USER MANUAL

Applicable Model: G3 Pro

Version: 1.0
Date: February 2020

Green Label

Copyright © ZKTeco 2020 All rights reserved.

Trademark

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.

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 numerous 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.

Since 1998, 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 of the industrialization of biometric verifications.

About this Manual

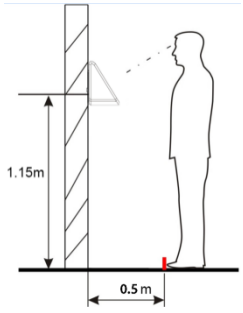
- This manual introduces the operations, interfaces and functions of G3 Pro. For installation, please refer to the ***Quick Start Guide*** of the product accordingly.
- Features and parameters with ★ are not available in all devices.
- All photos shown are for illustration purpose only. Photos in this manual may not be exactly consistent with the actual products.

Contents

1 Guidance Notes

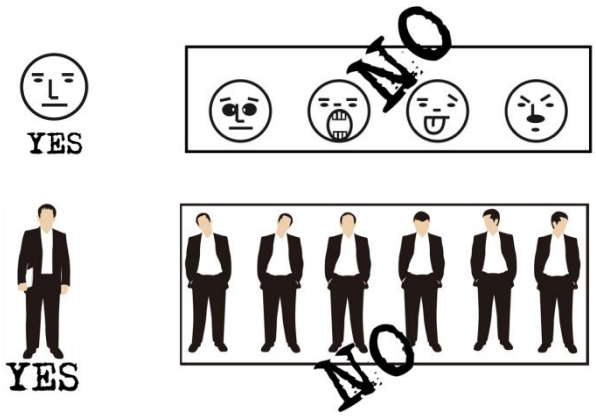
1.1 Standing Position, Facial Expression and Stance

- **Recommended Standing Position**



✓ The distance between a person and the device is recommended to be 0.5 meters (applicable height range from 1.5–1.8 meters). The distance can be adjusted based on the effect of facial image captured by the device.

- **Facial Expression and Stance**



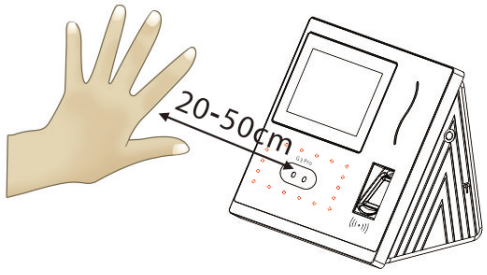
Note: During enrollment and verification, keep the facial expression and stance natural.

1.2 Posture for Enrollment and Comparison

During enrollment, you need to move forward or backward to ensure that the face is displayed in the center of the screen. Stay still until the registration succeeds.

1.3 Method for Enrolling Plam

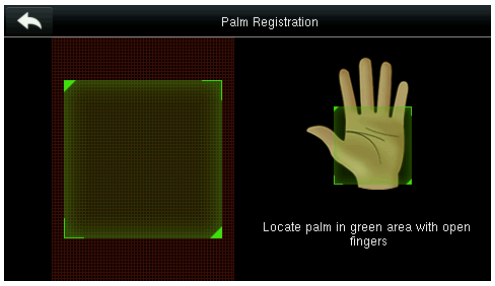
- **How to correctly enroll the palm**



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.

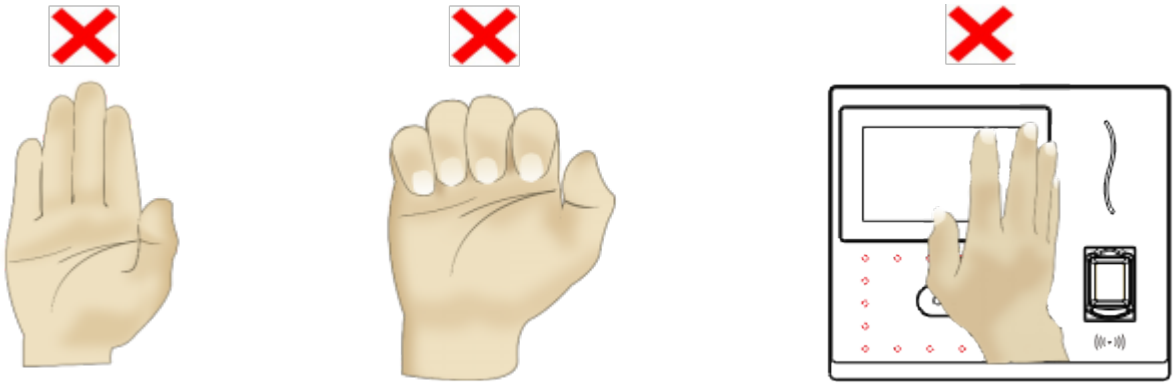
During enrollment locate your palm at the center of the screen, and follow the voice prompts "Focus the center of the palm inside the green box". The user needs to move forward and backward to adjust the palm position during the palm registration.

- **Verification**



Place your palm in the green area parallel to the device with space between the fingers.

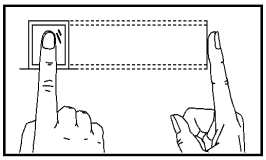
- **Incorrect palm gestures**



1.4 Method for Enrolling Fingerprint

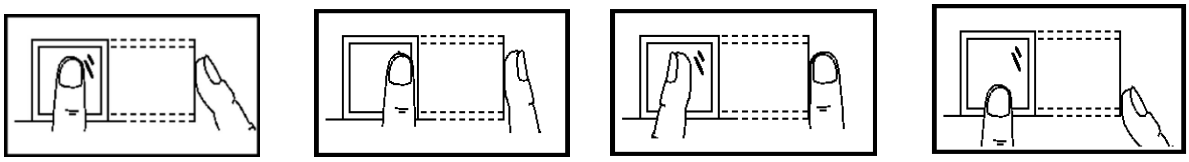
It is recommended to use the **index finger**, **middle finger** or **ring finger to enroll fingerprint**; avoid using the thumb or little finger

1. Correct way to press the fingerprint:



Place the finger horizontally onto the fingerprint sensor; the center of the fingerprint should be placed on that of the sensor.

2. Wrong ways to press the fingerprint:



Vertical Sides Slanted Too Low

Note: Please use the correct method of pressing fingerprint for registration and verification. Our company does not undertake the responsibility for the lowered verification performance caused by user's improper operation. The rights to final interpretation and amendment are reserved.

1.5 Usage of the Touch Screen

You may tap the touch screen, or tap and slide it using a finger pulp. Taping the screen with a fingertip or fingernail may compromise the use effect.

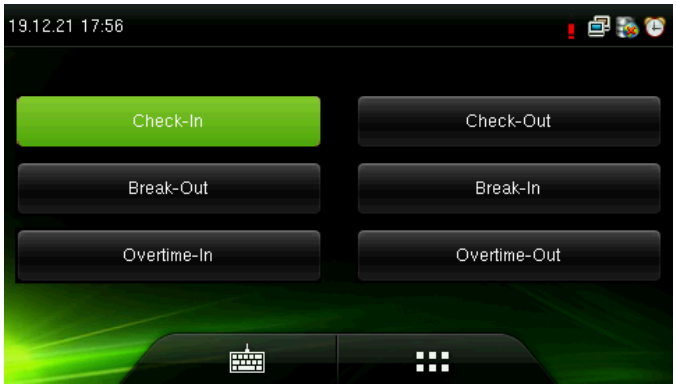
Smear or dust on the touch screen may affect the performance of the touch screen. Therefore, try to keep the screen clean and dust-free.

1.6 Initial Interface

When the device is turned ON, please press the power switch on the left side of the device and wait for a minute. Initial interface as shown below will be displayed.

Note:

- Attendance Status include Check-In, Check-Out, Break-In, Break-Out, Overtime-In, and Overtime-Out.
- You can change the Attendance Status by taping the initial screen where there is no icon.



You can press a corresponding shortcut key to select current attendance status, which is displayed in green. For details, refer to 8.5 Shortcut Key Settings.

- ✧ Tap to enter the main menu interface, please verify the admin when it is registered.
- ✧ Tap to enter the interface of 1:1 verify mode and enter the user ID. For details, refer section 1.9 Verification Mode.

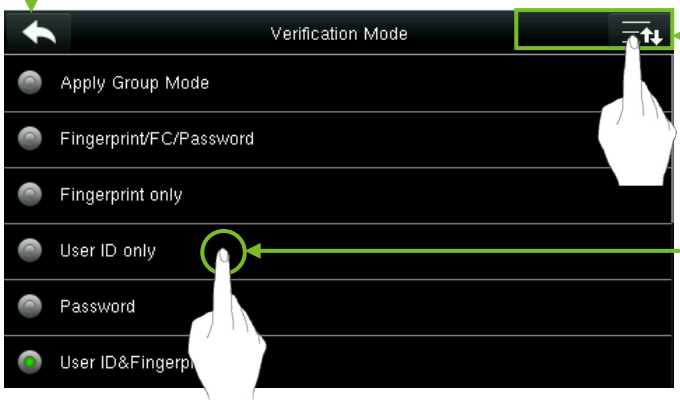
1.7 Status of Icons

Status Icon	Name	Description
	Cell signal	The status icons indicate whether you are within the coverage of the cellular mobile network, with more green bars indicating stronger signal. **G:** indicates that the current mobile network is GPRS network, over which the device accesses the Internet. **E:** indicates that the operator's EDGE (GSM) network is available, over which the device accesses the Internet. **W:** indicates that the current mobile network is WCDMA network, over which the device accesses the Internet. **H:** indicates that the current mobile network is HSDPA network, over which the device accesses the Internet. **T:** indicates that the current mobile network is TD-SCDMA network, over which the device accesses the Internet. **1X:** indicates that the current mobile network is CDMA 1X network, over which the device accesses the Internet. **3G:** indicates that the operator's 3G UMTS (GSM) or EV-DO (CDMA) network is available.
		Indicates that no mobile network is available.
	Bell	Indicates that you have set the bell.
		Indicates that a disassembly alarm.
	Ethernet	Indicates that the connection to Ethernet has been established.
		Indicates that the Ethernet is disconnected.
	ADMS Server	The connection between device and ADMS server is successful.
		The connection between device and ADMS server is failed.
		The communication data of ADMS are transmitting.

	Short Messages	There are public short messages.
	Wi-Fi signal	The Wi-Fi connection is normal.

1.8 Touch Operations

1.8.1 Basic Operations



Return and Save

Page Up and Page Down

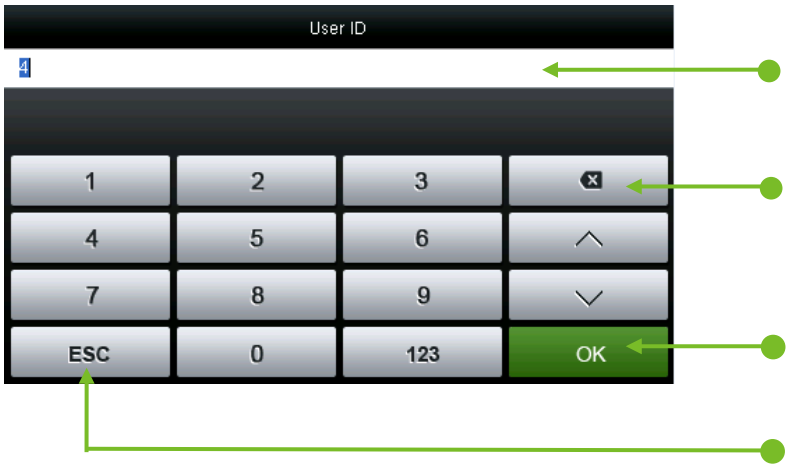
Note: If the list does not have much content and the menu can be completely displayed when you press **Page Down** just once, only the **Page Down** key is displayed here.

You can select an option by only taping the line where this menu option is, and the system automatically returns to the previous interface.

Note: After registering or modifying user information or setting parameters, you need to tap **Return/Save** to make the settings take effect. If timeout or no operations are performed on the interface, the system returns to the main interface without saving registration, user information modification or parameter settings.

1.8.2 Soft Keypad

- **Digital Keypad**



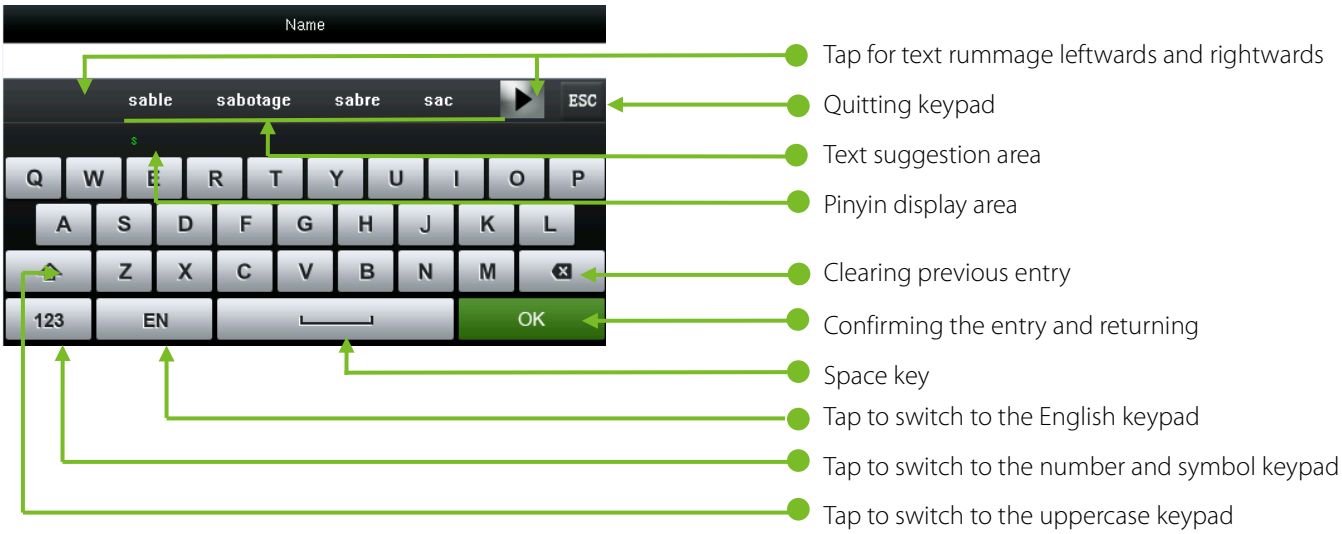
Content display area

Clearing previous entry

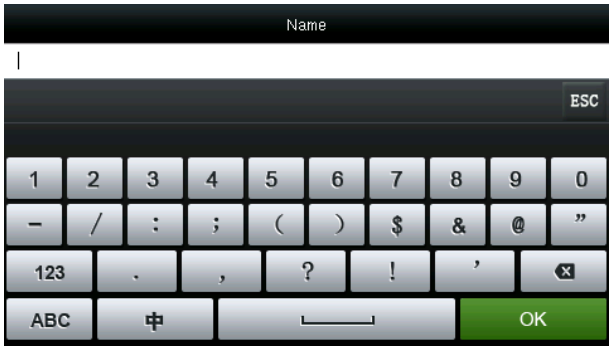
Confirming the entry

Return key

- **Letter Keypad**



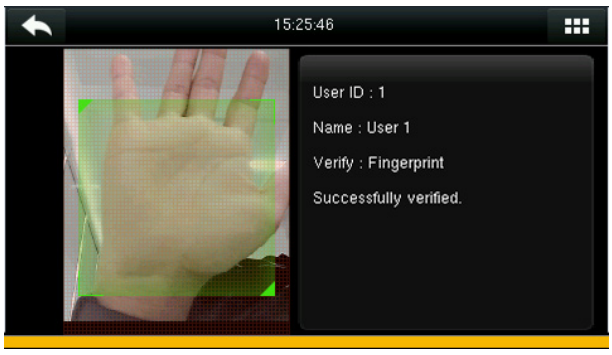
- **Digital and Letter Keypad**



1.9 Verification Mode

1.9.1 Palm Verification

The device compares the current palm with users' palm in the device. Use the proper way to enroll and verify.

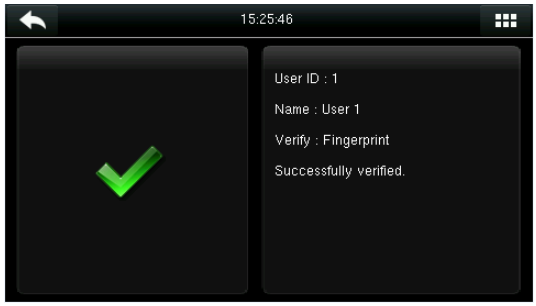


1.9.2 Fingerprint Verification

- **1:N Fingerprint Verification**

  In 1:N fingerprint verification method, a fingerprint collected by the sensor is verified with all the fingerprints stored in the device.

- To enter the fingerprint verification mode: The device automatically distinguishes face and fingerprint verification. Just pressfinger on the fingerprint collector/sensor, the device enters fingerprint authentication mode.
- Please use the correct way to press fingerprint onto the fingerprint sensor (for detailed instruction, please refer to 1.4 Method of Enrolling Fingerprint.



Verification Succeeds

Verification Fails

- **1:1 Fingerprint Verification**

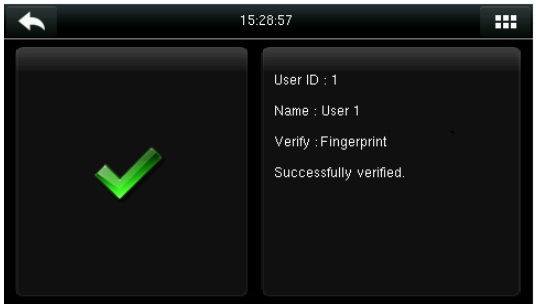
In 1:1 fingerprint verification method, a fingerprint collected by the sensor is verified with the fingerprint corresponding to the entered user ID.

Note: Adopt this mode only when it is difficult to recognize the finger.

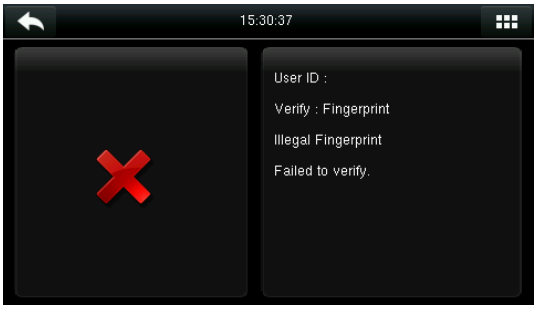
- Press  on the screen to enter 1:1 Verify Mode.

1.Enter your ID and tap [**OK**].

2.Press your fingerprint for verification.

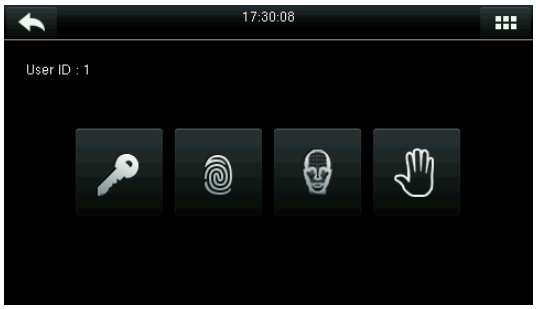


3.Verification succeeds.



4.Verification fails.

If you have registered multiple verification modes, the following interface appears after you enter your ID and tap [**OK**].



Tap the Fingerprint icon to access the fingerprint verification interface.

Press your finger onto the fingerprint scanner to scan your fingerprint for verification. The result is displayed as above.

Note: If you have registered only your fingerprint, you will access the fingerprint verification interface directly after entering your ID. If you have registered in multiple verification modes, the icons of registered verification modes are displayed, as the above figure with Password, Fingerprint and Face displayed.

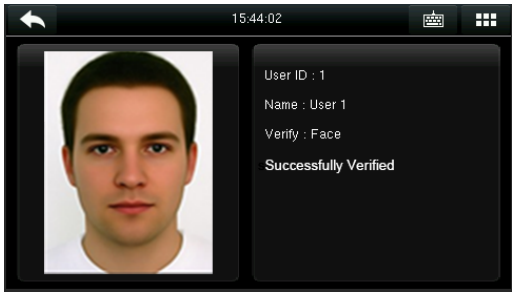
1.9.3 Facial Verification

- **1:N Facial Verification**

  Compare the facial image captured by the camera with all facial data in the device.

  - The device automatically differentiates between face and fingerprint verification modes. Show your face within the capture area of the camera (without your finger being placed at the fingerprint scanner), and the device automatically performs detection in face verification mode.

Conduct comparison in the correct way on the main interface.



Verification passed.

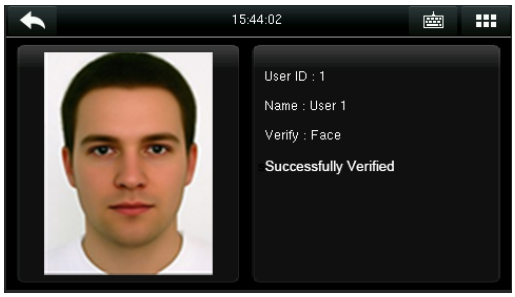
- **1:1 Facial Verification**

Compare the captured facial image with the facial image associated with the entered user ID.

Note: If the device prompts "No data registered" after the user enters the ID and press [**OK**], then the user corresponding to this ID does not exist.

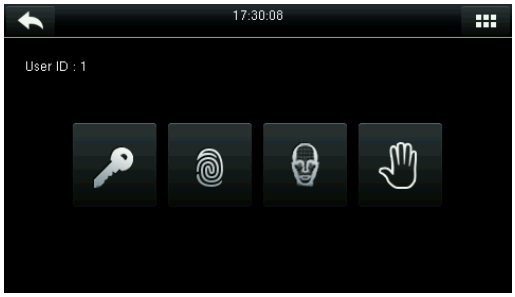
1.Enter the user ID into the main interface by using the keypad and then press [**OK**].

2.Compare the faces in the right way.



3.Verification passed. If the verification fails for 20 consecutive seconds, the system returns to the main interface.

If you have registered multiple verification modes, the following interface appears after you enter your ID and tap [**OK**].



Tap the **Face** icon to access face verification.

The verification result is displayed as above.

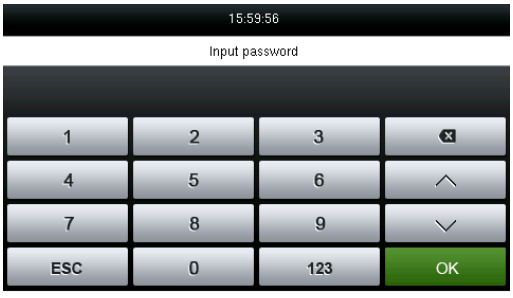
Note: If you have registered only your face, you will access the face verification interface directly after entering your ID. If you have registered in multiple verification modes, the icons of registered verification modes are displayed, as shown in the above figure with Password, Fingerprint and Face displayed.

1.9.4 Password Verification

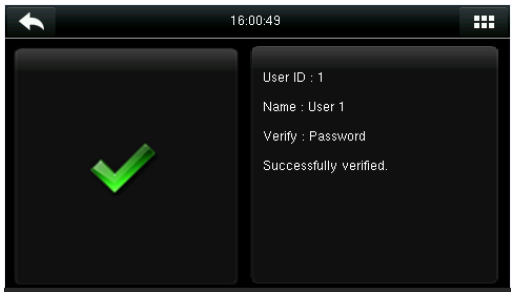
Under this verification method, the entered password is verified with the password of the entered user ID.

- Tap the [**1:1**] button on the main interface to enter 1:1 verification mode.

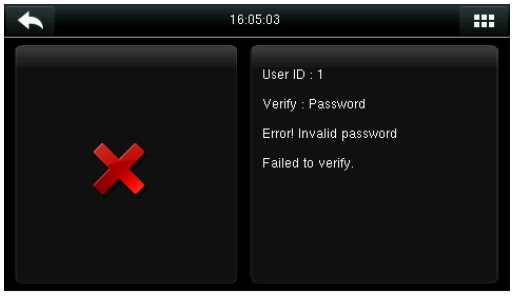
1.Input the user ID and press [**OK**].



2.Input the Password and press [**OK**].

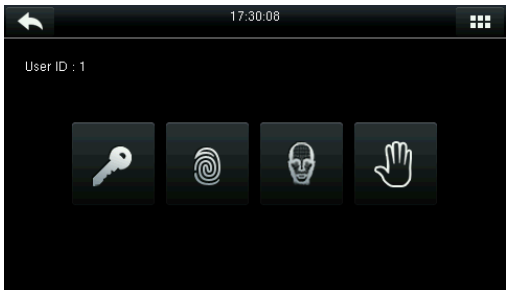


3.Verification succeeds.

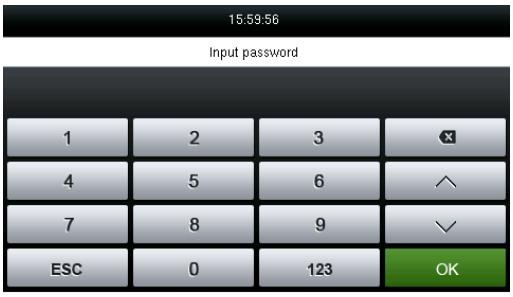


4.Verification fails.

If you have registered multiple verification modes, the following interface appears after you enter your ID and tap [**OK**].



Tap the Key icon to access password verification.



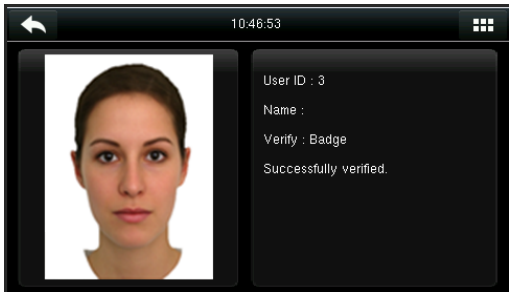
The verification result is displayed as above.

Note: If you have registered only the password, you will access the password verification interface directly after entering your ID. If you have registered in multiple verification modes, the icons of registered verification modes are displayed, just as the above figure showing that Password, Fingerprint and Face have been registered.

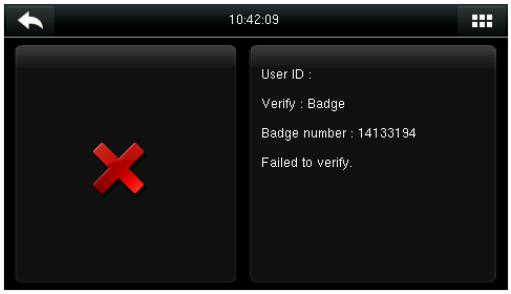
1.9.5 Card Verification★

Card function is optional, only products with a built-in card module are equipped with card verification function.

- Swipe the card above the card reader (the card must be registered first).



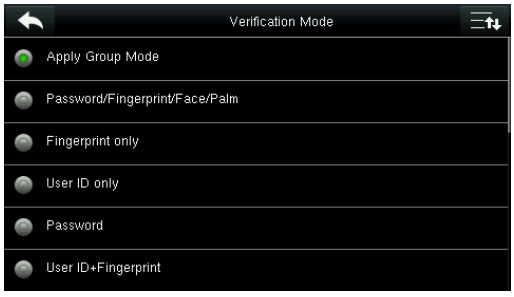
Verification succeeds.

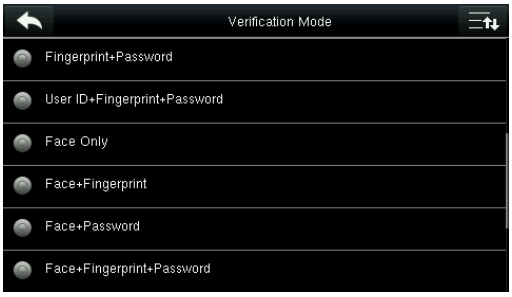


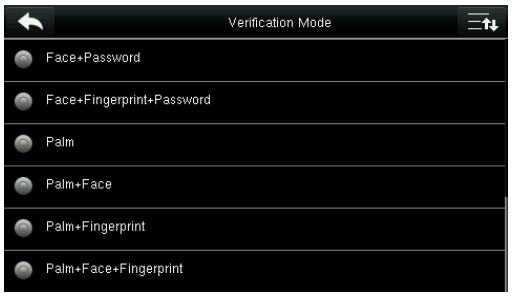
If the card is not registered, "Failed to verify" is prompted.

1.9.6 Combined Verification

In order to meet the needs of some access control occasions with high security and in consideration of the diversity of access control, the device provides a wide range of verification modes, which can be combined as required for individual users and user groups. The device supports 15 combinations of verification modes, as shown in the following figure.







Note:

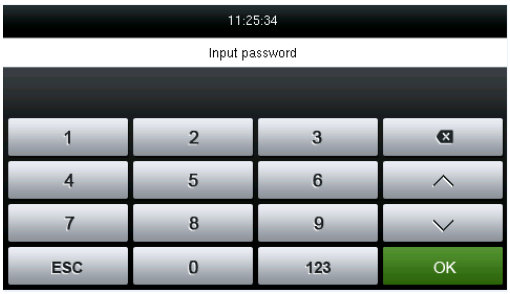
"**/**" means Or, and "**&**" means And.

In combined verification mode, you must register required verification information, otherwise the verification may fail. For example, if user A uses **Fingerprint Registration** but the verification mode is **PW**, this user will never pass verification.

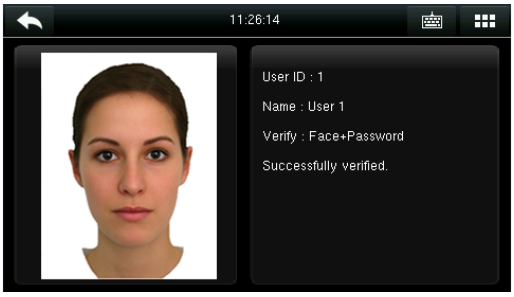
The following takes **Face&Password** as an example to introduce the combination verification mode.

Place your face within the capture area of the camera, and the device automatically performs detection in face verification mode.

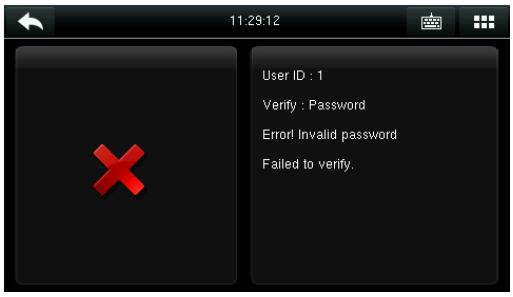
1. Face verification proceeds.



2. The password entry interface pops-up after verification passes. Enter the password and tap [**OK**]



3. Face & password verification succeeds.

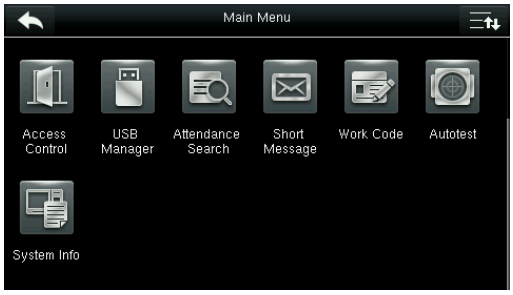


4. Face & password verification fails.

Note: The combination verification option is available only if corresponding verification modes are selected during user registration. For details, refer section 3.10 Setting the Access Control Rights.

2 Main Menu

When the device is in standby mode, press to open the main menu.



Menu Item	Description
User Mgt.	To manage basic information of registered users, including User ID, user role, Palm, Fingerprint, Face, badge★ (HID and MiFare card are optional), Password and Access Control Role.
User Role	To set user roles for accessing into the menu and changing settings.
Comm.	To set the related parameters of the communication between the device and PC, including Ethernet parameters such as IP address etc., Serial Comm, PC connection, Wi-Fi★, Cloud Server and Wiegand settings.
System	To set related parameters of the system and upgrade firmware, including setting Date time, Attendance, Face, Fingerprint and Palm Parameters, Reset to factory settings.
Personalize	This includes User Interface, Voice, Bell, Punch State Options and Shortcut key Mappings settings.
Data Mgt.	To delete all data including attendance data, admin role, screen savers, etc.
Access Control	To set the parameters of the lock. This includes setting the parameters of the lock.
USB Manager	To transfer data such as user data and attendance logs from the USB disk to the supporting software or other devices.
Attendance Search	To search for the records stored in the device after successful verification.
Print ★	To set printing information and functions (if printer is connected to the device).
Short Message	To set public or private short messages, which are read by specified objects within the specified time after attendance, facilitating information transmission.
Work Code	To mark different work categories, facilitating user attendance check.
Auto test	To automatically test different module's functions, including the LCD, Voice, Keyboard, Fingerprint Sensor, Face and Clock RTC test.
System Info	To check device capacity, device and firmware information.

Note: After registering or modifying user information or setting parameters, you need to tap **Return/Save** to make the settings take effect. If timeout or no operations are performed on the interface, the system returns to the main interface without saving registration, user information modification or parameter settings.

If no super administrator is available on the device, anyone can access the menu for operations by pressing  . After an administrator is set on the device, identity authentication needs to be conducted by the administrator for menu access. A user can access the menu only after successful identity authentication. For device security purposes, it is recommended to register an administrator when the device is used for the first time. For specific operations, refer section 3.3 Setting a User Role.

3 Adding a User

Tap **New User** on the main menu interface.

Tap **New User**.

Tap **Page Down** to view other options.

3.1 Entering a User ID

The device automatically assigns user IDs for personnel, starting from 1 and so on. The user ID can also be entered manually.

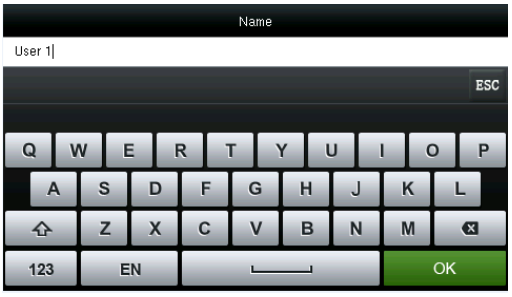
Select **User ID,**then press **OK** for confirmation.

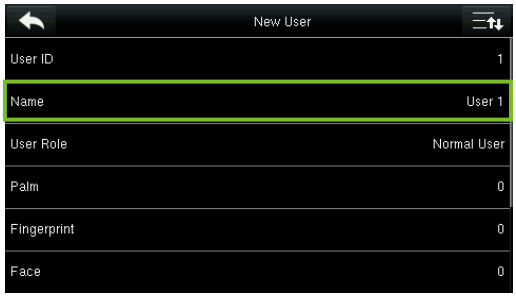
Note:

1. By default, a user ID contains 1-9 digits. To extend the length, consult our pre-sales technical support personnel.
2. During the initial registration, you can modify your ID, which cannot be modified after registration.
3. If "ID Already Exists" is prompted, this ID has been used. Please try different ID.

3.2 Entering a User Name

1. Select **User Role**





2. Enter your name and tap **OK** to save and return. The name entry is completed.

Note: By default, a user name contains 1-12 characters. For details, refer section 1.8.2 Soft Keypad.

3.3 Setting a User Role

There are two types of Roles respectively granted to two types of users: the User and Administrator.

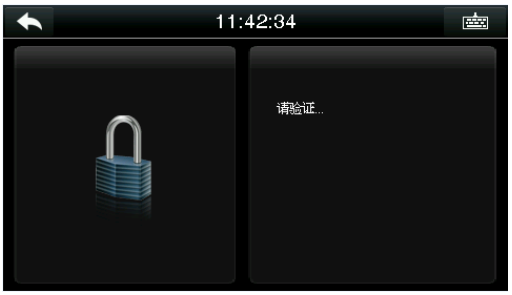
User: are only granted the rights of facial, fingerprint, or password verification.

Administrator: are granted the access to the main menu for various operations apart from having all the privileges granted to User.

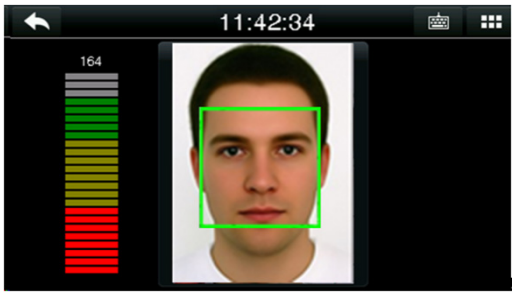
Tap **User Role**.

Select a user role. The user role selection is completed.

If the selected user role is **Super Admin**, identity authentication needs to be conducted for main menu access. The authentication process depends on the authentication mode that the super administrator has registered. The following is an example of accessing the main menu as the super administrator by face authentication.



Press  on the main interface.

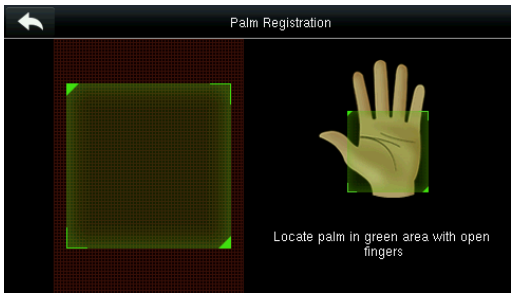


Place your face in front of the camera for authentication.

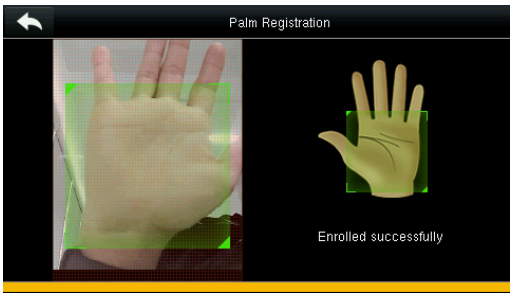
You can access the main menu interface directly after passing authentication.

3.4 Registering a Palm

Select a palm.



1. Follow the voice and interface prompts to move back and forth to place your Palm within the green frame.



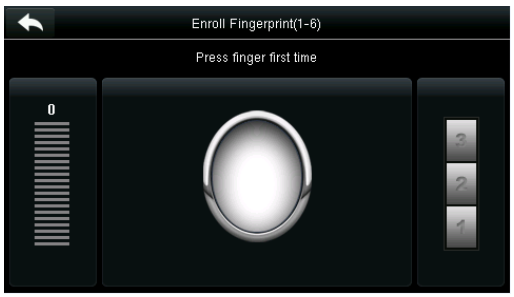
2. The Palm registration succeeds.

3. The system automatically returns to the **New User** interface.

If a duplicate Palm is registered, the system prompts: "Palm repeated".

3.5 Registering a Fingerprint

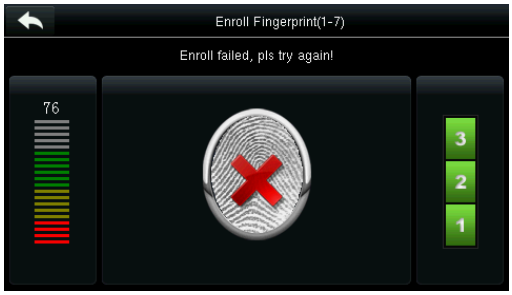
Select a finger



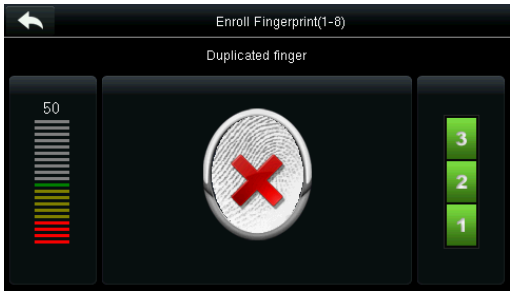
1. Tap to select a finger for fingerprint registration.
2. Press the same finger onto the fingerprint scanner for three consecutive times.

3. Fingerprint registration succeeds interface.

If the fingerprint registration fails, the following prompt appears.



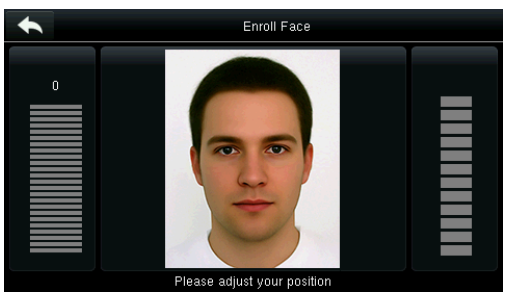
The fingerprint registration fails. You need to register the fingerprint again.



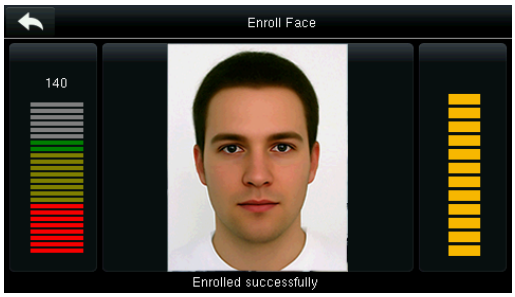
If the device prompts "Duplicated fingerprint", this fingerprint has already been registered.

Note: To register another fingerprint, return to the **New User** interface, tap **Fingerprint** again and repeat the above steps to select another finger for fingerprint **registration**.

3.6 Registering a Face

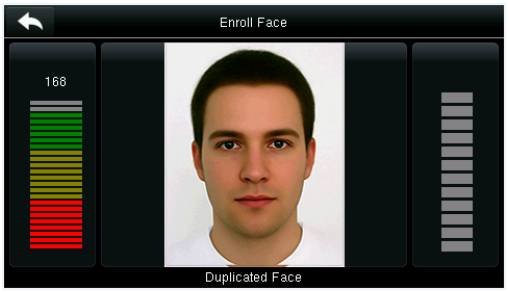


1. Follow the voice and interface prompts to move back and forth to place your eyes within the green frame.



2. The face registration succeeds.

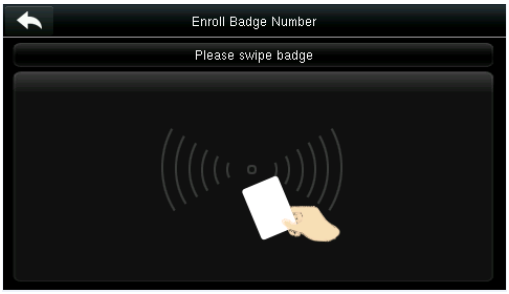
3. The system automatically returns to the **New User** interface.



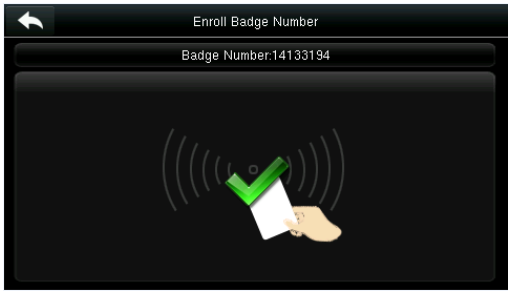
If a duplicate face is registered, the system prompts: "Duplicated Face".

3.7 Registering a Badge Number★

Tap **Badge Number**.

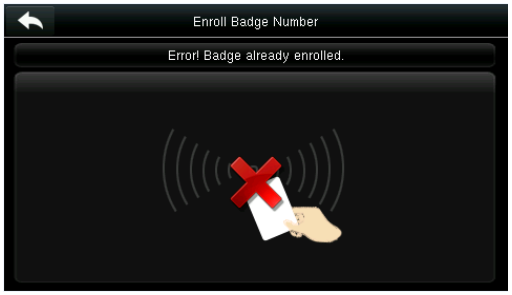


1. Press your badge close underneath the fingerprint collector.



2. The badge number registration succeeds.

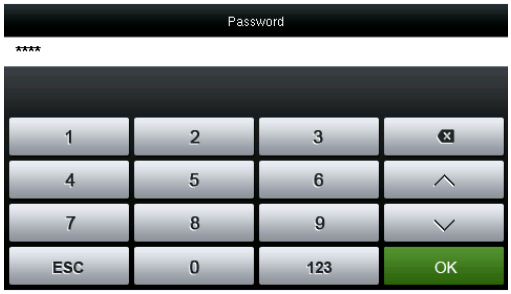
3. The system automatically returns to the New User interface.



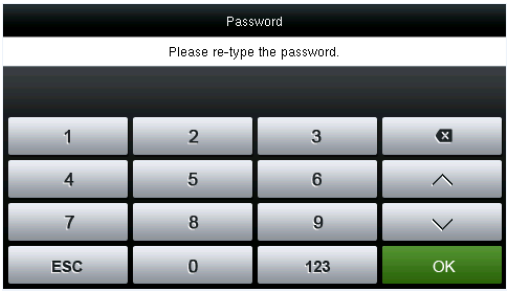
Note: If the badge has already been registered, "Error! Badge already enrolled" is prompted.

3.8 Registering a Password

Tap **Password**.

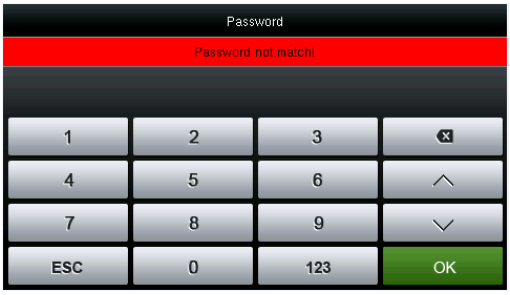


1. Enter your password and tap **OK**.



2. Enter the password again and tap **OK**.

3. The password registration succeeds and the system returns to the **New User** interface.



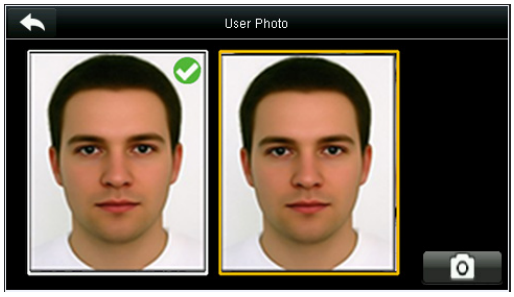
4. If the two entered passwords are different, "Password not match" is prompted.

Note: By default, a password contains 1-8 digits.

3.9 Registering a Photo

When a user registered with a photo passes the authentication, the registered user photo is displayed.

Tap **User Photo**.



Tap the camera icon to capture a photo.

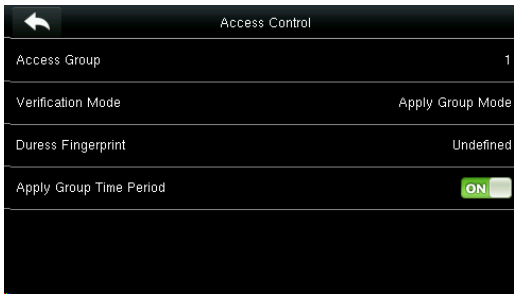
The photo taking is completed, and the system returns to the **New User** interface.

Note: After face registration is completed, the system automatically captures a photo. If you do not want to register a user photo, the photo automatically taken by the system is used by default.

3.10 Setting the Access Control Rights

You can set which group a user belongs to, access verification mode, whether to register a duress fingerprint, and whether to use the group time period. By default, the unlocking permission is granted to newly enrolled users.

Tap **Access Control Role**.

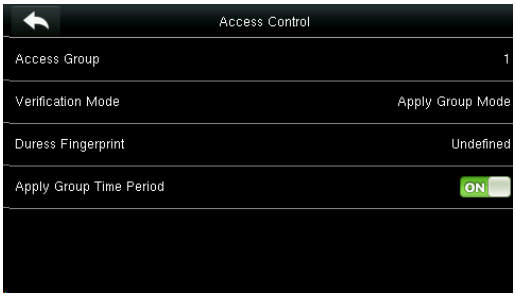


3.10.1 Access Group

Access Group: Select the belonged group. By default, a newly enrolled user belong to group one.

Tap **Access Group**.

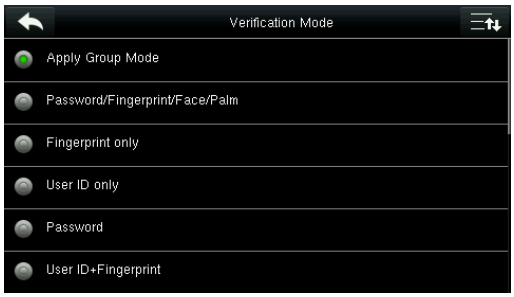
Enter the belonged group and tap **OK**.



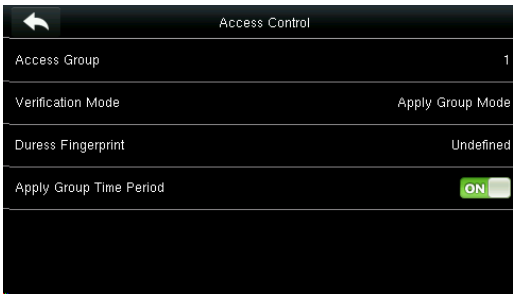
The system returns to the **Access Control** interface.

3.10.2 Verification Mode

Tap **Verification Mode**.



Select a verification mode.



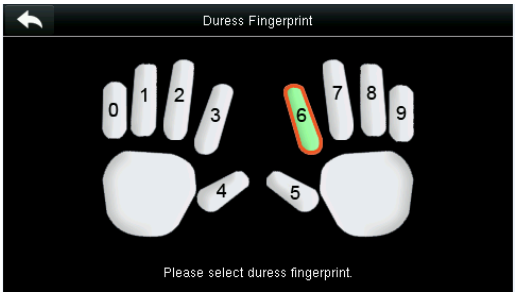
The system automatically returns to the **Access Control** interface.

Note: A user can select **Apply Group Mode**, that is, the user can be verified by using the verification mode of the group to which this user belongs, or by using an individual verification mode. For details on group settings, refer section 10.4 Access Group Settings.

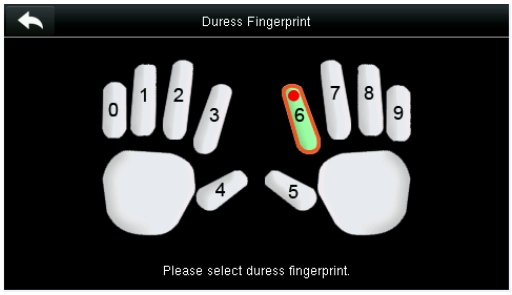
3.10.3 Duress Fingerprint

A fingerprint registered in the device is specially specified as a duress fingerprint. In any case, a duress alarm is generated when a fingerprint matches a duress fingerprint. After a duress fingerprint is cancelled, the fingerprint is not deleted and the corresponding finger can still be used for normal comparison.

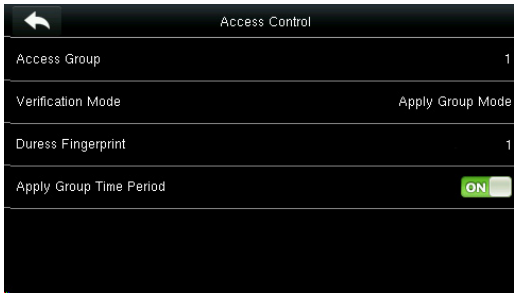
Tap **Duress Fingerprint**.



1. Select a duress fingerprint.



2. The selection succeeds. Tap the **Return** button.



3. The system returns to the Access Control interface.

Note:

1. The selected duress fingerprint must be a registered fingerprint.
2. If you do not want to use a duress fingerprint, access the same menu during user editing and cancel the duress fingerprint.

3.10.4 Apply Group Time Period

Choose whether to apply the group time period for this user, yes by default. If the group time period is not applied, you need to set the unlocking time for this user. At this time, the time period of this user does not affect the time period of any other member in this group.

When you set the unlocking time for this user, tap **Apply Group Time Period**.

1. Tap **Time Period 1**.

2. Enter the time period number and tap **OK**.

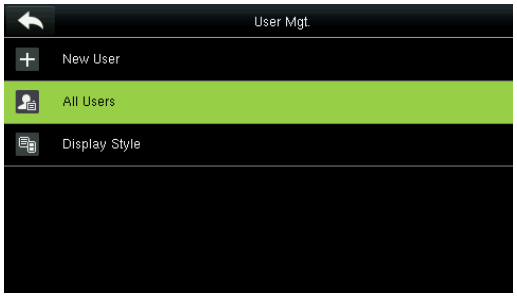
3. Select time period 2 and 3 in the same way, and enter the time period numbers.

Note: A total of 50 time periods can be set in the device and three time periods can be set for each user. For details, see 10.2 Time Schedule Settings

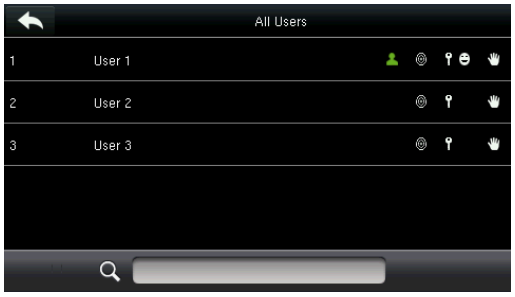
Note: After the above data is registered, tap  to return to the **New User** interface. To modify the registered data, tap the corresponding menu for re-registration. To save the registered data, tap  . If the menu is left unattended within the timeout period, the system returns to the main interface, and the registered information is not saved.

4 User Management

Press **User Mgt.** on the main menu interface.



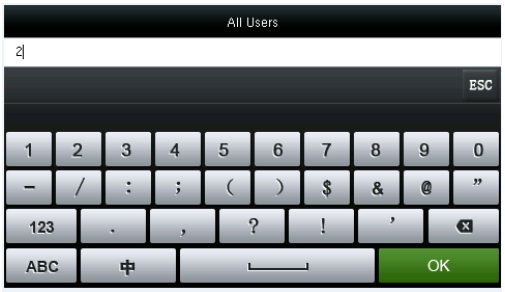
Tap **All Users**.



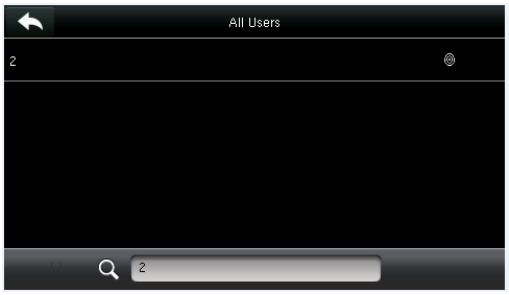
The **All Users** interface is displayed.

Note: The users are sorted by name, with  indicating the super administrator.

4.1 Searching for a User



Tap the search bar on user list and enter the retrieval keyword.



The system automatically finds the users related to entered keyword.

Note: The retrieval keyword can be ID, surname, given name or full name.

4.2 Editing a User

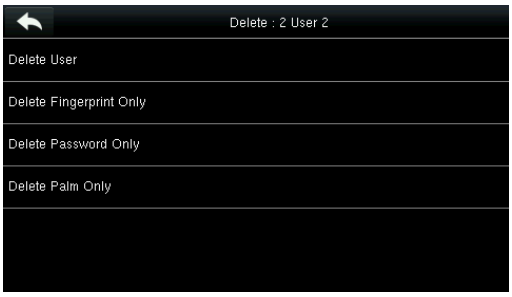
Choose a user from the list and tap **Edit**.

The **Edit User** interface is displayed.

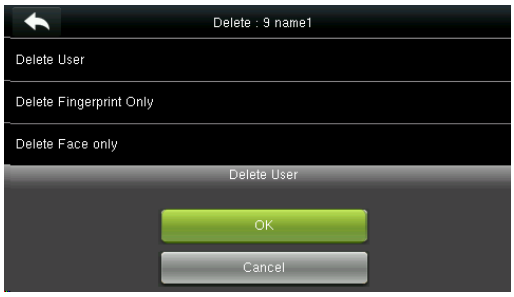
Note: The operation of editing a user is the same as that of adding a user except that the user ID cannot be modified in editing a user.

4.3 Deleting a User

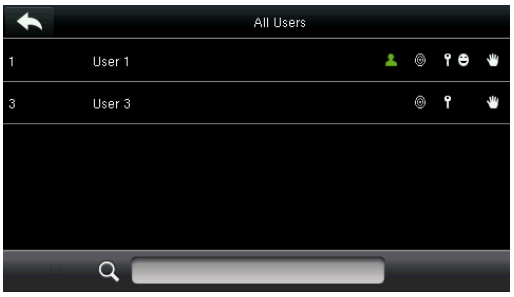
Choose a user from the list and tap **Delete**.



The delete user interface is displayed. (press down to view other information.)



Select the user information to be deleted and tap **OK**.

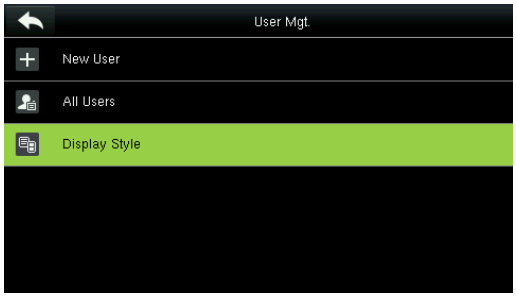


The user is deleted successfully and no longer displayed in the list.

Note:

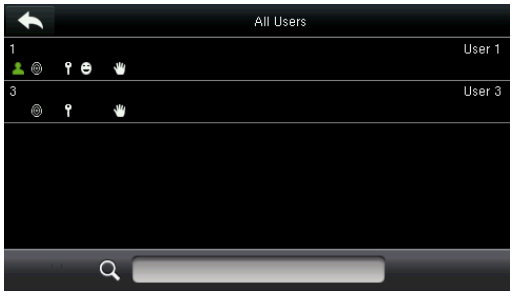
1. When deleting a user, you can choose to delete partial information such as the privilege or fingerprint of the user. If you select Delete User, all information of this user is deleted.
2. After the privileges of the super administrator is deleted, the super administrator becomes a common user, without super administrator privileges any more.

4.4 User Display Style

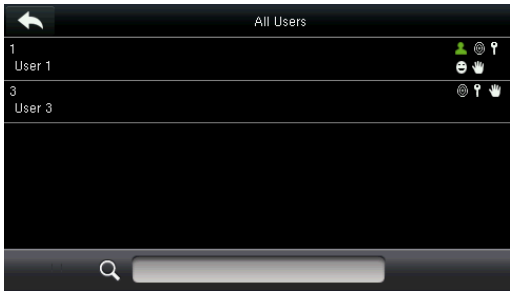


1. Tap **Display Style** on user MGt. interface.

2. The default style is single line.



3. The above figure shows all users in the **Multiple Line** style.

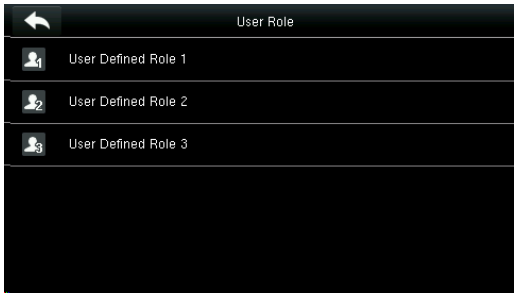


4. The above figure shows all users in the **Mixed Line** style.

5 User Role

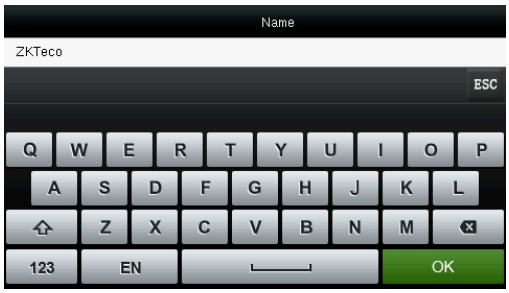
Setting user rights of operating the menu (a maximum of 3 roles can be set).

Tap **User Role** on the main menu interface.



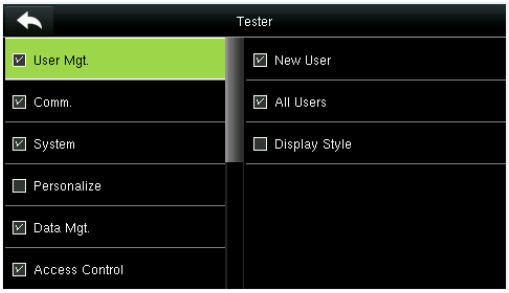
1. Tap any item to set a defined role.

2. Tap **Enable Defined Role** to enable this defined role.



3. Tap name to enter role name.

4. The system returns to the user defined role interface.



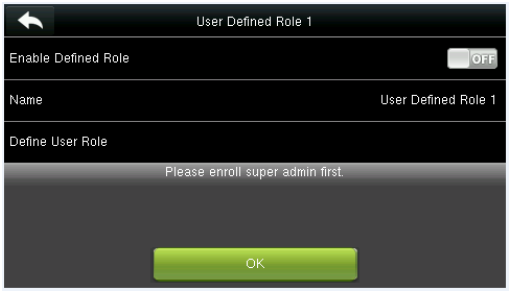
5. Tap **Define User** Role to assign privileges to the role.

6. The role definition is completed.

The privilege assignment is completed. Tap **Return**.

Note:

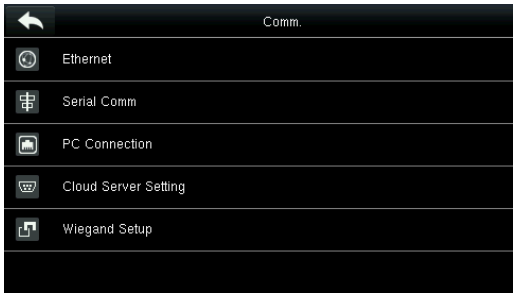
During privilege assignment, the main menu is on the left and its sub-menus on the right. You only need to select the features in sub-menus. If no super administrator is registered in the device, the following interface prompt appears after you tap **Enable Defined Role**.



6 Comm. Settings

Including Ethernet parameters such as IP address etc., serial Comm, PC connection, ADMS and Wiegand settings.

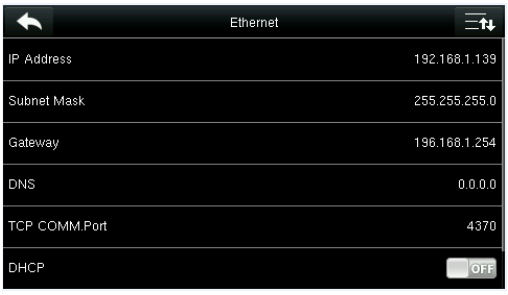
Tap [**Comm.**] on the main menu interface.

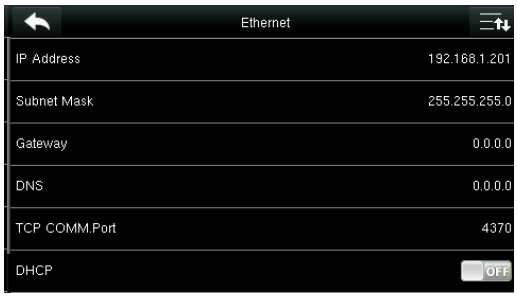


6.1 Ethernet Settings

When the device needs to communicate with a PC over the Ethernet, you need to configure network settings.

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





Menu Item	Description
IP Address	The factory default value is192.168.1.201, please adjust them according to the actual network situation.
Subnet Mask	The factory default value is 255.255.255.0, please adjust them according to the actual network situation.
Gateway	The factory default value is 0.0.0.0, please adjust them according to the actual network situation.
DNS	The factory default value is 0.0.0.0, please adjust them according to the actual network situation.
TCP COMM. Port	The factory default value is 4370, please adjust them according to the actual network situation.
DHCP	Dynamic Host Configuration Protocol, which is to dynamically allocate IP addresses for clients via server. **If DHCP is enabled, IP cannot be set manually.**
Display in Status Bar	To set whether to display the network icon on the status bar.

6.2 Serial Comm. Settings

To establish communication with the device through a serial port (RS232/RS485), you need to configure serial port settings.

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

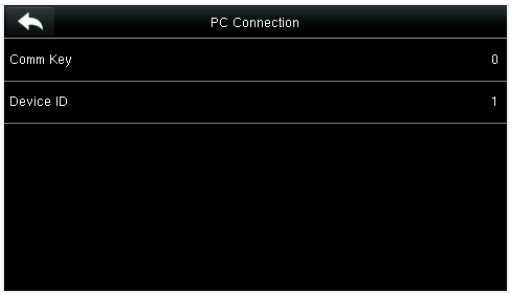
Menu Item	Description
Serial port	Including no using, RS232(PC) and RS485(PC), select RS232(PC) to communicate with the device through an RS232 serial port. Select RS485(PC) to communicate with the device through an RS485 serial port.
Baudrate	The rate of the communication with PC; there are 5 options of baud rate: 115200 (default), 57600, 38400, 19200 and 9600. The higher is the baud rate, the faster is the communication speed, but also the less reliable. In general, 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.

Note: If an RS485 serial port is used for communication with the device, the baud rate of the serial port should not be 9600 bps.

6.3 PC Connection

To improve security of data, a **Comm Key** to enable communication between the device and PC needs to be set.
If a **Comm Key** is set in the device, the correct connection password needs to be entered when the device is connected to the PC software, so that the device and software can communicate.

Tap **PC Connection** on the **Comm. Settings** interface.

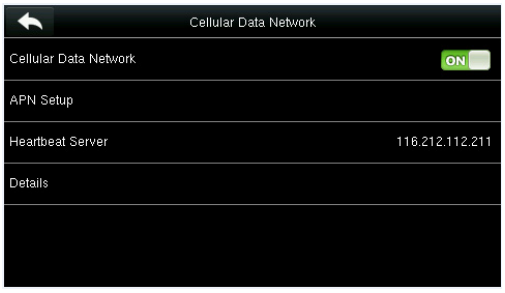


Menu Item	Description
Comm Key	**Comm Key:** The default password is 0 (no password). **Comm Key** can be 1~6 digits and ranges between 0~999999.
Device ID	Identity number of the device, which ranges between 1~254. If the communication method is RS232/RS485, inputting this device ID in the software communication interface is required.

6.4 Cellular Data Network★

When the device is applied on a dial-up network, ensure that the device is within the coverage of the mobile network signals (GPRS/3G). In addition, you must know the used APN and access number.

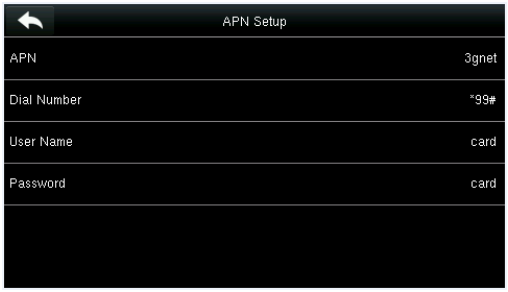
Tap **Cellular Data Network** on the **Comm. Settings** interface.



Menu Item	Description
Cellular Data Network	Whether to enable the mobile network.
APN Setup	To set APN information, such as the access number, user name and password.
Heartbeat server	To detect the connection status of the mobile network. The terminal periodically sends ICMP packets to the heartbeat server to detect whether the terminal is online. When the terminal is offline, the device automatically performs dial-up connection again. Therefore, when setting the heartbeat server, ensure that the heartbeat server can be pinged and remain online stably for a long term. **Note: Generally, the customer can set the heartbeat server address as the ADMS server address.**
Details	To view the information about mobile network connection, such as network mode, operator, IP address, received data, and sent data.

6.4.1 APN Setup

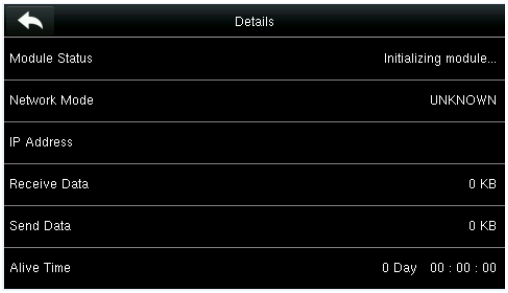
Tap **APN Setup** on the **Cellular Data Network** interface.



Menu Item	Description
APN	Access Point Name, provided by the operator and not supported in the CDMA network.
Dial Number	Number of the cellular data network.
User Name and Password	To verify whether the user has the privilege to use this network.

6.4.2 Details

Tap **Details** on the **Cellular Data Network** interface.



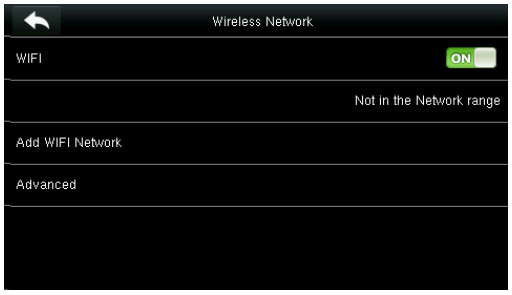
The information about device connection is displayed.

6.5 Wi-Fi Settings★

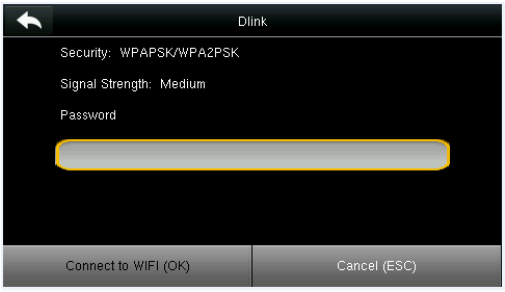
Wi-Fi is short for Wireless Fidelity. The device provides a Wi-Fi module, which can be built in the device mould or externally connected, to enable data transmission via Wi-Fi and establish a wireless network environment.

Wi-Fi is enabled in the system by default. If the Wi-Fi network does not need to be used, you can tap the 

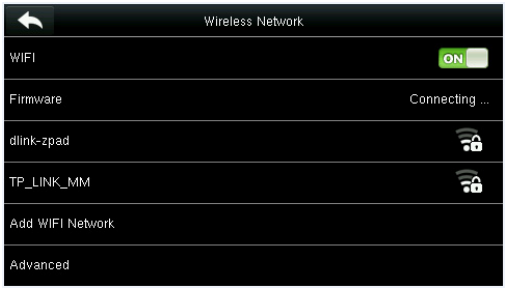
button to disable Wi-Fi.



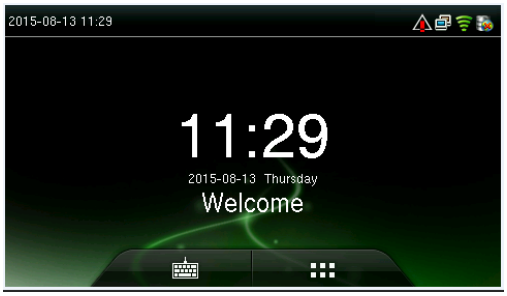
1. When Wi-Fi is enabled, tap the searched network.



2. Tap the password entry text box to enter the password, and tap Connect to **Wi-Fi (OK)**.



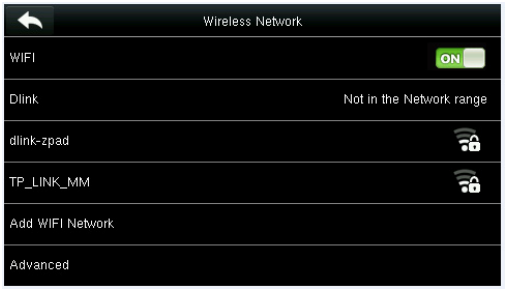
3. Connecting



4. The connection succeeds, with status displayed on the icon bar.

6.5.1 Adding Wi-Fi Network

If the desired Wi-Fi network is not in the list, you can add the Wi-Fi network manually.



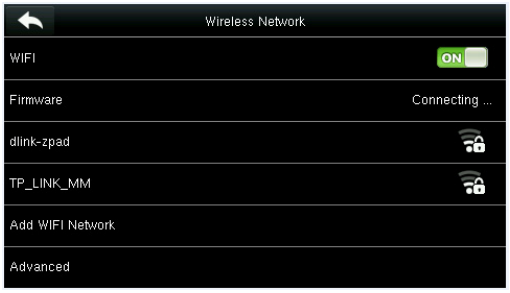
Tap **Page Down** and **Add Wi-Fi Network**.

Enter the parameters of Wi-Fi network. (The added network must exist.)

After adding, find the added Wi-Fi network in list and connect to the network in the above way.

6.5.2 Advanced Options

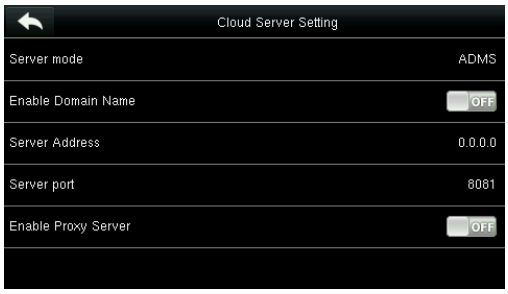
This is used to set Wi-Fi network parameters.



Menu Item	Description
DHCP	Short for Dynamic Host Configuration Protocol, which involves allocating dynamic IP addresses to network clients.
IP Address	IP address of the Wi-Fi network.
Subnet Mask	Subnet mask of the Wi-Fi network.
Gateway Address	Gateway address of the Wi-Fi network.

6.6 Cloud Server Settings

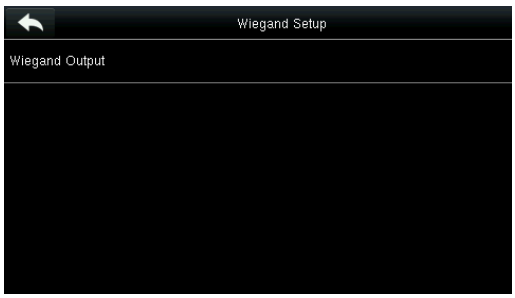
Settings used for connecting with Cloud server. Tap **PC Connection** on the **Comm. Settings** interface.



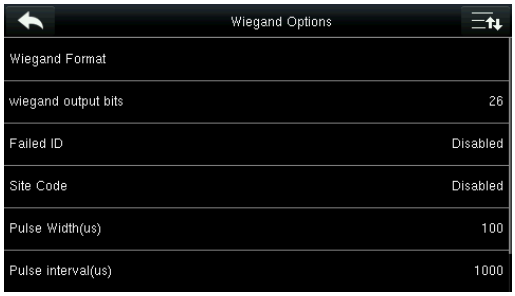
Menu Item	Description
Enable Domain Name	When this function is enabled, the domain name mode http://... will be used, such as http://www.XXX.com. XXX denotes the domain name when this mode is turned ON; when this mode is turned OFF, enter the IP address format in XXX.
Server Address	IP address of the ADMS server.
Server Port	Port used by the ADMS server.
Enable Proxy Server	Method of enabling proxy. To enable proxy, please set the IP address and port number of the proxy server.

6.7 Wiegand Setup

To set the Wiegand output parameters, tap **Wiegand Setup** on the **Comm. Settings** interface.



Tap **Wiegand Output** on the **Wiegand Setup** interface.



Menu Item	Description
Wiegand Format	Users can select the standard Wiegand formats built in the system. Although multiple choices are supported, the actual format is determined by **Wiegand output bits**.
Wiegand output bits	Number of bits of Wiegand data. After choosing **[Wiegand output bits]**, the device will use the set number of bits to find the suitable Wiegand format in **[Wiegand Format]**. For example, If Wiegand26, Wiegand34a, Wiegand36, Wiegand37a or Wiegand50 is selected in Wiegand Format but Wiegand output bits is set to 36, the Wiegand36 format takes effect.
Failed ID	It is defined as the output value of failed user verification. The output format depends on the **[Wiegand Format]** setting. The default value ranges from 0 to 65535.
Site Code	It is similar to device ID except that it can be set manually and repeatable with different devices. The default value ranges from 0 to 256.
Pulse Width (us)	The width of pulse sent by Wiegand. The default value is 100 microseconds, 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	Output content after successful verification. User ID or card number can be chosen.

Definitions of Various General Wiegand Formats:

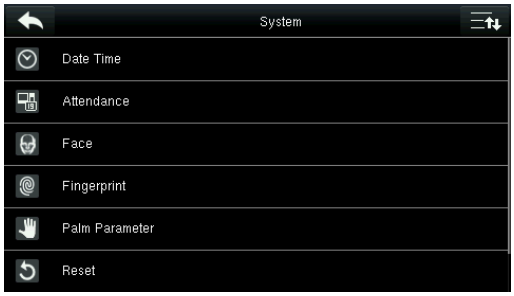
Wiegand Format	Definition
Wiegand26	ECCCCCCCCCCCCCCCCCCCCCCCCO Consists of 26 bits of binary code. The 1st bit is the even parity bit of the 2nd to 13th bits, while the 26th bit is the odd parity bit of the 14th to 25th bits. The 2nd to 25th bits are the card number.

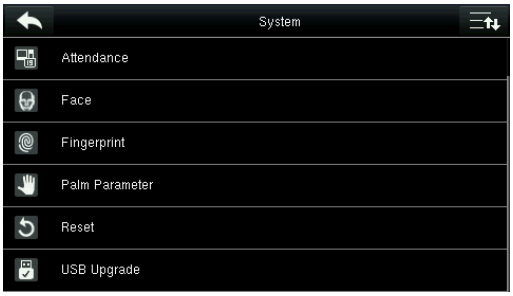
Wiegand26a	ESSSSSSSSCCCCCCCCCCCCCCCO Consists of 26 bits of binary code. The 1st bit is the even parity bit of the 2nd to 13th bits, while the 26th bit is the odd parity bit of the 14th to 25th bits. The 2nd to 9th bits are the site code, while the 10th to 25th bits are the card number.
Wiegand34	ECCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO 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 are the card number.
Wiegand34a	ESSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCO 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 are the site code, while the 10th to 25th bits are the card number.
Wiegand36	OFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCMME 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 are the device code, the 18th to 33rd bits are the card number, and the 34th to 35th bits are the manufacturer code.
Wiegand36a	EFFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCO 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 are the device code, and the 20th to 35th bits are the card number.
Wiegand37	OMMMMSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCE 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 are the manufacturer code, the 5th to 16th bits are the site code, and the 21st to 36th bits are the card number.
Wiegand37a	EMMMFFFFFFFFFSSSSSSCCCCCCCCCCCCCCCCO 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 35th bits. The 2nd to 4th bits are the manufacturer code, 5th to 14th bits are the device code, 15th to 20th bits are the site code, and the 21st to 36th bits are the card number.
Wiegand50	ESSSSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO 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 are the site code, and 18th to 49th bits are the card number.
C denotes card number, **E** denotes even parity bit, **O** denotes odd parity bit, **F** denotes device code, **M** denotes manufacturer code, **P** denotes parity bit, and **S** denotes site code.	

7 System Settings

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

Tap [**System**] on the main menu interface.

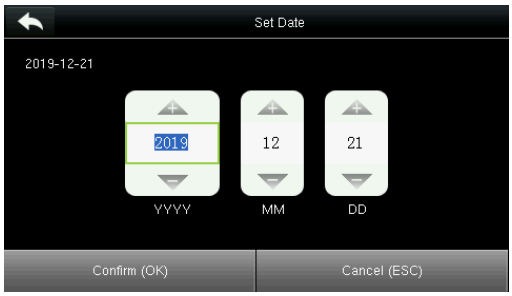




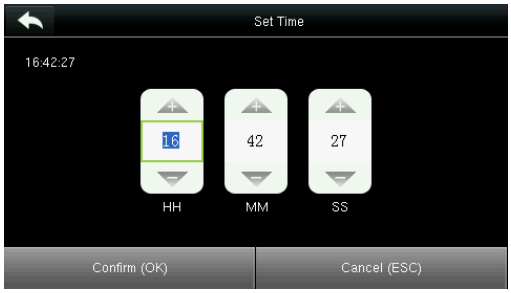
7.1 Date/Time Settings

Tap **Date Time** on the **System** interface.

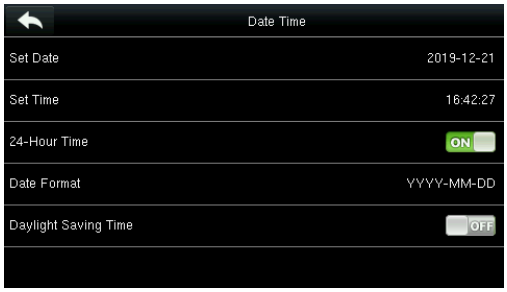
1. Tap **Set Date**.



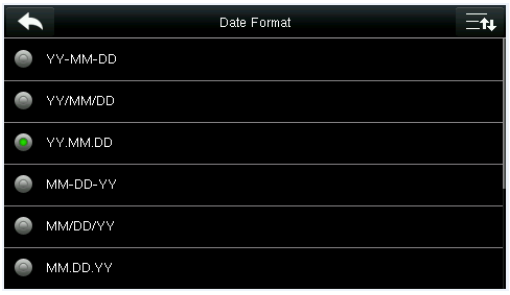
2. Press **Page Up** and **Page Down** to set the year, month and day, and then press **Confirm (OK)**.



3. Tap **Set Time** on the Date Time interface and press **Page Up** and **Page Down** to set the hour, minute and second.

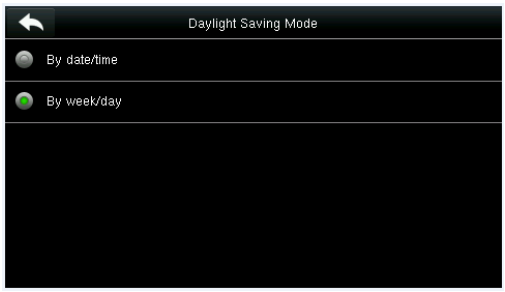


4. Tap **24-Hour Time** to choose whether to enable this format.



5. Tap **Date Format** on the **Date Time** interface to select the date display format.

6. Tap **Daylight Saving Time** to choose whether to enable the daylight saving time.

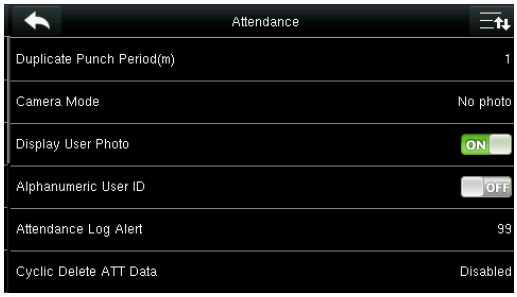


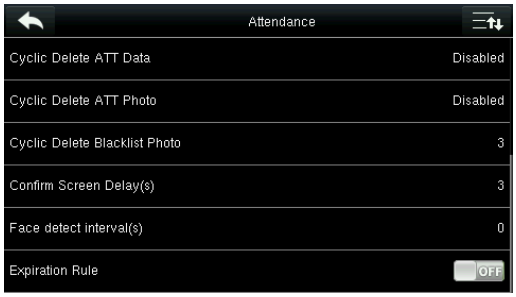
7. Select a daylight saving mode.

8. Set when to start and end the daylight saving time.

7.2 Attendance Parameters

Tap **Attendance** on the **System** interface.



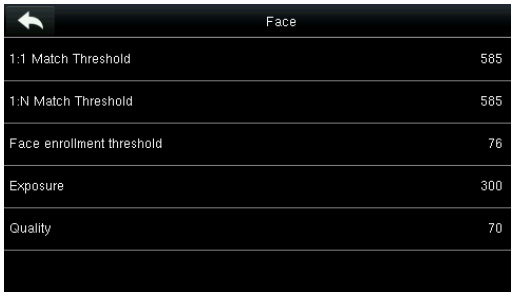


Menu Item	Description
Duplicate Punch Period (m)	Within a set time period (unit: minutes), the duplicated attendance logs will not be reserved (value ranges from 1 to 999999 minutes).
Camera Mode	To set whether to take and save photos in verification; applicable to all users. The following 5 modes are included: **No Photo:** No photo is taken in user verification. **Take photo, no save:** Photo is taken but not saved in verification. **Take photo and save:** Photo is taken and saved in verification. **Save on successful verification:** Photois taken and saved in successful verification. **Save on failed verification:** Photo is taken and saved in failed verification.
Display User Photo	To set user photo to be displayed when a user passes verification. Turn it **[ON]** to display user photo and **[OFF]** to disable it.
Alphanumeric User ID	Whether to support letters in employee ID.
Attendance Log Alert	When the remaining storage is smaller than the set value, the device will automatically alert users to the remaining storage information. It can be disabled or set to a value ranged from 1 to 9999.
Cyclic Delete ATT Data	The number of attendance logs allowed to be deleted in one time when the maximum storage is attained. It can be disabled or set to a value ranged from 1 to 999.
Cyclic Delete ATT Photo	The number of attendance photos allowed to be deleted in one time when the maximum storage is attained. It can be disabled or set to a value ranged from 1 to 99.
Confirm Screen Delay(s)	The display of the verification information interface after verification. Value ranges from 1 to 9 seconds.

Face Detect Interval (s)	To set the face comparison interval as required, within the range of 0-9 s.
Expiration Rule	Whether to enable the expiration rule. If yes, conduct the expiration settings, including: retaining user information, and not saving attendance record; retaining user information, and saving attendance record; and deleting user information.

7.3 Face Parameters

Tap **Face** on the **System** interface.



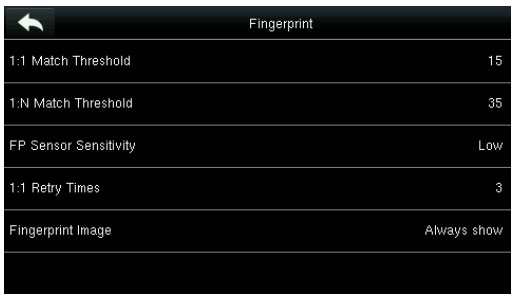
		Match Threshold	
FRR	**FAR**	1:N	1:1
High	Low	85	80
Medium	Medium	82	75
Low	High	80	70

Menu Item	Description
1:1 Match Threshold	Under 1:1 Verification Method, only when the similarity between the verifying face and the user's registered faces is greater than this value can the verification succeed. The valid value range is 70-120, with larger threshold leading to lower misjudgment rate and higher rejection rate, and vice versa.
1:N Match Threshold	Under 1:N Verification Method, only when the similarity between the verifying face and all registered faces is greater than this value can the verification succeed. The valid value range is 80-120, with larger threshold leading to lower misjudgment rate and higher rejection rate, and vice versa.
Face enrollment threshold	In face registration, 1:N comparison is used to determine whether the user has already registered.The device will match the similarity between the current face and the registered face template. When the similarity is greater than this value, the current face is registered.
Exposure	This parameter is used to set the exposure value of the camera.
Quality	This parameter is used to set a quality threshold for the facial images obtained. The FFR terminal accepts the facial images and processes them by adopting the facial algorithm when their quality is higher than the threshold; otherwise, it filters these facial images.

Note: Improper adjustment of the Exposure and Quality parameters may severely affect the performance of the FFR terminal. Please adjust the Exposure parameter only under the guidance of the after-sales service personnel from our company.

7.4 Fingerprint Parameters

Tap **Fingerprint** on the **System** interface.



		Match Threshold	
FRR	**FAR**	1:N	1:1
High	Low	45	25
Medium	Medium	35	15
Low	High	25	10

Menu Item	Description
1:1 Match Threshold	Under 1:1 Verification Method, only when the similarity between the verifying fingerprint and the user's registered fingerprint is greater than this value can the verification succeed.
1:N Match Threshold	Under 1:N Verification Method, only when the similarity between the verifying fingerprint and all registered fingerprints is greater than this value can the verification succeed.
FP Sensor Sensitivity	To set the sensibility of fingerprint collection. 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 Times	**1:1 Retry Times:** In 1:1 Verification or Password Verification, users might forget the registered fingerprint or password, or press the finger improperly. To reduce the process of re-entering user ID, retry is allowed.
Fingerprint Image	To set whether to display the fingerprint image on the screen in registration or verification. Four choices are available: **Show for enroll:** to display the fingerprint image on the screen only during registration. **Show for match:** to display the fingerprint image on the screen only during comparison. **Always Show:** to display the fingerprint image on screen both during registration and comparison. **None:** not to display the fingerprint image in any case.

7.5 Palm Parameters

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

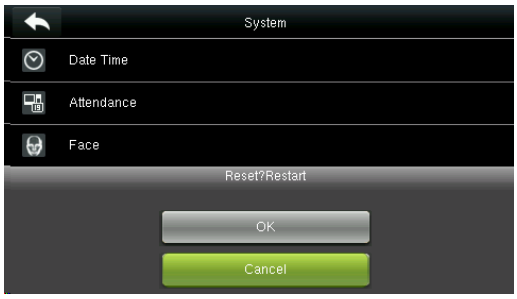
		Match Threshold	
FRR	**FAR**	1:N	1:1
High	Low	45	25
Medium	Medium	35	15
Low	High	25	10

Menu Item	Description
Palm 1:1 Matching Threshold	Under 1:1 Verification Method, only when the similarity between the verifying palm and the user's registered palm is greater than this value can the verification succeed.
Palm 1:N Matching Threshold	Under 1:N Verification Method, only when the similarity between the verifying palm and all registered palm is greater than this value can the verification succeed.

7.6 Reset to Factory Settings

Reset data such as communication settings and system settings to factory settings.

Tap Reset on the System interface.



Press **[OK]** to finish the reset setting.

7.7 USB Upgrade

With this option, the device firmware can be upgraded by using the upgrade file in a USB disk. Before conducting this operation, ensure that the USB disk is properly inserted into the device and contains the correct upgrade file.

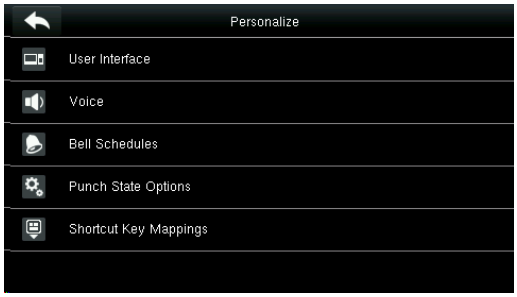
If no USB disk is inserted in, the system gives the following prompt after you tap **USB Upgrade** on the **System** interface.

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

8 Personalize Settings

Conduct related settings of user interface, voice, bell schedule, punch state options, and customize shortcut keys.

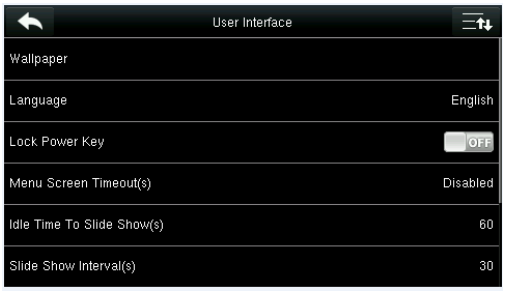
Tap [**Personalize**] on the main menu interface.

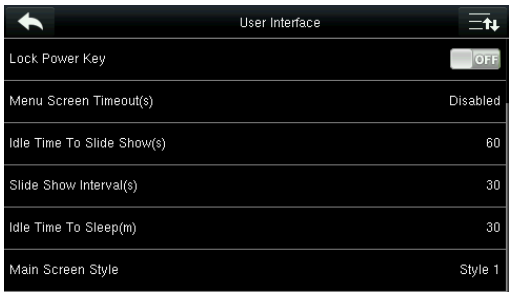


8.1 User Interface Settings

You can customize the display style of the home interface.

Tap **User Interface** on the Personalize interface.



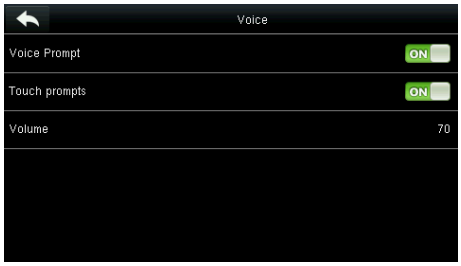


Menu Item	Description
Wallpaper	Select the wallpaper of main screen as required, you can find wallpapers of various styles in the device.
Language	Select the language of device as required.
Lock Power Key	To set whether to lock the power key. When this function is enabled, pressing the power key does not work. When this function is disabled, the system shuts down after you press the power key for three seconds.
Menu Screen Timeout (s)	When there is no operation in the menu interface and the time exceeds the set value, the device will automatically exit to the initial interface. You can disable it or set the value to 60~99999 seconds.
Idle Time To Slide Show (s)	When there is no operation in the initial interface and the time exceeds the set value, a slide show will be shown. It can be disabled (set to "**None** or set to 3~999 seconds.
Slide Show Interval (s)	This refers to the interval between displaying different slide show photos. It can be disabled or set to 3~999 s.

Idle Time To Sleep (m)	When there is no operation in the device and the set Sleep Time is attained, the device will enter standby mode. Press any key or finger to cancel standby mode. You can disable this function, or set the value to 1~999 minutes. If this function is turned to **[Disabled]**, the device will not enter standby mode.
Main Screen Style	Choosing the position and ways of the clock and status key.

8.2 Voice Settings

Tap **User Interface** on the Personalize interface.



Menu Item	Description
Voice Prompt	Select whether to enable voice prompts during operating, press **[ON]** to enable it.
Touch Prompt	Select whether to enable keyboard voice while pressing keyboard, press **[ON]** to enable it.
Volume	Set the volume of device.

8.3 Bells Settings

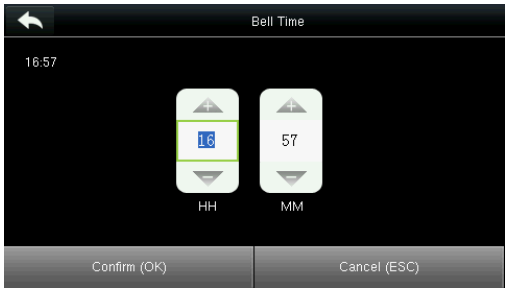
Many companies choose to use bell to signify on-duty and off-duty time. When reaching the scheduled time for bell, the device will play the selected ringtone automatically until the ringing duration is passed.

8.3.1 Add a Bell

Tap **Bell Schedules** on the **Personalize** interface.

1. Tap **New Bell Schedule**.

2. Tap **Bell Status** to enable the bell status.

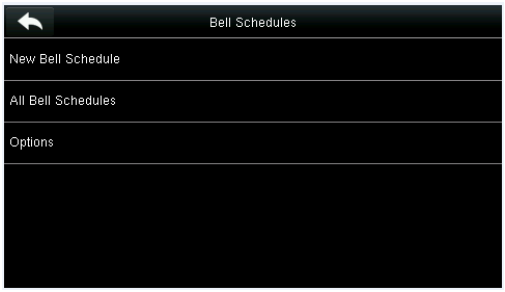


3. Set **Bell Time**.

4. Set **Repeat**.

5. Select a ring tone.

6. Select the internal bell delay.

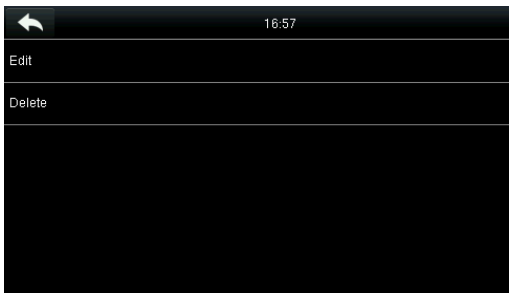


7. Return to the **Bell Schedules** interface and tap **All Bell Schedules**.

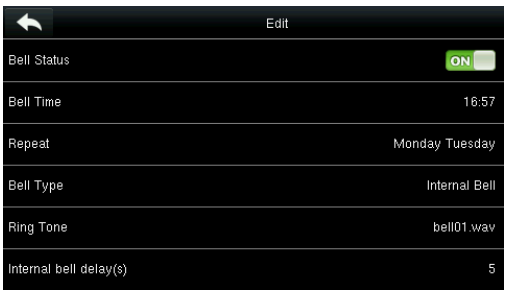
8. The added bells are displayed in a list.

8.3.2 Edit a Bell

On the **All Bell Schedules** interface, tap the bell item to be edited.



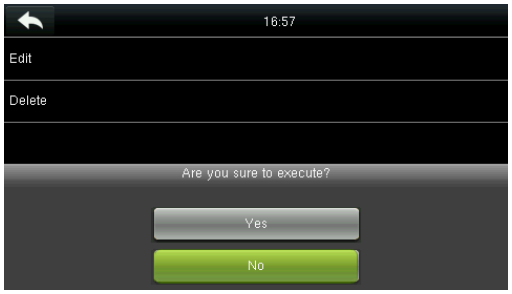
Tap **Edit**.



The editing method is the same as that of a new bell, and not described here.

8.3.3 Delete a Bell

On the **All Bell Schedules** interface, tap a bell item to be deleted.

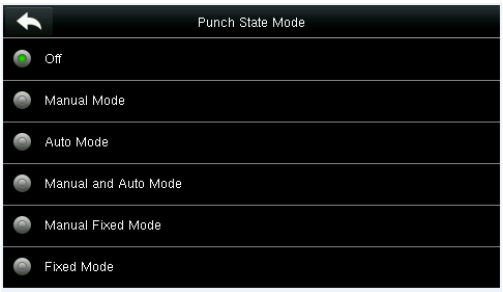


Tap **Delete** and select [**Yes**] to delete the bell.

The bell is deleted successfully.

8.4 Punch States Settings

Tap **Punch State Options** on the **Personalize** interface.



Menu Item	Description
Punch State Mode	Select a punch state mode, which can be: **Off:** To disable the punch state key function. The punch state key set under **Shortcut Key Mappings** menu will become invalid. **Manual Mode:** To switch the punch state key manually, and the punch state key will disappear after **Punch State Timeout**. **Auto Mode:** After this mode is chosen, set **the** switching time of punch state key in **Shortcut Key Mappings**; when the switching time is reached, the set punch state key will be switched automatically. **Manal and Auto Mode:** Under this mode, the main interface will display the auto-switching punch state key, meanwhile supports manually switching punch state key. After timeout, the manually switching punch state key will become auto-switching punch state key. **Manual Fixed Mode:** After punch state key is manually switched, the punch state key will remain unchanged until being manually switched next time. **Fixed Mode:** Only the fixed punch state key will be shown and it cannot be switched.

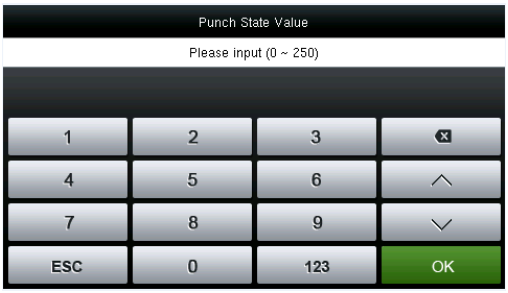
8.5 Shortcut Keys Settings

Shortcut keys can be defined as punch state keys or menu function key. When the device is on the main interface, pressing the set shortcut key will display the attendance state or enter the menu operation interface.

Tap **Shortcut Key Mappings** on the **Personalize** interface.

1. Tap the shortcut key to be set (For the name of corresponding key, refer section 1.6 Initial Interface).

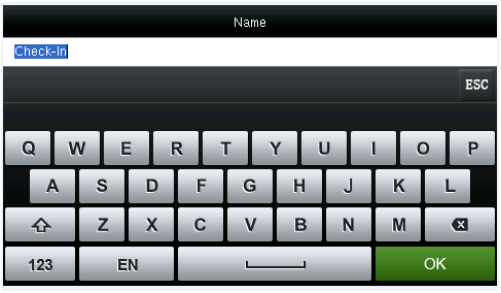
2. The shortcut key setting interface is displayed.



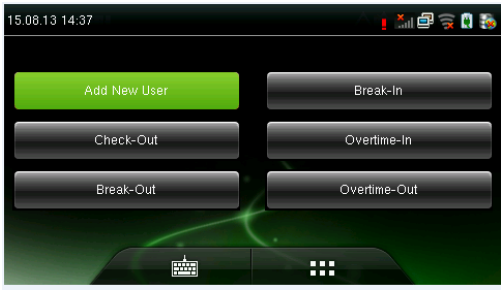
3. Set the state value (value range 0-250).

4. Set corresponding function for this touch key.

6. Set the state key name.



7. Customize and enter a name.



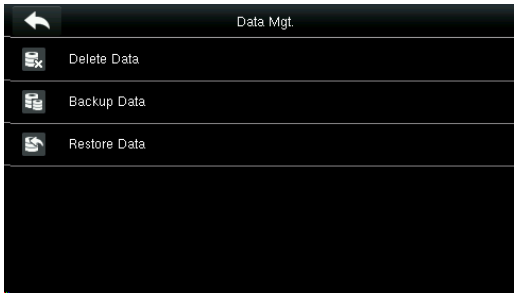
9. Tap the main interface to show the shortcut menu.

Tap the attendance state to make a switch. Tap the function to rapidly access the function settings. (Tap F1 **New User** to rapidly access this menu.)

9 Data Mgt.

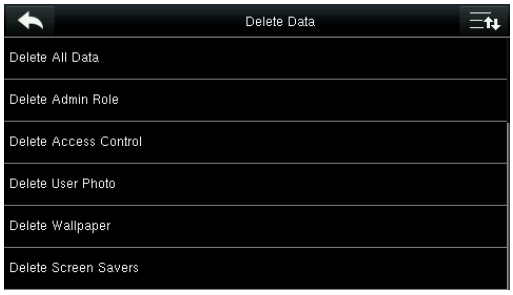
To manage data in the device, which includes delete data, backup data and restore data.

Tap **Data Mgt.** on the main menu interface.



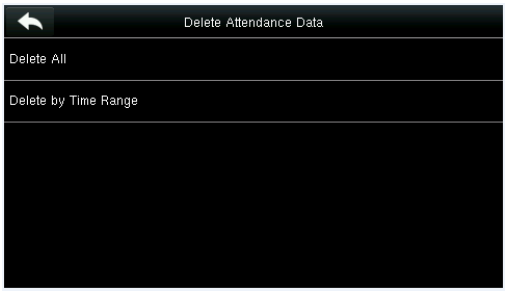
9.1 Delete Data

Tap **Delete Data** on the **Data Mgt.** interface.

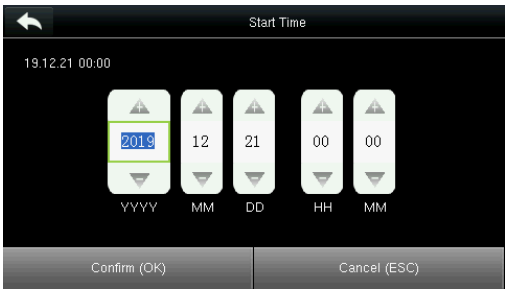


Menu Item	Description
Delete Attendance Data	To delete all attendance data in the device.
Delete Attendance Photo	To delete all users' attendance photos in the device.
Delete Blacklist Photo	To delete all blacklisted photos in the device, which means the photos taken after failed verifications.
Delete All Data	To delete all user information, fingerprints and attendance logs etc.
Delete Admin Role	To make all Administrators become Normal Users.
Delete Access Control	To delete all access data.
Delete User Photo	To delete all user photo in the device.
Delete Wallpaper	To delete all wallpapers in the device.
Delete Screen Savers	To delete all screen savers in the device.

Note: When deleting the attendance record, attendance photo or blacklist photo, you can select **Delete All** or **Delete by Time Range**. When **Delete by Time Range** is selected, you need to set the time range for data deletion.



Select **Delete by Time Range**.

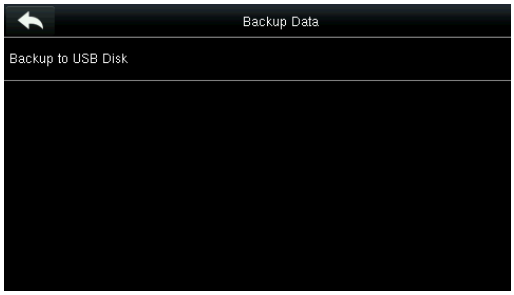


Set the time range and tap **Confirm (OK)**.

9.2 Data Backup

To backup the business data, or configuration data to the U-disk.

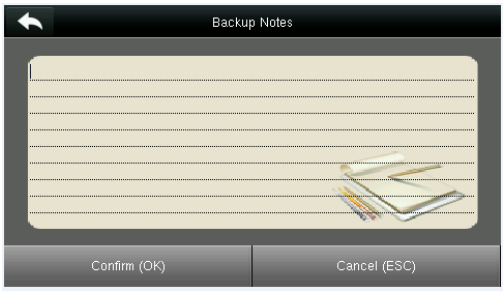
Tap **Backup Data** on the **Data Mgt.** interface.



1. Select **Backup to USB Disk**.

2. Tap **Backup Content**.

3. Select the content to be backed up.



4. Make a backup remark. (This step is optional.)

5. Tap **Backup Start**, and the backup succeeds.

When you choose to save data in a USB disk, ensure that the USB disk is properly plugged into the device.

9.3 Data Restoration

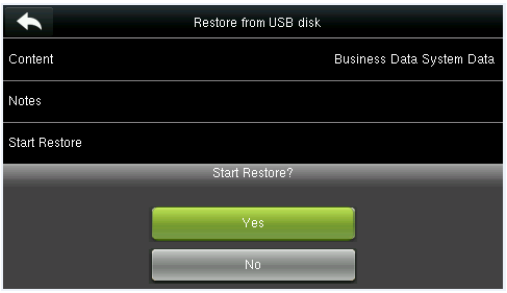
To restore the data in the USB disk to the device.

Tap **Restore Data** on the **Data Mgt.** interface.

1. Tap **Restore from USB Disk**.

2. Tap **Content**.

3. Select the data content to be restored.



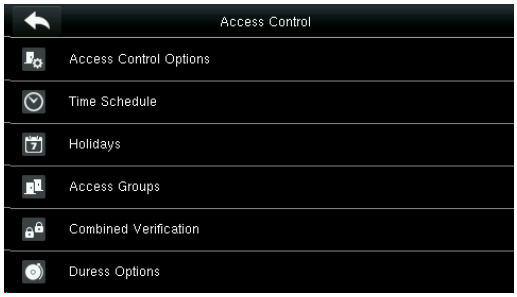
4. Tap start restore and select yes to confirm restoration.

When you choose to save data to a USB disk, ensure that the USB disk is properly plugged into the device and contains corresponding data to be restored.

10 Access Control

Access Control option is used to set the Time Schedule, Holidays, Access Groups, Combined Verification etc., the related parameters for the device to control the lock and other devices.

Tap [**Access Control**] on the main menu interface.



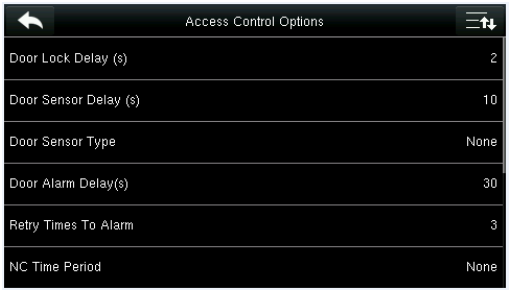
To gain access, the registered user must meet the following conditions:

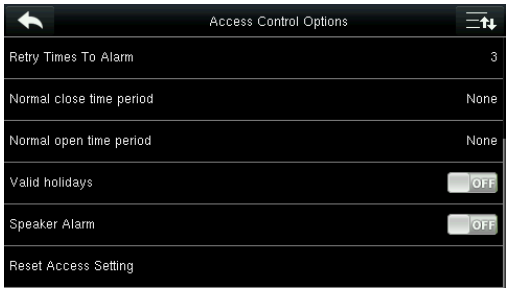
1. User's access time falls within either user's personal time zone or group time zone.
2. User's group must be in the access combo (when there are other groups in the same access combo, verification of members of those groups are also required to unlock the door).
   In default settings, new users are allocated into the first group with the default group time zone and access combo as "1(, and set in unlocking state.

10.1 Access Control Options Settings

To set the parameters of the equipment control lock and related equipment.

Tap **Access Control Options** on the **Access Control** interface.





Menu Item	Description
Door Lock Delay (s)	The period of time of unlocking (from door opening to closing automatically) after the electronic lock receives an open signal sent from the device (value ranges from 0 to 10 seconds).s
Door Sensor Delay (s)	When the door is opened, the door sensor will be checked after a time period; if the state of the door sensor is inconsistent with that of the door sensor mode, alarm will be triggered. The time period is the **Door Sensor Delay** (value ranges from 1 to 255 seconds).
Door Sensor Type	It includes **Normally Open**, **Normally Closed** and **No**. **No** means door sensor is not in use; **Normally Open** means the door is opened when electricity is on; **Normally Closed** means the door is closed when electricity is on.
Door Alarm Delay (s)	When the state of the door sensor is inconsistent with that of the door sensor type, alarm will be triggered after a time period; this time period is the **Door Alarm Delay** (the value ranges from 0 to 999 seconds).

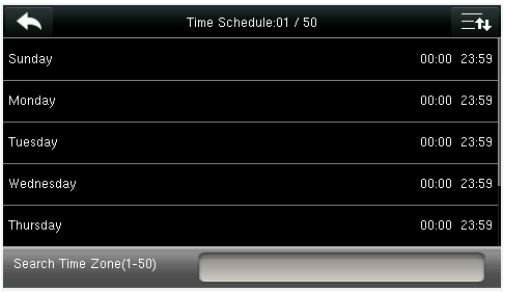
Retry Times To Alarm	When the number of failed verification reaches the set value (value ranges from 1 to 9 times), the alarm will be triggered. If the set value is None, the alarm will not be triggered after failed verification.
NC Time Period	To set time period for Normally Closed mode, so that no one can gain access during this period.
NO Time Period	To set time period for Normally Open, so that the door is always unlocked during this period.
Valid holidays	To set if **NC Time Period** or **NO Time Period** settings are valid in set holiday time period. Choose **[ON]** to enable the set **NC** or **NO** time period in holiday.
Speaker Alarm	When the **[Speaker Alarm]** is enabled, the speaker will raise an alarm when the device is being dismantled.
Reset Access Setting	To restore access control parameters.

Note: After setting NC Time Period, please lock the door well, otherwise alarm might be triggered during NC Time Period.

10.2 Time Schedule Settings

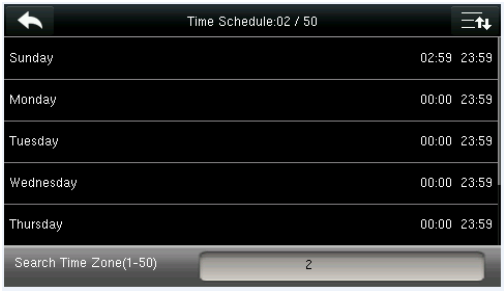
Time Schedule is the minimum time unit of access control settings; at most 50 **Time Schedules** can be set for the system. Each **Time Schedule** consists of 7 time sections (a week), and each time section is the valid time within 24 hrs.

Tap **Time Schedule** on the **Access Control** interface.

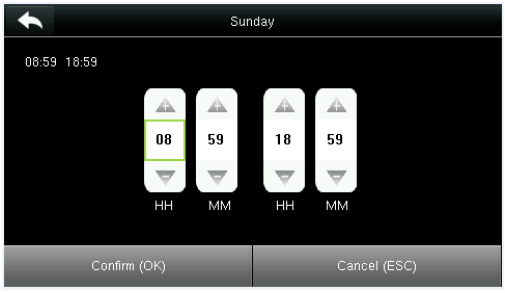


1. Tap the input box of search time zone.

2. Enter the number of time zone (50 in total to be searched.)



3. Tap the date on which time zone setting is required.



4. Press **Up and Down** to set the start and end time, and then press **Confirm (OK).**

Valid Time Schedule: 00:00 ~ 23:59 (Whole-day valid) or when the end time is greater than the start time.

1. **Invalid Time Schedule:** When the end time is smaller than the start time.
2. The default time zone 1 indicates that system is open all day long.

10.3 Holidays Settings

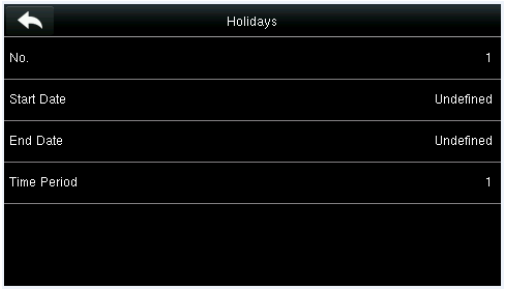
The concept of holiday and festival is introduced into access control. On holidays or festivals, special access control time may be required, but changing everyone's access control time is very tedious. Therefore, the access control time on holidays and festivals, which applies to all staff, can be set.

If the access control time on holidays and festivals is set, the opening period of time on holidays and festivals subjects to the time period set here.

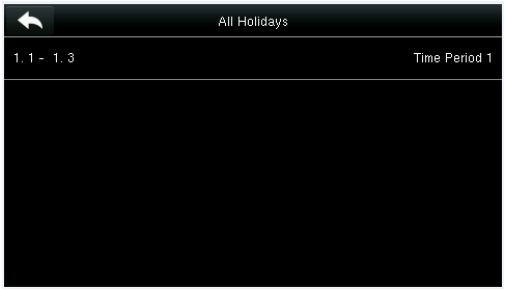
Tap **Holidays** on the **Access Control** interface.

10.3.1 Add a New Holiday

Tap **Add Holiday** on the **Holidays** interface.



Set holiday parameters.



The added holidays are displayed in a list.

10.3.2 Edit a Holiday

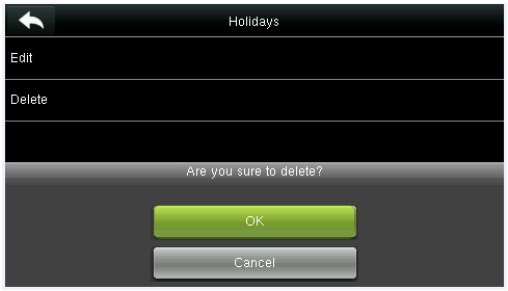
On the Holidays interface, tap to select an item to be modified.

Tap [**Edit**].

Modify holiday parameters.

10.3.3 Delete a Holiday

On the **Holidays** interface, tap to select a holiday item to be modified, and tap **Delete**.



Tap Ok to confirm deletion.

After deletion, this holiday is no longer displayed in All Holidays.

10.4 Access Groups Settings

Grouping is to manage users in the groups.

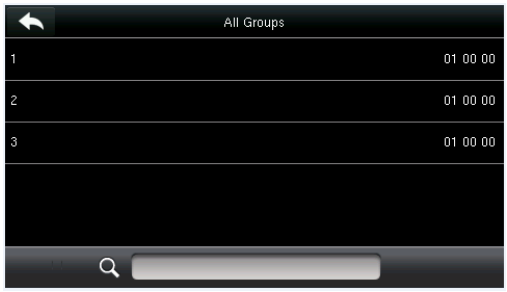
Group users' default time zone is set to be the group time zone, while users can set their personal time zone. When the group verification mode overlaps the user verification mode, the user verification modes prevails. Each group can set 3 time zones at most, as long as one of them is valid, the group can be verified successfully. By default, the newly enrolled user belongs to Access Group 1, and can also be allocated to other access group.

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

10.4.1 Add a New Group

Tap **New Group** on the **Access Groups** interface.

Set access group parameters.



The added access groups are displayed in a list. You can rapidly search for groups by number.

Note:

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

4. When the holiday is set to be invalid, the access control time of the personnel in this group is not affected by holidays.

10.4.2 Edit a Group

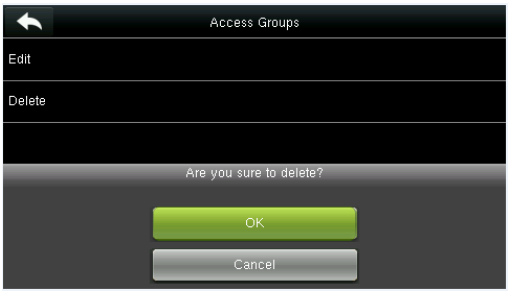
On the **All Groups** interface, tap to select the access group item to be modified.

Tap **Edit**.

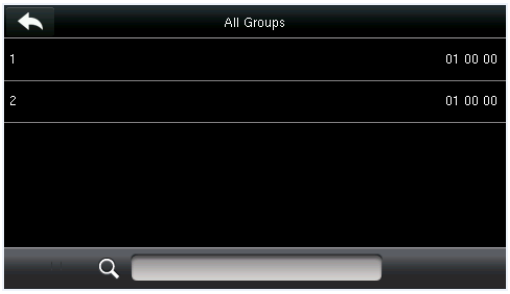
Modify access group parameters.

10.4.3 Delete a Group

On the **All Groups** interface, tap to select the access group item to be modified, and tap **Delete**.



Tap **OK** to confirm deletion.

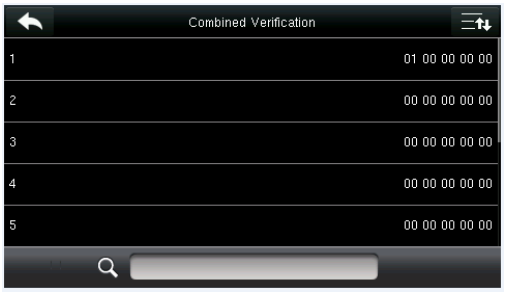


The deleted access group is no longer displayed in **All Groups**.

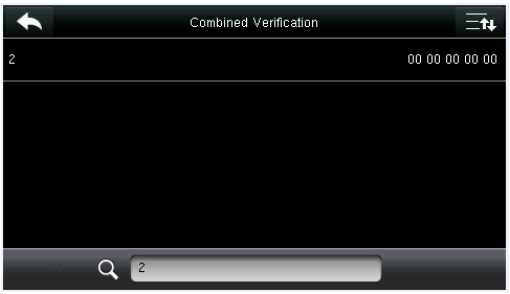
10.5 Combined Verification Settings

Combine two or more members to achieve multi-verification and improve security.

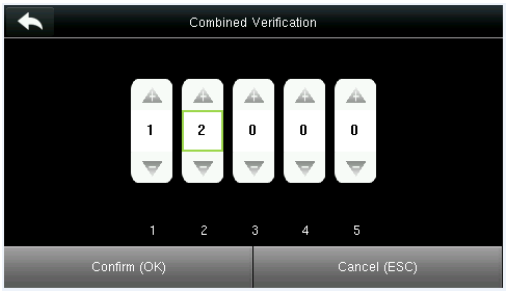
Tap **Combined Verification** on the **Access Control** interface.



1. Tap the unlocking combination to be set or tap the search bar and enter an unlocking combination number to find the specific combination.



2. Tap this unlocking combination item.



Note:

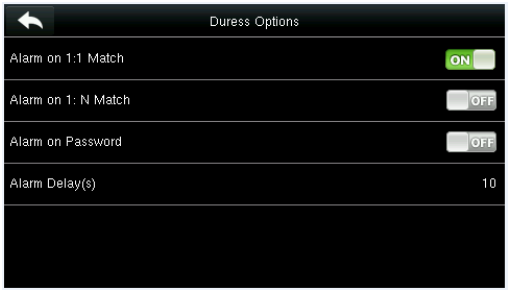
In a Combined Verification, the range of user number is: 0 ≤ N ≤ 5. If you need to delete an unlocking combination, directly set all digits of the combination number to 0. If you need to modify a combination, directly tap corresponding combination item to conduct setting again.

3. Tap **Up** and **Down** to enter the combination number, and then press [**Confirm (OK)**].

10.6 Duress Options Settings

When users come across duress, select duress alarm mode, the device will then open the door as usual and send the alarm signal to the backstage alarm.

Tap **Duress Options** on the **Access Control** interface.



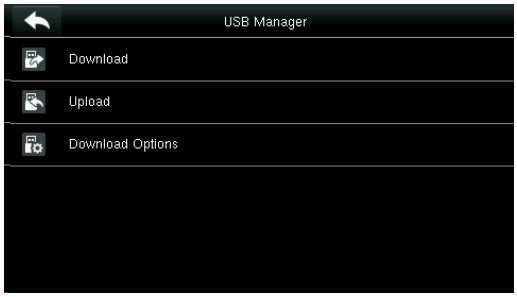
Menu Item	Description
Alarm on 1:1 Match	In **[ON]** state, when a user uses 1:1 Verification Method to verify any registered fingerprint, alarm will be triggered. In **[OFF]** state, no alarm signal will be triggered.
Alarm on 1: N Match	In **[ON]** state, when a user uses 1:N Verification Method to verify any registered fingerprint, alarm will be triggered. In **[OFF]** state, no alarm signal will be triggered.
Alarm on Password	In **[ON]** state, when a user uses password verification method, alarm will be triggered. In **[OFF]** state, no alarm signal will be triggered.
Alarm Delay (s)	When duress alarm is triggered, the device will send out alarm signal after 10 seconds (default); the alarm delay time can be changed (value ranges from 1 to 999 seconds).

11 USB Manager

You can import the user information, fingerprint template and attendance data in the machine to matching attendance software for processing by using a USB disk, or import the user information and fingerprints to other fingerprint devices for backup.

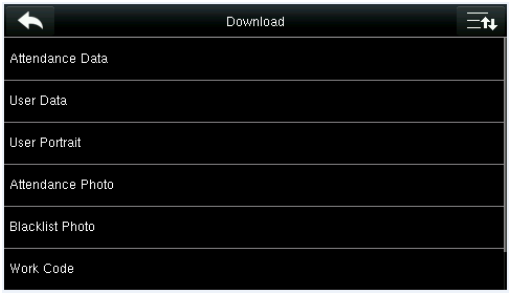
Before uploading/downloading data from/to the USB disk, insert the USB disk into the USB slot first.

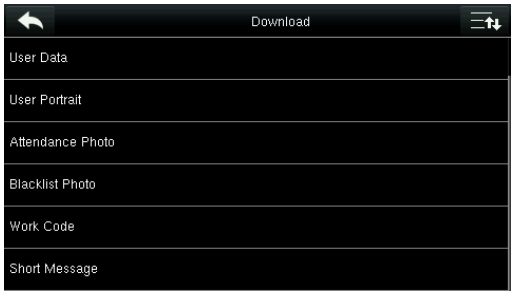
Tap **USB Manager** on the main menu interface.



11.1 USB Download

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

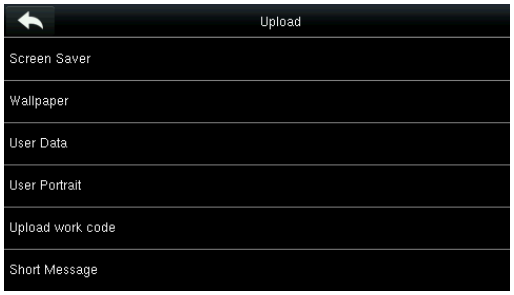




Menu Item	Description
Attendance Data	To download attendance data in specified time period into USB disk.
User Data	To download all user information and fingerprints from the device into USB disk.
User Portrait	To download all user photos from the device into a USB disk.
Attendance Photo	To download all attendance photos from the device into USB disk.
Blacklist Photo	To download all blacklisted photos (photos taken after failed verifications) from the device into USB disk.
Work Code	To save the work code in the device to a USB disk.
Short Message	To download the short message set in the device to a USB disk.

11.2 USB Upload

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



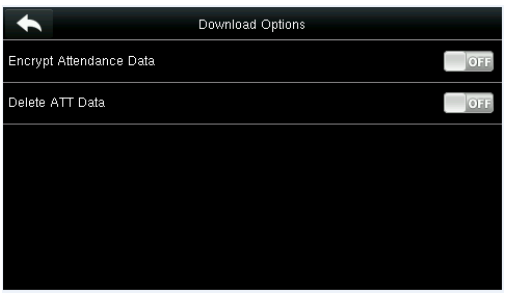
Menu Item	Description
Screen Saver	To upload all screen savers from USB disk into the device. You can choose **Upload selected photo** or **Upload all photos**. The images will be displayed on the device's main interface after upload. During uploading, you need to create a folder named "**advertise**" in the root directory of the USB disk, and put the advertising photos in this directory. A maximum of 20 photos are supported and each photo cannot exceed 30 KB. The photo name and format are not limited, with formats such as jpg, png and bmp supported.
Wallpaper	To upload all wallpapers from USB disk into the device. You can choose **Upload selected photo** or **Upload all photos**. The images will be displayed on the screen after upload. During uploading, you need to create a folder named "**wallpaper**" in the root directory of the USB disk, and put the wallpaper photos in this directory. A maximum of 20 photos are supported and each photo cannot exceed 30 KB. The photo name and format are not limited, with formats such as jpg, png and bmp supported.
User Data	To upload all user information and fingerprints from the device into USB disk.
User Portrait	To upload all user photos from the device into a USB disk.
Upload Work Code	To upload work codes in the USB disk to the device.
Short Message	To upload short messages saved in the USB disk to the device.

Note: The size of a single user photo or attendance photo does not exceed 10 KB, and the device can save a total of 10,000 user photos and attendance photos.

The optimal size of an advertising photo or wallpaper is 640*480.

11.3 Download Options Settings

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

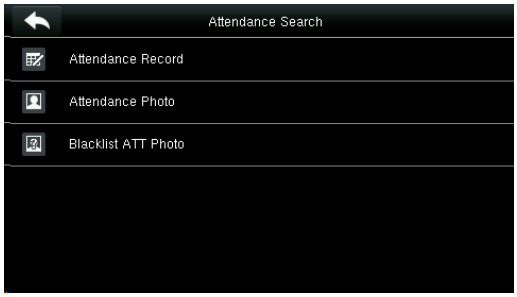


Menu Item	Description
Encrypt Attendance Data	During uploading and downloading, the attendance data is encrypted.
Delete ATT Data	After successful downloading, the attendance data on the device is deleted.

12 Attendance Search

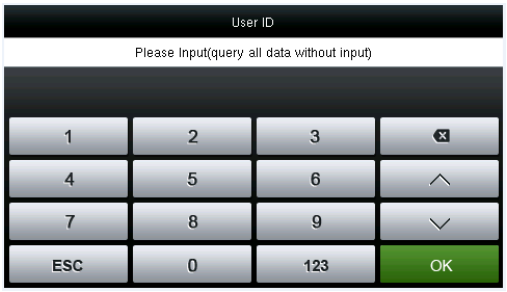
When users verify successfully, attendance records are saved in the device. This function enables users to check attendance logs.

Tap **Attendance Search** on the main menu interface.

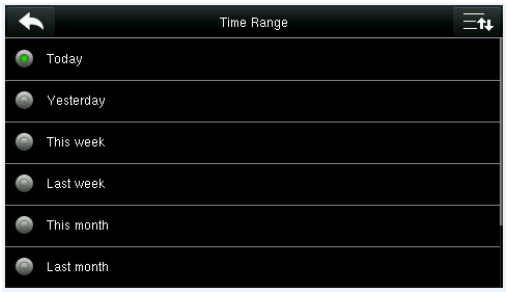


The process of querying attendance photos and blacklist photos is the same as that of querying attendance records. The following is an example of querying attendance records.

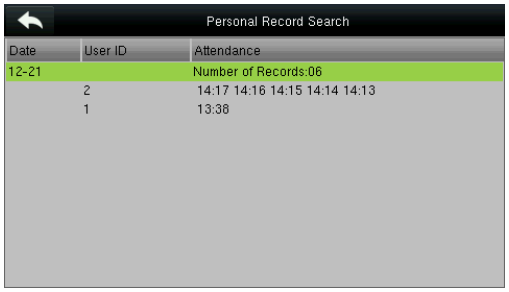
On the **Attendance Record** interface, tap **Attendance Record**.



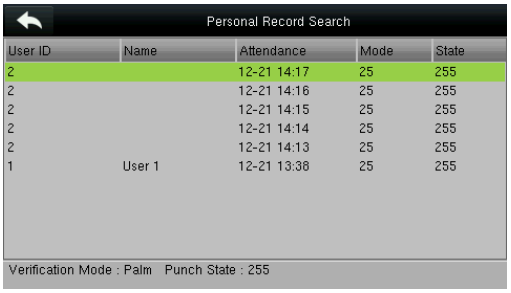
1. Enter the user ID to be searched and tap **OK**. Taping **OK** without entering a user ID searches the attendance records of all employees.



2. Select the time range for attendance record query.



3. The record search succeeds. Tap the record in green to view its details.

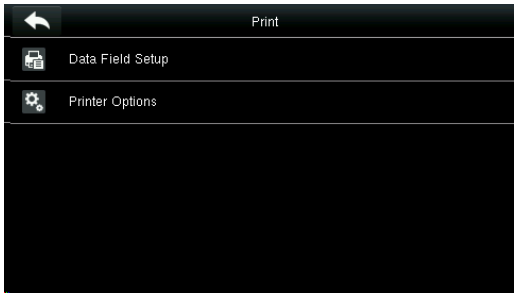


4. The above figure shows the details of this record.

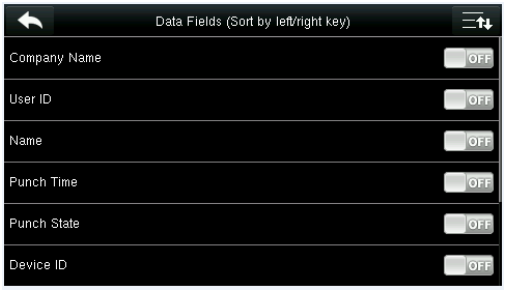
13 Print Settings ★

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

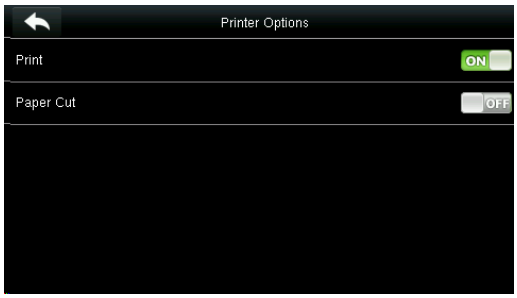
Tap [**Print**] on the main menu interface.



Tap **Data Field Setup** on the Print interface.



Press **ON/OFF** to turn on / off the fields needing to be printed.



Press **ON/OFF** to turn on / off the **Paper Cut** function.

Note:

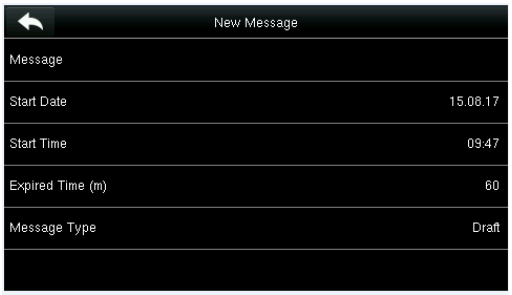
To turn on the **Paper Cut** function, it is required to connect the device with a printer with paper cutting function, so that the printer will cut papers according to the selected printing information when printing.

14 Short Messages

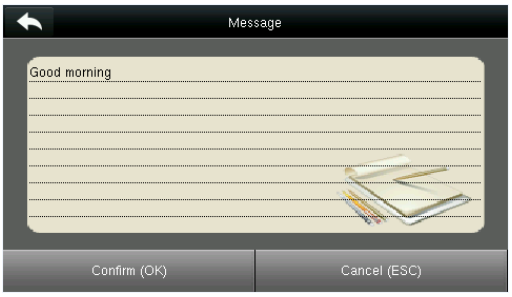
SMS is similar to notice. The operator can edit the notice content in advance and display it in SMS format on the screen. SMS includes common SMS and individual SMS. If common SMS is set,  will be displayed in information column at the top of the standby interface in specified time. If individual SMS is set, the employee who can receive SMS can see SMS after successful attendance.

14.1 Add a New Short Message

1. Entering the content: Enter the content of a short message with an input method.

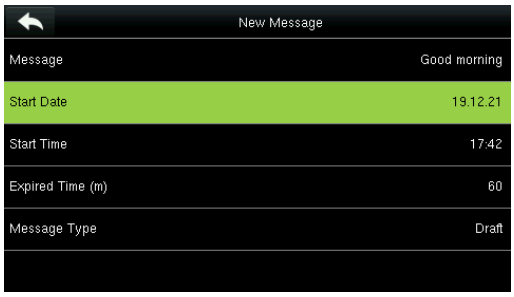


Tap **Message**.

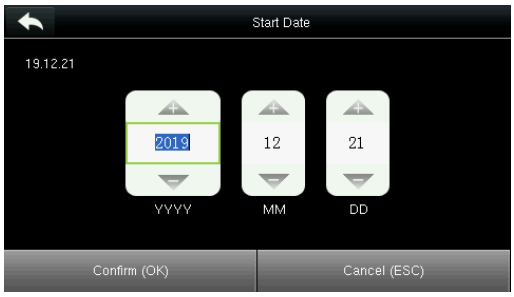


Enter the content and press **OK** to save the entered content and quit.

2. Setting the start date and time: the date and time when the short message becomes valid.



Select **Start Date** and press **OK**.



Press the numeric keys on the keypad to enter the date and press **OK**.

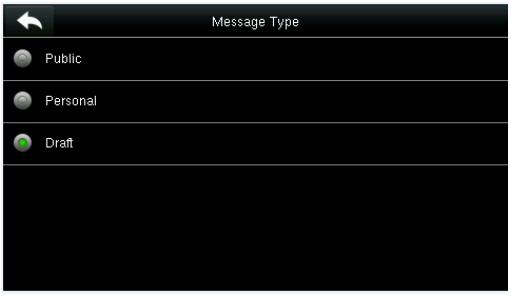
3. Set Expired time(m)SMS appears in the effective time. After the effective time, it won't appear.

Notes: For public short messages, the effective period is also the display period. For private short messages, you need to set a display period after setting an effective period. That is, the display period of a private short message can be viewed when you punch in or out during the effective period of the message.

4. Set Message type

Public: SMS able to be seen by all employees.
Personal: SMS aimed at individual only.
Draft: Preset SMS, no difference of individual SMS or common SMS.

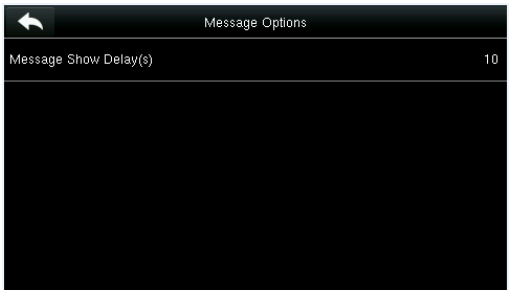
Select **Message** Type and press **OK**.

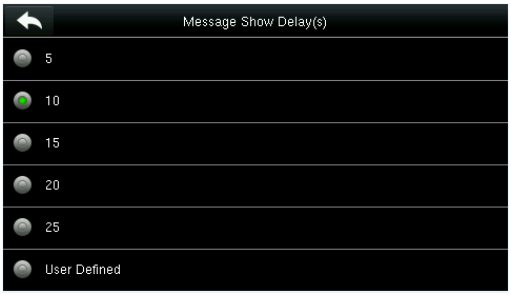


Press ▼ to select a type and press **OK** for confirmation.

14.2 Message Options

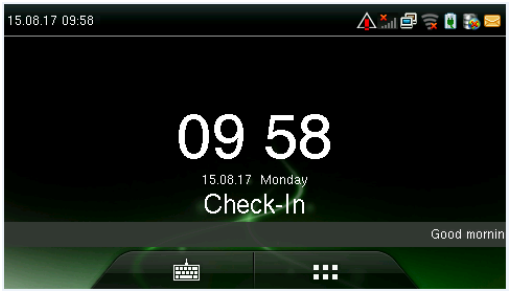
Set the personal Message Show Delay time on the initial interface.



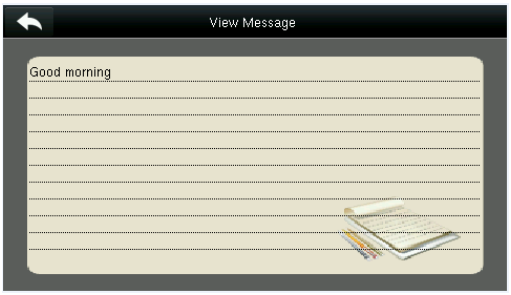


14.3 View the Public Messages and Personal Message

After a public short message is set, the short message icon is displayed on the upper right of the main interface, and the public short message content is displayed in scroll mode below. The content of a personal short message is displayed after successful user authentication.



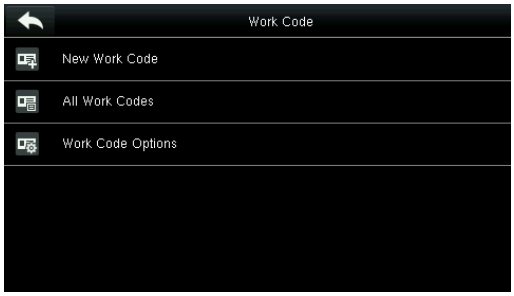
The public short message is -displayed in the lower part of the interface.



The personal short message is displayed after successful user authentication.

15 Work Code

Employees' salaries are subject to their attendance records. Employees may be engaged in different types of work which may vary with time periods. Considering the salaries vary with work types, the FFR terminal provides a parameter to indicate the corresponding work type for every attendance record to facilitate rapid understanding of different attendance situations during the handling of attendance data.

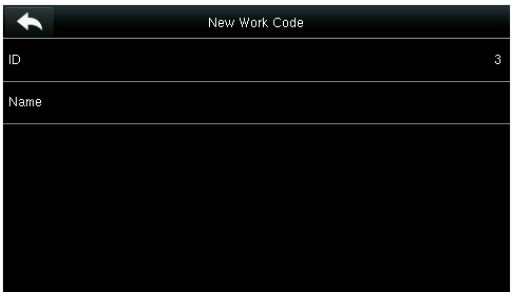


15.1 Add a Work Code

No.: A digital code of the work code.

Label: The meaning of the work code.

1. Editing an ID

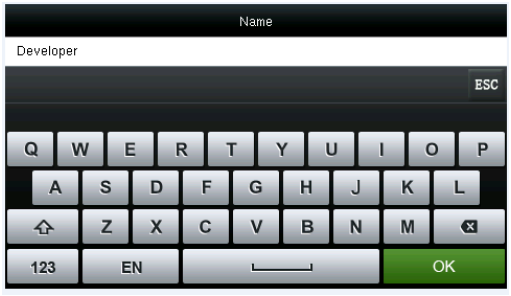


Select **ID**.

Press the numeric keys to assign a number between 1~99999999.

2. Editing a name

Select **Name**.

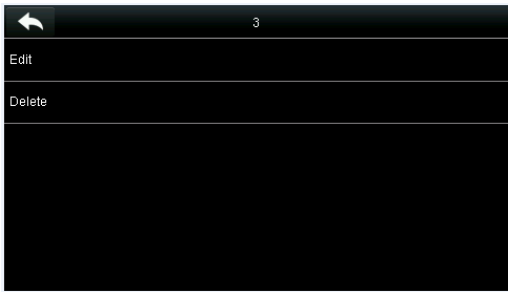


Press ***** to select an input method and enter a name.

15.2 All Work Codes List

You can view, edit and delete work codes **in All Work Codes** interface. The process of editing a work code is the same as that of adding a work code except that the ID is not allowed to be modified.

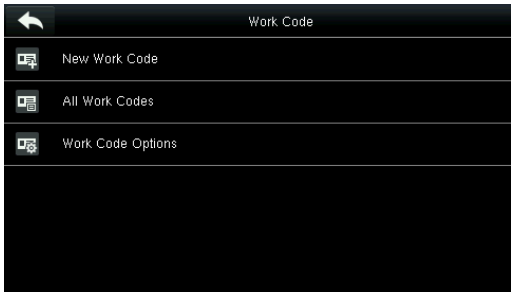
View the information about all work codes.



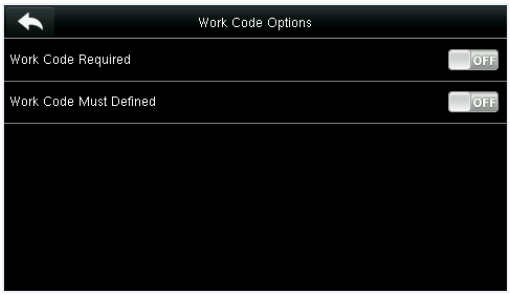
Edit or delete a work code.

15.3 Work Code Options

To set whether the work code must be entered and whether the entered work code must exist during authentication.



Select **Work Code Options**.

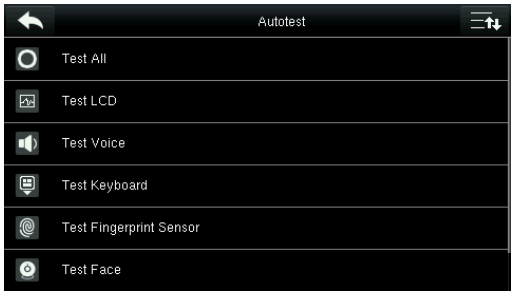


Press **ON/OFF** to turn on or off.

16 Autotest

To automatically test whether all modules in the device function properly, which include the LCD, voice, keyboard, fingerprint sensor, camera and RTC (Real-Time Clock).

In the initial interface, press **[Autotest]** to enter the **Autotest** interface.

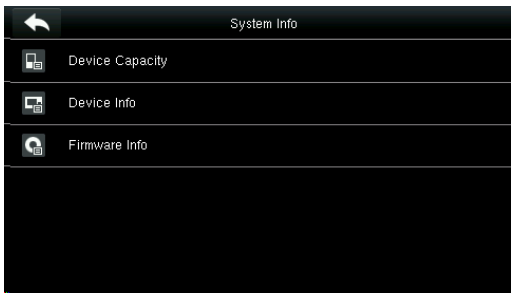


Menu Item	Description
Test All	To test LCD, Voice, Keyboard, Fingerprint Sensor, Face, and Clock RTC. During the test, Touch the screen to continue, while press [ ] to exit the test.
Test LCD	To test the display effect of LCD screen by displaying full color, pure white, and pure black to check whether the screen displays colors properly.
Test Voice	The device automatically tests whether the voice files stored in the device are complete and the voice quality is good.
Test Keyboard	Test if the keyboard is working by checking if the screen is normal enough.
Test Fingerprint Sensor	To test the fingerprint sensor by pressing fingerprint to check if the collected fingerprint image is clear. When pressing fingerprint on the sensor, the image will be displayed on the screen.
Test Face	To test if the camera functions properly by checking the photos taken are clear for use.
Test Clock RTC	To test the Real-Time Clock. The device tests whether the clock works properly and accurately by checking the stopwatch. Touch the screen to start counting time, and press it again to stop counting, to see if the stopwatch counts time accurately.

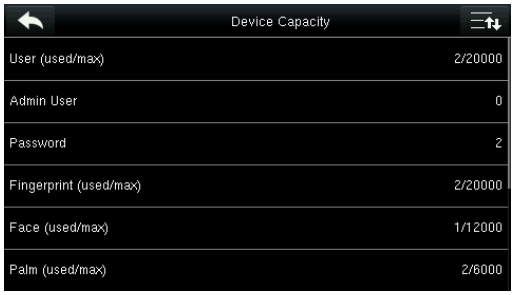
17 System Information

Check data capacity, device and firmware information.

Tap [**System Info**] on the main menu interface.



1. On the System Info interface, tap an information item to be browsed.



2. View the data capacity information, and press **Page Down** to view other information.

3. View the device information, and press **Page Down** to view other information.

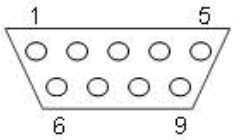
4. View the device firmware information.

Appendix 1 Printing Function ★

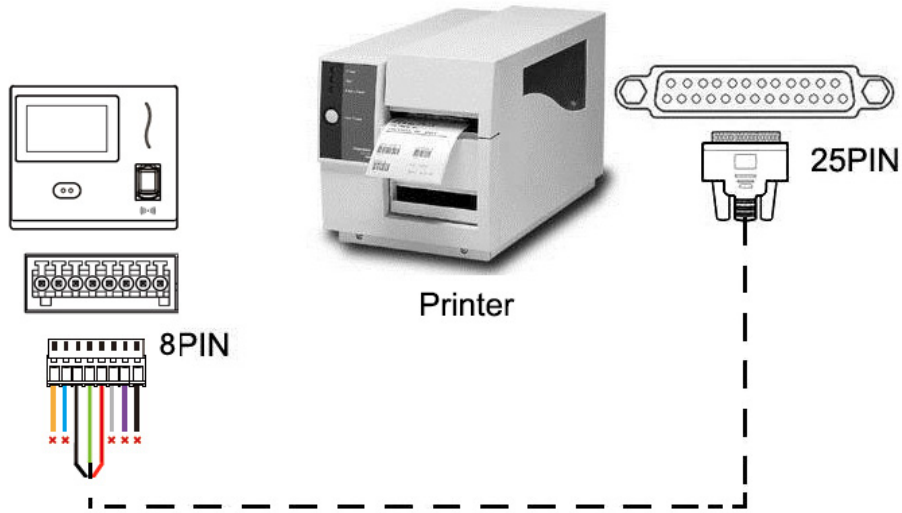
☺ **Remarks: Only some models support printing function.**

Function Instruction

This function only supports serial port but not parallel port printing. Printing content is output via RS232 format; verification information will be output every time to the serial port. Printing is available if a printer is connected, or a hyper terminal can be used to read output content.

Connection between the device and printer	**Device**		**Printer**
	2TXD	<----->	3 RXD
	3RXD	<----->	2 TXD
	5GND	<----->	7 FG
RS232 Pin-line order			

[Connection Diagram]



[Operation]

1. In the initial interface, press **[M/OK]** > **Comm.** > **Serial Comm** > **Baudrate**, and choose 19200 as the baud rate.
2. In the initial interface, press [M/OK] > Print. To set the printing format and parameters, please refer to 13 Print Settings ★

Note:

1. The baud rate of the device and printer (hyper terminal) should be consistent.
2. If the default printing format is not satisfactory, you may contact our company to customize other formats.

Appendix 2 Statement on the Right to Privacy

Dear Customers:

Thank you for choosing this hybrid biometric recognition product, which was designed and manufactured by ZKTeco. As a world-renowned provider of core biometric recognition technologies, we are constantly developing and researching new products, and strive to follow the privacy laws of each country in which our products are sold.

We Declare That:

1. All of our civilian fingerprint recognition devices capture only characteristics, not fingerprint images, and do not involve privacy protection.
2. None of the fingerprint characteristics that we capture can be used to reconstruct an image of the original fingerprint, and do not involve privacy protection.
3. As the provider of this device, we will assume no direct or indirect responsibility for any consequences that may result from your use of this device.
4. If you would like to dispute human rights or privacy issues concerning your use of our product, please directly contact your dealer.

Our other law-enforcement fingerprint devices or development tools can capture the original images of citizen's fingerprints. As to whether or not this constitutes an infringement of your rights, please contact your Government or the final supplier of the device. As the manufacturer of the device, we will assume no legal liability.

Note:

The Chineselaw includes the following provisions on the personal freedom of its citizens:

1. There shall be no illegal arrest, detention, search, or infringement of persons;
2. Personal dignity is related to personal freedom and shall not be infringed upon;
3. A citizen's house may not be infringed upon;
4. A citizen's right to communication and the confidentiality of that communication is protected by the law.

As a final point, we would like to further emphasize that biometric recognition is an advanced technology that will be certainly used in E-commerce, banking, insurance, judicial, and other sectors in the future. Every year the world is subjected to major losses due to the insecure nature of passwords. The Biometric products serve to protect your identity in high-security environments.

Appendix 3 Eco-friendly Operation

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

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

Hazardous or Toxic substances and their quantities

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

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

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

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

Green Label

ZKTeco Industrial Park, No.26, 188 Industrial Road,
Tangxia Town, Dongguan, China
Tel: +86 769-82109991
Fax: +86 755-89602394
www.zkteco.com