

USER MANUAL

FaceTima 8

Version: 1.0

Date: September 2026

English

Green
Label

Copyright © 2026 ZKTECO CO., LTD. All rights reserved.

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

Trademark

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

Disclaimer

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

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

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

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

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

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

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

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

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

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

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

ZKTeco Headquarters

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

Phone +86 769 - 82109991

Fax +86 755 - 89602394

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

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

About the Company

ZKTeco is one of the world's largest manufacturer of RFID and Biometric (Fingerprint, Facial, Finger-vein) readers. Product offerings include Access Control readers and panels, Near & Far-range Facial Recognition Cameras, Elevator/floor access controllers, Turnstiles, License Plate Recognition (LPR) gate controllers and Consumer products including battery-operated fingerprint and face 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 **FaceTima 8**.

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

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

Document Conventions

Conventions used in this manual are listed below:

GUI Conventions

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

Symbols

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

TABLE OF CONTENTS

DATA SECURITY STATEMENT	8
SAFETY MEASURES	8
1 INSTRUCTION FOR USE	10
1.1 Finger Positioning★	10
1.2 Standing Position, Posture and Facial Expression	10
1.3 Face Template Registration	11
1.4 Standby Interface	13
1.5 Virtual Keyboard	14
1.6 Verification Mode	14
1.6.1 Fingerprint Verification★	14
1.6.2 QR Code Verification★	17
1.6.3 Card Verification	17
1.6.4 Facial Verification	20
1.6.5 Password Verification.....	22
1.6.6 Combined Verification.....	24
2 MAIN MENU	25
3 USER MANAGEMENT	27
3.1 User Registration.....	27
3.1.1 User PIN and Name	27
3.1.2 User Role	28
3.1.3 Fingerprint★	29
3.1.4 Card Number.....	30
3.1.5 Password.....	31
3.1.6 Face	32
3.1.7 Access Control Role	32
3.2 Search for Users.....	33
3.3 Edit User	33
3.4 Delete User.....	34
4 ACCESS CONTROL.....	35
4.1 Access Control Options	35
4.2 Access Control Record Settings	37
4.3 Time Rules	38
4.4 Holiday Settings	40
4.5 Anti-passback Setup.....	41
4.6 Duress Alarm Settings.....	42
5 RECORD QUERY	44

6	DATA MANAGEMENT	46
7	NETWORK SETTINGS	48
7.1	TCP/IP Settings	48
7.2	Wi-Fi Settings	49
7.3	Mobile Network★	50
7.4	Cloud Services Settings	50
8	INTERCOM SETTINGS	52
9	BIOMETRIC PARAMETERS	53
9.1	Face Parameters	53
9.2	Fingerprint Parameters★	55
9.3	Password Parameters	56
9.4	Other Parameters	56
10	AUTO TESTING	58
11	SYSTEM SETTINGS	59
11.1	Date and Time	59
11.2	Language Settings	60
11.3	Sound Settings	61
11.4	Wiegand Settings	61
11.4.1	Wiegand Input	62
11.4.2	Wiegand Output	64
11.5	Display Settings	65
11.6	Equipment Maintenance	66
11.7	Security Settings	67
12	ABOUT DEVICE	68
13	WEBSERVER	69
13.1	Login WebServer	69
13.2	Dashboard	69
13.3	User	70
13.4	Access	72
13.4.1	Access Group	72
13.4.2	Multi-Person Group	72
13.5	Device	73
13.6	Communication	73
13.7	Reports	74
13.8	Intercom	75
13.8.1	Intercom Switch	75
13.8.2	SIP Server	75
13.8.3	Call Options	76
13.8.4	Butler Setting	77
13.8.5	Contacts	77

13.9	System.....	80
13.9.1	Device Maintenance.....	80
13.9.2	Theme Style	81
13.9.3	About.....	81
14	CONNECT TO ZKBIO CVSECURITY SOFTWARE.....	82
14.1	Set the Communication Address	82
14.2	Add Device on the Software	83
14.3	Add Personnel on the Software.....	84
14.4	Mobile Credential★	85
15	SIP VIDEO INTERCOM	89
15.1	Local Area Network Use	89
15.1.1	Call by Room Number / Contacts.....	90
15.1.2	Call Admin.....	91
15.2	SIP Server	92
15.2.1	SIP Server Configuration	92
15.2.2	Add Device	96
15.2.3	Create Extension Numbers.....	97
15.2.4	Contact List	99
15.2.5	Assignment of Extension Numbers and SIP Accounts	100
15.2.6	PC Client Functionality	106
15.2.7	Make a Call	109
APPENDIX 1		113
	Requirements of Live Collection and Registration of Visible Light Face Templates	113
	Requirements for Visible Light Digital Face Template Data	114
APPENDIX 2		115
	Privacy Policy.....	115
	Eco-friendly Operation	117

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.

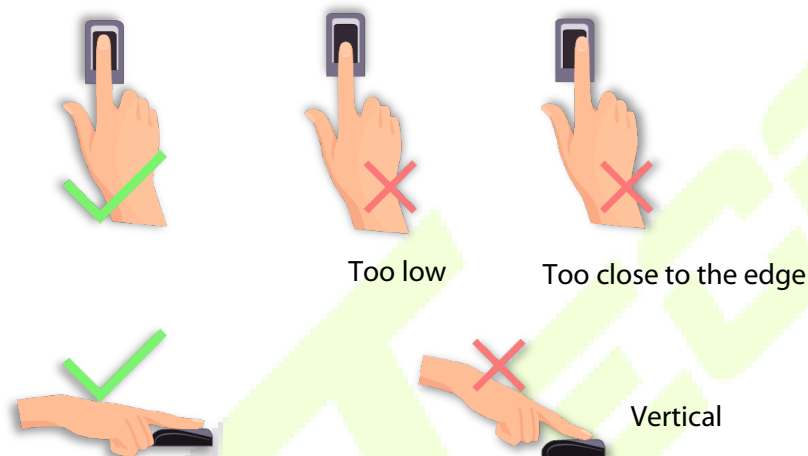


1 Instruction for Use

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

1.1 Finger Positioning★

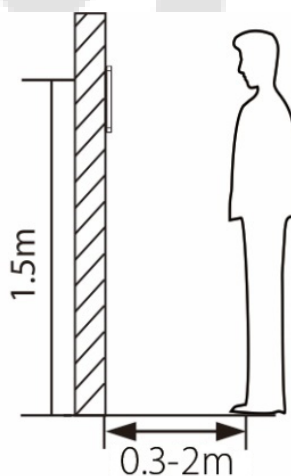
Recommended fingers: The index, middle, or ring fingers are recommended fingers to use, and avoid using the thumb or pinky, as they are difficult to position correctly onto the fingerprint reader.



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.

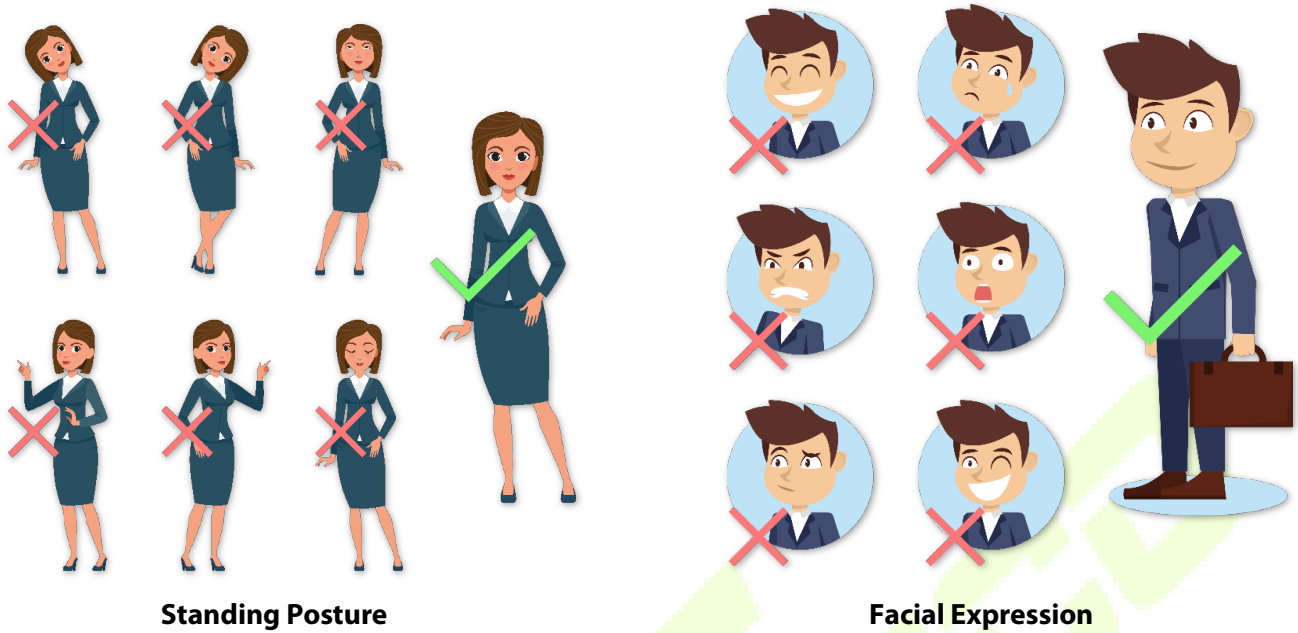
1.2 Standing Position, Posture and Facial Expression

- 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 0.3m to 2m. Users may slightly move forward or backward to improve the quality of facial images captured.

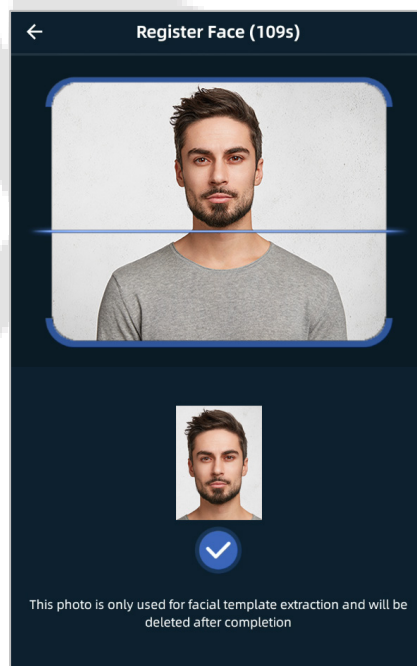
- **Recommended standing posture and facial expression:**



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 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

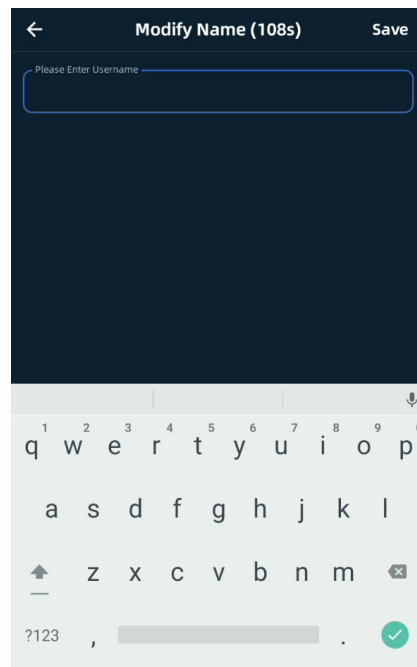
After connecting the power supply, the following standby interface template is displayed:



- Click  icon to enter the User ID input interface.
- Click  icon to enter the video intercom call page. For specific operation methods, please refer to the introduction in "[15 SIP Video Intercom](#)" below.
- Click  icon to open the contacts and select the one you want to call.
- When there is no Super Administrator set in the device, tap  icon at the top right corner to go to the menu.
- After setting the Administrator on the device, it requires the Administrator's verification before entering the menu functions.

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

1.5 Virtual Keyboard



Note:

The type of device keyboard will be consistent with the system language. Long press the "," button to set the keyboard language.

- Press **?123** to switch to the numeric and symbolic keyboard.
- Click **ABC** to return to the alphabetic keyboard.

1.6 Verification Mode

1.6.1 Fingerprint Verification★

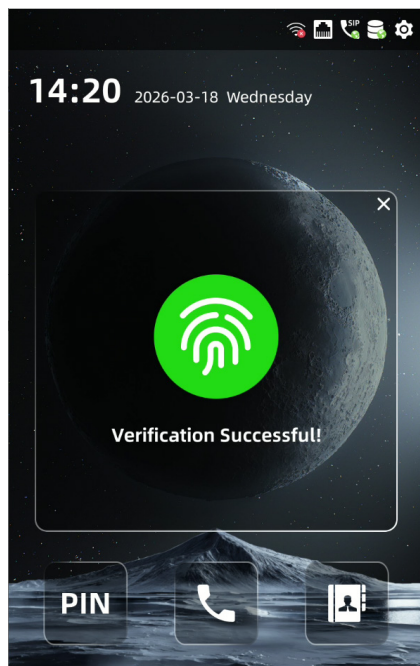
● 1: N Fingerprint Verification Mode

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

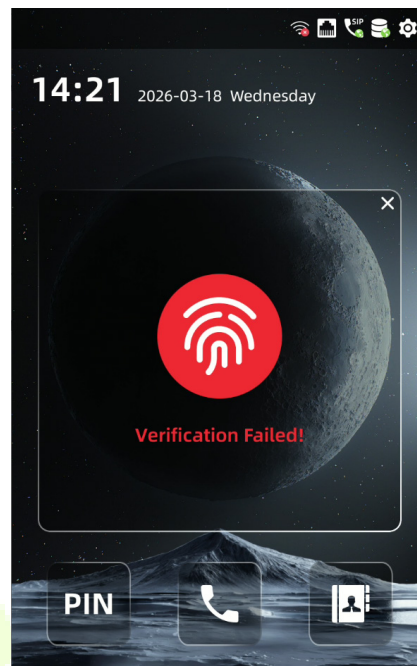
Fingerprint authentication mode is activated when a user places their finger onto the fingerprint scanner.

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:



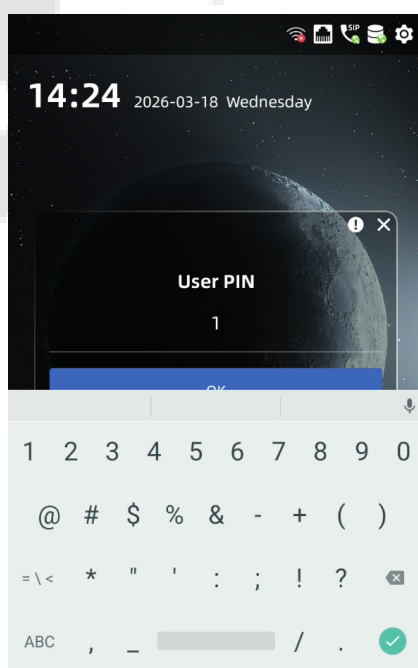
● 1: 1 Fingerprint Verification Mode

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

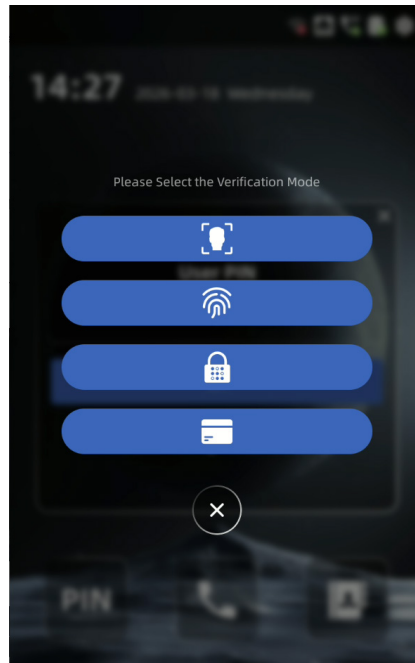
In case users are unable to gain access using the 1:N authentication method, they can attempt to verify their identity using the 1:1 verification mode.

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

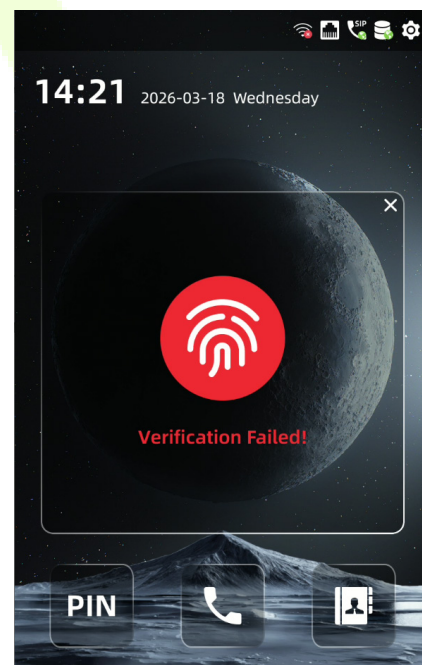


Press the fingerprint to verify.

Verification is successful:



Verification is failed:



1.6.2 QR Code Verification★

Tap **Mobile Credential** on the ZKBio Zexus Mobile Page, and a QR code will appear, which includes employee ID and card number information. The QR code can replace a physical card on a specific device to achieve contactless authentication. Please refer to [14.4 Mobile Credential](#).

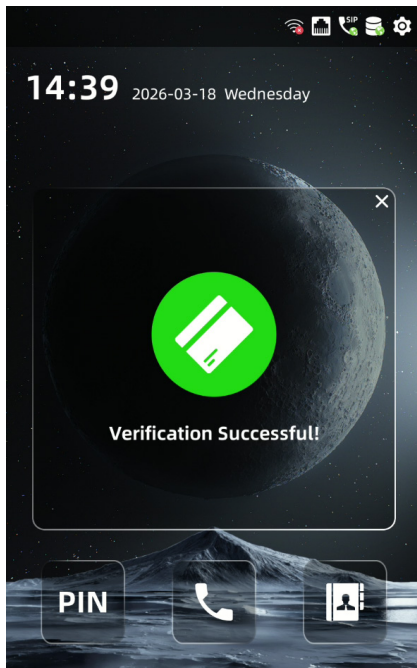


1.6.3 Card Verification

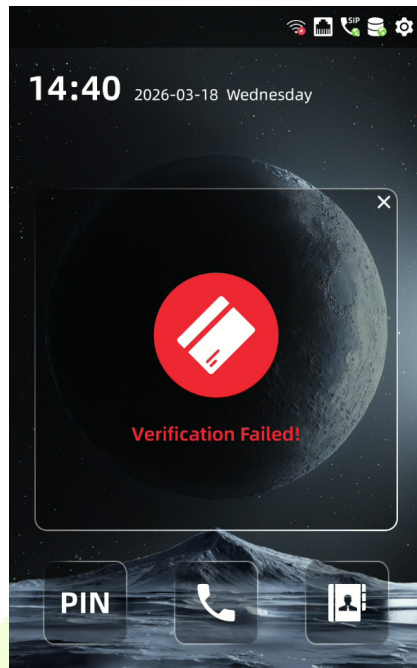
● 1:N card verification

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; The following screen displays on the card verification:

Verification is successful:



Verification is failed:

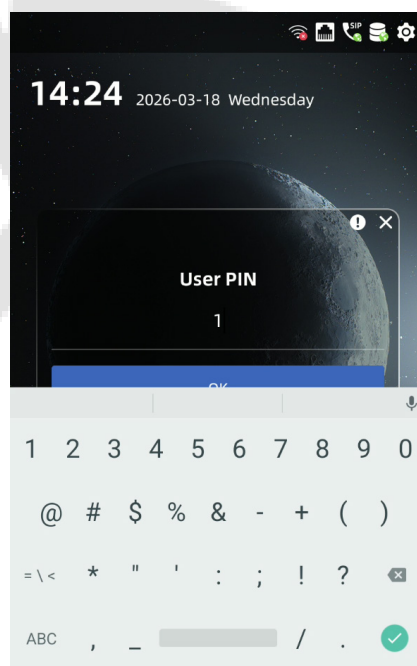


● 1:1 card verification

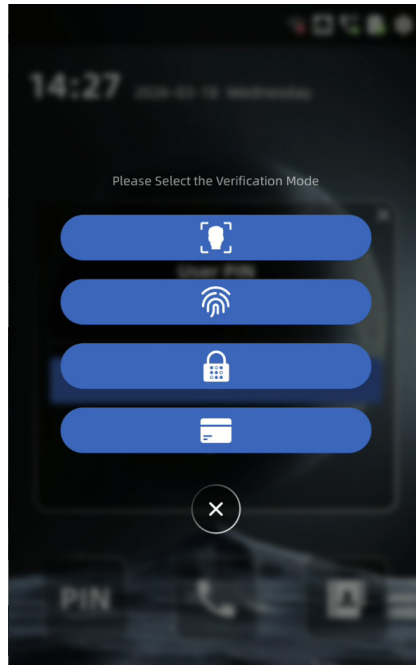
The 1:1 card verification mode compares the card number in the card induction area with the number associated with the employee's User ID registered in the device.

Press  in the main interface to open the 1:1 card verification mode.

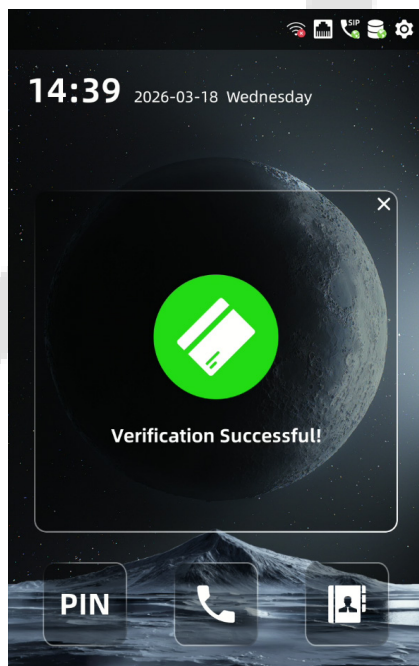
Enter the user ID and click **OK**.



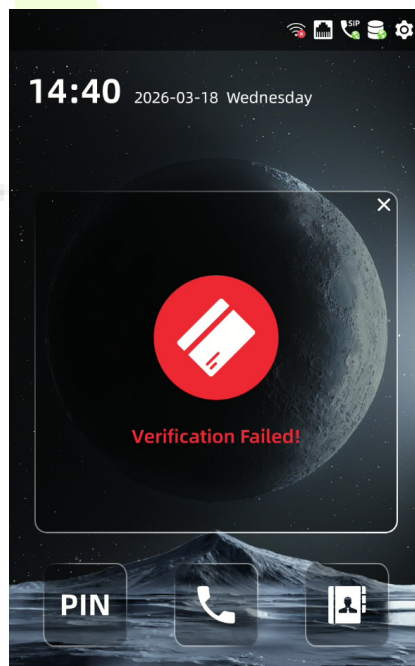
If the user has registered face template, fingerprint★ and password in addition to his/her card, and the verification method is set to Fingerprint/Password/Card/Face, the following screen will appear. Select the  icon to enter the card verification mode.



Verification is successful:



Verification is failed:

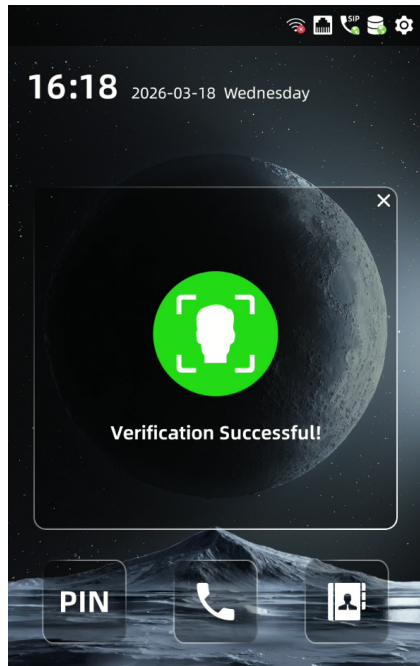


1.6.4 Facial Verification

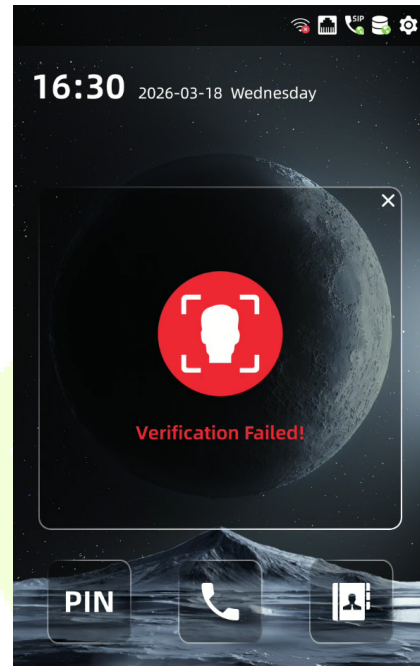
● 1:N Facial Verification

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

Verification is successful:

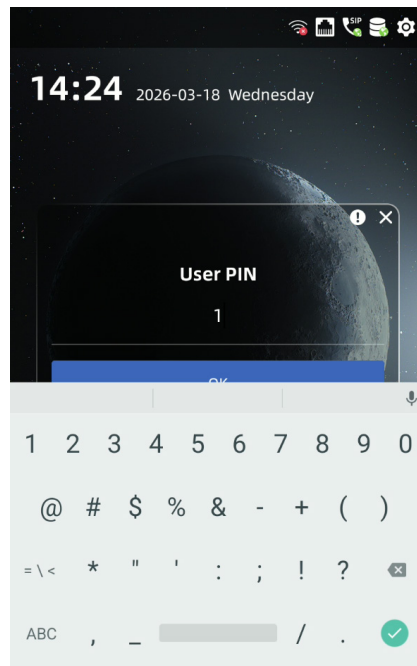


Verification is failed:

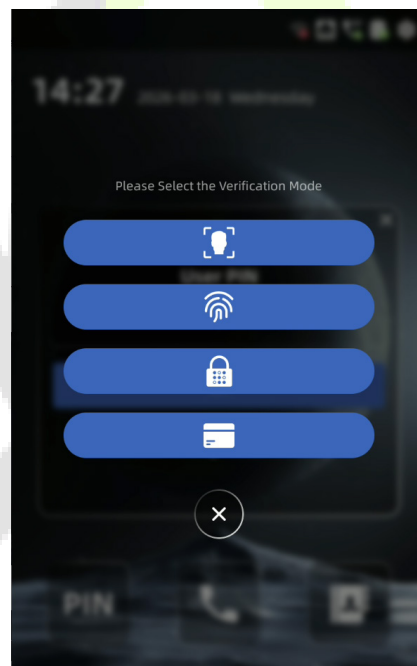


● 1:1 Facial Verification

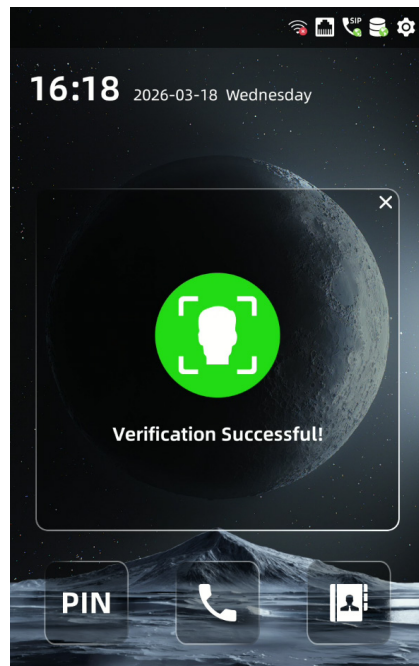
In this verification mode, the device compares the face template captured by the camera with the facial template related to the entered user ID. Press icon  in the main interface and enter the 1:1 facial verification mode and enter the user ID and click **OK**.



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



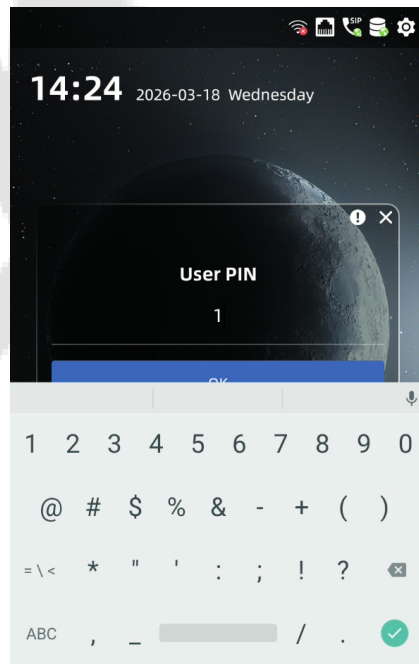
After successful verification, the prompt box displays **Verification Successful!**, as shown below:



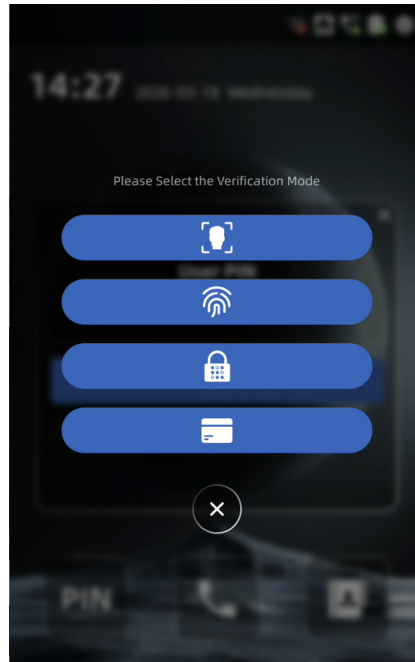
1.6.5 Password Verification

The device compares the entered password with the registered password associated with 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**.



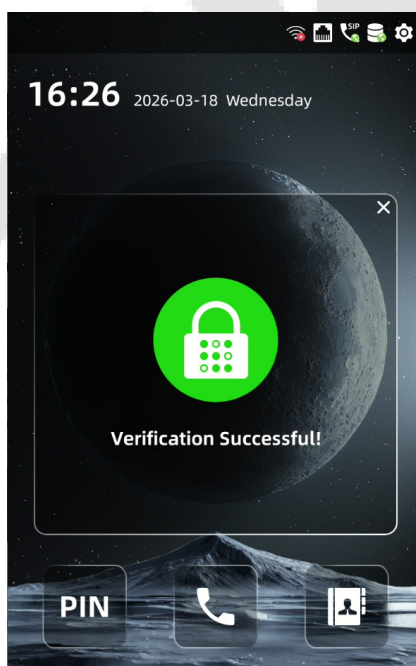
If the user has registered face template, fingerprint★ and card in addition to password, and the verification method is set to Fingerprint/Password/Card/Face, the following screen will appear. Select the  icon to enter password verification mode.



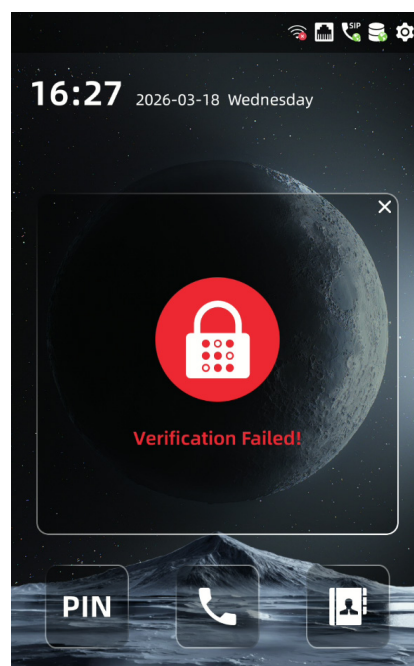
Input the password and press **OK**.

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

Verification is successful:



Verification is failed:

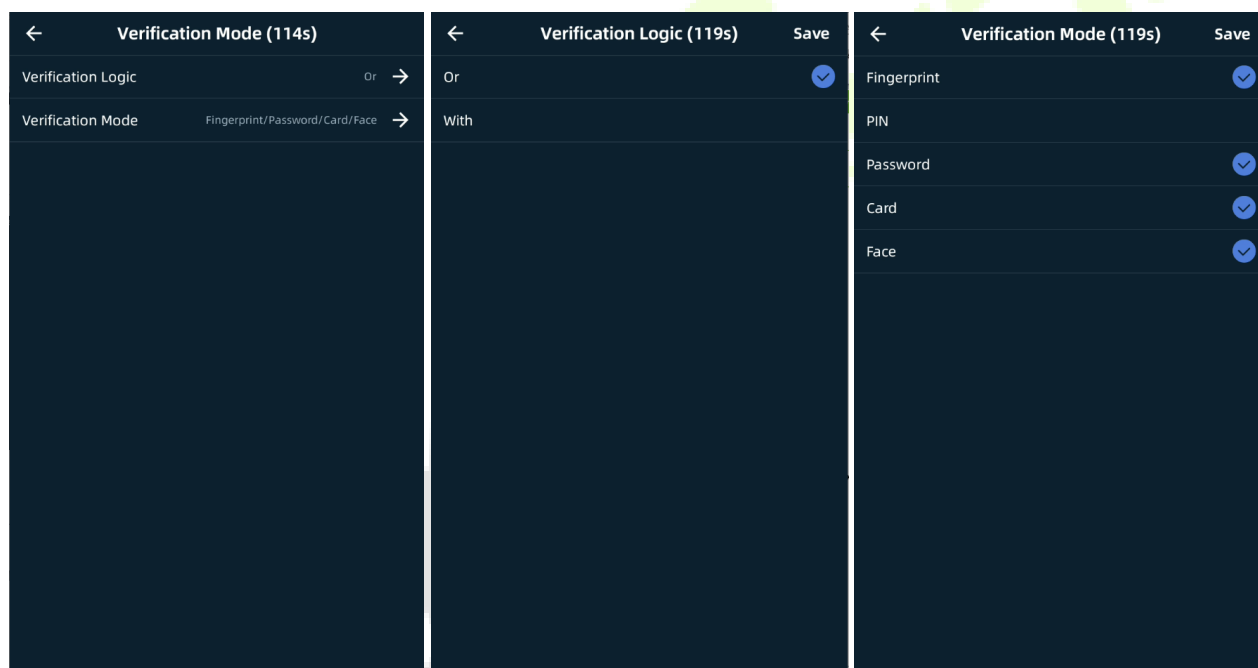


1.6.6 Combined Verification

To increase security, this device offers the option of using multiple forms of verification methods. 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.
+	with	This method compares the entered verification of a person with all the verification template previously stored to that Personnel ID in the Device.

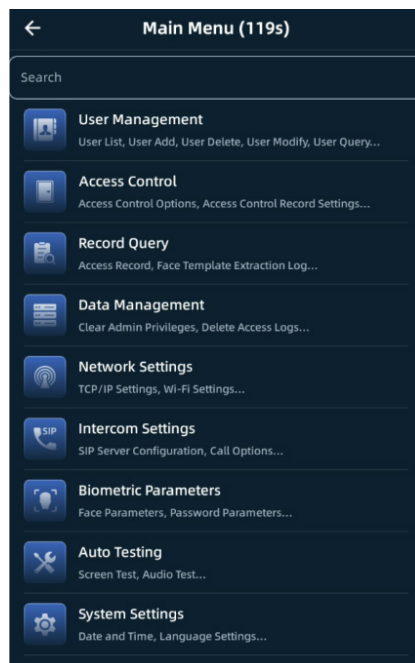


Procedure to set for Combined Verification Mode:

- 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 face template, but the Device verification mode is set as “Face + Password”, the employee will not be able to complete the verification process successfully.
- This is because the Device compares the scanned face template of the person with registered verification template (both the face template and the password) previously stored to that Personnel ID in the Device.
- But as the employee has registered only the face template but not the Password, the verification will not get completed and the Device displays Verification Failed.

2 Main Menu

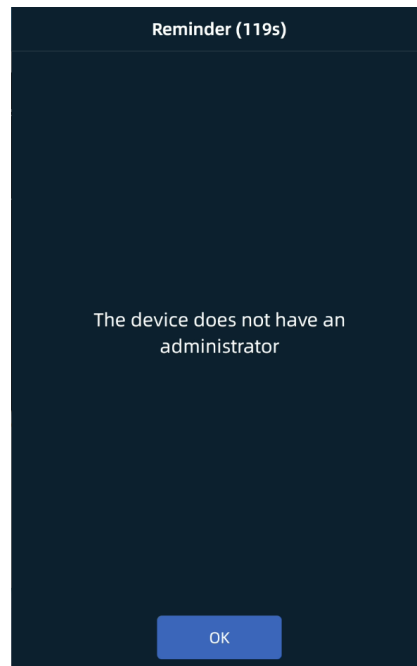
Press  at the top right corner of the Standby interface to enter the **Main Menu**, the following screen will be displayed:



Function Description

Menu	Descriptions
User Management	To add, edit, view, and delete basic information of a User.
Access Control	To set the parameters of the lock and the relevant access control device including options like access record settings, time rule, holiday settings, anti-passback setup, and duress alarm settings.
Record Query	To query the specified access records and face template extraction logs.
Data Management	To delete all relevant data in the device.
Network Settings	To set the relevant parameters of network, Wi-Fi, mobile network★ and cloud services.
Intercom Settings	To set the parameters related to the SIP.
Biometric Parameters	To set the parameters of face, fingerprint★, password and other.
Auto Testing	To automatically test whether each module functions properly, including the screen, audio, camera, network, Wiegand, RS485 and relay.
System Settings	To set the parameters related to the system, including date and time, language, sound, Wiegand, display, equipment maintenance and security settings.
About Device	To view data capacity, device and firmware information and online upgrade.

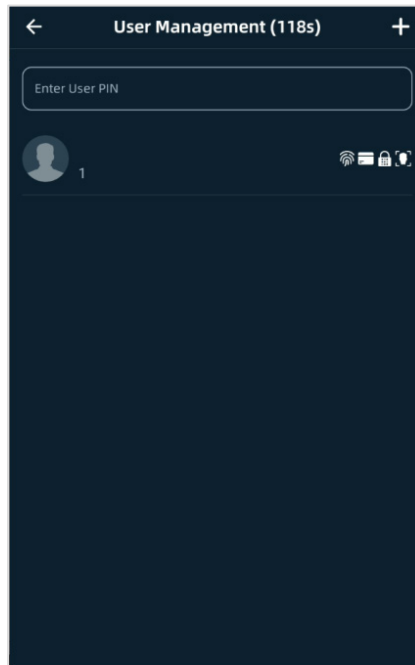
Note: When users use the product for the first time, they should operate it after setting administrator privileges. Tap **User Management** to add an administrator or edit user permissions as an administrator. If the product does not have an administrator setting, the system will show an administrator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



3 User Management

3.1 User Registration

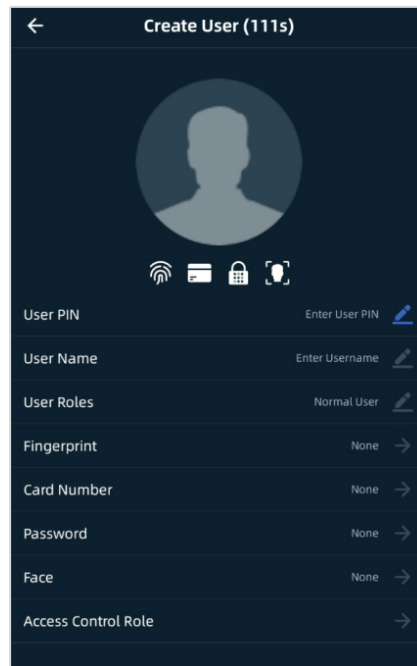
Click **User Management** on the main menu.



Click the  button in the top right corner of the User Management interface to enter the user creation interface.

3.1.1 User PIN and Name

Enter the **User PIN** and **User Name**.

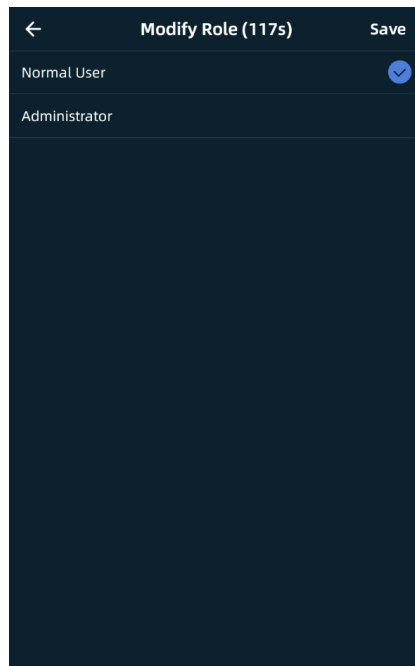
**Notes:**

- A username can contain a maximum of 34 characters.
- The user PIN may contain 1 to 14 digits and support letters by default.
- During the initial registration, you can set your ID, which cannot be modified after registration.
- If a message **Error: User Already Exists!** pops up, you must choose another ID as the enter User ID already exists.

3.1.2 User Role

On the Create User interface, tap on **User Roles** to set the role for the user as either **Normal User** or **Administrator**.

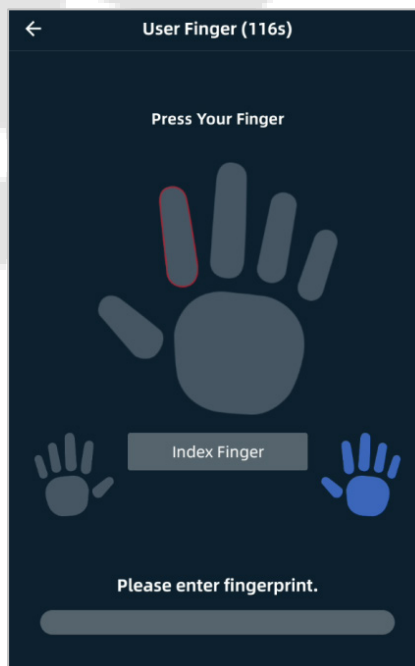
- **Administrator:** The Administrator owns all management privileges in the Device.
- **Normal User:** If the Administrator is already registered in the Device, then the Normal Users will not have the privileges to manage the system and can only access authentication verifications.

**Note:**

- 1) The user needs to enrol for the verification mode before setting the user role.
- 2) If the selected user role is the Administrator, the user must pass the identity authentication to access the main menu. The authentication is based on the authentication method(s) that the administrator has registered. Please refer to [1.6 Verification Mode](#).

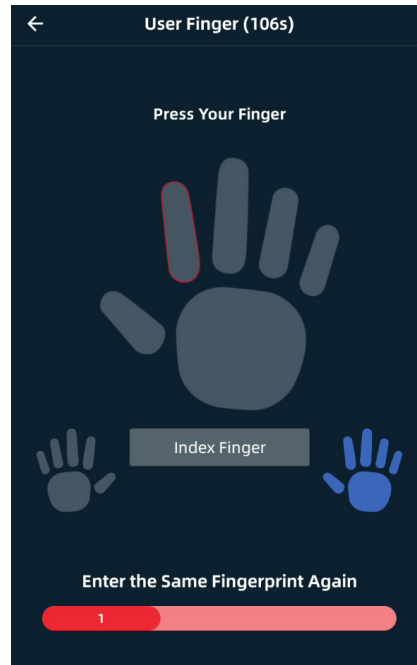
3.1.3 Fingerprint★

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



Press the same finger on the fingerprint reader three times. If the fingerprint is successfully registered, the system will proceed to enroll the next fingerprint.

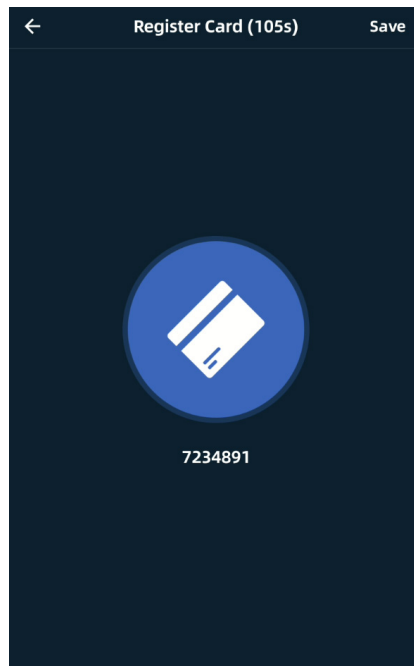
NOTE: If you tap different fingers onto the fingerprint scanner during the 2nd and 3rd time, the user will be prompted to "**Enter the Same Fingerprint Again**" as shown in the below image.



3.1.4 Card Number

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

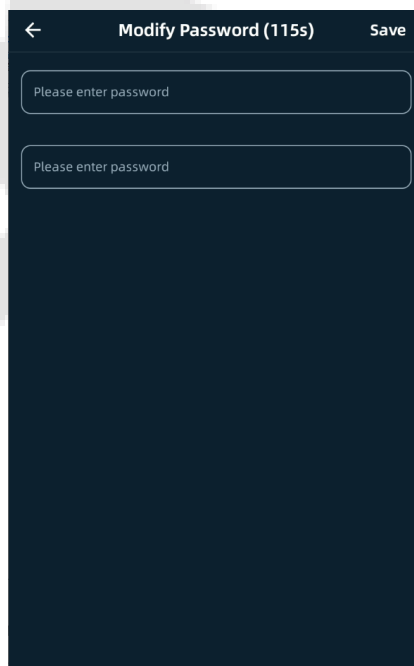
- On the Card interface, swiping card underneath the card reading area. The card registration will be successful.
- If the card is registered already then, the **Card number already registered** message shows up. The registration interface is as follows:



3.1.5 Password

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

- On the Password interface, enter the required password and re-enter to confirm it and tap **Save**.
- If the re-entered password is different from the initially entered password, then the device prompts the message as **Passwords Do Not Match**, where the user needs to re-confirm the password again.

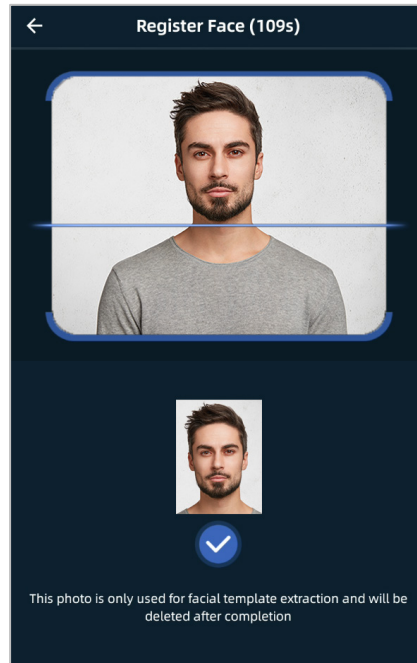


Note: The password may contain 6 to 8 digits by default.

3.1.6 Face

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

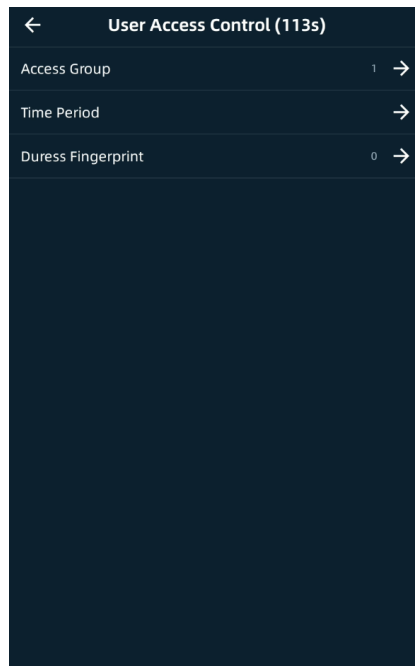
- Please face towards the camera and position your face inside the guiding box and stay still during face template registration. The registration interface is as follows:



3.1.7 Access Control Role

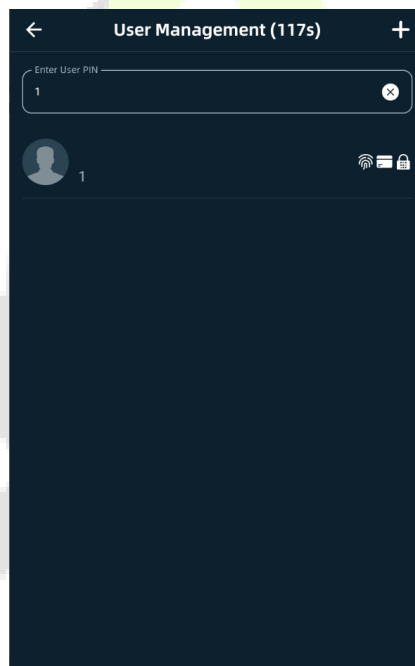
The **Access Control Role** sets the door access privilege for each user. This includes the access group, duress fingerprint★ and facilitates to set the group access time-period.

- Tap **Access Control Role > Access Group**, to assign the registered users to different groups for better management. The device supports up to 99 Access Control groups.
- Tap **Time Period**, to select the time rule to use.
- The user may specify one or more fingerprints that have been registered as a duress fingerprint(s). When a user presses the finger corresponding to the duress fingerprint on the sensor and pass the verification, the system will immediately generate an external alarm.



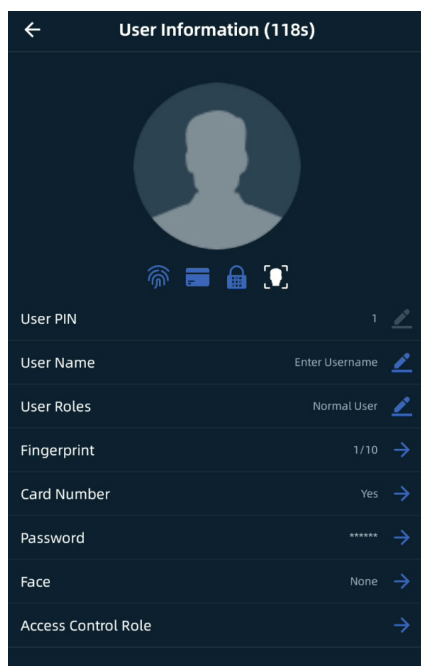
3.2 Search for Users

On the **User Management** interface, tap on the search bar and enter the User PIN, the system will search for the related user.



3.3 Edit User

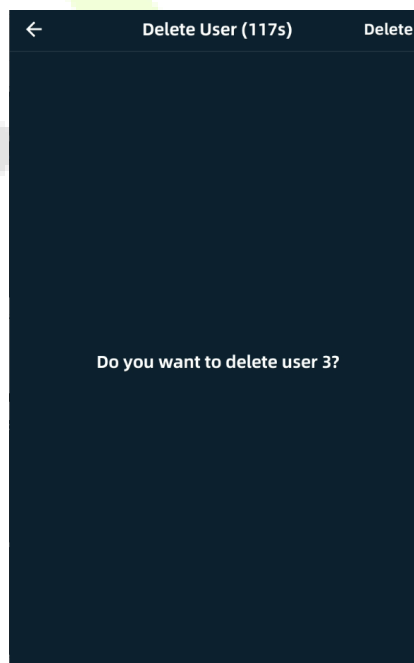
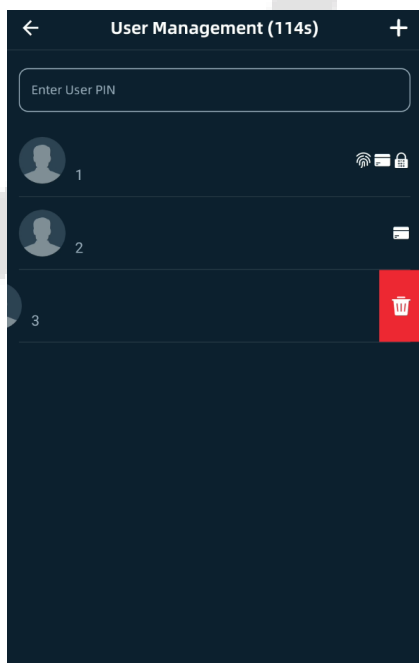
On **User Management** interface, tap on the required user from the list to edit the user information.



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. For details, refer to "[Section 3 User Management](#)".

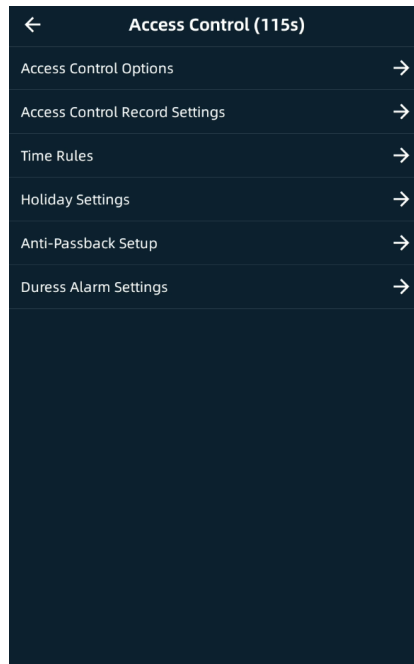
3.4 Delete User

On **User Management** interface, select the required user and slide left. Tap  to delete the user, then tap **Delete** to confirm the deletion.



4 Access Control

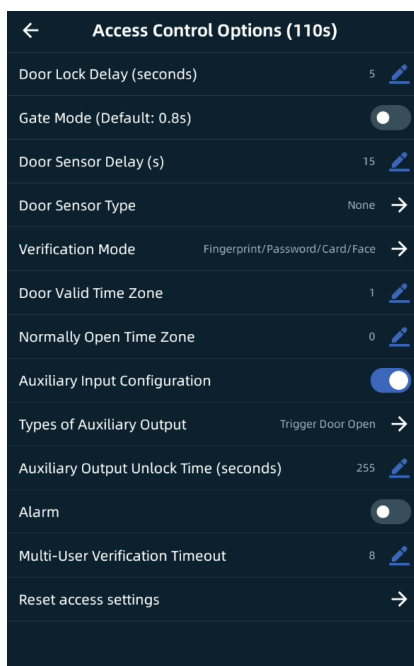
On the **Main Menu**, tap **Access Control** to set the schedule of door opening, locks control and to configure other parameters settings related to access control.



- **To gain access, the registered user must meet the following conditions:**
 - The relevant door's current unlock time must fall within any valid time zone of the user's period.
 - The user's group must be included in the door unlock combination. If other groups are also part of the same access combination, their members must be verified as well to unlock the door.

4.1 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.



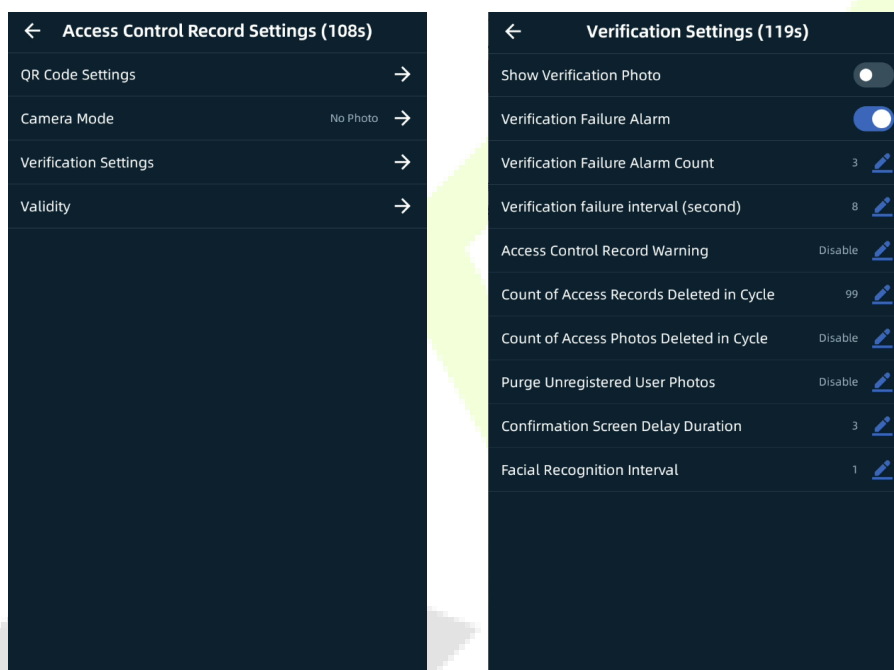
Function Description

Function Name	Description
Door Lock Delay (seconds)	The length of time that the device controls the electric lock to be in unlock state. Valid value: 1 to 254 seconds.
Gate Mode (Default: 0.8s)	Toggle between ON or OFF switch to get into gate control mode or not. When set to ON , Door Sensor Relay and Door Sensor Type options will be removed from this interface.
Door Sensor Delay (s)	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.
Door Sensor Type	There are three Sensor types: None , Normally Open and Normally Closed . None : It means door sensor is not in use. Normally Open : It means the door is always left opened when electric power is on. Normally Closed : It means the door is always left closed when electric power is on.
Verification Mode	Set the verification mode, where "/" represents "or" and "+" represents "with".
Door Valid Time Zone	To set time period for door, so that the door is available only during that period.
Normally Open Time Zone	Scheduled time period for "Normally Open" mode, so that the door is always left open during this period.
Auxiliary Input Configuration	Sets the door unlock time period and auxiliary output type of the auxiliary terminal device. Auxiliary output types include None, Trigger Door Open, Trigger Alarm, Trigger Door Open and Alarm.
Alarm	Set whether to enable the alarm function.

Multi-User Verification Timeout	Used to set the time for door opening verification during multi-person verification. Valid values range from 8 to 300 seconds.
Reset Access Settings	The access control reset parameters include door lock delay, door sensor delay, door sensor type, verification mode, door valid time zone, normally open time zone, and alarm. However, erased access control data in Data Management is excluded.

4.2 Access Control Record Settings

Click **Access Control Record Settings** on the Access Control interface.



Function Description:

Function Name	Description
QR Code Settings★	Unencrypted QR Code as Card Number: After enabled, the device supports static QR code.
Camera Mode	This function is disabled by default. When enabled, a security prompt will pop-up and the sound of shutter in the camera will turn on mandatorily. There are 4 modes: No Photo: No photo is taken during user verification. Capture and Save Photo: Photo is taken and saved during verification. Save After Successful Verification: Photo is taken and saved for each successful verification. Save After Failed Verification: Photo will be taken and saved only for each failed verification.

Verification Settings	Show Verification Photo: This function is disabled by default. When enabled, there will be a security prompt. Verification Failure Alarm: Choose whether to enable the verification failure alarm function. Once enabled, you can set the verification failure alarm count and verification failure interval. When the number of verification failures reaches the set value, an alarm signal will be generated (valid values are 3 to 100). Access Control Record Warning: When the record space of access reaches the maximum threshold value, the device will automatically display the memory space warning. Users may disable the function or set a valid value between 1 and 9999. Count of Access Records Deleted in Cycle: 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. Count of Access Photos Deleted in Cycle: When access photos have reached full capacity, the device will automatically delete a set of old access photos. Users may disable the function or set a valid value between 1 and 99. Purge Unregistered User Photos: When unregistered user photos have reached full capacity, the device will automatically delete a set of old unregistered user photos. Users may disable the function or set a valid value between 1 and 99. Confirmation Screen Delay Duration: The time length of the message of successful verification displays. Valid value: 1~9 seconds. Facial Recognition Interval: To set the facial template matching time interval as required. Valid value: 0~9 seconds.
Validity	User Validity Settings: Used to determine whether it supports setting the user validity period during user registration.

4.3 Time Rules

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

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

Tap the search bar to enter the required Time Rule number (maximum up to 50 rules).

← Time Rules (13s)

Please enter the time rule number (2~50) 🔍

2

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

3

Sunday	[00:00 00:00]	
Monday	[00:00 00:00]	
Tuesday	[00:00 00:00]	
Wednesday	[00:00 00:00]	
Thursday	[00:00 10:15]	[10:26 11:00] [20:01 23:00]
Friday	[00:00 00:00]	
Saturday	[00:00 00:00]	
Holiday 1	[00:00 00:00]	
Holiday 2	[00:00 00:00]	
Holiday 3	[00:00 10:10]	[14:00 16:00] [20:00 22:00]

4

Sunday	[00:00 00:00]	
--------	---------------	--

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

← Time Period2 (118s)

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

← Time Selection (108s)

00:00 To 00:00

00 : 00

01 01

02 02

Cancel OK

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

Notes:

- 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.

4.4 Holiday Settings

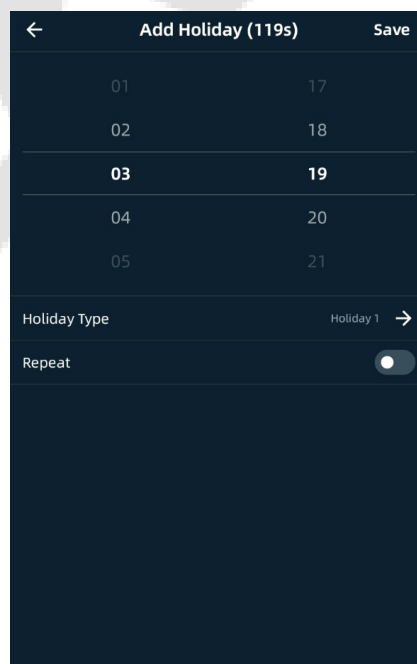
Whenever there is a holiday, you may need a special access time; but changing everyone's access time one by one is extremely cumbersome, so you can set a holiday access time which is applicable to all employees, and the user will be able to open the door during the holidays.

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



- **Add a new holiday:**

Click the  button in the top right corner of the **Holiday Settings** interface and set the holiday parameters.

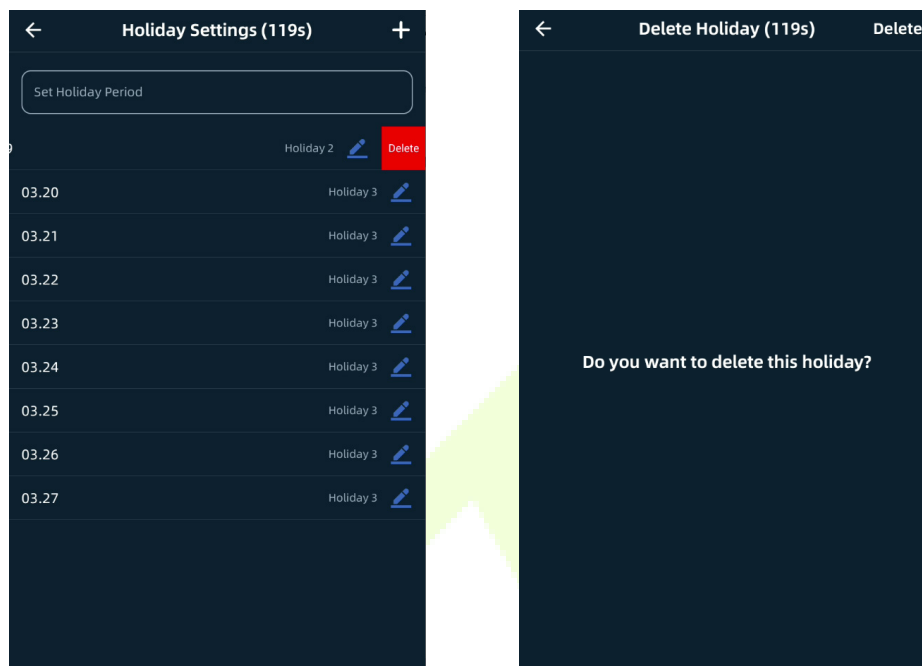


- **Edit a holiday:**

On the **Holiday Settings** interface, select a holiday item to be modified.

- **Delete a holiday:**

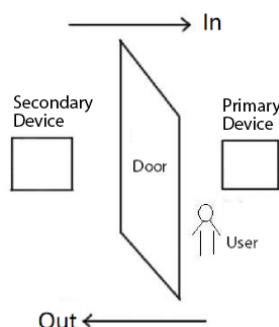
On the **Holiday Settings** interface, select a holiday item and slide left. Tap **Delete** to delete the holiday. Then tap **Delete** to confirm deletion. After deletion, this holiday is no longer displayed on **Holiday Settings** interface.



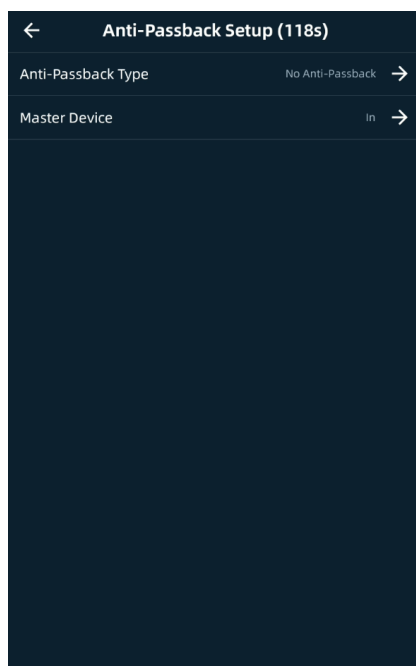
4.5 Anti-passback Setup

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 (primary device), and the other one is installed outside the door (secondary device). The two devices communicate via the Wiegand signal. The Wiegand format and Output type (User ID / Card Number) adopted by the primary device and secondary device must be consistent.



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



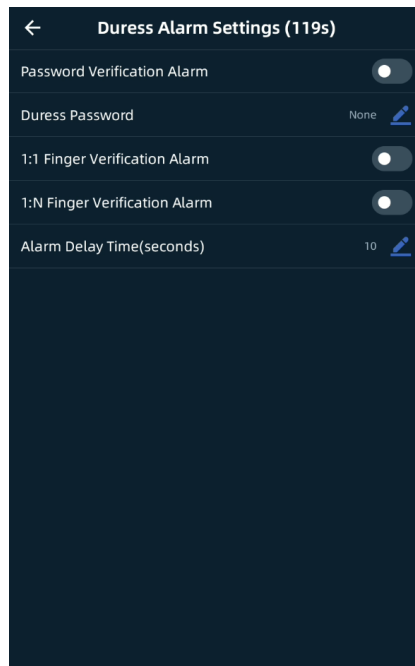
Function Description

Function Name	Description
Anti-passback Type	No Anti-passback: Anti-passback function is disabled, which means successful verification through either the primary device or secondary device can unlock the door. The attendance state is not saved in this option. Anti-passback Out: After a user check 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. Anti-passback In: After a user check 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. Anti-passback In/Out: After a user check 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.
Master Device	Set the state of the device as Out or In. Out: A record of verification on the device is a check-out record. In: A record of verification on the device is a check-in record.

4.6 Duress Alarm Settings

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 Alarm Settings** to configure the duress settings.



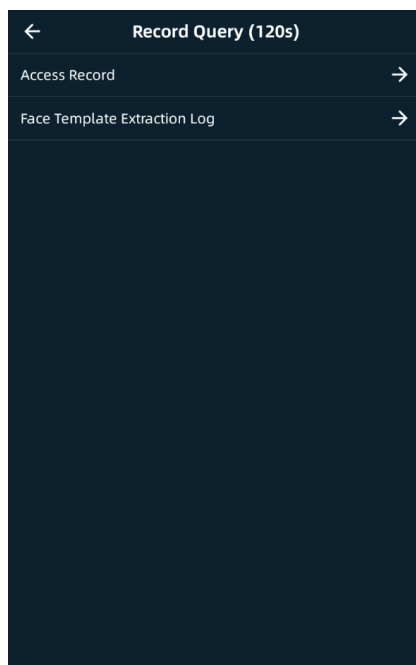
Function Description

Function Name	Description
Password Verification Alarm	After enabled, when a user uses the password verification method, an external alarm signal will be generated, otherwise there will be no alarm signal.
Duress Password	Set the 6-8 digits duress password. When the user enters this duress password for verification, an external alarm signal will be generated.
1:1 Finger Verification Alarm ★	After enabled, when a user uses any fingerprint to perform the 1:1 verification, an external alarm signal will be generated, otherwise there will be no alarm signal.
1:N Finger Verification Alarm ★	After enabled, when a user uses any fingerprint to perform 1:N verification, an external alarm signal will be generated, otherwise there will be no alarm signal.
Alarm Delay(s)	Alarm signal will not be transmitted until the alarm delay time is elapsed. The value ranges from 1 to 999 seconds.

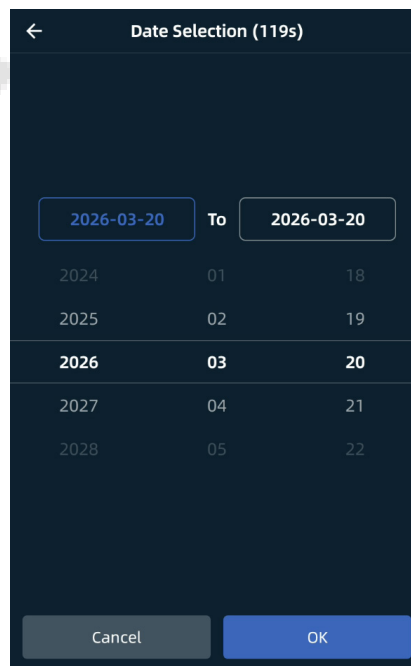
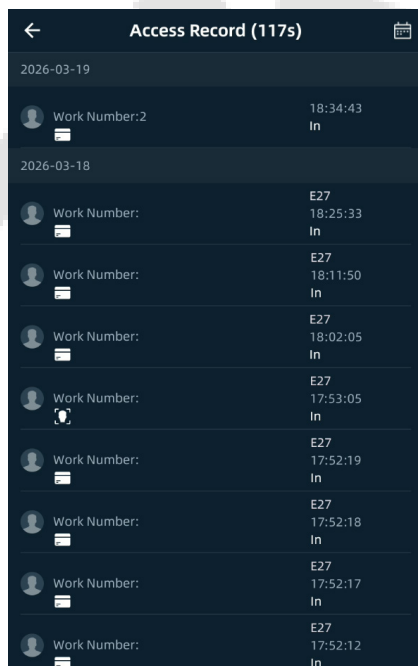
5 Record Query

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 **Record Query** on the **Main Menu** interface to search for the required event log.



On the **Record Query** interface, tap **Access Record**, all access records will be displayed. Click the  icon in the upper right corner to set the query time period.



On the **Record Query** interface, tap **Face Template Extraction Log**, all face template extraction logs will be displayed. Click  to view the user information associated with the face template extraction log.

←

Face Template Extraction Log

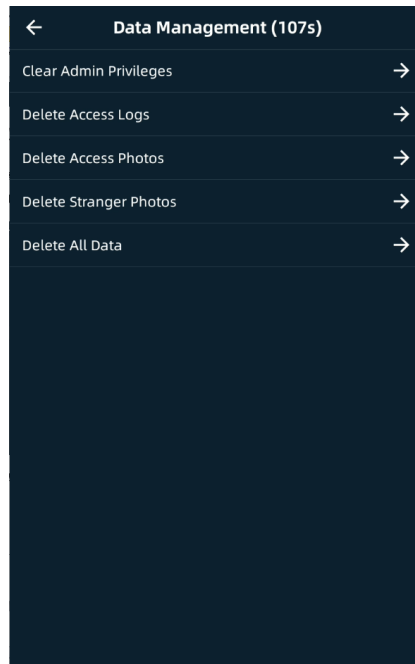
▼

📅

2026-03-18		
ID:1	14:24:11	✓
2026-03-17		
ID:217172...	15:45:13	✓
ID:2	14:57:44	✓
ID:2	14:57:23	✓
2026-03-06		
ID:1	17:20:01	✓
Total:5		

6 Data Management

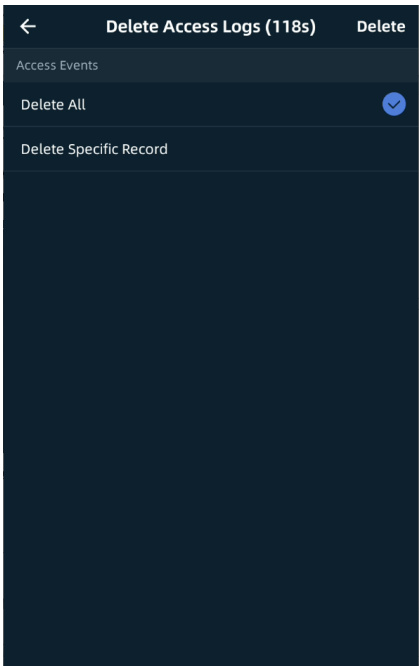
On the **Main Menu**, tap **Data Management** to delete the relevant data in the device.



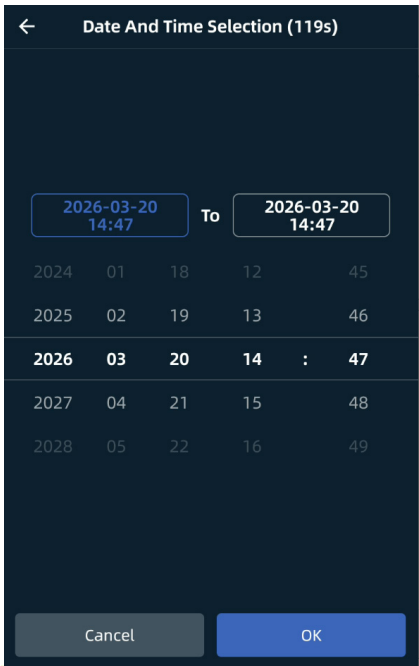
Function Description

Function Name	Description
Clear Admin Privileges	To remove all administrator privileges.
Delete Access Logs	To delete access records conditionally.
Delete Access Photos	To delete access photos of designated personnel.
Delete Stranger Photos	To delete the photos taken during failed verifications.
Delete All Data	To delete information and access records of all registered users.

The user may select Delete All or Delete Specific Record when deleting the access logs, access photos or stranger photos. Selecting Delete Specific Record, you need to set a specific time range to delete all data within a specific period.



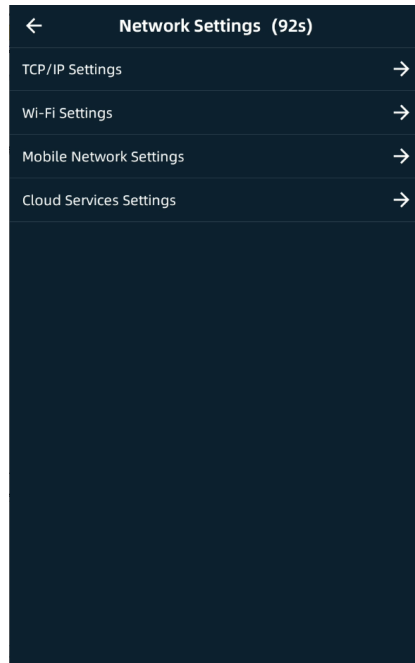
Select **Delete Specific Record**.



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

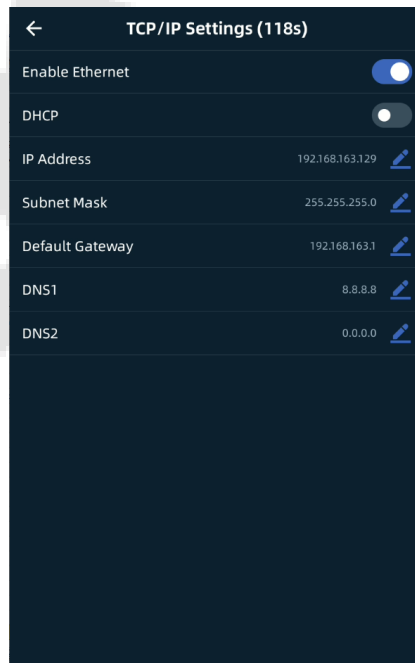
7 Network Settings

Tap **Network Settings** on the **Main Menu** to set the relevant parameters of TCP/IP, Wi-Fi, Mobile Network★and Cloud Service.



7.1 TCP/IP Settings

Tap **TCP/IP Settings** on the **Network Settings** interface to configure the settings.



Function Description

Function Name	Descriptions
Enable Ethernet	Once enabled, it can communicate using Ethernet and modify the Ethernet network address parameters.
DHCP	Dynamic Host Configuration Protocol is to dynamically allocate IP address for clients via server.
IP Address	The default IP address is 192.168.1.201. It can be modified according to the network availability.
Subnet Mask	The default Subnet Mask is 255.255.255.0. It can be modified according to the network availability.
Default Gateway	The default Gateway address is 0.0.0.0. It can be modified according to the network availability.
DNS1	The default DNS address is 0.0.0.0. It can be modified according to the network availability.
DNS2	It can be manually entered as needed.

7.2 Wi-Fi Settings

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

The Wi-Fi module enables data transmission via Wi-Fi (Wireless Fidelity) and establishes a wireless network environment.

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



- 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 **OK**.

7.3 Mobile Network★

When the device is applied to a dial-up network, make sure that the device is within the signal coverage of the mobile operator (GPRS/4G).

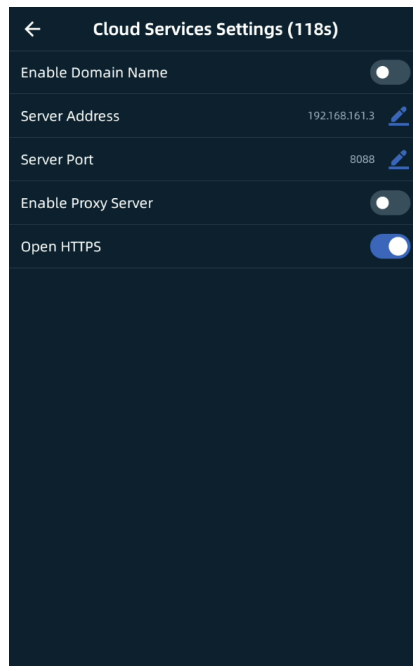
Please insert the SIM card into the SIM card slot before enabling. Then tap **Mobile Network** on the **Network Settings** interface to enable the mobile network.

Once turned on, the device is automatically connected.



7.4 Cloud Services Settings

Tap **Cloud Services Settings** on the **Network Settings** interface to connect with the ADMS server.



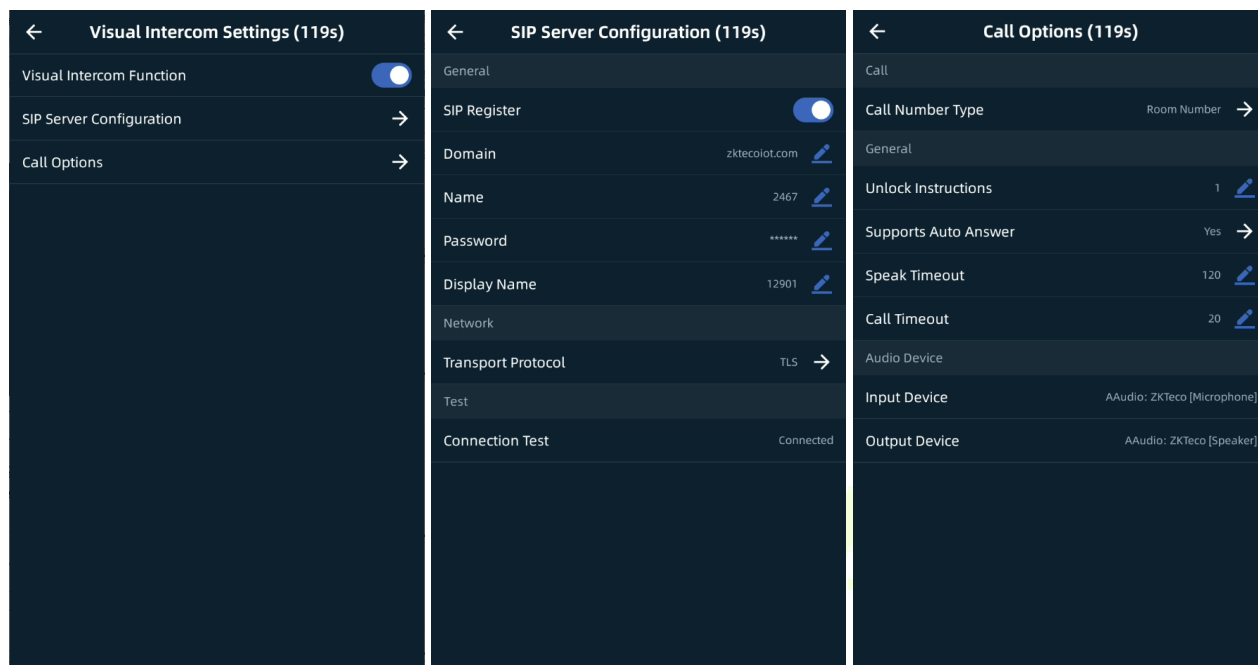
Function Description

Function Name		Description
Enable Domain Name	Server Address	Once this function is enabled, the domain name mode "http://..." will be used, such as http://www.XYZ.com, while "XYZ" denotes the domain name (when this mode is turned ON).
Disable Domain Name	Server Address	IP address of the ADMS server.
	Server Port	Port used by the ADMS server.
Enable Proxy Server		When you choose to enable the proxy, you need to set the IP address and port number of the proxy server.
Open HTTPS		If it is enabled, it needs to restart to take effect, and the data is uploaded to the push terminal. The address is changed from HTTP to HTTPS.

8 Intercom Settings

On the **Main Menu**, tap **Intercom Settings** to set relevant parameters of intercom.

The device achieves video intercom there are two modes, respectively, the LAN and SIP server. For more details, please refer to [15 SIP Video Intercom](#).

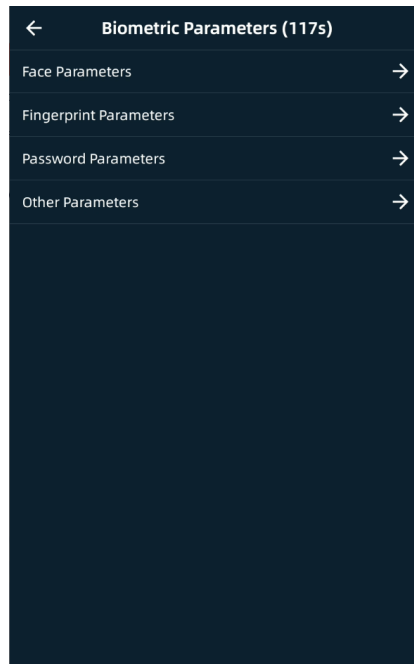


Function Description

Function Name	Description
Visual Intercom Function	Choose whether to enable the visual intercom function.
SIP Server Configuration	SIP Register: Select whether to enable the SIP server. When it is enable, the SIP account needs to be set. Note: 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. Transport Protocol: Set the transport protocol between the device and indoor monitor. Connection Test: Display the connection status of the SIP server.
Call Options	Call Number Type: The number type for device calls can be set to either Room Number or SIP Number. Unlock Instructions: The value should be set as same as the value of DTMF in the indoor monitor. Supports Auto Answer: Select whether to enable the auto answer function. When it is enabled, the device will automatically answer if the indoor monitor calls. Speak Timeout: Set the time of intercom, valid value 60 to 300 seconds. Call Timeout: Set the time of call, valid value 10 to 300 seconds. Input/Output Device: Display the audio input/output devices of the device.

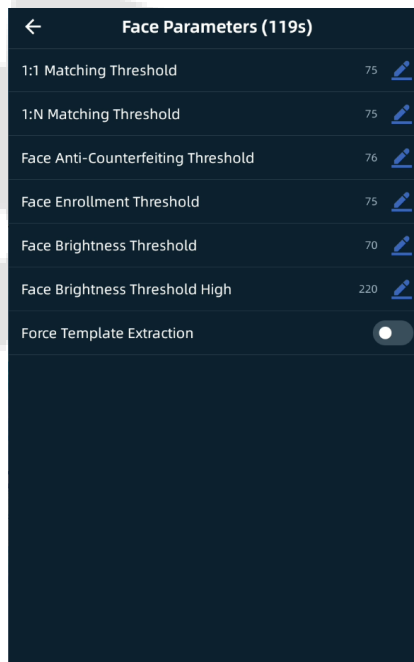
9 Biometric Parameters

On the **Main Menu**, tap **Biometric Parameters** to set the parameters of face, fingerprint★, password and other.



9.1 Face Parameters

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



Function Description

Function Name	Description
1:1 Matching Threshold	Under 1:1 verification mode, the verification will only be successful when the similarity between the acquired facial image and the user's facial templates enrolled in the device is greater than the set value. The valid value ranges from 0 to 100. The higher the thresholds, the lower the misjudgement rate, the higher the rejection rate, and vice versa. It is recommended to set the default value of 75.
1:N Matching Threshold	Under 1:N verification mode, the verification will only be successful when the similarity between the acquired facial image and all registered facial templates is greater than the set value. The valid value ranges from 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.
Face Anti-Counterfeiting Threshold	Facilitates to judge whether the captured visible image is really a person (a live human being). The larger the value, the better the anti-spoofing performance using visible light.
Face Enrollment Threshold	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.
Face Brightness Threshold	The minimum brightness for facial recognition by facial algorithm.
Face Brightness Threshold High	The highest brightness for facial recognition by facial algorithm.
Force Template Extraction	After enabled, when a facial photo is uploaded, the facial template in the photo will be extracted using the minimum requirements. Note: Enabling this feature will affect the accuracy of facial recognition. Please do not enable it during normal use.
Notes	Improper adjustment of the exposure and quality parameters may severely affect the performance of the device. Please adjust the exposure parameter only under the guidance of the after-sales service personnel of our company.

9.2 Fingerprint Parameters★

Tap **Fingerprint Parameters** on the **Biometric Parameters** interface.



Function Description

Function Name	Descriptions
1:1 Matching Threshold	Under 1:1 verification method, the verification will only be successful when the similarity between the acquired fingerprint data and the fingerprint template associated with the entered user ID enrolled in the device is greater than the set value.
1:N Matching Threshold	Under 1:N verification method, the verification will only be successful when the similarity between the acquired fingerprint data and the fingerprint templates enrolled in the device is greater than the set value.
1:1 Repetition Times	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.

9.3 Password Parameters

Tap **Password Parameters** on the **Biometric Parameters** interface.

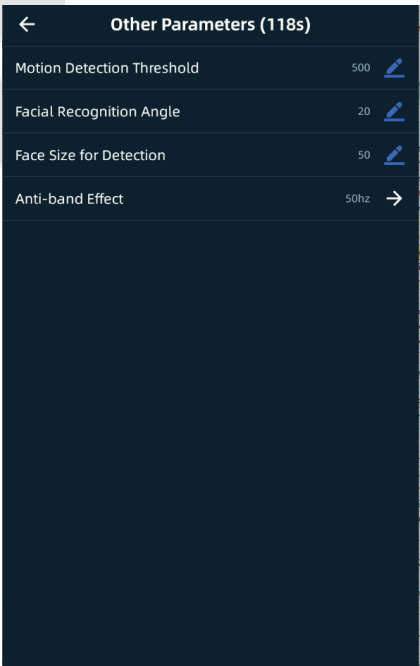


Function Description

Function Name	Descriptions
1:1 Repetition Times	When conducting 1:1 password verification, the number of repeatable comparisons can be set to a value between 1 and 9.

9.4 Other Parameters

Tap **Other Parameters** on the **Biometric Parameters** interface.

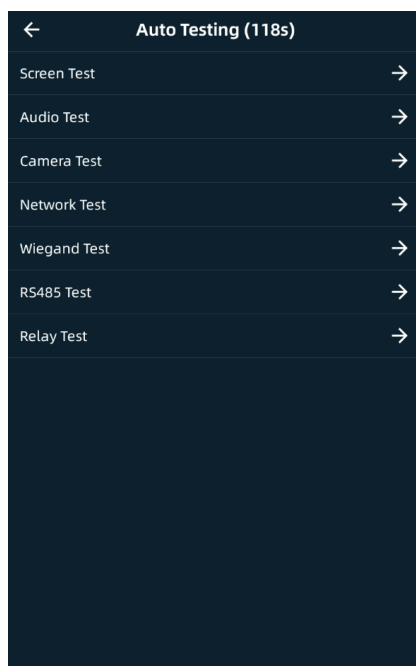


Function Description

Function Name	Descriptions
Motion Detection Threshold	It is used for detecting whether there is a moving person in front of the device to determine whether the face recognition function is enabled. The default value is 500.
Facial Recognition Angle	To limit the face angle at face recognition, the recommended threshold is 20.
Face Size for Detection	The size of the face when face recognition. The range is 50-512. The smaller the value, the farther the detectable distance is otherwise, the closer it is.
Anti-band Effect	When the banding effect is particularly pronounced, the image may appear particularly rough or unnatural, and issues such as gradation may appear in the camera's footage. You can try adjusting the frequency of this parameter to resolve such issues.

10 Auto Testing

On the **Main Menu**, tap **Auto-Testing** to automatically test whether all modules in the device are functioning properly. The test includes the screen, audio, camera, network, Wiegand, RS485 and relay.



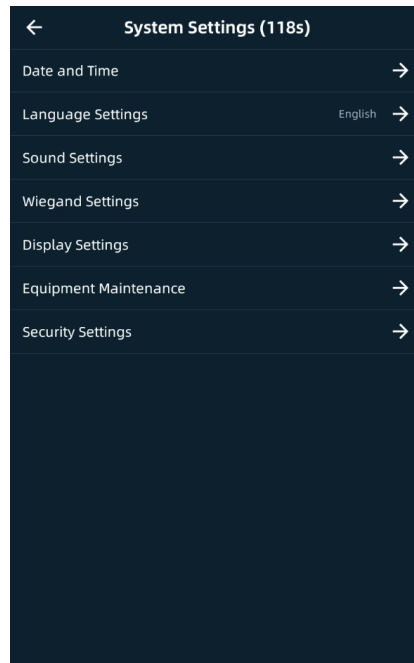
Function Description

Function Name	Description
Screen Test	It is used for testing the screen's display. The screen will display red, green, blue, white, and black tests. Check if the screen color is uniformly correct across each area of the screen. Tap on anywhere on the screen during testing to continue testing.
Audio Test	The device automatically tests audio prompts by playing back audio files that are stored in the device. Voice testing mainly test if the device's audio files are complete and if the audio effects are in good working order.
Camera Test	It is used for testing if the camera is functioning properly. Check captured image to see if the image quality is clear and usable.
Network Test	Test whether the network can connect normally.
Wiegand Test	Test whether the Wiegand can connect normally.
RS485 Test	Test whether the RS485 can connect normally.
Relay Test	Test whether the relay can connect normally.

11 System Settings

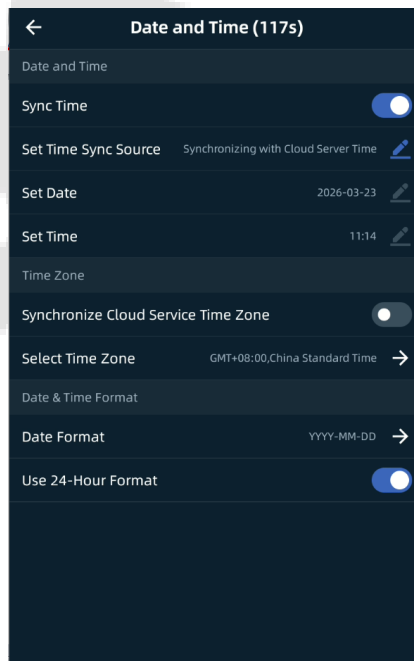
Set related system parameters to optimize the performance of the device.

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



11.1 Date and Time

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

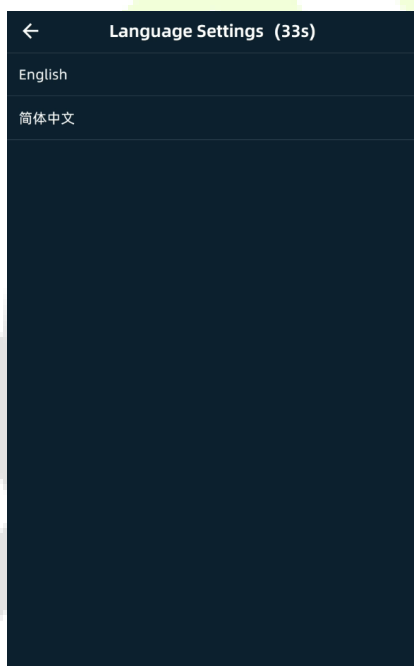


Function Description

Function Name	Descriptions
Sync Time	Enabled by default, users can set the time sync source and choose to synchronize with cloud server time or Internet time. If disabled, users can manually modify the date and time.
Synchronize Cloud Service Time Zone	Enabled by default, synchronizes the time zone of the cloud server. If disabled, users can manually select the appropriate time zone.
Date Format	Select the date format.
Use 24-Hour Format	Select whether to use the 24-Hour format.

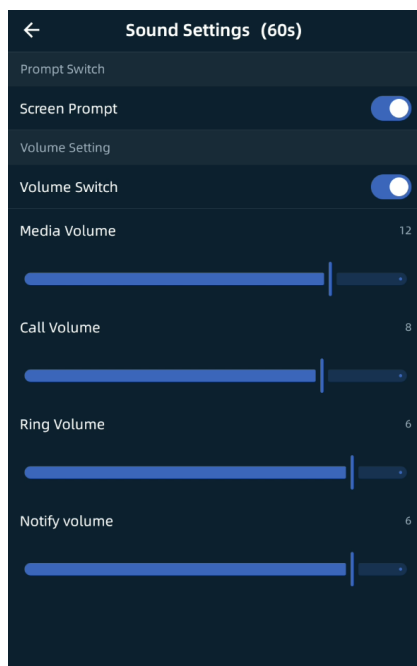
11.2 Language Settings

Tap **Language Settings** on the **System Settings** interface to choose between Simplified Chinese and English.



11.3 Sound Settings

Tap **Sound Settings** on the **System Settings** interface to configure the sound settings.



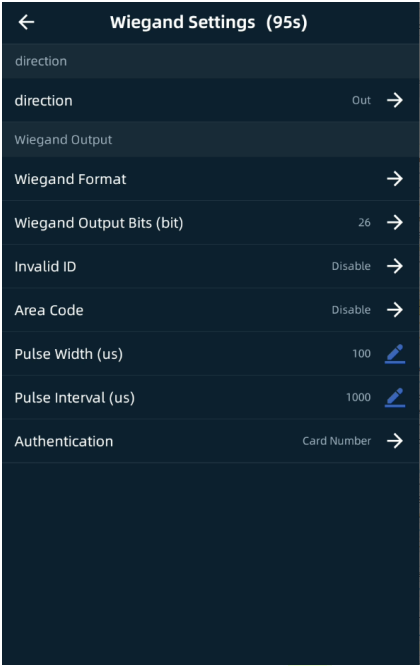
Function Description

Function Name	Description
Screen Prompt	Toggle to enable or disable the touchscreen prompt.
Volume Switch	When turned on, there will be voice prompts, and the volume of media, call, ring, and notify can be adjusted. When turned off, there will be no prompts.

11.4 Wiegand Settings

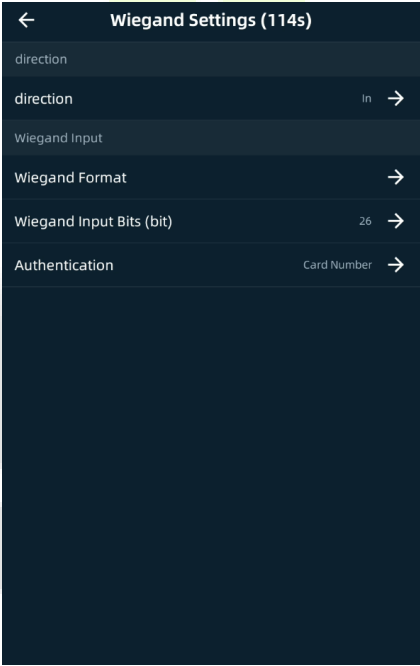
To set the Wiegand input and output parameters.

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



11.4.1 **Wiegand Input**

Select the direction as **In** on the **Wiegand Settings** interface.



Function Description

Function Name	Descriptions
Wiegand Format	Values range from 26 Bits, 34 Bits, 36 Bits, 37 Bits, 50 Bits and 66Bits.
Wiegand Input Bits (bit)	Number of bits of Wiegand data.
Authentication	Support Card number.

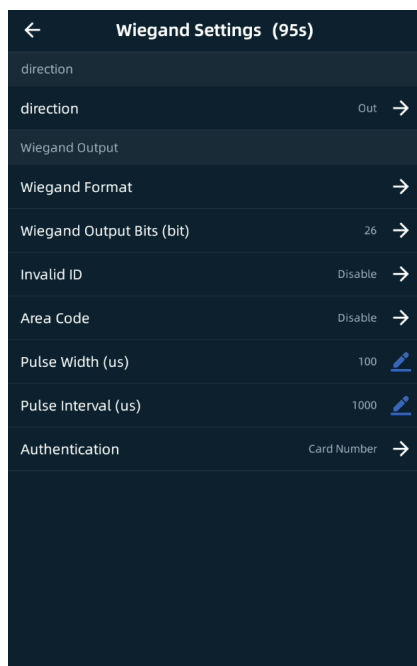
Various Common Wiegand Format Description

Wiegand Format	Description
Wiegand26	ECCCCCCCCCCCCCCCCCCCCCCCCCCO Consists of 26 bits of binary code. The 1 st bit is the even parity bit of the 2 nd to 13 th bits, while the 26 th bit is the odd parity bit of the 14 th to 25 th bits. The 2 nd to 25 th bits is the card numbers.
Wiegand26a	ESSSSSSSCCCCCCCCCCCCCCCCCCCCO Consists of 26 bits of binary code. The 1 st bit is the even parity bit of the 2 nd to 13 th bits, while the 26 th bit is the odd parity bit of the 14 th to 25 th bits. The 2 nd to 9 th bits is the site codes, while the 10 th to 25 th bits are the card numbers.
Wiegand34	ECCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO Consists of 34 bits of binary code. The 1 st bit is the even parity bit of the 2 nd to 17 th bits, while the 34 th bit is the odd parity bit of the 18 th to 33 rd bits. The 2 nd to 25 th bits is the card numbers.
Wiegand34a	ESSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCO Consists of 34 bits of binary code. The 1 st bit is the even parity bit of the 2 nd to 17 th bits, while the 34 th bit is the odd parity bit of the 18 th to 33 rd bits. The 2 nd to 9 th bits is the site codes, while the 10 th to 25 th bits are the card numbers.
Wiegand36	OFFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCMME Consists of 36 bits of binary code. The 1 st bit is the odd parity bit of the 2 nd to 18 th bits, while the 36 th bit is the even parity bit of the 19 th to 35 th bits. The 2 nd to 17 th bits is the device codes. The 18 th to 33 rd bits is the card numbers, and the 34 th to 35 th bits are the manufacturer codes.
Wiegand36a	EFFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCCO Consists of 36 bits of binary code. The 1 st bit is the even parity bit of the 2 nd to 18 th bits, while the 36 th bit is the odd parity bit of the 19 th to 35 th bits. The 2 nd to 19 th bits is the device codes, and the 20 th to 35 th bits are the card numbers.
Wiegand37	OMMMMSSSSSSSSSSSSSCCCCCCCCCCCCCCCCCE Consists of 37 bits of binary code. The 1 st bit is the odd parity bit of the 2 nd to 18 th bits, while the 37 th bit is the even parity bit of the 19 th to 36 th bits. The 2 nd to 4 th bits is the manufacturer codes. The 5 th to 16 th bits is the site codes, and the 21 st to 36 th bits are the card numbers.
Wiegand37a	EMMMFFFFFFFFFFFFSSSSSSSCCCCCCCCCCCCCCCCO Consists of 37 bits of binary code. The 1 st bit is the even parity bit of the 2 nd to 18 th bits, while the 37 th bit is the odd parity bit of the 19 th to 36 th bits. The 2 nd to 4 th bits is the manufacturer codes. The 5 th to 14 th bits is the device codes, and 15 th to 20 th bits are the site codes, and the 21 st to 36 th bits are the card numbers.
Wiegand50	ESSSSSSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCCCCCO Consists of 50 bits of binary code. The 1 st bit is the even parity bit of the 2 nd to 25 th bits, while the 50 th bit is the odd parity bit of the 26 th to 49 th bits. The 2 nd to 17 th bits is the site codes, and the 18 th to 49 th 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.

11.4.2 Wiegand Output

Select the direction as **Out** on the **Wiegand Settings** interface.

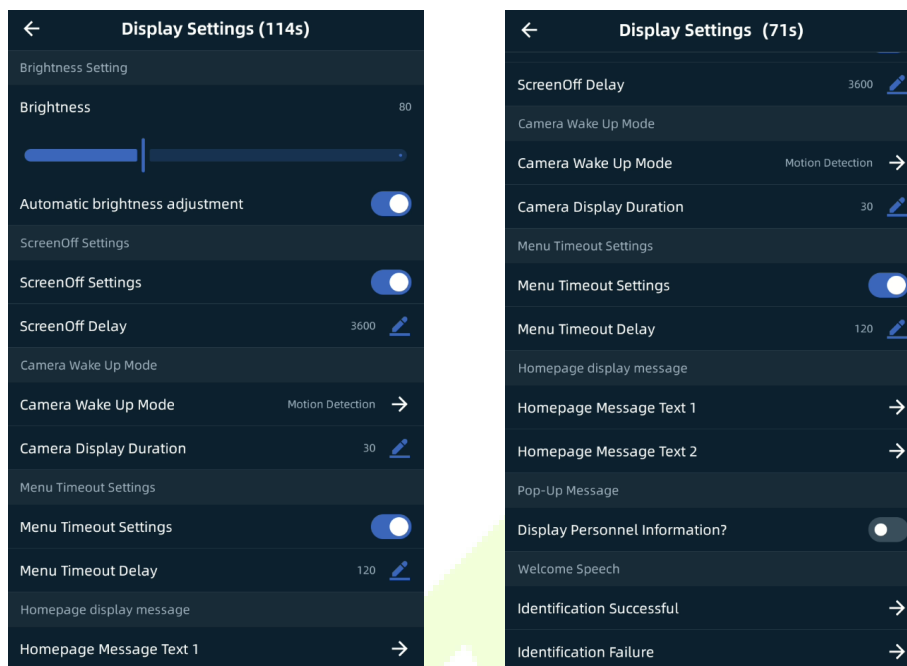


Function Description

Function Name	Descriptions
Wiegand Format	Values range from 26 bits, 34 bits, 36 bits, 37 bits, 50 bits and 66 bits.
Wiegand Output Bits (bit)	After selecting the required Wiegand format, select the corresponding output bit digits of the Wiegand format.
Invalid ID	If the verification is failed, the system will send the failed ID to the device and replace the card number or personnel ID with the new one.
Area Code	It is similar to the device ID. The difference is that a site code can be set manually, an\ is repeatable in a different device. The valid value ranges from 0 to 256 by default.
Pulse Width (us)	The time width represents the changes of the quantity of electric charge with regular high-frequency capacitance within a specified time.
Pulse Interval (us)	The time interval between pulses.
Authentication	Support Card number.

11.5 Display Settings

Tap **Display Settings** on the **System Settings** interface to customize the display style of the main interface.



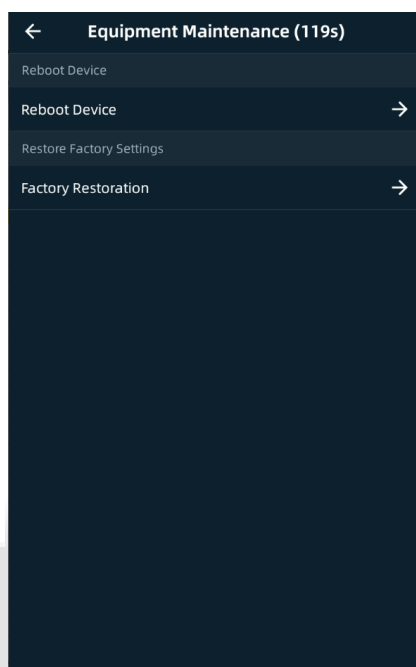
Function Description

Function Name	Description
Brightness	Used to set the brightness of the device screen, with valid values ranging from 1 to 255. The higher the value, the brighter the interface.
Automatic brightness adjustment	After enabled, the device will automatically adjust the screen brightness according to the ambient light.
ScreenOff Settings	Choose whether to enable the screen-off function. When the device enters standby mode and remains idle for the set automatic screen-off time, it will enter a screen-off state. The device can be woken up by detecting the face or tapping any position on the screen. Valid values are: 30~3600s.
Camera Wake Up Mode	When Motion Detection is selected, the camera will automatically detect and perform facial recognition. When Touch Screen is selected, the device will disable the automatic recognition sensing function of the camera. Only by clicking the icon  on the screen can the automatic recognition function of the device's camera be activated.
Camera Display Duration	Set the display duration of the camera view. Valid values are: 30~3600s.

Menu Timeout Settings	Choose whether to enable the menu timeout function. The Menu Timeout Delay refers to the time it takes to exit to the standby interface after entering the menu without any operation. Valid values are: 60~600s.
Homepage Message Text 1/2	The message displayed on the main interface can be customized.
Display Personnel Information?	After enabled, the user's name and ID information will be displayed following the personnel verification result.
Welcome Speech	Customize the prompts for successful and failed user authentication.

11.6 Equipment Maintenance

Tap **Equipment Maintenance** on the **System Settings** interface.

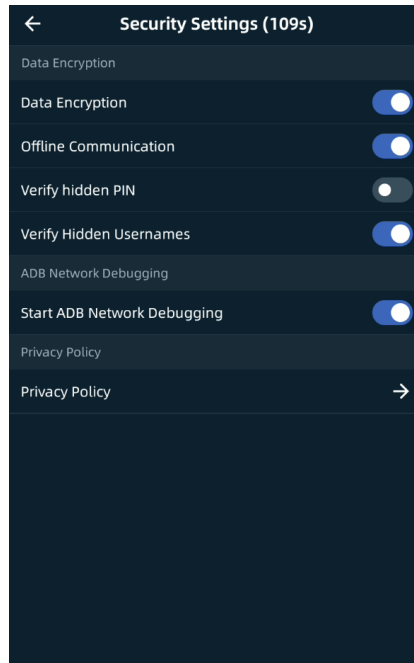


Function Description

Function Name	Descriptions
Reboot Device	Click "OK" in the pop-up dialog box to restart the device.
Factory Restoration	Restore the device's communication settings, system settings, etc. to their factory default settings. You can also check whether to Synchronize and clear all data.

11.7 Security Settings

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

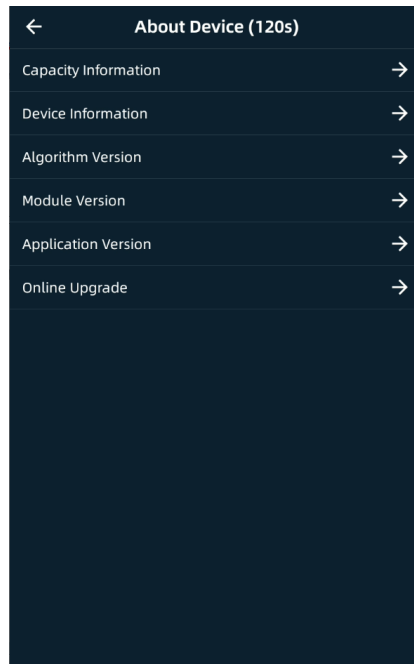


Function Description

Function Name	Description
Data Encryption	Choose whether to encrypt data.
Offline Communication	After enabled, the device is allowed to use the parameter tool.
Verify hidden PIN	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).
Verify Hidden Usernames	After enabled, the verification result will not display the name. After disabled, the user's name will be displayed after the personnel verification result.
Start ADB Network Debugging	Select whether to enable ADB network debugging. Once enabled, Android devices can be connected to the development computer via a local area network for remote debugging.
Privacy Policy	Display the device's privacy policy.

12 About Device

Tap **About Device** on the **Main Menu** interface to view data capacity, device and firmware information and online upgrade.



Function Description

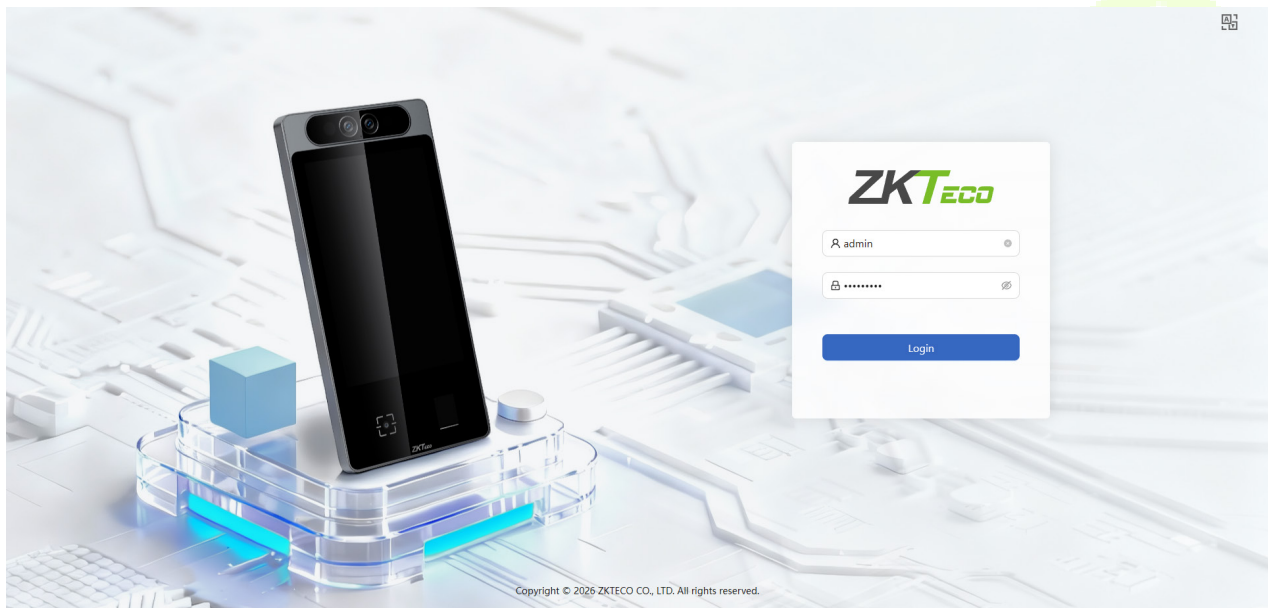
Function Name	Function Description
Capacity Information	It displays the current device's capacity of user, facial template, fingerprint★, card, access control records, access control photos, stranger photos, and user photos.
Device Information	It displays the device's name, device type, serial number, MAC address, platform version, platform information, and manufacturer.
Algorithm Version	It displays the device's face algorithm and fingerprint★ algorithm version.
Module Version	It displays the device's extension and fingerprint★ module, push version.
Application Version	It displays all the versions of all the system's app.
Online Upgrade	Clicking on "Check for Upgrade" will search for the latest firmware for the device.

13 WebServer

Users can remotely view device-related information, manage users, set parameters, and perform other operations through the WebServer.

13.1 Login WebServer

1. Open a browser to enter the address to log in to the WebServer, the address is **https://Serial IP Address:8443**. For example: **https://192.168.1.201:8443**.
2. Enter the WebServer account and password, the default account is: **admin**, password: **123456**.

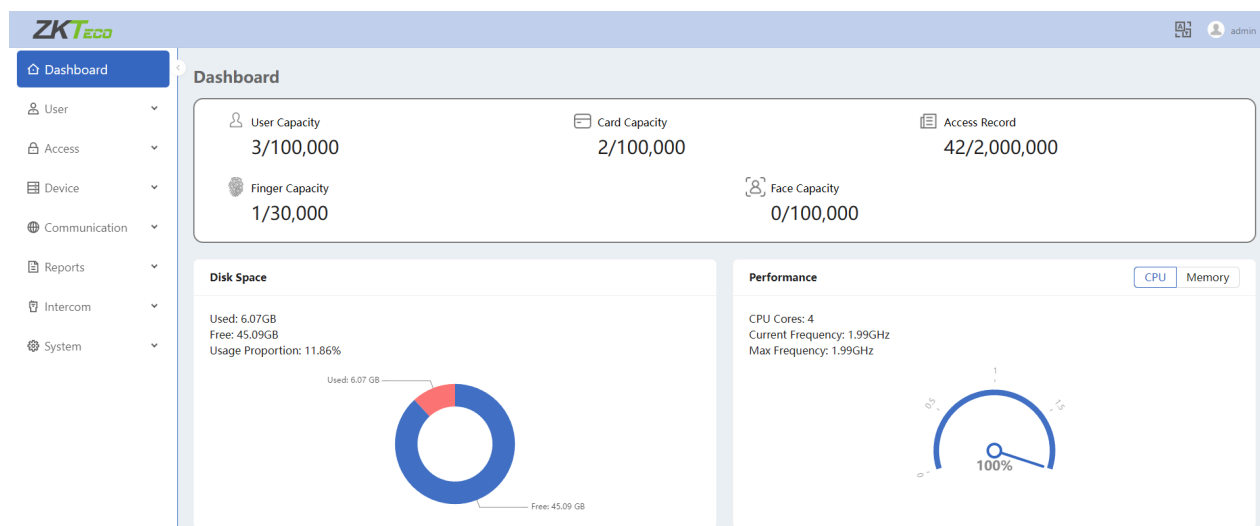


Note:

1. After logging in for the first time, it is required that the users change their original password.
2. If you forget the WebServer login password, you can reset the device to factory settings, and the password will be restored to the initial password (123456).

13.2 Dashboard

Click **Dashboard** on the WebServer. In this interface, you can view the device's capacity information, disk space, and performance status.



13.3 User

● Add Users

Click **User > +Add** to enter the user registration interface.

The 'Add' modal contains the following fields:

- Id:** Please enter
- Name:** Please enter
- Card No:** Please enter
- Password:** Please enter
- Access group:** 0
- Time Zones:** 1 x
- Admin:** ☐

Buttons: Cancel, OK

In this interface, you can register the User ID, Name, Card Number, Password, access group, time zones, and rights of the new user, click **OK** to save.

After registering the basic information, you can click on **Face** to upload the user's facial photo.

The 'Face' modal contains the following text:

- Click to upload

Buttons: Cancel, OK

Below the modal, a red warning message states: "The image size should not exceed 2MB. Supported formats: png, jpg, jpeg"

● Search for Users

Input relevant user information, and then click **Query**. The system will search for the relevant users and display them.

The screenshot shows the ZKTeco User Management interface. On the left is a sidebar with navigation links: Dashboard, User, Access, Device, Communication, and Reports. The main area is titled 'User / User'. It contains search filters: 'Id' (set to 1), 'Name' (Please enter), and 'Admin' (Please select). There are 'Reset' and 'Query' buttons. Below the filters is a '+ Add' button and a table of users.

Id	Name	Card No	Admin	Biological Template	Actions
1		2617732657	No		Face Edit Delete

1-1 of 1 items < 1 >

● Edit Users

Select the user you want to modify and click the **Edit** button behind it to enter the user editing interface.

The screenshot shows the ZKTeco User Management interface. The search filters are empty. The table below shows three users. The 'Edit' button for the first user (ID 1) is highlighted with a red box.

Id	Name	Card No	Admin	Biological Template	Actions
1		2617732657	No		Face Edit Delete
2		3808991060	No		Face Edit Delete
3			No		Face Edit Delete

1-3 of 3 items < 1 >

Note: Except for the User ID, which cannot be modified, other operations are similar to adding a new user, and will not be further elaborated here.

● Delete Users

Select the user you want to delete and click the **Delete** button next to it to proceed with the deletion.

The screenshot shows the ZKTeco User Management interface. The search filters are empty. The table below shows three users. The 'Delete' button for the third user (ID 3) is highlighted with a red box.

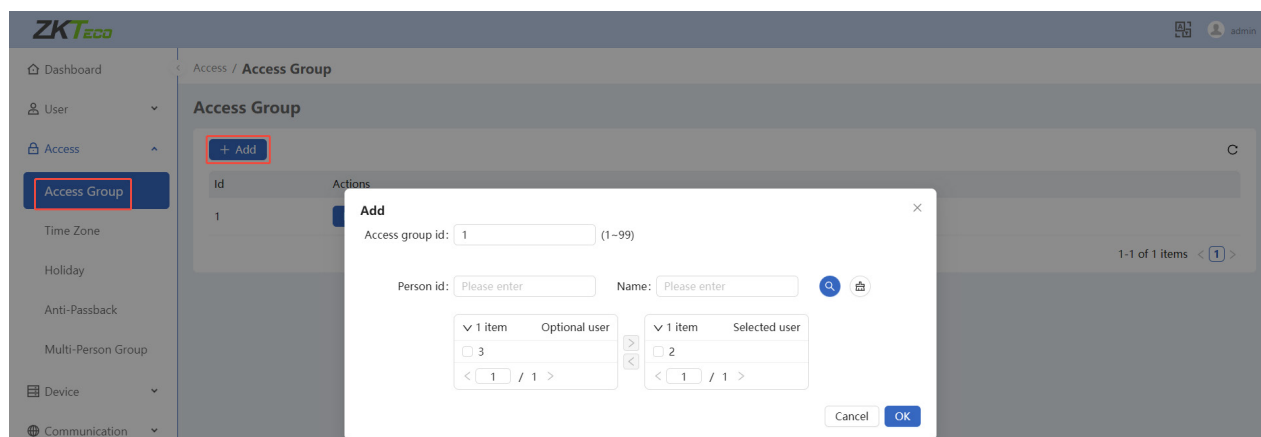
Id	Name	Card No	Admin	Biological Template	Actions
1		2617732657	No		Face Edit Delete
2		3808991060	No		Face Edit Delete
3			No		Face Edit Delete

1-3 of 3 items < 1 >

13.4 Access

13.4.1 Access Group

Click **Access > Access Group > +Add** to assign users to access groups. The device supports up to 99 access groups.

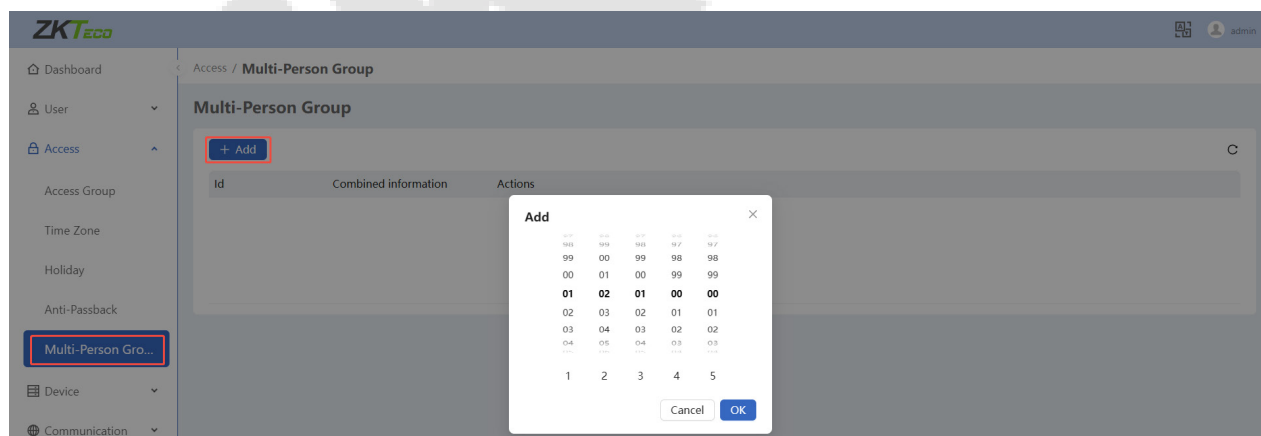


13.4.2 Multi-Person Group

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

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

Click **Multi-Person Group > +Add**, slide to set the group number, and then click **OK**.



For Example:

- If the **Door-unlock combination 1** is set as **(01 03 05 06 08)**. It indicates that the unlock combination 1 consists of 5 people and all the 5 individuals are from 5 groups, namely, AC Group 1, AC Group 3, AC Group 5, AC Group 6, and AC Group 8, respectively.
- If the **Door-unlock combination 2** is set as **(02 02 04 04 07)**. It indicates that the unlock combination 2 consists of 5 people; the first two are from AC Group 2, the next two are from AC

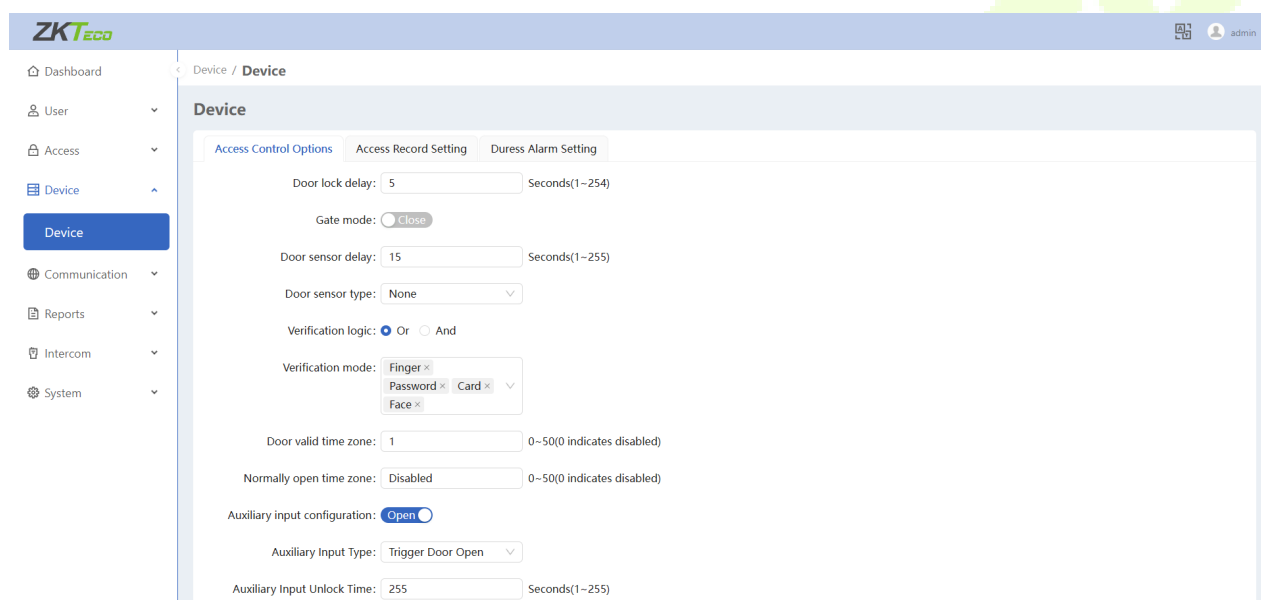
Group 4, and the last person is from AC Group 7.

- If the **Door-unlock combination 3** is set as **(09 09 09 09 09)**. It indicates that there are 5 people in this combination; all of which are from AC Group 9.
- If the **Door-unlock combination 4** is set as **(03 05 08 00 00)**. It indicates that the unlock combination 4 consists of only three people. The first person is from AC Group 3, the second person is from AC Group 5, and the third person is from AC Group 8.

Note: For settings related to time zone, holiday, and anti-passback operations, please refer to sections [4.3](#), [4.4](#), and [4.5](#).

13.5 Device

Click **Device**. For information on access control options, access record setting, and duress alarm setting, please refer to sections [4.1](#), [4.2](#), and [4.6](#).



ZKTeco admin

Dashboard / Device / Device

Device

Access Control Options | Access Record Setting | Duress Alarm Setting

Door lock delay: 5 Seconds(1~254)

Gate mode: ☒ Close

Door sensor delay: 15 Seconds(1~255)

Door sensor type: None

Verification logic: ☒ Or ☐ And

Verification mode: ☒ Finger ☐ Password ☐ Card ☐ Face

Door valid time zone: 1 0~50(0 indicates disabled)

Normally open time zone: Disabled 0~50(0 indicates disabled)

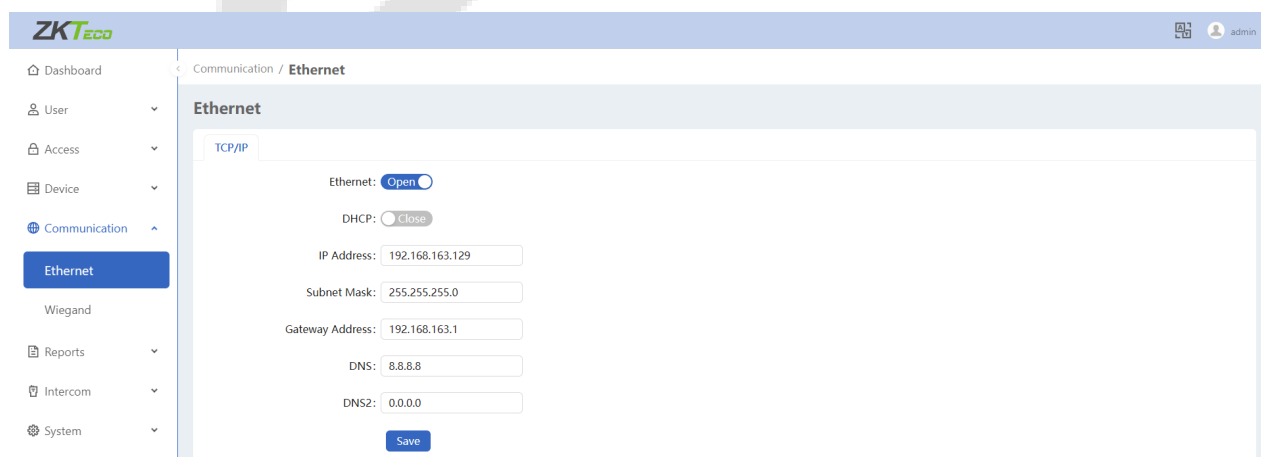
Auxiliary input configuration: ☒ Open

Auxiliary Input Type: Trigger Door Open

Auxiliary Input Unlock Time: 255 Seconds(1~255)

13.6 Communication

For settings related to Ethernet and Wiegand, please refer to Sections [7.1](#) and [11.4](#).



ZKTeco admin

Dashboard / Communication / Ethernet

Ethernet

TCP/IP

Ethernet: ☒ Open

DHCP: ☐ Close

IP Address: 192.168.163.129

Subnet Mask: 255.255.255.0

Gateway Address: 192.168.163.1

DNS: 8.8.8.8

DNS2: 0.0.0.0

Save

Note: After successfully changing the IP address of the device, the device will disconnect from the WebServer. You will need to enter the changed IP address to log in again.

13.7 Reports

Click on **Access Record**, **Face Ext Record**, and **Call Record** in the **Reports** column to view the relevant records of the device.

Access Record

Time: Please select → Please select User ID: Please enter

Time	User ID	Name	Event Type	Verification Mode	In/Out Status
2026-03-19 18:34:43	2		Normal Verify Open	Card	In
2026-03-18 18:25:33	-		Unregistered Personnel	Card	In
2026-03-18 18:11:50	-		Unregistered Personnel	Card	In
2026-03-18 18:02:05	-		Unregistered Personnel	Card	In
2026-03-18 17:53:05	-		Unregistered Personnel	Face	In
2026-03-18 17:52:19	-		Unregistered Personnel	Card	In
2026-03-18 17:52:18	-		Unregistered Personnel	Card	In
2026-03-18 17:52:17	-		Unregistered Personnel	Card	In
2026-03-18 17:52:12	-		Unregistered Personnel	Card	In
2026-03-18 17:48:45	-		Unregistered Personnel	Face	In

1-10 of 24 items < 1 2 3 >

Face Ext Record

User ID: Please enter Result: Please select Time: Please select → Please select

User ID	Result	Time
1	🟢	2026-03-18 14:24:11
217172421	🟢	2026-03-17 15:45:13
2	🟢	2026-03-17 14:57:44
2	🟢	2026-03-17 14:57:23
1	🟢	2026-03-06 17:20:01

1-5 of 5 items < 1 >

Call Record

Type: Please select Name: Please enter Recipient number: Please enter

Serial	Type	Name	Recipient number	Time
1	Outgoing call	Indoor-Monitor	sip:2469	2026-03-18 10:56:56
2	Outgoing call	Stella	sip:192.168.163.128	2026-03-17 17:18:14
3	Outgoing call	Stella	sip:192.168.163.128	2026-03-17 17:18:04
4	Outgoing call	192.168.163.128	sip:192.168.163.128	2026-03-17 16:14:54
5	Outgoing call	192.168.163.128	sip:192.168.163.128	2026-03-06 16:11:53

1-5 of 5 items < 1 >

13.8 Intercom

13.8.1 Intercom Switch

Click **Intercom** > **Intercom Switch** to enter the intercom switch setting interface.

The screenshot shows the ZKTeco web interface for the Intercom Switch settings. The sidebar on the left contains a navigation menu with options: Dashboard, User, Access, Device, Communication, Reports, and Intercom. The Intercom section is expanded, showing the Intercom Switch settings. The settings include: Switch status (Open), Video resolution (VGA), and Video bit rate (1024 kbps). A Save button is at the bottom.

Function Description

Function Name	Description
Switch status	Choose whether to enable the intercom function.
Video resolution	Select the video resolution of the intercom. The default is VGA (640x480). You can choose from 720P (1280x720), VGA, and QVGA (320x240).
Video bit rate	Select the video bit rate of the intercom, the larger the value, the higher the picture and sound quality of the video, and the greater the network requirements. The default is 1024kbps, with options available at 128, 256, 512, 1024, 2048, and 4096kbps.

13.8.2 SIP Server

Click **SIP Server** to enter the SIP server setting interface.

The screenshot shows the ZKTeco web interface for the SIP Server settings. The sidebar on the left contains a navigation menu with options: Dashboard, User, Access, Device, Communication, Reports, and Intercom. The Intercom section is expanded, showing the SIP Server settings. The settings include: SIP Registration (Open), Domain (zktcoiot.com), Name (2467), Password (masked), Display name (12901), Transport protocol (TLS), and Connection status (Connection successful). A Save button is at the bottom.

Function Description

Function Name	Description
SIP Registration	Select whether to enable the SIP server. When it is enable, the SIP account needs to be set. Note: 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.
Transport protocol	Set the transport protocol between the device and indoor monitor.
Connection status	Display the connection status of the SIP server.

13.8.3 Call Options

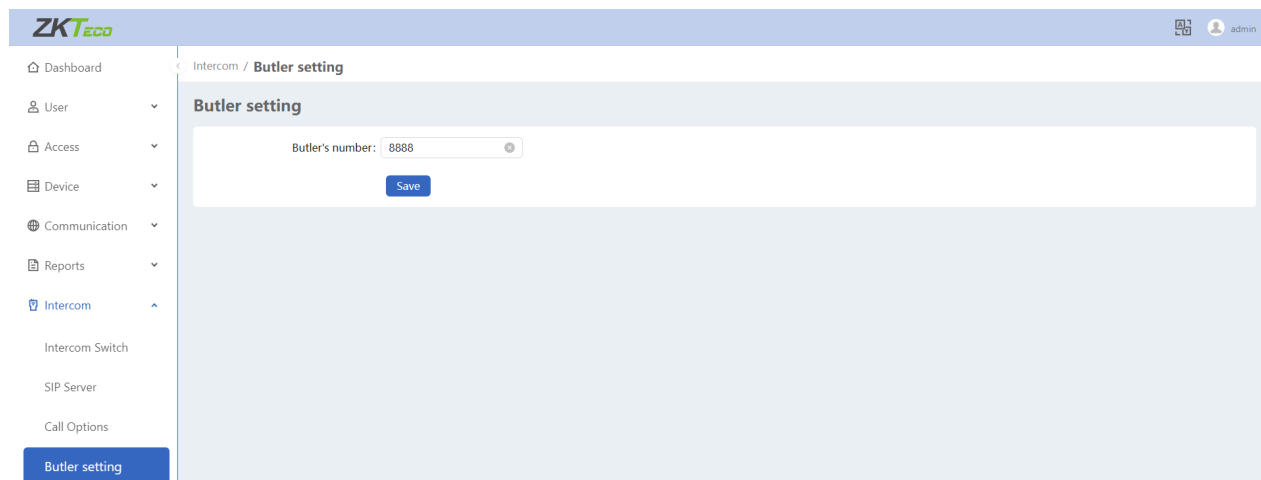
Click **Call Options** to enter the call options setting interface.

Function Description

Function Name	Description
Call number type	The number type for device calls can be set to either Group name or SIP Number.
Unlock Instruction	The value should be set as same as the value of DTMF in the indoor monitor.
Support automatic answering	Select whether to enable the auto answer function. When it is enabled, the device will automatically answer if the indoor monitor calls.
Conversation timeout duration	Set the time of intercom, valid value 60 to 300 seconds.
Call timeout duration	Set the time of call, valid value 10 to 300 seconds.

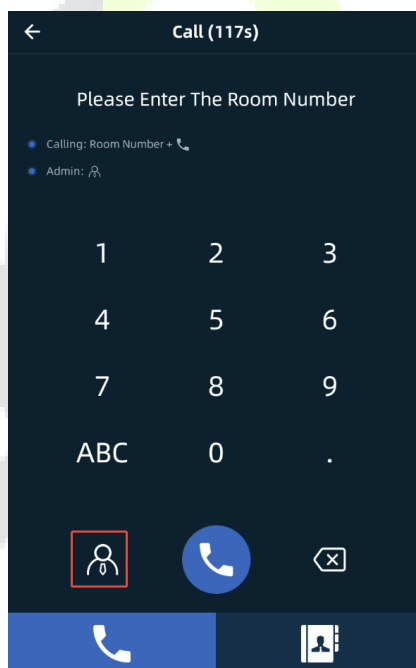
13.8.4 Butler Setting

Click **Butler Setting** to enter the butler setting interface.



Input the butler's number (this number must have been added to the contacts), and then click **Save**.

After the setting is complete, click the  icon on the device to enter the call page, and directly click the  icon to make a one-click call to the administrator.



13.8.5 Contacts

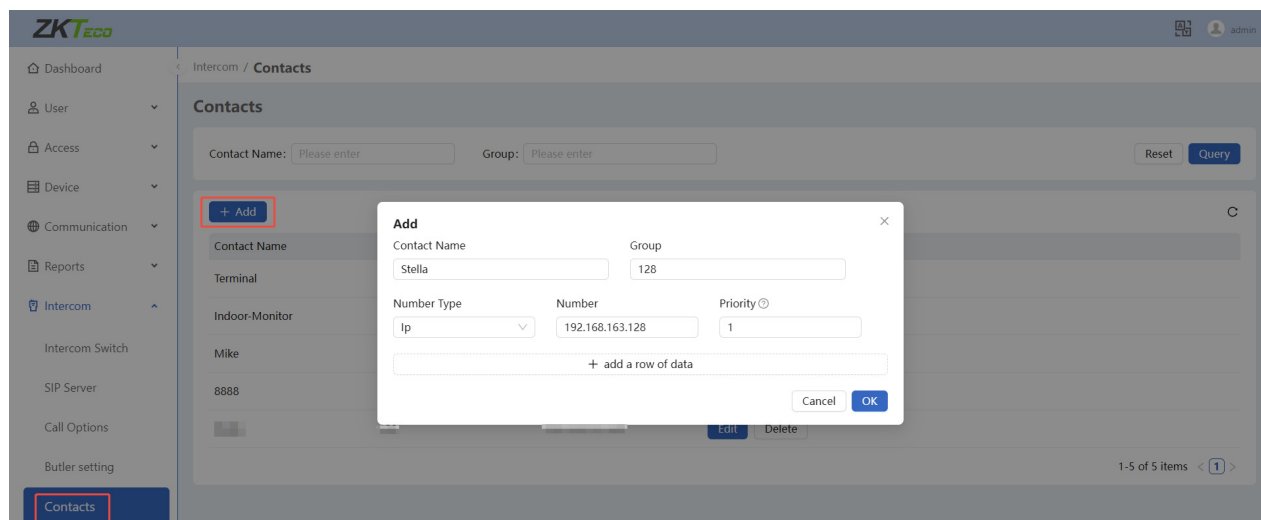
Click **Contacts** to enter the contacts setting interface.

● Add Contacts

Note: When assigning a SIP account to the device on ZKBio CVSecurity software, you can synchronize the contact list, eliminating the need to manually add it on the device.

Here, we will introduce the method of adding new contacts by taking the local area network (LAN) calling method as an example:

1. Click on **+Add** to enter the adding contacts interface, input relevant information, and then click **OK**.



Contact Name: Enter the name of the contact.

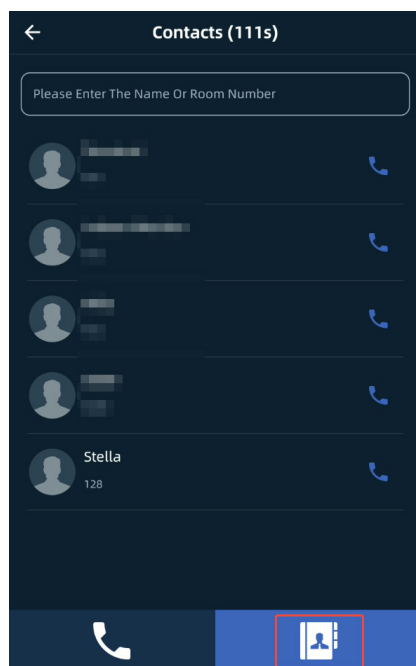
Group: Enter the group name.

Number Type: Select as Ip.

Number: Enter the IP address of the indoor monitor.

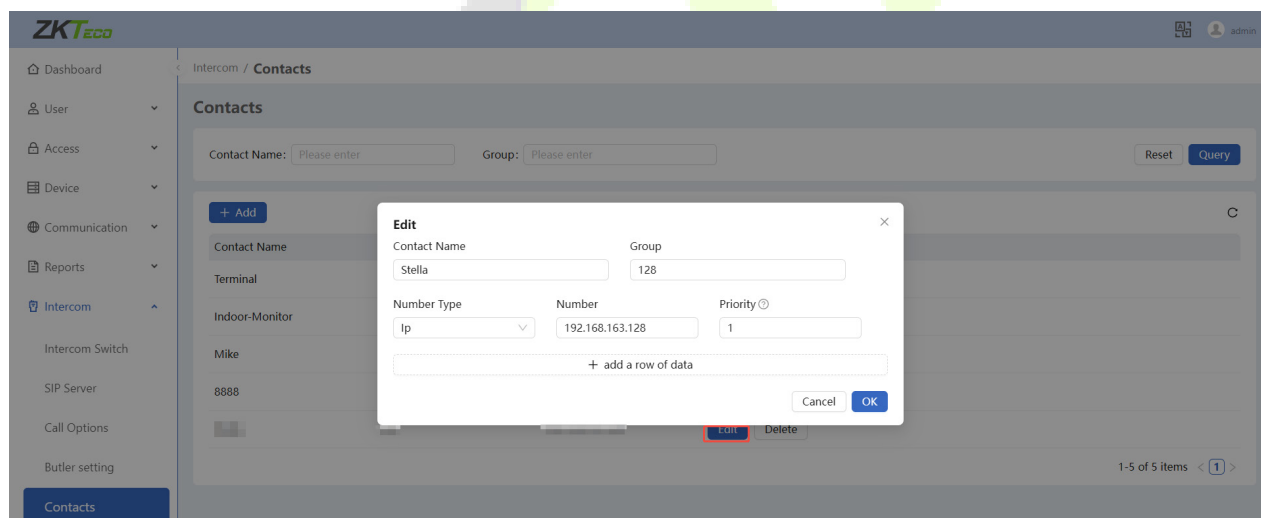
Priority: When multiple contact methods are configured for a contact, calls are made in order of priority. Value range: 0–99, default value is 1. Priority rule: The higher the number, the higher the priority. If priorities are the same, calls are initiated simultaneously. Special value 0 explanation: In a group call scenario, this number will not be called. However, when calling this contact individually, it can still be reached normally.

2. After adding, click the  icon on the device to enter the call page, click the  icon to open the contact list, and select the indoor monitor you want to call for quick calling.



● Edit Contacts

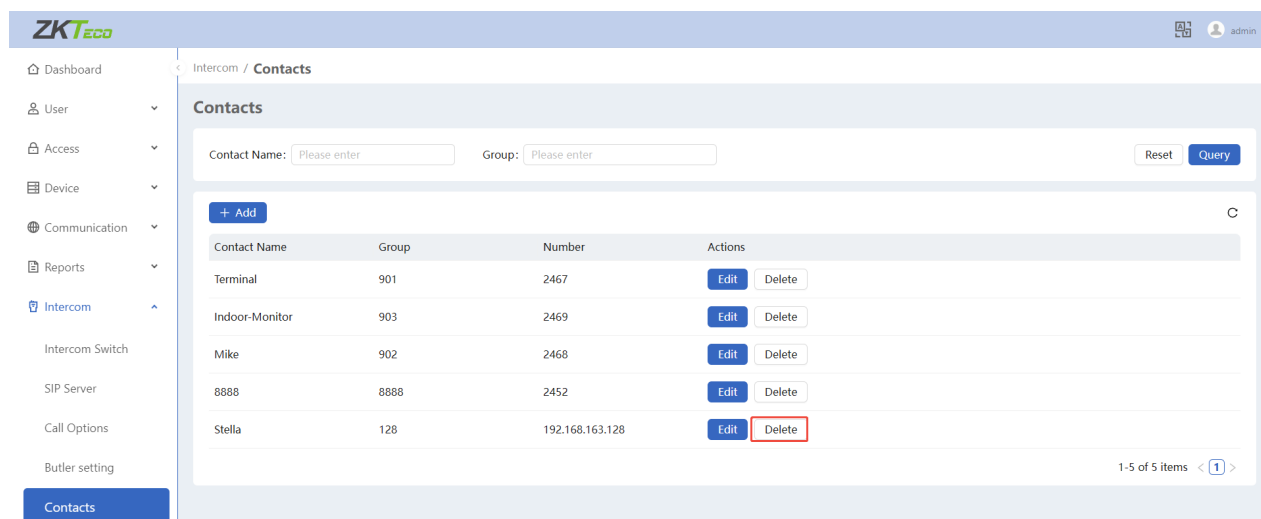
Select the contact you want to modify, and click on the **Edit** button behind it to enter the contact editing interface.



Note: The operation is similar to adding new contacts, so it will not be repeated here.

● Delete Contacts

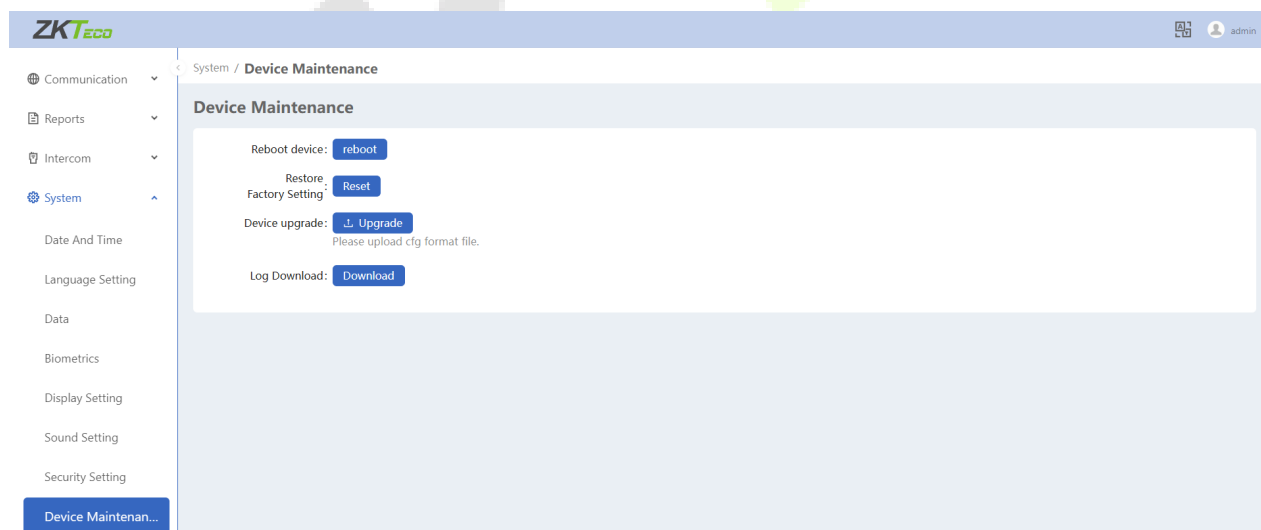
Select the contact you want to delete and click on the **Delete** button next to it to proceed with the deletion.



13.9 System

13.9.1 Device Maintenance

Click **System > Device Maintenance** to enter the device maintenance interface.



Function Description

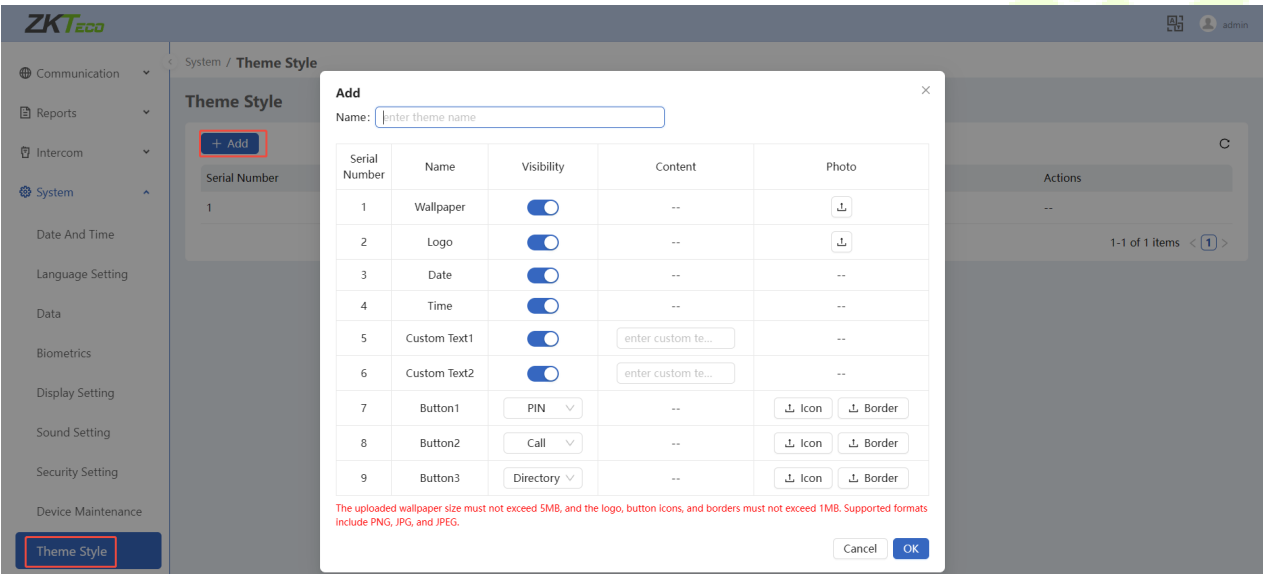
Function Name	Description
Reboot device	Click "OK" in the pop-up dialog box to restart the device.
Restore Factory Setting	Restore the device's communication settings, system settings, etc. to their factory default settings. You can also check whether to Synchronize and clear all data. You need to enter the current Web login password. Only when the

	passwords match can the factory reset operation be executed.
Device upgrade	Select the upgrade file to perform the firmware upgrade operation on the device. Note: If you need an upgrade file, please contact our technical support. Under normal circumstances, firmware upgrade is not recommended.
Log Download	Click Download allows you to download the device log for viewing.

13.9.2 Theme Style

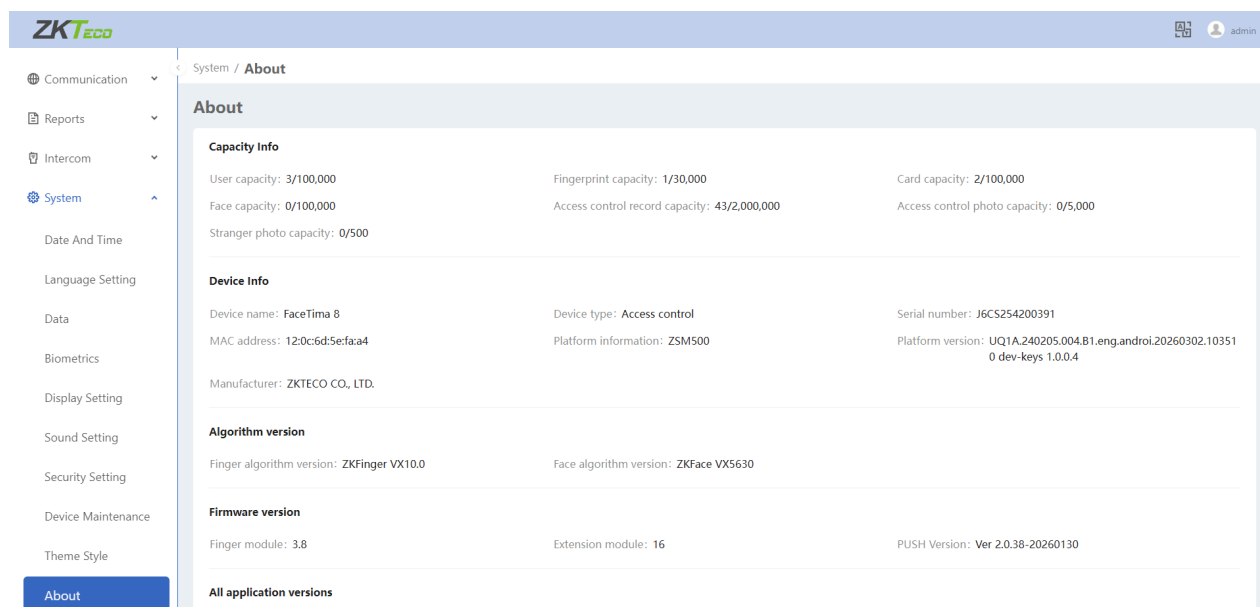
Click **Theme Style** to enter the theme style setting interface. Users can set the display style of the main interface according to their personal preferences.

Click on **+Add** to customize the theme style of the device by uploading wallpapers, logos, button icons, etc.



13.9.3 About

Click **About** allows you to view relevant information such as the device's capacity, algorithm, version, and more.



Other system settings and operation methods are similar to those of the device, and will not be elaborated here. Please refer to Chapters [6](#), [9](#), and [11](#) for details.

14 Connect to ZKBio CVSecurity Software

14.1 Set the Communication Address

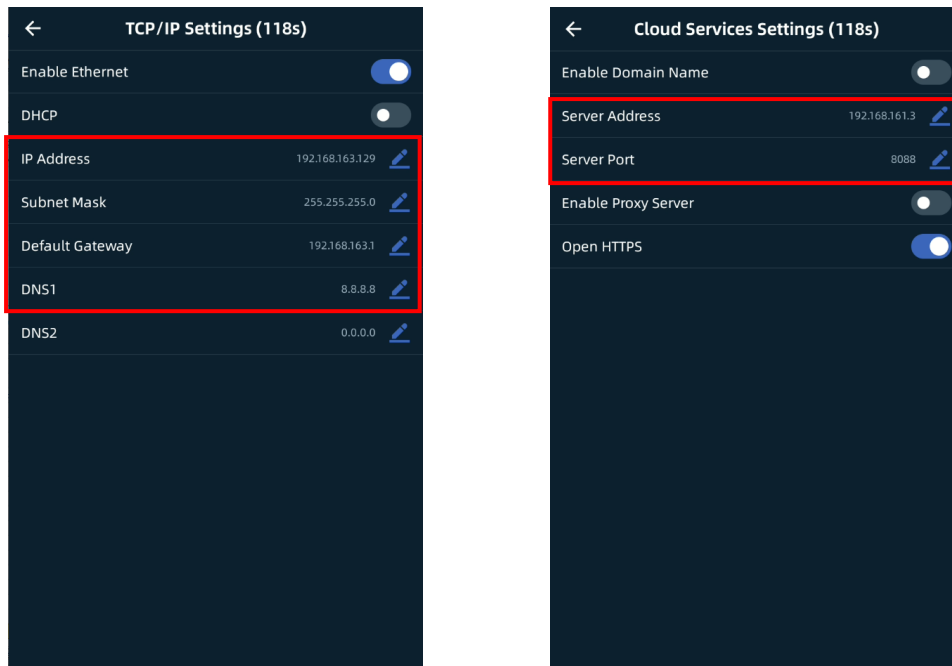
1. In the main menu, tap **Network Settings** > **TCP/IP Settings** to configure the device's IP address and gateway.

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

2. In the main menu, click **Network Settings** > **Cloud Services Settings** to set the server address and server port.

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

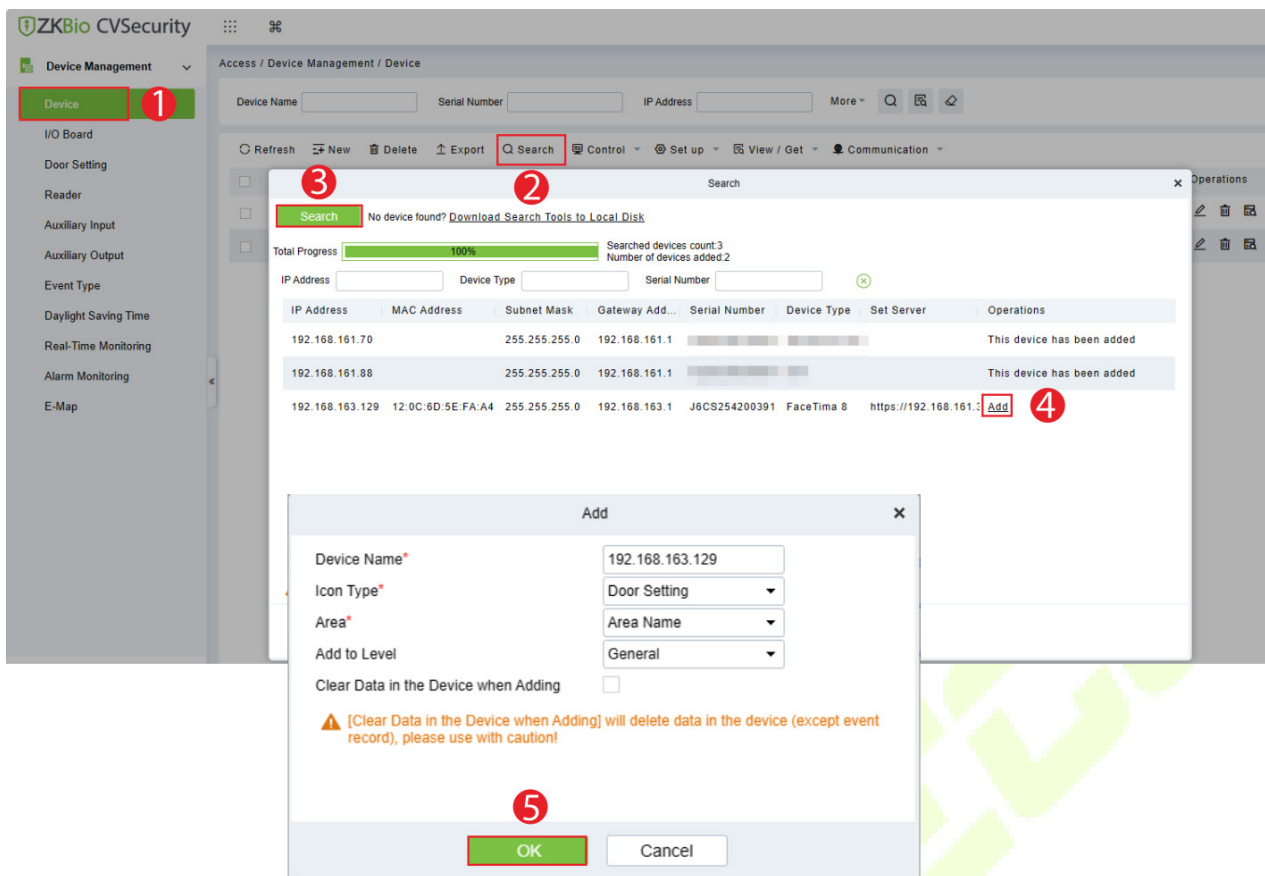
Server Port: Set the server port as of ZKBio CVSecurity.



14.2 Add Device on the Software

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

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



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

14.3 Add Personnel on the Software

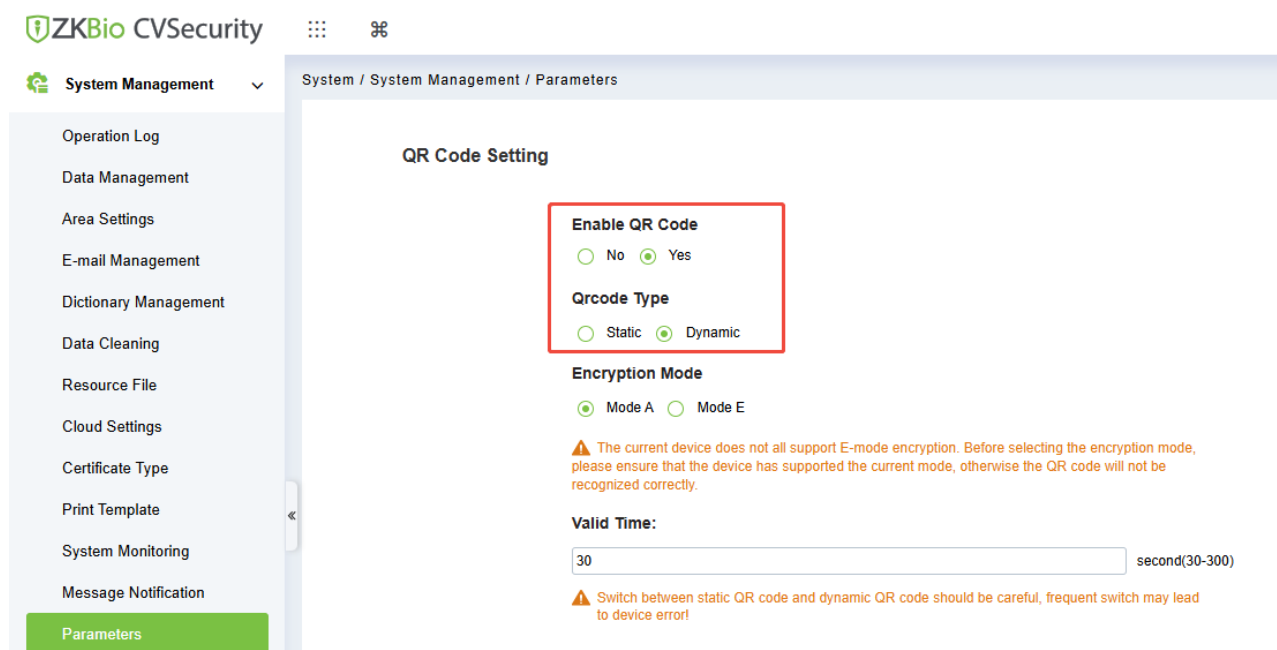
1. Click **Personnel > Person > New:**

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

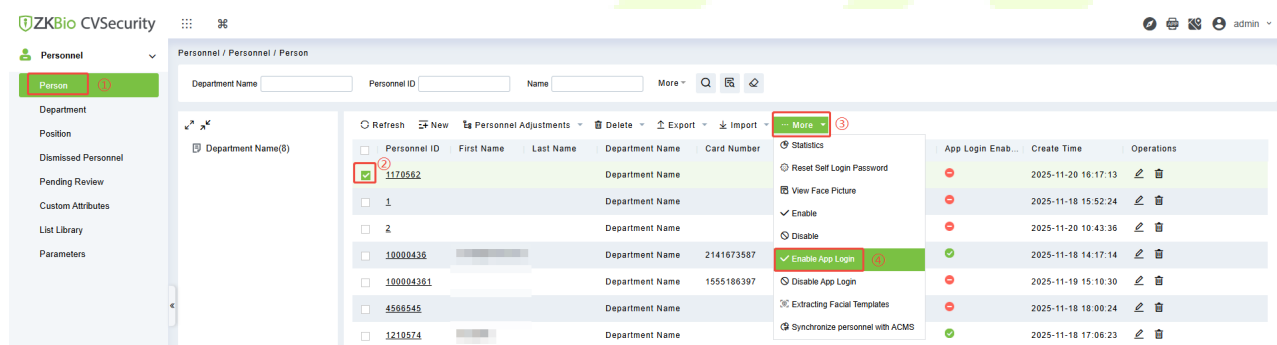
14.4 Mobile Credential★

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

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



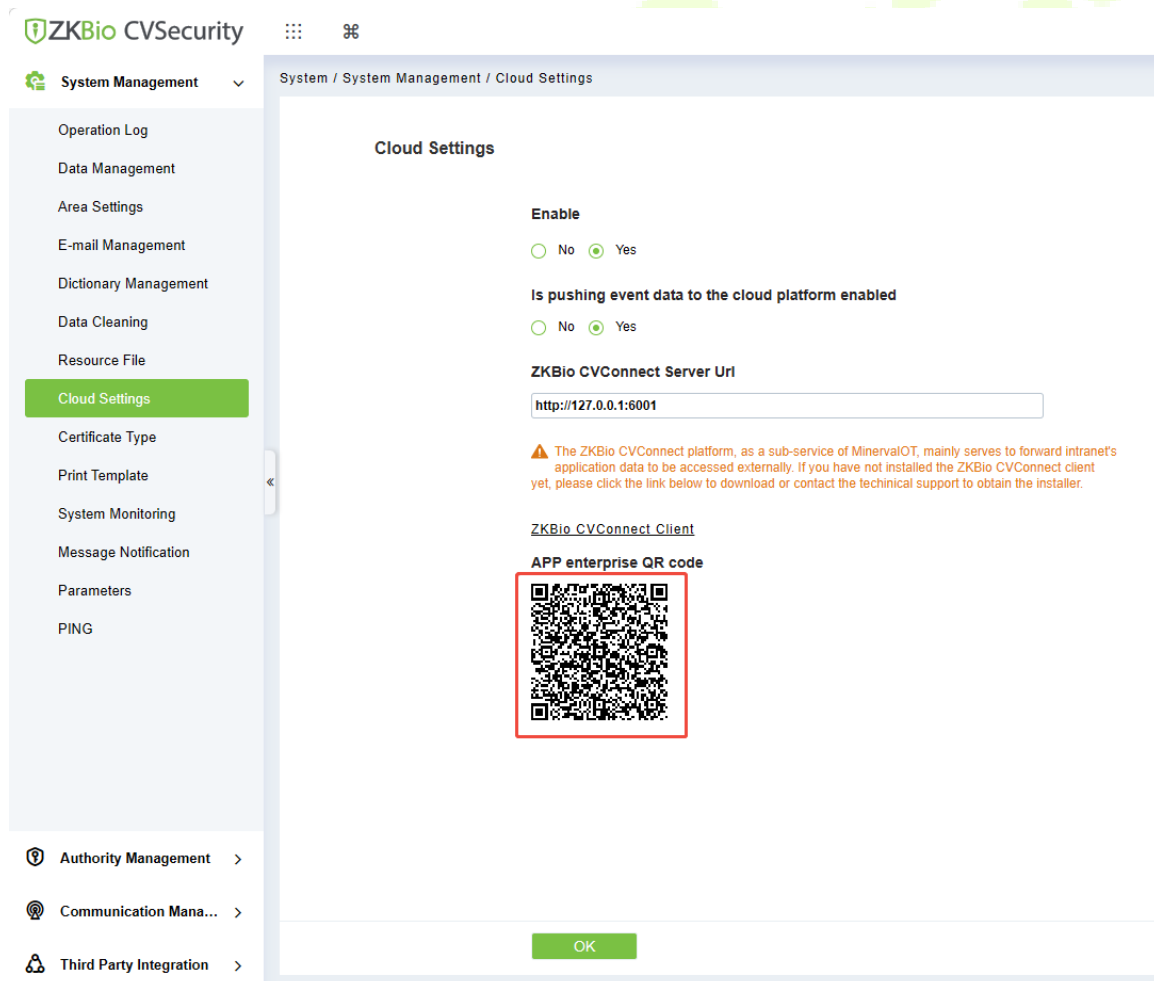
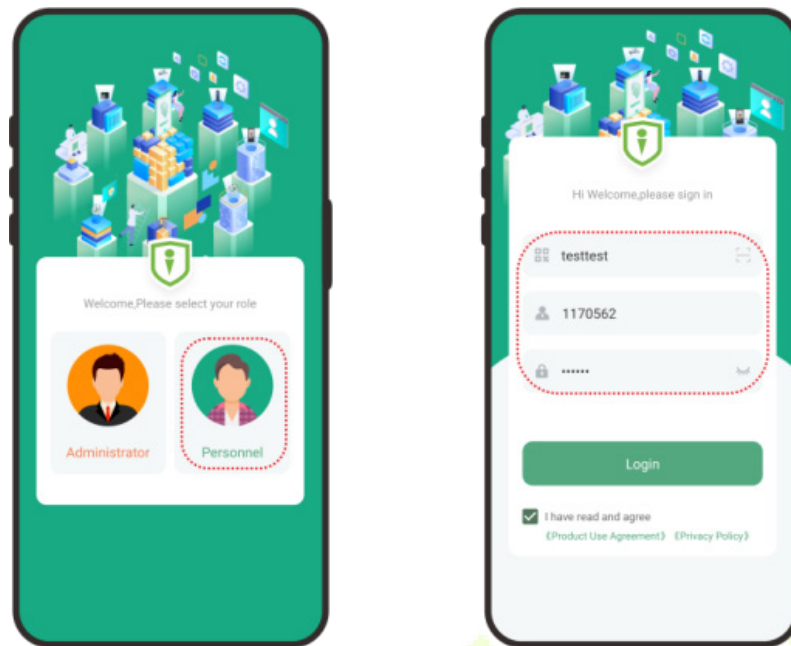
2. Click **Personnel > Personnel > Person**, select the personnel and click **More > Enable APP Login**.



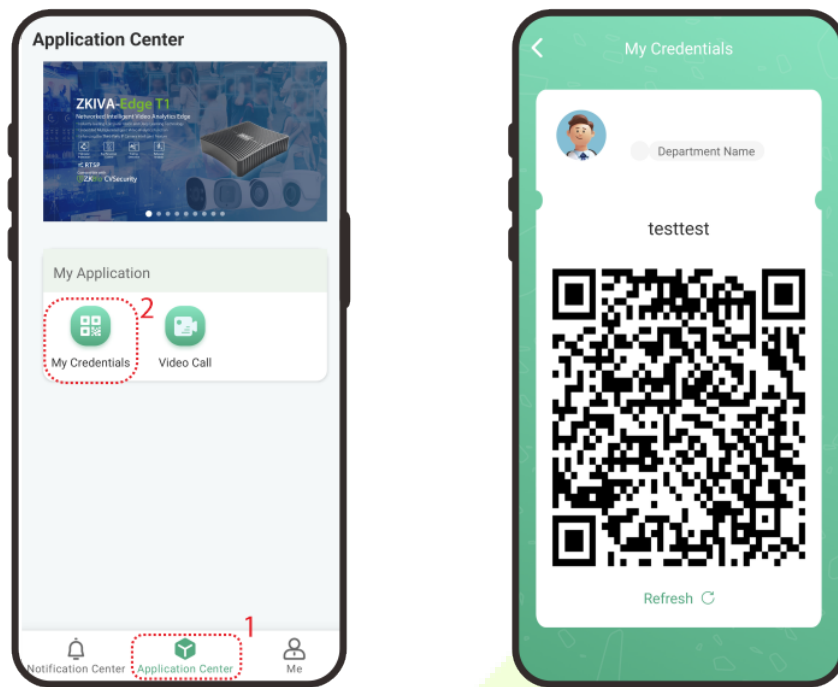
3. Open the App on the Smartphone. On the login screen, select the role **Personnel**, enter the account information, and click **Login**.

Organization Name: Scan the organization code you get before. (Enter **System > System Management > Cloud Setting > APP enterprise QR Code**)

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



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



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

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

15 SIP Video Intercom

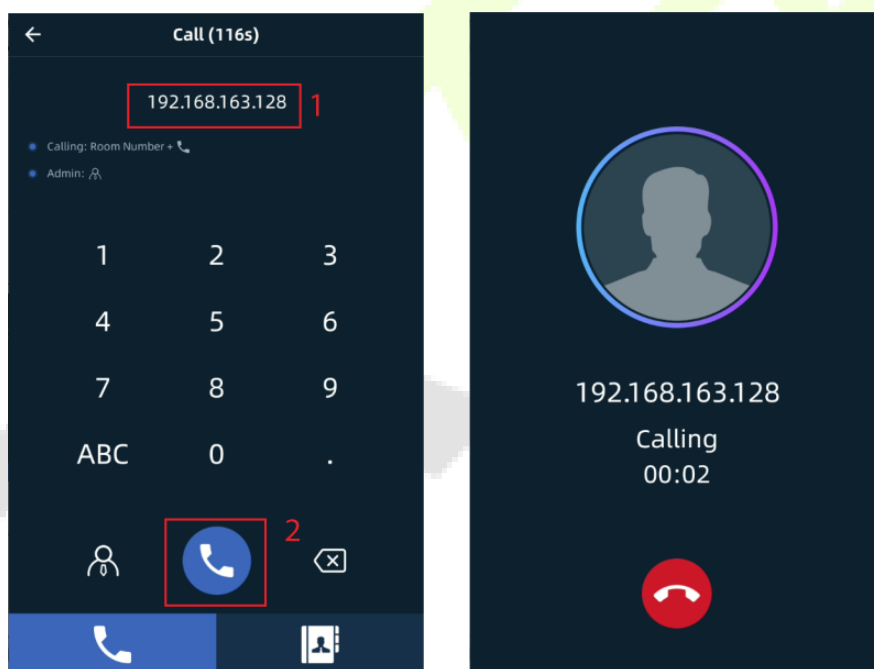
On the device's main menu interface, click **Intercom Settings > SIP Server Configuration**, and enable/disable **SIP Register** as needed.

SIP Register disabled: Suitable for standalone LAN-based intercom scenarios, where registration with a SIP server is not required.

SIP Register enabled: LAN calling is still possible; this setting only affects the online status registration and authentication of the SIP account.

15.1 Local Area Network Use

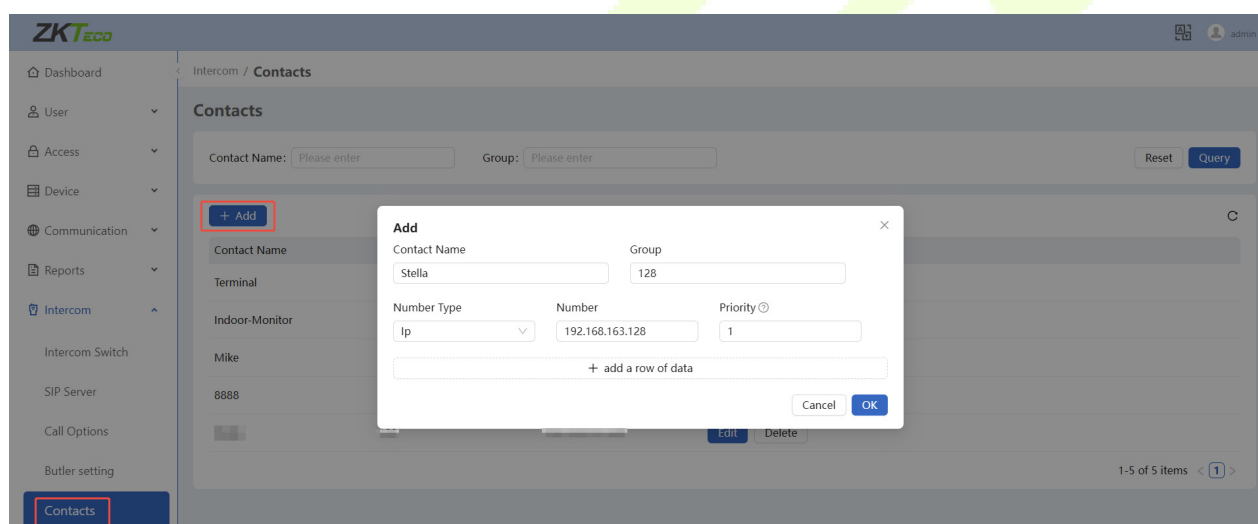
1. Ensure network connectivity between the device and the indoor station (i.e., they are on the same router or reachable). It is not mandatory for them to be on the same subnet.
2. To enable the video intercom function, click the icon  on the device and enter the IP address of the indoor monitor in the provided interface.





15.1.1 Call by Room Number / Contacts

1. On the device WebServer, click **Intercom** > **Contacts** > **+Add** to enter the adding contacts interface, input the relevant information of the indoor monitor, and then click **OK**.



Contact Name: Enter the name of the contact.

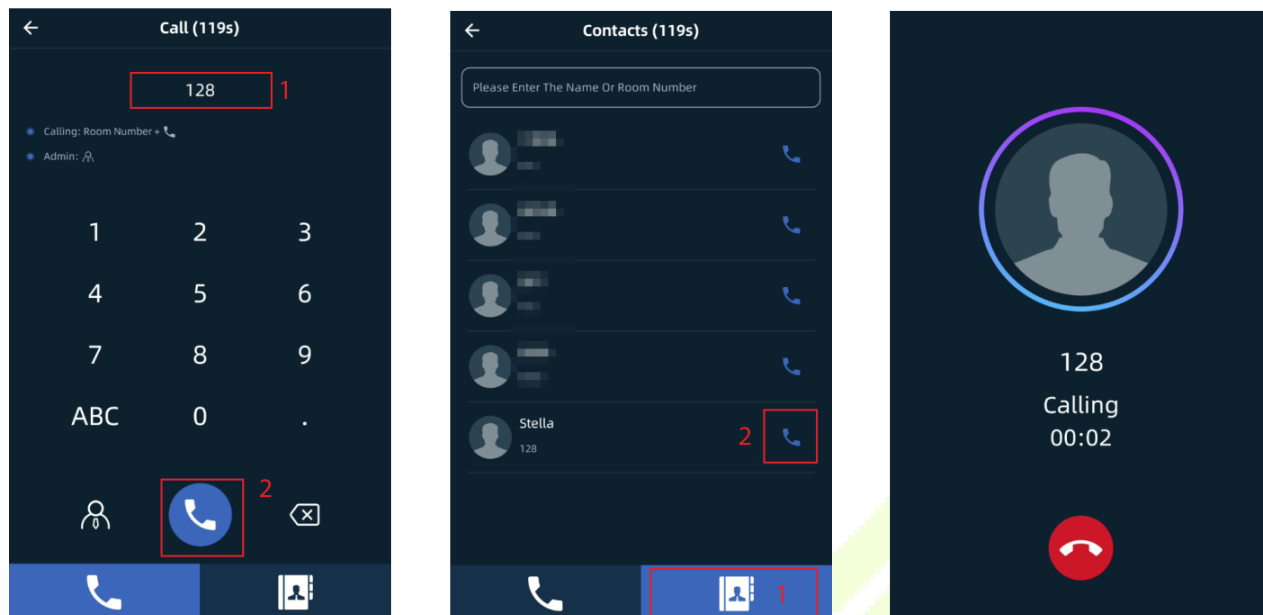
Group: Enter the group name.

Number Type: Select as Ip.

Number: Enter the IP address of the indoor monitor.

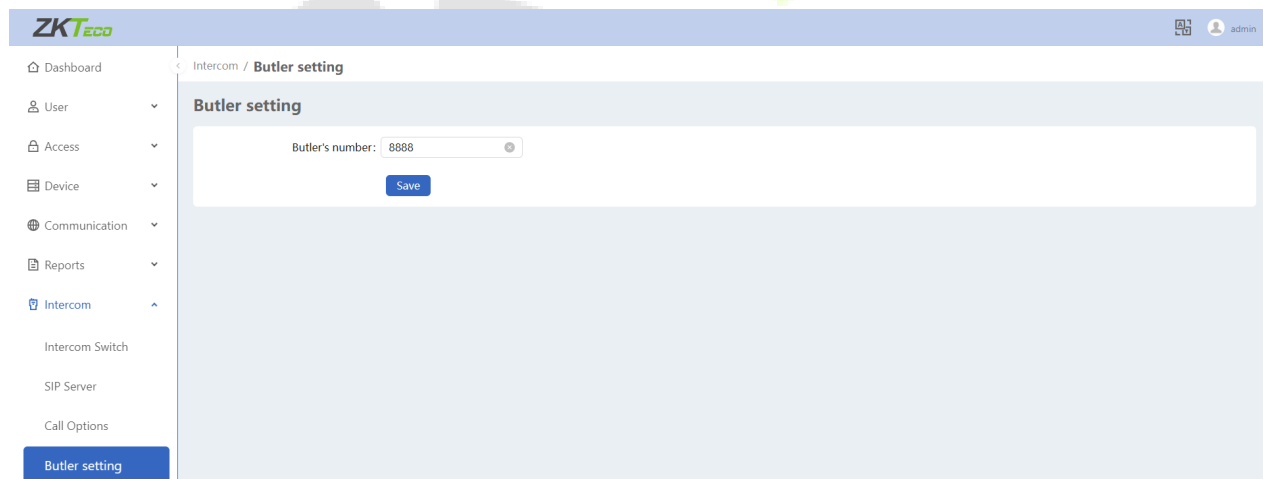
Priority: When multiple contact methods are configured for a contact, calls are made in order of priority. Value range: 0–99, default value is 1. Priority rule: The higher the number, the higher the priority. If priorities are the same, calls are initiated simultaneously. Special value 0 explanation: In a group call scenario, this number will not be called. However, when calling this contact individually, it can still be reached normally.

- After addition, click the  on the device to enter the call page, then you can directly enter the Room Number (i.e. Group Name) or click the  icon to open the contacts, select the indoor monitor you want to call.

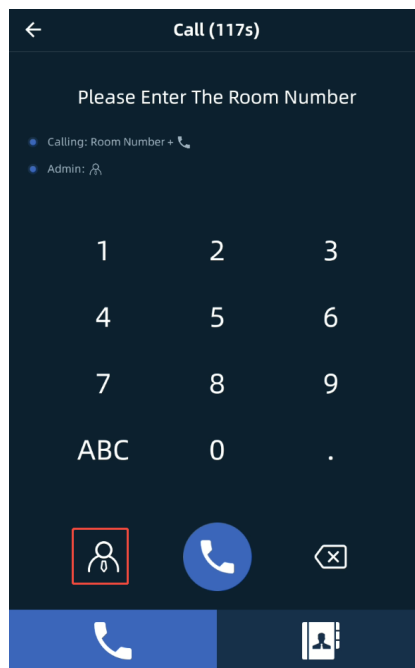


15.1.2 Call Admin

- On the device WebServer, click **Butler Setting** to enter the butler setting interface. Input the butler's number (this number must have been added to the contacts), and then click **Save**.

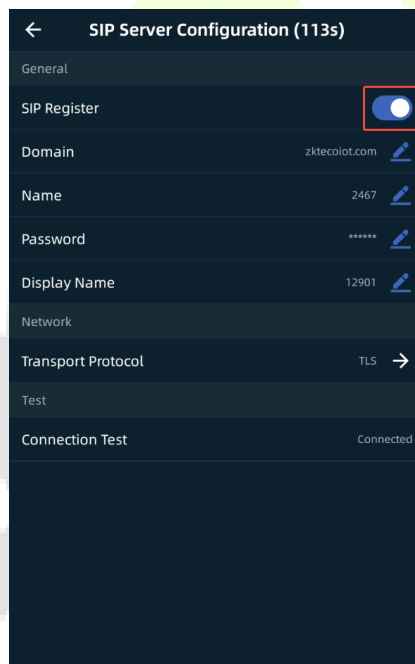


- After the setting is complete, click the  icon on the device to enter the call page, and directly click the  icon to make a one-click call to the administrator.



15.2 SIP Server

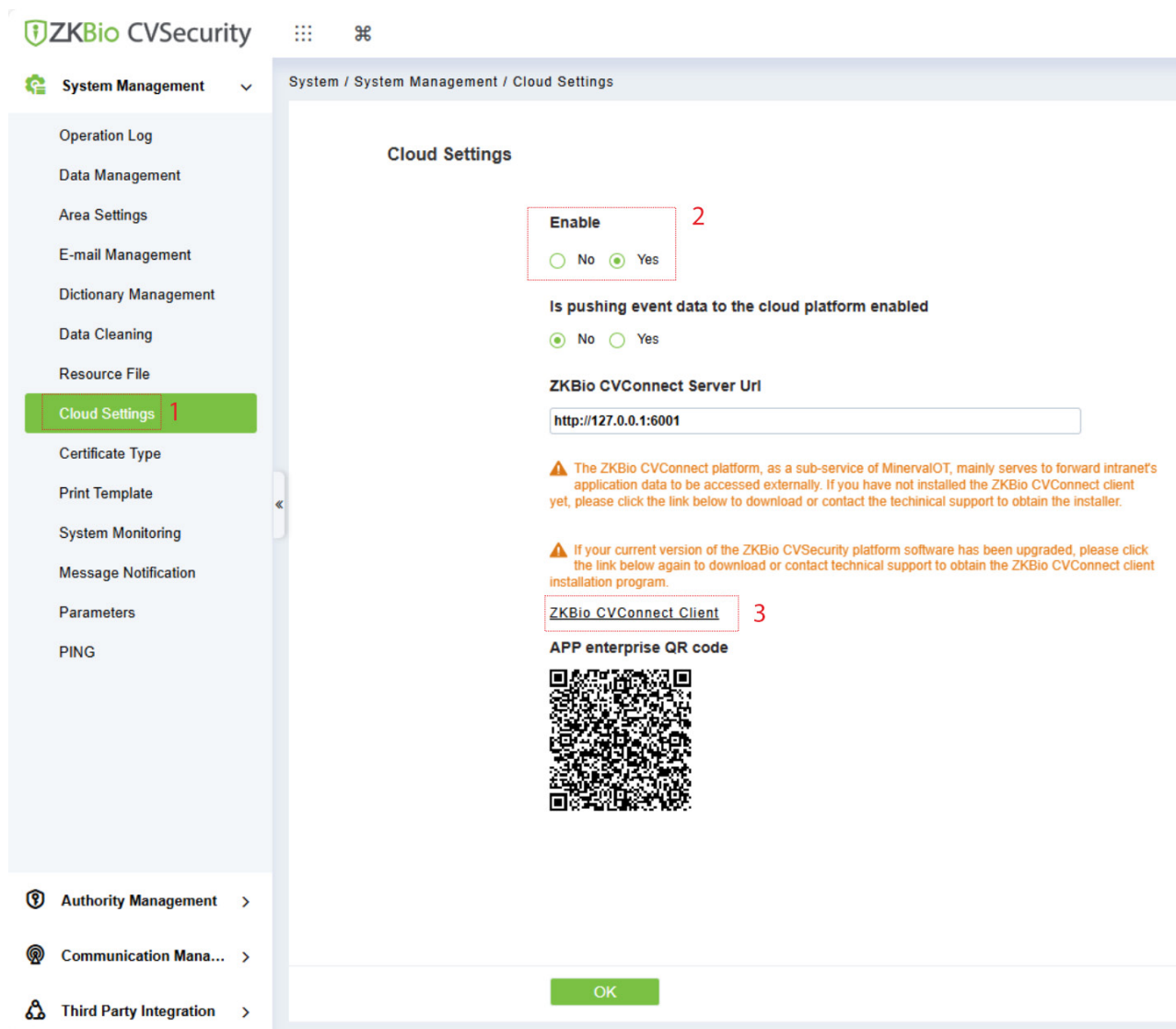
In this mode, please make sure that the SIP Server of the device is enabled.



This function needs to be used with the ZKBio CVSecurity server, ZKBio Zexus Mobile App, indoor monitor and PC Client BioTalk Pro.

15.2.1 SIP Server Configuration

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

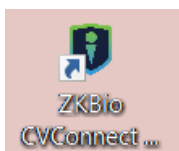


Note:

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

➤ ZKBio CVConnect Client Activation Steps

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



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

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

6seconds to automatically jump to the activation page

If the jump fails, go manually. [Manually jump](#)

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

1. Select Area

ZKBio CVConnect Activation
[Activation code activation >>](#)

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

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

* Area:

* Local Application:

Endpoint:

Next

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

2. Bind ZKBio CVConnect Account

ZKBio CVConnect Activation
[Activation code activation >>](#)

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

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

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

* Username:

* Password:

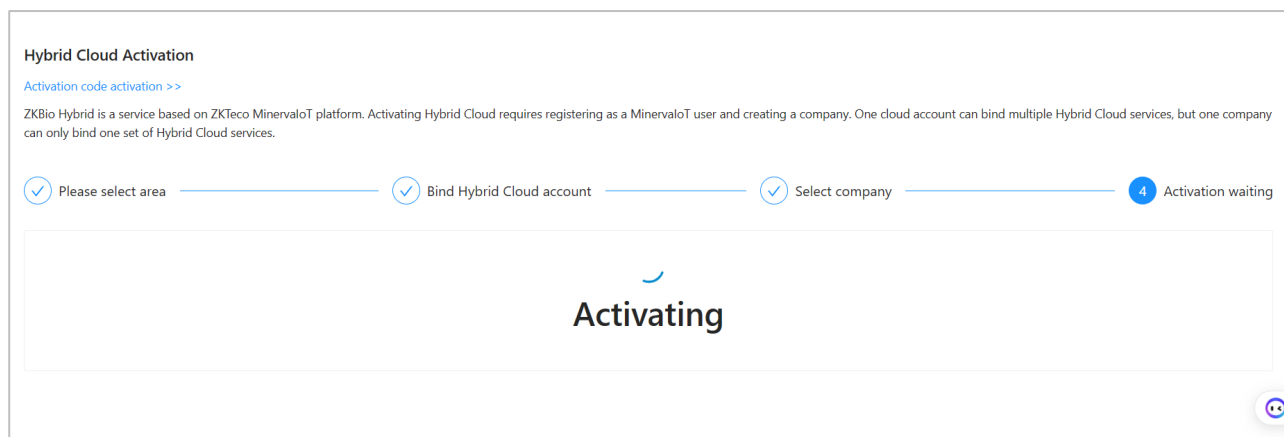
Previous Next

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

3. Select Company

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

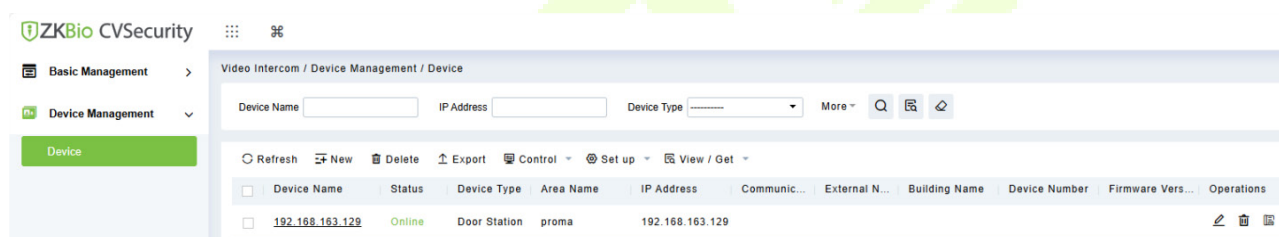
Start Activating and wait for 1-2 minutes until the Activation completely.



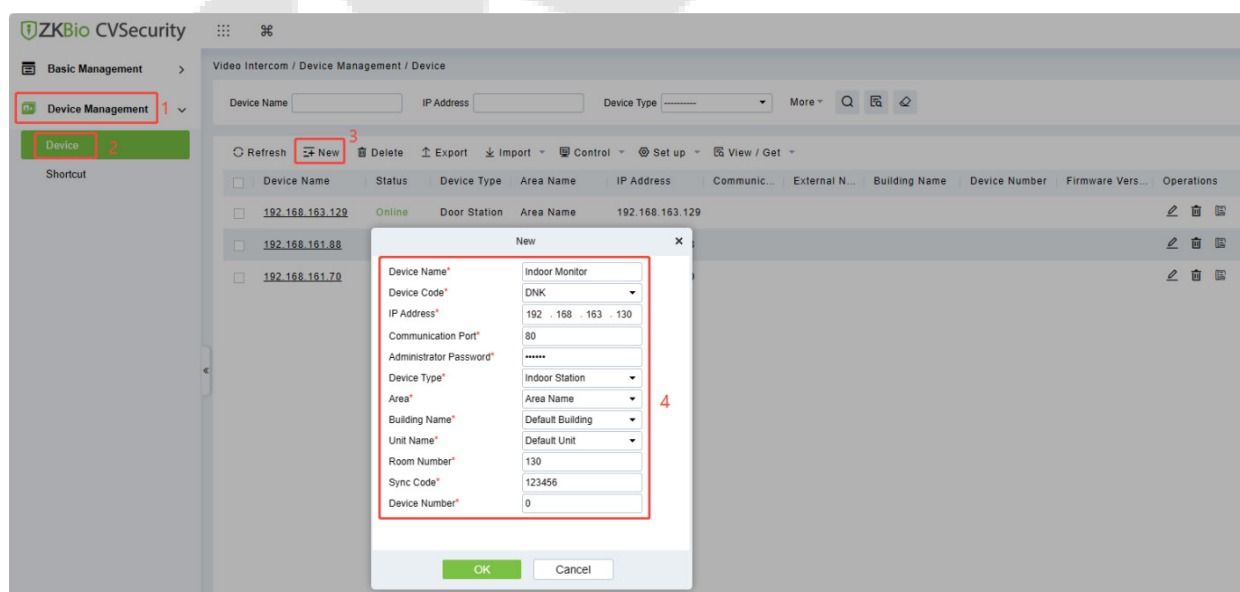
The specific installation and activation steps of the ZKBio CVConnect client can refer to ZKBio Zexus Mobile App User Manual.

15.2.2 Add Device

1. Add the device to the **Access** Module of the software. Then the device will be automatically synchronized to the **Video Intercom** module. (The adding method can refer to [14 Connect to ZKBio CVSecurity Software](#))

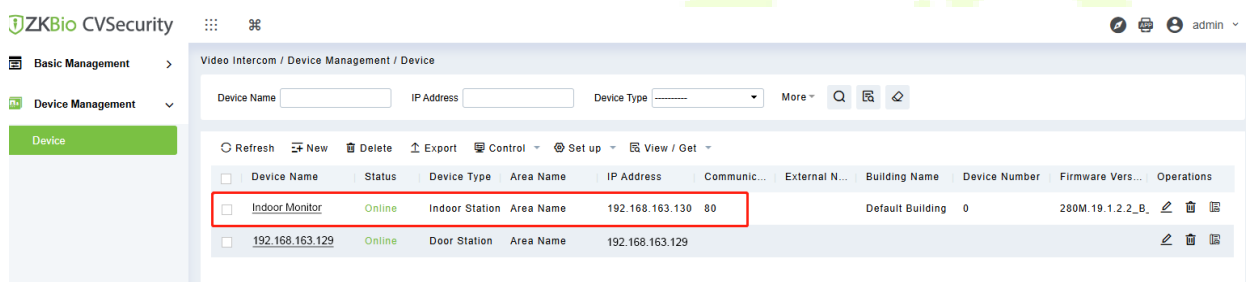


2. Click **Video Intercom > Device Management > Device > New** to add the indoor monitor.



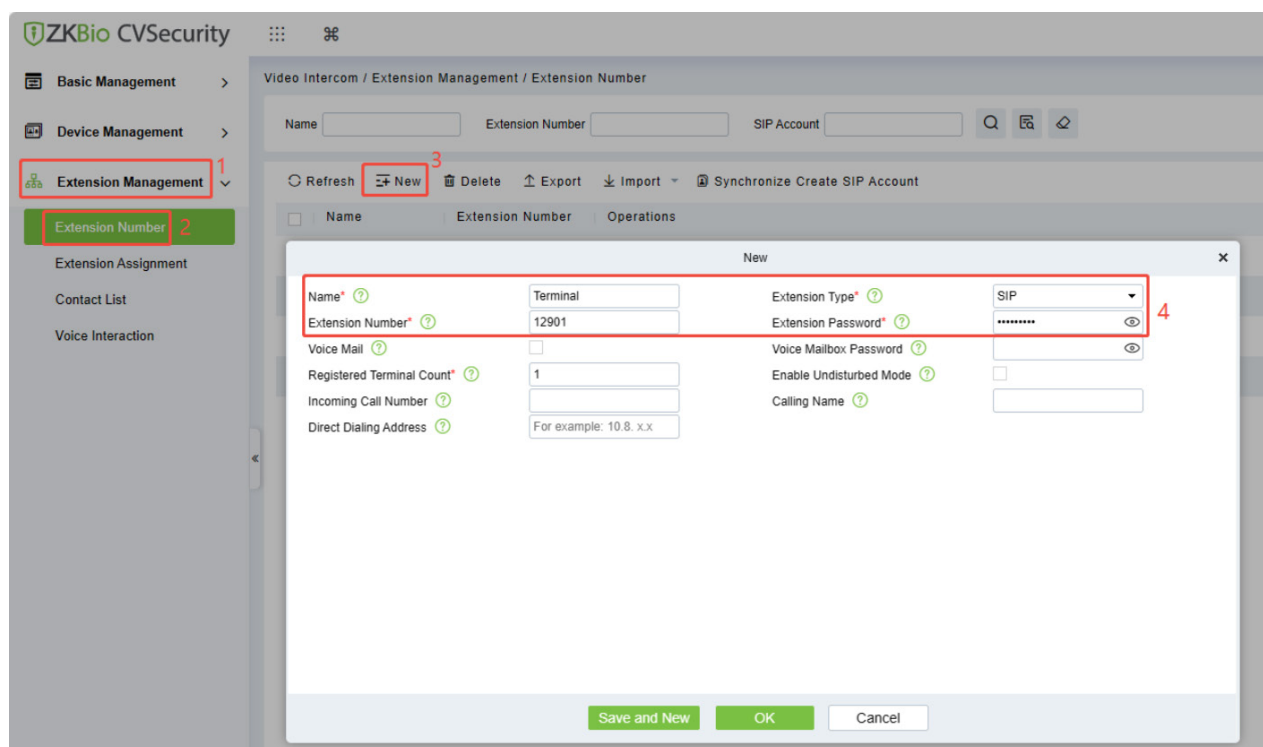
- **Device Name:** Enter the name of the indoor monitor.
- **Device Code:** Set as DNK.
- **IP Address:** Enter the IP address of the indoor monitor.
- **Communication Port:** 80 by default.
- **Administrator Password:** 123456 by default.
- **Device Type:** Set as Indoor Station.
- **Area/ Building 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.

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



15.2.3 Create Extension Numbers

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

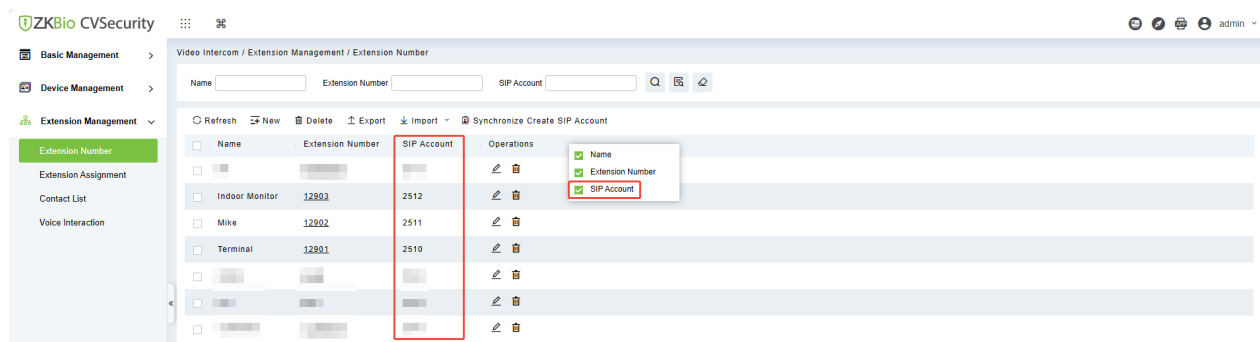


- **Name:** Customize the extension name. If it is a residential scene, the name can be set to the room number; if it is an office scene, the name can be set to the work number and name information.
- **Extension Type:** SIP by default.
- **Extension number:** Customize the extension number; for example, the number of Room 401, Unit 2, Building 1 can be defined as 12401 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 12901, the system automatically generates the SIP account as 2510, so the SIP Username used on the terminal is 2510.

Note:

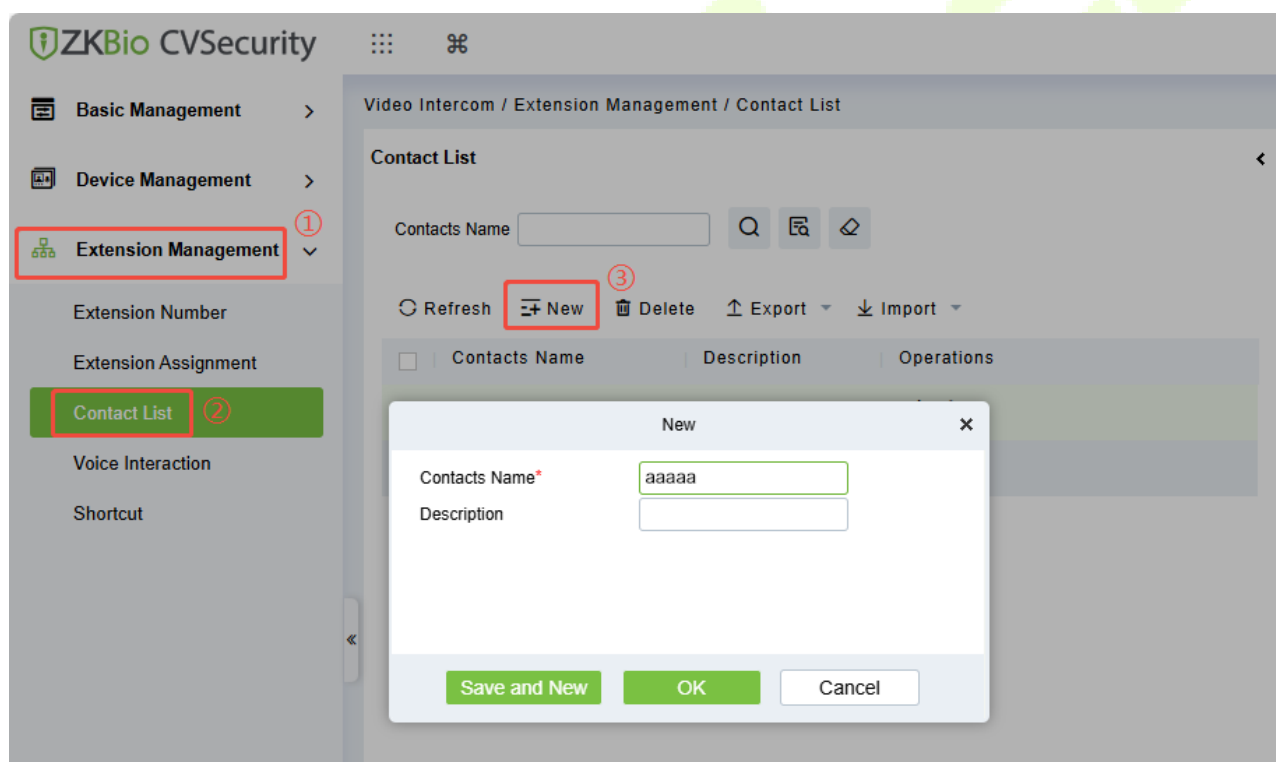
The SIP Account column is hidden by default. You can right-click the row which Operations is in and check the SIP Account to display it.



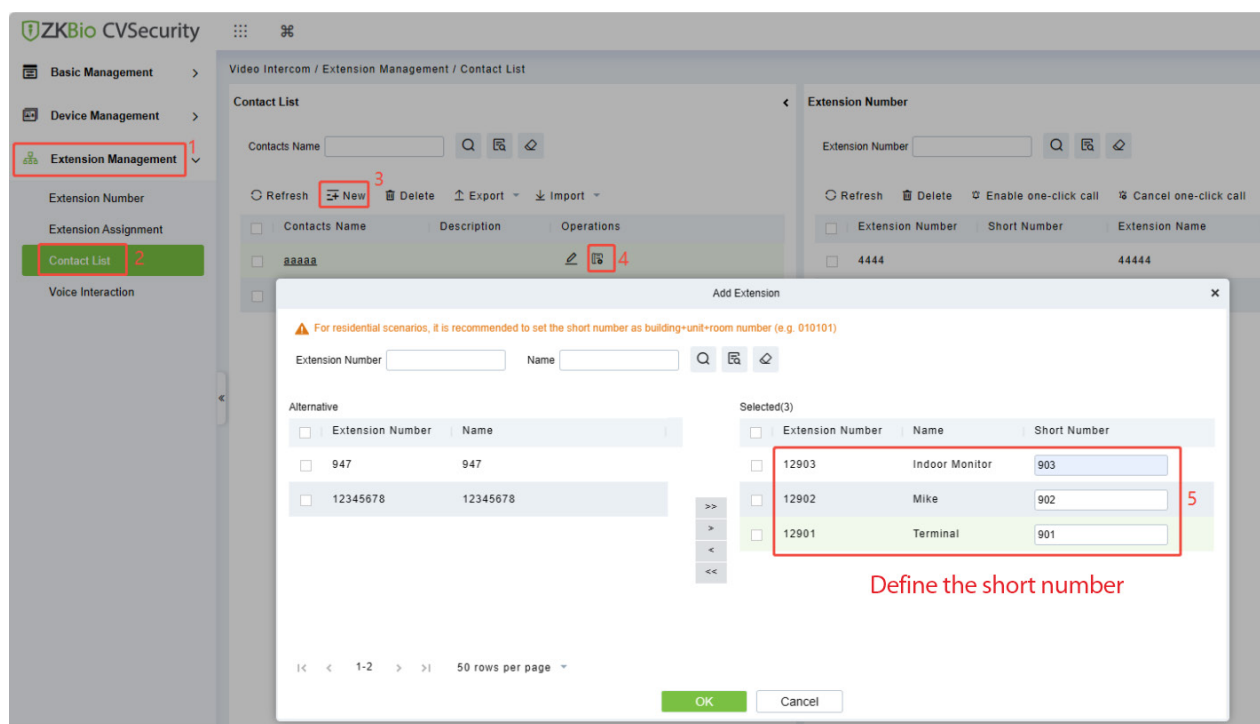
15.2.4 Contact List

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

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



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.



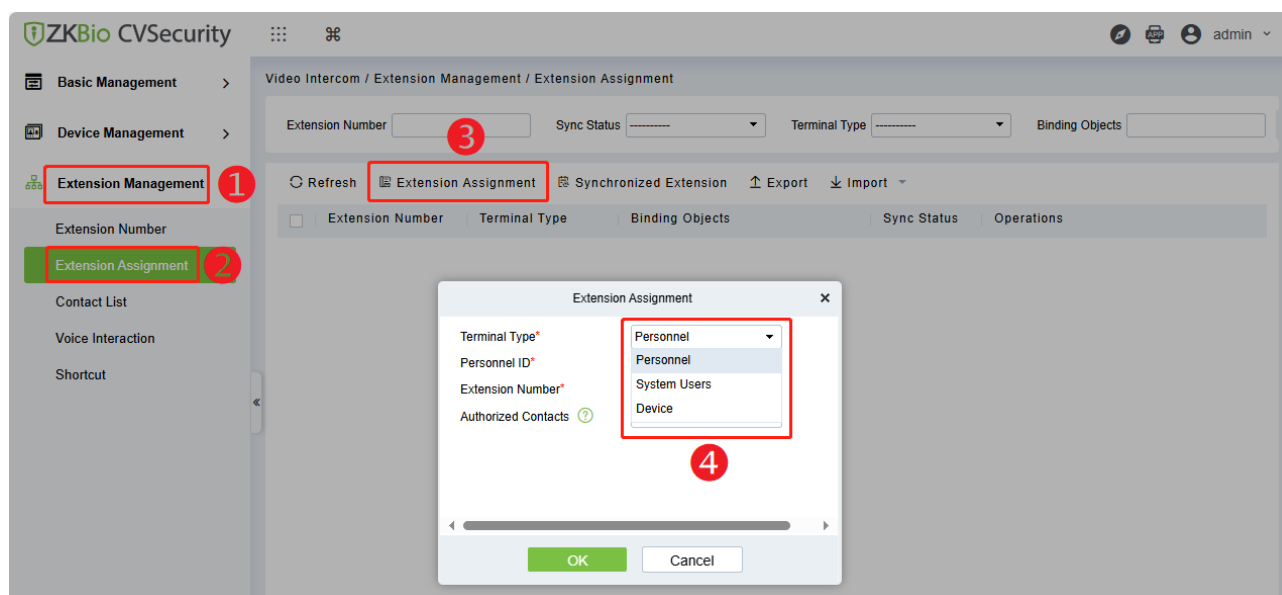
Note:

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.

15.2.5 Assignment of Extension Numbers and SIP Accounts

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

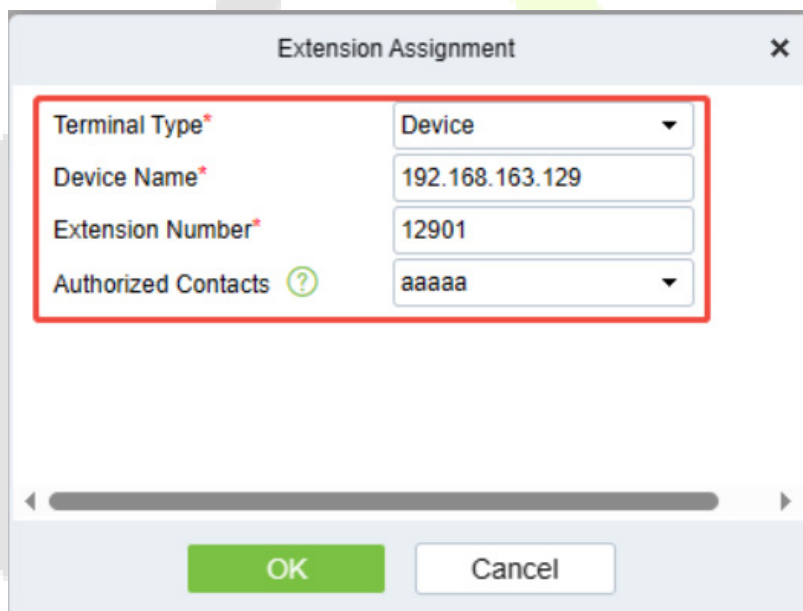
Click **Extension Management > Extension Assignment > Extension Assignment**, select the Terminal Type.



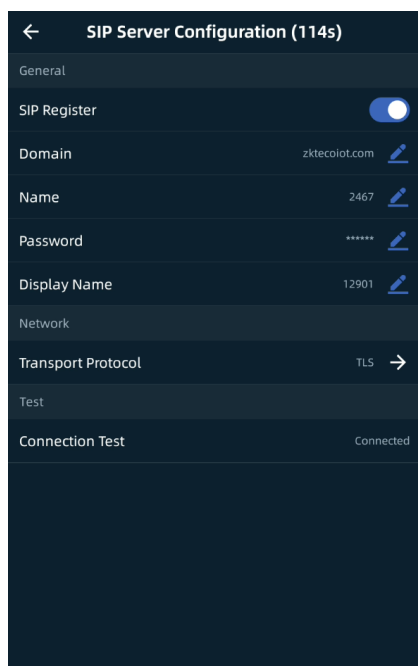
• Device Account Assignment

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

Note: The indoor monitor does not support the synchronization of contact list for the time being.



3. After successful assignment, the icon  will be displayed in the upper right corner of the device, indicates that the device is connected to the server. User can also click **Intercom Settings > SIP Server Configuration** to see that SIP server and account information have been automatically written, as shown in the following figure.

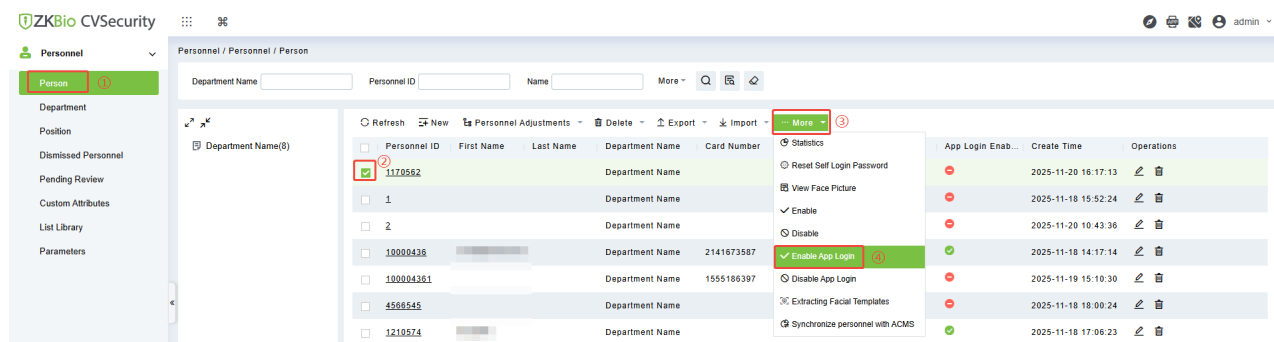


- **Personnel Account Assignment (ZKBio Zexus App)**

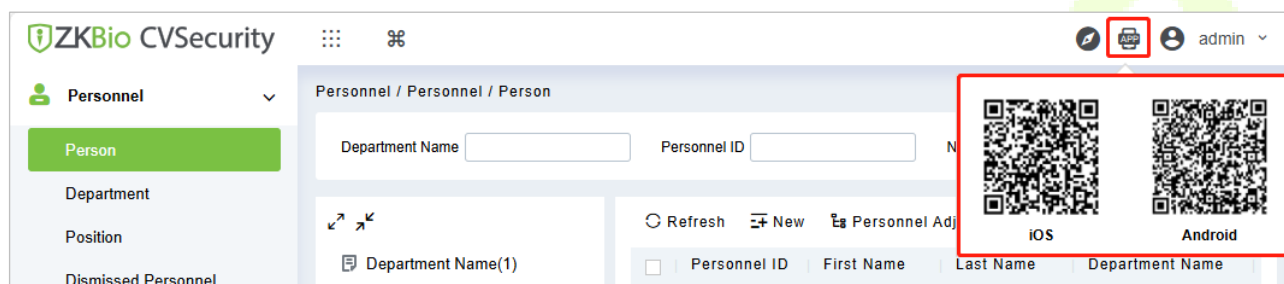
1. Select the Terminal Type as **Personnel**.
2. Select the person to be assigned an account and the extension number. Select the Authorized Contacts to assign the contact list to the individual, and after the assignment, the individual can view the contacts in the contact list upon logging into the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

Note:

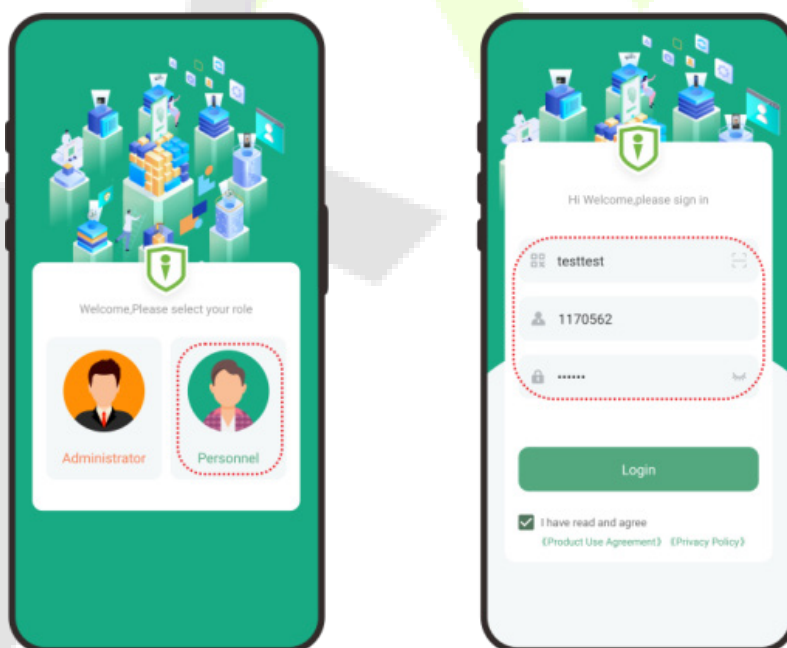
- 1) Before assign account to the personnel, you need first add personnel in ZKBio CVSecurity. The adding method can refer to [14 Connect to ZKBio CVSecurity Software](#).
- 2) The personnel need to enable APP Login. (Click **Personnel** > **Personnel** > **Person** > **More** > **Enable APP Login**.) Once a person has enabled APP login, they can directly access the Video Intercom feature upon logging into the App.



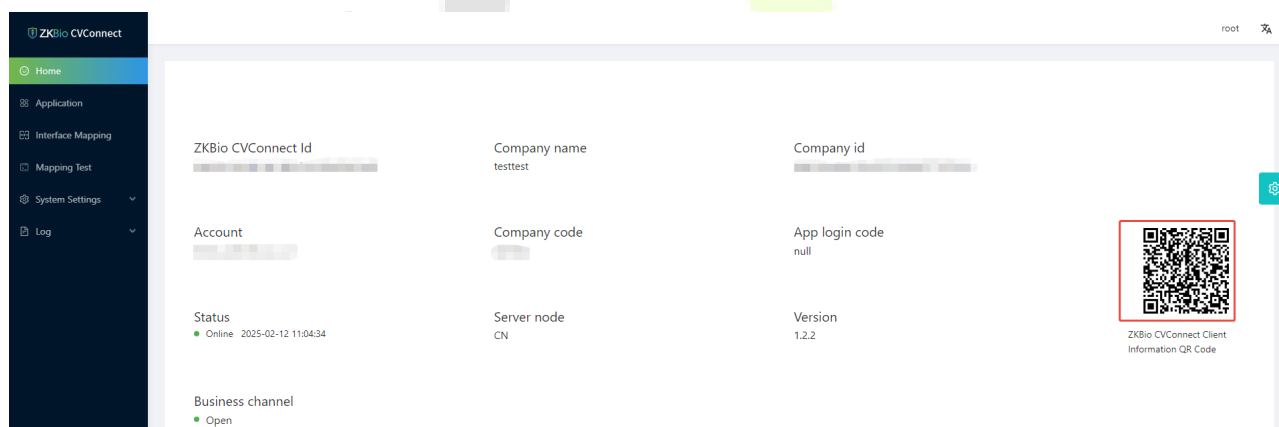
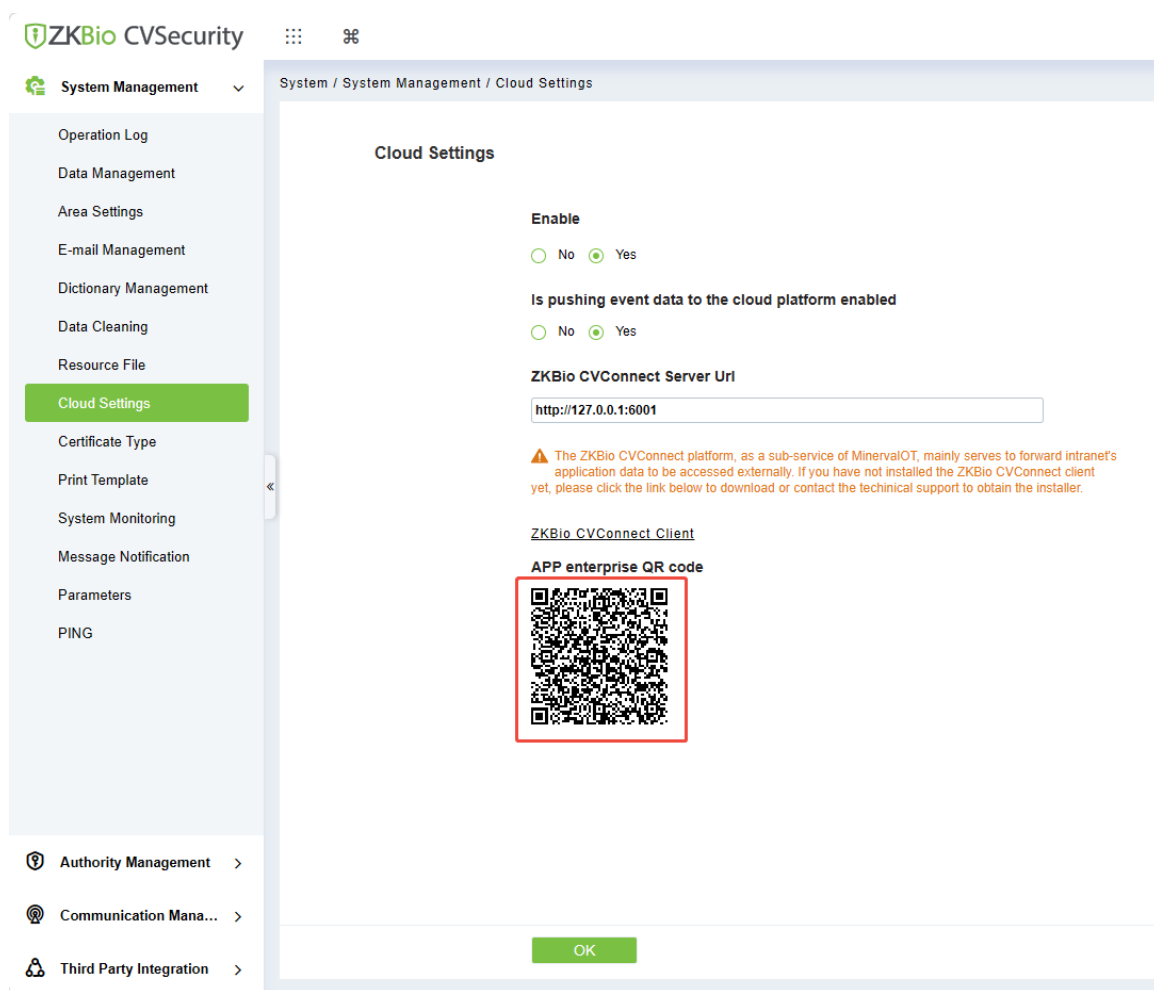
- 3) User can click the  icon at the right top corner of the ZKBio CVSecurity interface to scan the QR code to install the ZKBio Zexus App.



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

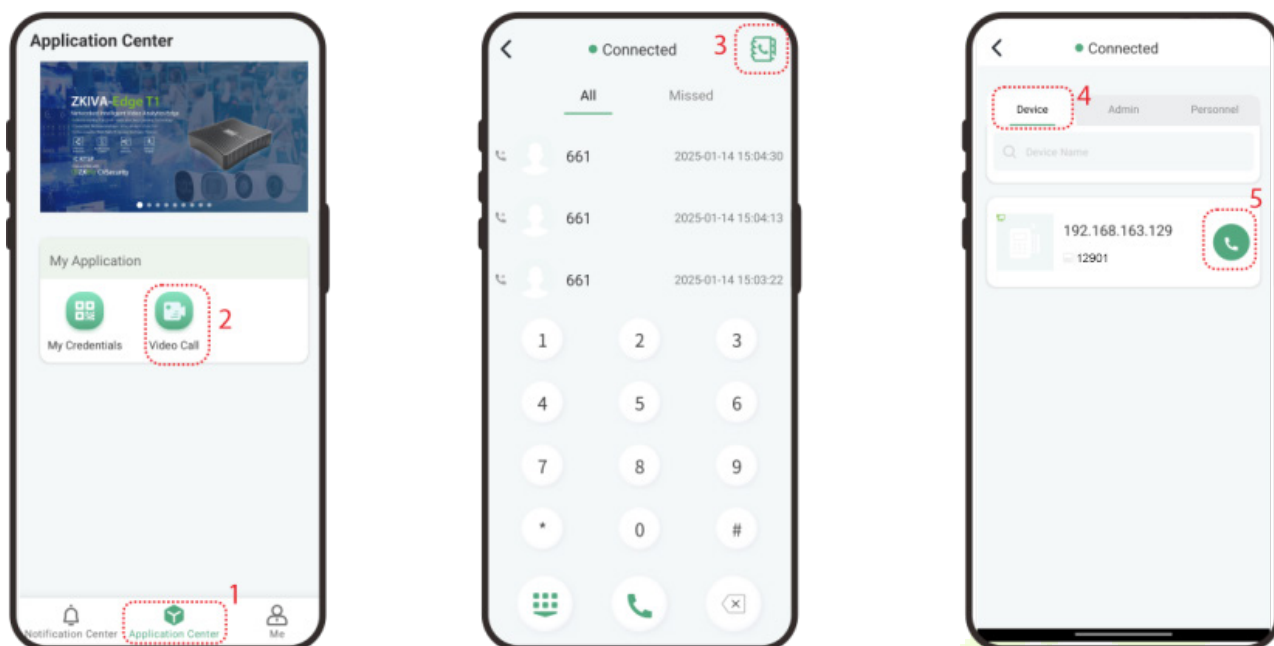


Organization Name: Scan the organization code you get before. (Go to ZKBio CVSecurity web, enter **System > System Management > Cloud Setting > APP enterprise QR Code**, or go to ZKBio CVConnect client, scan the ZKBio CVConnect Client Information QR Code.)



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

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



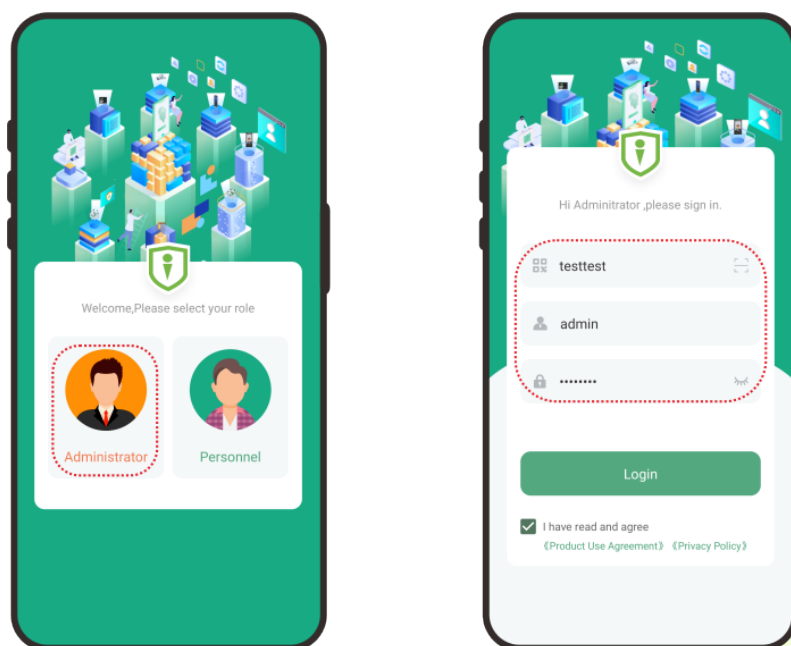
- **System User Account Assignment (ZKBio Zexus App)**

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

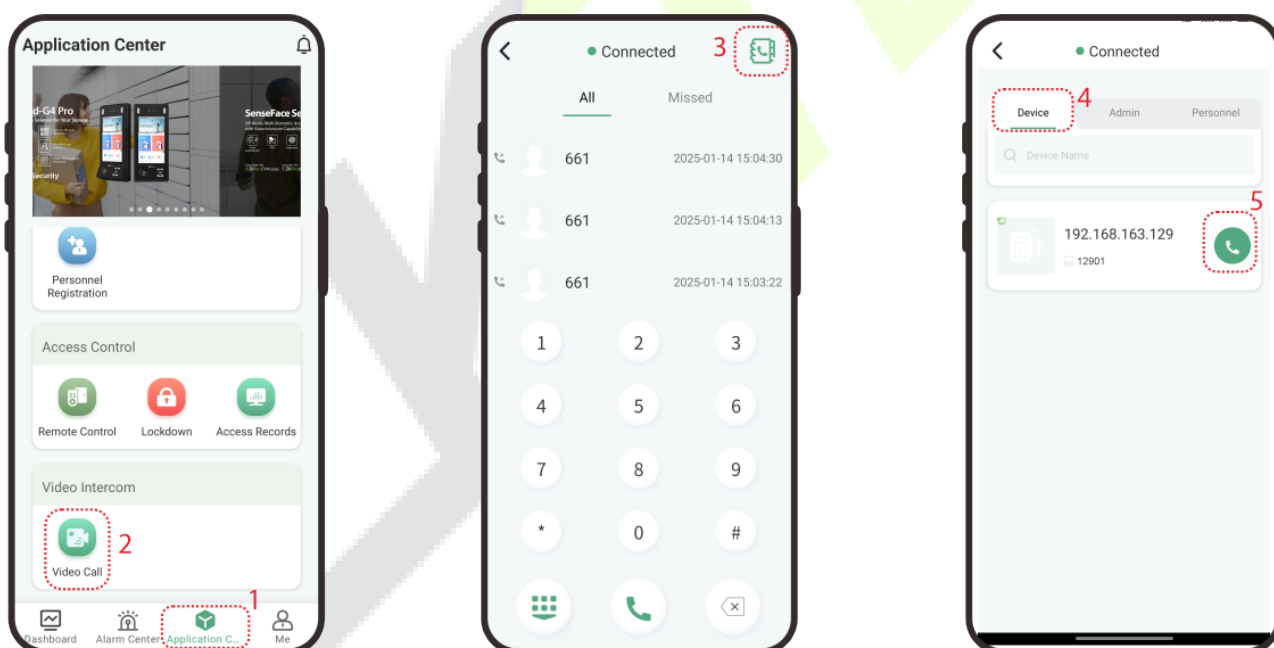
3. After successful assignment, the admin can login to the App. Select the role-**Administrator**, enter the account information, and click **Login**.

Organization Name: Scan the organization code you get before.

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



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



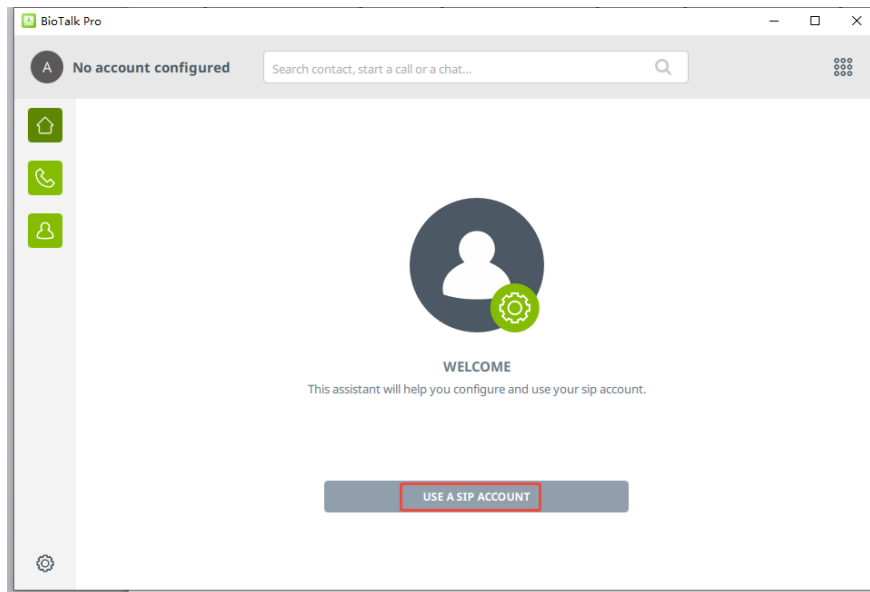
The App complete operation steps please refer to the ZKBio Zexus Mobile App User Manual.

15.2.6 PC Client Functionality

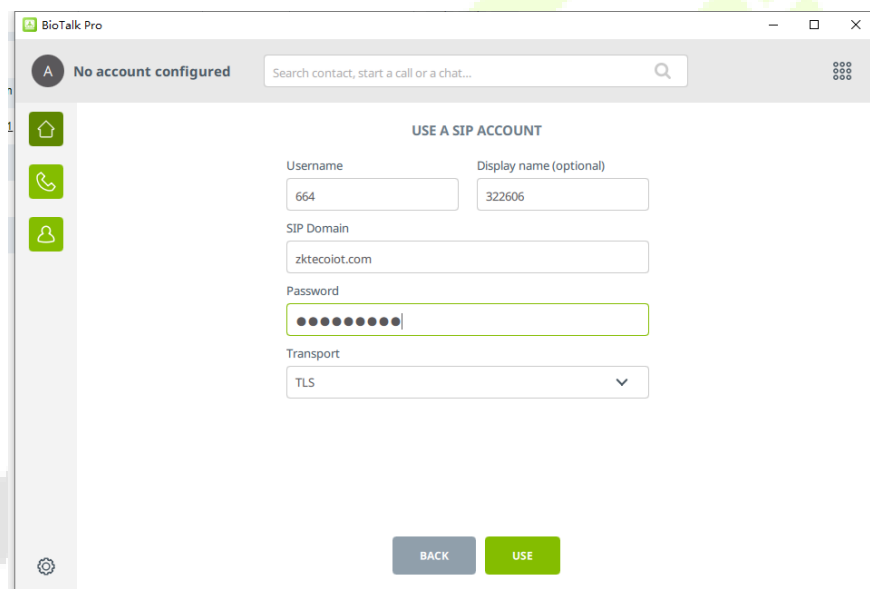
To use the BioTalk Pro PC client, please contact the appropriate person for an installation package.

Operation Guide

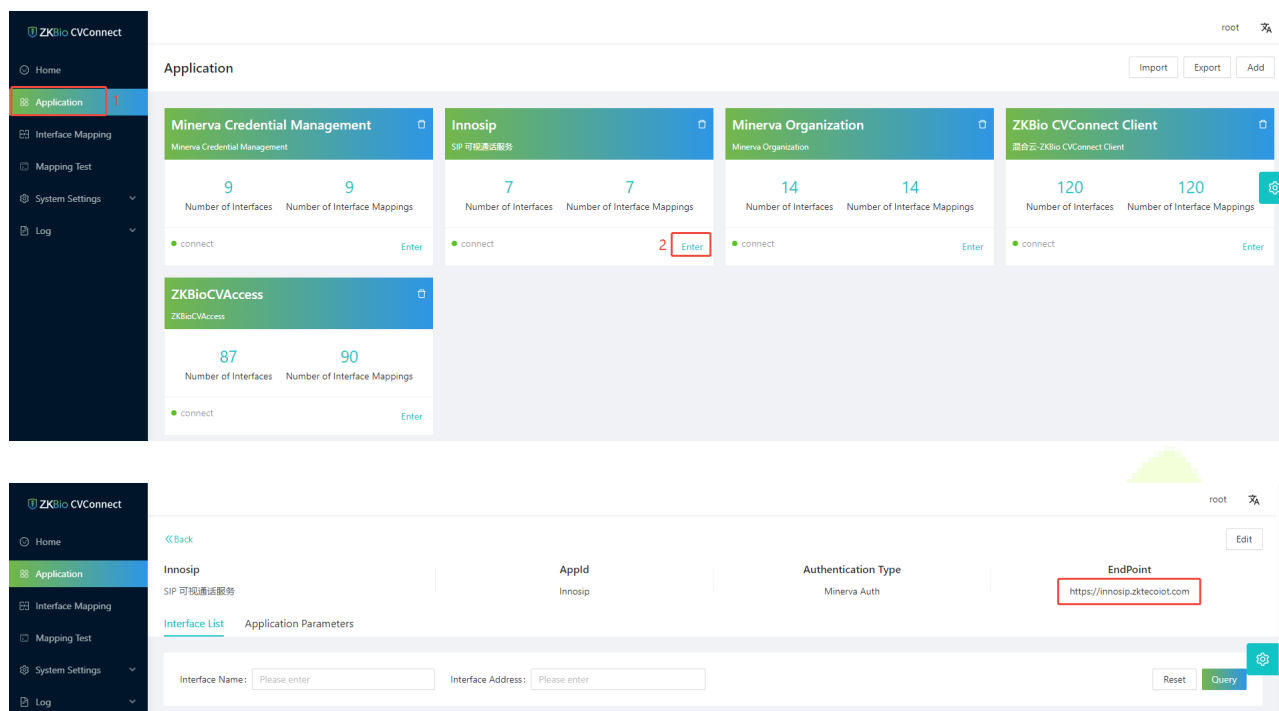
Step 1: Configure the SIP account: Click **USE A SIP ACCOUNT** button.



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

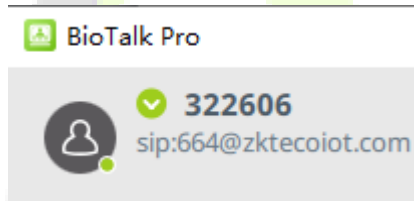


- **Username:** Enter the SIP account. (**Note:** You need to create a new SIP account for the PC client in ZKBio CVSecurity, then you can use the account to login to the PC client.)
- **Display Name:** It is the extension number.
- **SIP Domain:** The SIP Server Domain. (Go to ZKBio CVConnect client,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



- **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:

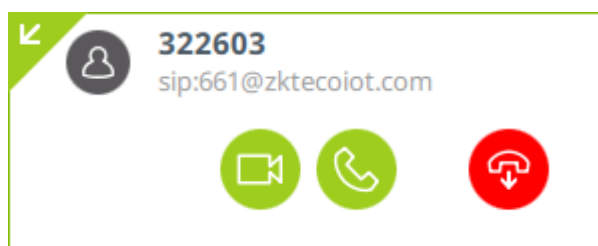


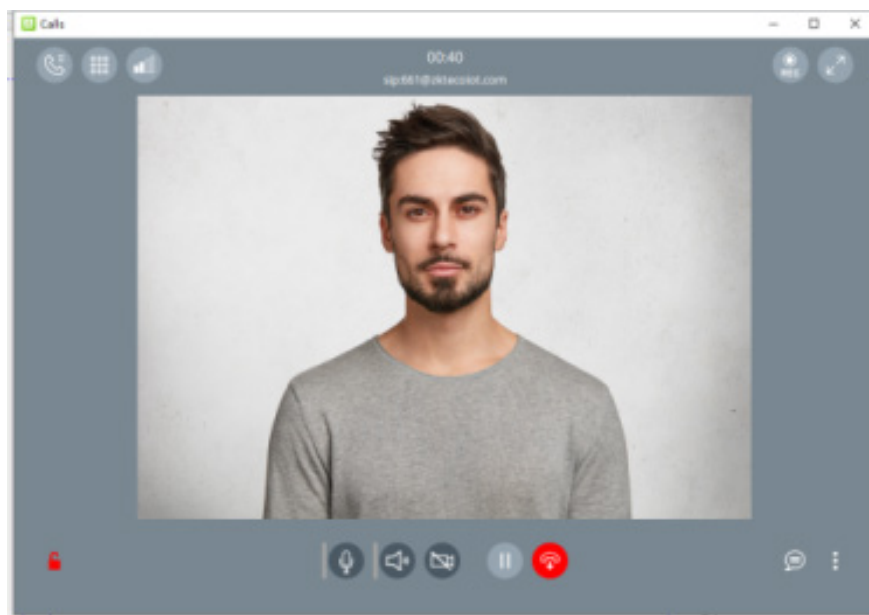
Note: In the Cloud SIP mode, if dialing is required, the PC Client should dial directly to the target SIP account. For example, if the extension number created on ZKBio CVSecurity is 322603, the corresponding generated SIP account is 661, then the PC Client should dial 661 when making a call. Therefore,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

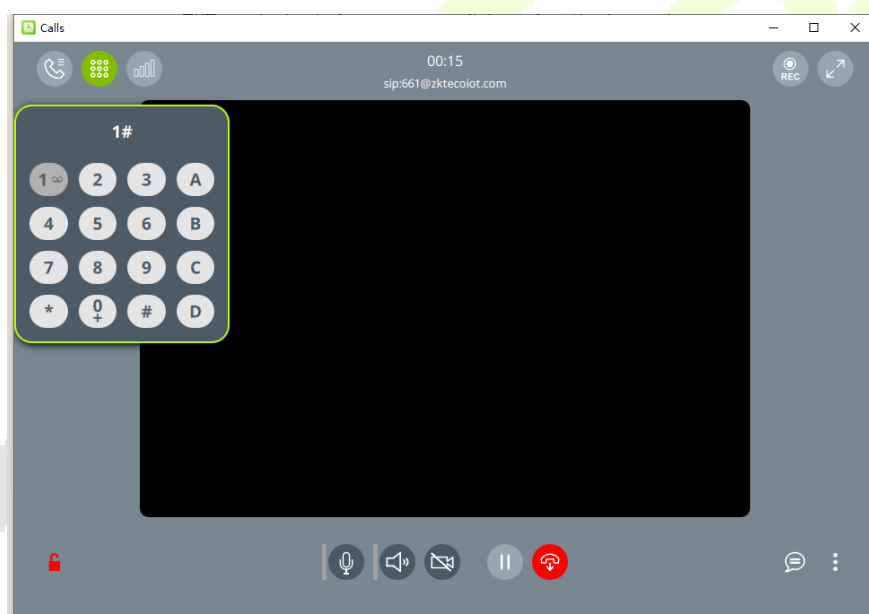
When the PC Client receives a call, a window alert will pop up in the lower right corner of the desktop.

Click the  icon to accept it.





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

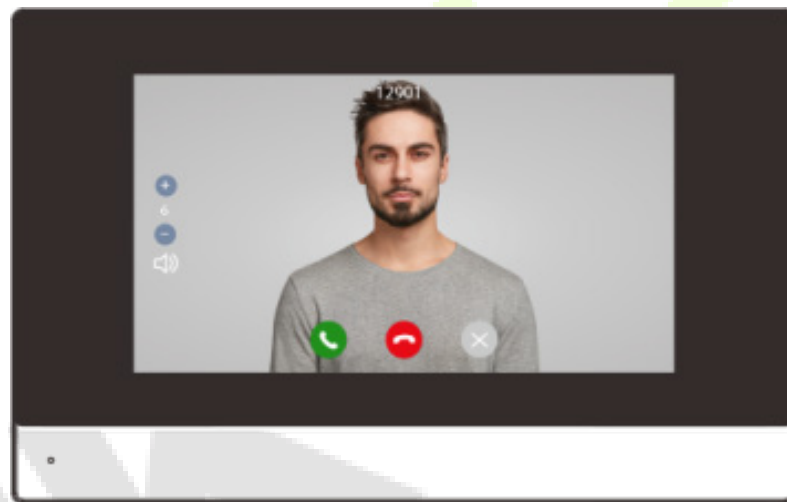
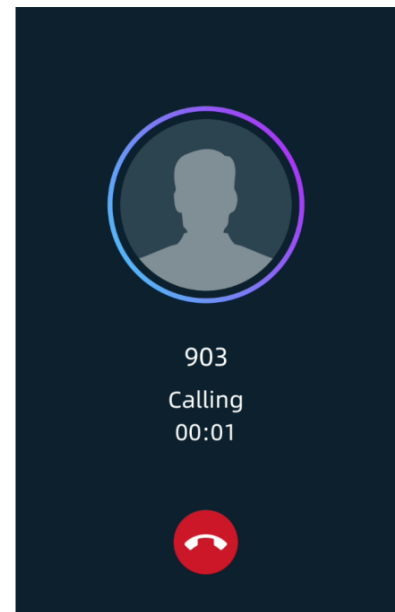
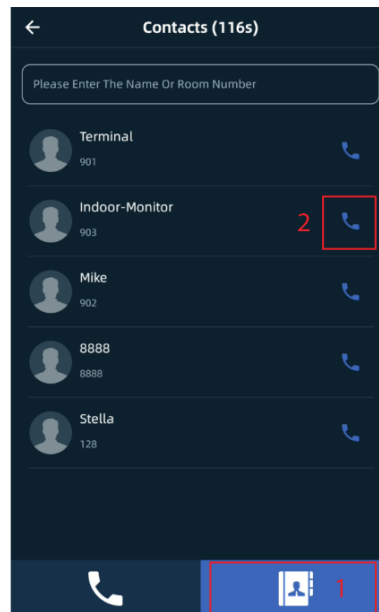
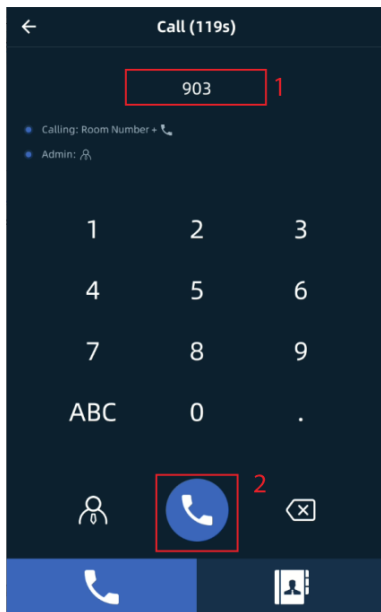


15.2.7 Make a Call

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

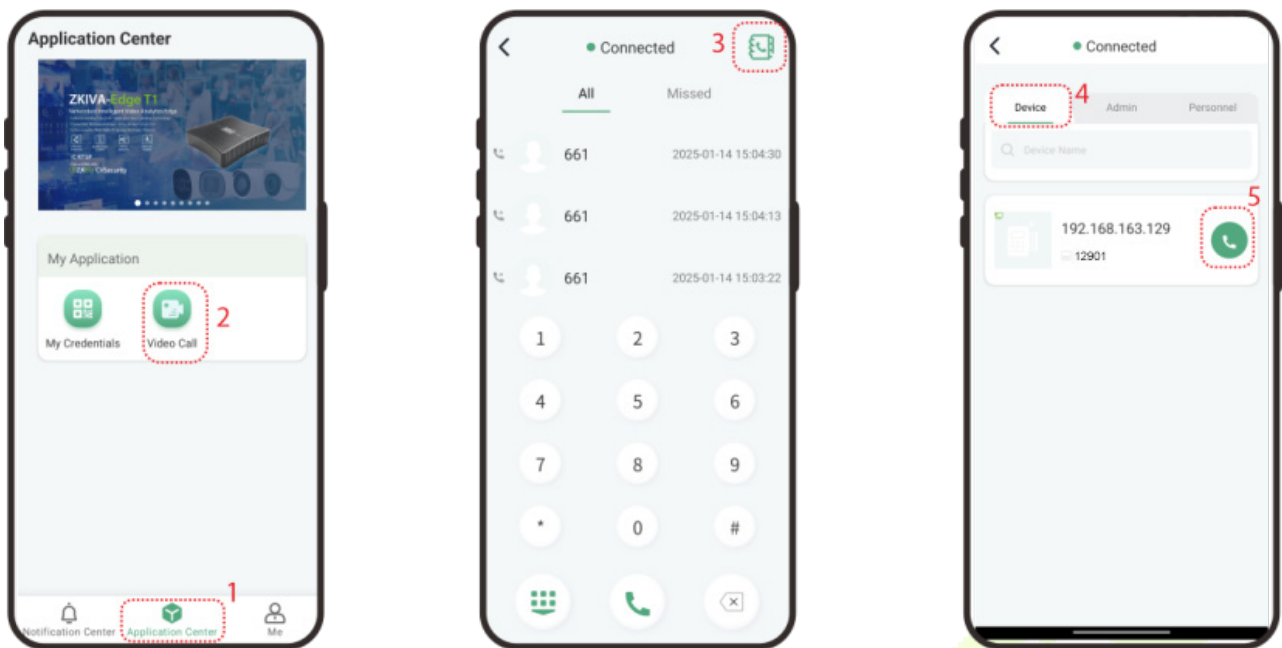
- **Device Calling**

Click the icon  on the device and enter the Number of the indoor monitor/personnel in the pop-up interface of the device. Or click the  icon on the call page to open the contacts and search for the indoor monitor/personnel to call.



• Phone Calling

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.



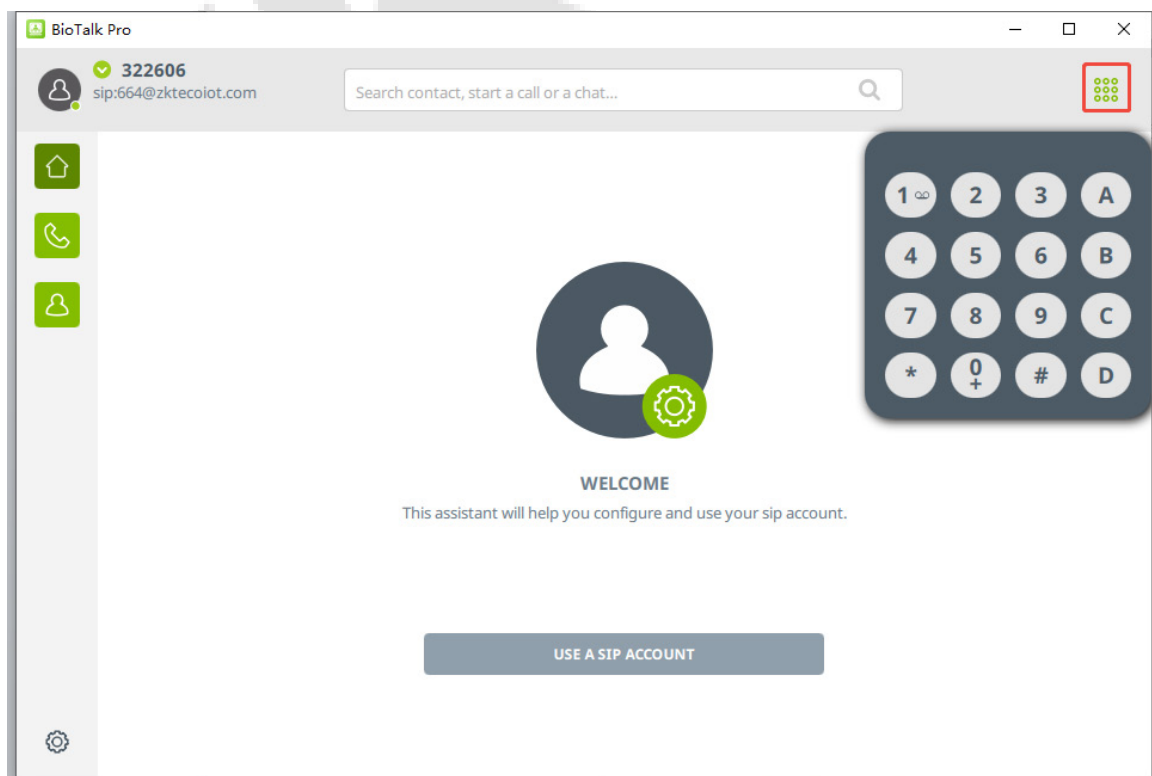
- **Indoor Monitor Calling**

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

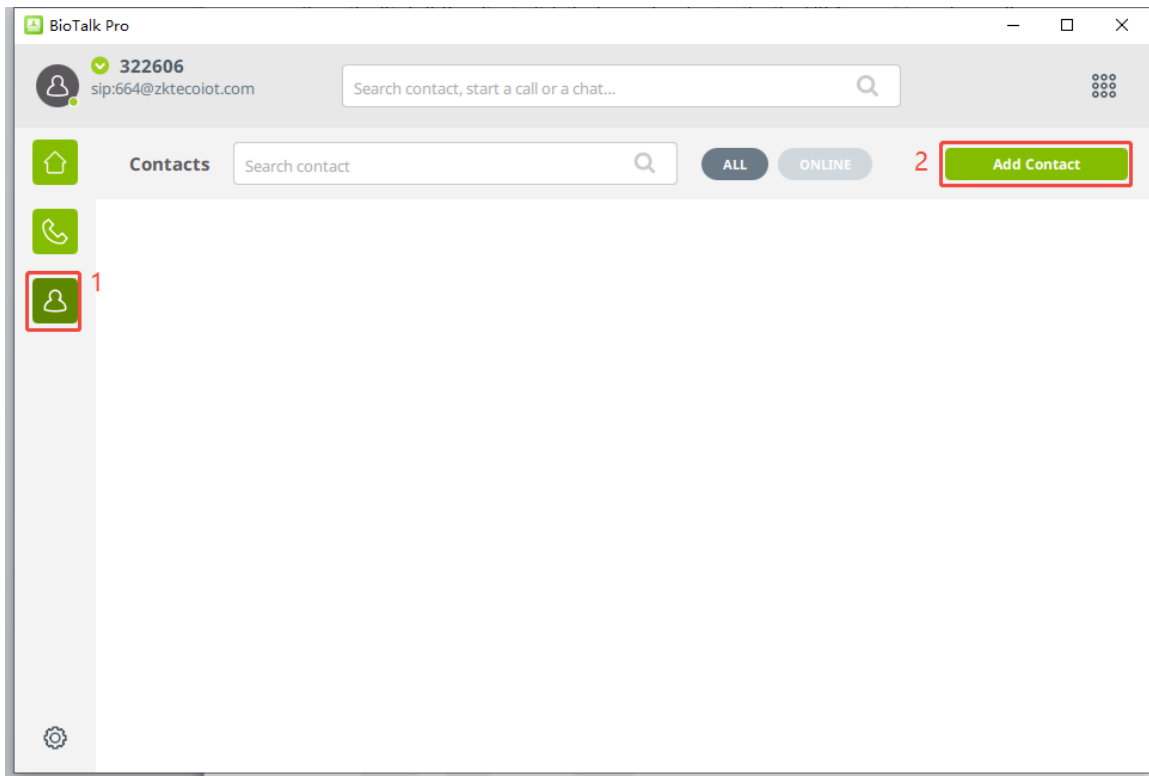
Note: The indoor monitor is not supported the assignment of the contact list in ZKBio CVSecurity.

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

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



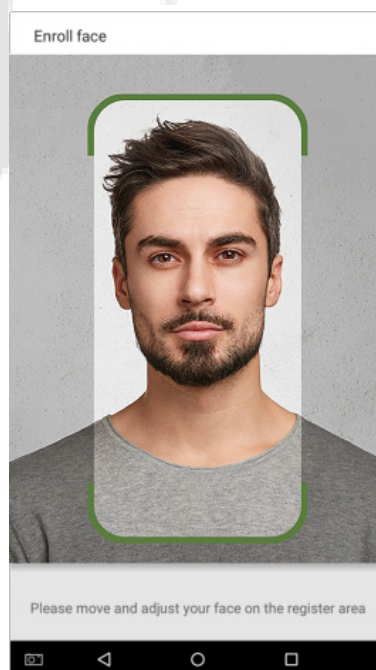
User can click the  icon > **Add Contact** to add the contact list manually.



Appendix 1

Requirements of Live Collection and Registration of Visible Light Face Templates

- 1) It is recommended to perform registration in an indoor environment with proper lighting to avoid 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 to learn more about how we collect, use, and securely store your personal information. To keep pace with the rapid development of technology, adjustment of business operations, and to cope with customer needs, we will constantly deliberate and optimize our privacy protection measures and policies. Welcome to visit our official website at any time to learn our latest privacy policy.

Eco-friendly Operation



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

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

Hazardous or Toxic substances and their quantities

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

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

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

×

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

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



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

Phone : +86 769 - 82109991

Fax : +86 755 - 89602394

www.zkteco.com

