

# USER MANUAL

## ProFace X

---

Version: 1.0

Date: November 2025

English

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](mailto:sales@zkteco.com).

To know more about our global branches, visit [www.zkteco.com](http://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 template-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 **ProFace X**.

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
<b>Bold font</b>	Used to identify software interface template names e.g. <b>OK</b> , <b>Confirm</b> , <b>Cancel</b> .
>	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

<b>DATA SECURITY STATEMENT .....</b>	<b>9</b>
<b>SAFETY MEASURES .....</b>	<b>9</b>
<b>1. INSTRUCTION FOR USE .....</b>	<b>11</b>
1.1 STANDING POSITION, POSTURE, AND FACIAL EXPRESSION .....	11
1.2 FACE TEMPLATE REGISTRATION .....	12
1.3 STANDBY INTERFACE .....	13
1.4 VIRTUAL KEYBOARD .....	14
1.5 VERIFICATION MODE .....	15
1.5.1 FACIAL VERIFICATION .....	15
1.5.2 CARD VERIFICATION .....	17
1.5.3 PASSWORD VERIFICATION .....	18
1.5.4 COMBINED VERIFICATION .....	21
<b>2. MAIN MENU .....</b>	<b>22</b>
<b>3. USER MANAGEMENT .....</b>	<b>24</b>
3.1 USER REGISTRATION .....	24
3.1.1 USER ID AND NAME .....	24
3.1.2 USER ROLE .....	25
3.1.3 FACE TEMPLATE .....	25
3.1.4 CARD .....	26
3.1.5 PASSWORD .....	27
3.1.6 PROFILE PHOTO .....	27
3.1.7 ACCESS CONTROL ROLE .....	28
3.2 SEARCH FOR USERS .....	28
3.3 EDIT USER .....	29
3.4 DELETE USER .....	30
3.5 DISPLAY STYLE .....	31
<b>4. USER ROLE .....</b>	<b>32</b>
<b>5. COMMUNICATION SETTINGS .....</b>	<b>34</b>
5.1 NETWORK SETTINGS .....	34
5.2 SERIAL COMM .....	35
5.3 WIRELESS NETWORK★ .....	36
5.4 PC CONNECTION .....	38
5.5 CLOUD SERVER SETTING .....	39
5.6 WIEGAND SETUP .....	40
5.6.1 WIEGAND INPUT .....	40
5.6.2 WIEGAND OUTPUT .....	43
5.7 NETWORK DIAGNOSIS .....	43
<b>6. SYSTEM SETTINGS .....</b>	<b>45</b>
6.1 DATE AND TIME .....	45
6.2 ACCESS LOGS SETTINGS/ATTENDANCE .....	47

6.3 FACE TEMPLATE PARAMETERS .....	49
6.4 TEMPERATURE MANAGEMENT .....	51
6.5 HEALTH PROTECTION .....	51
6.6 DEVICE TYPE SETTING .....	52
6.7 SECURITY SETTING .....	53
6.8 TAP-TO-UNLOCK.....	54
6.9 UPDATE FIRMWARE ONLINE .....	55
6.10 FACTORY RESET .....	56
<b>7. PERSONALIZE SETTINGS .....</b>	<b>57</b>
7.1 USER INTERFACE SETTINGS .....	57
7.2 VOICE SETTINGS .....	58
7.3 BELL SCHEDULES .....	58
7.4 PUNCH STATES OPTIONS .....	60
7.5 SHORTCUT KEYS MAPPINGS .....	61
<b>8. DATA MANAGEMENT .....</b>	<b>63</b>
8.1 DELETE DATA .....	63
<b>9. INTERCOM★ .....</b>	<b>65</b>
9.1 SIP SETTINGS .....	65
9.1.1 LOCAL SETTINGS .....	66
9.1.2 AUDIO OPTIONS .....	67
9.1.3 VIDEO OPTIONS .....	67
9.1.4 CALL OPTIONS .....	68
9.1.5 CONTACT LIST .....	69
9.1.6 CALLING SHORTCUT SETTINGS .....	70
9.1.7 ADVANCED SETTINGS .....	71
9.2 DOORBELL SETTING .....	72
9.3 ONVIF SETTINGS .....	72
<b>10. ACCESS CONTROL .....</b>	<b>75</b>
10.1 ACCESS CONTROL OPTIONS .....	76
10.2 TIME RULE SETTING/TIME SCHEDULE .....	78
10.3 HOLIDAYS .....	81
10.4 ACCESS GROUPS ★ .....	82
10.5 COMBINED VERIFICATION .....	83
10.6 ANTI-PASSBACK SETUP .....	84
10.7 DURESS OPTIONS .....	86
<b>11. ATTENDANCE SEARCH .....</b>	<b>87</b>
<b>12. AUTOTEST .....</b>	<b>89</b>
<b>13. SYSTEM INFORMATION .....</b>	<b>90</b>
<b>14. CONNECT TO ZKBIO CVSECURITY SOFTWARE .....</b>	<b>91</b>
14.1 SET THE COMMUNICATION ADDRESS .....	91
14.2 ADD DEVICE ON THE SOFTWARE .....	92

14.3 ADD PERSONNEL ON THE SOFTWARE AND ONLINE FINGERPRINT/FACE REGISTRATION .....	93
<b>15. SIP VIDEO INTERCOM .....</b>	<b>94</b>
15.1 LOCAL AREA NETWORK USE .....	94
15.1.1 CALL CONTACT LIST .....	100
15.1.2 CUSTOM THE CALLING SHORTCUT KEYS .....	100
15.1.3 DIRECT CALLING .....	101
15.2 SIP SERVER .....	102
15.2.1 SIP SERVER CONFIGURATION .....	103
15.2.2 ADD DEVICE .....	107
15.2.3 CREATE EXTENSION NUMBERS .....	109
15.2.4 CONTACT LIST .....	110
15.2.5 ASSIGNMENT OF EXTENSION NUMBERS AND SIP ACCOUNTS .....	112
15.2.6 PC CLIENT FUNCTIONALITY .....	118
15.2.7 MAKE A CALL .....	121
<b>APPENDIX 1 .....</b>	<b>127</b>
REQUIREMENTS OF LIVE COLLECTION AND REGISTRATION OF VISIBLE LIGHT FACE TEMPLATES .....	127
REQUIREMENTS FOR VISIBLE LIGHT DIGITAL FACE TEMPLATE DATA .....	128
<b>APPENDIX 2 .....</b>	<b>129</b>
PRIVACY POLICY .....	129
ECO-FRIENDLY OPERATION .....	131

## Data Security Statement

ZKTeco, as a smart product supplier, may also need to know and collect some of your personal information 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 following precautions are to keep the user's safety and prevent any damage. Please read carefully before installation.

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. Accessories not recommended by the manufacturer must not be used.
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 main AC or DC power source and refer service personnel under the following conditions:
  - When cord or connection control is affected.
  - When the liquid was spilled, or an item was dropped into the system.
  - If the system is exposed to water and/or inclement weather conditions (rain, snow, and more).
  - If the system is not operating normally under the operating instructions.

Just change the controls defined in the operating instructions. Improper adjustment of other controls may result in damage and require a qualified technician to return the device to normal operation.

7. **Replacement parts** - When replacement parts are required, service technicians must only use replacement parts provided by the supplier. Unauthorized substitutes can lead to the risk of burns, electric 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 unit.
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** - External lightning conductors can be installed to protect against electrical storms. It stops power-ups destroying the system.

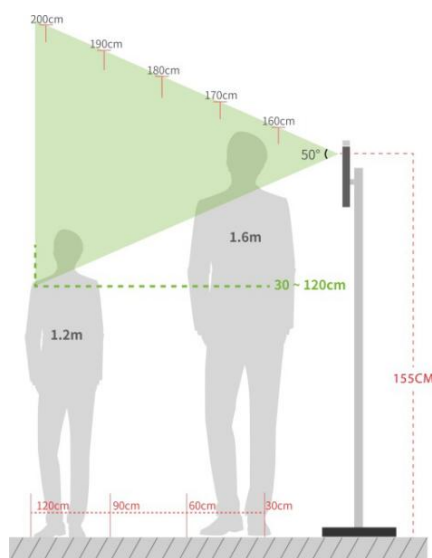
The devices should be installed in areas with limited access.

# 1. Instruction for Use

Before exploring the Device's features and functions, it is recommended to be familiar with the fundamentals listed below.

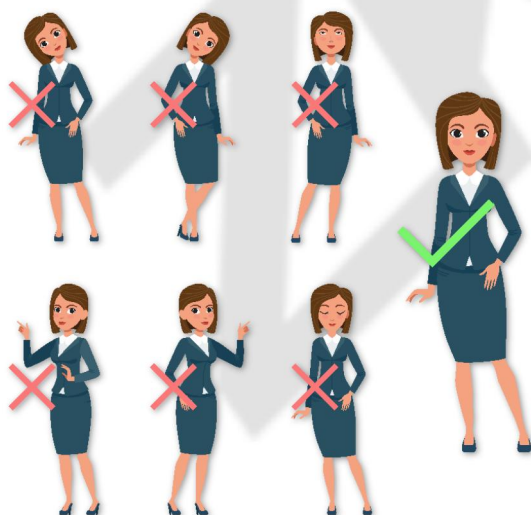
## 1.1 Standing Position, Posture, and Facial Expression

### ● The recommended distance



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

### ● Recommended standing posture and facial expression:



**Standing Posture**



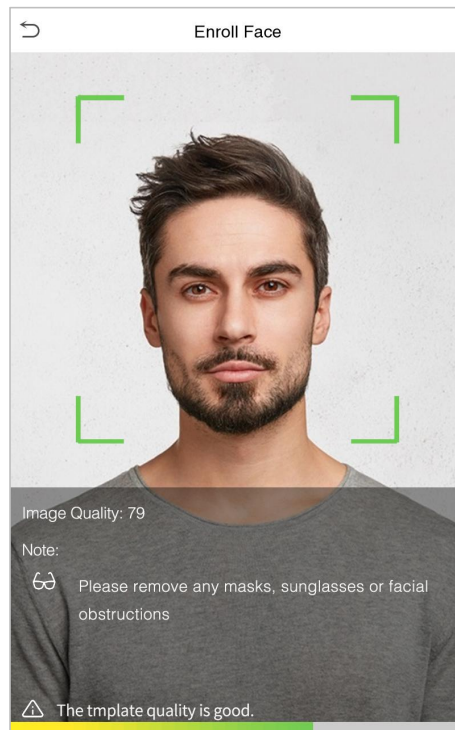
**Facial Expression**

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



## 1.2 Face Template Registration

Please make sure that the face template is in the center of the screen during registration. Please face towards the camera and stay still during face template registration. The screen should look like the image below:



### Correct face template registration and authentication method

#### ● Recommendation for Registering a Face Template

- When registering a face template, maintain a distance of 40 cm to 80 cm space between the device and the face template.
- Be careful not to change your facial expression. (Smiling face template, drawn face template, wink, etc.)
- If you do not follow the instructions on the screen, the face template 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 face templates on the screen. Register one person at a time.
- It is recommended for a user wearing glasses to register both face templates with and without glasses.

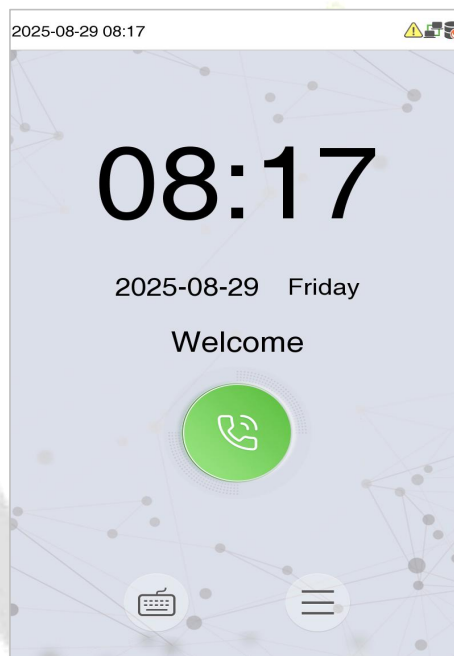





## ● Recommendation for Authenticating a Face Template

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

## 1.3 Standby Interface

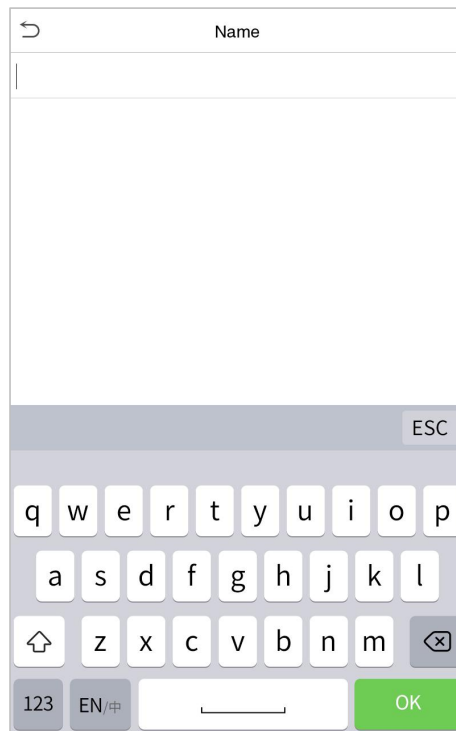
After connecting the power supply, the following standby interface template is displayed:



- Click  icon to enter the User ID input interface template.
- When there is no Super Administrator set in the device, tap  icon to go to the menu.
- After setting the Super Administrator on the device, it requires the Super Administrator's verification before entering the menu functions.
- Click  to make a video call with the connected phone.

**Note:** For the security of the device, it is recommended to register super administrator the first time you use the device.

## 1.4 Virtual Keyboard



**Note:**

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

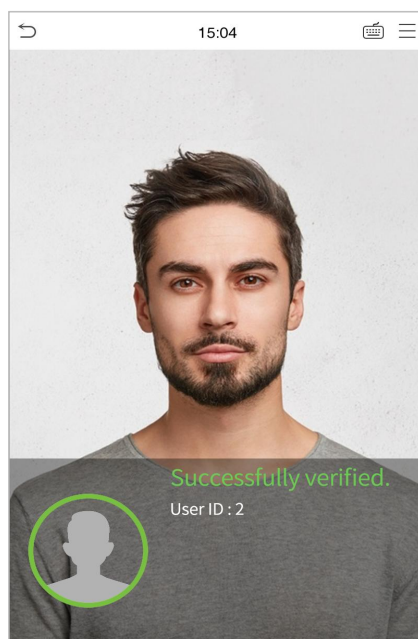
- Click **EN** to switch to the English keyboard.
- Press **123** to switch to the numeric and symbolic keyboard.
- Click **ABC** to return to the alphabetic keyboard.
- Click the input box, virtual keyboard appears.
- Click **ESC** to exit the virtual keyboard.

## 1.5 Verification Mode


### 1.5.1 Facial Verification

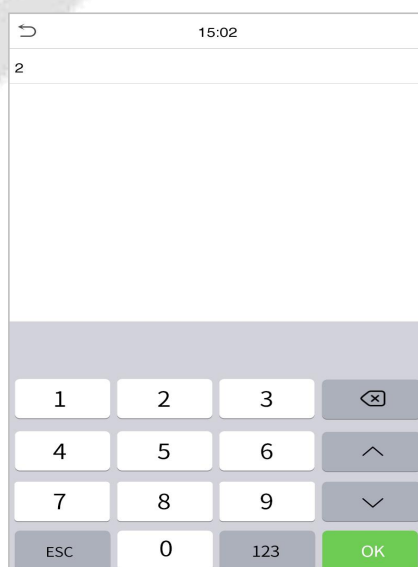
#### ● 1:N Facial Verification


The device compares the currently acquired facial images with all the registered face template data stored in its database. The following is the pop-up prompt box displaying the result of the comparison.

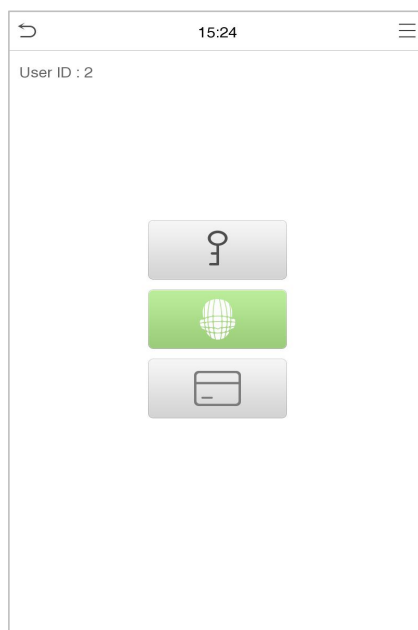


#### ● 1:1 Facial Verification

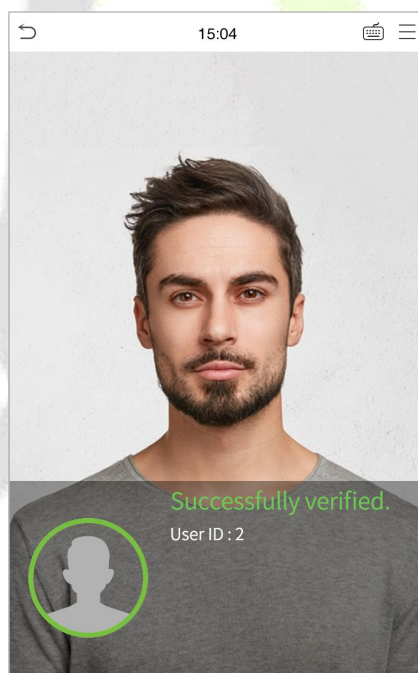
In this verification mode, the device compares the face template captured by the camera with the facial template related to the entered user ID. Press icon  in the main interface template and enter the 1:1 facial verification mode and enter the user ID, and click **OK**.



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



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



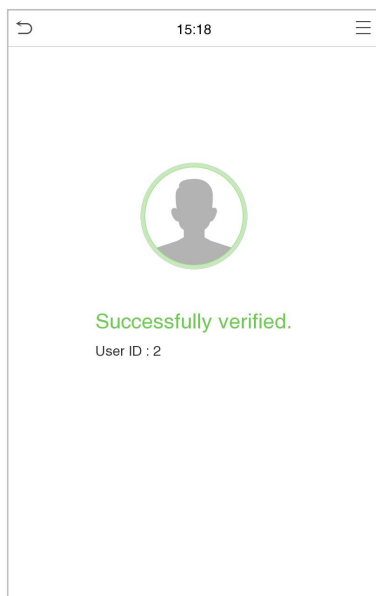
If the verification fails, it prompts **"Please adjust your position!"**.

## 1.5.2 Card Verification

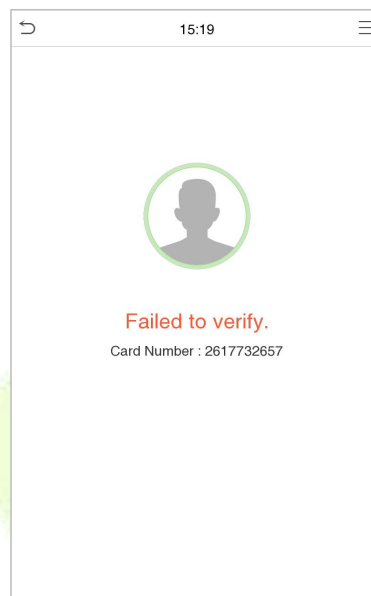
### ● 1:N Card Verification

The 1:N card verification mode compares the card number in the card induction area with all the card number data registered in the device. Place the card in the collection area for verification.

Verification is successful:




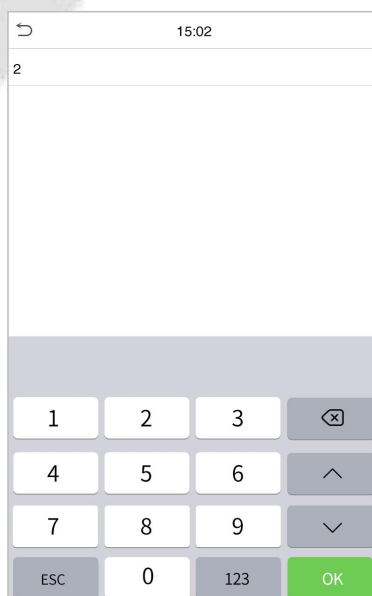
Verification failed:




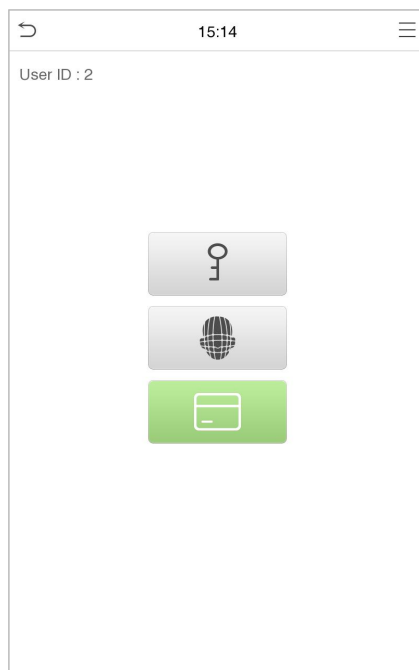
### ● 1:1 Card Verification

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

Press  in the main interface template to open the 1:1 card verification mode. Enter the user ID and click **OK**.

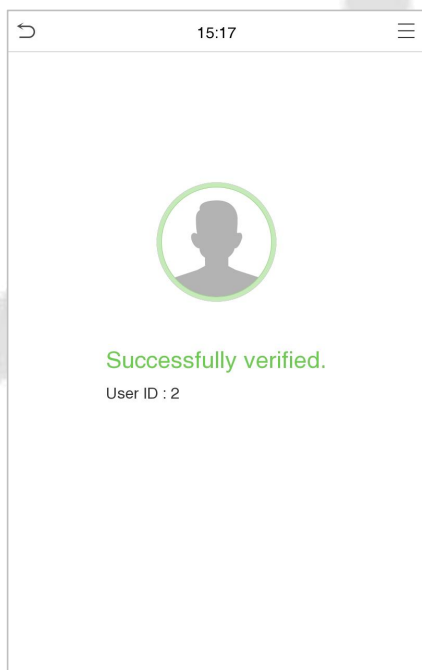


If the user has registered a face template and password in addition to his/her card, and the verification method is set to Password/Card/Face Verification, the following screen will appear. Select the  icon to enter the card verification mode.

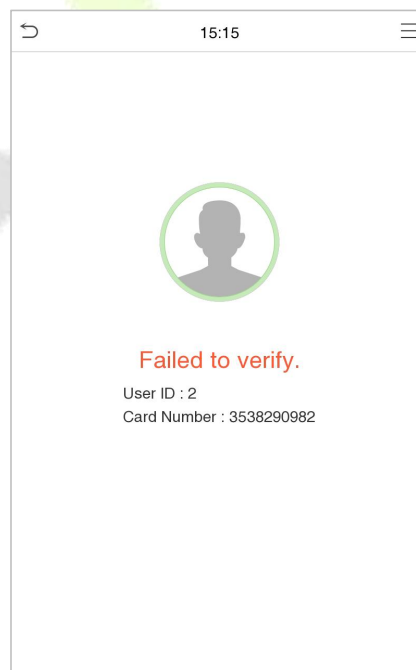


Place the card in the collection area for verification.

Verification is successful:




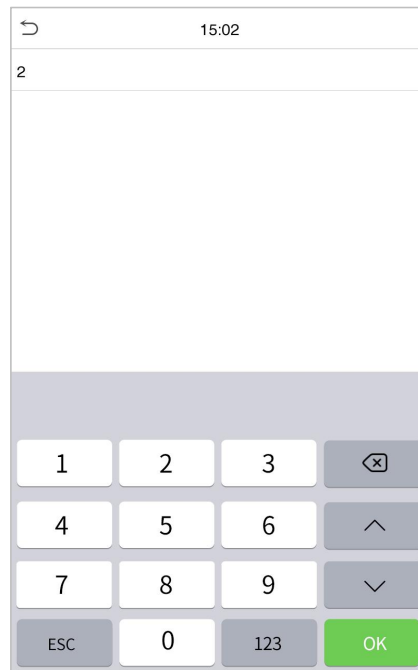
Verification failed:




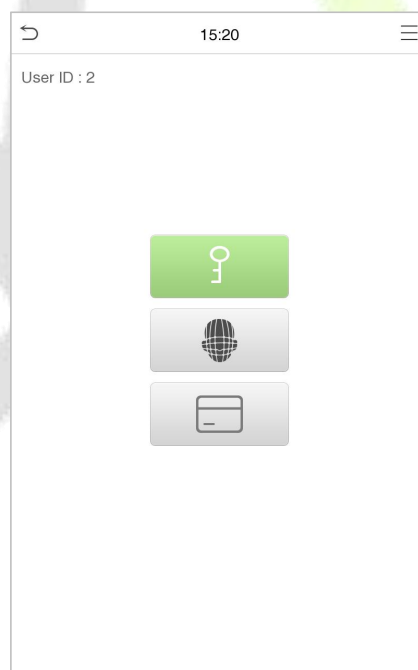
### 1.5.3 Password Verification

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

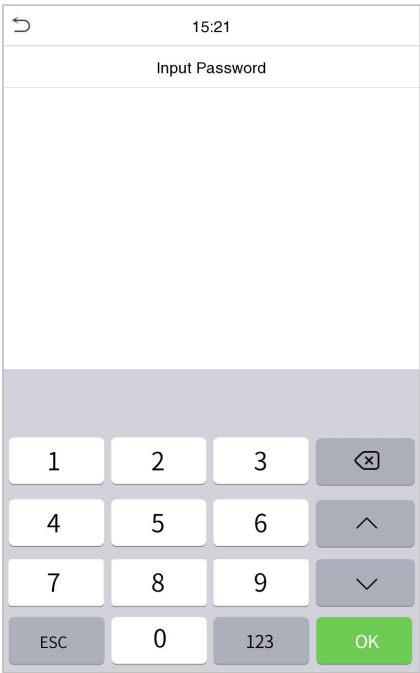
Click the  button on the main screen to enter the 1:1 password verification mode. Then, input the user ID and press **OK**.



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

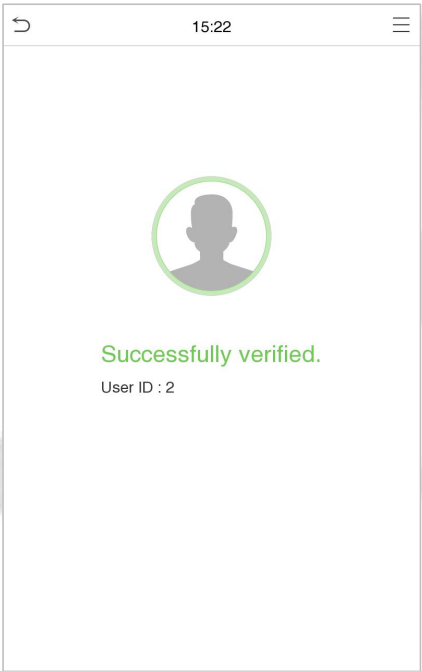


Input the password and press **OK**.

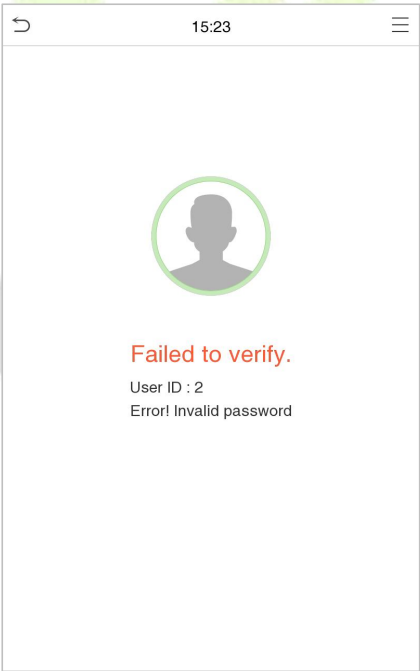


The following screen displays, after entering a correct password and a wrong password respectively.

Verification is successful:



Verification is failed:



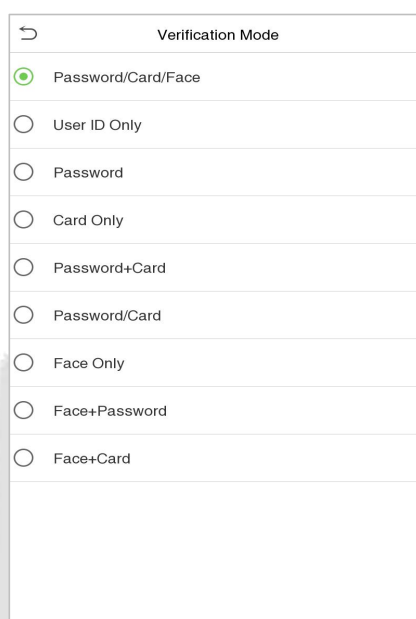


## 1.5.4 Combined Verification

To increase security, this device offers the option of using multiple forms of verification methods. A total of 9 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

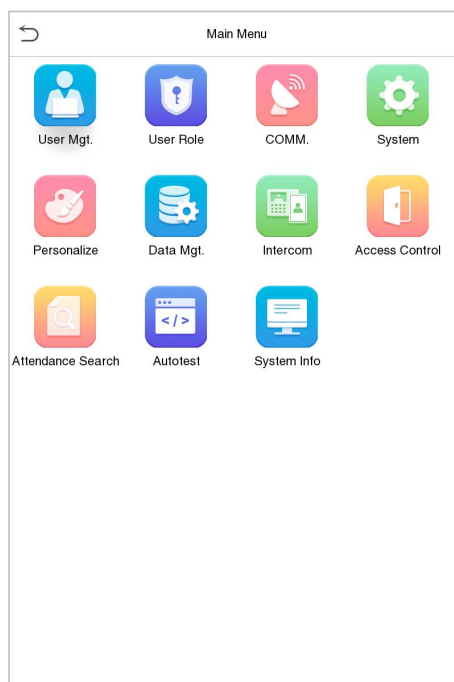
- ☒ Password/Card/Face
- ☐ User ID Only
- ☐ Password
- ☐ Card Only
- ☐ Password+Card
- ☐ Password/Card
- ☐ Face Only
- ☐ Face+Password
- ☐ Face+Card

### 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 of the person with the 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".

## 2. Main Menu

Press  on the Standby interface to enter the **Main Menu**. The following screen will be displayed:

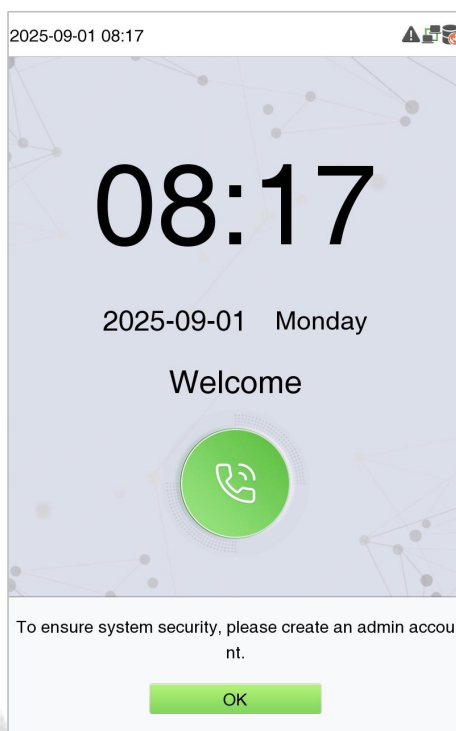


### Function Description

Menu	Descriptions
<b>User Mgt.</b>	To add, edit, view, and delete basic information of a User.
<b>User Role</b>	To set the permission scope of the custom role and enroller for the users, that is, the rights to operate the system.
<b>COMM.</b>	To set the relevant parameters of the network, serial comm, PC connection, cloud server, wiegand and network diagnosis.
<b>System</b>	To set the parameters related to the system, including date time, access logs setting, face template parameters, temperature management, health protection, device type setting, security setting, tap-to-unlock, update firmware online, and reset to factory.
<b>Personalize</b>	This includes user interface, voice, bell schedules, punch state options, and shortcut key mappings settings.
<b>Data Mgt.</b>	To delete all relevant data in the device.
<b>Intercom</b>	To set the parameters related to the SIP and NVR.
<b>Access Control</b>	To set the parameters of the lock and the relevant access control device including options like time rule, holiday settings, combine verification, anti-passback setup, and duress option settings.
<b>Attendance Search</b>	To query the specified event logs, check attendance photos and blocklist attendance photos.

<b>Autotest</b>	To automatically test whether each module functions properly, including the LCD screen, audio, microphone, camera, and real-time clock.
<b>System Info</b>	To view data capacity, device, and firmware information, and privacy policy of the device.

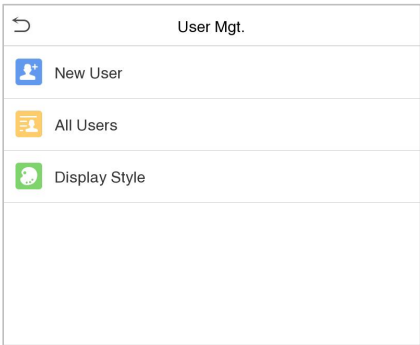
**Note:** When users use the product for the first time, they should operate it after setting administrator privileges. Tap **User Mgt.** to add an administrator or edit user permissions as a super administrator. If the product does not have an administrator setting, the system will show an administrator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



### 3. User Management

#### 3.1 User Registration

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



##### 3.1.1 User ID and Name

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

A screenshot of a mobile application form titled "New User". It has a back arrow icon in the top left corner. The form contains several input fields with labels and values: "User ID" with the value "1", "Name" with the value "Mick", "User Role" with the value "Normal User", "Face" with the value "0", "Card" with the value "0", "Password", "Profile Photo" with the value "0", and "Access Control Role". The form is enclosed in a light gray border.

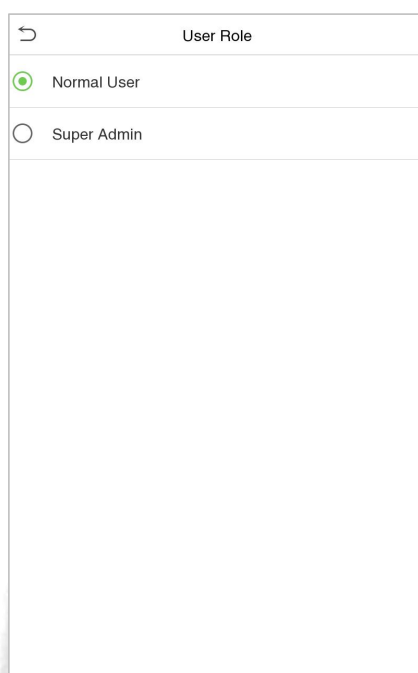
**Notes:**

- A username can contain a maximum of 34 characters.
- The user ID may contain 1 to 14 digits by default.
- During the initial registration, you can modify your ID, which cannot be modified after registration.
- If a message "**Duplicated!**" pops up, you must choose another ID as the entered User ID already exists.

### 3.1.2 User Role

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

- **Super Admin:** The Super Administrator owns all management privileges in the Device.
- **Normal User:** If the Super Admin is already registered in the Device, then the Normal Users will not have the privileges to manage the system and can only access authentication verifications.
- **User Defined Roles:** The Normal User can also be set with **User Defined Role**, which are the custom roles that can be set to the Normal User.

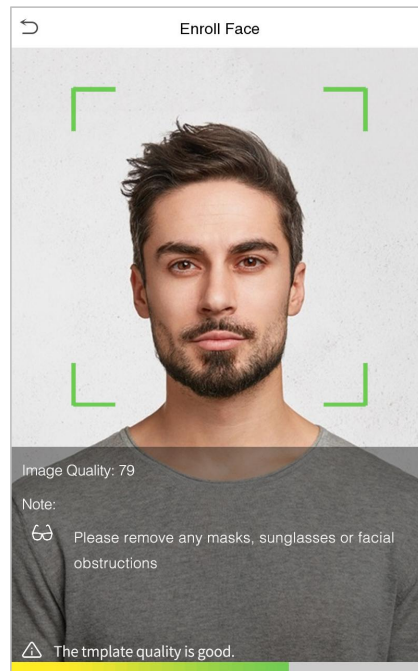


**Note:** If the selected user role is the Super Admin, the user must pass the identity authentication to access the main menu. The authentication is based on the authentication method(s) that the super administrator has registered. Please refer to [1.5 Verification Mode](#).

### 3.1.3 Face Template

Tap **Face** in the **New User** interface to enter the face template registration page.

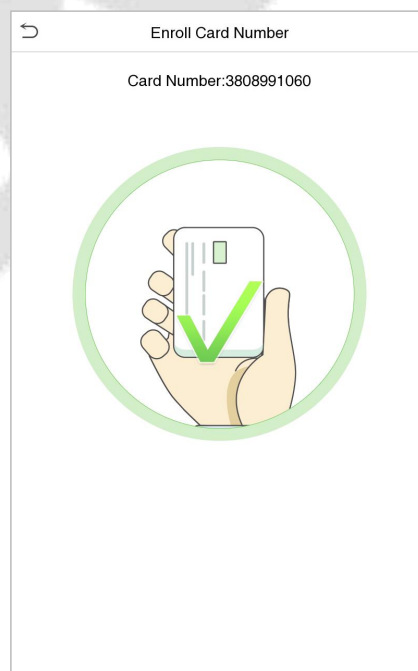
- Please face the camera directly and position your face within the white guiding box. Please remain still throughout the face template registration process.
- A progress bar will appear during the face template registration process, and the message **"Enrolled Successfully"** will be displayed upon completion.
- If the face template has already been registered, a **"Duplicate Face"** message will appear.
- The registration interface is shown below:



### 3.1.4 Card

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

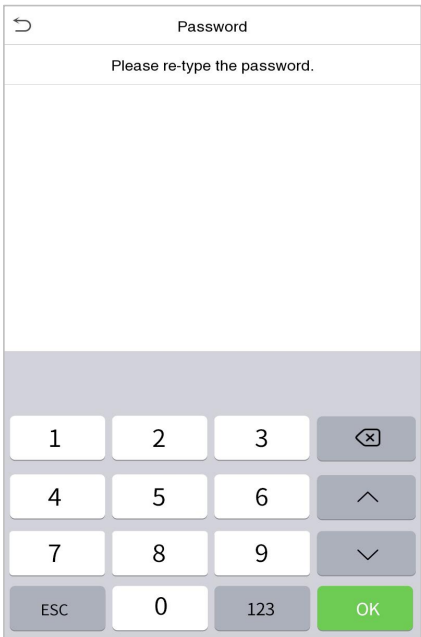
- On the Card interface, swiping card underneath the card reading area. The card registration will be successful.
- If the card is registered already, then, the “**Duplicate Card**” message will appear. The registration interface is as follows:



3.1.5 Password

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

- On the Password interface, enter the required password and re-enter to confirm it and tap **OK**.
- If the re-entered password is different from the initially entered password, then the device prompts the message as "**Password not match!**", where the user needs to re-confirm the password.

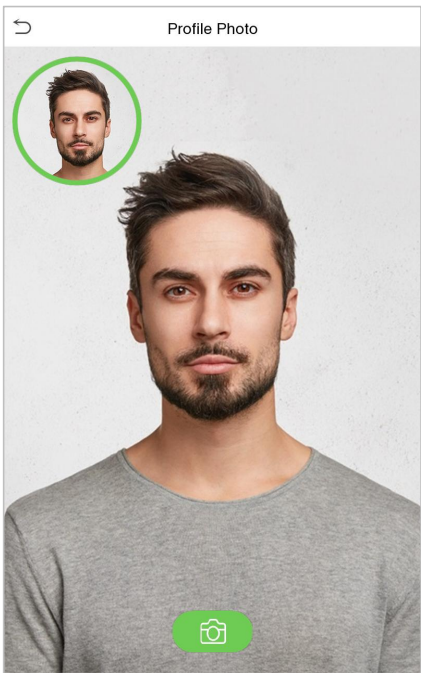


**Note:** The password may contain 6 to 8 digits by default.

3.1.6 Profile Photo

Tap on **Profile Photo** in the **New User** interface to go to the Profile Photo registration page.

New User	
User ID	1
Name	Mick
User Role	Normal User
Face	0
Card	0
Password	
Profile Photo	0
Access Control Role	



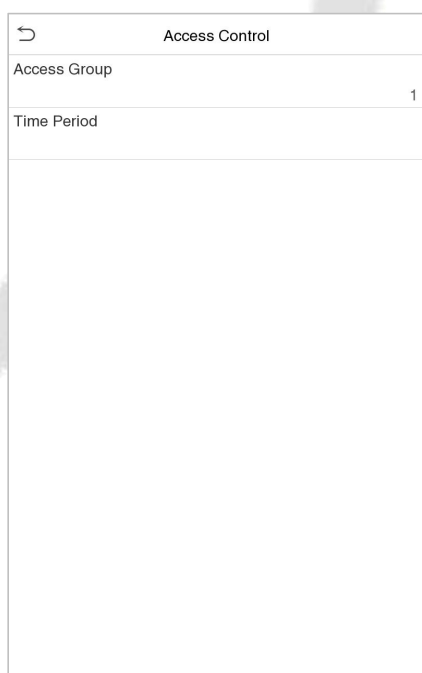
- When a user registers with a photo and passes the authentication, the registered photo will be displayed.
- Tap **Profile Photo**, the device's camera will open, then tap the camera icon to take a photo. The captured photo is displayed on the top left corner of the screen, and the camera opens again to take a new photo, after taking the initial photo.

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

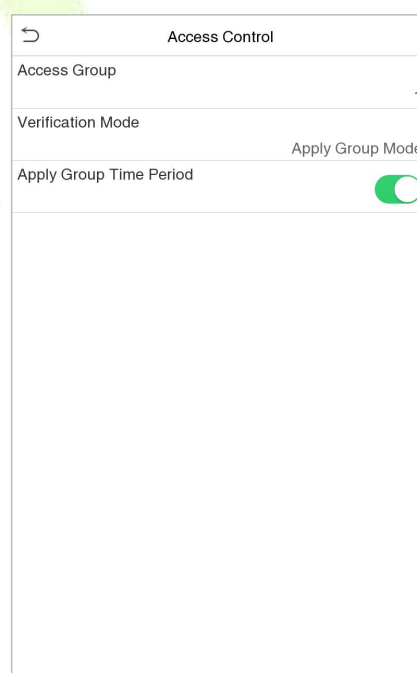
### 3.1.7 Access Control Role

The **Access Control Role** sets the door access privilege for each user. This includes the access group, duress fingerprint, and facilitates to set the group access time-period.

- Tap **Access Control Role > Access Group**, to assign the registered users to different groups for better management. New users belong to Group 1 by default and can be reassigned to other groups. The device supports up to 99 Access Control groups.
- Tap **Time Period**, to select the time period to use.
- Tap **Verification Mode**, to select the verification mode.



A&C Terminal



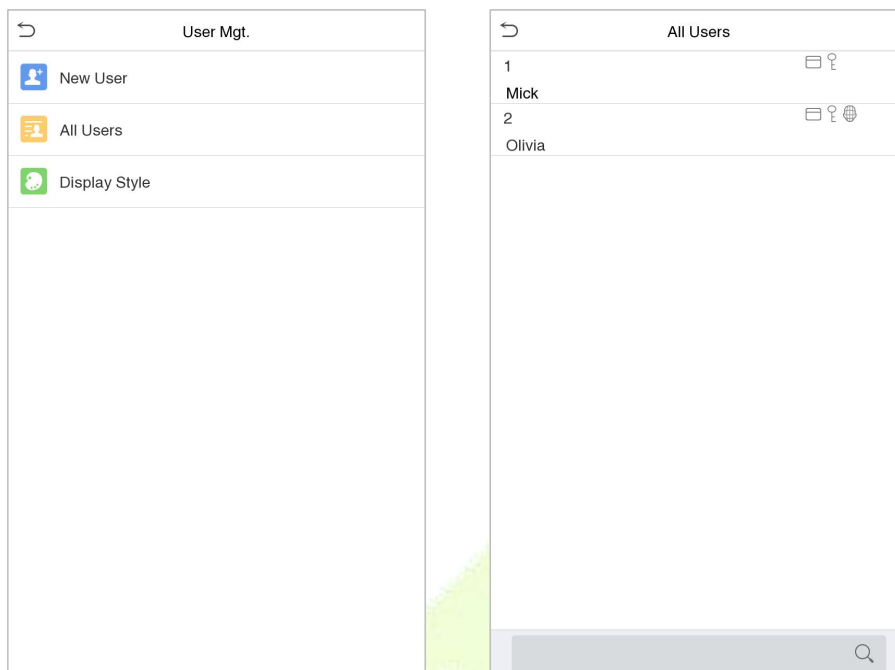
T&A Terminal

## 3.2 Search for Users

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

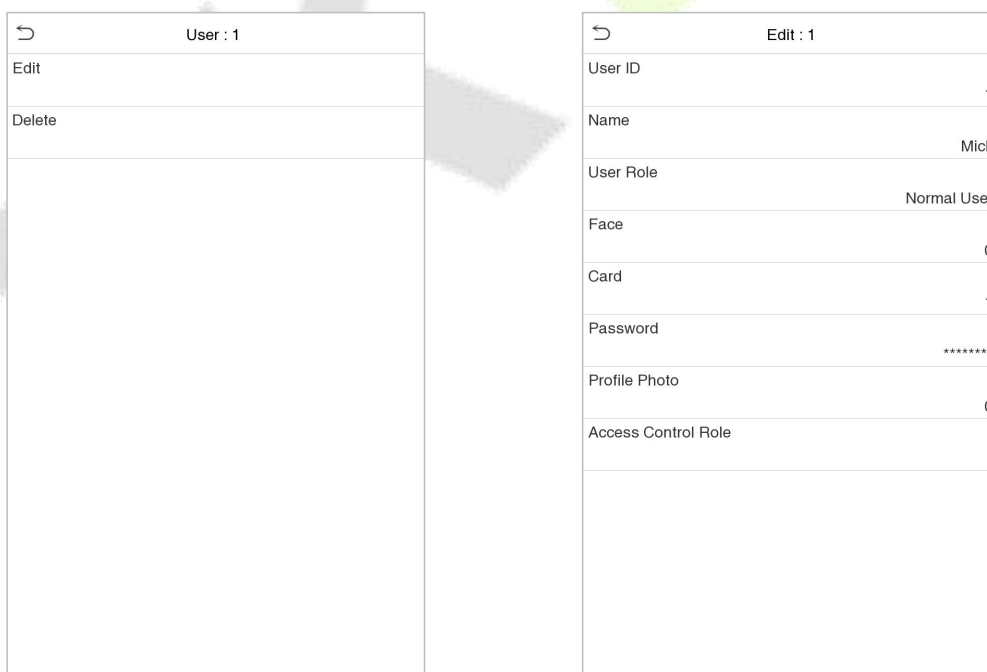


- On the **All-Users** interface, tap on the search bar on the user's list to enter the required retrieval keyword (where the keyword may be the user ID, surname or full name) and the system will search for the related user information.



### 3.3 Edit User

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



**Note:** The process of editing a user is the same as that of adding a user, except that the user ID cannot be modified when editing a user's details. The process in detail refers to ["3. User Management"](#).

## 3.4 Delete User

On **All Users** interface, tap on the required user from the list and tap **Delete** to delete the user or a 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:** All information of the user will be deleted (deletes the selected User as a whole) from the Device.

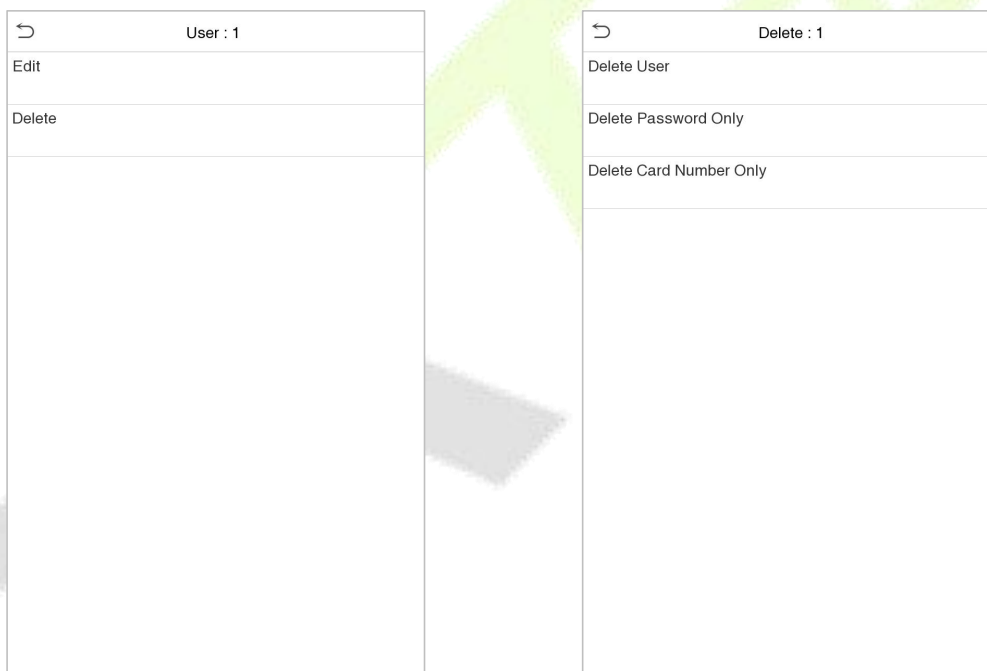
**Delete Fingerprint Only:** Deletes the fingerprint information of the selected user.

**Delete Face Only:** Deletes the face template information of the selected user.

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

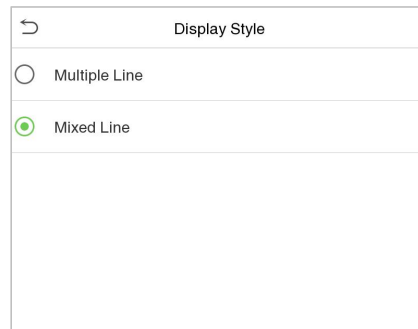
**Delete Card Number Only:** Deletes the card information of the selected user.

**Delete Profile Photo Only:** Deletes the profile photo of the selected user.



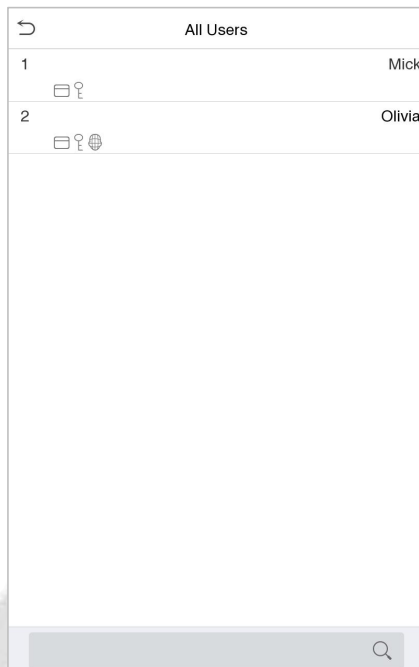
## 3.5 Display Style

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

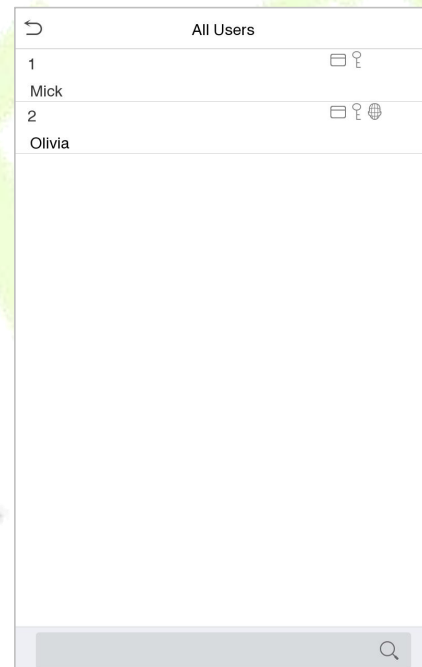


Different display styles are shown as below:

Multiple Line:



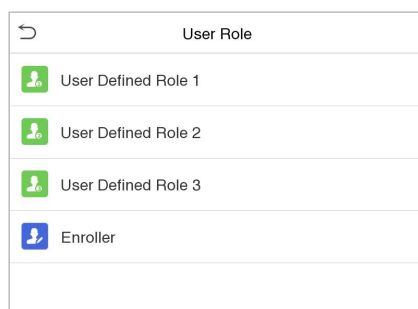
Mixed Line:



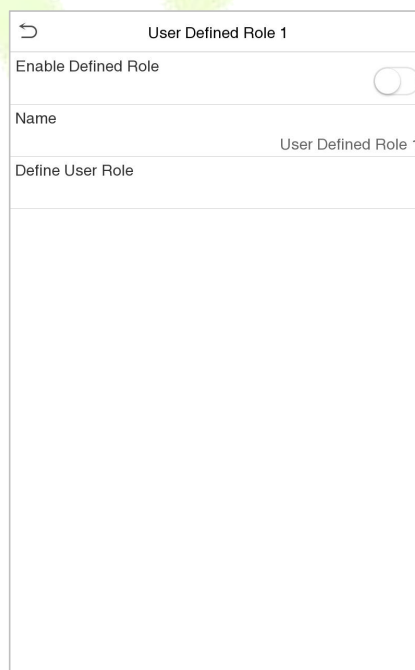
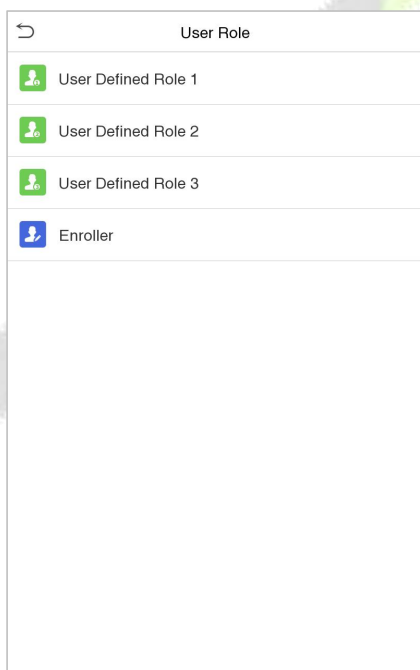
## 4. User Role

**User Role** facilitates to assign some specific permissions to specific users, based on the requirement.

- On the **Main** menu, tap **User Role**, and then tap on the **User Defined Role** to set the user-defined permissions.
- The permission scope of the custom role can be set up to 3 roles, that is, the custom operating scope of the menu functions of the user.



- On the **User Defined Role** interface, toggle **Enable Defined Role** to enable or disable the user defined role.
- Tap on **Name** and enter the custom name of the role.



- Then, tap on **User Defined 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** function name, and then select its required sub-menus from the list.

↶

User Defined Role 1

☒ User Mgt.

☒ COMM.

☒ System

☐ Personalize

☐ Data Mgt.

☒ Intercom

☒ Access Control

☐ Attendance Search

☐ Autotest

☐ System Info

↶

User Mgt.

☒ New User

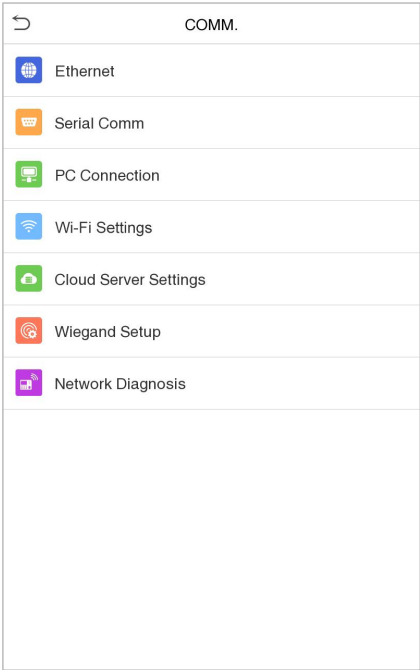
☒ All Users

☒ Display Style

**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.

## 5. Communication Settings

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



### 5.1 Network Settings

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

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



## Function Description

Function Name	Descriptions
<b>Display in Status Bar</b>	Toggle to set whether to display the network icon on the status bar.
<b>IP Protocol Version</b>	The default IP protocol version is IPv4.
<b>IP Address</b>	The default IP address is 192.168.1.201. It can be modified according to the network availability.
<b>Subnet Mask</b>	The default Subnet Mask is 255.255.255.0. It can be modified according to the network availability.
<b>Gateway</b>	The default Gateway address is 0.0.0.0. It can be modified according to the network availability.
<b>DNS</b>	The default DNS address is 0.0.0.0. It can be modified according to the network availability.
<b>DHCP</b>	Dynamic Host Configuration Protocol is to dynamically allocate IP address for clients via server.

## 5.2 Serial Comm

Serial Comm function facilitates to establish communication with the device through a serial port (RS485/Master Unit).

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

## Function Description

Function Name	Descriptions
<b>Serial Port</b>	<p><b>No Using:</b> Do not communicate with the device through the serial port.</p> <p><b>RS485(PC):</b> Communicates with the device through RS485 serial port.</p> <p><b>Master Unit:</b> When RS485 is used as the function of “<b>Master unit</b>”, the device will act as a master unit, and it can be connected to RS485 card reader.</p> <p><b>DM10:</b> Communicates with the DM10 through RS485 serial port.</p>

**Baud Rate**

The rate at which the data is communicated with PC, there are 4 options of baud rate: 115200 (default), 57600, 38400, and 19200.

The higher is the baud rate, the faster is the communication speed, but also the less reliable.

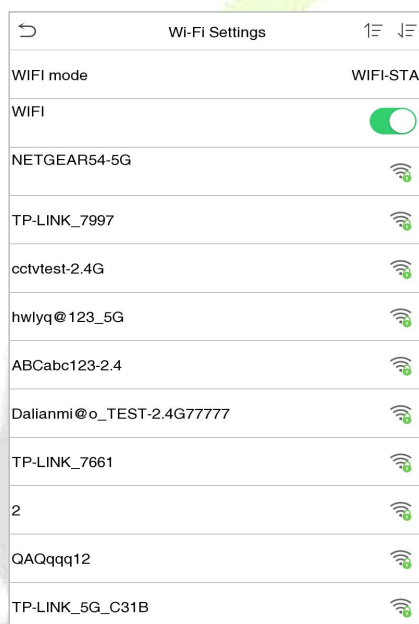
Hence, a higher baud rate can be used when the communication distance is short; when the communication distance is long, choosing a lower baud rate would be more reliable.

## 5.3 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.

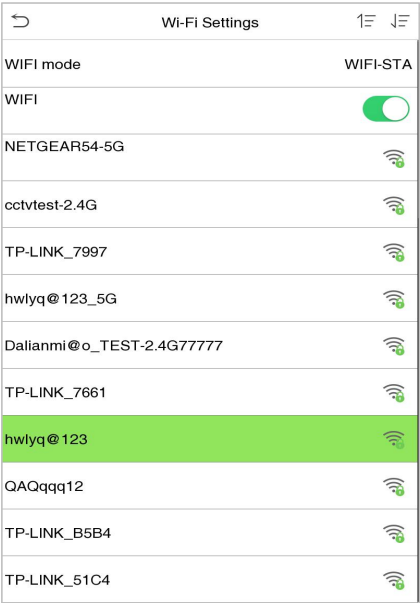
Tap **Wi-Fi Settings** on the **Comm.** Settings interface to configure the Wi-Fi settings.



### ● Search the Wi-Fi Network


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





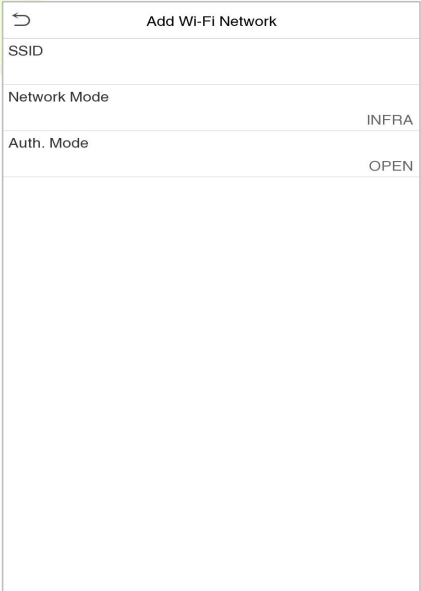
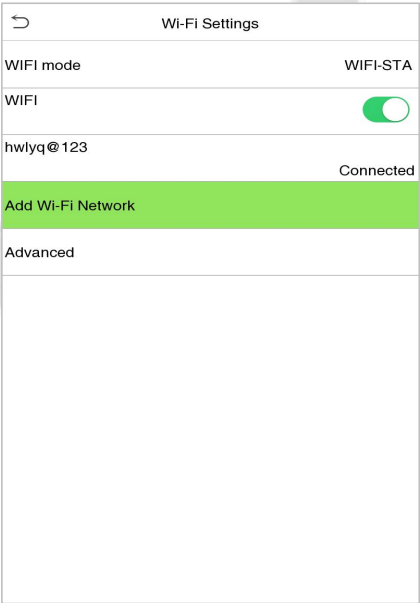
**WIFI Enabled:** Tap on the required network from the searched network list.

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 does not show on the list.



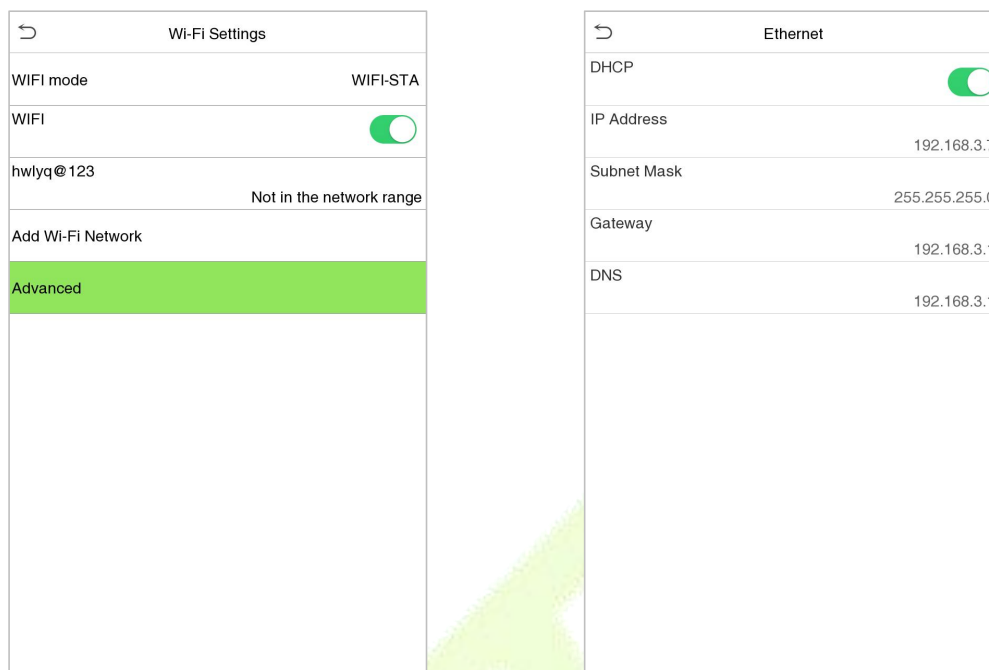
Tap on **Add Wi-Fi Network** to add the Wi-Fi manually.

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

**Note:** After successfully adding the WIFI manually, follow the same process to search for the added WIFI name. [Click here to view the process to search the WIFI network.](#)

## ● Advanced Setting

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



### Function Description

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

## 5.4 PC Connection

To improve the security of data, please set a Comm Key for communication between the device and the PC. The connection password needs to be entered before the device can be connected to the PC software if a Comm Key is set.

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	<input checked="" type="checkbox"/>

### Function Description

Function Name	Descriptions
<b>Comm Key</b>	The default password is 0 and can be changed. The Comm Key must be 6 digits.
<b>Device ID</b>	Identity number of the device, which ranges between 1 and 254. If the communication method is RS232/RS485, you need to input this device ID in the software communication interface.
<b>TCP COMM. Port</b>	The default TCP COMM Port value is 4370. It can be modified according to the network availability.
<b>HTTPS</b>	To increase the security of software access, users can enable the HTTPS protocol to create a secure and encrypted network transmission and assure the security of sent data through identity authentication and encrypted communication.  This function is enabled by default. This function can be enabled or disabled through the menu interface, and when changing the HTTPS status, the device will pop up a security prompt, and restart after confirmation.

## 5.5 Cloud Server Setting

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

Cloud Server Settings	
Server Mode	ADMS
IP Protocol Version	IPv4
Enable Domain Name	<input type="checkbox"/>
Server Address	0.0.0.0
Server Port	8081
Enable Proxy Server	<input type="checkbox"/>

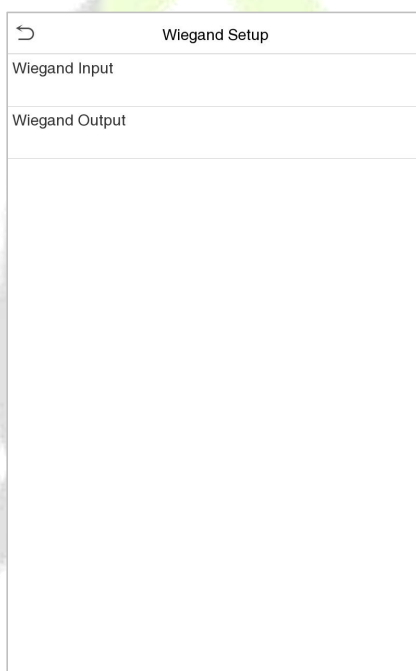
## Function Description

Function Name		Description
IP Protocol Version		Displays the IP protocol version, which defaults to IPv4.
Enable Domain Name	<b>Server Address</b>	Once this function is enabled, the domain name mode "http://..." will be used, such as http://www.XYZ.com, while "XYZ" denotes the domain name (when this mode is turned ON).
Disable Domain Name	<b>Server Address</b>	IP address of the ADMS server.
	<b>Server Port</b>	Port used by the ADMS server.
Enable Proxy Server		When you choose to enable the proxy, you need to set the IP address and port number of the proxy server.

## 5.6 Wiegand Setup

To set the Wiegand input or output parameters.

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



**Note:** The Wiegand interface is shared, and the user can choose to use either the Wiegand input or Wiegand output function to interface with different Wiegand devices.

### 5.6.1 Wiegand Input

Tap **Wiegand Input** on the **Wiegand Setup** interface.

Wiegand Setup

Wiegand Input

Wiegand Output

Wiegand Options

Wiegand Format

Wiegand Bits 26

Pulse Width(us) 100

Pulse Interval(us) 1000

ID Type User ID

### Function Description

Function Name	Descriptions
<b>Wiegand Format</b>	Values range from 26 Bits, 32 Bits, 34 Bits, 36 Bits, 37 Bits, 50 Bits and 64Bits.
<b>Wiegand Bits</b>	Number of bits of Wiegand data.
<b>Pulse Width(us)</b>	The value of the pulse width sent by Wiegand is 100 microseconds by default, which can be adjusted within the range of 20 to 400 microseconds.
<b>Pulse Interval(us)</b>	The default value is 1000 microseconds, which can be adjusted within the range of 200 to 20000 microseconds.
<b>ID Type</b>	Select between User ID and card number.

### Various Common Wiegand Format Description

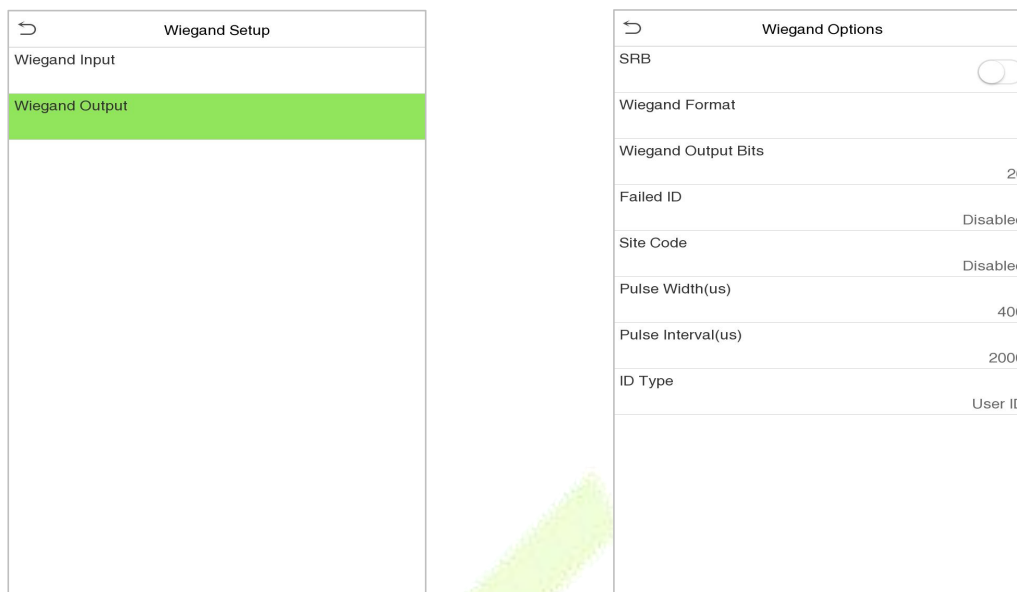
Wiegand Format	Description
<b>Wiegand26</b>	<p>EEEEEEEEEEEEEEEEEEEEEEEEEEEE</p> <p>Consists of 26 bits of binary code. The 1<sup>st</sup> bit is the even parity bit of the 2<sup>nd</sup> to 13<sup>th</sup> bits, while the 26<sup>th</sup> bit is the odd parity bit of the 14<sup>th</sup> to 25<sup>th</sup> bits. The 2<sup>nd</sup> to 25<sup>th</sup> bits is the card numbers.</p>
<b>Wiegand26a</b>	<p>ESSSSSSSSSSSSSSSSSSSSSSSSSS</p> <p>Consists of 26 bits of binary code. The 1<sup>st</sup> bit is the even parity bit of the 2<sup>nd</sup> to 13<sup>th</sup> bits, while the 26<sup>th</sup> bit is the odd parity bit of the 14<sup>th</sup> to 25<sup>th</sup> bits. The 2<sup>nd</sup> to 9<sup>th</sup> bits is the site codes, while the 10<sup>th</sup> to 25<sup>th</sup> bits are the card numbers.</p>
<b>Wiegand34</b>	<p>EEEEEEEEEEEEEEEEEEEEEEEEEEEE</p> <p>Consists of 34 bits of binary code. The 1<sup>st</sup> bit is the even parity bit of the 2<sup>nd</sup> to 17<sup>th</sup> bits, while the 34<sup>th</sup> bit is the odd parity bit of the 18<sup>th</sup> to 33<sup>rd</sup> bits. The 2<sup>nd</sup> to 25<sup>th</sup> bits is the card numbers.</p>

<b>Wiegand34a</b>	ESSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCO Consists of 34 bits of binary code. The 1 <sup>st</sup> bit is the even parity bit of the 2 <sup>nd</sup> to 17 <sup>th</sup> bits, while the 34 <sup>th</sup> bit is the odd parity bit of the 18 <sup>th</sup> to 33 <sup>rd</sup> bits. The 2 <sup>nd</sup> to 9 <sup>th</sup> bits is the site codes, while the 10 <sup>th</sup> to 25 <sup>th</sup> bits are the card numbers.
<b>Wiegand36</b>	OFFFFFFFFFCCCCCCCCCCCCCMMME Consists of 36 bits of binary code. The 1 <sup>st</sup> bit is the odd parity bit of the 2 <sup>nd</sup> to 18 <sup>th</sup> bits, while the 36 <sup>th</sup> bit is the even parity bit of the 19 <sup>th</sup> to 35 <sup>th</sup> bits. The 2 <sup>nd</sup> to 17 <sup>th</sup> bits is the device codes. The 18 <sup>th</sup> to 33 <sup>rd</sup> bits is the card numbers, and the 34 <sup>th</sup> to 35 <sup>th</sup> bits are the manufacturer codes.
<b>Wiegand36a</b>	EFFFFFFFFFFFFFCCCCCCCCCCCCCCO Consists of 36 bits of binary code. The 1 <sup>st</sup> bit is the even parity bit of the 2 <sup>nd</sup> to 18 <sup>th</sup> bits, while the 36 <sup>th</sup> bit is the odd parity bit of the 19 <sup>th</sup> to 35 <sup>th</sup> bits. The 2 <sup>nd</sup> to 19 <sup>th</sup> bits is the device codes, and the 20 <sup>th</sup> to 35 <sup>th</sup> bits are the card numbers.
<b>Wiegand37</b>	OMMMMSSSSSSSSSSSCCCCCCCCCCCCCCCCCE Consists of 37 bits of binary code. The 1 <sup>st</sup> bit is the odd parity bit of the 2 <sup>nd</sup> to 18 <sup>th</sup> bits, while the 37 <sup>th</sup> bit is the even parity bit of the 19 <sup>th</sup> to 36 <sup>th</sup> bits. The 2 <sup>nd</sup> to 4 <sup>th</sup> bits is the manufacturer codes. The 5 <sup>th</sup> to 16 <sup>th</sup> bits is the site codes, and the 21 <sup>st</sup> to 36 <sup>th</sup> bits are the card numbers.
<b>Wiegand37a</b>	EMMMFFFFFFFFFSSSSSSCCCCCCCCCCCCCCCO Consists of 37 bits of binary code. The 1 <sup>st</sup> bit is the even parity bit of the 2 <sup>nd</sup> to 18 <sup>th</sup> bits, while the 37 <sup>th</sup> bit is the odd parity bit of the 19 <sup>th</sup> to 36 <sup>th</sup> bits. The 2 <sup>nd</sup> to 4 <sup>th</sup> bits is the manufacturer codes. The 5 <sup>th</sup> to 14 <sup>th</sup> bits is the device codes, and 15 <sup>th</sup> to 20 <sup>th</sup> bits are the site codes, and the 21 <sup>st</sup> to 36 <sup>th</sup> bits are the card numbers.
<b>Wiegand50</b>	ESSSSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCCCO Consists of 50 bits of binary code. The 1 <sup>st</sup> bit is the even parity bit of the 2 <sup>nd</sup> to 25 <sup>th</sup> bits, while the 50 <sup>th</sup> bit is the odd parity bit of the 26 <sup>th</sup> to 49 <sup>th</sup> bits. The 2 <sup>nd</sup> to 17 <sup>th</sup> bits is the site codes, and the 18 <sup>th</sup> to 49 <sup>th</sup> bits are the card numbers.
<b>Wiegand64</b>	ECC CCCCO It consists of 64 bits of binary code. The 1 <sup>st</sup> bit is the even parity bit of the 2 <sup>nd</sup> to 32 <sup>nd</sup> bits, while the 64 <sup>th</sup> bit is the odd parity bit of the 33 <sup>rd</sup> to 63 <sup>rd</sup> bits. The 2 <sup>nd</sup> to 63 <sup>rd</sup> 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.

## 5.6.2 Wiegand Output

Tap **Wiegand Output** on the **Wiegand Setup** interface.



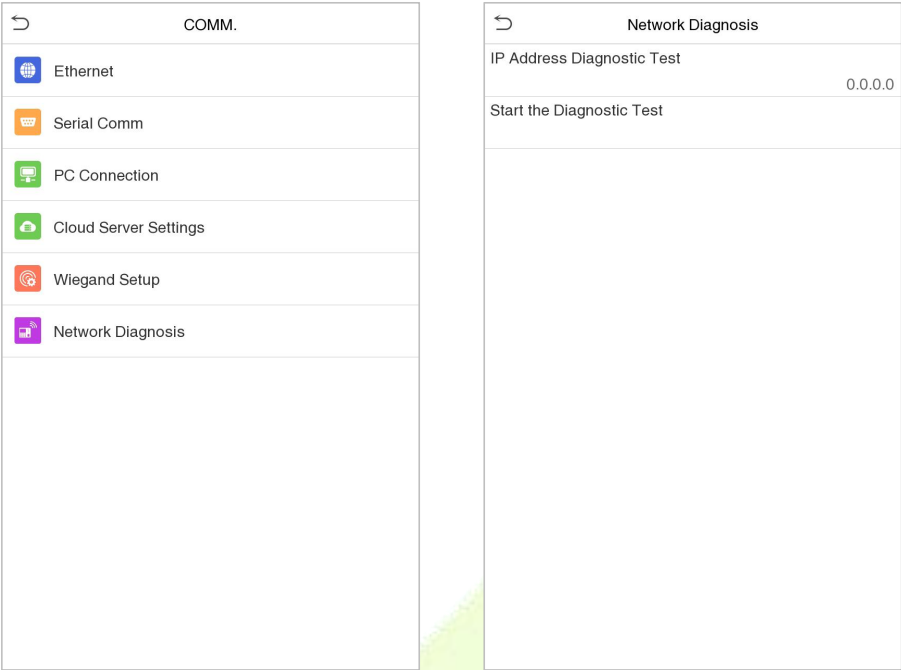
### Function Description

Function Name	Descriptions
<b>SRB★</b>	When SRB is enabled, the lock is controlled by the SRB to prevent the lock from being opened due to device removal.
<b>Wiegand Format</b>	Values range from 26 Bits, 32 Bits, 34 Bits, 36 Bits, 37 Bits, 50 Bits and 64Bits.
<b>Wiegand Output Bits</b>	After selecting the required Wiegand format, select the corresponding output bit digits of the Wiegand format.
<b>Failed ID</b>	If the verification is failed, the system will send the failed ID to the device and replace the card number or personnel ID with the new one.
<b>Site Code</b>	It is similar to the device ID. The difference is that a site code can be set manually, and is repeatable in a different device. The valid value ranges from 0 to 256 by default.
<b>Pulse Width(us)</b>	The time width represents the changes of the quantity of electric charge with regular high-frequency capacitance within a specified time.
<b>Pulse Interval(us)</b>	The time interval between pulses.
<b>ID Type</b>	Select the ID types as either User ID or card number.

## 5.7 Network Diagnosis

To set the network diagnosis parameters.

Tap **Network Diagnosis** on the **Comm.** Settings interface to set the IP address diagnostic and start the diagnostic parameters.

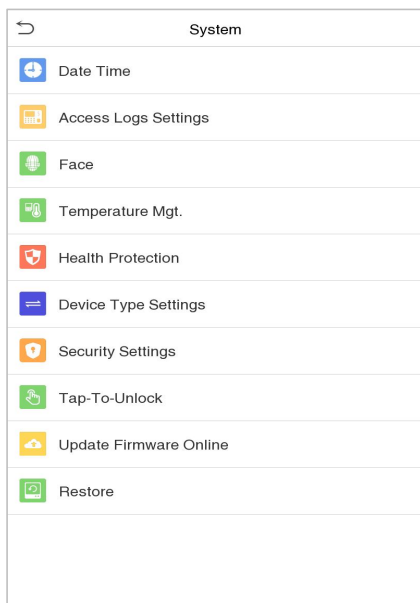




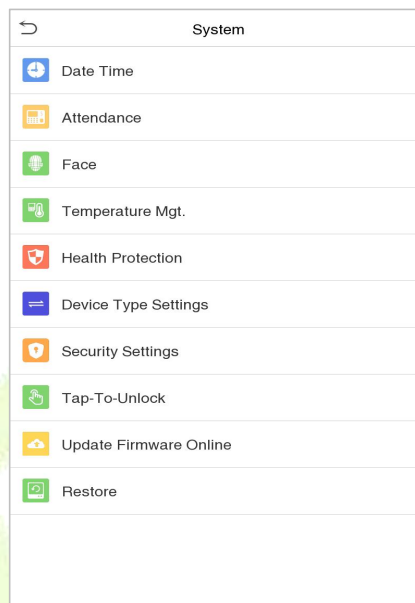
## 6. System Settings

Set related system parameters to optimize the performance of the device.

Tap **System** on the **Main Menu** interface to set the related system parameters to optimize the performance of the device.



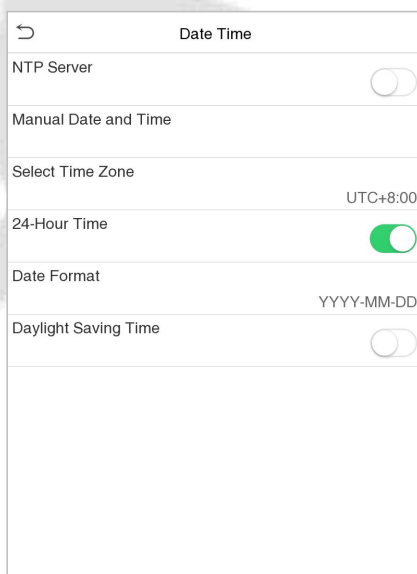
A&C Terminal



T&A Terminal

### 6.1 Date and Time

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

Date Time	
NTP Server	<input type="checkbox"/>
Manual Date and Time	
Select Time Zone	UTC+8:00
24-Hour Time	<input checked="" type="checkbox"/>
Date Format	YYYY-MM-DD
Daylight Saving Time	<input checked="" type="checkbox"/>
Daylight Saving Mode	By Date/Time
Daylight Saving Setup	

- Tap **24-Hour Time** to enable or disable this format. If enabled, then select the **Date Format** to set the date format.
- 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 Setup	
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 Setup	
Start Date	01-01
Start Time	00:00
End Date	01-02
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, 2019) to 18:30 on January 1, 2020. After restoring the factory settings, the time of the equipment will remain 18:30 on January 1, 2020.

## 6.2 Access Logs Settings/Attendance

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

Access Logs Settings	
Camera Mode	No photo
Display User Photo	<input type="checkbox"/>
Alphanumeric User ID	<input type="checkbox"/>
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	<input type="checkbox"/>
Alphanumeric User ID	<input type="checkbox"/>
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
Recognition Interval(s)	1

T&A Terminal

### Function Description of A&C Terminal:

Function Name	Description
<b>Camera Mode</b>	<p>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:</p> <p><b>No Photo:</b> No photo is taken during user verification.</p> <p><b>Take photo, no save:</b> Photo is taken but is not saved during verification.</p> <p><b>Take photo and save:</b> Photo is taken and saved during verification.</p> <p><b>Save on successful verification:</b> Photo is taken and saved for each successful verification.</p> <p><b>Save on failed verification:</b> Photo will be taken and saved only for each failed verification.</p>
<b>Display User Photo</b>	This function is disabled by default. When enabled, there will be a security prompt.
<b>Alphanumeric User ID</b>	Decides whether to support letters in a User ID.
<b>Access Logs Alert</b>	<p>When the record space of the attendance access reaches the maximum threshold value, the device will automatically display the memory space warning.</p> <p>Users may disable the function or set a valid value between 1 and 9999.</p>

<b>Periodic Del of Access Logs</b>	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.
<b>Periodic Del of T&amp;A Photo</b>	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.
<b>Periodic Del of Blocklist Photo</b>	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.
<b>Authentication Timeout(s)</b>	The time length of the message of successful verification displays. Valid value: 1~9 seconds.
<b>Recognition Interval (s)</b>	To set the facial template matching time interval as required. Valid value: 0~9 seconds.

### Function Description of T&A Terminal:

Function Name	Description
<b>Duplicate Punch Period(m)</b>	Within a set time period (unit: minutes), the duplicated attendance record will not be reserved (value ranges from 1 to 999999 minutes).
<b>Camera Mode</b>	<p>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:</p> <p><b>No photo:</b> No photo is taken during user verification.</p> <p><b>Take photo, no save:</b> Photo is taken but not saved during verification.</p> <p><b>Take photo and save:</b> All the photos taken during verification is saved.</p> <p><b>Save on successful verification:</b> Photo is taken and saved for each successful verification.</p> <p><b>Save on failed verification:</b> Photo is taken and saved only for each failed verification.</p>
<b>Display User Photo</b>	Whether to display the user photo when the user passes the verification.
<b>Alphanumeric User ID</b>	Enable/Disable the alphanumeric as User ID.
<b>Attendance Log Alert</b>	<p>When the record space of the attendance reaches the maximum threshold value, the device automatically displays the memory space warning.</p> <p>Users may disable the function or set a valid value between 1 and 9999.</p>
<b>Periodic Del of T&amp;A Data</b>	<p>When attendance records reach its maximum storage capacity, the device automatically deletes a set of old attendance records.</p> <p>Users may disable the function or set a valid value between 1 and 999.</p>

<b>Periodic Del of T&amp;A Photo</b>	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.
<b>Periodic Del of Blocklist Photo</b>	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.
<b>Authentication Timeout(s)</b>	The amount of time taken to display a successful verification message. Valid value: 1 to 9 seconds.
<b>Recognition Interval(s)</b>	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.

## 6.3 Face Template Parameters

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

<div> <div>↶</div> <div>Face</div> <div>1↓</div> </div> <div> <div>1:N Threshold</div> <div>84</div> </div> <div> <div>1:1 Threshold</div> <div>80</div> </div> <div> <div>Face Enrollment Threshold</div> <div>80</div> </div> <div> <div>Image Quality</div> <div>40</div> </div> <div> <div>Facial Recognition Distance</div> <div>Far</div> </div> <div> <div>Live Detection</div> <div><input checked="" type="checkbox"/></div> </div> <div> <div>Live Detection Threshold</div> <div>85</div> </div> <div> <div>Anti-spoofing Using NIR</div> <div><input checked="" type="checkbox"/></div> </div> <div> <div>Binocular Live Detection Threshold</div> <div>99</div> </div> <div> <div>Face AE</div> <div><input type="checkbox"/></div> </div> <div> <div>WDR</div> <div><input type="checkbox"/></div> </div> <div> <div>Anti-flicker Mode</div> <div>50Hz</div> </div>	<div> <div>↶</div> <div>Face</div> <div>1↓</div> </div> <div> <div>1:1 Threshold</div> <div>80</div> </div> <div> <div>Face Enrollment Threshold</div> <div>80</div> </div> <div> <div>Image Quality</div> <div>40</div> </div> <div> <div>Facial Recognition Distance</div> <div>Far</div> </div> <div> <div>Live Detection</div> <div><input checked="" type="checkbox"/></div> </div> <div> <div>Live Detection Threshold</div> <div>85</div> </div> <div> <div>Anti-spoofing Using NIR</div> <div><input checked="" type="checkbox"/></div> </div> <div> <div>Binocular Live Detection Threshold</div> <div>99</div> </div> <div> <div>Face AE</div> <div><input type="checkbox"/></div> </div> <div> <div>WDR</div> <div><input type="checkbox"/></div> </div> <div> <div>Anti-flicker Mode</div> <div>50Hz</div> </div> <div> <div>Face Algorithm</div> <div></div> </div>
---	--

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

## Function Description

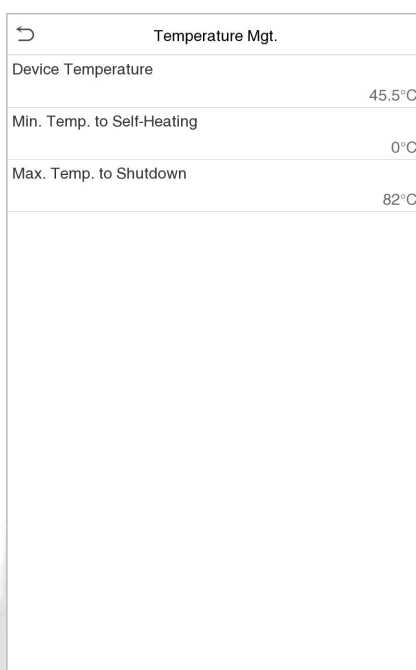
Function Name	Description
<b>1:N Threshold</b>	Under 1:N verification mode, the verification will only be successful when the similarity between the acquired facial image and all registered facial templates is greater than the set value. The valid value ranges from 0 to 100. The higher the thresholds, the lower the misjudgement rate, the higher the rejection rate, and vice versa. It is recommended to set the default value of 75.
<b>1:1 Threshold</b>	Under 1:1 verification mode, the verification will only be successful when the similarity between the acquired facial image and the user's facial templates enrolled in the device is greater than the set value. The valid value ranges from 0 to 100. The higher the thresholds, the lower the misjudgement rate, the higher the rejection rate, and vice versa. It is recommended to set the default value of 63.
<b>Face Enrollment Threshold</b>	During face template 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 this threshold, it indicates that the face template has already been registered.
<b>Image Quality</b>	Image quality for facial registration and comparison. The higher the value, the clearer the image requires.
<b>Facial Recognition Distance</b>	Face template recognition of the maximum distance, greater than this value will be filtered. The parameter value can be understood as the face template size required for registration and comparison. The farther the distance from people, the smaller the face template pixels obtained by the algorithm. When the value is 0, it means that the face template comparison distance is not limited.
<b>Live Detection</b>	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.
<b>Live Detection Threshold</b>	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.
<b>Anti-spoofing Using NIR</b>	Using near-infrared spectra imaging to identify and prevent fake photos and videos attack
<b>Binocular Live Detection Threshold</b>	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.
<b>Face AE</b>	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.
<b>WDR</b>	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.
<b>Anti-flicker Mode</b>	Used when WDR is turned off. This helps reduce flicker when the device's screen flashes at the same frequency as the light.

<b>Face Algorithm</b>	Facial algorithm related information and pause facial template update.
<b>Notes</b>	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.

## 6.4 Temperature Management

The device has a built-in temperature sensor, and when the environment temperature is too low or too high, it will trigger self-heating or shut down.

Tap **Temperature Mgt.** on the System interface.



Temperature Mgt.	
Device Temperature	45.5°C
Min. Temp. to Self-Heating	0°C
Max. Temp. to Shutdown	82°C

### Function Description

Function Name	Descriptions
<b>Device Temperature</b>	This column shows the real- time temperature of the device.
<b>Min. Temp. to Self-Heating</b>	Once the device temperature is lower than the set value, the device will start self-heating, the range is 0 to 10(°C).
<b>Max. Temp. to Shutdown</b>	When the device temperature is lower than the set value, it will shut down automatically to protect the hardware, the range is 70 to 90 (°C).

## 6.5 Health Protection

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



Health Protection	
Enable Mask Detection	<input checked="" type="checkbox"/>
Mask Detection Threshold	75
Deny Access Without Mask	<input type="checkbox"/>
Allow Unregistered People to Access	<input checked="" type="checkbox"/>
Enable Capture of Unregistered Person	<input type="checkbox"/>
Trigger External Alarm	<input type="checkbox"/>
Clear External Alarm	
External Alarm Delay(s)	10

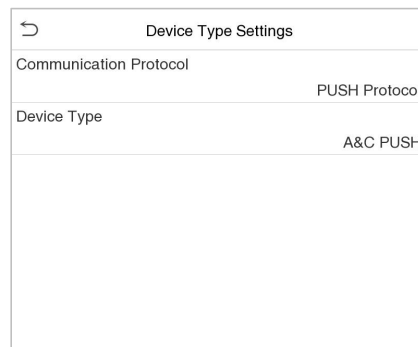
### Function Description

Function Name	Descriptions
<b>Enable Mask Detection</b>	It enables or disables the mask detection function. When enabled, the device identifies whether the user is wearing a mask or not during verification.
<b>Mask Detection Threshold</b>	Set the mask detection threshold. Valid values are 0 to 100.
<b>Deny Access Without Mask</b>	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.
<b>Allow Unregistered People to Access</b>	It enables or disables the access of an unregistered person. When enabled, the device allows the person to enter without registration.
<b>Enable Capture of Unregistered Person</b>	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 <b>Allow Unregistered People to Access</b> .
<b>Trigger External Alarm</b>	When enabled, if the user is not wearing a mask, the system will trigger an alarm.
<b>Clear External Alarm</b>	It clears the triggered alarm records of the device.
<b>External Alarm Delay(s)</b>	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.

## 6.6 Device Type Setting

Tap **Device Type Setting** on the System interface.



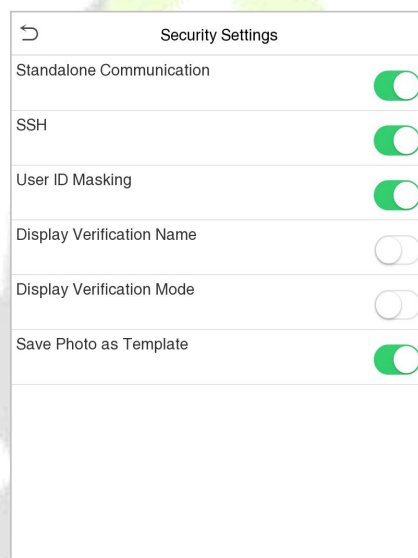


### Function Description

Function Name	Description
<b>Communication Protocol</b>	Set the device communication protocol.
<b>Device Type</b>	Set the device as time attendance terminal (T&A PUSH) or access control terminal (A&C PUSH).

## 6.7 Security Setting

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



### Function Description

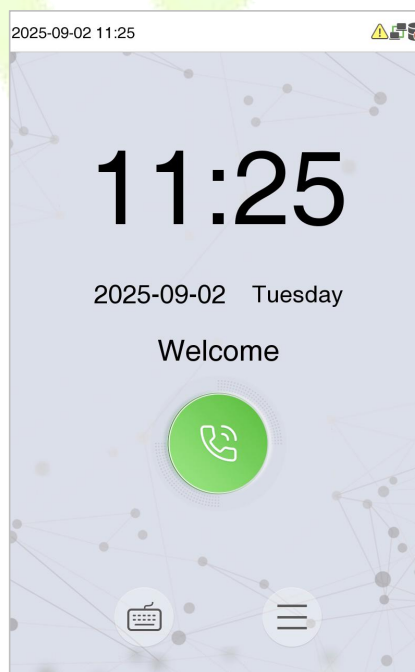
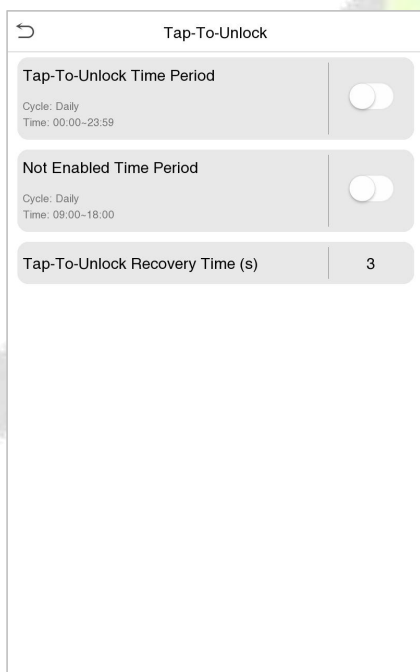
Function Name	Description
<b>Standalone Communication</b>	By default, this function is disabled. This function can be enabled or disabled via the menu interface. When it is switched on, a security prompt appears, and the device will restart after you confirm.
<b>SSH</b>	The device does not support the 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.

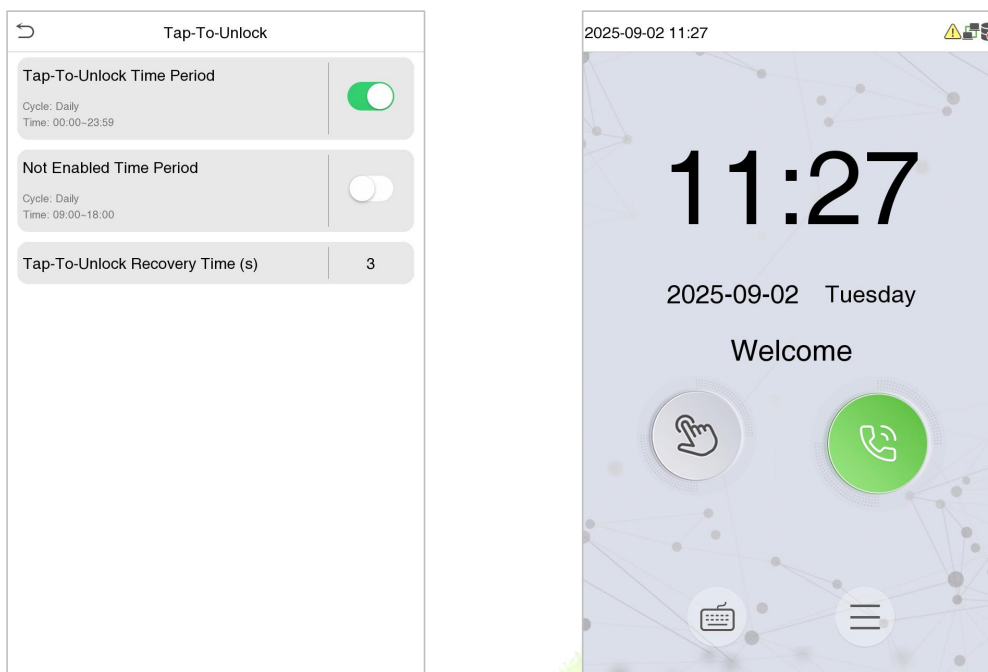
<b>User ID Masking</b>	After enabled, the User ID will be partially displayed after the personnel verification result (only the User ID with more than 2 digits supports the masking display), and it is enabled by default.
<b>Display Verification Name</b>	After enabled, the user's name will be displayed after the personnel verification result. The verification result will not show the name after disabling it.
<b>Display Verification Mode</b>	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.
<b>Save Photo as Template</b>	After disabling this function, face template re-registration is required after an algorithm upgrade.

## 6.8 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.

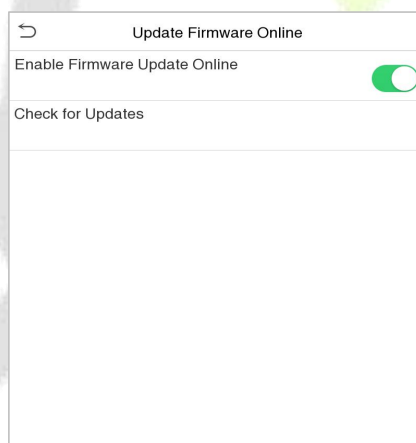




## 6.9 Update Firmware Online

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

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



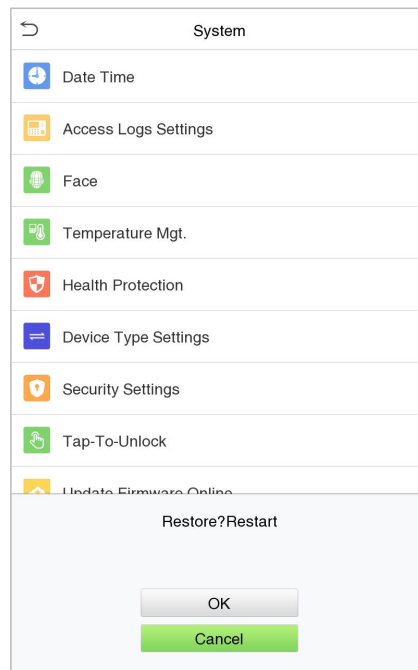
Click **Check for Updates** it may have the following 3 scenarios:

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

## 6.10 Factory Reset

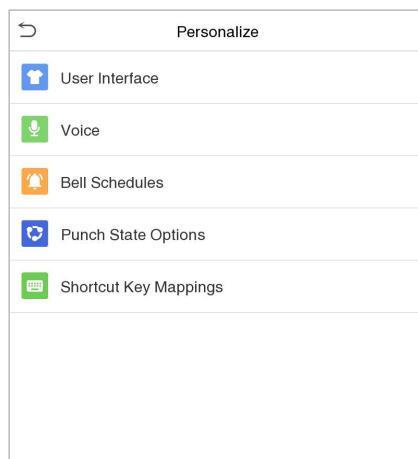
The Factory Reset function restores the device settings such as communication settings and system settings, to the default factory settings (This function does not clear registered user data).

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



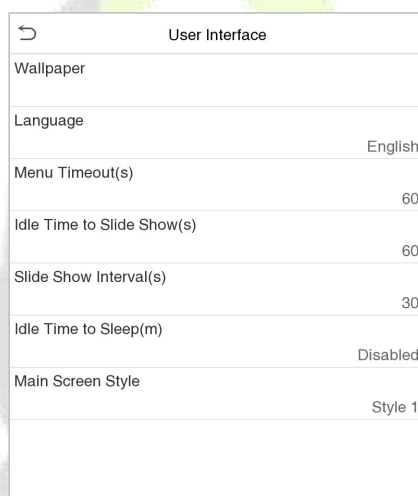
## 7. Personalize Settings

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



### 7.1 User Interface Settings

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



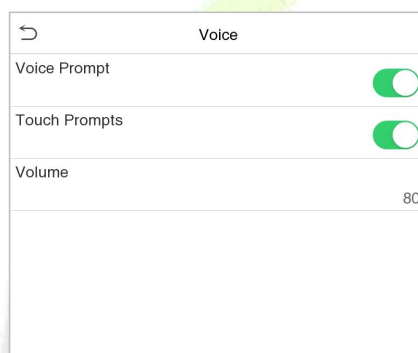
#### Function Description

Function Name	Description
<b>Wallpaper</b>	The main screen wallpaper can be selected according to the user preference.
<b>Language</b>	Select the language of the device.
<b>Menu Timeout (s)</b>	When there is no operation, and the time exceeds the set value, the device will automatically go back to the initial interface. The function either can be disabled or set the required value between 60 and 99999 seconds.

<b>Idle Time to Slide Show (s)</b>	When there is no operation, and the time exceeds the set value, a slide show will be played. The function can be disabled, or you may set the value between 3 and 999 seconds.
<b>Slide Show Interval (s)</b>	It is the time interval in switching between different slide show photos. The function can be disabled, or you may set the interval between 3 and 999 seconds.
<b>Idle Time to Sleep (m)</b>	If the sleep mode is activated, and when there is no operation in the device, then the device will enter standby mode. Tap the screen anywhere to resume normal working mode. This function can be disabled or set a value within 1-999 minutes.
<b>Main Screen Style</b>	The main screen style can be selected according to the user preference.

## 7.2 Voice Settings

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

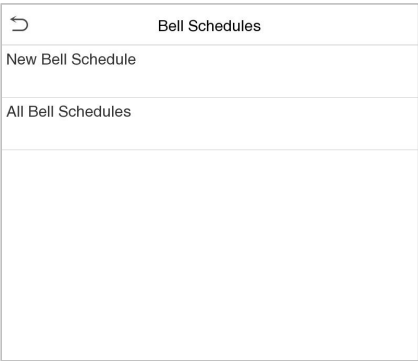


### Function Description

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

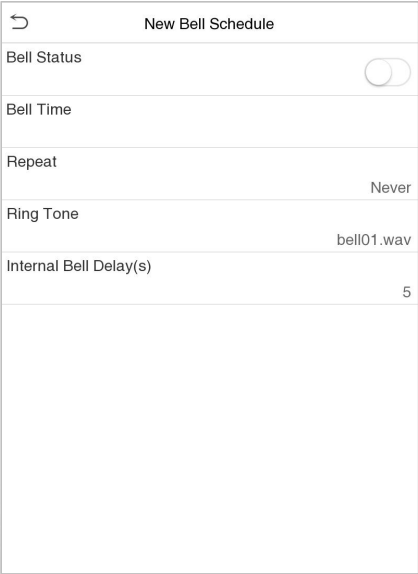
## 7.3 Bell Schedules

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



● **New bell schedule**

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



**Function Description**

Function Name	Description
<b>Bell Status</b>	Toggle to enable or disable the bell status.
<b>Bell Time</b>	Once the required time is set, the device will automatically trigger to ring the bell during that time.
<b>Repeat</b>	Set the required number of counts to repeat the scheduled bell.
<b>Ring Tone</b>	Select a ring tone.
<b>Internal Bell Delay(s)</b>	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:

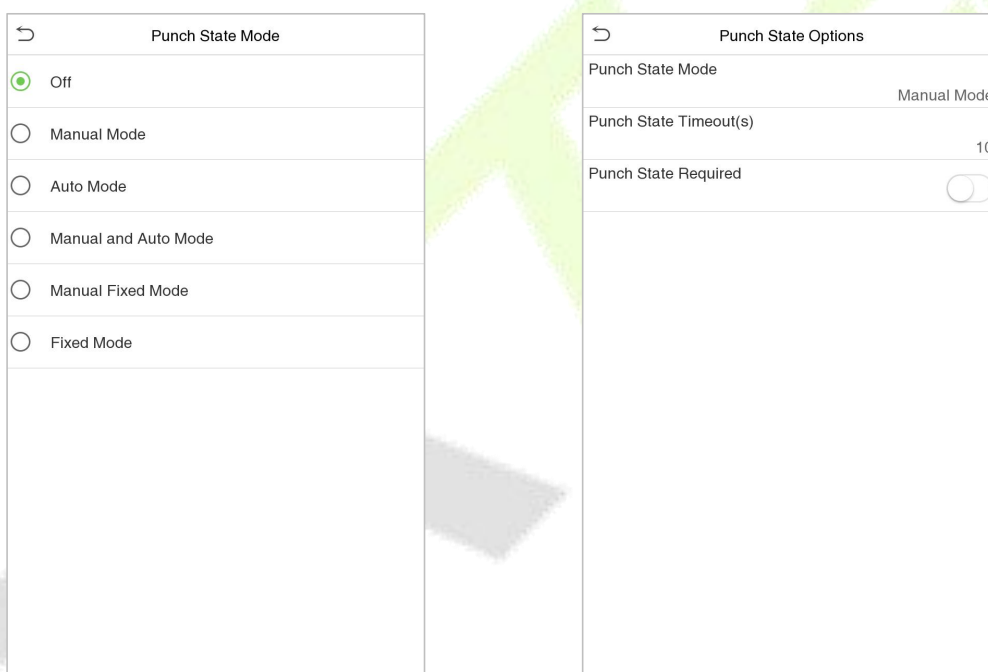
On the **All Bell Schedules** interface, tap on the required bell schedule, and tap **Edit** to edit the selected bell schedule. The editing method is the same as the operations of adding a new bell schedule.

### ● 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.

## 7.4 Punch States Options

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



### Function Description

Function Name	Description
<b>Punch State Mode</b>	<p>Select a punch state mode, which can be:</p> <p><b>Off:</b> It disables the punch state function. And the punch state key set under the <b>Shortcut Key Mappings</b> menu becomes invalid.</p> <p><b>Manual Mode:</b> Switch the punch state key manually, and the punch state key will disappear after <b>Punch State Timeout</b>.</p> <p><b>Auto Mode:</b> 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.</p> <p><b>Manual and Auto Mode:</b> 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</p>

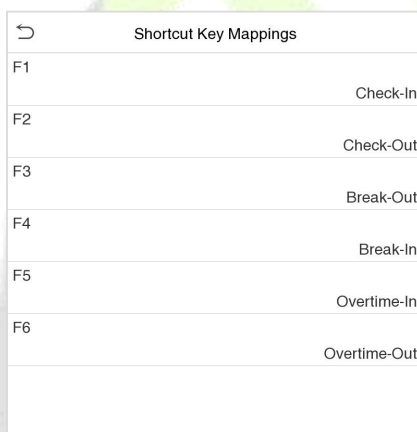


	<p>manual switching punch state key will become an auto-switch punch state key.</p> <p><b>Manual Fixed Mode:</b> After the punch state key is set manually to a particular punch status, the function will remain unchanged until manually switched again.</p> <p><b>Fixed Mode:</b> Only the manually fixed punch state key is shown. Users cannot change the status by pressing any other keys.</p>
<b>Punch State Timeout (s)</b>	It is the amount of time for which the punch state is displayed. The value ranges from 5~999 seconds.
<b>Punch State Required</b>	To choose whether an attendance state needs to be selected during verification.

## 7.5 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

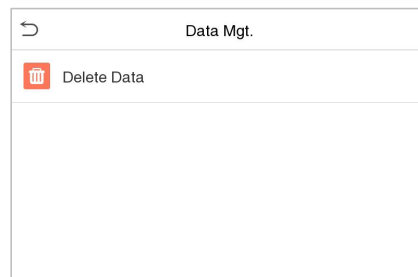
Function

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.

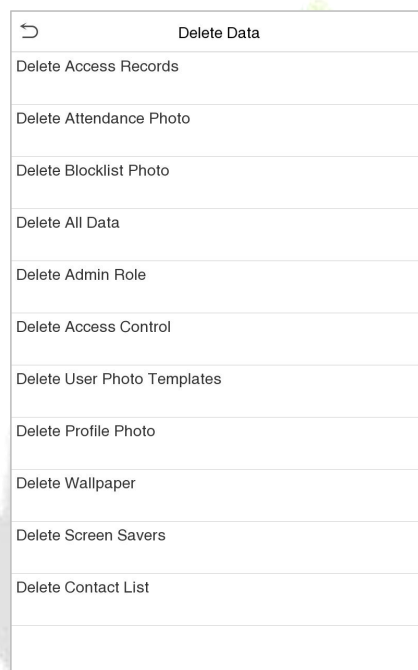
## 8. Data Management

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



### 8.1 Delete Data

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

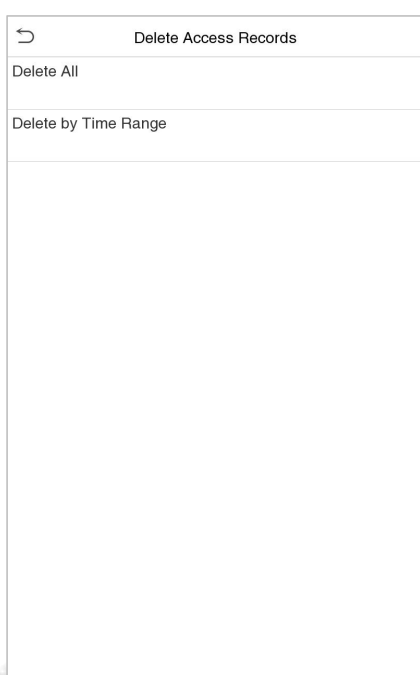


#### Function Description

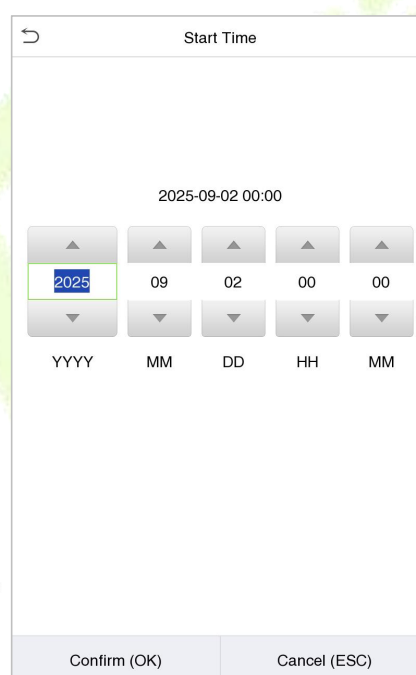
Function Name	Description
<b>Delete Access Records</b>	To delete access records conditionally.
<b>Delete Attendance Photo</b>	To delete attendance photos of designated personnel.
<b>Delete Blocklist Photo</b>	To delete the photos taken during failed verifications.
<b>Delete All Data</b>	To delete information and attendance logs/access records of all registered users.
<b>Delete Admin Role</b>	To remove all administrator privileges.
<b>Delete Access Control</b>	To delete all access data.

<b>Delete User Photo Templates</b>	To delete user photo templates in the device. When deleting template photos, there is a risk reminder: <b>"Face re-registration is required after an algorithm upgrade."</b>
<b>Delete Profile Photo</b>	To delete all user photos in the device.
<b>Delete Wallpaper</b>	To delete all wallpapers in the device.
<b>Delete Screen Savers</b>	To delete the screen savers in the device.
<b>Delete Contact List</b>	To delete all contact list of video intercom in the device.

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



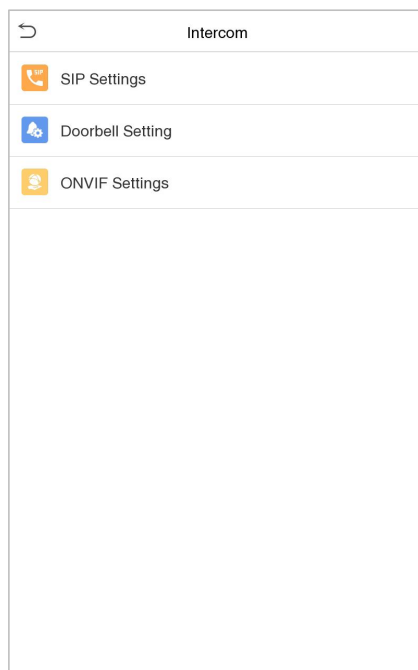
Select **Delete by Time Range**.



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

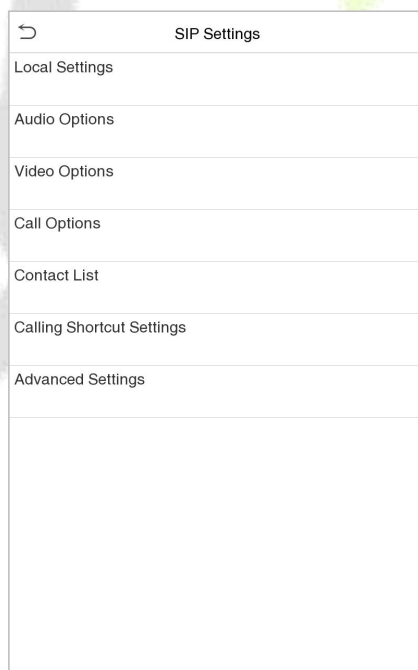
## 9. Intercom★

Click **Video intercom Parameters** on the **System** interface,



### 9.1 SIP Settings

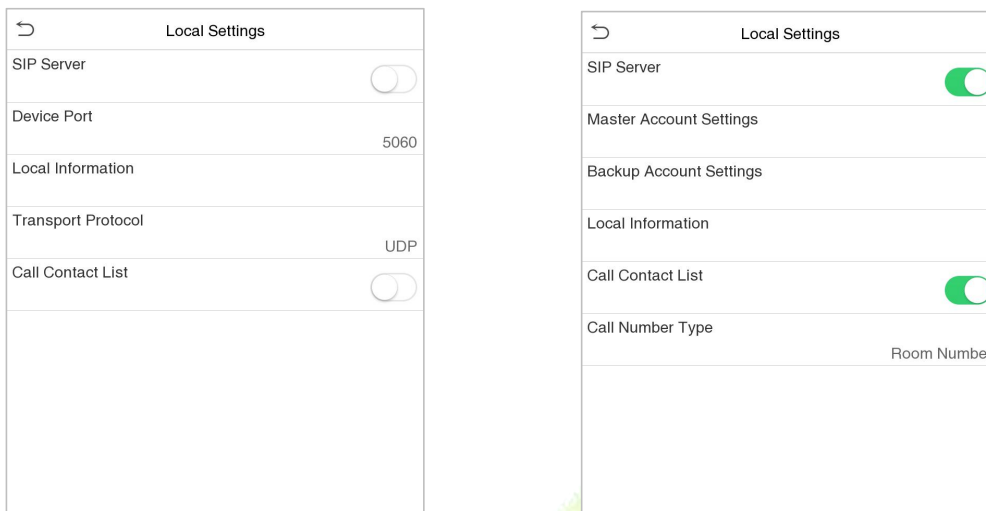
Tap **SIP Settings** on the **Video intercom Parameters** interface to navigate to the monitoring SIP settings.




**Note:** This function needs to be used with the indoor station.

### 9.1.1 Local Settings

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

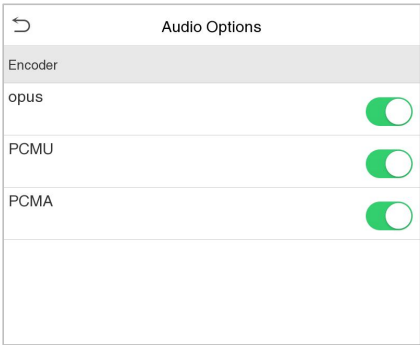


#### Function Description

Function Name	Description
<b>SIP Server</b>	Select whether to enable the SIP server. When it is enabled, the SIP account needs to be set. <b>Note:</b> Every time this feature is turned on or off, the contact list will be reset.
<b>Master Account Settings</b>	After assigning the SIP account to the device on the ZKBio CVSecurity, the account information will be automatically synchronized to the device. You don't need to configure it manually.
<b>Backup Account Settings</b>	Select whether to enable the backup account settings.
<b>Device Port</b>	When using a local area network for intercom, enter the device port number.
<b>Local Information</b>	<b>Device Type:</b> Set the device type as <b>Entrance Station</b> or <b>Fence Terminal</b> . 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. <b>Note:</b> The contact list will be cleared after changing the device type.
<b>Transport Protocol</b>	Set the transport protocol between the device and indoor monitor.
<b>Call Contact List</b>	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.
<b>Call Number Type</b>	<b>Room Number:</b> The device can call the extension number (short number) or room number. <b>SIP Account Number:</b> The device can only call the SIP account.

9.1.2 Audio Options

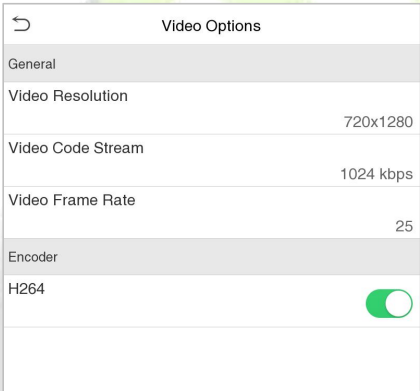
Tap **Audio Options** on the **SIP Settings** interface.



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

9.1.3 Video Options

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

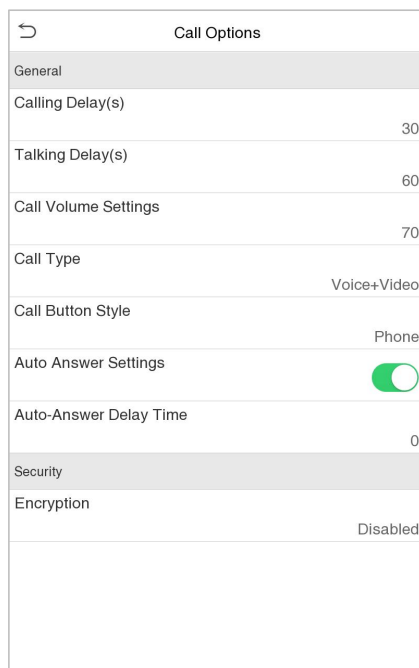


**Function Description**

Function Name	Description
<b>Video Resolution</b>	Select the video resolution of the intercom, 1024 x 576 (for landscape screen) or 720 x 1280 (for portrait screen). The device is suggested to set as 720 x 1280.
<b>Video Code Stream</b>	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.
<b>Video Frame Rate</b>	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.
<b>Encoder</b>	Whether to enable H264 Encoder.



## 9.1.4 Call Options

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



Call Options	
General	
Calling Delay(s)	30
Talking Delay(s)	60
Call Volume Settings	70
Call Type	Voice+Video
Call Button Style	Phone
Auto Answer Settings	<input checked="" type="checkbox"/>
Auto-Answer Delay Time	0
Security	
Encryption	Disabled

### Function Description

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

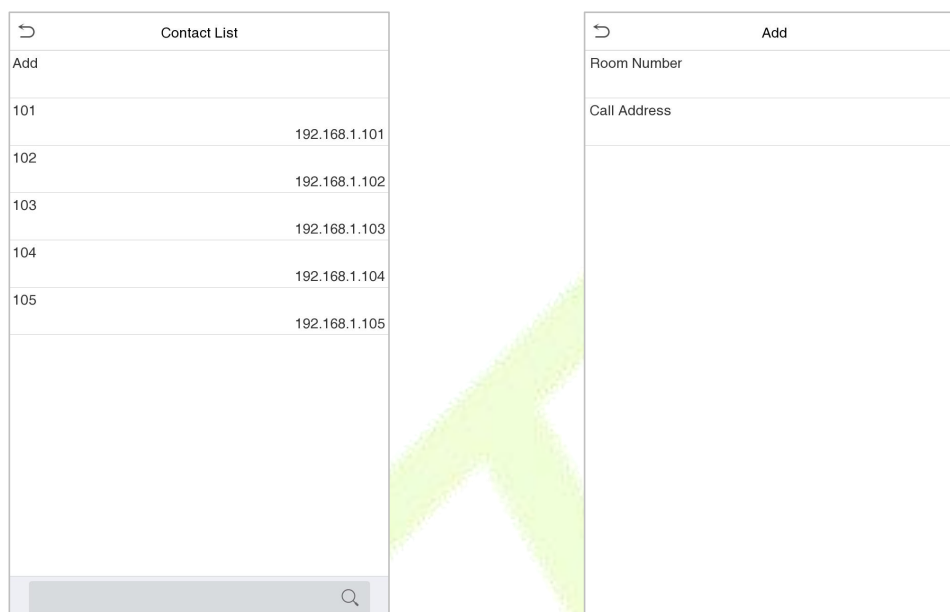


## 9.1.5 Contact List

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

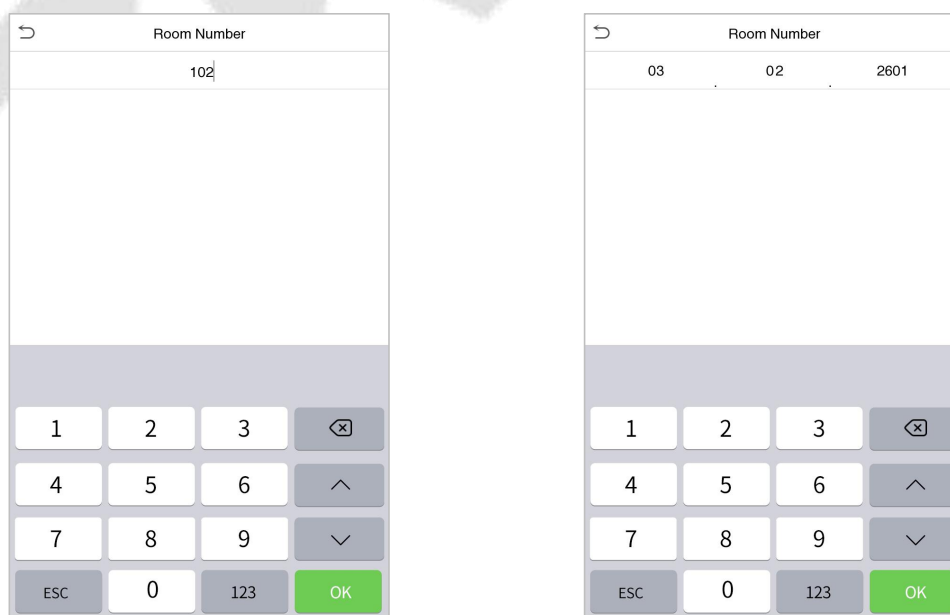
In SIP Server mode, the contact list is synchronized by the ZKBio CVSecurity Server to the device. The contact list can only be viewed, cannot be edited. When the SIP server is disabled, the room number and call address of the indoor monitors can be added here.

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



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

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



Entrance Station


Fence Terminal

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

## 9.1.6 Calling Shortcut Settings

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

Calling Shortcut Settings	
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 **2** shortcut keys that can be enabled and defined in the device: **ROOM1** and **ROOM**. You can set a shortcut key to call the indoor monitor quickly without entering the number of the indoor monitor each time.

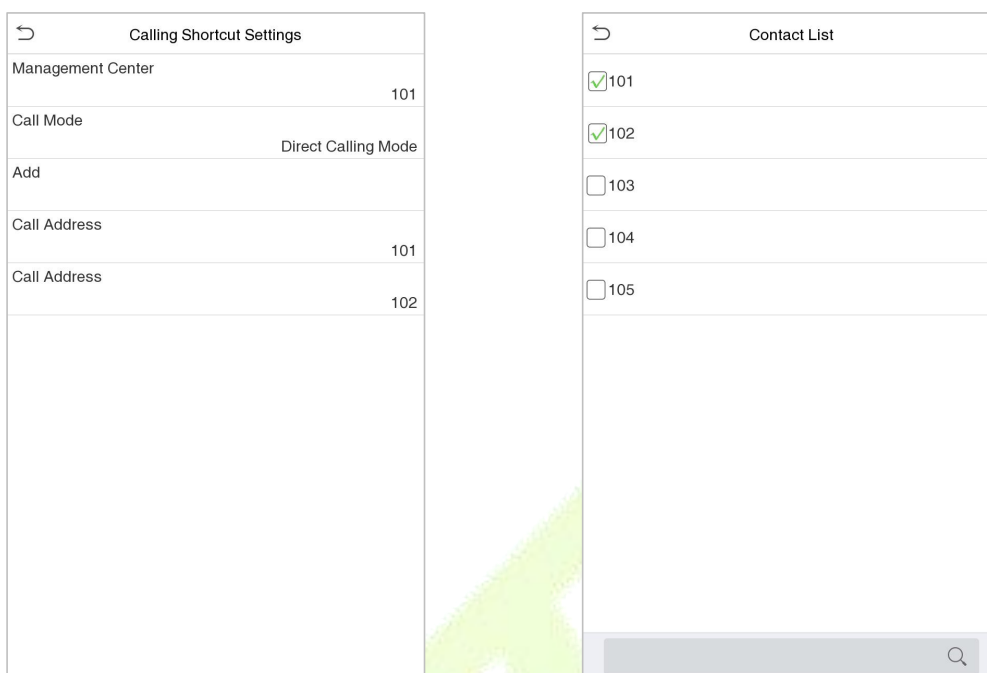
**Name:** Customize the name of the shortcut keys.

**Number:** Select the room number that set in the Contact List Menu.

Number : 101	
Enable	<input checked="" type="checkbox"/>
Name	Management Center
Number	101

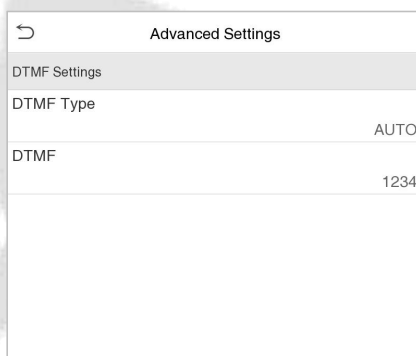
- In Direct Calling mode, the user can call multiple indoor monitors directly.

Click **Call Mode > Direct Calling Mode > Add**, select the indoor monitors that you want to call, then the indoor monitors will be displayed in the list.



### 9.1.7 Advanced Settings

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

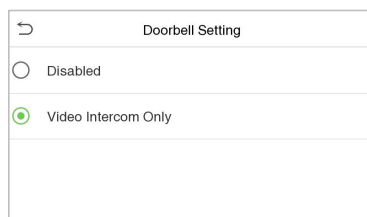


#### Function Description



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

## 9.2 Doorbell Setting

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



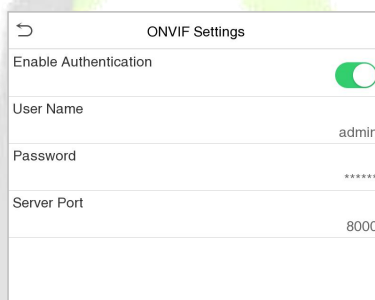
### Function Description

Function Name	Description
<b>Video Intercom Only</b>	Tap  or  icon on standby interface, calling indoor unit for video intercom.

## 9.3 ONVIF Settings

Set the device to the same network segment as the NVR.

1. Tap ONVIF Settings on the Video intercom Parameters interface.

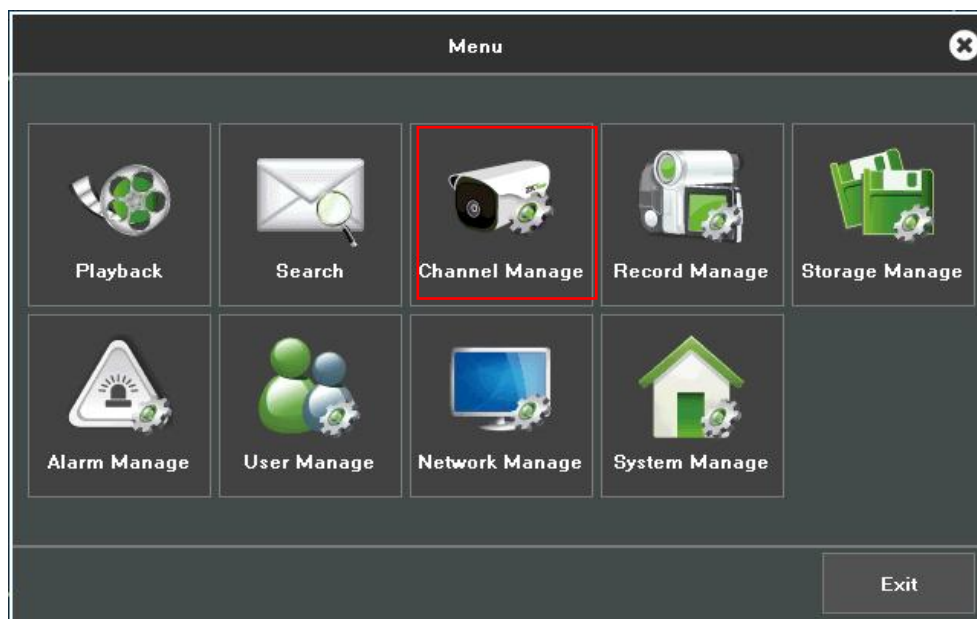


### Function Description

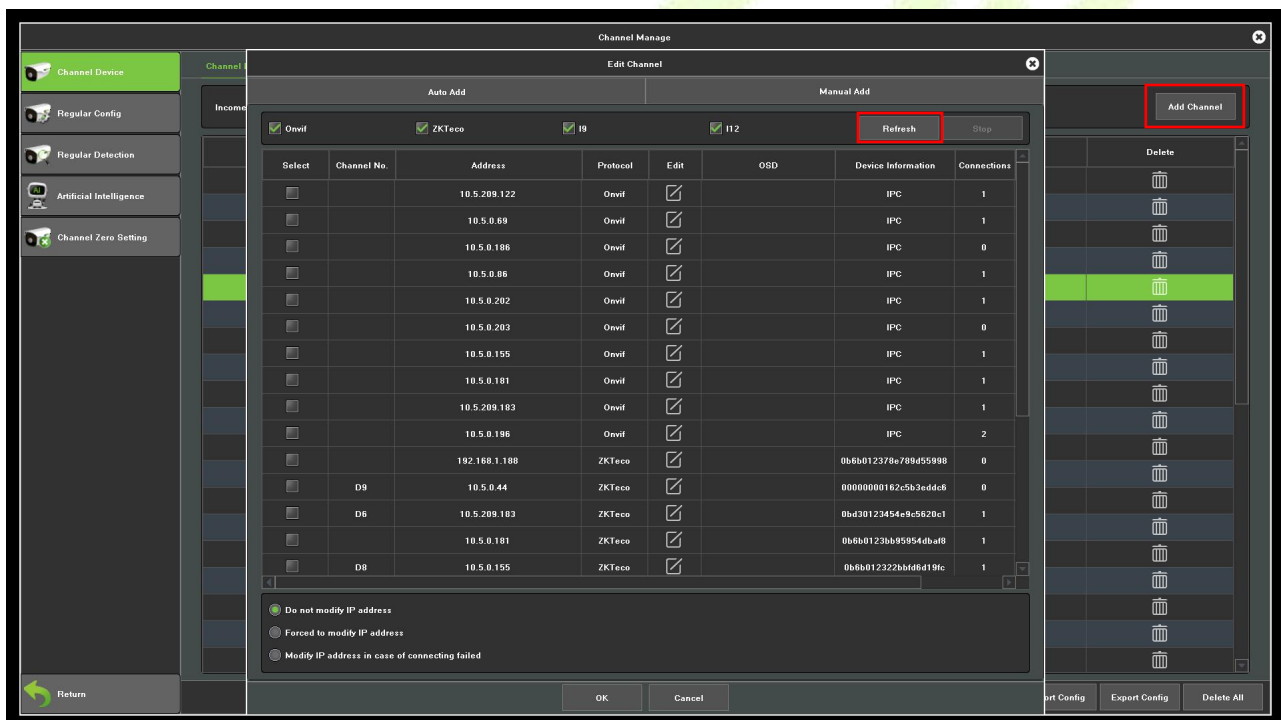
Function Name	Description
<b>Enable Authentication</b>	Enable/Disable the Authentication Function. When it is disabled, there is no need to input the Username and Password when adding the device to the NVR.
<b>Username</b>	Set the Username. The default is <b>admin</b> .
<b>Password</b>	Set the password. The default is <b>admin@123</b> .
<b>Server Port</b>	The default is 8000 and cannot be modified.

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

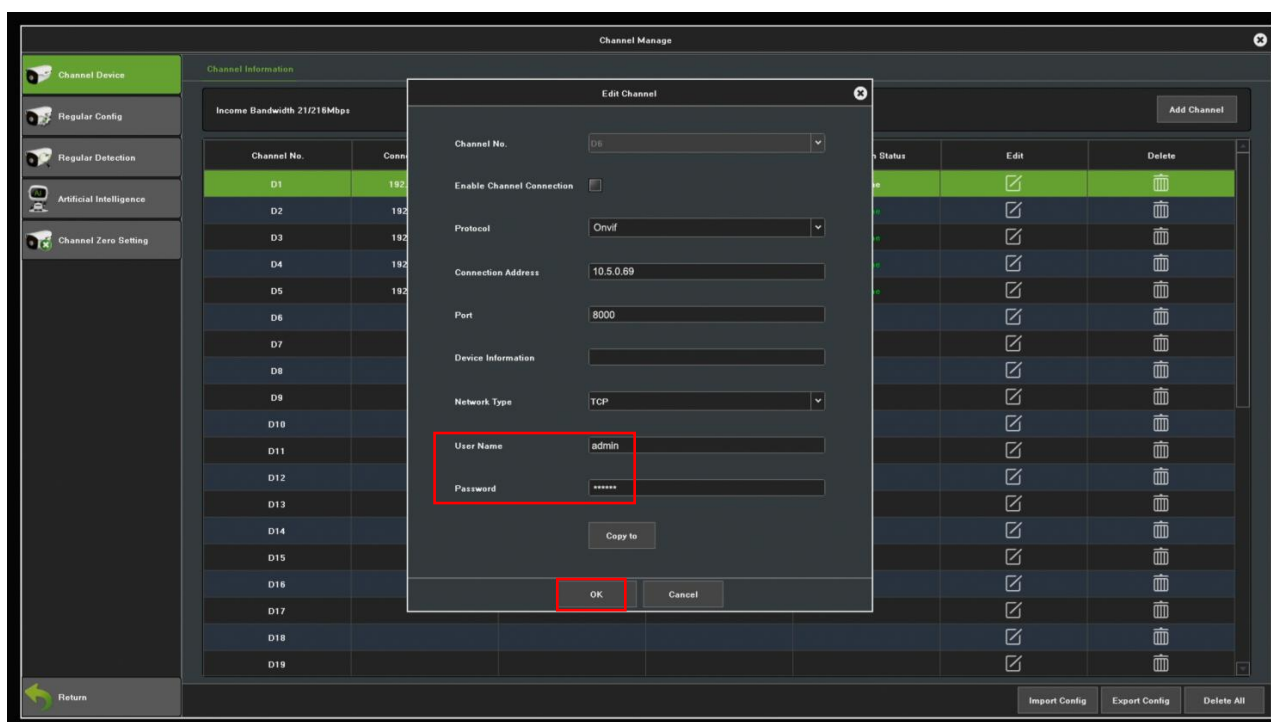
2. On the NVR system, click on **[Start]** > **[Menu]**, then the main menu will pop up.



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

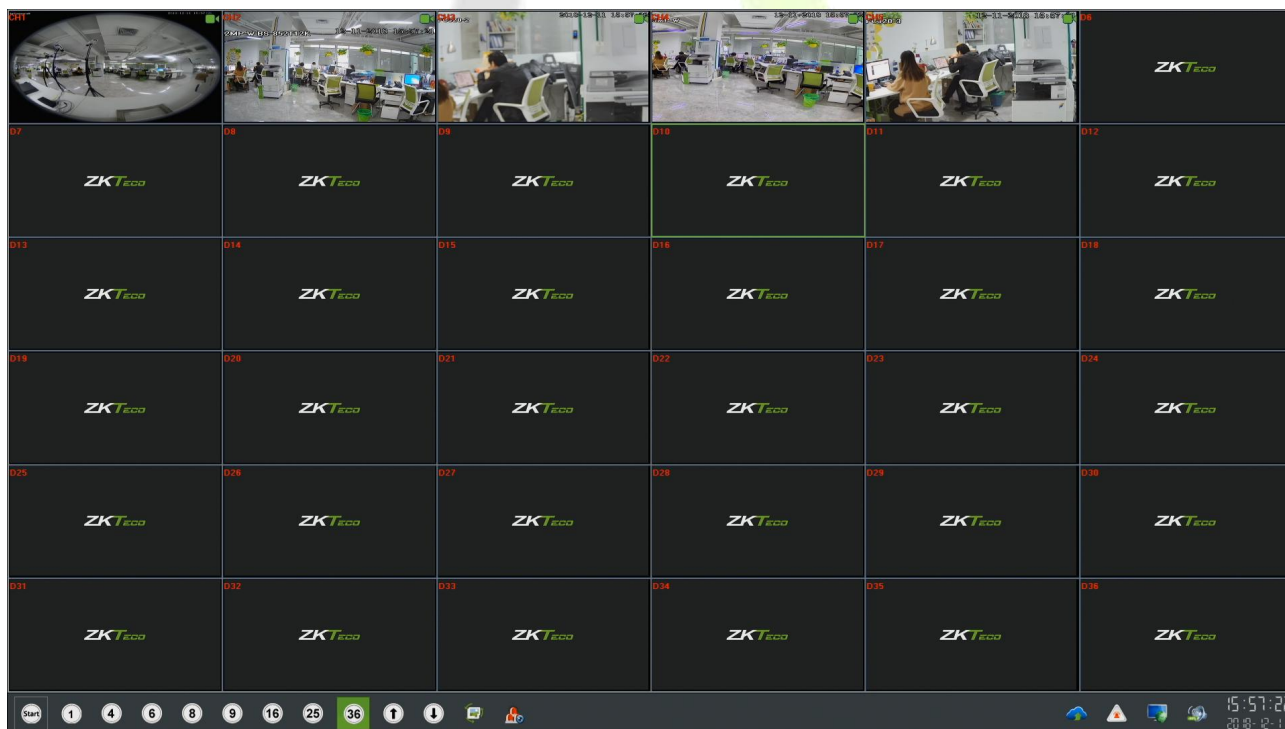


- Select the checkbox for the device you want to add and edit the parameters in the corresponding text field, then click on **[OK]** to add it to the connection list.



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

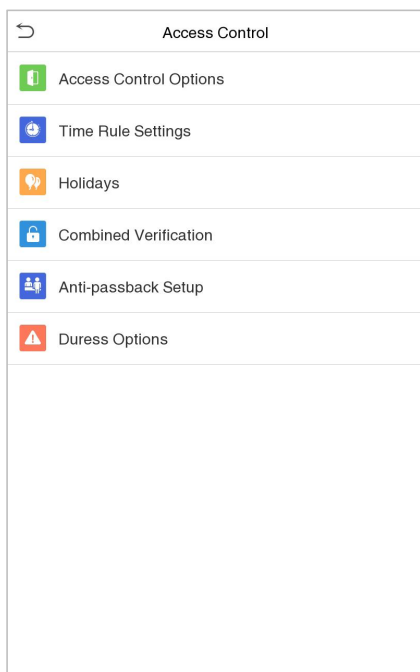
- After adding successfully, the video image obtaining from the device can be viewed in real-time.



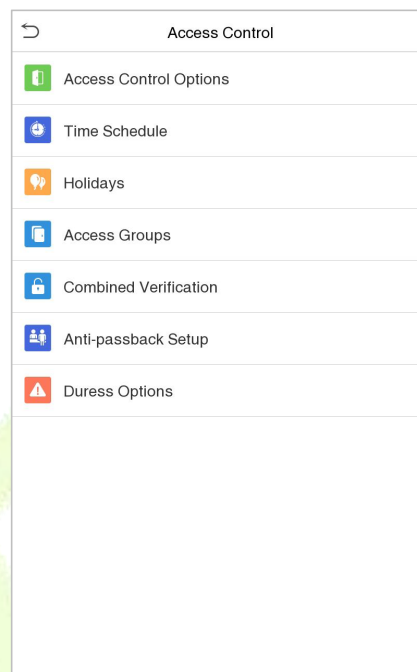
For more details, please refer to the **NVR User Manual**.

## 10. Access Control

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



A&C Terminal



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 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 are 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.

## 10.1 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	<input type="checkbox"/>
Door Lock Delay(s)	5
Door Sensor Delay(s)	10
Door Sensor Type	None
Verification Mode	Password/Card/Face
Door Available Time Period	1
Normal Open Time Period	None
Master Device	In
Slave Device	Out
Auxiliary Input Configuration	
Verify Mode by RS485	Card Only
Speaker Alarm	<input type="checkbox"/>

A&amp;C Terminal

Access Control Options	
Door Lock Delay(s)	5
Door Sensor Delay(s)	10
Door Sensor Type	None
Verification Mode	Password/Card/Face
Door Available Time Period	1
Normal Open Time Period	None
Master Device	In
Slave Device	Out
Auxiliary Input Configuration	
Verify Mode by RS485	Card Only
Speaker Alarm	<input type="checkbox"/>
Reset Access Settings	

T&amp;A Terminal

Access Control Options	
Door Lock Delay(s)	10
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	<input type="checkbox"/>
Speaker Alarm	<input type="checkbox"/>
Reset Access Settings	

### Function Description of A&C Terminal:

Function Name	Description
<b>Gate Control Mode</b>	Toggle between ON or OFF switch to get into gate control mode or not. When set to <b>ON</b> , on this interface will remove Door lock relay, Door sensor relay and Door sensor type options.
<b>Door Lock Delay (s)</b>	The length of time that the device controls the electric lock to be in unlock state. Valid value: 1~10 seconds; 0 second represents disabling the function.
<b>Door Sensor Delay (s)</b>	If the door is not locked and is being 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.
<b>Door Sensor Type</b>	There are three Sensor types: <b>None</b> , <b>Normal Open</b> and <b>Normal Closed</b> . <b>None</b> : It means door sensor is not in use. <b>Normal Open(NO)</b> : It means the door is always left opened when electric power is on. <b>Normal Closed(NC)</b> : It means the door is always left closed when electric power is on.
<b>Verification Mode</b>	The supported verification mode includes Password/Card/Face, User ID Only, Password, Card Only, Password + Card, Password/Card, Face Only, Face + Password, and Face + Card.



<b>Door Available Time Period</b>	To set time period for door, so that the door is available only during that period.
<b>Normal Open Time Period</b>	Scheduled time period for “Normal Open” mode, so that the door is always left open during this period.
<b>Master Device</b>	When setting up the master, the status of the master can be set to exit on enter. <b>Out:</b> The record verified on the host is the exit record. <b>In:</b> The record verified on the host is the entry record.
<b>Slave Device</b>	When setting up the slave, the status of the slave can be set to exit on enter. <b>Out:</b> The record verified on the host is the exit record. <b>In:</b> The record verified on the host is the entry record.
<b>Auxiliary Input Configuration</b>	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.
<b>Verify Mode by RS485</b>	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.
<b>Speaker Alarm</b>	Transmits a sound alarm or disassembly alarm from the local. When the door is closed or the verification is successful, the system will cancel the alarm from the local.
<b>Reset Access Settings</b>	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
<b>Door Lock Delay (s)</b>	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.
<b>Door Sensor Delay (s)</b>	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.
<b>Door Sensor Type</b>	There are three Sensor types: <b>None</b> , <b>Normal Open</b> , and <b>Normal Closed</b> . <b>None:</b> It means the door sensor is not in use. <b>Normally Open (NO):</b> It means the door is always left open when electric power is on. <b>Normally Closed (NC):</b> It means the door is always left closed when electric power is on.
<b>Door Alarm Delay (s)</b>	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 <b>Door Alarm Delay</b> . The valid value ranges from 1 to 999 seconds.

<b>Retry Times to Alarm</b>	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.
<b>Normal Close Time Period</b>	It is the scheduled time-period for "Normal Close" mode so that the door is always close during this period.
<b>Normal Open Time Period</b>	It is the scheduled time-period for "Normal Open" mode so that the door is always open during this period.
<b>Auxiliary Input Configuration</b>	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.
<b>Verify Mode by RS485</b>	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.
<b>Valid Holidays</b>	To set if <b>Normal Close Time Period</b> or <b>Normal Open Time Period</b> settings are valid in set holiday time period. Choose <b>[ON]</b> to enable the set <b>NC</b> or <b>NO</b> time period in holiday.
<b>Speaker Alarm</b>	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.
<b>Reset Access Settings</b>	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.

## 10.2 Time Rule Setting/Time Schedule

### Function Description of A&C Terminal:

Tap **Time Rule Setting** 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: 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

▲

00

▼

HH

▲

00

▼

MM

▲

23

▼

HH

▲

59

▼

MM

Confirm (OK)

Cancel (ESC)

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

**Notes:**

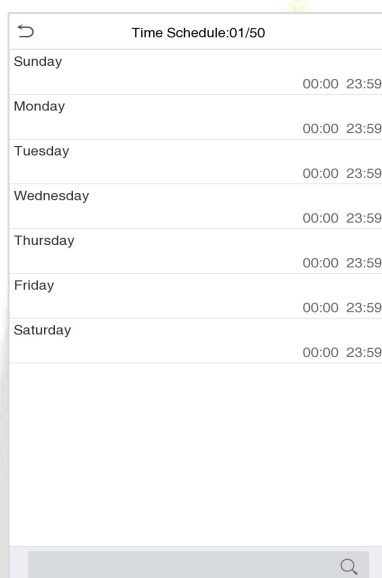
- When the End Time is earlier than the Start Time, (such as 23:57~23:56), it indicates that access is prohibited all day.
- When the End Time is later than the Start Time, (such as 00:00~23:59), it indicates that the interval is valid.
- The effective Time Period to keep the Door Unlock or open all day is (00:00 to 23:59) or also when the Ending Time is later than the Starting Time, (such as 08:00 to 23:59).
- The default Time Zone 1 indicates that 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
<input type="text"/>	

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

Monday

00:00 23:59

00 00 23 59

HH MM HH MM

Confirm (OK) Cancel (ESC)

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.

## 10.3 Holidays

Whenever there is a holiday, you may need a special access time; but changing everyone's access time one by one is extremely cumbersome, so you can set a holiday access time which is applicable 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.

Holidays

Add Holiday

All Holidays

- **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	<input checked="" type="checkbox"/>

- **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 deletion. After deletion, this holiday is no longer displayed on **All Holidays** interface.

## 10.4 Access Groups★

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.

Access Groups	
New Group	
All Groups	

- **Add a New Group**

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

Access Groups	
No.	2
Verification Mode	Password/Card/Face
Time Period 1	1
Time Period 2	0
Time Period 3	0
Include Holidays	<input type="checkbox"/>

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

## 10.5 Combined Verification

Access groups are arranged into different door-unlocking combinations to achieve multiple verifications and strengthen the security. In a door-unlocking combination, the range of the combined number N is:  $0 \leq N \leq 5$ , and the number of members N may all belong to one access group or may belong to five different access groups.

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
<input type="text"/>	



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:**

- The **Door-unlock combination 1** is set as **(01 03 05 06 08)**, indicating that the unlock combination 1 consists of 5 people, and the 5 individuals are from 5 groups, namely, **Access Control Group 1** (AC group 1), AC group 3, AC group 5, AC group 6, and AC group 8, respectively.
- The **Door-unlock combination 2** is set as **(02 02 04 04 07)**, indicating 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.
- The **Door-unlock combination 3** is set as **(09 09 09 09 09)**, indicating that there are 5 people in this combination; all of which are from AC group 9.
- The **Door-unlock combination 4** is set as **(03 05 08 00 00)**, indicating 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.

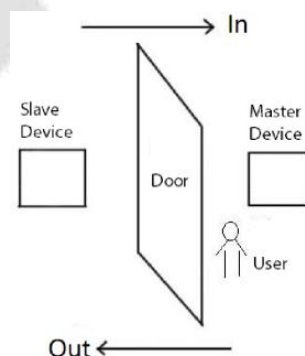
- **Delete a Door-unlocking Combination:**

Set all Door-unlock combinations to 0 if you want to delete door-unlock combinations.

## 10.6 Anti-passback Setup

It is possible that users may be followed by some persons to enter the door without verification, resulting in a security breach. So, to avoid such a situation, the Anti-Passback option was developed. Once it is enabled, the check-in record must match with the check-out record so as to open the door.

This function requires two devices to work together: one is installed inside the door (master device), and the other one is installed outside the door (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.



A&amp;C Terminal

T&amp;A Terminal

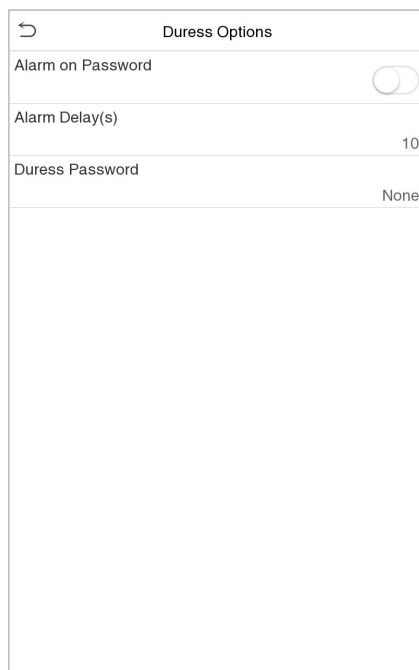
### Function Description

Function Name	Description
<b>Anti-passback Direction</b>	<p><b>No Anti-passback:</b> 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.</p> <p><b>Out Anti-passback:</b> After a user checks out, only if the last record is a check-in record, the user can check-out again; otherwise, the alarm will be triggered. However, the user can check-in freely.</p> <p><b>In Anti-passback:</b> After a user checks in, only if the last record is a check-out record, the user can check-in again; otherwise, the alarm will be triggered. However, the user can check-out freely.</p> <p><b>In/Out Anti-passback:</b> After a user checks in/out, only if the last record is a check-out record, the user can check-in again; or if it is a check-in record, the user can check-out again; otherwise, the alarm will be triggered.</p>
<b>Device Status</b>	<p>While configuring the master and slave devices, you may set the state of the master as <b>Out</b> or <b>In</b>.</p> <p><b>None:</b> Disables anti-passback functionality on this device.</p> <p><b>Out:</b> Records verified on this device are exit records.</p> <p><b>In:</b> Records verified on this device are entry records.</p>
<b>Slave Device</b>	<p>While configuring the master and slave devices, you may set the state of the slave as <b>Out</b> or <b>In</b>.</p> <p><b>None:</b> Disables anti-passback functionality of the slave device.</p> <p><b>Out:</b> A record of verification on the slave device is a check-out record.</p> <p><b>In:</b> A record of verification on the slave device is a check-in record.</p>

## 10.7 Duress Options

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

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



Duress Options

Alarm on Password ☐

Alarm Delay(s) 10

Duress Password None

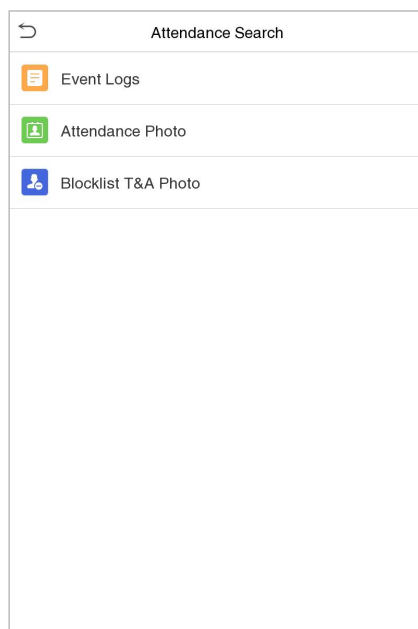
### Function Description

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

## 11. Attendance Search

Once the identity of a user is verified, the Event Logs will be saved in the device. This function enables users to check their access records.

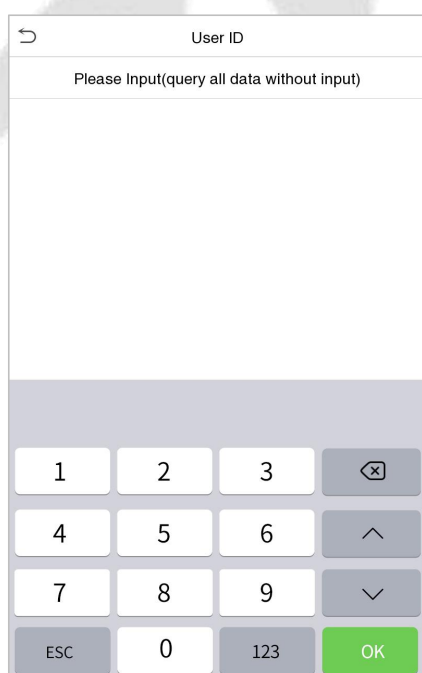
Click **Attendance Search** on the **Main Menu** interface to search for the required Access/Attendance log.



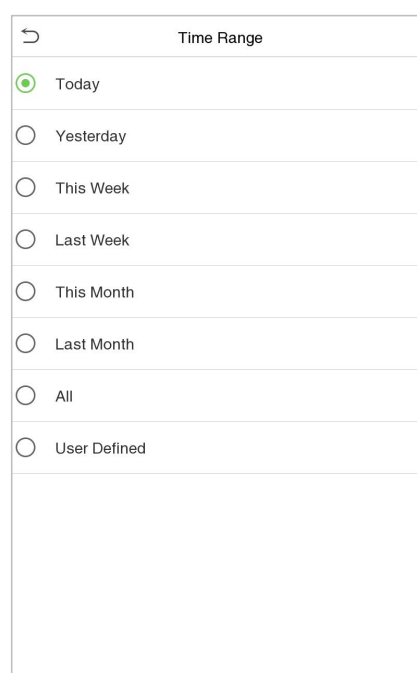
The process of searching for attendance and blocklist photos is similar to that of searching for event logs. The following is an example of searching for event logs.

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

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



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



3. Once the log search succeeds. Tap the login highlighted in green to view its details.

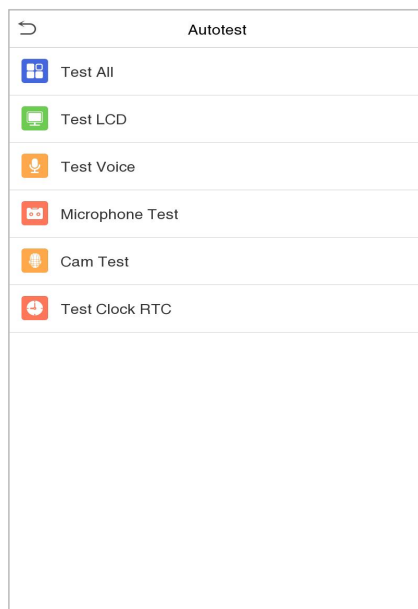
Personal Record Search		
Date	User ID	Time
09-01		Number of Records:11
	0	22:03 22:03
	2	06:29 06:29
	3	06:25 06:25 06:24 06:24
		06:24 06:24 06:24
08-31		Number of Records:14
	0	23:07 23:07 23:06 23:06
		23:06 23:06 23:06 23:06
		22:57 22:57 22:52 22:52
		22:08 22:08
08-29		Number of Records:5
	0	14:03 14:03 14:02 14:02
		14:02
08-27		Number of Records:8
	0	19:32 19:32 11:49 11:49
		11:49 11:49 11:48 11:48
08-21		Number of Records:2
	0	19:50 19:50
08-19		Number of Records:12
	0	16:32 16:32 16:32 16:32
		16:31 16:31 16:29 16:29
		16:19 16:19 16:14 16:14

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

Personal Record Search	
User ID	Time
0	09-01 22:03
0	09-01 22:03
2	09-01 06:29
2	09-01 06:29
3	09-01 06:25
3	09-01 06:25
3	09-01 06:25
3	09-01 06:24
3	09-01 06:24
3	09-01 06:24
3	09-01 06:24
3	09-01 06:24
3	09-01 06:24
Name : Status : Other Verification Mode : Other	

## 12. Autotest

On the **Main Menu**, tap **Autotest** to automatically test whether all modules in the device function properly, which include the LCD, Voice, Camera and Real-Time Clock (RTC).

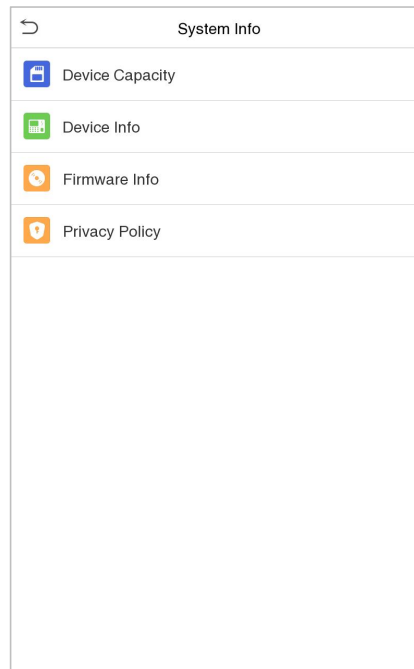


### Function Description

Function Name	Description
<b>Test All</b>	To automatically test whether the LCD, Audio, Camera and RTC are normal.
<b>Test LCD</b>	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.
<b>Test Voice</b>	To automatically test whether the audio files stored in the device are complete and the voice quality is good.
<b>Microphone Test</b>	Check whether the microphone is working by speaking to microphone and playing the microphone recording.
<b>Test Fingerprint Sensor</b>	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.
<b>Cam Test</b>	To test if the camera functions properly by checking the photos taken to see if they are clear enough. Same as " <b>Test Face</b> ".
<b>Test Clock RTC</b>	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.

## 13. 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
<b>Device Capacity</b>	Displays the current device's user storage, password, face template and card storage, access records, attendance and blocklist photos, and profile photos.
<b>Device Info</b>	Displays the device's name, serial number, MAC address, face template algorithm, platform information, MCU Version and manufacture date.
<b>Firmware Info</b>	Displays the firmware version and other version information of the device.
<b>Privacy Policy</b>	<p>The privacy policy control will appear when the gadget turns on for the first time. After clicking "<b>I have read it</b>," the customer can use the product regularly. Click <b>System Info &gt; Privacy Policy</b> to view the content of the privacy policy. The privacy policy's content does not allow for U disc export.</p> <p><b>Note:</b> 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.</p>

## 14. Connect to ZKBio CVSecurity Software

### 14.1 Set the Communication Address

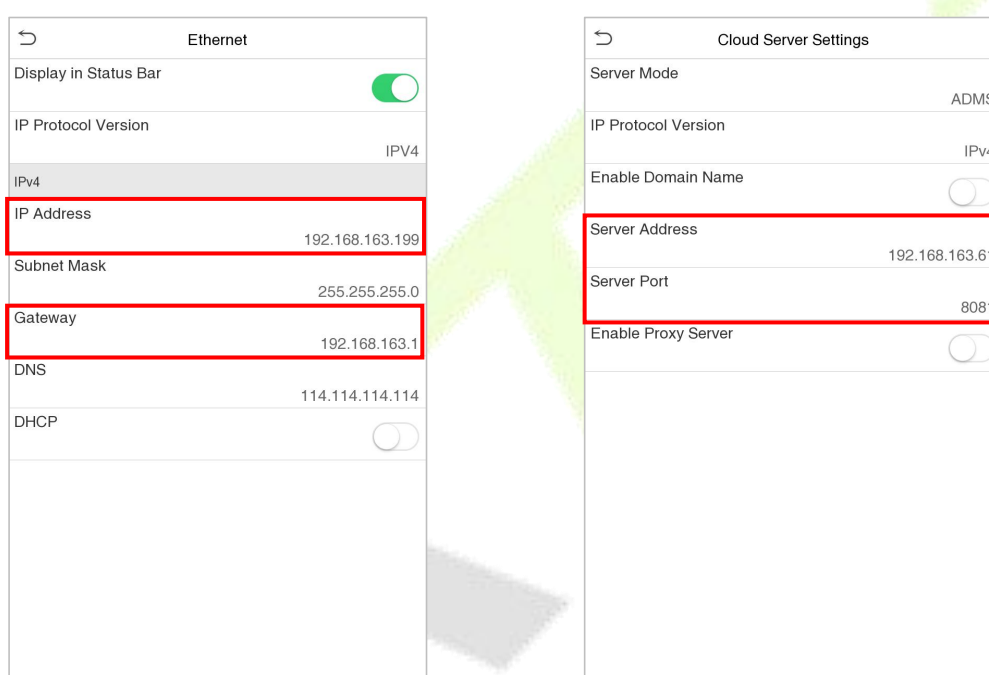
#### ● Device Side

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

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 CVSecurity server.

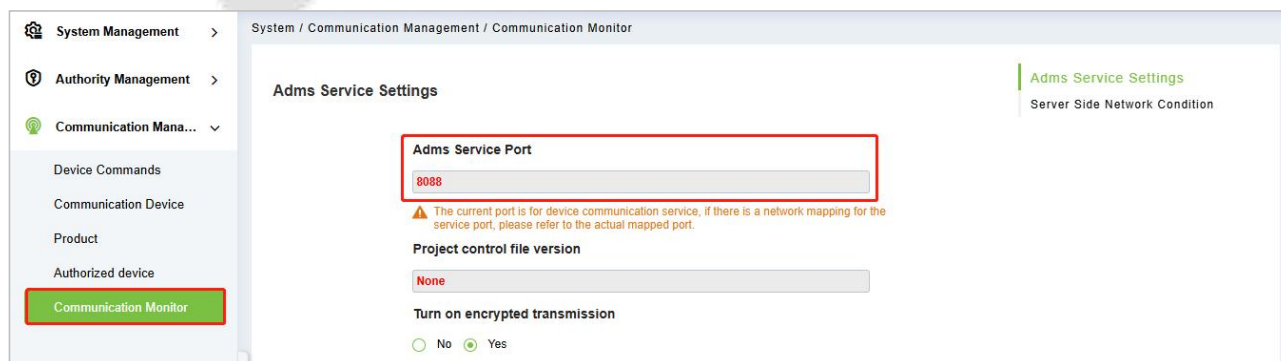
**Server port:** Set the server port as of ZKBio CVSecurity.



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

#### ● Software Side

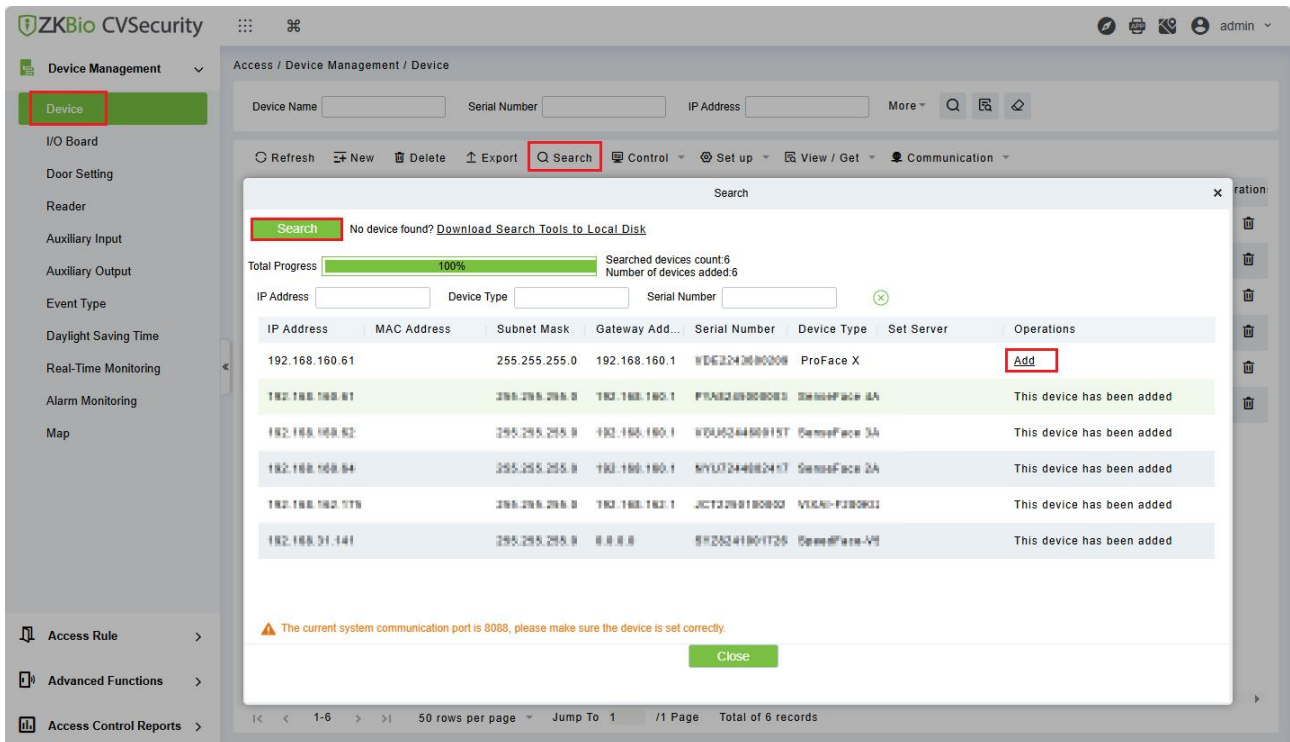
Login to ZKBio CVSecurity software, click **System > Communication > Communication Monitor** to set the ADMS service port, as shown in the figure below:



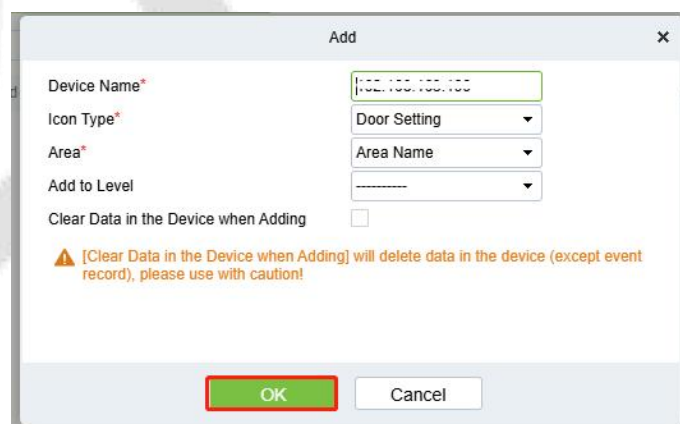
## 14.2 Add Device on the Software

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

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



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.

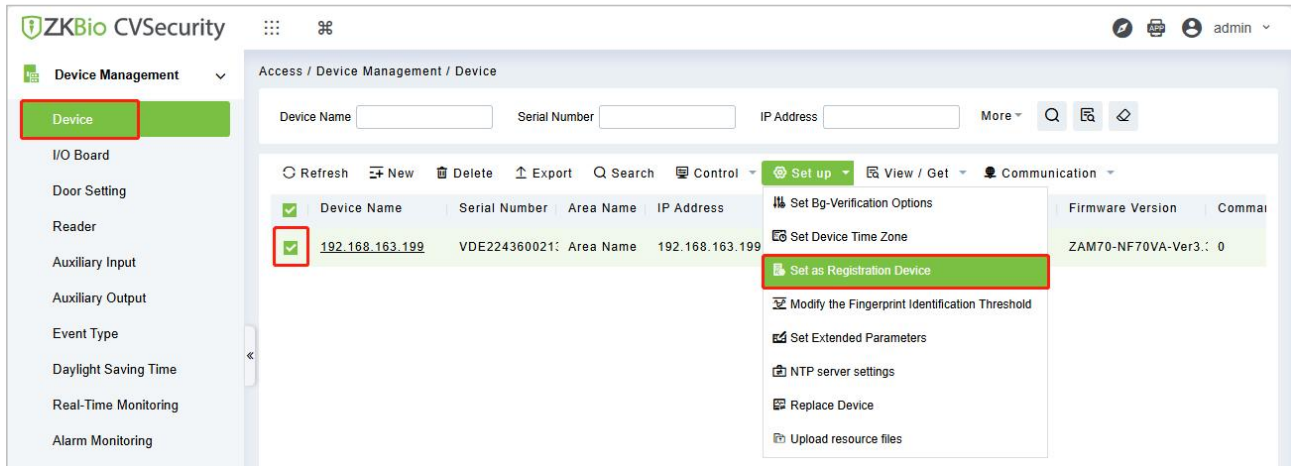


5. After the addition is successful, the device will be displayed in the device list.

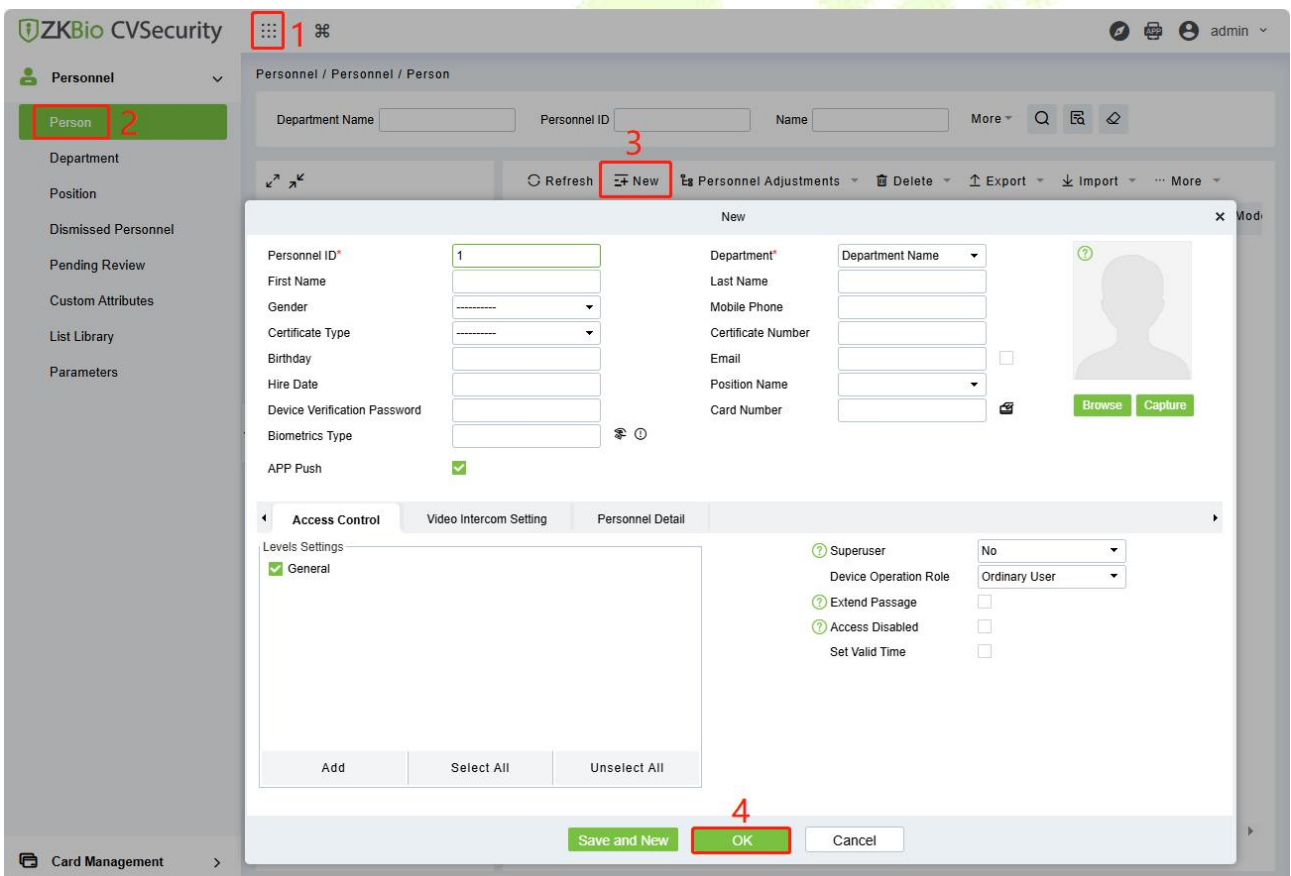


## 14.3 Add Personnel on the Software and Online Fingerprint/Face Registration

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



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



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

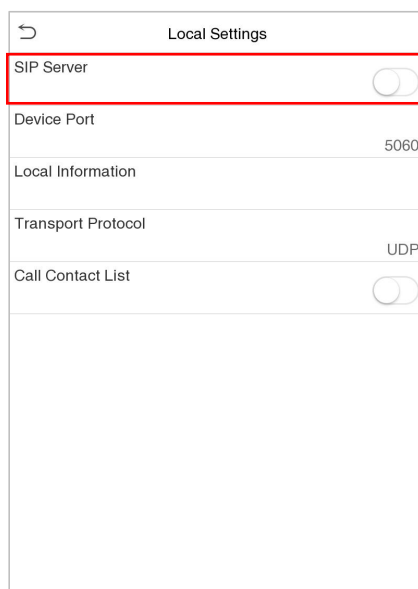
**Note:** For other specific operations, please refer the ZKBio CVSecurity User Manual.

## 15. SIP Video Intercom

### 15.1 Local Area Network Use


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

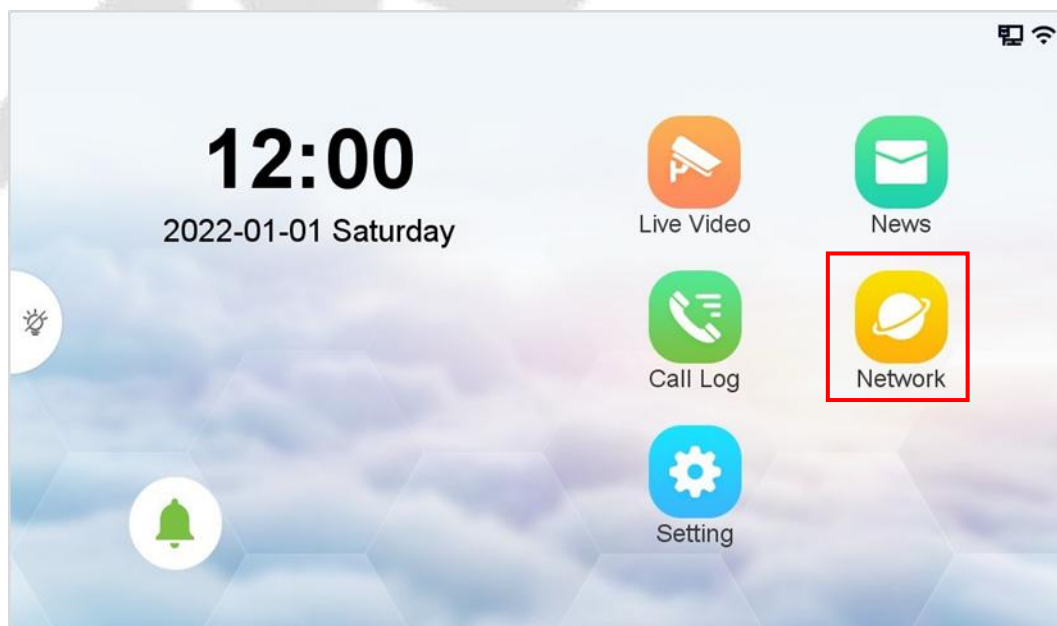
Click **Intercom** > **SIP Settings** > **Local Settings** to turn off the SIP server.



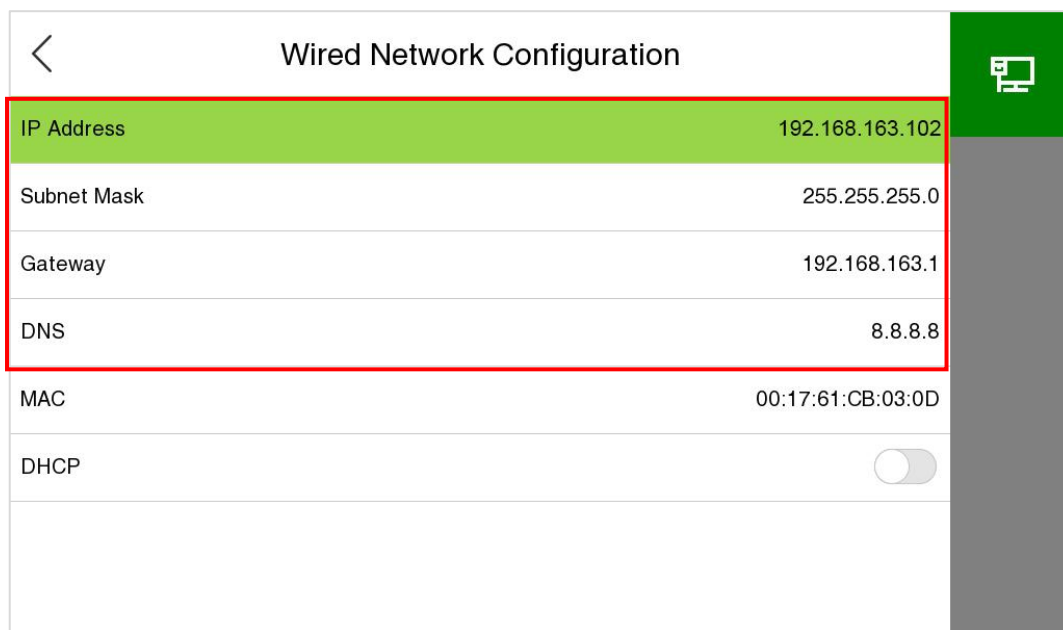
This function needs to be used with the indoor monitor VT07-B01.

- **On the Indoor Monitor:**

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

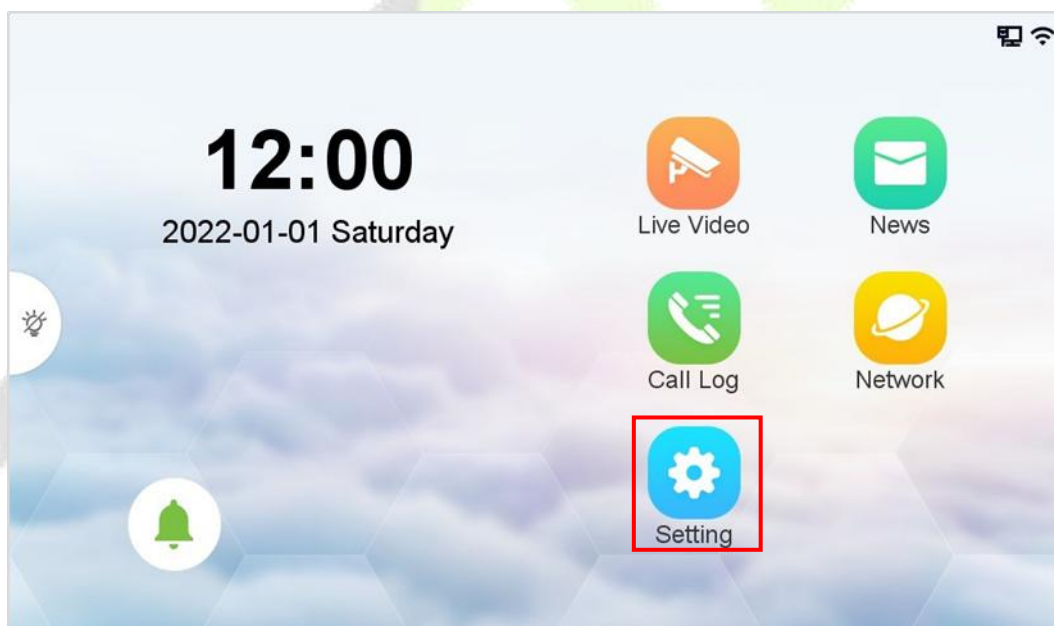


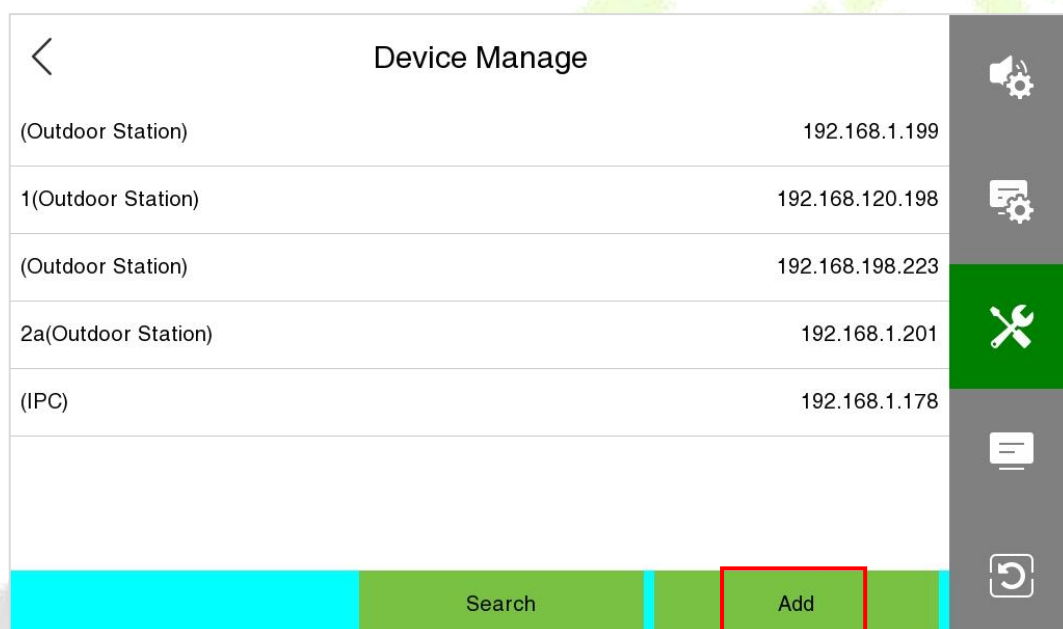
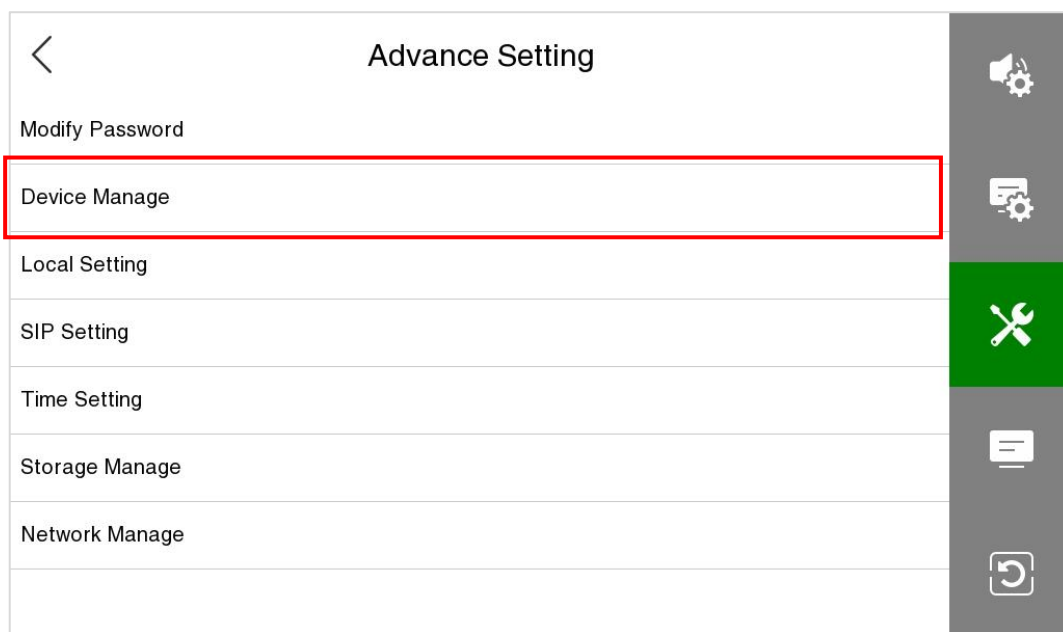
2. Set the IP Address and Gateway of the indoor monitor. (**Note:** The IP address should be in the same network segment as the device.)



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	<input type="checkbox"/>

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





4. Set the related information of the device, then click **Save**.

**Device Type:** Set as Outdoor Station.

**Device IP:** Enter the IP address of the device.

Device Port: 8000.

Username: admin.

Password: 123456.

Device Configuration		1↓
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 Device:** Click **[Intercom]** > **[SIP Settings]** > **[Contact List]** > **[Add]** to add the connected indoor monitors.

Intercom

- SIP Settings
- Doorbell Setting
- ONVIF Settings

SIP Settings

- Local Settings
- Audio Options
- Video Options
- Call Options
- Contact List
- Calling Shortcut Settings
- Advanced Settings

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 to 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".

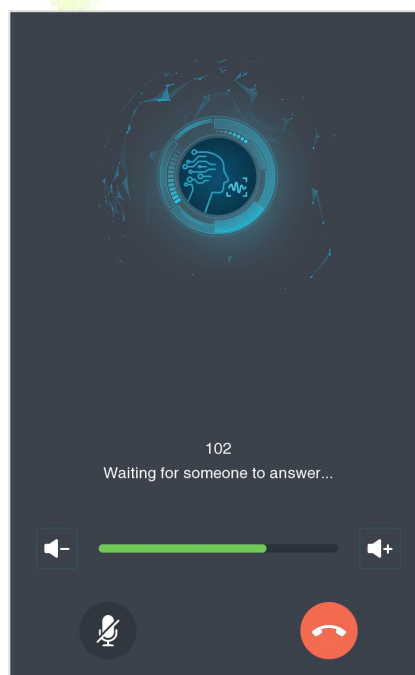
Entrance Station

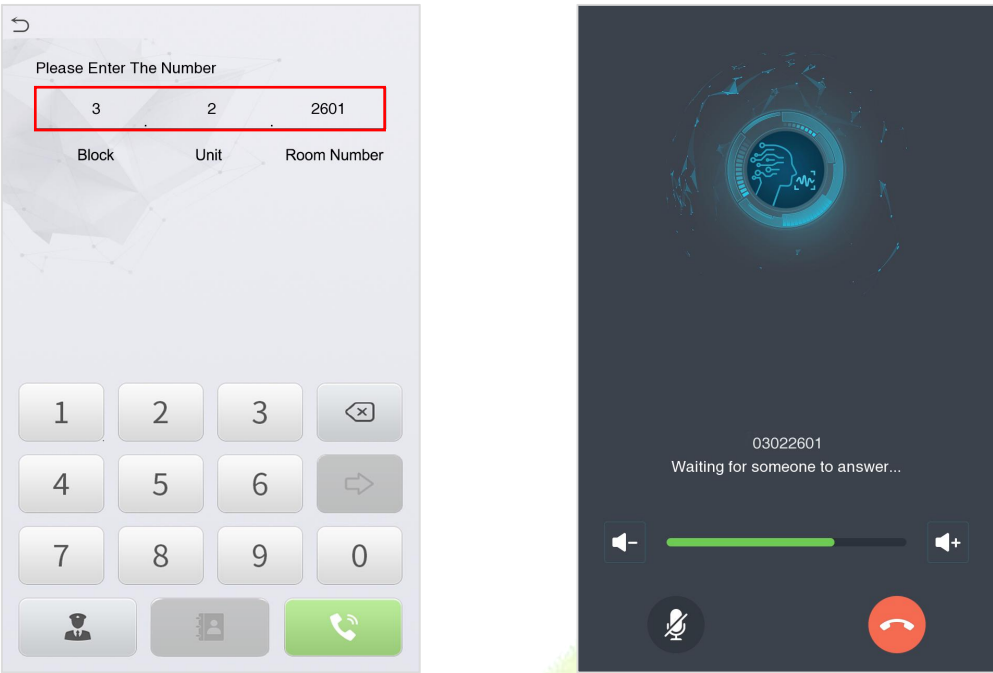
Fence Terminal

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

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

Entrance Station



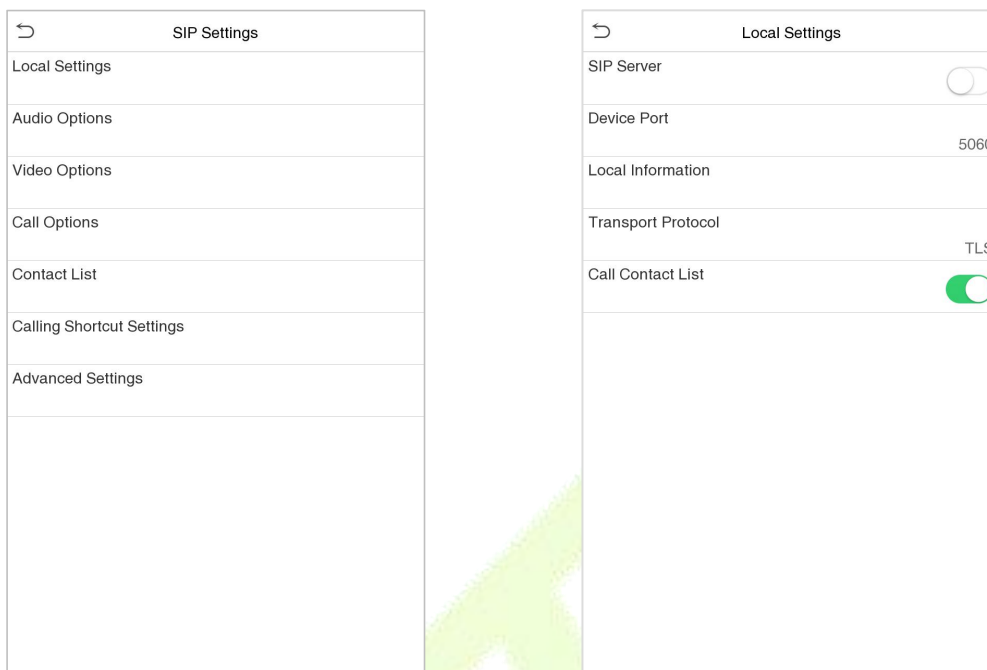




Fence Termina

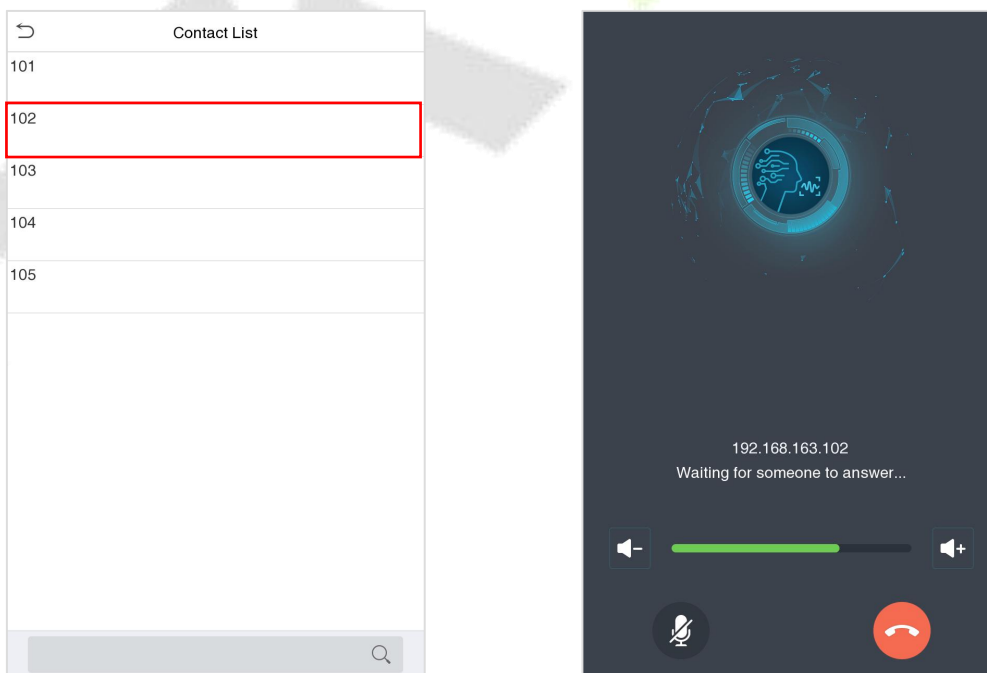


### 15.1.1 Call Contact List

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



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



### 15.1.2 Custom the Calling Shortcut Keys


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



SIP Settings	Calling Shortcut ...	Number : 102
Local Settings	Management Center	Enable <input checked="" type="checkbox"/>
Audio Options	Call Mode	Name ROOM1
Video Options	ROOM1	Number 102
Call Options	ROOM2	
Contact List	ROOM3	
Calling Shortcut Settings	ROOM4	
Advanced Settings		

**Name:** Customize the name of the shortcut keys.

**Number:** It is the room number that set in the **Contact List** Menu.

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

Please Enter The Number


ROOM1 ROOM2

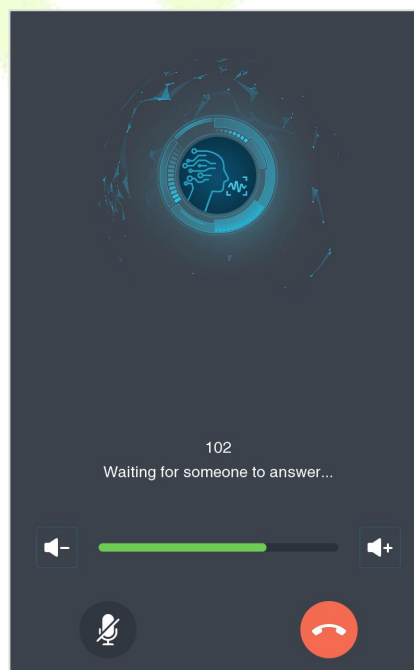
ROOM3 ROOM4

1 2 3

4 5 6

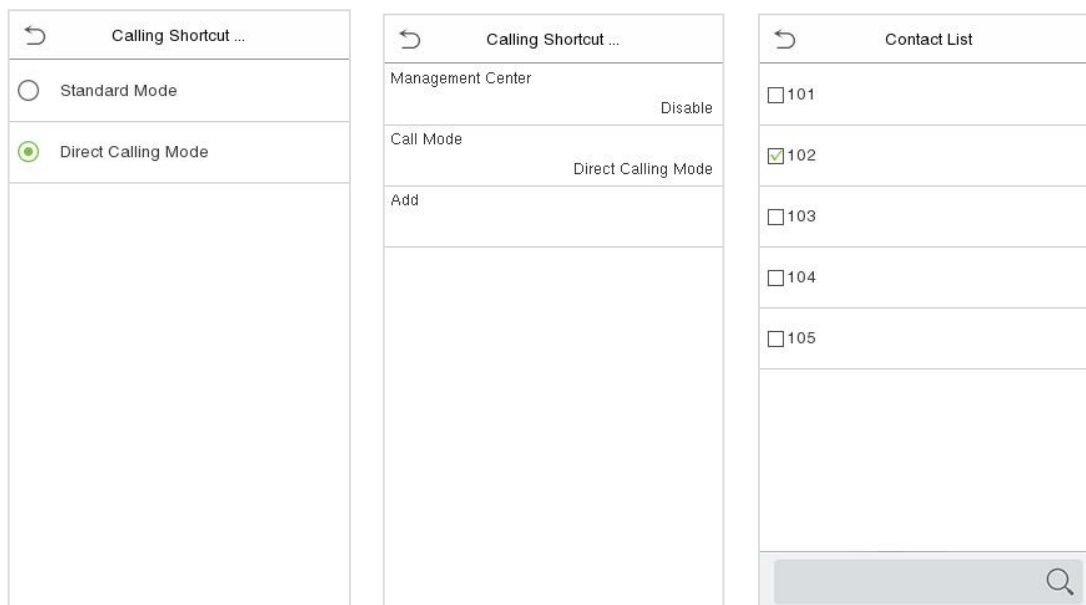
7 8 9 0




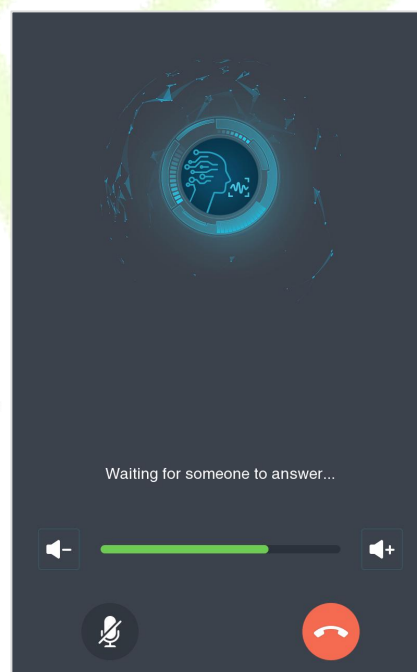
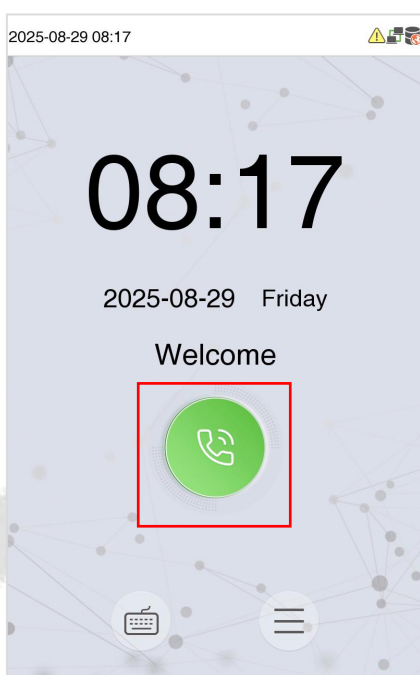


### 15.1.3 Direct Calling

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



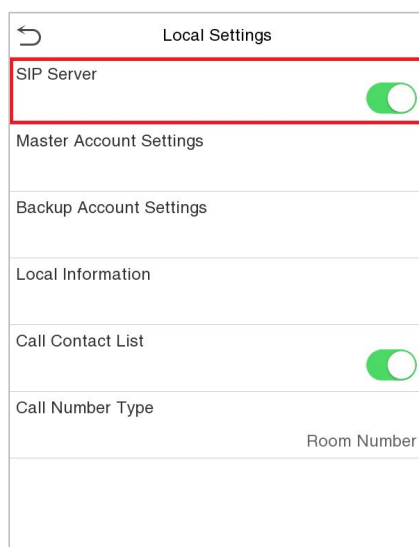
2. Then you can click the icon  on the device to call the indoor monitors directly.



## 15.2 SIP Server

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

Click **Intercom** > **SIP Settings** > **Local Settings** to enable the SIP server.



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

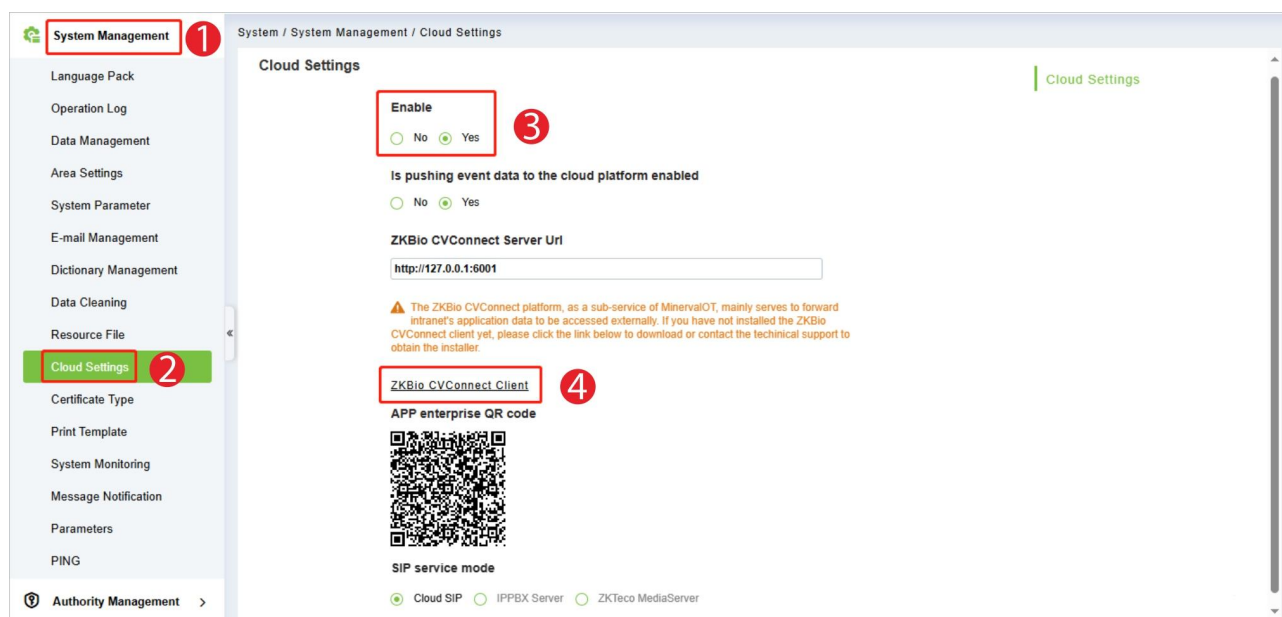
ZKBio CVSecurity supports 2 kinds of SIP server: **cloud SIP** and **PBX server**, users can choose one according to the actual situation.

- **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.

### 15.2.1 SIP Server Configuration

1. On ZKBio CVSecurity, click **System > System Management > Cloud Setting** to enable the Cloud SIP service.
2. Click **ZKBio CVConnect Client** to download and install it. (**Note:** The installation and activation of the client can see the ZKBio Zexus Mobile App User Manual. )

**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 CVSecurity

Endpoint:

Next

- **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 CVSecurity.
- **EndPoint:** The server address of your local application. For example, if your local application is ZKBio CVSecurity 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.

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

No account yet, please click [Register](#).

\* Username:

\* Password:

Previous      Next

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](#)

CONTACT US TERMS & CONDITIONS PRIVACY POLICY

### 3. Select 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.

1 Please select area 2 Bind Hybrid Cloud account 3 Select company 4 Activation waiting

\* Select company: Company-ZK-Popy-test

Use new company

Previous Next

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.

1 Please select area 2 Bind Hybrid Cloud account 3 Select company 4 Activation waiting

\* Country: United Arab Emirates

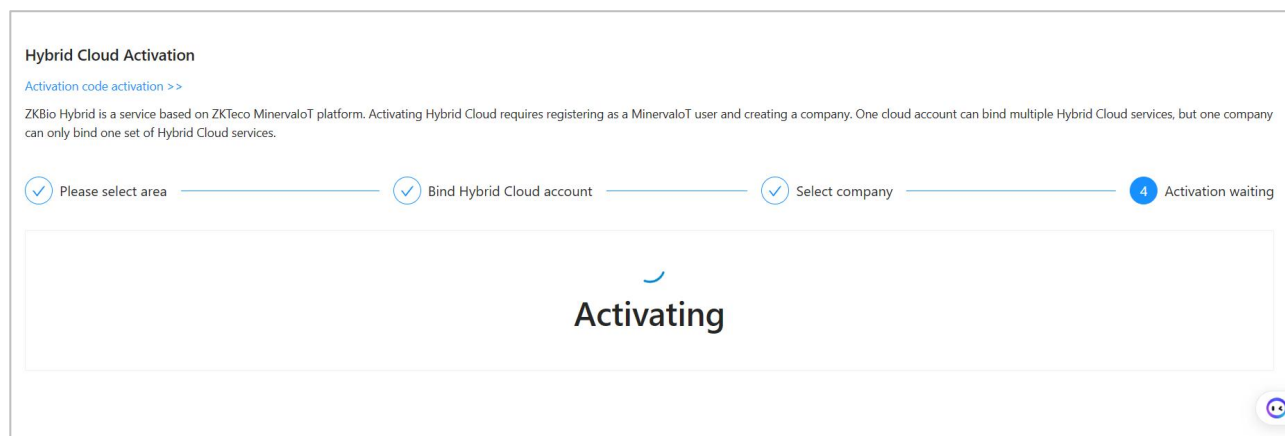
\* Name: Popy-test-company-1

\* Code: 1234567

Use existing company

Previous Create Company

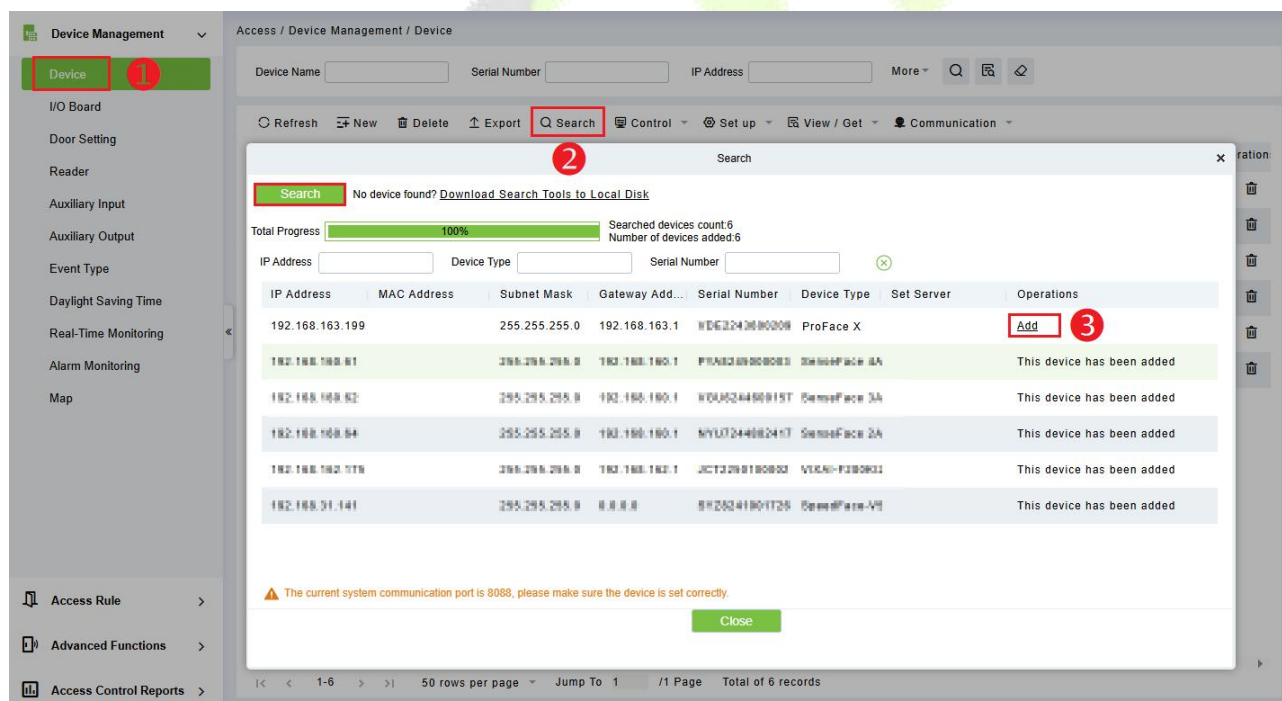
Start Activating and wait for 1-2 minutes until the Activation completely.



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

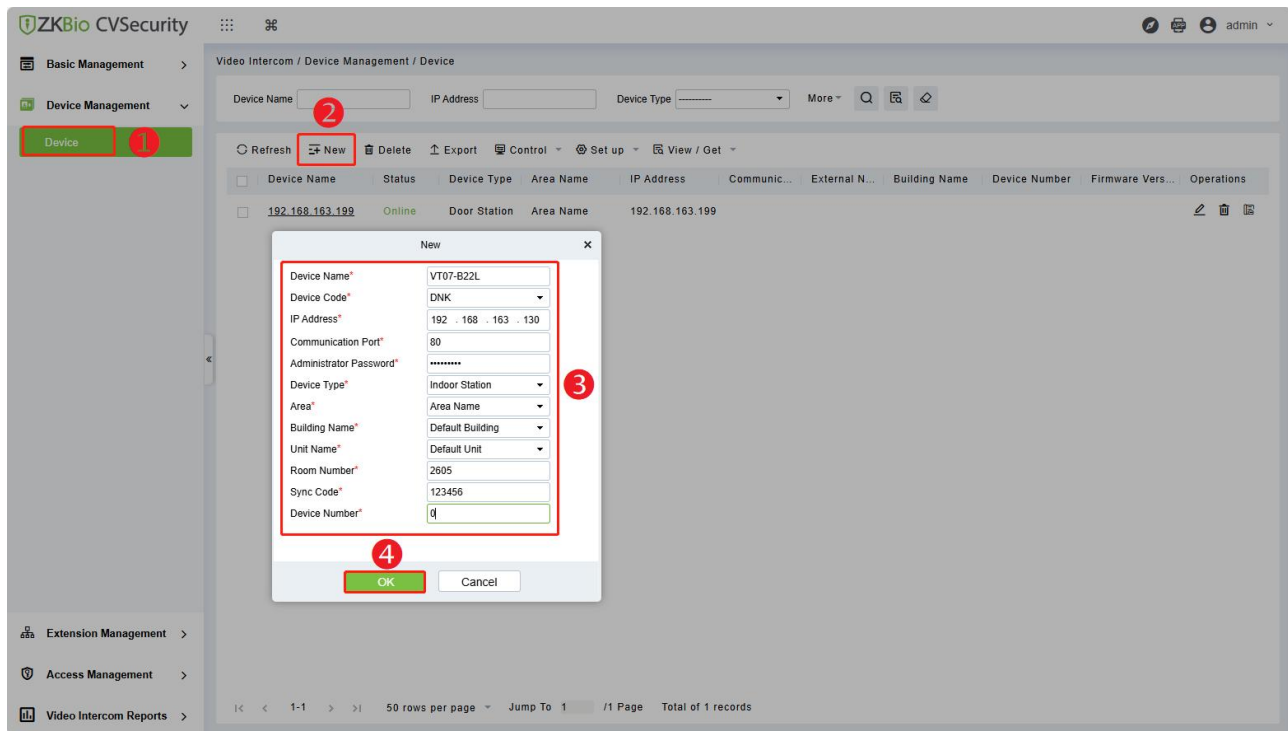
## 15.2.2 Add Device

1. On ZKBio CVSecurity, click **Access > Device Management > Device > Search > Search > Add** to add the device by searching. Then the device will be automatically synchronized to the **Video Intercom** module. (The adding method can refer to [17. Connect to ZKBio CVSecurity Software](#))



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

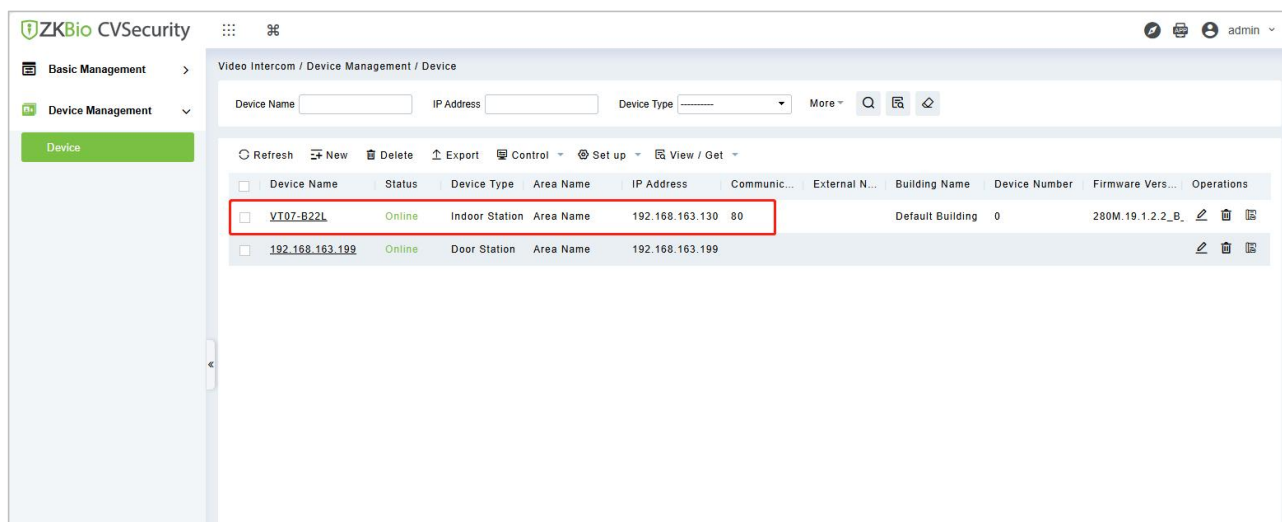




- **Device Name:** Enter the name of the indoor monitor.
- **Device Code:** Set as DNK.
- **IP Address:** Enter the IP address of the indoor monitor.
- Communication Port: 80 by default.
- Administrator Password: 123456 by default.
- **Device Type:** Set as Indoor Station.
- **Area/ Building Name/Unit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

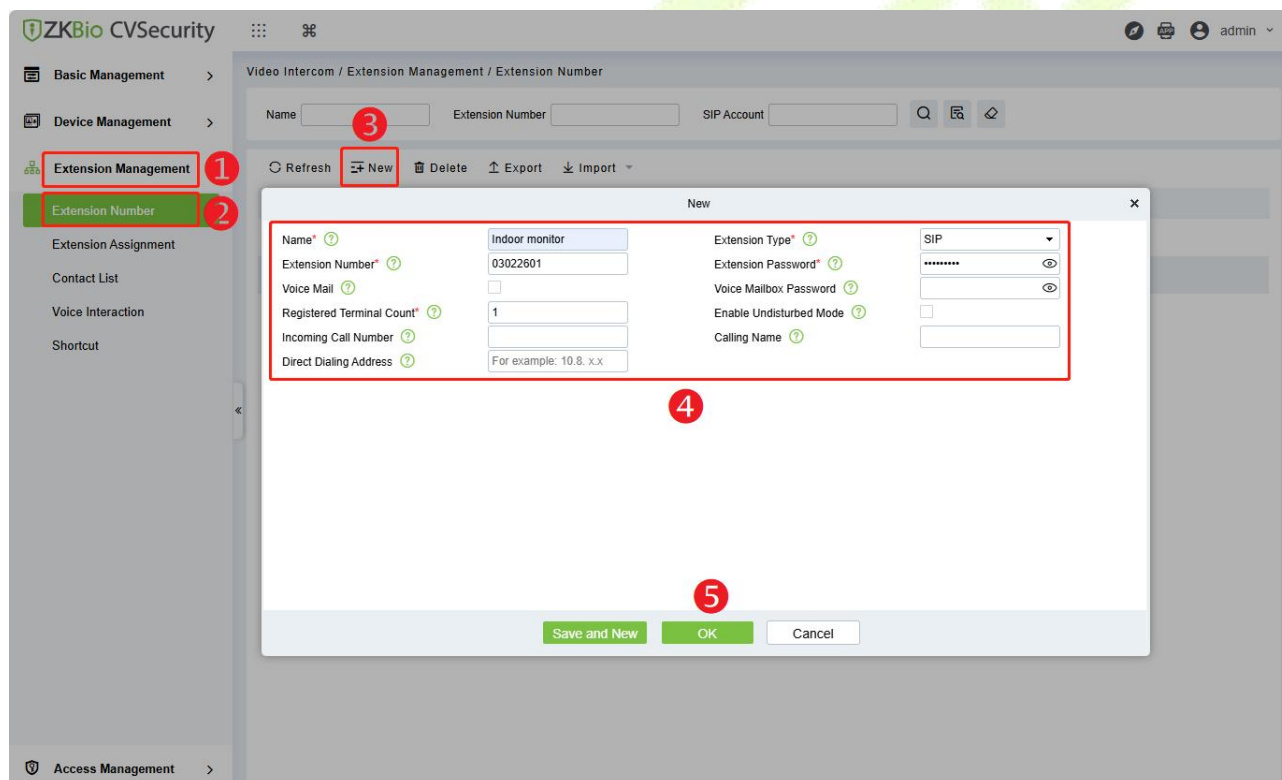
After the addition is successful, the indoor monitor will be displayed in the device list.





### 15.2.3 Create Extension Numbers

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



- **Name:** Customize the extension name. If it is a residential scene, the name can be set to the room number; if it is an office scene, the name can be set to the work number and name information.
- **Extension Type:** SIP by default.
- **Extension number:** Customize the extension number, it can be up to 8-digit; for example, the number of Room 401, Unit 2, Building 1 can be defined as 01020401 for quick internal identification.
- **Extension Password:** User's SIP account password, which can be used to request account registration from the SIP service.

- **Registered Terminal Count:** The maximum number of terminals that a user can register to the same number. When the number of concurrent registrations is 1, it means that new registrations are allowed to preempt the registration address. When the number of concurrent registrations is 2 or more, new registrations will be automatically blocked once the number of registrations reaches the limit.

After the user creates the extension number, the system will automatically generate a SIP account. For example, assuming the user has created the extension number 322603, the system automatically generates the SIP account as 678, so the SIP User Name used on the terminal is 678.

**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.

The screenshot shows the ZKBio CVSecurity web interface. On the left is a sidebar with navigation options: Basic Management, Device Management, and Extension Management (selected). Under Extension Management, there are sub-options: Extension Number (selected), Extension Assignment, Contact List, Voice Interaction, and Shortcut. The main content area is titled 'Video Intercom / Extension Management / Extension Number'. It features search filters for Name, Extension Number, and SIP Account. Below these are action buttons: Refresh, New, Delete, Export, and Import. A table lists extension entries with columns: Name, Extension Number, SIP Account, and Operations. The 'SIP Account' column is highlighted with a red box. A context menu is open over the 'Mick' row, with 'SIP Account' checked and highlighted by a red box.

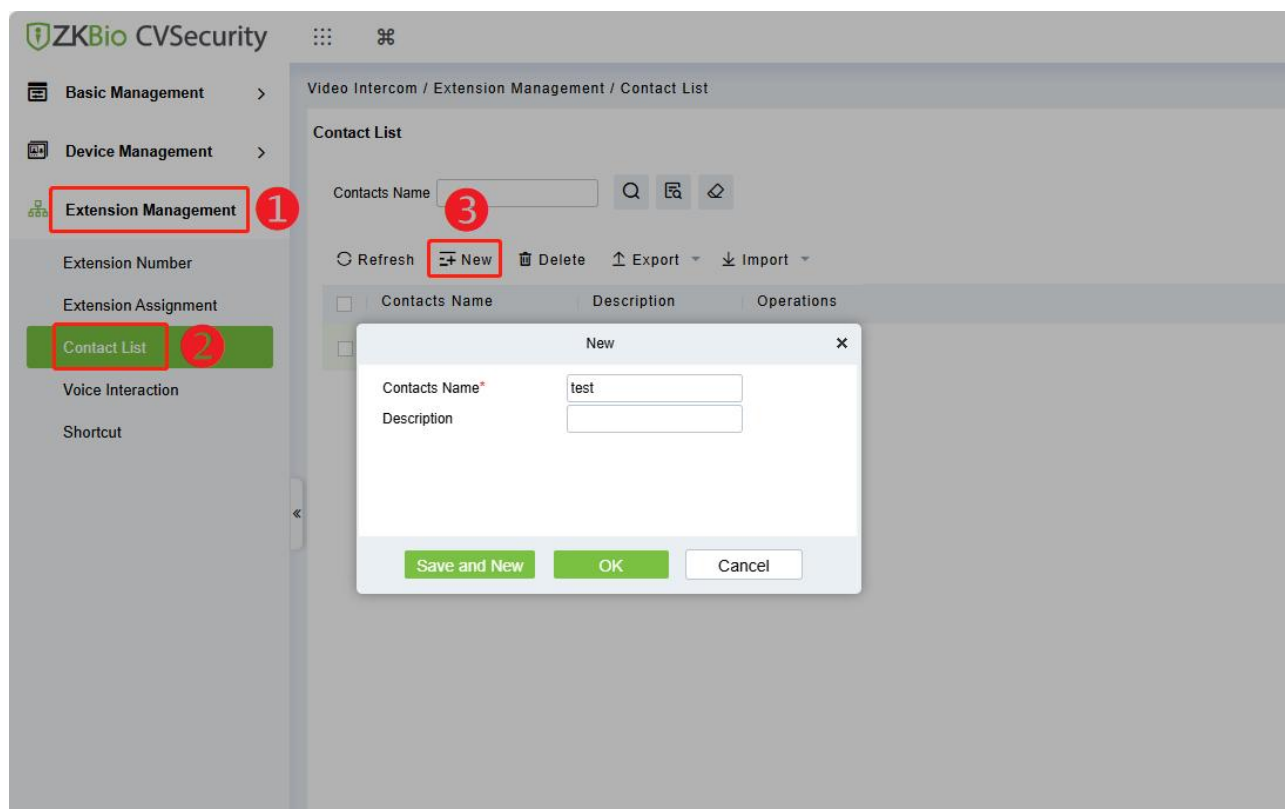
Name	Extension Number	SIP Account	Operations
Indoor monitor	03022601	717	[Edit] [Delete]
Mick	322604	679	[Edit] [Delete]
PC	322606	681	[Edit] [Delete]
ProFace X	322603	678	[Edit] [Delete]


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

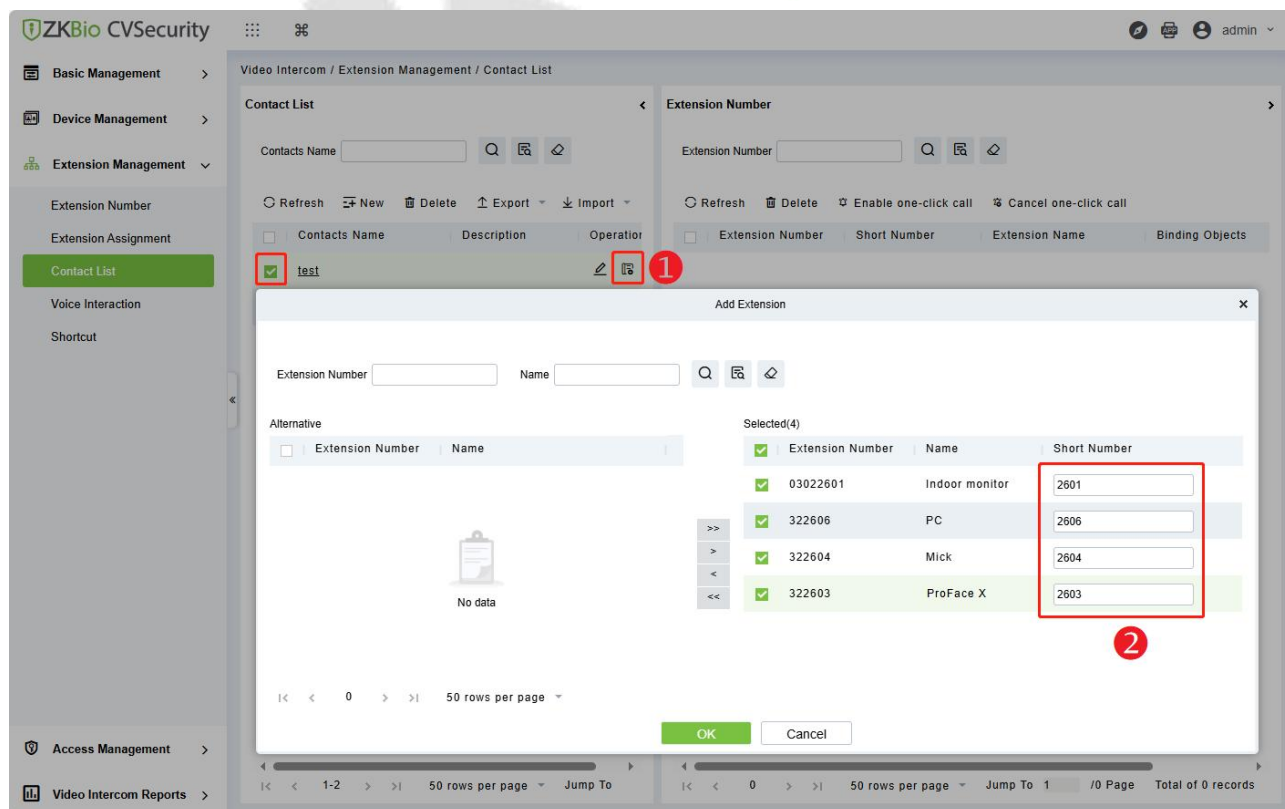
## 15.2.4 Contact List

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.



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



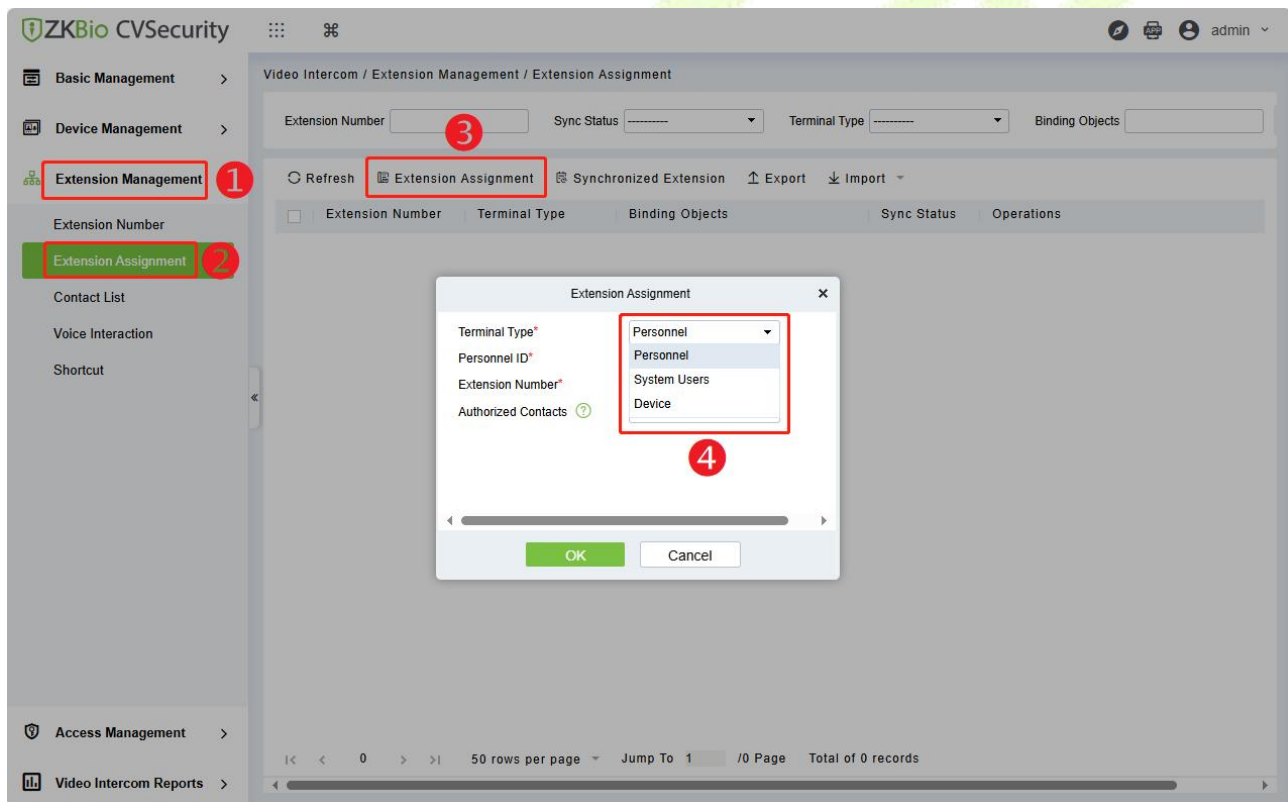
**Note:**

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

### 15.2.5 Assignment of Extension Numbers and SIP Accounts

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

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



#### ● Device Account Assignment

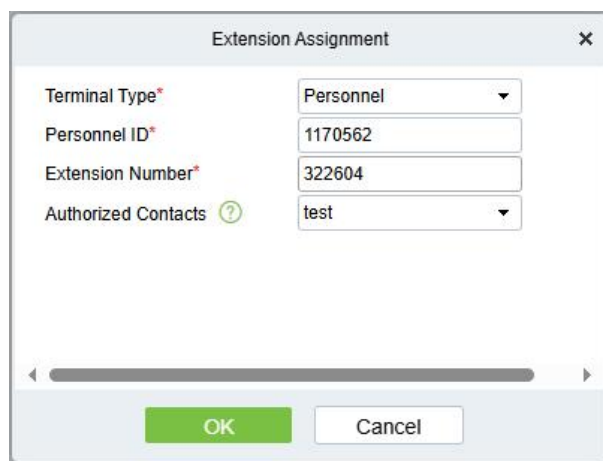
1. Select the Terminal Type as **Device**.
2. Select the device need to be bound (device or indoor monitor) and the extension number. The account information will be automatically synchronized to the device. Select the Authorized Contacts to assign the contact list to the device; only after the assignment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

3. After successful assignment, a green dot will appear in the upper right corner of the call page, indicates that the device is connected to the server. You can also enter **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 Settings	
Master Account Settings	<input checked="" type="checkbox"/>
Enable Domain Name	<input checked="" type="checkbox"/>
Server Address	zktecoiot.com
Server Port	5060
Display Name	322603
User Name	678
Verify ID	678
Password	*****
Network	
Transport Protocol	TLS

### ● **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

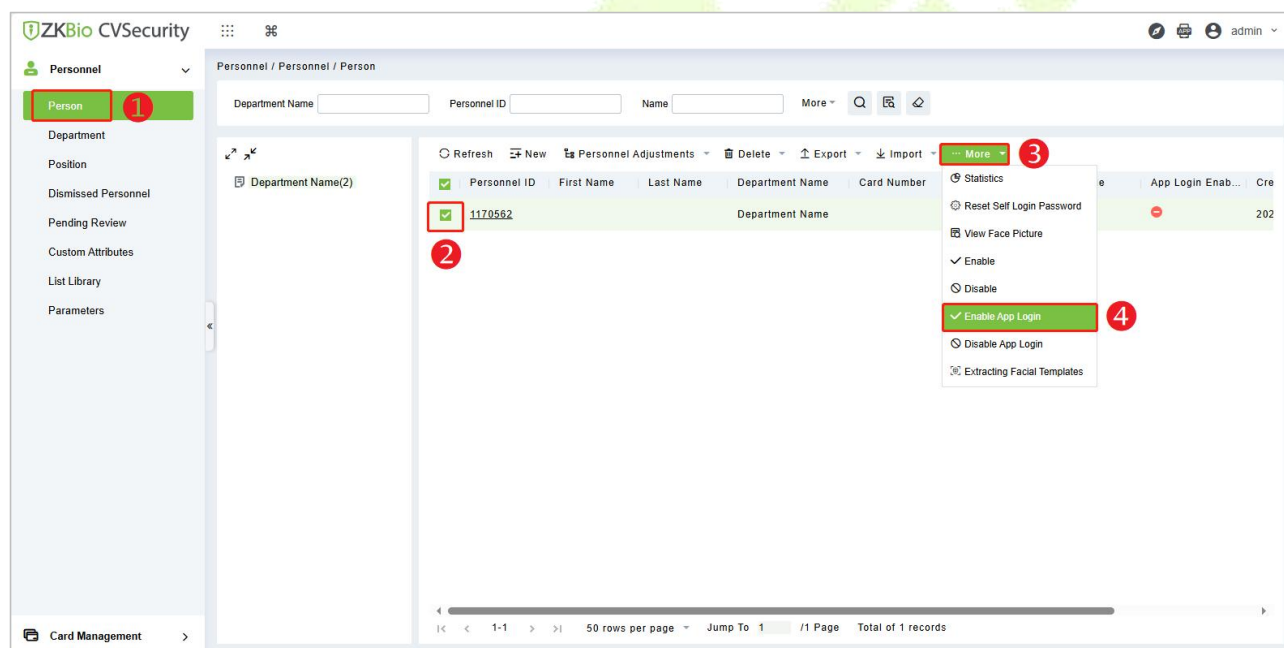
Extension Number\* 322604


Authorized Contacts ⓘ test

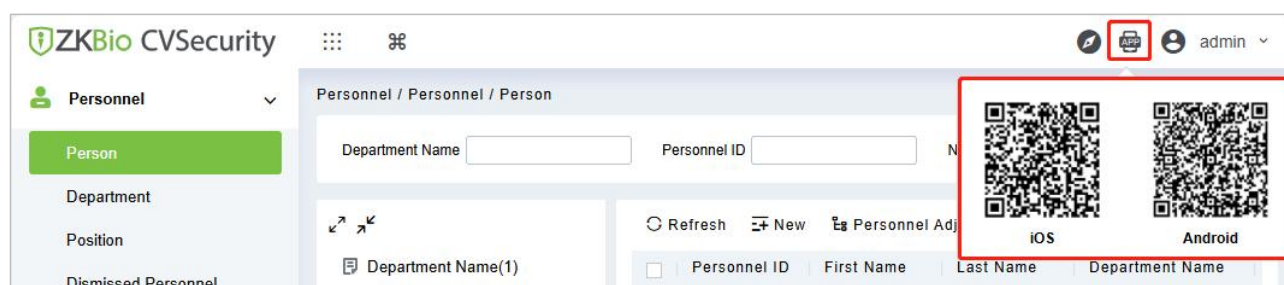
OK Cancel

**Note:**

- 1) Before assign account to the personnel, you need first add personnel in ZKBio CVSecurity. The adding method can refer to [17. Connect to ZKBio CVSecurity Software](#).
- 2) The personnel need to enable APP Login. (Click **Personnel** > **Personnel** > **Person** > **More** > **Enable APP Login**.) Once a person has enabled APP login, they can directly access the Video Intercom feature upon logging into the App.

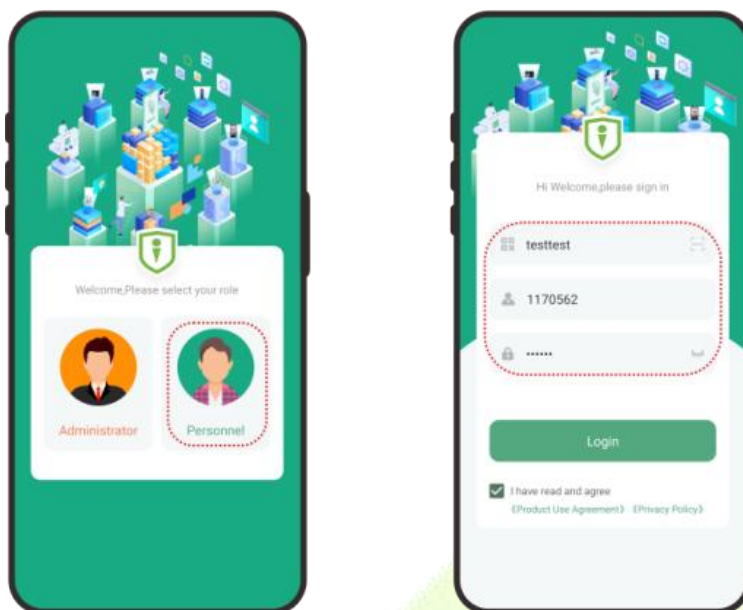


- 3) You can click the  icon at the right top corner of the ZKBio CVSecurity interface to scan the QR code to install the ZKBio Zexus App.



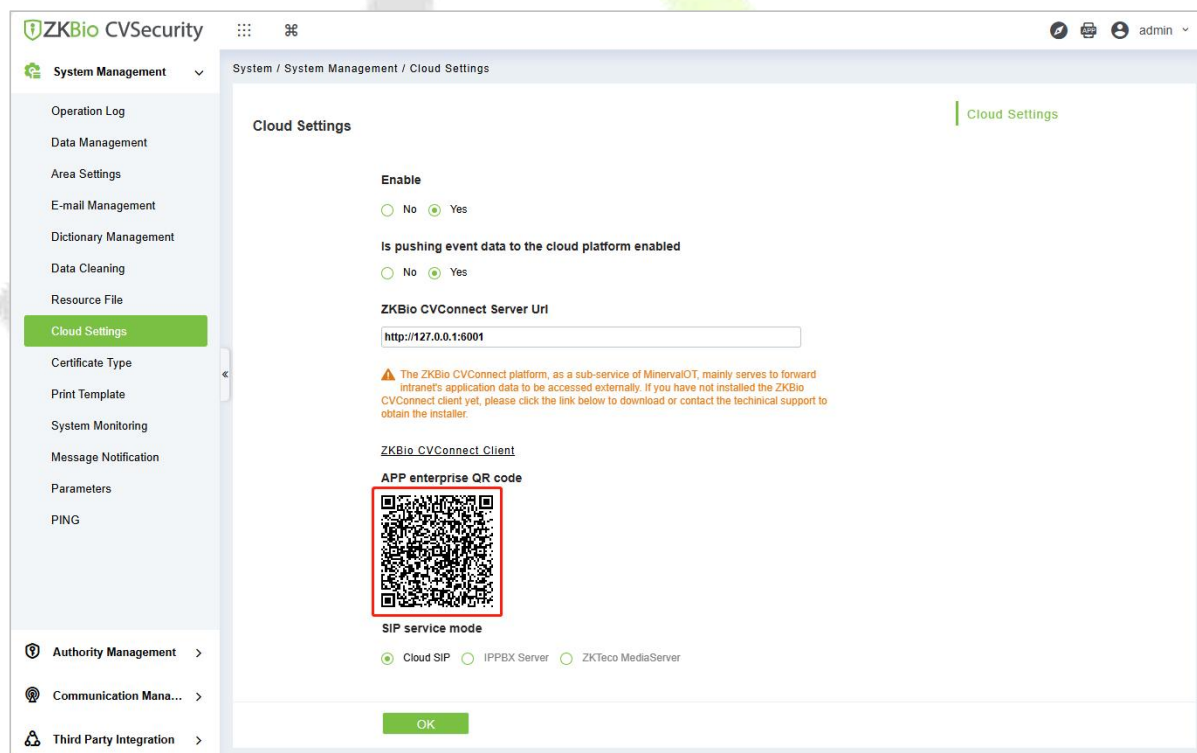


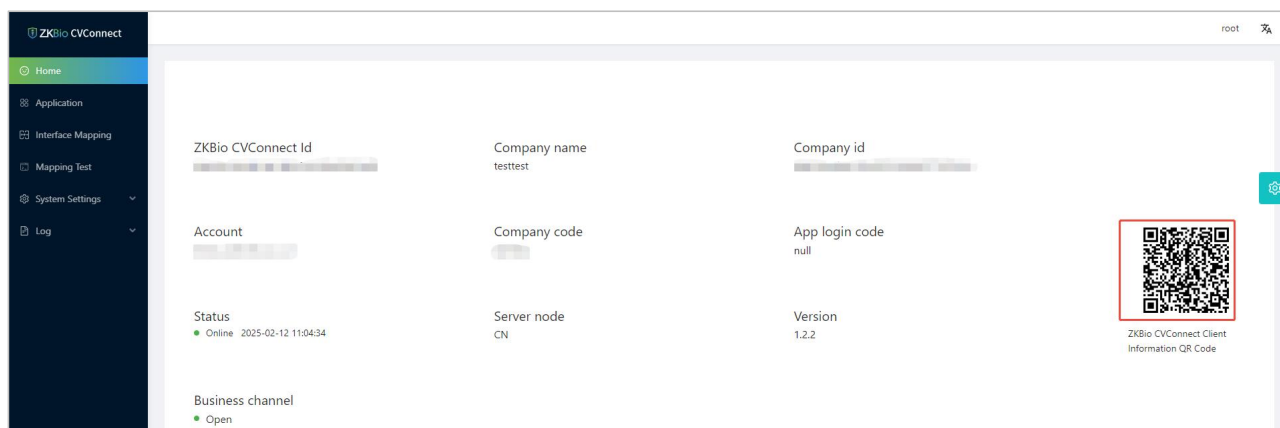
3. After successful assignment, the personnel can login to the App. Select the role-**Personnel** , enter the account information, and click **Login**.




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

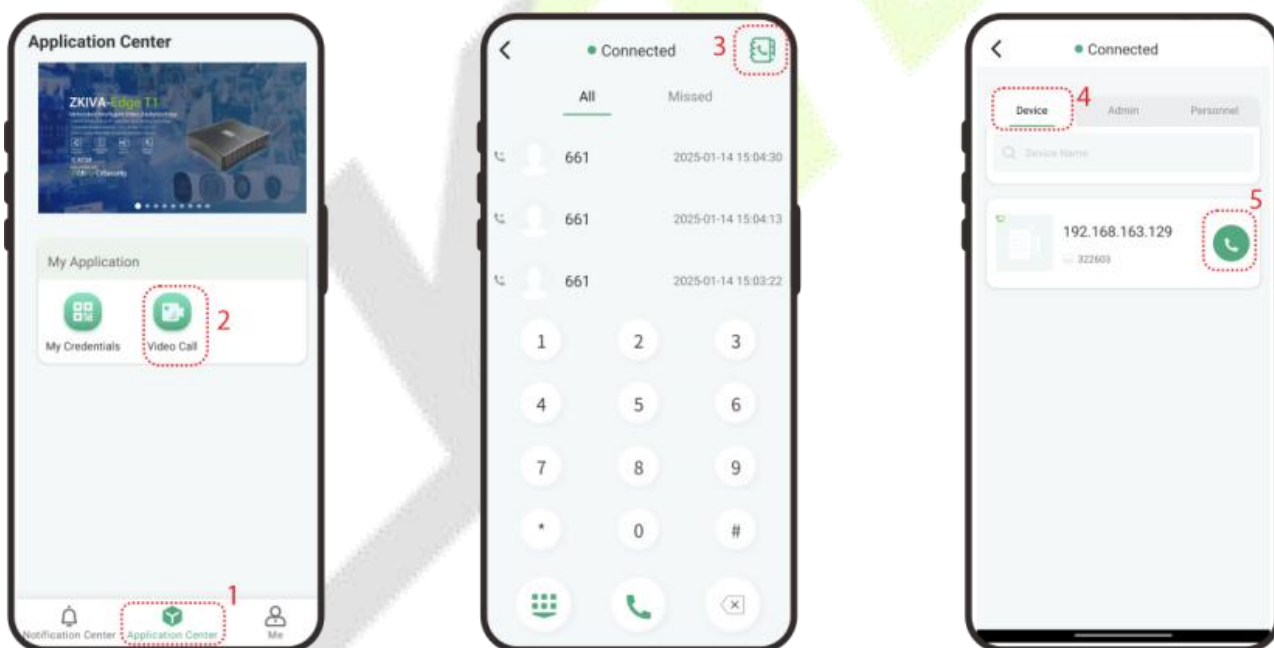
**Account & Password:** The personnel ID & password (default: 123456); Same account & password as ZKBio CVSecurity.





**Account & Password:** The personnel ID & password (default: **123456**); Same account & password as ZKBio CVSecurity.

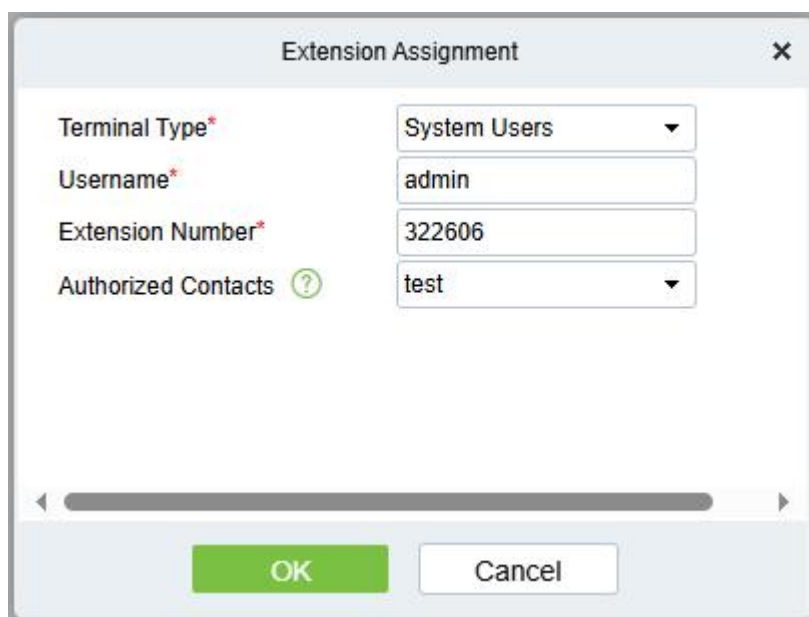
- Click **Application Center > Video Call** to enter the video call application, and the status will be displayed as **Connected**. If the person has not assigned an extension number, entering the application will prompt "you have not assigned an extension number, please contact the administrator". Then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



### ● **System User Account Assignment (ZKBio Zexus App)**

- Select the Terminal Type as **System Users**.
- 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.





The 'Extension Assignment' dialog box contains the following fields:

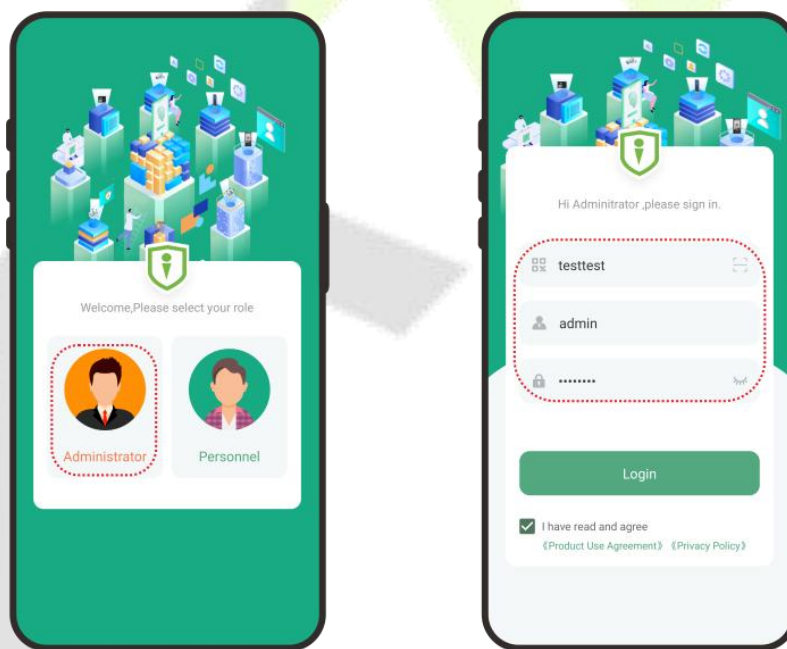
Field	Value
Terminal Type*	System Users
Username*	admin
Extension Number*	322606
Authorized Contacts ?	test


At the bottom, there are 'OK' and 'Cancel' buttons.

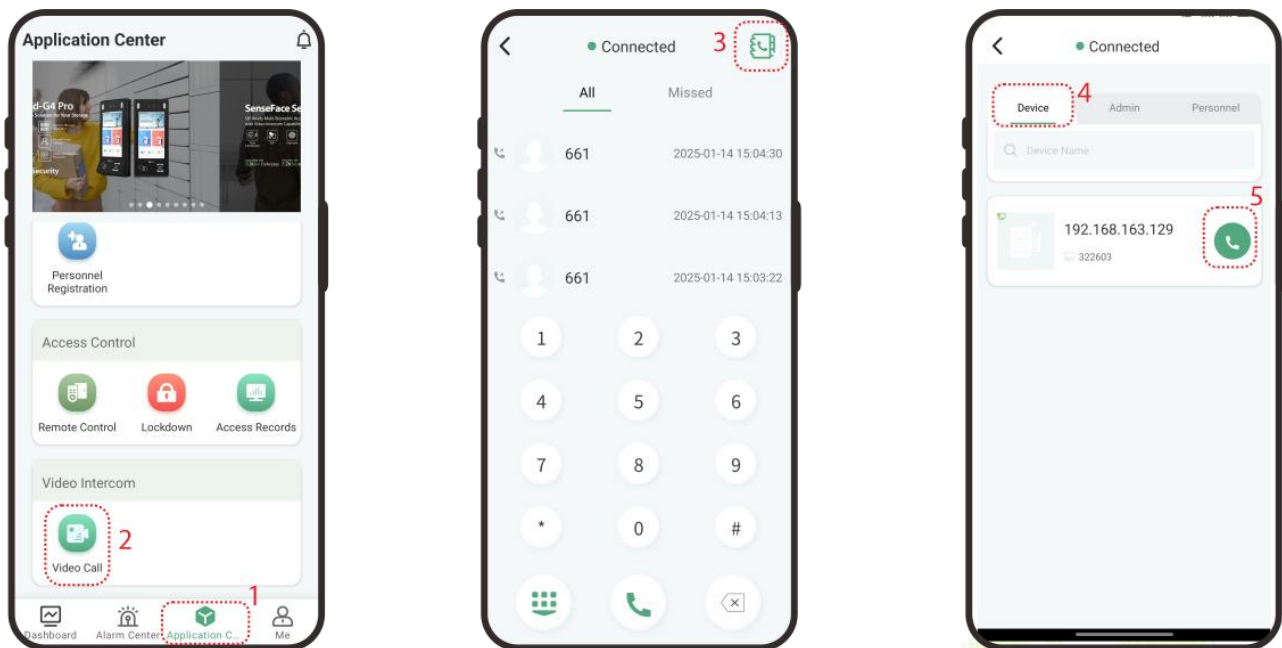
3. After successful assignment, the admin can login to the App. Select the role-**Administrator**, enter the account information, and click **Login**.

**Organization Name:** Scan the organization code you get before.

**Account & Password:** The administrator account; Same account & password as ZKBio CVSecurity.



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.



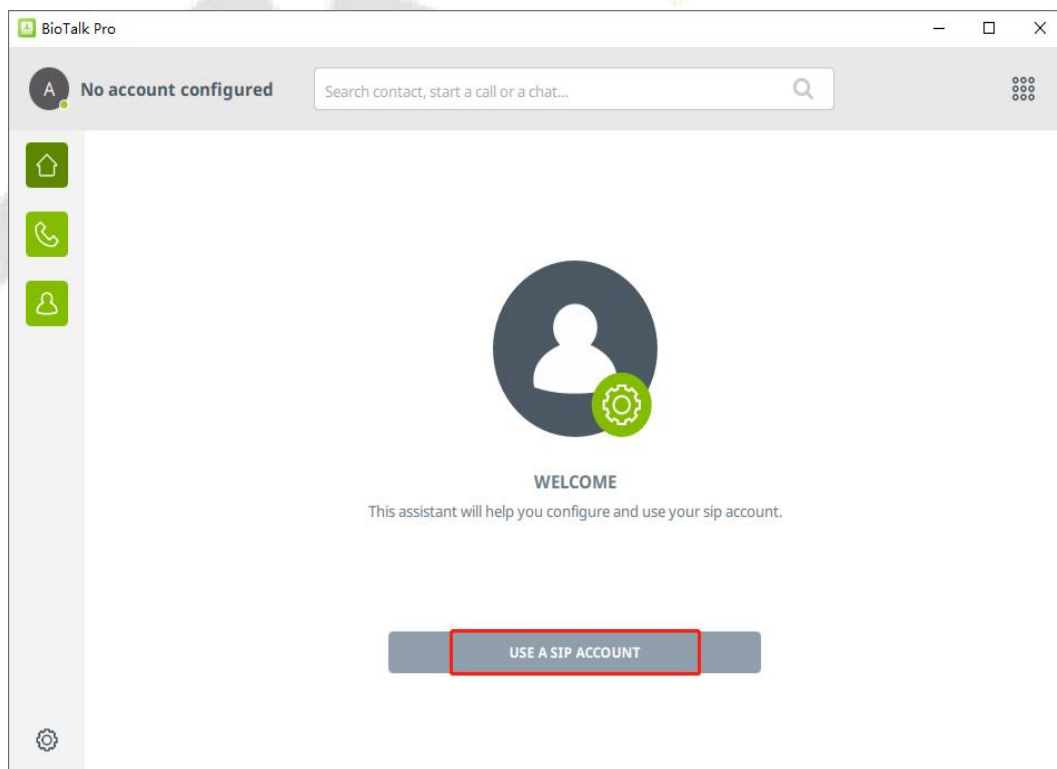
The App complete operation steps please refer to the ZKBio Zexus Mobile App User Manual.

## 15.2.6 PC Client Functionality

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

### Operation Guide

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



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

BioTalk Pro

No account configured

Search contact, start a call or a chat...

**USE A SIP ACCOUNT**

Username: 664

Display name (optional): 322606

SIP Domain: zktecoiot.com

Password: [Masked]

Transport: TLS

BACK USE

- **Username:** Enter the SIP account. (**Note:** You need to create a new SIP account for the PC client in ZKBio CVSecurity, 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 domain you need to enter on the PC Client.)

ZKBio CVConnect

Application

Minerva Credential Management

Minerva Organization

ZKBio CVConnect Client

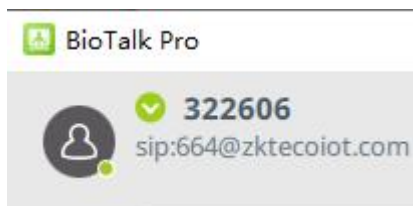
ZKBioCVAccess

Innosip

EndPoint: https://innosip.zktecoiot.com

- **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:

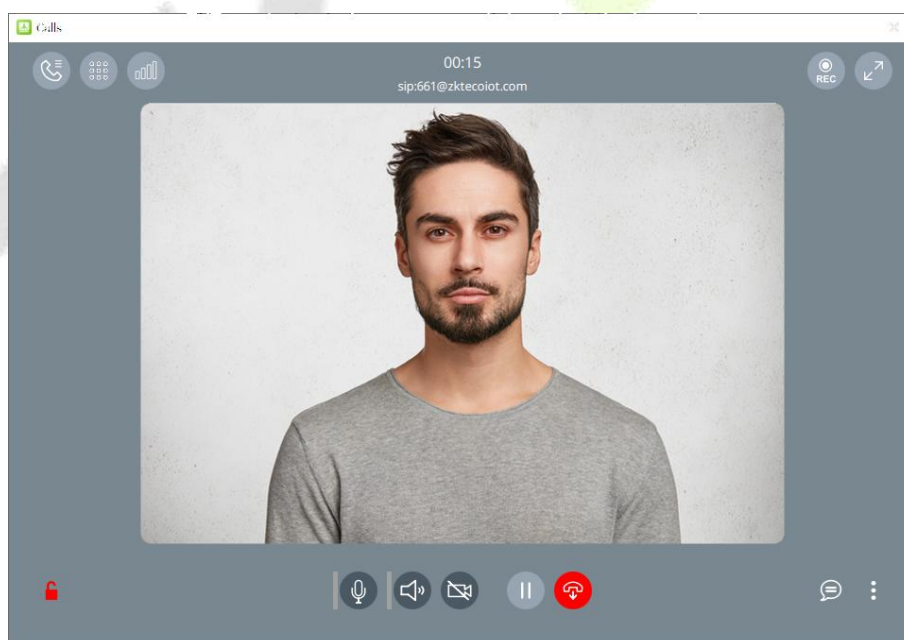


**Note:** In the Cloud SIP mode, if dialing is required, the PC Client should dial directly to the target SIP account. For example, if the extension number created on ZKBio CVSecurity is 322603, the corresponding generated SIP account is 661, then the PC Client should dial 661 when making a call. Therefore,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

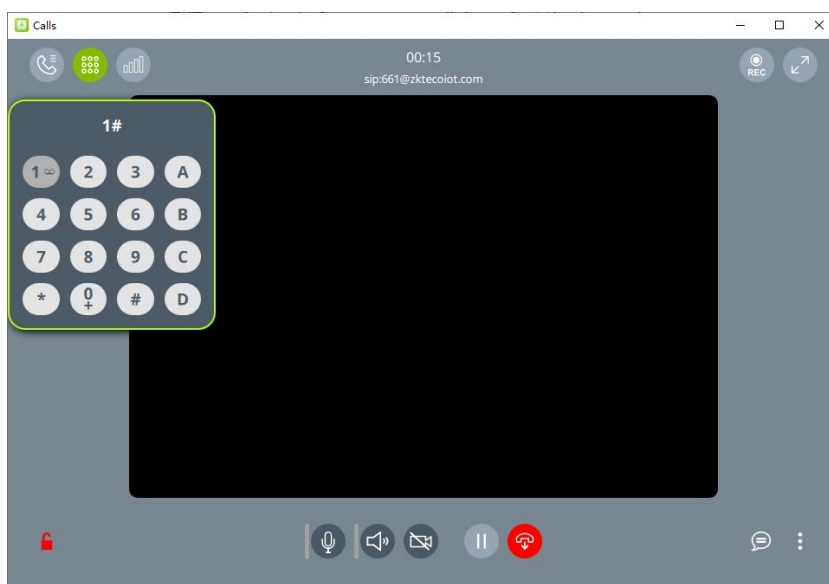
At this point you can start to use it normally, the PC client, the device and the App can call and answer each other.

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.

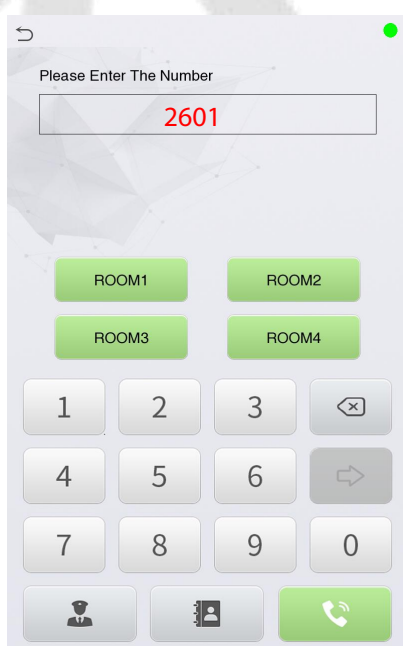


### 15.2.7 Make a Call

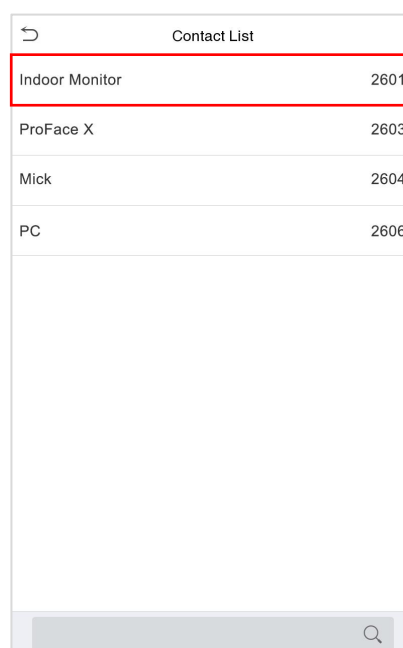
Two-way calls can be made between the device, indoor monitor, ZKBio Zexus App, and PC client (BioTalk Pro).

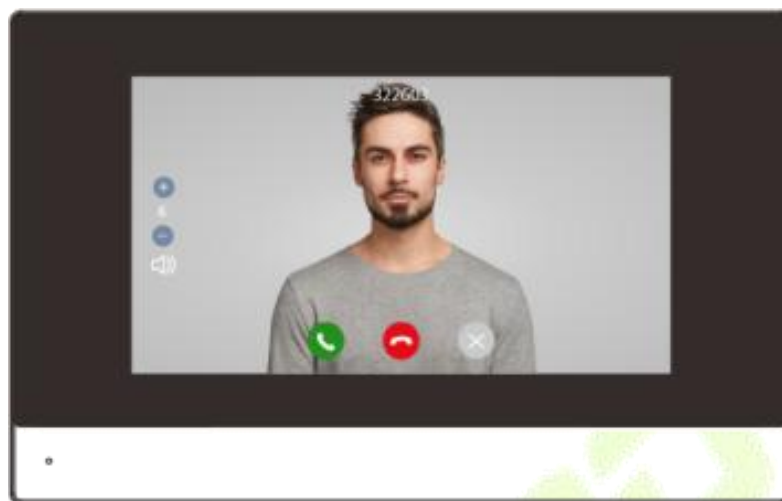
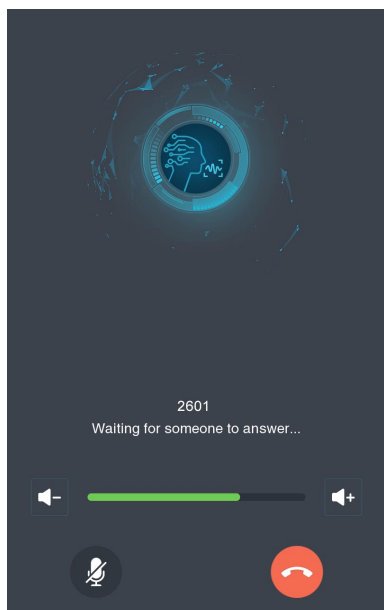
- **Device Call the Indoor Monitor (VT07-B26L-W / VT07-B22L)**

1. Add the indoor monitor on the ZKBio CVSecurity software, then assign an extension number to the indoor monitor. (The operations steps can refer to [15.2.2 Add Device](#) and [15.2.5 Assignment of Extension Numbers and SIP Accounts](#))
2. Click the icon  on the device and enter the Short Number of the indoor monitor in the pop-up interface of the device. Or click the  icon on the call page to open the contact list and search for the indoor monitor to call it.





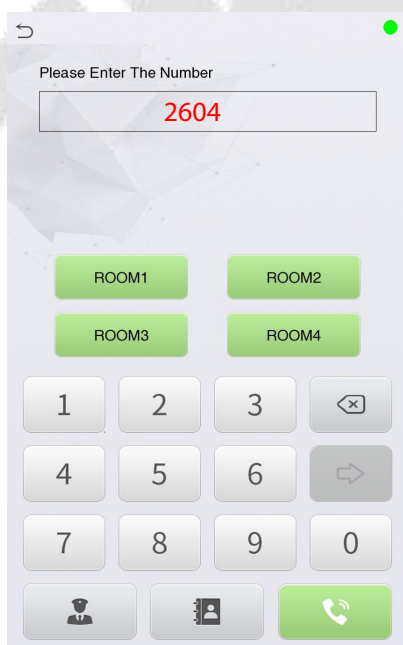
or



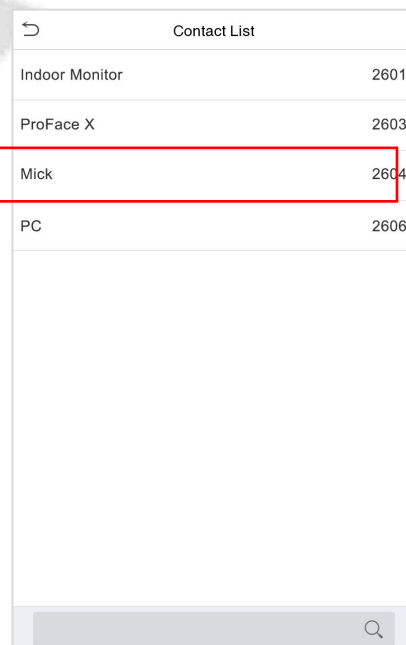


### ● **Device Call the Phone (ZKBio Zexus App)**

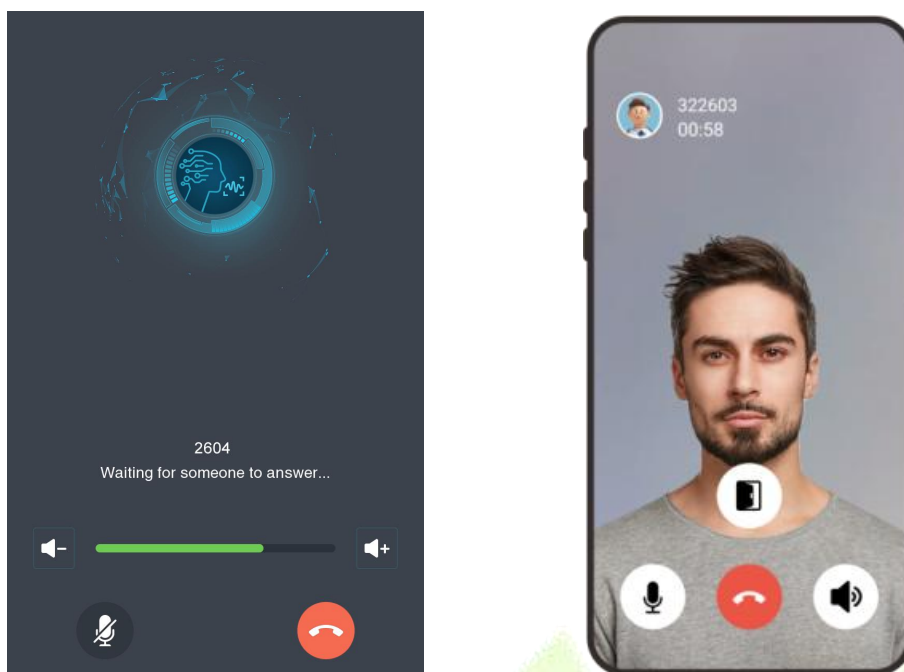
1. On the ZKBio CVSecurity software, assign an extension number to the personnel. (The operations steps can refer to [20.2.5 Assignment of Extension Numbers and SIP Accounts](#))
2. Click the icon  on the device and enter the Short Number of the personnel in the pop-up interface of the device. Or click the  icon on the call page to open the contact list and search for the personnel to call him/her.





or

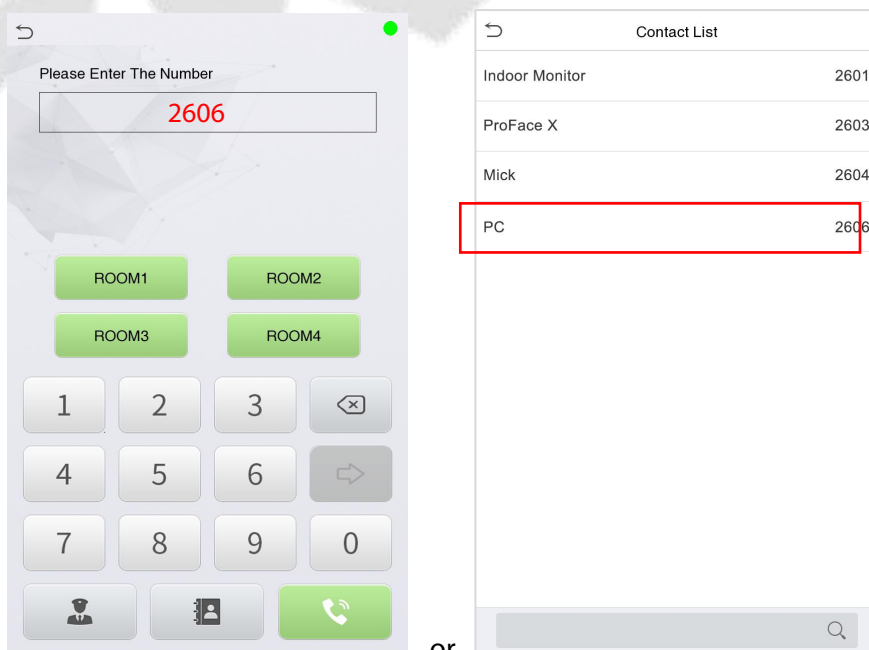




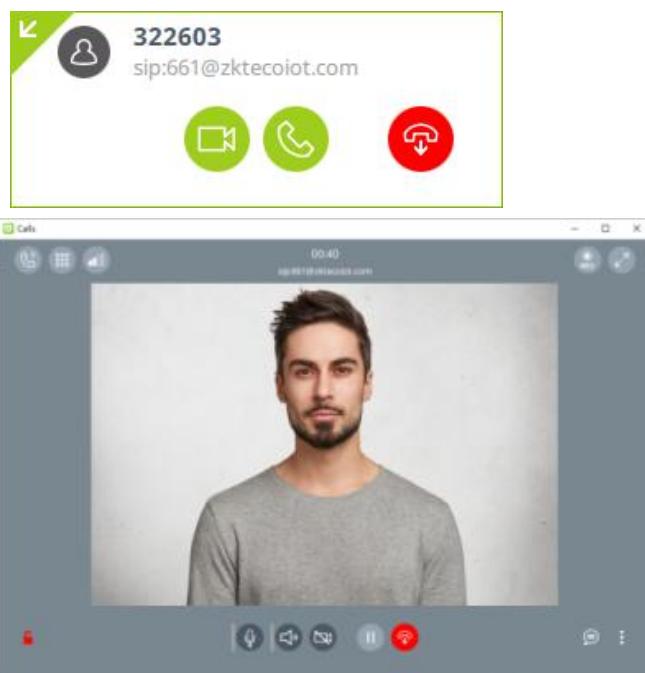
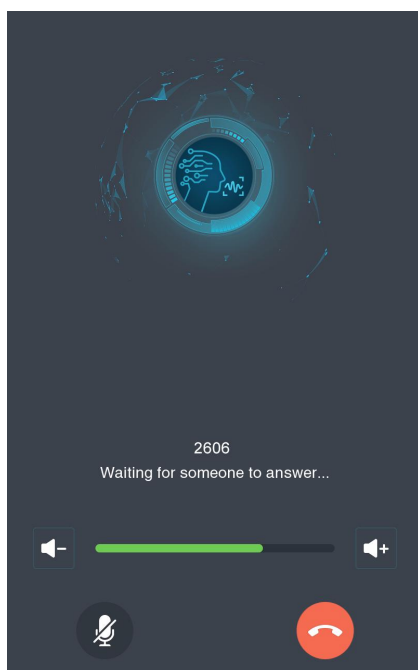


### ● **Device Call the PC Client (BioTalk Pro)**

1. Install the BioTalk Pro software and configure the SIP account. (The operations steps can refer to [20.2.6 PC Client Functionality](#))
2. Click the icon  on the device and enter the Short Number of the PC client in the pop-up interface of the device. Or click the  icon on the call page to open the contact list and search for the PC client to call it.

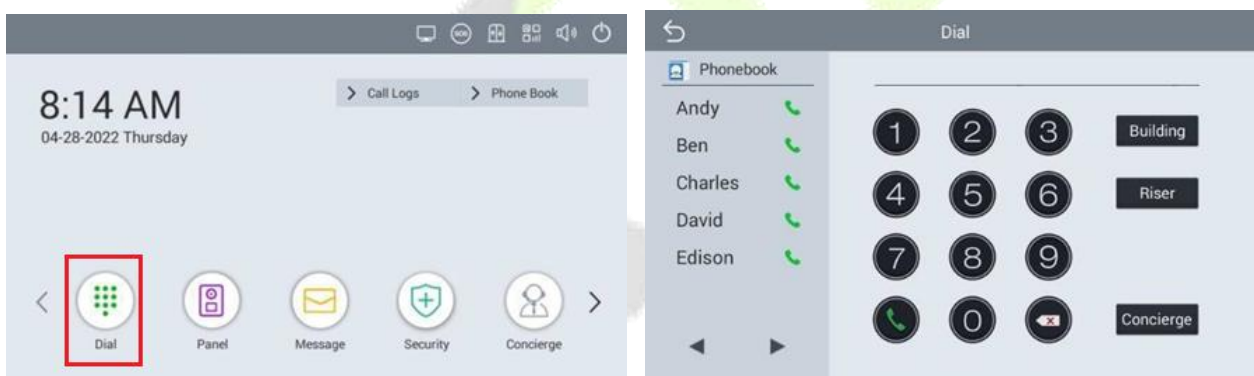


or




### ● **Indoor Monitor Call**

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

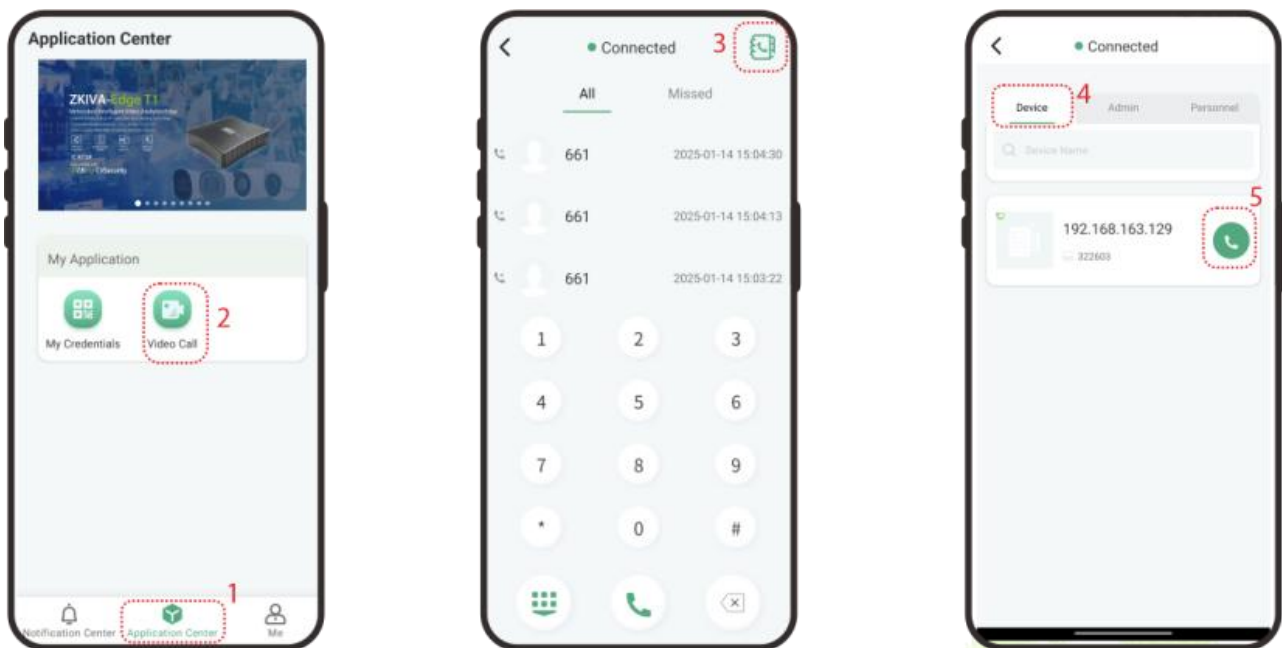


**Note:** The indoor monitor is not supported the assignment of the contact list in ZKBio CVSecurity.

### ● **Phone Call**

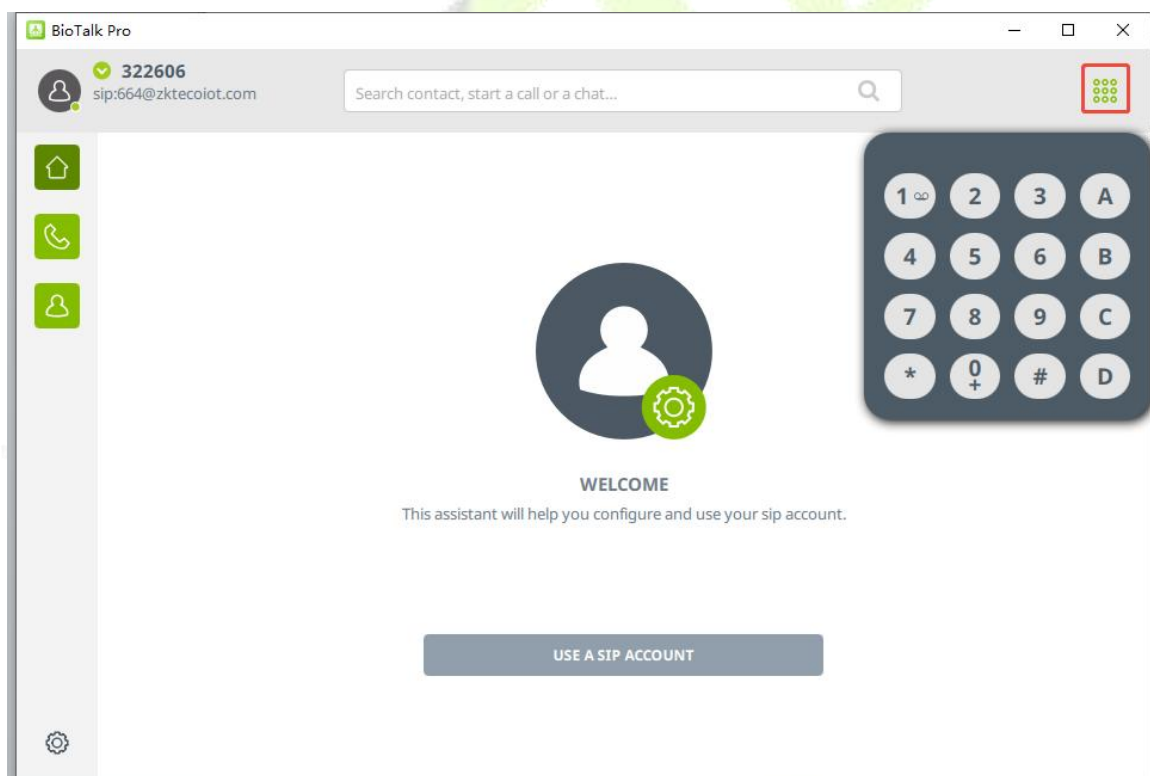
Login to the ZKBio Zexus App, click **Application Center > Video Call** to enter the video call application, Then you can directly enter the extension number or click the  icon to search for the one you want to call.



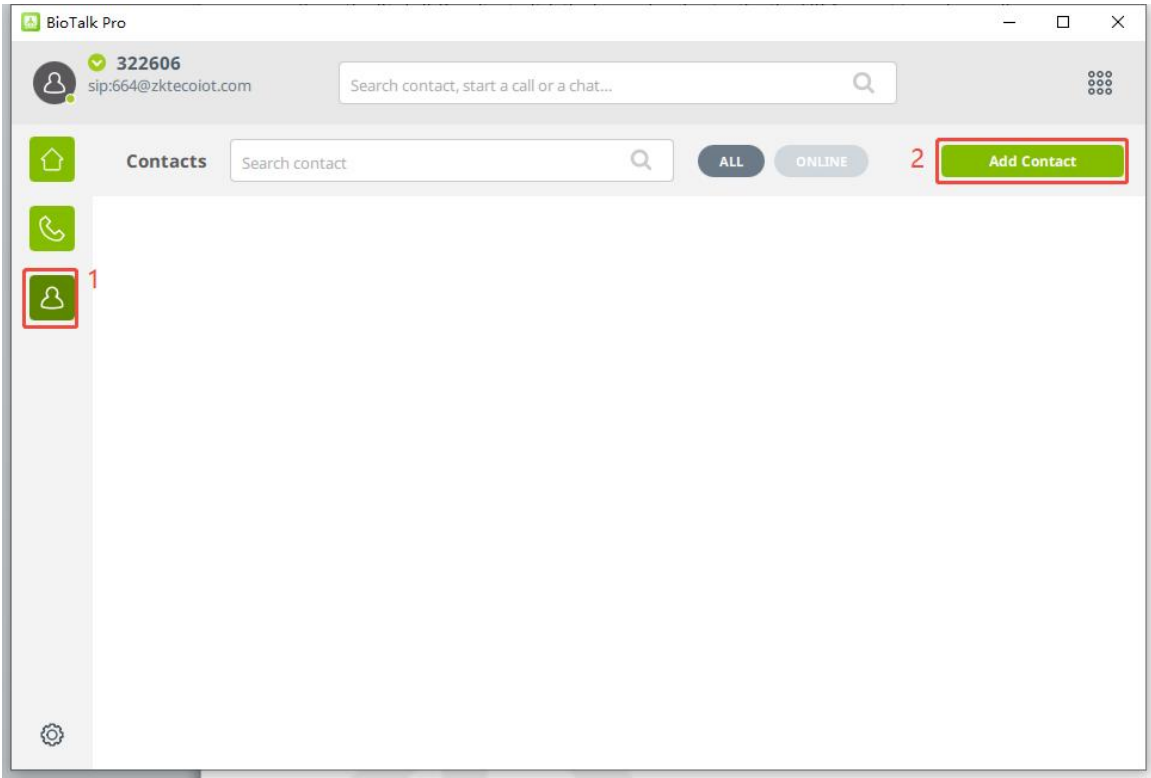


### ● PC Client (BioTalk Pro) Call

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



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



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



## Requirements for Visible Light Digital Face Template Data

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

- **Eye distance**

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

- **Facial expression**

Neutral face template or smile with eyes naturally open are recommended.

- **Gesture and angel**

Horizontal rotating angle should not exceed  $\pm 10^\circ$ , elevation should not exceed  $\pm 10^\circ$ , and depression angle should not exceed  $\pm 10^\circ$ .

- **Accessories**

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

- **Face template**

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

- **Template format**

Should be in BMP, JPG or JPEG.

- **Data requirement**

Should comply with the following requirements:

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

## Appendix 2

### Privacy Policy

#### Notice:

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

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

#### I. Collected Information

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

- 1. User Registration Information:** At your first registration, the feature template (**Fingerprint template/Face template 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

- 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).**
- 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](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](http://www.zkteco.com)



Copyright © 2025 ZKTECO CO., LTD. All Rights Reserved.