

User Manual

RevFace15

Date: January 2023

Doc Version: 1.1

English

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



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

Copyright © 2023 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 have 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 **RevFace15**.

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

Document Conventions

Conventions used in this manual are listed below:

GUI Conventions

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

Symbols






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


Table of Contents

1	SAFETY MEASURES	7
2	OVERVIEW.....	10
3	INSTRUCTION FOR USE	11
	3.1 STANDING POSITION, POSTURE AND FACIAL EXPRESSION	11
	3.2 FACE REGISTRATION.....	12
	3.3 STANDBY INTERFACE.....	13
	3.4 VIRTUAL KEYBOARD	14
	3.5 VERIFICATION MODE.....	15
	3.5.1 FACIAL VERIFICATION	15
	3.5.2 MULTI-FACE VERIFICATION	18
	3.5.3 CARD VERIFICATION	21
	3.5.4 PASSWORD VERIFICATION.....	23
4	MAIN MENU	26
5	USER MANAGEMENT.....	27
	5.1 USER REGISTRATION.....	27
	5.1.1 USER ID AND NAME	27
	5.1.2 USER ROLE	28
	5.1.3 FACE.....	28
	5.1.4 PASSWORD.....	29
	5.1.5 PROFILE PHOTO	30
	5.1.6 ACCESS CONTROL ROLE	30
	5.2 SEARCH USER.....	31
	5.3 EDIT USER	32
	5.4 DELETE USER	32
	5.5 DISPLAY STYLE	33
6	USER ROLE	34
7	COMMUNICATION SETTINGS	36
	7.1 NETWORK SETTINGS.....	36
	7.2 SERIAL COMM.....	37
	7.3 PC CONNECTION.....	38
	7.4 WIRELESS NETWORK	38
	7.5 CLOUD SERVER SETTINGS	41
	7.6 WIEGAND SETUP	41
	7.6.1 WIEGAND INPUT	42
	7.6.2 WIEGAND OUTPUT.....	44
	7.7 NETWORK DIAGNOSIS.....	45
8	SYSTEM SETTINGS.....	46
	8.1 DATE AND TIME.....	47

- 8.2 ACCESS LOGS SETTING AND ATTENDANCE48
- 8.3 FACE PARAMETERS50
- 8.4 DETECTION MANAGEMENT54
- 8.5 DEVICE TYPE SETTINGS55
- 8.6 SECURITY SETTINGS56
- 8.7 FACTORY RESET56
- 9 PERSONALIZE SETTINGS 58**
- 9.1 INTERFACE SETTINGS58
- 9.2 VOICE SETTINGS.....59
- 9.3 BELL SCHEDULES60
- 9.4 PUNCH STATES OPTIONS61
- 9.5 SHORTCUT KEY MAPPINGS.....62
- 10 DATA MANAGEMENT 64**
- 10.1 DELETE DATA64
- 11 ACCESS CONTROL 67**
- 11.1 ACCESS CONTROL OPTIONS68
- 11.2 TIME RULE SETTING AND TIME SCHEDULE71
- 11.3 HOLIDAYS73
- 11.4 ACCESS GROUPS74
- 11.5 COMBINED VERIFICATION75
- 11.6 ANTI-PASSBACK SETUP76
- 11.7 DURESS OPTIONS77
- 12 ATTENDANCE SEARCH 79**
- 13 PRINT SETTINGS 81**
- 13.1 PRINT DATA FIELD SETTINGS.....81
- 13.2 PRINT OPTIONS SETTINGS.....82
- 14 AUTOTEST 83**
- 15 SYSTEM INFORMATION 84**
- 16 CONNECT TO ZKBIOACCESS IVS SOFTWARE..... 85**
- 16.1 SET THE COMMUNICATION ADDRESS85
- 16.2 ADD DEVICE ON THE SOFTWARE.....86
- 16.3 ADD PERSONNEL ON THE SOFTWARE87
- APPENDIX 1 88**
- REQUIREMENTS OF LIVE COLLECTION AND REGISTRATION OF VISIBLE LIGHT FACE IMAGES.....88
- REQUIREMENTS FOR VISIBLE LIGHT DIGITAL FACE IMAGE DATA.....89
- APPENDIX 2 90**
- PRIVACY POLICY90
- ECO-FRIENDLY OPERATION.....92

1 Safety Measures

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

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

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

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

And do not connect multiple devices to one power adapter as adapter overload can cause over-heat or fire hazard.

7. **Replacement parts** - When replacement parts are needed, service technicians must only use replacement parts provided by the supplier. Unauthorized substitutes can result in a burn, shock, or other hazards.
8. **Safety check** - On completion of service or repair work on the unit, ask the service technician to perform safety checks to ensure proper operation of the device.
9. **Power sources** - Operate the system only from the label's power source form. If the sort of AC adapter to use is unclear, call your dealer.

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

Recommended installing the devices in areas with limited access.

Electrical Safety

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

Operation Safety

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

 **Note**

- Make sure whether the positive polarity and negative polarity of the DC 12V AC adapter is connected correctly. A reverse connection may damage the device. It is not advisable to connect the AC 24V AC adapter to the DC 12V input port.
- Make sure to connect the wires following the positive polarity and negative polarity shown on the device's nameplate.
- The warranty service does not cover accidental damage, damage caused by mis-operation, and damage due to independent installation or repair of the product by the user.



2 Overview

RevFace15 uses the latest **Computer Vision Technology**. It supports facial verification with large capacity and quick recognition and also improves security performance in all aspects.

It accepts touchless recognition technology and new functions namely **Masked Individual Identification** which eliminates hygiene concerns effectively. It is also equipped with the ultimate **Anti-Spoofing** algorithm for facial recognition against almost all types of fake photos and videos attack.

The terminal with mask detection is a perfect device to help reduce the spread of germs and help prevent infections at each access point of any premises and public areas such as hospitals, factories, schools, commercial buildings, stations during the recent global public health issue with its fast and accurate masked individual identification functions during facial verification.

Features

- Visible Light Facial Recognition.
- Better hygiene with touchless biometric authentication and masked individual identification.
- Anti-spoofing algorithm against printed photo attack (laser, color and B/W photos), videos attack and 3D mask attack.
- Multiple Verification Methods: **Password / Face / Card.**
- Multi-face Verification.

Other Specifications

- Mask detection.

3 Instruction for Use

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

3.1 Standing Position, Posture and Facial Expression


- **Recommended Standing Posture and Facial Expression**



Standing Posture



Facial Expression

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

3.2 Face Registration

Try to keep the face in the centre of the screen during registration. Please face towards the camera and stay still during face registration. The screen should look like this:



Correct face registration and authentication method

● Recommendation for registering a face

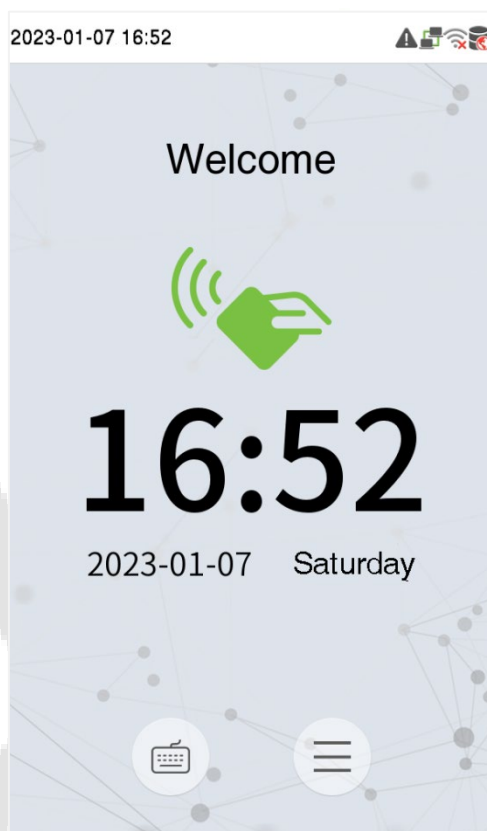
- When registering a face, maintain a distance of 40cm to 80cm between the device and the face.
- Be careful to keep your facial expression natural and not to change. (smiling, drawn face, wink, etc.)
- If you do not follow the instructions on the screen, the face registration may take a longer time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


- Ensure that the face appears inside the guideline displayed on the screen of the device.
- Sometimes, authentication may fail due to the change in the wearing glasses then the one used while registration. In such a case, you may require authenticating your face with the previously worn glasses. If your face was registered without glasses, you should authenticate your face without glasses further.
- 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.

3.3 Standby Interface

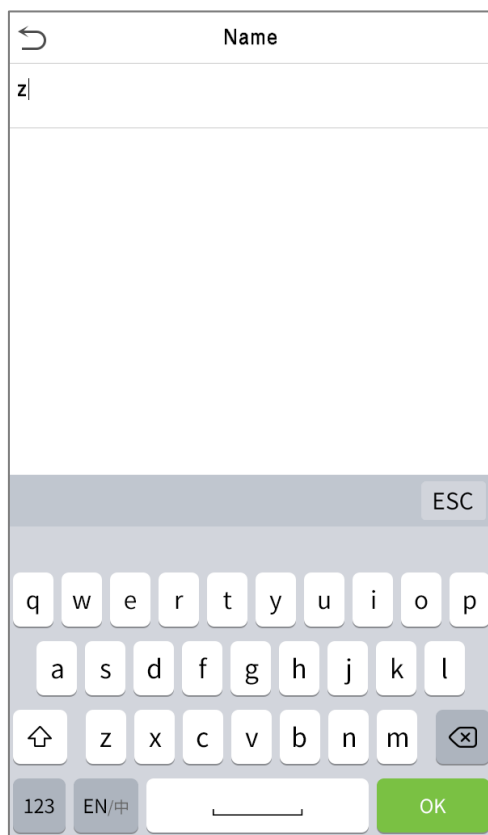
After connecting the AC adapter, the following standby interface is displayed:



- 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.

3.4 Virtual Keyboard



Note:

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

1. Tap **[En]** to switch to the English keyboard.
2. Press **[123]** to switch to the numeric and symbolic keyboard.
3. Tap **[ABC]** to return to the alphabetic keyboard.
4. Tap the input box, a virtual keyboard appears.
5. Tap **[ESC]** to exit the virtual keyboard.

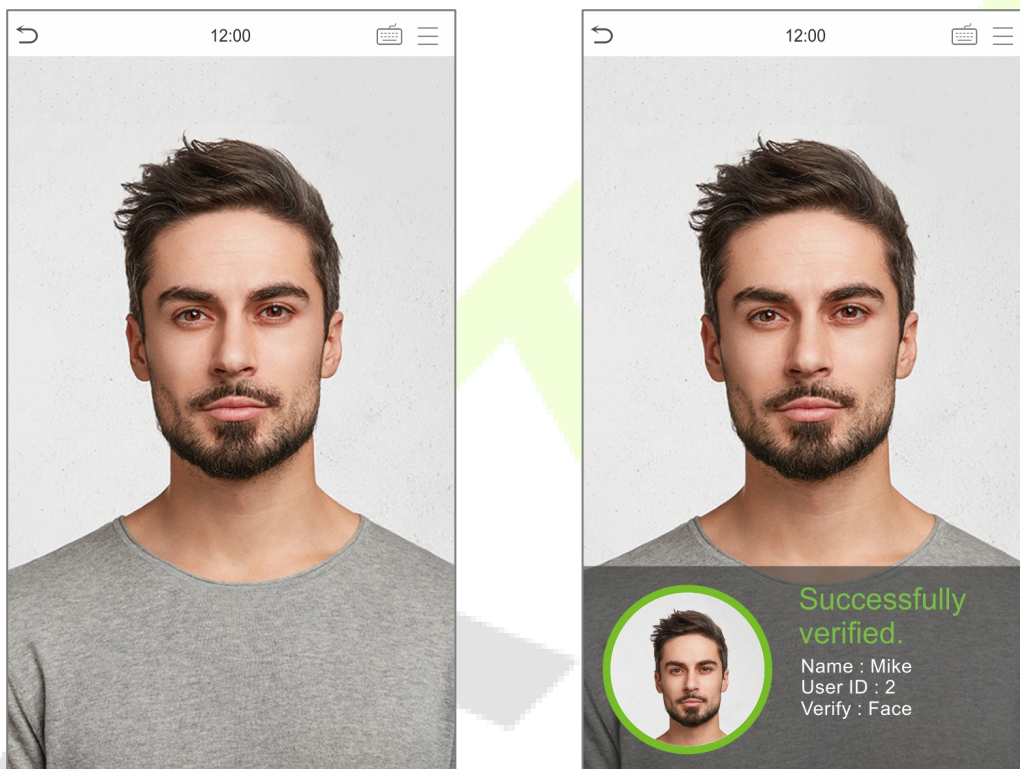
3.5 Verification Mode

3.5.1 Facial Verification

- **1:N Facial Verification**

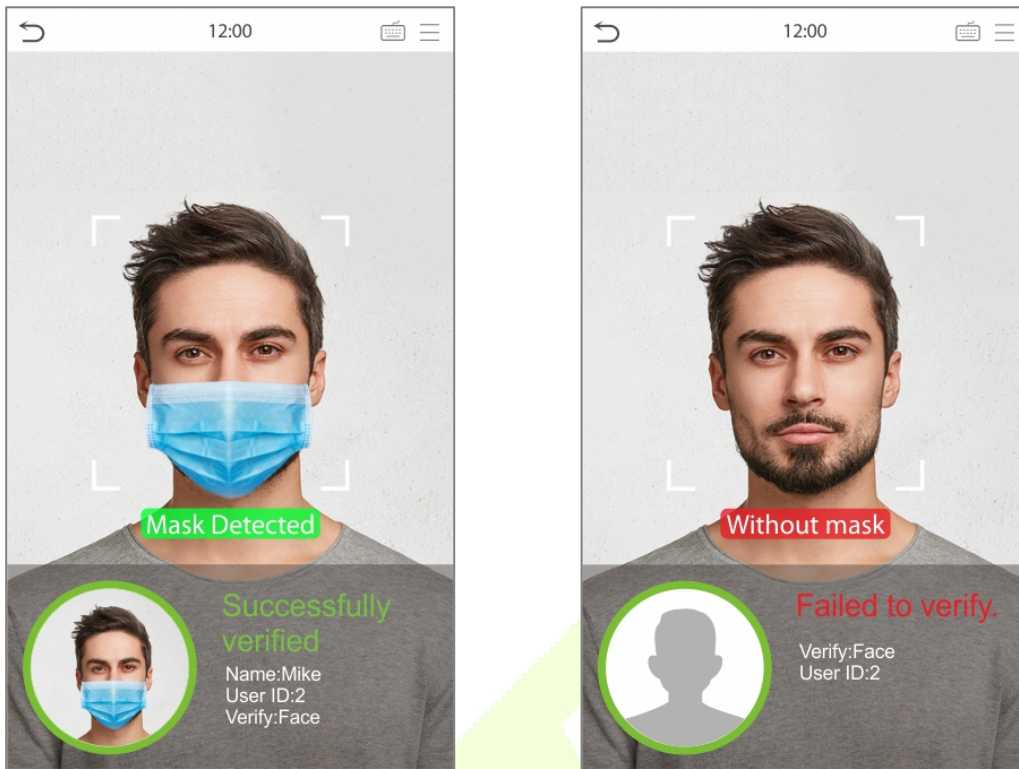
- 1. Conventional verification**

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




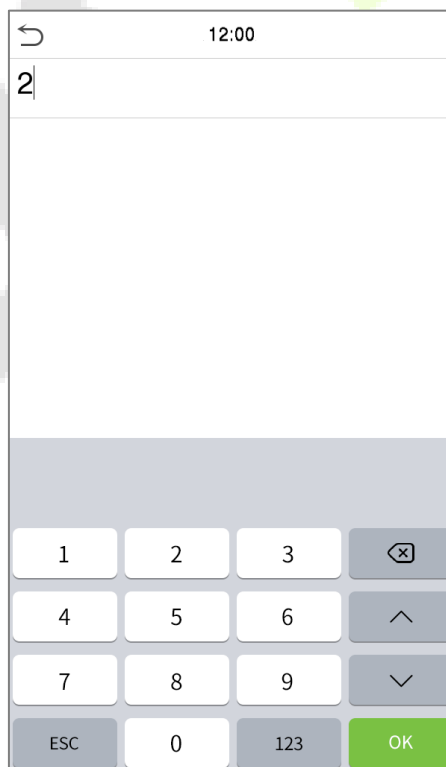
- 2. Enable mask detection**


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

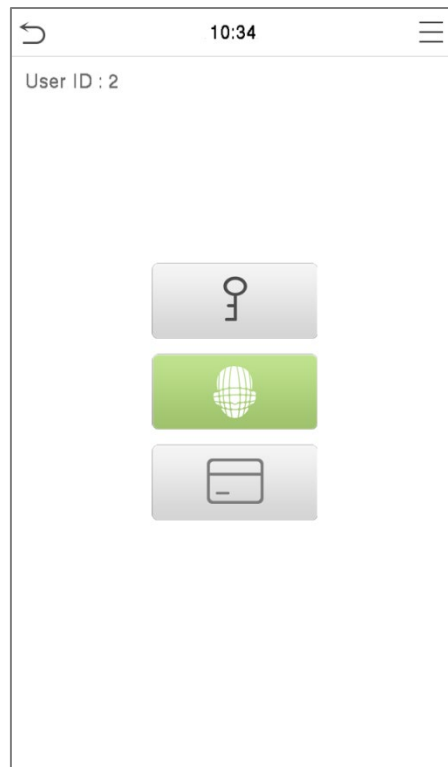


- **1:1 Facial Verification**

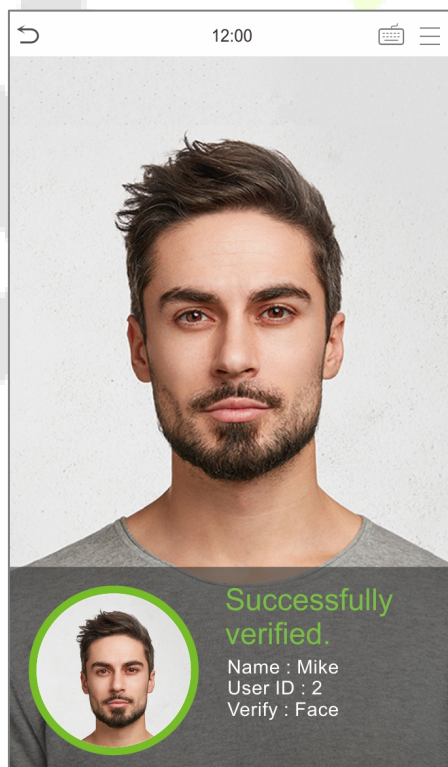
In this verification mode, the device compares the face captured by the camera with the facial template related to the entered user ID. Press  on the main interface and enter the 1:1 facial verification mode and enter the user ID and tap **[OK]**.



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

3.5.2 Multi-face Verification

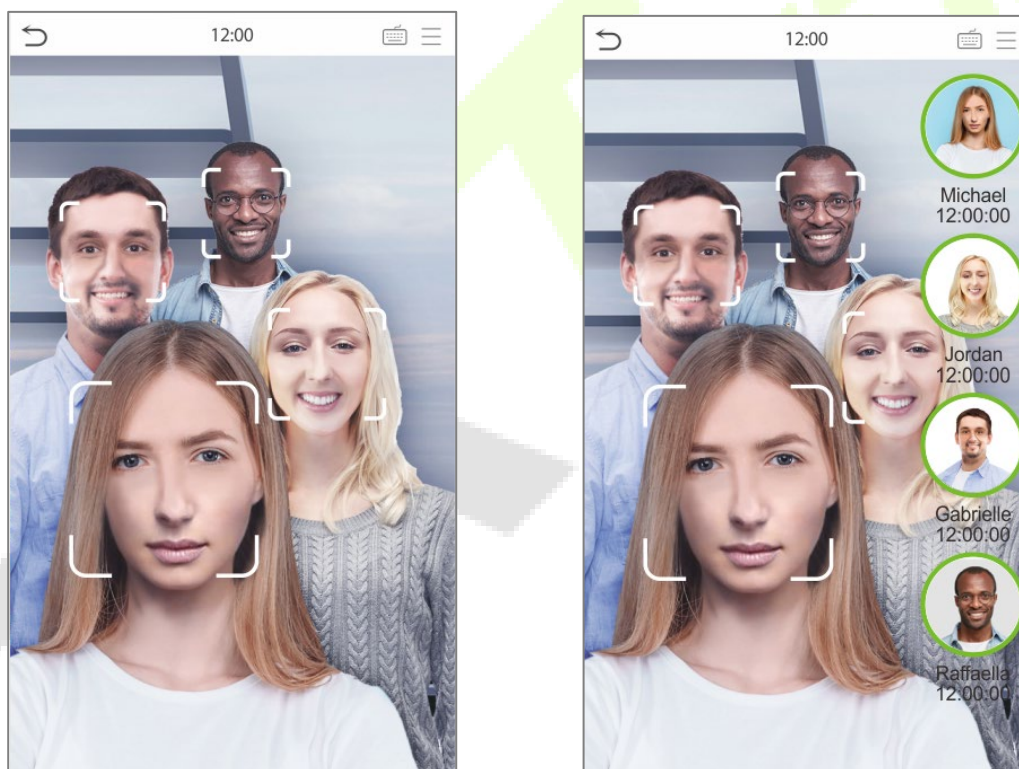
● 1:N Multi-face Verification

1. Conventional verification

In this verification mode, the device compares the collected multi-person facial images with all the face data registered in it. The device supports verification of up to 4 people at once. But the number of verification results to be displayed on the right side can be configured. The following image shows the pop-up prompt of a successful comparison result.

Tap **System > Face > Face Identifying Settings > Identifying Mode > Multi-face Identifying > Count to Display** to set the number of the verification results to be displayed.



 **Note:** The Count to Display can be set between 1 to 4.




2. Enable mask detection

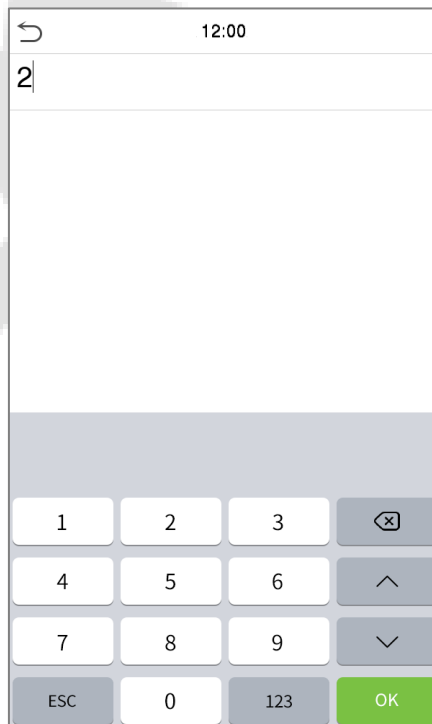
When the user enables the **Enable mask detection** function, the device identifies whether the user is wearing a mask while verification or not. The following are the popups of the comparison result prompt interface.




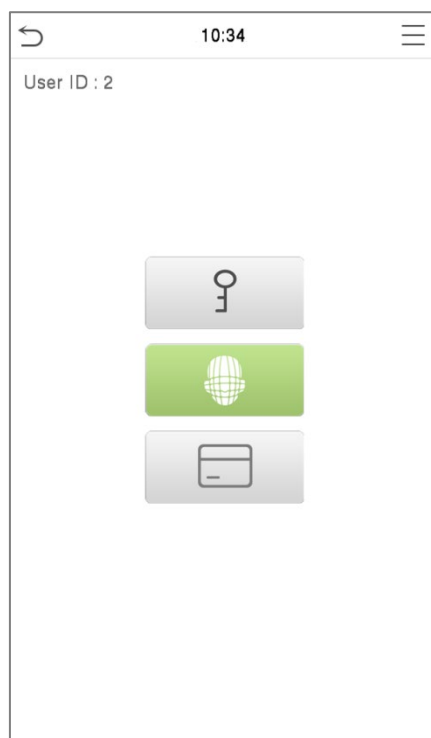
 **Note:** Not wearing a mask is displayed as  icon.

● **1:1 Multi-face Verification**

In this verification mode, the device compares the face captured by the camera with the facial template associated to the entered user ID. Press  on the main interface and select the 1:1 facial verification mode and enter the user ID and tap **[OK]**.



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



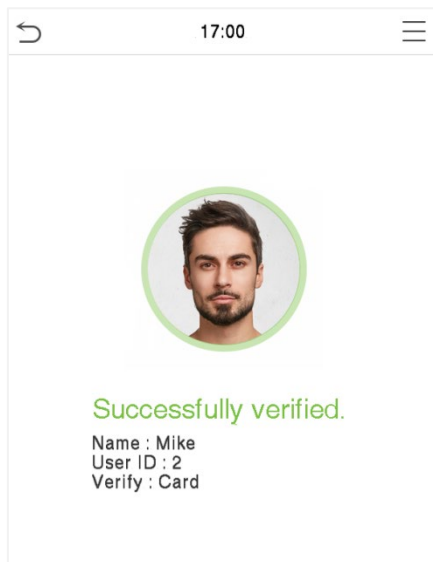
After the verification is successful, the prompt box will display the verification result, as shown in the figure below:




3.5.3 Card Verification

- **1:N Card Verification**

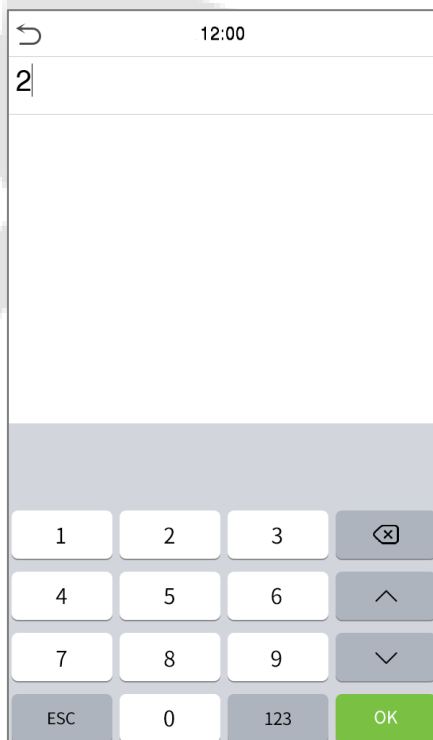
This verification mode compares the card number in the Card induction area with all the card number data registered in the device; the following is the card verification screen.




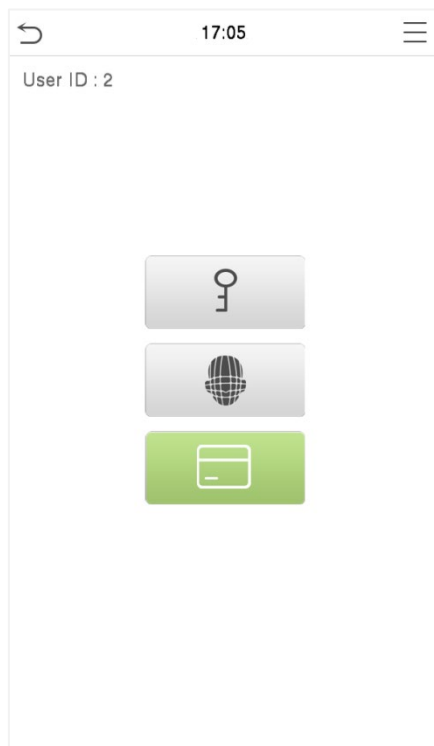
- **1:1 Card Verification**

Tap the  button on the main screen to open the 1:1 Card verification mode.

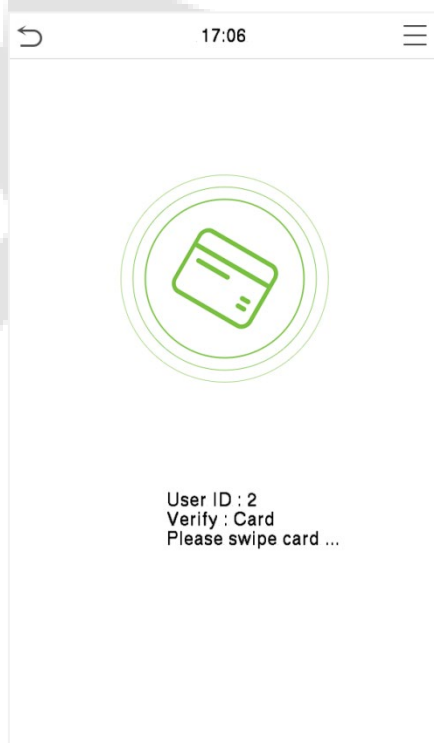
1. Input the user ID and tap **[OK]**.



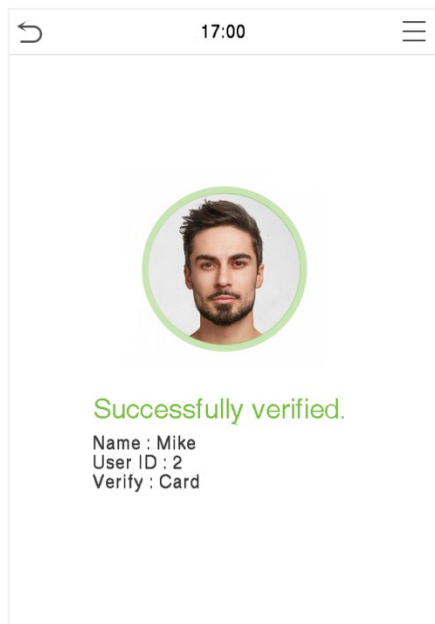
If an employee registers face and password in addition to card, and the verification method is set to Password/Face/Card, the following screen will appear. Select the  icon to enter the card verification mode.



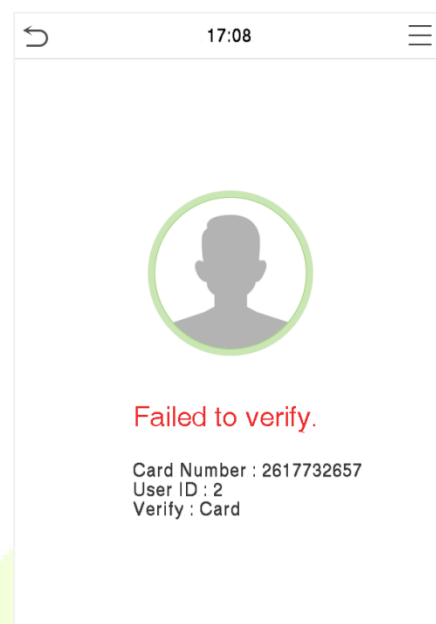
2. Swipe the card above the card area (the card must be registered first).



Successful Verification:




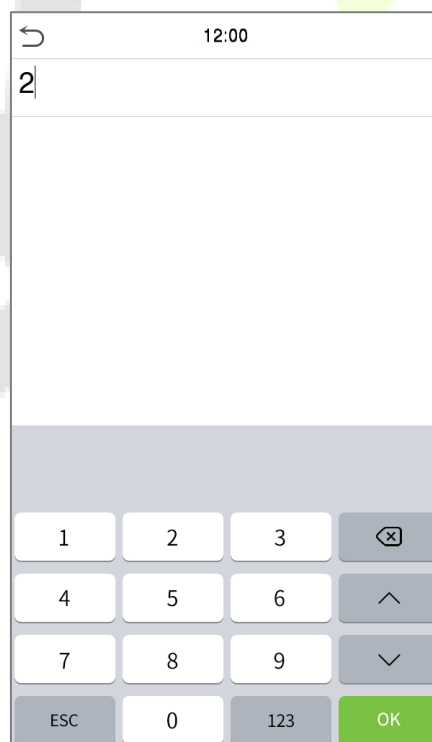
Failed Verification:




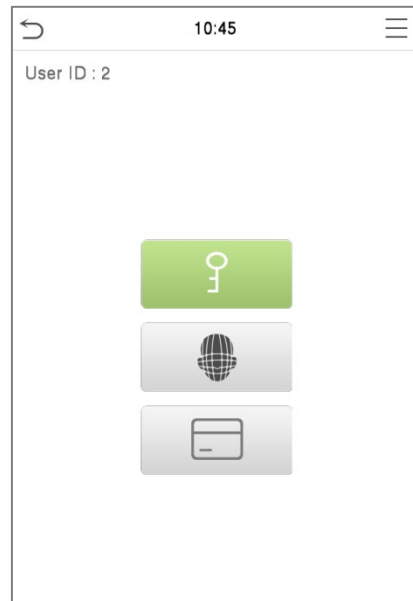
3.5.4 Password Verification

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

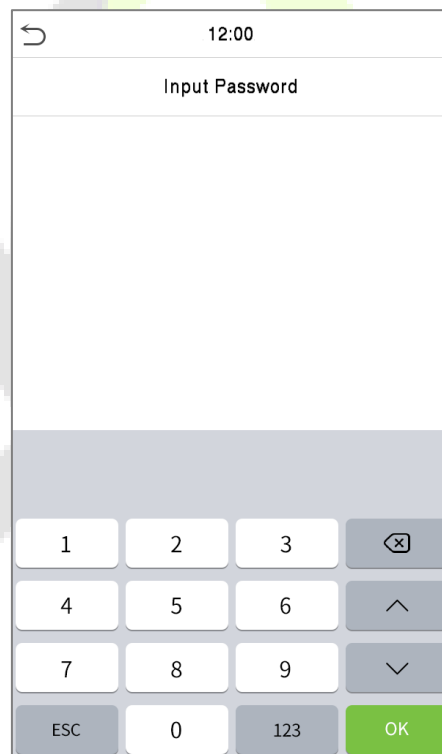
Tap the  button on the main screen to enter the 1:1 password verification mode. Then, input the user ID and press [OK].



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



Input the password and press **[OK]**.

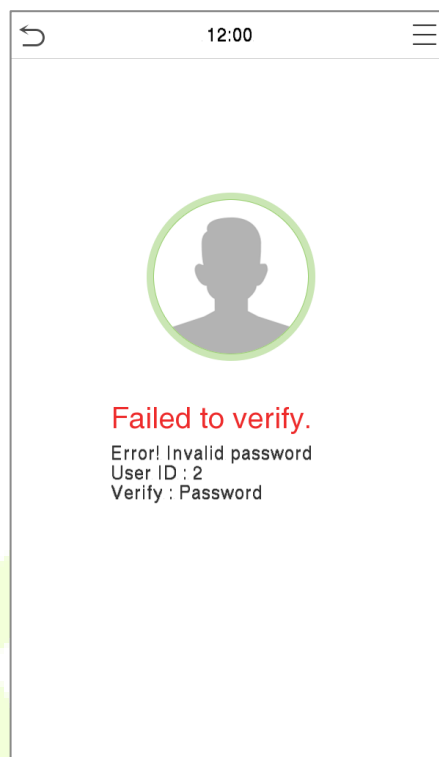


Following are the display screen after entering a correct password and a wrong password respectively.

Successful Verification:

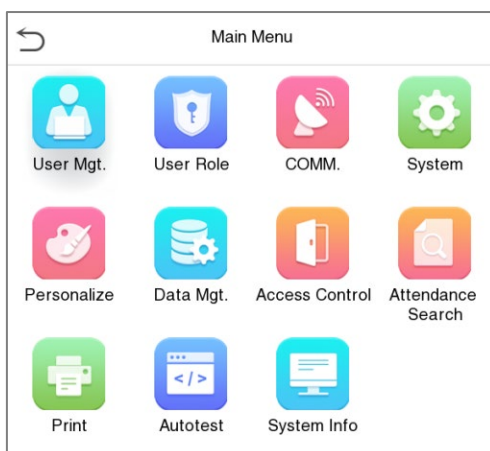


Failed Verification:



4 Main Menu

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



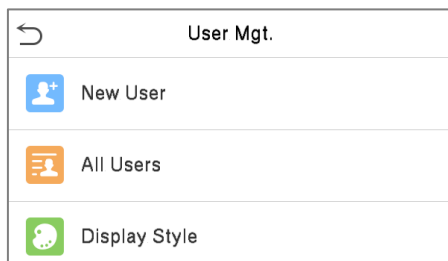
Function Description

Menu	Descriptions
User Mgt.	To Add, Edit, View, and Delete information of a User.
User Role	To set the permission scope of the custom role and enroller for the users, that is, the rights to operate the system.
COMM.	To set the relevant parameters of Network, Serial Comm., PC Connection, Wireless Network, Cloud Server, Wiegand and Network Diagnosis.
System	To set the parameters related to the system, including Date & Time, Access Logs Settings/Attendance, Face, Resetting to factory settings, Security Settings, Device Type Setting and Detection Management.
Personalize	To customize settings of User Interface, Voice, Bell Schedules, Punch State Options and Shortcut Key Mappings settings.
Data Mgt.	To delete all relevant data in the device.
Access Control	To set the parameters of the lock and the relevant access control device including options like Time schedule, Holiday Settings, Combine Verification, Anti-Passback Setup, and Duress Option Settings.
Attendance Search	To query the specified Event Logs, check Attendance Photos and Blocklist attendance photos.
Print	To set printing information and functions (if printer is connected to the device).
Autotest	To automatically test whether each module functions properly, including the LCD Screen, Audio, Camera, and real-time clock.
System Info	To view Data Capacity and Device and Firmware information of the current device.

5 User Management

5.1 User Registration

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



5.1.1 User ID and Name

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

New User	
User ID	5
Name	
User Role	Normal User
Face	0
Card Number	
Password	
Profile Photo	0
Access Control Role	

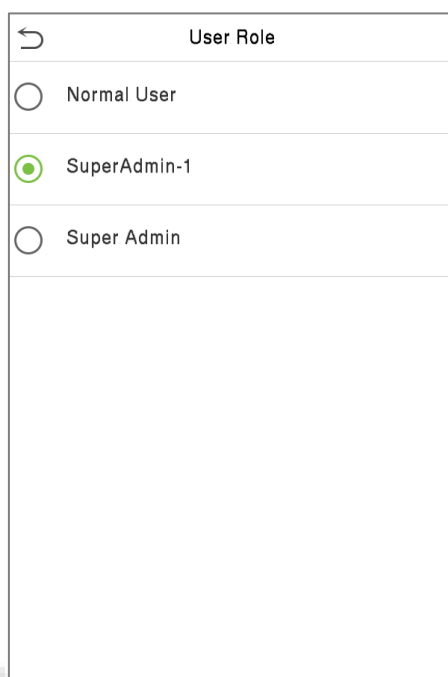
Note:

1. A name can take up to 34 characters.
2. The user ID may contain 1-9 digits by default.
3. You can modify your ID during the initial registration but not after registration.
4. If a message "**Duplicated!**" pops up, you must choose another ID as the entered User ID already exists.

5.1.2 User Role

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

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



User Role	
<input type="radio"/>	Normal User
<input checked="" type="radio"/>	SuperAdmin-1
<input type="radio"/>	Super Admin

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.

5.1.3 Face

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

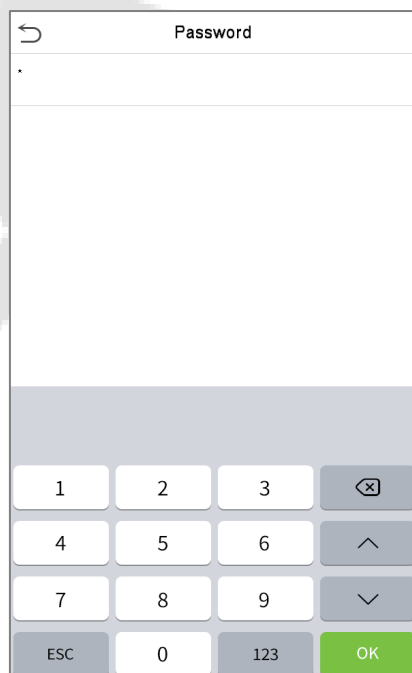
- Please face towards the camera and position yourself such that your face image fits inside the white guiding box and stay still during face registration.
- A progress bar shows up while registering the face and the "**Enrolled Successfully**" message is displayed as the progress bar completes.
- If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



5.1.4 Password

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

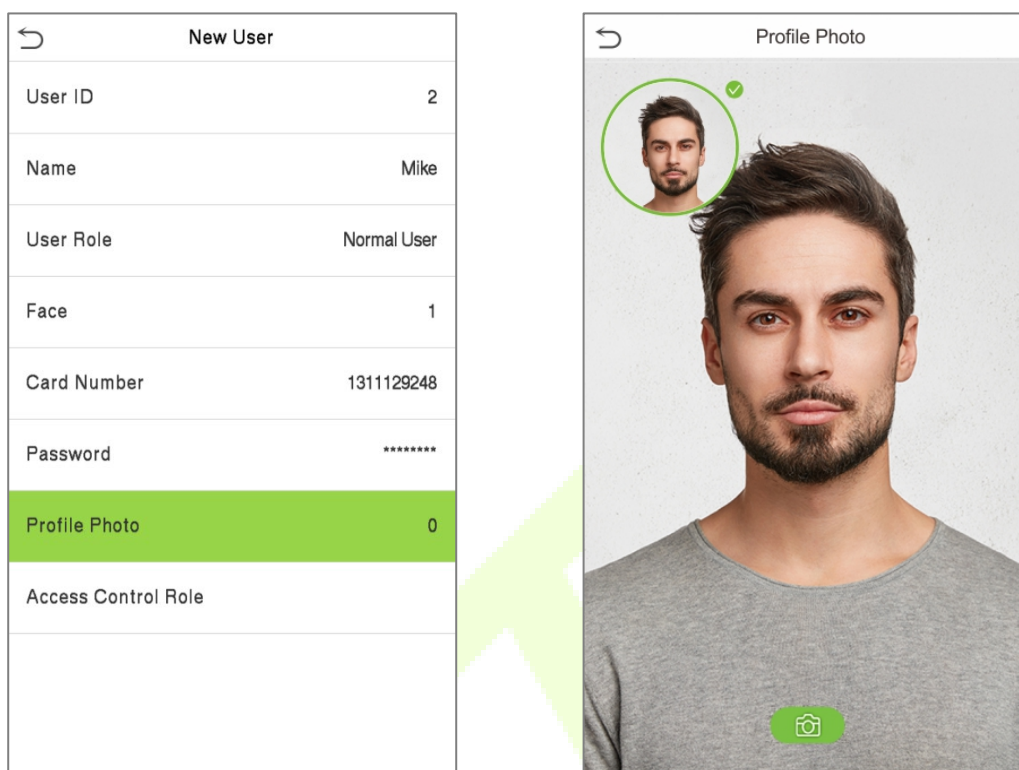
- On the Password interface, enter the required password and re-enter to confirm it and tap **OK**.
- If the re-entered password is different from the initially entered password, then the device prompts the message as "**Password not match!**", where the user needs to re-confirm the password again.



 **Note:** The password may contain 1 to 8 digits by default.

5.1.5 Profile Photo

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



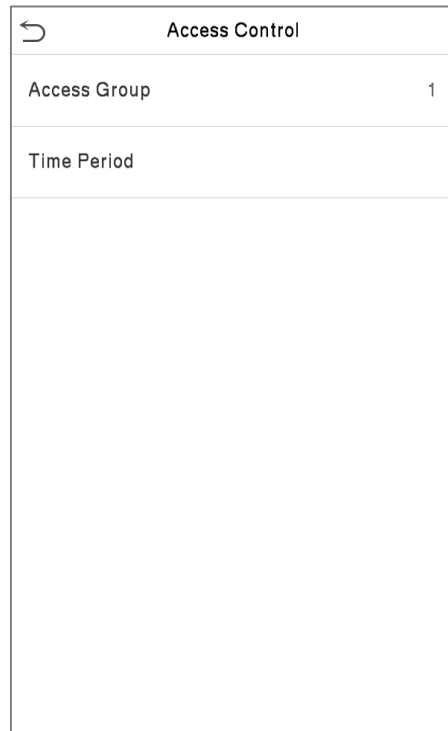
- When a user registered with a photo authenticates successfully, the user's registered photo is displayed.
- Tap **Profile Photo** to open the device's camera, then tap the camera icon to take a photo. The captured photo is displayed on the top left corner of the screen and the camera opens up again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

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

5.1.6 Access Control Role

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

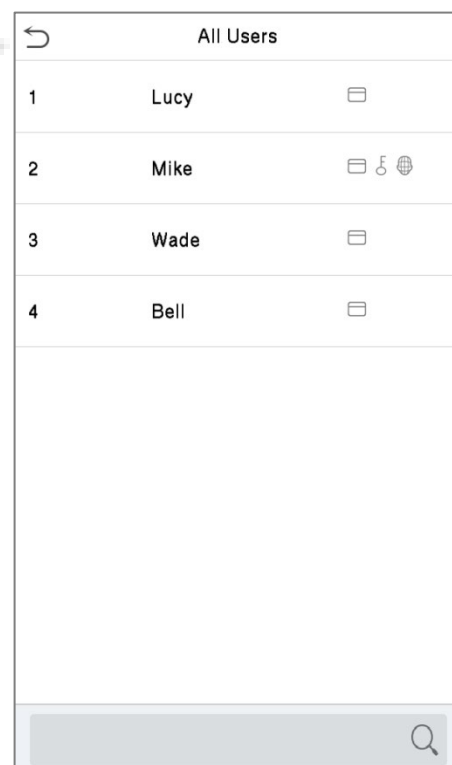
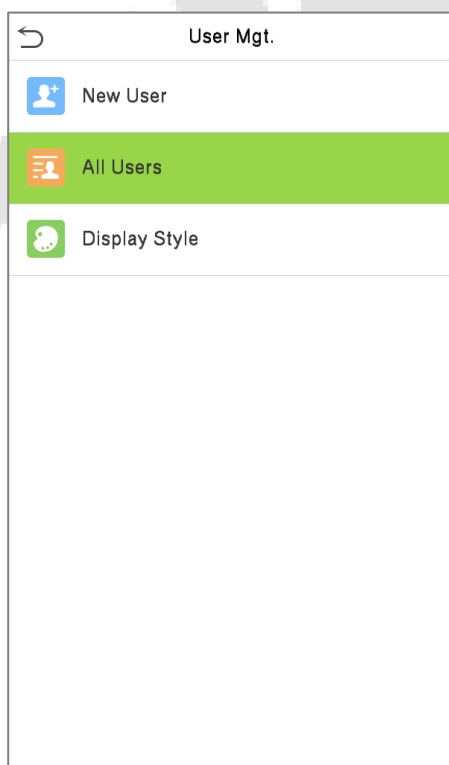
- Tap **Access Control Role > Access Group** to assign the registered users to different groups for better management. New users belong to Group 1 by default and can be reassigned to other groups. The device supports up to 99 Access Control groups.
- Tap **Time Period**, to select the time to use.



5.2 Search User

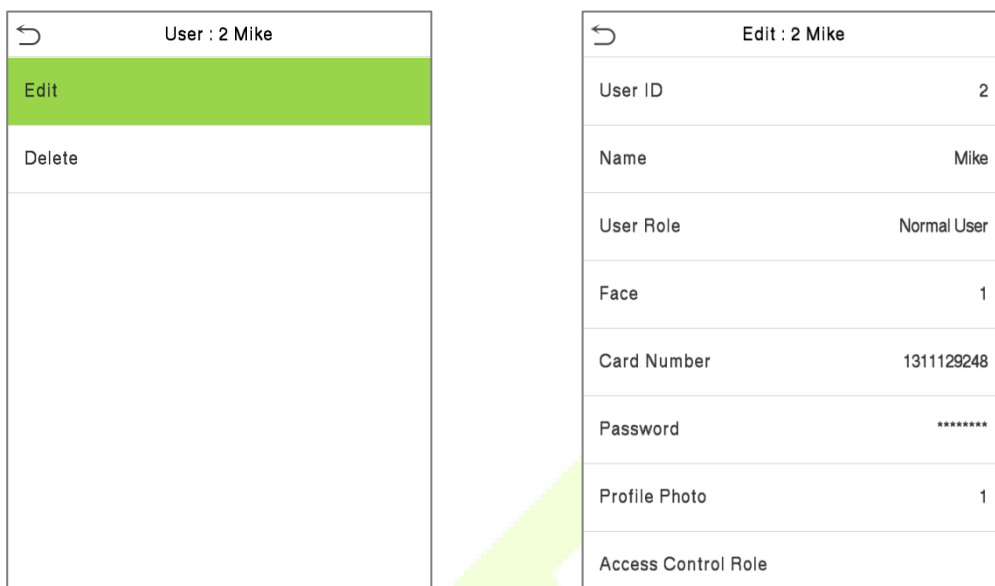
On the **Main Menu**, tap **User Mgt.**, and then tap **All Users** to search a User.

- 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.



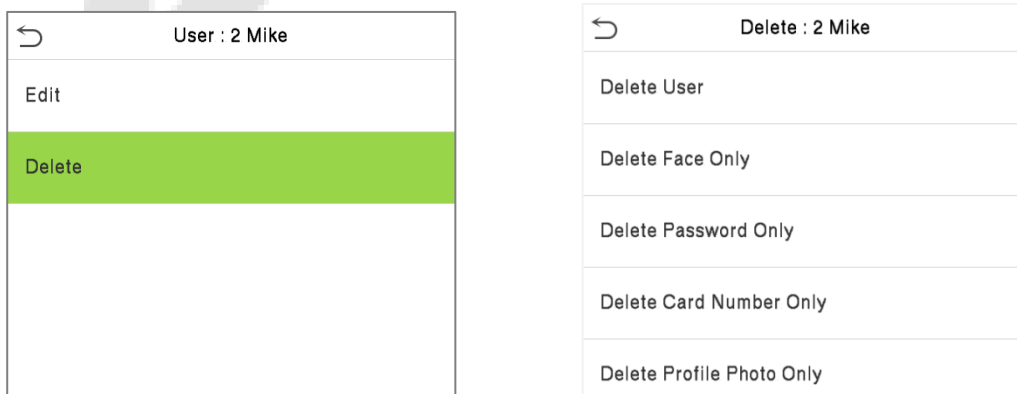
Note: The process of editing the user information is the same as adding a new user, except that the User ID cannot be modified when editing a user. The process in detail refers to "[5.1 User Registration](#)".

5.4 Delete User

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

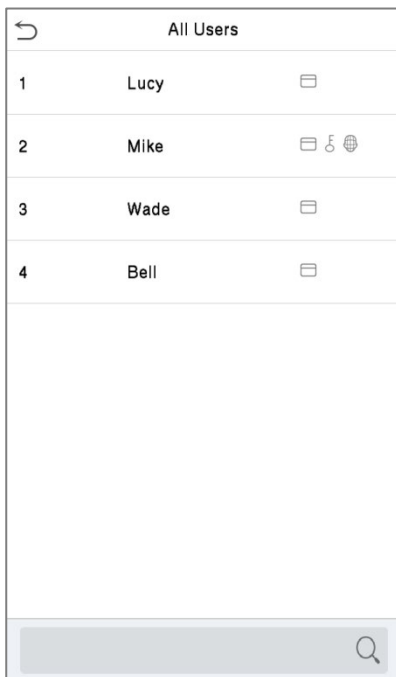


5.5 Display Style

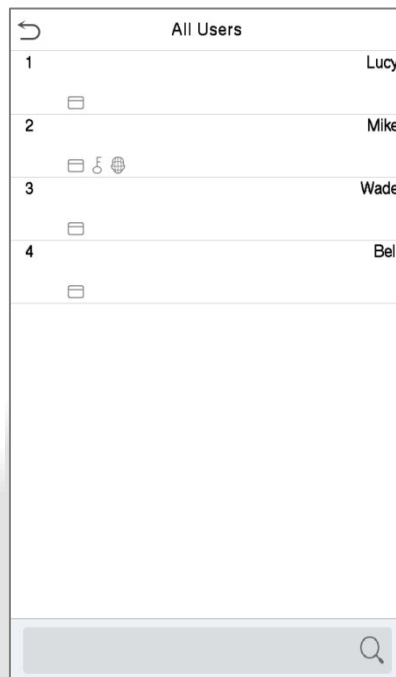
On the **Main Menu**, tap **User Mgt.**, and then tap **Display Style** to enter Display Style setting interface.



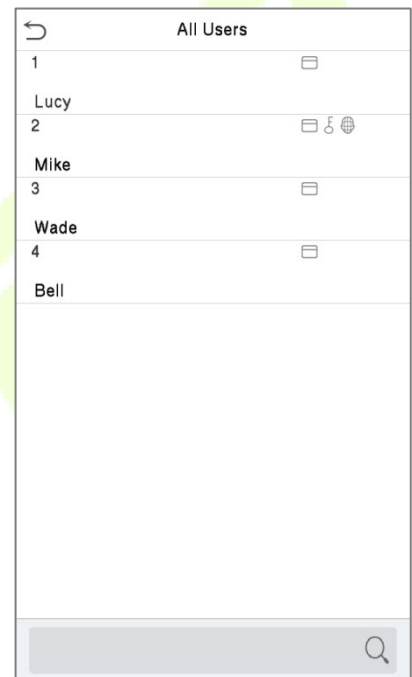
All the Display Styles are shown as below:



Single Line



Multiple Line

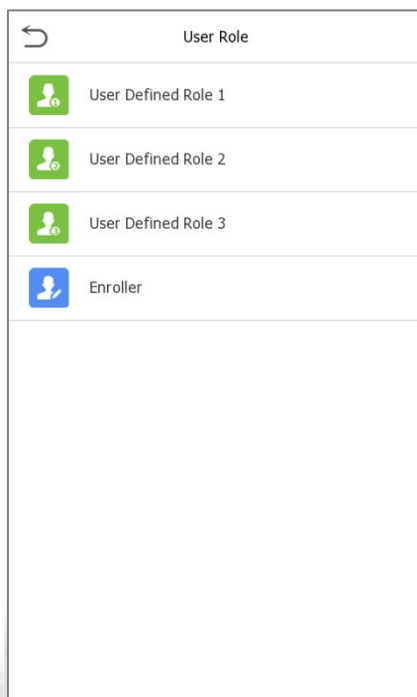


Mixed Line

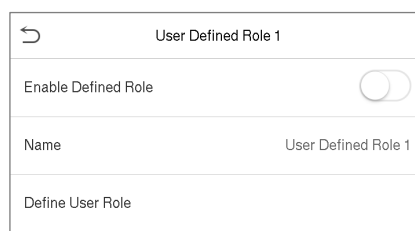
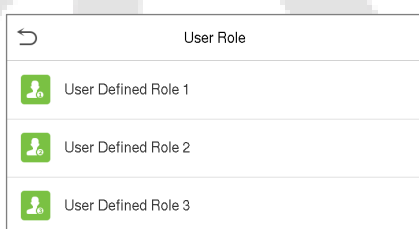
6 User Role

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 to 3 roles, that is, the custom operating scope of the menu functions of the user.



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



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

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 checked="" type="checkbox"/> Print	
<input type="checkbox"/> Autotest	
<input type="checkbox"/> System Info	

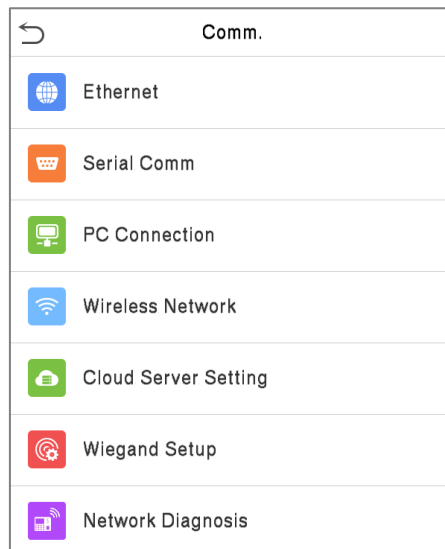
User Role
<input checked="" type="radio"/> Normal User
<input type="radio"/> User Defined Role 1
<input type="radio"/> Super Admin

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, Serial Comm, PC connection, Wireless Network, Cloud server, and Wiegand, Network Diagnosis.

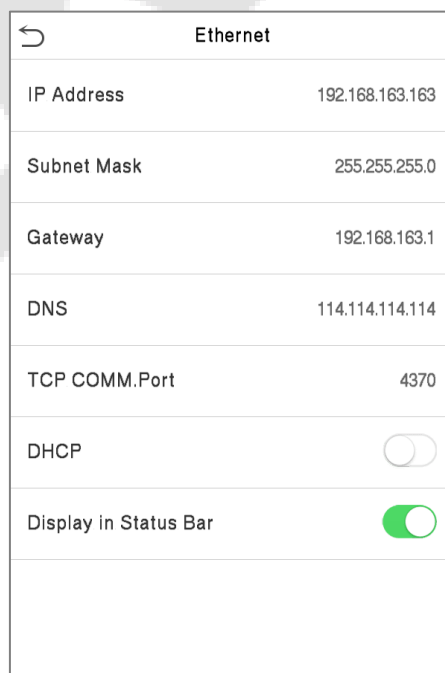
Tap **COMM.** on the main menu.



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 connect to the same network segment.

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



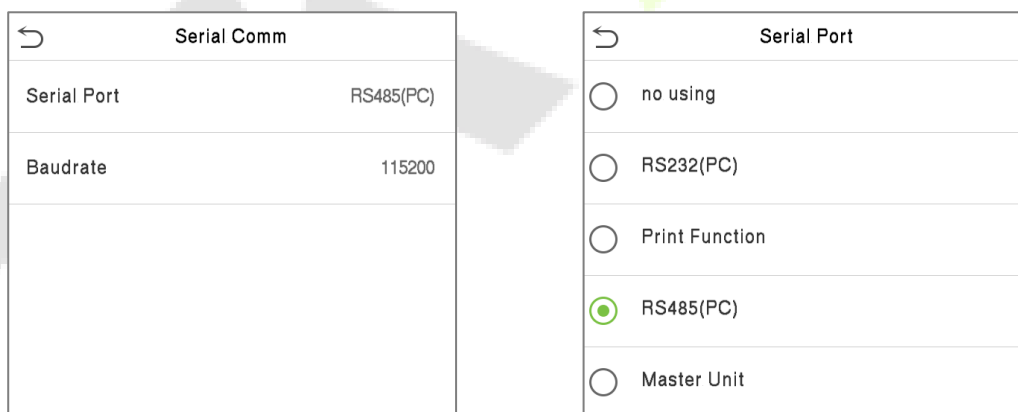
Function Description

Function Name	Descriptions
IP Address	The default IP address is 192.168.1.201. It can be modified according to the network availability.
Subnet Mask	The default Subnet Mask is 255.255.255.0. It can be modified according to the network availability.
Gateway	The default Gateway address is 0.0.0.0. It can be modified according to the network availability.
DNS	The default DNS address is 0.0.0.0. It can be modified according to the network availability.
TCP COMM. Port	The default TCP COMM Port value is 4370. It can be modified according to the network availability.
DHCP	Dynamic Host Configuration Protocol dynamically allocates IP addresses for clients via server.
Display in Status Bar	Toggle to set whether to display the network icon on the status bar.

7.2 Serial Comm

Serial Comm function establishes communication with the device through a serial port (RS232/ Printer/ RS485/ Master Unit).

Tap **Serial Comm.** on the **Comm.** Settings interface.



Function Description

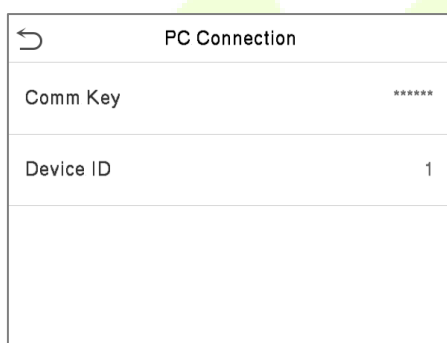
Function Name	Descriptions
Serial Port	<p>No Using: No communication with the device through the serial port.</p> <p>RS232(PC): Communicates with the device through the RS232 serial port.</p> <p>Print Function: The device can be connected to the printer when RS485 enables the print function.</p> <p>RS485(PC): Communicates with the device through the RS485 serial port.</p>

	Master Unit: When RS485 is used as the function of " Master unit ", it can be connected to a card reader.
Baud Rate	<p>There are 4 baud rate options at which the data communicates with PC. They are: 115200 (default), 57600, 38400, and 19200.</p> <p>The higher is the baud rate, the faster is the communication speed, but also the less reliable.</p> <p>Hence, a higher baud rate can be used when the communication distance is short; when the communication distance is long, choosing a lower baud rate is more reliable.</p>

7.3 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 Description

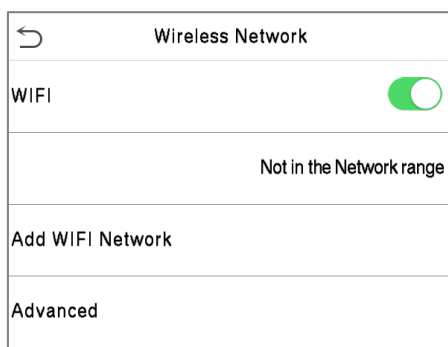
Function Name	Descriptions
Comm Key	The default password is 0 and can be changed. The Comm Key can contain 1-6 digits.
Device ID	It is the identification number of the device, which ranges between 1 and 254. If the communication method is RS232/RS485, you need to input this device ID in the software communication interface.

7.4 Wireless Network


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

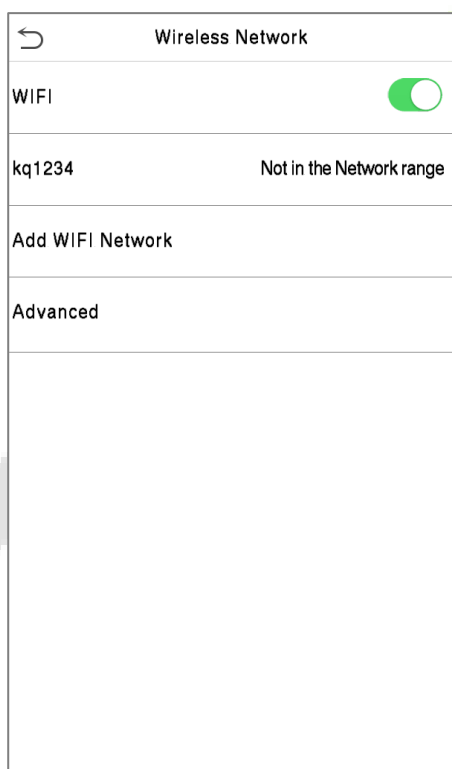
The WiFi module enables data transmission via WiFi (Wireless Fidelity) and establishes a wireless network environment. WiFi is enabled by default in the device. If you don't need to use the WiFi network, you can toggle the WiFi to disable the button.

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

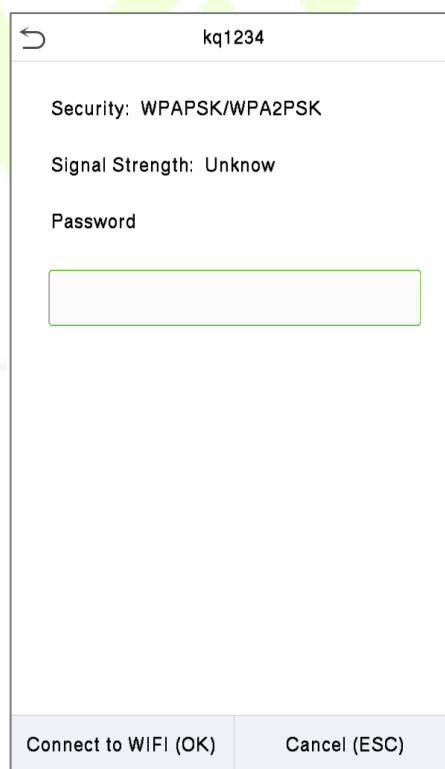


Searching the WiFi Network


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



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

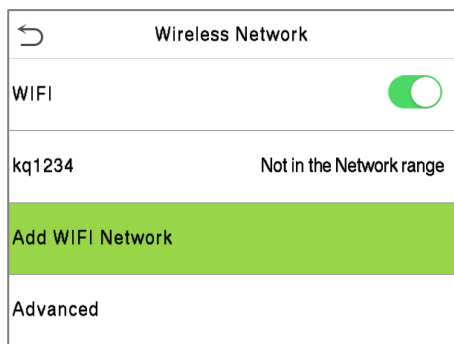


Tap on the password field to enter the password and tap on **Connect to WIFI (OK)**.

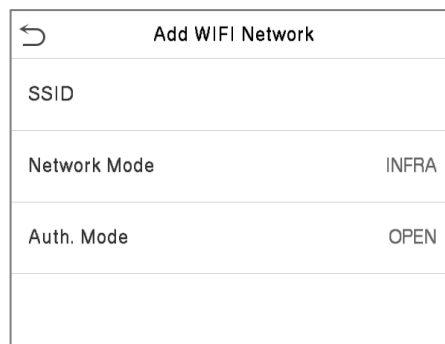
- When the WiFi is connected successfully, the initial interface will display the WiFi  logo.

Adding WiFi Network Manually

The WiFi can also be added manually if the required WiFi does not show on the list.



Tap on **Add WIFI Network** to add the WIFI manually.

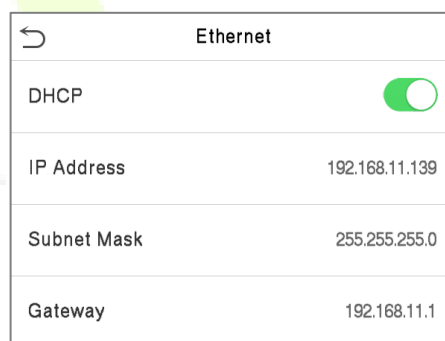
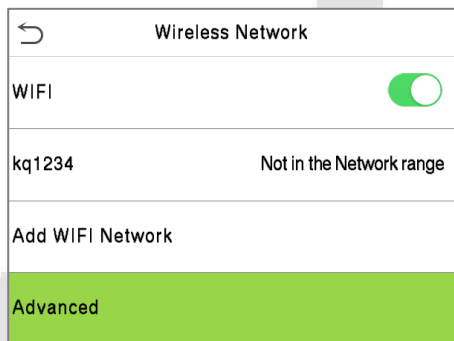


On this interface, enter the WiFi network parameters. (The added network must exist.)

Note: After successfully adding the WiFi manually, follow the same process to search for the added WiFi name. Click [here](#) to view the process to search the WiFi network.

Advanced Setting

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



Function Description

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

7.5 Cloud Server Settings

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

Cloud Server Setting	
Server Mode	ADMS
Enable Domain Name	<input type="checkbox"/>
Server Address	192.168.163.1
Server Port	8081
Enable Proxy Server	<input type="checkbox"/>
HTTPS	<input type="checkbox"/>

Function Description

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

7.6 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	

7.6.1 Wiegand input

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

Function Description

Function Name	Descriptions
Wiegand Format	Its value can be 26Bits, 34 Bits, 36 Bits, 37 Bits, 50 Bits and 64Bits.
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>ESSSSSSSCCCCCCCCCCCCCCO</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>EEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEE</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>ESSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSS</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>OFFFFFFFFFCCCCCCCCCCCCCCMMME</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>EFFFFFFFFFCCCCCCCCCCCCCCCO</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>OMMMSSSSSSSSSSSSSSSSSSSSSSSSSSSSSS</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>EMMMFFFFFFFSSSSSSSSSSSSSSSSSSSSSS</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>ESS</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>	

7.6.2 Wiegand output

Wiegand Options	
SRB	<input type="checkbox"/>
Wiegand Format	
Wiegand Output Bits	26
Failed ID	Disabled
Site Code	Disabled
Pulse Width(us)	100
Pulse Interval(us)	1000
ID Type	User ID

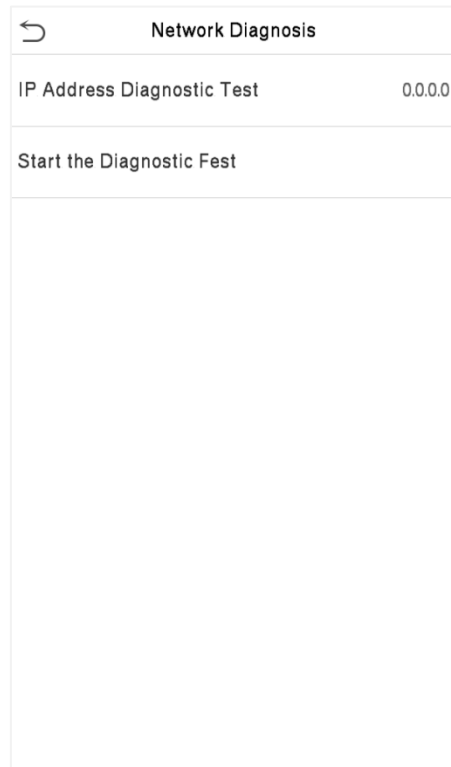
Function Description

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 26Bits, 34 Bits, 36 Bits, 37 Bits, 50 Bits and 64Bits.
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.

7.7 Network Diagnosis

It helps to set the network diagnosis parameters.

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



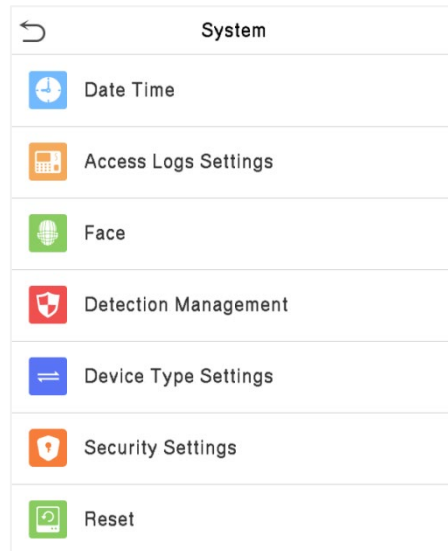
The screenshot shows a mobile application interface titled "Network Diagnosis". At the top left is a back arrow icon. Below the title, there is a text input field labeled "IP Address Diagnostic Test" with the value "0.0.0.0" entered. Below the input field is a button labeled "Start the Diagnostic Test". The interface is overlaid on a background with a large, faint watermark logo.

8 System Settings

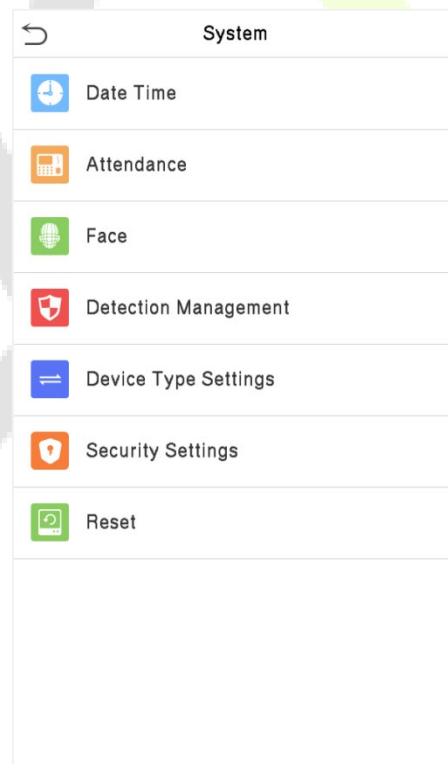
It helps to set related system parameters to optimize the accessibility of the device.

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

Access Control Terminal:

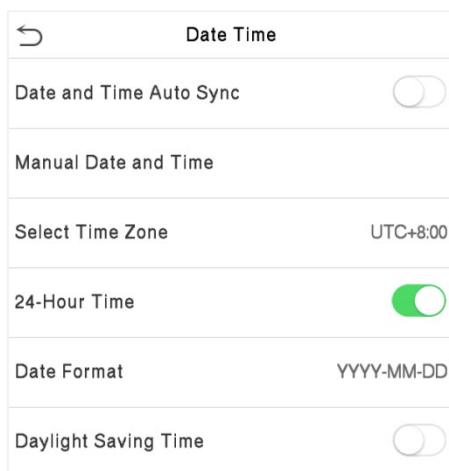


Time Attendance Terminal:



8.1 Date and Time

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



- Tap **Date and Time Auto Sync** to enable automatic time synchronization based on the service address you enter.
- Tap **Manual Date and Time** to manually set date and time and tap **Confirm** to save.
- Tap **Select Time Zone** to select a time zone then tap the return button to save and exit.
- Tap **24-Hour Time** to enable or disable this format. If enabled, then select the **Date Format** to set the date format i.e., the way date should be displayed on the device.
- Tap **Daylight Saving Time** to enable or disable the function. If enabled, tap **Daylight Saving Mode** to select a daylight-saving mode and then tap **Daylight Saving Setup** to set the switch time.

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

Week Mode

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

Date Mode

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

Note: For example, if a 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 remain at 18:30 on January 1, 2021.

8.2 Access Logs Setting and Attendance

Tap **Access Logs Setting** on the System interface.

Access Control Terminal:

Access Logs Setting	
Camera Mode	No photo
Display User Photo	<input checked="" type="checkbox"/>
Access Log Alert	99
Periodic Del of Access Logs	Disabled
Periodic Del of ATT Photo	99
Periodic Del of Blocklist Photo	99
Authentication Timeout(s)	3

Time Attendance Terminal:

Attendance	
Duplicate Punch Period(m)	1
Camera Mode	No photo
Display User Photo	<input checked="" type="checkbox"/>
Attendance Log Alert	99
Periodic Del of ATT Data	Disabled
Periodic Del of ATT Photo	99
Periodic Del of Blocklist Photo	99
Authentication Timeout(s)	3

Function Description of Access Control Terminal:

Function Name	Description
Camera Mode	<p>Choose whether to capture and save the current snapshot image during verification. 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	Choose whether to display the user photo when the user passes the verification.
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 ATT Photo	When attendance photos reach its maximum capacity, the device automatically deletes a set of old attendance photos. Users may disable the function or set a valid value between 1 and 99.
Periodic Del of Blocklist Photo	When block listed photos reach its maximum capacity, the device automatically deletes a set of old block listed photos. Users may disable the function or set a valid value between 1 and 99.
Authentication Timeout(s)	The amount of time taken to display a successful verification message. Valid value: 1 to 9 seconds.

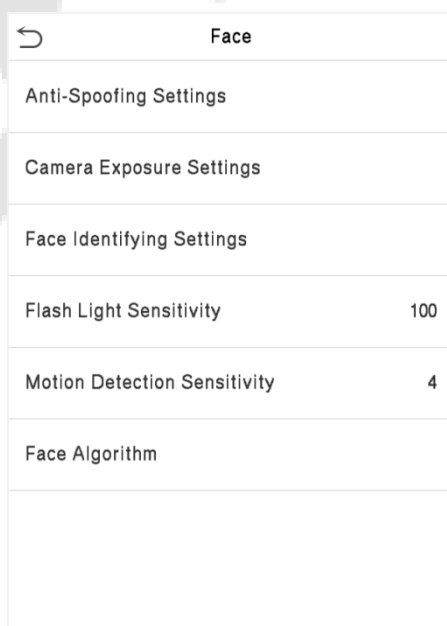
Function Description of Time Attendance Terminal:

Function Name	Description
Duplicate Punch Period(m)	Within a set time period (unit: minutes), the duplicated attendance record will not be reserved (value ranges from 1 to 999999 minutes).
Camera Mode	<p>Choose whether to capture and save the current snapshot image during verification. 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</p>

	<p>verification.</p> <p>Save on failed verification: Photo is taken and saved only for each failed verification.</p>
Display User Photo	<p>This function is disabled by default. When enabled, a security prompt will pop-up.</p>
Attendance Log Alert	<p>When the record space of the attendance reaches the maximum threshold value, the device automatically displays the memory space warning.</p> <p>Users may disable the function or set a valid value between 1 and 9999.</p>
Periodic Del of ATT Data	<p>When attendance records reach its maximum storage capacity, the device automatically deletes a set of old attendance records.</p> <p>Users may disable the function or set a valid value between 1 and 999.</p>
Periodic Del of ATT Photo	<p>When attendance photos reach its maximum storage capacity, the device automatically deletes a set of old attendance photos.</p> <p>Users may disable the function or set a valid value between 1 and 99.</p>
Periodic Del of Blocklist Photo	<p>When block listed photos reach its maximum storage capacity, the device automatically deletes a set of old block listed photos.</p> <p>Users may disable the function or set a valid value between 1 and 99.</p>
Authentication Timeout(s)	<p>The amount of time taken to display a successful verification message.</p> <p>Valid value: 1~9 seconds.</p>

8.3 Face Parameters

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



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

Function Description

Function Name	Description
Anti-Spoofing Settings	<p>2D Monocular Anti-Spoofing: 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.</p> <p>2D Monocular Anti-Spoofing 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.</p> <p>2D Binocular Anti-Spoofing: It uses near-infrared spectra imaging to identify and prevent fake photos and videos attack.</p> <p>2D Binocular 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.</p> <p>Note: For the Anti-Spoofing settings, the user needs to enable both 2D Monocular Anti-Spoofing and 2D Binocular Anti-Spoofing. By default, when one of the switches is turned on, the other one would be turned on simultaneously.</p> <p>When the option is turned on or off, the device reboots automatically to execute the function.</p>
Camera Exposure Settings	<p>Face AE: In the Face AE mode, when the face is in front of the camera, the brightness of the face area increases, and other areas become darker.</p> <p>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.</p> <p>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.</p>
Face Identifying Settings	<p>1:N Threshold Value: Under 1:N verification mode, the verification will only be successful when the similarity between the acquired facial image and all registered facial templates is greater than the set value.</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 90.</p>

1:1 Threshold Value: Under 1:1 verification mode, the verification will only be successful when the similarity between the acquired facial image and the user's facial templates enrolled in the device is greater than the set value.

The valid value ranges from 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 88.

Face Enrollment Threshold: During face enrollment, 1:N comparison is used to determine whether the user has already registered before.

When the similarity between the acquired facial image and all registered facial templates is greater than the set threshold, it indicates that the face has already been registered.

1: N Match Threshold for Masked People: The recognition rate of mask wearing under the setting of 1:N verification mode. The higher the thresholds, the lower are the misjudgement rate, and higher is the rejection rate, and vice versa. It is recommended to set the default value of 68.

Face Pitch Angle: It is the pitch angle tolerance of a face for facial template registration and comparison.

If a face's pitch angle exceeds the set value, it will be filtered by the algorithm, i.e., ignored by the terminal thus no registration and comparison interface will be triggered.

Face Rotation Angle: It is the rotation angle tolerance of a face for facial template registration and comparison.

If a face's rotation angle exceeds the set value, it will be filtered by the algorithm, i.e., ignored by the terminal thus no registration and comparison interface will be triggered.

Image Quality: It is the image quality for facial registration and comparison. The higher the value, the clearer image is required.

Minimum Face Size: It sets the minimum face size required for facial registration and comparison.

If the minimum size of the captured image is smaller than the set value, then it will be filtered off and not recognized as a face.

This value can also be interpreted as the face comparison distance. The farther the individual is, the smaller the face, and the smaller number of pixels of the face obtained by the algorithm. Therefore, adjusting this parameter can adjust the farthest comparison distance of faces. When the value is 0, the face comparison distance is not limited.

	<p>Identifying Mode</p>	<p>Multi-face Identifying: When it is toggled on, the device can identify multiple faces at once. The Content Mode to Display, and Count to Display can be configured only if it is toggled on.</p> <p>Content Mode to Display: You can select the content displayed below the user photo in the interface after the face verification is successful. Such as only display the User ID, display the Name, display the User ID + Name, display Timestamp, display User ID + Timestamp, display Name + Timestamp.</p> <p>Count to Display: You can choose the number of face verification results to be displayed in the interface at once, e.g., if set to 3, the interface displays up to 3 successful user verifications at once.</p> <p>Note: The Count to Display can be set from 1 to 4 users.</p> <p>Discrete Identifying: The same face can only be recognized once. To recognize it again, you must leave the face recognition area and re-enter it before it can be recognized again.</p>
	<p>Face Comparison 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.</p>	
<p>Flash Light Sensitivity</p>	<p>This value controls the turning on and off of the LED light. The larger the value, the LED light will turn on or off frequently.</p>	
<p>Motion Detection Sensitivity</p>	<p>It sets the value for change in a camera’s field of view known as potential motion detection that wakes up the terminal from standby to the comparison interface.</p> <p>The larger the value, the more sensitive the system would be, i.e., if a larger value is set, the comparison interface activates with much ease, and the motion detection is frequently triggered.</p>	
<p>Face Algorithm</p>	<p>It has facial algorithm related information and pause facial template update.</p>	

 **Note:**

1. 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.

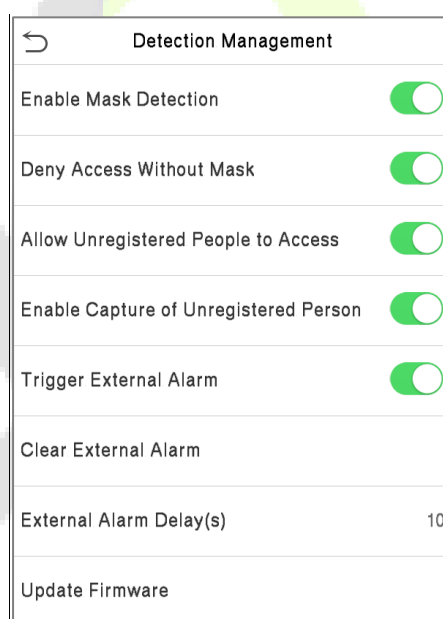
2. Face AE and Multi-face identifying are mutually exclusive options. When the Multi-face identifying feature switch is turned on, the Face AE switch will be automatically turned off. If you turn on Face AE at this time, the recognition mode will change to single face recognition mode.
3. The Face comparison interval and Tracking identification are mutually exclusive options. If the Tracking identification switch is turned on, the Face comparison interval function in the Face Identifying Settings will be disabled, and vice versa.

Process to modify the Facial Recognition Accuracy

- On the **System** interface, tap on **Face > Anti-Spoofing Settings** and then toggle to enable 2D Monocular Anti-Spoofing and 2D Binocular Anti-Spoofing to set the anti-spoofing.
- Then, on the **Main Menu**, tap **Auto-Test > 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 Detection Management

Tap **Detection Management** on the **System** interface to configure the Detection Management settings.



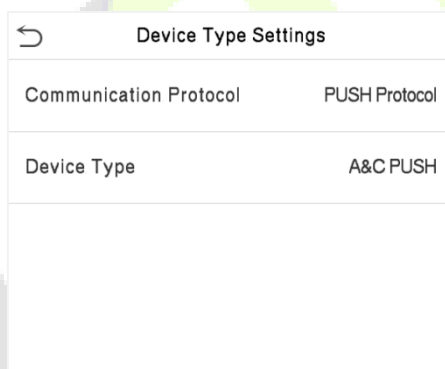
Function Description

Function Name	Description
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 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 unregistered person. When enabled, the device allows the person to enter without registration.
Enable Capture of Unregistered Person	To enable or disable capturing the unregistered person. When enabled, the device will automatically capture the photo of the unregistered 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.
Update Firmware	Update the detection firmware version.


8.5 Device Type Settings

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



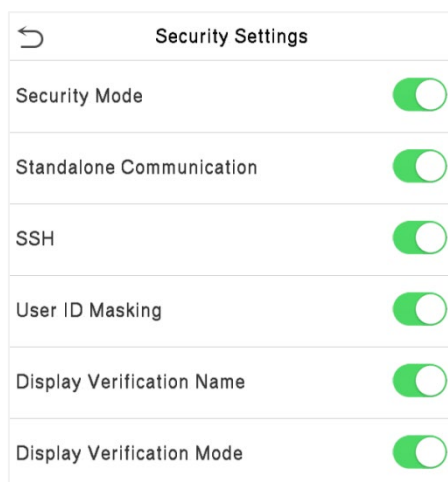
Function Description

Menu	Descriptions
Communication Protocol	Set the PUSH protocol.
Device Type	Set the device as a time attendance terminal or access control terminal.

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

8.6 Security settings

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



Function Description

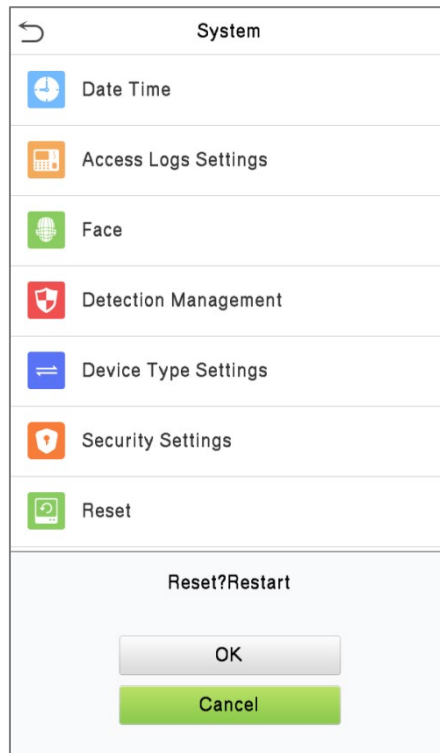
Function Name	Description
Security Mode	Select whether to enable the security mode to protect the device and the user's personal information. You can set the device to work offline and hide the user's personal information to prevent leakage during user verification.
Standalone Communication	To avoid being unable to use when the device is offline, you can download the C/S software (such as ZKAccess 3.5) on your computer in advance for offline use.
SSH	SSH is used to enter the background of the device for maintenance.
User ID Masking	When enabled, and then the user is successfully compared and verified, the User ID in the displayed verification result will be replaced with an * to achieve secure protection of sensitive private data.
Display Verification Name	Set whether to display the username in the verification result interface.
Display Verification Mode	Set whether to display the verification mode in the verification result interface.

8.7 Factory Reset

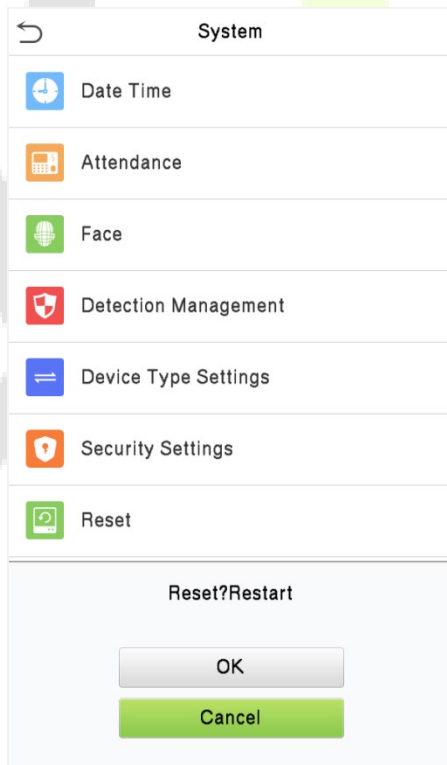
The Factory Reset function restores the device settings such as communication settings and system settings, to the default factory settings (this function does not clear registered user data).

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

Access Control Terminal:

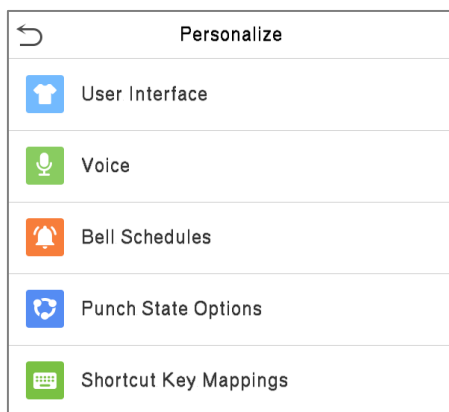


Time Attendance Terminal:



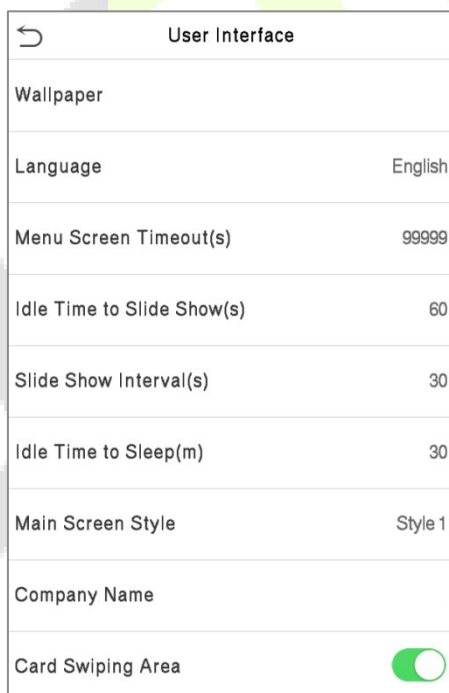
9 Personalize Settings

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



9.1 Interface Settings

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



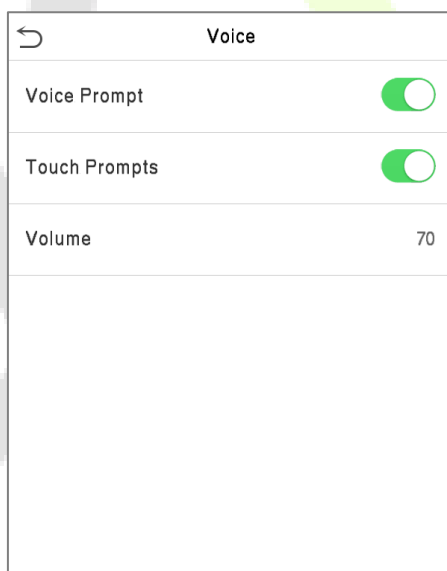
Function Description

Function Name	Description
Wallpaper	It helps to select the main screen wallpaper according to the user preference.
Language	It helps to select the language of the device.

Menu Screen 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.
Company Name	Enter the company name here. When the company name option is turned on in the print information setting, the company name is printed.
Card Swiping Area	Enable/disable the card swipe area icon on the standby interface.

9.2 Voice Settings

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



Function Description

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

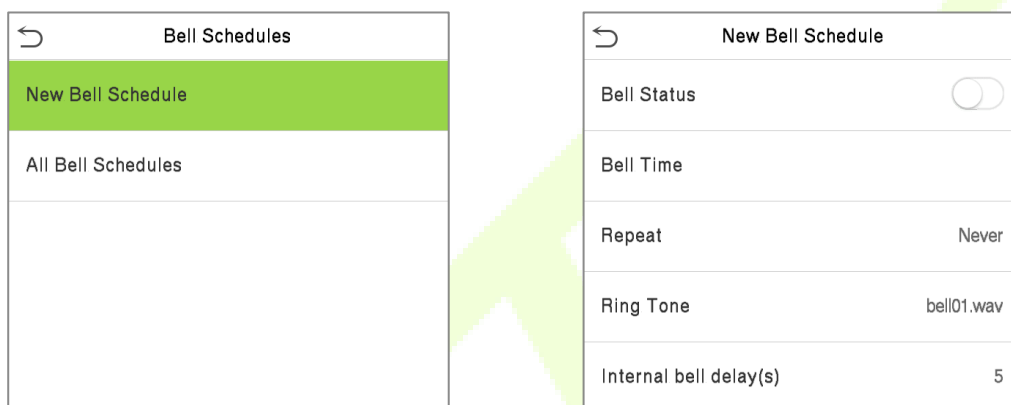
9.3 Bell Schedules

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.



Function Description

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

All Bell Schedules

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

Edit the scheduled bell

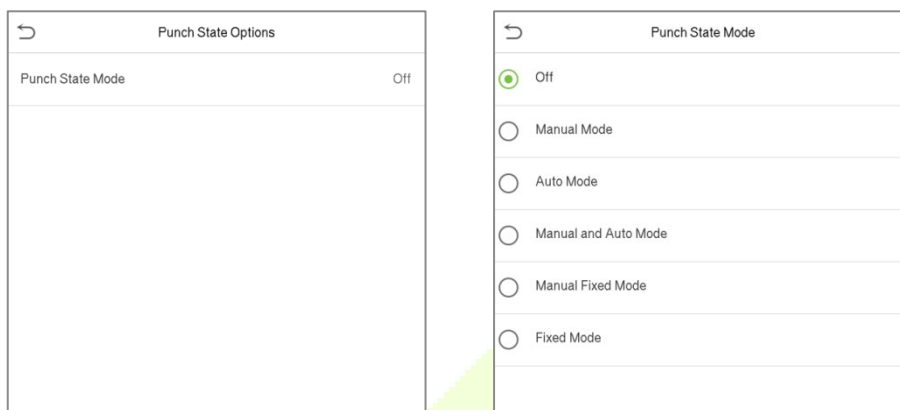
On the **All Bell Schedules** interface, tap on the required bell schedule, and tap **Edit** to edit the selected bell schedule. The editing method is the same as the operations of adding a new bell schedule.

Delete a bell

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.



Function Description

Function Name	Description
<p>Punch State Mode</p>	<p>Off: Disable the punch state function. Therefore, the punch state key set under Shortcut Key Mappings menu will become invalid.</p> <p>Manual Mode: Switch the punch state key manually, and the punch state key will disappear after Punch State Timeout.</p> <p>Auto Mode: The punch state key will automatically switch to a specific punch status according to the predefined time schedule which can be set in the Shortcut Key Mappings.</p> <p>Manual and Auto Mode: The main interface will display the auto-switch punch state key. However, the users will still be able to select alternative that is the manual attendance status. After timeout, the manual switching punch state key will become auto-switch punch state key.</p> <p>Manual Fixed Mode: After the punch state key is set manually to a particular punch status, the function will remain unchanged until being manually switched again.</p> <p>Fixed Mode: Only the manually fixed punch state key will be shown. Users cannot change the status by pressing any other keys.</p>

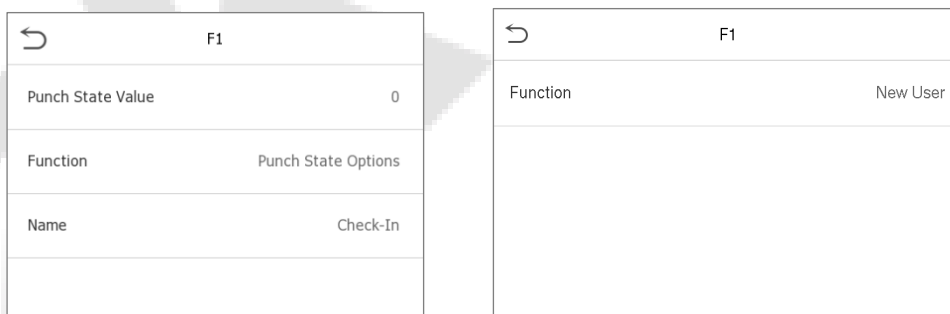
9.5 Shortcut Key Mappings

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

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

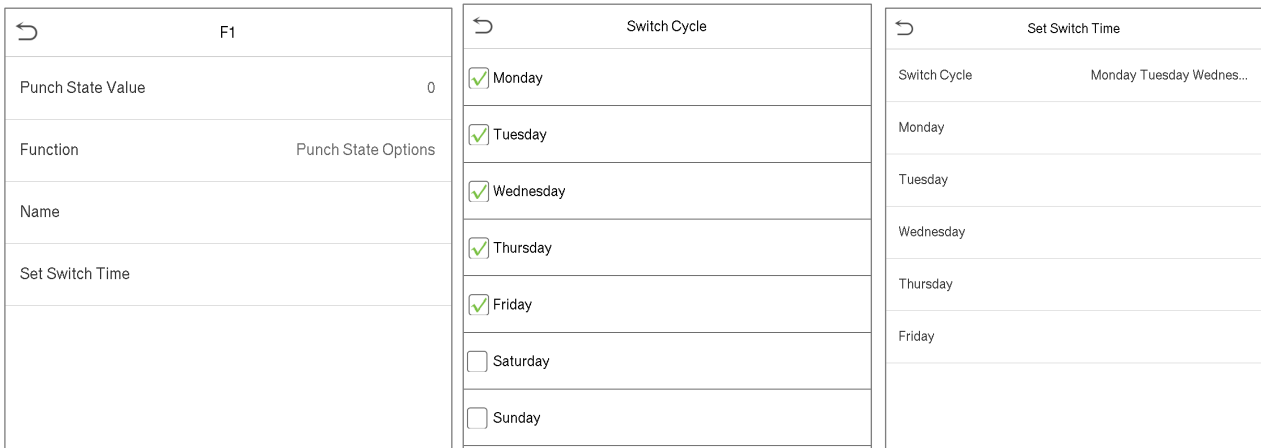
- On the **Shortcut Key Mappings** interface, tap on the required shortcut key to configure the shortcut key settings.
- On the **Shortcut Key** (that is "F1") interface, tap **function** to set the functional process of the shortcut key either as punch state key or function key.
- If the Shortcut key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



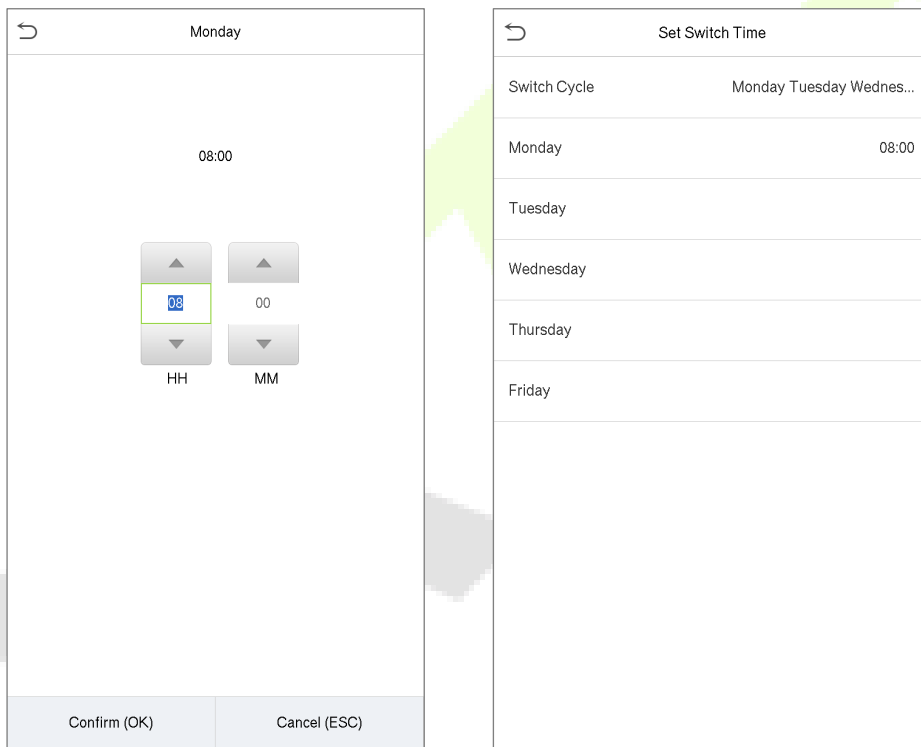
- If the Shortcut key is set as a punch state key (such as check in, check out, etc.), then it is required to set the punch state value (valid value 0~250), name.

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.



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



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

10 Data Management

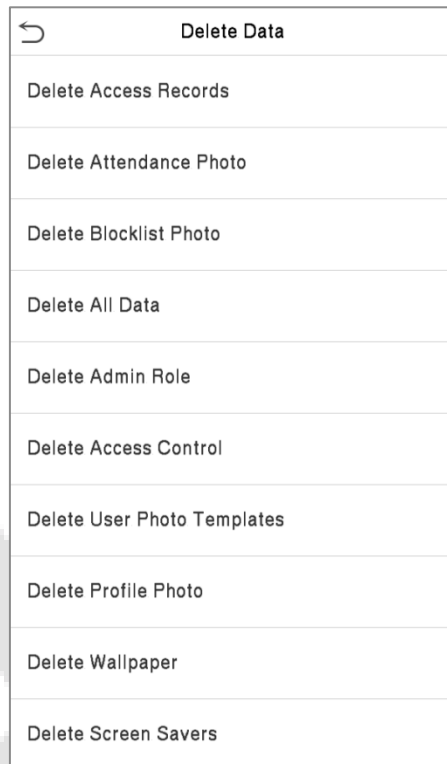
On the **Main Menu**, tap **Data Mgt.** to delete the relevant data in the device.



10.1 Delete Data

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

Access Control Terminal:



Time Attendance Terminal:

Delete Data
Delete Attendance Data
Delete Attendance Photo
Delete Blocklist Photo
Delete All Data
Delete Admin Role
Delete Access Control
Delete User Photo Templates
Delete Profile Photo
Delete Wallpaper
Delete Screen Savers

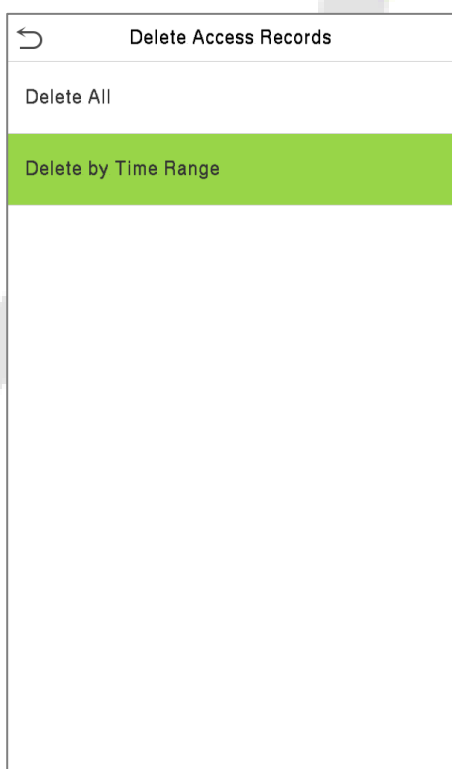
Function Description of Access Control Terminal:

Function Name	Description
Delete Access Records	To delete 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 the information and 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 all the user photo templates on the device.
Delete Profile Photo	To delete all user photos on the device.
Delete Wallpaper	To delete all wallpapers in the device.
Delete Screen Savers	To delete the screen savers in the device.

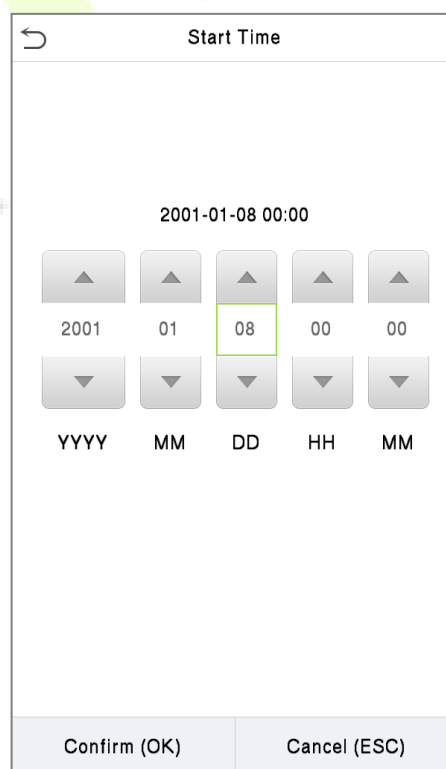
Function Description of Time Attendance Terminal:

Function Name	Description
Delete Attendance Data	To delete attendance data conditionally.
Delete Attendance Photo	To delete attendance photos of designated personnel.
Delete Blocklist Photo	To delete the photos taken during failed verifications.
Delete All Data	To delete the information and attendance data 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 all the user photo templates on the device.
Delete Profile Photo	To delete all user photos on the device.
Delete Wallpaper	To delete all wallpapers in the device.
Delete Screen Savers	To delete the screen savers in the device.

The user may select Delete All or Delete by Time Range when deleting the access records/attend data, 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.

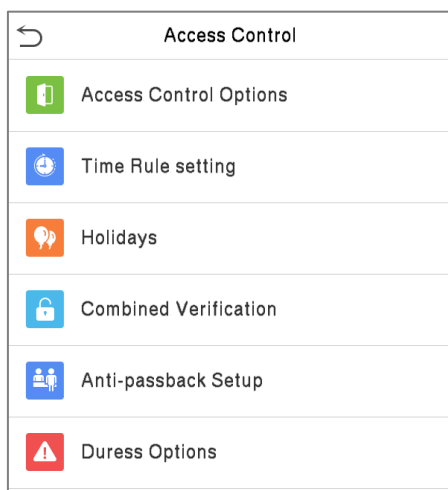


Set the time range and tap **OK**.

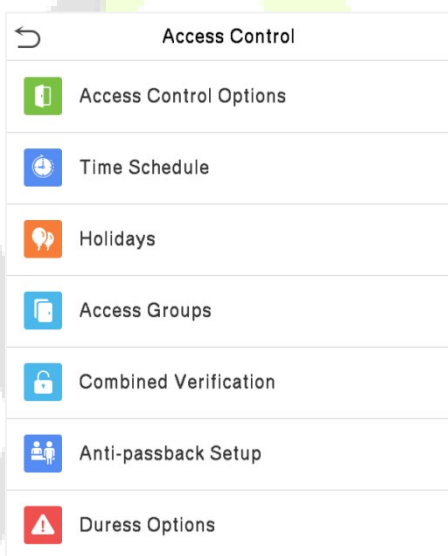
11 Access Control

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:

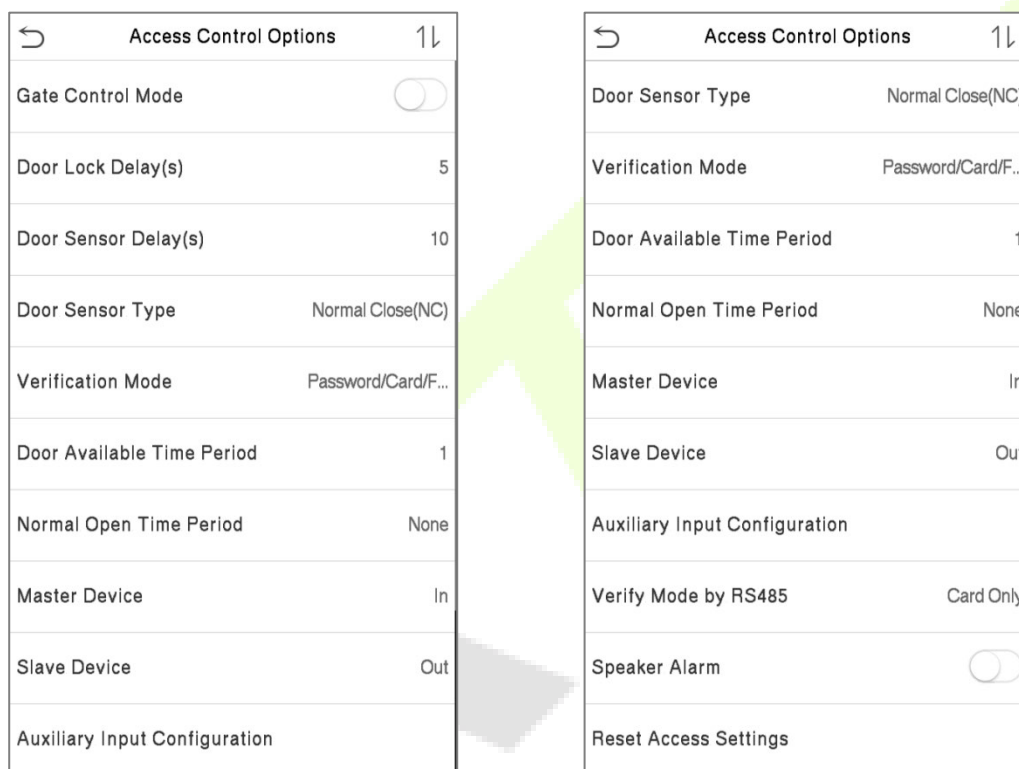
- The relevant door's current unlock time should be within any valid time zone of the user's time period.
- The corresponding user's group must be already set in the door unlock combination (and if there are other groups, being set in the same access combo, then the verification of those group's members 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.

11.1 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 Description of Access Control Terminal:

Function Name	Description
Gate Control Mode	It toggles between ON or OFF switch to get into gate control mode or not. When set to ON , the interface removes the Door lock 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 to 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	<p>There are three Sensor types: None, Normal Open(NO), and Normal Closed(NC).</p> <p>None: It means the door sensor is not in use.</p> <p>Normally Open(NO): It means the door is always left open when electric power is on.</p> <p>Normally Closed(NC): It means the door is always left closed when electric power is on.</p>
Verification Mode	The supported verification mode includes Password/Card/Face, User ID Only, Password, Card Only, Password+Card, Password/Card, Face Only, Face+Password, Face+Card.
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	<p>While configuring the master and slave devices, you may set the state of the master as Out or In.</p> <p>Out: A record of verification on the master device is a check-out record.</p> <p>In: A record of verification on the master device is a check-in record.</p>
Slave Device	<p>While configuring the master and slave devices, you may set the state of the slave as Out or In.</p> <p>Out: A record of verification on the slave device is a check-out record.</p> <p>In: A record of verification on the slave device is a check-in record.</p>
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.
Verify Mode by RS485	<p>The verification mode is used when the device is used either as a host or slave.</p> <p>The supported verification mode includes Card only, and Card + Password.</p>
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	
Verify Mode by RS485	Card Only
Valid Holidays	<input type="checkbox"/>

Access Control Options	
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	
Verify Mode by RS485	Card Only
Valid Holidays	<input type="checkbox"/>
Speaker Alarm	<input type="checkbox"/>
Reset Access Settings	

Function Description of Time Attendance Terminal:

Function Name	Description
Door Lock Delay (s)	The length of time that the device controls the electric lock to be in unlock state. Valid value: 1 to 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.
Verify Mode by RS485	The verification mode is used when the device is used either as a host or slave. The supported verification mode includes Card only, and Card + Password.
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.
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.

11.2 Time Rule Setting and Time Schedule

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

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**.

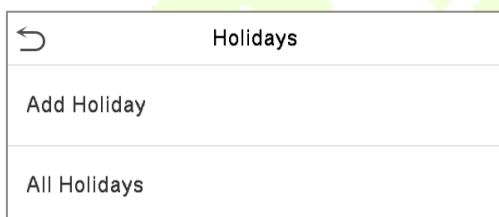
Note:

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

11.3 Holidays

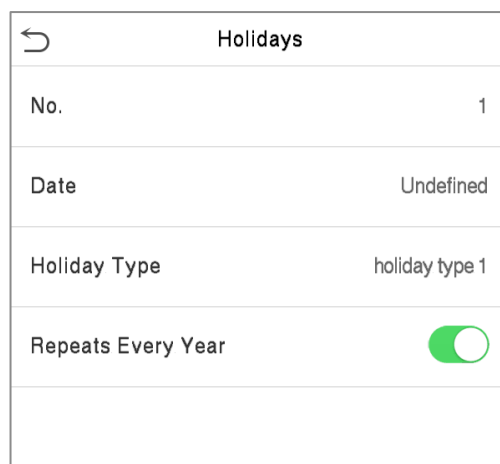
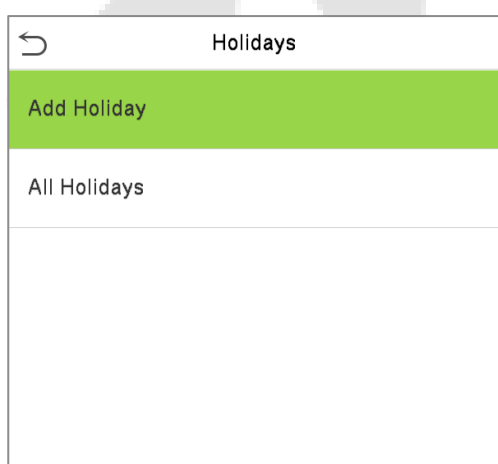
Whenever there is a holiday, you may need a distinct access time; but changing everyone's access time one by one is extremely cumbersome, so a holiday access time can be set that applies to all employees and the user will be able to open the door during the holidays.

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

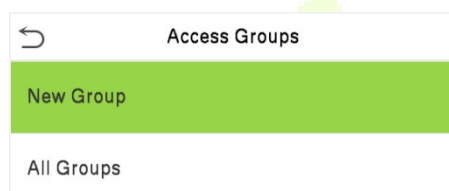
On the **Holidays** interface, select a holiday item to be deleted and tap **Delete**. Press **OK** to confirm the deletion. After deletion, this holiday does not display on the **All Holidays** interface.

11.4 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"/>

📌 Note:

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.

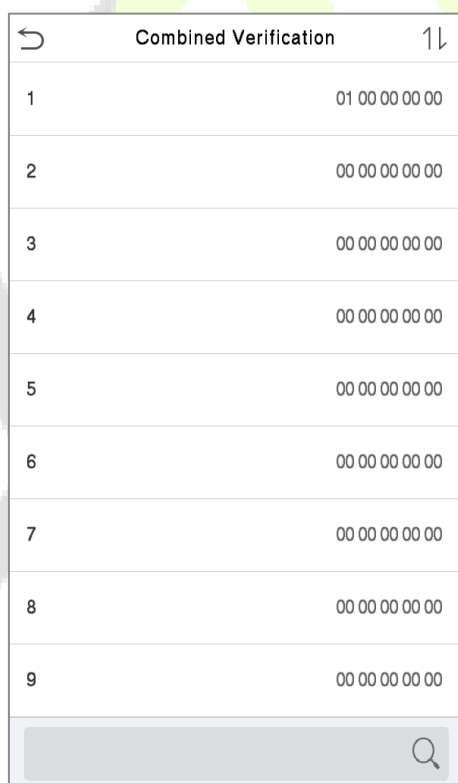
- **Delete a Group:**

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.

11.5 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

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

For Example:

- 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.

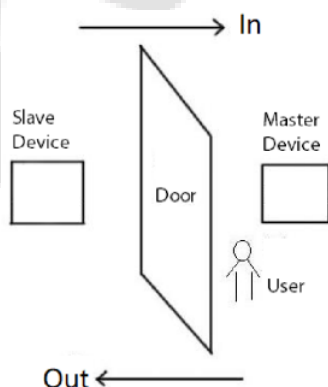
Note: To delete the door-unlock combination, set all Door-unlock combinations to 0.

11.6 Anti-Passback Setup

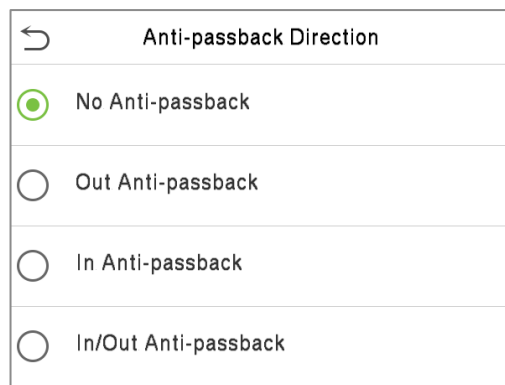
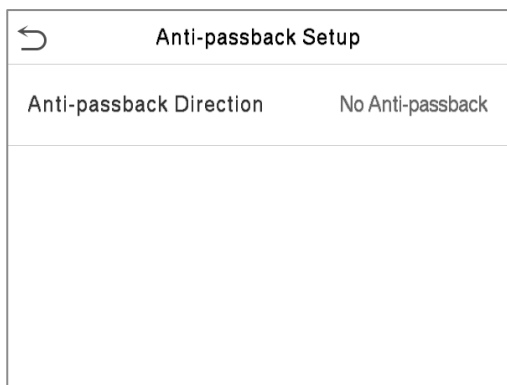
A user may be followed by some person(s) to enter the door without verification, resulting in a security breach. So, to avoid such situations, the Anti-Passback option was developed. Once it is enabled, the check-in and check-out record must occur alternatively to open the door to represent a consistent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

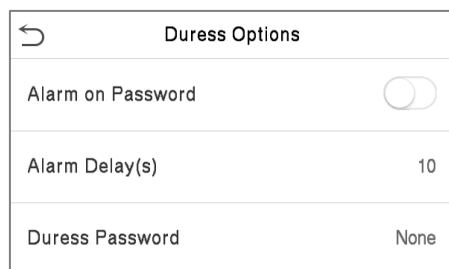
Function Name	Description
Anti-Passback Direction	<p>No Anti-Passback: The Anti-Passback function is disabled, which means successful verification through either the master device or slave device can unlock the door. The attendance state is not saved in this option.</p> <p>Out Anti-Passback: The user 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>

11.7 Duress Options

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:



Time Attendance Terminal:

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

Function Description of Access Control Terminal:

Function Name	Description
Alarm on Password	When a user uses the password verification method, an alarm signal is generated only when the password verification is successful otherwise there is no alarm signal.
Alarm Delay (s)	The alarm signal does not transmit until the alarm delay time elapses. 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 is generated.

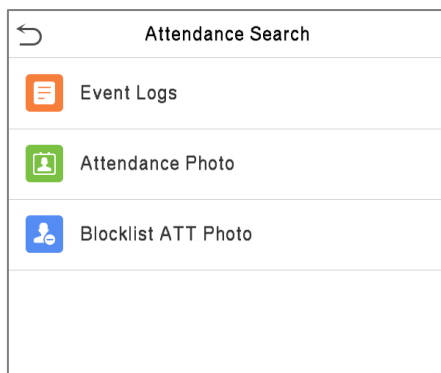
Function Description of Time Attendance Terminal:

Function Name	Description
Alarm on Password	When a user uses the password verification method, an alarm signal is generated only when the password verification is successful otherwise there is no alarm signal.
Alarm Delay (s)	The alarm signal does not transmit until the alarm delay time elapses. The value ranges from 1 to 999 seconds.

12 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.

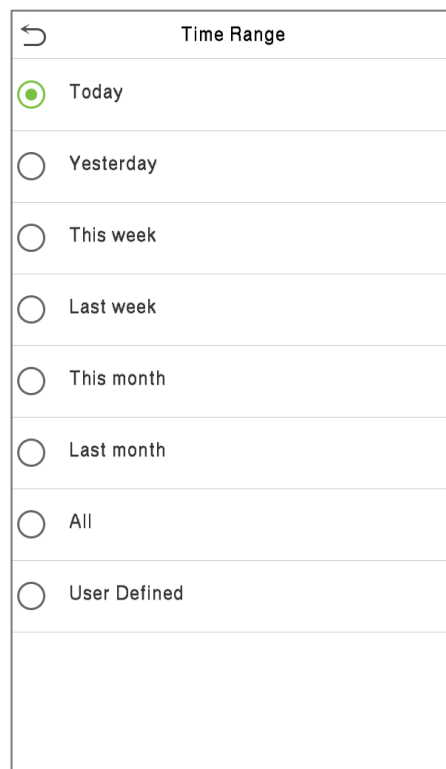
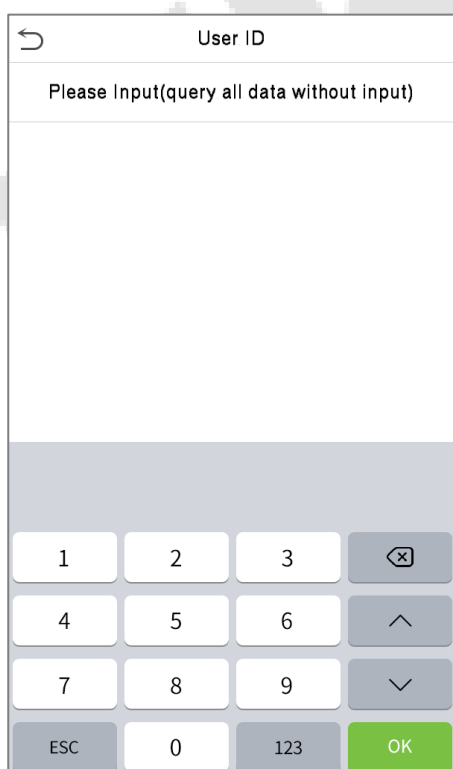
Select **Attendance Search** on the **Main Menu** interface to search for the required event logs.



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

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

1. Enter the user ID to be searched and 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.

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

Personal Record Search	
Date	User ID
11-09	Number of Records:48
0	17:15 16:10 16:09 16:09 16:09
	16:09 16:09 16:09 16:09 15:10
	15:01 15:01 15:01 12:57 12:07
2	16:09 16:09 16:09 16:09 15:29
	15:27 15:27 15:27 15:27 12:16
	12:16 12:16 12:16 12:16 12:16
	12:16 12:16 12:12 12:12 12:12
	12:12 12:12 12:12 12:12 12:11
	12:11 12:08 12:07 12:07 12:07
	12:07 12:07 12:07
11-08	Number of Records:05
1	15:00 15:00 15:00 15:00
0	15:00

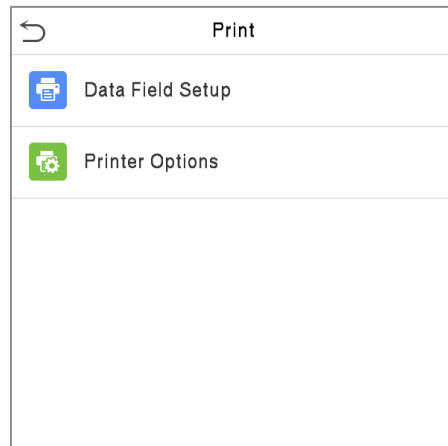
Personal Record Search				
User ID	Name	Time	Mode	State
2	Mike	11-09 16:09 15	15	1
2	Mike	11-09 16:09 15	15	1
2	Mike	11-09 16:09 25	25	0
2	Mike	11-09 16:09 25	25	0
2	Mike	11-09 15:29 3	3	0
2	Mike	11-09 15:27 15	15	0
2	Mike	11-09 15:27 15	15	0
2	Mike	11-09 15:27 15	15	0
2	Mike	11-09 15:27 3	3	0
2	Mike	11-09 12:16 15	15	0
2	Mike	11-09 12:16 15	15	0
2	Mike	11-09 12:16 15	15	0
2	Mike	11-09 12:16 15	15	0
2	Mike	11-09 12:16 15	15	0
2	Mike	11-09 12:16 15	15	0
2	Mike	11-09 12:16 15	15	0
2	Mike	11-09 12:12 15	15	0

Verification Mode : Face Status : Out

13 Print Settings

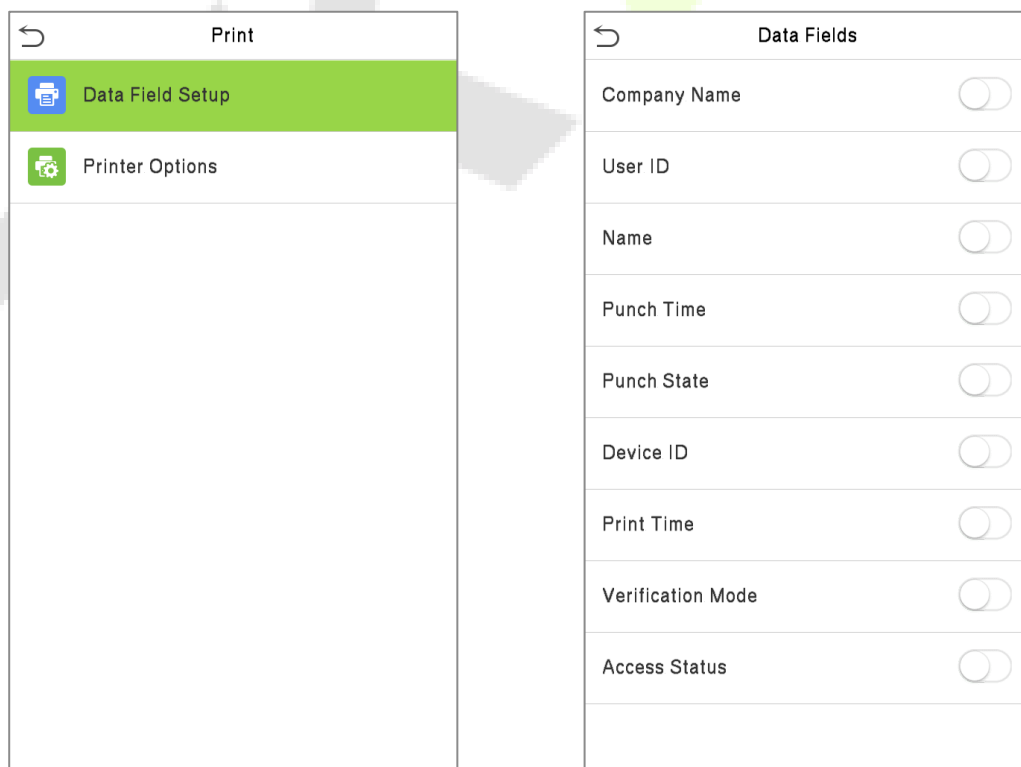
Devices with a printing function can print attendance records when a printer is connected (this function is optional and only implemented in some products).

Tap **Print** on the **Main Menu** interface.




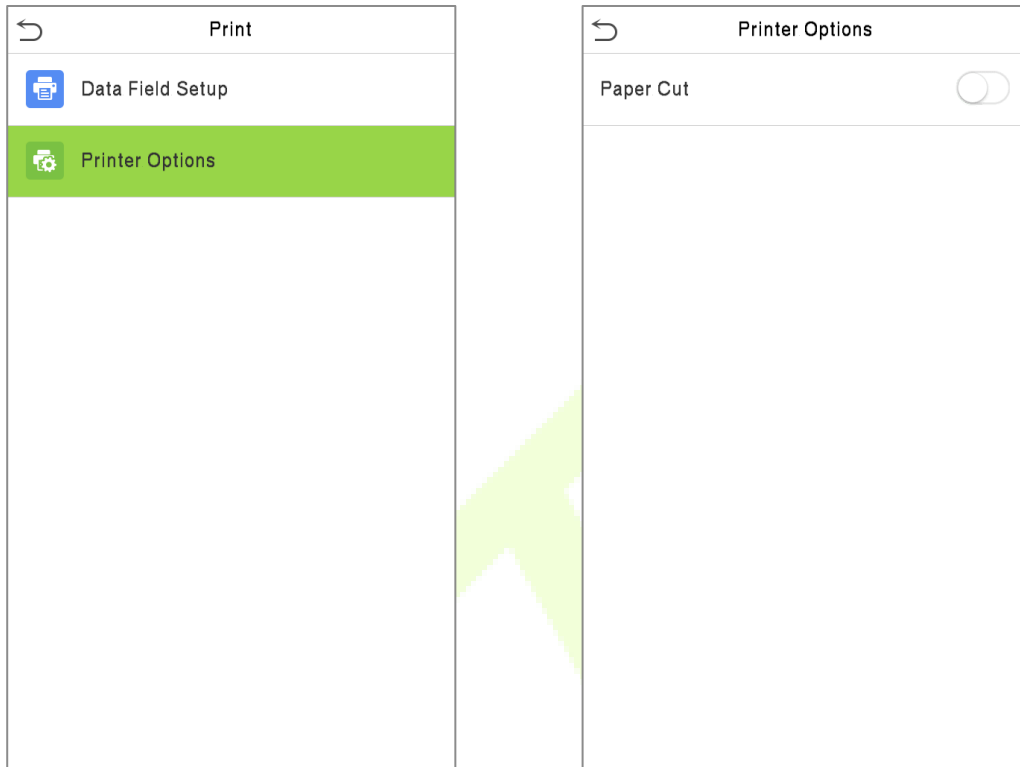
13.1 Print Data Field Settings

Select **Data Field Setup** on the **Print** interface. Toggle button to turn on/off the fields requiring a print.



13.2 Print Options Settings

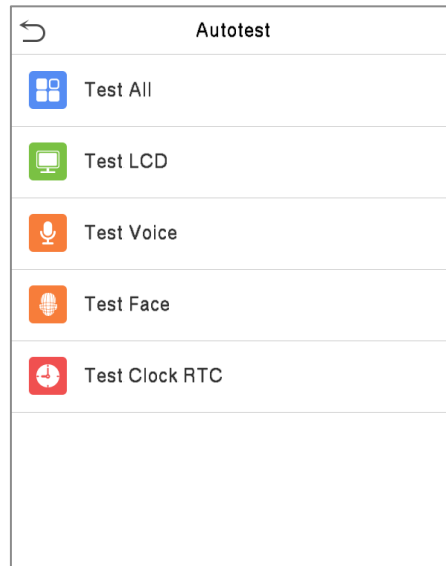
Select the **Printer Options** on the **Print** interface. Toggle  button to enable or disable the **Paper Cut** function.



Remarks: To turn on the **Paper Cut** function, it is required to connect the device with a printer with paper cutting function, so that the printer will cut papers according to the selected printing information while printing.

14 Autotest

Select **Main Menu**, tap **Autotest**. It enables the system to automatically test whether the functions of various modules are working normally, including the LCD, Voice, Camera, and Real-Time Clock (RTC).

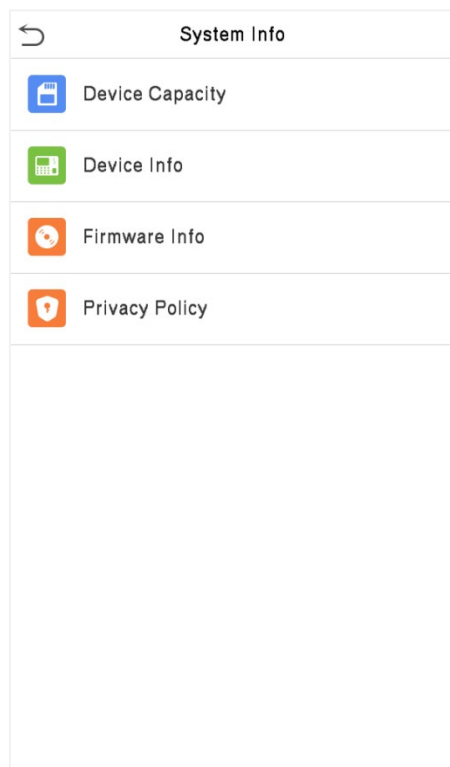


Function Description

Function Name	Description
Test All	To automatically test whether the LCD, Audio, Camera and RTC are working normally.
Test LCD	To automatically test the display of the LCD screen by displaying all the color bands including pure white and pure black to check whether the screen displays the colors accurately.
Test Voice	To automatically test whether the audio files stored in the device are complete and the voice quality is good.
Test Face	To test if the camera functions properly it checks the photos taken and determines if they are clear enough.
Test Clock RTC	To test the RTC. The device checks 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

On the **Main Menu**, tap **System Info** to view the storage status, the version information of the device, and firmware information.



Function Description


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

16 Connect to ZKBioAccess IVS Software

16.1 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 ZKBioAccess IVS server, preferably in the same network segment with the server address.)

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

Server address: Set the IP address as of the ZKBioAccess IVS server.

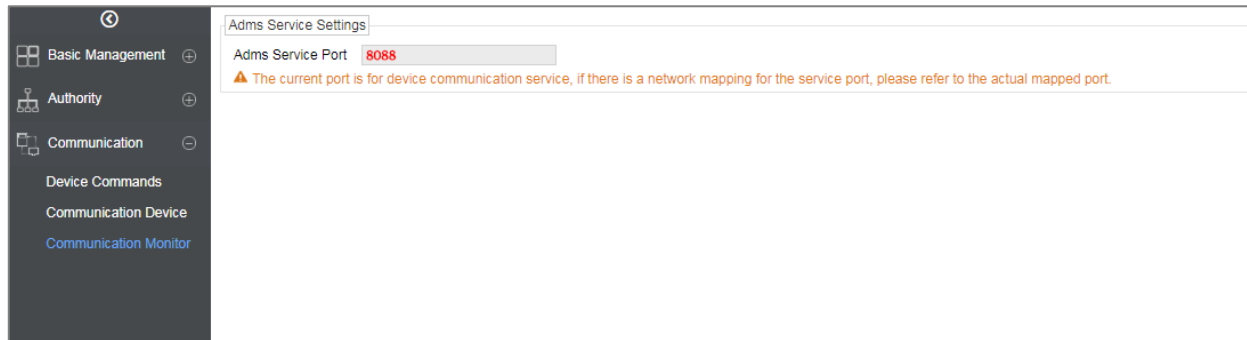
Server port: Set the server port as of ZKBioAccess IVS (The default is 8088).

Ethernet	
IP Address	192.168.163.150
Subnet Mask	255.255.255.0
Gateway	192.168.163.1
DNS	0.0.0.0
TCP COMM.Port	4370
DHCP	<input type="checkbox"/>
Display in Status Bar	<input checked="" type="checkbox"/>

Cloud Server Setting	
Server mode	ADMS
Enable Domain Name	<input type="checkbox"/>
Server Address	0.0.0.0
Server port	8081
Enable Proxy Server	<input type="checkbox"/>
HTTPS	<input type="checkbox"/>

● Software side

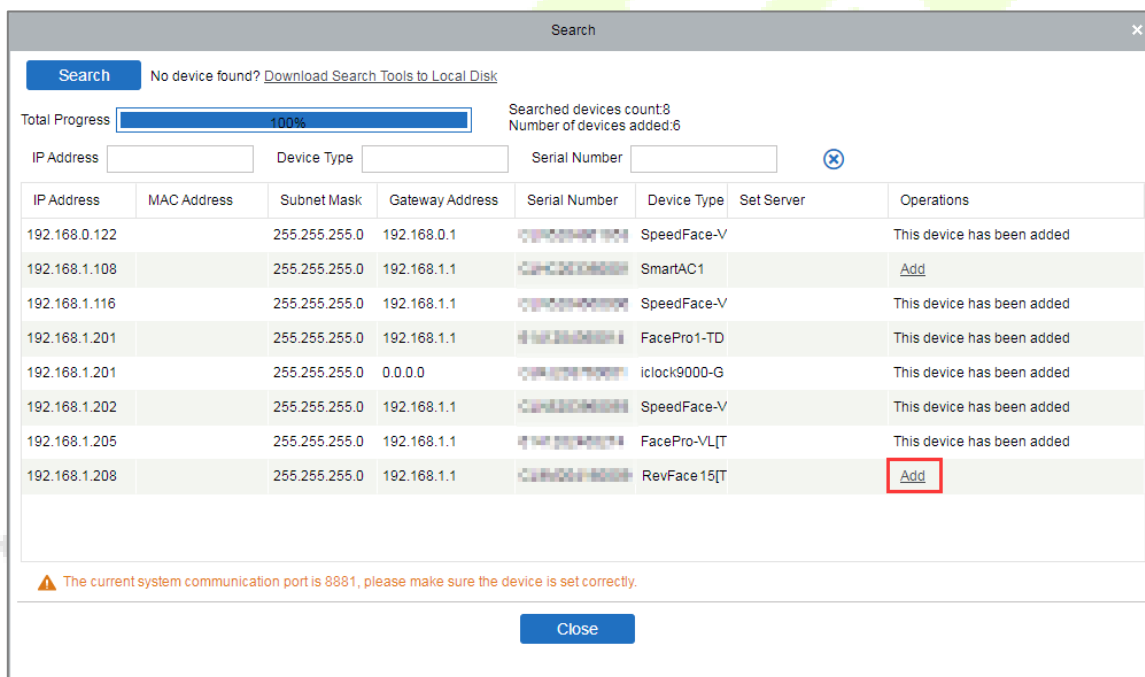
Login to ZKBioAccess IVS software, click **System** > **Communication** > **Communication Monitor** to set the ADMS service port, as shown in the figure below:



16.2 Add Device on the Software

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

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



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

16.3 Add Personnel on the Software

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

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

Note: For other specific operations, please refer to *ZKBioAccess IVS User Manual*.

Appendix 1

Requirements of Live Collection and Registration of Visible Light Face

Images

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



Requirements for Visible Light Digital Face Image Data

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

- **Eye Distance**

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

- **Facial Expression**

A neutral face or smile with eyes naturally open is recommended.

- **Gesture and Angel**

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

- **Accessories**

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

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

Appendix 2

Privacy Policy

Notice:

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

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

I. Collected Information

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

1. **User Registration Information:** At your first registration, the feature template (**Fingerprint template/Face template/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. 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

