FINGERSCAN™

Fingerscan Technical 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

STYLE CONVENTIONS

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

Contents

Introduction

Hardware overview

Sensor Module

- **Optics Assembly**

  This contains the sensor platen, and circuitry required to scan and digitise a person's finger. The optical system is activated by the entry of a valid ID number at the keypad, presentation of a card or activated by a PC. As the finger is placed on the platen, the scan is taken. There are no mechanical switches to trigger the scan.

- **Keypad**

  The keypad is a 16-key membrane that features numbers 0 to 9 and six function keys.

- **Display**

  The standard display is a 16 character, 2 line liquid crystal display with back lighting. Messages are brief and concise.

Processor Module

The processor board contains the Finger Image Processor (FIP), Motorola processor, plug-in non-volatile flash memory (expandable from 512Kbytes to 1.5Mbytes) for template storage, transaction log storage, door access list and time zones storage, RS232 and RS422/485 communications ports, TTL auxiliary port communications, a single solid state relay, four inputs and outputs, an auxiliary 12 volt dc reference voltage output and the necessary circuitry.

- Power Pack

  The power pack is a 12Volt AC 1 amp power pack with plug in connector. Alternatively a 24Volt DC power supply may be used for battery backup. The power requirement does not exceed 16 watts.

  Note that the unit cannot be run on 12Volts DC power.

Networking

FINGERSCAN has three communications ports, any two of which, a host and an auxiliary port, may be used at the same time. The host port can be selected for RS232 or RS422 / 485 and the auxiliary for RS232 (if the host port is RS422 / 485), or TTL interface. Full descriptions of recommended network procedures are given in this section.

- **RS232 Port**

  This allows the following communications:

  - Direct connection to a personal computer, laptop or printer
  - Connection via modem to a remote or regional host computer

- **RS422 / 485 Port**

  This is used when the FINGERSCAN units are networked over a multi-drop 4-wire LAN type system. The communications software runs on a PC through an RS232/485 converter which is externally mounted to the PC.

- **Auxiliary TTL Port**

  This may be used for any peripheral device such as a smart card sensor, a barcode wand, Wiegand, or a magnetic stripe sensor.

Modem Operation

Software is available to enable a FINGERSCAN unit to be accessed by a dial-up modem from the host computer either manually or at pre-set times. This will allow for templates to be uploaded and downloaded, the transaction log to be extracted, door access lists and user access time zones to be modified, and so on.

Diagnostics

On start up, FINGERSCAN performs a self test. Errors are detected and reported.

Networking diagnostic tools are a function of FINGERSCAN, showing the installer the condition of the network and where to look for faults. This is often used in conjunction with the FINGERSCAN software utility, FS_HOST, which polls the network and provides detailed information about the status of any FINGERSCAN polled.

Optional interfaces

Various set up choices are available and these are described in the relevant parts of Sections 2 and 3. In addition, the following options are currently available:

- Multi-door
- Wiegand card interface
- Standard smart card interfaces
- Proximity smart card interface
- Barcode System 39 interface
- Generic magnetic stripe card interface

Multi Door

This option allows one FINGERSCAN to be used for up to five different purposes by different users. For example, the FINGERSCAN could be used to open two different doors, activate or deactivate the alarm system, the lights and the air-conditioning. Different users could have different authorities to perform these tasks.

Wiegand Interface

Wiegand is a particular type of access control card. FINGERSCAN can be configured as a Wiegand sensor for output only, or can be used in conjunction with a Wiegand reader to receive Wigan input as well. The Wiegand output sends a Wiegand-format string to an external system on successful verification, just like a normal Wiegand sensor. The Wiegand input will accept a Wiegand-format string from a card sensor so that the user does not need to enter an ID number. The FINGERSCAN keypad can also be used to enter ID numbers as normal. Supervisor and Manager functions must be carried out using the FINGERSCAN keypad.

Smart Card Interfaces

A smart card is a credit card sized card with a computer chip imbedded in it. The memory in this chip can be used to store a user's template. In this way, the template travels with the user and can be used to verify that the holder of the card is the authorised user. In standard smart cards, such as Gemplus or G&D, a user inserts the smart card into the reader, the template is read from the chip and the user then performs a verification on FINGERSCAN in the normal way. In the proximity smart card, the essential difference is that the smart card does not have to be inserted in a reader but can be placed near to the FINGERSCAN reader.

BarCode Interface

Barcode is an inexpensive means of providing cards which users can use instead of entering their ID number on the keypad., which makes the verification process slightly faster. In this case, the ID number is carried in the card. Simply swipe the card and then place the finger for a verification. The protocol used by FINGERSCAN is 'system 39', an internationally accepted standard for barcode. Suitable barcode readers should be available in most localities. A different application is the use of barcode wands with FINGERSCAN to correlate barcode usage with a particular user. In this application, the barcode wand is interfaced via the TTL port.

Magnetic Stripe

Fingerscan can read an ID number from any device or system that outputs ASCII characters in serial format and can also pass on the entire received ASCII string (not just the ID number) in the event of a successful verification. A person's ID number is read from the ASCIII device (such as a keypad or magnetic swipe reader) instead of entering the ID number on the Fingerscan keypad.

Installation

Installing the Integral Unit

1. Remove FINGERSCAN from the packaging. Undo the bottom mounting screws and remove the bottom cover plate. Slide the anodised rear mounting plate from its sleeve in the main extrusion.

   The rear mounting plate has been pre-drilled with both screw fixing positions and two cable cut-outs.

   When deciding where to mount the unit, it is essential that it is mounted at a convenient height. This is normally about 1100mm (43 inches) above floor level.

1. FINGERSCAN is designed to be mounted so that the users can place their fingers on the platen with the arm approximately at right angles to the body. This is normally about 1100mm (43 inches) above floor level. This will be the top mark for the rear mounting plate. Make sure there is a clear and unobstructed surface of wall above the mark as it will be necessary to slide the main extrusion down over the rear mounting plate.

2. Using the appropriate holes in the rear mounting plate, fix it firmly to the wall. Make sure the plate is level.

3. You may need any of the following cables:

   - 12V AC 1 amp power cable
   - Lock wires (usually figure-8 bell wire or similar) or alarm cables
   - 24V DC battery back-up cable
   - RS485 cable (usually 4-core with foil shield and earth/ground) or
   - RS232 cable

4. If the cables are being run back through the wall (this is the usual method) drill or remove the wall in the area of the cut-outs in the rear mounting plate. Be very careful not to drill below the level of the plate as this will be visible when you mount FINGERSCAN.

5. Route the various cables through the wall so that approximately 200mm (8 inches) of cable is exposed.

6. Holding FINGERSCAN face down, fit the wiring to the circuit board according to the instructions below. The circuit board itself is also marked.

7. Each terminal is numbered. Terminal #1 on the 12 way strip is to the centre of the board. Refer to the diagram on page 11.

8. Slide the FINGERSCAN down over the rear mounting plate and secure the bottom cover plate.

Installing the Modular Units

1. Remove FINGERSCAN from the packaging. There are two modules: the sensor and the processor, and a 3-metre round-and-flat cable. Typically the sensor is mounted on the non-secure side and the processor in the ceiling space on the secure side.

2. On the sensor module, undo the bottom mounting screws and remove the bottom cover plate. Slide the anodised rear mounting plate from its sleeve in the main extrusion. It is essential to mount the unit at a convenient height. This is normally 1100mm (43 inches) above floor level.

3. FINGERSCAN is designed to be mounted so that the users can place their fingers on the platen with the arm approximately at right angles to the body. This is normally about 1100mm (43 inches) above floor level. This will be the top mark for the rear mounting plate. Make sure there is a clear and unobstructed surface of wall above the mark as it will be necessary to slide the main extrusion down over the rear mounting plate.

4. The rear mounting plate will be pre-drilled to accommodate the Sensor/Processor 3-metre round-and-flat cable. Drill through the wall in the exact position of the hole. Make sure that the hole is large enough to accommodate the cable end, while at the same time not so large as to effect the necessary screw mounting positions, nor to be visible after the sensor has been mounted.

5. Run the 3-metre cable down the wall cavity and out through the hole, so that approximately 200mm is exposed.

6. Drill the appropriate sized holes in the wall for the fasteners being used and fix the rear mounting plate firmly to the wall. Make sure that the mounting plate is level.

7. Connect the cable to the vacant connector on the interface circuit board. Note that the connector is polarised and can only be fitted in one direction. Make sure that the connector is well seated.

   IMPORTANT: Make sure that the cable fits down the side of the sensor and does not rest against the sensor circuit board. Make sure that the exposed ribbon cable cannot be cut by any sharp edges.

8. Fit the sensor to the wall.

9. Position the processor module as required (usually in the ceiling cavity), remove the cover and fit the other end of the 3-metre cable to the 30 way connector on the top of the processor.

10. Fit the wiring to the circuit board according to the instructions below. The circuit board itself is also marked. Each terminal is numbered. Terminal #1 on the 12 way strip is to the left of the terminal strip.

Refer to the diagram on the next page.

12 WAY TERMINAL STRIP											4 WAY STRIP			
1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4
ALARM OUTPUTS				DC	ALARM INPUTS				GND	LOCK		AC		DC	
01	02	03	04	12v	11	12	13	14				12v		24v	0v

Wiring Details

12 Way Terminal Strip	
1	Alarm output 1
2	Alarm output 2
3	Alarm output 3
4	Alarm output 4
5	Auxiliary 12V DC output
6	Alarm input 1
7	Alarm input 2
8	Alarm input 3
9	Alarm input 4
10	Ground
11	0V DC (positive terminal)
12	12V DC 1 amp output[1] (negative terminal)
4 Way Terminal Strip	
1 and 2	12 V AC power input[1]
3	24V DC battery back-up[1]
4	0V DC

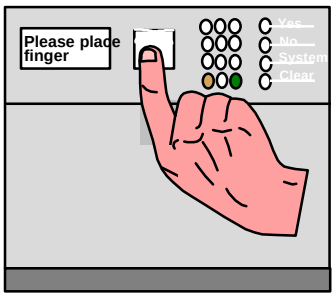
NOTE:

1 Lock Wiring

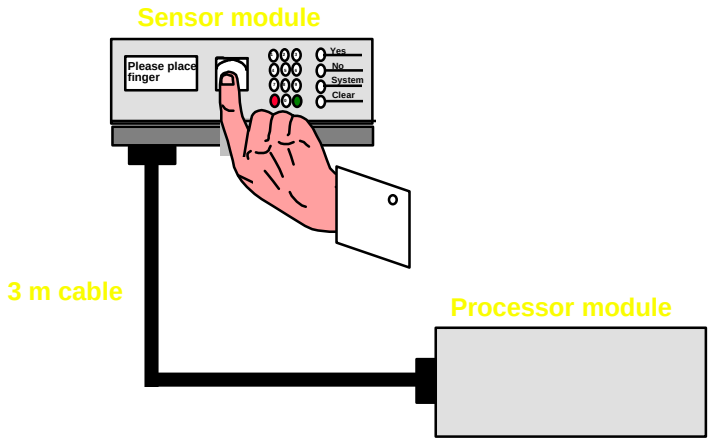
Outputs 11 and 12 on the 12 Way Terminal Strip can be used to power a locking mechanism. A pre-charge of 18V is provided to initially engage the lock and a continuous current of 150mA at 12V is provided to keep the lock engaged. For locks that operate at higher voltages and/or require larger currents to maintain them in the engaged state these outputs should be used to drive an external relay which, in turn, drives the lock.

The output may be either **normally open** or **normally closed**, depending on whether **power on to lock** or **power off to lock** is required.

Integral unit



Modular unit



FINGERSCAN Power

FINGERSCAN requires 12V AC power at 1 amp. If a power pack has been supplied with the unit, wire it in to points 1 and 2 on terminal strip 2. If no power pack has been supplied, it will be necessary to acquire a similar unregulated supply.

Battery Back-up

FINGERSCAN can be powered using a 24V DC battery back-up. The appropriate battery type depends on the length of time that FINGERSCAN must stay online.

A constant 24V DC charge is provided by wiring into points 3 and 4 on terminal strip 2, +24V DC is point 3 and common is 4.

Power Up

Before using FINGERSCAN verify that the unit is operating correctly with a simple power up self test.

When the unit is first plugged into the power outlet and switched on it will go through a self test routine and display the following sequence of messages:

	FIP Memory test
then…	**FIP Reset test**
then…	FINGERSCAN Vnn
then…	**Ser # nnnnnnnn**

where nn indicates the current version of the firmware. The unit's electronic serial number (ESN) will also be briefly displayed.

Once power up has been successfully completed the IDLE MODE prompt will be displayed as in the following example.

```
MON 15 AUG 14:55
ENTER ID NO.
```

If the card option has been loaded and turned on as part of the FINGERSCAN system set up the following message will be displayed:

```
MON 15 AUG 09:47
INSERT CARD
```

Board Settings

FINGERSCAN Hardware Board Settings

Read the following instructions in conjunction with Figure 2 at the end of this section.

J4 Jumper Block

It is necessary to adjust link settings on the FINGERSCAN processor according to the communication type required. Link settings are adjusted on the 18 way jumper block J2 located approximately 25mm (1 inch) above the main terminal strip on the bottom edge of the processor board. Three options are available:

HOST COMMS = RS232, AUX COMMS = TTL

HOST COMMS = RS485, AUX COMMS = RS232

HOST COMMS = RS485, AUX COMMS = TTL

J3 Connector

J3 is provision for a network terminating resistor. Some installations, particularly those involving long wiring runs, will require terminating resistors to minimise disruption to data signals. A professional installer will be able to determine if a terminating resistor is needed and where it should be located in the network.

Where a local RS485 network is to be used it is preferable to use a terminating resistor (100 Ohm is typical) on both pairs in the last wall box in the network (refer to the diagram at the end of the section).

J4 Connector (lower)

This is the auxiliary TTL-level communications connector. It is an 8 in line connector located right underneath the J4 jumper block.

Pin	Function
1	GND
2	TX
3	RX
4	RTS
5	CTS
6	CD
7	GND
8	+12V supply

Printer and Printer Cables

If a printer is connected directly to FINGERSCAN it must be a serial printer. The cable needed will depend on the type of printer used. FINGERSCAN uses CTS for handshaking.

J5 Connector

If an RS232 connection is required to communicate to a single FINGERSCAN a standard null modem cable is required between the PC and the DB9 connector on the bottom of the FINGERSCAN board.

The cable should be configured as shown in Figure 1.

NULL MODEM CABLE: db9 to db9

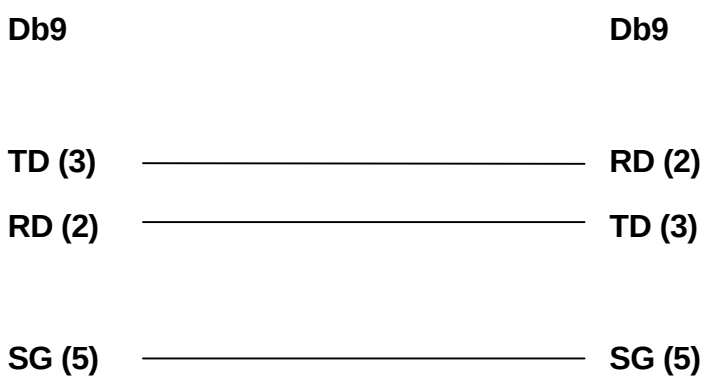
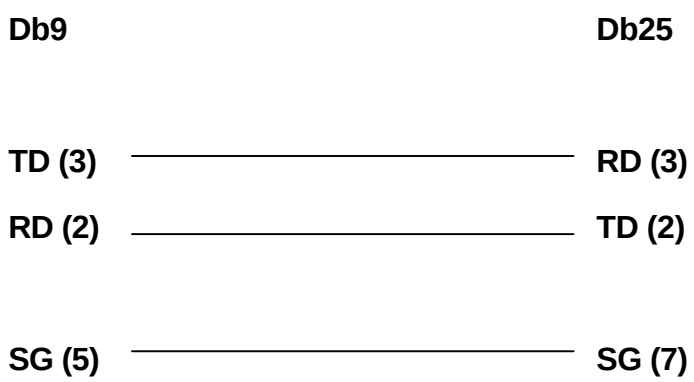


Figure 1: Null modem cable configurations

NULL MODEM CABLE: db9 to db 25



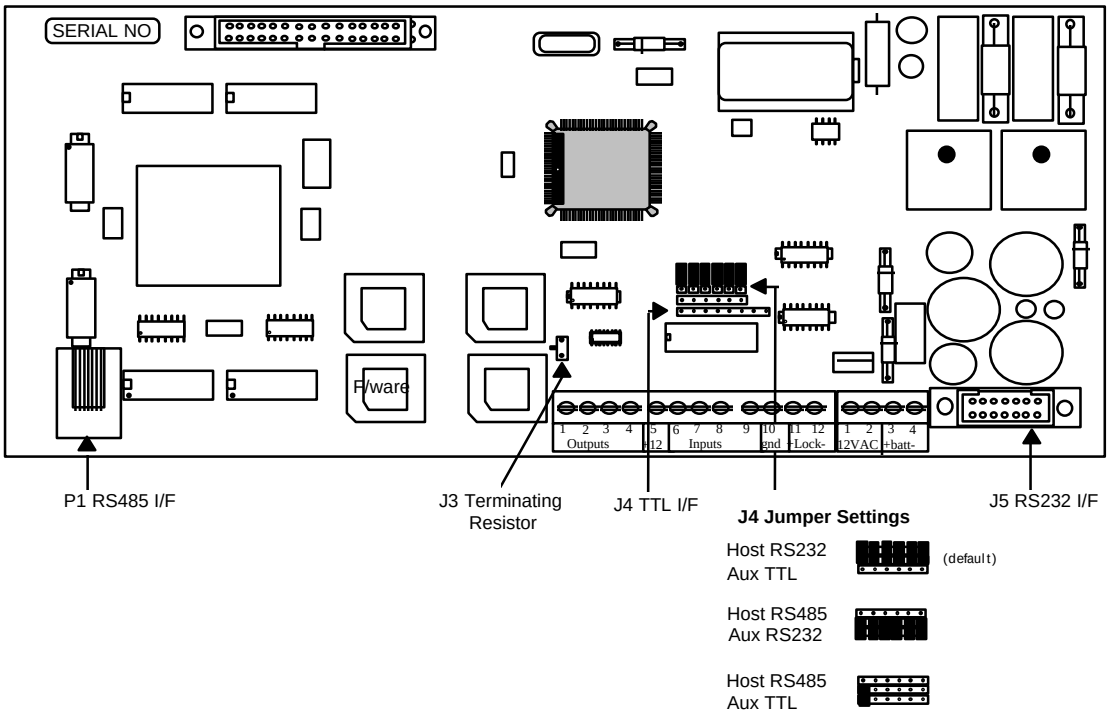


Figure 2 Main board and hardware settings.

Alarm Connections

Four inputs and four outputs are provided on the 12 way terminal strip.

12 WAY TERMINAL STRIP												4 WAY STRIP			
1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4
ALARM OUTPUTS				DC	ALARM INPUTS				GND	LOCK		AC		DC	
01	02	03	04	12v	11	12	13	14				12v		24v	0v

Inputs

Inputs are configured in the software (see **Fingerscan Supervisor & Manager User Guide**). Inputs 1 to 4 are numbered 6 to 9 on the terminal strip. The input state (**normally open** or **normally closed**) is also configured through the software.

Wire the inputs as follows:

1. Connect the selected input (for example, input 2 which is #7 on the terminal strip) to one end of the signalling device (such as a reed switch).

2. Connect the other end of the device to the +12V output (#5 on the terminal strip).

Outputs

Outputs are configured in the software (see **Fingerscan Supervisor & Manager User Guide**). Output 1 is numbered 1 on the terminal strip and so on. Outputs are triggered by inputs and can in turn drive other devices, such as audible alarms, automatic diallers, and can output 12V DC.

1. For **normally open** outputs connect one side of the external device to the selected output. Connect the other side to the +12V DC output (#5).

2. For **normally closed** outputs connect in a similar manner for all low voltage devices such as a small beeper or relay coil to a maximum of 5 watts. For higher current drawing devices use the output to drive a relay and power the device from a separate source.

Request to Exit (REX) and Door Switch

This facility configures one of the alarm inputs for use with a door switch and another for use with a REX push button. The door switch and REX switch are each wired between the 12V output and an alarm input (a different input for each). They may be used together or separately, with their functions being as follows:

Door switch

This indicates to FINGERSCAN the current state of the door (open or closed). If the door is opened without FINGERSCAN having first unlocked it, a **DOOR FORCED** alarm is raised and an entry made in the transaction log. If the door is unlocked by FINGERSCAN the lock will be released to allow immediate relocking upon closure.

If the door is held open for longer than the period set in the alarm set up a **DOOR OPEN TOO LONG** alarm is raised. When the door is closed after a door forced or open too long alarm the alarm is cancelled and a **DOOR CLOSED** entry is made in the transaction log.

REX switch

This allows the door to be unlocked from within the secure area in order to exit. The door will be unlocked as if it was a verification and an **EXIT GRANTED** entry made in the transaction log.

REX with barcode

When using the barcode option for the entry of the user PIN for verification, there is an additional option to use a second barcode reader usually fitted on the inside of the door to provide a barcode ‘Request to exit’ event. The barcode number is recorded against the ‘Exit’ event, however, it is not checked to establish if the same number was previously used as an entry, i.e. this is not to be confused with ‘anti-passback’ as is commonly used in card-based systems.

Networking

Read these instructions in conjunction with Figures 3, 4 and 5 in this section.

Setting node numbers

Before networking the units a node number must be defined for each FINGERSCAN**.** The default and lowest possible node number is 5. Numbers below 5 are reserved for internal system use only and are not recognised by the FINGERSCAN. All node numbers must be unique, numbered from 5 to 255.

Preparation

1. Each FINGERSCAN is connected to the network via a wall box which should be located within two metres of the unit and the host PC. Each wall box is connected in a daisy chain configuration back to the host PC. Wall boxes are commonly used in telephone or computer networks and should be available locally.

2. FINGERSCANs may be networked using the RS485 RJ11 connector on the bottom left hand side of the FINGERSCAN processor board. Use the J4 connector RS485 link setting.

3. A FINGERSCAN specific RS232/485 converter must be used, mounted between the host computer and the network. Only one converter is required for a network.

At the FINGERSCAN Unit

Using 4 way RJ11 connectors, connect a 2-metre length of telephone cable, crimped straight through (i.e. pin 1 same colour at each end) to the FINGERSCAN and to the wall box.

At the Wall Box

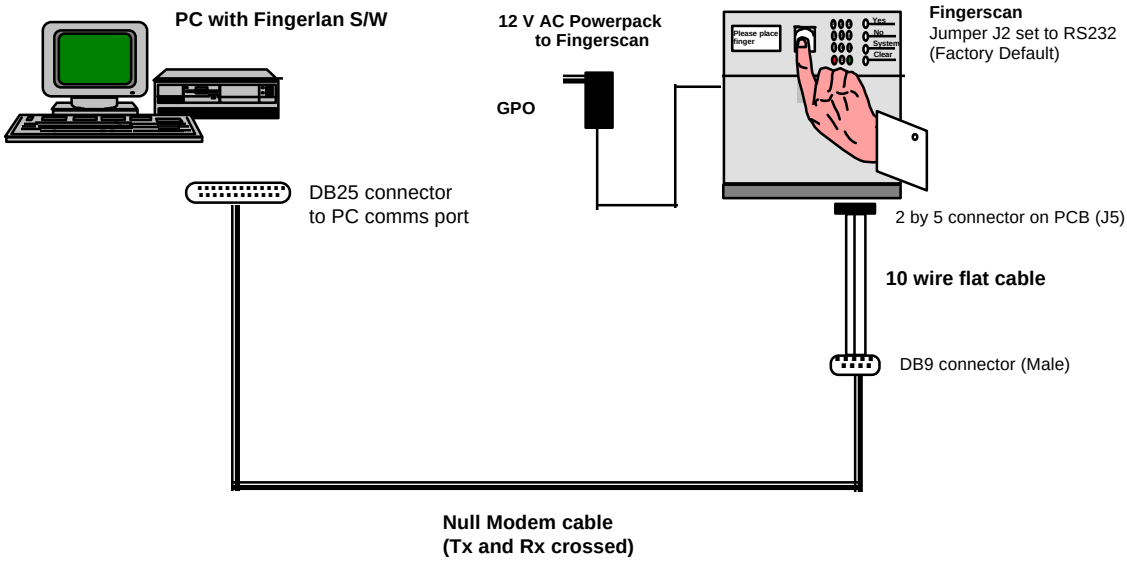
Connect each wall box in a daisy chain using 2 x twisted pair shielded cable with an earth drain. Connect one pair to 2 & 3, and the other to 4 & 5. The shield and earth are only terminated at the PC end. If terminating resistors are required, use 100 Ohm resistors on both pairs in the last wall box on the network.

At the Host PC

Connect the special RS232 converter to the selected communications port on the PC using the supplied cable.

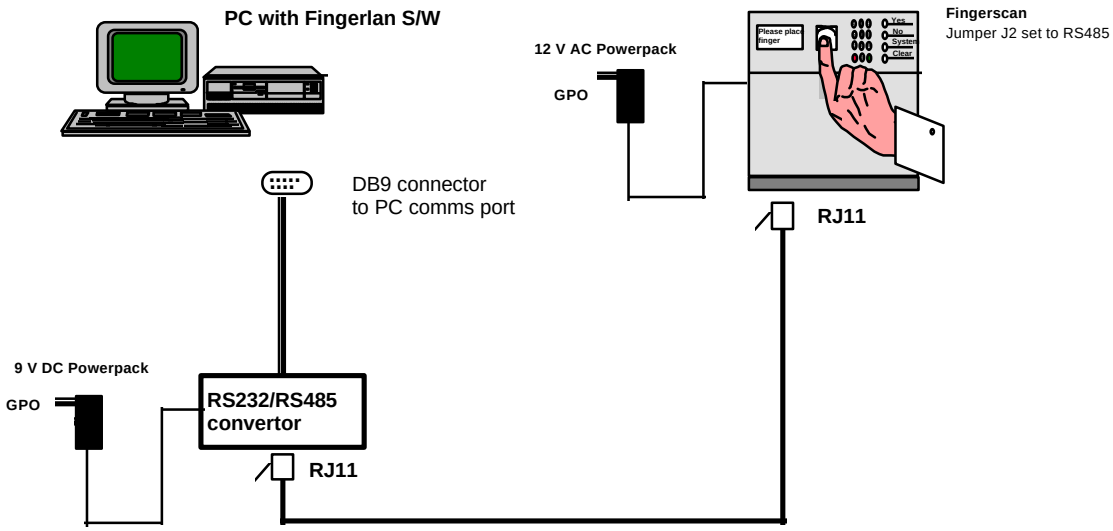
Connect the converter to the nearby wall box using 6-pin RJ12 connectors at each end of the 2-metre cable, crimped straight through (i.e. pin 1 same colour at each end).

In the wall box, link pin 1 and pin 6 and connect to the cable shield. Connect 2 & 3 to the first pair and 4 & 5 to the second.



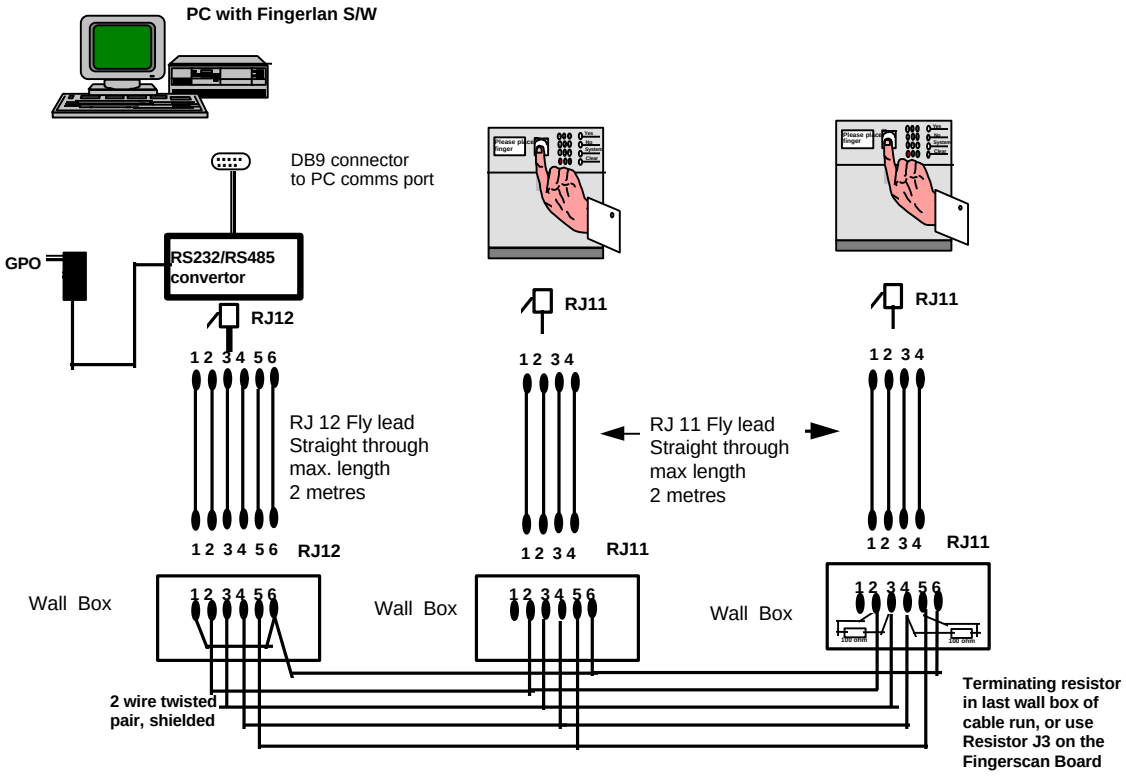
Note: The Null modem cable is not part of the standard Fingerscan product but is an industry standard component. The flat cable to the DB9 is supplied with Fingerscan.

Figure 3 FINGERSCAN to host PC RS232 connection



Note: The RS232/RS485 convertor (P10CE978) comes with a DB9 to DB9 cable for the RS232 port. and the 9V DC powerpack (Australia and New Zealand only). RJ11 cable is not part of the offering and is an industry standard component.

Figure 4 Single FINGERSCAN unit to host PC RS485 connection



Note: Pin 1 from the RJ12 fly lead connects to the pin 1 at the wall box.

Pin 1 from the RJ11 fly lead connects to the pin 2 at the wall box.

Figure 5 Multiple FINGERSCAN units RS485 LAN connection.

Diagnostics

FINGERSCAN Diagnostics

Self testing occurs during start up. Please refer to the ***Troubleshooting*** section in the **Fingerscan Supervisor and Manager User Guide**.

Optics Diagnostics

In firmware revision 1.57 and later, an optics diagnostic tool is included. This allows for the testing of the optics unit to determine the status of the illumination. It is essential that the test is carried out using a brand new and completely clean platen. Remember, this is not a test of the platen, but a test of the optics.

To access the test procedure, proceed to **SYSTEM** in the **SET UP** menu and press the **ALT** key. Select the illumination test option. The illumination test will be performed immediately. The optics LEDs will flash and a number will be displayed.

There are 2 types of test to be conducted; one with a new platen, that has never been used, and two, with a used or existing platen.

Test with new platen

Insert a new unused platen in the optics, and perform the illumination test.

If the number is outside the range of +500 or -500, then the illumination level may be faulty and the optics should be returned for repair.

If the platen is not new then the results will be invalid.

Test with a used platen

The illumination test can be used to test for a deteriorated platen.

In the case of a used platen, the test parameters are in the range of + 2500 to - 2500. Even at this level, the FINGERSCAN will work well for verifications, but, if used as an enrolment terminal, the enrolment quality may suffer.

Proceed as follows:

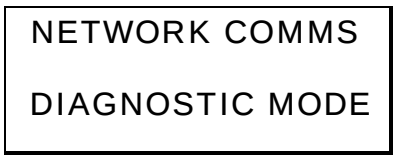
Perform the test. If the score is outside the range, change the platen and re-test.

NOTE: If the illumination test results are out of range or are deteriorating over a period of time when tested with a new platen, the optic assembly should be returned for repair.

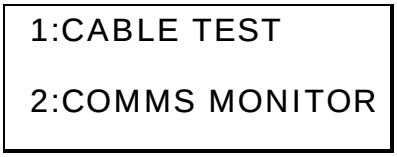
RS485 Network Diagnostics

FINGERSCAN firmware includes facilities for testing and debugging the RS485 network. To access these features display the Comms Menu:

and press the **ALT** key. The display shows



followed by the menu:



Option 1 allows the physical network cable to be tested; option 2 allows normal communications activity on the network to be monitored.

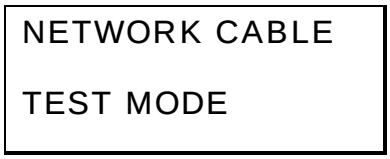
Testing the Network Cable

This test is run using a cable test box (described below). The normal RS232-485 converter at the host PC should be unplugged from the RS485 network cable and the cable test box plugged onto the cable in its place.

Temporarily disconnect any terminating resistors on the network.

Starting at the FINGERSCAN closest to the PC, place the unit in cable test mode by selecting **1-CABLE TEST**. Only one unit can be in cable test mode at any time.

The display shows;



The unit will stay in test mode until the **CLR** key is pressed. The state of the network cabling can be determined by checking the status of the LEDs on the cable test box against the conditions below. (a) to (h) refers to the larger coloured LEDs, (k) refers to the small central red LED, and (I) and (j) refer to all 5 LEDs.

The following line naming convention is used:

D+	RJ12 pin 4
D-	RJ12 pin 5
GND	RJ12 pins 2,3

(a) Correct LED sequence

The LEDs normally cycle through three states after which the pattern will repeat. The normal pattern is:

1	All LEDs off
2	RED and ORANGE bright, YELLOW and GREEN dim
3	RED and ORANGE dim, YELLOW and GREEN bright

(b) Reverse sequence

If the LEDs cycle in the reverse order:

1	All LEDs off
2	RED and ORANGE dim, YELLOW and GREEN bright
3	RED and ORANGE bright, YELLOW and GREEN dim

then D+ and D- are interchanged.

(c) GREEN and ORANGE always OFF

Both GND lines are open-circuited

(d) RED always OFF

D- open-circuited

(e) YELLOW always OFF

D+ open-circuited

(f) RED and YELLOW always OFF

D+ and D- shorted together

(g) YELLOW and GREEN always OFF

D+ and GND shorted together

(h) RED and ORANGE always OFF

D- and GND shorted together

(i) ALL LEDs always OFF

At least 2 lines open-circuited, or all 3 shorted

(j) No OFF cycle

Something else driving the lines

(k) Only small central LED ON

D+ and D- both interchanged with the 2 GND lines, most likely due to reverse-crimped RJ11 connector

Cable Test Box

A proprietary cable test box is available from the FINGERSCAN supplier. This consists of a box with an RJ12 connector wired to 4 coloured LEDs with resistors, the LEDs are arranged on the top of the box in the following pattern:

( ) RED ( ) ORANGE

( ) small red

( ) YELLOW ( ) GREEN

Comms Monitor

This mode allows normal communications activity on the RS485 network to be monitored. The FINGERSCAN can be placed in comms monitor mode by selecting 2-COMMS MONITOR from the Comms Menu. The display shows;

and the bottom line one of the following:

Bottom Line	Tone	Network activity
(blank)	(none)	Network is idle
Rx	high tone	Valid packet received
Rx + Tx	high tone	Valid packet received and packet sent in response
Rx IGNORED	medium tone	Packet for another node received and ignored
Rx CORRUPT	low tone	Corrupt data on network

The FINGERSCAN will remain in comms monitor mode until the **CLR** key is pressed. Any number of FINGERSCAN can be placed in Comms Test mode at one time.

Optional Interfaces

Major Interfaces

Wiegand Option

The FINGERSCAN system can be integrated with a Wiegand network without changing the whole network.

The Wiegand option allows the FINGERSCAN to be configured to output a particular Wiegand bit stream in the event of a VERIFY which transmits the verified id number in Wiegand format to the Wiegand controller. The Wiegand output only occurs on a VERIFY; no other transaction log messages are transmitted this way.

The verification cycle can be commenced either by the user entering their id number on the keypad in the normal way (output only configuration) or by swiping a Wiegand card through the card reader (input and output configuration).

Wiegand card input can also be used during enrolment to enter the number directly from the card. Care should be taken to check that the number received from the card is interpreted correctly, and does not result in an unknown template on file.

One of the FINGERLAN software packages can be used in conjunction with the Wiegand network to provide template and transaction log management.

The List Log facility is not available when the Wiegand option is activated.

Interface Hardware

The Wiegand interface is a dual-line system using the TTL-level serial interface connector (8-way 0.1" SIL J4 connector). The pin connections and jumper settings are as follows:

Output-only configuration

In this configuration a subset of the Aux. serial port (Tx,Rx,RTS) can still be connected to additional external devices such as a smart card reader. Configure the pins as follows:

Function	J4 Pin
Gnd	1
Aux. Tx	2
Aux. Rx	3
Aux. RTS	4
Data 1 out	5
Data 0 out	6
Gnd	7
+12V	8

Configure the following jumper settings:

HOST=RS232	AUX=TTL + Wiegand	LK1 to LK6 = 1-2
HOST=RS485	AUX=RS232 + Wiegand	LK1 to LK4 = 2-3; LK5 & LK6 = open
HOST=RS485	AUX=TTL + Wiegand	LK1=2-3; LK2 to LK6 = open

Input & Output configuration

In this configuration the Aux. serial port is not available. Configure the pins as follows:

Function	**J4 Pin**
Gnd	1
Data 1 out	2
Data 0 out	3
---	4
Data 1 in	5
Data 0 in	6
Gnd	7
=12V	8

Configure the following jumper settings:

HOST=RS232	AUX=Wiegand LK1 to LK6 = 1-2
HOST=RS485	AUX=Wiegant LK1 = 2-3; LK2 to LK6 = open

Electrical characteristics

Input HIGH voltage = +2.0 to +5.0V
Input LOW voltage = -0.3 to +0.8V
Input current (max) = 20uA
Output HIGH voltage = 4.0 to 5.0V
Output LOW voltage = 0 to 0.5V
Max output current = 10 mA (estimated)
Max capacitive load = 50nF

CAUTION: No isolation or ESD protection is provided on the Wiegand interface. If this is required (especially for long lines) it should be added externally.

Wiegand test cables

Loopback Test Connector

An 8-way 0.1" SIL connector may be wired as follows to perform a loopback test on the Wiegand interface.

1. Link pins 2 to 5 and 3 to 6.
2. Configure FINGERSCAN for INPUT & OUTPUT, and plug the loopback connector onto the Aux. serial connector J4 on the FINGERSCAN board.

If the Wiegand interface is working correctly, upon performing a successful verification FINGERSCAN will immediately prompt the user to again place their finger for another verification. This occurs because the Wiegand interface provides an output on successful verification. This is then connected directly back to the Wiegand input which provides the user id for the next verification.

The cycle will continue until either an unsuccessful verification or until verification is aborted by pressing the **CLEAR** key.

Two-Unit Test Cable:

A pair of 8-way 0.1" SIL connectors (named C1 and C2 in the connection table) may be interconnected with a length of cable as follows:

C1	C2
1 ----------	1
2 ----------	5
3 ----------	6
4	4 (not connected)
5 ----------	2 (do not connect if 1-way communications is required)
6 ----------	3 (do not connect if 1-way communications is required)
7 ----------	7
8	8 (not connected)

Each end of this cable may then be plugged onto connector J4 of two FINGERSCAN units, and both units configured for **INPUT** & **OUTPUT** with the same data format.

When a successful verification is performed on one FINGERSCAN, the other unit will immediately prompt the user to place their finger for verification (assuming the required template is also found by that machine). The first FINGERSCAN sends a Wiegand output to the second unit which then takes the user id to request a verification.

Configuring Wiegand using the keypad

A limited form of Wiegand configuration may be performed through the FINGERSCAN keypad.

Features such as facility codes cannot be entered into the Wiegand format through the keypad, it is therefore generally recommended that the Wiegand PC-based configuration utility WIEGAND.EXE be used.

Select option 4-Wiegand from the Comms Menu. The following message is displayed:

```
WIEGAND DISABLED
CHANGE    Yes/No ?
```

If **YES** is selected, the display changes to

```
WIEGAND BITS = 20
CHANGE    Yes/No ?
```

Continue to select **YES** until the required bit number appears in the screen. Then select **NO** and the following message appears

```
INPUT & OUTPUT
CHANGE    Yes/No ?
```

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

Configuring Wiegand using the WIEGAND.EXE utility

Refer to the document **WIEGAND.Interface User Guide** for detailed description of the use of the WIEGAND.EXE software utility. This can be used to configure a FINGERSCAN unit's Wiegand interface from a PC running Windows 3.1. The PIF file must be set up for it and the Execution: **Exclusive** option must be selected in the PIF editor.

The WIEGAND.EXE utility allows for a more complex setting of the Wiegand options than can normally be set via the Fingerscan keypad

The FINGERSCAN unit should be connected to the PC by the RS232 or RS485 interface and the node number and host baud rate of FINGERSCAN should be checked (defaults of 9600 baud and node 5 will apply if it is a completely new unit).

The command-line format of WIEGAND.EXE is:

WIEGAND [baud rate] [com#]

where the baud rate = optional communications speed (default=9600) and com# = optional PC COM port to use (default=1)

Example

WIEGAND 19200 2

for 19200 baud on COM2

or

WIEGAND

for 9600 baud on COM1

The main screen of the program displays a tabular representation of the Wiegand configuration with a menu at the bottom of the screen. The current COM port and baud rate are displayed at the top of the screen.

The top row of the table shows the numbers of the bits currently available in the Wiegand data format, bit 1 being the first transmitted. The middle row shows the current function of each bit of the format, the options being:

PRTY	=	Parity bit
C	=	Constant bit: the state is always shown in the bottom row
IDnn	=	ID number bit (nn is the bit number)The bottom row shows the state of each bit, the options being:

- E = Even parity bit
- O = Odd parity bit
- x = State of corresponding bit of user id
- 1 = (bit=1)
- 0 = (bit=0)

The menu options are described below.

Menu Option	Description
LOAD FROM DISK	Load a previously saved Wiegand configuration from the disk file WIEGAND.DTA. This is useful if many FINGERSCAN units are to be given similar configurations over several sessions. A message confirms the operation was completed successfully.
SAVE TO DISK	Save the current Wiegand configuration to the disk file WIEGAND.DTA. A message confirms the operation was completed successfully.
GET FROM F/S	Upload the current Wiegand interface configuration from a FINGERSCAN unit for display and/or modification. A message confirms the operation was completed successfully.
UPDATE F/S	Download the current Wiegand configuration as displayed on the PC to a FINGERSCAN unit. A message confirms the operation was completed successfully.
NODE=	Displays the current FINGERSCAN network node number (default=5) and allows this number to be changed to match that of a specific FINGERSCAN unit with valid numbers being in the range 5 to 255. This is useful if several units are connected via an RS485 network.
WIEGAND LENGTH=	Displays the current length of the Wiegand format (bits) and allows this to be changed in the range 20-40 bits. FINGERSCAN can handle Wiegand configurations of up to 48 bits but only 40 can be set by the current PC software. The current bit order (LSB if least significant bit first or MSB is most significant bit first) is then displayed and may be changed if required. The current interface type **OUTPUT ONLY** or **INPUT & OUTPUT** is displayed and may be changed if required.
ID SETTINGS	Displays and allows editing of the number of the first bit of the user id field and the number of bits in the field. The numbers entered are checked for validity, the valid ranges depend on the configuration. Bit 0 of the id (ID0) is the LSB which will be set last if the MSP option is selected.
CONST SETTINGS	Allows fields containing constants (numbers) to be entered into specific locations in the Wiegand format. The user is prompted to enter the position of the start of the number (starting bit number) the length of the number (bits) and the numeric value. The binary equivalent of the number is shown on the bottom row of the table, the bit order being as for the id number. The actual numeric value entered is not retained, only the corresponding bit pattern in the constant bit fields.
BIT TOGGLE	Allows the state of a single bit of the Wiegand format to be toggled (i.e. changed from 0 to 1, or 1 to 0). The user is prompted for the number of the bit to be changed and while any bit can be selected, parity bits and id number bits should normally be avoided but can be used for special purposes.
QUIT	Terminates the program and returns to the DOS prompt.

Multi-door Option

This function, which is ordered as a separate option, converts up to four alarm outputs into outputs personalised by different door id numbers. This enables users to activate different doors. For example, one user could be allowed to activate any door while another might be restricted to one door.

Using the existing FINGERSCAN relay this gives a total possibility of five different outputs. The outputs can be used for any number of purposes. One use could be to control up to five different doors from the same FINGERSCAN (hence the name multi-door).

Some menus are changed in this option.

Hardware

Wire the existing relays as described in the *Board Settings* section. This relay is always door #1. No additional relay is required.

Wire the four alarm inputs as follows:

1. Place a 12V relay between the 12V output (position 5 on the terminal strip) and output #1 (position 1 on the terminal strip). This becomes Door #1.

2. Refer to **Fingerscan Supervisor & Manager User Guide** - ***Selecting the Input Alarms*** for the output delay setting.

3. Continue to output #4 for as many auxiliary doors as required. The last output is Auxiliary door #4.

Set up

Refer to **Fingerscan Supervisor & Manager User Guide** for additional set up details.

Smart Card Option

The smart card option allows a user's template to be stored on a smart card as well as, or instead of, in the FINGERSCAN memory. FINGERSCAN supports the Gemplus smart card reader.

FPL Proximity Smart Card

Using this option the user places their smart card or tag in the vicinity of the FINGERSCAN key pad. FINGERSCAN reads the template from the card and performs a verification. There is no other visible hardware and there is no visible change to FINGERSCAN.

This option is factory fitted and the only configuration required is to turn the card reader option on. The user is prompted by messages appearing on the display.

All keypad operations occur in the normal way and it is possible to use either the keypad or the smart card.

Gemplus Smart Card

This option comes with special FINGERSCAN firmware which supports the use of Gemplus MCOS 16k EEPROM cards and greater.

Id numbers can also be entered as normal in the keypad where the template is stored within FINGERSCAN.

Interface Hardware

A Gemplus GCR200 or equivalent smart card adaptor is connected to the RS232 serial port on FINGERSCAN. Both the smart card adaptor and the FINGERSCAN Aux. comms baud rate must be set to at least 9600 baud and the smart card option enabled.

Initialising a new card

A software utility called SCARDINI.EXE is available to initialise new Gemplus smart cards for use with FINGERSCAN**.** Cards must be initialised once only before the card is used for the first time.

SCARDINI.EXE will run on an industry-compatible PC running under DOS or as a DOS program under Windows 3.1. The PIF file must be set up for it and the Execution:Exclusive option must be selected in the PIF editor.

A Gemplus GCR200 or equivalent card adaptor should be connected to a serial port on the PC.

The command-line format of SCARDINI.EXE is:

SCARDINI [baud rate] [com#] [code]

where:

baud rate = optional communications speed (default=9600)

com# = optional PC COM port to use (default=1)

code = either optional manufacturer batch secret number (4-digit hex e.g. A67B) or manufacturer secret code (8 alpha-numeric characters e.g. TESTCODE).

Example

SCARDINI 19200 2 A67B

for 19200 baud on COM2 and batch secret number A67B

or

SCARDINI

for 9600 baud on COM1

The supplier of the cards must provide either the manufacturer batch secret number or manufacturer secret code. If one of these is not entered on the command line the user will be prompted to enter one when it is required.

When the program starts the user is requested to insert a new (blank) card into the adaptor and the card is checked. If the batch secret number or secret code has not already been specified it will be requested and the card is then updated. Messages are displayed to indicate the progress of this operation, and finally the user is requested to remove the card.

If the PC appears to lock up at any stage of this process due to comms problems etc., the operation may be aborted by hitting the **ESC** key.

The card now has the required secret code, and is ready to be used for a FINGERSCAN enrolment.

Smart Card Utility

A software utility called FS_CARD.EXE can be used to perform some simple maintenance functions on a FINGERSCAN Gemplus smart card from an industry-compatible PC running under DOS or as a DOS program under Windows 3.1. The PIF file must be set up for it and the Execution:Exclusive option must be selected in the PIF editor.

A Gemplus GCR200 or equivalent card adaptor should be connected to a serial port on the PC.

The command-line format of FS_CARD.EXE is:

FS_CARD [baud rate] [com#]

where baud rate = optional communications speed (default=9600) and com# = optional PC COM port to use (default=1)

Example

FS_CARD 19200 2

for 19200 baud on COM2

or

FS_CARD

for 9600 baud on COM1

When the program is run the user is requested to insert the card, which is then checked, with messages indicating the progress of the operation.

If the card does not have the required secret code, a message will indicate that the card has not been correctly initialised.

The current status of the card is then displayed, including the total number of files in the root directory, the number of bytes free, and the template files if found. Due to limitations in file size on MCOS smart cards a FINGERSCAN template must be split between two files: one called 'T' and another called 't'. Both files must be present for a successful verification.

A single-line menu is displayed. The menu options are described below. Options are activated by selecting the key shown in the menu within square brackets.

Menu Option	Description
READ TEMPLATE	Read a FINGERSCAN template from the smart card and save it to a disk file. The card is checked for the pair of MCOS files which hold the template and if they are found each will be read and the entire template saved to a disk file. The name of a template file consists of the user id number with a dot-extension consisting of the finger number (1 digit) followed by -T. If an existing file is found with this name the option to use a different name is offered, otherwise the old file will be replaced.
WRITE TEMPLATE	Read a FINGERSCAN template from disk and write it to the smart card. The user is prompted to enter the id number and finger number of the template and a check is performed to verify that the corresponding file is available on disk. The name of a template file consists of the user id number with a dot-extension consisting of the finger number (1 digit) followed by -T. The smart card is then checked to ensure there are no existing template files present and if not, the template is written tot he card as the two files T and t.
ERASE CARD	This option allows all data on a card to be erased so that the card can be used to store a new template. The user is asked to confirm that they wish to proceed with this operation and if so, the data on the card is erased.
QUIT	Terminates the program and returns to the DOS prompt. The card is powered down and the user may remove the card.

Barcode Option

This option interfaces a Barcode reader to the FINGERSCAN so that the user's id number is carried on the Barcode card. The user simply swipes the card, the number is read from the card and the template associated with the number is presented for verification against the newly presented finger.

Barcode is available as an option in firmware version 1.54 and above.

Technical Description

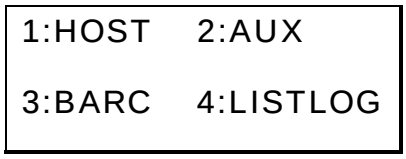
The barcode inputs will accept a raw TTL-level bit stream from a card reader (no internal controller required). The keypad may also be used as normal for the entry of id numbers. In firmware version 1.54, only the Code 39 barcode format is supported, and barcode lengths may be up to 25 characters.

Two barcode data inputs are provided, the main one (input#1) accepting a user id number from a barcode in place of a keypad entry for normal FINGERSCAN functions (e.g., verifications). The second input (input#2, which need not be connected if not required) accepts a user id number from a second barcode reader which would normally be mounted on the inside of a secured door (the main one being on the outside with the FINGERSCAN unit). When an id number is received from this second reader, the door is unlocked to allow exit and an **'EXIT GRANTED'** entry placed in the transaction log. This second barcode reader may thus replace a request-to-exit push-button, with the advantage that the exiting user's id is also stored in the transaction log.

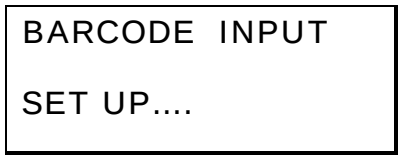
Set Up Procedure

When the barcode option is enabled in the FINGERSCAN, the

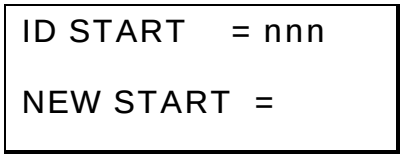
Communications menu reads as follows:



Select 3: BARC. The display will show:



This will be displayed for 2 seconds or until the clear key is pressed. The display now shows:



Counting from the first character at the left hand side, enter the starting position of the id number and press the **YES** key. Note that the first character of the text is number 1, excluding the start (*) character. For instance, if the id number commences at the 6th character from the left, enter 6. Please note that a figure of zero means that barcode is disabled. The id length is the same as that set for keypad entries.

NOTE that in the case of PC host-based configuration, the field of the configuration record used for the barcode ID starting position is that also used for the Wiegand ID starting position.

Once completed, the display will show:

CHECKSUM DISABLED
CHANGE YES/NO

If a checksum is being used, select **YES** and the checksum is then enabled. Select **NO** or **CLEAR** to confirm the selection. The display will now return to the main Communications menu.

In Idle Mode, the display will read 'SWIPE CARD' instead of 'ENTER ID NUMBER'.

Hardware Interface

The barcode interface consists of a pair of TTL-level inputs on the TTL serial interface connector (8-way 0.1" SIL connector J4). A subset of the Aux. serial port (Tx,Rx,RTS) is still available for connection of additional external devices (e.g., smart-card reader).

The pin connections and jumper settings are as follows:

(a) Pin Connections:

Function	J4 Pin	
Gnd	1	
Aux. Tx	2	
Aux. Rx	3	
Aux. RTS	4	
Barcode input #1	5	(main input)
Barcode input #2	6	(request-to-exit input)
Gnd	7	
+12v	8	

Note that if the barcode reader(s) require a +5v dc supply, a 3-terminal regulator (such as the 78L05 for currents up to 100mA) with a 100nF capacitor across it's output may be used to derive this from the +12v output on J4.

Also, some barcode readers may have open-collector outputs for data, which require additional pull-up resistors to +5v (10k should be suitable) when interfacing to FINGERSCAN.

(b) Jumper Settings:

(i)	HOST=RS232	AUX=TTL + barcode	LK1 to LK6 = 1-2
(ii)	HOST=RS485	AUX=RS232 + barcode	LK1 to LK4 = 2-3
			LK5 & LK6 = open
(iii)	HOST=RS485	AUX=TTL + barcode	LK1 = 2-3
			LK2 to LK6 = open

Electrical characteristics

Input HIGH voltage = +2.0 to +5.0 V

Input LOW voltage = -0.3 to +0.8 V

Input current (max) = 20uA

N.B: No isolation or ESD protection is provided on the barcode interface: if required (especially for long lines), it should be added externally.

2-D Barcode Option.

2-D barcode is a barcode system that can hold enough data on which a finger template can be recorded.

The current system that is interfaced is by a company called DATASTRIP. This Datastrip specification conforms to the PDF417 format. The 2-D barcode option must be enabled in the Fingerscan firmware before use. Ensure that the auxiliary baud rate is set to the rate of the 2-D Barcode reader. See the document **2D Barcode Firmware Qualification Test** for detailed discussion.

Minor Interfaces

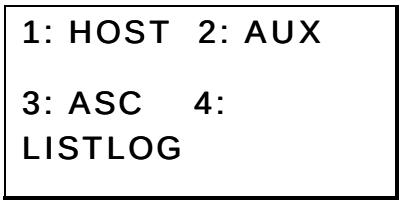
Clock In / Clock Out T&A option.

This is currently a firmware option. If this option is activated, then it is necessary to select either **YES/IN** or **NO/OUT** before entering the ID # and doing a verification. This change requires a user to select either **IN** or **OUT**.

ASCII I/O option.

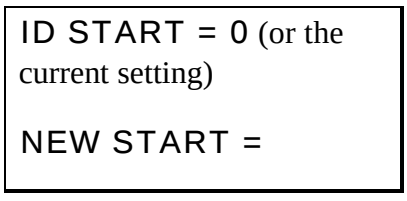
This is currently a firmware option. FINGERSCAN can now read an ID number from any device or system that outputs ASCII characters in serial format and will pass on the entire received ASCII string (not just the ID#) in the event of a successful verification. Once the option is available, proceed as follows:-

Go to the Communications Menu This will read:



Select **3: ASC** The display now reads:

Wait 2 seconds or so, or press **CLEAR**. The display now reads:



Enter the position in the ASCII string where the ID # starts, and press **YES.**

NOTE that the ID# end is the same as the length of the ID# already set as the ID length default If this is incorrect, then set the correct ID length required.

Electrical Interface

FINGERSCAN can use either the RS232 or the TTL port, using only the Rx (and optionally Tx if output is required) and Gnd pins with no handshaking.

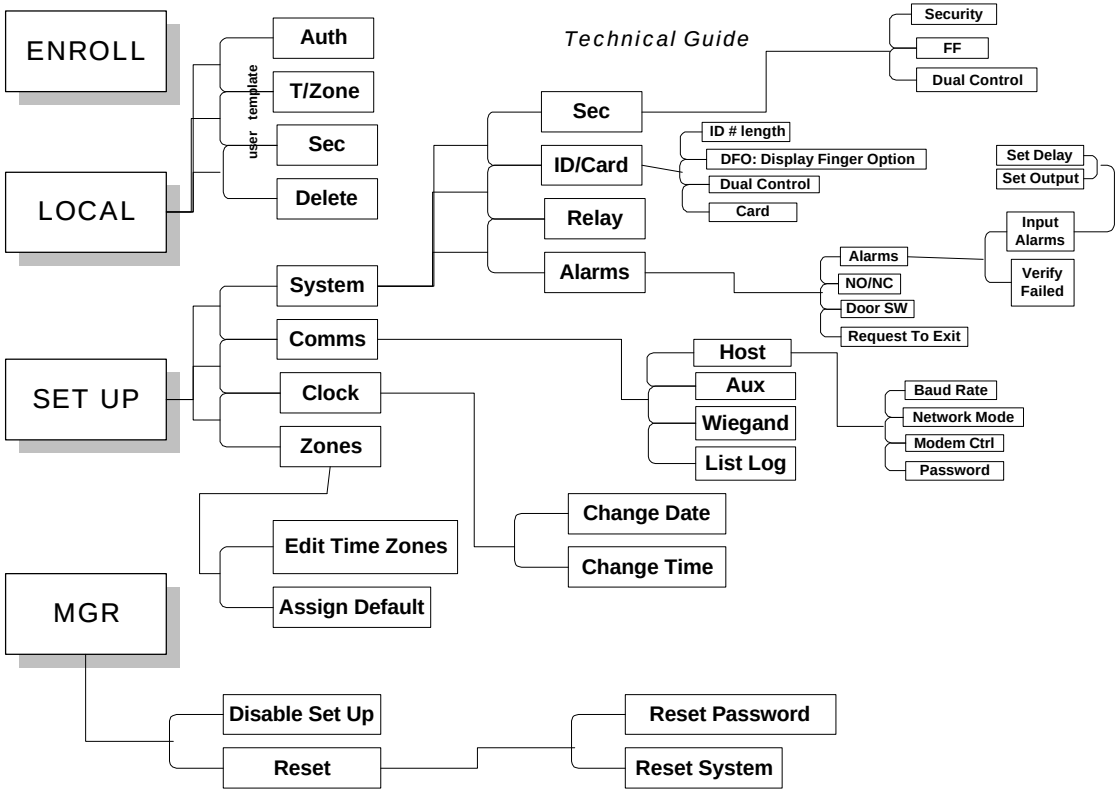
Technical Specifications

Main Board

CPU	Motorola 68302; 16mhz; 8-bit bus; watch-dog timer
Real-time Clock	Lithium battery backed; day-of-week register; leap year correction
Memory	512K to 1.5MB flash EEPROM in 512K increments
Keyboard Interface	16-key; 4 x 4 matrix; surge protected
LCD	16 characters x 2 line display; character mode; backlit
Speaker Interface	Speaker drive up to 12V, 500mA; volume adjustable
Alarm Interface	4 x TTL level compatible inputs; 1 to 30 sec delay; rated for input voltages of +30V to -30V; screw terminals 4 x open collector outputs; rated at 50V, 500mA; screw terminals 1 x 12V DC output; 10 ohm source impedance; screw terminals
Serial Interface	1 x serial port; jumper selectable for RS232/RS485 interface 1 x serial port, RS232 interface (if the first port is not RS232) and TTL level auxiliary connector; smart card interface
Solenoid Driver	Protected MOSFET switch rated at 60v, 10A Flywheel diode for inductive loads; 12V supply outputs; 68 ohms resistance 18 volts high pull-in current (capacitive reservoir); reduced holding current Software selectable for NO or NC. Activation period from 1 to 20 seconds
Verification	Accuracy verification is: False Acceptance Rate (FAR) (type 2 errors) 0.0001% False Rejection Rate (FRR) (type 1 errors) <1%
Power	
Input Requirements	12V AC at 50/50Hz; 1A; 500mA consumption in Idle mode
Battery backup (optional)	24V DC with provision for battery charging from the AC supply
Dimensions	Integral unit: W245mm x D85mm x H230mm Modular / portable unit Sensor: W245mm x D85mm x H110mm PCB enclosure: W245mm x D45mm x H120mm

Menu Trees

Technical Guide


ENROLL
LOCAL
SET UP
MGR
user template
Auth
T/Zone
Sec
Delete
System
Comms
Clock
Zones
Edit Time Zones
Assign Default
Disable Set Up
Reset
Sec
ID/Card
Relay
Alarms
Security
FF
Dual Control
ID # length
DFO: Display Finger Option
Dual Control
Card
Alarms
NO/NC
Door SW
Request To Exit
Set Delay
Set Output
Input Alarms
Verify Failed
Host
Aux
Wiegand
List Log
Baud Rate
Network Mode
Modem Ctrl
Password
Change Date
Change Time
Reset Password
Reset System

Index

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W