User Manual

SenseFace 2A

Date: August 2025

Doc Version: 1.1

English

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

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

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

Trademark

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

Disclaimer

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

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

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

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

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

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

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

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

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

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

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

ZKTeco Headquarters

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

Phone +86 769 - 82109991

Fax +86 755 - 89602394

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

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

About the Company

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

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

About the Manual

This manual introduces the operations of **SenseFace 2A**.

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

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

Document Conventions

Conventions used in this manual are listed below:

GUI Conventions

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

Symbols

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

Table of Contents

1 Safety Measures

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

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

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

   And do not connect multiple devices to one power adapter as adapter overload can cause over-heat or fire hazard.
7. **Replacement parts** - When replacement parts are required, service technicians must only use replacement parts provided by the supplier. Unauthorized substitutes can result in a burn, shock, or other hazards.
8. **Safety check** - On completion of service or repair work on the unit, ask the service technician to perform safety checks to ensure proper operation of the device.
9. **Power sources** - Operate the system only from the label's power source form. If the sort of power supply to use is unclear, call your dealer.
10. **Lightning** - Can install external lightning conductors to protect against electrical storms. It stops power-ups from destroying the system.

    Recommended installing the devices in areas with limited access.

2 Electrical Safety

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

3 Operation Safety

- If smoke, odour, or noise rise from the device, turn off the power at once and unplug the power cable, and then please contact the service centre.
- Transportation and other unpredictable causes may damage the device hardware. Check whether the device has any intense damage before installation.
- If the device has major defects that you cannot solve, contact your dealer as soon as possible.
- Dust, moisture, and abrupt temperature changes can affect the device's service life. You are advised not to keep the device under such conditions.
- Do not keep the device in a place that vibrates. Handle the device with care. Do not place heavy objects on top of the device.
- Do not apply rosin, alcohol, benzene, pesticides, and other volatile substances that may damage the device enclosure. Clean the device accessories with a piece of soft cloth or a small amount of cleaning agent.
- If you have any technical questions regarding usage, contact certified or experienced technical personnel.

Note:

- Make sure whether the positive polarity and negative polarity of the DC 12V power supply is connected correctly. A reverse connection may damage the device. It is not advisable to connect the AC 24V power supply to the DC 12V input port.
- Make sure to connect the wires following the positive polarity and negative polarity shown on the

device's nameplate.

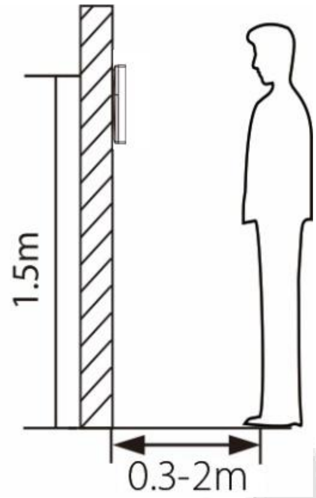
- The warranty service does not cover accidental damage, damage caused by mis-operation, and damage due to independent installation or repair of the product by the user.

4 Instruction for Use

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

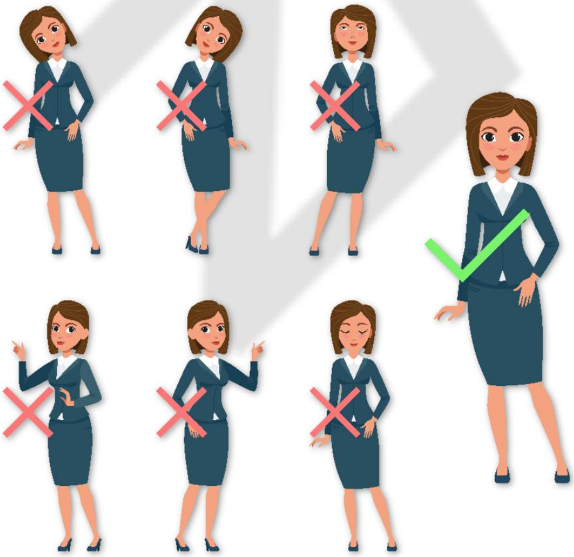
4.1 Standing Position, Posture and Facial Expression

- **The recommended distance**

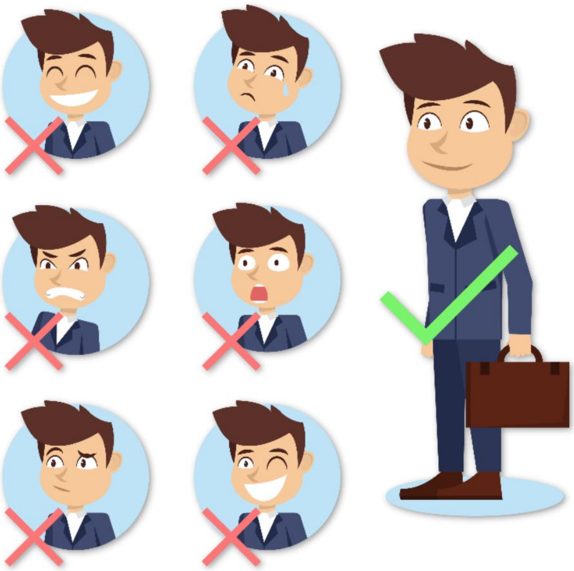


The distance between the device and a user whose height is in a range of 1.55m to 1.85m is recommended to be 0.3 to 2m. Users may slightly move forward or backward to improve the quality of facial images captured.

- **Recommended Standing Posture and Facial Expression**



Standing Posture

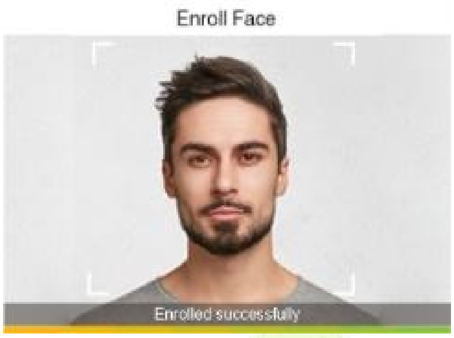


Facial Expression

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

4.2 Face Template Registration

Try to keep the face 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 this:



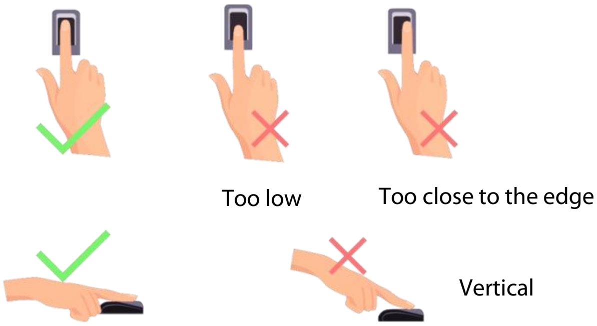
Correct face registration and authentication method

- **Recommendation for registering a face**
  - When registering a face template, maintain a distance of 40cm to 80cm between the device and the face.
  - Be careful not to change your facial expression. (Smiling face, drawn face, 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 faces on the screen. Register one person at a time.
  - It is recommended for a user wearing glasses to register both faces with and without glasses.

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

4.3 Finger Positioning

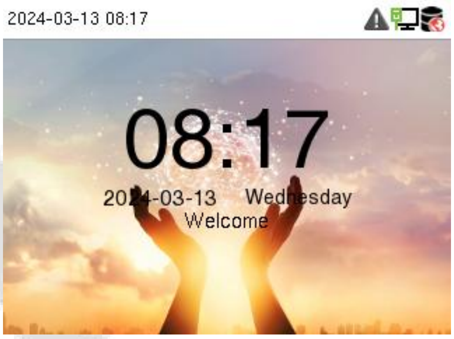
Recommended fingers: The index, middle, or ring finger and avoid using the thumb or pinky fingers, as they are difficult to accurately press onto the fingerprint reader.



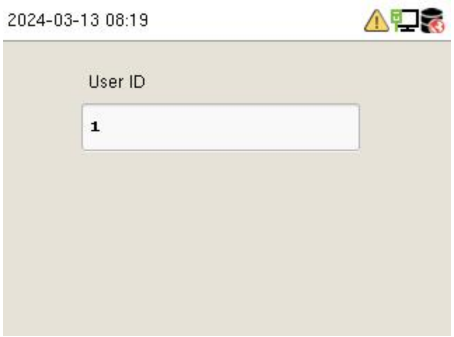
Note: Please use the correct method when pressing your fingers onto the fingerprint reader for registration and identification. Our company will assume no liability for recognition issues that may result from incorrect usage of the product. We reserve the right of final interpretation and modification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

4.4 Standby Interface

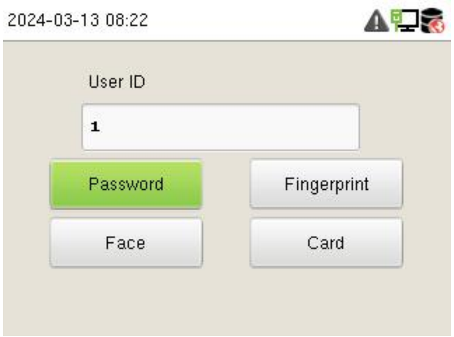
The device uses a 2.4-inch color screen, which all operations are performed through the keypad. After connecting the power supply, the following standby interface is displayed:



- Enter any number to access the User ID input interface.

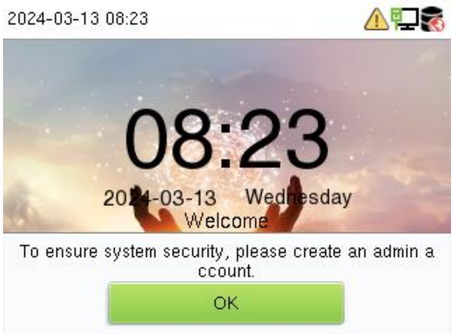

2024-03-13 08:19

User ID: 1


2024-03-13 08:22

User ID: 1

- When there is no Super Administrator set in the device, press **M/OK** to go to the menu.


2024-03-13 08:23

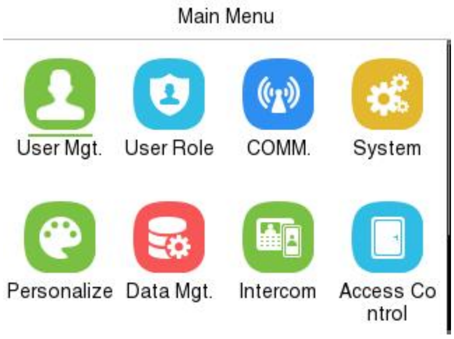
08:23

2024-03-13 Wednesday

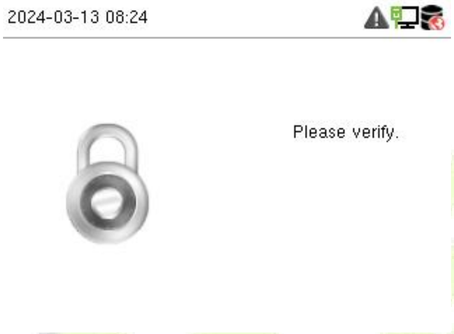
Welcome

To ensure system security, please create an admin a ccount.

OK



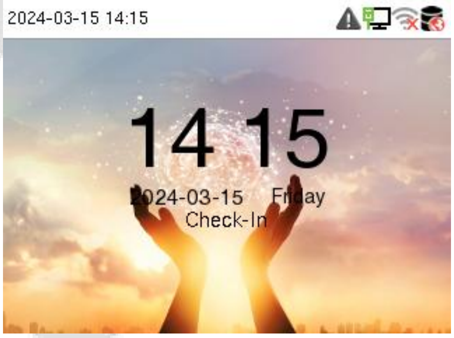
- After adding a Super Administrator on the device, it requires the Super Administrator’s verification before opening the menu functions.

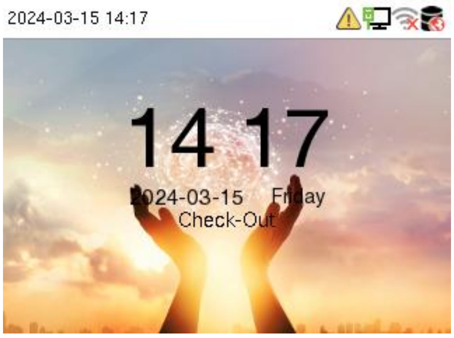

2024-03-13 08:24

Please verify.

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

- On the standby interface, the punch state options can also be shown and used directly. The shortcut key mappings will be displayed on the screen if you press the relevant shortcut key on the keypad, as shown in the picture below. For the specific operation method, please see "Shortcut Key Mappings."





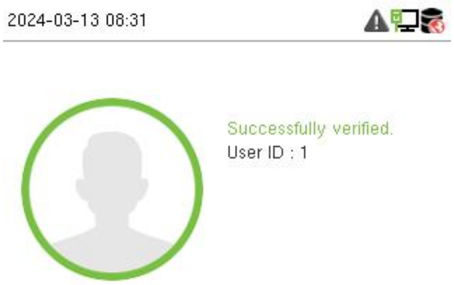
Note: The punch state options are disabled by default when the device type is set as an attendance terminal.

4.5 Verification Mode

4.5.1 Facial Verification

1: N Facial Verification

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



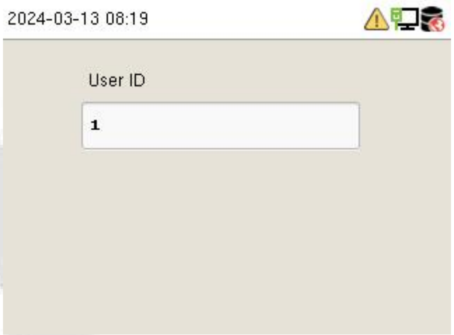
2024-03-13 08:31

Successfully verified.

User ID : 1

1:1 Facial Verification

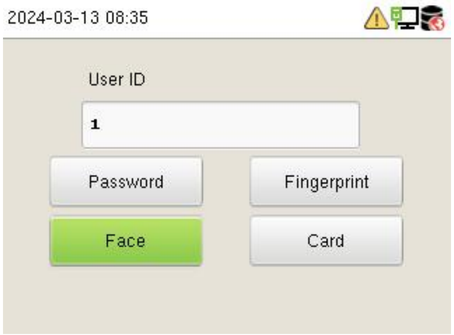
In this verification mode, the device compares the face captured by the camera with the facial template related to the entered user ID. Enter the user ID and press **M/OK** to enter the 1:1 facial verification mode.



2024-03-13 08:19

User ID: 1

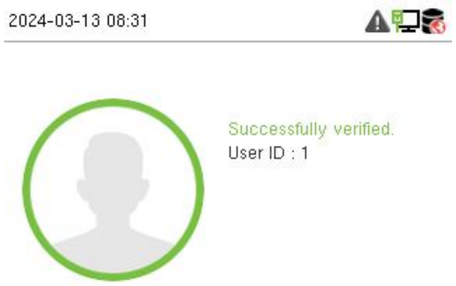
If the user has registered password, card and fingerprint in addition to the face, and the verification method is set to Password/Fingerprint/Card/Face, the following screen will appear. Select **Face** to enter the face verification mode.



2024-03-13 08:35

User ID: 1

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



2024-03-13 08:31

Successfully verified.

User ID : 1

4.5.2 Fingerprint Verification

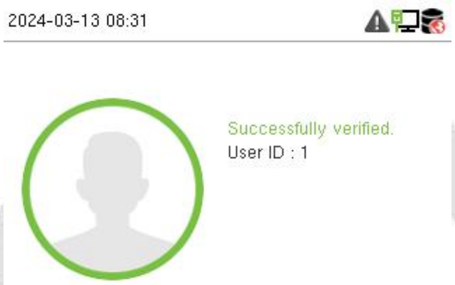
➢ **1: N Fingerprint Verification Mode**

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, refer to section Finger Positioning.

Verification is successful:

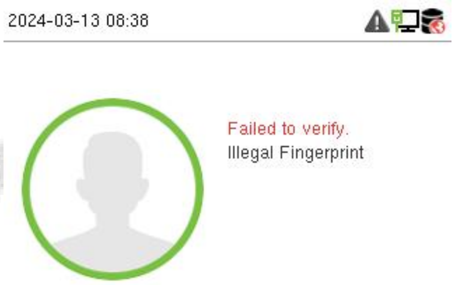


2024-03-13 08:31

Successfully verified.

User ID : 1

Verification is failed:



2024-03-13 08:38

Failed to verify.

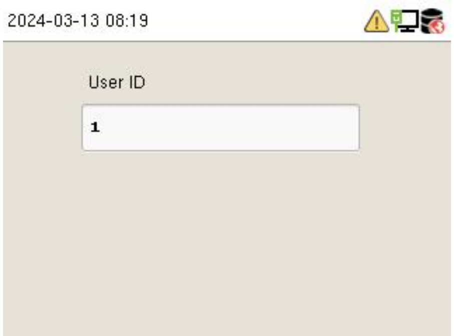
Illegal Fingerprint

➢ **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.

Enter the user ID and press **M/OK** to enter the 1:1 fingerprint verification mode.

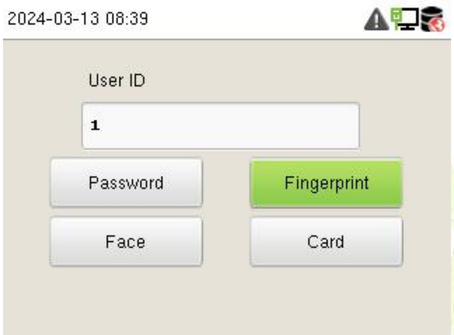


2024-03-13 08:19

User ID

1

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



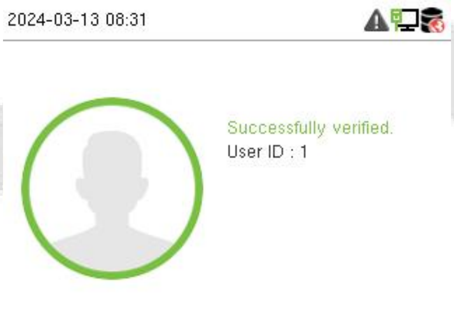
2024-03-13 08:39

User ID

1

Press the fingerprint to verify.

Verification is successful:

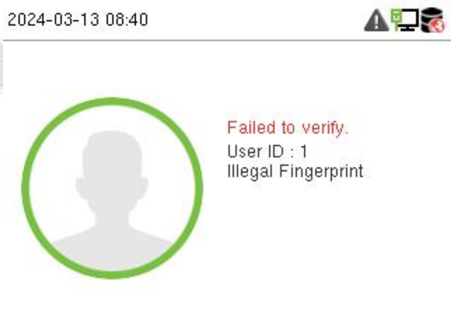


2024-03-13 08:31

Successfully verified.

User ID : 1

Verification is failed:



2024-03-13 08:40

Failed to verify.

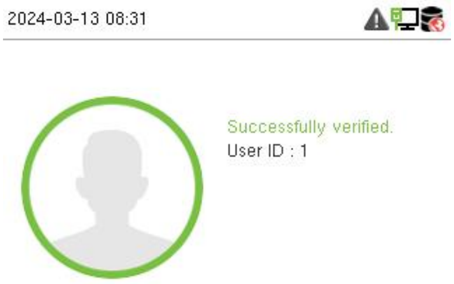
User ID : 1

Illegal Fingerprint

4.5.3 Card Verification

- **1: N Card Verification Mode**

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 screen.

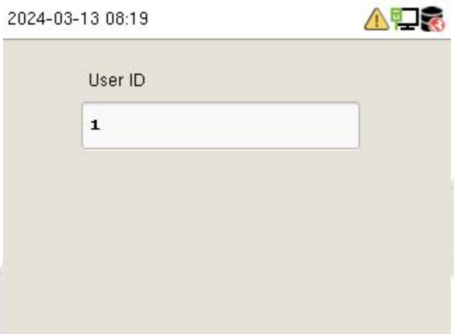

2024-03-13 08:31

Successfully verified.
User ID : 1

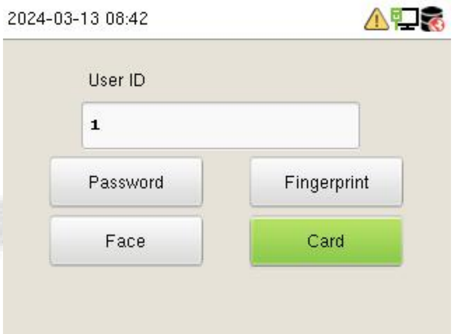
- **1:1 Card Verification Mode**

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.

Enter the user ID and press **M/OK** to enter the 1:1 card verification mode.

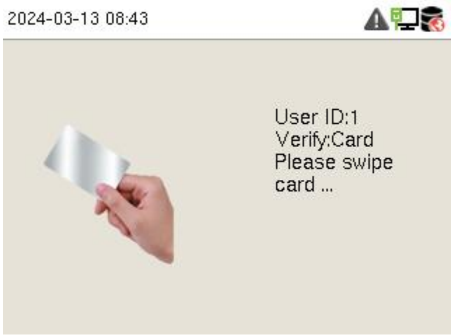

2024-03-13 08:19

User ID
1

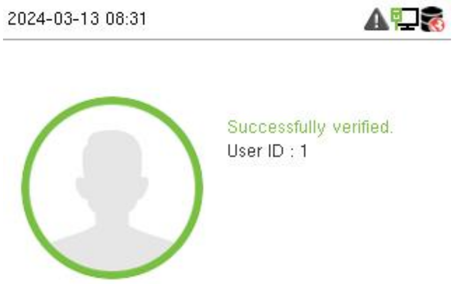

2024-03-13 08:42

User ID
1

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


2024-03-13 08:43

User ID:1
Verify:Card
Please swipe card ...

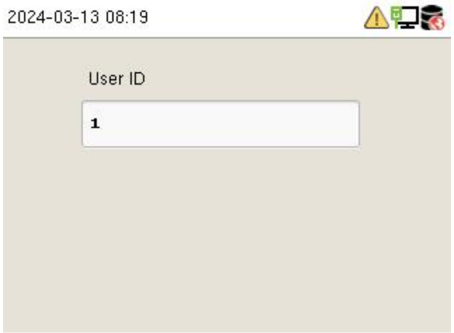

2024-03-13 08:31

Successfully verified.
User ID : 1

4.5.4 Password Verification

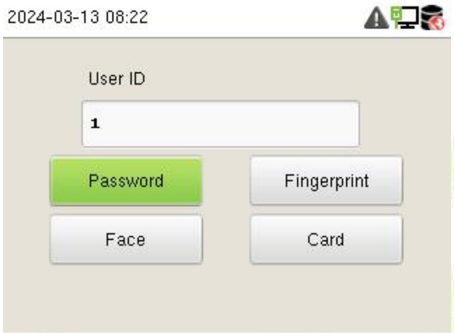
The device compares the entered password with the registered password and User ID.

Enter the user ID and press **M/OK** to enter the 1:1 password verification mode. Then, input the user ID and press **M/OK**.


2024-03-13 08:19

User ID

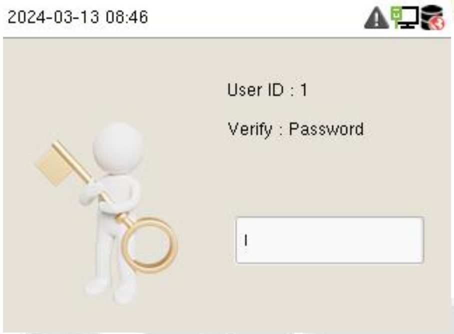
1


2024-03-13 08:22

User ID

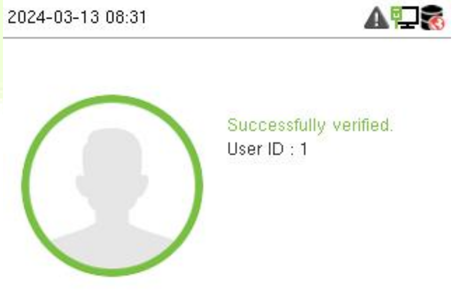
1

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


2024-03-13 08:46

User ID : 1

Verify : Password


2024-03-13 08:31

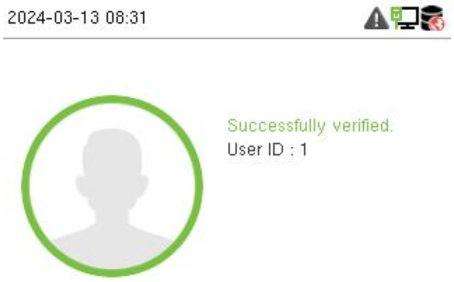
Successfully verified.

User ID : 1

Below are the display screens after entering a correct password and a wrong password, respectively.

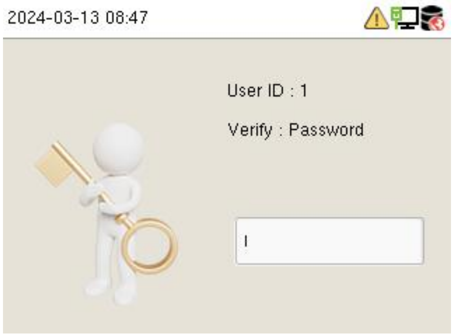
Verification is successful:

Verification is failed:


2024-03-13 08:31

Successfully verified.

User ID : 1


2024-03-13 08:47

User ID : 1

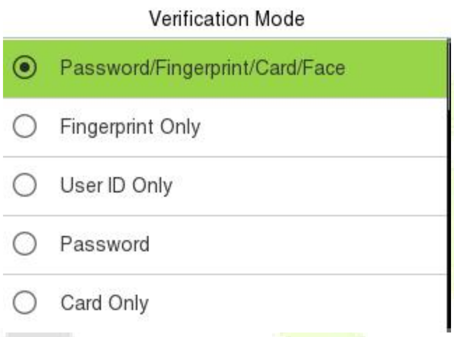
Verify : Password

4.5.5 Combined Verification

This device allows you to use different types of verification methods to increase security. There are a total of 21 different verification combinations that can be implemented, as listed below:

Combined Verification Symbol Definition

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


Verification Mode

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

Combined Verification Mode set up procedure:

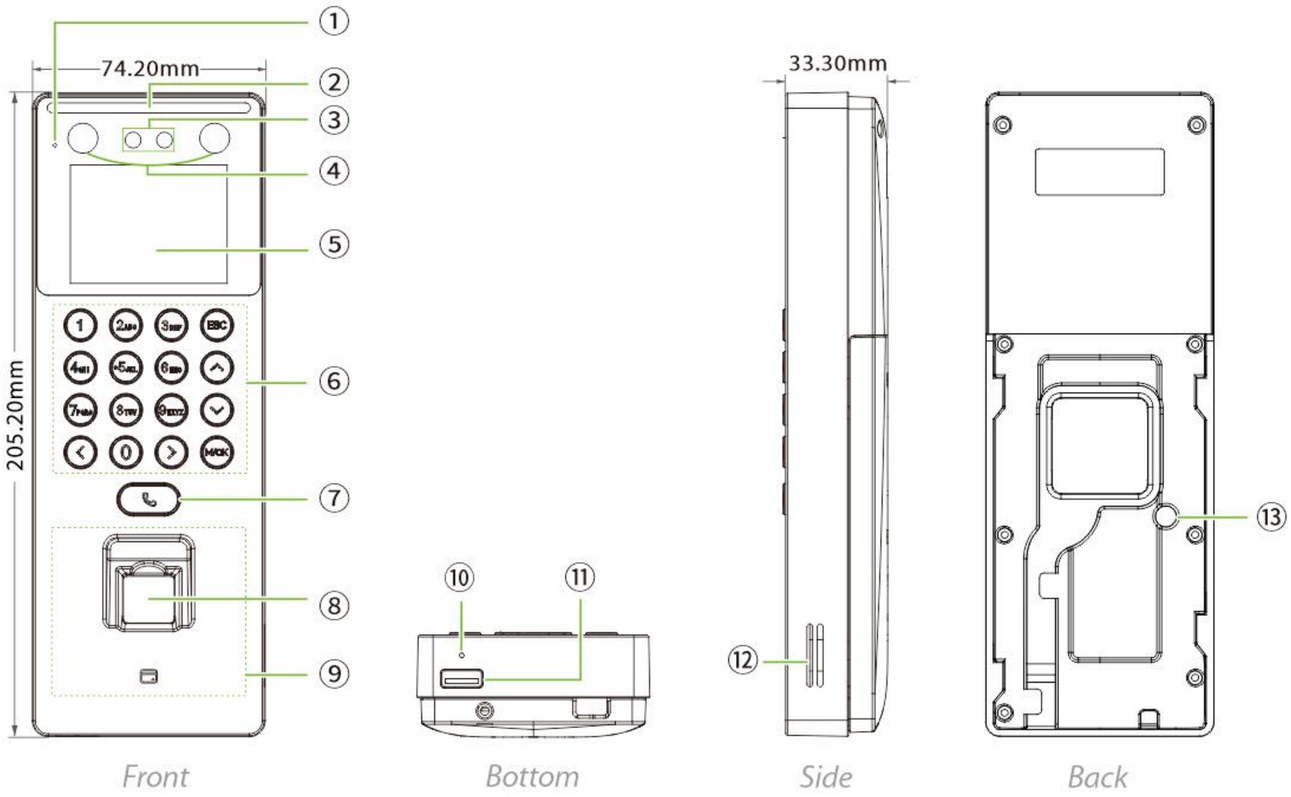
- Combined verification requires personnel to register all the different verification methods. Otherwise, employees will not be able to successfully verify the combined verification process.
- For example, if an employee has only registered for password data but the Device verification mode is set to "Password + Card," the employee will not be able to successfully complete the verification procedure.

Reason:

- This is because the Device compares the password template of the person with the registered verification template (both the Card and the Password) previously stored to that Personnel ID in the Device.
- But, since the employee has only registered their password and not their card, the verification process will not be successful, and the device will display the "Verification Failed."

5 Overview

5.1 Appearance

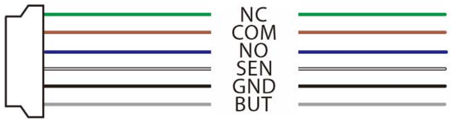
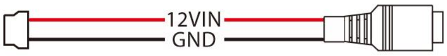
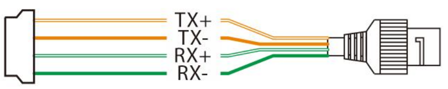


No.	Description
1	Microphone
2	Flash
3	Camera
4	Near-infrared Flash
5	2.4-inch Color Screen
6	Keypad
7	Doorbell Button
8	Fingerprint Sensor
9	Card Reading Area
10	Reset

11	USB
12	Speaker
13	Tamper Switch

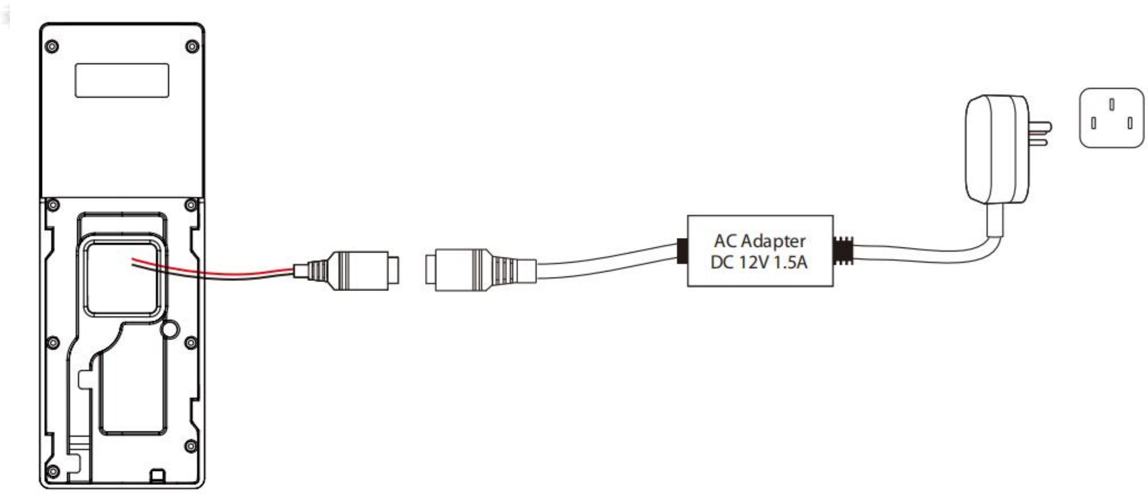
5.2 Terminal and Wiring Description

5.2.1 Terminal Description

Interface	Description	
	NC	Lock
	COM	
	NO	
	SEN	Door Sensor & Exit Button
	GND	
	BUT	
	12V Power in	
	Network Interface	

5.3 Wiring Description

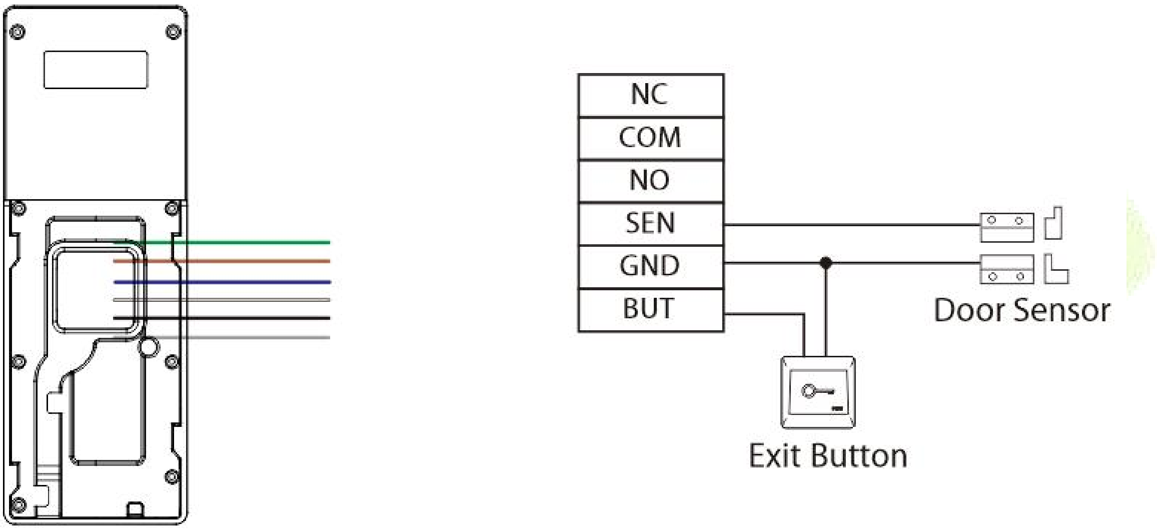
5.3.1 Power Connection



Recommended power supply

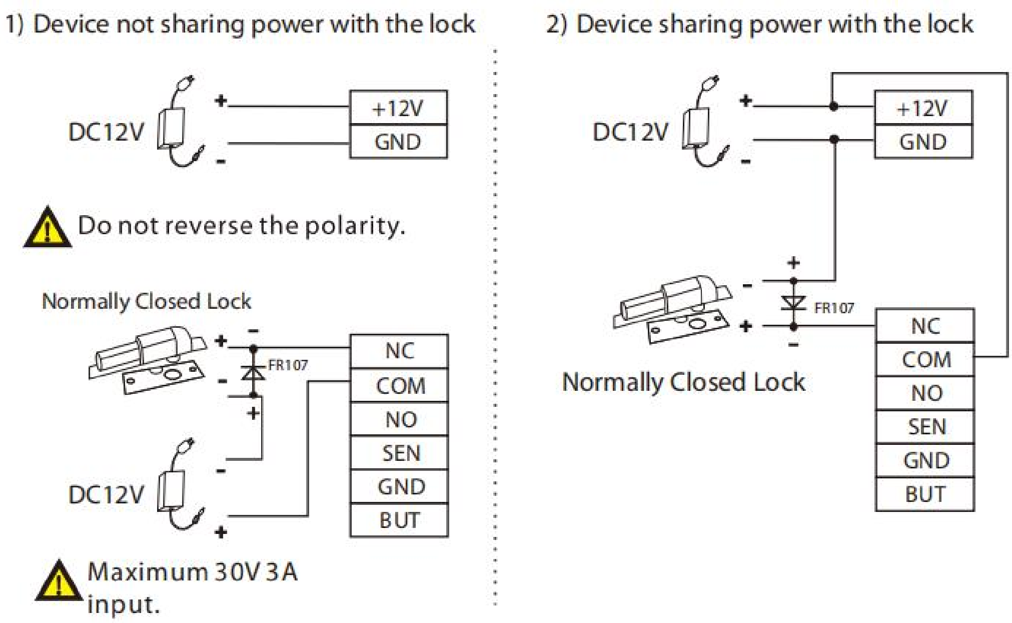
- Rating of 12V and 1.5A.
- To share the device's power with other devices, use a power supply with higher current ratings.

5.3.2 Door Sensor & Exit Button Connection



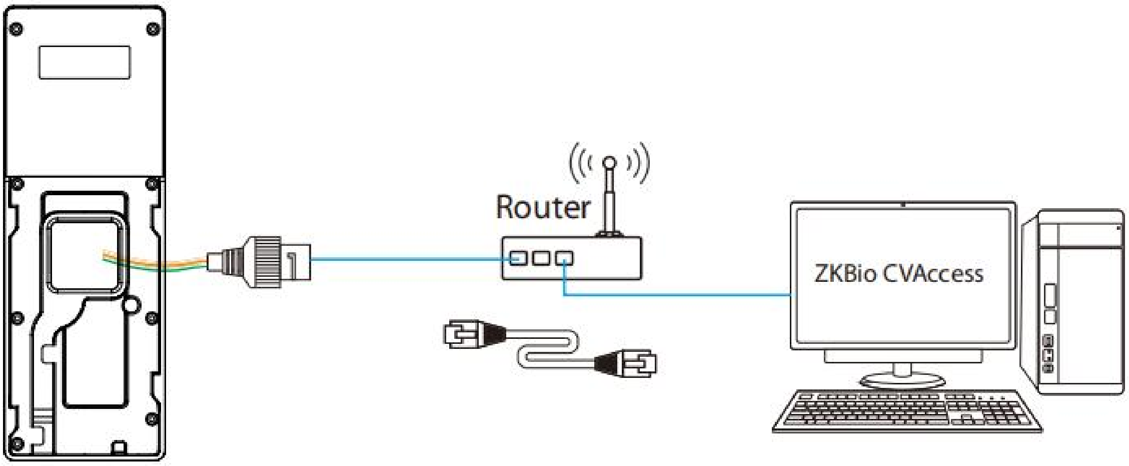
5.3.3 Lock Relay Connection

The system supports both Normally Opened Lock and Normally Closed Lock. The NO Lock (normally opened when powered) is connected with 'NO1' and 'COM1' terminals, and the NC Lock (normally closed when powered) is connected with 'NC1' and 'COM1' terminals. The power can be shared with the lock or can be used separately for the lock, as shown in the example with NC Lock below:



5.3.4 Ethernet Connection

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



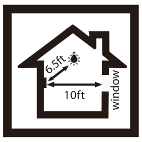
Enter **[COMM.] > [Ethernet]** to set the relevant parameters of network.

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

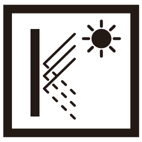
6 Installation

6.1 Installation Environment

Please refer to the following recommendations for installation.



KEEP DISTANCE



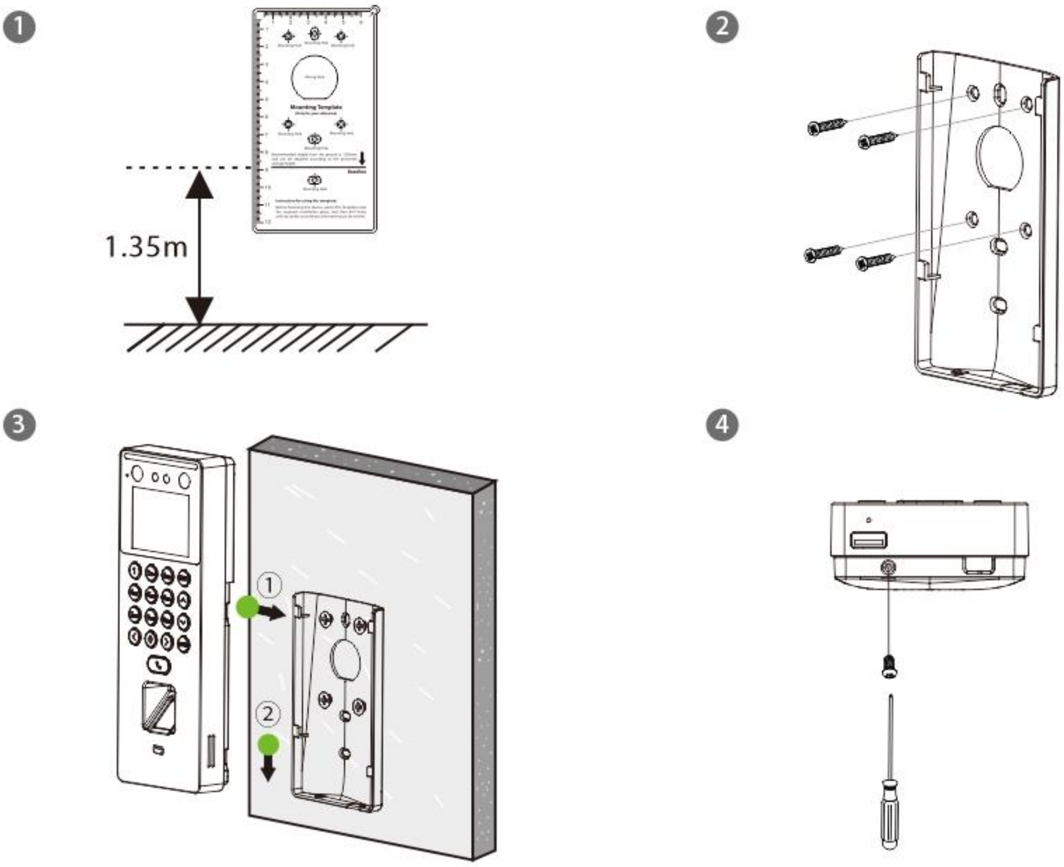
AVOID GLASS REFRACTION

AVOID DIRECT SUNLIGHT AND EXPOSURE

AVOID USE OF ANY HEAT SOURCE NEAR THE DEVICE

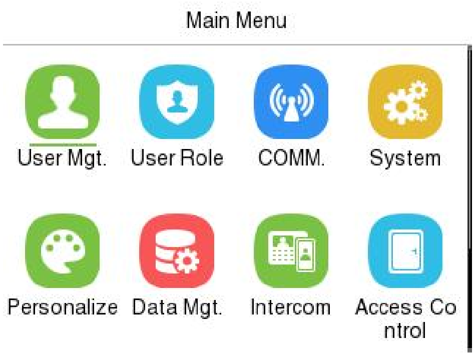
6.2 Device Installation

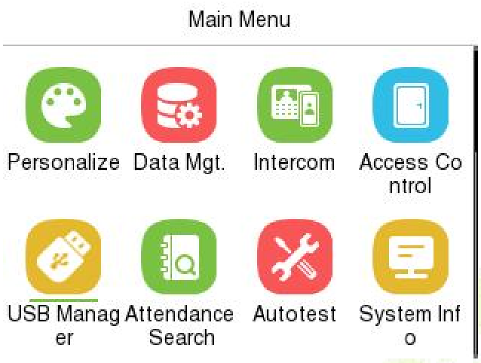
1. Stick the mounting template sticker to the wall and drill holes according to the mounting template sticker.
2. Fix the backplate on the wall using wall mounting screws.
3. Attach the device to the backplate.
4. Attach the device to the backplate with a security screw.



7 Main Menu

Press **M/OK** on the initial interface to enter the main menu, as shown below:





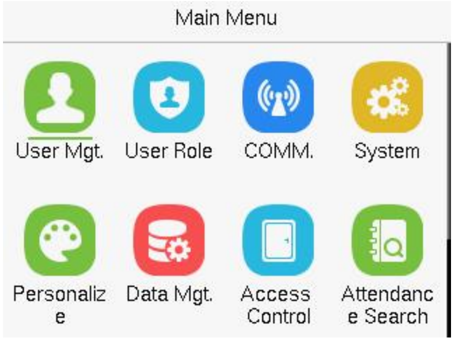
Function Description

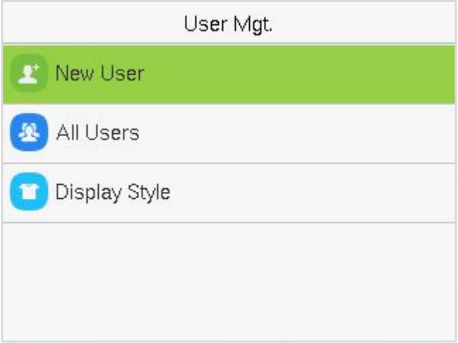
Menu	Description
User Mgt.	To Add, Edit, View, and Delete information of a User.
User Role	To set the permission scope of the custom role and enroller for the users, for example the system's operating rights.
COMM.	To set the relevant parameters of Network, PC Connection, Wi-Fi★, Cloud Server and Network Diagnosis.
System	To set parameters related to the system, including Date Time, Attendance/Access Logs Settings, Face, Fingerprint, Device Type Settings, Security Settings, USB Upgrade, Update Firmware Online and Resetting to factory settings.
Personalize	To customize settings of User Interface, Voice, Bell Schedules, Punch State Options and Shortcut Key Mappings settings.
Data Mgt.	To delete the data.
Intercom	To set relevant parameters of intercom, including SIP, Doorbell and ONVIF Settings.
Access Control	To set the parameters of the lock and the relevant access control device including options like Time rule, Holiday Settings, Combine verification and Duress Option Settings.
USB Manager	To upload or download the specific data by a USB drive.
Attendance Search	To query the specified event logs, check Attendance Photos and Blocklist attendance photos.
Autotest	To automatically test whether each module functions properly, including the LCD Screen, Audio, Microphone, Keyboard, fingerprint sensor, camera and Real-Time Clock.
System Info	To view Privacy Policy, Data Capacity and Device and Firmware information of the current device.

8 User Management

8.1 New User Registration

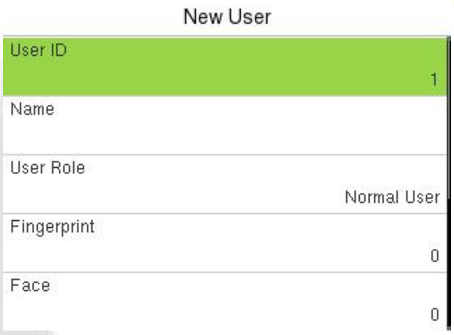
When the device is on the initial interface, press **M/OK** and enter [**User Mgt.**] > [**New User**].





8.1.1 Register a User ID and Name

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



New User

User ID: 1

Name:

User Role: Normal User

Fingerprint: 0

Face: 0

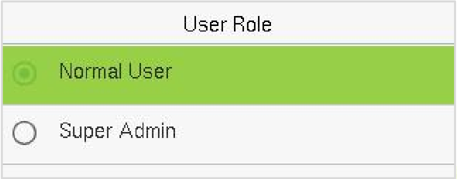
Note:

1. A name can be taken up to 36 characters long.
2. The user ID may contain 1 to 14 digits by default, supporting both numbers and alphabetic characters.
3. During the initial registration, you can modify your ID, but not after registration.
4. If the message "**Duplicated!**" appears, you must choose a different User ID because the one you entered already exists.

8.1.2 User Role

On the **New User** interface, select **User Role** to set the user's role as either **Normal User** or **Super Admin**.

- **Super Admin:** The Super Administrator owns all management privileges in the Device.
- **Normal User:** If the Super Admin is registered already in the device, then the Normal Users will not have the privilege to manage the system and can only access authentic verifications.
- **User Defined Roles:** The Normal User can also be assigned custom roles with User Defined Role. The user can be permitted to access several menu options as required.



User Role

● Normal User

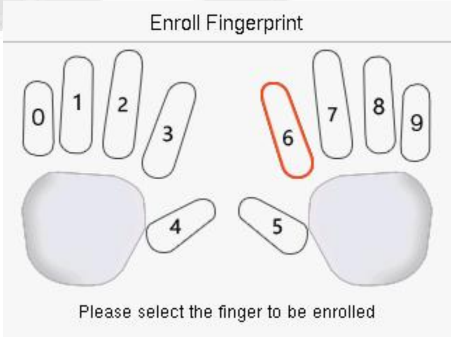
○ Super Admin

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

8.1.3 Register Fingerprint

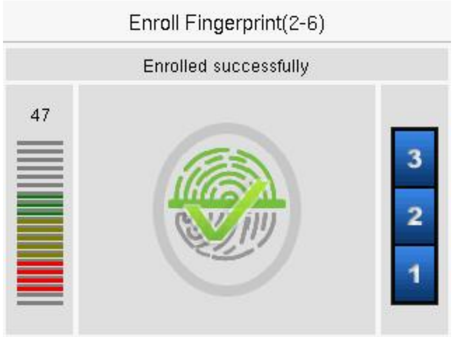
Select **Fingerprint** in the **New User** interface to enter the fingerprint registration page.

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



Enroll Fingerprint

Please select the finger to be enrolled



Enroll Fingerprint(2-6)

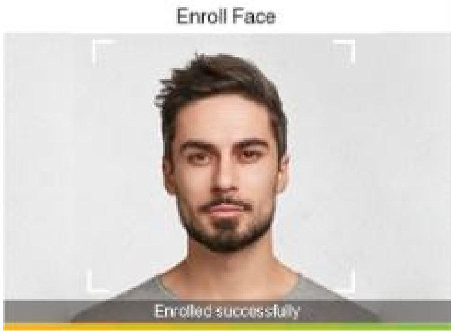
Enrolled successfully

8.1.4 Register Face

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

- Please face towards the camera and place yourself in such a way that your face image fits inside the white guiding box and stays still during face registration.

- A progress bar shows up while registering the face and then "**Enrolled Successfully**" message is displayed as the progress bar completes.
- If the face is registered already then, the "**Duplicated Face**" message shows up. The registration interface is as follows:

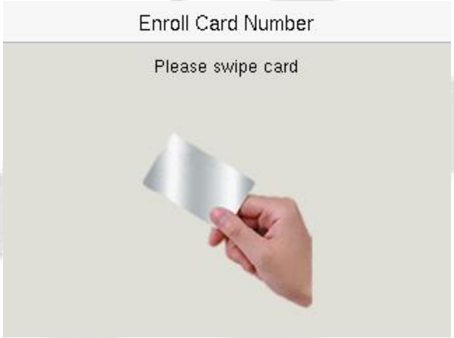

Enroll Face

Enrolled successfully

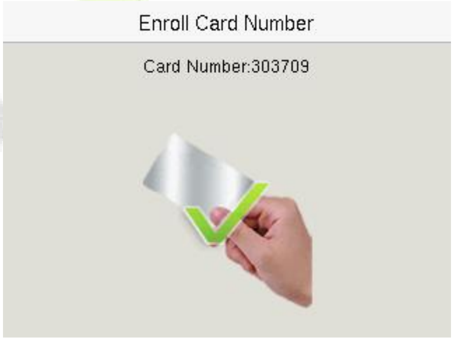
8.1.5 Card

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

- On the card interface, swipe the card under the card reading area. The registration of the card will be successful.
- If the card has already been registered, the message "**Error! Card already enrolled**" appears. The registration interface appears as follows:


Enroll Card Number

Please swipe card

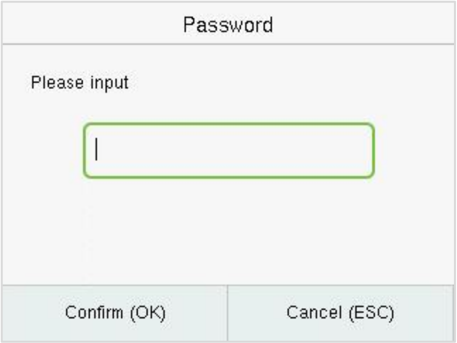

Enroll Card Number

Card Number:303709

8.1.6 Password

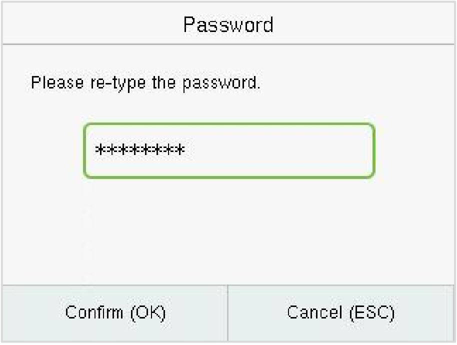
Select **Password** in the **New User** interface to enter the password registration page.

- On the Password interface, enter the required password and re-enter to confirm it and press **M/OK**.
- If the re-entered password is different from the initially entered password, then the device prompts the message as "**Password not match!**", where the user needs to re-confirm the password again.
- The password may contain 6 to 8 digits by default.



Password

Please input



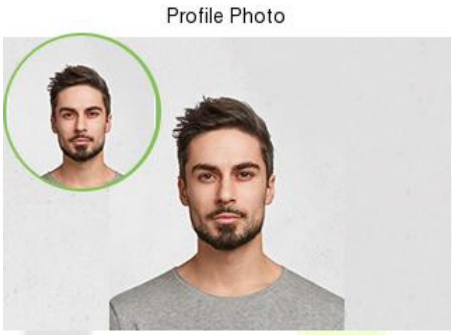
Password

Please re-type the password.

****

8.1.7 Profile Photo

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



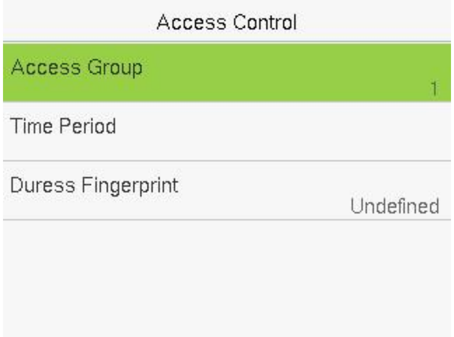
- Tap **Profile Photo**, the device's camera will open, then press **M/OK** to take a photo. The captured photo is displayed on the top left corner of the screen.

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

8.1.8 Access Control Role

The **Access Control Role** sets the door access privilege for each user. It includes the access group, time period and duress fingerprint.

- Enter [**Access Control Role**] > [**Access Group**] to assign the registered users to different groups for better management. New users belong to Group 1 by default and can be reassigned to other groups. The device supports up to 99 Access Control groups.
- Tap **Time Period**, to select the time to use.
- The user may specify one or more fingerprints that have been registered as a duress fingerprint(s). When press the finger corresponding to the duress fingerprint on the sensor and pass the verification, the system will immediately generate a duress alarm.



Access Control

Access Group 1

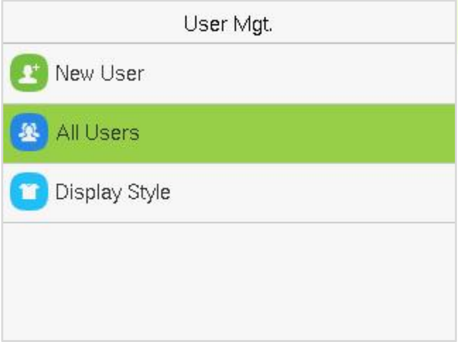
Time Period

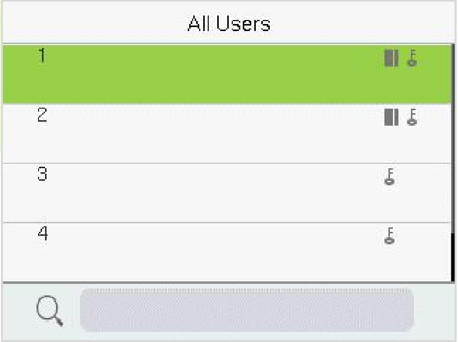
Duress Fingerprint Undefined

8.2 All Users

When the device is on the initial interface, press **M/OK** and enter [**User Mgt.**] >[**All Users**].

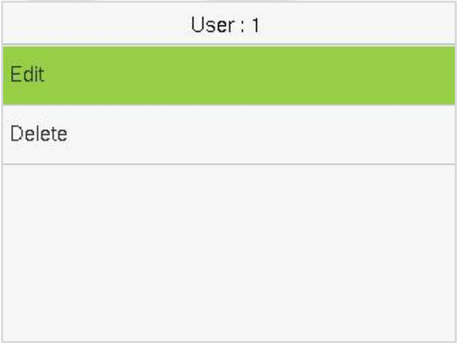
- On the **All Users** interface, tap on the search bar on the user's list to enter the required retrieval keyword (where the keyword may be the user ID, surname, or full name) and the system will search for the related user information.

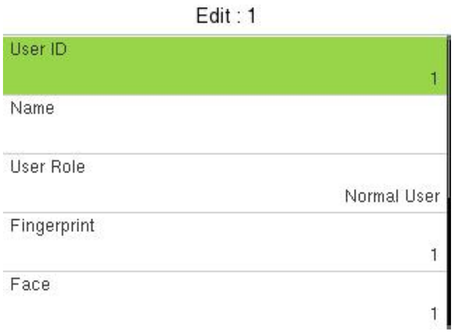




8.2.1 Edit User

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





Edit : 1

User ID 1

Name

User Role Normal User

Fingerprint 1

Face 1

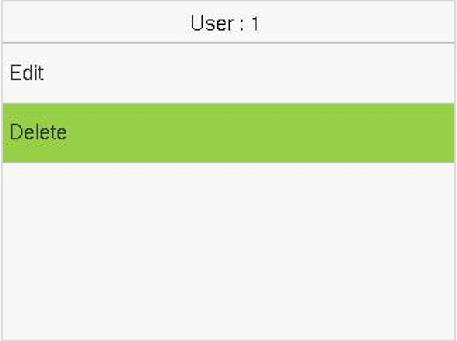
Note: The process of editing the user information is the same as adding a new user, except that the User ID cannot be modified while editing a user. The process in detail refers to "User Registration".

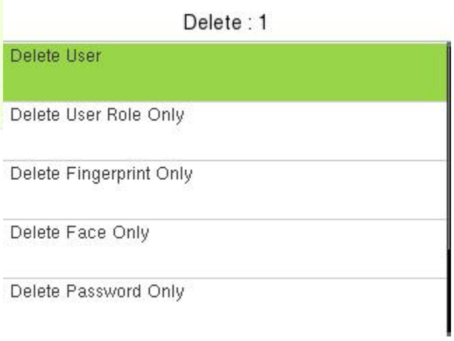
8.2.2 Delete User

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

Delete Operations:

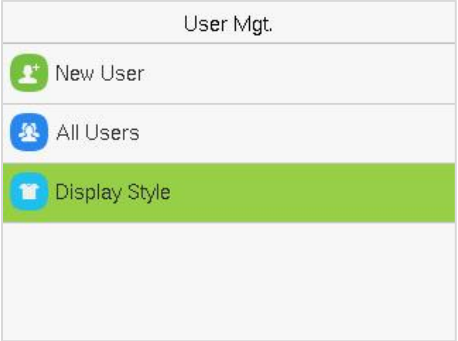
- **Delete User:** Deletes all the user information (deletes the selected User as a whole) from the Device.
- **Delete User Role Only:** Deletes the user's administrator privileges and make the user a normal user.
- **Delete Fingerprint Only:** Deletes the fingerprint information of the selected user.
- **Delete Face Only:** Deletes the face information of the selected user.
- **Delete Password Only:** Deletes the password information of the selected user.
- **Delete Card Number Only:** Deletes the card information of the selected user.
- **Delete Profile Photo Only:** Deletes the profile photo of the selected user.

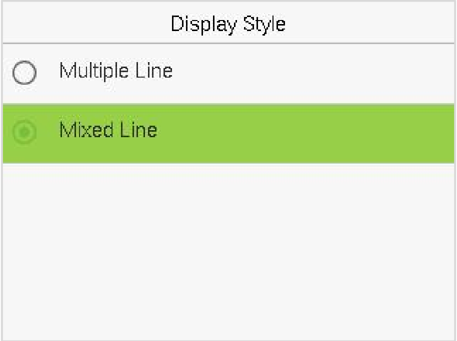




8.3 Display Style

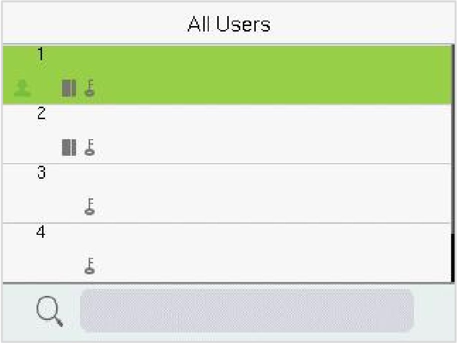
When the device is on the initial interface, press **M/OK** and enter [**User Mgt.**] > [**Display Style**].





All the Display Styles are shown as below:

Multiple Line:



All Users

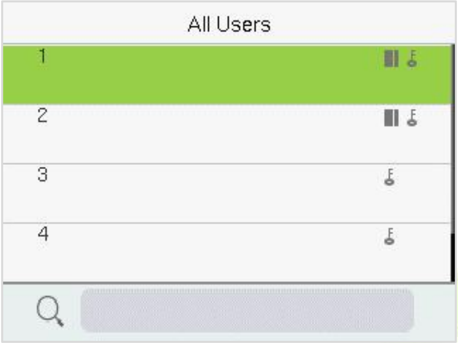
1

2

3

4

Mixed Line:



All Users

1

2

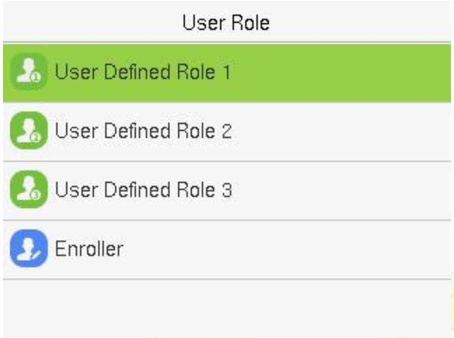
3

4

9 User Role

User Role allows you to assign specific permissions to certain users based on their requirements.

- When the device is on the initial interface, press **M/OK** and enter [**User Role**] > [**User Defined Role**] to set the user defined permissions.
- The permission scope of the custom role can be set up into 3 roles, that is, the custom operating scope of the menu functions of the user.



User Role

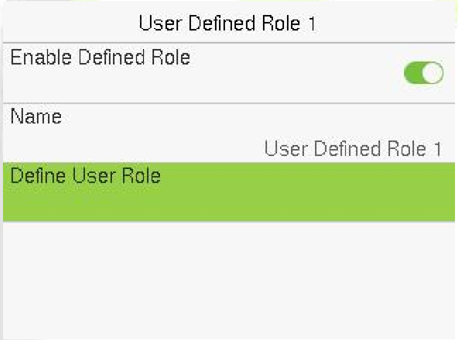
User Defined Role 1

User Defined Role 2

User Defined Role 3

Enroller

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



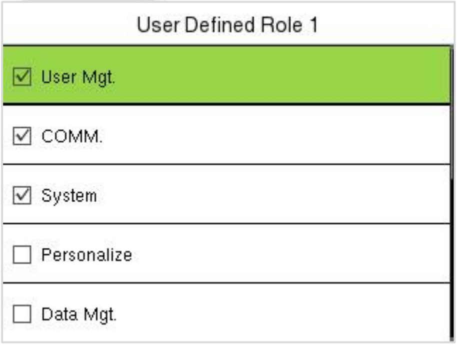
User Defined Role 1

Enable Defined Role ●

Name: User Defined Role 1

Define User Role

- Then, by selecting on Define User Role, select the required privileges for the new role, and then press the **M/OK** key.
- First tap on the required **Main Menu** function name, then press **M/OK** and select its required sub-menus from the list.



User Defined Role 1

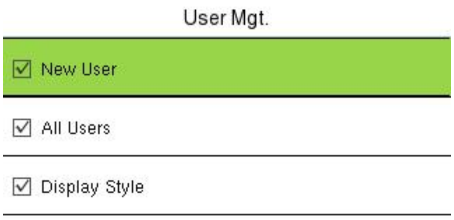
☑ User Mgt.

☑ COMM.

☑ System

☐ Personalize

☐ Data Mgt.



User Mgt.

☑ New User

☑ All Users

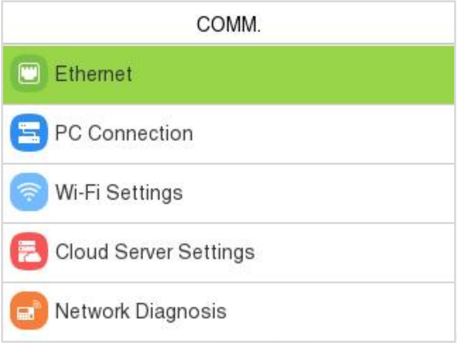
☑ Display Style

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

10 Communication

Communication Settings are used to set the parameters of the Network, PC Connection, Wi-Fi★, Cloud Server, and Network Diagnosis.

When the device is on the initial interface, press **M/OK** and select **COMM.**



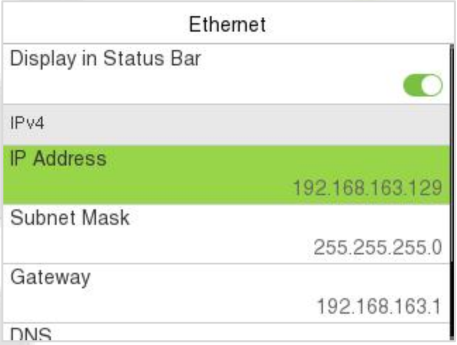
COMM.

- Ethernet
- PC Connection
- Wi-Fi Settings
- Cloud Server Settings
- Network Diagnosis

10.1 Ethernet

When the device needs to communicate with a PC via the Ethernet, you need to configure network settings and make sure that the device and the PC connecting to the same network segment.

Select **Ethernet** on the **COMM.** Settings interface to configure the settings.



Ethernet

Display in Status Bar

IPv4

IP Address 192.168.163.129

Subnet Mask 255.255.255.0

Gateway 192.168.163.1

DNS

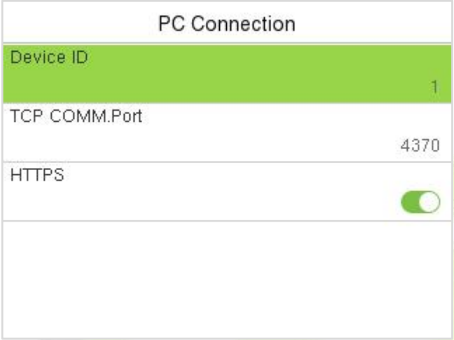
Function Description:

Function Name	Description
Display in Status Bar	Toggle to set whether to display the network icon on the status bar.
IP Address	The default IP address is 192.168.1.201. It can be modified according to the network availability.
Subnet Mask	The default Subnet Mask is 255.255.255.0. It can be modified according to the network availability.

Gateway	The Default Gateway address is 0.0.0.0. It can be modified according to the network availability.
DNS	The default DNS address is 0.0.0.0. It can be modified according to the network availability.
DHCP	Dynamic Host Configuration Protocol dynamically allocates IP address for clients via server.

10.2 PC Connection

Select **PC Connection** on the **COMM.** Settings interface to configure the communication settings.



PC Connection

Device ID: 1

TCP COMM.Port: 4370

HTTPS

Function Description

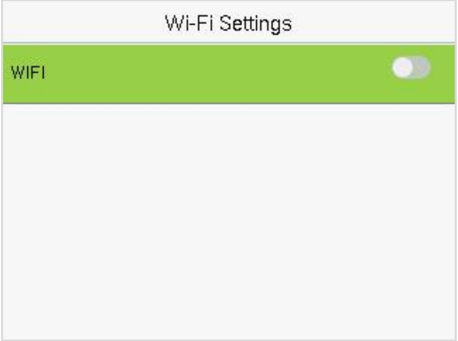
Function Name	Description
Device ID	It is the identification number of the device, which ranges between 1 and 254.
TCP COMM. Port	The factory default value is 4370. Please set the value as per the requirements.
HTTPS	To increase the security of software access, users can enable the HTTPS protocol to create a secure and encrypted network transmission and assure the security of sent data through identity authentication and encrypted communication. This function is enabled by default. This function can be enabled or disabled through the menu interface, and when changing the HTTPS status, the device will pop up a security prompt, and restart after confirmation.

10.3 Wi-Fi Settings★

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

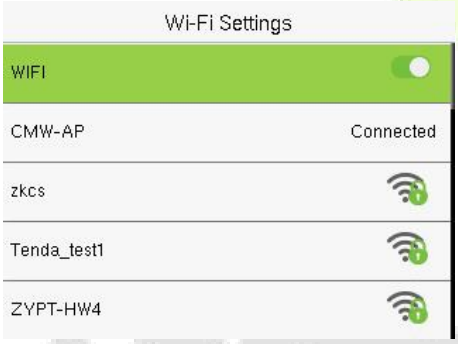
The Wi-Fi module enables data transmission via Wi-Fi (Wireless Fidelity) and establishes a wireless network environment. Wi-Fi is enabled by default in the device. If you don't need to use the Wi-Fi network, you can toggle the Wi-Fi to disable the button.

Select **Wi-Fi Settings** on the **COMM.** Settings interface to configure the Wi-Fi settings.



➢ Searching the Wi-Fi Network

- Wi-Fi is enabled in the device by default. Toggle the button to enable or disable Wi-Fi.
- Once the Wi-Fi is turned on, the device will search for the available Wi-Fi within the network range.
- Tap on the required Wi-Fi name from the available list and input the correct password in the password interface, and then press **M/OK**.

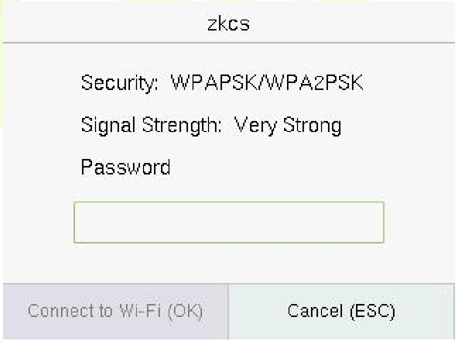


CMW-AP Connected

zkcs

Tenda_test1

ZYPT-HW4



Security: WPAPSK/WPA2PSK

Signal Strength: Very Strong

Password

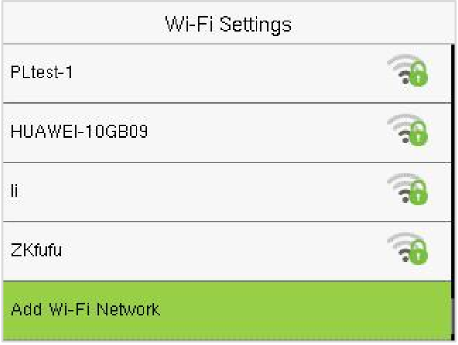
WIFI Enabled: Tap on the required network from the searched network list.

Tap on the password field to enter the password and press **M/OK.**

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

➢ Adding Wi-Fi Network Manually

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

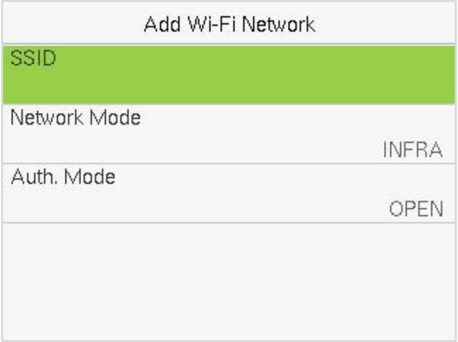


PLtest-1

HUAWEI-10GB09

li

ZKfufu



SSID

Network Mode INFRA

Auth. Mode OPEN

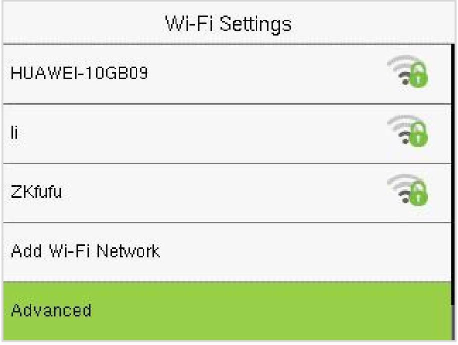
Tap on **Add Wi-Fi Network** to add the Wi-Fi manually.

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

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

➢ Advanced Setting

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



Wi-Fi Settings

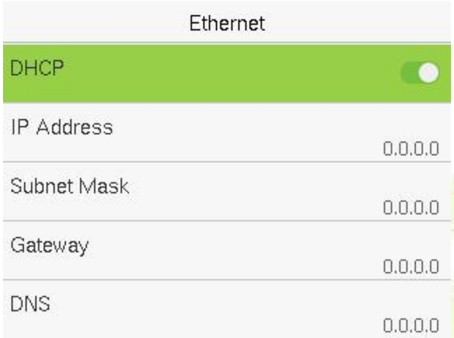
HUAWEI-10GB09

li

ZKfufu

Add Wi-Fi Network

Advanced



Ethernet

DHCP

IP Address 0.0.0.0

Subnet Mask 0.0.0.0

Gateway 0.0.0.0

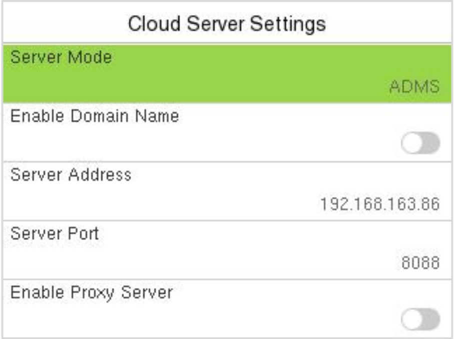
DNS 0.0.0.0

Function Description

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

10.4 Cloud Server Settings

Select **Cloud Server Settings** on the **COMM.** Settings interface to connect with the ADMS server.



Cloud Server Settings

Server Mode ADMS

Enable Domain Name

Server Address 192.168.163.86

Server Port 8088

Enable Proxy Server

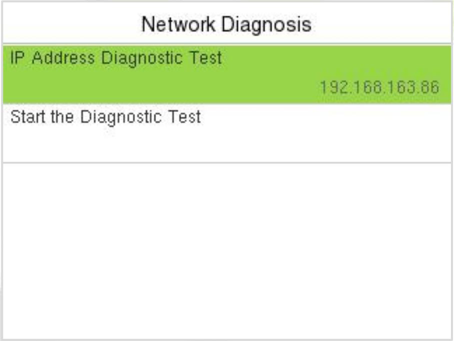
Function Description

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

10.5 Network Diagnosis

It helps to set the network diagnosis parameters.

Select **Network Diagnosis** on the **COMM.** Settings interface. Enter the IP address that needs to be diagnosed and tap **Start the Diagnostic Test** to check whether the network can connect to the device.



Network Diagnosis

IP Address Diagnostic Test
192.168.163.66

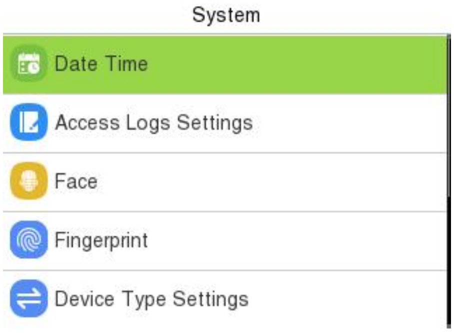
Start the Diagnostic Test

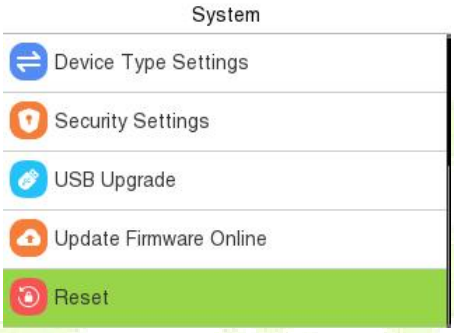
11 System Settings

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

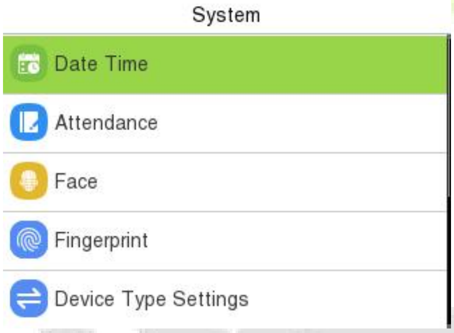
When the device is on the initial interface, press **M/OK** and select **System.**

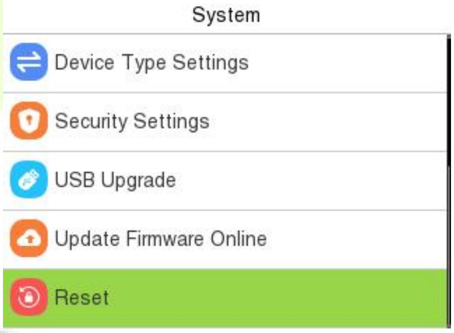
Access Control Terminal:





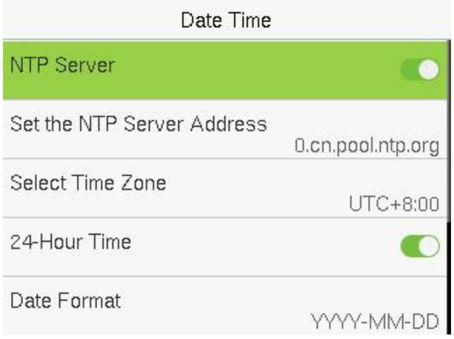
Time Attendance Terminal:





11.1 Date and Time

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



Date Time

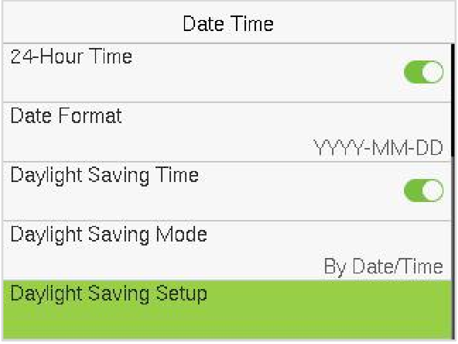
NTP Server

Set the NTP Server Address 0.cn.pool.ntp.org

Select Time Zone UTC+8:00

24-Hour Time

Date Format YYYY-MM-DD



Date Time

24-Hour Time

Date Format YYYY-MM-DD

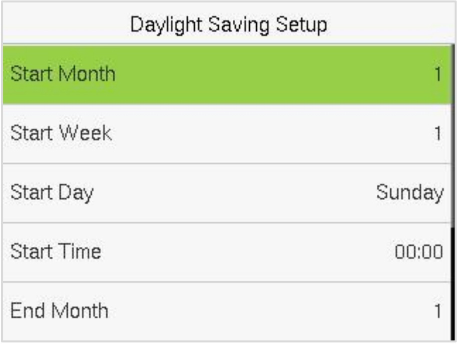
Daylight Saving Time

Daylight Saving Mode By Date/Time

Daylight Saving Setup

- Tap **NTP Server** to enable automatic time synchronization based on the service address you enter.
- Tap **Manual Date and Time** to manually set the date and time and then tap **Confirm** and save.

- Tap **Select Time Zone** to manually select the time zone where the device is located.
- Enable or disable this format by tapping 24-Hour Time. If enabled, then tap **Date Format** to set the date.
- Tap **Daylight Saving Time** to enable or disable the function. If enabled, tap **Daylight Saving Mode** to select a daylight-saving mode and then tap **Daylight Saving Setup** to set the switch time.



Daylight Saving Setup

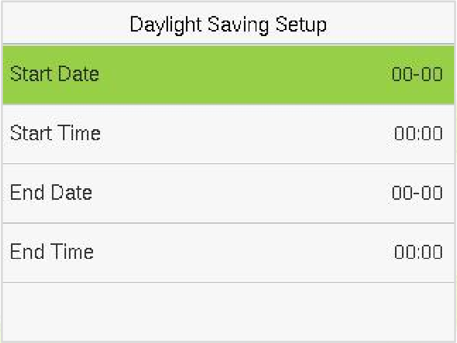
Start Month 1

Start Week 1

Start Day Sunday

Start Time 00:00

End Month 1



Daylight Saving Setup

Start Date 00-00

Start Time 00:00

End Date 00-00

End Time 00:00

Week Mode **Date Mode**

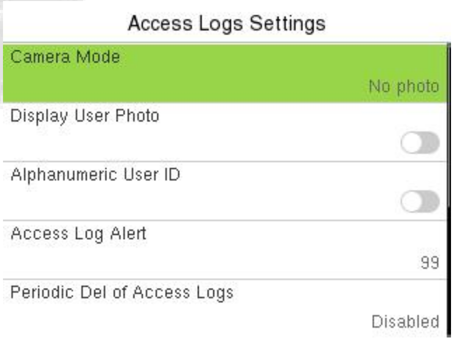
- When restoring the factory settings, the time (24-hour) and date format (YYYY-MM-DD) can be restored, but the device date and time cannot be restored.

Note: For example, if a user sets the time of the device from 18:35 on March 15, 2020 to 18:30 on January 1, 2021. After restoring the factory settings, the time of the device will remain at 18:30 on January 1, 2021.

11.2 Access Logs Settings / Attendance

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

Access Control Terminal:



Access Logs Settings

Camera Mode No photo

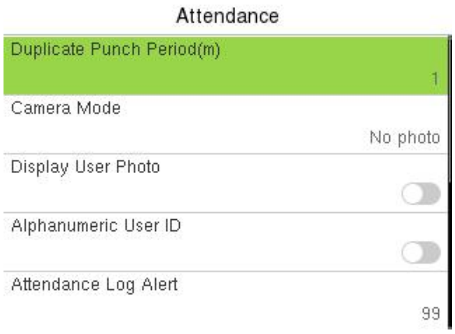
Display User Photo

Alphanumeric User ID

Access Log Alert 99

Periodic Del of Access Logs Disabled

Time Attendance Terminal:



Attendance

Duplicate Punch Period(m)
1

Camera Mode
No photo

Display User Photo

Alphanumeric User ID

Attendance Log Alert
99

Function Description of Access Control Terminal:

Function Name	Description
Camera Mode	This function is disabled by default. When enabled, a security prompt will pop-up and the sound of shutter in the camera will turn on mandatorily. There are 5 modes: **No photo:** No photo is taken during user verification. **Take photo, no save:** Photo is taken but not saved during verification. **Take photo and save:** All the photos taken during verification is saved. **Save on successful verification:** Photo is taken and saved for each successful verification. **Save on failed verification:** Photo is taken and saved only for each failed verification.
Display User Photo	Whether to display the user photo when the user passes the verification.
Alphanumeric User ID	Enable/Disable the alphanumeric as User ID.
Access Log Alert	When the record space of the attendance access reaches the maximum threshold value, the device automatically displays the memory space warning. Users may disable the function or set a valid value between 1 and 9999.

Periodic Del of Access Logs	When access logs reach its maximum capacity, the device automatically deletes a set of old access logs. Users may disable the function or set a valid value between 1 and 999.
Periodic Del of T&A Photo	When attendance photos reach its maximum capacity, the device automatically deletes a set of old attendance photos. Users may disable the function or set a valid value between 1 and 99.
Periodic Del of Blocklist Photo	When block listed photos reach its maximum capacity, the device automatically deletes a set of old block listed photos. Users may disable the function or set a valid value between 1 and 99.
Authentication Timeout(s)	The amount of time taken to display a successful verification message. Valid value: 1 to 9 seconds.
Recognition Interval(s)	After the interval identifying is clicked (selected), for example, if the comparison interval is set to 5 seconds, then the face recognition will verify the face every 5 seconds. Valid value: 0 to 9 seconds. 0 means continuous identifying, 1 to 9 means identifying at intervals.

Function Description of Time Attendance Terminal:

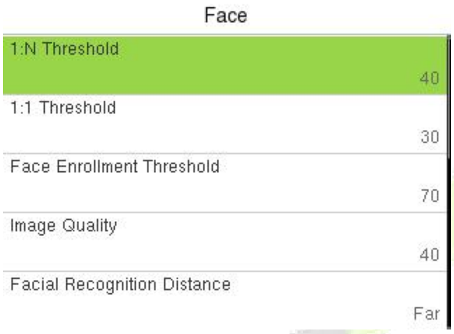
Function Name	Description
Duplicate Punch Period(m)	Within a set time period (unit: minutes), the duplicated attendance record will not be reserved (value ranges from 1 to 999999 minutes).

Camera Mode	This function is disabled by default. When enabled, a security prompt will pop-up and the sound of shutter in the camera will turn on mandatorily. There are 5 modes: **No photo:** No photo is taken during user verification. **Take photo, no save:** Photo is taken but not saved during verification. **Take photo and save:** All the photos taken during verification is saved. **Save on successful verification:** Photo is taken and saved for each successful verification. Save on failed verification: Photo is taken and saved only for each failed verification.
Display User Photo	Whether to display the user photo when the user passes the verification.
Alphanumeric User ID	Enable/Disable the alphanumeric as User ID.
Attendance Log Alert	When the record space of the attendance reaches the maximum threshold value, the device automatically displays the memory space warning. Users may disable the function or set a valid value between 1 and 9999.
Periodic Del of T&A Data	When attendance records reach its maximum storage capacity, the device automatically deletes a set of old attendance records. Users may disable the function or set a valid value between 1 and 999.
Periodic Del of T&A Photo	When attendance photos reach its maximum capacity, the device automatically deletes a set of old attendance photos. Users may disable the function or set a valid value between 1 and 99.
Periodic Del of Blocklist Photo	When block listed photos reach its maximum capacity, the device automatically deletes a set of old block listed photos. Users may disable the function or set a valid value between 1 and 99.

Authentication Timeout(s)	The amount of time taken to display a successful verification message. Valid value: 1 to 9 seconds.
Recognition Interval(s)	After the interval identifying is clicked (selected), for example, if the comparison interval is set to 5 seconds, then the face recognition will verify the face every 5 seconds. Valid value: 0 to 9 seconds. 0 means continuous identifying, 1 to 9 means identifying at intervals.

11.3 Face Parameters

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



Face

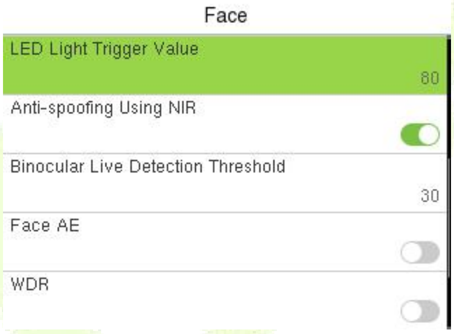
1:N Threshold 40

1:1 Threshold 30

Face Enrollment Threshold 70

Image Quality 40

Facial Recognition Distance Far



Face

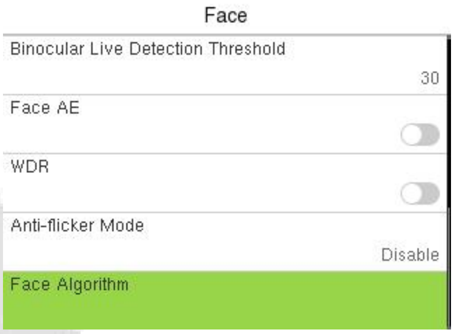
LED Light Trigger Value 80

Anti-spoofing Using NIR

Binocular Live Detection Threshold 30

Face AE

WDR



Face

Binocular Live Detection Threshold 30

Face AE

WDR

Anti-flicker Mode Disable

Face Algorithm

Function Description

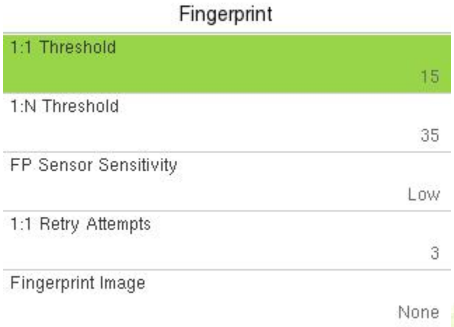
Function Name	Description
1:N Threshold Value	Under 1:N verification mode, the verification will only be successful when the similarity between the acquired facial image and all registered facial templates is greater than the set value. The valid value ranges from 0 to 100. The higher the thresholds, the lower the misjudgement rate and the higher the rejection rate, and vice versa. It is recommended to set the default value of 47.
1:1 Threshold Value	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 0to 100. The higher the thresholds, the lower the misjudgement rate and the higher the rejection rate, and vice versa. It is recommended to set the default value of 63.
Face Enrollment Threshold	During face enrollment, 1:N comparison is used to determine whether the user has already registered before. When the similarity between the acquired facial image and all registered facial templates is greater than the set threshold, it indicates that the face has already been registered.
Image Quality	It is the image quality for facial registration and comparison. The higher the value, the clearer image is required.
Face Recognition Distance	The farther the individual is, the smaller the face, and the smaller number of pixels of the face obtained by the algorithm. Therefore, adjusting this parameter can adjust the farthest comparison distance of faces.
LED Light Trigger Value	This value controls the turning on and off of the LED light. The larger the value, the LED light will turn on or off more frequently.
Anti-spoofing Using NIR	Using near-infrared spectra imaging to identify and prevent fake photos and videos attack.
Binocular Live Detection Threshold	It is convenient to judge whether the near-infrared spectral imaging is fake photo and video. The larger the value, the better the anti-spoofing performance of near-infrared spectral imaging.
Face AE	When the face is in front of the camera in Face AE mode, the brightness of the face area increases, while other areas become darker.
WDR	Wide Dynamic Range (WDR) balances light and extends image visibility for surveillance videos under high contrast lighting scenes and improves object identification under bright and dark environments.
Anti-flicker Mode	It is used when WDR is turned off. It helps to reduce flicker when the device's screen flashes at the same frequency as the light.

Face algorithm	It has facial algorithm related information and pause the facial template update.

11.4 Fingerprint

Select **Fingerprint** on the **System** interface to go to the Fingerprint parameter settings.



Fingerprint

1:1 Threshold 15

1:N Threshold 35

FP Sensor Sensitivity Low

1:1 Retry Attempts 3

Fingerprint Image None

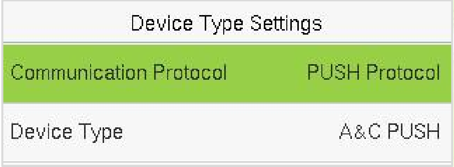
Function Description

Function Name	Description
1:1 Threshold	Under 1:1 verification method, the verification will only be successful when the similarity between the acquired fingerprint data and the fingerprint template associated with the entered user ID enrolled in the device is greater than the set value.
1:N Threshold	Under 1:N verification method, the verification will only be successful when the similarity between the acquired fingerprint data and the fingerprint templates enrolled in the device is greater than the set value.
FP Sensor Sensitivity	To set the sensibility of fingerprint acquisition. It is recommended to use the default level "**Medium**". When the environment is dry, resulting in slow fingerprint detection, you can set the level to **"High**" to raise the sensibility; when the environment is humid, making it hard to identify the fingerprint, you can set the level to "**Low**".
1:1 Retry Attempts	In 1:1 Verification, users might forget the registered fingerprint, or press the finger improperly. To reduce the process of re-entering user ID, retry is allowed.

Fingerprint Image	To set whether to display the fingerprint image on the screen during fingerprint enrollment or verification. Four choices are available: **Show for Enroll:** to display the fingerprint image on the screen only during enrollment. **Show for Match:** to display the fingerprint image on the screen only during verification. **Always Show:** to display the fingerprint image on screen during enrollment and verification. **None:** not to display the fingerprint image.

11.5 Device Type Settings

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



Device Type Settings

Communication Protocol PUSH Protocol

Device Type A&C PUSH

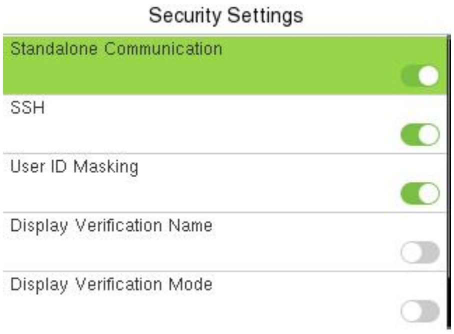
Function Description

Function Name	Description
Communication Protocol	Set the device communication protocol. (BEST protocol is suitable for ZKBio Zlink, please refer to 24 Connecting to ZKBio Zlink Mobile App and 25 Connecting to ZKBio Zlink Web Portal)
Device Type	Set the device as an access control terminal or attendance terminal.

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

11.6 Security Settings

Select **Security Settings** on the **System** interface to go to the Security settings.



Security Settings

Standalone Communication

SSH

User ID Masking

Display Verification Name

Display Verification Mode

Function Description

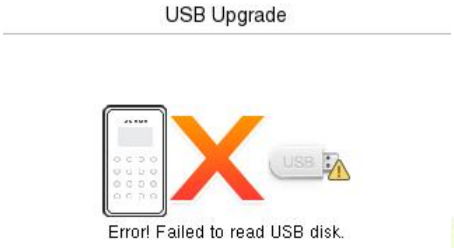
Function Name	Description
Standalone Communication	To avoid being unable to use when the device is offline, you can download the C/S software (such as ZKAccess 3.5) on your computer in advance for offline use.
SSH	SSH is used to enter the background of the device for maintenance.
User ID Masking	When enabled, and then the user is successfully compared and verified, the User ID in the displayed verification result will be replaced with an * to achieve secure protection of sensitive private data.
Display Verification Name	Set whether to display the username in the verification result interface.
Display Verification Mode	Set whether to display the verification mode in the verification result interface.
Save Photo as Template	After disable this function, face re-registration is required after an algorithm upgrade.

11.7 USB Upgrade

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

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

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



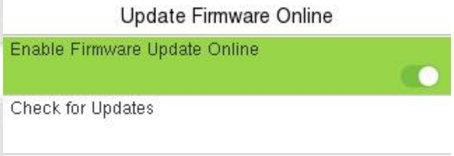
USB Upgrade

Error! Failed to read USB disk.

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

11.8 Update Firmware Online

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



Update Firmware Online

Enable Firmware Update Online

Check for Updates

The Firmware Update Online function is enabled by default. Tap **Check for Updates** it may have the following 3 scenarios:

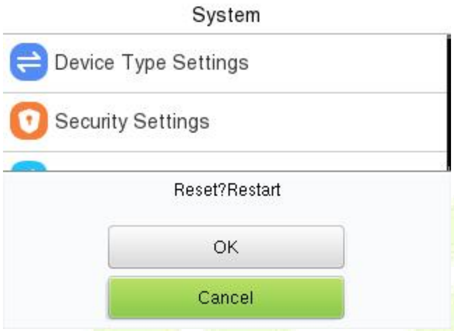
- If the query fails, the interface will prompt "Query failed".
- If the firmware version of the device is latest, it will prompt that the current firmware version is already the latest.

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

11.9 Factory Reset

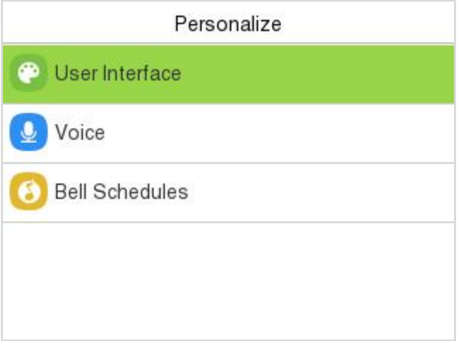
The Factory Reset function restores the device settings such as communication settings and system settings, to the default factory settings (this function does not clear registered user data).

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

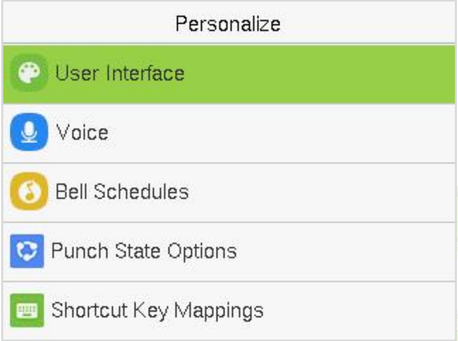


12 Personalize Settings

When the device is on the initial interface, press **M/OK** and select **Personalize** to customize the interface settings, voice, bell, punch state options, and shortcut key mappings.



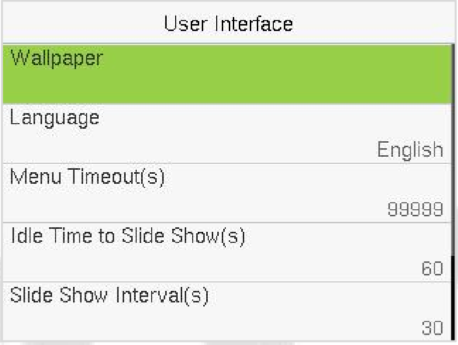
A&C Terminal



T&A Terminal

12.1 User Interface

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


User Interface

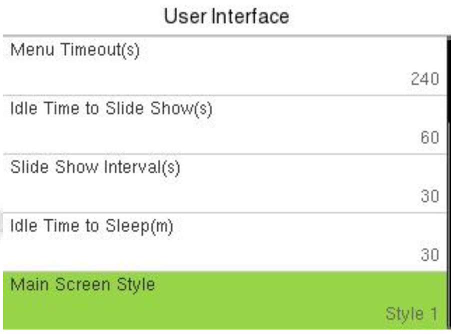
Wallpaper

Language: English

Menu Timeout(s): 99999

Idle Time to Slide Show(s): 60

Slide Show Interval(s): 30


User Interface

Menu Timeout(s): 240

Idle Time to Slide Show(s): 60

Slide Show Interval(s): 30

Idle Time to Sleep(m): 30

Main Screen Style: Style 1

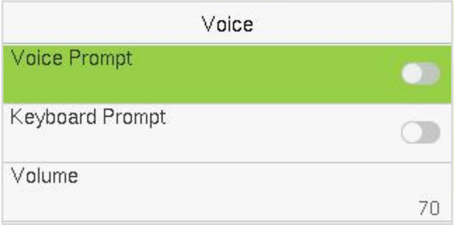
Function Description

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

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

12.2 Voice

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

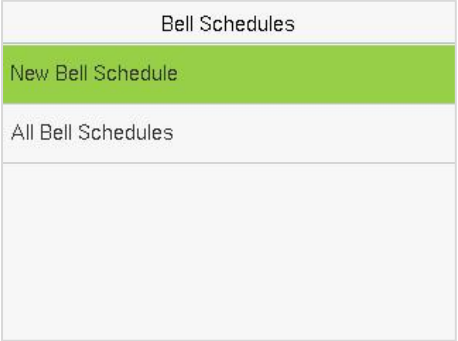


Function Description

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

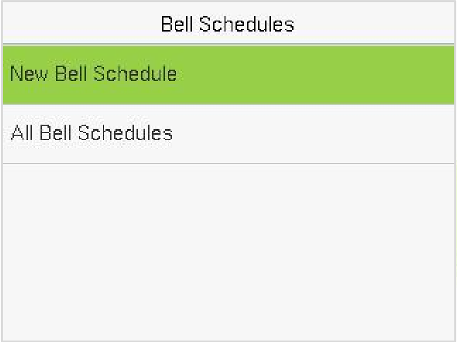
12.3 Bell Schedules

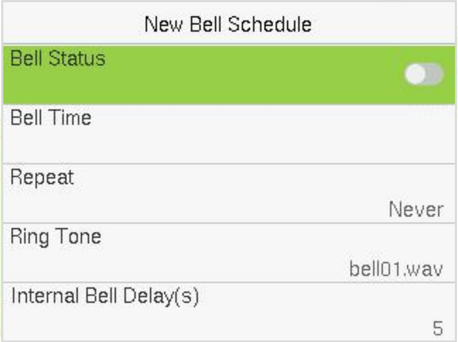
Select **Bell Schedules** on the **Personalize** interface to configure the Bell settings.



- **New Bell Schedule:**

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




New Bell Schedule

Bell Status

Bell Time

Repeat
Never

Ring Tone
bell01.wav

Internal Bell Delay(s)
5

Function Description

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

- **All Bell Schedules:**

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

- **Edit the Scheduled Bell:**

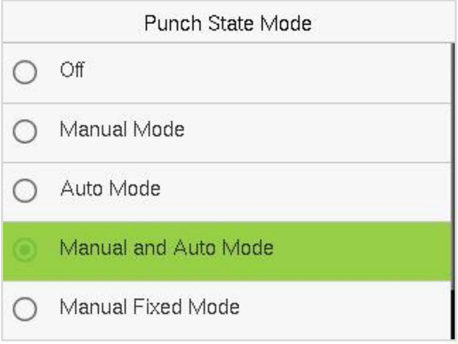
On the **All Bell Schedules** interface, tap on the required bell schedule, and tap **Edit** to edit the selected bell schedule. The editing method is the same as the operations of adding a new bell schedule.

- **Delete a Bell Schedules:**

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

12.4 Punch States Options

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



Punch State Mode

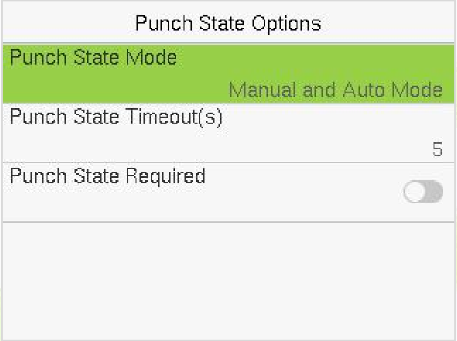
○ Off

○ Manual Mode

○ Auto Mode

● Manual and Auto Mode

○ Manual Fixed Mode



Punch State Options

Punch State Mode: Manual and Auto Mode

Punch State Timeout(s): 5

Punch State Required

Function Description

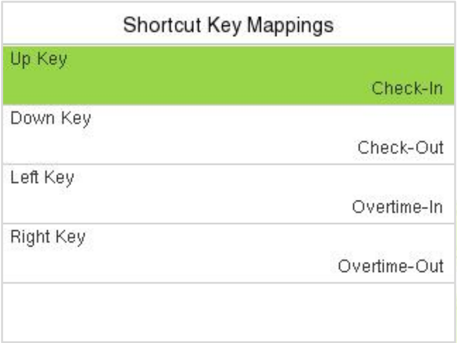
Function Name	Description
Punch State Mode	**Off:** Disable the punch state function. Therefore, the punch state key set under Shortcut Key Mappings menu will become invalid. **Manual Mode:** Switch the punch state key manually, and the punch state key will disappear after Punch State Timeout. **Auto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

	OFF: Attendance state need not requires to be selected after verification.

12.5 Shortcut Key Mappings

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

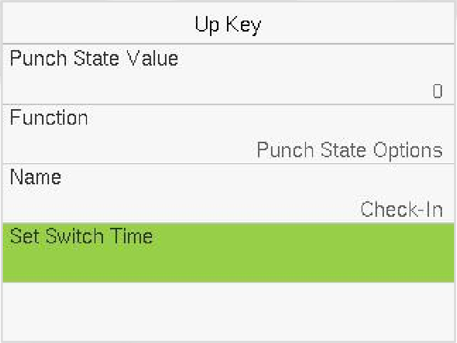
Select **Shortcut Key Mappings** on the **Personalize** interface to set the required shortcut keys.



Shortcut Key Mappings

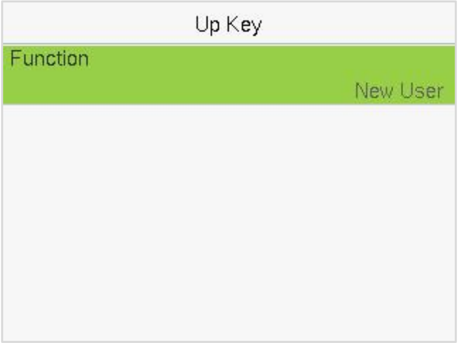
Up Key	Check-In
Down Key	Check-Out
Left Key	Overtime-In
Right Key	Overtime-Out

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



Up Key

Punch State Value	0
Function	Punch State Options
Name	Check-In
Set Switch Time	



Up Key

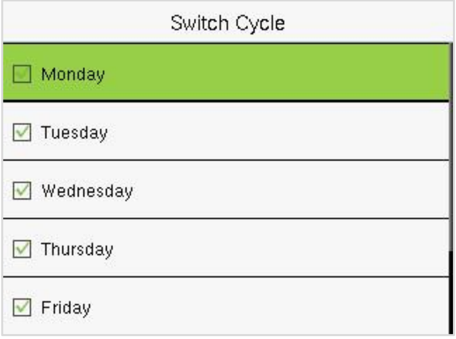
Function	New User

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

➢ **Set the Switch Time**

- The switch time is set in accordance with the punch state options.
- When the **Punch State Mode** is set to **Auto Mode**, the switch time should be set.
- On the **Shortcut Key** interface, tap **Set Switch Time** to set the switch time.

- On the **Switch Cycle** interface, select the switch cycle (Monday, Tuesday, etc.) as shown in the image below.



Switch Cycle

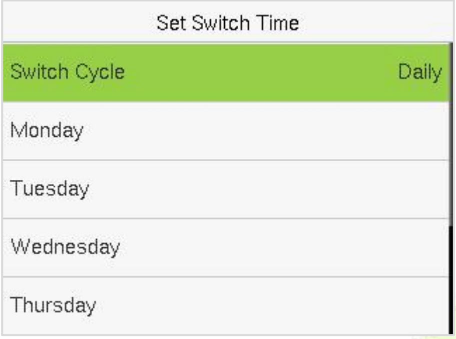
□ Monday

☑ Tuesday

☑ Wednesday

☑ Thursday

☑ Friday



Set Switch Time

Switch Cycle Daily

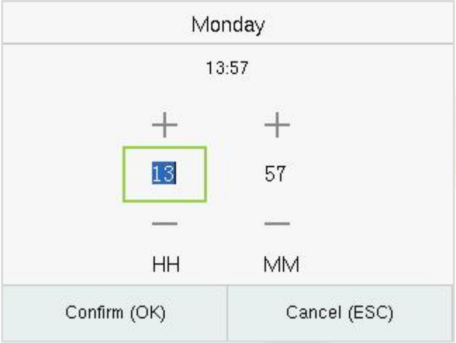
Monday

Tuesday

Wednesday

Thursday

- Once the Switch cycle is selected, set the switch time for each day, and tap **OK** to confirm, as shown in the image below.



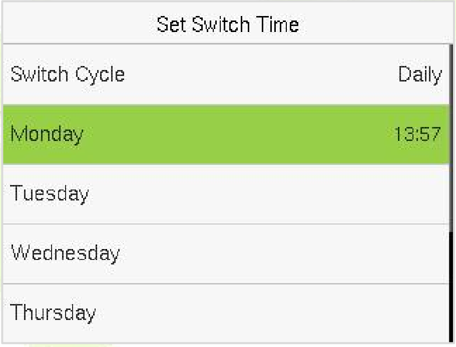
Monday

13:57

HH 13

MM 57

Confirm (OK) Cancel (ESC)



Set Switch Time

Switch Cycle Daily

Monday 13:57

Tuesday

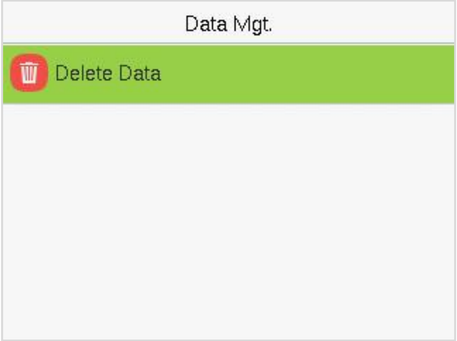
Wednesday

Thursday

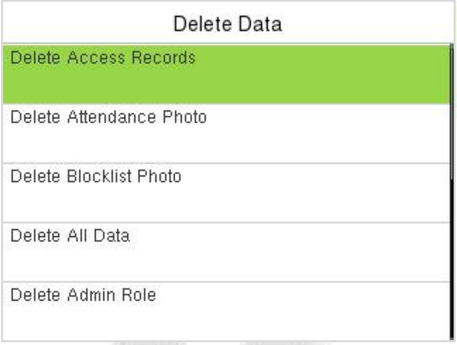
Note: When the function is set to Undefined, the device will not enable the punch state key.

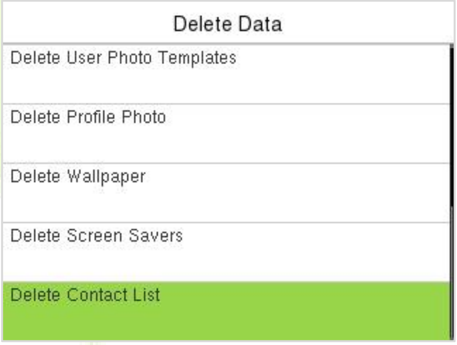
13 Data Management

When the device is on the initial interface, press **M/OK** and select **Data Mgt.** to manage the relevant data in the device.



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



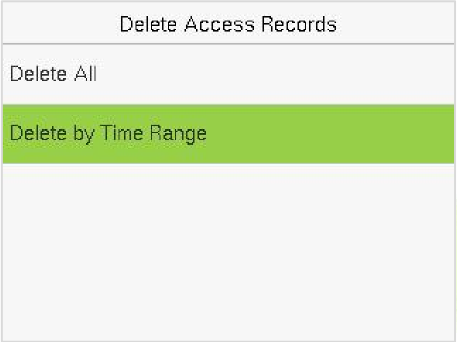


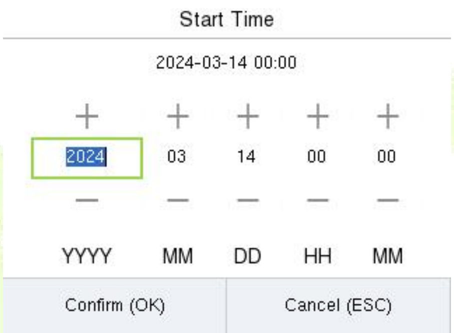
Function Description

Function Name	Description
Delete Access Records / Attendance Data	To delete the access records & attendance data conditionally.
Delete Attendance Photo	To delete attendance photos of designated personnel.
Delete Blocklist Photo	To delete the photos taken during failed verifications.
Delete All Data	To delete the information and access records & attendance data of all registered users.
Delete Admin Role	To remove all the administrator privileges.
Delete Access Control	To delete all the access data.
Delete User Photo Templates	To delete user photo templates in the device. When deleting template photos, there is a risk reminder: “Face re-registration is required after an algorithm upgrade.”

Delete Profile Photo	To delete all the profile photos on the device.
Delete Wallpaper	To delete all the wallpapers in the device.
Delete Screen Savers	To delete all the screen savers in the device.
Delete Contact List	To delete all contact list of video intercom in the device.

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





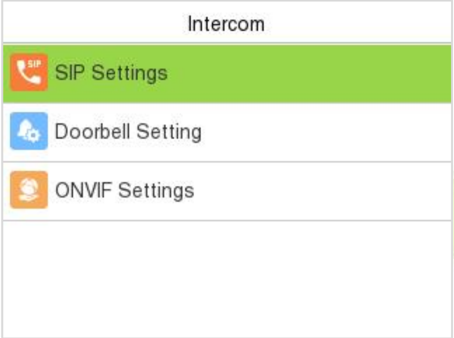
14 Intercom

When the device is on the initial interface, press **M/OK** and select **Intercom** to set relevant parameters of intercom, including SIP, Doorbell and ONVIF Settings.

The device achieves video intercom there are two modes, respectively, the LAN and SIP server. For more details, please refer to 23 SIP Video Intercom.

14.1 SIP Settings

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

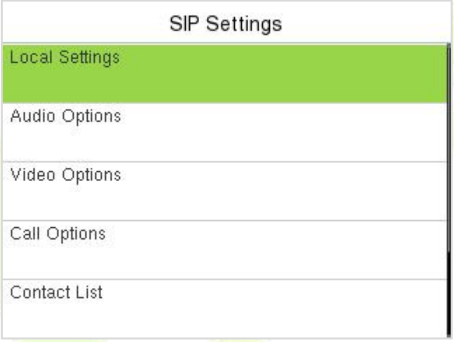


Intercom

SIP Settings

Doorbell Setting

ONVIF Settings



SIP Settings

Local Settings

Audio Options

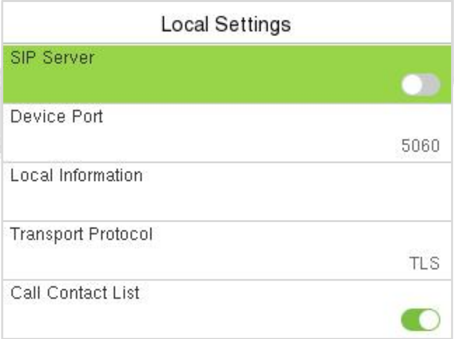
Video Options

Call Options

Contact List

14.1.1 Local Settings

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



Local Settings

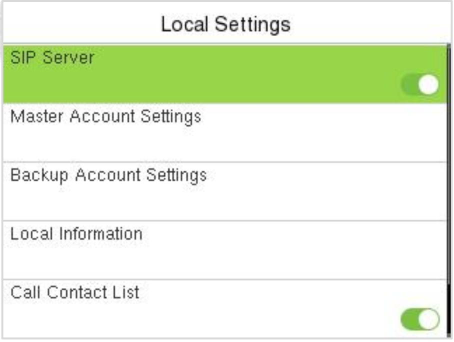
SIP Server

Device Port 5060

Local Information

Transport Protocol TLS

Call Contact List



Local Settings

SIP Server

Master Account Settings

Backup Account Settings

Local Information

Call Contact List

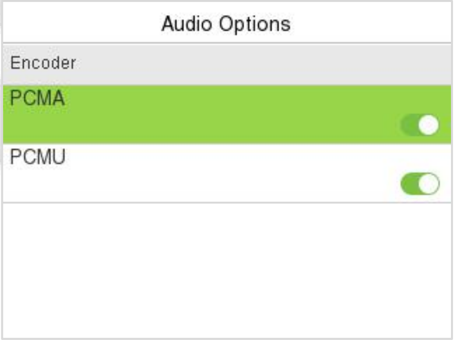
Function Description

Function Name	Description
SIP Server	Select whether to enable the SIP server. When it is enabled, the SIP account needs to be set. **Note:** Every time this feature is turned on or off, the contact list will be reset.

Master Account Settings	After assigning the SIP account to the device on the ZKBio CVAccess, the account information will be automatically synchronized to the device. You don't need to configure it manually.
Backup Account Settings	Select whether to enable the backup account settings.
Device Port	When using a local area network for intercom, enter the device port number.
Local Information	**Device Type:** Set the device type as **Entrance Station** or **Fence Terminal**. And set the specific location information of the device, including the block, unit (can be disabled), and room number. When it is set as Fence Terminal, the call page will display block, unit and room number. **Note:** The contact list will be cleared after changing the device type.
Transport Protocol	Set the transport protocol between the device and indoor monitor.
Call Contact List	Select whether to enable the contact list on the call page. When it is enabled, you can press the **Up Key** to open the contact list on the call page.
Call Number Type	**Room Number:** The device can call the extension number (short number) or room number. **SIP Account Number:** The device can only call the SIP account.

14.1.2 Audio Options

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


Audio Options

Encoder

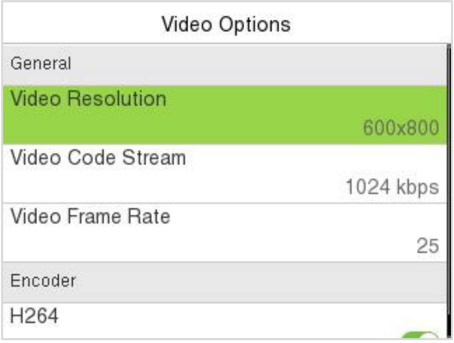
PCMA

PCMU

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

14.1.3 Video Options

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



Video Options

General

Video Resolution
600x800

Video Code Stream
1024 kbps

Video Frame Rate
25

Encoder

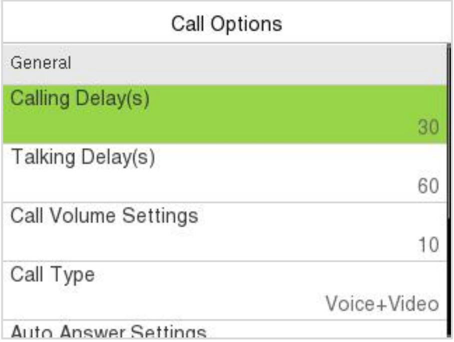
H264

Function Description

Function Name	Description
Video Resolution	Select the video resolution of the intercom, 1024 x 576 or 800 x 600. The device only supports landscape screen. It is suggested to set as 800 x 600.
Video Code Stream	Select the video code stream of the intercom, the larger the value, the higher the picture and sound quality of the video, and the greater the network requirements.
Video Frame Rate	Refers to the number of frames per second of the intercom video display, the larger the value the smoother, the device defaults to 25Hz, does not support modification.
Encoder	Whether to enable H264 Encoder.

14.1.4 Call Options

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



Call Options

General

Calling Delay(s)
30

Talking Delay(s)
60

Call Volume Settings
10

Call Type
Voice+Video

Auto Answer Settings

Function Description

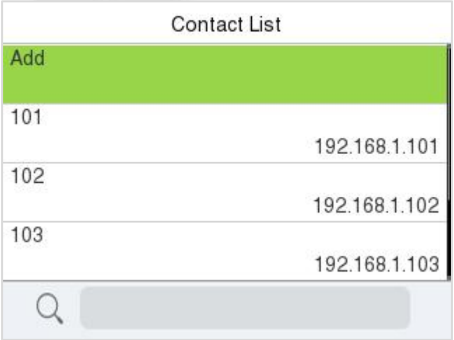
Function Name	Description
Calling Delay(s)	Set the time of call, valid value 30 to 60 seconds.
Talking Delay(s)	Set the time of intercom, valid value 60 to 120 seconds. It is suggested to set as 60s.
Call Volume Settings	Set the volume of the call, with valid value ranging from 0 to 100.
Call Type	Set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

14.1.5 Contact List

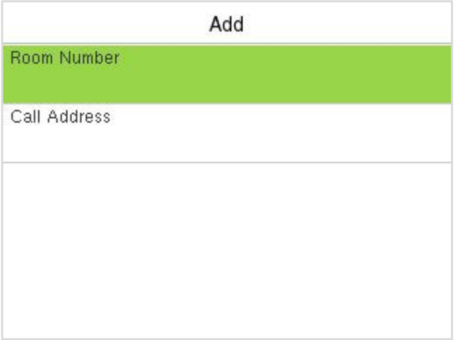
Select **Contact List** on the **SIP Settings** interface.

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

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

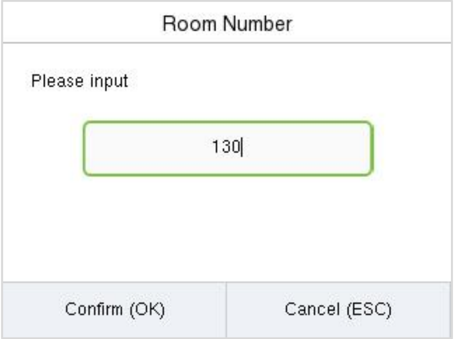


101	192.168.1.101
102	192.168.1.102
103	192.168.1.103



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

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



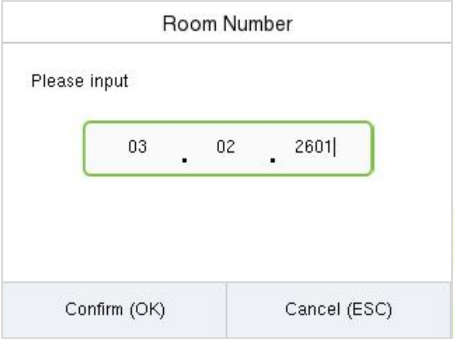
Room Number

Please input

130

Confirm (OK) Cancel (ESC)

Entrance Station



Room Number

Please input

03 . 02 . 2601

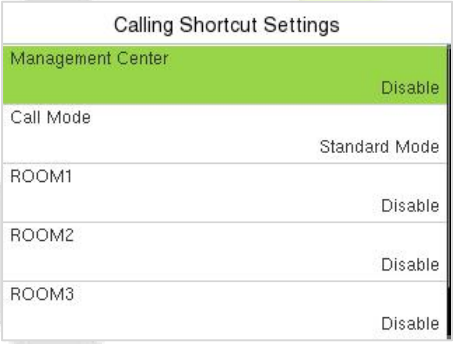
Confirm (OK) Cancel (ESC)

Fence Terminal

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

14.1.6 Calling Shortcut Settings

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



Calling Shortcut Settings

Management Center: Disable

Call Mode: Standard Mode

ROOM1: Disable

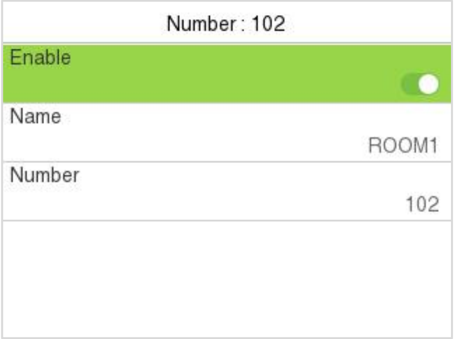
ROOM2: Disable

ROOM3: Disable

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

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

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



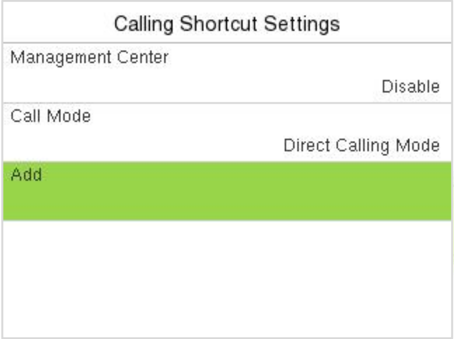
Number : 102

Enable

Name: ROOM1

Number: 102

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

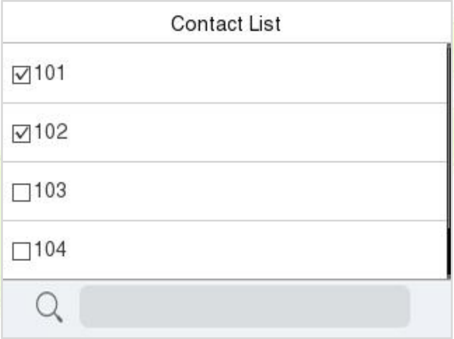


Calling Shortcut Settings

Management Center: Disable

Call Mode: Direct Calling Mode

Add



Contact List

☑101

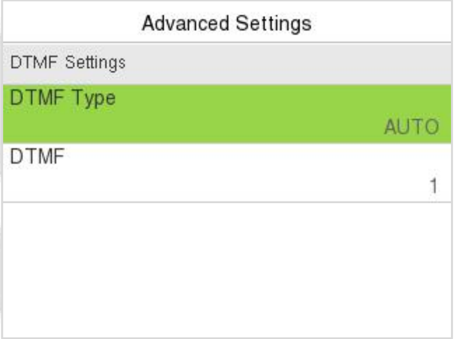
☑102

□103

□104

14.1.7 Advanced Settings

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



Advanced Settings

DTMF Settings

DTMF Type: AUTO

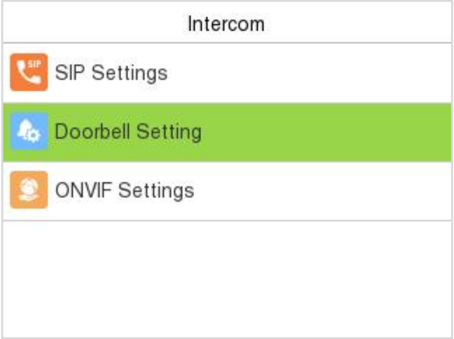
DTMF: 1

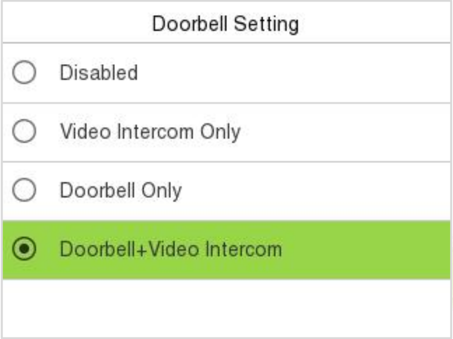
Function Description

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

14.2 Doorbell Setting

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





Doorbell Setting

○ Disabled

○ Video Intercom Only

○ Doorbell Only

● Doorbell+Video Intercom

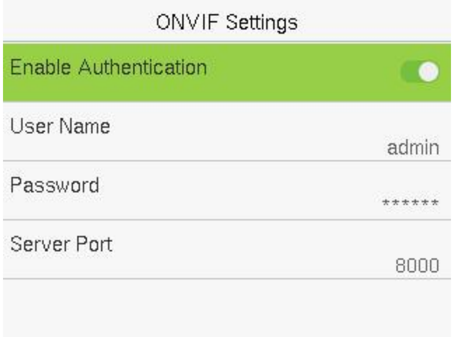
Function Description:

Function Name	Description
Doorbell Setting	**Disabled:** The doorbell button is disabled. **Doorbell Only:** When the user presses the doorbell button, only the doorbell rings. **Video Intercom Only:** When the user presses the doorbell button, only the device makes a call. **Doorbell+Video Intercom:** When the user presses the doorbell button, the doorbell rings and the device makes a call at the same time.

14.3 ONVIF Settings

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

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



ONVIF Settings

Enable Authentication: On

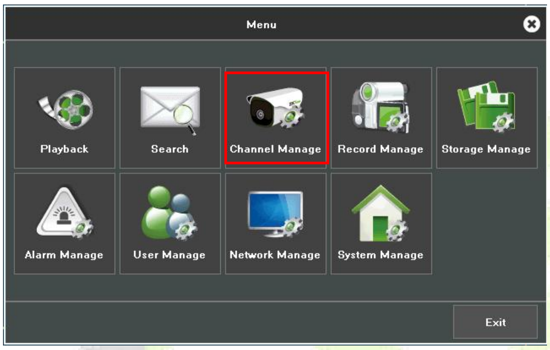
User Name: admin

Password: ******

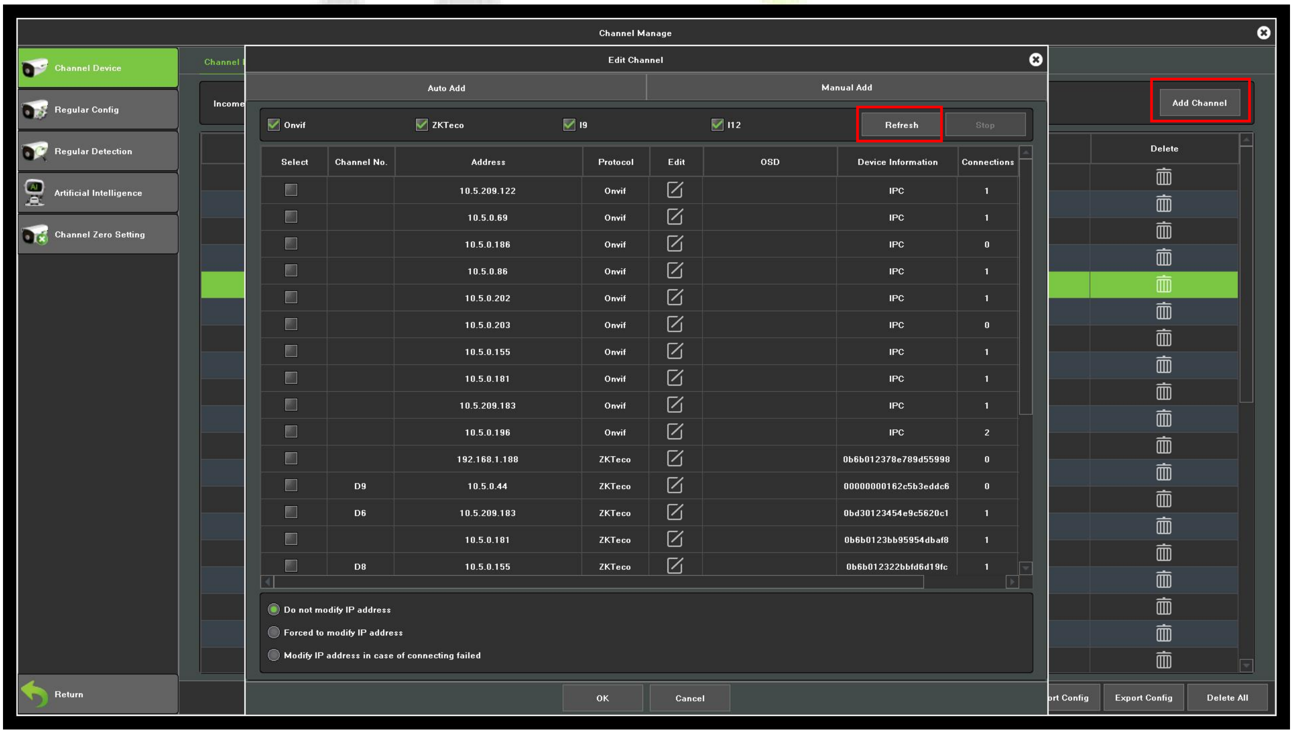
Server Port: 8000

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

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



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

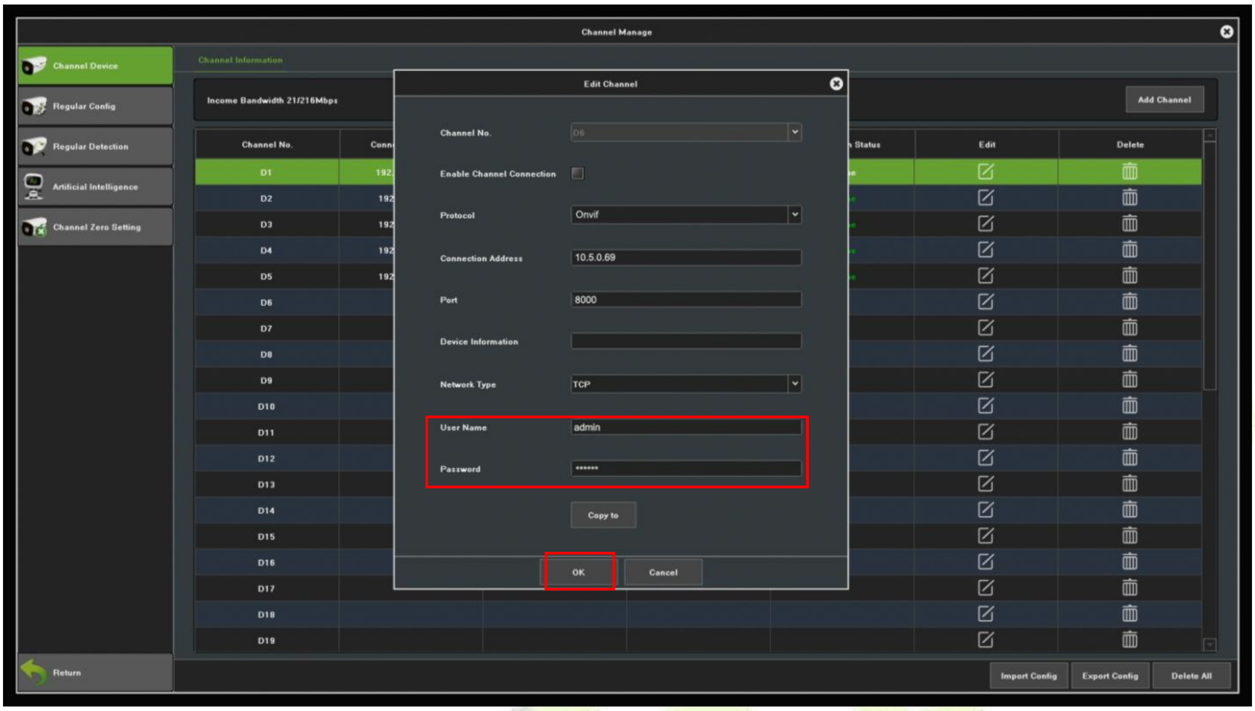


☑ Onvif ☑ ZKTeco ☑ I9 ☑ I12

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

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

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



Channel No. D6

Enable Channel Connection □

Protocol Onvif

Connection Address 10.5.0.69

Port 8000

Device Information

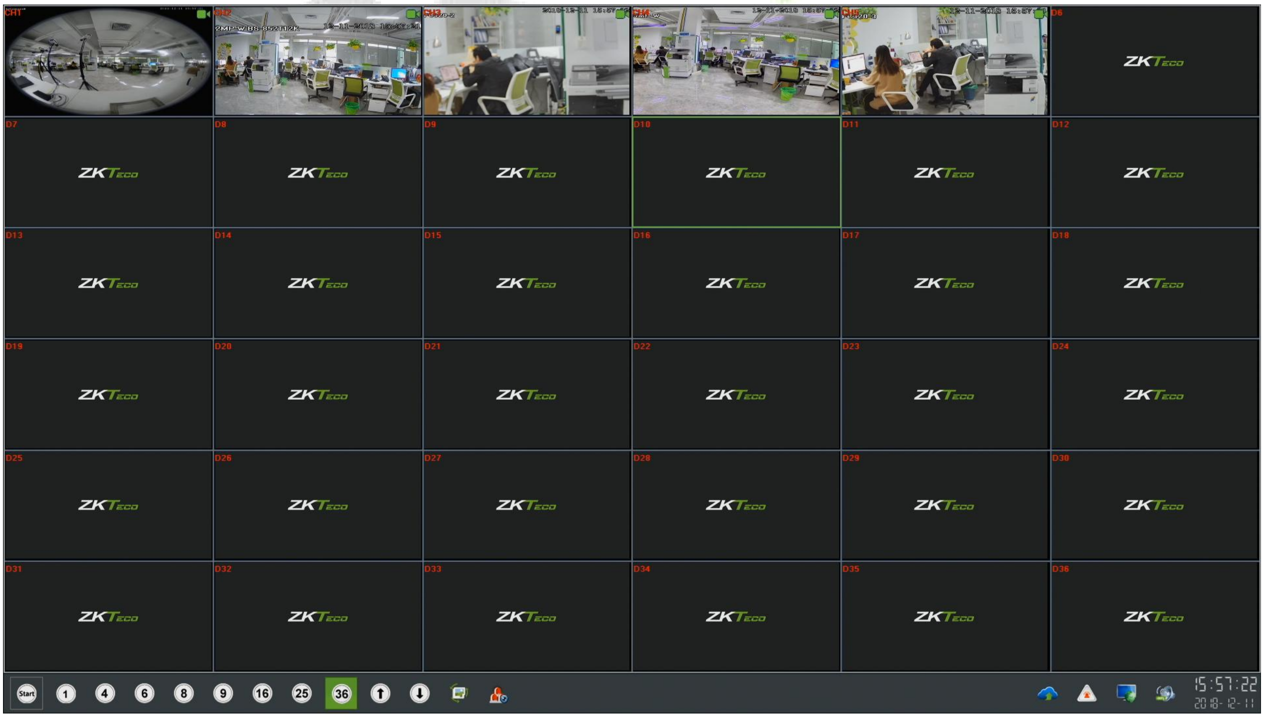
Network Type TCP

User Name admin

Password ******

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

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

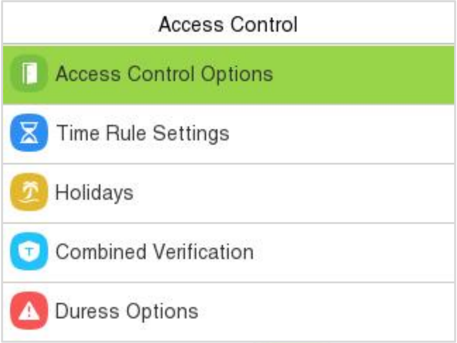


For more details, please refer to the *NVR User Manual*.

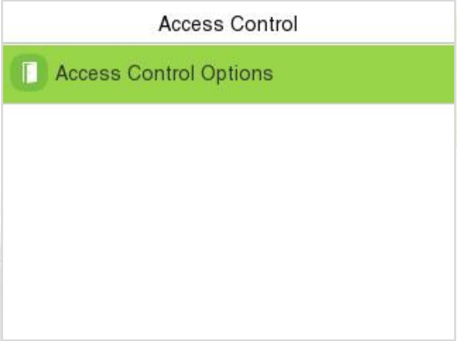
15 Access Control

When the device is on the initial interface, press **M/OK** and select **Access Control** to set the schedule of the door opening, locks control and to configure other parameters settings related to access control.

Access Control Terminal:



Time Attendance Terminal:



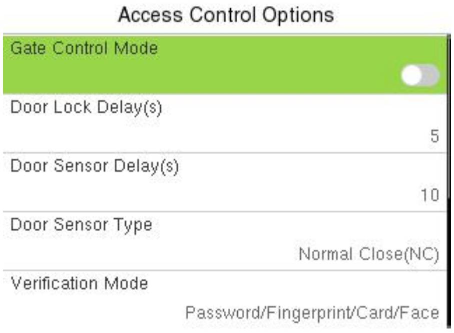
To get access, the registered user must meet the following conditions:

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

15.1 Access Control Options

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

Access Control Terminal:



Access Control Options

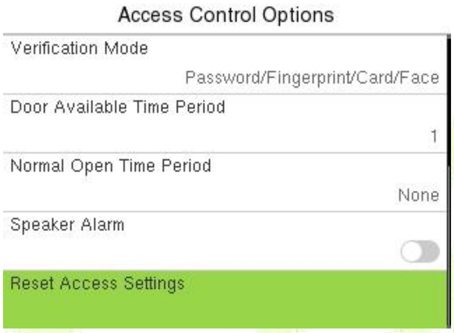
Gate Control Mode

Door Lock Delay(s): 5

Door Sensor Delay(s): 10

Door Sensor Type: Normal Close(NC)

Verification Mode: Password/Fingerprint/Card/Face



Access Control Options

Verification Mode: Password/Fingerprint/Card/Face

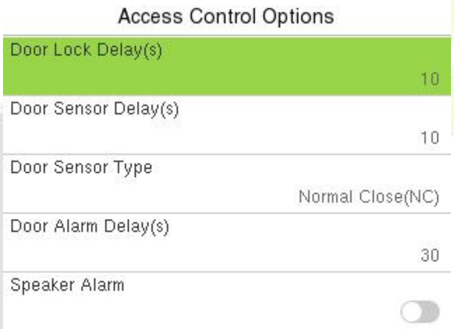
Door Available Time Period: 1

Normal Open Time Period: None

Speaker Alarm

Reset Access Settings

Time Attendance Terminal:



Access Control Options

Door Lock Delay(s): 10

Door Sensor Delay(s): 10

Door Sensor Type: Normal Close(NC)

Door Alarm Delay(s): 30

Speaker Alarm

Function Description of Access Control Terminal:

Function Name	Description
Gate Control Mode	It toggles between **ON** or **OFF** switch to get into gate control mode or not. When set to **ON**, the interface removes the Door Lock Delay, Door Sensor Delay, and Door Sensor Type options.
Door Lock Delay (s)	The length of time that the device controls the electric lock to be in unlock state. Valid value: 1~99 seconds.
Door Sensor Delay (s)	If the door is not locked and is left open for a certain duration (Door Sensor Delay), an alarm will be triggered. The valid value of Door Sensor Delay ranges from 1 to 255 seconds.

Door Sensor Type	There are three Sensor types: **None**, **Normal Open**, and **Normal Closed**. **None:** It means the door sensor is not in use. **Normally Open:** It means the door is always left open when electric power is on. **Normally Closed:** It means the door is always left closed when electric power is on.
Verification Mode	The supported verification mode includes Password/Fingerprint/Card/Face, Fingerprint Only, User ID Only, Password, Card Only and so on.
Door Available Time Period	It sets the timing for the door so that the door is accessible only during that period.
Normal Open Time Period	It is the scheduled time-period for "Normal Open" mode so that the door is always open during this period.
Speaker Alarm	It transmits a sound alarm or disassembly alarm from the local. When the door is closed or the verification is successful, the system cancels the alarm from the local.
Reset Access Setting	The access control reset parameters include door lock delay, door sensor delay, door sensor type, verification mode, door available time period, normal open time period, and alarm. However, erased access control data in Data Mgt. is excluded.

Function Description of Time Attendance Terminal:

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

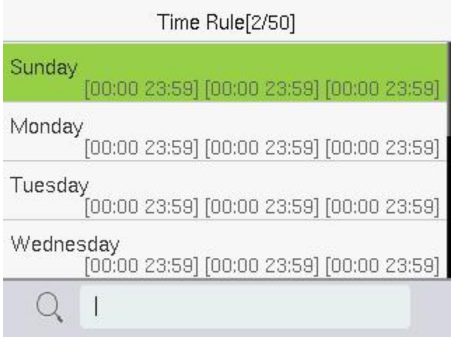
Door Sensor Type	There are three Sensor types: **None**, **Normal Open**, and **Normal Closed**. **None:** It means the door sensor is not in use. **Normally Open (NO):** It means the door is always left open when electric power is on. **Normally Closed (NC):** It means the door is always left closed when electric power is on.
Door Alarm Delay(s)	When the state of the door sensor is inconsistent with that of the door sensor type, alarm will be triggered after a time period; this time period is the Door Alarm Delay (the value ranges from 1 to 999 seconds).
Speaker Alarm	It transmits a sound alarm or disassembly alarm from the local. When the door is closed or the verification is successful, the system cancels the alarm from the local.

15.2 Time Rule Settings

Select **Time Rule Settings** 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 grey box to search the required Time Rule and specify the required Time Rule number (maximum up to 50 rules).



Time Rule[2/50]

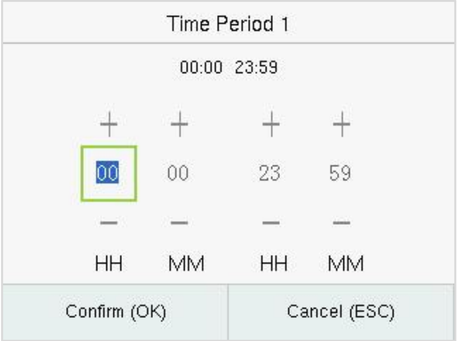
Sunday [00:00 23:59] [00:00 23:59] [00:00 23:59]

Monday [00:00 23:59] [00:00 23:59] [00:00 23:59]

Tuesday [00:00 23:59] [00:00 23:59] [00:00 23:59]

Wednesday [00:00 23:59] [00:00 23:59] [00:00 23:59]

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



Specify the start and the end time, and then press **M/OK**.

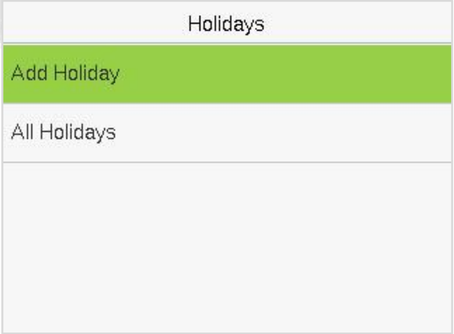
Note:

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

15.3 Holidays

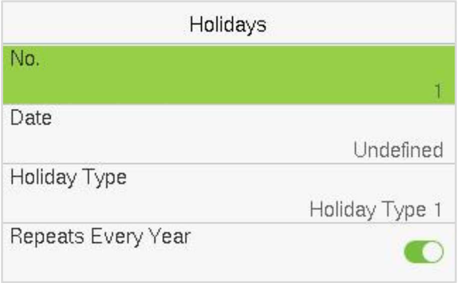
When there is a holiday, you may need a different access time; however, altering everyone's access time one by one is extremely time-consuming. Thus, a holiday access time that applies to all workers can be set, and the user will be able to open the door during the holidays.

Select **Holidays** on the **Access Control** interface to set the holiday access.



➢ **Add a New Holiday:**

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



Holidays

No. 1

Date Undefined

Holiday Type Holiday Type 1

Repeats Every Year

- **Edit a Holiday:**

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

- **Delete a Holiday:**

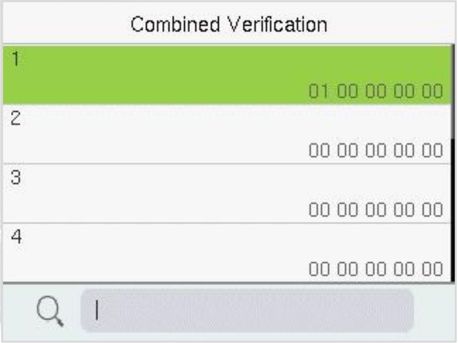
On the **Holidays** interface, select a holiday item to be deleted and tap **Delete**. Press **M/OK** to confirm the deletion. After deletion, this holiday does not display on the **All Holidays** interface.

15.4 Combined Verification

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

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

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



Combined Verification

1 01 00 00 00 00

2 00 00 00 00 00

3 00 00 00 00 00

4 00 00 00 00 00

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

For Example:

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

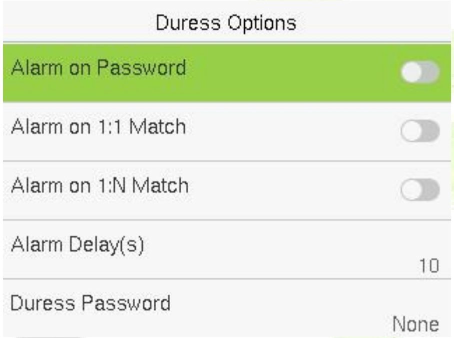
- If the **Door-unlock combination 3** is set as (**09 09 09 09 09**). It indicates that there are 5 people in this combination; all of which are from AC Group 9.
- If the **Door-unlock combination 4** is set as (**03 05 08 00 00**). It indicates that the unlock combination 4 consists of only three people.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

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

15.5 Duress Options Settings

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

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


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

Function Description:

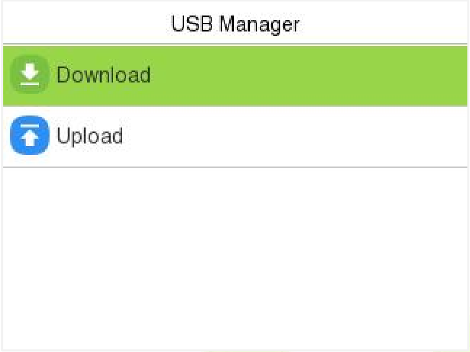
Function Name	Description
Alarm on Password	When a user uses the password verification method, an alarm signal will be generated, otherwise there will be no alarm signal.
Alarm on 1:1 Match	When a user uses the 1:1 verification method, an alarm signal will be generated, otherwise there will be no alarm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

16 USB Manager

You can import user information, access data and other data from a USB drive to computer or other devices.

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

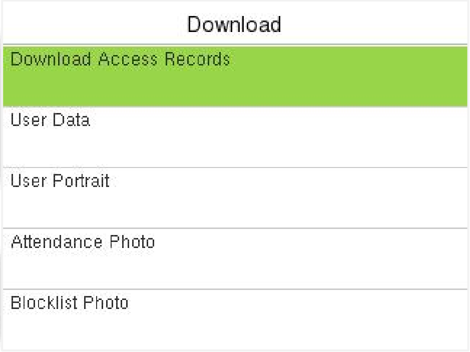
Select **USB Manager** on the main menu interface.



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

16.1 USB Download

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

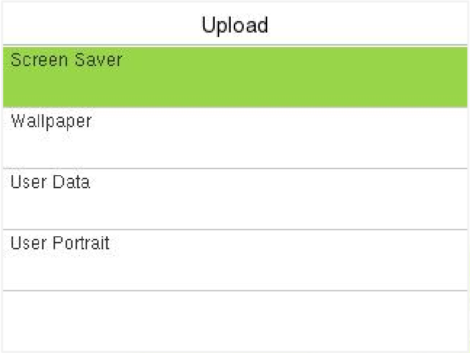


Menu	Description
Download Access Records	To download access record in specified time period into USB disk.
User Data	To download all user information from the device into USB disk.
User Portrait	To download all user portraits from the device into a USB disk.

Attendance Photo	To download all attendance photos from the device into USB disk.
Blocklist Photo	To download all blocklisted photos (photos taken after failed verifications) from the device into USB disk.

16.2 USB Upload

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

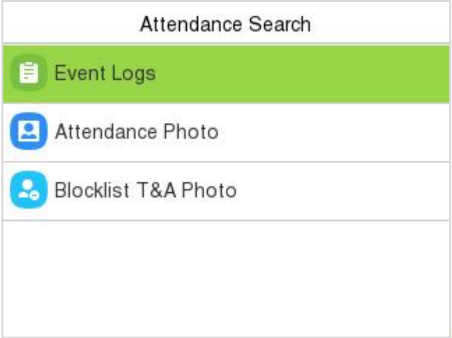


Menu	Description
Screen Save	To upload all screen savers from USB disk into the device. You can choose Upload selected photo or Upload all photos. The images will be displayed on the device's main interface after upload.
Wallpaper	To upload all wallpapers from USB disk into the device. You can choose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

17 Attendance Search

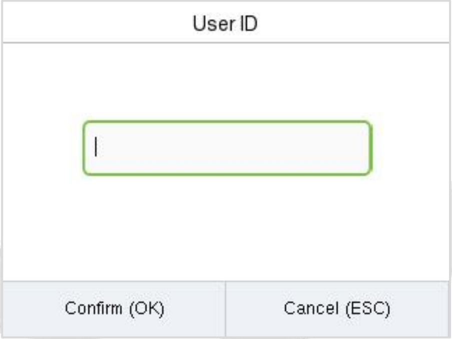
Once the identity of a user is verified, the access record is saved in the device. This function enables users to check their event logs.

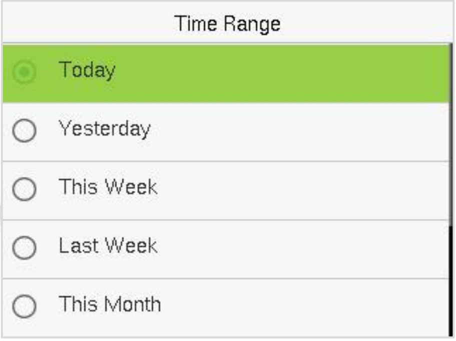
When the device is on the initial interface, press **M/OK** and select **Attendance Search** to search for the required event Logs.



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

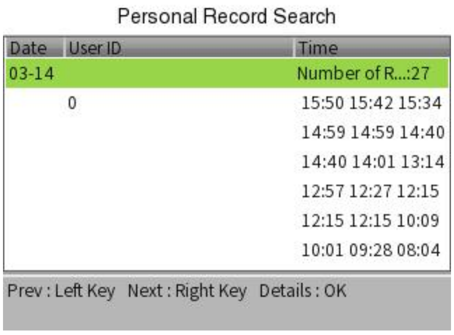
On the **Attendance Search** interface, select **Event Logs** to search for the required record.





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

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

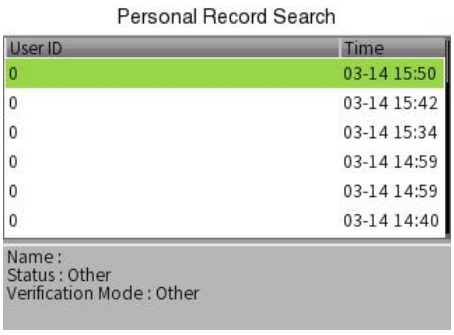


Personal Record Search

Date	User ID	Time
03-14		Number of R...:27
	0	15:50 15:42 15:34
		14:59 14:59 14:40
		14:40 14:01 13:14
		12:57 12:27 12:15
		12:15 12:15 10:09
		10:01 09:28 08:04

Prev : Left Key   Next : Right Key   Details : OK

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



Personal Record Search

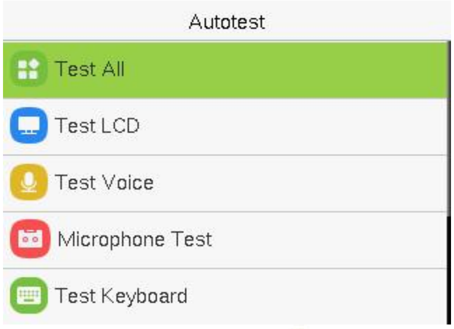
User ID	Time
0	03-14 15:50
0	03-14 15:42
0	03-14 15:34
0	03-14 14:59
0	03-14 14:59
0	03-14 14:40

Name :
Status : Other
Verification Mode : Other

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

18 Autotest

When the device is on the initial interface, press **M/OK** and select **Autotest**, it enables the system to automatically test whether the functions of various modules are working normally, including the LCD, Voice, Microphone, Keyboard, Fingerprint, Camera and Real-Time Clock (RTC).

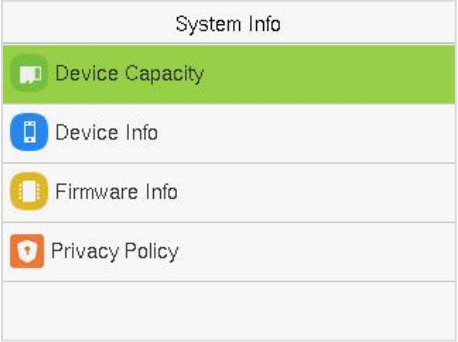


Function Description

Function Name	Description
Test All	To automatically test whether the LCD, Voice, Microphone, keyboard, Fingerprint, Camera and Real-Time Clock (RTC) are normal.
Test LCD	To automatically test the display effect of LCD screen by displaying full-color, pure white, and pure black to check whether the screen displays colors normally.
Test Voice	To automatically test whether the audio files stored in the device are complete and the voice quality is good.
Microphone test	To test if the microphone is working properly by speaking into the microphone.
Test Keyboard	The terminal tests whether every key on the keyboard works normally. Press any key on the **Test Keyboard** interface to check whether the pressed key matches the key displayed on the screen. The keys are displayed as dark grey before and turn green after pressed. Press **ESC** to exit the test.
Test Fingerprint Sensor	To test the fingerprint sensor by pressing a finger on the scanner to check if the acquired fingerprint image is clear. When you are pressing a finger on the scanner, the fingerprint image will display on the screen.
Cam Test	To test if the camera functions properly. (Same as "Test Face")
Test Clock RTC	To test the RTC. The device tests whether the clock works normally and accurately with a stopwatch. Press **M/OK** to start counting and press it again to stop counting.

19 System Information

When the device is on the initial interface, press **M/OK** and select **System Info** to view the storage status, version information of the device, firmware information and privacy policy.



System Info

Device Capacity

Device Info

Firmware Info

Privacy Policy

Function Description

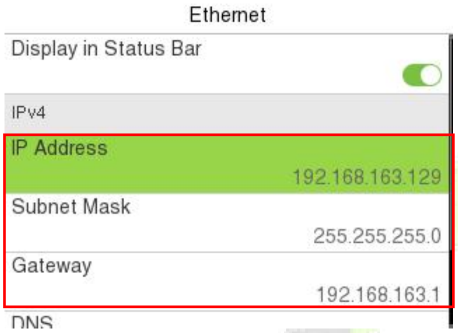
Function Name	Description
Device Capacity	Displays the current device's user storage, face, fingerprint, card and password storage, administrators, records, attendance, blocklist and profile photos.
Device Info	Displays the device's name, serial number, MAC address, Fingerprint algorithm, Face algorithm, Platform information, MCU Version and Manufacturer.
Firmware Info	Displays the firmware version and other version information of the device.
Privacy Policy	Display the device's privacy policy.

20 Connect to ZKBio CVAccess Software

20.1 Set the Communication Address

➢ **Device Side**

1. Press **M/OK** and enter **COMM.** > **Ethernet** to set the IP address and gateway of the device. (***Note:*** The IP address should be able to communicate with the ZKBio CVAccess server)
2. Press **M/OK** and enter **COMM.** > **Cloud Server Setting** to set the server address and server port.
   Server address: Set the IP address as of ZKBio CVAccess server.
   Server port: Set the server port as of ZKBio CVAccess.



Ethernet

Display in Status Bar

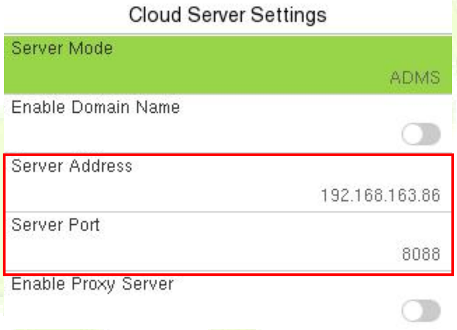
IPv4

IP Address 192.168.163.129

Subnet Mask 255.255.255.0

Gateway 192.168.163.1

DNS



Cloud Server Settings

Server Mode ADMS

Enable Domain Name

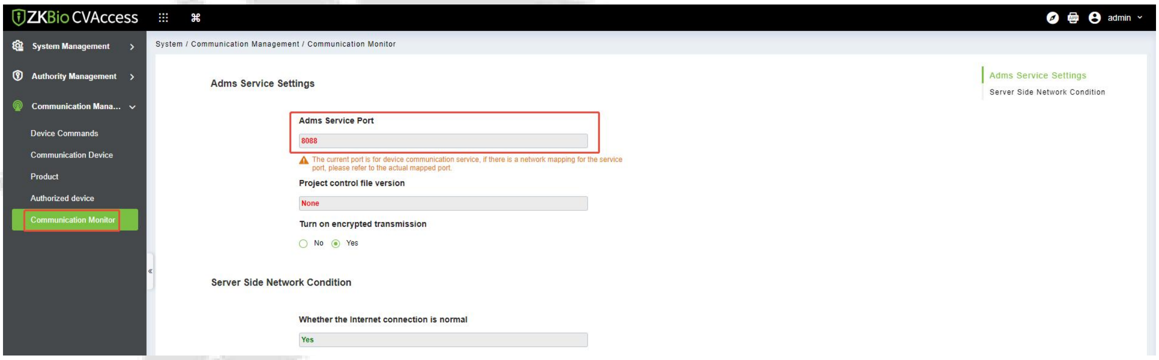
Server Address 192.168.163.86

Server Port 8088

Enable Proxy Server

➢ **Software Side**

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



System / Communication Management / Communication Monitor

Adms Service Settings

Adms Service Port: 8088

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

Project control file version: None

Turn on encrypted transmission: ○ No ● Yes

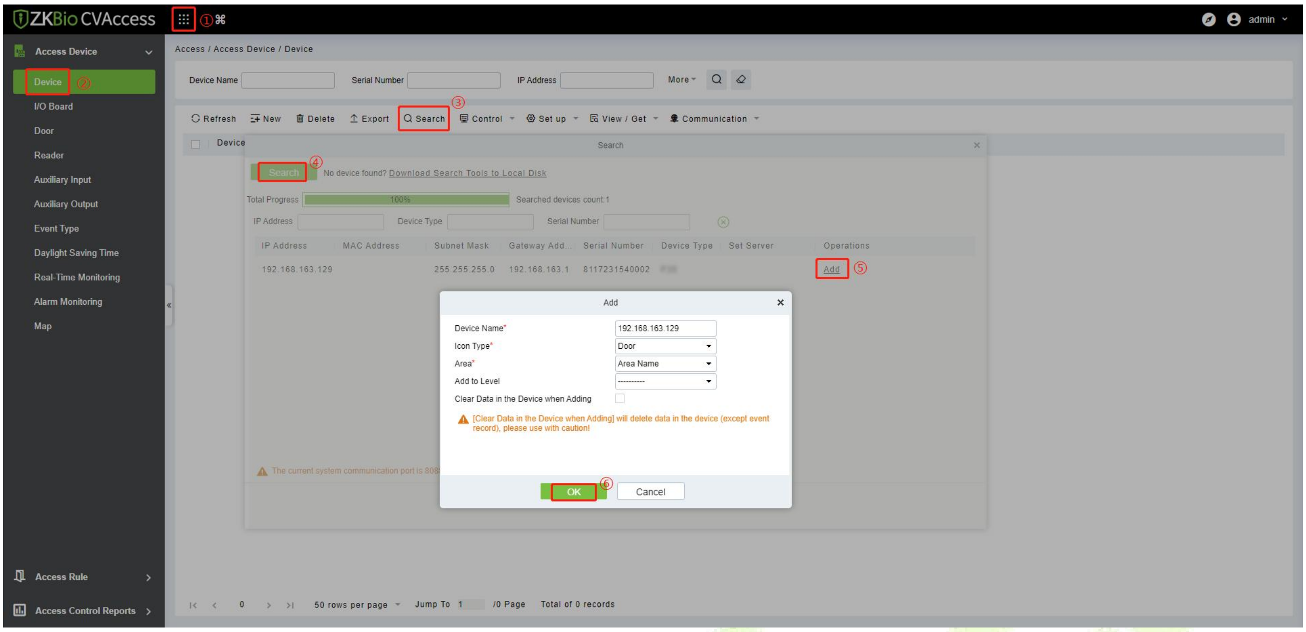
Server Side Network Condition

Whether the Internet connection is normal: Yes

20.2 Add Device on the Software

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

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



IP Address	MAC Address	Subnet Mask	Gateway Add...	Serial Number	Device Type	Set Server	Operations
192.168.163.129		255.255.255.0	192.168.163.1	8117231540002			Add

Add

Device Name* 192.168.163.129

Icon Type* Door

Area* Area Name

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

Clear Data in the Device when Adding □

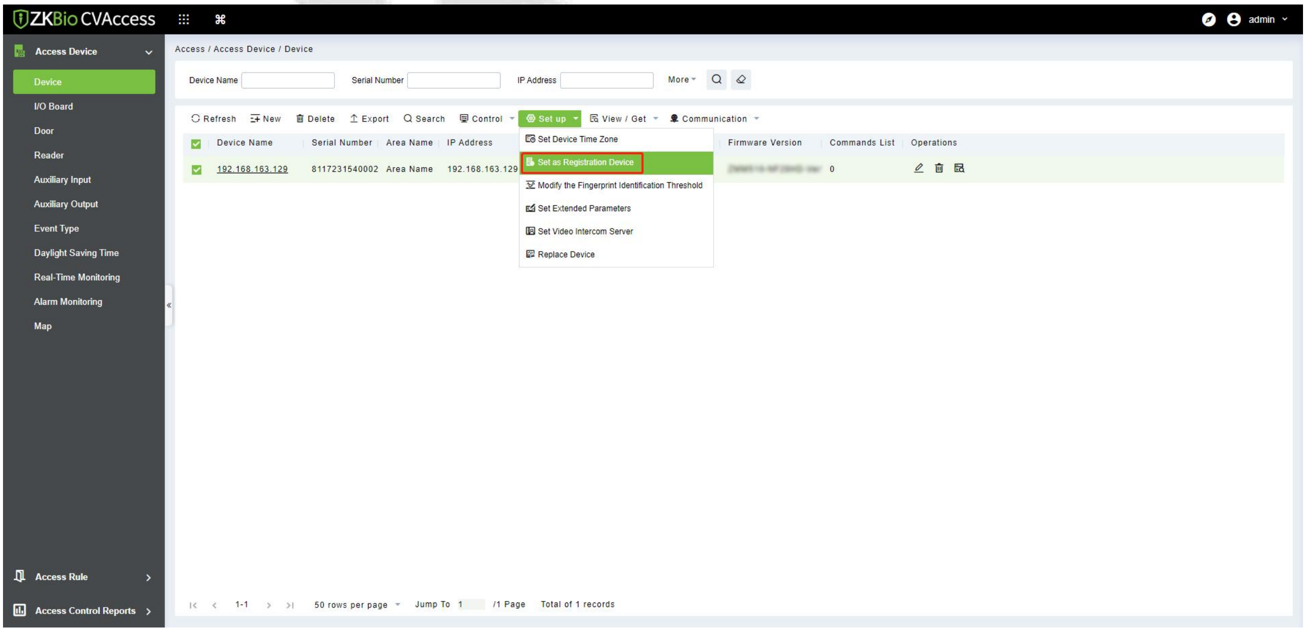
[Clear Data in the Device when Adding] will delete data in the device (except event record), please use with caution!

The current system communication port is 808

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.

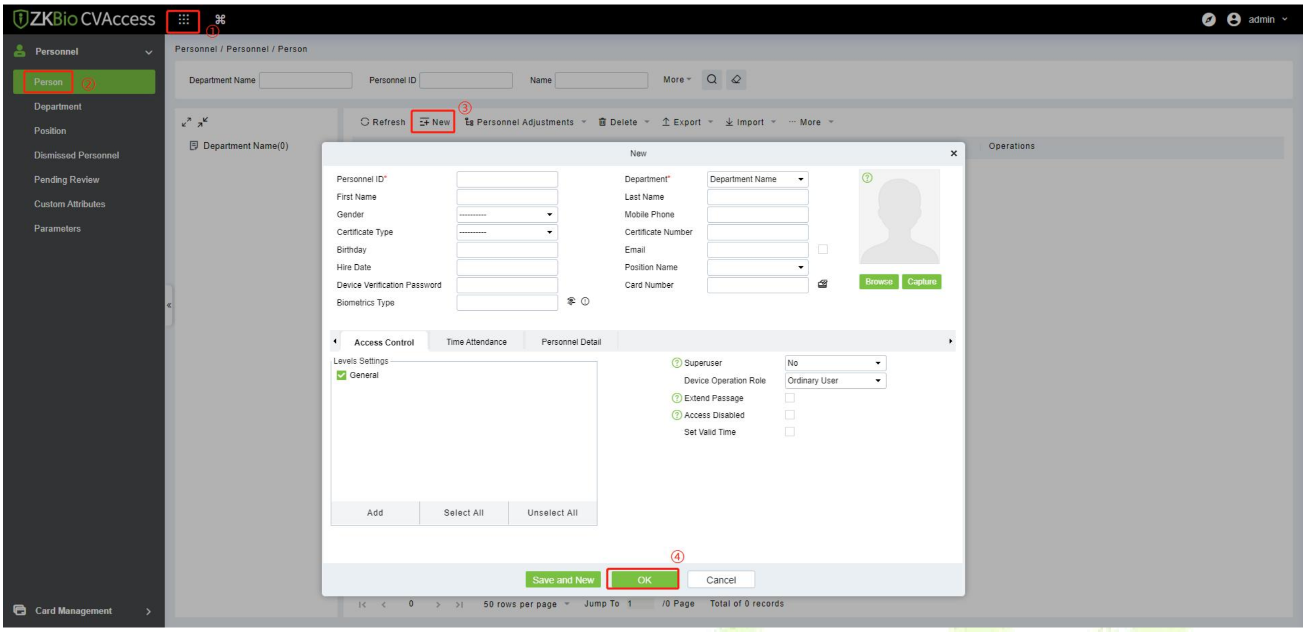
20.3 Add Personnel on the Software and Online Fingerprint/Face Registration

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

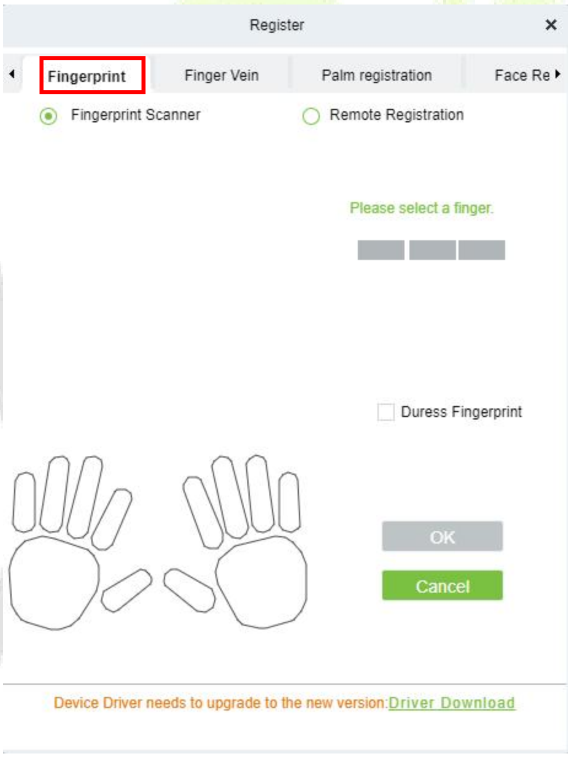


☑	Device Name	Serial Number	Area Name	IP Address	Firmware Version	Commands List	Operations
☑	192.168.163.129	8117231540002	Area Name	192.168.163.129		0	

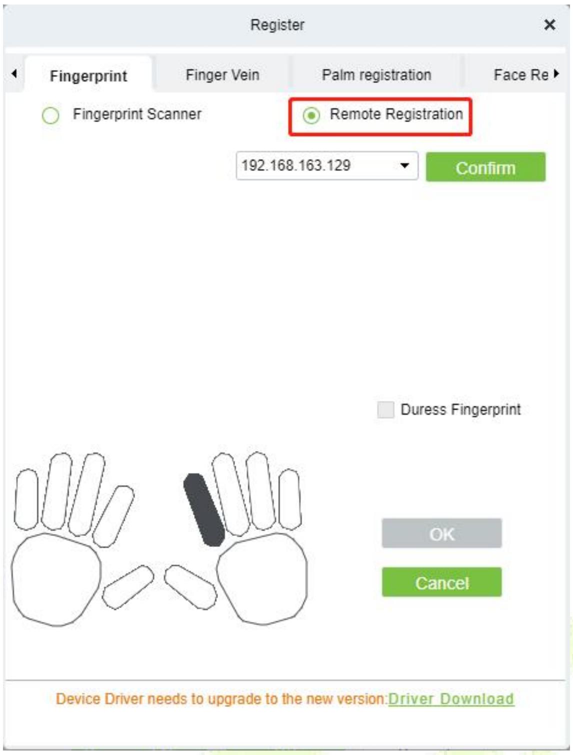
2. Click **Personnel** > **Person** > **New**:



3. Fill in all the required fields of the user and click and select **Fingerprint** to enter the online fingerprint registration interface.

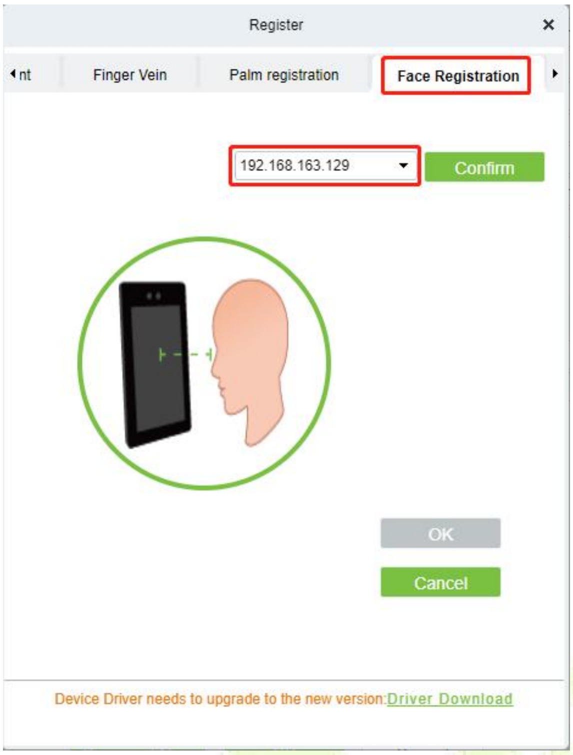


4. Click **Driver Download** to install the driver first.
5. Select **Remote Registration**, then select the IP address of the device and the finger you want to register, click **Confirm**.



Device Driver needs to upgrade to the new version:Driver Download

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



Device Driver needs to upgrade to the new version:Driver Download

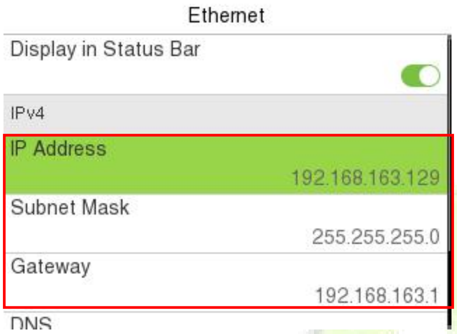
9. After the device prompts “Face registration begin”, face towards the camera and keep the face in the centre of the screen and stay still during face registration. If the face is successfully registered, the device will prompt "Registered successfully".
10. Click **OK** to save the user.
11. Click **Access** > **Device** > **Control** > **Synchronize All Data to Devices** to synchronize all the data to the device including the new users.

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

21 Connect to ZKBio Time Software

21.1 Set the Communication Address

1. Press **M/OK** and enter **COMM.** > **Ethernet** to set the IP address and gateway of the device. (***Note:*** The IP address should be able to communicate with the ZKBio Time server)
2. Press **M/OK** and enter **COMM.** > **Cloud Server Setting** to set the server address and server port.
   Server address: Set the IP address as of ZKBio Time server.
   Server port: Set the server port as of ZKBio Time server.



Ethernet

Display in Status Bar: on

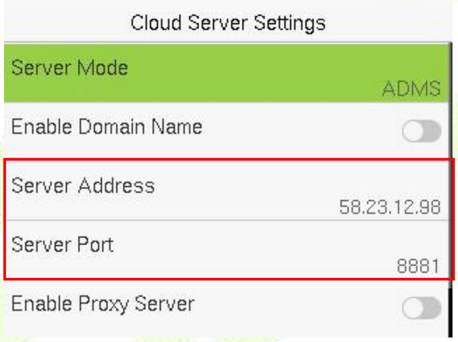
IPv4

IP Address: 192.168.163.129

Subnet Mask: 255.255.255.0

Gateway: 192.168.163.1

DNS



Cloud Server Settings

Server Mode: ADMS

Enable Domain Name: off

Server Address: 58.23.12.98

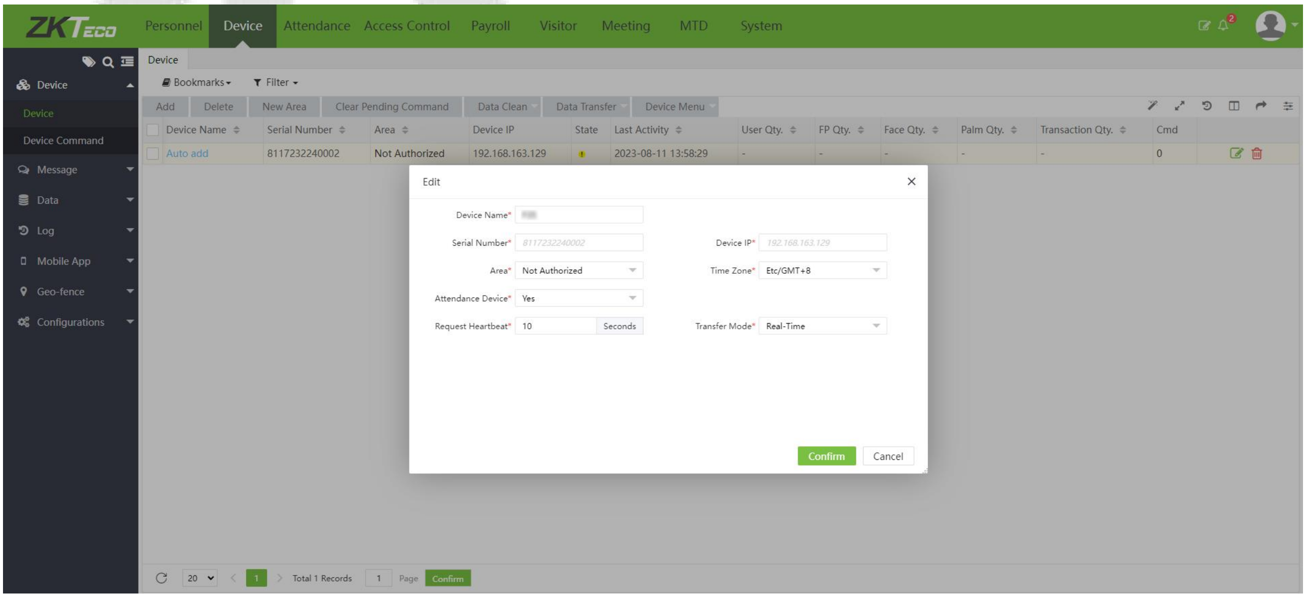
Server Port: 8881

Enable Proxy Server: off

21.2 Add Device on the Software

After setting on the device, the device will be automatically added to the software. Open the ZKBio Time software then select [**Device Module**] > [**Device**] > [**Device**], click the device in the list, change the Device Name and Area.

Note: The devices added automatically must be assigned to custom areas to communicate with the software.



Device Name	Serial Number	Area	Device IP	State	Last Activity	User Qty.	FP Qty.	Face Qty.	Palm Qty.	Transaction Qty.	Cmd
Auto add	8117232240002	Not Authorized	192.168.163.129	!	2023-08-11 13:58:29	-	-	-	-	-	0

Edit

Device Name*: [redacted]

Serial Number*: 8117232240002

Device IP*: 192.168.163.129

Area*: Not Authorized

Time Zone*: Etc/GMT+8

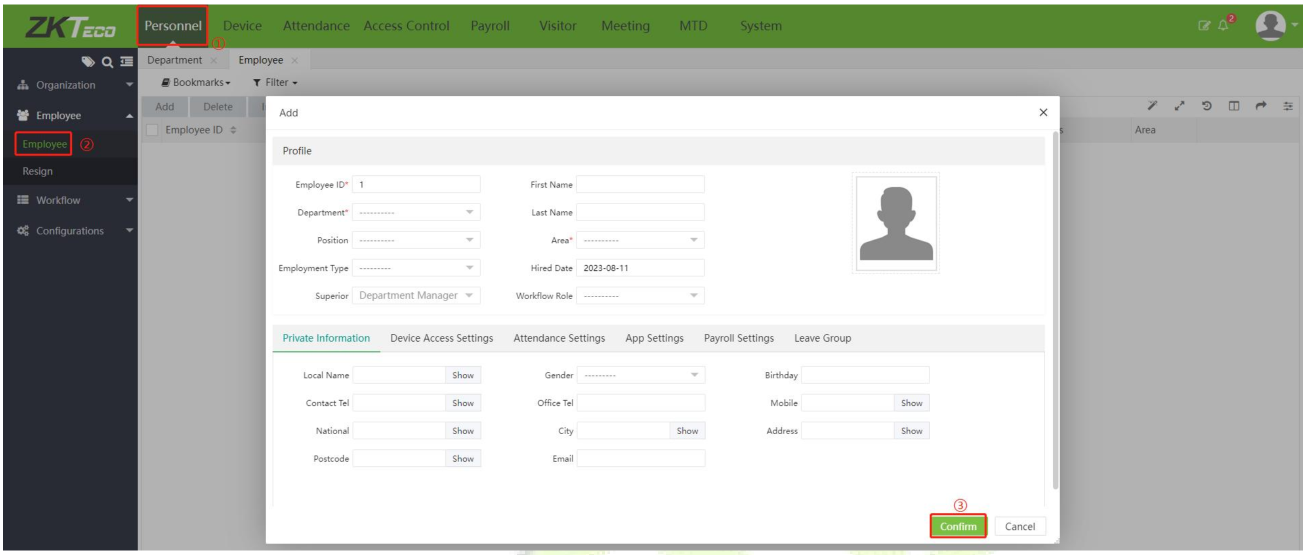
Attendance Device*: Yes

Request Heartbeat*: 10 Seconds

Transfer Mode*: Real-Time

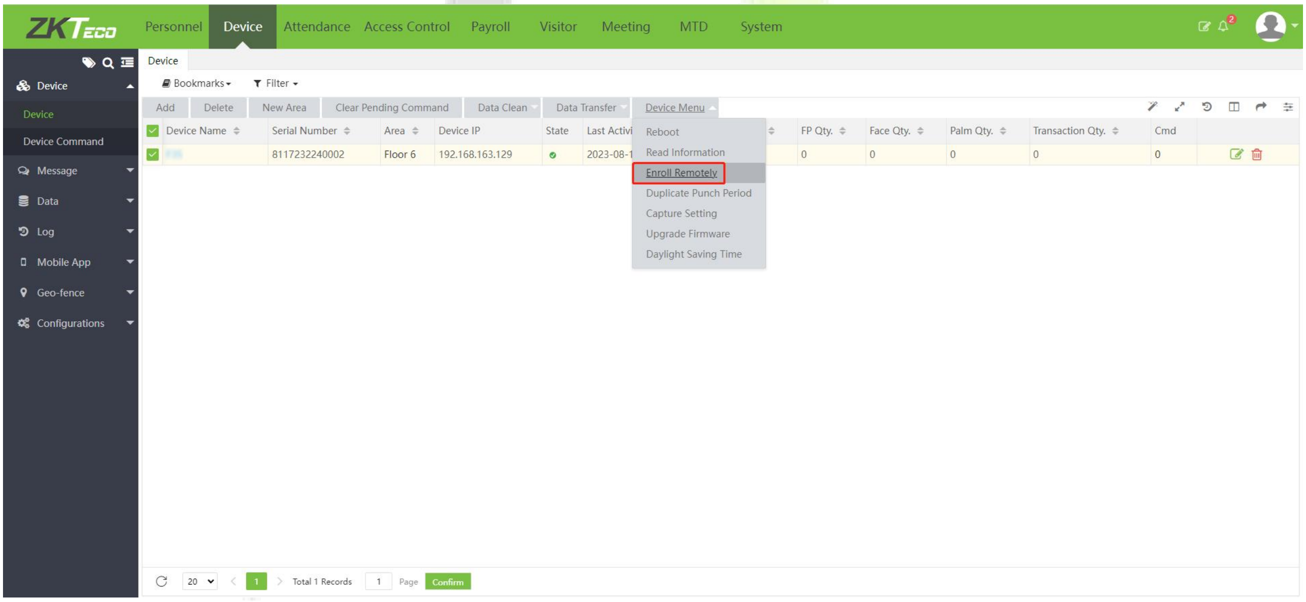
21.3 Add Personnel on the Software and Online Fingerprint Registration

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



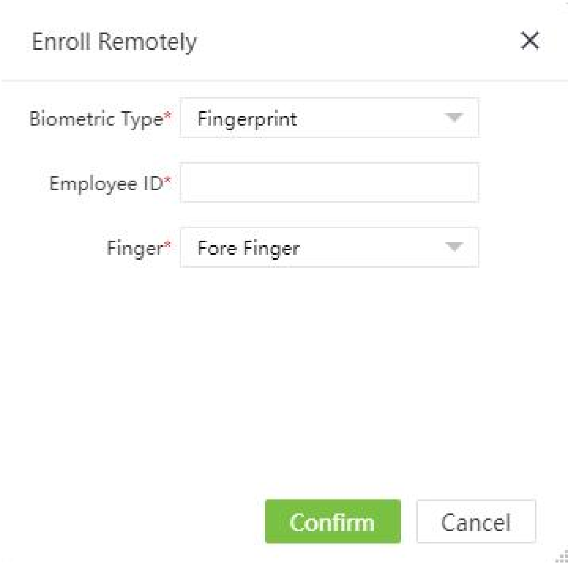
Employee ID*	1	First Name			
Department*	---------	Last Name			
Position	---------	Area*	---------		
Employment Type	---------	Hired Date	2023-08-11		
Superior	Department Manager	Workflow Role	---------		
Local Name		Gender	---------	Birthday	
Contact Tel		Office Tel		Mobile	
National		City		Address	
Postcode		Email			

2. Fill in all the required fields and click [**Confirm**] to register a new user.
3. Click **Device** > **Device**, select the device and click **Device Menu** > **Enroll Remotely**.



☑	Device Name	Serial Number	Area	Device IP	State	Last Activi	FP Qty.	Face Qty.	Palm Qty.	Transaction Qty.	Cmd
☑	[redacted]	8117232240002	Floor 6	192.168.163.129	●	2023-08-1	0	0	0	0	0

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



Enroll Remotely

Biometric Type* Fingerprint

Employee ID*

Finger* Fore Finger

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

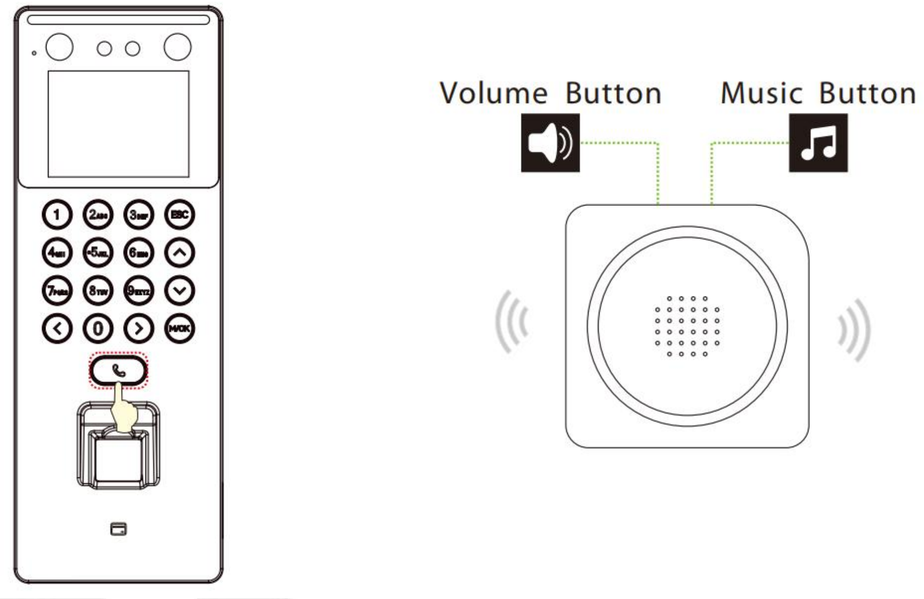
Note: For other specific operations, please refer the *ZKBio Time User Manual*.

22 Connecting to Wireless Doorbell★

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

22.1 Connect the Wireless Doorbell

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



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

Note:

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

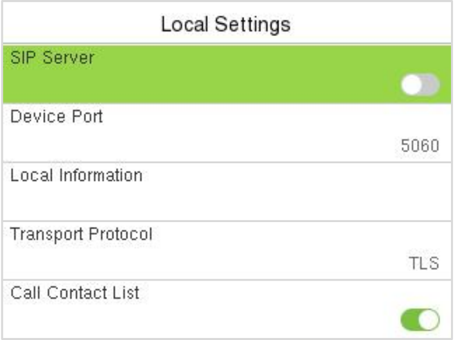
22.2 Unbinding the Wireless Doorbell

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

23 SIP Video Intercom

23.1 Local Area Network Use

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



Local Settings

SIP Server ○

Device Port 5060

Local Information

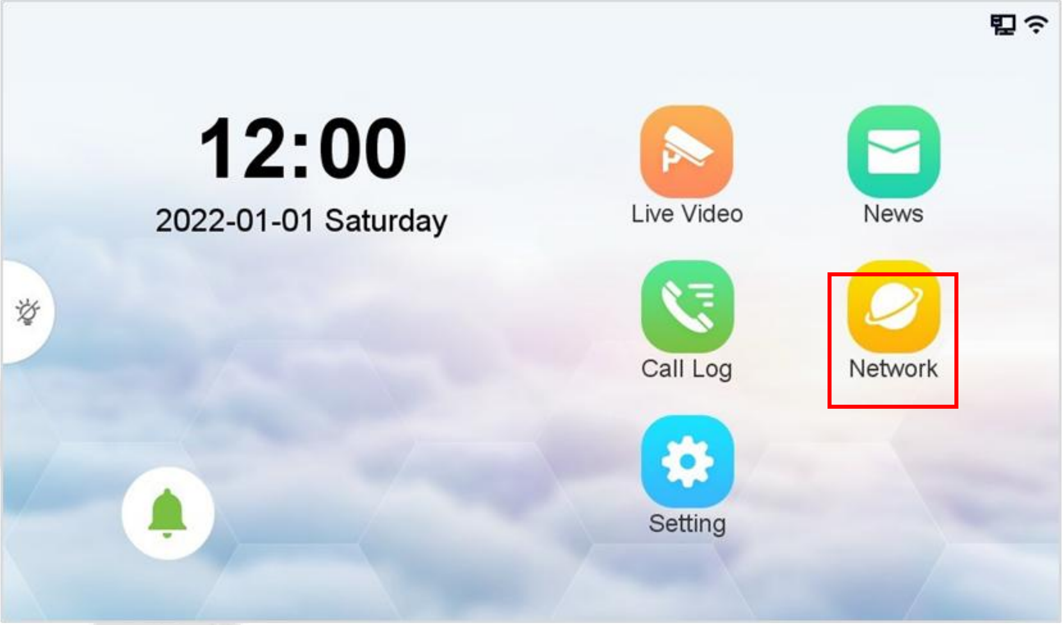
Transport Protocol TLS

Call Contact List ●

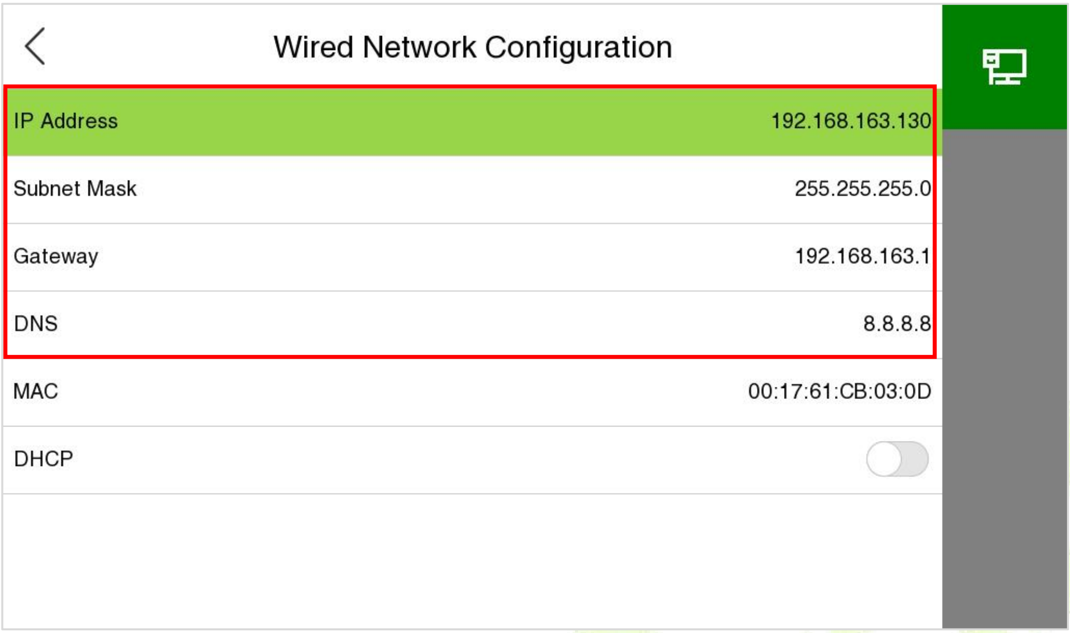
This function needs to be used with the indoor monitor VT07-B01.

- **On the Indoor Monitor:**

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



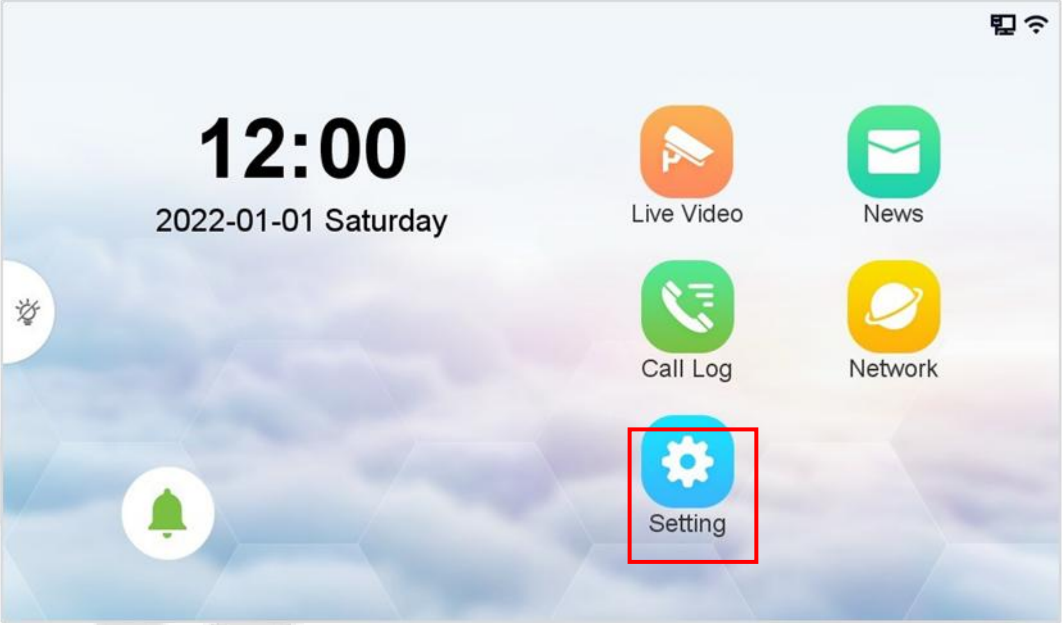
2. Set the IP Address and Gateway of the indoor monitor. (**Note:** The IP address should be in the same network segment as the device.)

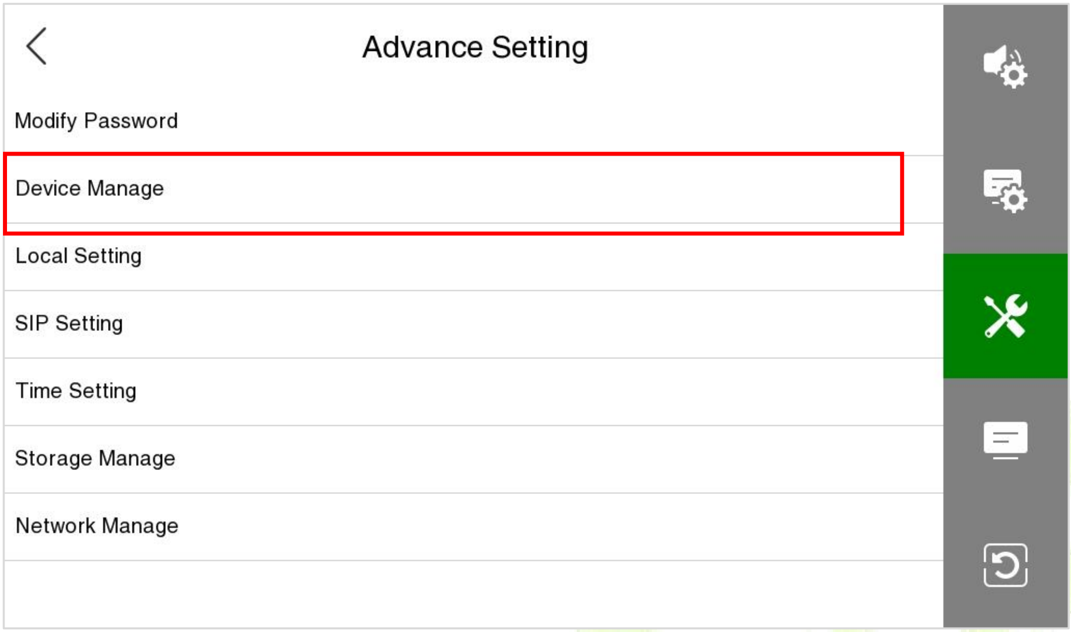


Wired Network Configuration

IP Address	192.168.163.130
Subnet Mask	255.255.255.0
Gateway	192.168.163.1
DNS	8.8.8.8
MAC	00:17:61:CB:03:0D
DHCP	○

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





Advance Setting

Modify Password

Device Manage

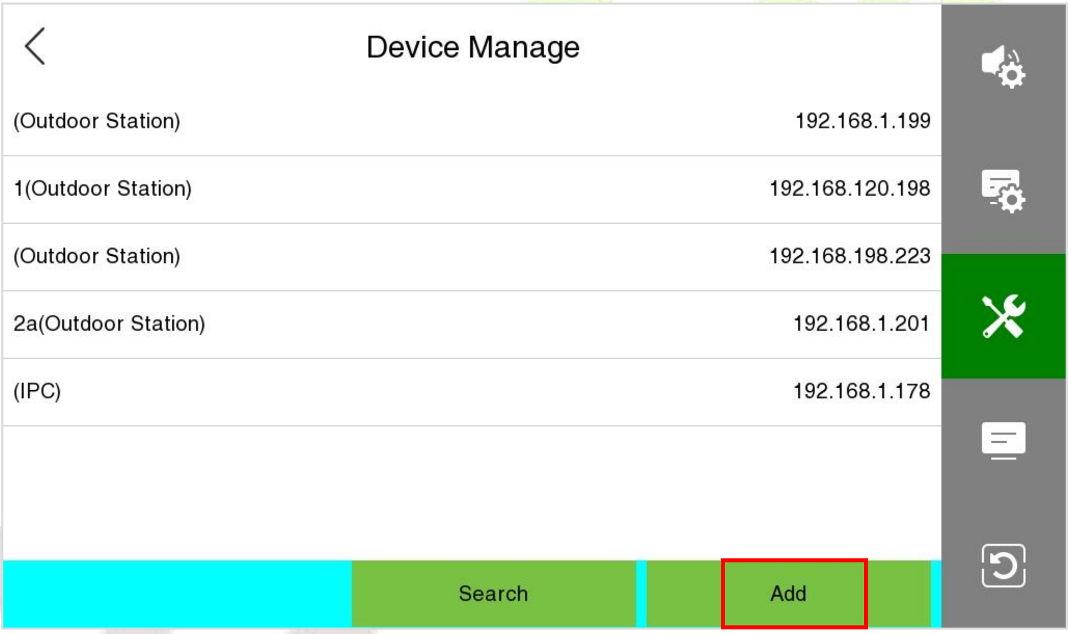
Local Setting

SIP Setting

Time Setting

Storage Manage

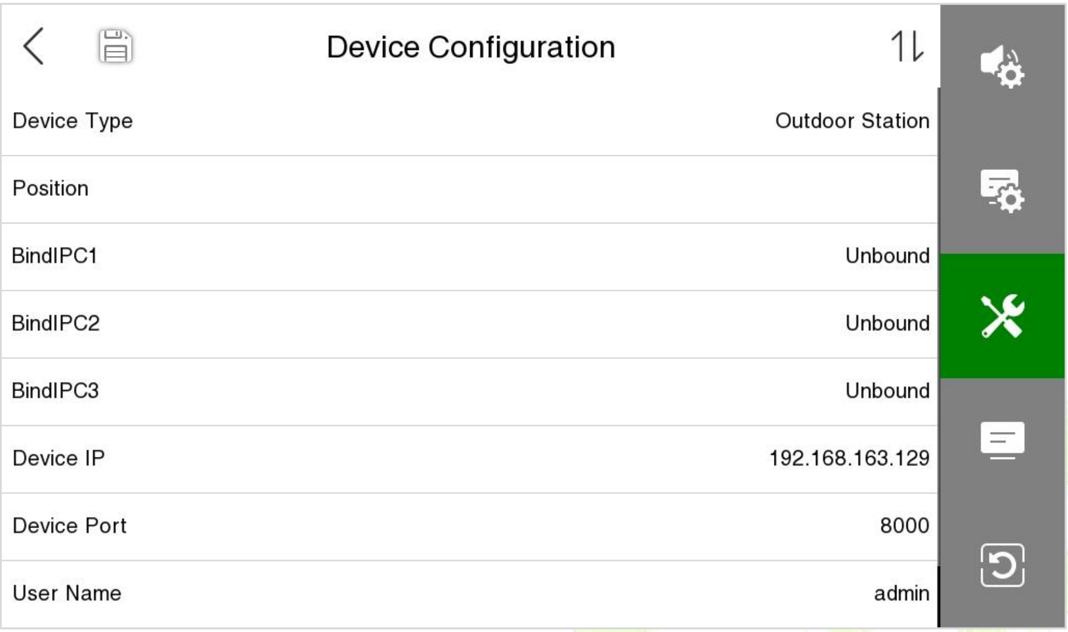
Network Manage



Device Manage

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

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

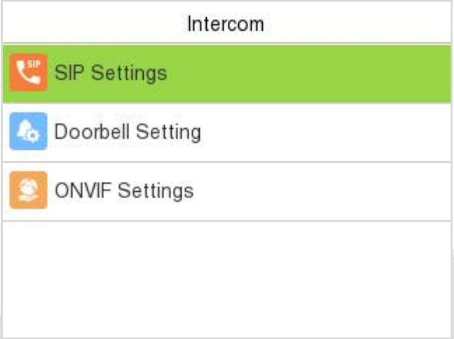


Device Configuration

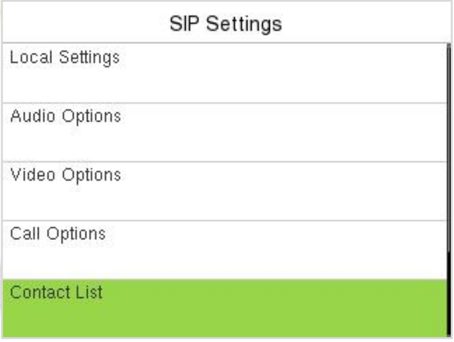
Device Type	Outdoor Station
Position	
BindIPC1	Unbound
BindIPC2	Unbound
BindIPC3	Unbound
Device IP	192.168.163.129
Device Port	8000
User Name	admin

- **On the Device:**

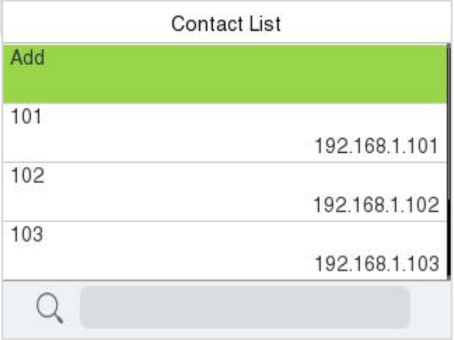
1. Press **M/OK** key and enter **[Intercom]** > **[SIP Settings]** > **[Contact List]** > **[Add]** to add the connected indoor monitors.



Intercom



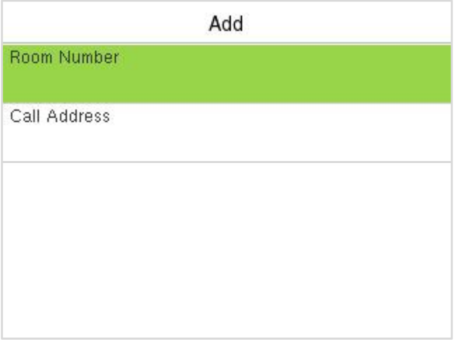
SIP Settings



Contact List

Add

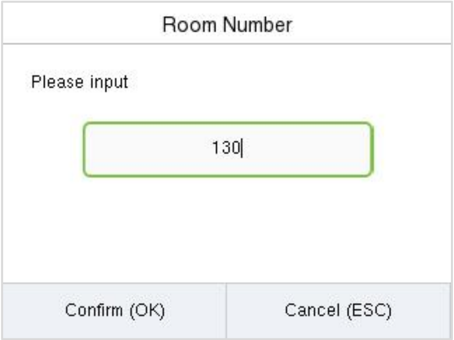
101	192.168.1.101
102	192.168.1.102
103	192.168.1.103



Add

Room Number: Customize the number of the indoor monitor.

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

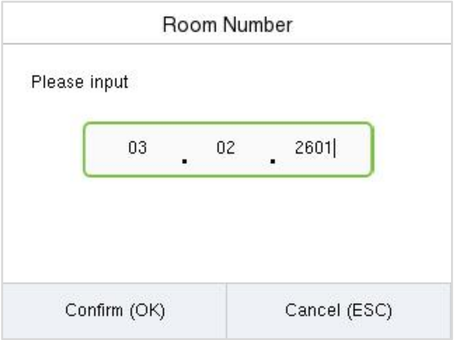


Room Number

Please input

130

Entrance Station



Room Number

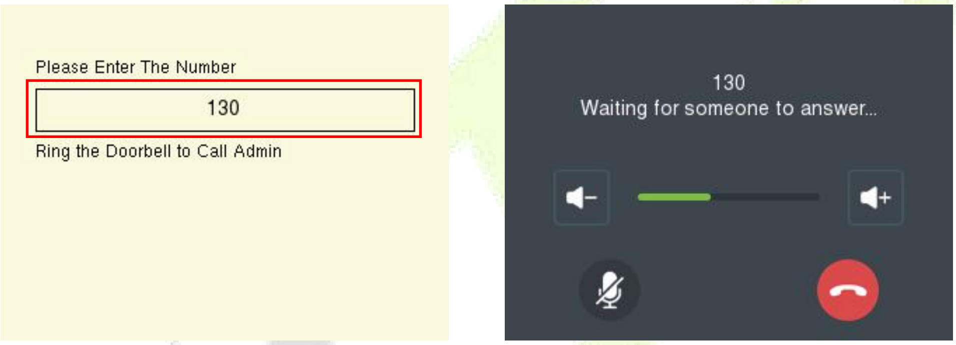
Please input

03 . 02 . 2601

Fence Terminal

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

2. To enable the video intercom function, press the doorbell button ☎ on the device and enter the number or IP address of the indoor monitor in the provided interface.



Please Enter The Number

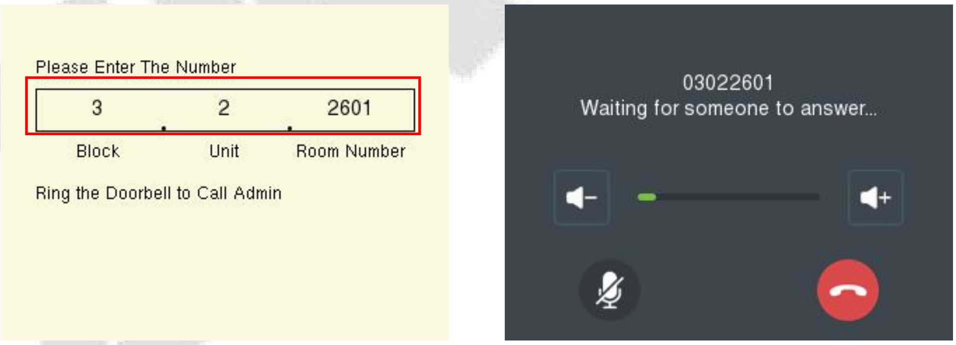
130

Ring the Doorbell to Call Admin

130

Waiting for someone to answer...

Entrance Station



Please Enter The Number

3 . 2 . 2601

Ring the Doorbell to Call Admin

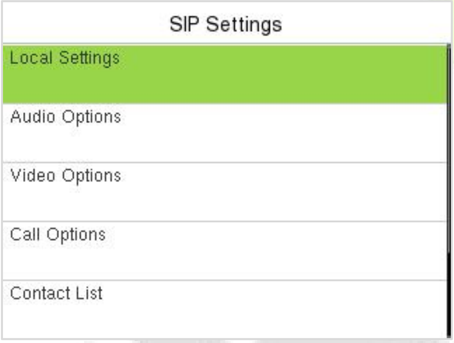
03022601

Waiting for someone to answer...

Fence Terminal

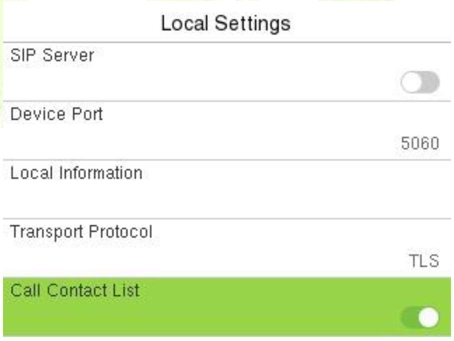
23.1.1 Call Contact List

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



SIP Settings

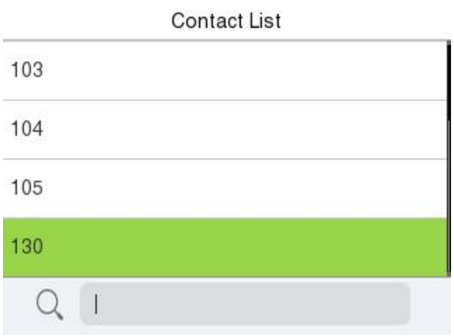
- Local Settings
- Audio Options
- Video Options
- Call Options
- Contact List



Local Settings

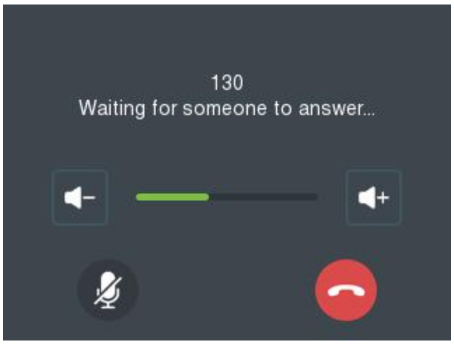
SIP Server	○
Device Port	5060
Local Information	
Transport Protocol	TLS
Call Contact List	●

2. Press the doorbell button ☎ on the device to enter the call page, then you can press the **Up** key to open the contact list, select the number of the indoor monitor you want to call.



Contact List

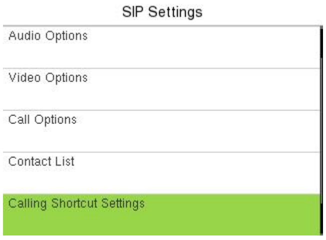
- 103
- 104
- 105
- 130

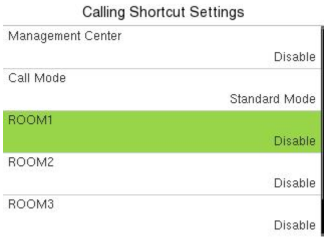


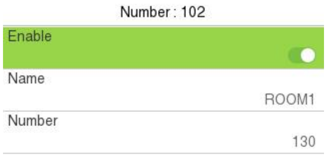
130
Waiting for someone to answer...

23.1.2 Custom the Calling Shortcut Keys

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


SIP Settings
Audio Options
Video Options
Call Options
Contact List
Calling Shortcut Settings

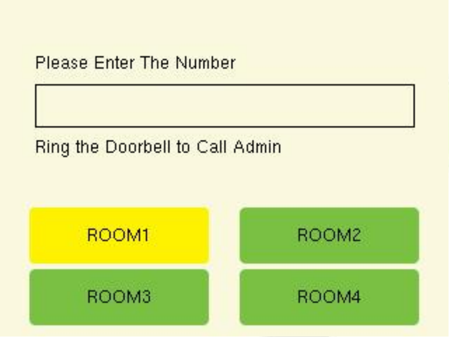

Calling Shortcut Settings
Management Center — Disable
Call Mode — Standard Mode
ROOM1 — Disable
ROOM2 — Disable
ROOM3 — Disable

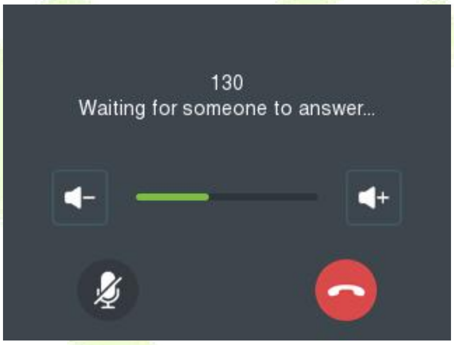

Number : 102
Enable
Name — ROOM1
Number — 130

Name: Customize the name of the shortcut keys.

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

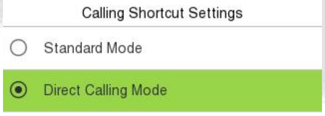
2. Then you can press the doorbell button ☎ on the device and select the calling shortcut keys to call the indoor monitor.

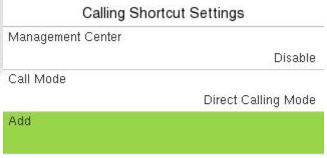

Please Enter The Number
Ring the Doorbell to Call Admin
ROOM1 ROOM2
ROOM3 ROOM4

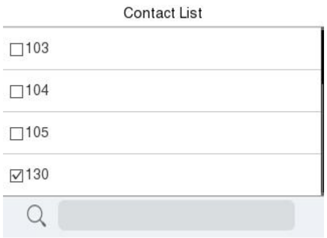

130
Waiting for someone to answer...

23.1.3 Direct Calling

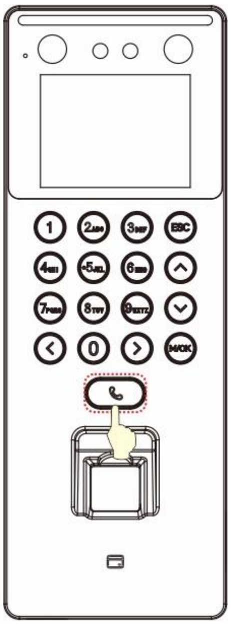
1. On the **SIP Settings** interface, enter [**Calling Shortcut Settings**] > [**Call Mode**] > [**Direct Calling Mode**] > [**Add**]. Select the IP address of the indoor monitors that you want to call, then the indoor monitors will be displayed in the list.

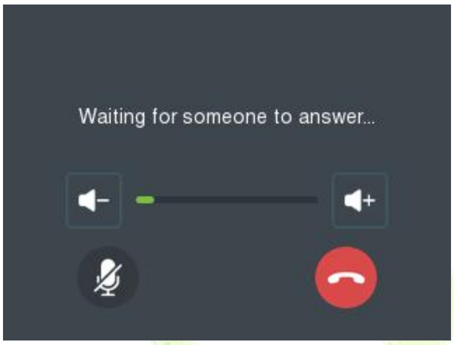

Calling Shortcut Settings
○ Standard Mode
● Direct Calling Mode


Calling Shortcut Settings
Management Center — Disable
Call Mode — Direct Calling Mode
Add


Contact List
□103
□104
□105
☑130

2. Then you can press the doorbell button ☎ on the device to call the indoor monitors directly.

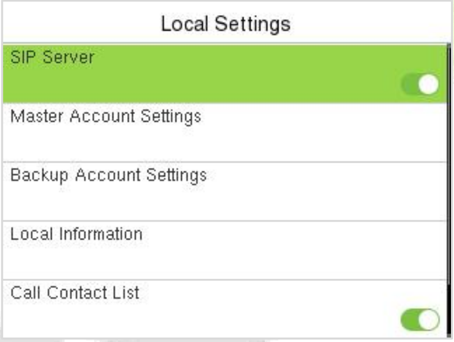




Waiting for someone to answer...

23.2 SIP Server

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



Local Settings

SIP Server

Master Account Settings

Backup Account Settings

Local Information

Call Contact List

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

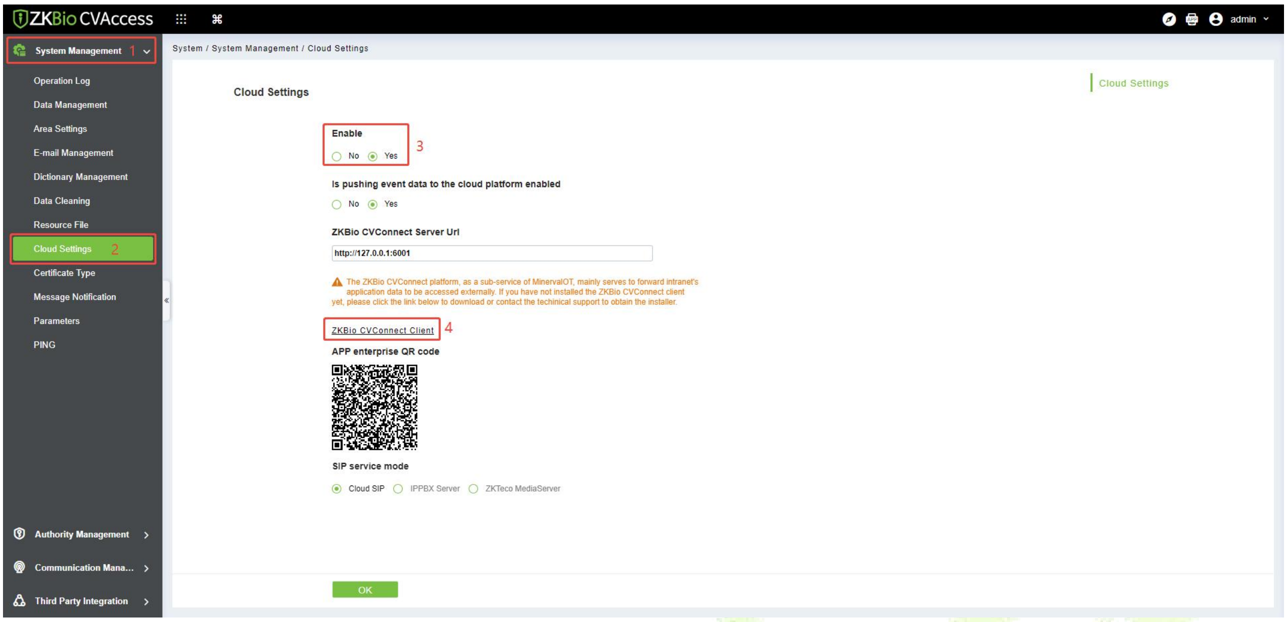
ZKBio CVAccess supports 2 kinds of SIP server: **cloud SIP** and **PBX server**, users can choose one according to the actual situation.

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

The following text mainly introduces the Cloud SIP mode.

23.2.1 SIP Server Configuration

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



System / System Management / Cloud Settings

Cloud Settings

Enable

○ No ● Yes

Is pushing event data to the cloud platform enabled

○ No ● Yes

ZKBio CVConnect Server Url

http://127.0.0.1:6001

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

ZKBio CVConnect Client

APP enterprise QR code

SIP service mode

● Cloud SIP ○ IPPBX Server ○ ZKTeco MediaServer

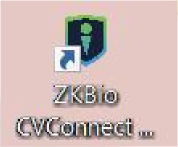
Note:

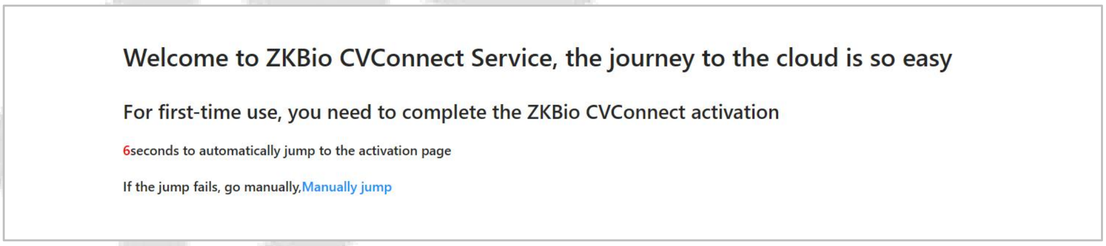
1) Ensure the ZKBio CVConnect client is installed if Cloud SIP is activated.

2) After cloud SIP is enabled, the device network needs to be able to connect to the external network before it can be used.

➢ ZKBio CVConnect Client Activation Steps

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





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

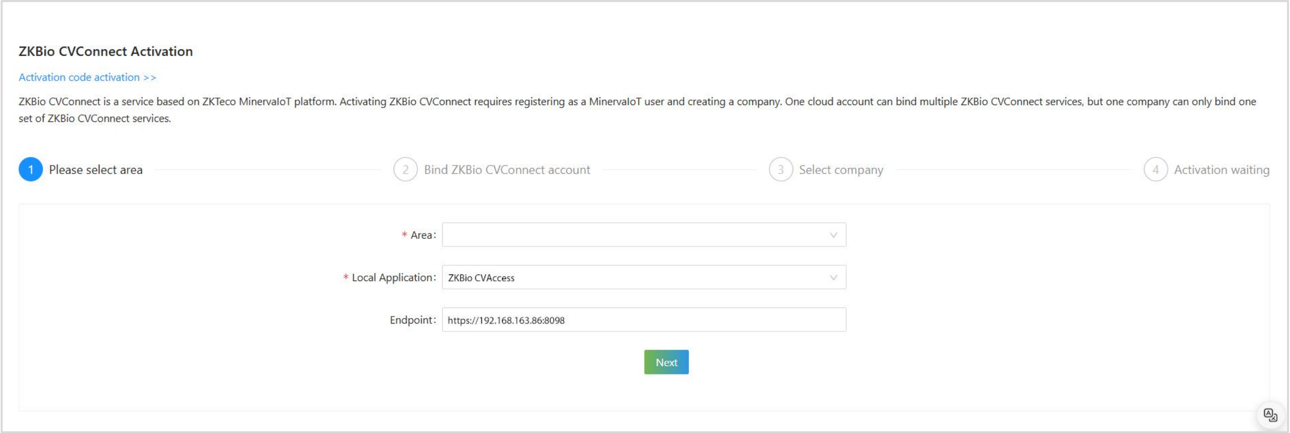
For first-time use, you need to complete the ZKBio CVConnect activation

6seconds to automatically jump to the activation page

If the jump fails, go manually,Manually jump

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

1. Select Area



ZKBio CVConnect Activation

Activation code activation >>

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

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

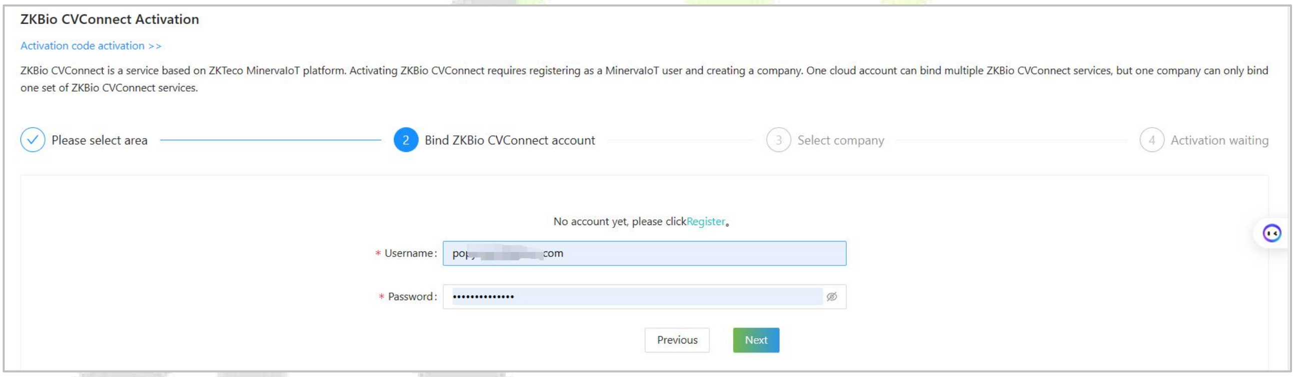
* Area:

* Local Application: ZKBio CVAccess

Endpoint: https://192.168.163.86:8098

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

2. Bind ZKBio CVConnect Account



ZKBio CVConnect Activation

Activation code activation >>

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

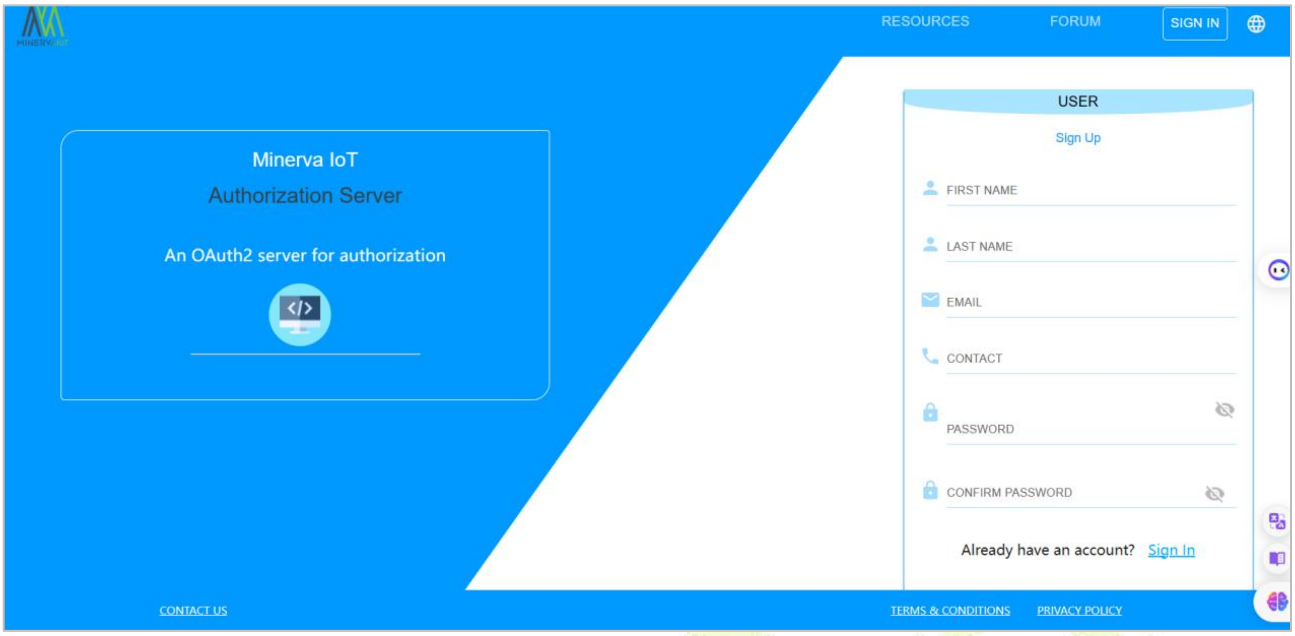
✓ Please select area — 2 Bind ZKBio CVConnect account — 3 Select company — 4 Activation waiting

No account yet, please clickRegister。

* Username: pop[redacted]com

* Password: ••••••••••••••

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



Minerva IoT

Authorization Server

An OAuth2 server for authorization

USER

Sign Up

FIRST NAME

LAST NAME

EMAIL

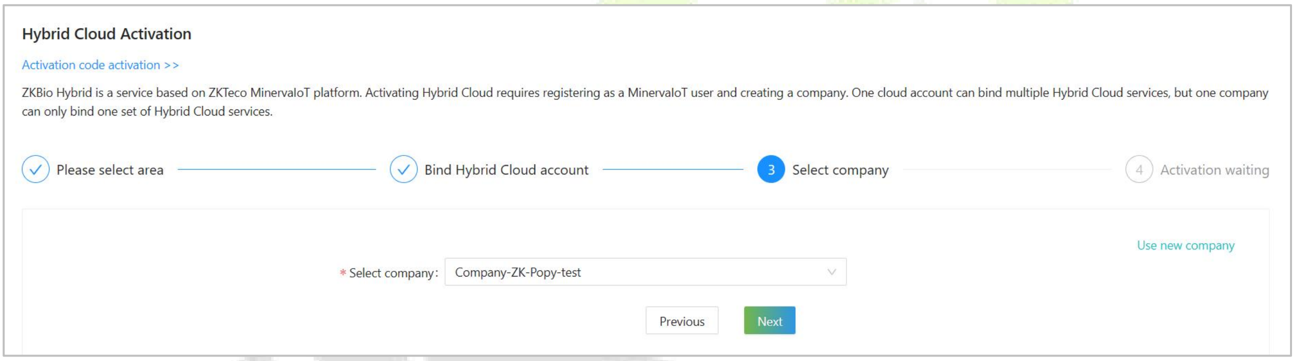
CONTACT

PASSWORD

CONFIRM PASSWORD

Already have an account? Sign In

3. Select Company



Hybrid Cloud Activation

Activation code activation >>

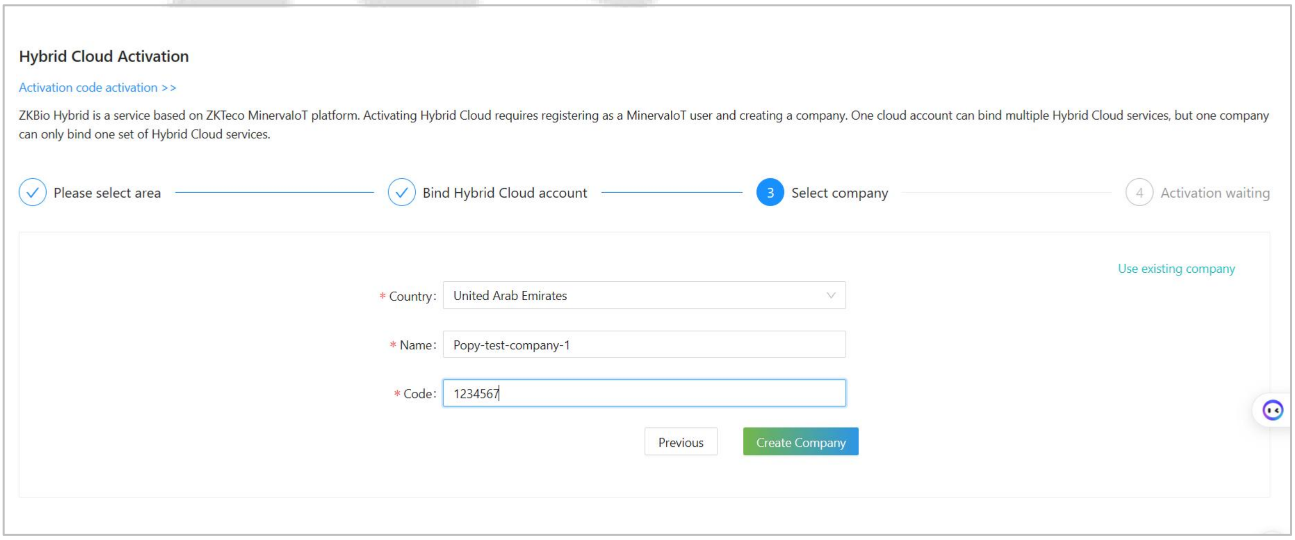
ZKBio Hybrid is a service based on ZKTeco MinervaIoT platform. Activating Hybrid Cloud requires registering as a MinervaIoT user and creating a company. One cloud account can bind multiple Hybrid Cloud services, but one company can only bind one set of Hybrid Cloud services.

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

Use new company

* Select company: Company-ZK-Popy-test

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



Hybrid Cloud Activation

Activation code activation >>

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

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

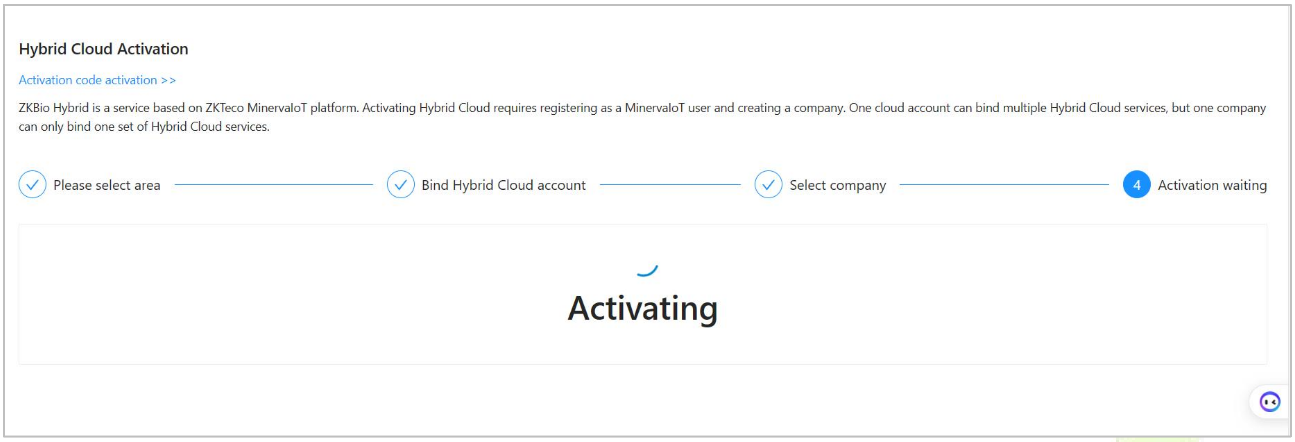
Use existing company

* Country: United Arab Emirates

* Name: Popy-test-company-1

* Code: 1234567

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



Hybrid Cloud Activation

Activation code activation >>

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

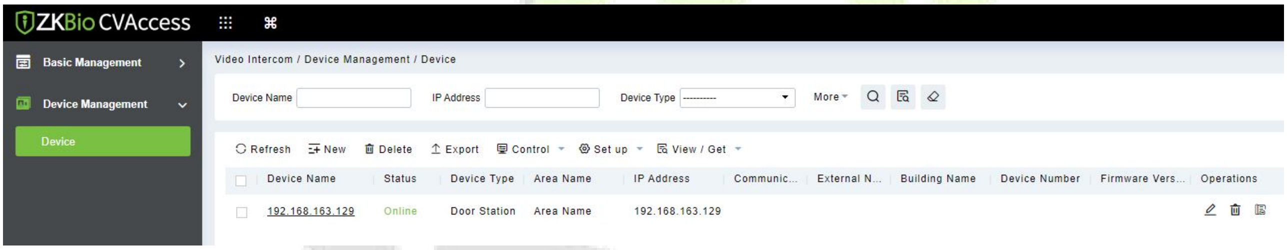
✓ Please select area — ✓ Bind Hybrid Cloud account — ✓ Select company — 4 Activation waiting

Activating

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

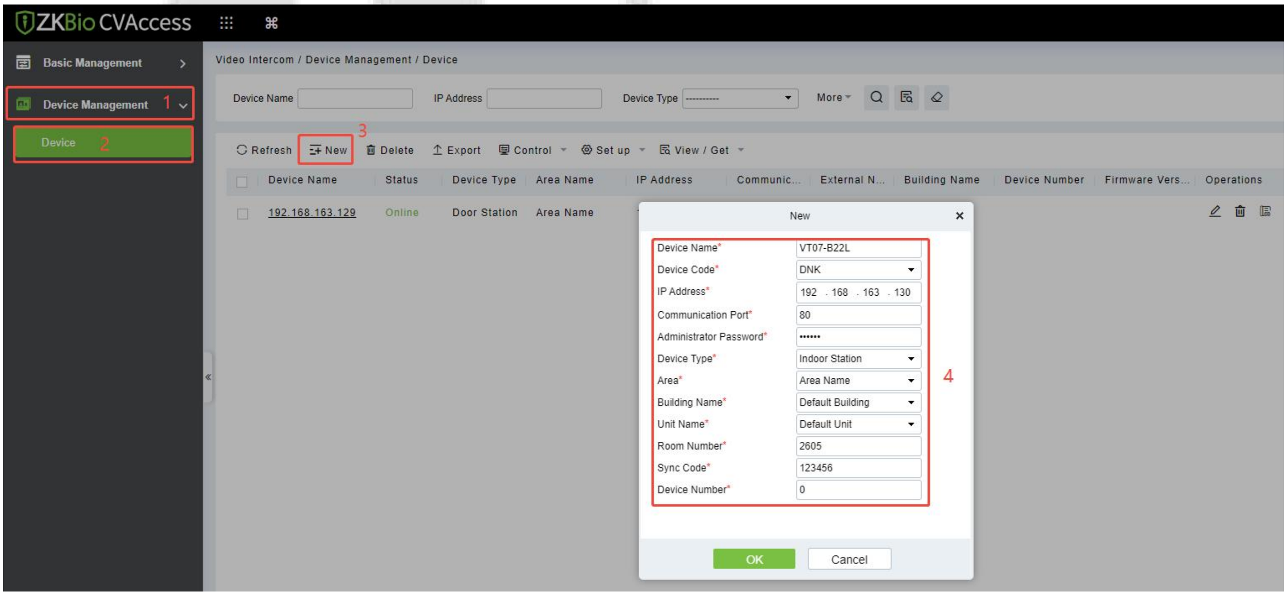
23.2.2 Add Device

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 [20 Connect to ZKBio CVAccess Software](#))



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

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

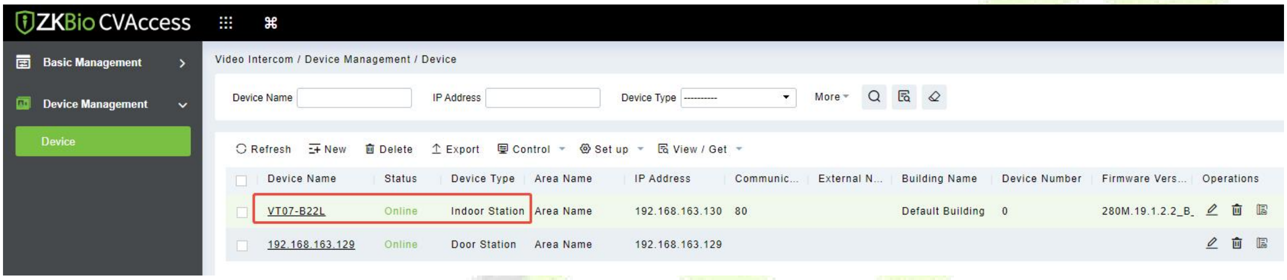


Device Name*	VT07-B22L
Device Code*	DNK
IP Address*	192 . 168 . 163 . 130
Communication Port*	80
Administrator Password*	••••••
Device Type*	Indoor Station
Area*	Area Name
Building Name*	Default Building
Unit Name*	Default Unit
Room Number*	2605
Sync Code*	123456
Device Number*	0

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

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

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



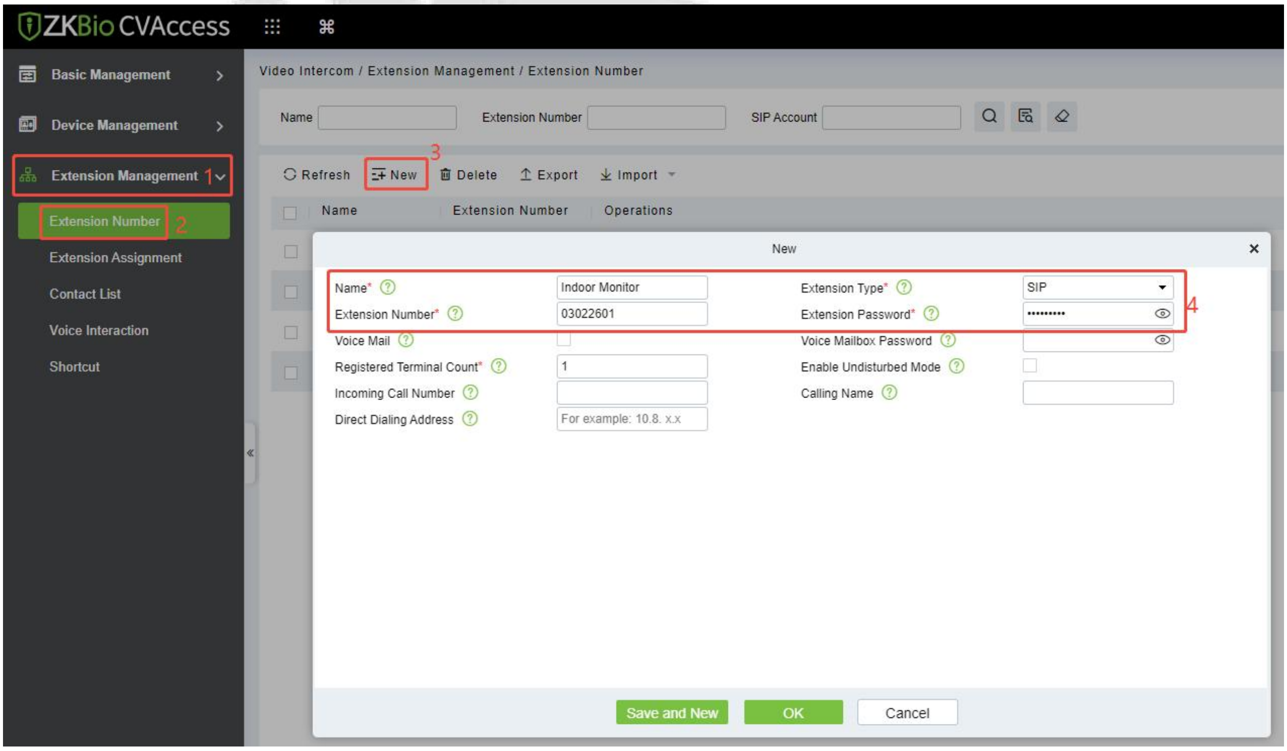
Video Intercom / Device Management / Device

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

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

23.2.3 Create Extension Numbers

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



Video Intercom / Extension Management / Extension Number

Name | Extension Number | SIP Account

Name	Extension Number	Operations

New

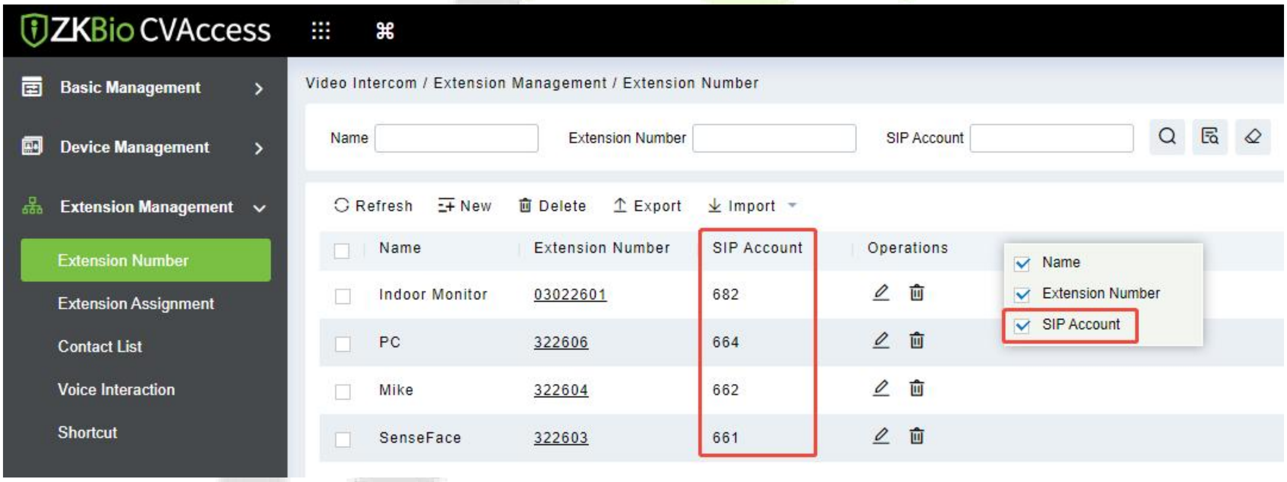
Name*	Indoor Monitor	Extension Type*	SIP
Extension Number*	03022601	Extension Password*	•••••••••
Voice Mail	□	Voice Mailbox Password	
Registered Terminal Count*	1	Enable Undisturbed Mode	□
Incoming Call Number		Calling Name	
Direct Dialing Address	For example: 10.8. x.x		

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

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

Note:

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



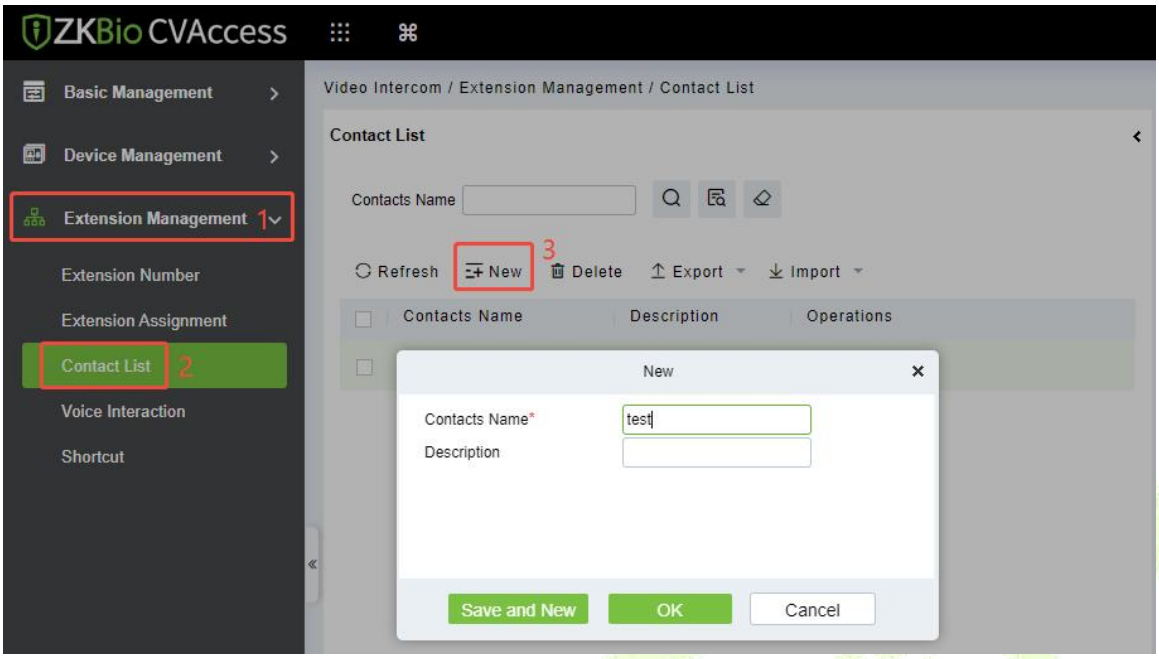
□	Name	Extension Number	SIP Account	Operations
□	Indoor Monitor	03022601	682	
□	PC	322606	664	
□	Mike	322604	662	
□	SenseFace	322603	661	

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

23.2.4 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.

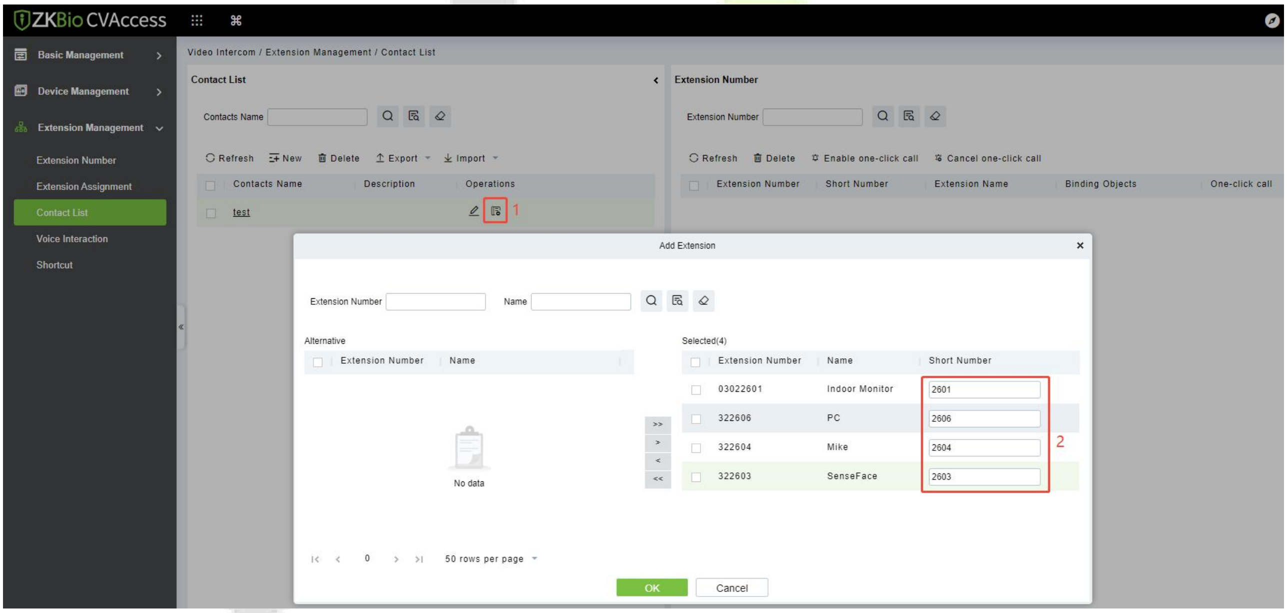


New

Contacts Name* test

Description

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



Selected(4)

Extension Number	Name	Short Number
03022601	Indoor Monitor	2601
322606	PC	2606
322604	Mike	2604
322603	SenseFace	2603

Note:

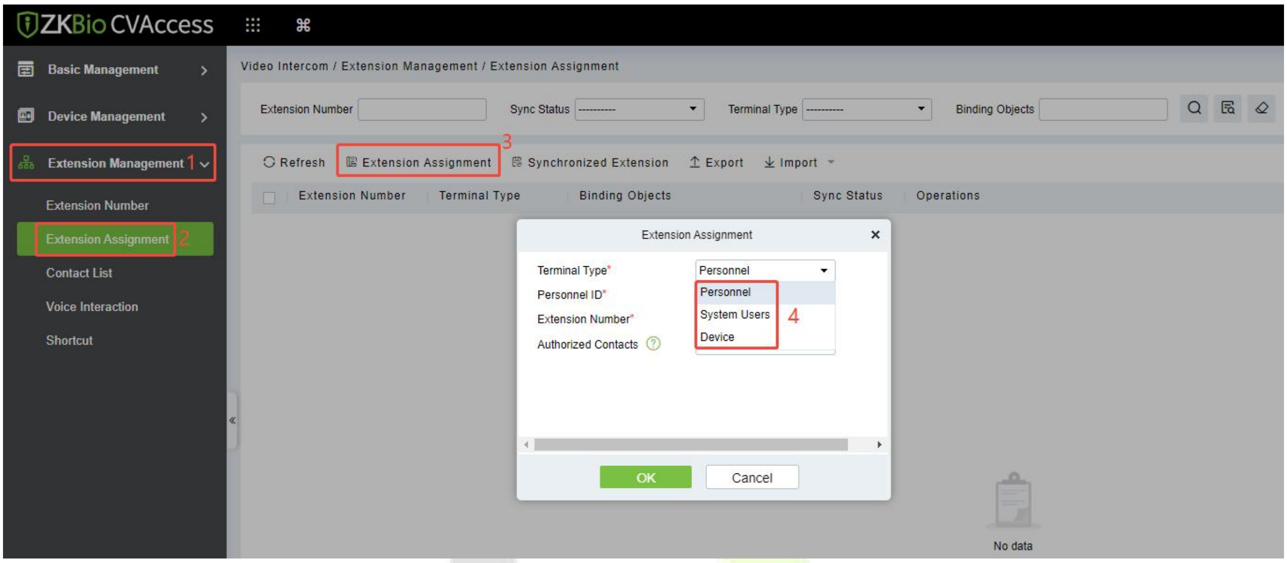
1) If you add an extension number to the contact list without editing the short number, and you wish to edit it later, you will need to delete the extension number from that contacts and then edit it when re-adding, or delete it and use the import function afterward.

2) If the device is set to be a fence terminal, please do not define the short number of the indoor monitors. You just need to input the block, unit and room number to call the indoor monitor.

23.2.5 Assignment of Extension Numbers and SIP Accounts

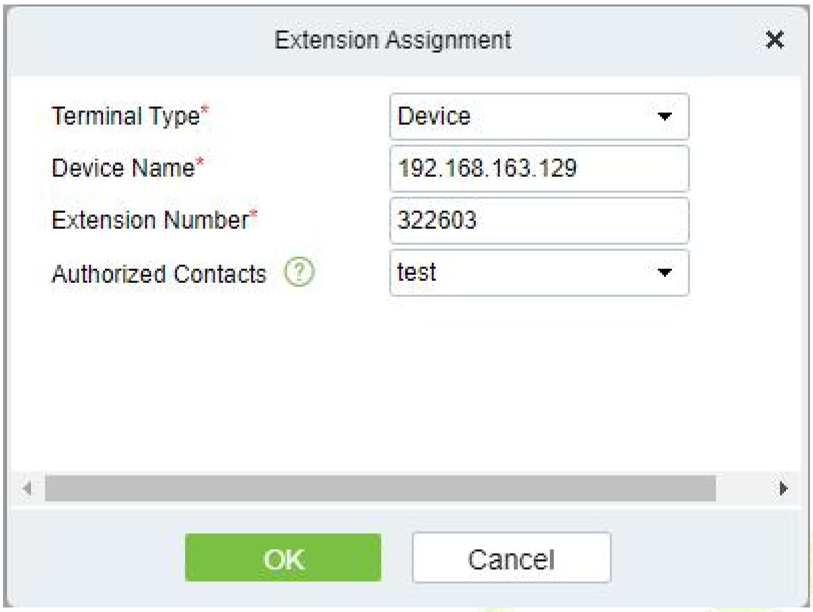
The extension number or SIP account can be assigned to personnel, devices or system users. After allocation, personnel and users' APP will be able to directly use video intercom for communication. The device can also be used directly without manual additional configuration.

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



- **Device Account Assignment**

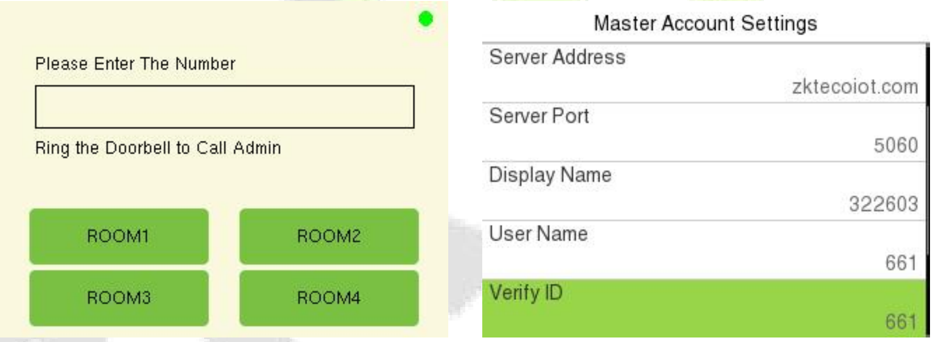
1. Select the Terminal Type as **Device**.
2. Select the device need to be bound (device or indoor monitor) and the extension number. The account information will be automatically synchronized to the device. Select the Authorized Contacts to assign the contact list to the device; only after the assignment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



Extension Assignment

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

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

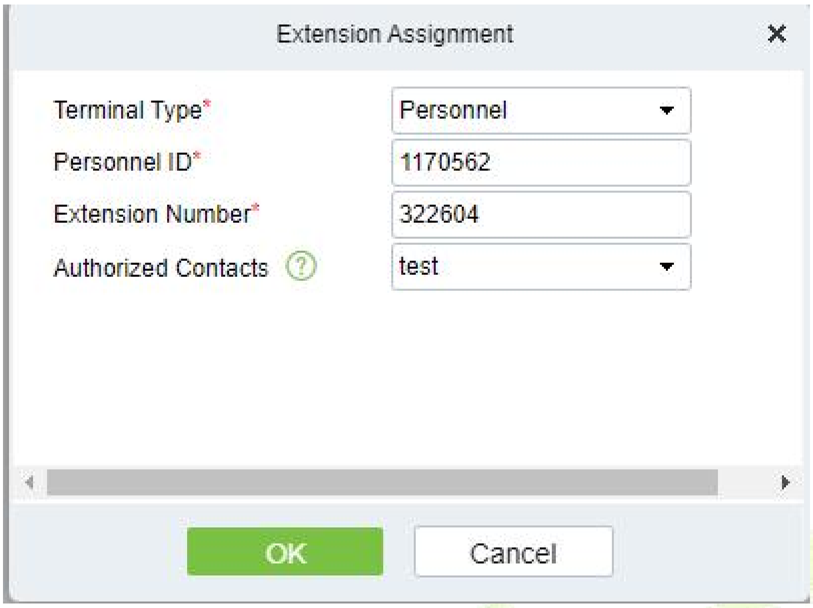


Master Account Settings

Server Address	zktecoiot.com
Server Port	5060
Display Name	322603
User Name	661
Verify ID	661

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

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



Extension Assignment

Terminal Type*: Personnel

Personnel ID*: 1170562

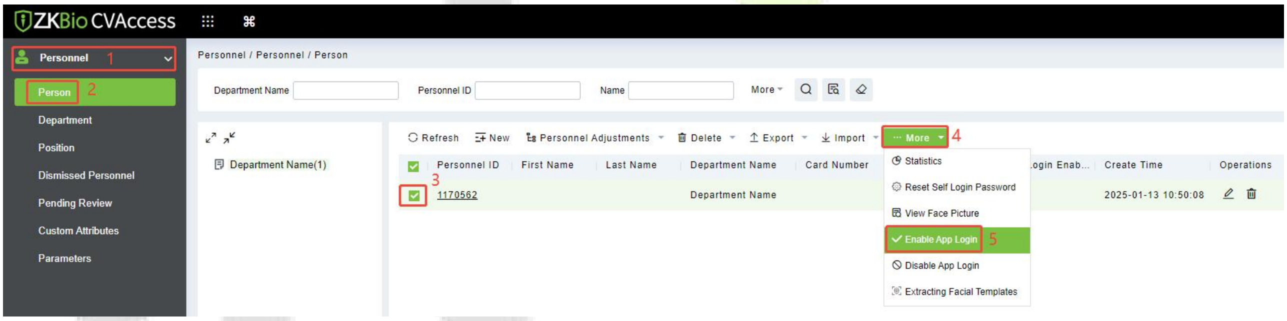
Extension Number*: 322604

Authorized Contacts: test

Note:

1) Before assign account to the personnel, you need first add personnel in ZKBio CVAccess. The adding method can refer to [20 Connect to ZKBio CVAccess Software](#).

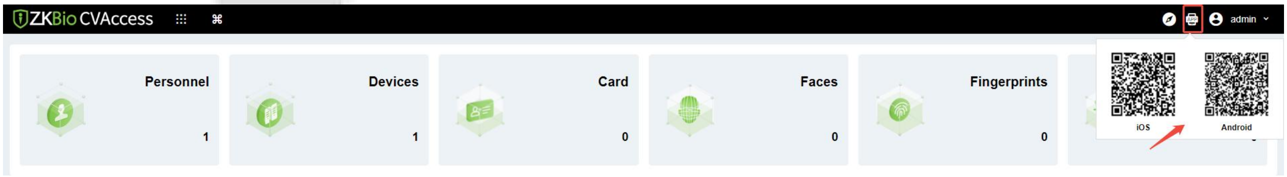
2) The personnel need to enable APP Login. (Click **Personnel > Personnel > Person > More > Enable APP Login**.) Once a person has enabled APP login, they can directly access the Video Intercom feature upon logging into the App.



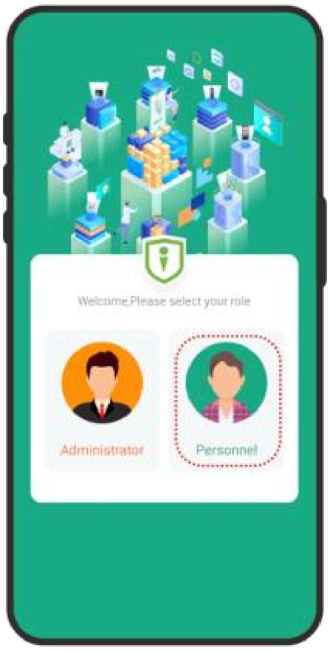
Personnel / Personnel / Person

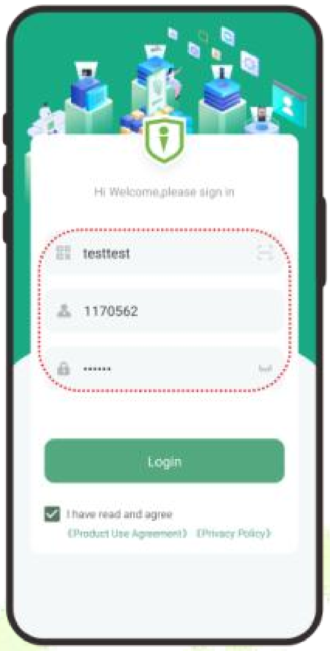
Personnel ID	First Name	Last Name	Department Name	Card Number	Login Enab...	Create Time	Operations
1170562			Department Name			2025-01-13 10:50:08	

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

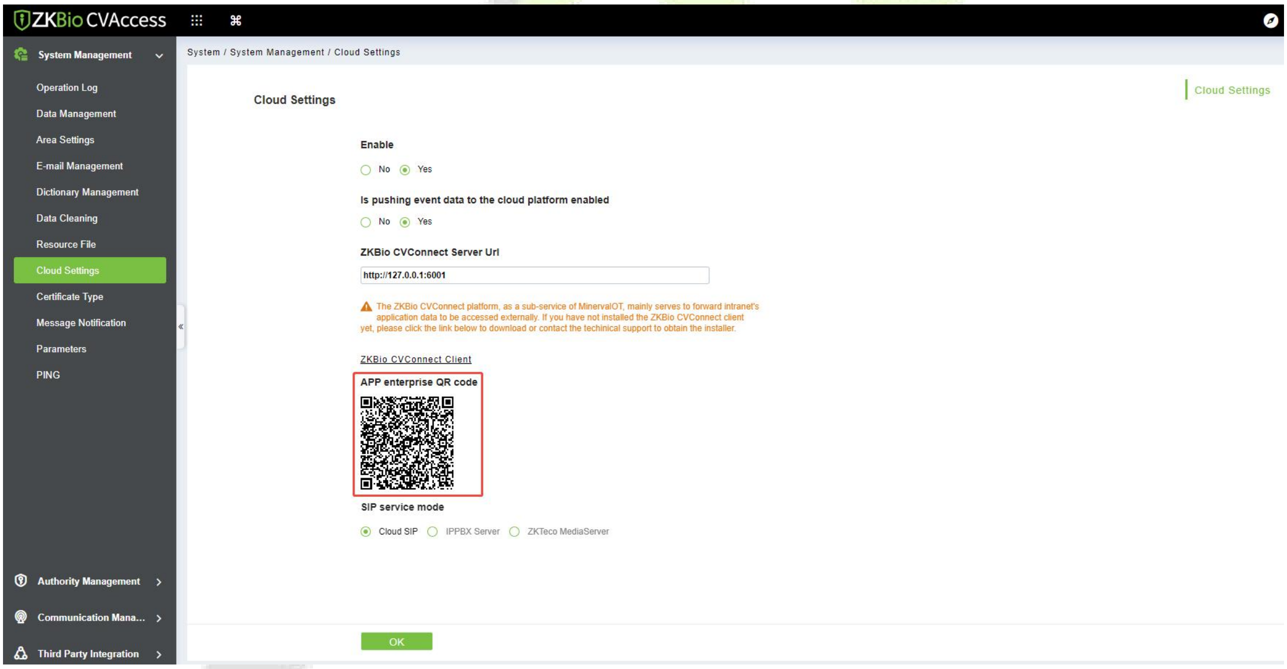


3. After successful assignment, the personnel can login to the App. Select the role-**Personnel** , enter the account information, and click **Login**.




Hi Welcome,please sign in
testtest
1170562
••••••
Login
☑ I have read and agree
《Product Use Agreement》《Privacy Policy》

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



Cloud Settings

Enable

○ No ● Yes

Is pushing event data to the cloud platform enabled

○ No ● Yes

ZKBio CVConnect Server Url

http://127.0.0.1:6001

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

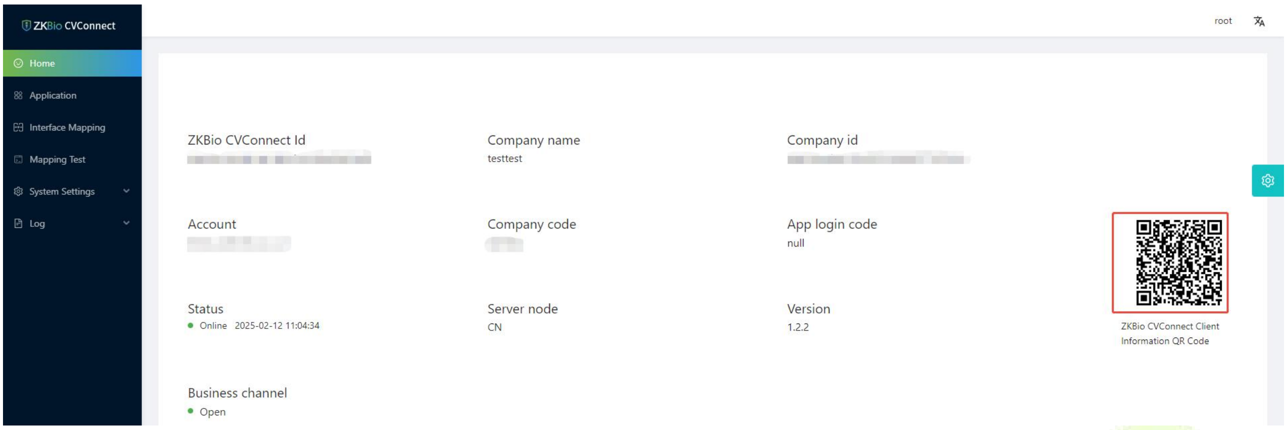
ZKBio CVConnect Client

APP enterprise QR code

SIP service mode

● Cloud SIP ○ IPPBX Server ○ ZKTeco MediaServer

OK



ZKBio CVConnect Id
[redacted]

Company name
testtest

Company id
[redacted]

Account
[redacted]

Company code
[redacted]

App login code
null

Status
Online 2025-02-12 11:04:34

Server node
CN

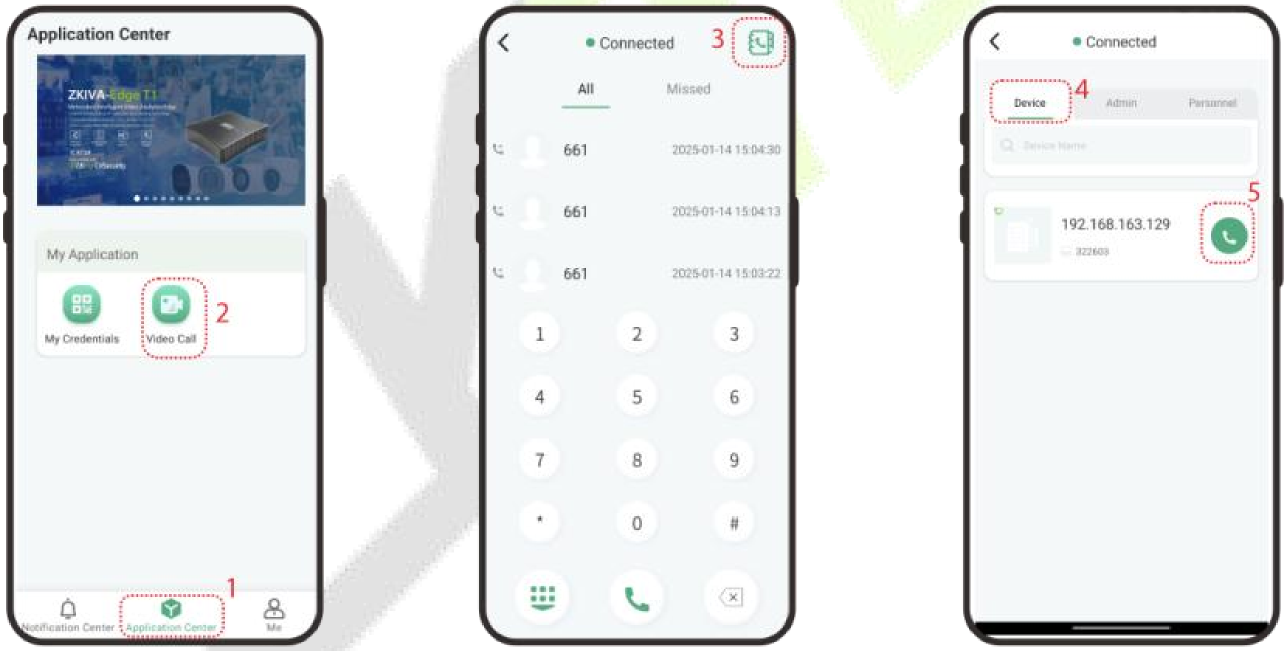
Version
1.2.2

ZKBio CVConnect Client Information QR Code

Business channel
Open

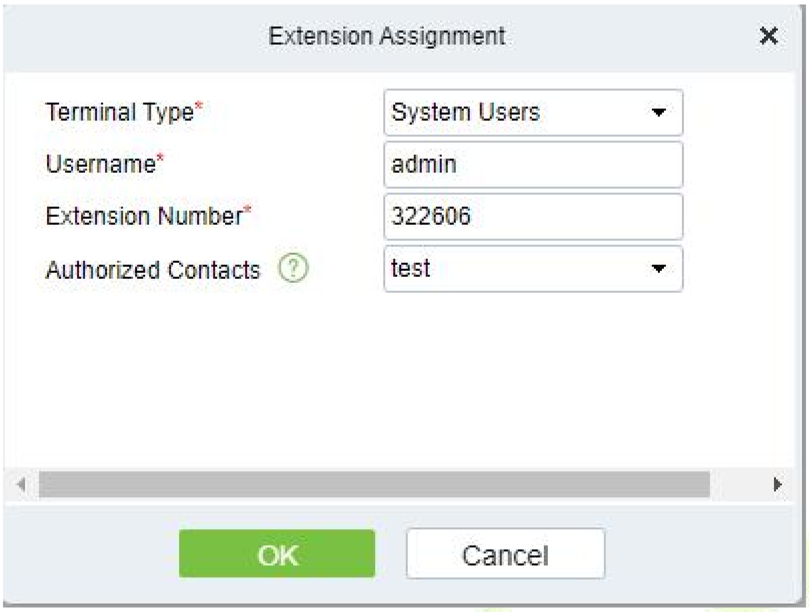
Account & Password: The personnel ID & password (default: 123456).

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



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

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



Extension Assignment

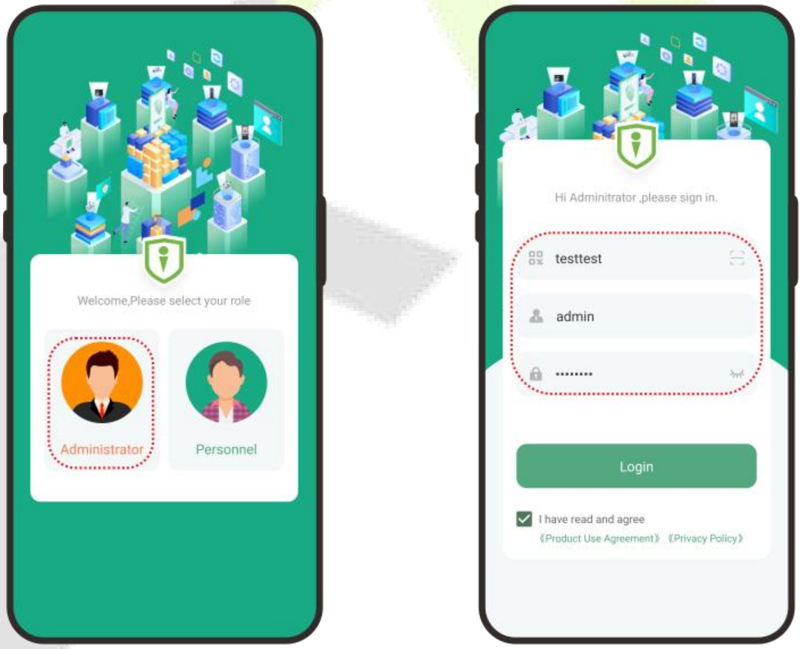
Terminal Type*: System Users

Username*: admin

Extension Number*: 322606

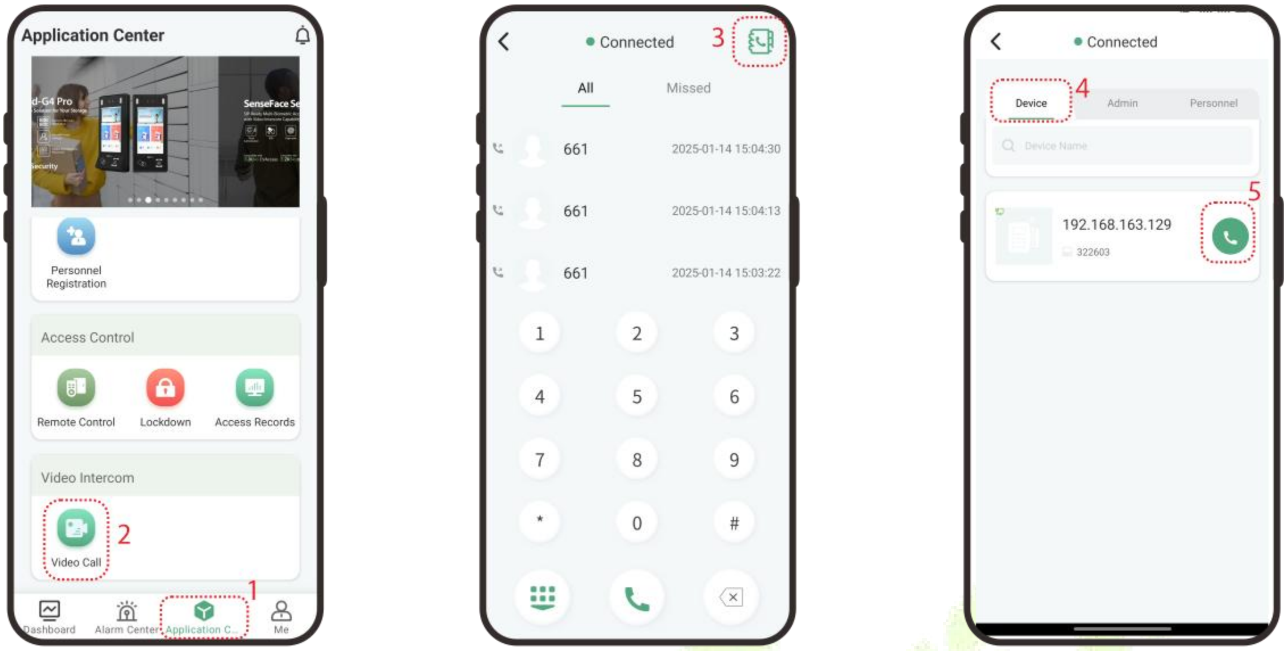
Authorized Contacts: test

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



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

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



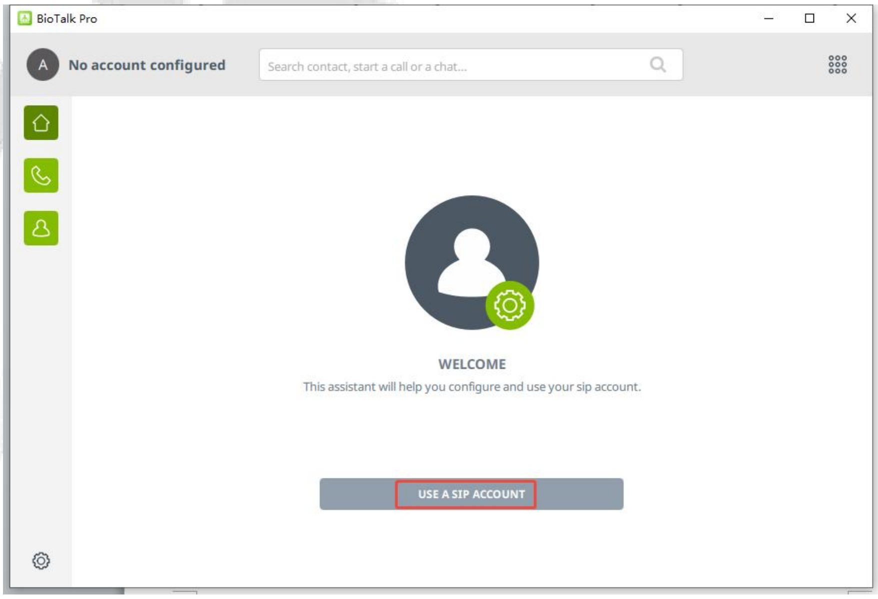
The App complete operation steps please refer to the ZKBio Zexus Mobile App User Manual.

23.2.6 PC Client Functionality

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

Operation Guide

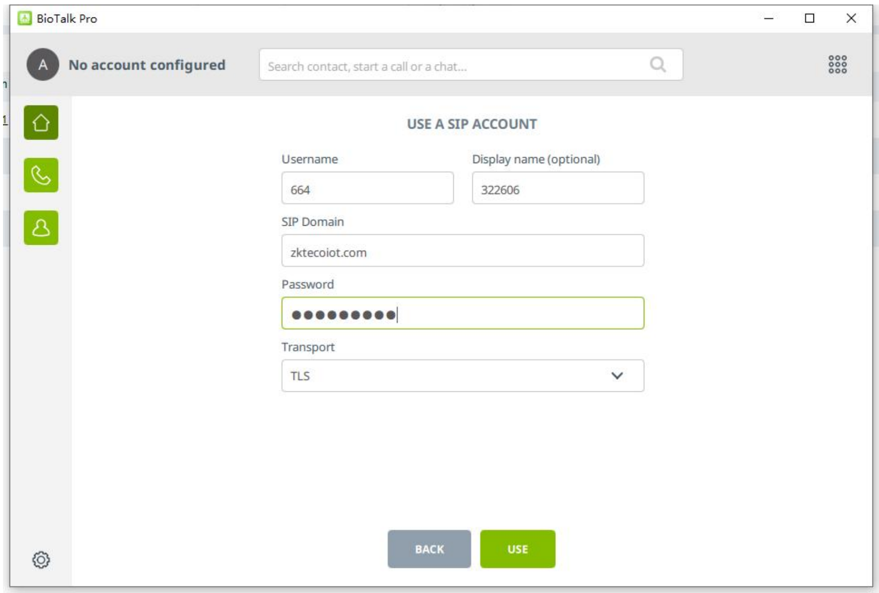
Step 1: Configure the SIP account: Click **USE A SIP ACCOUNT** button.



WELCOME

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

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



USE A SIP ACCOUNT

Username: 664

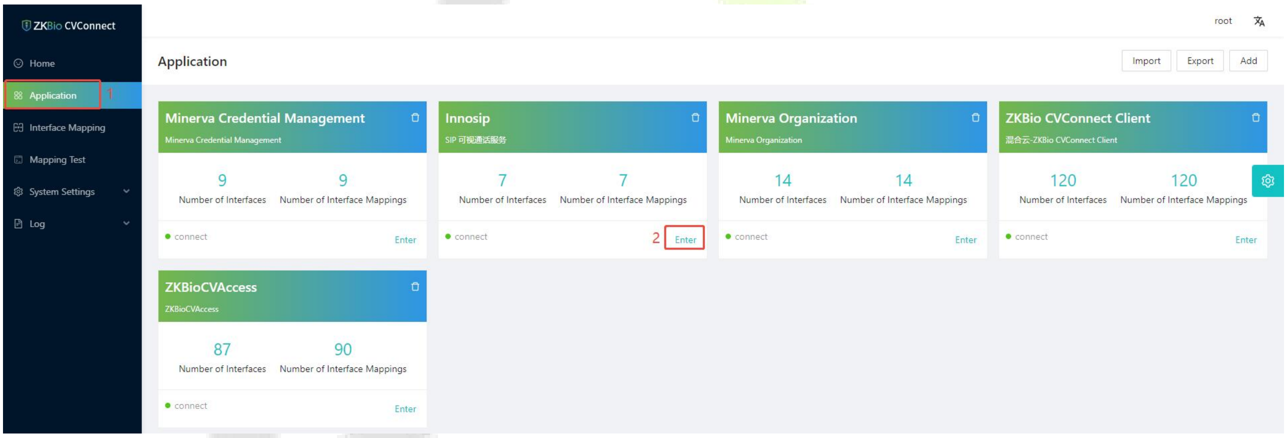
Display name (optional): 322606

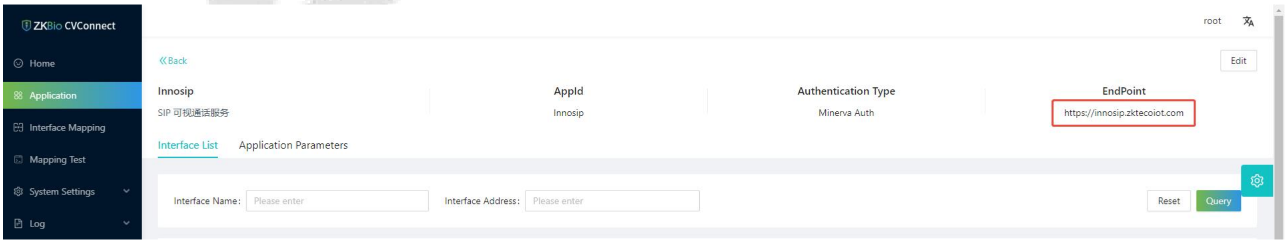
SIP Domain: zktecoiot.com

Password: ●●●●●●●●●

Transport: TLS

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





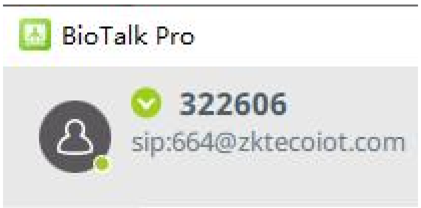
Innosip	AppId	Authentication Type	EndPoint
SIP 可视通话服务	Innosip	Minerva Auth	https://innosip.zktecoiot.com

Interface Name: Please enter

Interface Address: Please enter

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

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



BioTalk Pro

322606

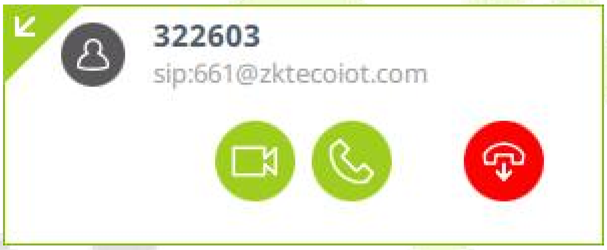
sip:664@zktecoiot.com

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

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

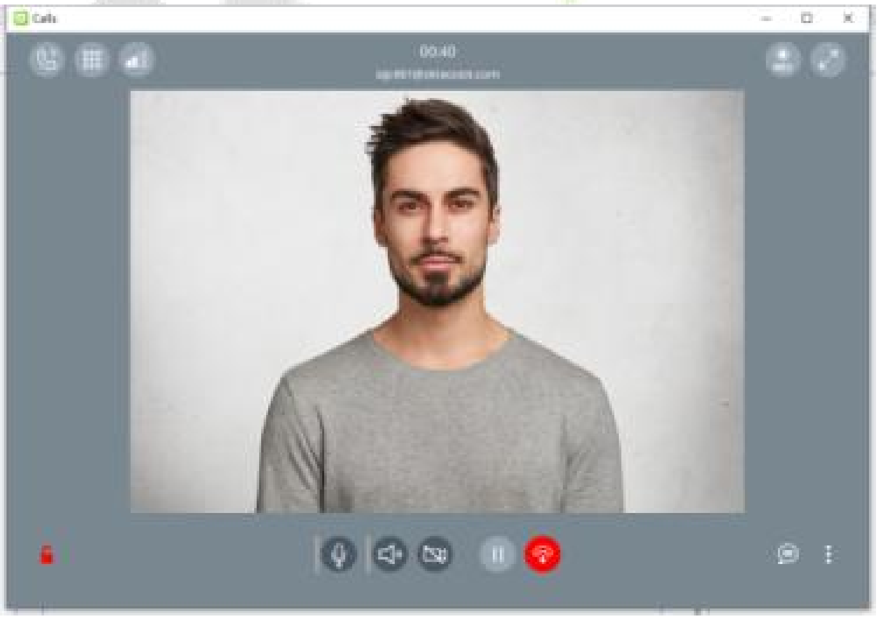
When the PC Client receives a call, a window alert will pop up in the lower right corner of the desktop.

Click the ☎ icon to accept it.



322603

sip:661@zktecoiot.com

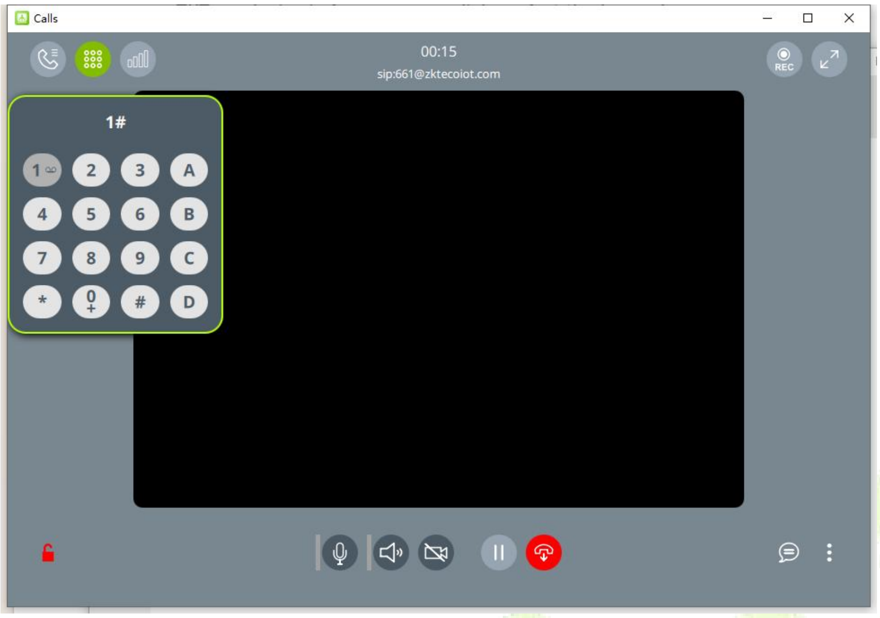


Calls

00:40

sip:661@zktecoiot.com

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



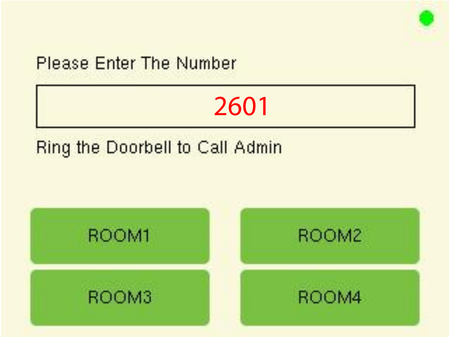
23.2.7 Make a Call

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

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

1. Add the indoor monitor on the ZKBio CVAccess software, then assign an extension number to the indoor monitor. (The operations steps can refer to 23.2.2 Add Device and 23.2.5 Assignment of Extension Numbers and SIP Accounts)

2. Press the ☎ key on the device and enter the Short Number of the indoor monitor in the pop-up interface of the device. Or press the **Up** key on the call page to open the contact list and search for the indoor monitor to call it.

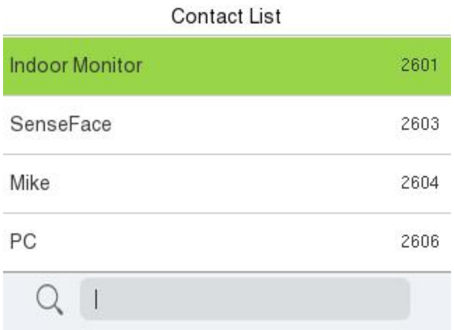


Please Enter The Number

2601

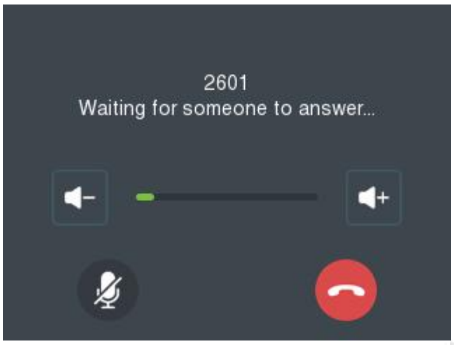
Ring the Doorbell to Call Admin

or



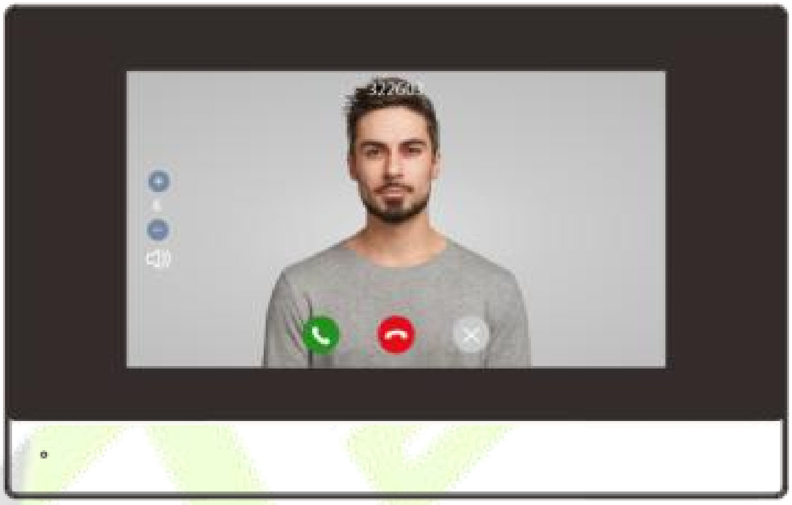
Contact List

Indoor Monitor	2601
SenseFace	2603
Mike	2604
PC	2606



2601

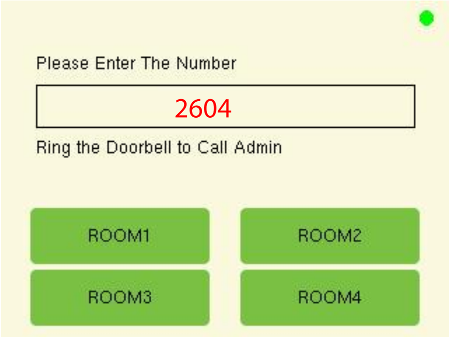
Waiting for someone to answer...



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

1. On the ZKBio CVAccess software, assign an extension number to the personnel. (The operations steps can refer to 23.2.5 Assignment of Extension Numbers and SIP Accounts)

2. Press the ☎ key on the device and enter the Short Number of the personnel in the pop-up interface of the device. Or press the **Up** key on the call page to open the contact list and search for the personnel to call him/her.

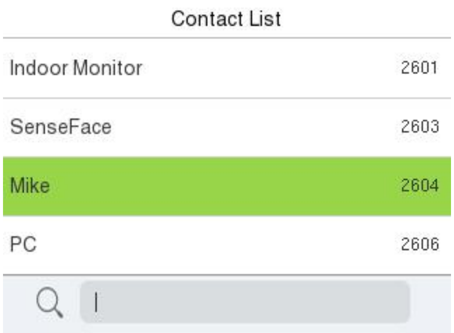


Please Enter The Number

2604

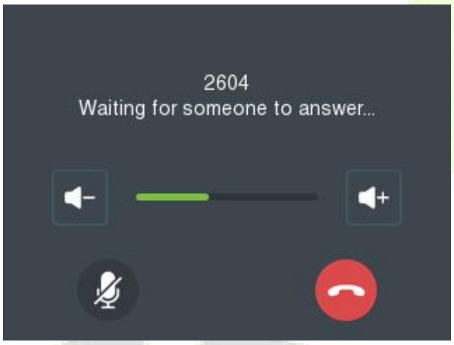
Ring the Doorbell to Call Admin

or



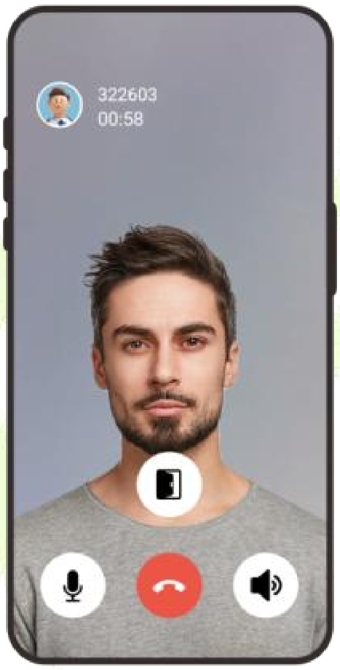
Contact List

Indoor Monitor	2601
SenseFace	2603
Mike	2604
PC	2606



2604

Waiting for someone to answer...

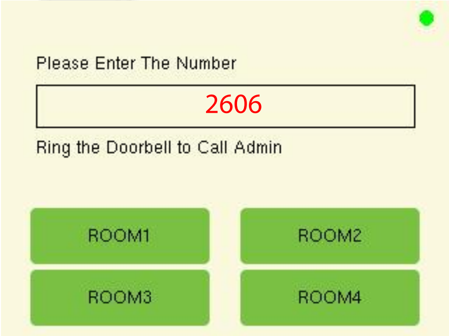


322603

00:58

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

1. Install the BioTalk Pro software and configure the SIP account. (The operations steps can refer to 23.2.6 PC Client Functionality)
2. Press the ☎ key on the device and enter the Short Number of the PC client in the pop-up interface of the device. Or press the **Up** key on the call page to open the contact list and search for the PC client to call it.

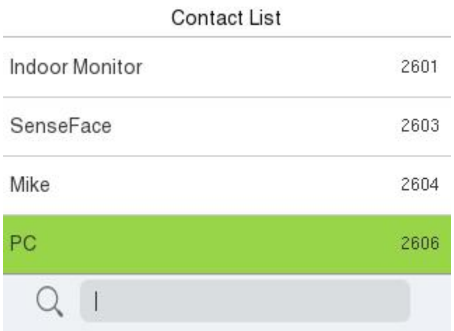


Please Enter The Number

2606

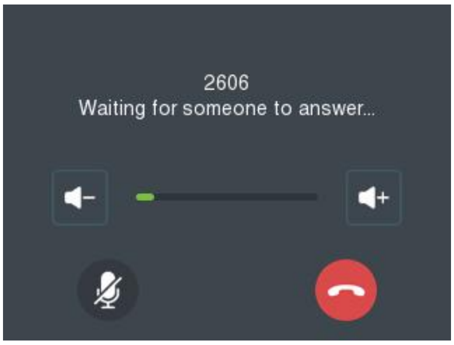
Ring the Doorbell to Call Admin

or

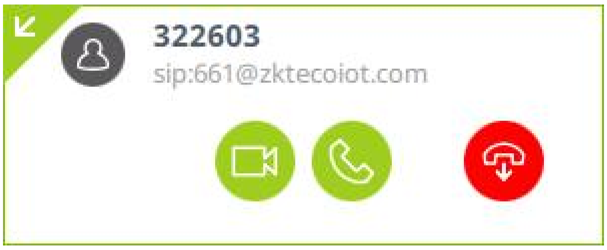


Contact List

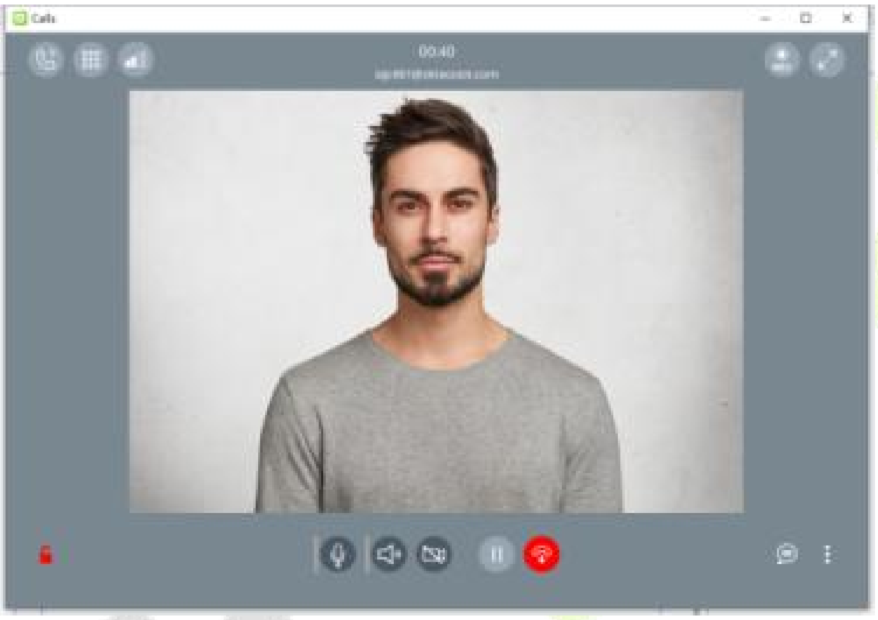
Indoor Monitor	2601
SenseFace	2603
Mike	2604
PC	2606



2606
Waiting for someone to answer...

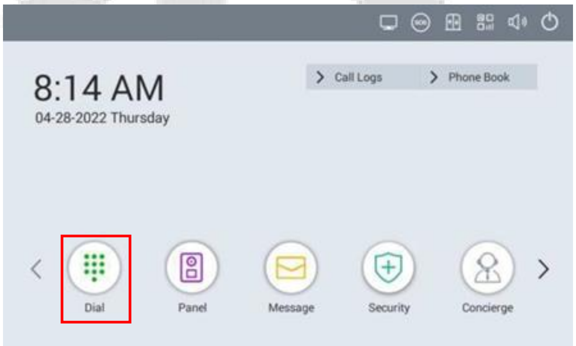


322603
sip:661@zktecoiot.com

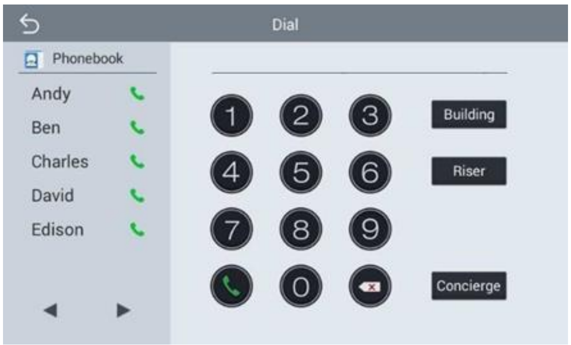


- **Indoor Monitor Call**

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



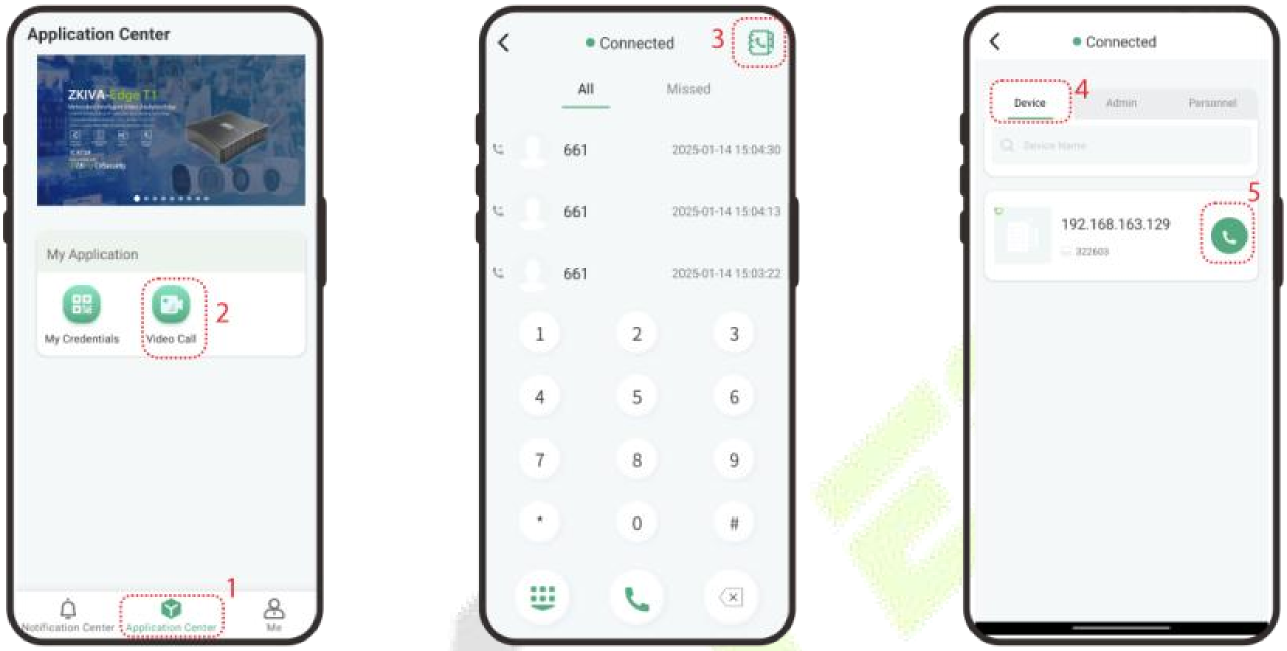
8:14 AM
04-28-2022 Thursday



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

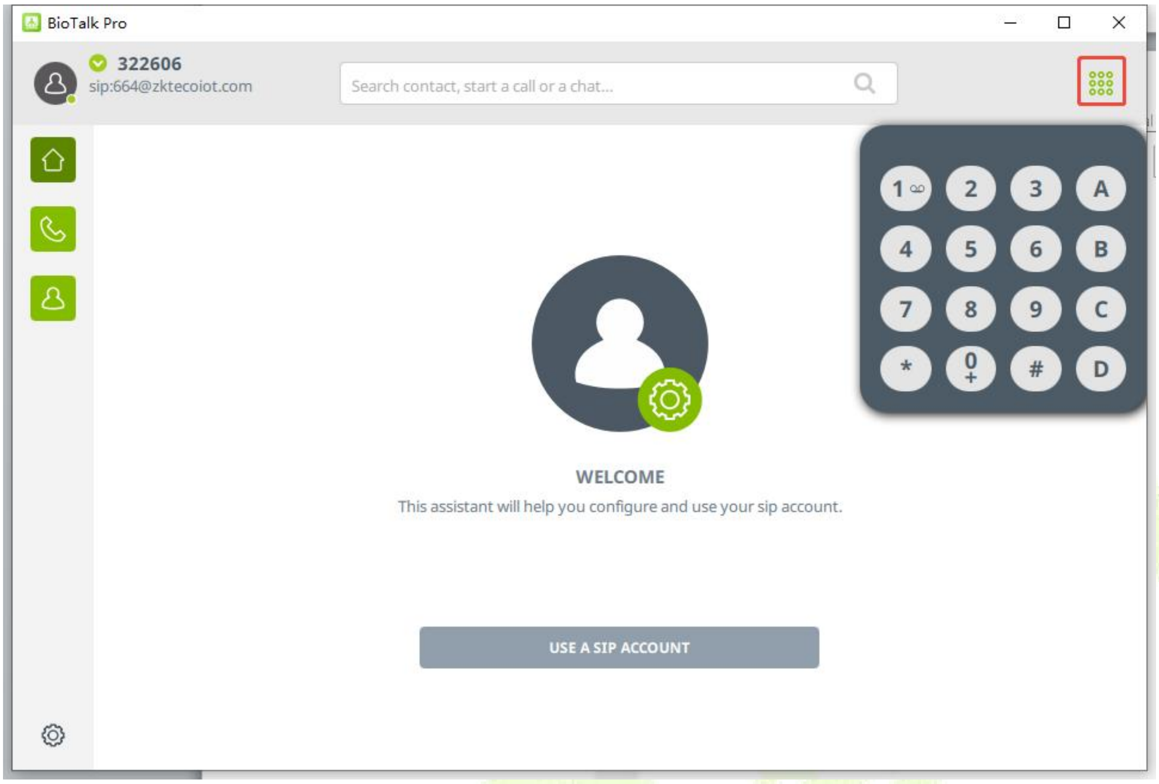
- **Phone Call**

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

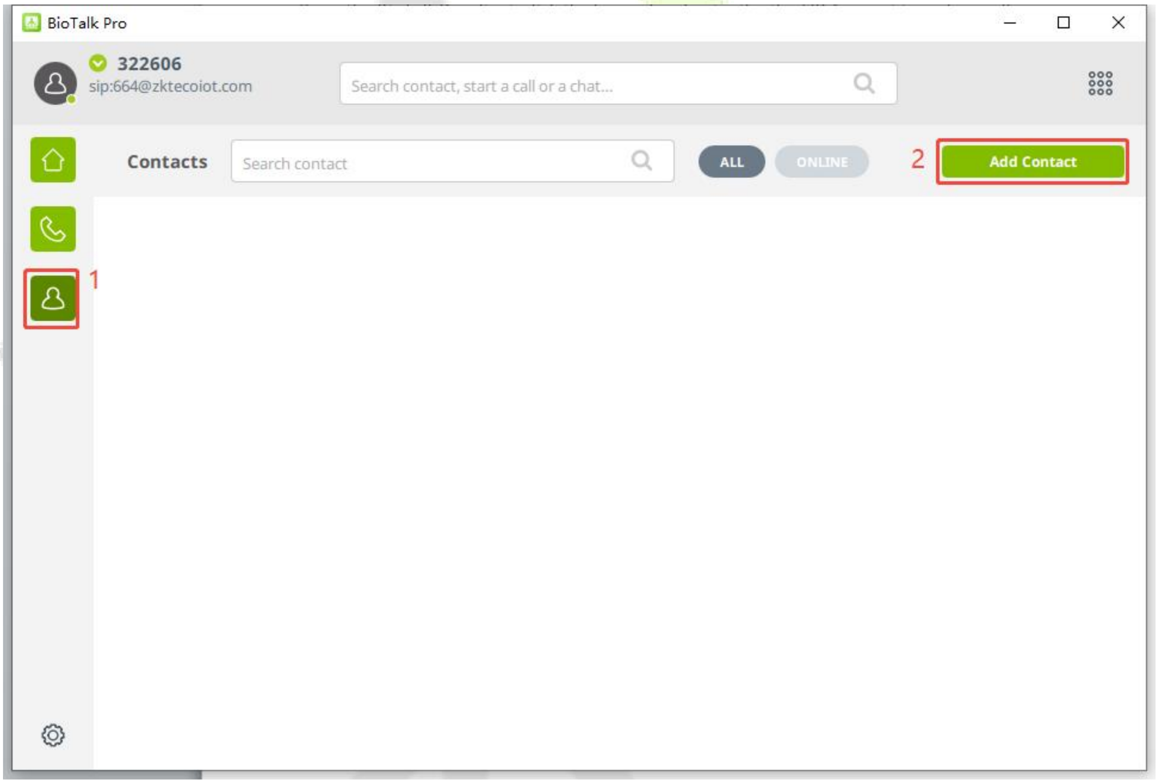


- **PC Client (BioTalk Pro) Call**

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


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

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



24 Connecting to ZKBio Zlink Mobile App

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

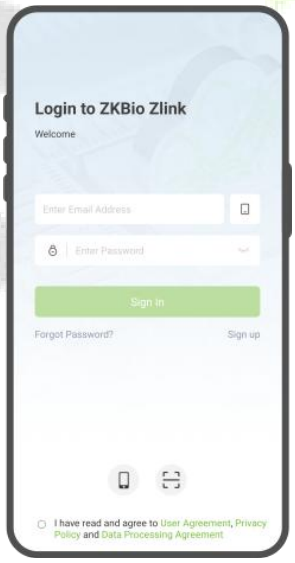
Change the device communication protocol to BEST protocol, then the device can be managed by ZKBio Zlink, please refer to 11.5 Device Type Setting.

- **Download the ZKBio Zlink Mobile App**

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

24.1 Login to the Mobile App

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



Login to ZKBio Zlink

Welcome

Enter Email Address

Enter Password

Sign In

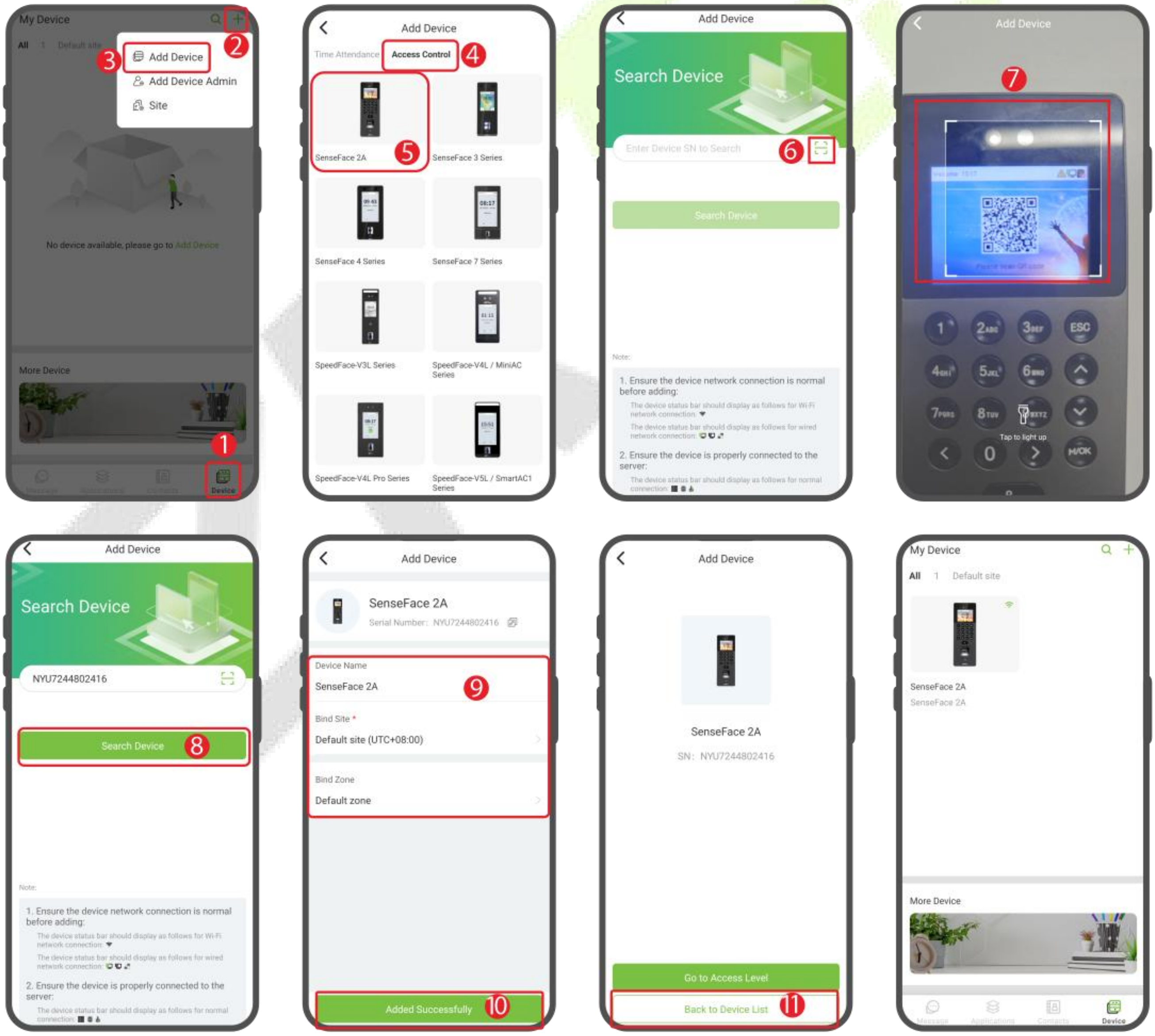
Forgot Password? Sign up

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

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

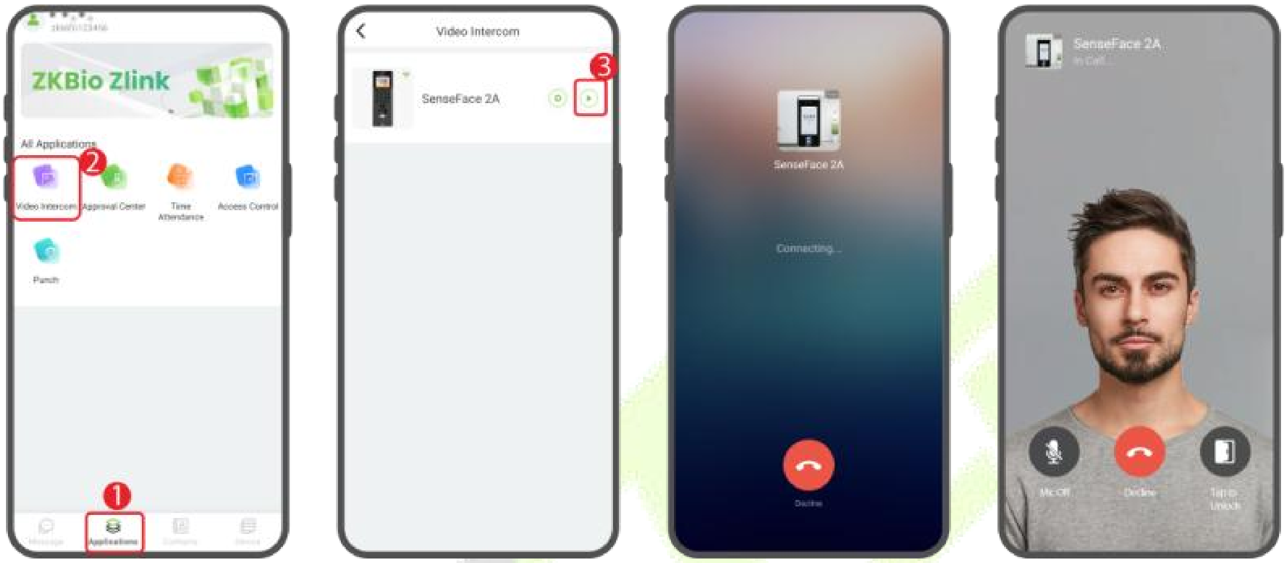
24.2 Add Device on the Mobile App

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


My Device
All 1 Default site
Add Device
Add Device Admin
Site
No device available, please go to Add Device
More Device
Message Applications Contacts Device
Add Device
Time Attendance
Access Control
SenseFace 2A
SenseFace 3 Series
SenseFace 4 Series
SenseFace 7 Series
SpeedFace-V3L Series
SpeedFace-V4L / MiniAC Series
SpeedFace-V4L Pro Series
SpeedFace-V5L / SmartAC1 Series
Search Device
Enter Device SN to Search
Note:
1. Ensure the device network connection is normal before adding:
The device status bar should display as follows for Wi-Fi network connection:
The device status bar should display as follows for wired network connection:
2. Ensure the device is properly connected to the server:
The device status bar should display as follows for normal connection:
Tap to light up
NYU7244802416
SenseFace 2A
Serial Number: NYU7244802416
Device Name
SenseFace 2A
Bind Site *
Default site (UTC+08:00)
Bind Zone
Default zone
Added Successfully
SN: NYU7244802416
Go to Access Level
Back to Device List
1
2
3
4
5
6
7
8
9
10
11

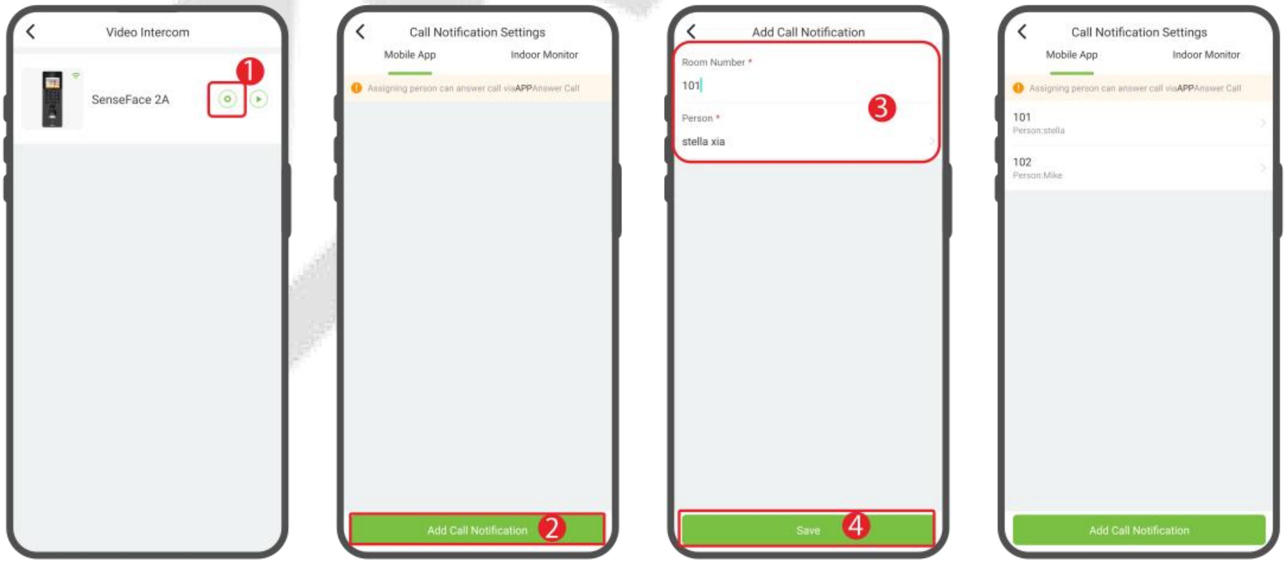
24.3 Video Intercom

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



2. Click ⚙ icon > **[Add Call Notification]** to assign person that can answer call via App.

- **Room Number:** Customize the number of the person.
- **Person:** One or multiple persons can be selected. If multiple persons are selected, all the persons will receive the call when the device calls the number.



Assigning person can answer call viaAPPAnswer Call

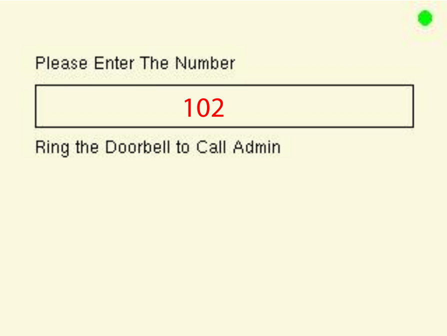
Room Number * 101

Person * stella xia

101 Person:stella

102 Person:Mike

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

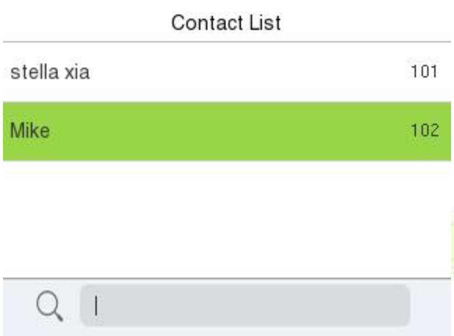


Please Enter The Number

102

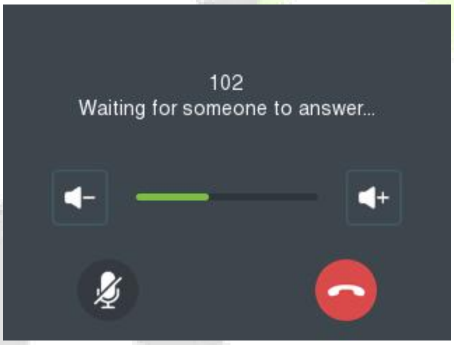
Ring the Doorbell to Call Admin

or

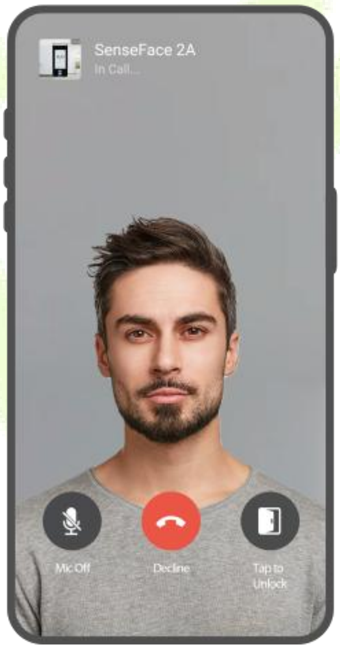


Contact List

stella xia	101
Mike	102



102
Waiting for someone to answer...



25 Connecting to ZKBio Zlink Web Portal

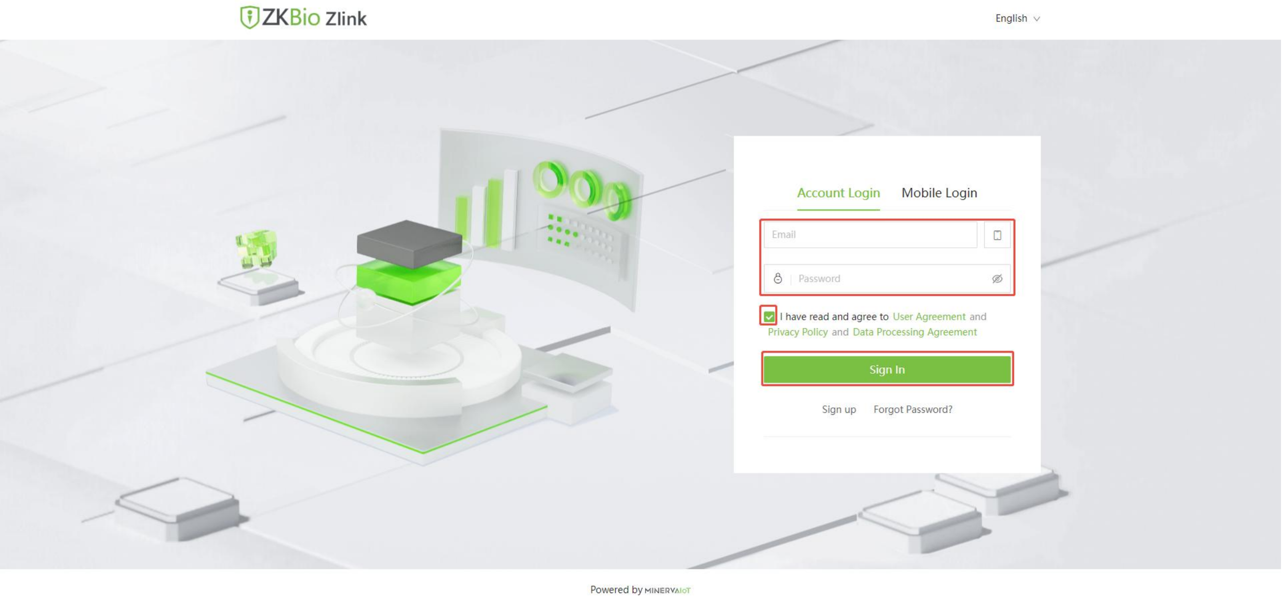
The Web Portal pages may vary depending on the version, and the document is for reference only.

Change the device communication protocol to BEST protocol, then the device can be managed by ZKBio Zlink, please refer to 11.5 Device Type Setting.

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

25.1 Login to the Web Portal

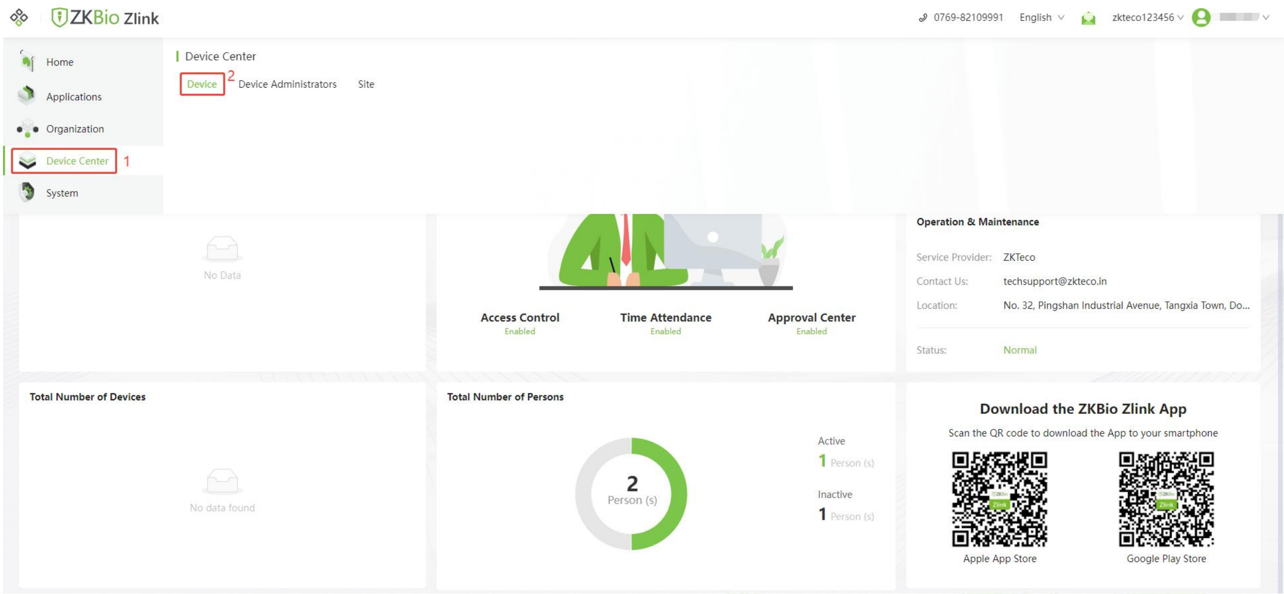
1. Please open the recommended browser and enter the IP address to access the ZKBio Zlink Web Portal: http://zlink.minervaiot.com.
2. Enter your registered account on the login screen, check "I have read and agree to User Agreement and Privacy Policy and Data Processing Agreement" and click [**Sign In**]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



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

25.2 Add Device on the Web Portal

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



Operation & Maintenance

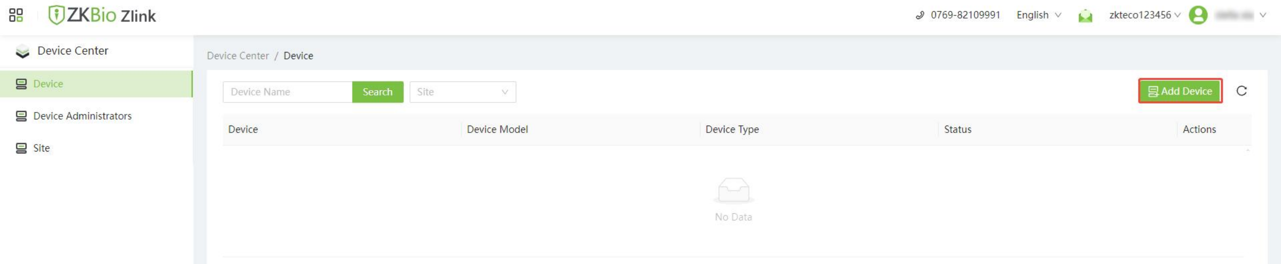
Service Provider: ZKTeco

Contact Us: techsupport@zkteco.in

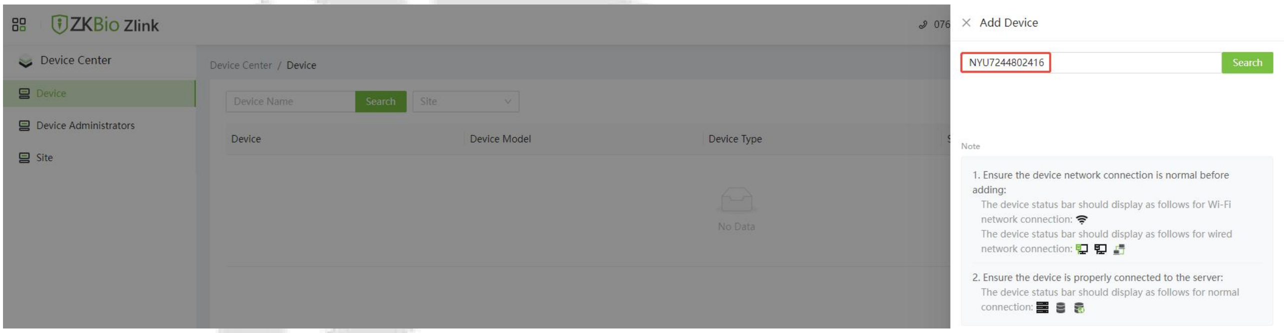
Location: No. 32, Pingshan Industrial Avenue, Tangxia Town, Do...

Status: Normal

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



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



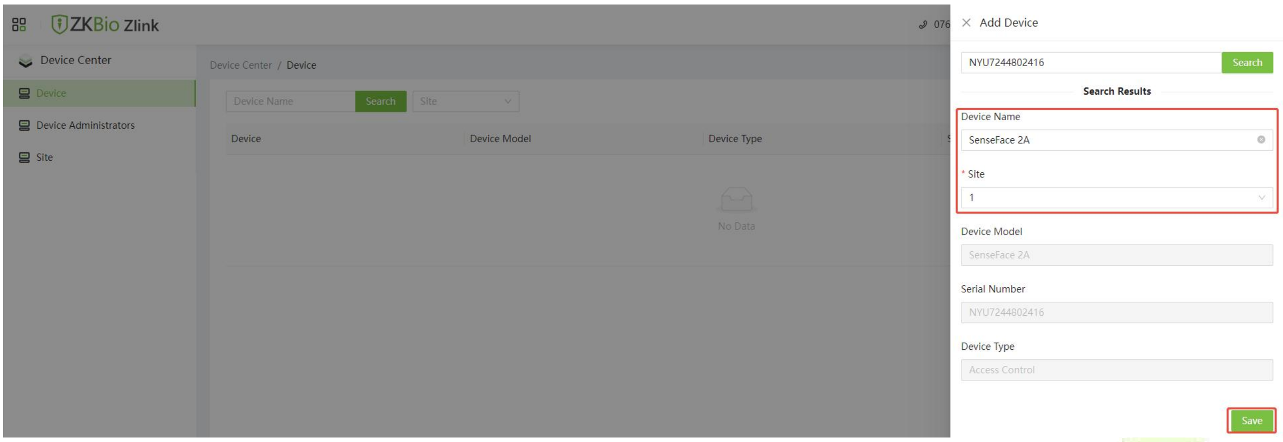
NYU7244802416

Note

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

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

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



NYU7244802416

Device Name: SenseFace 2A

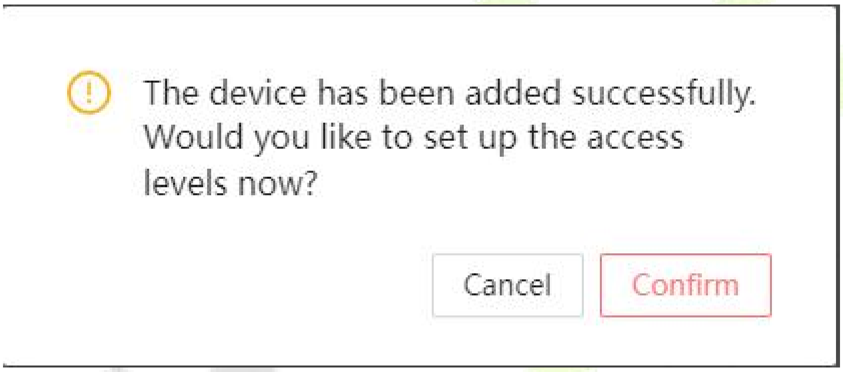
* Site: 1

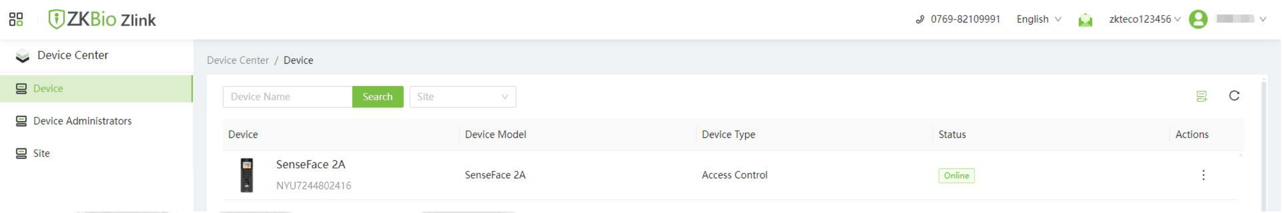
Device Model: SenseFace 2A

Serial Number: NYU7244802416

Device Type: Access Control

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


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



Device	Device Model	Device Type	Status	Actions
SenseFace 2A NYU7244802416	SenseFace 2A	Access Control	Online	⋮

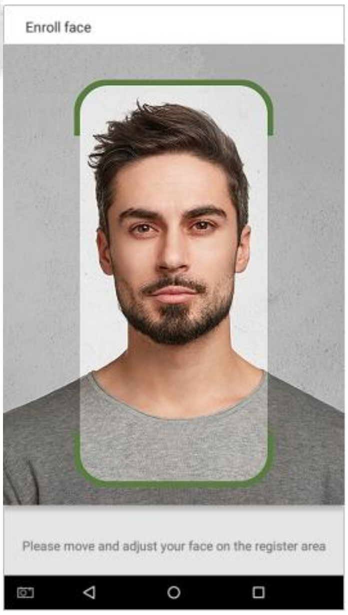
***Note:** Wait a moment for the device status to change from “**Offline**” to “**Online**”.*

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

Appendix

Requirements of Live Collection and Registration of Visible Light Face Templates

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



Enroll face

Please move and adjust your face on the register area

Requirements for Visible Light Digital Face Template Data

The digital photo should be straight-edged, 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 ±10°, elevation should not exceed ±10°, and depression angle should not exceed ±10°.

- **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.

Privacy Policy

Notice:

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

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

I. Collected Information

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

1. **User Registration Information: At your first registration, the feature template (Fingerprint template/Face template/Palm template**) will be saved on the device according to the device type you have selected to verify the unique similarity between you and the User ID you have registered. You can optionally enter your Name and Code. The above information is necessary for you to use our products. If you do not provide such information, you cannot use some features of the product regularly.
2. **Product information:** According to the product model and your granted permission when you install and use our services, the related information of the product on which our services are used will be collected when the product is connected to the software, including the Product Model, Firmware Version Number, Product Serial Number, and Product Capacity Information. **When you connect your product to the software, please carefully read the privacy policy for the specific software.**

II. Product Security and Management

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

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

specified in the privacy policy.

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

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

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

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

III. How we handle personal information of minors

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

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

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

IV. Others

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

Eco-friendly Operation

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

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

Hazardous or Toxic substances and their quantities

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

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