USER MANUAL

BioPro SA40

WIFI Access Control Terminal

Version: 1.0

Date: Sept. , 2016

About This Manual

- This manual introduces the operation of user interfaces and menu functions of 2.4 Inch TFT WIFI Access Control terminal.
- The pictures in this manual may not be exactly consistent with those of your product; the actual product's display shall prevail.
- Not all the devices have the function with ★, the real product prevails.

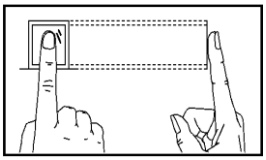
Contents

1 Guidance Notes

1.1 Method of Pressing Fingerprint

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

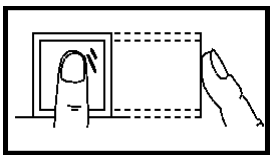
1. Correct way to press the fingerprint:



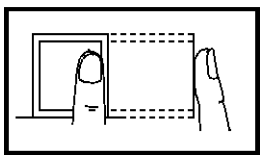
Press the finger horizontally onto the fingerprint sensor; the center of the fingerprint should be placed on that of the

2. Wrong ways to press the fingerprint:

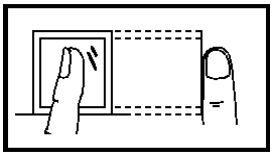
Vertical



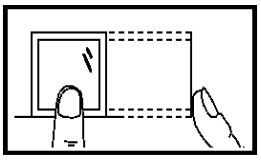
Sides



Slanted



Too Low



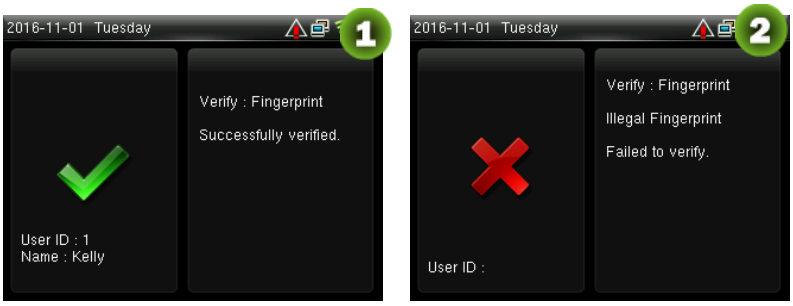
Please use the correct method of pressing fingerprint for registration and verification. Our company does not undertake the responsibility for the lowered verification performance caused by user's improper operation. The rights to final interpretation and amendment are reserved.

1.2 Verification Modes

1.2.1 1:N Fingerprint Verification

Under this fingerprint verification method, a fingerprint collected by the sensor is verified with all fingerprints stored in the device.

Please use the correct way to press fingerprint onto the fingerprint sensor (for detailed instruction, please refer to 1.1 Method of Pressing Fingerprint).

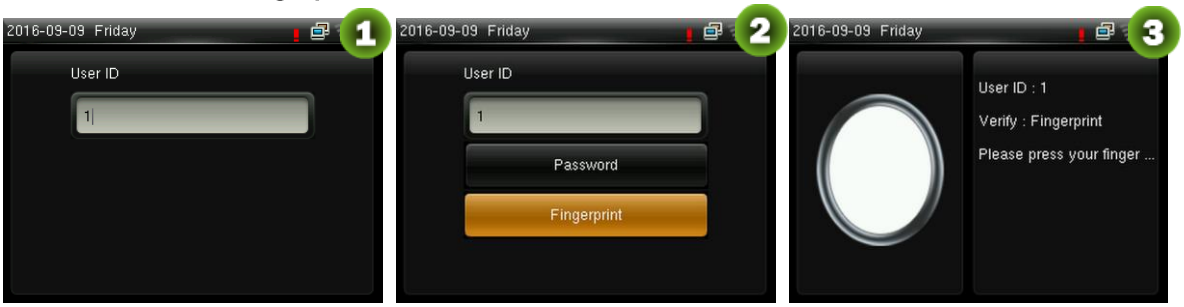


Verification Succeeds Verification Fails

Remarks：When the device displays “please press your finger again”, press your finger again onto the fingerprint sensor.

1.2.2 1:1 Fingerprint Verification

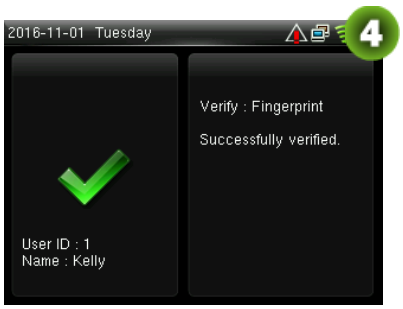
Under this fingerprint verification method, a fingerprint collected by the sensor is verified with the fingerprint corresponding to the entered user ID. Please use this method when difficulty is encountered in 1:N fingerprint verification.



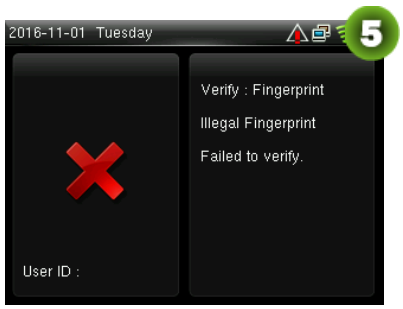
Input the user ID and press [M/OK].

Press ▼ button to choose “Fingerprint” and press [M/OK].

Press finger onto the sensor afterwards.



Verification succeeds



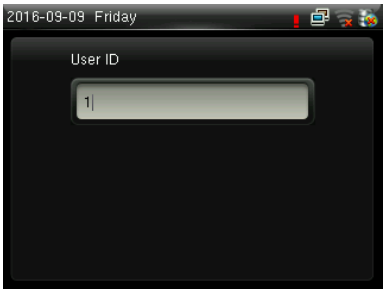
Verification fails

Remarks:

1. Input user ID in the initial interface and press [M/OK] button. If "Incorrect user ID!" is displayed, this means the user ID does not exist.
2. When the device displays "please press your finger again", press your finger again onto the fingerprint sensor. If verification still fails after 3 attempts, it will exit to the initial interface.

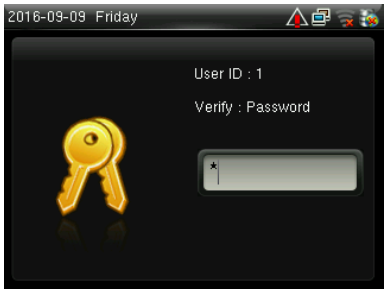
1.2.3 Password Verification

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

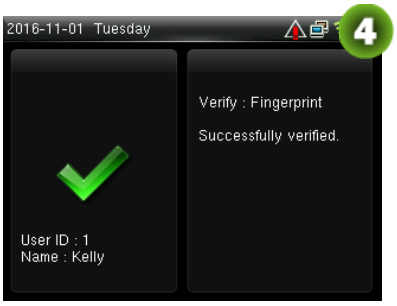


Input the user ID and press [M/OK]

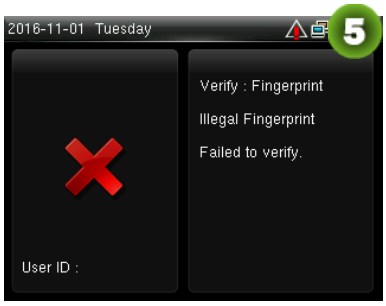
Choose "Password" and press [M/OK]



Input password



Verification succeeds

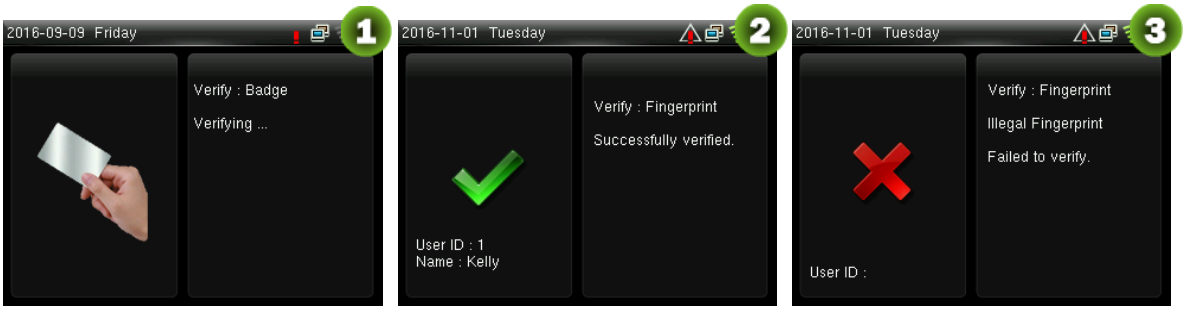


Verification fails

Remarks: If "Incorrect password" is displayed, please enter the password again. If verification still fails after 3 attempts, it will exit to the initial interface.

1.2.4 Card Verification ★

☺Remarks: 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.



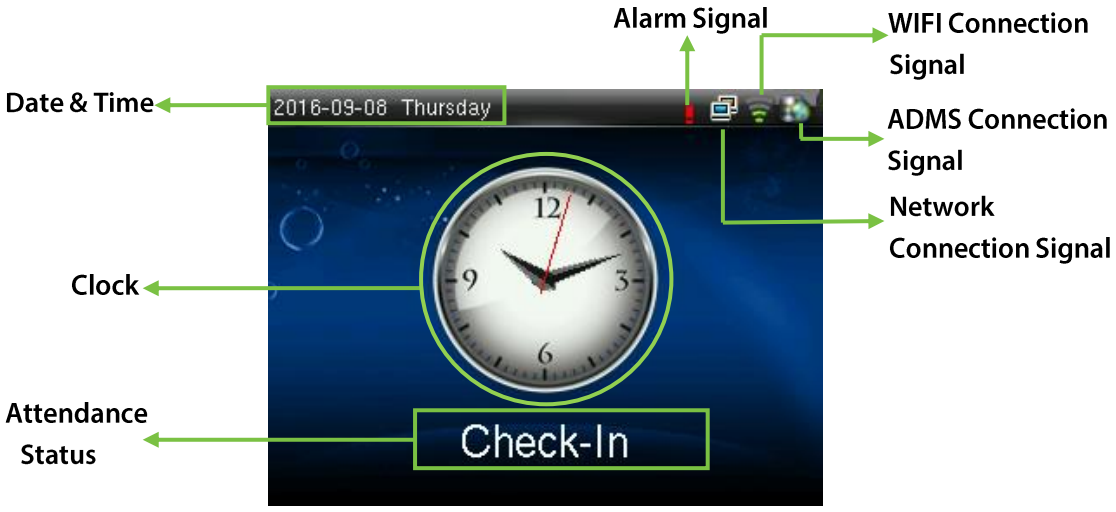
Swipe the card above the card reader (the card must be registered first)

Verification succeeds

Verification fails

1.3 Initial Interface

When the device is turned on, the initial interface is shown as below:



2 Main Menu

When the device is in standby mode, press [M/OK] to open the Main Menu.

User Mgt.: Basic information of registered users, including user ID, name, user role, fingerprint, badge ★ (ID and MiFare card are optional), password and access control role.

User Role: To set user roles for accessing into the menu and changing settings.

Comm.: To set the related parameters of the communication between the device and PC, including ethernet parameters such as IP address etc., serial Comm, PC connection, Wireless Network, ADMS★ and Wiegand settings.

System: To set related parameters of the system and upgrade firmware, including setting date & time, attendance and fingerprint parameters and resetting to factory settings.

Personalize: This includes interface display, voice, bell, punch state key mode and shortcut key settings.

Data Mgt.: delete attendance data, delete all data, delete admin role and delete screen savers etc.

Access Control: This includes setting the parameters of the lock.

USB Manager: To transfer data such as user data and attendance logs from the USB disk to the supporting software or other devices.

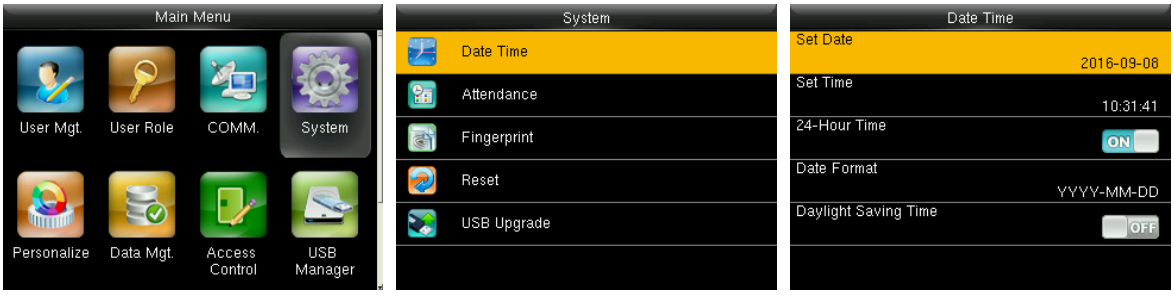
Attendance Search: To search for the records stored in the device after successful verification.

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

Autotest: To automatically test different module's functions, including the LCD, voice, keyboard, fingerprint sensor and clock RTC test.

System Info: To check device capacity, device and firmware information.

3 Date/Time Settings



In the initial interface, press [M/OK] > System > Date Time to enter the date/time setting interface. It includes setting date, time, 24-hour clock, date format and daylight saving time.

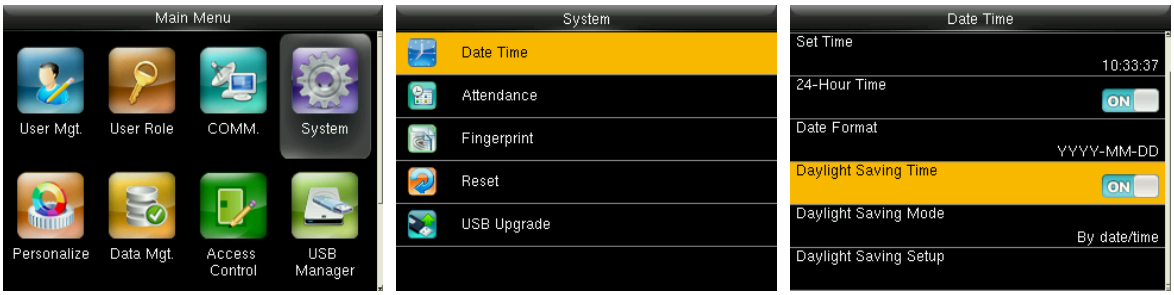
When resetting to factory settings, the date format can be restored (YYYY-MM-DD).

Remarks: When resetting to factory settings, the device's date/time will not be restored (if the date/time is set to 18:30 on January 1, 2020, after settings are reset, the date/time will stay at 18:30 on January 1, 2020).

3.1 Daylight Saving Time

DST, which is also called Daylight Saving Time, is a system adjusting local time in order to save energy. The time adopted during the set dates is called "DST". Usually, the time will be one hour forward in summer. This enables users to sleep or get up earlier, and also reduce device's lighting to save power. In autumn, the time will resume the standard time. Regulations are different in different countries. At present, nearly 110 countries adopt DST.

To meet the demand of DST, a special option can be customized. Make the time one hour forward at XX (hour) XX (day) XX (month), and make the time one hour backward at XX (hour) XX (day) XX (month).



Press [M/OK] > System > Date Time > Daylight Saving Time, then press [M/OK] to enable Daylight Saving Time.

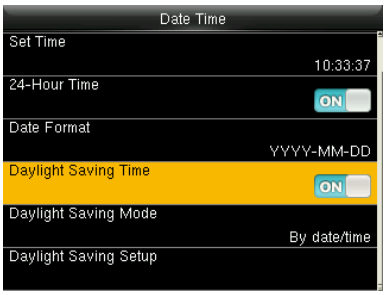
Daylight Saving Mode: Daylight Saving Time Mode, by date/time mode and by week/day mode for selection.

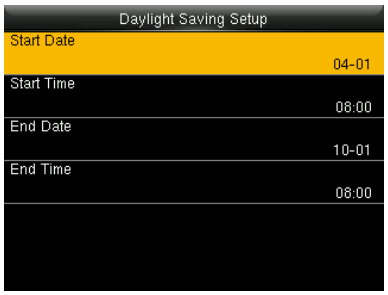
Daylight Saving Setup: Set date/time or week/day of the Daylight Saving Time according to the selection in Daylight Saving Mode.

How to set the Daylight Saving Time?

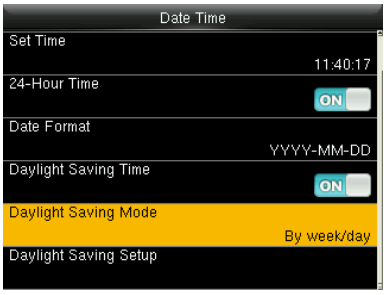
For example, adjust the clock forward one hour at 08: 00 on April 1 and backward one hour at 08: 00 on October 1 (the system turns back to the original time).

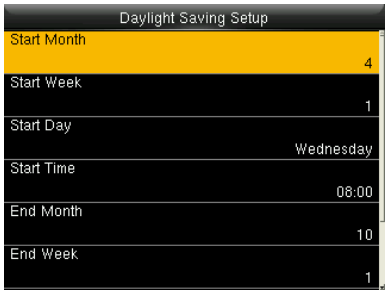
- By date/time mode:

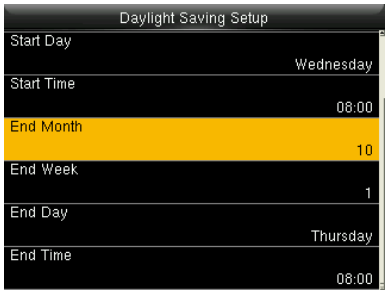




- By week/date mode:







Remarks:

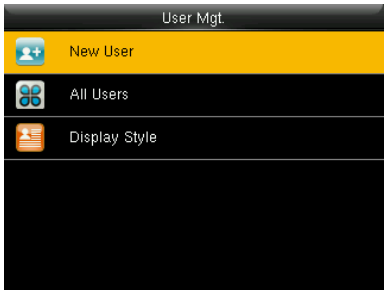
1. If the month when DST starts is later than that when DST ends, DST spans two different years. For example, the DST start time is 2014-9-1 4:00 and the DST end time is 2015-4-1 4:00.
2. Assume that the week /day mode is selected in [Daylight Saving Mode] and the DST starts from Sunday of the sixth week of September in 2013. According to the calendar, September of 2014 does not have six weeks but has five weeks. In this case, in 2014, DST starts at the corresponding time point of the last Sunday of September.
3. Assume that the DST starts from Monday of the first week of September in 2014. According to

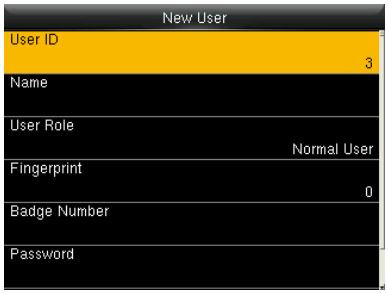
the calendar, the first week of September in 2015 does not have Monday. In this case, the DST starts from the first Monday of September in 2015.

4 User Management

4.1 Adding User

Including adding super admin and normal user.

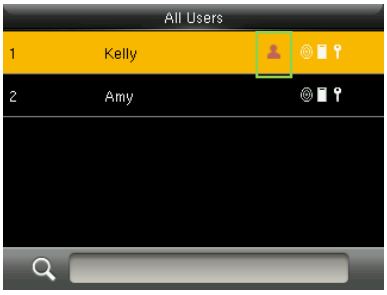




In the initial interface, press [M/OK] > User Mgt. > New User to enter New User setting interface. Settings include inputting User ID, Name, choosing User Role, registering Fingerprint and Badge Number ★(ID and Mifare card are optional), setting Password and setting Access Control Role.

Add a Super Admin: Choose "Super Admin" in [User Role], who is allowed to operate all the functions on the menu.

As shown below, the user with User ID 1 is a super admin.



Add a Normal User: Choose "Normal User" in [User Role]. When the Super Admin is set, Normal Users can only use fingerprint, password or card for verification; when the Super Admin is not yet set, Normal Users can operate all functions on the menu.

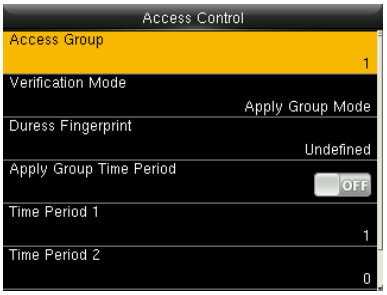
Password: 1 to 8 digits of password is accepted.

Remarks:

1. The device automatically allocates user ID for users in sequence, but user can set it manually as well.
2. The device supports user ID ranged from 1 to 9 digits.

4.2 Setting Access Control

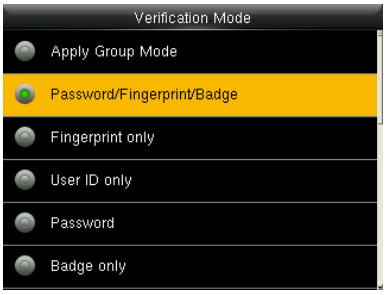
User access control option is to set open door access aimed at everybody, including access group setting, verification mode, using time zone, duress fingerprint management.

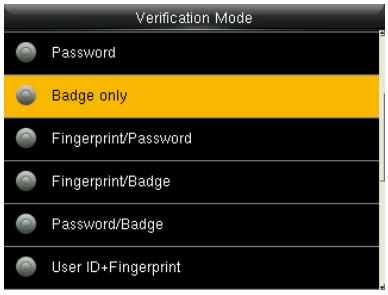


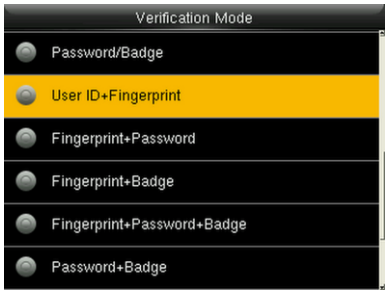
Access group: To allocate users to different access control groups for management. New users belong to Group 1 in default settings, who can be reallocated to other groups.

Verification mode: User can choose either group or individual verification. If individual verification is chosen, the verification method used by other group members will not be affected.

Individual Verification Type: Including password / fingerprint / badge, fingerprint only, user ID only, password, badge only, fingerprint / password, fingerprint / badge, password / badge, user ID & fingerprint, fingerprint & password, fingerprint & badge, fingerprint & password & badge, password & badge, user ID & fingerprint & password, fingerprint & (badge /user ID).

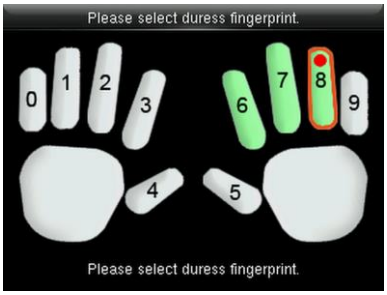






Remarks: Individual verification shall prevail over group verification.

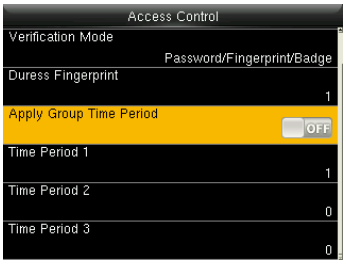
Duress Fingerprint: User can choose one or more registered fingerprint(s) as Duress Fingerprint. When that fingerprint is verified, duress alarm will be triggered.



Example: Among those registered fingerprints (6, 7, 8), choose the 8th fingerprint as the duress fingerprint.

Use Group Time Period:

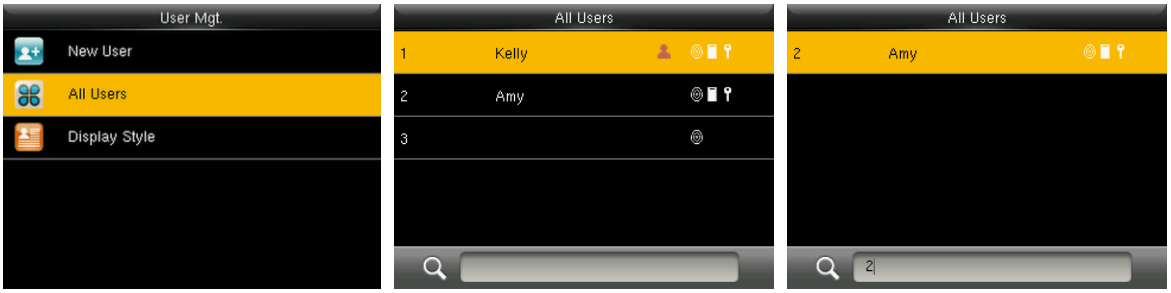
1. When this function is on, the user uses the default time zone of his/her group.
2. When this function is off, the user needs to set a personal time zone (not using the group time zone). This will not affect the access time zone of other group members.



Remarks: Every user can set a maximum of 3 time periods.

4.3 Searching User

Enter user ID on the User List to search for a user.



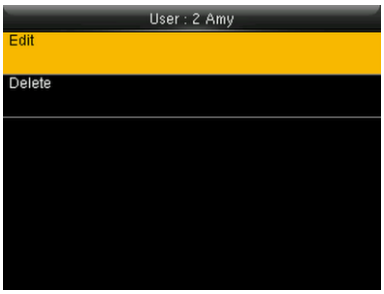
In the initial interface, press [M/OK] > User Mgt. > All User to enter All User interface. Input "User ID" in , the corresponding user will be shown. As shown in the above figure, search for the user with the user ID of "2".

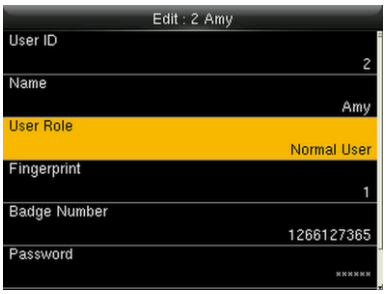
4.4 Editing User

After a user is chosen through 4.3 Searching User, press [M/OK] and select [Edit] to enter user editing interface.

Or in the initial interface press [M/OK] > User Mgt. > All User > Search a user > Press [M/OK] > Edit to enter user editing interface.

The operation method of editing user is the same with that of adding user, but the user ID cannot be edited.

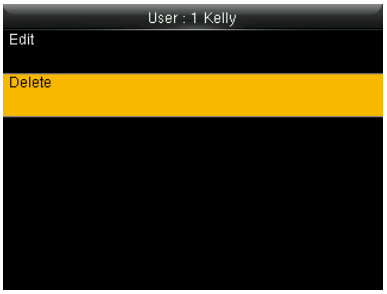


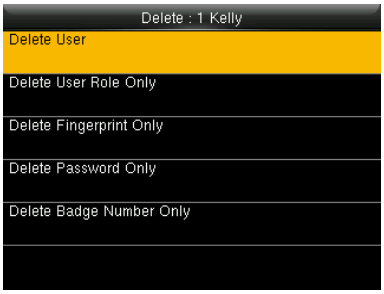


4.5 Deleting a User

After a user is chosen through 4.3 Searching User, press [M/OK] and select [Delete] to enter user deleting interface.

Or in the initial interface press [M/OK] > User Mgt. > All User > Search a user > Press [M/OK] > Delete to enter user deleting interface.

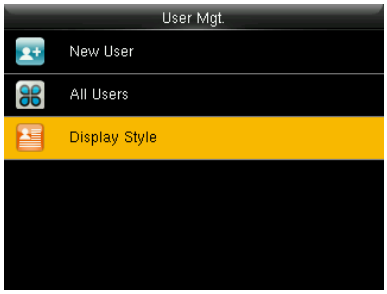




Note:

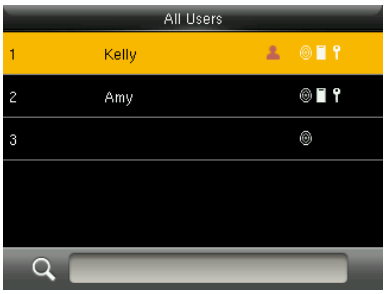
1. Only when the user has registered fingerprint, password and badge★, will the corresponding to-be-deleted item be shown.
2. Card function is optional.

4.6 User Display Style

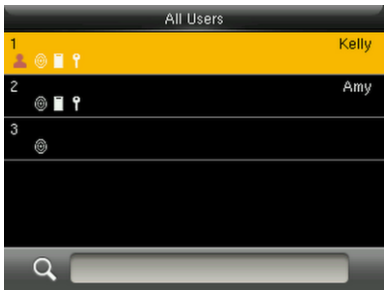


In the initial interface, press [M/OK] > User Mgt. > Display Style to enter Display Style setting interface.

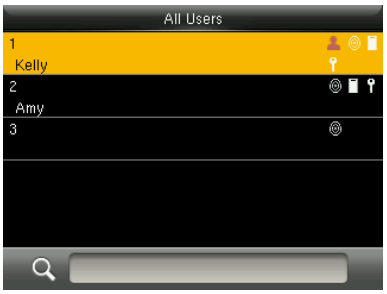
Several Display Styles are show as below:



Single Line Style



Multiple Line Style



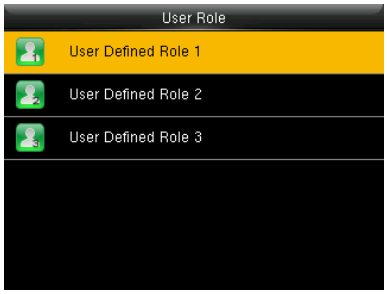
Mixed Line Style

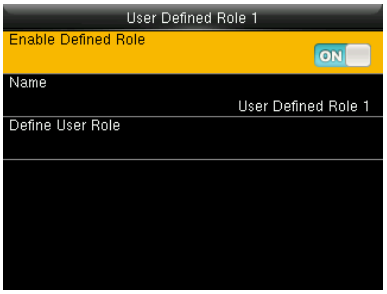
5 User Role

Setting user rights of operating the menu (a maximum of 3 roles can be set). When user role is enabled, in [User Mgt.] > [New User] > [User Role], you can allocate suitable user role to each user.

Role: Super user needs to allocate different rights to new users. To avoid setting rights for each user one by one, you can set user roles to categorize different permission levels in user management.

5.1 Enabling User Role



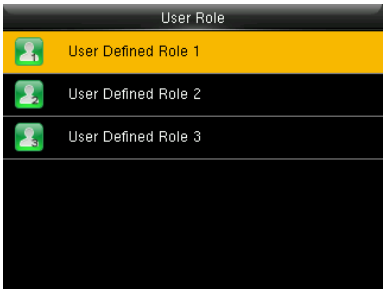


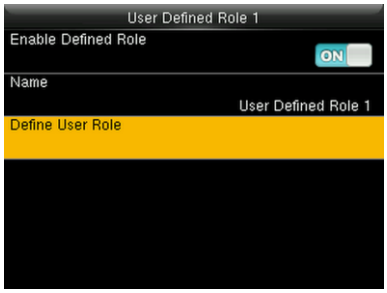
In the initial interface, press [M/OK] > User Role > User Defined Role 1 (2 / 3) > Enable Defined Role, Press [M/OK] to enable defined role.

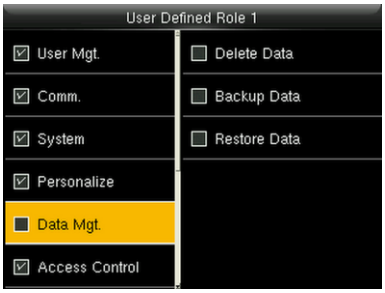
After enable defined roles, you can check the enabled user roles in [User Mgt.] > [New User] > [User Role].

☺ Remarks: At least one registered Administrator is required to enable user role.

5.2 Rights Allocation





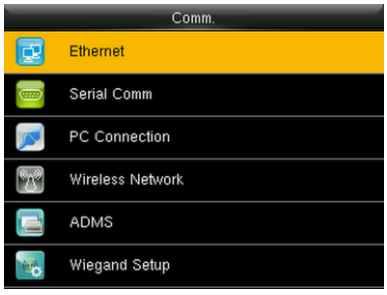


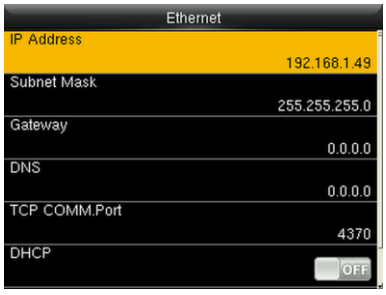
In the initial interface, press [M/OK] > User Role > User Defined Role 1 (2 / 3) > Define User Role to enter User Defined Role 1 (2 /3) rights allocating interface. Press [M/OK] to select or cancel the

operating right to each menu for User Defined Role 1 (2 /3).

6 Comm. Settings

6.1 Ethernet Settings





In the initial interface, press [M/OK] > Comm. > Ethernet to enter the Ethernet setting interface. The parameters below are the factory default values, please adjust them according to the actual network situation.

IP Address: 192.168.1.201

Subnet Mask: 255.255.255.0

Gateway: 0.0.0.0

DNS: 0.0.0.0

TCP COMM. Port: 4370

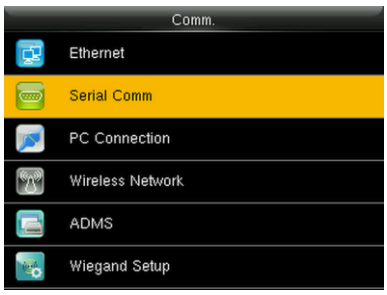
DHCP: Dynamic Host Configuration Protocol, which is to dynamically allocate IP addresses for clients via server. If DHCP is enabled, IP cannot be set manually.

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

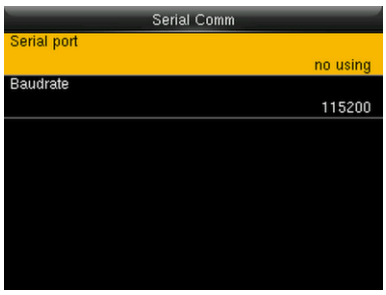
6.2 Serial Comm. Settings

- Turning On / OFF RS485 Function

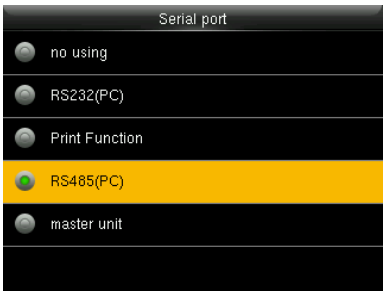
Press [M/OK] to enter main menu, and select Comm.



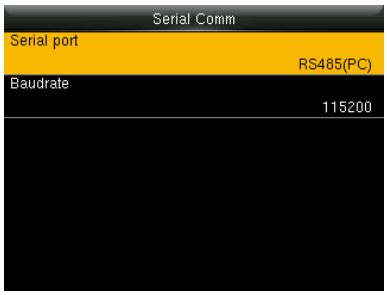
Press▼ key to select Serial Comm and press [M/OK] .



Press [M/OK] to enter Serial port.



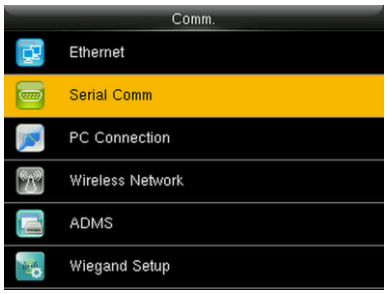
Press▼ key to select RS485(PC).



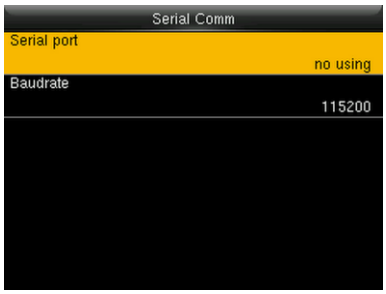
Finish.

- Turning On / OFF RS232 Function

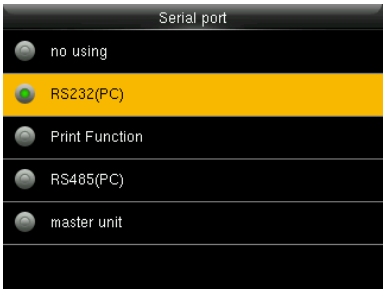
Press [M/OK] to enter main menu, and select Comm.



Press▼ key to select Serial Comm and press [M/OK].



Press [M/OK] to enter Serial port.



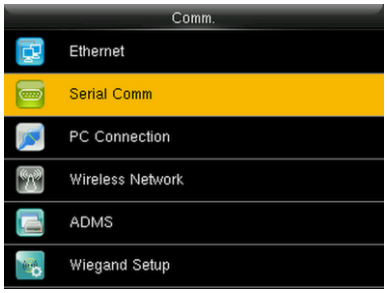
Press▼ key to select RS232(PC).

Finish.

Remarks:

1. RS485 Communication and RS232 Communication functions cannot be used at the same time.
2. When chooses "Print Function★" and the device is restarted, related printing information can be set in the submenu "Print". For more details of printing function, please refer to 17.4 Printing Function★.

- Baudrate Settings



In the initial interface, press [M/OK] > Comm. > Serial Comm > Baudrate to enter the Baudrate setting interface.

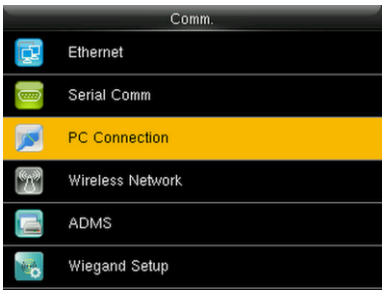
Baudrate: The rate of the communication with PC; there are 4 options of baud rate: 115200 (default), 57600, 38400 and 19200. The higher is the baudrate, the faster is the communication speed, but also the less reliable. In general, a higher baudrate can be used when the communication distance is short; when the communication distance is long, choosing a lower baudrate would be more reliable.

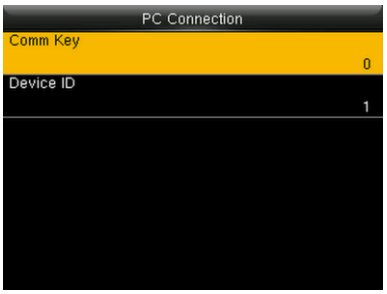
6.3 PC Connection

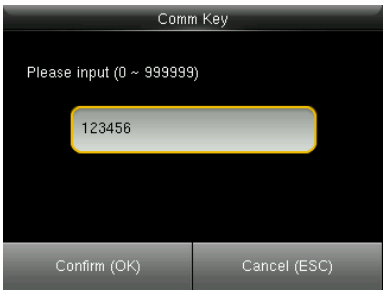
- Comm key Settings

To improve security of data, Comm Key for communication between the device and PC needs to be set.

If a Comm Key is set in the device, the correct connection password needs to be entered when the device is connected to the PC software, so that the device and software can communicate.





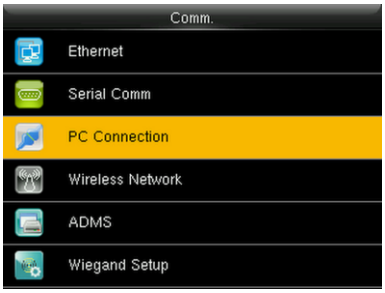


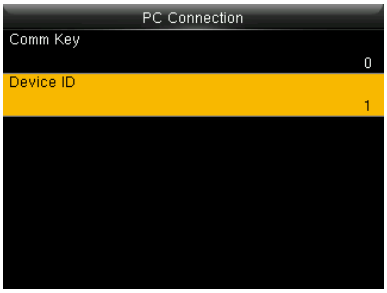
In the initial interface, press [M/OK] > Comm. > PC Connection > Comm Key to enter the Comm Key setting interface.

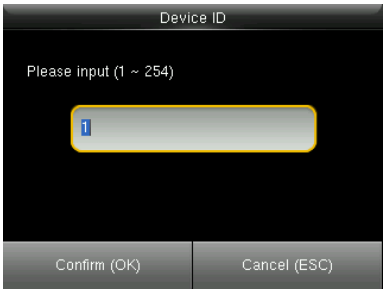
Comm Key: The default password is 0 (no password). Comm Key can be 1~6 digits and ranges between 0~999999.

- Device ID Settings

If the communication method is RS232/RS485, inputting this device ID in the software communication interface is required.







In the initial interface, press [M/OK] > Comm. > PC Connection > Device ID to enter the Device ID setting interface.

Device ID: Identity number of the device, which ranges between 1~254.

6.4 Wireless Network Settings

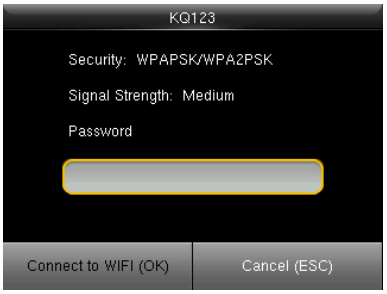
Wireless Network, can also be called WIFI. The WIFI module is built in the mold inside the device, in order to achieve the function of WIFI. To achieve through the WIFI wireless data transmission, provides a wireless network environment for the device.

- **WIFI Connection**

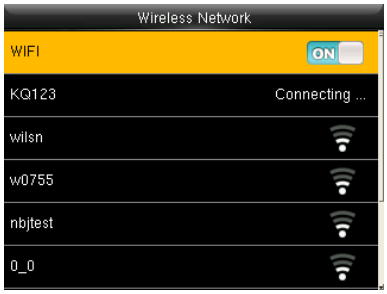
Press [M/OK] to enter main menu, and select Comm.

Press▼key to select Wireless Network and press [M/OK] to enter.

Press [M/OK] to open WIFI, device automatically searches for available WIFI.



Select an available WIFI, press [M/OK] to enter the password input interface.



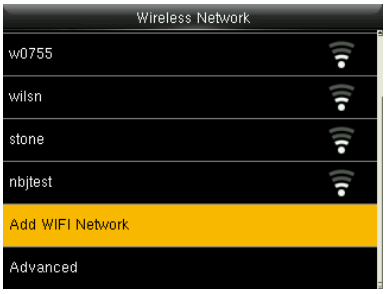
Connecting…

Finish.

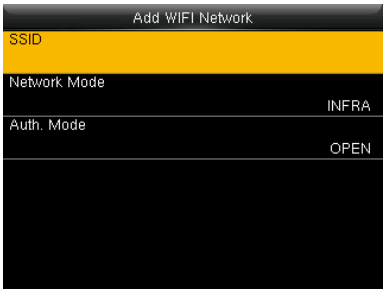
When the WIFI is connected successfully, the initial interface will display the logo.

- **Add WIFI Network**

You can manually add the WIFI network when there is no WIFI in the list that you want to connect to.



Press▼key to select "Add WIFI Network" and press [M/OK] to enter.

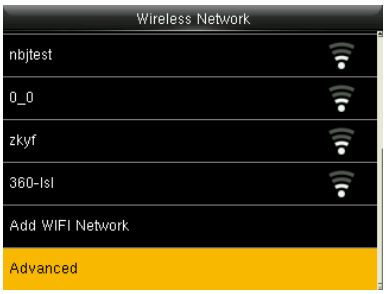


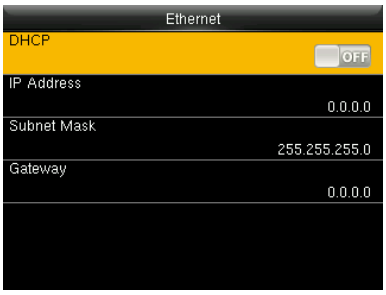
Enter the relevant parameters (The added network must exist).

Remarks: After manually add the WIFI network, to find the added items in the WIFI list,

for the connecting method, please refer to [WIFI Connection.]

- Advanced





Press▼key to select "Advanced" and press [M/OK] to enter.

Set the relevant parameters .

DHCP: Dynamic Host Configuration Protocol, which is to dynamically allocate IP addresses for clients via server. If DHCP is enabled, IP cannot be set manually.

IP Address: 0.0.0.0

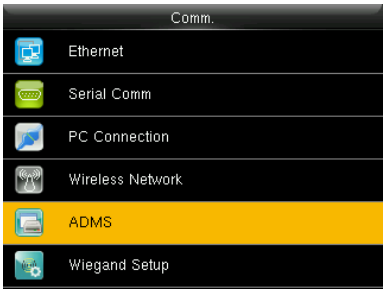
Subnet Mask: 255.255.255.0

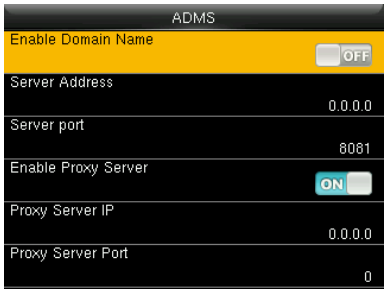
Gateway: 0.0.0.0

6.5 ADMS Settings★

☺ Remarks: Only some products are equipped with ADMS setting function.

Settings used for connecting with ADMS server, such as IP address and port settings, and whether to enable proxy server etc.





In the initial interface, press [M/OK] > Comm. > ADMS to enter the ADMS server setting interface.

When the Webserver is connected successfully, the main interface will display the logo.

Enable Domain Name: When this function is turned on, the domain name mode "http://..." will be used, such as http://www.XXX.com. XXX denotes the domain name when

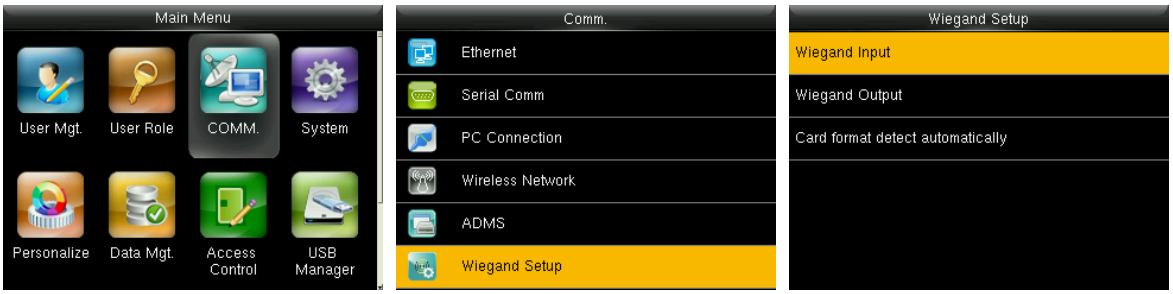
this mode is on; when this mode is off, enter the IP address format in XXX.

Server Address: IP address of the ADMS server.

Server Port: Port used by the ADMS server.

Enable Proxy Server: Method of enabling proxy. To enable proxy, please set the IP address and port number of the proxy server. Entering proxy IP and server address will be the same.

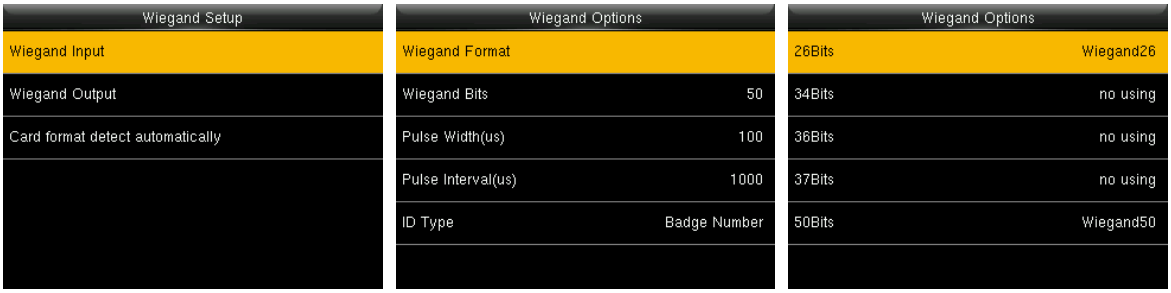
6.6 Wiegand Setup



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

6.6.1 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 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 and Wiegand 50.

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 400 microseconds.

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

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

Definitions of Wiegand Formats:

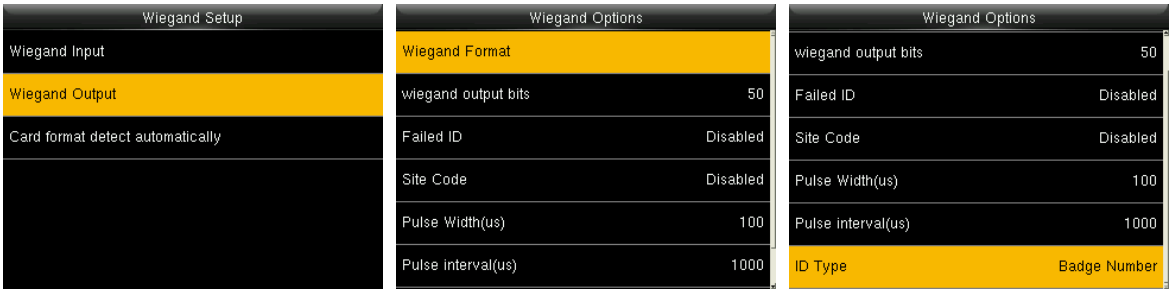
Wiegand Format	Definition
Wiegand26	ECCCCCCCCCCCCCCCCCCCCCCCCO Consists of 26 bits of binary code. The 1st bit is the even parity bit of the 2nd to 13th bits, while the 26th bit is the odd parity bit of the 14th to 25th bits. The 2nd to 25th bits are the card number.
Wiegand26a	ESSSSSSSSCCCCCCCCCCCCCCCCO Consists of 26 bits of binary code. The 1st bit is the even parity bit of the 2nd to 13th bits, while the 26th bit is the odd parity bit of the 14th to 25th bits. The 2nd to 9th bits are the site code, while the 10th to 25th bits are the card number.
Wiegand34	ECCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO Consists of 34 bits of binary code. The 1st bit is the even parity bit of the 2nd to 17th bits, while the 34th bit is the odd parity bit of the 18th to 33rd bits. The 2nd to 25th bits are the card number.
Wiegand34a	ESSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCO Consists of 34 bits of binary code. The 1st bit is the even parity bit of the 2nd to 17th bits, while the 34th bit is the odd parity bit of the 18th to 33rd bits. The 2nd to 9th bits are the site code, while the 10th to 25th bits are the card number.
Wiegand36	OFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCMME Consists of 36 bits of binary code. The 1st bit is the odd parity bit of the 2nd to 18th bits, while the 36th bit is the even parity bit of the

	19th to 35th bits. The 2nd to 17th bits are the device code, the 18th to 33rd bits are the card number, and the 34th to 35th bits are the manufacturer code.
Wiegand36a	EFFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCO Consists of 36 bits of binary code. The 1st bit is the even parity bit of the 2nd to 18th bits, while the 36th bit is the odd parity bit of the 19th to 35th bits. The 2nd to 19th bits are the device code, and the 20th to 35th bits are the card number.
Wiegand37	OMMMMSSSSSSSSSSSCCCCCCCCCCCCCCCCCCE Consists of 37 bits of binary code. The 1st bit is the odd parity bit of the 2nd to 18th bits, while the 37th bit is the even parity bit of the 19th to 36th bits. The 2nd to 4th bits are the manufacturer code, the 5th to 16th bits are the site code, and the 21st to 36th bits are the card number.
Wiegand37a	EMMMFFFFFFFFFSSSSSSCCCCCCCCCCCCCCCCO Consists of 37 bits of binary code. The 1st bit is the even parity bit of the 2nd to 18th bits, while the 37th bit is the odd parity bit of the 19th to 35th bits. The 2nd to 4th bits are the manufacturer code, 5th to 14th bits are the device code, 15th to 20th bits are the site code, and the 21st to 36th bits are the card number.
Wiegand50	ESSSSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO Consists of 50 bits of binary code. The 1st bit is the even parity bit of the 2nd to 25th bits, while the 50th bit is the odd parity bit of the 26th to 49th bits. The 2nd to 17th bits are the site code, and 18th to 49th bits are the card number.

Note: C denotes card number, E denotes even parity bit, O denotes odd parity bit, F denotes device code, M denotes manufacturer code, P denotes parity bit, and S denotes site code.

6.6.2 Wiegand Output

Wiegand Output connector connects the device as a slave device to another device (master device), forming a master/slave system.



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 and 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.

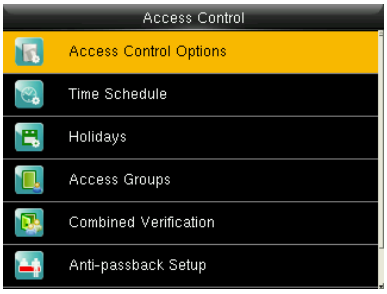
Pulse Width (us): The width of pulse sent by Wiegand. The default value is 100 microseconds, which can be adjusted within the range of 20 to 400 microseconds.

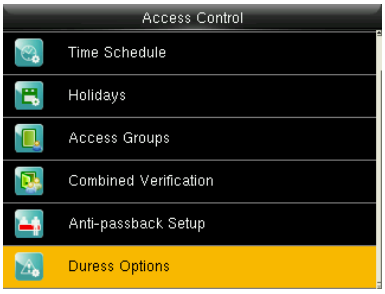
Pulse Interval (us): The default value is 1000 microseconds, which can be adjusted within the range of 200 to 20000 microseconds.

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

7 Access Control

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





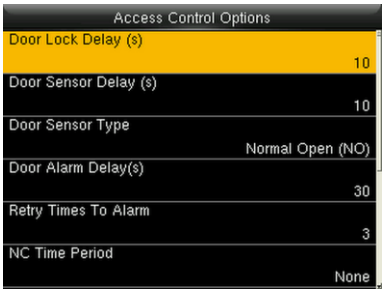
In the initial interface, press [M/OK] > Access Control to enter Access Control setting interface.

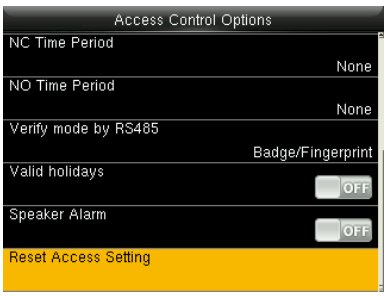
To gain access, the registered user must meet the following conditions:

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

In default settings, new users are allocated into the first group with the default group time zone and access combo as "1", and set in unlocking state.

7.1 Access Control Options Settings





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, Normally Open and Normally Closed. None means door sensor is not in use; Normally Open means the door is opened when electricity is on; Normally Closed means the door is closed when electricity is on.

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

Retry Times To Alarm: When the number of failed verification reaches the set value (value ranges from none, 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.

Verify Mode by RS485: To turn on RS485 reader function; it is the verification method used by the device when it is the master/slave device.

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, normally open / close for holidays, speaker alarm, anti-passback direction, 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.

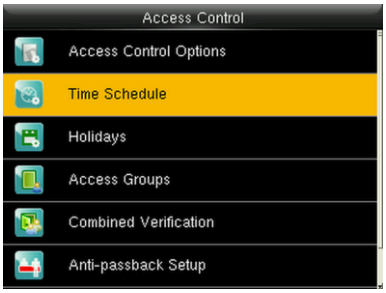
Access Parameters	Factory Default
Door Lock Delay	10 s

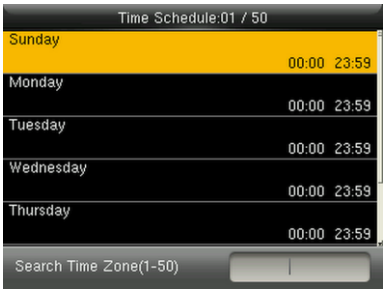
Door Sensor Delay	10 s
Door Sensor Type	None
Door Alarm Delay	30 s
Retry Times To Alarm	3 times
NC Time Period	None
NO Time Period	None
NO/NC Validity in Holiday	Off
Speaker Alarm	Off
Anti-Passback Direction	No anti-passback
Device Status	Out
Help Key	Off
1:1 Verification Alarm	Off
1:N Verification Alarm	Off
Password Verification Alarm	Off
Duress Alarm Delay	10 s

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

7.2 Time Schedule Settings

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





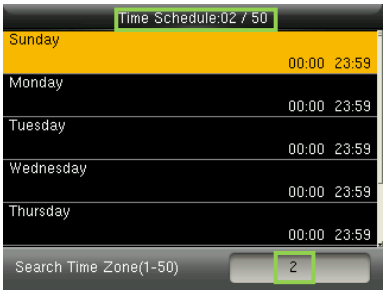
In the initial interface, press [M/OK] > Access Control > Time Schedule to enter the Time Schedule

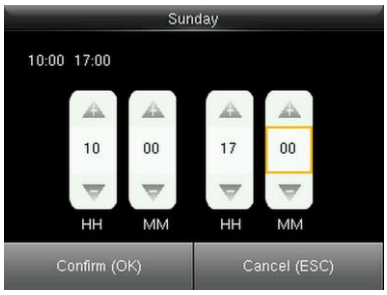
interface. The default Time Schedule No. is 1 (whole-day valid), which can be edited.

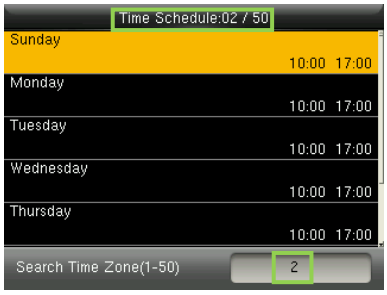
Valid Time Schedule: 00:00 ~ 23:59 (Whole-day valid) or when the end time is greater than the start time.

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

Example 1: Setting Time Schedule 02 (Valid)

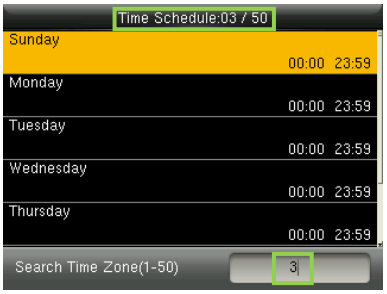


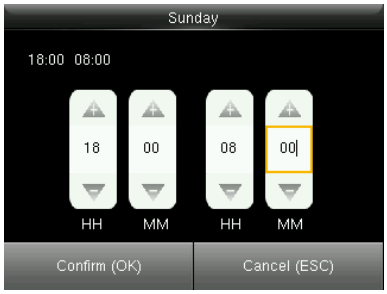


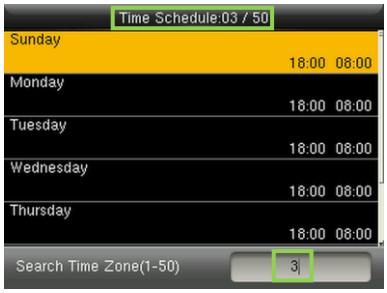


Setting it as 10:00 ~ 17:00 from Sunday to Saturday, since the end time is greater than the start time, Time Schedule 2 is valid.

Example 2: Setting Time Schedule 03 (Invalid)





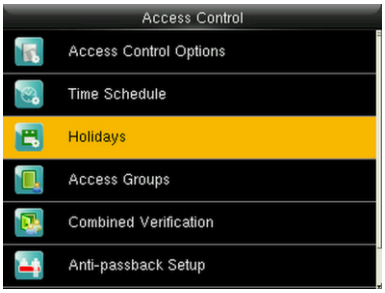


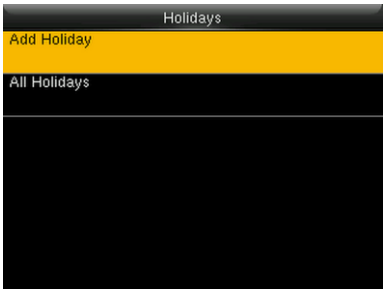
In Time Schedule 3, the everyday end time is smaller than the start time, so Time Zone 3 is invalid.

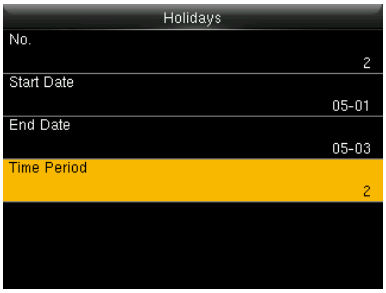
Remarks: The **Time Schedule** cannot be set across two days, which means that the end time must be greater than the start time.

7.3 Holidays Settings

The holiday access control time can be set, which is applicable for all users during holiday.







In the initial interface, press [M/OK] > Access Control > Holidays > Add Holiday to enter the Add Holiday interface. Settings include number, start time, end time and time period.

Remarks: Start/End Date only requires to set the month (MM) and date (DD), which is applicable to all years. As shown in above figure: Holiday 2 starts on the May 1 every year, ends on the May 3 every year, while adopting Time Period 2 (10:00 ~ 17:00 from Sunday to Saturday).

To enable Holiday function:

In the initial interface, press [M/OK] > Access Control > Access Groups > All Groups > select an access control group > Edit > Include Holidays, press [M/OK] to enable (ON) the holiday.

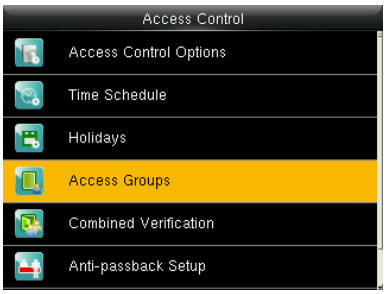
The turning on/off of the Holiday function is applicable to all users in the same access group.

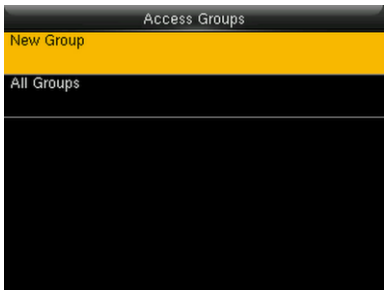
7.4 Access Groups Settings

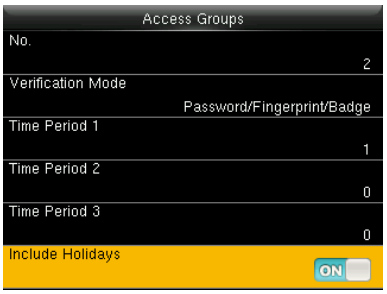
Grouping is to manage users in groups.

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.

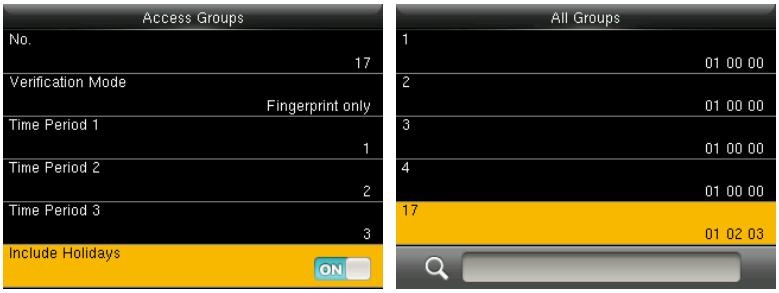






In the initial interface, press [M/OK] > Access Control > Access Groups > New Group to enter the New Group interface.

Taking below figures as an example:



As shown in the above figures, the Verification Mode of Access Group 17 is fingerprint only; Time Zone 1, 2 and 3 are set, while the Holiday function is enabled.

7.4.1 Set Holiday for Access Group

To enable Holiday function:

Set Time Schedule (including Access Time Schedule and Holiday Time Schedule) > set Holiday > allocate users to an access group > turn the [Include Holidays] of the access group to [ON].

Remarks:

1. When the Holiday function is enabled, only when the time schedules of access group and the holiday overlap can the members gain access.
2. When the Holiday function is disabled, the access time of users in an access group will not be affected.

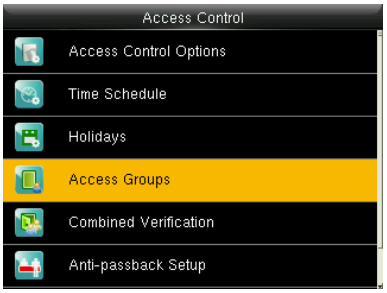
For example:

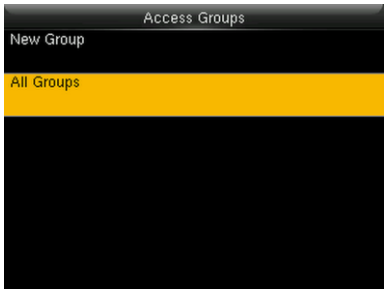
If Access Group 2 requires to use Holiday Time Schedule 2 in International Worker's Day, which means to let users gain access during 10:00 ~ 17:00 (Time Schedule 2) in May 1 to 3.

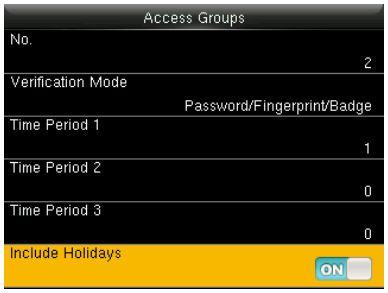
Operating Method:

1. Set Time Schedule 2 to 10:00 ~ 17:00 from Sunday to Saturday. For the setting method, please refer to the example of setting Time Zone 2 in 7.2 Time Schedule Settings.
2. Use Time Schedule 2 for holiday. For method of setting holiday, please refer to 7.3 Holidays Settings.
3. Setting access group, please refer to 7.4 Access Group Settings for instruction.
4. Enable Holiday function. In the initial interface, press [M/OK] > Access Control > Access Groups > All Groups > 2 > press [M/OK] > Edit > Include Holidays, press [M/OK] to the [Include

Holidays] to [ON] (enabled).







5. Users in Access Group 2 verify to gain access, setting succeeds.

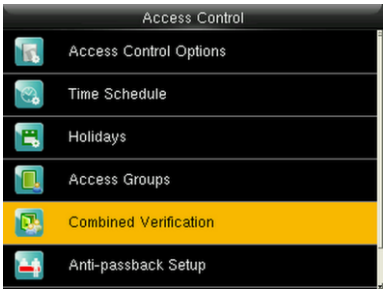
Remarks: If a holiday should be valid for all users, allocate all users to the same group or enable the [Include Holidays] for all access groups.

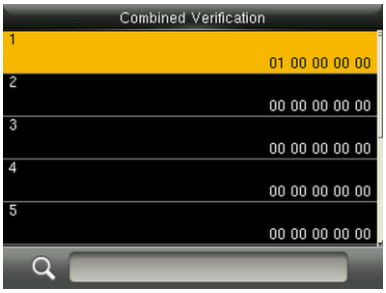
7.5 Combined Verification Settings

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

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

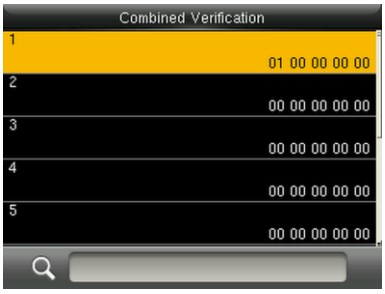
Remarks: Only group No. set in Access Group interface, can it be selected in the Combined Verification setting.

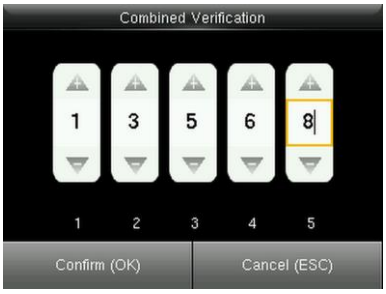


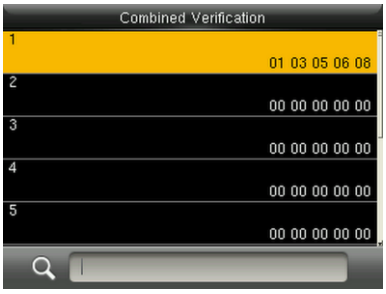


In the initial interface, press [M/OK] > Access Control > Combined Verification > 1 to enter the first Combined Verification setting interface.

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

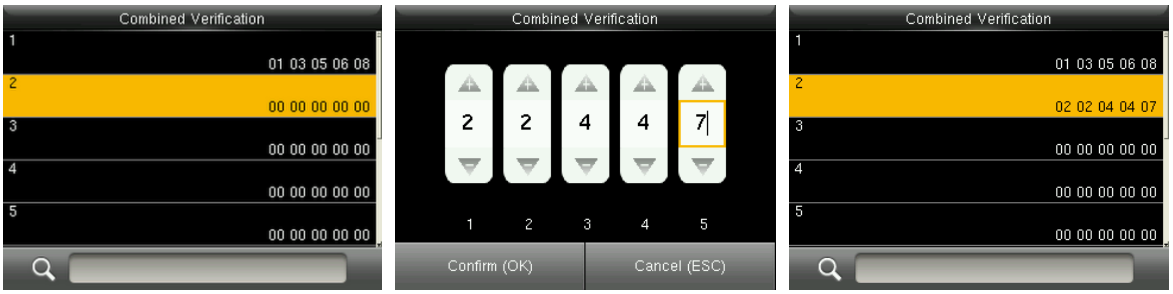




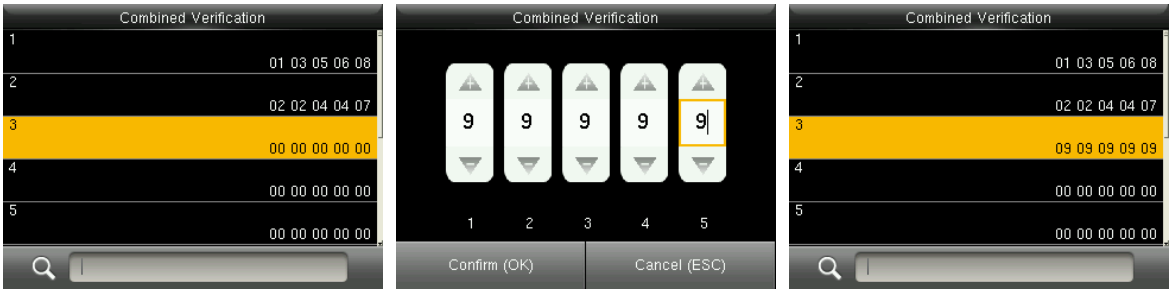


As the above figure, Combined Verification 1 is made up of five members coming from five

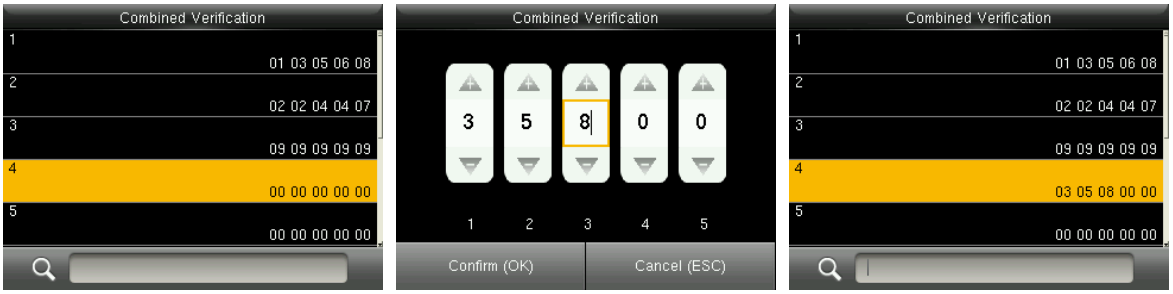
different groups---access group 1 / 3 / 5 / 6 / 8 respectively.



As the above figure, Combined Verification 2 is made up of five members coming from three different groups: two members from Access Group 2, two from Group 4, and one from group 7.



As the above figure, Combined Verification 3 is made up of five members, and all of them come from Access Group 9.

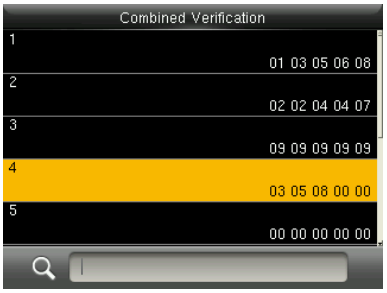


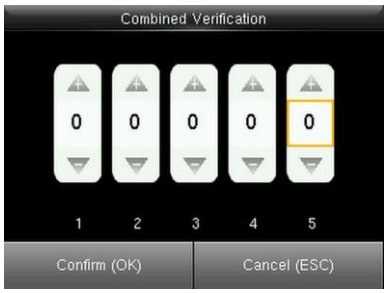
As the above figure, Combined Verification 4 is made up of three members coming from three different groups -- Access Group 3, 5, 8 respectively.

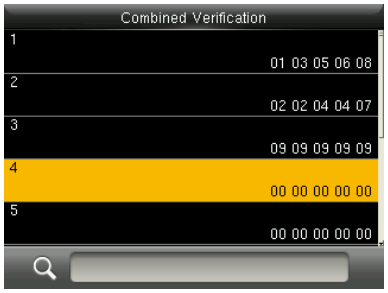
Deleting a Combined Verification

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

For example, to delete Combined Verification 4, please see the figures below:





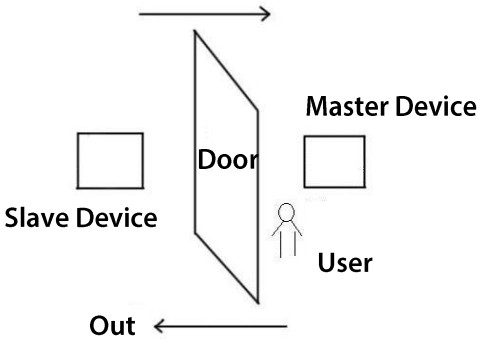


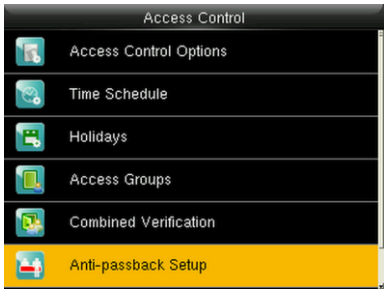
If all group numbers in Combined Verification 4 are set to 0, it will be deleted.

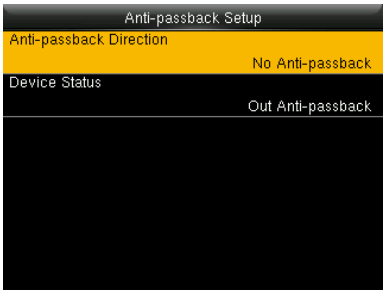
7.6 Anti-passback Settings

To avoid some persons following users to enter the door without verification, resulting in security problem, users can enable anti-passback function. The check-in record must match with check-out record so as to open the door.

This function requires two devices to work together: one is installed inside the door (master device), the other one is installed outside the door (slave device). The two devices communicate via Wiegand signal. The Wiegand format and Output type (User ID / Badge Number) adopted by the master device and slave device must be consistent.







In the initial interface, press [M/OK] > Access Control > Anti-passback Setup to enter the Anti-passback Setup interface. Select Anti-passback Direction and Device Status.

- Anti-Passback Direction

No Anti-passback: Anti-Passback function is disabled, which means passing verification of either master device or slave device can unlock the door. Attendance state is not reserved.

Out Anti-passback: After a user checks out, only if the last record is a check-in record can the user check out again; otherwise, the alarm will be triggered. However, the user can check in freely.

In Anti-passback: After a user checks in, only if the last record is a check-out record can the user check in again; otherwise, the alarm will be triggered. However, the user can check out freely.

In/Out Anti-passsback: After a user checks in/out, only if the last record is a check-out record can the user check in again, or a check-in record can the user check out again; otherwise, the alarm will be triggered.

Null and Save: Anti-passback function is disabled, but attendance state is reserved.

- Device Status

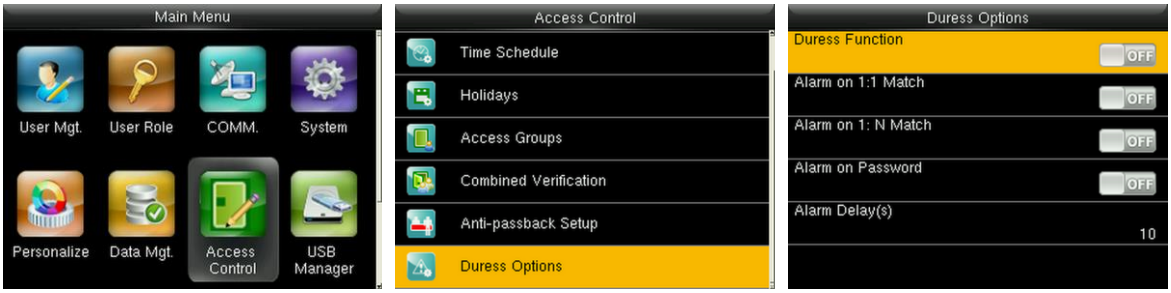
None: To disable the Anti-Passback function.

Out: All records on the device are check-out records.

In: All records on the device are check-in records

7.7 Duress Options Settings

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



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

Remarks: The above four types of duress alarm trigger methods (Duress Function, Alarm on 1:1 Match, Alarm on 1: N Match and Alarm on Password) are turned [OFF] in default settings.

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.

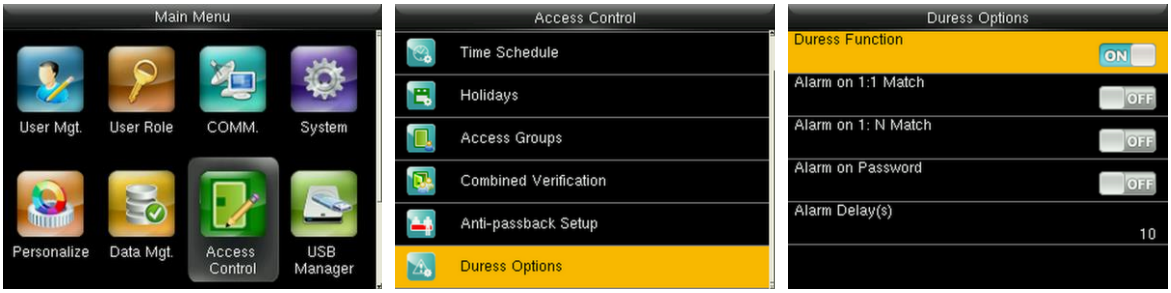
Alarm Delay (s): When duress alarm is triggered, the device will send out alarm signal after 10 seconds (default); the alarm delay time can be changed (value ranges from 1 to 999 seconds).

7.7.1 Duress Key Settings

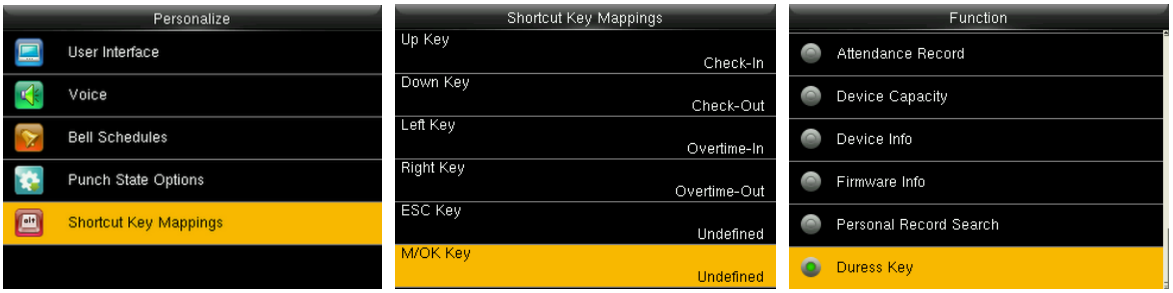
Duress Function: In [ON] state, press "Duress Key" and then press any registered fingerprint (within 10 seconds), duress alarm will be triggered after successful verification. In [OFF] state, pressing "Duress Key" will not trigger the alarm.

To Set (M/OK) as Duress Key

1. Turn On Duress Function: In the initial interface, press [M/OK] > Access Control > Duress Options > Duress Function, press [M/OK] to turn the Duress Function ON.



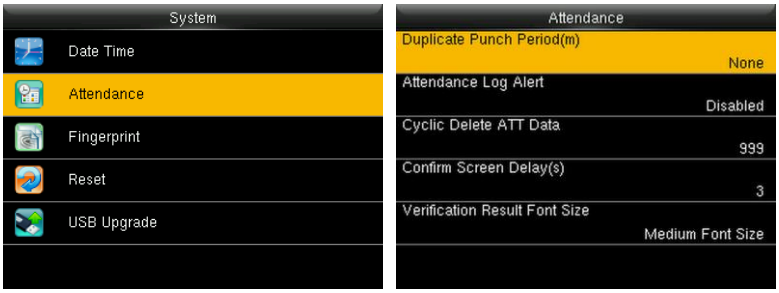
2. Setting Duress Key: In the initial interface, press [M/OK] > Personalize > Shortcut Key Mappings > select the [M/OK] key > press [M/OK] > Function > select the "Duress Key" option. (The Duress Key menu will be displayed after the Duress Function is turned on.)



Remarks: Direction keys or ESC can also be set as Duress Key.

8 System Settings

8.1 Attendance Parameters



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

Duplicate Punch Period (m): Within a set time period (unit: minutes), the duplicated attendance logs will not be reserved (value ranges from 1 to 999999 minutes).

Attendance Log Alert: When the remaining storage is smaller than the set value, the device will automatically alert users to the remaining storage information. It can be disabled or set to a value ranged from 1 to 9999.

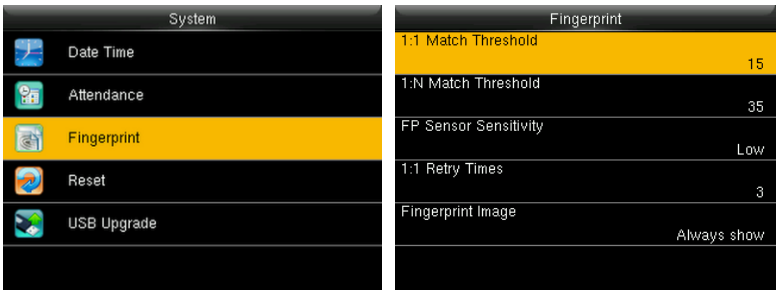
Cyclic Delete ATT Data: The number of attendance logs allowed to be deleted in one time when the maximum storage is attained. It can be disabled or set to a value ranged from 1 to 999.

Confirm Screen Delay(s): The display of the verification information interface after verification. Value ranges from 1 to 9 seconds.

For example, if the Confirm Screen Delay(s) is set to 5s, after successful verification, the verification information interface will be closed after 5s.

Verification Result Font Size: After verification, the verification result is displayed, there are 3 kinds of font sizes: Medium, Large and X-Large Font Size.

8.2 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

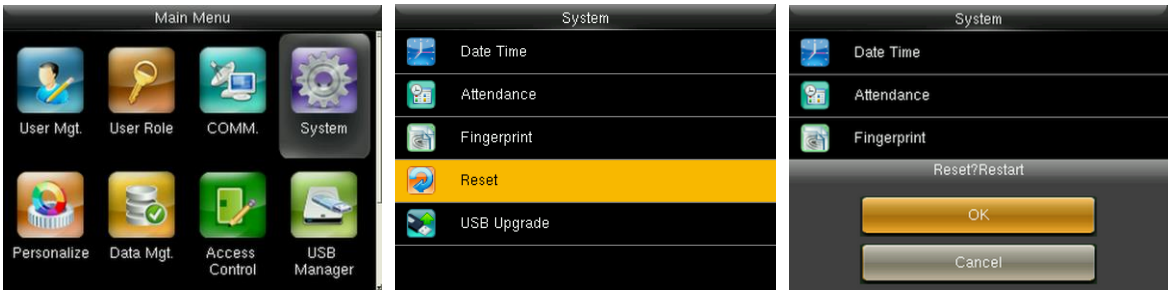
FP Sensor Sensitivity: To set the sensibility of fingerprint collection. It is recommended to use the default level "Medium". When the environment is dry, resulting in slow fingerprint detection, you can set the level to "High" to raise the sensibility; when the environment is humid, making it hard to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

8.3 Reset to Factory Settings

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



In the initial interface, press [M/OK] > System > Reset > OK to finish the reset setting.

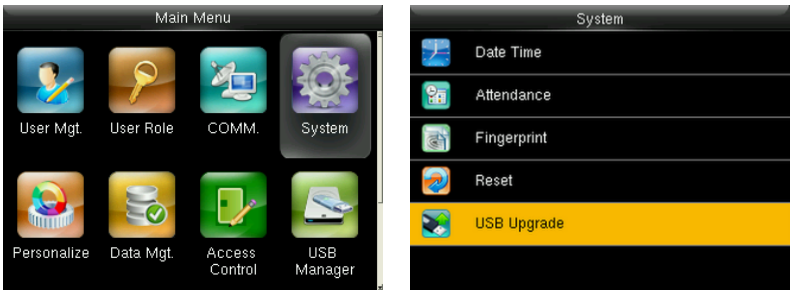
Reset parameters include Access Control Options, Duress Options, Anti-passback Setup, communication setting (namely, the setting of Ethernet, Serial Comm., PC Connection, WIFI, ADMS★ and Wiegand Setup), Personalize (such as Voice Prompt, Keyboard Prompt, Volume and Idle Time To Sleep), close punch state etc.

Parameters	Factory Defaults
Access Control Options	Door Lock Delay: 10 seconds Door Sensor Delay: 10 seconds Door Sensor Type: None Door Alarm Delay: 30 seconds Retry Times To Alarm: 3 times NC Time Period: None NO Time Period : None Normally open / close for holidays: OFF Speaker Alarm: OFF
Duress Options	Duress Function: OFF Alarm on 1:1 Match: OFF Alarm on 1: N Match: OFF Alarm on Password: OFF Alarm Delay: 10 seconds
Anti-passback Direction	No Anti-passback
Ethernet	IP Address: 192.168.1.201

	Subnet Mask: 255.255.255.0 Gateway: 0.0.0.0
PC Connection	Comm Key: 0 Device ID: 1
WIFI	DHCP: OFF IP Address: 0.0.0.0 Subnet Mask: 255.255.255.0 Gateway: 0.0.0.0
ADMS★	Enable Domain Name: OFF Server Address: 0.0.0.0 Server Port: 8081 Enable Proxy Server: ON Proxy Server IP: 0.0.0.0 Proxy Server Port: 0
Wiegand Setup	Wiegand Input / Output ID Type: User ID Pulse Width: 100 us Pulse interval: 1000 us
Idle Time To Slide Show	60 seconds
Idle Time To Sleep	30 minutes
Menu Screen Timeout	60 seconds
Keyboard Prompt	ON
Voice Prompt	ON
Volune	70

Remarks: When resetting to factory settings, the date and time will not be affected. For example, if the device date and time are set to 18:30 on January 1, 2020, the date and time will remain unchanged after resetting to factory settings.

8.4 USB Upgrade

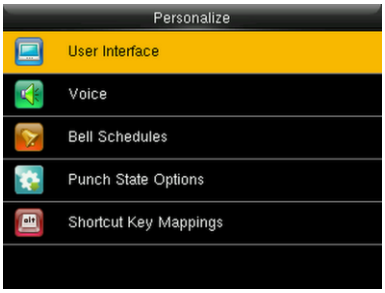


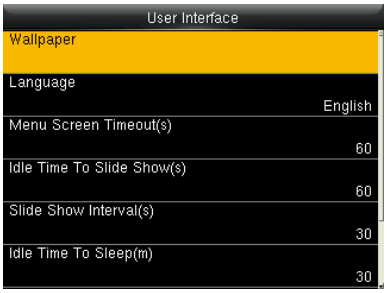
Insert the U disk with upgrade file into the device's USB port, and in the initial interface, press [M/OK] > System > USB Upgrade to complete firmware upgrade operation.

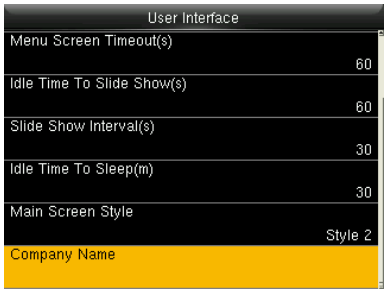
If upgrade file is needed, please contact out technical support. Firmware upgrade is not recommenced under normal

9 Personalize Settings

9.1 User Interface Settings







In the initial interface, press [M/OK] > Personalize > User Interface to set User Interface.

Wallpaper: Select the wallpaper of main screen as required, you can find wallpapers of various styles in the device.

Language: Select the language of device as required.

Menu Screen Timeout (s): When there is no operation in the menu interface and the time exceeds the set value, the device will automatically exit to the initial interface. You can disable it or set the value to 60~99999 seconds.

Remarks: If [Disabled] is chosen, the system will not exit the menu interface even when there is no operation. Disabling this function is not recommended due to great power used and insecurity.

Idle Time To Slide Show (s): When there is no operation in the initial interface and the time exceeds the set value, a slide show will be shown. It can be disabled (set to "None") or set to 3~999 seconds.

Slide Show Interval (s): This refers to the interval between displaying different slide show pictures. It can be disabled or set to 3~999 s.

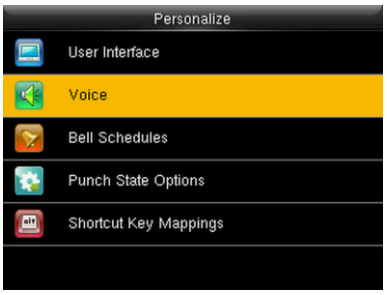
Idle Time To Sleep (m): When there is no operation in the device and the set Sleep Time is attained, the device will enter standby mode. Press any key or finger to cancel standby mode. You can disable this function, or set the value to 1~999 minutes. If this function is turned to [Disabled], the device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

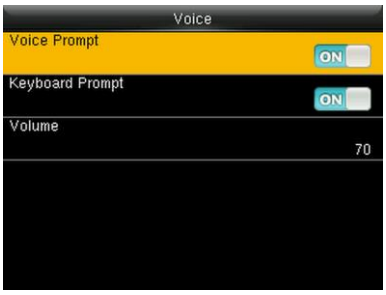
Remarks: Disabling this function is not recommended due to great power used.

Main Screen Style: Choosing the position and ways of the clock and status key.

Company Name: Input company name by related software.

9.2 Voice Settings





In the initial interface, press [M/OK] > Personalize > Voice to enter the Voice settings interface.

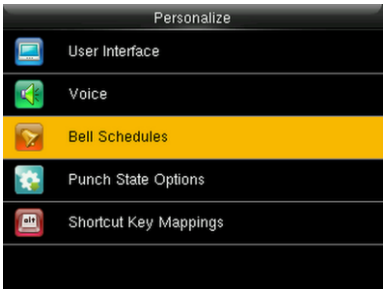
Voice Prompt: Select whether to enable voice prompts during operating, press [M/OK] to enable it.

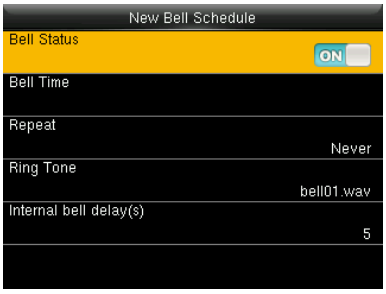
Keyboard Prompt: Select whether to enable keyboard voice while pressing keyboard, press [M/OK] to enable it.

Volume: Set the volume of device. Press ▶ key to increase the volume, press ◀ key to decrease the volume.

9.3 Bells Settings

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





In the initial interface, press [M/OK] > Personalize > Bell Schedules > New Bell Schedule to enter the New Bell Schedule adding interface.

Bell Status: [ON] is to enable the bell, while [OFF] is to disable it.

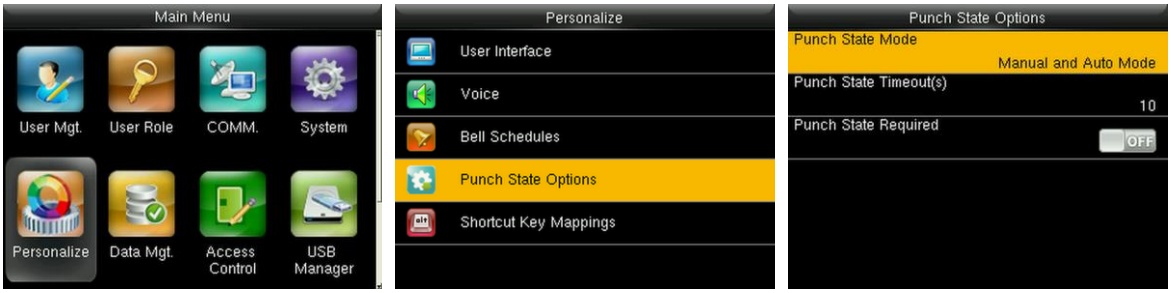
Bell Time: The bell rings automatically when reaching the specified time.

Repeat: To set whether to repeat the bell.

Ring Tone: Ringtone played for bell.

Interval bell delay (s): To set the ringing length. The value ranges from 1 to 999 seconds.

9.4 Punch States Settings



In the initial interface, press [M/OK] > Personalize > Punch State Options to enter the Punch State Options settings interface.

Punch State Mode: To choose the Punch State Mode, which includes the following modes:

1. Off: To disable the punch state key function. The punch state key set under Shortcut Key Mappings menu will become invalid.
2. Manual Mode: To switch the punch state key manually, and the punch state key will disappear after

   Punch State Timeout.
3. Auto Mode: After this mode is chosen, set the switching time of punch state key in Shortcut Key Mappings; when the switching time is reached, the set punch state key will be switched automatically.
4. Manual and Auto Mode: Under this mode, the main interface will display the auto-switching punch state key, meanwhile supports manually switching punch state key. After timeout, the manually switching punch state key will become auto-switching punch state key.
5. Manual Fixed Mode: After punch state key is manually switched, the punch state key will remain unchanged until being manually switched next time.
6. Fixed Mode: Only the fixed punch state key will be shown and it cannot be switched.

Punch State Timeout (s): The timeout time of the display of punch state. The value ranges from

5~999 seconds.

Punch State Required: Whether it is necessary to choose attendance state in verification.

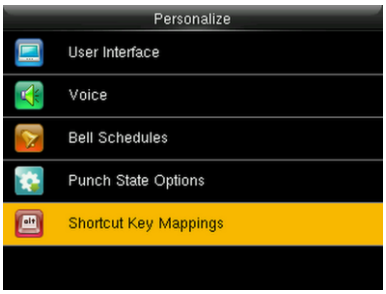
ON: Choosing attendance state is needed after verification.

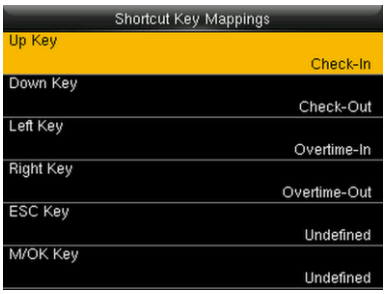
OFF: Choosing attendance state is not needed after verification.

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

9.5 Shortcut Keys Settings

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





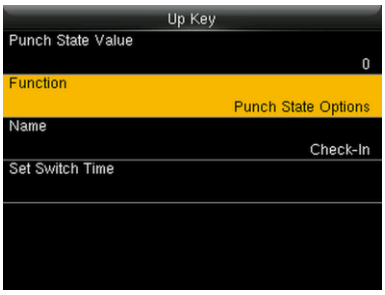
In the initial interface, press [M/OK] > Personalize > Shortcut Key Mappings to enter the Shortcut Key Mappings settings interface.

To Set (M/OK) as Duress Key: please refer to 7.7.1 Duress Key Settings

To set Auto Switching Time:

Choose any shortcut key, and select [Punch State Options] in [Function], so that auto switching time can be set.

Auto Switch: When the set time is reached, the device will switch the attendance state automatically.



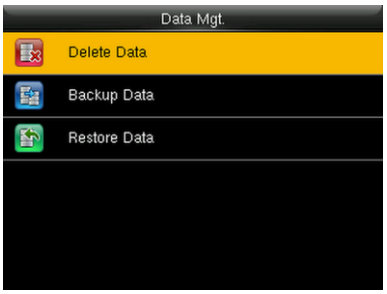
When the shortcut key is set to Punch State Key, but [OFF] mode is selected in the [Punch State

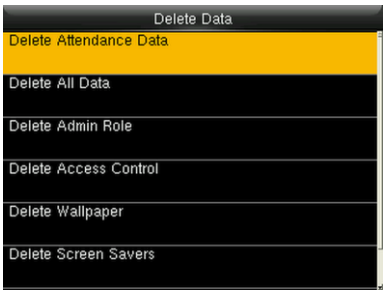
Mode] (Personalize > Punch State Options > Punch State Mode > Select OFF), then the shortcut key will not be enabled.

10 Data Mgt.

10.1 Deleting Data

To manage data in the device, which includes delete attendance data, delete all data, delete admin role and delete screen savers etc.





In the initial interface, press [M/OK] > Data Mgt. > Delete Data to enter the Delete Data settings interface.

Delete Attendance Data: To delete all attendance data in the device.

Delete All Data: To delete all user information, fingerprints and attendance logs etc.

Delete Admin Role: To make all Administrators become Normal Users.

Delete Access Control: To delete all access data.

Delete Wallpaper: To delete all wallpapers in the device.

Delete Screen Savers: To delete all screen savers in the device. (For details of uploading screen savers, please refer to 17.3 Image Uploading Rule.)

Delete Backup Data: To delete all backup data.

10.2 Data Backup

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

Backup to USB Disk

Insert the USB disk. In the initial interface, press [M/OK] > Data Mgt. > Backup Data > Backup to USB Disk > Backup Content > choose content to be backed up (Business Data / System Data) > Backup Start to start backup. Restarting the device is not needed after backup is completed.

Remarks: The operations of Backup to Device are the same as that of Backup to USB Disk.

10.3 Data Restoration

To restore the data in the device or U disk to the device.

Restore from USB disk

Insert the USB disk. In the initial interface, press [M/OK] > Data Mgt. > Restore Data > Restore from USB Disk > Content > choose content to be restored (Business Data / System Data) > Start Restore > select Yes to start restoring. After restoration completes, click [OK] to automatically restart the device.

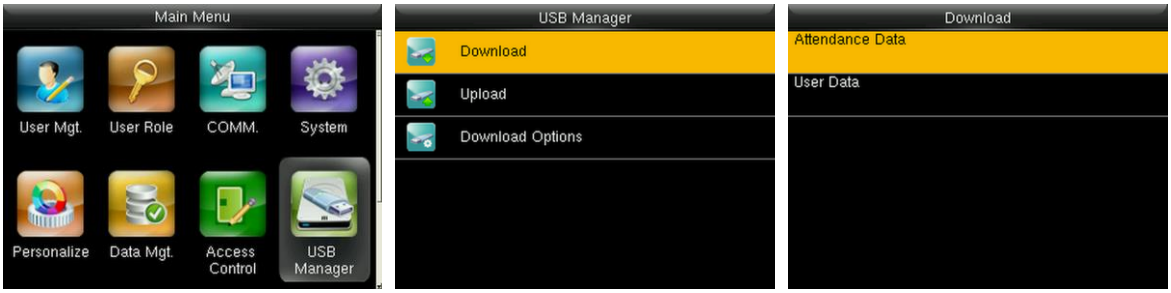
Remarks: The operations of Restore from Device are the same as that of Restore from USB Disk.

11 USB Manager

Upload or download data between device and the corresponding software by USB disk.

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

11.1 USB Download

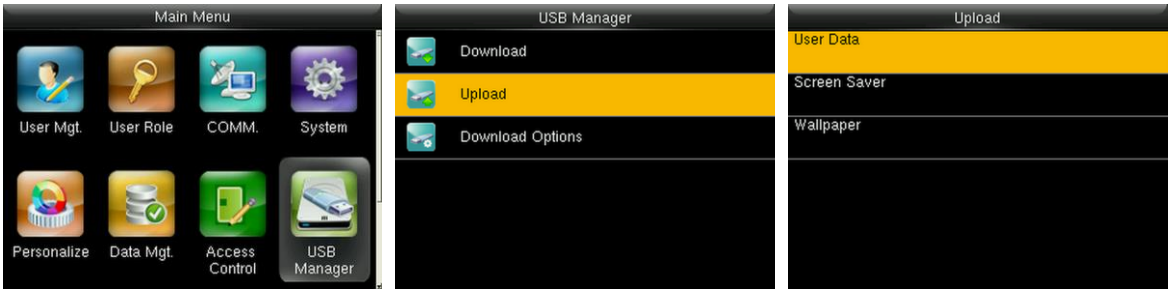


In the initial interface, press [M/OK] > USB Manager > Download to enter the USB Download interface. Time period is required to choose only in downloading Attendance Data.

Attendance Data: To download attendance data in specified time period into USB disk.

User Data: To download all user information and fingerprints from the device into USB disk.

11.2 USB Upload



In the initial interface, press [M/OK] > USB Manager > Upload to enter the USB Upload interface.

User Data: To upload all the user information and fingerprints from USB disk into the device.

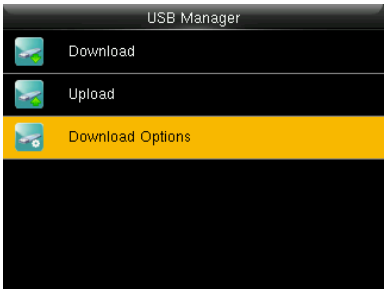
Screen Saver: To upload all screen savers from USB disk into the device. You can choose [Upload selected picture] or [Upload all pictures]. The images will be displayed on the device's main interface after upload (for the specifications of screen savers, please

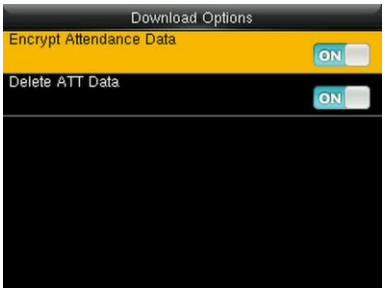
refer to 17.3 Image Uploading Rule).

Wallpaper: To upload all wallpapers from USB disk into the device. You can choose [Upload selected picture] or [Upload all pictures]. The images will be displayed on the screen after upload (for the specifications of wallpapers, please refer to 17.3 Image Uploading Rule).

11.3 Download Options Settings

To encrypt attendance data in the USB disk or delete attendance data.





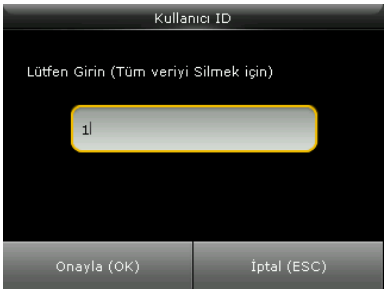
In the initial interface, press [M/OK] > USB Manager > Download Options to enter the Download Options settings interface.

Press [M/OK] to enable or disable the [Encrypt Attendance Data] and [Delete ATT Data] options.

Remarks: The encrypt attendance data can only be imported in the software of Access 3.5 .

12 Attendance Search

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

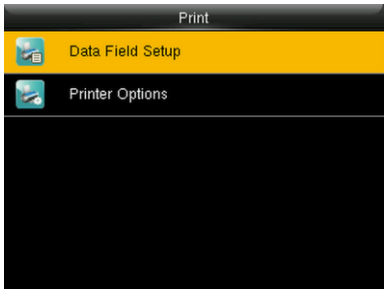


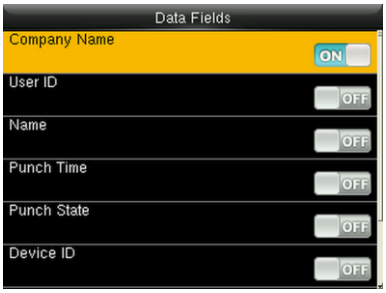
In the initial interface, press [M/OK] > Attendance Search > enter User ID (if no ID is entered, all user records will be searched) > select Time Range > press [M/OK], the corresponding attendance logs will then be shown.

13 Print Settings★

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

13.1 Print Data Field Settings

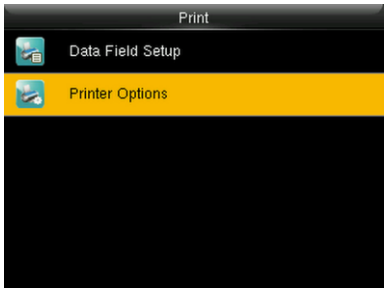


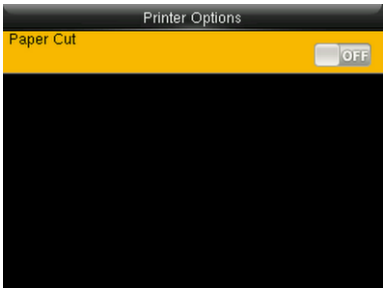


In the initial interface, press [M/OK] > Print > Data Field Setup > press [M/OK] to turn on / off the fields needing to be printed.

Remarks: In printing, the fields position of the information can be adjusted by the left / right key: press left key to move to the previous item, and press right key to move to the next item.

13.2 Print Options Settings



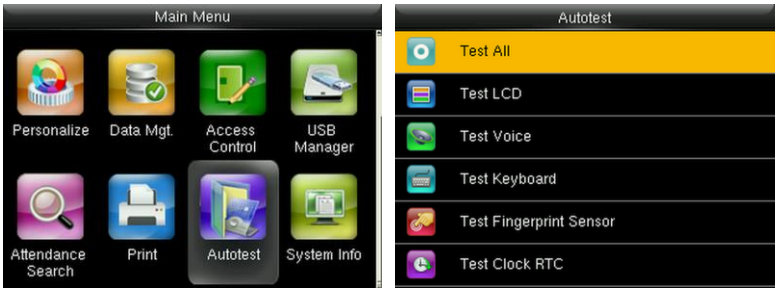


In the initial interface, press [M/OK] > Print > Printer Options > press [M/OK] to turn on / off the Paper Cut function.

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

14 Autotest

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



In the initial interface, press [M/OK] > Autotest to enter the Autotest interface.

Test All: To test LCD, voice, keyboard, fingerprint sensor, camera and RTC. During the test, press [M/OK] to continue to the next test, while press [ESC] to exit the test.

Test LCD: To test the display effect of LCD screen by displaying full color, pure white, and pure black to check whether the screen displays colors properly. During the test, press [M/OK] to continue to the next test, while press [ESC] to exit the test.

Test Voice: The device automatically tests whether the voice files stored in the device are complete and the voice quality is good. During the test, press [M/OK] to continue to the next test, while press [ESC] to exit the test.

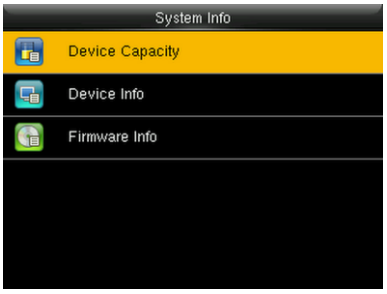
Test Keyboard: To test all keys to see if every key functions properly. Press any key in the Keyboard testing interface; if the pressed key is consistent with the key sign shown on the screen, then the key functions properly. Press [M/OK] or [ESC] to exit the test.

Test Fingerprint Sensor: To test the fingerprint sensor by pressing fingerprint to check if the collected fingerprint image is clear. When pressing fingerprint on the sensor, the image will be displayed on the screen. Press [M/OK] or [ESC] to exit the test.

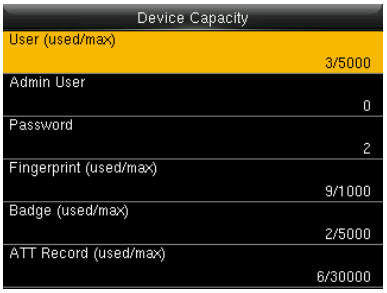
Test Clock RTC: To test the Real-Time Clock. The device tests whether the clock works properly and accurately by checking the stopwatch. Press [M/OK] to start counting time, and press it again to stop counting, to see if the stopwatch counts time accurately. Press [ESC] to exit the test.

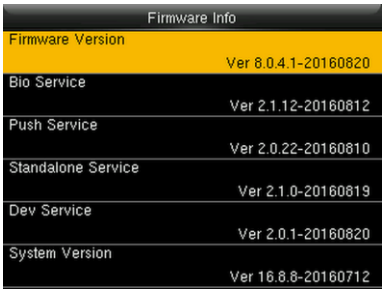
15 System Information

Check data capacity, device and firmware information.



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





Device Capacity Device Info Firmware Info

Device Capacity: To display the number of registered users, administrators, passwords, fingerprints, badges, attendance logs, also to check the total storage of users, fingerprints, badges and attendance records.

Device Info: To display the device name, serial number, MAC address, fingerprint algorithm, platform information, manufacturer and manufacturer date.

Firmware Info: To display the firmware version, Bio service, push service, standalone service and Dev service.

Remarks: The display of Device Capacity, Device Info and Firmware Info on the system information interface of different products may vary; the actual product shall prevail.

16 Troubleshooting

- Fingerprint sensor is not able to read and verify the fingerprint effectively.
  - Check whether the finger is wet, or the fingerprint sensor is wet or dusty.
  - Clean the finger and the fingerprint sensor and try again.
  - If the finger is too dry, blow air onto it and try again.

- "Invalid time zone" is displayed after verification.
  - Contact Administrator to check if the user has the privilege to gain access within that time schedule.

- Verification succeeds but the user cannot gain access.
  - Check whether the user privilege is set correctly.
  - Check whether the lock wiring is correct.

- The Tamper Alarm rings.
  - Check whether the device and the back plate is fixed together; if not, the tamper switch on the back of the device will be triggered and raises an alarm,  will be shown on the top right corner on the interface. Only when [Speaker Alarm] (Access Control > Access Control Options > Speaker Alarm) is [ON] will the speaker raise an alarm.

17 Appendices

17.1 Specifications

Fingerprint Capacity	1000
Badge Capacity	5000
ATT Record Capacity	30,000
Screen	2.4 inch TFT LCD
LED indicator	Red / Green
Communication ways	Ethernet (10/100M), RS232, RS485, USB-Host, WIFI
Wiegand Signal	Wiegand In / Wiegand Out
Recognition Speed	≤ 2 sec
FAR	≤ 0.0001%
FRR	≤ 1%
Work Temperature	0 ~ 45℃
Power	12V / 3A
Voltage	12V
Current	3A
Access Control Ports	Lock, Alarm, Exit Button, Reader and Door Sensor

17.2 Wiegand Introduction

Wiegand26 Protocol is a standard protocol on access control developed by the Access Control Standard Subcommittee affiliated to the Security Industry Association (SIA). It is a protocol used for contactless IC card reader port and output.

The protocol defines the port between the card reader and controller which are widely used in access control, security and other related industries. This has standardized the work of card reader designers and controller manufacturers. The access control devices produced by our company also apply this protocol.

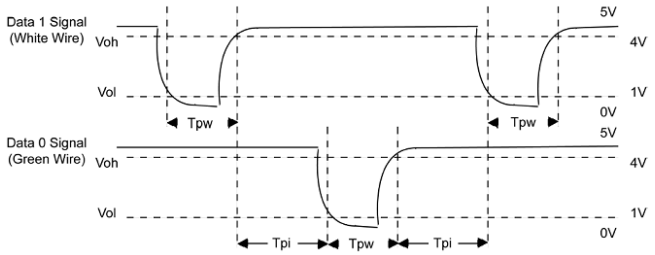
Digital Signal

Figure 1 shows the sequence diagram of the card reader sending digital signal in bits to the access controller. The Wiegand in this diagram follows the SIA access control standard protocol, which targets at 26-bit Wiegand card reader (with a pulse time within 20us to 100us and pulse hopping time within 200us and 20ms). Data1 and Data0 signals are high level (greater than Voh) until the card reader is ready to send a data stream. The card reader send out asynchronous low level pulse (less than vol), transmitting data stream via Data1 or Data0 wire to access control box (as the sawtooth wave in figure 1). Data1 and Data0 pulses do not overlap or synchronize. Figure 1 shows the maximum and minimum pulse width (successive pulses) and pulse hopping time (the time between two pulses) allowed by the F series fingerprint access control terminals.

Table1: Pulse Time

Sign	Definition	Card Reader Typical Value
Tpw	Pulse Width	100 μs
Tpi	Pulse Interval	1 ms

Figure1: Sequence Diagram



17.3 Image Uploading Rule

1. **User photo★:** It is required to create a file named as "photo" under the USB disk file, and put user photos into the file. The capacity is 8000 images (considering the actual capacity of the device, it is suggested to upload 5000 images at most), with each of them not exceeding 15k. The image name is x.jpg (x is the actual user ID, max. 9 digits). The photo format must be JPG.
2. Advertising image: It is required to create a file named as "advertise" under the USB disk file, and put advertising images into the file. The capacity is 20 images with each of them not

exceeding 30k. Image name and format are not restricted.

3. Wallpaper: It is required to create a file named as "wallpaper" under the USB disk file, and put wallpapers into the file. The capacity is 20 images with each of them not exceeding 30k. Image name and format are not restricted.

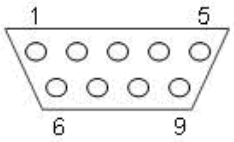
Note: When each user photo and attendance photo does not exceed 10k, the device can save a total number of 10000 user and attendance photos (considering the actual capacity of the device, it is strongly suggested to upload 5000 user and attendance photos at most).

17.4 Printing Function★

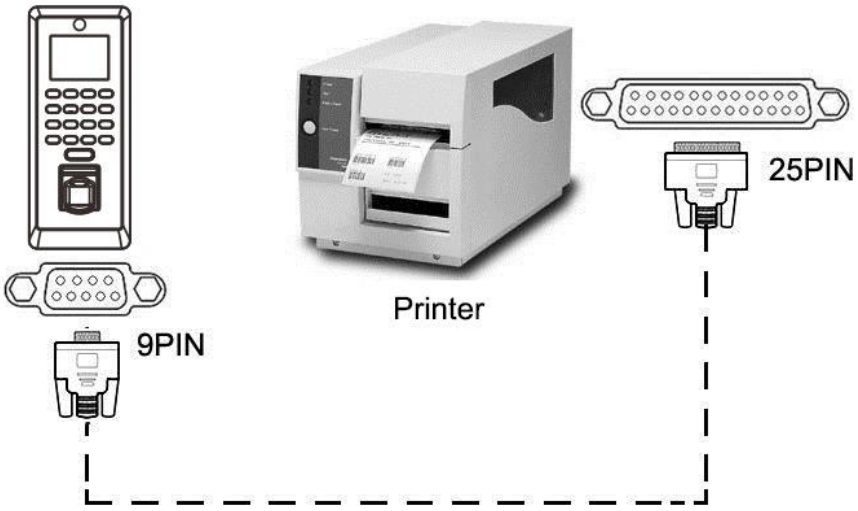
Remarks: Only some models support printing function.

Function Instruction

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

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

[Connection Diagram]



[Operation]

1. In the initial interface, press [M/OK] > Comm. > Serial Comm > Baudrate, and choose 19200 as the baud rate.

2. In the initial interface, press [M/OK] > Print. To set the printing format and parameters, please refer to 13 Print Settings★.

Note:

1. The baud rate of the device and printer (hyper terminal) should be consistent.

2. If the default printing format is not satisfactory, you may contact our company to customize other formats.

17.5 Statement on Human Rights and Privacy

Dear Customers:

Thank you for choosing the hybrid biometric products designed and manufactured by us. As a world-renowned provider of biometric technologies and services, we pay much attention to the compliance with the laws related to human rights and privacy in every country while constantly performing research and development.

We hereby make the following statements:

1. All of our fingerprint recognition devices for civil use only collect the characteristic points of fingerprints instead of the fingerprint images, and therefore no privacy issues are involved.
2. The characteristic points of fingerprints collected by our products cannot be used to restore the original fingerprint images, and therefore no privacy issues are involved.
3. We, as the equipment provider, shall not be held legally accountable, directly or indirectly, for any consequences arising due to the use of our products.
4. For any dispute involving the human rights or privacy when using our products, please contact your employer directly.

Our fingerprint products for police use, or development tools support the collection of the original fingerprint images. As for whether such a type of fingerprint collection constitutes an infringement of your privacy, please contact the government or the final equipment provider. We, as the original equipment manufacturer, shall not be held legally accountable for any infringement arising thereof.

The law of the People's Republic of China has the following regulations regarding the personal freedom:

1. Unlawful arrest, detention or search of citizens of the People's Republic of China is prohibited; infringement of individual privacy is prohibited.
2. The personal dignity of citizens of the People's Republic of China is inviolable.
3. The home of citizens of the People's Republic of China is inviolable.
4. The freedom and privacy of correspondence of citizens of the People's Republic of China are protected by law.

At last we stress once again that biometrics, as an advanced recognition technology, will be applied in a lot of sectors including e-commerce, banking, insurance and legal affairs. Every year people around the globe suffer from great loss due to the insecurity of passwords. The biometric products actually provide adequate protection for your identity under a high security environment.

17.6 Environment-Friendly Use Description

- The Environment Friendly Use Period (EFUP) marked on this product refers to the safety period of time in which the product is used under the conditions specified in the product instructions without leakage of noxious and harmful substances.
- The EFUP of this product does not cover the consumable parts that need to be replaced on a regular basis such as batteries and so on. The EFUP of batteries is 5 years.

Names and Concentration of Toxic and Hazardous Substances or Elements

Parts Name	Toxic and Hazardous Substances or Elements					
	Pb	Hg	Cd	Cr6+	PBB	PBDE
Chip resistor	×	○	○	○	○	○
Chip capacitor	×	○	○	○	○	○
Chip inductor	×	○	○	○	○	○
Chip diode	×	○	○	○	○	○
ESD components	×	○	○	○	○	○
Buzzer	×	○	○	○	○	○
Adapter	×	○	○	○	○	○
Screws	○	○	○	×	○	○

○: Indicates that this toxic or hazardous substance contained in all of the homogeneous materials for this part is below the limit requirement in SJ/T11363-2006.

×: Indicates that this toxic or hazardous substance contained in at least one of the homogeneous materials for this part is above the limit requirement in SJ/T11363-2006.

Note: 80% of the parts in this product are manufactured with non-hazardous

environment-friendly materials. The hazardous substances or elements contained cannot be replaced with environment-friendly materials at present due to technical or economical constraints.