User Manual

SpeedFace-V5L [TI]

Date: August 2020

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.

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. 26, 188 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 SpeedFace-V5L [TI] Product.

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

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

Document Conventions

Conventions used in this manual are listed below:

GUI Conventions

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

Symbols

Convention	Description
	This implies about the notice or pays attention to, in the manual
	The general information which helps in performing the operations faster
	The information which is significant
	Care taken to avoid danger or mistakes
	The statement or event that warns of something or that serves as a cautionary example.

Table of Contents

1 Safety Measures

The 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. Accessories not recommended by the manufacturer must not be used.
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 exposed to water and/or inclement weather (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 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 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** - External lightning conductors can be installed to protect against electrical storms. It stops power-ups destroying the system.

The devices should be installed in areas with limited access.

2 Overview

SpeedFace-V5L [TI] uses **Thermal Imaging Intelligent Engineering Facial Recognition** algorithms and the latest **Computer Vision Technology**. It supports both facial and palm verification with large capacity and speedy recognition, as well as improves security performance in all aspects.

It adopts touchless recognition technology and new functions namely **Temperature Detection** and **Masked Individual Identification** which eliminates hygiene concerns effectively. It is also equipped with the ultimate **Ant Spoofing** algorithm for facial recognition against almost all types of fake photos and videos attack. It has 3-in-1 palm recognition (Palm Shape, Palm Print, and Palm Vein) is performed in 0.35 sec per hand; the palm data acquired is compared with a maximum of 3,000 palm templates.

The terminal with temperature and 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 body temperature measurement and masked individual identification functions during facial and palm verification.

Features

- Visible Light Facial Recognition.
- Better hygiene with touchless biometric authentication, temperature detection and masked individual identification.
- Thermal Imaging Temperature Detection, 0.1s high-speed detection, measurement distance of 30 to 120cm.
- Anti-spoofing algorithm against print attack (laser, color and B/W photos), videos attack and 3D mask attack.
- Multiple Verification Methods: **Face / Palm / Fingerprint / Password**

Special Functions

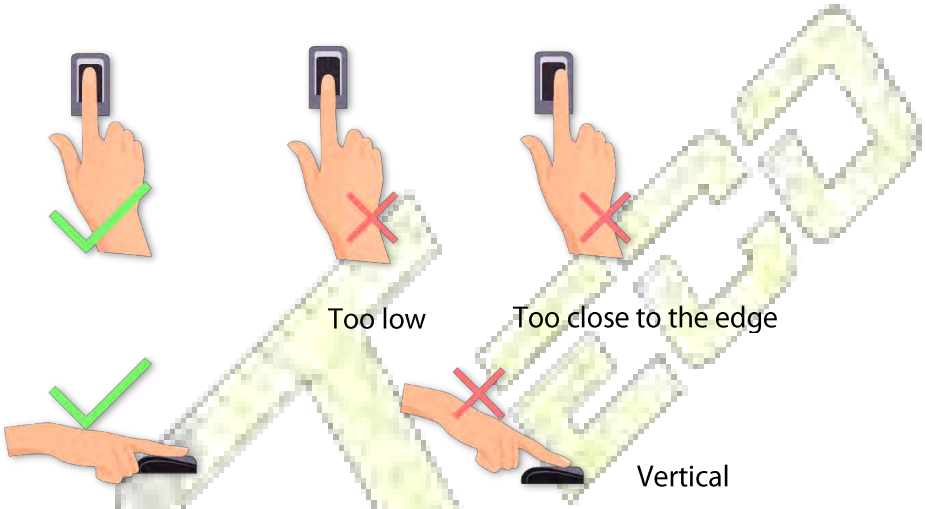
- Mask detection.
- Body temperature detection.
- Temperature Measurement Distance: **30cm ~ 120cm (0.98ft~ 3.94ft).**
- Temperature Measurement Accuracy: **±0.3°C (±0.54°F)**
  (Tested at a distance of 80cm (2.63ft) under 25°C (77° F) temperature)
- Temperature Measurement Range: **20°C ~ 50°C (68°F ~ 122°F)**

3 Instruction for Use

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

3.1 Finger Positioning

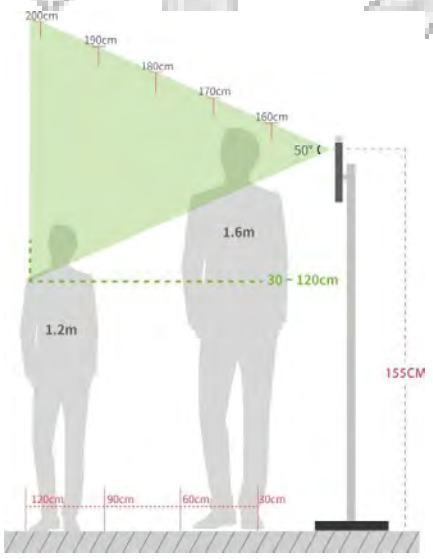
Recommended fingers: It is recommended to use index, middle, or ring finger for registration and avoid using the thumb or pinky, as they are difficult to accurately press onto the fingerprint reader.



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

3.2 Standing Position, Posture and Facial Expression

- **The recommended distance**



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

- **Recommended Standing Posture and Facial Expression**

Standing Posture

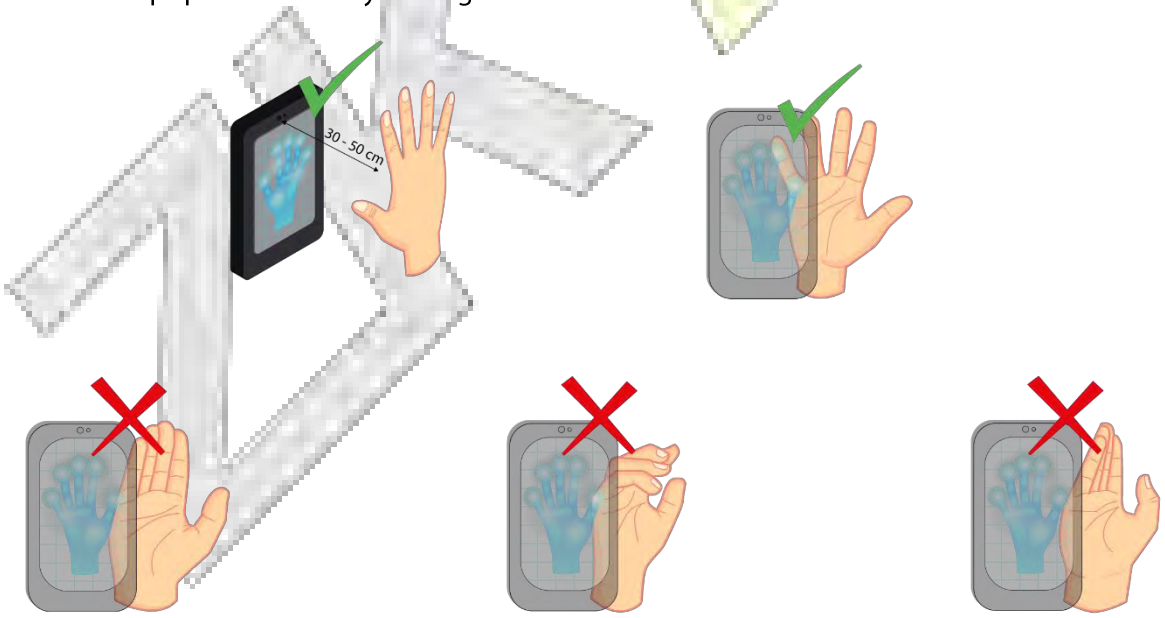
Facial Expression

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

3.3 Palm Registration

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

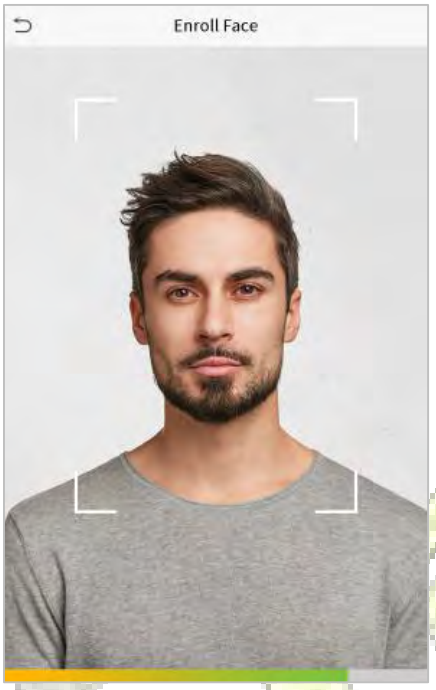
Make sure to keep space between your fingers.



NOTE: Place your palm within 30-50cm of the device.

3.4 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

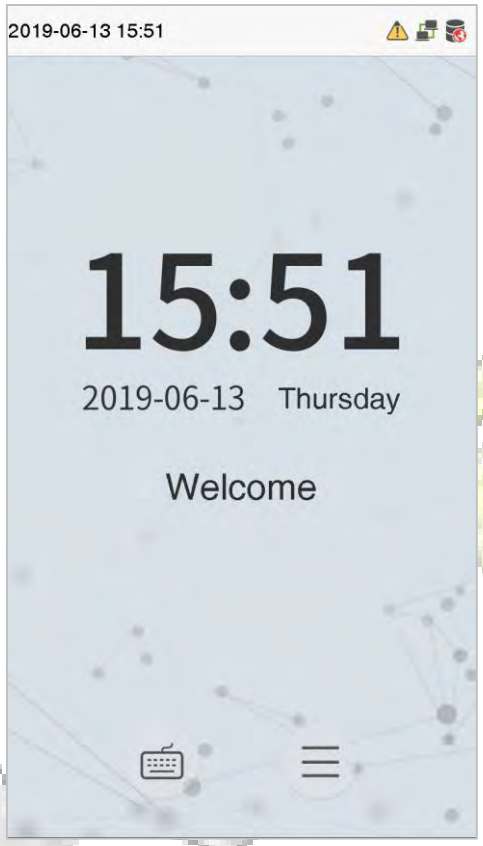
- **Recommendation for registering a face**
  - When registering a face, maintain a distance of 40cm to 80cm between the device and the face.
  - Be careful not to change your facial expression. (smiling face, drawn face, wink, etc.)
  - If you do not follow the instructions on the screen, the face registration may take longer or may fail.
  - Be careful not to cover the eyes or eyebrows.
  - Do not wear hats, masks, sunglasses, or eyeglasses.
  - Be careful not to display two faces on the screen. Register one person at a time.
  - It is recommended for a user wearing glasses to register both faces with and without glasses.

- **Recommendation for authenticating a face**
  - Ensure that the face appears inside the guideline displayed on the screen of the device.
  - If the glasses have been changed, authentication may fail. If the face without glasses has been registered, authenticate the face without glasses further. If the face with glasses has been registered, authenticate the face with the previously worn glasses.

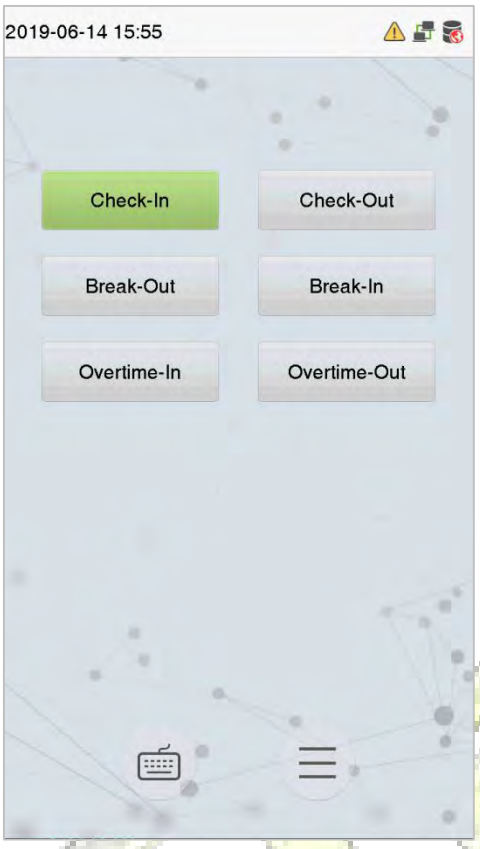
- If a part of the face is covered with a hat, a mask, an eye patch, or sunglasses, authentication may fail. Do not cover the face, allow the device to recognize both the eyebrows and the face.

3.5 Standby Interface

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



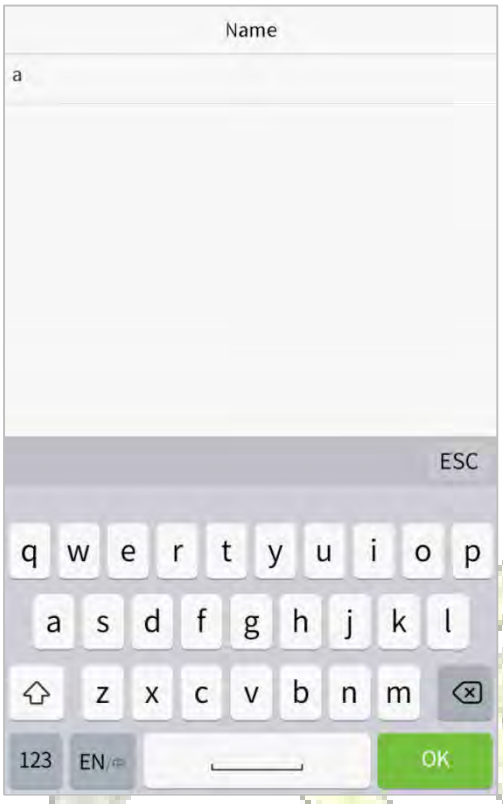
- Click to enter the User ID input interface.
- When there is no Super Administrator set in the device, tap to go to the menu.
- After setting the Super Administrator on the device, it requires the Super Administrator's verification before entering the menu functions.
  NOTE: For the security of the device, it is recommended to register super administrator the first time you use the device.
- The punch state options can also be displayed and used directly on the standby interface. 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 "9.4 Punch States Options" in order to get the punch state options on the standby screen.

3.6 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.

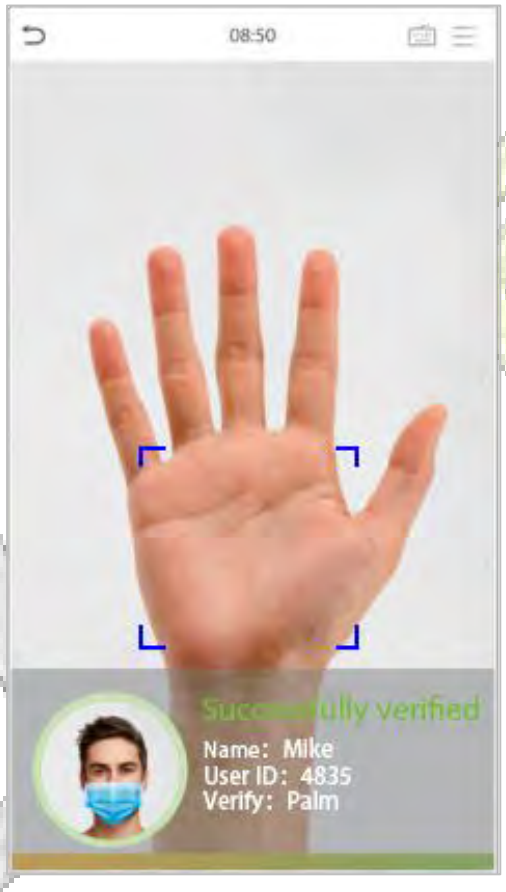
3.7 Verification Mode

3.7.1 Palm Verification

- **1: N Palm Verification mode**

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

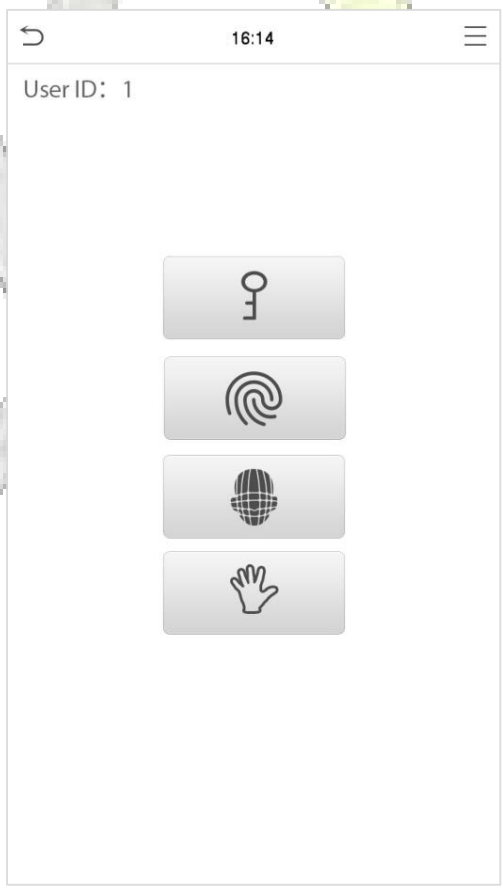
The device automatically distinguishes between the palm and the face verification mode as the user places his/her palm in the scanning area. Then the palm image is collected by the palm collector, and the device matches the collected palm image with all the registered palm and returns an output.



- **1: 1 Palm Verification mode**

Click the button on the main screen to enter 1:1 palm verification mode and input the user ID and press [OK], as shown in image below.

If the user has registered the fingerprint, face, and password in addition to his/her palm, and the verification method is set to palm/ fingerprint/ face/ password verification, the following screen will appear. Select the palm icon to enter palm verification mode. Then place your palm for verification.



3.7.2 Fingerprint Verification

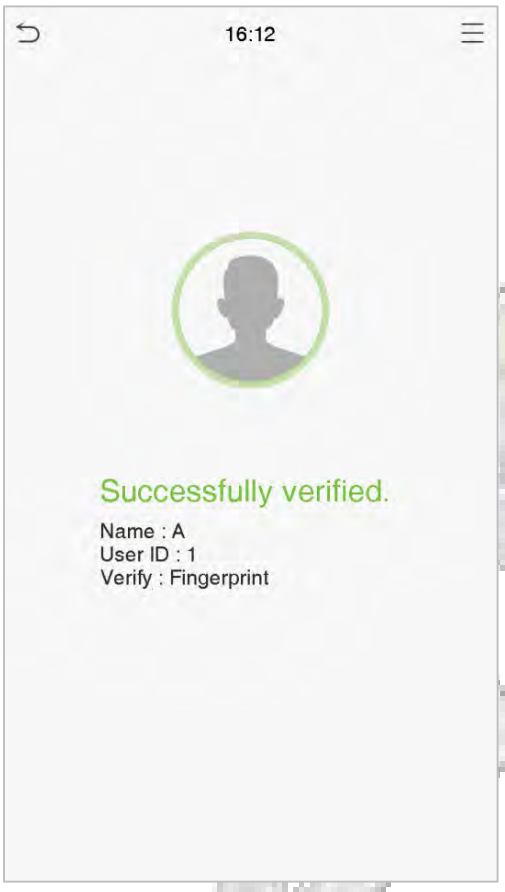
- **1: N fingerprint verification mode**

In this verification mode, the device compares the fingerprint that is being pressed onto the fingerprint reader with all the fingerprint data that is stored in the device and returns an output.

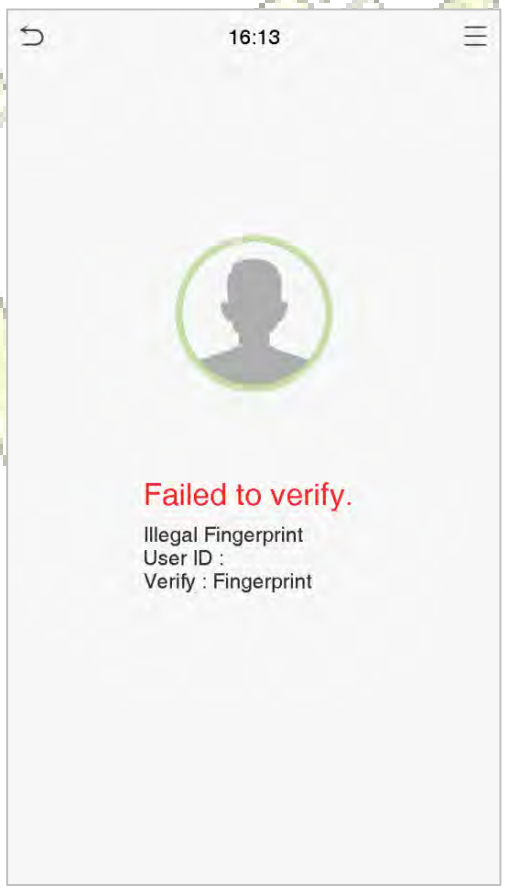
The device enters the fingerprint authentication mode when a user presses his/her finger onto the fingerprint scanner.

NOTE: Please follow the correct way to place your finger onto the sensor. For details, please refer to Finger Positioning

Verification is successful.



Verification is failed.



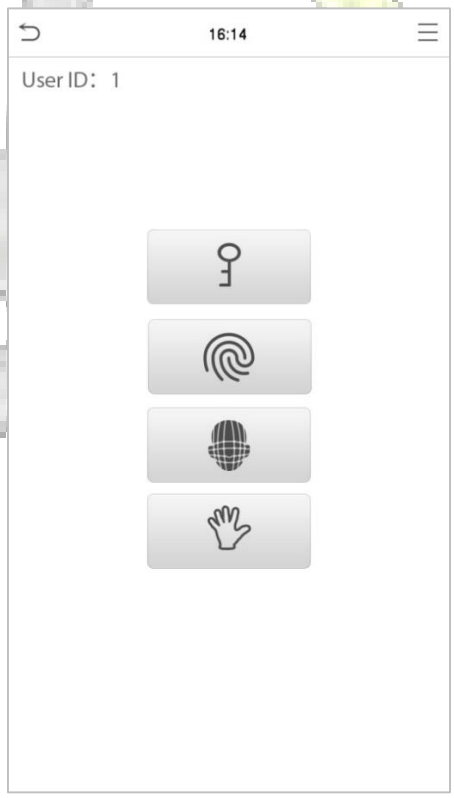
- **1: 1 fingerprint verification mode**

In this mode, the device compares the fingerprint that is being pressed onto the fingerprint reader with the fingerprints that are linked to the User ID input via the virtual keyboard.

Users may try verifying their identities with 1:1 verification mode when they cannot gain access with 1: N authentication method.

Click the button on the main screen to enter 1:1 fingerprint verification mode and input the user ID and press [**OK**].

If the user has registered palm, face, and password in addition to his/her fingerprints, and the verification method is set to palm/ fingerprint/ face /password verification, the following screen will appear. Select the fingerprint icon to enter fingerprint verification mode. Then take fingerprint by pressing onto the fingerprint reader for verification.

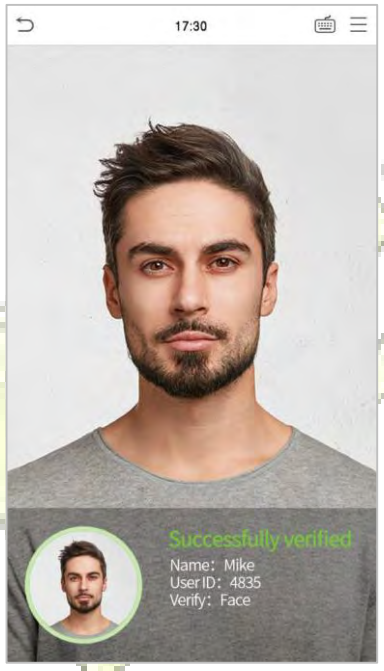


3.7.3 Facial Verification

- **1:N Facial Verification**

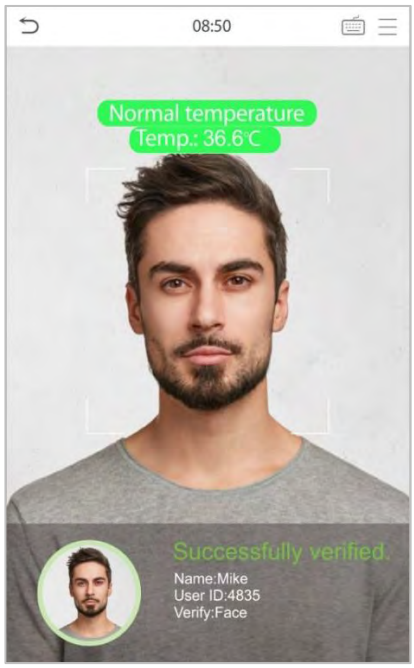
1. Conventional verification

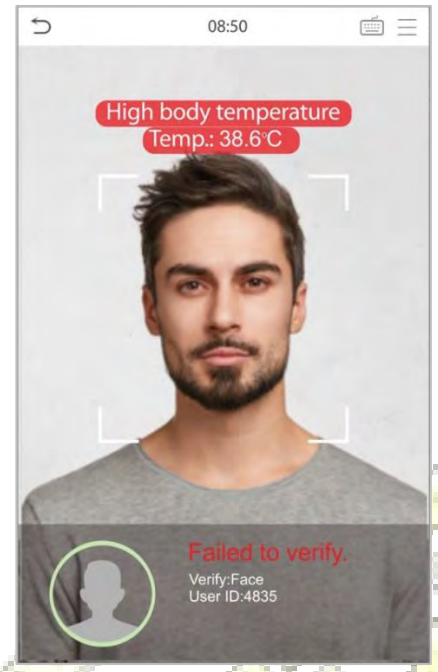
In this verification mode, the device compares the collected facial images with all face data registered in the device. The following is the pop-up prompt of a successful comparison result.



2. Enable temperature screening with infrared

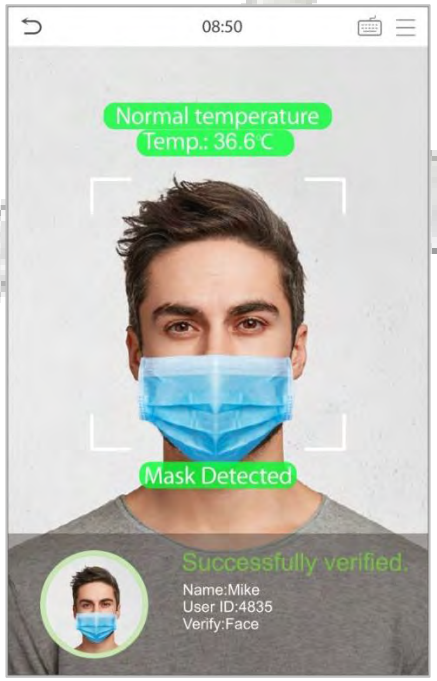
When the user enables the **Enable temperature screening with infrared** function, during user verification, in addition to the conventional verification method, the user's face must be aligned with the temperature measurement area to measure the body temperature before the verification can be conducted. The following are the popups of the comparison result prompt interface. (Note: This function is only applicable to products with temperature measurement module.)

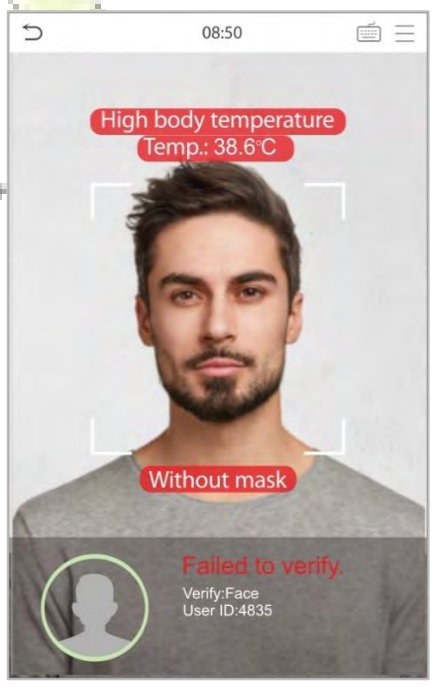




3. Enable mask detection

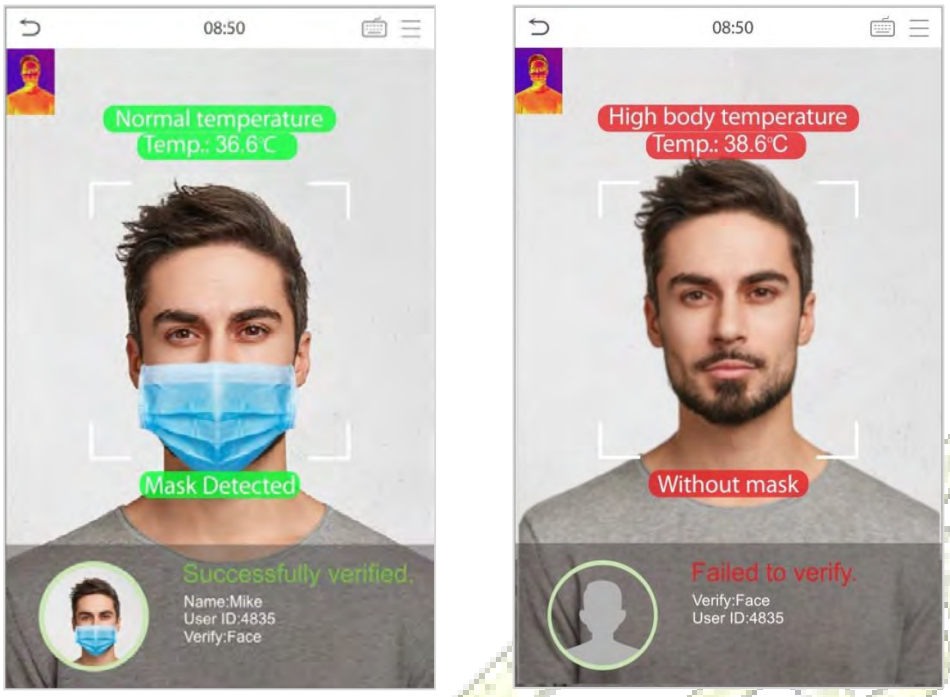
When the user enables the **Enable mask detection** function, the device will identify whether the user is wearing a mask or not while verification. The following are the popups of the comparison result prompt interface. (Note: This function is only applicable to products with temperature measurement module.)





4. Display Thermodynamics Figure

When the user enables the **Display Thermodynamics Figure** function, the thermal image of the person is displayed in the upper left corner of the device, while verification. As shown in the images below:



- **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 click [**OK**].

If the user has registered palm, fingerprint, and password in addition to face, and the verification method is set to palm/ fingerprint/ face /password 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:

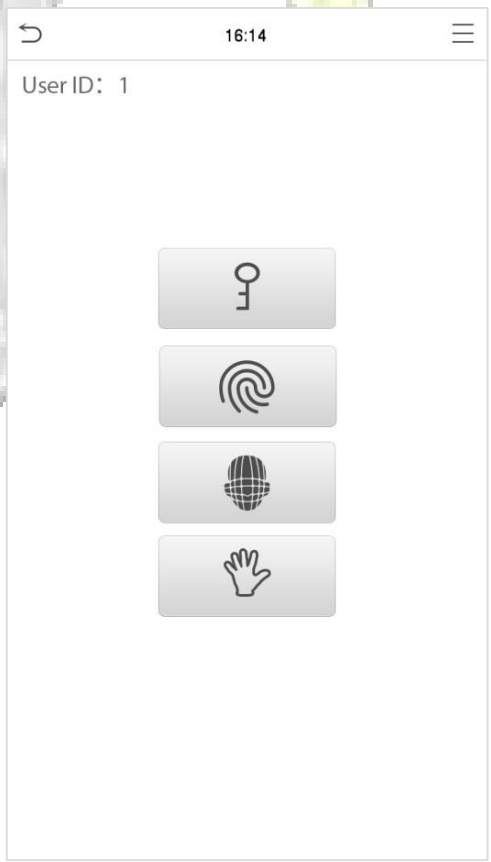
If the verification is failed, it prompts “Please adjust your position!”.

3.7.4 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 palm, fingerprint, and face in addition to password, and the verification method is set to palm/ fingerprint/ face /password verification, the following screen will appear. Select the icon to enter password verification mode.

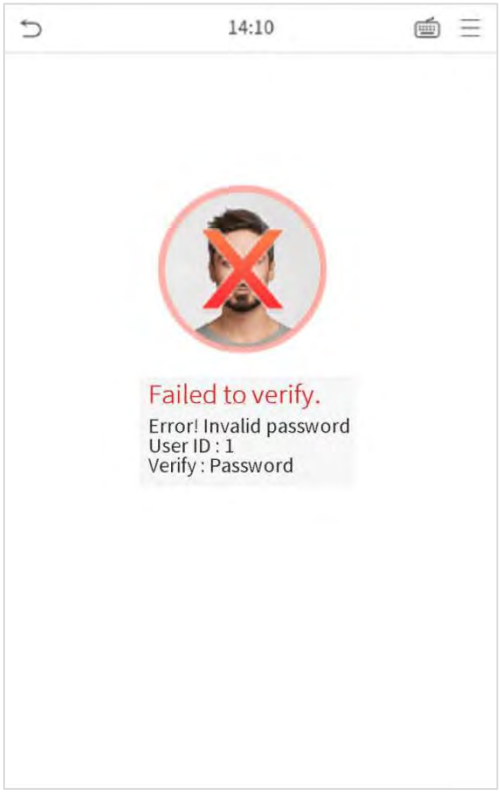


Input the password and press [**OK**].

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

Verification is successful:

Verification is failed:

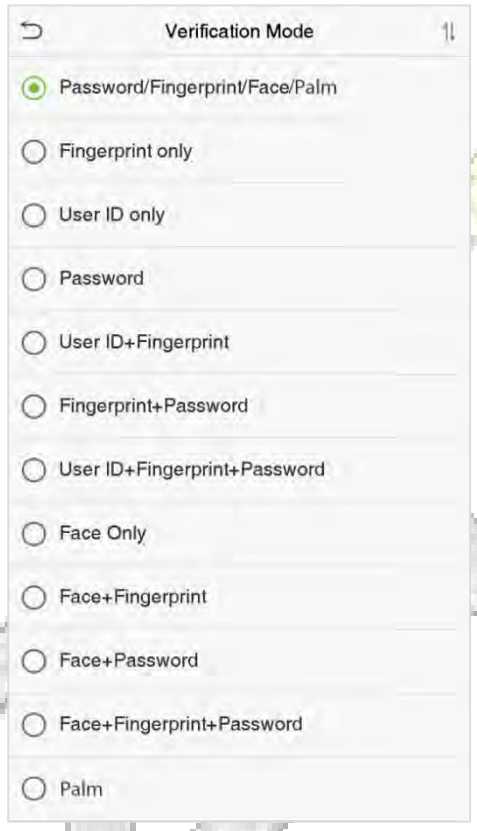


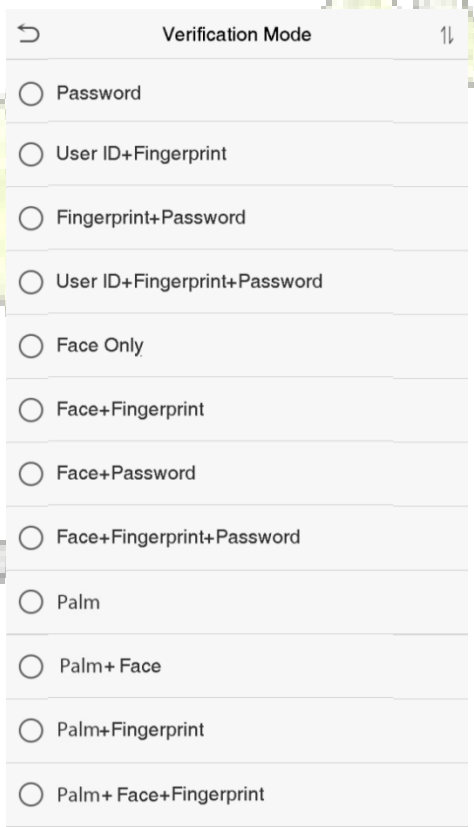
3.7.5 Combined Verification

To increase security, this device offers the option of using multiple forms of verification methods. A total of 15 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.





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 fingerprint data, but the Device verification mode is set as "Fingerprint + Password", the employee will not be able to complete the verification process successfully.
- This is because the Device compares the scanned fingerprint template of the person with registered verification template (both the Fingerprint and the Password) previously stored to that Personnel ID in the Device.

- But as the employee has registered only the Fingerprint but not the Password, the verification will not get completed and the Device displays “Verification Failed”.

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 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 and Wiegand.
System	To set parameters related to the system, including Date & Time, Access Logs Setting, Face, Fingerprint, and Palm parameter, Resetting to factory settings and Detection Management.
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.
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 Attendance record, check Attendance Photos and Blocklist attendance photos.
Autotest	To automatically test whether each module functions properly, including the LCD Screen, Audio, Camera, Fingerprint sensor, and real-time clock.
System Info	To view Data Capacity and Device and Firmware information of the current device.

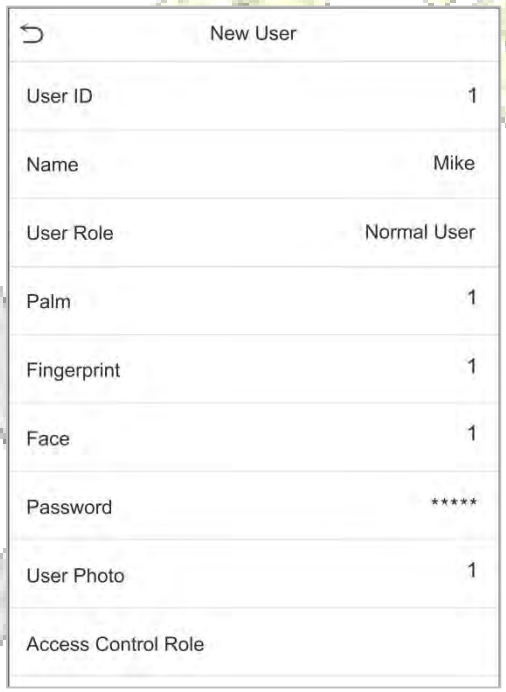
5 User Management

5.1 User Registration

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

5.1.1 User ID and Name

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



Notes:

1) A name can take up to 17 characters.

2) The user ID may contain 1-9 digits by default.

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

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

5.1.2 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 3.7 Verification Method.

5.1.3 Palm

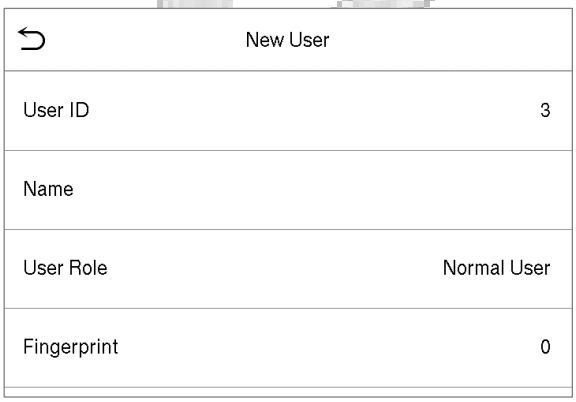
Tap **Palm** in the **New User** interface to enter the palm registration page.

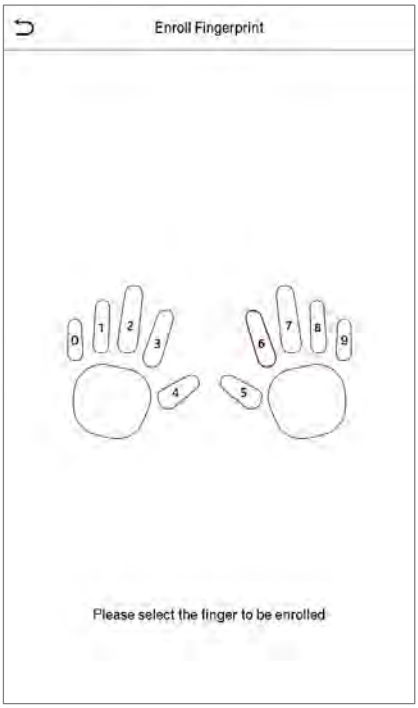
- Select the palm to be enrolled.
- Please place your palm inside the guiding box and keep it still while registering.
- A progress bar shows up while registering the palm and a **"Enrolled Successfully"** is displayed as the progress bar completes.
- If the palm is registered already then, the **"Duplicate Palm"** message shows up. The registration interface is as follows:

5.1.4 Fingerprint

On the **New User** interface, tap on **Fingerprint** to go to the fingerprint registration page.

- On the **Enroll Fingerprint** interface, select the finger to be enrolled.



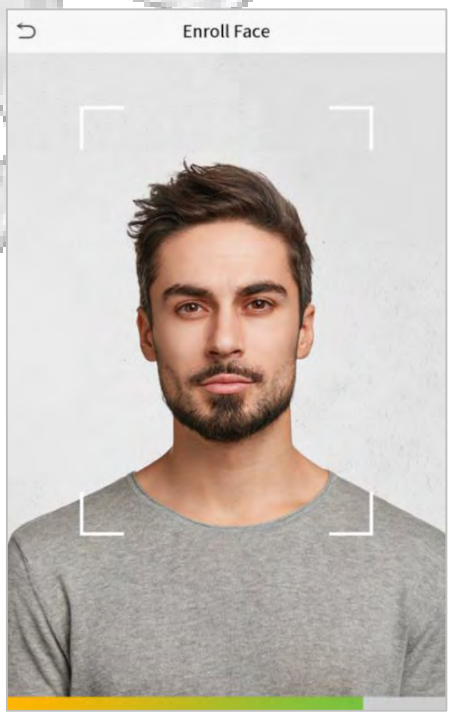


- After the selecting the required finger, press the same finger on the fingerprint reader three times.
- Green indicates that the fingerprint was enrolled successfully.

5.1.5 Face

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

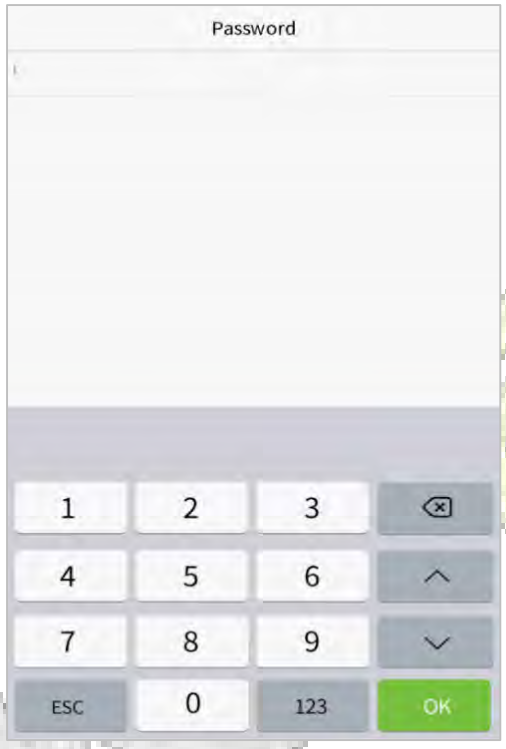
- Please face towards the camera and position your face inside the white guiding box and stay still during face registration.
- A progress bar shows up while registering the face and a **"Enrolled Successfully"** is displayed as the progress bar completes.
- If the face is registered already then the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



5.1.6 Password

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

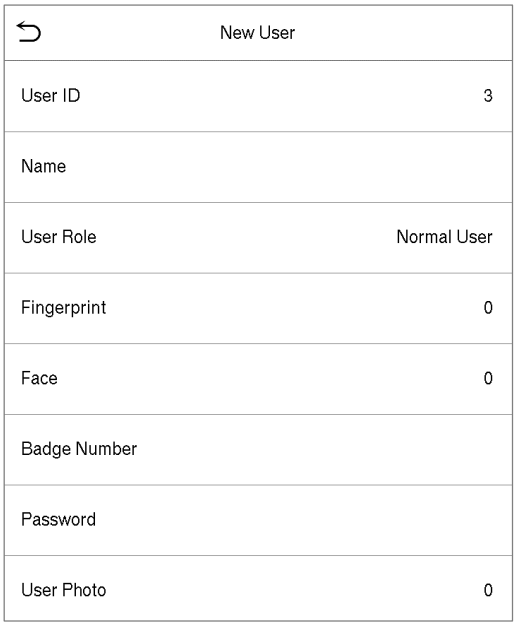
- On the Password interface, enter the required password and re-enter to confirm it and tap **OK**.
- If the re-entered password is different from the initially entered password, then the device prompts the message as "**Password not match!**", where the user needs to re-confirm the password again.

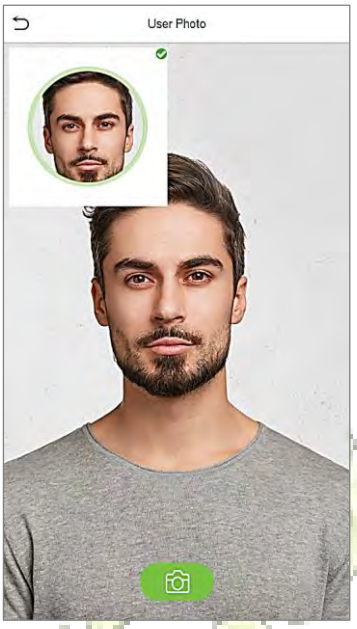


Note: The password may contain 1 to 8 digits by default.

5.1.7 User photo

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





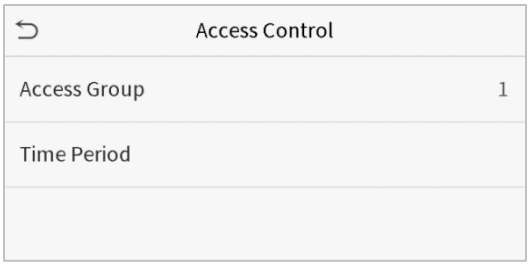
- When a user registered with a photo passes the authentication, the registered photo will be displayed.
- Tap **User Photo**, the device's camera will open, then tap the camera icon to take a photo. The captured photo is displayed on the top left corner of the screen and the camera opens up again to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

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

5.1.8 Access Control Role

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

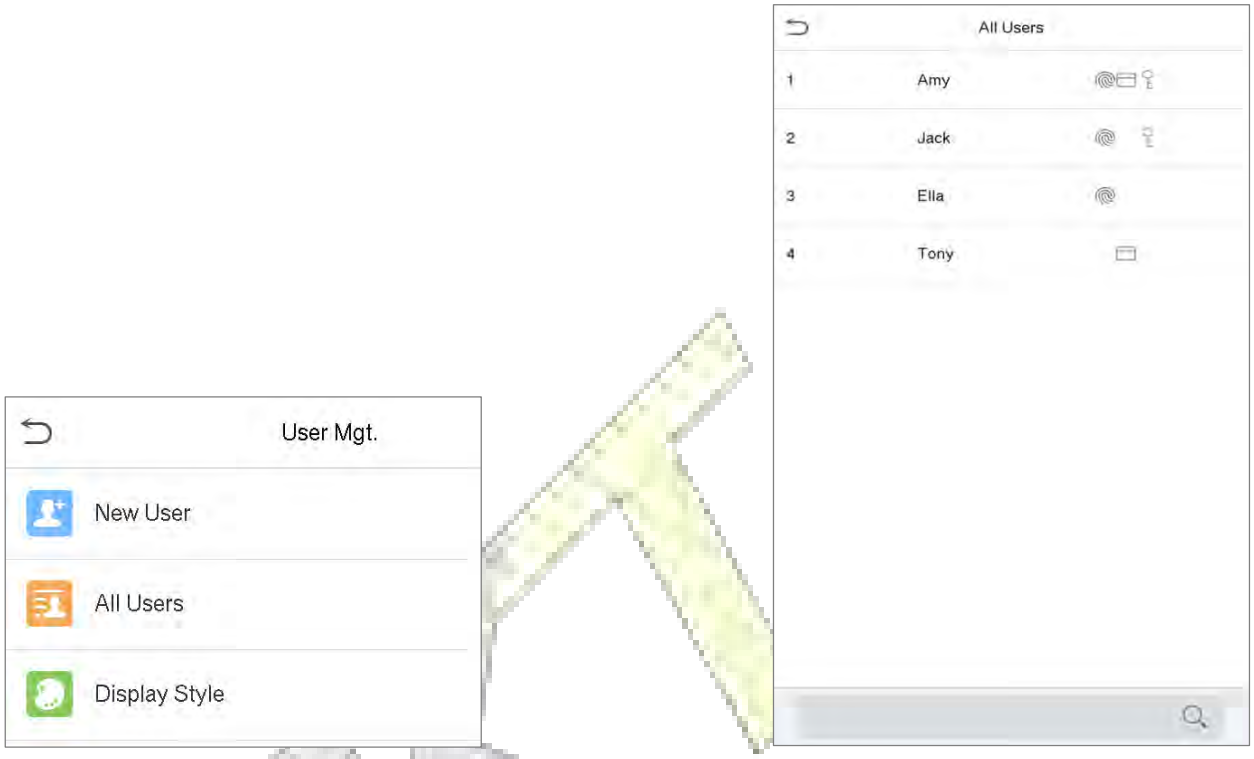
- Tap **Access Control Role** > **Access Group**, to assign the registered users to different groups for better management. New users belong to Group 1 by default and can be reassigned to other groups. The device supports up to 99 Access Control groups.
- Tap **Time Period**, to select the time period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



5.2 Search for Users

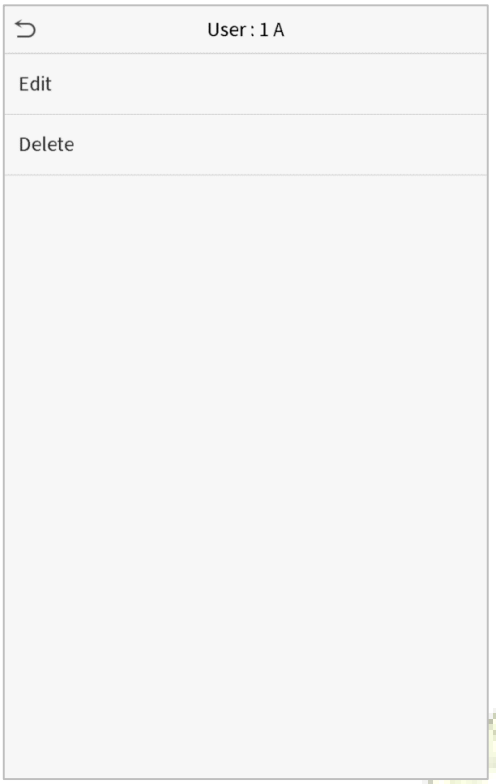
On the **Main Menu**, tap **User Mgt.,** and then tap **All Users** to search for a User.

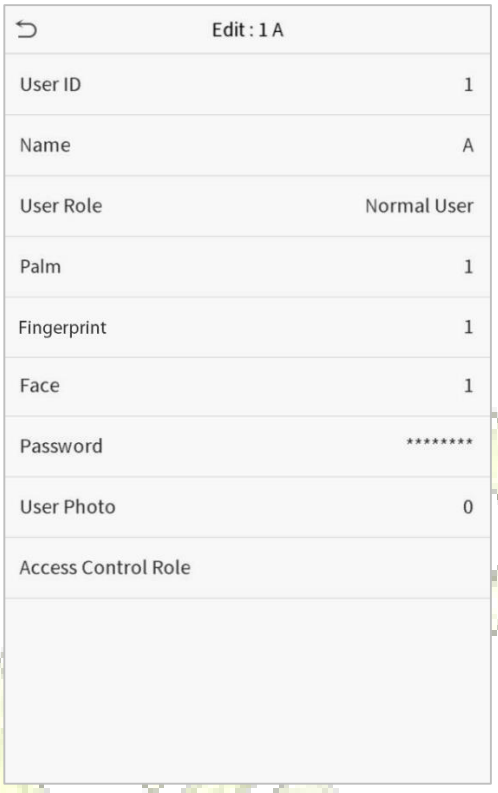
- On the **All Users** interface, tap on the search bar on the user's list to enter the required retrieval keyword (where the keyword may be the user ID, surname or full name) and the system will search for the related user information.



5.3 Edit User

On **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 that of 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 Management".

5.4 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.

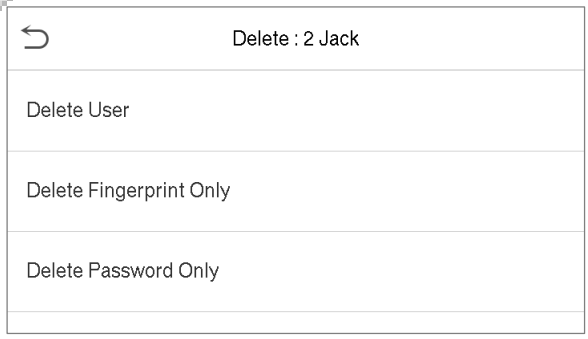
Delete Operations

Delete User: Deletes all the user information (deletes the selected User as a whole) from the Device.

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

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

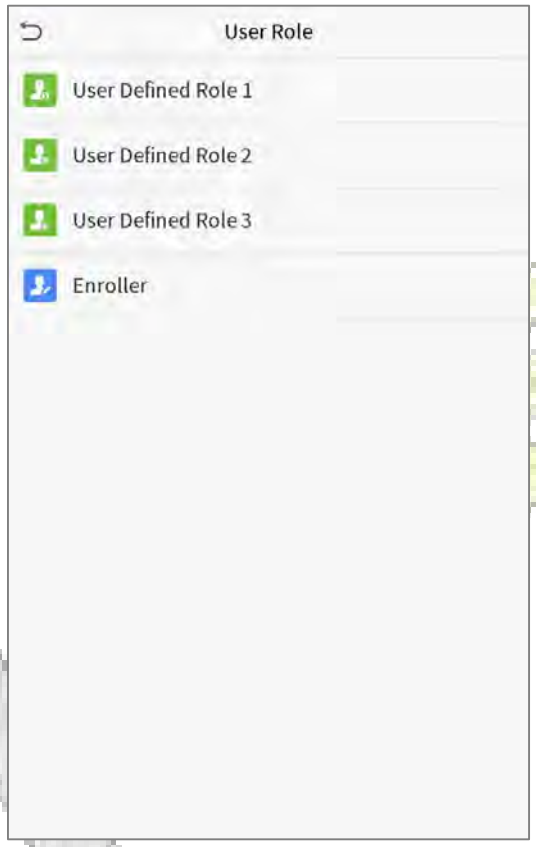
Delete Face Only: Deletes the Face information of the selected user.



6 User Role

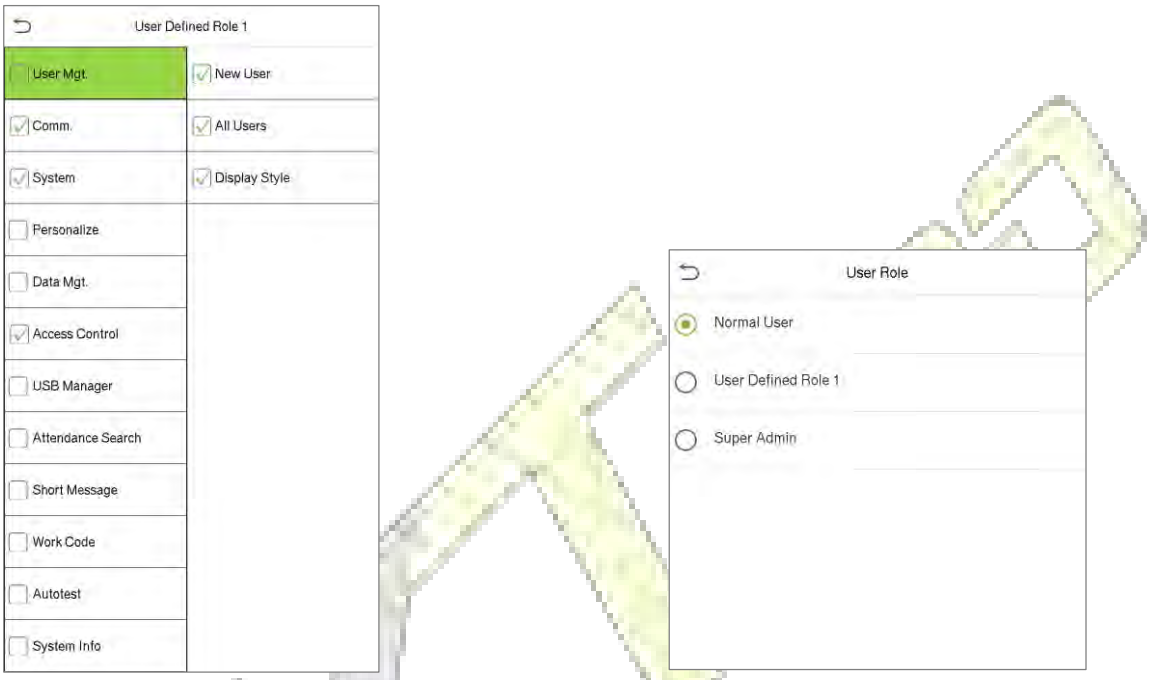
User Role facilitates to assign some specific permissions to certain users, based on the requirement.

- 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.

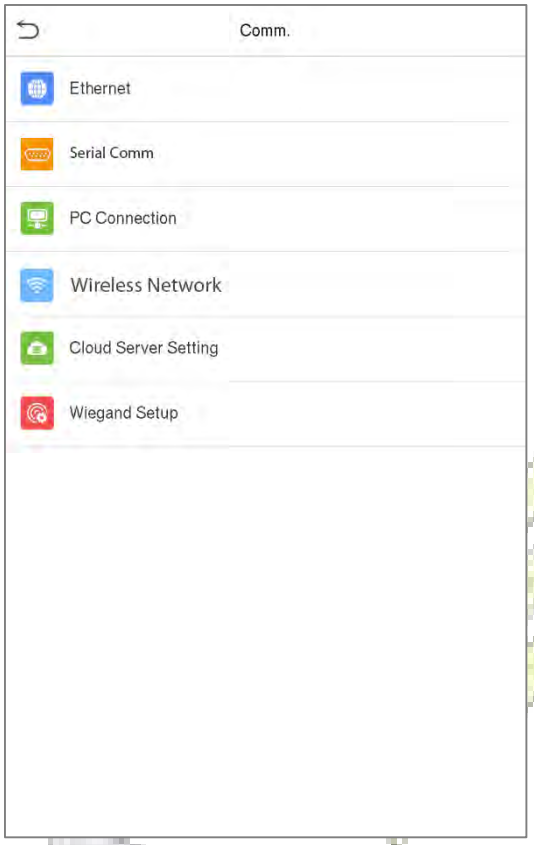
- Then, tap on **Define User Role** and select the required privileges to assign to the new role, and then tap on the **Return** button.
- During privilege assignment, the main menu function names will be displayed on the left and its sub-menus will be listed on its right.
- First tap on the required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



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

Tap **COMM.** on the **Main Menu** to set the Ethernet PC connection, Cloud Server setting and Wiegand.



7.1 Network Settings

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

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

Function 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 is to dynamically allocate 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 facilitates to establish communication with the device through a serial port (/RS485/ Master Unit).

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

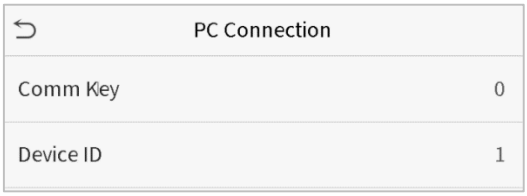
Function Description

Function Name	Descriptions
Serial Port	**Disable:** 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 fingerprint & card reader.
Baud Rate	The rate at which the data is communicated with PC, there are 4 options of baud rate: 115200 (default), 57600, 38400, and 19200. 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.

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, its connection password must be provided before the device gets connected 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, which can be changed. The Comm Key can contain1-6 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.

7.4 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 WiFi settings.

Search the WIFI 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 WIFI within the network range.
- Tap on the appropriate 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 then tap on **Connect to WIFI (OK).**

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

Add WIFI Network Manually

The WIFI can also be added manually if the required WIFI is not displayed 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

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	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.

7.5 Cloud Server Setting

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