Black-and-White Screen Series Products User Manual

Version: 3.2.1

Date: Dec. 2011

About This Manual

This manual introduces the interface and menu operations of the black-and-white screen series products. For the product installation, see related installation guide.

Contents

1 Instruction for Use

Thank you for using our black-and-white (B&W) screen series fingerprint recognition terminal (FRT). 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 FRT 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 FRT 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 FRTs outdoors. We recommend you to use the FRT properly so as to achieve the optimal recognition effect and verification speed.

1. Install a B&W screen FRT and then enroll your fingerprint for comparison.

Installation Enrollment Recognition

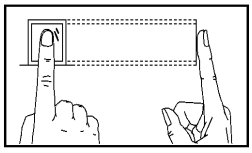
Recognition Installation Enrollment

2. 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).

3. Finger Placement

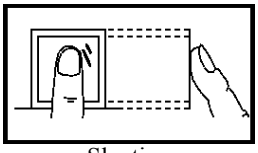
1) Proper finger placement:



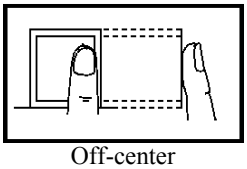
The finger is flat to the surface and centered in fingered guide.

2）Improper finger placement:

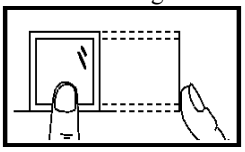
Not flat to the surface



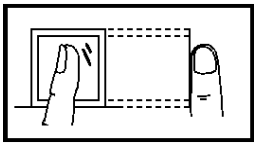
Off-center



Slanting



Off-center



Note:

Please enroll and verify your fingerprint by using the proper finger placement mode to avoid degradation of verification performance due to improper operations. We reserve all rights for the final interpretation and modification of these rules.

4. LED Colors and Their Meanings

B&W screen FRT 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.

---

5. 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 FRTs. 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.
- FRT and FRTs in this manual that means fingerprint terminal (or fingerprint device / machine)

2 Basic Concepts

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

- User enrollment
- User verification
- Match threshold
- User ID
- Authority class

The most important two functions supported by B&W screen series are 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 still perform fingerprint matching even if one or more of his/her fingers get cut or damaged. 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 use any of the enrolled fingerprints for recognition even if he/she forgets which fingerprint has been enrolled.

2.2 User Verification

When a user enters a password after placing his/her finger on the fingerprint reader, or scans his/her fingerprint after entering an ID number, the B&W screen FRT compares the newly scanned fingerprint with a fingerprint stored in template. The fingerprint template is used to check the user ID. If a user enrolls his/her fingerprints on an FRT, the user can keep attendance records on this FRT through fingerprint verification which takes about 2 seconds. Upon verification, the system displays a prompt about whether the verification succeeds or not and then stores the successful matching record in the B&W screen FRT.

2.3 Match Threshold

The match threshold is set to achieve a trade-off between the possibilities of false rejection and false acceptance. The false acceptance means the fingerprint recognition device mistakes the fingerprint of user A for that of user B, while the false rejection means the fingerprint recognition device refuses to recognize an enrolled fingerprint.

You can set a match threshold for all users. For fingerprints that fail to pass the verification, you can adopt the "ID + Fingerprint" verification mode (that is, 1:1 match) so that the system adopts the data set in 1:1 match threshold when matching the fingerprints.

If a user's fingers are severely worn out or damaged, lower the match threshold (**see Table 3-1**).

☺ **Note**: The false acceptance rate (FAR) and false rejection rate (FRR) mutually influence each other. Reducing the FAR will increase the FRR, and vice versa. The default match threshold is **35** and the default 1:1 match threshold is 15. **Table 3-1** lists the settings of match thresholds in different scenarios.

Table 2-1 Match Threshold

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

2.4 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).

2.5 Authority Classes

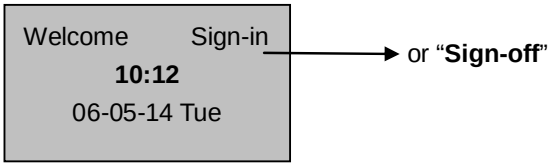
The B&W screen series FRTs include four authority classes:

- Users: refer to those who are required to verify their identity for a purpose, for example, opening the door through the B&W screen FRT or keeping their entry/exit records.
- Registrars: refer to the users who are granted the right to enroll or delete users.
- Administrators: refer to the users who are granted the right to perform all operations except performing advanced settings and enrolling administrators and super administrators.
- Super administrators: refer to users who have access to all system functions and modify all system settings.

Note: When the super administrators are not enrolled, the registrars can enroll the administrators and super administrators. Similarly, the administrators can enroll super administrators in the absence of super administrators. Once super administrators are enrolled, administrators of lower class cannot enroll those of higher class.

2.6 Main 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. Further, it describes how to verify the validity of enrolled fingerprints.

This chapter includes the following parts:

- ✧ Enroll users
- ✧ Check enrollment effects
- ✧ Enroll spare fingerprints
- ✧ Verify identity.
- ✧ Prompts for successful enrollment

Note:

To enroll a new user, you must have the authority of a registrar, administrator or super administrator. For details, see 2.5 Authority Classes.

3.1 Enroll a User

If no administrator has been enrolled, any user has the right to enroll a new user. If an administrator has already been enrolled, you can only enroll a new user after passing the administrator verification.

The RFT supports the following three enrollment modes that respectively apply to the general public with three different types of fingerprint quality:

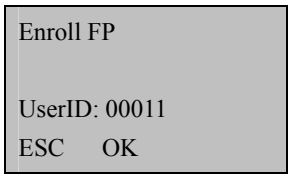
- Fingerprint enrollment: This enrollment mode applies to the majority of the general public with good quality fingerprints.
- Fingerprint + Password enrollment: This enrollment mode applies to a small portion of the general public who can enroll their fingerprints successfully but have difficulty in fingerprint verification due to their poor fingerprint quality.
- Password enrollment: This enrollment mode applies to about one percent (the actual number may vary slightly) of the general public who are unable to enroll their fingerprints successfully.

If an administrator has already been enrolled, you need to verify the administrator identity by pressing **MENU**. The system then prompts you to swipe your finger or enter a password for administrator verification.

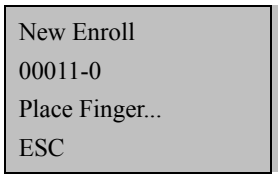
Note: If no administrator has been enrolled, administrator verification is not required.

3.1.1 Enroll a 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.

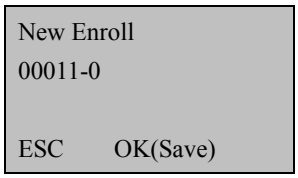


2) Input a number (from 1–65534) in the [User ID] field. Press **OK** for 3 seconds to display the fingerprint enrollment interface.



Note: The last digit "0" in "000011-0" denotes the first fingerprint.

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.

Notes:①The FTP displays 5-digit numbers, and automatically adds 0 as prefix to the numbers less than 5 digits. For example, if you input "11", the FRT will display "00011".

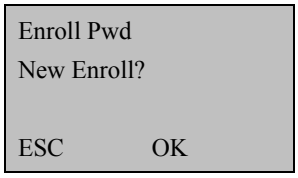
②Enrollment number could only be input in order before, but now for technology updating, you can freely enter the number with maximum to 65534.

③For non-numeric key models, such as F6, you can use the "▲" or "▼" key and the "OK" button to input the enrollment number.

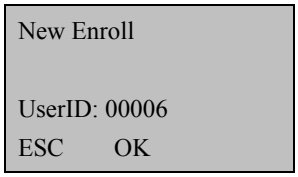
Operations: on the fingerprint enrollment interface → press "▲" or "▼" key to select the digit you want to enter, such as the "hundreds place" → press "OK" button - press "▲" or "▼" key to select the number you want to enter →press "OK" button, then move to the "ten place", as the operation above → press "OK" button for 3 seconds to confirm the enrollment.

3.1.2 Enroll a Password

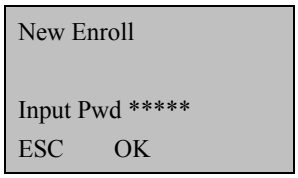
1) Select **Menu → User Manage → User Enrollment** to display the [User Enrollment] interface. Select [Enroll Pwd] and press **OK** to display the [Enroll Pwd] interface.



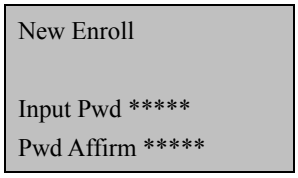
2) Press **OK** to confirm and proceed.



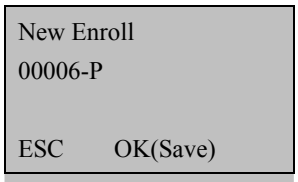
3) Input a number (from 1–2147483646) in the [User ID] field. Press **OK** to display the password input interface.



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.

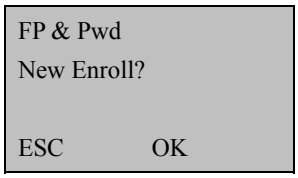


Note: The last digit "P" in "00006-P" denotes password.

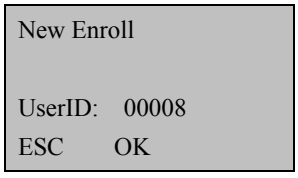
6) Press **OK** to save the enrolled data and exit the password enrollment.

3.1.3 Enroll Both Fingerprint and Password

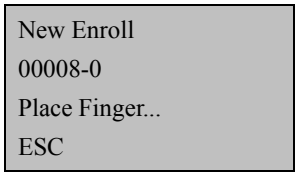
1) Select **Menu → User Manage → User Enrollment** to display the [User Enrollment] interface. Select [FP&Pwd] and press **OK** to proceed.



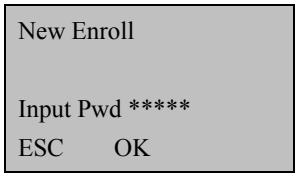
2) Press **OK** to confirm and proceed.



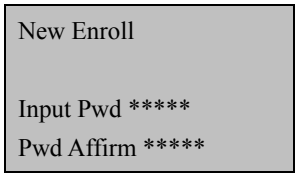
3) Input a number (from 1–65534) in the [User ID] field. Press **OK** to display the fingerprint enrollment interface.



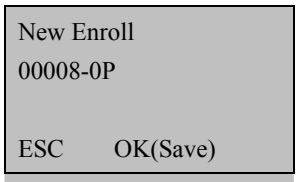
4) Place the same finger for three consecutive times on the fingerprint reader according to system prompts. If the enrollment succeeds, the following information is displayed:



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



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

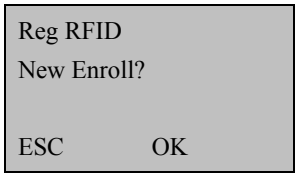


Note: The second digit "0" from the bottom in "00008-0P" denotes one fingerprint, and the last digit "P" denotes password.

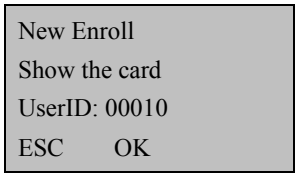
7) Press **OK** to save the enrolled data and complete the fingerprint and password enrollment.

3.1.4 Enroll an ID Card★

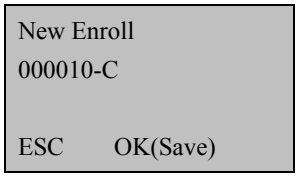
1) Select **Menu → User Manage → User Enrollment** to display the [User Enrollment] interface. Select [Reg RFID] and press **OK** to proceed.



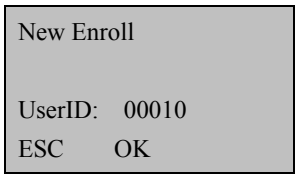
2) Press **OK** to confirm and proceed.



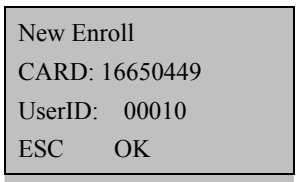
3) Input a number (from 1–65534) in the [User ID] field. Press **OK** to display the ID card enrollment interface.



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



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



Note: The last digit "C" in "00010-C" denotes ID card.

6) Press **OK** to save the enrolled data and complete the ID card enrollment.

Note:

The ID card verification is an optional function. To customize an ID-card-capable FRT, please consult our commercial representatives or pre-sale technical support engineers.

3.1.5 Enroll an HID Card★

The enrollment procedure of HID cards is the same as that of ID cards.

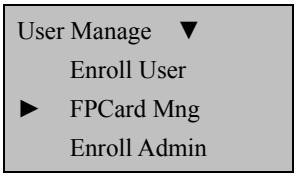
The standard HID card adopts the ID of dedicated format and the facility code for encryption.

Note:

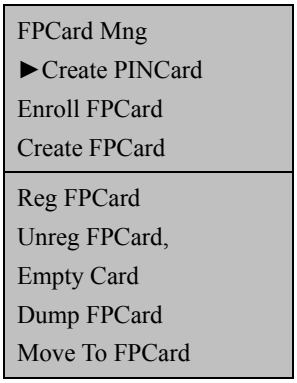
The HID card verification is an optional function. To customize an HID-card-capable FRT, please consult our commercial representatives or pre-sale technical support engineers.

3.1.6 Enroll a Mifare Card★

1) Select **Menu → User Manage → FPCard Mng** to display the [FPCard Mng] interface.



2) Press **OK** to proceed. The following information is displayed:



Create PINCard: Create a PIN card for every user enrolled in FRT. Users can log attendance records by using their PIN cards instead of fingerprints.

Enroll FPCard: Fingerprints are stored directly in users' PIN cards instead of the FRT. Users can verify their IDs by using "cards and fingerprints", that is, swiping their PIN cards and then placing their fingers on the fingerprint reader.

Create FPCard: Duplicate the enrolled fingerprints (from the FRT) to the user's PIN card to create a fingerprint card (FP card) so that users can verify their IDs by using their "fingerprints" or "cards and fingerprints".

Reg FPCard: To use an FP card of an FRT on another FRT, you must register a new FP card on current FRT.

Unreg FPCard: To prohibit the use of an FP card on an FRT, you must deregister this card from this FRT.

Empty FPCard: Delete all the data (fingerprints and numbers) of the FP card.

Duplicate FP in Card: After duplicating the fingerprints from an FP card to the FRT, you can verify user ID through fingerprints.

Transfer FP to Card: If the fingerprints in an FRT are transferred to an FP card, these fingerprints will only exist in this FP card and no longer present in the FRT.

Note:

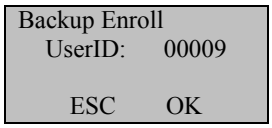
The Mifare card verification is an optional function. To customize a Mifare-card-capable FRT, please consult our commercial representatives or pre-sale technical support engineers. For details, see *Mifare Card User Guide*.

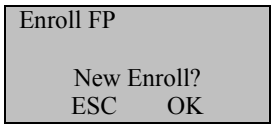
3.2 Check Enrollment Effect

After enrolling a fingerprint, you need to verify its validity by placing your corresponding finger properly on the initial interface of the FRT. If the FRT recognizes your fingerprint successfully, it proves that your fingerprint is clear and recognizable; otherwise, you need to re-enroll your fingerprint or change another finger for enrollment. If it still does not work, it proves that your fingerprints are not suitable for recognition and you need to adopt the fingerprint and password verification mode.

3.3 Backup Enrollment

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





The following steps of backup enrollment are the same with those of new enrollment, while the only difference is the "New Enroll" on the top right corner changes into "Backup Enroll".

Note: It is recommended that a long-term user should enroll at least two fingerprints.

3.4 Verification Modes

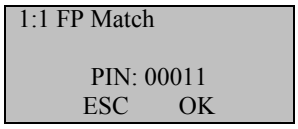
3.4.1 Fingerprint Verification

You can adopt 1:1 and 1:N matching modes for fingerprint identification.

(1) 1:1 fingerprint matching (ID + fingerprint)

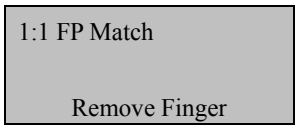
In the 1:1 fingerprint matching mode, the FRT compares the current fingerprint collected through the fingerprint reader with that in relation to the user ID entered through keyboard.

Operation steps:

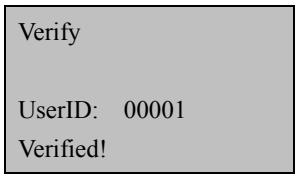


Enter a user ID through keyboard on the initial interface.

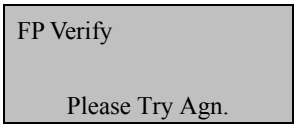
Note: The FRT displays 5-digit numbers, and automatically adds 0 as prefix to the numbers less than 5 digits. For example, if you input "11, the FRT will display "00011".



Press **OK** and then place your finger on the fingerprint reader, or 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:



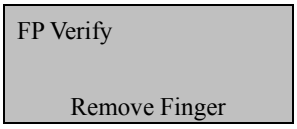
If the verification fails, the system will generate a voice announcement "Please try again!" and display the following interface:

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

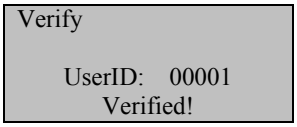
(2) 1:N fingerprint verification

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

Operation steps:

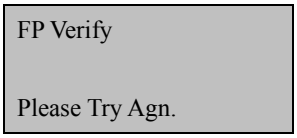


Place your finger on the initial interface to display the following interface:



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:

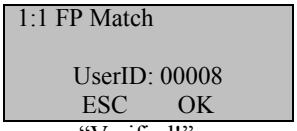
If the verification fails, the system will generate a voice announcement "Please try again!" and display the following interface:



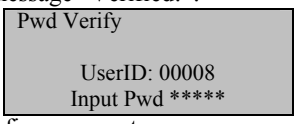
After the above interface is displayed 0.5 seconds, the system will return to the initial interface.

3.4.2 Password Verification

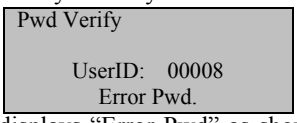
Input your ID on the initial interface.



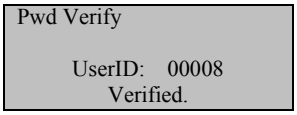
Press **OK** and the system displays a prompt message "Verified!".



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



If you enter a wrong password, the system displays "Error Pwd" as shown below and returns to the password input interface:



3.4.3 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.

3.4.4 Mifare Card Verification★

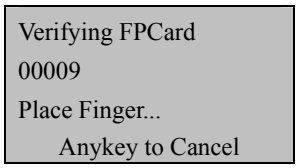
If you use your PIN card for Mifare card enrollment, you need to select **Menu → Options → System Opt → Adv Option** to display the [Adv Option] interface. Select the "**Card Only**" option through the "▲/▼" key, and set this option to **Y**.

Swipe your PIN card at the swiping area on the initial interface to display the following interface (Do not place your card too far from the swiping area; otherwise, your card may not be sensed.):

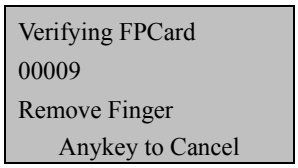
If you adopt other modes (for example, FP card) for Mifare card enrollment and set the "**Card Only**" option to **Y**, the verification process is the same with the above.

If you set the "**Card Only**" option to **N**, the verification process is as follows:

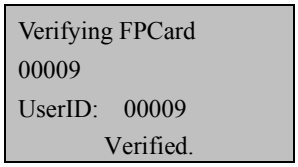
Swipe your PIN card at the swiping area on the initial interface to display the following interface (Do not place your card too far from the swiping area; otherwise, your card may not be sensed.):



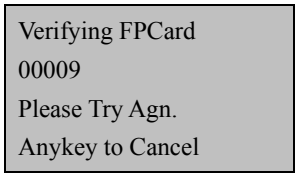
Place your finger on the fingerprint reader and the following interface is displayed:



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.

Note:

Besides the verification modes above, the B&W screen FRT also provides other modes. For details, see Appendix Multiple Verification Modes. If you need other verification modes, please consult our commercial representatives or pre-sales technical support engineers.

3.5 Prompts for Successful Enrollment

A high fingerprint enrollment quality assures quick verification speed, while a poor fingerprint enrollment quality may easily lead to false rejection and slow verification.

To enhance the quality of enrolled fingerprints, refer to Table 4-1

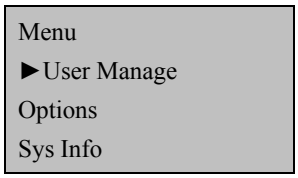
Table 3-1 Common Causes of Enrollment Failure or Poor Fingerprint Quality

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.

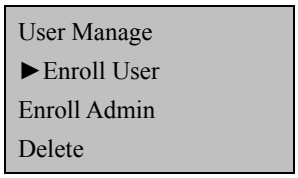
3.6 Administrator Enrollment

The B&W screen FRT provides administrator settings to prevent unauthorized users changing system data and ensure system security. The operations on administrator settings are as follows:

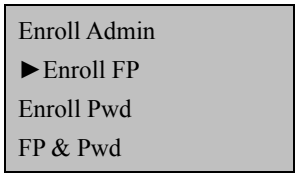
1) The brand new FRT does not assign any administrator, so you can press **Menu** to access the system directly and the following interface is displayed.



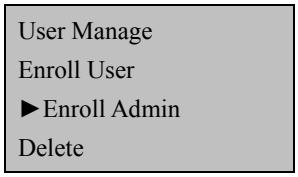
2) Press **OK** to display the [User Manage] interface.



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



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

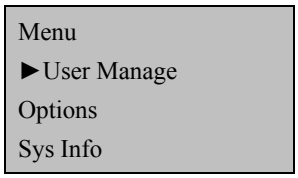


5) Select an enrollment mode and press **OK** to display the administrator enrollment interface. Administrator enrollment includes three modes: Enroll Recorder, Enroll Ordinary Admin, and Enroll Super Admin. For details, see 3.1.5 Authority Class. The enrollment mode of administrator is consistent with that of a new enrolled user. For details, see 4.1 Enroll a User.

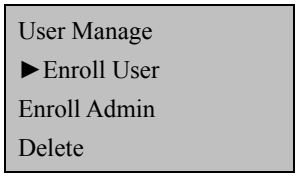
3.7 Delete Enrollment Data

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

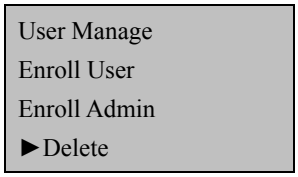
1) Press **Menu** to access related menu item for verification, and the following interface is displayed:



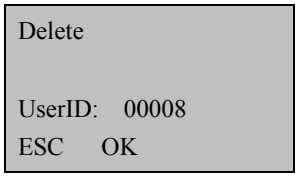
2) Press **OK** to display the [User Manage] interface.



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. There are such items in the "Advanced Settings" on some models of devices. for detail please refer to“4.1.7Advanced Settings”.

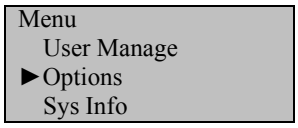
Such deletions can also be executed by " Access Control Management Software ". Steps as below: Open the “ Access Control Management Software”, Click “Basic settings”-- “Device management” -- “others” -- “read options” at bottom (can read all data of connection machine) -- “Clear Admin’ Privilege”.

Deleting "All Users" can also be executed through the "Equipment Management" menu. Therefore, all depends on users' need and their actual models of Products.

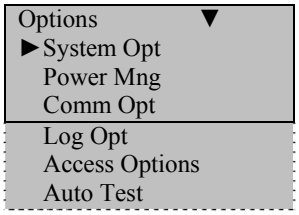
---

4 Settings

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



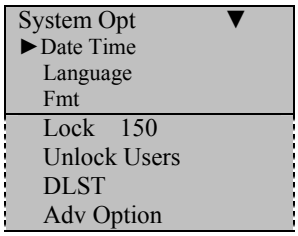
Select **Options** and press **OK** to proceed.



The **Options** menu contains six submenus: **System Opt**, **Power Mng**, **Comm Opt**, **Log Opt**, **GPRS** (Only professional access control devices provide this setting), and **Auto Test**. These submenus will be described in the following part.

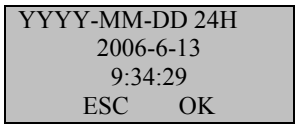
4.1 System Settings

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



4.1.1 Time Settings

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

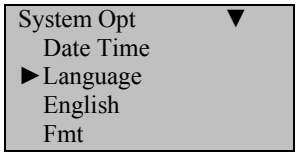


To modify date and time, place the cursor to the desired field through the ▲/▼ key, input correct date and time, and press **OK** to save the changes.

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 FRT 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 FRT screen. Select **Format** and press **OK** to display the format setting interface. Select a desired date format through the ▲/▼ key. The FRT 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.

Welcome Sign-in **10:12** 05/14/06 Tue	Welcome Sign-in **10:12** 06-05-14 Tue

4.1.4 Lock Driver Duration★

The lock driver duration refers to the duration within which the electric lock is opened upon the fingerprint verification. 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.

The unit of quantity for this duration is 20 ms and you can set it to 254 at most, that is, 5.08s.

To disable this function, set the duration to "0".

Note:

This parameter is only available for the FRTs with the simple access control function. For FRTs with professional access control function, this parameter is contained in the access control settings.
The unit of quantity and the maximum value of this parameter here are standard configurations. If you need larger parameter values, please consult our commercial representatives or pre-sales technical support engineers.

4.1.5 Number of Users★

To set the number of users required to unlock the FRT, select **Unlock Users** and press **OK**. Then enter a desired number through the numeric pad, and press **ESC** to exit and save the setting.

This parameter is set to 1 by default, that is, the FRT sends the lock control signal as long as one user passes the verification. If it is set to 3, then the FRT sends the lock control signal only after all these three users pass the verification and the verification interval cannot exceed 30s. This parameter can be set to 5 at most.

Note:

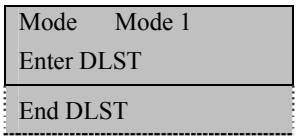
This parameter is only available for the FRTs with the simple access control function.

4.1.6 Daylight Saving Time (DLST) ★

Select Menu → Options → System Opt → DLST to set the "DLST".

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

DLST	▼
►DLST	Y



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

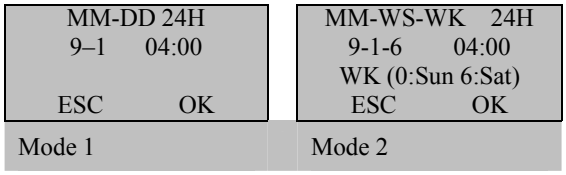
After enabling the DLST, you need to set the events related to the start and end of the DLST. You can set two modes for the DLST format: Mode 1 and Mode 2.

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:



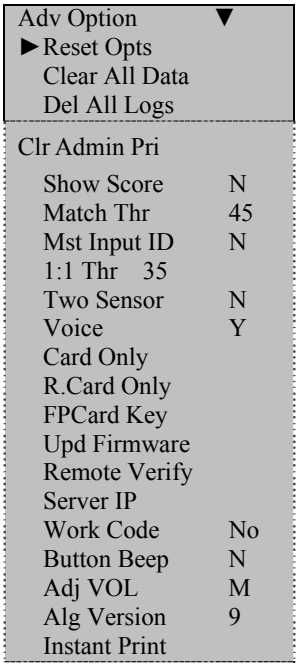
Note: 1. If the month set in the DLST start time is later than that set in the DLST end time, the DLST will span two years, for example, the DLST starts at 2007-9-1 4: 00 and ends at 2008-4-1 4:00.

2. If you select Mode 2 and set the DLST to start on Sunday of the sixth week and current year is 2007, then the system will start the DLST at the specified timepoint on the last Sunday of current month in 2008 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 2008, 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 2009.

4.1.7 Advanced Settings

Through the advanced settings, you can perform such operations as restoring factory defaults, clearing management rights, deleting attendance records, clearing all data, setting match thresholds and setting voice prompts, as shown below:



Anti-PB	No

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**) Clear All Data**

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

3) Del All Logs

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

4) **Clr admin pri**

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

5) **Show Score**

This option is used to set whether to display the fingerprint quality value on the top right corner of the screen.

(Note: The setting of this option affects the image capture speed of the FRT.)

6) **Match Threshold**

This option is used to set the extent of matching between an input fingerprint and that stored in templates. For details, see **2.1.3** Match Threshold.

7) **Mst Input ID**

This option is used to set whether the user must input an ID number before fingerprint matching. If you select Y, you must input an ID number before 1:1 fingerprint matching; if you select N, you do not have to input an ID number before 1:1 fingerprint matching.

8) **1:1 threshold**

This option is used to set the extent of matching between an input ID/fingerprint and that stored in templates in the ID and fingerprint identification mode. For details, see **2.1.3** Match Threshold.

9) Two Sensor★

If you select Y, you can install an external fingerprint sensor through the USB interface and use this external sensor together with the fingerprint reader accompanied with the FRT. If you select N, you cannot install any external fingerprint sensor. For details, see Appendix External Connection with the Fingerprint Reader.

10) Voice★

This option is used to set whether to play voice prompts during the operation of the FRT. Select Y to enable the voice prompt, and select N to play beep sound only.

11) Upd firmware

You can select “Upd Firmware” to upgrade the firmware of an FRT 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.

12) Card Only★

If you select Yes, you only need to verify your ID card. If you select No, you need to verify both your ID card and fingerprint.

13) R.card Only★

If you select Y, you must swipe a card registered on the FRT for verification. If you select N, you do not need to swipe a registered card.

14) FPCard Key★

When you set a value for this parameter, you set a password for your FP card and the FRT will write this password in your enrolled FP card.

15) Remote Verify★

After Remote Verify is set to Yes, the FRT can be used for verification on the background server.

You can select the following four verification modes:

LO: Local verification only. Only the fingerprints that have been enrolled on local FRT can pass the verification.

NO: Remote verification only. The FRT only searches the remote database for matched fingerprints.

LN: Local verification comes before remote verification. The FRT first searches local database for matched fingerprints and then the remote database if it fails to locate matched fingerprints in local database.

LN: Remote verification comes before local verification. The FRT first searches remote database for matched fingerprints and then the local database if it fails to locate matched fingerprints in remote database.

16) Server IP★

This option is used to set the IP address of the RIS server.

17) Work Code★

This option is used to set whether to use the work code and to set the mode of work code. There are three options: None, Mode1, and Mode2. For details, see Appendix Work Code.

18) Keypad tone★

This option is used to set whether to generate a beep sound in response to every keystroke. Select Y to enable the beep sound, and select N to mute.

19) Adj VOL★

This option is used to adjust the volume of the keypad tone among High, Medium and Low.

20) Alg Version

This option is used to set the version number of the fingerprint algorithm. Select 9 to adopt algorithm version 9.0 and 10 to adopt algorithm version 10.0. Please select the algorithm version with caution because the fingerprint templates of these two algorithm versions are incompatible.

Note: some of the device will be prompted to remove the user information and attendance data when change the algorithm. So we proposed to back up user information and attendance data before change the algorithm.

21) Imdt Prt (Immediate Print) ★

After this option is set to RS232, the FRT outputs the verification information each time after successful verification to the serial port. The verification information can be directly printed if the serial port is connected with a printer. The verification information can be viewed through a HyperTerminal. For the cable connection between the serial port and printer, see Appendix Print.

22) Anti-Passback★

This option has four values: None, Exit, Entry and Entry and Exit. For details, see Appendix Anti-Passback.

Note:

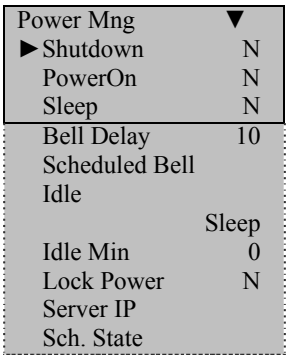
1. The options **Two Sensor** and **Upd Firmware** are available only on the USB-capable FRTs.
2. The option **Card Only** is available only on the Mifare-card-capable or ID-card-capable FRTs.
3. The options **R.card Only** and **FPCard Key** are available only on the Mifare-card-capable FRTs.
4. The options **Remote Verify** and **Server IP** are available only on the RIS-capable FRTs.
5. The options **Keypad Tone** and **Adj VOL** are available only on the FRTs that adopt the URU sensor.
6. The option **Work Code** is available only on the FRTs that support the work code feature.
7. The option **Imdt Prt** is available only on the print-capable FRTs.
8. The option **Anti Passback** is available only on the anti-passback-capable FRTs.

4.2 Power Management★

Through power management, you can set the timing power-on/shutdown, power-on/shutdown time, lock power key, and timing state switching.

4.2.1 Power Settings

Press **Menu** to access system menu. Select **Options → Power Mng** to display the following interface.

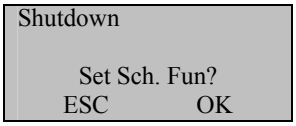


The B&W screen FRT adopts an intelligent power management system and supports such functions as timing power-on/shutdown and sleep timing.

1) Shutdown

This option is used to automatically shut down the FRT at specified time.

Select **Shutdown** and press **OK**.



Press **OK** to set the automatic shutdown time. Press **ESC** to disable the automatic shutdown function.

After setting the time, press **OK** and the timing shutdown function is enabled.

2) PowerOn

This option is used to automatically power on the FRT at specified time. The settings of timing power-on are similar to those of timing power-off.

3) Sleep

This option is used to set the FRT to automatically enter sleep mode at specified time. You can wake up the FRT from sleep mode by pressing any key. The setting steps of this parameter are similar with those of timing shutdown.

4) 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.

5) Scheduled Bell & Bell Delay★

There are 8 time segments available every day of a week. You can set the alarm time as required. The FRT will automatically alarm at the specified time every week and stop the alarm after the alarm duration times out.

6) WEB SERVER IP★

This option is used to set the IP address of the web server.

7) Adj VOL★

You can adjust the MP3 playing volume as required.

8) Lock Power★

If you set this option to Y, the power-off key on the keyboard cannot be used, and the option Power-Off is displayed under the menu. If you set the option to N, the power-off key on the keyboard can be used.

Note:

1) If you have not found this Option, shutdown, Power on, it belongs to the normal state. Only some device have the time state selection function, if you have any question, please contact our technician.

2) Web Master IP setting is valid unless the fingerprint device own playing MP3 function. Please refer to Appendix MP3 Function Introduction.

3) Time ring and the duration of ringing only belong to these fingerprint device with Time ring and Playing MP3 function.

4) Only the device with a power key, the Lock power button function is available.

5) For some type of devices, when you set the time of shutdown, power on or sleep, please press Menu key for confirm.

4.2.2 Timing State Switching★

State switching: Different attendance states need to be recorded in different time segments, so there are 6 state keys on the keyboard to switch between different states for the FRT of some models. You need to change the state manually by pressing related status key. To use an attendance state, press related state key. To reduce manual operations, a timing state switching option is provided.

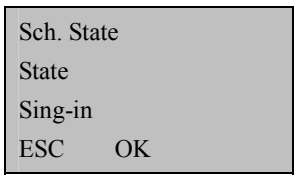
Definition of Timing State Switching

The FRT automatically switches the attendance state at the specified time. Current attendance state is displayed on the initial interface.

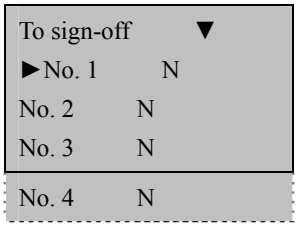
Setting of Timing State Switching

Set state switching time

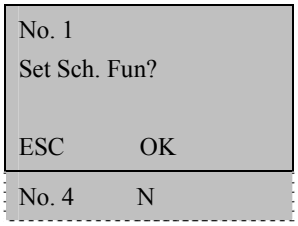
1. Select **Menu → Options → Power Mng → Sch. State** to display the following interface:



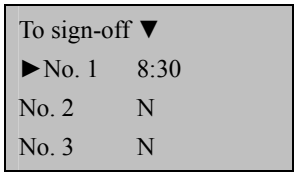
2. Select an attendance state through the ▲/▼ key from sign-in, sign-off, sign-in for overtime work, and sign-off for overtime work. Press **OK** to set the selected state. Take ”sign-off” as an example:



3. Select the time for setting, for example, select 1 and press **OK**.

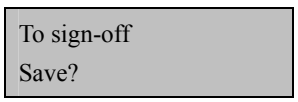


4. In the displayed interface as shown below, input a number, for example, 8:30, as the sign-off time through the keyboard.



5. Select the time for setting through the ▲/▼ key, with the similar operation as Step 4.

6. After completing the setting, press **ESC** to exit. When prompted to save your settings, press **OK** to confirm or press **ESC** to cancel.

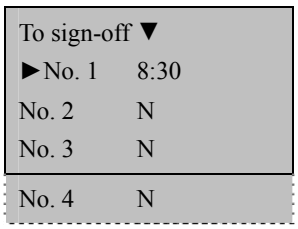


7. If you save your settings, these settings will take effect and the attendance state will change into "sign-off" at the specified time.

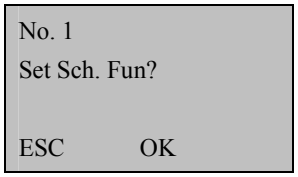
Cancel the set state switching time

Display the set state switching time interface to cancel the above "Sign-off" time setting.

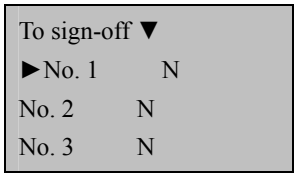
1. Select **Menu → Options → Power Mng → Sch. State**, and select "Sign-off" as shown below:



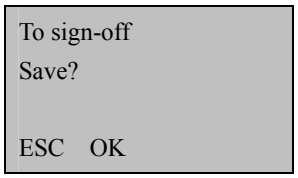
2. To cancel time 1, select time 1 and press **OK**.



3. Press **ESC** to cancel time 1.



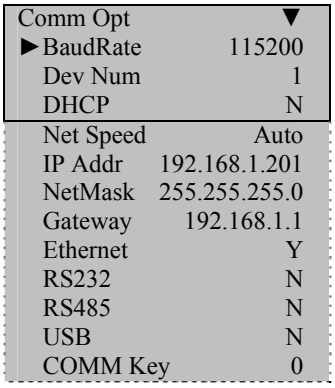
4. After completing the setting, press **ESC** to exit. When prompted to save your settings, press **OK** to confirm or press **ESC** to cancel.



5. If you save your settings, these settings will take effect and the "Sign-off" switching time 1 will be cancelled.

4.3 Communication-related Settings

Select **Comm. Opt** and the information displayed on the screen is shown in the following figure:



1. BaudRate

This option is used to set the baud rate for the communication between the FRT 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. Dynamic Host Configuration★

If this option is set to Yes, the FRT requests the DHCP server on the network to dynamically assign an IP address.

4. IP Addr★

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

5. Net speed★

This parameter refers to the network rate, including five options: ATUO, 10M-F, 10M-H, 100M-F and 100M-H. "10M-F" is recommended for the ZEM100 product series and "AUTO" is recommended for the ZEM200 product series.

6. Net Mask★

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

7. Gateway★

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

8. Ethernet★

This parameter is used to set whether to adopt the Ethernet for communications. To adopt the Ethernet, set this parameter to Y; otherwise set it to N.

9. RS232

This parameter is used to set whether to adopt the RS232 for communications. To adopt the RS232, set this parameter to Y; otherwise set it to N.

10. RS485

This parameter is used to set whether to adopt the RS485 for communications. To adopt the RS485, set this parameter to Y; otherwise set it to N.

11. USB★

This parameter is used to set whether to adopt the USB for communications. To adopt the USB, set this parameter to Y; otherwise set it to N.

12. COMM Key

When the password is set to 0, no password is required for communication; when the password is set to a non-zero value, this value is required for communication connection.

13. Extern MODEM★

If this option is set to **Y**, the FRT can access network through a Modem. For details, see Appendix Modem.

Note: 1. The option **Ethernet** is unavailable on the FRTs with the two options **Gateway** and **Net Mask**, and the Ethernet function is enabled by default; for the FRTs without the two options **Gateway** and **Net Mask**, the option **Ethernet** is available and must be set to **Y** before the use of Ethernet communications.

2. After finishing the settings above, you need to restart the FRT to enable the settings.

4.4 Log Settings

Select **Log Opt** and the information displayed on the screen is shown in the following figure:

1. Alm AttLog

When the available space for storage of attendance logs reaches the specified value, the FRT automatically generates an alarm.

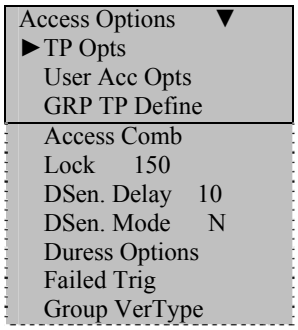
2. Recheck Min

If a user's attendance record already exists and the user checks in again within the specified period (unit: minute), his/her second attendance record will not be stored.

4.5 Access Options★

The access control settings are valid for the FRTs with professional access control functions. The menu item "Access Options" is inexistent in the fingerprint time attendance machines and the devices with simple access control functions.

Select **Access Options** and the information displayed on the screen is shown in the following figure:



The **Access Options** includes the following options:

1. Def TP

Define the unlocking time segments every day of a week.

2. User Acc Opts

Set the unlocking time, the group that the user belongs to, and the unlocking combination.

3. GRP TP Define

Define the available time segments for users of a certain group to unlock.

4. Access Comb

Define diverse unlocking combinations. Each combination is composed of different groups.

5. Lock

Set the duration from successful fingerprint matching to unlocking.

6. 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.

7. 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.

8. Duress Options★

Set the automatic alarm function to prevent enrollment under duress. In times of duress, the system will silently send a duress signal after a period of time when a fingerprint passes the match.

9. Failed Trig★

The system automatically generates an alarm when the number of consecutive verification failures exceeds the upper limit.

10. Group VerType★

Set the verification type adopted by the user in a group.

Note:The "Group VerType" option is available only for the devices supporting 14 verification modes. To customize this function, please consult our commercial representatives or pre-sales technical support engineers.

4.5.1 Access Control Function Description

The access control setting items include the user's access time segments and access combinations.

The setting items for each user include: the group that the user belongs to, and the available access time segments for group and user. User grouping means the allocation of a user to a certain group, for example, Group 1 or Group 2. A group or user can be set with three preset access time segments at most, and these time segments have an "OR" relation with one another (that is, unlocking is available for a group/user at any one of these time segments). For details on the relationship between the use of group TSs and the user TPs, see 4.5.3.3 User Access Control Settings.

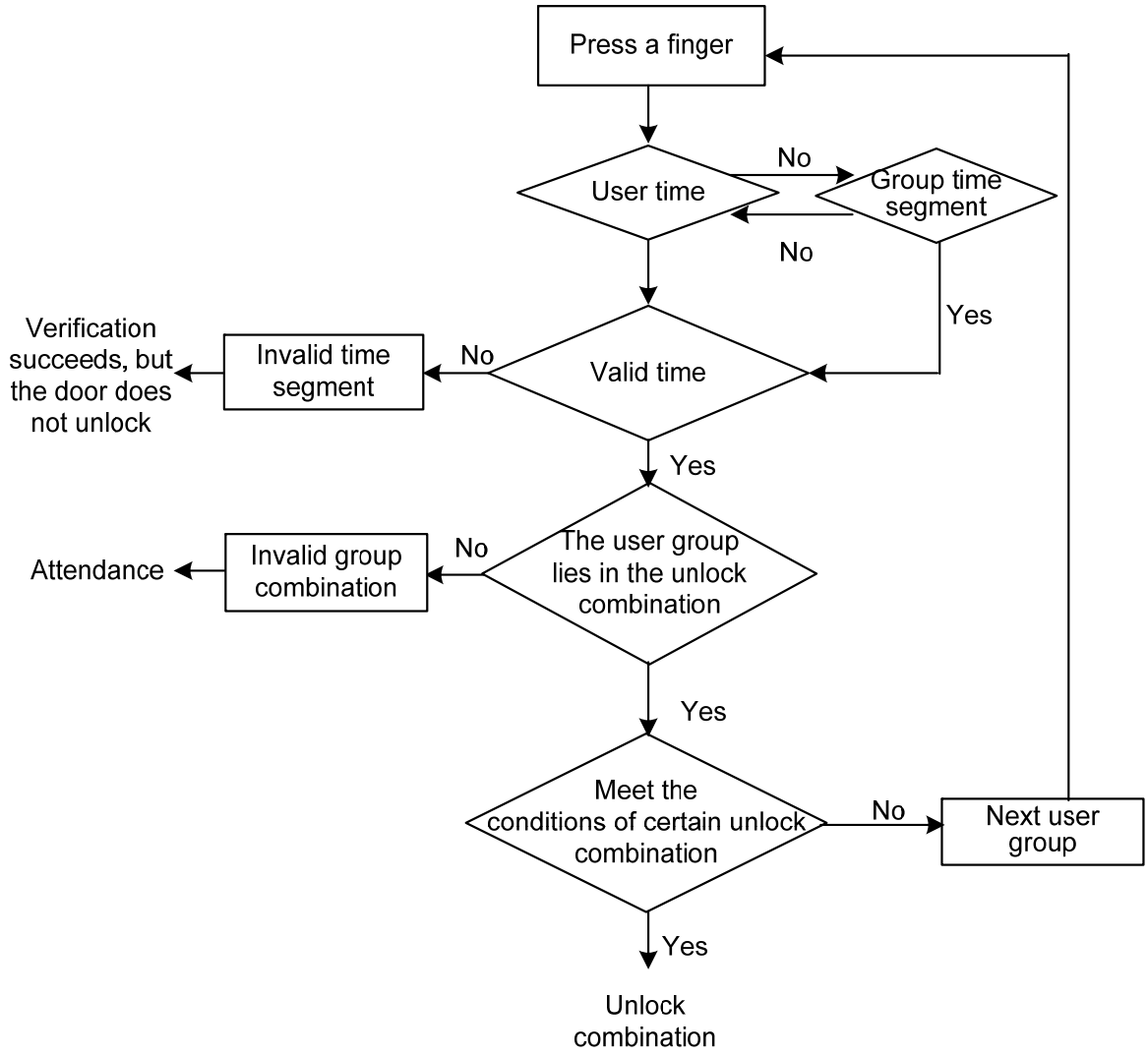
In a simple word, the unlocking conditions for an enrolled user are as follows:

1. The group to which the user belongs must lie in an access combination (or it can share the same access combination with other groups and unlock together with them).

2. The current unlocking time must remain within any one of valid access time segments.

Newly enrolled users are classified into Group 1 by default. The default group time segment is "1". When Group 1 and time segment 1 both adopt factory defaults, the newly enrolled users are in Open state. (If a user modifies the access control settings, the system will also change these settings accordingly.)If the group to which a user belongs is inexistent in access combination settings, the user can only mark his/her attendance but cannot unlock.

4.5.2 Access Control Verification Flow



4.5.3 Function Introduction

4.5.3.1 Define Time Segments

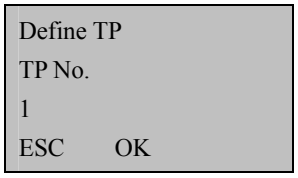
Time segment is the minimum time unit for access control setting. The entire system can be defined with a maximum of 50 time segments. Each time segment is divided into 7 time buckets, that is, one week. Each time bucket is the valid time segment within 24 hours every day. Every user can be set with up to 3 time segments which have an "OR" relation with one another. The verification time is deemed valid only if it remains within one of these time segments. The time bucket format is **HH:MM-HH:MM** using a 24-hour clock.

If the end time is earlier than the start time (23:57–23:56), unlock is prohibited for a whole day. If end time is later than the start time (00:00–23:59), unlock is valid within this time bucket.

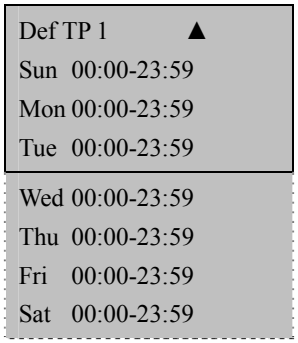
Valid time segments for unlock: whole day (00:00–23:59), or the period from start to end time.

✍ **Tip**: The default time segment 1 indicates the whole day access (that is, the newly enrolled users are allowed to unlock).

Select **Define TP** to display the following information:



Press **OK** to display the **Define TP1** interface as follows:



The TP1 above is defined as whole day access, that is, the factory default.

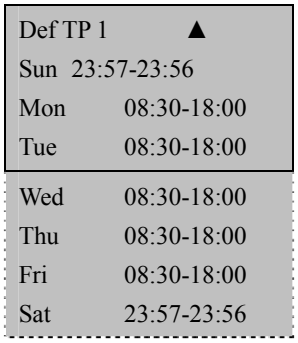
Time segment can be reset. Take TP1 as an example:

Inaccessible on Saturday and Sunday;

Accessible during the work time from Monday to Friday.

Work time: 08:30–18:00

The specific settings are as follows:



Multiple time segments can be defined as required and the entire system can be defined with 50 time segments at most.

4.5.3.2 Define Grouping Functions

By using the grouping functions, you can divide users into different groups and combine diverse groups to form different access combinations, so as to facilitate access control management. The system defines 5 groups: Group 1, Group 2, Group 3, Group 4 and Group 5. Newly enrolled users belong to Group 1 by default, but they can also be reassigned to other groups.

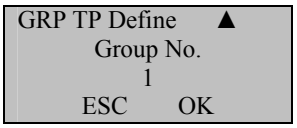
Group TS: This parameter is used to set the unlocking time of groups. In **Group TS**, select a set TP No.

The newly enrolled user adopts the time segment of Group 1 by default, but after resetting the group that he/she belongs to, the user will use the related time segment of the new group. Therefore, the default time segment of every group shall be defined in advance.

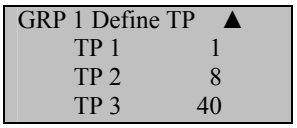
For details on how to **Use Grp TPs**, see User Access Control Settings.

✍ **Tip**: The time segment of Group 1 is numbered "1" by default. (That is, the newly enrolled users are allowed to unlock by default.)

a) Select **GRP TP Define** and then select "1" as Group No.:



Press **OK** to display the **Group1 Default TS** interface.

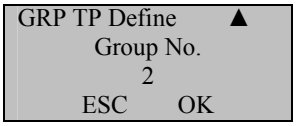


There are three default time segments which have an "OR" relation with one another.

Group 1 is allowed to unlock within the time segments 1, 8 and 40. You can also select other defined time segments.

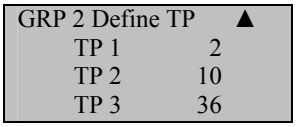
b) Select **GRP TP Define** and then select "2" as Group No.

Press **OK** to display the **Group2 Default TS** interface.



Group 2 is allowed to unlock within the time segments 2, 10 and 36. You can also select other defined time segments.

The time segments of every group can be defined as required and the entire system can be defined with the time segments of 5 groups at most.



4.5.3.3 User Access Control Settings

The user access control settings can be performed based on user requirements.

You can access the **User Acc Opts** menu to query the access control setting state of a user.

The User Acc Opts menu includes the options: Belong to GRP, Group TS, User TS, Group VerType, and Individual VerType. .

✧ **Belong to GRP**: Divide the enrolled users into several groups to facilitate management.

✧ **Group TS**: Set whether the user adopts the default time segments of the group that he/she belongs to.

✧ **User TS**: Set the user's unlocking time and select a set time segment number.

✧ **Group VerType**: Set whether the user adopts the verification types of the group that he/she belongs to.

✧ **Individual VerType**: Select a verification type for an individual user without using group verification types or affecting other group members' verification types.

☺ **Note**: 1. Relationship between group time segments and user time segments.

The value of the option **Use Grp TPs** only works for the following user time segments:

(1) If "**Use Grp TPs**" is set to **Y**, the user time segment will be automatically assigned the time segment No. of the group that the user belongs to. (Group time segments must be set in advance.)

(2) If the user time segment changes, "**Use Grp TPs**" will be automatically set to **N**.

2. Relationship between group verification types and individual verification types.

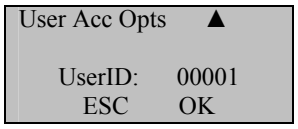
(1) If the option **Group VerType** is set to **Y**, the user will use the group verification type.

(2) If the option **Group VerType** is set to **N**, the user will use the individual verification type.

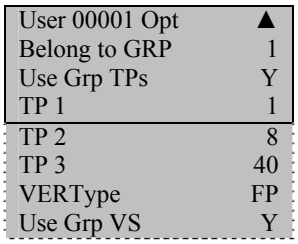
Examples:

A. Users 00001 and 00002 are classified into Groups 1 and 2 respectively.

Select **User Acc Opts** and set the UserID to 00001.



Press **OK** to display the setting interface of user 00001. Press ▲/▼ to select **Y** for the option **Use Grp TPs**. As mentioned above, Group 1 has been allowed to unlock within the time segments 1, 8 and 40. Select **Y** for the option **Use Grp VS**. Here we assume that the verification type of Group 1 is password verification (which can be set through the option **Group VerType** under the menu "**Access Options**"). The following information is displayed on the screen:



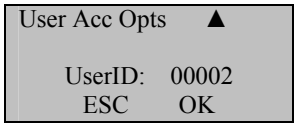
User 00001:

i. User 00001 belongs to Group 1 and adopts the time segment of Group 1 (The user time segment No. is the group time segment No).

User 00001 is allowed to unlock within the time segments 1, 8 and 40.

ii. If user 00001 adopts a group verification type (password verification), this type shall prevail even if user 00001 selects another individual verification type.

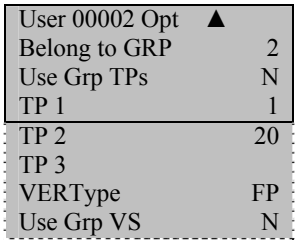
B. Select **User Acc Opts** and set the UserID to 00002.



Press **OK** to display the setting interface of user 00002.

If the user time segments are numbered 1 and 20, the system will automatically set the option **Use Grp TPs** to **N**.

To set "**Group VerType**" to **N**, set the option **VERType** (individual verification type) to **FP** as shown in the following figure:



User 00002:

i. User 00002 belongs to Group 2 and adopts the user time segment instead of group time segment (which means user 00002 is allowed to unlock within the time segments 1 and 20).

If user 00002 wants to adopt the group time segments, he/she can select **Y**, and then the user time segment No. will be automatically assigned the group time segment No. If user 00002 wants to adopt the user time segments, he/she can directly modify the user time segment No. and the system will automatically set the option **Use Grp TPs** to **N**.

ii. The individual verification type adopted by user 00002 is fingerprint verification.

4.5.3.4 Definition of Unlock Combinations

The unlock combinations are defined to control the unlocking. For example, to make all enrolled users unable to unlock, leave all the ten unlock combinations BLANK.

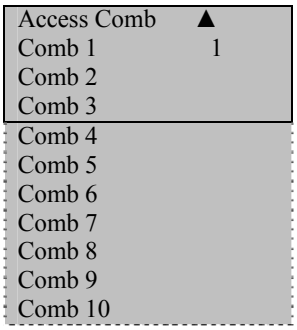
The unlock combinations are user-defined combinations to unlock the door, and each combination consists of different groups. The unlock combinations specify the group number(s) permitted to unlock the door, leaving the user verification sequence out of account. For example,

- "123" means the door unlocks only after at least three users respectively from Group 1, Group 2 and Group 3 pass the verification within the specified time segment.
- "4" means the door unlocks after one user of Group 4 passes the verification.

You can define a maximum of 10 unlock combinations for the FRT and the door unlocks as long as one of them passes the verification.

✍**Tip**: The default unlock combination is "1" (that is, new enrolled users can unlock the FRT by default).

On the initial interface, press **Menu → Options → Access Options → Access Comb**, as shown in the following figure:

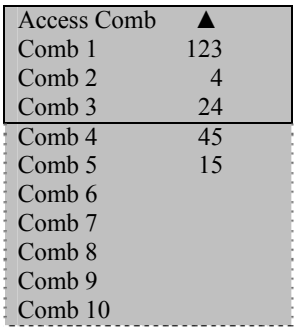


The default unlock combination is "1" and other unlock combinations are left blank.

To make all users unable to unlock, leave all these ten unlock combinations BLANK.

To enable unlocking for some of the groups, you need to define the unlock combinations, as shown below:

Example 1:



As shown in the figure above, five unlock combinations are set in total:

Unlock combination 1: 123.

Unlock combination 2: 4.

Unlock combination 3: 24.

Unlock combination 4: 45.

Unlock combination 5: 15.

Unlock combination 1: The door unlocks only after at least three users respectively from Group 1, Group 2 and Group 3 pass the verification within the specified period.

Unlock combination 2: The door unlocks as long as one user from Group 4 passes the verification.

Unlock combination 3: The door unlocks only after at least two users respectively from Group 2 and Group 4 pass the verification within the specified period.

Unlock combination 4: The door unlocks only after at least two users respectively from Group 4 and Group 5 pass the verification within the specified period.

Unlock combination 5: The door unlocks only after at least two users respectively from Group 1 and Group 5 pass the verification within the specified period.

To sum up, the door unlocks only when users of each group in an unlock combination pass the verification within the specified period.

☺ **Note:**

1. The verification will fail in any of the following cases:

✧ The user time segment number is not selected.

✧ The default group time segment number is not selected (when the group time segment is used).

✧The verification does not remain within any of the user-defined time segments.

✧ The time segment is defined as "Disabled".

2. Users set a time segment within which the verification fails:

❶If the conditions of unlock combination 2 are met, users of "Invalid Group" cannot unlock but are allowed to register attendance. (If there are other users meeting the unlocking condition in Group 4, then the unlock combination 2 is allowed to unlock)

❷If the conditions of unlock combinations 1, 3, 4 and 5 are met, users of "Invalid Group" cannot unlock but are allowed to register attendance.

2) Example 2:

To set the vault of a bank to unlock only in the presence of three people, proceed as follows:

These three people respectively belong to Group 2, Group 4 and Group 5 and are granted the right to unlock within the same time segment. Select "**Comb 1**" and press **OK**. Then enter "245" through the numeric pad and press **ESC** to exit and save the setting.

✍ **Tip**: Once the "245" combination is set, combinations such as 24, 25 and 45 are not allowed.

4.5.3.5 Lock Driver Duration

The lock driver duration refers to the duration within which the electric lock is opened upon the fingerprint verification. 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.

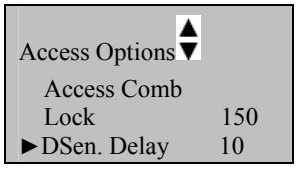
The unit of quantity for this duration is 20 ms and you can set it to 254 at most, that is, 5.08s.

To disable this function, set the duration to "0".

4.5.3.6 Door Sensor Delay

DSen. Delay (Door Sensor Delay): indicates the delay in checking the door sensor after the door is open. If door sensor state is inconsistent with the normal state set by the door sensor switch, an alarm will be generated, and this period of time is regarded as the "door sensor delay".

To set **DSen. Delay**, press **Menu → Options → Access Options**, and then select **DSen. Delay** through the ▲/▼ key, as shown in the following figure:



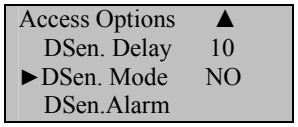
Press **OK** and modify the value of **DSen. Delay** through the ▲/▼ key.

4.5.3.7 Door Sensor Switch

The door sensor switch includes three modes:

- NONE: The door sensor switch is not used.
- **NO**: The lock is open as long as the door is open.
- **NC**: The lock is closed after the door is closed.

To set **DSen. Mode**, press **Menu → Options → Access Options**, and then select **DSen. Mode** through the ▲/▼ key, as shown in the following figure:

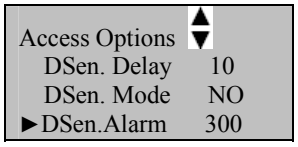


Press **OK** and then switch among the door sensor switch modes through the ▲/▼ key. The door sensor switch includes three modes: NONE, NO and NC.

4.5.3.8 Door Sensor Alarm Delay

The door sensor alarm delay refers to the delay in generating the alarm signal after a door sensor alarm is triggered. You can set the alarm delay between 0 and 999s.

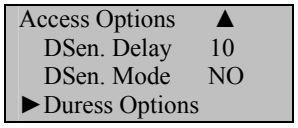
To set **DSen.Alarm**, press **Menu → Options → Access Options**, and then select **DSen.Alarm** through the ▲/▼ key, as shown in the following figure:



Press **OK** and modify the value of **DSen.Alarm** through the ▲/▼ key.

4.5.4 Duress Alarm

To set **Duress Options**, press **Menu → Options → Access Options**, and then select **Duress Options** through the ▲/▼ key, as shown in the following figure:

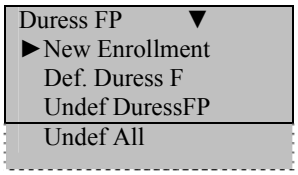


The Duress Options include such options as the Duress FP Mng, Help Key, 1:1 Trig, 1:n Trig, Pwd Trig and Alarm Delay.

4.5.4.1 Duress Fingerprint Management

Users may specially enroll a new or specify an existing fingerprint as the "Duress Fingerprint". Under any circumstances, a duress alarm is generated once this fingerprint passes the match.

Access **Duress Options** and select **Duress FP Mng** through the ▲/▼ key. Press **OK** to display the interface as shown in the following figure:



1) New Enrollment

This option is used to enroll a new fingerprint as the duress fingerprint.

2) Def. Duress FP

This option is used to change an enrolled fingerprint as the duress fingerprint.

3) Undef DuressFP

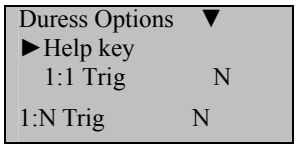
This option is used to cancel a single duress fingerprint.

4) Undef All

This option is used to cancel all duress fingerprints.

4.5.4.2 Help Key

Select **Duress Options**, and press ▲/▼ key to select **Help Key**, as shown in the following figure:

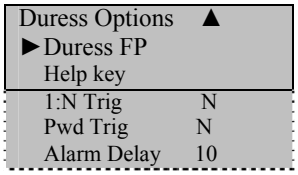


If the option **Help Key** is set to **Y**, press and hold ▼ (over 3 seconds) to signal for help; if you press and hold ▼ (less than 3 seconds) and then input your fingerprint or ID card number, a duress alarm will be generated at the same time when you pass the verification successfully.

If the option **Help Key** is set to **N**, the system will not send signals seeking for help even if you press and hold ▼.

4.5.4.3 Verification Alarms

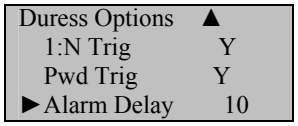
Our FRT supports three fingerprint verification modes: 1:1 verification, 1:N verification, and password verification. Press ▲/▼ in the following interface to select one or more verification modes as the duress alarm mode. When you perform verification by using a verification mode which is set to **Y**, the system will generate an alarm signal.



4.5.4.4 Alarm Delay

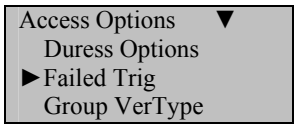
Define automatic alarm time: You can define an alarm delay to enable the system to automatically send a duress alarm signal after a period of time (0–255 seconds).

Under the menu **Duress Options**, press ▲/▼ to select **Alarm Delay**.



4.5.5 Verification Failure Alarm

Define the number of verification failures: The system automatically generates an alarm when the number of consecutive verification failures exceeds the upper limit.



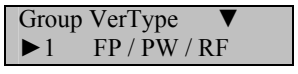
Under the menu **Access Options**, press ▲/▼ to select **Failed Trig**.

Press **OK**. Then select a number from 0–9 through the ▲/▼ key. Here, 0 denotes the deactivation of verification failure alarm, and other numbers denote the specific number of verification failures.

4.5.6 Group Verification Type★

There are 14 group verification types available. For details, see Appendix Multiple Verification Modes.

Under the menu **Access Options**, press ▲/▼ to select **Group VerType** and press **OK** as shown below:



2	FP / PW / RF
3	FP / PW / RF
4	FP / PW / RF
5	FP / PW / RF

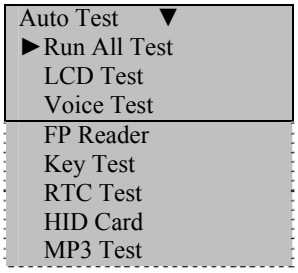
First select a group through the ▲/▼ key and press **OK**. Then press ▲/▼ to select a verification type for this group and press **OK** to confirm your selection. Finally press **ESC** to exit current interface, and when the system prompts you to save your changes, press **OK**.

Note:

The "Group VerType" option is available only for the devices supporting multiple verification modes.

4.6 Automatic Test

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



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

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

Voice Test: The FRT automatically tests whether the voice files are complete and the voice quality is good by playing the voice files stored in the FRT. You can continue the test by touching the screen or exit it by pressing [Auto Test].

Fingerprint Reader Test: The FRT 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 FRT 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.

Realtime Clock (RTC) Test: The FRT tests whether its clock works properly by checking the stopwatch of the clock. After select it, press "OK" to test, Press " ESC " to exit the test.

★**HID Card Test**: The FRT detects the format of user's HID card.

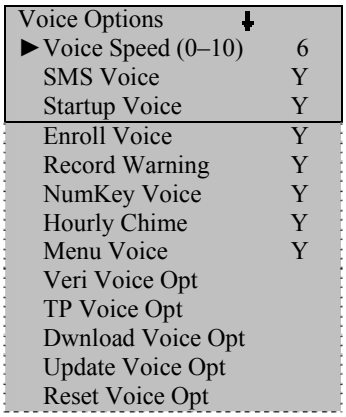
Note: When the FRT fails to identify the HID card number, please inform us of the characters detected through the HID card test and your HID card number, and our development personnel will troubleshoot as soon as possible.

★**MP3 Test**: You can check whether the MP3 works properly by playing the MP3 files stored in the FRT.

5 Voice Settings ★

5.1 5.1 Setting through Device

Select **Voice Options** and the information displayed on the screen is shown in the following figure:



1. Voice Speed

This option is used to set the voice playing speed. Value range: 0–10. The larger the value, the faster the voice speed.

2. SMS Voice

This option is used to set whether to play a voice prompt when the user receives an SMS after passing the attendance verification.

3. Startup Voice

This option is used to set whether to play a voice prompt when the FRT starts up.

4. Enrollment Voice

This option is used to set whether to play a voice prompt during fingerprint or password enrollment.

5. Record Warning

When the number of remaining records in the FRT exceeds the threshold, the FRT will play a warning voice after successful verification each time.

6. Numeric Key Voice

The FRT will read the corresponding number after you press a numeric key.

7. Hourly Chime

The FRT chimes on each full hour.

8. Menu Voice

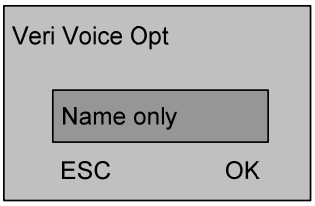
The FRT automatically reads the menu item over which the cursor hovers.

To modify the settings of any of the above options from 1) to 8), first select an option through the ▲/▼ key, and press OK to place the cursor on the field. Then press ▲/▼ to select a desired value and press OK. Finally press ESC to exit current interface, and when the system prompts you to save your changes, press OK.

9. Verification Voice Option

This option is used to select a voice playing mode after the completion of verification. There are 4 modes available: Name only, Name+Time segment greetings, Time segment greetings only, and No read.

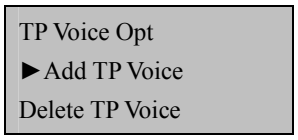
Press OK to display the setting interface.



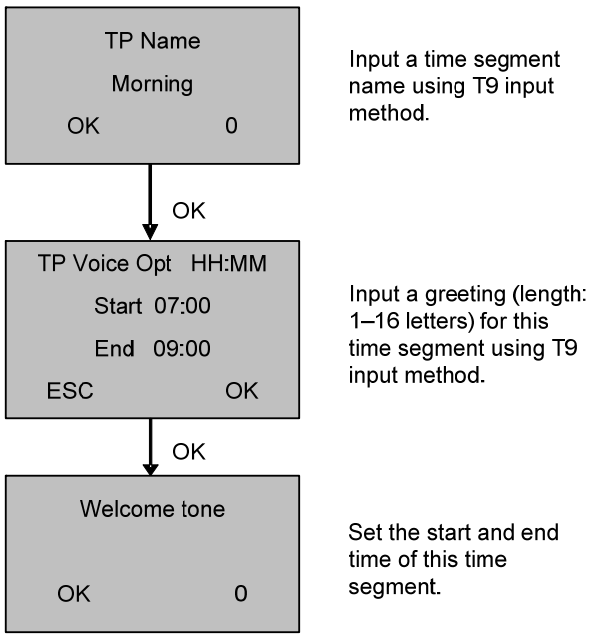
10. Time Segment Voice

This option is used to play customized voice within a specified time segment. After a user passes the verification, the FRT will play a greeting of current time segment if the time segment greeting is activated in verification voice settings.

For example, set a time segment 07:00–09:00, and a greeting "Good Morning!".

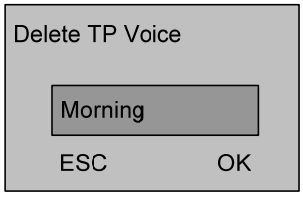


(1) Add a time segment greeting:



Tip: Time segments can be defined as infinite, but they shall not overlap with one another.

(2) Delete a time segment welcome voice:



Select a desired time segment through the ▲/▼ key and press OK to confirm your selection. Press ESC to exit.

11. Download Voice Configuration

This option is used to download the voice configuration file from the FRT to a USB pen drive. Users can modify voice in this text file.

12. Update Voice Configuration

This option is used to upload the voice configuration file from a USB pen drive to the FRT. After upload, the voice in the FRT will be updated.

13. Restore Voice Configuration

This option is used to restore all the voice configurations of the FRT to factory defaults.

5.2 TTS web server

Input the FRT's IP address (for example, http://192.168.1.115) into your IE browser and press Enter to access the web server login interface. You can use the user name "admin" and the password "0" to log in to the TTS web server. Here, the user name "admin" is unchangeable but the password is not. (Select **Menu → Options → Comm Opt → COMM Key** and you can change your password in the displayed interface, and then use the new password for re-login.)

Modify the TTS related statements in the text boxes shown in the figure above and save your changes. These changes will take effect after system restart.

Description of the voice configuration file format:

Voice configuration file is of TXT format.

For example, the startup greeting in this text file is defined as follows:

127=Welcome to use **** fingerprint recognition terminal

1) Users can change the statement "Welcome to use **** fingerprint recognition terminal".

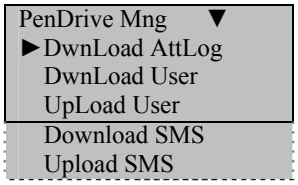
2) "127" denotes the serial number of the startup greeting, and it is recognizable for the FRT. If this number is changed, the FRT will fail to identify the statement above as the startup greeting.

3) Users shall not add any serial number or statement because the FRT cannot identify new serial numbers.

☺ **Note:** Please modify voice strictly in compliance with the format of text contents. Do not change the file format. Otherwise, it may lead to failure in playing specified voice. In the event of any problem, please restore the voice configurations to factory defaults.

6 USB Pen Drive Management ★

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

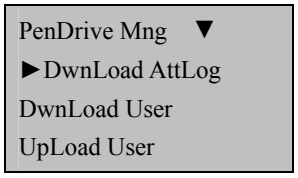


You can download the attendance data, employee data and short messages and upload employee data and short messages with a USB pen drive.

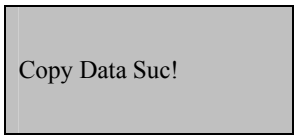
6.1 Download Attendance Data

1. Insert a USB pen drive into the USB interface on the FRT.

2. Select **PenDrive Mng** and select the desired attendance 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. Three files **X_attlog.dat** (attendance records), **X_oplog.dat** (management records) and **X_user** (where "X" refers to the device ID) are stored in the USB pen drive.

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

6.2 Download Employee Data

Employee data downloading is similar to the downloading of attendance records. Press ▲/▼ to select "DwnLoad User" from the "PenDrive Mng" menu. The files user.dat (user profile) and Template.dat (fingerprint template) will be concurrently downloaded to the USB pen drive.

6.3 Upload Employee Data

Press ▲/▼ to select "UpLoad User" from the "PenDrive Mng" menu and then press **OK**. The files user.dat (user profile) and Template.dat (fingerprint template) stored in the USB pen drive will be concurrently uploaded to the FRT.

6.4 Download Short Messages★

Short message downloading is similar to the downloading of attendance records. Press ▲/▼ to select "Download SMS" from the "PenDrive Mng" menu. Press **OK** to start download. The system will prompt whether the download is successful or not.

6.5 Upload Short Messages★

Edit a short message by selecting **External Program → SMS Mng** 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 USB interface on the FRT upon successful export, and select **Menu → PenDrive Mng → Upload SMS** to upload the short message from the USB pen drive.

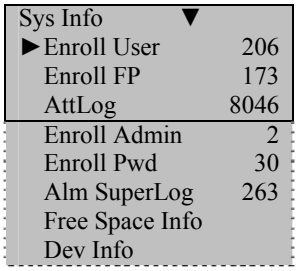
Note:

The option **PenDrive Mng** is available only on the FRTs configured with USB slots. The options **Upload SMS** and **Download SMS** are available only on the SMS-capable FRTs. If you need FRTs that support these functions, please consult our commercial representatives or pre-sales technical support engineers.

---

7 System Information

Through the **Sys Info** menu, you can check all information of the FRT, 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:



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.

8 Turn Off (Clear) Alarm ★

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

Note:

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

9 Query Attendance Records ★

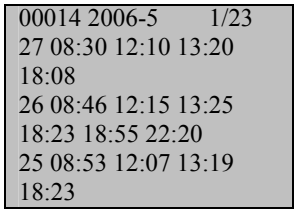
You can query the attendance records of an individual or all employees through the FRT without connection with the attendance software.

1) Query modes of attendance records

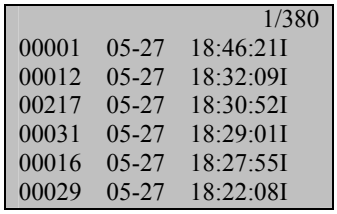
You can query the attendance records in the following two ways:

- Select **Menu → Query Attendance Records** and enter the ID of the user to be queried. Then press **OK** to query the attendance records of the specified user. If the user ID is left unspecified, that is, leave it to "00000", then the attendance records of all employees can be queried.
- You can query your own attendance records by pressing **Menu** before the interface returns to the initial attendance records interface.

For example, the attendance records of the user with ID of 00014 are displayed as follows:



The attendance records of all employees are displayed as follows:

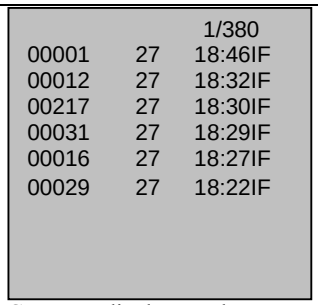


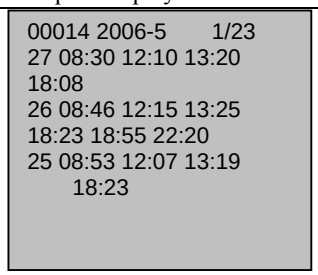
2) Browse of attendance records

The attendance records are arranged in reverse chronological order, that is, the most recent record comes first and the least recent record last. You can press the following keys during the browse:

Key	Function
▲	Scroll up one page.
▼	Scroll down one page.
1	Move the display one column left.
3	Move the display one column right.
OK	Restore the display to the initial value.
2	Move the display one row up.
5	Move the display one row down.
4	Switch between the compact and complete display modes. For example, the two figures on the right respectively display the complete and compact display of "All attendance records". • Complete display mode: refers to the format designed to display the complete field values. • Compact display mode: refers to the format designed to display as much information as possible on the LCD.

Complete display mode

<table>
<tr><th>Key</th><th colspan="2">Function</th></tr>
<tr><td></td><td></td><td> 

Compact display mode</td></tr>
<tr><td>6</td><td>Switch between the large and small fonts. The two figures on the right take the “Individual Attendance Interface” as an example to show the display of attendance records in small and large fonts respectively.</td><td> 

Small font
 

Large font</td></tr>
<tr><td>9</td><td colspan="2">The latest record</td></tr>
<tr><td>0</td><td colspan="2">The earlier record</td></tr>
</table>

3) Print of displayed attendance records

When querying the attendance records on the FRT, you can print the records currently displayed on the screen by pressing **OK**.

You can also check the output with a HyperTerminal.

Note:

The attendance tracking is an optional function. If you need this function, please consult our commercial representatives or pre-sales technical support engineers.

10 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 FRT operates, the following maintenance guide might be of some help to you:

Table 10-1 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 FRT, 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 FRT:

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.

11 FAQs

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 employees:

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

Question: What are the possible causes of FRT 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 FRT.

③ The FRT is not connected with the power supply or the PC.

④ The FRT 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.

Question: What are the possible causes of incomplete display (sometimes half-screen display) or blurred screen after the FRT 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 FRT for repair.

Question: How can I delete a FRT administrator?

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

Question: Why is there a beep sound during the communication between FRT and PC?

Answer:

① If the beep sound occurs in RS-232 communication mode, the baud rate settings of the PC and FRT 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.

Question: Why does the FRT 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 FRT for maintenance.

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 FRT, for example, set it to 19200 or 9600 before reading the attendance data again.

12 Appendix

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

12.1 USB

USB Host

The FRT 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 FRT, 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 FRT 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 FRT and computers.

For the operations of the FRT used as the USB host, see 7. USB pen drive Management.

USB Client

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

When the FRT is used as the USB Client, the USB communication options will be displayed in the FRT communication setting menu. For details, see 5.3 Communication Settings.

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

12.2 Status Key

Different events relate to different statuses. For example, the attendance involves such statuses as sign-in, sign-off, sign-in for overtime work, sign-off for overtime work, leave and return. The access control system involves such statuses as entry and exit.

Some FRTs have 6 status keys on their keyboards to set current status, while others have the ▲/▼ key to select current status. But these statuses must be manually set, that is, to use a status, press related status key. To reduce manual options, our company has developed the timed status switchover function that enables the FRT to automatically switch over current status at user-specified time and display the status on the initial interface.

For details, see 5.2.2 Timed Status Switchover.

12.3 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 FRT. The options **Bell Delay** and **Bell Time Segment** are available on the FRTs 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 FRT will automatically ring at the specified time every week and stop the ring after the ring duration times out.

The FRT rings the bell in the following two ways:

Ring the bell through the speaker configured on the FRT.

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

12.4 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 FRT 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.

Note:
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.

12.5 Modem

[Overview]

To enable remote communication between a PC and the FRT in areas where Internet access is unavailable, some FRTs 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 FRT must also connect with a Modem which is then connected with the PSTN over a telephone cable. The FRT accesses the network upon successful dial-up.

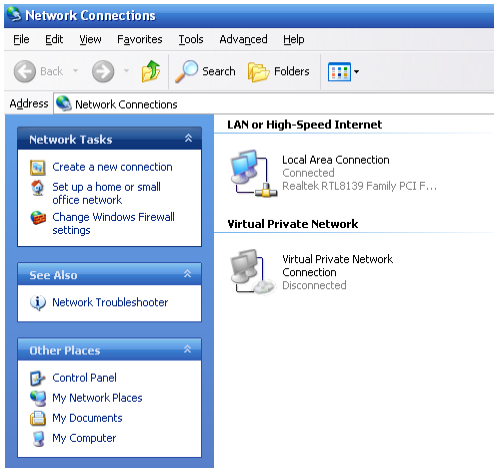
[Operation Steps]

1. Connect the FRT with the Modem by using the delivery-attached cable marked with “Modem”. Power on the FRT and Modem respectively and then connect the telephone cable to Modem.

2. Select **Option → Comm Opt** on the FRT and set the option **Extern Modem** to **Y**. Save the setting and exit. Then restart the FRT.

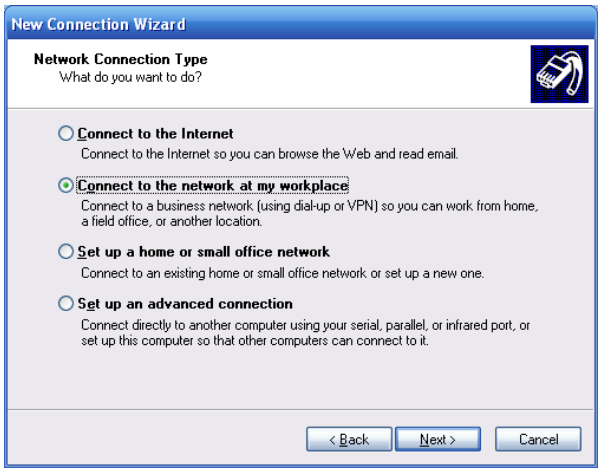
3. The following takes Windows XP dial-up setup as an example to illustrate the procedures of creating a dial-up connection:

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.

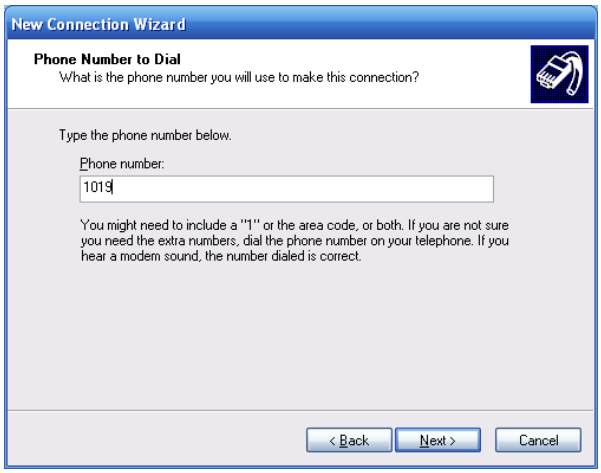
3） Click the **Next** button to begin, as shown in the following figure:



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 dialup 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.

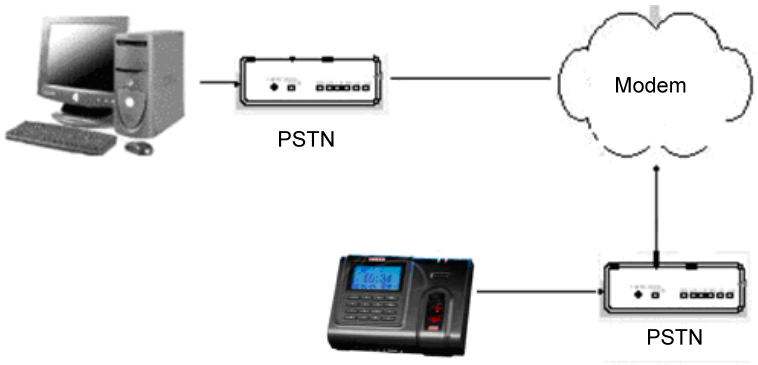
9） After finishing the connection setup, double-click the new connection and the interface as shown in the following figure is displayed:

10) Both the user name and password are "ppp". After typing the user name and password, click **Dial** to start connection. The default FRT 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 FRT 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 FRT, set the option **Extern MODEM** (**MENU → Options → Comm Opt → Extern MODEM**) on the FRT to **Y**.
4. When Modem is used, the RS232 and RS485 functions of the FRT 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 FRT. 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.

12.6 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 FRT 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.

12.7 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 wireline Ethernet, making the networking cost even lower.

Our FRT 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.

12.8 Attendance Query

You can query the attendance data of an individual or all employees directly on the FRT 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.

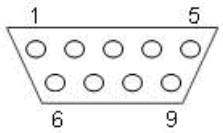
You can query the attendance data of not only an individual but also all employees on the FRT.

For details, see Chapter 10 Query Attendance Record.

12.9 Print

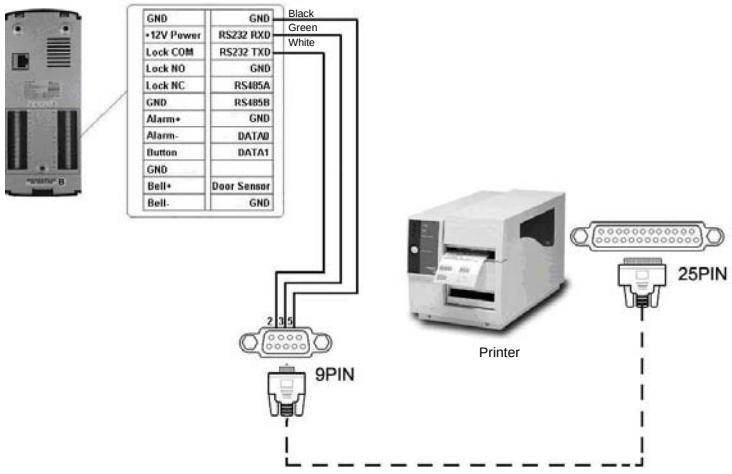
[Function Description]

The FRT supports only the serial port print function. The printed contents are output in RS232 mode and each time after a user passes the verification, the verification result is output through the serial port. If the FRT is connected with a printer, the output can be directly printed or queried through a HyperTerminal.

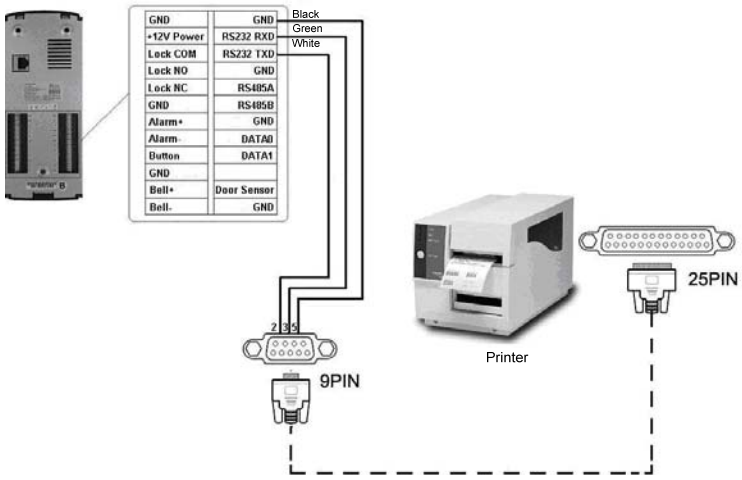
Cable connection between FRT and printer	FRT Printer 2 TXD <-----> 3 RXD 3 RXD <-----> 2 TXD 5 GND <-----> 7 FG
RS232 port pin-out sequence	

Schematic diagrams of cable connection between FRT and printer

The FRT has a 9-PIN serial port.



The FRT has a connecting terminal



[Operation Description]

Select **Menu → Options → System Opt → Adv Option → Print Format** on the FRT. The FRT supports 10 print formats in total.

For example, the piece of attendance record that Jack checks in at 13: 24: 55 on November 1st 2007 can be printed in the following 10 formats:

Format 1:

00001 07-11-01 13:24:55

Format 2:

User ID: 00001

Date Time Check-In

13:24:55

Format 3:

00001 Jack 07-11-01 13:24:55

Format 4 – Format 10

00001 07-11-01 13:24:55

Note:

1. The baud rates of the FRT and printer (HyperTerminal) must be the same.
2. If the default print format falls short of your requirements, please contact our commercial representatives to customize other formats.

12.10 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 FRTs 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 FRT to play at the specified time, thus making your office more employee-friendly.

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

MP3 play setting

Under the menu item **Menu → Options → Power Mng → Scheduled Bell**, there are 8 time segments available for you to select. You can set the time segment as required. The FRT automatically plays an MP3 file at the specified time segment.

Note:

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 FRT is playing an MP3 file.

4. While the FRT is playing an MP3 file, you can press any menu key to stop the play.

MP3 file access

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

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

- Volume control

The FRT 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 FRT.

- MP3 file format

The FRT 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 FRT because it is compressed by a standard (e.g. MPEG I Layer 1 or Layer 2) that the FRT 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 FRT.

12.11 Short Message

FRTs of some models 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 FRT.

The public short messages are displayed on the screen all the time once the FRT 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 FRT, 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 ×× in the ×× meeting room" (you can edit it as required) through the background software and upload it to the FRT. Then on June 19th, this short message will be displayed all the time on the screen once the FRT is started.

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

- Direct import by connecting the software to the FRT.
- 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 to the FRT and upload it to the FRT.

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 FRT 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 FRT 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 FRT.

12.12 Multiple Verification Modes

Currently the FRT 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 FRT 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.

Note: 1) Mifare can be deemed as RF in the verification process and Mifare card verification is only available for Mifare-card-capable FRTs.

2) Except for some FRTs of specific models, the B&W screen series FRTs support only the fingerprint and password verification modes. The Mifare-card-capable FRTs also support the Mifare card verification apart from the fingerprint and password verification modes.

3) The FRT 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 FRT. The verification modes are listed as follows:

Type	Description
FP	Fingerprint verification only
	PIN+FP (1: 1) 2) FP (1: N) 3) RF+FP (1: 1)
PIN	ID number verification only
	Users can pass the verification as long as they type their ID numbers through keyboard regardless of their enrollment modes.
PW	Password verification only

Type	Description
	1) PIN+"←"+PW 2) RF+PW
RF	RF Card verification only
	1) RF
FP/PW	Fingerprint or password verification
	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)
FP & PIN /RF	Fingerprint and ID number or fingerprint and RF verification
	1) FP+ PIN 2) FP +RF 3) PIN+FP(1:1) + PIN

Type	Description
	4) PIN+FP(1:1) +RF

Users enroll their fingerprints or passwords on the FRT. 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) 3) FP(1:N) 4) PIN+"←"+ FP(1:1) 5) 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

Type	Description	
	Enroll fingerprint	Enroll password
		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

Note: 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.

12.13 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 FRT with built-in non-contact RF EM card reader module. By integrating the EM read-only card, this FRT can be conveniently consolidated into the existing telephone, canteen POS and access control system. This FRT 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 FRT with non-contact RF HID card reader module. By integrating the HID read-only card, this FRT can be conveniently consolidated into the existing telephone, canteen POS and access control system. This FRT 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 FRT 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 FRT with non-contact RF Mifare card reader module. By integrating the Mifare card, the FRT can be conveniently consolidated into the existing telephone, canteen POS and access control system. This FRT 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 FRT 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 FRT with non-contact RF iClass card reader module. By integrating the iClass card, the FRT can be conveniently consolidated into the existing telephone, canteen POS and access control system. The FRT 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 FRT 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*.

12.14 Master-slave function ★

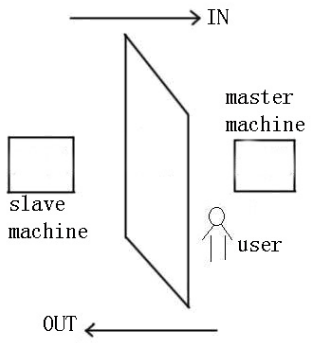
Two devices, a master and a slave, both controlling the same lock, are connected by RS232/RS485/Wiegand.

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 mode 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:

Master		Slave
485+	<----->	485+
485-	<----->	485-
GND	<----->	GND

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.

12.15 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 FRT. Even if the FRT is highly scalable, the offline running speed of the FRT 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.

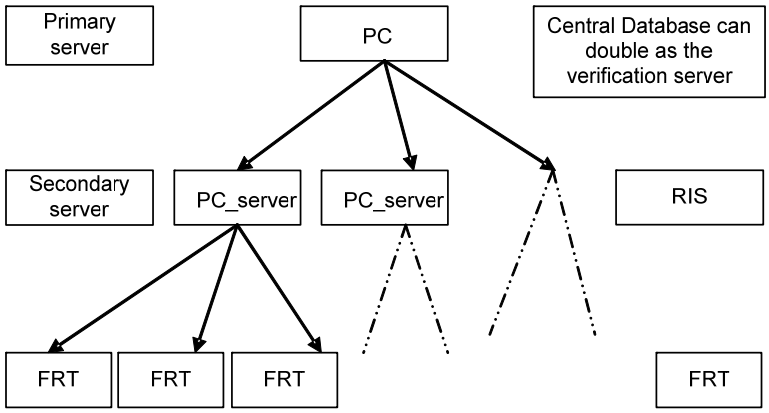
Operating Principle of the RIS

The RIS solution uses the FRT as the fingerprint reader while retaining its offline verification function. By using the network function of the FRT, 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 FRT.

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 FRT 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 FRT only serves as the fingerprint reader and sends fingerprints to the RIS. The RIS verifies the fingerprint templates from the FRT by taking advantage of the powerful processing capability of PC, stores the verification results in the center database and returns them to the FRT for display at the same time. At present the verification speed of the FRT 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 FRT 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 FRT 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.

For details of the RIS, see *RIS Specifications*.

12.16 iClock Attendance System

Overview of iClock

The iClock series is a type of Web Server-based attendance system that adopts the common Web page requests to handle and manage data. It centralizes multiple functions such as the onsite data collection, onsite smart interface (RS232/RS485), communication protocol conversion, image capturing, alarm data storage and Web server. The uniform monitoring platform underpinned by the iClock can conveniently provide integrated solutions for onsite device management and attendance tracking. The iClock 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. Further, the iClock can help management personnel to query employees’ attendance/on-the-job information anytime and handle important services such as the attendance, access control and salary report after going online. With the iClock, customers can really have real-time synchronization at hand anywhere at any time.

Role of Built-in Web Server

1. Lightly-attended or unattended

The Web Server can be reliably and stably deployed on site through TCP/IP and Ethernet. You can perform remote query and operation of the data stored in the equipment in real-time, upload/download data and upgrade system through the browser without resorting to any software or tools.

2. Interworking with other related software

The Web Server features excellent compatibility with other related software to meet customer needs in a more flexible way.

3. More stable and fast remote data communication mode

You can stably and quickly download data to a local PC through the Web Server. You can download all data in the device within a short time through the browser without worrying about the data reliability.

4. More flexible and easy-to-use data management and resource sharing mode

The applications constructed based on the Web Server platform make the data management more flexible and easier.

5. The Web Server can easily interconnect or integrate with the OA and CRM systems to implement the complete network-based HR management solutions.

Use of iClock Series FRTs

The iClock series supports three connection modes: LAN, telephone line dialup network and Internet. When successfully accessing the Web server through browser, you need to enter a username and password. The default username is “administrator” and password is “123456”. For details of iClock series, see *iClock User Guide*.

12.17 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 FRT, 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*.

12.18 Automatic IP Address Collection

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

12.19 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 FRT 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 Vol) 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
Tpw	Pulse Width	100 μs
Tpi	Pulse Interval	1 ms

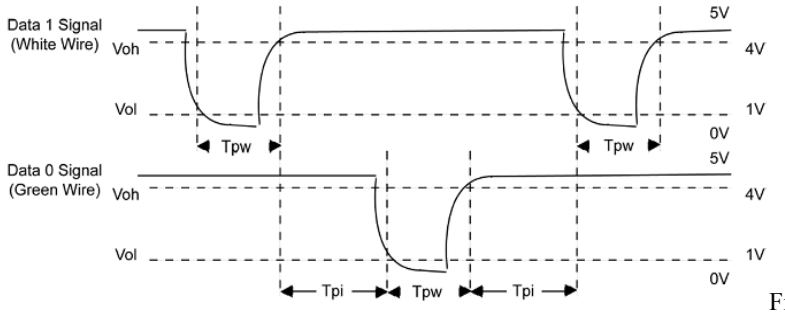


Figure 1 Sequence Diagram

Wiegand Format

The Wiegand format adopted by the FRT 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.

1 2 9 10 25 26

EP	FC	CC	OP

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

12.20 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 FRT 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 FRT. 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 error". 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.

12.21 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 an FRT with a built-in PoE module to the PoE system, the FRT 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 FRT 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 creepage 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.

12.22 Backup Battery (Mini-UPS)

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

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.

12.23 9-digit Enrollment Number

The standard user IDs supported by the FRT 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.

12.24 Automatic Time Calibration

Considering the huge workload for one-by-one time calibration of multiple FRTs 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 FRTs in a network support the automatic time calibration function. Set FRT A to the time server. The display time of FRT 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 FRT 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.

12.25 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 FRT supports the DLST function to adjust forward one hour at ×× (Hour): ×× (Minute) ×× (Day) ×× (Month) and backward one hour at ×× (Hour): ×× (Minute) ×× (Day) ×× (Month).

For the operations of the FRT menu settings, see 5.1.6 Daylight Saving Time.

12.26 Play Voice Within Specified Time Segment (By Time Segment or Group)

When the user operates the FRT, the FRT often plays voice prompts. For example, the FRT 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 FRTs more user-friendly, we enables the FRTs 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 FRT 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 FRT 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 FRT 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 FRT restart.

12.27 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 FRT 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.

Note:

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 FRT after pressing "▲", the FRT 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.

Note: 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.

12.28 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 FRT uses the DHCP, it needs a DHCP server and our FRT works as a client.

On the FRT supporting DHCP, select **Menu → Options → Comm Opt → Dyn Host Opt**, and set the option **Dyn Host Opt** to **Y**. After accessing the network, restart the FRT and the FRT 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 FRT based on the configured address. After the FRT acquires an IP address, you can select **Menu → Options → Comm Opt** to query the acquired IP address, subnet mask, and gateway.

If you set the option **Dyn Host Opt** to **N**, the DHCP function will not be activated. You need to manually input an IP address, subnet mask, and gateway.

12.29 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 FRT 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.

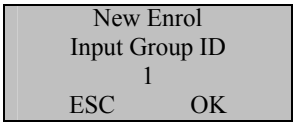
Setting of the "Match by Group" function

On the FRT 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 FRT 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 FRT for verification. For details, see **3.4.1 Fingerprint Verification**.

Note: The users in "Default Group" can directly place their fingers on the FRT 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.

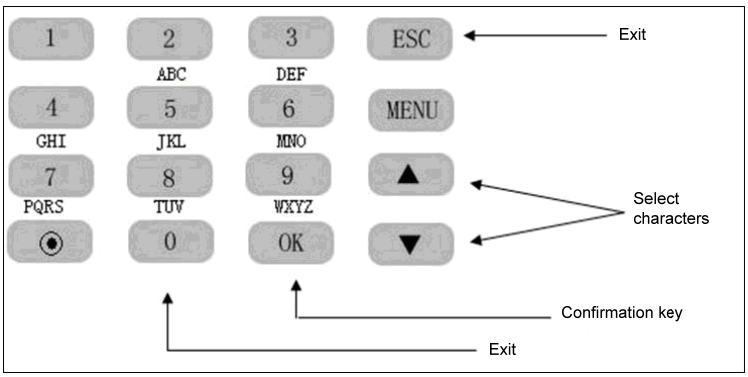
Note:

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.

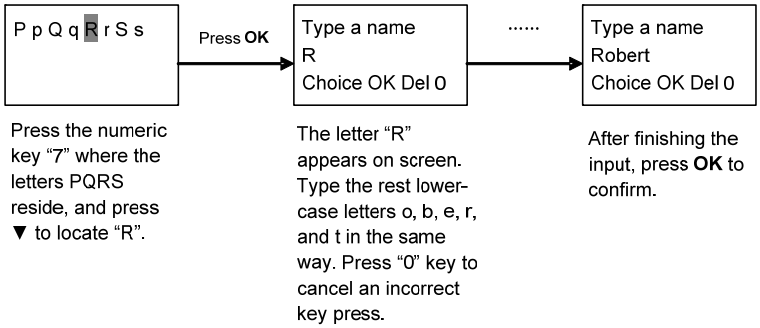
12.30 T9 Input Method

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:



12.31 TTS Function

By use of the TTS technology, the FRT converts normal language text into the speech that can be output as WAV files. The FRT 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.

For detailed operations, see **5. Voice Settings**.

Note: The FRT 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.

12.32 Menu Items

The menu items marked with "★" in this manual are only supported by a specific or tailor-made device and they have been described above.

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.

12.33 Environment-Friendly Use Description

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

Names and Concentration of Toxic and Hazardous Substances or Elements

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

○: Indicates that this toxic or hazardous substance contained in all of the homogeneous materials for this part is below the limit requirement in SJ/T11363-2006.
×: Indicates that this toxic or hazardous substance contained in at least one of the homogeneous materials for this part is above the limit requirement in SJ/T11363-2006.
Note: 80% of the parts in this product are manufactured with non-hazardous environment-friendly materials. The hazardous substances or elements contained cannot be replaced with environment-friendly materials at present due to technical or economical constraints.