



XD401

1000 User Digital Biometric 'Fingerprint'
Access Control & Time/Attendance Unit

OPERATION MANUAL



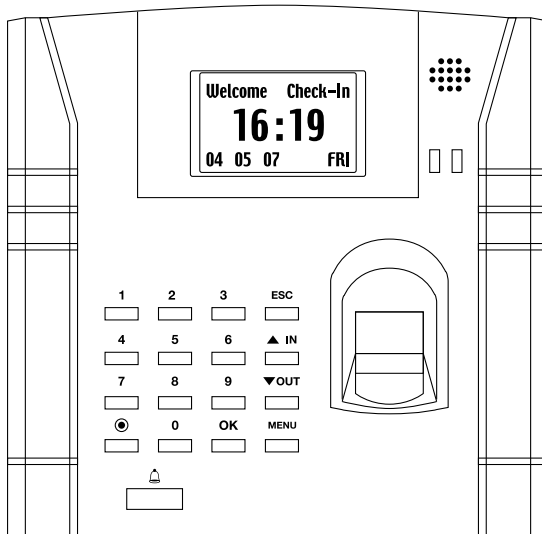
TABLE OF CONTENTS

I. Introduction	3
1.1 Basic Concepts	4
1.1.1 User Enrollment	4
1.1.2 User Verification	4
1.1.3 Match Threshold Levels	4
1.1.4 User ID Numbers	5
1.1.5 Authority (status) Levels	5
1.1.6 Start-up window	6
1.2 How to place the finger	6
II. Enrollment and Verification Procedures	7
2.1 Enrolling User	7
2.2 Testing an Enrollment	11
2.3 Enrolling a fingerprint for backup	12
2.4 Verifying Your Identity	12
2.4.1 Fingerprint Verification	12
2.4.2 Password Verification	13
2.4.3 ID & Fingerprint	14
2.5 Hints for Successful Enrollments	14
III. System Options	15
3.1 System Options	15
3.1.1 Date Time	16
3.1.2 Language	16
3.1.3 Lock Controller	16
3.1.4 Advanced Options	16
3.2 Power Manager	17
3.3 Communication Option	18
3.4 Log Options	18
3.5 Auto Test	19
IV. System Information	19
V. Maintenance	20

I. Introduction

This chapter is about the Main Features of the XD401 Fingerprint unit.

Product Appearance



Key Controls

- **OK - Confirm key:** Confirm your present operation.
- **MENU - Menu key:** Press down the key for seconds to enter the management interface in the initial status.
- **Cancel key:** Cancel your present operation.
- **Scrolling up key:** Scrolling up the menu
- **Scrolling down key:** Scrolling down the menu
- **IN - Check for ON of work**
- **OUT - Check OUT of work**
- **Power key:** Control the power on and off
- **Door bell**

1.1 Basic Concepts

This section contains definitions and descriptions of the XD401's features, including:

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

The two most important XD401's Functions are User Enrollment and User Verification.

1.1.1 User Enrollment

- Enrollment is the process to 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 Mach Threshold is a number that represents the degree to which the 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 normally called up via the keypad, but they can be called up through other means such as RF Card.

1.1.5 Authority (status) Levels

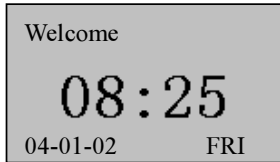
XD401 has four authority or status levels:

- 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.
- Managers can do other operations, except set advanced option and enroll manager's authority.
- Supervisors are Users who access to all functions and change all setup in the system.

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

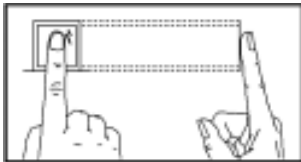
1.1.6 Start-up window

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

1. The correct way is:

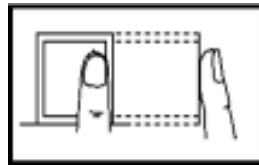


Place a finger **flat** on the sensor surface
Place it to the **center** of the sensor surface

2. The wrong way is:



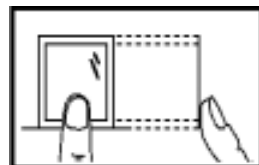
Vertical



Offset



Inclined



Lower

Note: Please adopt the correct way to place the finger. Xvision is not responsible for the malfunctioning results arising from improper pressing manners. Our company reserve ultimate the interpreting and modifying right for this.

II. Enrollment and Verification Procedures

This chapter describes how to enroll and verify users on the XD401 unit.

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, Manager, or Supervisor status to enroll users. For information on status levels, see “Authority (Status) Levels” on 1.1.5.

2.1 Enrolling Users

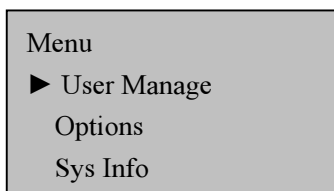
If this is the first enrollment in a new or empty system, everyone will become an enroller. If there is a manager in the system, you will have Manager status to enroll a new user. There are three ways of enrollment, fingerprint enrollment, password enrollment, fingerprint & password are suitable for 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.

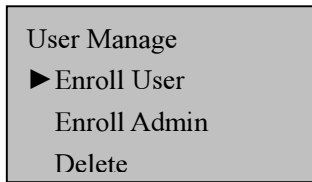
To start the enrollment process, identify yourself firstly - press [Menu], enter your ID number or fingerprint, and then verify your identity.

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

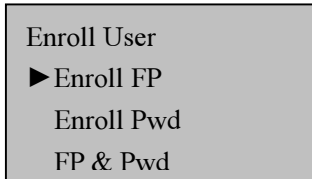
The following message appears on the display:



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

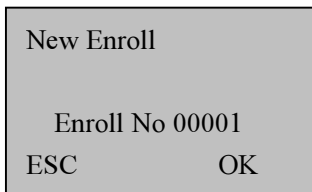


Press [OK], access the User Enrollment, the following message display:

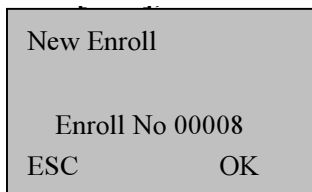


1. Fingerprint Enrollment

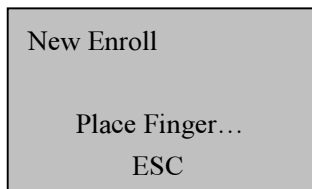
(1) Access the Enroll Fingerprint to press [OK], the following display:



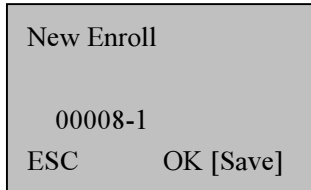
(2) Press [OK], the following appears:



(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:



```
New Enroll

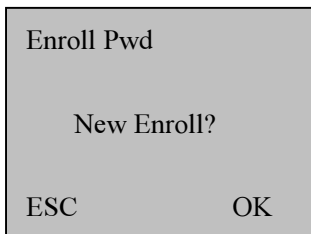
00008-1
ESC      OK [Save]
```

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. Password Enrollment

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

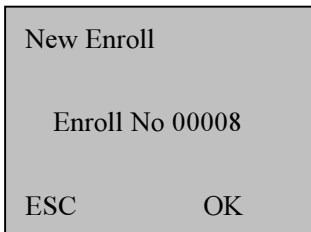


```
Enroll Pwd

New Enroll?

ESC      OK
```

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

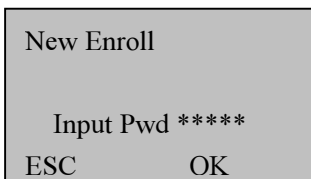


```
New Enroll

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.Fingerprint & Password

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

```
FP & Pwd

New Enroll
ESC      OK
```

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

```
New Enroll

Enroll No 00008
ESC      OK
```

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

```
New Enroll

Please finger...
ESC
```

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

```
New Enroll

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

(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.

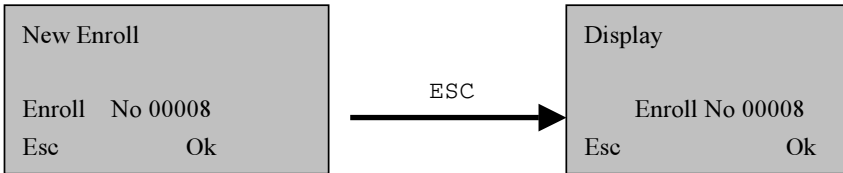
Press [OK], the previous message continues to be displayed while the template is created.

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 (for backup)

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



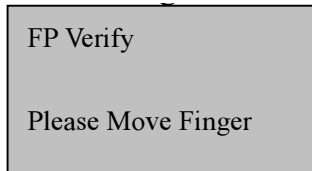
Note: Where system memory permits, it is advisable to have at least two fingers enrolled for a long-term user.

2.4 Verifying Your Identity

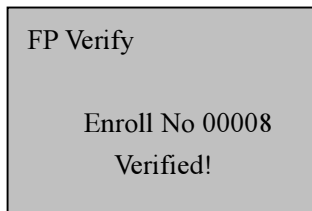
If visitors use XD401 to verify their identity, the system defaults to three ways of verification: Fingerprint verification, Password verification, ID number & Fingerprint. The following appears:

2.4.1 Fingerprint Verification

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

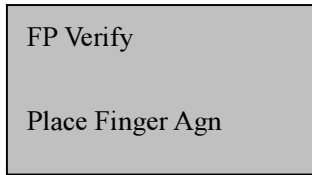


It continues for about 0.5 seconds. If the test is successful, it will say "Thank you", the following appears:



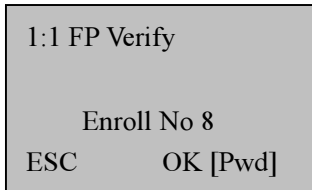
If your identity cannot be verified, you are prompted to try again, the following appears:

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

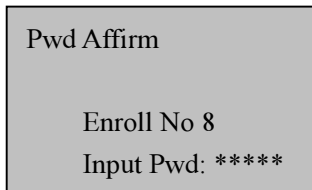


2.4.2 Password Verification

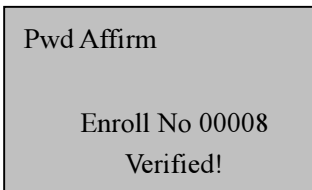
To start the enrollment process, enter your ID number, the following appears:



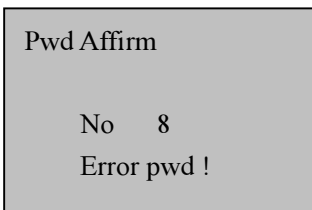
Press [OK], the following appears:



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



If the password cannot be verified, the following appears:



2.4.3 ID number & Fingerprint

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

1:1 FP Verify

Enroll No 8
ESC OK [Pwd]

If your identity is verified, the following appears:

1 1 FP Verify

Enroll No 00008
Verified!

2.5 Hints for Successful Enrollments

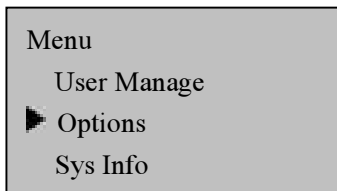
The fingerprint is of good quality, the verification speed will be fast; Otherwise, it will verify slowly or occur to FRR.

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

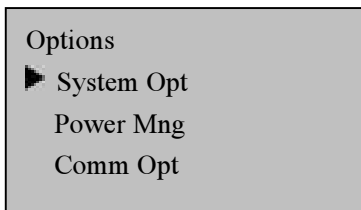
Dry or dirty fingerprints	<ul style="list-style-type: none"> • If the fingerprint is dry, you can adopt the way of wetting up the finger, such as breathing at the finger's tip. Pls. keep your finger in clean.
Have no enough to bring pressure	The user should place a finger firmly and squarely on the sensor surface.
How to select the finger?	<ul style="list-style-type: none"> • 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 is less, you will select the thumb.
How to place the finger?	<ul style="list-style-type: none"> • Place your finger firmly and touch the sensor surface must be over 2/3. • 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.
The influence of the fingerprints change	<ul style="list-style-type: none"> • For users with worn or damaged fingers, the identification can be influenced. • If the finger quality was poor, you will select password verification.
Others	<ul style="list-style-type: none"> • 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.

III. System Options

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



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

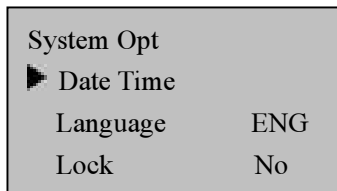


The following topics included:

- System Options
- Power Manage
- Communication Options
- Log Options
- Auto Test.

3.1 System Options

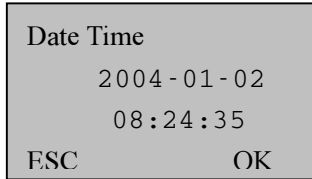
Access System Opt, the following appears:



The setup facility covers four areas: System Options, Language, Lock and Advanced Options.

3.1.1 Date Time

Access Date Time, the following appears:



3.1.2 Changing the Default Language

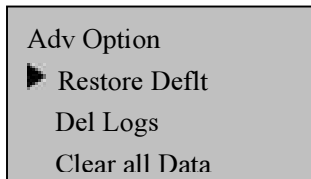
Access Language, press [OK], it defaults to SCH. Press to select another language. The XD401 unit comes with three built-in languages, simplified Chinese, traditional Chinese, and English for all displays. Select the language that you will use, press [OK], then Press [ESC] to return the Options. The system will ask for confirmation of the displayed language. Press [OK] to accept the language displayed.

3.1.3 Lock Controller

It defaults to close the lock signal output in the system. If you use access control feature, you will change [No] to [Yes], press [OK] to confirm, and then press [ESC] to return the Options. The system will ask for confirmation of the displayed controller, press [OK] to confirm.

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:

Power Mng	
▶ Shutdown	No
Power On	No
Sleep	No

Power Mng	±
Sleep	No
Idle	Off
▶ Idle Min	0

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:

Shutdown	
Setup On time Fun?	
ESC	OK

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
IP address	

Comm Opt	
Ethernet	±
RS232	No
▶ RS485	Yes

The XD401 supports RS232, RS485, TCP/IP, whether you use Single-Board Computer (SBC) or Networking Computer.

- **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; The speed of low communication is stable, recommend to use RS485.
- **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.
- **RS485:** whether use RS485 or not.

3.4 Log Options

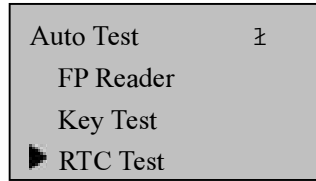
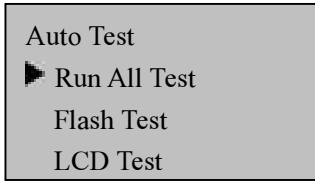
Access Log Opt, the following message appears:

Log Opt	
▶ Alm AttLog	1
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

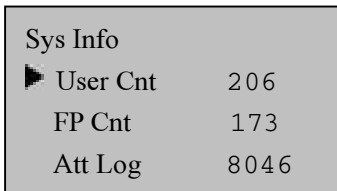
Access Auto Test, the following message appears:



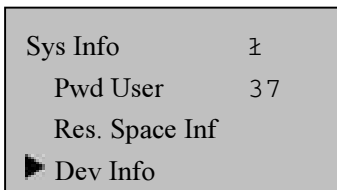
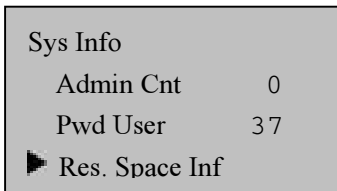
In the option, you can run system device test. If the unit breaks down, it can analyse the cause of the device's fault and the devices were quickly and easily maintained. It tests the Memory, LCD, Sound, Fingerprint sensor, keypad and clock. During the course of the test, you should guarantee the stability of the power. Otherwise, the system's hardware was probably damaged, especially if it runs the memory test.

IV. System Information

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



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 manufacturer information are in the system.



V. 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.

Table 5-1 Cleaning Schedule

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.

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.