

# User Manual

## BioFace D1

Next-Gen Access Control Terminal- High  
Capacity Edition (V2.0)

Date: August 2025

Doc Version: 1.1

English

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



For further details, please visit our Company's website  
[www.zkteco.com](http://www.zkteco.com).

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

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

## Trademark

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

## Disclaimer

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

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

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

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

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

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

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

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

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

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

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

## ZKTeco Headquarters

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

**Phone** +86 769 - 82109991

**Fax** +86 755 - 89602394

For business related queries, please write to us at: [sales@zkteco.com](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 **BioFace D1**.

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 FINGER POSITIONING .....	11
1.2 STANDING POSITION, POSTURE AND FACIAL EXPRESSION .....	11
1.3 FACE TEMPLATE REGISTRATION .....	12
1.4 STANDBY INTERFACE .....	13
1.5 VIRTUAL KEYBOARD .....	14
1.6 VERIFICATION MODE .....	15
1.6.1 FINGERPRINT VERIFICATION ★ .....	15
1.6.2 QR CODE VERIFICATION ★ .....	17
1.6.3 CARD VERIFICATION .....	18
1.6.4 FACIAL VERIFICATION .....	20
1.6.5 PASSWORD VERIFICATION .....	22
1.6.6 COMBINED VERIFICATION .....	24
<b>2. OVERVIEW .....</b>	<b>25</b>
2.1 APPEARANCE .....	25
2.2 TERMINAL AND WIRING DESCRIPTION .....	27
2.3 WIRING DESCRIPTION .....	27
2.3.1 POWER CONNECTION .....	27
2.3.2 ETHERNET CONNECTION .....	28
2.3.3 EXIT BUTTON, DOOR SENSOR & AUXILIARY CONNECTION .....	28
2.3.4 RS485 CONNECTION .....	29
2.3.5 LOCK RELAY CONNECTION .....	29
2.3.6 WIEGAND READER CONNECTION .....	30
<b>3. INSTALLATION .....</b>	<b>31</b>
3.1 INSTALLATION ENVIRONMENT .....	31
3.2 DEVICE INSTALLATION .....	31
<b>4. MAIN MENU .....</b>	<b>32</b>
<b>5. USER MANAGEMENT .....</b>	<b>34</b>
5.1 USER REGISTRATION .....	34
5.1.1 USER ID AND NAME .....	34
5.1.2 USER ROLE .....	35
5.1.3 FINGERPRINT ★ .....	36
5.1.4 FACE TEMPLATE .....	36
5.1.5 CARD .....	37
5.1.6 PASSWORD .....	38
5.1.7 PROFILE PHOTO .....	38
5.1.8 ACCESS CONTROL ROLE .....	39
5.2 SEARCH FOR USERS .....	40

5.3 EDIT USER.....	40
5.4 DELETE USER.....	41
5.5 DISPLAY STYLE .....	41
<b>6. USER ROLE .....</b>	<b>43</b>
<b>7. COMMUNICATION SETTINGS .....</b>	<b>45</b>
7.1 NETWORK SETTINGS .....	45
7.2 SERIAL COMM.....	46
7.3 PC CONNECTION.....	47
7.4 WIRELESS NETWORK★ .....	48
7.5 CLOUD SERVER SETTING .....	51
7.6 WIEGAND SETUP .....	51
7.6.1 WIEGAND INPUT .....	52
7.6.2 WIEGAND OUTPUT .....	54
7.7 NETWORK DIAGNOSIS .....	55
<b>8. SYSTEM SETTINGS .....</b>	<b>56</b>
8.1 DATE AND TIME .....	56
8.2 ACCESS LOGS SETTINGS .....	58
8.3 FACE TEMPLATE PARAMETERS.....	59
8.4 FINGERPRINT PARAMETERS★ .....	61
8.5 DEVICE TYPE SETTING .....	62
8.6 SECURITY SETTING .....	62
8.7 USB UPGRADE.....	63
8.8 UPDATE FIRMWARE ONLINE.....	64
8.9 FACTORY RESET .....	65
<b>9. PERSONALIZE SETTINGS .....</b>	<b>66</b>
9.1 USER INTERFACE SETTINGS.....	66
9.2 VOICE SETTINGS.....	67
9.3 BELL SCHEDULES .....	68
<b>10. DATA MANAGEMENT .....</b>	<b>70</b>
10.1 DELETE DATA .....	70
<b>11. INTERCOM.....</b>	<b>72</b>
11.1 SIP SETTINGS .....	72
11.1.1 LOCAL SETTINGS .....	73
11.1.2 AUDIO OPTIONS .....	74
11.1.3 VIDEO OPTIONS.....	74
11.1.4 CALL OPTIONS .....	75
11.1.5 CONTACT LIST.....	76
11.1.6 CALLING SHORTCUT SETTINGS.....	78
11.1.7 ADVANCED SETTINGS .....	79
11.2 DOORBELL SETTING .....	80
11.2.1 CONNECT THE WIRELESS DOORBELL ★ .....	80
11.3 ONVIF SETTINGS.....	81



<b>12. ACCESS CONTROL .....</b>	<b>84</b>
12.1 ACCESS CONTROL OPTIONS .....	85
12.2 TIME RULE SETTING .....	86
12.3 HOLIDAYS .....	88
12.4 ACCESS GROUPS ★ .....	89
12.5 COMBINED VERIFICATION .....	90
12.6 ANTI-PASSBACK SETUP .....	91
12.7 DURESS OPTIONS .....	92
<b>13. USB MANAGER .....</b>	<b>94</b>
13.1 USB DOWNLOAD .....	94
13.2 USB UPLOAD .....	95
<b>14. ATTENDANCE SEARCH .....</b>	<b>96</b>
<b>15. AUTOTEST .....</b>	<b>98</b>
<b>16. SYSTEM INFORMATION .....</b>	<b>99</b>
<b>17. CONNECT TO ZKBIO CVSECURITY SOFTWARE .....</b>	<b>100</b>
17.1 SET THE COMMUNICATION ADDRESS .....	100
17.2 ADD DEVICE ON THE SOFTWARE .....	101
17.3 ADD PERSONNEL ON THE SOFTWARE AND ONLINE FINGERPRINT/FACE REGISTRATION .....	102
<b>18. CONNECT TO ZKBIOTIME SOFTWARE .....</b>	<b>105</b>
18.1 SET THE COMMUNICATION ADDRESS .....	105
18.2 ADD DEVICE ON THE SOFTWARE .....	105
18.3 ADD PERSONNEL ON THE SOFTWARE AND ONLINE FINGERPRINT REGISTRATION .....	106
<b>19. CONNECTING TO WIRELESS DOORBELL ★ .....</b>	<b>108</b>
19.1 CONNECT THE WIRELESS DOORBELL .....	108
19.2 UNBINDING THE WIRELESS DOORBELL .....	108
<b>20. SIP VIDEO INTERCOM .....</b>	<b>109</b>
20.1 LOCAL AREA NETWORK USE .....	109
20.1.1 CALL CONTACT LIST .....	114
20.1.2 CUSTOM THE CALLING SHORTCUT KEYS .....	115
20.1.3 DIRECT CALLING .....	116
20.2 SIP SERVER .....	117
20.2.1 SIP SERVER CONFIGURATION .....	118
20.2.2 ADD DEVICE .....	121
20.2.3 CREATE EXTENSION NUMBERS .....	123
20.2.4 CONTACT LIST .....	124
20.2.5 ASSIGNMENT OF EXTENSION NUMBERS AND SIP ACCOUNTS .....	126
20.2.6 PC CLIENT FUNCTIONALITY .....	132
20.2.7 MAKE A CALL .....	135
<b>21. CONNECTING TO ZKBIO ZLINK MOBILE APP .....</b>	<b>143</b>



21.1 LOGIN TO THE MOBILE APP ..... 143

21.2 ADD DEVICE ON THE MOBILE APP ..... 144

    21.2.1 VIDEO INTERCOM..... 145

**22. CONNECTING TO ZKBIO ZLINK WEB PORTAL .....151**

    22.1 LOGIN TO THE WEB PORTAL..... 151

    22.2 ADD DEVICE ON THE WEB PORTAL ..... 151

**APPENDIX 1 ..... 154**

    REQUIREMENTS OF LIVE COLLECTION AND REGISTRATION OF VISIBLE LIGHT FACE TEMPLATES..... 154

    REQUIREMENTS FOR VISIBLE LIGHT DIGITAL FACE TEMPLATE DATA ..... 155

**APPENDIX 2 ..... 156**

    PRIVACY POLICY ..... 156

    ECO-FRIENDLY OPERATION ..... 158

## 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. Please do not use any other components other than manufacturer suggested materials.
4. **Precautions for the installation** - Do not place this device on an unstable stand or frame. It may fall and cause serious injury to persons and damage to the device.
5. **Service** - Do not try to service this unit yourself. Opening or removing covers may expose you to hazardous voltages or other hazards.
6. **Damage requiring service** - Disconnect the system from the 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 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 operating instructions.

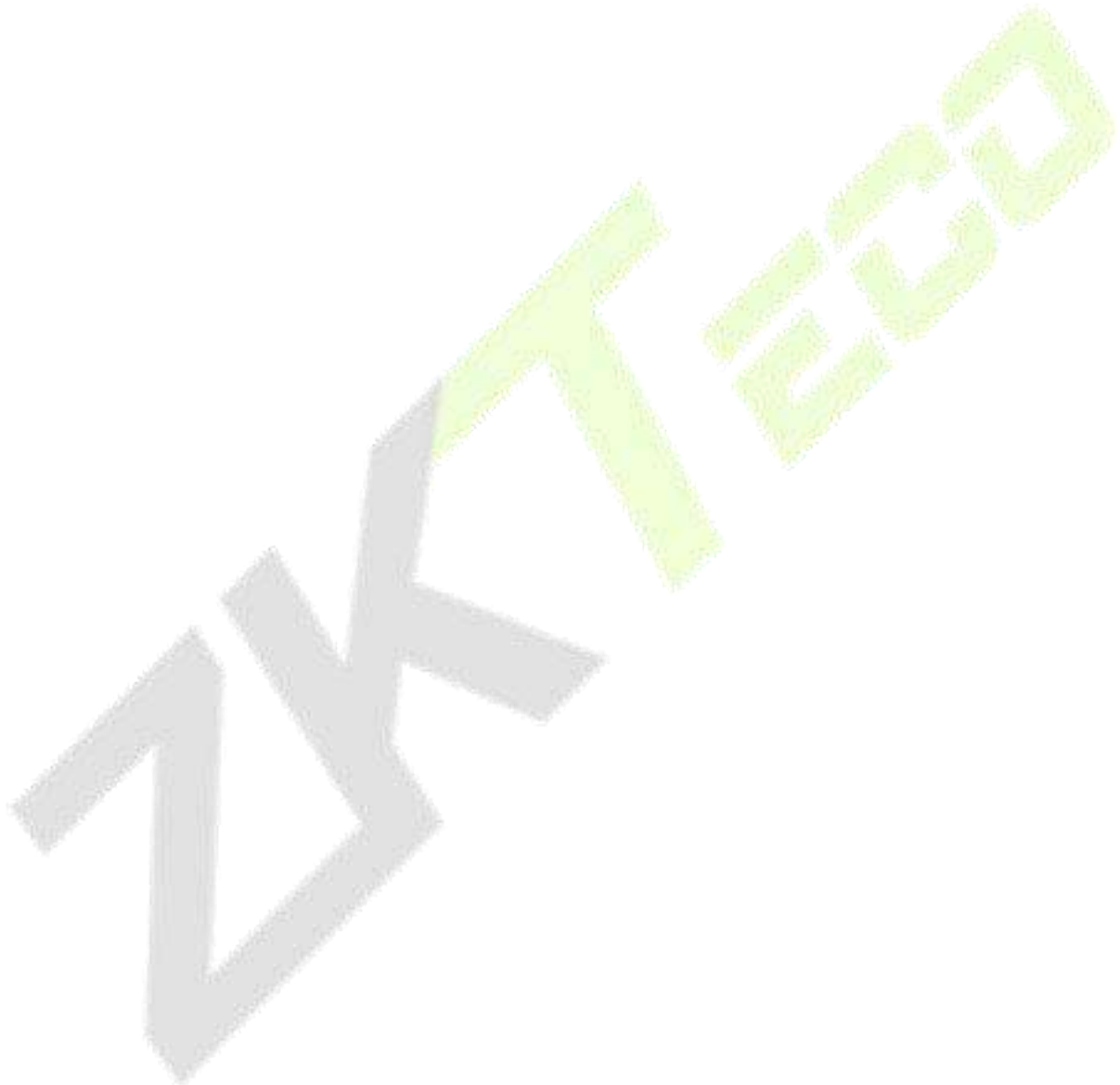
Just change controls defined in operating instructions. Improper adjustment of other controls may result in damage and involve a qualified technician to return the device to normal operation.

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** - Can install external lightning conductors to protect against electrical storms. It stops power-ups destroying the system.

The devices should be installed in areas with limited access.

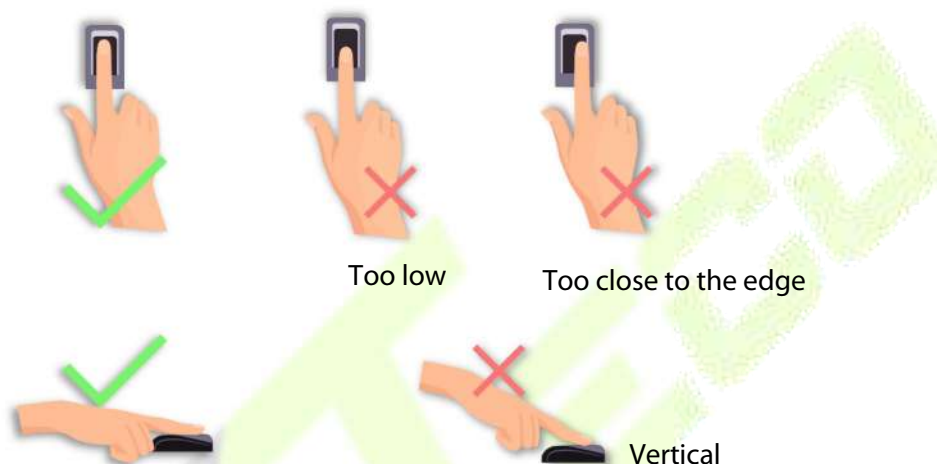


## 1. Instruction for Use

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

### 1.1 Finger Positioning

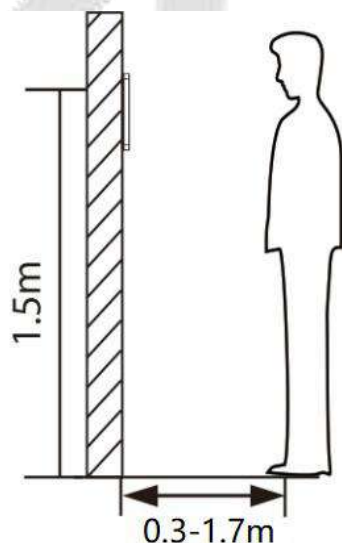
**Recommended fingers:** The index, middle, or ring fingers are recommended fingers to use, and avoid using the thumb or pinky, as they are difficult to position correctly onto the fingerprint reader.



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

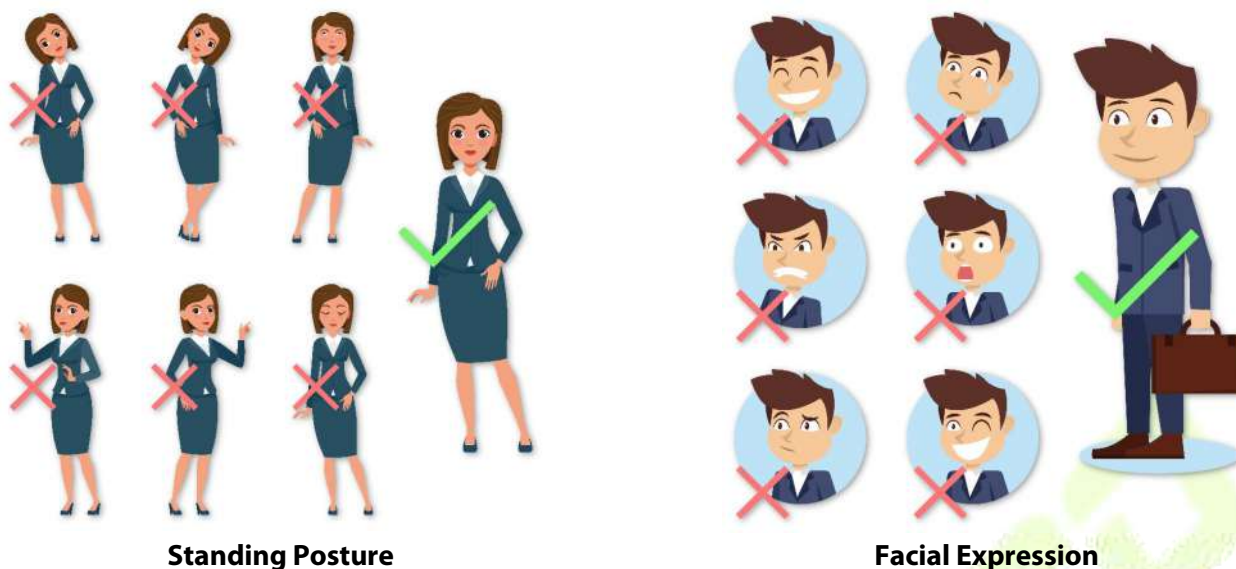
### 1.2 Standing Position, Posture and Facial Expression

- **The recommended distance**



The distance between the device and a user whose height is in a range of 1.55 m to 1.85 m is recommended to be 0.3 m to 1.7 m. Users may slightly move forward or backward to improve the quality of facial images captured.

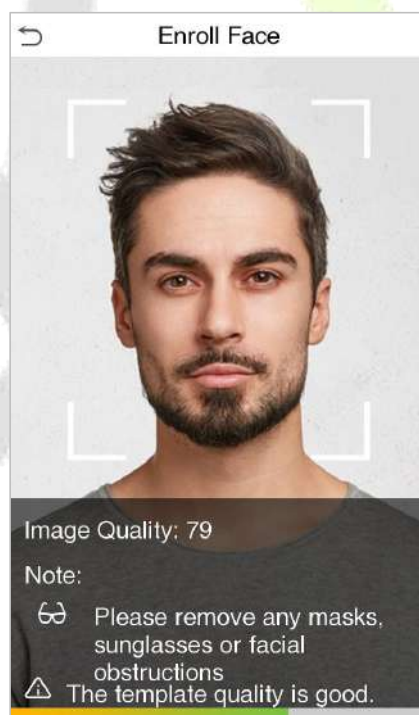
- **Recommended standing posture and facial expression:**



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

### 1.3 Face Template Registration

Please make sure that the face template is in the centre 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

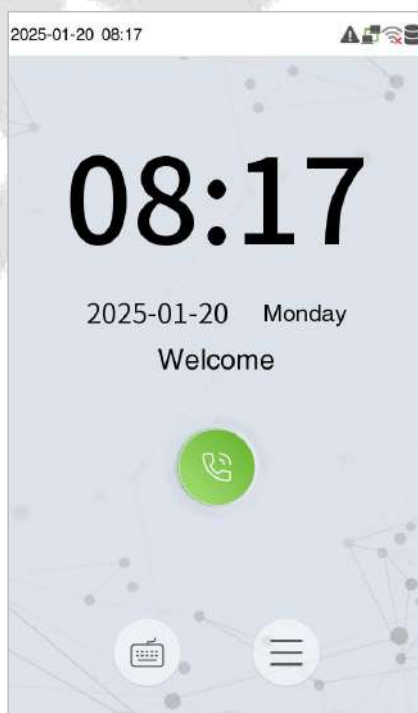
- **Recommendation for Registering a Face Template**

- 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.

## 1.4 Standby Interface

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

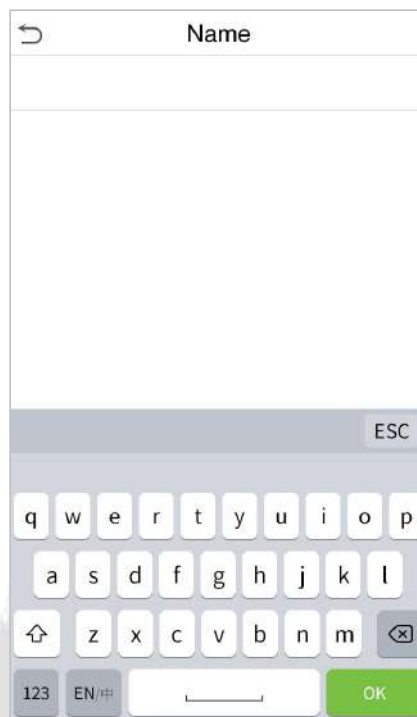




- Click  icon to enter the User ID input interface template.
- When there is no Super Administrator set in the device, tap  icon to go to the menu.
- After setting the Super Administrator on the device, it requires the Super Administrator's verification before entering the menu functions.

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

## 1.5 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.



## 1.6 Verification Mode

### 1.6.1 Fingerprint Verification★

**Note:** This function is only for BioFace D1.

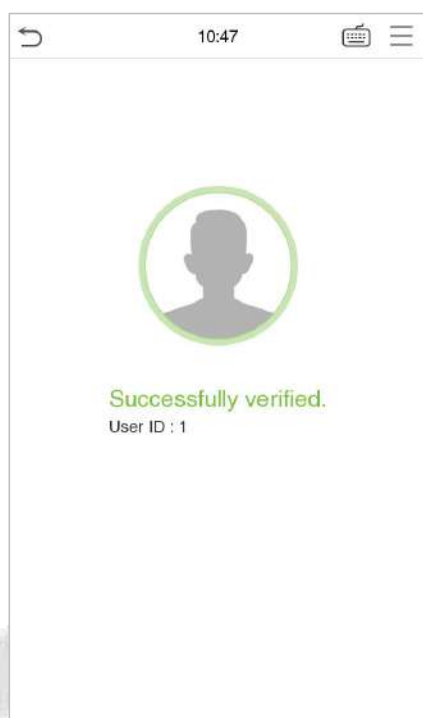
#### ● 1: N Fingerprint Verification Mode

The device compares the current fingerprint with the available fingerprint data stored in its database.

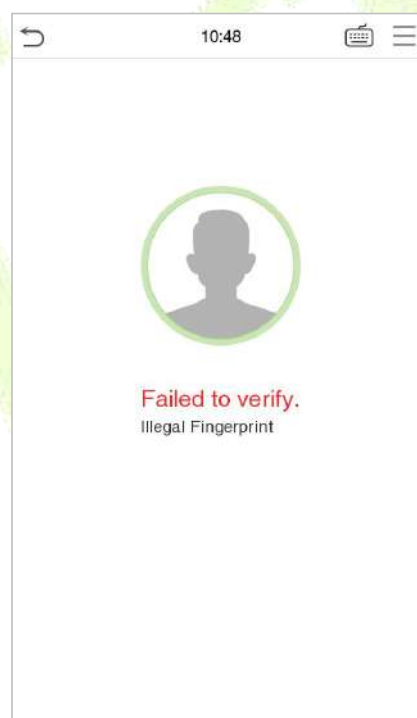
Fingerprint authentication mode is activated when a user places their finger onto the fingerprint scanner.

Please follow the recommended way to place your finger onto the sensor. For details, please refer to section [Finger Positioning](#).

Verification is successful:




Verification is failed:



#### ● 1: 1 Fingerprint Verification Mode


The device compares the current fingerprint with the fingerprints linked to the entered User ID through the virtual keyboard

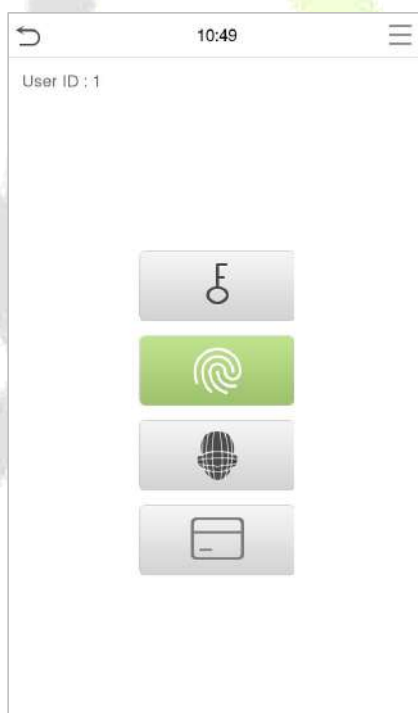
In case users are unable to gain access using the 1:N authentication method, they can attempt to verify their identity using the 1:1 verification mode.

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

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

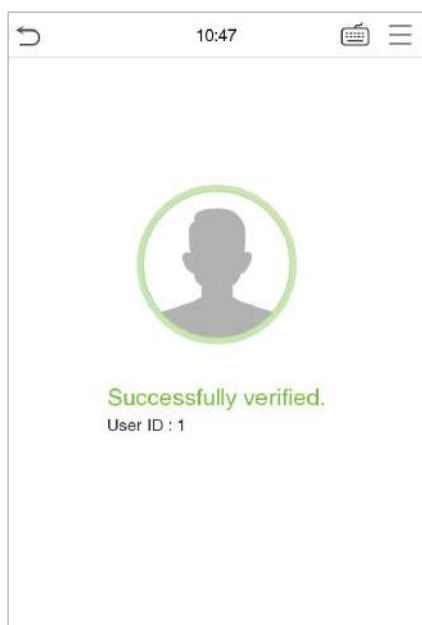


If the user has registered face template, card and password in addition to his/her fingerprints and the verification method is set to Password/Fingerprint/Card/Face template verification, the following screen will appear. Select the fingerprint icon to  enter fingerprint verification mode.

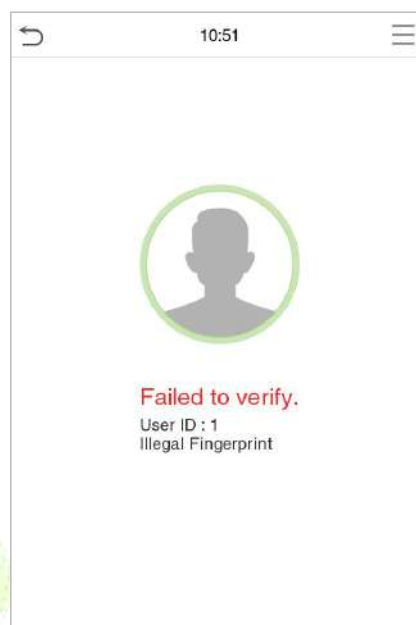


Press the fingerprint to verify.

Verification is successful:



Verification is failed:



## 1.6.2 QR Code Verification ★

**Note:** This function is only for BioFace D1.

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

Tap **Mobile Credential** on the ZKBioAccess Mobile Page, and a QR code will appear, which includes employee ID and card number (static QR code only includes card number) information. The QR code can replace a physical card on a specific device to achieve contactless authentication. Please refer to [15.4 Mobile Credential](#).

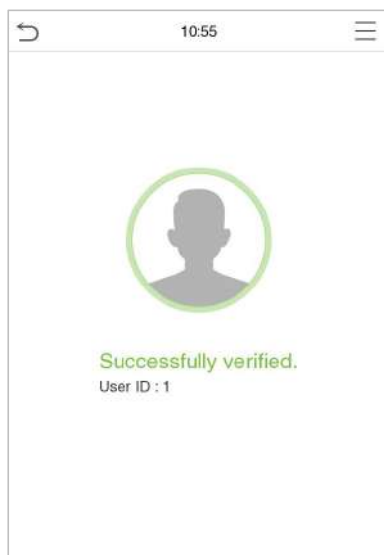


## 1.6.3 Card Verification

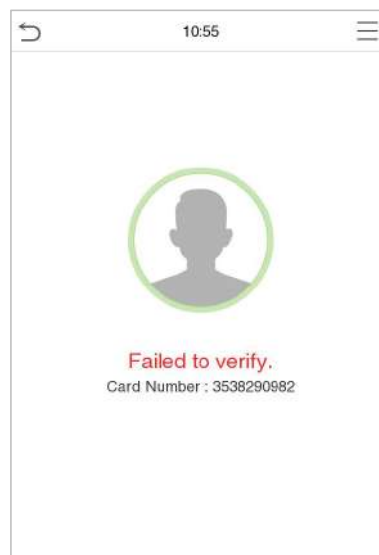
### ● 1:N Card Verification

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 is failed:

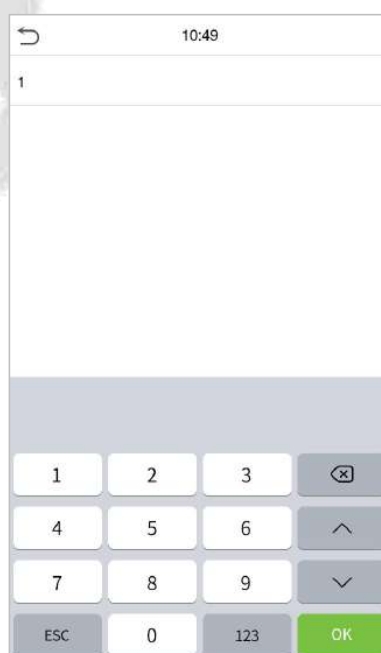



### ● 1:1 Card Verification

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**.

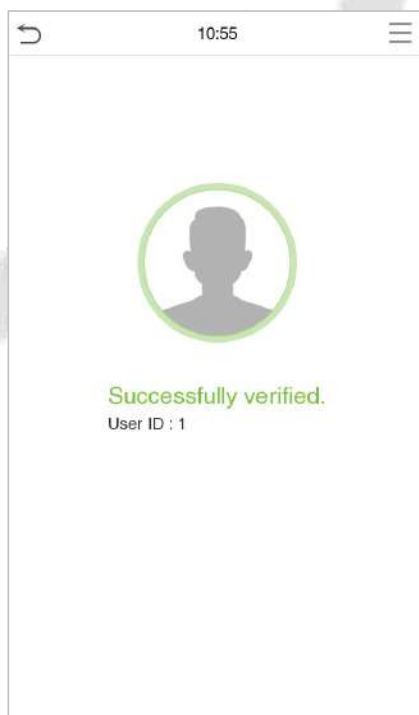


If the user has registered face template, card and password in addition to his/her card, and the verification method is set to Password/Fingerprint/Card/Face verification, the following screen will appear. Select the  icon to enter the card verification mode.

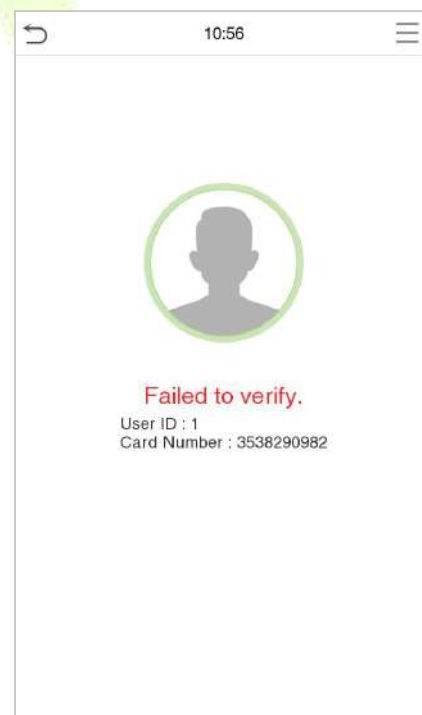


Place the card in the collection area for verification.

Verification is successful:



Verification is failed:



## 1.6.4 Facial Verification

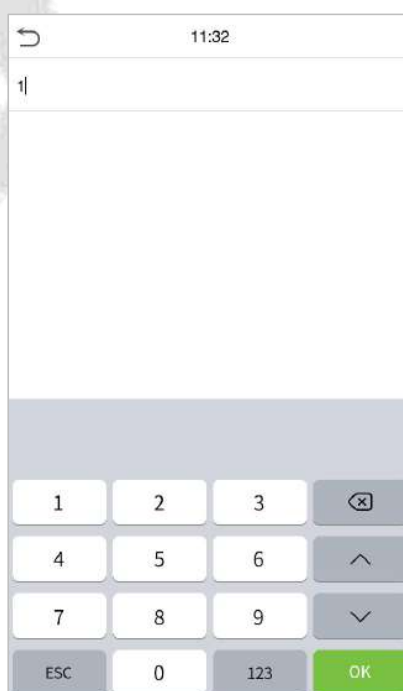
### ● 1:N Facial Verification


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 card, fingerprint and password in addition to his/her face template, and the verification method is set to Password/Fingerprint/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:




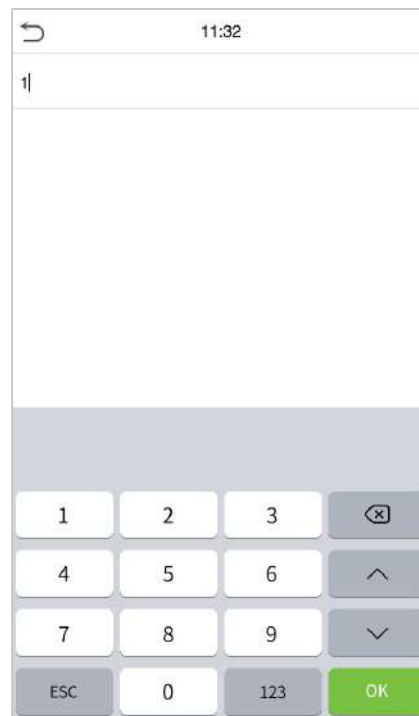
If the verification is failed, it prompts "**Please adjust your position!**".




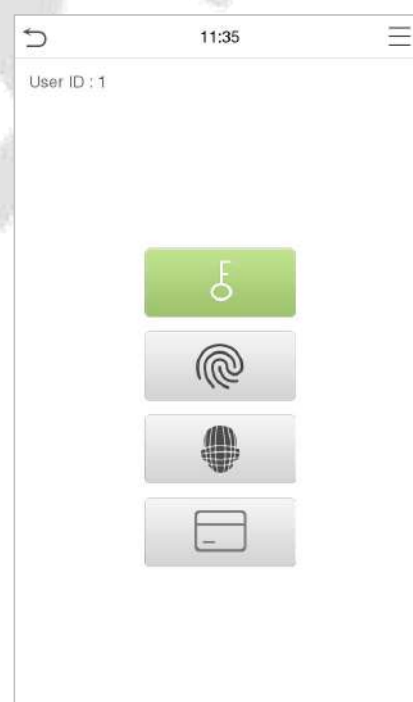
## 1.6.5 Password Verification

The device compares the entered password with the registered password by 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 card in addition to password, and the verification method is set to Password/Fingerprint/Card/Face verification, the following screen will appear. Select the  icon to enter password verification mode.

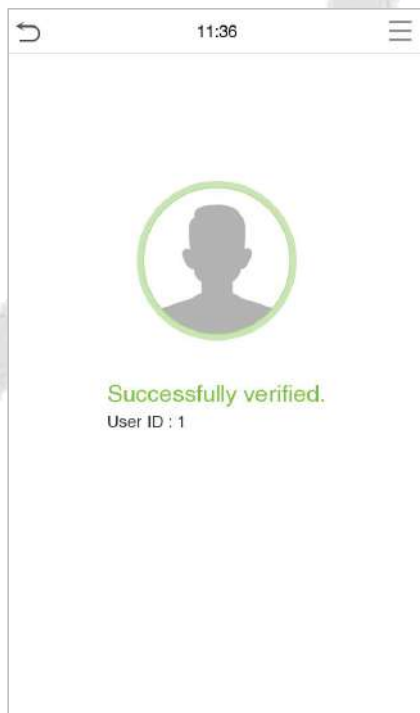


Input the password and press **OK**.

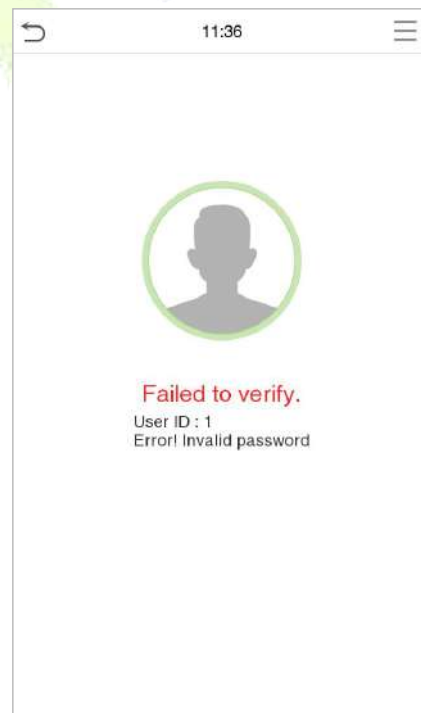


The following screen displays, after inputting a correct password and a wrong password respectively.

Verification is successful:



Verification is failed:



## 1.6.6 Combined Verification

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

### Combined Verification Symbol Definition:

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

Verification Mode	Verification Mode	Verification Mode
<input checked="" type="radio"/> Password/Fingerprint/Card/Face	<input type="radio"/> Fingerprint+Password+Card	<input type="radio"/> Password+Card
<input type="radio"/> Fingerprint Only	<input type="radio"/> Password+Card	<input type="radio"/> Password/Card
<input type="radio"/> User ID Only	<input type="radio"/> Password/Card	<input type="radio"/> User ID+Fingerprint+Password
<input type="radio"/> Password	<input type="radio"/> User ID+Fingerprint+Password	<input type="radio"/> Fingerprint+(Card/User ID)
<input type="radio"/> Card Only	<input type="radio"/> Fingerprint+(Card/User ID)	<input type="radio"/> Face Only
<input type="radio"/> Fingerprint/Password	<input type="radio"/> Face Only	<input type="radio"/> Face+Fingerprint
<input type="radio"/> Fingerprint/Card	<input type="radio"/> Face+Fingerprint	<input type="radio"/> Face+Password
<input type="radio"/> User ID+Fingerprint	<input type="radio"/> Face+Password	<input type="radio"/> Face+Card
<input type="radio"/> Fingerprint+Password	<input type="radio"/> Face+Card	<input type="radio"/> Face+Fingerprint+Card
<input type="radio"/> Fingerprint+Card	<input type="radio"/> Face+Fingerprint+Card	<input type="radio"/> Face+Fingerprint+Password

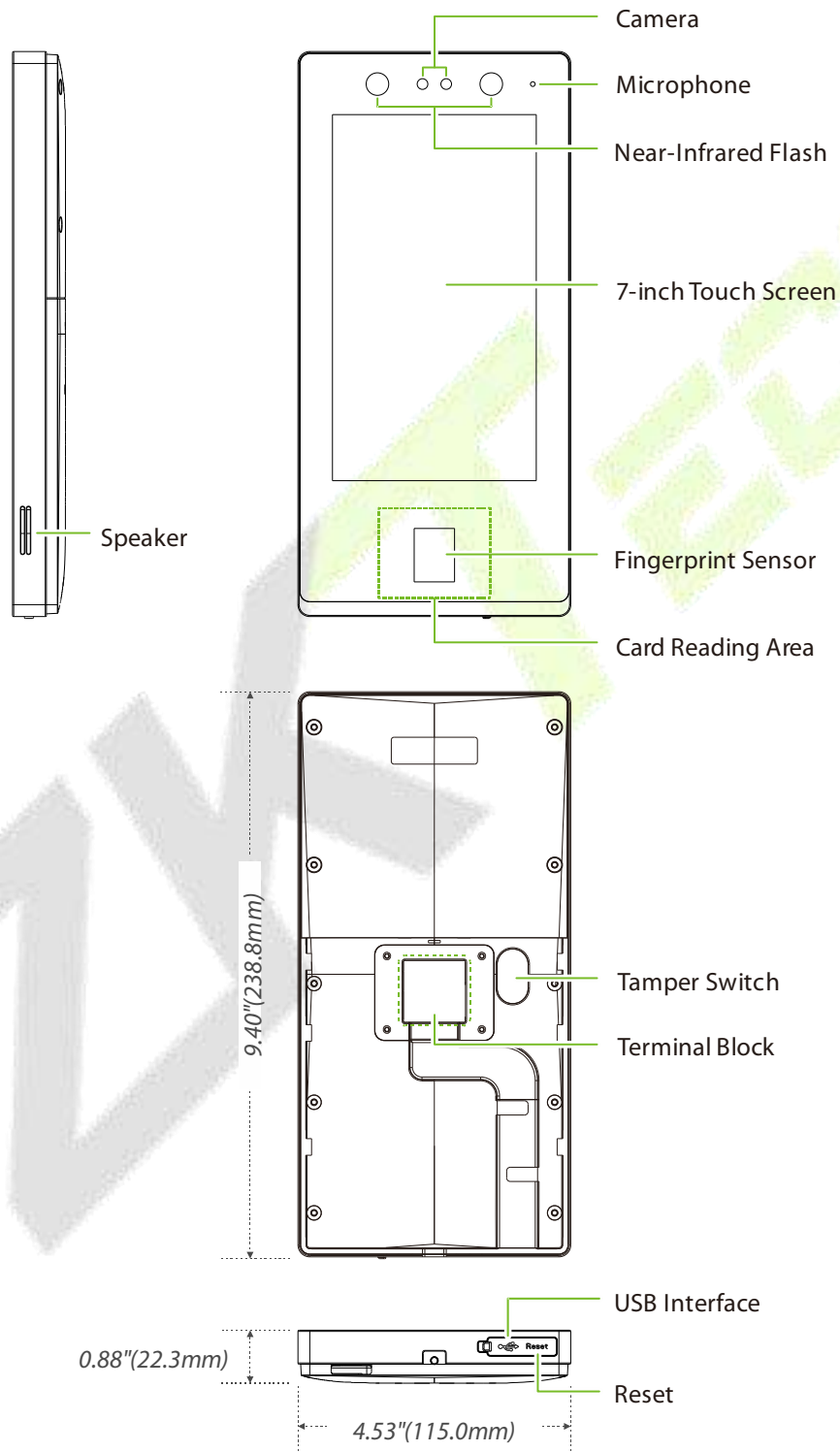
### Procedure to set for Combined Verification Mode:

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

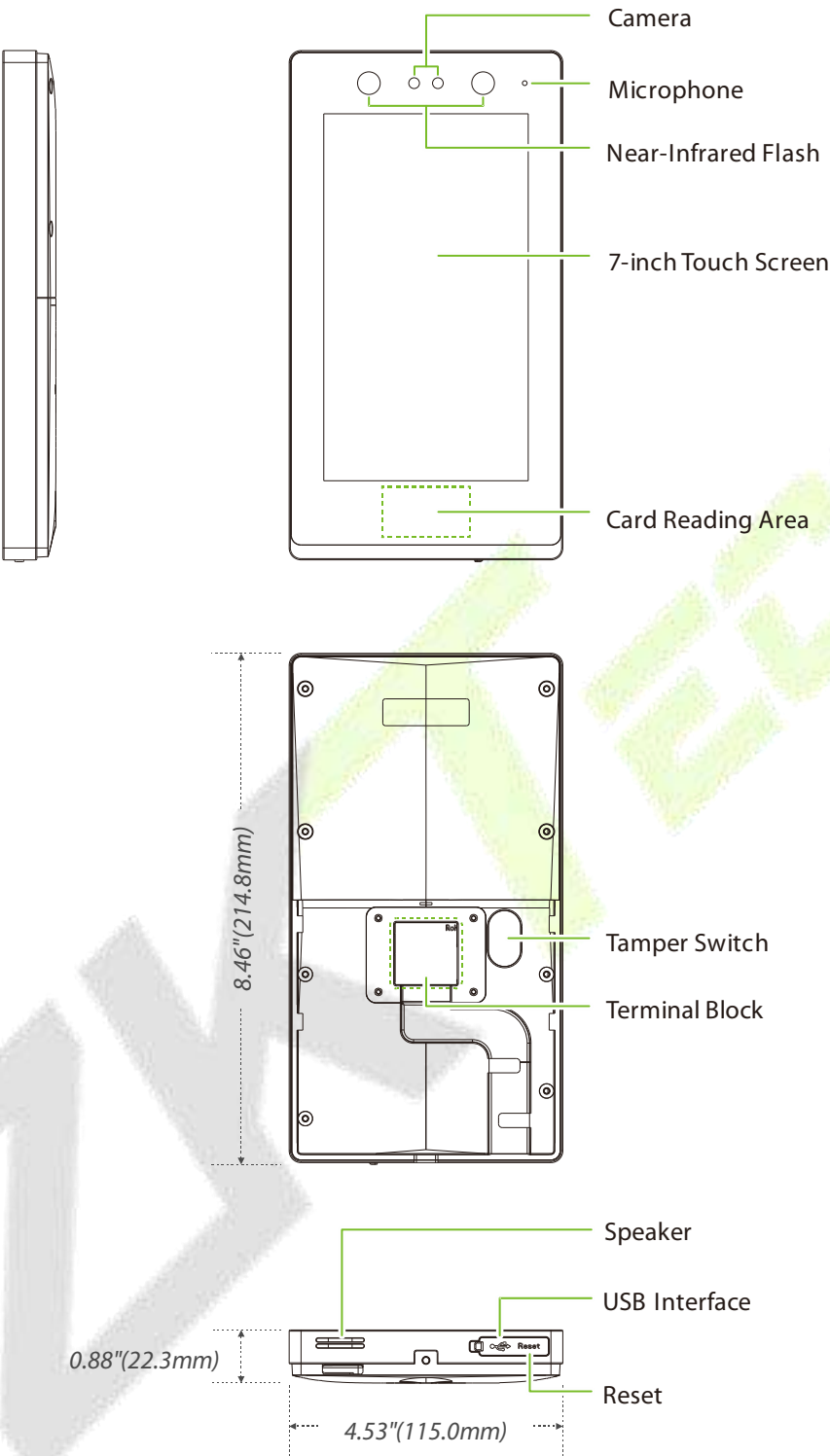
## 2. Overview

### 2.1 Appearance

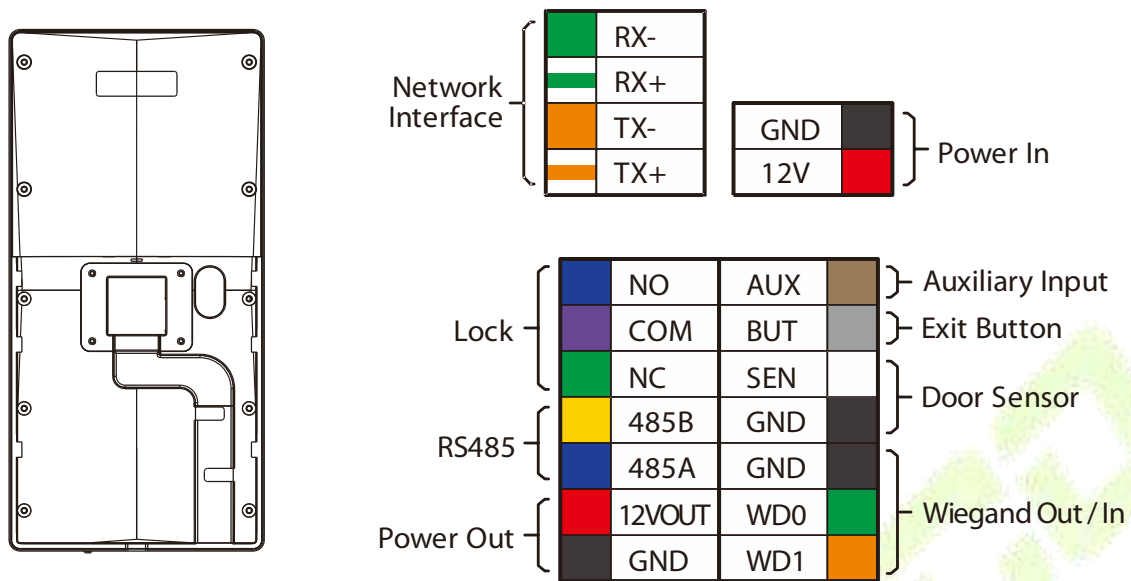
#### **BioFace D1**



**BioFace D1**

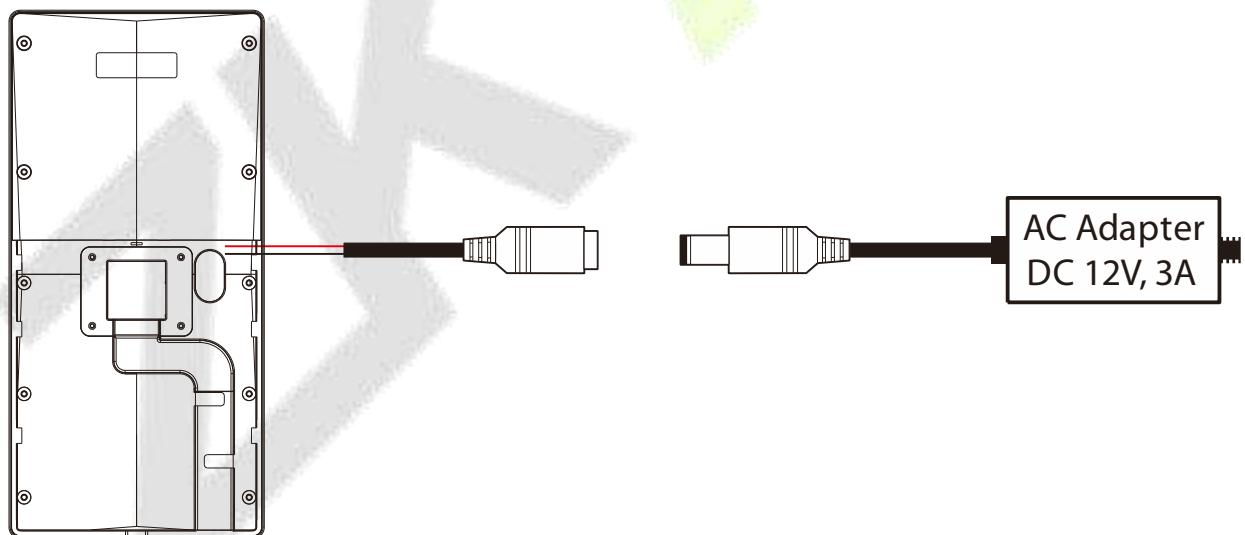


## 2.2 Terminal and Wiring Description



## 2.3 Wiring Description

### 2.3.1 Power Connection

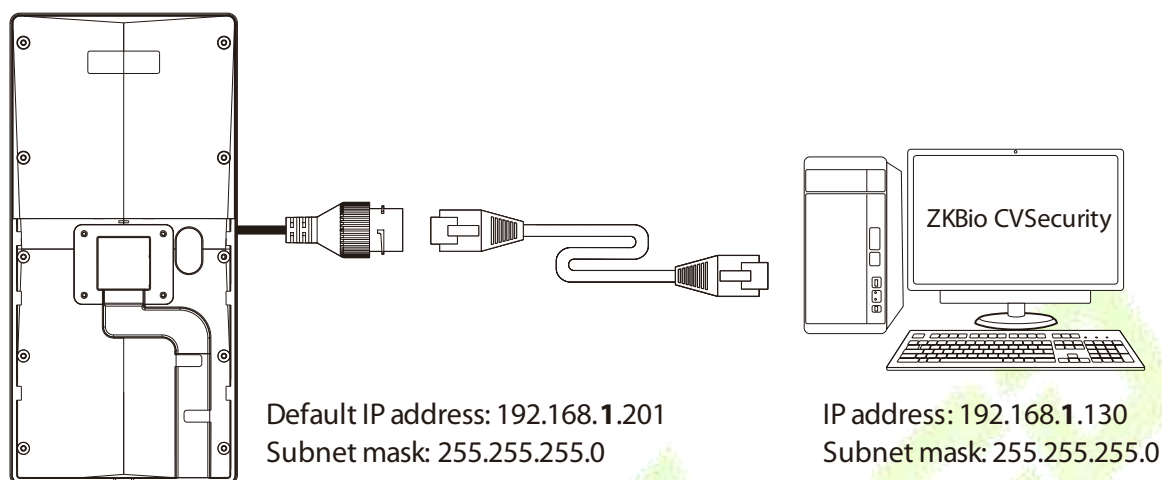


#### Recommended power supply

- Recommended AC adapter: **12V, 3A**.
- To share power with other devices, use an AC adapter with higher current ratings.

## 2.3.2 Ethernet Connection

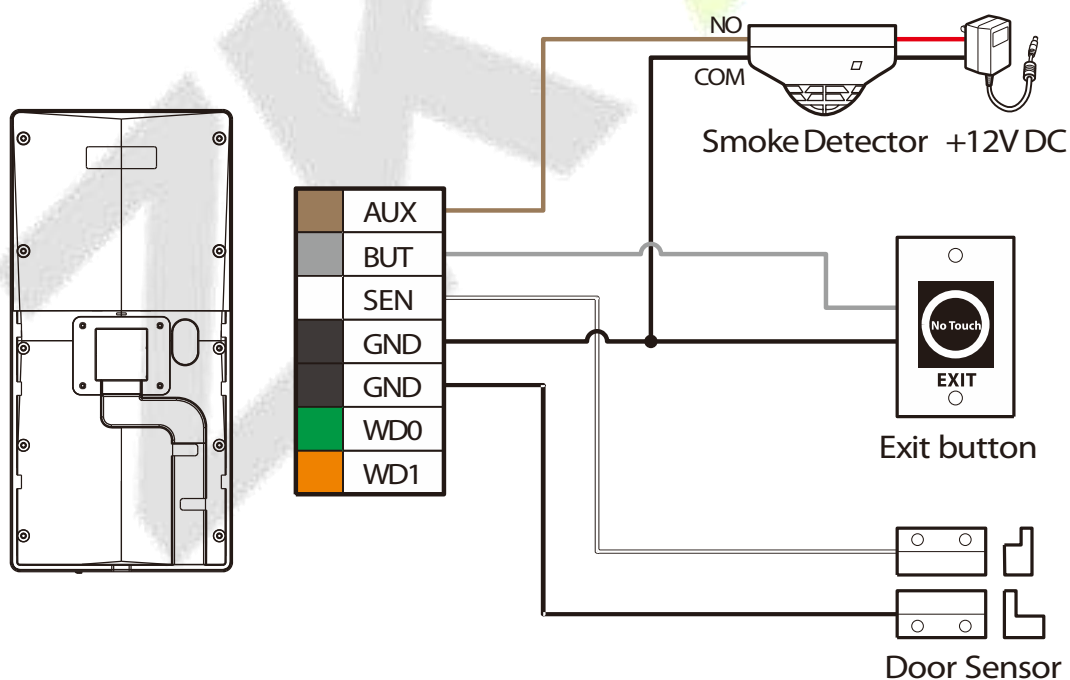
Connect the device to the computer software using an Ethernet cable. An example is shown below:



Click **Comm.** > **Ethernet** > **IP Address** to input the IP address.

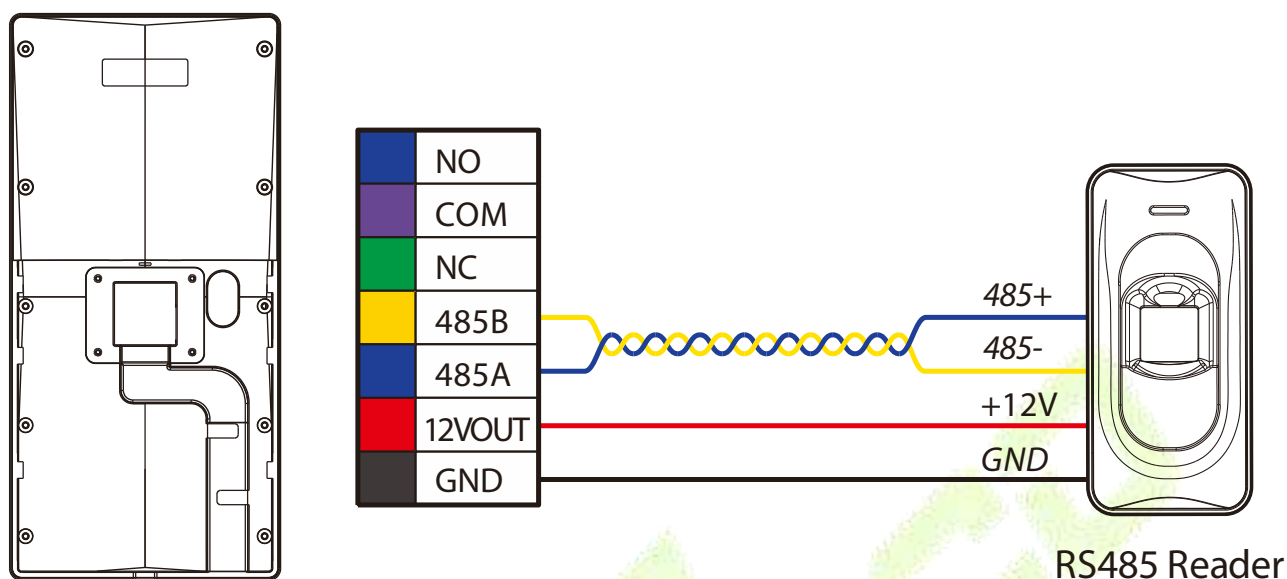
**Note:** In LAN, IP address of the server (PC) and the device must be in the same network segment when connecting to the software.

## 2.3.3 Exit Button, Door Sensor & Auxiliary Connection





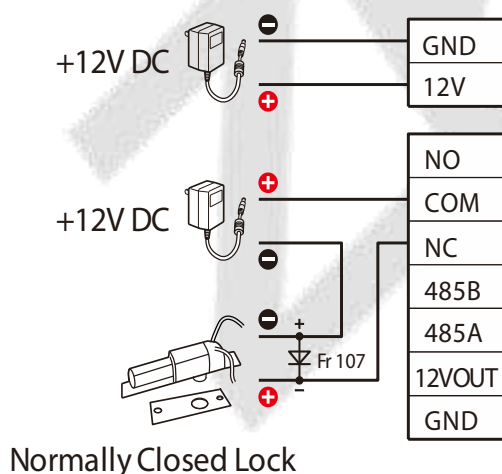
### 2.3.4 RS485 Connection



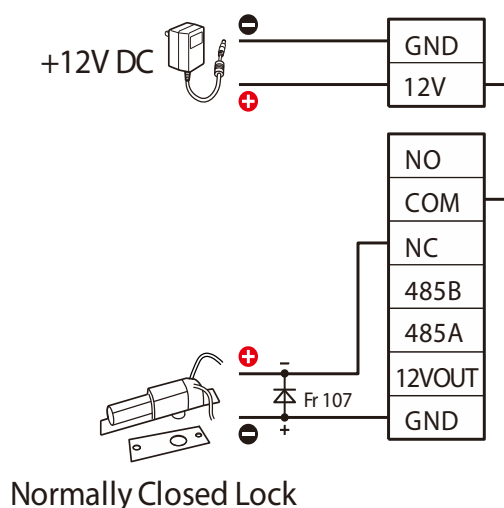
### 2.3.5 Lock Relay Connection

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

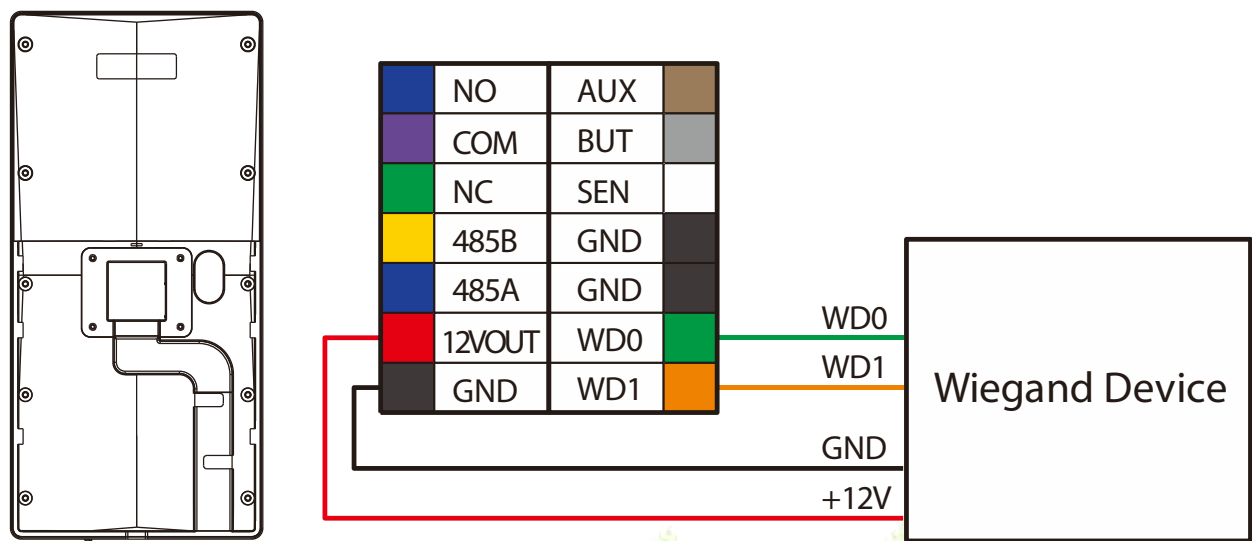
#### 1) Device not sharing power with the lock



#### 2) Device sharing power with the lock



2.3.6 Wiegand Reader Connection



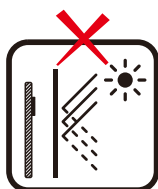
## 3. Installation

### 3.1 Installation Environment

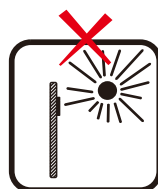
Please refer to the following recommendations for installation.



INSTALL INDOORS  
ONLY



AVOID INSTALLATION  
NEAR  
GLASS WINDOWS



AVOID DIRECT  
SUNLIGHT  
AND EXPOSURE

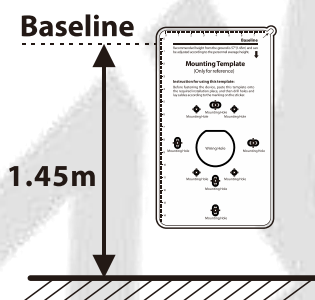


AVOID USE OF ANY  
HEAT SOURCE  
NEAR THE DEVICE

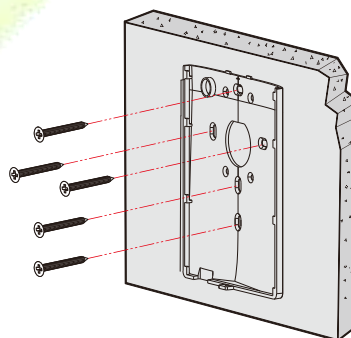
### 3.2 Device Installation

1. Attach the mounting template sticker to the wall, and drill holes according to the mounting paper.
2. Fix the backplate on the wall with the wall mounting screws.
3. After passing the wires through the wiring hole and connecting them to the device, and then snap the device onto the backplate and push it down into place.
4. Fasten the device to the backplate with a security screw.

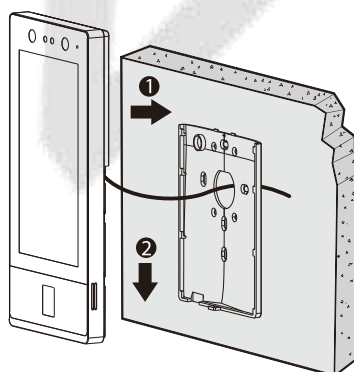
1



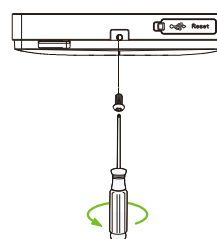
2



3

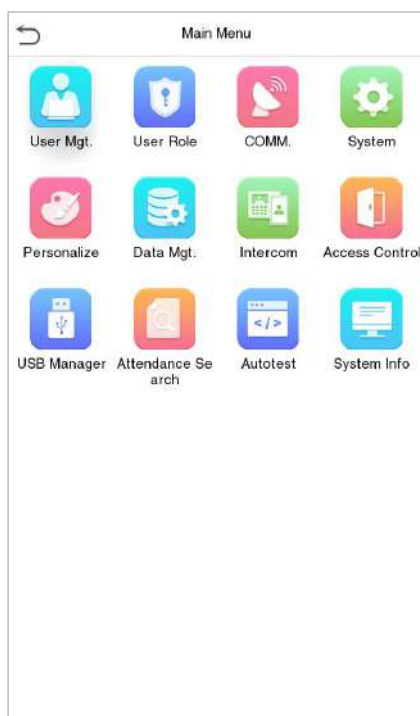


4



## 4. Main Menu

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

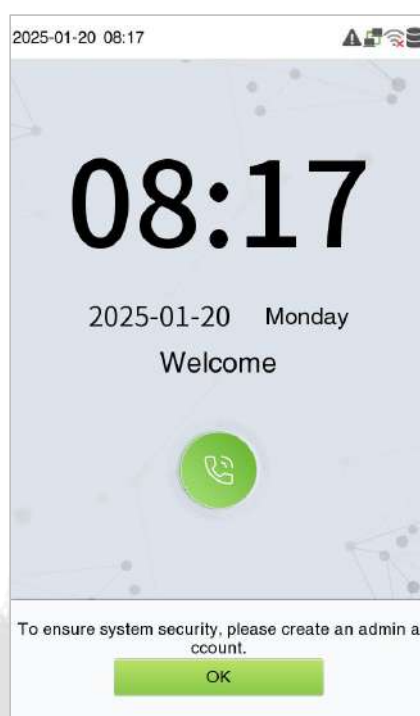


### Function Description

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 network, serial comm, pc connection, wireless network, 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 & fingerprint parameters★, device type setting, security setting, update firmware online, USB upgrade, 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, and duress option settings.
<b>USB Manager</b>	To upload or download the specific data by a USB drive.

<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, fingerprint sensor★ and real-time clock.
<b>System Info</b>	To view data capacity, device and firmware information and privacy policy of the device.

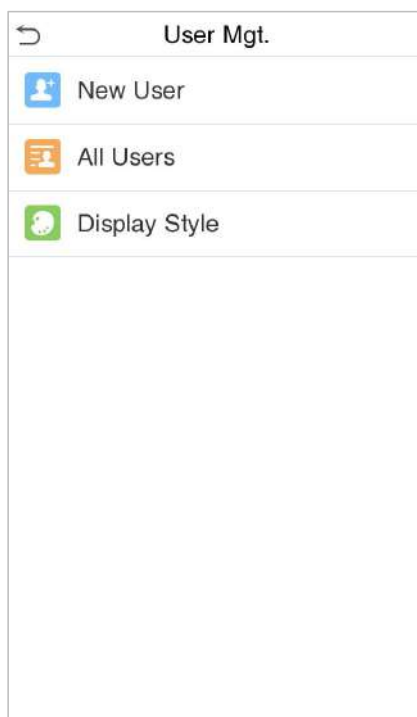
**Note:** When users use the product for the first time, they should operate it after setting administrator privileges. Tap **User Mgt.** to add an administrator or edit user permissions as a super administrator. If the product does not have an administrator setting, the system will show an administrator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



## 5. User Management

### 5.1 User Registration

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



#### 5.1.1 User ID and Name

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

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

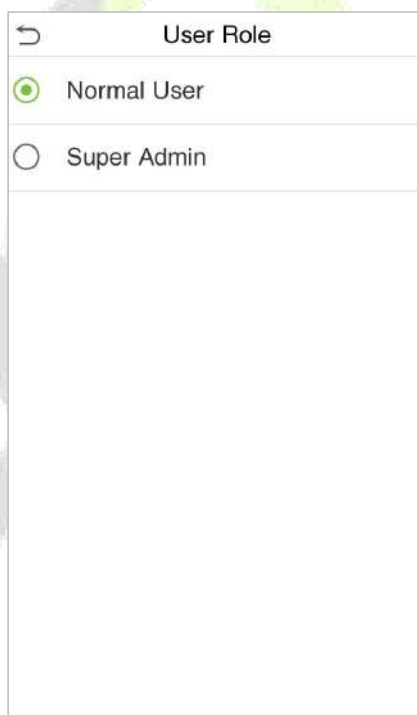
**Notes:**

- 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 enter User ID already exists.

### 5.1.2 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.



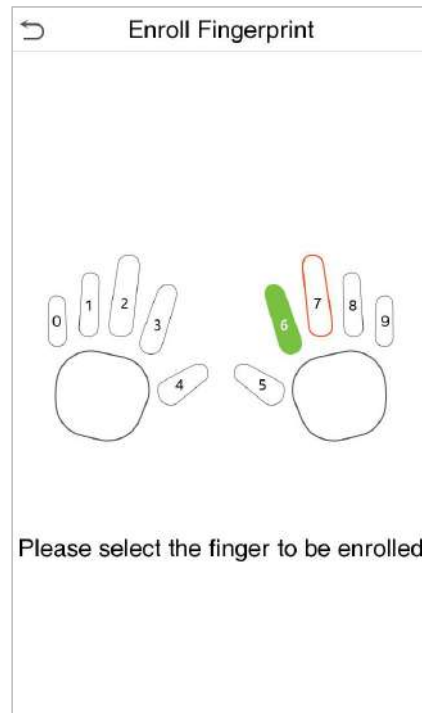
The screenshot shows a modal dialog titled "User Role". It contains two radio button options: "Normal User" (which is selected, indicated by a green dot) and "Super Admin" (which is unselected, indicated by a grey dot). The dialog has a back arrow in the top left corner.

**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 [1.6 Verification Mode](#).

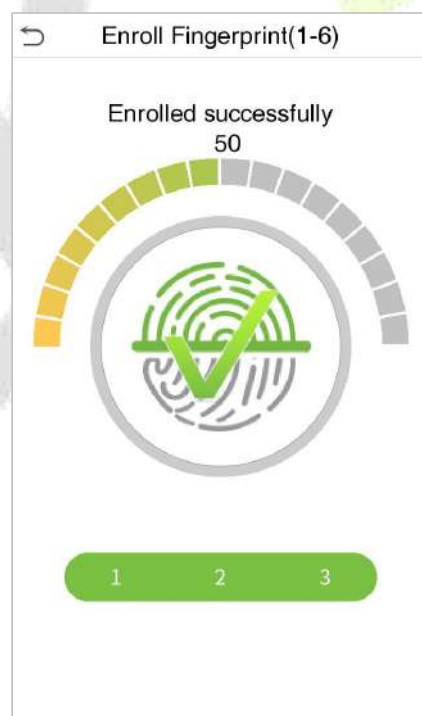


### 5.1.3 Fingerprint★

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



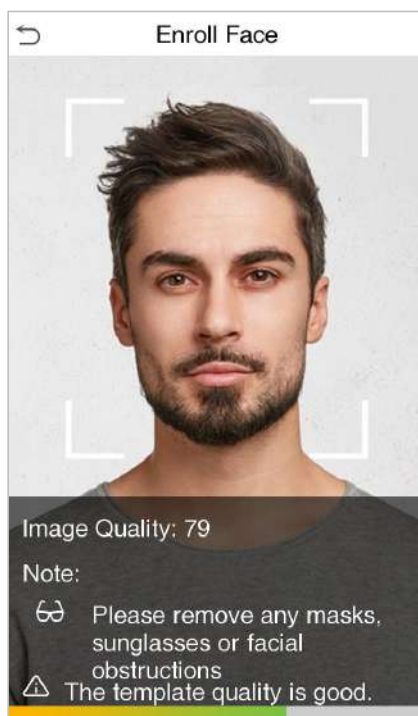
Press the same finger on the fingerprint reader three times. Green indicates that the fingerprint was enrolled successfully.



### 5.1.4 Face Template

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

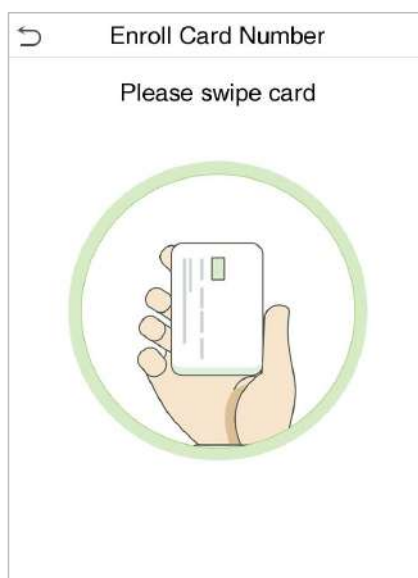
- Please face towards the camera and position your face template inside the white guiding box and stay still during face template registration.
- A progress bar shows up while registering the face template and a **“Enrolled Successfully”** is displayed as the progress bar completes.
- If the face template is registered already then, the **“Duplicate Face”** message shows up. The registration interface is as follows:



### 5.1.5 Card

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

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



### 5.1.6 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 again.



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

### 5.1.7 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
Fingerprint	0
Face	0
Card	0
Password	
Profile Photo	0
Access Control Role	



- When a user registered with a photo 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.

### 5.1.8 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.

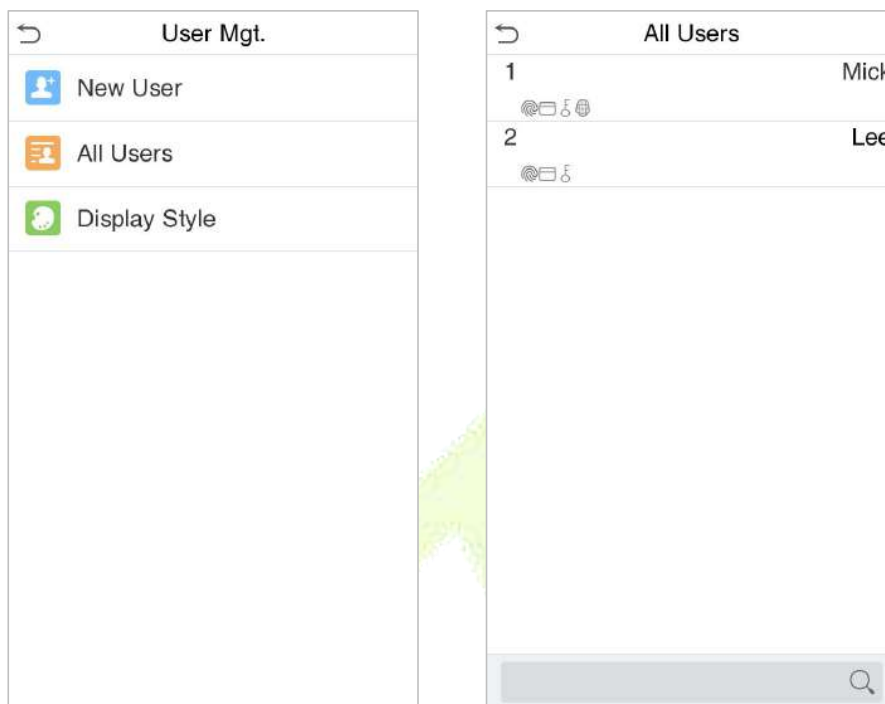
- Tap **Access Control Role > Access Group**, to assign the registered users to different groups for better management. New users belong to Group 1 by default and can be reassigned to other groups. The device supports up to 99 Access Control groups.
- Tap **Time Period**, to select the time period to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

Access Control	
Access Group	1
Time Period	
Duress Fingerprint	Undefined

## 5.2 Search for Users

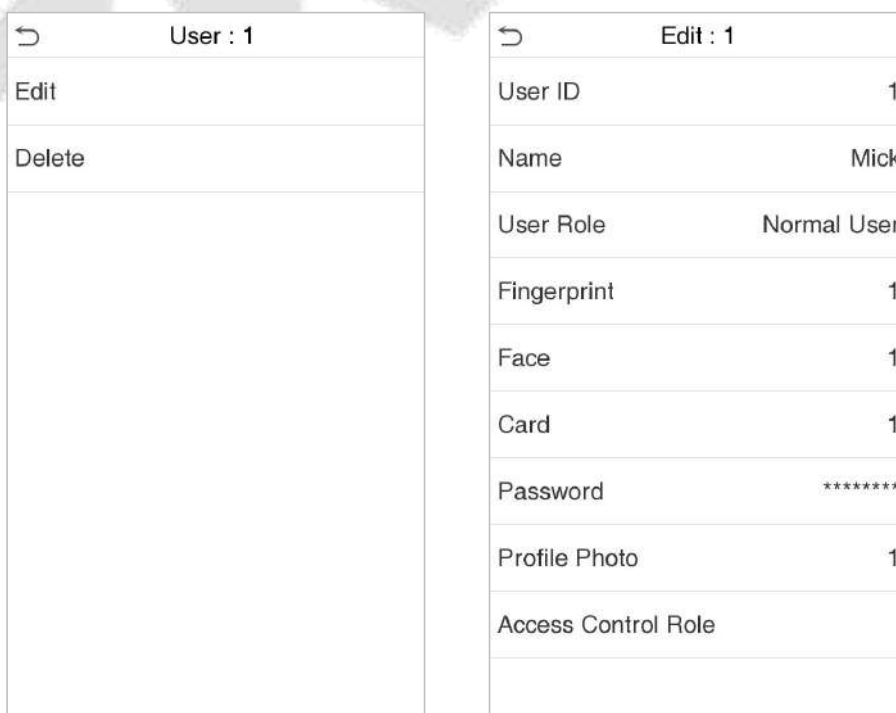
On the **Main Menu**, tap **User Mgt.**, and then tap **All Users** to search for a User.

- 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.



## 5.3 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 detail. The process in detail refers to ["3. User Management"](#).

## 5.4 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.

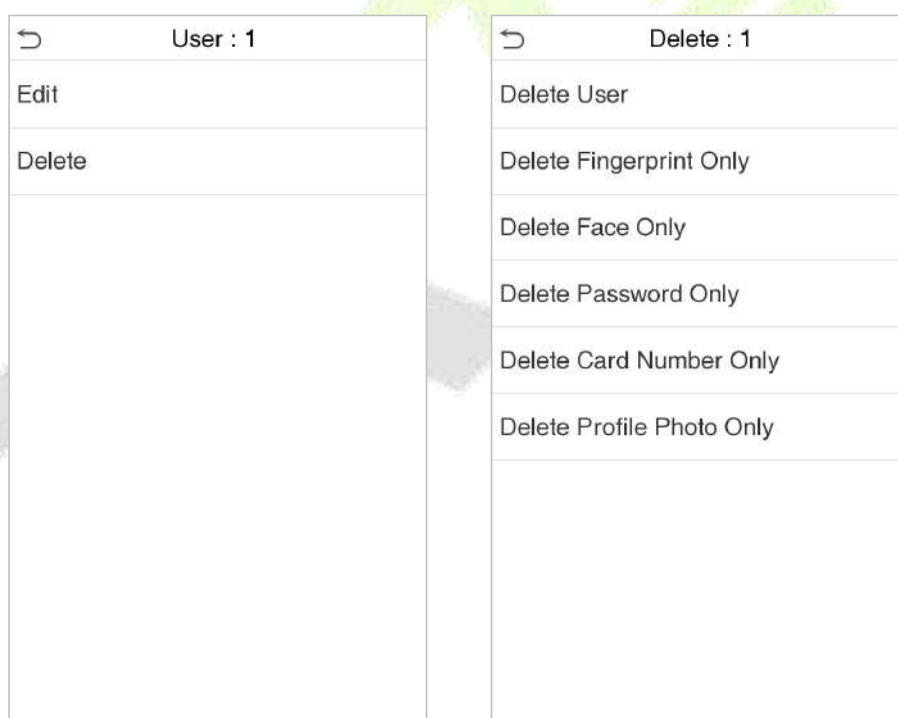
**Delete Fingerprint Only:** Deletes the fingerprint information of the selected user.

**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.



## 5.5 Display Style

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

↶

Display Style

☒

Multiple Line

☐

Mixed Line

Different display styles are shown as below:

Multiple Line:

↶

All Users

1

Mick

2

Lee

Mixed Line:

↶

All Users

1

Mick

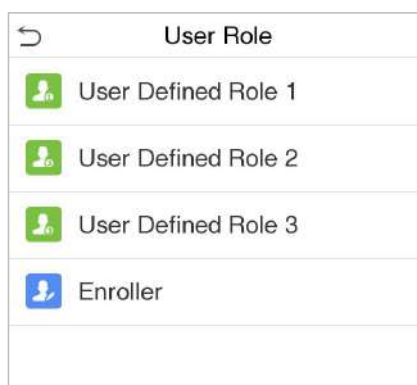
2

Lee

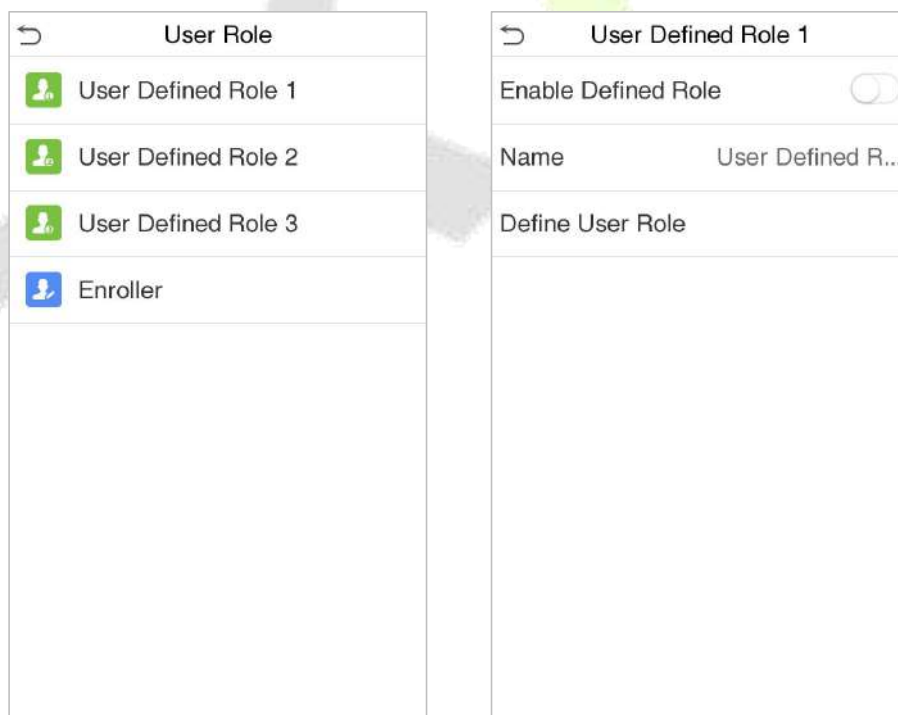
## 6. User Role

**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.



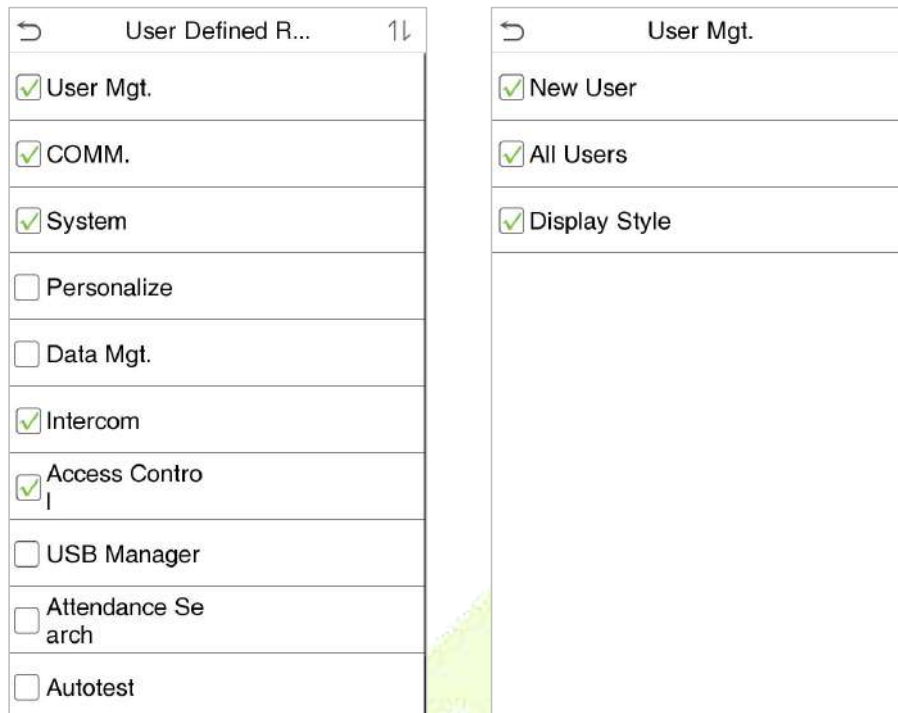
- On the **User Defined Role** interface, toggle **Enable Defined Role** to enable or disable the user defined role.
- Tap on **Name** and enter the custom name of the role.



- 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.



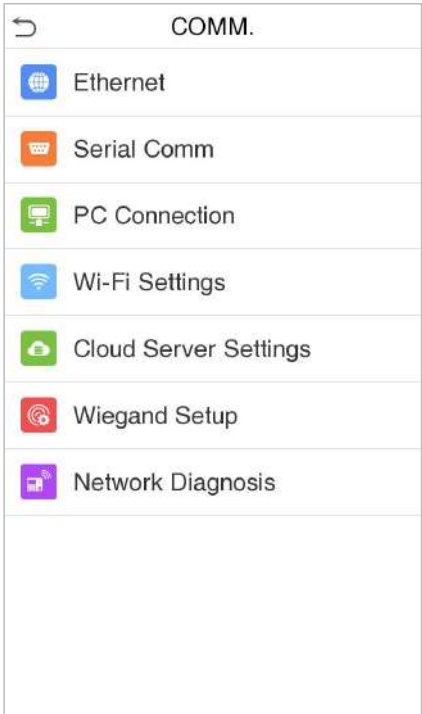
- First tap on the required **Main Menu** function name, and then select its required sub-menus from the list.



**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.

## 7. Communication Settings

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



### 7.1 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.



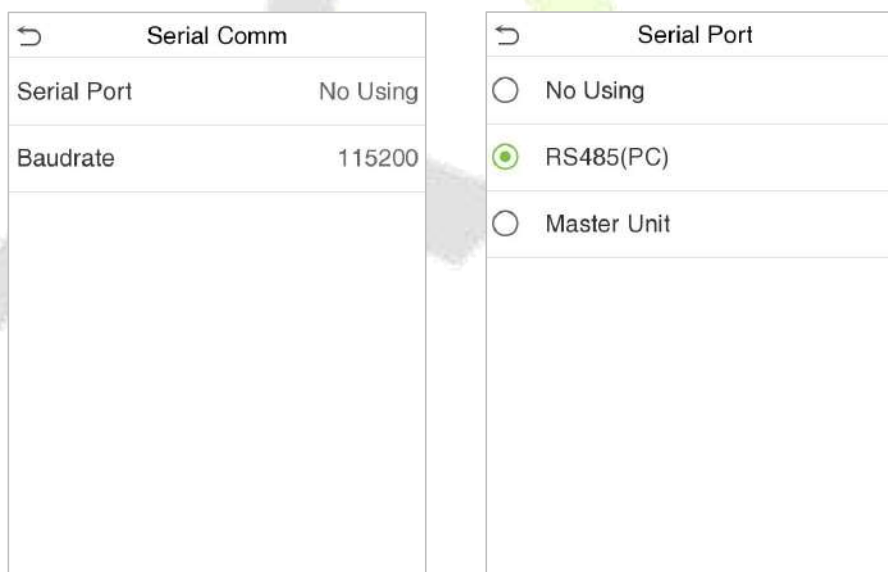
## Function Description

Function Name	Descriptions
<b>Display in Status Bar</b>	Toggle to set whether to display the network icon on the status bar.
<b>IP 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.

## 7.2 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>
<b>Baud Rate</b>	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.

## 7.3 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.

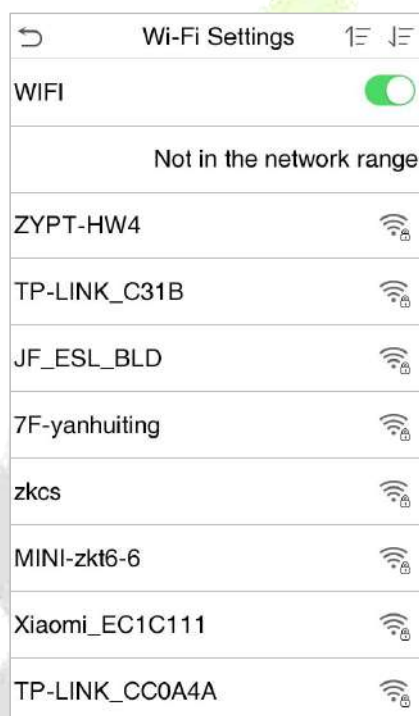
This function is enabled by default. This function can be enabled or disabled through the menu interface, and when changing the HTTPS status, the device will pop up a security prompt, and restart after confirmation.

## 7.4 Wireless Network★


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

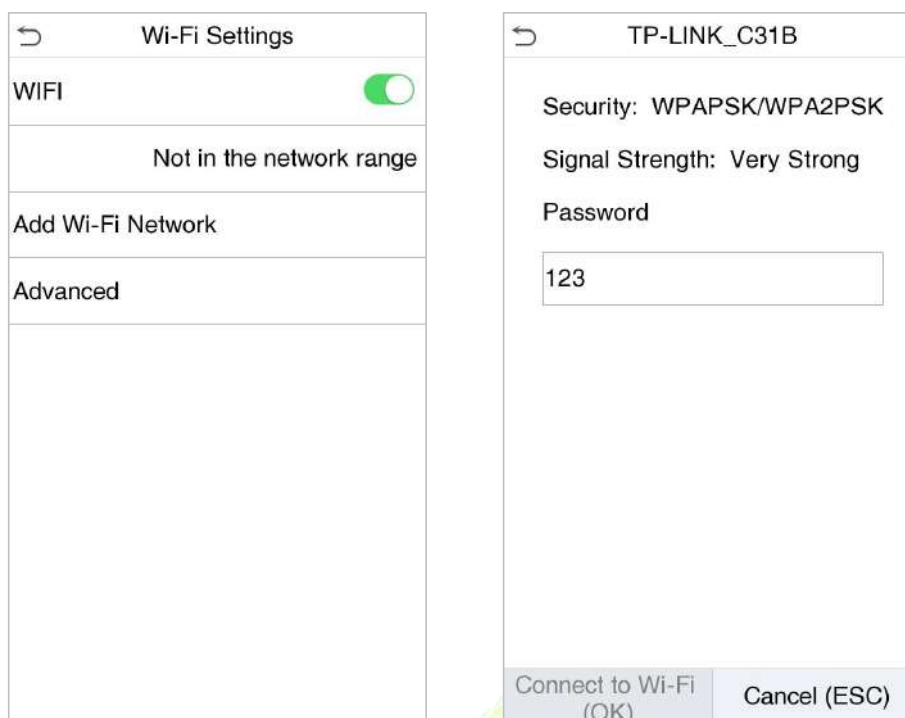
The Wi-Fi module enables data transmission via Wi-Fi (Wireless Fidelity) and establishes a wireless network environment. Wi-Fi is enabled by default in the device. If you don't need to use the Wi-Fi network, you can toggle the Wi-Fi to disable button.

Tap **Wireless Network** 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)**.

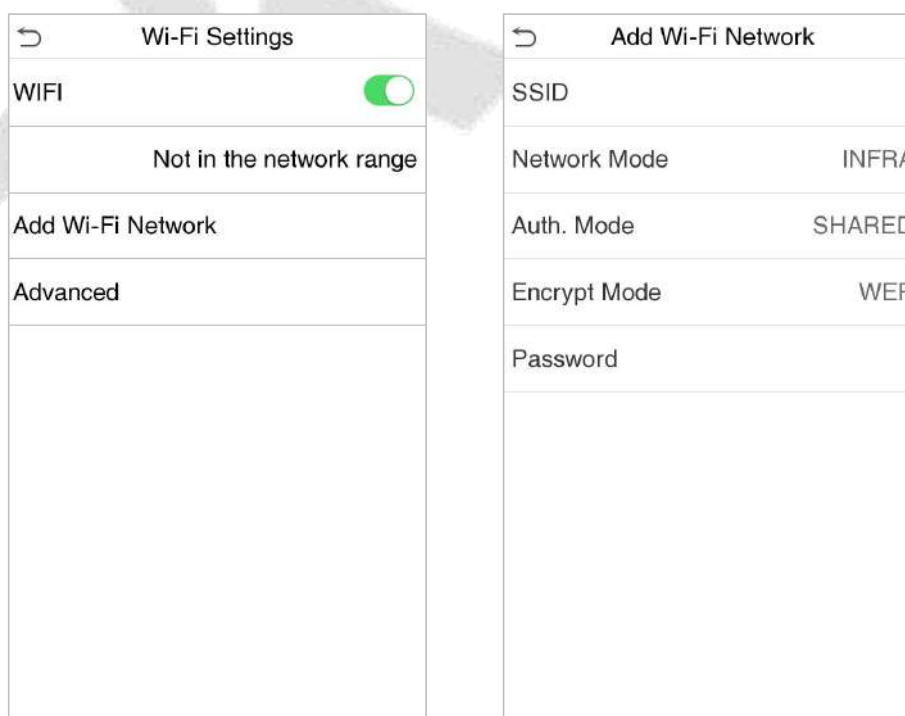


**WIFI Enabled:** Tap on the required network from the searched network list.

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 WIFI Network Manually**

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



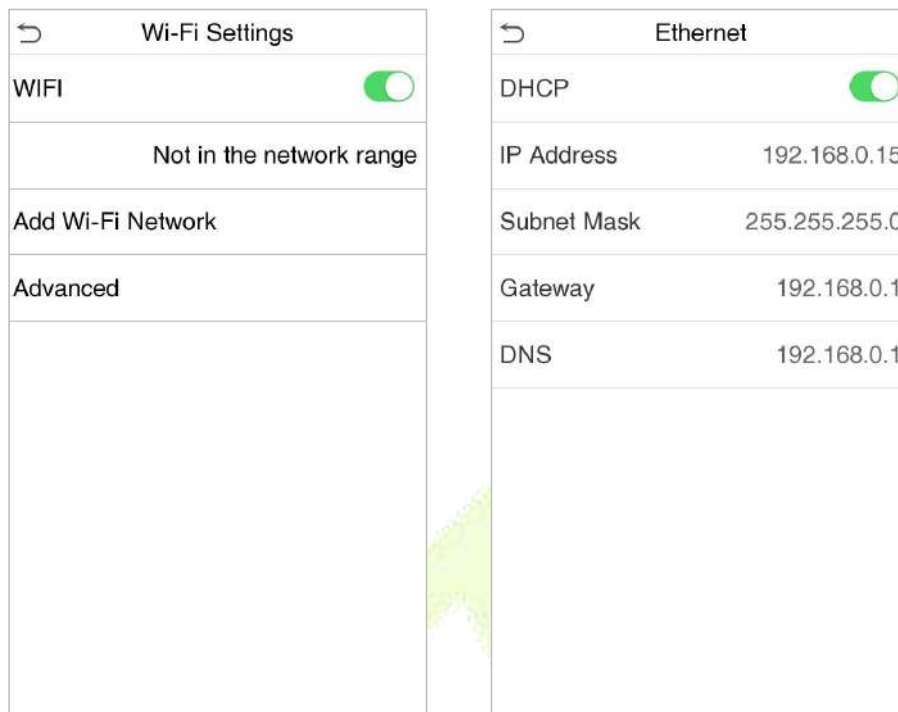
Tap on **Add Wi-Fi Network** to add the Wi-Fi manually.

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 **Wireless Network** 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.

## 7.5 Cloud Server Setting

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

Cloud Server Settings	
Server Mode	ADMS
Enable Domain Name	<input type="checkbox"/>
Server Address	192.168.163.61
Server Port	8081
Enable Proxy Server	<input type="checkbox"/>

### Function Description

Function Name		Description
<b>Enable Domain Name</b>	<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).
<b>Disable Domain Name</b>	<b>Server Address</b>	IP address of the ADMS server.
	<b>Server Port</b>	Port used by the ADMS server.
<b>Enable Proxy Server</b>		When you choose to enable the proxy, you need to set the IP address and port number of the proxy server.

## 7.6 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.

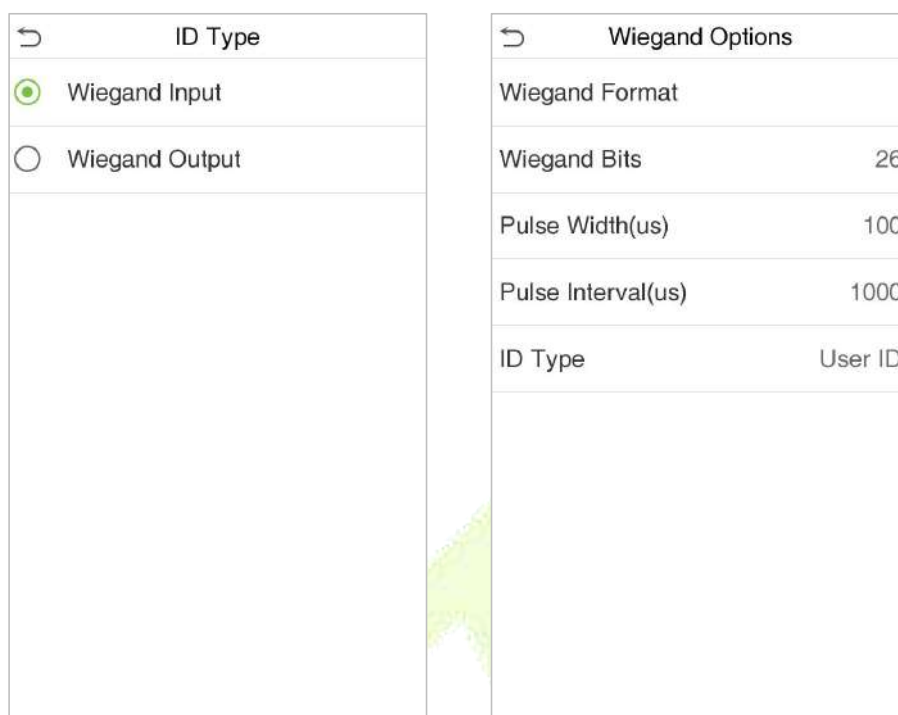
Wiegand Setup	
ID Type	Wiegand Output
Wiegand Options	

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



## 7.6.1 Wiegand Input

Tap **ID Type** on the **Wiegand Setup**, select **Wiegand Input**, and then tap **Wiegand Options** on the **Wiegand Setup**.



### 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

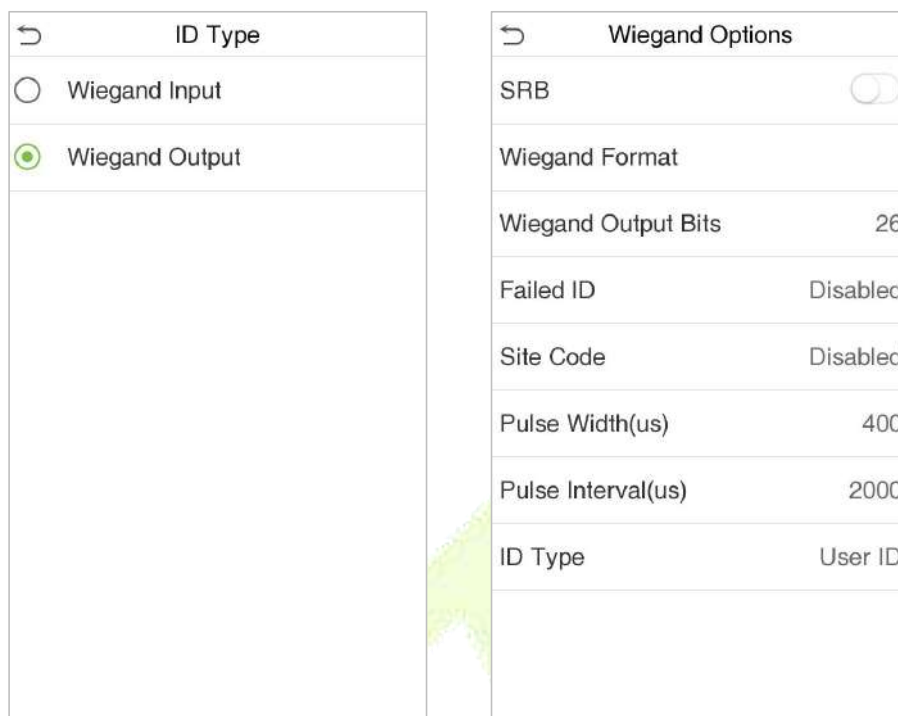
Wiegand Format	Description
<b>Wiegand26</b>	<p>EEEEEEEEEEEEEEEEEEEEEEEEEEEE</p> <p>Consists of 26 bits of binary code. The 1<sup>st</sup> bit is the even parity bit of the 2<sup>nd</sup> to 13<sup>th</sup> bits, while the 26<sup>th</sup> bit is the odd parity bit of the 14<sup>th</sup> to 25<sup>th</sup> bits. The 2<sup>nd</sup> to 25<sup>th</sup> bits is the card numbers.</p>

<b>Wiegand26a</b>	ESSSSSSSSCCCCCCCCCCCCCCCCCCCO 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.
<b>Wiegand34</b>	ECCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO 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.
<b>Wiegand34a</b>	ESSSSSSSSCCCCCCCCCCCCCCCCCCCCCCO 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>	OFFFFFFFFFCCCCCCCCCCCCCCCCMME 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>	EFFFFFFFFFCCCCCCCCCCCCCCCCCCO 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>	OMMMMSSSSSSSSSSSSCCCCCCCCCCCCCCCCE 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>	ESSSSSSSSSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO 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.

"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.

## 7.6.2 Wiegand Output

Tap **ID Type** on the **Wiegand Setup**, select **Wiegand Output**, and then tap **Wiegand Options** on the **Wiegand Setup**.



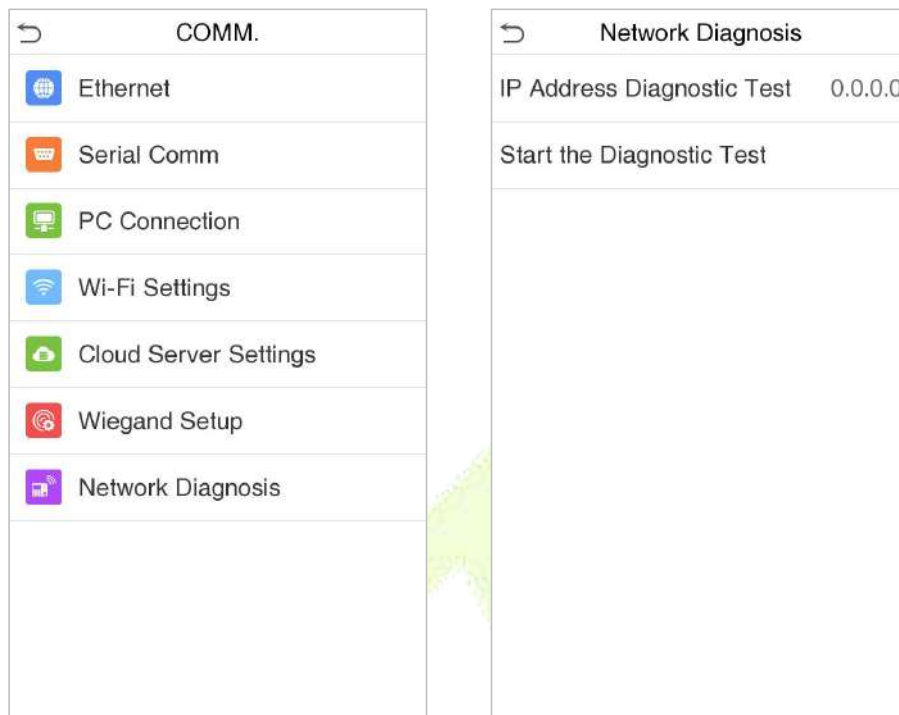
### Function Description

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, and 50 bits.
<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.

## 7.7 Network Diagnosis

To set the network diagnosis parameters.

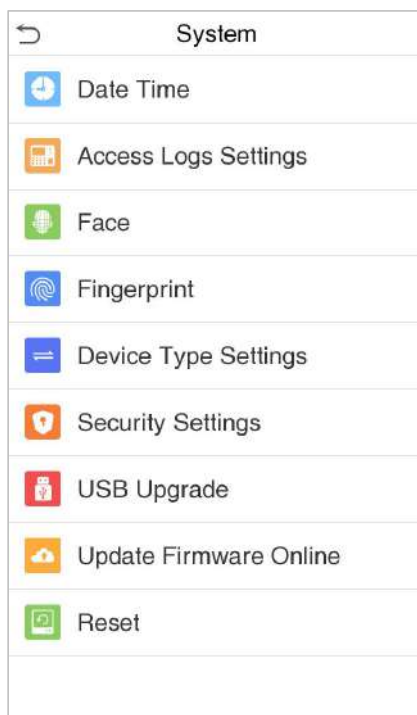
Tap **Network Diagnosis** on the **Comm.** Settings interface to set the IP address diagnostic and start the diagnostic parameters.



## 8. System Settings

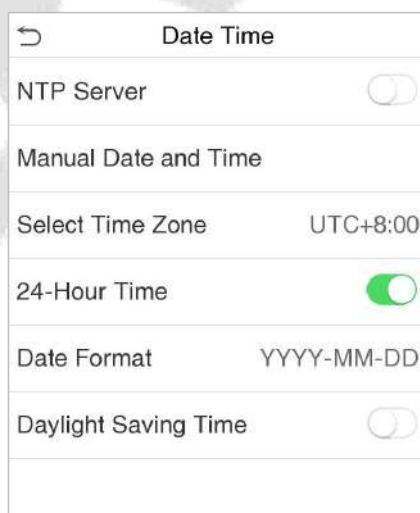
Set related system parameters to optimize the performance of the device.

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



### 8.1 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

☐

Manual Date and Time

Select Time Zone

UTC+8:00

24-Hour Time

☒

Date Format

YYYY-MM-DD

Daylight Saving Time

☒

Daylight Saving Mode

By Date/Time

Daylight Saving Setup

- Tap **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

00-00

Start Time

00:00

End Date

00-00

End Time

00:00

Date mode

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

**Note:** For example, the user sets the time of the device (18:35 on March 15, 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.

## 8.2 Access Logs Settings

Click **Access Logs Settings** 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

### Function Description

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>	<p>This function is disabled by default. When enabled, there will be a security prompt.</p>
<b>Alphanumeric User ID</b>	<p>Decides whether to support letters in a User ID.</p>
<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.

## 8.3 Face Template Parameters

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

Face	1↓	Face	1↓
1:N Threshold	40	1:1 Threshold	30
1:1 Threshold	30	Face Enrollment Threshold	70
Face Enrollment Threshold	70	Image Quality	40
Image Quality	40	Facial Recognition Distance	Far
Facial Recognition Distance	Far	Anti-spoofing Using NIR	<input checked="" type="checkbox"/>
Anti-spoofing Using NIR	<input checked="" type="checkbox"/>	Binocular Live Detection Thresh hold	30
Binocular Live Detection Thresh hold	30	Face AE	<input type="checkbox"/>
Face AE	<input type="checkbox"/>	WDR	<input type="checkbox"/>
WDR	<input type="checkbox"/>	Anti-flicker Mode	Disable
Anti-flicker Mode	Disable	Face Algorithm	

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



## Function Description

Function Name	Description
<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>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.

## 8.4 Fingerprint Parameters★

Click **Fingerprint** on the System interface.

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

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

### Function Description

Function Name	Descriptions
<b>1:1 Threshold</b>	Under 1:1 verification method, the verification will only be successful when the similarity between the acquired fingerprint data and the fingerprint template associated with the entered user ID enrolled in the device is greater than the set value.
<b>1:N Threshold</b>	Under 1:N verification method, the verification will only be successful when the similarity between the acquired fingerprint data and the fingerprint templates enrolled in the device is greater than the set value.
<b>FP Sensor Sensitivity</b>	To set the sensibility of fingerprint acquisition. It is recommended to use the default level " <b>Medium</b> ". When the environment is dry, resulting in slow fingerprint detection, you can set the level to " <b>High</b> " to raise the sensibility; when the environment is humid, making it hard to identify the fingerprint, you can set the level to " <b>Low</b> ".
<b>1:1 Retry Attempts</b>	In 1:1 Verification, users might forget the registered fingerprint, or press the finger improperly. To reduce the process of re-entering user ID, retry is allowed.
<b>Fingerprint Algorithm</b>	Used to switch the version of the fingerprint algorithm, Finger VX13.0 or Finger VX10.0.
<b>Fingerprint Image</b>	This function is disabled by default. After disabling it, the fingerprint image will not be displayed when registering and verifying fingerprints. The menu interface allows to enable or disable this function, and there are security prompts when

switching. Four choices are available:

**Show for enroll:** to display the fingerprint image on the screen only during enrollment.

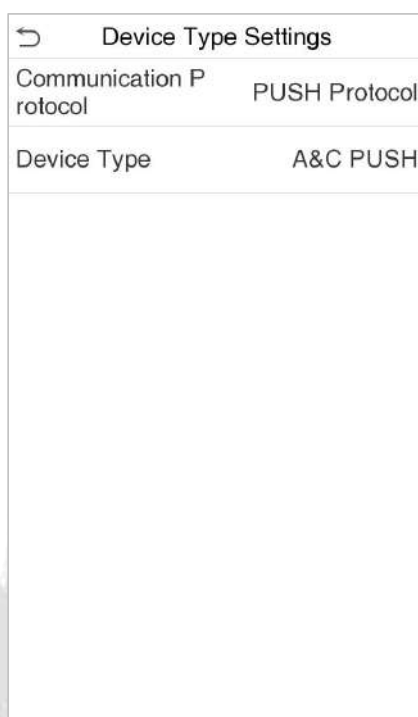
**Show for match:** to display the fingerprint image on the screen only during verification.

**Always show:** to display the fingerprint image on screen during enrollment and verification.

**None:** not to display the fingerprint image.

## 8.5 Device Type Setting

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

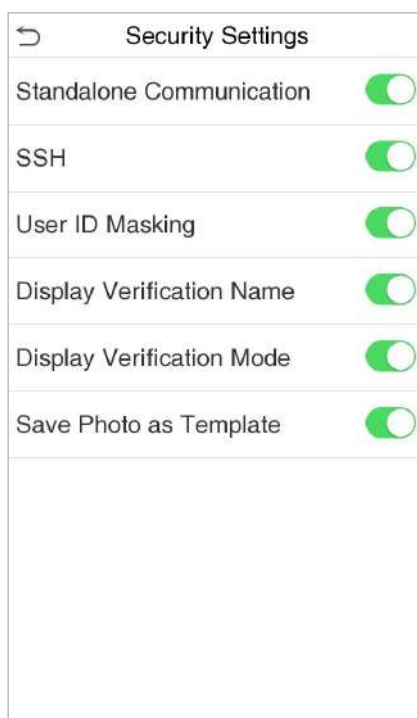


### Function Description

Function Name	Description
<b>Communication Protocol</b>	Set the device communication protocol. (BEST protocol is managed by ZKBio Zlink, please refer to <a href="#">15 Connecting to ZKBio Zlink Web</a> and <a href="#">16 Connecting to ZKBio Zlink App</a> .)
<b>Device Type</b>	Set the device as time attendance terminal (T&A PUSH) or access control terminal (A&C PUSH).

## 8.6 Security Setting

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



### Function Description

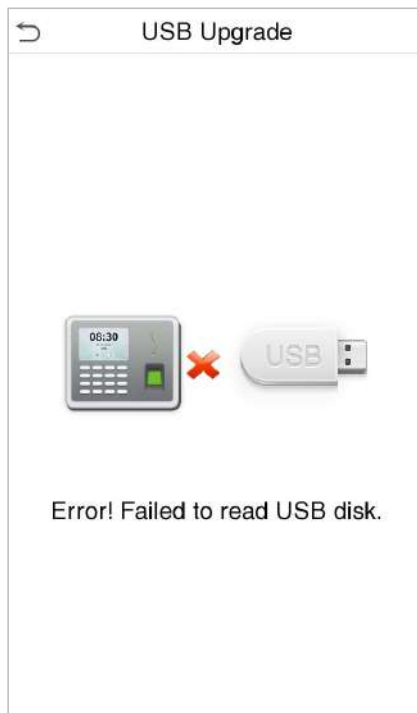
Function Name	Description
<b>Standalone Communication</b>	By default, this function is disabled. This function can be enabled or disabled via the menu interface. When it is switched on, a security prompt appears, and the device will restart after you confirm.
<b>SSH</b>	The device does not support the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

## 8.7 USB Upgrade

Tap **USB Upgrade** on the **System** interface.

The device's firmware program can be upgraded with the upgrade file in a USB drive. Before conducting this operation, please ensure that the USB drive contains the correct upgrade file and is properly inserted into the device.

If no USB disk is inserted in, the system gives the following prompt after you tap **USB Upgrade** on the System interface.



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

## 8.8 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).



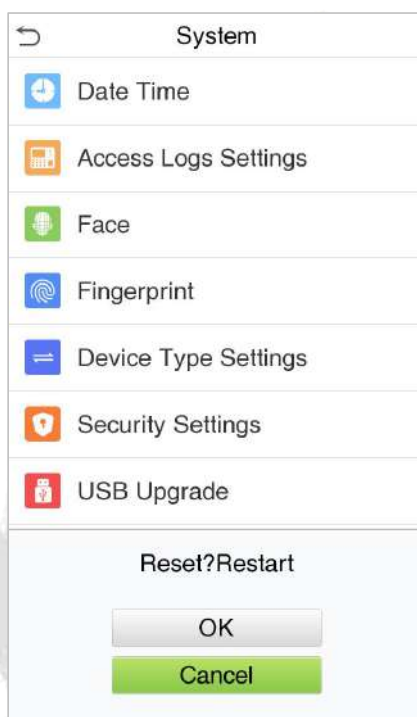
Click **Check for Updates** it may have the following 3 scenarios:

- 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.

## 8.9 Factory Reset

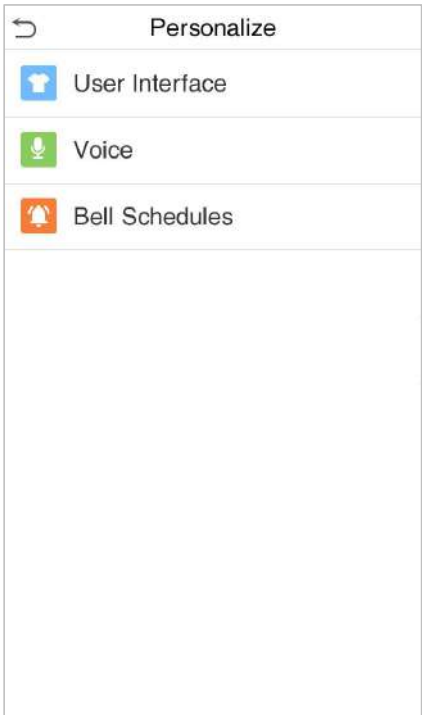
The Factory Reset function restores the device settings such as communication settings and system settings, to the default factory settings (This function does not clear registered user data).

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



## 9. Personalize Settings

Tap **Personalize** on the **Main Menu** interface to customize interface settings, voice and bell.



### 9.1 User Interface Settings

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



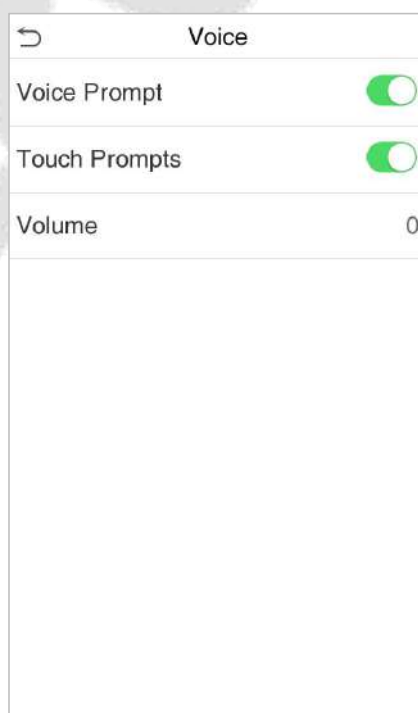


## Function Description

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.

## 9.2 Voice Settings

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



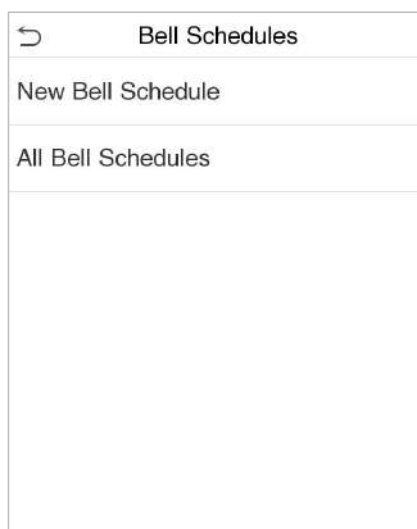


## Function Description

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.

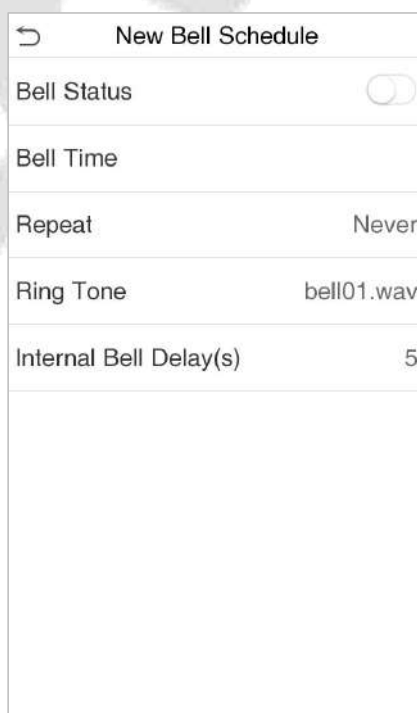
## 9.3 Bell Schedules

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:**

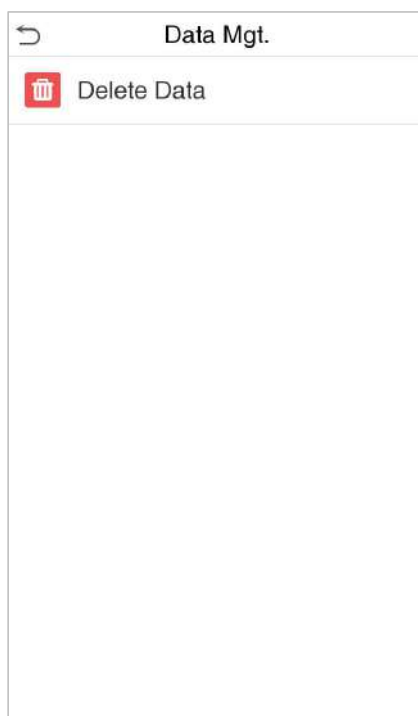
On the **All Bell Schedules** interface, tap on the required bell schedule, and tap **Edit** to edit the selected bell schedule. The editing method is the same as the operations of adding a new bell schedule.

- **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.

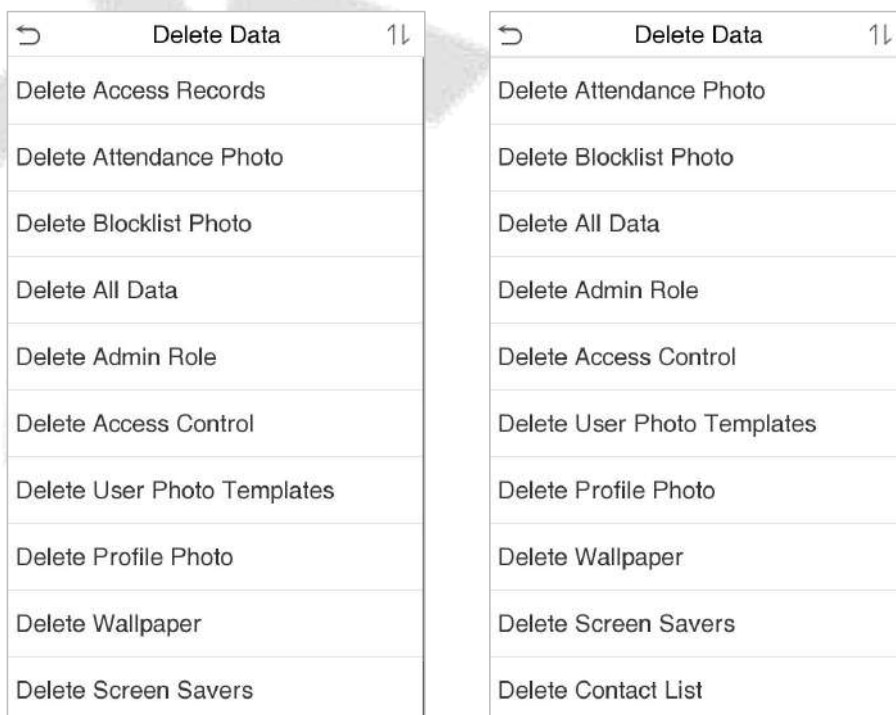
## 10. Data Management

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



### 10.1 Delete Data

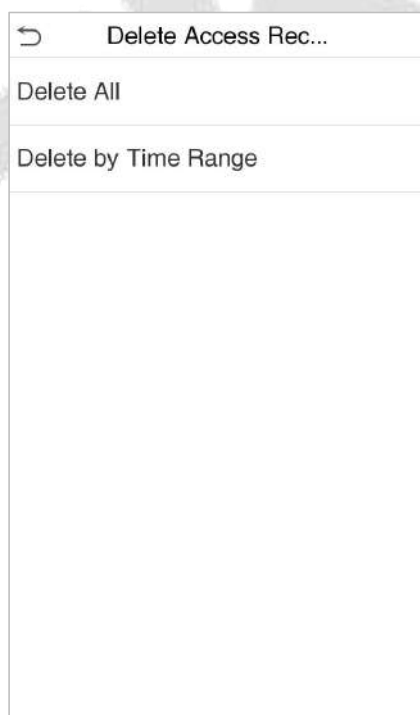
Tap **Delete Data** on the **Data Mgt.** interface to delete the required data.



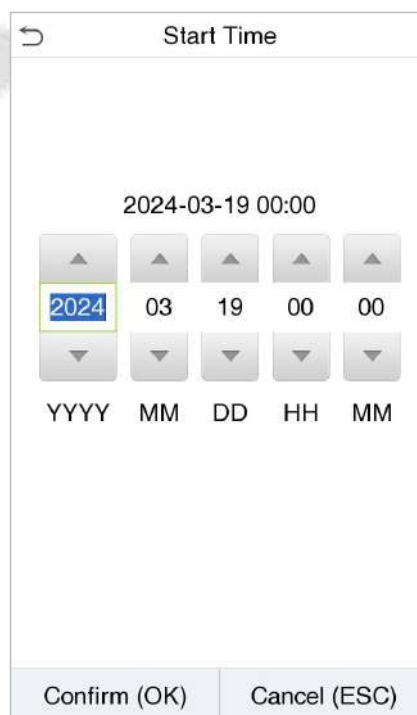
## Function Description

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.



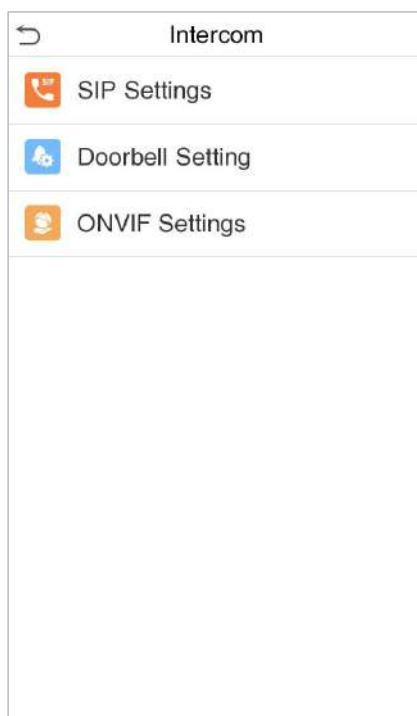
Select **Delete by Time Range**.



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

## 11. Intercom

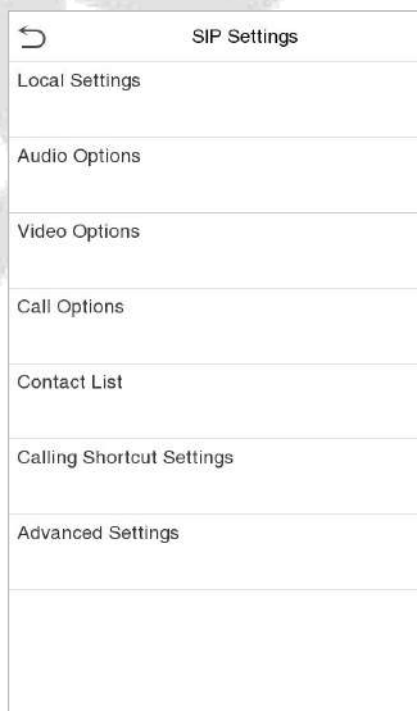
Click **Video intercom Parameters** on the System interface.



### 11.1 SIP Settings

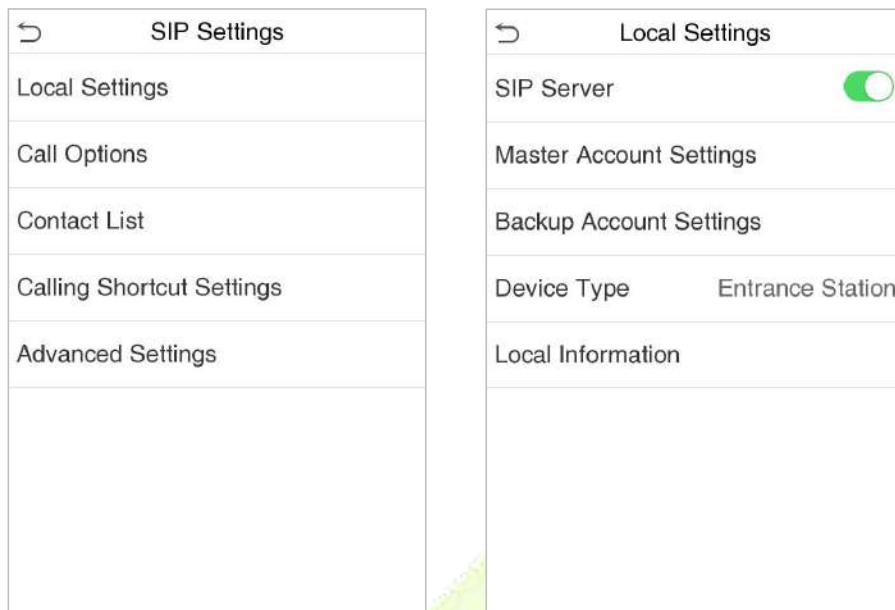
**Note:** This function needs to be used with the indoor station.

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




### 11.1.1 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>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>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.

### 11.1.2 Audio Options

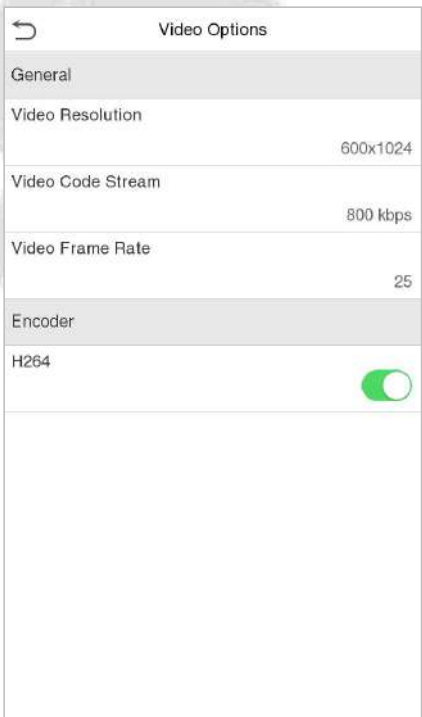
Tap **Audio Options** on the **SIP Settings** interface.



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

### 11.1.3 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 600 x 1024 (for portrait screen). The device is suggested to set as 600 x 1024.
<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>Note:</b> When using the intercom feature with the app, brief video stuttering may occur on the app side due to network fluctuations. It is recommended to keep the default at 800 kbps. You can also switch to 500 kbps or 1024 kbps as needed.
<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.



### 11.1.4 Call Options

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

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



**Function Description**

Function Name	Description
<b>Calling Delay(s)</b>	Set the time of call, valid value 30 to 60 seconds. The default is 30 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>	<p>User can choose whether to enable the <b>Auto Answer Settings</b> function. When enabled, the device will automatically answer incoming calls.</p> <p><b>Note:</b></p> <p><b>When Auto Answer is disabled:</b> If a call is made via the app, the device will display the call screen and require manual acceptance. If no action is taken, the call will automatically disconnect after a set timeout.</p> <ul style="list-style-type: none"> <li>• <b>Default timeout:</b> 30 seconds</li> <li>• To change the timeout, go to <b>Call Options &gt; Calling Delay(s)</b>.</li> </ul> <p><b>When Auto Answer is enabled:</b> If a call is received via the app and the <b>Auto-Answer Delay</b> is set to 10 seconds, the call screen will appear, allowing you time to answer manually. If no action is taken, the system will automatically answer the call after 10 seconds.</p> <ul style="list-style-type: none"> <li>• <b>Default Auto-Answer Delay:</b> 0 seconds (immediate answer)</li> <li>• User can adjust this setting in the <b>Call Options</b> menu</li> </ul>
<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. The default is 0 seconds.
<b>Encryption</b>	It is disabled by default.

**11.1.5 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 enter the Add Contact List interface.

Contact List		
Add		
101		192.168.1.101
102		192.168.1.102
103		192.168.1.103
104		192.168.1.104
105		192.168.1.105

Add	
Room Number	
Call Address	

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

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

Room Number	
102	

Entrance Station

Room Number	
00.00.0000	


Fence Terminal

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

## 11.1.6 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.

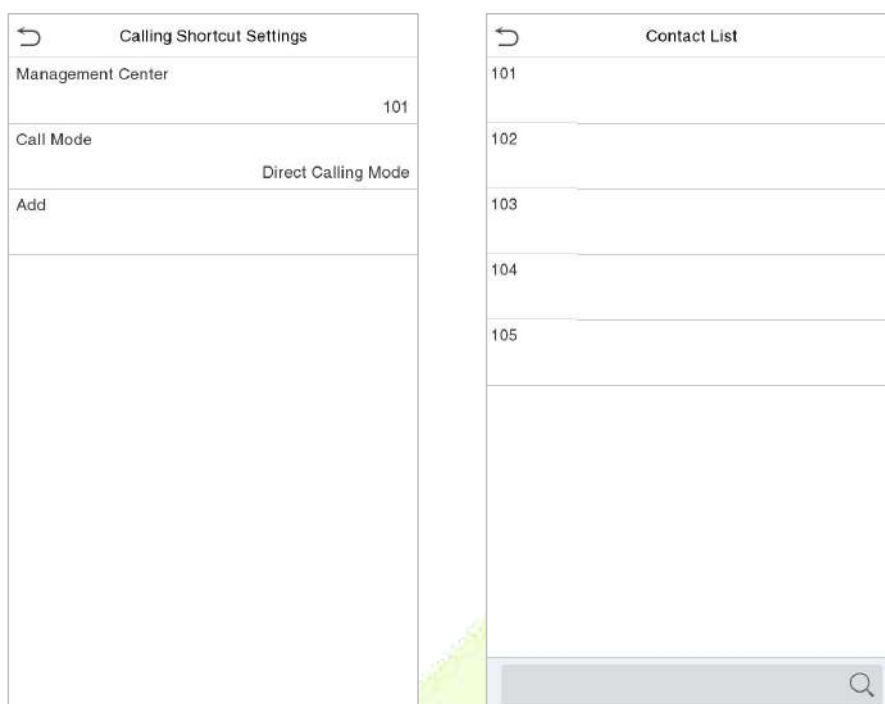
**Name:** Customize the name of the shortcut keys.

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

Number : 102	
Enable	<input checked="" type="checkbox"/>
Name	ROOM1
Number	102

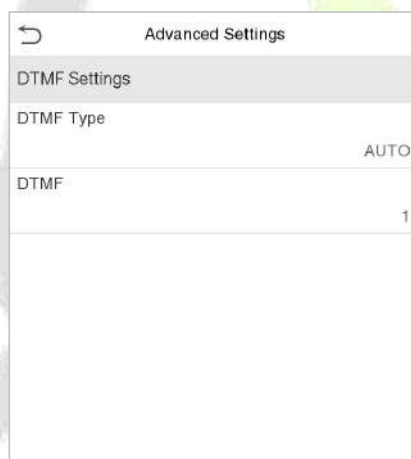
- In Direct Calling mode, the user can call multiple indoor monitors directly.

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



### 11.1.7 Advanced Settings

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

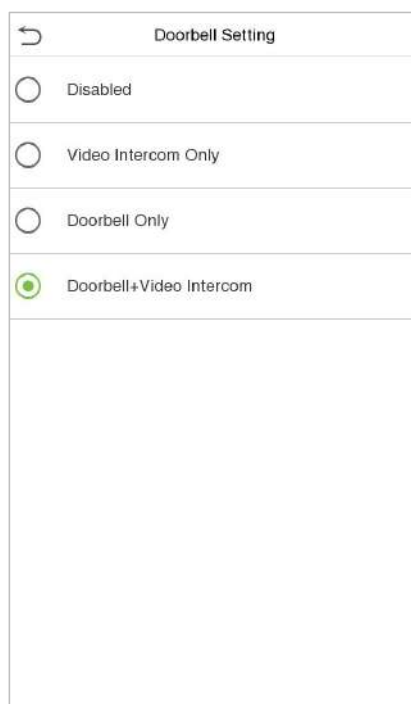


#### **Function Description**







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.

## 11.2 Doorbell Setting

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





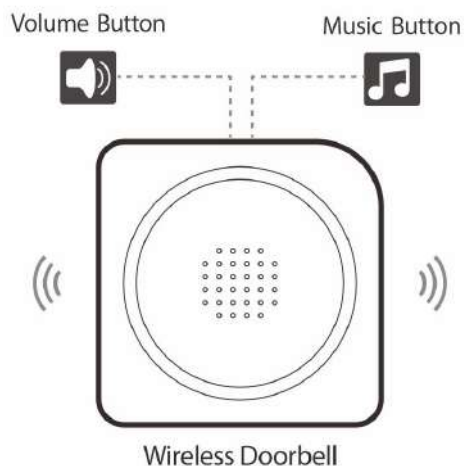
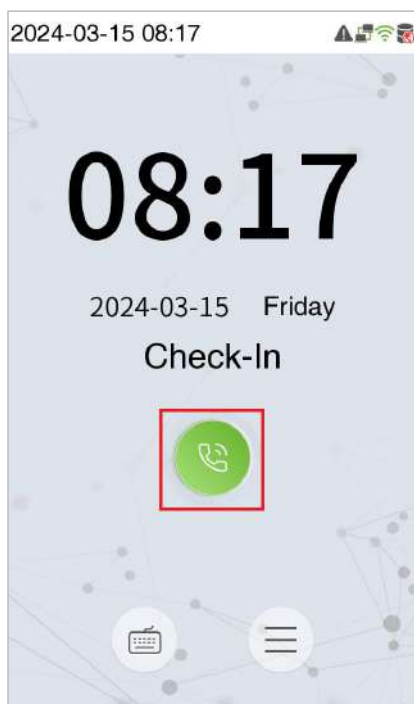
### Function Description

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

### 11.2.1 Connect the Wireless Doorbell ★

**Note:** This function needs to be used with the wireless doorbell.


- First, power on the wireless doorbell. Then, press and hold the music button  for 1.5 seconds until the indicator flashes to indicate it's in pairing mode. After that, click on the BioFace D1 device icon , if the wireless doorbell rings and the indicator flashes, it means the connection is successful.



- After a successful pairing, clicking the icon  of BioFace D1 device will ring the wireless doorbell.

**Note:** Generally, each BioFace D1 device connects to wireless doorbell.

### ● Unbinding the Wireless Doorbell

Power off the wireless doorbell first, then re-installing the batteries while pressing and holding the music button  until the indicator is on, indicating that the unbinding is successful.

## 11.3 ONVIF Settings

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

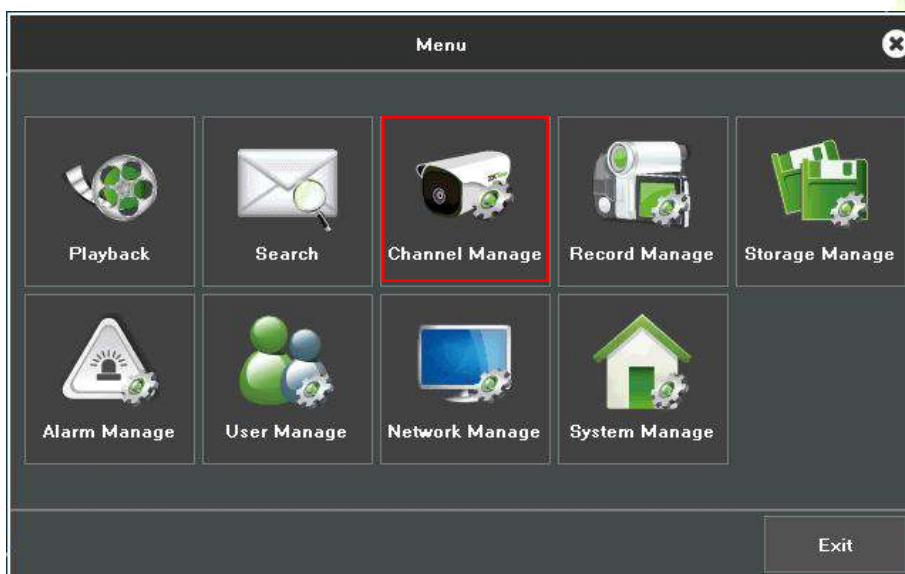
- Set the device to the same network segment as the NVR.
- Tap **ONVIF Settings** on the **Video intercom Parameters** interface.

ONVIF Settings	
Enable Authentication	<input checked="" type="checkbox"/>
User Name	admin
Password	*****
Server Port	8000

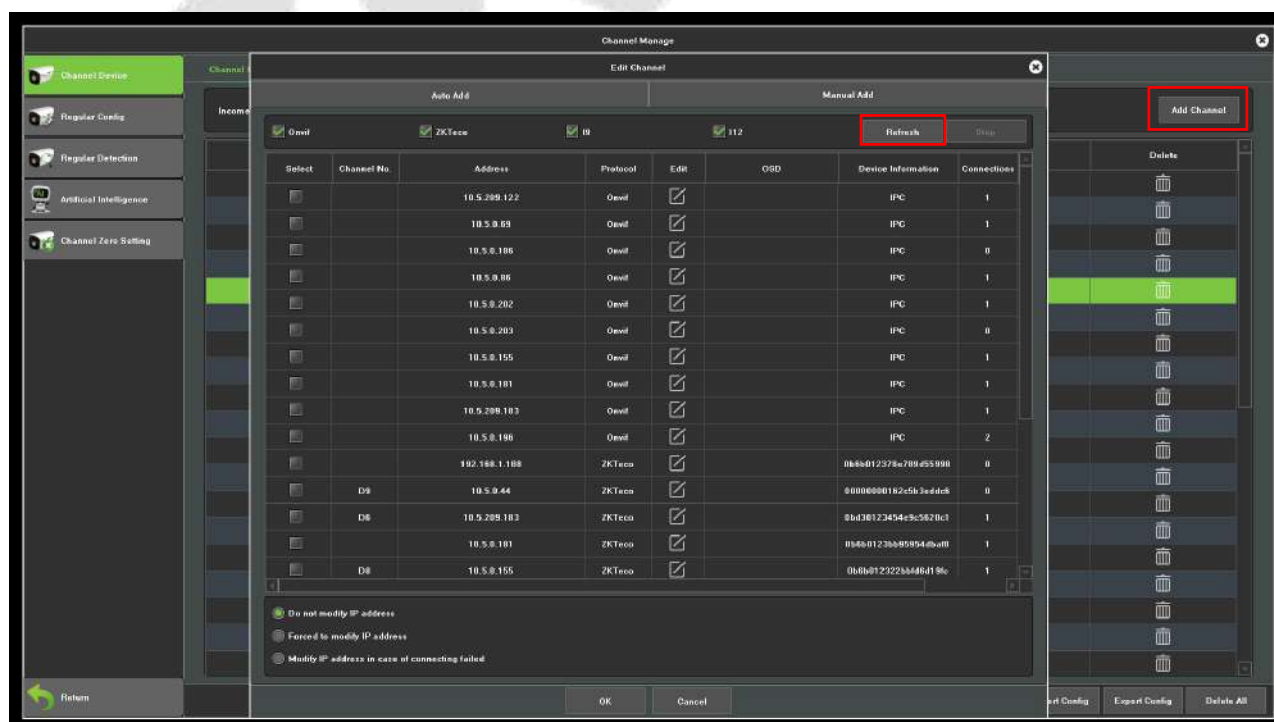
## Function Description

Function Name	Description
<b>Enable Authentication</b>	Enable/Disable the Authentication Function. When it is disabled, there is no need to input the User Name and Password when adding the device to the NVR.
<b>User Name</b>	Set the User Name. 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.

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

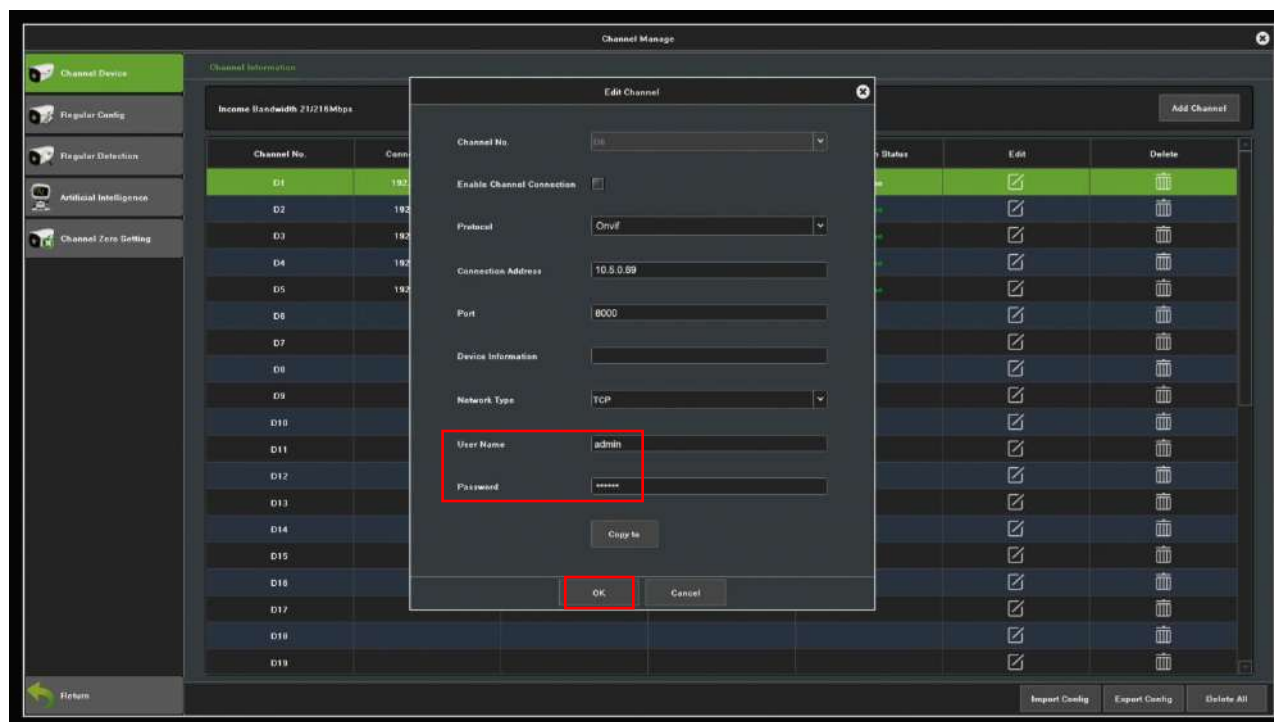


4. Click **[Channel Manage]** > **[Add Channel]** > **[Refresh]** to search for the device.



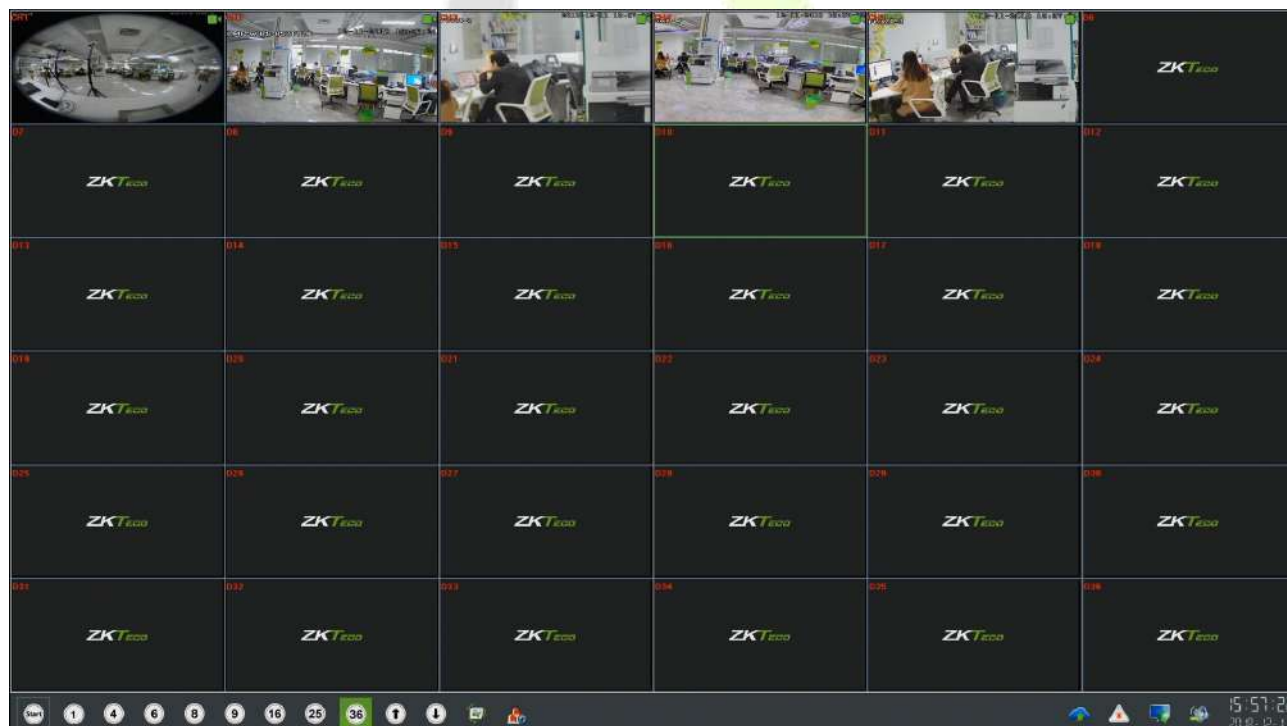


- Select the checkbox for the device you want to add and edit the parameters in the corresponding text field, then click on **[OK]** to add it to the connection list.



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

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

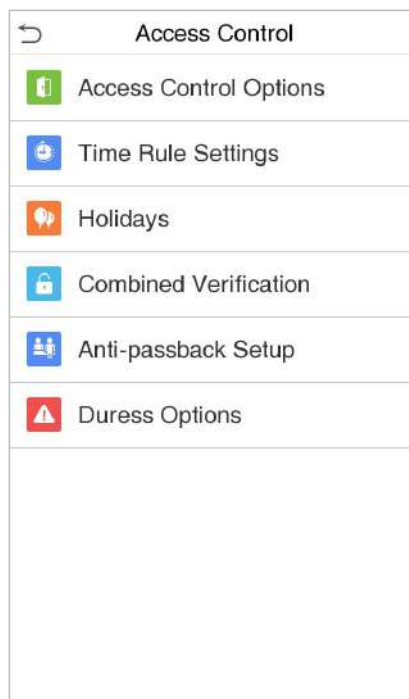


For more details, please refer to the **NVR User Manual**.



## 12. 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.



- **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.

## 12.1 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 Opti...	1↓
Gate Control Mode	<input type="checkbox"/>
Door Lock Delay(s)	5
Door Sensor Delay(s)	10
Door Sensor Type	Normal Close(NC)
Verification Mode	Password/Fingerprint/Card/Face
Door Available Time Period	1
Normal Open Time Period	None
Master Device	In
Slave Device	Out
Auxiliary Input Configuration	

Access Control Opti...	1↓
Door Sensor Type	Normal Close(NC)
Verification Mode	Password/Fingerprint/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	

### Function Description

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</b> : It means the door is always left opened when electric power is on. <b>Normal Closed</b> : It means the door is always left closed when electric power is on.
<b>Verification Mode</b>	The supported verification mode includes Password/Fingerprint/Card/Face, Fingerprint Only, User ID Only, Password, Card Only, Fingerprint/Password, Fingerprint/Card, User ID + Fingerprint, Fingerprint + Password, Fingerprint + Card, Fingerprint + Password + Card, Password + Card, Password/Card, User ID + Fingerprint + Password, Fingerprint + (Card/User ID), Face Only, Face + Fingerprint, Face + Password, Face + Card, Face + Fingerprint+ Card, and Face + Fingerprint + Password.

<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.

## 12.2 Time Rule Setting

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...]
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...]
Holiday Type 1	[00:00 23:59...]
Holiday Type 2	[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	00	23	59
▼	▼	▼	▼
HH	MM	HH	MM
Confirm (OK)		Cancel (ESC)	

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

**Notes:**

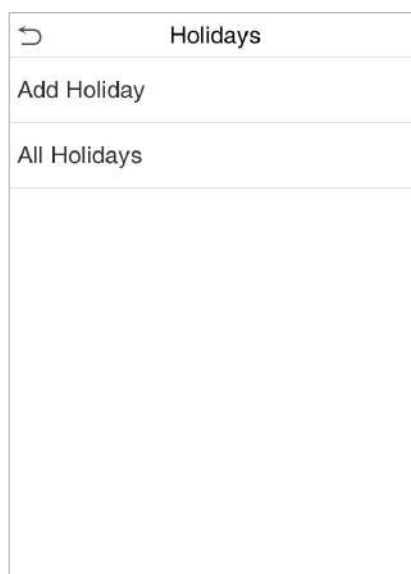
- When the End Time is earlier than the Start Time, (such as 23:57~23:56), it indicates that access is prohibited all day.
- When the End Time is later than the Start Time, (such as 00:00~23:59), it indicates that the interval is valid.

- The effective Time Period to keep the Door Unlock or open all day is (00:00~23:59) or also when the Ending Time is later than the Starting Time, (such as 08:00~23:59).
- The default Time Zone 1 indicates that door is open all day long.

## 12.3 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.

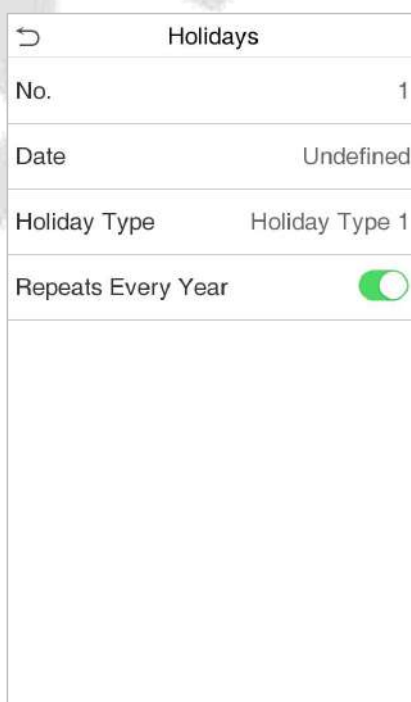
Tap **Holidays** on the **Access Control** interface to set the Holiday access.



The screenshot shows a mobile application interface titled 'Holidays'. At the top, there is a back arrow icon and the title 'Holidays'. Below the title, there are two options: 'Add Holiday' and 'All Holidays'. The rest of the screen is empty, suggesting a list of holidays.

- **Add a new holiday:**

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



The screenshot shows a mobile application interface for adding a new holiday. It has a title bar with a back arrow and 'Holidays'. Below the title bar, there are four rows of input fields: 'No.' with the value '1', 'Date' with the value 'Undefined', 'Holiday Type' with the value 'Holiday Type 1', and 'Repeats Every Year' with a green toggle switch. The bottom of the screen is empty.

- **Edit a holiday:**

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

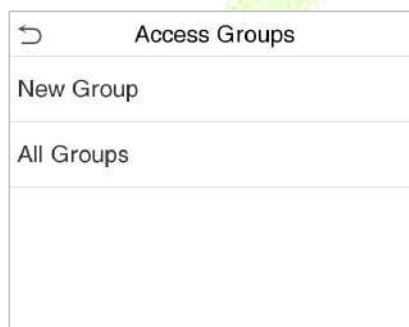
- **Delete a Holiday:**

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.

## 12.4 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.



- **Add a New Group**

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

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

**Notes:**

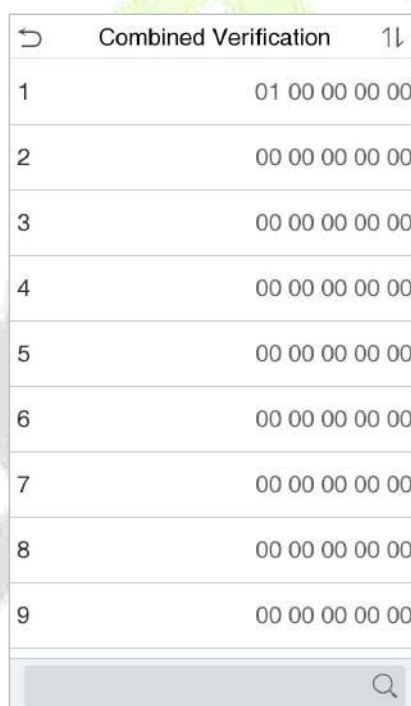
- This function is only used under attendance push (T&A PUSH).
- There is a default access group numbered 1, which cannot be deleted, but can be modified.
- A number cannot be modified after being set.
- When the holiday is set to be valid, personnel in a group may only open the door when the group time 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.

## 12.5 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

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.

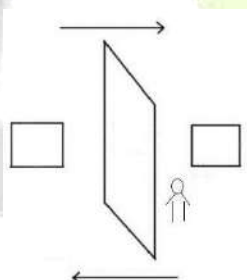
- **Delete a Door-unlocking Combination:**

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

## 12.6 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.

Anti-passback Setup	
Anti-passback Direction	No Anti-passback



## 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>

## 12.7 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	<input type="checkbox"/>
Alarm on 1:1 Match	<input type="checkbox"/>
Alarm on 1:N Match	<input type="checkbox"/>
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 on 1:1 Match</b>	When a user uses any fingerprint to perform the 1:1 verification, an alarm signal will be generated, otherwise there will be no alarm signal.
<b>Alarm on 1:N Match</b>	When a user uses any fingerprint to perform 1:N verification, 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.

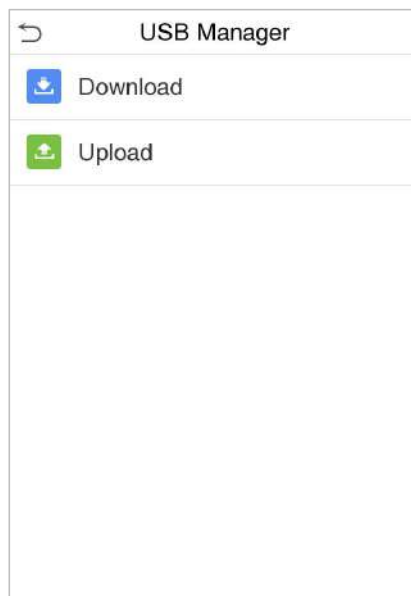
## 13. USB Manager

You can import the user information, and attendance data in the machine to matching attendance software for processing by using a USB disk, or import the user information to other devices for backup.

Before uploading/downloading data from/to the USB disk, insert the USB disk into the USB slot first.

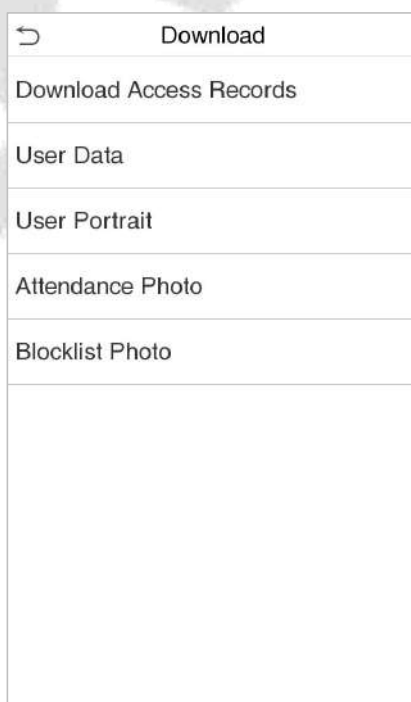
**Note:** Only FAT32 format is supported when downloading data using USB disk.

Tap **USB Manager** on the main menu interface.



### 13.1 USB Download

On the **USB Manager** interface, tap **Download**.

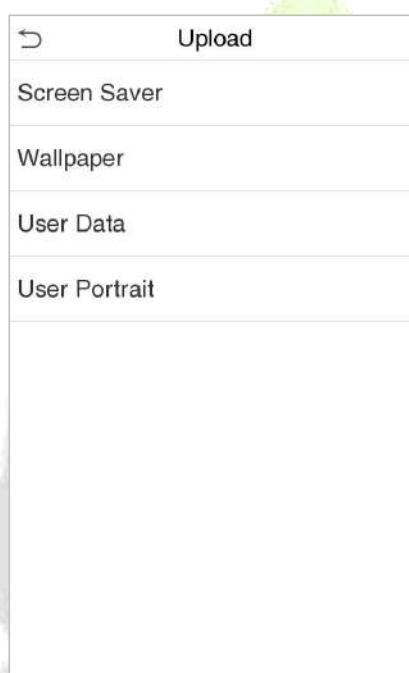


## Function Description

Function Name	Description
<b>Download Access Records</b>	To download all access records in specified time period into USB disk.
<b>User Data</b>	To download all user information from the device into USB disk.
<b>User Portrait</b>	To download all user portraits from the device into USB disk.
<b>Attendance Photo</b>	To download all attendance photos from the device into USB disk.
<b>Blocklist Photo</b>	To download all blocklisted photos (photos taken after failed verifications) from the device into USB disk.

## 13.2 USB Upload

On the **USB Manager** interface, tap **Download**.



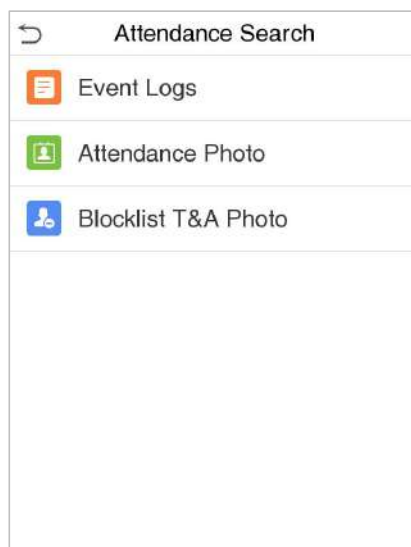
## Function Description

Function Name	Description
<b>Screen Saver</b>	To upload all screen savers from USB disk into the device. You can choose Upload selected photo or upload all photos. The images will be displayed on the device's main interface after upload.
<b>Wallpaper</b>	To upload all wallpapers from USB disk into the device. You can choose Upload selected photo or upload all photos. The images will be displayed on the screen after upload.
<b>User Data</b>	To upload all the user information from USB disk into the device.
<b>User Portrait</b>	To upload all user portraits from USB disk into the device.

## 14. 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.

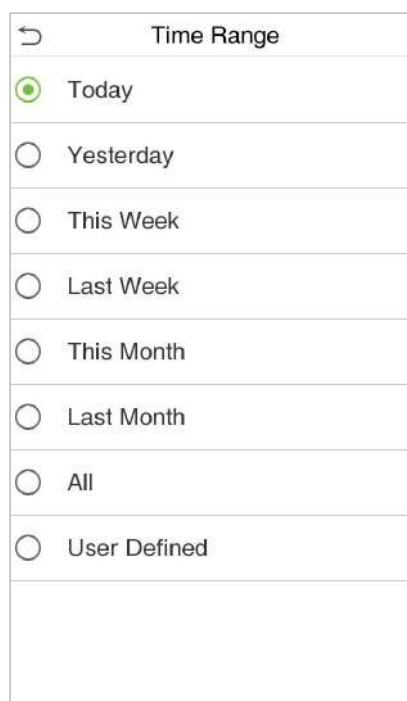
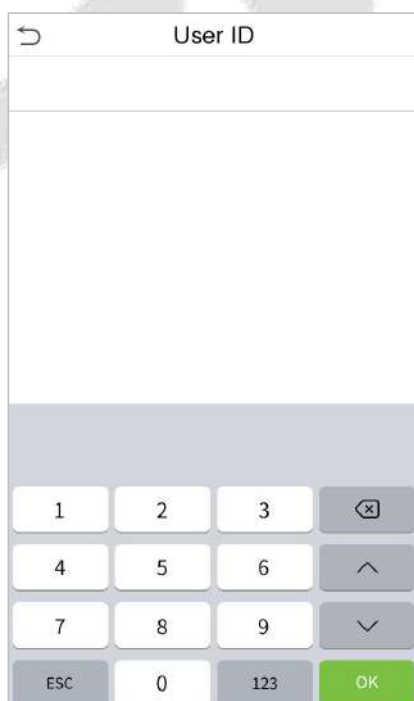
Click **Attendance Search** on the **Main Menu** interface to search for the required Access/Attendance log.



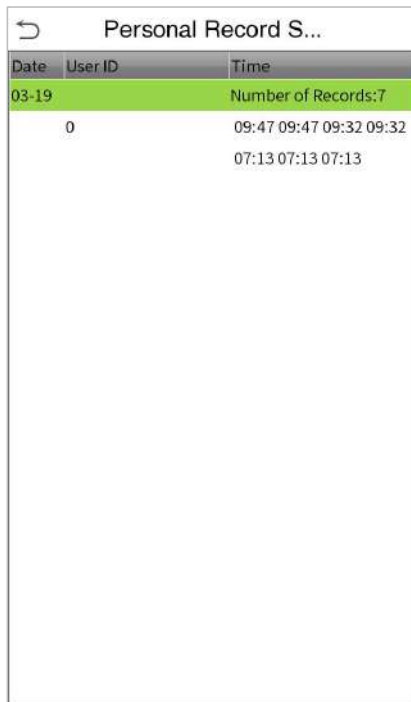
The process of searching for attendance and blocklist photos is similar to that of searching for event logs. The following is an example of searching for event logs.

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.

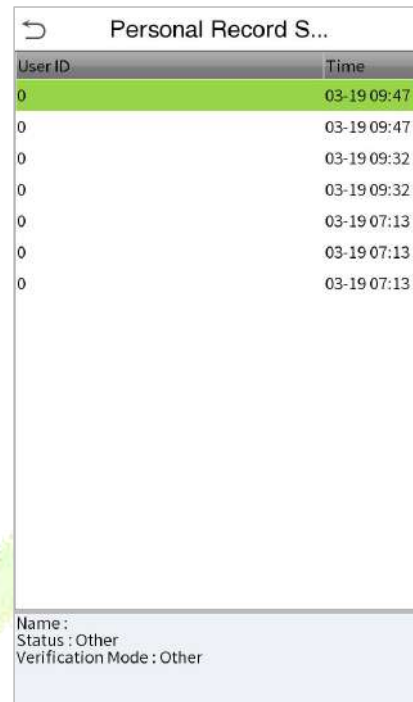


3. Once the log search succeeds. Tap the login highlighted in green to view its details.



Date	User ID	Time
03-19		Number of Records:7
	0	09:47 09:47 09:32 09:32 07:13 07:13 07:13

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

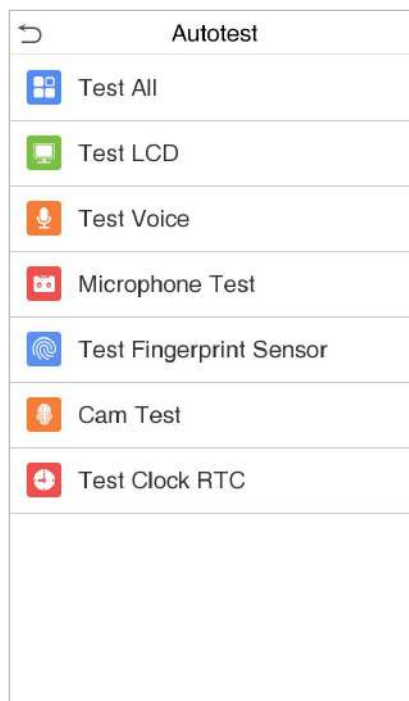


User ID	Time
0	03-19 09:47
0	03-19 09:47
0	03-19 09:32
0	03-19 09:32
0	03-19 07:13
0	03-19 07:13
0	03-19 07:13

Name :  
Status : Other  
Verification Mode : Other

## 15. 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).

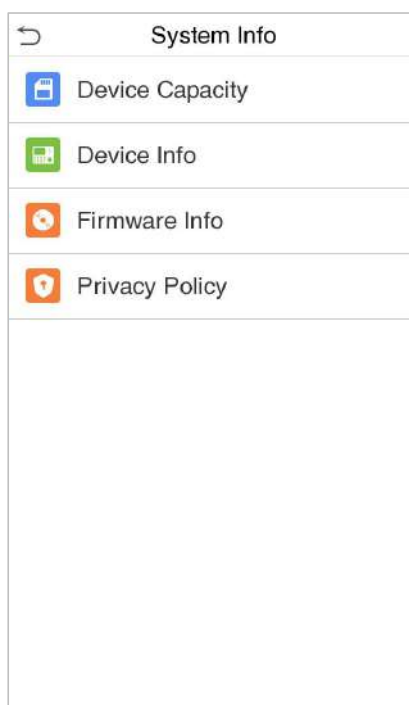


### Function Description

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.

## 16. 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, fingerprint 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, fingerprint algorithm★, 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>



## 17. Connect to ZKBio CVSecurity Software

### 17.1 Set the Communication Address

#### ● Device Side

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

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

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

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

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

Ethernet		Cloud Server Settings	
Display in Status Bar	<input checked="" type="checkbox"/>	Server Mode	ADMS
IPv4		Enable Domain Name	<input type="checkbox"/>
IP Address	192.168.163.199	Server Address	192.168.163.61
Subnet Mask	255.255.255.0	Server Port	8081
Gateway	192.168.163.1	Enable Proxy Server	<input type="checkbox"/>
DNS	0.0.0.0		
DHCP	<input type="checkbox"/>		

#### ● Software Side

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

System Management > System / Communication Management / Communication Monitor

Adms Service Settings

Adms Service Port: 8088

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

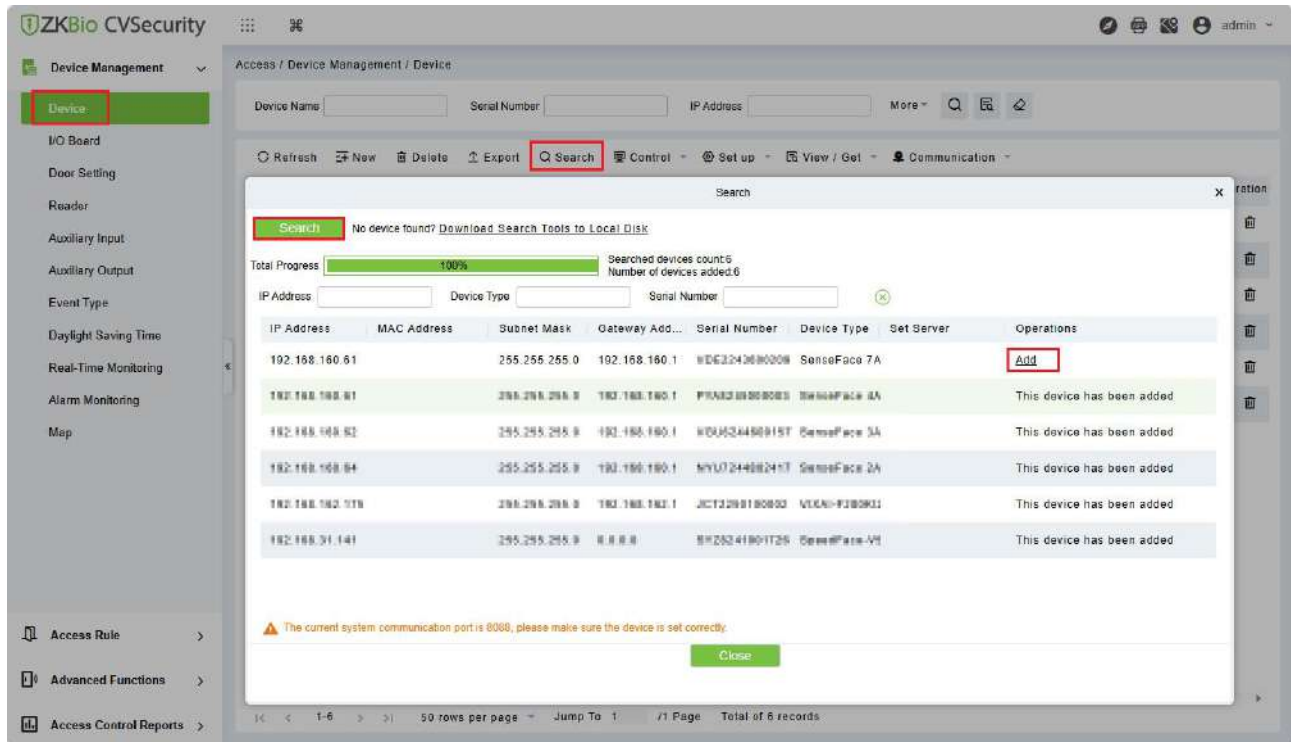
Project control file version: None

Turn on encrypted transmission: ☐ No ☒ Yes

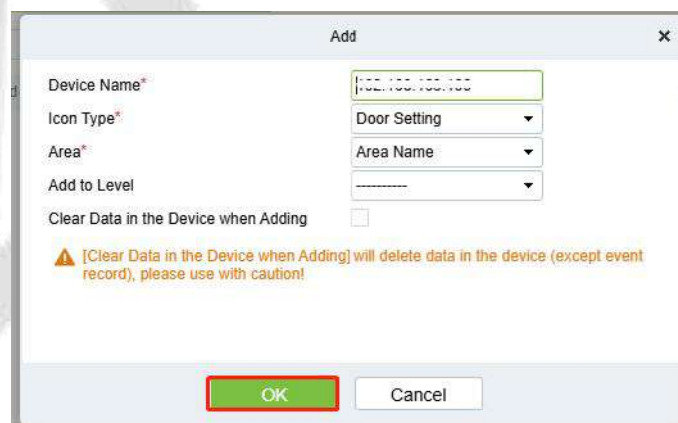
## 17.2 Add Device on the Software

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.



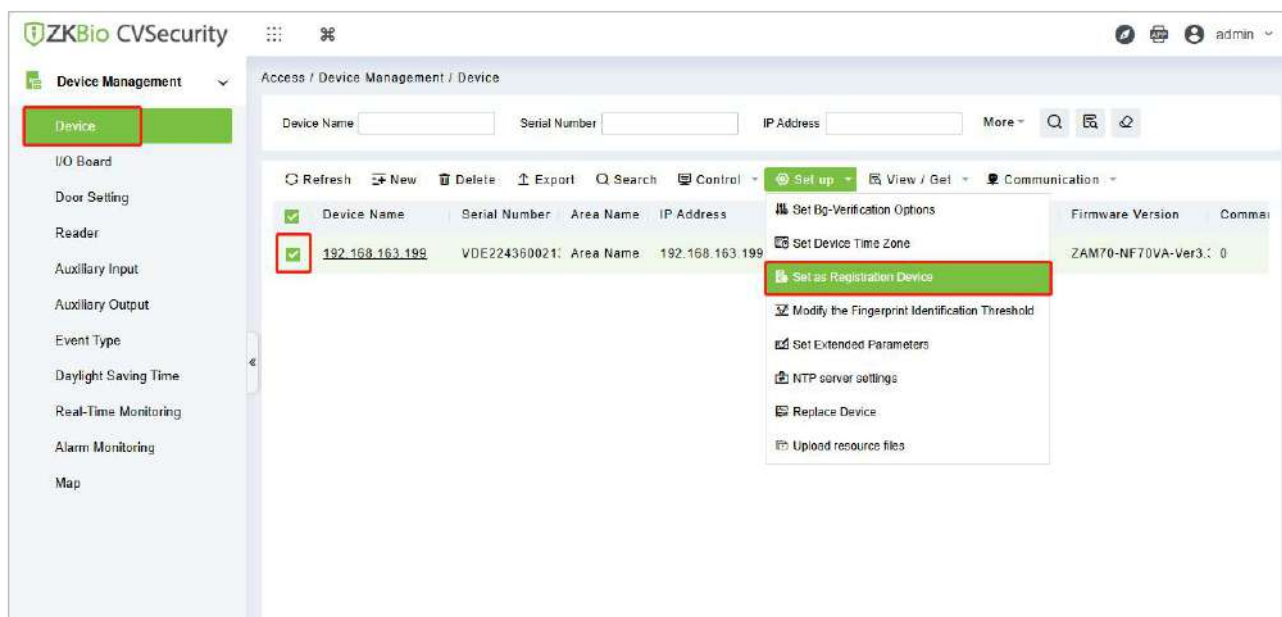
4. Click **Add** in operation column, a new window will pop-up. Select Icon type, Area, and Add to Level from each dropdown and click **OK** to add the device.



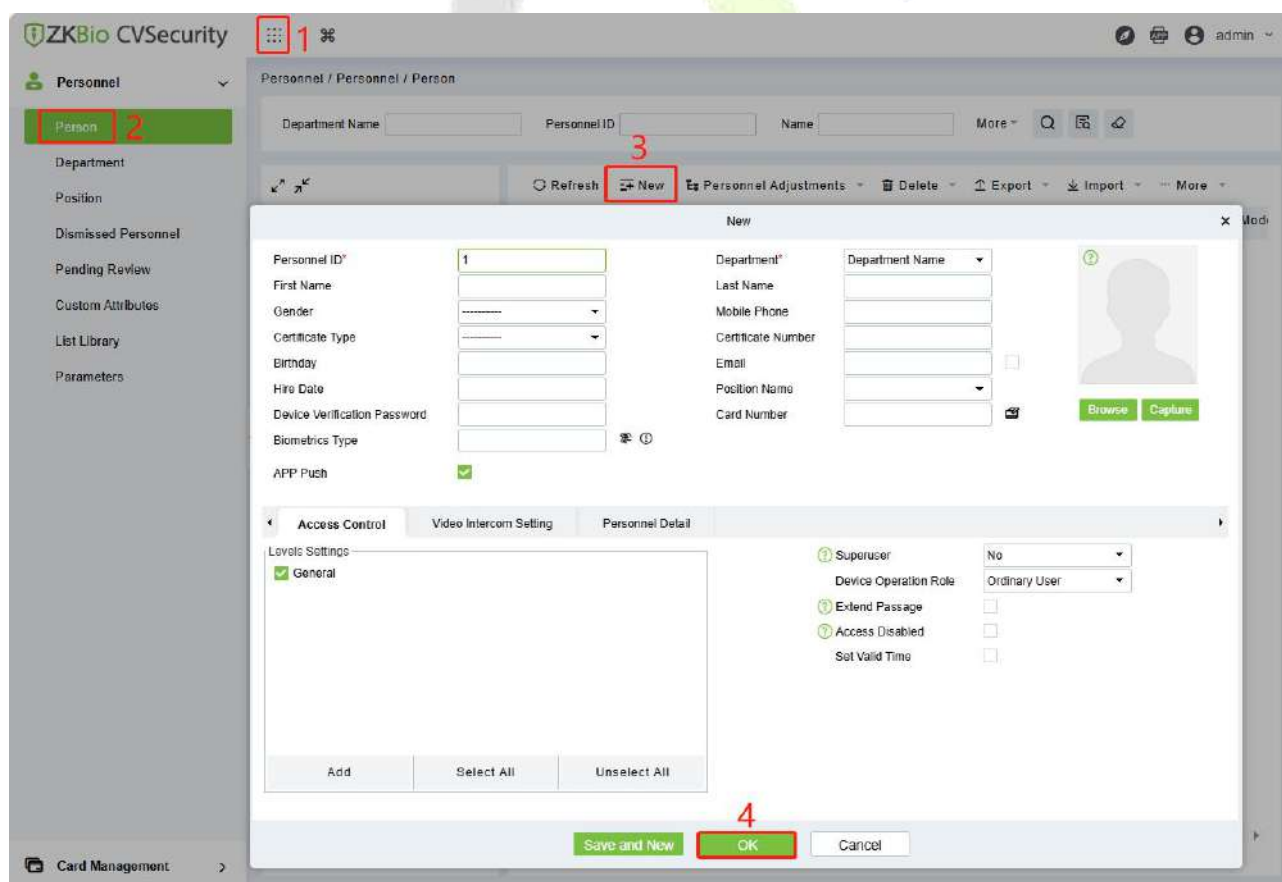
5. After the addition is successful, the device will be displayed in the device list.


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

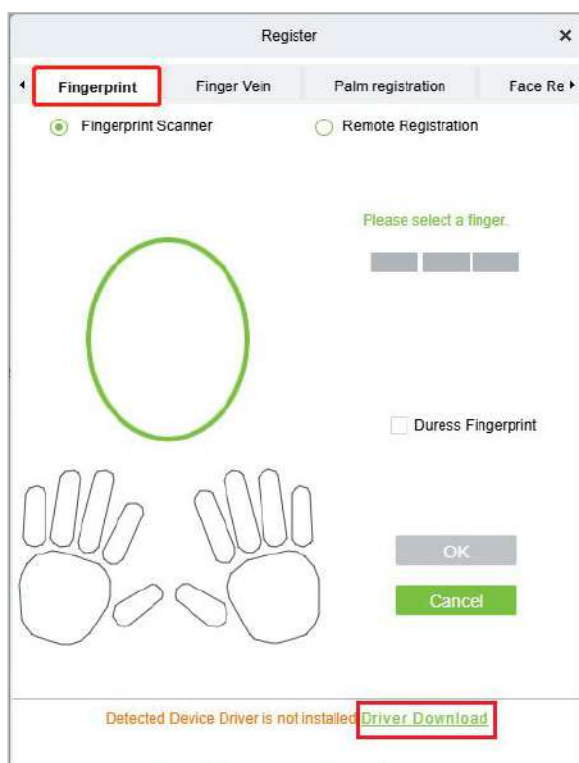
1. In the device list, select the device and click **Set up > Set as Registration Device**.



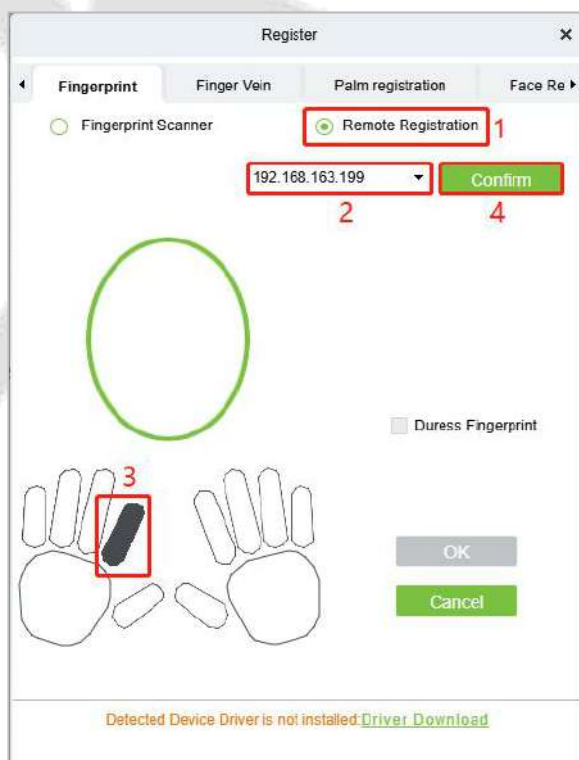
2. Click **Personnel > Person > New**:



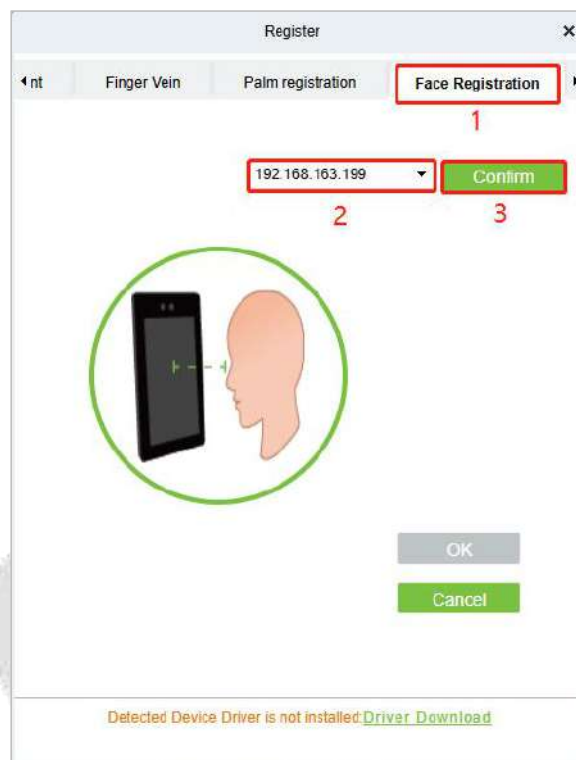
3. Fill in all the required fields of the user and click  and select **Fingerprint** to enter the online fingerprint registration interface
4. Click **Driver Download** to install the driver first.



5. Select **Remote Registration**, then select the IP address of the device and the finger you want to register, click **Confirm**.



6. After the device prompts "Please press your finger", press your finger on the fingerprint sensor of the device three times. If the fingerprint is successfully registered, the device will prompt "Registered successfully".
7. If you want to register a duress fingerprint, you can click **Duress Fingerprint** before registering the fingerprint.
  - **Duress fingerprint:** In any case, a duress alarm is generated when a fingerprint matches a duress fingerprint.
8. Click **Face Registration** to enter the online face registration interface. Select the IP address of the device and click **Confirm**.



9. After the device prompts "Face registration begin", face towards the camera and keep the face in the centre of the screen and stay still during face registration. If the face is successfully registered, the device will prompt "Registered successfully".
10. Click **OK** to save the user.
11. 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*.

## 18. Connect to ZKBioTime Software

### 18.1 Set the Communication Address

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

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

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

**Server address:** Set the IP address as of ZKBio Time server.

**Server port:** Set the server port as of ZKBio Time (The default is 8081).

Ethernet
Display in Status Bar
IPv4
IP Address 192.168.163.199
Subnet Mask 255.255.255.0
Gateway 192.168.163.1
DNS 0.0.0.0
DHCP

Cloud Server Settings
Server Mode ADMS
Enable Domain Name
Server Address 192.168.163.61
Server Port 8081
Enable Proxy Server

### 18.2 Add Device on the Software

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

1. Click **Device > Device > Add**, to add the device on the software.
2. A new window pops-up on clicking **Add**. Enter the required information about the device and click **Confirm**, then the added devices are displayed automatically.

The screenshot shows the ZKTECO software interface with the 'Device' tab selected. An 'Add' dialog box is open, allowing users to input device details. The fields include:

- Device Name: # Fkx#
- Serial Number: 669021300\*\*\*\*
- Area: TEST
- Attendance Device: Yes
- Request Heartbeat: 10 Seconds
- Enable Access Control: Yes
- Device IP: 192.168.163.199
- Timezone: Rtc/SMT+8
- Registration Device: No
- Transfer Mode: Real-Time

The 'Confirm' button is highlighted in green at the bottom right of the dialog box.



## 18.3 Add Personnel on the Software and Online Fingerprint Registration

1. Click **Personnel** > **Employee** > **Add**:

The screenshot shows the ZKTeco software interface. The top navigation bar includes 'Personnel', 'Device', 'Attendance', 'Access Control', 'Payroll', 'Visitor', 'Meeting', 'MTD', and 'System'. The left sidebar has 'Organization', 'Employee', 'Resign', 'Workflow', and 'Configurations'. The 'Employee' menu item is highlighted. The main area displays the 'Add Employee' form. The 'Profile' tab is selected, showing fields for Employee ID, First Name, Last Name, Department, Position, Area, Employment Type, Hired Date, Superior, and Workflow Role. A 'Confirm' button is highlighted in the bottom right corner.

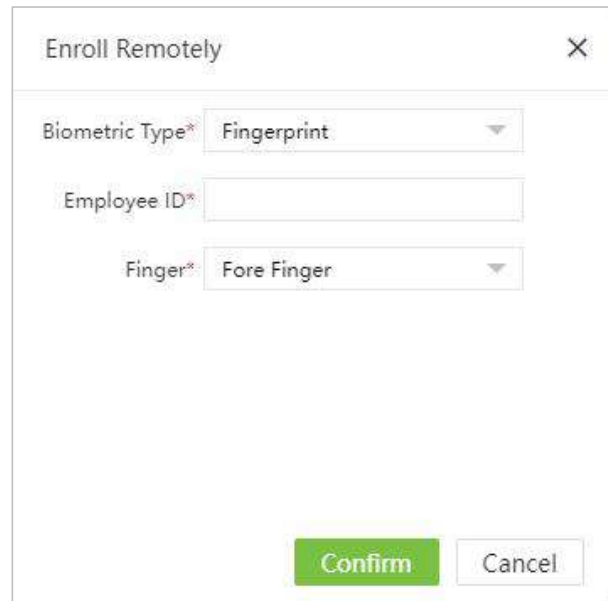
2. Fill in all the required fields and click **Confirm** to register a new user.

3. Click **Device** > **Device**, select the device and click **Device Menu** > **Enroll Remotely**.

The screenshot shows the ZKTeco software interface. The top navigation bar includes 'Personnel', 'Device', 'Attendance', 'Access Control', 'Payroll', 'Visitor', 'Meeting', 'MTD', and 'System'. The left sidebar has 'Device', 'Device Command', 'Message', 'Data', 'Log', 'Mobile App', 'Geo-fence', and 'Configurations'. The 'Device' menu item is highlighted. The main area displays a table of devices. The 'Device Menu' dropdown is open, and the 'Enroll Remotely' option is highlighted.

Device Name	Serial Number	Area	Device IP	State	Last Active	Reboot	Read Information	Enroll Remotely	Duplicate Punch Period	Capture Setting	Upgrade Firmware	Daylight Saving Time
✓	8117232240002	Floor 6	192.168.163.129	✓	2023-08-1		0	0				

4. Enter the Employee ID and select the finger you want to register and press your finger on the fingerprint sensor of the device three times. If the fingerprint is successfully registered, the device will prompt "Enrolled successfully".



The screenshot shows a dialog box titled "Enroll Remotely" with a close button (X) in the top right corner. Inside the dialog, there are three labeled fields: "Biometric Type\*" with a dropdown menu currently set to "Fingerprint", "Employee ID\*" with an empty text input field, and "Finger\*" with a dropdown menu currently set to "Fore Finger". At the bottom of the dialog, there are two buttons: a green "Confirm" button and a white "Cancel" button with a grey border.

5. Click **Device > Device > Data Transfer > Sync Data to the Device** to synchronize all the data to the device including the new users.

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



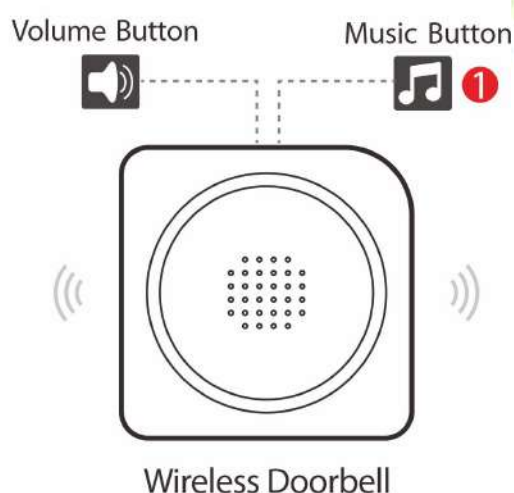
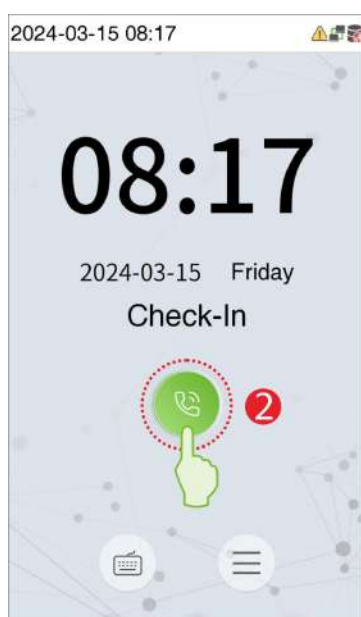
## 19. Connecting to Wireless Doorbell★



**Note:** This function needs to be used with the wireless doorbell.

### 19.1 Connect the Wireless Doorbell

1. First, power on the wireless doorbell. Then, press and hold the music button for 1.5 seconds until the indicator flashes to indicate it's in pairing mode. After that, press the doorbell button on the device, if the wireless doorbell rings and the indicator flashes, it means the pairing was successful.



2. After a successful pairing, press the doorbell button on the device will ring the wireless doorbell.

**Note:**

- 1) To use this function, you need to enter the menu ([**Intercom**] > [**Doorbell Setting**]) and set it as **Doorbell Only** or **Doorbell + Video Intercom**.
- 2) Each BioFace D1 only supports one wireless doorbell.
- 3) Wireless doorbell needs to be purchased by the customers themselves.

### 19.2 Unbinding the Wireless Doorbell

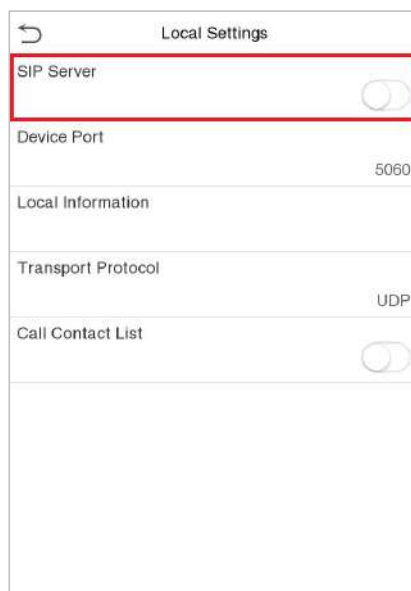
Power off the wireless doorbell first, then re-installing the batteries while pressing and holding the music button until the indicator is on, indicating that the unbinding is successful.

## 20. SIP Video Intercom

### 20.1 Local Area Network Use


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

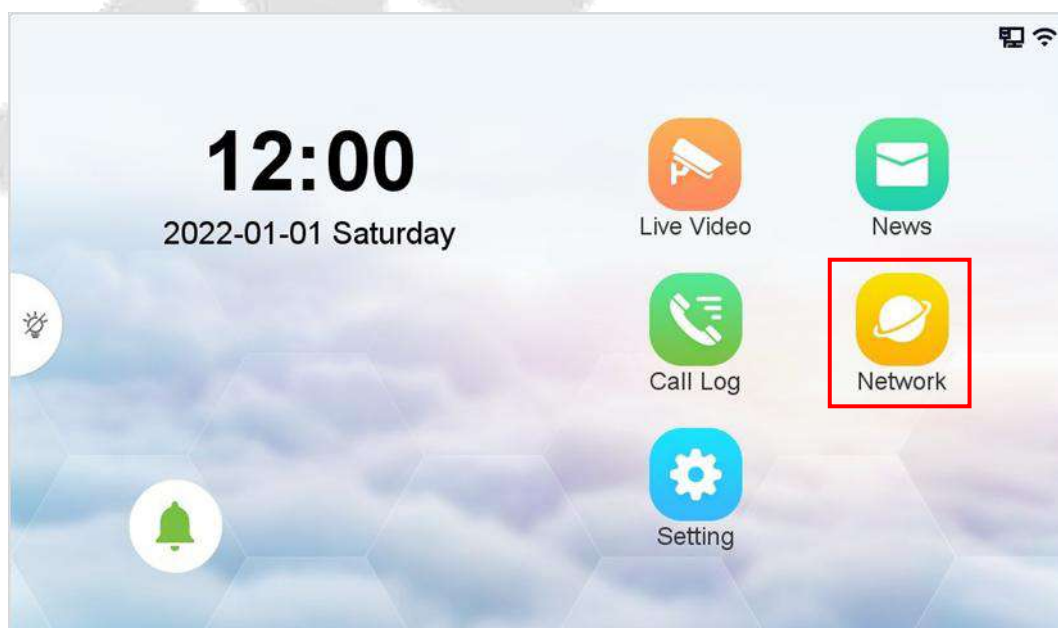
Click **Intercom** > **SIP Settings** > **Local Settings** to turn off the SIP server.



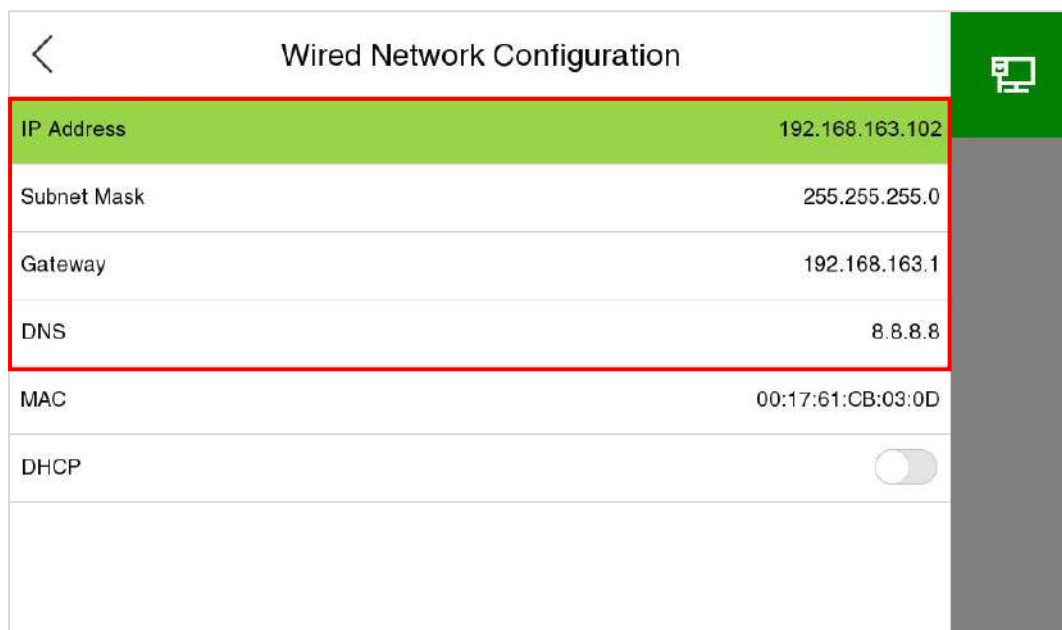
This function needs to be used with the indoor monitor VT07-B01.

- **On the Indoor Monitor:**

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



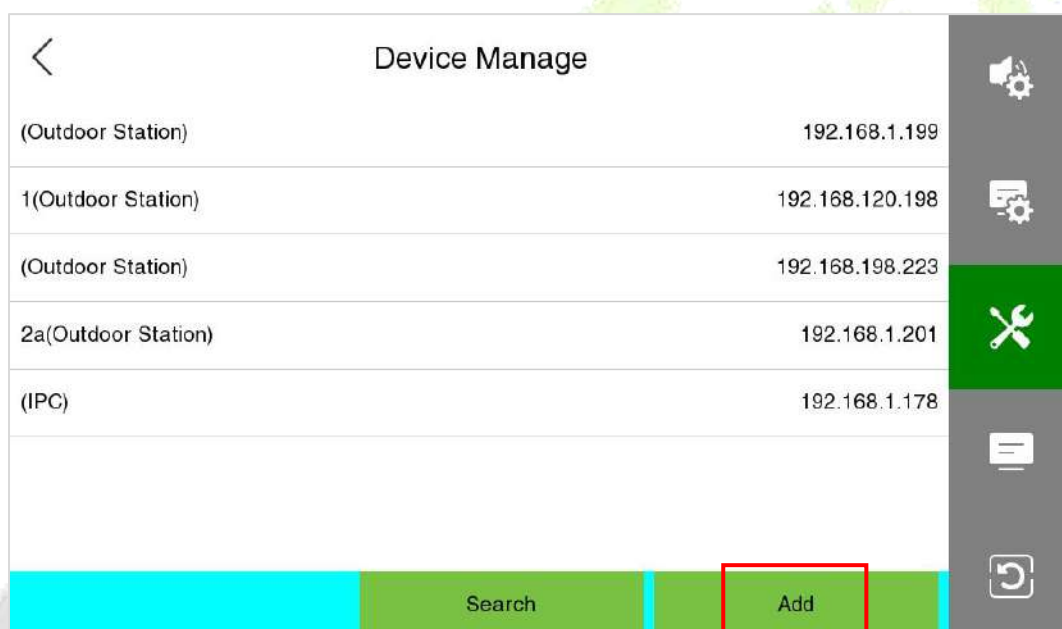
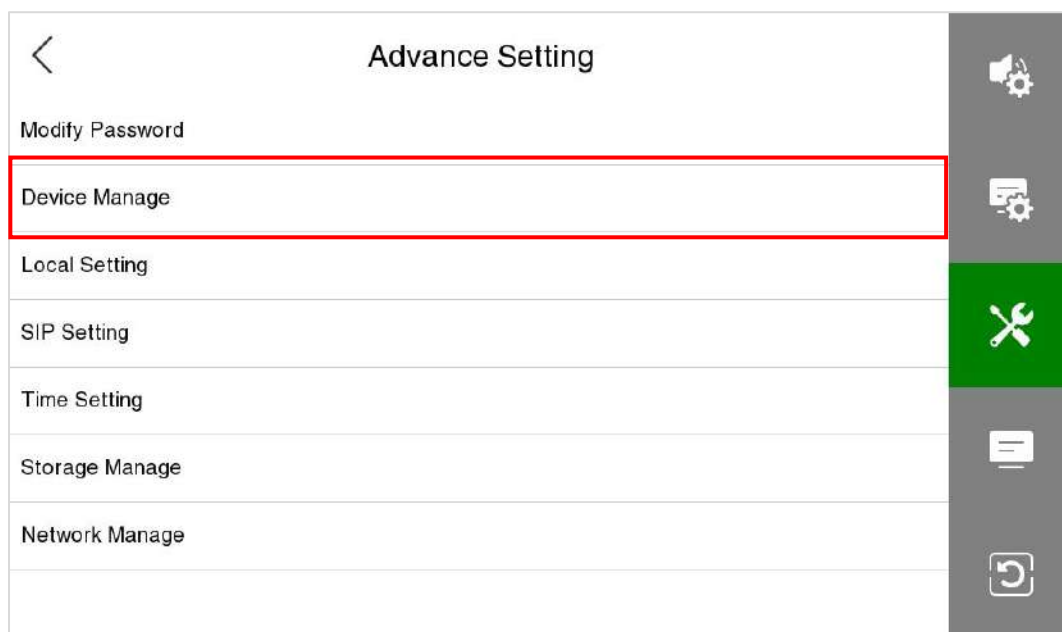
2. Set the IP Address and Gateway of the indoor monitor. (**Note:** The IP address should be in the same network segment as the device.)



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.

**User Name:** 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	Contact List	Add
<div>SIP Settings</div> <div>Doorbell Setting</div> <div>ONVIF Settings</div>	<div>Local Settings</div> <div>Audio Options</div> <div>Video Options</div> <div>Call Options</div> <div>Contact List</div> <div>Calling Shortcut Settings</div> <div>Advanced Settings</div>	<div>Add</div> <div>101 192.168.1.101</div> <div>102 192.168.1.102</div> <div>103 192.168.1.103</div> <div>104 192.168.1.104</div> <div>105 192.168.1.105</div>	<div>Room Number</div> <div>Call Address</div>

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

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




Entrance Station



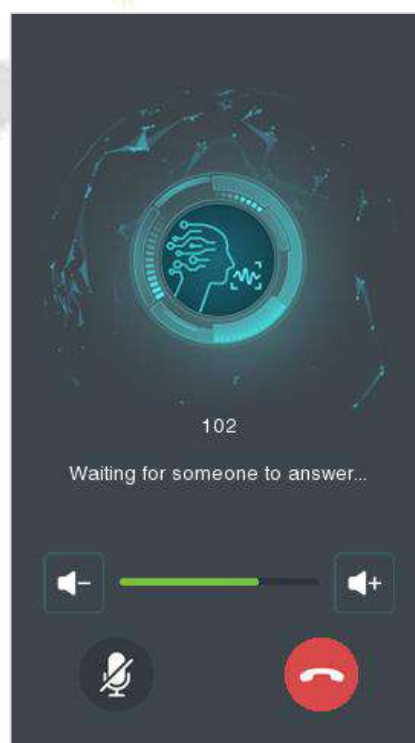
Fence Terminal

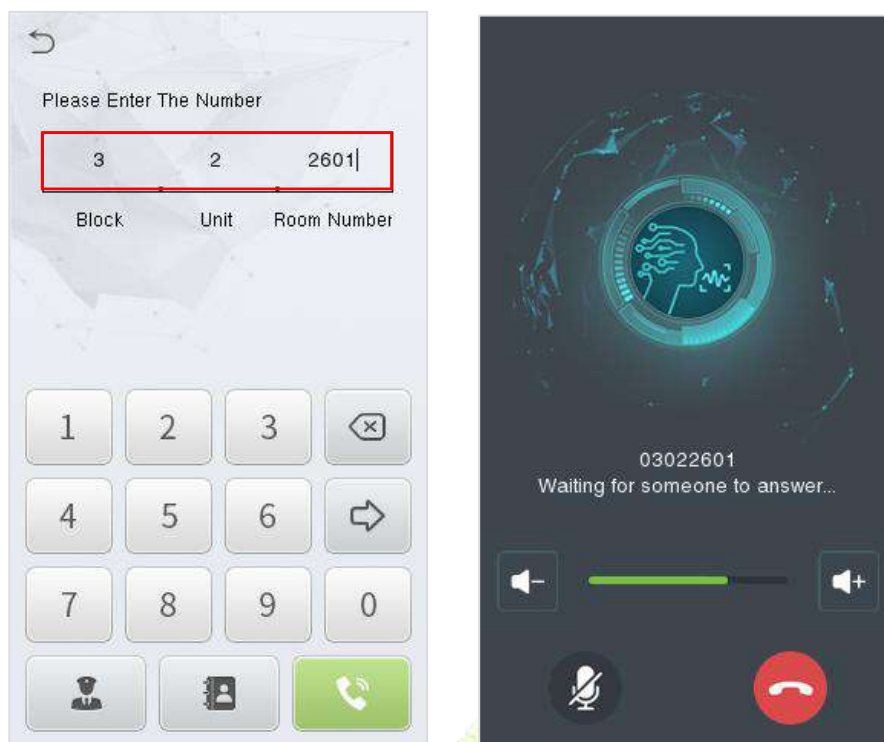
**Call Address:** It is the IP Address of the indoor monitor.

- 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.

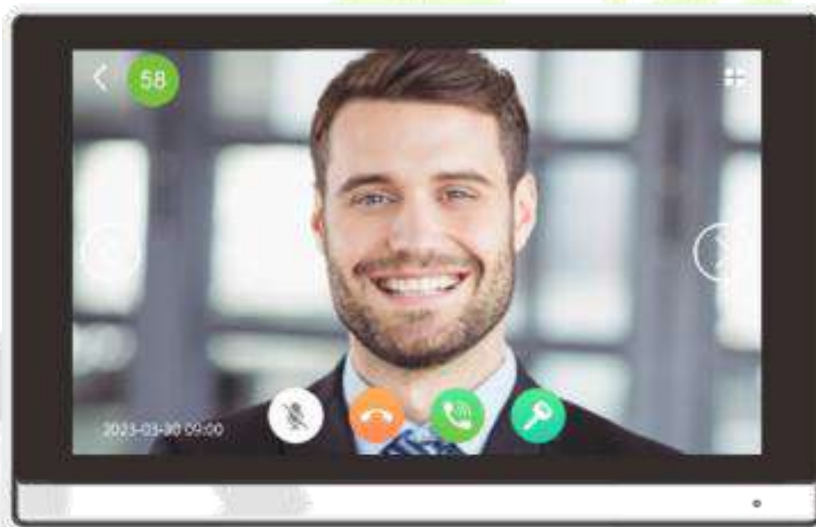


Entrance Station





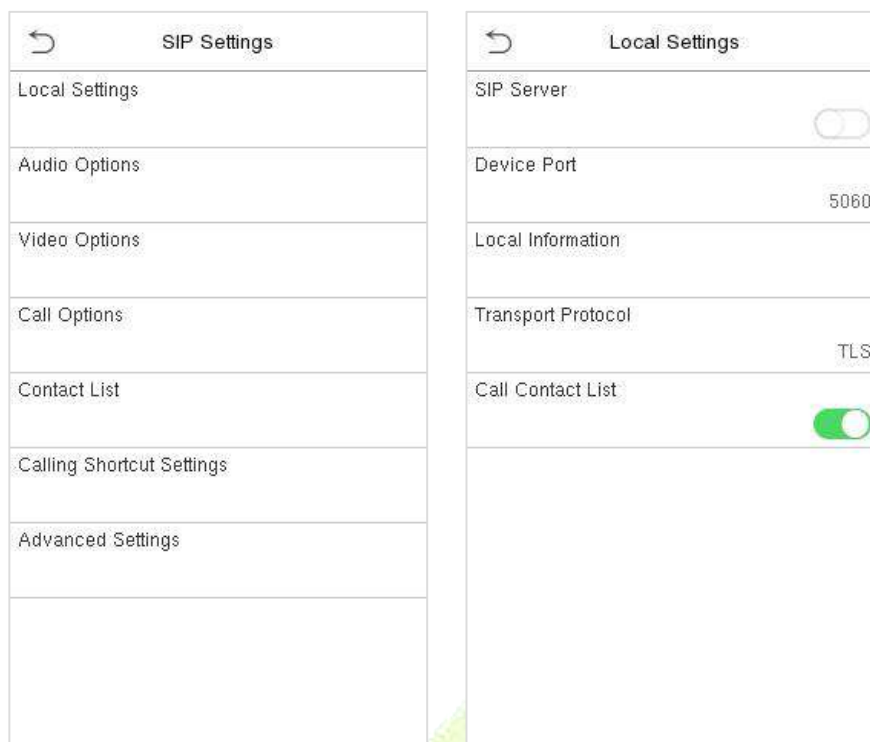
Fence Termina





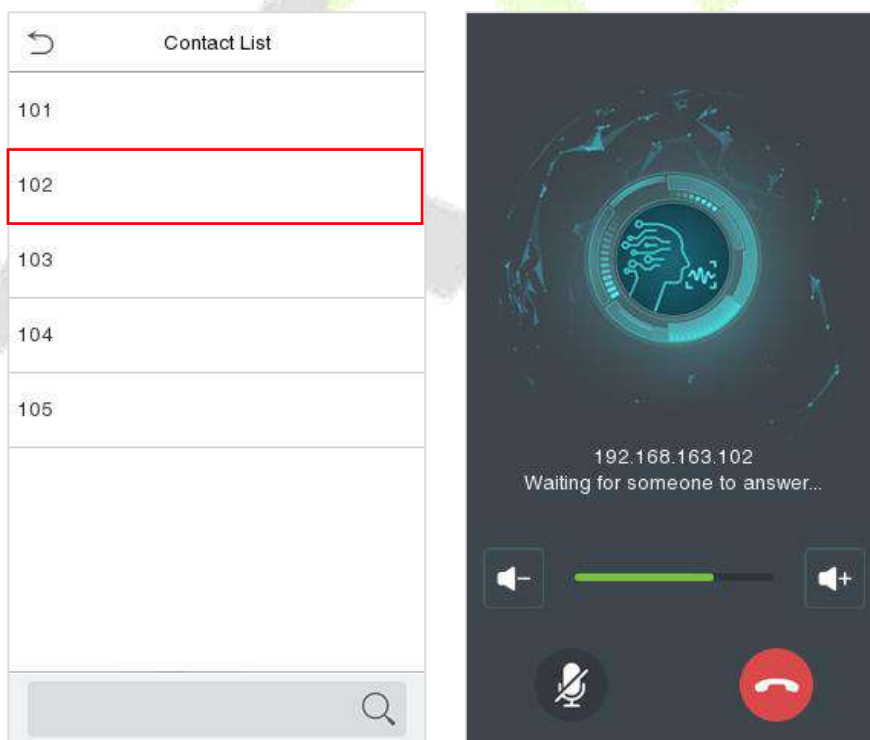
### 20.1.1 Call Contact List

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





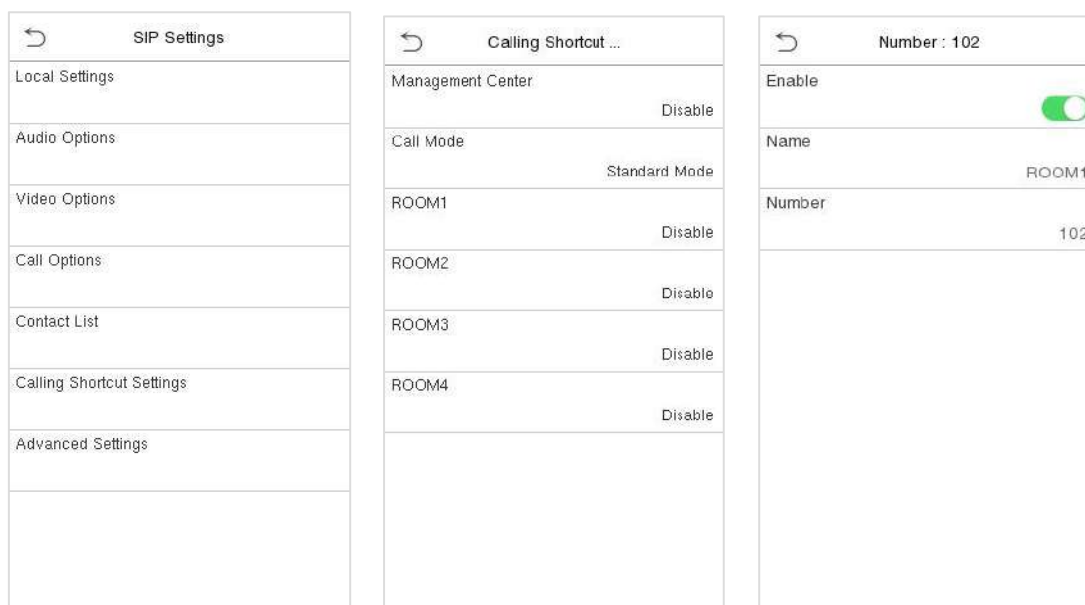
2. Click the icon  on the device to enter the call page, then you can click the  icon to open the contact list, select the number of the indoor monitor you want to call.



### 20.1.2 Custom the Calling Shortcut Keys


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

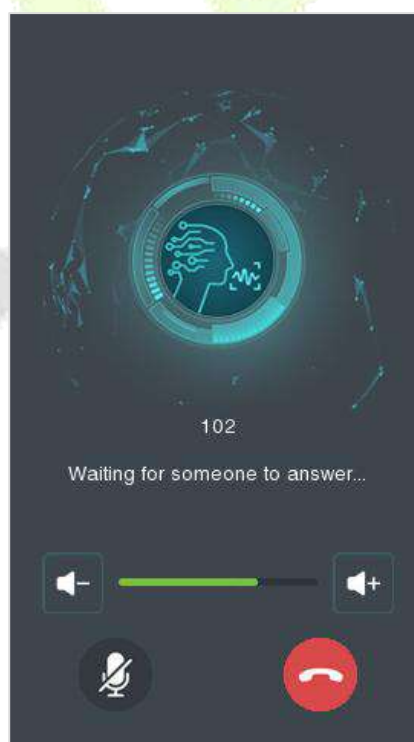
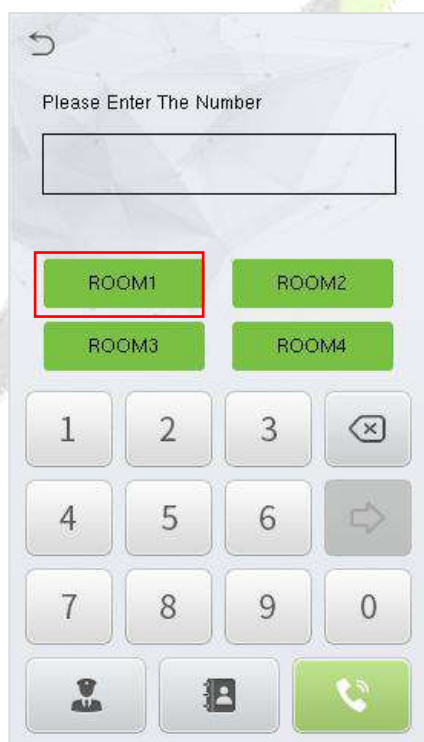




**Name:** Customize the name of the shortcut keys.

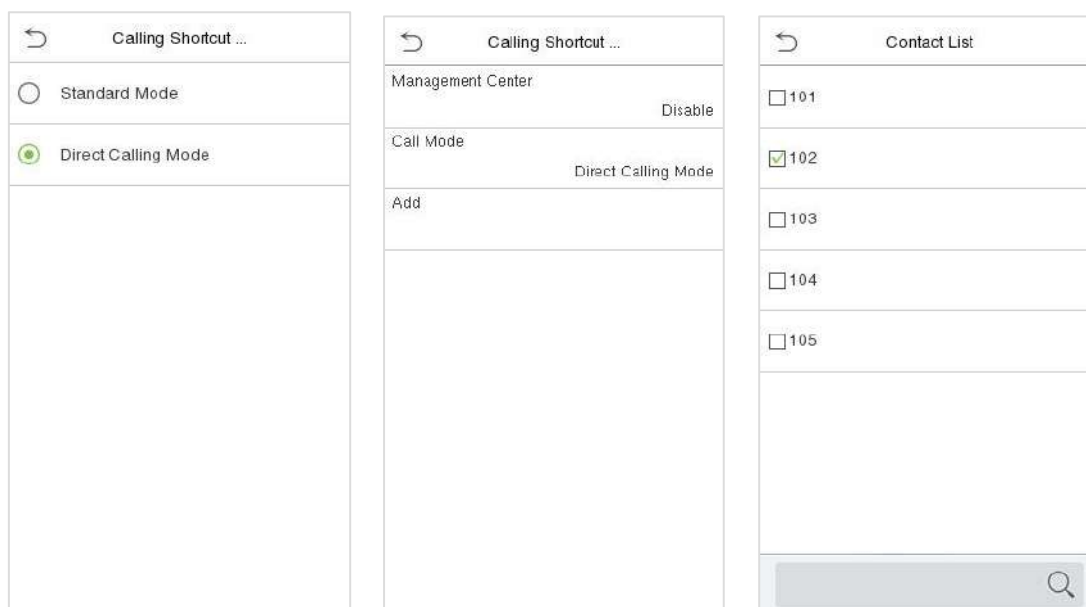
**Number:** It is the room number that set in the **Contact List** Menu.


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

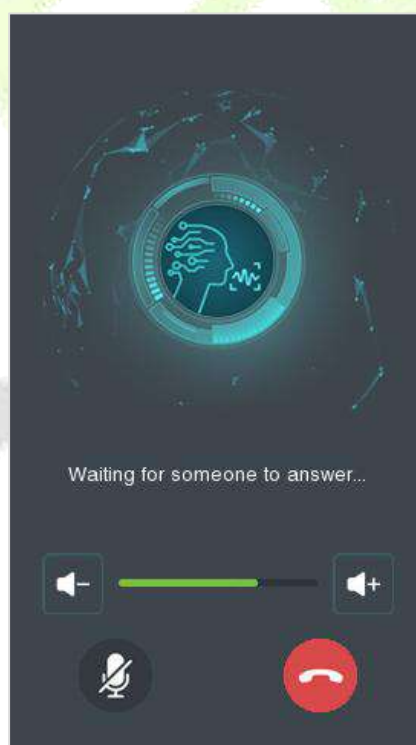
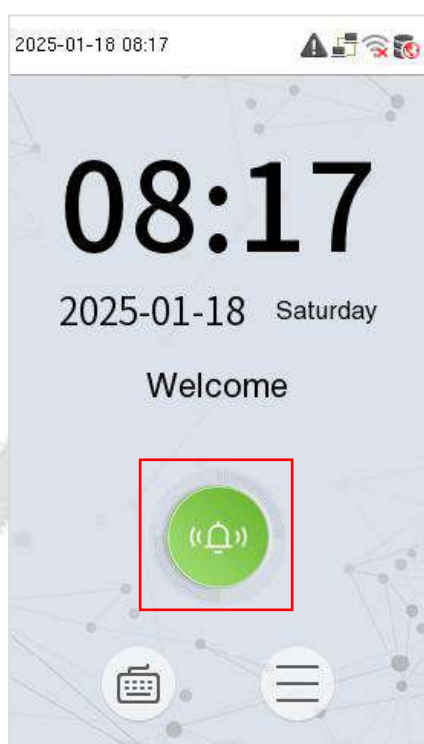


### 20.1.3 Direct Calling

- 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.

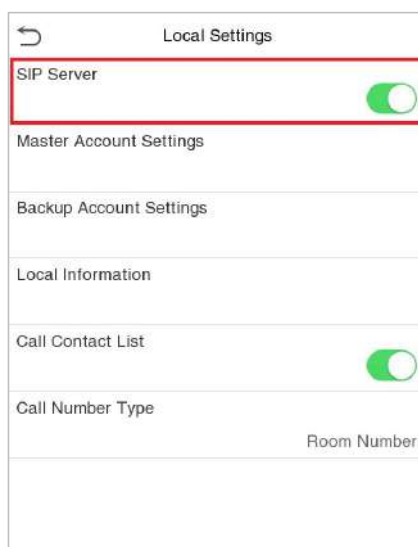


2. Then you can click the icon  on the device to call the indoor monitors directly.



## 20.2 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.

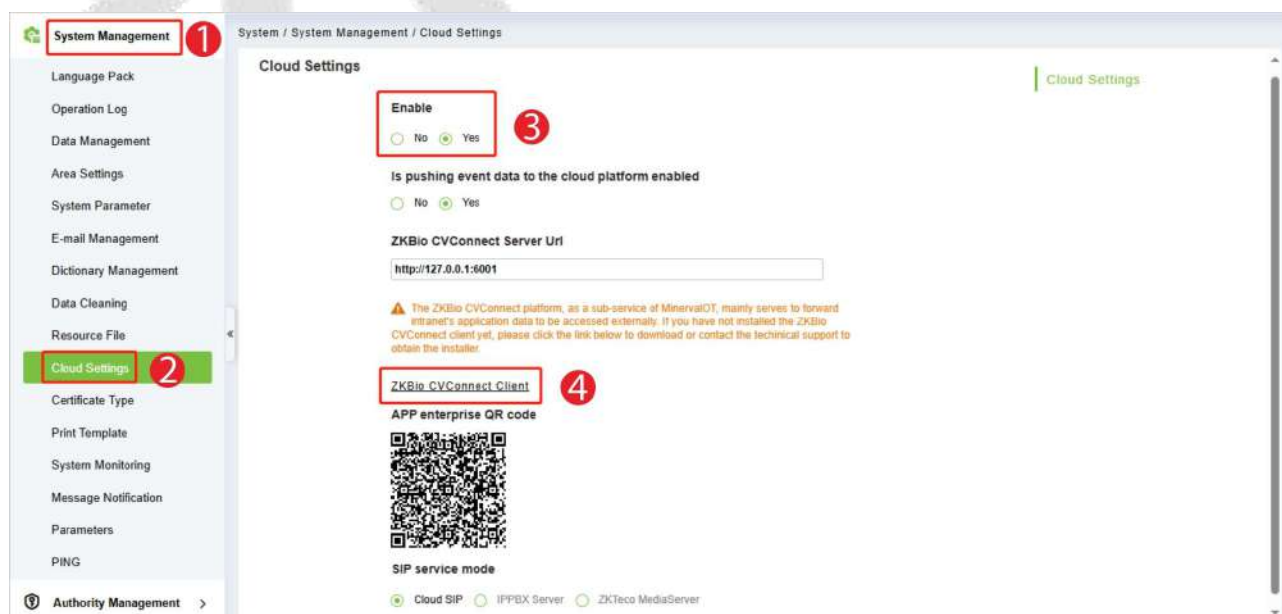
ZKBio CVSecurity supports 2 kinds of SIP server: **cloud SIP** and **PBX server**, users can choose one according to the actual situation.

- **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.

### 20.2.1 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**A screenshot of the ZKBio CVConnect Activation page. The page has a title 'ZKBio CVConnect Activation' and a subtitle 'Activation code activation >>'. Below the subtitle is a paragraph explaining that ZKBio CVConnect is a service based on ZKTECO MinervaIoT platform and that activating it requires registering as a MinervaIoT user and creating a company. The page features a progress bar with four steps: 1. Please select area (active), 2. Bind ZKBio CVConnect account, 3. Select company, and 4. Activation waiting. The main form area contains three fields: 'Area' (a dropdown menu), 'Local Application' (a dropdown menu with 'ZKBio CVSecurity' selected), and 'Endpoint' (a text input field with 'https://192.168.163.86:8098' entered). A green 'Next' button is located at the bottom right of the form.

- **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:

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

[CONTACT US](#) [RESOURCES](#) [FORUM](#) [SIGN IN](#)

**USER**

[Sign Up](#)

FIRST NAME

LAST NAME

EMAIL

CONTACT

PASSWORD

CONFIRM PASSWORD

Already have an account? [Sign In](#)

[TERMS & CONDITIONS](#) [PRIVACY POLICY](#)

## 3. Select Company

**Hybrid Cloud Activation**

[Activation code activation >>](#)

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

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

\* Select company:

[Use new company](#)

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

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

Use existing company

\* Country: United Arab Emirates

\* Name: Popy-test-company-1

\* Code: 1234567

Previous Create Company

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

**Hybrid Cloud Activation**

[Activation code activation >>](#)

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

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

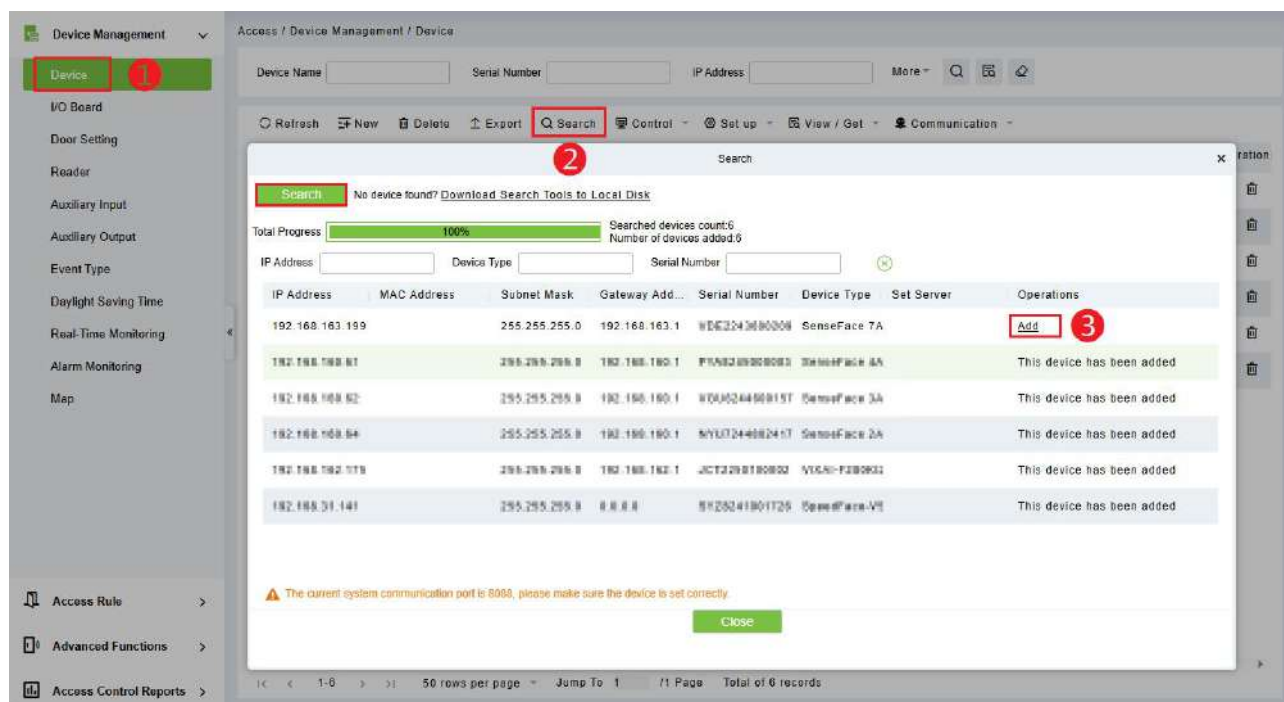
Activating

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

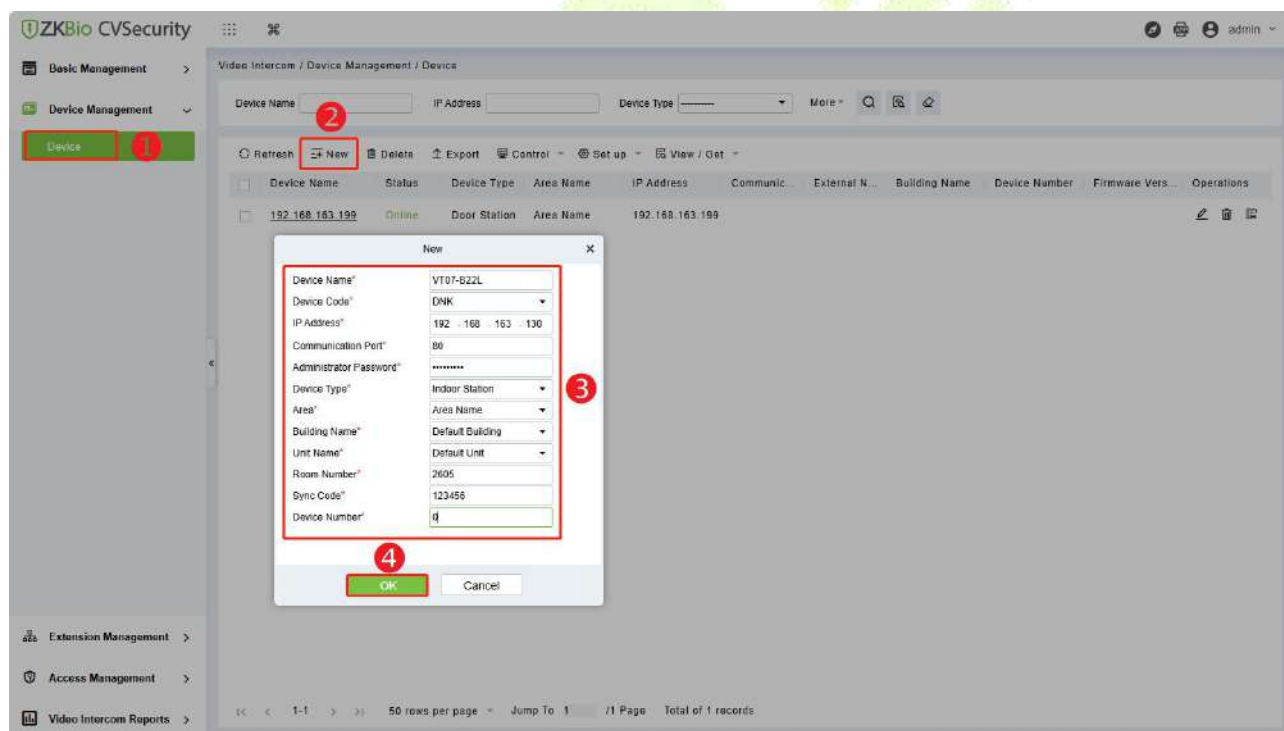
## 20.2.2 Add Device

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](#))





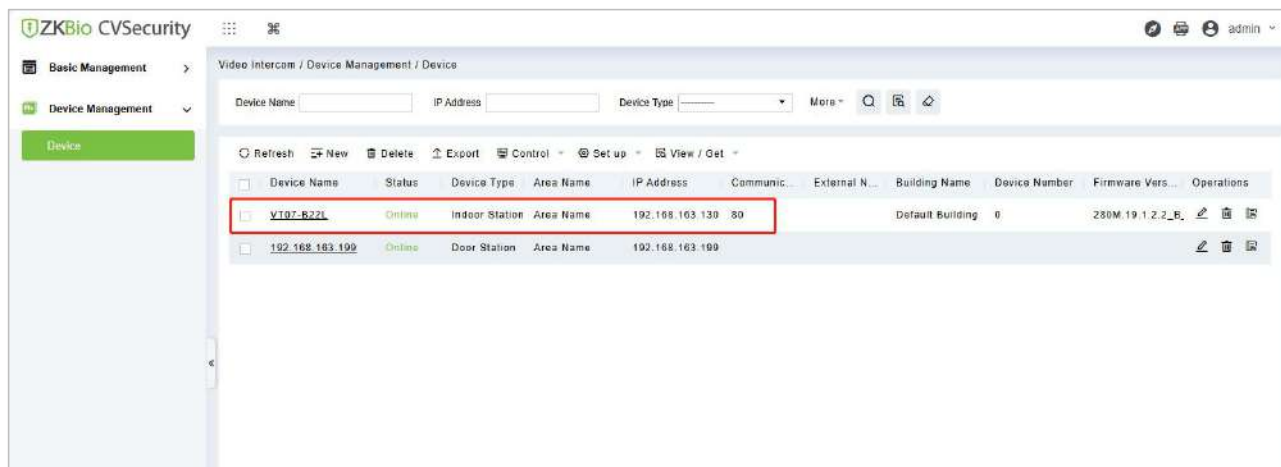
2. Click **Video Intercom > Device Management > Device > New** to add the indoor monitor.



- **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.

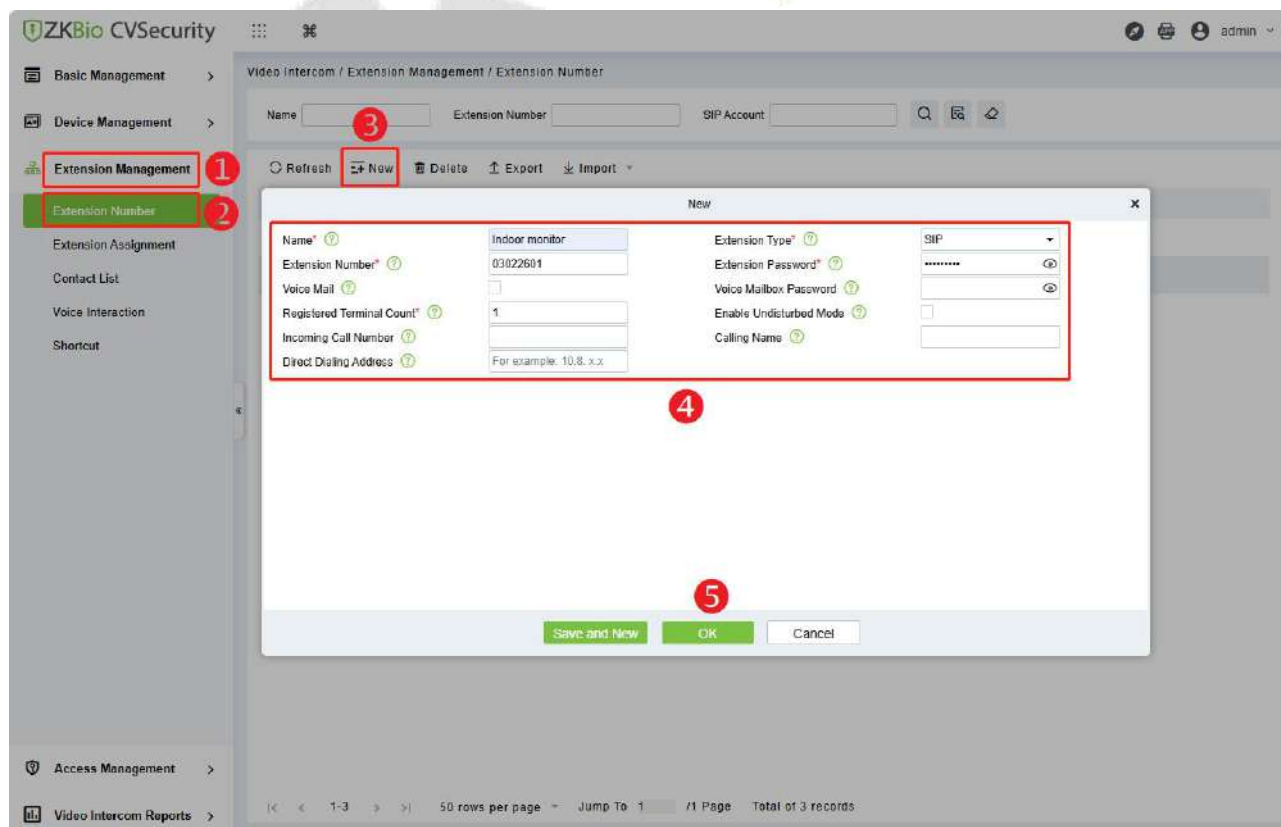
- **Room Number:** Customize the number of the indoor monitor.
- **Sync Code:** Can be customized by the user. (It is used when a resident has multiple indoor monitors. The indoor monitors which have the same Sync Code will be called at the same time.)
- **Device Number:** The setting range is 0-9. For 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.



### 20.2.3 Create Extension Numbers

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



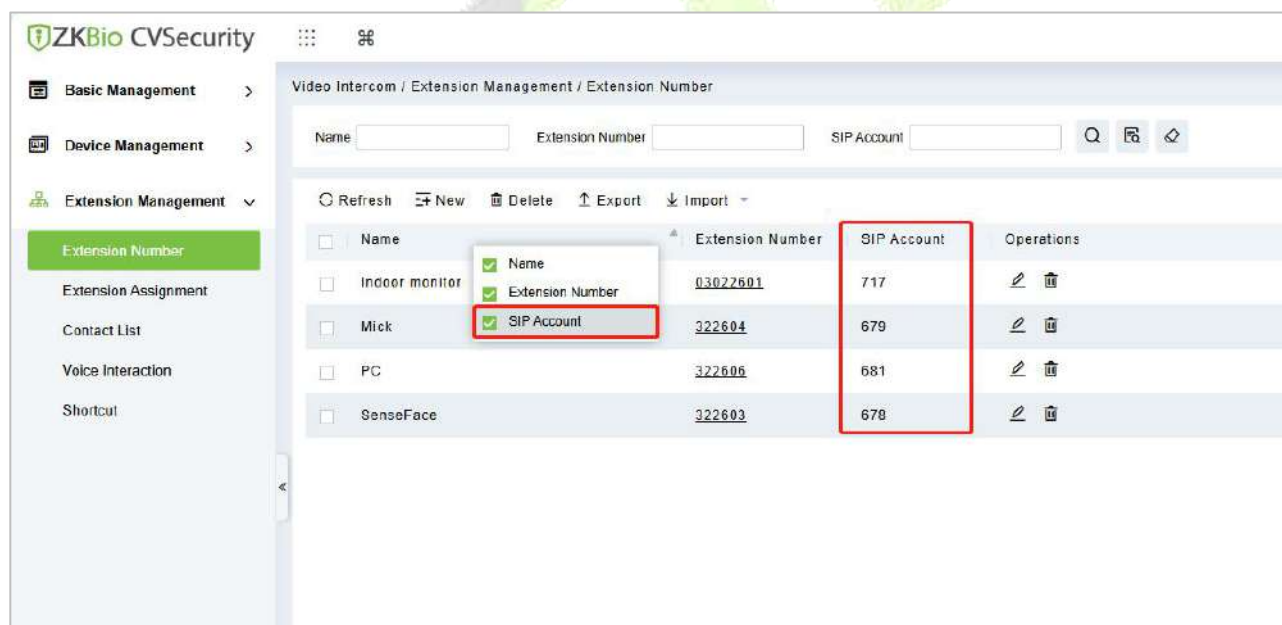


- **Name:** Customize the extension name. If it is a residential scene, the name can be set to the room number; if it is an office scene, the name can be set to the work number and name information.
- **Extension Type:** SIP by default.
- **Extension number:** Customize the extension number, it can be 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.

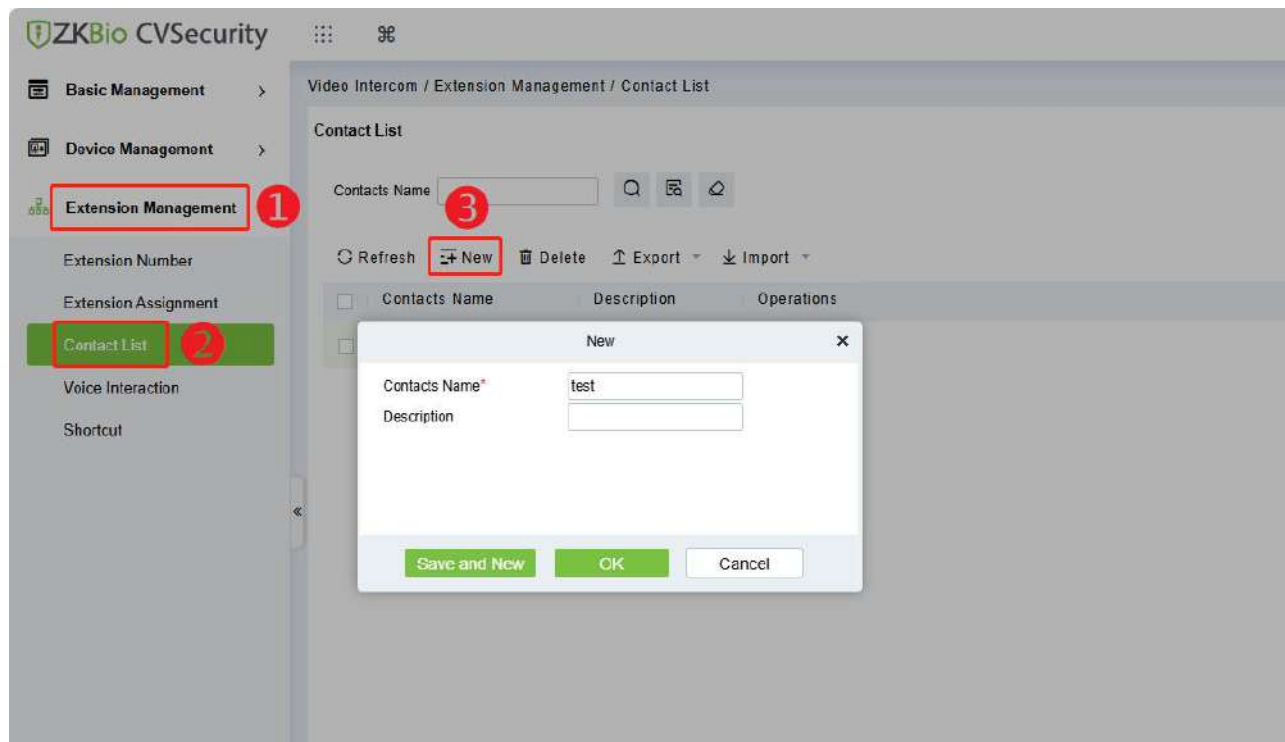



- 2) If you use a PBX, the extension number will be directly used, and the SIP account list will be empty.

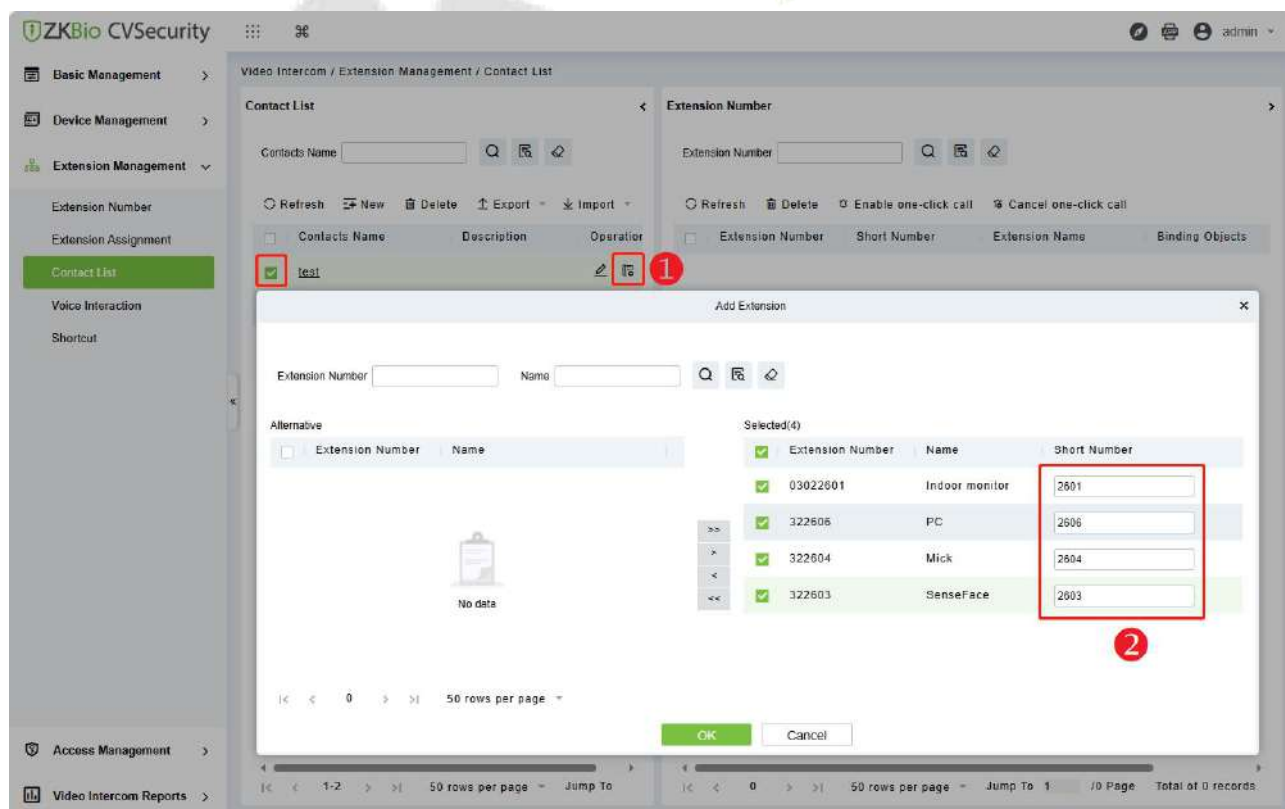
## 20.2.4 Contact List

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

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



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



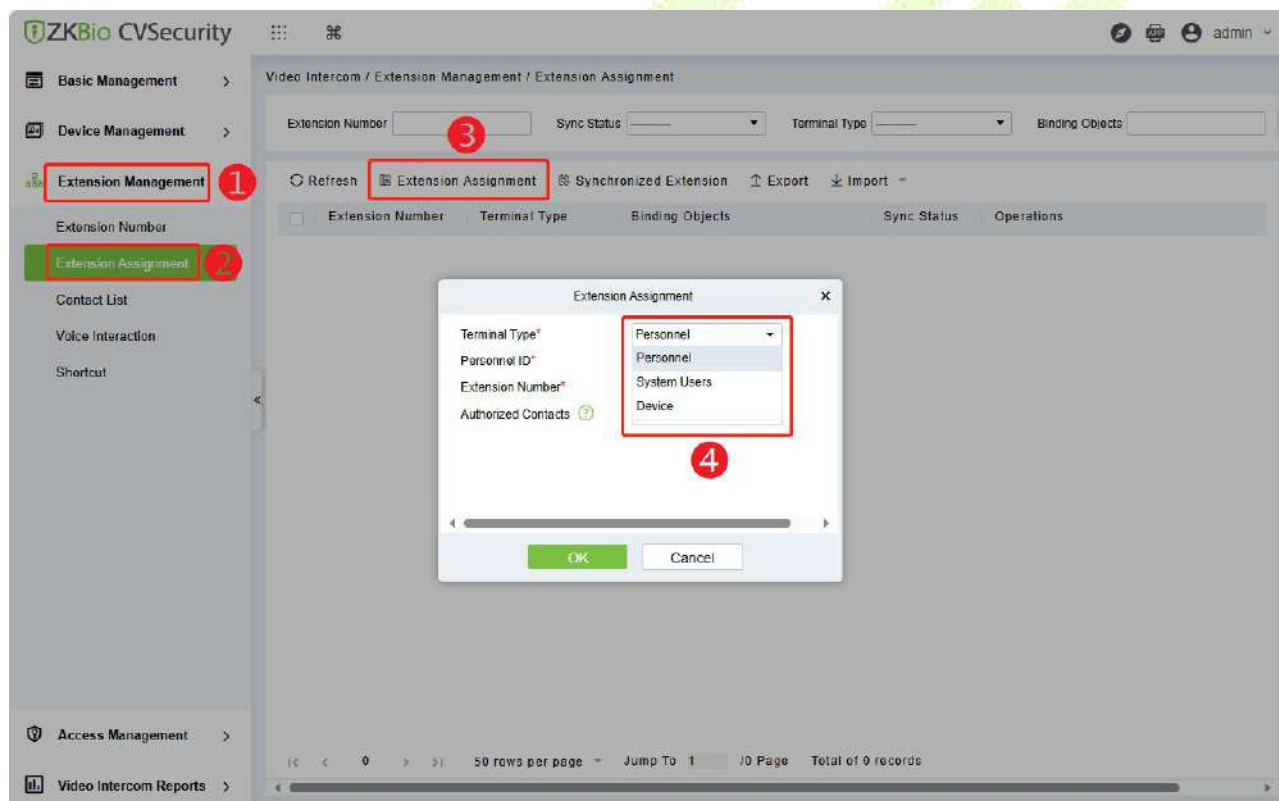
**Note:**

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

### 20.2.5 Assignment of Extension Numbers and SIP Accounts

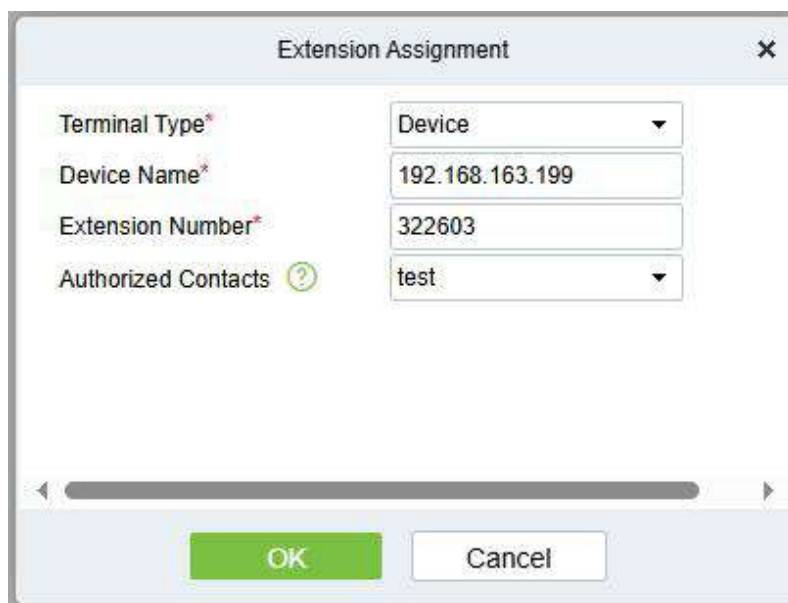
The extension number or SIP account can be assigned to personnel, devices or system users. After allocation, personnel and users' APP will be able to directly use video intercom for communication. The device can also be used directly without manual additional configuration.

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.

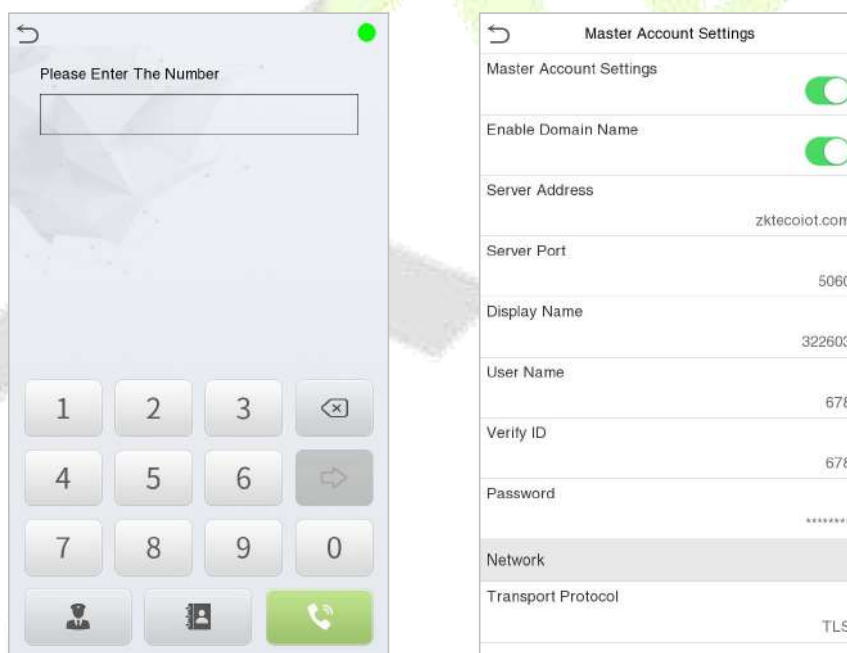


The 'Extension Assignment' dialog box contains the following fields:

Field	Value
Terminal Type*	Device
Device Name*	192.168.163.199
Extension Number*	322603
Authorized Contacts ?	test

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

- 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.

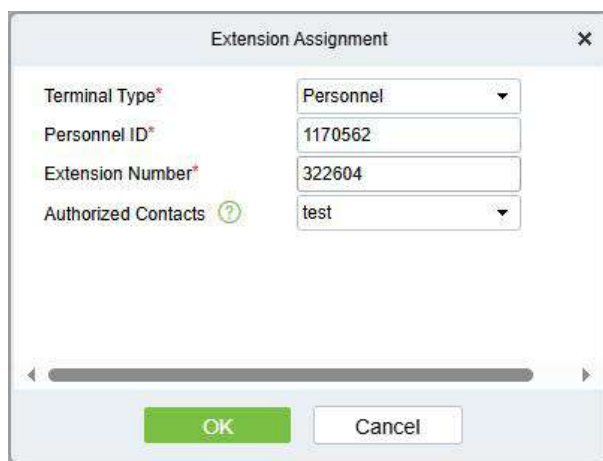


The figure shows two screenshots. The left screenshot is a call page with a green dot in the top right corner. The right screenshot is the 'Master Account Settings' screen with the following details:

Setting	Value
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)**

- Select the Terminal Type as **Personnel**.
- 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

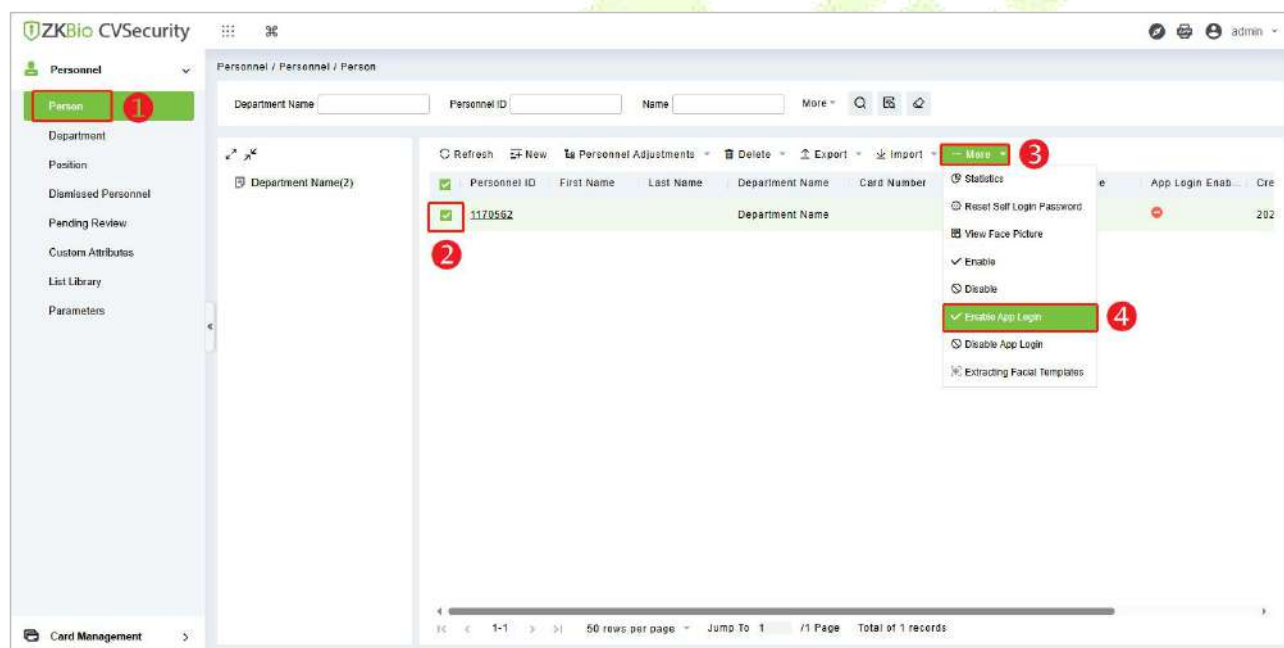
Extension Number\* 322604


Authorized Contacts ? test

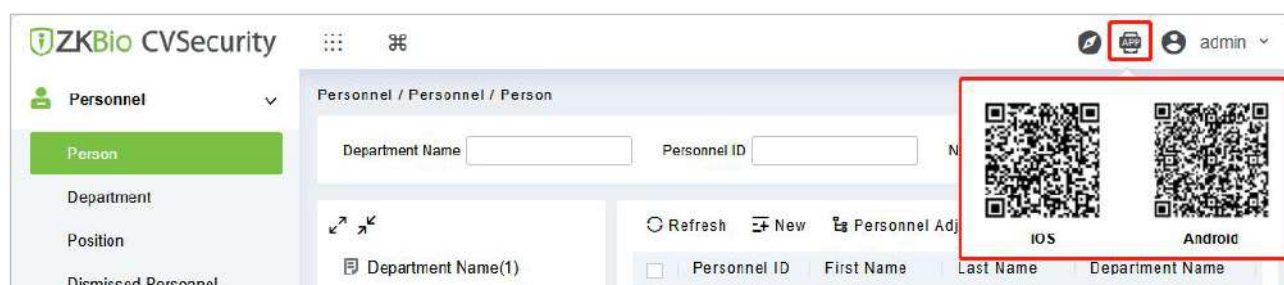
OK Cancel

**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.

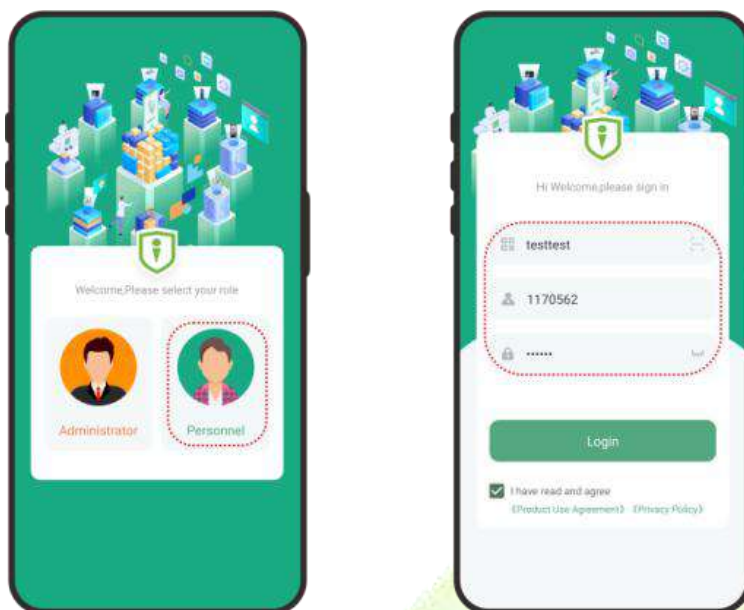


- 3) You can click the  icon at the right top corner of the ZKBio CVSecurity interface to scan the QR code to install the ZKBio Zexus App.



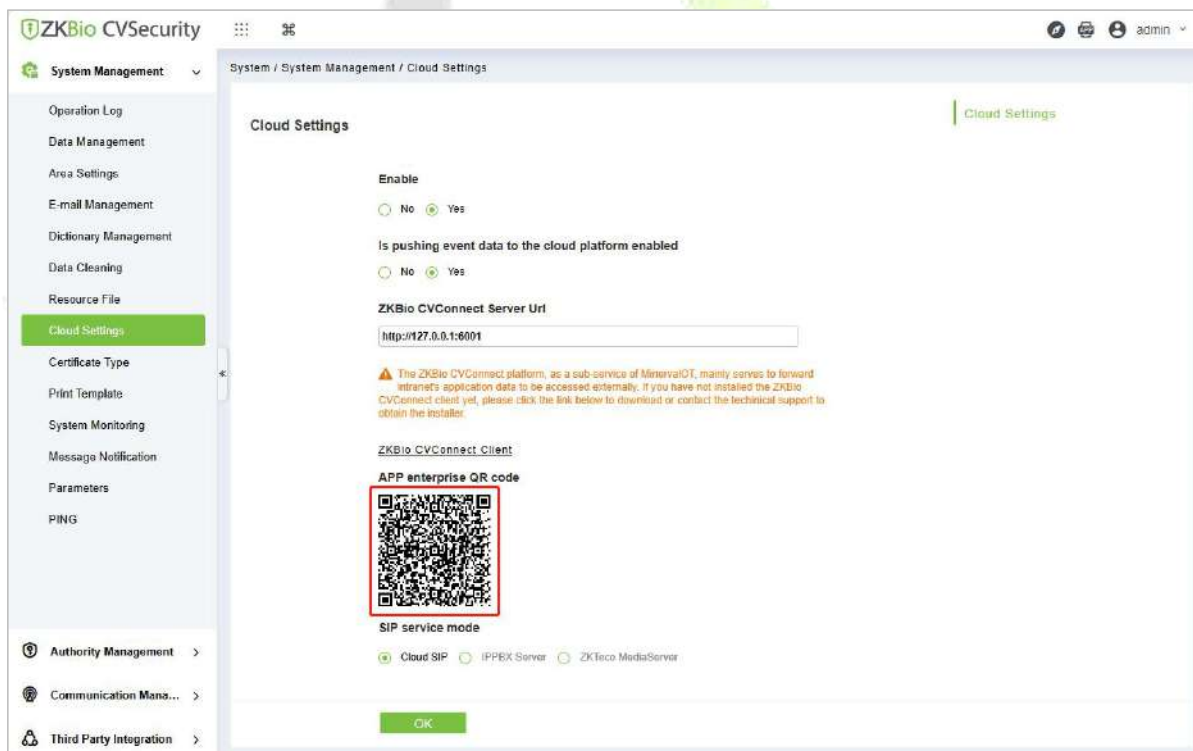


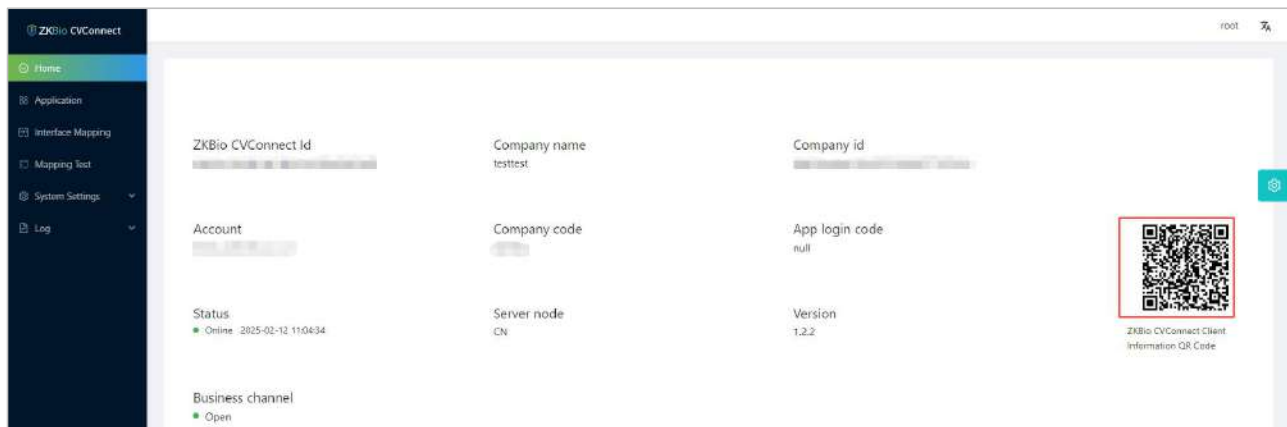
3. After successful assignment, the personnel can login to the App. Select the role-**Personnel** , enter the account information, and click **Login**.




**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.)

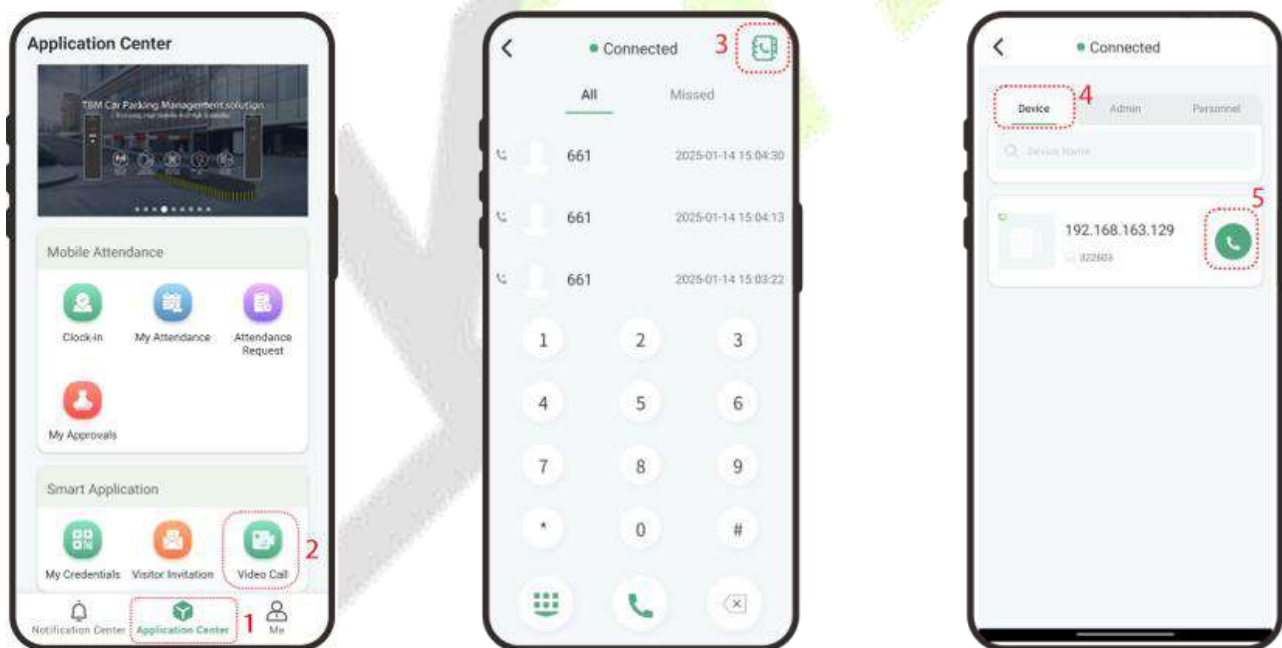
**Account & Password:** The personnel ID & password (default: 123456); Same account & password as ZKBio CVSecurity.





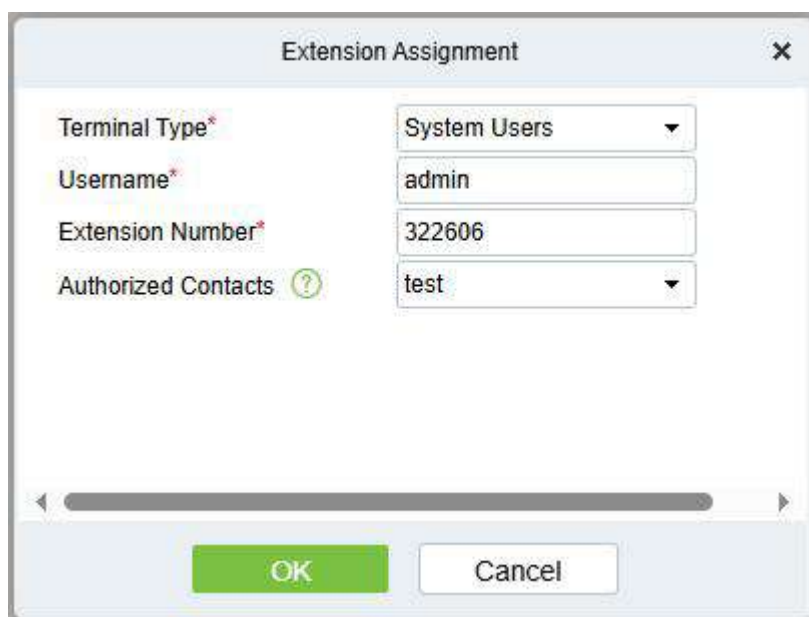
**Account & Password:** The personnel ID & password (default: **123456**); Same account & password as ZKBio CVSecurity.

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



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

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



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

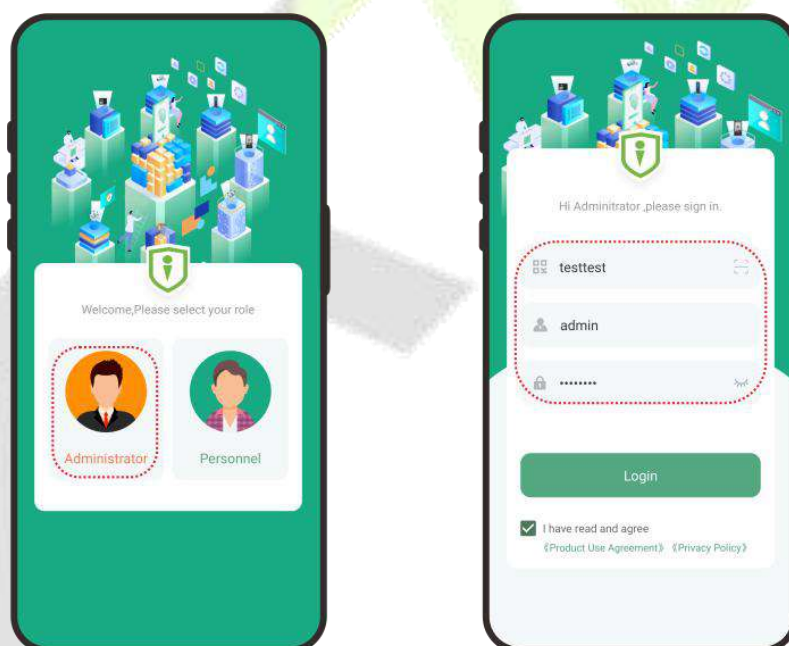
Field	Value
Terminal Type*	System Users
Username*	admin
Extension Number*	322606
Authorized Contacts ?	test


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**.

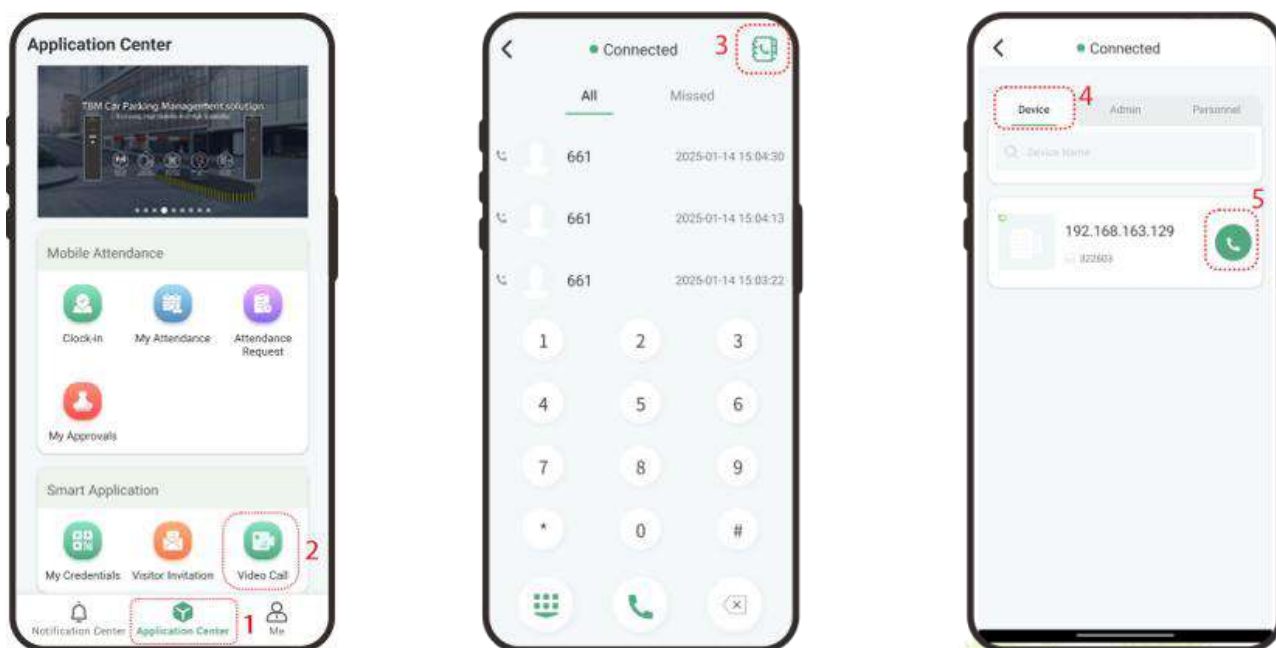
**Organization Name:** Scan the organization code you get before.

**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.





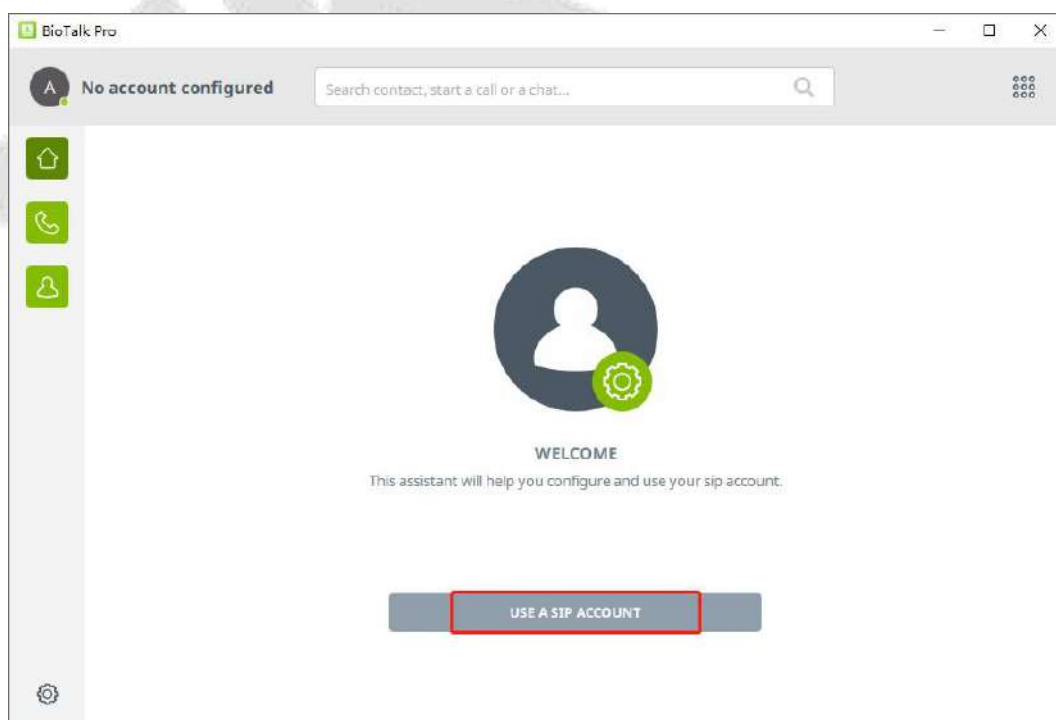
The App complete operation steps please refer to the ZKBio Zexus Mobile App User Manual.

## 20.2.6 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: zktectoiot.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.zktectoiot.com". Then 'zktectoiot.com' is the actual SIP server domain you need to enter on the PC Client.)

ZKBio CVConnect

Home Applications Interface Mapping Mapping Test System Settings Log

Application

Application	Number of Interfaces	Number of Interface Mappings	connect
Minerva Credential Management	9	9	Enter
Innosip	7	7	2 Enter
Minerva Organization	14	14	Enter
ZKBio CVConnect Client	120	120	Enter
ZKBioCVAccess	87	90	Enter

Back Innosip SIP 可快速连接

Applid Innosip

Authentication Type Minerva Auth

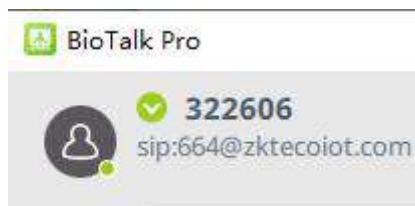
EndPoint https://innosip.zktectoiot.com

Interface Name: Please enter Interface Address: Please enter

Reset Query

- **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:

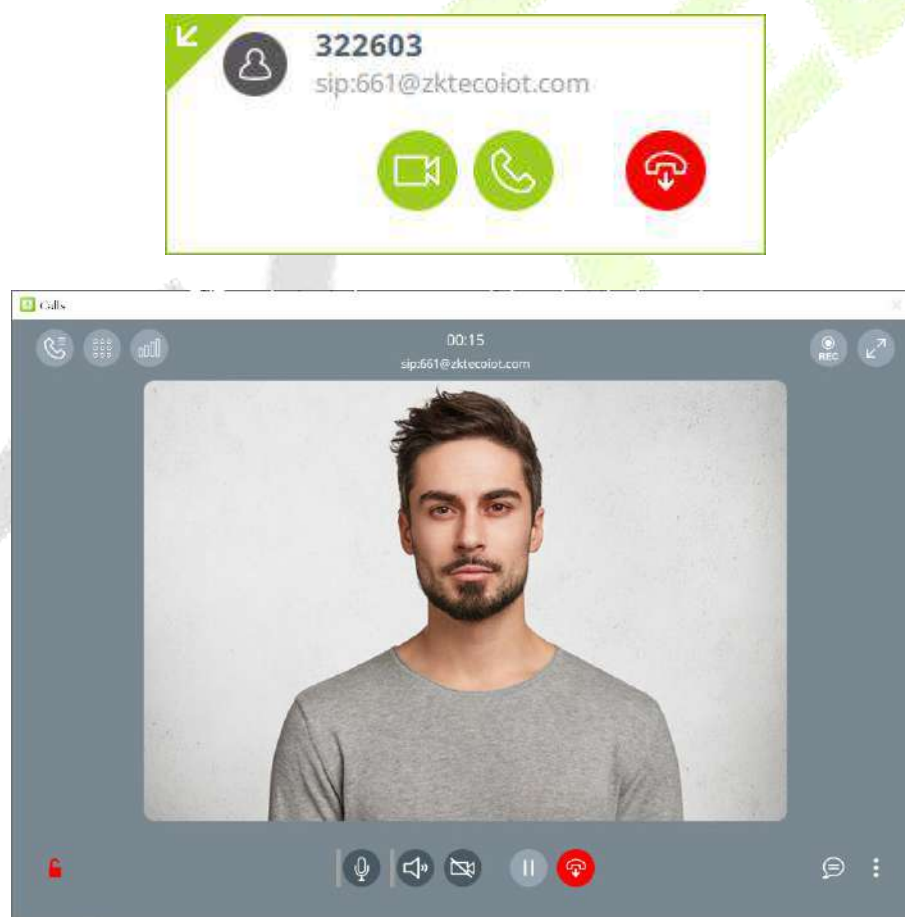


**Note:** In the Cloud SIP mode, if dialing is required, the PC Client should dial directly to the target SIP account. For example, if the extension number created on ZKBio CVSecurity is 322603, the corresponding generated SIP account is 661, then the PC Client should dial 661 when making a call. Therefore,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

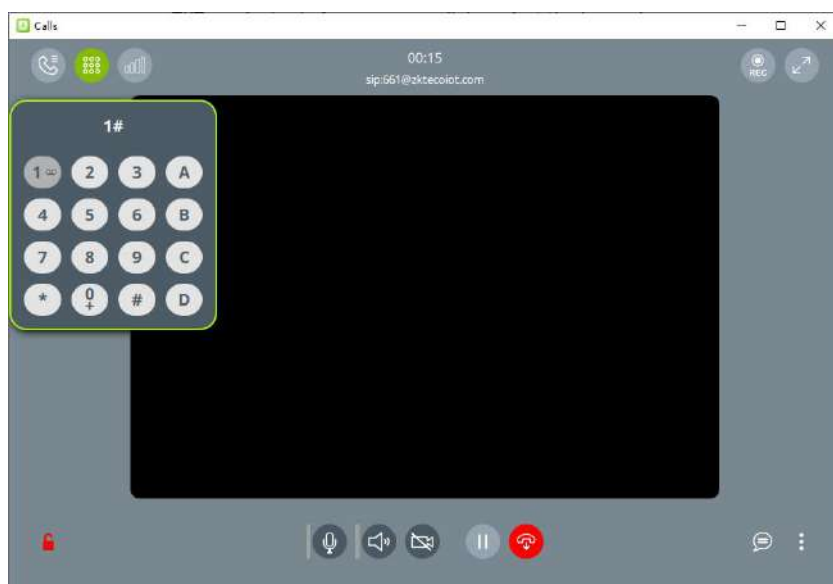
At this point you can start to use it normally, the PC client, the device and the App can call and answer each other.

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.

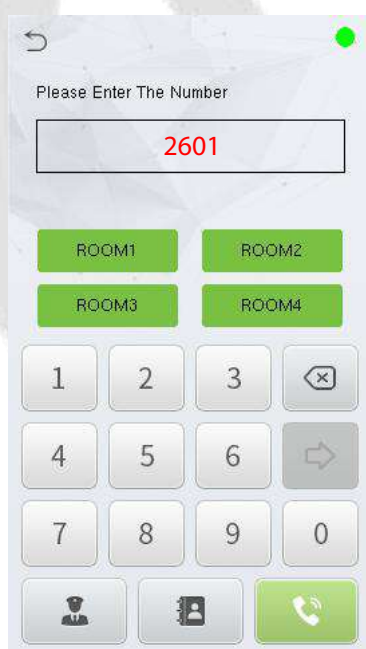


## 20.2.7 Make a Call

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

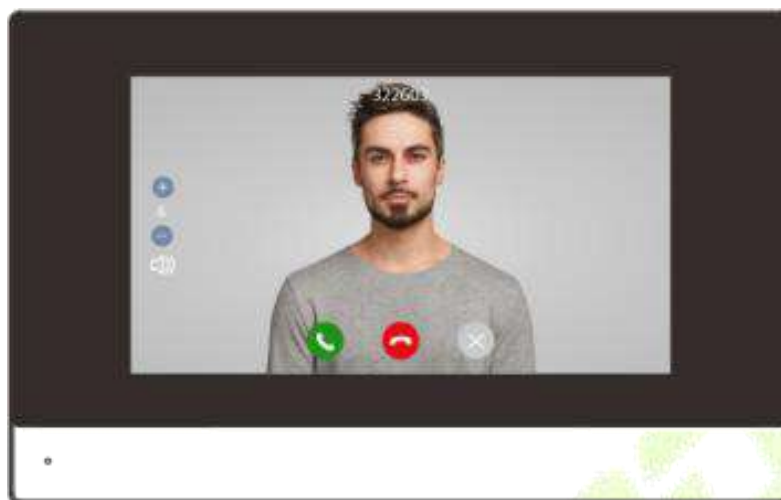
- **Device Call the Indoor Monitor (VT07-B26L-W / VT07-B22L)**

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 [20.2.2 Add Device](#) and [20.2.5 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.





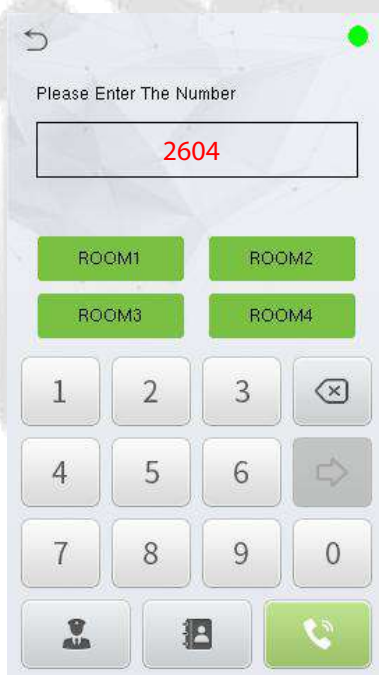
or






### ● **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



3. When the device calls the phone, the mobile app pops up the answer interface shown below. Click the  icon to answer.





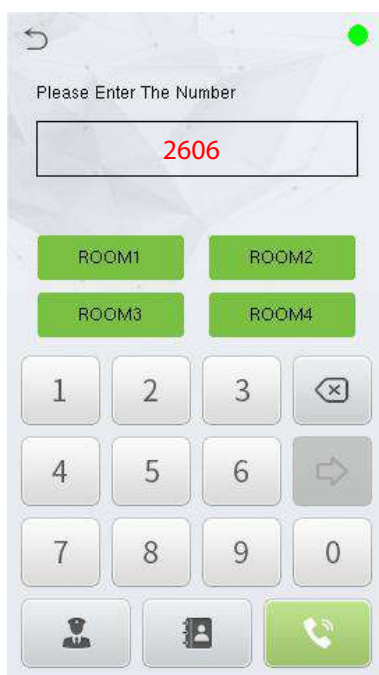
4. After answering the call, you will enter the call interface shown in the figure.



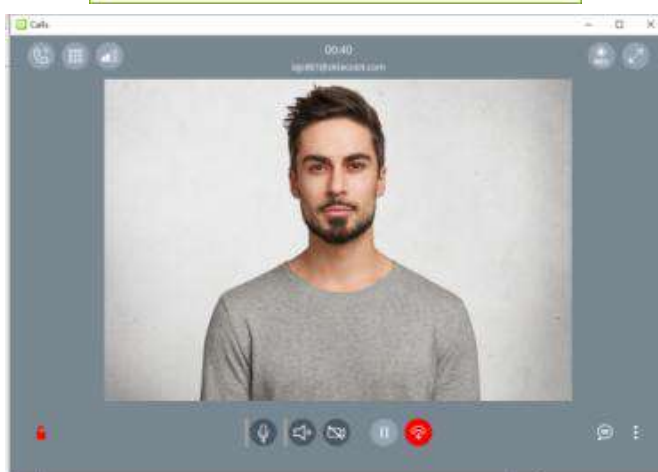
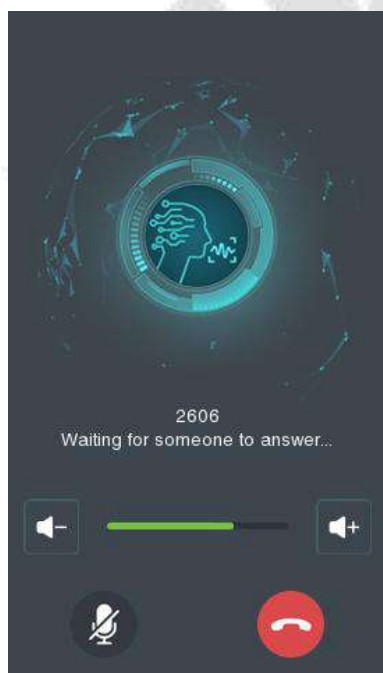
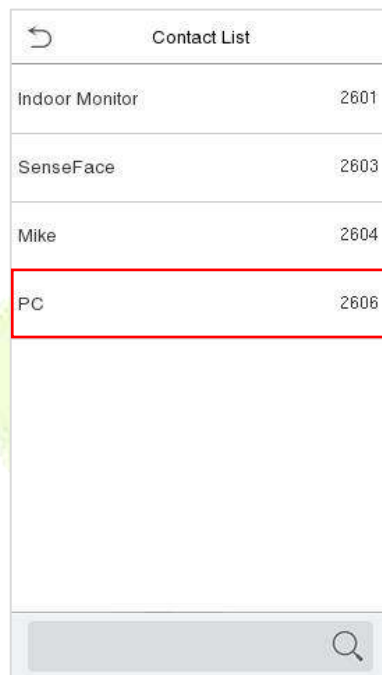


## ● **Device Call the PC Client (BioTalk Pro)**

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.



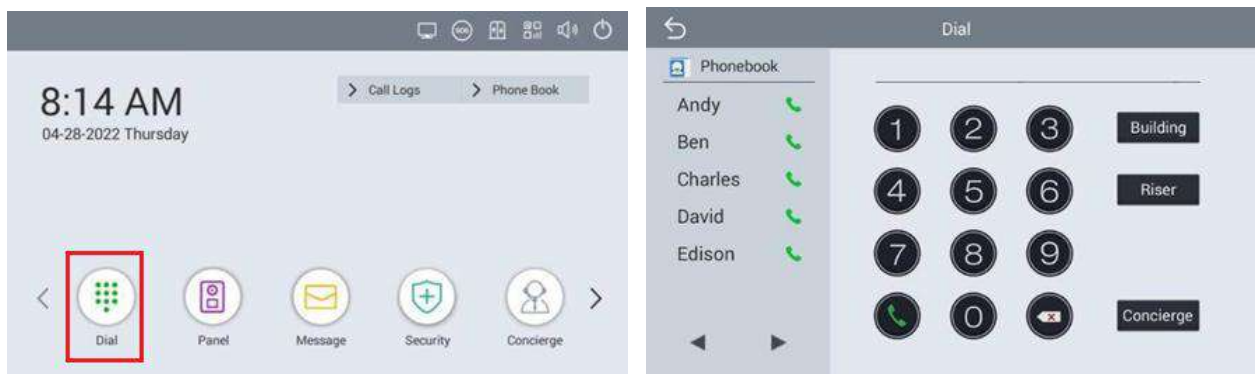
or






## ● **Indoor Monitor Call**

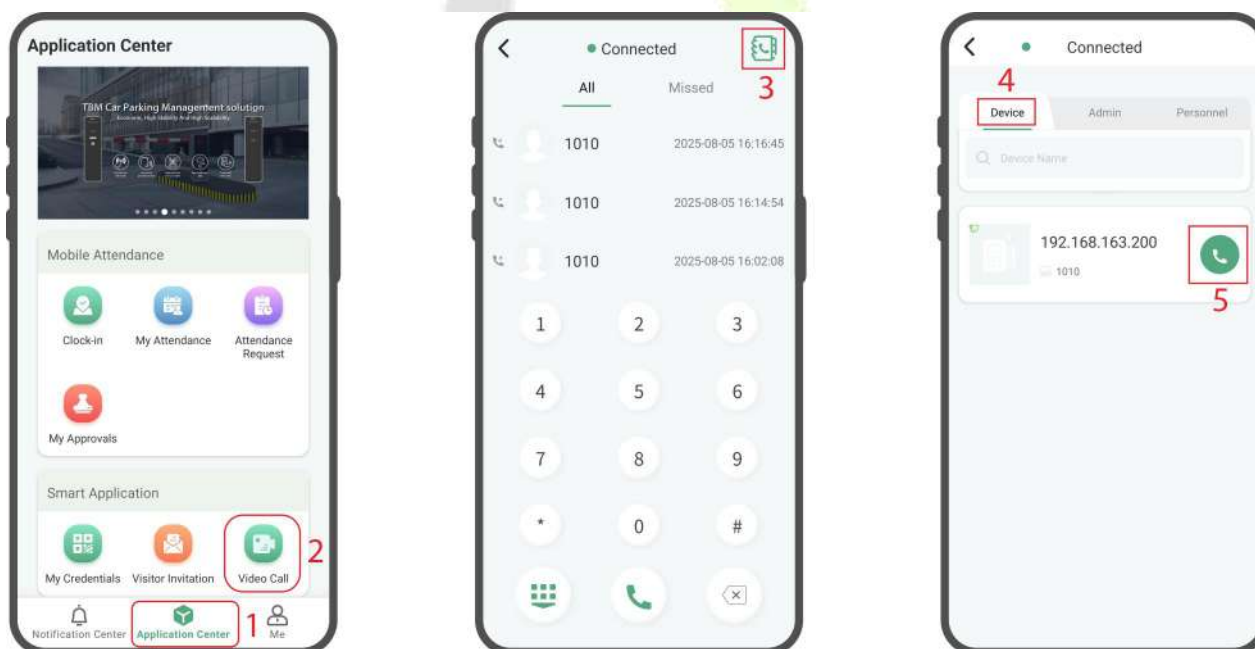
Click the **Dial** icon, then enter the SIP Account to make a call.




**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.




When you make a call in the app, the device will display the call answering interface. Click the  icon to initiate a video call, as shown in the figure below.



After answering the call, you will enter the call interface shown in the figure.



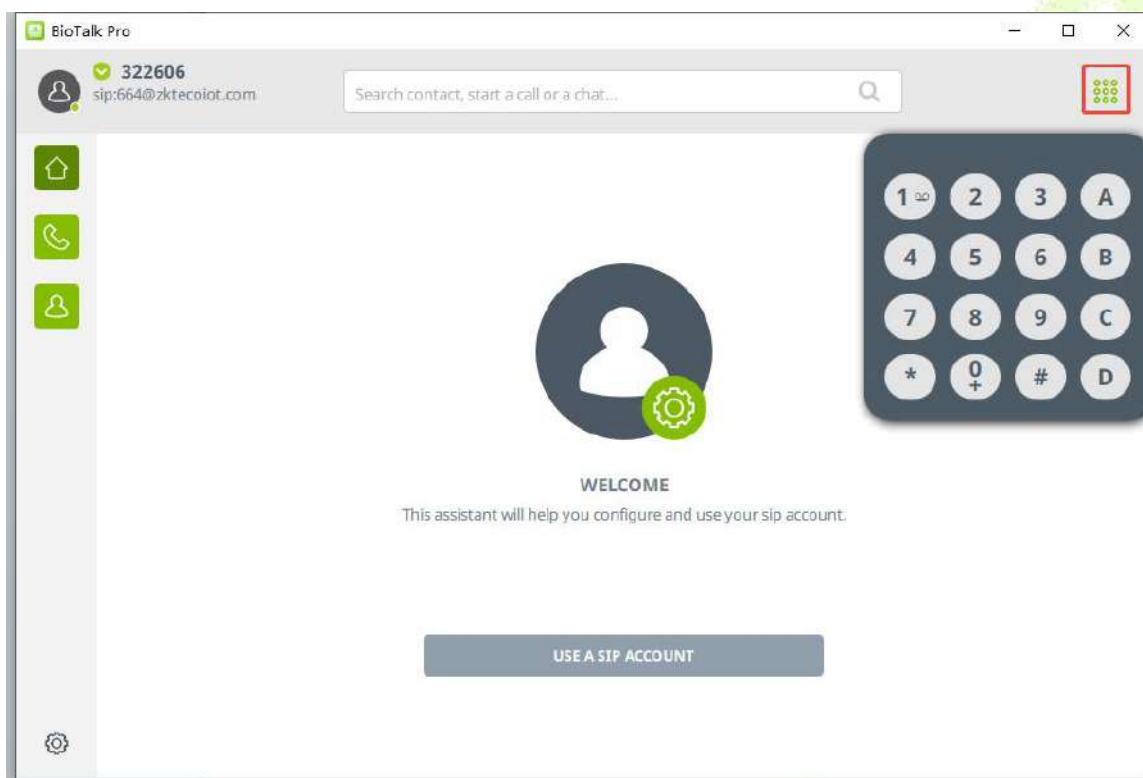
**Note:**

- 1) Big capacity version device. When you click the  (Call) icon in the app while the device is on the **Recognition Interface**, it will first exit the recognition interface, then display the **Call Interface**, and automatically answer the call.
- 2) **Auto Answer Disabled:** If you go to **SIP Settings > Call Options** and **Disable Auto Answer**, the device will display the call screen when a call is dialed from the app. You must manually answer the call. If no action is taken, the call will timeout and automatically disconnect after the set duration.

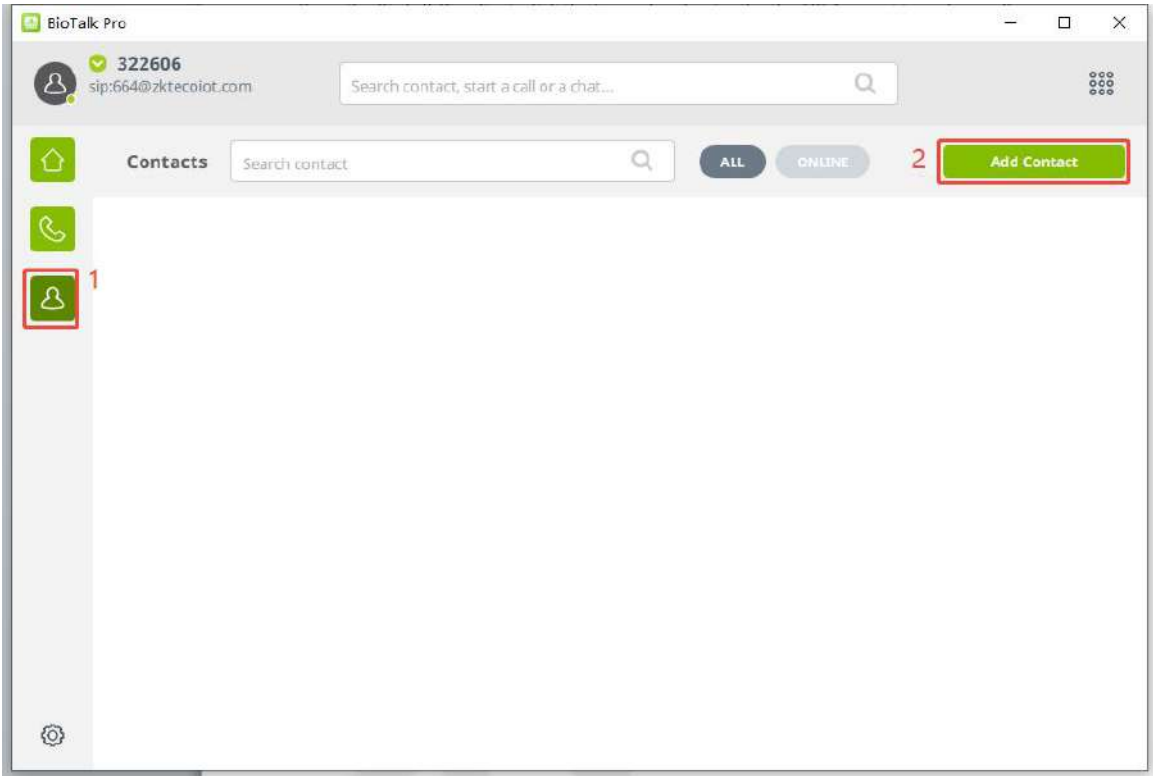
- 3) **Auto Answer Enabled with Delay:** If you go to **SIP Settings > Call Options**, enable **Auto Answer**, and set the **Auto-Answer Delay Time** to **10 seconds**, the device will display the call screen when a call is received from the app. If the call is not answered manually, the device will automatically answer after 10 seconds.
- 4) **Default Auto Answer Settings:** Device-side **Intercom > SIP Settings > Call Options > Auto Answer Settings** is enabled by default. The default **Auto-Answer Delay Time** is **0 seconds** (calls are answered immediately).

- **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.



## 21. Connecting to ZKBio Zlink Mobile App

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

Change the device communication protocol to BEST protocol, then the device can be managed by ZKBio Zlink, please refer to [8.5 Device Type Setting](#).

### ● Download the ZKBio Zlink Mobile App

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



Apple App Store

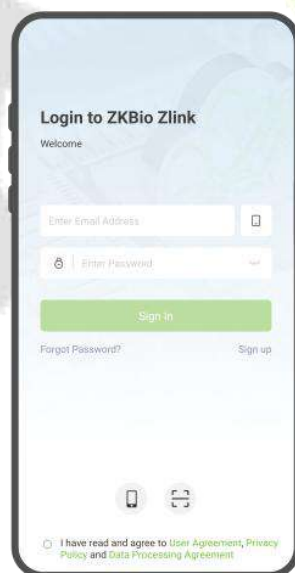


Google Play Store




### 21.1 Login to the Mobile App

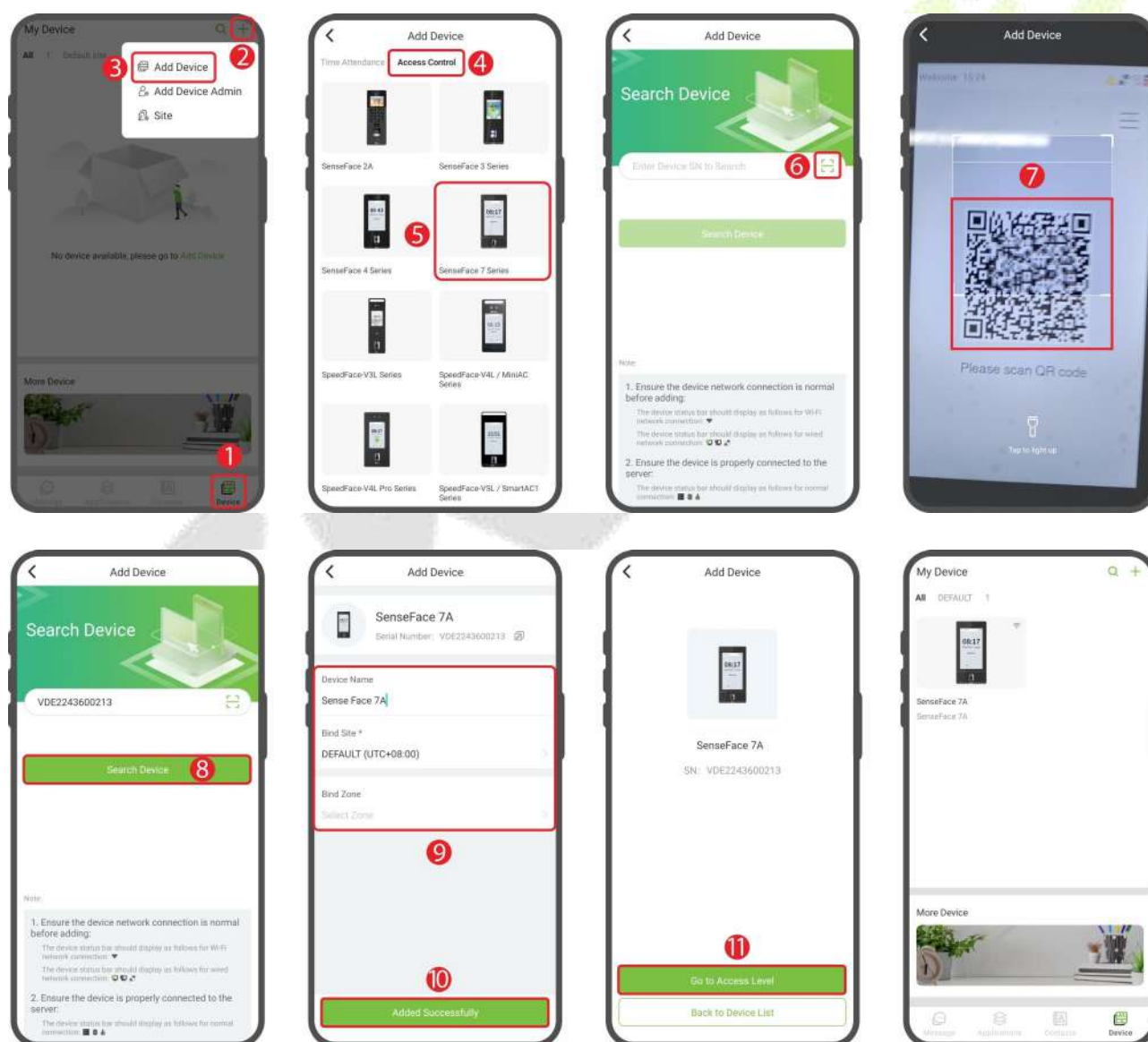
Enter your registered account and password, check "I have read and agree to User Agreement, Privacy Policy and Data Processing Agreement" and click **Sign In** to log in to the Mobile App.



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

## 21.2 Add Device on the Mobile App

1. Access the ZKBio Zlink Mobile App and click on **[Device]** > **+** icon > **[Add Device]** > **[Access Control]** > **[BioFace D1]**.
2. Click  icon to scan the QR code on the device. The serial number of the device will be displayed in the bar. Then click **[Search Device]**.
3. Enter the device name and specify the device to a site and zone. Click **[Added Successfully]** to complete the addition. At the same time, the device voice prompts **"Device is added successfully"** indicating that the addition is complete.
4. Once successfully added, the device is displayed in the list of the device interface. Then you can set the access levels and video intercom function as needed.

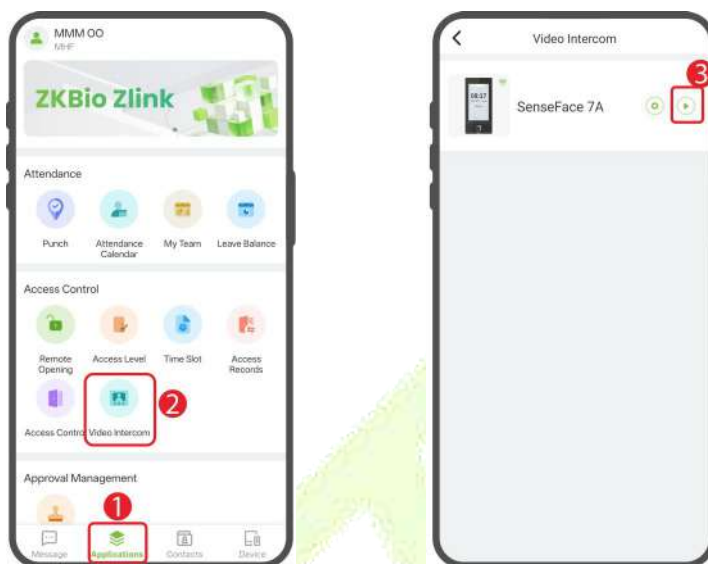





## 21.2.1 Video Intercom

### ● **Phone Call the Device**

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



2. When you make a call in the app, the device will display the call answering interface. Click the  icon to initiate a video call, as shown in the figure below.




3. After answering the call, you will enter the call interface shown in the figure.




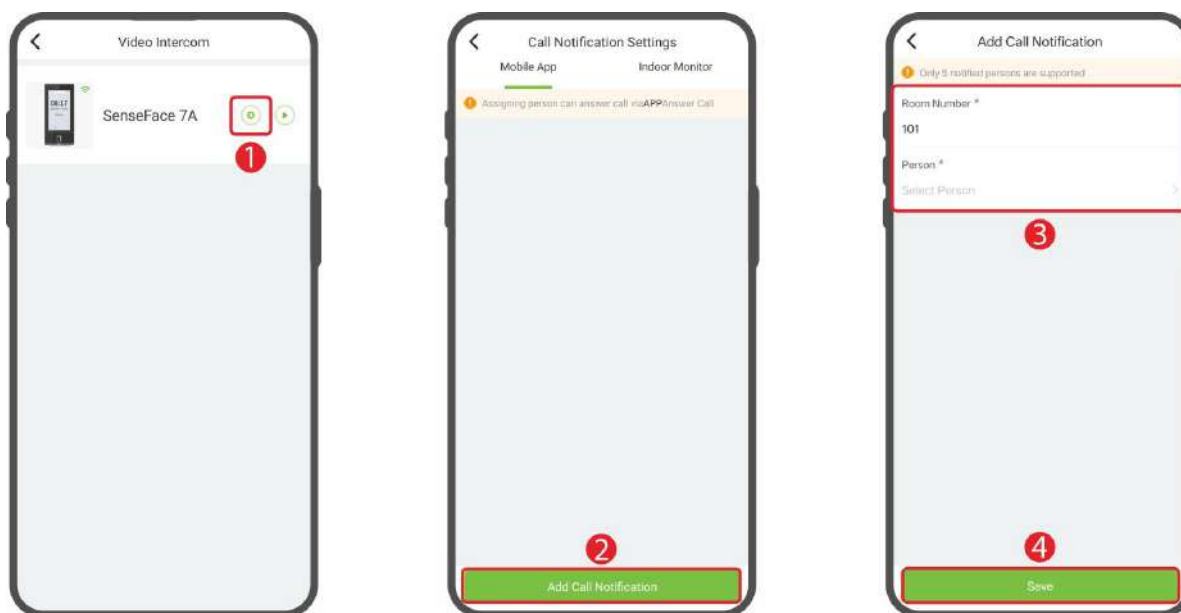


### Note:

- 1) Big capacity version device. When you click the  icon in the app while the device is on the **Recognition Interface**, it will first exit the recognition interface, then display the **Call Interface**, and automatically answer the call.
- 2) **Auto Answer Disabled:** If you go to **SIP Settings > Call Options** and **Disable Auto Answer**, the device will display the call screen when a call is dialed from the app. You must **manually answer the call**. If no action is taken, the call will **timeout and automatically disconnect** after the set duration.
- 3) **Auto Answer Enabled with Delay:** If you go to **SIP Settings > Call Options**, enable **Auto Answer**, and set the **Auto-Answer Delay Time** to **10 seconds**, the device will display the call screen when a call is received from the app. If the call is not answered manually, the device will automatically answer after 10 seconds.
- 4) **Default Auto Answer Settings:** Device-side **Intercom > SIP Settings > Call Options > Auto Answer Settings** is enabled by default. The default **Auto-Answer Delay Time** is **0 seconds** (calls are answered immediately).

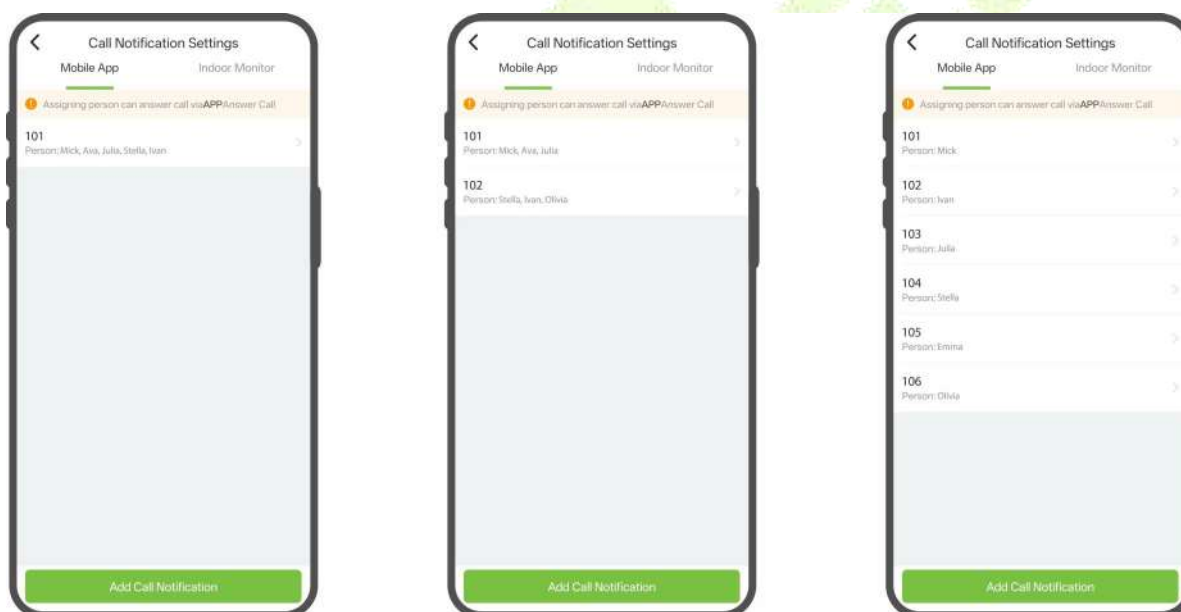
### ● Device Call the Phone (ZKBio Zlink App)

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

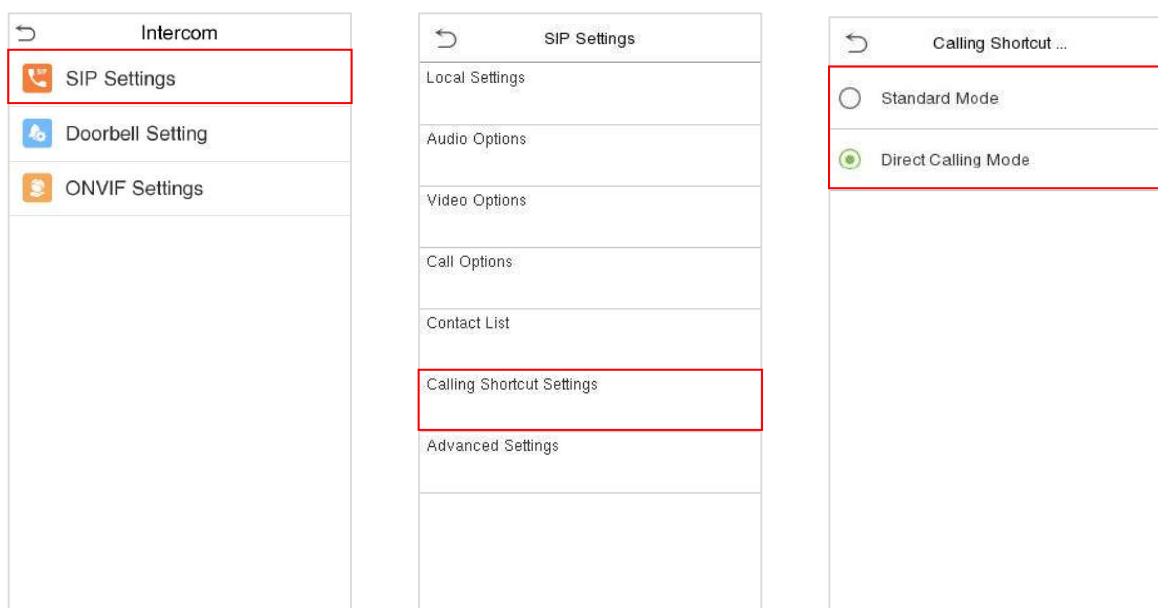


### For example:

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





- **Scenario 1:** One room number assigned to five people. You can select up to five people.
  - **Scenario 2:** Two room numbers, each with three people assigned.
  - **Scenario 3:** Six room numbers, each assigned to one person.
2. Click **Intercom > SIP Settings > Calling Shortcut Settings > Call Mode** and set the call mode to **Standard Mode** or **Direct Calling Mode**, the person who receives the call will vary depending on the selected call mode and the setup in each of the above scenarios. Refer to the figure below for visual guidance on configuring Call Mode.



### ● **Standard Mode:**


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



### ● **Direct Calling Mode:**

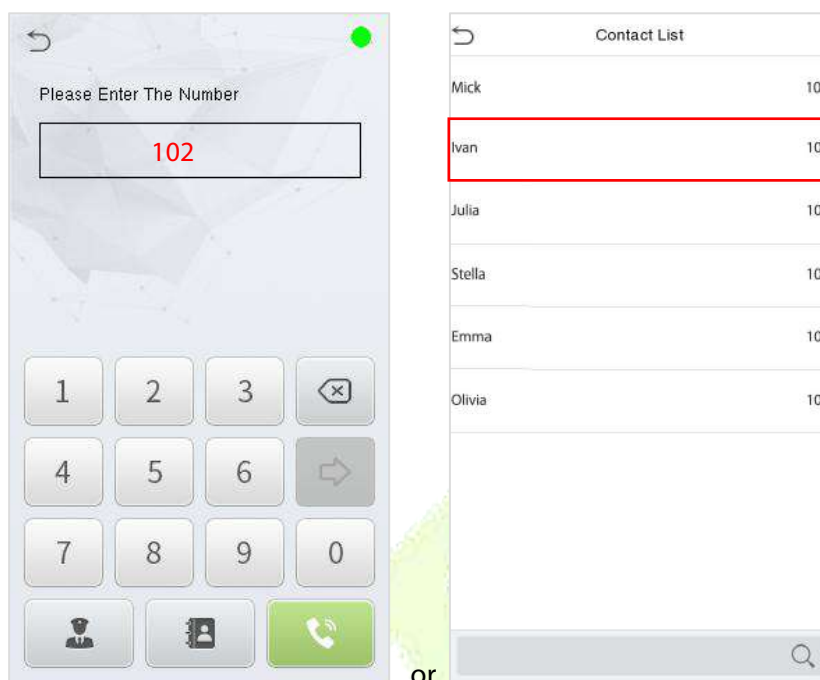
- **Scenario 1:** When you press the  key, all five people in the room will be called simultaneously. Once one person answers, the calls to the others will be automatically disconnected.
- **Scenario 2:** When you press the  key, you can only call the first five people listed in the app. These first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


totaling five people. E.g.

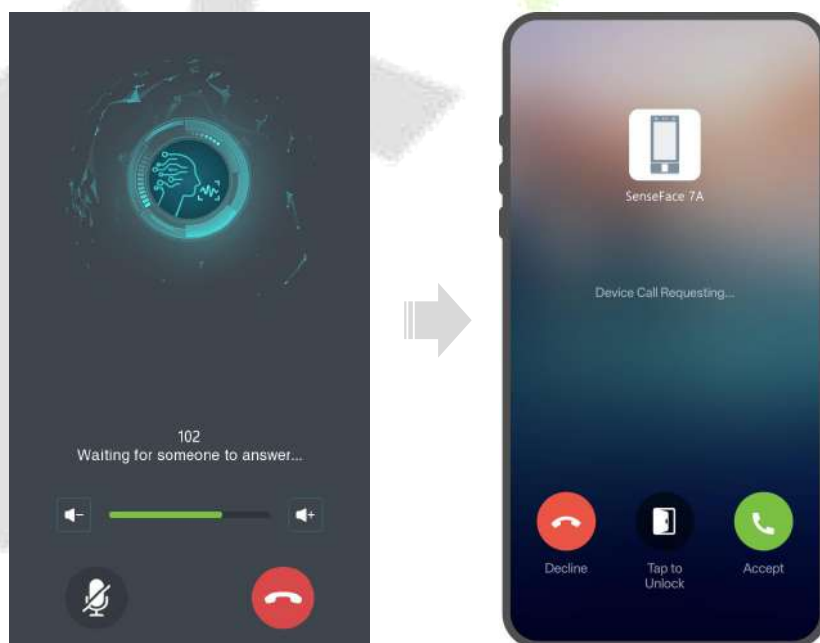


- **Scenario 3:** When you press the  key, you can only call the first five people listed in the app. These first five people appear on the app interface, with each room sorted from left to right, totaling five people.

3. After the setting is successful, you can Press the  key on the device and enter the person's number in the pop-up interface to call them or click the  icon on the call page to open the contact list, then search and select the person from the pop-up interface to place the call.



4. When the device places a call to the phone, the mobile app will display the answer interface as shown below. Click the  icon to answer the call.



5. After answering the call, you will enter the call interface shown in the figure.



## 22. Connecting to ZKBio Zlink Web Portal

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

Change the device communication protocol to BEST protocol, then the device can be managed by ZKBio Zlink, please refer to [8.5 Device Type Setting](#).


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

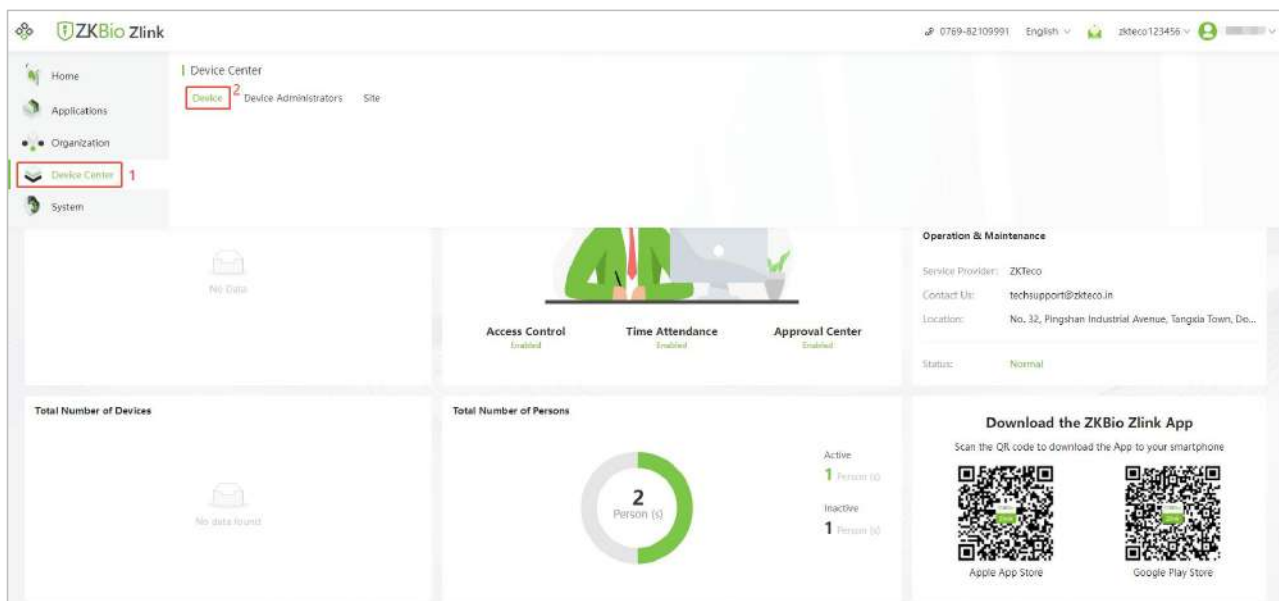
### 22.1 Login to the Web Portal

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

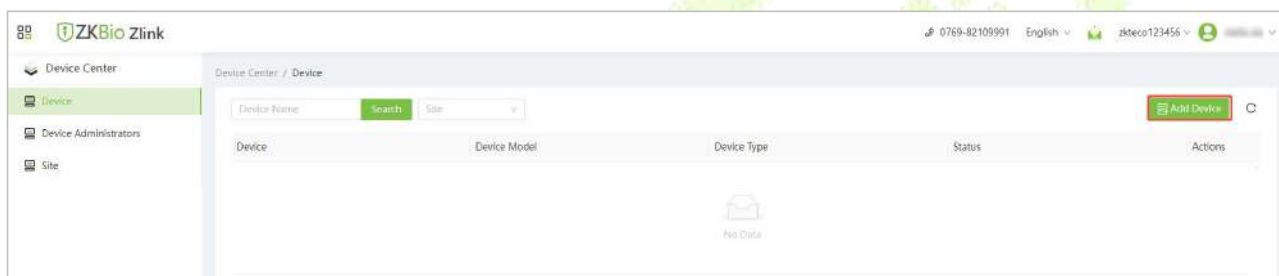


### 22.2 Add Device on the Web Portal

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



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

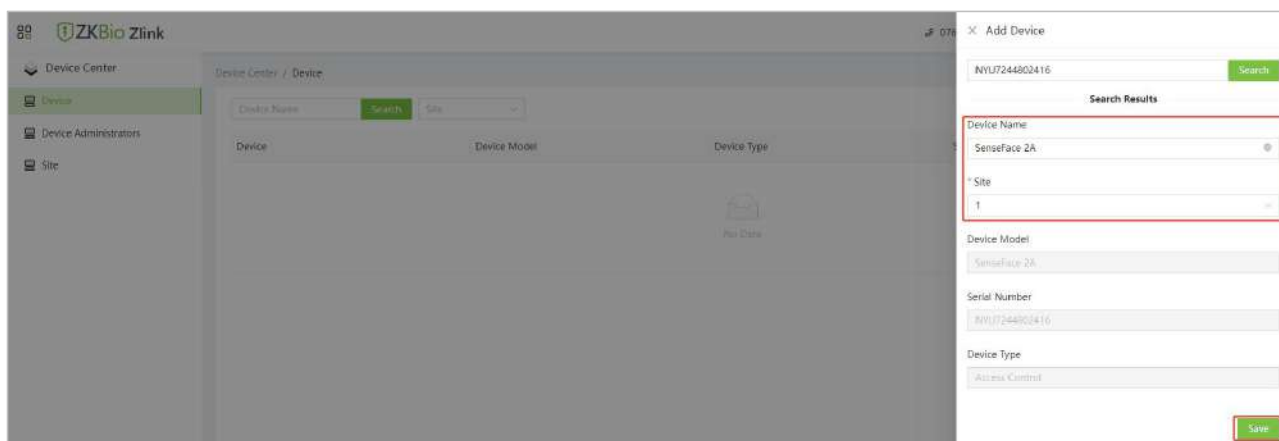


3. Enter the Serial Number and click **[Search]**.

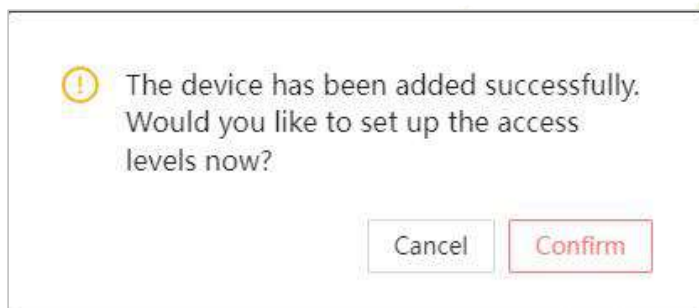


4. Then enter the device name and specify the device to a site. Select Site from the drop- down menu. Click **[Save]** to complete the addition.





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



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

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

## 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**

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

2. All the functions of displaying the biometric information are disabled in our products by default. You can choose Menu > System Settings to set whether to display the biometric information. If you enable these functions, we assume that you are aware of the personal privacy security risks specified in the privacy policy.
3. Only your user ID is displayed by default. You can set whether to display other user verification information (such as Name, Department, Photo, etc.) under the Administrator privilege. **If you choose to display such information, we assume that you are aware of the potential security risks (for example, your photo will be displayed on the device interface).**
4. The camera function is disabled in our products by default. If you want to enable this function to take pictures of yourself for attendance recording or take pictures of strangers for access control, the product will enable the prompt tone of the camera. **Once you enable this function, we assume that you are aware of the potential security risks.**
5. All the data collected by our products is encrypted using the AES 256 algorithm. All the data uploaded by the Administrator to our products are automatically encrypted using the AES 256 algorithm and stored securely. If the Administrator downloads data from our products, we assume that you need to process the data and you have known the potential security risk. In such a case, you shall take the responsibility for storing the data. You shall know that some data cannot be downloaded for sake of data security.
6. All the personal information in our products can be queried, modified, or deleted. If you no longer use our products, please clear your personal data.

### III. How we handle personal information of minors

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

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

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

### IV. Others

You can visit [https://www.zkteco.com/cn/index/Index/privacy\\_protection.html](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)

