www

TIME CLOCK WORLD

888 534-5994

AMANO

FPT-40

USER MANUAL

AMANO®

Time Guardian®
FPT-40 Fingerprint
Data Collection Terminal

Installation & Operation Guide

Proprietary Notice

This document contains proprietary information and such information may not be reproduced in whole or part without the written permission from Amano Cincinnati, Inc. 140 Harrison Ave., Roseland, New Jersey 07068.

Amano Cincinnati, Inc. reserves the right to make equipment changes and improvements, which may not be reflected in this document. Portions of this document may have been updated to include the latest hardware or firmware version, if applicable.

To ensure safe use of this terminal, be sure to thoroughly read this manual in its entirety before any attempt is made to operate the equipment. After you have finished reading this manual, be sure to store it and in a safe place for further reference.

Thank You….

For purchasing another fine product from
Amano Cincinnati, Inc.

For more information about Amano's complete line of products, visit our web site at:

www.amano.com

About This Manual

This manual covers the following FPT-40 Fingerprint terminal with Amano Part Numbers:

- **FPT-40/A842** - Fingerprint terminal only.
- **FPT-40/A843** - package with USB 50 ft. CommStik™ cable, 6ft Cat 5 network cable, and Time Guardian software.
- **AUS-10035X** - CommStik 50 ft. cable only.
- **EOE-108540** - Ethernet 6 ft. Cat 5 cable only.

Table of Contents

Table of Contents i

Chapter 1: Introduction & Installation 1-1

Introduction 1-1
FPT-40 Fingerprint Terminal..1-2
Benefits 1-2
Specifications..1-2
Installation..1-3
Unpacking Fingerprint Terminal/Time Guardian Package....1-3
Before Installing FPT-40 Fingerprint Terminal......................1-3
Understanding the FPT-40 Fingerprint Terminal Front Panel 1-4
Mounting the FPT-40 Fingerprint Terminal...........................1-5
Communication Connections 1-7
Serial Connection (Direct Connect) 1-7
Ethernet Connection 1-9

Chapter 2: Fingerprint Operation 2-1

Getting Started..2-1
Start-up Welcome Screen (Power On) 2-1
Normal Punch IN/OUT Display 2-2
Normal Use...2-3
Punching with a Fingerprint (FP) 2-3
Punching with a Password (Pwd) 2-4
Punching with a Fingerprint (FP) and Password (Pwd) 2-6
Enrolling Users at the FPT-40 Terminal 2-6
Introduction 2-7
User Identification/Verification 2-7
Threshold 2-7
Priviledge (Status) Levels 2-8
Proper Finger Placement...2-8
How to Enroll a User with a Fingerprint 2-10
How to Enroll a User with a Password................................2-14
How to Change a User Password with Backup Enroll 2-17
How to Enroll a User with Fingerprint and Password..........2-20
How to Enroll Multiple Fingers for a User 2-23
Defining Privileges with Enrolling Admin Option....................2-31
Deleting Users 2-33
How to Restore Deleted Users From Time Guardian 2-36

Table of Contents

Options Menu 2-36
System Option Menu 2-36
Setting the Terminal Date & Time....................................2-37
Setting the Display Time Format......................................2-38
Setting the Language..2-39
Setting the Display Date Format 2-39
How to Set Daylight Saving (DLS) Time 2-40
Advanced Options (Adv Option) Menu 2-41
Power Management Menu...2-43
Communications Options Menu...2-45
Log Options Menu 2-48
Auto Test 2-49
Sys Info Menu...2-50

Chapter 3: Troubleshooting...3-1
Diagnostics 3-1
Run All Test 3-2
FLASH Test 3-3
LCD Test..3-3
Voice Test 3-4
FP Reader Test..3-4
Key Test...3-5
RTC Test..3-5
Frequently Asked Questions (FAQs) 3-5
Maintenance 3-7
Cleaning..3-7
Cleaning the Keypad and Display......................................3-8
Cleaning the Optical Sensor 3-8
Replacing Optical Sensor Lens 3-9

Chapter 4: Time Guardian Interaction 4-1
Configuring Time Guardian for the FPT-40 Terminal 4-1
Clock Tab (Communication Settings) 4-1
Connecting a Fingerprint Terminal to Time Guardian........4-2
Assignments Tab - Clock 4-5
Using the Fingerprint Commands Tab 4-6
Communication Menu..4-9
Employee Privileges Setup 4-11

Chapter 1: Introduction & Installation

Introduction

The FPT-40 Fingerprint terminal provides a sophisticated fingerprint recognition and data collection terminal for use directly with Time Guardian to provide a complete PC-based time and attendance solution for small business. Fingerprint recognition is considered to be one of the good forms of biometric security because of its accuracy, affordability, and ease-of-use.

The FPT-40 Fingerprint terminal and Time Guardian provides a system that automatically calculates and accumulates hours worked based on a company's payroll policies. This system separates the hours worked into regular and overtime pay categories and displays them at the terminal (see Normal Punch IN/OUT Display on page 2-2).

The Time Guardian time and attendance software also offers many sophisticated features to simplify payroll preparation, such as: Lock Out, Revision, Red Print with Grace Zones, Flexible Rounding Rules, Unpaid and Paid Breaks, and Time Card Reports, to name a few. In addition, easy-to-read management reports are available in hours or dollars to provide accurate and timely labor information.

See Configuring Time Guardian for the FPT-40 Terminal on page 4-1 for details on setting up the Time Guardian time software on the host PC to communicate with the Fingerprint terminal.

In order to use fingerprint recognition, a user must enroll their fingerprint in the fingerprint template database. The FPT-40 Fingerprint terminal will record the user's fingerprint template, encrypt it, and store the data. When a user presents their finger for verification, a new template is captured and compared to the pre-enrolled fingerprint in the database. If there is a match, the user will be accepted by the FPT-40 Fingerprint terminal.

One of the main benefits of this system is that it eliminates fraudulent punches ("Buddy Punching"), while providing a comprehensive and secure method when coupled with the Time Guardian software of accurately accounting for employee labor costs.

The FPT-40 Fingerprint terminal also provides repunch protection at the terminal when the "ReCheck Min" feature is set. Multiple punches within the setting time frame will be verified but not recorded at the terminal in flash memory (see Log Options Menu).

FPT-40 Fingerprint Terminal

Benefits

- Sophisticated algorithms provide dependable and accurate identification speed to process fingerprints within 2 seconds.
- A built in embedded standalone module (ZEM100) with robust Intel 32-bit X-scale CPU.
- Supports 360-degree finger rotation for easy-to-use identification.
- Sensor window design improves image quality, while accepting dry, or wet fingers.
- CMOS automated exposure and intelligent compensation provides improved image quality.
- Adjusts for image distortion to assure fingerprint matching consistency.

Specifications

Operating Environment:	32°F to 105°F (0°C to 42°C) with 20 - 80% relative humidity, non-condensing.
AC Adapter Power Input:	100 - 240 VAC ±10%, 50-60 Hz
AC Adapter Power Output:	DC 5V 2A
Dimensions:	7.90." L X 5.35" W X 1.96" D (200 mm L X 136 mm W X 50 mm D)
Weight:	1.35 lbs. (0.61 kg)
Daylight Saving Time (DST):	Settings are programmable at the terminal and/or through Time Guardian software.
User Capacity:	1500
Transaction Storage:	30000
Verification Method:	Fingerprint, Password, Fingerprint + Password.
Verification Mode:	1:N
Verification Time:	≤ 1 second
Identification Time:	≤ 2 seconds
Enrollment Time:	≤ 5 seconds
False Acceptance Rate (FAR):	≤ 0.001%
False Rejection Rate (FRR):	≤ 1%
Communication:	Ethernet: 10 Base-T/100 Base-TX (TCP/IP) RS-485, or RS-232C
Communication Speed:	38400/19200/9600 BPS, TCP/IP: 10M

Specifications (Cont.)

Memory Backup:	Provides up to 3 years of continuous memory backup without AC power.
Display:	2.8” diagonal, 128 x 64 dots resolution LCD reflective (backlight).
Keypad:	4x4 keypad (0~9, OK, ESC) + 4 function keys.
Clock:	Quartz oscillator, accuracy within ± 3 seconds per week at normal temperature.

* Specifications and/or operational characteristics are subject to change without notice. The AC adapter is UL listed E215890.

CE

Installation

Unpacking Fingerprint Terminal/Time Guardian Package

In addition to this guide, your package should include the following:

- Fingerprint Data Collection Terminal
- AC Adapter
- USB-to-serial connector (RJ-11) with 50ft cable
- 6 foot Ethernet cable
- Terminal mounting plate and hardware
- Time Guardian Software Installation Manual
- Time Guardian CD
- Spare sensor lens/prism (see Replacing Optical Sensor Lens). **Locate this item and store in a safe place for possible future use!! DO NOT DISCARD.**

Before Installing FPT-40 Fingerprint Terminal

- Before installation, please make sure the unit is not connected to power. Connect the power to the unit as the last step.
- The recommended proper height to mount the device is 55 – 60 " (1.4 – 1.5 meters).
- Use only the AC adapter provided. Use of another AC adapter may damage the unit and void the warranty.

- Before connecting the device, please read and follow the installation instructions. Failure to do so could cause equipment failure; Amano is not responsible for any damages.
- Please use the enclosed cable [either 6ft Ethernet, or 50 ft USB-to-Serial cable to connect the FPT-40 Fingerprint terminal. If longer serial cables for direct connect are required please consult Amano.

Understanding the FPT-40 Fingerprint Terminal Front Panel

The front panel of the FPT-40 Fingerprint terminal (see **Figure 1-1**) contains the following controls:

- **LEDs:** During normal standby operation (power on), the **Green LED** will flash once per second, and stay on momentarily when a user successfully verifies. If a user fails to verify, the **Red LED** will momentarily stay on.

Note: If the fingerprint reader does not follow the standard LED operational parameters, please consult support.

- **Speaker:** Provides audible voice verification of operations, i.e., "*Thank you*", *"Incorrect Password"*, "*Access Denied*", "*Invalid Id*", *"Please try again"*, etc. See Advanced Options on page 2-41 for voice control.
- **LCD Screen:** Displays time, date, day, and operational information.
- **Fingerprint Sensor:** Enrolls (creates) template and verifies fingerprint.
- **Keypad:** Used to input User ID, password, and perform menu operation with the following keys:
  - **ESC –** to perform exit, cancel, ignore when using the Menus.
  - **MENU** – to access Menu structure.
  - **OK** – to confirm and/or save selection.
  - **⦿ -** power ON/OFF button.
  - ▼ or ▲ - to scroll down or up for menu operations.

Note: Press the Power ON/OFF ⦿ button to turn off the terminal.

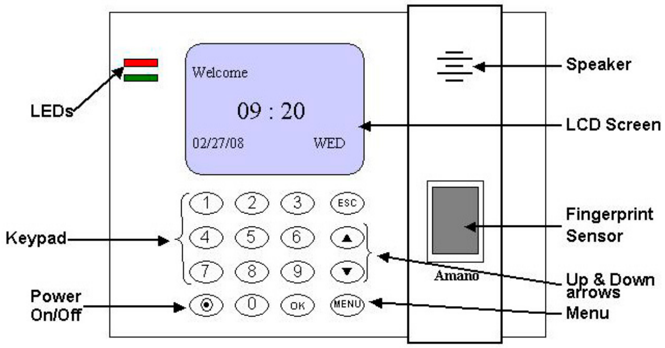


Figure 1-1 FPT-40 Fingerprint Terminal Front Panel

Mounting the FPT-40 Fingerprint Terminal

Warning! Before selecting a mounting location for your FPT-40 Fingerprint terminal, you must consider the following:

- The mounting surface and hardware must be able to support the unit's weight, 1.35 lbs. (0.61 kg).
- The area must be within the specified operating temperature & humidity range (see Specifications on page 1-2).
- The FPT-40 Fingerprint terminal should be mounted in an environment that avoids the conditions pictured in the following figure:

HEAT SOURCE
DIRECT SUNLIGHT
AND HUMIDITY
RAIN
WATER
STRONG
VIBRATION
AND SHOCK
DUST, CORROSIVE
GAS, STEAM AND SALT
DAMAGE

- Close proximity to a wall outlet (≤ 6 ft), and a wall that can accommodate signal and/or power conduits.
- If using Ethernet, close proximity to an Ethernet connection (≤ 6 ft).

Once a mounting location has been chosen, perform the following:

1. Loosen and remove the four (4) back plate retaining screws to remove the back plate as shown (see **Figure 1-2**). Set the FPT-40 terminal face up on a flat surface.

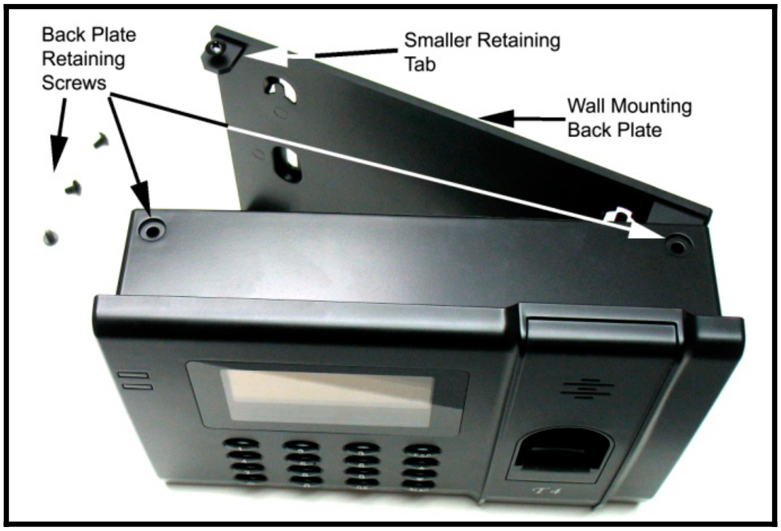


Figure 1-2 Back Plate For Wall Mounting

2. Using the back plate as a template, mark the location of the upper mounting holes on the wall. Mark a vertical line on the wall as a guide to align the lower mounting holes.

Note: Pay attention to the orientation. The back plate should only be mounted one-way as it is keyed to fit into the back of the fingerprint reader.

3. Install a screw or anchor at the mark and hang the back plate from the top-mounting holes. Level the back plate by centering the vertical line in the bottom holes.
4. Mark the location of the bottom holes.
5. Install the screws or anchors for the bottom-mounting holes and secure the back plate to the wall.
6. Insert the back of the fingerprint reader onto the four (4) retaining tabs. The tabs are keyed to accept the fingerprint reader only one way! Secure the reader to the tabs by inserting and tightening the 4 retaining screws.
7. Your fingerprint reader is now mounted to the wall and ready to connect the data and power lines. After wall mounting, remove the dustproof film on the sensor window. Proceed to the next section, *Communication Connections*.

Communication Connections

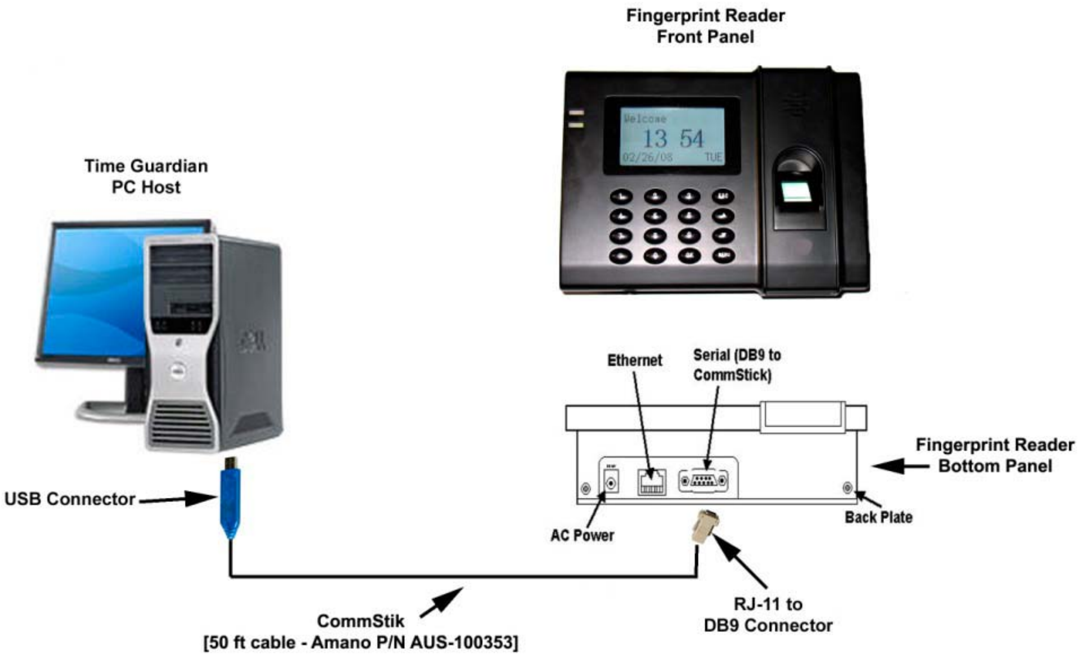
A connection between your Host PC and the terminal(s) is/are based upon your application.

Serial Connection (Direct Connect)

You should use the Amano CommStik™ [part number AUS-10035x] (50 foot RJ-11 to USB) Communications Cable (included) to interface with the host PC.

RS-485 communications can be used for systems requiring up to 31 terminals. You will require the following accessories for each additional RS-485 terminal:

- AMX-206950: Communications Cable – 10’, 6 conductor RJ-11
- AMX-206700: Junction Box



Fingerprint Reader Front Panel
Welcome
13 54
02/26/08
TUE
Time Guardian PC Host
Ethernet
Serial (DB9 to CommStick)
Fingerprint Reader Bottom Panel
USB Connector
Back Plate
AC Power
RJ-11 to DB9 Connector
CommStik
[50 ft cable - Amano P/N AUS-100353]

Figure 1-3 Serial Direct Connection with CommStik

Note: If the distance between the terminal and the host PC is more than 50 feet, two junction boxes will be required.

The connections between the host PC and multiple serial terminals for this application are as follows:

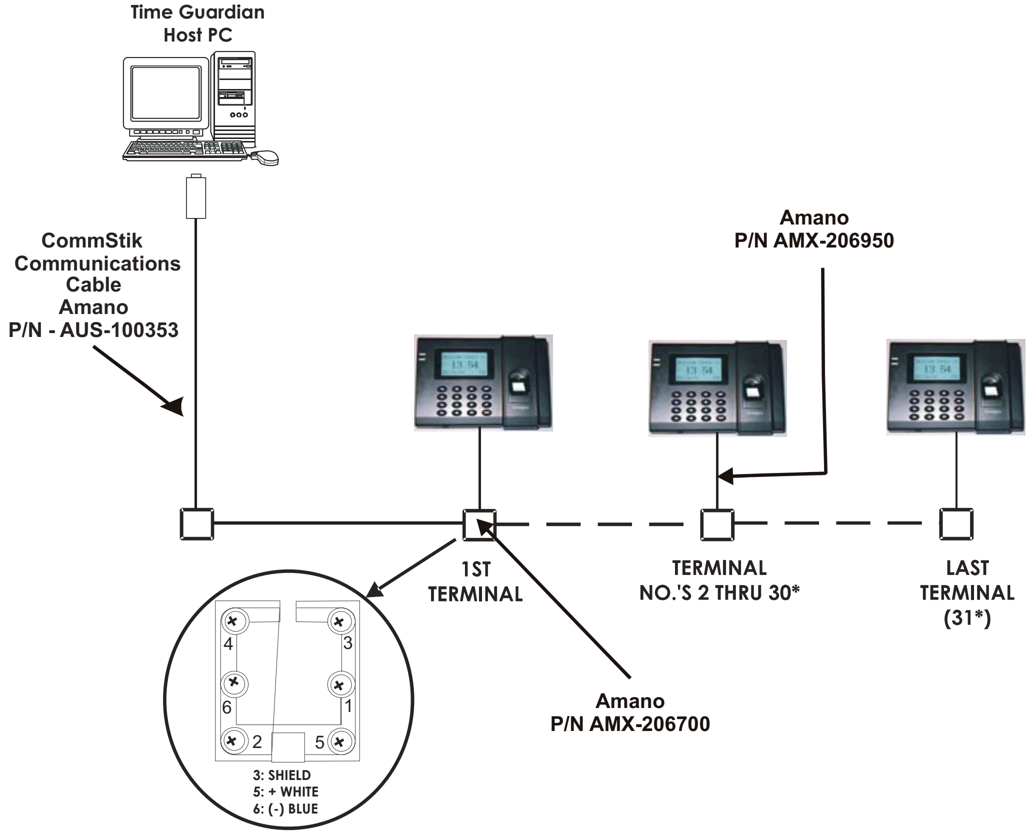


Figure 1-4 Multiple Direct Connect Serial Terminals

* The maximum number of terminals is dependent upon the distance and the quality of cabling used. It is recommended that Belden Low Voltage Computer Cable, P/N 9841 or equivalent, be used to connect the junction boxes for this application.

Warning! Please note that terminal #3 (used for the RS-485 cable Shield) is disconnected from the internal RJ-11 receptacle of the junction box. This is deliberate; the shield connection is **NOT** fed through to the Terminal.

Ethernet Connection

Networked terminals can be connected to a standard 10Base-T or 100BaseTX computer network. In addition, each networked terminal can have a group of up to 29 serial terminals connected via RS-485.

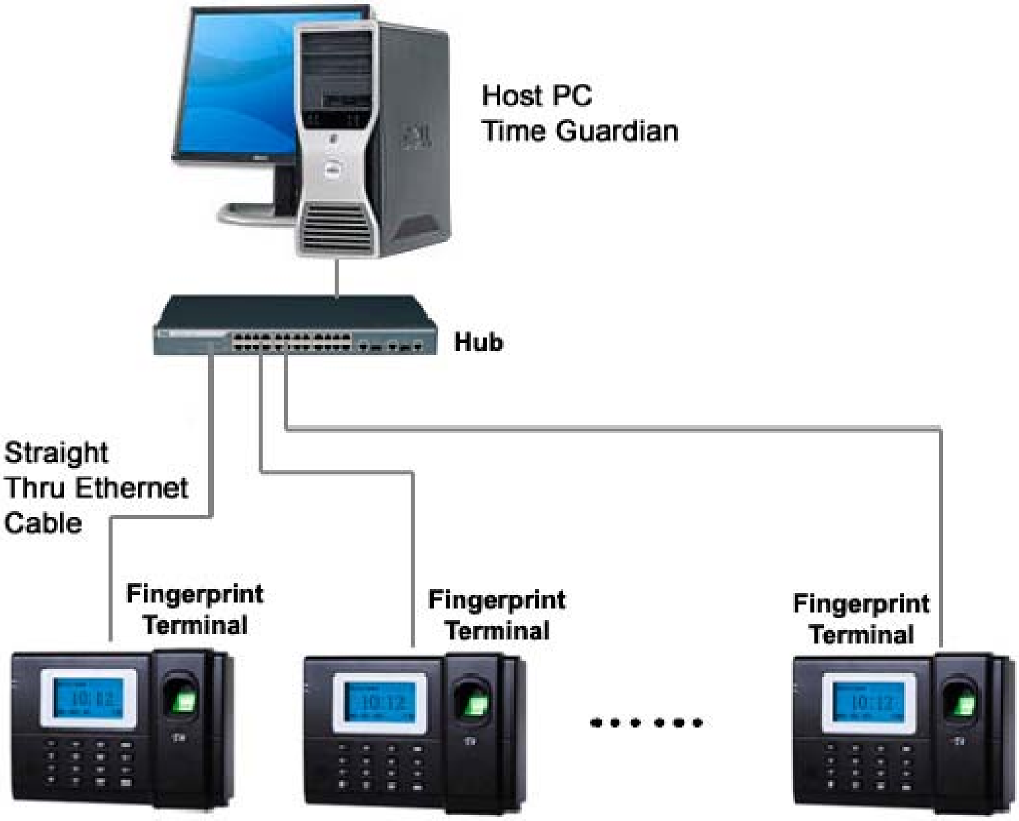


Figure 1-5 Networked Terminal(s)

Note: The serial connections for the RS-485 branch network are the same as for the RS-485 wiring described previously.

This page intentionally left blank.

Chapter 2: Fingerprint Operation

Getting Started

Start-up Welcome Screen (Power On)

Once the terminal is wall mounted and the communication connections have been made, connect the terminal to AC power (see figure) and power on to setup and enroll users.

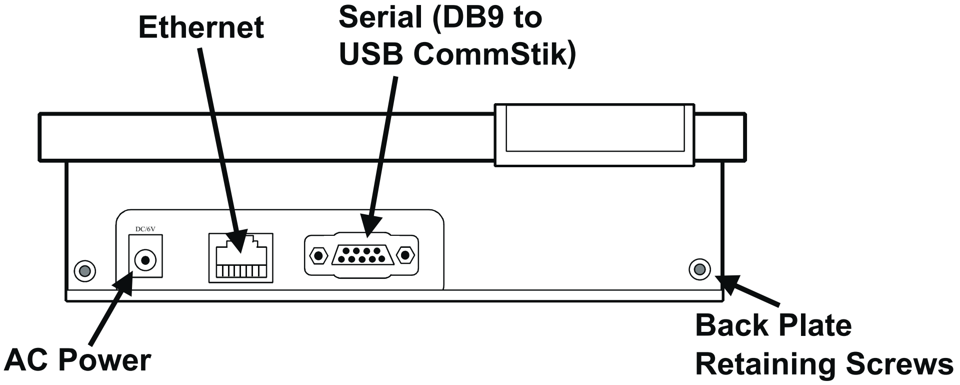
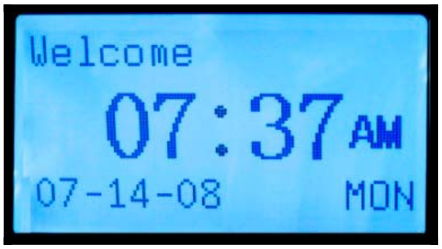


Figure 2-1 FPT-40 Fingerprint Terminal Bottom View

To start-up perform the following:

- Ensure the AC Power Adapter is connected to the FPT-40 terminal and plugged into an outlet. Press the power ⦿ button. The FPT-40 terminal, will display the splash screen, perform a diagnostic check, and then display the Welcome screen (see figure).



Welcome
07:37 AM
07-14-08 MON

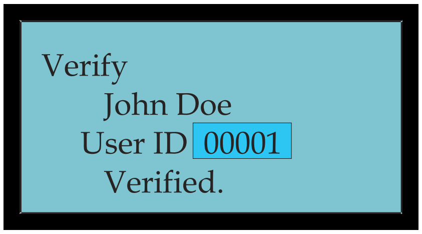
Figure 2-2 Welcome Screen

Note: The time and date can be set with the terminal keypad, or downloaded to the terminal from the host PC utilizing the Time Guardian software. The information such as date, time, daylight saving time (DST), finger templates, and hours worked sent from Time Guardian will have precedence over existing similar information. That is to say Time Guardian will act as the master.

- Upon power up, the **Green LED** indicator will blink once every second to signify the terminal is operating properly. The FPT-40 terminal should now be ready to enroll users.
- All normal time and attendance functions (validation for punch in/out) must be performed from the "Welcome" screen.
- Press the power On/Off ⦿ button to shutdown the FPT-40 Fingerprint terminal and display "*halting system….Shutdown 2 secs, 1sec*". The FPT-40 terminal will retain all templates and transactions while the power is off. See Power Management Menu on page 2-43 for additional information on configuring the terminal for auto-sleep and wake up functions.
- If necessary additional diagnostic tests can be performed to confirm the unit is performing properly (see Diagnostics on page 3-1).

Normal Punch IN/OUT Display

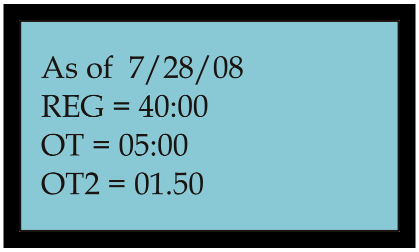
The system is ready to use after the FPT-40 terminal and the host PC with Time Guardian software are connected and setup. Upon recognition at the terminal, the terminal will first briefly display his/hers name [first 8 characters of the first and last name combined], followed by the User ID and validation status (see figure).



```
Verify
     John Doe
   User ID 00001
     Verified.
```

Figure 2-3 Validation Screen

Next, the terminal will display the "*As of*" date followed by the current pay period hours worked for the user that just punched in (see figure for example).



```
As of  7/28/08
REG = 40:00
OT = 05:00
OT2 = 01.50
```

Figure 2-4 Hours Worked for Pay Period

Note: The current pay period information is transferred from Time Guardian to the terminal(s) during a download and can be retained at the terminal for up to 14 days between downloads.

Normal Use

The following "Normal Use" sections assume the FPT-40 Fingerprint terminal has been setup with enrolled users and system options have been defined. Please see Enrolling Users on page 2-6 and the other sections for enrollment details, etc.

Punching with a Fingerprint (FP)

1. From the Welcome screen place your enrolled finger in the sensor window (see figure).

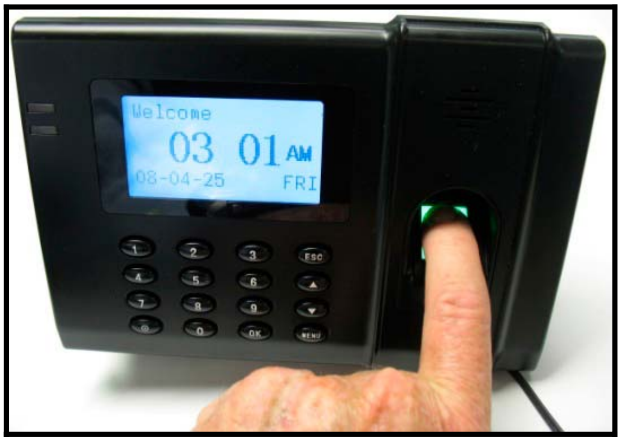
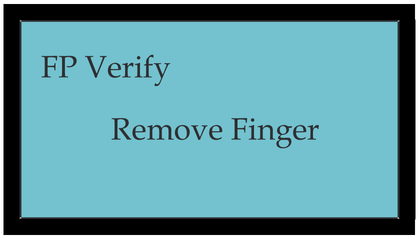


Figure 2-5 Punching Using Biometrics

Note: If your primary finger is damaged [i.e., cut], please use an enrolled backup finger or a password to ensure a successful punch.

2. Follow the on screen prompt, *"FP Verify…Remove Finger"* (see figure).

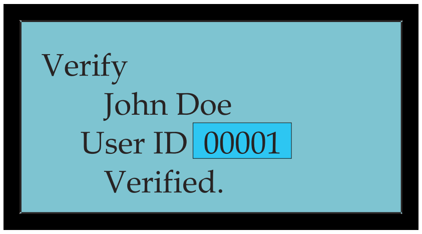


FP Verify

Remove Finger

Figure 2-6 Fingerprint (FP) Verify

3. Upon verification, the **Green LED** will momentarily stay on, the screen will briefly display your Name, User ID, and the confirmation "*Verified.*" (see figure) with the voice prompt "*Thank you*", followed by the momentary display of your hours worked (see **Figure 2-4**) for the active pay period.



Verify
John Doe
User ID 00001
Verified.

Figure 2-7 Validation Screen

Note: The name, assignments, and current pay period information are downloaded from Time Guardian to the FPT-40 terminal.

Note: An invalid finger entry will flash the error message, "*Please Try Agn.*", with the same voice prompt. The **Red LED** will momentarily stay on.

Note: When ReCheck Min is set, if an employee punches more than once within the time setting [usually 1 – 2 mins.], the voice prompt will be "Punch accepted…thank you" and no pay period hours will be displayed (see Log Options Menu).

Punching with a Password (Pwd)

1. From the Welcome screen enter your User ID using the keypad and press **OK** to confirm ID (see figure).

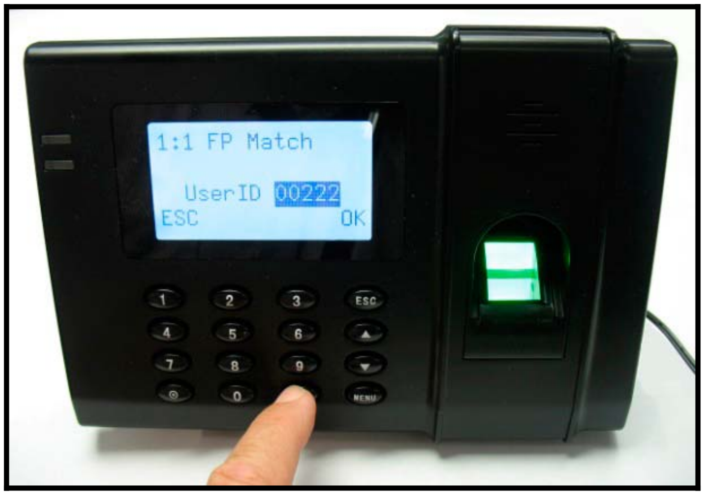
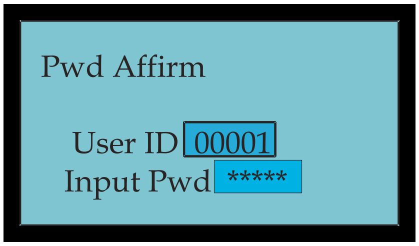


Figure 2-8 Enter User ID

2. Input your password to affirm (see figure).



Pwd Affirm

User ID 00001
Input Pwd *****

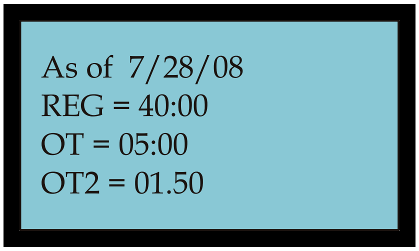
Figure 2-9 Input Password

Note: An invalid password entry will flash the error message, "*Error Pwd.*", and the voice prompt, "*Incorrect password*". The **Red LED** will stay on until the correct password is entered or the password entry times out and the terminal returns to the Welcome screen.

Note: The user will be prompted to "*Place Finger*" if they do not have a password.

3. Upon verification, the screen will display your Name, User ID, and the confirmation "*Verified.*" with the voice prompt "*Thank you*".

   Next, the display will momentarily show the "*As of*" date followed by the current pay period hours worked for the user that just punched in (see figure for example).



As of 7/28/08
REG = 40:00
OT = 05:00
OT2 = 01.50

Figure 2-10 Hours Worked for Pay Period

Note: When ReCheck Min is set, if an employee punches more than once within the time setting [usually 1 – 2 mins.], the voice prompt will be "Punch accepted…thank you" and no pay period hours will be displayed (see Log Options Menu).

Punching with a Fingerprint (FP) and Password (Pwd)

1. From the Welcome screen either place your finger on the sensor or enter your assigned User ID using the keypad.

2. Follow the on screen prompt to remove finger (see figure) or input your password.

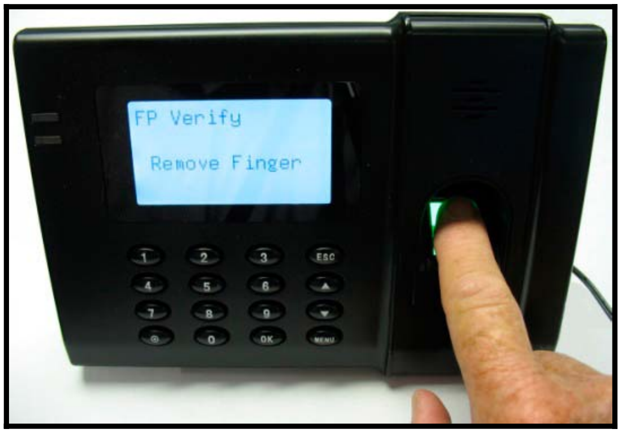


Figure 2-11 Remove Finger

3. Upon verification, the screen will display your Name, User ID, and the confirmation "*Verified.*" with the voice prompt "*Thank you*" followed by the momentary display of your hours worked for the active pay period.

Note: The advantage of being enrolled as a user with a fingerprint template and password is that you can use either method to punch. This provides an automatic backup should you encounter any problems with fingerprint validation. Therefore, the first method used and accepted is the only method you need to validate a punch.

Enrolling Users at the FPT-40 Terminal

After installing the FPT-40 Fingerprint terminal and powering on, you may begin enrolling users. If this is the first enrollment in a new or empty system, everyone will be able to enroll. However, if there any users with privileges already setup in the system, you will have to be enrolled by a user with privileges. The FPT-40 fingerprint reader provides the following three methods for enrollement; fingerprint, password, or fingerprint and password [in this instance the 1st method submitted and accepted is used].

⚠ ***Caution!*** Use care when enrolling users at the terminal as the **ESC** button can alter the entry fuctions during some operations.

Introduction

User Identification/Verification

This is the process of comparing a user's finger against the stored map, and/or verifying a user from a stored password number (5 digit max). After performing the verification process the system will indicate success or failure while also storing all verified punches for transfer to Time Guardian.

Threshold

The threshold is a predefined number, often controlled by the administrator, which establishes the degree of correlation necessary for a sucessful match. If the score from the template comparison exceeds the threshold, the templates are considered a match. The threshold establishes a balance between False Acceptance Rate (FAR) and False Rejection Rate (FRR). FAR indicates the probability that a biometric system will incorrectly identify an individual or will fail to reject an imposter.

You can set the threshold for all users. For a user who has a difficult fingerprint verification, it is recommended to use ID & fingerprint verification (match one-to-one). Raising the threshold increases security, while lowering it increases the passing ratio. The correct balance can be vital. For example, a user whose finger is worn or injured should have a reduced threshold.

The FAR and FRR values affect each other. As FAR is increased, FRR should be decreased. The default one-to-many threshold is 35, while the 1:1 matching default threshold is 15 (see the following table).

Table 2-1 Recommended Threshold Level Settings

FRR	FAR	One-to-Many	One-to-One
High	Low	45	25
Middle	Middle	35	15
Low	High	25	10

Priviledge (Status) Levels

The status levels define the ability of a user to perform specified administrator and other tasks including the ability to view, edit, add, and renew specified information categories. The four status levels can be assigned at the FPT-40 terminal or from Time Guardian, and modified as required. These four (4) levels (see Defining Privileges with Enrolling Admin Option on page 2-31) are:

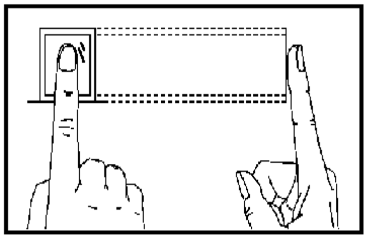
- User – person whose identity must be verified to punch and have their attendance recorded in Time Guardian. Cannot perform any enroller, supervisor, and administrator functions.
- Enroller – person who is authorized to enroll users or delete them from the FPT-40 Fingerprint terminal.
- Supervisor – person who can perform all operations, except set advanced options and enroll a user with Admin priviledges.
- Administrator – person who has access to all functions, including system setup. (see procedure for clearing).

Proper Finger Placement

Make sure the fingerprint image captured contains the core part of desired finger, because a fingerprint is the impression of the friction ridges of all or any part of the finger. Also when enrolling a finger, use a slightly adjusted angle for each finger press, i.e, one to the center, one inclined slightly to the left, and a third inclined slightly to the right. If these techniques are followed; the success rate should increase dramatically.

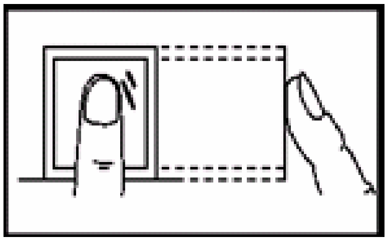
The correct way to place a finger on the sensor is:

- Place the finger flat on the center of the sensor surface (see figure for front and side view).

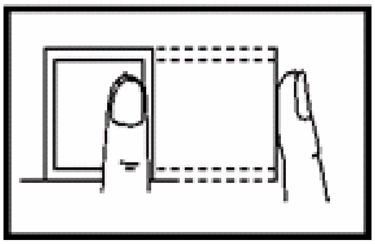


The wrong ways to place a finger on the sensor are:

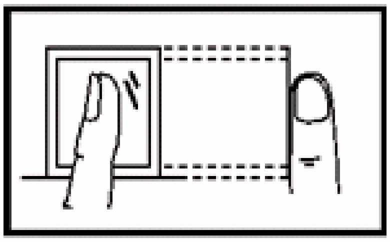
Vertical



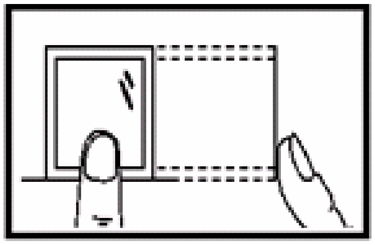
Offset



Inclined



Lower



The following hints are provided as suggestions to help obtain a good fingerprint enrollement.

Table 2-2 Fingerprint Enrollment Hints

Problem	Suggested Solution
Fingerprint is too dry or dirty.	Wipe finger, and/or moisten.
Not enough pressure.	Place finger firmly and flat on the sensor.
How to select finger?	Use the finger alongside your thumb. Select fingers that are not worn or injured. If the fingers are small, use the thumb.
Finger placement?	Place at least 2/3 of the finger firmly on the sensor. Do not touch the finger too fast and do not move the finger on the sensor until prompted.
Finger pattern change?	Re-enroll your finger if your fingerprint changes as a result of an injury, etc.
Other reasons	Use password registration as an alternative for people with poor quality fingerprints. Also, the threshold setting can be reduced.

Enrollment is the procedure to associate a User ID with a fingerprint by scanning a user's finger three (3) times to create a template (see figure).

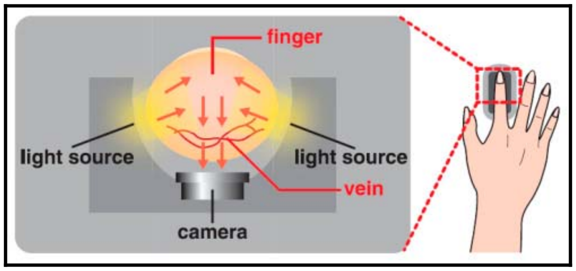


Figure 2-12 Finger Template Creation

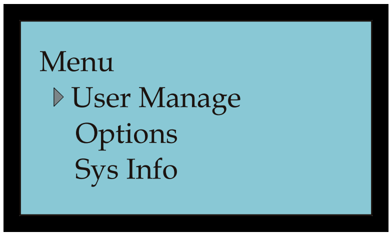
Note: Enrolling more than two (2) fingers per user might adversely effect the amount of user templates that can be stored in the fingerprint reader.

How to Enroll a User with a Fingerprint

The following procedure details how to enroll a new user with a fingerprint template. It is suggested to enroll 2 fingers so the employee has a backup finger when needed, i.e., bandaid or finger injury.

To enroll a fingerprint at the FPT-40 terminal perform the following:

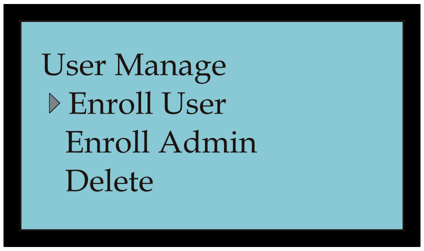
1. Press the **Menu** button to display the main menu (see figure), or display "*Admin Affirm 1*" and login with privileges.



Menu
▷ User Manage
Options
Sys Info

Figure 2-13 Main Menu

2. Press **OK** to display the User Manage menu (see figure)



User Manage
▷ Enroll User
Enroll Admin
Delete

Figure 2-14 User Manage Menu

3. Press **OK** to display the Enroll User menu and select Enroll FP (see **Figure 2-15**). The possible enrollment choices using the ▼ or ▲ buttons are; FP = fingerprint, Pwd = password only, and FP & Pwd = fingerprint & password).

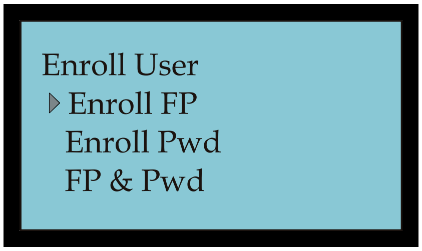


Figure 2-15 Enroll User Menu

4. Press **OK** and Enroll FP New Enroll? will appear (see **Figure 2-16**).

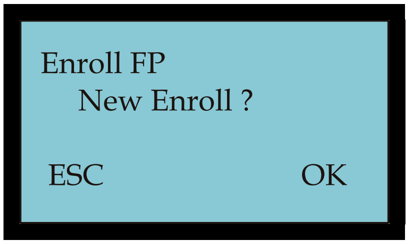
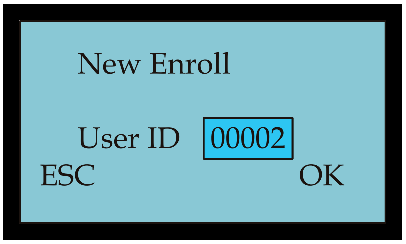


Figure 2-16 New Enroll FP Screen

Note: If this is the first User ID the display will show "*New Enroll User ID 00001*". Pressing **ESC** at this step will place the terminal into the Backup Enroll mode (see How to Enroll Multiple Fingers for a User on page 2-23).

5. Press **OK** to begin enrollment, and New Enroll User ID will appear to accept/enter the User ID (see figure). Enter the User ID using the keypad and/or the ▼ or ▲ buttons. Press **ESC** to exit and return to the Enroll User menu.

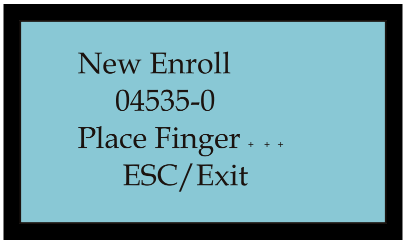

New Enroll

User ID 00002

Figure 2-17 New Enroll User ID Screen

Note: The default User ID is 5 digits, so any number less than 5 digits will have zeros in front of it, i.e., if the number is 2, 00002 will be displayed. The User ID will auto-sequence each new User ID + 1 digit. [the range is 00001 to 65534].

6. Press **OK** to proceed and display "*New Enroll Place Finger…*" (see figure). Follow the on screen prompts for a total of 3 finger presses to complete the process, or press **ESC** to exit to the Enroll User menu.



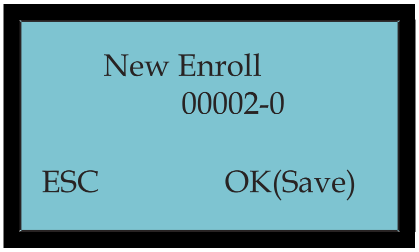
New Enroll
04535-0
Place Finger . . .
ESC/Exit

Figure 2-18 Place Finger 1st Pass

Note: The system may prompt you with voice and on screen warnings if errors in the FP enrollment process occur. For example, if that ID already has the same finger enrolled, the voice prompt will say "*Duplicate Finger*" while the screen will display "*FP Enrolled Alrd*" [for fingerprint enrolled already].

Note: The system will not allow duplicate enrollment of the same finger for the same or different User IDs. You must enroll a different finger.

7. After the 3rd successful finger press, the display will show the User ID followed by " **– 0**" (see figure) to indicate that one (1) finger template exists for this ID.

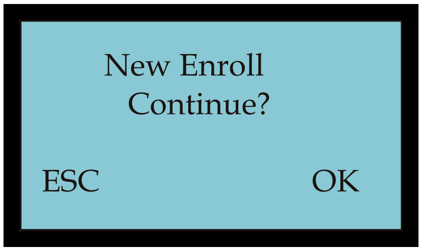


New Enroll
00002-0
ESC OK(Save)

Figure 2-19 Save User ID with FP Template

8. Press **OK** to save the finger template, and the system will prompt to continue for another user enrollment (see figure).

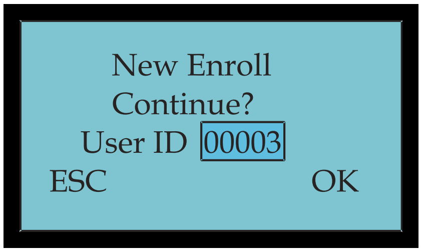
Note: At this time if you press **ESC** you will exit New FP enrollment and enter the Backup Enroll mode. This mode can be used to create more than one (1) finger template for a User ID. A backup finger is recommended as an alternate identification resource.



New Enroll
Continue?
ESC OK

Figure 2-20 Continue FP Enrollemnt

9. Press **OK** to continue. Enter the next User ID using the keypad and/or the ▼ or ▲ buttons and press **OK** to accept the User ID. [go back to Step 6 to continue with FP enrollment]. Press **ESC** to end FP Enrollment and return to the Enroll User menu.



New Enroll
Continue?
User ID 00003
ESC OK

Figure 2-21 Continue FP Enrollment with User ID

Note: If no keypad entries are made within a minute at any time during the enrollment process, the terminal will beep two (2) times and return back to the Welcome screen (see **Figure 2-2**).

How to Enroll a User with a Password

To enroll at the FPT-40 terminal with a password perform:

1. Press the **Menu** button to display the main menu (see figure), or display "*Admin Affirm 1*" and login with privileges.

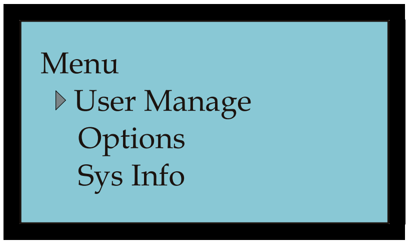


Figure 2-22 Menu Screen

2. Press **OK** to display the User Manage menu (see figure).

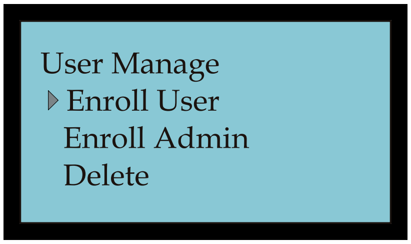


Figure 2-23 User Manage Menu

3. Press **OK** to display the Enroll User menu and select Enroll Pwd (see **Figure 2-24**).

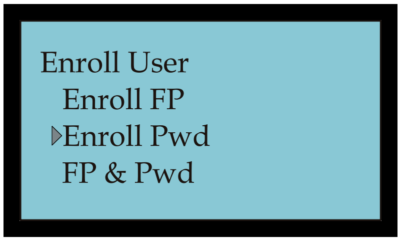


Figure 2-24 Enroll User Menu

4. Press **OK** and Enroll Pwd New Enroll? will appear (see **Figure 2-25**).

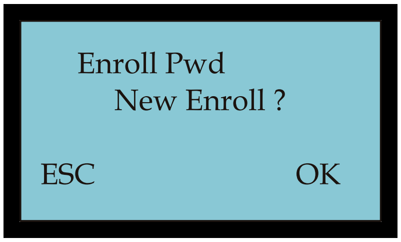
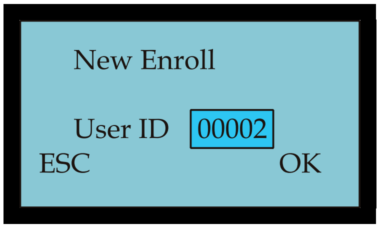


Figure 2-25 New Enroll Pwd Screen

5. Press **OK** to begin Enrollment, and the New Enroll User ID will appear to accept/enter the User ID (see figure). Use the keypad and/or the ▼ or ▲ buttons to enter the User ID. Press **ESC** to exit and return to Enroll User menu.

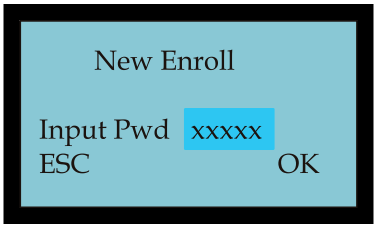


New Enroll

User ID 00002
ESC OK

Figure 2-26 New Enroll Enter User ID Screen

6. Press **OK** to proceed with New Enroll for password, and input the password [the range is 1 to 65534] using the keypad (see figure). Press **OK** to enter the password if less than 5 digits. Press **ESC** to exit and return to the Enroll User menu.

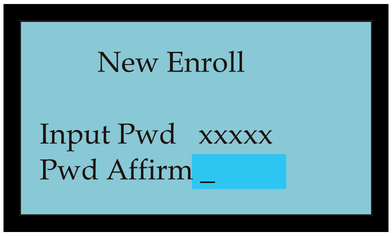


New Enroll

Input Pwd xxxxx
ESC OK

Figure 2-27 New Enroll Input Pasword

7. Repeat the password entry to affirm (see figure).

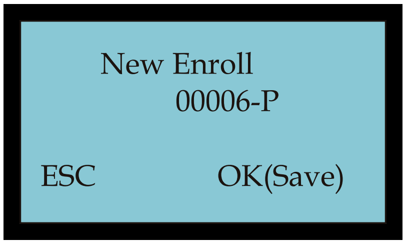


New Enroll

Input Pwd xxxxx
Pwd Affirm _

Figure 2-28 Affirm Password

8. Press **OK** to save password for the User ID. After password entry, the User ID will have a “**dash P**” to indicate that a password has been created (see figure).

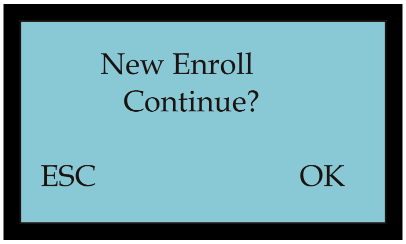


```
      New Enroll
           00006-P

ESC            OK(Save)
```

Figure 2-29 Save Password for User ID

9. Press **OK** to continue entering a password for the next User ID (see figure), or press **ESC** to change the password. See How to Change a User Password with Backup Enroll on page 2-17 for more details on changing a password.

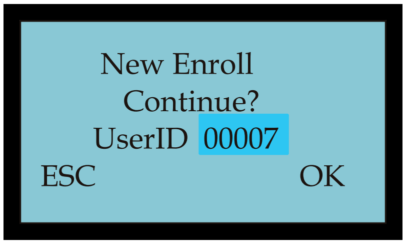


```
      New Enroll
        Continue?

ESC                  OK
```

Figure 2-30 New Enroll Continue?

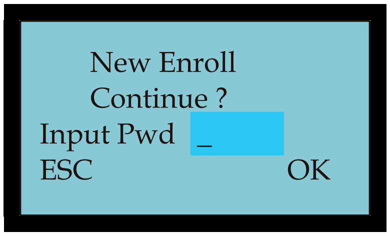
10. Use the keypad and/or the ▼ or ▲ buttons to select the next User ID for password entry, and press **OK** to continue (see figure). Press **ESC** to abort and return to the Enroll User menu.



```
      New Enroll
        Continue?
      UserID 00007
ESC                  OK
```

Figure 2-31 Continue with Next User ID

11. Input the password using the keypad [press **OK** if less than 5 digits], and repeat the password entry to affirm. Press **ESC** to abort password entry and return to the Enroll User menu.



New Enroll
Continue ?
Input Pwd _
ESC OK

Figure 2-32 Input Password with Next User ID

12. Go back to Step 8 to continue the process for the next user. Press **ESC** to end enrollment and return to the Enroll User menu.

How to Change a User Password with Backup Enroll

The following procedure details how to change an existing user password. The FP & Pwd Enroll procedure could also be used to change the password, but you will have to enroll another finger to get password access. Therefore, the following is recommended as the easiest method for changing a password.

To change a user's password at the FPT-40 terminal perform:

1. Press the **Menu** button to display the main menu (see figure), or display "*Admin Affirm 1*" and login with privileges.

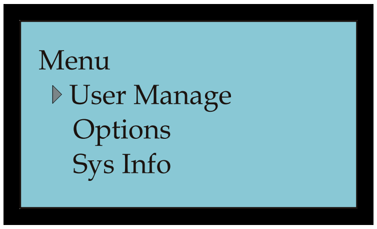


Figure 2-33 Menu Screen

2. Press **OK** to display the User Manage menu (see figure).

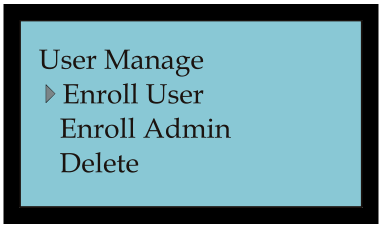


Figure 2-34 User Manage Menu

3. Press **OK** to display the Enroll User menu and select Enroll Pwd (see **Figure 2-35**).

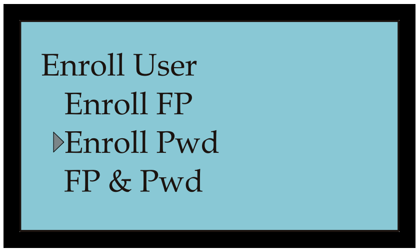
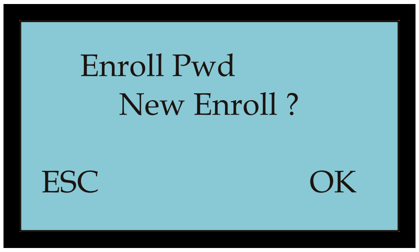


Figure 2-35 Enroll User Menu

4. Press **OK** and Enroll Pwd New Enroll? will appear (see **Figure 2-36**).

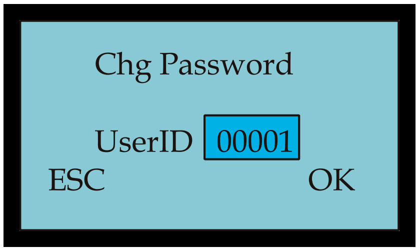

Enroll Pwd

New Enroll ?

Figure 2-36 Enroll Pwd New Enroll Screen

5. Press **ESC** to change the password, and Chg Password User ID will appear to accept/enter the User ID (see figure). Use the keypad and/or the ▼ or ▲ buttons to select the desired User ID. Press **ESC** to exit and return to the Enroll User menu.

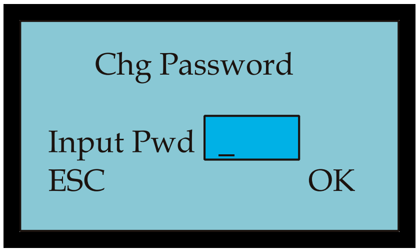
Note: If an unknown User ID is entered, the warning "*No Enroll!*" will appear.


Chg Password

UserID 00001

Figure 2-37 Change Password Select User ID

6. Press **OK** to input the replacement password [the range is 1 to 65534] using the keypad. Press **ESC** to abort changing the password and return to the Enroll User menu.



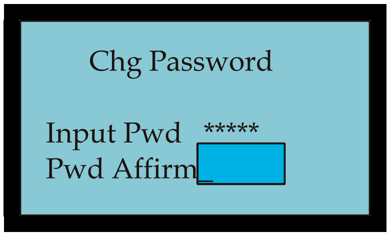
Chg Password

Input Pwd _

ESC OK

Figure 2-38 Change Password - Input Pwd

7. Repeat the password entry to affirm (see figure).



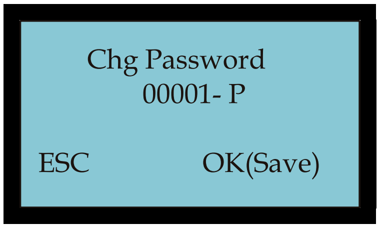
Chg Password

Input Pwd *****

Pwd Affirm _

Figure 2-39 Change Password - Affirm

8. Press **OK** to save the changed password. The User ID will have a "***-P***" after it to indicate a password has been created (see figure).



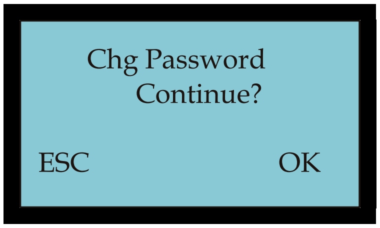
Chg Password

00001- P

ESC OK(Save)

Figure 2-40 Change Password - Save

9. Press **OK** to continue changing passwords for other Users (see figure), or press **ESC** to exit changing passwords and go to "New Enroll" (see How to Enroll a User with a Password on page 2-14.



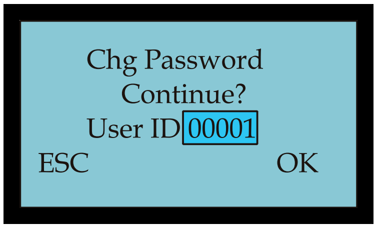
Chg Password

Continue?

ESC OK

Figure 2-41 Continue with Next User ID

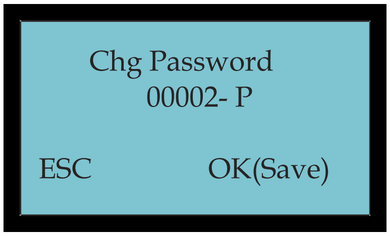
10. Use the keypad and/or the ▼ or ▲ buttons to select the next User ID for password change (see figure), and press **OK** to input the new password. Press **ESC** to return to the Enroll User menu.



Chg Password
Continue?
User ID 00001
ESC OK

Figure 2-42 New Enroll Input Pwd

11. Input the new password and affirm. See Step 8 to continue the process, or press **ESC** to exit and return to the Enroll User menu.



Chg Password
00002- P
ESC OK(Save)

Figure 2-43 Save Change Password

How to Enroll a User with Fingerprint and Password

The following procedure details how to enroll a new user using both a fingerprint and a password. When this procedure is used, the user only has to validate with either a fingerprint or a password. The user does not have to use both the fingerprint and password to validate an in/out punch for time recording.

To enroll at the FPT-40 terminal with a FP & Pwd perform:

1. Press the **Menu** button to display the main menu (see figure), or display "*Admin Affirm 1*" and login with privileges.

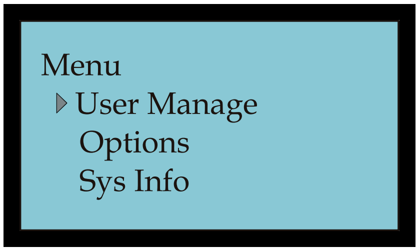


Figure 2-44 Menu Screen

2. Press **OK** to display the User Manage menu (see figure)

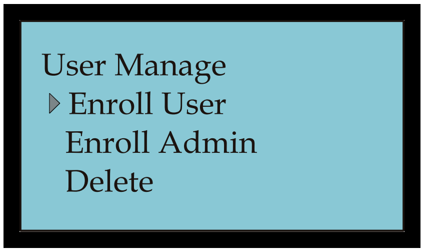


Figure 2-45 User Manage Menu

3. Press **OK** to display the Enroll User menu and select FP & Pwd (see **Figure 2-46**).

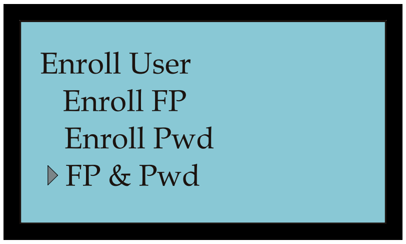


Figure 2-46 Enroll User Menu

4. Press **OK** and FP & Pwd New Enroll? will appear (see **Figure 2-47**).

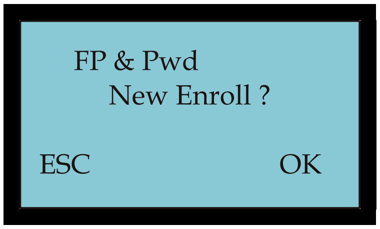


Figure 2-47 New Enroll FP & Pwd Screen

5. Press **OK** to enter a User ID (see figure). Enter the User ID using the keypad and/or the ▼ or ▲ buttons. Press **ESC** to exit to Backup Enroll (see How to Change a User Password on page 2-17).

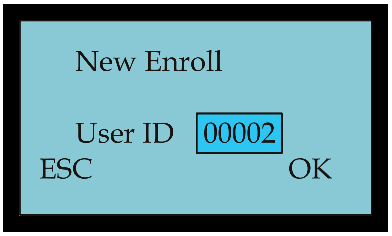
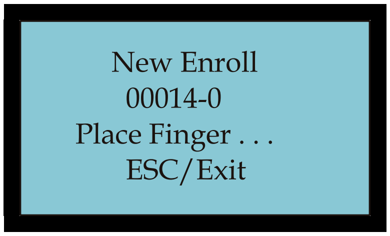


Figure 2-48 New Enroll User ID Screen

6. Press **OK** to continue with New Enrollment for finger template and display the New Enroll Place Finger… (see figure). Follow the on screen prompts for a total of 3 finger presses to complete the process. Wait for the screen to prompt you each time to place your finger!

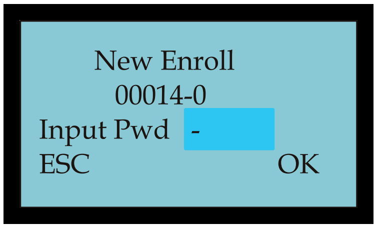
Note: Pressing **ESC** at this step will bypass finger enrollment and move to New Enroll for password input.



```
New Enroll
00014-0
Place Finger . . .
ESC/Exit
```

Figure 2-49 Create Fingerprint Template

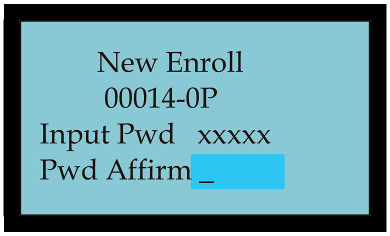
7. Next, input the password (see figure) using the keypad. If less than 5 digits, press **OK** to enter. Press **ESC** to exit password entry and save just the fingerprint.



```
New Enroll
00014-0
Input Pwd  -
ESC                OK
```

Figure 2-50 New Enroll Input Pasword

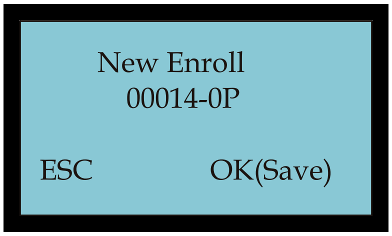
8. Repeat the password entry to affirm, and display the User ID with a "***-0P***" (see **Figure 2-52**) to indicate that this User has 1 finger template ("*0*") and a password ("*P*")



```
New Enroll
00014-0P
Input Pwd   xxxxx
Pwd Affirm _
```

Figure 2-51 Affirm New Password

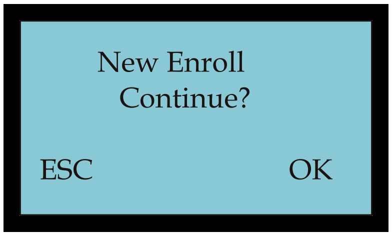
9. Press **OK** to save the finger template & password (see figure) and display New Enroll Continue?



New Enroll
00014-0P
ESC OK(Save)

Figure 2-52 Save Password for User ID

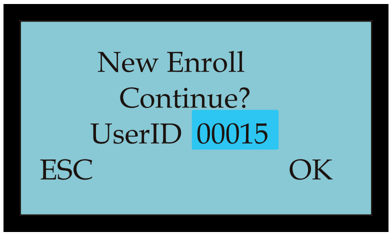
10. Press **OK** to Continue (see figure) with FP & Pwd enrollment, or press **ESC** to move to Backup Enroll Continue? to change finger template and password for a User ID.



New Enroll
Continue?
ESC OK

Figure 2-53 New Enroll Continue?

11. Press **OK** to enter the next User ID (see figure) for a finger template and password. See Step 6 to continue the process to enroll the next user. Press **ESC** to display Input Pwd screen to enter a password.



New Enroll
Continue?
UserID 00015
ESC OK

Figure 2-54 Continue with Next User ID

How to Enroll Multiple Fingers for a User

The following procedure details how to enroll multiple fingerprint templates for a single user. When this procedure is used, the user now has an alternate finger to use as a backup. Two separate fingers per user are recommended to be enrolled for backup, but enrolling more than two fingers per user will reduce the amount of users that can be stored in the reader.

There are two different scenarios for enrolling multiple fingers for the same user. The first scenario is to add an additional finger template for an exisiting enrolled user. The second scenario is to enroll more than 1 finger for a user during initial FP enrollment at the terminal.

To enroll a backup finger for a User ID <u>already enrolled</u> perform the following:

1. Press the **Menu** button to display the main menu (see figure), or display "*Admin Affirm 1*" and login with privileges.

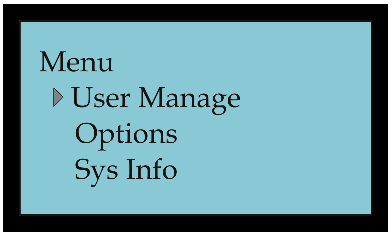


Figure 2-55 Menu Screen

2. Press **OK** to display the User Manage menu (see figure).

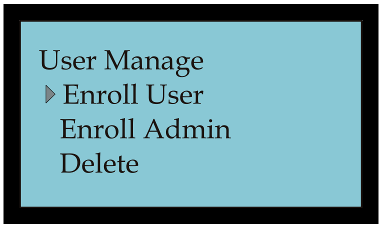


Figure 2-56 User Manage Menu

3. Press **OK** to display the Enroll User menu and select Enroll FP (see **Figure 2-57**).

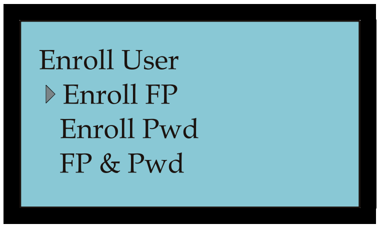
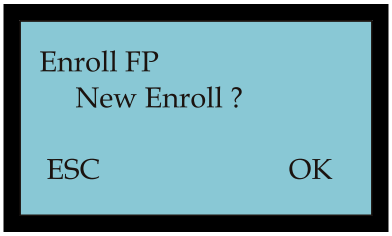


Figure 2-57 Enroll User Menu

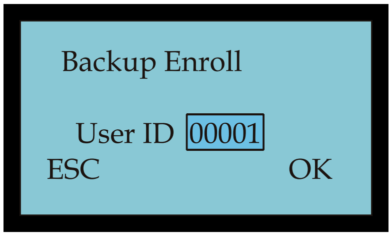
4. Press **OK** and Enroll FP New Enroll? will appear (see **Figure 2-58**).



Enroll FP
New Enroll ?
ESC OK

Figure 2-58 Enroll FP Screen

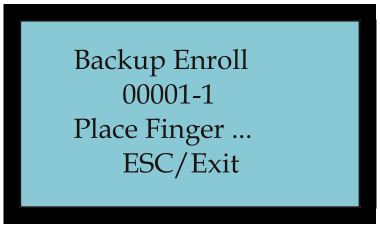
5. Press **ESC** to exit New Enroll and initiate Backup Enroll. The lowest numeric User ID will be shown first, and the User IDs will be listed in ascending numeric order. Use the keypad and/or the ▼ or ▲ buttons to enter/select the User ID you want to add a finger template to.



Backup Enroll
User ID 00001
ESC OK

Figure 2-59 Backup Enroll User ID Screen

6. With the desired User ID selected, press **OK** to add another finger template (see figure), and the User ID will indicate that an additional template is being added by the dash number after the User ID [i.e., 00010 – 1 means user ID # 10 has 2 templates] (see figure).



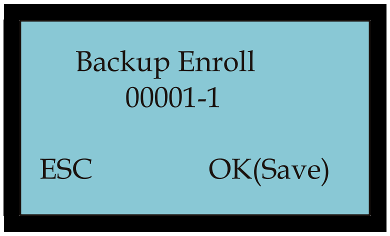
Backup Enroll
00001-1
Place Finger ...
ESC/Exit

Figure 2-60 Backup Finger Enrollemnt - Place Finger 1st Pass

Note: The system may prompt you with voice and on screen warnings if errors in the enrollment process occur. For example, if that ID already has the same finger enrolled, the voice prompt will say "*Duplicate Finger*" while the screen will display "FP Enrolled Alrd".

Note: The system will not allow duplicate enrollment of the same finger. You must enroll a different finger.

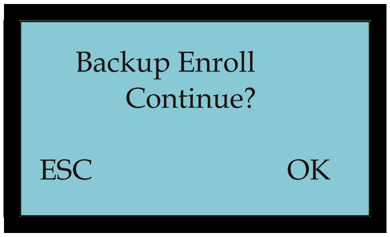
7. Follow the on screen prompts for a total of 3 finger presses to add the finger template, or press **ESC** to return to the Enroll User menu. Press **OK** to save the 2nd finger template which is indicated by the 5-digit User ID followed by a "***dash 1***" (see figure).



Backup Enroll
00001-1
ESC OK(Save)

Figure 2-61 Backup Enroll User ID

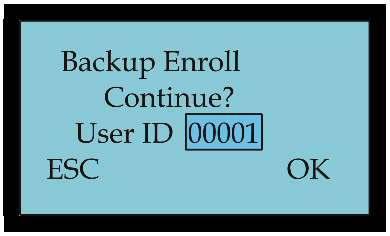
8. Press **OK**, to continue with Backup Enrollment (see figure), or press **ESC** to discontinue the Backup Enrollment process and return to the Enroll User menu.



Backup Enroll
Continue?
ESC OK

Figure 2-62 Backup Enroll Continue

9. The current numeric User ID will be shown first, and the User IDs will be listed in ascending numeric order. Use the keypad and/or the ▼ or ▲ buttons to enter/select the User ID you want to add a finger template to, and press **OK**. See Step 6 to continue with the backup enrollment process. Press **ESC** to abort the process and return back to the Enroll User menu.



Backup Enroll
Continue?
User ID 00001
ESC OK

Figure 2-63 Backup Enroll Continue with User ID

To enroll multiple fingers for a User during <u>initial enrollment</u> perform the following:

1. Press the **Menu** button to display the main menu (see figure), or display "*Admin Affirm 1*" and login with privileges.

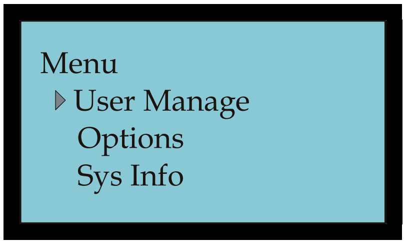


Figure 2-64 Menu Screen

2. Press **OK** to display the User Manage menu (see figure)

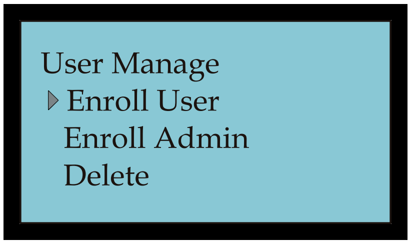


Figure 2-65 User Manage Menu

3. Press **OK** to display the Enroll User menu and select Enroll FP (see **Figure 2-66**).

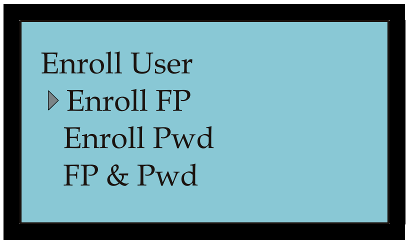


Figure 2-66 Enroll User Menu

4. Press **OK** and Enroll FP New Enroll? will appear (see **Figure 2-67**).

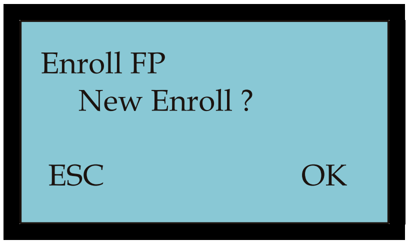
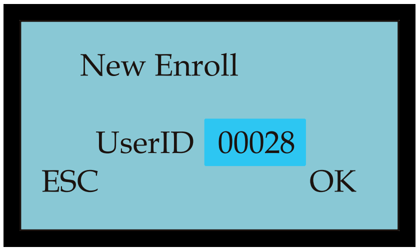


Figure 2-67 New Enroll FP Screen

5. Press **OK** to begin new enrollment, and New Enroll User ID will appear to enter the User ID (see figure) using the keypad and/or the ▼ or ▲ buttons. Press **ESC** to exit and return to the Enroll User menu.



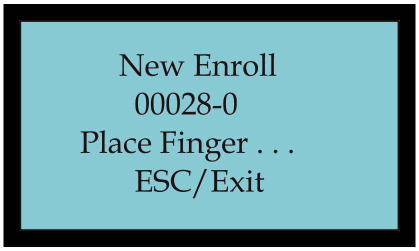
New Enroll

UserID 00028

ESC OK

Figure 2-68 New Enroll User ID Screen

6. Press **OK** to proceed with the selected User ID and display New Enroll Place Finger… (see figure). Follow the on screen prompts for a total of 3 finger presses to complete the process, or press **ESC** to exit and return to the Enroll User menu.



New Enroll

00028-0

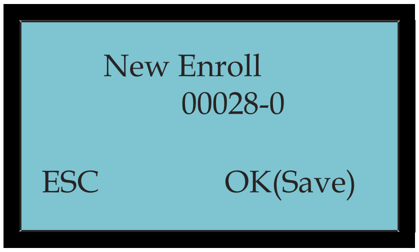
Place Finger . . .

ESC/Exit

Figure 2-69 New Enroll - Place Finger 1st Pass

Note: The FPT-40 Fingerprint terminal will not allow duplicate finger enrollment for the same or even different User IDs. You must enroll a different finger.

7. After the 3rd successful finger press, the display will show the 5-digit User ID followed by "**– 0**" (see figure) to indicate that the first (0) finger template has been created for this ID.



New Enroll

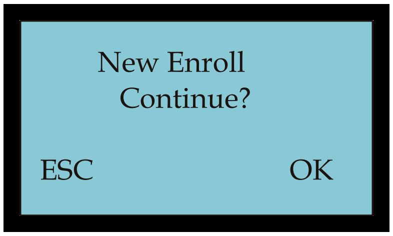
00028-0

ESC OK(Save)

Figure 2-70 Save User ID with FP Template

8. Press **OK** to save the finger template, and the system will prompt to continue with another new enrollment (see figure) for the next User ID.

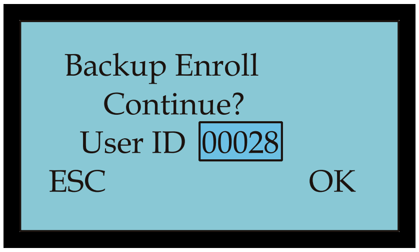
Note: At this time if you press **ESC** you will exit New FP enrollment and enter the Backup Enroll mode. This mode can be used to create an additional finger template for the User ID. A backup finger is recommended as an alternate identification resource.



New Enroll
Continue?
ESC OK

Figure 2-71 Continue FP Enrollemnt

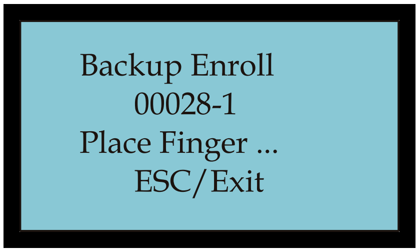
9. Press **ESC** to initiate Backup Enroll to add a second finger template for this User ID.



Backup Enroll
Continue?
User ID 00028
ESC OK

Figure 2-72 Backup Enroll User ID Screen

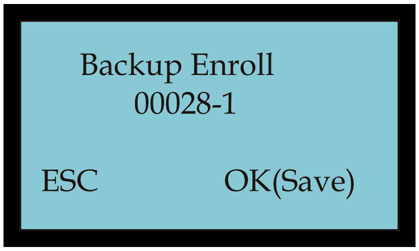
10. With the same User ID selected, press **OK** to add the 2nd finger (see figure), and follow the on screen prompts for a total of 3 finger presses to add the 2nd finger, or press **ESC** to exit and return to the Enroll User menu.



Backup Enroll
00028-1
Place Finger ...
ESC/Exit

Figure 2-73 Backup Finger Enrollemnt - Place Finger

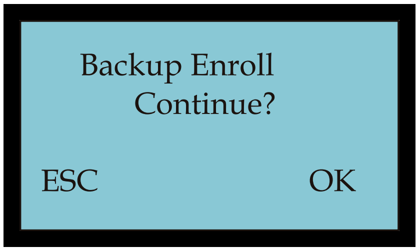
11. After the 3rd successful finger press, the display will show the 5-digit User ID followed by a “**–1**” (see figure) to indicate that a 2nd finger template has been created for this ID.



Backup Enroll
00028-1
ESC OK(Save)

Figure 2-74 Confirm User ID & FP Template

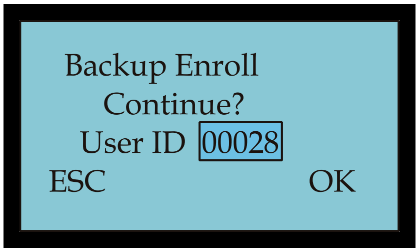
12. Press **OK** to save the 2nd finger template for the User ID, and the system will prompt to continue backup enrollment (see figure). Press **ESC** to discontinue the Backup Enrollment process and return to the Enroll User menu to select another form of enrollment.



Backup Enroll
Continue?
ESC OK

Figure 2-75 Backup Enroll Continue

13. Press **OK**, and the Backup Enroll Continue? User ID will appear (see figure) with the current User ID or enter a different User ID to continue the backup enrollment process. Press **ESC** to abort the process and return back to the Enroll User menu when finished enrolling finger templates for this User ID.



Backup Enroll
Continue?
User ID 00028
ESC OK

Figure 2-76 Backup Enroll Continue User ID

Defining Privileges with Enrolling Admin Option

After power on and setting up the FPT-40 Fingerprint terminal, you may begin enrolling users. If this is the first enrollment in a new or empty system, everyone will be able to enroll. However, if there are any user privileges setup in the terminal, you will need, at a minimum, "Enroller" level privileges to enroll a new user. The FPT-40 Fingerprint terminal contains a privileges option to prevent unauthorized personel from changing terminal parameters. This security option provides three (3) different levels of authorized use, which are: an enroller, a supervisor, and an administrator with the following privileges:

Enroller Privilege Level

- The Enroller can only access the User Manage and Sys Info menus.
- The Enroller can not delete any user's at the terminal.
- The Enroller has full access to the enrollment functions for a new user, and also changing an existing user via Backup Enroll.
- The Enroller has access to the "Enroll Admin" function, but can only create a user with "Enroller" level privileges.

Supervisor Privilege Level

- A Supervisor can access all 3 main menus; the User Manage, Options, and Sys Info menus. However, a Supervisor can not access the Auto Test menu [from Options menu], the Comm Key [from Comm Opt menu, and most importantly, the Adv Opt menu [from System Options].
- A Supervisor can only delete a user with no privileges or Enroller privileges at the terminal.
- A Supervisor has full access to the enrollment functions for a new user, and also changing an existing user via Backup Enroll.
- A Supevisor has access to the "Enroll Admin" function, but can only create a user with "Supervisor" and "Enroller" level privileges.

Admin Privilege Level

- The Administrator has full access to all menus, user deletion [**can not delete an Admin**], enrollment, and deleting privileges and/or data from the Adv Opt menu.

Note: The only way to delete a user with Admin privileges at the terminal is to use the "*Clear Admin Pri*" [clear administrator priorities] command from the Adv Option menu.

Note: When creating privileges at the terminal it is strongly recommended to create at least one user with "Admin" privileges first so that you would always have full access at the terminal if required. User privileges can also be set from Time Guardian.

To enroll a User at the FPT-40 terminal with privileges perform the following:

1. Press the **Menu** button to display the main menu (see figure). If users with privileges have already been setup the Welcome screen will display "*Admin Affirm 1*" on the top. If this is the case, you must login with privileges first to get access to the main menu.

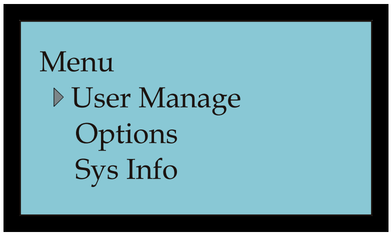


Figure 2-77 Main Menu

2. Press **OK** to display the User Manage menu and select Enroll Admin (see figure).

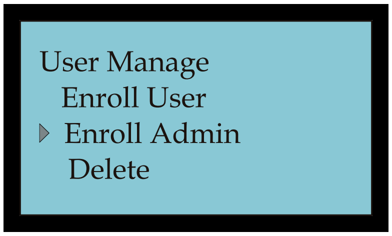


Figure 2-78 User Manage Menu

3. Press **OK** to display the Enroll Admin menu (see **Figure 2-79**).

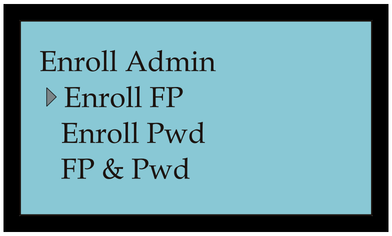
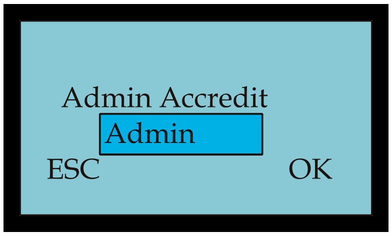


Figure 2-79 Enroll Admin Menu

4. Select Enroll FP, Enroll Pwd, or FP & Pwd using the ▼ button, and press **OK**. The screen to select the privilege level [Admin, Supervisor, or Enroller] will appear (see **Figure 2-80**).


Admin Accredit

Admin

ESC OK

Figure 2-80 Admin Accredit Selection Screen

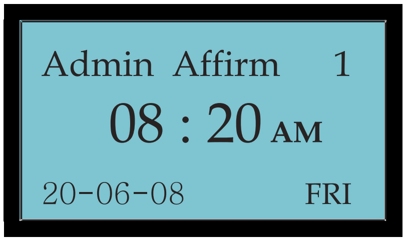
5. After selecting the authorization level, press **OK**, and the enrollment process will be the same as the regular FP, Pwd, or FP & Pwd enrollment. If you continue to enroll users with privileges without exiting to the Enroll Admin menu, the privilege level will remain the same. When finished enrolling a user with privileges, or desiring to switch privilege levels, press **ESC** to return back to Enroll Admin menu.

Deleting Users

Note: If you try to delete a User at the terminal without having the required privilege, a message "Access Deny!" will briefly appear, and the display will return to the previous screen.

To delete a user at the FPT-40 terminal perform the following:

1. Press the **Menu** button to display the main menu, or display "*Admin Affirm 1*" on the top of the Welcome screen (see figure) and login as a user with privileges.


Admin Affirm 1

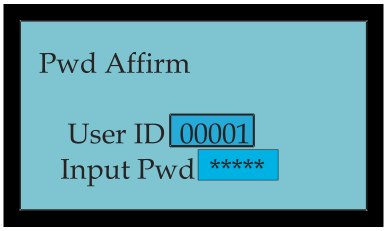
08 : 20 AM

20-06-08 FRI

Figure 2-81 Menu Screen

2. To login from the Welcome screen either place your finger on the sensor <u>or</u> enter your assigned User ID using the keypad.

3. Follow the on screen prompt to remove finger Or input your password (see figure).



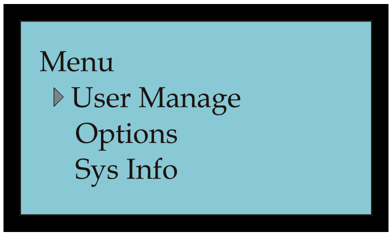
Pwd Affirm

User ID 00001

Input Pwd *****

Figure 2-82 Input Password

4. Once accepted, the main Menu will display (see figure).



Menu

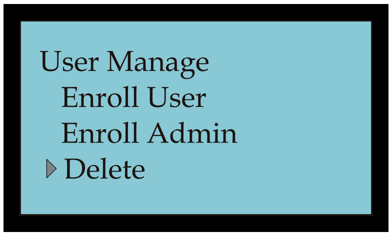
▷ User Manage

Options

Sys Info

Figure 2-83 Main Menu

5. Press **OK** to display the User Manage menu and select Delete (see figure).



User Manage

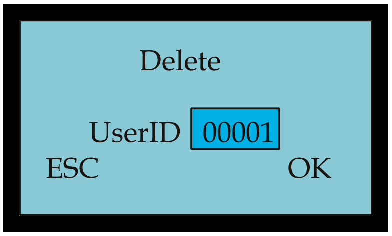
Enroll User

Enroll Admin

▷ Delete

Figure 2-84 User Manage Menu

6. Press **OK** to select the User ID (see **Figure 2-85**). Use the keypad and/or the ▼ or ▲ buttons to navigate to the desired User ID. Press **ESC** to return to the User Manage menu.



Delete

UserID 00001

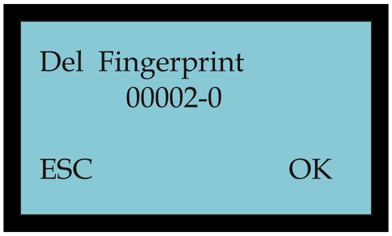
ESC OK

Figure 2-85 Delete Enrolled User ID

Note: The screen will display "*No Enroll!*" if an invalid user ID is entered.

7. Press **OK** to confirm the User ID, or press **ESC** to return to the User Manage menu.

8. Press **OK** to begin the deletion process. The sequence of any deletion is: 1st the fingerprint (see figure), 2nd the password, and last the User ID (see figure). The items deleted will depend upon what the user has created. First press **OK** to delete the fingerprint. or press **ESC** to exit the deletion process, and return to the User Manage menu.

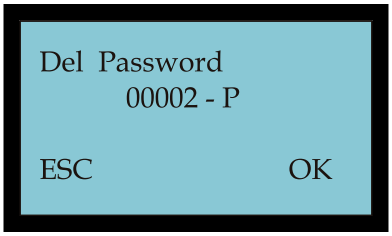


Del Fingerprint
00002-0
ESC OK

Figure 2-86 Delete Fingerprint

Note: If the user has multiple finger templates the sequence of deletion will be the last finger template to first, next the password, etc.

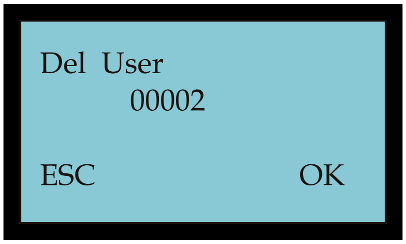
9. Next press **OK** to delete the password, or press **ESC** to exit the password deletion process, and return to the User Manage menu.



Del Password
00002 - P
ESC OK

Figure 2-87 Delete Password

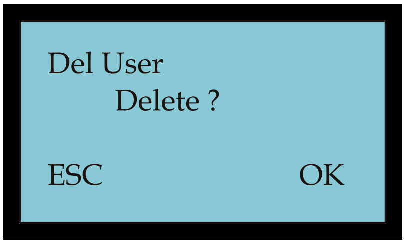
10. Finally press **OK** to delete the user, or press **ESC** to exit the user deletion process, and return to the User Manage menu.



Del User
00002
ESC OK

Figure 2-88 Delete User ID

11. Press **OK** to confirm the user deletion (see figure), and return to the User Manage menu. Press **ESC** to exit without confirming deletion and return to the User Manage menu.



Del User

Delete ?

ESC OK

Figure 2-89 Confirm User ID for Deletion

How to Restore Deleted Users From Time Guardian

You can still retrieve the Users you just deleted at the terminal [location] from Time Guardian. Also, it is recommended to utilize the TG system backup feature to protect the database which contains the maps, etc.

The sequence to restore users from Time Guardian is:

1. First press the Download button from the TG Fingerprint Commands screen (see Using the Fingerprint Commands Tab) to load employee ID's, etc. into the terminal.
2. Next press Send Maps TG Fingerprint Commands screen to transfer all template maps to the terminal.

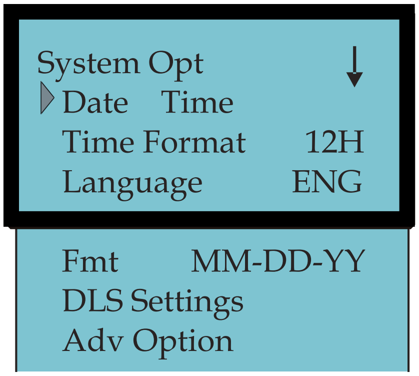
Options Menu

Use the Options Menu to configure such functions as, system options, power management, communications options, log options, and perform diagnostics (see Diagnostics on page 3-1).

System Option Menu

From the **Options** menu select the **System Opt** menu (see figure) to set the date & time, time format, language, date format, DLS settings, and advanced options. See the following sections for additional information.

If user privileges have been setup, only a user with Admin privilege will be able to access the **Adv Option** menu.



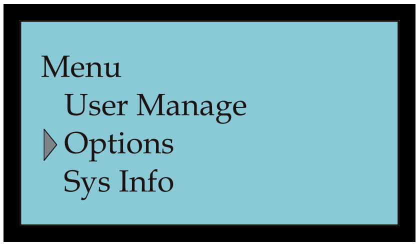
```
System Opt              ↓
▷Date   Time
 Time Format        12H
 Language           ENG
 Fmt          MM-DD-YY
 DLS Settings
 Adv Option
```

Figure 2-90 System Options Menu

Setting the Terminal Date & Time

Use this function to set the date and time for the FPT-40 terminal with the following procedure:

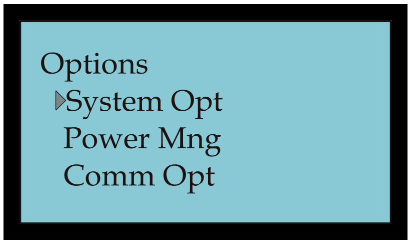
1. Press the **Menu** button and select Options (see figure).



```
Menu
 User Manage
▷Options
 Sys Info
```

Figure 2-91 Main Menu

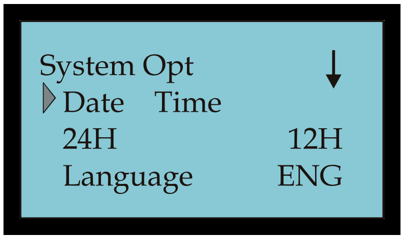
2. Press **OK** to display the Options menu and select System Opt (see **Figure 2-92**).



```
Options
 ▷System Opt
  Power Mng
  Comm Opt
```

Figure 2-92 Options Menu

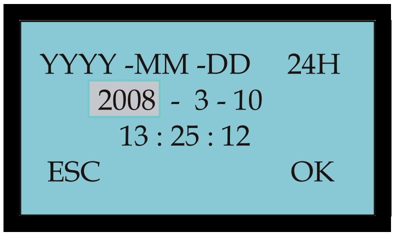
3. Press **OK** to display the System Opt menu and select Date Time (see **Figure 2-93**).



System Opt ↓
▷Date Time
24H 12H
Language ENG

Figure 2-93 Date/Time

4. Press **OK** to display the Date & Time (see **Figure 2-94** for an example). Press the down ▼ or ▲ up arrow buttons to move forward or backward, one field per press. Use the numeric keypad to enter the changes to the date and time values. Only allowable values for each field will be accepted, i.e., 14 for month is not a valid value.



YYYY -MM -DD 24H
2008 - 3 - 10
13 : 25 : 12
ESC OK

Figure 2-94 Date & Time Example

Note: The date entry format is fixed as YYYY-MM-DD with a 24H time format.

5. Press **OK** to save the settings, and return to the System Opt menu.

6. Keep pressing **ESC** to return to the Welcome screen, or just let the terminal automatically default to the Welcome screen. From the System Opt menu select Adv Option if changes to advanced options are required.

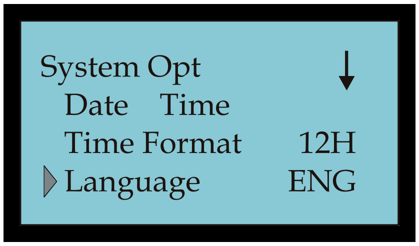
Setting the Display Time Format

From the System Opt menu select Time Format, and then choose **24H** for military time, or **12H** for AM/PM time format. The default time format is 12H. The display time format can be set at the terminal or downloaded from Time Guardian. Time Guardian should be set in the same time format as the terminal.

Note: This format does not change the time format of the FPT-40 terminal, as it only changes the terminal display format.

Setting the Language

1. From the System Opt menu select Language (see **Figure 2-95**).



System Opt ↓
Date Time
Time Format 12H
▷ Language ENG

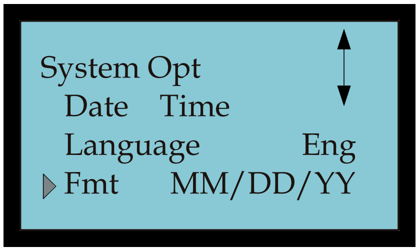
Figure 2-95 System Options Language

2. Press **OK** to highlight the current Language. Use the ▼ or ▲ buttons to move between choices, which are; English or Spanish.
3. Press **OK** to save the selection, or press **ESC** to keep the default selection; which is English. You must restart the terminal for the selected language to take effect.

Setting the Display Date Format

The default display date format is MM/DD/YY.

1. From the System Opt menu select Fmt [format] (see **Figure 2-95**).



System Opt ↕
Date Time
Language Eng
▷ Fmt MM/DD/YY

Figure 2-96 Date Format

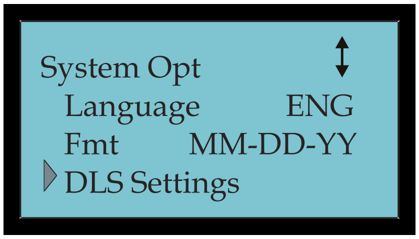
2. Press **OK** to highlight the display format setting. Use the ▼ or ▲ buttons to select one of the formats, which are; YY-MM-DD, YY/MM/DD, YY.MM.DD, MM-DD-YY, MM/DD/YY, MM.DD.YY, DD-MM-YY, DD/MM/YY, DD.MM.YY, or YYYYMMDD.
3. Press **OK** to save the selection, or press **ESC** to keep the default.

Note: This format does not change the date format of the FPT-40 terminal, as it only changes the terminal display format.

How to Set Daylight Saving (DLS) Time

Use this function to set the Daylight Saving (DLS) Time start/end dates and times at the FPT-40 terminal with the following procedure:

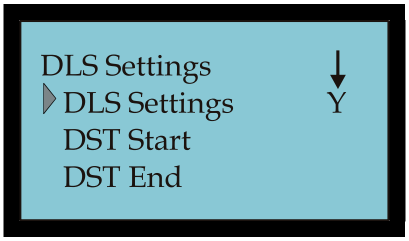
1. From the System Opt menu select DLS Settings (see figure).



System Opt ↕
Language ENG
Fmt MM-DD-YY
▷ DLS Settings

Figure 2-97 Selecting DLS

2. Press **OK** to display the DLS Settings menu (see **Figure 2-98**) and select DLS Settings.

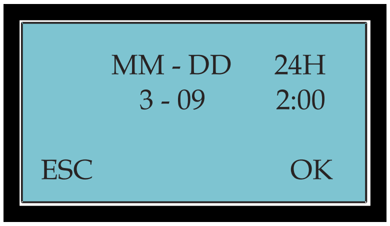


DLS Settings ↓
▷ DLS Settings Y
DST Start
DST End

Figure 2-98 DLS Settings

3. Press **OK** to highlight the setting and select **Y** or **N**. Press **OK** to save the selection.

4. Select DST Start, and press **OK** to enter the begin date/time for DST (see figure for example). Use the ▼ or ▲ buttons to move between choices and the keypad to enter values. Press **OK** to save or **ESC** to exit with default settings.



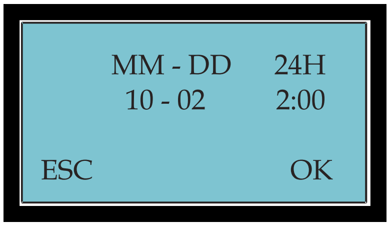
MM - DD 24H
3 - 09 2:00

ESC OK

Figure 2-99 DST Start Date/Time

Note: The DST Start and End time format is fixed as a 24H format.

5. Select DST End, and press **OK** to enter the end date/time for DST (see figure for example). Use the ▼ or ▲ buttons to move between choices and the keypad to enter values. Press **OK** to save or **ESC** to exit with default settings.

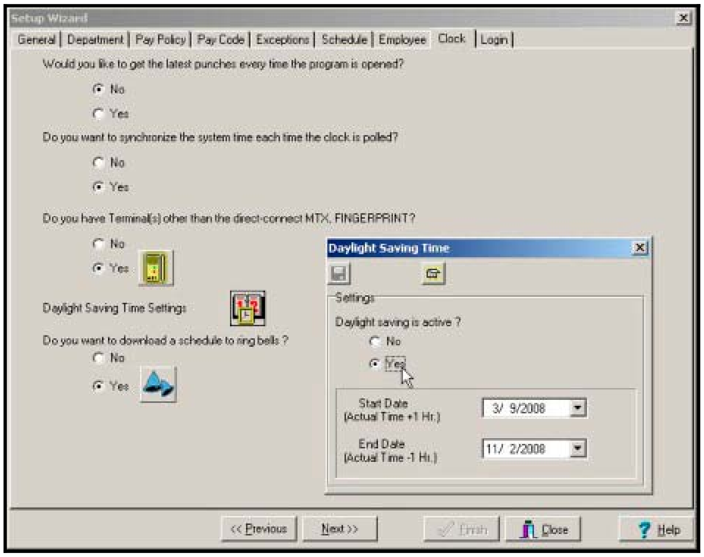


MM - DD 24H
10 - 02 2:00

ESC OK

Figure 2-100 DST End Date/Time

Note: The FPT-40 Fingerprint terminal will utilize these settings to adjust the terminal's future clock time based upon the DLS date settings. However, the Time Guardian DST settings (see figure) will have precedent.



Setup Wizard

General | Department | Pay Policy | Pay Code | Exceptions | Schedule | Employee | Clock | Login |

Would you like to get the latest punches every time the program is opened?
● No
○ Yes

Do you want to synchronize the system time each time the clock is polled?
○ No
● Yes

Do you have Terminal(s) other than the direct-connect MTX, FINGERPRINT?
○ No
● Yes

Daylight Saving Time Settings

Do you want to download a schedule to ring bells ?
○ No
● Yes

Daylight Saving Time

Settings

Daylight saving is active ?
○ No
● Yes

Start Date (Actual Time +1 Hr.) 3/ 9/2008

End Date (Actual Time -1 Hr.) 11/ 2/2008

Figure 2-101 Time Guardian DLS Settings

Advanced Options (Adv Option) Menu

Use the Adv Option menu at the FPT-40 terminal to:

- **Reset Opts.:** selecting this command will restore all setup information in the terminal to the factory default settings.
- **Del AttLogs**: selecting this command will delete all user logs from the flash memory.

- **Clear All Data**: selecting this command will delete all enrolled user information including templates, passwords and logs from the flash memory of the terminal. Time Guardian can be used to restore this information from the "Fingerprint Commands" (see page 4-6).
- **Clear Admin Pri:** selecting this command will clear all administrative privileges currently set in the terminal and reset all user privileges to ordinary users.
- **Show Score**: selecting this command will set whether or not to display a quality value for the fingerprint template on the LCD screen.
- **Match Thr:** selecting this command sets the threshold level for a one-to-many match, see Table 2-1. A one-to-many threshold is used to compare the finger template to the database of user templates to determine the user (ID) that just punched.
- **Mst Input ID:** selecting this command sets whether or not [**Y** or **N**] if you <u>must</u> enter your User ID when punching. When this command is set to Y, all users are compared with a 1:1 match to their ID with their finger template or password.
- **1:1 Thr:** selecting this command sets the one-to-one threshold level when comparing an ID to a fingerprint or password.
- **Voice:** selecting this command is used to set (**Y**), so the terminal will produce an audible prompt sound for every operation. For example, after a successful verification, the machine will say ("*Thank you*"). If the Voice is set to (**N**) the machine will not produce an audible prompt, but instead just beep once to signify a sucessful verification. In this instance, if the verification was negative, the machine will beep twice.
- **Adj VOL(%)**: selecting this command will adjust the voice speaker volume for audible prompts.

To set Advanced Options:

1. From the System Opt menu select Adv Option (see figure).

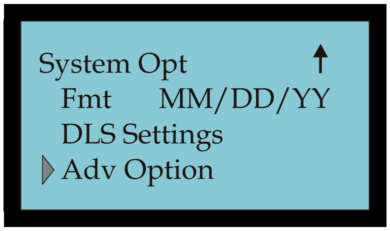
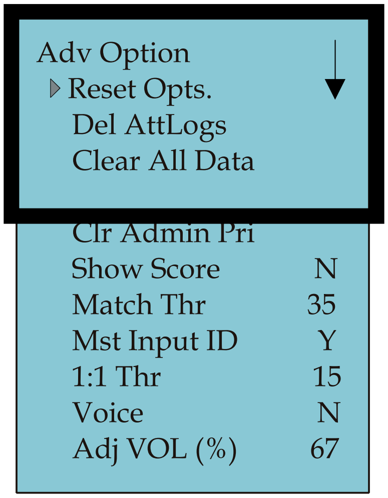


Figure 2-102 Select Adv Option Menu

2. Press **OK** to display the Adv Option menu (see **Figure 2-103**). Press the "▲/▼" buttons to scroll up or down to select the desired option.



```
Adv Option              ↓
 ▷ Reset Opts.
   Del AttLogs
   Clear All Data
   Clr Admin Pri
   Show Score          N
   Match Thr          35
   Mst Input ID        Y
   1:1 Thr            15
   Voice               N
   Adj VOL (%)        67
```

Figure 2-103 Adv Option Menu

2. For Adv Options such as; Match Thr, 1:1 Thr, and Adj VOL(%), use the numeric keypad or "▲/▼" to enter the desired value.

Power Management Menu

Use the Power Mng menu at the FPT-40 terminal to set:

- **Shutdown.:** The default is "**N**". If active, set in military time format the time of day you want the terminal to automatically power off.
- **PowerOn:** The default is "**N**". If active, set in military time format the time of day you want the terminal to automatically power on.
- **Sleep:** The default is "**N**". If active, set in military time format the time of day for the unit to enter sleep mode. Pressing any key once the unit enters the sleep mode will wake the unit up.
- **Idle:** This option and Idle Min are directly related. When the Idle Min = zero, the Idle = closed [**SLP**]. For example, if Idle Min is set to 1 minute, and there is no user activity within that minute, then the unit will enter the idle state (sleep) provided Idle is set to SLP [sleep]. However, if Idle is set to **OFF**, then the terminal will power off when the idle min is reached.
- **Idle Min:** The default is "**0**". See previous.
- **Lock Power:** The default is "**N**". If this option is set to "**Y**", when the power On/Off button is pressed nothing will happen as this button will be locked out.

To set Power Mng Options:

1. Press the **Menu** button and select Options (see figure).

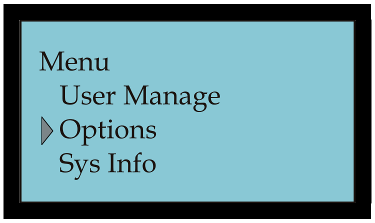


Figure 2-104 Select Options

2. Press **OK** to display Options menu and select Power Mng (see **Figure 2-105**).

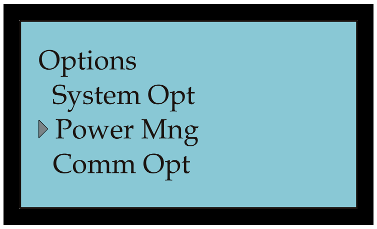
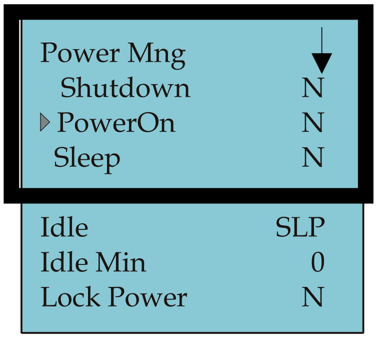


Figure 2-105 Select Power Management

3. Press **OK** to display the Power Mng menu (see **Figure 2-106**).



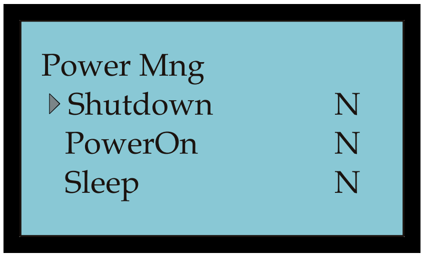
```
Power Mng
  Shutdown      N
▷ PowerOn       N
  Sleep         N
Idle          SLP
Idle Min        0
Lock Power      N
```

Figure 2-106 Power Management Menu

4. Press "▲/▼" to scroll up or down the screen to select the desired option. For Power Management options Idle & Lock Power, press **OK** and use "▲/▼" to enter the desired state. For all other power management options, press **OK** and use the numeric keypad and/or "▲/▼" to enter the desired value (see figure for example). For all power management options, pressing **ESC** will return the default value/state, and exit to the Power Mng menu.

Follow this example to set the shutdown time:

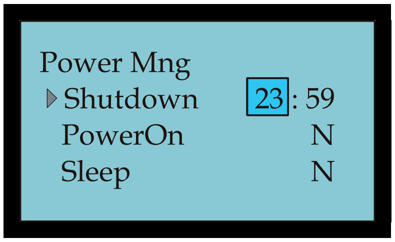
1. Press **OK** from the Power Mng menu, with Shutdown selected (see figure).



```
Power Mng
▷Shutdown        N
 PowerOn         N
 Sleep           N
```

Figure 2-107 Select Shutdown Time

2. Press **OK** to enter shutdown time of day in 24 hour format (see **Figure 2-108**). Use "▲/▼" to move between hours and minutes and the keypad to enter time.



```
Power Mng
▷Shutdown     23 : 59
 PowerOn           N
 Sleep             N
```

Figure 2-108 Shutdown Screen

3. Once the desired shutdown time of day in 24H format is set, press **OK** to exit and display the Power Mng menu (see **Figure 2-106**).

Communications Options Menu

Use the Comm Opt menu at the FPT-40 terminal to set:

- **BaudRate:** The default is "**115200**". The five (5) communications speed options are; 115200, 57600, 38400, 19200, and 9600. The value must be set consistent with the communications ports of the Time Guardian host PC.
- **Dev Num:** The default is "**1**". The range is 1 to 255. The device number is unique for each terminal. If there are two terminals with the same number in the network, they will not work properly and Time Guardian will be confused when polling the terminals.
- **IP Addr:** The default is "**192.168.1.201**". The IP address for the terminal must be unique in the LAN.

- **Net Speed:** The network default speed is "**AUTO**". The other choices are: 10M-H, 100M-H, 10M-F and 100M-F.
- **Net Mask:** The default is "**255.255.255.0**". The subnet mask must be consistent to the LAN IP address of the device.
- **Gateway:** The default is "**0.0.0.0**". If Gateway and Net Mask are not defined, Ethernet will not be active.
- **Ethernet:** select "**Y**" or "**N**" for Ethernet TCP/IP communications. This option must be set to (**Y**)es to utilize Ethernet.
- **RS232:** select "**Y**" or "**N**" for RS232 serial communications.
- **RS485:** select "**Y**" or "**N**" for RS485 serial communications [used for transmission distances over 50 feet].
- **COMM Key:** The default is "**0**". The range is 1 to 999999. This function is not used.

To set communication options:

1. Press the **Menu** button and select Options (see figure).

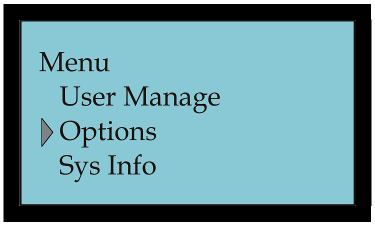


Figure 2-109 Select Options

2. Press **OK** to display Options menu and select Comm Opt (see **Figure 2-110**).

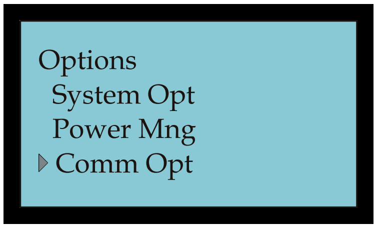
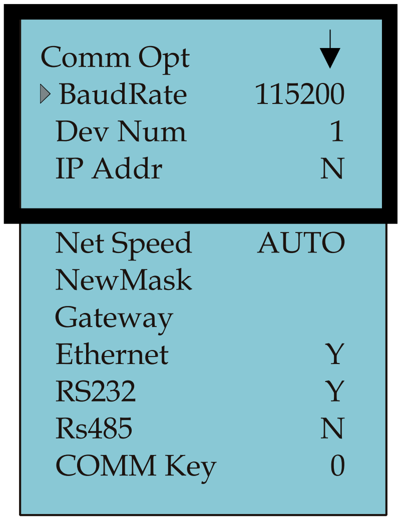


Figure 2-110 Select Comm Opt

3. Press **OK** to display the Comm Opt menu (see **Figure 2-111**).



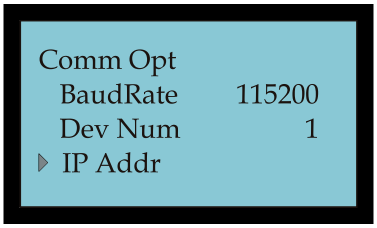
```
Comm Opt          ↓
▷BaudRate   115200
 Dev Num         1
 IP Addr         N
 Net Speed    AUTO
 NewMask
 Gateway
 Ethernet        Y
 RS232           Y
 Rs485           N
 COMM Key        0
```

Figure 2-111 Comm Opt Menu

4. Press "▲/▼" to scroll up or down to select the desired option. Press **OK** and use the numeric keypad and/or "▲/▼" to enter the desired value. For all Comm options, pressing **ESC** will return to the Comm Opt menu with the default value/state.

Follow this example to enter the IP Address:

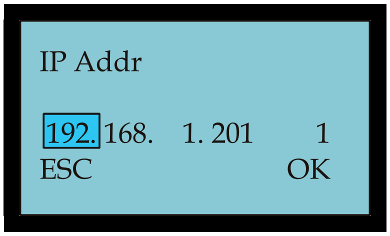
1. From the Comm Opt menu, select IP Addr [IP address] (see figure) and press **OK**.



```
Comm Opt
  BaudRate    115200
  Dev Num          1
▷ IP Addr
```

Figure 2-112 Comm Opt Menu – IP Addr

2. Enter the desired IP address (see **Figure 2-113**) by using "▲/▼" to move forward or backward and the keypad to enter a number.



```
IP Addr

192. 168.   1. 201      1
ESC                    OK
```

Figure 2-113 Enter IP Address

3. Once the correct IP address is entered, press **OK** to save, or **ESC** to exit with the default IP address [192.168.1.201].

Log Options Menu

Use the Log Opt menu at the terminal to:

- **Alm SuperLog:** The default is "99". The range is 0 to 99. When the supervisor capacity log numerical value is reached, an alarm will sound to automatically indicate that the logs are full.
- **Alm AttLog:** The default is "99". The range is 0 to 99. When the attendance log capacity numerical value is reached, an alarm will sound to automatically indicate that the logs are full.
- **ReCheck Min:** The default is "0". Each unit = a minute, i.e., 2 = 2 minutes. This feature is dissabled when set to 0. Recommended setting is 1 or 2 minutes. This feature provides repunch protection. For example, when set to 1 minute, if an employee punches multiple times at the terminal within the 1 minute, only the first punch will be recorded in flash memory. All verified additional punches within the ReCheck Min setting will be follwed by the voice prompt, "*Punch accepted….thank you*".

To set Log Options:

1. Press the **Menu** button and select Options (see figure).

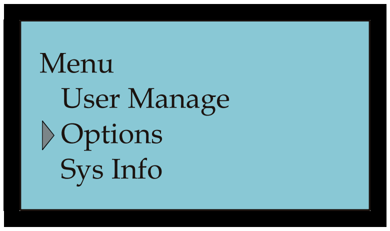


Figure 2-114 Select Options

2. Press **OK** to display the Options menu and select Log Options (see **Figure 2-115**).

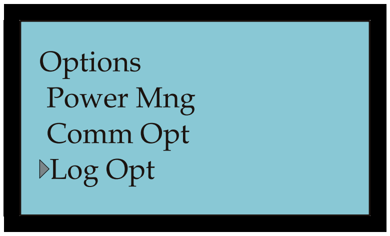
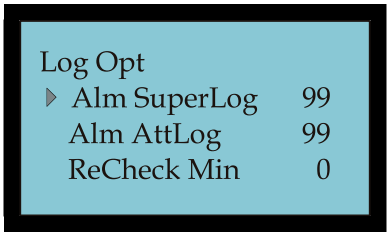


Figure 2-115 Select Log Opt Menu

3. Press **OK** to display the Log Opt menu (see **Figure 2-116**).



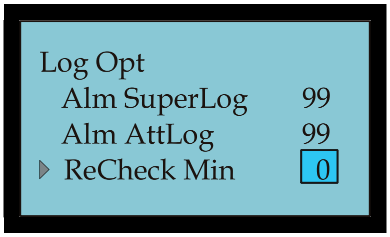
```
Log Opt
▷ Alm SuperLog    99
  Alm AttLog      99
  ReCheck Min      0
```

Figure 2-116 Log Options Menu

4. Select the desired option. For log options, press **OK** and use the numeric keypad and/or "▲/▼" to enter/select the desired value (see figure for example). For all Log options, pressing **ESC** will return to the default value/state and exit to the Log Opt menu.

Follow this example to enter the ReCheck Min:

1. From the Log Opt menu, select ReCheck Min (see figure), and press **OK**.



```
Log Opt
  Alm SuperLog    99
  Alm AttLog      99
▷ ReCheck Min      0
```

Figure 2-117 Log Opt Menu – ReCheck Min

2. Enter the ReCheck Min time (see **Figure 2-117**) by using the "▲/▼" buttons or the keypad to move between minutes [the range is 0 to 99] for time entry.
3. Once the desired ReCheck Min is set, press **OK** to save and return to the Log Opt menu.

Auto Test

This option is designed to run assorted tests on the unit to analyze a failure for quick and easy maintenance. These tests check such things as the memory, LCD display, sound, fingerprint sensor, keypad, and clock. During these tests the power should be maintained to prevent any hardware damage; especially during the memory test. See Diagnostics on page 3-1 for additional information and operational details.

Note: if any users have been setup with privileges, you must be a user with Admin privileges to have access to the Auto Test menu.

Sys Info Menu

This menu can be used to display the following system information:

- **User Cnt:** Displays the total amount of users stored in the terminal.
- **FP Cnt:** Displays the total number of fingerprint templates stored in the terminal.
- **Att Log:** Displays the total number of punches [attendance] stored in the terminal.
- **Admin Cnt:** Displays the total number of administrators stored in the terminal.
- **Pwd Usr:** Displays the total number of users stored in the terminal who are using a password for authentication.
- **S Logs:** Displays the total number of system logs that have occurred. Everytime anything is changed at the terminal it is added in this log. For example, this could include just pressing the **MENU** button.
- **Free Space Info:** Press **OK** to display the following Free Space Info menu to show the remainder of the log capacity:
  - **FP Cnt** – Displays the remaining capacity for fingerprint templates to be stored in flash memory at the terminal.
  - **Att Log** – Displays the remaining capacity for attendance (punches) to be stored in flash memory at the terminal..
  - **S Logs**– Displays the remaining capacity for system logs to be stored in flash memory at the terminal.
- **Dev Info:** Press **OK** to display the following device information for the terminal:
  - **FPCnt (100)** – Displays the total fingerprint template capacity [1500].
  - **AttLog (10K)** – Displays the total attendance (punches) capacity [30,000].
  - **S Logs**– Displays the total capacity of system log capacity [4096].
  - **Manu Time**– Press **OK** to display the date and time the terminal was manufactured. Press **OK** or **ESC** to return to Dev Info menu.
  - **Serial Num**– Press **OK** to display the terminal serial number. Press **OK** or **ESC** to return to Dev Info menu.

- **Vendor**– Not operational. Press **OK** or **ESC** to return to Dev Info menu.
- **Device Name**– Not operational. Press **OK** or **ESC** to return to Dev Info menu.
- **Alg Version**– Press **OK** to display the algorithm version. Press **OK** or **ESC** to return to Dev Info menu.
- **Firmware Ver**– Press **OK** to display the firmware version and release date. Press **OK** or **ESC** to return to Dev Info menu.

To display system information:

1. Press the **Menu** button and select Sys Info (see figure).

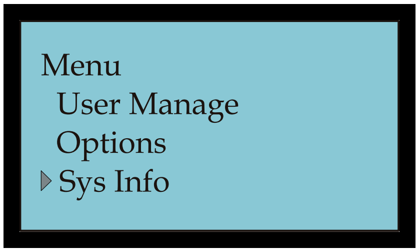
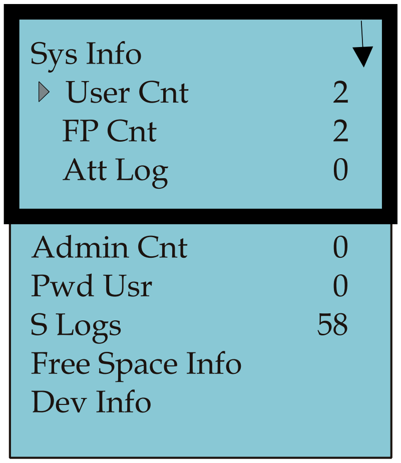


Figure 2-118 Select Sys Info

2. Press **OK** to display the Sys Info menu (see **Figure 2-119**).



Sys Info ▼
▸ User Cnt 2
FP Cnt 2
Att Log 0
Admin Cnt 0
Pwd Usr 0
S Logs 58
Free Space Info
Dev Info

Figure 2-119 System Information Menu

3. Press the "▲/▼" buttons to select/view the desired system info. For Free Space and Dev info, press **OK** to view additional information, or press **ESC** to exit to the main menu.

This page intentionally left blank.

Chapter 3: Troubleshooting

Diagnostics

In addition to system diagnostics which run automatically every time during power up, the FPT-40 Fingerprint terminal has an internal diagnostic utility. This utility can be used to verify the correct operation of the terminal to help isolate faulty operation.

To access diagnostics, perform the following:

1. Press the **Menu** button and select Options (see figure).

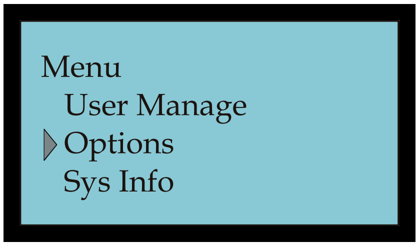


Figure 3-1 Select Options

Note: If no keypad entries are made within a minute, the terminal will beep two (2) times and return to the Welcome screen.

2. Press **OK** to display the Options menu and select Auto Test (see **Figure 3-2**).

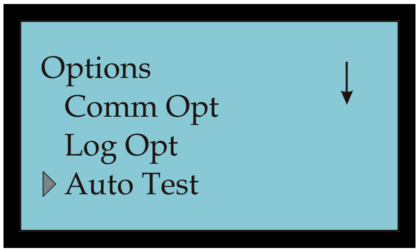


Figure 3-2 Options Menu with Auto Test Selected

Note: If any users have been setup with privileges, you must be a user with Admin privileges to access the Auto Test menu.

3. Press **OK** to display the Auto Test menu (see **Figure 3-3**).

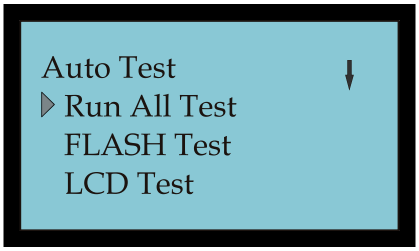
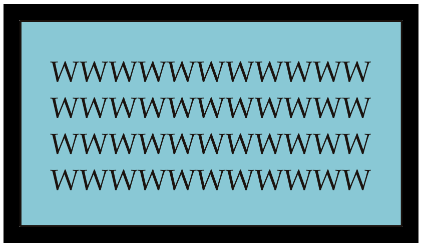


Figure 3-3 Auto Test Menu

4. Use the down ▼ or ▲ up arrow buttons to select the desired test, and press **OK** to run that test (see **Figure 3-4** for an example of LCD test).



```
WWWWWWWWWWW
WWWWWWWWWWW
WWWWWWWWWWW
WWWWWWWWWWW
```

Figure 3-4 LCD Test Screen

5. Follow the on screen prompts. All the tests, except the LCD test, require you to press **ESC** or **OK** at their completion. The LCD test requires that you press **OK** to step through each phase of the test.

Run All Test

Select this test to run all six of the built-in diagnostic tests in the following order; FLASH Test, LCD Test, Voice Test, FP Reader, Key Test, and RTC Test. At the completion of each test press **OK** to move to the next test or press **ESC** to abort testing and return to the Auto Test menu.

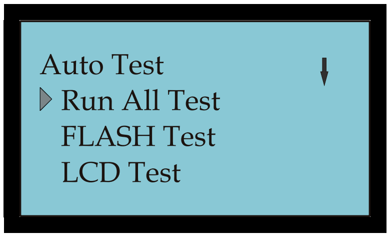
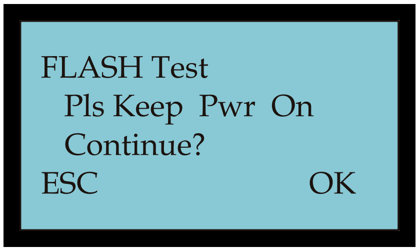


Figure 3-5 Run All Tests

FLASH Test

This will test the flash memory in the FPT-40 Fingerprint terminal and indicate the functional status. Select the FLASH test, and press **OK** to run (see figure).

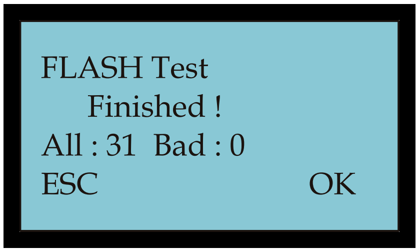
Note: Once this test is started do not interrupt the power as this could cause damage to the internal flash memory.



```
FLASH Test
  Pls Keep  Pwr  On
  Continue?
ESC                    OK
```

Figure 3-6 FLASH Test

The test will display Finished! if the flash memory is good (see figure).



```
FLASH Test
    Finished !
All : 31  Bad : 0
ESC                    OK
```

Figure 3-7 FLASH Test Finished

Press **OK** or press **ESC** to return to the Auto Test menu.

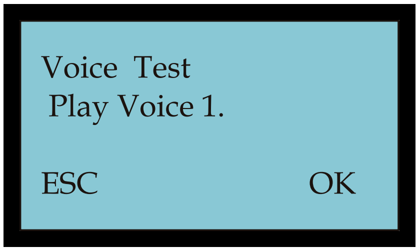
LCD Test

This diagnostic tests the display by turning on all the pixels. Any spots would indicate a defective pixel.

Press **OK** to complete each phase of the test, or press **ESC** to exit the test and return to the Auto Test menu.

Voice Test

This will test the voice prompts stored in the FPT-40 Fingerprint terminal. Press **OK** to play the selected voice prompt (see figure).



Voice Test
Play Voice 1.

Figure 3-8 Voice Test 1

Press **OK** to perform each of the 10 voice tests, or press **ESC** to exit the test and return to the Auto Test menu. The voice test responses are:

Voice 1 = "*Thank you*"

Voice 2 = "*Incorrect password*"

Voice 3 = "*Access denied*"

Voice 4 = "*Invalid ID*"

Voice 5 = "*Please try again*"

Voice 6 = "*Re-enter ID*"

Voice 7 = "*The clock is full*"

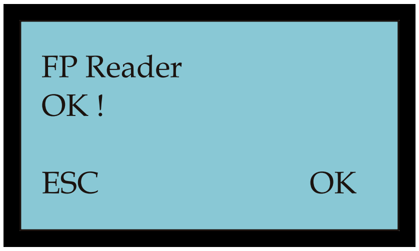
Voice 8 = "*The clock is full*"

Voice 9 = "*Duplicate finger*"

Voice 10 = "*Punch accepted, thank you*"

FP Reader Test

This will test the FP reader in the FPT-40 Fingerprint terminal and indicate the functional status. Select FP Reader test, and press **OK** to perform test. The test will display OK! if the reader status is operational (see figure). Press **OK** or press **ESC** to return to the Auto Test menu.

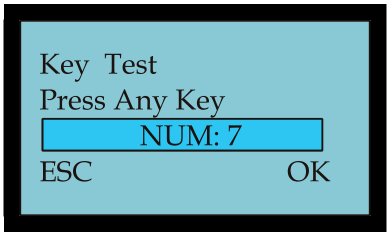


FP Reader
OK !

Figure 3-9 FP Reader OK

Key Test

Once the Key Test has started, pressing any numeric key will display the number on the highlighted test line (see figure). **MENU** will indicate “MENU” and ▼ or ▲ will display “UP” or "DOWN". Press **OK** or press **ESC** to return to the Auto Test menu.

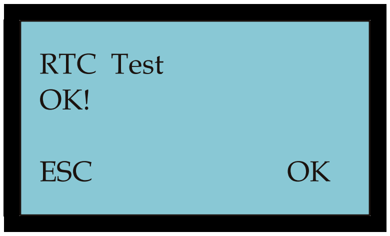


Key Test
Press Any Key
NUM: 7

Figure 3-10 Key Test Example

RTC Test

This will test the Real Time Clock in the FPT-40 Fingerprint terminal and indicate the functional status. Press **OK** to perform test. The test will display OK! if the RTC status is operational (see figure). Press **OK** or press **ESC** to return to the Auto Test menu.



RTC Test
OK!

Figure 3-11 RTC Test Ok

Frequently Asked Questions (FAQs)

1. **Q: Some user's fingerprints occasionally cannot be verified?**

A: The following reasons could lead to a poor fingerprint template:

- Smooth fingerprint
- The fingerprint contains too many drapes [ridges] and/or they change too often
- The fingerprint in question has serious skin shed

Resolution: Select a different fingerprint (less crinkle, no sloughed off skin, clear image), and make your fingerprint touch a larger area of the sensor. Also, enroll more than 1 fingerprint, and use 1:1 match method with password verification method.

2. **Q: FPT-40 Fingerprint terminal(s) fail to communicate?**

   A: The following reasons could lead to faulty communications:

   - COM port configuration is not correct. COM port currently selected is not the actual COM port being used.
   - The Baud rate settings between the fingerprint reader and the PC COM port are different
   - The fingerprint reader has failed to connect with the computer.
   - The fingerprint reader has connected but it is not starting up.
   - The serial number of linked fingerprint reader is not correct.
   - The Data line or converter (CommStik) fails to communicate.
   - The PC COM port breaks down.

3. **Q: Upon power up, the FPT-40 Fingerprint terminal LCD displays incompletely; only half, sometimes jumbled, etc?**

   A: The possible reasons are:

   - Bad motherboard in fingerprint terminal.
   - Bad LCD display, seek service/repair/replacement.

4. **Q: How to clear administrator from the FPT-40 terminal?**

   A: The following method could be used:

   From the FPT-40 Fingerprint terminal clear the Administrator privileges utilizing the "*Clr Admin Pri*" [clear administrator privileges] command from the Adv Option menu. However, if you cannot gain access to do this, you must use the "Clear Maps" command from Time Guardian. See Using the Fingerprint Commands Tab.

   From the Fingerprint terminal follow this procedure:

   Step 1. Press the **MENU** button.

   Step 2. Enter administrator User ID.

   Step 3. Press **OK**, and enter password or press enrolled finger.

   Step 4. Select Options menu with arrow keys, and press **OK**.

   Step 5. From Options menu select System Opt, and press **OK**.

   Step 6. From System Opt menu select Adv Option menu, and press **OK**.

Step 7. Select Clr Admin Pri, and press **OK**.

Step 8. Press **OK** again to confirm, and reset Admin.

Note: Only an administrator will have access to the Adv Opt menu to reset the privileges. When setting up privileges, always setup an Admin first before setting up a Supervisor and Enroller. Failure to do so could result in not being able to get to the menu options for additional setup changes.

5. **Q: When the fingerprint terminal connects serially, and the sound "ding, ding" occurs?**

   A: The possible reasons are:

   - With RS-232 communications, the computer Baud rate may not match the terminal setting.
   - With RS-485 communication, two lines of the converter may be joined.

6. **Q: After fingerprint terminal power up, display always shows "Please try again"?**

   A: The following reasons could lead to fingerprint sensor problems:

   - After a lot of use the surface of the fingerprint sensor becomes dirty, or there are some scratches on it, so the machine thinks that it is a fingerprint and tried to identify it. Clean sensor surface [see Cleaning or Replacing the Optical Sensor].
   - The fingerprint sensor cable may be loose, or possible problem on the circuit PCB. Contact support for service.

Maintenance

Note: Do not attempt to service the fingerprint reader unless you are a trained service technician.

Cleaning

Occasionally, the surface of the optical sensor, the keypad and display window may require cleaning. Since working environments differ, it is not possible to define when cleaning should be performed, but the following is a suggested guide.

Item	Cleaning Frequency
Keypad and display window	Clean when visibly dirty and hard to read. See cleaning procedure.
Optical Sensor	Do not over clean. The sensor is designed to work under greasy or dirty conditions.
	Clean if the sensor performance has degraded to where people are reporting recognition problems. See cleaning procedure.

Cleaning the Keypad and Display

To clean the keypad and display use a soft cloth to wipe.

Cleaning the Optical Sensor

To clean the optical sensor:

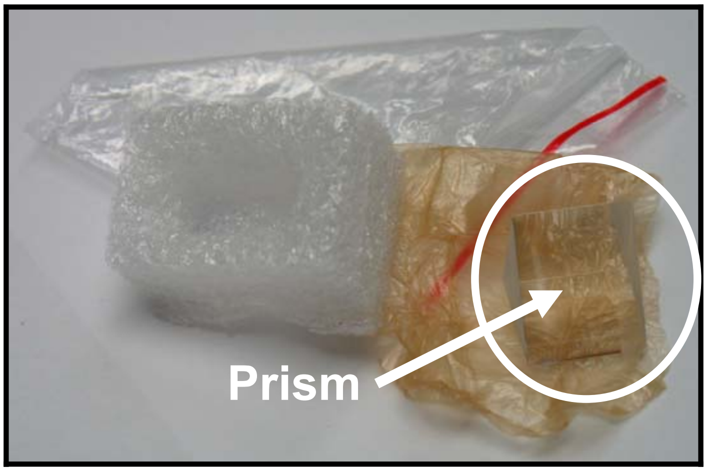
1. If dusty or gritty, first blow on the sensor surface to clean off loose particles.
2. Use adhesive tape to clean the surface.
3. Use a non-abrasive soft dry cloth to wipe the sensor surface. Be careful not to scratch the sensor surface with loose particles (see Step 1).

CAUTION: Do not use any cleaning solutions, as this could damage the optical sensor. Also, cleaning solvents that contain alcohol or other strong substances may discolor or crack the fingerprint reader cabinet.

Replacing Optical Sensor Lens

To replace the optical sensor lens:

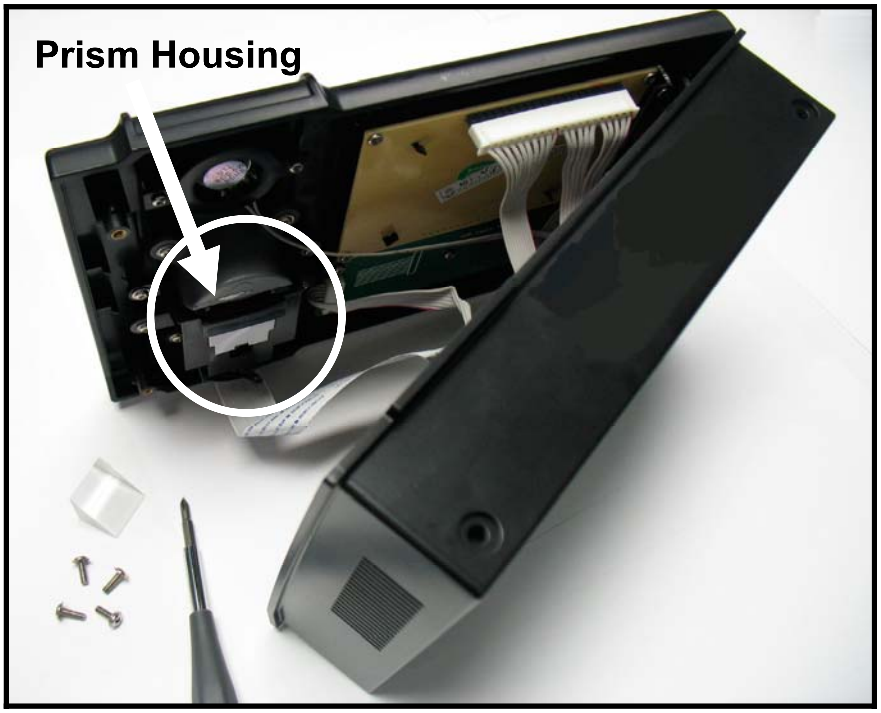
1. If optical sensor lens becomes damaged (scratched) and cannot be cleaned, replacement may be necessary.
2. Use the replacement [spare] optical sensor lens included with the terminal. Remove the spare sensor lens from the protective packaging (see figure), using care not to touch the prism.



3-12 Spare Prism & Packaging

3. Disconnect the AC Power Adapter from the bottom of the terminal.
4. Disconnect the communication cable (either Ethernet or serial DB9 connector)
5. Loosen and remove the four (4) back plate retaining screws and remove the terminal from the wall mounted back plate.
6. Place the terminal on a soft surface face down. Located and remove the four (4) Phillips Head screws holding the case front cover. There will be one screw in each corner on the back of the case.
7. After removing the screws, place the terminal right-side up on the back of the case and VERY CAREFULLY lift the front cover up.
8. The sensor housing must be removed by unscrewing the four (4) Phillips head screws holding it down to access the optical sensor lens (see figure).

9. Loosen and remove the four (4) Phillips head screws holding the sensor/prism housing to access the sensor prism and replace. Use CAUTION not to break any of the ribbon cables. Also, the replacement prism must be mounted with the soft side facing outward.



10. Replace the sensor lens with the new spare, and perform the reverse procedure to re-install the sensor housing, screw the back case on, and remount the terminal to the wall bracket.
11. Reconnect the communication cable, and Power Adapter connector.

Note: It is recommended that the above procedure be performed by someone with electronics knowledge.

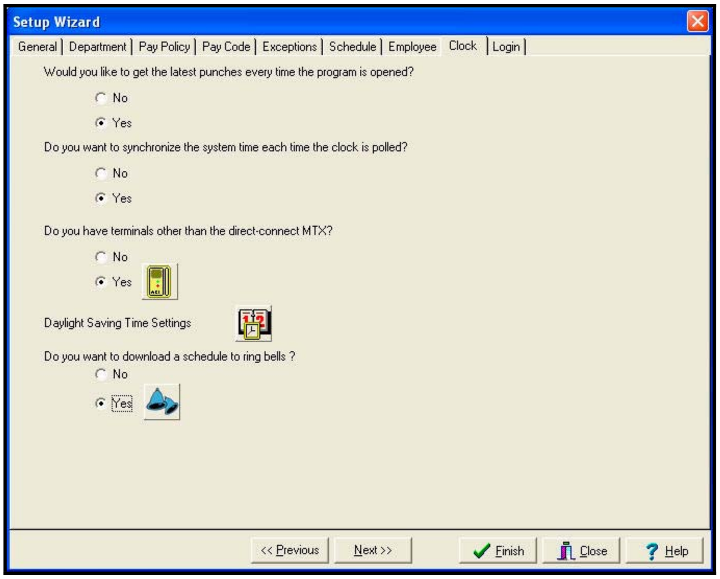
Chapter 4: Time Guardian Interaction

Configuring Time Guardian for the FPT-40 Terminal

See the Time Guardian User's Guide [AMX-20350X] for detailed operation information.

Clock Tab (Communication Settings)

The Setup Wizard in Time Guardian allows you to add, and/or edit terminal(s). To access this module, select the **Setup** menu from the Time Guardian main menu and select the **Wizard** submenu, or click the Wizard icon from the Toolbar. From the Time Guardian Setup Wizard window click on the **Clock** tab (see figure).



Setup Wizard

General | Department | Pay Policy | Pay Code | Exceptions | Schedule | Employee | Clock | Login

Would you like to get the latest punches every time the program is opened?

○ No
● Yes

Do you want to synchronize the system time each time the clock is polled?

○ No
● Yes

Do you have terminals other than the direct-connect MTX?

○ No
● Yes

Daylight Saving Time Settings

Do you want to download a schedule to ring bells ?

○ No
● Yes

<< Previous
Next >>
Finish
Close
Help

__Figure 4-1 Time Guardian Setup Wizard__

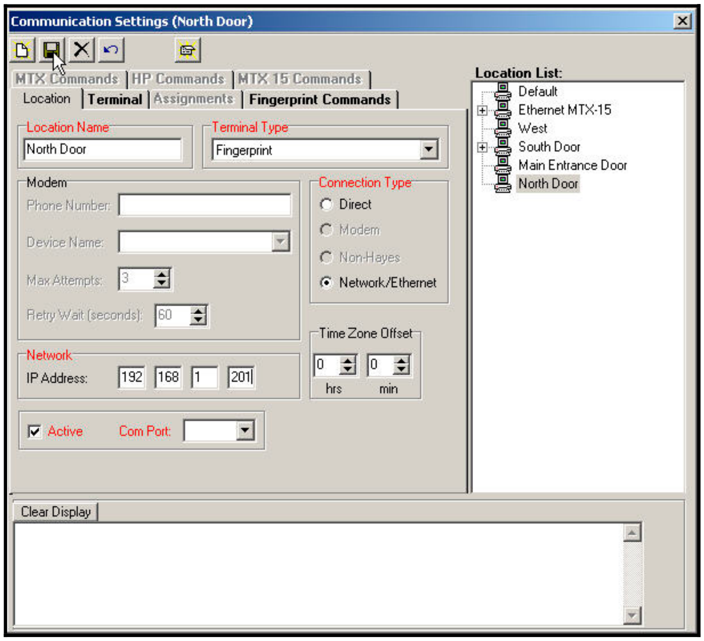
To configure the FPT-40 Fingerprint terminal, click on the button, and the Communications Settings screen will appear. Also, you can access the Communications Settings by selecting the **Setup** menu from the Time Guardian main menu and then selecting **Terminal**.

If you are configuring a networked Ethernet FPT-40 Fingerprint terminal, obtain the correct IP address from your network administrator and enter the IP address in the Location tab screen.

If you are configuring a direct connect serial FPT-40 Fingerprint terminal, determine the PC Comm port that the USB CommStik is connected to and select it in the Location tab screen.

Connecting a Fingerprint Terminal to Time Guardian

The Location tab on the Communication Settings screen (see figure) is used to setup communications between Time Guardian and the FPT-40 Fingerprint terminal. Only one terminal type can be used per Location. If you have more than one terminal type, you must configure multiple Locations.



Communication Settings (North Door)

MTX Commands | HP Commands | MTX 15 Commands |
Location | Terminal | Assignments | Fingerprint Commands |

Location Name: North Door
Terminal Type: Fingerprint

Modem
Phone Number:
Device Name:
Max Attempts: 3
Retry Wait (seconds): 60

Connection Type
○ Direct
○ Modem
○ Non-Hayes
● Network/Ethernet

Network
IP Address: 192 168 1 201

Time Zone Offset
0 hrs 0 min

☑ Active Com Port:

Location List:
- Default
- Ethernet MTX-15
- West
- South Door
- Main Entrance Door
- North Door

Figure 4-2 TG Communication Settings Location Tab

Note: If you fail to connect to the fingerprint terminal, confirm that the Comm Opt settings at the terminal are correct. For example, if your terminal is network connected, the Ethernet connection should be set to Y(es), and the proper IP address set.

How to configure Time Guardian for connection:

1. Create a new Location in Time Guardian for the FPT-40 Fingerprint terminal by clicking on the **New Location** button, and entering the following:

    - **Location Name**: Enter a unique name that will be used to describe the area or site where a terminal or a group of terminals is located.

    - **Terminal Type**: Select Fingerprint from the drop down list as the terminal type.

    - **Connection Type**: If you answered, “Yes” to the question, “Do you have Terminal(s) other than direct-connect MTX, Fingerprint?” in the Clock tab of the Wizard, you must configure those terminals for remote operation. The FPT-40 Fingerprint terminal can communicate with your PC via a direct connection (RS-232C or RS-485C) or Ethernet (network) connections (IP address required).

2. If you selected a Connection Type of **Direct** for your FPT-40 Fingerprint terminal, you should complete the following:

    - **Time Zone Offset**: This can be used if your PC and the Location (terminals) are located in different time zones. The default value is 0:00. Use the drop down lists to configure the offset.

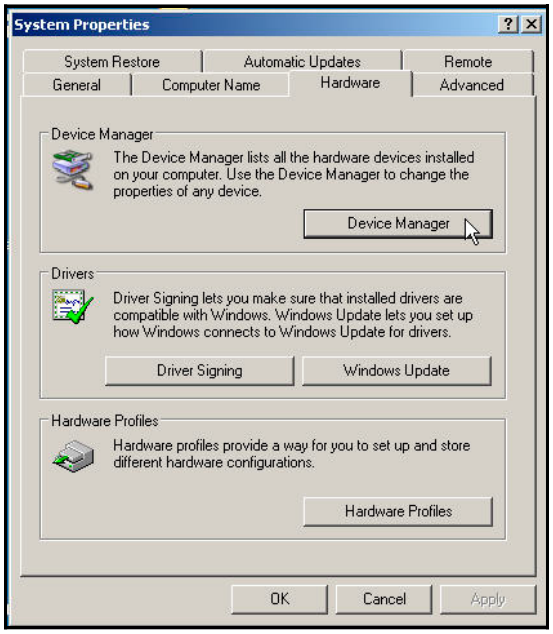
    - **Active**: When checked, the Location will begin sending and receiving data.

    - **Com Port**: Select the Com Port for the PC [that the USB CommStik is connected to] that will communicate with the fingerprint terminal.

        Note: If the terminal is connected to the PC with the CommStik cable when during TG installation with the Setup Wizard, the terminal will be auto-detected and you will not need to determine the Comm Port number.

        See the following for an example of how to determine the Comm Port number using Windows® XP as your operating system:

        Select **Start** from the task bar and right-click on **My Computer**. Select **Properties** from the pop-up menu, and the System Properties screen (see figure) will appear:



Device Manager

The Device Manager lists all the hardware devices installed on your computer. Use the Device Manager to change the properties of any device.

Drivers

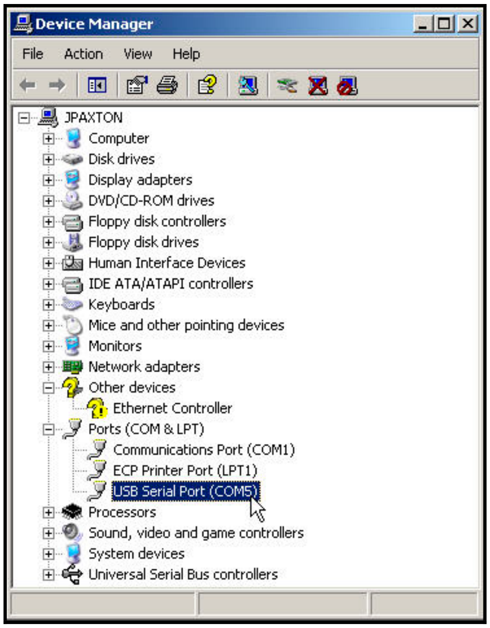
Driver Signing lets you make sure that installed drivers are compatible with Windows. Windows Update lets you set up how Windows connects to Windows Update for drivers.

Hardware Profiles

Hardware profiles provide a way for you to set up and store different hardware configurations.

Figure 4-3 Windows System Properties

Select the Hardware tab (see above figure), and then click on the "**Device Manager**" button, and the Device Manager screen (see figure) will appear. Expand the **Ports (Comm & LPT)** from the tree view, and find the "USB Serial Port" (see example figure). This is your Comm Port number to select from the drop down on the Time Guardian Communications Settings screen.



JPAXTON
- Computer
- Disk drives
- Display adapters
- DVD/CD-ROM drives
- Floppy disk controllers
- Floppy disk drives
- Human Interface Devices
- IDE ATA/ATAPI controllers
- Keyboards
- Mice and other pointing devices
- Monitors
- Network adapters
- Other devices
  - Ethernet Controller
- Ports (COM & LPT)
  - Communications Port (COM1)
  - ECP Printer Port (LPT1)
  - USB Serial Port (COM5)
- Processors
- Sound, video and game controllers
- System devices
- Universal Serial Bus controllers

Figure 4-4 Windows Device Manager

3. If you selected **Network** as the Connection Type for your FPT-40 Fingerprint terminal, enter the IP Address in the spaces provided.

   - **IP Address**: The IP Address of the terminal(s). You may have to obtain this from network administrator. see Communications Opt for default Ethernet address and configuration at the terminal.
   - **Time Zone Offset**: This can be used if your PC and the Location (terminals) are located in different time zones. The default value is 0:00. Use the dropdown lists to configure the offset.
   - **Active**: When checked, the Location will begin sending and receiving data.

Note: During TG installation and using the Setup Wizard, an Ethernet connected Fingerprint terminal will not be auto-detected.

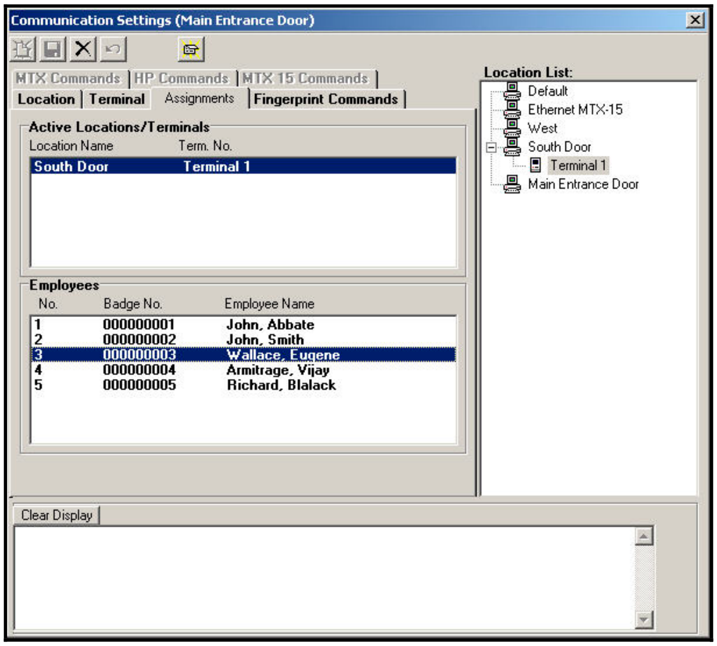
4. After you entered the correct information, click on the **Save** button. The new Location Name will appear in the Location List. To clear any terminal information entered in the Time Guardian Communications Settings, click on the **Cancel** button.

   To delete a Location, select the desired Location from the Location List and click on the **Delete** button. A message will appear to confirm your selection.

5. To exit the Time Guardian Communication Settings dialog, click on the **Close** button to return back to the Time Guardian main screen.

Assignments Tab - Clock

The Assignments tab in Time Guardian (see figure) can be used to manually assign employees/users to a terminal or a group of terminals. If employees' records already exist in the database, polling a terminal will automatically create employee terminal assignments.



Active Locations/Terminals

Location Name	Term. No.
South Door	Terminal 1

Employees

No.	Badge No.	Employee Name
1	000000001	John, Abbate
2	000000002	John, Smith
3	000000003	Wallace, Eugene
4	000000004	Armitrage, Vijay
5	000000005	Richard, Blalack

Figure 4-5 TG Communication Settings Assignments Tab

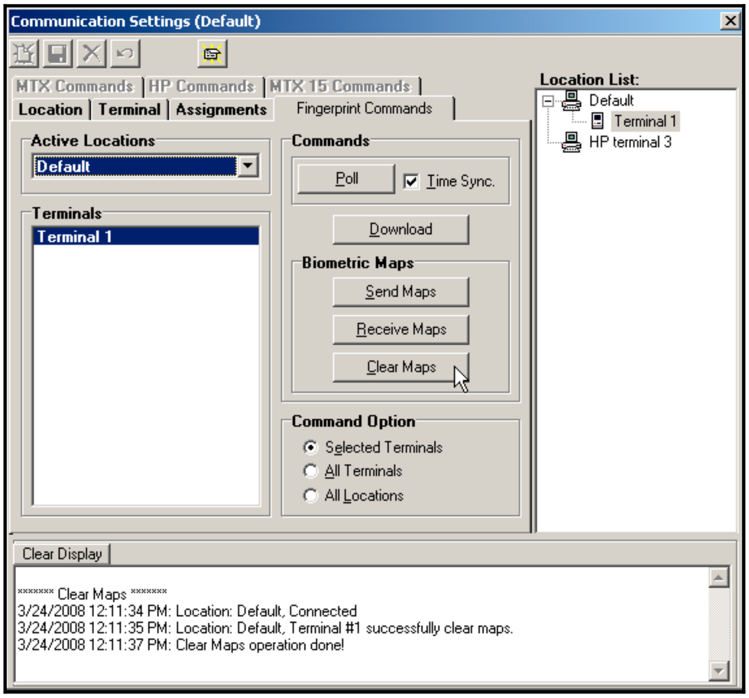
The Assignments tab consists of Locations/Terminals and Employees lists. The Locations/Terminal list displays all the Locations in the system and their terminals. Selecting one or more of the terminals allows the user to assign employees to the selection. When a terminal is selected, the employees assigned to it will be displayed in the Employees window. If multiple terminals are selected, only those employees common to all selected terminals will be displayed.

Using the Fingerprint Commands Tab

From the Time Guardian Communication Settings screen, this tab allows you to perform the following functions with the FPT-40 Fingerprint terminal:

- **Poll:** Press the Poll button to collect the most recent data from the terminal(s) (i.e., fingerprint templates and punches). When checked, Time Sync. performs time synchronization between the Host PC and the terminal(s) including Daylight Saving settings.

- **Download:** Press the Download button to send time, Daylight Saving Time settings, hours worked for the current pay period, and employee assignments. The hours worked will be retained at the terminal from the date of the last download for up to 14 days. If no new download occurs within 14 days, the hours worked will not appear after 14 days.



Active Locations: Default

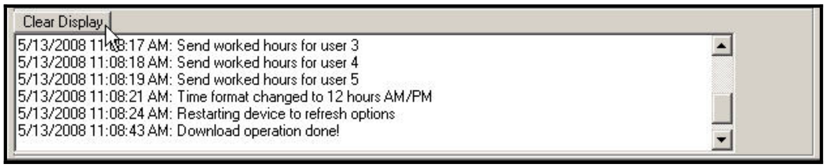
☑ Time Sync.

Command Option
- ● Selected Terminals
- ○ All Terminals
- ○ All Locations

```
******* Clear Maps *******
3/24/2008 12:11:34 PM: Location: Default, Connected
3/24/2008 12:11:35 PM: Location: Default, Terminal #1 successfully clear maps.
3/24/2008 12:11:37 PM: Clear Maps operation done!
```

Figure 4-6 TG Communication Settings Fingerprint Commands Tab

Note: When this button is pressed, the terminal display will show **Downloading….**, followed by **Working….**, and finish with **Restarting…..**The terminal will power off then back on to refresh with the options just downloaded to it. Simultaneously the lower portion of the Time Guardian Fingerprint Commands screen will display the location, terminal # downloaded date/time, hours worked sent for users X to Y, time format changes, restarting device, and download operation done (see figure). Click on Clear Display to clear the displayed information.



```
5/13/2008 11:08:17 AM: Send worked hours for user 3
5/13/2008 11:08:18 AM: Send worked hours for user 4
5/13/2008 11:08:19 AM: Send worked hours for user 5
5/13/2008 11:08:21 AM: Time format changed to 12 hours AM/PM
5/13/2008 11:08:24 AM: Restarting device to refresh options
5/13/2008 11:08:43 AM: Download operation done!
```

Figure 4-7 TG Download Communications Display

Biometric Maps: The terminal must be polled before performing the following operations. Polling the terminals will save biometric fingerprint templates for newly enrolled employees, automatically update the database with templates for employees who have punched at the terminal, and create terminal assignments for employees that have not yet been enrolled in the database.

Note: If a newly enrolled employee does not exist in the employee database, then the template in the terminal will not be saved. If the template data is inadvertently lost, it must be reassigned to the terminal through the Assignments tab.

Each time an employee punches at the FPT-40 Fingerprint terminal, their finger template (map) will automatically be updated in the employee database with the most recent template from the terminal. This feature is for maintaining accurate fingerprint templates. However, if the employee does not exist in the employee database, then a message will be displayed in the message window at the bottom of the tab.

Once an employee is added to the Employee database, their template will not automatically be uploaded unless the employee is removed and re-enrolled at the terminal, or a punch is received from the terminal. Once this is done, however, the employee's template will be saved and an assignment will automatically be created.

- **Send Maps:** Press the Send Maps button to send user(s) biometric map(s) from the employee database in Time Guardian to the selected terminals. Only employees assigned to terminals will be sent. Employees are assigned to terminals from the Assignments tab, or by polling. Because the "*Send Maps*" operation consists of first clearing all templates from the terminal and then loading assigned employee templates, a confirmation dialog box will appear before this command executes to click the Yes button on the Confirm dialog to proceed.

- **Receive Maps:** Press the Receive Maps button to receive employee templates from the selected terminal(s) to the Time Guardian database. Only templates assigned to the selected terminals will be uploaded to TG. Employees are manually assigned to the terminals in the Assignments tab.

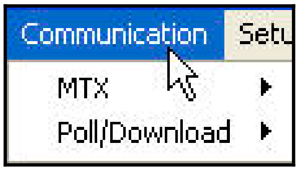
- **Clear Maps:** Press the Clear Maps button to clear (delete) all assigned employee templates from the terminal. Because the Clear Maps operation consists of clearing all templates from the terminal, a confirmation dialog box will appear before this command executes. Must click the Yes button on Confirm dialog to proceed.

⚠ ***Caution!*** This command can be used to clear [reset] the terminal if an Administrator has been setup and the password is lost, etc. Access at the terminal to the menu options, etc. maybe denied unless it is an Administrator.

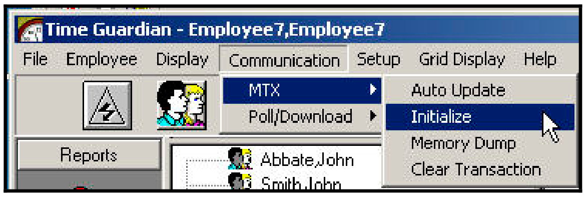
Note: All the above command options can be performed at either Selected Terminals, All Terminals, or All Locations. Whereas, the "Polling" and "Downloading" commands from the Communication menu can only be performed on All Terminals at All Locations.

Communication Menu

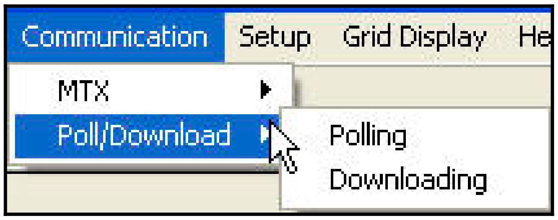
The Communication menu can be used to remotely perform functions on active terminals from the Host PC. It is divided into two groups, those functions distinct to MTX terminals, and those for polling and downloading to the all terminals connected to Time Guardian. Click on **Communication** from the main Time Guardian screen view and the following dropdown menu will appear:



The **MTX** submenu selections (see figure) only allows you to perform the following operations on active MTX Time Guardian terminals:



The **Poll/Download** submenu selection allows you to perform the following operations on all active Time Guardian terminals, including FPT-40 Fingerprint, MTX, and Hand Punch terminals. Click on **Poll/Download** submenu from the Communication menu and the following pop up menu will appear:



Descriptions of the Communications/Fingerprint, MTX, and Hand Punch functions follow:

- **Polling**: This operation collects the most recent data from the terminal. When checked, Time Sync. performs time synchronization between the Host PC and the terminal including Daylight Saving settings. See Using the Fingerprint Commands Tab on page 4-6 for more detail.

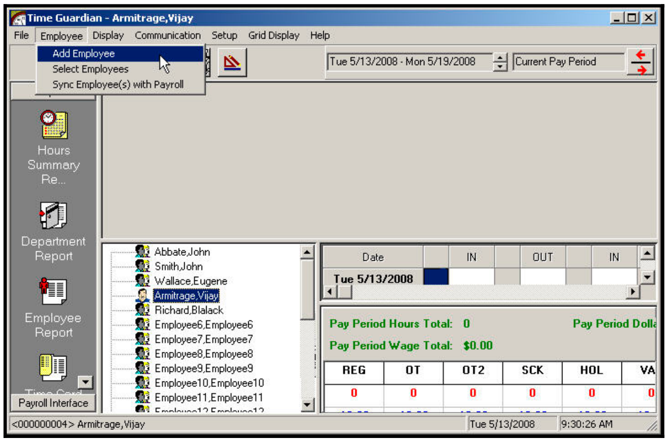
- **Downloading**: Sends Daylight Saving Time (DST) settings, employee assignments and Bell and Door Schedules to the terminal. See Using the Fingerprint Commands Tab on page 4-6 for more detail.

Note: When this command is issued, the fingerprint terminal display will show **Download….**, followed by **Working….**, and finish with **Restarting…..**The terminal will power off then back on to refresh the options just downloaded to it. Simultaneously the lower portion of the Fingerprint Commands screen will display all sent assigned users, and any time format changes (see the following figure). Click on Clear Display to clear the displayed information.

⚠ ***Caution!*** The Poll and Download commands, when used from the **Communications** menu in Time Guardian will perform these functions to selected terminals, all terminals, and all locations.

Employee Privileges Setup

From the main menu of Time Guardian, select **Employee** => **Add Employee** (see figure) and the following Employee Information screen will appear:



Tue 5/13/2008 - Mon 5/19/2008 | Current Pay Period

Abbate,John
Smith,John
Wallace,Eugene
Armitrage,Vijay
Richard,Blalack
Employee6,Employee6
Employee7,Employee7
Employee8,Employee8
Employee9,Employee9
Employee10,Employee10
Employee11,Employee11

Date		IN		OUT		IN
Tue 5/13/2008						

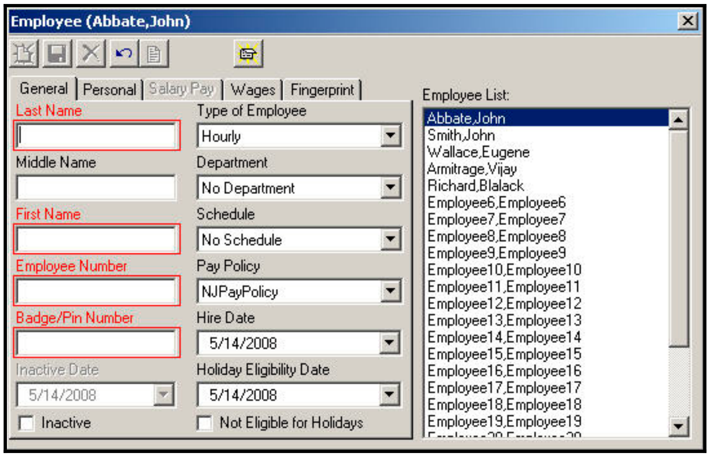
Pay Period Hours Total: 0 Pay Period Dolla

Pay Period Wage Total: $0.00

REG	OT	OT2	SCK	HOL	VA
0	0	0	0	0	0

<000000004> Armitrage,Vijay | Tue 5/13/2008 | 9:30:26 AM

or just double-click on the desired employee from the employee list (see above figure) and the following Employee Information screen will appear:



Last Name:

Middle Name:

First Name:

Employee Number:

Badge/Pin Number:

Inactive Date: 5/14/2008

□ Inactive

Type of Employee: Hourly

Department: No Department

Schedule: No Schedule

Pay Policy: NJPayPolicy

Hire Date: 5/14/2008

Holiday Eligibility Date: 5/14/2008

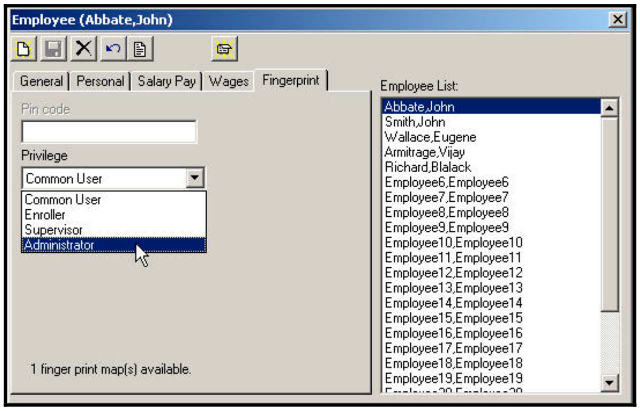
□ Not Eligible for Holidays

Employee List:
Abbate,John
Smith,John
Wallace,Eugene
Armitrage,Vijay
Richard,Blalack
Employee6,Employee6
Employee7,Employee7
Employee8,Employee8
Employee9,Employee9
Employee10,Employee10
Employee11,Employee11
Employee12,Employee12
Employee13,Employee13
Employee14,Employee14
Employee15,Employee15
Employee16,Employee16
Employee17,Employee17
Employee18,Employee18
Employee19,Employee19

Select the desired employee from the "*Employee List*", and click on the **Finger Print** tab.

Note: The Finger Print tab is only available if the employee has been assigned to a location which has a “Fingerprint” selected as the terminal type.

This tab can be used to set Employee privileges at the fingerprint terminal (see the following figure). This screen will also display the amount of fingerprint maps currently enrolled for this employee. Maps are sent to Time Guardian when the fingerprint terminal(s) is/are polled. Maps can be cleared from Time Guardian, and are also sent to the terminals from Time Guardian when the Send Maps button is pressed from the Fingerprint Commands screen (see Send Maps on page 4-7).



Employee (Abbate,John)

Pin code

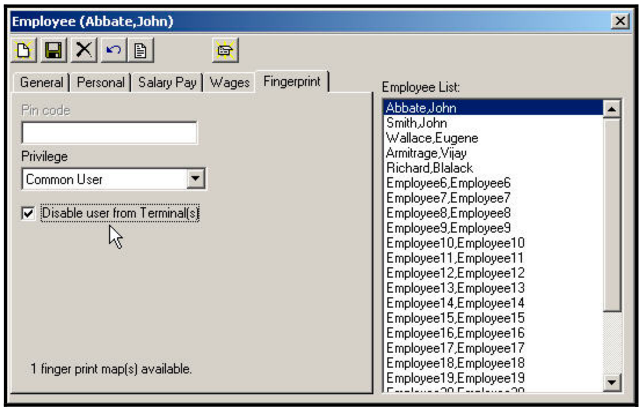
Privilege: Common User

1 finger print map(s) available.

Employee List:
Abbate,John
Smith,John
Wallace,Eugene
Armitrage,Vijay
Richard,Blalack
Employee6,Employee6
Employee7,Employee7
Employee8,Employee8
Employee9,Employee9
Employee10,Employee10
Employee11,Employee11
Employee12,Employee12
Employee13,Employee13
Employee14,Employee14
Employee15,Employee15
Employee16,Employee16
Employee17,Employee17
Employee18,Employee18
Employee19,Employee19

Figure 4-8 TG Employee Fingerprint Tab

- **Privilege:** Select the desired terminal access privilege from the drop down menu. The choices are: Common User, Enroller, Administrator, and Supervisor. In order to update the user privileges defined in Time Guardian, you must press the Send Maps button to send this information to the terminal(s).
- **Disable user from Terminal(s):** Check this box to prevent this employee from having access at this terminal (see figure). In order to actually disable users at the terminal(s), you must press the Send Maps button to send this information to the terminal(s).



Employee (Abbate,John)

Pin code

Privilege: Common User

☑ Disable user from Terminal(s)

1 finger print map(s) available.

Employee List:
Abbate,John
Smith,John
Wallace,Eugene
Armitrage,Vijay
Richard,Blalack
Employee6,Employee6
Employee7,Employee7
Employee8,Employee8
Employee9,Employee9
Employee10,Employee10
Employee11,Employee11
Employee12,Employee12
Employee13,Employee13
Employee14,Employee14
Employee15,Employee15
Employee16,Employee16
Employee17,Employee17
Employee18,Employee18
Employee19,Employee19

Figure 4-9 TG Employee Disable User

- **PIN code:** Shown with masked password [asteriks] when employee has a password with a statement on the bottom of the screen such as; "*1 finger print map(s) and Password available*". This field can be used to change the employee's password.

Note: The employee must have had a password originally created at the terminal. If no password exists for this employee you can not access this field. **<u>This field can only be used to change an existing password, not create one!!</u>**

NOTES

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures: Reorient or relocate the receiving antenna; Increase the separation between the equipment and receiver; Connect the equipment into an outlet on a circuit different from that to which the receiver is connected; Consult the dealer or an experienced radio/TV technician for help.