

Black-and-White Screen Series Standalone Access Controller and Reader User Manual (Professional Version)

Version: 1.0

Date: Nov. 2012

About This Manual

This manual introduces the interface and menu operations of The Black-and-White Screen Series Standalone Access Controller and Reader, bundled Access3.5 Security System are used together. For the product installation, see related installation guide.

Contents

1. Notice for Use.....	1
2. Basic Concepts.....	3
2.1 User Enrollment.....	3
2.2 User Verification.....	3
2.3 User ID.....	3
2.4 Authority Classes.....	3
2.5 Appearance of Device.....	4
3. Enrollment and Verification.....	5
3.1 Enroll a User.....	5
3.1.1 Enroll Fingerprint.....	5
3.1.2 Backup Enrollment.....	6
3.1.3 Enroll Password.....	7
3.1.4 Enroll ID Card.....	8
3.2 Prompts for Successful Enrollment.....	9
3.3 Verification Modes.....	10
3.3.1 Fingerprint Verification.....	10
3.3.2 Password Verification.....	11
3.3.3 Verification Through Card Swiping★.....	12
3.4 Administrator Enrollment.....	12
3.5 Delete Enrollment Data.....	13
4. Settings.....	14
4.1 System Settings.....	14
4.1.1 Time Settings.....	14
4.1.2 Languages★.....	15
4.1.3 Date Format.....	15
4.1.4 Advanced Settings.....	15
4.2 Power Management★.....	17
4.3 Communication-related Settings.....	17
4.4 Access Options★.....	18
4.4.1 Lock.....	18
4.4.2 DSen. Delay.....	18
4.4.3 DSen. Mode.....	18
4.4.4 485Reader★.....	19
4.4.5 Master State★.....	20
4.4.6 Verify Mode.....	20
4.5 Automatic Test.....	20
5. USB Pen Drive Management★.....	21
5.1 Download Attendance Data.....	21
5.2 Download User Data.....	21
5.3 Upload User Data.....	22

Contents

6. Systems Information	23
7. Turn Off Alarm ★	24
8. Maintenance	25
9. FAQs	26
10. Appendix	28
10.1 USB.....	28
10.2 Scheduled Bell.....	28
10.3 External Connection with the Fingerprint Reader.....	29
10.4 Modem.....	29
10.5 GPRS Functions.....	32
10.6 WIFI Functions.....	32
10.7 Attendance Query.....	32
10.9 MP3 Function Description.....	33
10.10 Short Message.....	34
10.11 Multiple Verification Modes.....	35
10.12 EM Read-only Card, HID Card, Mifare Card, iClass Card.....	38
10.13 Master-slave function ★.....	39
10.14 Remote Identification Server (RIS).....	41
10.15 Web Server Access Control.....	43
10.16 Automatic IP Address Collection.....	43
10.17 Wiegand Protocol.....	43
10.18 Soap Interface.....	46
10.19 POE Function.....	47
10.20 Backup Battery (Mini-UPS).....	48
10.21 9-digit Enrollment Number.....	49
10.22 Automatic Time Calibration.....	50
10.23 Daylight Saving Time (Time Zone Settings).....	50
10.24 Play Voice within Specified Time Segment (By Time Segment or Group).....	51
10.25 Work Code.....	52
10.26 DHCP.....	53
10.27 User Grouping.....	53
10.28 T9 Input Method.....	55
10.29 TTS Function.....	55
10.30 Statement on Human Rights and Privacy.....	56
10.31 Environment-Friendly Use Description.....	57

1. Notice for Use

Thank you for using our Black-and-White (B&W) Screen Series Standalone Access Controller and Reader Products. Please read this manual carefully before using this product for a comprehensive understanding so as to avoid causing unnecessary damages to the product.

Protect the device from exposure to direct sunlight or strong beam as strong beam greatly affects the fingerprint collection and leads to fingerprint verification failure.

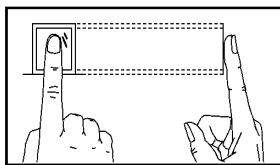
Avoid using the product outdoors in summer. The working temperature of B&W screen series ranges from 0–40°C. The heat dissipated during long-term operation may easily lead to response slowdown and verification pass rate decrease. It is recommended to use sunshades and heat sink devices for protection of the product at outdoors. We recommend you to use the device properly so as to achieve the optimal recognition effect and verification speed.

1. Recommended fingers

Recommended fingers: The index finger, middle finger or the ring finger; the thumb and little finger are not recommended (because they are usually clumsy on the fingerprint collection screen).

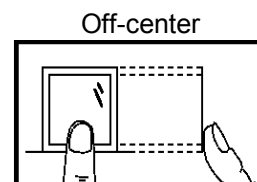
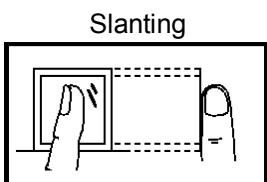
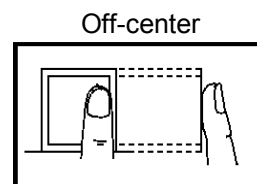
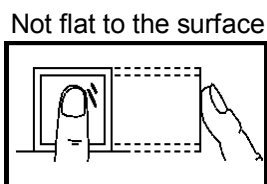
2. Fingers Placement

1) Proper finger placement:



The finger is flat to the surface and centered in fingered guide.

2) Improper finger placement:



☺ **Note:** Please enroll and verify your fingerprint by using the proper finger placement mode to avoid degradation of verification performance due to improper operations.

3. LED Colors and Their Meanings

Works normally: The green LED blinks once every other second.

Verification fails: The red LED is solid on for 3 seconds.

Verification succeeds: The green LED is solid on for 3 seconds.

 **Note:** If the LED display is inconsistent with the above conditions, please contact our technical personnel.

4. About This Manual

- Our products are subject to update from time to time, so our company will neither make a commitment to guarantee the consistency between the actual products and this document, nor assume any responsibility for any dispute arising out of the discrepancy between the actual technical parameters and this manual. This document is subject to change without prior notice.
- The functions marked with ★ in this manual are optional for some B&W screen series standalone access controller and reader products. Please refer to the actual product for the specific function description.
- Picture descriptions in this manual may vary slightly from actual product. Please refer to the actual product for exact descriptions.
- Reserve the rights to change and interpret by our company.

2. Basic Concepts

This section introduces the definitions and descriptions of the following basic concepts:

- User enrollment
- User verification
- User ID
- Authority class
- Appearance of device

The most important two functions supported by user enrollment and verification.

2.1 User Enrollment

A user can enroll up to 10 different fingerprints using one ID number to have multiple verification selections.

Theoretically all the fingers of a user need to be enrolled so that the user can use any of the enrolled fingerprints for recognition even if he/she forgets which fingerprint has been enrolled.

Generally it is recommended that a user shall enroll at least two fingerprints, for example, the index fingers of both hands, so that the user can still perform fingerprint matching even if one or more of his/her fingers get cut or damaged.

2.2 User Verification

When a user scans his/her fingerprint on the fingerprint reader(1:N), or enters a password / placing his/her finger after entering an ID number(1:1), the device compares the newly scanned fingerprint with a fingerprint stored in template. The fingerprint template is used to check the user ID. Upon verification, the system displays a prompt about whether the verification succeeds or not and then stores the successful matching record in the device.

2.3 User ID

When enrolling fingerprints, a user will be allocated with an unused ID. When the user starts to verify his/her identity, this ID is used to associate the fingerprint feature template or password.

You can enter the ID through the mini keyboard or other storage means, for example, the RF card (the fingerprint recognition device must be configured with the RF card reader).

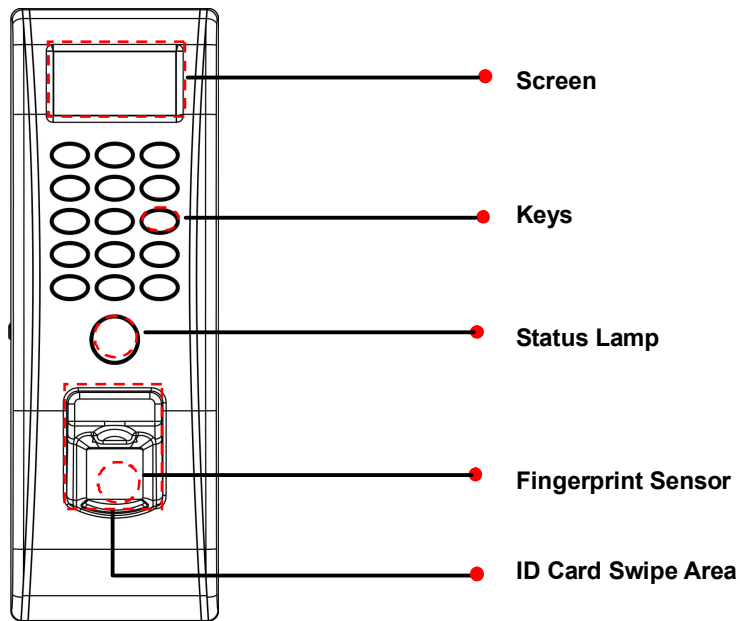
2.4 Authority Classes

The B&W Screen Series Standalone Access Controller and Reader products have two authority classes:

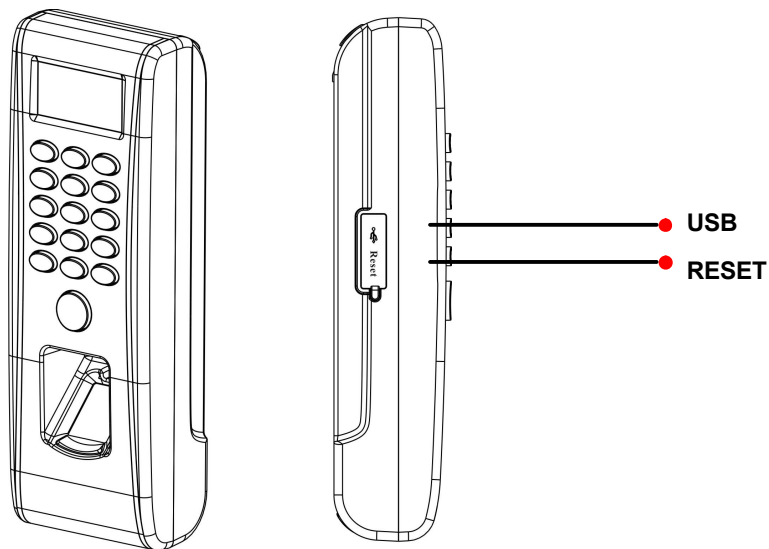
- Users: refer to those who are required to verify their identity for a purpose, for example, opening the door or keeping their entry/exit records.
- Administrators: Having all the privileges grants to ordinary users, and access to the main menu for various operations.

2.5 Appearance of Device

Front View:

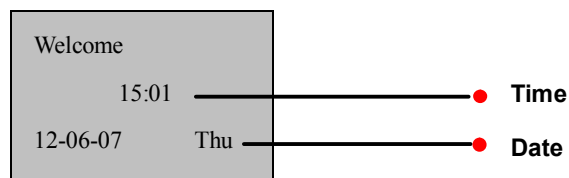


Side View:



Initial Interface:

The first interface displayed on the screen upon equipment power-on is referred to as the “Initial Interface”, as shown in the following figure.



3. Enrollment and Verification

This chapter introduces how to enroll users on the B&W Screen Series Standalone Access Controller and Reader Products. Further, it describes how to verify the validity of enrolled fingerprints.

This chapter includes the following parts:

- ✧ Enroll users
- ✧ Enroll backup fingerprints
- ✧ Prompts for successful enrollment
- ✧ Verify identity.
- ✧ Administrator enrollment
- ✧ Delete enrollment data

😊 **Note:** To enroll a new user, you must have the authority of administrator. For details, see [2.4 Authority Classes](#).

3.1 Enroll a User

The B&W Screen Series Standalone Access Controller and Reader Products supports three enrollment modes: Fingerprint enrollment, Password enrollment and RFID enrollment.

If no administrator has been enrolled, any user has the right to enroll a new user.

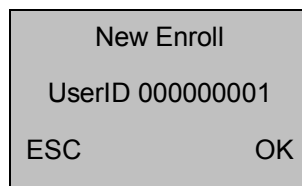
If an administrator has already been enrolled, that you enroll a new user, need to verify the administrator identity firstly by pressing MENU. The system then prompts you to press your finger or enter a password or swipe card for administrator verification.

😊 **Note:**

1. If you want to clear the administrator Privilege, please click on "Setting" -- "Advanced Settings" to select.
2. Verify Type is fingerprint or swipe card by default, so if you registration, choose enroll fingerprint or card is the best.
3. To ensure device security, it is recommended to set an administrator when using the terminal initially.

3.1.1 Enroll Fingerprint

1) Select **Menu** → **User Manage** → **User Enrollment** to display the [User Enrollment] interface. Select [Enroll FP] and press **OK** to display the [Enroll FP] interface.



2) Input a number (from 1-99999999) in the [User ID]. Press **OK** to display the fingerprint enrollment interface.

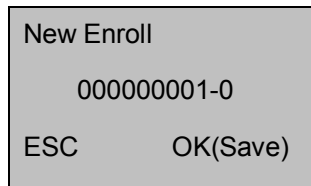


 Note:

The last digit “0” in “000000001-0” denotes the first fingerprint. “000000001-1” the last digit “1” denotes the second fingerprint, means backup fingerprint.

The device displays 9-digit numbers, and automatically adds 0 as prefix to the numbers less than 9 digits. For example, if you input "11", the device will display "000000011".

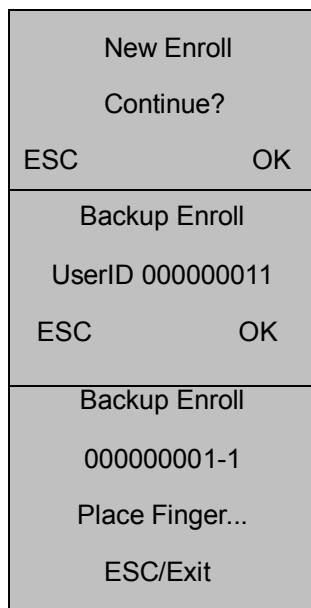
3) Place the same finger for three consecutive times on the fingerprint reader according to system prompts. If the enrollment succeeds, the following information is displayed:



4) Press **OK** to save the enrolled fingerprint. If the enrollment fails, the system will prompt you to re-enter your user ID and restart the enrollment from Step 2.

3.1.2 Backup Enrollment

If you press **ESC** on the [New Enroll] interface, you can cancel the new enrollment and display the [Backup Enroll] interface, press **OK** and then as shown in the following figure:



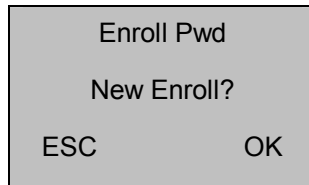
The following steps of backup enrollment are the same with those of new enrollment.

😊 **Note:**

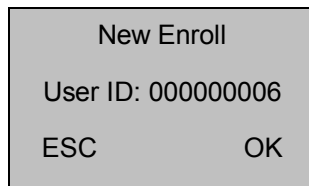
It is recommended that a long-term user should enroll two fingerprints at least. Backup registration can choose fingerprint or password or card.

3.1.3 Enroll Password

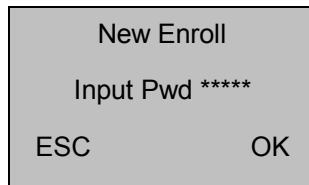
1) Select **Menu** → **User Manage** → **User Enrollment** to display the [User Enrollment] interface. Select [Enroll Pwd] and press **OK** to display the [Enroll Pwd] interface.



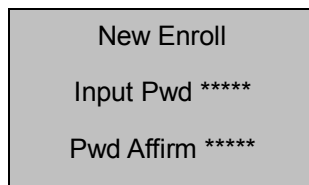
2) Press **OK** to confirm and proceed.



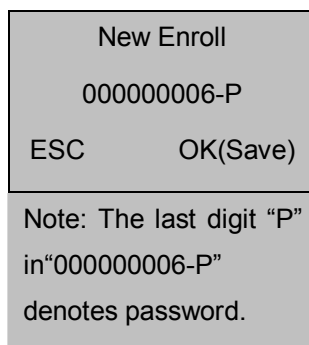
3) Input a number (from 1–99999999) in the [User ID] field. Press **OK** to display the password input interface.



4) Input your password in the [Input Pwd] field and press **OK** to proceed.



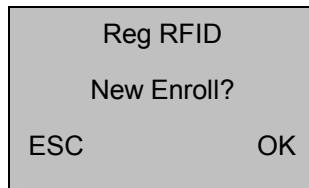
5) Re-enter your password in the [Pwd Affirm] field and press **OK** to confirm your entry and proceed.



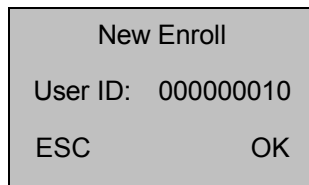
6) Press **OK** to save the enrolled data and exit the password enrollment. Press **ESC** to entry modification password interface,the following steps are the same with those of new password enrollment.

3.1.4 Enroll ID Card

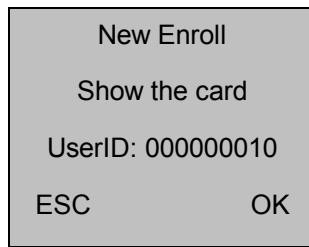
1) Select **Menu** → **User Manage** → **User Enrollment** to display the [User Enrollment] interface. Select [Reg RFID] and press **OK** to proceed.



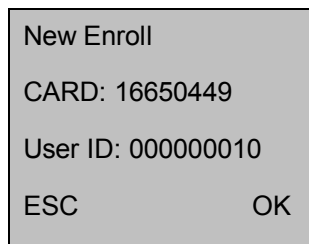
2) Press **OK** to confirm and proceed.



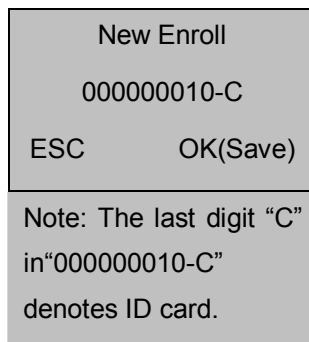
3) Input a number (from 1–999999999) in the [User ID] field. Press **OK** to display the ID card enrollment interface.



4) Swipe your card and the system reads your card number.



5) Press **OK** to confirm and proceed.



6) Press **OK** to save the enrolled data and complete the ID card enrollment. Press **ESC** to entry modification ID number interface.

😊 **Note:** HID Card or Mifare Card is an optional function. If you want to customize, please consult our commercial representatives or pre-sale technical support engineers.

3.2 Prompts for Successful Enrollment

A registered fingerprint with high quality assures quick verification speed while the one with poor quality may easily lead to false rejection and slow verification.

To enhance the quality of enrolled fingerprints, refer to Table 3-1

Table 3-1 Common Causes of Enrollment Failure or Poor Fingerprint Quality

Finger is too dry or dirty	Rub your fingers against your palm because rubbing yields oil. Moisturize your finger by breathing on it.
Apply insufficient pressure	Apply pressure lightly and evenly during the capturing process.
Select fingers for enrollment	Left and right index fingers or middle fingers are recommended. Select the fingers without worn-out or damaged fingerprints. Users usually select their index fingers, but if their index fingers do not have high fingerprint quality, they can select their middle fingers or ring fingers. For users with small fingers, they can opt for their thumbs. To enroll spare fingerprints, users can select fingers not prone to wear-out or damage, for example, the ring fingers.
Finger placement	Press your finger flatly on the fingerprint sensor and be sure that the pad (not the tip) covers as much of the sensor window as possible. Do not press your finger perpendicular to the fingerprint sensor; do not knock your finger on the sensor quickly; keep your finger still.
Impact of the fingerprint image change	The change of fingerprint image due to skin peeling-off or injury will affect the verification performance. If the fingerprint quality of a user is poor due to the skin peeling-off and the user cannot pass the verification one week later, the user needs to re-enroll his/her fingerprint or adopt the password verification mode.
Other causes	There may be a small amount of people who cannot pass the verification no matter how hard they try due to very poor fingerprint quality. In that case, you can adopt the ID + fingerprint verification mode, duly lower the 1: 1 match threshold or adopt the password verification mode.

3.3 Verification Modes

After enrollment, you can verify validity that registered fingerprints or ID card or password on the initial interface.

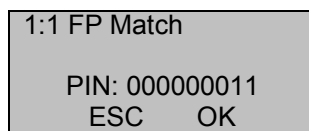
3.3.1 Fingerprint Verification

1:1 and 1: N matching modes for fingerprint identification.


(1) 1:1 fingerprint matching

In the 1:1 fingerprint matching mode, the device compares the current fingerprint collected through the fingerprint reader with that in relation to the user ID entered through keyboard.

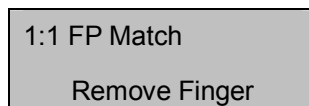
Operation steps:



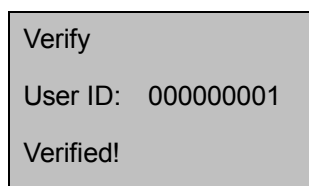
Enter a user ID through keyboard on the initial interface.

 **Note:** If the user have been registered password, press **OK** in the verification, it will automatically enter the password verification interface. If have not, it will can enter the fingerprint verification interface.

We suggest users in the use of 1:1 fingerprint comparison, directly press fingerprint, do not press **OK** button.

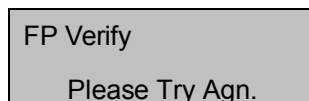


And then, directly place your finger on the fingerprint reader to display the following interface:



If the verification succeeds, the system will generate a voice announcement "Thank you!" .

After the above interface is displayed about 0.5 seconds, and then the following interface will be displayed:



If the verification fails, the system will generate a voice announcement "Please try again!" and display the following interface:

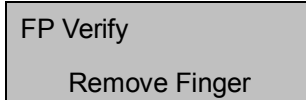
After the above interface is displayed 0.5 seconds, the system will return to the initial interface.

(2) 1: N fingerprint verification

In the 1: N fingerprint matching mode, the device compares the current fingerprint collected through the fingerprint reader with all the fingerprints stored in the device.

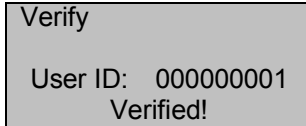
3. Enrollment and Verification

Operation steps:



FP Verify
Remove Finger

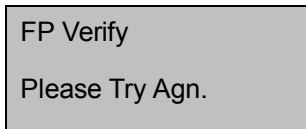
Place your finger on the initial interface to display the following interface:



Verify
User ID: 000000001
Verified!

If the verification succeeds, the system will generate a voice announcement “Thank you!” after the above interface is displayed about 0.5 seconds, and then the following interface will be displayed:

If the verification fails, the system will generate a voice announcement “Please try again!” and display the following interface:

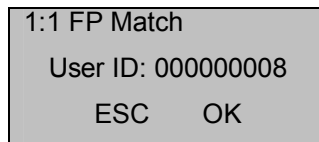


FP Verify
Please Try Agn.

After the above interface is displayed 0.5 seconds, the system will return to the initial interface.

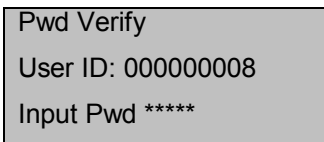
3.3.2 Password Verification

Input your ID Number on the initial interface.



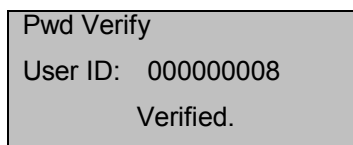
1:1 FP Match
User ID: 000000008
ESC OK

Press **OK** and the system displays a prompt message “Verified!”



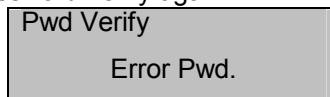
Pwd Verify
User ID: 000000008
Input Pwd *****

Input a correct password and press **OK** to confirm your entry.



Pwd Verify
User ID: 000000008
Verified.

If you enter a wrong password, the system displays “Error Pwd” as shown below and returns to the password input interface, you should proceed password verify again.



Pwd Verify
Error Pwd.

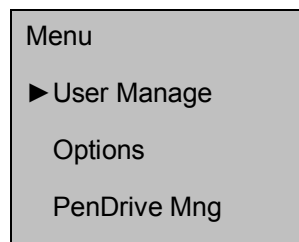
3.3.3 Verification Through Card Swiping★

If you have your ID card number enrolled in the system, you can pass the verification by swiping your ID card at the swiping area in a proper way.

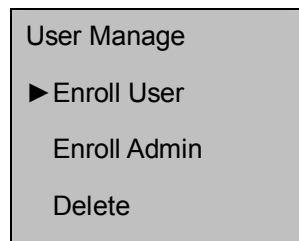
3.4 Administrator Enrollment

The B&W Screen Series Standalone Access Controller and Reader Products provide administrator settings to prevent unauthorized users changing system data and ensure system security. The operations on administrator settings are as following:

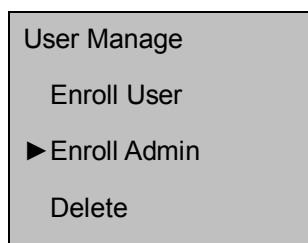
1) The brand new device does not assign any administrator, so you can press **Menu** to access the system directly and the following interface is displayed.



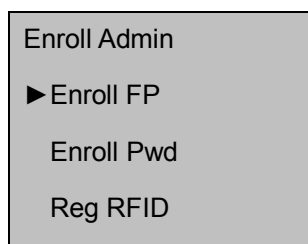
2) Press **OK** to display the [User Manage] interface.



3) Select **Enroll Admin** through the ▲/▼ key.



4) Press **OK** to display the [Enroll Admin] interface.

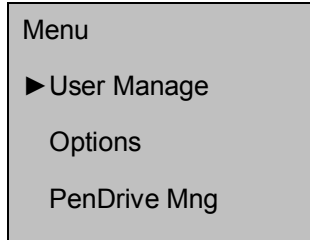


5) Select an enrollment mode and press **OK** to display the administrator enrollment interface. The enrollment mode of administrator is consistent with that of a new enrolled user. For details, see 3.1.1 [Enroll a User](#).

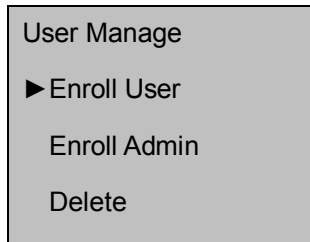
3.5 Delete Enrollment Data

To delete an enrolled user from the system, perform as follows:

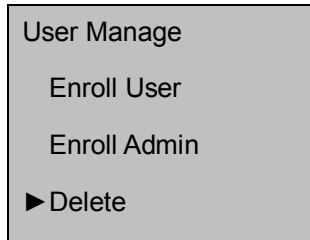
- 1) Press **Menu** to access related menu item for verification, and the following interface is displayed:



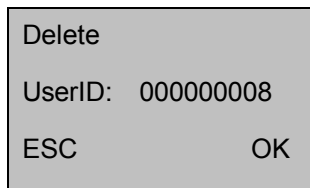
- 2) Press **OK** to display the [User Manage] interface.



- 3) Select **Delete** through the ▲/▼ key.



- 4) Press **OK** to display the [Delete] interface.

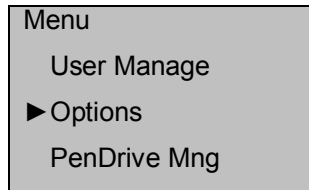


- 5) Enter a number in the [User ID] field and press **OK** to confirm your entry. Then delete the user according to system prompt.

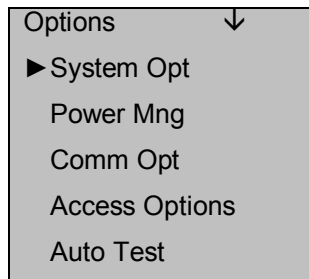
😊 **Note:** About deleting the Administrator Privilege and Clear All Data, you can press "Menu"-- "Options" -- "Syms Opt" -- "Adv option"-- "Clr Admin' Pri" or "Clear All Data". For detail, please refer to "[4.1.4Advanced Settings](#)". Besides, you can also through *Access3.5 Security System* to delete data.

4. Settings

Press **Menu** on the initial interface. After verifying your administrative rights, the system displays the following interface.



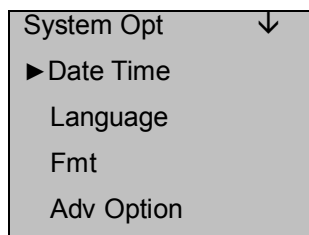
Select **Options** and press **OK** to proceed.



The **Options** menu contains five submenus: **System Opt**, **Power Mng**, **Comm Opt**, **Access Options** and **Auto Test**. These submenus will be described in the following parts.

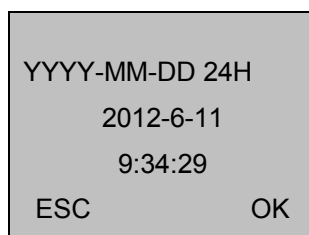
4.1 System Settings

Select **System Opt** and the information displayed on the screen are shown in the following figure:




4.1.1 Time Settings

Set the current date and time displayed on the device screen. Select **Set Date Time** and press **OK** to display the following interface.

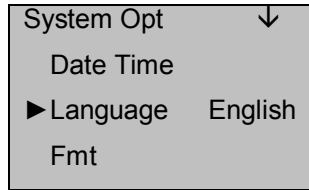


To modify date and time, place the cursor to the desired field through the **▲/▼** key, input correct date and time, and press **OK** to save the changes.


 **Note:** For some type of devices, you need to press Menu key about 3seconds for confirm.

4.1.2 Languages★

You can set the language displayed on the device screen. Select **Language** and press **OK** to display the language editing interface. If you select **English**, the information on screen will be displayed in English.



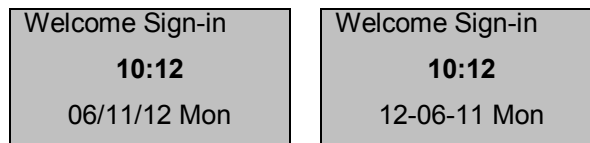
You can change the types of languages through the ▲/▼ key. Select a desired language and press **OK**. Then press **ESC** to exit the [System Opt] interface. When prompted to save your settings, press **OK** to save the settings. The system prompts you that your settings will take effective after the restart of your device.

 **Note:** Language selection is a non-standard function. If you need this function, please consult our commercial representatives or pre-sales technical support engineers.

4.1.3 Date Format

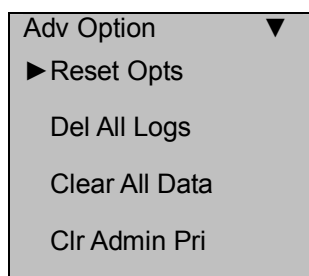
You can set the date format displayed on the device screen. Select **Format** and press **OK** to display the format setting interface. Select a desired date format through the ▲/▼ key. The device supports 10 date formats: YY-MM-DD, YY/MM/DD, YY.MM.DD, MM-DD-YY, MM/DD/YY, MM.DD.YY, DD-MM-YY, DD/MM/YY, DD.MM.YY and YYYYMMDD. Select desired date format and press **OK** to confirm your selection. Then press **ESC** to exit the system settings. When prompted to save the settings, press **OK** and the date format of the system is modified.

For example, the date formats **MM/DD/YY** and **YY-MM-DD** are displayed in the above figures on the left and right respectively.



4.1.4 Advanced Settings

Through the advanced settings, you can perform such operations as restoring factory defaults, deleting attendance records, clearing all data, clearing administrator privilege, upgrade firmware, buzzer, outdoor mode as shown below:



Upd Firmware	
Buzzer	Y
Outdoor	Y

☺ **Note:** The menu options above contain some optional functions. If the actual product does not have one or several of the options above, then this product does not support the related function(s).

Select a desired option through the ▲/▼ key, and perform settings as required.

1) Reset Opts

This option is used to restore all the settings to factory defaults.

2) Del All Logs

This option is used to delete all verification records in the chip.

3) Clear All Data

This option is used to delete all the enrolled fingerprints and records.

4) Clr admin pri

This option is used to set all the administrators to ordinary users.

5) Upd firmware

You can select “Upd Firmware” to upgrade the firmware of device through the upgrade files in the USB pen drive.

☺ **Note:** If you need firmware upgrade files, please contact our technical support engineers. Generally it is not recommended to upgrade the firmware.

6) Buzzer

The device makes sound from the buzzer, selecting “Y” to open the buzzer so that buttons or menu function can make a sound while selecting “N” to close.

7) Outdoor Mode

Choosing outdoor mode, please select “Y” and the screen will display black titles on white background after restart device, which is convenient for outdoor use.

On the contrary, select “N” and the screen will display white titles on black background after restart device, which is convenient for indoor use.

4.2 Power Management★

Press **Menu** to select **Options** → **Power Mng** and the information displayed on the screen is shown in the following figure:

Power Mng	▼
▶ Idle Min	3

Idle& Idle min

These two options are closely associated. When idle min is 0, the idle function is disabled. When Idle min is a non-zero number (unit: minute), for example, 1, the system will enter a specified state if there is no operation in 1 minute.

4.3 Communication-related Settings

Press **Menu** to select **Options** → **Comm. Opt** and the information displayed on the screen is shown in the following figure:

Comm Opt	▼
▶ BaudRate	115200
Dev Num	1
Net Speed	Auto
IP Addr	192.168.1.201
NetMask	255.255.255.0
Gateway	0. 0. 0. 0

1. Baudrate

This option is used to set the baud rate for the communication between the device and the PC. It includes five options: 9600, 19200, 38400, 57600, and 115200. The high baud rate is recommended for the RS232 communication to achieve high communication speed, while the low baud rate is recommended for the RS485 communication to achieve stable low-speed communication.

2. Dev Num

This option refers to the device ID numbered from 1 to 255.

3. Net speed

This parameter refers to the network rate, including five options: AUTO, 10M-H, 100M-H, 10M-F and 100M-F.

4. IP Addr

The default IP address is 192.168.1.201. You can modify the IP address as required.

5. Net Mask

The default subnet mask is 255.255.255.0. You can modify the subnet address as required.

6. Gateway

The default gateway is 0.0.0.0. You can modify the gateway as required.

4.4 Access Options★

The Black-and-White Screen Series Standalone Access Controller and Reader Products, work with bundled *Access3.5 Security System* as standard configuration to achieve a series of functions including Access Time-zones, Time Holidays, Linkage, Anti-passback, First-Card Normal, Multi-Card Opening functions etc., But no Interlock function. In details operation, please refer to *Access3.5 Software User Manual*.

Press **Menu** to select **Options** → **Access Options** and the information displayed on the screen is shown in the following figure:

Access Options	▼
▶ Lock	5
DSen. Delay	15
DSen. Mode	None
485Reader	Master
Master State	Out
VerifyMD	FP/RF

4.4.1 Lock

The time duration of electronic lock works from open to close when user's verification succeeds (In case the door is closed).

To set this duration, proceed as follows: Select Lock, and press OK. Then enter a desired number through the numeric pad, and press ESC to exit and save the setting.

“S (second)” is chosen as the unit of lock driver duration, and you can set it 1~10s (some devices can set 254s at most).

If set the duration to “0” , means Lock driver duration is closed. Normally, we do not suggest set it is “0” .

4.4.2 DSen. Delay

Set the door sensor delay. An alarm will be generated if the door is left open for a period of time, and this period is called door sensor delay.

4.4.3 DSen. Mode

Door sensor switch includes three modes: NONE, Normal Open (NO), and Normal Close (NC).

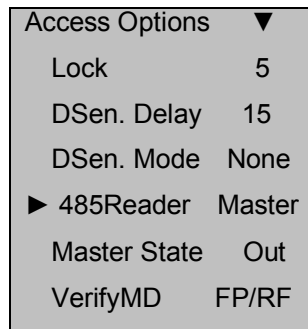
“NONE”: Door sensor switch is not used.

“NO”: Both door and lock are open; otherwise, an alarm will be generated after the door sensor delay.

“NC”: Both door and lock are closed; otherwise, an alarm will be generated after the door sensor delay.

4.4.4 485Reader★

Press **Menu** to select **Options** → **Access Options** → **485Reader**, as shown below:



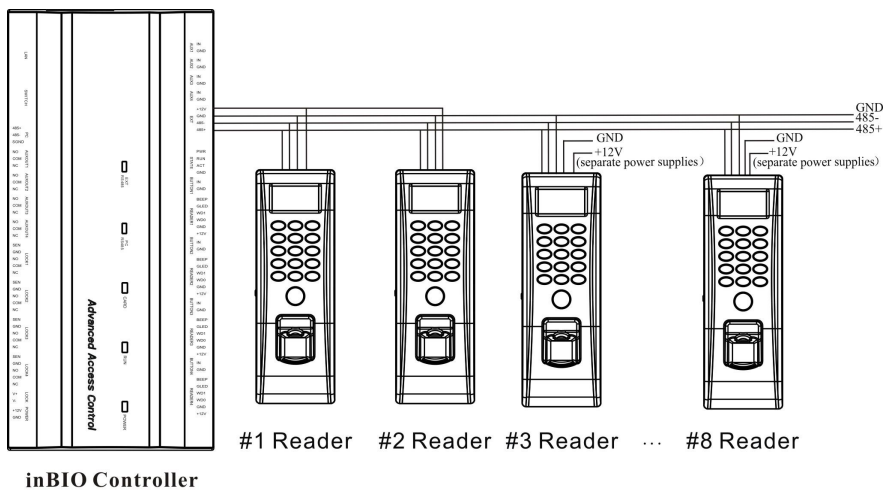
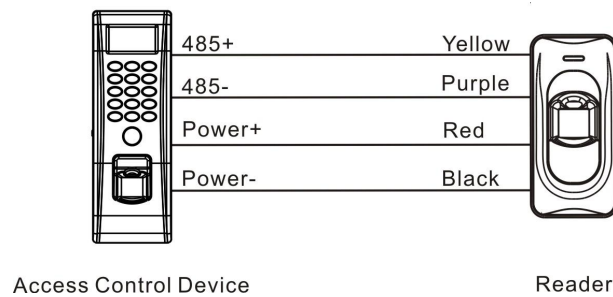
Equipment supports 485reader function, can be through the 485communication connect with FR1200 reader; Meanwhile, it can act as Master-slaver which Access Controller for master, FR1200 reader for slaver, to achieve 485 Anti-passback functions.

If select “Master”, 485reader function is opened, and the device act as Access Controller;

If select “Slave”, the device will act as Reader;

If select “No”, 485reader function is closed, the device can connect with PC through 485communications.

😊 **Note:** The device act as Maser or Slaver, due to 485reader function is opened, so the device cannot with PC through 485communications. Besides, Change any one step, should restart the equipment to take effect.



Note: Set the RS485 address(device number) by Access3. 5 software.

4.4.5 Master State ★

Master State has two types: Out or In.

Master Status set "Out" by default, and install at indoor; Slaver State set "In" and install at outside. Records of out and in are save in the master device.

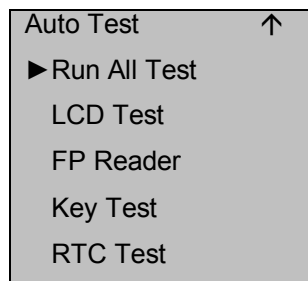
4.4.6 Verify Mode

The device supports various verification modes, including Fingerprint or ID Card(FP/RF), Fingerprint plus ID Card(FP&RF), Password plus ID Card(PW&RF), Fingerprint, Password(PW), Promixity Card(RF).The default verification mode is fingerprint or ID Card(FP/RF).

If you need to choose a verification mode except the defaulted one, you can enter Menu to modify the verification mode first. The paths: MENU →Options → Access Options→ VerifyMD.

4.5 Automatic Test

Select **Auto Test** and the information displayed on the screen are shown in the following figure:



Through this menu, you can test the system components. The auto test function helps troubleshoot the device quickly and facilitates the device maintenance.

LCD Test: The device automatically tests the display effect of its LCD and check whether its LCD displays integral images.

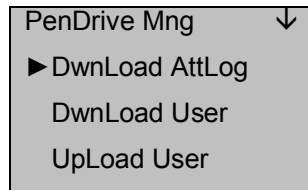
Fingerprint Reader Test: The device automatically tests whether the fingerprint reader works properly by checking. After select it, press "OK" to test, and check it whether normal. Press" ESC "to exit the test.

Keyboard Test: The device tests whether every key on the keyboard works normally. Press any key on the [Keyboard Test] interface to check whether the pressed key matches the key displayed on screen. Press "ESC" to exit the test.

Real-time Clock (RTC) Test: The device tests whether its clock works properly by checking the stopwatch of the clock. After selecting it, press "OK" to test and press "ESC" to exit the test.

5. USB Pen Drive Management ★

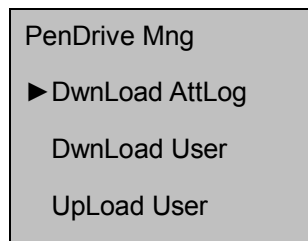
Select **PenDrive Mng** and the information displayed on the screen is shown in the following figure:



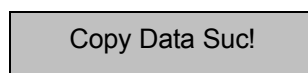
You can download the attendance data, employee data and short messages and upload employee data and short messages with a USB pen drive.

5.1 Download Attendance Data

1. Insert a USB pen drive into the USB interface on the device.
2. Select **PenDrive Mng** and select the desired access control data to be downloaded through the "▲/▼" key. The interface displayed is shown as follows:



3. Press **OK** to confirm your selection and start the download. The interface displayed upon successful download is shown as follows:

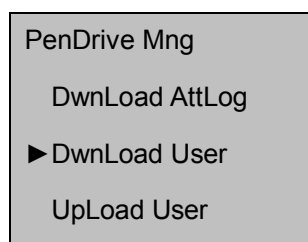


4. Press **ESC** to return to the initial interface and then remove the USB pen drive. The files form is **attlog.dat**.

😊 **Note:** If the download succeeds, a prompt "Copy Data Suc" will pop up. If the system displays the prompt "Plug Pen Drive?" please checks whether the USB pen drive is plugged in properly.

5.2 Download User Data

User data downloading is similar to the downloading of access control records. Press ▲/▼ to select "DwnLoad User" from the "PenDrive Mng" menu.

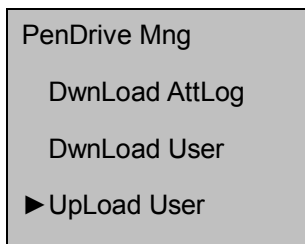


The files user.dat (user information), userauth.dat (user privilege) and timezone.dat (time period) will be concurrently downloaded to the USB pen drive. Three files download at the same time.

☺ **Note:** Has the fingerprint function device download fingerprint template name for "template.fp10".

5.3 Upload User Data

Press ▲/▼ to select "UpLoad User" from the "PenDrive Mng" menu and then press **OK**. The files user.dat (user information), userauth.dat (user privilege) and timezone.dat (Timezone) stored in the USB pen drive will be concurrently uploaded to the device.



6. Systems Information

Through the **Sys Info** menu, you can check all information of the device, including the enrolled fingerprint count, enrolled users, attendance records, administration records and equipment information. On the **Menu** interface, select **Sys Info** and press **OK** to display the interface as shown in the following figure:

Sys Info	↓
▶ User Cnt	206
FP Cnt	173
Att Log	8046
Admin Cnt	0
Pwd User	1
S Logs	4096
Free Space Info	
Dev Info	

On the screen as shown in the figure above, you can check the **User Cnt** (Number of enrolled users), **FP Cnt** (Number of enrolled fingerprints), **Att Log** (Piece of attendance records), **Admin Cnt** (Number of enrolled administrators), **Pwd User** (Number of passwords) and **Super Logs** (Number of enrolled super administrators). Through **Free Space Inf**, you can check the free space in the storage device.

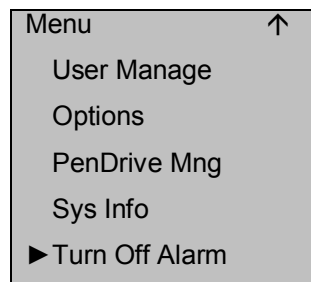
Through **Dev Info**, you can check such information as the storage capacity, date of manufacture, serial number, manufacturer, algorithm version number and firmware version number.

Dev Info	↓
▶ FPCnt(100)	30
Attlog (10K)	10
S Logs	4096
Manu Time	
Serial Num	
Vendor	
Device Name	
Alg Version	
Firmware Ver	
View MAC	
MCU Version	

7. Turn Off Alarm ★

The option **Turn Off Alarm** is available only after the device generates an alarm and is used to clear an alarm.

Path: On the **Menu** interface, select **Turn Off Alarm**.



😊 **Note:** The option Turn Off Alarm is available only after an alarm signal is generated.

8. Maintenance

1. Cleaning

Sometimes the optical lens, keyboards and display screens need to be cleaned. Although the specific cleaning cycle is dependent upon the ambient environment where the device operates, the following maintenance guide might be of some help to you:

Table 1-1 Maintenance Description

Item	Cleaning
Keyboards and display screens	Clean the keyboards or display screens when the surface of them is dirty or the screens look blurry. Please refer to the following descriptions.
Optical lens	Do not clean the optical lens frequently. The optical lens work better with oil or grease.
	Clean the optical lens if they get blurry and the verification performance is affected. Please refer to the following descriptions.

2. Clean keyboards and LCD screens

Before cleaning keyboards and LCD screens, power off the device, clean them with a piece of wet cloth or a neutral detergent and then wipe them with a piece of dry cloth.

3. Clean optical lens

Follow the suggestions below to clean the optical lens after powering off the device:

- 1) Blow off the dust or dirt on the surface of the optical lens.
- 2) Clean the display screens with adhesive tape.

Warning: Do not clean the optical lens with water or non-neutral detergents; otherwise the optical lens may be damaged.

- 3) Wipe the optical lens with a fine micro-fiber cloth. Be careful not to scratch the lens. If there are micro fibers left on the lens, try to blast them off after the lens get dry.

9. FAQs

1. Question: How do I address the problem that some employees fail to pass the fingerprint verification more often than not?

Answer: The following factors will make fingerprint verification hard or even impossible for some users:

- ①. The fingerprints of some fingers wear out.
- ②. The fingers have too many wrinkles which change frequently.
- ③ The skin on the fingers peels off badly.

For users whose fingerprints are beyond recognition, they can delete these fingerprints and enroll them again or enroll a fingerprint of another finger.

It is recommended to select fingers with good fingerprint quality (few wrinkles, no peeling-off and distinct fingerprint) for fingerprint enrollment. Press the finger flatly on the fingerprint sensor and be sure that the pad (not the tip) covers as much of the sensor window as possible. Perform fingerprint match test after finishing enrollment. It is recommended to enroll the fingerprints of several fingers as backup.

Furthermore, the device provides the 1:1 matching and password verification functions especially for users who have difficulty in or cannot pass fingerprint verification.

2. Question: What are the possible causes of the device communication failure?

Answer: The possible causes are listed as follows:

- ① The setting of communication port is incorrect. The port set for communication is not the COM port actually used.
- ② The setting of the communication port baud rate of the PC is not consistent with that of the device.
- ③ The device is not connected with the power supply or the PC.
- ④ The device is connected with the PC but not powered on.
- ⑤ The No. of the connected terminal is incorrect.
- ⑥ The data cable or converter is faulty.
- ⑦ The COM port of the PC is faulty.

3. Question: What are the possible causes of incomplete display (sometimes half-screen display) or blurred screen after the device is powered on? How to fix it?

Answer: The possible causes are listed as follows:

- ① The main board is faulty.
- ② The LCD display is faulty.

In either of the above cases, you need to contact the supplier and return the device for repair.

4. Question: How can I delete administrator?

Answer: You can press **Menu--Options--Syms Opt -- Adv option-- Clr Admin Pri** to delete administrator.

Besides, Connect the device with a PC and establish communication between them. Select the device management tab, and click **Delete Administrator** to delete the device administrator. You can access the device menu after disconnecting the device with the PC.

5. Question: Why is there a beep sound during the communication between device and PC?

Answer:

- ① If the beep sound occurs in RS-232 communication mode, the baud rate settings of the PC and device are inconsistent.
- ② If the beep sound occurs in RS-485 communication mode, it is possible that the two communication cables of the converter are inversely connected or stuck together.

6. Question: Why does the device constantly display “Please press (remove) your finger again”? How to fix it?

Answer: The possible causes are as follows:

- ① There is dirt, grease or scratch on the surface of the fingerprint sensor, which may lead the fingerprint sensor to mistakenly think there is a finger pressing on the surface. Remove the dirt or grease on the surface of the fingerprint sensor with an adhesive tape.
- ② The connection cable of fingerprint sensor comes loose or disconnected.
- ③ The chip of the main board is faulty.

For the last two cases, contact the supplier and return the device for maintenance.

7. Question: Why does a failure or error occurs when I read the attendance data while I can download fingerprint and password data properly? How to fix it?

Answer: This problem may relate to the data cable, converter or the COM port setting of the PC. You may try decreasing the baud rate of the PC and device, for example, set it to 19200 or 9600 before reading the attendance data again.

10. Appendix

The functions described in Appendix are all optional. If you need these functions, please consult our commercial representatives or pre-sales technical support engineers.

10.1 USB

USB Host

The device is used as the USB Host to externally connect with a USB pen drive for data exchange.

The conventional fingerprint readers transfer data only through the RS232, RS485 or Ethernet. Bulk data transfer may take a long time due to the restriction of physical conditions. The USB far outperforms any other previous transfer modes in terms of data transfer rate. Insert the USB pen drive to the USB slot on the device, download data to the USB pen drive, and then connect the USB pen drive to a computer to import the data to the computer. Further, the device also supports the exchange of user information and fingerprint data between two devices, which helps dispense with the hassle of conventional cable connection for data transfer between the device and computers.

For the operations of the device used as the USB host, see [5.USB Pen Drive Management](#) ★.

USB Client

Connect the device with the PC as the mobile storage device, and transfer the data stored in the device to the PC through the USB connection cable.

When the device is used as the USB Client, the USB communication options will be displayed in the device communication setting menu. For details, see [4.3Communication-related Settings](#)

Note: When the device connects with the PC as the USB Client, the PC must be installed with related driver.

10.2 Scheduled Bell

Lots of companies need to ring their bells to signal the start and end of work shifts, and they usually manually ring their bells or use electric bells. To save costs and facilitate management, our company integrates the scheduled bell function into the device. The options **Bell Delay** and **Bell Time Segment** are available on the devices that support the scheduled bell function. There are 8 time segments available every day of a week. You can set the ring time as required. The device will automatically ring at the specified time every week and stop the ring after the ring duration times out.

The device rings the bell in the following two ways:

Ring the bell through the speaker configured on the device.

Connect an electric bell to the device. The device will send a relay signal to trigger the electric bell at the specified time.

10.3 External Connection with the Fingerprint Reader

This function is especially for devices configured with USB interfaces. Insert the fingerprint reader into the USB slot, select the fingerprint reader **Menu** → **Options** → **Adv Option** → **Connect with FP Reader** and set the option **Connect with FP Reader** to **Y**. After that, the externally connected fingerprint reader and the built-in fingerprint reader of the device can be used concurrently.

When used for time & attendance management, the externally connected fingerprint reader can help siphon off some of the users at peak time; when used for access control, the externally connected fingerprint reader can be placed outside of the door and the host is placed inside, which not only implements the fingerprint access control both inside and outside of the door, but also ensures the host security.

Notes:

- 1) After connected, the fingerprint reader can only be used after restart.
- 2) Only the fingerprint readers with the SDK license can be used for external connection.

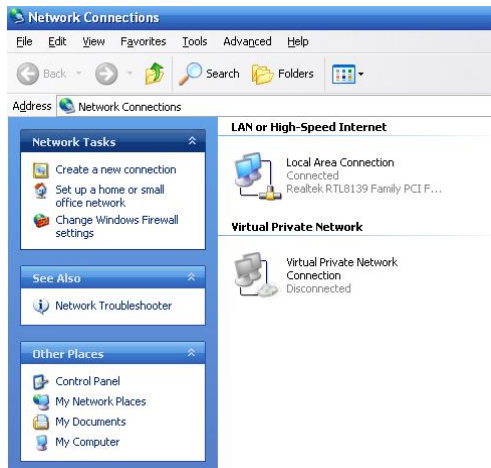
10.4 Modem

[Overview]

To enable remote communication between a PC and the device in areas where Internet access is unavailable, some devices support the Point-to-Point Protocol (PPP) connection. The PPP connection is a type of end-to-end connection over telephone cables. The PC implements dial-up network access through a Modem. The device must also connect with a Modem which is then connected with the PSTN over a telephone cable. The device accesses the network upon successful dial-up.

[Operation Steps]

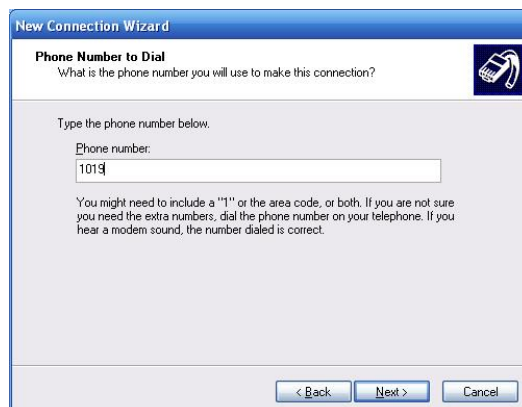
1. Connect the device with the Modem by using the delivery-attached cable marked with “Modem”. Power on the device and Modem respectively and then connect the telephone cable to Modem.
2. Select **Option** → **Comm Opt** on the device and set the option **Extern Modem** to **Y**. Save the setting and exit. Then restart the device.
3. The following takes Windows XP dial-up setup as an example to illustrate the procedures of creating a dial-up connection:
 - 1) From the **Start** menu, choose **Control Panel**. Click the **Network and Internet Connections** icon and disable **Local Connection**, as shown in the following figure:



- 2) Select "Create a new connection" from **Network Tasks**. The **New Connection Wizard** will start.
- 3) Click the **Next** button to begin, as shown in the following figure:



- 4) Make sure the **Connect to the network at my workplace** option is selected and click the **Next** button, as shown in the following figure:
- 5) Select the **Set up my connection manually** option and click the **Next** button.
- 6) On the next screen you will be prompted to enter a name for the dial-up connection. You can name this connection anything you wish (e.g. 1019). After you have entered your connection name click the **Next** button.



7) On the next screen you will be prompted for the phone number for the ISP. Enter the number of the telephone cable connected with Modem. When entering the local access number, pay attention to the following cases:

- i. Extension-to-extension dial up within a company: Enter the number of extension connected with Modem. "1019" in the figure above is an extension number.
- ii. Dialing extension from an external line: First you need to enter the exchange number and then the extension number. The exchange and extension numbers are separated with comma(s). Each comma indicates a pause of 3 seconds. Add several commas in between if necessary. Note that you need to prefix an area code to the exchange number if you dial the extension from another city.
- iii. Direct dialup: Enter the telephone number to be dialed and prefix an area code to the telephone number if you dial the direct line from another city.
- iv. Direct outward dialup: Enter 0 or 9 and then the number to be dialed. The number 0 or 9 and the number to be dialed are separated with a comma, for example, "9,02150814442".

8) After entering the phone number, click the **Next** button.

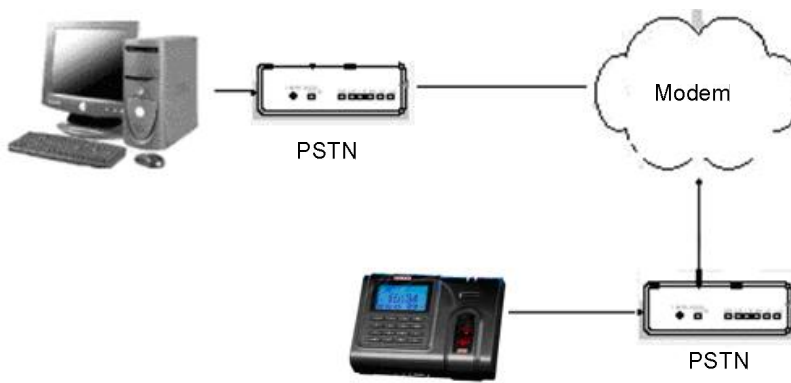
9) After finishing the connection setup, double-click the new connection and the interface as shown in the following figure is displayed:

10) Both the user name and password are "ppp". After typing the user name and password, click **Dial** to start connection. The default device IP address after successful connection is 192.168.1.100.

11) Start the attendance tracking software, and change the IP address into 192.168.1.100.

12) Click the **Connect** button. You can upload or download data upon successful connection (as shown in the figure below).

[Schematic Diagram of Connection]



[Precautions]

1. Connect Modem with the device using the delivery-attached cable marked with "**Modem Cable**" in the packing box.
2. Use the delivery-attached C1 control box (12V) to power the Modem.
3. Before connecting Modem with the device, set the option **Extern MODEM (MENU → Options → Comm Opt → Extern MODEM)** on the device to **Y**.

4. When Modem is used, the RS232 and RS485 functions of the device will be disabled; when the option **Extern MODEM** is set to **N** (that is, Modem is not used), the RS232 and RS485 functions are enabled.
5. The PPP Server is integrated into the device. Please adopt Windows-based PPP client dialup program to connect A11. The default user name and password are both "ppp". After the PPP connection is set up, the IP address of A11 is 192.168.1.100 and that of PC is 192.168.1.133 by default.

10.5 GPRS Functions

The General Packet Radio Service (GPRS) is a new packet data bearer service developed based on the Global System for Mobile Communications (GSM). As a packet switched system, the GPRS is especially suitable for intermittent and sporadic or frequent and small packet data transmission and also suitable for occasional bulky data transmission. This feature is ideal for a majority of mobile applications, for example, the mobile office and Internet access. The GPRS demonstrates outstanding capabilities in terms of transmission rate, radio resource management and billing.

Our device is also GPRS-capable. It supports either built-in or external GPRS module to implement data transmission over the GPRS.

For detailed GPRS operations, see related operation instructions.

10.6 WIFI Functions

Wireless Fidelity (Wi-Fi) is also known as the [802.11b](#) standard. The greatest advantage of Wi-Fi is its high transmission rate up to 11Mbps. Wi-Fi also features long transmission distance and excellent compatibility with various existing 802.11 DSSS devices. IEEE 802.11b is a radio-based variant of IEEE 802.11. The bandwidth of IEEE 802.11b can be up to 11 Mbps and automatically adjusted to 5.5Mbps, 2Mbps and 1Mbps depending the signal strength and interference level, thus effectively ensuring network stability and reliability. Major advantages: High transfer speed and reliability. The communication distance can be up to 305 m in an open area and 76 m to 122 m in an enclosed area. Wi-Fi can be conveniently integrated with the existing wire-line Ethernet, making the networking cost even lower.

Our device is also WIFI-capable. It supports either built-in or external WIFI module to implement wireless data transmission over the WIFI.

For detailed WIFI operations, see related operation instructions.

10.7 Attendance Query

You can query the attendance data of an individual or all employees directly on the device that supports the attendance query feature. This helps remove the hassle of installing software and connecting device for attendance downloading and query, and facilitates employees to query their own attendance data.

You can query the attendance data of not only an individual but also all employees on the device.

10.9 MP3 Function Description

The MP3 function enables the play of hi-fi MP3 music by real-time decoding MP3 files with an MP3 player. The MP3-capable devices have a built-in MP3 player to play MP3 voice files of MPEG1.0 Layer III format. Similar to the scheduled bell, the MP3 function allows users to set 8 time segments and automatically plays MP3 files at user-specified time segments.

You can also set an MP3 file to signal the start of work and noon break, or place an announcement into an MP3 file for the device to play at the specified time, thus making your office more employee-friendly.

The device can either play MP3 files through its own speakers or through an external sound box.

there are 8 time segments available for you to select. You can set the time segment as required. The device automatically plays an MP3 file at the specified time segment.

Notes:

1. All the 8 time segments adopt the 24-hour time system.
2. The time segment 1 relates to file 1.mp3, the time segment 2 relates to file 2.mp3 and so on and so forth.
3. You cannot perform other operations while the device is playing an MP3 file.
4. While the device is playing an MP3 file, you can press any menu key to stop the play.

MP3 file access

The device itself cannot store MP3 files, but it can access MP3 files in the following two ways:


- Access MP3 files through webserver.

Step 1: Select **Menu** → **Options** → **Power Mng** → **WEB Server IP** on the device and enter the IP address of the PC where the web server is installed.

Step 2: Copy MP3 files to the web server.

If you have already installed web server (IIS, or Apache) on the PC, you can create a folder with the name of “MP3” under the root directory of the virtual host of the web server. Then copy MP3 files to this folder. Type `http://xxx.xxx.xxx.xxx/mp3/y.mp3` in the IE address bar to check whether you can access the MP3 file normally.

If you have not installed WEB server in your PC, you can install the web server software provided the software in the following way: Decompress the “web server .rar” file to a certain directory (take d:\ as an example). Double-click **webs.exe** under the directory `d:\webserver\main` to run the Web server and ensure the Web server runs in the entire process. Copy the MP3 to be played to `d:\webserver\web\mp3`. Type `http://xxx.xxx.xxx.xxx/mp3/y.mp3` in the IE address bar to check whether you can access the MP3 file normally.

 **Note:** “xxx.xxx.xxx.xxx” refers to the IP address of the PC where the Web server is installed and “y” in “y.mp3” refers to the number of an MP3 file.

Step 3: The device reads and plays the mp3 file through web server at user-specified time segment.

- Access MP3 file through a USB pen drive.

Copy MP3 files to a USB pen drive. The device automatically searches the set MP3 file in the USB pen drive to play at the user-specified time segment.

 **Note:** The device searches and plays MP3 files in the following sequence:

Search MP3 files on the Web server.

Search MP3 files in the USB pen drive if no MP3 file is specified on the Web server or the Web server cannot be accessed.

Play its own ring-tone if the USB pen drive is not inserted or the specified MP3 file is not found in the USB pen drive.

MP3 play modes

The device can either play MP3 files through its own speakers or through an external sound box.

- **Volume control**

The device supports the volume control function. If the volume of the MP3 player is too high or low, you can adjust the volume by selecting **Menu** → **Options** → **System Opt** → **Adv Option** → **Volume Control** on the device.

- **MP3 file format**

The device supports MP3 files of MPEG1.0 Layer III format. (The MPEG1.0 Layer III format is the common format for MP3 files. If an MP3 file cannot be played by the device because it is compressed by a standard (e.g. MPEG I Layer 1 or Layer 2) that the device does not support, replace it with another MP3 file.)

- **MP3 file detection**

To check whether an MP3 can be played, select **Menu** → **Options** → **Auto Test** → **MP3 Test** on the device.

10.10 Short Message

Some models of device support the transfer of public and private short messages at the specified time and for a specified individual. You can edit public or short messages through the background software and then upload them to the device. The public short messages are displayed on the screen all the time once the device is started, while private short messages are displayed upon the fingerprint verification. This function helps reduce the workload for the HR department and greatly enhance working efficiency.

A short message for an individual: For example, if an employee's birthday is October 20th, then you can edit a short message "Happy birthday to you!" through the background software, upload the short message to the device, and set it to be displayed on October 20th. This message will be displayed on the screen once this employee verifies his/her fingerprint.

A short message for a group of employees: for example, for a plenary meeting scheduled to be held on June 19th, you can edit a short message "Please attend the plenary meeting at xx in the xx meeting room" (you can edit it as required) through the background software and upload it to the device. Then on June 19th, this short message will be displayed all the time on the screen once the device is started.


Setting of short messages: After setting the short message in the attendance software, upload it to the device. The device supports the import of short messages in two modes:

- Direct import by connecting the software to the device.
- Import from a USB pen drive.

Operation Description:

1. Edit a short message by selecting the **External Program**→ **SMS Mng** menu item of the attendance software, connect the attendance software and upload it to the device.
2. Edit a short message by selecting the **External Program**→ **SMS Mng** menu item of the attendance software. Select **External Program**→ **PenDrive Mng**→ **Export** → **Export to PenDrive** to export the edited short message to the USB pen drive. Insert the USB pen drive into the slot on the device upon successful export, and select **Menu** → **PenDrive Mng** → **Upload SMS** to upload the short message from the USB pen drive.

Display of short messages: Public short messages are displayed all the time on the screen once the device is started. Private short messages are displayed upon fingerprint verification.

 **Note:** You can upload a maximum of 1024 public or private short messages to the device.

10.11 Multiple Verification Modes

Currently the device falls short of the requirements for high-security access control by providing the fingerprint only, password only and ID + fingerprint verification modes. To provide feature-rich access control systems, we support customization of multiple verification modes for individuals or groups to meet the most stringent security requirements of customers. Apart from the fingerprint only, password only and ID + fingerprint verification modes, the device also supports a combination of the ID (PIN), fingerprint (FP), password (PW) and RF verification to achieve up to 15 verification modes as listed in the following tables.

 **Notes:**

- 1) Mifare can be deemed as RF in the verification process and Mifare card verification is only available for Mifare-card-capable devices.
- 2) Except for some devices of specific models, the B&W screen series devices support only the fingerprint and password verification modes. The Mifare-card-capable devices also support the Mifare card verification apart from the fingerprint and password verification modes.
- 3) The device supports up to 15 verification modes to meet the requirements of different customers. “/” means “or”, “&” means “and” and “←” means confirmation (OK).

Users enroll their fingerprints and passwords on the device. The verification modes are listed as follows:

Type	Description
FP	Fingerprint verification only
	1)PIN+FP (1: 1) 2) FP (1: N) 3) RF+FP (1: 1)
PIN	ID number verification only

Type	Description
	Users can pass the verification as long as they type their ID numbers through keyboard regardless of their enrollment modes.
PW	Password verification only
	1) PIN+“←”+PW 2) RF+PW
RF	RF Card verification only
	1) RF
FP/PW	Fingerprint or password verification
	1) PIN+FP(1:1) 2) FP(1:N) 3) PIN+“←”+PW 4) RF+PW
FP/RF	Fingerprint or RF verification
	1) PIN+FP(1:1) 2) FP(1:N) 3) RF
PW/RF	Password or RF verification
	1) RF 2) PIN+“←”+PW
FP/PW/RF	Fingerprint or password or RF verification
	1) PIN+FP(1:1) 2) FP(1:N) 3) PIN+PW 4) RF
PIN & FP	ID number and fingerprint verification
	1) PIN+“←”+FP(1:1) 2) RF+ PIN+“←”+FP(1:1)
FP&PW	Fingerprint and password verification
	1) FP(1:N)+PW 2) PIN+FP(1:1)+PW 3) RF+PW + FP(1:1)
FP&RF	Fingerprint and RF verification
	1) RF+FP(1:1) 2) FP(1:N)+RF 3) PIN+FP(1:1)+RF
PW&RF	Password and RF verification
	RF+PW PIN+“←”+PW+RF
FP&PW&RF	Fingerprint, password and RF verification
	1) FP(1:N)+PW+RF 2) PIN+FP(1:1)+PW+RF 3) RF+ PW+ FP(1:1)
PIN & FP &PW	ID number, fingerprint and password
	1) PIN+“←”+PW+FP(1:1) 2) RF+ PIN+“←”+PW+FP(1:1)

Type	Description
FP & PIN /RF	Fingerprint and ID number or fingerprint and RF verification
	1) FP+ PIN 2) FP +RF 3) PIN+FP(1:1) + PIN 4) PIN+FP(1:1) +RF

Users enroll their fingerprints or passwords on the device. The verification modes are listed as follows:

Type	Description	
	Enroll fingerprint	Enroll password
FP	Fingerprint verification only 1) PIN+FP (1:1) 2) FP (1:N) 3) RF+FP(1:1)	Verification failure
PIN	ID number verification only 1) PIN is entered through the keyboard.	1) PIN is entered through the keyboard.
PW	Password verification only Password error	1) PIN+“←”+PW 2) RF+PW
RF	RF Card verification only 1) RF	1) RF
FP/PW	Fingerprint or password verification 1) PIN+FP(1:1) 2) FP(1:N) 3) PIN+“←”+ FP(1:1) 4) RF+FP(1:1)	1) PIN+“←”+PW 2) RF+PW
FP/RF	Fingerprint or RF verification 1) PIN+FP(1:1) 2) FP(1:N) 3) RF	1) RF
PW/RF	Password or RF verification 1) RF 2) PIN+“←”+RF	1) PIN+“←”+PW 2) RF
FP/PW/RF	Fingerprint or password or RF verification 1) PIN+FP(1:1) 2) FP(1:N) 3) PIN+“←”+ FP(1:1) 4) RF	1) PIN+“←”+PW 2) RF
FP&PIN	Fingerprint and ID number verification 1) PIN+“←”+FP(1:1) 2) RF+ PIN+“←”+FP(1:1)	Verification failure
FP&PW	Fingerprint and password verification Verification failure	Verification failure
FP&RF	Fingerprint and RF verification 1) RF+FP(1:1) 2) FP(1:N)+RF 3) PIN+FP(1:1)+RF	Verification failure
PW&RF	Password and RF verification Verification failure	RF+PW PIN+“←”+PW+RF
FP&PW&RF	Fingerprint, password and RF verification	
	Verification failure	Verification failure
FP&PIN&PW	Fingerprint, ID number and password	
	Verification failure	Verification failure

😊 Notes:

1) **1:N** also includes **1:H** and **1:G**.

2) It is recommended to **enroll both fingerprints and passwords** for the combined verification mode; otherwise, it may lead to verification failure.

For example, user A only enrolls his/her **fingerprint**, but the verification mode is **PW**, so user A will fail the verification.

10.12 EM Read-only Card, HID Card, Mifare Card, iClass Card

To accommodate the market demand for the currently popular RF cards, we have developed the device with built-in non-contact RF EM card reader module. By integrating the EM read-only card, this device can be conveniently consolidated into the existing telephone, canteen POS and access control system. This device supports multiple verification modes including the fingerprint verification, password verification, card verification, card + fingerprint verification and card + password verification to meet the diversified customer needs.

EM Read-only Card

The EM Read-only Card supports thick (1.88 mm), thin (0.88 mm) and medium-thickness (1.05 mm) ID/EM cards with working frequency of 125 kHz and card reading distance of 5m.

HID Card

To accommodate to the market demand for the currently popular RF cards, we have developed the device with non-contact RF HID card reader module. By integrating the HID read-only card, this device can be conveniently consolidated into the existing telephone, canteen POS and access control system. This device supports multiple verification modes including the fingerprint verification, password verification, card verification, card + fingerprint verification and card + password verification to meet the diversified customer needs.

The device supports HID cards with working frequency of 125 kHz and card reading distance of 2m to 5m.

Mifare Card

To accommodate the market demand for the currently popular RF cards, we have developed the device with non-contact RF Mifare card reader module. By integrating the Mifare card, the device can be conveniently consolidated into the existing telephone, canteen POS and access control system. This device supports multiple verification modes including the fingerprint verification, password verification, card verification, card + fingerprint verification and card + password verification to meet the diversified customer needs.

The device supports MIFARE non-contact smart cards with working frequency of 13.56 MHz and card reading distance of 3m to 5m.

For the operations of the Mifare cards, see *Mifare Card User Guide*.

iClass Card

To accommodate to the market demand for the currently popular iClass cards, we have developed the device with non-contact RF iClass card reader module. By integrating the iClass card, the device can be conveniently

consolidated into the existing telephone, canteen POS and access control system. The device supports multiple verification modes including the fingerprint verification, password verification, card verification, card + fingerprint verification and card + password verification to meet the diversified customer needs.

The device supports iClass read/write non-contact smart cards with working frequency of 13.56 MHz and card reading distance of 2m to 5m.

For the operations of the iClass cards, see *iClass Card User Guide*.

10.13 Master-slave function ★

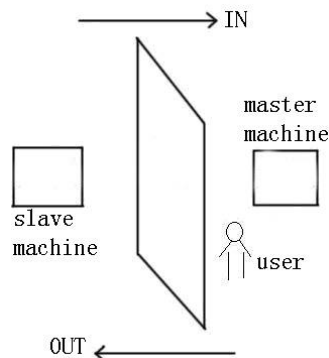
Two devices, a master and a slave, both controlling the same lock, are connected by RS232/RS485/Wiegand.

1. The Applications of the Master and the Slave

1) Record storage:

By default, the master status is exit and the slave status is entry. The records of entry and exit are both saved on the master.

2) Anti-Passback function:



Whether to perform the anti-passback function is determined by the latest record of the user's entry and exit. With this function, the exit record must match the entry record. The function supports "Out", "In", "In & Out", "None and save " or "None" anti-passback. By default, the identification status of the master is exit and that of the slave is entry, so if " out anti-passback " has been set and when the last record of the user's entry is not "entry", the system will prompt anti-passback refusal" and refuse to open the door if the user wants to exit. The logic is the same with "out anti-passback" and "in & out anti-passback".

For example, now A wants to exit.

- ① If the last record for A is not entry, the device will prompt anti-passback refusal and refuse to open the door.
- ② If the last record for A is entry, after the fingerprint identification is passed, the device will open the door.

3) Alarm function

If the slave is equipped with alarm function (e.g. F10), when an alarm incident occurs, the slave will forward it for the master to process. There is no such function on device that is not equipped with alarm function.

2. The Connection of the Master and the Slave

Currently, three modes—RS232, Wiegand and RS485 are applicable for the connection of the master and the slave. Of the three, RS232 is less often used due to its deficiency that its connection distance is short. For example, it can be used when the master and the slave are just installed respectively inside and outside a door. Its connection principle is similar to that of RS485, which is omitted here. The Wiegand connection is widely used most of whose devices on the market are applicable to the master and the slave. RS485, whose transmission distance is great (however it is recommended that the distance should not be over 600 meters), applies to most occasions, but the slave must be equipped with the inBIO reader (which is used for collecting fingerprint or swiping card).

If Wiegand connection is to be used, the connection and setting for anti-passback are as follows:

1) Select model:

Master machine: Machine with Wiegand in function, except for F10 Reader.

Slave machine: Machine with Wiegand Out function.

2) Master-slave menu setting:

This machine supports out, in, out-in, No, No and saved anti-pass back (enter **Menu** -> **setting** -> **system setting** -> **advanced setting** -> **anti-passback**).

3) Modify device's Wiegand output format:

If the two devices are communicating, only Wiegand signals without device ID can be received. Enter device Menu -> Comm. Opt -> Wiegand option or enter software: Basic setting -> device management -> Wiegand, to modify “defined format” as “wiegand26 without device ID”.

4) Enroll user:

The user must be on master machine and slave machine at the same time, and user PIN must be the same. Therefore, it is necessary to enroll user on master machine and slave machine at the same time.

5) Connection instruction:

Wiegand communication is adopted for master machine and slave machine. Refer to the following for connection:

Master		Slave
IND0	<----->	WD0
IND1	<----->	WD1
GND	<----->	GND

If RS485 connection is to be used, the connection and setting for anti-passback are as follows:

The mode of RS485 is a new application in the connection of the master and the slave. In this mode, user information, fingerprint verification, card verification and authority verification are all processed on the master

and the slave is only used as a collector. Therefore, the software only needs to manage user information and record information on the master.

1) Choosing devices:

The master: It must have the 485 communication function (upgrade firmware required).

The slave: It must use the inBIO readers (reader only responsible for collecting fingerprint, such as F11 and SR200).

2) Setting the menu on the master:

Setting the master:

①Access Menu>Settings>System Settings>Advanced Settings>Anti- passback. The setting can be "Out", "In", "In Out", "None and save " or "None".

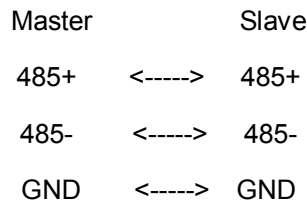
②Access Menu>Settings> Access Options>485 reader. If "Yes" is chosen, the master and slave function of 485 modes is started and at the same time the communication function with PC is forbidden. If "No" is chosen, the machine runs normally the communication function of PC.

Setting the slave:

Set the device number, identical to the master.

3) Connecting the master and the slave

The master and the slave are for RS485 communication, whose connection is shown as in the figure:



3. The Use of the Master and the Slave

After the devices are started, the master works the same as common access control. The slave cannot verify. When a fingerprint is pressed or a card is swiped on the slave, the indicator will blink and "click, click" will sound to prompt and the verification result will be displayed on the master.

10.14 Remote Identification Server (RIS)

Due to the capacity and speed constraints, it is unlikely to store a hefty amount of fingerprints (for example, thousands of fingerprints) offline on the device. Even if the device is highly scalable, the offline running speed of the device is way too slow as opposed to the PC. Therefore, the offline RFT falls short of the requirements raised by some large verification system for large fingerprint storage capacity and high match efficiency. To accommodate to these requirements, our company delivers the Remote Identification Server (RIS) solution.

Operating Principle of the RIS

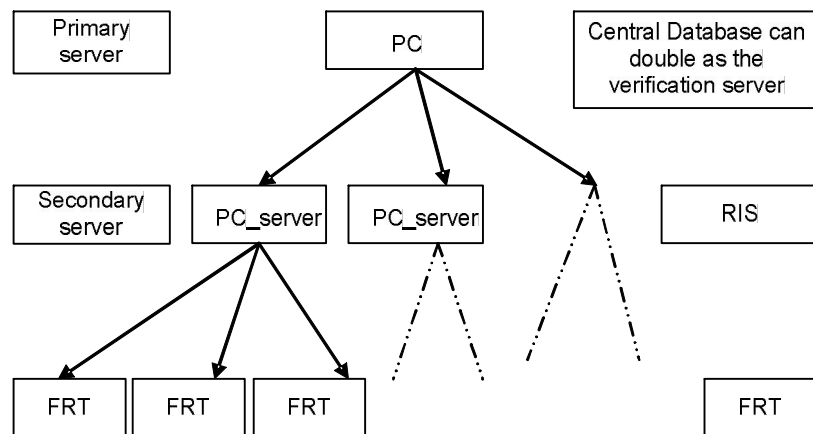
The RIS solution uses the device as the fingerprint reader while retaining its offline verification function. By using the network function of the device, it sends the data such as the fingerprint verification templates and

fingerprint images to the background for verification, stores verification results in background database and displays them on the LCD screen of the device.

The RIS solution is especially suited to large database match of factories with a headcount of 1000 to 3000 employees, making time & attendance tracking highly efficient. Furthermore, to address the issue of cross-factory staff mobility, we also propose the zone and quasi-DNS solutions. By logically dividing server locations and dynamically identifying staff mobility, the device realizes free staff mobility and dispenses with manual configurations. The quasi-DNS solution developed based on the DNS ensures stable system running and even and efficient resource allocations even in the case of traffic burst.

RIS Architecture

The basic mode of the RIS is client/server (c/s) mode, as shown in the following figure. The device only serves as the fingerprint reader and sends fingerprints to the RIS. The RIS verifies the fingerprint templates from the device by taking advantage of the powerful processing capability of PC, stores the verification results in the center database and returns them to the device for display at the same time. At present the verification speed of the device is less than 2s when the total number of fingerprints is 5,000.



RIS Operation Description

Menu setting

Select **Menu** → **Options** → **System Opt** → **Adv Option** on the RIS-capable device and you can see the following two options:

- **Remote Verify:** This option includes four values: "NO", "NL", "LO" and "LN".
- **Server IP:** This option is used to set the IP address of the RIS.

After the device is successfully connected with the RIS, select **Menu** → **User Manage** → **Enroll User** and the following option is displayed:

Remote FP Enroll: The remote fingerprint enrollment is available after this option is set to **Y**.

RIS software

The RIS software includes three parts: Fingerprint enrollment, verification server personnel configuration and fingerprint verification server.

10.15 Web Server Access Control

Overview of Web Server Access Control Software

The Web server access control system is remote data collection/access control system based on the Web Server technology and underpinned by the standard TCP/IP network structure. It adopts the common Web page requests to handle and manage data. It is free from geographical restrictions and does not require the installation of other software. You can download the employee data stored in the remote fingerprint terminal through various types of browsers such as IE and Netscape, and prepare statistical reports for enterprise management and decision-making. With the Web Server access control software, customers can really have real-time synchronization at hand anywhere at any time.

Role of Built-in Web Server

See iClock Attendance.

Use of Webserver Access Control Software

When using the webserver access control software, you need to set the IP address of the device, for example, 192.168.1.115. Then type <http://192.168.1.115> in the IE address bar. The default username of the super administrator is “admin” and password is “admin888”.

For details of the webserver access control software, see *Webserver Access Control Software Specifications*.

10.16 Automatic IP Address Collection

It is possible that the administrator may forget the IP addresses of the devices when multiple devices are managed on the same LAN. To remove the hassle of querying the IP addresses of devices one by one, we develop a type of software that automatically collects the IP addresses of devices on the LAN.

All you need is to copy all dll files to the system directory System32, and select **Start** → **Run** to run **regsvr32 zkemkeeper.dll**. After the system prompts registration success, double-click **DeviceSearch.exe** to run the software.

10.17 Wiegand Protocol

Wiegand26 is an access control standard protocol established by the Access Control Standard Subcommittee affiliated to the Security Industry Association (SIA). It is a non-contact IC card reader interface and output protocol.

Wiegand26 defines the interface between the card reader and controller used in the access control, security and other related industrial fields. Wiegand26 helps standardize the work of the card reader designers and controller manufacturers. The device is also designed in compliance with Wiegand26.

Digital Signals

Figure 1 is a sequence diagram in which the card reader sends digital signals in bit format to the access controller. In this sequence diagram, Wiegand follows the SIA's access control standard protocol for the 26-bit Wiegand card reader (one pulse time ranges between 20us and 100us, and the pulse jump time ranges between 200us and 20ms). Data1 and Data0 are high level (larger than Voh) signals till the card reader

prepares to send a data stream. The asynchronous low-level pulse (smaller than V_{ol}) generated by the card reader is sent to the access control panel (The saw-tooth wave as shown in Figure 1) through Data1 or Data0. Data1 and Data0 pulses will neither overlap nor be generated synchronously. Table 1 lists the maximum and minimum pulse widths (a consecutive pulse) and pulse jump time (time between pulses) allowed by the F series fingerprint access control terminal.

Table 1 Pulse Time

Symbol	Definition	Typical Value of Reader
T_{pw}	Pulse Width	100 μ s
T_{pi}	Pulse Interval	1 ms

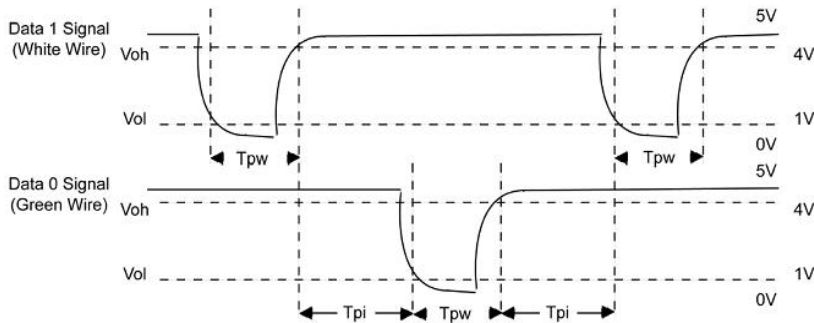


Figure 1 Sequence Diagram

Wiegand Format

The Wiegand format adopted by the device is the universal access control protocol.

26-Bit Wiegand Format

The composition of the open de facto 26 Bit Weigand industry standard contains 8 bits for the facility code and 16 bits for the ID number field. Mathematically, these 8 facility codes allows for a total of just 256 (0 to 255) facility codes, while the 16 ID number bits allow for a total of only 65,536 (0 to 65,536) individual ID's within each facility code.

26-Bit Wiegand format is of 26 bits in length, including 2 bits for parity bits.

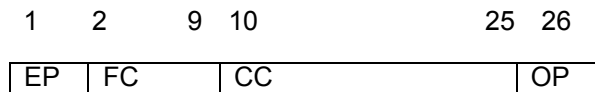


Table 2 Definition of Fields

Field	Purpose
EP	Even Parity bit (EP) is judged based on field 1 to 13 bit. EP is 1 if the number of "1" is even; otherwise, EP is 0.
FC(bit2-bit 9)	Facility Code (0-255) Bit 2 is the Most Significant Bit (MSB).
CC (bit10-bit 25)	Card Code (0-65 535). Bit10 is the MSB.
OP	The value of Odd Parity bit is determined by 14–26 bit. OP is 1 if the number of "1" is even; otherwise, OP is 0.

Pyramid Wiegand format

Several alternatives exist for customers who require more codes. The first is to switch to Keri's standard 39 bit Pyramid format. This 39 bit Wiegand format contains 17 bits for the facility code field and 20 bits for the ID number field. Mathematically these 17 facility code bits allow for a total of 131,072 (0 to 131,071) facility codes, while the 20 ID number bits allow for a total of 1,048,576 (0 to 1,048,575) individual ID's within each facility code. Since there are so many facility codes in the Pyramid format, a new facility code may be selected for each project. Additionally the large number of ID's per facility code makes the Pyramid format ideal for very large projects. For added security, Keri Systems tracks credential coding to ensure that no duplication occurs. Table 3 provides a summary of the Pyramid Wiegand format.

Table 3 Pyramid Wiegand Format

Bit Number	Meaning
Bit 1	Even parity over bits 2 to 9
Bits 2 to 18	Facility code (0 to 131,071); Bit 2 is MSB
Bits 19 to 38	ID Number (0 to 1,048,575); Bit 19 is MSB
Bit 39	Odd parity over bits 20 to 38

Custom Wiegand Formats

The second alternative is to create a custom Wiegand format. Typically, up to 64 bits are available for creating a custom Wiegand format. With certain limitations, formats with greater than 64 bits may be created. If a customer currently has a custom Wiegand format from Wiegand or from other proximity manufacturers, Keri can normally match that format. Although the customer is primarily responsible for custom format card coding, as an added benefit Keri Systems tracks card coding for additional security. Table 4 provides an example of one possible custom Wiegand format.

Table 4 Example of a Custom Wiegand Format

Bit Number	Purpose
Bit 1	Even parity over bits 2 to 22
Bits 2 to 9	OEM code (0 to 255); Bit 2 is MSB
Bits 10 to 21	Facility code (0 to 4,096); Bit 10 is MSB
Bits 22 to 43	ID Number (0 to 524,287); Bit 22 is MSB
Bit 44	Even parity over bits 23 to 43

10.18 Soap Interface

Definition of SOAP

SOAP is a lightweight protocol for exchange of information in a decentralized, distributed environment. SOAP defines a type of scalable message handling framework by using the XML technology and provides a structure for exchange of information through multiple underlying protocols. The framework has been designed to be independent of any particular programming model and other implementation specific semantics.

Application of SOAP Interface

The device supports the XML-based SOAP data interface. By embedding the SOAP requests in the program, you can upload and download the user information, fingerprint data and verification records to and from the device. Furthermore, you can conveniently import the user information, fingerprint data and verification records to the enterprise database or software to meet different software requirements as well as the special needs for personnel management.

IClock-based SOAP Specifications

Convention:

All parameters are transferred in form of <Arg/>. The “<Arg PIN=”2”/><Arg>” in the parameter value is equivalent to “<PIN>2</PIN></Arg>”.

All return values are returned in the form of <Return/>. The return values are returned in the form of attribute values, for example, <Return PIN=”2”/></Return>.

All SOAP requests are submitted by adopting the POST method.

If a fault occurs, the standard SOAP fault code will be returned.

```
<SOAP-ENV:Fault>
<faultcode>500</faultcode>
<faultstring>Internal Error</faultstring>
</SOAP-ENV:Fault>
```

Other faults comply with the HTTP fault status codes.

If the SOAP-XML format submit does not comply with WELL FORMAT or the accessed method name does not exist, the system will return “500 Common service errors”. For example, for the error of access service name, error 404 will be returned in the HTTP header.

Service name: iWsService

This service name specifies the SOAP service to be provided by the Web Server.

HTTP header:

Follow the standard SOAP-HTTP header rules

POST /iWsService HTTP/1.0 'SOAP' service is required

Content-Type: text/xml 'The SOAP resolution format must be specified to be XML.

Content-Length: nnnnn 'The XML size of the SOAP request must be specified.

SOAPAction:"uri:someuri" 'Extended HTTP. It means the URI behind the action domain of the SOAP can be null. For example, the acceptable formats include:

SOAPAction:

SOAPAction:""

SOAPAction:"uri:someuri"

The URI can be any valid domain name.

The server returns the following after responding to the SOAP request:

HTTP/1.0 200 OK '200 means success

Server: WEBSERVER

Content-Type: text/xml

Returned XML-SOAP data

 **Note:** For further development and technical plans, please contact our technical personnel.

10.19 POE Function

1. Overview

Power over Ethernet (POE) is a technology that enables DC power along with data to be provided to the Ethernet-based terminal equipment (such as an IP phone or a wireless LAN access point) without any changes in current Ethernet cabling architecture. A POE system essentially consists of two major components; the Power Sourcing Equipment (PSE), which delivers power, and Powered Devices (PDs), which receive and use the power. POE integrates power and data in the same cabling system, and delivers data and DC power through a Cat5/5E cable.

2. Application

If you connect a device with a built-in POE module to the POE system, the device can work properly by using the power provided by the POE system without any dedicated power adaptor. Thus it not only saves cost but also facilitates cabling and installation. Table 1 lists the definitions of RJ45 wires on the device after the access of the POE module.

Table 1 Pin Definition of RJ45

Pin (socket notch to top; from right to left)	Definition
1	TX+
2	TX-
3	RX+
4	Power

5	Power
6	RX-
7	GND
8	GND

3. Advantages

Cost-effective

A POE system only needs to support one cable. In many cases, the POE system needs to be installed in the places where AC power is hard to deploy. The POE system enables an increasing number of devices over Ethernet to dispense with local power and thus greatly reduces deployment costs and simplifies device management.

Easy-to-install and easy-to-manage

The POE can co-exist with the legacy devices and Ethernet cables on network.

Safe

The PSE only supplies power to the devices that need power supply. The Ethernet cable has a voltage only when the PSE connects with the PD, which eliminates the creep age risk.

Ease of management of network devices

When a remote device connects with a network, the POE can implement remote control, re-allocation or re-set of this remote device.

10.20 Backup Battery (Mini-UPS)

A prerequisite for device's proper work is the normal power supply in any cases. Apart from power adaptors, we also provide 5V and 12V Mini-UPSs which can reduce the impact of power failure as a result of power supply problems on the device operation to the greatest extent.

1. Operating principle

Usually the backup battery remains in idle state, and the power adaptor converts AC to DC power supply for the device. If the backup battery is in non-saturated state, it will charge automatically. In the event of power failure, the backup battery will automatically switch into the discharge state to supply power to the device.

2. Model

1) 5V Mini-UPS

Input: DC5V-2A

Output: DC5V-0.8A

Charge time: ≥ 7.5 H

Discharge time: 3.0 ± 0.5 H

Indicator: The red indicator is on during charge. The green indicator is on when the battery is saturated.

2) 12V Mini-UPS

Input: DC12V/2A

Output: DC7-12V/0.8A

Charge time: ≥ 5.0 H

Discharge time: 3.0 ± 0.5 H

Indicator: The red indicator is on during charge. The green indicator is on when the battery is saturated.

3. Connection mode



Tip: Please first connect the Mini-UPS to the FRP and then charge the Mini-UPS.

4. Storage

During long term storage (over 3 months), keep batteries with 50% of rated capacity (perform charging once every 3 months) and put them in a cool and dry place with an ambient temperature from -10°C – 30°C , far away from erosive substances, fire and heating sources.

5. Precautions for use of batteries

Failure to read the following precautions carefully may lead to battery leakage, overheat, sparking, explosion or rupture.

- Do not connect anode and cathode of the battery directly.
- Do not use batteries in places with ambient temperature over 45°C .
- Do not expose batteries to water or get wet.
- Do not use or store batteries near heating sources (for example, fire or heater).
- Use the original factory charger.
- Do not reverse the positive (+) and negative (-) terminals.
- Do not connect the battery directly to any wall-mounted socket or vehicle-mounted cigarette lighter socket.
- Do not put the battery into fire or apply heat to them. Do not connect anode and cathode of the battery using a conductor or other metal objects to avoid a short circuit. Do not transport or store batteries together with necklaces, hair pins or other metal objects.
- Do not disassemble the battery or form a short circuit.
- Do not strike the battery with any sharp edge parts.

10.21 9-digit Enrollment Number

The standard user IDs supported by the device for user enrollment are 5 digits long (ranging between 1 and 65534). In practice, customers may require user IDs with digits more than 5 digits. We can customize devices supporting 9-digit user IDs to meet your needs.

10.22 Automatic Time Calibration

Considering the huge workload for one-by-one time calibration of multiple devices in a network, you can specify a device or PC in this network as a time server, and set the **Automatic Time Calibration** option of the to-be-calibrated devices to the IP address of the specified time server. Then other devices will automatically connect with this server for time calibration. You only need to ensure that all the devices can access the time server.

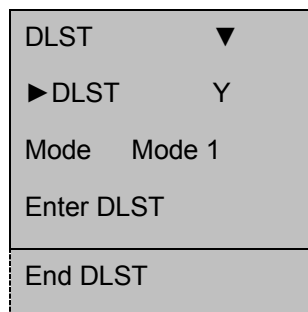
For example, several devices in a network support the automatic time calibration function. Set device A to the time server. The display time of device A is 11:00 on October 28th 2006, and its IP address is assumed "192.168.1.100". You need to set the time of devices in the quantity of M in this network to be synchronous with the device A. Access these devices and select **Menu** → **Options** → **System Opt** → **Adv Option**. In the displayed [Adv Option] interface, check the **Automatic Time Calibration** option and set it to the IP address of the time server. After completing these settings, restart the devices. These devices will automatically search the time server after a period of time to keep synchronous with the time of the time server.

10.23 Daylight Saving Time (Time Zone Settings)

The Daylight Saving Time (DLST) is a widely used system of adjusting the official local time forward to save energy. The uniform time adopted during the implementation of this system is known as the DLST. Typically clocks are adjusted forward one hour in the summer to make people early to bed and early to rise so as to make full use of illumination resources and save electricity. Clocks are adjusted backward in autumn. The specific DLST regulations vary with countries. At present, the DLST system is adopted every year by about 110 countries in the world.

To meet the DLST requirement, the device supports the DLST function to adjust forward one hour at $\times\times$ (Hour): $\times\times$ (Minute) $\times\times$ (Day) $\times\times$ (Month) and backward one hour at $\times\times$ (Hour): $\times\times$ (Minute) $\times\times$ (Day) $\times\times$ (Month).

On the interface as shown in the following figure, you can set the DLST.



To enable the DLST, select **Y** and press **OK**; to disable the DLST, select **N**.

After enabling the DLST, you need to set the events related to the start and end of the DLST. You can set two modes for the DLST format: Mode 1 and Mode 2.


In the default Mode 1, the DLST is set in the format of "Month-Day Hour: Minute".

In Mode 2, the DLST is set in the format of "Month-Week-Specific Day of the Week Hour: Minute".

The value scope of week (WS): 1 – 6. 1 means the first week, 2 the second week and so on and so forth. The value scope of day (WK): 0 – 6. 0 means Sunday, 1 means Monday and so on and so forth.

Let's take 4:00 September 1st 2008 (that is, Saturday of the first week in September 2008) as an example to illustrate these two modes:

MM-DD 24H 9-1 04:00	MM-WS-WK 24H 9-1-6 04:00 WK (0:Sun 6:Sat)
ESC OK	ESC OK
Mode 1	Mode 2

 **Note:** 1. If the month set in the DLST start time is later than that set in the DLST end time, the DLST will span two years, for example, the DLST starts at 2012-9-1 4: 00 and ends at 2013-4-1 4:00.

2. If you select Mode 2 and set the DLST to start on Sunday of the sixth week and current year is 2012, then the system will start the DLST at the specified time point on the last Sunday of current month in 2013 once finding out that there are only 5 weeks in current month.

3. If you set the DLST to start on Monday of the first week in September and current year is 2012, then the system will automatically start the DLST on the first Monday in current month once finding out that the first day is Tuesday instead of Monday in 2013.

10.24 Play Voice within Specified Time Segment (By Time Segment or Group)

When the user operates the device, the device often plays voice prompts. For example, the device voices "Thank you!" after the user passes the fingerprint verification, and voices "Place try again!" if the user fails to pass the verification.

To make the devices more user-friendly, we enable the devices to play the specified voice prompts in response to different user operations.

For instance, if the employee signs in during 6:00–8:00 a.m., the device will voice "Thank you!" but if the employee signs in during 8:00–10:00 a.m., the prompt will become "You are late. Thank you!"

The voice prompts can be set in two ways:

By time segment: The device plays different voice prompts in response to the same operation performed within different time segments.

By group (which is available only on the devices supporting advanced access control functions): The device plays different voice prompts in response to the same operation performed by the users from different groups.

To set voice prompts for different time segments, proceed as follows:

You can set a total of 8 time segment voice prompts for a whole day. Select Menu → Options → System Opt → Adv Option, and select the option TZ Voice. Set the play of voice 001 during 07:00–09:00 a.m. and voice 002 during 10:00–12:00 a.m. as shown below:

TZ Voice	
001	07:00–09:00
002	10:00–12:00
003	00:00–00:00
004	00:00–00:00
005	00:00–00:00
006	00:00–00:00
007	00:00–00:00
008	00:00–00:00

After completing the settings, press OK. These settings will take effect after the device restart.

10.25 Work Code

[Function Description]

The concept of work code is introduced to facilitate the software to handle the verification records according to different cases. For example, we define “1” for eating, “2” for seeing a doctor and “3” for smoking, and input corresponding value when performing a specific action. In this way, the software can easily differentiate among events 1, 2 and 3.

[Operation Description]

You can set the “Work Code” by selecting **Menu** → **Options** → **System Opt** → **Adv Option**. The “Work Code” includes three options: Mode 1, Mode 2 and “None”.

Select “**Mode 1**”, that is, input the work code (one to nine digits) upon the fingerprint verification, and press **OK** to save the records together with the input work code.


Note:

If you press OK without entering any work code upon successful verification, the work code is left to the default value “0”.

If you enter the work code upon successful verification without pressing OK, the work code is left to the default value “0”


If you perform no operation upon successful verification, the device will automatically save the record and leave the work code to “0” five seconds later.

Select “**Mode 2**”, that is, press “▲” and then input the work code (one to nine digits). Press **OK** and then place your finger on the sensor by following the prompt. The records will be saved together with the input work code upon successful fingerprint verification.

 **Notes:** If you forget to press “▲” and perform verification directly, you still can pass the verification, but the work code in the record is “0”.

If you perform no operation of the device after pressing “▲”, the device will return to the initial interface 10 seconds later.

If you select “**None**”, this function is not enabled. And you will not be prompted to enter the work code by the system in response to any of your operations.

 **Notes:** 1. The existing attendance software can save the field to the database when downloading the attendance records, but it cannot handle the work code.

2. The existing offline communication development kit supports the work code for users to handle the work code in the second development. Users can perform classified handling of the records based on the different work codes so as to collect statistics of different events and verification modes.

10.26 DHCP

The Dynamic Host Configuration Protocol (DHCP) provides a framework for allocating dynamic IP addresses to hosts on a TCP/IP network. DHCP consists of two components: server and client. The DHCP server performs centralized management of all the IP network configuration data and handles with the DHCP requests from client. The client uses the IP address allocated by server.

When our device uses the DHCP, it needs a DHCP server and our device works as a client.

If select “**Y**” , after accessing the network, restart the device and the device will send a message to the DHCP server, requesting a dynamic IP address, and a prompt “Acquiring IP address” will be displayed on the screen. The DHCP server will provide a usable IP address and a subnet mask for the device based on the configured address. After the device acquires an IP address, you can select **Menu** → **Options** → **Comm Opt** to query the acquired IP address, subnet mask, and gateway.

If you select “**N**”, the DHCP function won’t be activated. You need to manually input an IP address, subnet mask, and gateway.

10.27 User Grouping

Divide users into different groups. The user needs to first input the number of the group that he/she belongs to and then place his/her finger on the device for recognition. You can also set the unlock time for every group to facilitate the access control management. The system defines 5 groups: Group 1, Group 2, Group 3, Group 4 and Group 5.

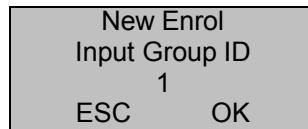
Setting of the “Match by Group” function


On the device supporting this function, select **Menu** → **Options** → **System Opt** → **Adv Option** and set the option **Allow Group** on the “**Adv Option**” interface. If you select **Y**, the user needs to first input the number of the group that he/she belongs to and then place his/her finger on the device for match. If you select **N**, the match by group is deactivated during user verification.

You can set and modify the “**Default Group**” on the “**Adv Option**” interface by selecting **Menu** → **Options** → **System Opt** → **Adv Option**.

User enrollment


If “**Allow Group**” is set to **Y**, the following dialog box will be displayed during the enrollment of a new user. The new user needs to first set the group that he/she belongs to and then enroll the system.



 **Note:** Current group number is a default value. If you want to change this group number, you only need to input a new number.

“Match by Group” mode

When “**Allow Group**” is set to **Y**, the system adopts the “match by group” mode for verification. Therefore, users are divided into different groups and they need to first input the number of the group that they belong to and then place their fingers on the device for verification. For details, see **3.4.1 Fingerprint Verification**.


 **Note:** The users in “Default Group” can directly place their fingers on the device for fingerprint match without inputting their group numbers. The system deems current group as “Default Group” by default.

Group attributes

Select **Menu** → **Options** → **Access Options** → **User Acc Opts**, and on the displayed “**User Acc Opts**” interface, you can view the group that a certain user belongs to and modify related settings, including the group setting, group time segment, user time segment, and so on. For details, see **4.5.3.3 User Access Control Settings**.

View group information

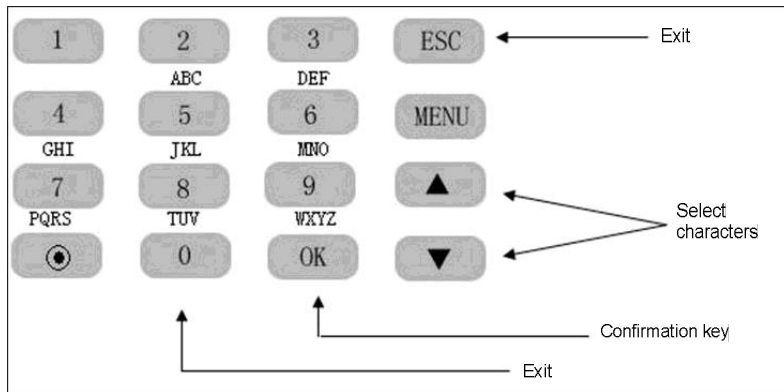
Select **Menu** → **Sys Info** → **Group FP Info** and on the displayed “**Group FP Info**” interface you can view the number of fingerprints contained in every group.

 **Note:** The default fingerprint count is 600 for every group. If you need to modify this capacity, please consult our commercial representatives or pre-sales technical support engineers.

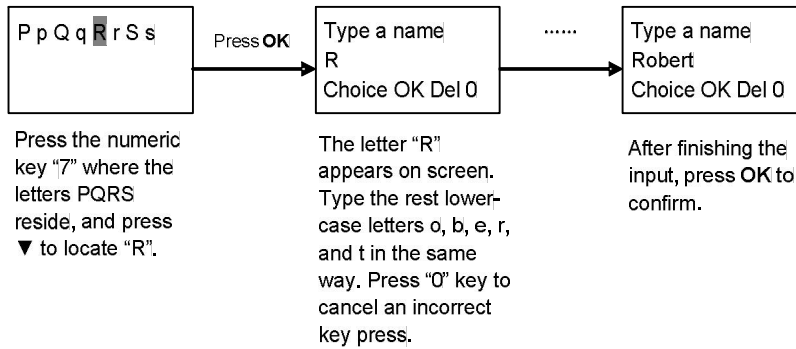
10.28 T9 Input Method

Every of the number keys 2–9 is distributed with 3 or 4 English letters, for example, key 1 has three letters A, B, and C. You only need to type the key for the desired letter once, all the corresponding upper-case and lower-case letters come up. You can press ▲/▼ to choose the desired letter. The user can type his/her name, department name, and work shift by T9 input method.

The keyboard layout of T9 input method is as follows:



For example: To input a user name “Robert”, proceed as follows:



10.29 TTS Function

By use of the TTS technology, the device converts normal language text into the speech that can be output as WAV files. The device dynamically edits and plays the speech so that users can enjoy clear natural voice. Users can modify or customize individualized voice prompts as desired by using PC software.

☺ **Note:** The device supporting 9-digit user IDs must upload user data first and then fingerprint data instead of uploading user and fingerprint data concurrently during the high-speed upload of fingerprint data in RS485 mode.

10.30 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.

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

Unlawful arrest, detention or search of citizens of the People's Republic of China is prohibited; infringement of individual privacy is prohibited.


The personal dignity of citizens of the People's Republic of China is inviolable.

The home of citizens of the People's Republic of China is inviolable.

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 fingerprint recognition actually provides adequate protection for your identity under a high security environment.

10.31 Environment-Friendly Use Description

	<p>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.</p> <p>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.</p>					
	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	○	○	○	×	○	○
<p>○: 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.</p> <p>×: 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.</p> <p>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.</p>						