



Contents

- 1. Introduction.....3**
 - 1.1 Basic Concepts..... 4**
 - 1.1.1 User Enrollment 4
 - 1.1.2 User Verification 5
 - 1.1.3 Match Threshold Levels 5
 - 1.1.4 User ID Numbers 6
 - 1.1.5 Authority (status) Levels 6
 - 1.1.6 Start-up window..... 6
 - 1.2 How to place the finger..... 7**
- 2. Enrollment and Verification Procedures.....7**
 - 2.1 Enrolling Users..... 8**
 - 2.1.1 Fingerprint Enrollment..... 9
 - 2.1.2 Password Enrollment 10
 - 2.3.1.3Fingerprint & Password..... 12
 - 2.2 Testing an Enrollment.....13**
 - 2.3 Enrolling a User with the Display Finger Option On13**
 - 2.4 Verifying Your Identity14**
 - 2.4.1 Fingerprint Verification 14
 - 2.4.2 Password Verification..... 15
 - 2.4.3 ID number & Fingerprint..... 16
 - 2.5 Hints for Successful Enrollments16**
- 3. System Options18**
 - 3.1 System Options.....18**

3.1.1 Date Time..... 19

3.1.4 Advanced Options..... 19

3.2 Power Manager.....20

3.3 Communication Options.....21

3.4 Log Options21

3.5Auto Test.....22

4. System Information22








5. Trouble shooting.....23

1. Introduction

Figure 1~2 keypad



Keypad Definition

-  Confirm the current present.
-  Access to manage.
-  Escape or cancel.
-  Scroll up.
-  Scroll down.
-  Power button.
-  : Numerical key.

1.1 Basic Concepts

This section contains definitions and descriptions of Fingerprint T&A Concepts, including:

- .User Enrollment
- .User Verification
- .Match Threshold Levels
- .User ID Numbers
- .Authority (Status) Levels

The two most important Fingerprint T&A Functions are user enrollment and user verification.

1.1.1 User Enrollment

Enrollment is the process of create an ID number and scanning a user's finger to create a template three times. This template is associated with a user ID number and stored.

During user verification, the stored template is compared to the current fingerprint scan to confirm the user's identity.

Enrollment is performed at designated units. The user can verify on the time recorder that enroll his fingerprint. The enrollment process takes approximately 2 seconds.

Up to ten fingers can be enrolled for the same ID number, so the user may have more verifications way.

Ideally, everyone finger on each hand should be enrolled so that if the user injures the enrolled finger had, an alternate finger template is available. While recording the finger type is optional, it is recommended such as left or right index, so that at verification the user is prompted as to which finger to use.

1.1.2 User Verification

Verification occurs when a user either enters an ID number or places a finger in the fingerprint sensor, then input password for comparison with the stored template.

1.1.3 Match Threshold Levels

The Match Threshold is a number that represents the degree to which a verification is examined to ensure that the person is the person claimed.

The Match Threshold Levels establishes a balance between False Acceptance Rate (FAR) and False Rejection Rate (FRR). FAR measures how often a non-authorized user is falsely recognized and granted access to the system. FRR measures how often an enrolled and authorized user, who should be granted access to the system, is denied on the basis that the system did not recognize him.

You can set match threshold levels on a per-use basis. For the fingerprint verification is difficult, you can adopt ID & Fingerprint verification (match one to one).

Raising the threshold increases security, while lowering it increases throughput. The correct balance is essential.

For users with worn or damaged fingers, match threshold levels can (and should) be reduced.

Different sites have different requirements.

Table 1—1 Suggested Match Threshold Settings

FRR	FAR	One-to-many	One-to-one
High	Low	45	25
Middle	Middle	35	15

Low	High
-----	------

25

10

1.1.4 User ID Numbers

Before beginning fingerprint enrollment, a user is assigned User ID Number. This ID number is used to call up the fingerprint template each time that verification is requested.

ID numbers are called up via the keypad

1.1.5 Authority (status) Levels

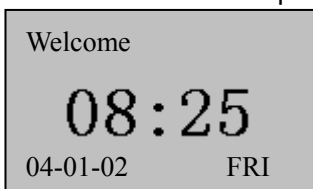
Fingerprint T&A has four authority or status levels:

- ✧ -Users are people whose identity must be verified, such to gain access to a facility or to have their attendance recorded.
- ✧ -Enrollers are Users who are authorized to enroll new users or delete on to the system.
- ✧ -Administrator can do other operations, except set advanced option and enroll administrator authority.
- ✧ -Supervisors are Users who access to all functions and change all setup in the system.

Note: Without Administrator and Supervisor status in the system, the Enroller will enroll them. And if there isn't a Supervisor in the system, the Administrator will enroll him.

1.1.6 Start-up window

Click the power button and the screen showed on, a display of a window was called the Start-up window. The following appears:

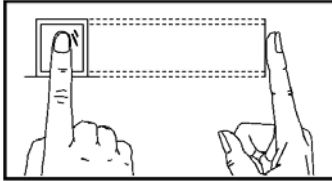


1.2 How to place the finger

◇ **The correct way is:**

Place a finger flatware on the sensor surface

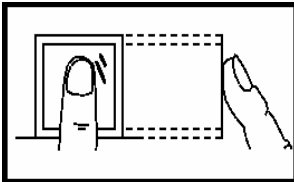
Place it to the center of the sensor surface



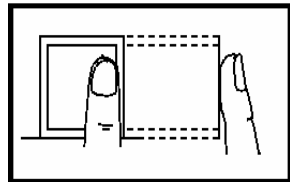
◇ **The wrong way is:**

Upright

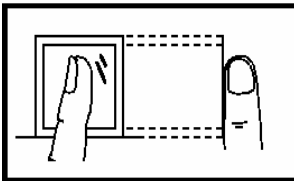
+



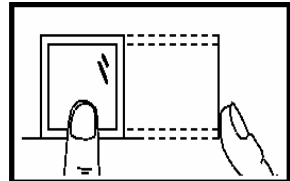
Unfettering



askew



part



Note: Please adopt the correct way to place the finger,

2. Enrollment and Verification Procedures

This chapter describes how to enroll and verify users on the Fingerprint T&A verification system.

The following topics are included:

- -Enrolling User
- -Testing an Enrollment
- -Enrolling a User with the Display Finger Option On
- -Verifying Your Identity
- -Hints for Successful Enrollments

Note: You must have Enroller, Administrator, or Supervisor status to enroll users. For information on status levels, **see “Authority (Status) Levels” on 1.1.5.**

2.1 Enrolling Users

If this is the first enrollment in a new or empty system, everyone will become an enroller.

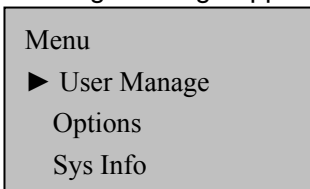
If there is a manager in the system, you will have Administrator status to enroll a new user.

There are three ways of enrollment, fingerprint enrollment, password enrollment, fingerprint & password are suitable for three different crowds. Fingerprint enrollment suited the most people who have better quality fingerprints; Fingerprint & Password suited few people who enrolling successful, but verification was difficult; Password enrollment suited 1% people who verification unsuccessful.

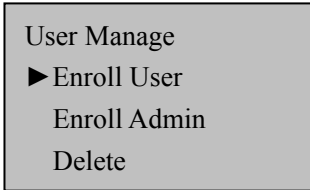
To start the enrollment process, identify yourself firstly—press [Menu], enter your ID number or fingerprint, and then verify your identity.

Note: If this is the first enrollment in a new or empty system, you will not be prompted for verification.

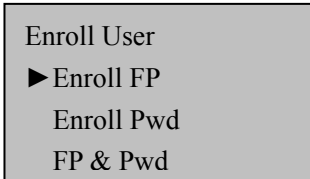
The following message appears on the display:



Press [OK], access the User Manager, the following message display:

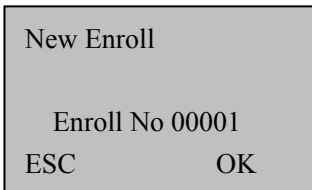


Press [OK], access the User Enrollment, the following message display:

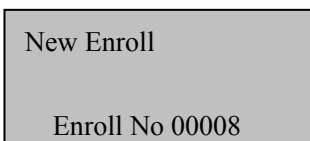


2.1.1 Fingerprint Enrollment

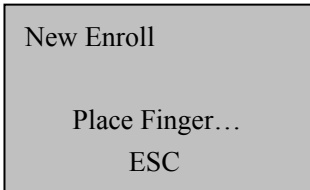
(1) Access the Enroll Fingerprint to press [OK], the following display:



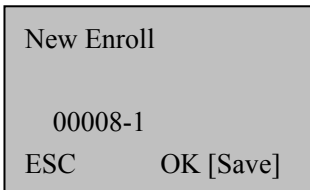
(2) Press [OK], the following appears:



(3) Input the enrolling number (the range is 1 to 65534), press [OK], the following appears:



(4) If the test is successful three times in a row, the following appears:



Note: 07711-1

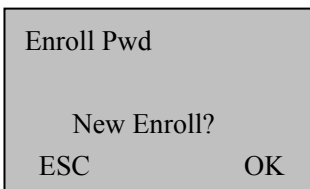
The last number 1 means the first fingerprint.

Press [OK], the previous message continues to be displayed while the template is created.

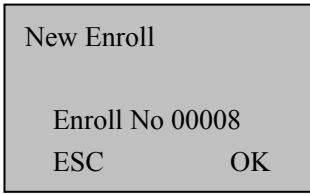
If your identity cannot be verified, you are prompted to try again. And you must restart the verification procedure (step 3).

2.1.2 Password Enrollment

(1) Access the password enrollment, press [OK], the following appears:



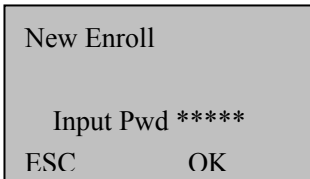
(2) Press [OK], the following appears:



```
New Enroll

Enroll No 00008
ESC          OK
```

(3) Input the enroll number (the range is 1 to 65534), press [OK], the following appears:

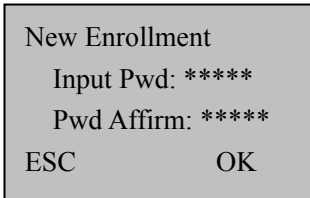


```
New Enroll

Input Pwd *****
ESC          OK
```

Note: The password range is 1 to 5.

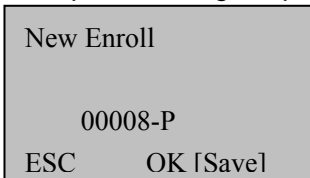
(4) Input the password, press [OK], the following appears:



```
New Enrollment

Input Pwd: *****
Pwd Affirm: *****
ESC          OK
```

(5) Input the password again, press [OK], the following appears:



```
New Enroll

00008-P
ESC      OK [Save]
```

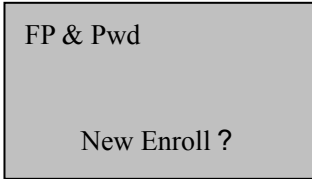
Note: 00008-P

The last letter P means password.

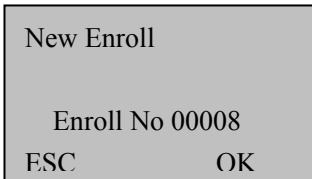
Press [OK], the previous message continues to be displayed while the template is created.

3.1.3 Fingerprint & Password

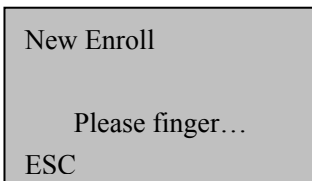
Access the Fingerprint & Password, press [OK], the following appears:



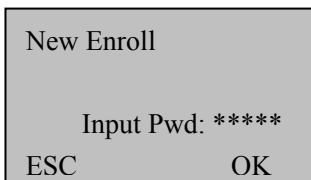
(2) Press [OK], the following appears:



(3) Input the password (range is 1 to 65534), press [OK], the following appears:



(4) If the test is successful three times in a row, the following appears:



(5) Input your password, the following appears:

```

New Enroll
  Input Pwd: *****
  Pwd Affirm: *****
ESC          OK
    
```

(6) Input the password again, press [OK], the following appears:

```

New Enroll

          00008-1P
ESC      OK [Save]
    
```

Note: 00008—1P
 The second from the last 1 means
 one fingerprint
 The last letter P means password.

Press [OK], the previous message continues to be displayed while the template is created.

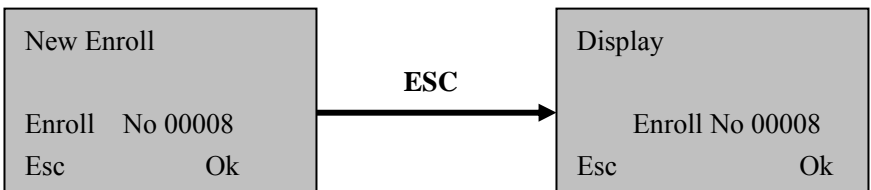
2.2 Testing an Enrollment

Ask the users to place their finger to perform a test verification. If the test was successful, you will adopt Fingerprint enrollment. If the poor quality of fingerprint, you will be recommended to use Fingerprint & Password.

2.3 Enrolling a User with the Display Finger

Option On

Press [ESC] to the Display Dinger Option On, the following appears:



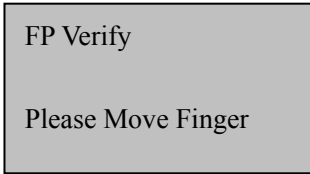
Note: Where system memory permits, it is advisable to have at least two fingers enrolled for a long-term user.

2.4 Verifying Your Identity

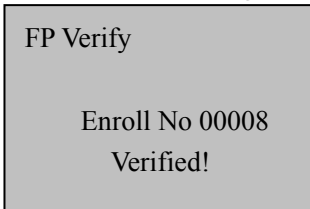
The workers used Fingerprint T&A to verify their identity. The system defaults to three ways of verification: Fingerprint verification, Password verification, ID number & Fingerprint. The following appears:

2.4.1 Fingerprint Verification

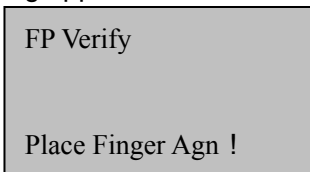
Place the finger on the sensor surface, the following appears:



It continues for about 0.5 seconds. If the test is successful, it will say "Thank you", the following appears:



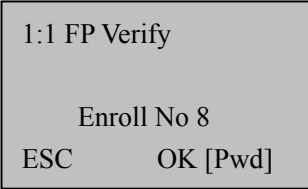
If your identity cannot be verified, you are prompted to try again, the following appears:



It continues for about 0.5 seconds, return to the start-up window.

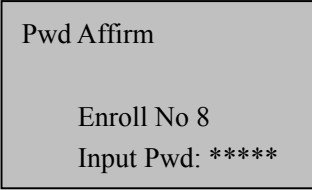
2.4.2 Password Verification

To start the enrollment process, enter your ID number, the following appears:



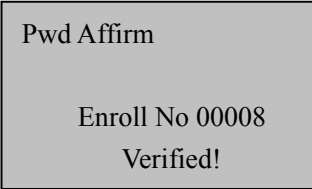
1:1 FP Verify
Enroll No 8
ESC OK [Pwd]

Press [OK], the following appears:



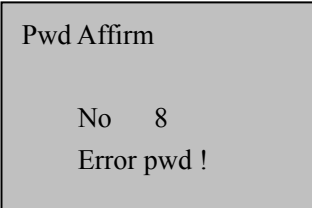
Pwd Affirm
Enroll No 8
Input Pwd: *****

Input correct password, press [OK], the following appears:



Pwd Affirm
Enroll No 00008
Verified!

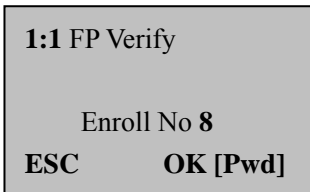
If the password cannot be verified, the following appears:



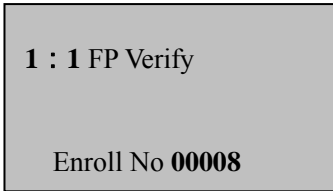
Pwd Affirm
No 8
Error pwd !

2.4.3 ID number & Fingerprint

To start the enrollment process, enter your ID number, the following appears:



If your identity is verified, the following appears:



2.5 Hints for Successful Enrollments

The fingerprint is of good quality, the verification speed will fast; Otherwise, it will verify slowly or occur to FRR.

In order to improve the fingerprint verification quality, the following hint appears:

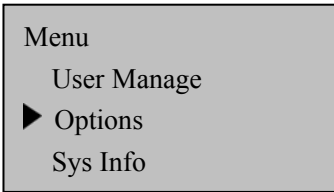
Table 2—1 Enrolled unsuccessful or the fingerprint of poor quality

Dry or dirty fingerprints	Solve the dry problem that rub the dry finger and palm. If the fingerprint is dry, you will adopt the way of wetting up the finger.
Have no enough to bring pressure	The user should place a finger firmly and squarely on the sensor surface.

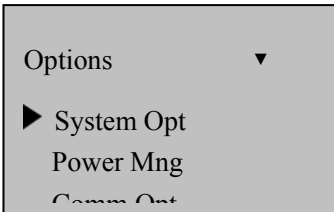
<p>How to select the finger?</p>	<p>Recommend to left or right index or middle finger. Use fingerprints of good quality, without worn or hurt. The user usually selects the forefinger, if it was of a poor quality, you will be recommended to middle finger or ring finger. If the user's finger area is less, you will select the thumb.</p>
<p>How to place the finger?</p>	<p>Place your finger firmly and touch the sensor surface must cover over 2/3 area. The fingerprint does not touch upright on the sensor surface. Do not touch the finger too fast; Do not move the finger on the sensor surface.</p>
<p>The influence of the fingerprints change</p>	<p>For users with worn or damaged fingers, the identification can be influenced. If the finger quality was poor, you will select password verification.</p>
<p>Others</p>	<p>However, few people's fingerprint quality is too poor to verify the fingerprint in gear. Please use ID & fingerprint verification, and the Match Threshold Levels can be reduced or use password verification.</p>

3. System Options

Press the [Menu], then verify your identity. The following appears:



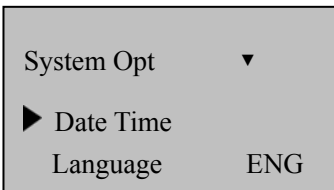
Access Options, press [OK], the following appears:



The following topics included: System Options, Power Manage, Communication Options, Log Options and Auto Test.

3.1 System Options

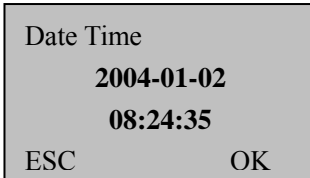
Access System Opt, the following appears:





The setup facility covers: System Options and Advanced Options.

3.1.1 Date Time

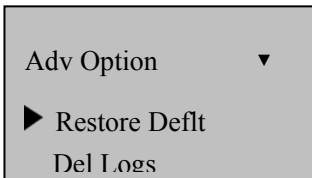
Access Date Time, the following appears:





To change the date, press  and , then input the correct date and time, press [OK]

3.1.4 Advanced Options

Access Advanced Option, press [OK], the following appears:



Press  and  to scroll up or down the screen to select the option.

Restore Default: restore all setup information to default.

Clear all Data: delete all enrolling fingerprints and logs.

Delete Logs: delete all logs of flash disk.

Clear Managers' rights: change the managers' rights into ordinary users' rights.

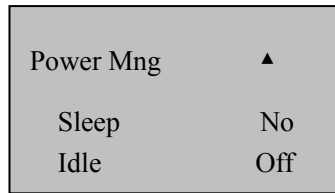
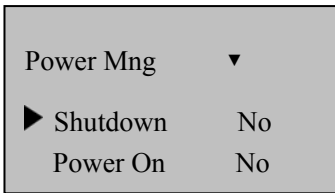
Show Score: whether show the quality value of fingerprint in the screen or not;

Match Threshold Levels: For helping in selecting threshold level settings, see Table 1.1.3.

Sound: whether use to phonic hint or not.

3.2 Power Manager

Access Power Manage, the following appears:



This product uses smart manage system, supports the time switch and resting features, it can satisfy the user's different demands.

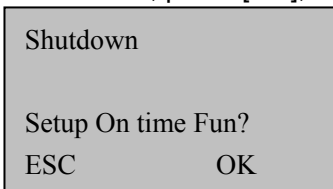
Shutdown: auto shut-off in the timed.

Power on: auto open-up in the timed.

Sleep: automatic resting in the timed, press any key to enter working state.

Idle and Idle Minute, they are related each other, while the idle minute is zero, the idle is closed; while the idle minute is not zero (unit was minute), for example, it is one minute, the user does not do anything in one minute, the system will enter the idle state.

Select Shutdown, press [OK], the following appears:



Press [OK], then enter Shutdown, press [ESC] to cancel.

3.3 Communication Options

Access Comm Opt, the following message appears:

Comm Opt	▼
▶ Dev Num	1
Baud Rate	1115200

Comm Opt	▲
Ethernet	Yes
RS232	Yes

Fingerprint T&A support **RS232**, **TCP/IP**, whether you use Single-Board Computer (SBC) or Networking, Fingerprint T&A will satisfy the user's demands.

Device Number: machine ID, the range is **1 to 255**.

Baud Rate: there are three options, 9600, 38400, 115200; The speed of communication is fast, recommend to use RS232; **IP address:** it defaults to IP address is 192.168.1.201.

Ethernet: whether use TCP/IP protocol or not.

RS232: whether use RS232 or not.

Link code: it defaults to code is 0, but can setting up

3.4 Log Options

Access Log Opt, the following message appears:

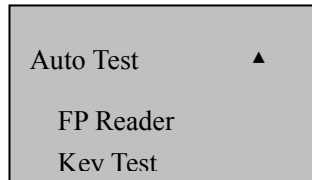
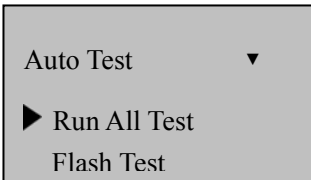
Log Opt	
▶ Alm AttLog	10
ReCheck Min	0

Alarm Attendance Log: when the remainder log capacity reached set numerical value, it will automatically sound a warning that logs were full.

Recheck Minute: Set within compass (Unit: minute). Someone's enrollment has enrolled, then, the log twice was not displayed in the system.

3.5 Auto Test

Access auto test, the following message appears:

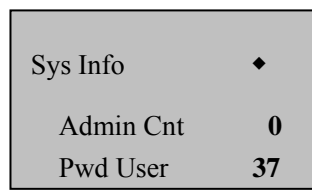
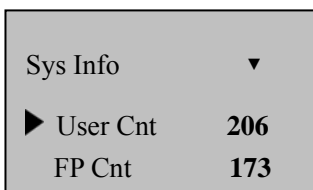


In the option, you can run system device test. When the device broken down, it can analyse the cause of the device's fault and the devices were quickly and easily maintained.

It tests the Memory, LCD, Sound, Fingerprint sensor, keypad and clock. In the course of test, you should guarantee the stability of the power. Otherwise, the system's hardware was probably damaged, especially it runs the memory test.

4. System Information

Access [Menu] to Sys Info, press [OK], the following appears:



Sys Info	▲
Pwd User	37
Res. Space Inf	

It displays user numbers, password numbers, fingerprint numbers, manager and log numbers in the screen. You can see some information such as the remainder log capacity in the memory, the device capacity, the defaults date, machine number and OEM's information are in the system.

5. Trouble shooting

1. Cleaning

From time to time, the optical platen, the keypad and display window require cleaning. Since working environments differ, it is not possible to define when cleaning should be performed. Following is guide:

Item	Cleaning Frequency
Keypad and display window	Cleaning when visibly dirty and hard to read. See cleaning the keypad and display below.
Optical platen	Do not over clean. The platen is designed to work under greasy or dirty conditions.

	However, do clean if the platen is obstructed or people are reporting deteriorating performance. See cleaning the Optical Platen below.
--	---

Table 5-1 Cleaning Schedule

2. Cleaning the Keypad and Display

To clean the keypad and display, use the same cleaning products as for the platen, and wipe dry.

3. Cleaning the Optical Platen

Clean the optical platen as follows:

(1) If dusty or gritty, first blow on the platen to clean off any loose particles.

(2) Spray on a light coating of a window cleaning product or other similar neutral detergent.

Warning: Do not use any other cleaner or the platen may become damaged.

(3) Using a non-abrasive and lint-free cloth, pat dry. Be careful not to scratch the platen. If lint particles adhere to the platen surface, blow them off when the platen is dry.