User Manual

uFace Plus Series Terminal

Date: April 2020

Doc Version: 1.0

English

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

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

Copyright © 2020 ZKTECO CO., LTD. All rights reserved.

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

Trademark

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

Disclaimer

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

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

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

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

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

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

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

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

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

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

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

ZKTeco Headquarters

Address ZKTeco Industrial Park, No. 26, 188 Industrial Road,
Tangxia Town, Dongguan, China.

Phone +86 769 - 82109991

Fax +86 755 - 89602394

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

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

About the Company

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

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

About the Manual

This manual introduces the operations of uFace Plus Series Terminals.

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

Features and parameters with ★ are not available on all the devices.

Document Conventions

Conventions used in this manual are listed below:

GUI Conventions

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

Symbols

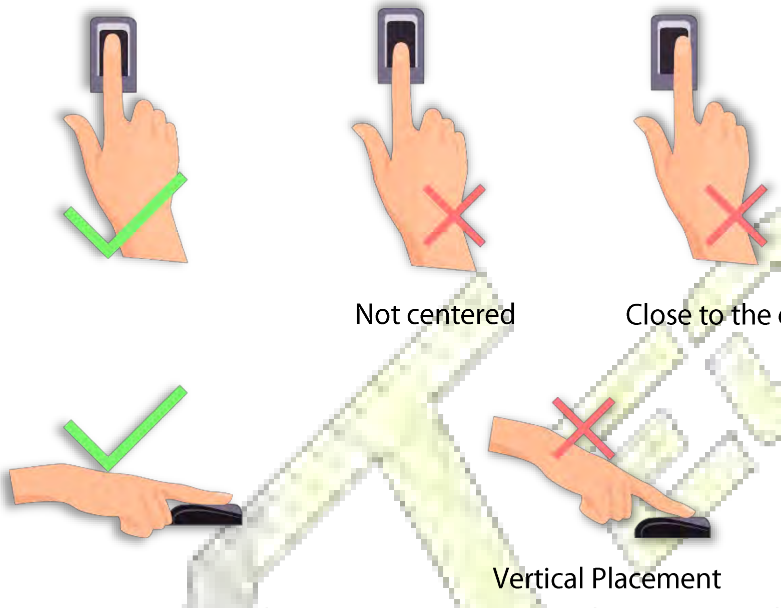
Convention	Description
📝	This implies about the notice or pays attention to, in the manual
💡	The general information which helps in performing the operations faster
★	The information which is significant
🛑	Care taken to avoid danger or mistakes
⚠	The statement or event that warns of something or that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

Table of Contents

1. Instructions for use

1.1 Finger Positioning

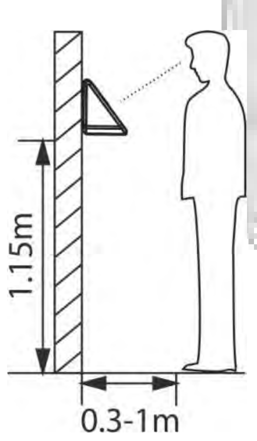
Recommended fingers: It is recommended to use index, middle, or ring fingers. Avoid using the thumb or little finger, as they are difficult to press accurately on the fingerprint reader.



Note: Please follow the instructions carefully when pressing your finger on the fingerprint reader for registration and identification. Our company will assume no liability for recognition issues that may result from incorrect usage of the product. We reserve the right of final interpretation and modification concerning this point.

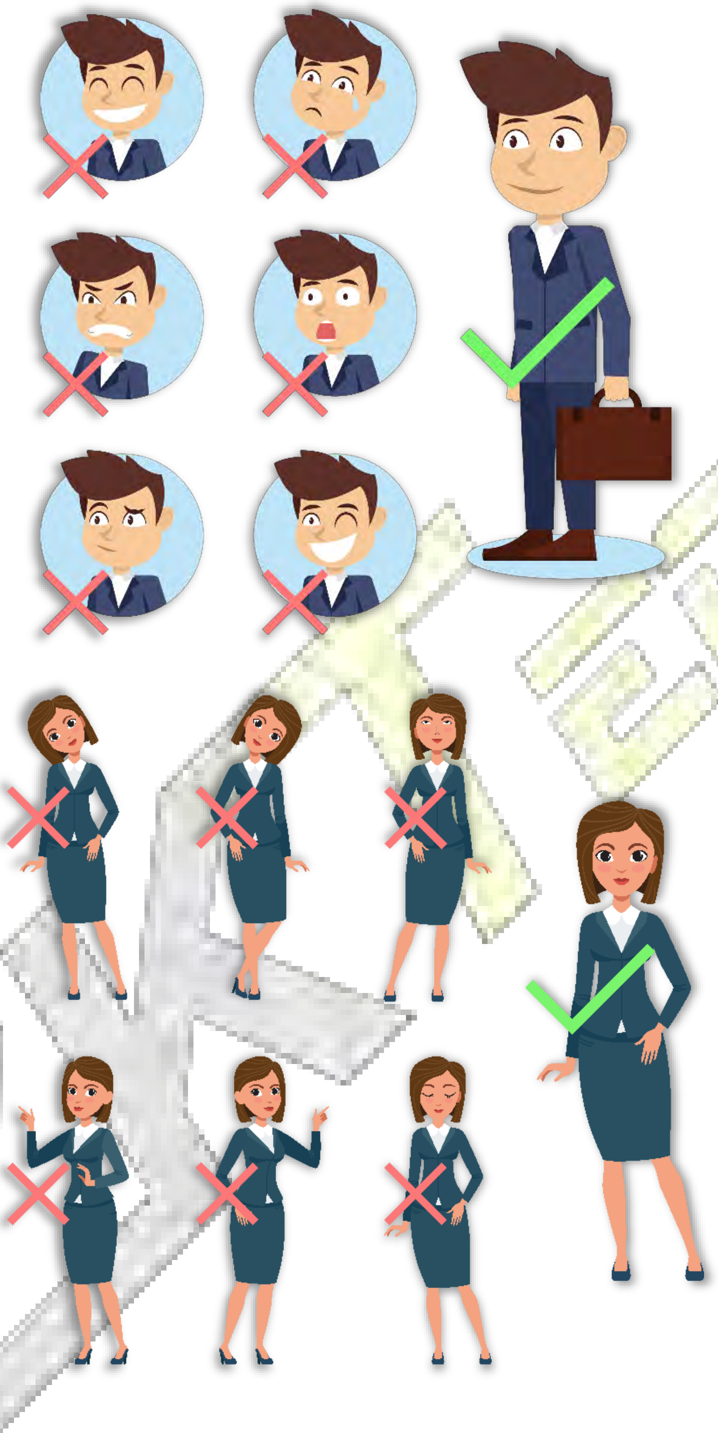
1.2 Standing Position, Facial Expression and Standing Posture

Recommended distance



The distance between the device and a user whose height is within 1.55m to 1.85m is recommended to be 0.3 to 1m. Users may slightly move forward and backward to improve the quality of the captured facial images.

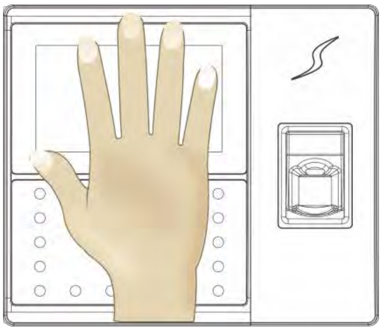
Facial expressions and Standing postures



Note: During enrollment and verification, please keep natural facial expression and standing posture.

1.3 Palm Position

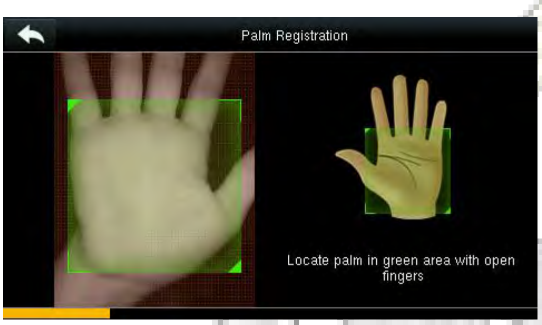
How to enroll the palm correctly



Place your palm in the palm collection area, such that the palm is placed parallel to the device. Make sure to keep space between your fingers.

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 the palm forward and backward to adjust the palm position during palm registration.

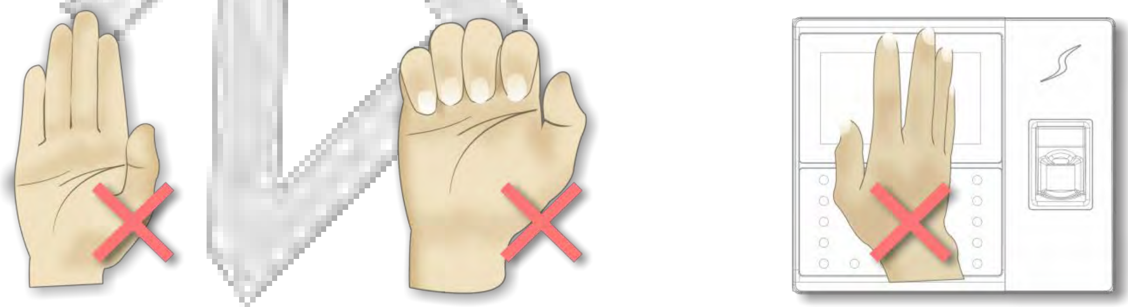
Verification



Locate palm in green area with open fingers

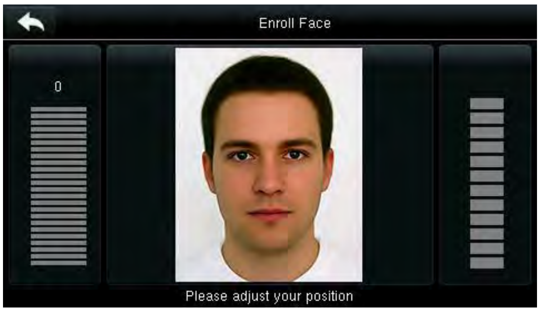
Place your palm in the green area parallel to the device with space between the fingers.

Incorrect palm gestures



1.4 Face Registration

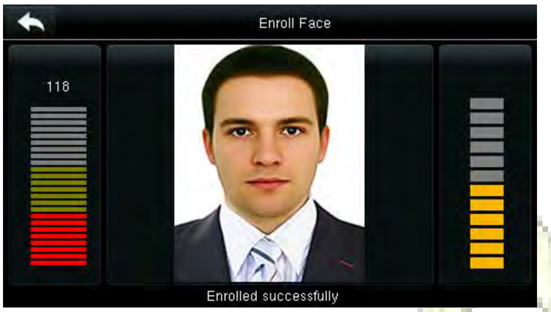
During face registration, you need to move forward or backward to ensure that your face is displayed in the center of the screen until the success prompt appears.



Enroll Face

0

Please adjust your position



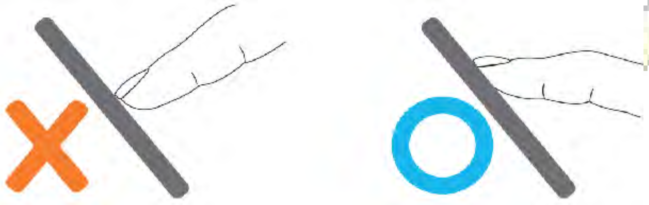
Enroll Face

118

Enrolled successfully

1.5 Touch Screen

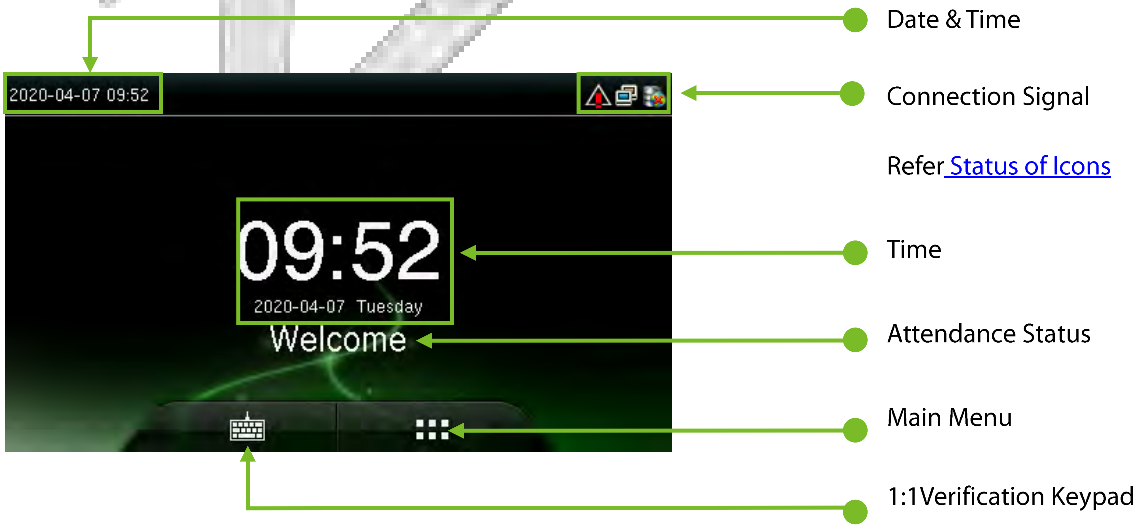
You may tap the touch screen or tap and slide it using the finger pulp. Taping the screen with fingertips or fingernails may damage the touchscreen resulting in performance degradation.



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 Home Screen

When the device is turned ON, press the power switch on the left side of the device and wait for a minute. The Home Screen will be displayed as shown below:



2020-04-07 09:52

09:52

2020-04-07 Tuesday

Welcome

Date & Time

Connection Signal

Refer Status of Icons

Time

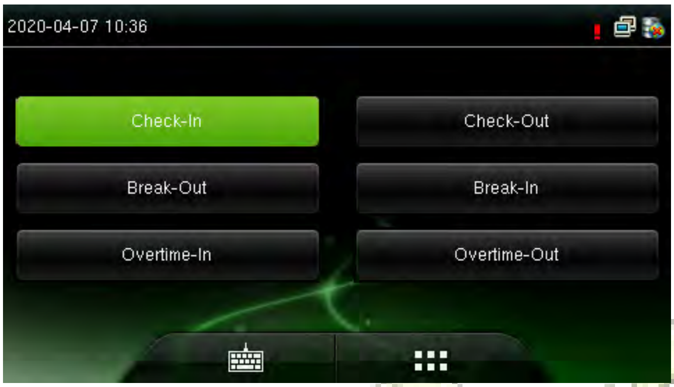
Attendance Status

Main Menu

1:1Verification Keypad

Note:

- The Attendance Status includes 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 the corresponding shortcut key to select the current attendance status, which is displayed in green. For details, refer Shortcut Key Settings.

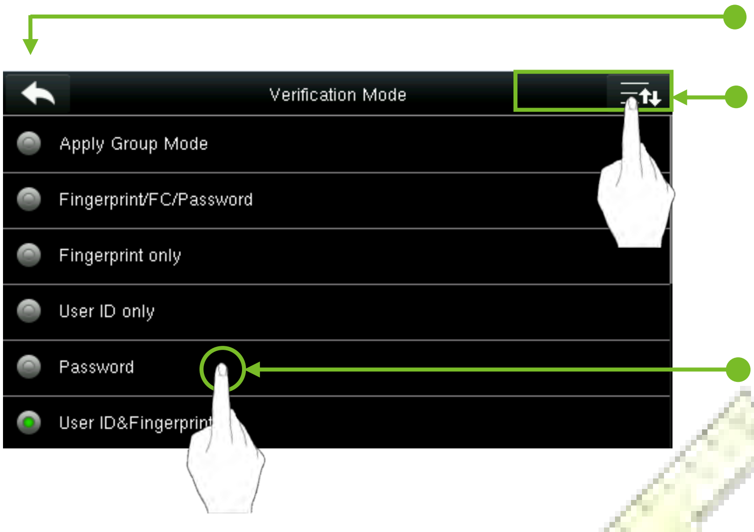
- Tap ▦ to open the main menu interface, Admin verification is required when admin is registered.
- Tap ⌨ to open the interface of 1:1 verification mode and enter the User ID. For details, refer Verification Mode.

1.7 Status Icons

Status Icon	Name	Description
G	Mobile signal	The status icons indicate whether you are within the coverage of the cellular mobile network, the green bars indicate the strength of the signal. **G:** Indicates that the current mobile network is GPRS, 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, over which the device accesses the Internet. **H:** Indicates that the current mobile network is HSDPA, over which the device accesses the Internet. **T:** Indicates that the current mobile network is TD-SCDMA, over which the device accesses the Internet. **1X:** Indicates that the current mobile network is CDMA 1X, over which the device accesses the Internet. **3G:** Indicates that the operator's 3G UMTS (GSM) or EV-DO (CDMA) network is available.
E		
W		
H		
T		
1X		
3G		
✗		Indicates that no mobile network is available.
⏰	Bell	Indicates that you have set the bell.
⚠		Indicates a disassembly alarm.
🖧	Ethernet	Indicates that the Ethernet connection has been established.
🖧✗		Indicates that the Ethernet is disconnected.
🌐	ADMS Server	The connection between the device and the ADMS Server is successful.
🌐✗		The connection between the device and the ADMS Server is failed.
⇅		The communication data of ADMS is being transmitted.
✉	Short Messages	Public short messages notification.
📶	Wi-Fi signal	Wi-Fi connection is normal.
📶✗		No Wi-Fi Connection

1.8 Touch Operations

1.8.1 Basic Operations



Return and Save

Page Up and Page Down

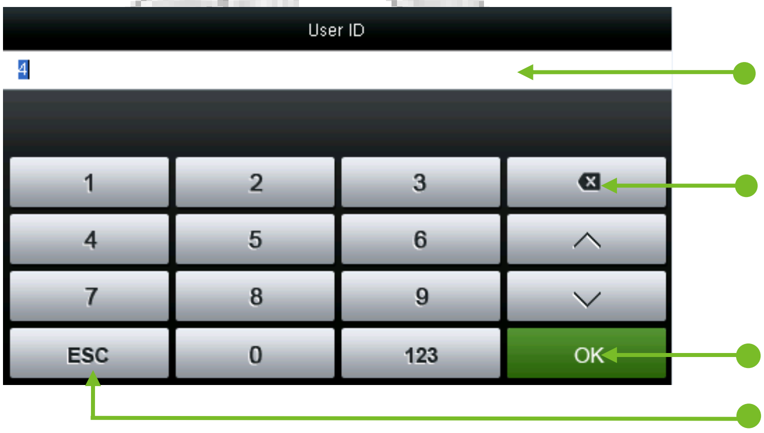
Note: If the list does not have much content, the menu can be completely displayed when you press **Page Down** just once.

You can select an option by taping the same line of menu option.

Note: After registering or modifying the user information or setting the parameters, you need to tap **Return/Save** to save the settings. If time is out 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 Keypad

Numeric Keypad



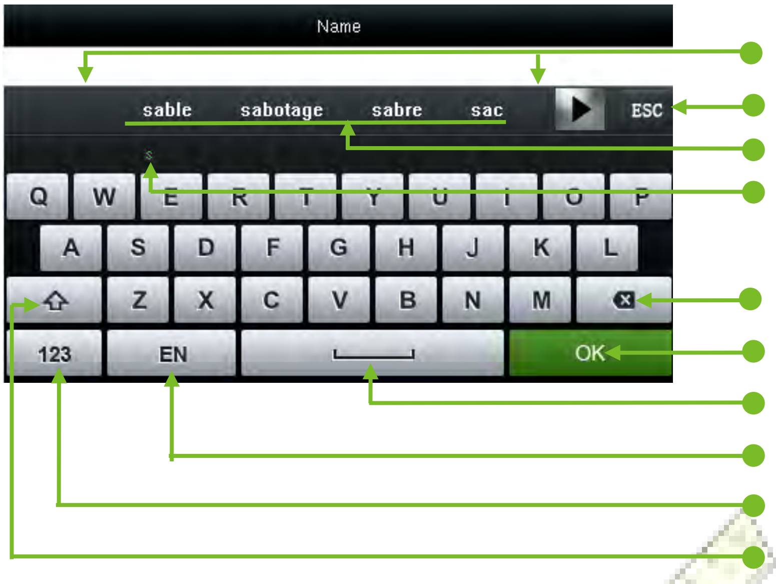
Content display area

Clear previous entry

Confirm the entry

Return key

Alphabetic Keypad



Tap leftwards and rightwards to view the text

Exit keypad

Text suggestion area

Pinyin display area

Clear previous entry

Confirm the entry and return

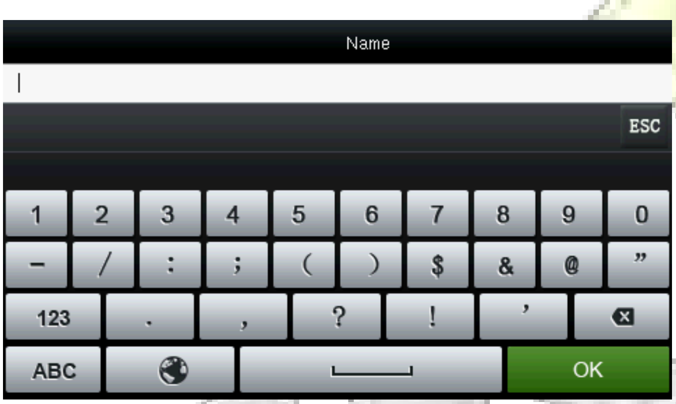
Space key

Tap to switch to the English keypad

Tap to switch to the number and symbol keypad

Tap to switch to the uppercase keypad

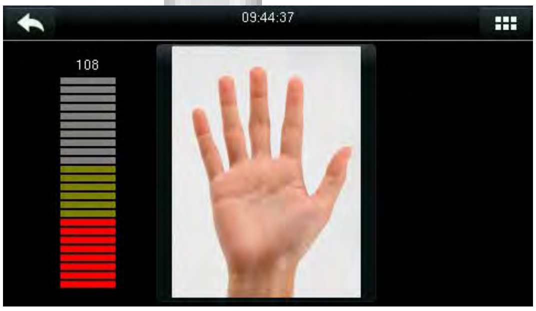
Numeric and Alphabetic Keypad

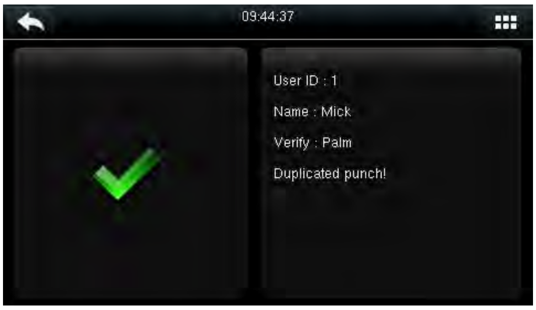


1.9 Verification Modes

1.9.1 Palm Verification

The device compares the current palm with users' registered palm in the device. Please follow the instructions to enroll and verify.





User ID : 1

Name : Mick

Verify : Palm

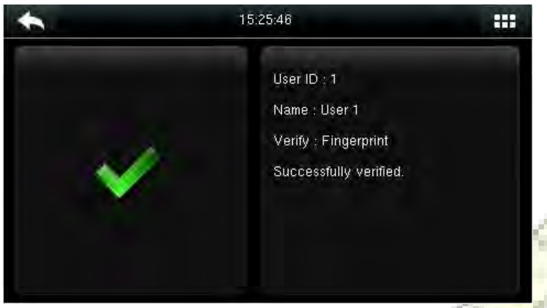
Duplicated punch!

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 registered in the device.

- The device automatically distinguishes between the face and fingerprint verification. Just press your finger on the fingerprint collector/sensor, the device displays the fingerprint authentication screen.
- Please follow the instructions to press your finger on the fingerprint sensor (for detailed instructions, please refer Finger Positioning.

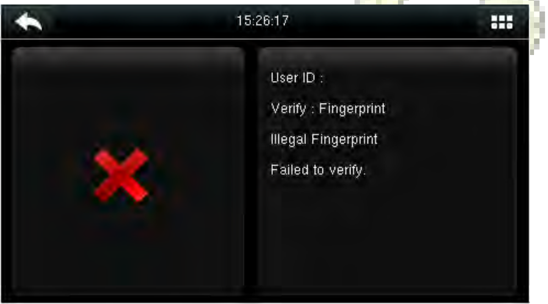


User ID : 1

Name : User 1

Verify : Fingerprint

Successfully verified.



User ID :

Verify : Fingerprint

Illegal Fingerprint

Failed to verify.

Successful Verification

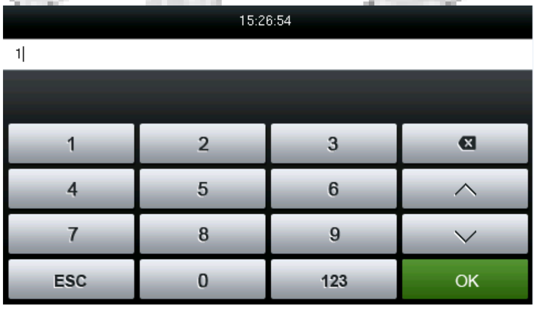
Failed Verification

1:1 Fingerprint Verification

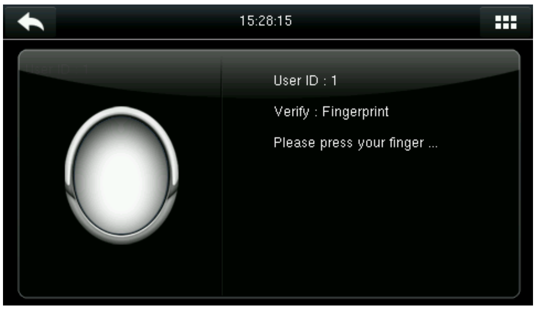
In 1:1 fingerprint verification method, a fingerprint collected by the sensor is verified with the fingerprint corresponding to the entered User ID.

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

- Press ⌨ on the screen to open the 1:1 Verification screen.



1

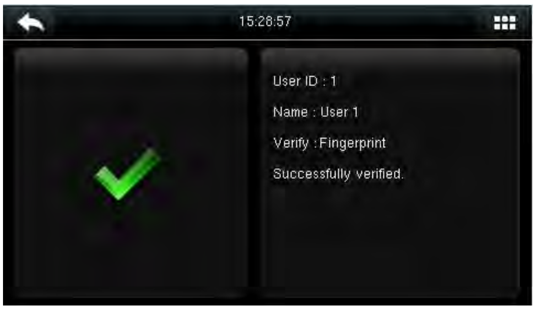


User ID : 1

Verify : Fingerprint

Please press your finger ...

- Enter your ID and tap **[OK]**. Press your fingerprint for verification.



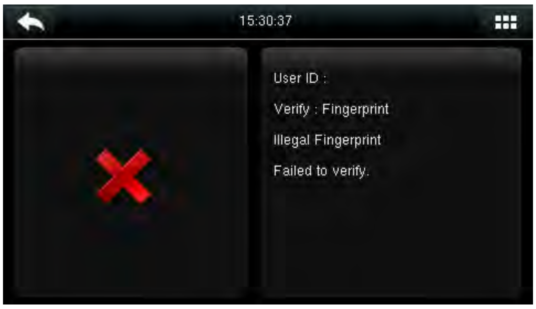
User ID : 1

Name : User 1

Verify :Fingerprint

Successfully verified.

Successful Verification



User ID :

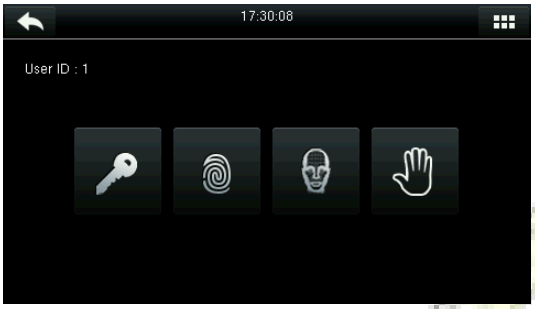
Verify : Fingerprint

Illegal Fingerprint

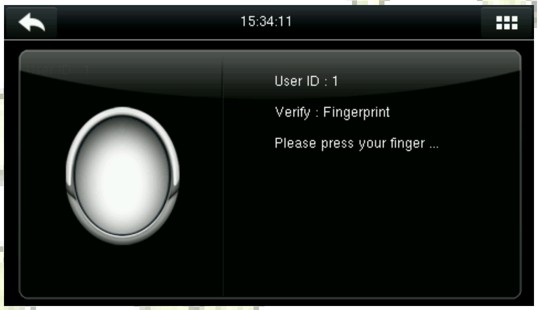
Failed to verify.

Failed Verification

- If you have registered multiple verification modes, the following interface appears after you enter your ID.



User ID : 1



User ID : 1

Verify : Fingerprint

Please press your finger ...

Tap the Fingerprint icon to access the fingerprint verification interface. Press your finger on the fingerprint scanner to scan your fingerprint for verification. The result will be displayed as shown above.

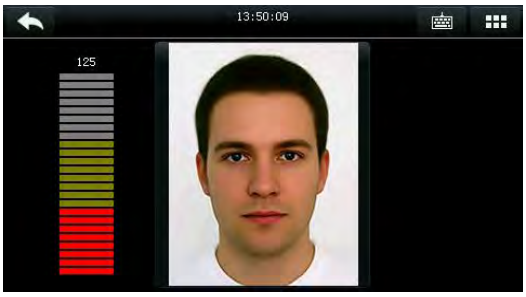
Note: If you have registered only your fingerprint, you can access the fingerprint verification interface directly after entering your ID. If you have registered multiple verification modes, the icons of the registered verification modes are displayed, as shown in the above figure with Password, Fingerprint,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

1.9.3 Facial Verification

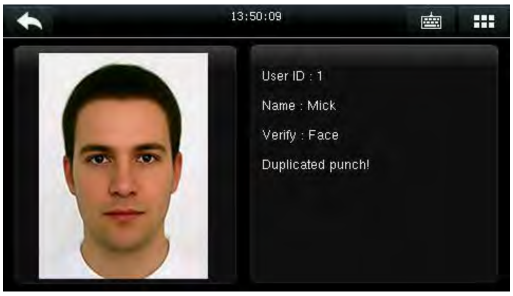
1:N Facial Verification

In 1:N Facial Verification method, the facial image captured by the camera is compared with all the facial data in the device.

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



Face Comparison



User ID : 1
Name : Mick
Verify : Face
Duplicated punch!

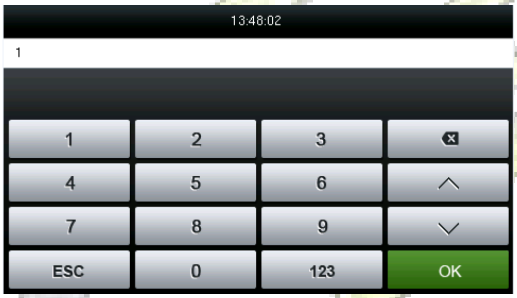
Successful Verification

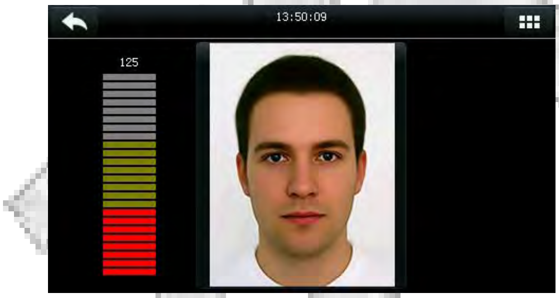
1:1 Facial Verification

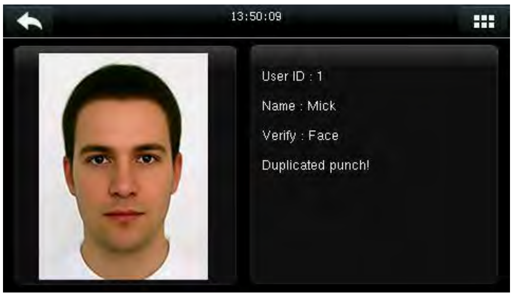
In 1:1 Facial Verification method, the captured facial image is compared with the facial image associated with the entered user ID.

Note: If the device prompts **"No data registered"**, then the user corresponding to this ID does not exist.

- Enter the User ID and press [OK].





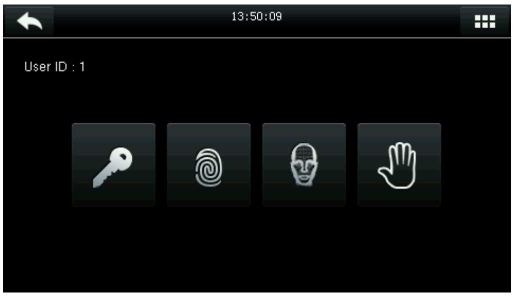


User ID : 1
Name : Mick
Verify : Face
Duplicated punch!

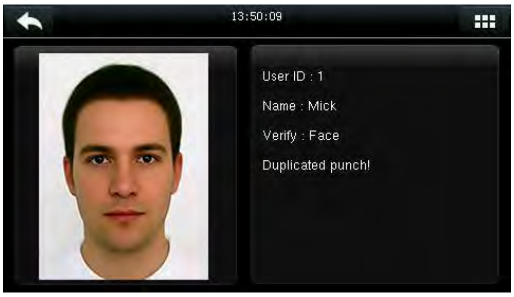
Face Verification Successful Verification

If the verification fails consecutively for 20 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**.


13:50:09

User ID : 1


13:50:09

User ID : 1

Name : Mick

Verify : Face

Duplicated punch!

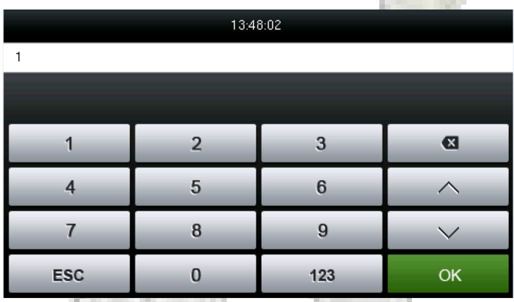
Tap the **Face** icon and the verification result will be displayed as shown above.

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

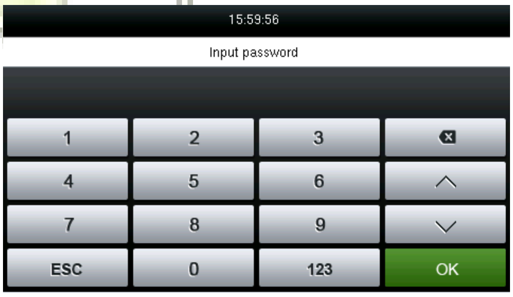
1.9.4 Password Verification

In the Password verification method, the entered password is verified with the registered password of the entered user ID.

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

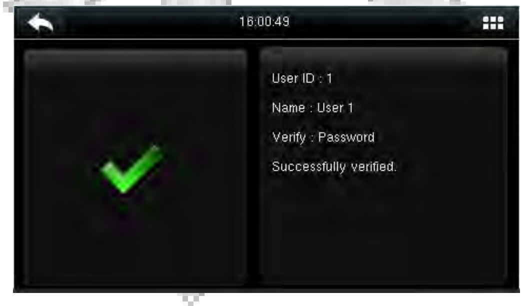

13:48:02

1


15:59:56

Input password

- Enter the user ID and press **OK**. In the next interface, enter the password and press **OK**


16:00:49

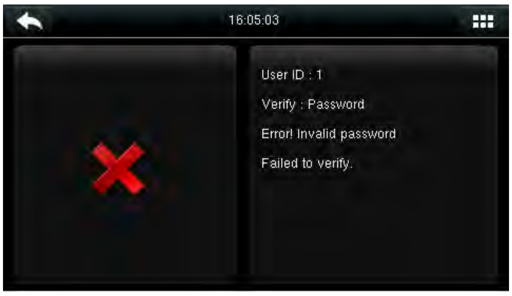
User ID : 1

Name : User 1

Verify : Password

Successfully verified.

Successful Verification


16:05:03

User ID : 1

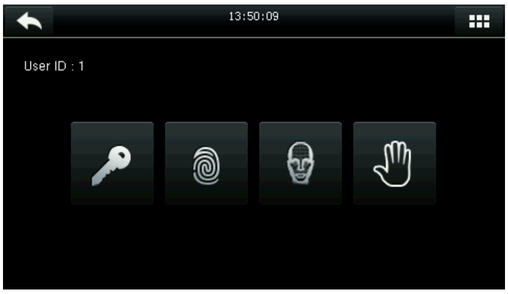
Verify : Password

Error! Invalid password

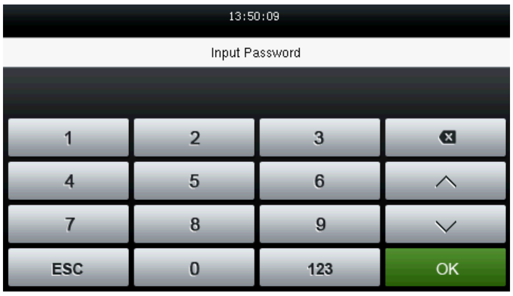
Failed to verify.

Failed Verification

- If you have registered multiple verification modes, the following interface appears after you enter your ID and tap **OK**.
- Tap the Key icon and enter your password.


13:50:09

User ID : 1


13:50:09

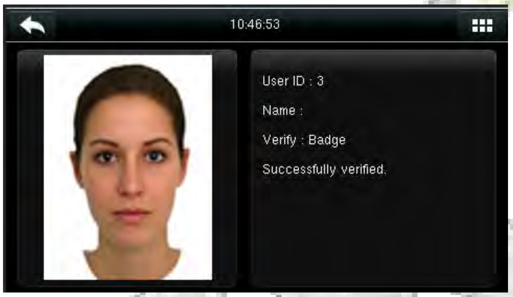
Input Password

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

1.9.5 Card Verification★

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

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


10:46:53

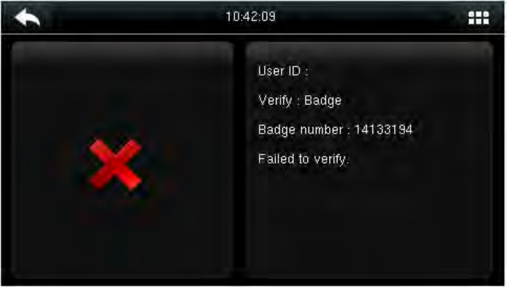
User ID : 3

Name :

Verify : Badge

Successfully verified.

Successful Verification


10:42:09

User ID :

Verify : Badge

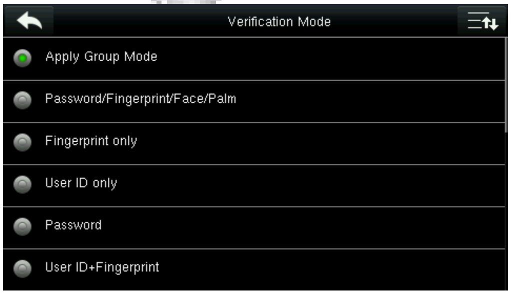
Badge number : 14133194

Failed to verify.

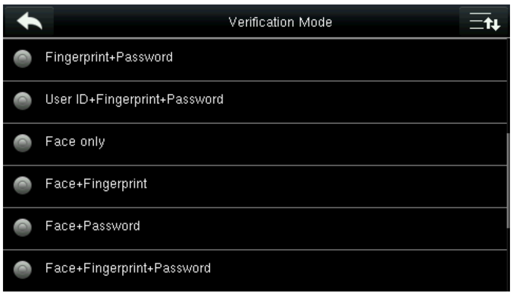
Card is not registered

1.9.6 Combined Verification

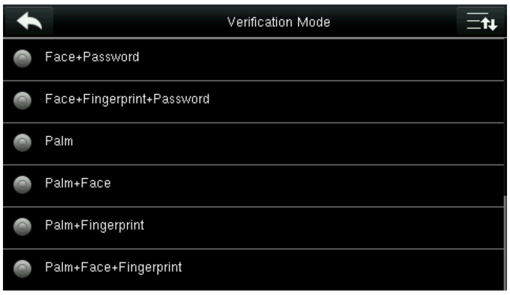
To meet the needs of some access control requirements with high security and considering the diversity of access control, the device provides a wide range of verification modes, which can be combined as required for individual users and user groups. The device supports 15 combinations of verification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


Verification Mode

- ● Apply Group Mode
- ○ Password/Fingerprint/Face/Palm
- ○ Fingerprint only
- ○ User ID only
- ○ Password
- ○ User ID+Fingerprint


Verification Mode

- ○ Fingerprint+Password
- ○ User ID+Fingerprint+Password
- ○ Face only
- ○ Face+Fingerprint
- ○ Face+Password
- ○ Face+Fingerprint+Password


Verification Mode

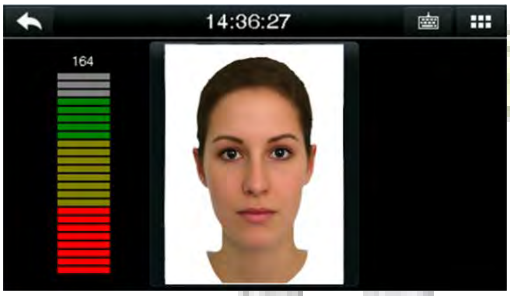
- Face+Password
- Face+Fingerprint+Password
- Palm
- Palm+Face
- Palm+Fingerprint
- Palm+Face+Fingerprint

Note: "/" means OR, and "&" means AND.

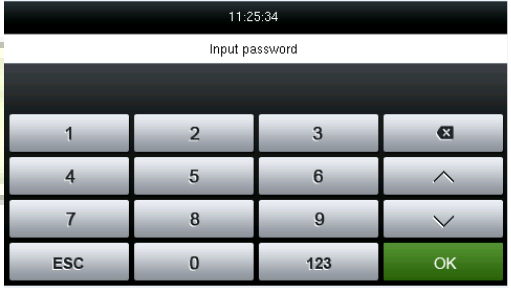
In the combined verification mode, you must register the required verification information, otherwise, the verification may fail. For example, if a user uses **Fingerprint Registration** but the verification mode is **PW**, this user will never succeed verification.

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

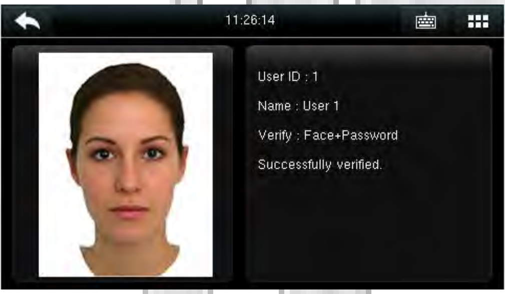
Place your face within the capture area of the camera, and the device automatically performs face verification.



1.Face Verification

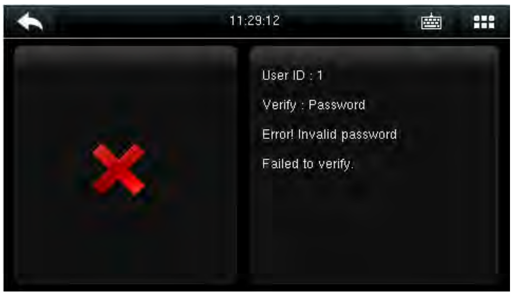


2. Password Verification


11:26:14

User ID : 1
Name : User 1
Verify : Face+Password
Successfully verified.

3. Successful Face Verification


11:29:12

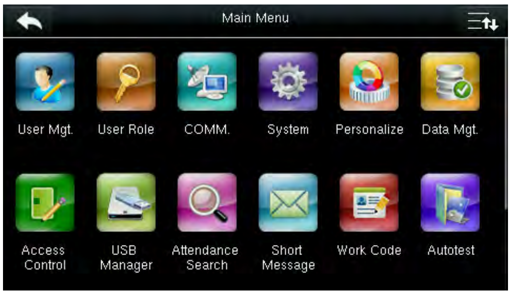
User ID : 1
Verify : Password
Error! Invalid password
Failed to verify.

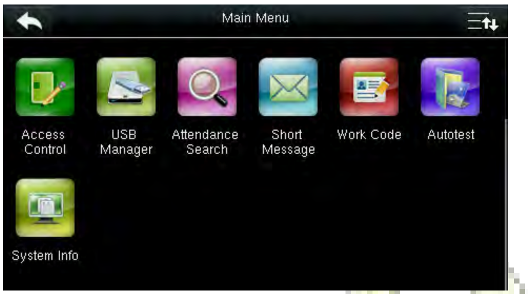
4. Failed Password Verification.

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

2. Main Menu

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





Menu	Description
User Mgt.	To manage the basic information of the registered users, including User ID, Name, User Role, Palm, Fingerprint, Face, Badge★ (HID and MiFare cards are optional), Password, User Photo, and Access Control Role.
User Role	To set the user roles for accessing the menu and change settings.
Comm.	To set the related communication parameters between the device and PC, including Ethernet parameters such as IP address, Serial Comm, PC connection, Wi-Fi★, Cloud Server, and Wiegand settings.
System	To set the related parameters of the system and Firmware upgradation, including setting the 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 the data including attendance data, admin role, screen savers, etc.
Access Control	To set 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, checking attendance photos, and blacklist photos.
Short Message	To set public or private short messages, which are read by specified users within the specified time after attendance verification, facilitating information transmission.
Work Code	To mark different work categories, facilitating user attendance verification

Autotest	To automatically test different module's functions, including LCD, Voice, Keyboard, Fingerprint Sensor, Face, and Clock RTC.
System Info	To check the device capacity, device information, and firmware information.

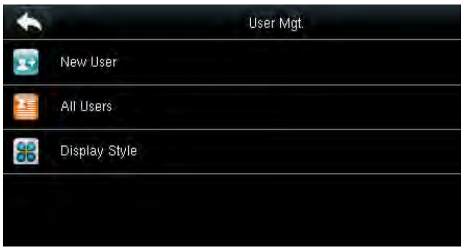
Note: After registering or modifying the user information or setting parameters, you need to tap **Return/Save** to save the settings. If the time is out or no operations are performed on the interface, the system returns to the main interface without saving registration, user information modification,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

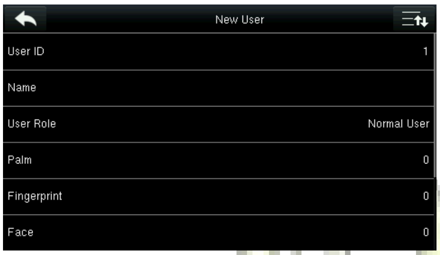
If no Super administrator is registered, anyone can access the menu by pressing ▦. After an administrator is set, identity authentication is required for menu access. A user can access the menu only after successful identity authentication. To improve security, it is recommended to register an administrator when the device is used for the first time. For other details, refer Setting a User Role.

3. User Management

3.1 Add a User

Tap **New User** on the main menu interface and tap **Page Down** to view other options.



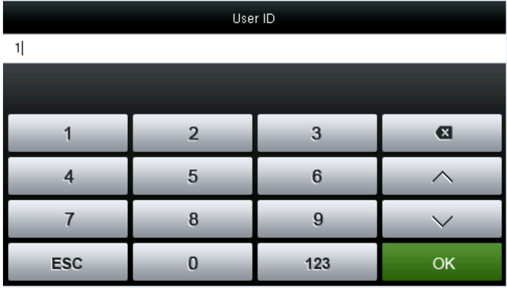


User ID 1
Name
User Role Normal User
Palm 0
Fingerprint 0
Face 0

3.2 Enter a User ID

The device automatically assigns User ID's for users, starting from 1. The User ID can also be entered manually.

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



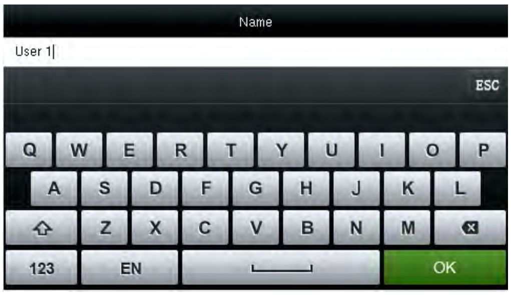
Note:

1. By default, a User ID contains 1 to 9 digits. To extend the length, contact our pre-sales technician.
2. During the initial registration, you can modify your ID, which cannot be modified after registration.
3. If "ID Already Exists" is prompted, it means the ID has been used already. In that case, please try a different ID.

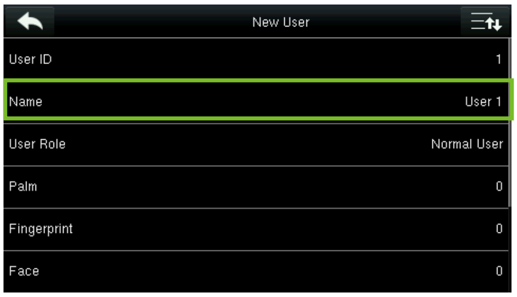
3.3 Enter a Username

The procedure to enter a Username is given below:

- Select **User Role**
- Enter the name and tap OK to save and exit.



Name: User 1



User ID 1
Name User 1
User Role Normal User
Palm 0
Fingerprint 0
Face 0

Note: By default, a username contains 1 to 12 characters. For details, refer 1.8.2 Soft Keypad.

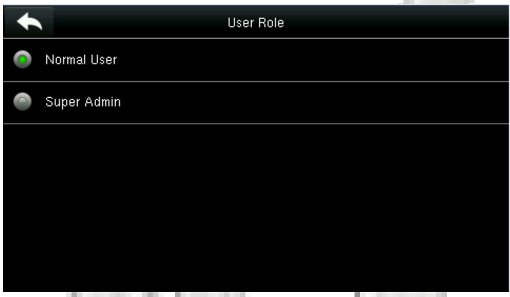
3.4 Set a User Role

There are two types of roles granted to two types of users namely User and Administrator.

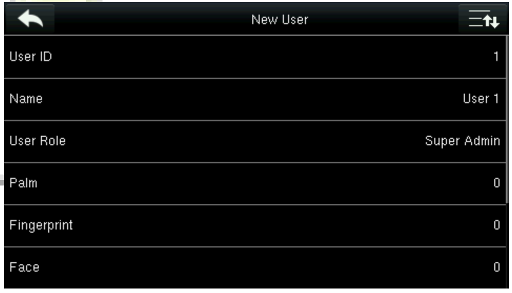
Users are only granted the rights of facial, fingerprint, or password verification.

Administrators are granted access to the main menu for various operations apart from having all the privileges granted to the user.

- Tap **User Role** and select a User role.
- If the selected user role is Super Admin, then identity authentication is required for main menu access. The authentication process depends on the authentication mode that the super administrator has registered.

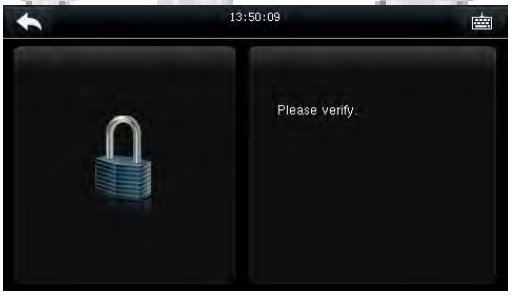


● Normal User
○ Super Admin

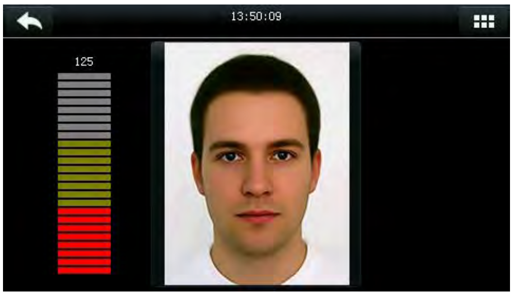


User ID 1
Name User 1
User Role Super Admin
Palm 0
Fingerprint 0
Face 0

The following is an example of accessing the main menu as the Super Admin by face authentication.



Please verify.

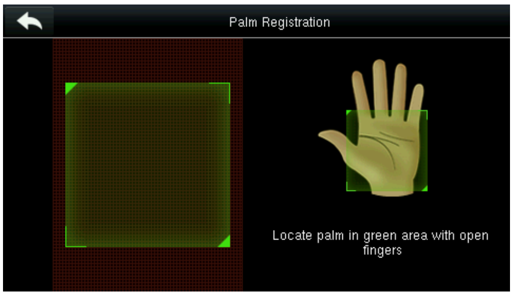


- Press ▦ on the main interface and face the camera for authentication. You can access the main menu interface directly after authentication.

3.5 Register a Palm

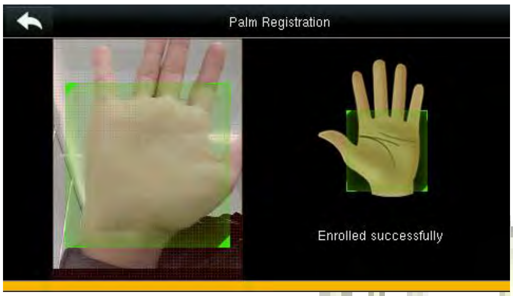
The procedure to register a palm is given below:

- Select **Palm** on the New User interface. Follow the voice and interface prompts to move back and forth to place your palm within the green frame.



Palm Registration

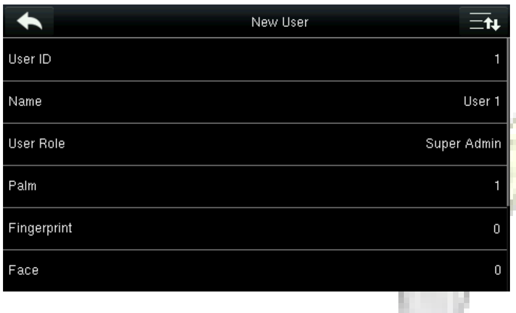
Locate palm in green area with open fingers



Palm Registration

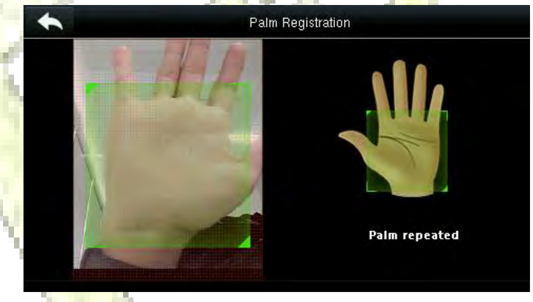
Enrolled successfully

- The palm registration success message will be displayed as shown above and the system returns to the new user interface.



New User

User ID	1
Name	User 1
User Role	Super Admin
Palm	1
Fingerprint	0
Face	0



Palm Registration

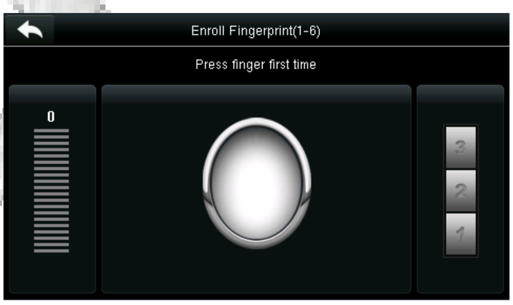
Palm repeated

- If a duplicate palm is registered, the system prompts **"Palm repeated"**

3.6 Register a Fingerprint

The procedure to register a Fingerprint is given below:

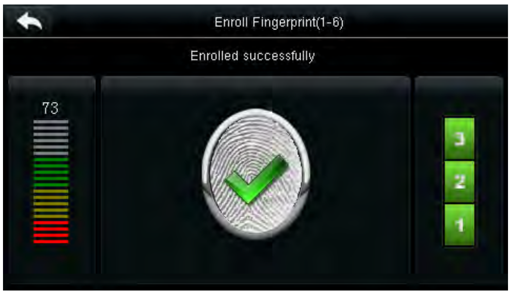
- Select **Fingerprint** on the **New User** interface.



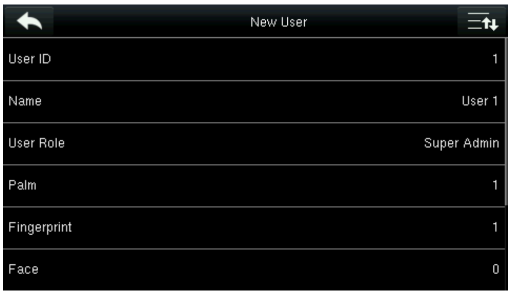
Enroll Fingerprint(1-6)

Press finger first time

- Select a finger for fingerprint registration.
- Press the same finger onto the fingerprint scanner consecutively until the success message appears as shown below:

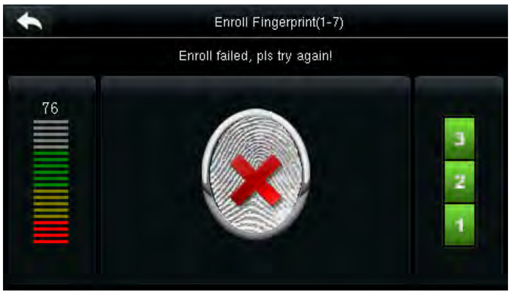

Enroll Fingerprint(1-6)

Enrolled successfully


New User

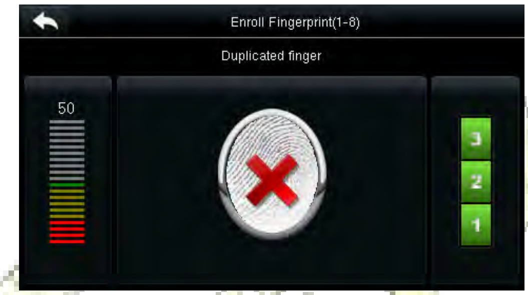
User ID	1
Name	User 1
User Role	Super Admin
Palm	1
Fingerprint	1
Face	0

- If the fingerprint registration fails, the following prompt appears.


Enroll Fingerprint(1-7)

Enroll failed, pls try again!

Fingerprint registration failed


Enroll Fingerprint(1-8)

Duplicated finger

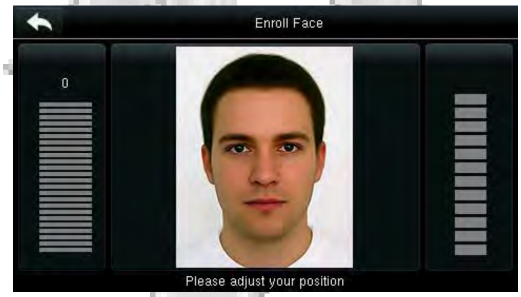
Fingerprint already registered

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**.

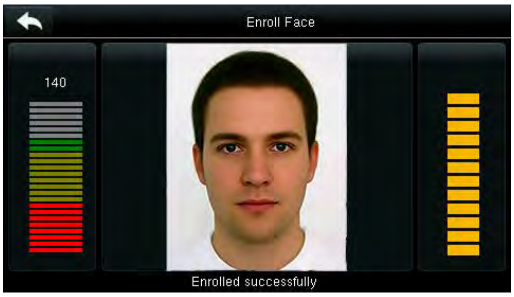
3.7 Register a Face

The procedure to register a face is given below:

- Select **Face** on the New User interface.
- Follow the voice and interface prompts to move back and forth to place your face within the green frame.

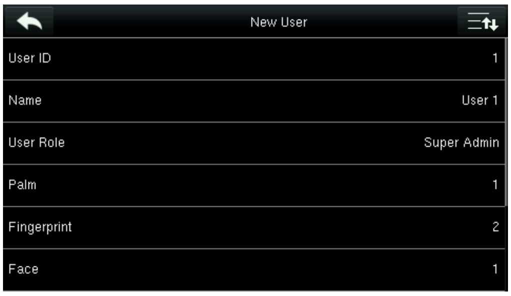

Enroll Face

Please adjust your position


Enroll Face

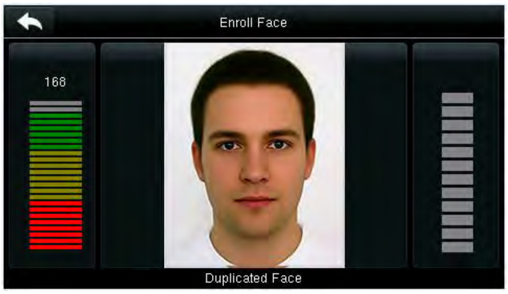
Enrolled successfully

- After successful registration, the system automatically returns to the **New User** interface.
- If the face has been already registered, the system prompts **"Duplicated Face"** as shown below:



New User

User ID	1
Name	User 1
User Role	Super Admin
Palm	1
Fingerprint	2
Face	1



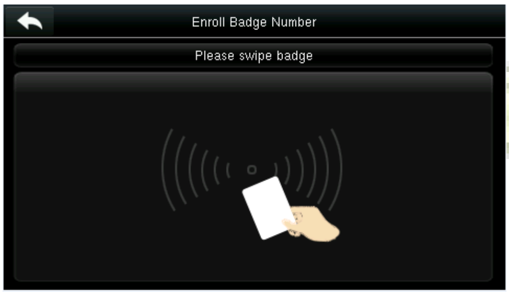
Enroll Face

Duplicated Face

3.8 Register a Badge Number★

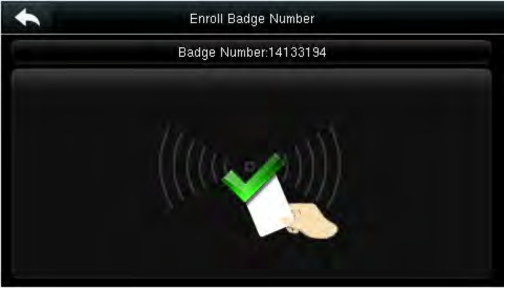
The procedure to register a Badge Number is given below:

- Select **Badge Number** on the New User interface.
- Place your badge underneath the fingerprint sensor.



Enroll Badge Number

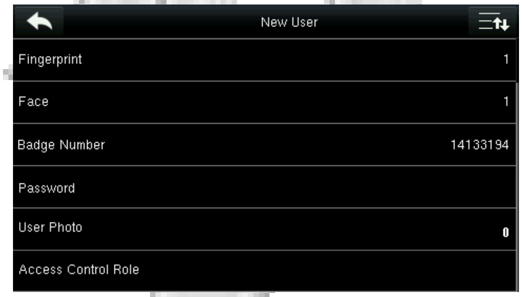
Please swipe badge



Enroll Badge Number

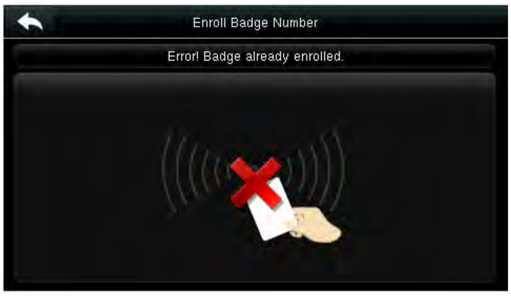
Badge Number:14133194

- After successful registration, the system automatically returns to the **New User** interface.
- If the badge has been already registered, the system prompts "Error! Badge already enrolled" as shown below:



New User

Fingerprint	1
Face	1
Badge Number	14133194
Password	
User Photo	0
Access Control Role	



Enroll Badge Number

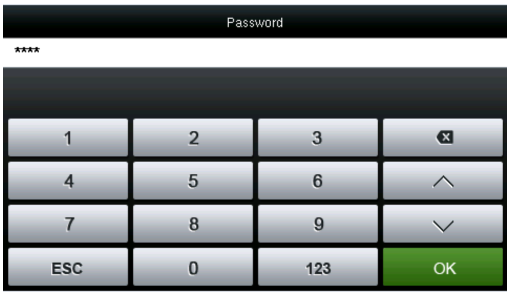
Error! Badge already enrolled.

3.9 Register a Password

The procedure to register a Password is given below:

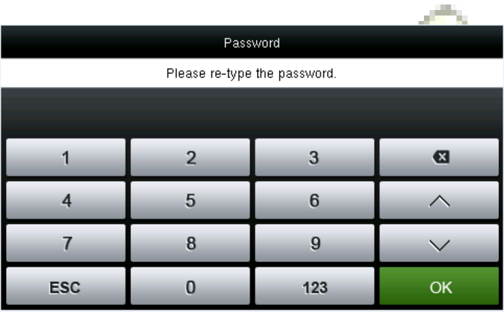
- Select **Password** on the New User interface.
- Enter your Password and tap **OK**. Re-enter your password on the next interface and tap **OK.**

The password may contain 1 to 8 digits.



Password

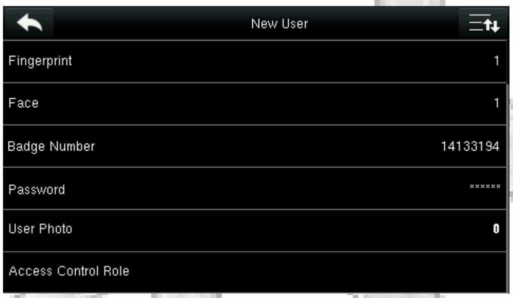
****



Password

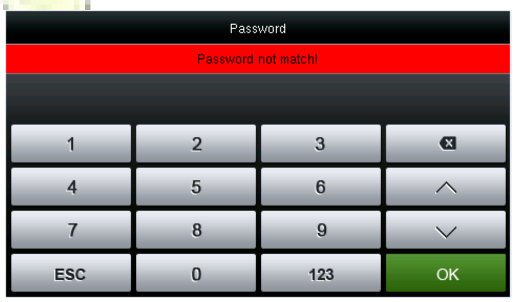
Please re-type the password.

- After successful registration, the system automatically returns to the **New User** interface.
- If the two entered passwords are different, the system prompts "Password not match" as shown below:



New User

Fingerprint	1
Face	1
Badge Number	14133194
Password	******
User Photo	0
Access Control Role	



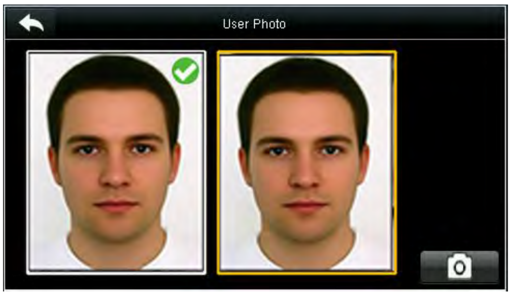
Password

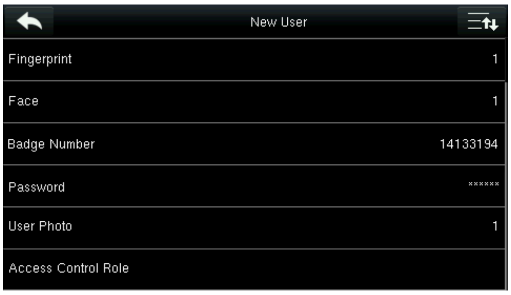
Password not match!

3.10 Registering a Photo

When a user with a registered photo is verified successfully, the registered user photo is displayed.

- Select **User Photo** on the New User interface.
- Tap the Camera icon to capture the photo.




New User

Fingerprint	1
Face	1
Badge Number	14133194
Password	******
User Photo	1
Access Control Role	

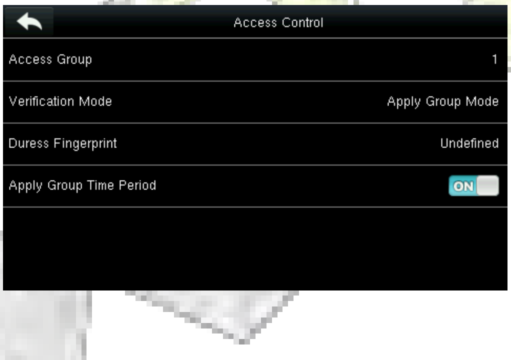
- After capturing the photo, the system automatically returns to the **New User** interface.

Note: After the 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 as a default one.

3.11 Set the Access Control Rights

You can configure a group to which the 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 new users.

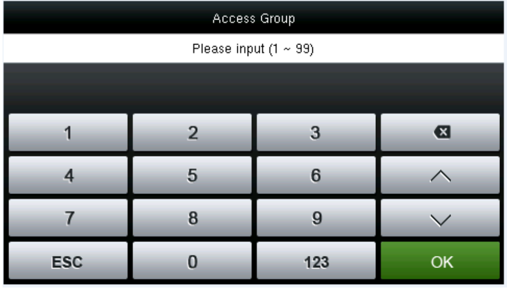
- Select **Access Control Role** on the **New User** interface


Access Control

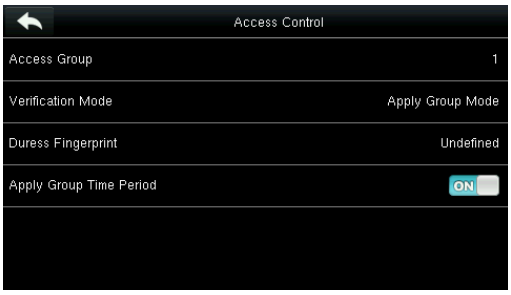
Access Group	1
Verification Mode	Apply Group Mode
Duress Fingerprint	Undefined
Apply Group Time Period	ON

3.11.1 Access Group

- Select **Access Group** on the Access Control interface.
- Then enter the user access group ID. By default, a newly enrolled user belongs to group one.


Access Group

Please input (1 ~ 99)

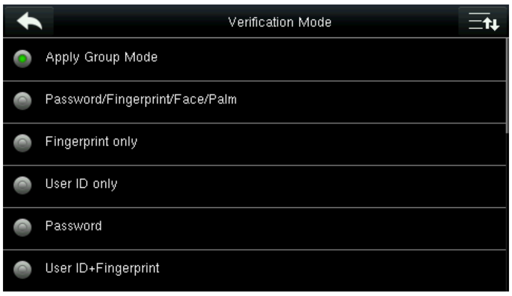

Access Control

Access Group	1
Verification Mode	Apply Group Mode
Duress Fingerprint	Undefined
Apply Group Time Period	ON

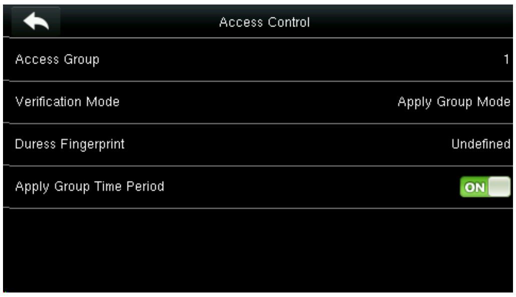
3.11.2 Verification Mode

- Select **Verification Mode** on the Access Control interface.

- Then, select the applicable Verification mode.


Verification Mode

- ● Apply Group Mode
- ○ Password/Fingerprint/Face/Palm
- ○ Fingerprint only
- ○ User ID only
- ○ Password
- ○ User ID+Fingerprint


Access Control

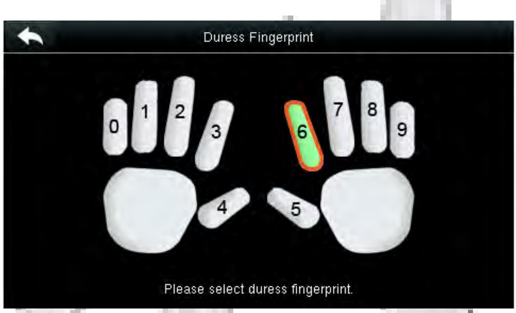
Access Group	1
Verification Mode	Apply Group Mode
Duress Fingerprint	Undefined
Apply Group Time Period	ON

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. For details on group settings, refer 10.4 Access Group Settings.

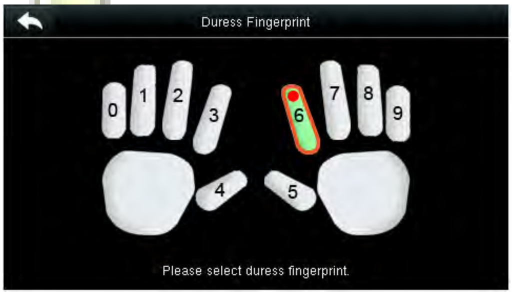
3.11.3 Duress Fingerprint

A Duress fingerprint is registered in the device for emergency purposes. In such cases, a duress alarm will be generated when a fingerprint matches a duress fingerprint. The duress fingerprint cannot be used for normal operations until the duress fingerprint is not deleted in the system.

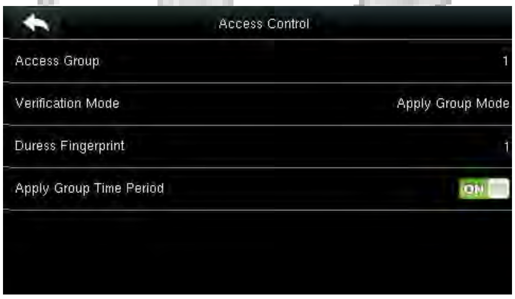
- Select **Duress Fingerprint** on the Access Control interface.
- Select a finger to be registered as a duress fingerprint.
- After successful registration, the system automatically returns the Access Control interface.


Duress Fingerprint

Please select duress fingerprint.


Duress Fingerprint

Please select duress fingerprint.


Access Control

Access Group	1
Verification Mode	Apply Group Mode
Duress Fingerprint	1
Apply Group Time Period	ON

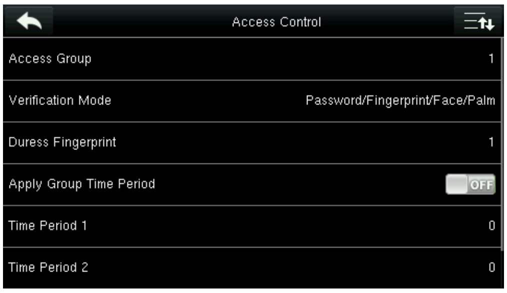
Note:

- The selected duress fingerprint must be a registered fingerprint.
- If you do not want to use a duress fingerprint, open the same menu to edit the user details and cancel the duress fingerprint.

3.11.4 Apply Group Time Period

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

- To set the unlocking time for this user, tap **Apply Group Time Period** > **Time Period 1**.
- Enter the Time Period number and tap **OK.**


Access Control

Access Group 1

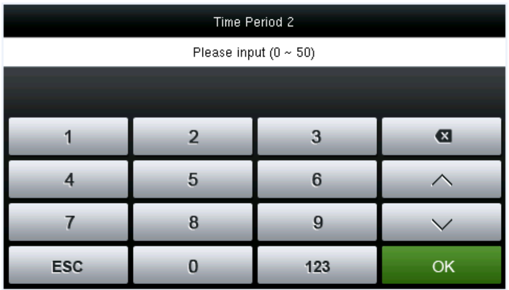
Verification Mode Password/Fingerprint/Face/Palm

Duress Fingerprint 1

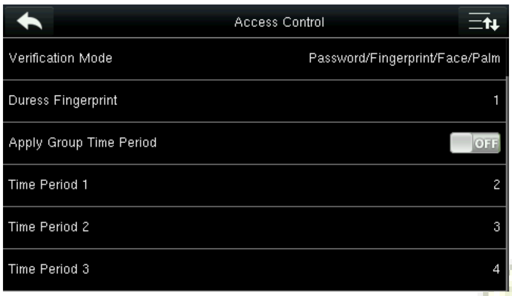
Apply Group Time Period OFF

Time Period 1 0

Time Period 2 0


Time Period 2

Please input (0 ~ 50)


Access Control

Verification Mode Password/Fingerprint/Face/Palm

Duress Fingerprint 1

Apply Group Time Period OFF

Time Period 1 2

Time Period 2 3

Time Period 3 4

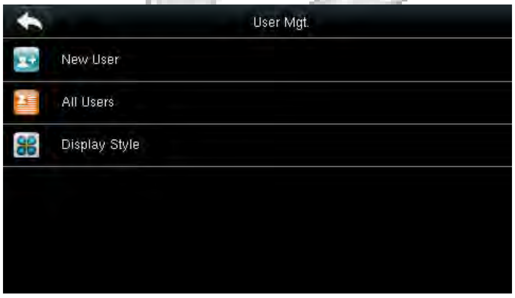
Note: 50 time periods can be set in the device and three time periods can be set for each user. For details, see Time Schedule Settings.

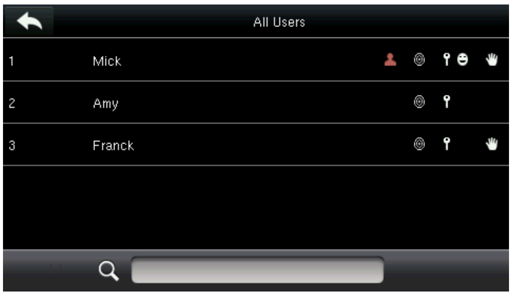
- Select Time Period 2 and 3 in the same way and enter the time period numbers.

Note: 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 will not be saved.

3.12 User List

- Press **User Mgt.** on the main interface.
- All the user's list will be displayed.



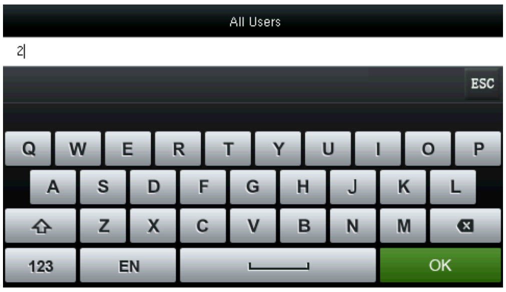

All Users

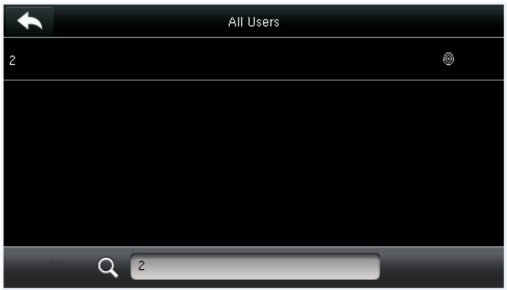
1	Mick	
2	Amy	
3	Franck	

Note: 👤 indicates Super Administrator.

3.12.1 Search a User

- Tap the search bar on the user's list and enter the retrieval keyword.
- The system automatically displays the users related to the entered keyword.

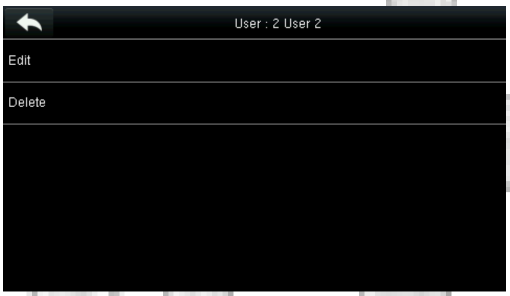


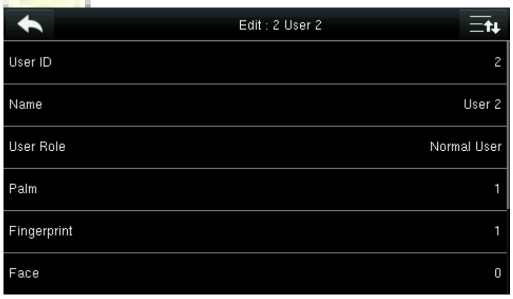


Note: The retrieval keyword can be ID, Surname, or Full name.

3.12.2 Edit a User

- Select a user from the list and tap **Edit**. The **Edit User** interface will be displayed as shown below:




Edit : 2 User 2

User ID 2

Name User 2

User Role Normal User

Palm 1

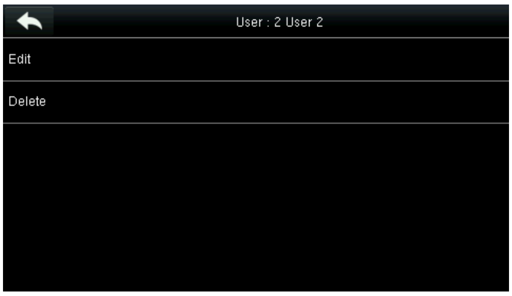
Fingerprint 1

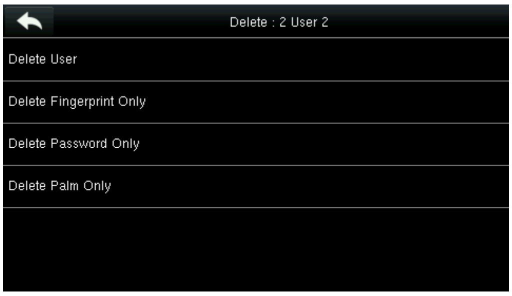
Face 0

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

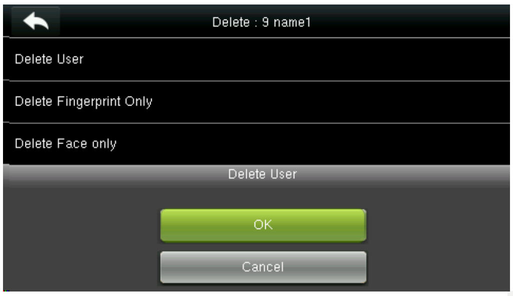
3.12.3 Delete a User

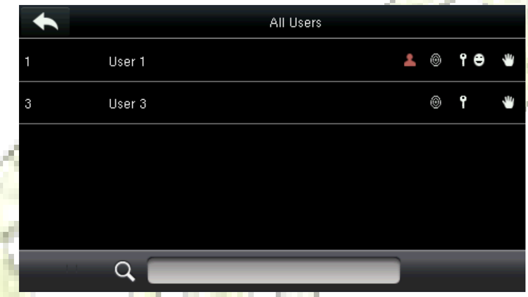
- Select a user from the user's list and tap Delete.
- The Delete User interface will be displayed as shown below:





- Select the User information to be deleted and then tap OK.
- The user information will be deleted and no longer will be displayed in the list.



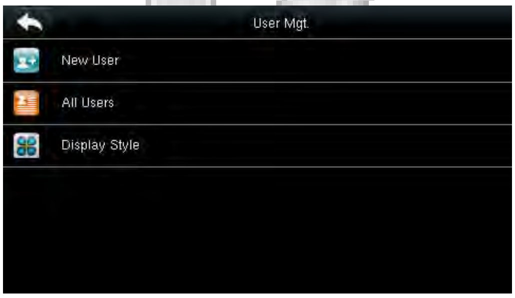


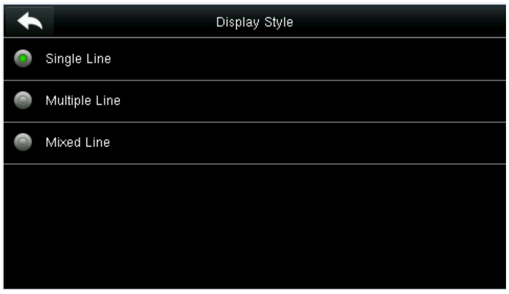
Note:

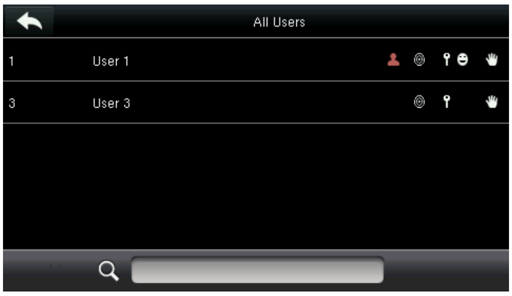
- When deleting a user, you can choose to delete partial information such as the privilege or fingerprint of the user. If you select Delete User, all information of this user is deleted.
- After the privileges of the super administrator are deleted, the super administrator becomes a common user, without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

3.13 User Display Style

- Tap **Display Style** on the **User Mgt.** interface.
- The default style is a single line.





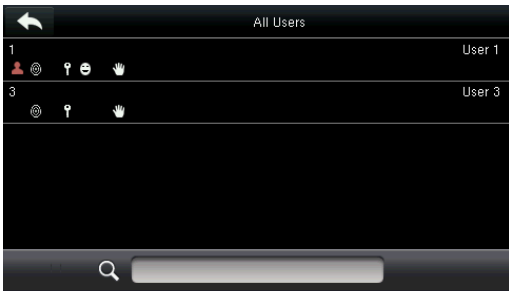


All Users

1 User 1

3 User 3

Single-line Style

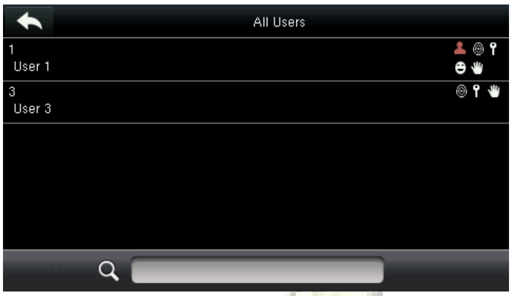


All Users

1 User 1

3 User 3

Multiple-line Style



All Users

1 User 1

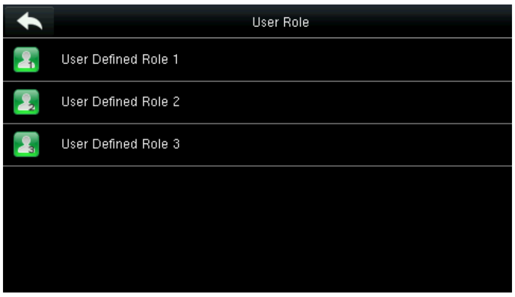
3 User 3

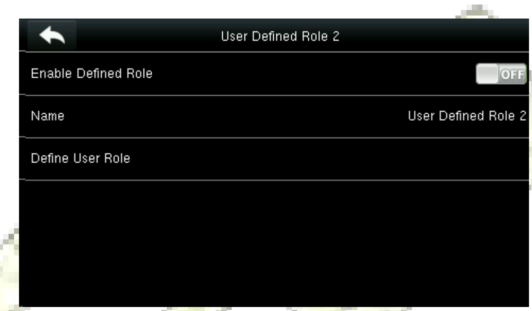
Mixed-line Style

4. User Role

The User-role helps to set the user rights of operating the menu (a maximum of 3 roles can be set).

- Tap **User Role** on the main menu interface.
- Select a User Defined Role.
- Tap **Enable Defined Role** to enable this defined role as shown below:

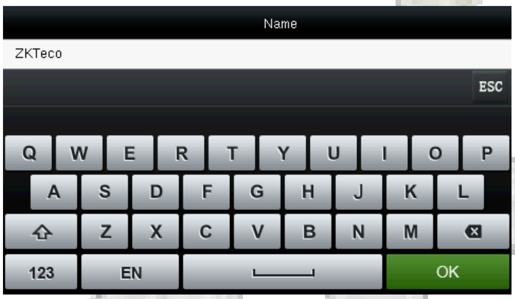




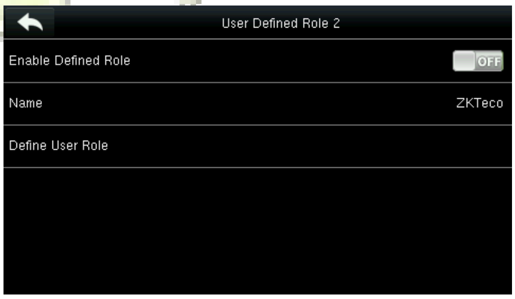
Enable Defined Role: OFF

Name: User Defined Role 2

- Enter the name of the User-defined role.



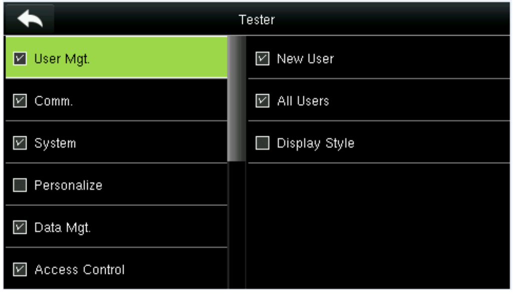
Name: ZKTeco



Enable Defined Role: OFF

Name: ZKTeco

- Return to the previous interface and then tap **Define User Role.**
- Specify the user role and tap **Return** to exit the interface.



☑ User Mgt.

☑ Comm.

☑ System

☐ Personalize

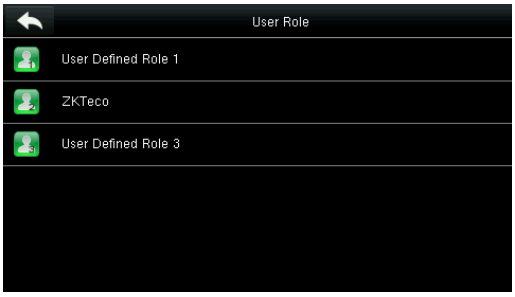
☑ Data Mgt.

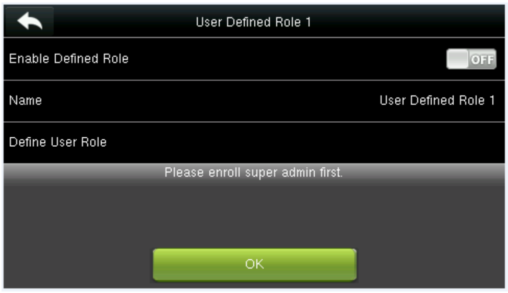
☑ Access Control

☑ New User

☑ All Users

☐ Display Style





User Defined Role 1

Enable Defined Role OFF

Name User Defined Role 1

Define User Role

Please enroll super admin first.

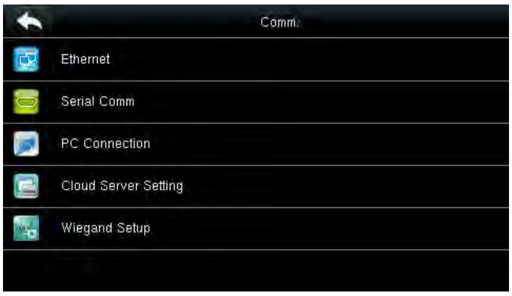
OK

Note: During privilege assignment, the main menu is on the left-side and its sub-menus are on the right-side of the interface. 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**.

5. Comm. Settings

The Communication Settings includes Ethernet parameters such as IP Address, Serial Communication parameters, PC connection, Cloud Server, and Wiegand settings.

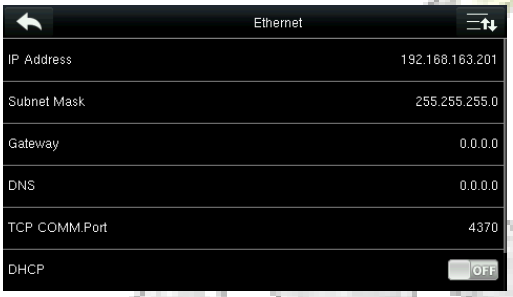
Tap **Comm.** on the main menu interface.



5.1 Ethernet Settings

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

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


Ethernet

IP Address 192.168.163.201

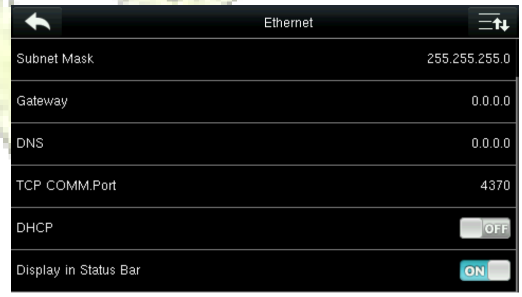
Subnet Mask 255.255.255.0

Gateway 0.0.0.0

DNS 0.0.0.0

TCP COMM.Port 4370

DHCP OFF


Ethernet

Subnet Mask 255.255.255.0

Gateway 0.0.0.0

DNS 0.0.0.0

TCP COMM.Port 4370

DHCP OFF

Display in Status Bar ON

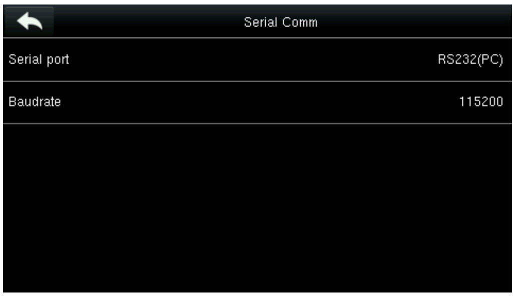
Menu	Description
IP Address	The default value is192.168.1.201, please adjust them according to the actual network parameters.
Subnet Mask	The default value is 255.255.255.0, please adjust them according to the actual network parameters.
Gateway	The default value is 0.0.0.0, please adjust them according to the actual network parameters.
DNS	The default value is 0.0.0.0, please adjust them according to the actual network parameters.
TCP COMM. Port	The default value is 4370, please adjust them according to the actual network parameters.
DHCP	Dynamic Host Configuration Protocol, which is to dynamically allocate the IP addresses for clients via server. If DHCP is enabled, IP addresses cannot be set manually.

Display in Status Bar	To set whether to display the network icon on the status bar.

5.2 Serial Communication. Settings

The Serial Communication Settings enable communication with the device through a serial port (RS232/RS485). You need to configure the serial port settings to achieve this.

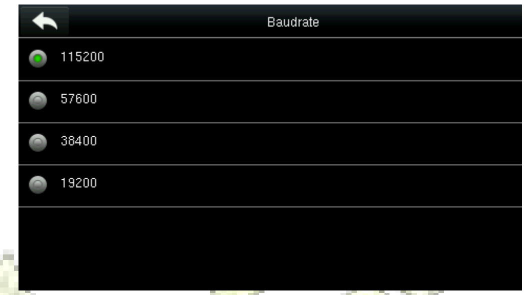
- Tap **Serial Comm** on the **Comm Settings** interface.



Serial Comm

Serial port RS232(PC)

Baudrate 115200



Baudrate

● 115200

○ 57600

○ 38400

○ 19200

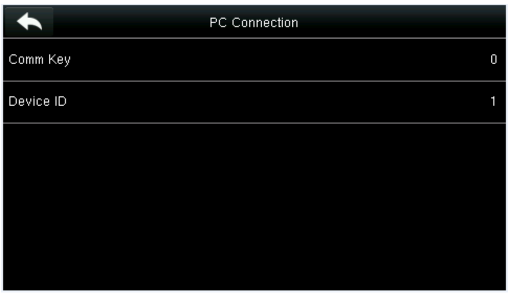
Menu	Description
Serial Port	Includes no usage, RS232(PC), and RS485(PC). Select RS232(PC) to communicate with the device through an RS232 serial port. Select RS485(PC) to communicate with the device through an RS485 serial port.
Baudrate	The rate of communication with PC; there are 5 options of baud rate: 115200 (default), 57600, 38400, 19200 and 9600. The higher the baud rate, the faster the communication speed, but also less reliable. In general, a higher baud rate can be used when the communication distance is short. When the communication distance is long, choose a lower baud rate for reliable communication.

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

5.3 PC Connection

To enable communication between the device and PC, tap **Comm Key**. If the **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.



PC Connection

Comm Key 0

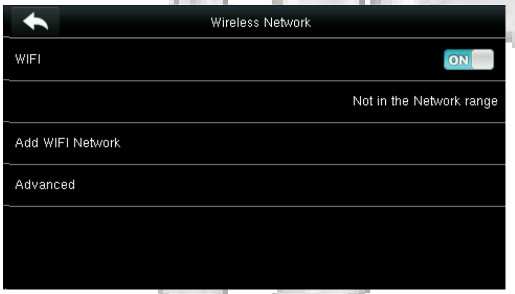
Device ID 1

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

5.4 Wi-Fi Settings★

The device supports a Wi-Fi module, which can be built in the device hardware 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 is not needed, you can tap the ON button to disable Wi-Fi.

- When Wi-Fi is enabled, tap the network to be connected.
- Enter the Password in the password text box and then tap **Connect to Wi-Fi.**



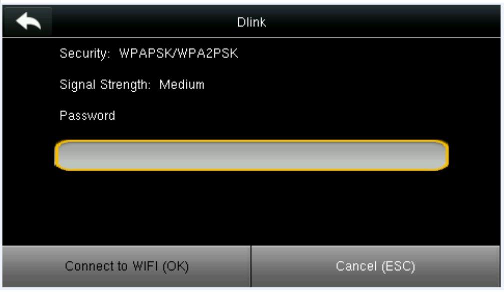
Wireless Network

WIFI ON

Not in the Network range

Add WIFI Network

Advanced



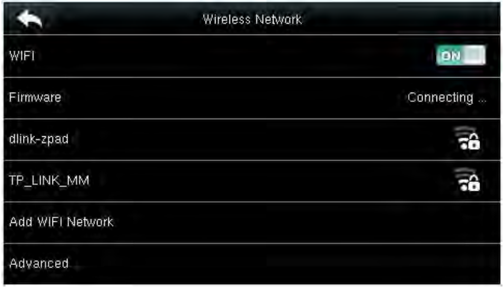
Dlink

Security: WPAPSK/WPA2PSK

Signal Strength: Medium

Password

- After successful verification, the interface will be displayed as shown below



Wireless Network

WIFI ON

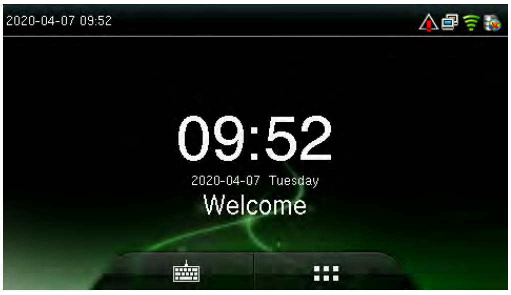
Firmware Connecting ...

dlink-zpad

TP_LINK_MM

Add WIFI Network

Advanced



2020-04-07 09:52

09:52

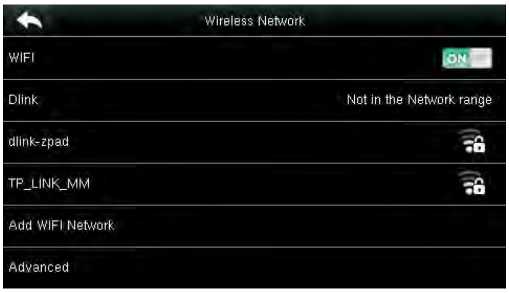
2020-04-07 Tuesday

Welcome

5.4.1 Add a 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 then **Add Wi-Fi Network**
- Enter the parameters of the Wi-Fi network (The added network must exist.)
- After adding, find the added Wi-Fi network in the list and connect to the network as explained above.



Wireless Network

WIFI ON

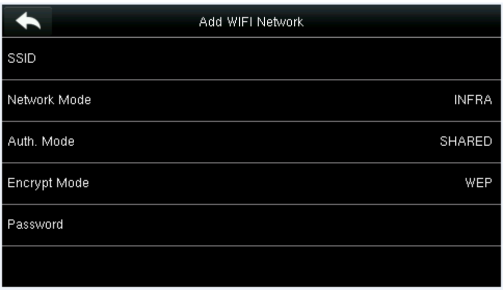
Dlink Not in the Network range

dlink-zpad

TP_LINK_MM

Add WIFI Network

Advanced



Add WIFI Network

SSID

Network Mode INFRA

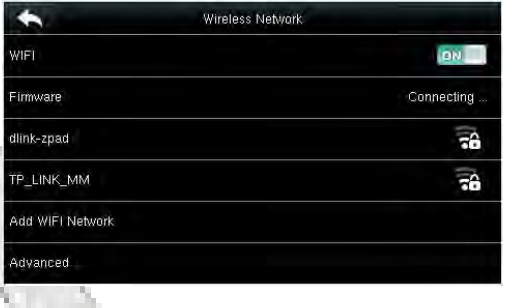
Auth. Mode SHARED

Encrypt Mode WEP

Password

5.4.2 Advanced Options

The advanced options are used to set the Wi-Fi network parameters.



Wireless Network

WIFI ON

Firmware Connecting ...

dlink-zpad

TP_LINK_MM

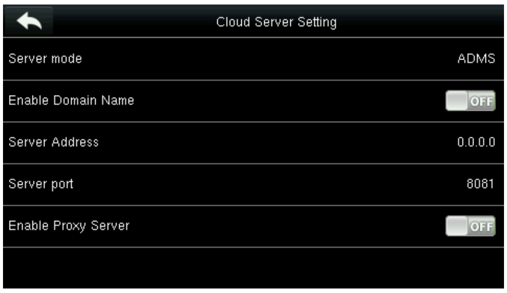
Add WIFI Network

Advanced

Menu	Description
DHCP	Dynamic Host Configuration Protocol, which involves allocating dynamic IP addresses to the 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.

5.5 Cloud Server Settings

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


Cloud Server Setting

Server mode ADMS

Enable Domain Name OFF

Server Address 0.0.0.0

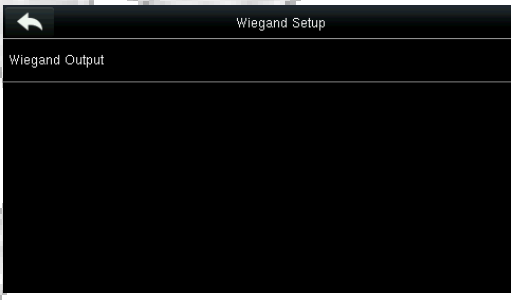
Server port 8081

Enable Proxy Server OFF

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

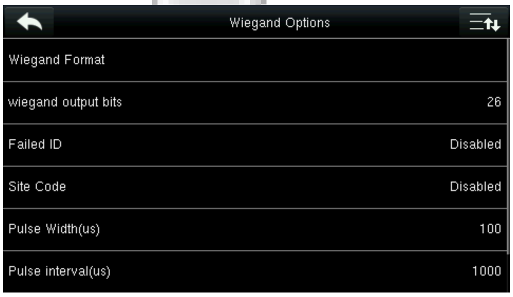
5.6 Wiegand Setup

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


Wiegand Setup

Wiegand Output

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


Wiegand Options

Wiegand Format

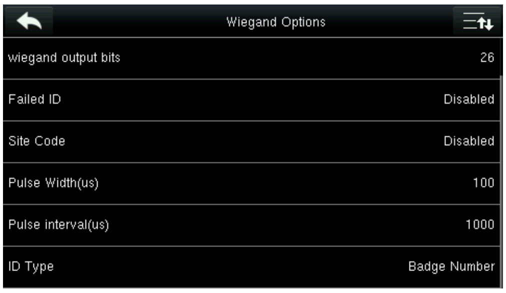
wiegand output bits 26

Failed ID Disabled

Site Code Disabled

Pulse Width(us) 100

Pulse interval(us) 1000


Wiegand Options

wiegand output bits 26

Failed ID Disabled

Site Code Disabled

Pulse Width(us) 100

Pulse interval(us) 1000

ID Type Badge Number

Menu	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 the **Wiegand output bits**.
Wiegand output bits	Number of bits of Wiegand data. After choosing **[Wiegand output bits]**, the device will use the 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 like 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 is the card number.
Wiegand26a	ESSSSSSSSCCCCCCCCCCCCCCCCO Consists of 26 bits of binary code. The 1st bit is the even parity bit of the 2nd to 13th bits, while the 26th bit is the odd parity bit of the 14th to 25th bits. The 2nd to 9th bits is the site code, while the 10th to 25th bits is 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 is 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 is the site code, while the 10th to 25th bits is 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 is the device code, the 18th to 33rd bits are the card number, and the 34th to 35th bits is the manufacturer code.
Wiegand36a	EFFFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCO Consists of 36 bits of binary code. The 1st bit is the even parity bit of the 2nd to 18th bits, while the 36th bit is the odd parity bit of the 19th to 35th bits. The 2nd to 19th bits is the device code, and the 20th to 35th bits is the card number.
Wiegand37	OMMMMSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCE Consists of 37 bits of binary code. The 1st bit is the odd parity bit of the 2nd to 18th bits, while the 37th bit is the even parity bit of the 19th to 36th bits. The 2nd to 4th bits is the manufacturer code, the 5th to 16th bits are the site code, and the 21st to 36th bits is the card number.
Wiegand37a	EMMMFFFFFFFFFFSSSSSSCCCCCCCCCCCCCCCCO Consists of 37 bits of binary code. The 1st bit is the even parity bit of the 2nd to 18th bits, while the 37th bit is the odd parity bit of the 19th to 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 is the card number.
Wiegand50	ESSSSSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO Consists of 50 bits of binary code. The 1st bit is the even parity bit of the 2nd to 25th bits, while the 50th bit is the odd parity bit of the 26th to 49th bits. The 2nd to 17th bits is the site code, and 18th to 49th bits is 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.	

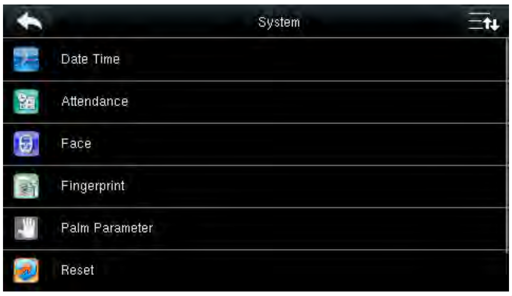
6. System Settings

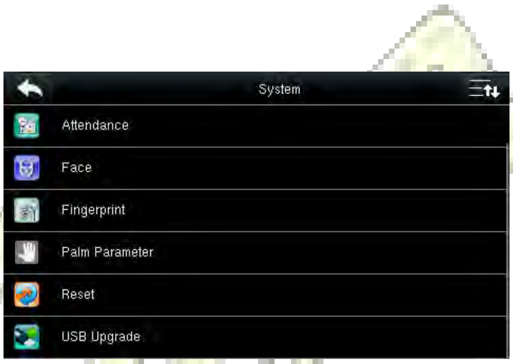
The System Settings define the system parameters to maximize the performance of the device.

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

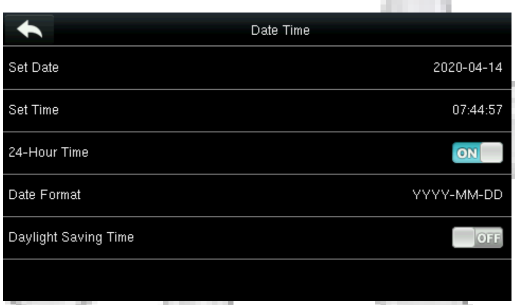
6.1 Date and Time

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



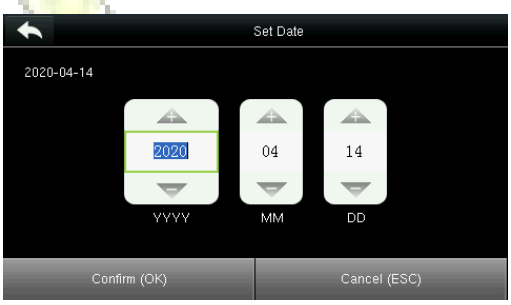


- Press Up and Down arrows to set the year, month, and day.
- Tap **Confirm** to save the date as shown below:



Date Time

Set Date 2020-04-14
Set Time 07:44:57
24-Hour Time ON
Date Format YYYY-MM-DD
Daylight Saving Time OFF

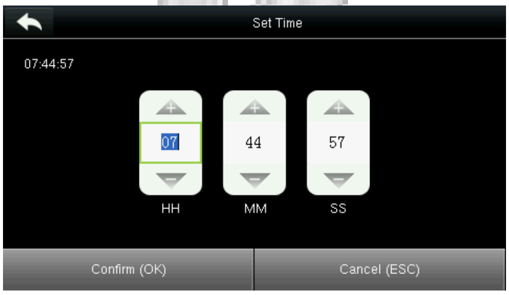


Set Date

2020-04-14

YYYY 2020 MM 04 DD 14

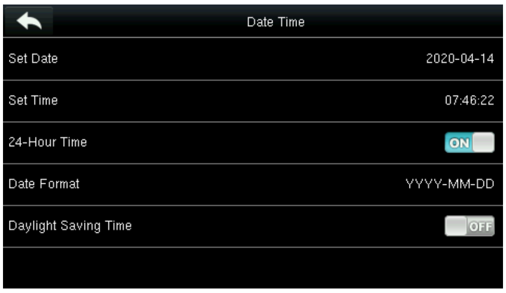
- Tap **Set Time** on the Date Time interface and press **Up** and **Down** arrows to set the hour, minute, and second.



Set Time

07:44:57

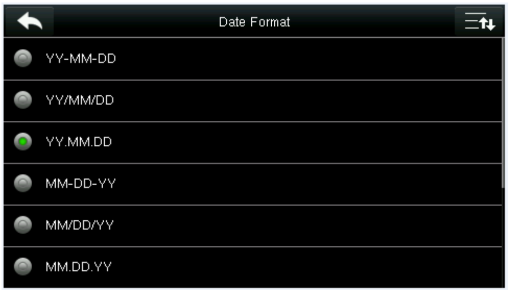
HH 07 MM 44 SS 57



Date Time

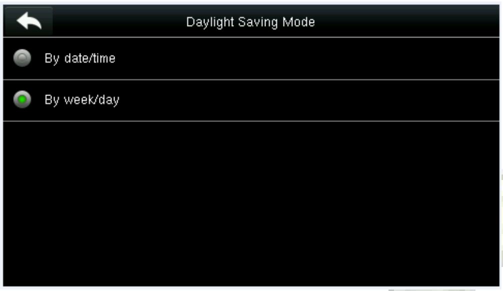
Set Date 2020-04-14
Set Time 07:46:22
24-Hour Time ON
Date Format YYYY-MM-DD
Daylight Saving Time OFF

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

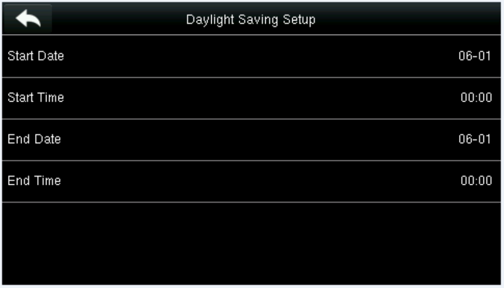

Date Format

○ YY-MM-DD
○ YY/MM/DD
● YY.MM.DD
○ MM-DD-YY
○ MM/DD/YY
○ MM.DD.YY

- Tap **Daylight Saving Time** to choose whether to enable the daylight-saving time.
- Select a daylight-saving mode.
- Set the start and end the daylight-saving time.


Daylight Saving Mode

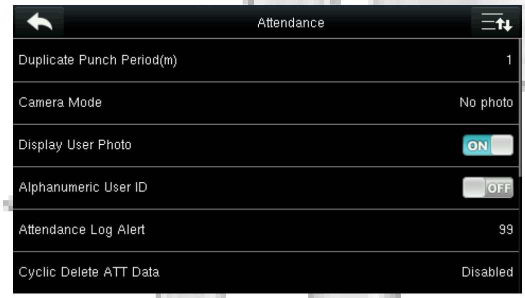
○ By date/time
● By week/day


Daylight Saving Setup

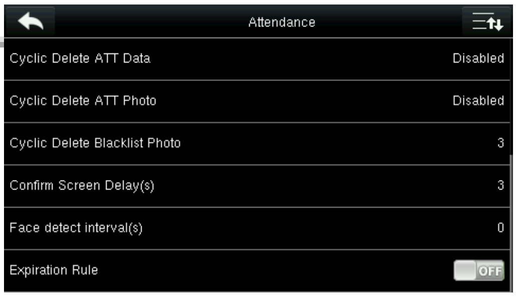
Start Date	06-01
Start Time	00:00
End Date	06-01
End Time	00:00

6.2 Attendance Parameters

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


Attendance

Duplicate Punch Period(m)	1
Camera Mode	No photo
Display User Photo	ON
Alphanumeric User ID	OFF
Attendance Log Alert	99
Cyclic Delete ATT Data	Disabled


Attendance

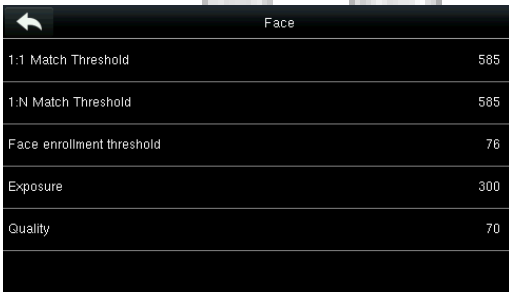
Cyclic Delete ATT Data	Disabled
Cyclic Delete ATT Photo	Disabled
Cyclic Delete Blacklist Photo	3
Confirm Screen Delay(s)	3
Face detect interval(s)	0
Expiration Rule	OFF

Menu	Description
Duplicate Punch Period (m)	Within a set time period (unit: minutes), the repeated attendance logs will not be saved (value ranges from 1 to 999999 minutes).
Camera Mode	To set whether to take and save photos during the verification and it is applicable to all the users. The following 5 modes are applicable: **No Photo:** No photo is taken during user verification. **Take photo, no save:** Photo is taken but not saved during verification. **Take photo and save:** Photo is taken and saved during verification.

	Save on successful verification: Photo is taken and saved after successful verification. **Save on failed verification:** Photo is taken and saved after a failed verification.
Display User Photo	To set the user photo which is to be displayed after a successful verification. Turn it **[ON]** to display user photos and **[OFF]** to disable it.
Alphanumeric User ID	Whether to support letters in Employee ID.
Attendance Log Alert	When the remaining storage value is not sufficient, the device will automatically alert the users. 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 ranging 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 ranging from 1 to 99.
Confirm Screen Delay(s)	The display of the verification information interface after verification. The value ranges from 1 to 9 seconds.
Face Comparison Interval (s)	Sets the face comparison interval as required, within the range of 0 to 9s.
Expiration Rule	Whether to enable the expiration rule. If yes, conduct the expiration settings, including retaining user information, and not saving attendance records; retaining user information, and saving attendance records; and deleting user information.

6.3 Face Parameters

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



Face

1:1 Match Threshold 585

1:N Match Threshold 585

Face enrollment threshold 76

Exposure 300

Quality 70

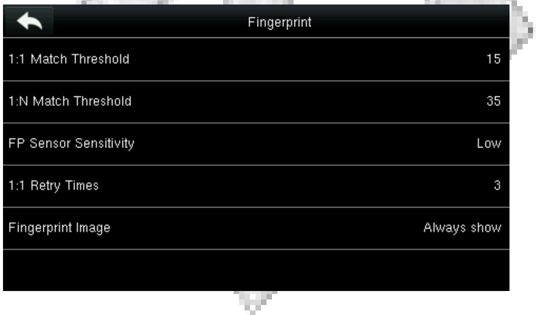
FRR	FAR	Match Threshold	
		1:N	1:1
High	Low	85	80
Medium	Medium	82	75
Low	High	80	70

Menu	Description
1:1 Match Threshold	In the 1:1 Verification method, only when the similarity between the verifying face and the user's registered faces is greater than this value, the verification succeeds. The valid value range is 70 to 120, with a larger threshold leading to lower misjudgment rate and higher rejection rate, and vice versa.
1:N Match Threshold	In the 1:N Verification method, only when the similarity between the verifying face and all registered faces is greater than this value, the verification succeeds. The valid value range is 80 to 120, with a larger threshold leading to lower misjudgment rate and higher rejection rate, and vice versa.
Face enrollment threshold	In the 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 technician of our company.

6.4 Fingerprint Parameters

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



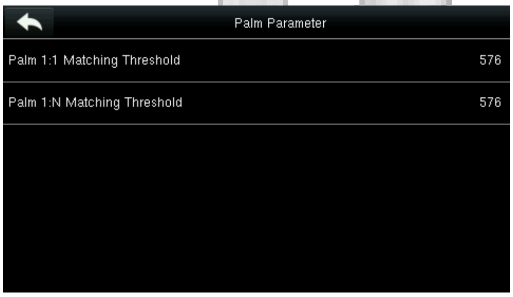
1:1 Match Threshold 15
1:N Match Threshold 35
FP Sensor Sensitivity Low
1:1 Retry Times 3
Fingerprint Image Always show

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

Menu	Description
1:1 Match Threshold	In the 1:1 Verification method, only when the similarity between the verifying fingerprint and the user's registered fingerprint is greater than this value, the verification succeeds.
1:N Match Threshold	In the 1:N Verification method, only when the similarity between the verifying fingerprint and all registered fingerprints is greater than this value, the verification succeeds.
FP Sensor Sensitivity	To set the sensibility of fingerprint collection. It is recommended to use the default level “**Medium** (When the environment is dry it results in slow fingerprint detection. In such a case, you can set the level to“**High** 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 options are available: **Show for enroll** displays the fingerprint image on the screen only during registration. **Show for match** displays the fingerprint image on the screen only during the comparison. **Always Show** displays the fingerprint image on screen both during registration and comparison. **None:** Does not display the fingerprint image in any case.

6.5 Palm Parameters

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



Palm Parameter

Palm 1:1 Matching Threshold 576

Palm 1:N Matching Threshold 576

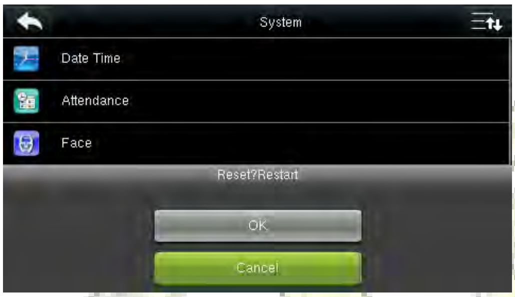
FRR	FAR	Match Threshold	
		1:N	1:1
High	Low	45	25
Medium	Medium	35	15
Low	High	25	10

Menu	Description
Palm 1:1 Matching Threshold	In 1:1 Verification method, only when the similarity between the verifying palm and the user's registered palm is greater than this value, the verification succeeds.
Palm 1:N Matching Threshold	In 1:N Verification method, only when the similarity between the verifying palm and all registered palm is greater than this value, the verification succeeds.

6.6 Reset to Factory Settings

This function resets the data such as communication settings and system settings to factory settings.

- Tap Reset on the System interface.

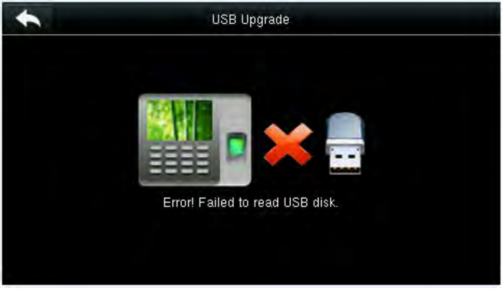


- Tap **OK** to finish the reset settings.

6.7 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, the system gives the following prompt after you tap **USB Upgrade** on the **System** interface.



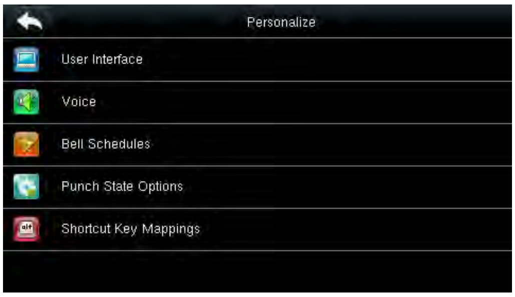
Error! Failed to read USB disk.

Note: If the upgrade file is needed, please contact our technical support team. The Firmware upgrade is not recommenced under normal circumstances.

7. Personalize Settings

This function customizes the related settings of the user interface, voice, bell schedule, punch state options, and customize shortcut keys.

- Tap **Personalize** on the main menu interface.



Personalize

User Interface

Voice

Bell Schedules

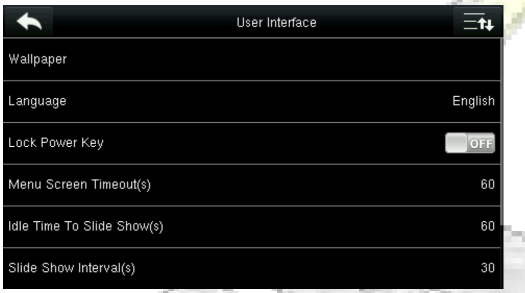
Punch State Options

Shortcut Key Mappings

7.1 User Interface Settings

You can customize the display style of the home screen.

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



User Interface

Wallpaper

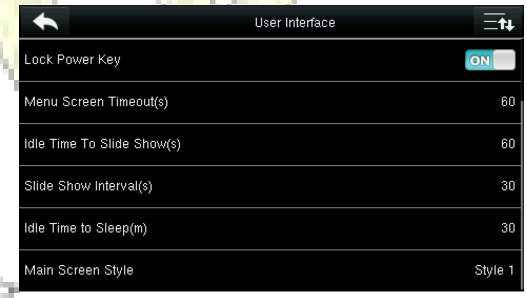
Language English

Lock Power Key OFF

Menu Screen Timeout(s) 60

Idle Time To Slide Show(s) 60

Slide Show Interval(s) 30



User Interface

Lock Power Key ON

Menu Screen Timeout(s) 60

Idle Time To Slide Show(s) 60

Slide Show Interval(s) 30

Idle Time to Sleep(m) 30

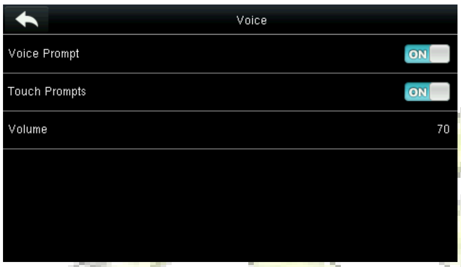
Main Screen Style Style 1

Menu	Description
Wallpaper	Select the wallpaper of the main screen as required, you can find wallpapers of various styles in the device.
Language	Select the language of the 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 preset value, the device will automatically exit back to the initial interface. You can disable it or set the value from 60 to 99999 seconds.
Idle Time To Slide Show (s)	When there is no operation in the initial interface and the time exceeds the preset value, a slide show will be shown. It can be disabled (set to "**None** or set from 3 to 999 seconds.

Slide Show Interval (s)	This refers to the interval between displaying different slide show photos. It can be disabled or set from 3 to 999s.
Idle Time To Sleep (m)	When there is no operation in the device and the preset sleep time is attained, the device will enter the standby mode. Press any key or finger to cancel the standby mode. You can disable this function or set the value from 1 to 999 minutes. If this function is **[Disabled]**, the device will not enter standby mode.
Main Screen Style	Choose the position of the clock and status key.

7.2 Voice Settings

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



Voice Prompt ON
Touch Prompts ON
Volume 70

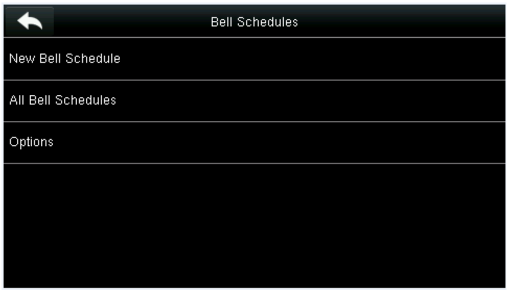
Menu	Description
Voice Prompt	Select whether to enable voice prompts during operating, press **ON** to enable it.
Touch Prompt	Select whether to enable the keyboard voice while pressing the keyboard, press **ON** to enable it.
Volume	Set the volume of the device.

7.3 Bells Settings

Many companies choose to use a bell to intimate the 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 over.

7.3.1 Add a Bell

- Tap **Bell Schedules** on the **Personalize** interface.
- Tap **New Bell Schedule** and then **Bell Status** to enable the bell status.

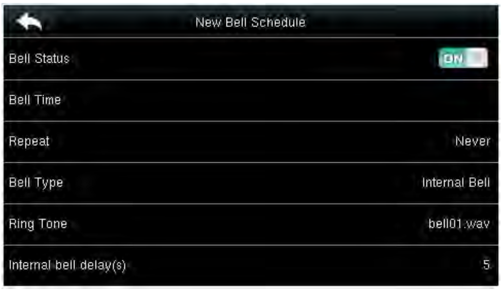


Bell Schedules

New Bell Schedule

All Bell Schedules

Options



New Bell Schedule

Bell Status: ON

Bell Time

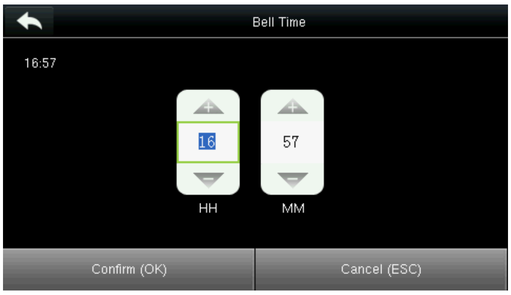
Repeat: Never

Bell Type: Internal Bell

Ring Tone: bell01.wav

Internal bell delay(s): 5

- Set the Bell Time and then set the repeating days as shown below:

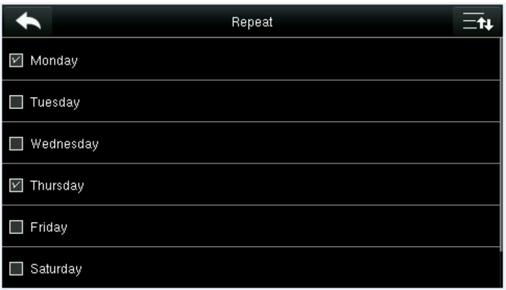


Bell Time

16:57

16 (HH) : 57 (MM)

Confirm (OK) | Cancel (ESC)



Repeat

☑ Monday

☐ Tuesday

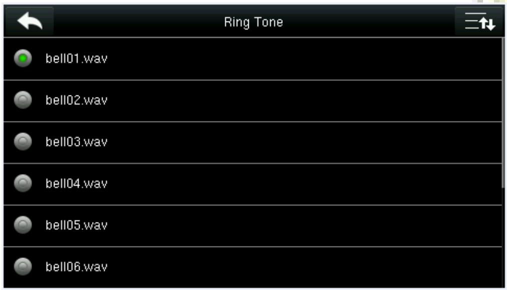
☐ Wednesday

☑ Thursday

☐ Friday

☐ Saturday

- Select the ringtone and select the internal bell delay.



Ring Tone

● bell01.wav

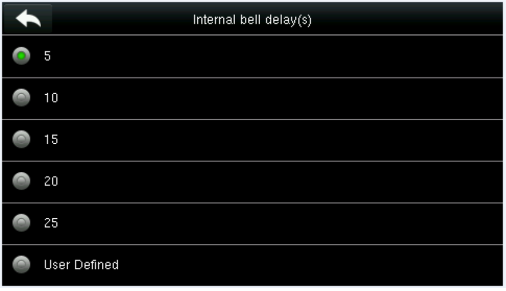
○ bell02.wav

○ bell03.wav

○ bell04.wav

○ bell05.wav

○ bell06.wav



Internal bell delay(s)

● 5

○ 10

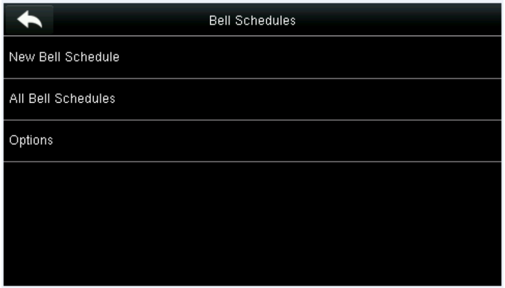
○ 15

○ 20

○ 25

○ User Defined

The added bells will be displayed as shown below:

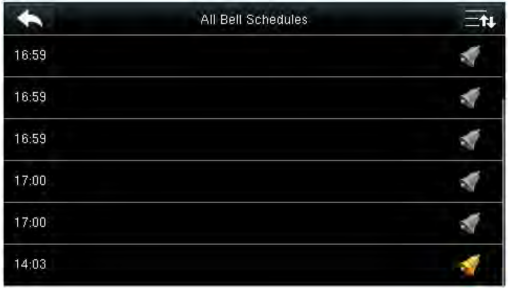


Bell Schedules

New Bell Schedule

All Bell Schedules

Options



All Bell Schedules

16:59

16:59

16:59

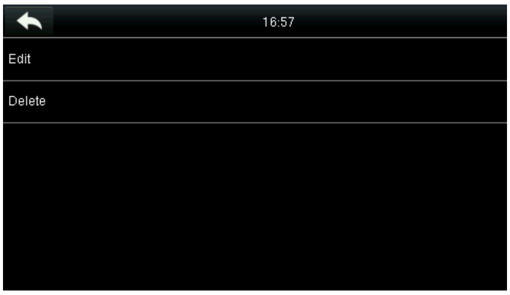
17:00

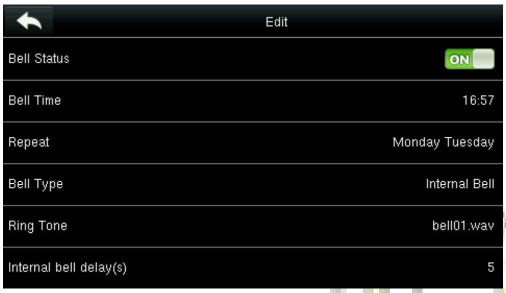
17:00

14:03

7.3.2 Edit a Bell

- On the All Bell Schedules interface, tap the bell item to be edited.
- Then tap **Edit** and make the required changes.




Edit

Bell Status ON

Bell Time 16:57

Repeat Monday Tuesday

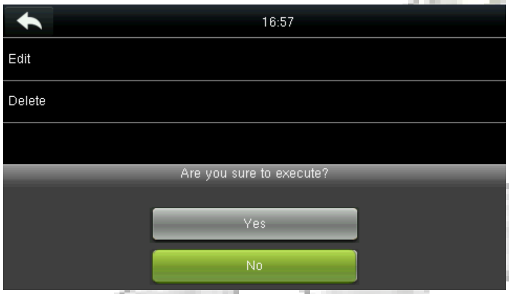
Bell Type Internal Bell

Ring Tone bell01.wav

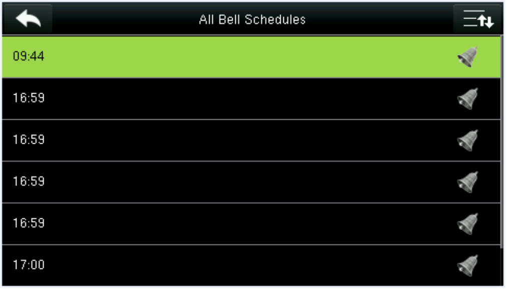
Internal bell delay(s) 5

7.3.3 Delete a Bell

- On the All Bell Schedules interface, tap the bell item to be deleted
- Then tap **Delete.**

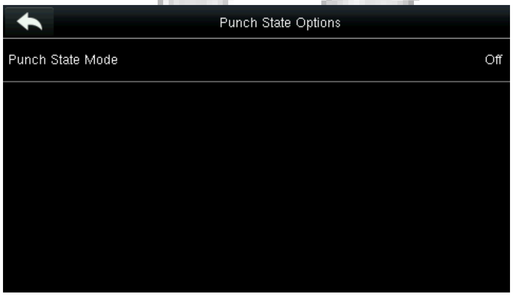


Are you sure to execute?

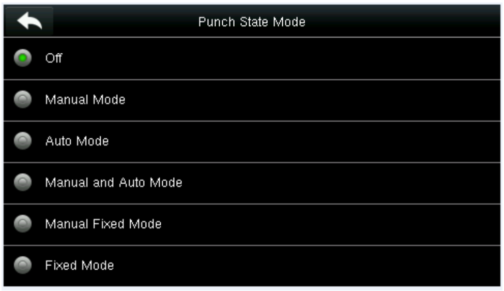


7.4 Punch States Settings

- Tap Punch State Options on the Personalize interface.


Punch State Options

Punch State Mode Off



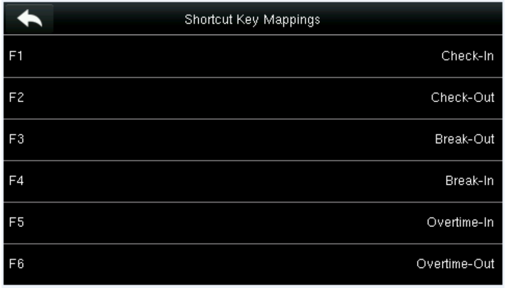
Menu	Description
Punch State Mode	Select a punch state mode, the available options are given below:

	Off: Disables the punch state key function. The punch state key set under the **Shortcut Key Mappings** menu will become invalid. **Manual Mode:** Switches 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 punch state key will be switched automatically. **Manal and Auto Mode:** In this mode, the main interface will display the auto-switching punch state key, meanwhile it also supports manual switching punch state key. After the timeout, the manually switching punch state key will become an auto-switching punch state key. **Manual Fixed Mode:** After the 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.

7.5 Shortcut Keys Settings

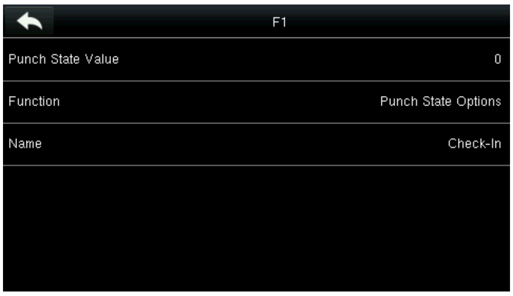
Shortcut keys can be defined as punch state keys or menu function keys. On the main interface, pressing the shortcut key will display the attendance state or open the menu operation interface.

- Tap **Shortcut Key Mappings** on the **Personalize** interface.
- Tap the shortcut key to be set (For the name of the corresponding key, refer 1.6 Initial Interface).
- The shortcut key setting interface is displayed as shown below:



Shortcut Key Mappings

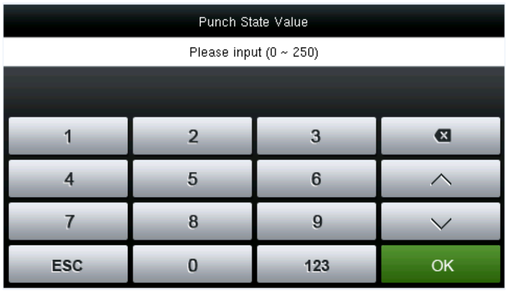
F1	Check-In
F2	Check-Out
F3	Break-Out
F4	Break-In
F5	Overtime-In
F6	Overtime-Out

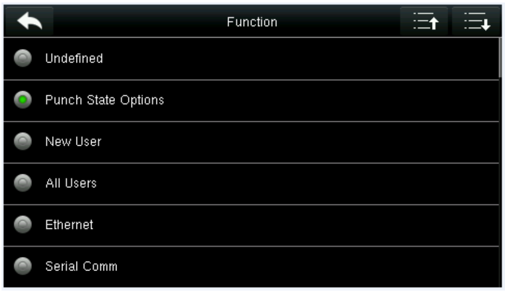


F1

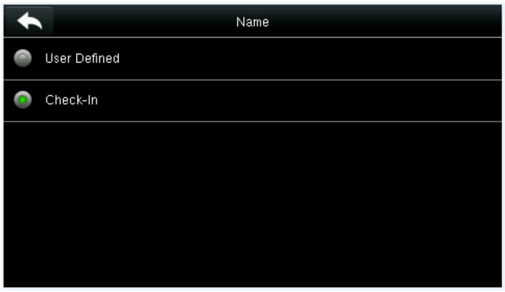
Punch State Value	0
Function	Punch State Options
Name	Check-In

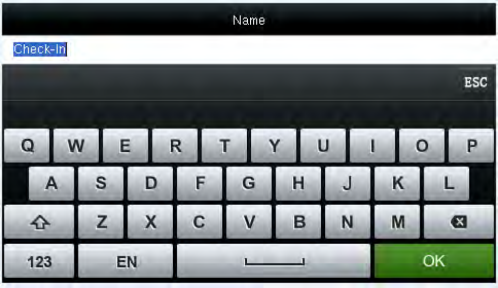
- Set the punch state value range (0-250).
- Set the corresponding function for this touch key.



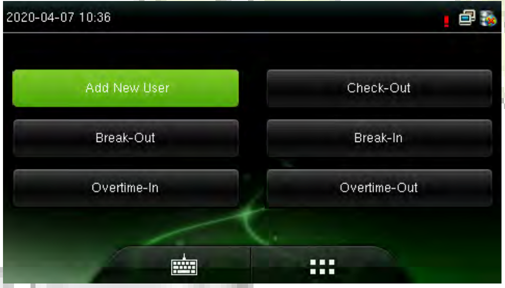


- Set the state key name as shown below:





- Tap the main interface to view the shortcut menu as shown below:

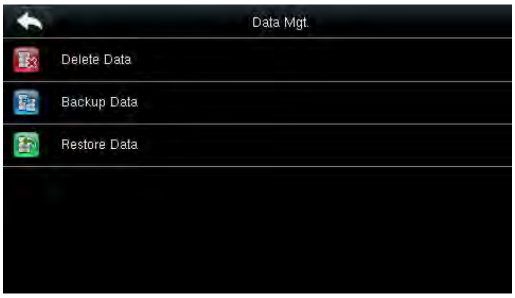


Tap the attendance state to make a switch. Tap the function to rapidly access the function settings. (Tap F1 **New User** to rapidly access this menu.)

8 Data Mgt.

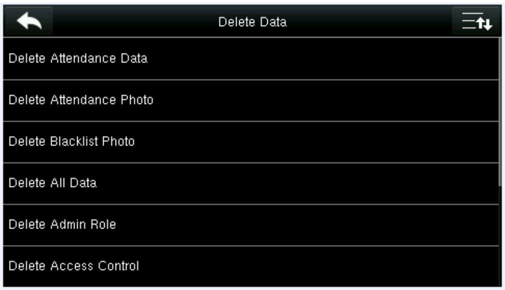
Data Management manages the data in the device, which includes delete, backup, and restore options.

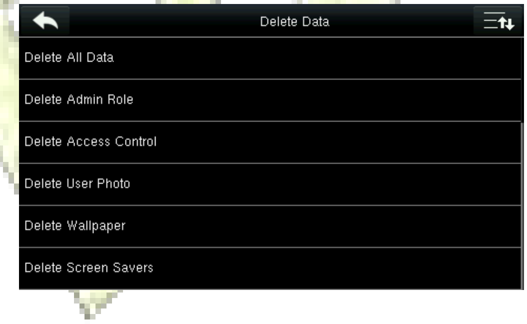
- Tap **Data Mgt.** on the main menu interface.



8.1 Delete Data

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

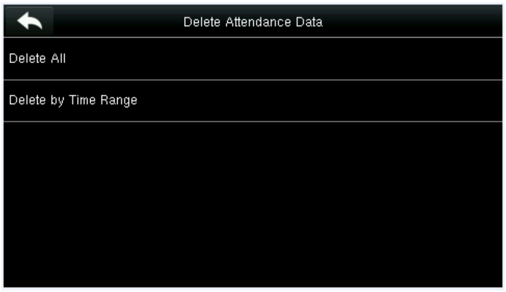


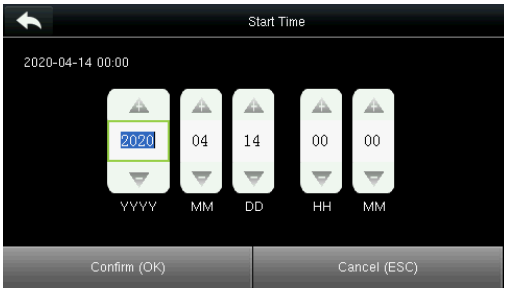


Menu	Description
Delete Attendance Data	To delete all the attendance data in the device.
Delete Attendance Photo	To delete all the users' attendance photos in the device.
Delete Blacklist Photo	To delete all the blacklisted photos in the device, which means the photos taken after failed verifications.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





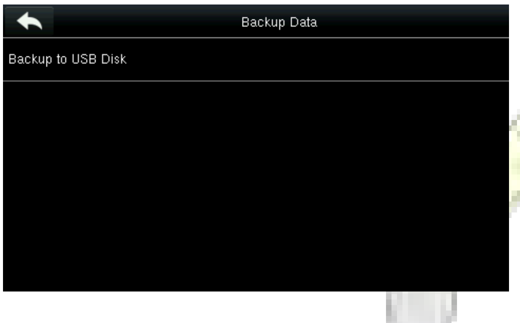
2020-04-14 00:00

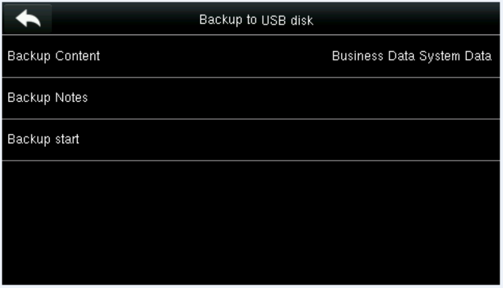
2020 04 14 00 00

8.2 Data Backup

Data Backup is used to back up the business data or send data to the U-disk.

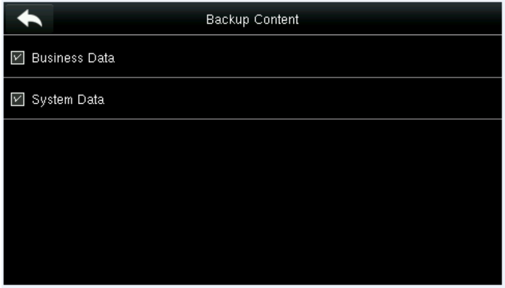
- Tap **Backup Data** on the **Data Mgt.** interface.
- Select **Backup to USB Disk** and then **Backup Content**.





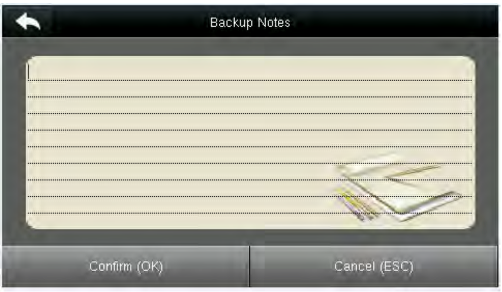
Backup Content Business Data System Data

- Select the content to be backed up.
- Enter a backup remark(optional) as shown below:

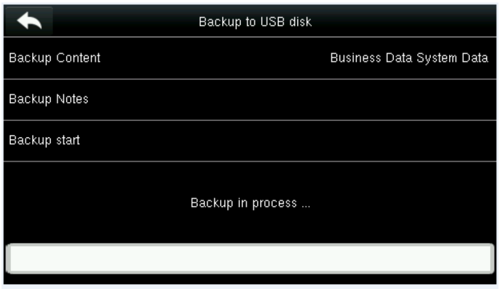


☑ Business Data

☑ System Data



- Tap **Backup Start** to start data backup.



Backup Content Business Data System Data

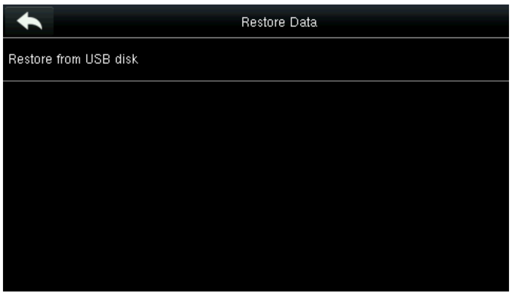
Backup in process ...

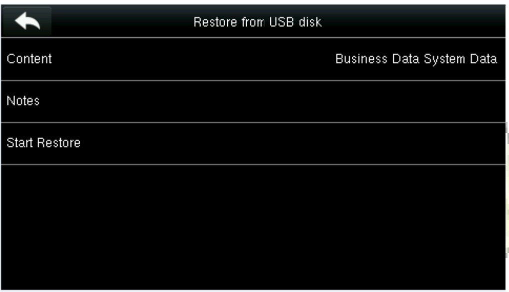
When you choose to save the data in a USB disk, ensure that the USB disk is properly plugged into the device.

8.3 Data Restoration

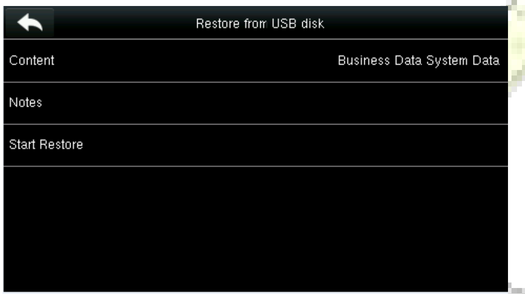
Data Restoration is used to restore the data in the USB disk to the device.

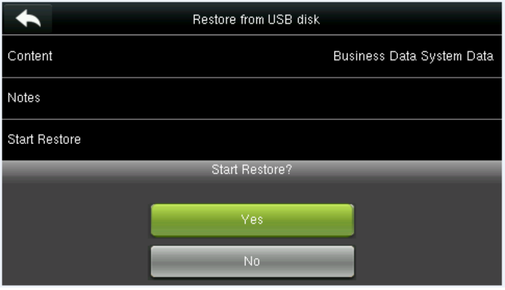
- Tap **Restore Data** on the **Data Mgt.** interface.
- Tap **Restore from USB Disk** and then Tap **Content**





- Select the data content to be restored
- Tap **Start Restore** and select **Yes** to confirm the restoration.



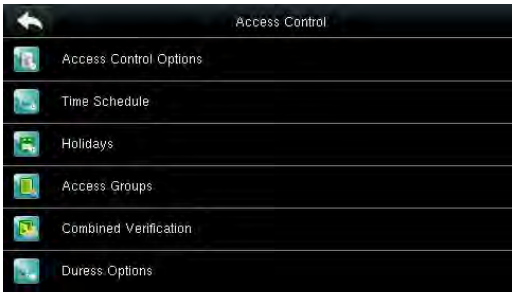


When you choose to save data to a USB disk, ensure that the USB disk is properly plugged into the device and contains the corresponding data to be restored.

9 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:

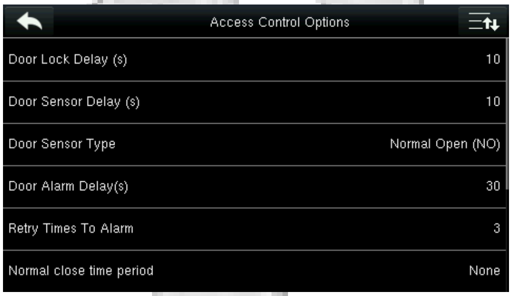
1. User's access time must fall within either the user's personal time zone or group time zone.
2. The User group must be in the access combination (when there are other groups in the same access combination, verification of members of those groups are also required to unlock the door).

By default, the new users are allocated into the first group with the default group time zone and access combination as "1" and set in an unlocking state.

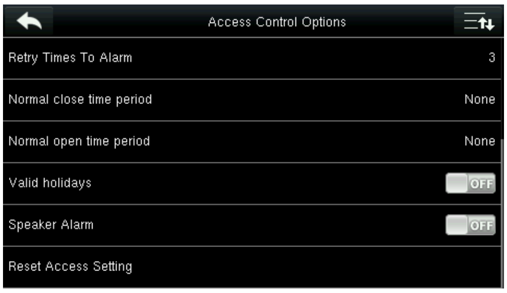
9.1 Access Control Options Settings

Access Control options are used to set the parameters of the equipment control lock and the related equipment.

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



Door Lock Delay (s) 10
Door Sensor Delay (s) 10
Door Sensor Type Normal Open (NO)
Door Alarm Delay(s) 30
Retry Times To Alarm 3
Normal close time period None



Retry Times To Alarm 3
Normal close time period None
Normal open time period None
Valid holidays OFF
Speaker Alarm OFF
Reset Access Setting

Menu	Description
Door Lock Delay (s)	The period of time of unlocking (from the 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

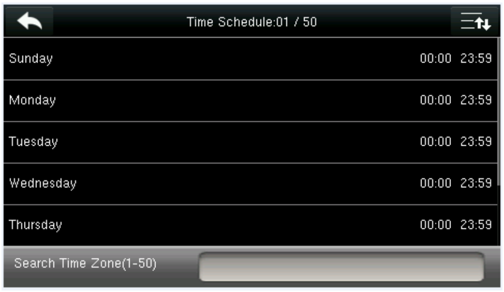
Door Sensor Delay (s)	When the door is opened, the door sensor will be checked after a time period; if the state of the door sensor is inconsistent with that of the door sensor mode, an alarm will be triggered. The time period is the **Door Sensor Delay** (value ranges from 1 to 255 seconds).
Door Sensor 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, an 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 a failed verification.
Normal close time period	To set time period for Normally Closed mode, so that no one can gain access during this period.
Normal open time period	To set time period for Normally Open, so that the door is always unlocked during this period.
Valid holidays	To set if **Normal close time period** or **Normal open time period** settings are valid in the set holiday time period. Choose **[ON]** to enable the set **NC** or **NO** time period in the 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 the access control parameters.

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

9.2 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.

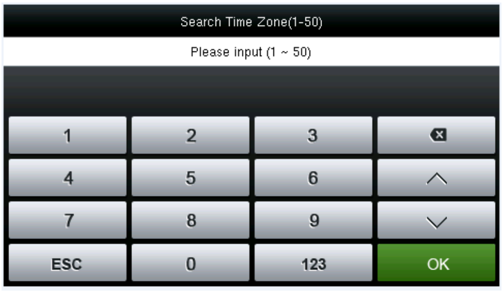
- Tap **Time Schedule** on the **Access Control** interface.
- Tap the input box to search time zone.
- Enter the number of the time zone.



Time Schedule:01 / 50

Sunday	00:00 23:59
Monday	00:00 23:59
Tuesday	00:00 23:59
Wednesday	00:00 23:59
Thursday	00:00 23:59

Search Time Zone(1-50)

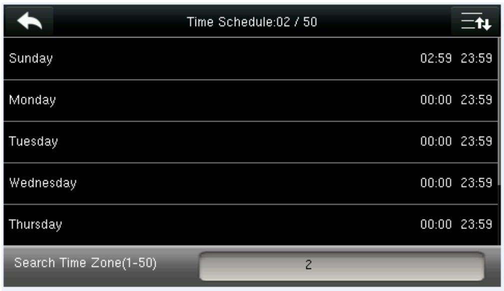


Search Time Zone(1-50)

Please input (1 ~ 50)

Tap the date on which time zone setting is required.

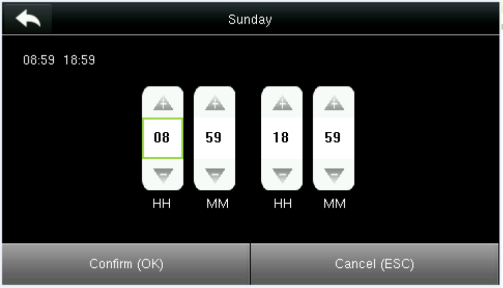
- Tap the date on which time zone setting is required.
- Press the **Up and Down** keys to set the start and end time, and then press **Confirm (OK).**



Time Schedule:02 / 50

Sunday	02:59 23:59
Monday	00:00 23:59
Tuesday	00:00 23:59
Wednesday	00:00 23:59
Thursday	00:00 23:59

Search Time Zone(1-50) 2



Sunday

08:59 18:59

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

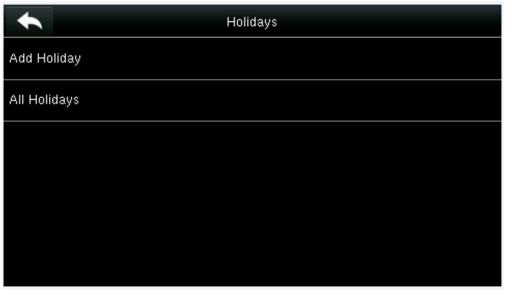
1. **Invalid Time Schedule:** When the end time is smaller than the start time.
2. The default time zone 1 indicates that the system is open all day long.

9.3 Holidays Settings

The concept of holiday and festival can be incorporated 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 can be set on holidays and festivals, which applies to all the users.

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

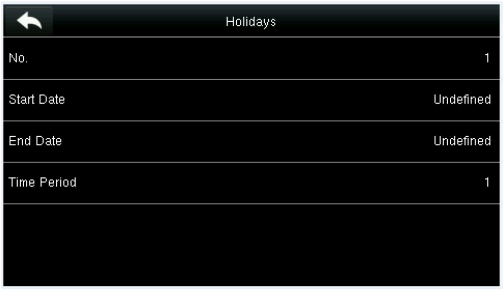
- Tap **Holidays** on the **Access Control** interface.



Holidays

9.3.1 Add a New Holiday

- Tap **Add Holiday** on the **Holidays** interface.
- Set the holiday parameters.
- The added holidays are displayed in a list as shown below:

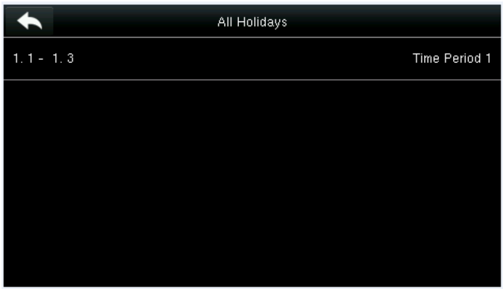

Holidays

No. 1

Start Date Undefined

End Date Undefined

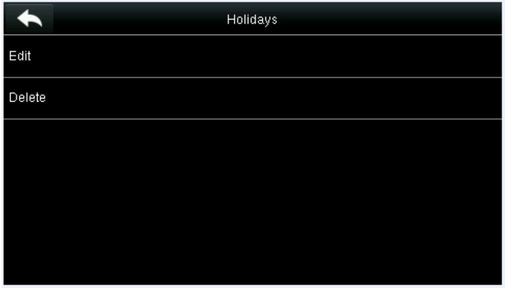
Time Period 1

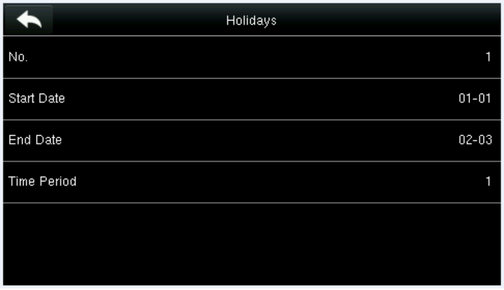

All Holidays

1. 1 - 1. 3 Time Period 1

9.3.2 Edit a Holiday

- On the Holidays interface, tap to select an item to be modified.
- Tap **Edit** and then modify the holiday parameters




Holidays

No. 1

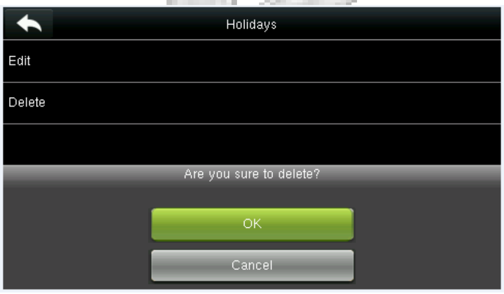
Start Date 01-01

End Date 02-03

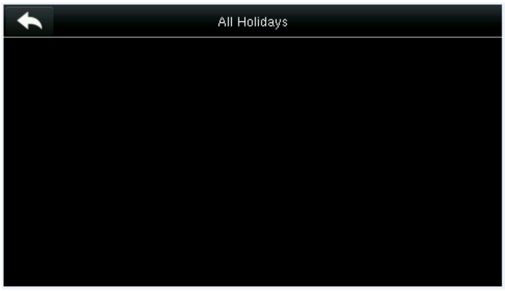
Time Period 1

9.3.3 Delete a Holiday

- On the **Holidays** interface, tap to select a holiday item to be modified, and tap **Delete**.
- Tap **OK** to confirm the deletion.



Are you sure to delete?

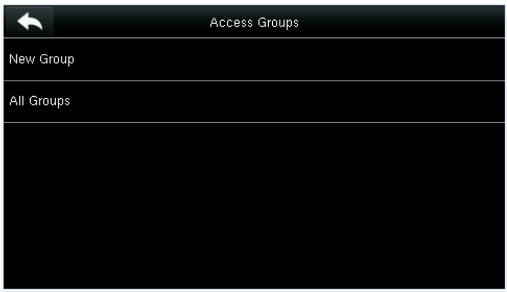


9.4 Access Groups Settings

The Access Group is used to manage the users in the groups.

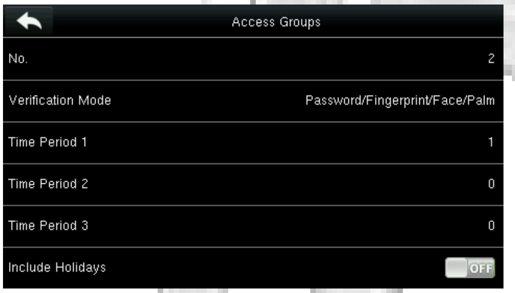
The time zone of the users in a specific group is set to be the group time zone, while the users can set their personal time zone. When the group verification mode overlaps the user verification mode, the user verification modes prevail. Each group can set 3 time zones at most. As long as one of them 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 groups if required.

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



9.4.1 Add a New Group

- Tap **New Group** on the **Access Groups** interface.
- Set the access group parameters.
- The added access groups are displayed in the list as shown below:


Access Groups

No. 2

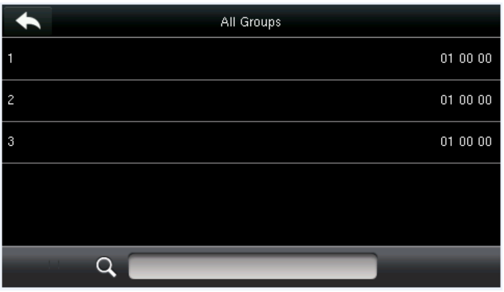
Verification Mode Password/Fingerprint/Face/Palm

Time Period 1 1

Time Period 2 0

Time Period 3 0

Include Holidays OFF


All Groups

1 01 00 00

2 01 00 00

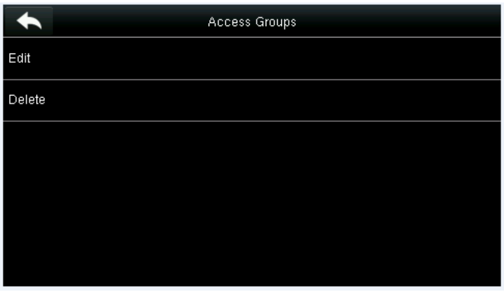
3 01 00 00

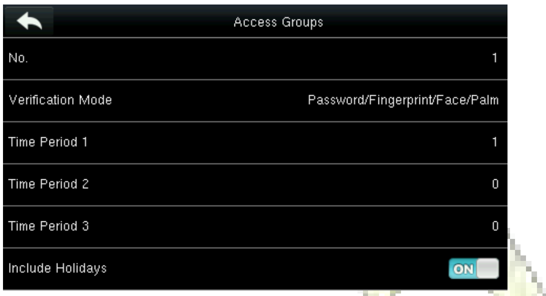
Note:

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 the 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.

9.4.2 Edit a Group

- On the **All Groups** interface, tap to select the access group item to be modified.
- Tap Edit to edit the access group and modify the access group parameters.

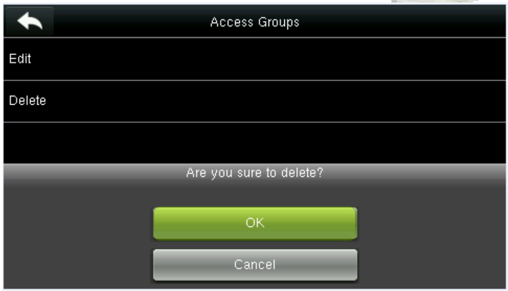


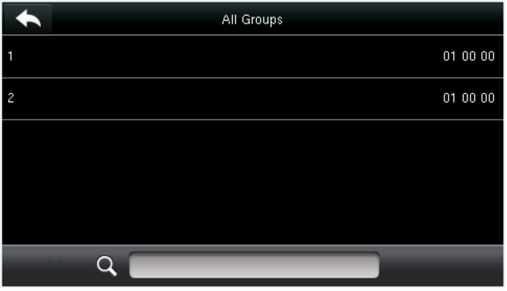

Access Groups

No.	1
Verification Mode	Password/Fingerprint/Face/Palm
Time Period 1	1
Time Period 2	0
Time Period 3	0
Include Holidays	ON

9.4.3 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 the deletion.



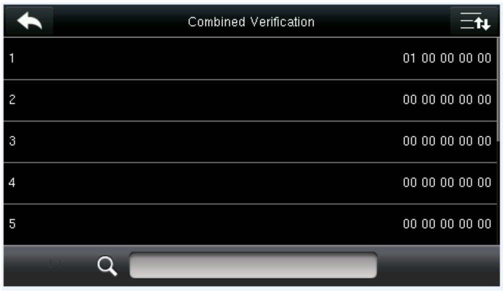

All Groups

1	01 00 00
2	01 00 00

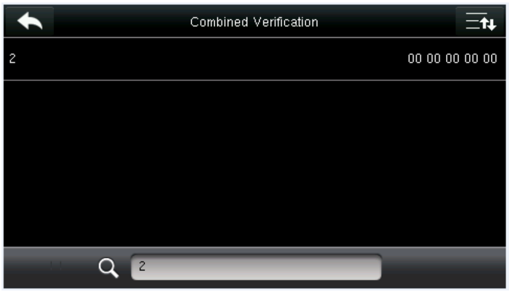
9.5 Combined Verification Settings

The Combined Verification Settings combines two or more members to achieve multi-verification to improve security.

- Tap **Combined Verification** on the **Access Control** interface.
- Tap the unlocking combination to be set or tap the search bar and enter an unlocking combination number to find the specific combination.

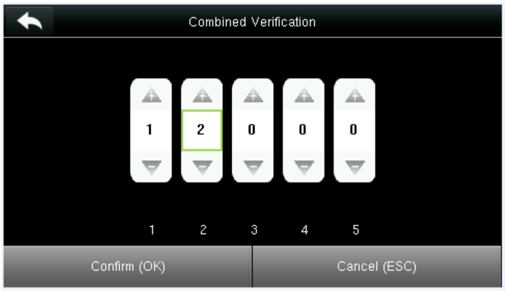


1	01 00 00 00 00
2	00 00 00 00 00
3	00 00 00 00 00
4	00 00 00 00 00
5	00 00 00 00 00



2	00 00 00 00 00

Search: 2



1 2 0 0 0

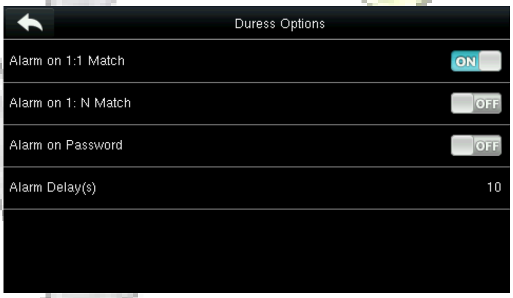
Note: In a Combined Verification, the range of user number is: 0 ≤ N ≤ 5. If you need to delete an unlocking combination, directly set all the digits of the combination number to 0. If you need to modify a combination, directly tap the corresponding combination item to perform the setting again.

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

9.6 Duress Options Settings

When there is an emergency situation, select the duress alarm mode, the device will then open the door as usual and send the alarm signal.

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



Alarm on 1:1 Match	ON
Alarm on 1: N Match	OFF
Alarm on Password	OFF
Alarm Delay(s)	10

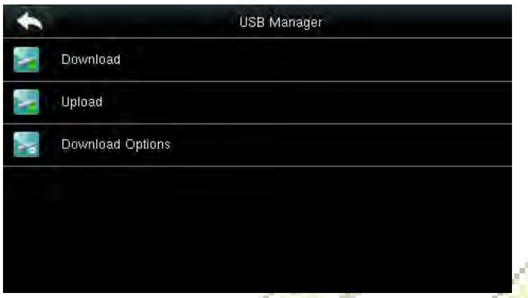
Menu	Description
Alarm on 1:1 Match	In **[ON]** state, when a user uses 1:1 Verification Method to verify any registered fingerprint, an alarm will be triggered. In **[OFF]** state, no alarm signal will be triggered.
Alarm on 1: N Match	In **[ON]** state, when a user uses 1:N Verification Method to verify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

10 USB Manager

You can import the user information, fingerprint template, and attendance data in the device to an attendance software for processing, or import the user information and fingerprints to other fingerprint devices for backup.

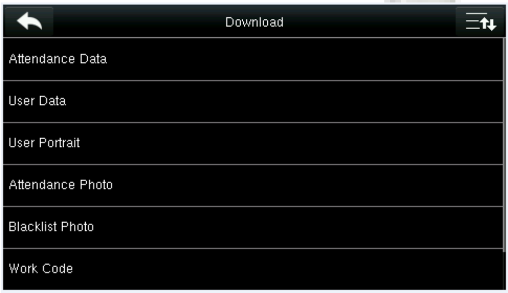
Before uploading/downloading data from/to the USB disk, insert the USB disk into the USB slot first.

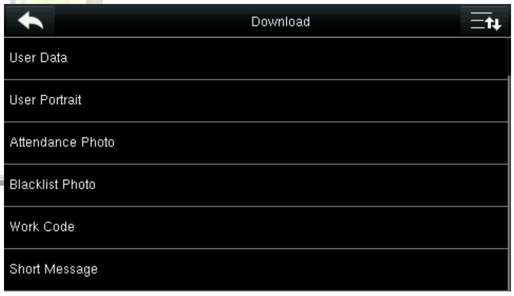
- Tap **USB Manager** on the main menu interface.



10.1 USB Download

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

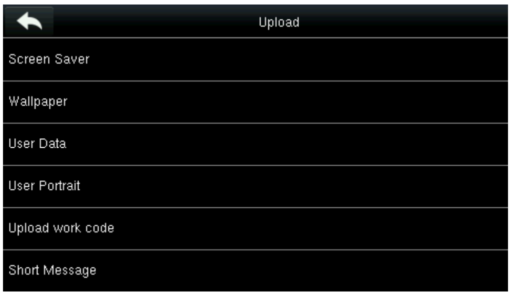




Menu	Description
Attendance Data	To download the attendance data in a specified time period into USB disk.
User Data	To download all the user information and fingerprint data from the device into USB disk.
User Portrait	To download all the user photos from the device into a USB disk.
Attendance Photo	To download all the attendance photos from the device into USB disk.
Blacklist Photo	To download all the 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.

10.2 USB Upload

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


Upload

Screen Saver

Wallpaper

User Data

User Portrait

Upload work code

Short Message

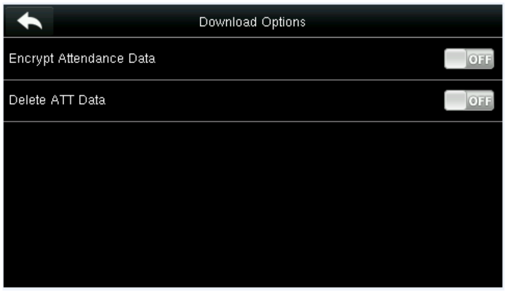
Menu	Description
Screen Saver	To upload all the screen savers from the USB disk to the device. You can choose **Upload selected photo** or **Upload all photos.** The images will be displayed on the device's main interface after uploading it. During uploading, you need to create a folder named "**advertise**" in the root directory of the USB disk and save 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 are supported.
Wallpaper	To upload all the 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 uploading. During uploading, you need to create a folder named "**wallpaper**" in the root directory of the USB disk and save 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 are supported.
User Data	To upload all the user information and fingerprints from the device into the USB disk.
User Portrait	To upload all the user photos from the device into the USB disk.
Upload Work Code	To upload the work codes in the USB disk to the device.
Short Message	To upload the 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 pixels.

10.3 Download Options Settings

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



Encrypt Attendance Data OFF

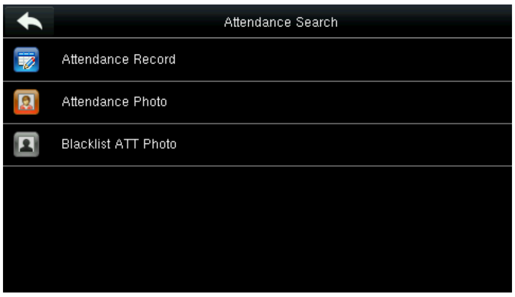
Delete ATT Data OFF

Menu	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.

11 Attendance Search

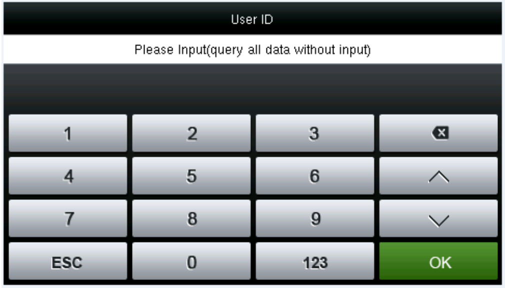
When a user is verified successfully, the attendance records are saved in the device. This function enables us to check the attendance logs.

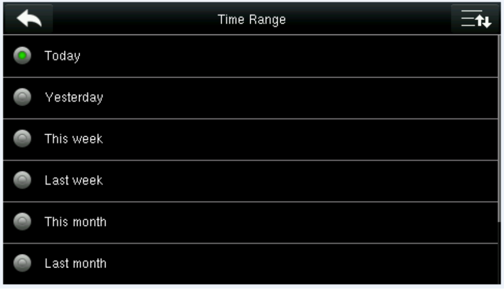
- Tap **Attendance Search** on the main menu interface.



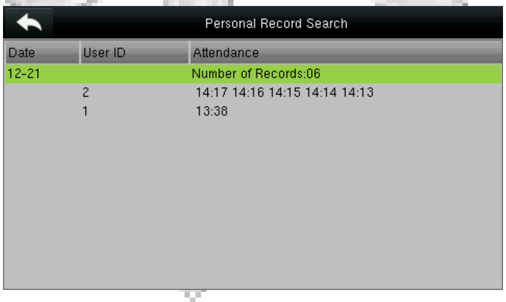
The process of searching for attendance photos and blacklist photos is the same as that of searching attendance records. The following is an example of searching for attendance records.

- On the **Attendance Record** interface, tap **Attendance Record**.
- Enter the User ID to be searched and tap **OK**. Taping **OK** without entering a user ID searches the attendance records of all the employees.
- Select the time range to search the attendance record.

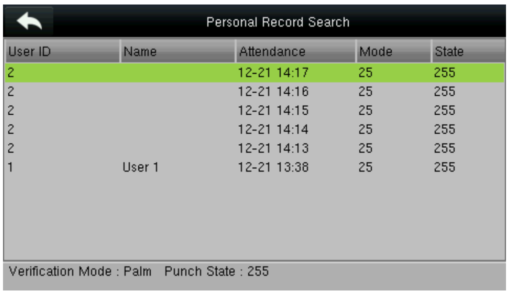




- The Attendance record will be displayed as shown below:


Personal Record Search

Date	User ID	Attendance
12-21		Number of Records:06
	2	14:17 14:16 14:15 14:14 14:13
	1	13:38


Personal Record Search

User ID	Name	Attendance	Mode	State
2		12-21 14:17	25	255
2		12-21 14:16	25	255
2		12-21 14:15	25	255
2		12-21 14:14	25	255
2		12-21 13:13	25	255
1	User 1	12-21 13:38	25	255

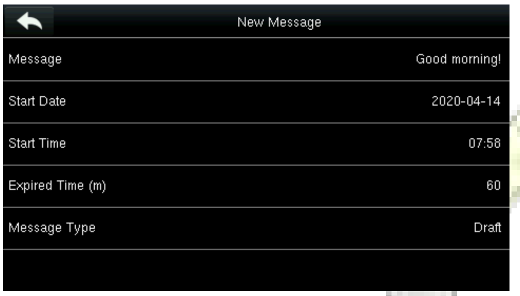
Verification Mode : Palm Punch State : 255

12 Short Messages

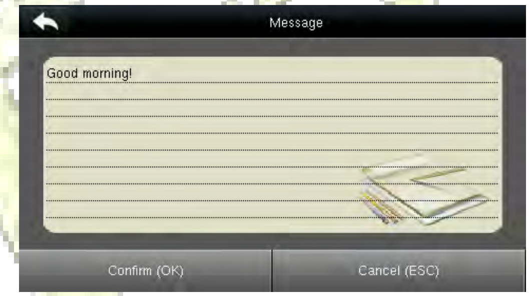
The Short Message is similar to sending a notification to the designated users. The operator can edit the notification content in advance and display it in SMS format on the screen. The SMS includes common SMS and individual SMS. If common SMS is set, ✉ will be displayed in the information column at the top of the standby interface in a specified time. If individual SMS is set, the specified employee receives the SMS after successful attendance.

12.1 Add a New Short Message

- Tap **Message** on the Short Message interface.
- Enter the content and press **OK** to save the entered content.

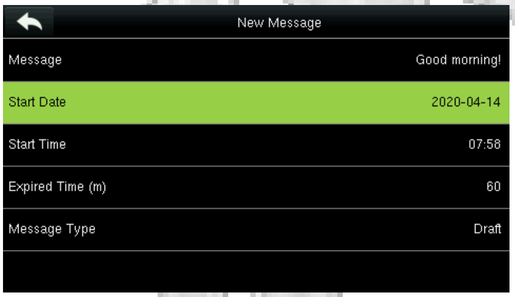


Message	Good morning!
Start Date	2020-04-14
Start Time	07:58
Expired Time (m)	60
Message Type	Draft

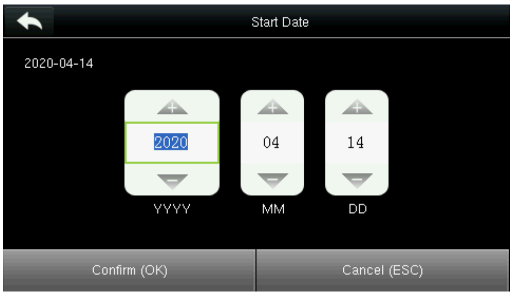


Good morning!

- Select Start Date and press OK.
- Press the Up and Down keys to enter the date and press **OK**.



Message	Good morning!
Start Date	2020-04-14
Start Time	07:58
Expired Time (m)	60
Message Type	Draft



2020-04-14

2020 04 14

- Set the Expiry time(m) after which the message 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.

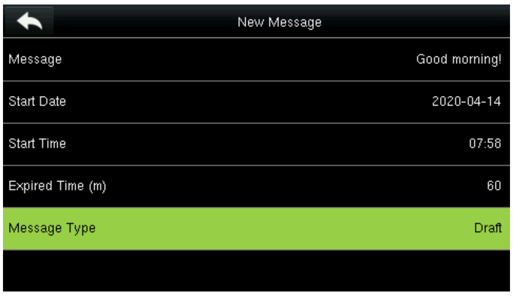
Set Message type

Public: SMS can be seen by all employees.

Personal: SMS can be seen by individuals only.

Draft: Preset SMS, no difference between individual SMS or common SMS.

- Select **Message Type** and press **OK.**
- Select a type and press **OK** for confirmation


New Message

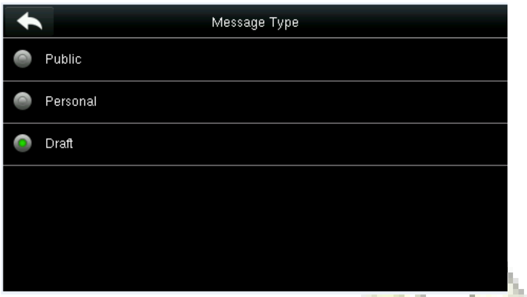
Message: Good morning!

Start Date: 2020-04-14

Start Time: 07:58

Expired Time (m): 60

Message Type: Draft


Message Type

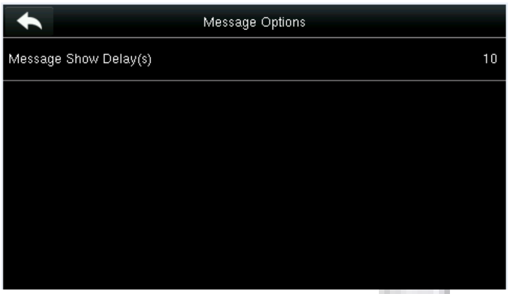
○ Public

○ Personal

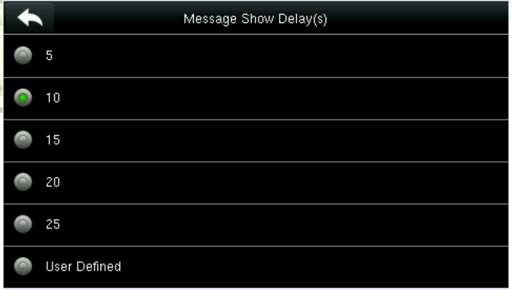
● Draft

12.2 Message Options

The Message Option sets the personal message display delay time on the initial interface.


Message Options

Message Show Delay(s): 10


Message Show Delay(s)

○ 5

● 10

○ 15

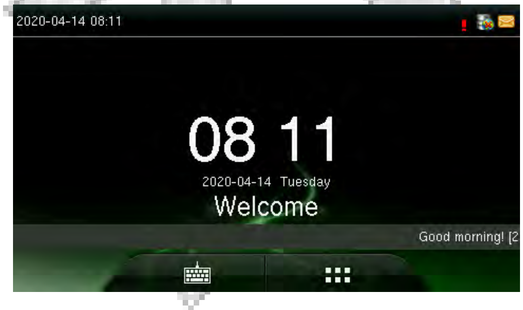
○ 20

○ 25

○ User Defined

12.3 View Public Messages and Personal Messages

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. The content of a personal short message is displayed after successful user authentication.

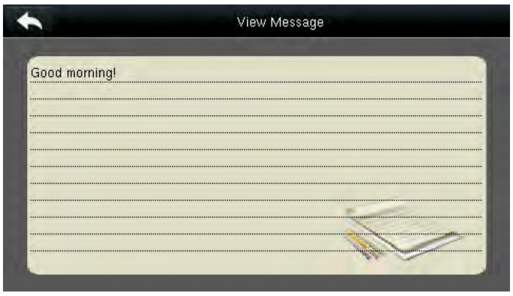

2020-04-14 08:11

08 11

2020-04-14 Tuesday

Welcome

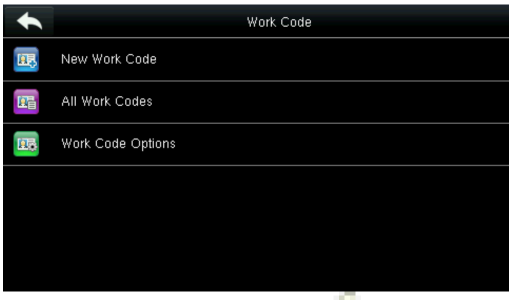
Good morning! [2


View Message

Good morning!

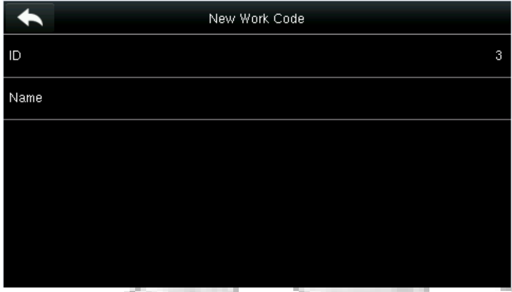
13 Work Code

Employees' payroll calculations are based on their attendance records. Employees may be engaged in different types of work which may vary with time period. Since 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 data during payroll calculation.

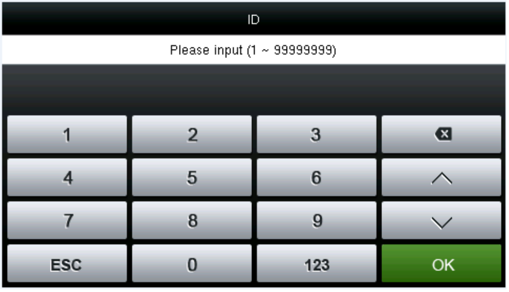


13.1 Add a Work Code

- Select **New Work Code** on the Work Code interface.
- Select ID and enter the Work Code ID.

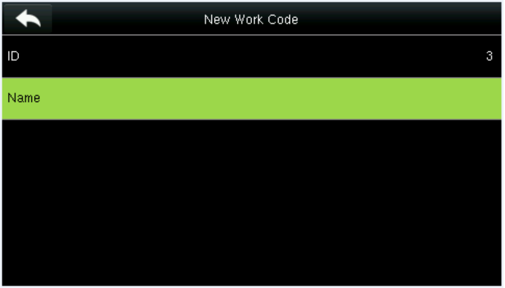


ID 3
Name

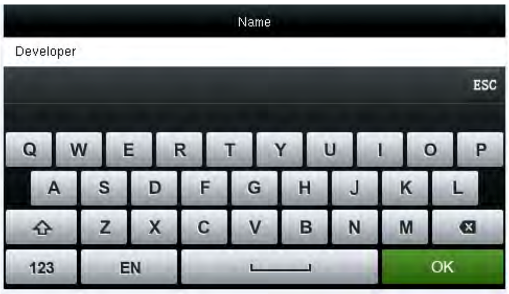


Please input (1 ~ 99999999)

- Select **Name** and enter the Work Code Name



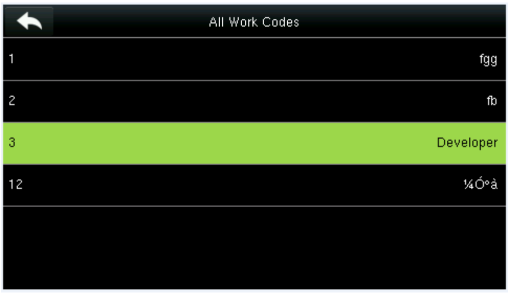
ID 3
Name



Developer

13.2 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 cannot be modified.

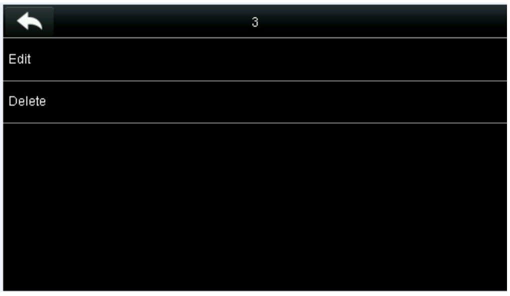


1 fgg

2 fb

3 Developer

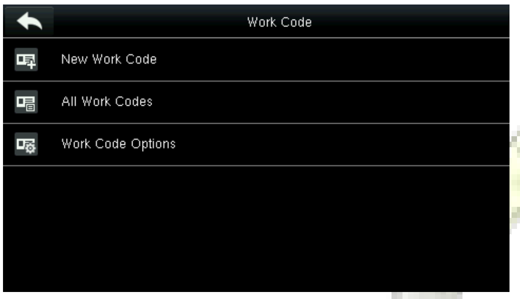
12 ¼Ó°à

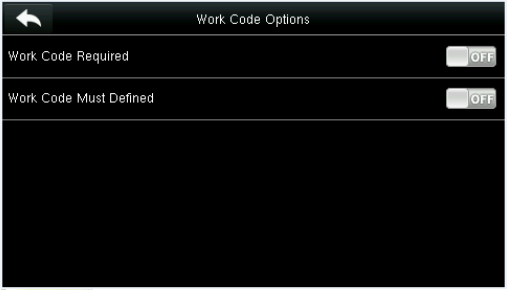


13.3 Work Code Options

The Work Code option enables us to set whether the work code must be entered and whether the entered work code must exist during authentication.

- Select **Work Code Options.**
- Turn ON or OFF the Work Code parameters





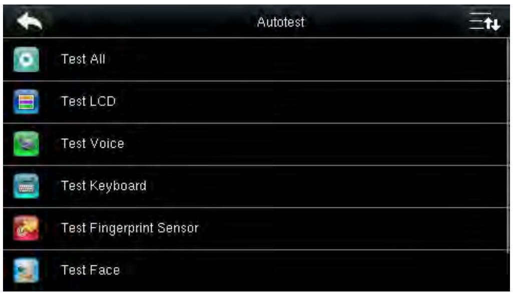
Work Code Required OFF

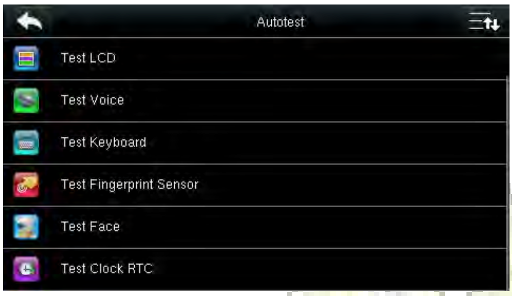
Work Code Must Defined OFF

14 Autotest

The Autotest function automatically tests whether all the modules in the device function properly, including LCD, voice, keyboard, fingerprint sensor, camera, and RTC (Real-Time Clock).

- In the initial interface, tap **Autotest** to open the **Autotest** interface.



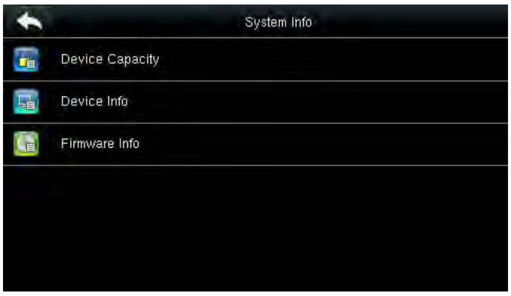


Menu	Description
Test All	To test the LCD, Voice, Keyboard, Fingerprint Sensor, Face, and Clock RTC. During the test, touch the screen to continue, and press ↩ to exit the test.
Test LCD	To test the display effect of LCD screen by displaying full color, pure white, and pure black to check whether the screen displays the 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	Tests if the keyboard is working normally.
Test Fingerprint Sensor	To test the fingerprint sensor by pressing a 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	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 the time accurately.

15 System Information

The System information displays the data capacity, device, and firmware information.

- Tap **System Info** on the main menu interface.

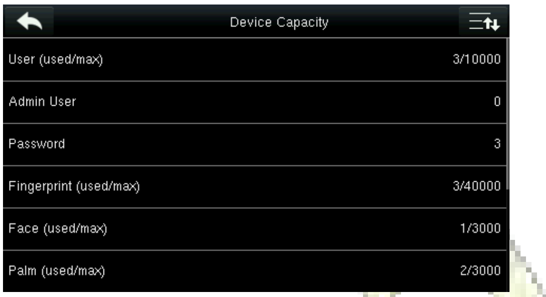


System Info

Device Capacity

Device Info

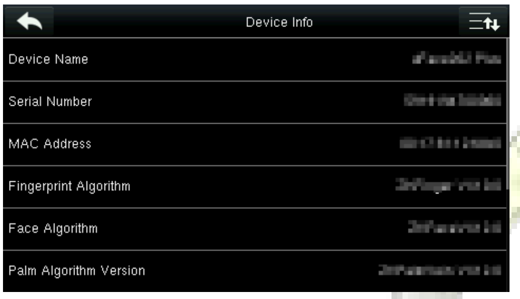
Firmware Info



Device Capacity

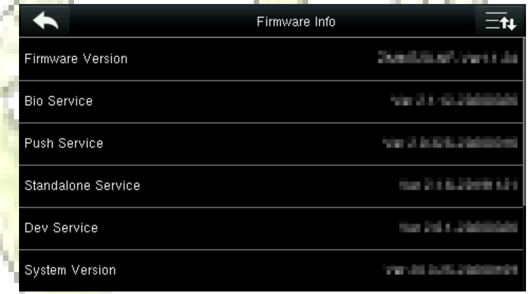
User (used/max)	3/10000
Admin User	0
Password	3
Fingerprint (used/max)	3/40000
Face (used/max)	1/3000
Palm (used/max)	2/3000

- On the System Info interface, tap information to be viewed.
- You can view the data capacity information, and press **Page Down** to view other information.



Device Info

Device Name	[illegible]
Serial Number	[illegible]
MAC Address	[illegible]
Fingerprint Algorithm	[illegible]
Face Algorithm	[illegible]
Palm Algorithm Version	[illegible]



Firmware Info

Firmware Version	[illegible]
Bio Service	[illegible]
Push Service	[illegible]
Standalone Service	[illegible]
Dev Service	[illegible]
System Version	[illegible]

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 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 Chinese law 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.

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.

ZKTeco Industrial Park, No. 26, 188 Industrial Road,
Tangxia Town, Dongguan, China.

Phone : +86 769 - 82109991

Fax : +86 755 - 89602394

www.zkteco.com