

USER MANUAL

Applicable Models: G4L

Version: 1.1

Date: July 2020

English

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

Without the prior written consent of ZKTECO CO., LTD, 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 CO., LTD. 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 product. The copyright in all the documents, drawings, etc. in relation to the ZKTeco supplied product 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 product. 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 product.

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/product. It is further essential for the safe operation of the machine/unit/product that personnel have read, understood and followed the safety instructions contained in the manual.

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

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

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

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

This manual and the information contained therein may include technical, other inaccuracies or typographical errors. ZKTeco periodically changes the information herein which will be incorporated into new additions/amendments to the manual. ZKTeco reserves the right to add, delete, amend or modify the information contained in the manual from time to time in the form of circulars, letters, notes, etc. for better operation and safety of the machine/unit/product. The said additions or amendments are meant for improvement /better operations of the machine/unit/product 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/product malfunctions due to any non-compliance of the instructions contained in this manual (ii) in case of operation of the machine/unit/product beyond the rate limits (iii) in case of operation of the machine and product 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 **G4L** product.

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

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

Document Conventions

Conventions used in this manual are listed below:

GUI Conventions

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

Symbols

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

Table of Contents

1 SAFETY MEASURES	8
2 OVERVIEW	9
3 INSTRUCTION FOR USE	9
3.1 FINGER PLACEMENT	9
3.2 STANDING POSITION, FACIAL EXPRESSION AND STANDING POSTURE	11
3.3 FACE REGISTRATION	12
3.4 STANDBY INTERFACE	13
3.5 VIRTUAL KEYBOARD	15
3.6 VERIFICATION MODE	16
3.6.1 FINGERPRINT VERIFICATION	16
3.6.2 PASSWORD VERIFICATION	19
3.6.3 FACIAL VERIFICATION.....	21
3.6.4 COMBINED VERIFICATION.....	23
4 MAIN MENU	25
5 USER MANAGEMENT.....	26
5.1 USER REGISTRATION.....	26
5.1.1 USER ID AND NAME.....	26
5.1.2 USER ROLE	27
5.1.3 FINGERPRINT	28
5.1.4 FACE.....	29
5.1.5 BADGE NUMBER	29
5.1.6 PASSWORD	30
5.1.7 USER PHOTO	31
5.1.8 ACCESS CONTROL ROLE.....	31
5.2 SEARCH FOR USERS.....	34
5.3 EDIT USER	35
5.4 DELETE USER	35
6 USER ROLE	36
7 COMMUNICATION SETTINGS.....	38
7.1 NETWORK SETTINGS	38
7.2 SERIAL COMM	39
7.3 PC CONNECTION.....	40
7.4 WIRELESS NETWORK	41

7.5 CLOUD SERVER SETTING	43
7.6 WIEGAND SETUP.....	43
7.6.1 WIEGAND INPUT	44
7.6.2 WIEGAND OUTPUT.....	45
8 SYSTEM SETTINGS.....	47
8.1 DATE AND TIME.....	47
8.2 ATTENDANCE/ACCESS LOGS SETTING	48
8.3 FACE PARAMETERS	50
8.4 FINGERPRINT PARAMETERS.....	52
8.5 FACTORY RESET	54
8.6 USB UPGRADE	54
9 PERSONALIZE SETTINGS.....	55
9.1 INTERFACE SETTINGS.....	55
9.2 VOICE SETTINGS.....	56
9.3 BELL SCHEDULES	57
9.4 PUNCH STATE OPTIONS.....	58
9.6 SHORTCUT KEY MAPPINGS.....	59
10 DATA MANAGEMENT	62
10.1 DELETE DATA.....	62
11 ACCESS CONTROL	64
11.1 ACCESS CONTROL OPTIONS	64
11.2 TIME SCHEDULE.....	66
11.3 HOLIDAY SETTINGS.....	68
11.4 ACCESS GROUPS.....	69
11.5 COMBINED VERIFICATION SETTINGS	70
11.6 DURESS OPTIONS SETTINGS.....	72
12 USB MANAGER	73
12.1 DOWNLOAD	73
12.2 UPLOAD	74
12.3 DOWNLOAD OPTIONS.....	75
13 ATTENDANCE SEARCH	76
14 SHORT MESSAGE.....	78
14.1 ADD A NEW SHORT MESSAGE	78
14.2 MESSAGE OPTIONS.....	81

14.3 VIEW THE PUBLIC MESSAGES AND PERSONAL MESSAGE.....	82
15 WORK CODE.....	83
15.1 ADD A WORK CODE	83
15.2 ALL WORK CODES LIST	85
15.3 WORK CODE OPTIONS	85
16 AUTOTEST	86
17 SYSTEM INFORMATION.....	87
APPENDIX 1 STATEMENT ON THE RIGHT TO PRIVACY	88
APPENDIX 2 ECO-FRIENDLY OPERATION.....	89

1 Safety Measures

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

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

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

7. **Replacement parts** - When replacement parts are needed, service technicians must only use replacement parts provided by the supplier. Unauthorized substitutes can result in a burn, shock, or other hazards.
8. **Safety check** - On completion of service or repair work on the unit, ask the service technician to perform safety checks to ensure proper operation of the unit.
9. **Power sources** - Operate the system only from the label's power source form. If the sort of power supply to use is unclear, call your dealer.
10. **Lightning** - External lightning conductors can be installed to protect against electrical storms. It stops power-ups destroying the system.

The devices should be installed in areas with limited access.

2 Overview

Our G4L Device facilitates users to access the cloud features, which includes data collection, storage, and analysis. This benefits the organization to store the Bio template information on the cloud server, and the data can be retrieved whenever required. This product of ours provides end to end solutions, and the cloud technology benefits to maintain updates and monitor the data on the cloud in real-time.

This product can be used for both Access Control and Attendance System, which is cloud-based. Our goal is to make a unique platform, with hardware and software services at a very low cost, and at the same time, support development by providing access via different platforms like mobile and web.

Scope

- Sync with Bio Cloud Software
- Easy Access
- Easy Integration
- Multi-Level Data Encryption and Protection
- Quick Deployment and Setup

3 Instruction for Use

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

3.1 Finger Placement

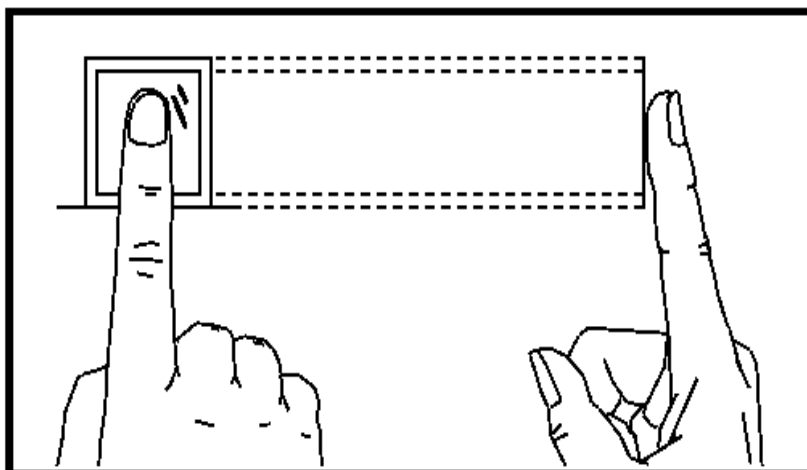
- Recommended fingers are index, middle, or ring fingers.
- Avoid using the thumb or pinky, as they are difficult to accurately press onto the fingerprint reader.

Correct and Incorrect Finger Placement

Recommended

- Place the finger on the Scanning Area and press it onto the Fingerprint Reader.
- Ensure that the center of your finger is aligned with the center of the Fingerprint Reader.

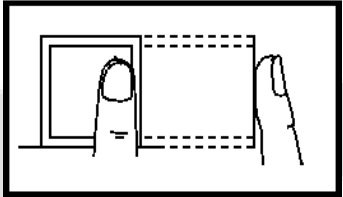
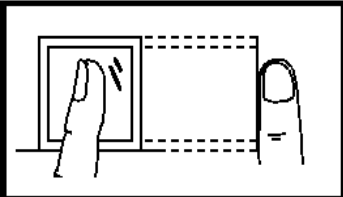
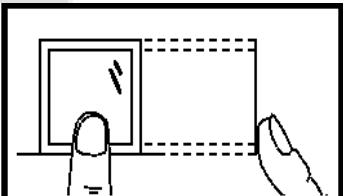
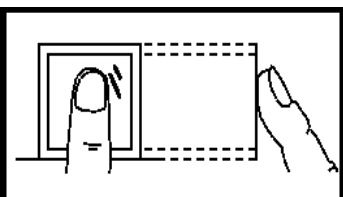
Diagrammatic Representation



Proper finger placement on the Fingerprint Reader

Not Recommended

- Incorrect ways of pressing the finger on the Fingerprint Reader.

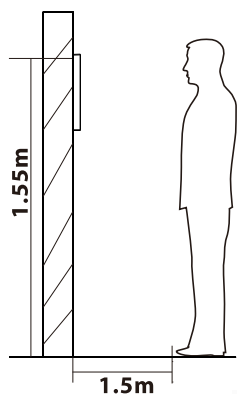
Finger Placement	Description
	Not recommended to place the finger away from the center of the Scanning Area.
	Not recommended to place the finger on the side ways.
	Not recommended to place the finger in a corner of the Scanning Area.
	Not recommended to place the finger in an uplifted position.

**Note:**

- It is recommended to use the proper finger placement during Enrollment and Verification process.
- Our company will assume no liability for recognition issues that may result from incorrect usage of the product. We reserve the right of final interpretation and modification concerning this point.

3.2 Standing Position, Facial Expression and Standing Posture

Recommended Distance



The distance between the device and the user (whose height is within 1.55m to 1.85m) is recommended to be 1.5m. Users may slightly move forward and backward to improve the quality of the captured facial images.

Recommended Facial expression



Recommended Standing postures



Note: During enrollment and verification, it is recommended to maintain natural facial expression and standing posture.

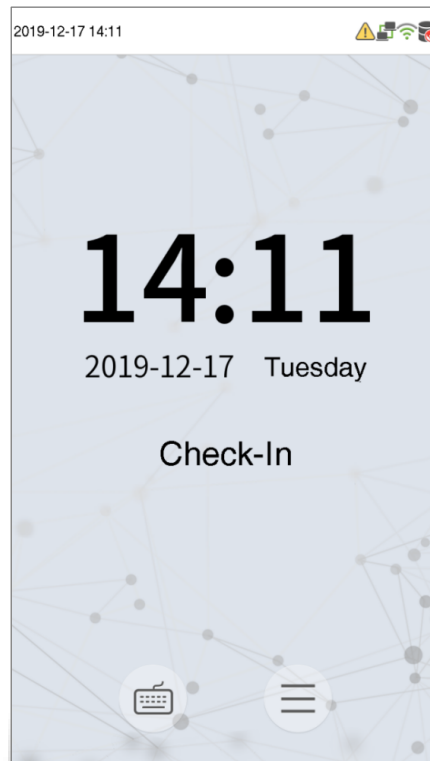
3.3 Face Registration

During registration, it is recommended to face the camera and stay still to the center of the device screen as shown below.



3.4 Standby Interface

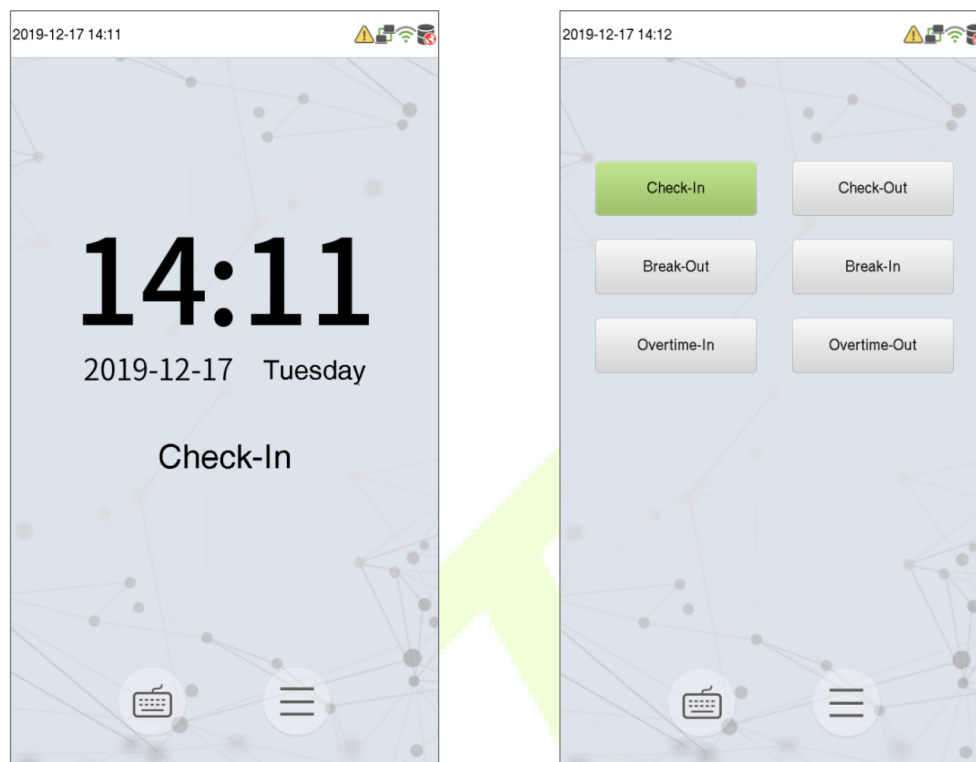
After connecting the power supply, the Device displays the following standby interface.



Notes:

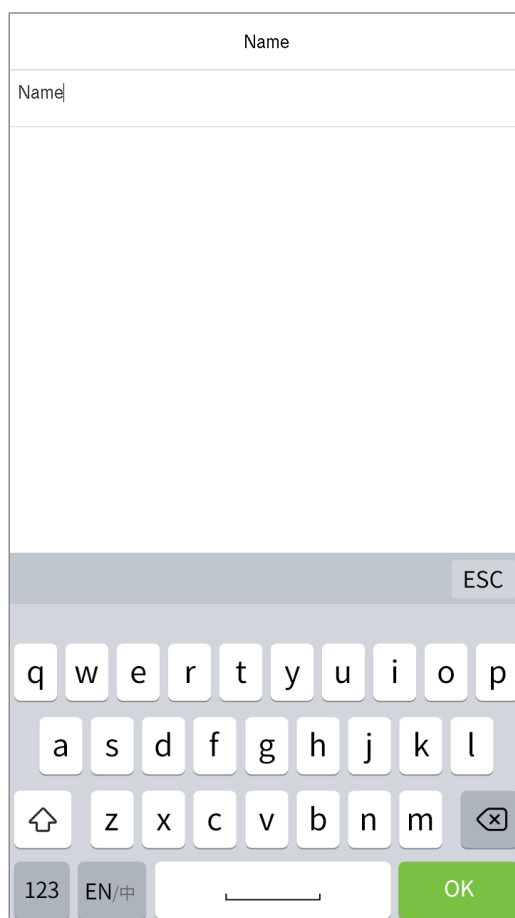
- Tap on  button to go to the User ID input interface.
- If the Super Administrator access is not set in the Device, tap on  button to go to the menu.
- If the Super Administrator is set in the Device, then it requires the Super Administrator's verification to go to the menu functions.
- For the security of the Device, it is recommended to register Super Administrator access for the first time you use the Device.

- The Device punch state can be set directly by using the screen shortcut keys.



- Tap anywhere on the screen (without tapping on the icons), to view the six punch state options as shown on the right image.
- Press the corresponding shortcut key to select the current punch state, which is shown in green. Please refer to "[7.5 Shortcut Key Mappings](#)" below for the specific operation method.

3.5 Virtual Keyboard



Note:

This device supports Chinese, English, numbers, and symbols.

- Tap **[EN]** to switch to the English keyboard;
- Tap **[123]** to switch to the numbers and symbols keyboard;
- Tap **[ABC]** to return to the alphabet keyboard.
- Tap on the input box for virtual keyboard.
- Tap **[ESC]** to exit the input.

3.6 Verification Mode

The Biometric matching process can be categorized as, One-to-many or “Identification” (1:N), and one-to-one or “Verification” (1:1). Below is a description of each matching type and how its features are described.

1:N Identification Process

A one-to-many (1:N) biometric identification process instantly compares the person’s captured biometric template against ALL stored biometric templates in the system.

1:1 Verification Process

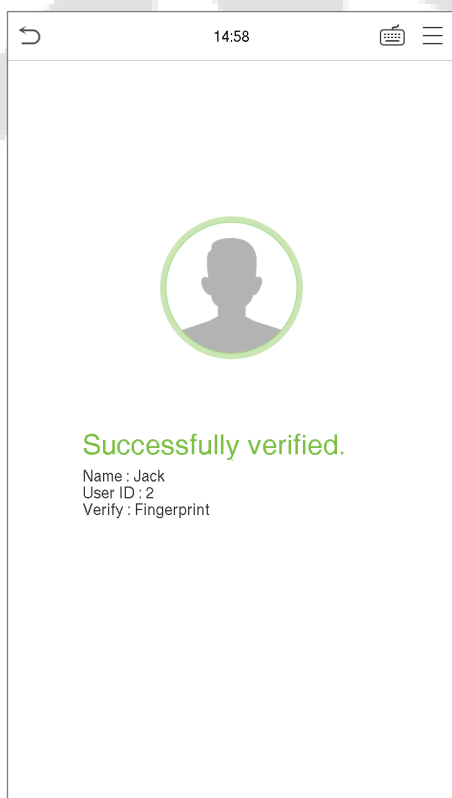
1:1 biometric verification process authenticates a person’s identity by comparing the captured biometric template with a biometric template of that person pre-stored in the database.

3.6.1 Fingerprint Verification

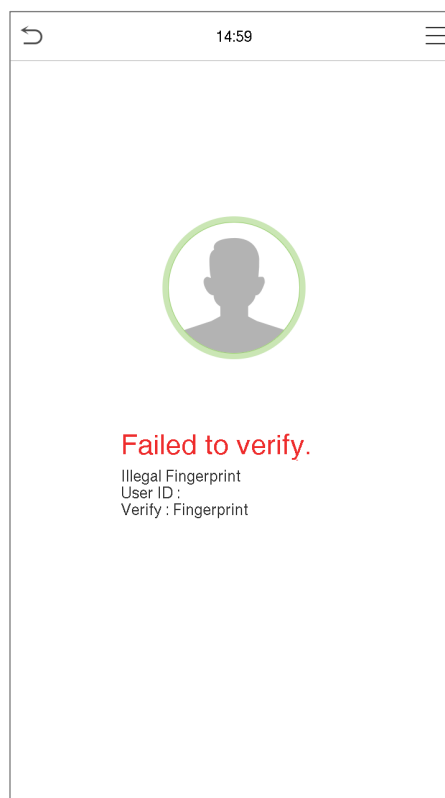
1: N fingerprint Identification Process

- This method compares the fingerprint that is being pressed and scanned onto the fingerprint reader with all of the fingerprint data that is stored in the device.
- Once the user presses his/her finger on the fingerprint scanner the device will go to the fingerprint authentication mode. It is essential to follow the proper way to place the finger on the fingerprint sensor.

Successful Verification

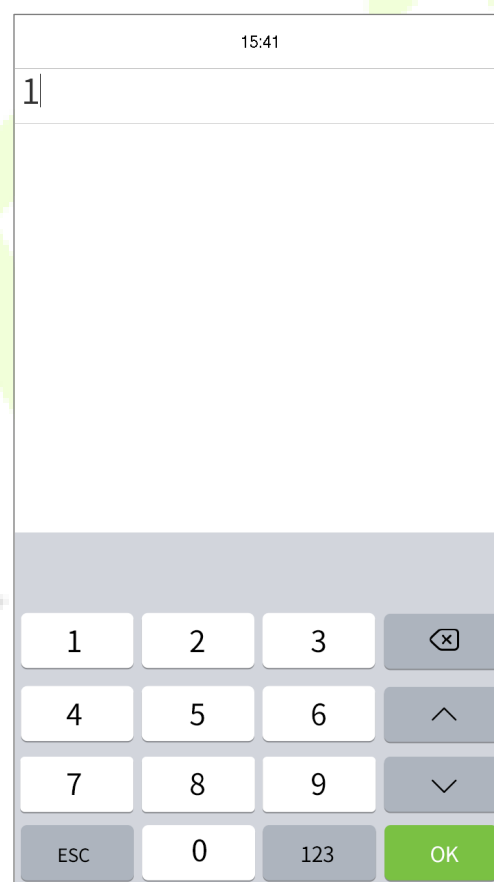
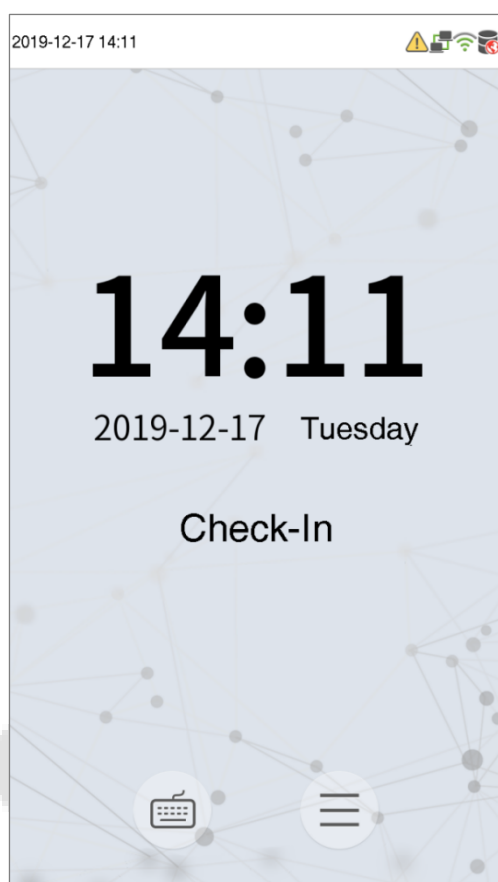


Failed Verification

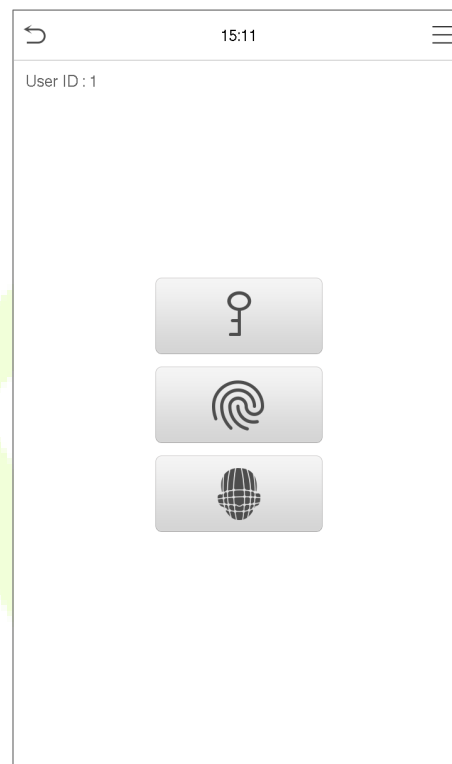
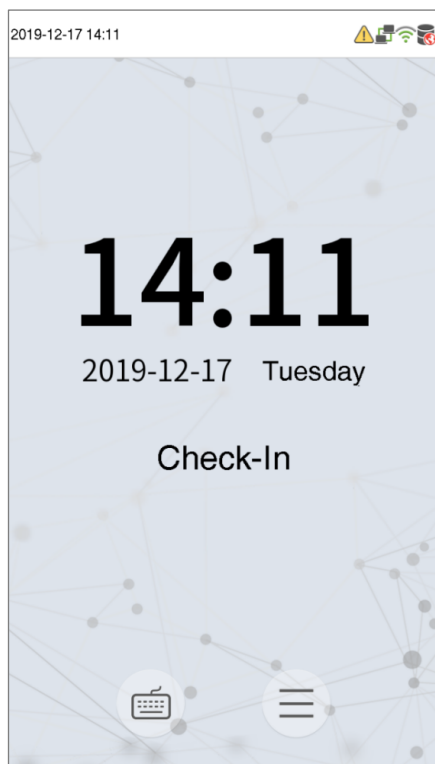


1: 1 Fingerprint Verification Process

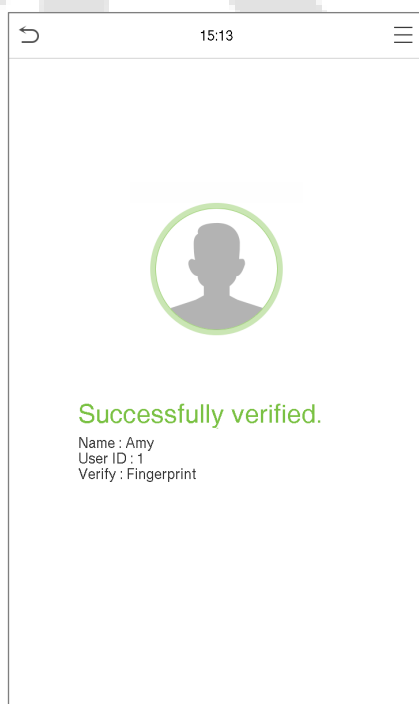
- This method compares the fingerprint that is being pressed onto the fingerprint reader with the fingerprints that are linked to the specific User ID input via the virtual keyboard.
- Users may try verifying their identities with 1:1 verification mode when they are not able to access with 1: N authentication process.
- On the Main screen, tap on  button to go to the 1:1 fingerprint verification mode.
- On the screen, enter the user ID and tap **OK**.



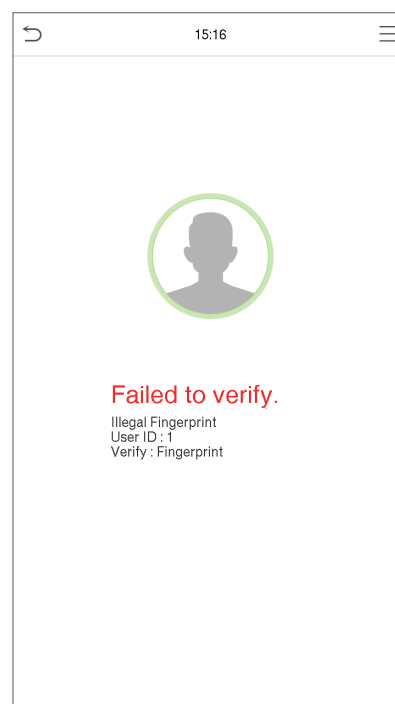
- If the user has registered face and password in addition to the fingerprint, then the verification method is set to fingerprint/ password/ face verification and the below screen will appear in the Device.
- Tap on  fingerprint icon to go to the fingerprint verification mode and press the fingerprint to verify.



Successful Verification

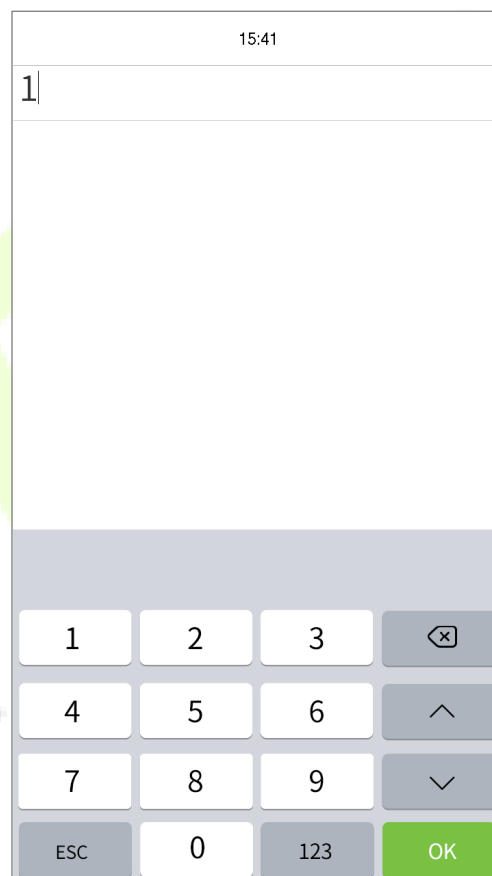
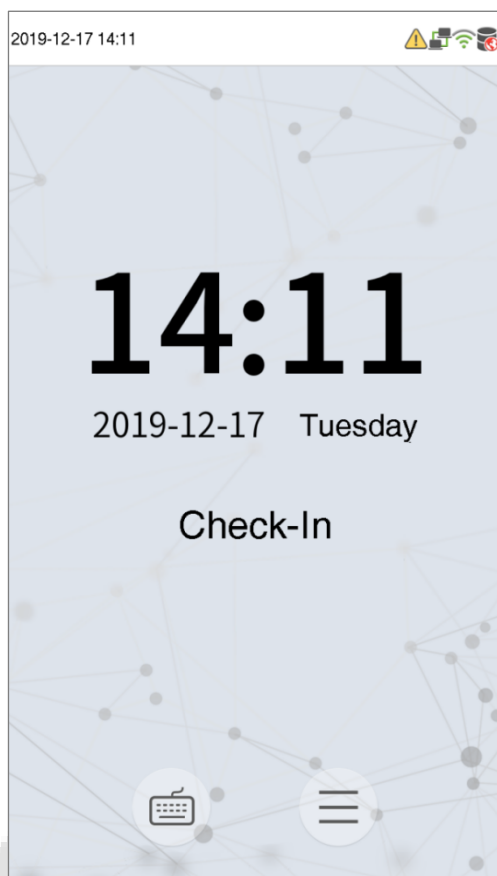


Failed Verification

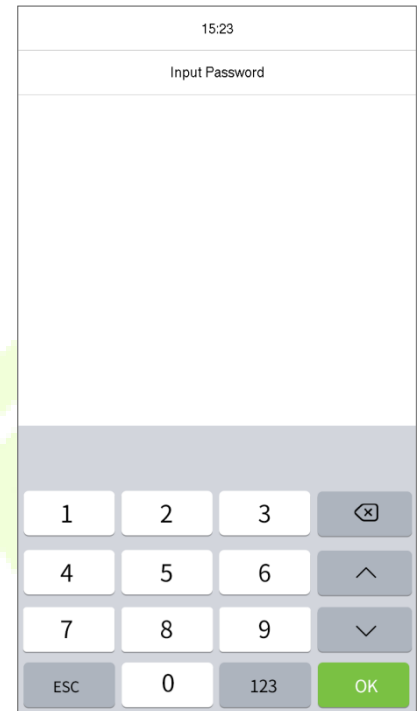
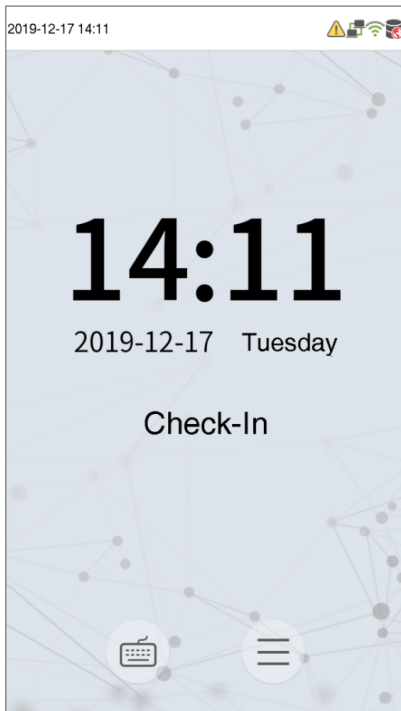


3.6.2 Password Verification

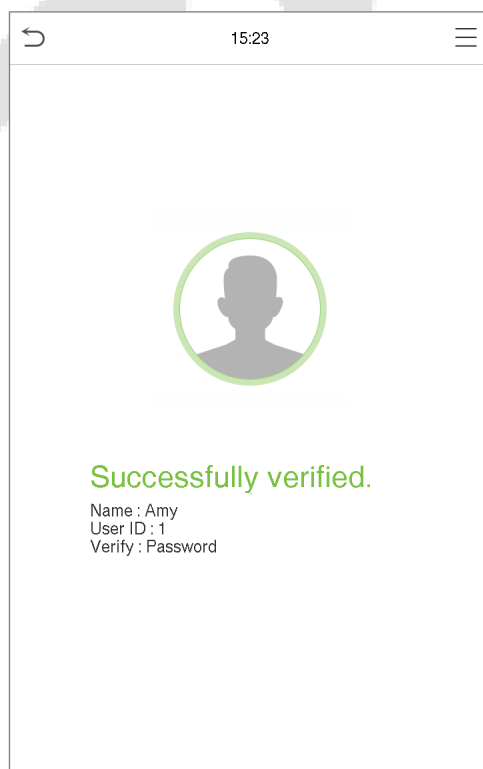
- This method compares the entered password with the registered User ID and password.
- On the Menu screen, tap on  button to go to the 1:1 password verification mode.
- On the input screen, enter the user ID and press **OK**.



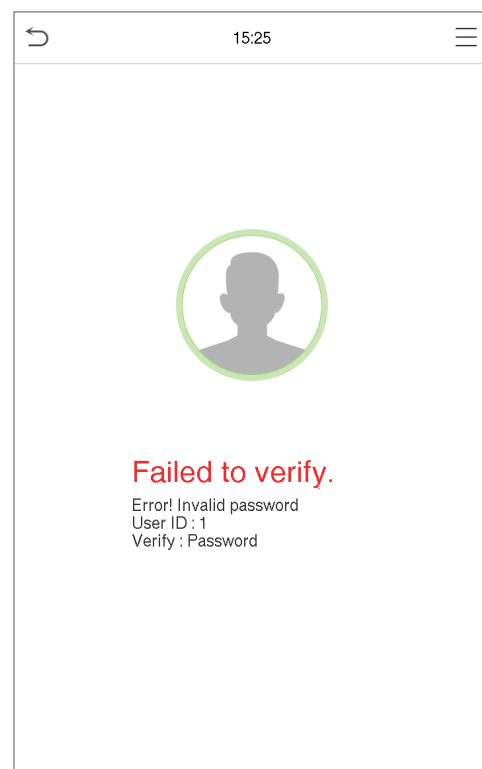
- If the user has registered face and fingerprint in addition to the password, then the verification method is set to fingerprint/ password/ face verification and the below screen will appear in the Device.
- Tap on  the button to go to the password verification mode, then enter the password, and then tap **OK**.



Successful Verification



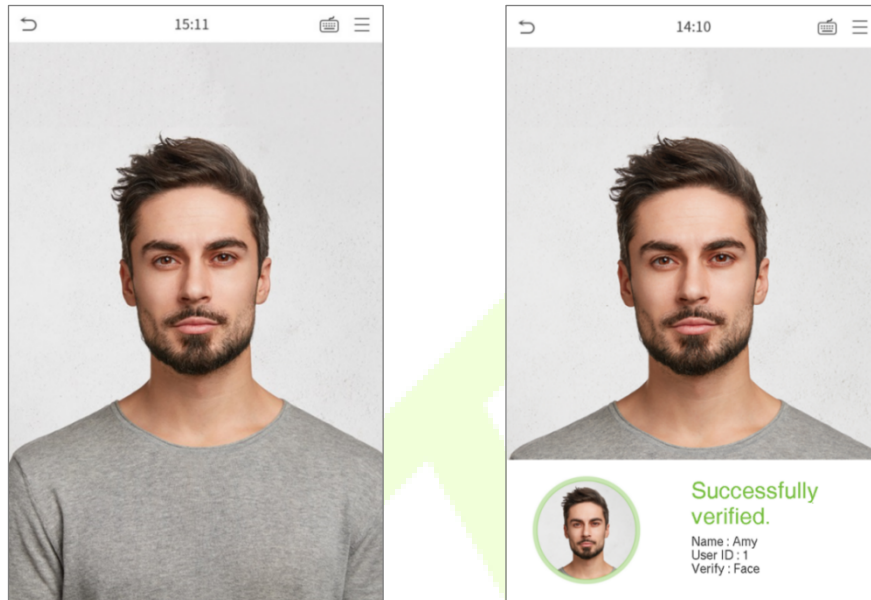
Failed Verification



3.6.3 Facial Verification

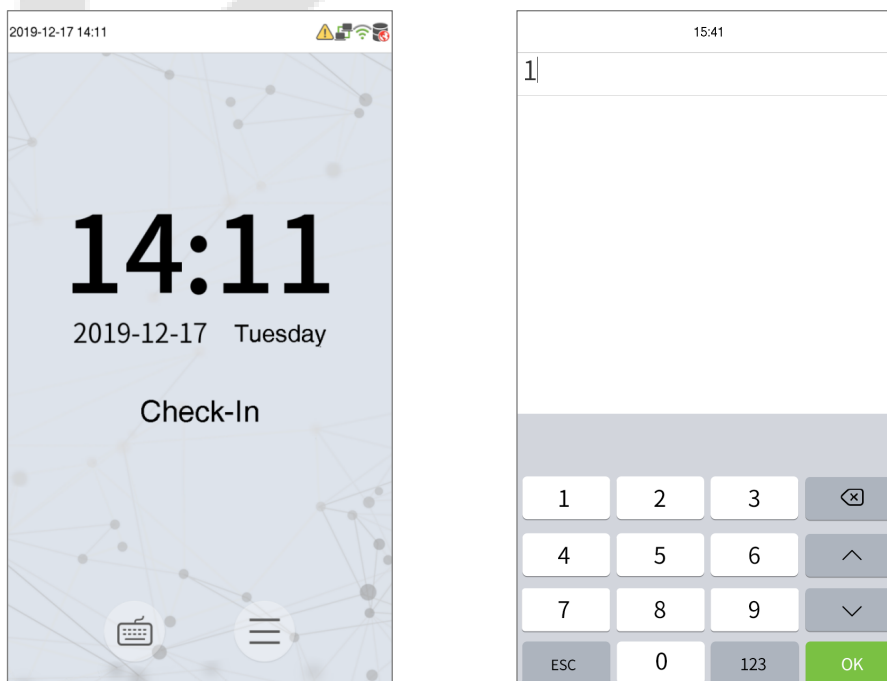
1:N Face Identification

- This method compares the acquired facial images with all the face data registered in the device.
- The following is the prompt message of the comparison result.

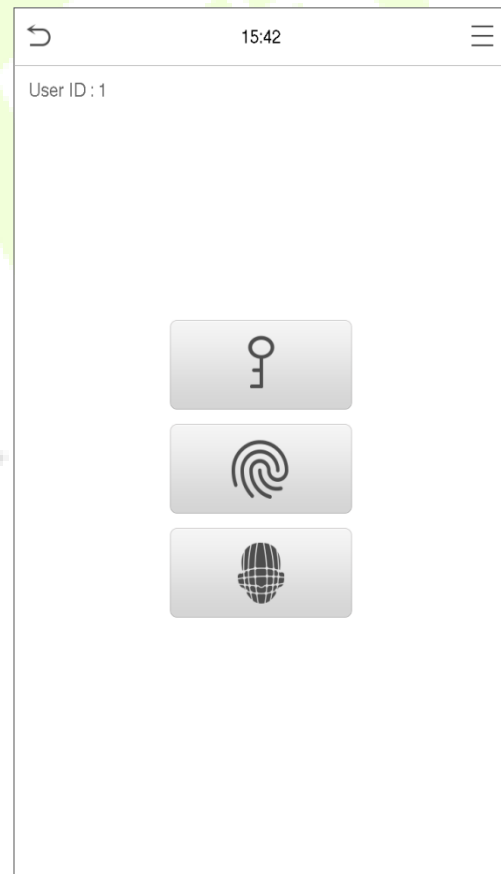
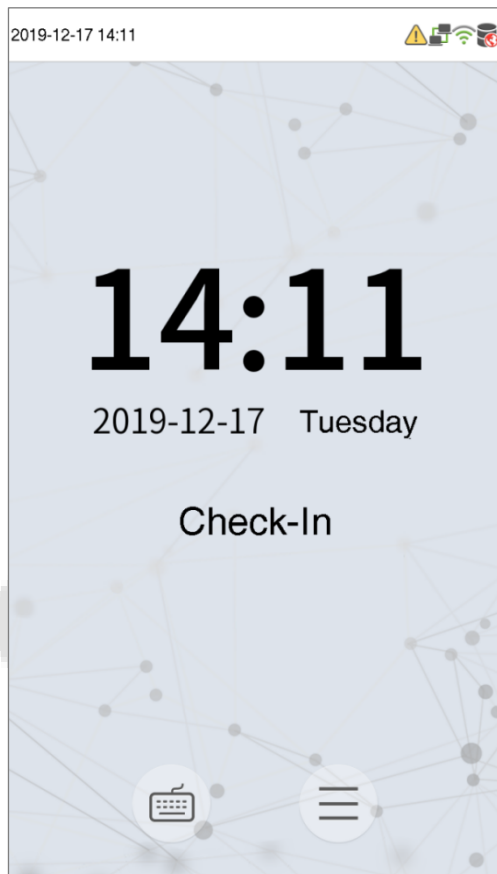


1:1 Face Verification

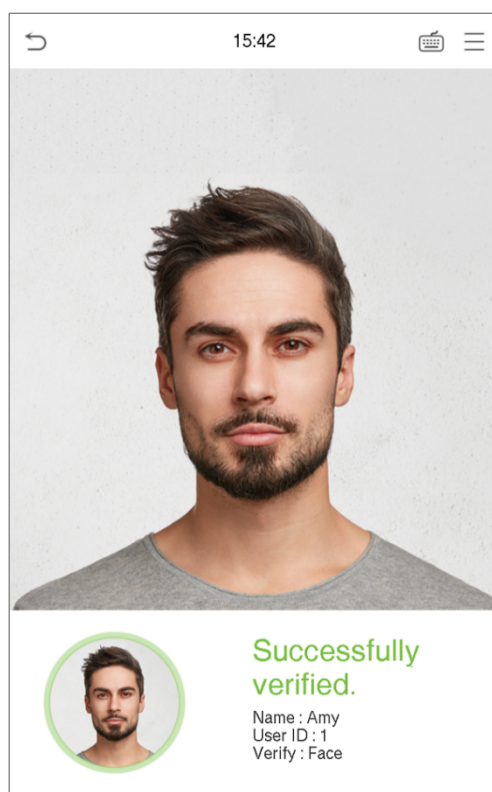
- This method compares the face captured by the camera with the facial template related to the entered user ID.
- On the main interface, tap on  the button to go to the 1:1 facial verification mode.



- Enter the user ID and click **OK**.
- If the user has registered password and fingerprint in addition to face, then the verification method is set to fingerprint/ password/ face verification and the below screen will appear in the Device.
- Tap on  the button to go to the face verification mode.
- If the user has registered face and fingerprint in addition to the password, then the verification method is set to fingerprint/ password/ face verification and the below screen will appear in the Device.
- Tap on  the button to go to the password verification mode, then enter the password, and then tap **OK**.



After successful verification, the prompt message "successfully verified" will be displayed.



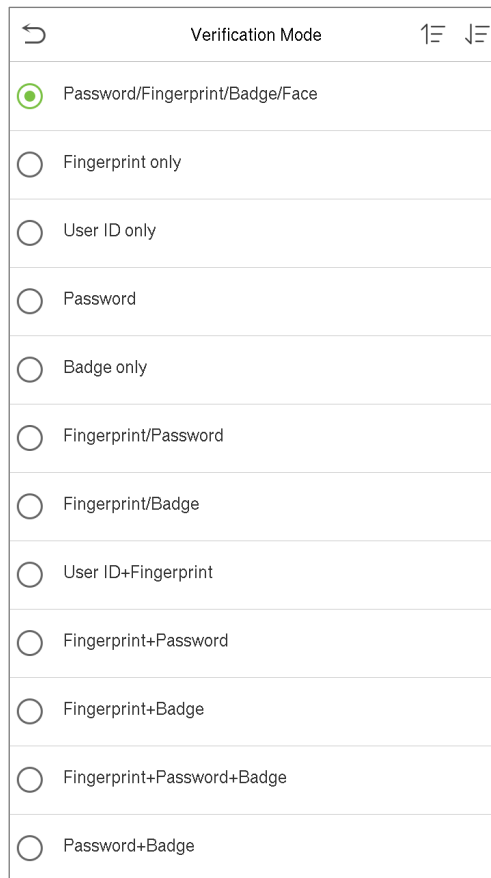
If the verification is failed, the prompt message "Please adjust your position!" will be displayed.

3.6.4 Combined Verification

To increase the security, this device provides the option of using multiple forms of verification mode. In this Device, a total of 11 different verification combinations can be used.

Combined Verification Symbol Definition

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



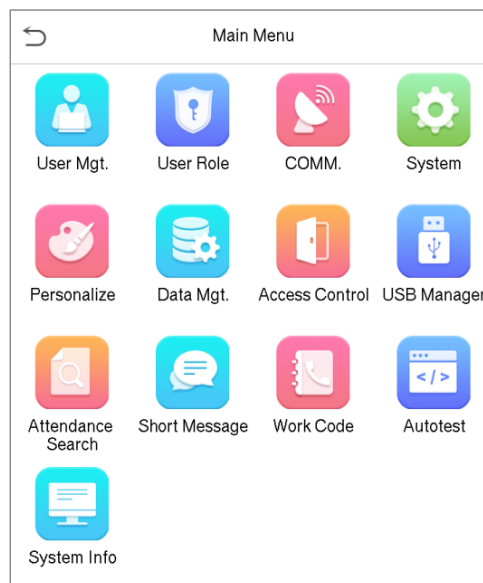
Verification Mode	
☒	Password/Fingerprint/Badge/Face
☐	Fingerprint only
☐	User ID only
☐	Password
☐	Badge only
☐	Fingerprint/Password
☐	Fingerprint/Badge
☐	User ID+Fingerprint
☐	Fingerprint+Password
☐	Fingerprint+Badge
☐	Fingerprint+Password+Badge
☐	Password+Badge

Procedure to set for Combined Verification Mode

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

4 Main Menu

- On the **Standby** interface, tap on  button to go to the **Main Menu**:



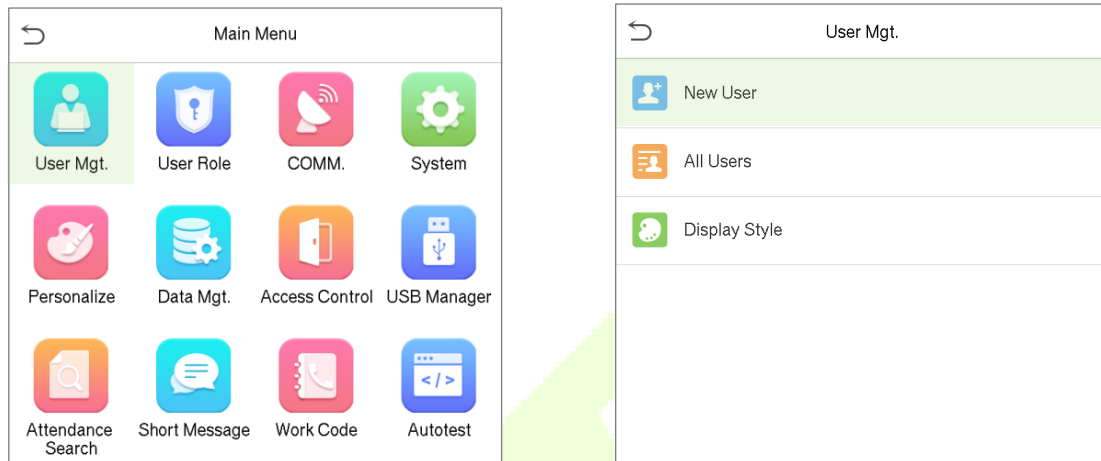
Menu Operations

Menu	Descriptions
User Mgt.	To Add, Edit, View, and Delete the basic information about a User.
User Role	To set the permission scope of the custom role, that is, to set the access rights to operate the system.
COMM.	To set the relevant Network parameters, PC connection, Cloud Server and Wiegand details.
System	To set parameters related to the system, including date & time, attendance/access logs setting, face, fingerprint parameters, reset to factory and USB upgrade.
Personalize	To customize settings of interface display, voice, bell, punch state options and shortcut key.
Data Mgt.	To delete all relevant data in the device.
Access Control	To set the parameters of the lock and the relevant access control device.
USB Manager	To upload or download specific data from a USB drive.
Attendance Search	Query the specified attendance record, check attendance photos and blacklist photos.
Short Message	Add/check/edit/delete public and personal messages. Set options.
Work Code	To mark different work categories, facilitating user attendance check.
Autotest	To automatically test whether each module functions properly, including the LCD, voice, fingerprint sensor, camera and clock RTC.
System Info	To view data capacity, device and firmware information of the current device.

5 User Management

5.1 User Registration

- On the **Main** menu, tap **User Mgt.**, and then tap **New User** to add a new User.



5.1.1 User ID and Name

- On the **New User** interface, enter the **User ID** and **Name**.

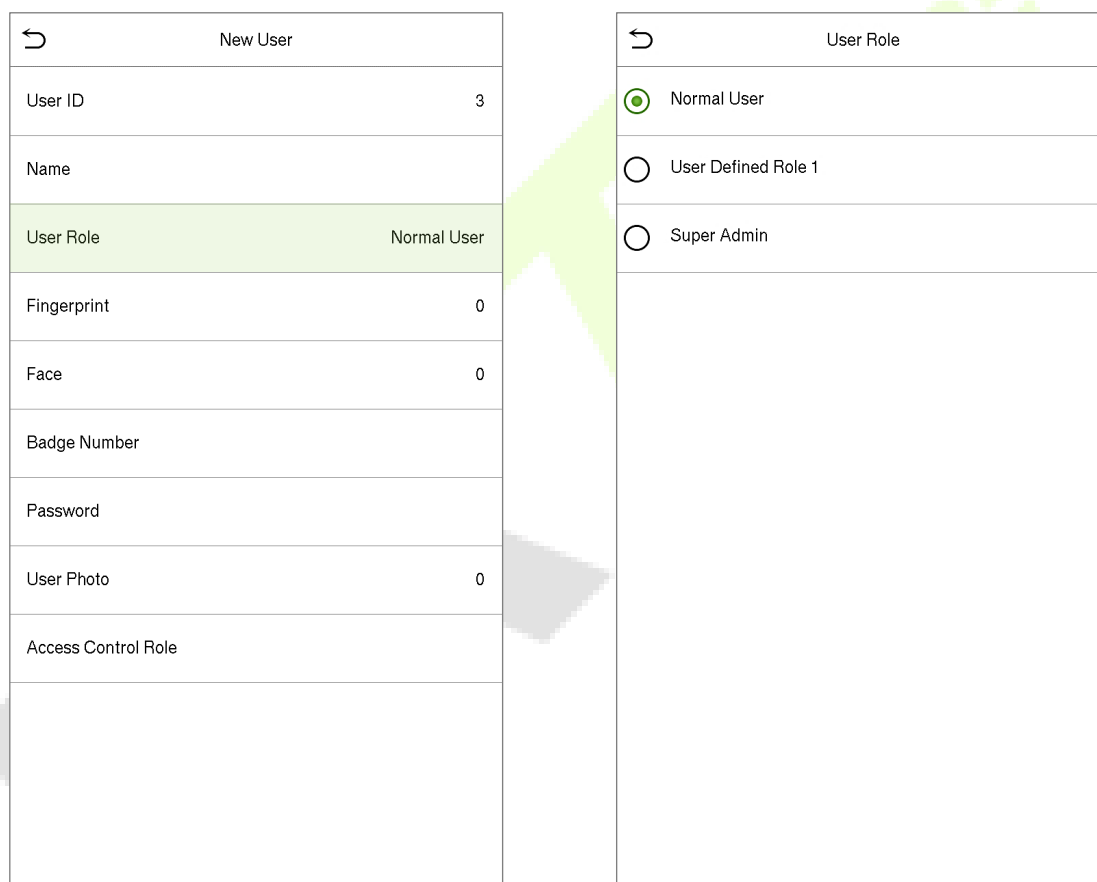
New User	
User ID	3
Name	
User Role	Normal User
Fingerprint	0
Face	0
Badge Number	
Password	
User Photo	0
Access Control Role	

Notes:

- A user name can contain 17 characters.
- The user ID can contain 1-9 digits by default.
- During the initial registration, you can modify your ID, which cannot be modified after registration.
- If a message "Duplicated ID" pops up, it is recommended to choose another User ID.

5.1.2 User Role

- On the New User interface, tap on **User Role** to set the role for the user as either **Normal User** or **Super Admin**.
- **Super Admin:** The Super Administrator owns all management privileges in the Device.
- **Normal User:** If the Super Admin is already registered in the Device, then the Normal Users will not have the privileges to manage the system and can only access authentication verifications.
- **User Defined Roles:** The Normal User can also be set with **User Defined Role** which are the custom roles that can be set to the Normal User.



New User	
User ID	3
Name	
User Role	Normal User
Fingerprint	0
Face	0
Badge Number	
Password	
User Photo	0
Access Control Role	

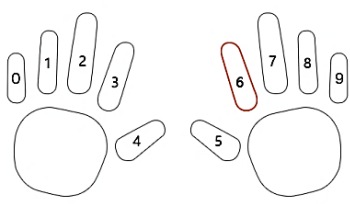
User Role	
☒	Normal User
☐	User Defined Role 1
☐	Super Admin

Note: If the selected user role is the Super Admin, then only the Super Admin can provide the identity authentication to access the Main Menu. The authentication is based on the [verification](#) method(s) that the Super Administrator has registered.

5.1.3 Fingerprint

- On the **New User** interface, tap on **Fingerprint** to go to the fingerprint registration page.
- On the **Enroll Fingerprint** interface, select the finger to be enrolled.

New User	
User ID	3
Name	
User Role	Normal User
Fingerprint	0
Face	0
Badge Number	
Password	
User Photo	0
Access Control Role	

Enroll Fingerprint	
	
Please select the finger to be enrolled	

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

Enroll Fingerprint(3-6)	
Enrolled successfully	
	
1 2 3	

5.1.4 Face

- On the **New User** interface, tap on **Face** to enter the face registration page.
- During the Face registration process, the user should look the camera and stay still as shown below.

New User	
User ID	3
Name	
User Role	Normal User
Fingerprint	0
Face	0
Badge Number	
Password	
User Photo	0
Access Control Role	



5.1.5 Badge Number

- On the **New User** interface, tap on **Badge Number** to go to the badge number registration page.
- On the **Enroll Badge Number** interface, the user should swipe the badge on the IC card reader to register the card number.

New User	
User ID	3
Name	
User Role	Normal User
Fingerprint	0
Face	0
Badge Number	
Password	
User Photo	0

Enroll Badge Number
Please swipe badge


5.1.6 Password

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

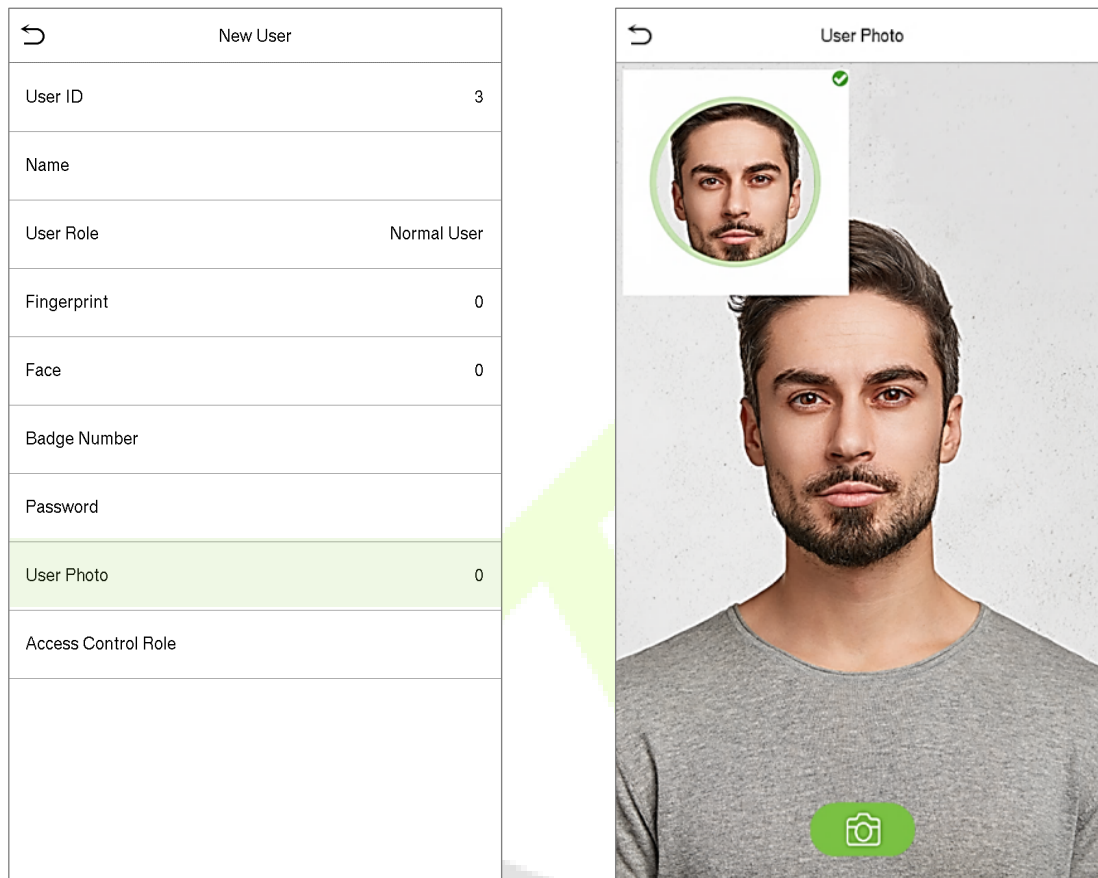
New User	
User ID	3
Name	
User Role	Normal User
Fingerprint	0
Face	0
Badge Number	
Password	
User Photo	0
Access Control Role	

Password
1 2 3 ⌫ 4 5 6 ⤴ 7 8 9 ⤵ ESC 0 123 OK

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

5.1.7 User photo

- On the **New User** interface, tap on **User Photo** to go to the User photo registration page.



- When a user registered with a photo passes the authentication, the registered photo will be displayed.
- Tap **User Photo**, tap the camera button to snap a photo. The system will return to the New User interface after the photo is being clicked.

Note: While registering for face, the system will automatically capture the image of the user and set it as the user photo by default. Hence, even if the user did not want to register a user photo, the system will automatically set the captured picture as the default User photo.

5.1.8 Access Control Role

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

- On the **New User** interface, tap on **Access Control Role** to go to the Access Control interface.

New User	
User ID	3
Name	
User Role	Normal User
Fingerprint	0
Face	0
Badge Number	
Password	
User Photo	0
Access Control Role	

Access Control	
Access Group	1
Verification Mode	Apply Group Mode
Duress Fingerprint	Undefined
Apply Group Time Period	☒

Set the Access Group

- On the **Access Control Role**, tap on **Access Group** to assign the registered users to different groups for better management.

Access Control	
Access Group	1
Verification Mode	Apply Group Mode
Duress Fingerprint	Undefined
Apply Group Time Period	☒

- New users will be added to Group 1 by default, which can be reassigned to other required groups.
- The device supports up to 99 access control groups.

Set the Verification Mode

- On the **Access Group** interface, tap on **Verification Mode** to set the verification type for the user.

Access Control	
Access Group	1
Verification Mode	Apply Group Mode
Duress Fingerprint	Undefined
Apply Group Time Period	☒

Verification Mode	
☒	Apply Group Mode
☐	Password/Fingerprint/Badge/Face
☐	Fingerprint only
☐	User ID only
☐	Password
☐	Badge only
☐	Fingerprint/Password
☐	Fingerprint/Badge
☐	User ID+Fingerprint
☐	Fingerprint+Password
☐	Fingerprint+Badge
☐	Fingerprint+Password+Badge

- On the **Verification Mode** interface, select the required verification type from the list.

Duress Fingerprint

- On the Access Control Interface, tap on Duress Fingerprint to go to the duress fingerprint page.
- The user may specify one or more fingerprints to register as duress fingerprint(s). Hence, once the user presses the corresponding finger on the sensor, and if the verification is successful, then the system will immediately generate the alarm.

Access Control	
Access Group	1
Verification Mode	Apply Group Mode
Duress Fingerprint	Undefined
Apply Group Time Period	☒

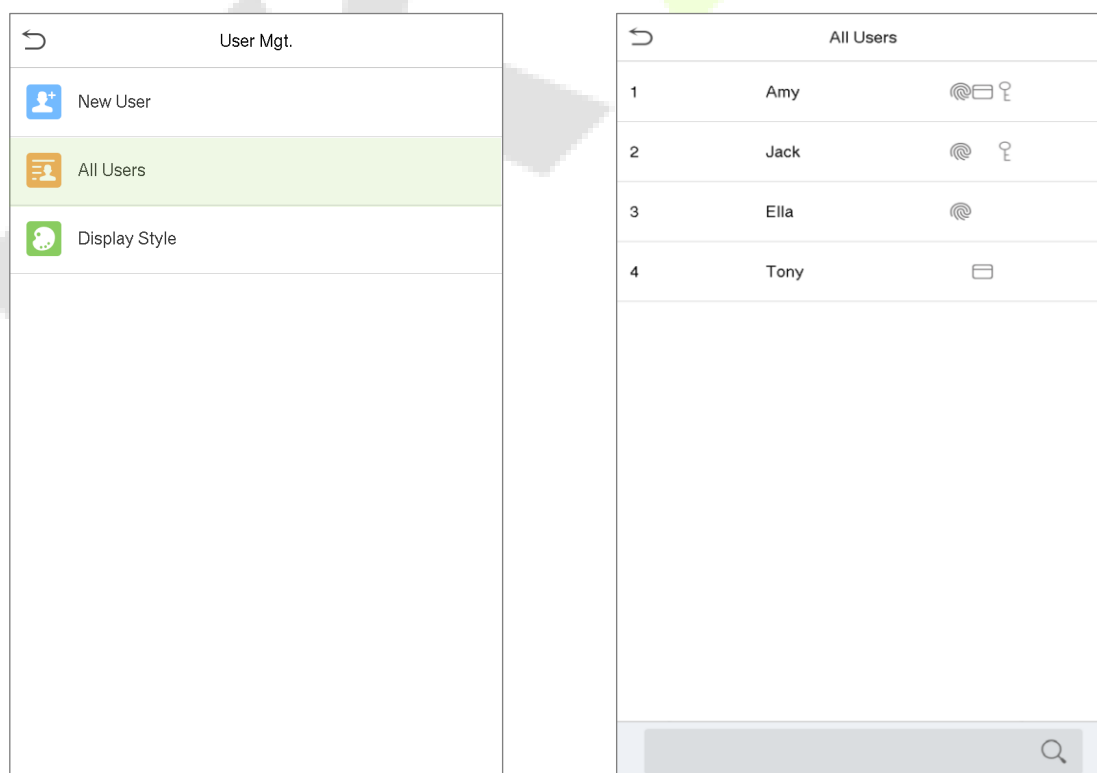
Apply Group Time Period

On the **Access Control** interface, toggle on **Apply Group Time Period** to enable or disable the group time period for each access group.

Access Control	
Access Group	1
Verification Mode	Apply Group Mode
Duress Fingerprint	Undefined
Apply Group Time Period	☒

5.2 Search for Users

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



5.3 Edit User

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

All Users		User : 1 Amy		Edit : 1 Amy	
1	Amy	Edit		User ID	1
2	Jack	Delete		Name	Amy
3	Ella			User Role	Normal User
4	Tony			Fingerprint	1
				Face	0
				Badge Number	783560236
				Password	*****
				User Photo	0
				Access Control Role	

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

5.4 Delete User

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

Delete Operations

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

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

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

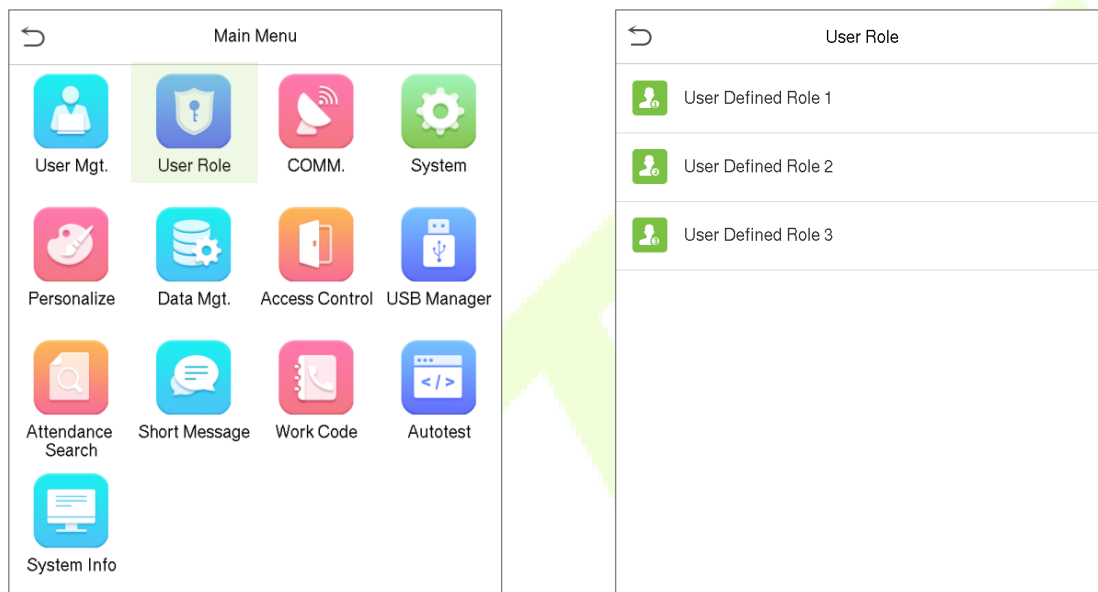
Delete Card Number Only: Deletes the card number information of the selected user.

User : 2 Jack	Delete : 2 Jack
Edit	Delete User
Delete	Delete Fingerprint Only
	Delete Password Only
	Delete Badge Number Only

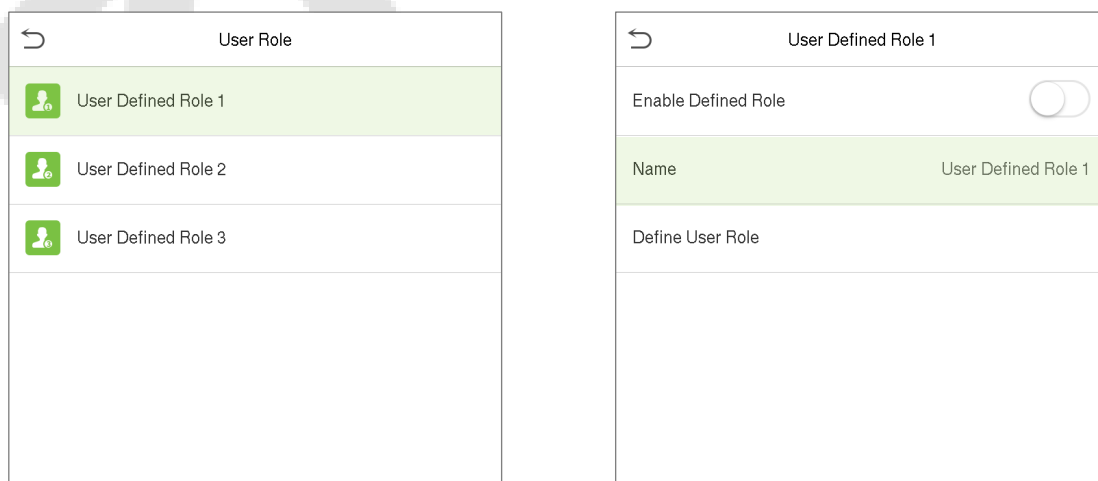
6 User Role

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

- On the **Main** menu, tap **User Role**, and then tap on the **User Defined Role** to set the user defined permissions.
- The permission scope of the custom role can be set up to 3 roles, that is, the custom operating scope of the menu functions of the user.



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



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

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

The image displays two screenshots of the G4L user management interface, connected by a large green arrow pointing from left to right.

Left Screenshot: User Defined Role 1

User Defined Role 1	
☒ User Mgt.	☒ New User
☒ Comm.	☒ All Users
☒ System	☒ Display Style
☐ Personalize	
☐ Data Mgt.	
☒ Access Control	
☐ USB Manager	
☐ Attendance Search	
☐ Short Message	
☐ Work Code	
☐ Autotest	
☐ System Info	

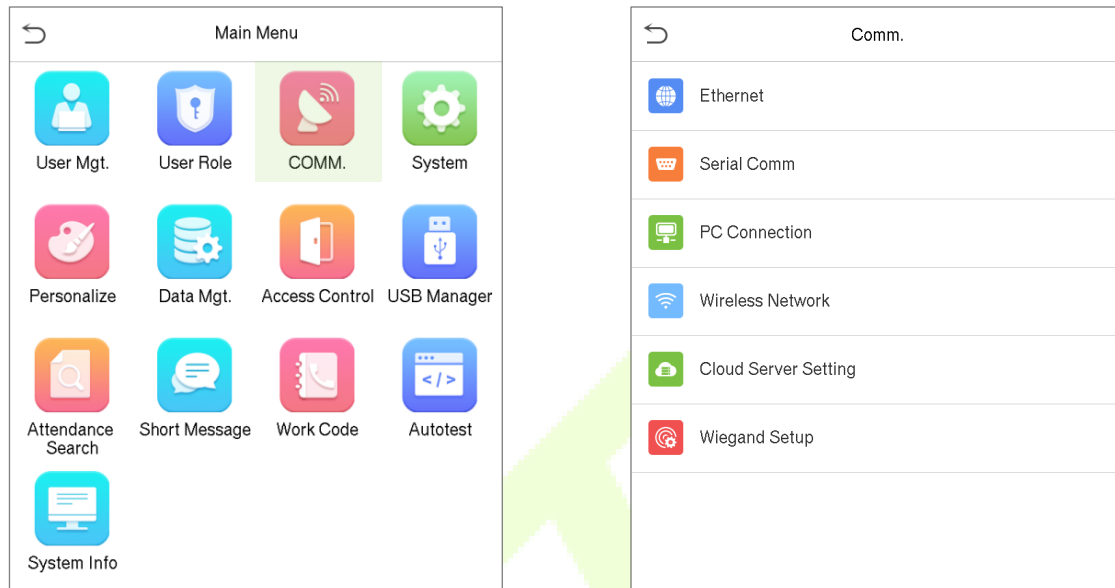
Right Screenshot: User Role

User Role
☒ Normal User
☐ User Defined Role 1
☐ Super Admin

Note: If the User Role is enabled for the Device, tap on **User Mgt. > New User > User Role** to assign the created roles to the required users. But if there is no super administrator registered in the Device, then the device will prompt "Please enroll super admin first!" when enabling the User Role function.

7 Communication Settings

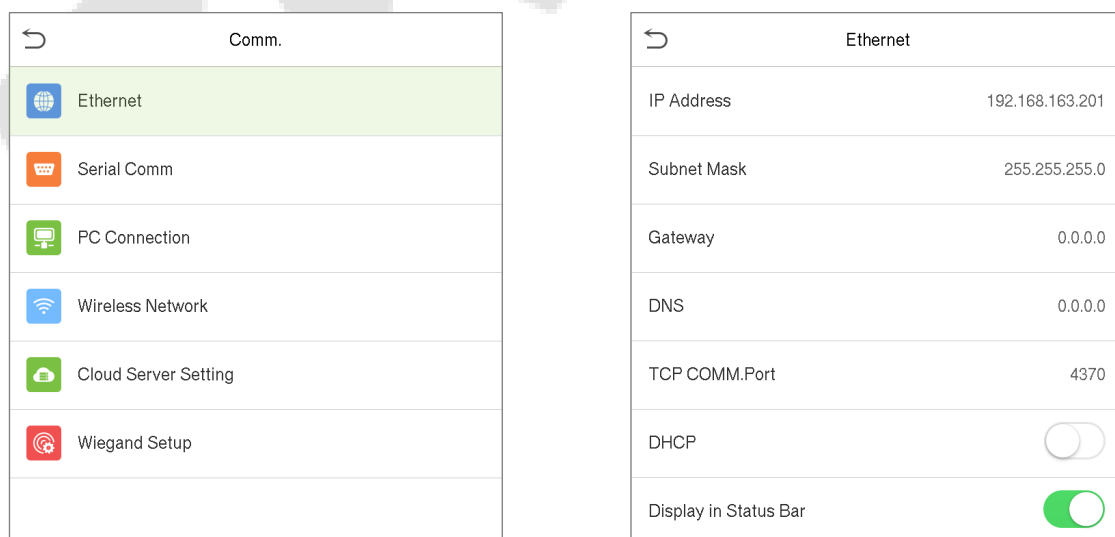
- On the **Main Menu**, tap **COMM.** to set the Ethernet, PC Connection, Cloud Server and Cloud Service parameters



7.1 Network Settings

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

- On the **Comm.** Interface, tap **Ethernet** to configure the settings.



Function Description

Function Name	Description
IP Address	The default IP address is 192.168.1.201. Can be modified according to the network availability.

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

7.2 Serial Comm

Serial Comm function facilitates to establish communication with the device through a serial port number using RS485 communication.

- On the **Comm.** Interface, tap **Serial Comm** to configure the serial port settings.

The image displays three sequential screenshots of the device's configuration interface for Serial Communication.

- First Screenshot (Comm. menu):** Shows a list of communication options: Ethernet, Serial Comm (highlighted), PC Connection, Wireless Network, Cloud Server Setting, and Wiegand Setup.
- Second Screenshot (Serial Comm settings):** Shows the configuration for the selected Serial Comm. It includes a 'Serial Port' dropdown menu set to 'Master Unit' and a 'Baudrate' field set to '115200'.
- Third Screenshot (Serial Port selection):** Shows the options for the Serial Port: 'no using', 'RS485(PC)', and 'Master Unit' (which is selected with a green dot).

Function Description

Function Name	Description
Serial port	Disable: Do not communicate with the device through the serial port. RS485(PC): Communicates with the device through RS485 serial port. Master Unit: When RS485 is used as the function of "Master unit", the device will act as a master unit, and it can be connected to RS485 fingerprint & card reader.

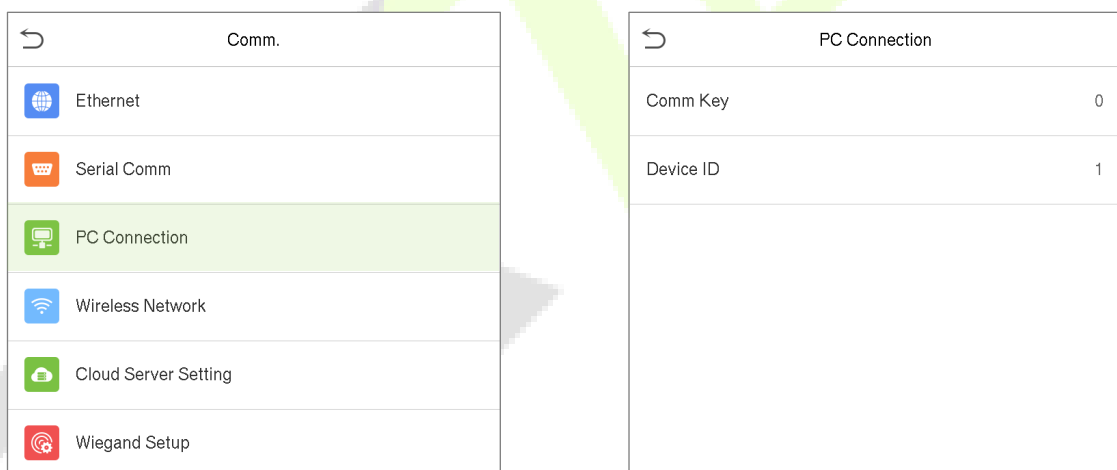
Baud Rate	The rate at which the data is communicated with PC. There are 4 options of baud rate: 115200 (default), 57600, 38400, and 19200. The higher is the baud rate, the faster is the communication speed, but also the less reliable. Hence, a higher baud rate can be used when the communication distance is short; when the communication distance is long, choosing a lower baud rate would be more reliable.
------------------	--

7.3 PC Connection

Comm Key facilitates to improve the security of data by setting the communication between device and PC.

Once the Comm Key is set, its connection password must be provided before the device gets connected to the PC software.

- On the **Comm.** Interface, tap **PC Connection** to configure the communication settings.



Function Description

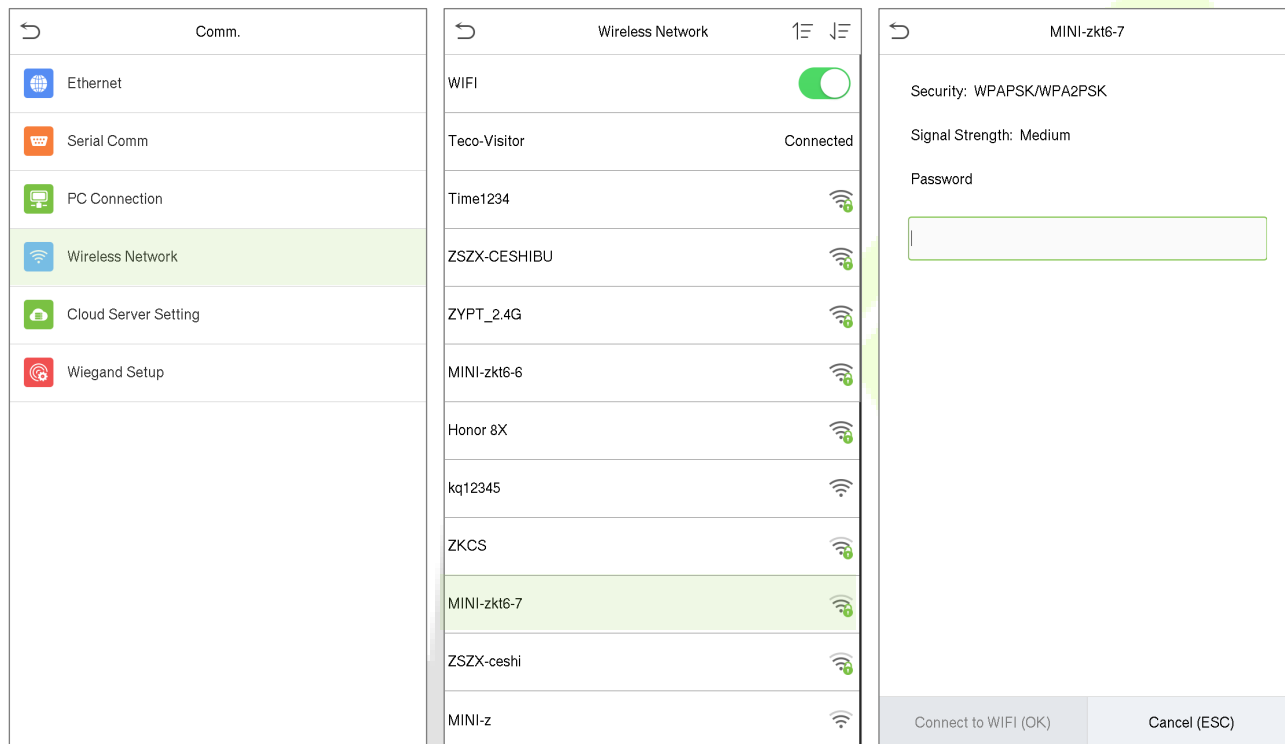
Function Name	Descriptions
Comm Key	The default password is 0, and can be modified. The Comm Key can contain 1-6 digits.
Device ID	Identity number of the device, which ranges between 1 and 254. If the communication method is RS232/RS485, you need to input this device ID in the software communication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

7.4 Wireless Network

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

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

- On the **Comm.** Interface, tap **Wireless Network** to configure WIFI settings.



Search the WIFI Network

- Once the Wi-Fi is turned on, the device will search for the available WIFI within the network range.
- Tap on the appropriate WiFi name from the available list, and input the correct password in the password interface, and then tap **Connect to WIFI (OK)**.
- When the WIFI is connected successfully, the initial interface will display the Wi-Fi  logo.

Add WIFI Network Manually

- The WIFI can also be added manually if the required WIFI is not displayed on the list.
- On the **Wireless Network** interface, tap on **Add WIFI Network** to provide the relevant parameters (It is essential that the added network must exist).

Wireless Network	
WIFI	☒
MINI-zkt6-7	Connected
Add WIFI Network	
Advanced	

Add WIFI Network	
SSID	
Network Mode	INFRA
Auth. Mode	OPEN

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

Advanced Setting

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

Wireless Network	
WIFI	☒
MINI-zkt6-7	Connected
Add WIFI Network	
Advanced	

Ethernet	
DHCP	☒
IP Address	10.1.20.25
Subnet Mask	255.255.252.0
Gateway	0.0.0.0

Function Description

Function Name	Descriptions
DHCP	Dynamic Host Configuration Protocol, which is to dynamically allocate IP address for clients via server. If the DHCP is enabled, then the IP cannot be set manually.
IP Address	IP address for WIFI network, the default is 0.0.0.0. Can be modified according to the network availability.
Subnet Mask	The default Subnet Mask is 255.255.255.0. Can be modified according to the network availability.
Gateway	The default Gateway address is 0.0.0.0. Can be modified according to the network availability.

Note: WIFI function is optional, only products with the built-in WIFI module are equipped with WIFI function. Please contact our technical support for any further information.

7.5 Cloud Server Setting

- On the **Comm.** Interface, tap **Cloud Server Setting** to connect with the ADMS server.

Comm.

Ethernet
Serial Comm
PC Connection
Wireless Network
Cloud Server Setting
Wiegand Setup

Cloud Server Setting

Server ModeADMS
Enable Domain Name
Server Address0.0.0.0
Server Port8081
Enable Proxy Server

Function Description

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

7.6 Wiegand Setup

- On the **Comm.** Interface, tap **Wiegand Setup** to set the Wiegand input and output parameters.

Comm.

Ethernet
Serial Comm
PC Connection
Wireless Network
Cloud Server Setting
Wiegand Setup

Wiegand Setup

Wiegand Input
Wiegand Output

7.6.1 Wiegand input

Wiegand Setup
Wiegand Input
Wiegand Output

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

Function Description

Function Name	Descriptions
Wiegand Format	Value ranges from 26 bits, 34 bits, 36 bits, 37 bits, and 50 bits.
Wiegand Bits	Number of bits of Wiegand Data.
Pulse Width(us)	The value of the pulse width sent by Wiegand is 100 microseconds by default, and can be modified within the range of 20 to 100 microseconds.
Pulse Interval(us)	The default value is 1000 microseconds, and can be modified within the range of 200 to 20000 microseconds.
ID Type	Select the ID type as either User ID or Card number.

Various Common Wiegand Format Description:

Wiegand Format	Description
Wiegand26	EEEEEEEEEEEEEEEEEEEEEEEEEEEE Consists of 26 bits 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. 2nd to 25th bits are the card numbers.
Wiegand26a	ESSSSSSSSSSSSSSSSSSSSSSSSSS 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. 2nd to 9th bits are the site codes, while the 10th to 25th bits are the card numbers.
Wiegand34	EEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEE 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. 2nd to 25th bits are the card numbers.
Wiegand34a	ESSSSSSSSSSSSSSSSSSSSSSSSSSSS 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. 2nd to 9th bits are the site codes, while the 10th to 25th bits are the card numbers.

Wiegand36	OFFFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCMME 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. 2nd to 17th bits are the device codes. The 18th to 33rd bits are the card numbers, and the 34th to 35th bits are the manufacturer codes.
Wiegand36a	EEEEFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCO 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. 2nd to 19th bits are the device codes, and the 20th to 35th bits are the card numbers.
Wiegand37	OMMMMMSSSSSSSSSSSSCCCCCCCCCCCCCCCCCE 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. 2nd to 4th bits are the manufacturer codes. 5th to 16th bits are the site codes, and the 21st to 36th bits are the card numbers.
Wiegand37a	EMMMFFFFFFFFFSSSSSSCCCCCCCCCCCCCCCCCO Consists of 37 bits of binary code. The 1st bit is the even parity bit of the 2nd to 18th bits, while the 37th bit is the odd parity bit of the 19th to 36th bits. 2nd to 4th bits are the manufacturer codes. 5th to 14th bits are the device codes, and 15th to 20th bits are the site codes, and the 21st to 36th bits are the card numbers.
Wiegand50	ESSSSSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCCO 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. 2nd to 17th bits are the site codes, and the 18th to 49th bits are the card numbers.
"C" denotes the card number; "E" denotes the even parity bit; "O" denotes the odd parity bit; "F" denotes the facility code; "M" denotes the manufacturer code; "P" denotes the parity bit; and "S" denotes the site code.	

7.6.2 Wiegand output

Wiegand Setup

Wiegand Input

Wiegand Output

Wiegand Options

Wiegand Format

Wiegand output bits 26

Failed ID Disabled

Site Code Disabled

Pulse Width(us) 100

Pulse Interval(us) 1000

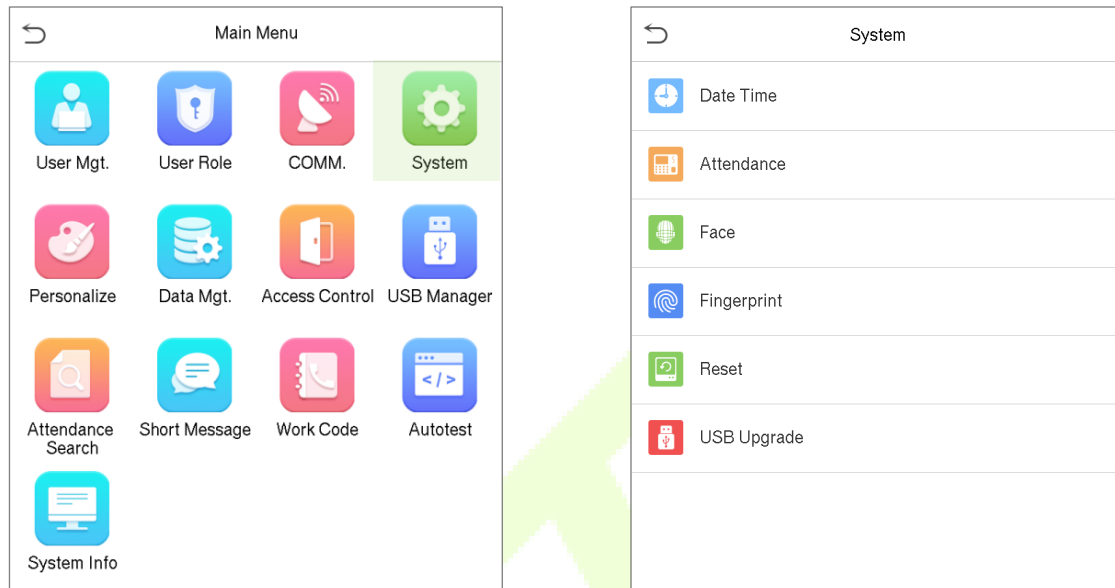
ID Type Badge Number

Function Description

Function Name	Descriptions
Wiegand Format	Value ranges from 26 bits, 34 bits, 36 bits, 37 bits, and 50 bits.
Wiegand output bits	After selecting the required Wiegand format, select the corresponding output bit digits of the Wiegand format .
Failed ID	If the verification is failed, the system will send the failed ID to the device and replace the card number or personnel ID with the new one.
Site Code	It is similar to the device ID. The difference is that a site code can be set manually, and is repeatable in different device. The valid value ranges from 0 to 256 by default.
Pulse Width(us)	The time width represents the change in the quantity of electric charge with regular high-frequency capacitance within the specified time.
Pulse Interval(us)	The time interval between pulses.
ID Type	Select the ID type as either User ID or Card number.

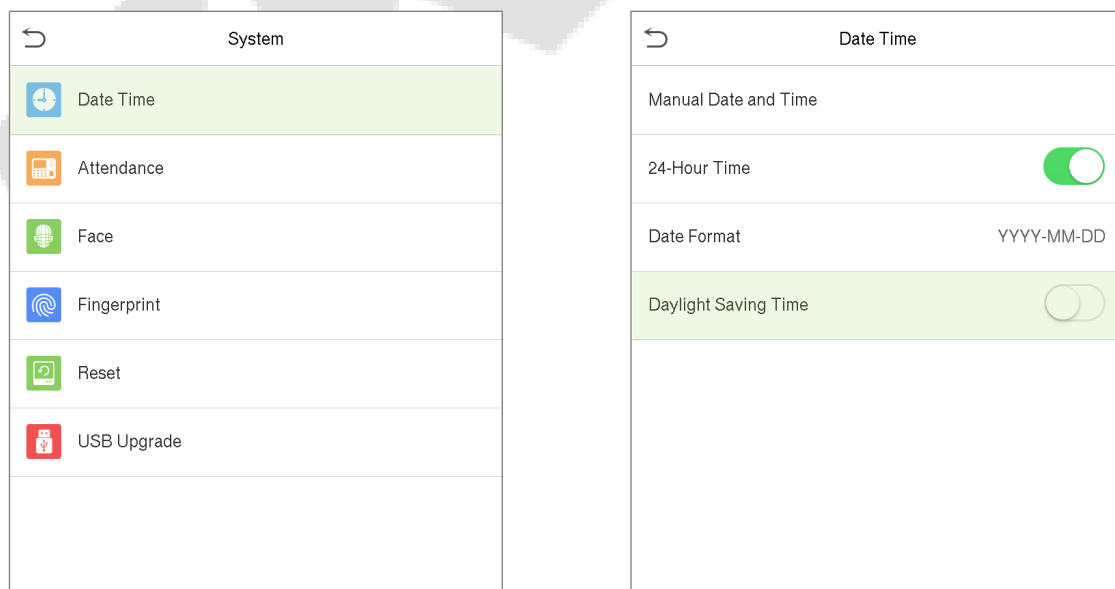
8 System Settings

- On the **Main Menu**, tap **System** to set the related system parameters so as to optimize the performance of the device.



8.1 Date and Time

- On the **System** Interface, tap **Date Time** to set the date and time.



- Tap **Manual date and time** to manually set the date and time and tap **Confirm** to save.
- Tap **24-Hour Time** to enable or disable this format. If enabled, then tap **Date Format** to set the date format.

- ★ Tap **Daylight Saving Time** to enable or disable the function. If enabled, tap **Daylight Saving Mode** to select a daylight-saving mode and then tap **Daylight Saving Setup** to set the switch time.

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

Week mode

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

Date mode

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

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

8.2 Attendance/Access Logs Setting

- On the **System** interface, tap **Attendance** to go to the access or the attendance log settings.

System	
	Date Time
	Attendance
	Face
	Fingerprint
	Reset
	USB Upgrade

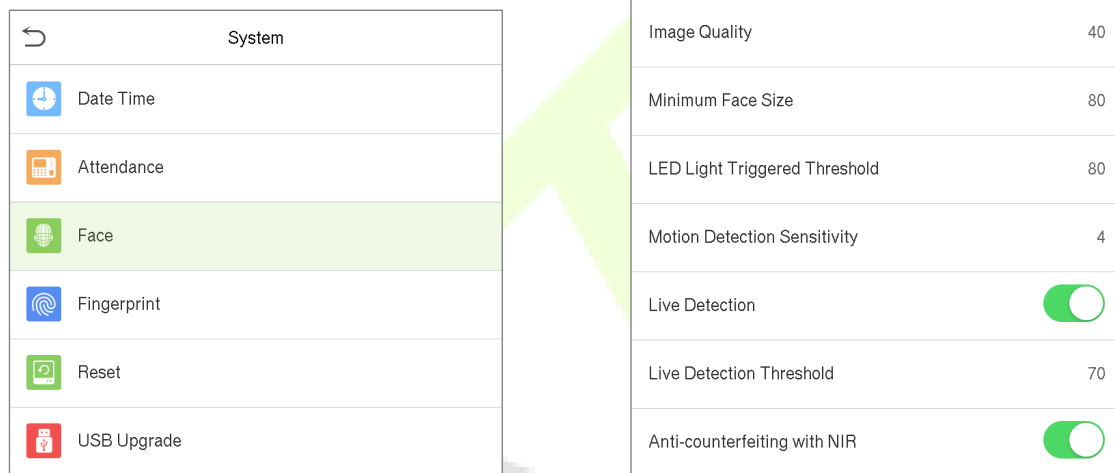
Attendance	
Duplicate Punch Period(m)	None
Camera Mode	No photo
Display User Photo	☒
Attendance Log Alert	99
Cyclic Delete ATT Data	Disabled
Cyclic Delete ATT Photo	99
Cyclic Delete Blacklist Photo	99
Confirm Screen Delay(s)	3
Face comparison interval(s)	1

Function Description

Function Name	Description
Duplicate Punch Period (m)	Once the time range is set, the attendance record of the same person will not be saved; the valid value ranges from 1 to 999999 minutes.
Camera Mode	Whether to capture and save the current snapshot image during verification. There are 5 modes: No Photo: No photo will be taken during user verification. Take photo, no save: Photo will be taken but will not be saved during verification. Take photo and save: Photo will be taken and saved during verification. Save on successful verification: Photo will be taken and saved only for each successful verification. Save on failed verification: Photo will be taken and saved only for each failed verification.
Display User Photo	Whether to display the user photo when the user passes the verification.
Attendance Log Alert/ Access Logs Warning	When the record space of the attendance log/ access log reaches the maximum threshold value, the device will automatically display the memory space warning. You may either clear the logs or disable the function or set a valid value between 1 and 9999.
Cyclic Delete ATT Data/Access Records	When the attendance/access records have reached full capacity, the device will automatically delete a set of old attendance/access records. You may disable the function or set a valid value between 1 and 999.
Cyclic Delete ATT Photo	When attendance photos have reached full capacity, the device will automatically delete a set of old attendance photos. You may disable the function or set a valid value between 1 and 99.
Cyclic Delete Blacklist Photo	When blacklisted photos have reached full capacity, the device will automatically delete a set of old blacklisted photos. You may disable the function or set a valid value between 1 and 99.
Confirm Screen Delay(s)	The time length that the message of successful verification displays. Valid value: 1~9 seconds.
Face Detect Interval (s)	Sets the facial template matching time interval as required. Valid value: 0~9 seconds.

8.3 Face Parameters

- On the **System** interface, tap **Face** to go to the face parameter settings.



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

Function Description

Function Name	Description
1:N Threshold Value	Under 1:N verification mode, the verification will only be successful when the similarity between the acquired facial image and all registered facial templates is greater than the set value. The valid value ranges from 65 to 120. The higher the threshold is, the lower the misjudgment rate, the higher the rejection rate, and vice versa. It is recommended to set the default value of 75.

1:1 Threshold Value	Under 1:1 verification mode, the verification will only be successful when the similarity between the acquired facial image and the user's facial templates enrolled in the device is greater than the set value. The valid value ranges from 55 to 120. The higher the thresholds, the lower the misjudgment rate, the higher the rejection rate, and vice versa. It is recommended to set the default value of 63.
Enrollment Threshold Value	During face enrollment, 1:N comparison is used to determine whether the user has already registered before. When the similarity between the acquired facial image and all registered facial templates is greater than this threshold value, it indicates that the face has already been registered.
Face Pitch Angle	The pitch angle tolerance of a face for facial registration and comparison. If a face's pitch angle exceeds this set value, it will be filtered by the algorithm, i.e. ignored by the terminal thus no registration and comparison interface will be triggered.
Face Rotation Angle	The rotation angle tolerance of a face for facial template registration and comparison. If a face's rotation angle exceeds this set value, it will be filtered by the algorithm, i.e. ignored by the terminal thus no registration and comparison interface will be triggered.
Image Quality	Image quality for facial registration and comparison. The higher the value, the clearer the image requires.
Minimum Recognition Value	Required for facial registration and comparison. If the minimum size of the captured figure is smaller than this set value, then it will be filtered off and will not be recognized as a face. This value can be understood as the face comparison distance. The farther the person is, the smaller the face is, and the smaller the face pixel will be obtained by the algorithm. Therefore, adjusting this parameter can adjust the furthest comparison distance of faces. When the value is set to 0, the face comparison distance is not limited.
LED Light Trigger Value	This value controls the on and off of the LED light. The larger the value, the more frequently the LED light will be turned on.
Motion Detection Sensitivity	It is to set the value for the amount of change in the camera's field of view, which is known as potential motion detection value, that wakes up the terminal from standby to the comparison interface. The larger the value is, the more sensitive the system would be, i.e. if a larger value is set, the comparison interface is much easier and the motion detection is frequently triggered.
Live Detection	Detecting the spoof attempt using visible light images to determine if the provided biometric source sample is really a person (a live human being) or false representation.
Live Detection Threshold Value	Facilitates to judge whether the captured visible image is really a person (a live human being). The larger the value, the better the anti-spoofing performance using visible light.

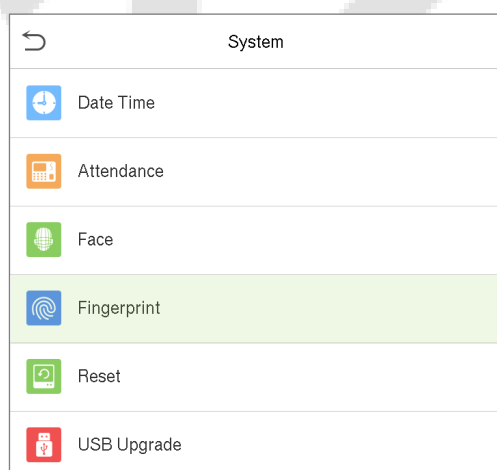
Anti-spoofing using NIR	Uses near-infrared spectra imaging to identify and prevent fake photos and video attacks.
WDR	Wide Dynamic Range (WDR), which balances light and extends image visibility for surveillance videos under high contrast lighting scenes and improves object identification under bright and dark environment.
Anti-flicker Mode	Is used when WDR is turned off. This helps reduce flicker when the device's screen flashes at the same frequency as the light.
Notes	Improper adjustment of the exposure and quality parameters may severely affect the performance of the device. Please adjust the exposure parameter only under the guidance of the after-sales service personnel of our company.

Process to modify the Face Recognition Accuracy

- On the **System** interface, tap on **Face** and then toggle to enable Anti-Spoofing using NIR to set the anti-spoofing.
- Then, on the **Main Menu**, tap **Auto-Test > Test Face** and perform the face test.
- Tap three times for the scores on the right upper corner of the screen, and the red rectangular box appears to start adjusting the mode.
- Keep one arm distance between the device and the face, and recommended not to move the face in wide range.

8.4 Fingerprint Parameters

- On the **System** interface, tap **Fingerprint** to configure the fingerprint settings.



Fingerprint	
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	Recommended Matching Thresholds	
		1:N	1:1
High	Low	45	25
Medium	Medium	35	15
Low	High	25	10

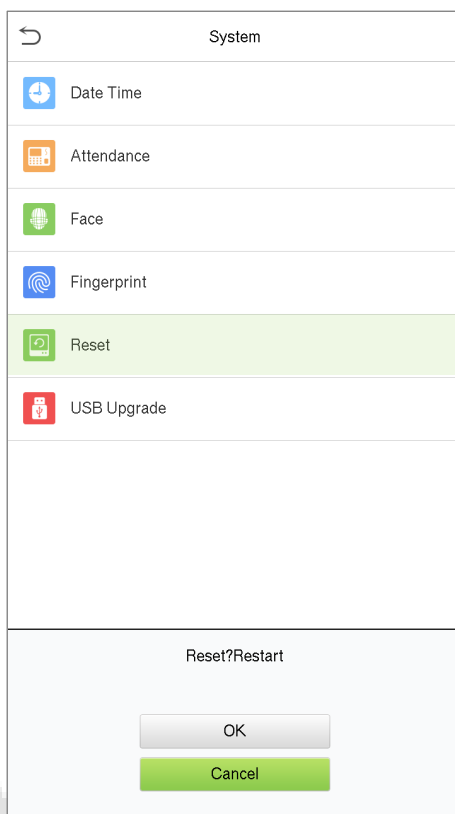
Function Description

Function Name	Descriptions
1:1 Threshold	Under 1:1 verification method, the verification will only be successful when the similarity between the acquired fingerprint data and the fingerprint template associated with the entered user ID that is enrolled in the device is greater than the set value.
1:N Threshold	Under 1:N verification method, the verification will only be successful when the similarity between the acquired fingerprint data and the fingerprint templates enrolled in the device is greater than the set value.
FP Sensor Sensitivity	To set the sensibility of fingerprint acquisition. It is recommended to use the default level " Medium ". When the environment is dry, resulting in slow fingerprint detection, you can set the level to " High " to raise the sensibility; when the environment is humid, making it hard to identify the fingerprint, you can set the level to " Low ".
1:1 Retry Attempts	Users might forget the registered fingerprint, or press the finger improperly. 1:1 Verification allows to set the retry authentication attempts for the users in order to reduce the process of re-entering the user ID and increase the security.
Fingerprint Image	To set whether to display the fingerprint image on the screen during fingerprint enrollment or verification. Four choices are available: • Show for enroll: to display the fingerprint image on the screen only during enrollment. • Show for match: to display the fingerprint image on the screen only during verification. • Always show: to display the fingerprint image on screen during enrollment and verification. • None: not to display the fingerprint image.

8.5 Factory Reset

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

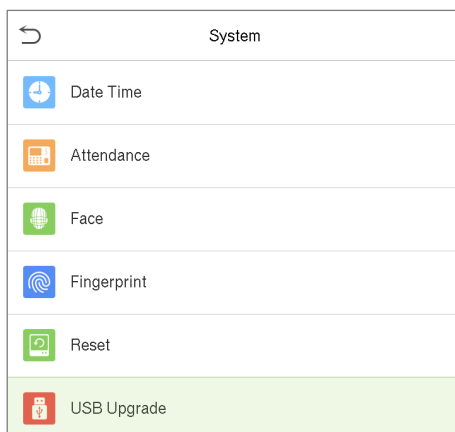
- On the **System** interface, tap **Reset** and then tap **OK** to restore to default factory settings.



8.6 USB Upgrade

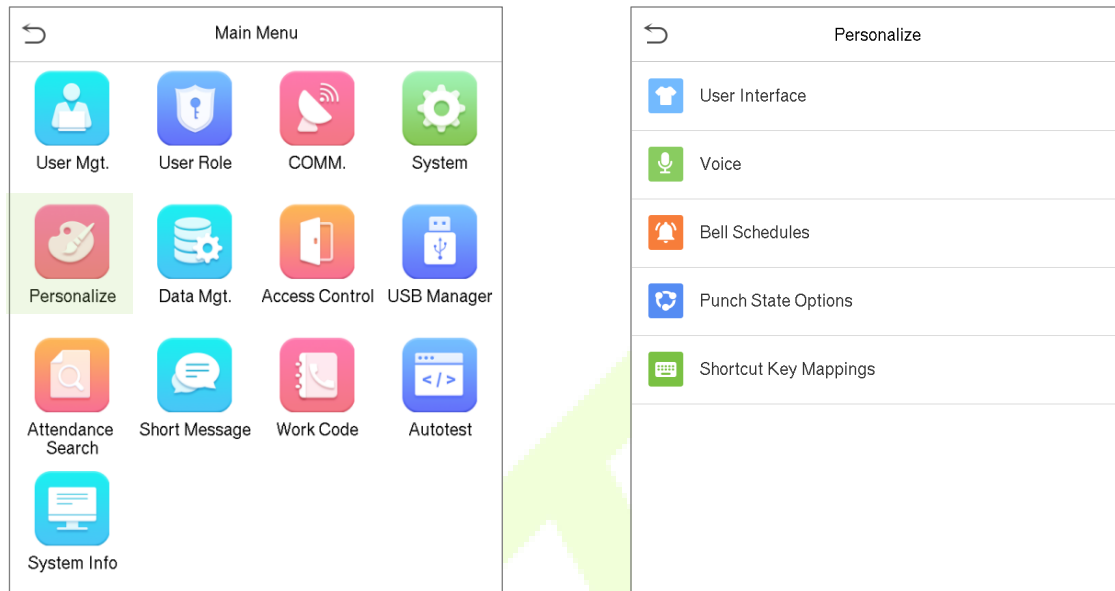
The device firmware program can be upgraded with the upgrade file in a USB drive. Before conducting this operation, please ensure that the USB drive contains the correct upgrade file and is properly inserted into the device.

- On the **System** interface, tap **USB Upgrade** to upgrade the Device firmware.



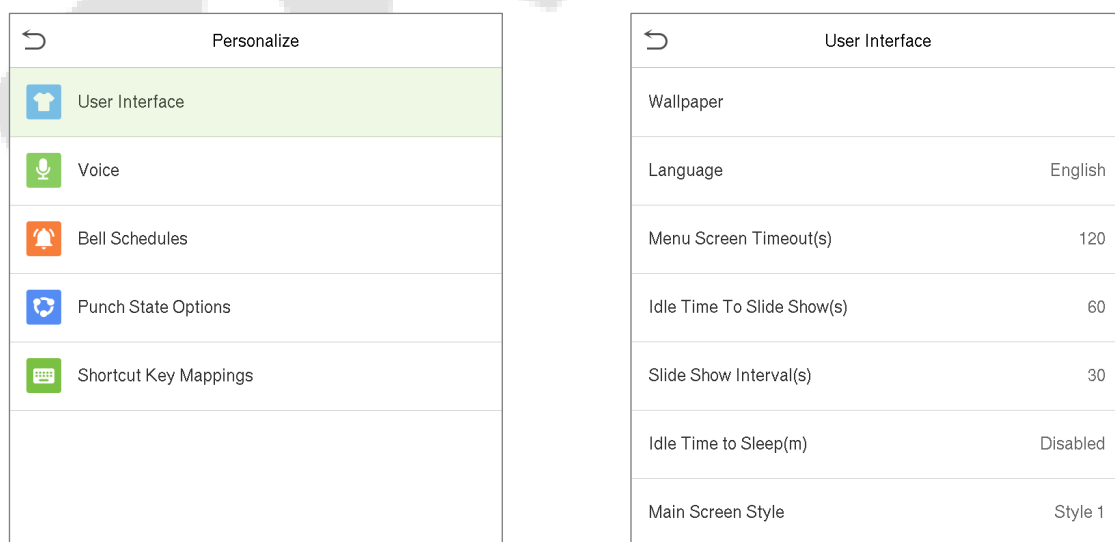
9 Personalize Settings

- On the **Main Menu**, tap **Personalize** customize interface settings, voice, bell, punch state options and shortcut key mappings ★.



9.1 Interface Settings

- On the **Personalize** interface, tap **User Interface** to customize the display style of the main interface.



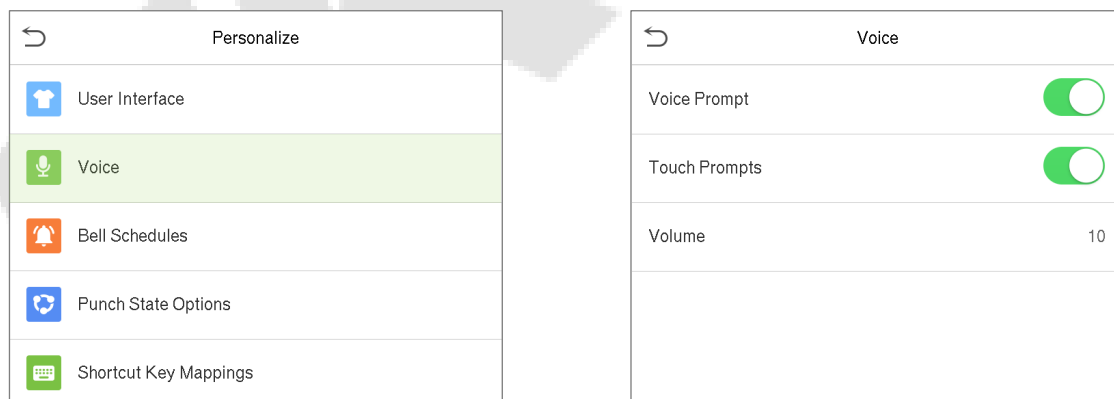
Function Description

Function Name	Description
Wallpaper	The main screen wallpaper can be selected according to the user preference.

Language	Select the language of the device.
Menu Screen Timeout (s)	When there is no operation, and the time exceeds the set value, the device will automatically go back to the initial interface. This function either can disabled or set the required value between 60 and 99999 seconds.
Idle Time To Slide Show (s)	When there is no operation, and the time exceeds the set value, a slide show will be played. This function can be disabled, or set the required value between 3 and 999 seconds.
Slide Show Interval (s)	It is time interval in switching between different images as a slide show process. The function can be disabled, or set the required time interval between 3 and 999 seconds.
Idle Time to Sleep (m)	If the sleep mode is activated, and when there is no operation in the device, then the device will go to the standby mode. Press any key or finger to resume normal working mode. This function can be disables or set a value within 1-999 minutes.
Main Screen Style	The main screen style can be selected according to the user preference.

9.2 Voice Settings

- On the **Personalize** interface, tap **Voice** to configure the voice settings.

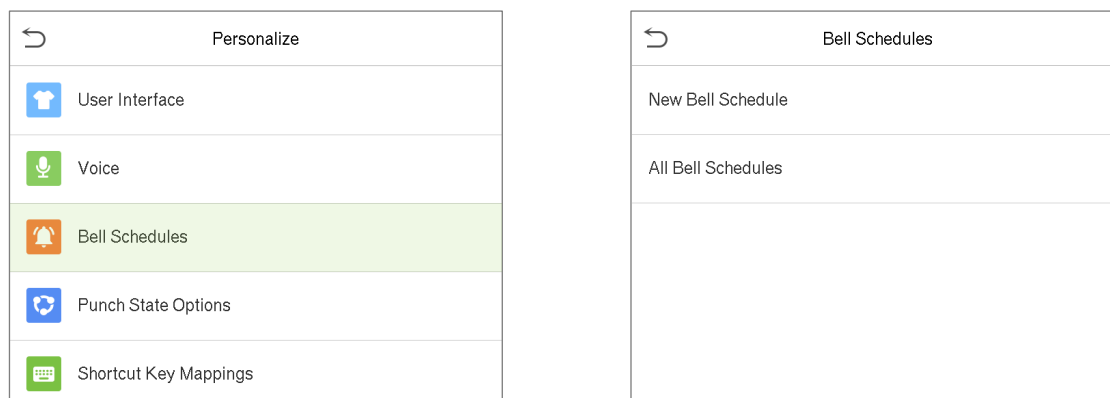


Function Description

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

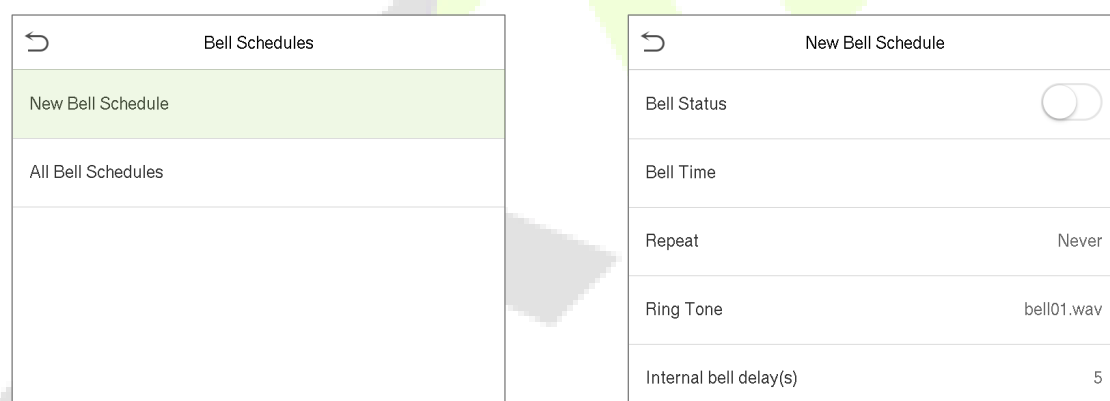
9.3 Bell Schedules

- On the **Personalize** interface, tap **Bell Schedules** to configure the Bell settings.



New Bell Schedule

- On the **Bell Schedules** interface, tap **New Bell Schedule** to add a new bell schedule.



Function Description

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

All Bell Schedules

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

Edit the scheduled bell

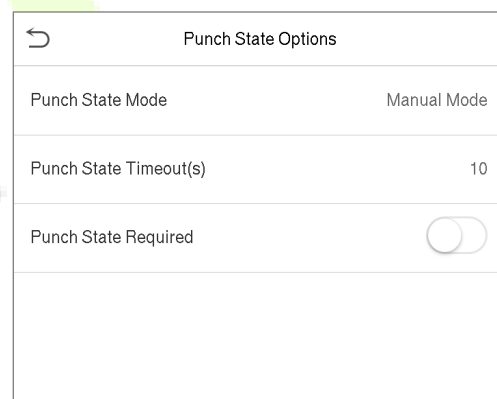
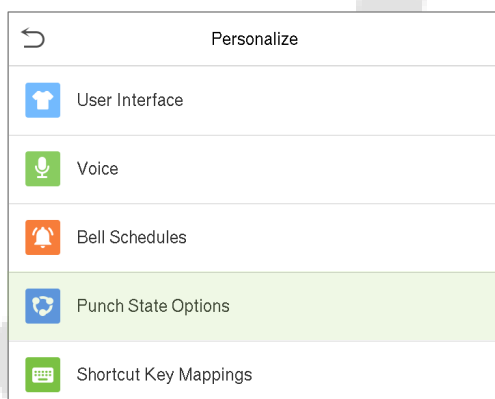
- On the **All Bell Schedules** interface, tap on the required bell schedule, and tap **Edit** to edit the selected bell schedule.
- The editing method is the same as the operations of adding a new bell schedule.

Delete a bell

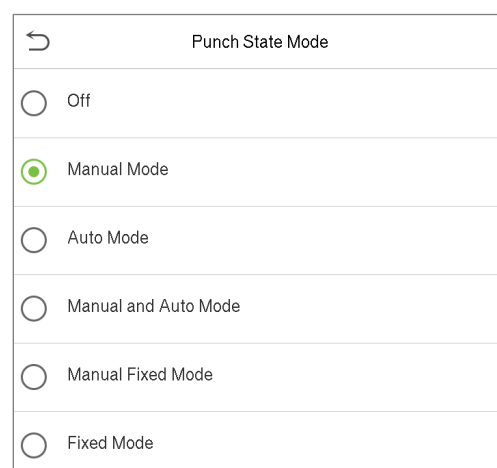
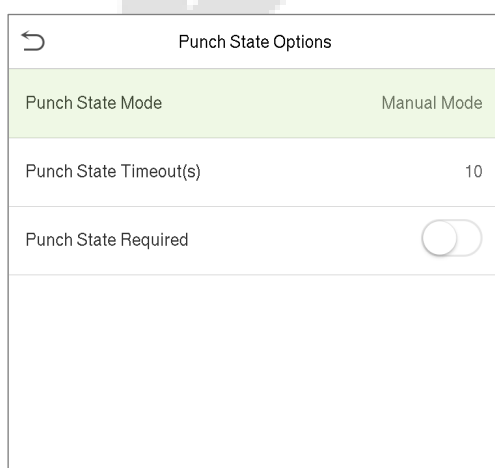
- On the All Bell Schedules interface, tap the required bell schedule, and tap **Delete**, and then tap **Yes** to delete the selected bell.

9.4 Punch State Options

- On the **Personalize** interface, tap **Punch State Options** to configure the punch state settings.



Punch State Mode



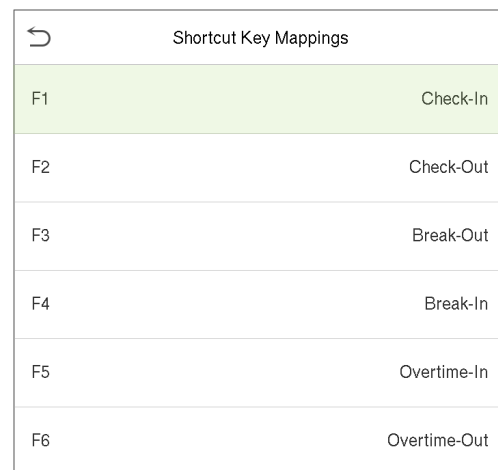
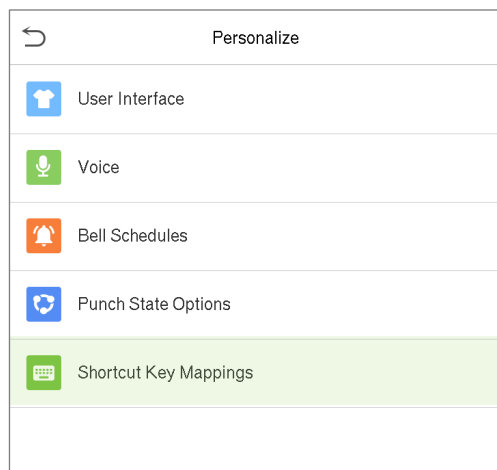
Function Description

Item	Description
Punch State Mode	Off: Disables the punch state function. Therefore, the punch state key set under Shortcut Key Mappings menu will not operate. Manual Mode: Switches the punch state key manually; the attendance status will be automatically reset after timeout. Auto Mode: The punch state key will automatically switch to a specific punch status according to the predefined time schedule which can be set in the Shortcut Key Mappings. Manual and Auto Mode: The main interface will display the auto-switch punch state key. However, the users will still be able to select alternative that is the manual attendance status. After timeout, the manual switching punch state key will become auto-switch punch state key. Manual Fixed Mode: After the punch state key is set manually to a particular punch status, the function will remain unchanged until being manually switched again. Fixed Mode: Only the manually fixed punch state key will be shown. Users cannot change the status by pressing any other keys.
Punch State Timeout (s)	The time duration for the time out, i.e. remaining inactive in the main menu.
Punch State Required	To set whether the attendance status must be selected during verification.

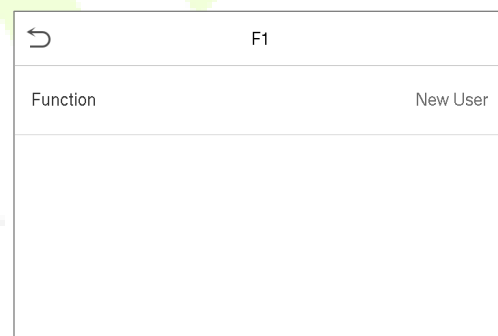
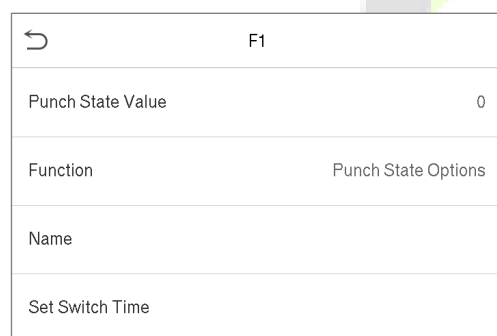
9.5 Shortcut Key Mappings

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

- On the **Personalize** interface, tap **Shortcut Key Mappings** to set the required shortcut keys.



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



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

Set the switch time

- The switch time is set in accordance with the punch state options.
- When the **punch state mode** is set to **auto mode**, the switch time should be set.
- On the **Shortcut Key** interface, tap **Set Switch Time** to set the switch time.
- On the **Switch Cycle** interface, select the switch cycle (Monday, Tuesday etc.) as shown in the image below.

F1		Set Switch Time		Switch Cycle	
Punch State Value	0	Switch Cycle	Monday Tuesday Wednes...	☒ Monday	
Function	Punch State Options	Monday		☒ Tuesday	
Name		Tuesday		☒ Wednesday	
Set Switch Time		Wednesday		☒ Thursday	
		Thursday		☒ Friday	
		Friday		☐ Saturday	
				☐ Sunday	

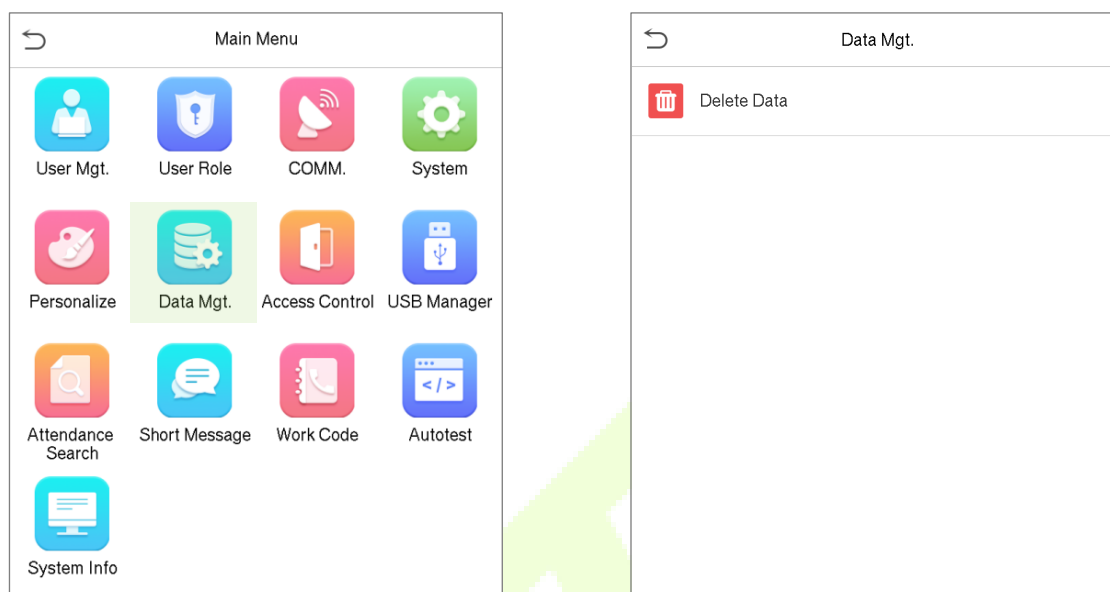
- Once the Switch cycle is selected, set the switch time for each day and tap **OK** to confirm, as shown in the image below.

Monday	Set Switch Time
08:00	Switch Cycle Monday Tuesday Wednes...
08 00 HH MM	Monday 08:00
	Tuesday
	Wednesday
	Thursday
	Friday
Confirm (OK)	
Cancel (ESC)	

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

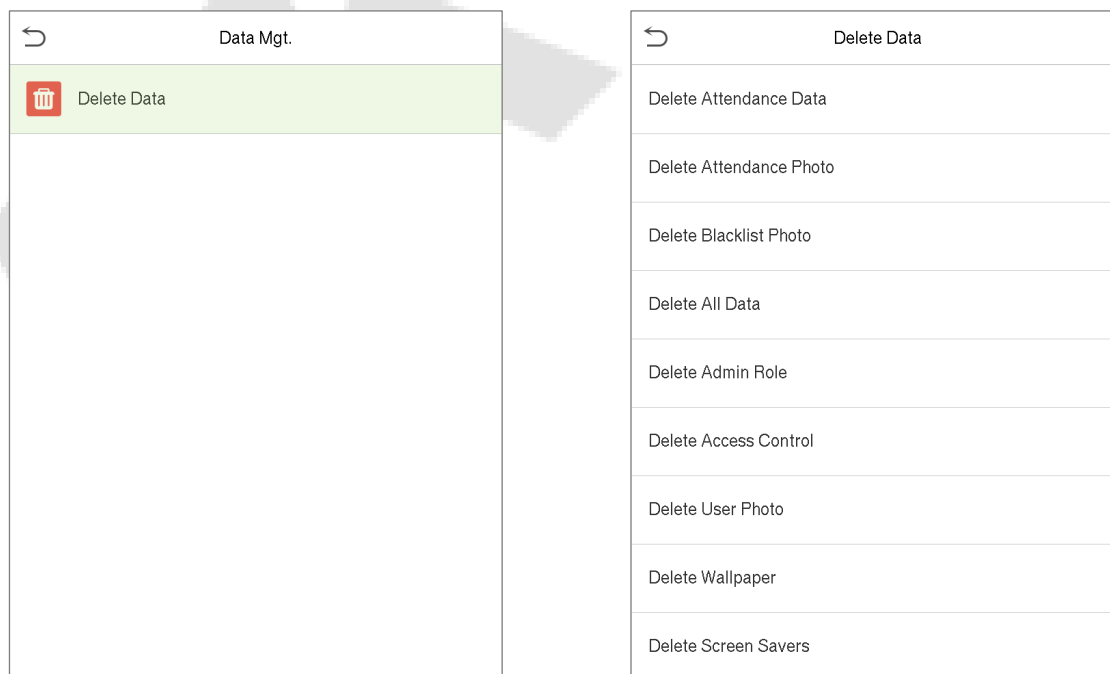
10 Data Management

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



10.1 Delete Data

- On the **Main Menu**, tap **Delete Data** to delete the required data.

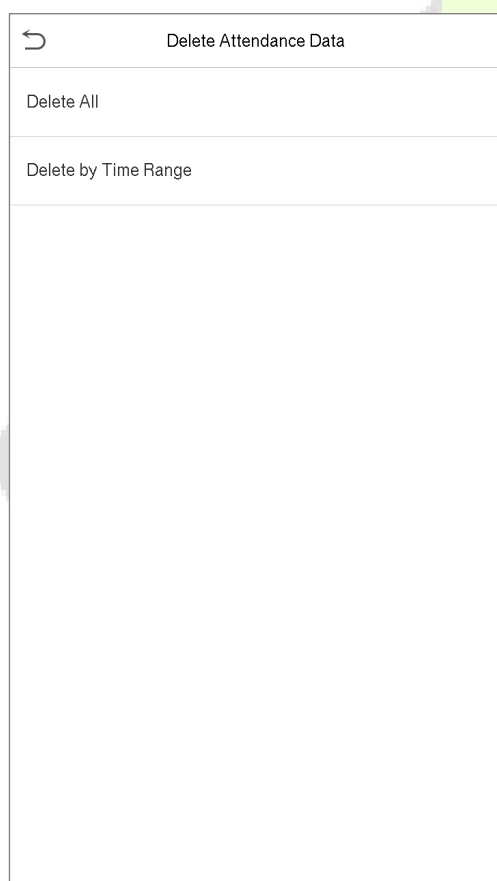


Function Description

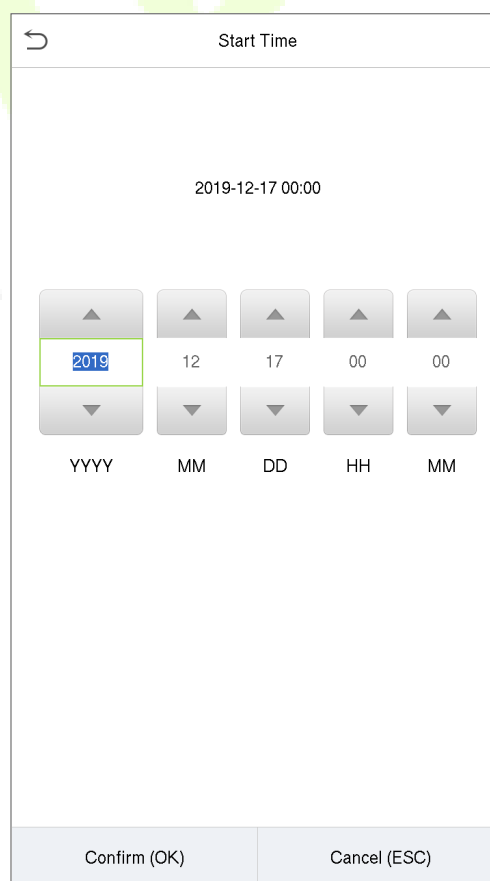
Function Name	Description
Delete Attendance Data / Access Records	Deletes the attendance data/access records conditionally.

Delete Attendance Photo	Deletes the attendance photos of the designated personnel.
Delete Blacklist Photo	Deletes the photos of the failed verifications.
Delete All Data	Deletes data and attendance logs/access records of all registered users.
Delete Admin Role	Removes all the administrator privileges.
Delete Access Control	Deletes all the access data.
Delete User Photo	Deletes all the user photos in the device.
Delete Wallpaper	Deletes all the wallpapers in the device.
Delete Screen Savers	Deletes all the screen savers in the device.

- The user may select Delete All or Delete by Time Range when deleting the attendance data/access records, attendance photos or blacklisted photos.
- If Delete by Time Range is selected, then it is required to set a specific time range to delete all data within the specific period.



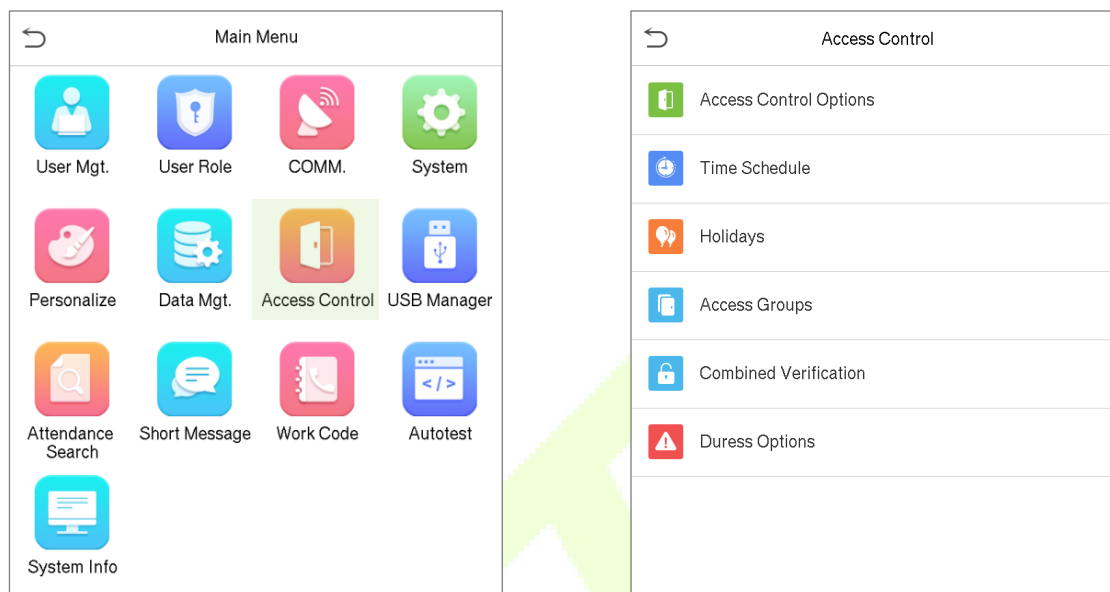
Select Delete by Time Range.



Set the time range and click OK.

11 Access Control

- On the **Main Menu**, tap **Access Control** to set the schedule for door opening, locks control and to configure other parameters settings related to access control.

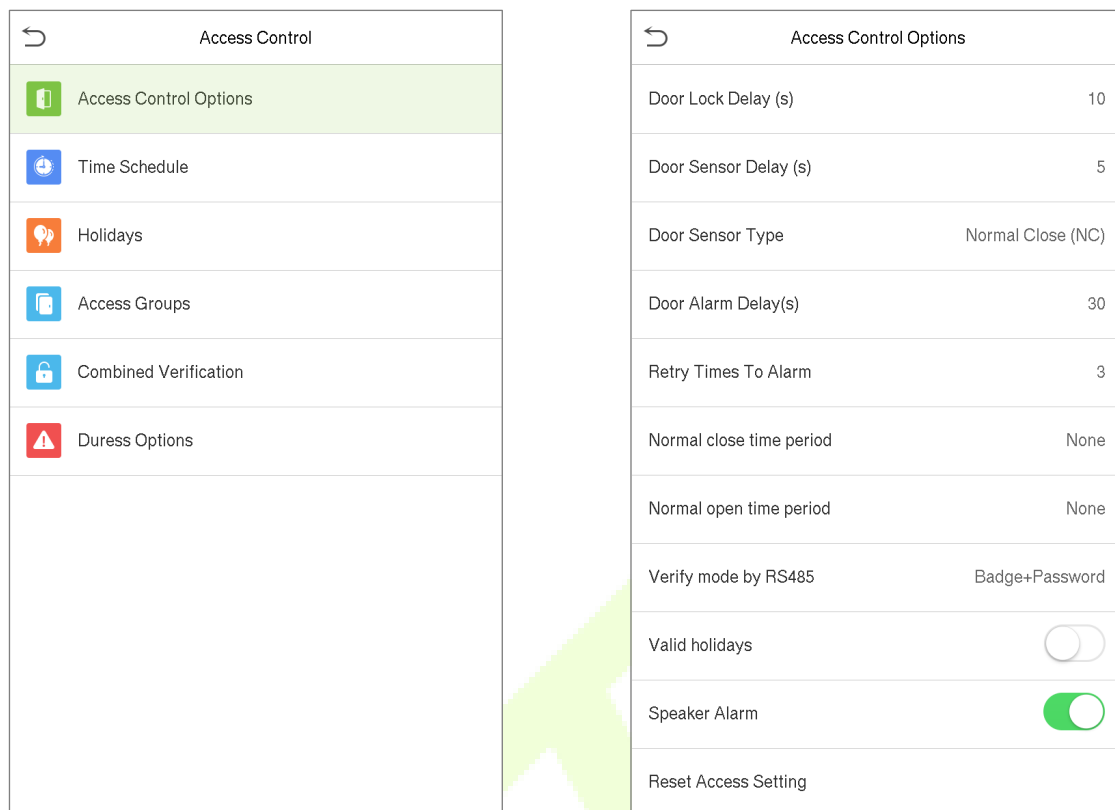


To gain access, the registered user must meet the following conditions.

- The relevant door's current unlock time should be within the valid time zone of the user time period.
- The corresponding user's group must be already set in the door unlock combination (and if there are other user groups, being set in the same access combo, then the verification of those group's members is also required, in order to unlock the door).
- In default settings, new users are allocated into the first group with the default group time zone, where the access combo is "1" and is set in unlock state by default.

11.1 Access Control Options

- On the **Access Control** interface, tap **Access Control Options** to set the parameters of the control lock for the device and other related components.



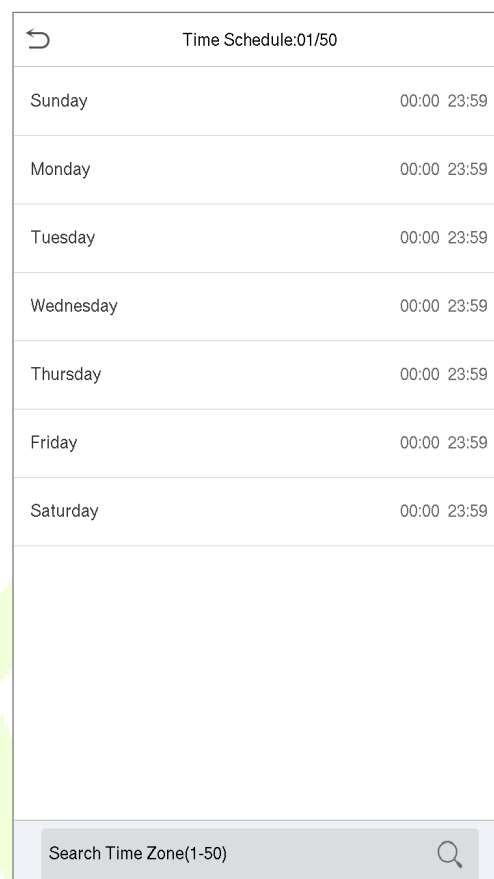
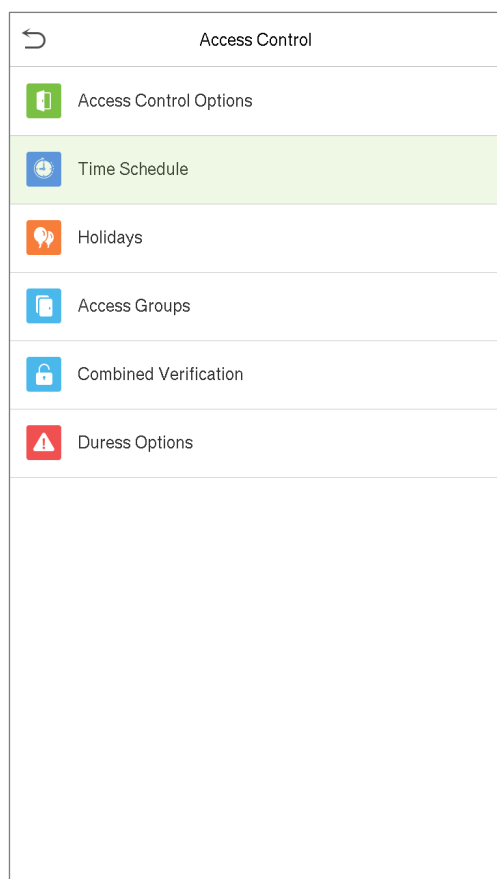
Function Description

Function Name	Description
Door Lock Delay (s)	The length of time that the device controls the electric lock to be in unlock state. Valid value: 1~10 seconds; 0 second represents disabling the function.
Door Sensor Delay (s)	If the door is not locked and is being left open for a certain duration (Door Sensor Delay), an alarm will be triggered. The valid value of Door Sensor Delay ranges from 1 to 255 seconds.
Door Sensor Type	There are three Sensor types: None, Normal Open, and Normal Close. None: It means the door sensor is not in use. Normal Open: It means the door is always left opened when electric power is on. Normal Close: It means the door is always left closed when electric power is on.
Door Alarm Delay (s)	When the state of the door sensor is inconsistent with that of the door sensor type, an alarm will be triggered after a specific time period, i.e. the Door Alarm Delay. The valid value ranges from 1 to 999 seconds and 0 means immediate alarm.
Retry Times to Alarm	When the number of failed verifications reaches a set value, which ranges from 1 to 9 times, an alarm will be triggered. If the set value is "None", the alarm will never be triggered for the failed verifications.

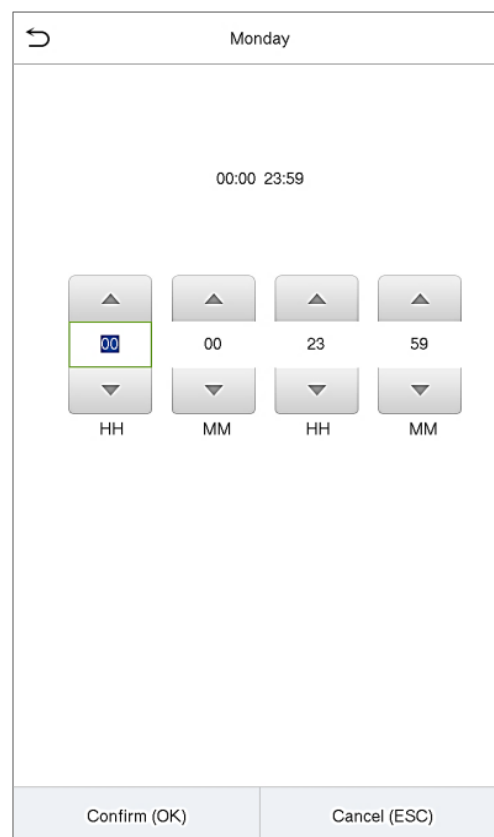
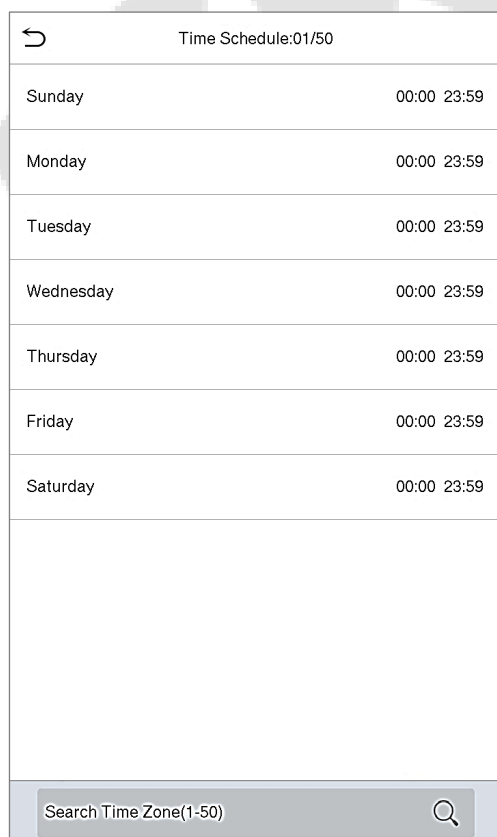
Function Name	Description
Normal close time period	Scheduled time period for “Normal Close” mode, so that no one can avail access during this period.
Normal open time period	Scheduled time period for “Normal Open” mode, so that the door is always left open during this period.
Verify mode by RS485	The verification mode is used when the device is used either as a host or slave. The supported verification mode includes Card/Fingerprint, Fingerprint only, Card only, Fingerprint + Password, Card + Password, Card + Fingerprint, and Card + Fingerprint + Password.
Valid holidays	Configures the Normal Close Period or Normal Open Period settings to be effective in the set holiday time period. Toggle to enable or disable the function during holiday.
Speaker Alarm	Transmits a sound alarm or disassembly alarm from the local. When the door is closed or the verification is successful, the system will cancel the alarm from the local.
Reset Access Setting	The access control reset parameters include door lock delay, door sensor delay, door sensor type, normal close time period, normal open time period, auxiliary input configuration and alarm. Except for the erased access control data in Data Mgt. is excluded.

11.2 Time Schedule

- On the **Access Control** interface, tap **Time Schedule** to configure the time settings.
- The entire system can be defined up to **50** Time Periods.
- Each Time Period represents **7** Time Zones, i.e. **1** week, and each Time Zone is a standard 24-hour period per day and the user can only verify within the valid time period.
- The Time Zone format of each Time Period: HH MM-HH MM, which is accurate to minutes according to the 24-hour clock.
- Tap on the grey box to search for the required Time Zone and specify the required Time Zone number (can specify up to 50 zones).



- On the selected Time Zone number interface, tap on the required day (that is Monday, Tuesday etc.) to set the time.
- Specify the start and end time, and then tap **OK**.



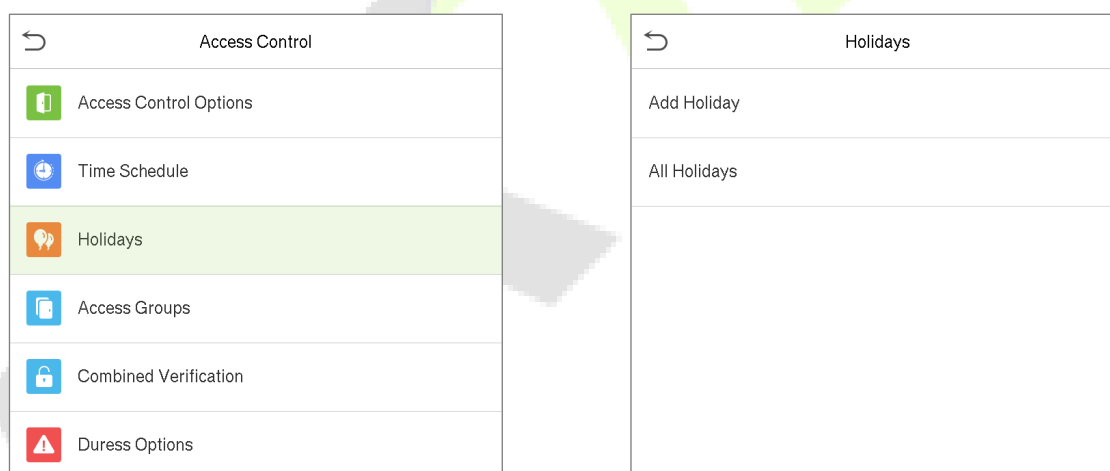
Notes:

- When the End Time is earlier than the Start Time, (such as 23:57~23:56), it indicates that access is prohibited all day.
- When the End Time is later than the Start Time, (such as 00:00~23:59), it indicates that the interval is valid.
- The effective Time Period to keep the Door unlock or open all the day is (00:00~23:59) and also when the End Time is later than the Start Time, (such as 08:00~23:59).
- The default Time Zone **1** indicates that door is open all day long.

11.3 Holiday Settings

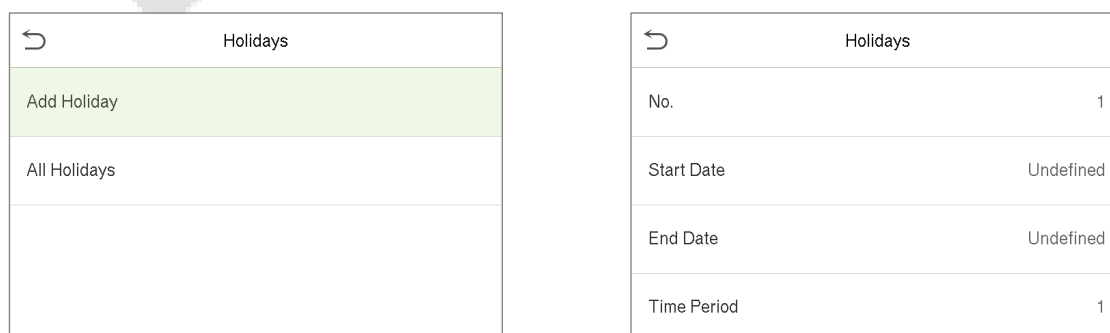
Whenever there is a holiday, you may need a special access time; but changing everyone's access time one by one is extremely cumbersome, so you can set a holiday access time which is applicable to all employees, and the user will be able to open the door during the holidays.

- On the **Access Control** interface, tap **Holidays** to set the Holiday access.



Add a New Holiday

- On the **Holidays** interface, tap **Add Holiday** to set the holiday parameters.



Edit a Holiday

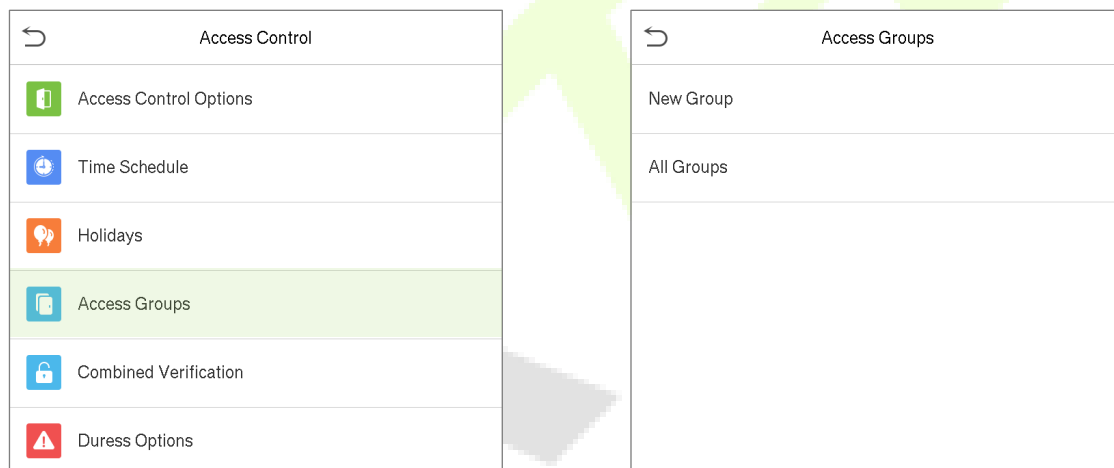
- On the **Holidays** interface, tap on a holiday item to be modified. Tap **Edit** to modify holiday parameters.

Delete a Holiday

- On the **Holidays** interface, tap on a holiday item to be deleted and tap **Delete**. Tap **OK** to confirm deletion. After deletion, this holiday will be no longer displayed on **All Holidays** interface.

11.4 Access Groups

- On the **Access Control** interface, tap **Access Groups** to easily manage the different group of users in different access groups.



- The configuration of access group such as access time zones are applicable to all the users in the group by default where the users can manually set the time zones as required.
- If the group authentication mode overlaps with the individual authentication, the user authentication takes precedence over group authentication.
- Each group can set a maximum of three Time Zones. By default, newly enrolled users are assigned to Access Group 1; they can be assigned to other access groups later as per the requirement.

Add a New Group

- On the **Access Groups** interface, tap **New Group** to set the access group parameters.

Access Groups
New Group
All Groups

Access Groups	
No.	2
Verification Mode	Password/Fingerprint/Badge...
Time Period 1	1
Time Period 2	0
Time Period 3	0
Include Holidays	☐

Note:

- There is a default access group numbered 1, which cannot be deleted, but can be modified.
- The Access Group number cannot be modified after being set.
- When the holiday is set to be valid, personnel in a group may only open the door when the group time zone overlaps with the holiday time period.
- When the holiday is set to be invalid, the access control time of the personnel in a group is not affected during holidays.

Edit a Group

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

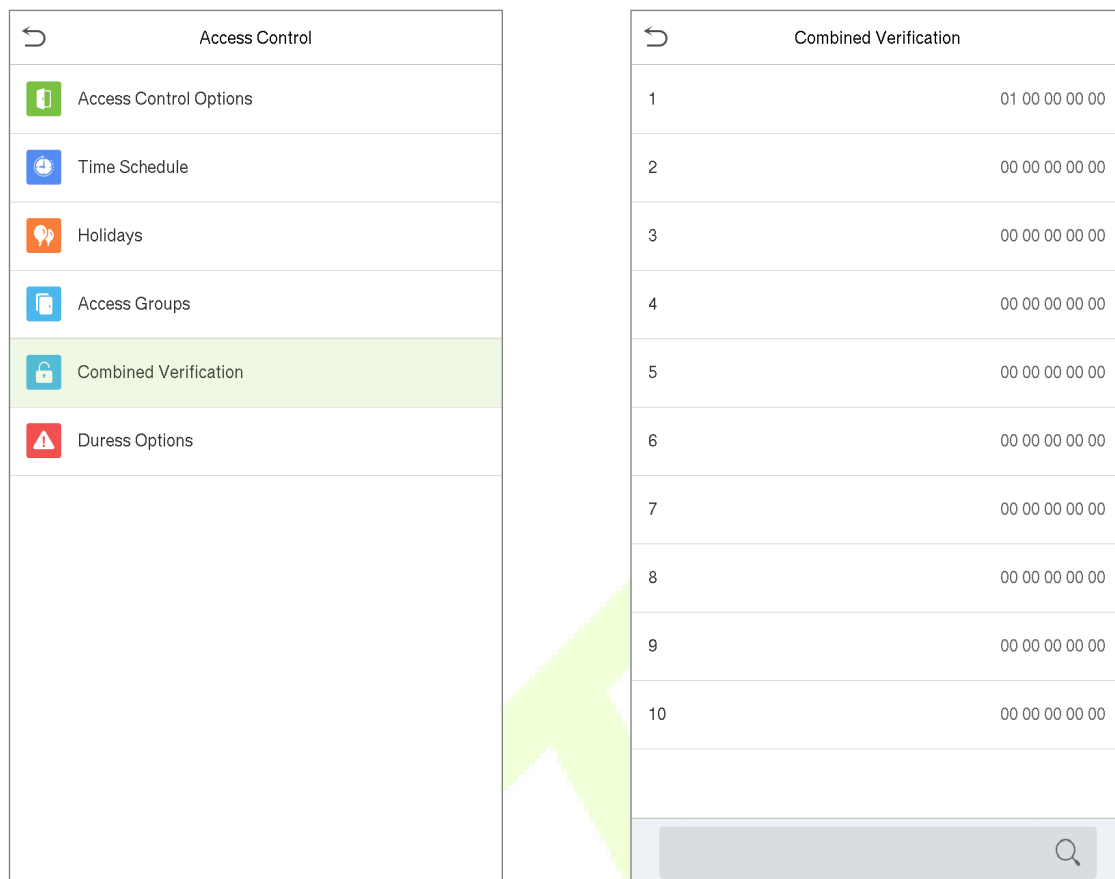
Delete a Group

- On **All Groups** interface, select the access group item to be deleted and click **Delete**.
- Tap **OK** to confirm deletion. The deleted access group will be no longer displayed in All Groups interface.

11.5 Combined Verification Settings

Access groups are arranged into different door-unlock combinations to achieve multiple verifications and increase the security. In a door-unlocking combination, the range of the combined number N is: $0 \leq N \leq 5$, and the number of members N may all belong to one access group or may belong to five different access groups.

- On the **Access Control** interface, tap **Combined Verification** to configure the combined verification settings.



- On the Combined verification interface, tap on the required Door-unlock combination to be set, and tap the **up** and **down** arrows to input the combination number, and then tap **OK**

For Example:

- The **Door-unlock combination 1** is set as **(01 03 05 06 08)**, indicating that the unlock combination 1 consists of 5 people, and the 5 individuals are from 5 groups, namely, **Access Control Group 1** (AC Group 1), AC Group 3, AC Group 5, AC Group 6, and AC Group 8, respectively.
- The **Door-unlock combination 2** is set as **(02 02 04 04 07)**, indicating that the unlock combination 2 consists of 5 people; the first two are from AC group 2, the next two are from AC group 4, and the last person is from AC group 7.
- The **Door-unlock combination 3** is set as **(09 09 09 09 09)**, indicating that there are 5 people in this combination; and all of them are from AC group 9.
- The **Door-unlock combination 4** is set as **(03 05 08 00 00)**, indicating that the unlock combination 4 consists of only 3 people. The first person is from AC group 3, the second person is from AC group 5, and the third person is from AC group 8.

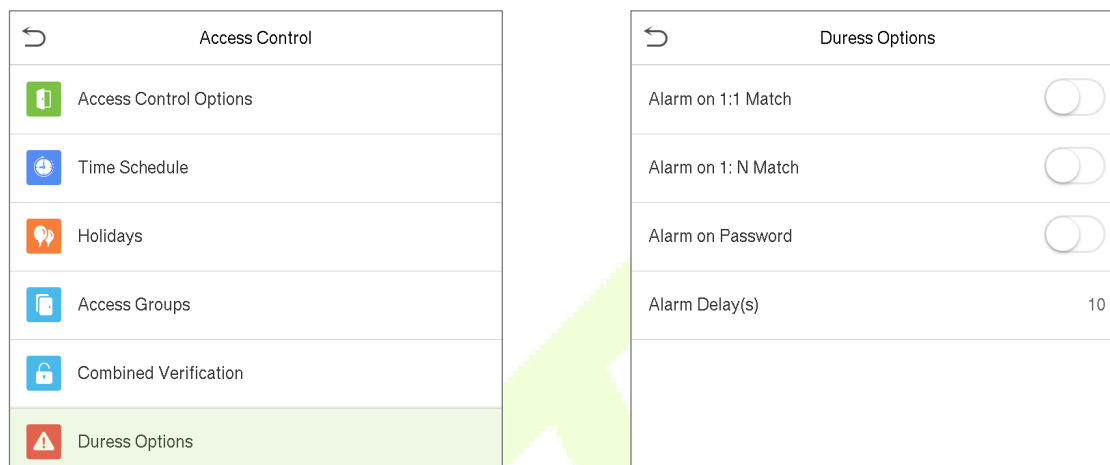
Delete a door-unlocking combination

- Set all Door-unlock combinations to 0 if you want to delete all the door-unlock combinations.

11.6 Duress Options Settings

Once a user activates the duress verification function with a specific authentication method(s), and when he/she is under coercion and authenticates using duress verification, the device will unlock the door as usual, but at the same time, a signal will be sent to trigger the alarm.

- On the **Access Control** interface, tap **Duress Options** to configure the duress settings.

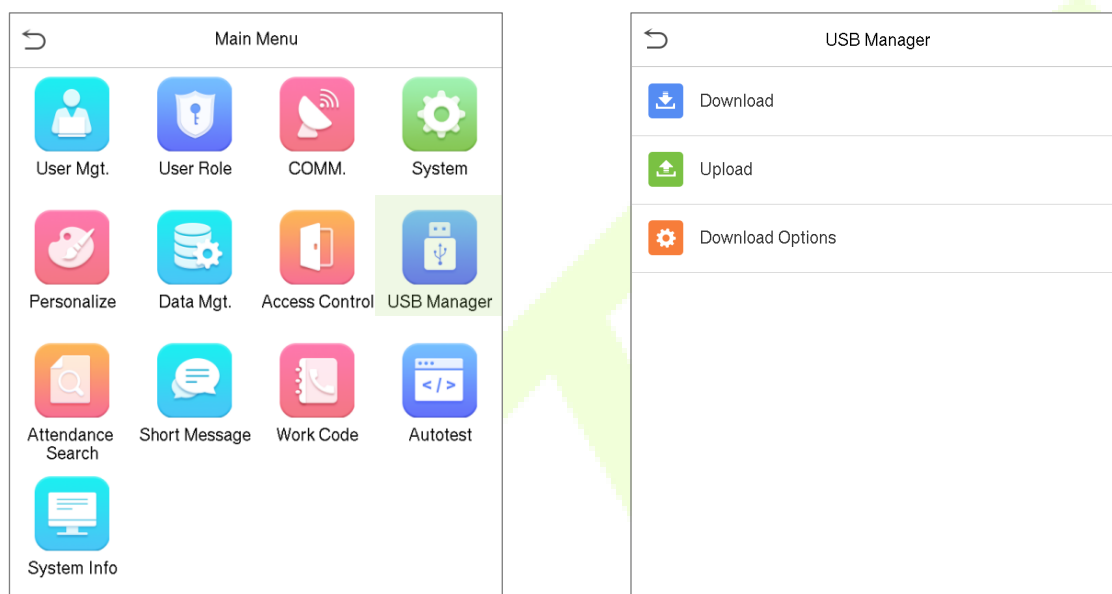


Function Description

Function Name	Description
Alarm on 1:1 Verification	When a user uses any fingerprint to perform the 1:1 verification, an alarm signal will be generated only when the 1:1 verification is successful, otherwise there will be no alarm signal.
Alarm on 1:N Identification	When a user uses any fingerprint to perform 1:N verification, an alarm signal will be generated only when the 1:N identification is successful, otherwise there will be no alarm signal.
Alarm on Password	When a user uses the password verification method, an alarm signal will be generated only when the password verification is successful, otherwise there will be no alarm signal.
Alarm Delay (s)	Alarm signal will not be transmitted until the alarm delay time is elapsed. The value ranges from 1 to 999 seconds.

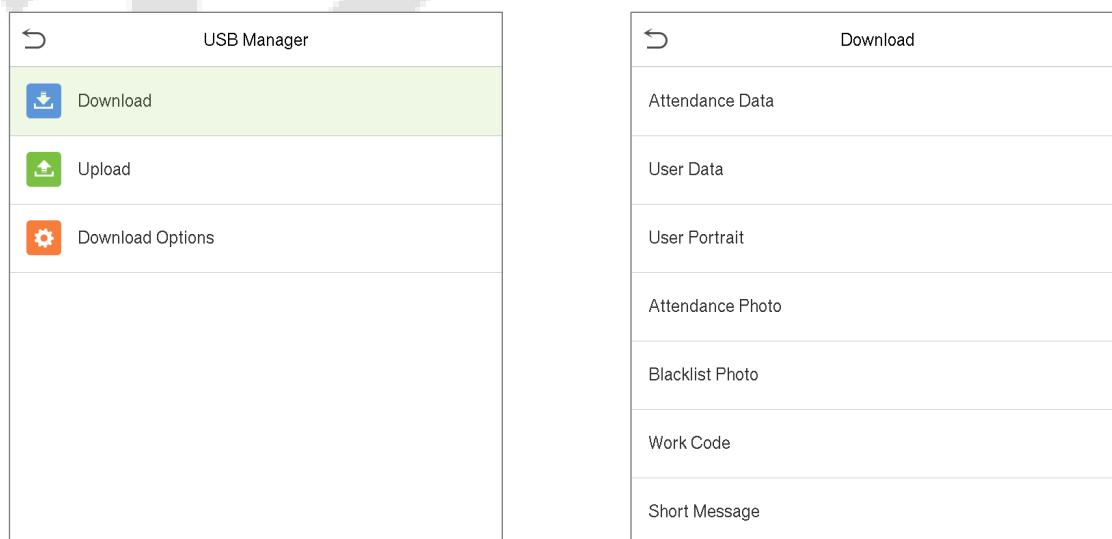
12 USB Manager

- On the **Main Menu**, tap **USB Manager** to manage the data through USB drive.
- You can import user information, access data and other data from a USB drive to computer or other devices.
- Before uploading or downloading data from or to the USB drive, insert the USB drive into the USB slot first.



12.1 Download

- On the **USB Manager** interface, tap **Download** to download the required data from the device to USB drive.

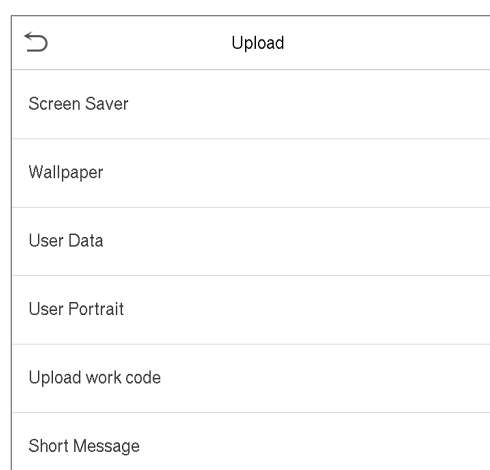
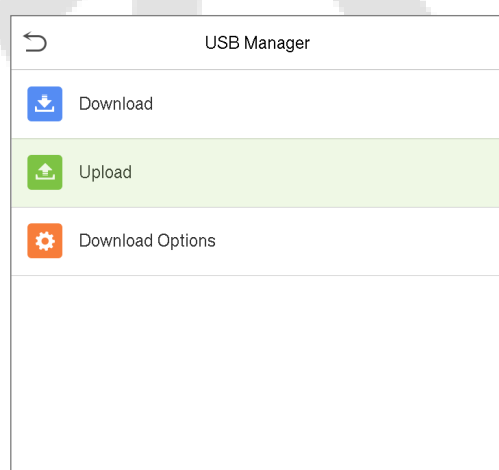


Function Description

Function Name	Descriptions
Attendance Data	Permits to either download attendance data stored in the device within a specified time period or all attendance data from the device to the USB drive.
User Data	Permits to download all user information from the device to the USB drive.
User Portrait	Permits to download all user pictures from the device to the USB drive.
Attendance Photo	Permits to either download attendance photos stored in the device within a specified time period or all attendance photos from the device to the USB drive. Picture format is JPG
Blacklist Photo	Permits to either download blacklisted photos taken after failed verifications within a specified time period or all pictures taken after failed verifications from the device to the USB drive.
Work Code	Permits to download all work codes from the device to the USB drive.
Short Message	Permits to download a set of public or private short messages, which are read by specified objects within the specified time after attendance, facilitating information transmission.

12.2 Upload

- On the **USB Manager** interface, tap **upload** to upload the required data to the device from USB drive.

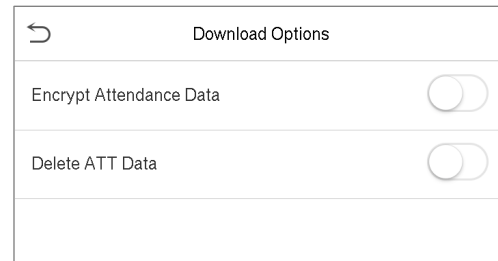
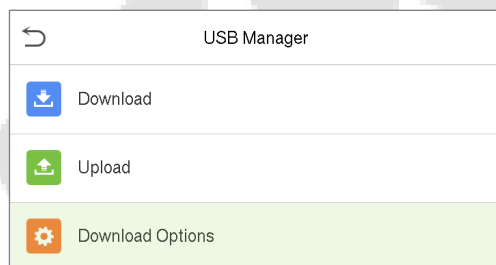


Function Description

Function Name	Description
Screen Saver	Can upload screen saver from the USB drive to the device. Before uploading, you may select Upload selected picture or Upload all pictures .
Wallpaper	Can upload wallpaper from the USB drive to the device. Before uploading, you may select Upload selected picture or Upload all pictures . The images will be displayed on the screen after manual settings.
User Data	Can upload all user information from a USB drive to the device.
User Portrait	Can upload the JPG picture named with a user ID from the USB drive to the device. Before uploading, you may select Upload Current Picture or Upload All Pictures .
Upload work code	Can upload work codes from the USB drive to the device.
Short Message	Can upload a set of public or private short messages, which are read by specified objects within the specified time after attendance, facilitating information transmission.

12.3 Download Options

- On the **USB Manager** interface, tap **Download Options** to set the required download process.

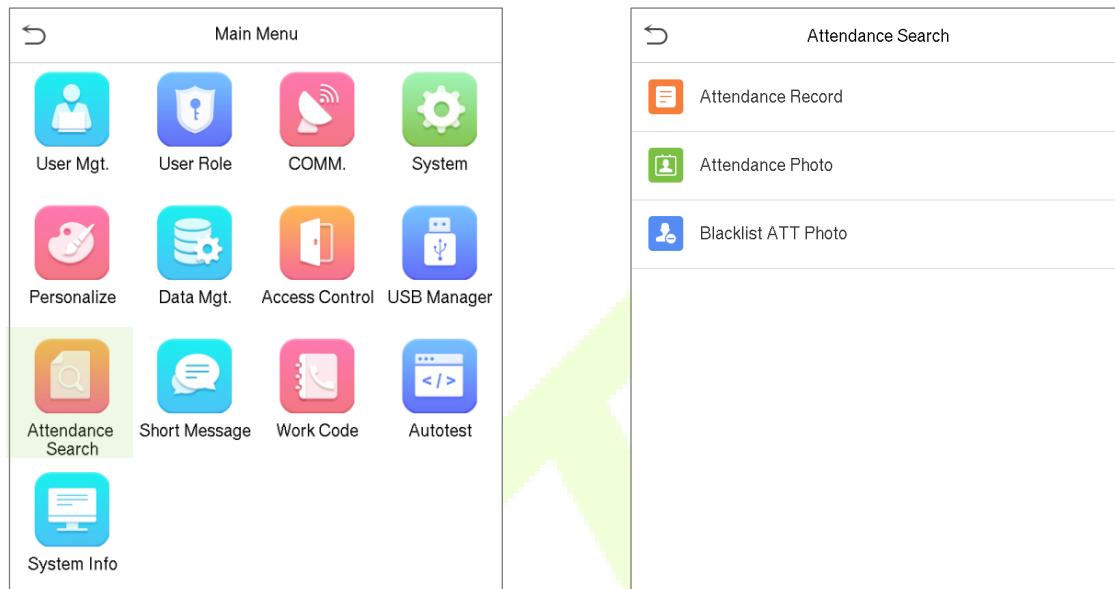


- Encrypt Attendance Data:** Toggle **Encrypt Attendance Data** to enable or disable the encryption for Attendance Data.
- Delete ATT Data:** Toggle **Delete ATT Data** to enable or disable the deletion for Attendance data.

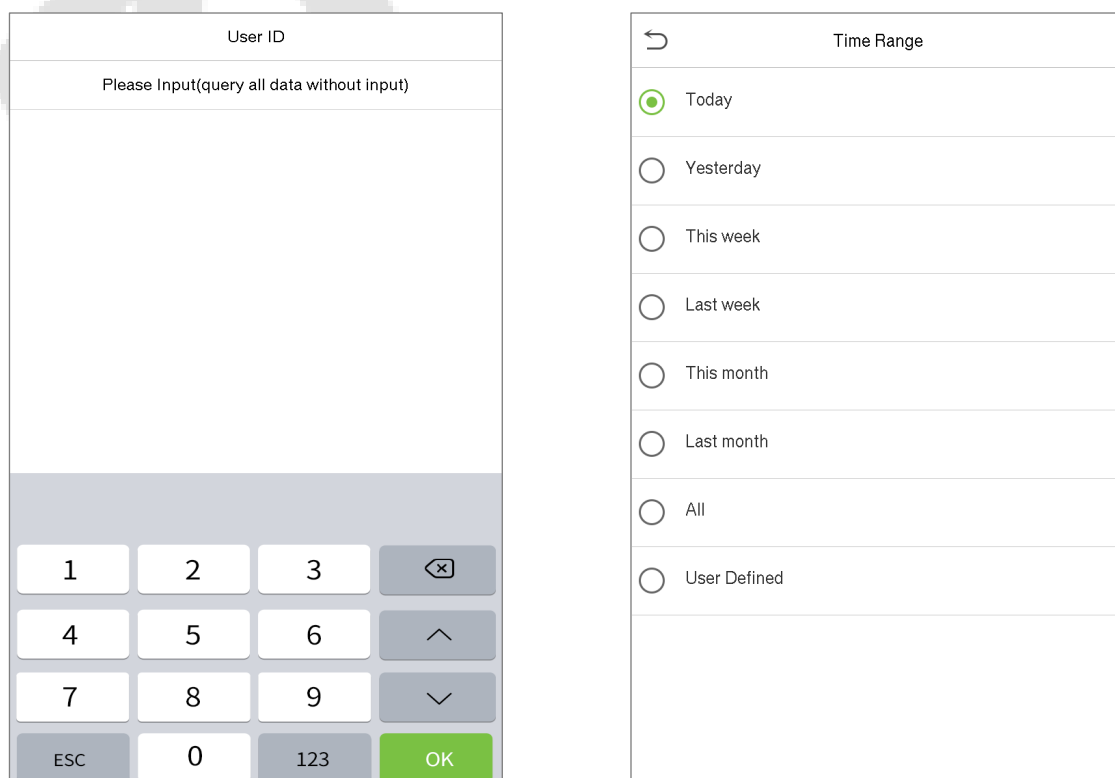
Note: The encrypt attendance data can only be imported in the software with Access 3.5 version.

13 Attendance Search

- Once the identity of a user is verified, the attendance/access record will be saved in the device. This function enables users to check their attendance/access logs.
- On the **Main Menu**, tap **Attendance Search** to search for the required Access/Attendance log.



- The process of searching for attendance and blacklist photos is similar to that of searching for attendance/access records. The following is an example of searching for attendance/access records.
- On the **Attendance Search** interface, tap **Attendance/Access Record** to search for the required record.



- Enter the user ID to be searched and tap OK.
- If you want to search for records of all users, tap OK without providing any user ID.
- Select the time range from which the records need to be searched.

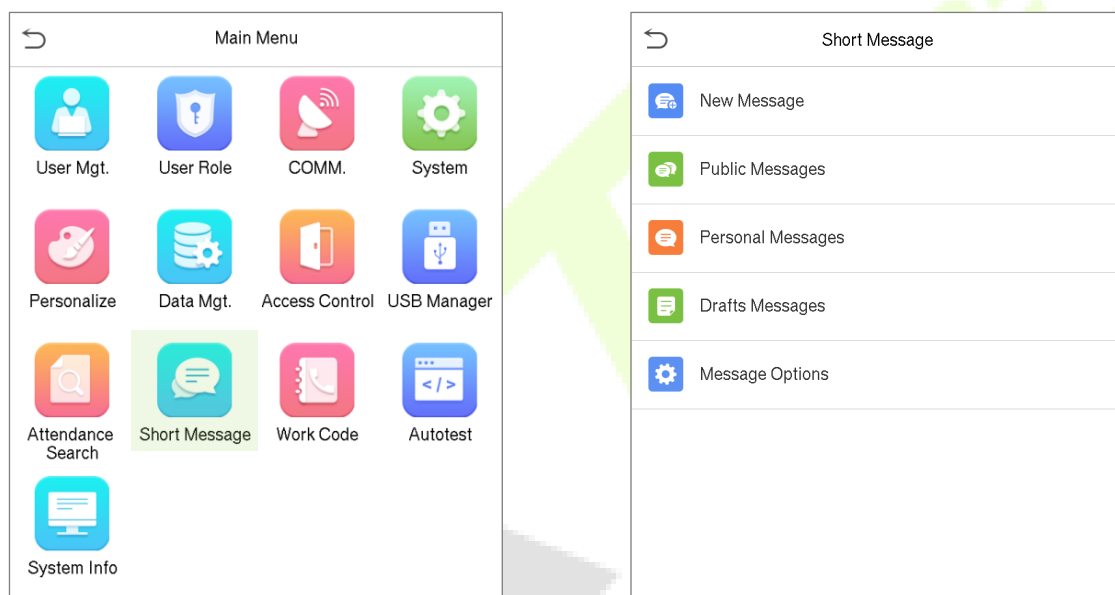
Personal Record Search		
Date	User ID	Time
12-17		Number of Records:02
	1	11:05 11:05
12-16		Number of Records:28
	1	14:00 13:59 13:58 13:57 13:57
		13:56 13:55 13:54 13:52 13:51
		13:50 13:42 13:38 11:58 11:55
		11:55 11:37 11:37 10:21 10:20
		10:20 10:19 10:19 10:18 10:16
		10:15 09:53 09:44

Personal Record Search				
User ID	Name	Time	Mode	State
1	Amy	12-16 14:00	11	255
1	Amy	12-16 13:59	11	255
1	Amy	12-16 13:58	11	255
1	Amy	12-16 13:57	11	255
1	Amy	12-16 13:57	11	255
1	Amy	12-16 13:56	12	255
1	Amy	12-16 13:55	10	255
1	Amy	12-16 13:54	4	255
1	Amy	12-16 13:52	3	255
1	Amy	12-16 13:51	4	255
1	Amy	12-16 13:50	4	255
1	Amy	12-16 13:42	3	255
1	Amy	12-16 13:38	1	255
1	Amy	12-16 11:58	1	255
1	Amy	12-16 11:55	3	255
1	Amy	12-16 11:55	1	255
1	Amy	12-16 11:37	1	255
1	Amy	12-16 11:37	1	255
1	Amy	12-16 10:21	3	255
1	Amy	12-16 10:20	3	255
1	Amy	12-16 10:20	3	255
1	Amy	12-16 10:19	3	255
1	Amy	12-16 10:19	3	255
1	Amy	12-16 10:18	3	255
Verification Mode : Password + Badge Punch State : 255				

- Once the record search succeeds, tap the record in highlighted in green to view its details.
- The above figure displays the details of the selected record.

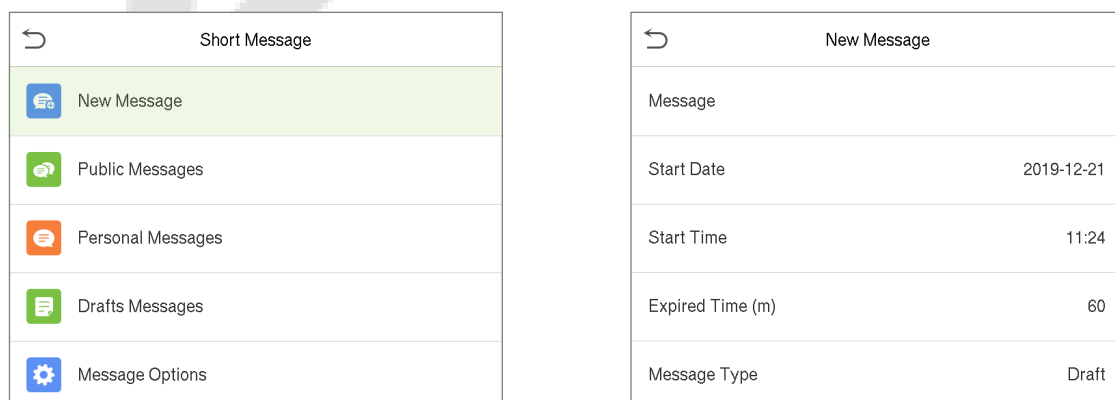
14 Short Message

- On the **Main Menu**, tap **Short Message** to set the short messages.
- SMS is similar to notice. The operator can edit the notice content in advance and make it into SMS and display on the screen.
- SMS includes common SMS and individual SMS. If common SMS is set, the common SMS  icon will be displayed on the information column at the top of standby interface in the specified time.
- If individual SMS is set, the employee who can receive SMS can see SMS after successful attendance.



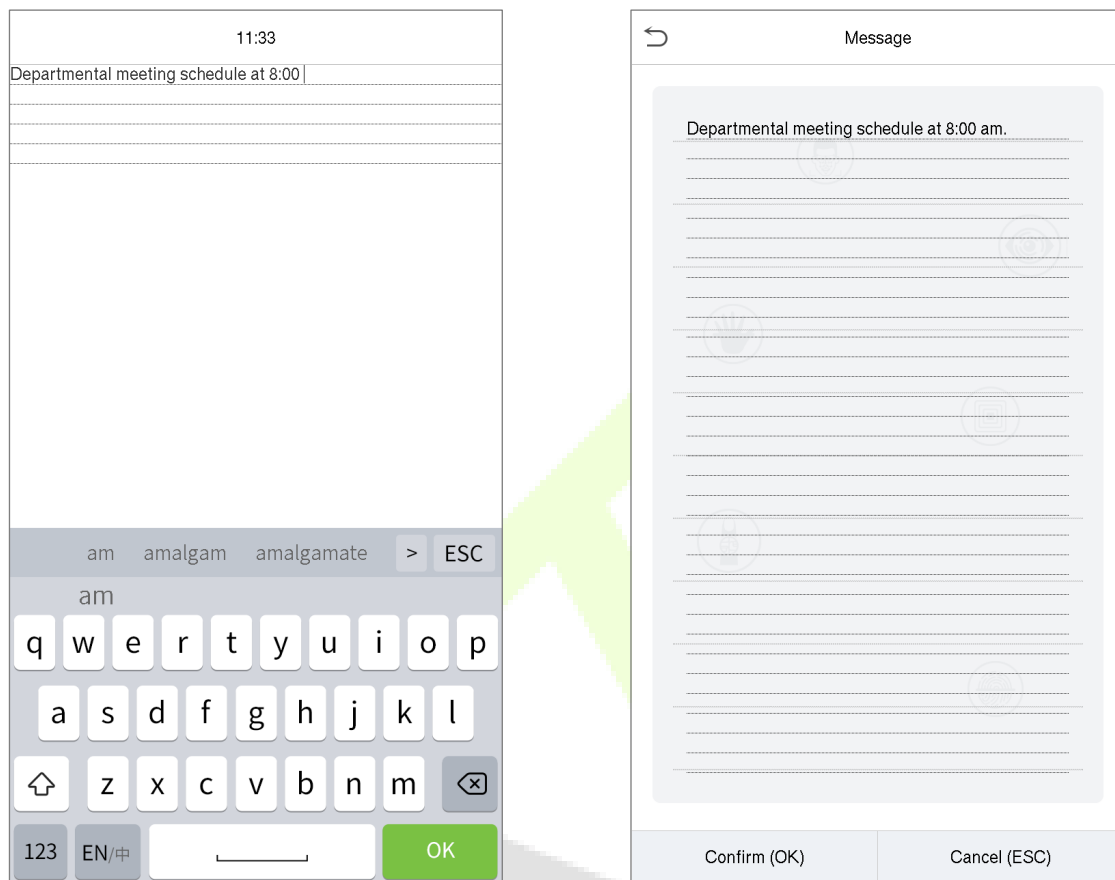
14.1 Add a New Short Message

- On the **Short Message** interface, tap **New Message** to add a new short message.



Provide the content

- On the **Short Message** interface, provide the content of the message and tap **Confirm(OK)** to save the content and quit from the Message interface.



Set the Start Date and Time

- On the **New Message** interface, tap the **Start date** and **Start time** to set the sending period for the created short message.
- The date and time will be enabled once the content for the short message is provided.

New Message		Start Date		Start Time	
Message					
Start Date	2019-12-21	2019-12-21		07:00	
Start Time	11:24	2019 12 21 YYYY MM DD		07 00 HH MM	
Expired Time (m)	60				
Message Type	Draft				
		Confirm (OK) Cancel (ESC)		Confirm (OK) Cancel (ESC)	

Setting the Expired time(m)

- On the **New Message** interface, tap the **Expired Time** to set the validity period for the SMS.
- This displays the SMS to appear within the effective time and the message will not be displayed beyond the expire time.

New Message		Expired Time (m)		New Message	
Message		☒ Never Expire		Message Departmental meeting sch...	
Start Date	2019-12-21	☐ 30		Start Date 2019-12-21	
Start Time	11:24	☐ 60		Start Time 07:00	
Expired Time (m)	60	☐ 90		Expired Time (m) Never Expire	
Message Type	Draft	☐ 120		Message Type Personal	
		☐ User Defined		Recipient	

Note: For public short messages, the effective period also comprises the display period. For private short messages, you need to set both the effective time period and the display 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.

Setting the Message Type

New Message		Message Type		New Message	
Message		☐ Public		Message	Departmental meeting sch...
Start Date	2019-12-21	☒ Personal		Start Date	2019-12-21
Start Time	11:24	☐ Draft		Start Time	07:00
Expired Time (m)	60			Expired Time (m)	Never Expire
Message Type	Draft			Message Type	Personal
				Recipient	

Public: Message will be seen by all person.

Personal: Message will be seen by selected individuals only.

Draft: Stores the text message that you wrote so far, so you can add some more content on to it later or send it later.

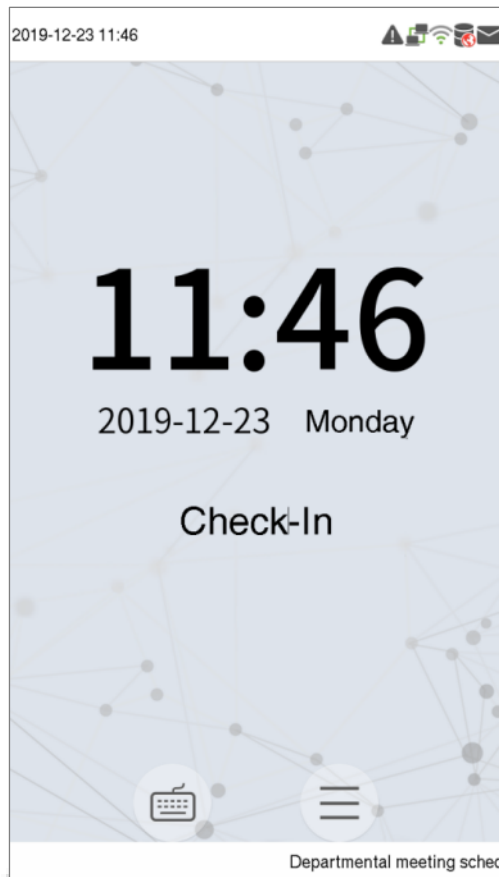
14.2 Message Options

- On the **Short Message** interface, tap **Message Options** to set the personal Message display Delay time on the initial interface.

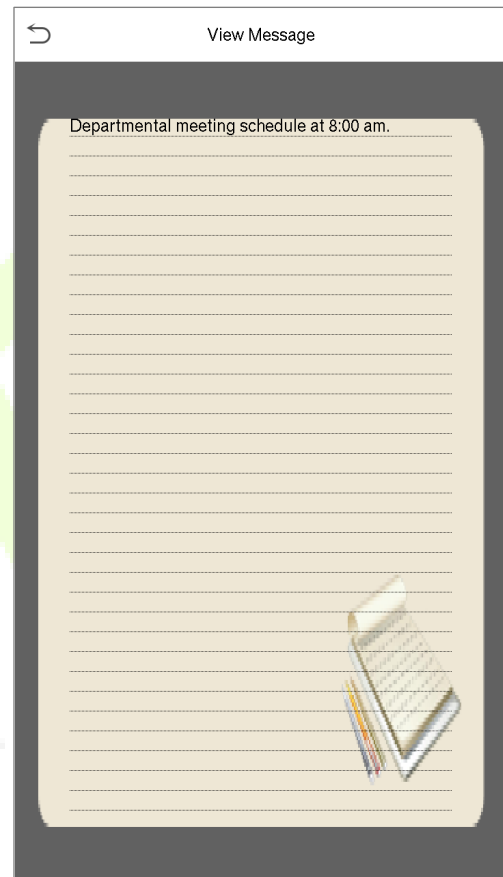
Short Message	Message Options	Expired Time (m)
☐ New Message ☒ Public Messages ☐ Personal Messages ☐ Drafts Messages ☒ Message Options	Message Show Delay(s) 60	☒ Never Expire ☐ 30 ☐ 60 ☐ 90 ☐ 120 ☐ User Defined

14.3 View the Public Messages and Personal Message

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



The public short message will be displayed in the lower part of the interface.

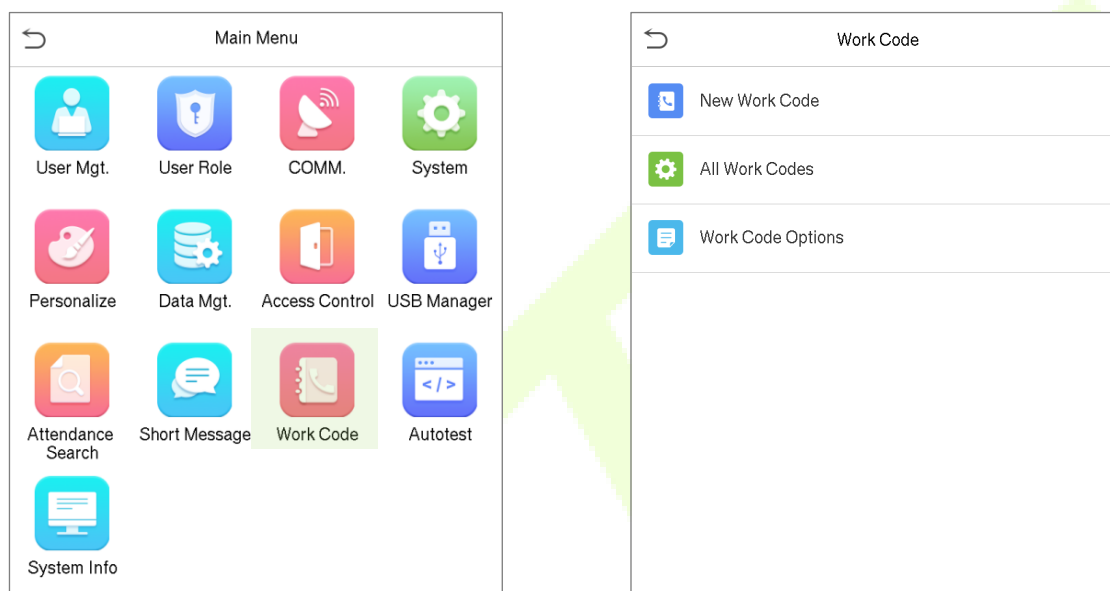


The personal short message will be displayed after successful user authentication.

15 Work Code

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

- On the **Main Menu**, tap **Work Code** to configure the work code settings.



15.1 Add a Work Code

- On the **Work Code** interface, tap **New Work Code** to add a new work code.
- On the **New Work Code** interface, fill in the following details.

ID: Provide the unique code of the work code.

Name: Provide the name of the work code.

Editing an ID

- On the **New Work Code** interface, tap on the ID field to edit ID.

The 'New Work Code' interface shows a form with two fields: 'ID' and 'Name'. The 'ID' field is highlighted in green and contains the value '1'. A green arrow points from the 'ID' field to a numeric keypad. The keypad has buttons for digits 1-9, 0, and 123, along with navigation and function keys like ESC, OK, and a backspace key.

Editing a name

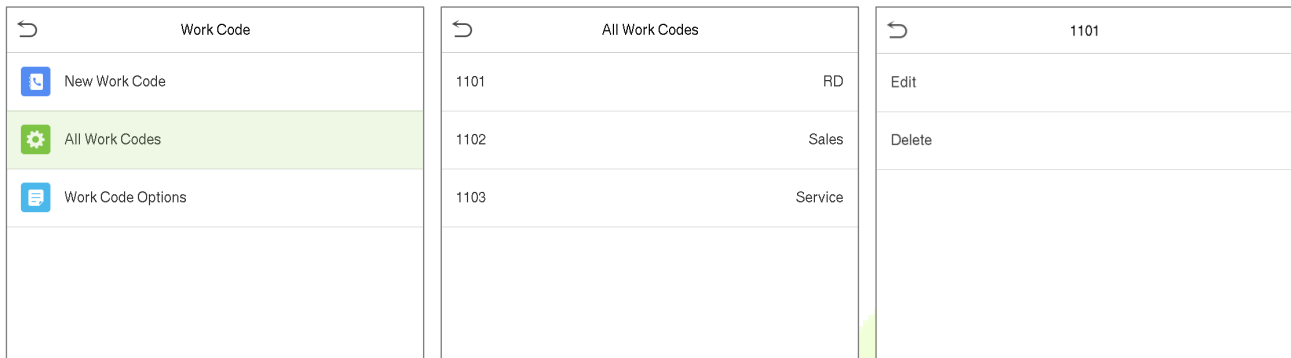
- On the **New Work Code** interface, tap on the ID field to edit ID.

The 'New Work Code' interface shows a form with two fields: 'ID' and 'Name'. The 'ID' field is highlighted in green and contains the value '1101'. A green arrow points from the 'ID' field to a QWERTY keyboard. The keyboard has buttons for letters, numbers, and symbols, along with navigation and function keys like ESC, OK, and a backspace key.

15.2 All Work Codes List

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

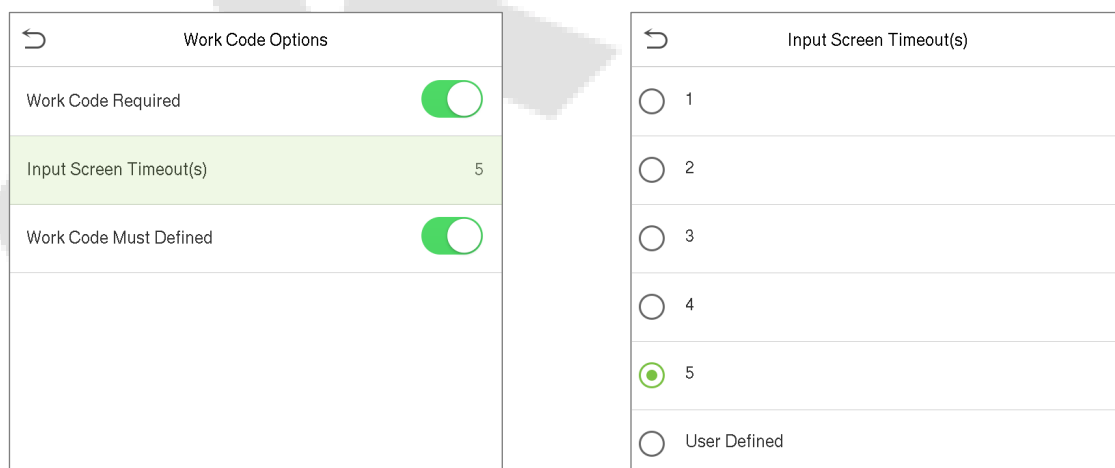
- On the **Work Code** interface, tap **All Work Code** to view and edit the required work code.



15.3 Work Code Options

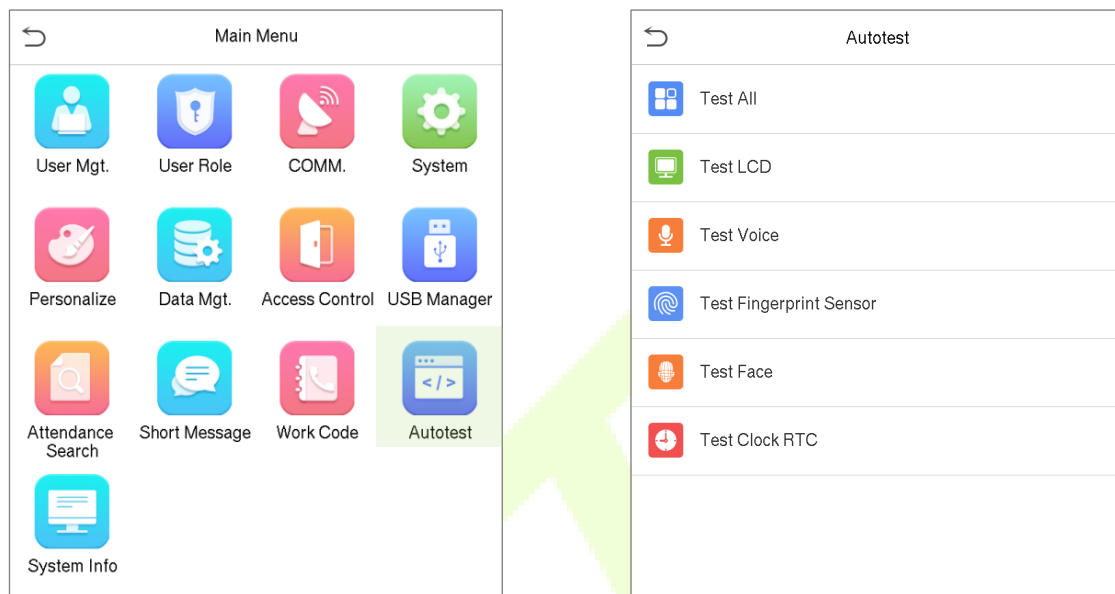
To set whether the work code must be entered and whether the entered work code must exist during authentication.

- On the **Work Code** interface, tap **Work Code Options** to configure the work code settings.



16 Autotest

- On the **Main Menu**, tap **Autotest** to automatically test whether all modules in the device function properly, which include the LCD, voice, fingerprint sensor, camera and real-time clock (RTC).

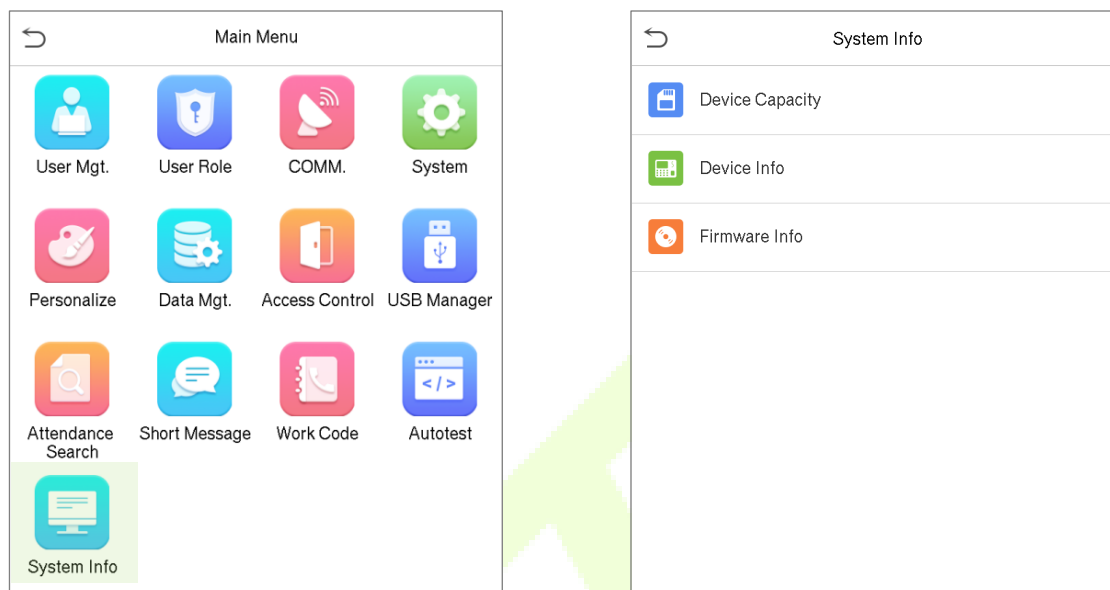


Function Description

Function Name	Description
Test All	To automatically test the LCD, Audio, Camera and the Real-Time Clock (RTC).
Test LCD	To automatically test the display effect of LCD screen by displaying full-color, pure white, and pure black to check whether the screen displays colors normally.
Test Voice	To automatically test whether the audio files stored in the device are complete and the voice quality is good.
Test Fingerprint Sensor	To test the fingerprint sensor by pressing a finger on the scanner to check if the acquired fingerprint image is clear. When you are pressing a finger on the scanner, the fingerprint image will display on the screen.
Test Face	To test if the camera functions properly by checking the pictures taken to see if they are clear enough.
Test Clock RTC	To test the RTC. The device tests whether the clock works normally and accurately with a stopwatch. For Stopwatch tap on the screen to start the counting and tap on it again to stop the counting.

17 System Information

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



Function Description

Function Name	Description
Device Capacity	Displays the current device's user storage, admin user, password, fingerprint, face storage, badge storage, attendance records, attendance and blacklist photos, and user photos.
Device Info	Displays the device's name, serial number, MAC address, fingerprint algorithm, face algorithm, platform information, version information, manufacturer and manufacture date.
Firmware Info	Displays the firmware version and other version information of the device.

Appendix 1 Statement on the Right to Privacy

Dear Customers:

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

We Declare That:

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

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

Note:

The 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.

Appendix 2 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.



ZK Building, Wuhe Road, Gangtou, Bantian, Buji Town,
Longgang District, Shenzhen China 518129

Tel: +86 755-89602345

Fax: +86 755-89602394

