User Manual

SenseFace 7 Series

Date: March 2024

Doc Version: 1.0

English

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

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

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

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

Trademark

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

Disclaimer

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

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

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

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

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

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

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

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

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

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

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

ZKTeco Headquarters

Address	ZKTeco Industrial Park, No. 32, Industrial Road,
	Tangxia Town, Dongguan, China.
Phone	+86 769 - 82109991
Fax	+86 755 - 89602394

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

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

About the Company

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

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

About the Manual

This manual introduces the operations of **SenseFace 7 Series**.

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

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

Document Conventions

Conventions used in this manual are listed below:

GUI Conventions

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

Symbols

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

TABLE OF CONTENTS

Data Security Statement

ZKTeco, as a smart product supplier, may also need to know and collect some of your personal information to better assist you in using ZKTeco's goods and services, and will treat your privacy carefully by developing a Privacy Policy.

Please read and understand completely all the privacy protection policy regulations and key points that appear on the device before using ZKTeco products.

As a product user, you must comply with applicable laws and regulations related to personal data protection when collecting, storing, and using personal data, including but not limited to taking protective measures for personal data, such as performing reasonable rights management for devices, strengthening the physical security of device application scenarios, and so on.

Safety Measures

The following precautions are to keep the user's safety and prevent any damage. Please read carefully before installation.

1. **Read, follow, and retain instructions** - All safety and operational instructions must be properly read and followed before bringing the device into service.

2. **Do not ignore warnings** - Adhere to all warnings on the unit and in the operating instructions.

3. **Accessories** - Use only manufacturer-recommended or product-sold accessories. Please do not use any other components other than manufacturer suggested materials.

4. **Precautions for the installation** – Do not place this device on an unstable stand or frame. It may fall and cause serious injury to persons and damage to the device.

5. **Service** - Do not try to service this unit yourself. Opening or removing covers may expose you to hazardous voltages or other hazards.

6. **Damage requiring service** - Disconnect the system from the main AC or DC power source and refer service personnel under the following conditions:

   - When cord or connection control is affected.

   - When the liquid was spilled, or an item dropped into the system.

   - If the system is exposed to water and/or inclement weather conditions (rain, snow, and more).

   - If the system is not operating normally under operating instructions.

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

7. **Replacement parts** - When replacement parts are required, service technicians must only use replacement parts provided by the supplier. Unauthorized substitutes can lead to the risk of burns, electric shock, or other hazards.

8. **Safety check** - On completion of service or repair work on the unit, ask the service technician to

perform safety checks to ensure proper operation of the unit.

9. **Power sources** - Operate the system only from the label's power source form. If the sort of power supply to use is unclear, call your dealer.

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

The devices should be installed in areas with limited access.

1. Instruction for Use

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

1.1 Finger Positioning

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

Too low   Too close to the edge

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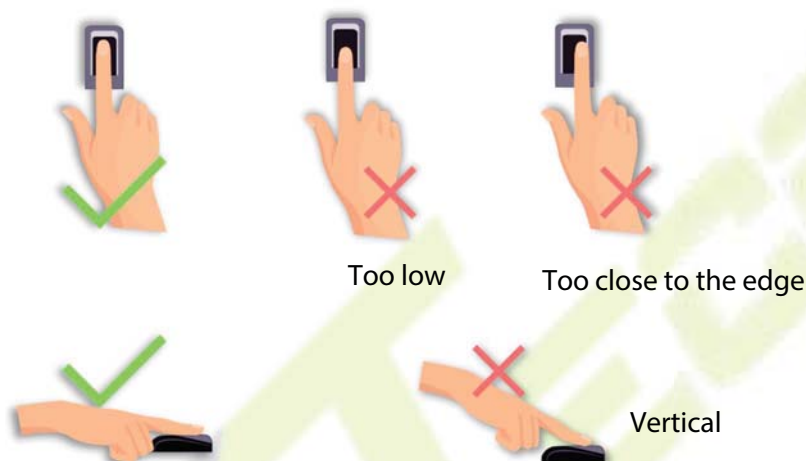
Note: Please use the correct method when pressing your fingers onto the fingerprint reader for registration and identification. Our company will assume no liability for recognition issues that may result from incorrect usage of the product. We reserve the right of final interpretation and modification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

1.2 Standing Position, Posture and Facial Expression

● **The recommended distance**
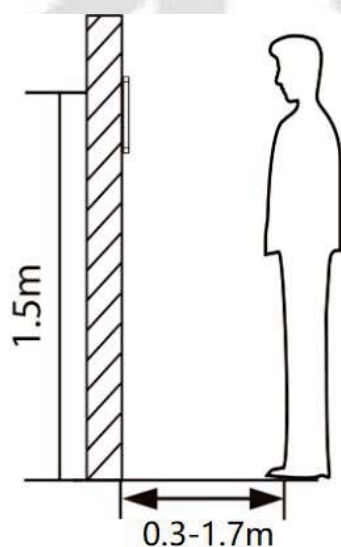
The distance between the device and a user whose height is in a range of 1.55 m to 1.85 m is recommended to be 0.3 m to 1.7 m. Users may slightly move forward or backward to improve the quality of facial images captured.

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

Standing Posture   **Facial Expression**
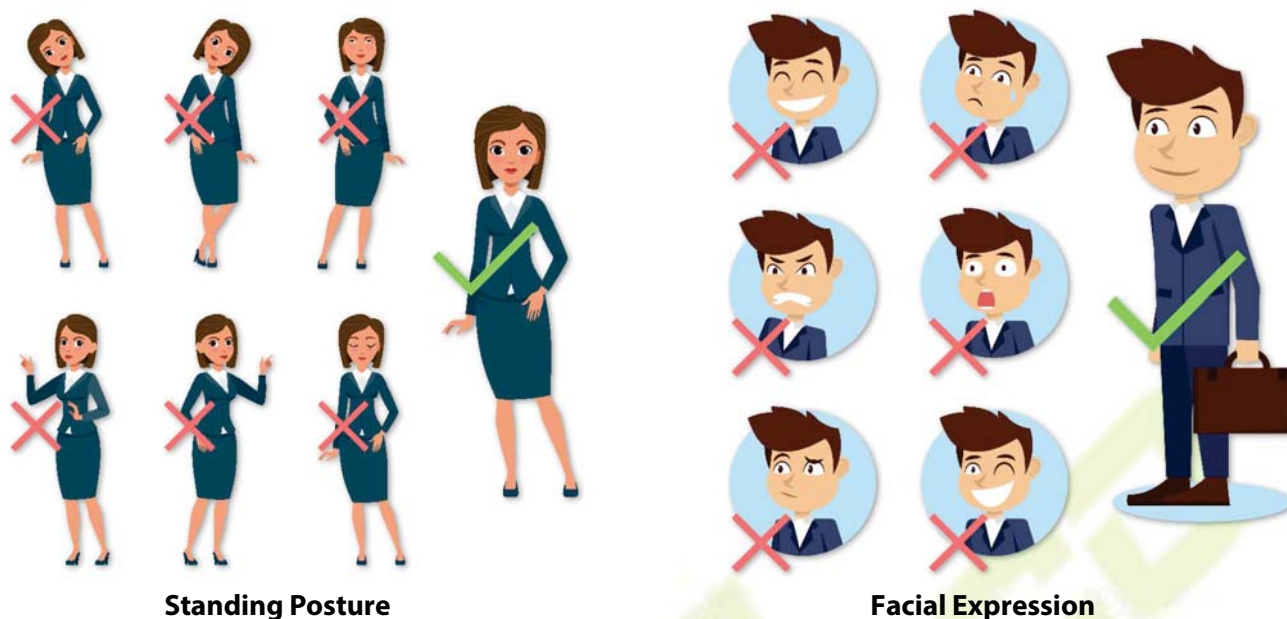
Note: *During enrollment and verification, please remain natural facial expression and standing posture.*

1.3   Face Template Registration

Please make sure that the face template in the centre of the screen during registration. Please face towards the camera and stay still during face template registration. The screen should look like the image below:
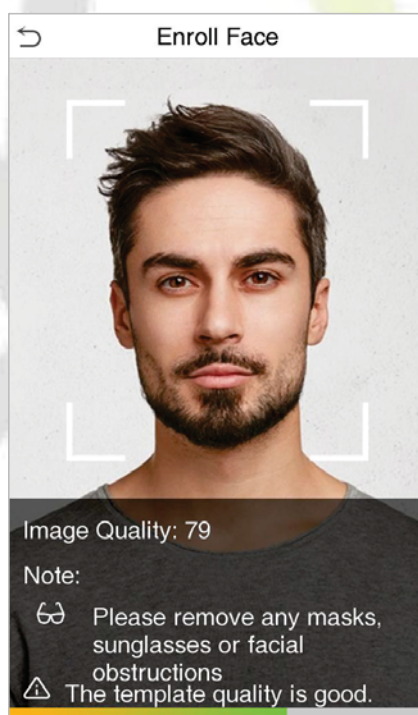
Correct face template registration and authentication method

- **Recommendation for Registering a Face Template**
  - When registering a face template, maintain a distance of 40 cm to 80 cm space between the device and the face template.

- Be careful not to change your facial expression. (Smiling face template, drawn face template, wink, etc.)

- If you do not follow the instructions on the screen, the face template registration may take longer or may fail.

- Be careful not to cover the eyes or eyebrows.

- Do not wear hats, masks, sunglasses, or eyeglasses.

- Be careful not to display two face templates on the screen. Register one person at a time.

- It is recommended for a user wearing glasses to register both face templates with and without glasses.

- **Recommendation for Authenticating a Face Template**

  - Ensure that the face template appears inside the guideline displayed on the screen of the device.

  - If the glasses have been changed, authentication may fail. If the face template without glasses has been registered, authenticate the face template without glasses further. If the face template with glasses has been registered, authenticate the face template with the previously worn glasses.

  - If a part of the face template is covered with a hat, a mask, an eye patch, or sunglasses, authentication may fail. Do not cover the face template, allow the device to recognize both the eyebrows and the face template.

1.4 Standby Interface

After connecting the power supply, the following standby interface template is displayed:
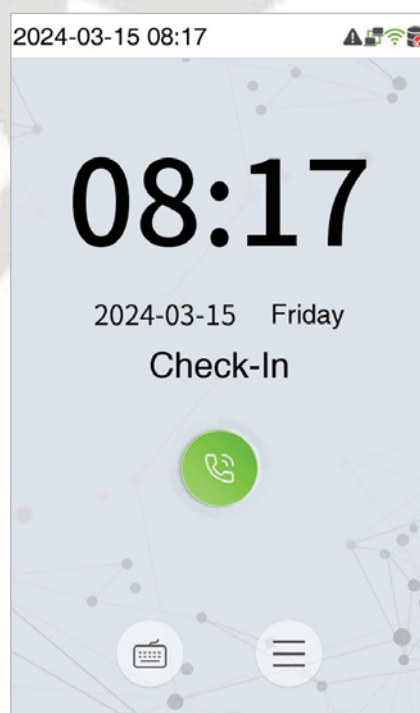
- Click ⌨ icon to enter the User ID input interface template.

- When there is no Super Administrator set in the device, tap ☰ icon to go to the menu.

- After setting the Super Administrator on the device, it requires the Super Administrator's verification before entering the menu functions.

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

- On the standby interface template, the punch state options can also be shown and used directly. Click anywhere on the screen apart from the icons, and six shortcut keys appears on the screen, as shown in the figure below:
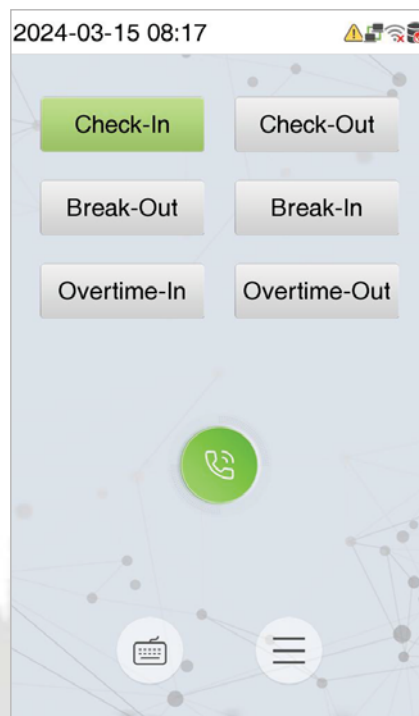
- Press the corresponding punch state key to select your current punch state, which is displayed in green.

Note: *The punch state options are off by default and need to be changed to other option in the* [*"7.5 Shortcut Key Mappings"*](#) *to get the punch state options on the standby screen.*

1.5   Virtual Keyboard
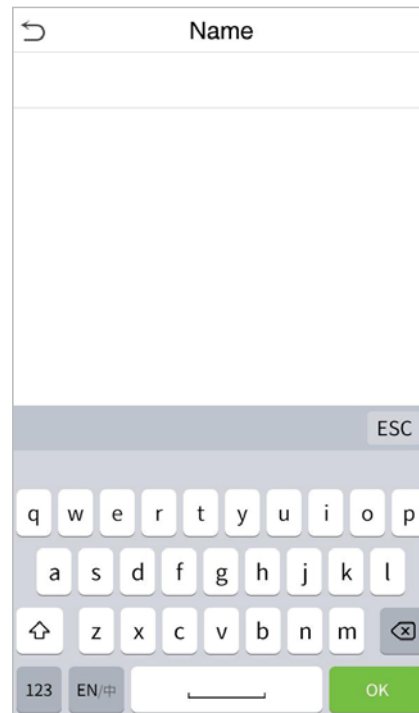
Note:

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

- _Click **EN** to switch to the English keyboard._

- _Press **123** to switch to the numeric and symbolic keyboard._

- _Click **ABC** to return to the alphabetic keyboard._

- _Click the input box, virtual keyboard appears._

- _Click **ESC** to exit the virtual keyboard._

1.6   Verification Mode

1.6.1 Fingerprint Verification★

Note: This function is only for SenseFace 7A.

● **1: N Fingerprint Verification Mode**

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

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

Please follow the recommended way to place your finger onto the sensor. For details, please refer to section [Finger Positioning](#).

<table>
<tr><td>Verification is successful:</td><td>Verification is failed:</td></tr>
</table>
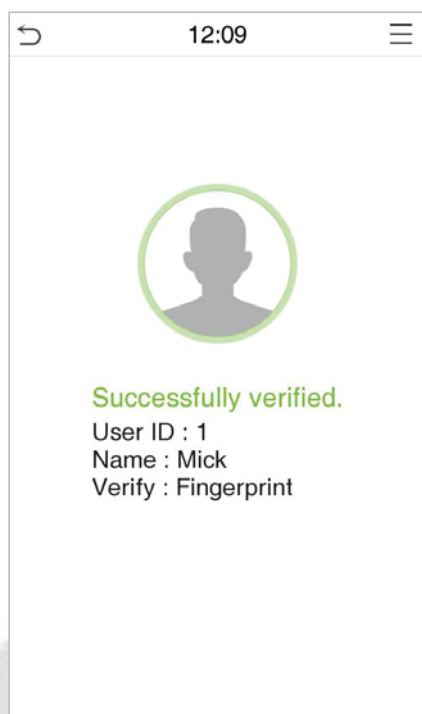
12:09	12:16
Successfully verified. User ID : 1 Name : Mick Verify : Fingerprint	**Failed to verify.** Verify : Fingerprint Illegal Fingerprint
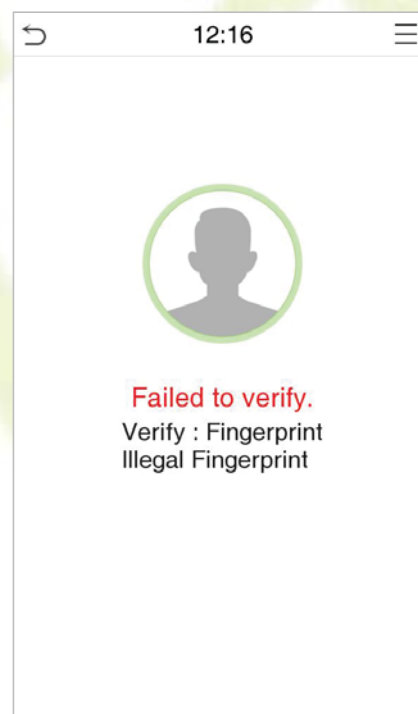
● **1: 1 Fingerprint Verification Mode**

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

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

Click the ⌨ button on the main screen to enter 1:1 fingerprint verification mode.

Input the user ID and press **OK**.
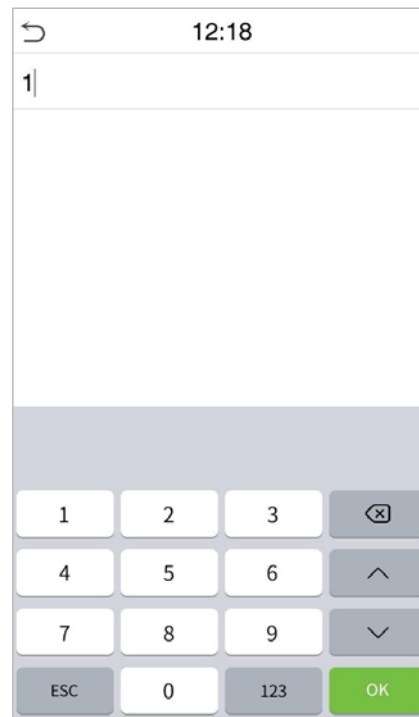
If the user has registered face template, card and password in addition to his/her fingerprints and the verification method is set to Password/Fingerprint/Card/Face template verification, the following screen will appear. Select the fingerprint icon to enter fingerprint verification mode.
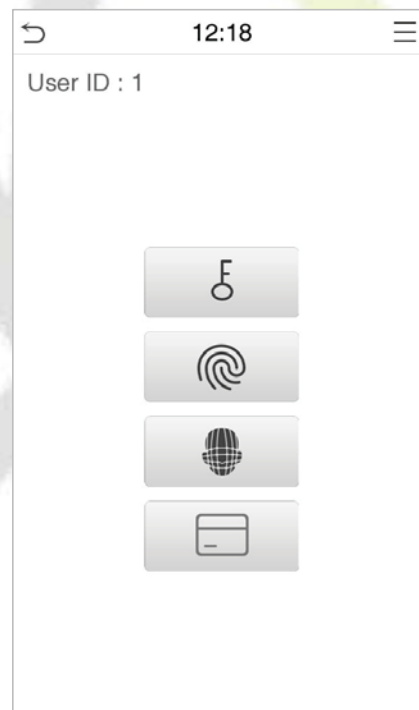
Press the fingerprint to verify.
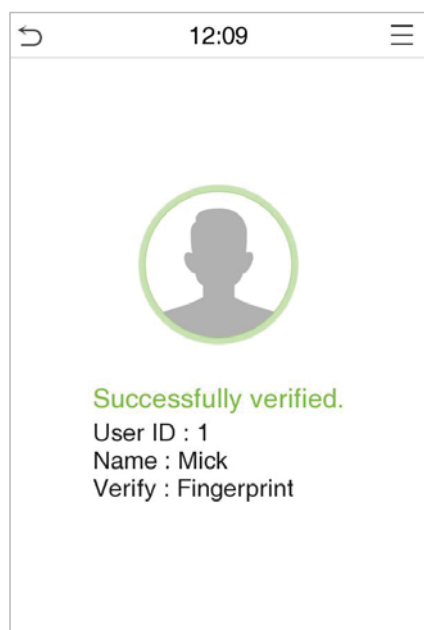
Verification is successful: Verification is failed:
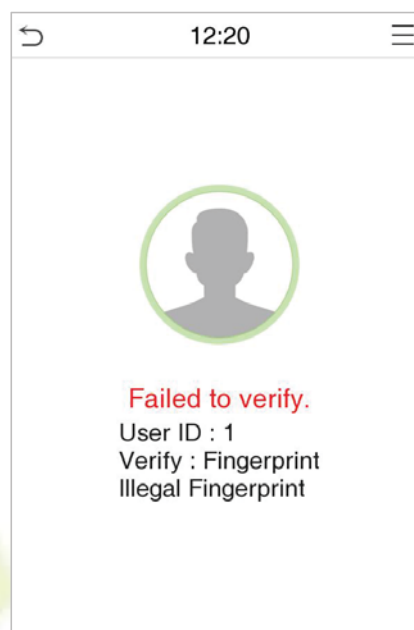
1.6.2 QR Code Verification★

Note: This function is only for SenseFace 7C.

In this verification mode, the device compares the QR code image collected by the QR code collector with all the QR code data in the device.

Tap **Mobile Credential** on the ZKBioAccess Mobile Page, and a QR code will appear, which includes employee ID and card number (static QR code only includes card number) information. The QR code can replace a physical card on a specific device to achieve contactless authentication. Please refer to 15.4 Mobile Credential.

1.6.3 Card Verification

● **1:N card verification**

The 1:N card verification mode compares the card number in the card induction area with all the card number data registered in the device; The following screen displays on the card verification:
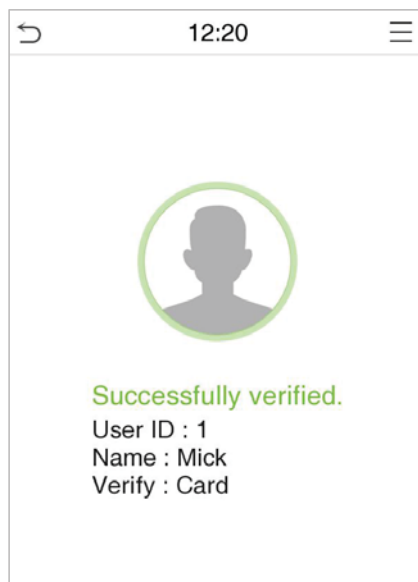
● **1:1 card verification**

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

Press 🎹 in the main interface template to open the 1:1 card verification mode.
Enter the user ID and click **OK.**
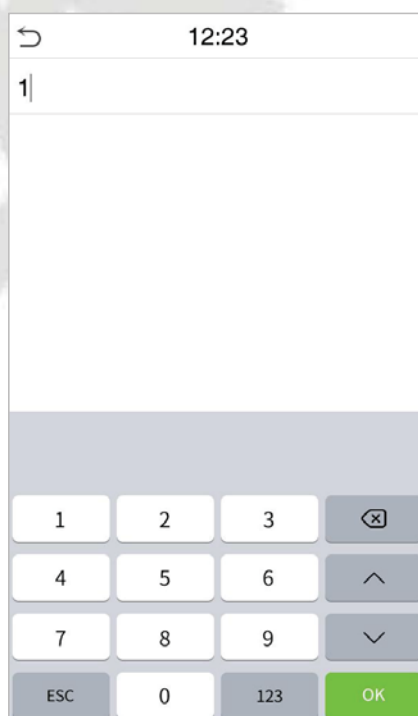
If the user has registered face template, card and password in addition to his/her card, and the verification method is set to Password/Fingerprint/Card/Face verification, the following screen will appear. Select the ⬚ icon to enter the card verification mode.

Place the card in the collection area for verification.
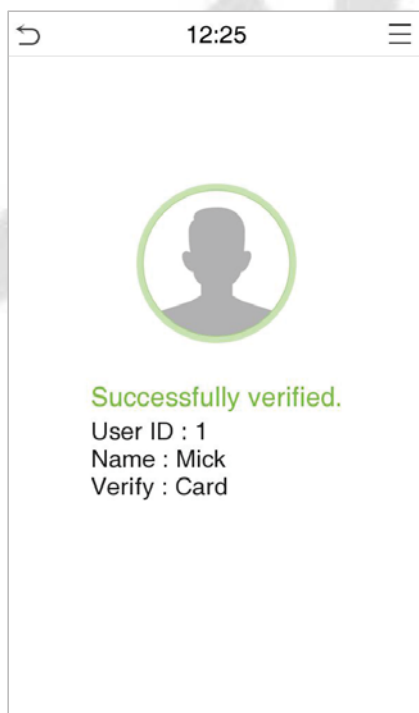
Verification is successful: Verification is failed:
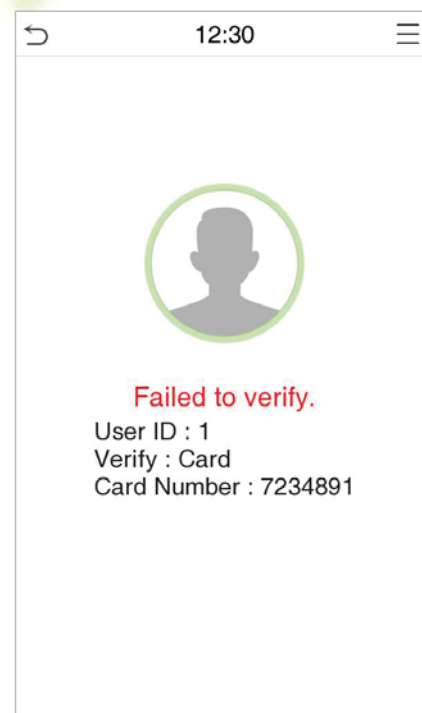
1.6.4 Facial Verification

● **1:N Facial Verification**

device compares the currently acquired facial images with all the registered face template data stored in its database. The following is the pop-up prompt box displaying the result of the comparison.
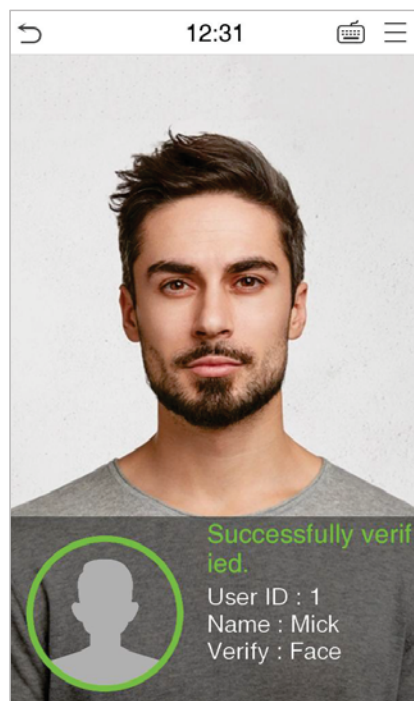
● **1:1 Facial Verification**

In this verification mode, the device compares the face template captured by the camera with the facial

template related to the entered user ID. Press icon in the main interface template and enter the 1:1 facial verification mode and enter the user ID and click **OK**.
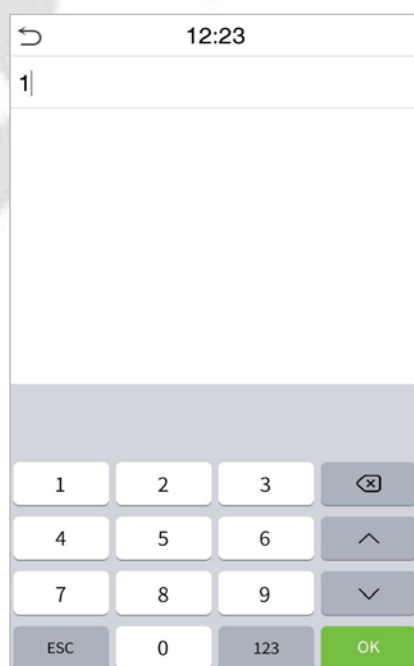
If the user has registered card, fingerprint and password in addition to his/her face template, and the verification method is set to Password/Fingerprint/Card/Face verification, the following screen will appear. Select the [icon] icon to enter the face template verification mode.

After successful verification, the prompt box displays "**Successfully Verified**", as shown below:
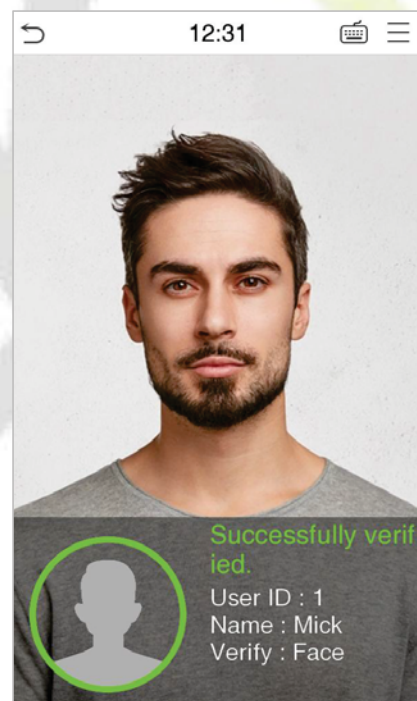
If the verification is failed, it prompts "**Please adjust your position!**".

1.6.5 Password Verification

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

Click the 🖮 button on the main screen to enter the 1:1 password verification mode. Then, input the user ID and press **OK**.
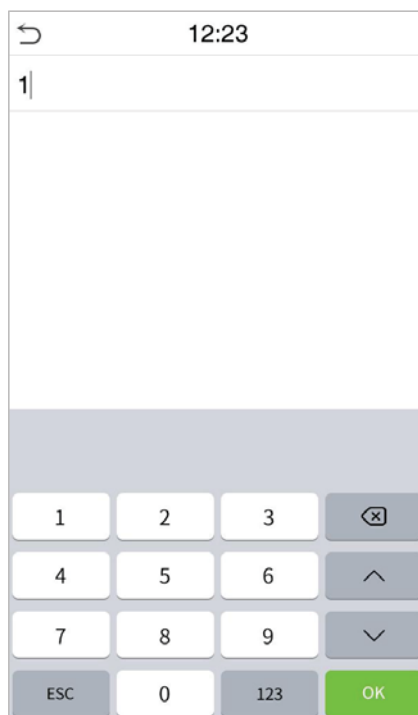
If the user has registered face template and card in addition to password, and the verification method is set to Password/Fingerprint/Card/Face verification, the following screen will appear. Select the 🔑 icon to enter password verification mode.
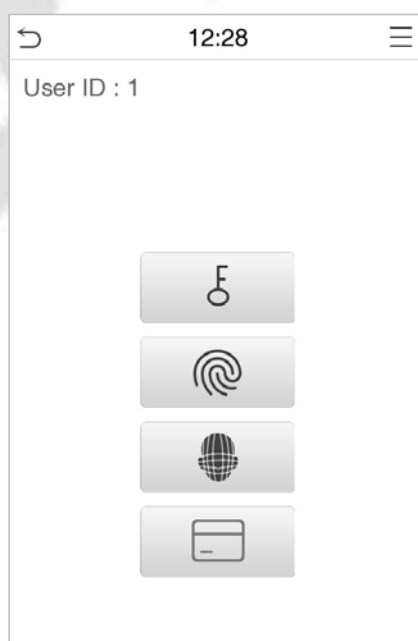
Input the password and press **OK**.
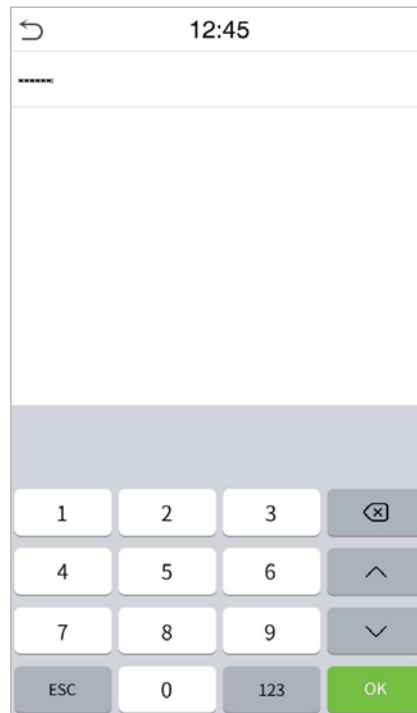
The following screen displays, after inputting a correct password and a wrong password respectively.
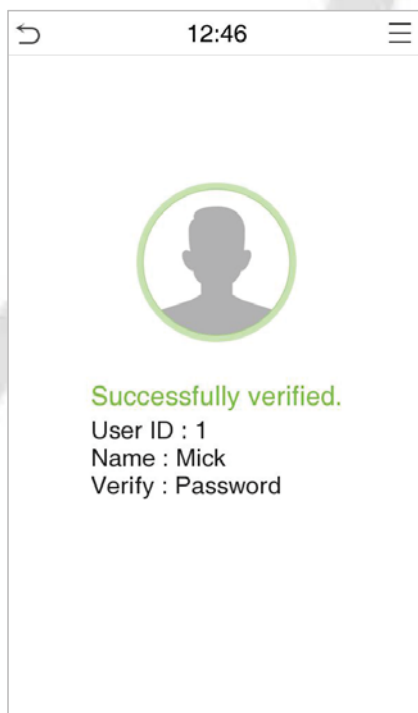
Verification is successful: Verification is failed:
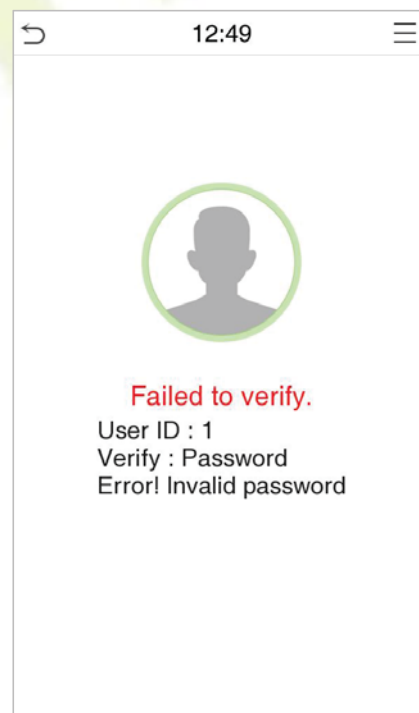
1.6.6 Combined Verification

To increase security, this device offers the option of using multiple forms of verification methods. A total of 21 different verification combinations can be used, as shown below:

Combined Verification Symbol Definition:

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

Verification Mode	Verification Mode	Verification Mode
● Password/Fingerprint/Card/Face	○ Fingerprint+Password+Card	○ Password+Card
○ Fingerprint Only	○ Password+Card	○ Password/Card
○ User ID Only	○ Password/Card	○ User ID+Fingerprint+Password
○ Password	○ User ID+Fingerprint+Password	○ Fingerprint+(Card/User ID)
○ Card Only	○ Fingerprint+(Card/User ID)	○ Face Only
○ Fingerprint/Password	○ Face Only	○ Face+Fingerprint
○ Fingerprint/Card	○ Face+Fingerprint	○ Face+Password
○ User ID+Fingerprint	○ Face+Password	○ Face+Card
○ Fingerprint+Password	○ Face+Card	○ Face+Fingerprint+Card
○ Fingerprint+Card	○ Face+Fingerprint+Card	○ Face+Fingerprint+Password

Procedure to set for Combined Verification Mode:

- Combined verification requires personnel to register all the different verification method. Otherwise, employees will not be able to successfully verify the combined verification process.
- For instance, when an employee has registered only the data, but the Device verification mode is set as "Face + Password", the employee will not be able to complete the verification process successfully.
- This is because the Device compares the scanned face template template of the person with registered verification template (both the Face template and the Password) previously stored to that Personnel ID in the Device.
- But as the employee has registered only the Face template but not the Password, the verification will not get completed and the Device displays "Verification Failed".

2. Main Menu

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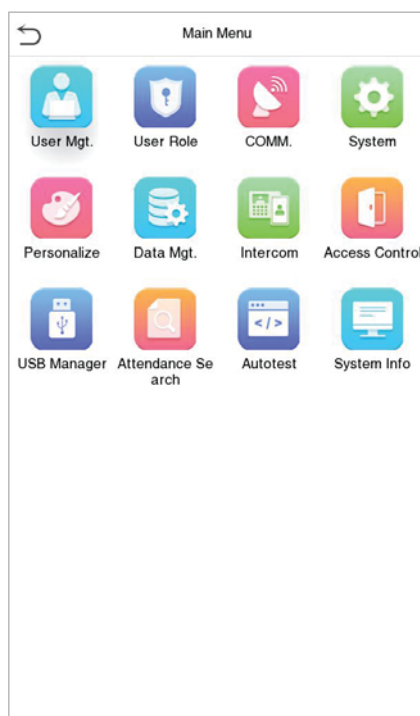
Function Description

Menu	Descriptions
User Mgt.	To add, edit, view, and delete basic 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 setting, face template & fingerprint parameters★, device type setting, security setting, update firmware online, USB upgrade, and reset to factory.
Personalize	This includes user interface, voice, bell schedules, punch state options and shortcut key mappings settings.
Data Mgt.	To delete all relevant data in the device.
Intercom	To set the parameters related to the SIP and NVR.
Access Control	To set the parameters of the lock and the relevant access control device including options like time rule, holiday settings, combine verification, and duress option settings.
USB Manager	To upload or download the specific data by a USB drive.

Attendance Search	To query the specified event logs, check attendance photos and blocklist attendance photos.
Autotest	To automatically test whether each module functions properly, including the LCD screen, audio, microphone, camera, fingerprint sensor★ and real-time clock.
System Info	To view data capacity, device and firmware information and privacy policy of the device.

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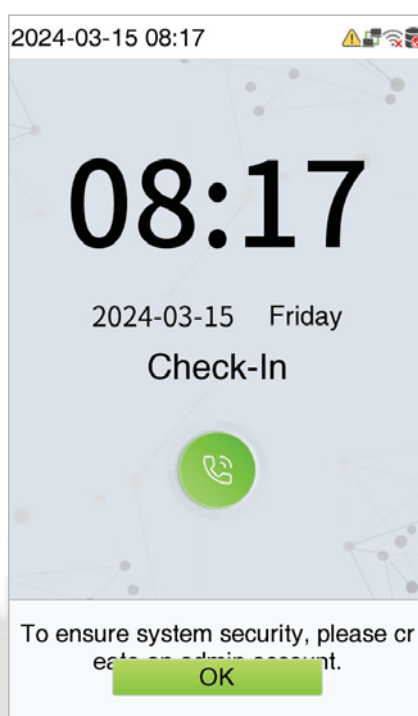
3. **User Management**

3.1 **User Registration**

Click **User Mgt.** on the main menu.
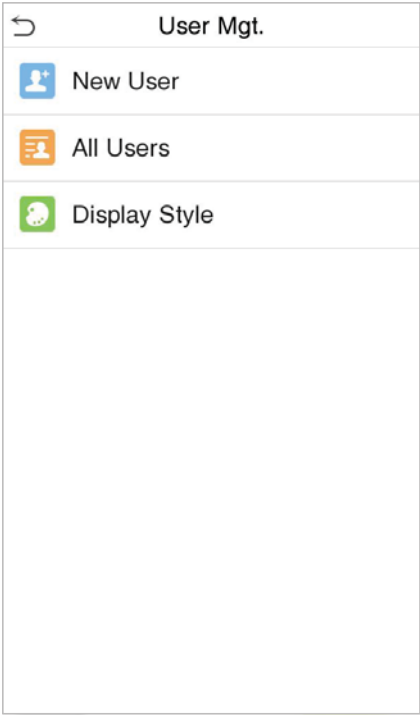
3.1.1 **User ID and Name**

Tap **New User.** Enter the **User ID** and **Name.**
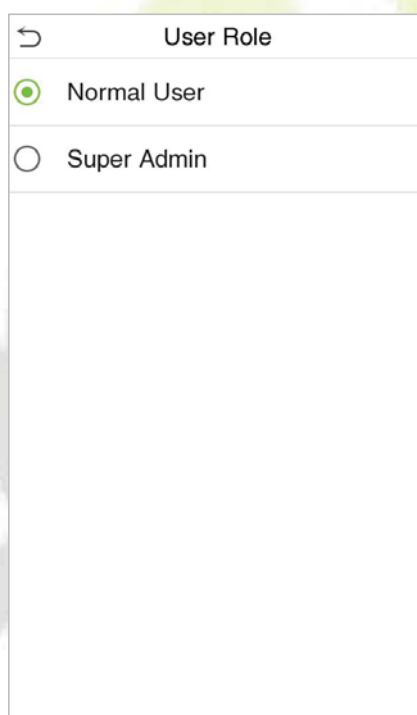
Notes:

- *A username can contain a maximum of 34 characters.*

- *The user ID may contain 1 to 14 digits by default.*

- *During the initial registration, you can modify your ID, which cannot be modified after registration.*

- *If a message "**Duplicated!**" pops up, you must choose another ID as the enter User ID already exists.*

3.1.2 User Role

On the New User interface, tap on **User Role** to set the role for the user 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 already registered in the Device, then the Normal Users will not have the privileges to manage the system and can only access authentication verifications.

- **User Defined Roles:** The Normal User can also be set with **User Defined Role** which are the custom roles that can be set to the Normal User.

Note: *If the selected user role is the Super Admin, the user must pass the identity authentication to access the main menu. The authentication is based on the authentication method(s) that the super administrator has registered. Please refer to* [1.6 Verification Mode](#)*.*

3.1.3 Fingerprint★

Click **Fingerprint** to enter the fingerprint registration page. Select the finger to be enrolled.
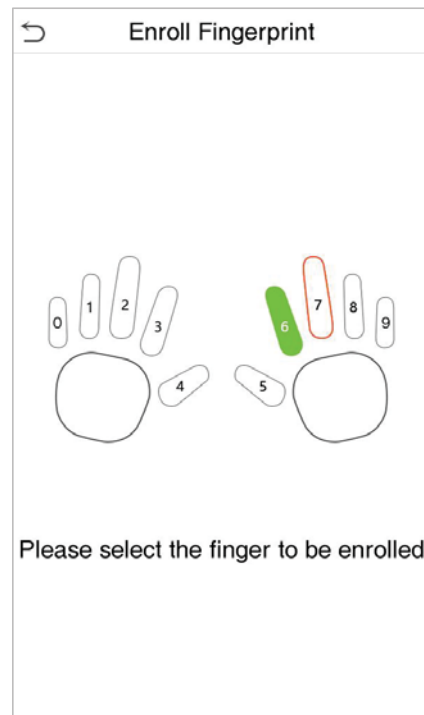
Press the same finger on the fingerprint reader three times. Green indicates that the fingerprint was enrolled successfully.

3.1.4 Face Template

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

- Please face towards the camera and position your face template inside the white guiding box and stay still during face template registration.

- A progress bar shows up while registering the face template and a **"Enrolled Successfully"** is displayed as the progress bar completes.

- If the face template is registered already then, the **"Duplicate Face"** message shows up. The registration interface is as follows:
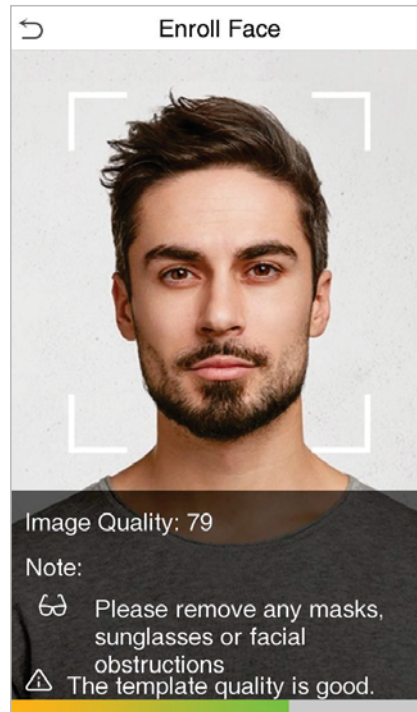
3.1.5 Card

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

- On the Card interface, swiping card underneath the card reading area. The card registration will be successful.

- If the card is registered already then, the "**Duplicate Card**" message shows up. The registration interface is as follows:
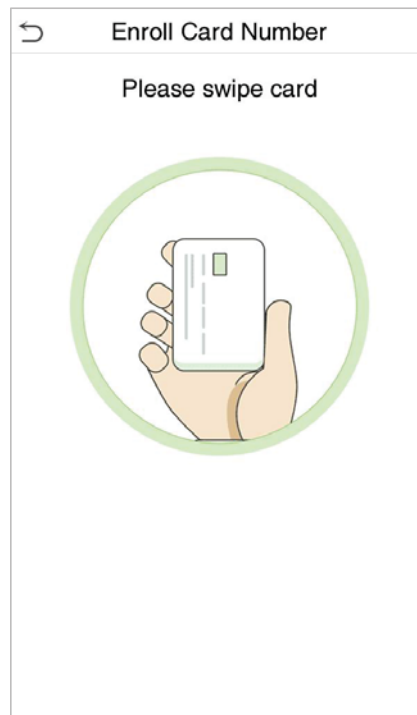
3.1.6 Password

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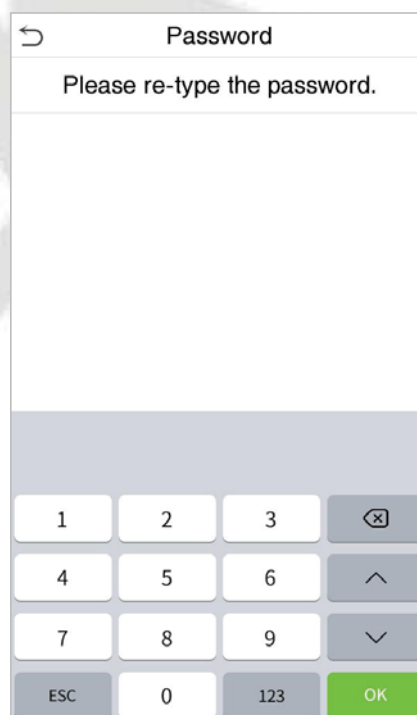
Note: *The password may contain 6 to 8 digits by default.*

3.1.7 Profile Photo

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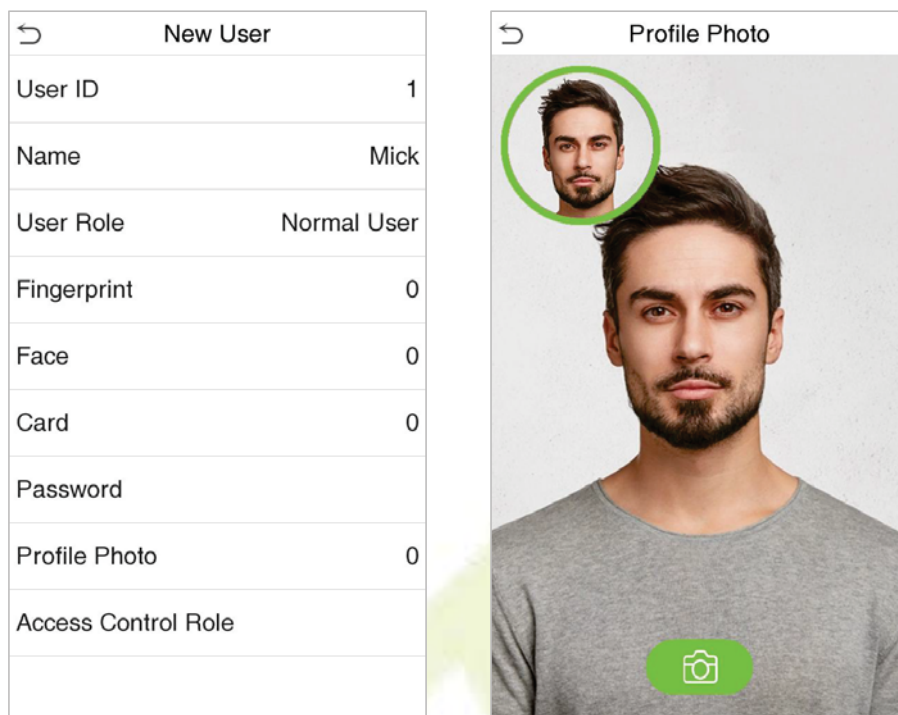
- When a user registered with a photo passes the authentication, the registered photo will be displayed.
- Tap **Profile Photo**, the device's camera will open, then tap the camera icon to take a photo. The captured photo is displayed on the top left corner of the screen and the camera opens again to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

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

3.1.8 Access Control Role

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

- Tap **Access Control Role** > **Access Group**, to assign the registered users to different groups for better management. 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 period to use.

3.2   Search for Users

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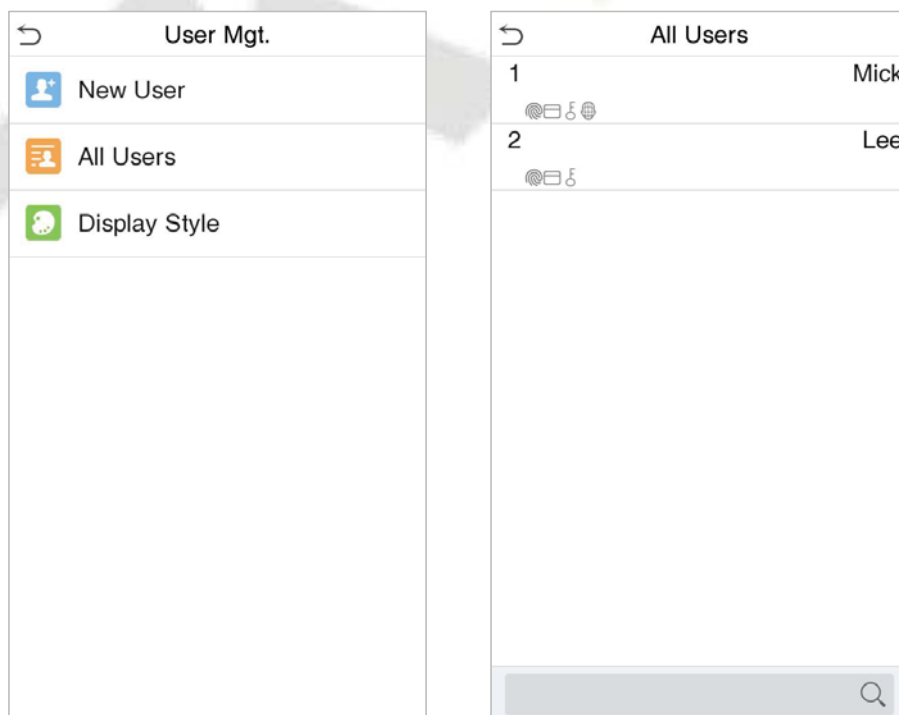
3.3 Edit User

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

↰ User : 1	↰ Edit : 1
Edit	User ID 1
Delete	Name Mick
	User Role Normal User
	Fingerprint 1
	Face 1
	Card 1
	Password ********
	Profile Photo 1
	Access Control Role

Note: The process of editing a user is the same as that of adding a user, except that the user ID cannot be modified when editing a user's detail. The process in detail refers to "3. User Management".

3.4 Delete User

On **All Users** interface, tap on the required user from the list and tap **Delete** to delete the user or a 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: All information of the user will be deleted (deletes the selected User as a whole) from the Device.

Delete Fingerprint Only: Deletes the fingerprint information of the selected user.

Delete Face Only: Deletes the face template information of the selected user.

Delete Password Only: Deletes the password information of the selected user.

Delete Card Number Only: Deletes the card information of the selected user.

Delete Profile Photo Only: Deletes the profile photo of the selected user.

↩	User : 1
Edit	
Delete	

↩	Delete : 1
Delete User	
Delete Fingerprint Only	
Delete Face Only	
Delete Password Only	
Delete Card Number Only	
Delete Profile Photo Only	
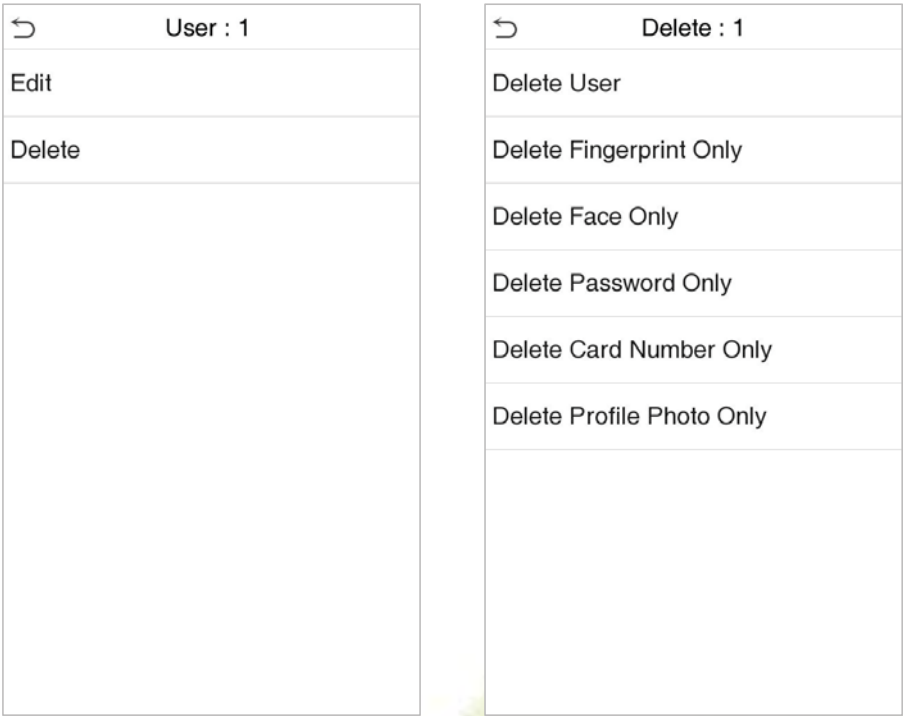
3.5 Display Style

Tap on **User Mgt.** > **Display Style** to choose the style of **All Users** interface's list.

↩	Display Style
◉	Multiple Line
○	Mixed Line
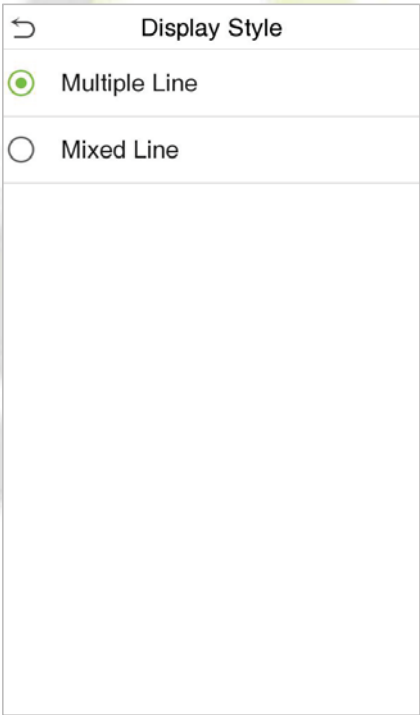
Different display styles are shown as below:

Multiple Line: Mixed Line:
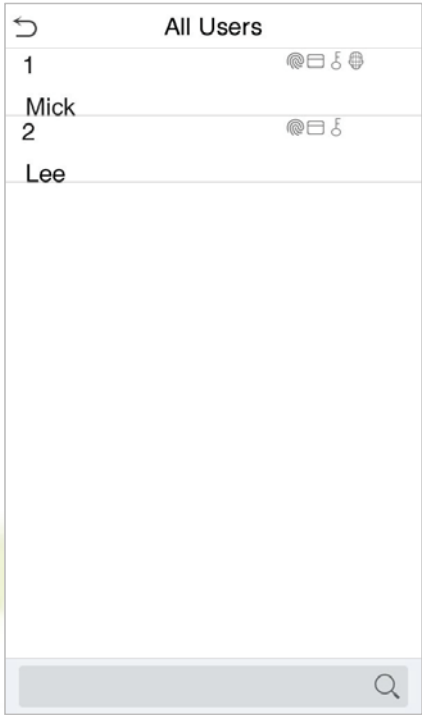
4. User Role

User Role facilitates to assign some specific permissions to specific 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.

	User Role
👤	User Defined Role 1
👤	User Defined Role 2
👤	User Defined Role 3
👤	Enroller
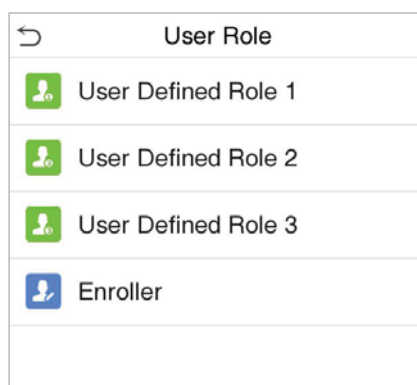
- On the **User Defined Role** interface, toggle **Enable Defined Role** to enable or disable the user defined role.
- Tap on **Name** and enter the custom name of the role.

	User Role		User Defined Role 1	
👤	User Defined Role 1	Enable Defined Role		⚪
👤	User Defined Role 2	Name	User Defined R...	
👤	User Defined Role 3	Define User Role		
👤	Enroller			
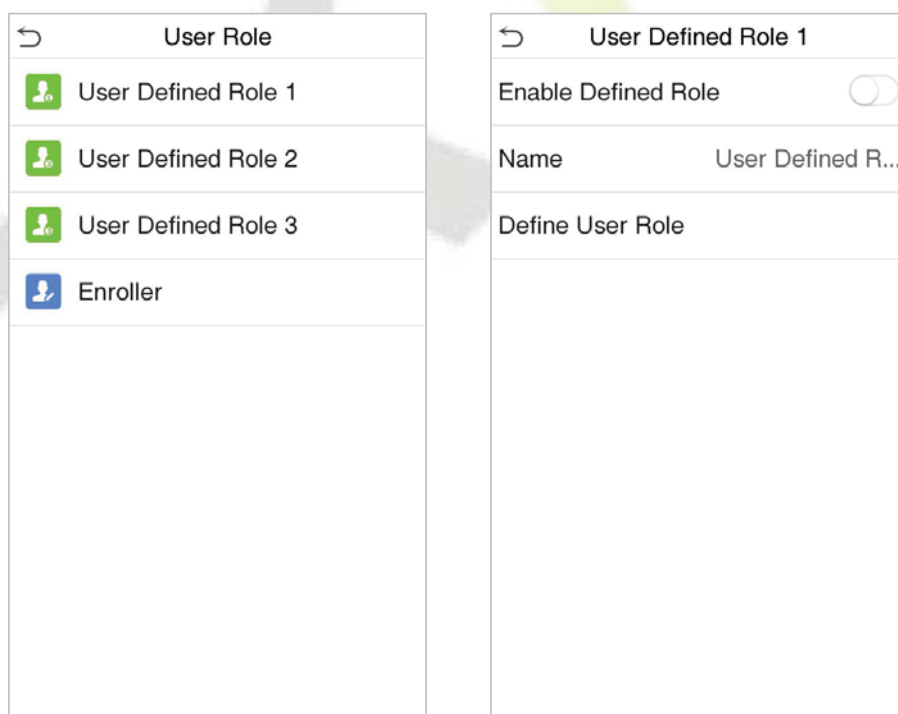
- Then, tap on **User Defined Role** and select the required privileges to assign to the new role, and then tap on the **Return** button.
- During privilege assignment, the main menu function names will be displayed on the left and its sub-menus will be listed on its right.

- First tap on the required **Main Menu** function name, and then select its required sub-menus from the list.

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.*

5. Communication Settings

Tap **COMM.** on the **Main Menu** to set the relevant parameters of Network, Serial Comm, PC Connection, Wireless Network, Cloud Server, Wiegand and Network Diagnosis.
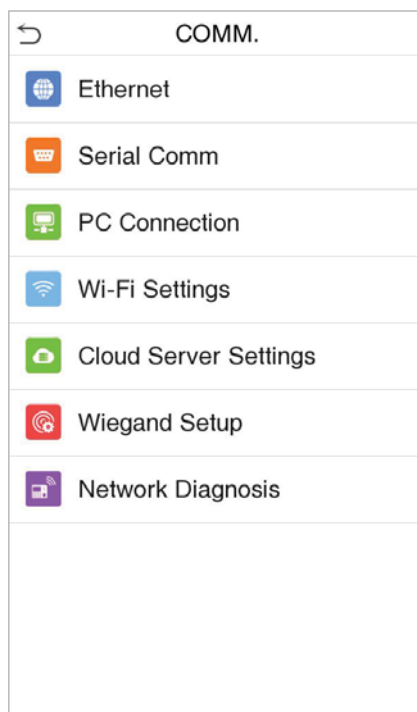
5.1 Network Settings

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

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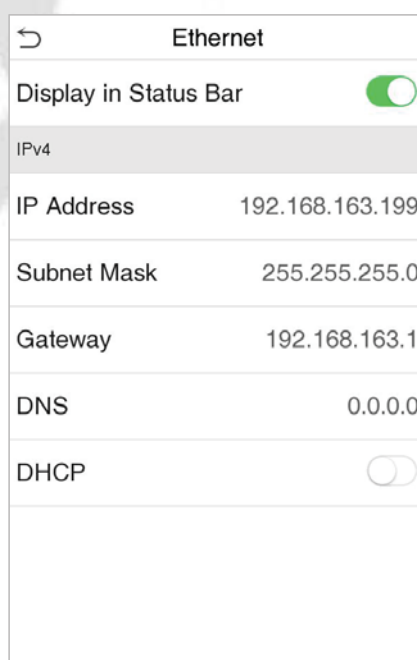
Function Description

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

5.2 Serial Comm

Serial Comm function facilitates to establish communication with the device through a serial port (RS485/ Master Unit).

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

Serial Comm		Serial Port
Serial Port	No Using	○ No Using
Baudrate	115200	◉ RS485(PC)
		○ Master Unit

Function Description

Function Name	Descriptions
Serial Port	**no using:** Do not communicate with the device through the serial port. **RS485(PC):** Communicates with the device through RS485 serial port. **Master Unit:** When RS485 is used as the function of "**Master unit**", the device will act as a master unit, and it can be connected to RS485 card reader.

	The rate at which the data is communicated with PC, there are 4 options of baud rate: 115200 (default), 57600, 38400, and 19200.
Baud Rate	The higher is the baud rate, the faster is the communication speed, but also the less reliable.
	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 would be more reliable.

5.3 PC Connection

To improve the security of data, please set a Comm Key for communication between the device and the PC. The connection password needs to be entered before the device can be connected to the PC software if a Comm Key is set.

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 must be 6 digits.
Device ID	Identity 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.
TCP COMM. Port	The default TCP COMM Port value is 4370. It can be modified according to the network availability.

HTTPS	To increase the security of software access, users can enable the HTTPS protocol to create a secure and encrypted network transmission and assure the security of sent data through identity authentication and encrypted communication. This function is enabled by default. This function can be enabled or disabled through the menu interface, and when changing the HTTPS status, the device will pop up a security prompt, and restart after confirmation.

5.4   Wireless Network★

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

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

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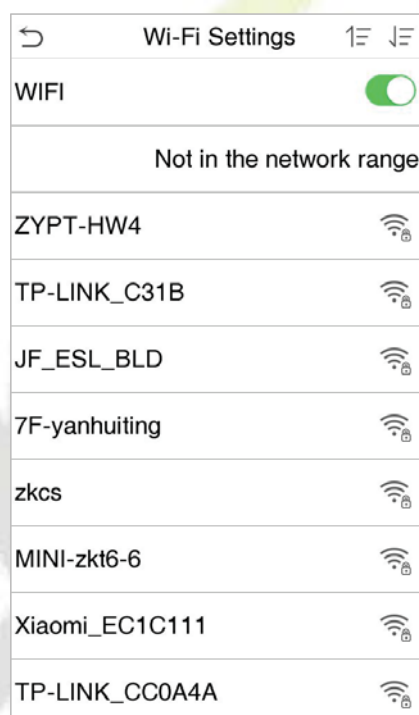
● **Search the Wi-Fi Network**

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

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

- Choose the appropriate Wi-Fi name from the available list, and input the correct password in the password interface, and then tap **Connect to Wi-Fi (OK)**.
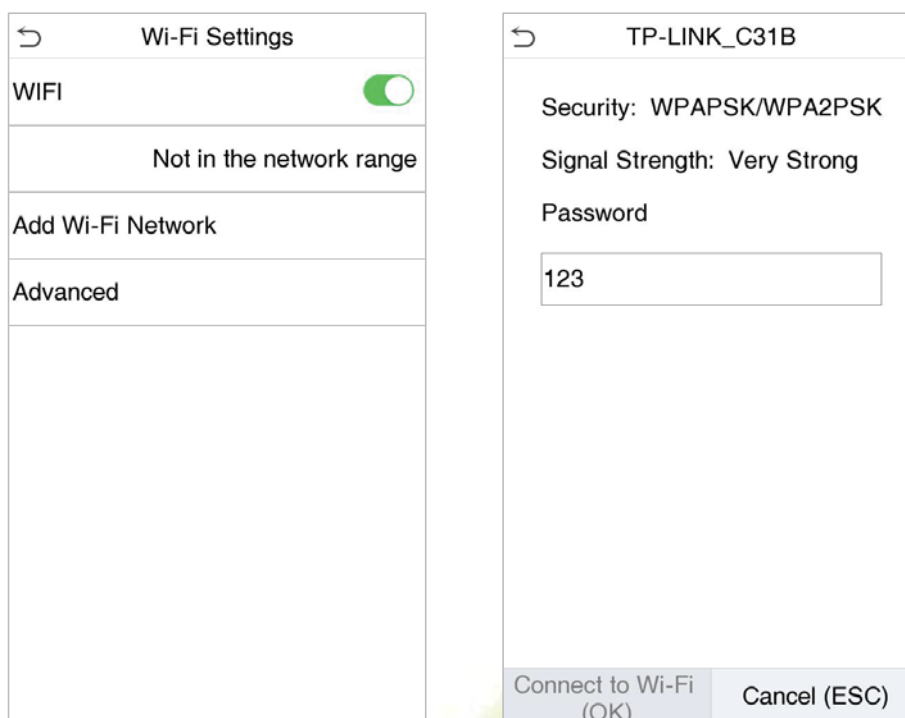
WIFI Enabled: Tap on the required network from the searched network list.

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

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

● **Add WIFI Network Manually**

The Wi-Fi can also be added manually if the required Wi-Fi does not show on the list.
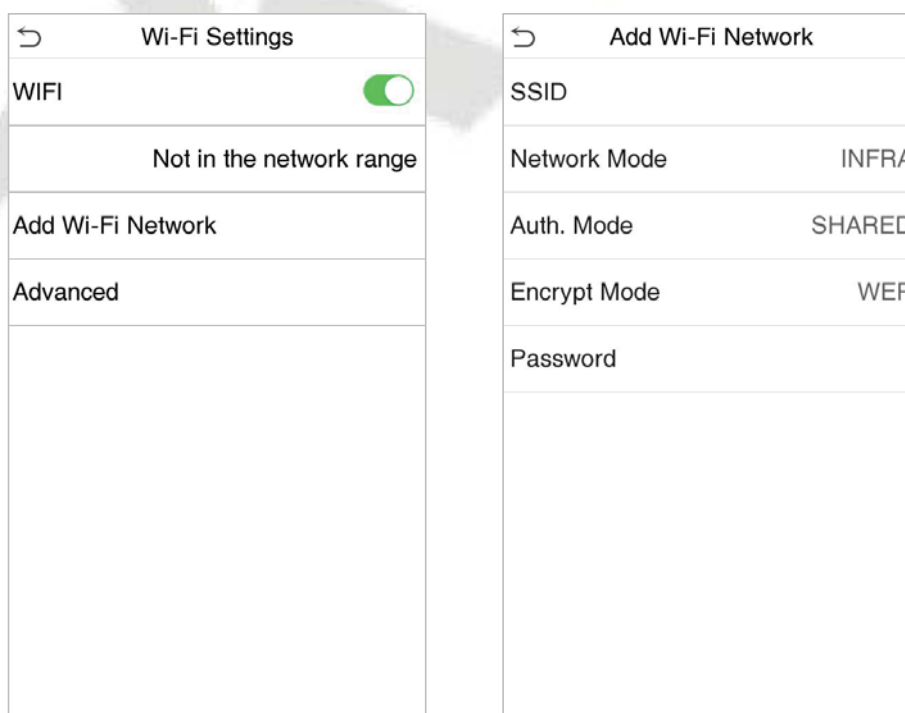
Tap on **Add Wi-Fi Network** to add the Wi-Fi manually.

On this interface template, enter the Wi-Fi 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.

Wi-Fi Settings		Ethernet	
WIFI	⬤	DHCP	⬤
	Not in the network range	IP Address	192.168.0.15
Add Wi-Fi Network		Subnet Mask	255.255.255.0
Advanced		Gateway	192.168.0.1
		DNS	192.168.0.1
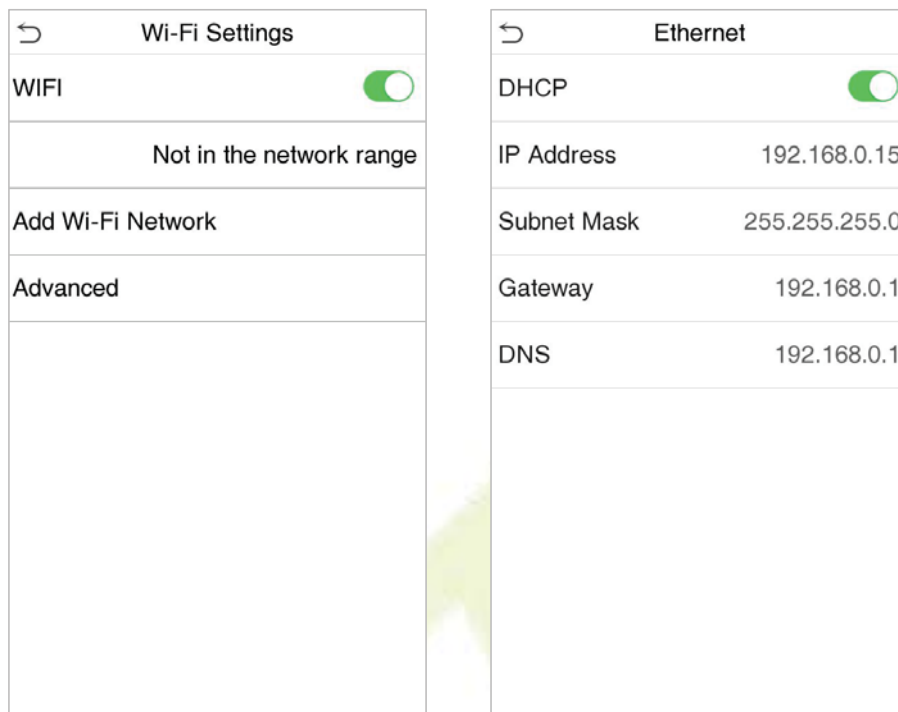
Function Description

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	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. 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.

5.5 Cloud Server Setting

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

Cloud Server Settings	
Server Mode	ADMS
Enable Domain Name	◯
Server Address	192.168.163.61
Server Port	8081
Enable Proxy Server	◯

Function Description

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

5.6 Wiegand Setup

To set the Wiegand input or output parameters.

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

Wiegand Setup	
ID Type	Wiegand Output
Wiegand Options	

Note: The Wiegand interface is shared, and the user can choose to use either the Wiegand input orWiegand outputfunction to interface with differentWiegand devices.

5.6.1 Wiegand Input

Tap **ID Type** on the **Wiegand Setup**, select **Wiegand Input**, and then tap **Wiegand Options** on the
Wiegand Setup.

ID Type	Wiegand Options	
⦿ Wiegand Input	Wiegand Format	
○ Wiegand Output	Wiegand Bits	26
	Pulse Width(us)	100
	Pulse Interval(us)	1000
	ID Type	User ID
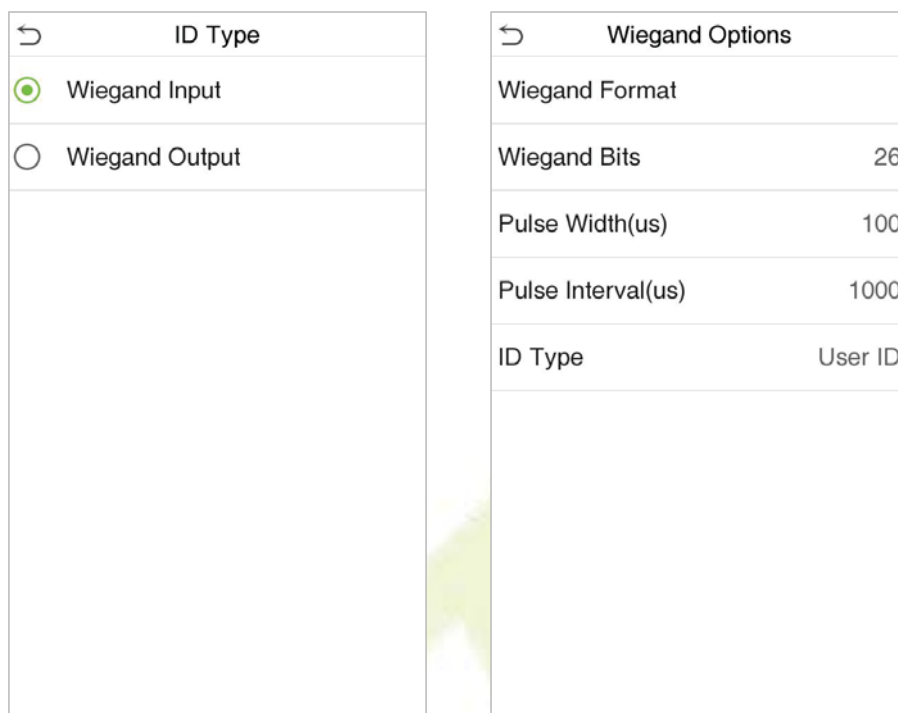
Function Description

Function Name	Descriptions
Wiegand Format	Values range from 26 Bits, 32 Bits, 34 Bits, 36 Bits, 37 Bits, 50 Bits and 64Bits.
Wiegand Bits	Number of bits of 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, which can be adjusted within the range of 200 to 20000 microseconds.
ID Type	Select between User ID and card number.

Various Common Wiegand Format Description

Wiegand Format	Description
Wiegand26	ECCCCCCCCCCCCCCCCCCCCCCCCO 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.

Wiegand26a	ESSSSSSSSSCCCCCCCCCCCCCCCCO 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.
Wiegand34	ECCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO 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.
Wiegand34a	ESSSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCO 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.
Wiegand36	OFFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCMME 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.
Wiegand36a	EFFFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCO 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.
Wiegand37	OMMMMSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCE 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.
Wiegand37a	EMMMFFFFFFFFFFSSSSSSCCCCCCCCCCCCCCCCO 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, and15th to 20th bits are the site codes, and the 21st to 36th bits are the card numbers.
Wiegand50	ESSSSSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO 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.
"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.

5.6.2 Wiegand Output

Tap **ID Type** on the **Wiegand Setup**, select **Wiegand Output**, and then tap **Wiegand Options** on the **Wiegand Setup**.

ID Type	Wiegand Options	
○ Wiegand Input	SRB	
⦿ Wiegand Output	Wiegand Format	
	Wiegand Output Bits	26
	Failed ID	Disabled
	Site Code	Disabled
	Pulse Width(us)	400
	Pulse Interval(us)	2000
	ID Type	User ID
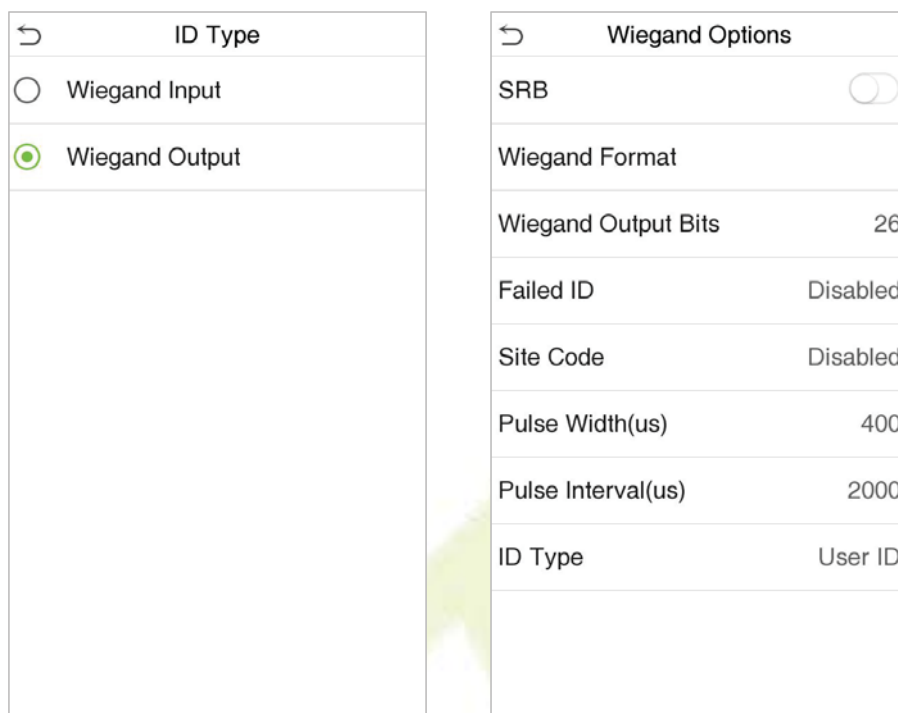
Function Description

Function Name	Descriptions
SRB★	When SRB is enabled, the lock is controlled by the SRB to prevent the lock from being opened due to device removal.
Wiegand Format	Values range from 26 bits, 32 Bits, 34 bits, 36 bits, 37 bits, and 50 bits.
Wiegand Output Bits	After selecting the required Wiegand format, select the corresponding output bit digits of the Wiegand format.
Failed ID	If the verification is failed, 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 in a different device. The valid value ranges from 0 to 256 by default.
Pulse Width(us)	The time width represents the changes of the quantity of electric charge with regular high-frequency capacitance within a specified time.
Pulse Interval(us)	The time interval between pulses.
ID Type	Select the ID types as either User ID or card number.

5.7   Network Diagnosis

To set the network diagnosis parameters.

Tap **Network Diagnosis** on the **Comm.** Settings interface to set the IP address diagnostic and start the diagnostic parameters.
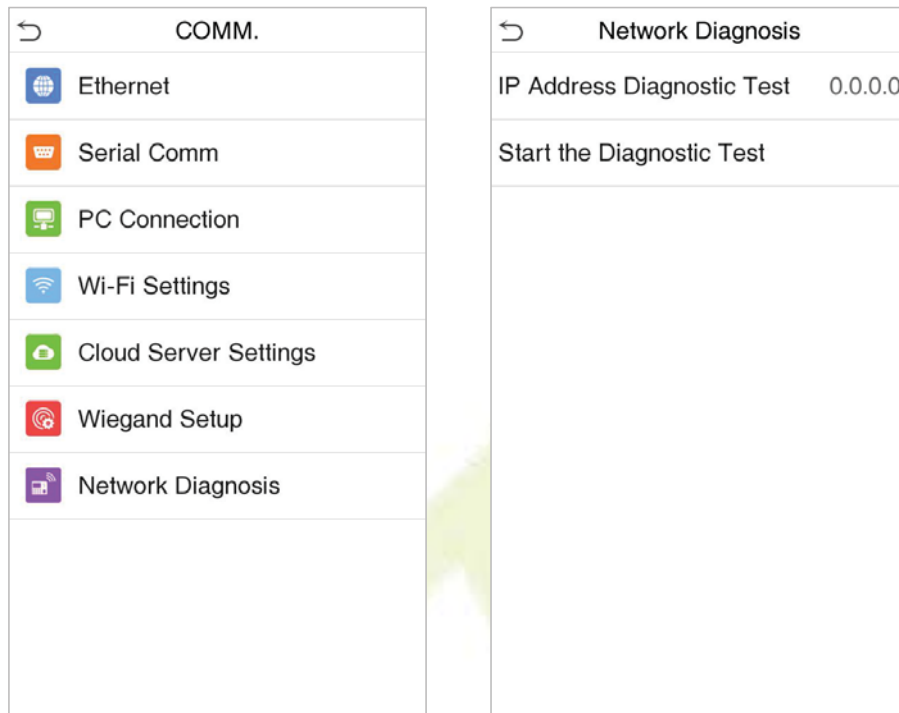
6. <u>System Settings</u>

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

Tap **System** on the **Main Menu** interface to set the related system parameters to optimize the performance of the device.
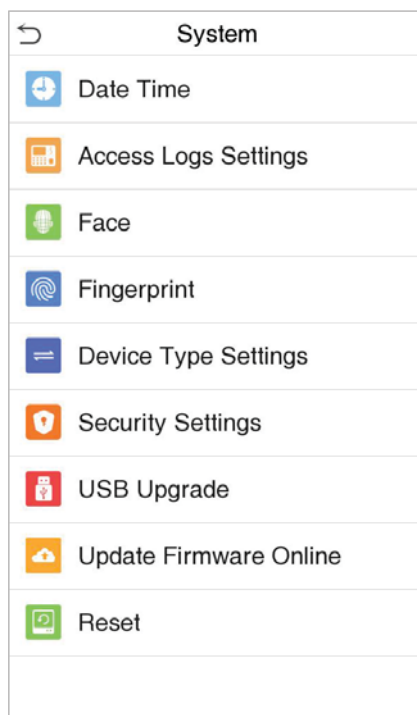
6.1 Date and Time

Tap **Date Time** on the **System** interface to set the date and time.
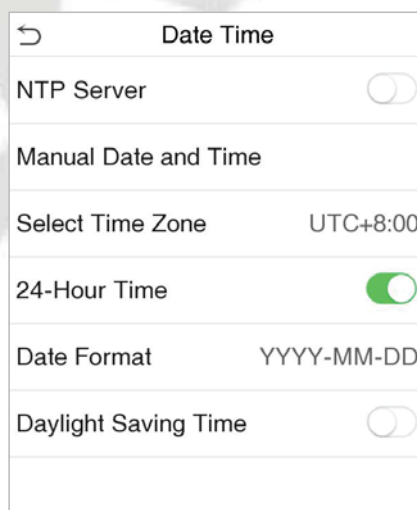
- The product supports the NTP synchronization time system by default. This function takes effect after **NTP Server** is enabled and the corresponding NTP server address link is set.
- If users need to set date and time manually, disable **NTP Server** first, and then tap **Manual Data and Time** to set date and time and tap **Confirm** to save.

- Tap **24-Hour Time** to enable or disable this format. If enabled, then select the **Date Format** to set the date format.

- 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.

Week mode   Date mode

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

Note: *For example, the user sets the time of the device (18:35 on March 15, 2019) to 18:30 on January 1, 2020. After restoring the factory settings, the time of the equipment will remain 18:30 on January 1, 2020.*

6.2   Access Logs Settings

Click **Access Logs Settings** on the System interface.

Function Description

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

Periodic Del of Access Logs	When access records have reached full capacity, the device will automatically delete a set of old access records. Users may disable the function or set a valid value between 1 and 999.
Periodic Del of T&A Photo	When attendance photos have reached full capacity, the device will automatically delete 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 have reached full capacity, the device will automatically delete 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 time length of the message of successful verification displays. Valid value: 1~9 seconds.
Recognition Interval (s)	To set the facial template matching time interval as required. Valid value: 0~9 seconds.

6.3   Face Template Parameters

Tap **Face** on the **System** interface to go to the face template 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
1:N Threshold	Under 1:N verification mode, the verification will only be successful when the similarity between the acquired facial image and all registered facial templates is greater than the set value. The valid value ranges from 0 to 100. The higher the thresholds, the lower the misjudgement rate, the higher the rejection rate, and vice versa. It is recommended to set the default value of 75.
1:1 Threshold	Under 1:1 verification mode, the verification will only be successful when the similarity between the acquired facial image and the user's facial templates enrolled in the device is greater than the set value. The valid value ranges from 0 to 100. The higher the thresholds, the lower the misjudgement rate, the higher the rejection rate, and vice versa. It is recommended to set the default value of 63.
Face Enrollment Threshold	During face template enrollment, 1:N comparison is used to determine whether the user has already registered before. When the similarity between the acquired facial image and all registered facial templates is greater than this threshold, it indicates that the face template has already been registered.
Image Quality	Image quality for facial registration and comparison. The higher the value, the clearer the image requires.
Facial Recognition Distance	Face template recognition of the maximum distance, greater than this value will be filtered. The parameter value can be understood as the face template size required for registration and comparison. The farther the distance from people, the smaller the face template pixels obtained by the algorithm. When the value is 0, it means that the face template comparison distance is not limited.
Anti-spoofing Using NIR	Using near-infrared spectra imaging to identify and prevent fake photos and videos attack
Binocular Live Detection Threshold	It is convenient to judge whether the near-infrared spectral imaging is fake photo and video. The larger the value, the better the anti-spoofing performance of near-infrared spectral imaging.
Face AE	When the face is in front of the camera in Face AE mode, the brightness of the face area increases, while other areas become darker.
WDR	Wide Dynamic Range (WDR) balances light and extends image visibility for surveillance videos under high contrast lighting scenes and improves object identification under bright and dark environments.
Anti-flicker Mode	Used when WDR is turned off. This helps reduce flicker when the device's screen flashes at the same frequency as the light.
Face Algorithm	Facial algorithm related information and pause facial template update.
Notes	Improper adjustment of the exposure and quality parameters may severely affect the performance of the device. Please adjust the exposure parameter only under the guidance of the after-sales service personnel of our company.

6.4   Fingerprint Parameters★

Click **Fingerprint** on the System interface.

	Fingerprint	
1:1 Threshold		15
1:N Threshold		35
FP Sensor Sensitivity		Low
1:1 Retry Attempts		3
Fingerprint Algorithm	ZKFinger VX13.0	
Fingerprint Image		None

FRR	FAR	Recommended matching thresholds	
		1:N	1:1
High	Low	45	25
Medium	Medium	35	15
Low	High	25	10

Function Description

Function Name	Descriptions
1:1 Threshold	Under 1:1 verification method, the verification will only be successful when the similarity between the acquired fingerprint data and the fingerprint template associated with the entered user ID enrolled in the device is greater than the set value.
1:N Threshold	Under 1:N verification method, the verification will only be successful when the similarity between the acquired fingerprint data and the fingerprint templates enrolled in the device is greater than the set value.
FP Sensor Sensitivity	To set the sensibility of fingerprint acquisition. It is recommended to use the default level "**Medium**". When the environment is dry, resulting in slow fingerprint detection, you can set the level to "**High**" to raise the sensibility; when the environment is humid, making it hard to identify the fingerprint, you can set the level to "**Low**".
1:1 Retry Attempts	In 1:1 Verification, users might forget the registered fingerprint, or press the finger improperly. To reduce the process of re-entering user ID, retry is allowed.
Fingerprint Algorithm	Used to switch the version of the fingerprint algorithm, Finger VX13.0 or Finger VX10.0.

Fingerprint Image	This function is disabled by default. After disabling it, the fingerprint image will not be displayed when registering and verifying fingerprints. The menu interface allows to enable or disable this function, and there are security prompts when switching. Four choices are available: **Show for enroll**: to display the fingerprint image on the screen only during enrollment. **Show for match**: to display the fingerprint image on the screen only during verification. **Always show**: to display the fingerprint image on screen during enrollment and verification. **None**: not to display the fingerprint image.

6.5   Device Type Setting

Tap **Device Type Setting** on the System interface.

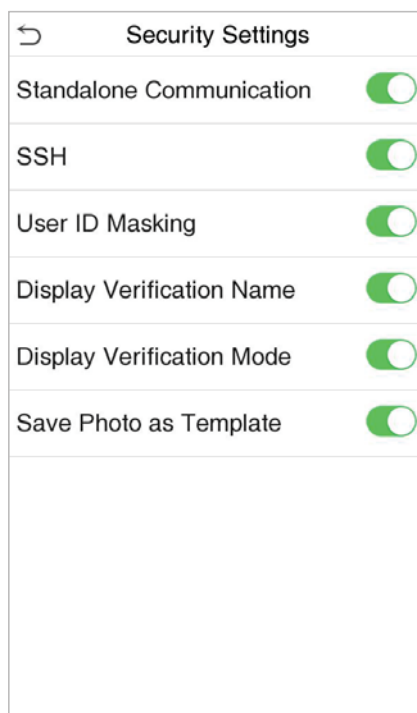| Device Type Settings	
Communication Protocol	PUSH Protocol
Device Type	A&C PUSH
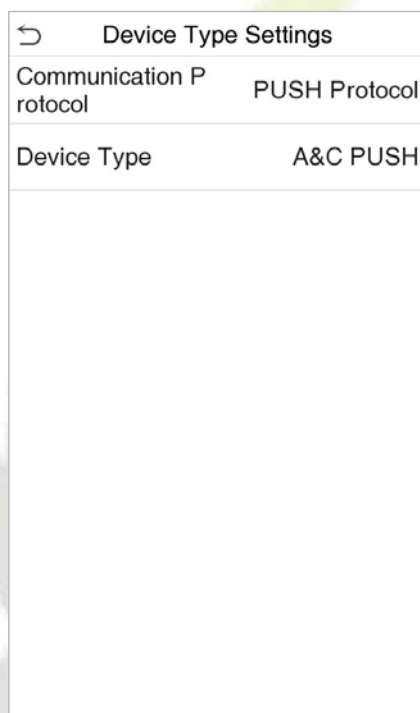
Function Description

Function Name	Description
Communication Protocol	Set the device communication protocol. (BEST protocol is managed by ZKBio Zlink, please refer to 15 Connecting to ZKBio Zlink Web and 16 Connecting to ZKBio Zlink App.)
Device Type	Set the device as time attendance terminal (T&A PUSH) or access control terminal (A&C PUSH).

6.6   Security Setting

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

Function Description

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

6.7   USB Upgrade

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

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

If no USB disk is inserted in, the system gives the following prompt after you tap **USB Upgrade** on the System interface.
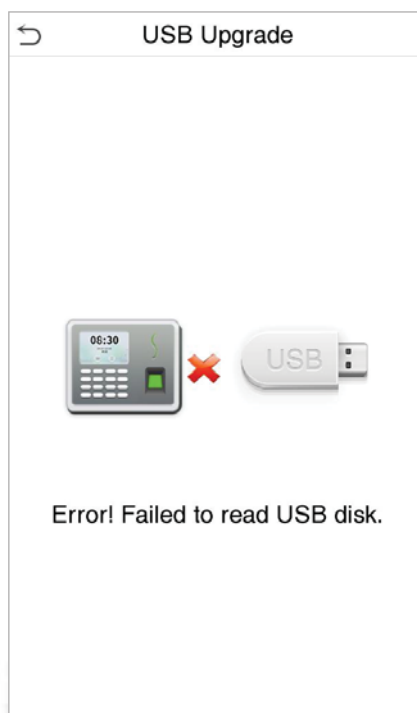
Note: *If upgrade file is needed, please contact our technical support. Firmware upgrade is not recommenced under normal circumstances.*

6.8   Update Firmware Online

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

Click **Enable firmware update online** function, the device will prompt that the update may bring some data security risks, which requires manual confirmation by the user (If the security setting function is turned off, the risk warning will not be displayed when the online update is turned on).
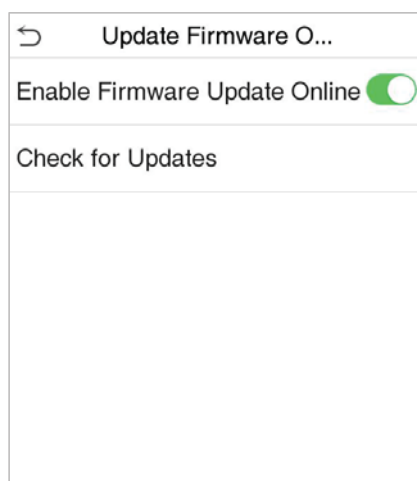
Click **Check for Updates** it may have the following 3 scenarios:

- If the query fails, the interface will prompt "Query failed".
- If the firmware version of the device is latest, it will prompt that the current firmware version is already the latest.
- If the firmware version of the device is not the latest, the version number and change log of the latest version will be displayed. Users can choose whether to update to the latest firmware version.

6.9 Factory Reset

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

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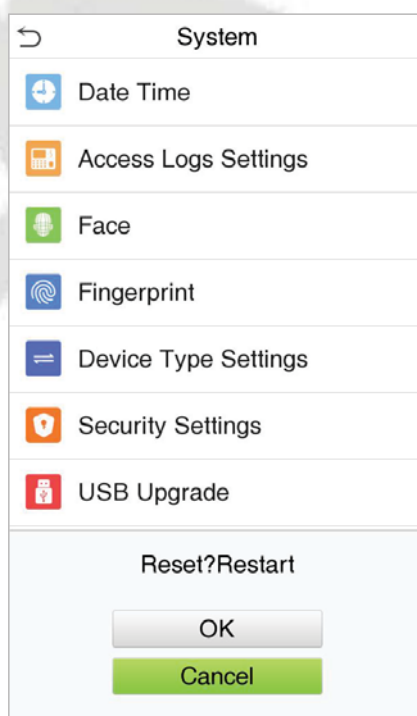
7. Personalize Settings

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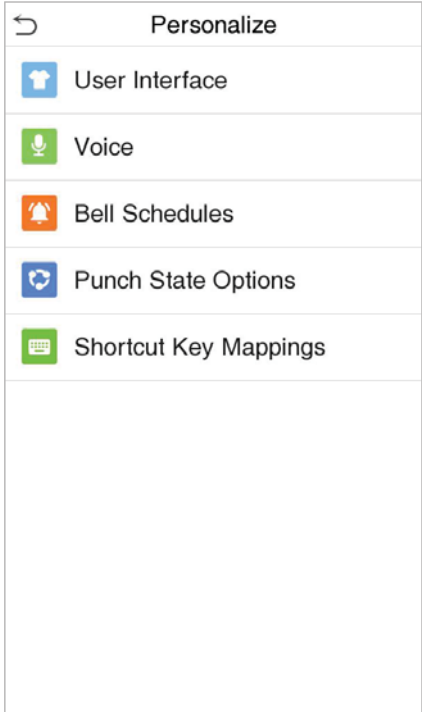
7.1 User Interface Settings

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

Function Description

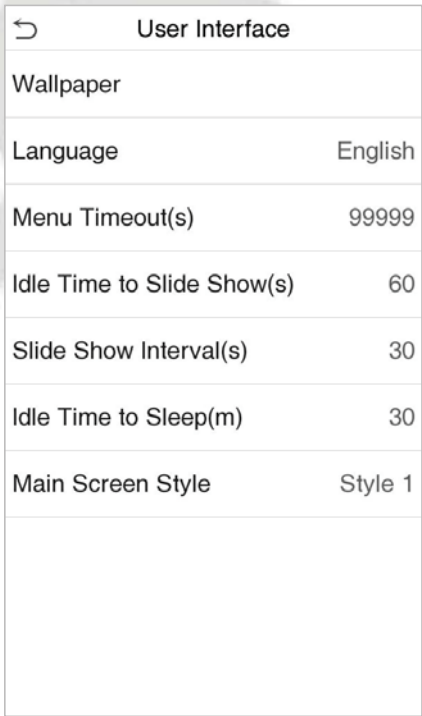| Function Name	Description
Wallpaper	The main screen wallpaper can be selected according to the user preference.
Language	Select the language of the device.
Menu Timeout (s)	When there is no operation, and the time exceeds the set value, the device will automatically go back to the initial interface. The function either can 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 will be played. 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 photos. 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. Tap the screen anywhere to resume normal working mode. This function can be disabled or set a value within 1-999 minutes.
Main Screen Style	The main screen style can be selected according to the user preference.

7.2   Voice Settings

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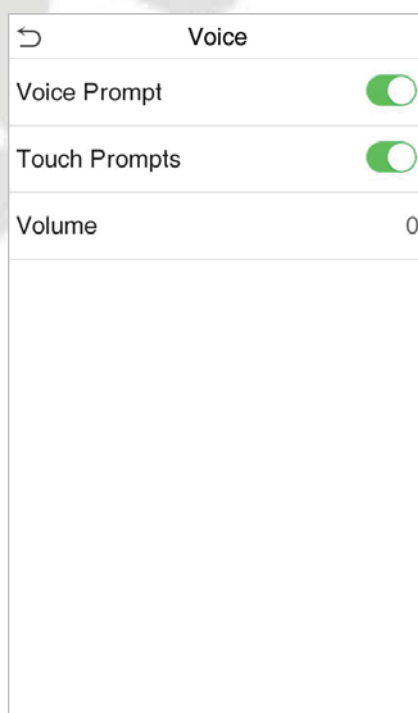
Function Description

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 to 100.

7.3 Bell Schedules

Tap **Bell Schedules** on the **Personalize** interface to configure the Bell settings.
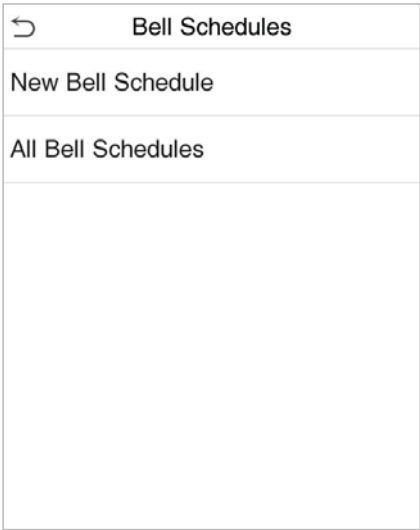
● **New bell schedule**

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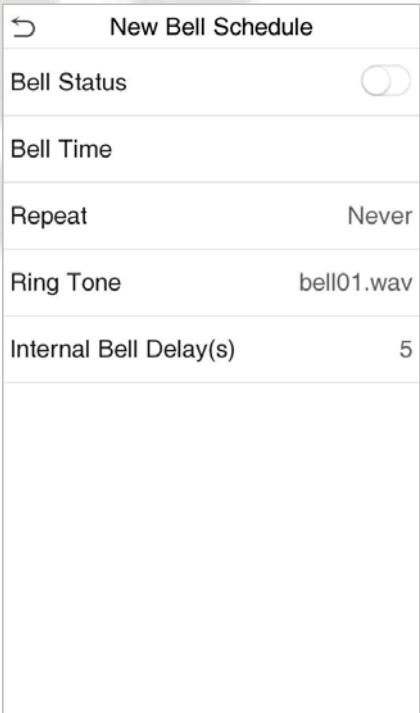
Function Description

Function Name	Description
Bell Status	Toggle to enable or disable the bell status.
Bell Time	Once the required time is set, the device will automatically trigger to ring the bell during that time.
Repeat	Set the required number of counts to repeat the scheduled bell.
Ring Tone	Select a ring tone.
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.

7.4 Punch States Options

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

Function Description

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

7.5　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 Mappi...	
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.

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

- **Set the Switch Time**
    - The switch time is set in accordance with the punch state options.
    - On the **Punch States Options** interface, 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.

↩	Punch State Mode
○	Off
○	Manual Mode
⊙	Auto Mode
○	Manual and Auto Mode
○	Manual Fixed Mode
○	Fixed Mode

↩	F1	
Punch State Value		0
Function		Punch State Options
Name		
Set Switch Time		

↩	Switch Cycle
☑	Monday
☑	Tuesday
☑	Wednesday
☑	Thursday
☑	Friday
☑	Saturday
☑	Sunday

↩	Set Switch Time	
Switch Cycle		Daily
Monday		
Tuesday		
Wednesday		
Thursday		
Friday		
Saturday		
Sunday		

Monday

11:30

▲   ▲

11   30

▼   ▼

HH   MM

Confirm (OK)   Cancel (ESC)

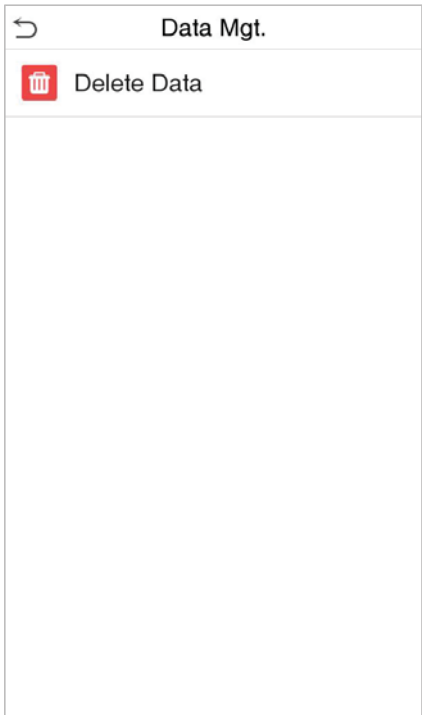| ↩	Set Switch Time	
Switch Cycle		Daily
Monday		11:30
Tuesday		
Wednesday		
Thursday		
Friday		
Saturday		
Sunday		

8. Data Management

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

Data Mgt.
🗑 Delete Data

8.1 Delete Data

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

Delete Data ⇅
Delete Access Records
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

Delete 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
Delete Contact List

Function Description

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 information and attendance logs/access records of all registered users.
Delete Admin Role	To remove all administrator privileges.
Delete Access Control	To delete all access data.
Delete User Photo Templates	To delete user photo templates in the device. When deleting template photos, there is a risk reminder: "**Face re-registration is required after an algorithm upgrade.**"
Delete Profile Photo	To delete all user photos in the device.
Delete Wallpaper	To delete all wallpapers in the device.
Delete Screen Savers	To delete the screen savers in the device.
Delete Contact List	To delete all contact list of video intercom in the device.

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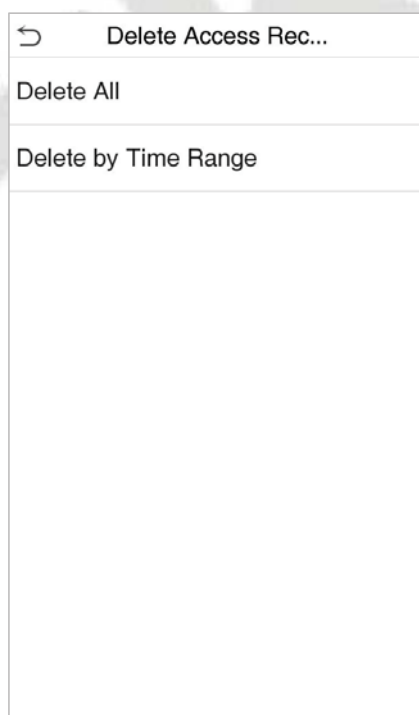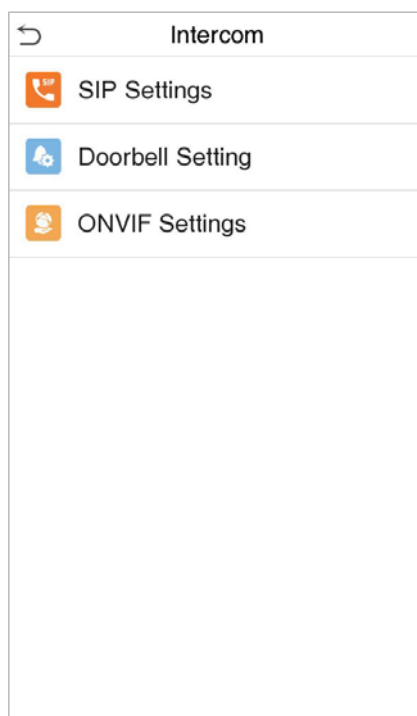

Select **Delete by Time Range**.   Set the time range and click **OK**.
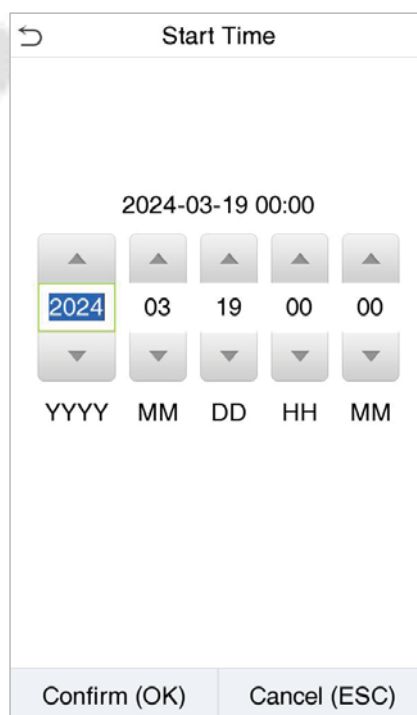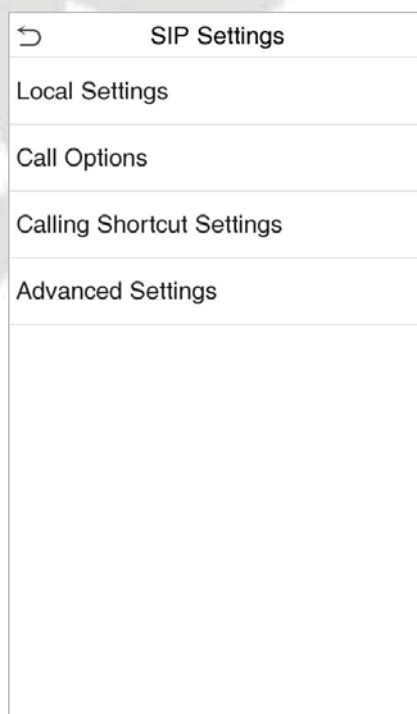
9. <u>Intercom</u>

Click **Video intercom Parameters** on the System interface.

9.1 SIP Settings

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

Tap **SIP Settings** on the **Video intercom Parameters** interface to go to the monitoring SIP settings.

Function Description

Function Name		Description
Local Settings	**SIP Server**	Select whether to enable the server address. Once enabled, you need to set the server address, server port, display name, user name and password.
	Master Account Settings	Select whether to enable the master server address. Once enabled, you need to set the server address, server port, display name, user name and password. ***Note:*** *Turning off this feature disables the SIP server function.* **Enable Domain Mode:** Select whether to enable domain mode. **Server Address:** Enter the server address. **Server Port:** Enter the server port. **Display Name:** Enter the display name of the server. **User Name:** Enter the user name of the server. **Verify ID:** Enter the authentication ID of the server. **Password:** Enter the password of the server. **Transport Protocol:** Set the transmission protocol between the device and indoor unit.
	Backup Account Settings	Select whether to enable the backup server address. Once enabled, you need to set the server address, server port, display name, user name and password. **Enable Domain Mode:** Select whether to enable domain mode. **Server Address:** Enter the server address. **Server Port:** Enter the server port. **Display Name:** Enter the display name of the server. **User Name:** Enter the user name of the server. **Verify ID:** Enter the authentication ID of the server. **Password:** Enter the password of the server. **Transport Protocol:** Set the transmission protocol between the device and indoor unit.
	Device Port	When using the LAN for visual intercom, enter the network port number of the LAN.
	Device Type	You can set the type of the device as entrance station, access control terminal or fence terminal.
	Local Information	Set the information of the householder that the device specifically corresponds to, including block, unit, floor and door.
	Transport Protocol	Set the transmission protocol between the device and indoor unit.

Call Options	Calling Delay(s)	Set the duration of the calling, valid values are 30 to 60 seconds.
	Talking Delay(s)	Set the duration of the talking, valid values are 60 to 120 seconds.
	Call Volume Settings	Set the volume of the call, valid values are 0 to 100.
	Call Type	Set the type of the call to voice only or voice + video.
	Call Button Style	Change the visual intercom call button on the standby interface of the device, optional doorbell label or phone label .
	Auto Answer Settings	When the indoor unit dials the device successfully, it is automatically connected within the set answer time.
	Encryption	Whether to enable intercom call encryption function.
Contact List		When the SIP server is disabled, you can add the device number and call address of the indoor unit here.
Calling Shortcut Settings		Set the quick call shortcuts in the call interface of visual intercom, the system defaults 5 shortcuts, including a management center and 4 customizable shortcuts. After enabling the shortcuts, customize the name, enter the device number set in the **Contact List**, then automatically match the IP address, after the operation is completed, then click on the generated customized name (shortcut) in the call interface of the visual intercom to call directly. Support standard mode and direct calling mode, in direct calling mode, users can call multiple indoor units at the same time. **Note:** *When the SIP server is enabled, Direct Calling Mode can only call the Management Center*
Advanced Settings		Set the DTMF type and DTMF value of the device, the value should be set to the same as the DTMF value of the indoor unit.

9.1.1 Connecting to SIP Server

Note: *When the SIP server is enabled, it is advised to select TCP mode first and UDP mode second, because TCP mode is more stable. When this function is enabled, the Contact List are not displayed.*

Tap **SIP Settings** > **Local Settings** on the **Video intercom Parameters** interface to go to the monitoring parameter settings.
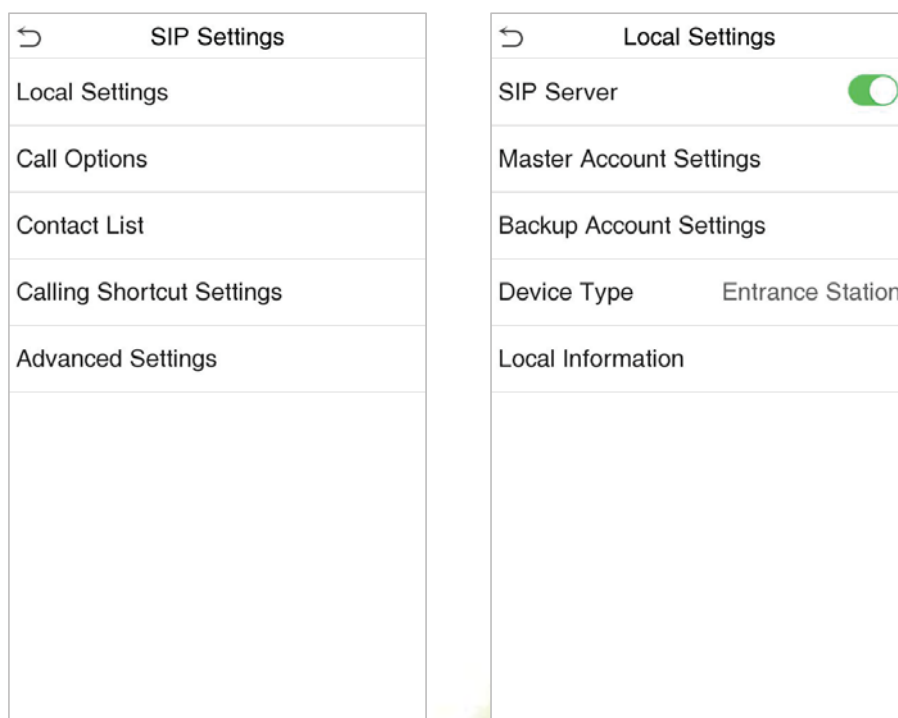
1. On SenseFace 7 Series device, tap **Local Settings** on the **SIP Settings** interface, after the device is rebooted, enter the server-related parameters.

2. Once the SIP is set up correctly, a green dot will appear in the upper right corner of the call page to indicate that the SenseFace 7 Series device is connected to the server. You can call the account name of the indoor station.

    Note: When users need to enable SIP server, they need to purchase the server address and password from the distributor, or build the server confidently.