

USER MANUAL



FGA-2000

Fingerprint + Card + Access control

The latest BioID anti-fake fingerprint
High speed ID Card Verification
Advanced access control function



FOLLOW US
www.iomotech.com

About the Manual

This manual introduces the operations of FGA-2000 product.

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

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.
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	OVERVIEW	6
1.1	INTRODUCTION	6
1.2	FEATURES	6
1.3	SPECIFICATIONS.....	6
2	INSTRUCTIONS FOR USE.....	7
2.1	FINGER PLACEMENT.....	7
2.2	VERIFICATION MODES.....	7
2.2.1	BIOMETRICS.....	7
2.2.2	PASSWORD	9
2.2.3	ACCESS CARD★	9
3	MAIN MENU	9
4	USER MANAGEMENT	11
4.1	ADDING A NEW USER.....	11
4.1.1	ENTER USER ID AND NAME.....	11
4.1.2	ENTER USER ROLE.....	11
4.1.3	VERIFICATION MODE.....	12
4.1.4	ENROLLING A FINGERPRINT.....	12
4.1.5	ENROLLING A BADGE★	12
4.1.6	ENROLLING A PASSWORD	13
4.2	MANAGING EXISTING USERS.....	13
4.2.1	EDIT USER	13
4.2.2	DELETE USER.....	13
4.3	DISPLAY STYLE.....	14
5	USER ROLE	14
5.1	CREATING A NEW ROLE AND ITS FUNCTION	15
6	COMMUNICATION SETTING.....	15
6.1	ETHERNET.....	16
6.2	SERIAL COMM	16
6.3	PC CONNECTION.....	16
6.4	WIEGAND SETUP★	17
6.4.1	WIEGAND INPUT★	17
6.4.2	WIEGAND OUTPUT★	19
7	SYSTEM	20
7.1	DATE TIME	21
7.2	ATTENDANCE.....	21
7.3	FINGERPRINT PARAMETERS.....	22
7.4	RESET.....	23
7.5	USB UPGRADE.....	23

8	PERSONALIZE.....	24
8.1	USER INTERFACE	24
8.2	VOICE	25
8.3	BELL SCHEDULE	25
8.3.1	NEW BELL SCHEDULE	25
8.3.2	ALL BELL SCHEDULE	26
8.3.3	OPTIONS	26
8.4	PUNCH STATE OPTIONS.....	26
8.5	SHORTCUT KEY MAPPINGS.....	27
9	DATA MGT.....	29
9.1	DELETE DATA.....	29
9.2	BACKUP DATA	29
9.3	RESTORE DATA.....	30
10	ACCESS CONTROL	30
10.1	SETTING DOOR PROPERTIES.....	31
10.2	DEFINING TIME SCHEDULES.....	32
10.3	SETTING HOLIDAYS.....	33
10.4	CREATING ACCESS GROUPS	33
10.5	MULTI-USER AUTHENTICATION	34
10.6	DURESS SETTINGS.....	35
11	USB MANAGER.....	35
11.1	DOWNLOAD	36
11.2	UPLOAD	36
11.3	DOWNLOAD OPTIONS	37
12	ATTENDANCE SEARCH	37
13	PRINT.....	38
13.1	DATA FIELD SETUP.....	38
13.2	PRINTER OPTIONS.....	39
15	WORK CODE.....	39
15.1	NEW WORK CODE.....	40
15.2	ALL WORK CODE	40
15.3	WORK CODE OPTIONS	40
16	AUTOTEST	41
17	SYSTEM INFO.....	41
19	APPENDIX	42
19.1	T9 INPUT.....	42
19.2	RULES TO UPLOAD PICTURE	42
	ECO-FRIENDLY OPERATION	44

1 Overview

1.1 Introduction

P160 is a multibiometric identification time & attendance and access control terminal, which can connect with third party electric lock, door sensor, and exit button etc.

With the latest palm/fingerprint identification algorithm and streamlined technology, it can hold up to 3000 fingerprint templates without dividing into groups.

Communicating via TCP/IP, and USB client, it ensures a smooth connection and data transfer. Amazing verification speed and intuitive operation process make it popular. Elaborately designed and finely processed, it matches your slap-up office perfectly.

1.2 Specifications

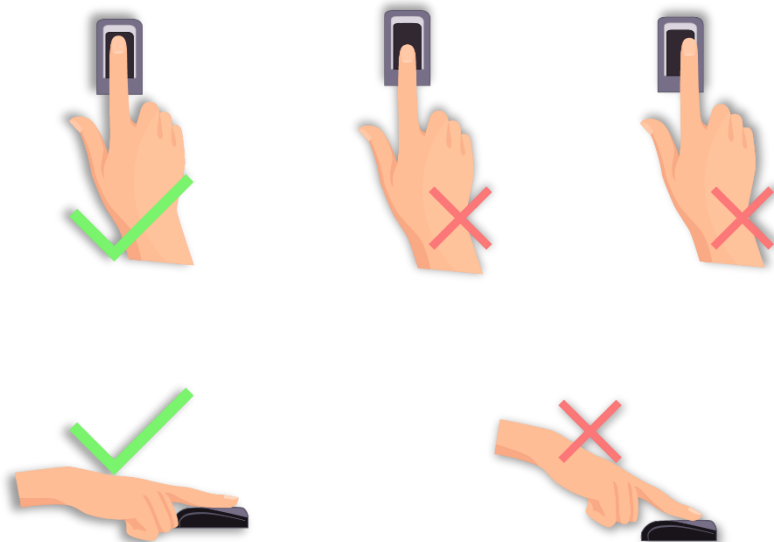
Display	2.8-inch TFT color Display
Capacity	Fingerprint templates: 5,000
ID Card Capacity	10,000 Card
Logs Capacity	200,000
Communication	TCP/IP, USB,
Standard Functions	Automatic Status Switch, Self-Service Query, AC module 1: Exit Button, Door Lock, Alarm, 12V OUT, AUX IN, Door Sensor; Work Code, T9 Input, 9 Digit User ID, DST, Scheduled-bell
Optional Functions	ID Card, Mifare Card, RS485, Wiegand IN/OUT; PoE, Battery Module, ADMS
Power Supply	12V/1.5A
Verification Speed	≤1 sec
Operating Temperature	0-45 °C
Operating Humidity	20%-80%

2 Instructions for Use

2.1 Finger Placement

Recommended fingers: The index finger, middle finger or ring finger; avoid using the thumb and little finger (because they press the collection window is usually very clumsy).

➤ **Recommended placement**



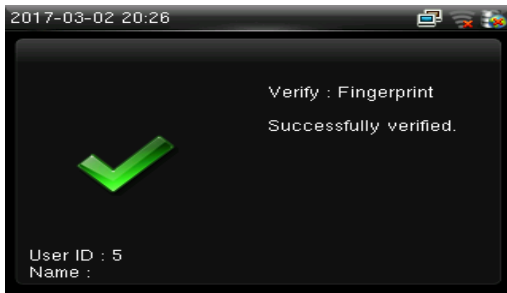
2.2 Verification Modes

2.2.1 Biometrics

➤ **Fingerprint**

- **1:N fingerprint verification**

The device compares the current fingerprint with all users' fingerprints in the device. Use the proper way with one of the recommended fingers to enroll and verify. There are two responses after verification: **Successfully verified** and **Failed to verify**.



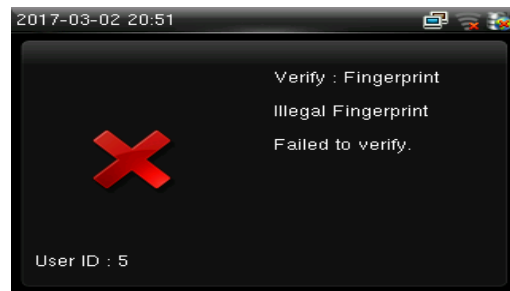
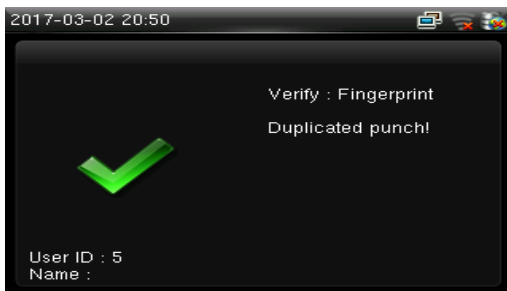
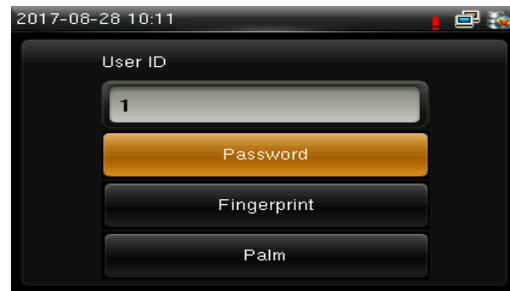
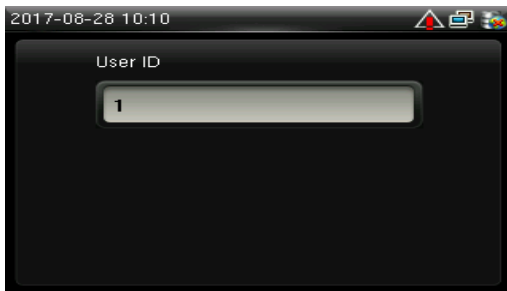
Successfully verified



Failed to verify

- **1:1 fingerprint verification**

The device compares the current fingerprint with the fingerprint of the user whose ID is entered. The user chooses this mode unless poor recognition. Enter User ID and press "fingerprint", there are two responses after verification: **Successfully verified** and **Failed to verify**.

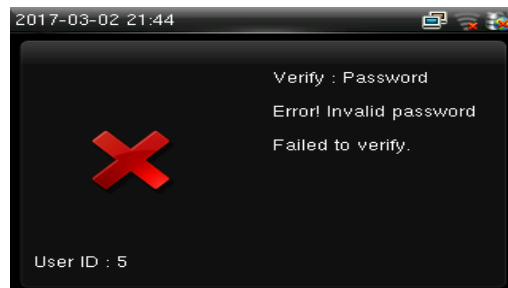
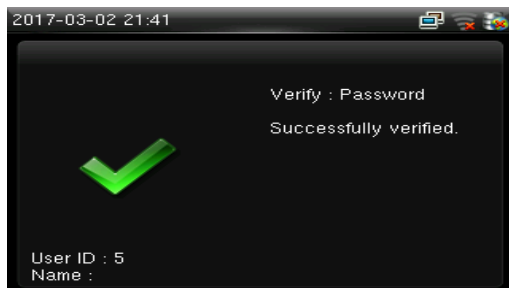


Note:

- 1) The device prompts "Invalid ID" when there is no such user.
- 2) The device prompts "Please try again" when failed to verify. After 2 attempts, if it fails the 3rd time, it returns to the initial interface.

2.2.2 Password

The device compares entered password with one user's password whose ID is input. Enter user ID, press "Password" and enter your password. There are two responses after verification:

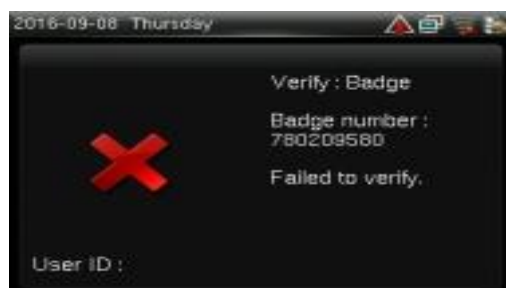
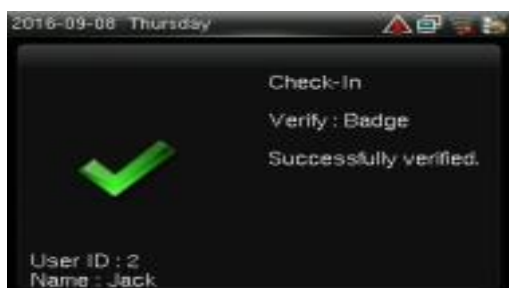


Note: The device prompts "Incorrect password" when failed to verify. After 2 attempts, if it fails after the 3rd time, it returns to the initial interface.

2.2.3 Access Card★

Card function is optional, only products with a built-in card module are equipped with card verification function. Please contact our technical support as required.

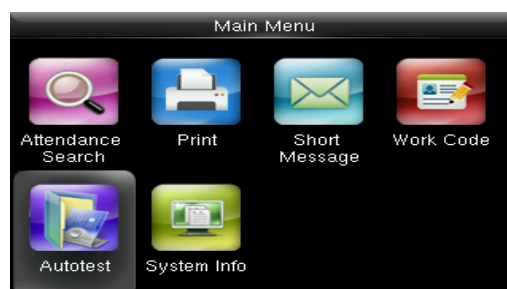
Swipe your registered badge surround the fingerprint sensor in standby mode:



The device "prompts" Duplicated Punch" when you swipe badge twice. The device prompts "Ou-Ou" when the badge is unregistered.

3 Main Menu

Start the device; press [M/OK] to enter the Main Menu. Press ▼ to scroll the page down.



Function Definition:

User Mgt. (User Management): Add, edit, and delete users' information, including user ID, name, user role, fingerprint, palm, password, badge number★ and access control role.

User Role: Set the privilege of defined roles, that is, the privilege of operating menu.

Comm. (Communication Setting): Set the communication parameters between device and PC, including ethernet parameters such as IP address etc., Serial Comm, PC connection, Wireless Network★, Cloud Server★ and Wiegand settings★.

System: Set system parameters, such as date/time, attendance parameters, palm and fingerprint parameters, reset and USB upgrade.

Personalize: Set user interface parameters, voice, bell schedules, punch state options and shortcut key mappings.

Data Mgt. (Data Management): Delete/ Backup/ Restore data stored in the device.

Access Control: Set access control options, time schedule/holidays/access group/combined verification group, and duress options.

USB Manager: Download and upload attendance data, user data, work code, short message, etc. With USB disk, you can import data restored in the device into attendance software, or import data into other devices.

Attendance Search: It is convenient for employees to search his or her attendance record restored in this device.

Print: To set printing information and functions (if printer is connected to the device).

Short Message: Add/check/edit/delete public and personal messages. Set options.

Work Code: Add/check/edit/delete work code. If this function is enabled, you must select one or enter an existence work code after verification.

Autotest: Test whether each module is available or not, including LCD, voice, keyboard, fingerprint sensor, palm and clock RTC.

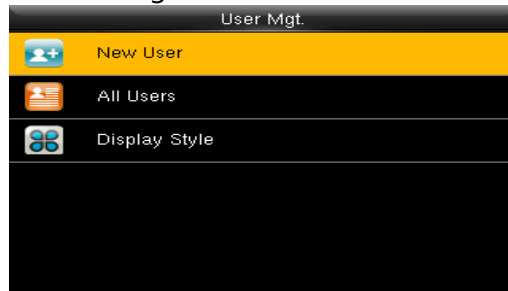
System Info: Check device capacity, basic information, and firmware information etc.

4 User Management

4.1 Adding a New user

Only the registered user can make verification in the device.

Start the device, enter into the Main Menu. Enter into "User Mgt." → "New User".



4.1.1 Enter User ID and Name

Press ▼/▲ to select any of the fields on the New User interface, press [M/OK]:

New User	
User ID	3
Name	
User Role	Normal User
Palm	0
Fingerprint	0
Badge Number	

Note: You can input an ID, or use which is allotted by the device.

4.1.2 Enter User Role

Press ▼ / ▲ to select "User Role" on the New User interface, press [M/OK]:

User Role	
Normal User	
Super Admin	

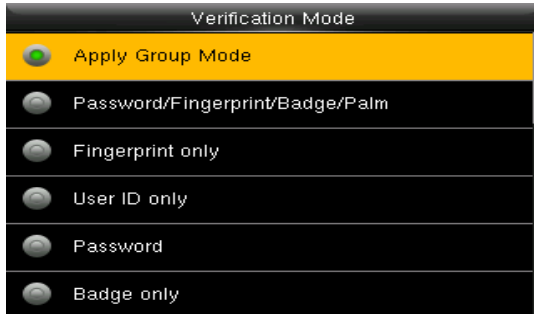
Super Admin: A super admin is granted rights to operate all functions and menus in the device.

Normal User: Normal user is only allowed to punch, query its own attendance record, check messages.

Note: You had better to enroll a super admin for

4.1.3 Verification Mode

Enter into "New user" → "Access Control Role". Press ▼ / ▲ to select "Verification Mode" on the interface, press [M/OK]:



There are several optional modes to set the verification way.

4.1.4 Enrolling a Fingerprint

Press ▼ / ▲ to select "Fingerprint" on the New User interface, press [M/OK]:



1. Press numeric key corresponding to the fingerprint as you want, then press [M/OK].
2. Press your fingerprint on the sensor three times upon prompting by the device.

Note: You need to re-enroll if the device says "Please try again".

4.1.5 Enrolling a Badge★

Press ▼ / ▲ to select "Badge Number" on the New User interface, press [M/OK]:

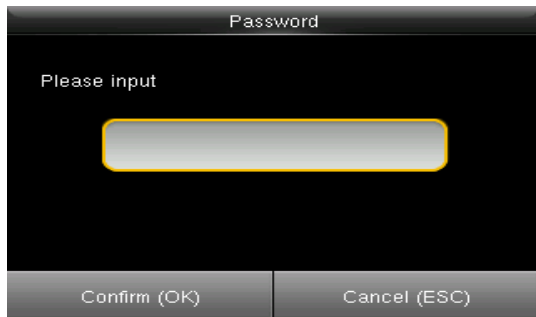


Swipe your badge around the fingerprint sensor.

Note: Please take another badge if the device displays "Error! Badge already enrolled". The Badge must be ID/IC card.

4.1.6 Enrolling a Password

Press ▼ / ▲ to select “Password” on the New User interface, press [M/OK]:

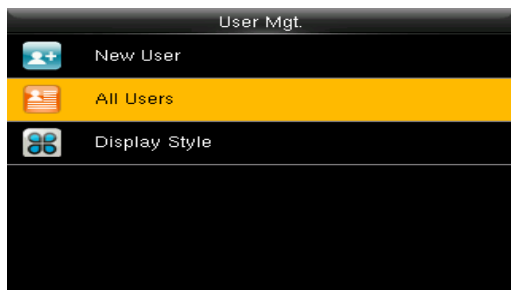


The screen is titled "Password". It displays the text "Please input" above a rectangular input field with a yellow border. At the bottom, there are two buttons: "Confirm (OK)" on the left and "Cancel (ESC)" on the right.

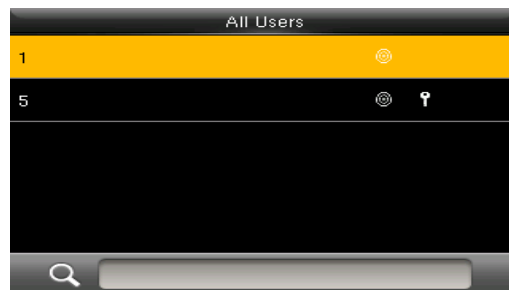
Input 1-8 digits password and press [M/OK], then re-type the password.

4.2 Managing Existing Users

Start the device, enter into the Main Menu. Enter into “User Mgt.”→“All Users”.

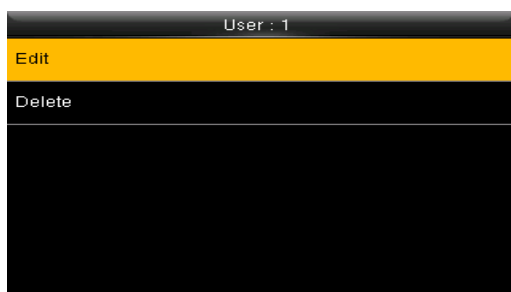


The screen is titled "User Mgt.". It shows three menu items: "New User" with a person icon, "All Users" with a list icon and highlighted in yellow, and "Display Style" with a gear icon.



The screen is titled "All Users". It displays a list of users. The first user has ID "1" and a fingerprint icon. The second user has ID "5" and icons for both fingerprint and password. At the bottom, there is a search bar with a magnifying glass icon.

4.2.1 Edit User



The screen is titled "User : 1". It shows two menu items: "Edit" with a pencil icon and highlighted in yellow, and "Delete" with a trash can icon.



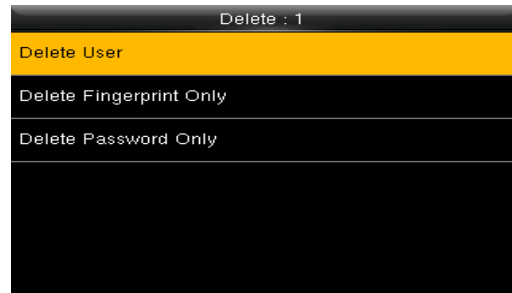
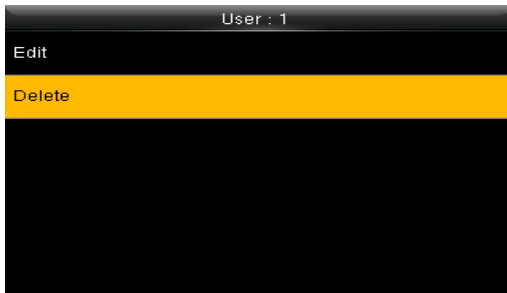
The screen is titled "Edit : 1". It displays a list of user details:

User ID	1
Name	
User Role	Normal User
Palm	0
Fingerprint	1
Password	XXXXXX

All information can be modified except User ID.

4.2.2 Delete User

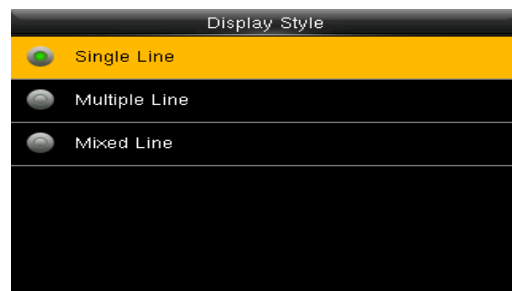
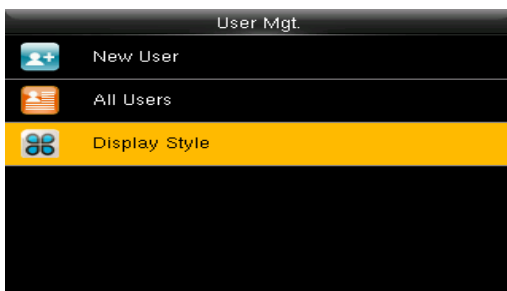
Press ▼ / ▲ to select a user to edit and press [M/OK]. Enter into “Delete”:



You can choose different kinds of user data to delete.

4.3 Display Style

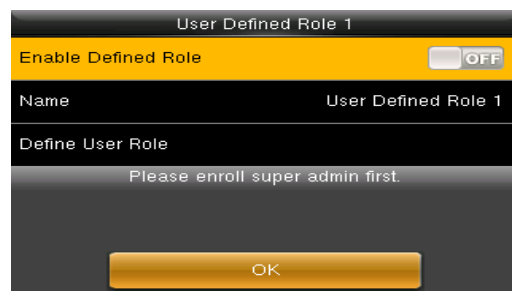
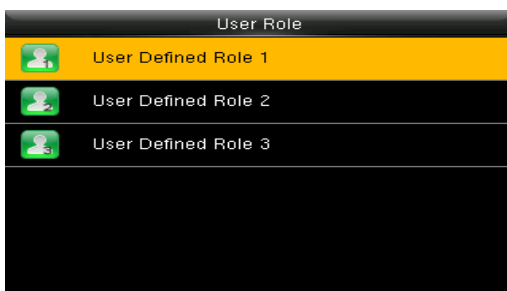
The default style is "Single Line". Enter into "User Mgt." → "Display Style":



5 User Role

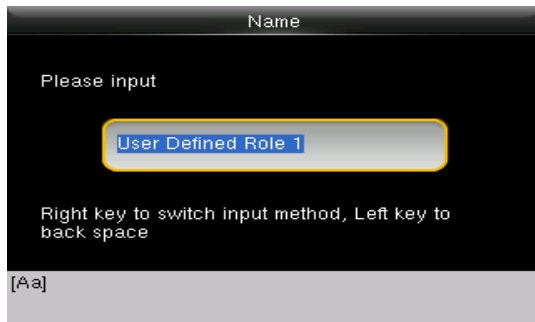
Use to define roles to operate the device. You can specify the available menus to operate for a role. There are 3 roles.

Enter into "User Role". Press one of the three roles to edit:



A Super admin must be enrolled before a new role is defined.

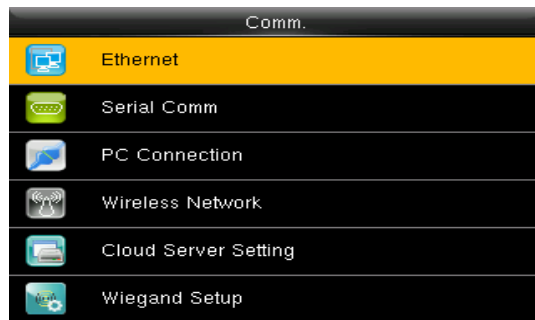
5.1 Creating a New Role and its Function



1. Enter name with T9 Input.
2. You can define more than one available menu for a role. Press [M/OK] to select.

6 Communication Setting

Set communication parameters. Enter into "Comm."



1. **Ethernet:** The device can communicate with PC each other via the parameters you set.
2. **Serial Comm:** The device can communicate with PC each other via the serial port parameters you set.
3. **PC Connection:** Set the password and device ID so that you can connect the device with software in PC.
4. **Wireless Network★:** Turn on /off the WIFI setting.
5. **Cloud Server Setting★:** Settings used for connecting with ADMS server.
6. **Wiegand Setup★:** The device can communicate with other device via the

6.1 Ethernet

Enter into "Comm." → "Ethernet".

Ethernet	
IP Address	192.168.6.202
Subnet Mask	255.255.255.0
Gateway	0.0.0.0
DNS	0.0.0.0
TCP COMM.Port	4370
DHCP	<input type="checkbox"/> OFF

1. **IP Address:** Modify it if necessary. It cannot be same with PC.
2. **Subnet Mask:** Modify it if necessary.
3. **Gateway:** It is necessary to set an address if the device and PC are in different network segment. Modify it if necessary.
4. **DNS:** Set the address of your DNS server.
5. **TCP COMM Port:** Set the TCP communication port.
6. **DHCP:** Dynamic Host Configuration Protocol, which is used to allocate dynamic IP addresses to clients by a server.
7. **Display in Status Bar:** Whether to display

6.2 Serial Comm

Serial Comm	
Serial port	master unit
Baudrate	115200
USB	Print Function
USB Baudrate	9600

1. **Serial port:** When serial port (RS232/RS485) is used for communication of device and PC, this setting need to be checked:
2. **Baudrate:** Used for communication with PC. RS232 is recommended for high speed.

Note: There are 5 baudrate types available for RS232: 9600, 19200, 38400, 57600 and 115200; "9600" is not applicable to RS485. Reboot the device to make the change active.

6.3 PC Connection

To improve the security of attendance data, connection password needs to be set here. Enter into Comm. → "PC Connection".

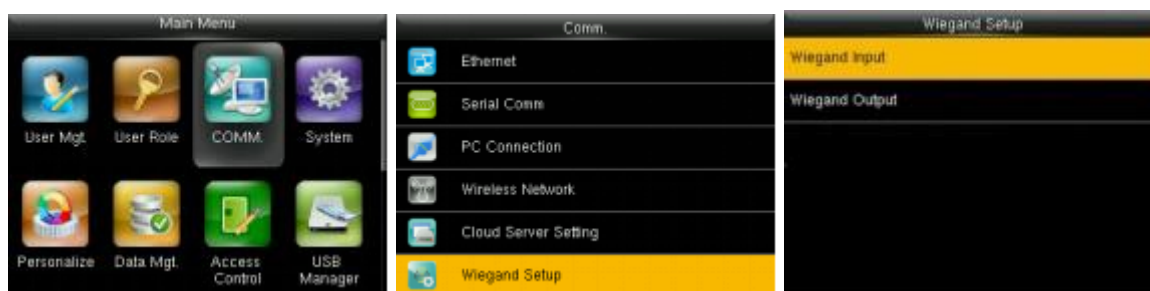
PC Connection	
Comm Key	0
Device ID	1

1. **Comm Key:** Set 1-6 digits connection password, the password must be input when PC software is to connect device to read data.
2. **Device ID:** The ID is in the range of 1-254. If RS232 or RS485 is enabled, this ID needs to be input in the software communication interface.

Cloud Server Setting	
Server mode	ADMS
Enable Domain Name	<input type="checkbox"/> OFF
Server Address	0.0.0.0
Server port	8081
Enable Proxy Server	<input type="checkbox"/> OFF

1. **Enable Domain Name:** When the domain name mode is enabled, you access a website using a domain name in the format of http://; otherwise, you must enter an IP address for website access.
2. **Server Address:** IP address of Webserver
3. **Server port:** Port used by Webserver
4. **Enable Proxy Server:** When you enable the proxy function, set the IP address and port number of the proxy server. This option indicates whether to use a proxy IP address. You may choose to enter the proxy IP address or the server address for Internet access,

6.4 Wiegand Setup★



In the initial interface, press [M/OK] > **COMM.** > **Wiegand Setup** to enter the **Wiegand Setup** interface.

6.4.1 Wiegand Input★

Wiegand Input connector supports card reader, or connects the device as a master device to another device (slave device), forming a master/slave system.

Wiegand Setup		Wiegand Options		Wiegand Options	
Wiegand Input		Wiegand Format		26Bits	Wiegand26
Wiegand Output		Wiegand Bits	26	34Bits	no using
		Pulse Width(us)	100	36Bits	no using
		Pulse Interval(us)	1000	37Bits	no using
		ID Type	Badge Number	50Bits	no using

Wiegand Format: User can choose among the following built-in Wiegand formats: Wiegand 26, Wiegand 26a, Wiegand 34, Wiegand 34a, Wiegand 36, Wiegand 36a, Wiegand 37, Wiegand 37a, Wiegand 50 and **No using**. The value **no using** means that the format with this bit number is not used. The following table describes all the formats.

Wiegand Bits: Number of bits of Wiegand data. After choosing [Wiegand input bits], the device will use the set number of bits to find the suitable Wiegand format in [Wiegand Format].

Pulse Width (us): The width of pulse sent by Wiegand. The default value is 100 microseconds, which can be adjusted within the range of 20 to 100 microseconds.

Pulse Interval (us): The default value is 1000 microseconds, which can be adjusted within the range of 200 to 20000 microseconds.

ID Type: Input content included in Wiegand input signal. **User ID** or **Badge Number** can be chosen.

Definitions of Wiegand Formats:

Wiegand Format	Definition
Wiegand26	EEEEEEEEEEEEEEEEEEEEEEEEEEEECO Consists of 26 bits of binary code. The 1 st bit is the even parity bit of the 2 nd to 13 th bits, while the 26 th bit is the odd parity bit of the 14 th to 25 th bits. The 2 nd to 25 th bits are the card number.
Wiegand26a	ESSSSSSSSSSSSSSSSSSSSSSSSSSSSCO Consists of 26 bits of binary code. The 1 st bit is the even parity bit of the 2 nd to 13 th bits, while the 26 th bit is the odd parity bit of the 14 th to 25 th bits. The 2 nd to 9 th bits are the site code, while the 10 th to 25 th bits are the card number.
Wiegand34	EEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEECO Consists of 34 bits of binary code. The 1 st bit is the even parity bit of the 2 nd to 17 th bits, while the 34 th bit is the odd parity bit of the 18 th to 33 rd bits. The 2 nd to 25 th bits are the card number.
Wiegand34a	ESSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSCO Consists of 34 bits of binary code. The 1 st bit is the even parity bit of the 2 nd to 17 th bits, while the 34 th bit is the odd parity bit of the 18 th to 33 rd bits. The 2 nd to 9 th bits are the site code, while the 10 th to 25 th bits are the card number.
Wiegand36	FFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCMME Consists of 36 bits of binary code. The 1 st bit is the odd parity bit of the 2 nd to 18 th bits, while the 36 th bit is the even parity bit of the 19 th to 35 th bits. The 2 nd to 17 th bits are the device code, the 18 th to 33 rd bits are the card number, and the 34 th to 35 th bits are the manufacturer code.
Wiegand36a	FFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCCO

Wiegand 50. Multiple selections are available, but the actual Wiegand format will depend on the option in **[Wiegand output bits]**.

For Example: If the 26-bit Wiegand26, 34-bit Wiegand34a, 36-bit Wiegand36, 37-bit Wiegand37a and 50-bit Wiegand50 are chosen in **[Wiegand Format]**, but 36 bits is selected in **[Wiegand output bits]**, then the actual Wiegand format for use will be 36-bit Wiegand36.

Wiegand output bits: Number of bits of Wiegand data. After choosing **[Wiegand output bits]**, the device will use the set number of bits to find the suitable Wiegand format in **[Wiegand Format]**.

Failed ID: It is defined as the output value of failed user verification. The output format depends on the **[Wiegand Format]** setting. The default value ranges from 0 to 65535.

Site Code: It is similar to device ID except that it can be set manually and repeatable with different devices. The default value ranges from 0 to 256.

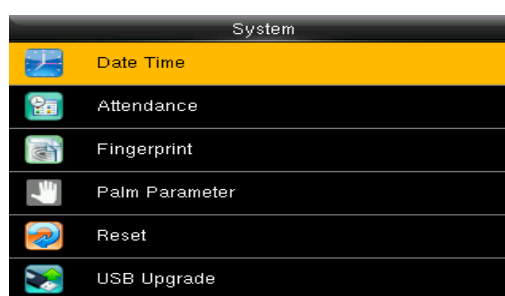
Pulse Width (us): The width of pulse sent by Wiegand. The default value is 100 microseconds, which can be adjusted within the range of 20 to 100 microseconds.

Pulse Interval (us): The default value is 1000 microseconds, which can be adjusted within the range of 200 to 20000 microseconds.

ID Type: Output content after successful verification. User ID or card number can be chosen.

7 System

Set system parameters to meet user's demand as many as possible. Including the Date Time, Attendance, Fingerprint and so on.



7.1 Date Time

Set the system data and time. Enter into "System" → "Date Time".



1. **Set Date/Time:** Set date and time of device.
2. **24-Hour Time:** Whether to use the 24-hour display mode. If not, the 12-hour display mode is adopted.
3. **Date Format:** Set the date format: YY-MM-

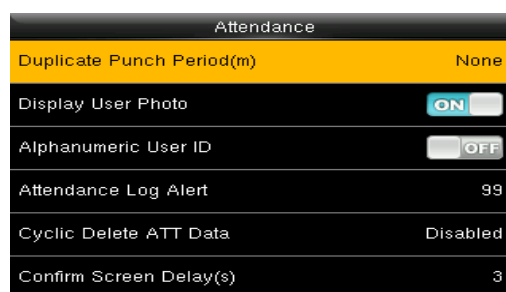
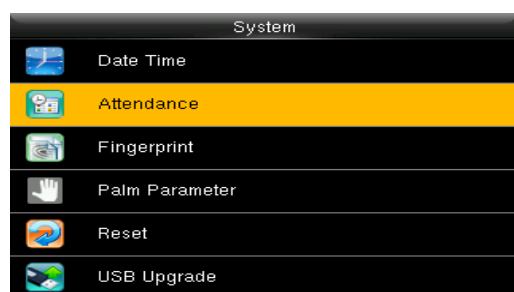
Daylight Saving Time:

The DST is a widely-used system of adjusting the local time forward to save energy. The uniform time adopted during the implementation of this system is known as the DST. Typically, clocks are adjusted forward one hour in the summer to make full use of illumination resources and save electricity. Clocks are adjusted backward in autumn. The DST regulations vary with countries. The device supports the DST function to adjust forward one hour at $\times\times$ (Hour): $\times\times$ (Minute) $\times\times$ (Day) $\times\times$ (Month) and backward one hour at $\times\times$ (Hour): $\times\times$ (Minute) $\times\times$ (Day) $\times\times$ (Month). For example, adjust the clock forward one hour at 08: 00 on April 1 and backward one hour at 08: 00 on October 1. Daylight Saving Mode: Select the date mode or week mode. Daylight Saving Setup: Set the DST start time and end time.

Note: The end time of DST cannot be set for next year. More specifically, the end time must be later than the start time in the same year.

7.2 Attendance

Enter into "System" → "Attendance".



Parameters of Attendance interface state as below:

Duplicate Punch Period (m): In set time period (unit: minute), repeated attendance record of a user will not be saved (the valid time is 1~999999 minutes).

Display User Photo:

No Photo: The device does not take photo as users verify.

Take Photo, no save: Take photo, but not save photo as users verify.

Take photo and save: Take and save photo as users verify.

Save on successful verification: Take and save photo as users verify successfully.

Save on failed verification: Take and save photo as users fail to verify.

Attendance Log Alert: When remainder log capacity is less than the set value, the device will prompt an alert message automatically. The valid value is 1~9999.

Cyclic Delete ATT Data: When Attendance records reach to the maximum capacity, the amount to delete attendance Data one time. The valid value is 1~999.

Confirm Screen Delay (s): The delay to display the verification result, the value is 1~9.

Expiration Rule: The choices for the function of the users' validity.

Expiration Rule Options: The settings for the end of validity.

7.3 Fingerprint Parameters



In the initial interface, press **[M/OK]** > **System** > **Fingerprint** to enter the **Fingerprint** setting interface.

1:1 Match Threshold: Under 1:1 Verification Method, only when the similarity between the verifying fingerprint and the user's registered fingerprint is greater than this value can the verification succeed.

1:N Match Threshold: Under 1:N Verification Method, only when the similarity between the verifying fingerprint and all registered fingerprints is greater than this value can the verification succeed.

Recommended Match Threshold:

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

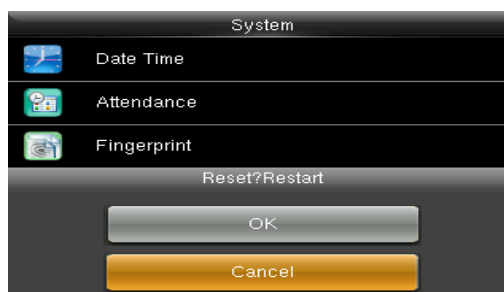
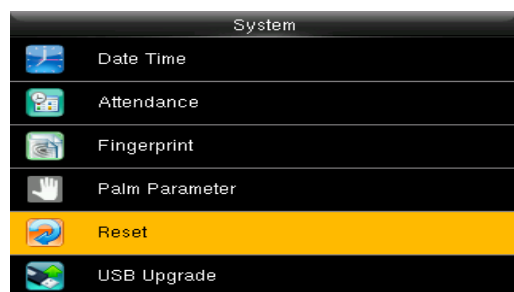
FP Sensor Sensitivity: To set the sensibility of fingerprint collection. It is recommended to use the default level “**Medium**”. When the environment is dry, resulting in slow fingerprint detection, you can set the level to “**High**” to raise the sensibility; when the environment is humid, making it hard to identify the fingerprint, you can set the level to “**Low**”.

1:1 Retry Times: In 1:1 Verification or Password Verification, users might forget the registered fingerprint or password, or press the finger improperly. To reduce the process of re-entering user ID, retry is allowed; the number of retry can be within 1~9.

Fingerprint Image: To set whether to display the fingerprint image on the screen in registration or verification. Four choices are available: Show for enroll, Show for match, Always show, None.

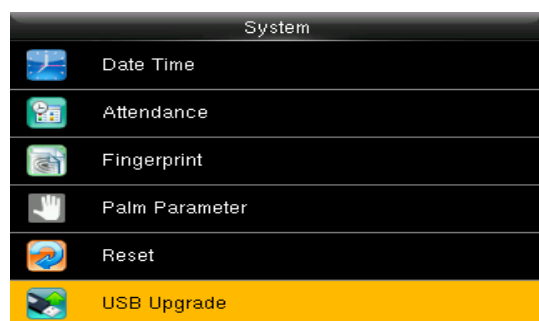
7.4 Reset

Reset communication settings, system settings, personalize settings etc.



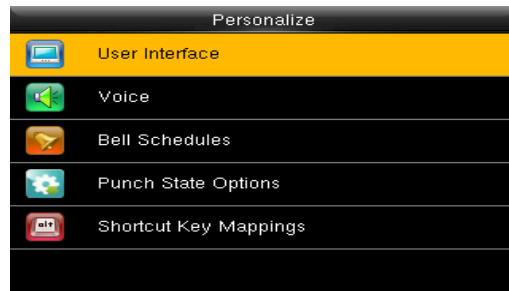
7.5 USB Upgrade

The firmware program of device can be updated with upgrade package in USB disk. You are not suggested to upgrade. If you need the upgrade file, please contact our technical support personnel.



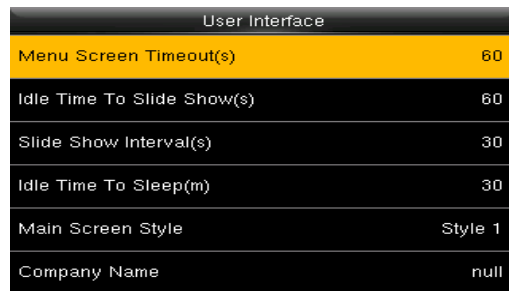
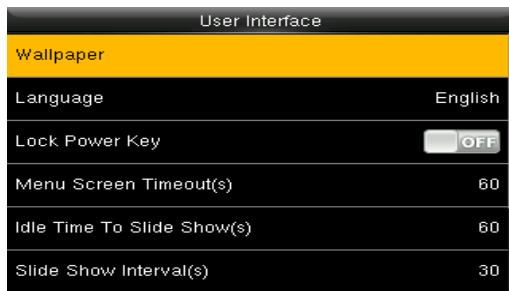
8 Personalize

To set some usual parameters. Enter into "Personalize".



8.1 User Interface

To set displayed parameters. Enter into "Personalize" → "User Interface".



Wallpaper: Select the wallpaper of the main screen as required.

Language: Select the language of device as required.

Menu Screen Timeout (s): When operating standby time is larger than this value, the system will return to initial interface. The valid value scope is 60~99999 seconds.

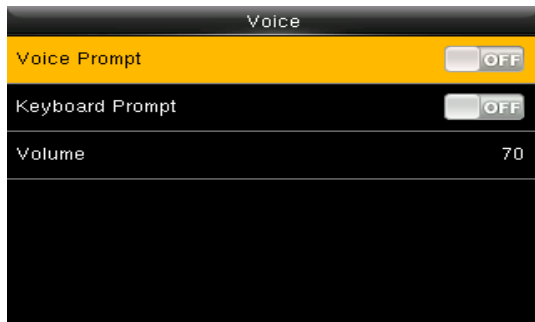
Idle Time To Slide Show (s): When standby time in main screen is larger than this value, the main screen will display a slide show. The valid value scope is 3~999 seconds.

Slide Show Interval (s): Set interval to change displayed pictures in the slide show, the value scope is 3~999 seconds.

Idle Time To Sleep (m): When operating standby time reaches to this value, the device will go to sleep. Pressing any keyboard or fingerprint will wake the device. The valid value scope is 1~999 minutes.

Main Screen Style: Select one displayed style as required (3 styles available).

8.2 Voice



Voice Prompt: This parameter is used to set whether to play voice prompts during the operation of the FFR terminal. Select "ON" to enable the voice prompt, and select "OFF" to mute.

Keyboard Prompt: This parameter is used to set whether to generate beep sound in response to every keyboard touch. Select "ON" to enable the beep sound, and select "OFF" to mute.

Volume: This parameter is used to adjust the

8.3 Bell Schedule

Many companies need a bell for on-duty and off-duty. Some uses manual bell and some uses electronic. To save cost and provide convenience to management, we integrate bell functions to fingerprint sensor. You can set the time for the bell. When it is the scheduled time, the device will automatically play the selected ringtone and trigger the relay signal. The ringtone playing does not stop until the ringing duration has elapsed.

8.3.1 New Bell Schedule

Enter into "Personalize" → "Bell Schedules" → "New Bell Schedule".



Bell Status: Enable/Disable this bell.

Bell Time: The bell rings automatically when it is the specified time.

Repeat: Specifies whether to repeat the ringtone.

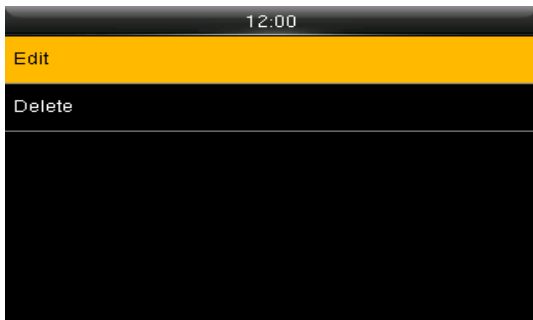
Bell Type: You can select between internal ringing and external ringing. For internal ringing, the ring tone is played by the loudspeaker of the terminal. For external ringing, the ring tone is played by an external electric bell that is wired with the terminal.

Ring Tone: Bell ring

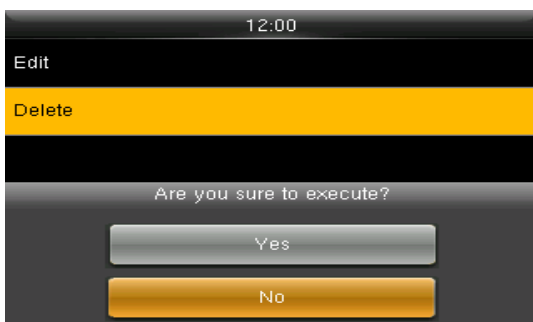
Internal bell delay (s): Specifies the duration for

8.3.2 All Bell Schedule

For editing the scheduled bells.



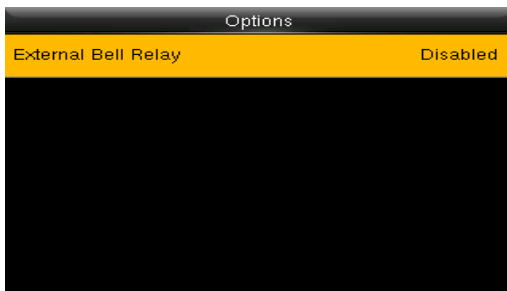
1. Select a bell to edit.
2. Press "Edit" to modify data.



1. Select a bell to delete it.
2. Press "Delete" to remove bell.

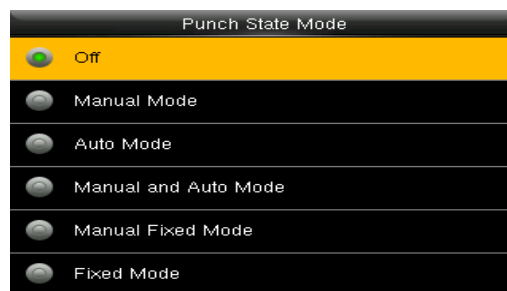
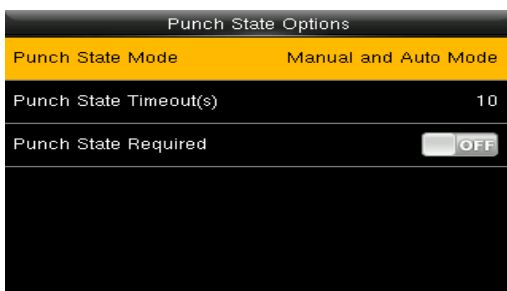
8.3.3 Options

When the function of external ringing is used, set the output terminal of external ringing.



8.4 Punch State Options

To set the mode of state keys. Enter into "Personalize" → "Punch State Options":



Punch State Mode: Off: Disable the punch state key function.

Manual Mode: User manually switches punch state by pressing corresponding shortcut key.

Auto Mode: The set punch states will auto switch when reaching switch time.

Manual and Auto Mode: A status key manually switching will switch to the automatic plan upon a timeout.

Manual Fixed Mode: After manually switching, it will keep this state until next manual switching.

Fixed Mode: Displaying the fixed punch state.

Punch State Timeout (s): The time of one punch state displays. The punch state will disappear or switch to other punch states as the time is out. The value is 5~999 seconds.

Punch State Required: Set whether to select punch state during verification.

Note: There are four punch states: Check-In, Check-Out, Overtime-In, and Overtime-Out.

8.5 Shortcut Key Mappings

You can define six shortcut keys as attendance status shortcut keys or functional shortcut keys. On the main interface of the FFR terminal, press corresponding keys and the attendance status will be displayed or the function interface will be rapidly displayed.

Shortcut Key Mappings	
Up Key	Check-In
Down Key	Check-Out
Left Key	Overtime-In
Right Key	Overtime-Out
ESC/[-> Key	Undefined
M/OK/->] Key	Undefined

Note: Only when Punch State is selected as function, will Punch State Value, Name, Set Switch Time options appear on the interface. The punch state can be set as auto switch. Punch state will switch automatically once the setting switch time is out.

Select Function of shortcut key as Punch State Option, the shortcut key will not take effect under that Punch State Mode is set as OFF.

Punch State Value: The device sets 4 different values corresponding to four punch states by default. Value 0 corresponds to punch state Check-In, 1 for Check-Out, 4 for Overtime-In, 5 for Overtime-Out. The value ranges from 0 to 250.

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

Punch State Value
Please input (0 ~ 250)
<input type="text" value="0"/>
Confirm (OK) Cancel (ESC)

Function: Select punch state options or menu function options.

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

Function
<input checked="" type="radio"/> Undefined
<input type="radio"/> Punch State Options
<input type="radio"/> New User
<input type="radio"/> All Users
<input type="radio"/> Ethernet
<input type="radio"/> PC Connection

Name: Enter the name of punch state.

Up Key	
Punch State Value	0
Function	Punch State Options
Name	Check-In
Set Switch Time	

Name
<input type="radio"/> User Defined
<input checked="" type="radio"/> Check-In
<input type="radio"/> Break-Out
<input type="radio"/> Break-In

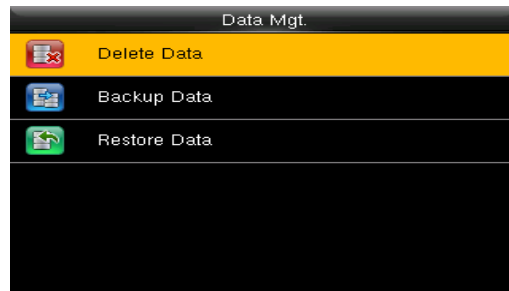
Set Switch Time: Set switch time for punch state.

Up Key	
Punch State Value	0
Function	Punch State Options
Name	Check-In
Set Switch Time	

Set Switch Time	
Switch Cycle	Never

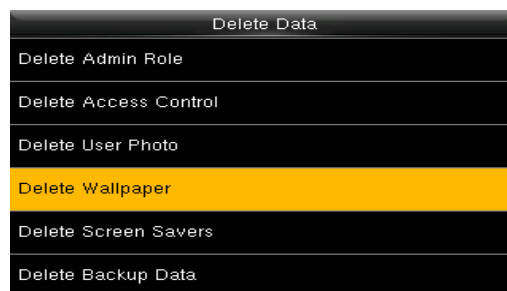
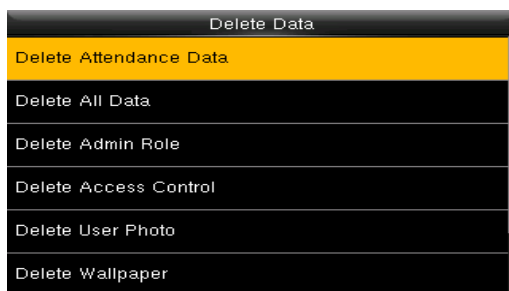
9 Data Mgt.

Manage data saved in the device. Enter into "Data Mgt."



9.1 Delete Data

Through the [**Data Mgt.**] menu, you can perform management of data stored on the FFR terminal, for example, deleting the attendance record, all data and promotional pictures, purging management rights and resetting the FFR terminal to factory defaults.



Delete Attendance Data: Delete all attendance data.

Delete All Data: Delete all enrolled users' information, fingerprints, attendance records, short messages and work codes etc.

Delete Admin Role: Change all administrators into normal users.

Delete Access Control: Delete the settings of access control.

Delete User Photo: Delete all enrolled users' photos.

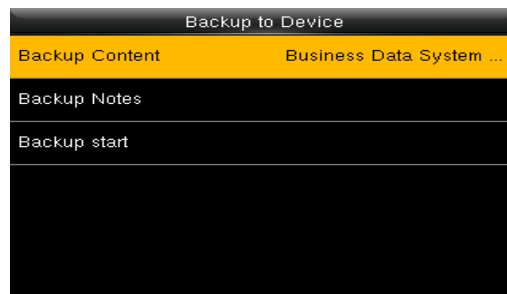
Delete Wallpaper: Delete all wallpapers in the device.

Delete Screen Savers: Delete all screen savers of the device.

Delete Backup Data: Delete data backup of the device.

9.2 Backup Data

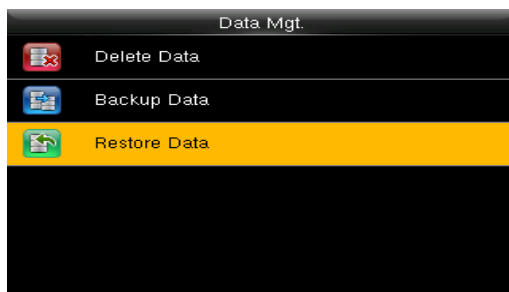
Back up the service data or configuration data of the device to the device or a USB drive.



Note: When Backup data to USB Disk, you need to insert a USB Disk into the device at first, and then press [M/OK] to backup data to USB disk.

9.3 Restore Data

Restore the data stored on the device or on the USB drive inserted into the device.

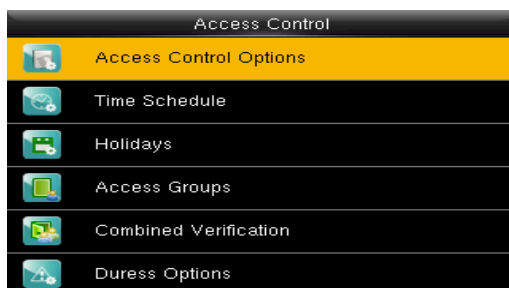


1. Select a route.
2. Select the data type.
3. Start the restore.

Note: When restoring data from a USB Disk, you need to insert a USB Disk into the device at first, which has the restored data.

10 Access Control

Access control option is to set user's open door Lock delay.

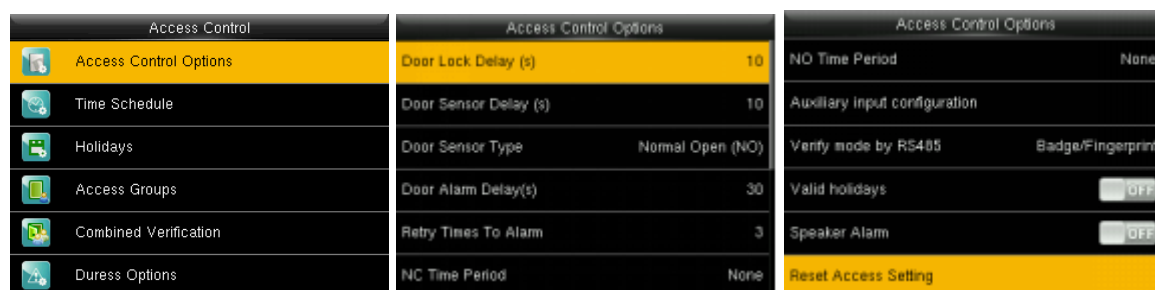


To unlock, the enrolled users must have owned these conditions:

1. The current unlock time should be within the effective time of user time zone or group zone.

- The group a user belongs to must be in access controlling. The new enrolled user is allocated in the group 1 and in time zone 1 by default, in time zone as 1. The new enrolled user is in unlock status. You can modify the status in user editing.

10.1 Setting Door Properties



In the initial interface, press **[M/OK] > Access Control > Access Control Options** to enter the **Access Control Options** setting interface.

Door Lock Delay (s): The period of time of unlocking (from door opening to closing automatically) after the electronic lock receives an open signal sent from the device (value ranges from 0 to 10 seconds).

Door Sensor Delay (s): When the door is opened, the door sensor will be checked after a time period; if the state of the door sensor is inconsistent with that of the door sensor mode, alarm will be triggered. The time period is the **Door Sensor Delay** (value ranges from 1 to 255 seconds).

Door Sensor Type: It includes **None**, **Normal Open (NO)** and **Normal Close (NC)**. **None** means door sensor is not in use; **Normal Open** means the door is opened when electricity is on; **Normal Close** means the door is closed when electricity is on.

Door Alarm Delay (s): When the state of the door sensor is inconsistent with that of the door sensor type, alarm will be triggered after a time period; this time period is the **Door Alarm Delay** (the value ranges from 1 to 999 seconds).

Retry Times To Alarm: When the number of failed verification reaches the set value (value ranges from 1 to 9 times), the alarm will be triggered. If the set value is none, the alarm will not be triggered after failed verification.

NC Time Period: To set time period for Normally Closed mode, so that no one can gain access during this period.

NO Time Period: To set time period for Normally Open, so that the door is always unlocked during this period.

Auxiliary Input Configuration: To set the **Aux output/lock open time** and **Aux Output type** for the device with auxiliary connector. **Aux Output type** includes **None**, **trigger door open**, **trigger Alarm**, and **trigger Door open and Alarm**.

Verify Mode by RS485: It is the verification mode used by the device when it is the master unit. This option will be displayed only if RS485 reader function is enabled.

You can enable it by following these steps: In the initial interface, press **[M/OK] > COMM. > Serial Comm > Serial Port > Master Unit.**

Valid holidays: To set if **NC Time Period** or **NO Time Period** settings are valid in set holiday time period. Choose **[ON]** to enable the set **NC** or **NO** time period in holiday.

Speaker Alarm: When the **[Speaker Alarm]** is enabled, the speaker will raise an alarm when the device is being dismantled.

Reset Access Setting: To reset parameters of door lock delay, door sensor delay, door sensor type, door alarm delay, retry times to alarm, NC time period, NO time period, valid holidays, speaker alarm, device status, duress function, alarm on 1:1 match, alarm on 1: N match, alarm on password and alarm delay. However, the content of the Access Data Deletion in **[Data Mgt.]** will not be affected.

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

10.2 Defining Time Schedules

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



Sunday	00:00	23:59
Monday	00:00	23:59
Tuesday	00:00	23:59
Wednesday	00:00	23:59
Thursday	00:00	23:59
Search Time Zone(1-50)		

The default Time Schedule No. is 1 (whole-day valid), which can be edited.

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

Invalid Time Schedule: When the end time is smaller than the start time.

The following examples as explanation:

Valid

Invalid

Note: The **Time Schedule** cannot be set across two days, which means that the end time must be greater than the start time.

10.3 Setting Holidays

The holiday access control time can be set, which is applicable for all users during holiday. Enter into "Access Control"→"Holidays", press "Add Holiday" and enter into the interface.

Holidays	
No.	1
Start Date	Undefined
End Date	Undefined
Time Period	1

Settings include number, start time, end time and time period.

Holidays	
No.	1
Start Date	10-01
End Date	10-07
Time Period	2

Note: Start/End Date only requires to set the month (MM) and date (DD), which is applicable to all years.

Time period: The valid time Schedule used in the holiday.

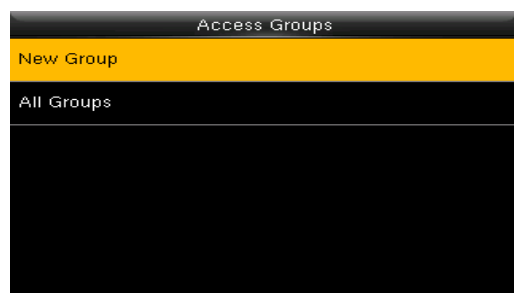
As shown in above figure: Holiday 1 starts on the October 1 every year, ends on the October 3 every year.

10.4 Creating Access Groups

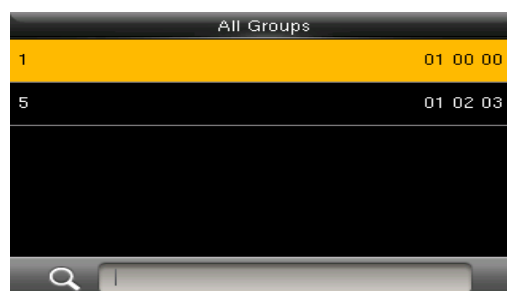
Grouping is to manage users in groups.

Group users' default time zone is set to be the group time zone, while users can set their personal time zone. Each group can set 3 time zones at most, as long as one of them is valid, the group can be verified successfully.

By default, the new enrolled user belongs to Access Group 1, and can also be allocated to other access group. Enter into "Access Control" → "Access Groups" → "New Group".



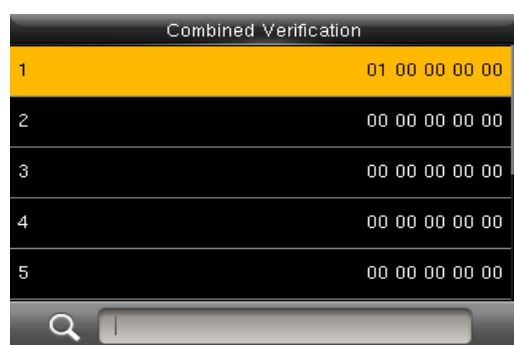
As shown in the following figures, the **Verification Mode** of **Access Group 5** is fingerprint only; Time Zone 1, 2 and 3 are set, while the Holiday function is enabled.



10.5 Multi-user Authentication

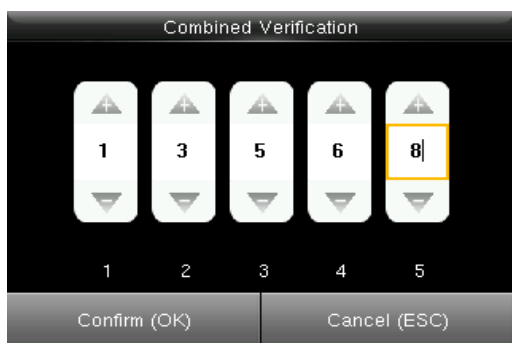
Combine two or more members to achieve multi-verification and improve security.

In a Combined Verification, the range of user number is: $0 \leq N \leq 5$; the users can all belong to a single group, or belong to 5 different groups at most.



Note: Only group No. set in Access Group interface, can it be selected in the Combined Verification setting.

For Example, (The following access groups have been set in **Access Group** interface):

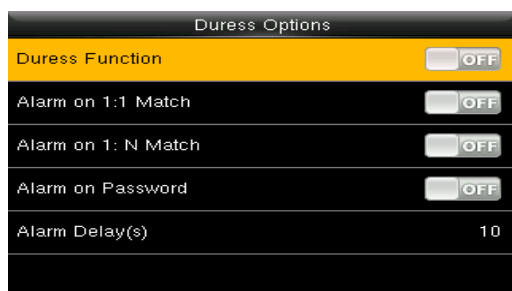


As the figure says, Combined Verification 1 is made up of five members coming from five different groups---access group 1 / 3 / 5 / 6 / 8 respectively.

Note: To delete a Combined Verification, set all access group numbers to 0.

10.6 Duress Settings

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



Duress Function: In [ON] state, press "Duress Key" and then press any registered fingerprint (within 10 seconds), duress alarm will be triggered after successful verification. In [OFF] state, pressing "Duress Key" will not trigger the alarm.

Alarm on 1:1 Match: In [ON] state, when a user uses 1:1 Verification Method to verify any registered fingerprint, alarm will be triggered. In [OFF] state, no alarm signal will be triggered.

Alarm on 1: N Match: In [ON] state, when a user uses 1:N Verification Method to verify any registered fingerprint, alarm will be triggered. In [OFF] state, no alarm signal will be triggered.

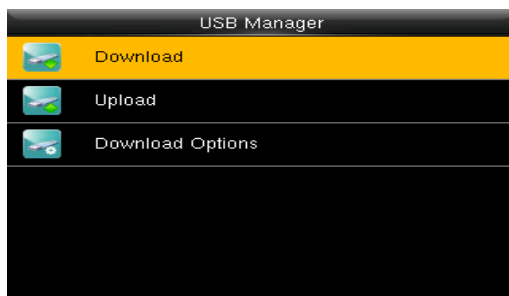
Alarm on Password: In [ON] state, when a user uses password verification method, alarm will be triggered. In [OFF] state, no alarm signal will be triggered.

Alarm Delay (s): When duress alarm is triggered, the device will send out alarm signal after 10 seconds (default); the alarm delay time can be changed (value ranges from 0 to 999 seconds).

11 USB Manager

Import user information, fingerprint template, attendance data and so on in the device to attendance software or import user information and fingerprint to other devices through U disk.

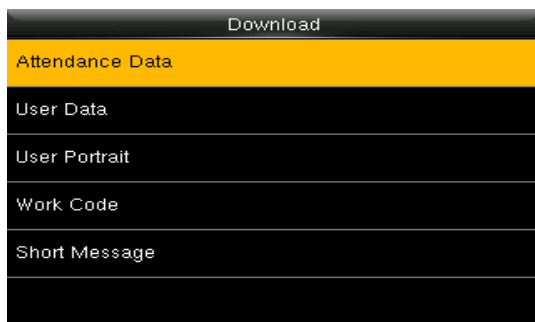
Enter into "USB Manager" → "Download"/"Upload".



Note: Before you upload/download data from/to a USB drive, insert the USB drive into the USB interface of the device.

11.1 Download

Download data to USB drive from the device.



Attendance Data: Download attendance data to USB disk.

User Data: Download all user data to USB disk.

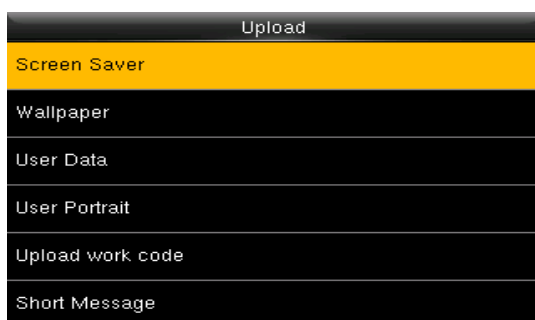
User Portrait: Download attendance photos to USB disk.

Work Code: Download all work codes to USB disk.

Short Message: Download all short messages to USB

11.2 Upload

Upload data to the device through the USB drive.



Screen Saver: Upload screen saver saved in USB disk.

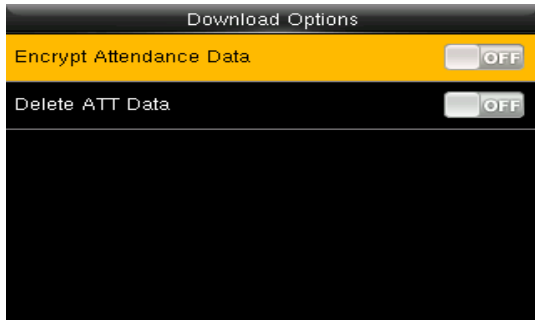
Wallpaper: Upload wallpapers saved in USB disk

User Data: Upload user data saved in USB disk to the device.

User Portrait: Upload user photos saved in USB disk to the device.

Upload work code: Upload all work code saved in USB disk.

11.3 Download Options



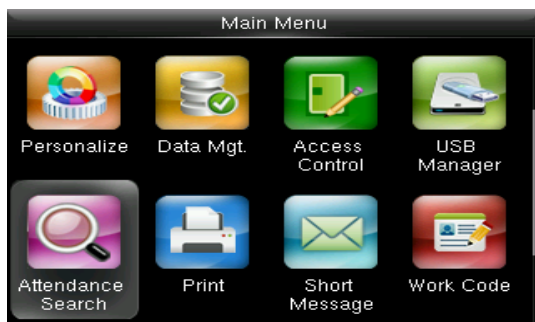
You can encrypt the data in a USB drive and set to delete data after being downloaded.

During downloading the attendance records, you can also set the calendar type displayed in the attendance time.

The device supports three calendar types which are Gregorian, Iran Gregorian, and Iran .

12 Attendance Search

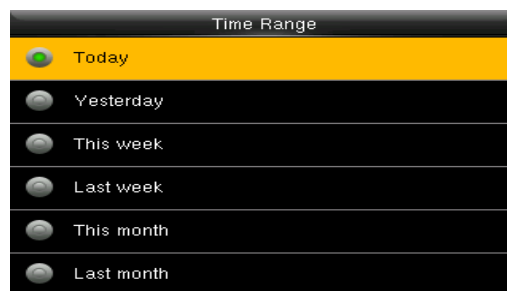
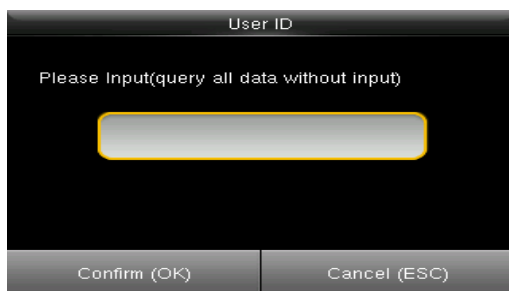
Employee's attendance record will be saved in the device. For query convenience, the attendance search function is provided.



Attendance Record: Search the attendance records in the device. When you have verified in the device, the record is saved.

Attendance photo: Search the attendance record restored in the device. When you have verified, the device's camera will capture a photo to save in the device.

Go to Attendance Record.



1. Input the user ID to search.
2. Select the time period of attendance record.

Note: You can input nothing in user ID box to search all users' attendance record.

Personal Record Search		
Date	User ID	Attendance
03-03		Number of Records:09
	5	20:44 20:37 19:51 19:47 17:46 17:27 17:01 13:53 13:39
Prev : Left key Next : Right key Details : OK		

Personal Record Search				
User ID	Name	Attendance	Mode	State
5		03-03 20:44	1	255
5		03-03 20:37	1	255
5		03-03 19:51	1	255
5		03-03 19:47	1	255
5		03-03 17:46	1	255
5		03-03 17:27	1	255
5		03-03 17:01	1	255
5		03-03 13:53	1	255
5		03-03 13:39	1	255
Verify By : Fingerprint Punch State : 255				

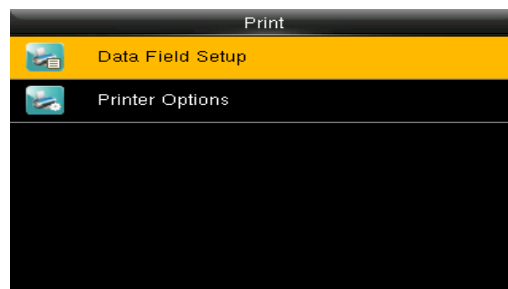
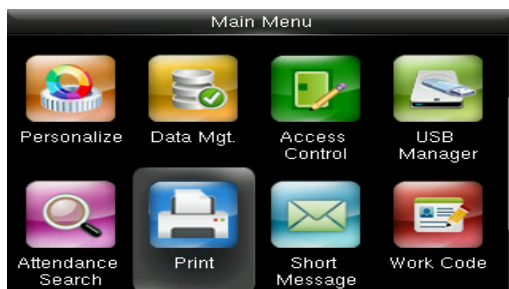
3. The record list is displayed.
4. Select any to check details.

13 Print

Devices with printing function can print attendance records out when a printer is connected.

13.1 Data Field Setup

In the initial interface, press **[M/OK]** > **Print** > **Data Field Setup** > press **[M/OK]** to turn on / off the fields needing to be printed.

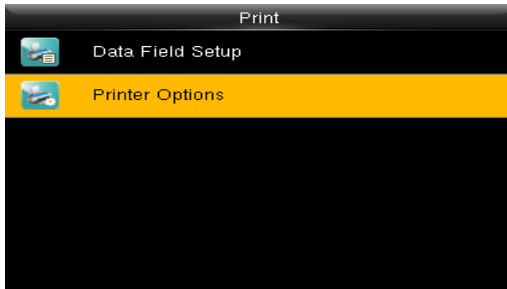


Data Fields	
Company Name	<input type="checkbox"/> OFF
User ID	<input type="checkbox"/> OFF
Name	<input type="checkbox"/> OFF
Punch Time	<input type="checkbox"/> OFF
Punch State	<input type="checkbox"/> OFF
Device ID	<input type="checkbox"/> OFF

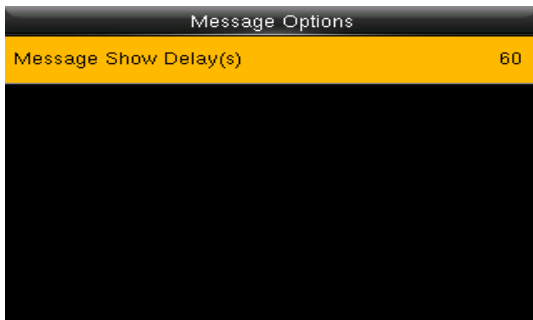
Data Fields	
Punch Time	<input type="checkbox"/> OFF
Punch State	<input type="checkbox"/> OFF
Device ID	<input type="checkbox"/> OFF
Print Time	<input type="checkbox"/> OFF
Work Code	<input type="checkbox"/> OFF
Verification Mode	<input type="checkbox"/> OFF

13.2 Printer Options

Enter into "Print"→"Printer Options". Press [M/OK] to turn on / off the **Paper Cut** function.



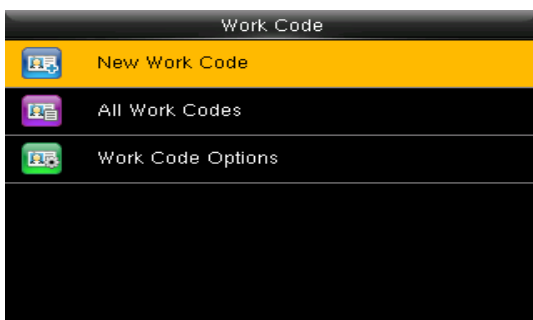
Note: To turn on the **Paper Cut** function, it is required to connect the device with a printer with paper cutting function, so that the printer will cut papers according to the selected printing information when printing.



Message Show Delay (s): It means the duration that personal message shows. The personal message showing interface will back to initial interface after reaching Message Show Delay.

The valid value is 1-99999 seconds.

14 Work Code



Salary is based on attendance. There are many work types for employees. An employee may have different work type in different time period. Different work types have different pays. Therefore, in order to distinguish different attendance states when user is dealing with attendance data, the device has provided a parameter to mark which attendance record belongs to which work type. Work codes are downloaded together with attendance records. Users can use relevant data based on the specific

New Work Code

ID 1

Name

14.1 New Work Code

ID: The allocated working number. The range is 1-99999999.

Name: Input a name with T9 input. 23-characters are limited.

Note: The work code cannot be modified once confirmed.

14.2 All Work Code

You can view, edit or delete the work code from the work codes list. The ID cannot be modified, and the other operations are similar to those performed to add a work code when edit.

1

Edit

Delete

1. Select a work code.
2. Press "Edit" to modify the name. Press "Delete" to delete.

14.3 Work Code options

Work Code Options

Work Code Required OFF

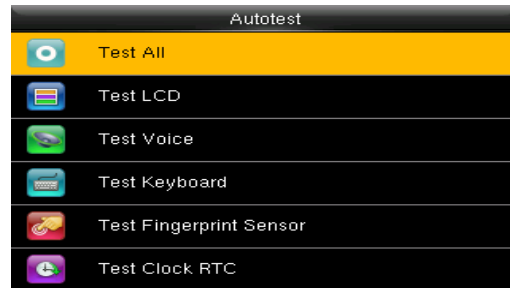
Work Code Must Defined OFF

Work Code Required: The work code must be input during verification. Select whether to enable this function.

Work Code Must Defined: The input work code has to exist during verification. Select whether to enable this function.

15 Autotest

The auto test enables the system to automatically test whether the functions of various modules are normal, including the LCD, voice, sensor, keyboard and clock tests.



Test All: The terminal automatically tests the LCD, voice, sensor, keyboard and click, press [OK] to continue and press [ESC] to exit.

Test LCD: Checks the LCD (Liquid Crystal Display).

Test Voice: Checks if the voice prompts are displayed normally.

Test Keyboard: Checks if the keyboard is available.

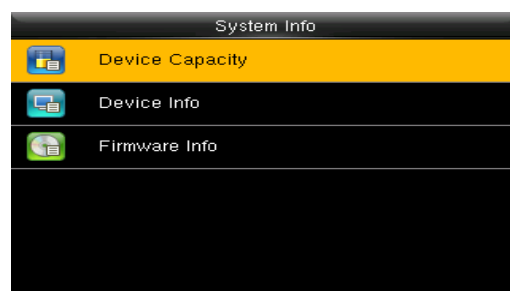
Test Fingerprint Sensor: Checks if the fingerprint sensor is available to use.

Test Clock RTC: Checks if the RTC (Real-Time Clock) is accurate.

While checking modules, please follow the prompts in the specific interface.

16 System Info

You can check the storage status as well as firmware information of the terminal through the [System Info] option.



Click specific option to check the parameters:

Device Capacity: Number of users, admin users, password and the most capacity of fingerprints, palm, badge★, attendance record and user photos number.

Device Info. (Information): Device name, serial number, MAC address, fingerprint algorithm, palm algorithm, platform information, manufacturer, manufacturer date.

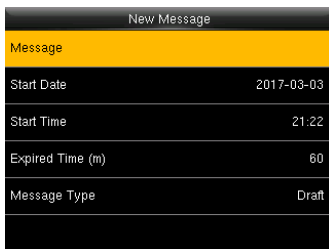
Firmware info: Firmware version, bio service, standalone service, device service.

All information here is not allowed to modify.

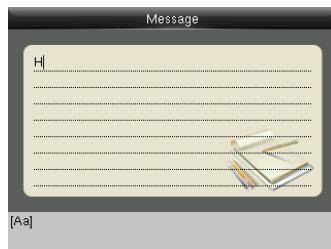
17 Appendix

17.1 T9 Input

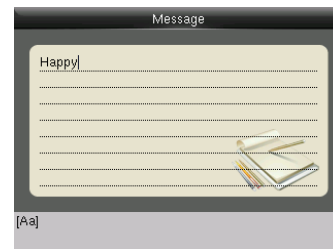
T9 input (intelligent input) is quick and high efficient. There are 3 or 4 letters on the numeric keys (2~9), for example, A, B, C are on numeric key 2. Press the corresponding key once, and the program will generate effective spelling. Refer below example to understand the methods:



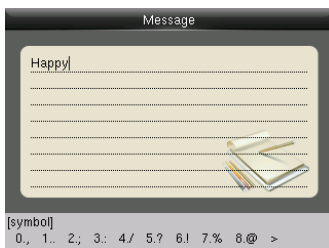
Enter into "New Message".



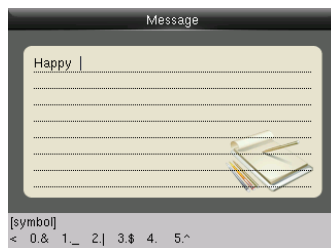
Press [4] twice to input H.



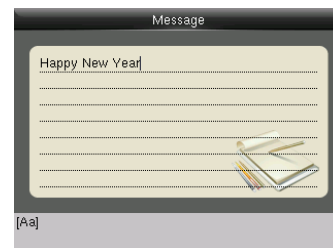
Input "appy" with the same way.



Press ► to "symbol" type

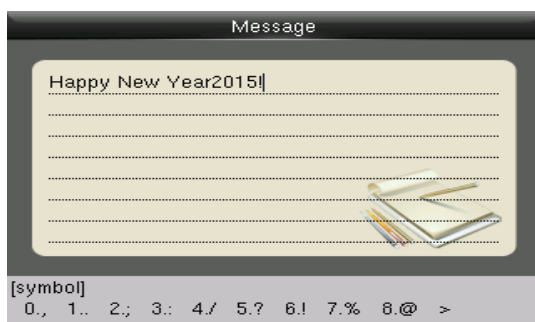


Press ► to find to "4" .



Input "New Year" with that way

Press 4 to input a blank Press ► to numeric type.



1. Input "2015", press ► to "symbol" type.
2. Press "6" to input "!"

17.2 Rules to upload picture

- **User Photo:** First, create a directory named "photo" in the root directory of USB disk, and then put user photos in the directory. Max capacity of the directory is 2000 photos. The size of each photo is smaller or equal 15K. Name of the photo is X.jpg (X represents User ID, which does not limit digits). The format of the photo must be .JPG.

- **Screen Saver:** First, create a directory named "advertise" in the root directory of USB disk, and then put screen savers in the directory. Max capacity of the directory is 20 pictures. The size of each screen saver is smaller or equal 30K. There is no limit on the name and format of the screen saver.
- **Wallpaper:** First, create a directory named "wallpaper" in the root directory of USB disk, and then put wallpapers in the directory. Max capacity of the directory is 20 pictures. The size of each wallpaper is smaller or equal 30K. There is no limit on the name and format of the wallpaper. It supports format of jpg, png, bmp etc.

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.

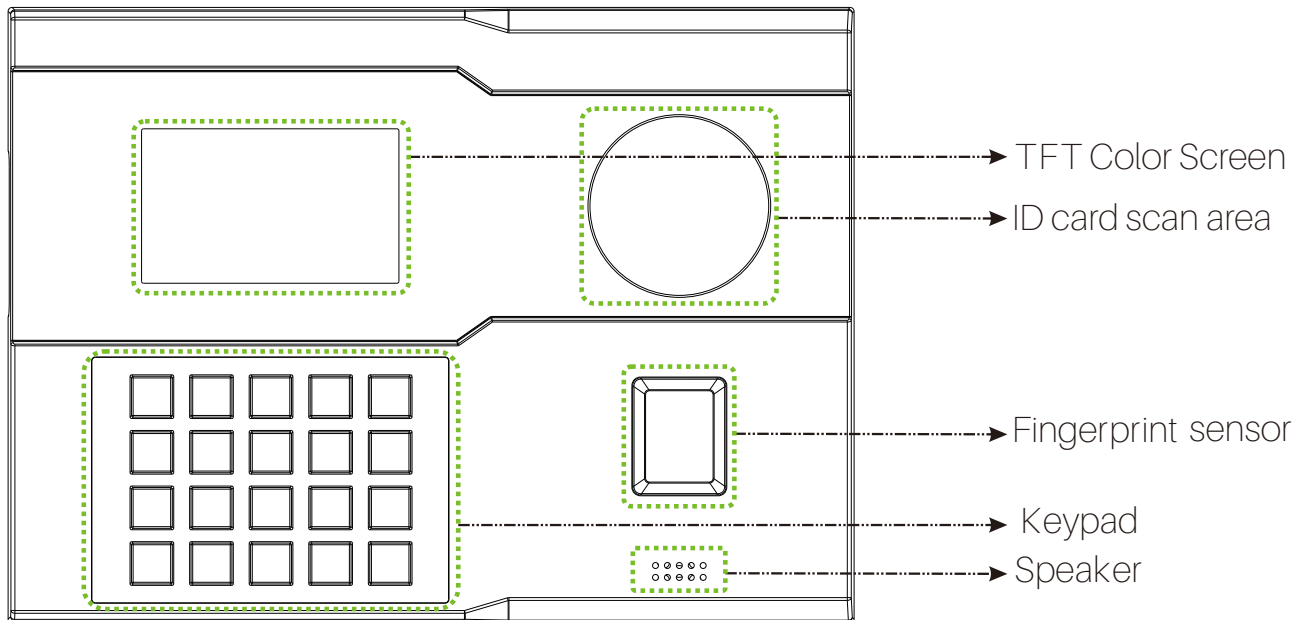
Note: 80% of this product's components are manufactured using non-toxic and eco-friendly materials. The components which contain toxins or harmful elements are included due to the current economic or technical limitations which prevent their replacement with non-toxic materials or elements.



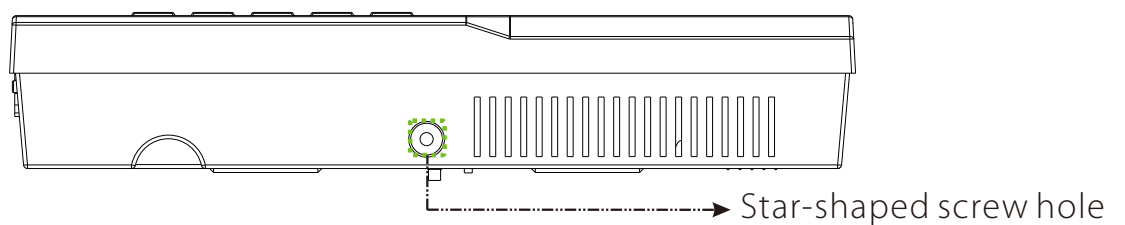
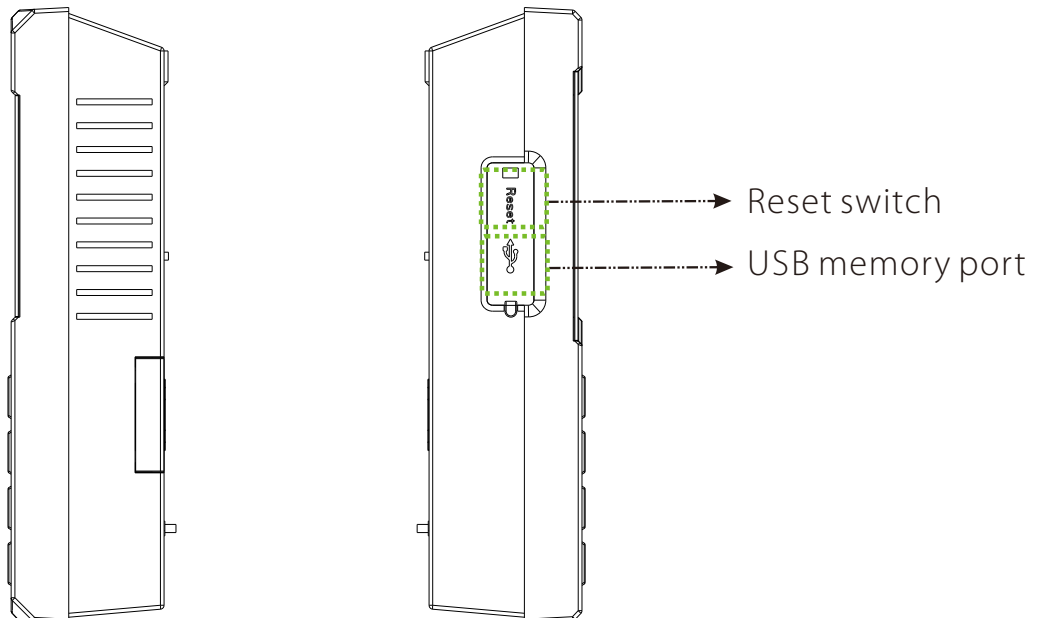
Installation Guide

Device Overview

Front

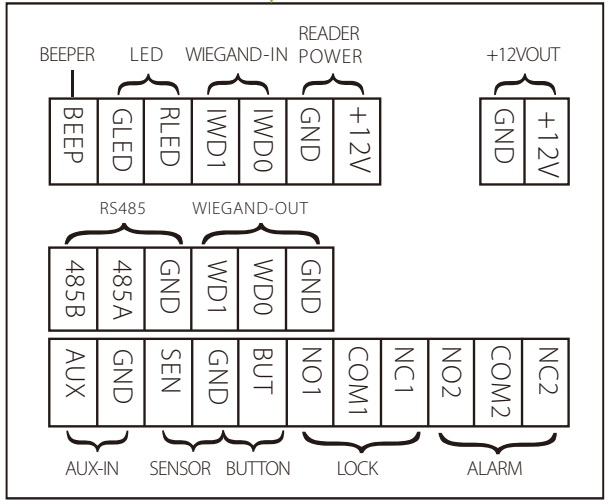
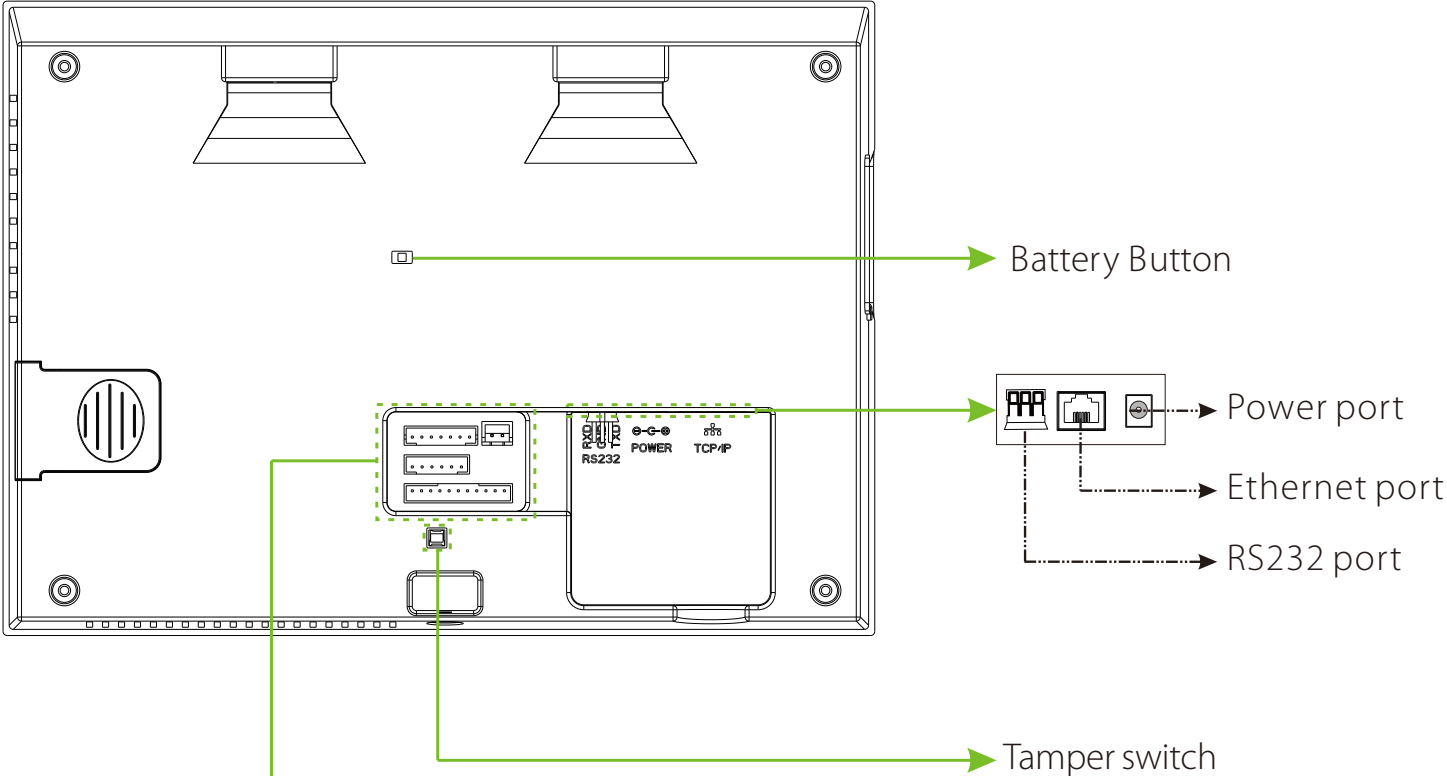


Side



Product PIN Diagram

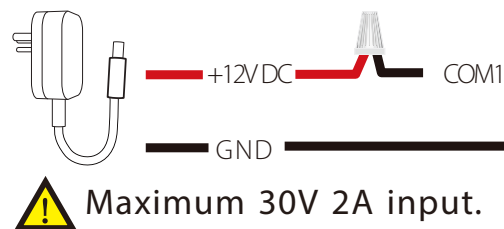
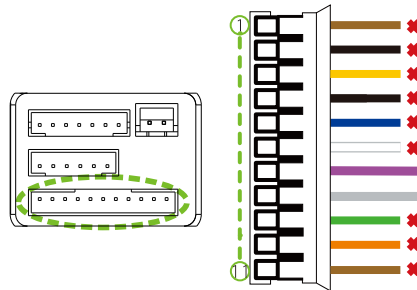
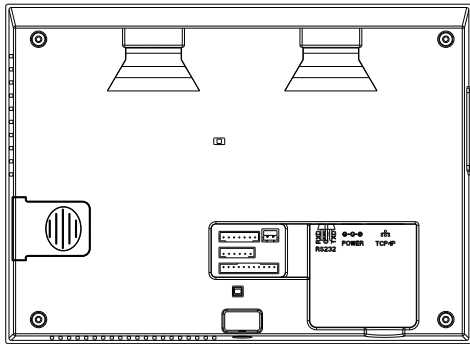
Back



Lock Relay Connection

The system supports Normally Opened Lock and Normally Closed Lock. For example the NO LOCK (normally)opened

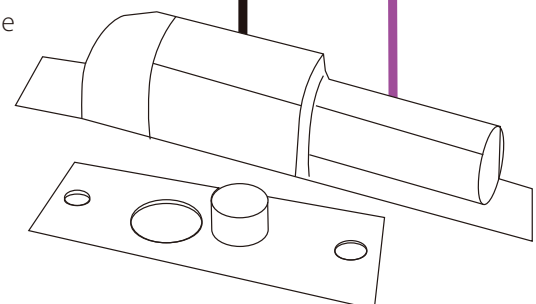
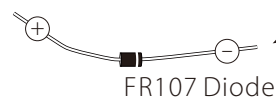
Device not sharing power with the lock



PIN	DESCRIPTION	WIRE
1	Aux	✗ Brown
2	GND	✗ Black
3	SEN	✗ Yellow
4	GND	✗ Black
5	BUT	✗ Blue
6	NO1	✗ White
7	COM1	Purple
8	NC1	Gray
9	NO2	✗ Green
10	COM2	✗ Orange
11	NC2	✗ Brown

✗ Do not use

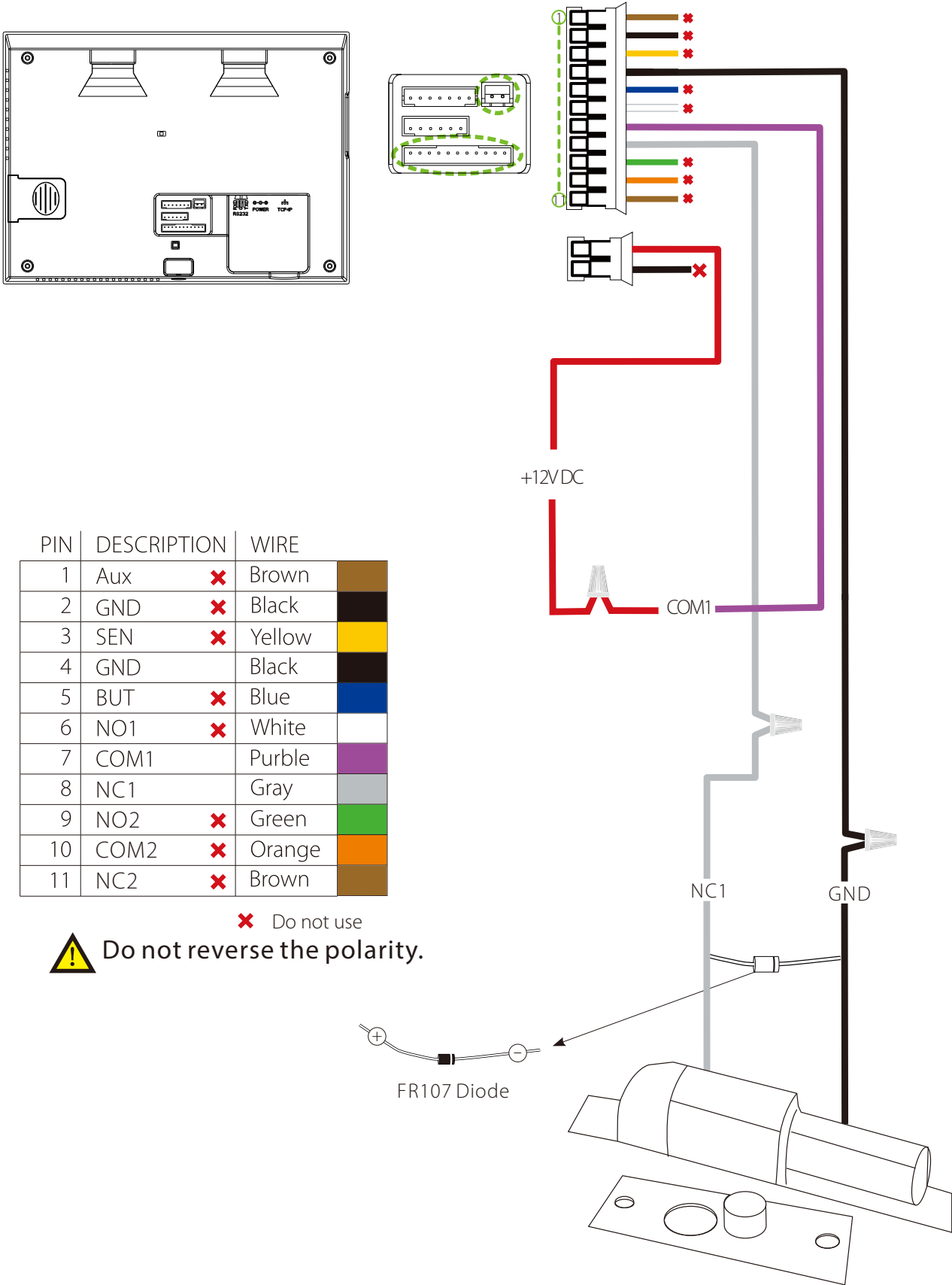
⚠ Do not reverse the polarity.



Normally Closed Lock

Lock Relay Connection

Device sharing power with the lock



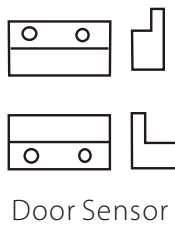
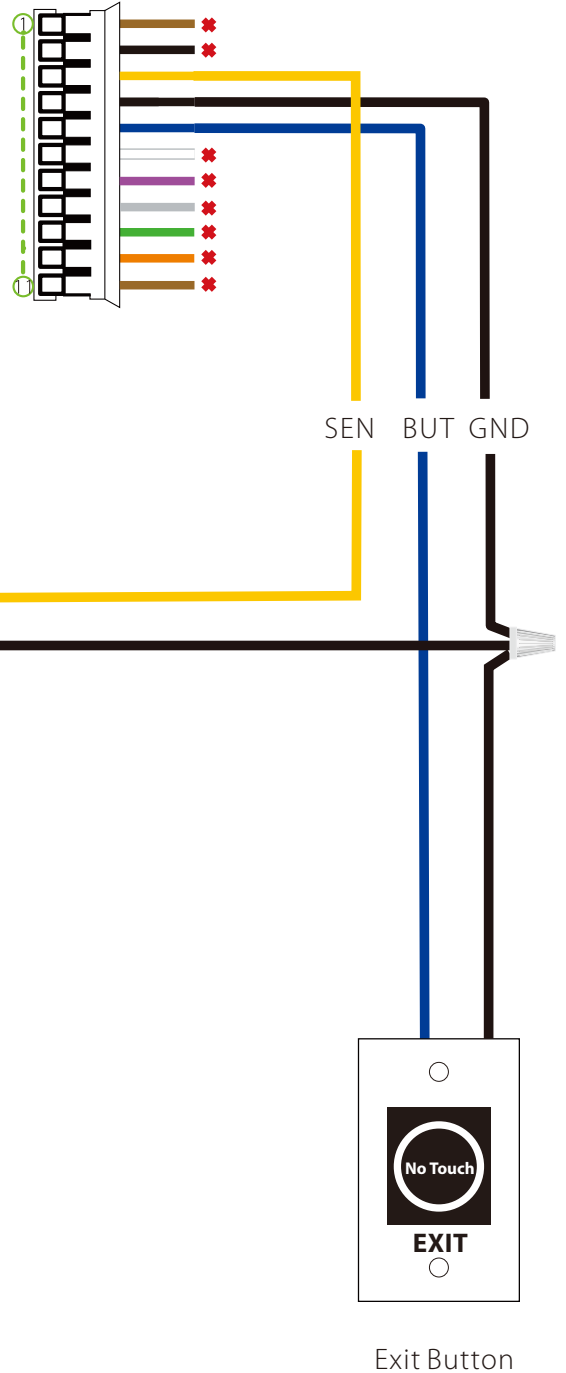
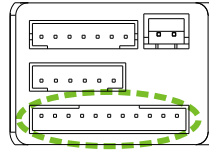
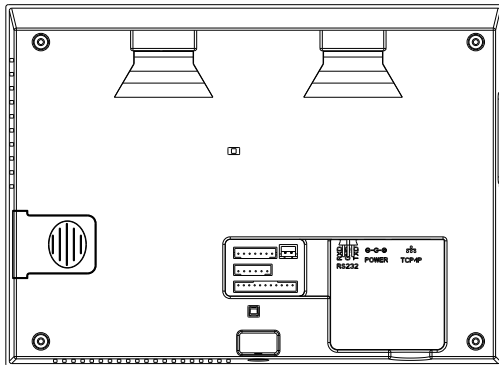
PIN	DESCRIPTION	WIRE
1	Aux	Brown
2	GND	Black
3	SEN	Yellow
4	GND	Black
5	BUT	Blue
6	NO1	White
7	COM1	Purple
8	NC1	Gray
9	NO2	Green
10	COM2	Orange
11	NC2	Brown

⚠ Do not reverse the polarity.

Normally Closed Lock

⚠ Maximum 12V 2A input.

Button & Sensor Connection



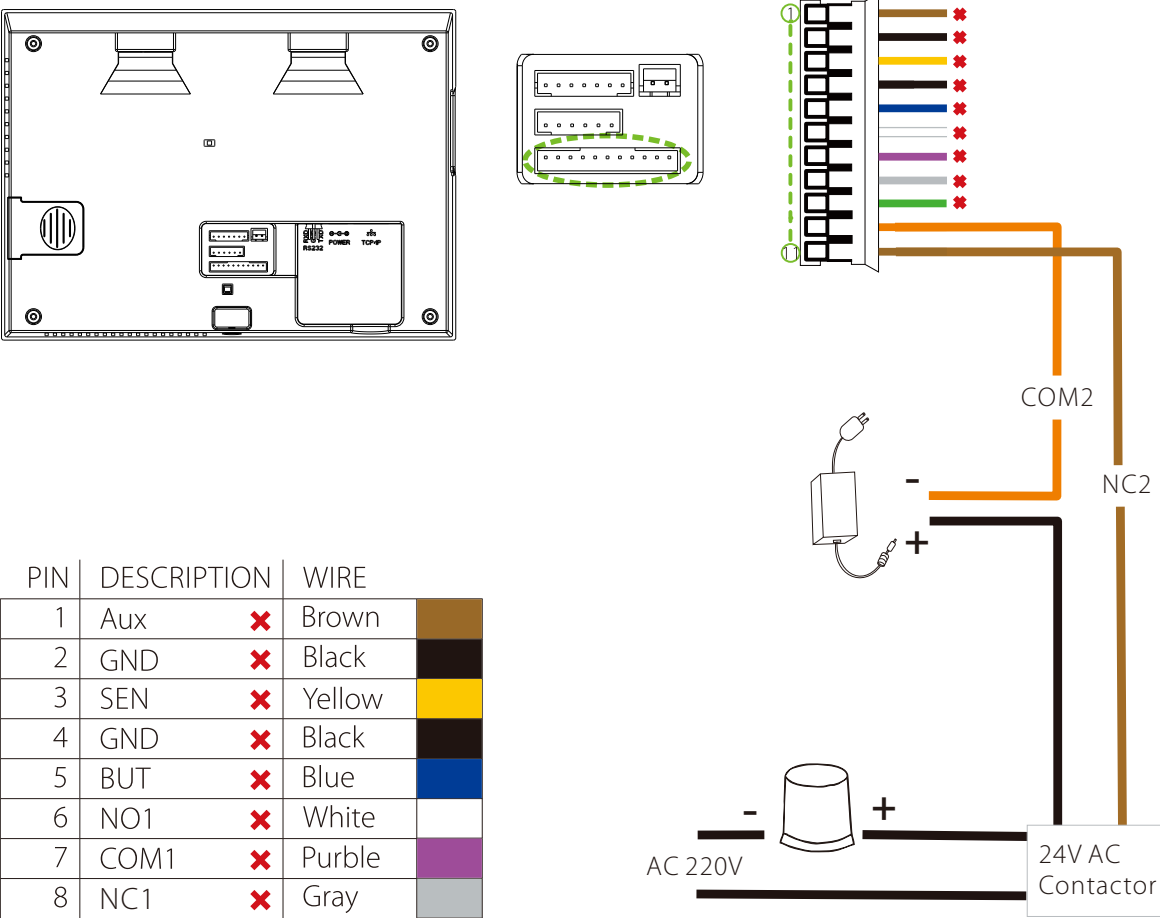
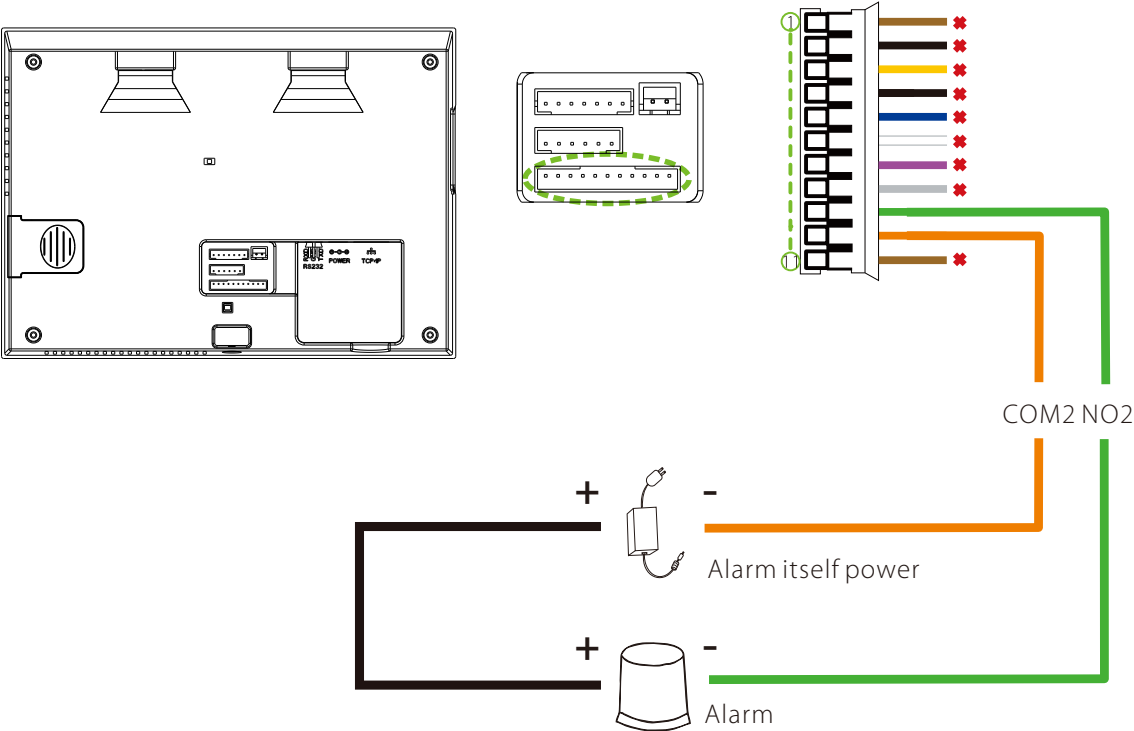
PIN	DESCRIPTION	WIRE
1	Aux	Brown
2	GND	Black
3	SEN	Yellow
4	GND	Black
5	BUT	Blue
6	NO1	White
7	COM1	Purple
8	NC1	Gray
9	NO2	Green
10	COM2	Orange
11	NC2	Brown

✗ Do not use



Do not reverse the polarity.

Alarm Connection

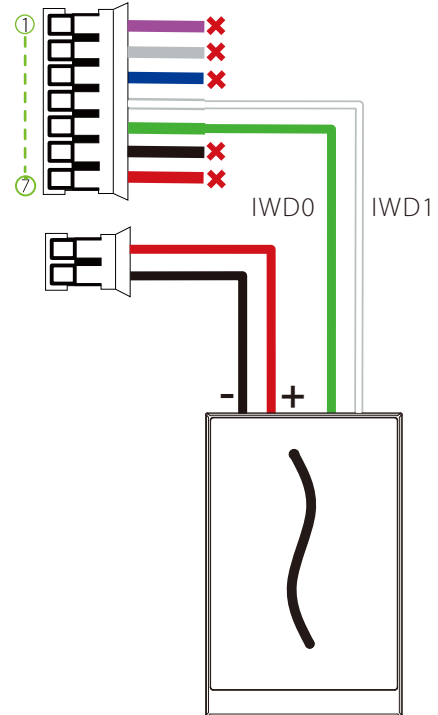
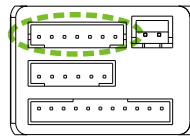
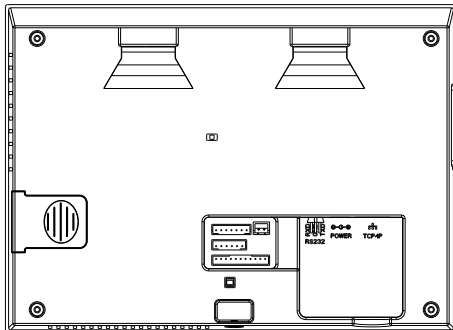


PIN	DESCRIPTION	WIRE
1	Aux	Brown
2	GND	Black
3	SEN	Yellow
4	GND	Black
5	BUT	Blue
6	NO1	White
7	COM1	Purple
8	NC1	Gray
9	NO2	Green
10	COM2	Orange
11	NC2	Brown

✗ Do not use

Wiegand Input & Output Connection

Wiegand In connection

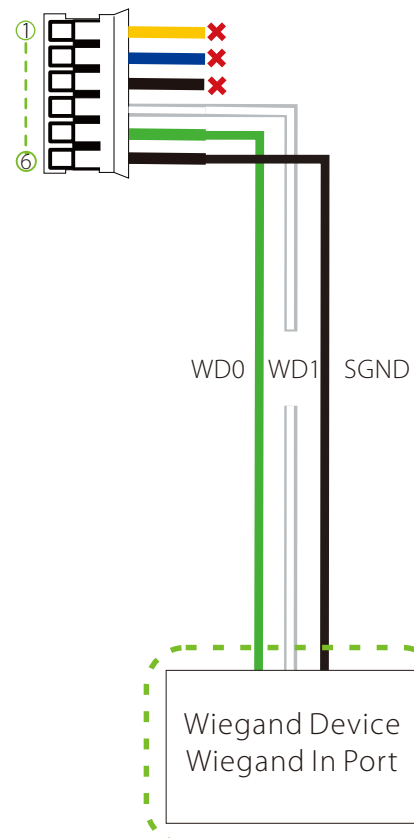
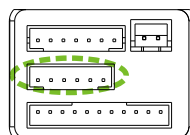
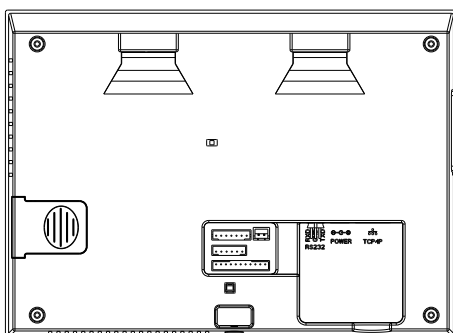


PIN	DESCRIPTION	WIRE
1	BEEP	Purple
2	GLED	Gray
3	RLED	Blue
4	IWD1	White
5	IWD0	Green
6	GND	Black
7	+12V	Red

✗ Do not use

Wiegand reader

Wiegand Out connection

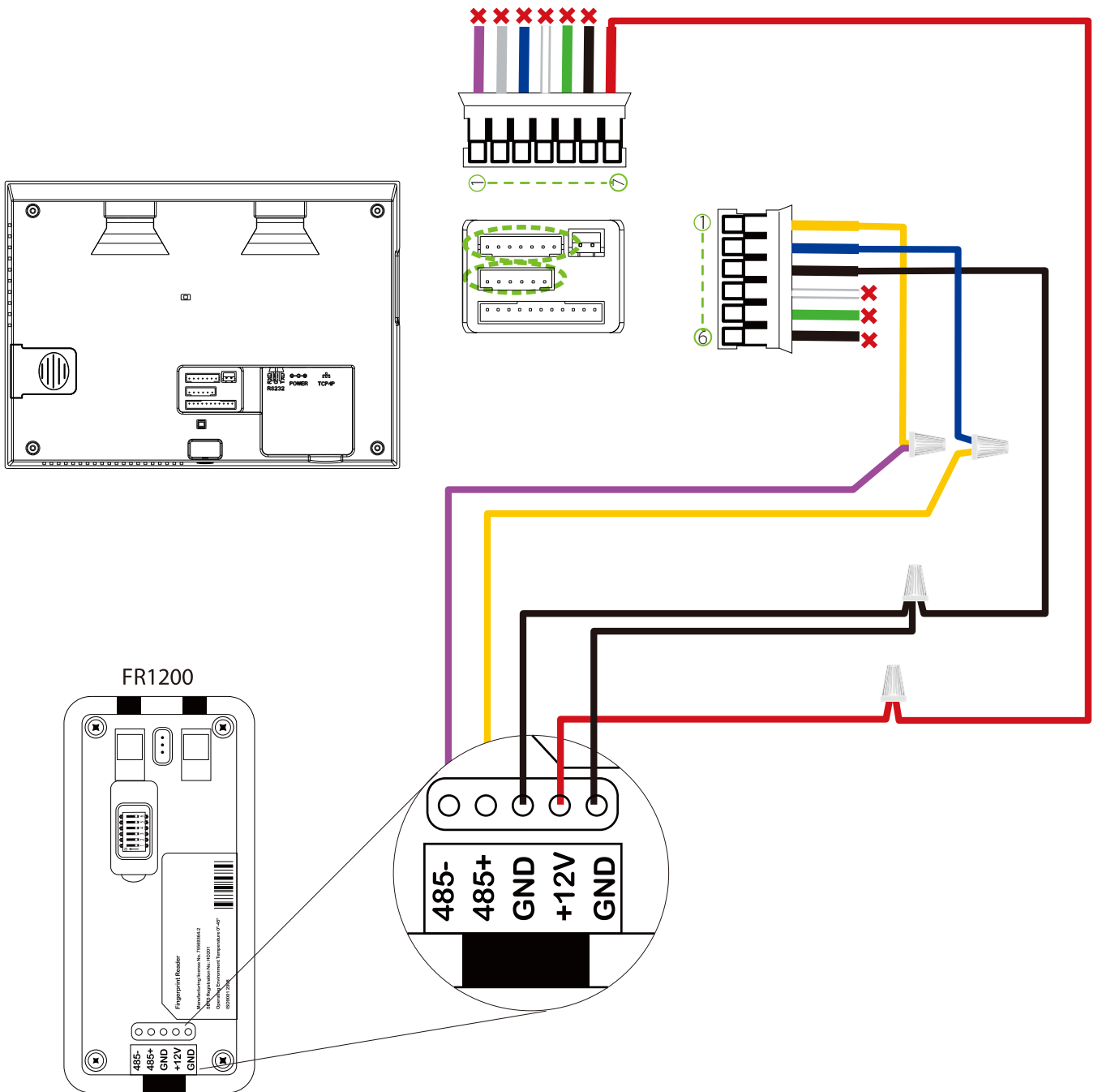








PIN	DESCRIPTION	WIRE
1	485B	Yellow
2	485A	Blue
3	GND	Black
4	WD1	White
5	WD0	Green
6	GND	Black

✗ Do not use

Wiegand Device
Wiegand In Port

RS485 Connection



PIN	DESCRIPTION	WIRE	
1	485B	Yellow	
2	485A	Blue	
3	GND	Black	
4	WD1	White	
5	WD0	Green	
6	GND	Black	

✗ Do not use

PIN	DESCRIPTION	WIRE
1	BEEP ❌	Purple
2	GLEED ❌	Gray
3	RLED ❌	Blue
4	IWD1 ❌	White
5	IWD0 ❌	Green
6	GND ❌	Black
7	+12V	Red

✗ Do not use

Device Operation

Quick flows

1) Enroll New Users(Main Menu > User Management > New User)



New User	
User ID	4
Name	
User Role	Normal User
Palm	0
Fingerprint	0
Badge Number	

User ID: Enroll user ID; it supports 1-9 digits of numbers.

Use Role: Select the user role between Normal User and Super Admin.

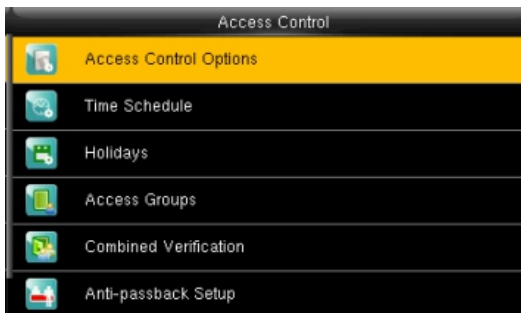
Verification Mode: Select required mode from list.

Fingerprint:★ Enroll a fingerprint or fingerprints. **Palm:** Enroll palm according to the prompts of screen and voice.

Badge Number ★ Enroll a badge by swiping the badge.

Password: Enroll the password; it supports 1-9 digits of numbers.

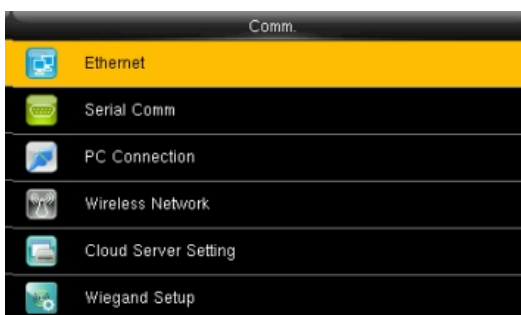
2)Access Control Setting (Main Menu > Access Control)



Access Control	
Access Control Options	
Time Schedule	
Holidays	
Access Groups	
Combined Verification	
Anti-passback Setup	

Access Control Options: Including Door Lock Delay, Door Sensor Delay, Door Sensor Type, NC / NO Time Period etc.

3)Comm Setting (Main Menu > Comm.)



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

Ethernet: The device can communicate with PC via the Ethernet parameters.

Serial Comm: The device can communicate with PC via the serial port according to the user-defined parameters.

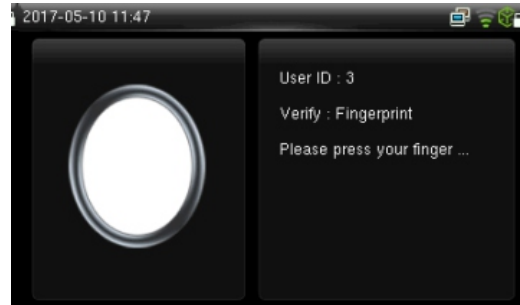
PC Connection: Set the password and device ID so that you can connect the device with software in PC.

Cloud Server Setting★ Settings used for connecting with ADMS server.

Device Operation

4) Verification(1:1 verification mode for example)

a. Fingerprint Verification Mode



b. Password Verification Mode



5) Attendance Record

a. View records in the device(Main Menu > Attendance Search > Attendance Record)



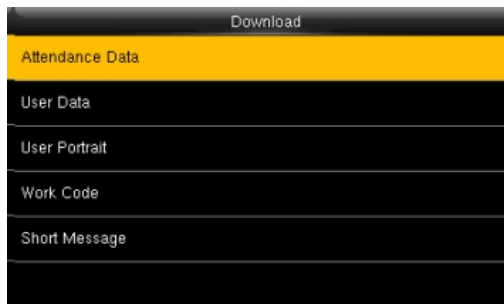
Enter the user ID to search.



Select the time range for attendance record query.

Device Operation

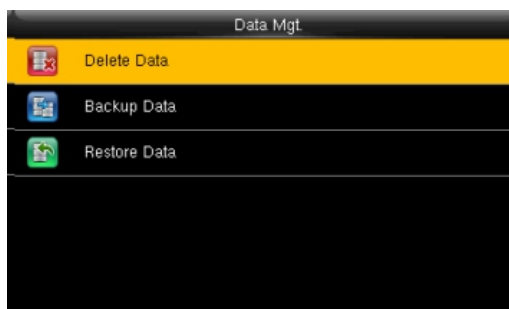
b. View records on computer (Main Menu > USB Manager > Download > Attendance Data)



1. Insert the USB disk correctly.
 2. Download the attendance data to the disk.
 3. Upload the attendance data from the disk to your computer.
 4. Name the downloaded data as "Device Serial Number.dat".
- You can open the downloaded data and view it.

6) Backup data

To avoid data loss due to mis-operation, you can back up the data to local drive or USB disk at any time.



1. Enter Main Menu > Data Management > Backup Data > Saving Type > Data Type to backup.
2. Select the content to-be-backed up.

7) Some miscellaneous settings

a. Date Time(Main Menu > System > Date Time)

Set the date, time and time format for the device.

b. Work Code(Main Menu > Work Code > New Work Code)

c. Short Message(Main Menu > Short Message)

Troubleshooting

Q: The palm is not recognized by the device while verification.

A: 1.Check out if the palm postures and distance is same in enrolling and verifying.

2.Check out if the sunlight is direct to the device or if the device is near to the windows.

Q: The device make a misjudgment while verification.

A: There is a certain probability of misjudgment, you can re-enroll the palm.



Workplace Intelligence

2525 FYI Center, Building 1, 5th Floor,
Unit 1/506, Rama 4 Road, Klong Toei,
KlongToei, Bangkok 10110, Thailand

Tel : (+66) 2 784-5855