



## **Fingerscan Supervisor and Manager User Guide**

**Version 4.00**

**November 1996**

**FUJITSU Australia Limited**

376 Lane Cove Road  
North Ryde, NSW 2113, Australia  
Tel: +61 2 9887 9222  
Fax: +61 2 9878 5150

© Copyright Fingerscan Pty Ltd. All rights reserved. Under the copyright laws this manual cannot be reproduced in any form without the prior written permission of Fingerscan Pty Ltd. No patent liability is assumed with respect of the information contained herein.

FINGERSCAN is a registered trademark of Fingerscan Pty Ltd.

Windows is a trademark of Microsoft Corporation.

Disclaimer. Fingerscan Pty Ltd makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims any warranties, merchantability or fitness for any particular purpose. Any software described in this document is sold or licensed “as is”.

This company reserves the right to revise this document and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or changes.

#### STYLE CONVENTIONS

<b>BOLD</b>	External document or heading
<b>Lowercase Bold</b>	Selection option (check box or radio button) or menu option
<i>ITALIC</i>	Internal cross-reference
[xyz]	manually keyed input
<u>UNDERLINE</u>	Note, Caution or Warning or emphasis

# Contents

<b><u>Introduction</u></b>	<b>5</b>
Maintaining the local database	5
ID Number	5
Finger Type	6
Finger Image Record	6
Security Threshold	6
Authority/Management Control	6
Time Zones	7
System Set Up and Manager Functions	7
<b><u>Accessing the SYSTEM menu</u></b>	<b>8</b>
<b><u>Setting up the System</u></b>	<b>9</b>
Changing Security Defaults	10
Changing the Default Security Threshold	11
Changing the False Finger Default Setting	12
Changing the HS Platen default	13
Changing the Number of Verifications Default	14
Changing ID Defaults	14
Changing the ID Number Length	14
Activating the Display Finger Option	15
Changing the Display ID Number Option	15
ID # Search = Standalone Mode ONLY	16
Activating the Card/ Smart Card Reader	16
Setting the Relay	17
Changing the Alarm Defaults	18
Selecting the Input Alarms	19
Activating an Alarm on Unsuccessful Verification	20
Changing the <i>Normally Open</i> Alarm Default	20
Activating a Door Switch Alarm	21
<b><u>Setting up Communications</u></b>	<b>23</b>
Setting up Host Communications	23
Setting the Auxiliary Baud Rate	24
Activating the Wiegand Option	25
Changing the List Log Printing Options	25
Transaction Log and <i>FINGERSCAN</i> Messages	27
<b><u>Setting the Clock</u></b>	<b>30</b>

## Contents

---

### **Setting Time Zones** **32**

---

Setting Specific Time Zones	32
Assigning a Default Time Zone	33
Deleting a Time Zone	34

### **Manager Functions** **35**

---

Disabling Access to the Set up Menu	35
Resetting the System	35

### **Maintaining the Local Database** **37**

---

Searching for a Specific ID Number	37
Modifying a Single Database Entry	38
Changing a User's Authority Level	38
Changing a User's Time Zone	39
Changing a User's Verification Threshold	40
Changing the False Finger Threshold on an Individual Basis.	41
Changing a User's Door Access	41
Deleting a User's Template	42

### **Troubleshooting** **43**

---

### **Cleaning and Maintenance** **46**

---

### **Menu Trees** **47**

---

Maintaining the Local Database	47
Setup & Manager's Facility	47

### **Index** **50**

---

## Introduction

The system set up should be followed when FINGERSCAN is first installed to check system defaults and customise the system to the specific requirements of your site. This is described in full in the section - *Setting Up the System* of this Section. If the FINGERSCAN is brand new, or has been fully reset, then the template database is empty. In this condition, the FINGERSCAN will permit managerial access to anyone until the first enrolment has been done. Therefore, it is not necessary to be enrolled in the system to carry out the set up actions. The first enrolment will always be assigned the authority level of 'manager'.

Once the system is operational, and enrolments have been done, those assigned with Supervisors or Manager authority can maintain the template and user id database and make changes to the system set up using the procedures detailed in the Section - *Maintaining the Local Database* of this Section.

## Maintaining the local database

The local database consists of the templates (enrolment records) of those enrolled on the system. The template consists of;

- The user's id number
- Optionally, the finger type (such as 'right index' or 'left middle')
- The finger image record
- The security threshold
- The user's authority
- Optionally, any of two time zones assigned to the user.

While default values for all of the above are assigned at the time of enrolment, all of them other than the finger image record, can be modified after the initial enrolment. Further, they can be deleted.

## ID Number

Each template must have some means of identifying to whom it belongs. When a verification request is made, the id number is used to locate the required template. Otherwise the FINGERSCAN would have to check each template in its memory and this would slow down the verification process. ID numbers are normally called up via the keypad, but can be called up through other storage means, such as a magnetic stripe, barcode or Wiegand card.

## Finger Type

It is recommended that the particular finger used is recorded during enrolment so that, at verification, the user can be prompted as to which finger to use. This is especially important where alternate fingers are also enrolled under the same common number. Up to three fingers can be enrolled under one number.

## Finger Image Record

This is the actual record of the selected 3-dimensional image characteristics of the finger. A template typically is 1247 bytes in length. Templates are normally stored in the local database, but can be stored on a PC, or a smart card or any other suitable medium, either instead of or as well as the local database.

## Security Threshold

This is the degree to which the verification is examined to ensure that the person is the person claimed. The threshold can be raised or lowered. Raising the threshold increases security, while lowering it increases throughput. The correct balance is essential for a smooth running system. This is described in detail in the section - *Setting Up the System: Changing Security Defaults*.

## Authority/Management Control

FINGERSCAN has four levels of management control:

- **User**

A user submits a finger for verification after entering an ID number

- **Enroller**

An enroller has user status and can also enrol users onto the system

- **Supervisor**

A supervisor has enroller status and can also perform initial system set up procedures, set time zones, set alarm codes, and add and delete templates

- **Manager**

A manager has supervisor status and can also perform a total system reset, and disable the supervisor's ability to change the setup.

## Time Zones

Users may have time periods assigned during which they can gain access and outside which they cannot. Up to thirty global or individual time zones can be defined in FINGERSCAN. Each user can have up to two active time zones at any time. Users may be allocated a default time zone at enrolment, which can be changed by the system supervisor.

## System Set Up and Manager Functions

Each FINGERSCAN comes from the factory with preset default settings. However, some of these may not suit the particular application.

The Set Up facility covers five major areas:

- Setting up the default enrolment values. While these can be individually changed as described in the section - *Maintaining the Local Database*, the default values can be changed at set up so that the correct values are being assigned to all new enrollee's, as close as can be done.
- Setting up the default output values. This includes the relay and the four alarm inputs and outputs.
- Setting up the system communications so that the FINGERSCAN can be connected to a PC, laptop or over a network.
- Managing the transaction log.
- Setting up the FINGERSCAN date and time.

The Manager's functions include resetting the password, disabling the set up facility and doing a complete memory reset.

The *Troubleshooting* and the *Maintenance* sections are included at the end of this manual.

## Accessing the SYSTEM menu

To maintain FINGERSCAN operations via the keypad, it is necessary to first access the SYSTEM menu.

Users do not have authority to access this menu. Enrollers and Supervisors have limited menu access. Managers have full access to all operations. Normally there are very few managers.

To access the SYSTEM menu, press the **SYSTEM** button, enter a valid ID with an authority greater than User, and then verify normally. The SYSTEM menu is then shown.

NOTE: System entry verifications will not activate door lock outputs.

## Setting up the System

Each FINGERSCAN is set up in the factory with certain default settings. These affect facilities such as verification thresholds, relays and alarms.

Once the unit has been installed the defaults should be checked and changed where necessary, following the procedures in this section, to meet your specific site's requirements.

Note that is NOT necessary to be enrolled on the FINGERSCAN to perform the set up functions, provided it is brand new or just fully reset and therefore has no templates in the database. If the unit has been used, then only those with Manager or Supervisor authority can perform the set up functions.

1. To change the system default settings on a new or empty unit, press **3-SET UP** from the Main Menu and enter any 4 digit number.

The **SET UP MENU** is displayed

1:SYSTEM	2:COMMS
3:CLOCK	4:ZONES

2. Select **1-SYSTEM**

**NOTE:** The option exists for the system Manager to disable the set up functions. In this case options 1, 3, and 4 on the set up menu may be disabled.

The **SYSTEM MENU** will be displayed

1:SEC	2:ID/CARD
3:RELAY	4:ALARMS

From the **SYSTEM MENU** you can change

- **Security settings**
- **ID and Smart Card settings**
- **Relays**
- **Alarms**

## Changing Security Defaults

1. Select **1-SEC** to set up the security settings. From this menu you can
  - Change the overall security threshold
  - Change the false finger reading level
  - Change the HS platen reading
  - Change the number of verifications required for access

### Security Threshold

The threshold setting provides a balance between False Acceptance and False Rejection rates. There is a trade-off between these. The lower you make one, the higher the chance that the other error might occur and vice versa.

A variable threshold is provided due to different installation requirements. Sites which desire high rates of throughput (such as time & attendance, factory or health club access and so on) will probably want a low False Rejection rate. On the other hand, sites which require a high degree of security and an irrefutable audit trail (such as bank vault doors, secure information centres), will want a False Acceptance rate of one in a million.

Recommended Security Threshold settings for different security levels are:

Heavy throughput / low security	050-080
Commercial / industrial security	100+/-
High security	125 (there is little advantage to setting the level above 125 where the chance of false acceptance is less than 0.000001)

The security threshold default is 100, which means that each new enrollee is automatically assigned a security threshold of 100. The default Security Threshold setting can be changed as described below.

Security threshold settings are applied to individual user templates at the time of enrolment. The individual's threshold can be changed at any time using the MODIFY function in the LOCAL MENU (see the *Database Maintenance* section).

Changing the overall threshold will not affect existing templates, only the new enrolments. Existing templates must be changed using database maintenance functions.

## Changing the Default Security Threshold

1. Select **1-SEC** from the **Set up** Menu.
2. Select **1-SECURITY** from the **Security** Menu. The display will show

SECURITY = 100  
CHANGE Yes/No ?

where '100' is the factory default security threshold assigned to all new enrolments.

3. Select **NO** to accept the current default and the menu returns to the previous level.
4. Select **YES** to change the default.

ENTER SECURITY  
LEVEL

5. Enter any number from [0] to [200] and the security setting will be changed. The value will be displayed.
6. If the new value is the one you want press **YES** to confirm.
7. If the value is incorrect press **NO** and re-enter a value.

The Security Menu will be displayed.

NOTE that '0' is a true '0' threshold and the user assigned this value will be operating on id number only.

## False Finger Level

This security setting determines the degree to which the FINGERSCAN checks to see if the finger being presented is a live or fake finger. The scale is between 0 and 200, with 0 being minimum.

While completely different from the security threshold, a higher False Finger level will increase the chances of a False Rejection. Consequently, unless high security is required, it is recommended that the factory default setting of 10 is maintained. The settings for different security requirements are:

Heavy throughput/extremely low security	0-10
Medium throughput/normal security	10
Low throughput/high security	40
Top secret security	100+ (there is little advantage gained above 100)

## High Security Platen

The HS Platen is normally deactivated. When activated, it acts in conjunction with the False Finger Level to detect the presence of a fake finger. The HS Platen normally does not effect the false rejection rates at lower settings. The scale is between 0 and 200, with the recommended setting of not greater than 20, as under some conditions this can have a serious reduction in verification quality.

## Changing the False Finger Default Setting

1. Select **2-FF** from the **Security** Menu.

FF LEVEL = 10  
CHANGE Yes/No ?

where '10' is the factory False Finger Level default assigned to all new enrolments.

2. Select **NO** to accept the current default and the menu returns to the previous level.
3. Select **YES** to change the default.

ENTER FF  
LEVEL

4. Enter any number from [0] to [200] and the security setting will be changed. The value will be displayed.
5. If the new value is the one you want press **YES** to confirm.
6. If the value is incorrect press **NO** and re-enter a value.

The HS Platen option will be displayed.

### Changing the HS Platen default

1. Select **2-FF** from the **Security** Menu and choose **NO** to the question FF LEVEL = CHANGE Yes/No ? The display will show

HS PLATEN = 0  
CHANGE Yes/No ?

2. The default value 0 means the HS Platen is not activated. To activate select **YES**.

ENTER HS PLATEN  
LEVEL

3. Select any number from [0] to [200]. A maximum value of 20 is recommended. The FINGERSCAN performs a memory test and displays the message

HIGH SECURITY  
PLATEN ACTIVE

before returning to the previous menu. The platen can be turned off again by entering a value of **0**.

## Changing the Number of Verifications Default

The Verifications Option allows for multiple fingers to be verified to gain access. This option would be used if more than one user is required to achieve access rights, for example, to open a safe.

1. Select **3-VERIFICATIONS** from the **Security** Menu. The display will show

VERIFICATIONS = 1
CHANGE Yes/No ?

2. To request 2 verifications, select **YES**. The number 2 will be displayed.
3. Press **NO** to select 2 or **YES** to change the number to 3. Repeat the process to select 4 verifications.
4. When the required number is displayed press **NO**.

## Changing ID Defaults

1. Select **2-ID / CARD** to set up the id settings. From this menu you can;
  - Change the id number length
  - Activate the display finger number option
  - Activate the display id number option
  - Activate the smart card reader

## Changing the ID Number Length

The default setting for the id number length is 4 digits. This can be changed to any length from 1 to 9. It is recommended that you select the lowest number of digits that will accommodate your present and future needs.

If templates are stored in the unit the length cannot be reduced. If the number of digits is being increased, leading zeros must be added to the existing numbers to make them the new length. The length of the PIN cannot be reduced unless the unit is reset.

1. Select **1-ID#** from the **ID / Card** Menu. The display will show

ID LENGTH = 4
NEW LENGTH = n

2. Press any number from [1] to [9]. Do not press **0** or **CLR**.

The System Menu will be displayed.

### Activating the Display Finger Option

This option determines whether FINGERSCAN will display the name of the finger that is enrolled (for example, the right index) or refer to it as the 1st or 2nd finger. If the option is turned ON, the finger name will be identified on enrolment. The default is **OFF** but it is recommended to turn the option **ON**.

1. Select **2-DFO** from the **ID / Card** Menu. The display will show

Disp finger = OFF
CHANGE Yes/No ?

2. Select **YES** to activate. The display returns to the ID/Card Menu.

### Changing the Display ID Number Option

When activated, this option causes the user's id number to be displayed as it is entered. The default is to display asterisks in place of the number.

This allows a user to check that they have entered the correct number. Where the security threshold has been set low, displaying the user's id number can be a small exposure (displaying the number does not actually change the False Acceptance risk). Displaying the user's number may also tend to slow the verification process if users take time to check their number before placing their finger on the reader.

1. Select **2-DFO** from the **ID/Card** Menu. The display will show

Display ID = OK
CHANGE Yes/No
?

2. Select **YES** to activate. The display returns to the ID/Card Menu.

## ID # Search = Standalone Mode ONLY

As a hidden feature, FINGERSCAN can now search its local database for any unique number and displays “Present Finger” as soon as the unique number is located. For example, if a user’s ID # is 1234 and there are NO OTHER numbers starting 12, then as soon as the 12 is entered, the system go to verification of that number. As another example, the overall ID length might be 6 digits, but the system manager reserves the number 9. Provided no other numbers start with 9, then the verification will proceed immediately 9 is pressed. It should be stressed that this only works in standalone mode. If the required template is not in the local database, then the complete number must be entered. To activate the option:

1. Enter the **DNO** (Display Number Option) from the **SETUP:SYSTEM:ID/CARD** Menu
2. Press **NO**.
3. The display now shows

<p><b>ID SEARCH = OFF</b> <b>CHANGE YES/NO</b></p>
--

Select **YES** to activate the ID Search facility.

## Activating the Card/ Smart Card Reader

If this option is selected, the user will not use the keypad to enter their ID number but will instead insert their card in the card reader. The default setting is card reader **OFF**.

In the case of smart cards, those enrolled as Supervisors or Managers will have their templates written to the FINGERSCAN database as well as to the smart card.

Card-based verifications are treated exactly the same as verifications based on an id number for all local FINGERSCAN functions.

1. Select **4-CARD** from the **ID/Card** Menu. The display will show

<p>Card reader = OFF CHANGE Yes/No ?</p>
--

2. Select **YES** or **NO**, as required.
3. Press CLR to return to the System Menu.

## Setting the Relay

Each FINGERSCAN has a relay which may or may not be in use in your installation. If used, it is important to set the state of the relay as either *normally open* or *normally closed*. The default is *normally open*. It may also be necessary to change the length of time the relay stays open or closed; the default is 4 seconds.

1. Select 3-RELAY from the ID/Card Menu. The display will show

Relay duration  
4s: CHANGE ?

2. Press **YES** to change. The display will show

ENTER RELAY  
DURATION:

3. Press any two numbers from 00 to 20.
4. Press **YES** to confirm, **NO** to return to the default.

The relay state message will be displayed. This is either Normally Open (power on to lock) or Normally Closed (power off to lock). The default is Normally Open.

Relay = N/OPEN  
CHANGE Yes/No ?

Select **YES** to change or **NO** to keep the current value. The display now shows

OUT UNLOCK = OFF  
CHANGE Yes/No  
?

Select **OFF** and the door will not open on an out entry. This could occur, for instance, where the unit is outside and is being used for Time & Attendance. The user may log out without causing the door to unlock. Select **YES** and the relay will be driven by an out entry.

6. The display returns to the previous menu OR if the multi-door option is installed the following message is displayed

AUX DOORS = 0  
CHANGE Yes/No ?

7. The auxiliary door default is **0**. To change the default select **YES** until the number of doors you want to set is displayed (up to 4).

## Changing the Alarm Defaults

Each FINGERSCAN is equipped with four alarm inputs and four alarm outputs as standard. Inputs can be used to generate entries in the transaction log, cause an alarm 'flag' on a computer when the system is part of a network, or activate an output.

Typically, alarm inputs will be used in conjunction with door status switches. For example, a switch on a door might activate each time the door is opened causing an alarm input. In conjunction with the input, an alarm output might be generated if the input stays activated for more than, say, 10 seconds. This would cause an alert if the door is propped open.

The alarm output is used to activate external devices such as local alarms, or telephone diallers to security firms.

The default alarm settings are: when activated, each input is recorded in the transaction log and the corresponding output is activated. The default delay in activating an output is **0** seconds.

To change the alarms defaults:

1. Select **4-ALARMS** from the **ID/Card** Menu. The display will show

1:ALARMS  
2:NO/NC  
3:DOOR SW 4:REX

## Selecting the Input Alarms

1. Select **1- ALARMS** from the **Alarms** Menu. The display will show

1:INPUT ALARMS  
2: VERIFY FAILED

2. Select **1: INPUT ALARMS** to set up the alarm options.

SELECT INPUT  
1,2,3,4 :

3. Select the alarm input to be set [1], [2], [3], or [4].

1:SET DELAY  
2:SET OUTPUTS

4. Select **1-SET DELAY** to set a time delay before the input activates the corresponding output.

INPUT 1 DELAY = 0  
NEW DELAY =

5. Enter the required delay from [00] to [60] seconds. Press **YES**.
6. Select **2- SELECT OUTPUTS** to select the outputs to be activated.

OUTPUT 1 = OFF  
CHANGE Yes/No ?

7. If output 1 is to be activated when input 1 is activated, choose **YES**. Otherwise, choose **NO**. Immediately output 2 will be displayed showing the same message. Repeat the step.

All four outputs may be activated from a single input. To reset alarm outputs at a later stage, follow the steps above.

### Activating an Alarm on Unsuccessful Verification

At verification a user is given three chances to verify after which the message UNSUCCESSFUL is displayed and a VERIFY FAIL entry is made in the transaction log.

The VERIFY FAILED option allows for an alarm output to be activated if a verification attempt is unsuccessful which can be actioned as required.

1. Select **2-VERIFY FAILED**. The display will show

NO V/FAIL OUTPUT  
CHANGE Yes/No ?

2. To activate an output select **YES**.

V/FAIL OUTPUT = 1  
CHANGE Yes/No ?

3. Enter **YES** to change the output number to [2], [3], or [4] or go back to **NO V/FAIL OUTPUT**.

### Changing the *Normally Open* Alarm Default

1. Select **2-NO/NC**. The display will show

INPUT # 1 N/O  
CHANGE Yes/No ?

2. Select **YES** to change to Normally Closed, or **NO** to stay with the default. Repeat for the remaining inputs. When all inputs have been displayed, the outputs are displayed

OUTPUT # 1	N/O
CHANGE	Yes/No ?

3. Repeat the steps as for the inputs.

### Activating a Door Switch Alarm

This option is selected when a door switch is to be used to detect a forced door and a door open too long condition.

FINGERSCAN is used on one side of the door. A Request to Exit (REX) button is on the other side of the door. This button is used to avoid causing an alarm when the door is opened from the non-FINGERSCAN side. The door position is indicated either by the tongue of the electric strike (when an alarmed strike is used), or by a reed switch or other signalling device. An alarm will occur if

- The door is opened by means other than FINGERSCAN or the REX button
- The door is held open for longer than the predetermined time

The alarm will reset once the door has been opened and closed.

1. To select which alarm input will correspond to the door alarm select **2-DOOR SW**.

The display will show

NO DOOR SW INPUT
CHANGE Yes/No ?

2. Select **YES** to change. Select **YES** until the alarm input number you require is displayed. Normally select input 1.
3. To allow for a Request to Exit button to override the forced door alarm select **4-REX**.

NO REX SW INPUT
CHANGE Yes/No ?

4. Select **YES** to step through the input options. Normally select **REX SW INPUT=2**.

NO REX UNLOCK CHANGE Yes/No ?
----------------------------------

5. Select **YES** if the REX is to cause the door to unlock. Select **NO** if the REX is not to unlock the door. For example, if an electric strike is being used with a turning handle on the inside, there is no need for the REX button to cause the strike to unlock. On the other hand, if there is no turning inside handle then it will be necessary to use the REX unlock facility.

## Setting up Communications

FINGERSCAN has three communication ports, any two of which can be used at the same time.

The communications set up facility allows a Supervisor or Manager to access the FINGERSCAN communications facility via the selected communications port.

To gain access to the communications port, or to alter the default communications settings, press **2-COMMS** from the Systems Menu. The default display will show

1:HOST	2:AUX
3:WIEGAND	4:LISTLOG

### Setting up Host Communications

This selection allows FINGERSCAN to communicate with a host, either singly or in a network.

1. Select **1-HOST**. The display will show

Host Baud = 9600
New Speed =

2. Enter the new host communications speed, and press **YES**. This may be either the network communications speed or modem speed. If a modem is used on the normal RS232 port, the modem speed must be entered here. The display now shows

Network Node = 5
New Node =

3. Enter the node number or press **CLR**, and the display shows

Modem Ctrl OFF
CHANGE Yes/No ?

Selecting **YES** immediately changes the state to ON or OFF.

**NOTE:** By setting the modem control to **ON** the Fingerscan will automatically send the modem command “ATZ” to the modem at a regular interval (30 - 50 seconds) to ensure that the modem remains in a ready state to receive the next call. The “ATZ” command is equivalent to a soft reset of the modem.

The next message is displayed

```
Password OFF
CHANGE Yes/No ?
```

Password control can be used on any network, but is generally only required where a modem is used. A centralised software system is required to generate and control the passwords. Unless this is in place, do not activate the password option.

## Setting the Auxiliary Baud Rate

The auxiliary baud rate setting is required when a second comm port is being used. This can be either Rs232 or TTL.

1. Select **2-AUX** from the Communications menu. The display will show

```
Aux Baud = 2400
New Speed =
```

2. Set the speed for the auxiliary (TTL) port.

## Activating the Wiegand Option

If FINGERSCAN is connecting to a Wiegand system, activate the Wiegand option. There are two methods of configuring the Fingerscan for Wiegand operation. One, via the keypad, where limited settings can be made; or two, via the WIEGAND.EXE utility. Refer the **Wiegand Interface User Guide** for full details.

1. Select **3-WIEGAND** from the Communication Menu. The display will show

WIEGAND DISABLED

CHANGE Yes/No ?

2. Select **YES** to enable the option. The display will show

WEIGAND BITS = 20

CHANGE Yes/No ?

3. Continue to select **YES** until the required bit number appears in the screen (after 40 the display returns to WIEGAND DISABLED.) Then select **NO**, and the following message appears

INPUT & OUTPUT

CHANGE Yes/No ?

4. Select **NO** if the Wiegand configuration is to be both input and output or **YES** to select output only.

## Changing the List Log Printing Options

The List Log facility can only be used if the Wiegand option is disabled because it uses the same auxiliary port. If Wiegand is activated the display shows

DISABLE WIEGAND

TO ENABLE LIST

The List Log printing option allows the user to select which transactions are to be printed to the serial port, either all transactions since the last printing, or all transactions after a specified serial number.

1. Select **4-LIST LOG** from the Communications Menu. The display will show

1: LAST BATCH  
2: FROM SERIAL #

2. Select **1** to start printing from the last time printing occurred.

PRINTING:  
Please wait....

3. Select **2** to start printing from a specified serial number.

STARTING SERIAL# =

4. Enter up to 10 digits from the starting serial number and press **YES**. The PRINTING, PLEASE WAIT message will be displayed.

If no printer is connected, or to abort the print run, press **CLR**.

NOTE: that most of the FINGERSCAN software packages and utilities provide for the retrieval of the transactions from FINGERSCAN to a PC.

## Transaction Log and *FINGERSCAN* Messages

The Transaction Log is a record of all activity on the FINGERSCAN system:

- Power on and off
- All verification attempts
- All enrolments
- All access to System Mode and most of the Supervisor and Manager changes
- Alarm inputs

The log maintains at least the last 1000 records. The log is never erased except by a complete system reset. When the log is full it replaces the earliest record with the last record.

Each transaction is approximately 14 bytes long and records the finger number, the transaction result, the transaction audit number, the user id number, and the date and time.

The transaction results are shown in the table on the following page:

## ◆ *FINGERSCAN Messages*

0	Cold Start	Unit turned on
1	Warm Restart	Unit reset, or turned off for a short period
2	Verify OK	Successful verification has occurred
3	Verify Failed	Verification attempt was unsuccessful
4	Invalid Time	An attempted Time Zone violation
5	Invalid ID	The ID# entered is not in the database
6	Host Unavailable	The host computer did not respond to a request
7	IN Entry	A user is indicating he/she is arriving
8	OUT Entry	A user is indicating he/she is leaving
9	BRK Entry	A user is taking a break
10	Authority Denied	No authority
11	Enrol OK	An enrolment recorded
12	Database Denied	Unauthorised access attempt to database
13	Modify Authority	A change in an ID #'s authority
14	Modify Time Zone	A change in an ID #'s Time Zone
15	Modify Threshold	A change in an ID#'s Security Threshold
16	Delete ID	A user is deleted from the FINGERSCAN
17	Modify Security	The Global Security Threshold is changed
18	Modify FF	The Global Security Threshold is changed
19	Modify PIN len	The Global ID# length is changed
20	Modify Solenoid	The relay duration is changed
21	Modify I/O	An alarm setting has been changed
22	Comms Enabled	A supervisor has gained comms access
23	Comms Denied	An invalid attempt to access comms
24	Modify Date	The system date has been changed
25	Modify Time	The system time has been changed
26	Mod Date Format	Change the format of the date presentation
27	Modify Local	The Set Up facility has been disabled
28	Reset Password	The password has been set to default

## Setting up Communications

29	Modify Comms	Any change to the comms set up
30	System Entry	An authorised user has entered System Mode
31	Alarm State	An alarm has been activated
32	Door Too Long	Door held too long
33	Door Forced	The door has been forced open
34	Door Reclosed	The door was opened and is now closed
35	Invalid Access	Not authorised for access to door
36	REX Exit Granted	Rex granted and door opened
37	REX Exit denied	Rex denied
38	Firmware Upgr	Firmware upgraded by download
39	Log Printed	Dump transactions to printer
40	Mod Verifies	Modify number of verifies to unlock
41	Multi Unlock	A chosen door is unlocked
42	Mod Access Doors	Access to multi doors has been changed
43	Enroll cancel	An enrolment has been cancelled/aborted
44	Read Smart Card	A smart card has been read
45	Mod Tzones Table	Modify Global Timezones Table
46	Mod Default Tzone	Modify Default Timezones for New Enrolments
47	Verify Cancelled	Verification Aborted ( "Clear" or "Timed Out")
48	Verify OK (aux # 1)	Multi-Door Option only (Verify Door 2)
49	Verify OK (aux # 2)	Multi-Door Option only (Verify Door 3)
50	Verify OK (aux # 3)	Multi-Door Option only (Verify Door 4)
51	Verify OK (aux # 4)	Multi-Door Option only (Verify Door 5)

## Setting the Clock

1. Select **3-CLOCK** to set the date and time. The display will show the current settings

```
TIME = 17:15:06
THU   24/03/1995
```

2. To leave the settings as they are, press **CLR** within 3 seconds, otherwise the following menu appears

```
1: CHANGE DATE
2: CHANGE TIME
```

3. Select **1** to change the date. The following prompt appears

```
DATE =
(DDMMYYYY)
```

4. Enter the date in the format [ddmmyyyy] (example: 18081995 for the 18th of August 1995).

```
SET DAY OF WEEK
SUN=1 .. SAT=7
```

5. Enter the day number of the current day; Sunday is day **1**.
6. Select **2** to change the time.

```
TIME = (HHMMSS)
```

## Setting the Clock

---

7. Enter the time in the format [hhmmss] (example: 182309 for 23 minutes, 9 seconds past 6pm). The clock is a 24-hour clock.

The Set up Menu will be displayed.

## Setting Time Zones

Time zones control the time during which users can do verifications. Time zones are appended to templates and are part of the individual record. Two time zones can be assigned to each user.

There is no default time zone setting. All users have 24 hour/7 day unrestricted FINGERSCAN use unless the default time zone is changed or a time zone is defined to the user on enrolment.

There are 30 possible time zones, numbered from 1 to 30. These can be set at any start and finish time from midnight to midnight, 7 days per week.

### Setting Specific Time Zones

1. Select **4-ZONES** from the Communications Menu. The display will show

1: EDIT TIMEZONE  
2: ASSIGN DEFAULT

2. To create or modify time zones select **1: EDIT TIMEZONES**.

ENTER ZONE #  
(1..30):

3. Press the time zone numbers, example, **1** for time zone 1. Press **YES**.

#1: CHANGE Y/N ?  
SUN 00:00 23:59

4. The access times for Sunday are displayed. Choose **YES** to change.

#1: ENTER START  
SUN (HHMM)

5. Enter the start time in a 24-hour format, example for 7.30am press[ 0730].

```
#1: ENTER ENT  
SN (HHMM)
```

6. Enter the end time. For no access on the day, enter [0000] to [0001]. For 24 hour access, leave the times as displayed. Press **YES**.

The next day is displayed. This would also be displayed if **NO** had been chosen for Sunday.

```
#1: CHANGE Y/N ?  
MON: 00:00 - 23:59
```

Continue through all of the days of the week.

## Assigning a Default Time Zone

A default time zone can be set which will automatically be assigned to new enrollees. An individual user's time zone can be changed using the LOCAL menu described in the *Database Maintenance* section.

1. Set the time zone as described in the previous section.
2. From the ZONES menu select **2-ASSIGN DEFAULT**. The display will show

```
DEFAULT ZONE = 1  
NEW DFT ZONE =
```

3. Enter the 2-digit time zone number. Press **YES**.

## Deleting a Time Zone

Time zones are not deleted as such but are set to 24-hour access.

1. Use the **1-EDIT TIMEZONE** function to display the time zone you want to delete.
2. When the day is displayed press the **ALT** key.

#2: SUN: ALLOW  
24hr ACCESS Y/N ?

3. Choose **YES** and the next day is now displayed.

Press **CLR** twice to return to the Main Menu.

## Manager Functions

Managers have specific privileges which can effect the overall security of the installation. It is highly recommended that the number of managers on a particular FINGERSCAN be kept to an absolute minimum.

Managers can disable Supervisor access to the Set up Menu and can reset the FINGERSCAN password or clear the entire memory.

1. To select Manager Functions press **4-MGR**. The display will show

1: DISABLE SET UP  
2: RESET

### Disabling Access to the Set up Menu

The default is access enabled. If access is disabled set up functions will only be available from a PC connected to the FINGERSCAN serial port. Once disabled, the only set up option available from the FINGERSCAN unit is **2-COMMS**. This means that system Supervisors cannot change the current defaults.

1. Select **1- DISABLE SET UP**. The display will show

LOCAL SET UP: ON  
CHANGE Yes/No ?

(or LOCAL SET UP: OFF)

2. Select **YES** to disable or **NO** to return to the previous menu.

### Resetting the System

This option allows the system password to be reset or the transaction log, or template database to be erased.

1. Select **2-RESET**. The display will show

1:RESET PASSWORD  
2:RESET SYSTEM

2. To reset the password select **1-RESET PASSWORD**. The display will show

RESET PASSWORD  
Yes/No ?

3. Select **YES** to reset the password to DEFAULT.
4. To reset the system select **2-RESET SYSTEM**.

ERASE ALL DATA  
Yes/No ?

5. Select **YES** to clear the memory. The display will show

ERASING...

followed by

POWER DOWN OR  
[YES] TO RESTART

The FINGERSCAN unit will now restart as a new unit.

## Maintaining the Local Database

This facility allows a Supervisor or Manager to make changes to the records contained in the FINGERSCAN database. Records can be altered, deleted, or listed by a Supervisor or Manager.

To carry out database maintenance, from the Main Menu select

2-LOCAL

### Searching for a Specific ID Number

1. Select **2 - LOCAL** from the Main Menu. The display will show

Enter ID (ALT=\*)

(Alt=\*) indicates you can press **ALT** on the keypad to display an asterisk (\*) in place of any id digit, if you are not sure of the exact id number you require.

#### Example

To search for a four digit id number where you know the first three digits are 999, enter [999\*]. The system will display all numbers in the database from 9990 to 9999 in the order that they were enrolled.

OR

To search for an id number starting with 6 and ending in 89, enter [6\*89].

To search the entire database enter an [\*] for every digit in the id number if you know how many digits are in the numbers. If you do not know how many digits make up the user id number enter [\*] until the display changes.

Once the selected user id numbers have been displayed, the following message appears

No more matching records

## Modifying a Single Database Entry

1. Enter the user ID number you want to modify. The display will show

```
ID No.  nnnn
Finger 1  Accept ?
```

where nnnn is the entered ID number or the first number in a database search, and the finger number indicates whether this is the primary or alternate finger.

If the number is not correct press **NO**, and the next finger or ID number will be displayed.

If correct, press **YES** and the Modify Menu will be displayed:

```
1:AUTH  2:T/ZONE
3:SEC   4:DELETE
```

You can now perform the following database maintenance activities.

2. To exit from the Modify Menu when you have finished updating the database:

Press **CLR** to return to the **LOCAL** menu. Press **CLR** again to return to the **Main** Menu.

## Changing a User's Authority Level

1. Select **1-AUTH** from the Modify Menu. The display will show

```
AUTH =  xxxx
Accept  Yes/No ?
```

where xxxx is the current authority (User, Enroller, Supervisor or Manager). Pressing **NO** will display the next authority level.

Press **YES** when the level you require is displayed.

The Modify Menu, or the next id number, will be displayed.

**NOTE:** It is not possible to assign a higher authority level than that of the person who accessed the main menu.

## Changing a User's Time Zone

Time zones are blocks of time during which a user can have their identity verified. Each user ID can be assigned two time zones; up to 30 time zones can be defined in FINGERSCAN. If the user attempts a verification outside of their time zone they will not be granted access and a time zone violation entry will be added to the transaction log.

To change a user's time zone:

1. Select **2-T/ZONE** from the **Modify** Menu. If the multi-door option is in use select **2-ACCESS** and then **1-TIME ZONE** from the displayed submenu. The display will show

TIMEZONE 1 = nn  
CHANGE Yes/No ?

where nn is the current time zone or is blank representing no time zone.

2. To accept the current time zone press **NO**.
3. To change the time zone press **YES**.

ENTER NEW  
TIMEZONE:

4. Enter the required time zone number, from [1] to [30]. This number will overwrite "nn". If an invalid number is entered the original time zone will remain unchanged.
5. Press **YES** to confirm.

TIMEZONE 2 = nn  
CHANGE Yes/No ?

6. To accept the time zone change press **NO** or repeat from step 3.

The Modify Menu or the next id number will be displayed.

## Changing a User's Verification Threshold

At enrolment, each template is assigned a default verification threshold value. This value ranges from 000 to 200 and is used to determine the degree of security used during verification.

To change a user's verification threshold:

1. Select **3-SEC** from the Modify Menu. The display will show

THRESHOLD = nn  
CHANGE Yes/No ?

where nnn is the current security threshold value.

2. Press **YES**.

ENTER NEW  
THRESHOLD

3. Enter a 3-digit number between [000] and [200], where 000 is no security and 200 is maximum security. This will be displayed in place of "nnn".
4. Press **YES** to record the change and the **Modify** Menu or the next user ID will be displayed.

## Changing the False Finger Threshold on an Individual Basis.

It is now possible to alter the False Finger Threshold from the Local Menu, on a user by user basis. Previous to Firmware Version 1.6x, the False Finger threshold was set at enrolment and could only be changed by re-enrolling the user. To use,

1. In the Local Menu as above, enter the user's ID #, and
2. Select **3-SEC** from the Modify menu.
3. Change the Security Threshold or select '**NO**' .
4. The following message is displayed:

```
FF THRESHOLD =nn
CHANGE YES/NO?
```

Enter the required value and press **YES**.

## Changing a User's Door Access

This function is available if the multi-door option is installed, and is used to change the doors which a user can be verified against to gain entry.

1. Select **2-ACCESS** from the **Modify** Menu and **2-DOORS** from the displayed submenu.

```
DOORS =    nn
CHANGE Yes/No ?
```

2. Press **YES** to change.

```
ENTER DOORS
FOR ACCESS: nnnn
```

3. Enter the door number(s) and press **YES**.

### Deleting a User's Template

- **WARNING !!!!**
- **PROCEED WITH CAUTION**
- **THERE IS NO SECOND CHANCE ON THIS MENU.**

When you select DELETE, the template of the currently selected user id number will be deleted **immediately!**

1. To delete the currently selected user id number select **4-DELETE** from the Modify Menu. The display will show

**\*\*DELETED\*\***

NOTE: A Manager cannot delete his or her own user ID number. A manager can only be deleted by another Manager.

## Troubleshooting

Symptom	Probable cause	Solution
<b>NO DISPLAY</b>	1. No power	Check power supply/ connection
	2. Loose Cable	Seat cables correctly
	3. Faulty Program Chip	Replace program chip (see Note 2)
	4. Faulty Memory Chip	Replace memory chip (see Note 2)
	5. Defective LCD	Change LCD (Note1)
	6. Defective Main PCB	Change PCB (Note1)
	7. Defective Interface PCB	Change interface PCB (Note1)
<b>HIEROGLYPHICS ON KEYPAD</b>	1. Excessive static electricity	Ensure FINGERSCAN is well grounded
	2. Defective LCD	Change LCD (Note 1)
	3. Defective Main PCB	Change PCB (Note 1)
<b>NO KEYPAD</b>	1. Loose cable	Seat keypad cable correctly
	2. Defective Keypad	Change keypad (Note1)
	3. Defective Main PCB	Change main PCB(Note1)
	4. Defective Interface PCB	Change interface PCB(Note1)
<b>MISSING LINE ON KEYPAD</b>	1. Loose cable	Seat keypad cable correctly
	2. Defective keypad	Change keypad (Note1)
<b>FIP MEMORY TEST (LOCKED IN THIS STATE)</b>	1. Defective memory/program chips.	Replace
	2. Defective main PCB	Replace (Note 1)
<b>FIP RESET TEST</b>	1. Loose cable/s	Seat cables correctly, especially optics/interface card cable
<b>FIP RESET ERROR #</b>	2. Defective Sensor	Replace sensor (Note1)
	3. Defective Main PCB	Change PCB (Note1)
	4. Defective Interface PCB	Change Interface PCB(Note1)
<b>SENSOR IMMEDIATELY "FIRES" ON ENTERING ID#, BEFORE A FINGER IS PLACED ON PLATEN</b>	1. Defective sensor	Replace sensor (Note1)
	2. Defective Main PCB	Replace PCB (Note1)

Symptom	Probable cause	Solution
<b>SENSOR FAILS TO 'FIRE' ONCE A FINGER IS PRESENTED</b>	1. User is not pressing firmly enough, or needs re-enrolling	Educate or re-enrol user
	2. Environment is very dry or cold	Apply grease to the finger.
	3. Defective sensor	Replace sensor (Note1)
	4. Defective Main PCB	Replace PCB (Note1)
<b>USERS REPORT EXCESSIVE FAILURES TO VERIFY</b>	1. User difficulty	Educate or re-enrol user/s
	2. Security set too high	Lower individual security setting (Section 6)
	3. Damaged / worn platen	If the platen is clearly damaged or stained with dirt change the platen. (Note1)
	4. Sensor out of alignment	If problem is universal among users, change sensor (Note1)
<b>ALARM INPUTS/OUTPUTS NOT WORKING</b>	1. Incorrectly wired	Check wiring
<b>LOCK NOT WORKING</b>	1. Incorrectly wired or configured	Check wiring
<b>'LOST: MEMORY CAPACITY</b>	1. FINGERSCAN Memory manager is busy	Leave FINGERSCAN idle for several minutes.
	2. Defective chip socket or chip pins	Inspect chip pins and socket Ensure chip is well seated in the socket
	3. Defective Memory chip	Replace with new chip. (Note1)
<b>AT STARTUP, DISPLAY SHOWS CORRUPT MEMORY RECOVERING...</b>	The system has found some corrupt memory sectors.	Do nothing. The system will sort itself out.
<b>AFTER CHANGING MEMORY CHIPS: INVALID SERIAL NUMBER: HALTED</b>	The system has found chips with different serial numbers.	See Note 2.

**NOTE 1:** This data is given for information rather than for an indication of work to be performed in the field. It should be performed by Fujitsu Australia or its Authorised Service Agents. Unauthorised work could result in the voiding of the warranty.

**NOTE 2:** FINGERSCANs are equipped with a Program chip (U13) and one or more Memory chips (U11, 12 and 14). At the time of manufacture, each FINGERSCAN is given an Electronic Serial Number (ESN) which is factory assigned. All of the chips carry this number. Unless the program chip 'sees' the correct ESN at start up, the program will not start and displays a message indicating that the serial numbers are incompatible. This means that Memory chips cannot be reused or swapped between FINGERSCANs. However, it can happen that Memory or Program chips become corrupted or defective for one reason or another. In addition, it can be necessary to regain the information of a defective chip. In most cases, using firmware version 1.5 or above, if the defective chip is a Memory chip, the Program chip will remedy the defect and loss of performance will be noted.

However, to resolve defective chips, proceed as follows.

First, ensure that the problem *is* a defective chip and *not* a problem with the socket, chip seating etc. This can be accomplished by removing the Program and Memory chips and very carefully ease out the socket strings with a jewellers screw driver. Then replace the chips ensuring that they are firmly seated. If a Memory chip, replace it with a brand new blank memory chip. The FINGERSCAN will now boot up, allocating to the blank chip the correct ESN. If the defective chip is a Program chip, it will be necessary to get a new memory chip from your FINGERSCAN supplier with NO serial number assigned.

## Cleaning and Maintenance

From time to time, the Optical Platen, the Keypad and Display Window will require cleaning. As working environments differ, it is not possible to dictate when cleaning should be performed but the following is a guide:

- |    |                                  |   |
|----|----------------------------------|---|
| a) | <i>Keypad and Display Window</i> | Clean when visibly dirty and hard to read.  |
| b) | <i>Optical Platen</i>            | DO NOT OVERCLEAN. The platen is designed to work under greasy or dirty conditions. However, do clean if the platen is obstructed or people are reporting deteriorating performance. |

### *Cleaning the Optical Platen:*

1. If dusty or gritty, first blow on the platen to clean off any loose particles.
2. Spray on a light coating of a window cleaning product or other similar neutral detergent. DO NOT USE ANY OTHER TYPE OF CLEANER OR THE PLATEN MAY BECOME DAMAGED.
3. Using a NON ABRASIVE and NON LINTING cloth, pat dry. Be careful not to scratch the platen. You may still get a few lint particles adhering to the platen surface. Just blow off when dry.

### *Cleaning the Keypad and Display:*

Use the same cleaning products as for the platen and wipe dry.

### *Maintenance:*

The following checks should be performed every month or every 1000 operations, whichever is the later:

- a) Is the electrical plug pack firmly plugged in to the wall socket?
- b) Does the FINGERSCAN look as though it has been damaged? Inspect the Coated Optical Platen in particular, and, if obviously damaged, replace it.
- c) Perform a verification cycle. If the FINGERSCAN operates some other device (such as a door), make sure that it works as well (if a door, it should unlock and open).
- d) Perform an enrolment. (if this is just a check, remember to delete it once you have ascertained that the system performed as required.)
- e) **Make sure you have taken a BACKUP diskette of all templates.**

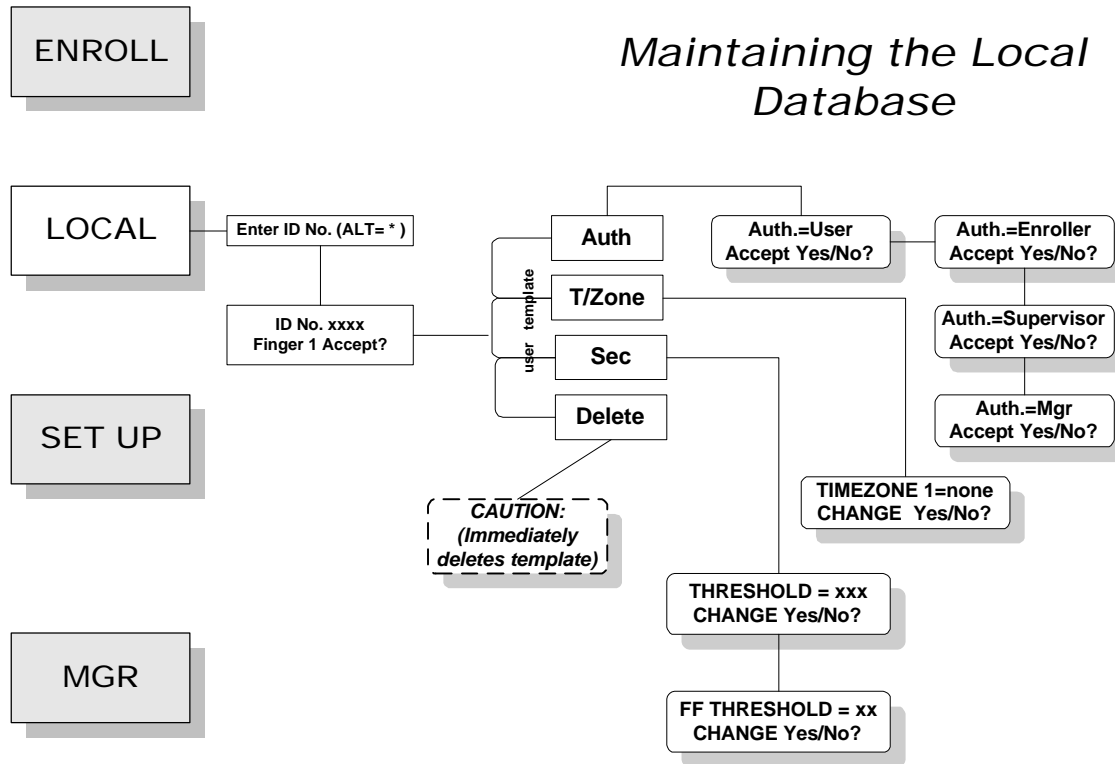
## **Menu Trees**

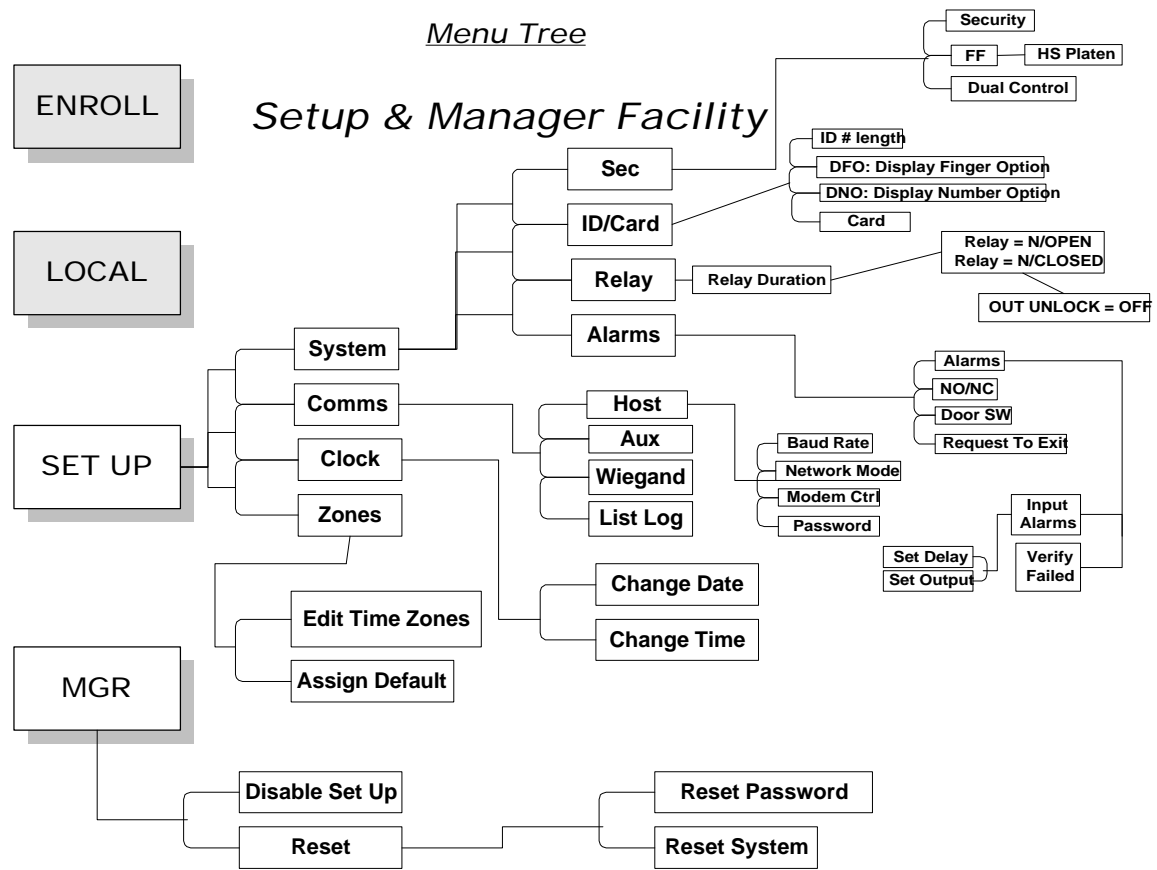
Maintaining the Local Database

Setup & Manager's Facility

Menu Tree

# Maintaining the Local Database





# Index

## 1

1- DISABLE SET UP, 34  
 1-RESET PASSWORD, 35  
**1-SET DELAY.** *See Changing the alarm defaults*  
 1st finger. *See Display Finger Option*

## 2

**2- SELECT OUTPUTS.** *See Changing the alarm defaults*  
**2-AUX,** 24  
**2-COMMS,** 34  
**2-DFO.** *See Display Finger Option*  
**2-ID / CARD,** 14  
**2-LOCAL,** 36  
 2nd finger. *See Display Finger Option*  
**2-NO/NC.,** 20  
**2-RESET.** *See Resetting the system*  
**2-VERIFY FAILED.** *See Activating an alarm on unsuccessful verification*

## 3

**3-CLOCK,** 29  
 3-dimensional image, 6  
**3-RELAY.** *See Setting the relay*  
**3-SET UP,** 9

## 4

**4-ALARMS,** 18. *See Changing alarm defaults*  
**4-CARD,** 16  
**4-LIST LOG,** 25  
**4-MGR,** 34  
**4-REX.** *See Activating an alarm on unsuccessful verification*  
**4-ZONES,** 31

## A

access times, 31  
 accessed, 38  
 Activating a Door Switch Alarm, 21  
 Activating the Display Finger Option, 15  
 Activating the Wiegand Option, 24  
 active time zones, 7. *See Time-Zones. See Time-Zones*  
 alarm codes, 6  
 alarm 'flag', 18  
 alarm inputs, 18, 43  
 alarm inputs and outputs, 7  
 Alarm on Unsuccessful Verification, 20  
 alarm outputs, 18, 43  
 alarm settings - settings, 18  
 Alarm State, 28  
**Alarms,** 9  
 Fingerscan Supervisor & Manager Guide

Alarms Menu, 19  
 alarms., 9  
 all transactions, 25  
 altered, 36  
 alternate finger, 37  
 alternate fingers, 6  
 AUTH, 37  
 Authority, 6  
 Authority Denied, 27  
 authority level, 5  
 AUX DOORS, 18  
 auxiliary baud rate - setting, 24  
 auxiliary door, 18

## B

balance between FAR & FRR, 10  
 bank vault doors, 10  
 barcode, 5  
 brand new, 9  
 BRK Entry, 27

## C

Card / Smart Card Reader, 16  
 Card-based verifications, 16  
 centralised software system, 24  
 CHANGE DATE, 29  
 change the setup, 6  
 Changing ID Defaults, 14  
**CHANGING MEMORY CHIPS,** 43  
 Changing Security Defaults, 10  
 Changing the Alarm, 18  
 Changing the ID Number Length, 14  
 Changing the List Log Printing, 25  
 Changing the *Normally Open* Alarm Default, 20  
 characteristics, 6  
 Cleaning, 45  
 clear memory, 35  
**CLR,** 33  
 Cold Start, 27  
 Commercial / industrial security, 10  
 Comms Denied, 27  
*communication ports.* *See Setting up communications*  
 communications facility. *See Setting up communications*  
 Communications menu, 24  
 complete memory reset, 7  
 control the passwords, 24  
 correct balance, 6  
 correct number. *See Display ID number*  
**CORRUPT MEMORY,** 43  
 current security threshold, 39  
 customise, 5

## D

Database Denied, 27  
 database maintenance activities, 37

## Index

---

date and time, 7  
default communications settings, 23  
default delay, 18  
default enrolment values, 7  
default output values, 7  
default time zone, 31. *See* Time-Zones  
defaults, 9  
defective chip, 44  
defined, 38  
Delete ID, 27  
deleted, 36  
Deleting, 41  
disable, 6  
disable functions, 9  
Disabling Access, 34  
display finger number option, 14  
Display Finger Option - activating. *See* activating  
    display finger option  
Display ID Number, 15  
door - open, 18  
door - opened. *See* Changing alarm defaults  
door - propped open. *See* Changing the alarm  
    defaults  
door - unlock, 18  
Door Access, 40  
Door Forced, 28  
door open too long, 21  
Door Reclosed, 28  
Door Too Long, 28  
doors - numbers, 18

### E

EDIT TIMEZONES, 31  
electric strike, 21  
empty unit, 9  
Enrol OK, 27  
Enroll cancel, 28  
enrolled finger, 15  
**Enroller**, 6  
ERASING, 35  
ESN. *See* Electronic serial number  
**EXCESSIVE FAILURES TO VERIFY**, 43  
external devices, 18

### F

factory, 10  
factory default setting, 12  
factory default settings., 9  
fake finger, 12  
False Acceptance, 10  
False Acceptance rate, 10  
False Acceptance Risk, 15  
false finger, 10  
False Finger Threshold, 40  
False Finger Default, 12  
false finger reading, 10  
False Rejection, 10  
FAR - low, 10  
finger type, 5  
finger -fake, 12  
finger image record, 5, 6  
finger -live, 12  
Fingerscan Supervisor & Manager Guide

finger name. *See* Display Finger Option  
finger number, 26  
*FINGERSCAN Messages*, 27  
*FINGERSCAN software packages*, 26  
finish time, 31  
**FIP MEMORY TEST**, 42  
**FIP RESET ERROR**, 42  
**FIP RESET TEST**, 42  
firmware, 44  
Firmware Upgr, 28  
Firmware Version, 40  
first enrolment, 5  
forced door, 21  
four digit id, 36  
fully reset, 9

### G

gain entry, 40  
global or individual time zones, 7. *See* Time-Zones

### H

Heavy throughput / low security, 10  
Heavy throughput/extremely low security, 12  
hidden feature, 16  
**HIEROGLYPHICS ON KEYPAD**, 42  
high security, 10, 12  
High Security Platen. *See* HS platen  
high throughput, 10  
higher authority level, 38  
higher False Finger level, 12  
Host Baud, 23  
host communications speed, 23  
Host Unavailable, 27  
HS platen, 10, 12, 13. *See* High Security Platen  
HS Platen default, 13  
HS Platen default - changing, 13  
HS platen reading, 10

### I

ID # Search, 16  
ID / Card Menu. *See* Display Finger Option  
ID Defaults, 14  
ID length, 16  
id number, 5, 16, 39  
ID Number Length, 14  
id number length - default setting, 14  
**ID settings**, 9, 14  
ID/Card Menu, 15  
IN Entry, 27  
information centres, 10  
Input Alarms, 19  
installation, 10  
installation.. *See* Setting the relay  
Invalid Access, 28  
Invalid ID, 27  
**INVALID SERIAL NUMBER**, 43  
Invalid Time, 27  
irrefutable audit trail, 10

**K**

keypad, 5, 45

**L**

laptop, 7  
 last 1000 records, 26  
 leading zeros, 14  
 length of the PIN, 14  
 length of time. *See* Setting the relay  
 List Log facility, 25  
 live finger, 12  
 live or fake finger, 12  
 local alarms, 18  
 local database, 6, 16  
 LOCAL MENU, 10  
 LOCAL SET UP, 34  
**LOCK NOT WORKING**, 43  
 Log Printed, 28  
**LOST MEMORY CAPACITY**, 43  
 low False Rejection rate. *See* FRR  
 Low throughput/high security, 12

**M**

Main Menu, 9, 33  
 Maintenance, 45  
 Management Control, 6  
 manager, 5, 6, 9, 41  
 Manager Functions, 34  
 Manager's functions, 7  
 managerial access, 5  
 maximum security., 39  
 Medium throughput/normal security, 12  
 Memory chips, 44  
 memory reset, 7  
 memory test, 13  
**MISSING LINE ON KEYPAD**, 42  
 Mod Access Doors, 28  
 Mod Date Format, 27  
 Mod Default Tzone, 28  
 Mod Tzones Table, 28  
 Mod Verifies, 28  
 modem speed, 23  
 Modify Authority, 27  
 Modify Comms, 28  
 Modify Date, 27  
 Modify FF, 27  
 Modify I/O, 27  
 Modify Local, 27  
 Modify Menu, 37, 39  
 Modify PIN len, 27  
 Modify Security, 27  
 Modify Solenoid, 27  
 Modify Time, 27  
 Modify Time Zone, 27  
 Modifying, 37  
 Modifying Single Database Entry, 37  
 Multi Unlock, 28  
 multi-door option, 18, 40

**N**

network, 18  
 Network Node, 23  
 network communications, 23  
 new (or empty) unit, 9  
 new enrollee, 10  
 new enrollee's, 7  
**NO DISPLAY**, 42  
**NO** for default. *See* Setting the relay  
**NO KEYPAD**, 42  
 No more matching Records, 36  
 no security, 39  
 no templates, 9  
**NO V/FAIL OUTPUT**. *See* Activating an alarm on  
     unsuccessful verification  
*normally closed*, 21. *See* Setting the relay  
*normally open*. *See* Setting the relay  
 number of verifications, 10, 14

**O**

open safe, 14  
 operational., 5  
 Optical Lens, 45  
 OUT Entry, 27  
 overall security threshold, 10  
 overwrite, 38

**P**

Password control, 24  
 password option, 24  
 PC, 7  
 PC., 6  
 PIN, 14  
**POWER DOWN**, 35  
 Present Finger, 16  
 preset default settings, 7  
**press CLR**, 29  
 previous menu, 18  
 primary finger, 37  
 privileges, 34  
 Program chip, 44

**R**

Read Smart Card, 28  
 Recommended Security Threshold settings, 10  
 Records, 36  
 relay, 7. *See* Setting the relay  
 Relay - Setting the., *See* Setting the relay  
 Relay duration. *See* Setting the relay  
 Relay, state of. *See* Setting the relay  
 relays, 9  
 Request to Exit (REX), 21  
 reset, 9  
 Reset Password, 28, 34  
 resetting the password, 7  
 Resetting the System, 34  
 restart, 35

## Index

---

REX. *See* Activating an alarm on unsuccessful verification  
REX Exit denied, 28  
REX Exit Granted, 28  
Rs232 or TTL, 24  
RS232 port, 23

### S

search database, 36  
Searching, 36  
second comm port, 24  
security, 6, 39  
security - high, 10  
SECURITY LEVEL, 11  
Security Defaults, 10  
**Security settings**, 9, 10  
security threshold, 5, 6, 10, 15  
security threshold default, 10  
**SENSOR**, 42  
serial numbers, 44  
serial port, 25  
set up actions, 5  
Set Up facility, 7  
set up functions, 9  
Set up Menu, 34  
Setting Specific Time Zones, 31  
Setting the Auxiliary Baud Rate, 24  
Setting the Clock, 29  
Setting the Relay, 17  
Setting Time Zones, 31  
Setting up Communications, 23  
Setting up Host Communications, 23  
signaling device, 21  
Sites, 10  
Smart Card, 16  
smart card reader, 14, 16  
**Smart Card settings**, 9  
socket strings, 44  
Specific ID Number, 36  
Standalone Mode. *See* I/d # Standalone Mode  
start time. *See*  
STARTING SERIAL #, 26  
state of the relay, 17  
submenu, 38  
**Supervisor**, 6, 9  
Supervisor access, 34  
system set up, 5  
system communications, 7  
system default, 9  
System Entry, 28  
system manager, 16  
System Mode, 26  
system reset, 26  
system reset,, 6

### T

**T/ZONE**, 38  
telephone diallers (to security firms), 18  
template, 5  
template database, 5  
templates, 9  
three digits, 36

Fingerscan Supervisor & Manager Guide

throughput, 6  
throughput - high, 10  
time & attendance, 10, 18  
Time blocks, 38  
time delay. *See* Changing the Alarm Defaults  
time periods, 7  
time zone violation, 38  
time zones, 5, 7, 38  
Time-zone, current, 38  
Time-zones, Changing, 38  
Top secret security, 12  
transaction audit number, 26  
transaction log, 7, 18, 26, 38  
transaction result, 26  
transaction results, 26  
Troubleshooting, 42  
Two time zones, 31

### U

unique number, 16  
updating database, 37  
**User**, 6  
user id database, 5  
user id number, 26  
user's authority, 5  
user's id, 15  
user's id number, 15

### V

variable threshold, 10  
verification, 15, 16, 38  
verification thresholds,, 9  
verification process, 15  
Verification Threshold, 39  
Verification threshold, default, 39  
verifications, 10, 14  
Verifications - number of, 14  
Verify Cancelled, 28  
Verify Failed, 27  
Verify OK, 27, 28

### W

Warm Restart, 27  
WEIGAND BITS, 25  
Wiegand, 24  
Wiegand card, 5  
Wiegand configuration, 25  
WIEGAND DISABLED, 25  
Wiegand option, 24  
Wiegand system, 24  
working environments, 45

### Y

**YES** to confirm. *See* Setting the relay

