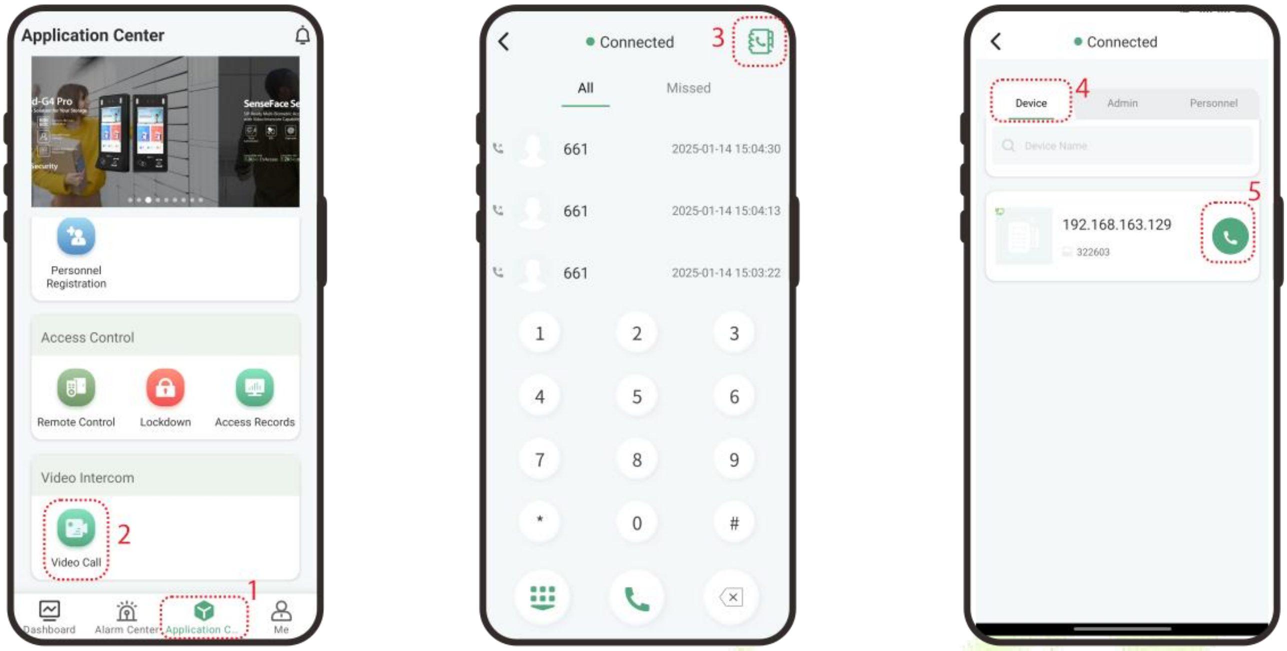
Terminal Type*	System Users
Username*	admin
Extension Number*	322606
Authorized Contacts	test

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.



Welcome,Please select your role
Administrator
Personnel
Hi Adminitrator ,please sign in.
testtest
admin
••••••••
Login
I have read and agree
《Product Use Agreement》《Privacy Policy》

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.



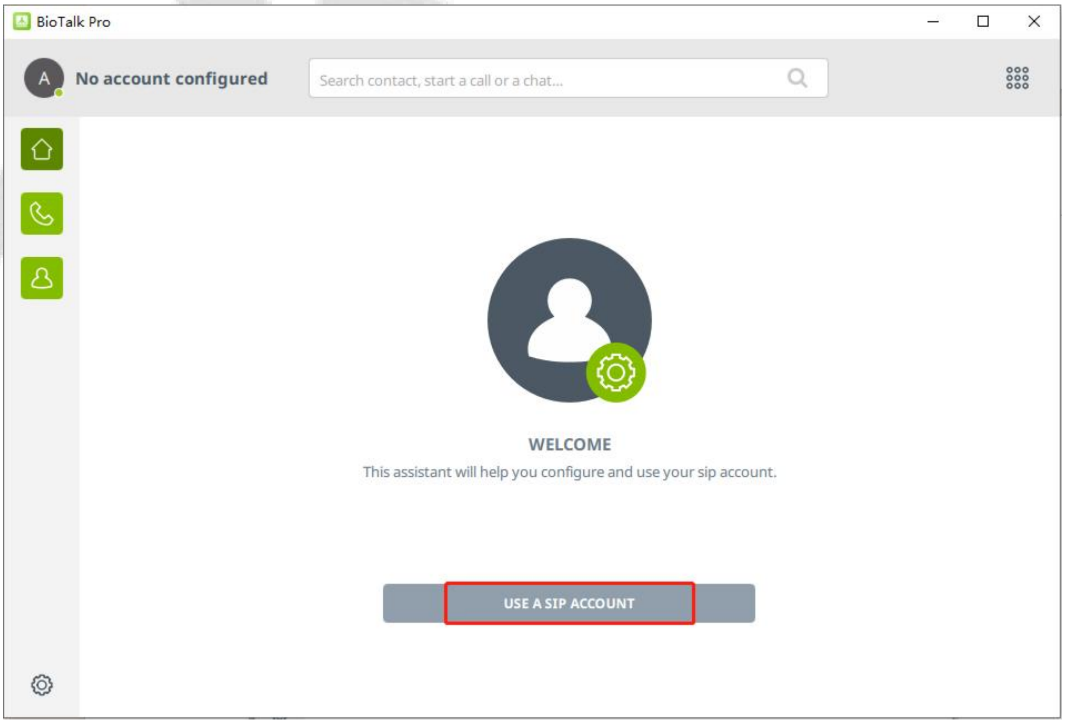
The App complete operation steps please refer to the ZKBio Zexus Mobile App User Manual.

16.2.6 PC Client Functionality

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

Operation Guide

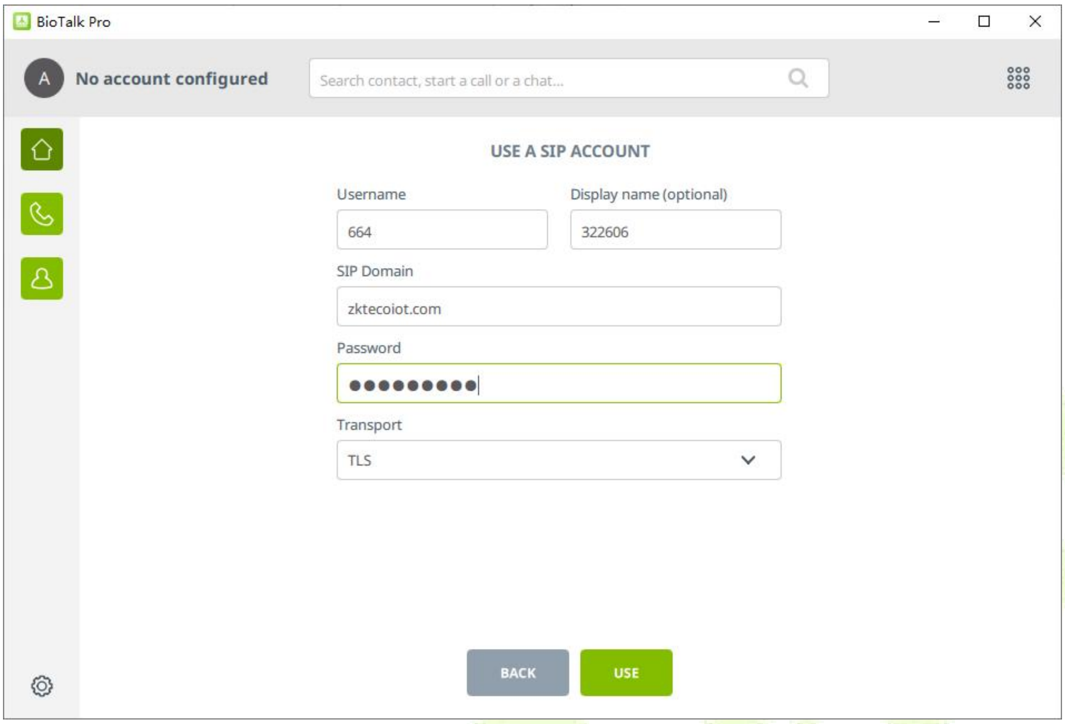
Step 1: Configure the SIP account: Click **USE A SIP ACCOUNT** button.



WELCOME

This assistant will help you configure and use your sip account.

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



USE A SIP ACCOUNT

Username: 664

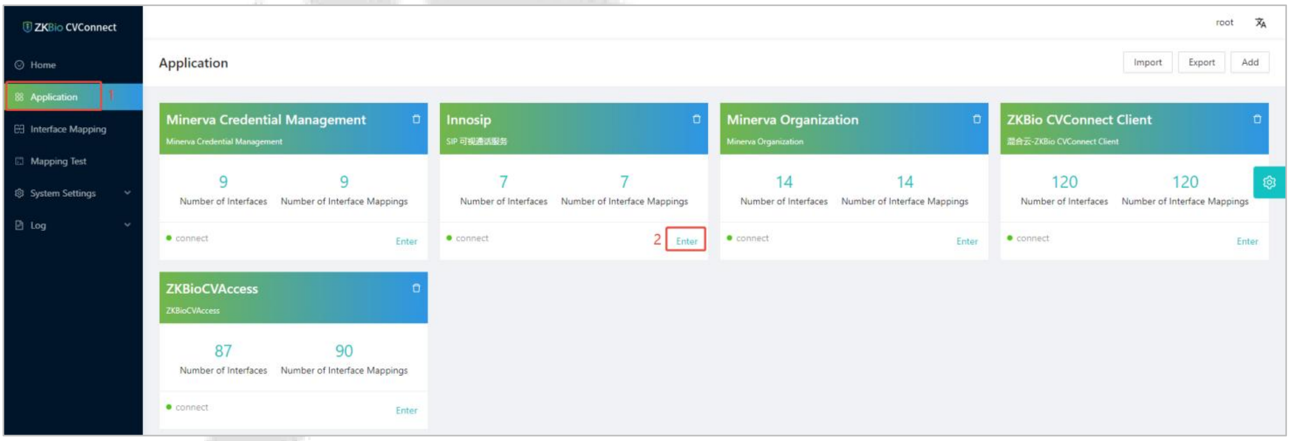
Display name (optional): 322606

SIP Domain: zktecoiot.com

Password: ●●●●●●●●●

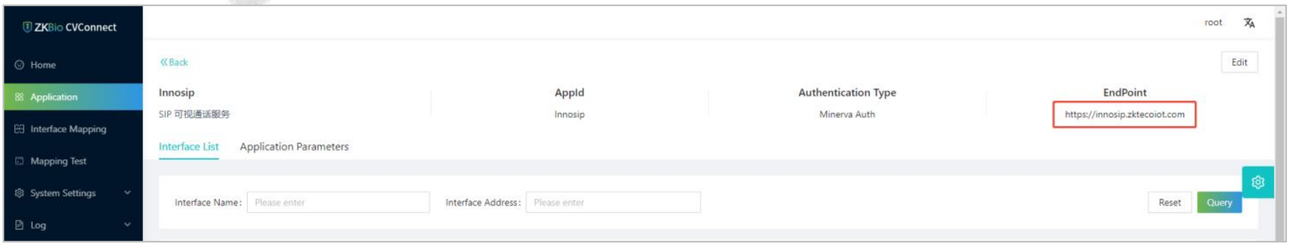
Transport: TLS

- **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.zktecoiot.com”. Then 'zktecoiot.com' is the actual SIP server domian you need to enter on the PC Client.)



Application

Application	Number of Interfaces	Number of Interface Mappings	Status
Minerva Credential Management Minerva Credential Management	9	9	connect
Innosip SIP 可视通话服务	7	7	connect
Minerva Organization Minerva Organization	14	14	connect
ZKBio CVConnect Client 混合云-ZKBio CVConnect Client	120	120	connect
ZKBioCVAccess ZKBioCVAccess	87	90	connect



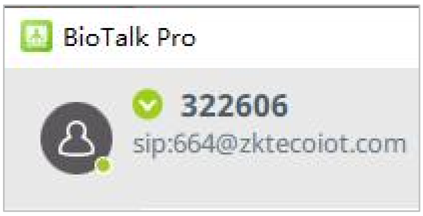
Innosip	AppId	Authentication Type	EndPoint
SIP 可视通话服务	Innosip	Minerva Auth	https://innosip.zktecoiot.com

Interface Name: Please enter

Interface Address: Please enter

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

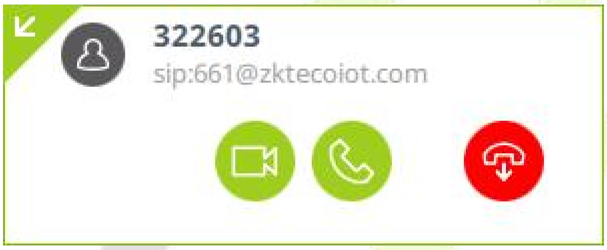
Wait 1 minute until the status shows Connected, as shown below:

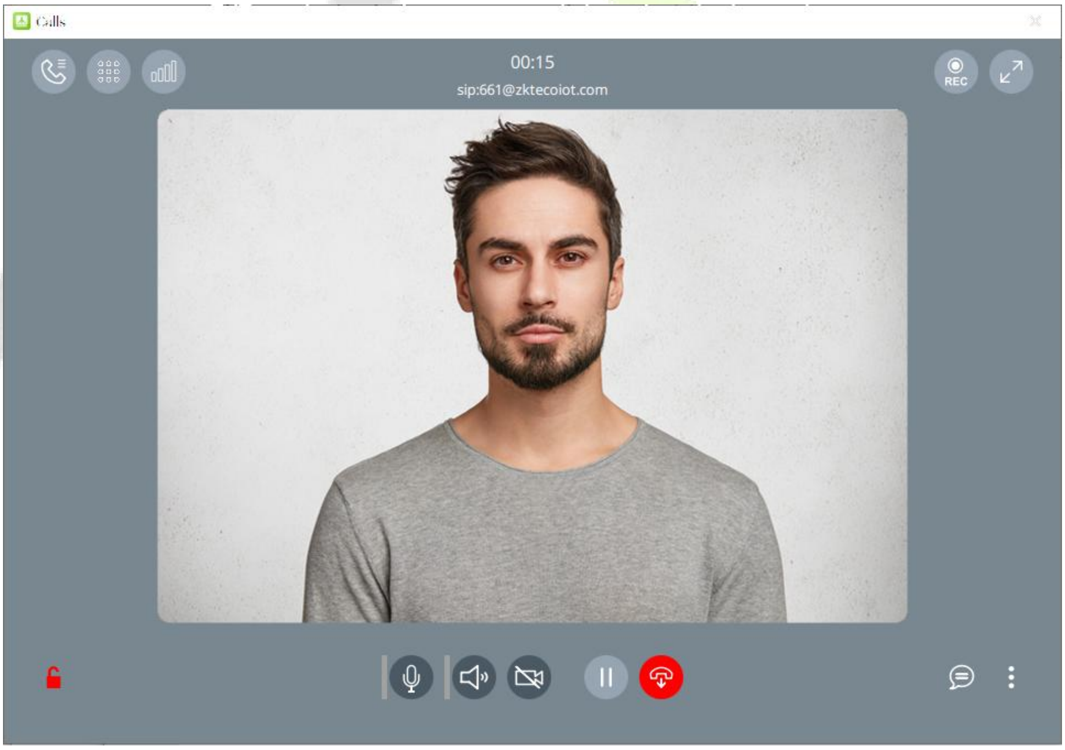


Note: In the Cloud SIP mode, if dialing is required, the PC Client should dial directly to the target SIP account. For example, if the extension number created on ZKBio CVAccess is 322603, the corresponding generated SIP account is 661, then the PC Client should dial 661 when making a call. Therefore,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

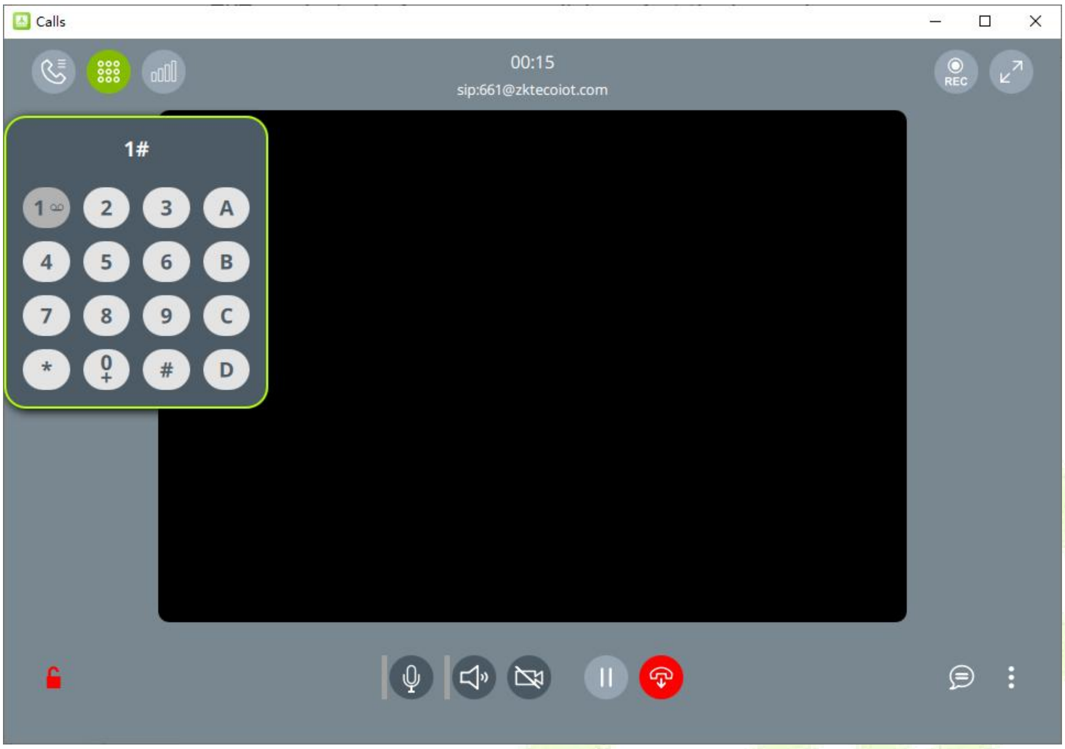
At this point you can start to use it normally, the PC client, the device and the App can call and answer each other.

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.

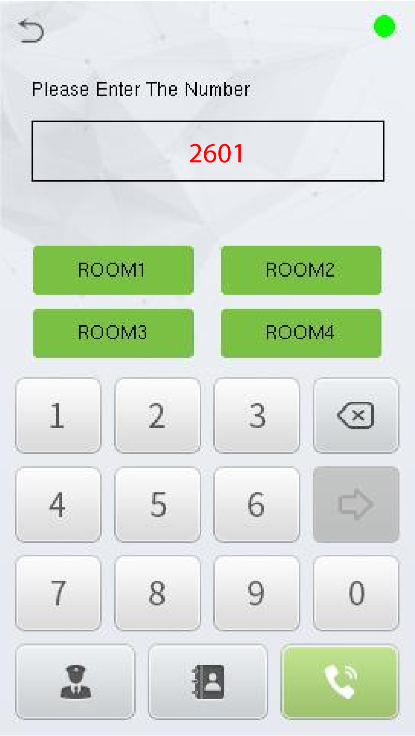


16.2.7 Make a Call

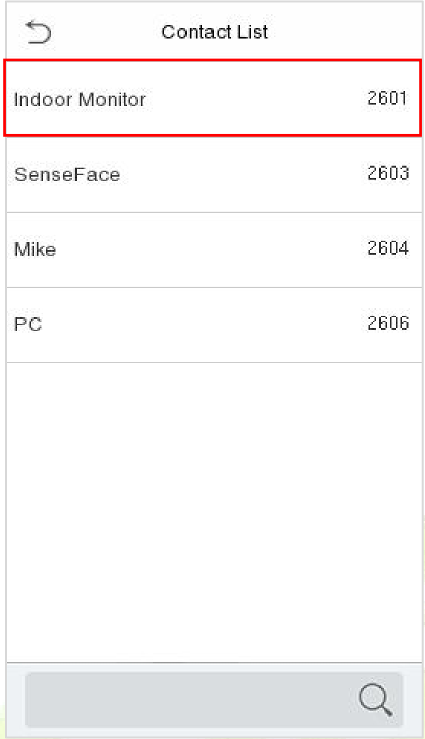
Two-way calls can be made between the device, indoor monitor, ZKBio Zexus App, and PC client (BioTalk Pro).

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

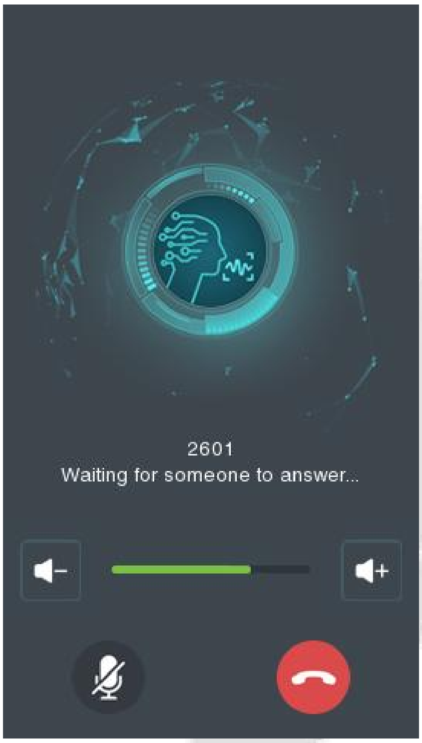
1. Add the indoor monitor on the ZKBio CVAccess software, then assign an extension number to the indoor monitor. (The operations steps can refer to 16.2.2 Add Device and 16.2.5 Assignment of Extension Numbers and SIP Accounts)
2. Click the icon ☎ on the device and enter the Short Number of the indoor 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.

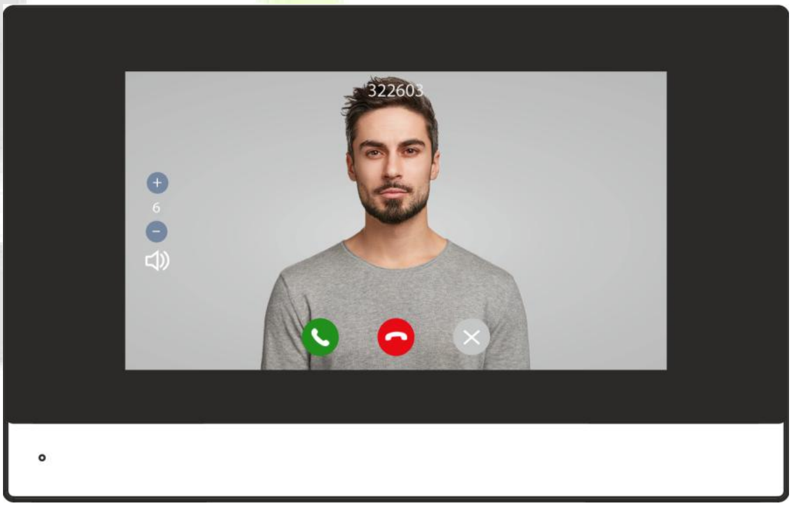


or


Contact List

Indoor Monitor	2601
SenseFace	2603
Mike	2604
PC	2606

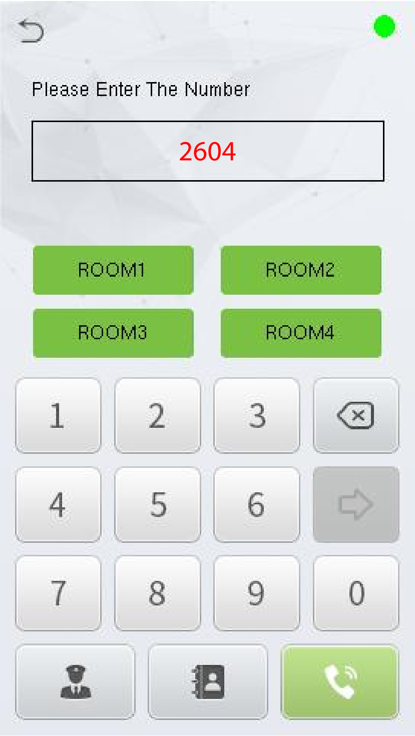

2601
Waiting for someone to answer...



- **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)

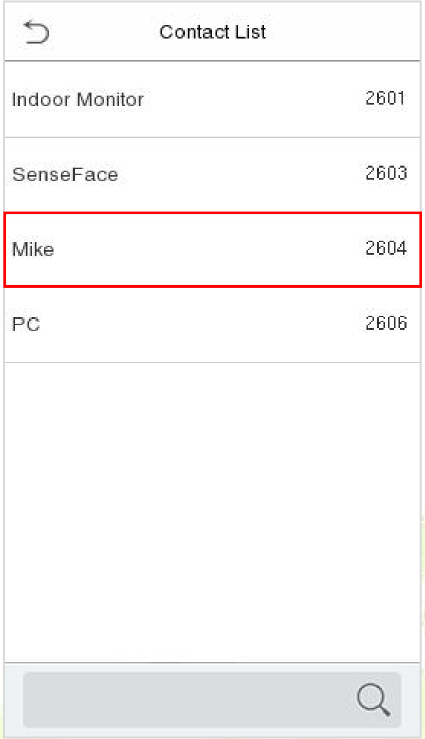
2. Click the icon ☎ on the device and enter the Short Number of the personnel in the pop-up interface of the device. Or click the ▤ icon on the call page to open the contact list and search for the personnel to call him/her.



Please Enter The Number

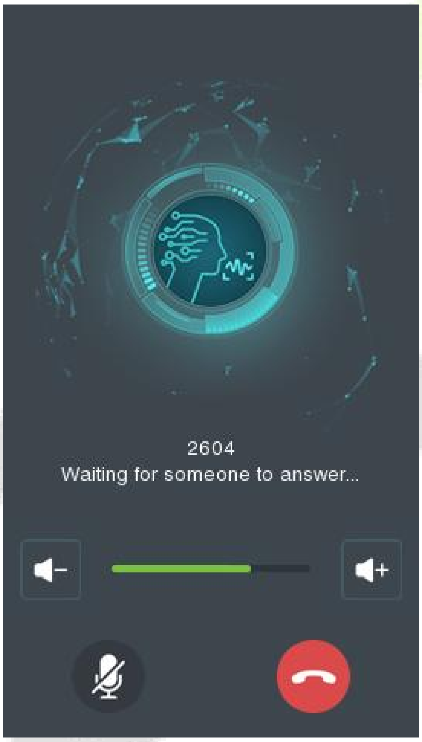
2604

or

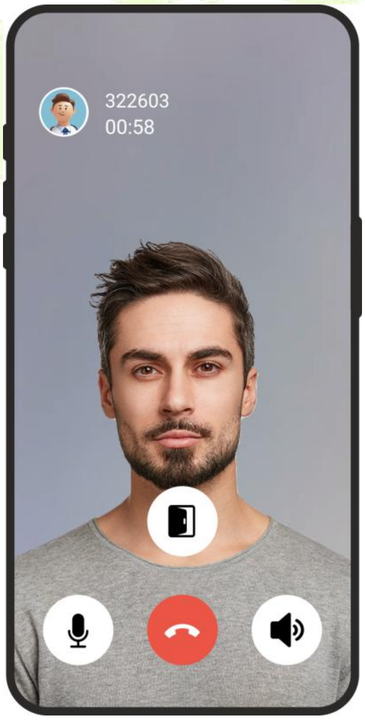


Contact List

Indoor Monitor	2601
SenseFace	2603
Mike	2604
PC	2606



2604
Waiting for someone to answer...

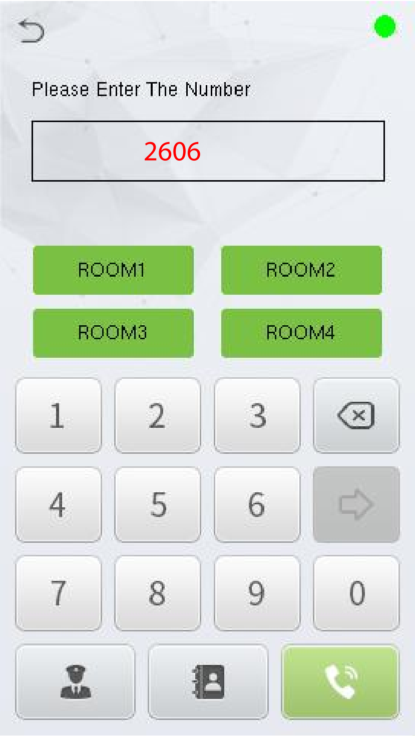


322603
00:58

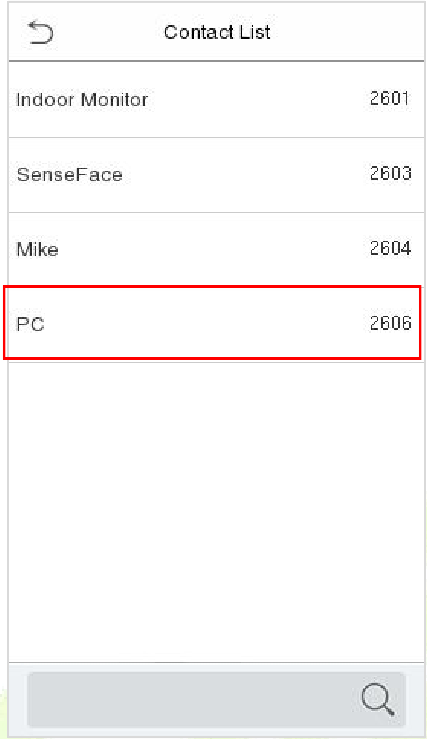
- **Device Call the PC Client (BioTalk Pro)**

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.

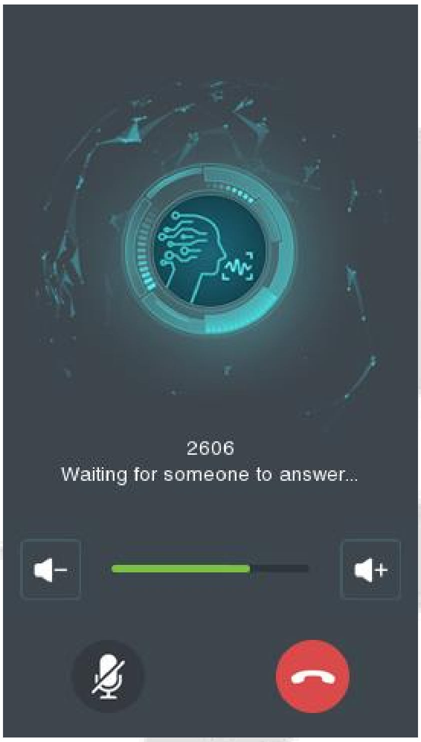


or

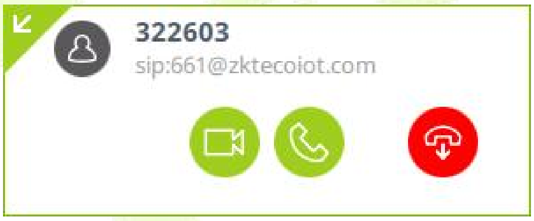


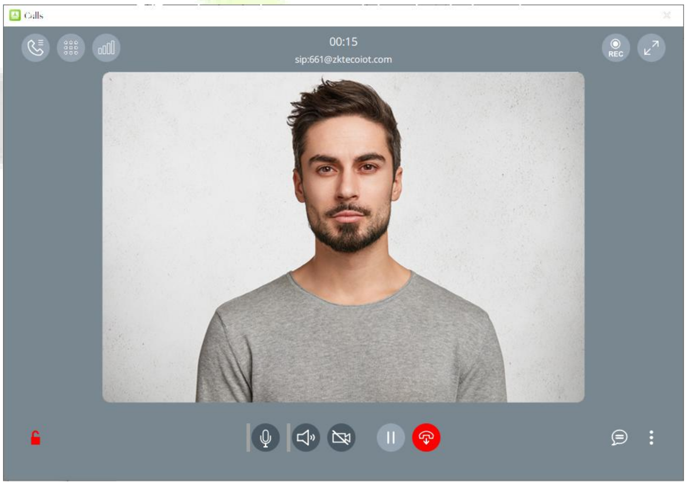
Contact List

Indoor Monitor	2601
SenseFace	2603
Mike	2604
PC	2606



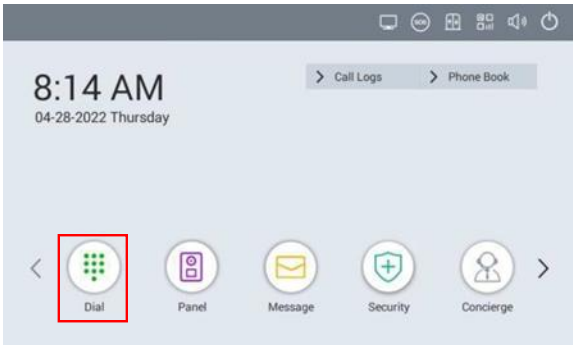
2606
Waiting for someone to answer...

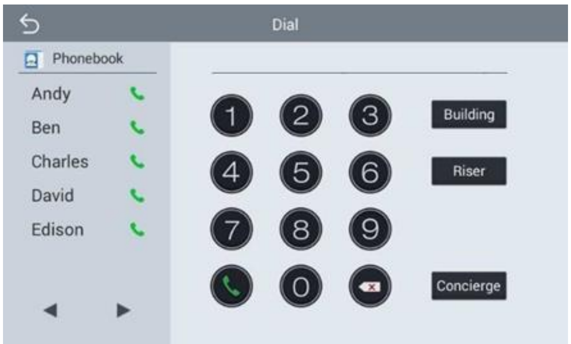




- **Indoor Monitor Call**

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

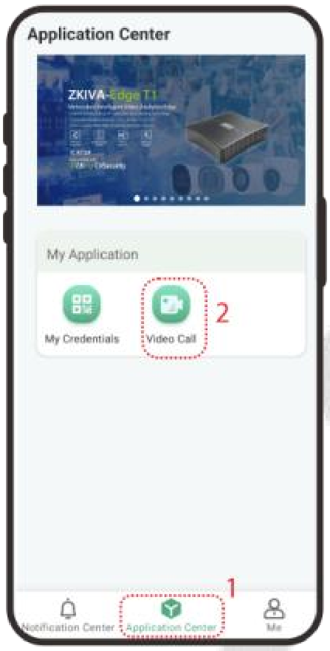


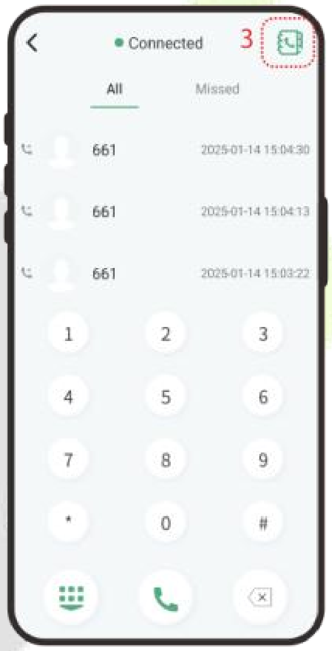


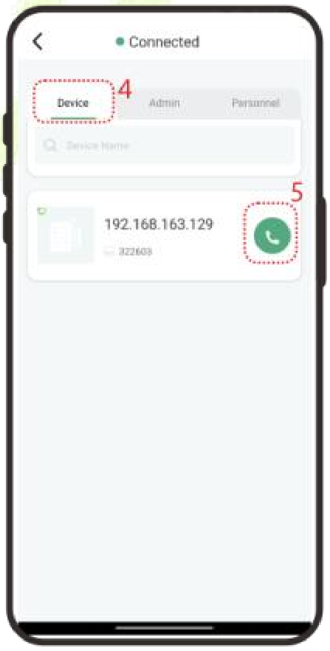
Note: The indoor monitor is not supported the assignment of the contact list in ZKBio CVAccess.

- **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.

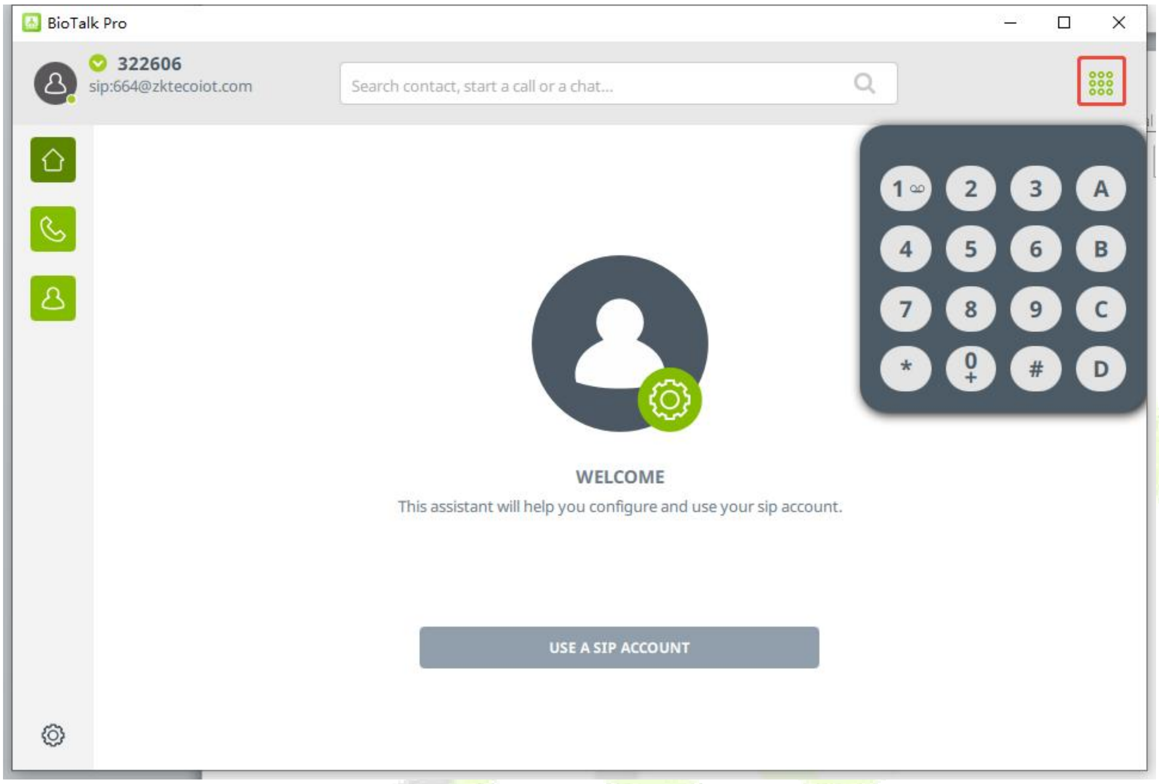




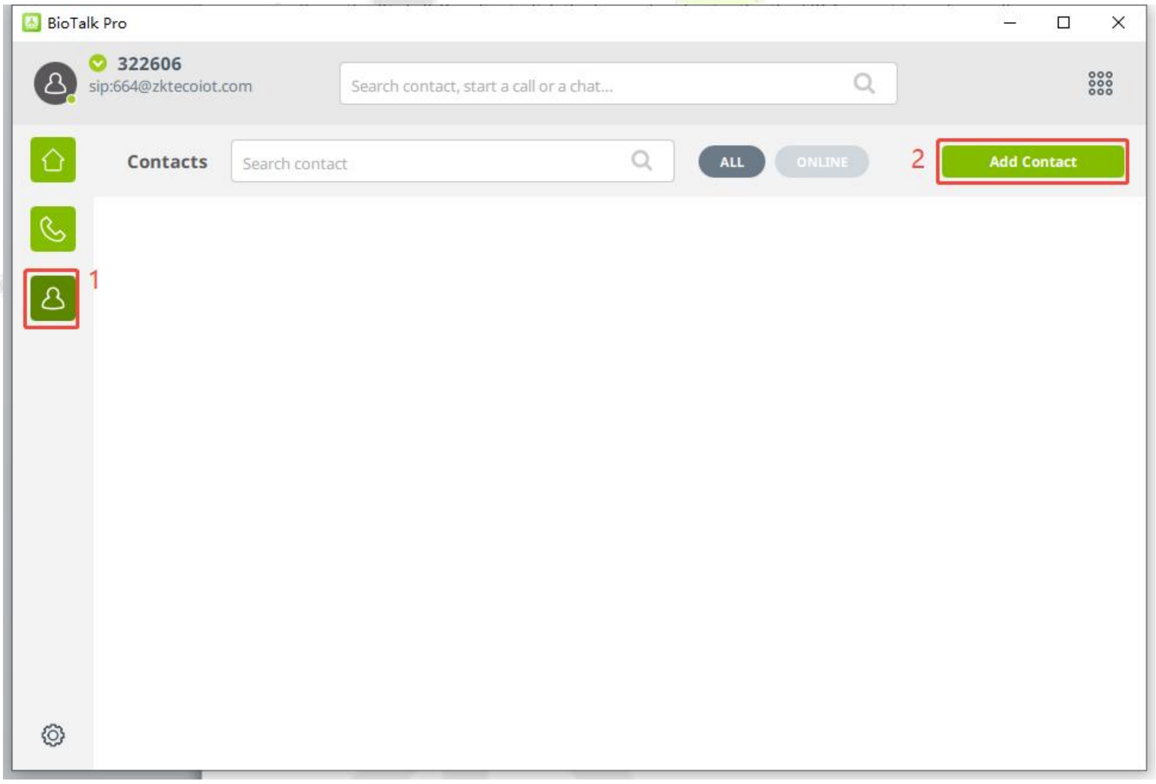


- **PC Client (BioTalk Pro) Call**

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


BioTalk Pro
322606
sip:664@zktecoiot.com
Search contact, start a call or a chat...
1 2 3 A
4 5 6 B
7 8 9 C
* 0 + # D
WELCOME
This assistant will help you configure and use your sip account.
USE A SIP ACCOUNT

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



17 Connecting to ZKBio Zlink App

The 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 7.6 Device Type Settings.

- **Download the ZKBio Zlink App**

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

Apple App Store

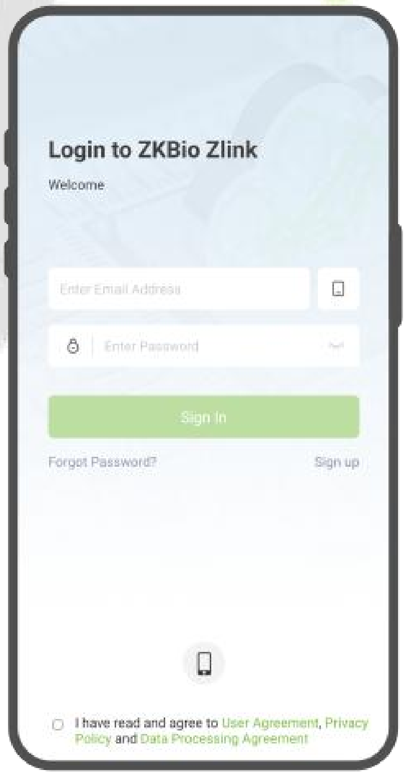
Google Play Store

Download on the App Store

GET IT ON Google Play

17.1 Login to the 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 App.


Login to ZKBio Zlink

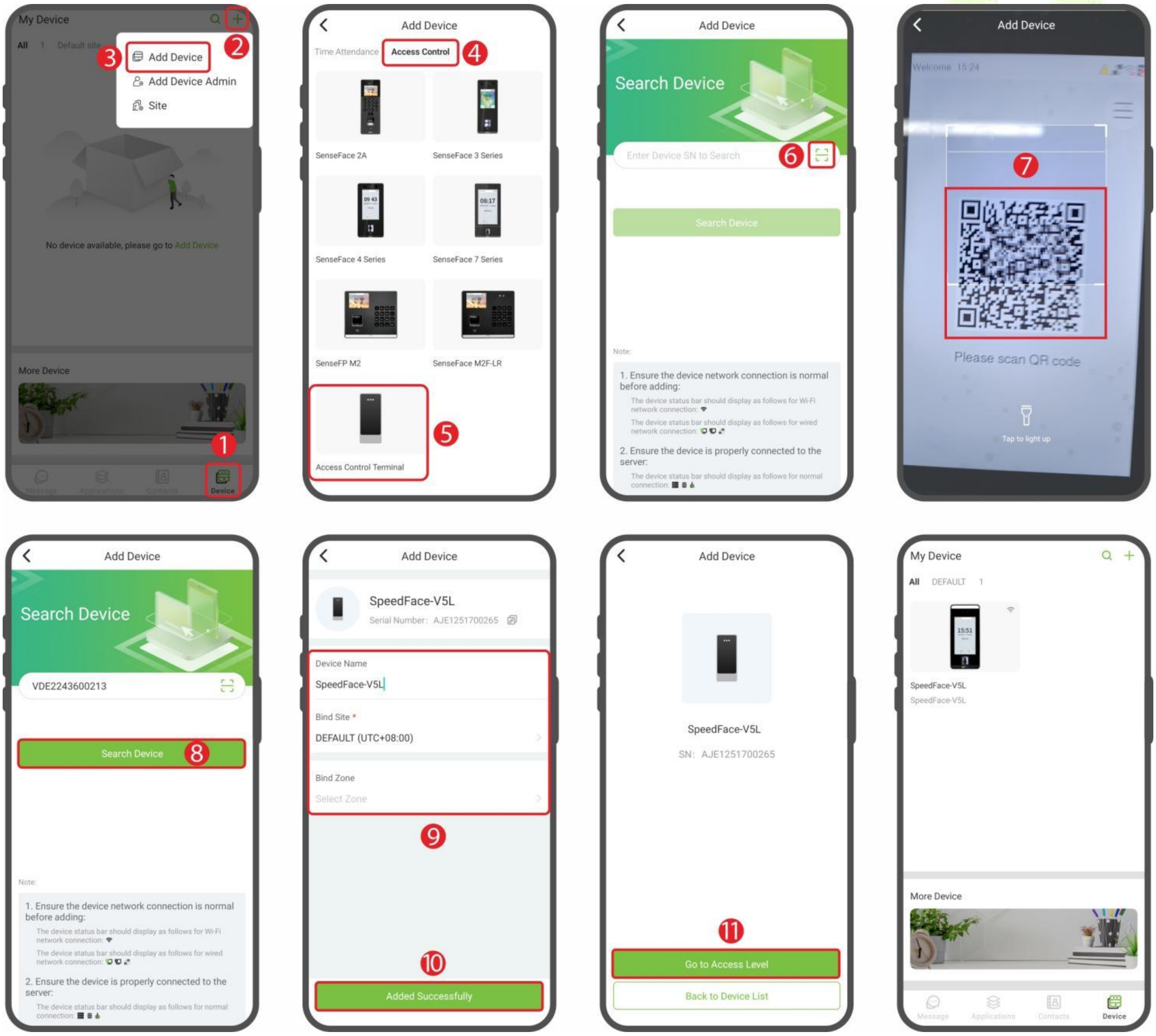
Welcome

○ I have read and agree to User Agreement, Privacy Policy and Data Processing Agreement

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

17.2 Add Device on the App

- Access the ZKBio Zlink App and click on [**Device**] > + icon > [**Add Device**] > [**Access Control**] > **[Access Control Terminal]**. (1,2,3,4,5)
- 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]**. (6,7,8)
- 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. (9,10,11)
- Once successfully added, the device is displayed in the list of the device interface.

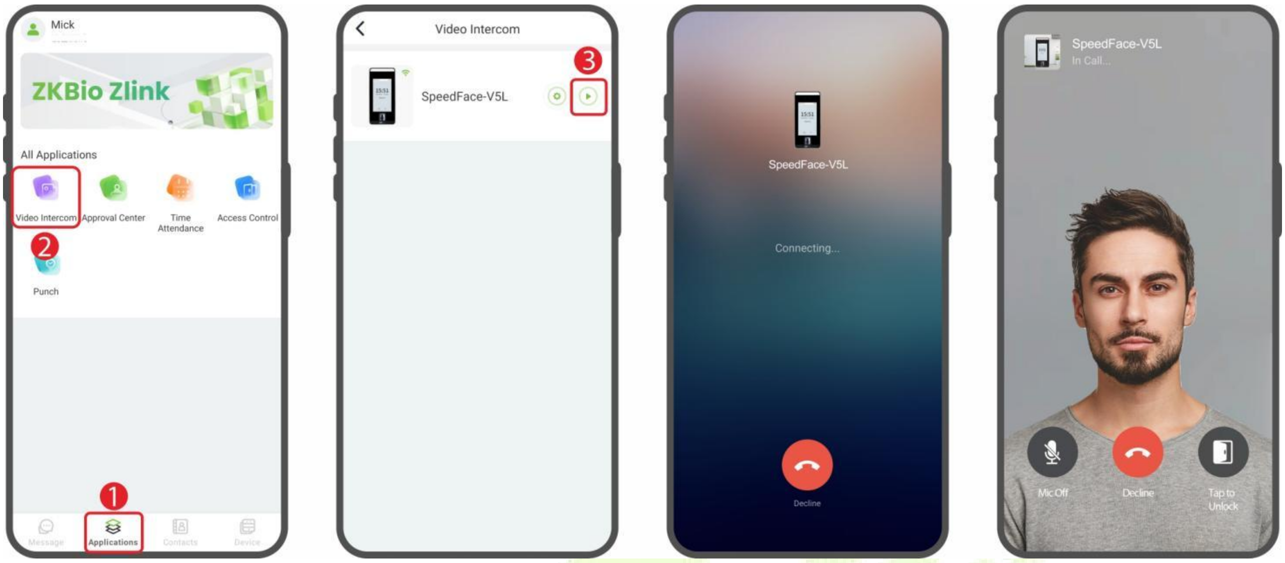


Note:

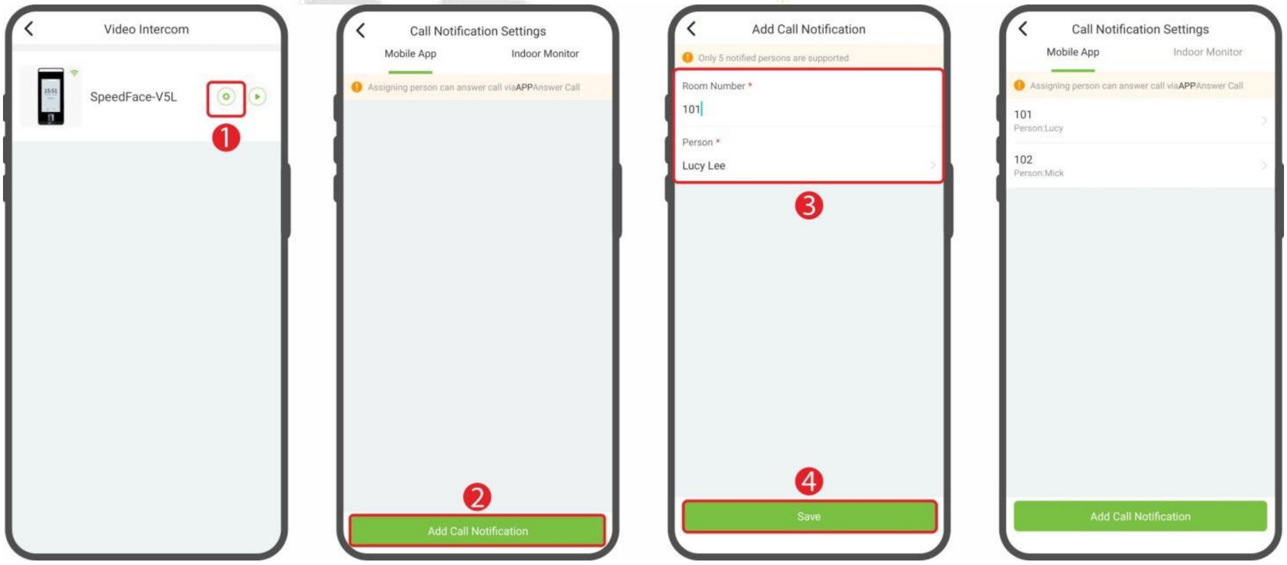
1. Ensure the device network connection is normal before adding:
   The device status bar should display as follows for Wi-Fi network connection:
   The device status bar should display as follows for wired network connection:
2. Ensure the device is properly connected to the server:
   The device status bar should display as follows for normal connection:

17.3 Video Intercom

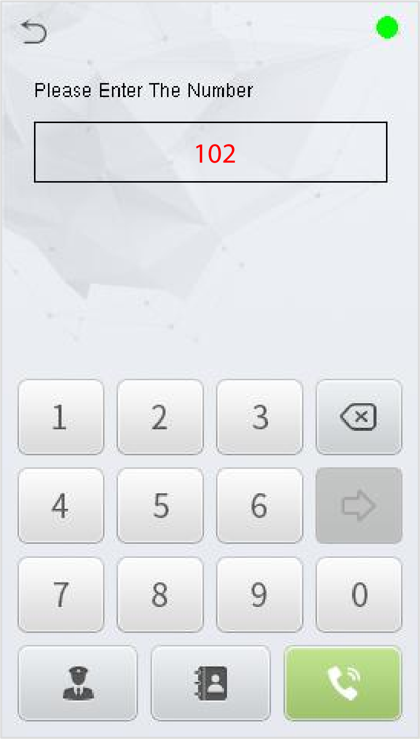
- Click [**Applications**] > [**Video Intercom**] > ▶ icon can call the device. Click **Tap to Unlock** icon can open the door remotely.



- Click ⚙ icon > **[Add Call Notification]** to assign person that can answer call via App.
  - **Room Number:** Customize the number of the person.
  - **Person:** One or multiple persons can be selected. If multiple persons are selected, all the persons will receive the call when the device calls the number.



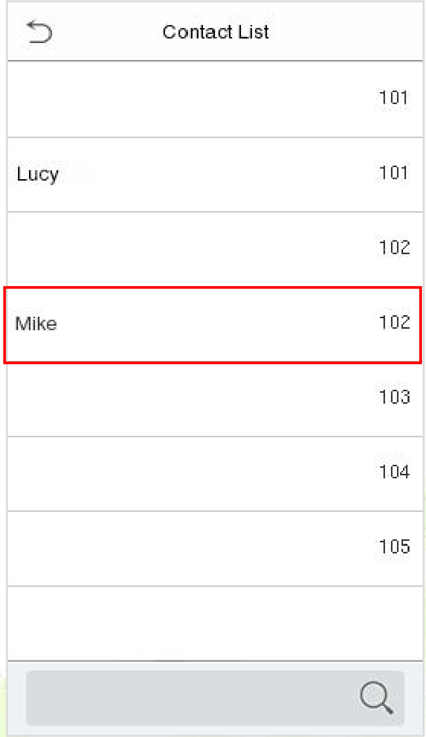
- After the setting is successful, you can click the icon ☎ on the device and enter the Number of the person in the pop-up interface of the device. Or click the 📇 icon on the call page to open the contact list and search for the person to call him/her.



Please Enter The Number

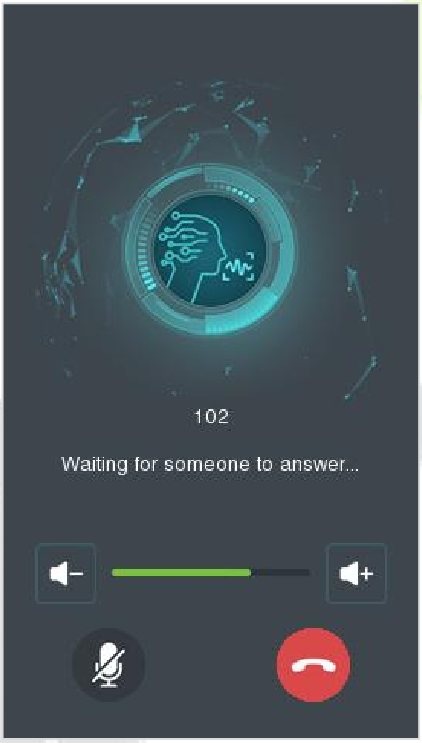
102

or



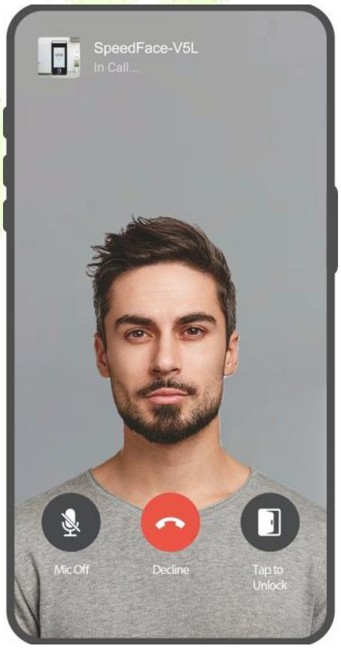
Contact List

	101
Lucy	101
	102
Mike	102
	103
	104
	105



102

Waiting for someone to answer...



SpeedFace-V5L

In Call...

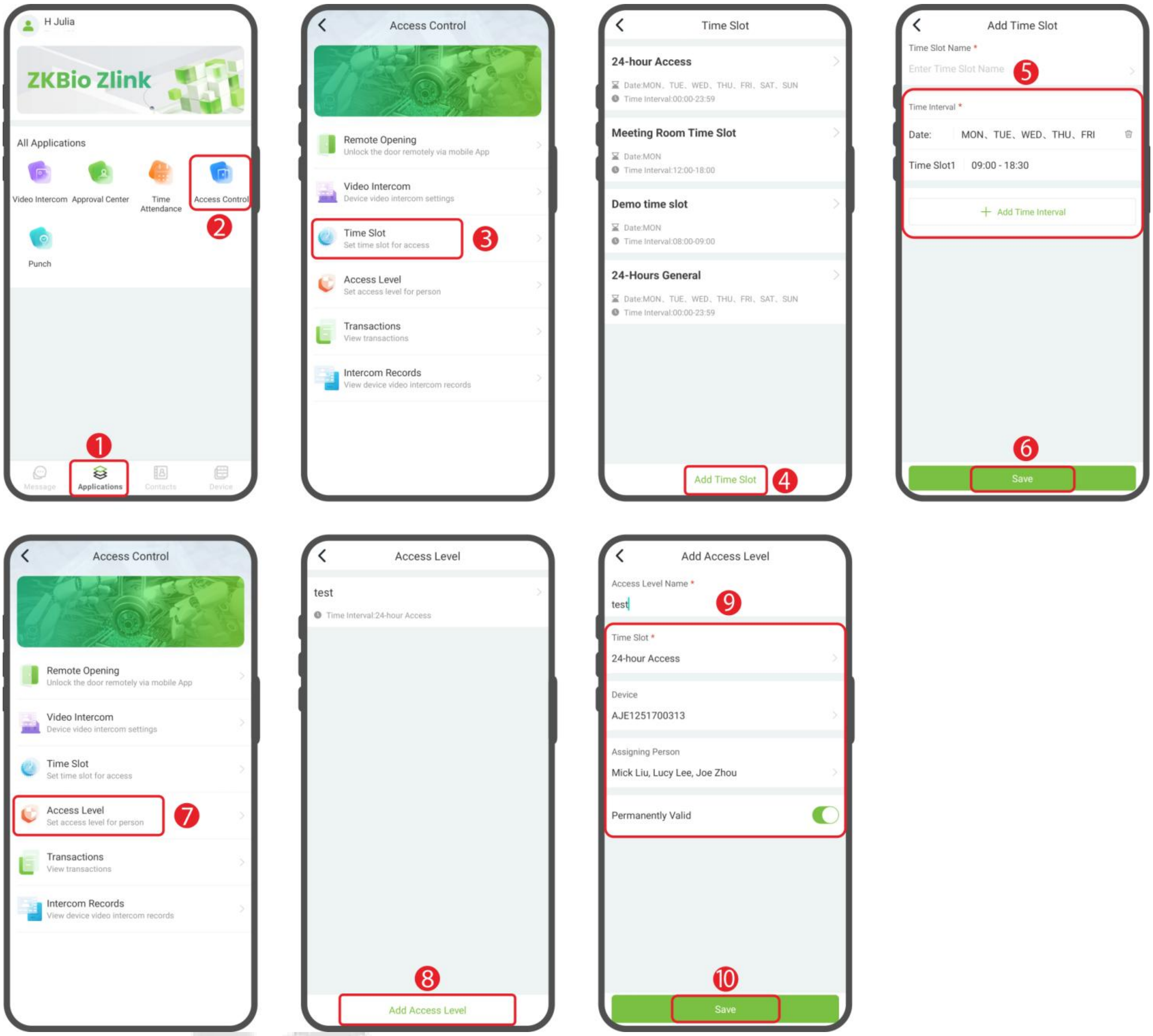
17.4 Set Access Levels

- Click [**Applications**] > [**Access Control**] > [**Time Slot**] > **[Add Time Slot]** to add a time slot. (1,2,3,4)

- Set the name and time intervals, and click [**Save**]. Then the time slot will be displayed in the list. (5,6)

  Note: There is a default timeslot named **24-hour Access** in the system.

- Click [**Access Level**] > **[Add Access Level]** to add an access level. (7,8)
- Set the name, select the time slot, device, and persons, and click [**Save**] to synchronize the access level to the device. (9,10)



Time Slot:

24-hour Access
Date:MON、TUE、WED、THU、FRI、SAT、SUN
Time Interval:00:00-23:59

Meeting Room Time Slot
Date:MON
Time Interval:12:00-18:00

Demo time slot
Date:MON
Time Interval:08:00-09:00

24-Hours General
Date:MON、TUE、WED、THU、FRI、SAT、SUN
Time Interval:00:00-23:59

Add Time Slot:

Time Slot Name * Enter Time Slot Name
Time Interval *
Date: MON、TUE、WED、THU、FRI
Time Slot1 09:00 - 18:30

Access Level:

test
Time Interval:24-hour Access

Add Access Level:

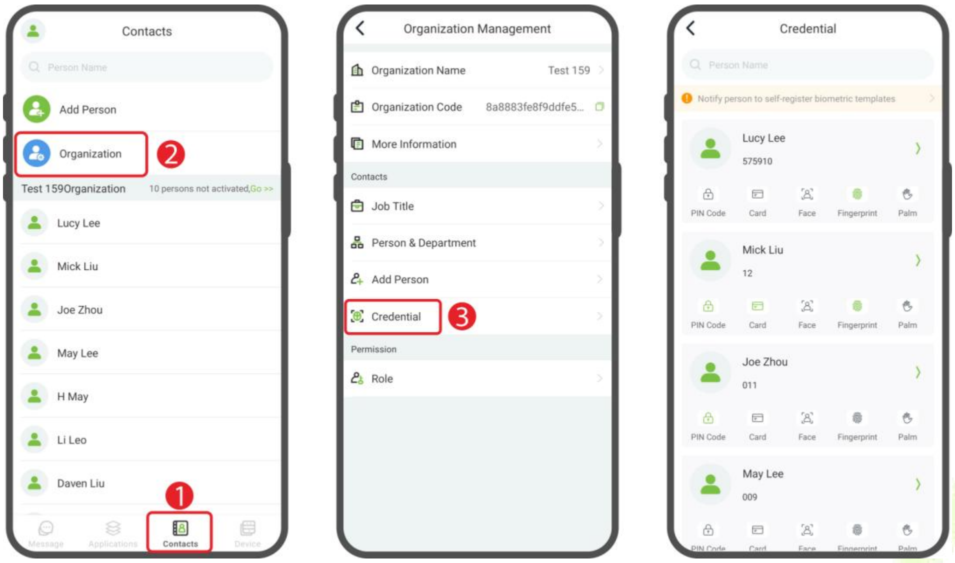
Access Level Name * test
Time Slot * 24-hour Access
Device AJE1251700313
Assigning Person Mick Liu, Lucy Lee, Joe Zhou
Permanently Valid

17.5 Register Verification Mode on the App

Once you have added persons to the device, you can register verification modes to them.

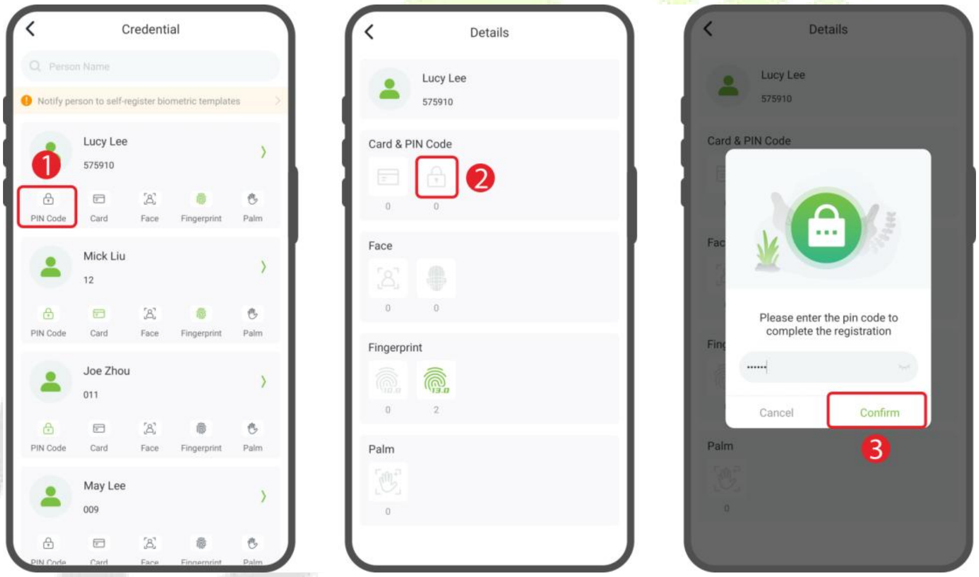
Note: It must be based on the functions actually supported by the device.

Click [**Contacts**] > [**Organization**] > [**Credential**] to enter the Credential screen. (1,2,3)



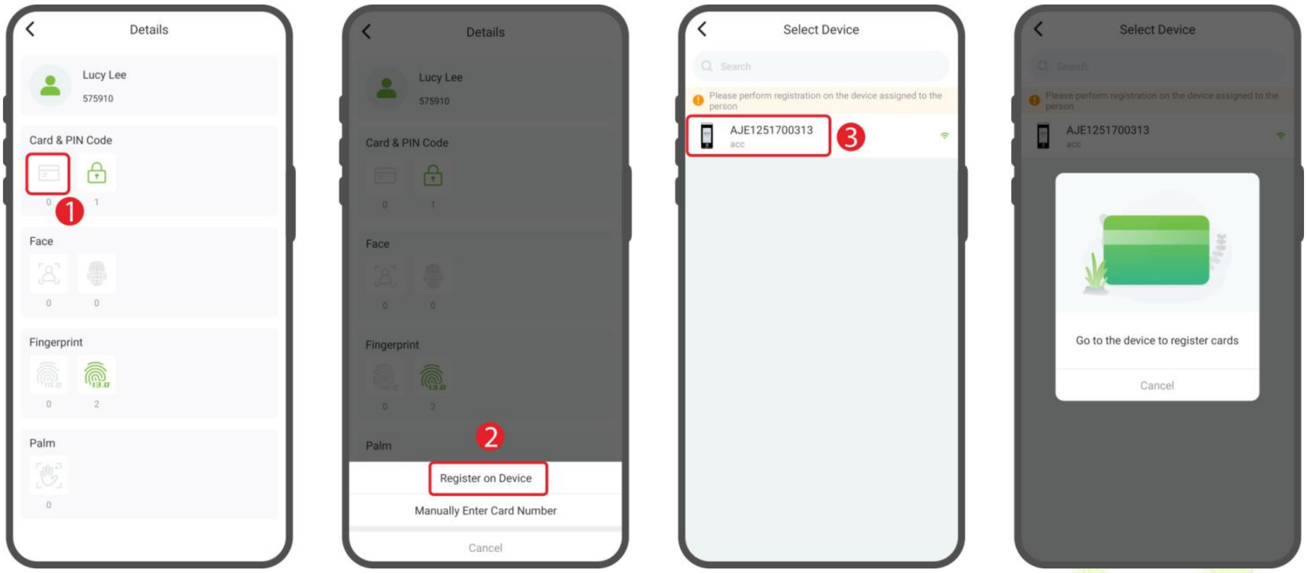
Register Password

In the Credential interface, click on the 🔒 icon and enter the password in the pop-up window. Click [**Confirm**] to confirm. (1,2,3)



Register Card

- In the Credential interface, click on the 💳 icon. You can select Register on Device or Manually Enter Card Number. If you want to register on device, then click **Register on Device**. (1,2)
- Select the registration device, at the same time, the device displays the Enroll Card Number interface. Place the card in the swipe area, when the display shows "**Card registered successfully**", it means the card is successfully registered. (3)

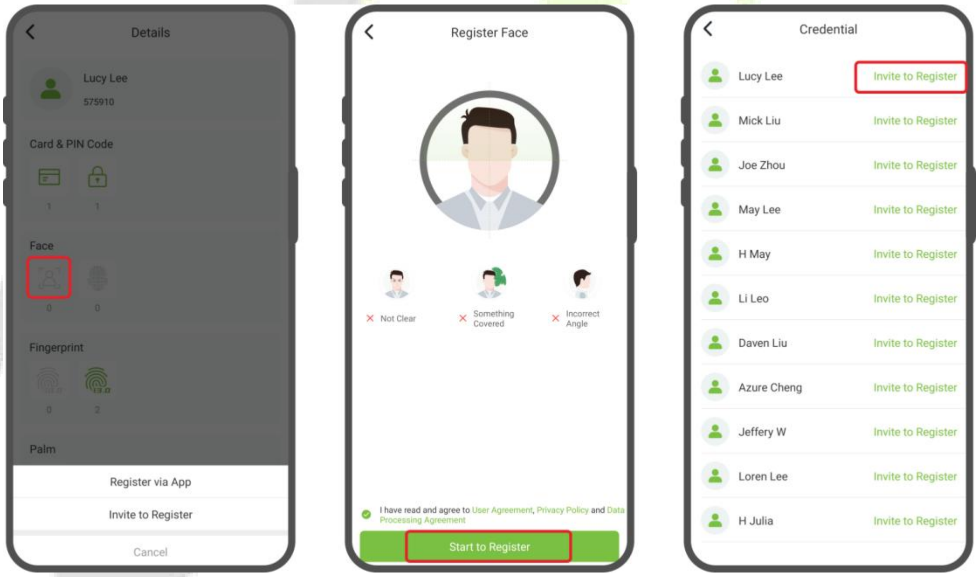


Please perform registration on the device assigned to the person

Go to the device to register cards

Register Face

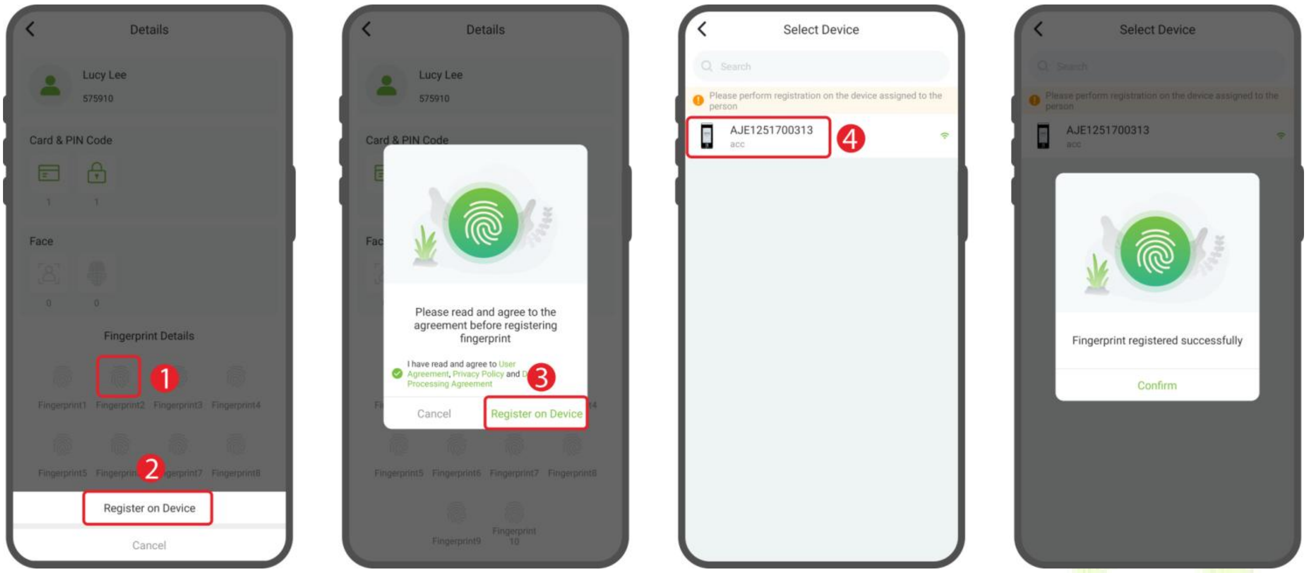
- In the Credential interface, click on the icon. You can select Register via App or Invite to Register. If you want to register via App, then click **Register via App** > **Start to Register** to take a shot.
- You can also click **Invite to Register** > **Invite to Registration** to send a message to the person to upload the facial photo. (**Note:** The person should be activated.)



I have read and agree to User Agreement, Privacy Policy and Data Processing Agreement

Register Fingerprint

- In the Credential interface, click on the icon > **Register on Device** > **Register on Device**. (1,2)
- Select the registration device, at the same time, the device displays the fingerprint registration screen. According to the prompts, place your finger on the fingerprint sensor and press **3** times. When the interface prompts "**Enrolled successfully**", it means the fingerprint registration is successful. (3,4)



Please read and agree to the agreement before registering fingerprint

I have read and agree to User Agreement, Privacy Policy and Data Processing Agreement

Please perform registration on the device assigned to the person

Fingerprint registered successfully

18 Connecting to ZKBio Zlink Web

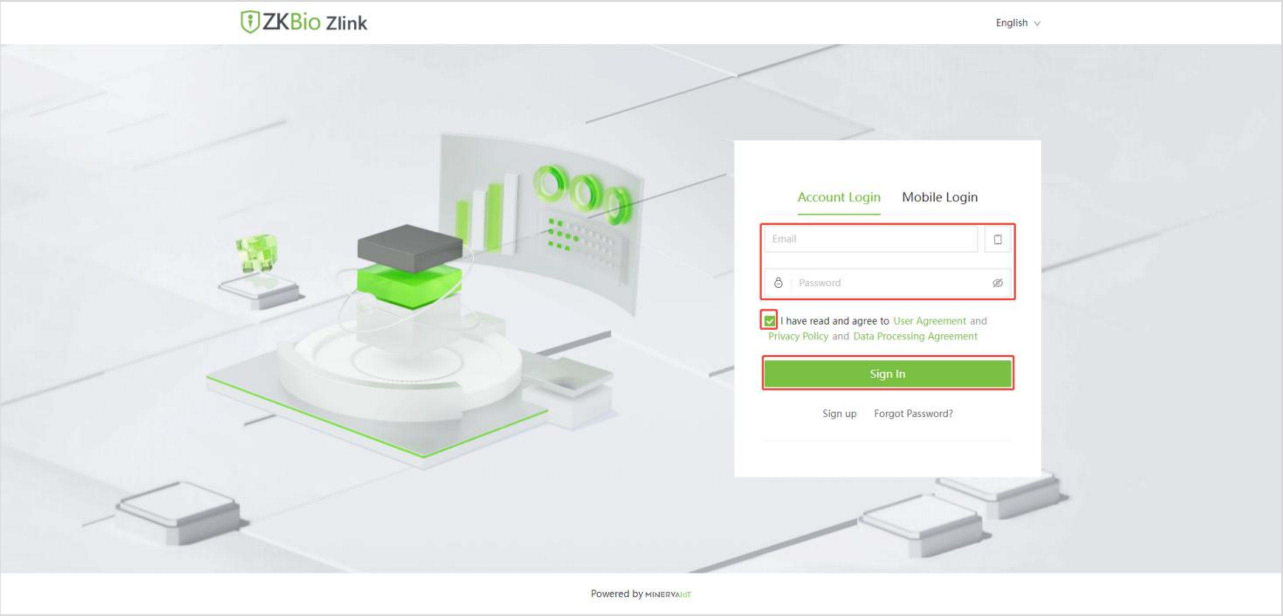
The web pages may vary depending on the version, and the document is for reference only.

Change the device communication protocol to BEST protocol, then the device can be managed by ZKBio Zlink, please refer to 6.5 Device Type Setting.

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

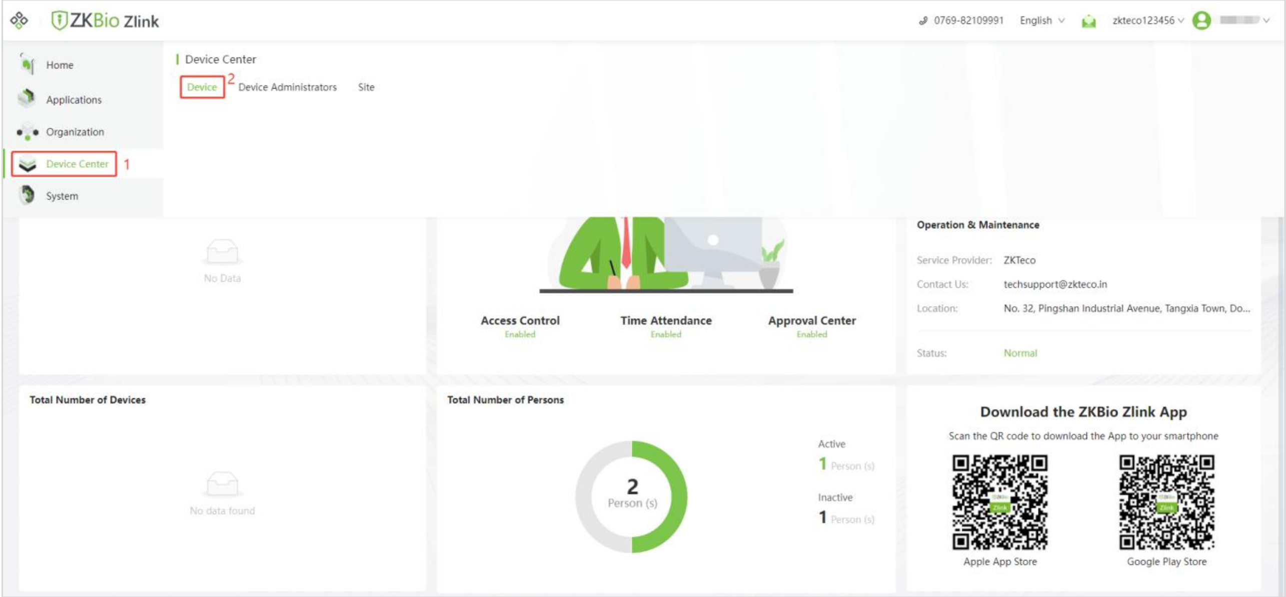
18.1 Login to the Web

1. Please open the recommended browser and enter the IP address to access the ZKBio Zlink Web: http://zlink.minervaiot.com.
2. Enter your Email ID and password 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

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



Operation & Maintenance

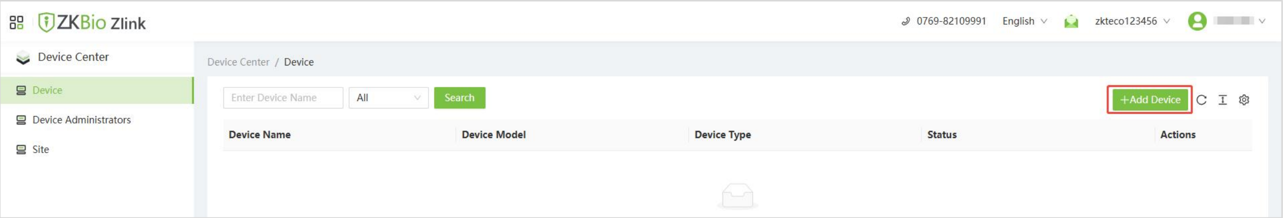
Service Provider: ZKTeco

Contact Us: techsupport@zkteco.in

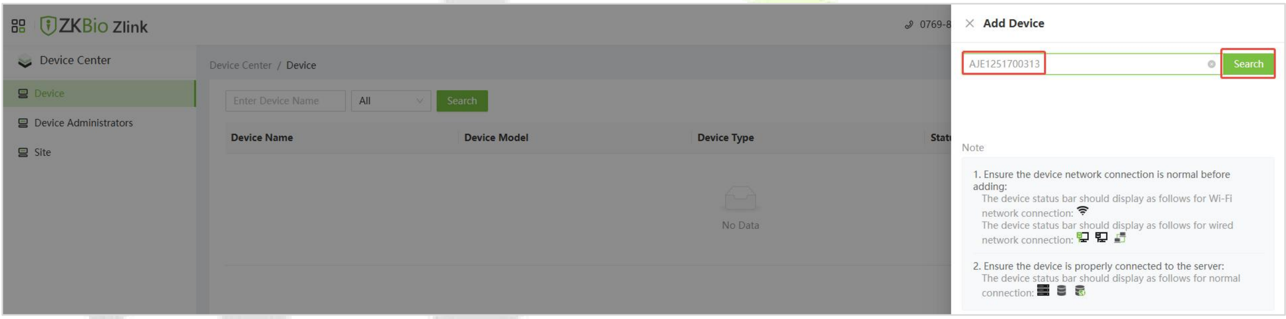
Location: No. 32, Pingshan Industrial Avenue, Tangxia Town, Do...

Status: Normal

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



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

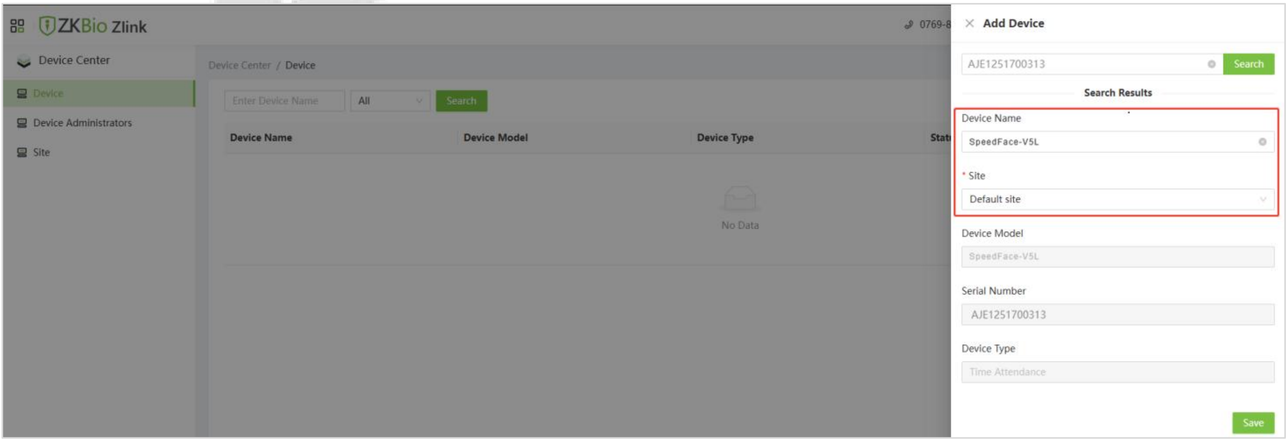


Note

1. Ensure the device network connection is normal before adding:
   The device status bar should display as follows for Wi-Fi network connection:
   The device status bar should display as follows for wired network connection:

2. Ensure the device is properly connected to the server:
   The device status bar should display as follows for normal connection:

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.



AJE1251700313

Device Name: SpeedFace-V5L

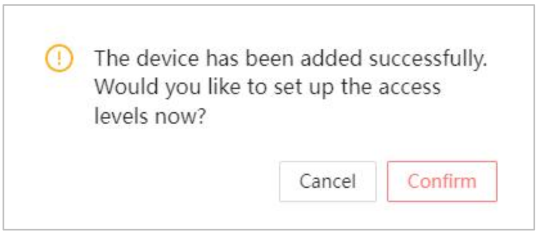
* Site: Default site

Device Model: SpeedFace-V5L

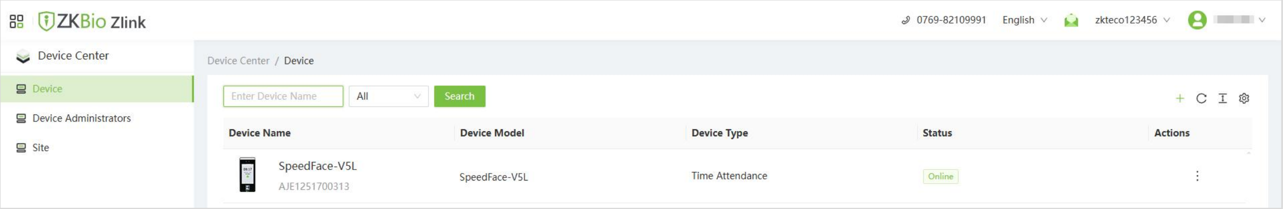
Serial Number: AJE1251700313

Device Type: Time Attendance

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.



The device has been added successfully. Would you like to set up the access levels now?

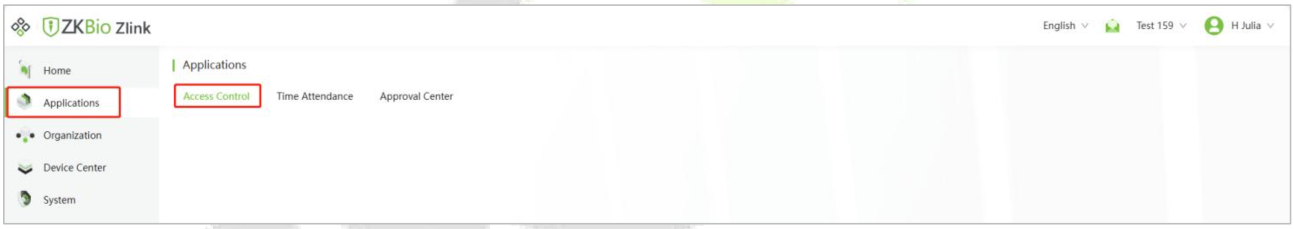


Device Name	Device Model	Device Type	Status	Actions
SpeedFace-V5L AJE1251700313	SpeedFace-V5L	Time Attendance	Online	⋮

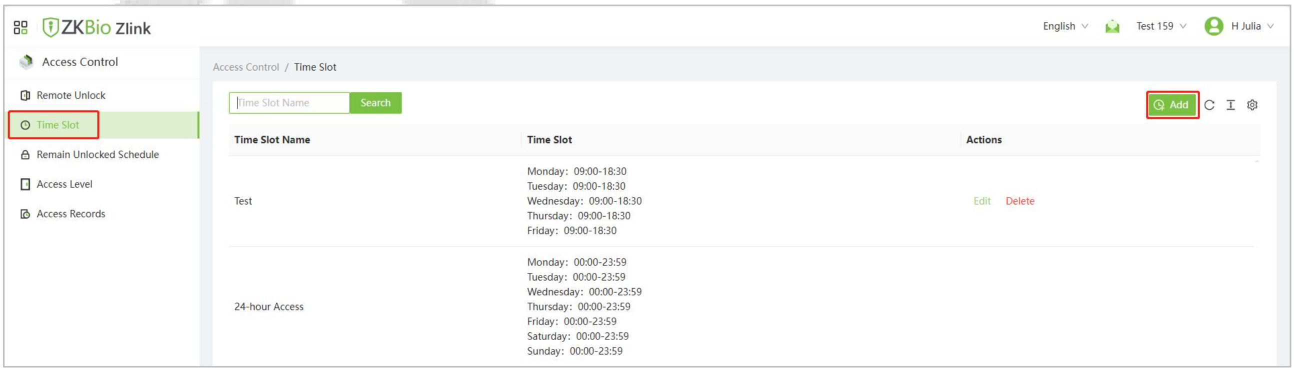
Note: *Wait a moment for the device status to change from "**Offline**" to "**Online**".*

18.3 Set Access Levels

1. Click the icon on the top left corner, and click [**Applications**] > [**Access Control**] to enter the access control settings interface.

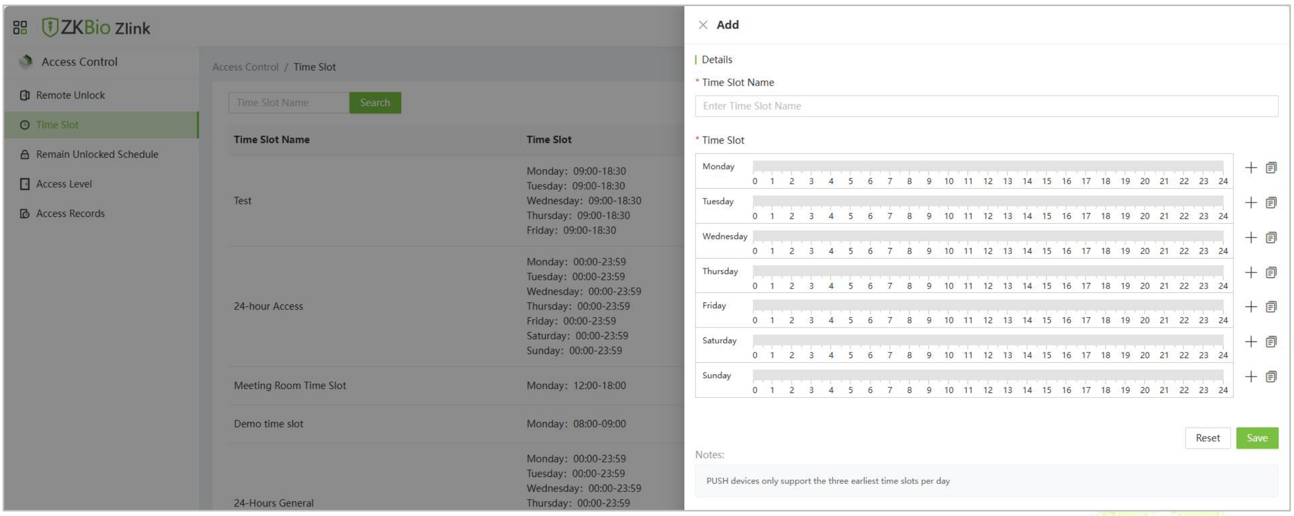


2. Click [**Time Slot**] > [**Add**] to add a time slot.



Time Slot Name	Time Slot	Actions
Test	Monday: 09:00-18:30 Tuesday: 09:00-18:30 Wednesday: 09:00-18:30 Thursday: 09:00-18:30 Friday: 09:00-18:30	Edit Delete
24-hour Access	Monday: 00:00-23:59 Tuesday: 00:00-23:59 Wednesday: 00:00-23:59 Thursday: 00:00-23:59 Friday: 00:00-23:59 Saturday: 00:00-23:59 Sunday: 00:00-23:59	

3. Set the name and time slot, and click [**Save**]. Then the time lot will be displayed in the list. (**Note:** There is a default timeslot named **24-hour Access** in the system.)



Time Slot Name	Time Slot
Test	Monday: 09:00-18:30 Tuesday: 09:00-18:30 Wednesday: 09:00-18:30 Thursday: 09:00-18:30 Friday: 09:00-18:30
24-hour Access	Monday: 00:00-23:59 Tuesday: 00:00-23:59 Wednesday: 00:00-23:59 Thursday: 00:00-23:59 Friday: 00:00-23:59 Saturday: 00:00-23:59 Sunday: 00:00-23:59
Meeting Room Time Slot	Monday: 12:00-18:00
Demo time slot	Monday: 08:00-09:00
24-Hours General	Monday: 00:00-23:59 Tuesday: 00:00-23:59 Wednesday: 00:00-23:59 Thursday: 00:00-23:59

Add

Details

* Time Slot Name: Enter Time Slot Name

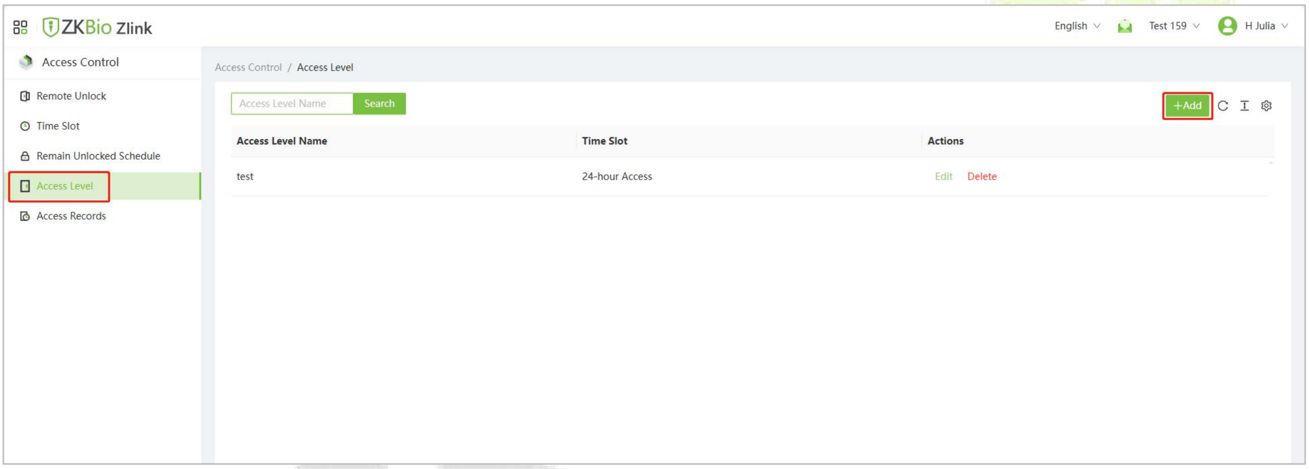
* Time Slot: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday (0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24)

Reset Save

Notes:

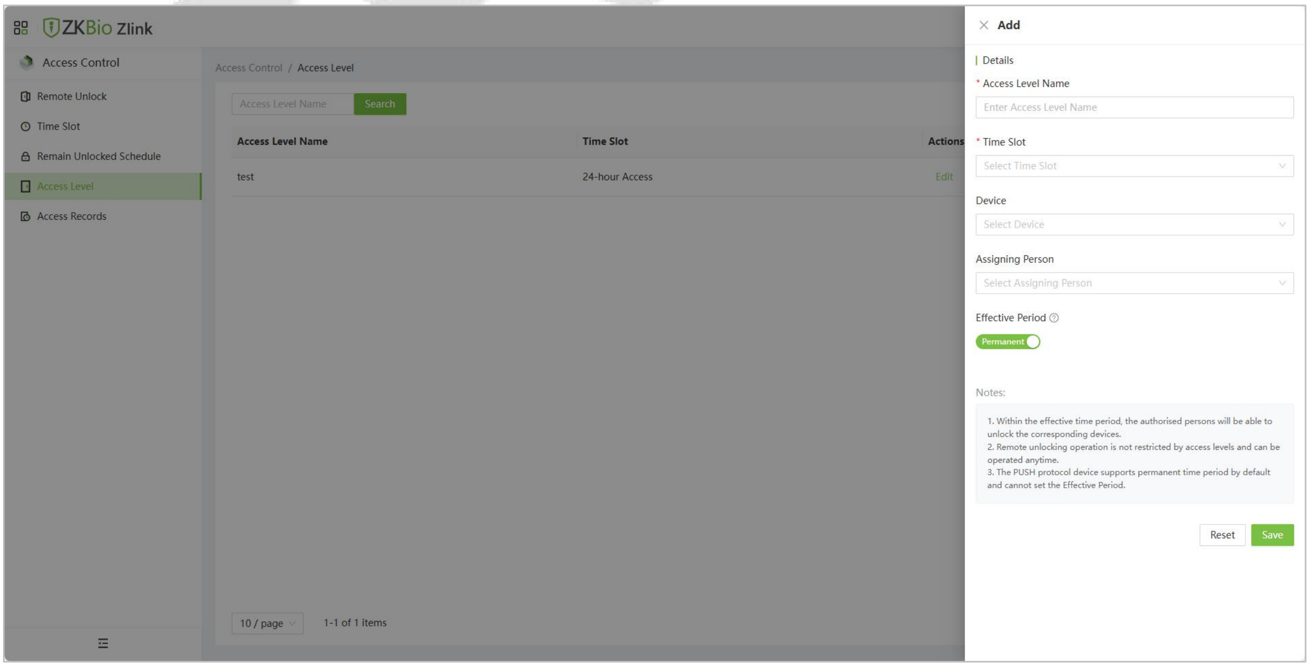
PUSH devices only support the three earliest time slots per day

4. Click [**Access Level**] > [**Add**] to add an access level.



Access Level Name	Time Slot	Actions
test	24-hour Access	Edit Delete

5. Set the access level name, select the time slot, device, and persons, then click **Save** to synchronize the access level to the device.



Access Level Name	Time Slot	Actions
test	24-hour Access	Edit

Add

Details

* Access Level Name: Enter Access Level Name

* Time Slot: Select Time Slot

Device: Select Device

Assigning Person: Select Assigning Person

Effective Period: Permanent

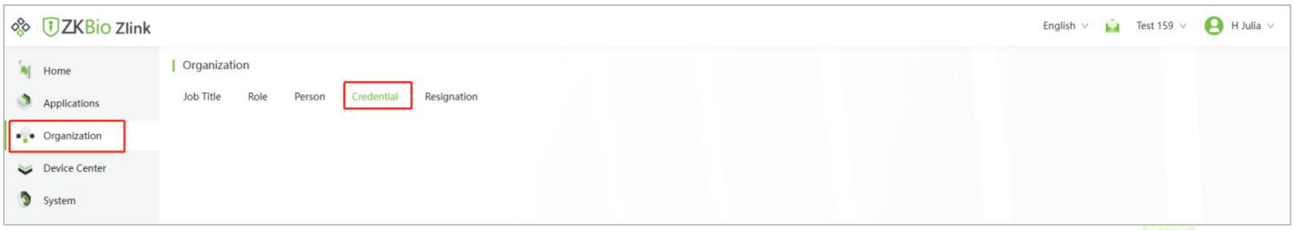
Notes:

1. Within the effective time period, the authorised persons will be able to unlock the corresponding devices.
2. Remote unlocking operation is not restricted by access levels and can be operated anytime.
3. The PUSH protocol device supports permanent time period by default and cannot set the Effective Period.

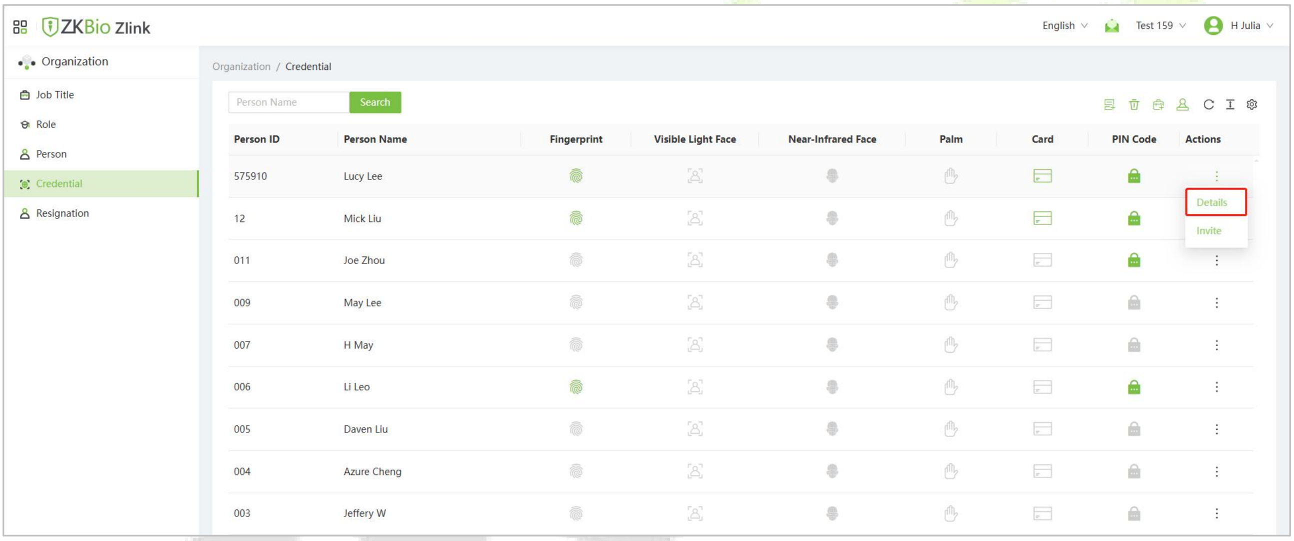
Reset Save

18.4 Register Verification Mode on the Web

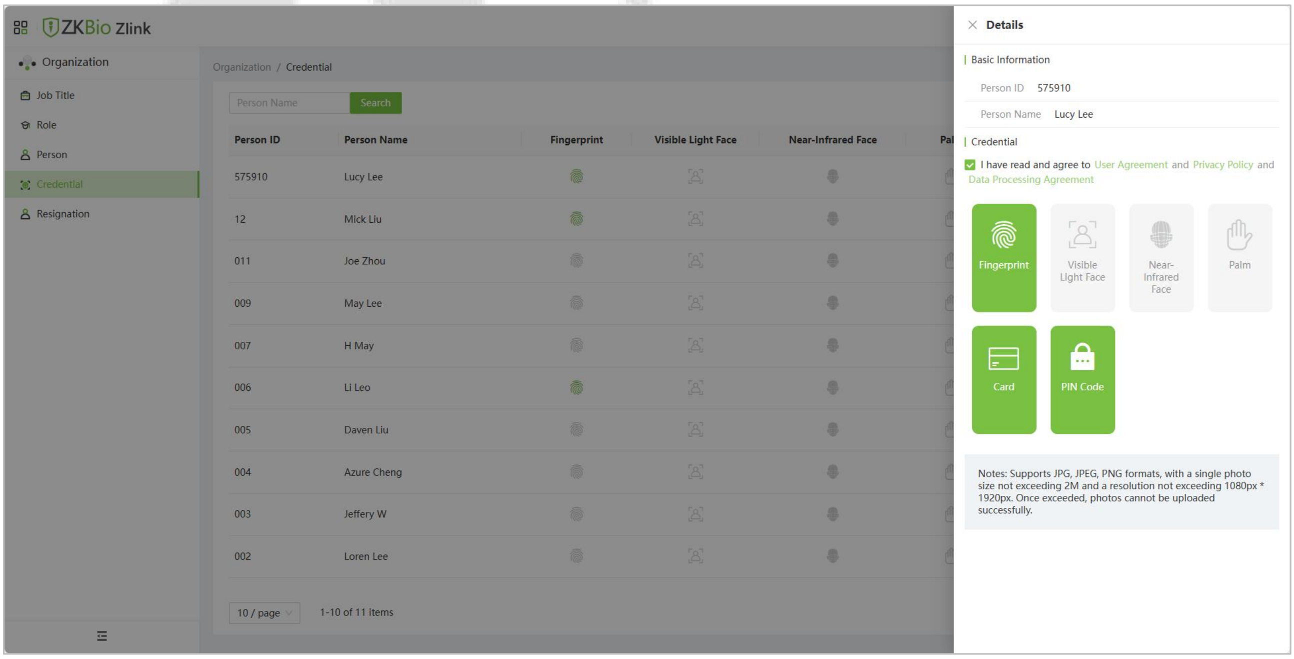
1. Click the 88 icon on the top left corner, and click [**Organization**] > [**Credential**] to enter the credentials setting interface.



2. Select the person and click **Details** that follows, check "I have read and agree to User Agreement and Privacy Policy and Data Processing Agreement" and click **Fingerprint/Face★/Card/PIN Code** to remotely register the personnel biometric verification mode.



Person ID	Person Name	Fingerprint	Visible Light Face	Near-Infrared Face	Palm	Card	PIN Code	Actions
575910	Lucy Lee	●	○	○	○	●	●	⋮
12	Mick Liu	●	○	○	○	●	●	⋮
011	Joe Zhou	○	○	○	○	○	●	⋮
009	May Lee	○	○	○	○	○	○	⋮
007	H May	○	○	○	○	○	○	⋮
006	Li Leo	●	○	○	○	○	●	⋮
005	Daven Liu	○	○	○	○	○	○	⋮
004	Azure Cheng	○	○	○	○	○	○	⋮
003	Jeffery W	○	○	○	○	○	○	⋮



Details

Basic Information

Person ID 575910

Person Name Lucy Lee

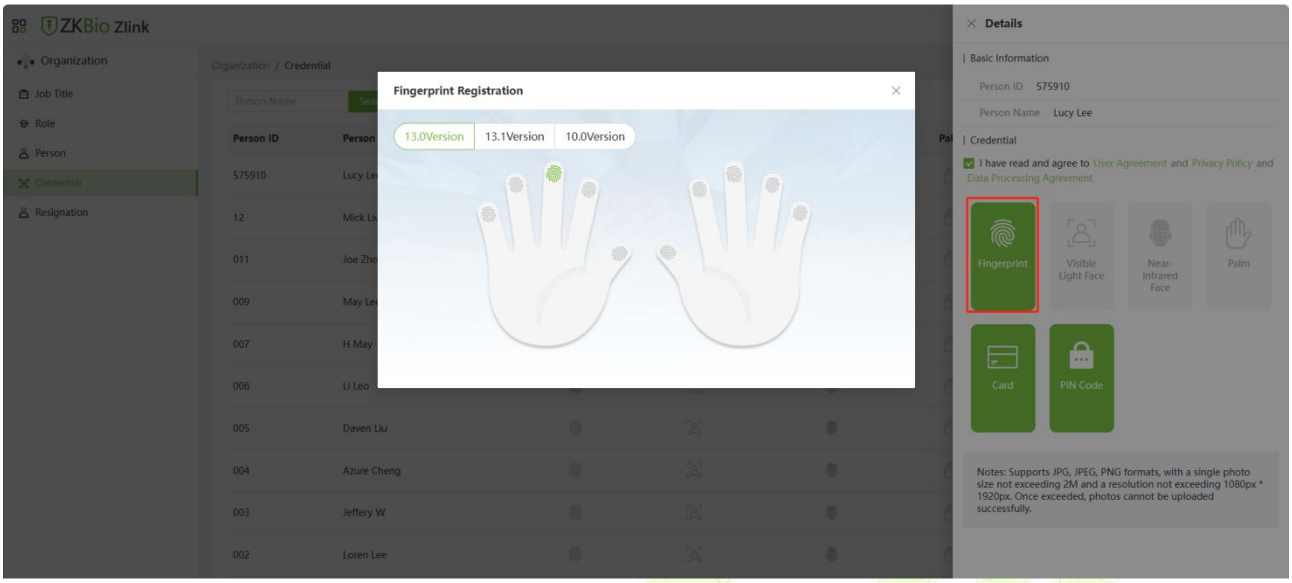
Credential

☑ I have read and agree to User Agreement and Privacy Policy and Data Processing Agreement

Notes: Supports JPG, JPEG, PNG formats, with a single photo size not exceeding 2M and a resolution not exceeding 1080px * 1920px. Once exceeded, photos cannot be uploaded successfully.

- **Register Fingerprint**

1. Click **Fingerprint** in the Details page. Choose the hand and finger to be enrolled in the pop-up prompt window.



Person ID	Person
575910	Lucy Le
12	Mick Li
011	Joe Zho
009	May Le
007	H May
006	Li Leo
005	Daven Liu
004	Azure Cheng
003	Jeffery W
002	Loren Lee

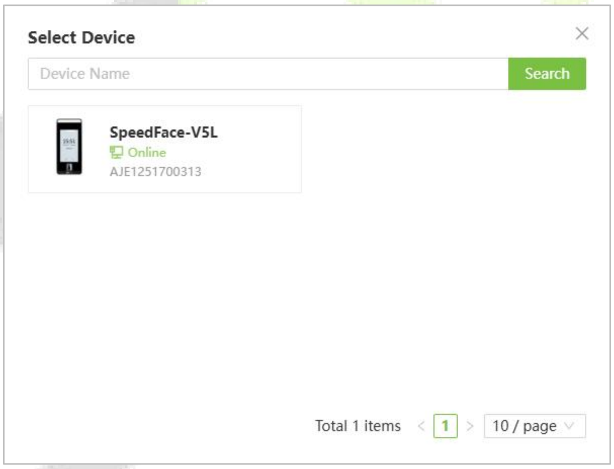
Person ID 575910

Person Name Lucy Lee

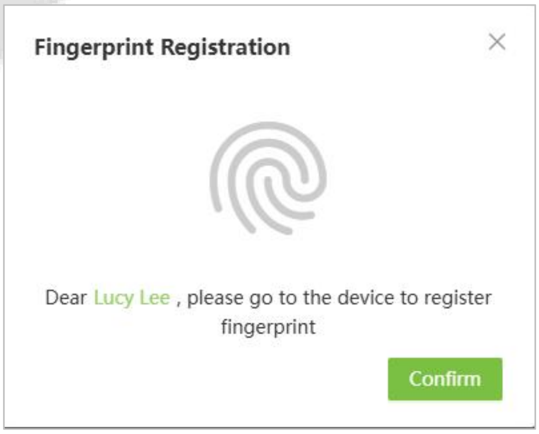
☑ I have read and agree to User Agreement and Privacy Policy and Data Processing Agreement

Notes: Supports JPG, JPEG, PNG formats, with a single photo size not exceeding 2M and a resolution not exceeding 1080px * 1920px. Once exceeded, photos cannot be uploaded successfully.

2. Select the registration device, the device will display the fingerprint registration screen. According to the prompts, place your finger on the fingerprint sensor and press 3 times. When the interface prompts "Enrolled Successfully", it means the fingerprint registration is successful.



SpeedFace-V5L
Online
AJE1251700313

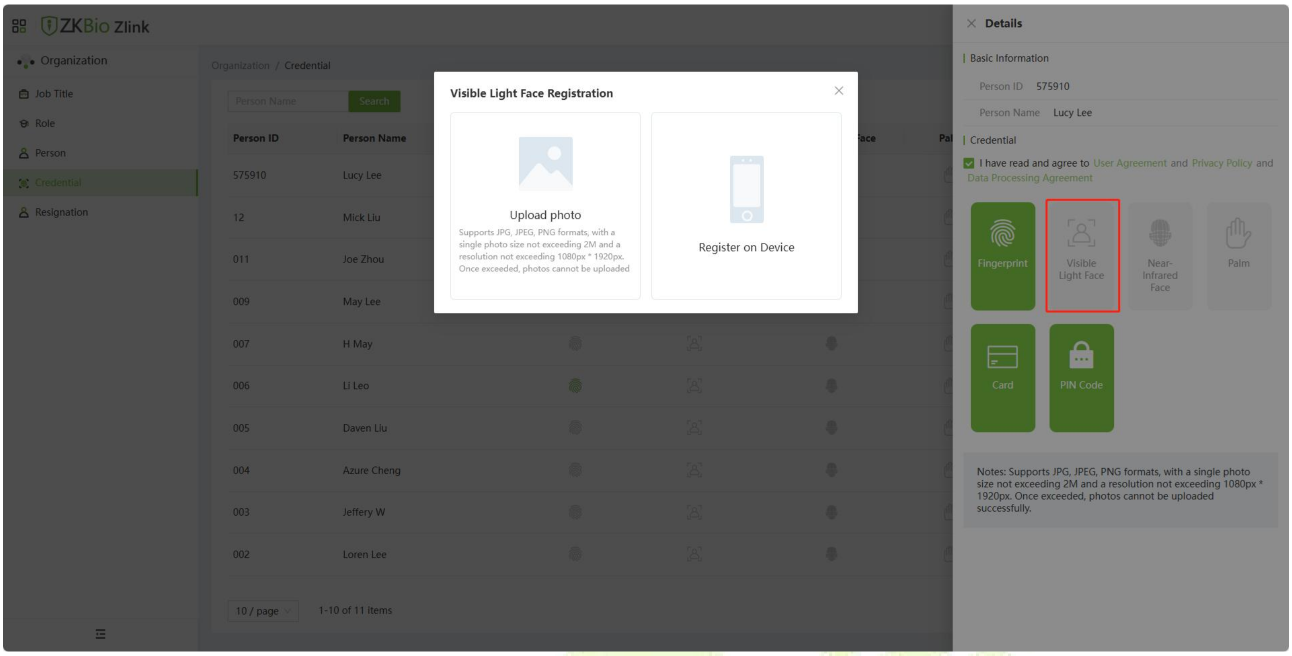


Dear Lucy Lee , please go to the device to register fingerprint

3. And you can repeat the above operation to register other fingers.

- **Register Face**

1. Click **Visible Light Face** in the Details page. You can select **Upload photo** or **Register on Device** to Register.



Person ID	Person Name
575910	Lucy Lee
12	Mick Liu
011	Joe Zhou
009	May Lee
007	H May
006	Li Leo
005	Daven Liu
004	Azure Cheng
003	Jeffery W
002	Loren Lee

Visible Light Face Registration

Upload photo

Supports JPG, JPEG, PNG formats, with a single photo size not exceeding 2M and a resolution not exceeding 1080px * 1920px. Once exceeded, photos cannot be uploaded

Register on Device

Details

Basic Information

Person ID 575910

Person Name Lucy Lee

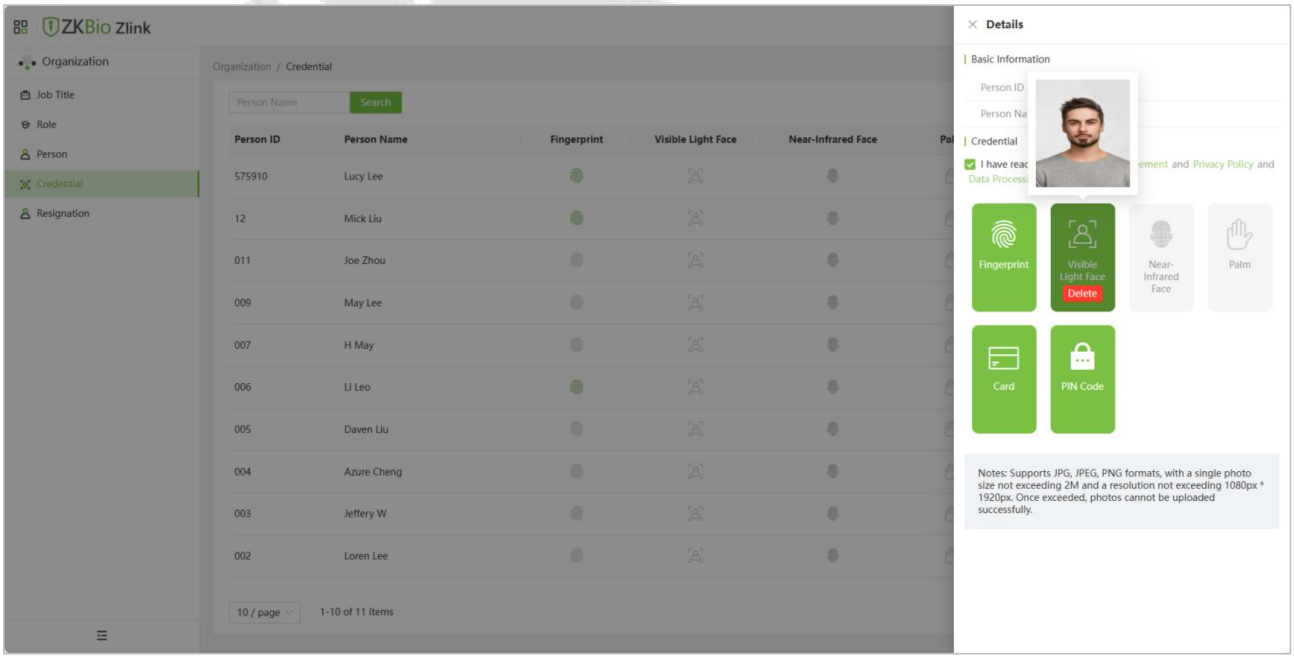
Credential

☑ I have read and agree to User Agreement and Privacy Policy and Data Processing Agreement

Notes: Supports JPG, JPEG, PNG formats, with a single photo size not exceeding 2M and a resolution not exceeding 1080px * 1920px. Once exceeded, photos cannot be uploaded successfully.

✧ Upload photo

Click **Upload photo** on the pop-up window. After selecting the facial photo to be uploaded in the open folder, the photos will be uploaded automatically. When "**Added Successfully**" is prompted, it means the upload is successful. When the mouse moves to the **Visible Light Face** menu, the photo will be displayed.The effect is as shown in the picture below.



Person ID	Person Name	Fingerprint	Visible Light Face	Near-Infrared Face
575910	Lucy Lee	●	○	○
12	Mick Liu	●	○	○
011	Joe Zhou	○	○	○
009	May Lee	○	○	○
007	H May	○	○	○
006	Li Leo	●	○	○
005	Daven Liu	○	○	○
004	Azure Cheng	○	○	○
003	Jeffery W	○	○	○
002	Loren Lee	○	○	○

Details

Basic Information

Person ID

Person Na

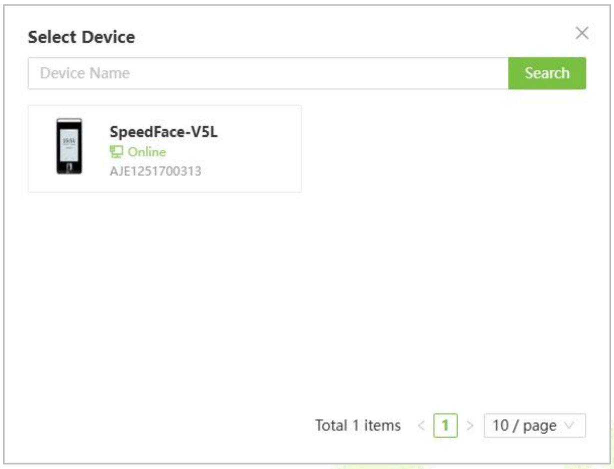
Credential

☑ I have reac ement and Privacy Policy and Data Process

Notes: Supports JPG, JPEG, PNG formats, with a single photo size not exceeding 2M and a resolution not exceeding 1080px * 1920px. Once exceeded, photos cannot be uploaded successfully.

✧ Register on Device

Click **Register on Device** on the pop-up window. Select the registration device, the device will display the facial registration screen. Please make sure that the face template in the centre of the screen during registration. When the interface prompts "Data synced successfully", it means the face registration is successful.

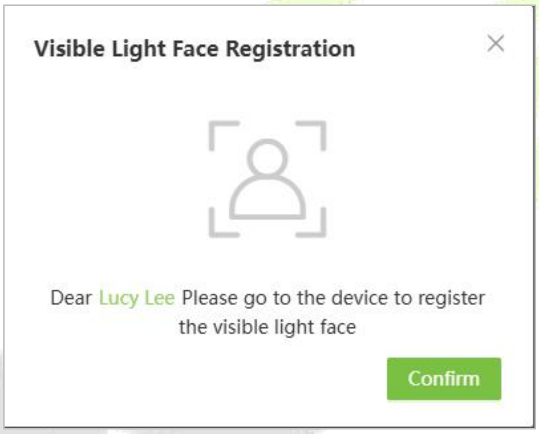


Select Device

Device Name

SpeedFace-V5L
Online
AJE1251700313

Total 1 items < 1 > 10 / page

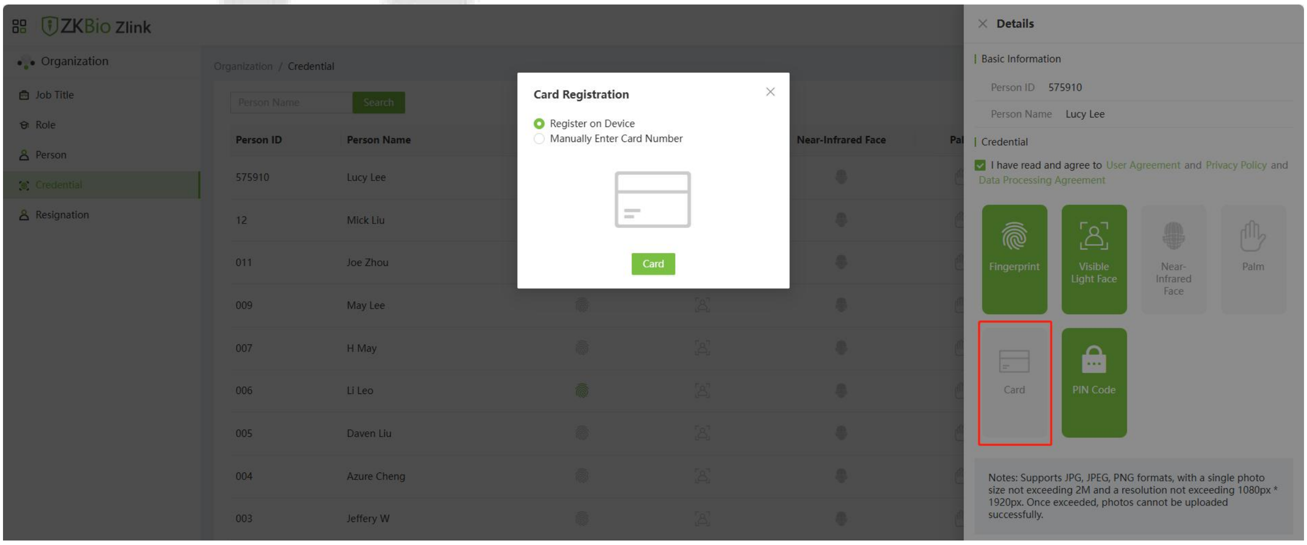


Visible Light Face Registration

Dear Lucy Lee Please go to the device to register the visible light face

- **Register Card**

1. Click **Card** in the Details page. You can select Register on Device or Manually Enter Card Number. If you want to register on device, then click **Register on Device**.



Person ID	Person Name
575910	Lucy Lee
12	Mick Liu
011	Joe Zhou
009	May Lee
007	H May
006	Li Leo
005	Daven Liu
004	Azure Cheng
003	Jeffery W

Card Registration

● Register on Device
○ Manually Enter Card Number

Details

Basic Information

Person ID 575910

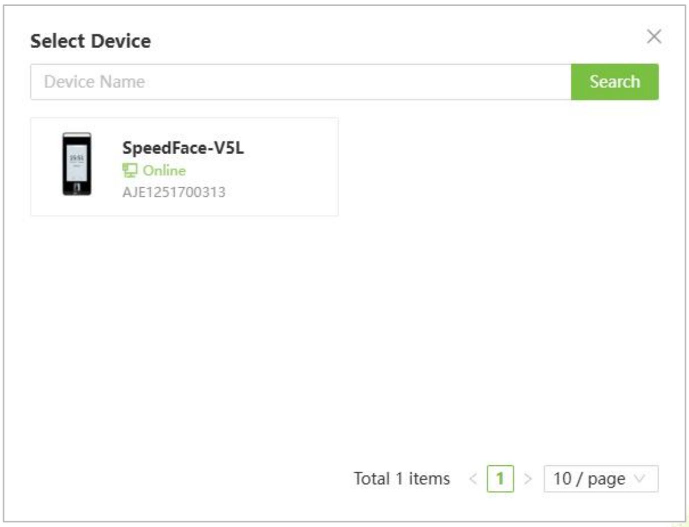
Person Name Lucy Lee

Credential

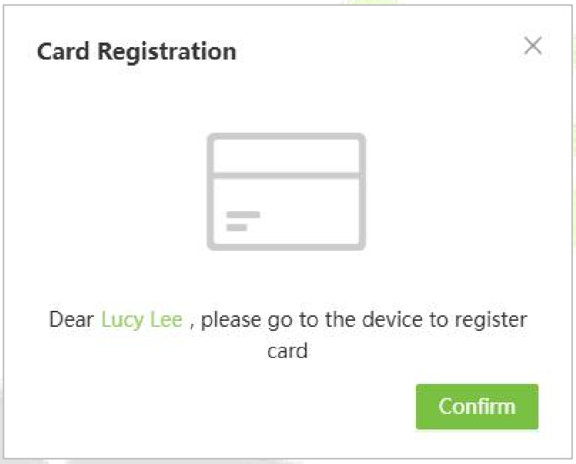
☑ I have read and agree to User Agreement and Privacy Policy and Data Processing Agreement

Notes: Supports JPG, JPEG, PNG formats, with a single photo size not exceeding 2M and a resolution not exceeding 1080px * 1920px. Once exceeded, photos cannot be uploaded successfully.

2. Select the registration device, the device will display the **Enroll Card Number** interface. Place the card in the swipe area, when the display shows green √ , it means the card is successfully registered.



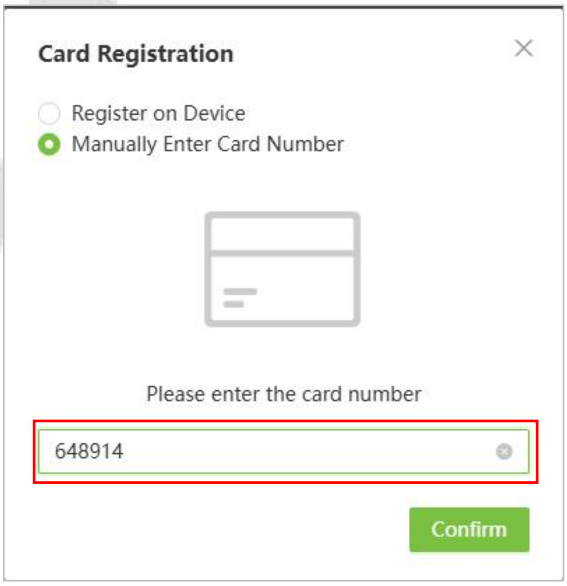
Select Device



Card Registration

Dear Lucy Lee , please go to the device to register card

3. If you select **Manually Enter Card Number**. Simply enter your card number directly into the input field below.



Card Registration

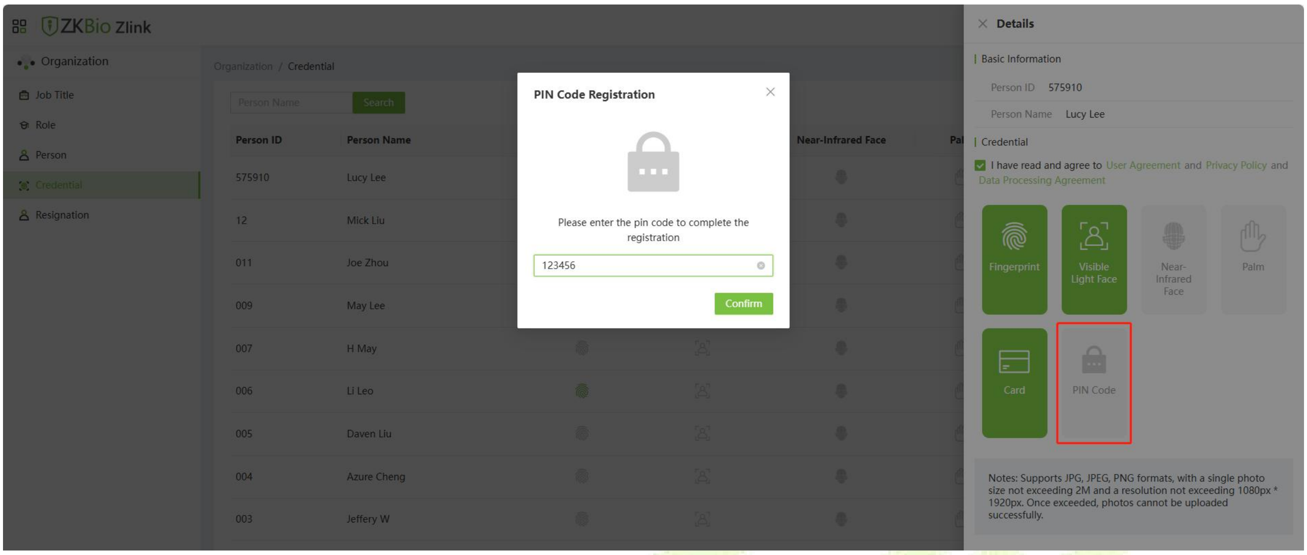
○ Register on Device
● Manually Enter Card Number

Please enter the card number

648914

- **Register Password**

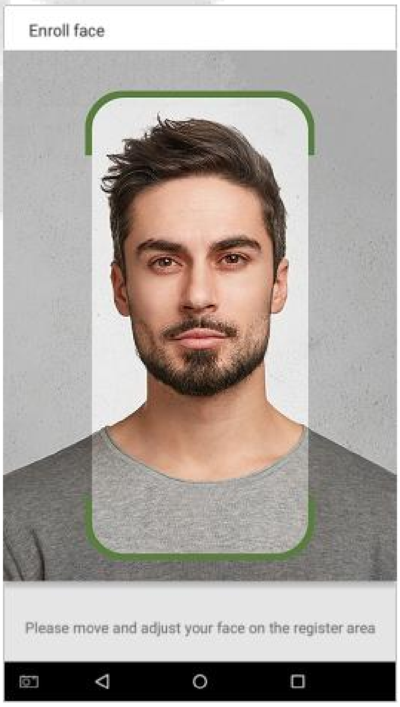
Click **PIN Code** in the Details page. Set the password in the pop-up prompt window, and then click [**Confirm**].



Appendix 1

Requirements of 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 on the face.
2) Do not place the device towards outdoor light sources like door or window or other harsh light sources.
3) Dark-color apparels other than the background color are recommended for registration.
4) Expose your face and forehead properly and do not cover your face and eyebrows with your hair.
5) It is recommended to show a normal facial expression. (A smile is acceptable, but do not close your eyes, or incline your head to any orientation).
6) Two images are required for persons with eyeglasses, one image with eyeglasses and one other without them.
7) Do not wear accessories like scarf or mask that may cover your mouth or chin.
8) Please face right towards the capturing device and locate your face in the image capturing area as shown in the image below.
9) Do not include more than one face in the capturing area.
10) A distance of 50cm to 80cm is recommended for capturing the image. (the distance is adjustable, subject to body height).



Enroll face

Please move and adjust your face on the register area

Requirements for Visible Light Digital Face Template Data

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

- **Eye Distance**

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

- **Facial Expression**

A neutral face or smile with eyes naturally open are recommended.

- **Gesture and Angel**

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

- **Accessories**

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

- **Face**

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

- **Image Format**

Should be in BMP, JPG or JPEG.

- **Data Requirement**

Should comply with the following requirements:

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

Appendix 2

Privacy Policy

Notice:

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

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

I. Collected Information

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

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

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

II. Product Security and Management

1. When you use our products for the first time, you shall set the Administrator privilege before performing specific operations. Otherwise, you will be frequently reminded to set the Administrator privilege when you enter the main menu interface. **If you still do not set the Administrator privilege after receiving the system prompt, you should be aware of the possible security risk (for example, the data may be manually modified).**

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

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

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

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

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

III. How we handle personal information of minors

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

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

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

IV. Others

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

Eco-friendly Operation

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

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

Hazardous or Toxic substances and their quantities

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

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

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

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

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

Phone : +86 769 - 82109991

Fax : +86 755 - 89602394

www.zkteco.com