

User Manual

SpeedPalm-V5L

Date: July 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 **SpeedPalm-V5L**.

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	INSTRUCTION FOR USE	8
1.1	STANDING POSITION, FACIAL EXPRESSION AND STANDING POSTURE	8
1.2	FACE TEMPLATE REGISTRATION	9
1.3	PALM REGISTRATION.....	10
1.4	STANDBY INTERFACE.....	10
1.5	VIRTUAL KEYBOARD.....	12
1.6	VERIFICATION MODE	13
1.6.1	PALM VERIFICATION	13
1.6.2	FACIAL VERIFICATION	15
1.6.3	CARD VERIFICATION	18
1.6.4	PASSWORD VERIFICATION.....	20
1.6.5	COMBINED VERIFICATION.....	23
2	OVERVIEW.....	24
2.1	APPEARANCE.....	24
2.2	WIRING DESCRIPTION.....	25
3	INSTALLATION.....	28
3.1	INSTALLATION ENVIRONMENT.....	28
3.2	HOW TO INSTALL THE DEVICE ON THE WALL?.....	28
4	MAIN MENU	31
5	USER MANAGEMENT.....	33
5.1	USER REGISTRATION	33
5.1.1	REGISTER A USER ID AND NAME	33
5.1.2	SETTING THE USER ROLE	34
5.1.3	REGISTER PALM.....	34
5.1.4	REGISTER FACE TEMPLATE.....	35
5.1.5	REGISTER CARD NUMBER.....	36
5.1.6	REGISTER PASSWORD.....	37
5.1.7	REGISTER PROFILE PHOTO.....	37
5.1.8	ACCESS CONTROL ROLE.....	38
5.2	SEARCH USER.....	39
5.3	EDIT USER.....	39
5.4	DELETING USER.....	40
5.5	DISPLAY STYLE.....	40
6	USER ROLE	42
7	COMMUNICATION SETTINGS.....	44
7.1	NETWORK SETTINGS	44
7.2	PC CONNECTION	45
7.3	WIRELESS NETWORK.....	45
7.4	CLOUD SERVER SETTING	48
7.5	WIEGAND SETUP	48

7.5.1	WIEGAND INPUT	49
7.5.2	WIEGAND OUTPUT	51
7.6	NETWORK DIAGNOSIS.....	52
8	SYSTEM SETTINGS.....	53
8.1	DATE AND TIME	54
8.2	ACCESS LOGS SETTING/ATTENDANCE	55
8.3	FACE PARAMETERS.....	57
8.4	PALM PARAMETERS	59
8.5	HEALTH PROTECTION.....	60
8.6	DEVICE TYPE SETTINGS	61
8.7	SECURITY SETTINGS	61
8.8	TAP-TO UNLOCK.....	62
8.9	UPDATE FIRMWARE ONLINE.....	63
8.10	FACTORY RESET	66
9	PERSONALIZE SETTINGS	67
9.1	INTERFACE SETTINGS.....	67
9.2	VOICE SETTINGS.....	68
9.3	BELL SCHEDULES.....	68
9.4	PUNCH STATES OPTIONS.....	69
9.5	SHORTCUT KEYS MAPPINGS.....	70
10	DATA MANAGEMENT	72
10.1	DELETE DATA.....	72
11	INTERCOM	74
11.1.1	LOCAL AREA NETWORK USE	76
11.1.2	SIP SERVER	79
12	ACCESS CONTROL.....	81
12.1	ACCESS CONTROL OPTIONS.....	82
12.2	TIME RULE SETTINGS/ TIME SCHEDULE.....	85
12.3	HOLIDAYS	86
12.4	ACCESS GROUPS	87
12.5	COMBINED VERIFICATION	88
12.6	ANTI-PASSBACK SETUP	89
12.7	DURESS OPTIONS SETTINGS	91
13	ATTENDANCE SEARCH	92
14	AUTOTEST	94
15	SYSTEM INFORMATION.....	95
16	CONNECT TO ZKBIO TIME SOFTWARE.....	96
16.1	SET THE COMMUNICATION ADDRESS	96
16.2	ADD DEVICE ON THE SOFTWARE.....	96
16.3	ADD PERSONNEL TO THE SOFTWARE.....	97

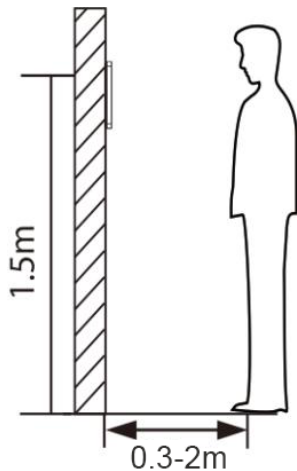
17	CONNECT TO ZKBIO CVACCESS SOFTWARE	98
17.1	SET THE COMMUNICATION ADDRESS	98
17.2	ADD DEVICE ON THE SOFTWARE.....	99
17.3	ADD PERSONNEL TO THE SOFTWARE.....	100
18	CONNECT TO ZKBIO CVSECURITY SOFTWARE.....	101
18.1	SET THE COMMUNICATION ADDRESS	101
18.2	ADD DEVICE ON THE SOFTWARE.....	102
18.3	ADD PERSONNEL TO THE SOFTWARE.....	103
APPENDIX 1	104
	REQUIREMENTS OF LIVE COLLECTION AND REGISTRATION OF VISIBLE LIGHT FACE TEMPLATES	104
	REQUIREMENTS FOR VISIBLE LIGHT DIGITAL FACE TEMPLATE DATA	105
APPENDIX 2	106
	PRIVACY POLICY	106
	ECO-FRIENDLY OPERATION	109

1 Instruction for Use

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

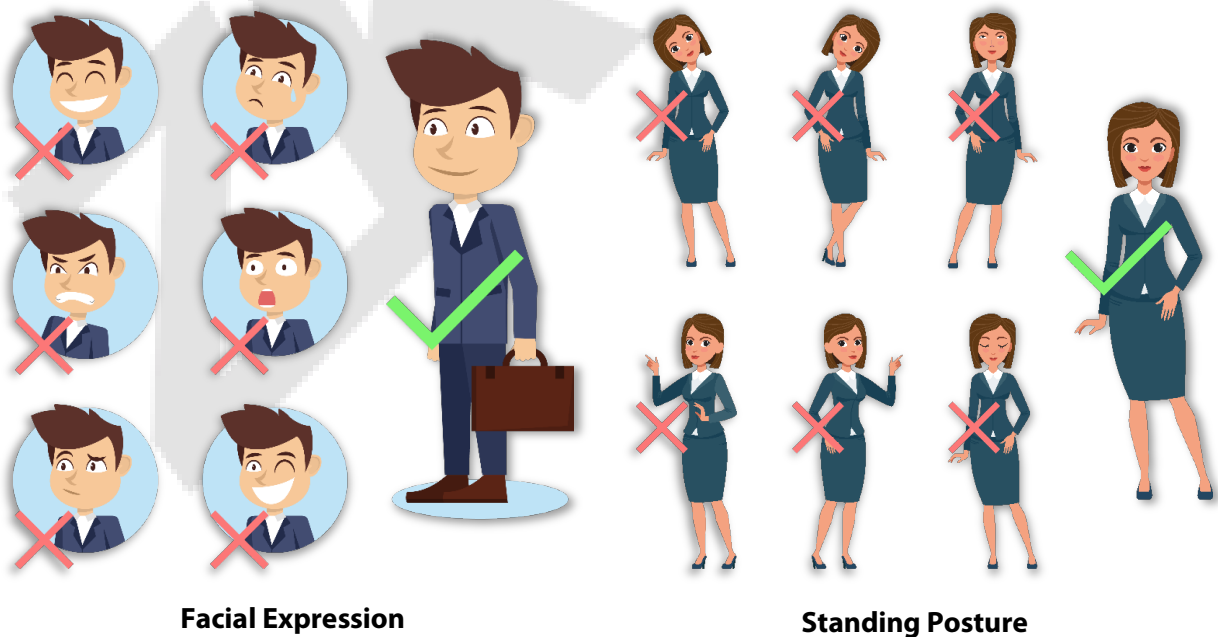
1.1 Standing Position, Facial Expression and Standing Posture

● The Recommended Distance



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

● Recommended Standing Posture and Facial Expression



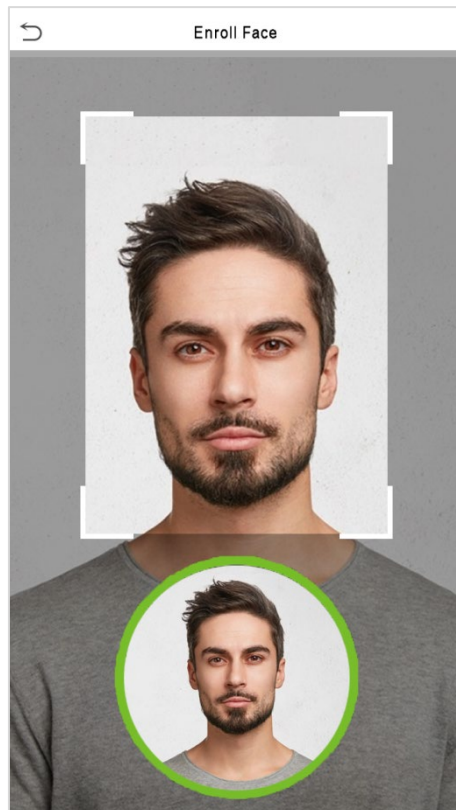
Facial Expression

Standing Posture

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

1.2 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 Template

- 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.

1.3 Palm Registration

Place your palm in the palm collection area, such that the palm is placed parallel to the device.

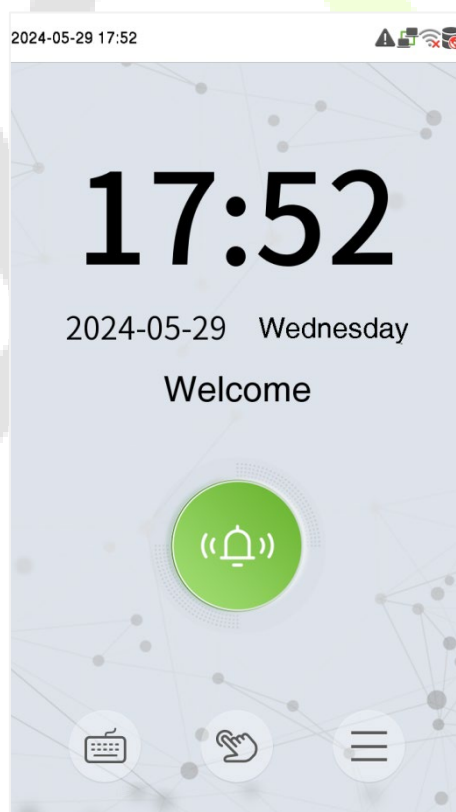
Make sure to keep space between your fingers.





1. Place your palm within 5 to 15 cm of the device.
2. Place your palm in front of the biometric module, such that the palm is placed parallel to the device.
3. Make sure to keep space between your fingers.


1.4 Standby Interface

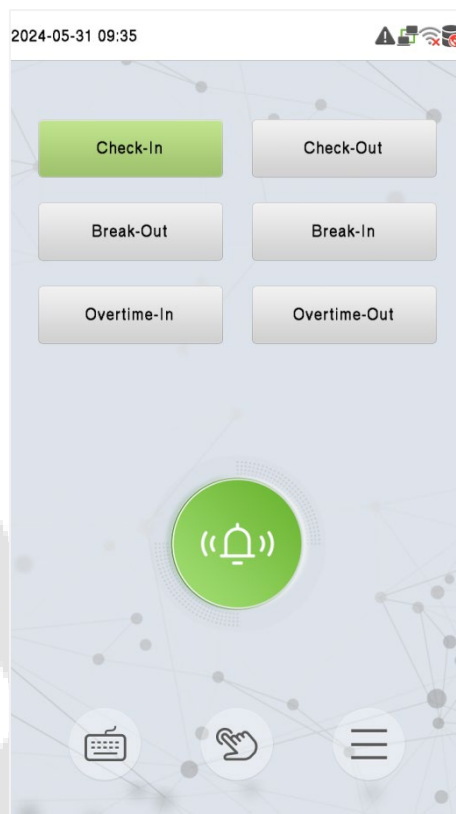
After connecting the power supply, the following standby interface is displayed:



- Tap  to enter the User ID input interface.
- When there is no Super Administrator set in the device, tap  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.

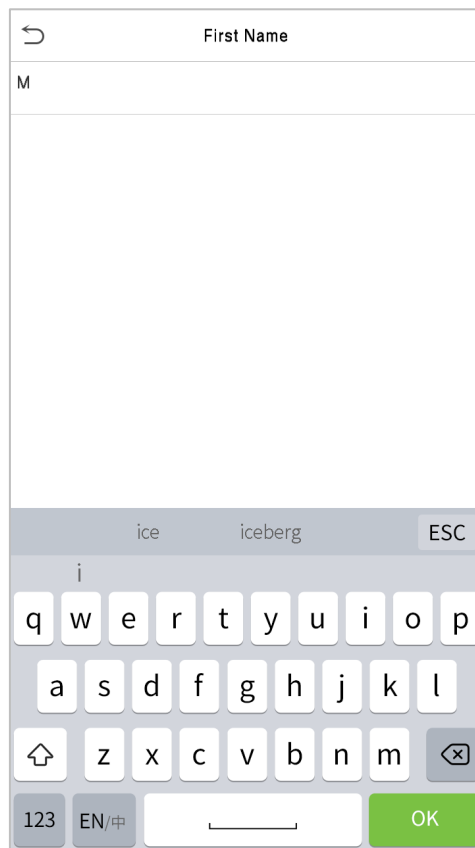
- Visitors tap  to [make a call](#) and the phone will ring.
- The punch state options can also be displayed and used directly on the standby interface. Tap anywhere on the screen apart from the icons, and six shortcut keys appears on the screen, as shown in the figure below:



- Press the corresponding punch state key to select your current punch state, which is displayed in green. Please refer to "[Shortcut Key Mappings](#)" for the specific operation method.

Note: The punch state options are off by default and need to select other mode options in the "[Punch States Options](#)" to get the punch state options on the standby screen.

1.5 Virtual Keyboard



Note: The device supports the input in English language, numbers, and symbols.

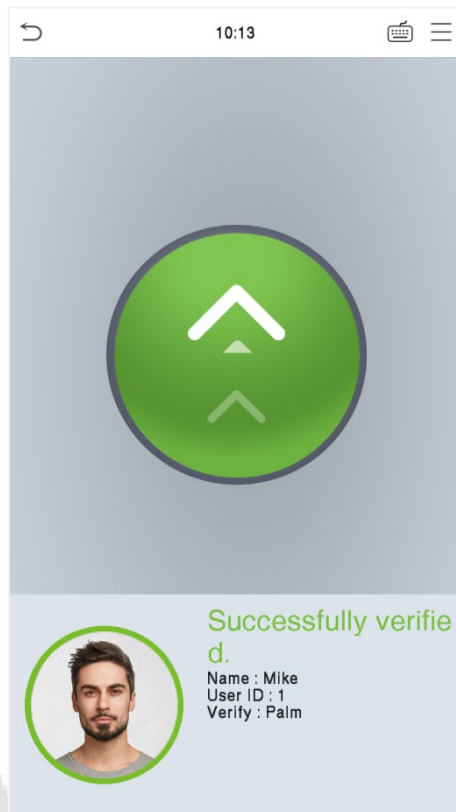
- Tap [**123**] to switch to the numeric and symbolic keyboard.
- Tap [**ABC**] to return to the alphabetic keyboard.
- Tap the input box, a virtual keyboard appears.
- Tap [**ESC**] to exit the virtual keyboard.

1.6 Verification Mode


1.6.1 Palm Verification

- **1: N Palm Verification Mode**

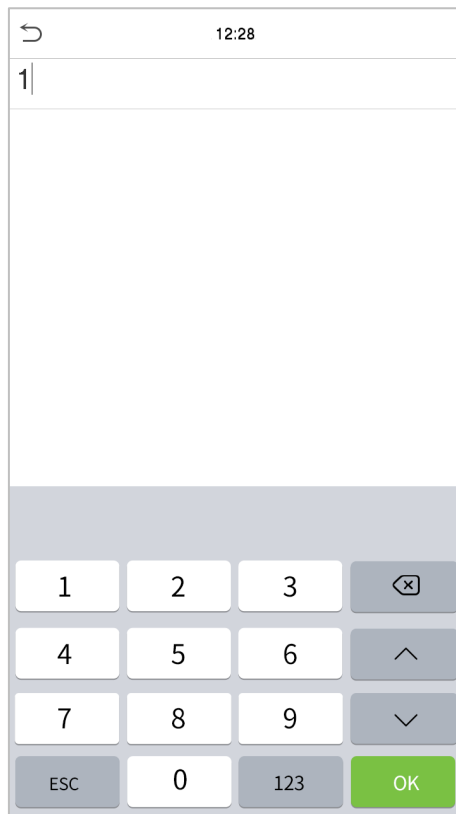
In this verification mode, the device compares the palm image collected by the biometric module with all the palm data in the device.



- **1: 1 Palm Verification Mode**

Tap the  button on the main screen to enter 1:1 palm verification mode.

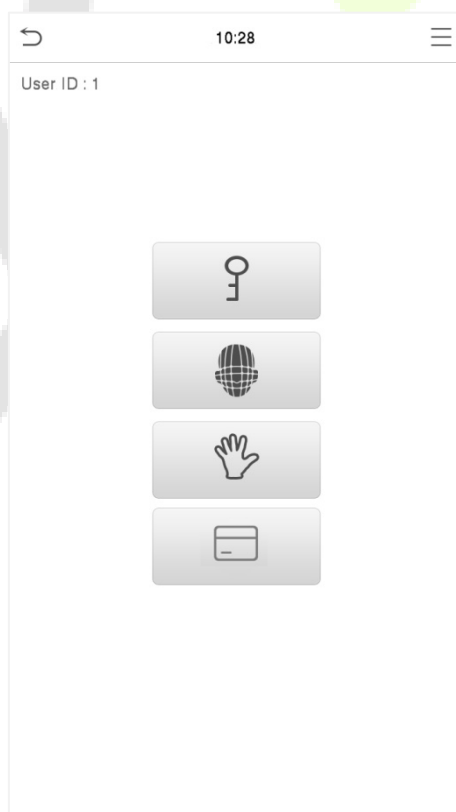
Input the user ID and tap **[OK]**.



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



icon to enter palm verification mode.

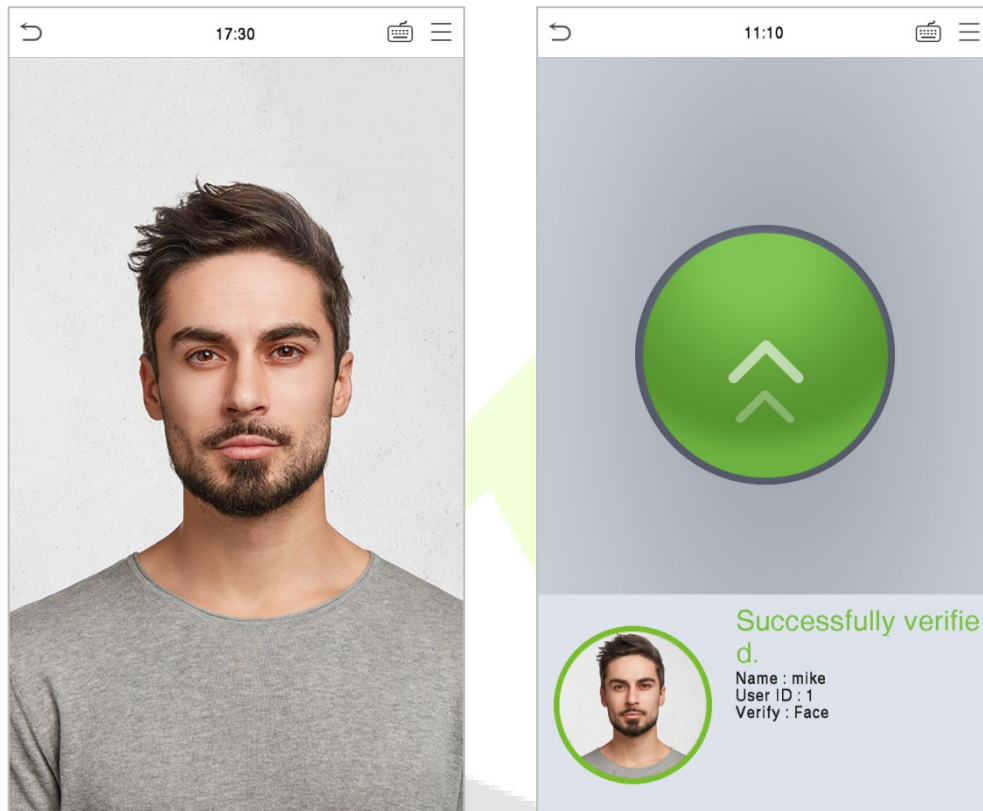


1.6.2 Facial Verification

- **1:N Facial Verification**

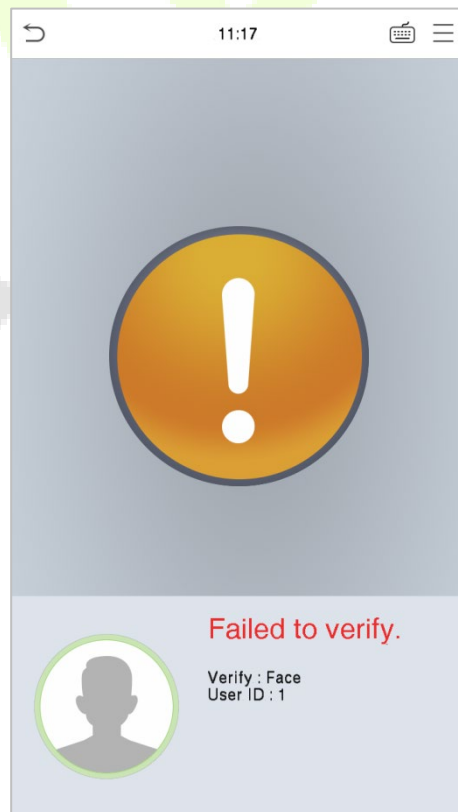
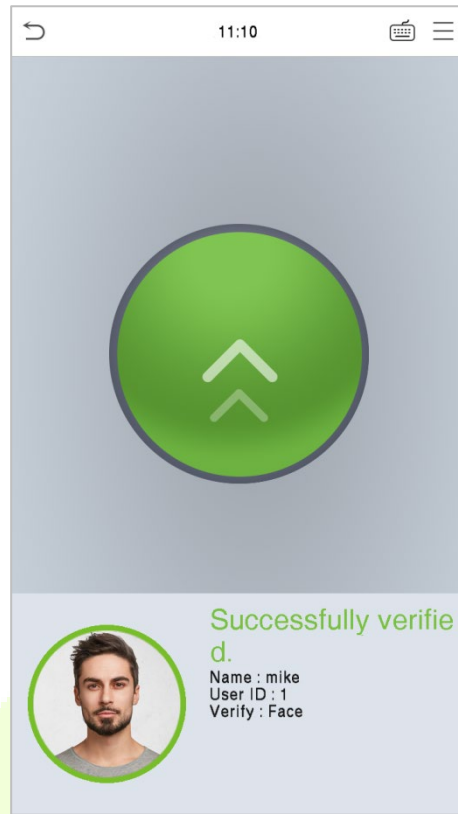
Conventional Verification

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




Enable Mask Detection

When the user enables the **Enable mask detection** function, the device will identify whether the user is wearing a mask or not while verification. The following are the popups of the comparison result prompt interface.

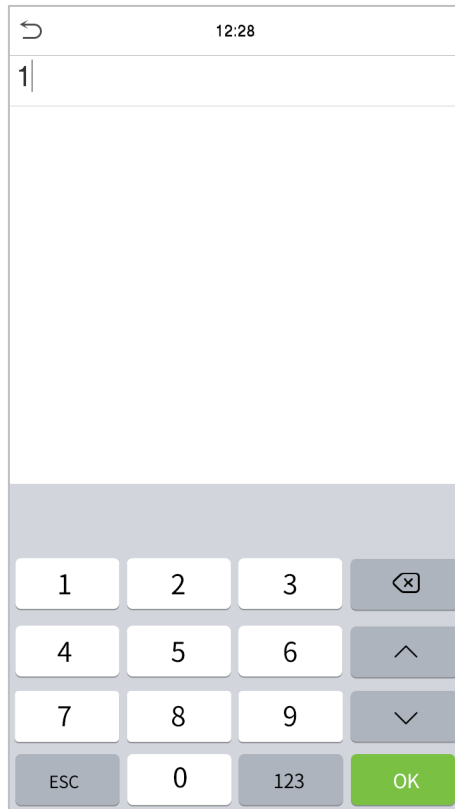


● 1:1 Facial Verification


Compare the face captured by the camera with the facial template related to the entered user ID.

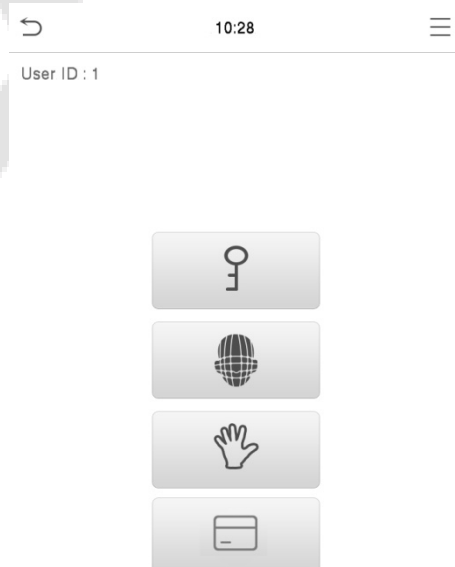
Tap  on the main interface and enter the 1:1 facial verification mode.

Enter the user ID and tap **[OK]**.

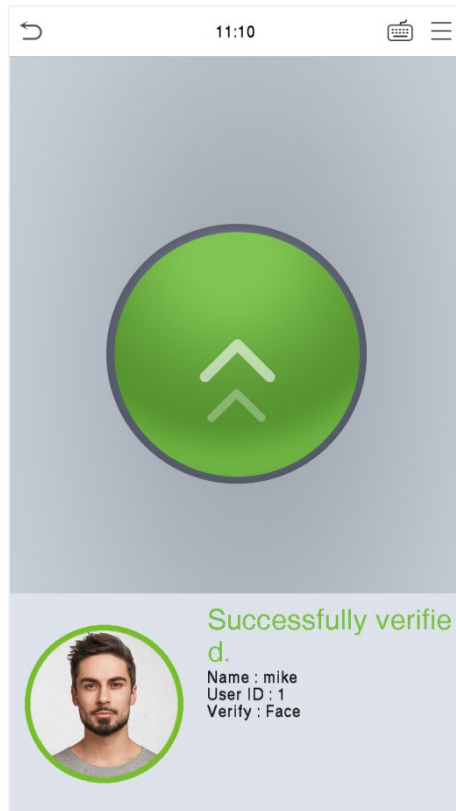


If the user has registered password, palm and card in addition to his/her face template and the verification method is set to Password/Face/Palm/Card verification, the following screen will appear. Select the face

 icon to enter face verification mode.



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

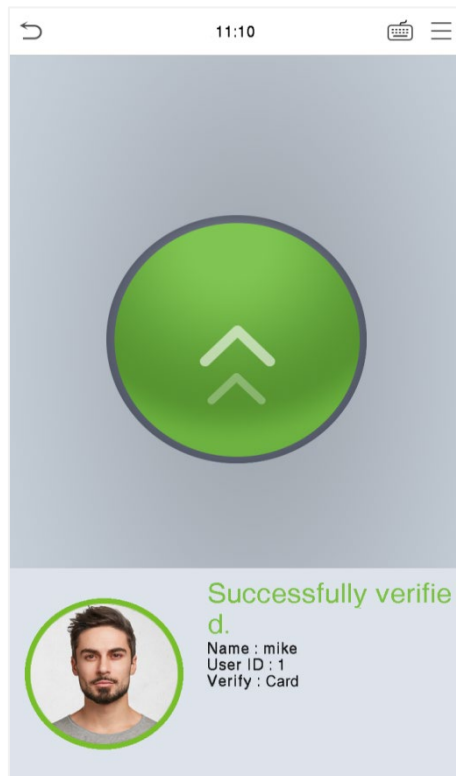


If the verification is failed, it prompts "**Please adjust your position!**".

1.6.3 Card Verification


- **1:N Card Verification**

The 1: N Card Verification mode compares the card number in the card induction area with all the card number data registered in the device; The following is the card verification screen.

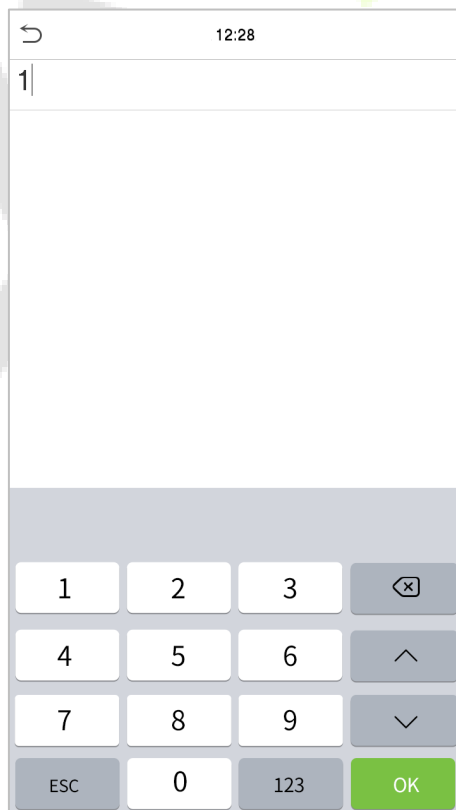


- **1:1 Card Verification**

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

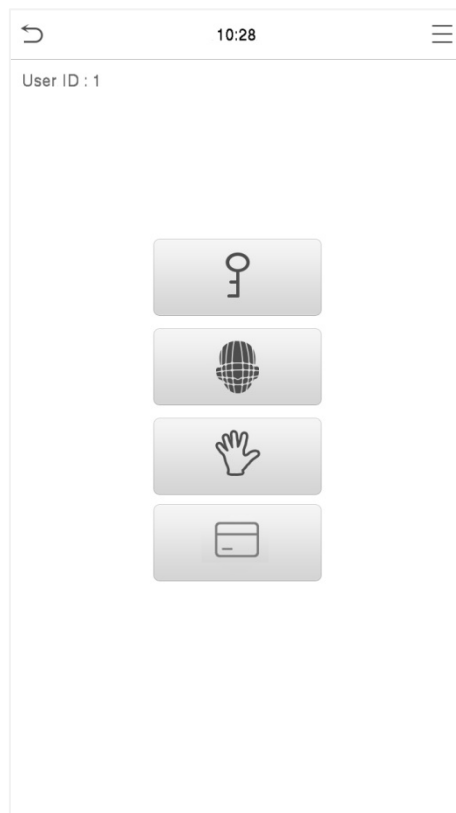
Tap  on the main interface and enter the 1:1 card verification mode.

Enter the user ID and tap **[OK]**.




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

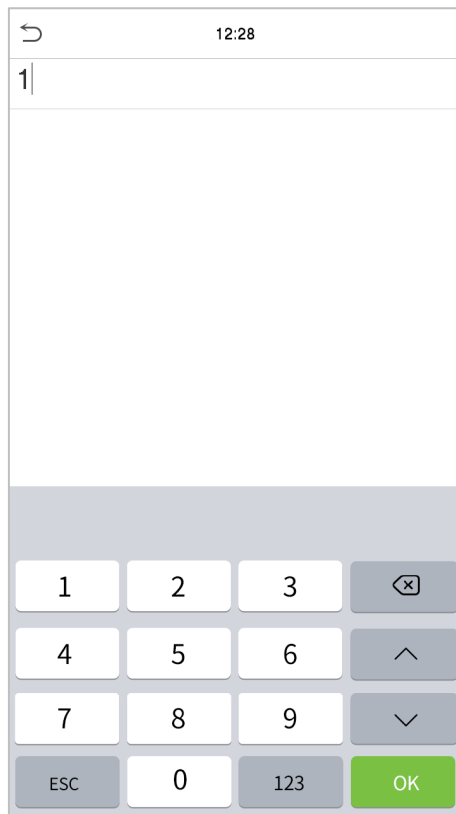
 icon to enter card verification mode.




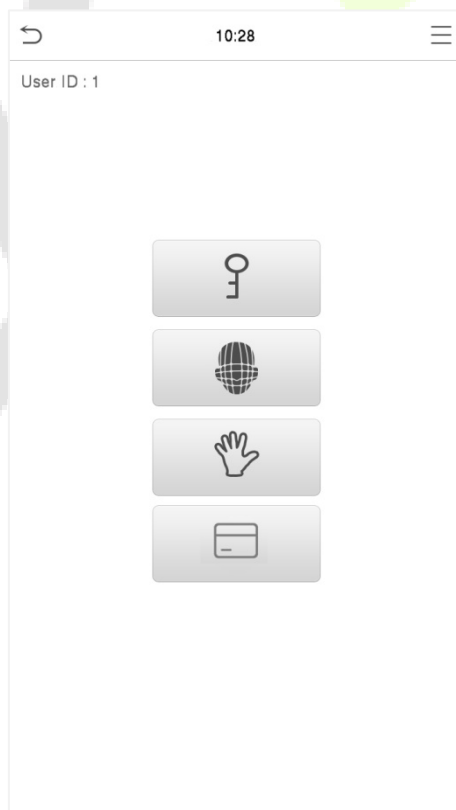
1.6.4 Password Verification

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

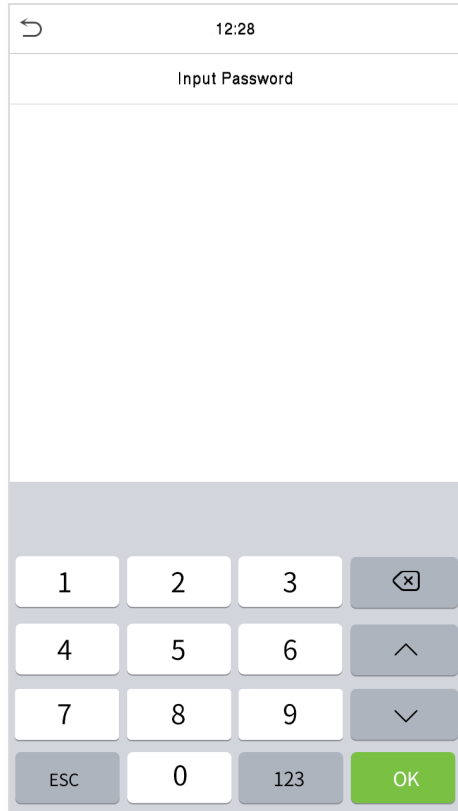
Tap the  button on the main screen to enter the 1:1 password verification mode. Then, input the user ID and tap **[OK]**.



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

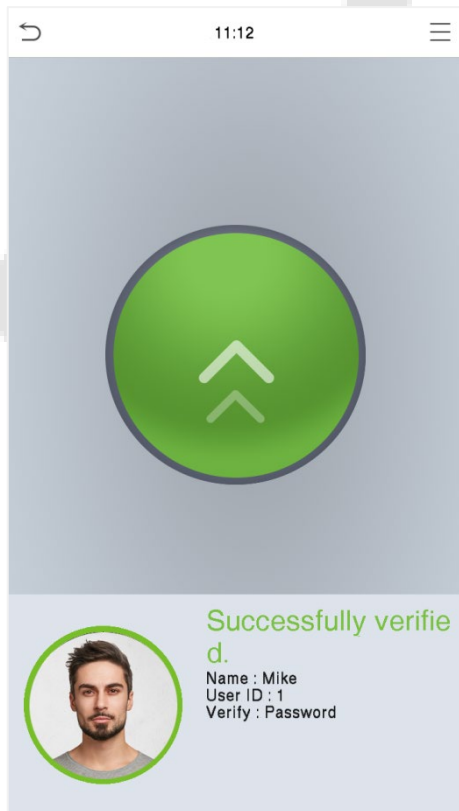


Input the password and tap [OK].

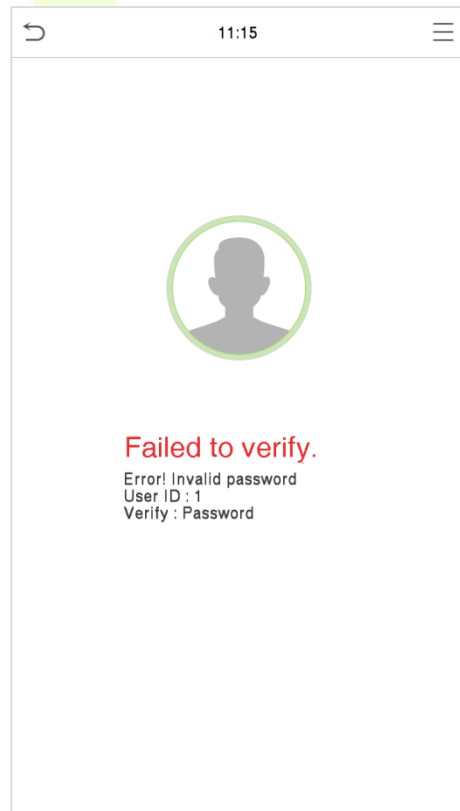


Following are the display screen after entering a correct password and a wrong password respectively.

Verification is successful:



Verification is failed:

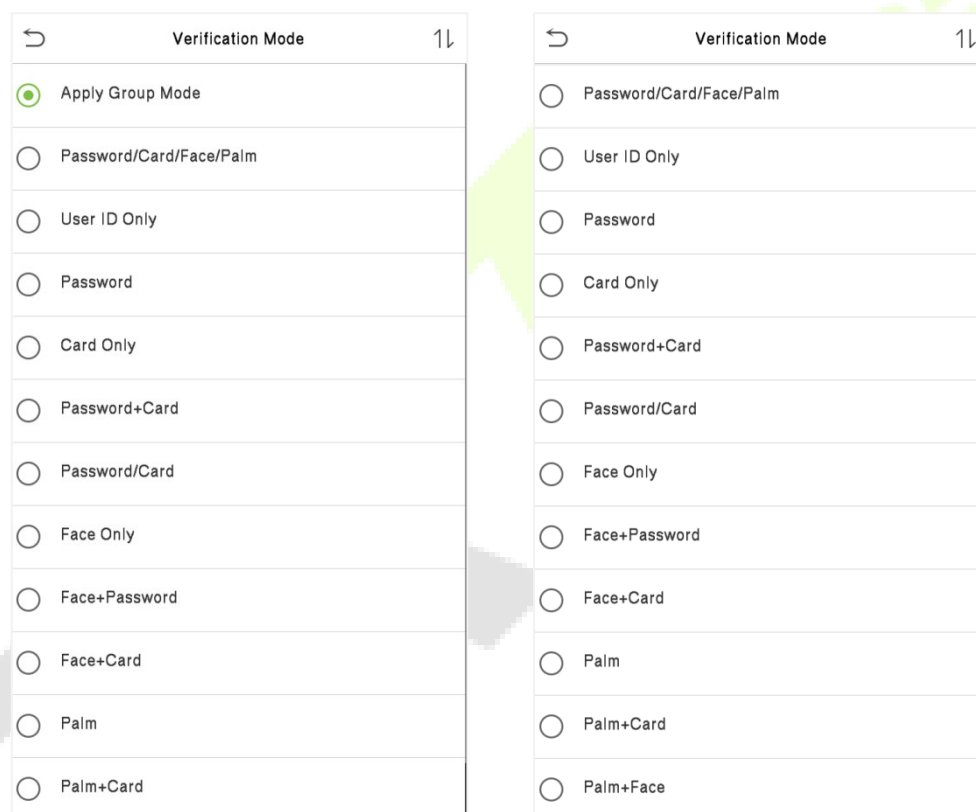


1.6.5 Combined Verification

This device allows you to use a variety of verification methods to increase security. There are a total of 13 distinct 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.

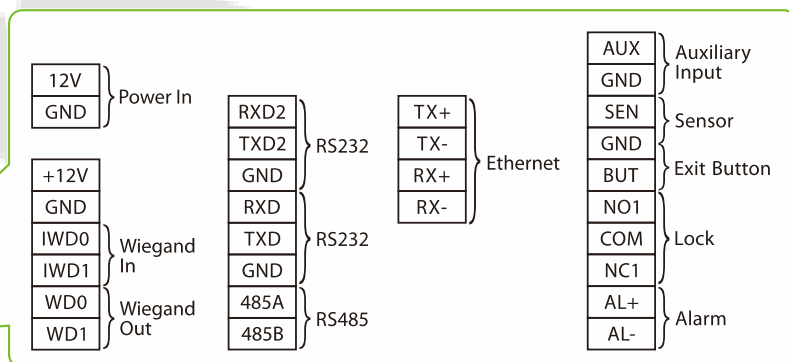
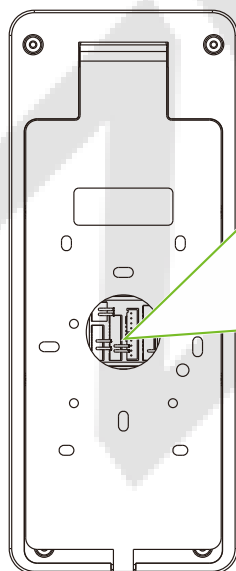
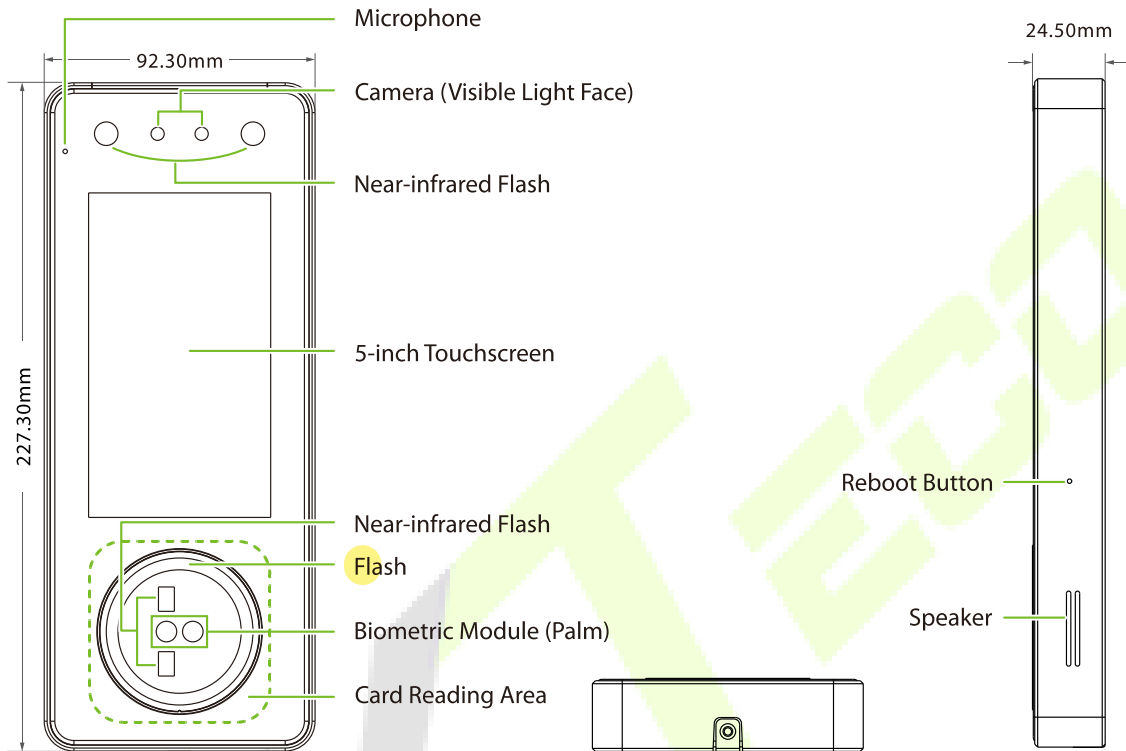


Procedure to Set for Combined Verification Mode

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

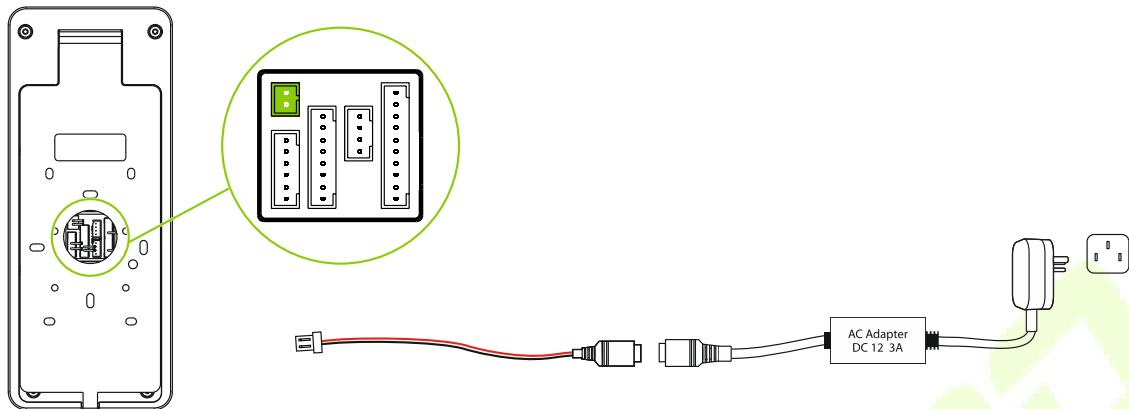
2 Overview

2.1 Appearance



2.2 Wiring Description

● Power Connection

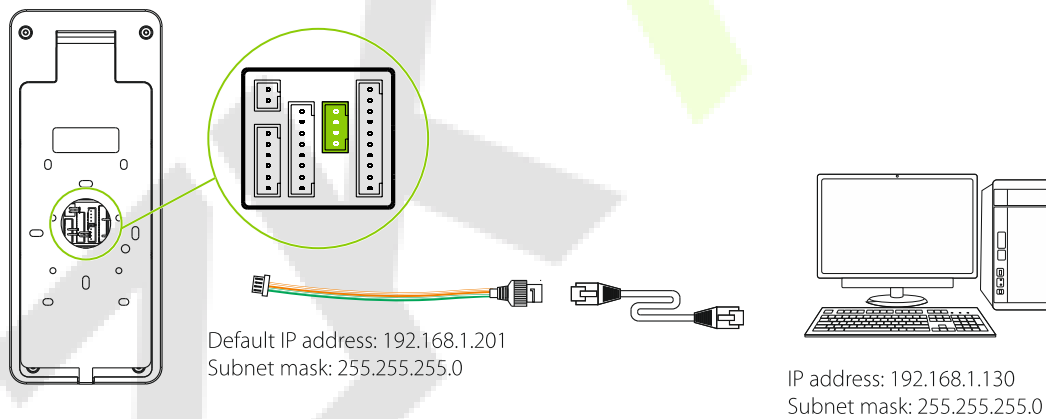


Recommended power supply

- Rating of 12V and 3A
- To share the power with other devices, use an AC Adapter with higher current ratings.

● Ethernet Connection

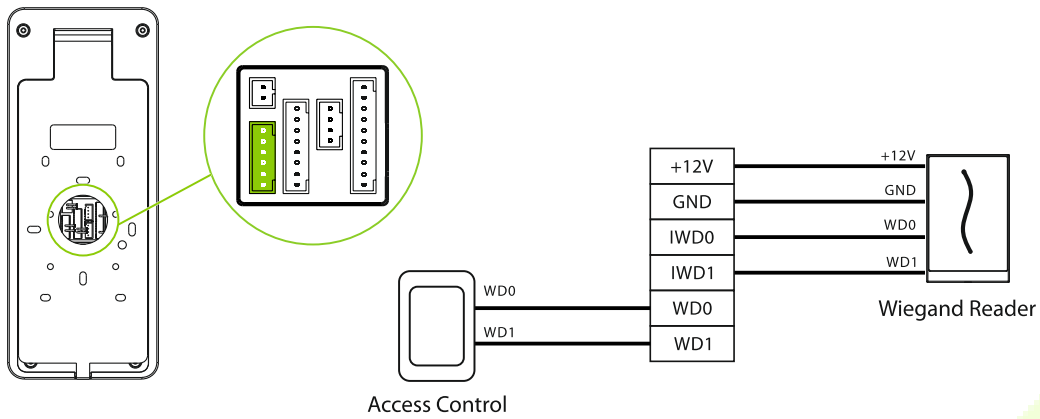
Connect the device and computer software over an Ethernet cable. As shown in the example below:



Tap on **[COMM.]** > **[Ethernet]** > **[IP Address]**, input the IP address and tap on **[OK]**.

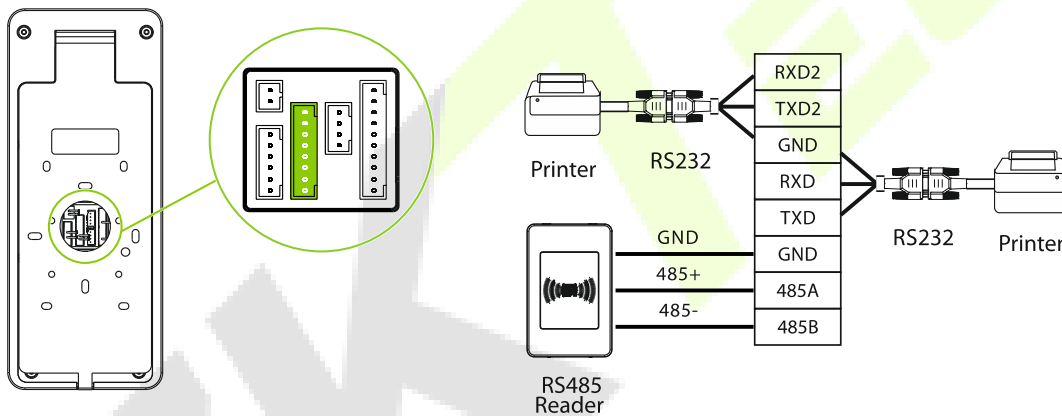
Note: In LAN, the IP addresses of the server (PC) and the device must be in the same network segment when connecting to the ZKBio CVAccess/ZKBio Time /ZKBio CVSecurity software.

● **Wiegand Reader Connection**

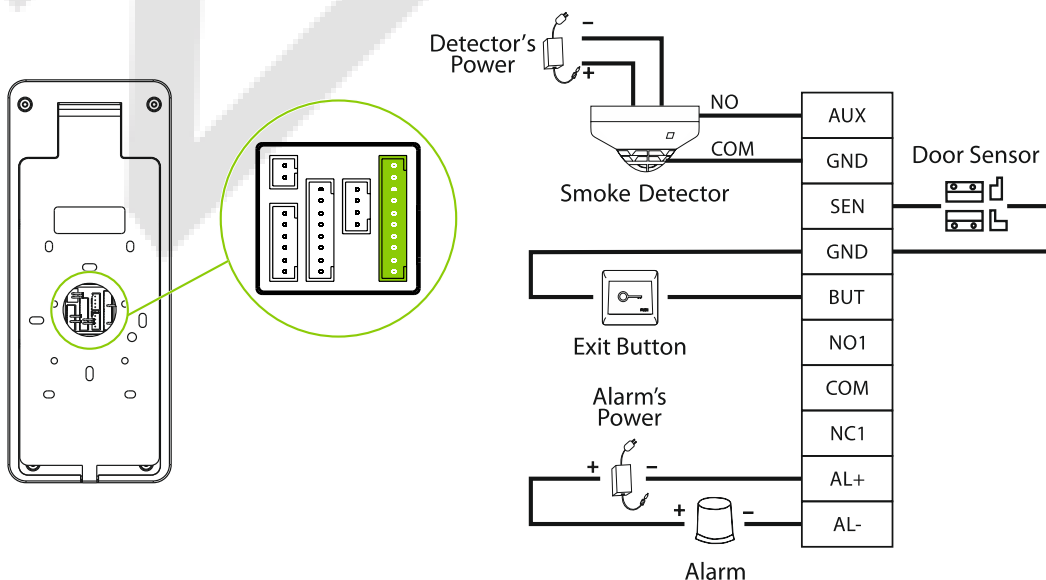


● **RS485 and RS232 Connection★**

The RS485 and the RS232 lets user connect to multiple readers to the device. The RS232 and RS485 can be connected to the terminal, as shown in the figure below.

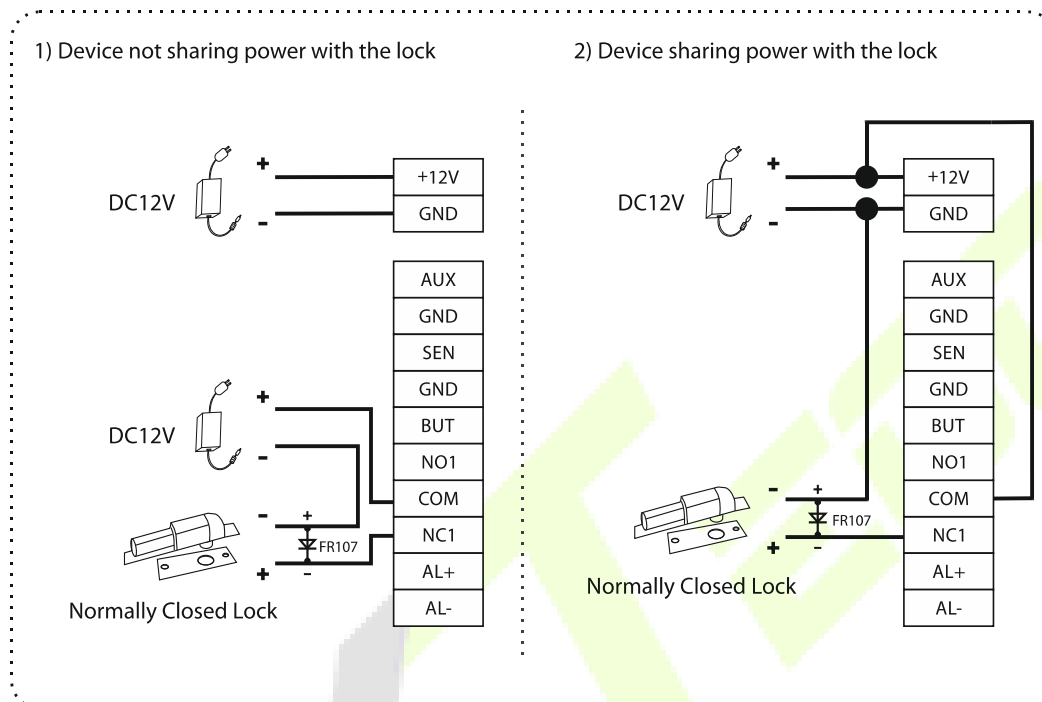


● **Door Sensor, Exit Button & Auxiliary Connection**



● 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 'COM' terminals, and the NC Lock (normally closed when powered) is connected with 'NC1' and 'COM' terminals. The power can be shared with the lock or can be used separately for the lock, as shown in the example with NC Lock below:



3 Installation

3.1 Installation Environment

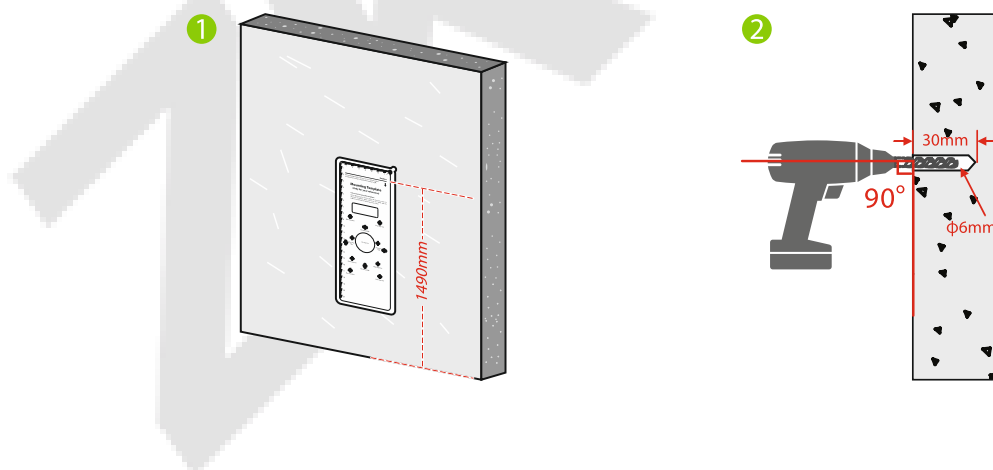
Please refer to the following recommendations for installation.



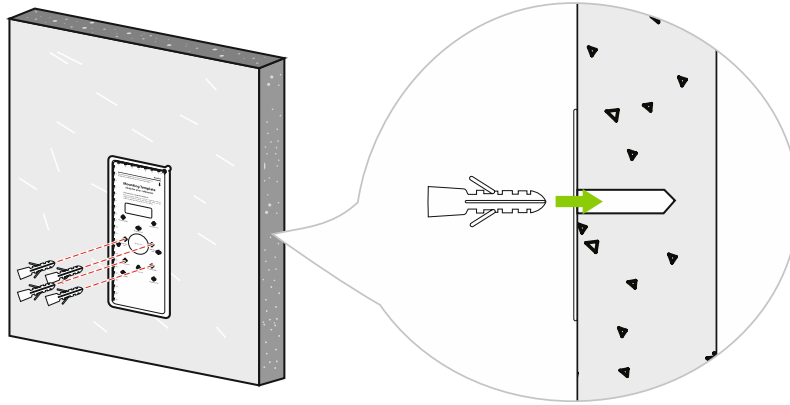
- Avoid direct contact to sunlight for a long time.
- Protect the device from moisture, water, and rain.
- Handle the device with care.
- Ensure that the device is not installed near the sea or in other locations where metal oxidation and rust may develop if the device is exposed for an extended period.
- Protect the device from lightning.
- Avoid using the device in acidic or alkaline environments for extended periods.

3.2 How to Install the Device on the Wall?

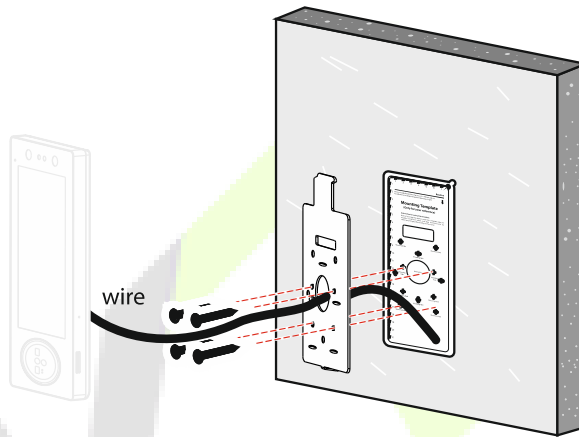
1. Stick the mounting template to the wall and drill holes according to the mounting template.



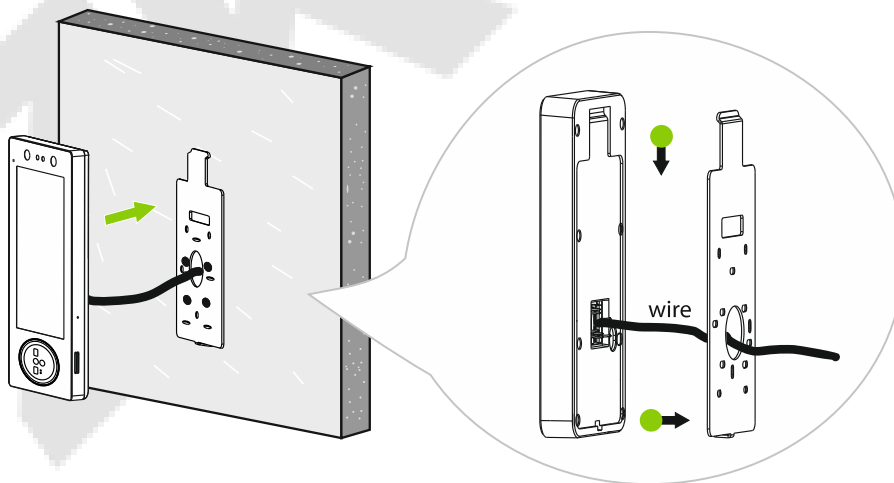
- 2. Insert the expansion tubes into the mounting holes.



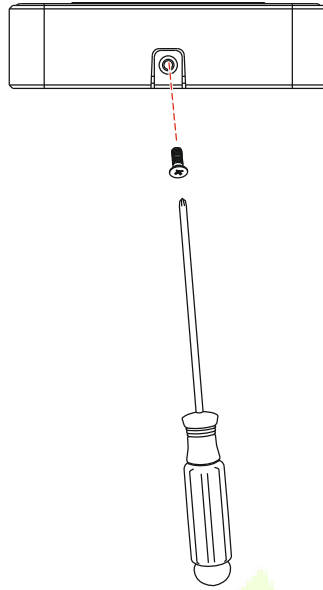
- 3. Attach the backplate on the wall using the wall mounting screws.




- 4. Attach the terminal to the backplate.

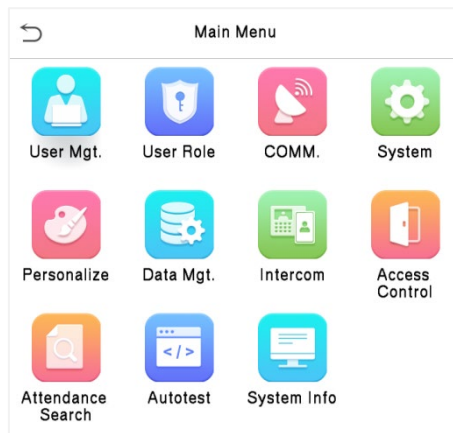


5. Fasten the terminal to the backplate with a security screw.



4 Main Menu

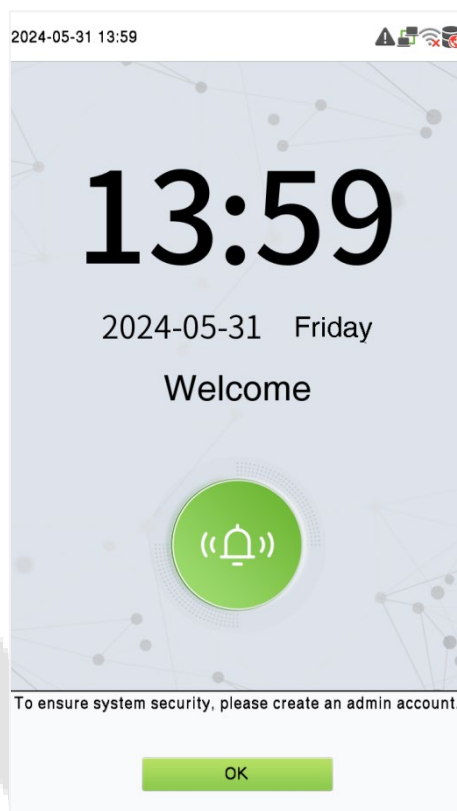
Tap  on the initial interface to enter the main menu, as shown below:



Menu	Description
User Mgt.	To add, edit, view, and delete the basic information about a user.
User Role	To set the permission scope of the custom role, that is, the rights to operate the system.
COMM.	To set the relevant parameters of the network, PC Connection, Wi-Fi, Cloud Server, Wiegand and Network Diagnosis.
System	To set the parameters related to the system, including Date Time, Tap-To-Unlock, Attendance/Access Logs, Facial and Palm templates, Resetting to factory settings, Security Settings, Update Firmware Online, Device Type Setting and Health Protection.
Personalize	To customize settings of User Interface, Voice, Bell Schedules, Punch State Options and Shortcut Key Mappings settings.
Data Mgt.	To delete all the relevant data in the device.
Intercom	To set the parameters related to the SIP.
Access Control	To set the parameters of the lock and the relevant access control device including options like Time Rule Setting/Time Schedule, Holiday Settings, Access Groups, Combine Verification, Anti-passback Setup and Duress Option Settings.
Attendance Search	To query the specified attendance record, check Attendance Photos and Blocklist attendance photos.

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

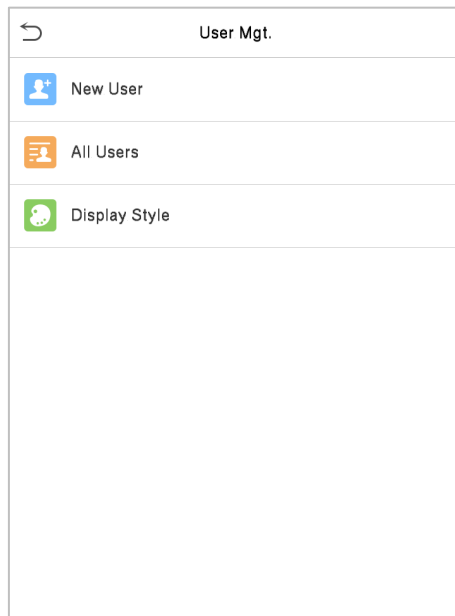
Note: When users use the product for the first time, they should operate it after setting administrator privileges. Tap User Mgt. to add an administrator or edit user permissions as a super administrator. If the product does not have an administrator setting, the system will show an administrator setting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



5 User Management

5.1 User Registration

Tap [**User Mgt.**] on the **Main Menu** interface.



5.1.1 Register a User ID and Name

Tap [**New User**] and enter the **User ID** and **Name**.

 A screenshot of the 'New User' registration form. At the top, there is a back arrow and the title 'New User'. The form consists of several rows, each with a label on the left and a value on the right:

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

 The bottom part of the form is empty.

Note:

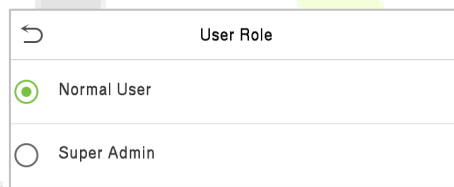
- A name can take up to 34 characters.
- The user ID may contain 1-14 digits by default, supporting both numbers and alphabetic characters.
- You can modify your ID during the initial registration but not after registration.
- If a message "**Duplicated!**" pops up, you must choose another ID as the entered User ID already exists.

5.1.2 Setting the User Role

On the New User interface, tap on [**User Role**] to set the user's duty as either **Normal User** or **Super Admin**.

Tap [**User Role**] to select 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.



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

5.1.3 Register Palm

Tap [**Palm**] in the **New User** interface to enter the palm registration page.

- Please place your palm inside the guiding box and keep it still while registering.
- A progress bar shows up while registering the palm and a "**Enrolled Successfully**" is displayed as the progress bar completes.

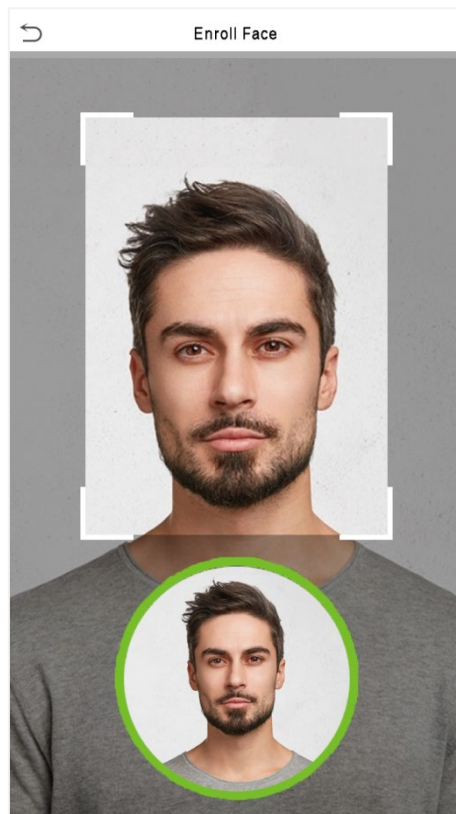
If the palm is registered already then, the "**Palm repeated**" message shows up. The registration interface is as follows:



5.1.4 Register Face Template

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

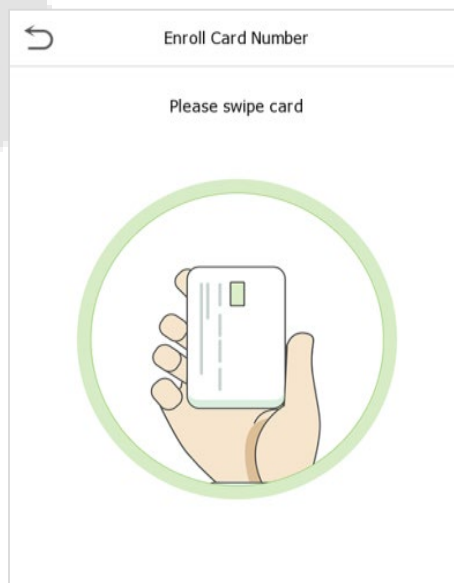
- Please face towards the camera and place yourself in such a way that your face image fits inside the white guiding box and stays still during face registration.
- A progress bar shows up while registering the face and then "**Enrolled Successfully**" message is displayed as the progress bar completes.
- If the face is registered already then, the "**Duplicated Face**" message shows up. The registration interface is as follows:



5.1.5 Register Card Number

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

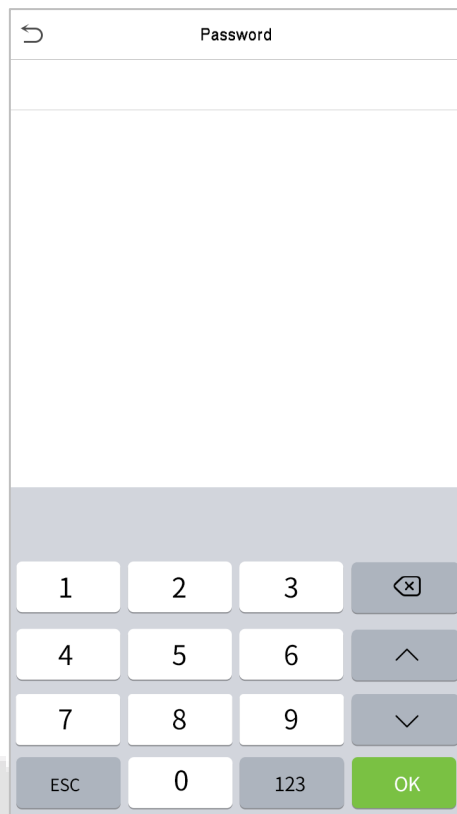
- On the Card interface, swiping card underneath the card reading area. The card registration will be successful.
- If the card is registered already then the “**Duplicate Card**” message shows up. The registration interface is as follows:



5.1.6 Register Password

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

- On the Password interface, enter the required password and re-enter to confirm it and tap [**OK**].
- If the re-entered password is different from the initially entered password, then the device prompts the message as "**Password does not match!**", where the user needs to re-confirm the password again.
- The password may contain 1 to 8 digits by default.

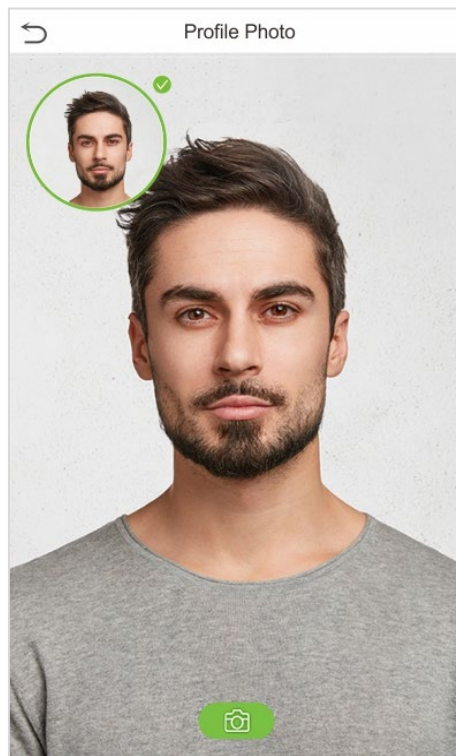


5.1.7 Register Profile Photo

Tap [**Profile Photo**] in the **New User** interface to enter the profile photo registration page.

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

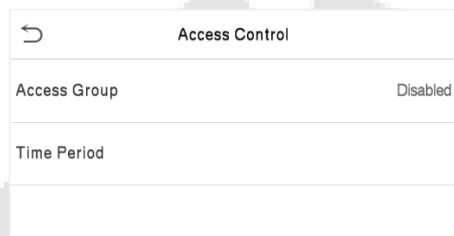
Note: While registering a face, the system automatically captures a photo as the user photo. If you do not register a user photo, the system automatically sets the photo captured while registration as the default photo.



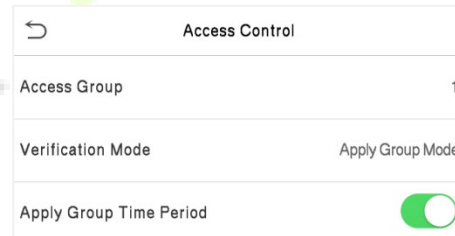
5.1.8 Access Control Role

The **[Access Control Role]** sets the door access privilege for each user. It includes the access group, verification mode and it facilitates setting the group access time period.

Access Control Terminal:



Time Attendance Terminal:

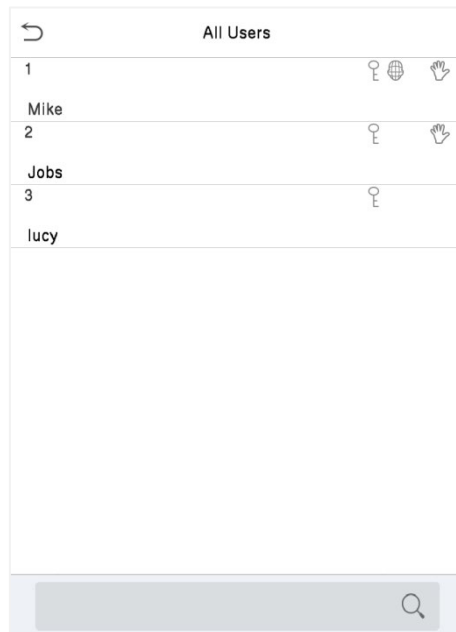


- Tap **[Access Control Role]** > **[Access Group]** to assign the registered users to different groups for better management. New users belong to Group 1 by default and can be reassigned to other groups. The device supports up to 99 Access Control groups.
- Tap **[Time Period]**, to select the time to use.
- Select verification mode for the user, tap **[Access Control Role]** > **[Verification Mode]**.
- Select whether to apply the group time period for this user. It is enabled by default. If the group time period is not applied, you need to set the unlocking time for this user. The time period of this user does not affect the time period of any other member in this group. To set the unlocking time for this user, tap **[Apply Group Time Period]** > **[Time Period 1]**. Enter the Time Period number and tap **[OK]**. 50 time periods can be set in the device and three time periods can be set for each user. For details, see Time Schedule Settings.

5.2 Search User

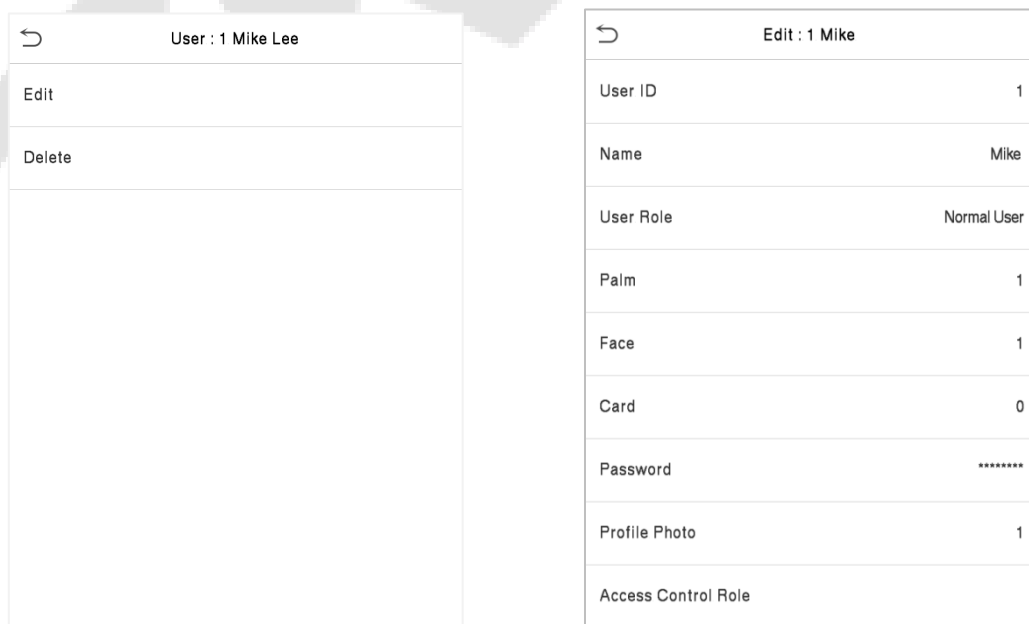
On the **Main Menu**, tap [**User Mgt.**], and then tap [**All Users**] to search a User.

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



5.3 Edit User

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



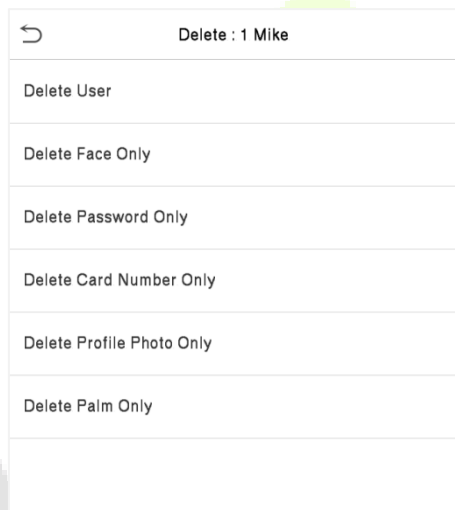
Note: The process of editing the user information is the same as adding a new user, except that the User ID cannot be modified when editing a user. The process in detail refers to "[User Registration](#)".

5.4 Deleting 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 tap [**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 Face Only:** Deletes the face information of the selected user.
- **Delete Password Only:** Deletes the password information of the selected user.
- **Delete Card Only:** Deletes the card information of the selected user.
- **Delete Profile Photo Only:** Deletes the profile photo of the selected user.
- **Delete Palm Only:** Deletes the palm information of the selected user.



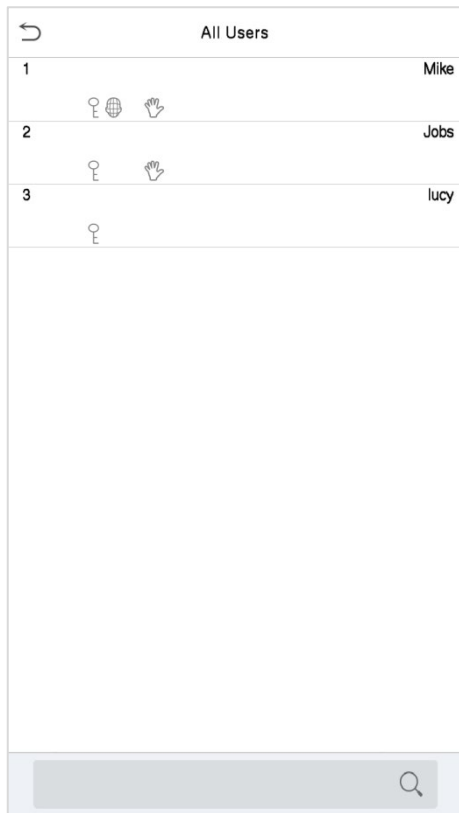
5.5 Display Style

On the **Main Menu**, tap [**User Mgt.**], and then tap [**Display Style**] to enter **Display Style** setting interface.

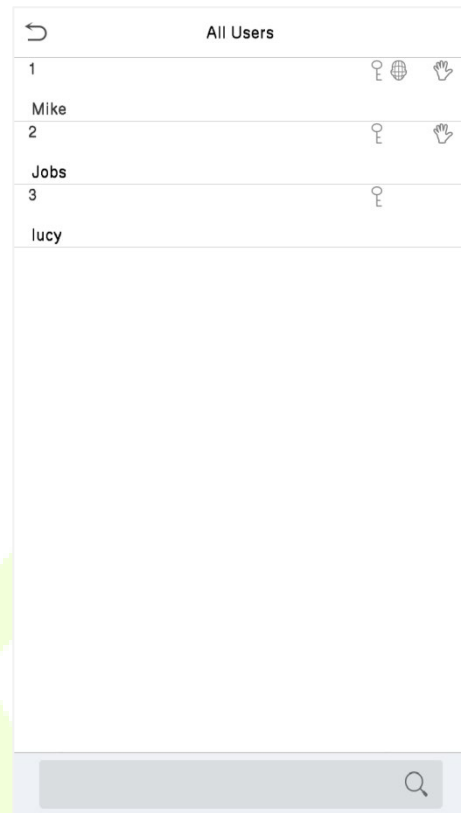


All the Display Styles are shown as below:

Multiple Line:



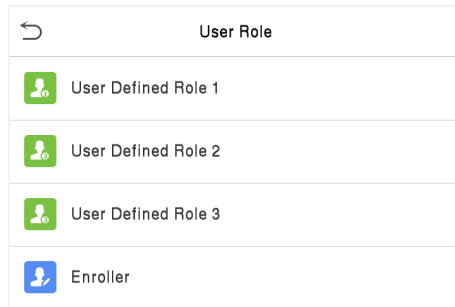
Mixed Line:



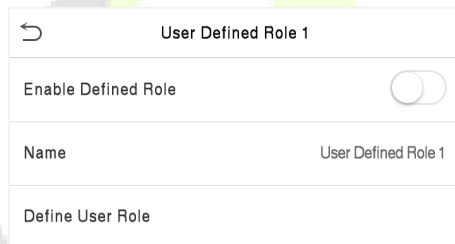
6 User Role

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

- On the **Main** menu, tap [**User Role**], and then tap on the **User Defined Role** to set the user defined permissions.
- The permission scope of the custom role can be set up 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.
- Tap on [**Name**] and enter the custom name of the role.



- Then, by tapping on **Define User Role**, select the required privileges for the new role, and then tap the Return button.
- During privilege assignment, the main menu function names will be displayed on the left and its sub-menus will be listed on the right.
- First tap on the required **Main Menu** function name, and then select its required sub-menus from the list.

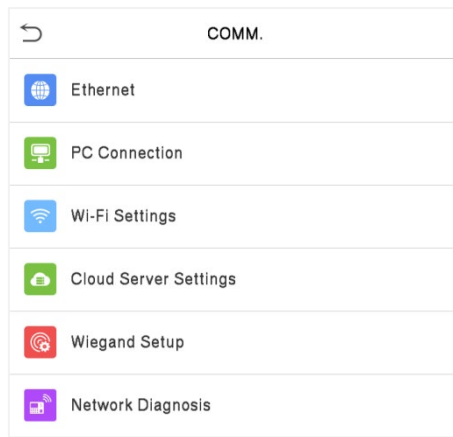
User Defined Role 1	
<input checked="" type="checkbox"/> User Mgt.	<input checked="" type="checkbox"/> New User
<input checked="" type="checkbox"/> COMM.	<input checked="" type="checkbox"/> All Users
<input checked="" type="checkbox"/> System	<input checked="" type="checkbox"/> Display Style
<input type="checkbox"/> Personalize	
<input type="checkbox"/> Data Mgt.	
<input checked="" type="checkbox"/> Access Control	
<input type="checkbox"/> Attendance Search	
<input type="checkbox"/> Autotest	
<input type="checkbox"/> System Info	

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

7 Communication Settings

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

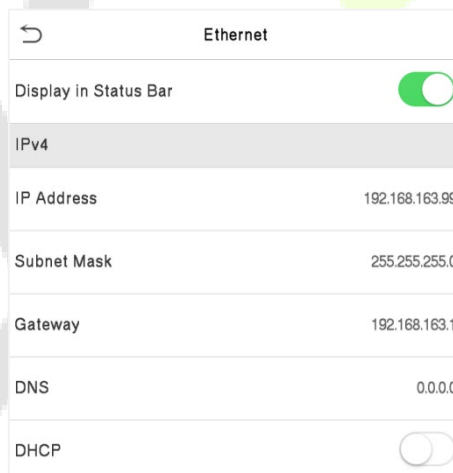
Tap [**COMM.**] on the **Main Menu**.



7.1 Network Settings

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

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



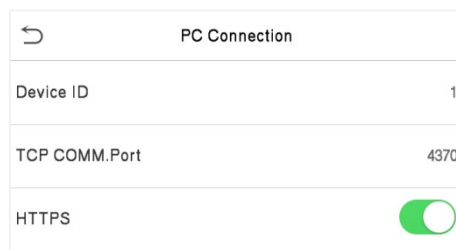
Function Name	Descriptions
Display in Status Bar	To set whether to display the network icon on the status bar.
IP Address	The factory default value is 192.168.1.201. Please set the IP Address as per the requirements.
Subnet Mask	The factory default value is 255.255.255.0. Please set the value as per the requirements.
Gateway	The factory default address is 0.0.0.0. Please set the value as per the requirements.

DNS	The factory default address is 0.0.0.0. Please set the value as per the requirements.
TCP COMM. Port	The factory default value is 4370. Please set the value as per the requirements.
DHCP	Dynamic Host Configuration Protocol, which is to dynamically allocate IP addresses for clients via server.

7.2 PC Connection

Comm Key facilitates to improve the security of data by setting 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.

Tap [**PC Connection**] on the **Comm.** Settings interface to configure the communication settings.



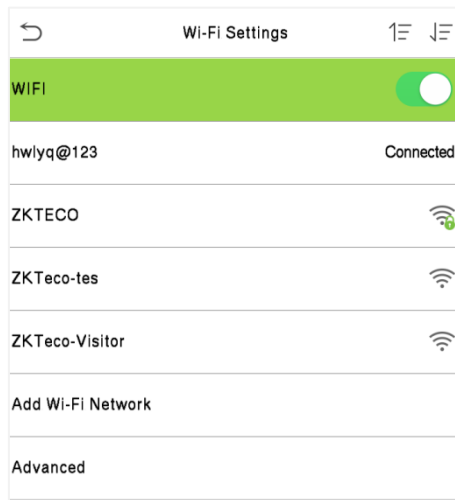
Function Name	Descriptions
Device ID	The default password is 0 and can be changed. The Comm Key can contain 1-6 digits.
TCP COMM. Port	The factory default value is 4370. Please set the value as per the requirements.
HTTPS	To increase the security of software access, users can enable the HTTPS protocol 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.

7.3 Wireless Network

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

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

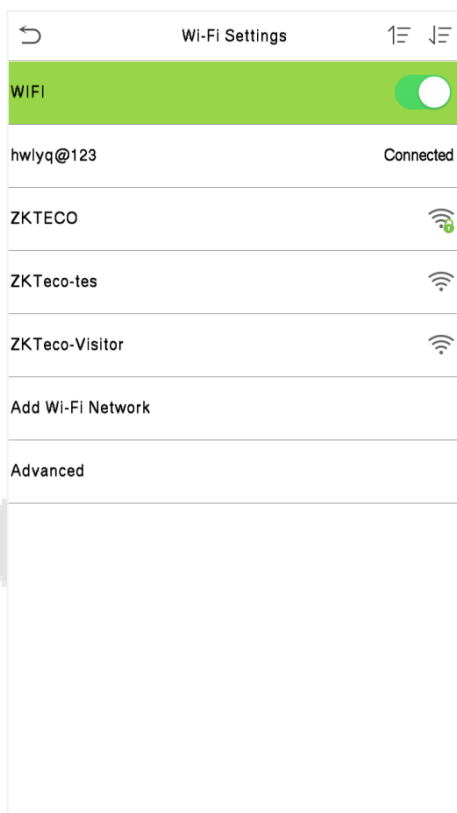
Tap [**Wi-Fi Settings**] on the **Comm.** Settings interface to configure the Wi-Fi settings.



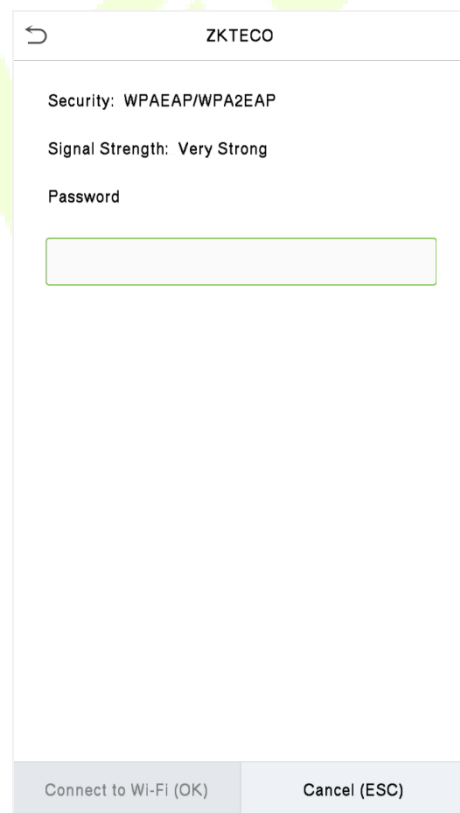
Wi-Fi is enabled in the Device by default. Toggle on  button to enable or disable Wi-Fi.

Once the Wi-Fi is turned on, the device will search for the available Wi-Fi within the network range.


Tap on the appropriate Wi-Fi name from the available list, and input the correct password in the password interface, and then tap [**Connect to Wi-Fi (OK)**].



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

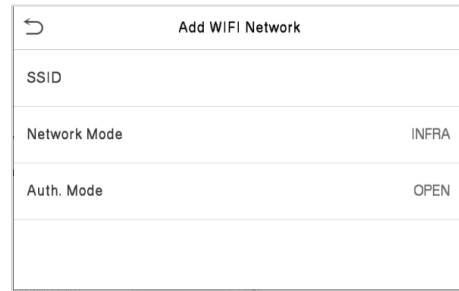
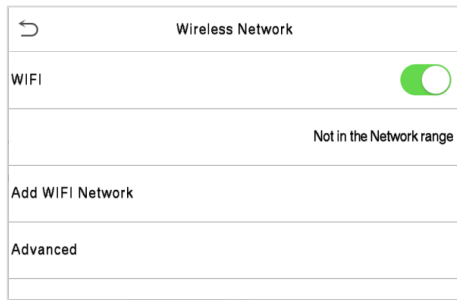


Tap on the password field to enter the password, and then tap on **Connect to Wi-Fi (OK)**.

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

● **Add Wi-Fi Network Manually**

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



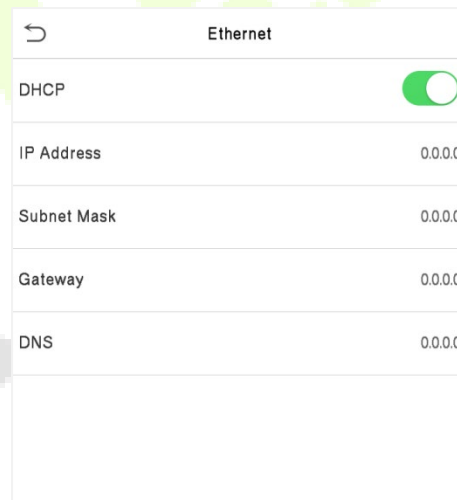
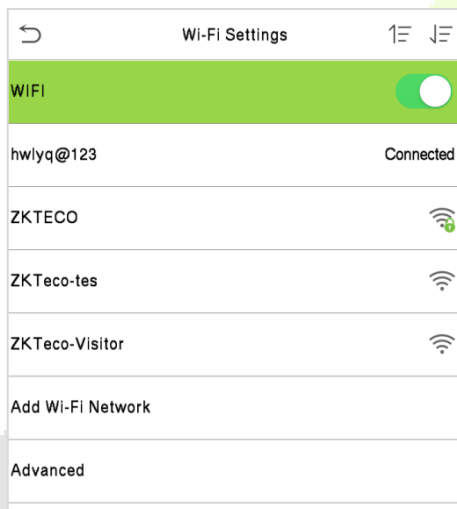
Tap on **Add WIFI Network** to add the Wi-Fi manually.

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 **Wireless Network** interface, tap on **Advanced** to set the relevant parameters as required.



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	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. 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.

7.4 Cloud Server Setting

This represents the settings used for connecting the ADMS server.

Tap [**Cloud Server Setting**] on the **Comm.** Settings interface.

Cloud Server Setting	
Server Mode	ADMS
Enable Domain Name	<input type="checkbox"/>
Server Address	192.168.163.61
Server Port	8088
Enable Proxy Server	<input type="checkbox"/>

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.

7.5 Wiegand Setup

It is used to set the Wiegand input and output parameters.

Tap [**Wiegand Setup**] on the **Comm.** Settings interface to set the Wiegand input and output parameters.

Wiegand Setup	
Wiegand Input	
Wiegand Output	

7.5.1 Wiegand Input

Wiegand Options	
Wiegand Format	
Wiegand Bits	26
Pulse Width(us)	100
Pulse Interval(us)	1000
ID Type	User ID

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

Various Common Wiegand Format Description

Wiegand Format	Description
Wiegand26	<p>ECCCCCCCCCCCCCCCCCCCCCCCCCO</p> <p>It consists of 26 bits of binary code. The 1st bit is the even parity bit of the 2nd to 13th bits, while the 26th bit is the odd parity bit of the 14th to 25th bits. The 2nd to 25th bits is the card numbers.</p>
Wiegand26a	<p>ESSSSSSSSCCCCCCCCCCCCCCCCCO</p> <p>It consists of 26 bits of binary code. The 1st bit is the even parity bit of the 2nd to 13th bits, while the 26th bit is the odd parity bit of the 14th to 25th bits. The 2nd to 9th bits is the site codes, while the 10th to 25th bits are the card numbers.</p>
Wiegand34	<p>ECCCCCCCCCCCCCCCCCCCCCCCCCCCCCO</p> <p>It consists of 34 bits of binary code. The 1st bit is the even parity bit of the 2nd to 17th bits, while the 34th bit is the odd parity bit of the 18th to 33rd bits. The 2nd to 25th bits is the card numbers.</p>
Wiegand34a	<p>ESSSSSSSSCCCCCCCCCCCCCCCCCCCCCO</p> <p>It consists of 34 bits of binary code. The 1st bit is the even parity bit of the 2nd to 17th bits, while the 34th bit is the odd parity bit of the 18th to 33rd bits. The 2nd to 9th bits is the site codes, while the 10th to 25th bits are the card numbers.</p>

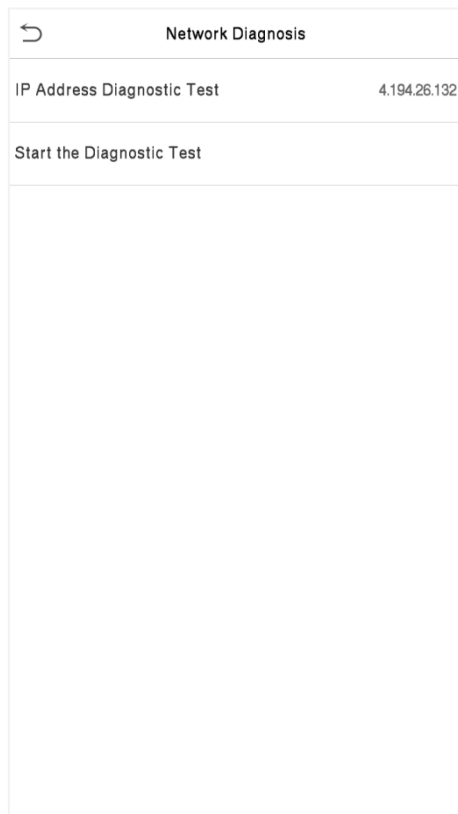
Wiegand36	<p>OFFFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCMME</p> <p>It consists of 36 bits of binary code. The 1st bit is the odd parity bit of the 2nd to 18th bits, while the 36th bit is the even parity bit of the 19th to 35th bits. The 2nd to 17th bits is the device codes. The 18th to 33rd bits is the card numbers, and the 34th to 35th bits are the manufacturer codes.</p>
Wiegand36a	<p>EEEEEEEEEEEEEEEEFFFFFFFFCCCCCCCCCCCCCCCCO</p> <p>It consists of 36 bits of binary code. The 1st bit is the even parity bit of the 2nd to 18th bits, while the 36th bit is the odd parity bit of the 19th to 35th bits. The 2nd to 19th bits is the device codes, and the 20th to 35th bits are the card numbers.</p>
Wiegand37	<p>OMMMMMSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCCCE</p> <p>It consists of 37 bits of binary code. The 1st bit is the odd parity bit of the 2nd to 18th bits, while the 37th bit is the even parity bit of the 19th to 36th bits. The 2nd to 4th bits is the manufacturer codes. The 5th to 16th bits is the site codes, and the 21st to 36th bits are the card numbers.</p>
Wiegand37a	<p>EMMMFFFFFFFFFSSSSSSCCCCCCCCCCCCCCCCCCCCCO</p> <p>It consists of 37 bits of binary code. The 1st bit is the even parity bit of the 2nd to 18th bits, while the 37th bit is the odd parity bit of the 19th to 36th bits. The 2nd to 4th bits is the manufacturer codes. The 5th to 14th bits is the device codes, and 15th to 20th bits are the site codes, and the 21st to 36th bits are the card numbers.</p>
Wiegand50	<p>ESSSSSSSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO</p> <p>It consists of 50 bits of binary code. The 1st bit is the even parity bit of the 2nd to 25th bits, while the 50th bit is the odd parity bit of the 26th to 49th bits. The 2nd to 17th bits is the site codes, and the 18th to 49th bits are the card numbers.</p>
<p>"C" denotes the card number; "E" denotes the even parity bit; "O" denotes the odd parity bit; "F" denotes the facility code; "M" denotes the manufacturer code; "P" denotes the parity bit; and "S" denotes the site code.</p>	

7.5.2 Wiegand Output

Wiegand Options	
SRB	<input type="checkbox"/>
Wiegand Format	
Wiegand Output Bits	26
Failed ID	Disabled
Site Code	Disabled
Pulse Width(us)	400
Pulse Interval(us)	2000
ID Type	Card Number

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

7.6 Network Diagnosis



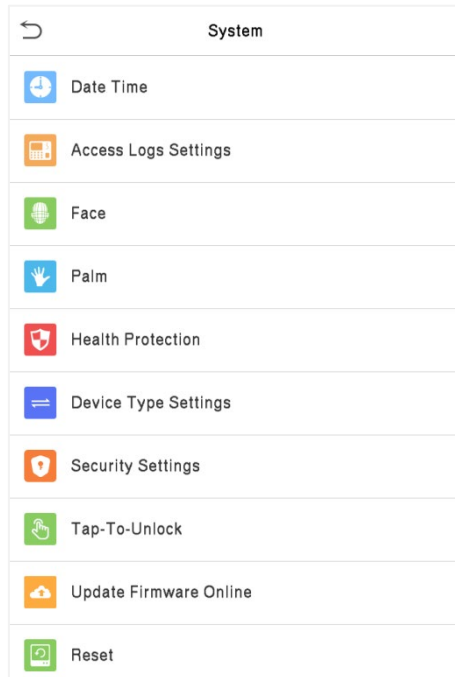
Function Name	Descriptions
IP Address Diagnostic Test	The factory default address is 0.0.0.0. Please set the value as per the requirements.
Start the Diagnostic Test	Tap start to automatically diagnose the network.

8 System Settings

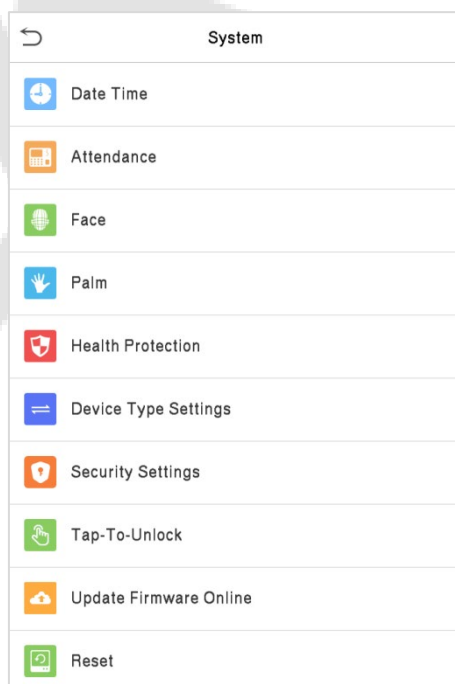
The System Settings is used to set the related system parameters to optimize the performance of the device.

Tap [**System**] on the **Main Menu** interface to get into its menu options.

Access Control Terminal:



Time Attendance Terminal:



8.1 Date and Time

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

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

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

Note: For example, the user sets the time of the device (18:35 on March 15, 2020) to 18:30 on January 1, 2021. After restoring the factory settings, the time of the device will change to 18:30, January 1, 2021.

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

Week Mode

Daylight Saving Setup	
Start Date	00-00
Start Time	00:00
End Date	00-00
End Time	00:00

Date Mode

8.2 Access Logs Setting/Attendance

Tap [Access Logs Settings] / [Attendance] on the **System** interface.

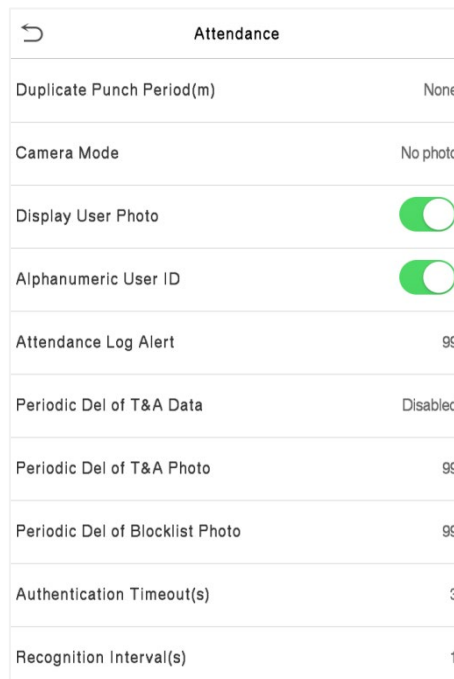
Access Control Terminal:

Access Logs Settings	
Camera Mode	No photo
Display User Photo	<input checked="" type="checkbox"/>
Alphanumeric User ID	<input checked="" type="checkbox"/>
Access Log Alert	99
Periodic Del of Access Logs	Disabled
Periodic Del of T&A Photo	99
Periodic Del of Blocklist Photo	99
Authentication Timeout(s)	3
Recognition Interval(s)	1

Function 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>
Display User Photo	This function is disabled by default. When enabled, a security prompt will pop-up.
Alphanumeric User ID	Enable/Disable the alphanumeric as User ID.
Access Log Alert	When the record space of the attendance access reaches the maximum threshold value, the device automatically displays the memory space warning. Users may disable the function or set a valid value between 1 and 9999.
Periodic Del of Access Logs	When access logs reach its maximum capacity, the device automatically deletes a set of old access logs. Users may disable the function or set a valid value between 1 and 999.
Periodic Del of T&A Photo	When attendance photos reach its maximum capacity, the device automatically deletes a set of old attendance photos. Users may disable the function or set a valid value between 1 and 99.

Periodic Del of Blocklist Photo	When block listed photos reach its maximum capacity, the device automatically deletes a set of old block listed photos. Users may disable the function or set a valid value between 1 and 99.
Authentication Timeout (s)	The amount of time taken to display a successful verification message. Valid value: 1~9 seconds.
Recognition Interval(s)	The amount of time required to compare facial templates. Valid value: 0~9 seconds.

Time Attendance Terminal:



Attendance	
Duplicate Punch Period(m)	None
Camera Mode	No photo
Display User Photo	<input checked="" type="checkbox"/>
Alphanumeric User ID	<input checked="" type="checkbox"/>
Attendance Log Alert	99
Periodic Del of T&A Data	Disabled
Periodic Del of T&A Photo	99
Periodic Del of Blocklist Photo	99
Authentication Timeout(s)	3
Recognition Interval(s)	1

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

Attendance Log Alert	When the record space of the attendance reaches the maximum threshold value, the device automatically displays the memory space warning. Users may disable the function or set a valid value between 1 and 9999.
Periodic Del of T&A Data	When attendance records reach its maximum storage capacity, the device automatically deletes a set of old attendance records. Users may disable the function or set a valid value between 1 and 999.
Periodic Del of T&A Photo	When attendance photos reach its maximum storage capacity, the device automatically deletes a set of old attendance photos. Users may disable the function or set a valid value between 1 and 99.
Periodic Del of Blocklist Photo	When blocklisted photos reach its maximum storage capacity, the device automatically deletes a set of old block listed photos. Users may disable the function or set a valid value between 1 and 99.
Authentication Timeout(s)	The amount of time taken to display a successful verification message. Valid value: 1~9 seconds.
Recognition Interval(s)	After the interval identifying is clicked (selected), for example, if the comparison interval is set to 5 seconds, then the face recognition will verify the face every 5 seconds. Valid value: 0 to 9 seconds. 0 means continuous identifying, 1 to 9 means identifying at intervals.

8.3 Face Parameters

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

Parameter	Value
1:N Threshold	72
1:N Match Threshold for Masked People	68
1:1 Threshold	70
Face Enrollment Threshold	70
Image Quality	40
Facial Recognition Distance	Far
LED Light Trigger Value	80
Live Detection	<input checked="" type="checkbox"/>
Live Detection Threshold	70
Anti-spoofing Using NIR	<input checked="" type="checkbox"/>
Binocular Live Detection Threshold	75
Face AE	<input checked="" type="checkbox"/>
WDR	<input type="checkbox"/>
Anti-flicker Mode	50Hz
Face Algorithm	

Function Name	Description
1:N Threshold	<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 72.</p>
1:1 Match Threshold of Masked People	<p>During face enrolment, 1: N comparison is used to determine 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>
1:1 Threshold	<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 70.</p>
Face Enrollment Threshold	<p>During face enrollment, 1:N comparison is used to determine 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.
Facial Recognition Distance	Face template recognition of the maximum distance, greater than this value will be filtered. The parameter value can be understood as the face template size required for registration and comparison. The farther the distance from people, the smaller the face template pixels obtained by the algorithm. When the value is 0, it means that the face template comparison distance is not limited.
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.
Live Detection	It detects the spoof attempt using visible light images to determine if the provided biometric source sample is of a real person (a live human being) or a false representation.
Live Detection Threshold	It facilitates judging whether the captured visible image is a real person (a live human being). The larger the value, the better the anti-spoofing performance using visible light.
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 the 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 facial template update.

Note: Improper adjustment of the exposure and quality parameters may severely affect the performance of the device. Please adjust the exposure parameter only under the guidance of the after-sales service personnel of our company.

- **Process to modify the Face Recognition Accuracy**
- On the **System** interface, tap on **[Face]** and then toggle to enable **[Anti-Spoofing using NIR]** to set the anti-spoofing.
- Then, on the **Main Menu**, tap **[Autotest] > [Test Face]** and perform the face test.
- Tap three times for the scores on the right upper corner of the screen, and the red rectangular box appears to start adjusting the mode.
- Keep one arm distance between the device and the face. It is recommended not to move the face in a wide range.

8.4 Palm Parameters

Tap **[Palm]** on the **System** interface.

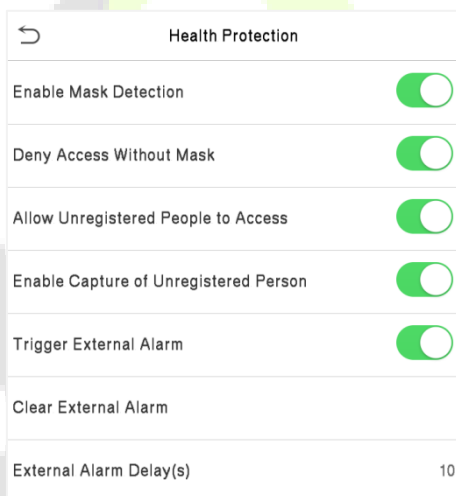
Palm	
Palm 1:1 Matching Threshold	46
Palm 1:N Matching Threshold	50
Image Quality	60
Palm AE	<input checked="" type="checkbox"/>
Anti-Spoofing for Palm	<input checked="" type="checkbox"/>
Palm Anti-Spoofing Threshold	70
Recognition Interval(s)	0

Function Name	Descriptions
Palm 1:1 Matching Threshold	In 1:1 Verification Method, only when the similarity between the verifying palm and the user's registered palm is greater than this value can the verification succeed.

Palm 1:N Matching Threshold	In 1: N Verification Method, only when the similarity between the verifying palm and all the registered palm is greater than this value can the verification succeed.
Image Quality	Image quality for palm registration and comparison. The higher the value, the clearer the image requires.
Palm AE	When the palm is in front of the camera in Palm AE mode, the brightness of the palm area increases, while other areas become darker.
Anti-Spoofing for palm	Using near-infrared spectra imaging to identify and prevent fake photos and videos attack.
Palm Anti-Spoofing 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.
Recognition Interval(s)	After the interval identifying is clicked (selected), for example, if the comparison interval is set to 5 seconds, then the palm recognition will verify the palm every 5 seconds. Valid value: 0 to 9 seconds. 0 means continuous identifying, 1 to 9 means identifying at intervals.

8.5 Health Protection

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

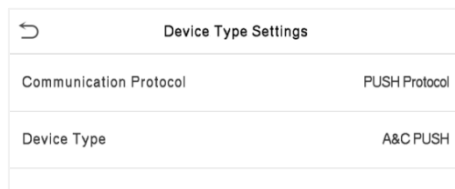


Function Name	Descriptions
Enable Mask Detection	It enables or disables the mask detection function. When enabled, the device identifies whether the user is wearing a mask or not during verification.
Deny Access Without Mask	It enables or disables the access of a person without a mask. When enabled, the device denies access of a person, if not wearing a mask.
Allow Unregistered People to Access	It enables or disables the access of an unregistered person. When enabled, the device allows the person to enter without registration.
Enable Capture of Unregistered	To enable or disable capturing the unregistered person. When enabled, the device will automatically capture the photo of the unregistered

Person	person, enabling this feature requires to enable Allow Unregistered People to Access .
Trigger External Alarm	When enabled, if the user is not wearing a mask, the system will trigger an alarm.
Clear External Alarm	It clears the triggered alarm records of the device.
External Alarm Delay(s)	It is the delay(s) time for triggering an external alarm. It can be set in seconds. Users may disable the function or set a value between 1 to 255.

8.6 Device Type Settings

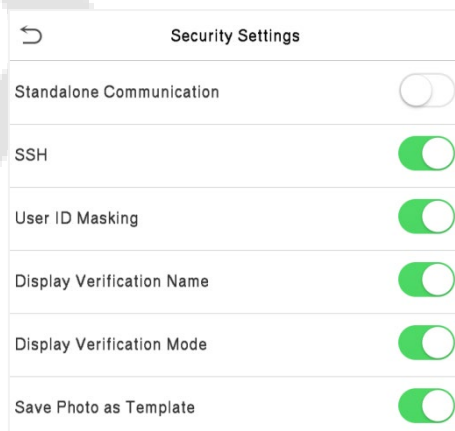
Tap **[Device Type Settings]** on the **System** interface to configure the Device Type Setting settings.



Function Name	Descriptions
Communication Protocol	Set the PUSH protocol.
Device Type	Set the device as an access control terminal or attendance terminal.

8.7 Security Settings

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



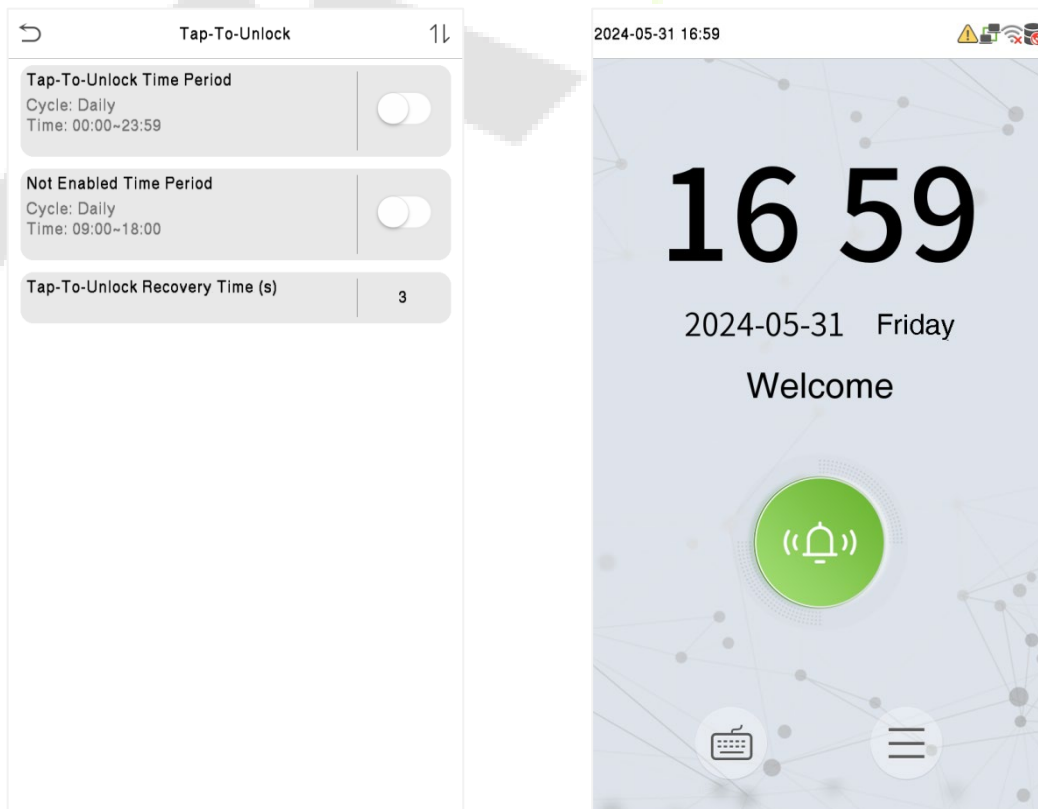
Function Name	Description
Standalone Communication	By default, this function is disabled. This function can be enabled or disabled via the menu interface. When it is switched on, a security prompt appears, and the device will restart after you confirm.

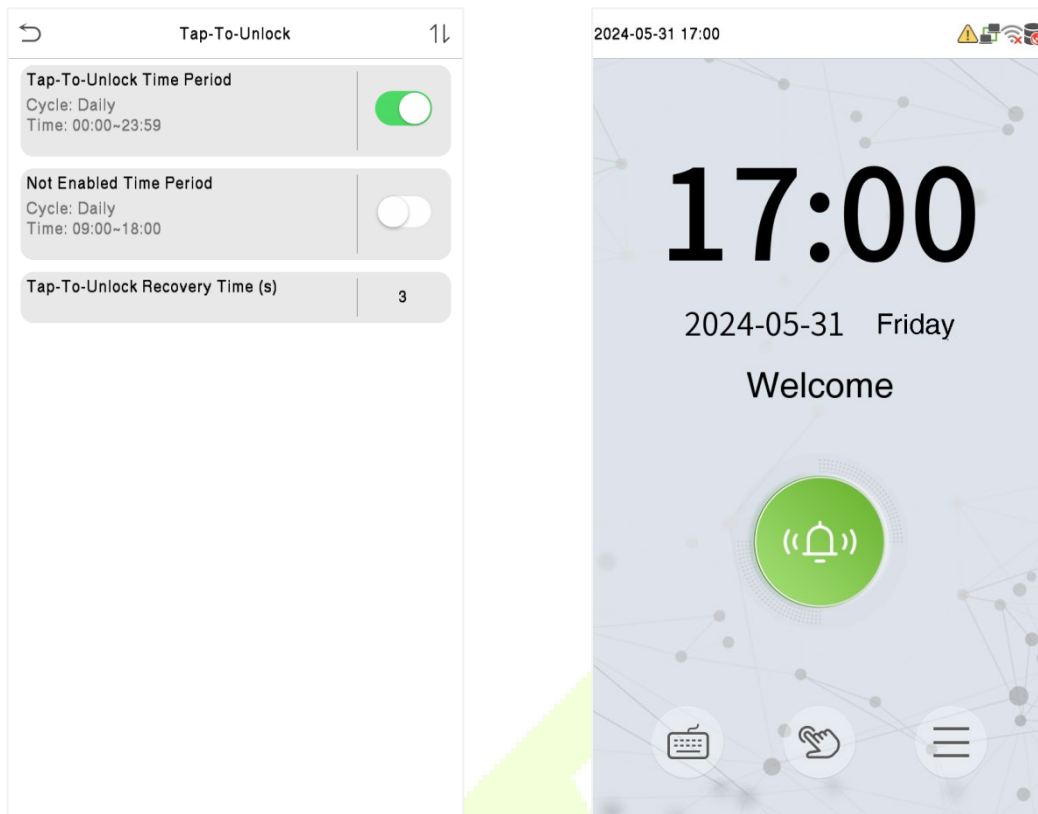
SSH	The device does not support the Telnet feature, hence SSH is typically used for remote debugging. By default, SSH is enabled. The menu interface allows you to enable and disable SSH. When enabled, there will be a security prompt, but the device will not need to be restarted after confirmation.
User ID Masking	After enabled, the User ID will be partially displayed after the personnel verification result (only the User ID with more than 2 digits supports the masking display), and it is enabled by default.
Display Verification Name	After enabled, the user's name will be displayed after the personnel verification result. The verification result will not show the name after disabling it.
Display Verification Mode	After enabled, the personnel verification result will show the user's verification mode. The verification result will not show the verification mode after you disable it.
Save Photo as Template	After disable this function, face re-registration is required after an algorithm upgrade.

8.8 Tap-To Unlock

Enable **Tap-To-Unlock**, and it will take effect after the device restarts. Once enabled, the camera's auto-identification sensing function will be disabled. Only touching the device screen can wake up the camera for auto-identification.

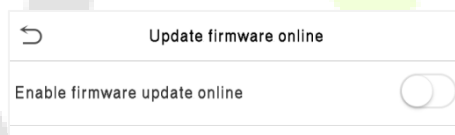
Tap [**Tap-To-Unlock**] on the **System** interface to enable this function.



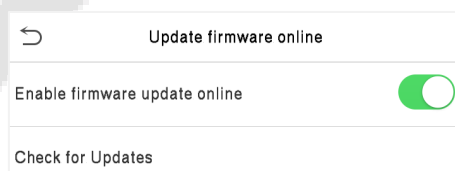


8.9 Update Firmware Online

Tap [**Update Firmware Online**] on the **System** interface.



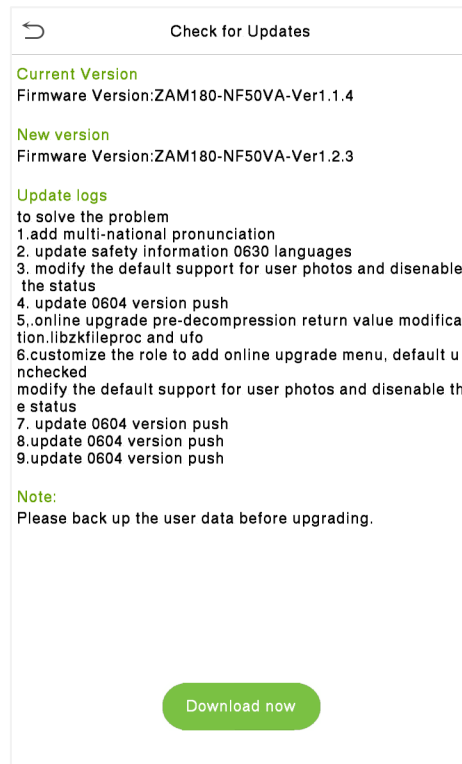
Tap [**Enable firmware Update Online**] function, the device will prompt that the update may bring some data security risks, which requires manual confirmation by the user (If the security setting function is turned off, the risk warning will not be displayed when the online update is turned on).



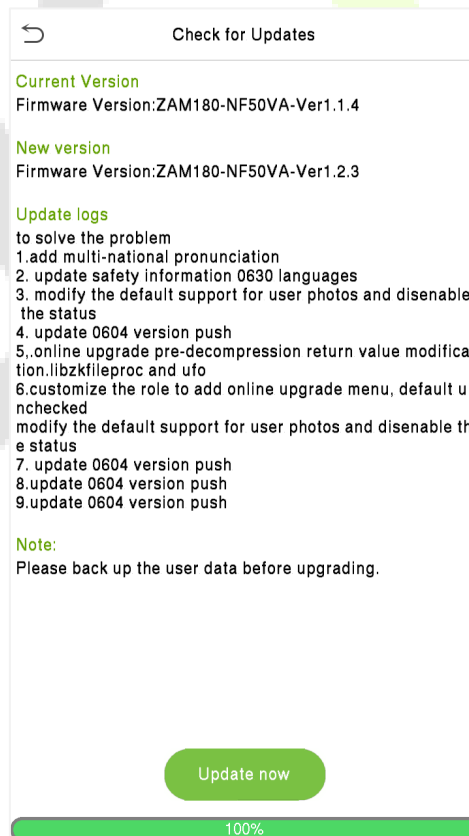
Tap [**Check for Updates**] it may have the following 3 scenarios:

- 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.

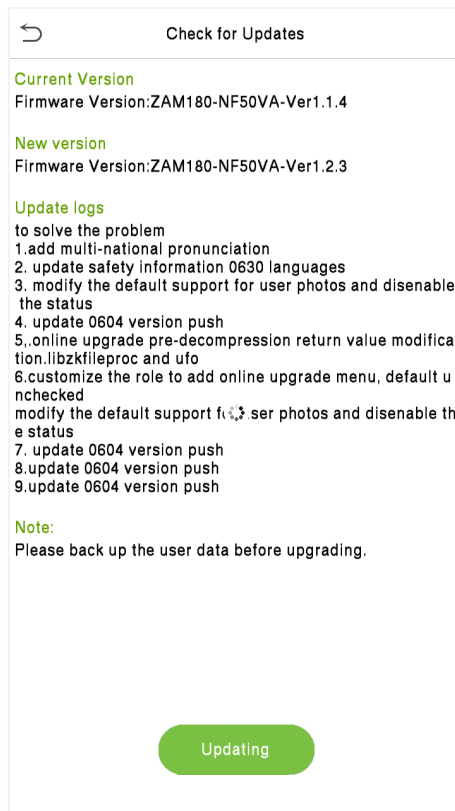
1. Tap [**Download now**] to start the download. After the download is complete, you can choose whether to update immediately.



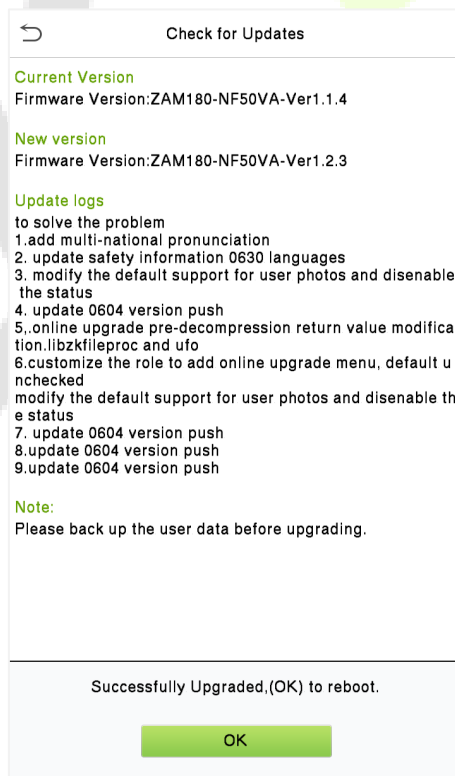
2. During the download process, you can press the back button to go to other menus, and then return to this menu to update after the download is complete.



3. The download speed is related to the user's network environment, and it may take about 10 minutes to complete the download. The update may take about 3 minutes.



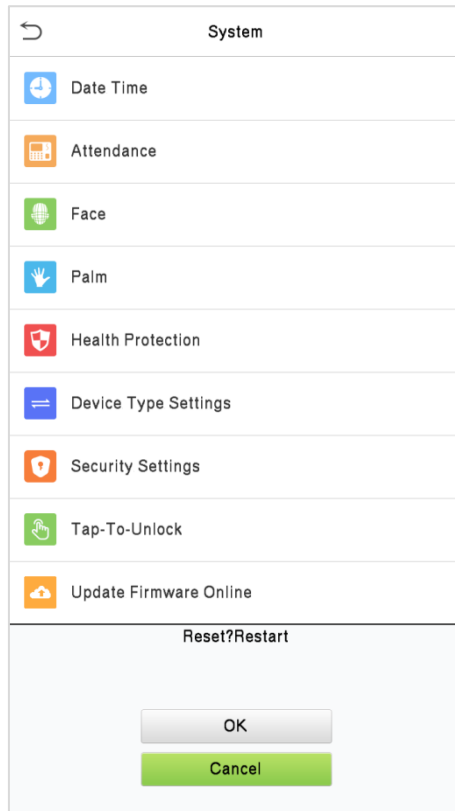
4. After the update is complete, the device will prompt to restart. After restarting, you can enter the **System Information** to view the latest firmware version after the update.



8.10 Factory Reset

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

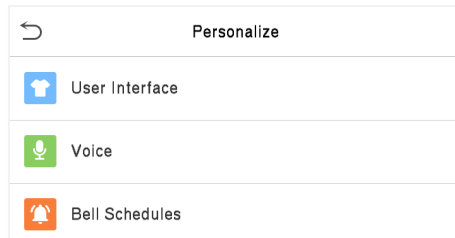
Tap [**Reset**] on the **System** interface and then tap [**OK**] to restore the default factory settings.



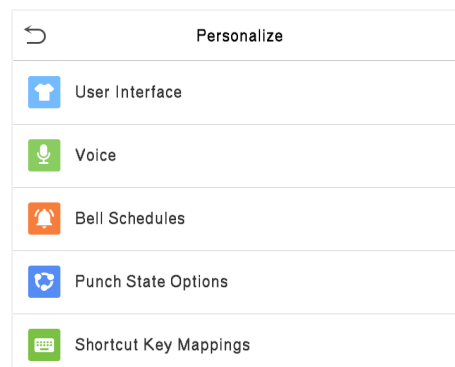
9 Personalize Settings

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

Access Control Terminal:

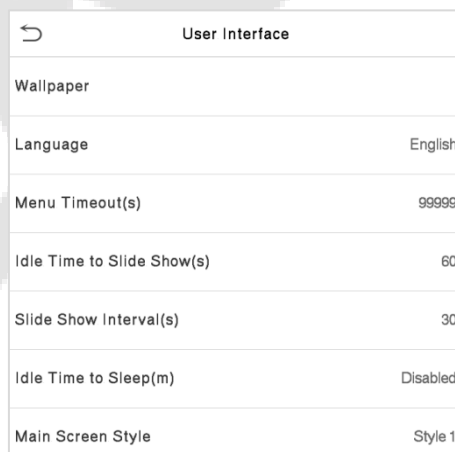


Time Attendance Terminal:



9.1 Interface Settings

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

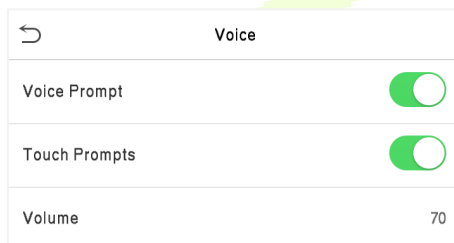


Function Name	Description
Wallpaper	It helps to select the main screen wallpaper according to the user preference.
Language	It helps to select the language of the device.
Menu Timeout(s)	When there is no operation, and the time exceeds the set value, the device automatically goes back to the initial 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 1-999 minutes.
Main Screen Style	The style of the main screen can be selected according to the user preference.

9.2 Voice Settings

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



Function Name	Description
Voice Prompt	Select whether to enable voice prompts during operating.
Touch Prompt	Select whether to enable keypad sounds.
Volume	Adjust the volume of the device; valid value: 0-100.

9.3 Bell Schedules

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



● New Bell Schedule

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

New Bell Schedule	
Bell Status	<input type="checkbox"/>
Bell Time	
Repeat	Never
Ring Tone	bell01.wav
Internal bell delay(s)	5

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**

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

9.4 Punch States Options

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

Note: This function only for Time Attendance Terminal.

Punch State Options	
Punch State Mode	Manual Mode
Punch State Timeout(s)	10
Punch State Required	<input type="checkbox"/>

Function Name	Description
Punch State Mode	<p>Select a punch state mode, which can be:</p> <p>Off: It disables the punch state function. And the punch state key set under the Shortcut Key Mappings menu becomes 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 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 an alternative that is the manual attendance status. After the timeout, the manual switching punch state key will become an 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 manually switched again.</p> <p>Fixed Mode: Only the manually fixed punch state key is shown. Users cannot change the status by pressing any other keys.</p>
Punch State Timeout (s)	It is the amount of time for which the punch state is displayed. The value ranges from 5~999 seconds.
Punch State Required	To choose whether an attendance state needs to be selected during verification.

9.5 Shortcut Keys Mappings

Users may define shortcut keys for attendance status and functional keys on the main interface. So, on the main interface, when the shortcut keys are pressed, the corresponding attendance status or the function interface displays directly. **Note:** This function only for Time Attendance Terminal.

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

Shortcut Key Mappings	
F1	Check-In
F2	Check-Out
F3	Break-Out
F4	Break-In
F5	Overtime-In
F6	Overtime-Out

- On the **Shortcut Key Mappings** interface, tap on the required shortcut key to configure the shortcut key settings.

- On the **Shortcut Key** ("F1") interface, tap **function** to set the functional process of the shortcut key either as punch state key or function key.
- If the Shortcut key is defined as a function key (such as New user, All users, etc.), the configuration is done as shown in the image below.

F3	
Punch State Value	2
Function	Punch State Options
Name	Break-Out
Set Switch Time	

F1	
Function	New User

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

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.

Set Switch Time	
Switch Cycle	Never

Switch Cycle	
<input checked="" type="checkbox"/>	Monday
<input checked="" type="checkbox"/>	Tuesday
<input checked="" type="checkbox"/>	Wednesday
<input checked="" type="checkbox"/>	Thursday
<input checked="" type="checkbox"/>	Friday
<input checked="" type="checkbox"/>	Saturday
<input checked="" type="checkbox"/>	Sunday

10 Data Management

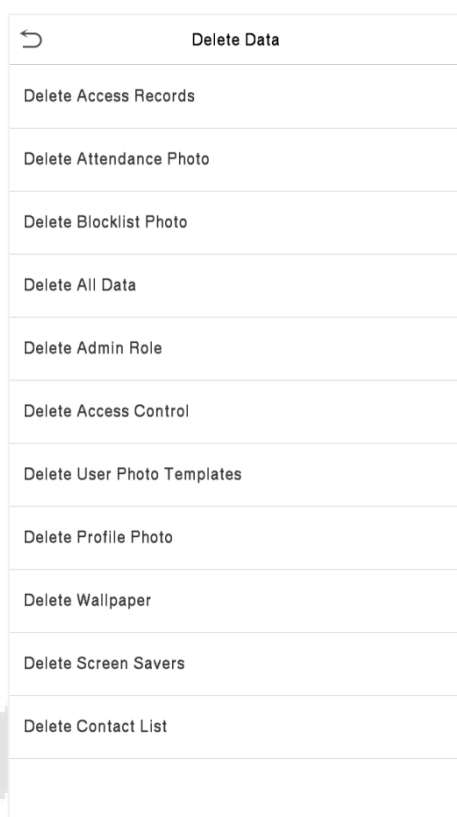
On the **Main Menu**, tap [**Data Mgt.**] to delete the relevant data in the device.



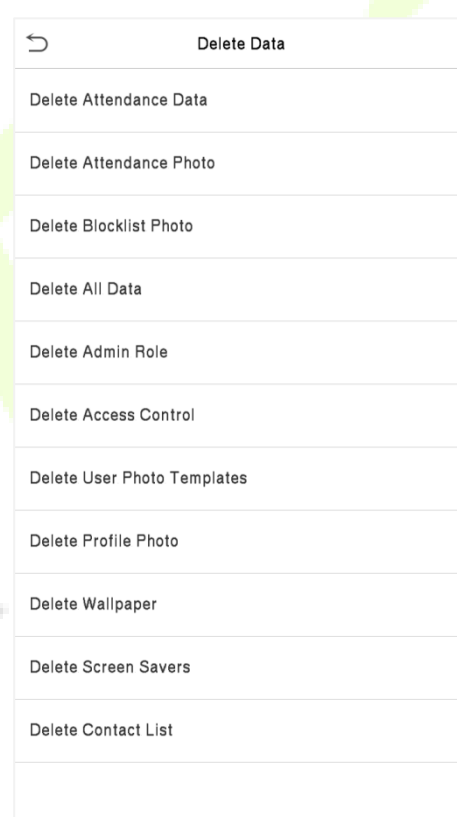
10.1 Delete Data

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

Access Control Terminal:



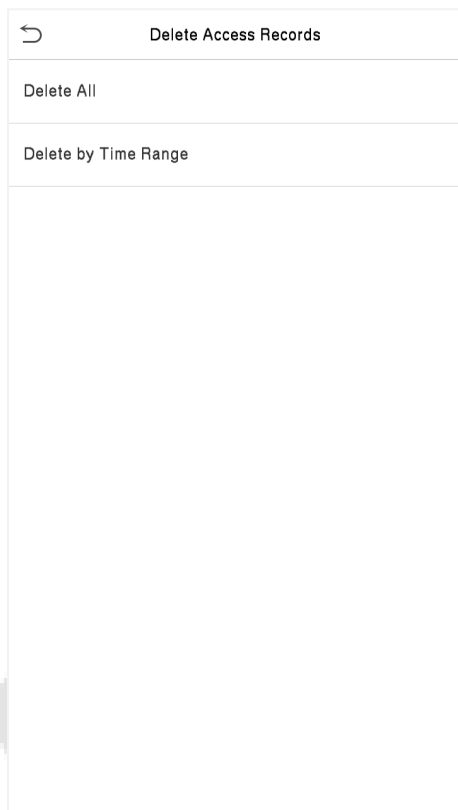
Time Attendance Terminal:



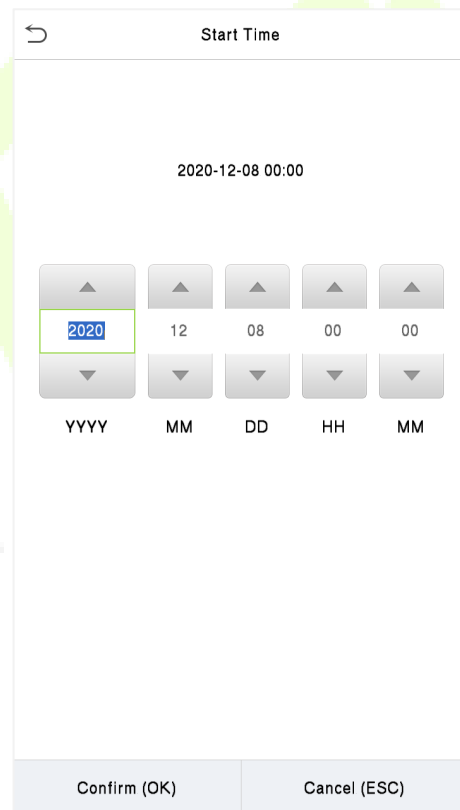
Function Name	Description
Delete Access Records / Delete Attendance Data	To delete attendance data/access records conditionally.
Delete Attendance Photo	To delete attendance photos of designated personnel.
Delete Blocklist Photo	To delete the photos taken during failed verifications.
Delete All Data	To delete information and attendance logs/access records of all registered users.
Delete Admin Role	To remove all administrator privileges.
Delete Access Control	To delete all 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 user photos in the device.
Delete Wallpaper	To delete all wallpapers in the device.
Delete Screen Savers	To delete the screen savers in the device.
Delete Contact List	To delete the contact list in the device.

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



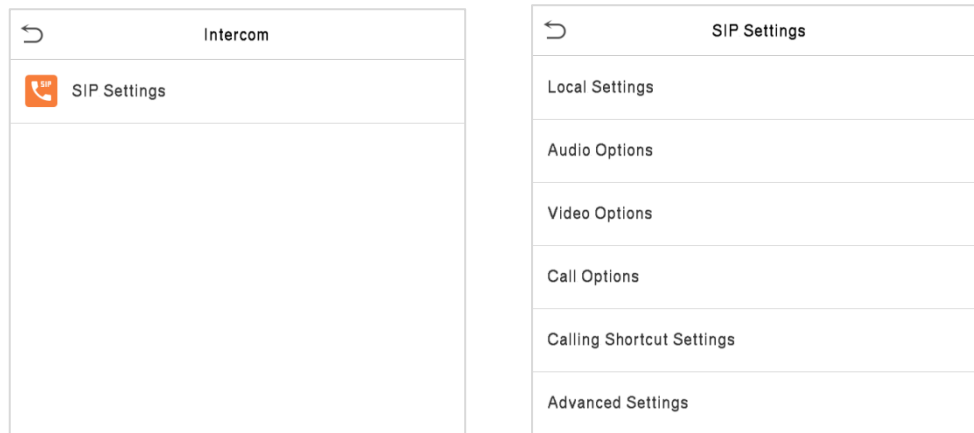
Select Delete by Time Range





Set the time range and tap [**OK**]

11 Intercom

Tap **[Intercom]** on the **Main Menu** interface to get into its menu options.



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. STUN Server: Set up STUN server docking. 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 the LAN for visual intercom, enter the network port number of the LAN.
	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.

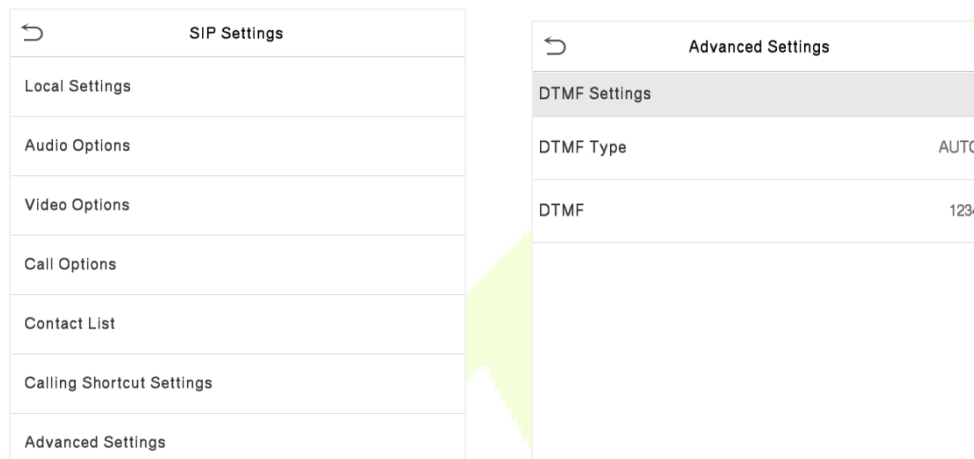
Audio Options	Select the audio encoder for intercom. Both PCMU and PCMA provide better voice quality, but they take up more bandwidth, requiring 64kbps.
Video Options	<p>General</p> <p>Video Resolution: Select the video resolution of the intercom.</p> <p>Video Code Stream: Select the video code stream of the intercom, the larger the value, the higher the picture and sound quality of the video, and the greater the network requirements.</p> <p>Video Frame Rate: Refers to the number of frames per second of the intercom video display, the larger the value the smoother, the device defaults to 25Hz, does not support modification.</p>
	<p>Encoder</p> <p>Whether to enable H264 Encoder.</p>
Call Options	<p>Calling Delay(s)</p> <p>Set the time of call, valid value 30 to 60 seconds.</p>
	<p>Talking Delay(s)</p> <p>Set the time of intercom, valid value 60 to 120 seconds.</p>
	<p>Call Volume Settings</p> <p>Adjust the volume of the intercom; valid value: 0-100.</p>
	<p>Call Type</p> <p>Set the call type to Voice only or Voice+Video.</p>
	<p>Call Button Style</p> <p>Change the visual intercom call button on the standby interface of the device, optional doorbell label  or phone label .</p>
	<p>Auto Answer Settings</p> <p>When the indoor unit dials the device successfully, it is automatically connected within the set answer time.</p>
	<p>Verification Timeout</p> <p>Sets the verification timeout for intercom, valid values are 1 to 60 seconds.</p>
	<p>Encryption</p> <p>Whether to enable intercom call encryption function.</p>
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	<p>Set the quick call shortcuts in the call interface of visual intercom, the system defaults 5 shortcuts, including a management center and 4 customizable shortcuts. After enabling the shortcuts, customize the name, enter the device number set in the Contact List, then automatically match the IP address, after the operation is completed, then click on the generated customized name (shortcut) in the call interface of the visual intercom to call directly.</p> <p>Support standard mode and direct calling mode, in direct calling mode, users can call multiple indoor units at the same time.</p> <p>Note: When the SIP server is enabled, Direct Calling Mode can only call the Management Center</p>
Advanced Settings	Set the DTMF type and DTMF value of the device, the value should be set to the same as the DTMF value of the indoor unit.

The SpeedPalm-V5L and the indoor station to achieve video intercom there are two modes, respectively, the LAN and SIP server.

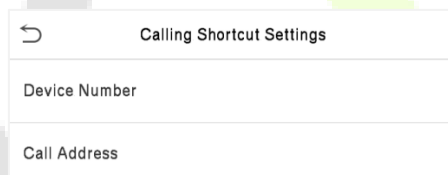
11.1.1 Local Area Network Use

- **Enter the IP Address/Device Number of the Indoor Station**

1. Set the indoor station to the same network segment as the device.
2. On the **SIP Settings** interface, tap on [**Advanced Settings**] > [**Dtmf**] to set the value as same as the value of DTMF in the indoor station.




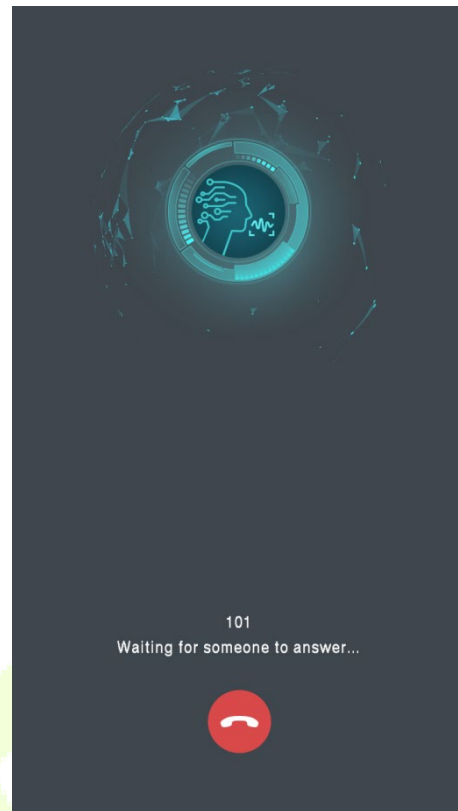
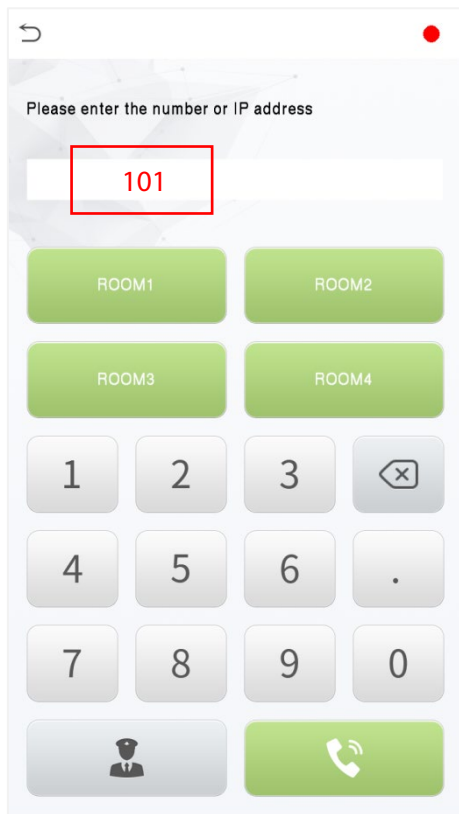
3. On the **SIP Settings** interface, tap on [**Contact List**] > [**Add**] to add the connected indoor station.



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.

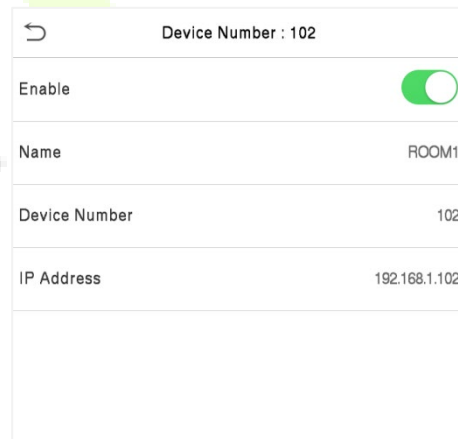
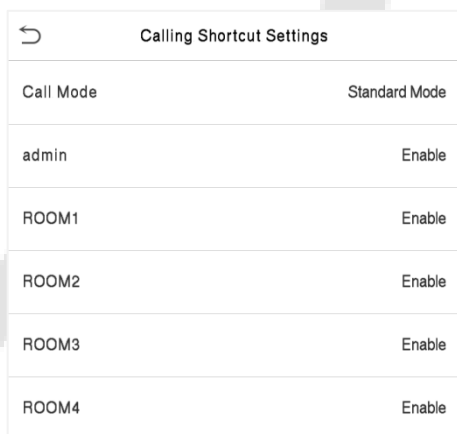
Call Address: It is the IP Address of the indoor station.

4. To enable the video intercom function, tap the  icon on the SpeedPalm-V5L and enter the IP address or device number of the indoor station in the provided interface.



- **Custom the Calling Shortcut Keys**


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

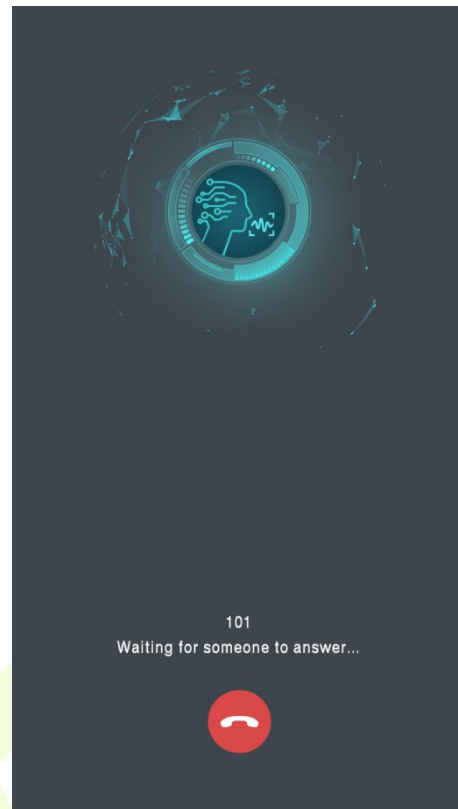
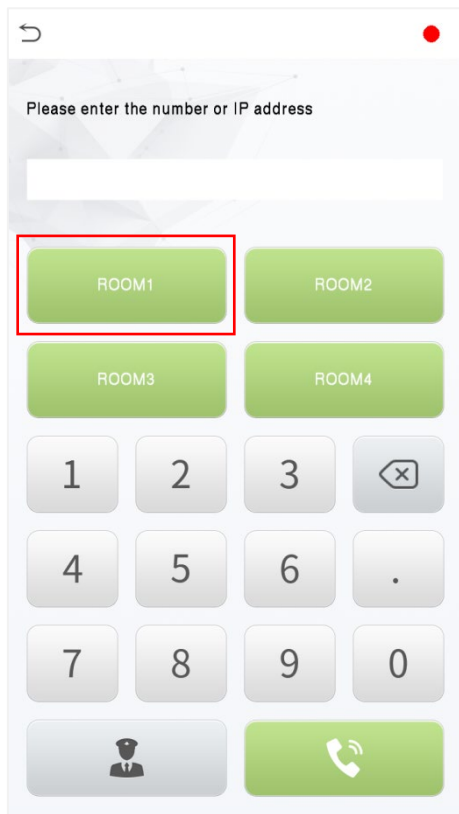


Name: Customize the name of the shortcut keys.

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

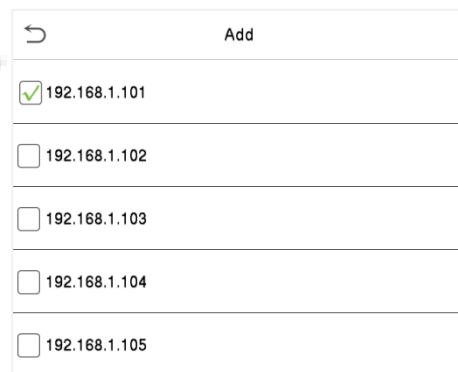
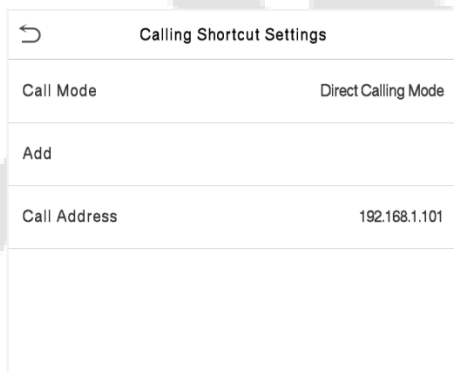
IP Address: Once the device number is set, it will be automatically displayed.

2. Then you can tap the  icon on the SpeedPalm-V5L and tap the calling shortcut keys to call the indoor station.

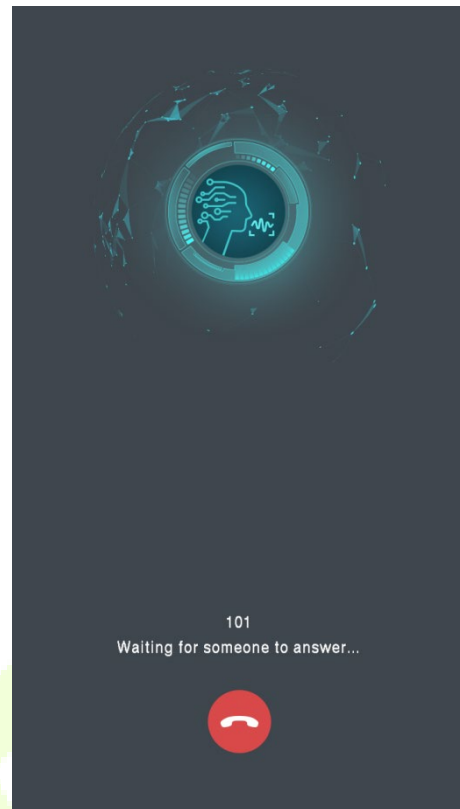
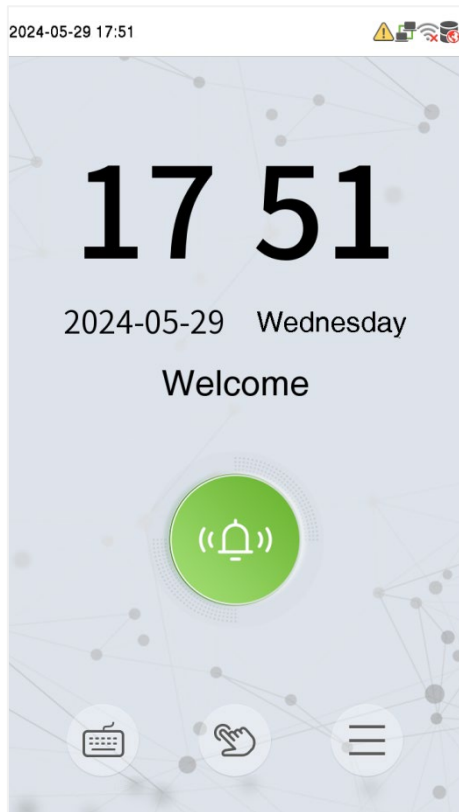


● Direct Calling

1. On the **SIP Settings** interface, tap on [**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.

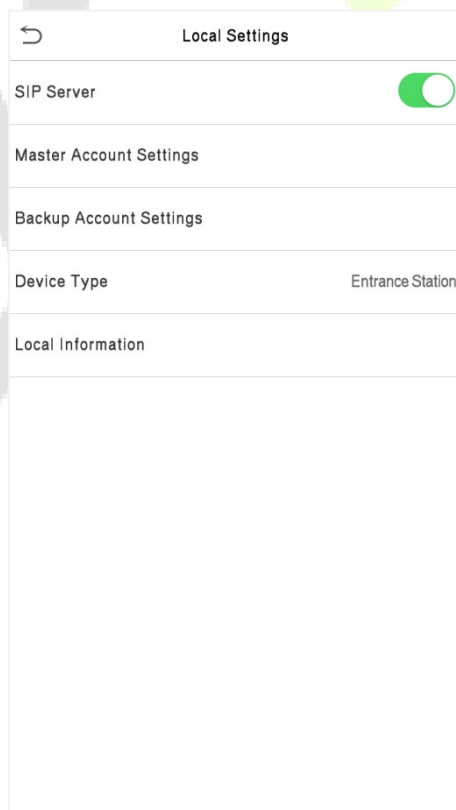


2. Then you can tap the  icon on the SpeedPalm-V5L to call the indoor stations at the same time.



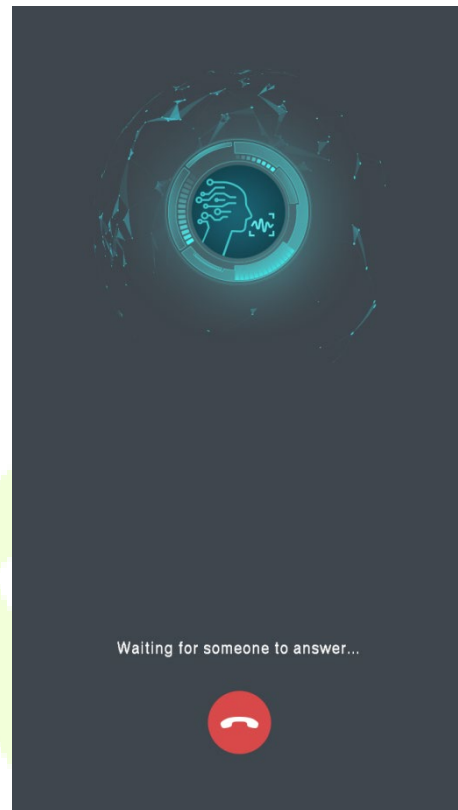
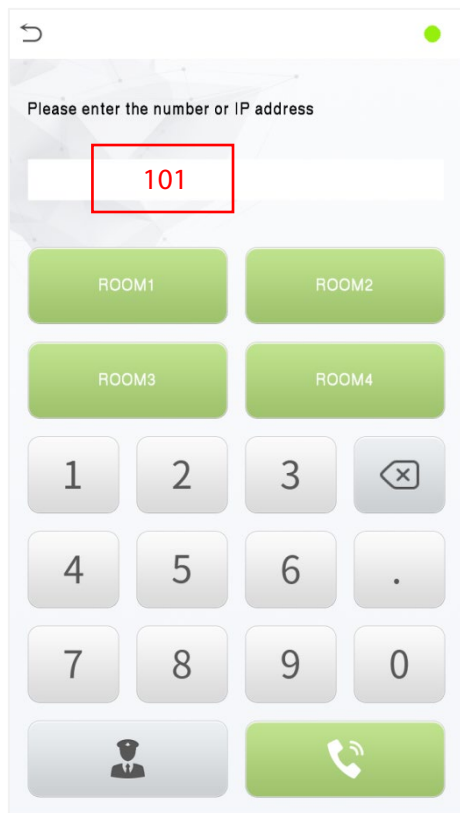
11.1.2 SIP Server

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



- After correctly setting up the SIP, a green dot will appear in the upper right corner of the call page, indicating that the SpeedPalm-V5L is connected to the server. You can then initiate a call to the account name of the indoor station."

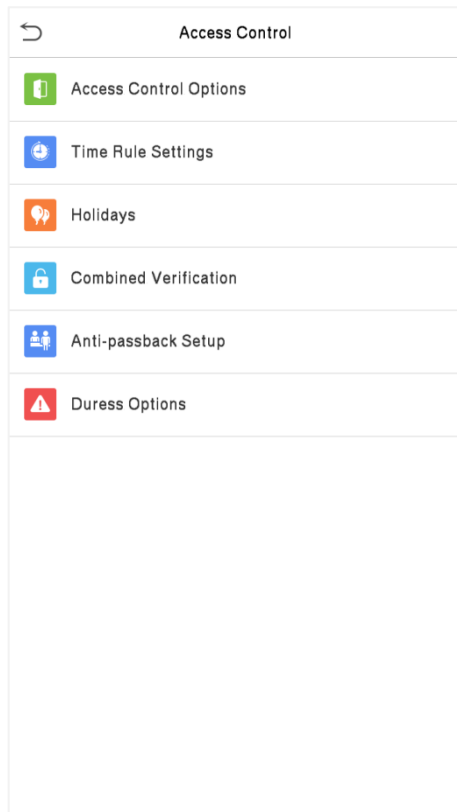
Note: Customers create their own SIP server.



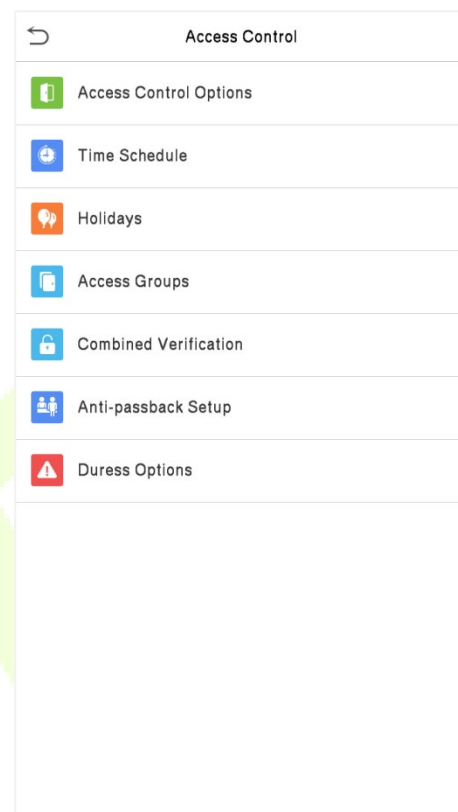
12 Access Control

On the **Main Menu**, tap [**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:



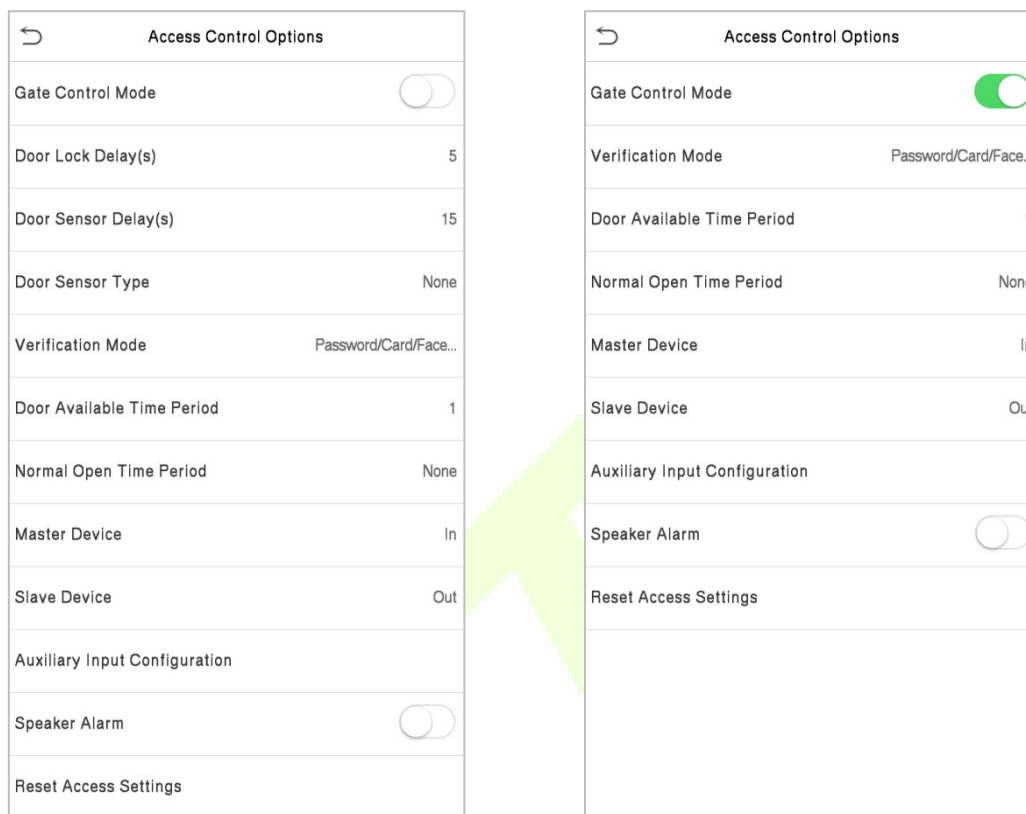
To gain access, the registered user must meet the following conditions:

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

12.1 Access Control Options

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

Access Control 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 relay, Door sensor relay, 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; 0 seconds represents disabling the function.
Door Sensor Delay (s)	If the door is not locked and is left open for a certain duration (Door Sensor Delay), an alarm will be triggered. The valid value of Door Sensor Delay ranges from 1 to 255 seconds.
Door Sensor Type	There are three Sensor types: None , Normal Open(NO) , and Normal Closed(NC) . None : It means the door sensor is not in use. Normally Open(NO) : It means the door is always left open when electric power is on. Normally Closed(NC) : It means the door is always left closed when electric power is on.
Verification Mode	The supported verification mode includes Password/Card/Face/Palm, User ID Only, Password, Card Only, Password+Card, Password/Card, Face Only, Face+Password, Face+Card, Palm, Palm+Card, Palm+Face.

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.
Master Device	While configuring the master and slave devices, you may set the state of the master as Out or In . Out: A record of verification on the master device is a check-out record. In: A record of verification on the master device is a check-in record.
Slave Device	While configuring the master and slave devices, you may set the state of the slave as Out or In . Out: A record of verification on the slave device is a check-out record. In: A record of verification on the slave device is a check-in record.
Auxiliary Input Configuration	Sets the door unlock time period and auxiliary output type of the auxiliary terminal device. Auxiliary output types include None, Trigger door open, Trigger Alarm, Trigger door open and Alarm.
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, master device, and alarm. However, erased access control data in Data Mgt. is excluded.

Time Attendance Terminal:

←
Access Control Options

Door Lock Delay(s)	10
Door Sensor Delay(s)	10
Door Sensor Type	Normal Close(NC)
Door Alarm Delay(s)	30
Retry Times to Alarm	3
Normal Close Time Period	None
Normal Open Time Period	None
Auxiliary Input Configuration	
Valid Holidays	<input checked="" type="checkbox"/>
Speaker Alarm	<input type="checkbox"/>
Reset Access Settings	

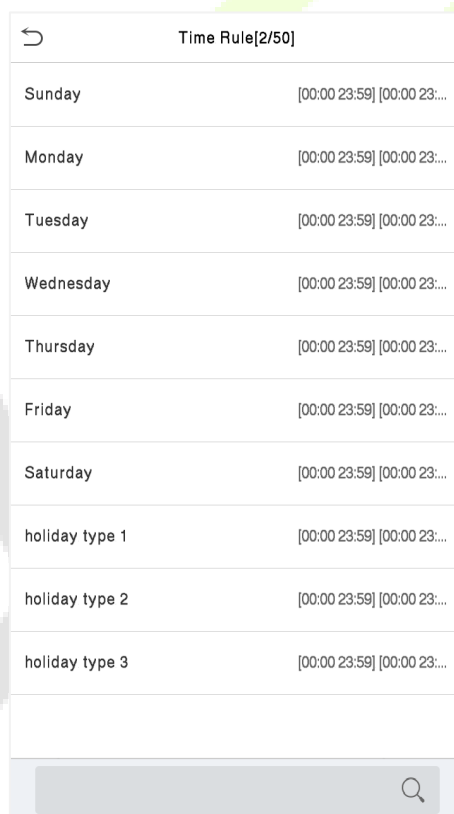
Function Name	Description
Door Lock Delay (s)	The length of time that the device controls the electric lock to be in unlock state. Valid value: 1~10 seconds; 0 seconds represents disabling the function.
Door Sensor Delay (s)	If the door is not locked and is left open for a certain duration (Door Sensor Delay), an alarm will be triggered. The valid value of Door Sensor Delay ranges from 1 to 255 seconds.
Door Sensor Type	There are three Sensor types: None , Normal Open(NO) , and Normal Closed(NC) . None: It means the door sensor is not in use. Normally Open(NO): It means the door is always left open when electric power is on. Normally Closed(NC): It means the door is always left closed when electric power is on.
Door Alarm Delay(s)	When the state of the door sensor is inconsistent with that of the door sensor type, alarm will be triggered after a time period; this time period is the Door Alarm Delay (the value ranges from 1 to 999 seconds).
Retry Times to Alarm	When the number of failed verification reaches the set value (value ranges from 1 to 9 times), the alarm will be triggered. If the set value is None, the alarm will not be triggered after failed verification.
Normal Close Time Period	It is the scheduled time-period for "Normal Close" mode so that the door is always close during this 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.
Auxiliary Input Configuration	Sets the door unlock time period and auxiliary output type of the auxiliary terminal device. Auxiliary output types include None, Trigger door open, Trigger Alarm, Trigger door open and Alarm.
Valid Holidays	To set if Normal Close Time Period or Normal Open Time Period settings are valid in set holiday time period. Choose [ON] to enable the set NC or NO time period in holiday.
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, master device, and alarm. However, erased access control data in Data Mgt. is excluded.

12.2 Time Rule Settings/ Time Schedule

Tap [**Time Rule Settings**] / [**Time Schedule**] on the **Access Control** interface to configure the time settings.

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

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



Time Rule[2/50]	
Sunday	[00:00 23:59] [00:00 23:...
Monday	[00:00 23:59] [00:00 23:...
Tuesday	[00:00 23:59] [00:00 23:...
Wednesday	[00:00 23:59] [00:00 23:...
Thursday	[00:00 23:59] [00:00 23:...
Friday	[00:00 23:59] [00:00 23:...
Saturday	[00:00 23:59] [00:00 23:...
holiday type 1	[00:00 23:59] [00:00 23:...
holiday type 2	[00:00 23:59] [00:00 23:...
holiday type 3	[00:00 23:59] [00:00 23:...

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

Time Period 1

00:00 23:59

00 00 23 59

HH MM HH MM

Confirm (OK) Cancel (ESC)

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

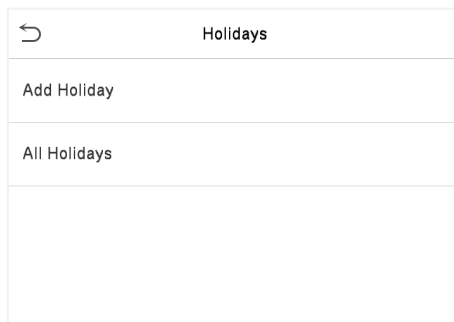
Note:

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

12.3 Holidays

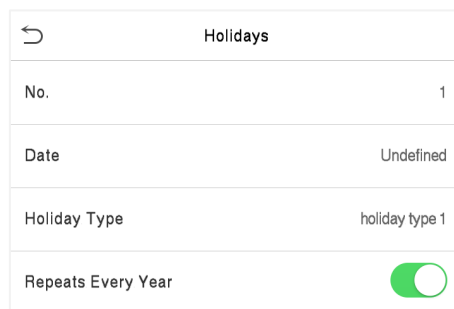
Whenever there is a holiday, you may need a distinct access time; but changing everyone's access time one by one is extremely cumbersome, so a holiday access time can be set that applies to all employees and the user will be able to open the door during the holidays.

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



- **Add a New Holiday**

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



- **Edit a Holiday**

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

- **Delete a Holiday**

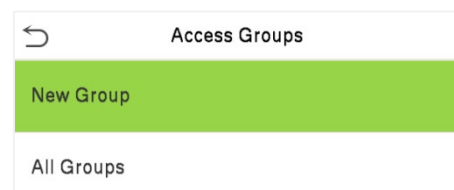
On the **Holidays** interface, select a holiday item to be deleted and tap [**Delete**]. Tap [**OK**] to confirm the deletion. After deletion, this holiday does not display on the **All Holidays** interface.

12.4 Access Groups

Grouping is to manage users in groups, only for time attendance terminal.

The default time zone for group members is the group time zone, while users can set their personal time zone. When the group verification mode and the user verification mode overlap, the user verification mode takes priority. Each group can set a maximum of 3 time zones; as long as one of them is valid, the group can be successfully verified. The newly enrolled user is assigned to Access Group 1 by default, but can be assigned to another access group.

Tap [**Access Groups**] on the **Access Control** interface.



● Add a New Holiday

Tap [**New Group**] on the **Access Group** interface.

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

1. The system has a default access group numbered 1, which cannot be deleted but can be modified.
2. A number cannot be modified again after being set.
3. When the holiday is set to be valid, the personnel in a group can open the door only when group time period overlaps with the holiday time period.
4. When the holiday is set to be invalid, the access control time of the personnel in this group is not affected by holidays.

● Edit Group

On the **All Group** interface, tap to select the access group item to be modified. Tap [**Edit**] to modify group parameters.

● Delete a Group

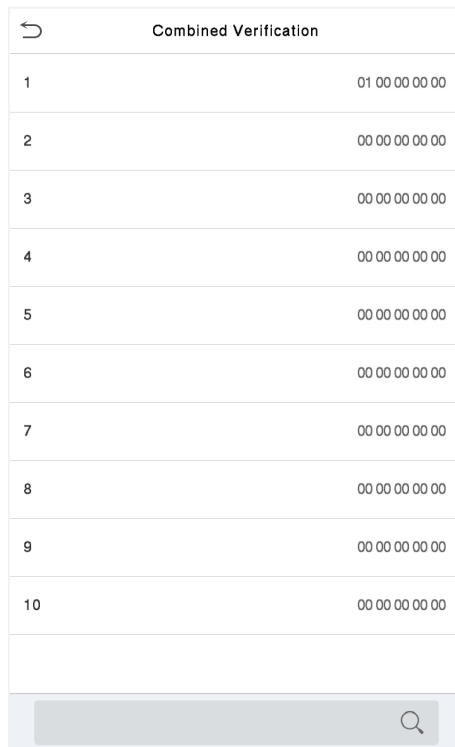
On the **All Group** interface, select a access group item to be deleted and tap [**Delete**]. After deletion, this group does not display on the **All Group** interface.

12.5 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.

Tap [**Combined Verification**] on the **Access Control** interface to configure the combined verification setting.



Combined Verification	
1	01 00 00 00 00
2	00 00 00 00 00
3	00 00 00 00 00
4	00 00 00 00 00
5	00 00 00 00 00
6	00 00 00 00 00
7	00 00 00 00 00
8	00 00 00 00 00
9	00 00 00 00 00
10	00 00 00 00 00

On the combined verification interface, tap the Door-unlock combination to be set, and tap the [up] and [down] arrows to input the combination number, and then tap [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.

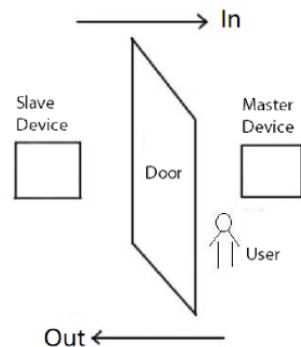
Note: To delete the door-unlock combination, set all Door-unlock combinations to 0.

12.6 Anti-passback Setup

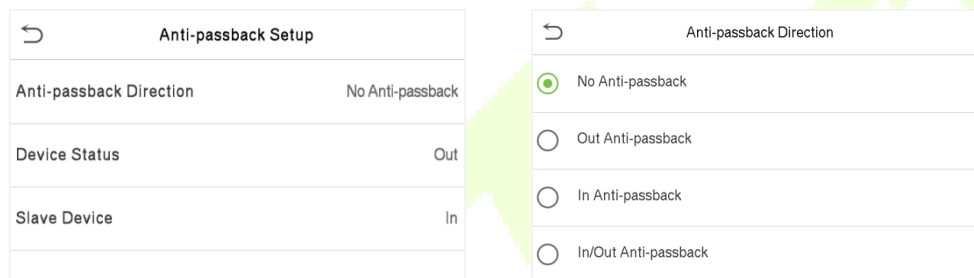
A user may be followed by some person(s) to enter the door without verification, resulting in a security breach. So, to avoid such situations, the Anti-Passback option was developed. Once it is enabled, the check-in and check-out record must occur alternatively to open the door to represent a consistent pattern.

This function requires two devices to work together:

One device is installed on the indoor side of the door (master device), and the other one is installed on the outdoor side of the door (the slave device). The two devices communicate via the Wiegand signal. The Wiegand format and Output type (User ID / Card Number) adopted by the master device and slave device must be consistent.



Tap [**Anti-Passback Setup**] on the **Access Control** interface.



Function Name	Description
Anti-passback Direction	<p>No Anti-passback: The Anti-Passback function is disabled, which means successful verification through either the master device or slave device can unlock the door. The attendance state is not saved in this option.</p> <p>Out Anti-passback: The user can check-out only if the last record is a check-in record otherwise an alarm is raised. However, the user can check-in freely.</p> <p>In Anti-passback: The user can check-in again only if the last record is a check-out record otherwise an alarm is raised. However, the user can check-out freely.</p> <p>In/Out Anti-passback: In this case, a user can check-in only if the last record is a check-out or the user can check-out only if the last record is a check-in otherwise the alarm is triggered.</p>
Device Status	Set the device to in/out/none. Note: This function only for Time Attendance Terminal.
Slave Device	Set the slave device to in/out/none. Note: This function only for Time Attendance Terminal.

12.7 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 trigger the alarm as well.

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

Access Control Terminal:

Duress Options	
Alarm on Password	<input type="checkbox"/>
Alarm Delay(s)	10
Duress Password	None

Time Attendance Terminal:

Duress Options	
Alarm on Password	<input checked="" type="checkbox"/>
Alarm Delay(s)	10
Duress Password	

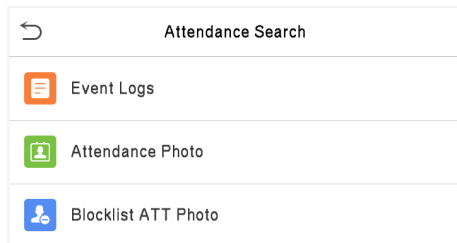
Function Name	Description
Alarm on Password	When a user uses the password verification method, an alarm signal will be generated, otherwise there will be no alarm signal.
Alarm Delay (s)	Alarm signal will not be transmitted until the alarm delay time is elapsed. The value ranges from 1 to 999 seconds.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

13 Attendance Search

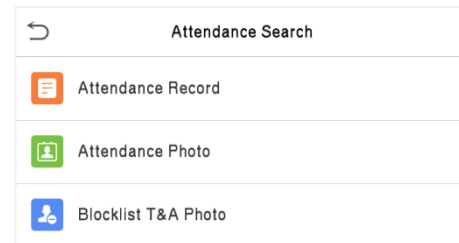
Once the identity of a user is verified, the access record is saved in the device. This function enables users to check their event logs.

Select [**Attendance Search**] on the **Main Menu** interface to search for the required event Logs.

Access Control Terminal:



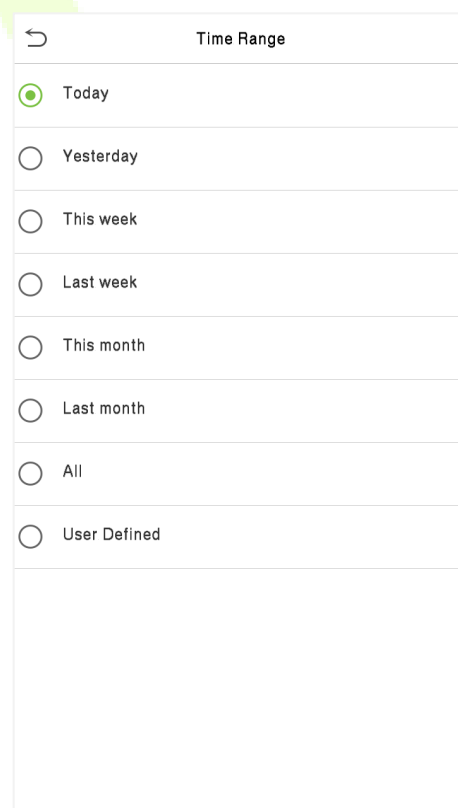
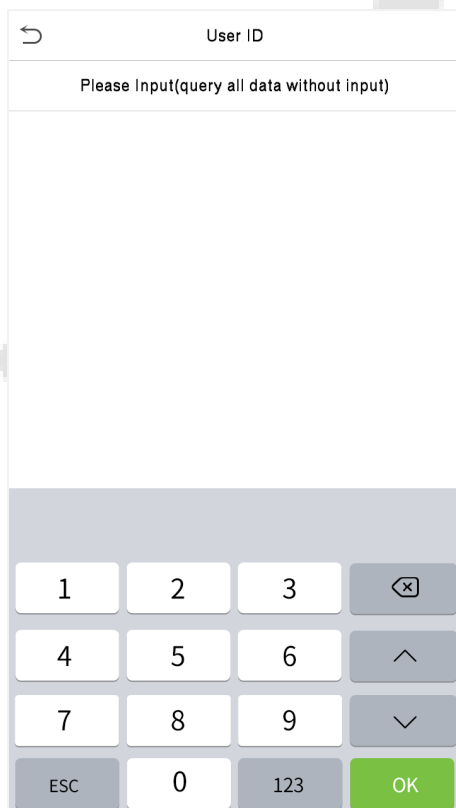
Time Attendance Terminal:



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

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

1. Enter the user ID to be searched and tap [**OK**].
If you want to search for records of all users, tap [**OK**] without entering any user ID.
2. Select the time range in which the records need to be searched.

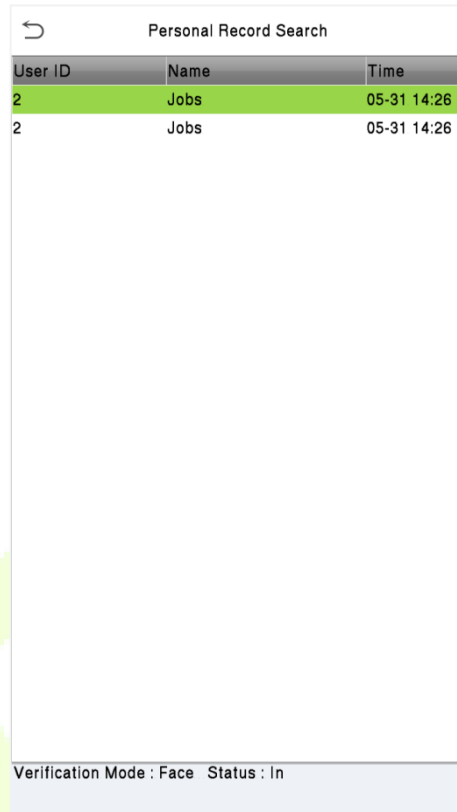


3. Once the record search completes. Tap the record highlighted in green to view its details.



Date	User ID	Time
12-08		Number of Records:05
	0	08:16 08:16 06:19 06:18 06:18
12-07		Number of Records:48
	0	15:05 15:05 13:41 13:41 13:31 13:30 13:29 13:28 13:27 13:27 13:27 13:27 13:26 13:26 13:26 13:25 12:26 12:26 10:54 10:54 10:50 10:50 10:50 10:49 10:28 10:28 10:28 10:27 10:26 10:26 09:09 09:09
	1	15:00 14:59 14:55 14:55 14:55 14:24 14:24 14:24 14:24 14:24 14:24 14:24 14:23 14:23 12:21 12:21

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



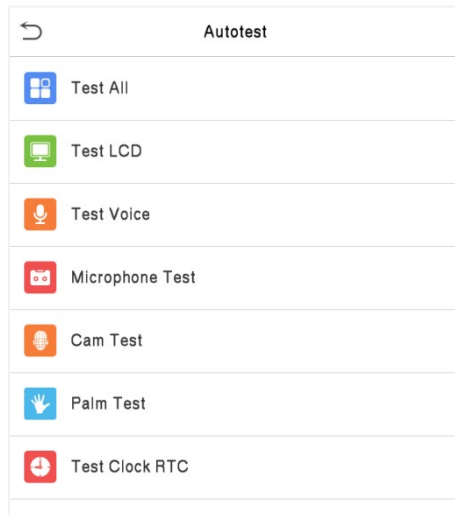
User ID	Name	Time
2	Jobs	05-31 14:26
2	Jobs	05-31 14:26

Verification Mode : Face Status : In

14 Autotest

To automatically test whether all modules in the device function properly, which include the LCD, Audio, Microphone, Camera, Palm and real-time clock (RTC).

Tap [**Autotest**] on the **Main Menu** interface.

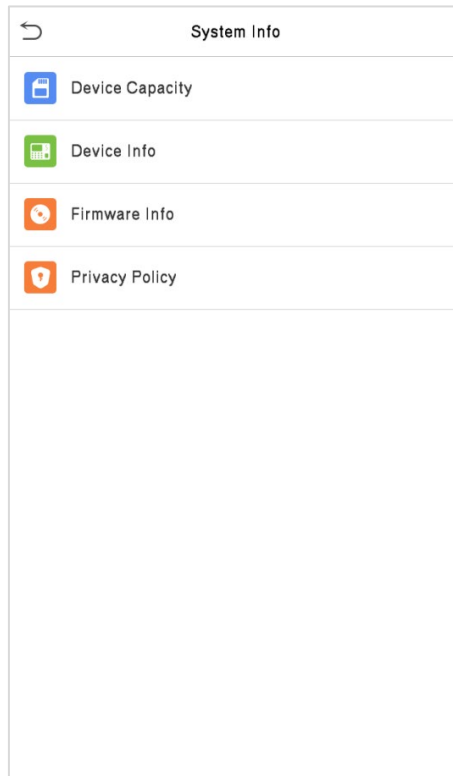


Function Name	Description
Test All	To automatically test whether the LCD, audio, camera and RTC are normal.
Test LCD	To automatically test the display effect of LCD screen by displaying full-color, pure white, and pure black to check whether the screen displays colors normally.
Test Voice	To automatically 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.
Camera Test	To test if the camera functions properly by checking the pictures taken to see if they are clear enough.
Palm Test	To test if the camera functions properly by checking the pictures taken to see if they are clear enough.
Test Clock RTC	To test the RTC. The device tests whether the clock works normally and accurately with a stopwatch. Touch the screen to start counting and press it again to stop counting.

15 System Information

With the system information option, you can view the storage status, the version information of the device, and so on.

Tap [**System Info**] on the **Main Menu** interface.



Function Name	Description
Device Capacity	Displays the current device's user storage, password, palm, face and card storage, administrators, T&A Record/attendance records, T&A Photo/attendance and blocklist photos, and Profile photos.
Device Info	Displays the device's name, serial number, MAC address, face algorithm, platform information, and manufacturer and manufacture date.
Firmware Info	Displays the firmware version and other version information of the device.
Privacy Policy	<p>The privacy policy control will appear when the gadget turns on for the first time. After taping "I have read it," the customer can use the product regularly. Tap System Info -> Privacy Policy to view the content of the privacy policy. The privacy policy's content does not allow for U disc export.</p> <p>Note: The current privacy policy's text is only available in Simplified Chinese/English. However, translation of other multi-language content is underway, with more iterations.</p>

16 Connect to ZKBio Time Software

16.1 Set the Communication Address

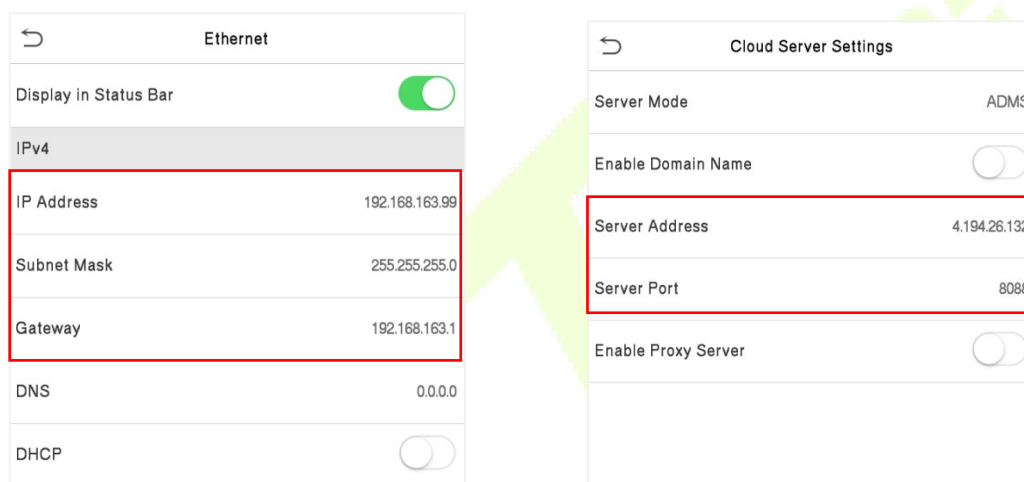
1. Tap **[COMM.] > [Ethernet]** in the **Main Menu** to set the IP address and gateway of the device.

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

2. In the **Main Menu**, tap **[COMM.] > [Cloud Server Settings]** to set the server address and server port.

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

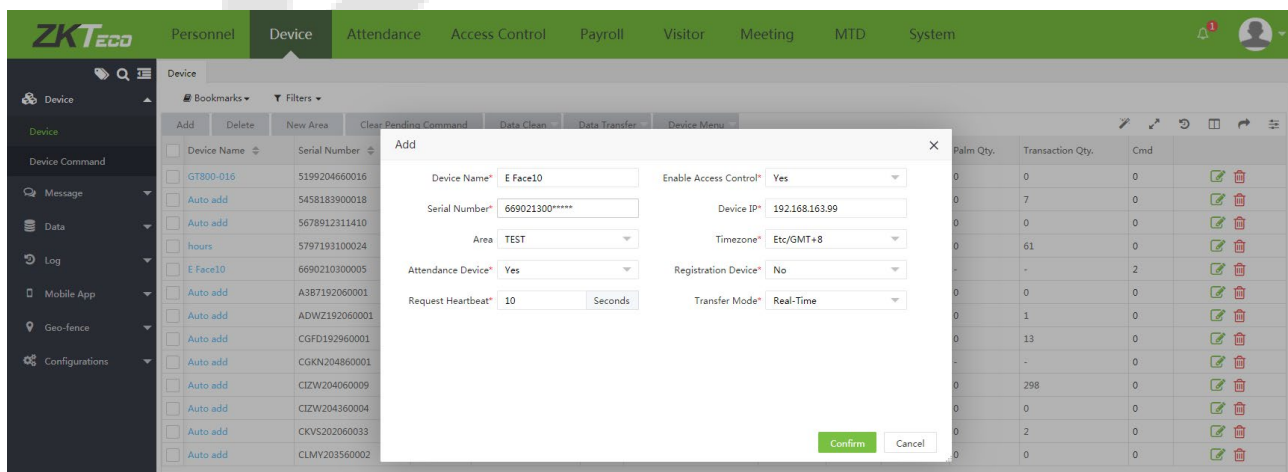
Server Port: Set the server port as of ZKBio Time (The default is 8088).



16.2 Add Device on the Software

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

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



16.3 Add Personnel to the Software

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

The screenshot shows a web form titled "Add" with a close button (X) in the top right corner. The form is organized into two main sections: "Profile" and "Private Information".

Profile Section:

- Employee ID*: 18259606107
- Department*: [Dropdown menu]
- Position: [Dropdown menu]
- Employment Type: [Dropdown menu]
- First Name: [Text input]
- Last Name: [Text input]
- Area*: [Dropdown menu]
- Hired Date: 2021-01-26

Private Information Section:

- SSN: [Text input]
- Passport NO.: [Text input]
- Contact Tel: [Text input]
- National: [Text input]
- Address: [Text input]
- Birthday: [Text input]
- Local Name: [Text input]
- Automobile License: [Text input]
- Office Tel: [Text input]
- Religion: [Text input]
- Postcode: [Text input]
- Gender: [Dropdown menu]
- Motorcycle License: [Text input]
- Mobile: [Text input]
- City: [Text input]
- Email: [Text input]

At the bottom right of the form, there are two buttons: "Confirm" (green) and "Cancel" (grey).

2. Fill in all the required fields and click **[Confirm]** to register a new user.
3. Click **[Device]** > **[Device]** > **[Data Transfer]** > **[Sync Data to Device]** to synchronize all the data to the device including the new users.

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

17 Connect to ZKBio CVAccess Software

17.1 Set the Communication Address

● Device Side

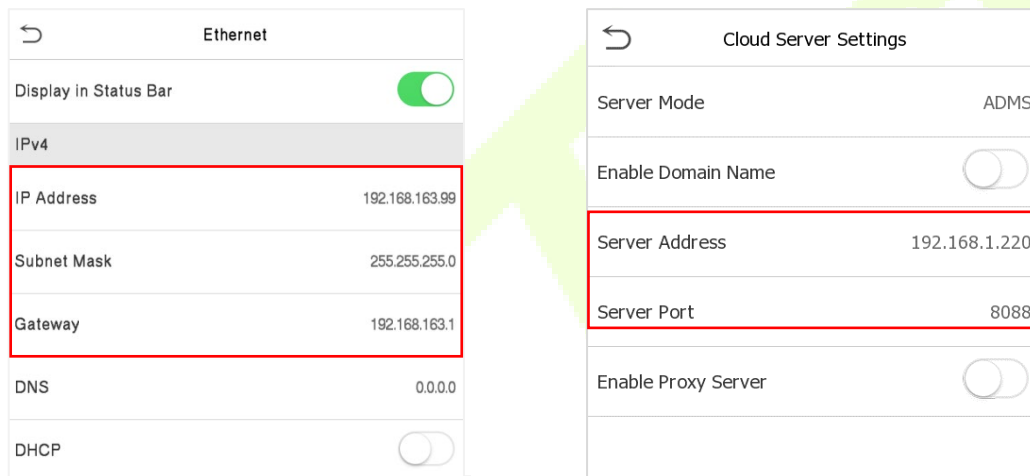
1. Tap [**COMM.**] > [**Ethernet**] in the **Main Menu** to set the IP address and gateway of the device.

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

2. In the **Main Menu**, tap [**COMM.**] > [**Cloud Server Settings**] to set the server address and server port.

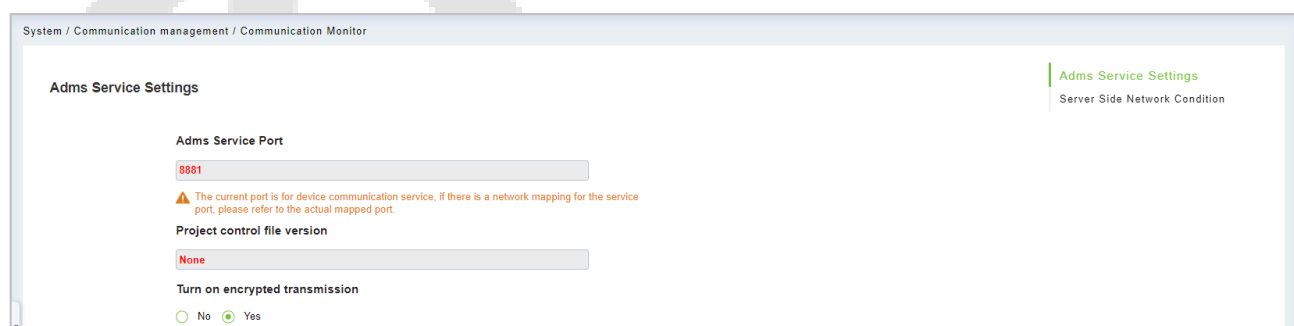
Server Address: Set the IP address as of ZKBio CVAccess server.

Server Port: Set the server port as of ZKBio CVAccess (The default is 8088).



● Software Side

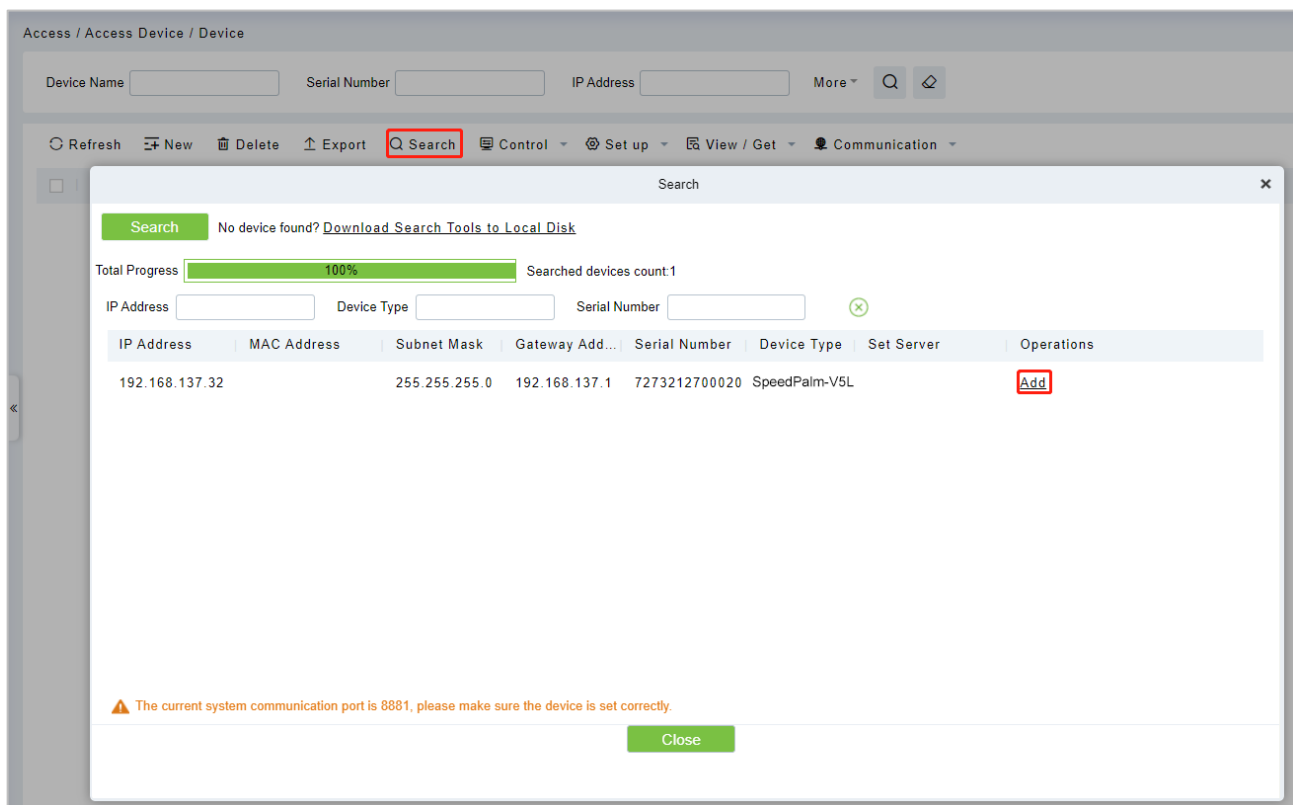
Login to ZKBio CVAccess software, click [**System**] > [**Communication**] > [**Communication Monitor**] to set the ADMS service port, as shown in the figure below:



17.2 Add Device on the Software

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

1. Click **[Access]** > **[Device]** > **[Search Device]**, 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 the operation column, and a new window will pop-up. Select Icon type, Area, and Add to Level from each dropdown and click **[OK]** to add the device.

17.3 Add Personnel to the Software

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

2. Fill in all the required fields and click **[OK]** to register a new user.
3. Click **[Attendance]** > **[Attendance Device]** > **[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 to *ZKBio CVAccess User Manual*.

18 Connect to ZKBio CVSecurity Software

18.1 Set the Communication Address

● Device Side

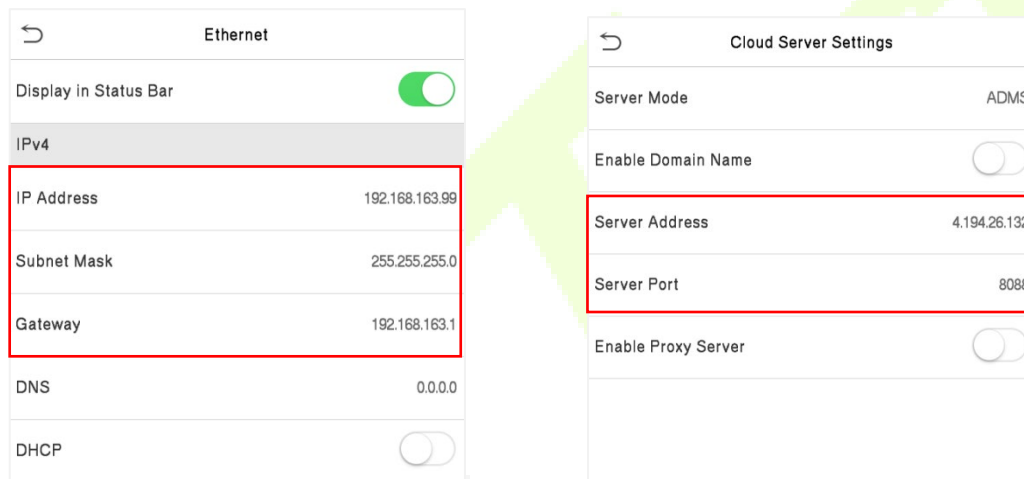
1. Tap **[COMM.]** > **[Ethernet]** in the **Main Menu** to set the IP address and gateway of the device.

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

2. In the **Main Menu**, tap **[COMM.]** > **[Cloud Server Settings]** to set the server address and server port.

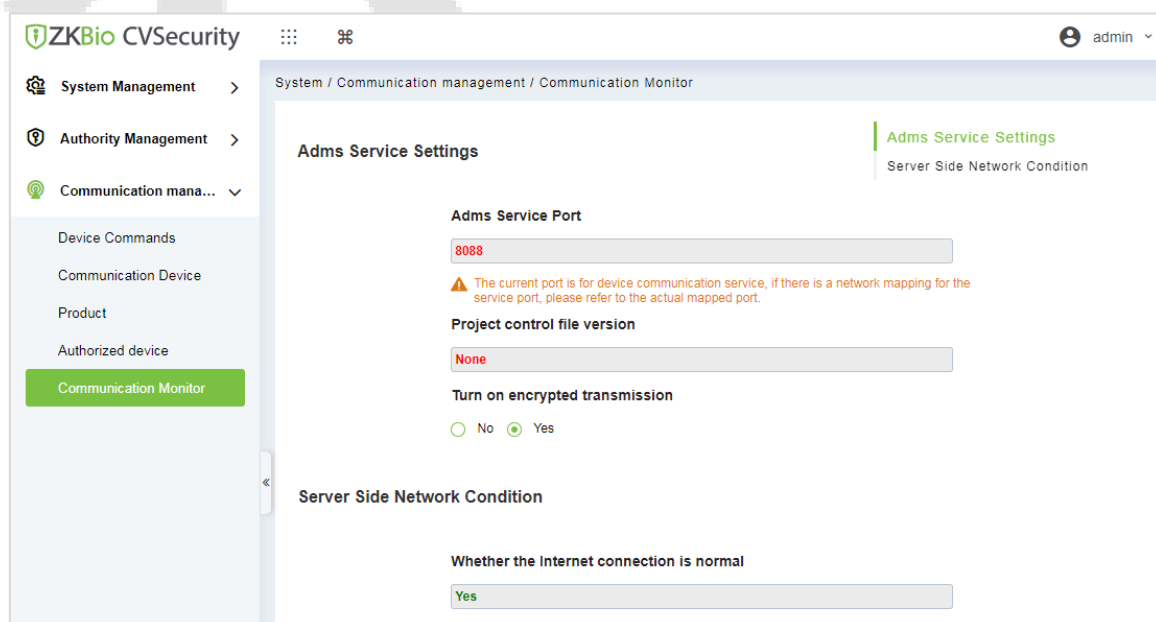
Server Address: Set the IP address as of ZKBio CVSecurity server.

Server Port: Set the server port as of ZKBio CVSecurity (The default is 8088).



● Software Side

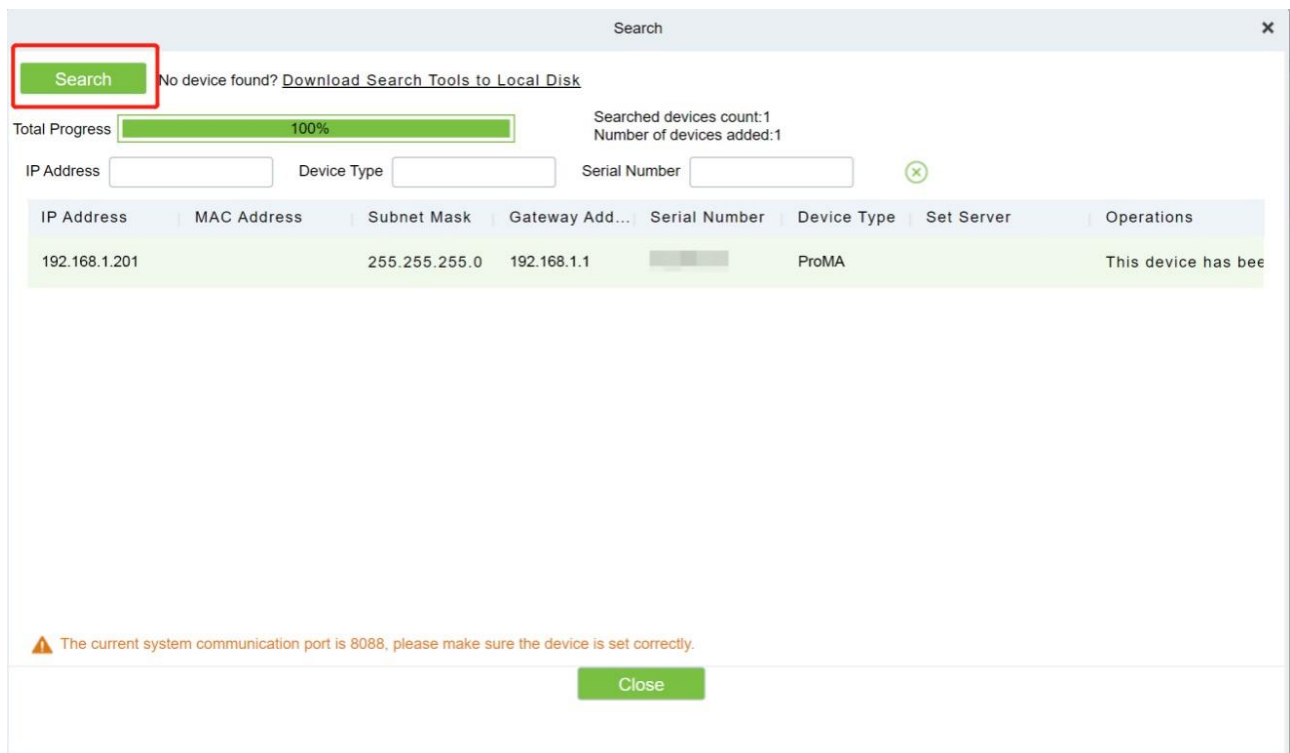
Login to ZKBio CVSecurity software, click **[System]** > **[Communication Management]** > **[Communication Monitor]** to set the ADMS service port, as shown in the figure below:



18.2 Add Device on the Software

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

1. Click **[Access]** > **[Device]** > **[Search Device]**, 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 the operation column, and a new window will pop-up. Select Icon type, Area, and Add to Level from each dropdown and click **[OK]** to add the device.

18.3 Add Personnel to the Software

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

The screenshot shows a 'New' personnel registration window. It contains two columns of input fields. The left column includes: Personnel ID* (text input), First Name (text input), Gender (dropdown), Certificate Type (dropdown), Birthday (text input), Hire Date (text input), Device Verification Password (text input), and Biometrics Type (text input). The right column includes: Department* (dropdown with 'Departement Name'), Last Name (text input), Mobile Phone (text input with a checkbox), Certificate Number (text input), Email (text input with a checkbox), Position Name (dropdown), Card Number (text input with a camera icon and checkbox), and WhatsApp (text input with a checkbox). To the right of these fields is a profile picture placeholder with a question mark icon and two buttons: 'Browse' and 'Capture'. Below the input fields is a tabbed interface with 'Access Control' selected. Under 'Access Control', there is a 'Levels Settings' section with a 'General' checkbox checked. To the right of this are several settings: 'Superuser' (dropdown set to 'No'), 'Device Operation Role' (dropdown set to 'Ordinary User'), 'Extend Passage' (checkbox), 'Access Disabled' (checkbox), and 'Set Valid Time' (checkbox). At the bottom of the 'Access Control' section are three buttons: 'Add', 'Select All', and 'Unselect All'. At the very bottom of the window are three buttons: 'Save and New', 'OK', and 'Cancel'.

2. Fill in all the required fields and click **[OK]** to register a new user.
3. Click **[Access]** > **[Access Device]** > **[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 to *ZKBio CVSecurity User Manual*.

Appendix 1

Requirements of Live Collection and Registration of Visible Light Face Templates

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

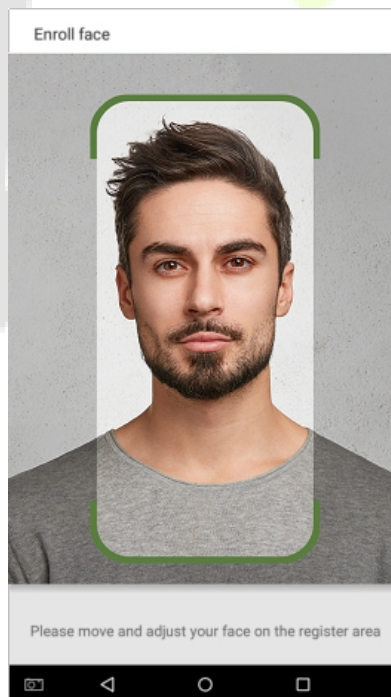


Image1 Face Capture Area

Requirements for Visible Light Digital Face Template Data

Digital photo should be straightly edged, colored, half-portrayed with only one person, and the person should be uncharted and not in uniform. Persons who wear eyeglasses should remain to put on eyeglasses for photo capturing.

- **Eye Distance**

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

- **Facial Expression**

Plain face 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 and colored eyeglasses are not allowed. The frame of the eyeglasses should not shield eyes and should not reflect light. For persons with thick eyeglasses frame, it is recommended to capture two images, one with eyeglasses and the other one without.

- **Face**

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

- **Image 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 image with not more than 20kb size.
- 4) Definition rate between 358 x 441 to 1080 x 1920.
- 5) The vertical scale of head and body should be 2:1.
- 6) The photo should include the captured person's shoulders at the same horizontal level.
- 7) The captured person should be eyes-open and with clearly seen iris.
- 8) Plain face or smile is preferred, showing teeth is not preferred.
- 9) The captured person should be clearly seen, natural in color, and without image obvious twist, no shadow, light spot or reflection in face or background, and appropriate contrast and lightness level.

Appendix 2

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

