

User Manual

SenseFace 2A

Date: March 2024

Doc Version: 1.0

English

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



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

Copyright © 2024 ZKTECO CO., LTD. All rights reserved.

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

Trademark

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

Disclaimer

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

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

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

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

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

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

ZKTeco in no event shall be liable to the user or any third party for any incidental, consequential, indirect, special, or exemplary damages, including, without limitation, loss of business, loss of profits, business interruption, loss of business information or any pecuniary loss, arising out of, in connection with, or

relating to the use of the information contained in or referenced by this manual, even if ZKTeco has been advised of the possibility of such damages.

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

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

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

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

ZKTeco Headquarters

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

Phone +86 769 - 82109991

Fax +86 755 - 89602394

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

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

About the Company

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

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

About the Manual

This manual introduces the operations of **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.....	9
2	ELECTRICAL SAFETY	10
3	OPERATION SAFETY	10
4	INSTRUCTION FOR USE	11
4.1	STANDING POSITION, POSTURE AND FACIAL EXPRESSION.....	11
4.2	FACE TEMPLATE REGISTRATION.....	12
4.3	FINGER POSITIONING	13
4.4	STANDBY INTERFACE	13
4.5	VERIFICATION MODE	15
4.5.1	FACIAL VERIFICATION	15
4.5.2	FINGERPRINT VERIFICATION.....	16
4.5.3	CARD VERIFICATION	18
4.5.4	PASSWORD VERIFICATION.....	19
4.5.5	COMBINED VERIFICATION.....	20
5	OVERVIEW.....	21
5.1	APPEARANCE.....	21
5.2	TERMINAL AND WIRING DESCRIPTION	22
5.2.1	TERMINAL DESCRIPTION	22
5.3	WIRING DESCRIPTION.....	22
5.3.1	POWER CONNECTION	22
5.3.2	DOOR SENSOR & EXIT BUTTON CONNECTION	23
5.3.3	LOCK RELAY CONNECTION.....	23
5.3.4	ETHERNET CONNECTION.....	24
6	INSTALLATION.....	25
6.1	INSTALLATION ENVIRONMENT	25
6.2	DEVICE INSTALLATION	25
7	MAIN MENU	26
8	USER MANAGEMENT.....	27
8.1	NEW USER REGISTRATION.....	27
8.1.1	REGISTER A USER ID AND NAME	27
8.1.2	USER ROLE	28
8.1.3	REGISTER FINGERPRINT	28
8.1.4	REGISTER FACE	28
8.1.5	CARD.....	29
8.1.6	PASSWORD.....	29
8.1.7	PROFILE PHOTO	30
8.1.8	ACCESS CONTROL ROLE	30
8.2	ALL USERS	31


8.2.1	EDIT USER.....	31
8.2.2	DELETE USER.....	32
8.3	DISPLAY STYLE.....	32
9	USER ROLE	34
10	COMMUNICATION	36
10.1	ETHERNET	36
10.2	PC CONNECTION	37
10.3	WI-FI SETTINGS★.....	38
10.4	CLOUD SERVER SETTINGS.....	40
10.5	NETWORK DIAGNOSIS	40
11	SYSTEM SETTINGS	41
11.1	DATE AND TIME	41
11.2	ACCESS LOGS SETTINGS / ATTENDANCE	42
11.3	FACE PARAMETERS	46
11.4	FINGERPRINT.....	48
11.5	DEVICE TYPE SETTINGS.....	49
11.6	SECURITY SETTINGS	50
11.7	USB UPGRADE.....	51
11.8	UPDATE FIRMWARE ONLINE	51
11.9	FACTORY RESET.....	52
12	PERSONALIZE SETTINGS	53
12.1	USER INTERFACE	53
12.2	VOICE	54
12.3	BELL SCHEDULES.....	54
12.4	PUNCH STATES OPTIONS	56
12.5	SHORTCUT KEY MAPPINGS	57
13	DATA MANAGEMENT	59
14	INTERCOM.....	61
14.1	SIP SETTINGS	61
14.1.1	LOCAL AREA NETWORK USE	63
14.1.2	SIP SERVER	66
14.2	DOORBELL SETTING.....	67
14.3	ONVIF SETTINGS.....	67
15	ACCESS CONTROL.....	70
15.1	ACCESS CONTROL OPTIONS	71
15.2	TIME RULE SETTINGS	73
15.3	HOLIDAYS.....	74
15.4	COMBINED VERIFICATION.....	75
15.5	DURESS OPTIONS SETTINGS.....	76

16	USB MANAGER.....	77
16.1	USB DOWNLOAD.....	77
16.2	USB UPLOAD.....	78
17	ATTENDANCE SEARCH	79
18	AUTOTEST	81
19	SYSTEM INFORMATION.....	82
20	CONNECT TO ZKBIO CVACCESS SOFTWARE	83
20.1	SET THE COMMUNICATION ADDRESS.....	83
20.2	ADD DEVICE ON THE SOFTWARE	83
20.3	ADD PERSONNEL ON THE SOFTWARE AND ONLINE FINGERPRINT/FACE REGISTRATION.....	84
21	CONNECT TO ZKBIO TIME SOFTWARE	88
21.1	SET THE COMMUNICATION ADDRESS.....	88
21.2	ADD DEVICE ON THE SOFTWARE	88
21.3	ADD PERSONNEL ON THE SOFTWARE AND ONLINE FINGERPRINT REGISTRATION.....	89
22	CONNECTING TO ZKBIO ZLINK WEB.....	91
22.1	REGISTER ACCOUNT.....	91
22.2	ADD DEVICE.....	93
22.2.1	SET ORGANIZATION (ADD PERSON).....	93
22.2.2	ADD DEVICE	95
22.3	TIME SLOT	97
22.3.1	SET TIME SLOT	97
22.3.2	SET DOOR ACCESS TIME.....	97
22.3.3	SET GROUP ACCESS TIME.....	98
22.4	SYNCHRONIZE PERSON TO DEVICE.....	99
22.5	USER REGISTRATION	102
22.5.1	REGISTER A USER ID AND NAME	102
22.5.2	SETTING THE USER ROLE	102
22.5.3	REGISTER FINGERPRINT	103
22.5.4	REGISTER FACE TEMPLATE.....	104
22.5.5	REGISTER PASSWORD.....	105
22.5.6	REGISTER CARD	107
22.6	DATA SEARCH.....	108
22.6.1	DASHBOARD.....	108
22.6.2	EVENT REPORT.....	108
23	CONNECTING TO ZKBIO ZLINK APP.....	110
23.1	REGISTER ACCOUNT.....	110
23.2	ADD PERSON.....	111
23.3	ADD DEVICE.....	113
23.3.1	ADD SITE AND ZONE	113
23.3.2	ADD DEVICE	114

24	CONNECTING TO WIRELESS DOORBELL★	117
24.1	CONNECT THE WIRELESS DOORBELL	117
24.2	UNBINDING THE WIRELESS DOORBELL	117
APPENDIX		118
	REQUIREMENTS OF LIVE COLLECTION AND REGISTRATION OF VISIBLE LIGHT FACE TEMPLATES	118
	REQUIREMENTS FOR VISIBLE LIGHT DIGITAL FACE TEMPLATE DATA	119
	PRIVACY POLICY	120
	ECO-FRIENDLY OPERATION	123

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.

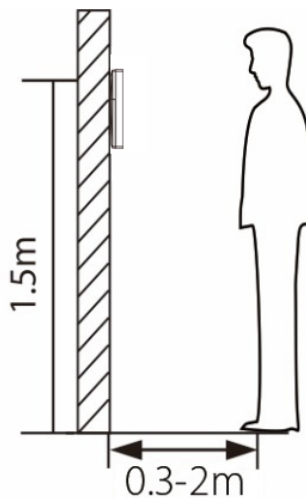
- The warranty service does not cover accidental damage, damage caused by mis-operation, and damage due to independent installation or repair of the product by the user.

4 Instruction for Use

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

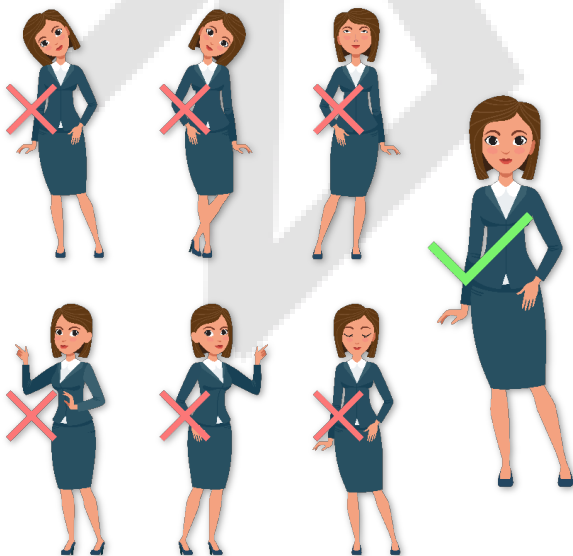
4.1 Standing Position, Posture and Facial Expression

- **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



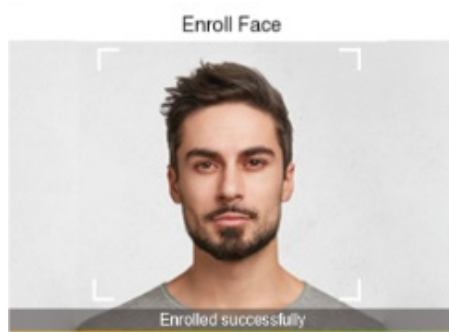
Facial Expression



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

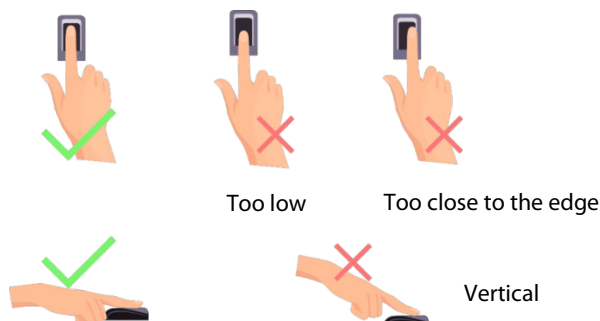
- When registering a face template, maintain a distance of 40cm to 80cm between the device and the face.
- Be careful not to change your facial expression. (Smiling face, drawn face, wink, etc.)
- If you do not follow the instructions on the screen, the face template registration may take longer or may 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

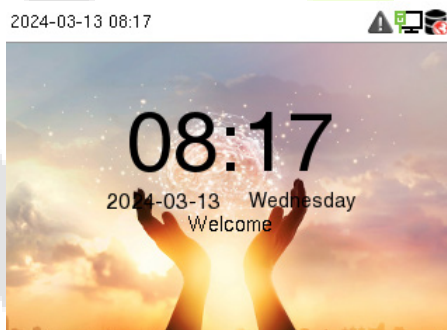
Recommended fingers: The index, middle, or ring finger and avoid using the thumb or pinky fingers, as they are difficult to accurately press onto the fingerprint reader.



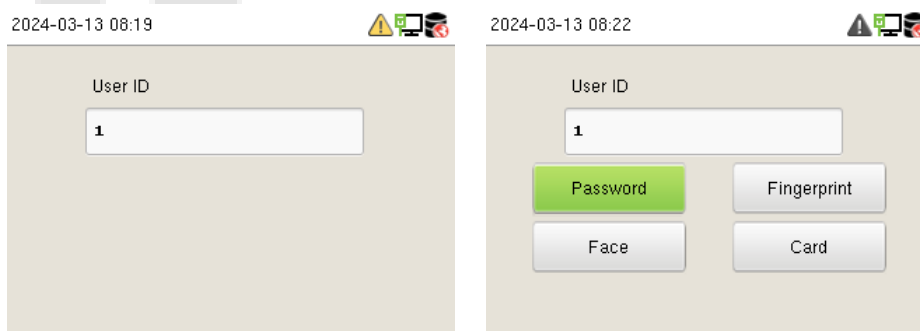
Note: Please use the correct method when pressing your fingers onto the fingerprint reader for registration and identification. Our company will assume no liability for recognition issues that may result from incorrect usage of the product. We reserve the right of final interpretation and modification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

4.4 Standby Interface

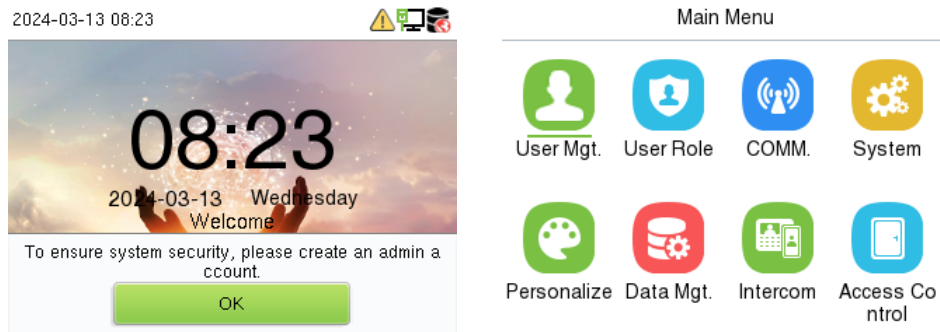
The device uses a 2.4-inch color screen, which all operations are performed through the keypad. After connecting the power supply, the following standby interface is displayed:



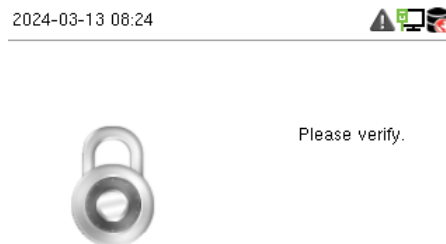
- Enter any number to access the User ID input interface.



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

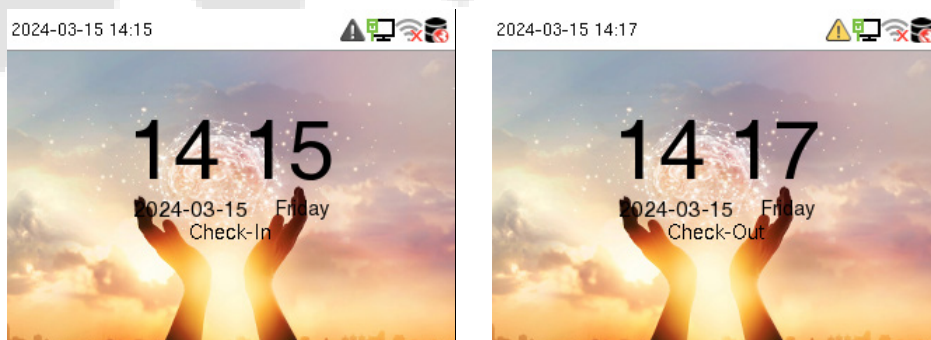


- After adding a Super Administrator on the device, it requires the Super Administrator's verification before opening the menu functions.



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

- 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."



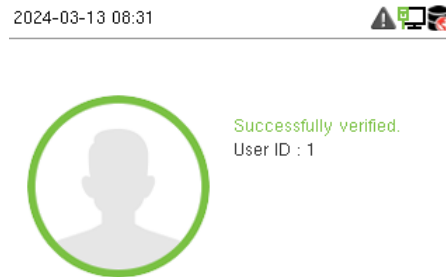
Note: The punch state options are enabled by default when the device type is set as an attendance terminal.

4.5 Verification Mode

4.5.1 Facial Verification

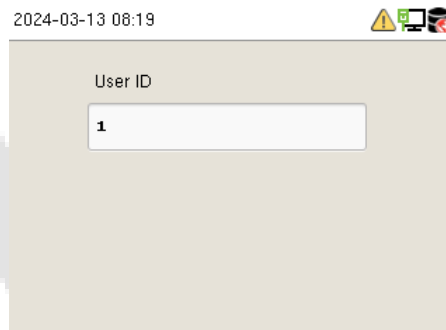
1: N Facial Verification

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.

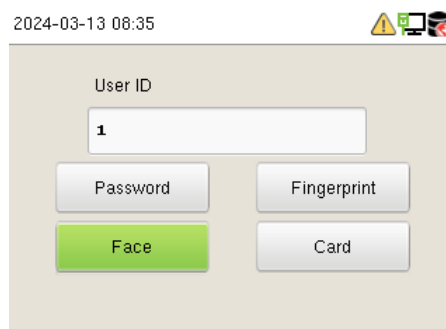


1:1 Facial Verification

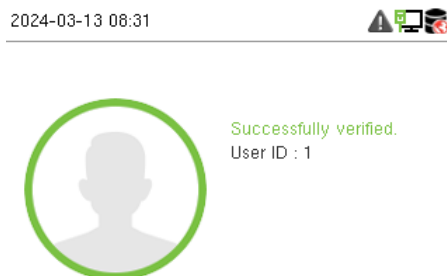
In this verification mode, the device compares the face captured by the camera with the facial template related to the entered user ID. Enter the user ID and press **M/OK** to enter the 1:1 facial verification mode.



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.



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



4.5.2 Fingerprint Verification

➤ 1: N Fingerprint Verification Mode

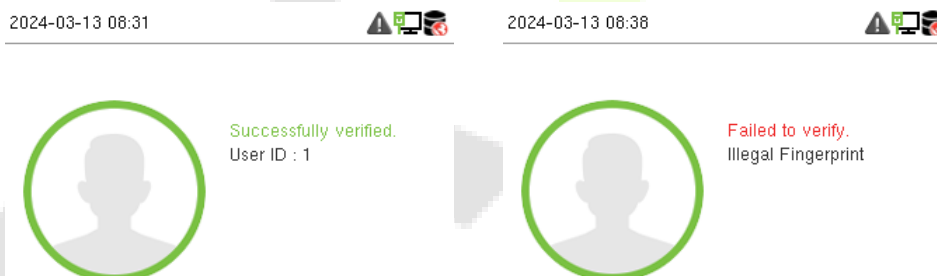
The device compares the current fingerprint with the available fingerprint data stored in its database.

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:

Verification is failed:

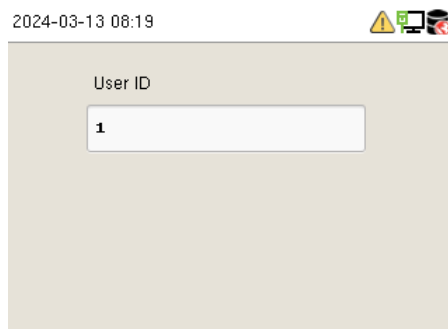


➤ 1:1 Fingerprint Verification Mode

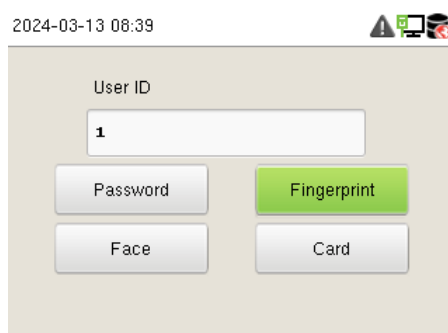
The device compares the current fingerprint with the fingerprints linked to the entered User ID through the virtual keyboard.

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

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



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.



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

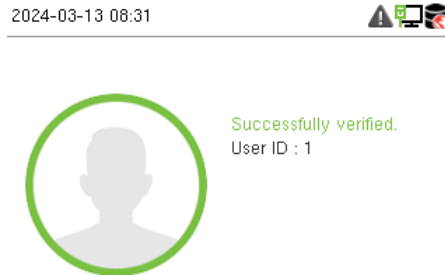


Failed to verify.
User ID : 1
Illegal Fingerprint

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.



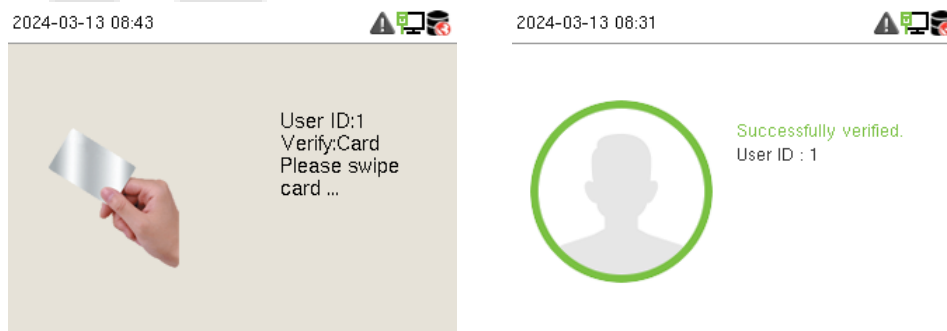
➤ 1:1 Card Verification Mode

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.



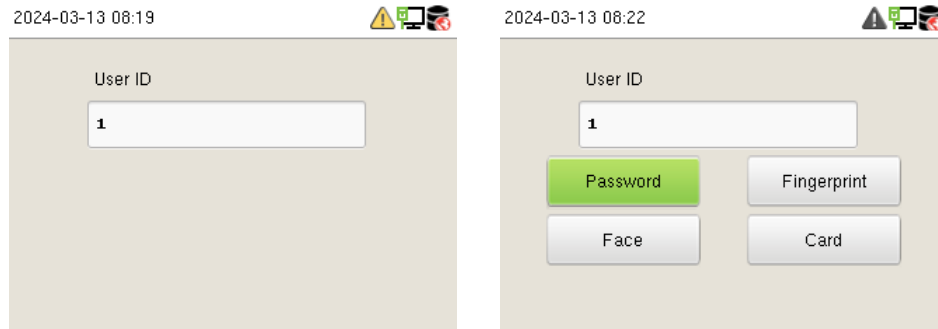
If an employee registers a fingerprint, face and password in addition to the card, the following screen will appear. Select **Card** to enter card verification mode.



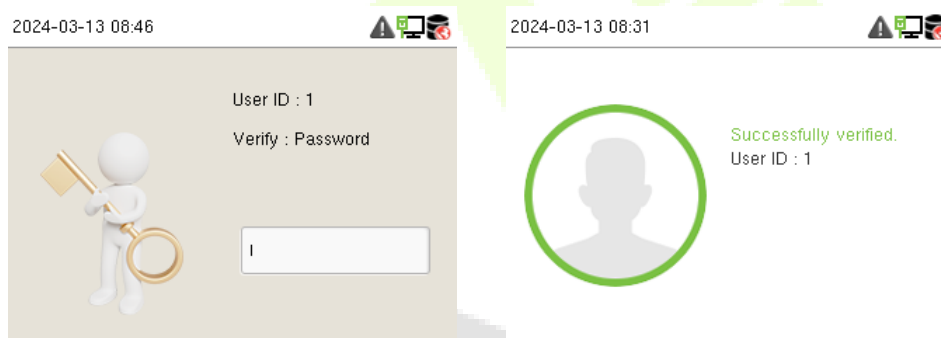
4.5.4 Password Verification

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**.

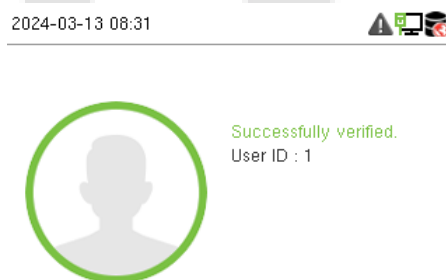


If an employee registers a fingerprint, face and card in addition to the password, the following screen will appear. Select **Password** to enter card verification mode.

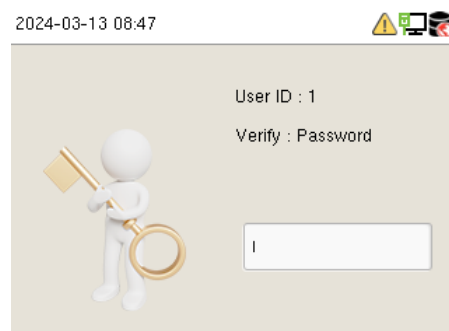


Below are the display screens after entering a correct password and a wrong password, respectively.

Verification is successful:



Verification is failed:



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:

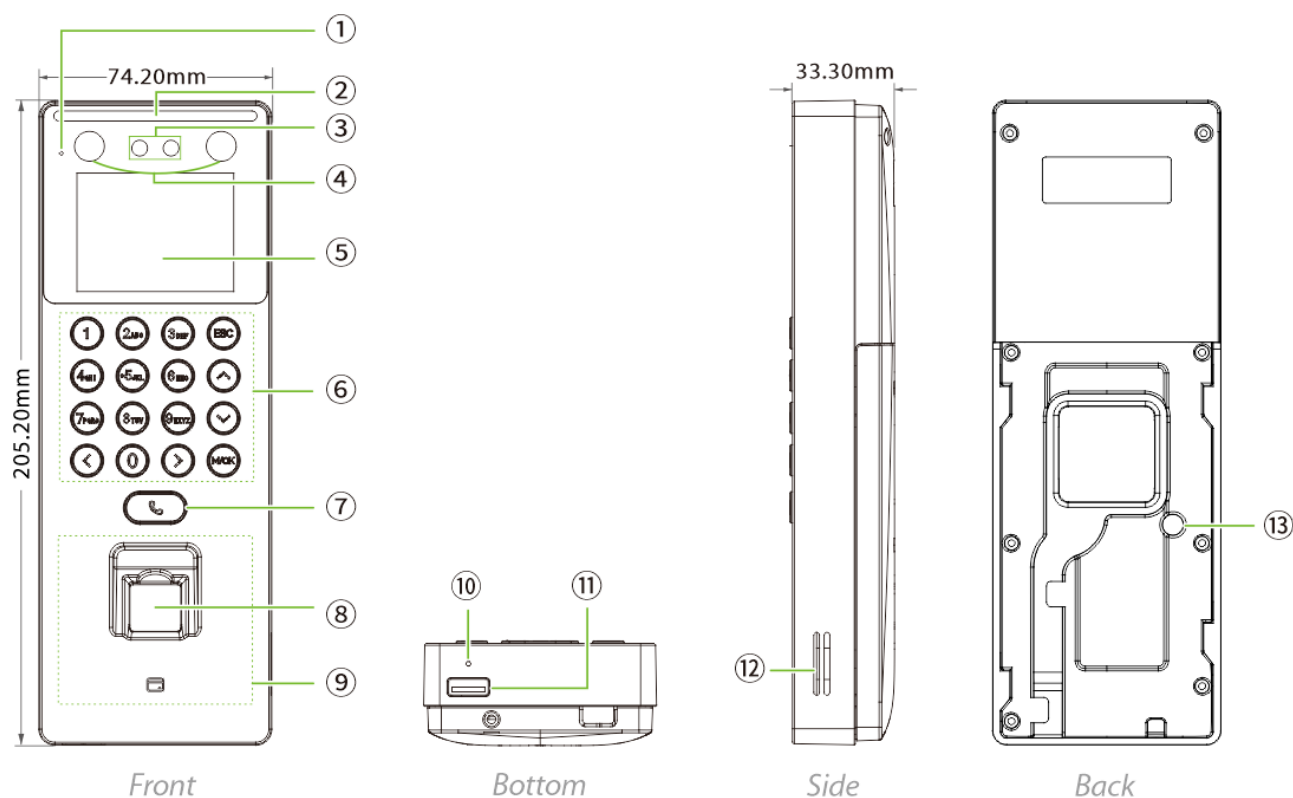
- Combined verification requires personnel to register all the different verification methods. Otherwise, employees will not be able to successfully verify the combined verification process.
- For example, if an employee has only registered for password data but the Device verification mode is set to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

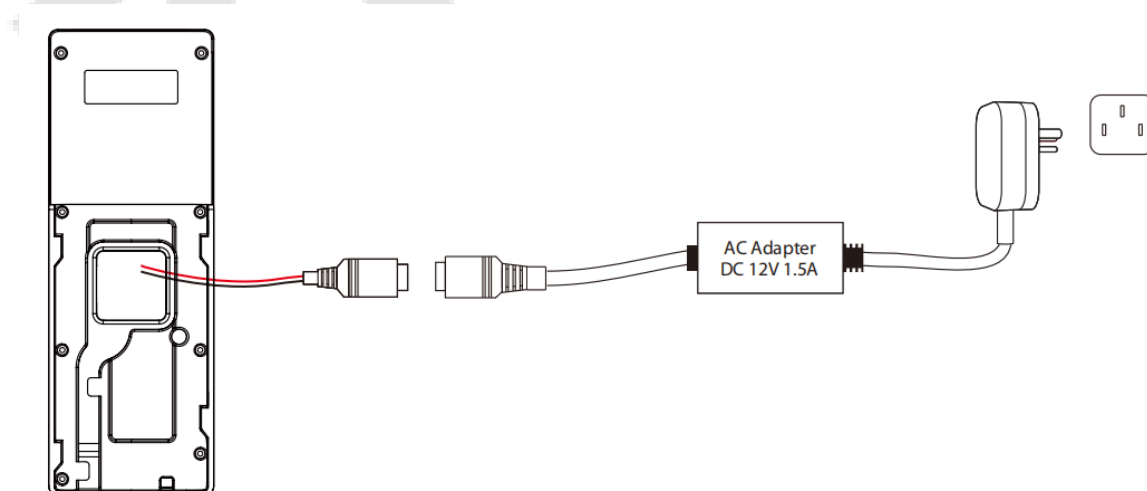
5.2 Terminal and Wiring Description

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

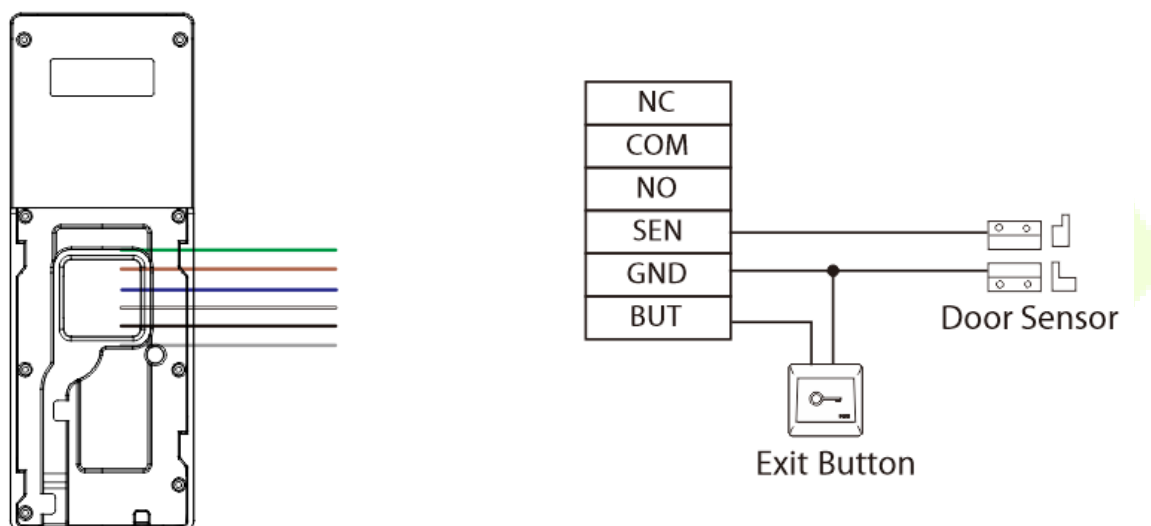
5.3.1 Power Connection



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.

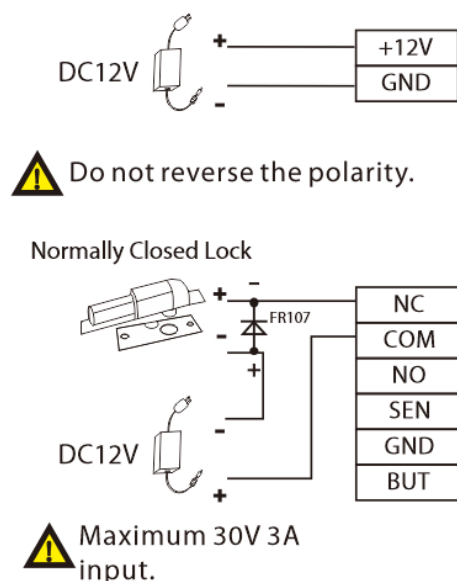
5.3.2 Door Sensor & Exit Button Connection



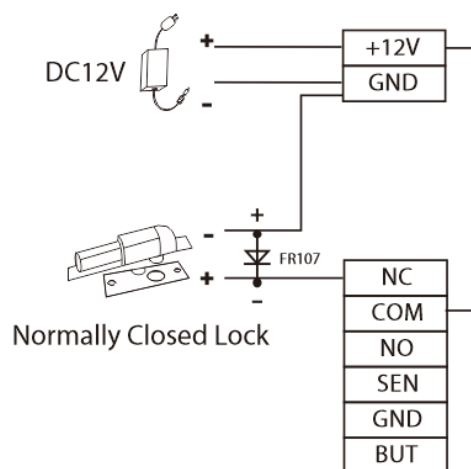
5.3.3 Lock Relay Connection

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:

1) Device not sharing power with the lock

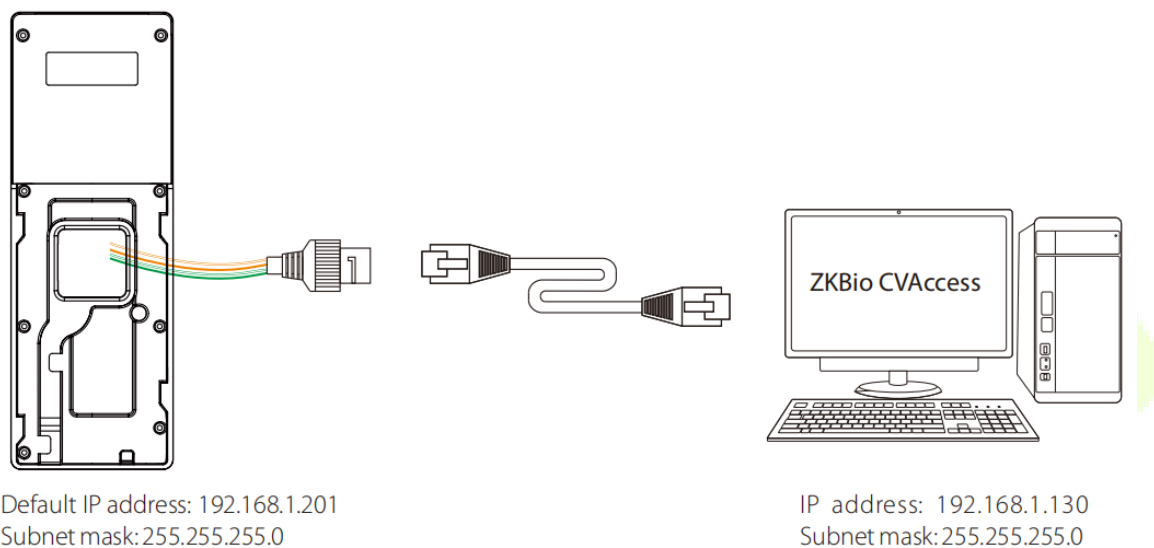


2) Device sharing power with the lock



5.3.4 Ethernet Connection

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



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



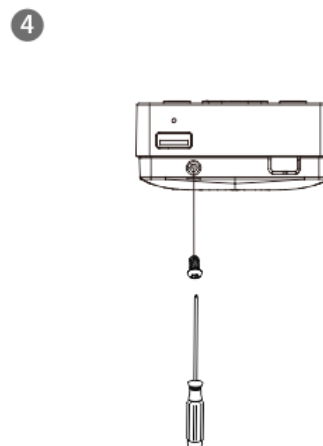
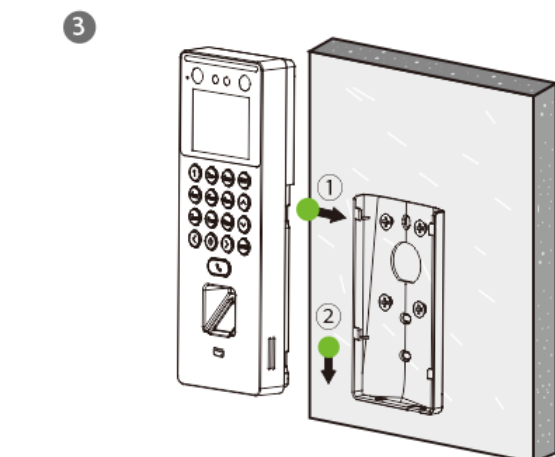
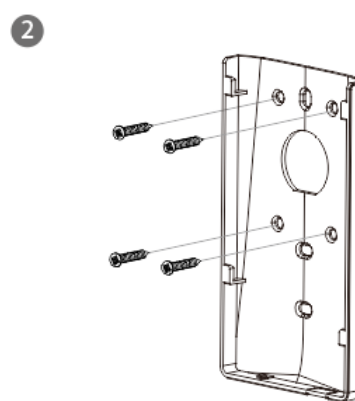
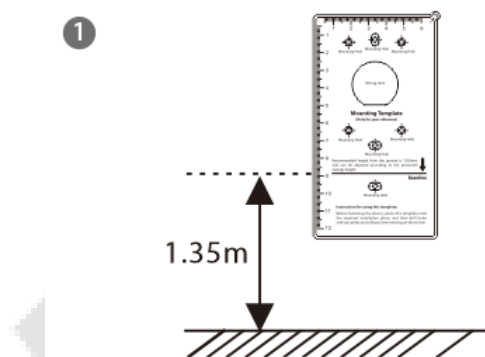
AVOID DIRECT
SUNLIGHT
AND EXPOSURE



AVOID USE OF
ANY HEAT SOURCE
NEAR THE DEVICE

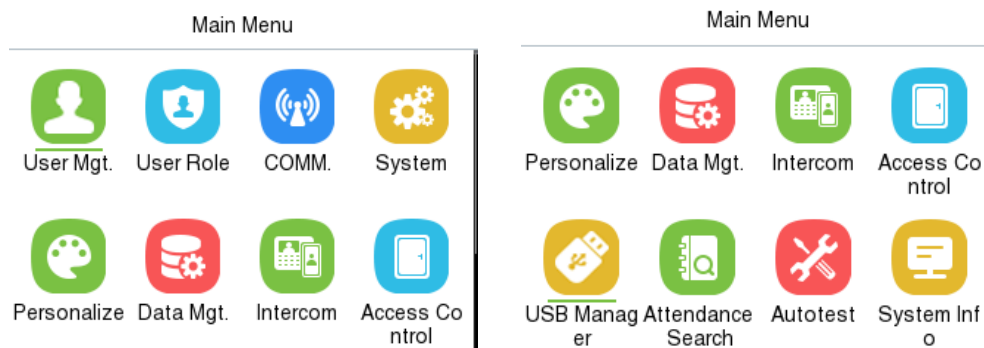
6.2 Device Installation

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:



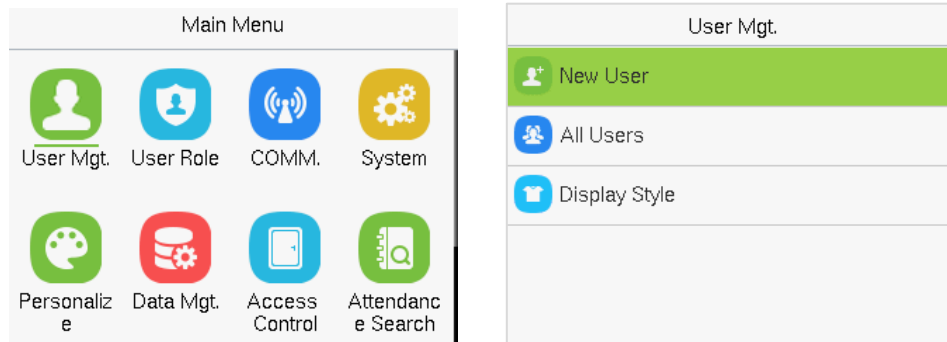
Function Description

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

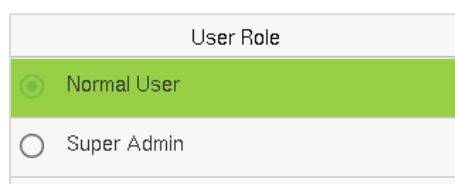
Note:

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.



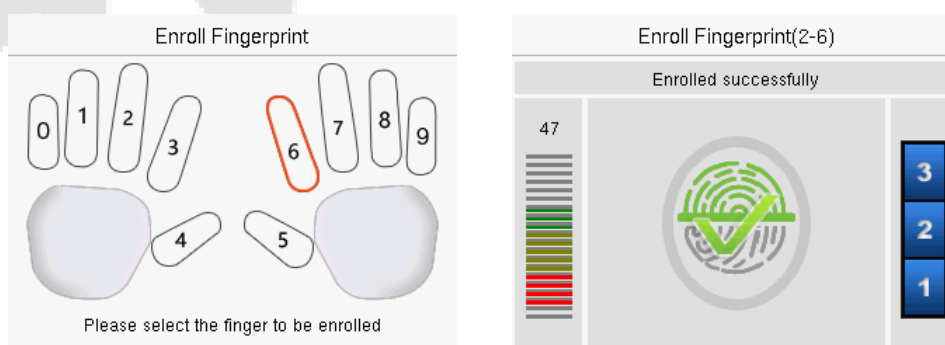
The image shows a 'User Role' selection interface. It has a title 'User Role' at the top. Below the title, there are two radio button options. The first option is 'Normal User', which is selected (indicated by a green dot). The second option is 'Super Admin', which is not selected (indicated by an empty circle).

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.

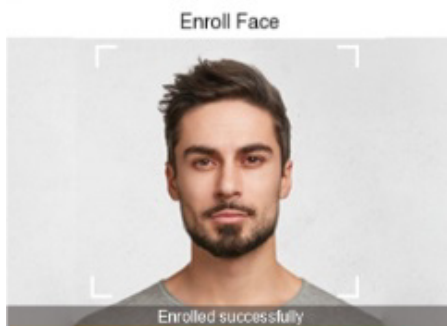


8.1.4 Register Face

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.

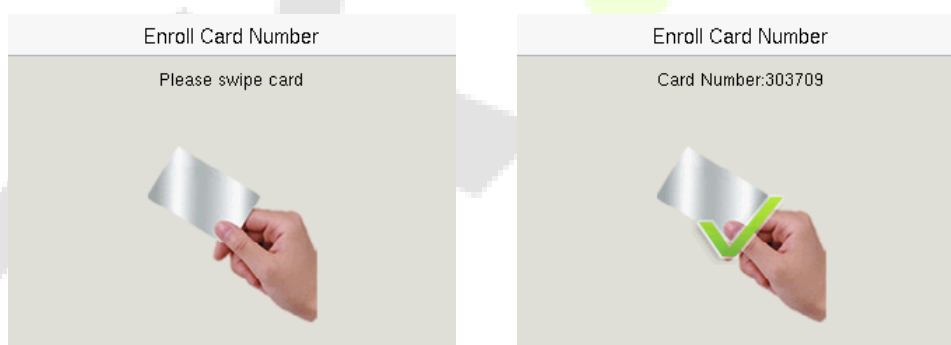
- A progress bar shows up while registering the face and then "**Enrolled Successfully**" message is displayed as the progress bar completes.
- If the face is registered already then, the "**Duplicated Face**" message shows up. The registration interface is as follows:



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:



8.1.6 Password

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

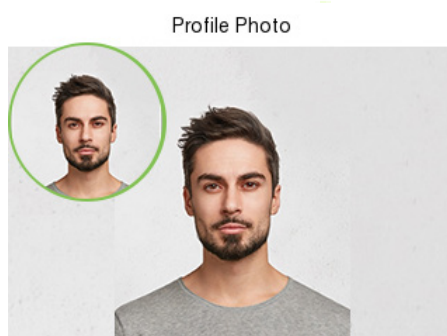
- On the Password interface, enter the required password and re-enter to confirm it and press **M/OK**.
- If the re-entered password is different from the initially entered password, then the device prompts the message as "**Password not match!**", where the user needs to re-confirm the password again.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

Password	
Please input	
<input type="password"/>	
Confirm (OK)	Cancel (ESC)

Password	
Please re-type the password.	
<input type="password" value="*****"/>	
Confirm (OK)	Cancel (ESC)

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.

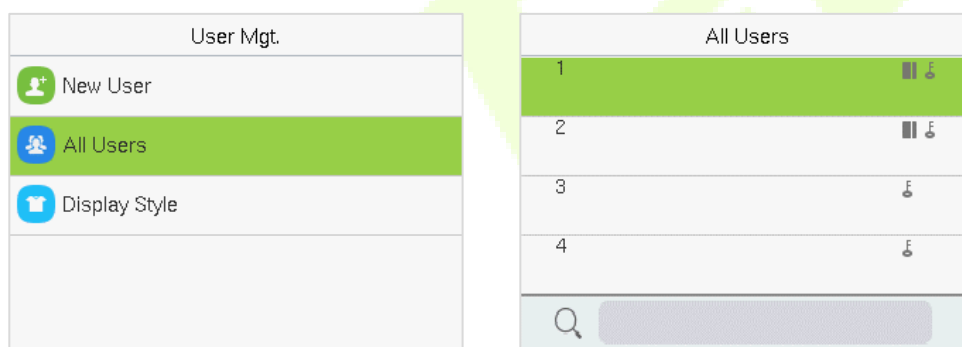
- Enter **[Access Control Role] > [Access Group]** to assign the registered users to different groups for better management. New users belong to Group 1 by default and can be reassigned to other groups. The device supports up to 99 Access Control groups.
- Tap **Time Period**, to select the time to use.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

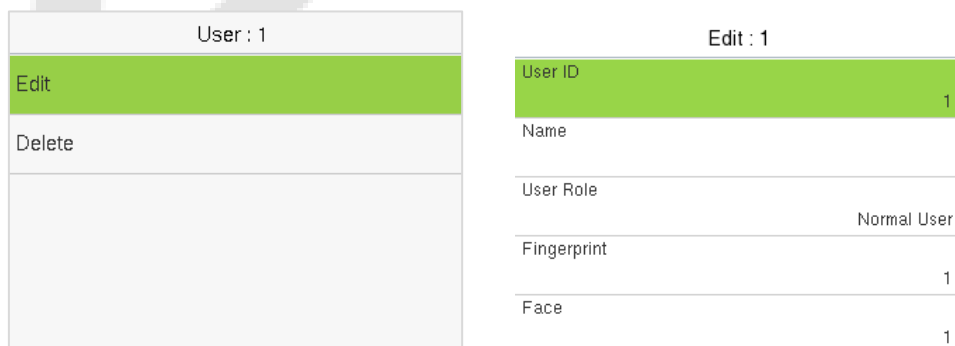
When the device is on the initial interface, press **M/OK** and enter [**User Mgt.**] > [**All Users**].

- 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.



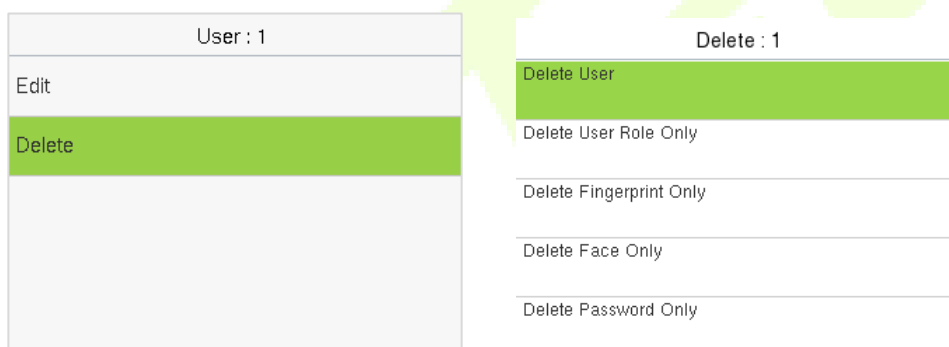
Note: The process of editing the user information is the same as adding a new user, except that the User ID cannot be modified while editing a user. The process in detail refers to "[User Registration](#)".

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.

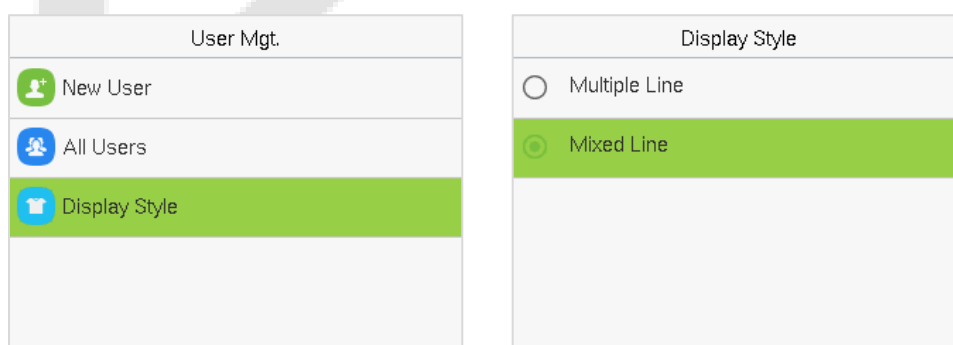
Delete Operations:

- **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	
 <input type="text"/>	

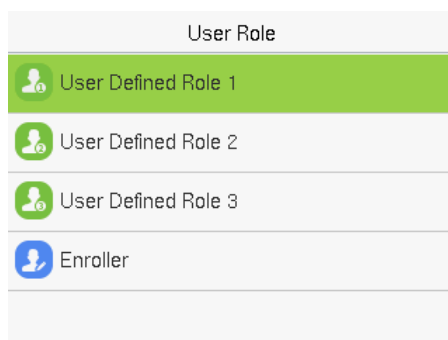
Mixed Line:

All Users	
1	 
2	 
3	
4	
 <input type="text"/>	

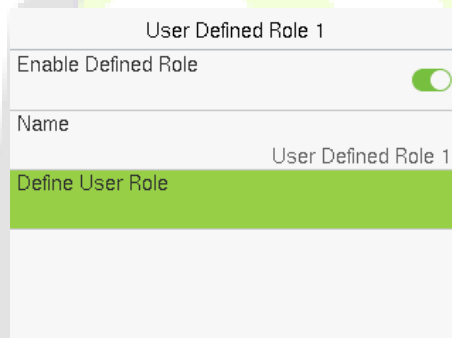
9 User Role

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

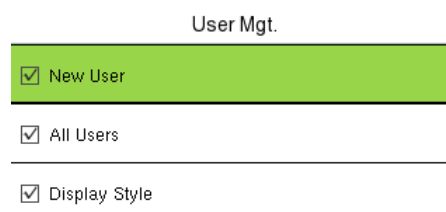
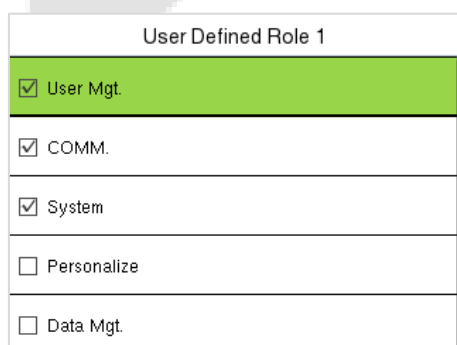
- When the device is on the initial interface, press **M/OK** and enter [**User Role**] > [**User Defined Role**] to set the user defined permissions.
- The permission scope of the custom role can be set up into 3 roles, that is, the custom operating scope of the menu functions of the user.



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



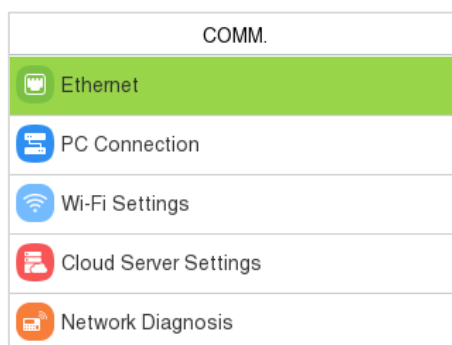
Note: If the User Role is enabled for the Device, enter **[User Mgt.] > [New User] > [User Role]** to assign the created roles to the required users. But if there is no super administrator registered in the Device, then the device will prompt **"Please enroll super admin first!"** when enabling the User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



10 Communication

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

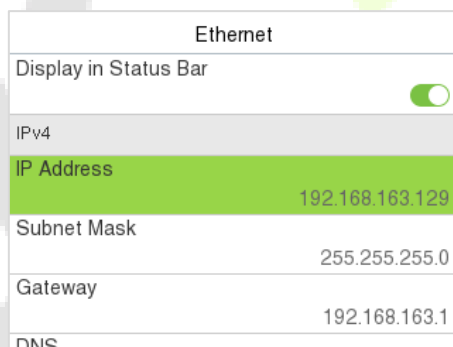
When the device is on the initial interface, press **M/OK** and select **COMM.**



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.



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 addresses for clients via server.

10.2 PC Connection

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

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

Function Description

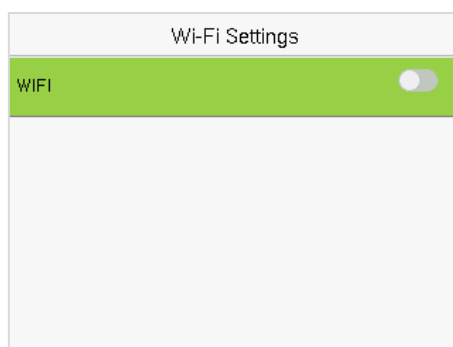
Function Name	Description
Comm Key	The default password is 0 and can be changed. The Comm Key can contain 1 to 6 digits.
Device ID	It is the identification number of the device, which ranges between 1 and 254.
TCP COMM. Port	The factory default value is 4370. Please set the value as per the requirements.
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.

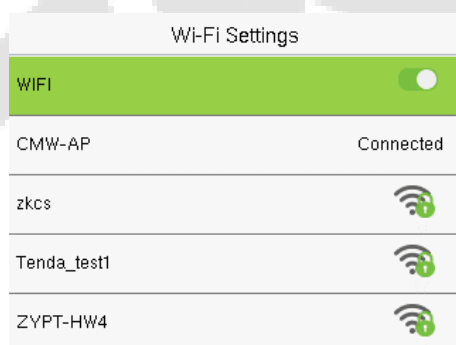
The Wi-Fi module enables data transmission via Wi-Fi (Wireless Fidelity) and establishes a wireless network environment. Wi-Fi is enabled by default in the device. If you don't need to use the Wi-Fi network, you can toggle the Wi-Fi to disable the button.

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

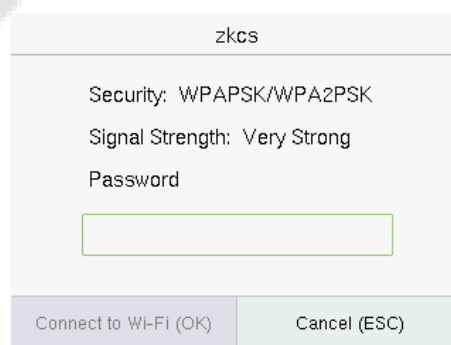


➤ Searching the Wi-Fi Network


- 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**.



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

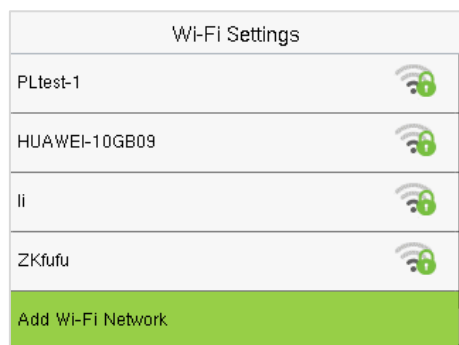


Tap on the password field to enter the password and press **M/OK**.

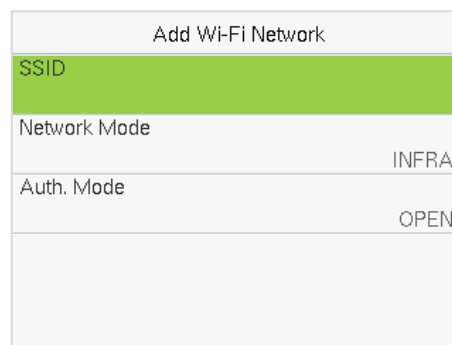
- When the Wi-Fi is connected successfully, the initial interface will display the Wi-Fi  logo.

➤ Adding Wi-Fi Network Manually

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



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

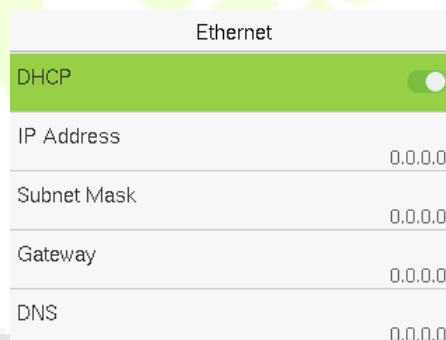
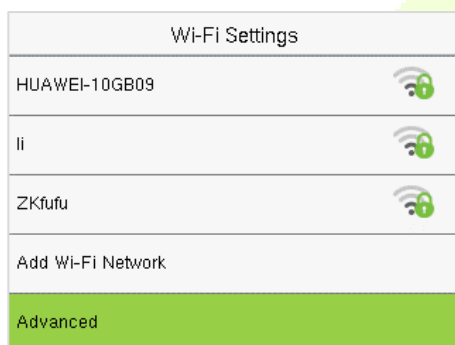


On this interface, enter the Wi-Fi network parameters. (The added network must exist.)

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.



Function Description

Function Name	Description
DHCP	Dynamic Host Configuration Protocol (DHCP) dynamically allocates IP addresses to network clients. If the DHCP is enabled, then the IP cannot be set manually.
IP Address	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	<input type="checkbox"/>
Server Address	0.0.0.0
Server Port	8081
Enable Proxy Server	<input type="checkbox"/>

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.

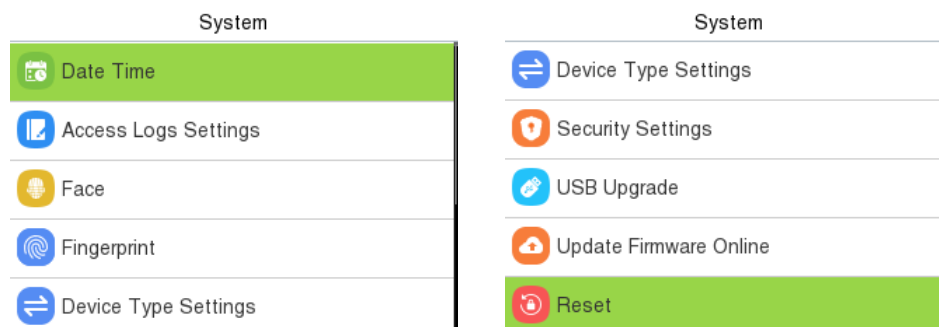
Network Diagnosis	
IP Address Diagnostic Test	110.80.38.74
Start the Diagnostic Test	

11 System Settings

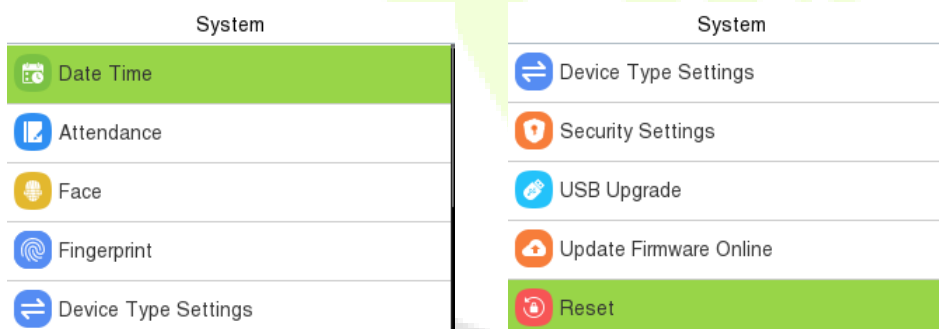
It helps to set related system parameters to optimize the accessibility of the device.

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

Access Control Terminal:

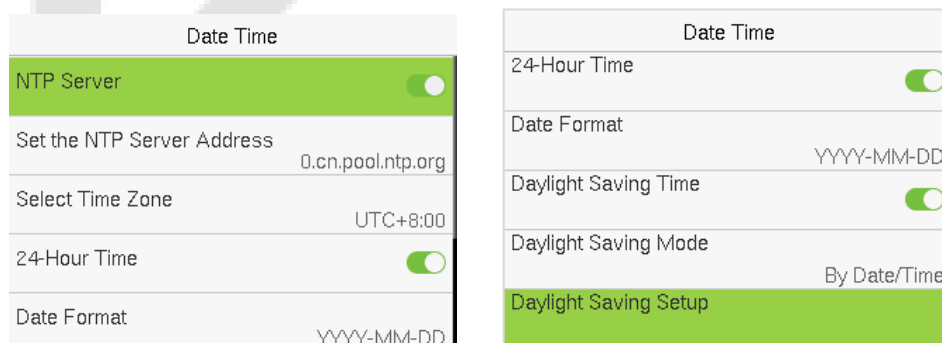


Time Attendance Terminal:



11.1 Date and Time

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



- 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		Daylight Saving Setup	
Start Month	1	Start Date	00-00
Start Week	1	Start Time	00:00
Start Day	Sunday	End Date	00-00
Start Time	00:00	End Time	00:00
End Month	1		

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	<input type="checkbox"/>
Alphanumeric User ID	<input type="checkbox"/>
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	<input type="checkbox"/>
Alphanumeric User ID	<input type="checkbox"/>
Attendance Log Alert	

99

Function Description of Access Control Terminal:

Function Name	Description
Camera Mode	<p>This function is disabled by default. When enabled, a security prompt will pop-up and the sound of shutter in the camera will turn on mandatorily. There are 5 modes:</p> <p>No photo: No photo is taken during user verification.</p> <p>Take photo, no save: Photo is taken but not saved during verification.</p> <p>Take photo and save: All the photos taken during verification is saved.</p> <p>Save on successful verification: Photo is taken and saved for each successful verification.</p> <p>Save on failed verification: Photo is taken and saved only for each failed verification.</p>
Alphanumeric User ID	Enable/Disable the alphanumeric as User ID.
Access Log Alert	<p>When the record space of the attendance access reaches the maximum threshold value, the device automatically displays the memory space warning.</p> <p>Users may disable the function or set a valid value between 1 and 9999.</p>
Periodic Del of Access Logs	<p>When access logs reach its maximum capacity, the device automatically deletes a set of old access logs.</p> <p>Users may disable the function or set a valid value between 1 and 999.</p>

Periodic Del of T&A Photo	<p>When attendance photos reach its maximum capacity, the device automatically deletes a set of old attendance photos.</p> <p>Users may disable the function or set a valid value between 1 and 99.</p>
Periodic Del of Blocklist Photo	<p>When block listed photos reach its maximum capacity, the device automatically deletes a set of old block listed photos.</p> <p>Users may disable the function or set a valid value between 1 and 99.</p>
Authentication Timeout(s)	<p>The amount of time taken to display a successful verification message.</p> <p>Valid value: 1 to 9 seconds.</p>

Function Description of Time Attendance Terminal:

Function Name	Description
Duplicate Punch Period(m)	<p>Within a set time period (unit: minutes), the duplicated attendance record will not be reserved (value ranges from 1 to 999999 minutes).</p>
Camera Mode	<p>This function is disabled by default. When enabled, a security prompt will pop-up and the sound of shutter in the camera will turn on mandatorily. There are 5 modes:</p> <p>No photo: No photo is taken during user verification.</p> <p>Take photo, no save: Photo is taken but not saved during verification.</p> <p>Take photo and save: All the photos taken during verification is saved.</p> <p>Save on successful verification: Photo is taken and saved for each successful verification.</p> <p>Save on failed verification: Photo is taken and saved only for each failed verification.</p>
Display User Photo	<p>Whether to display the user photo when the user passes the verification.</p>
Alphanumeric User ID	<p>Enable/Disable the alphanumeric as User ID.</p>

Attendance Log Alert	<p>When the record space of the attendance reaches the maximum threshold value, the device automatically displays the memory space warning.</p> <p>Users may disable the function or set a valid value between 1 and 9999.</p>
Periodic Del of T&A Data	<p>When attendance records reach its maximum storage capacity, the device automatically deletes a set of old attendance records.</p> <p>Users may disable the function or set a valid value between 1 and 999.</p>
Periodic Del of T&A Photo	<p>When attendance photos reach its maximum capacity, the device automatically deletes a set of old attendance photos.</p> <p>Users may disable the function or set a valid value between 1 and 99.</p>
Periodic Del of Blocklist Photo	<p>When block listed photos reach its maximum capacity, the device automatically deletes a set of old block listed photos.</p> <p>Users may disable the function or set a valid value between 1 and 99.</p>
Authentication Timeout(s)	<p>The amount of time taken to display a successful verification message.</p> <p>Valid value: 1 to 9 seconds.</p>
Recognition Interval(s)	<p>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.</p>

11.3 Face Parameters

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

Function Description

Function Name	Description
1:N Threshold Value	<p>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.</p> <p>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.</p>
1:1 Threshold Value	<p>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.</p> <p>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 63.</p>
Face Enrollment Threshold	During face enrollment, 1:N comparison is used to determine

	<p>whether the user has already registered before.</p> <p>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.</p>
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 Algorithm	Finger VX13.0

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 Algorithm	Used to switch the version of the fingerprint algorithm. The default is Finger VX13.0, can switch to Finger VX10.0.

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

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

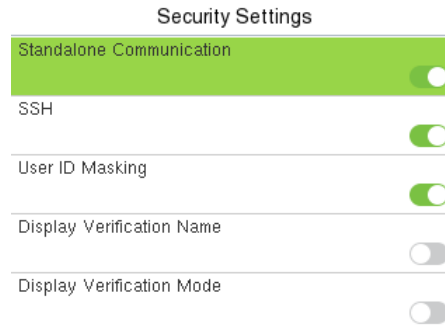
Function Description

Function Name	Description
Communication Protocol	Set the device communication protocol. (BEST protocol is suitable for ZKBio Zlink, please refer to 22 Connecting to ZKBio Zlink Web.)
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.



Function Description

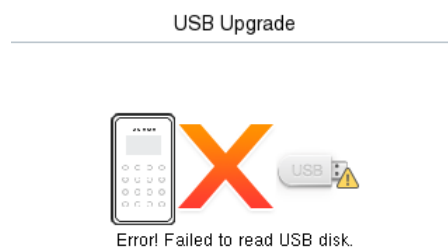
Function Name	Description
Standalone Communication	To avoid being unable to use when the device is offline, you can download the C/S software (such as ZKAccess 3.5) on your computer in advance for offline use.
SSH	SSH is used to enter the background of the device for maintenance.
User ID Masking	When 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.

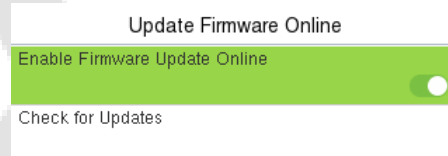
Select **USB Upgrade** on the **System** interface.



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

11.8 Update Firmware Online

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



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

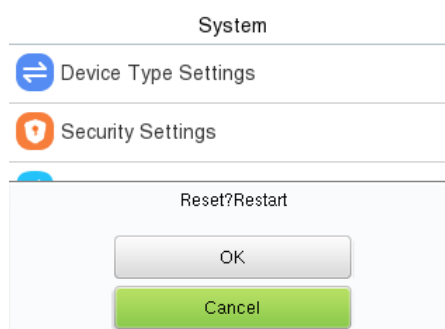
- If the query fails, the interface will prompt "Query failed".
- If the firmware version of the device is latest, it will prompt that the current firmware version is already the latest.

- 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

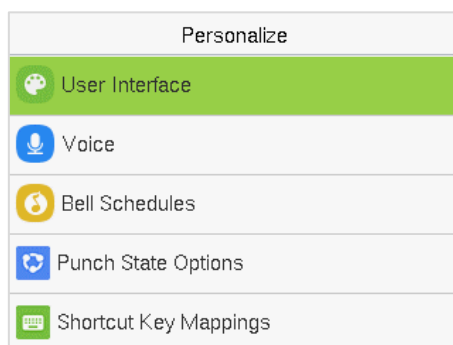
The Factory Reset function restores the device settings such as communication settings and system settings, to the default factory settings (this function does not clear registered user data).

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.



12.1 User Interface

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



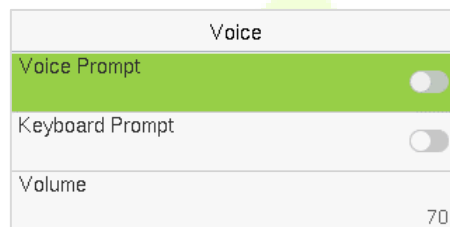
Function Description

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.

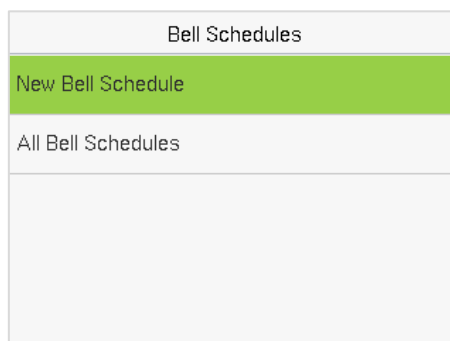


Function Description

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.

Bell Schedules	New Bell Schedule
New Bell Schedule	Bell Status <input type="checkbox"/>
All Bell Schedules	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	<p>Off: Disable the punch state function. Therefore, the punch state key set under Shortcut Key Mappings menu will become invalid.</p> <p>Manual Mode: Switch the punch state key manually, and the punch state key will disappear after Punch State Timeout.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>Fixed Mode: Only the manually fixed punch state key will be shown. Users cannot change the status by tapping any other keys.</p>
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	<p>Select whether an attendance state needs to be selected after verification.</p> <p>ON: Attendance state needs to be selected after verification.</p> <p>OFF: Attendance state need not requires to be selected after verification.</p>

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
<input type="checkbox"/> Monday
<input checked="" type="checkbox"/> Tuesday
<input checked="" type="checkbox"/> Wednesday
<input checked="" type="checkbox"/> Thursday
<input checked="" type="checkbox"/> 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.

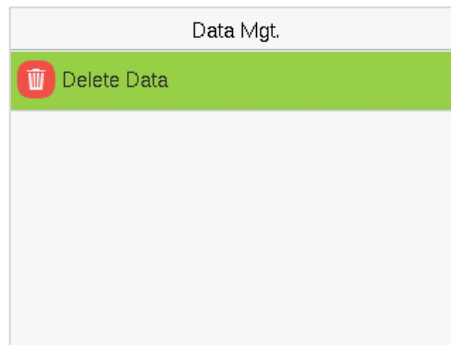
Monday	
13:57	
<div><div>+</div><div>13</div><div>-</div></div>	<div><div>+</div><div>57</div><div>-</div></div>
HH	MM
Confirm (OK)	Cancel (ESC)

Set Switch Time	
Switch Cycle	Daily
Monday	13:57
Tuesday	
Wednesday	
Thursday	

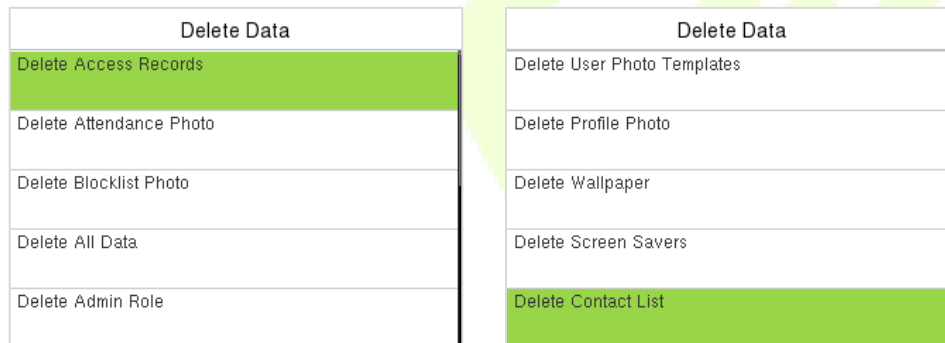
Note: When the function is set to Undefined, the device will not enable the punch state key.

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.

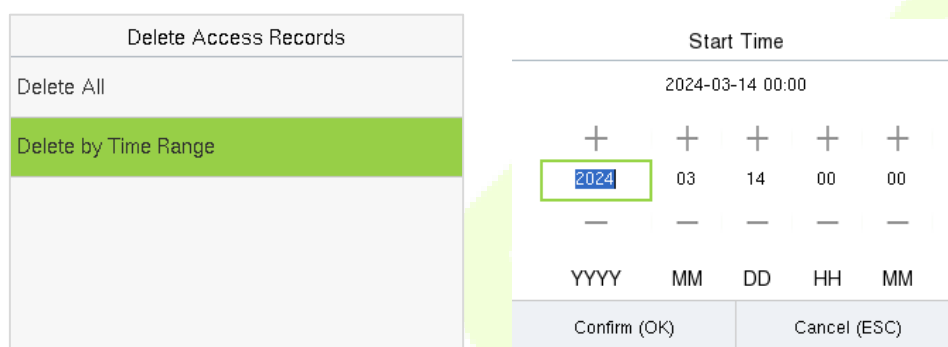


Function Description

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.



Delete Access Records

Delete All
Delete by Time Range

Start Time
2024-03-14 00:00

+

+

+

+

+

2024

03

14

00

00

-

-

-

-

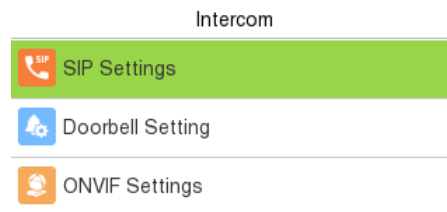
-

YYYY
MM
DD
HH
MM

Confirm (OK)
Cancel (ESC)

14 Intercom

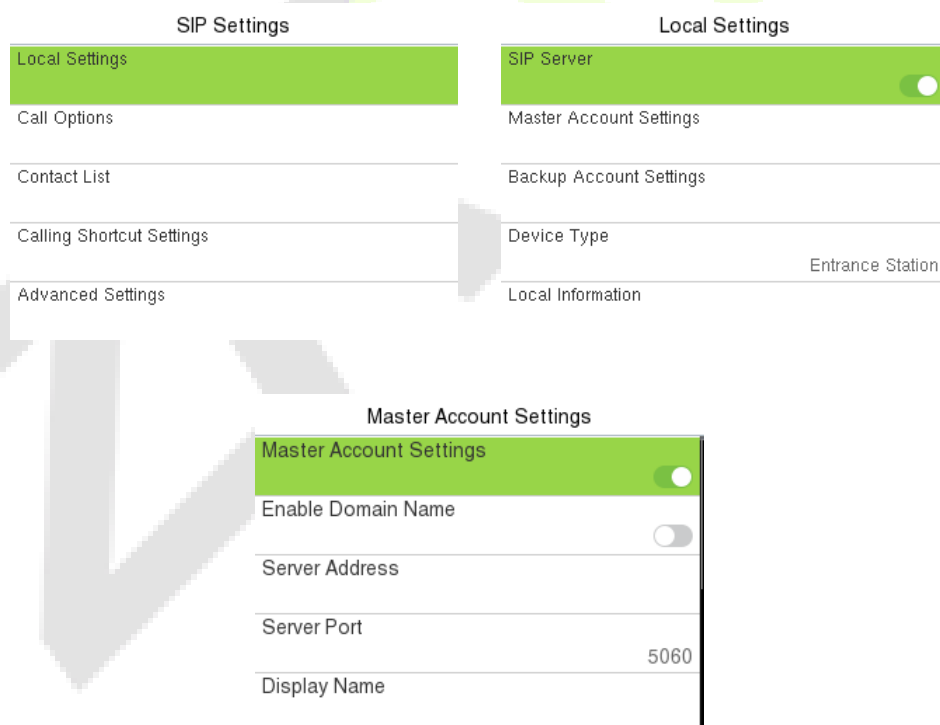
When the device is on the initial interface, press **M/OK** and select **Intercom** to set relevant parameters of intercom, including SIP, Doorbell and ONVIF Settings.



14.1 SIP Settings

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

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



Function Description

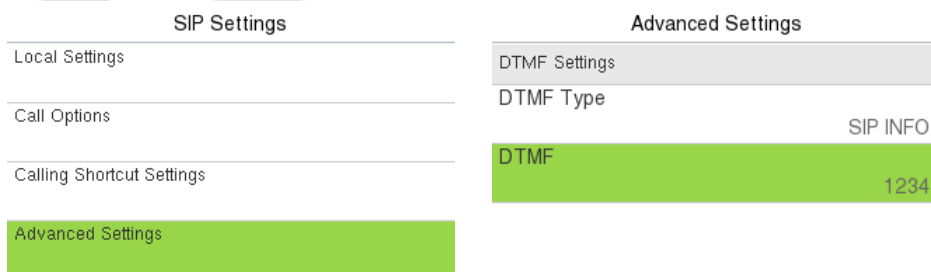
Function Name		Description
Local Settings	SIP Server	Select whether to enable the SIP server. When it is enabled, the server account needs to be set.
	Master Account Settings	Select whether to enable the master account settings. After enabling, it is necessary to set the server address, server port, display name, user name, verify ID, password and transport protocol. (Note: Turning off this feature will disable the SIP server function.) Enable Domain Name: Select whether to enable the domain name mode. Server Address: Enter the server address. Server Port: Enter the server port. Display Name: Enter the display name of server. User Name: Enter the username of server. Verify ID: Enter the verify ID of server. Password: Enter the password of server. Transport Protocol: Set the transport protocol between the device and indoor station.
	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.
	Device Type	Can be set as Entrance Station, Access Control Terminal or Fence Terminal.
	Local Information	Set specific location information of the device, including the block, unit, floor and door number.
	Transport Protocol	Set the transport protocol between the device and indoor station.
Call Options	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.
	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 station calls.
	Auto-Answer Delay Time	The device will automatically answer after the set delay time if the indoor station calls, valid value 0 to 10 seconds.

	Encryption	It is disabled by default.
Contact List		When the SIP server is disabled, the device number and call address of the indoor stations can be added here.
Calling Shortcut Settings	Call Mode	<p>It can be set as Standard Mode or Direct Calling Mode.</p> <ul style="list-style-type: none"> In Standard mode, there are 3 shortcut keys that can be defined in the device: Management Center, ROOM1 and ROOM2. You can set a shortcut key to call the indoor station quickly without entering the IP address or number of the indoor station each time. In Direct Calling mode, the user can call multiple indoor stations at the same time.
Advanced Settings	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 station.

The device and the indoor station to achieve video intercom there are two modes, respectively, the LAN and SIP server.

14.1.1 Local Area Network Use

- Set the indoor station to the same network segment as the device.
- On the **SIP Settings** interface, enter [**Advanced Settings**] > [**DTMF**] to set the value as same as the value of DTMF in the indoor station.



- On the **SIP Settings** interface, enter [**Contact List**] > [**Add**] to add the connected indoor station.

Note: The **Contact List** is only available when the SIP Server is disabled.

SIP Settings		Contact List		Calling Shortcut Settings	
Local Settings		Add		Device Number	
Call Options		101 192.168.1.101		Call Address	
Contact List		102 192.168.1.102			
Calling Shortcut Settings		103 192.168.1.103			
Advanced Settings		<input type="text"/>			

Device Number

Please input


00 . 02 . 32

Confirm (OK)

Cancel (ESC)

Device Number: Customize the number of the indoor station, you can enter this number on the device to call the indoor station quickly for video intercom. (For example, **232** corresponds to **00.02.32** in the Device Number setting.)

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

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

232

Ring the Doorbell to Call Admin

Press Up Key to enter "."

Confirm (OK)

Cancel (ESC)

232

Waiting for someone to answer...

Speaker

Microphone

Call End

Custom the Calling Shortcut Keys


- On the **SIP Settings** interface, tap **Calling Shortcut Settings** to define the shortcut keys.

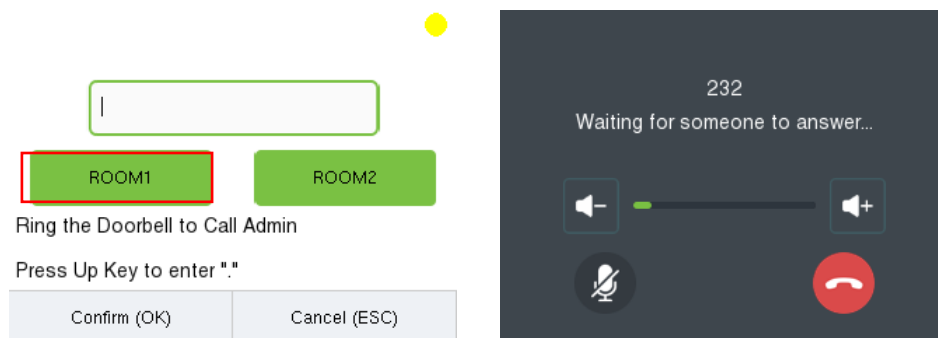
SIP Settings		Calling Shortcut Settings		Device Number : 232	
Local Settings		Management Center		Enable	
Call Options		101		Name	
Contact List		Standard Mode		ROOM1	
Calling Shortcut Settings		ROOM1 Enable		Device Number	
Advanced Settings		ROOM2 Enable		232	
				IP Address	
				192.168.161.232	

Name: Customize the name of the shortcut keys.

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

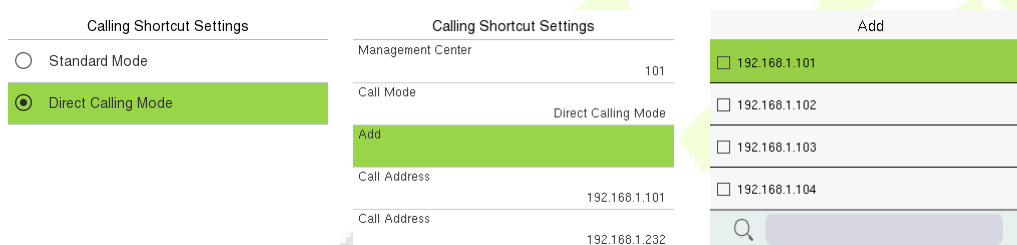
IP Address: Once the device number is set, it will be automatically displayed.


- Then you can press the doorbell button  on the device and select the calling shortcut keys to call the indoor station.

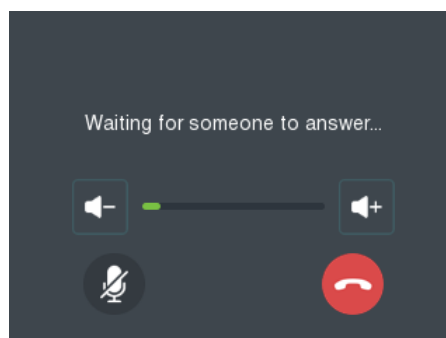
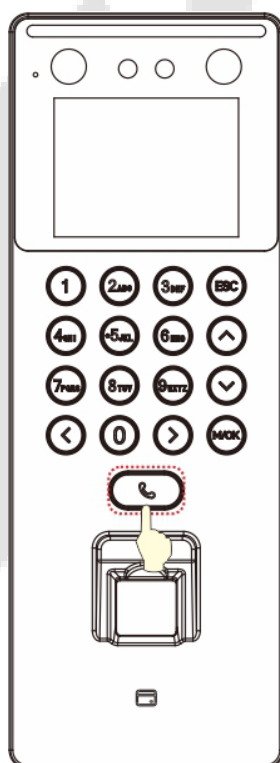


● Direct Calling

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



2. Then you can press the doorbell button  on the device to call the indoor stations at the same time.



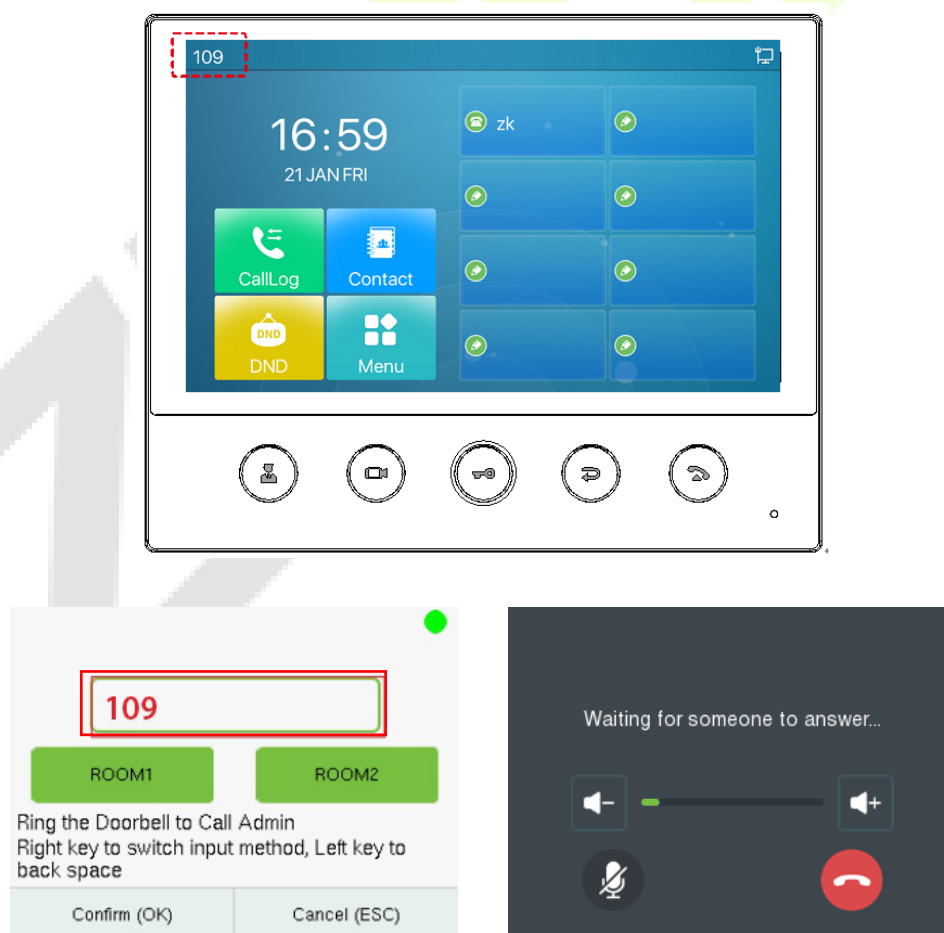
14.1.2 SIP Server

1. On the **SIP Settings** interface, enter **[Local Settings]>[SIP Server]** to enable it, and enter **[Master Account Settings]** to set the server-related parameters, as shown below:

Local Settings		Master Account Settings	
SIP Server <input checked="" type="checkbox"/>		Master Account Settings <input checked="" type="checkbox"/>	
Master Account Settings		Enable Domain Name <input type="checkbox"/>	
Backup Account Settings		Server Address	
Device Type		Server Port	
Entrance Station		5060	
Local Information		Display Name	

2. After correctly setting up the SIP, the yellow dot in the upper right corner of the call page will become green, indicating that the device is connected to the server. You can then initiate a call to the account name of the indoor station.

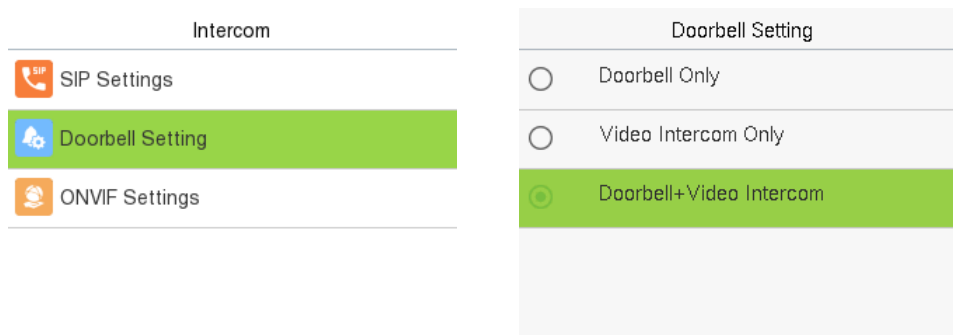
Note: Customers create their own SIP server.



For details on the operation and use of the indoor station, please refer to the *Indoor Station User Manual*.

14.2 Doorbell Setting

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



Function Description:

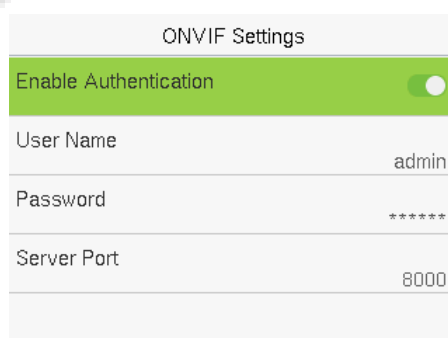
Function Name	Description
Doorbell Setting	<p>Doorbell Only: When the user clicks on the doorbell button, only the doorbell rings.</p> <p>Video Intercom Only: When the user clicks on the doorbell button, only the device makes a call.</p> <p>Doorbell+Video Intercom: When the user clicks on the doorbell button, the doorbell rings and the device makes a call at the same time.</p>

14.3 ONVIF Settings



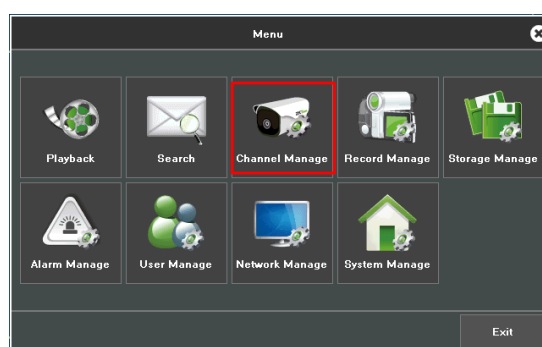
Note: This function needs to be used with the network video recorder (NVR).

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

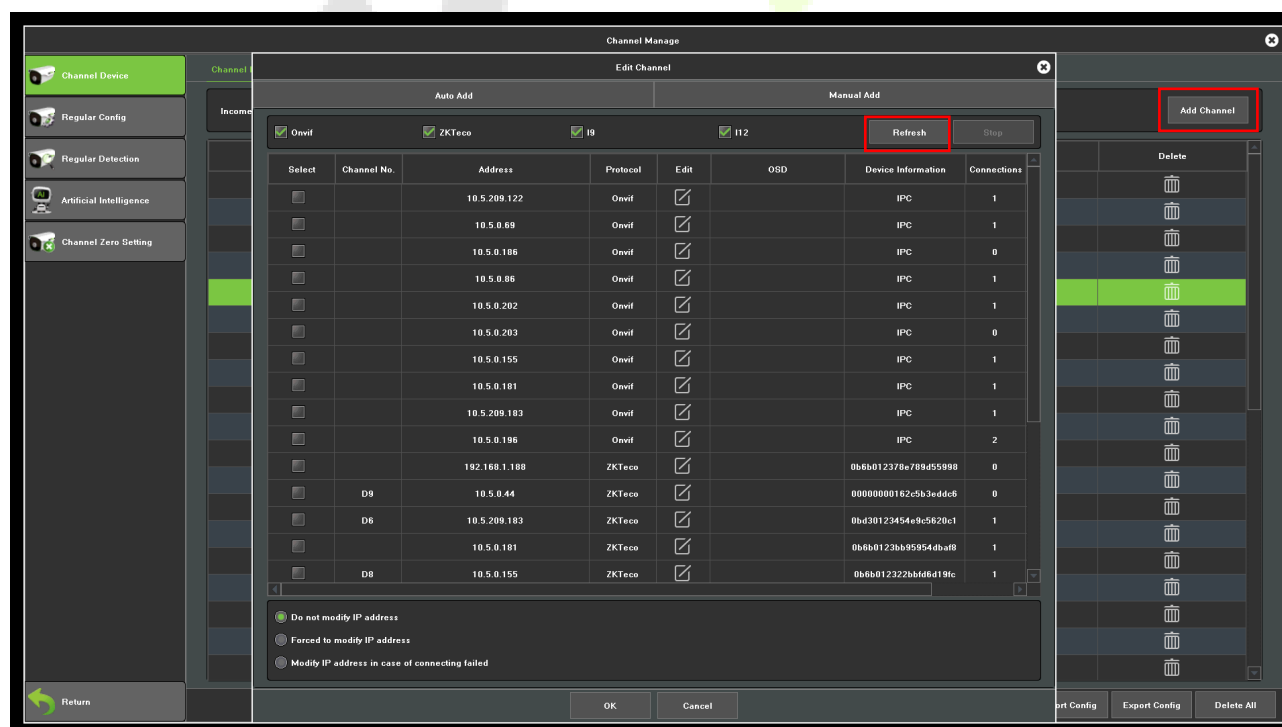


Function Name	Description
Enable Authentication	Enable/Disable the Authentication Function. When it is disabled, there is no need to input the User Name and Password when adding the device to the NVR.
User Name	Set the User Name. The default is admin.
Password	Set the password. The default is admin.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

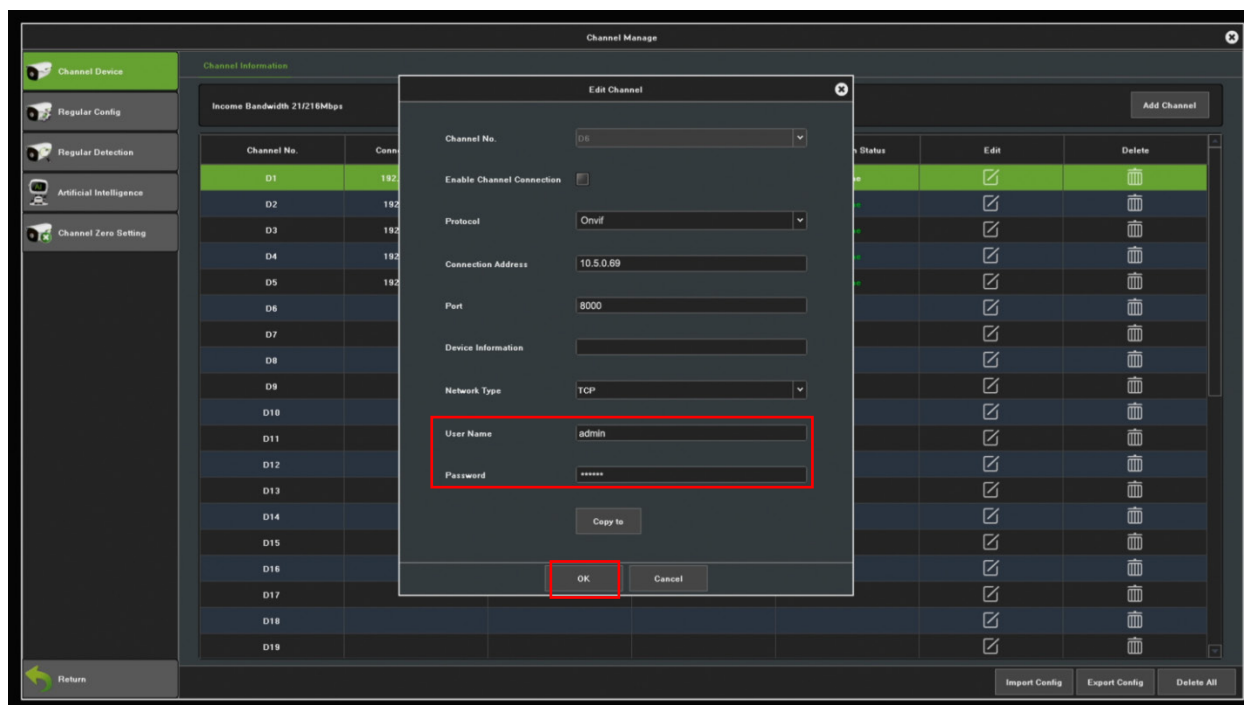
3. On the NVR system, click on **[Start]** > **[Menu]**, then the main menu will pop up.



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

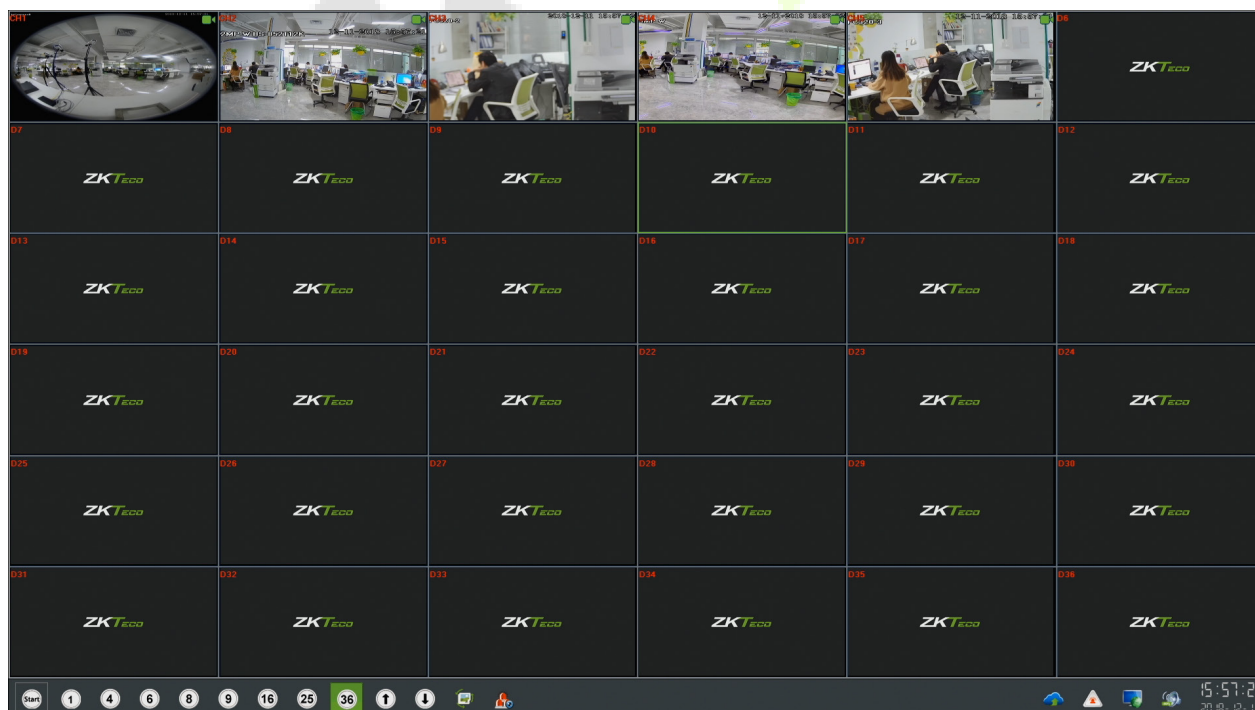


- Select the checkbox for the device you want to add and edit the parameters in the corresponding text field, then click on **OK** to add it to the connection list.



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

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

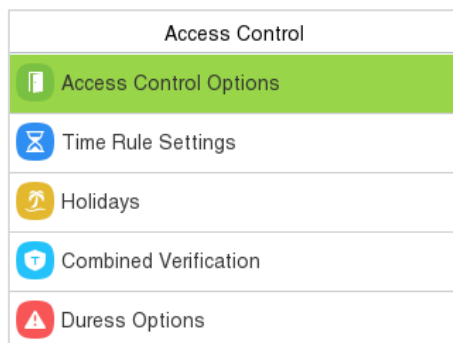


For more details, please refer to the *NVR User Manual*.

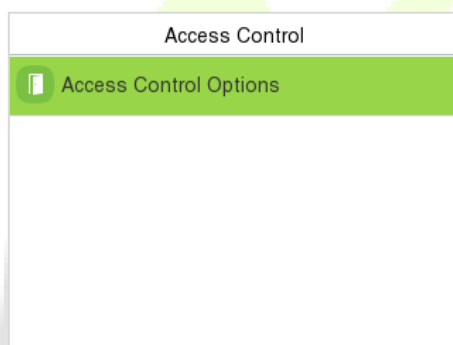
15 Access Control

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:

Time Attendance Terminal:

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	<p>There are three Sensor types: None, Normal Open, and Normal Closed.</p> <p>None: It means the door sensor is not in use.</p> <p>Normally Open: It means the door is always left open when electric power is on.</p> <p>Normally Closed: It means the door is always left closed when electric power is on.</p>
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)	<p>The length of time that the device controls the electric lock to be in unlock state.</p> <p>Valid value: 0 to 10 seconds.</p>
Door Sensor Delay (s)	<p>If the door is not locked and is left open for a certain duration (Door Sensor Delay), an alarm will be triggered.</p> <p>The valid value of Door Sensor Delay ranges from 1 to 255 seconds.</p>

Door Sensor Type	<p>There are three Sensor types: None, Normal Open, and Normal Closed.</p> <p>None: It means the door sensor is not in use.</p> <p>Normally Open (NO): It means the door is always left open when electric power is on.</p> <p>Normally Closed (NC): It means the door is always left closed when electric power is on.</p>
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 Periods.
- Each time-period represents **10** Time Zones, i.e., **1** week and **3** holidays, and each time zone is a standard 24 hour period per day and the user can only verify within the valid time-period.
- One can set a maximum of 3 time periods for every time zone. The relationship among these time-periods is "**OR**". Thus, when the verification time falls in any one of these time-periods, the verification is valid.
- The Time Zone format of each time-period is **HH MM-HH MM**, which is accurate to minutes according to the 24-hour clock.

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

Time Rule[2/50]

Sunday	[00:00 23:59] [00:00 23:59] [00:00 23:59]
Monday	[00:00 23:59] [00:00 23:59] [00:00 23:59]
Tuesday	[00:00 23:59] [00:00 23:59] [00:00 23:59]
Wednesday	[00:00 23:59] [00:00 23:59] [00:00 23:59]

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

Time Period 1			
00:00 23:59			
+	+	+	+
00	00	23	59
-	-	-	-
HH	MM	HH	MM
Confirm (OK)		Cancel (ESC)	

Specify the start and the end time, and then 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.

Holidays
Add Holiday
All Holidays

➤ **Add a New Holiday:**

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

Holidays	
No.	1
Date	Undefined
Holiday Type	Holiday Type 1
Repeats Every Year	<input checked="" type="checkbox"/>

➤ **Edit a Holiday:**

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

➤ **Delete a Holiday:**

On the **Holidays** interface, select a holiday item to be deleted and tap **Delete**. Press **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 $0 \leq N \leq 5$ and the number of members N may all belong to one access group or may belong to five different access groups.

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.

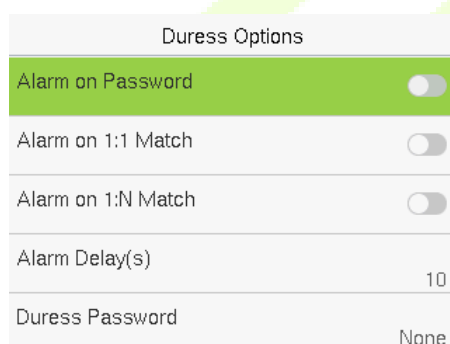
- If the **Door-unlock combination 3** is set as (09 09 09 09 09). It indicates that there are 5 people in this combination; all of which are from AC Group 9.
- If the **Door-unlock combination 4** is set as (03 05 08 00 00). It indicates that the unlock combination 4 consists of only three people. The 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	<input checked="" type="checkbox"/>
Alarm on 1:1 Match	<input type="checkbox"/>
Alarm on 1:N Match	<input type="checkbox"/>
Alarm Delay(s)	10
Duress Password	None

Function Description:

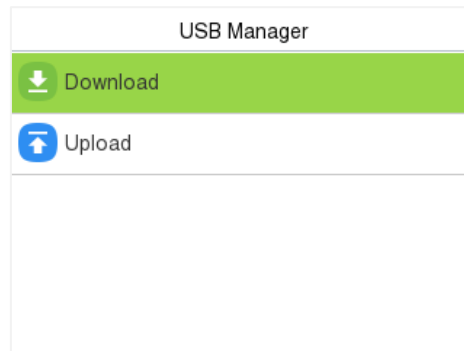
Function Name	Description
Alarm on Password	When a user uses the password verification method, an alarm signal will be generated, otherwise there will be no alarm signal.
Alarm on 1:1 Match	When a user uses the 1:1 verification method, an alarm signal will be generated, otherwise there will be no alarm 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.

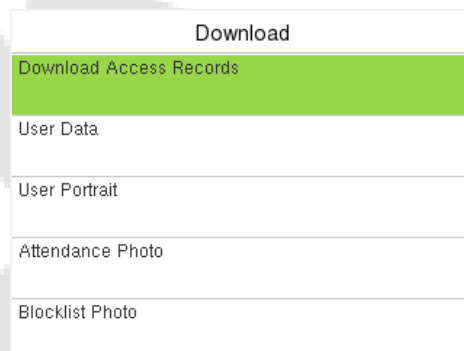
Select **USB Manager** on the main menu interface.



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

16.1 USB Download

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

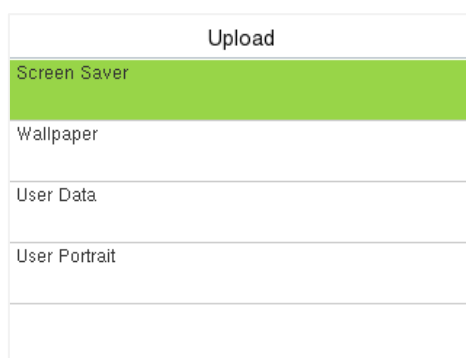


Menu	Description
Download Access Records	To download access record in specified time period into USB disk.
User Data	To download all user information from the device into USB disk.
User Portrait	To download all user portraits from the device into a USB disk.

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**.

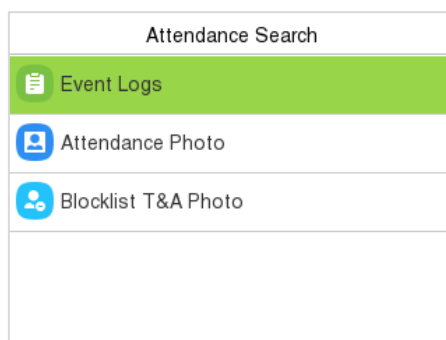


Menu	Description
Screen Save	To upload all screen savers from USB disk into the device. You can choose Upload selected photo or Upload all photos. The images will be displayed on the device's main interface after upload.
Wallpaper	To upload all wallpapers from USB disk into the device. You can choose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

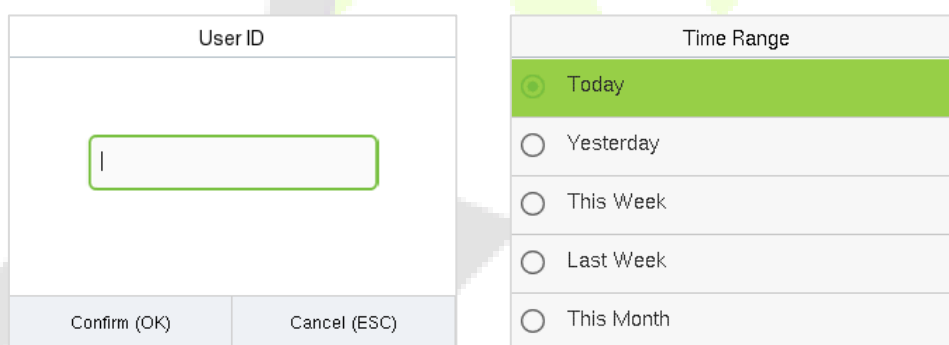
Once the identity of a user is verified, the access record is saved in the device. This function enables users to check their event logs.

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.

The image shows two side-by-side input forms. The left form is titled "User ID" and has a text input field with a green border. Below the input field are two buttons: "Confirm (OK)" and "Cancel (ESC)". The right form is titled "Time Range" and has five radio button options: "Today" (selected and highlighted in green), "Yesterday", "This Week", "Last Week", and "This Month".

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.

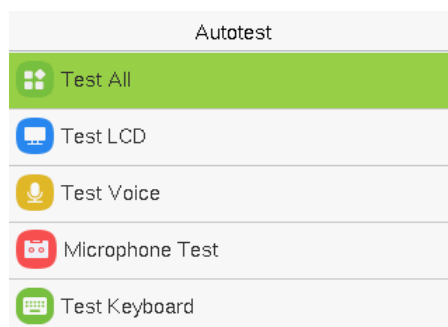
Personal Record Search		
Date	User ID	Time
03-14		Number of R...:27
	0	15:50 15:42 15:34
		14:59 14:59 14:40
		14:40 14:01 13:14
		12:57 12:27 12:15
		12:15 12:15 10:09
		10:01 09:28 08:04
Prev : Left Key Next : Right Key Details : OK		

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	

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

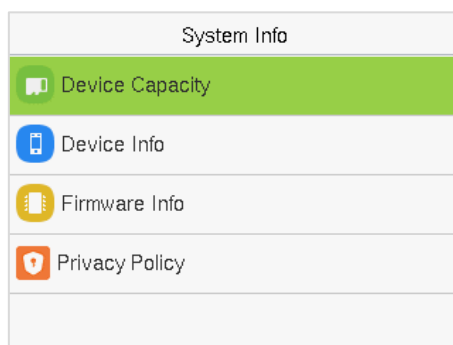


Function Description

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.



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.

The figure shows two screenshots from a device's configuration menu. The left screenshot is titled 'Ethernet' and shows a table for IPv4 settings: IP Address (192.168.163.129), Subnet Mask (255.255.255.0), and Gateway (192.168.163.1). The right screenshot is titled 'Cloud Server Settings' and shows: Server Mode (ADMS), Enable Domain Name (disabled), Server Address (58.23.12.98), Server Port (8881), and Enable Proxy Server (disabled). Red boxes highlight the IP Address, Subnet Mask, Gateway, Server Address, and Server Port fields in both screenshots.

➤ 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:

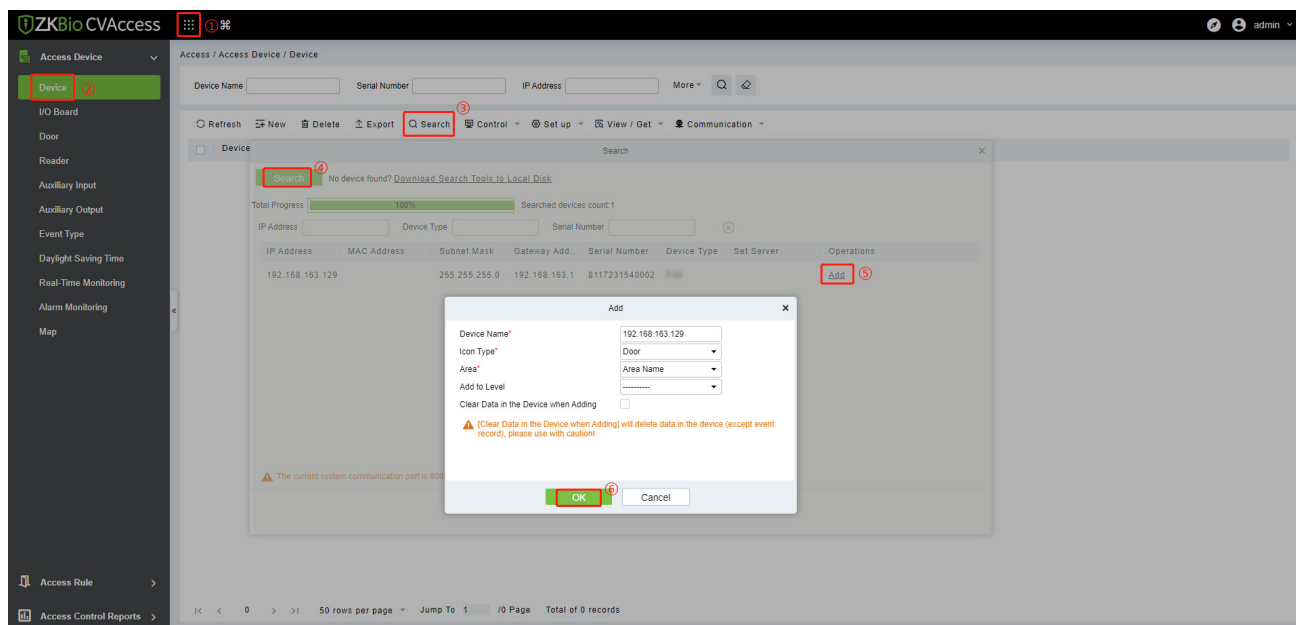
The figure is a screenshot of the ZKBio CVAccess web interface. The left sidebar shows a menu with 'Communication Monitor' highlighted. The main content area is titled 'Adms Service Settings' and contains three input fields: 'Adms Service Port' (set to 8881), 'Project control file version' (set to None), and 'Turn on encrypted transmission' (radio buttons for No and Yes, with 'No' selected). A red box highlights the 'Adms Service Port' field. A warning message below the first field states: '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.'

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.

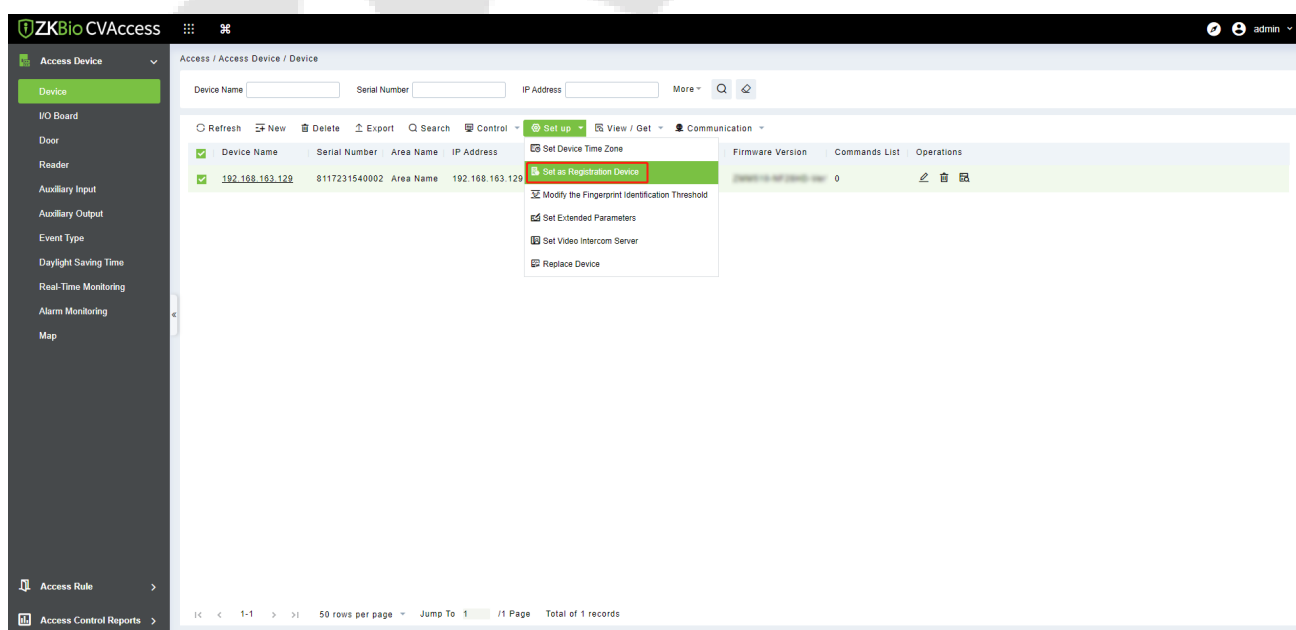
2. Click **Search**, and it will prompt **[Searching.....]**.
3. After searching, the list and total number of access controllers will be displayed.



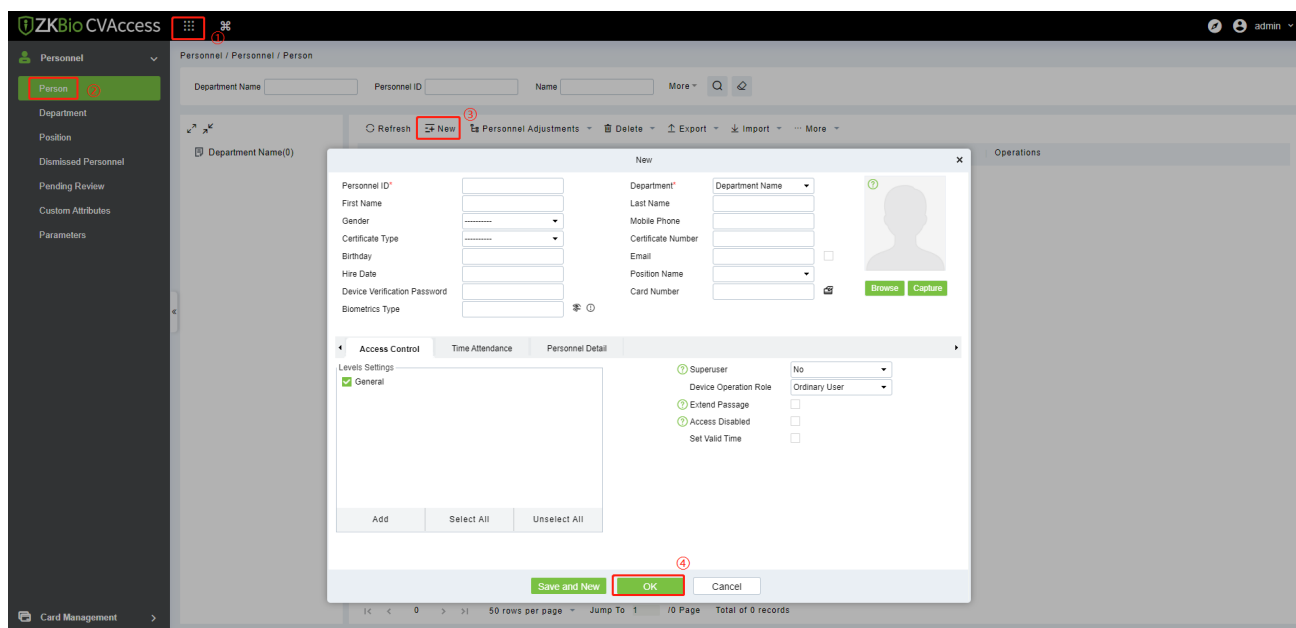
4. Click **[Add]** in operation column, a new window will pop-up. Select Icon type, Area, and Add to Level from each dropdown and click **[OK]** to add the device.
5. After the addition is successful, the device will be displayed in the device list.

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

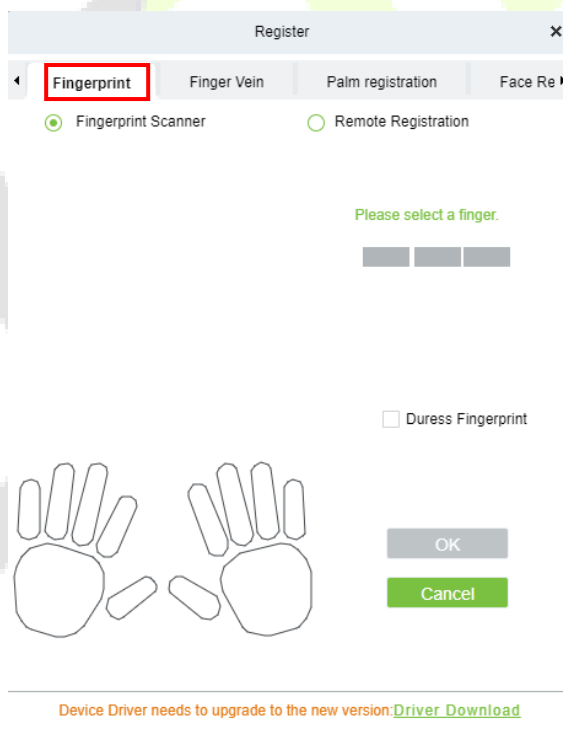
1. In the device list, select the device and click **Set up > Set as Registration Device**.



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

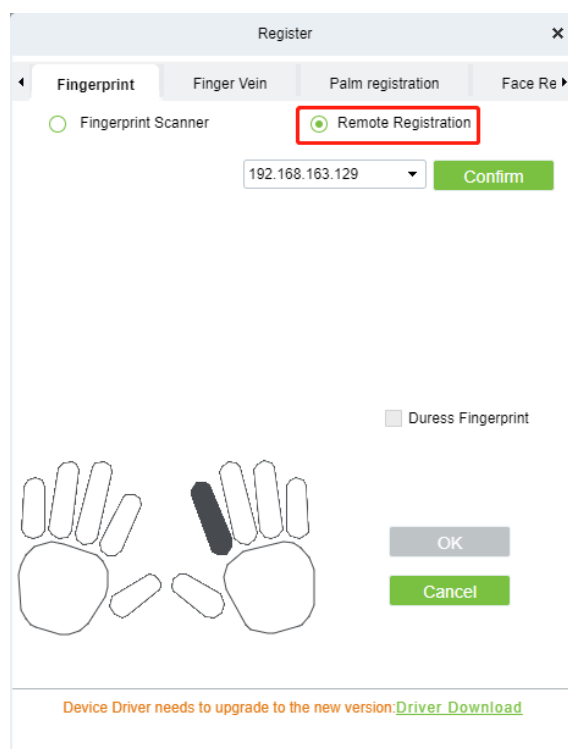


3. Fill in all the required fields of the user and click and select **Fingerprint** to enter the online fingerprint registration interface.

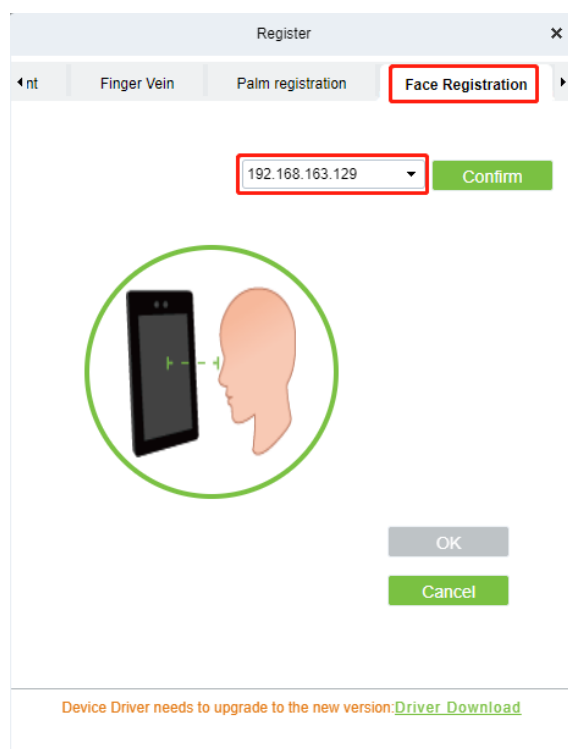


4. Click **Driver Download** to install the driver first.

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



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



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

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

21 Connect to ZKBio Time Software

21.1 Set the Communication Address

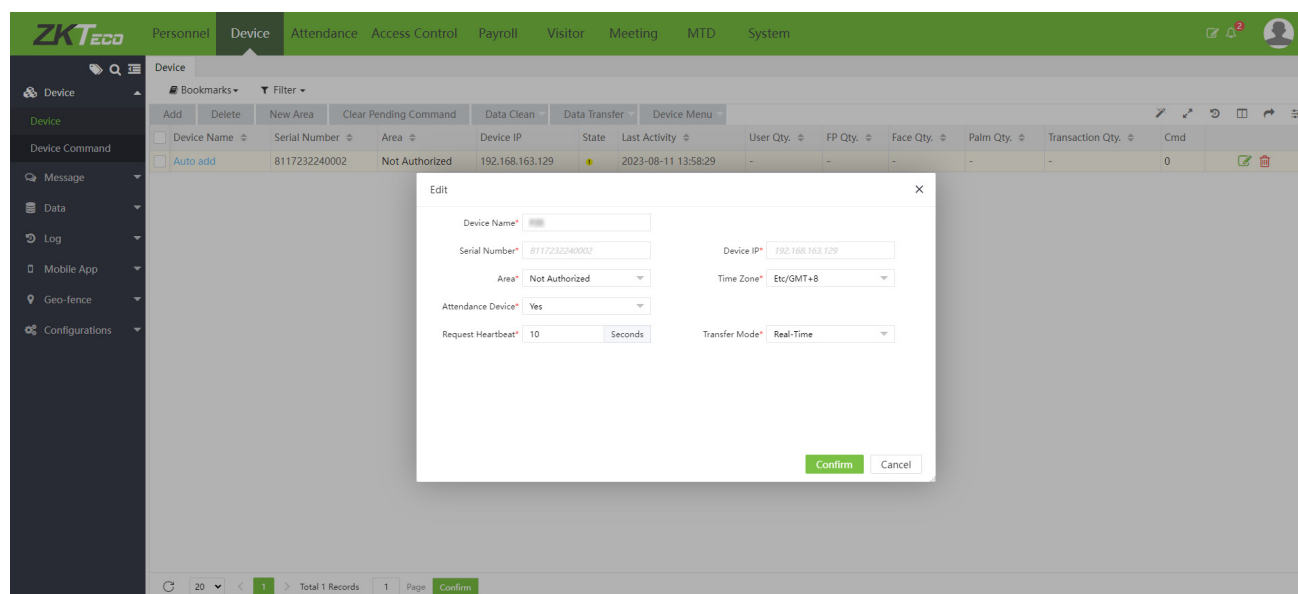
1. Press **M/OK** and enter **COMM.** > **Ethernet** to set the IP address and gateway of the device.
(**Note:** The IP address should be able to communicate with the ZKBio Time server, preferably in the same network segment with the server address)
2. Press **M/OK** and enter **COMM.** > **Cloud Server 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		Cloud Server Settings	
Display in Status Bar	<input checked="" type="checkbox"/>	Server Mode	ADMS
IPv4		Enable Domain Name	<input type="checkbox"/>
IP Address	192.168.163.129	Server Address	58.23.12.98
Subnet Mask	255.255.255.0	Server Port	8881
Gateway	192.168.163.1	Enable Proxy Server	<input type="checkbox"/>
DNS			

21.2 Add Device on the Software

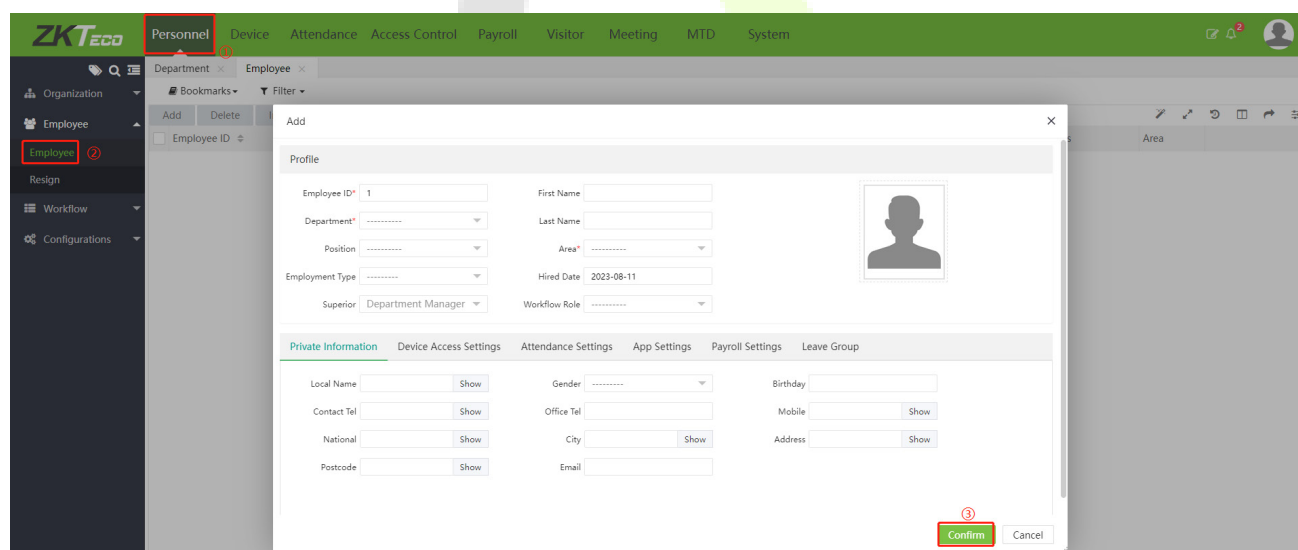
After setting on the device, the device will be automatically added to the software. Open the ZKBio Time software then select [**Device Module**] > [**Device**] > [**Device**], click the device in the list, change the Device Name and Area.

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

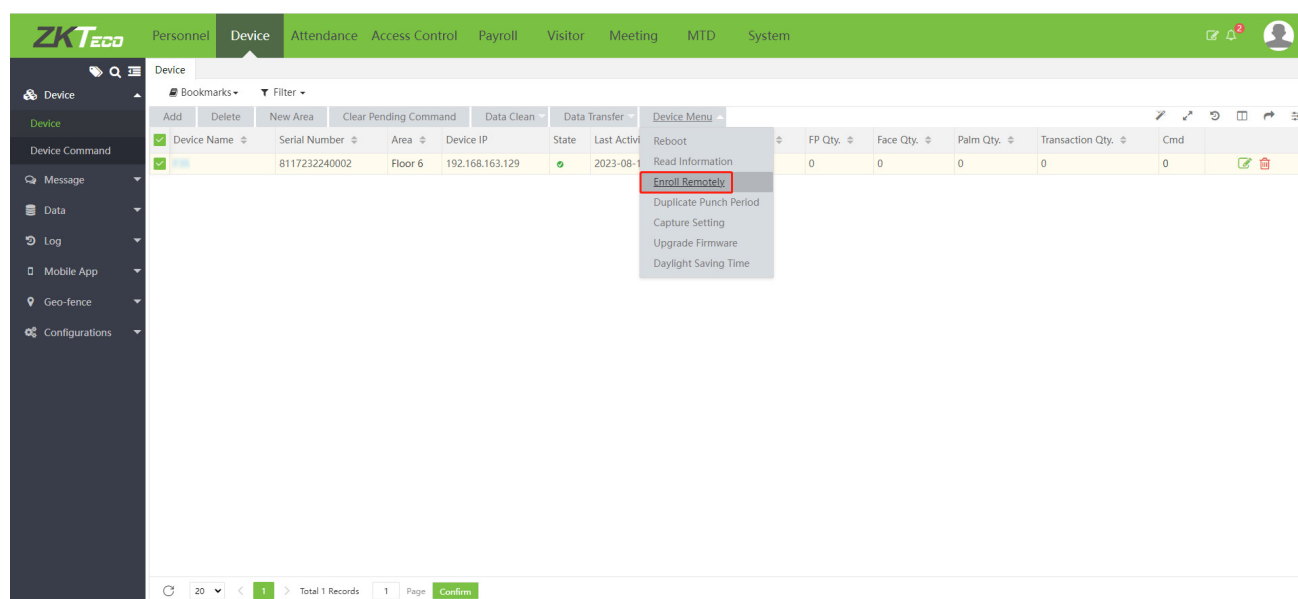


21.3 Add Personnel on the Software and Online Fingerprint Registration

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



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**.



- 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

Confirm

Cancel

- 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*.

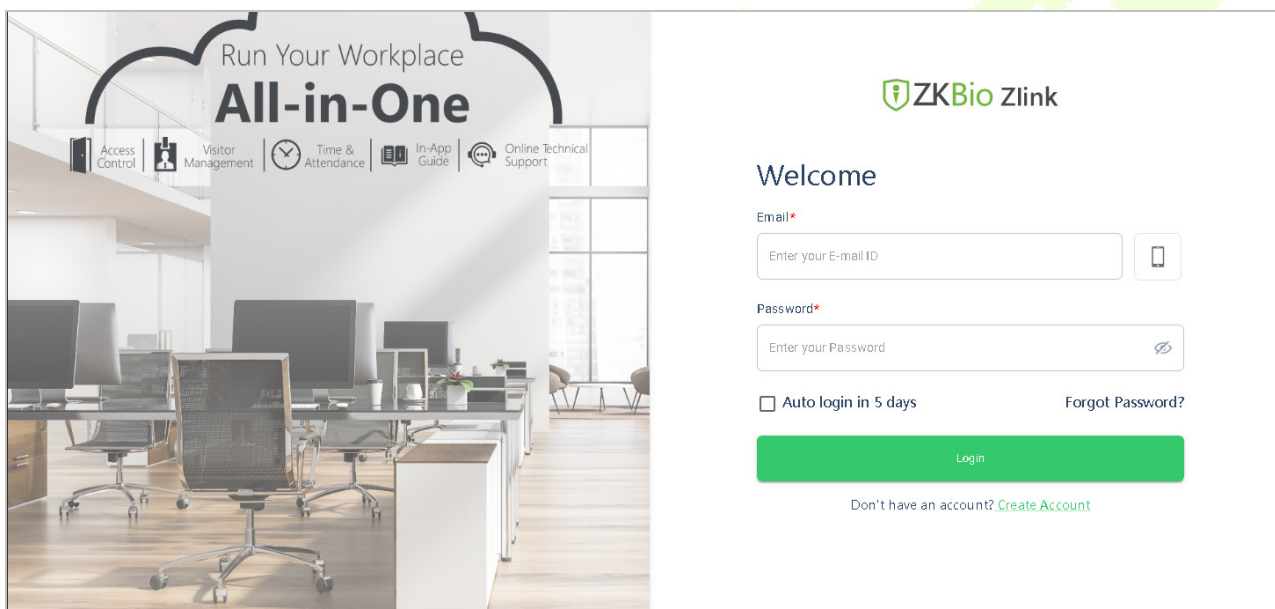
22 Connecting to ZKBio Zlink Web

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](#).

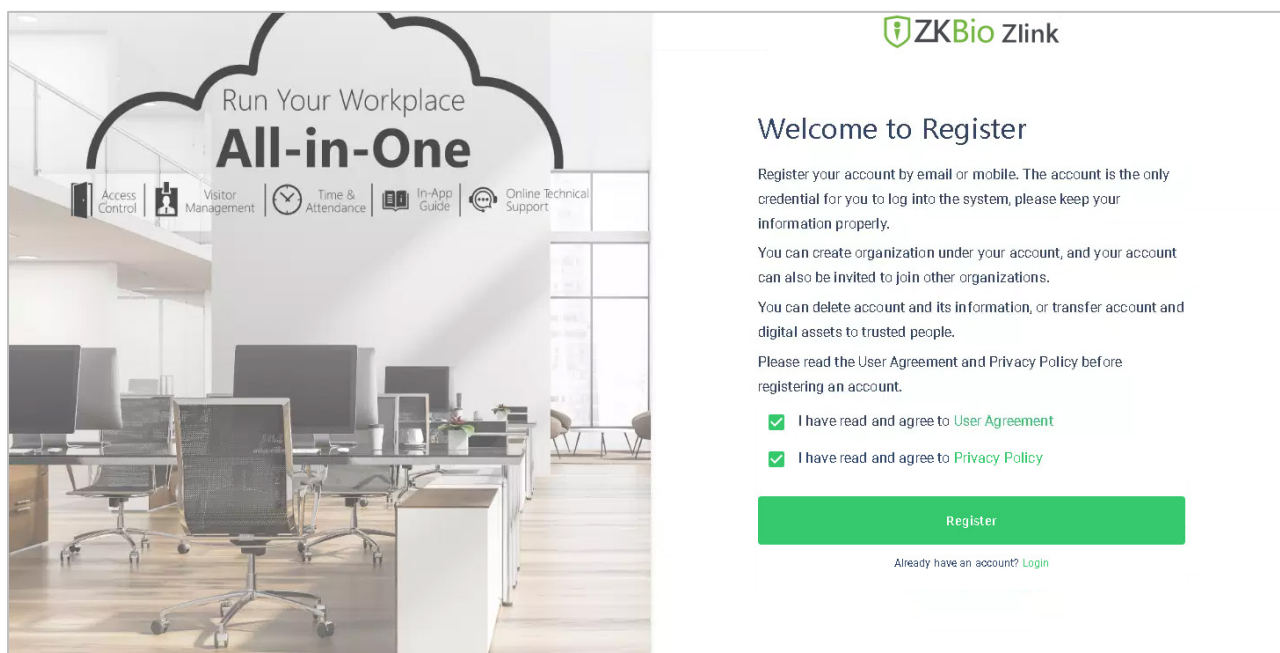
Users can use the created account to access ZKBio Zlink Web to connect devices, add new personnel, register the verification method of registered personnel, synchronize personnel to devices and query records.

22.1 Register Account

1. Access the ZKBio Zlink website (<http://zlink.minervaiot.com>).
2. If you do not have an account, please click **Create Account** to add a new account.



3. Read and agree to User Agreement and Privacy Policy, then click **Register**.



4. Enter user's information and set password, then click **Register**.

ZKBio Zlink

Register

First Name*

Please enter your First Name

Last Name*

Please enter your Last Name

Email*

Please enter your Email

Country*

Select your Country

Create Password*

Create your Password

Confirm Password*

Confirm your Password

Register

5. Set the organization's name and Organization code, click **Create**, then complete registration. If you do have an organization, please click **Select an Organization**.

Run Your Workplace
All-in-One

Access Control | Visitor Management | Time & Attendance | In-App Guide | Online Technical Support

ZKBio Zlink

Create Organization

Organization Name*
Please enter your Organization Name ?

Organization Code*
Please enter your Organization Code ?

Create

Already have an Organization? [Select an Organization](#)

[Back to Login](#)

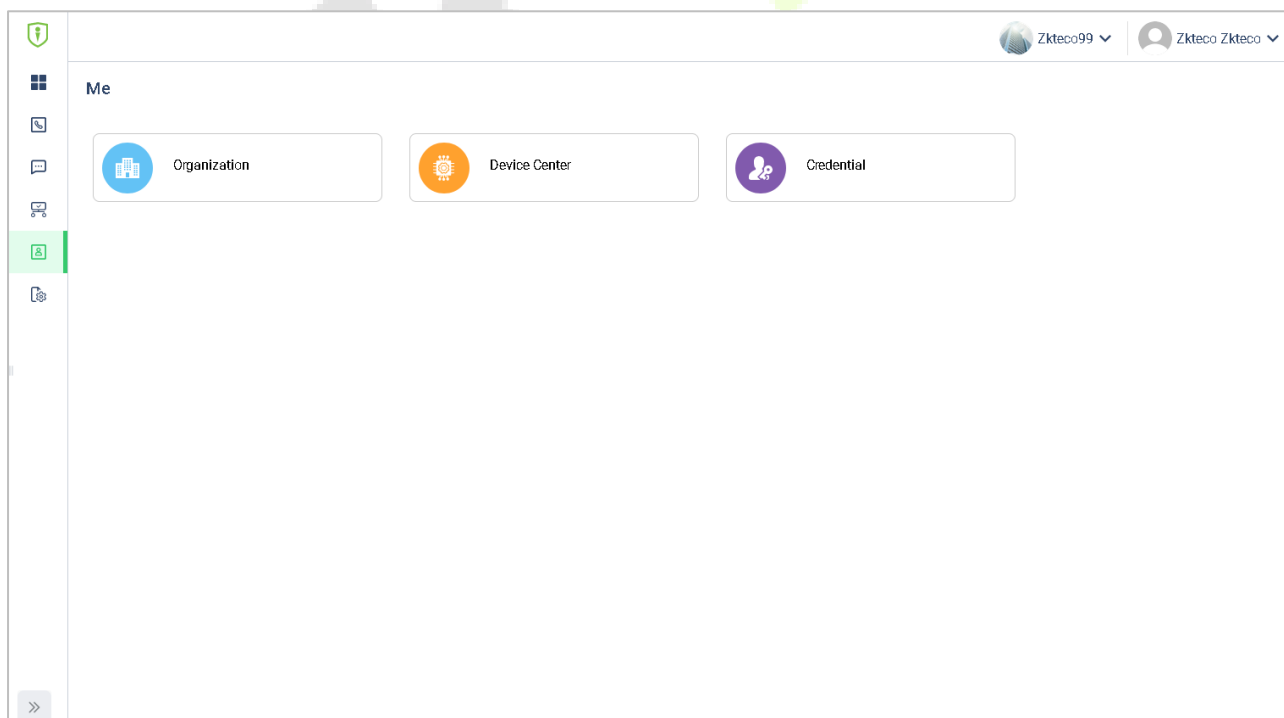
*Functions will be limited subject to region, please contact support team for details


Powered by MINERVAIoT

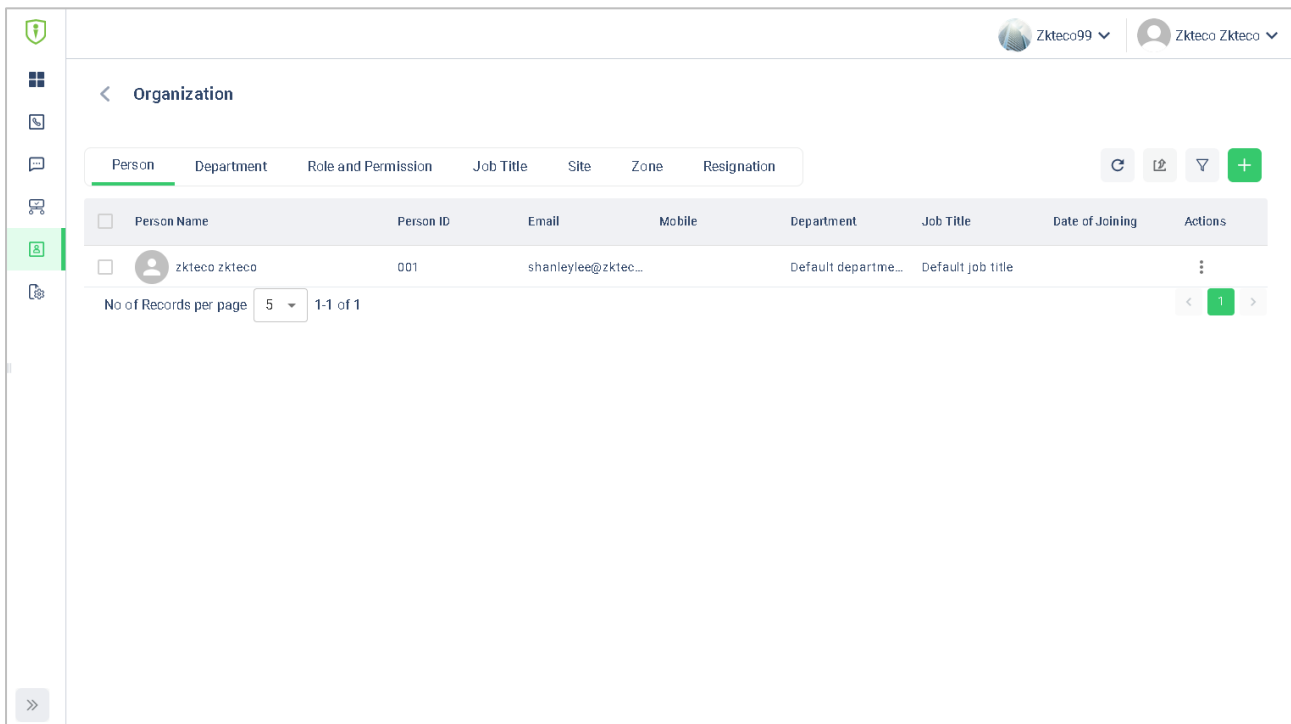
22.2 Add Device

22.2.1 Set Organization (Add Person)

1. Click **Me > Organization** on the main menu.

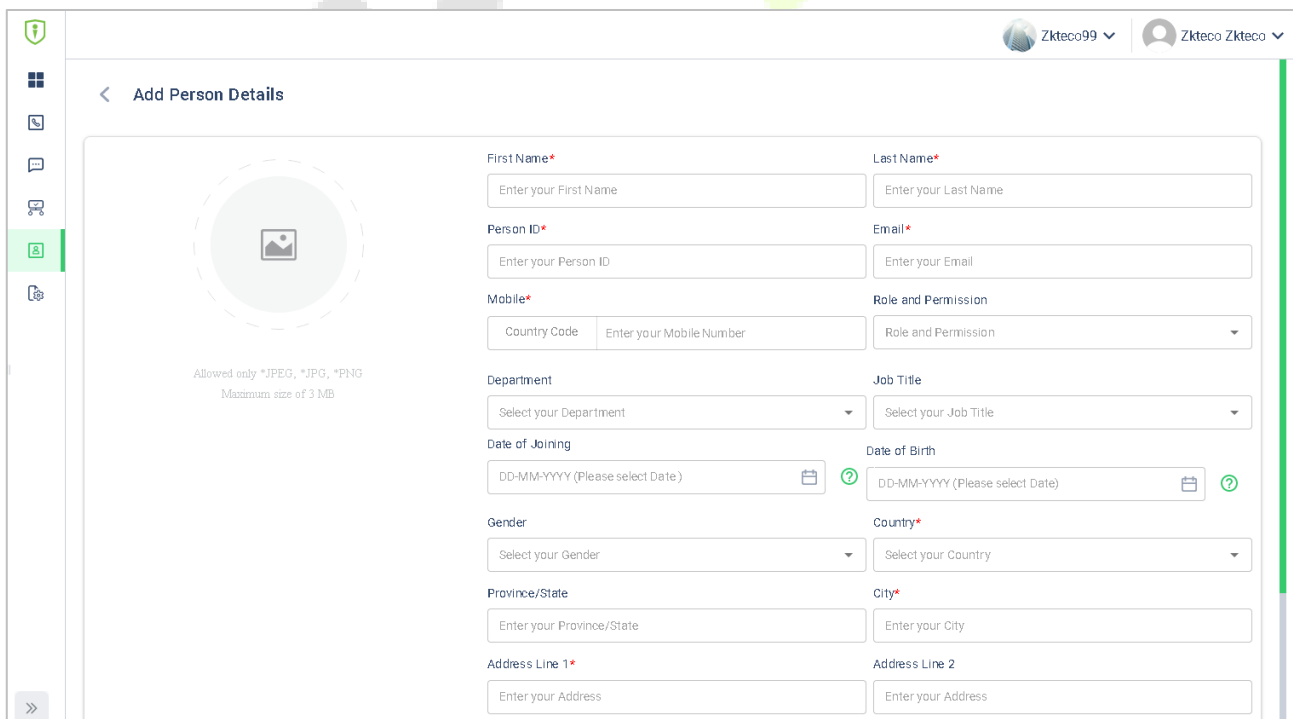


- Click **Add** icon  to add a new person (Repeat adding the department, role and permission, job title, site list, and zone list).



The screenshot shows the 'Organization' management page. At the top, there are tabs for 'Person', 'Department', 'Role and Permission', 'Job Title', 'Site', 'Zone', and 'Resignation'. The 'Person' tab is active. Below the tabs is a table with the following columns: Person Name, Person ID, Email, Mobile, Department, Job Title, Date of Joining, and Actions. The table contains one record for a person named 'zkteco zkteco' with ID '001' and email 'shanylee@zkteco...'. At the bottom of the table, there is a 'No of Records per page' dropdown set to '5' and a pagination indicator '1-1 of 1'. A green '+ Add' button is located in the top right corner of the table area.

- Enter the person's details and click **Save** (Repeat adding the department, role and permission, job title, site list, and zone list).



The screenshot shows the 'Add Person Details' form. On the left, there is a circular placeholder for a profile picture with the text 'Allowed only *.JPEG, *.JPG, *.PNG' and 'Maximum size of 3 MB'. The form contains the following fields:

- First Name***: Text input field.
- Last Name***: Text input field.
- Person ID***: Text input field.
- Email***: Text input field.
- Mobile***: Text input field with a 'Country Code' dropdown.
- Role and Permission**: Dropdown menu.
- Department**: Dropdown menu.
- Job Title**: Dropdown menu.
- Date of Joining**: Date picker (DD-MM-YYYY).
- Date of Birth**: Date picker (DD-MM-YYYY).
- Gender**: Dropdown menu.
- Country***: Dropdown menu.
- Province/State**: Text input field.
- City***: Text input field.
- Address Line 1***: Text input field.
- Address Line 2**: Text input field.

22.2.2 Add Device

1. Press **M/OK** and enter **COMM. > Ethernet** on the device to set the IP address and gateway of the device.

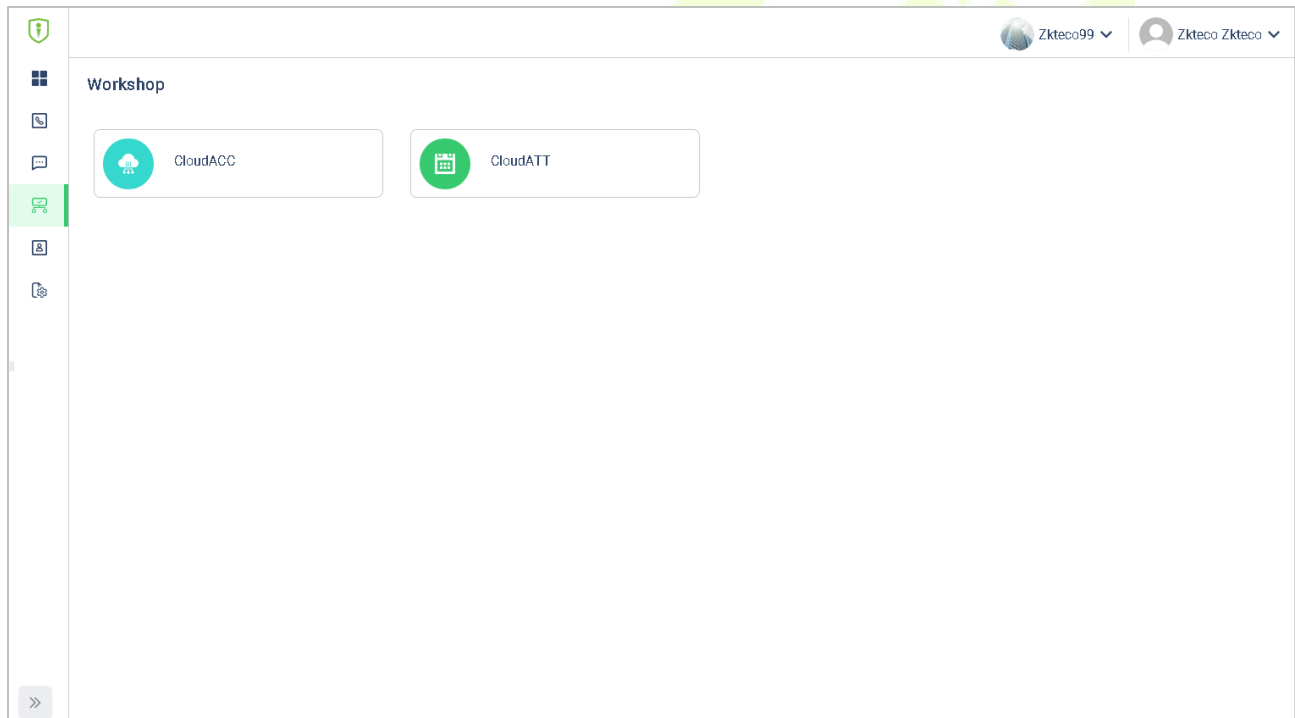
Ethernet

Display in Status Bar ☒

IPv4

IP Address	192.168.163.129
Subnet Mask	255.255.255.0
Gateway	192.168.163.1
DNS	

2. Click **Workshop > CloudACC** on the main menu to enter the **ZKBio Cloud Access** interface.



3. Click **Device Management > Device** to enter the **Device** interface in the **ZKBio Cloud Access**.
4. Click **+Add Device** button to add a new device.
5. Read and check to the instructions, then click **Continue**.

The screenshot shows the 'Cloud ACC' interface with the 'Add Device' page selected. The left sidebar contains a menu with 'Device Management' highlighted. The main content area is titled 'Add Device' and 'Device Network Configuration Steps'. It contains three steps: Step 1: Power up and turn on the Device, Step 2: Configure the Network, and Step 3: Restore the Factory Settings. Each step has a corresponding icon and a brief description. At the bottom, there is a checkbox 'I have read these instructions' and a 'Continue' button.

Cloud ACC

zkteco99 | zkteco zkteco

< Add Device

Device Network Configuration Steps

Step 1: Power up and turn on the Device
If the Device has a network, it will automatically connect to the network and start working.

Step 2: Configure the Network
You may use Bluetooth to set up the network. Or some Device has touch screen that has network setting in Firmware.

Step 3: Restore the Factory Settings
Some Devices can not have network setting. You may try to Reset the Device factory setting.

☐ I have read these instructions

Continue

version V 2.1.0

6. Enter the device's serial number, then click **Add**. (Press **M/OK** and enter **System Info > Device Info** on the device to view the serial number)

The screenshot shows the 'Cloud ACC' interface with the 'Add Device' page selected. The left sidebar contains a menu with 'Device Management' highlighted. The main content area is titled 'Add Device' and 'Manual Register Device'. It contains a section 'Power Up and Set Device Network' with four numbered steps. Below this, there is a 'Device Serial Number' section with a text input field and an 'Add' button.

Cloud ACC

zkteco99 | zkteco zkteco

< Add Device

Manual Register Device

Power Up and Set Device Network

1. Plug in the network cable if Device support Ethernet function.
2. Enter your Device Ethernet setting/WiFi setting menu to enter communication setting page. Network setup is successful, Device will display a QR code in standby page.
3. On the side of Device box or on the back of Device, can find the Device Serial Number.
4. Fill in Device Serial Number on system.

Device Serial Number


Please Enter Device Serial Number

Add

version V 2.1.0

7. Choose a site and a zone, then click **Bind** to finish.

Bind Device to your Organization

 NYU7240500231

Please bind the Device to a Site and Mapped Zone

Bind Site *

Please select your Site

Bind Zone *

Please select your Zone

Bind

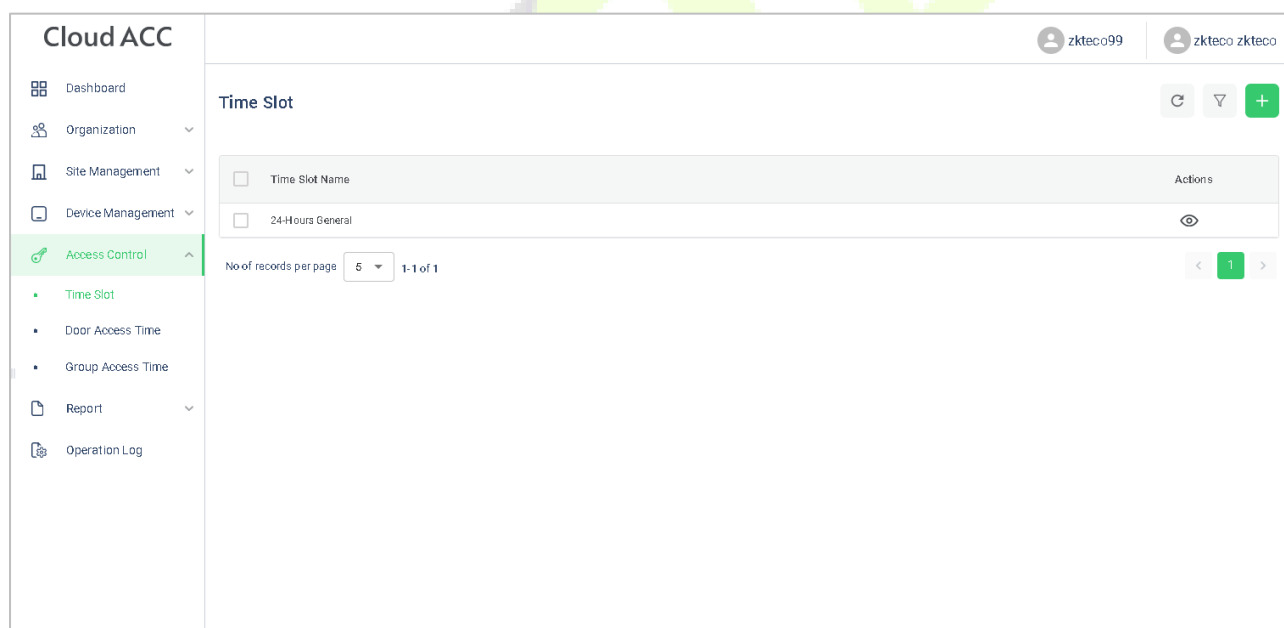
Clear


22.3 Time Slot

Time Slot is used to set the access time period for person or doors.

22.3.1 Set Time Slot

In **ZKBio Cloud Access** interface, click **Access Control > Time Slots** to set time slot.



Click **+Add Time slots** to add a new slot, or click  to modify an existing slot.

22.3.2 Set Door Access Time

In **ZKBio Cloud Access** interface, click **Access Control > Door Access Time** and click  to allocate a time slot to this door.

Cloud ACC

zkteco99 | zkteco zkteco

Door Access Time

<input type="checkbox"/>	Door Name	Device Name	Device Serial Num...	Door Number	Enable	Active Time Slot	Verification Mode	Actions
<input type="checkbox"/>	Door-1	zkteco099	zkteco099	1	✓	24-Hours General		

No of records per page: 5 | 1-1 of 1

version V 2.1.0

22.3.3 Set Group Access Time

You can set a group to control the access time of the person and the door at the same time.

In **ZKBio Cloud Access** interface, click **Access Control > Group Access Time**.

Cloud ACC

zkteco99 | zkteco zkteco

Group Access Time


<input type="checkbox"/>	Name	Time Slot	Start Date and Time	End Date and Time	Actions
<input type="checkbox"/>	1	24-Hours General	10:37 01-08-2023	11:37 10-08-2023	


No of records per page: 5 | 1-1 of 1

version V 2.1.0

Click **+ Add Group Access Time** to add a new group.

Click to allocate doors to this group.

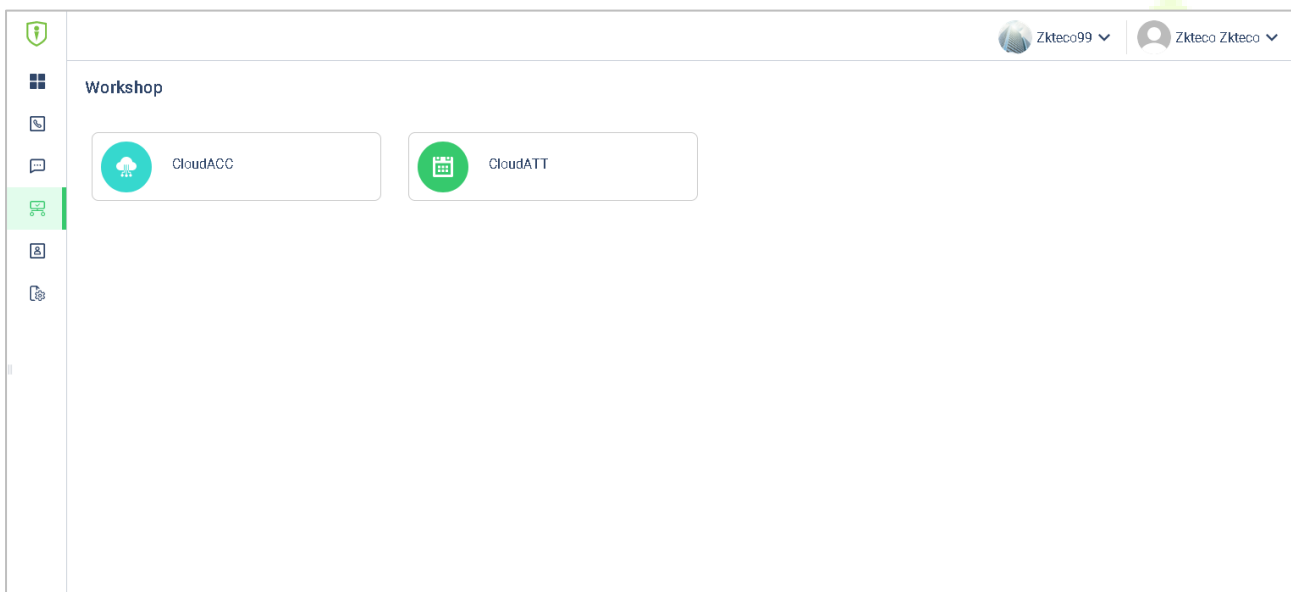
Click  to allocate person to this group.

Click  to allocate a time slot to this group.

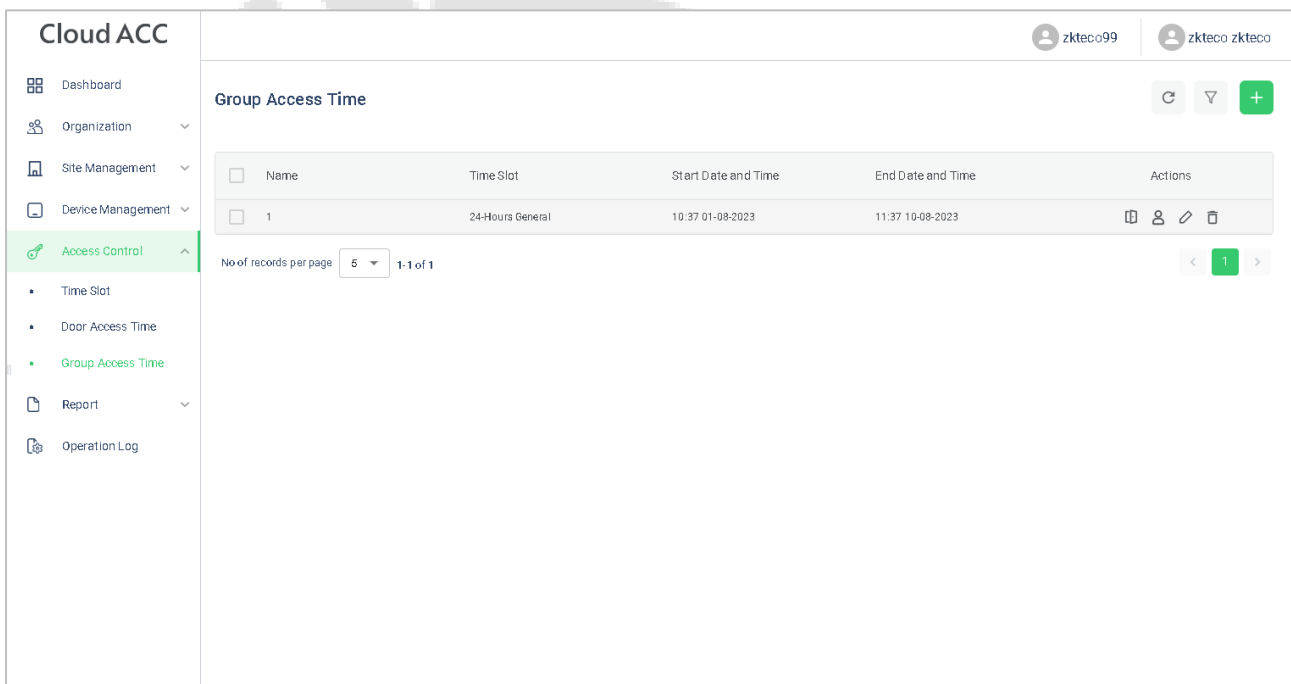
Click  to delete this group.

22.4 Synchronize Person to Device

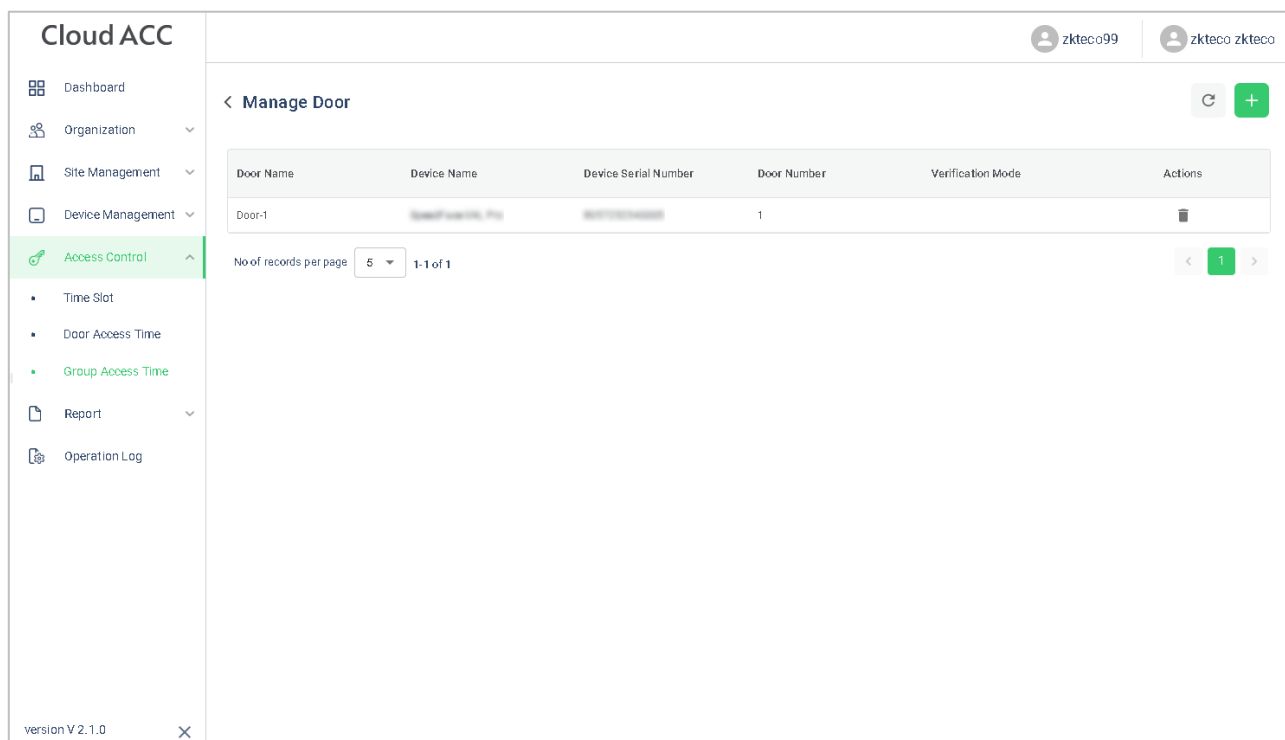
1. Click **Workshop > CloudACC** on the main menu to enter the **ZKBio Cloud Access** interface.



2. Click **Access Control > Group Access Time**.






3. Click  >  to choose a device.






Cloud ACC

zkteco99 | zkteco zkteco

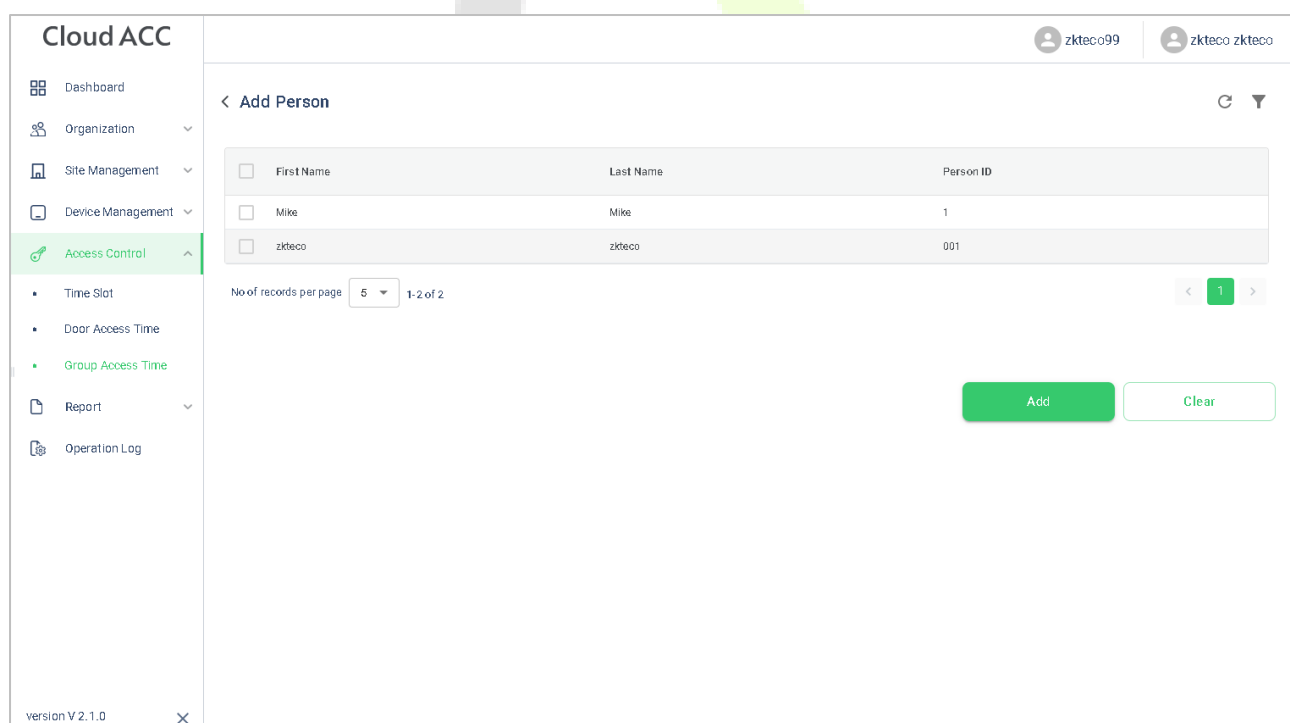
< Manage Door  

Door Name	Device Name	Device Serial Number	Door Number	Verification Mode	Actions
Door-1	Zkteco099	001	1		

No of records per page 1-1 of 1   



version V 2.1.0

4. Click  >  to allocate person to this device.






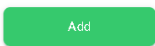

Cloud ACC

zkteco99 | zkteco zkteco

< Add Person  

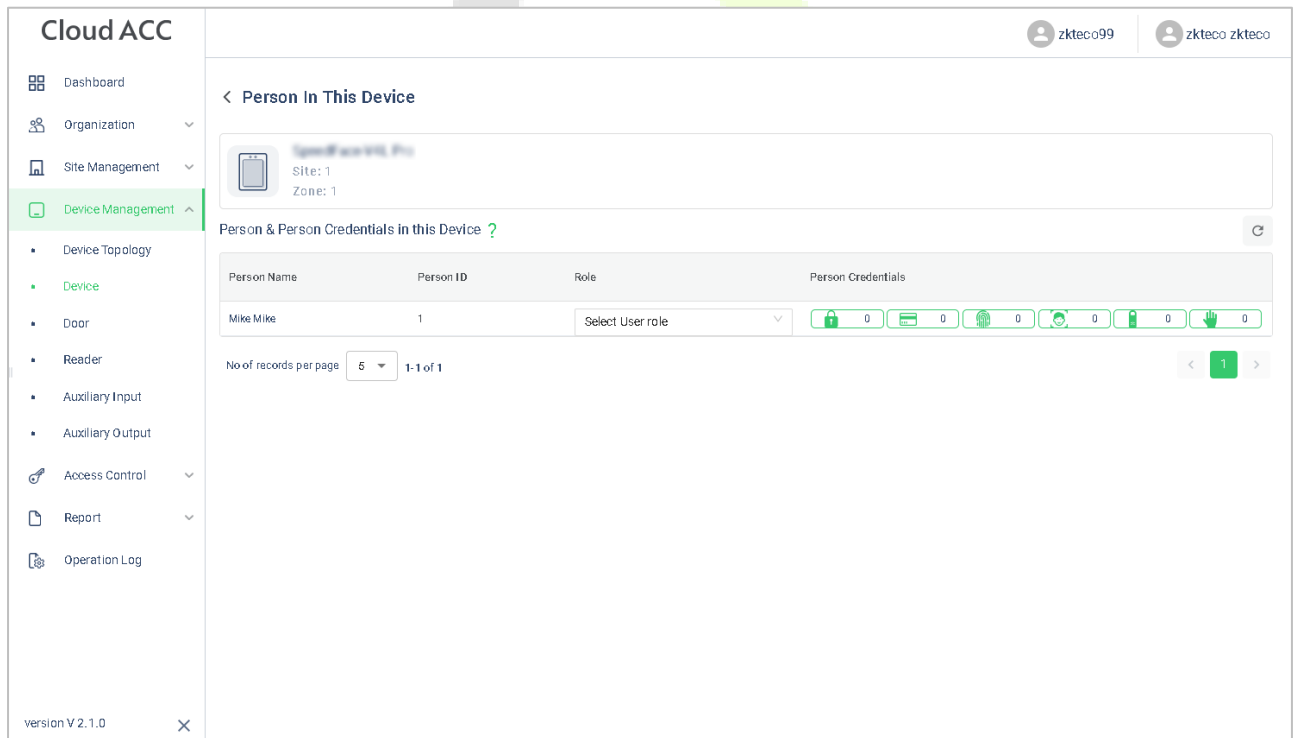
<input type="checkbox"/>	First Name	Last Name	Person ID
<input type="checkbox"/>	Mike	Mike	1
<input type="checkbox"/>	zkteco	zkteco	001

No of records per page 1-2 of 2   

version V 2.1.0

6. Choose a device and click **Persons in the Device** icon  to view the person list.



22.5 User Registration

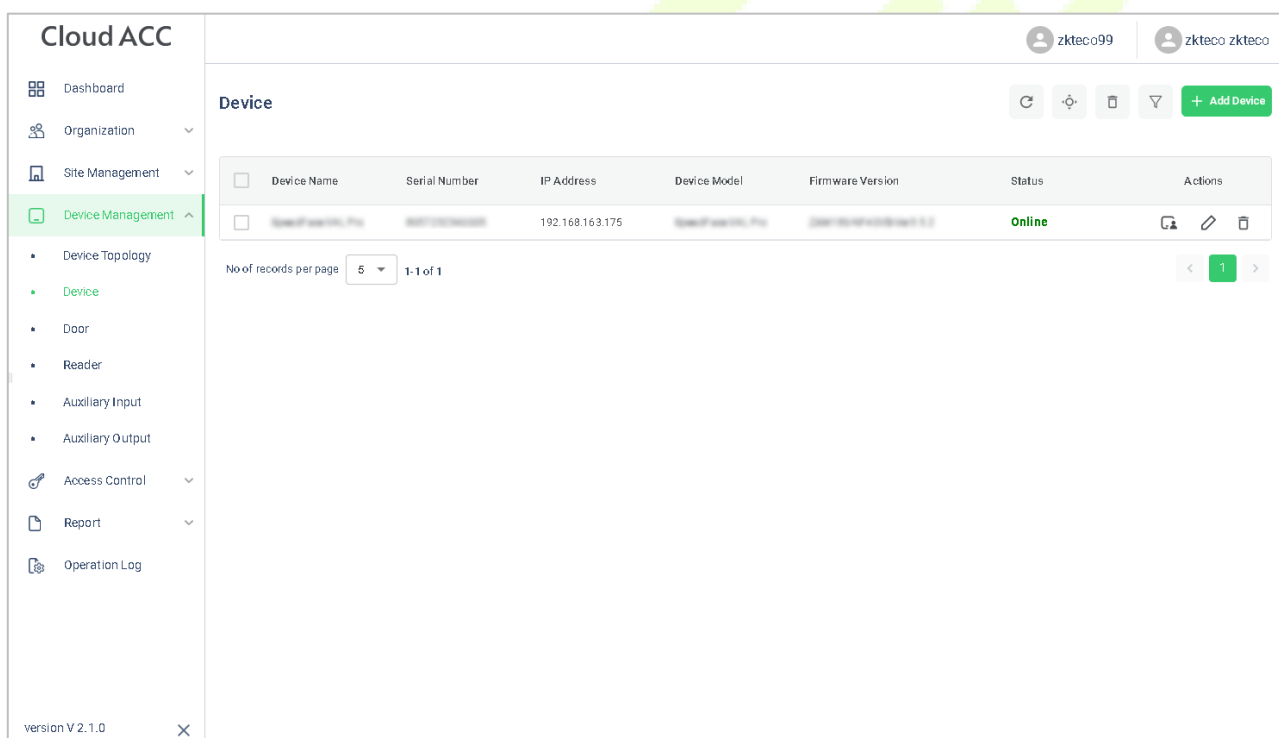
22.5.1 Register a User ID and Name

Please refer to [22.2.1 Set Organization](#).

22.5.2 Setting the User Role

There are two types of user accounts: the **Normal User** and the **Super Admin**. If there is already a registered administrator, the normal users have no rights to manage the system and may only access authentication verifications. The administrator owns all management privileges.

1. Click **Device Management > Device** on **ZKBio Cloud Access** interface to enter the **Device** interface.
2. Choose a device and click **Persons in the Device** icon  to view the person list.



Cloud ACC

zkteco99 | zkteco zkteco




Device Management

- Dashboard
- Organization
- Site Management
- Device Management**
 - Device Topology
 - Device**
 - Door
 - Reader
 - Auxiliary Input
 - Auxiliary Output
- Access Control
- Report
- Operation Log

version V 2.1.0

Device

+ Add Device

<input type="checkbox"/>	Device Name	Serial Number	IP Address	Device Model	Firmware Version	Status	Actions
<input type="checkbox"/>	zkteco99	zkteco99	192.168.163.175	zkteco99	zkteco99	Online	  

No of records per page: 5 | 1-1 of 1

< 1 >

3. Choose the **Select User** role.

Cloud ACC

zkteco99 | zkteco zkteco

< Person In This Device

SpeedFaceV10 Pro
Site: 1
Zone: 1

Person & Person Credentials in this Device ?

Person Name	Person ID	Role	Person Credentials
Mike Mike	1	Select User role	<input type="checkbox"/> 0 <input type="checkbox"/> 0 <input type="checkbox"/> 0 <input type="checkbox"/> 0 <input type="checkbox"/> 0 <input type="checkbox"/> 0 <input type="checkbox"/> 0

No of records per page: 5 | 1-1 of 1

version V 2.1.0

22.5.3 Register Fingerprint

1. Click **Device Management > Device** on **ZKBio Cloud Access** interface to enter the **Device** interface.
2. Choose a device and click **Persons in the Device** icon to view the person list.

Cloud ACC

zkteco99 | zkteco zkteco

Device

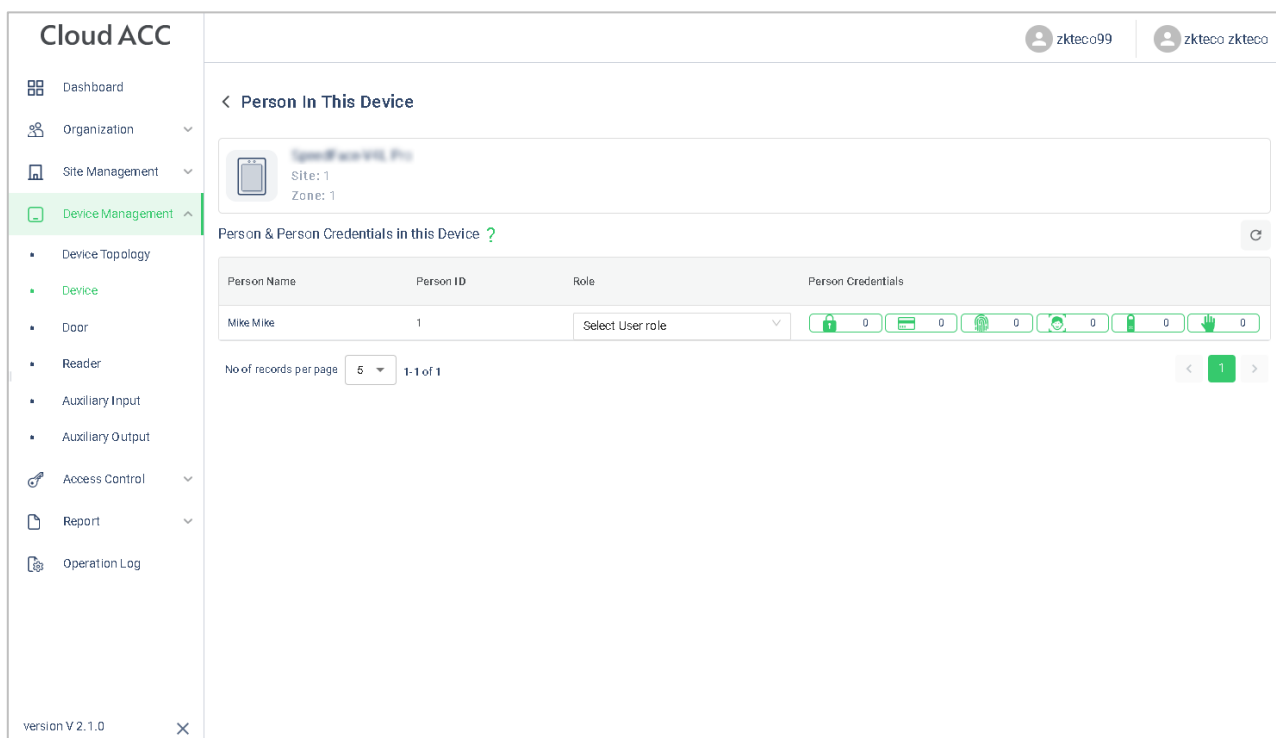
+ Add Device

<input type="checkbox"/>	Device Name	Serial Number	IP Address	Device Model	Firmware Version	Status	Actions
<input type="checkbox"/>	SpeedFaceV10 Pro	88871027640008	192.168.163.175	SpeedFaceV10 Pro	zkfacecloudAccess V2.0	Online	

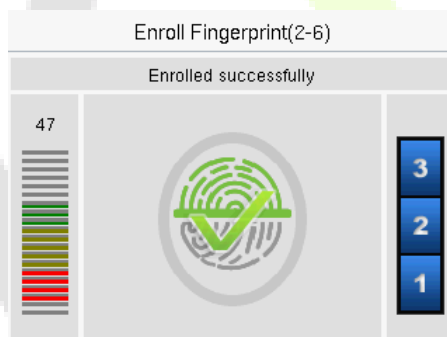
No of records per page: 5 | 1-1 of 1

version V 2.1.0

3. Click  icon to choose a finger, click **Submit**, then register fingerprint on the device.



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



22.5.4 Register Face Template

1. Click **Device Management > Device** on **ZKBio Cloud Access** interface to enter the **Device** interface.
2. Choose a device and click **Persons in the Device** icon  to view the person list.



- Copyright © 2024 ZKTECO CO., LTD. All rights reserved.

The screenshot shows the Cloud ACC web interface. On the left is a sidebar with navigation options: Dashboard, Organization, Site Management, Device Management (highlighted), Device Topology, Device, Door, Reader, Auxiliary Input, Auxiliary Output, Access Control, Report, and Operation Log. The main area is titled 'Device' and contains a table with the following columns: Device Name, Serial Number, IP Address, Device Model, Firmware Version, Status, and Actions. A single device is listed with the status 'Online'. Below the table, there are pagination controls showing 'No of records per page' set to 5 and '1-1 of 1'. At the bottom left, the version 'V 2.1.0' is displayed.

Device Name	Serial Number	IP Address	Device Model	Firmware Version	Status	Actions
SpeedFaceV1s Pro	888710278400000	192.168.163.175	SpeedFaceV1s Pro	SpeedFaceV1s Pro V2.0	Online	[Add] [Edit] [Delete]

3. Click  icon to register password on the device.

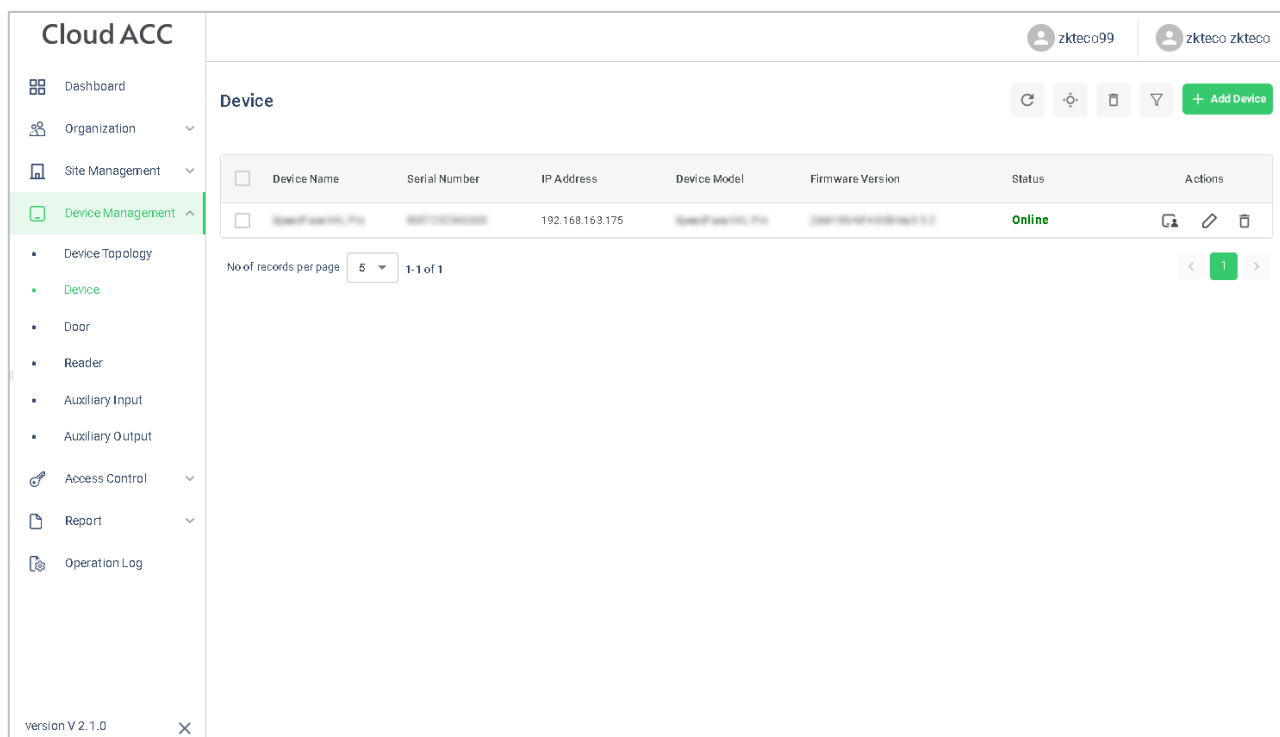
The screenshot shows the 'Person In This Device' configuration page. It displays the device name 'SpeedFaceV1s Pro' and its location 'Site: 1, Zone: 1'. Below this, there is a section titled 'Person & Person Credentials in this Device' with a table for managing user credentials. The table has columns for Person Name, Person ID, Role, and Person Credentials. One user, 'Mike Mike' with ID '1', is listed. The Role is set to 'Select User role'. The Person Credentials column shows various credential types with counts: Password (0), Card (0), Fingerprint (0), Face (0), and others. At the bottom, there are pagination controls showing 'No of records per page' set to 5 and '1-1 of 1'. The version 'V 2.1.0' is shown at the bottom left.

Person Name	Person ID	Role	Person Credentials
Mike Mike	1	Select User role	0 0 0 0 0 0




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

22.5.6 Register Card

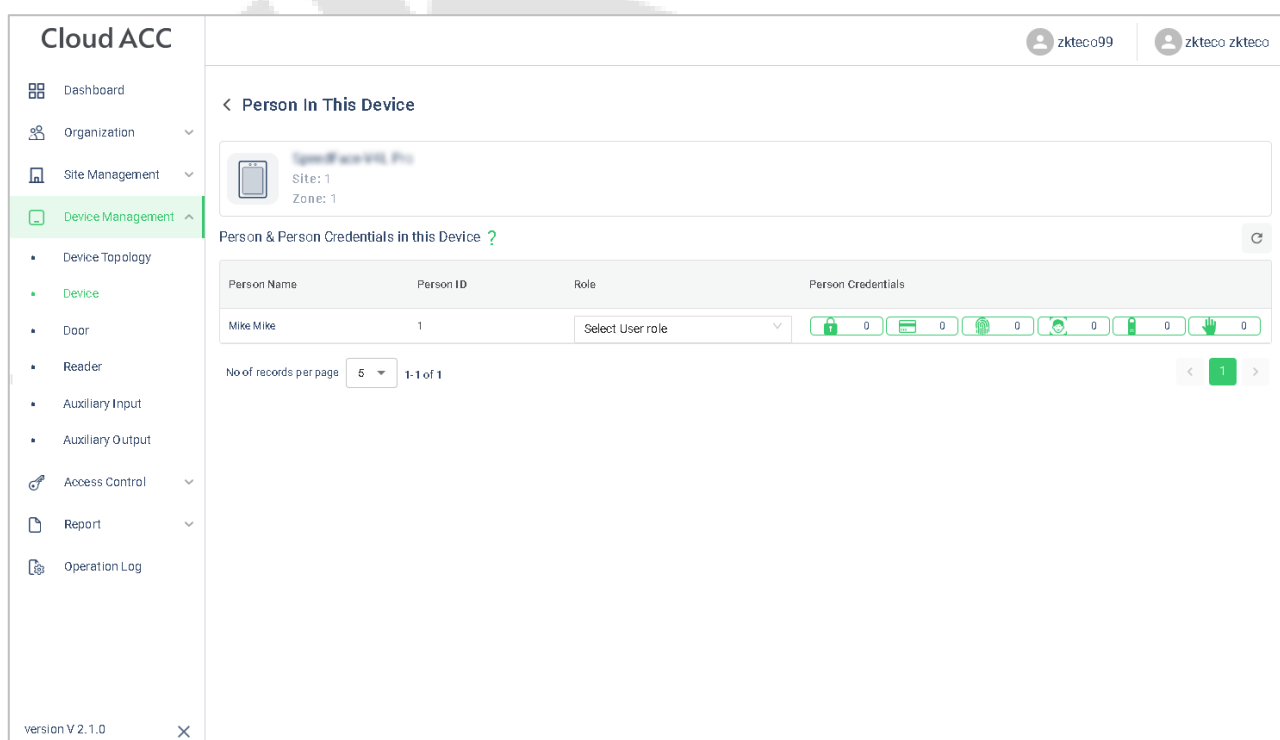
1. Click **Device Management > Device** on **ZKBio Cloud Access** interface to enter the **Device** interface.
2. Choose a device and click **Persons in the Device** icon  to view the person list.









The screenshot shows the 'Cloud ACC' interface. On the left is a sidebar with navigation options: Dashboard, Organization, Site Management, Device Management (highlighted), Device Topology, Device, Door, Reader, Auxiliary Input, Auxiliary Output, Access Control, Report, and Operation Log. The main area is titled 'Device' and contains a table with columns: Device Name, Serial Number, IP Address, Device Model, Firmware Version, Status, and Actions. A single device is listed with status 'Online'. Below the table, there are pagination controls showing 'No of records per page' set to 5 and '1-1 of 1'. At the bottom left, it says 'version V 2.1.0'.

Device Name	Serial Number	IP Address	Device Model	Firmware Version	Status	Actions
SpeedFaceV10 Pro	88871027888888	192.168.163.175	SpeedFaceV10 Pro	SpeedFaceV10 Pro V2.1.0	Online	  

3. Click  icon to register password on the device.



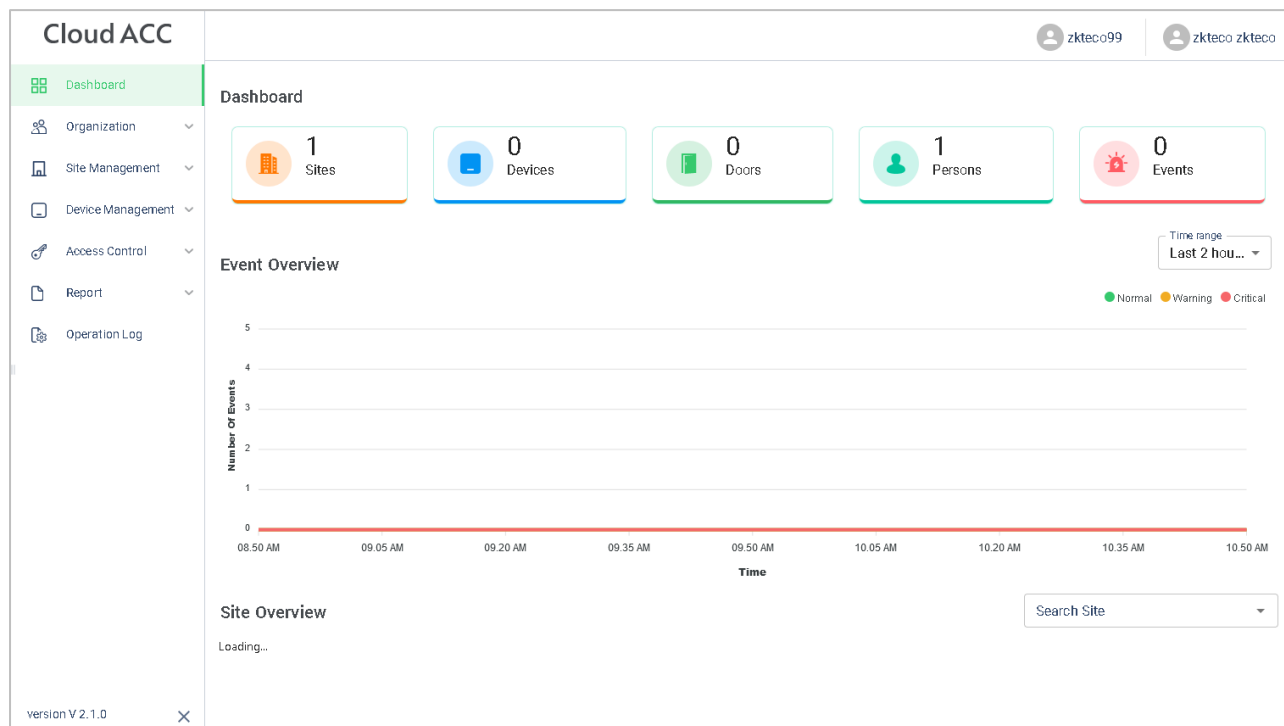
The screenshot shows the 'Person In This Device' interface. The sidebar is the same as the previous screenshot. The main area is titled '< Person In This Device'. It shows a device card for 'SpeedFaceV10 Pro' with 'Site: 1' and 'Zone: 1'. Below this, there's a section 'Person & Person Credentials in this Device' with a table. The table has columns: Person Name, Person ID, Role, and Person Credentials. One person, 'Mike Mike', is listed with Person ID '1' and Role 'Select User role'. The 'Person Credentials' column shows various icons with counts: 0 for each. At the bottom, there are pagination controls showing 'No of records per page' set to 5 and '1-1 of 1'. At the bottom left, it says 'version V 2.1.0'.

Person Name	Person ID	Role	Person Credentials
Mike Mike	1	Select User role	 0  0  0  0  0  0

22.6 Data Search

22.6.1 Dashboard

In **ZKBio Cloud Access** interface, click **Dashboard** to check the sites, devices, doors, person of this application, events overview graph, and sites overview map.



22.6.2 Event Report

In **ZKBio Cloud Access** interface, click **Report > Events** to check the specific information of all devices' events.

Cloud ACC

Dashboard

Organization

Site Management

Device Management

Access Control

Report

Events

Operation Log

zkteco99

zkteco zkteco

Events

↺

⌵

📄

Person ID	Person Name	Device Name	Device Serial Number	Event Time	Event Address	Event Name	Verification Mode
10220		SpeedFace V4L...	8057232340305	2023-08-11 10:4...	1		
		SpeedFace V4L...	8057232340305	2023-08-11 10:4...	1		
		SpeedFace V4L...	8057232340305	2023-08-11 10:4...	1		
			8057232340305	2023-08-11 10:3...	1		
			8057232340305	2023-08-11 10:3...	1		

No of records per page

5

1-5 of 12

<

1

2

3

>

version V 2.1.0

✕

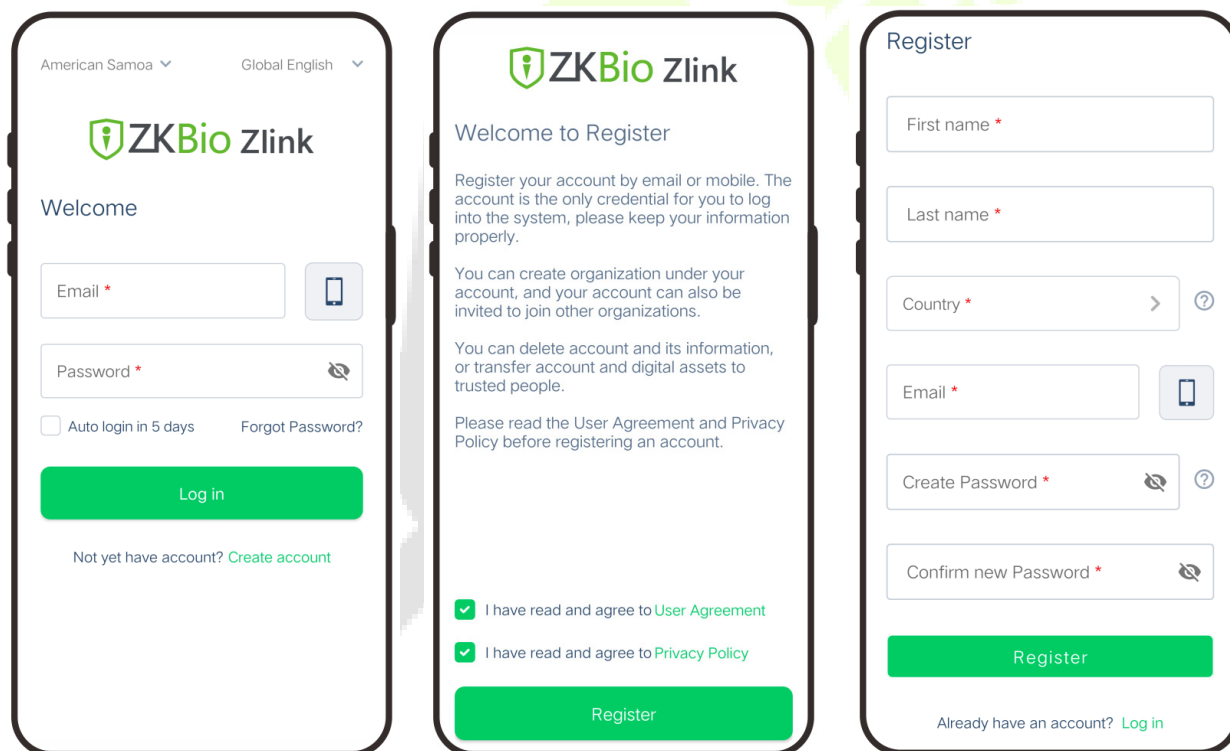
23 Connecting to ZKBio Zlink App

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 App to connect devices, unlock the device remotely and query records.

23.1 Register Account


1. Search for the ZKBio Zlink App in Apple App Store or Google Play Store and download the App to your smartphone.
2. Open the ZKBio Zlink App and if you do not have an account, please click **Create account** to add a new account.
3. Read and agree to User Agreement and Privacy Policy, then click **Register**.
4. Enter user's information and set password, then click **Register**.

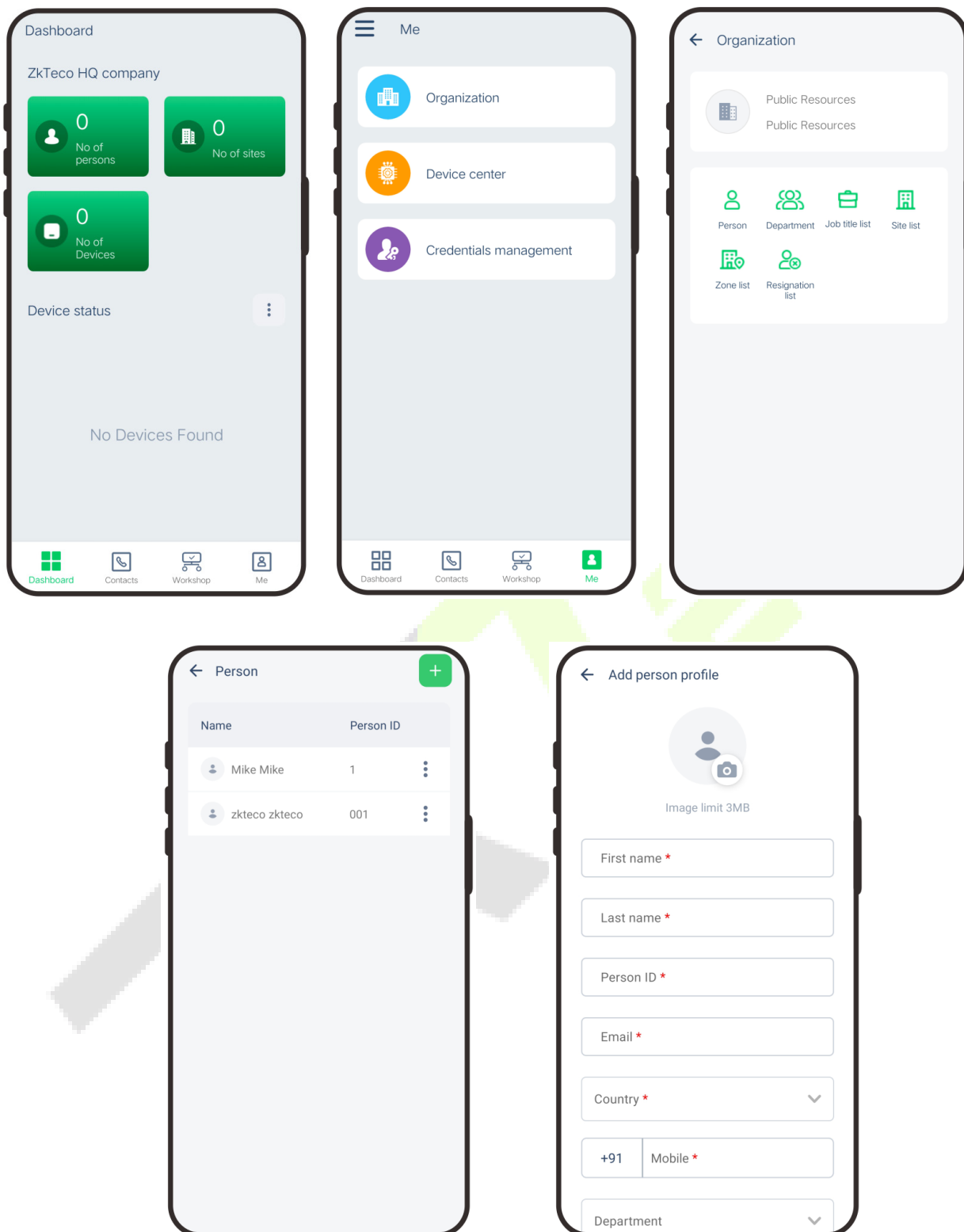


5. Choose an organization, click **Enter**, then complete registration. If you do not have an organization, please click **Create one**.

The image shows two mobile app screens for ZKBio Zlink. The left screen is titled 'Select organization' and contains the following text: 'Please select the organization you created and enter this organization.', 'You can also switch between your multiple organizations after logging in.', a dropdown menu labeled 'Select organization name*', a green 'Enter' button, and a link 'Don't have an organization? Create one'. The right screen is titled 'Create organization' and contains the following text: 'Organization name*' with a dropdown menu showing 'Public Resources', 'Organization code*' with a dropdown menu showing 'Public Resources', a green 'Create' button, and a link 'Already have an organization? Select an organization'.


23.2 Add Person

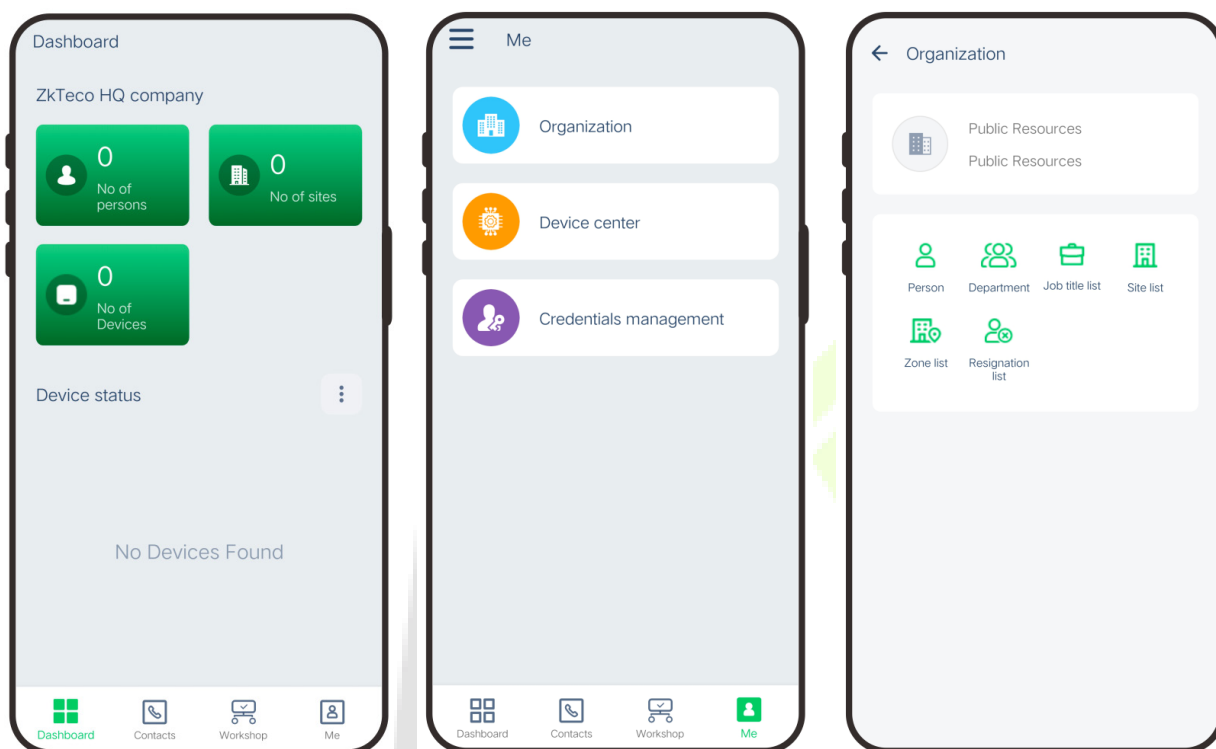
1. Click **Me > Organization > Person** on the main menu.
2. Click  icon to add a new person. Enter the information, and click **Save**.

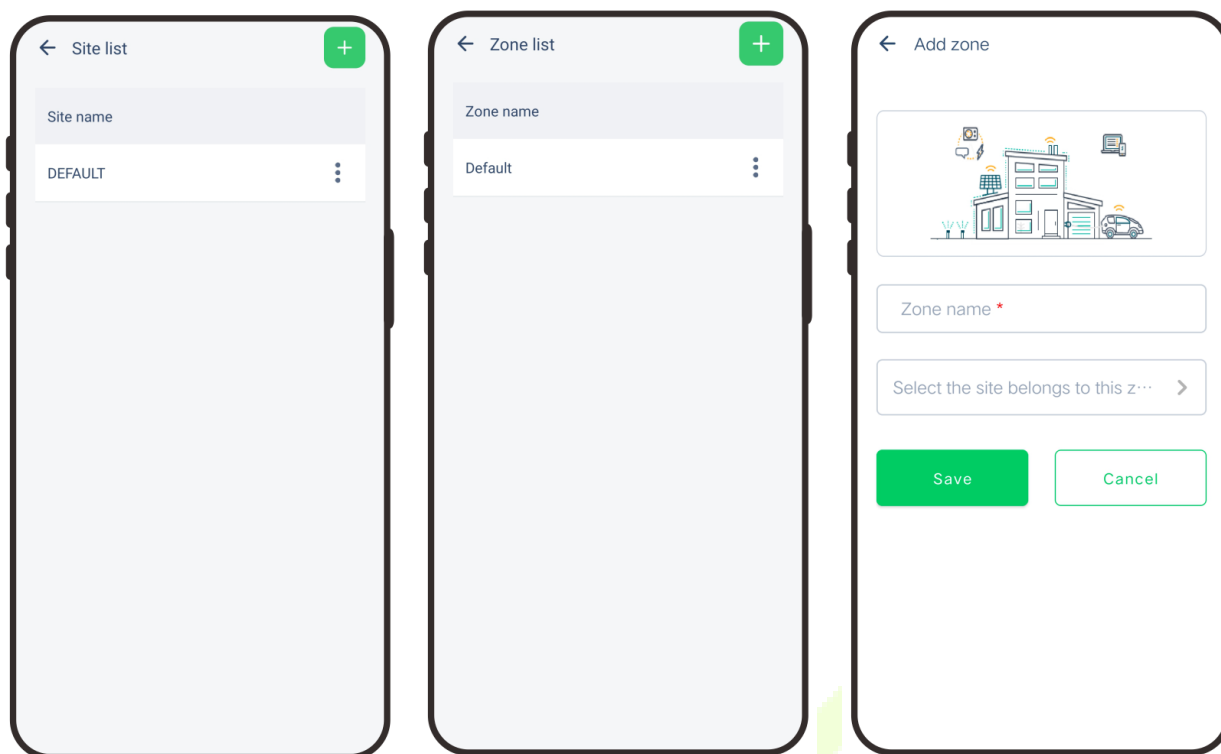


23.3 Add Device


23.3.1 Add Site and Zone

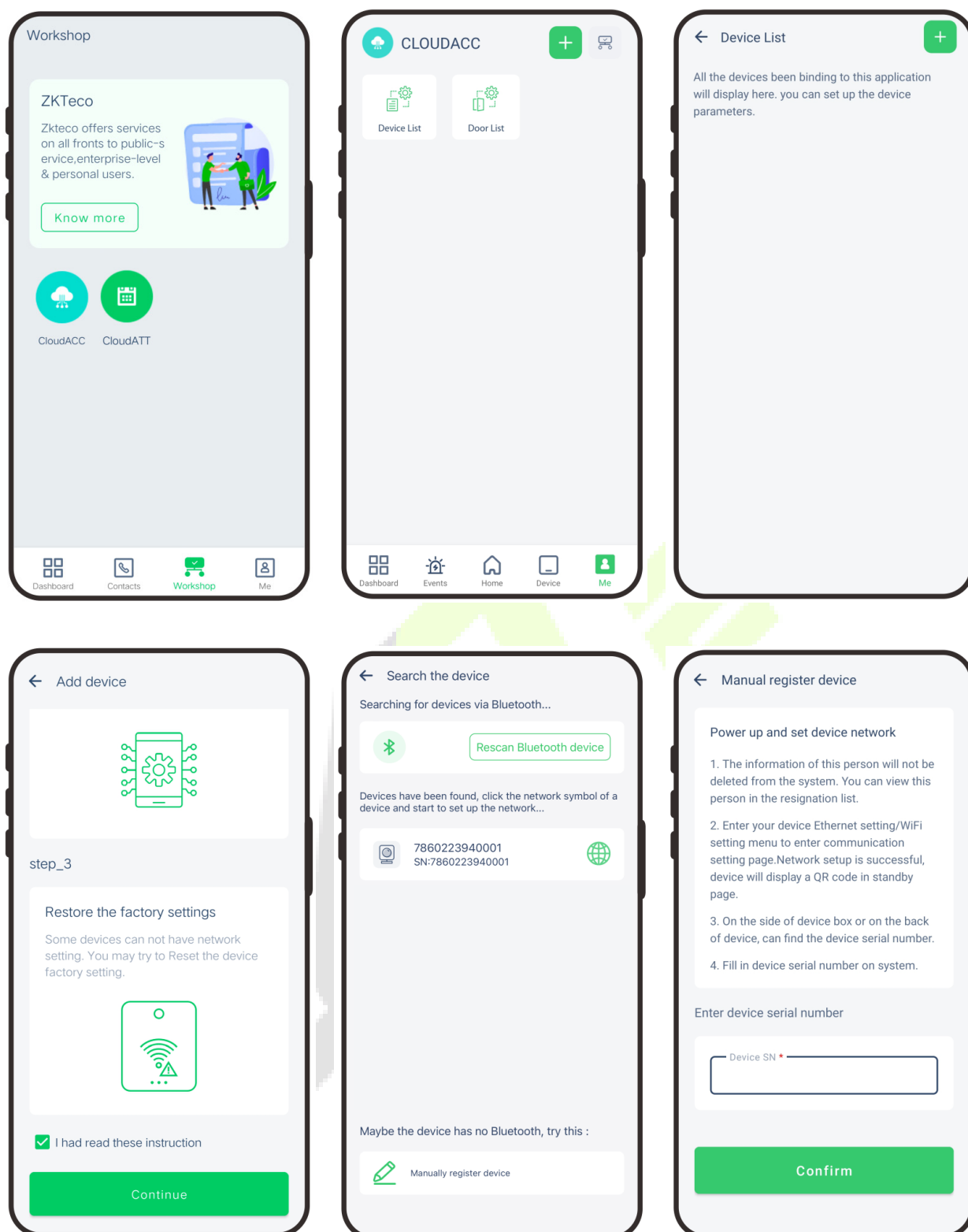
1. Click **Me > Organization > Site (or Zone)** on the main menu.
2. Click  icon to add a new site or zone. Enter the information, and click **Save**.



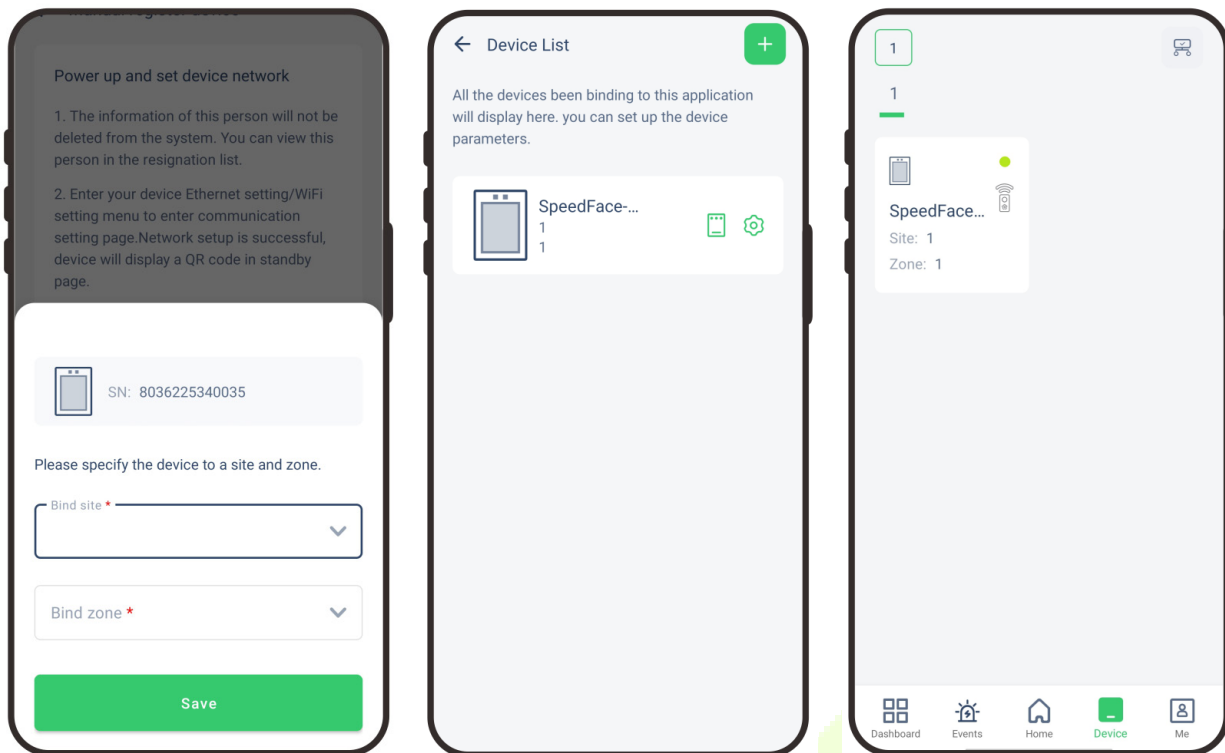


23.3.2 Add Device

1. Press **M/OK** and enter **COMM.** > **Ethernet** on the device to set the IP address and gateway of the device.
2. Click **Workshop** > **CloudACC** on the main menu to enter the **ZKBio Cloud Access** interface.
3. Click **Me** > **Device List** to enter the **Device** interface. And click  icon to add a new device.
4. Click **Manually register device**.
5. Read and check to the instructions, then click **Continue**.
6. Enter the device's serial number, then click **Confirm**. (Press **M/OK** and enter **System Info** > **Device Info** on the device to view the serial number.)



7. Choose a site and a zone, then click **Save** to finish.
8. Then click **Device**, users can view the device status and unlock remotely in this interface.



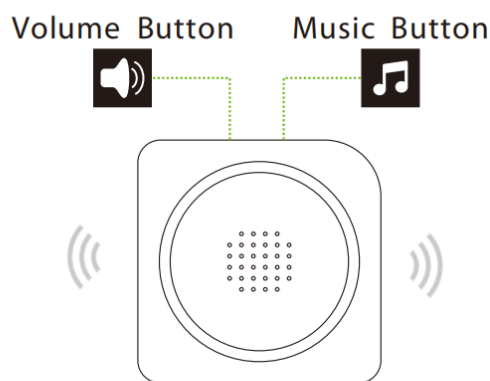
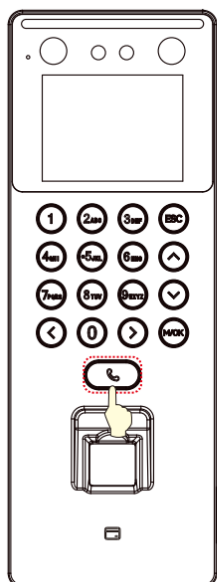
24 Connecting to Wireless Doorbell★



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

24.1 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 F35 only supports one wireless doorbell.
- 3) Wireless doorbell needs to be purchased by the customers themselves.

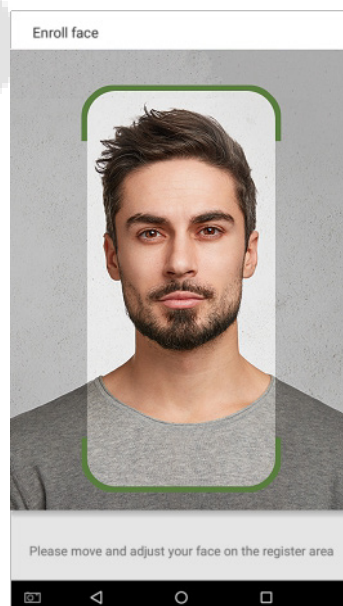
24.2 Unbinding the Wireless Doorbell

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.

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).



Requirements for Visible Light Digital Face Template Data

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

- **Eye distance**

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

- **Facial expression**

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

- **Gesture and angel**

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

- **Accessories**

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

- **Face template**

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

- **Template format**

Should be in BMP, JPG or JPEG.

- **Data requirement**

Should comply with the following requirements:

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

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. If you do not agree to the relevant agreement or any of its terms, you must stop using our products and services.

I. Collected Information

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

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

II. Product Security and Management

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

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

III. How we handle personal information of minors

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

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

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

IV. Others

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



Eco-friendly Operation



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

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

Hazardous or Toxic substances and their quantities

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

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

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

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

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

Phone : +86 769 - 82109991

Fax : +86 755 - 89602394

www.zkteco.com

