



1	Safety Information	1
1	IMPORTANT SAFETY INSTRUCTIONS	3
2	General	4
3	Features	5
4	Specifications	6
5	Identifying Supplied Parts	8
6	Product Overview	9
1	Functions	9
2	Product Explanation	10
2.1	Panel Description	10
2.2	Color Coded & Wiring Table	12
7	Installation Tips & Check Point	14
1	Check Points before Installation	14
1.1	Selection of Cable	14
1.2	Recommended Cable Type and Permissible Length of Cable	15
2	Check Point during Installation	16
2.1	Termination Resistor	16
2.2	How to Connect Termination Resistors	16
	Termination Resistors for 2-Wire RS485 Communication System	16
	Termination Resistors for 4-Wire RS422 Communication System	17
2.3	Grounding System for Communication Cable	17

8	Installation of the Product	19
1	Template	19
2	System Initialization	20
3	Wiring	21
3.1	Power	21
3.2	Output Connections	21
	Wiegand Data Connection	21
	Control Signal Connection	21
	External Reader Connection [Wiegand Input]	22
9	Communication	23
1	RS232 Communication Port Connection	23
2	RS422 Communication Port Connection	23
2.1	RS422 Connection (Single FINGER006 Connection)	23
2.2	RS422 Connection (Multiple FINGER006 Connections)	24
3	TCP/IP Converter (External Version)	25
10	Basic Setting	27
1	Initialization of FINGER006	27
2	How to Enter the Setup Menu	28
3	Time / Date Setting	28
4	Maximum Number of Cardholder IDs	29
5	Registering Cardholder IDs	29
11	Operation	30
1	Normal Operation	30
2	Default Setting	31
12	Setting Changes	32
1	Setup Menu F1	33
1.1	Time Setting	34
1.2	Communication Address	34
1.3	BAUD RATE	35
1.4	Reader1 Mode	35
1.5	Reader 2 Mode	36
1.6	Master ID Registration	37
1.7	System Initialization	38
1.8	Card ID Clear	38
1.9	Event Clear	39

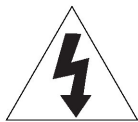
2	Setup Menu F2	40
2.1	LCD DISPLAY	41
2.2	BUZZER STATUS	41
2.3	OUTPUT MODE	42
2.4	LED_BUZZER_CONTROL	42
2.5	RF PIN INPUT	43
2.6	KEY OUTPUT MODE	43
2.7	KEY OUTPUT MODE	43
2.8	STAND ALONE	44
2.9	DATA BYTE (FINGER006SR ONLY)	44
3	Setup Menu F3	45
3.1	ID Registration	45
	Description of Fields	47
3.2	ID Deletion	47
3.3	ID List	48
3.4	Registered ID Count	49
3.5	ID Memory	49
4	Setup Menu F4	50
4.1	Firmware Version	52
4.2	Memory Test	52
4.3	Output Test	53
4.4	LCD Test	54
4.5	Keypad Test	54
4.6	Reader Test	55
4.7	Input / DIP Switch Test	55
4.8	Communication Test	56
4.9	Identification Mode	57
4.10	Dual Fingerprint Mode	57
4.11	ADAPTIVE MODE	58
4.12	FP STATUS	58
4.13	HIGH SECURITY 설정	58
4.14	FP QUALITY	59
4.15	FP LEVEL	59
4.16	Fingerprint Module Version	60
4.17	Fingerprint Count	60
4.18	Fingerprint Module Test	60

4.19 Fingerprint Device Information Check	60
13 Appendix	61
1 Default Values for Parameters	61
2 Output Format	61
2.1 26bit Wiegand Output Format	62
2.2 34bit Wiegand Output Format	62
2.3 ABA TRACK II (SELECTABLE USING THE SOFTWARE)	63
Data format	63
Output timing	63
3 Normal Output Mode (Default)	64
4 Extended Output Mode (Selectable using the software)	64
14 Troubleshooting	65
1 The device dose not communicate with PC.	65
1.1 Please check wiring.	65
In the case of RS232 communication	65
In the case of RS422 communication	66
1.2 Please check if the communication ID is good.	66
Check communication address setting of software and the device.	66
1.3 Please check if the communication port setting is good.	67
2 Cards which were being used are not authenticated after executing batch transmission o f IDs from software to the device.	67
2.1 The ID of the card may not be registered to software.	67
3 When configuring the device using MASTER ID, suddenly the device goes back to the no rmal mode.	67
3.1 If you do not input anything for 60 seconds in setting mode, the device goes back to t he normal mode.	67
4 The device does not go to setting mode after inputting MASTER ID.	68
4.1 A MASTER ID may have changed.	68
5 The device work well with RF Card, but does not work when inputting card number.	68
5.1 Please check if Keypad is set to "USE".	68
6 A buzzer keeps making sounds. "Bee~~~~~"	69
6.1 Check if the tamper switch is pressed well.	69
7 I want to access with card only, without password.	70
8 I want to access with fingerprint only, without card or password.	70
9 A fingerprint is not recognized.	71
9.1 Please check the status of the fingerprint.	71

9.2 If the status of the fingerprint is OK, register your fingerprint again.	71
10 I want to register 2 fingerprints for 1 ID.	71
10.1 Please check if Dual Fingerprint Mode is set to "USE".	71
15 FCC REGISTRATION INFORMATION	73

Safety Information

1



CAUTION: TO REDUCE THE RISK OF ELECTRIC SHOCK, DO NOT REMOVE COVER (OR BACK) NO USER SERVICEABLE PARTS INSIDE. REFER SERVICING TO QUALIFIED SERVICE PERSONNEL.



This symbol indicates that dangerous voltage consisting a risk of electric shock is present within this unit.



This exclamation point symbol is intended to alert the user to the presence of important operating and maintenance (servicing) instructions in the literature accompanying the appliance.

WARNING

To reduce the risk of fire or electric shock, do not expose this appliance to rain or moisture.

WARNING

1. Be sure to use only the standard adapter that is specified in the specification sheet. Using any other adapter could cause fire, electrical shock, or damage to the product.
2. Incorrectly connecting the power supply or replacing battery may cause explosion, fire, electric shock, or damage to the product.

3. Do not connect multiple controllers to a single adapter. Exceeding the capacity may cause abnormal heat generation or fire.
4. Securely plug the power cord into the power receptacle. Insecure connection may cause fire.
5. When installing the controller, fasten it securely and firmly. The fall of controller may cause personal injury.
6. Do not place conductive objects (e.g. screwdrivers, coins, metal parts, etc.) or containers filled with water on top of the controller. Doing so may cause personal injury due to fire, electric shock, or falling objects.
7. Do not install the unit in humid, dusty, or sooty locations. Doing so may cause fire or electric shock.
8. If any unusual smells or smoke come from the unit, stop using the product. In such case, immediately disconnect the power source and contact the service center. Continued use in such a condition may cause fire or electric shock.
9. If this product fails to operate normally, contact the nearest service center. Never disassemble or modify this product in any way. (SAMSUNG is not liable for problems caused by unauthorized modifications or attempted repair.)
10. When cleaning, do not spray water directly onto parts of the product. Doing so may cause fire or electric shock.

CAUTION

1. Do not drop objects on the product or apply strong blows to it. Keep away from a location subject to excessive vibration or magnetic interference.
2. Do not install in a location subject to high temperature (over 50°C), low temperature (below -30°C), or high humidity. Doing so may cause fire or electric shock.
3. If you want to relocate the already installed product, be sure to turn off the power and then move or reinstall it.
4. Remove the power plug from the outlet when there is a lightning storm. Neglecting to do so may cause fire or damage to the product.
5. Keep out of direct sunlight and heat radiation sources. It may cause fire.
6. Install it in a place with good ventilation.
7. Avoid aiming the controller directly towards extremely bright objects such as sun.
8. Apparatus shall not be exposed to dripping or splashing and no objects filled with liquids, such as vases, shall be placed on the apparatus.
9. The Mains plug is used as a disconnect device and shall stay readily operable at any time.

1 IMPORTANT SAFETY INSTRUCTIONS

1. Read these instructions.
2. Keep these instructions.
3. Heed all warnings.
4. Follow all instructions.
5. Do not use this apparatus near water.
6. Clean only with dry cloth.
7. Do not block any ventilation openings. Install in accordance with the manufacturer's instructions.
8. Do not install near any heat sources such as radiators, heat registers, or other apparatus (including amplifiers) that produce heat.
9. Do not defeat the safety purpose of the polarized or grounding-type plug. A polarized plug has two blades with one wider than the other. A grounding type plug has two blades and a third grounding prong. The wide blade or the third prong is provided for your safety. If the provided plug does not fit into your outlet, consult an electrician for replacement of the obsolete outlet.
10. Protect the power cord from being walked on or pinched particularly at plugs, convenience receptacles, and the point where they exit from the apparatus.
11. Only use attachments/accessories specified by the manufacturer.
12. Use only with cart, stand, tripod, bracket, or table specified by the manufacturer, or sold with the apparatus.
13. Unplug this apparatus when a card is used. Use caution when moving the cart/ apparatus combination to avoid injury from tip-over.
14. Refer all servicing to qualified service personnel. Servicing is required when the apparatus has been damaged in any way, such as power supply cord or plug is damaged, liquid has been spilled or objects have fallen into the apparatus, the apparatus has been exposed to rain or moisture, does not operate normally, or has been dropped.

The Star FINGER006 / iPASS IP-FINGER006 / IDTECK FINGER006SR is such a highly advanced and intelligent fingerprint reader (with a keypad) with a powerful 32bit and dual 8bit micro processor to meet the market requirement for a robust integrated solution for access control and time & attendance.

The unit has been designed to be flexible and reliable in providing the ultimate biometrics high security at a reasonable cost.

This user-friendly device allows you to register up to 4,000 fingerprint IDs (optional 1,000/2,000) and 50,000 cards and add / delete user IDs (Cards) conveniently.

With the built-in 4" RF reader, the keypad for Personal Identification Numbers (PIN), and a sophisticated

biometric fingerprint module, the FINGER006 offers up to three levels of ID verification.

Any combination of Proximity, PIN, and Biometric may be used and different verification levels can be customer programmed for each user or user group.

Features

3

- 125KHz Proximity / PIN and Fingerprint Recognition
- 1,000 / 2,000 / 4,000 Fingerprint Users
- 1:1 Verification and 1: N Identification
- 2 Fingerprint Storage Templates
- Identification Method:
 - by PIN Key (default)
 - by Auto Touch Sensor
- ID Only Function for Persons with Unregisterable Fingerprints
- Network Communication via RS232 / RS422 (Max.32ch)
TCP/IP (Internal LAN Converter Required)
- 1 ea of External Reader Port: 26bit Wiegand, 4 / 8bit Burst
- 26bit Wiegand and ABA Track II Output Format
- High Protection from Scratch and ESD (Electro Static Discharge)
- High Quality Optical Sensor
- Dual Tamper Switches
- Options:
 - TCP/IP Communication (FINGER006T, FINGER006PT, IP-FINGER006T)
 - Supervisory Signal
- Compatible Software: STARWATCH DUAL PRO I / II, STARWATCH iTDC PRO I / II, STARWATCH STANDARD
- Compatible Controller: iCON100, iTDC, Third Party Controller, Standalone Controller

Specifications

4

Model			FINGER006/ IP-FINGER006/FINGER006SR
CPU			32bit ARM9 and Dual 8bit Microprocessor
Memory	Fingerprint Module	Program Memory	1MByte flash memory
		Data Memory	1MByte / 2MByte / 4MByte flash memory
	Controller	Program Memory	128KByte flash memory
		Data Memory	1MByte flash memory
Fingerprint Users			1,000 / 2,000 / 4,000
Event Buffer			10,000 - 50,000 event buffer (The sum of users and events cannot exceed 60,000.)
Fingerprint Templates Size			800 Bytes for 2 fingerprint templates
Range		FINGER006	IDC80 / IDC170 :Up to 4 inches (10cm)
		IP-FINGER006	IPC80 / IPC170 :Up to 4 inches (10cm)
		FINGER006SR	IHC80 :Up to 2 inches (5cm)ISC80 :Up to 4 inches (10cm)
Reading Time (Card)			30ms
Verification / Identification Time			Less than 1sec. / Less than 2sec.
Power / Current			DC 12V / Max.300mA
Communication			RS232 / RS422 (Max.32ch)
			TCP/IP (An optional built-in module or external converter required)
Baud Rate	Serial	9600bps (Recommended) / 4800bps, 19200bps, 38400bps, 57600bps and 11520	

		0bps (Selectable)
	Ethernet	10/100Mbps
Input Port		2ea (Error-Input, OK-Input)
Output Port		3ea (Error-Output , OK-Output, Temper-Output(Open Collector Output))
Output Format		26bit Wiegand(Default) 34bit Wiegand(Default)
LCD		Character LCD (2 Lines x 16 Char) / 65.6mm x 13.8mm (2.62" x 0.55") Screen
Keypad		16 Key Numeric Keypad with Back Lighting
LED Indicator		7 Array LED Indicators (Red, Green and Yellow)
Beeper		Piezo Buzzer
Operating Temperature	Fingerprint Module	-20° to +60°C (-4° to +140°F)
	LCD	0° to +50°C (+32° to +122°F)
	Main	-15° to +70°C (+5° to +158°F)
	RF Reader	-35° to + 65°C (-31° to +149°F)
Operating Humidity		10% to 90% relative humidity non-condensing
Color / Material		Dark Pearl Gray / Polycarbonate
Dimension (W x H x T)		6.36" x 5.28" x 1.9" (161.5mm x 134mm x 48.5mm)
Weight		547g (1.21lbs)
Certification		KC

Fingerprint module specifications

Resolution	500dpi
Captured Image Size	412X 303 pixels
Extraction Image Size	260 X 300 pixels
Sensing Area	13mm X 15.2mm
Scanner	High Quality Optical Sensor
FAR(False Acceptance Ratio)	0.001%
FRR(False Reject Ratio)	0.1%
ESD(Electro Static Discharge)	15KV

Identifying Supplied Parts

5



Main unit
(1 Unit)



Wall mount
(1 PC)



O-ring
(5 PCS)



User's manual
(1 Copy)



Screws
(4 PCS)



Cable & Diode
Cable(5 ea)

1 Functions

Operation with the Host Computer

ID data transactions can be managed via the host computer. The data transmitted from the controller can be displayed and stored on the host PC.

Data Backup

The reader retains all registered card data in the case of power failure.

Keypad Registration

The built-in keypad and the LCD screen let you perform manual programming without a PC connected.

Dual Finger Mode

Dual Finger Mode is a function that lets a user register two fingers for one ID so that the user can receive authentication with either of the two registered fingers. This is useful when a user's finger is injured.

1:N Identification

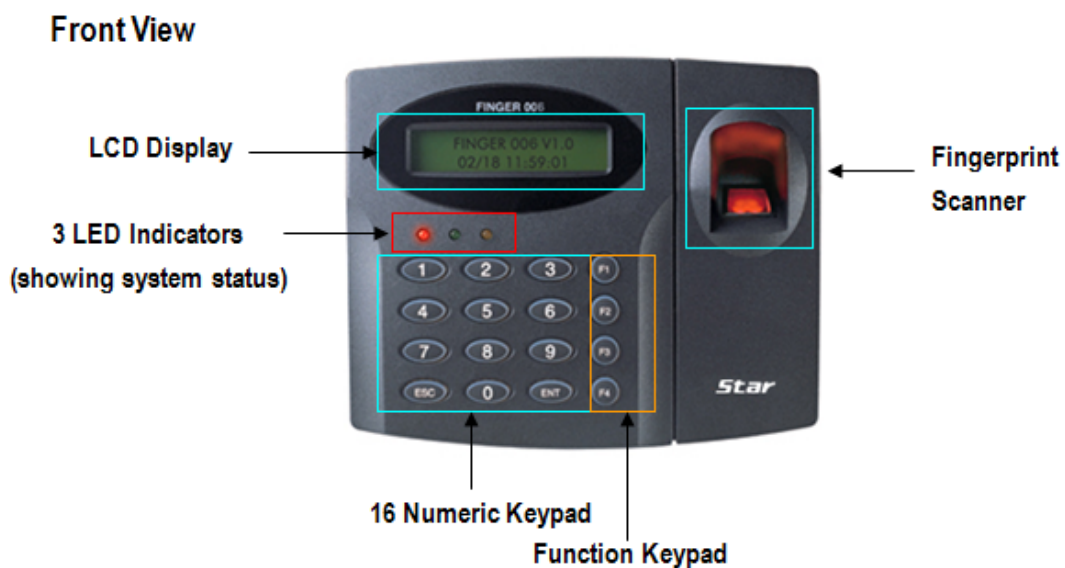
A user can gain authentication using the fingerprint alone without RF card or PIN. You can set this function through the <TYPE SELECTION> in SETUP MENU F1. In the IDENTIFICATION MODE, the security level is automatically increased and it causes FRR(False Rejection Ratio) to get higher, which may result in reduction of successful recognition rate. When using this mode, the user has to press the <ENT> key first, and then the fingerprint scanner waits for a fingerprint to be scanned. When the fingerprint-scan

is completed, FINGER006 identifies the user and makes corresponding outputs.

FINGER006 has a sensor. Normally, a user needs to press <ENT> in the identification mode before placing their finger on the sensor. However, if a sensor is installed, FINGER006 detects the user's finger and scans it automatically.

2 Product Explanation

2.1 Panel Description



LCD Display

LCD displays FINGER006's status.

3 LED Indicators (showing system status)

The red LED turns on with power supply.

The green LED turns on if access has granted. .

The yellow LED turns on if access has failed.

Finger Print Scanner

When users put their finger on the scanner, red light will turn on.

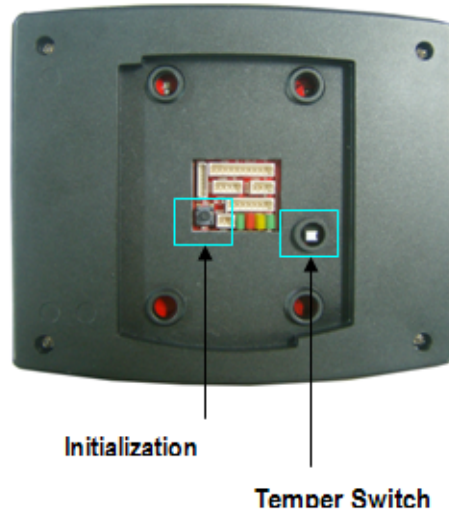
16 Numeric Keypad

Card data registration, deletion and various function settings are possible through keypad input without host computer control.

Function Keypad

There are four function keys: F1, F2, F3 and F4

Rear View



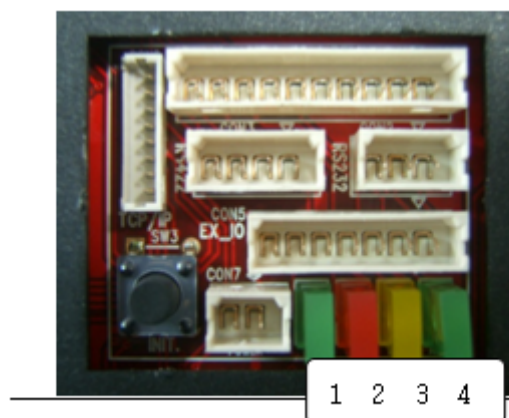
Initialization Switch

This switch is used to initialize Star FINGER006. For initialization, press down this switch and then keep it more than 2 seconds. Refer to '8.2 System Initialization' for more details.

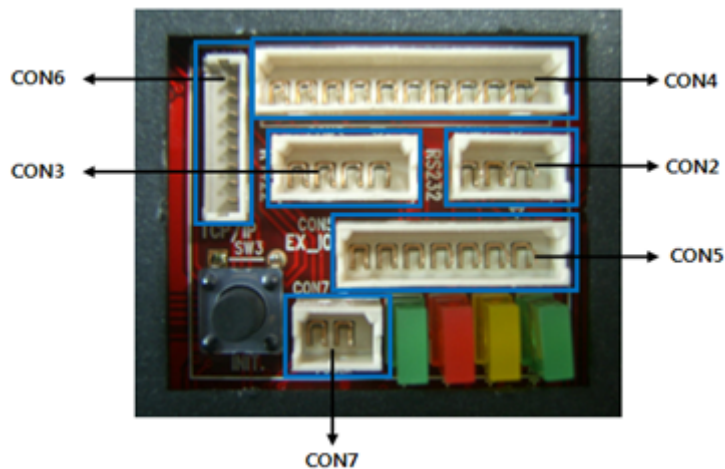
Communication Display LED

3, 4(yellow, green) LED will twinkle during RS232, RS422 and TCP/IP communication.

If the LAN is connected normally during TCP/IP communication, green LED will turn on. But in the collision status, #2 LED (red) will turn on.



2.2 Color Coded & Wiring Table



IO PORT NAME	SIGNAL NAME	COLOR CODED
POWER	(CON7)	
Main Power(+12V)	DC +12V	Red
Power Ground	GND	Black
INPUT	(CON4)	
OK Input IN1	(OK input)	Green
Error Input IN2	(Error input)	Green with White Stripe
EXTERNAL READER PORT	(CON5)	
Wiegand Data0	Wiegand DATA0 Input	Pink
Wiegand Data1	Wiegand DATA1 Input	Cyan
OUTPUT	(CON5)	
Wiegand Output1	DATA0	Orange with White
Wiegand Output2	DATA1	Brown with White Stripe
OK Signal Out	OK Out	Green with Red Stripe
Error Signal Out	Error Out	Blue with Red Stripe
Tamper Switch Out	Tamper Switch Out	Yellow with White Stripe
RS232 INTERFACE	(CON2)	
RS232-TX	TXD	Black with White Stripe
RS232-RX	RXD	Red with White Stripe

IO PORT NAME	SIGNAL NAME	COLOR CODED
Ground	GND	Black
RS422 INTERFACE	(CON3)	
RS422-TX(-)	TX(-)	Yellow
RS422-TX(+)	TX(+)	Gray
RS422-RX(-)	RX(-)	Blue
RS422-RX(+)	RX(+)	Brown
TCP/IP Communication	(CON6)	
	TCP/IP Communication (Optional)	8PIN connector module

Installation Tips & Check Point

7

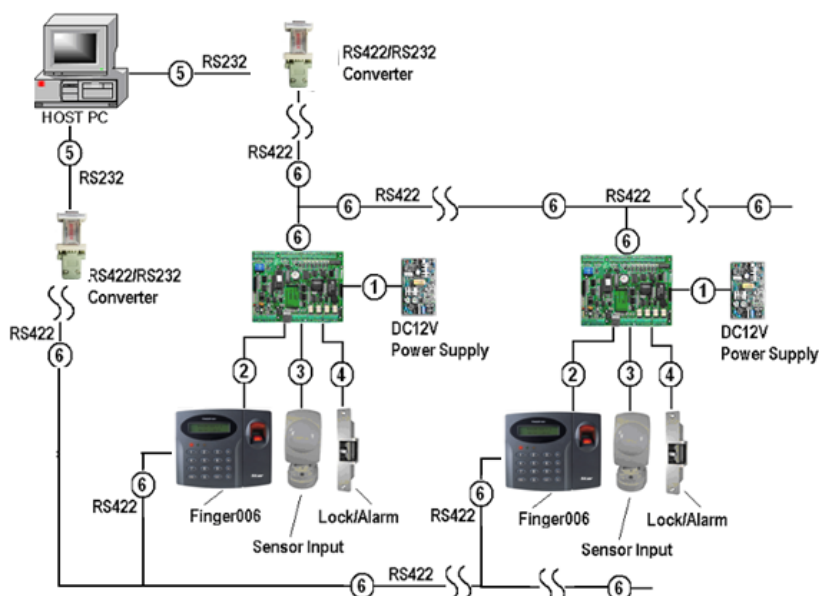
Installing the Star FINGER006/ iPASS IP-FINGER006 / IDTECK FINGER006SR is an easy task. It can be installed with common hand tools and readily available communications wires.

This section provides information about wiring, wire runs and other information to make the installation quick and easy.

1 Check Points before Installation

1.1 Selection of Cable

System installation cabling will be configured as follow:



1.2 Recommended Cable Type and Permissible Length of Cable

Reference	Description	Cable specification
1	Controller Power (DC12V) DC Power → Controller	Belden #9409, 18 AWG 2 conductor, unshielded
2	Reader (Power and Data) Finger006 → Controller	Belden #9512, 22 AWG 4 conductor, shielded Belden #9514, 22 AWG 8 conductor, shielded
3	Door Contact Exit Button Sensor Input Input → Controller	Belden #9512, 22 AWG 4 conductor, shielded Belden #9514, 22 AWG 8 conductor, shielded
4	Door Lock, Alarm Device Lock (Alarm) → Controller	Belden #9409, 18AWG 2 conductor, unshielded
5	RS232 Cable Converter → Host P.C.	Belden #9829, 24 AWG 2-twisted pair, shielded
6	RS485 Cable Controller → Converter Controller → Controller Controller → Finger006 Finger006 → Finger006 Finger006 → Converter	Belden #9829, 24 AWG 2-twisted pair, shielded
	S422 Cable Controller → Converter Controller → Controller Controller → Finger006 Finger006 → Finger006 Finger006 → Converter	Belden #9830, 24 AWG 3-twisted pair, shielded



Thicker wires are necessary if the connected reader consumes a higher current.

2 Check Point during Installation

2.1 Termination Resistor

Termination resistors are used to match impedance of the network to the impedance of the transmission line being used. When impedance is mismatched, the transmitted signal is not completely absorbed by the receiver and a portion of signal is reflected back into the transmission line.

The decision whether or not to use termination resistors should be based on the cable length and data rate used by the communication system.

For example, if you use 9,600 baud rate and 1,200m length of cable, the propagation velocity of cable is 0.66 x speed of light (This value is specified by the cable manufacturer), if we assume the reflections will damp out in three round trip up and down the cable length, the transmitted signal will stabilize 18.6 μ s after the leading edge of a bit. Since the data bit is captured in the middle of the bit which is approximately 52 μ s after the leading edge of a bit. The reflection stabilizing time 18.6 μ s is much before the center of the bit therefore the termination resistors are not required.

However, if you install the cable to maximum length, the impedance of cable and network is mismatched and the transmitted signal is overlapped by the reflected signal. In this case, it is recommended to add termination resistors to the end of the receiver lines. A 120 Ω resistor can be used for termination resistor in parallel between the receiver lines "A" and "B" for 2 wires RS485 system or "RX+" and "RX-" for 4 wires RS422 system. A termination resistor of less than 90 Ω should not be used and no more than 2 terminations should be used in one networking system.

2.2 How to Connect Termination Resistors

Termination Resistors for 2-Wire RS485 Communication System





2.3 Grounding System for Communication Cable

We recommend using proper grounding system on the communication cable. The best method for grounding system is to put the shield wire of the communication cable to the 1st class earth grounding; however it is not so easy to bring the earth ground to the communication cable and also the installation cost is raised.

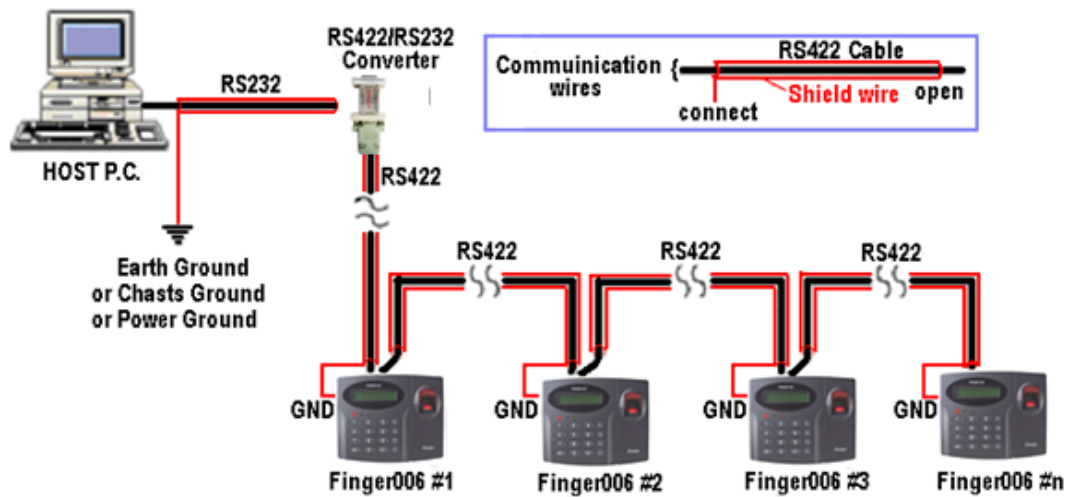
There will be three grounding points where you can find during installation;

- Earth Ground
- Chassis Ground
- Power Ground

The most important point for grounding system is not to connect both ends of shield wires to the grounding system; in this case there will be a current flow through the shield wire when the voltage level of both ends of shield wire is not equal and this current flow will create noise and interfere to communications.

For the good grounding, we recommend to connecting ONLY one end of shield wire of communication cable to the grounding system; If you find earth ground nearby, then connect one end of shield wire to earth ground; If you do not have earth ground nearby, then find chassis ground and connect one end of shield wire to chassis ground; If you do not find both earth ground and chassis ground, then connect one end of shield wire to power ground. (GND of FINGER006)

Note that if the chassis ground is not properly connected to the earth and floated from the ground level, then grounding to the chassis ground will give the worst communication; in this case we recommend to using power ground instead of chassis ground.



Installation of the Product

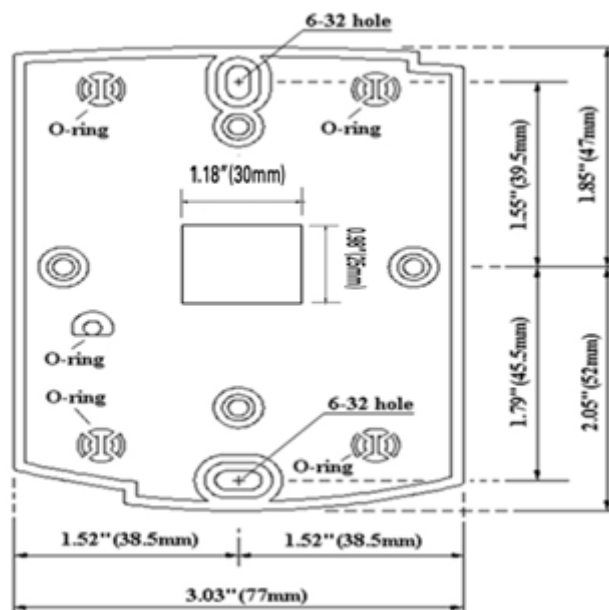
8

1 Template

1. Tear off the Template page at the back of this manual and use the Template to drill two 6-32 holes and one $\frac{1}{2}$ " hole on the proper location of the wall to mount the Wall Mount bracket as shown below.



If the gang box is installed on the wall, skip this step.



2. Using 2 screws, install wall mount to the wall.
3. Insert 5 O-Rings to the Wall Mount as indicated, then run the cable from the main unit through the center hole and snap in place the main unit to Wall Mount. Make sure that the main unit is secure locked in place with Wall Mount.



Before mounting the Star FINGER006 / iPASS IP-FINGER006 / IDTECK FINGER006S R unit to the Wall Mount bracket, an operational test of the unit should be completed, because the locking pins will lock the unit to the Wall Mount.

Removing the unit from the Wall Mount bracket after it has been snapped in place may cause damage to the bracket and prevent reattachment.

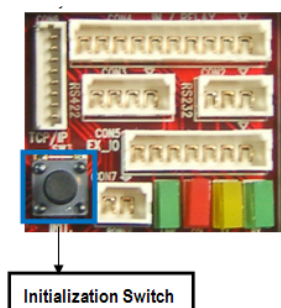
2 System Initialization

You have to initialize the FINGER006 unit prior to first installation.

Once power is supplied to the FINGER006, press the initialization switch in the back of the FINGER006 for more than 2 seconds. If you want initialization, press key <1> otherwise press key <0>.



- 1 Press the key <1> if you wish to initialize the system.
- 2 Initialization is progressing
- 3 Rebooted automatically after Initialization.





If you initialize the system by the method described above, all setting values will be cleared including Board ID.

Besides the method described above, there is one more method for system initialization, which is by entering setting menu. In this case all setting values will be cleared except Board ID. If you want to know details, please refer to '12.1.2 Communication Address Setting'

3 Wiring

3.1 Power

- Connect the (+) wire of DC 12V power to the +12V port (Red).
- Connect the GND (-) wire of DC 12V power to the GND port (Black).

3.2 Output Connections

Wiegand Data Connection

- Connect Data 0 wire of the controller to Wiegand Data 0 Out wire (Orange with White Stripe).
- Connect Data 1 wire of the controller to Wiegand Data 1 Out Wire (Brown with White Stripe).
- If you disconnect the power from the FINGER006, connect the GND port between controller and FINGER006.

Control Signal Connection

- Connect Error input wire of the controller to Error Signal Out wire (Blue with Red Stripe).
- Connect Ok input wire of the controller to OK Signal Out wire (Green with Red Stripe).
- Connect Error output wire of the controller to Error Signal In wire (Green with White stripe).
- Connect Ok wire output of the controller to OK Signal In wire (Green).
- Connect Tamper input wire of the controller to Tamper Switch Out wire (Yellow with White stripe).

External Reader Connection [Wiegand Input]

- Connect Data 0 wire of the external reader to Wiegand Data 0 In (EX) wire (Pink).
- Connect Data1 wire of the external reader to Wiegand Data 1 In (EX) wire (Cyan).



If you disconnect the power from the external reader, connect the GND port between external readers.

1 RS232 Communication Port Connection

A 9-pin connector (Serial communication connector, female) is required to connect the FINGER006 to a host computer via RS232 communication. Please follow the instructions.

- Connect RS232-TX port of FINGER006 to the pin 2 of the 9-pin connector.
- Connect RS232-RX port of FINGER006 to the pin 3 of the 9-pin connector.
- Connect RS232-GND of FINGER006 to the pin 5 of the 9-pin connector.
- Plug in the 9-pin connector to COM1 or COM2 Port of the host PC.
- Install and run FINGER006 Application Software.

2 RS422 Communication Port Connection

2.1 RS422 Connection (Single FINGER006 Connection)

RS422/RS232 converter (INC400) is required to use RS422 communication between the FINGER006 and a host computer. Please follow the instructions.

- Connect RS422-TX(+) (Gray wire) of the FINGER006 to RS422-RX(+) port of the converter.
- Connect RS422-TX(-) (Yellow wire) of the FINGER006 to RS422-RX(-) port of the converter.

ter.

- Connect RS422-RX(+) (Brown wire) of the FINGER006 to RS422-TX(+) port of the converter.
- Connect RS422-RX(-) (Blue wire) of the FINGER006 to RS422-TX(-) port of the converter.
- Plug in the RS232 9pin connector of the converter to the COM1 or COM2 Port of the PC.
- Install and run the FINGER006 Application Software.

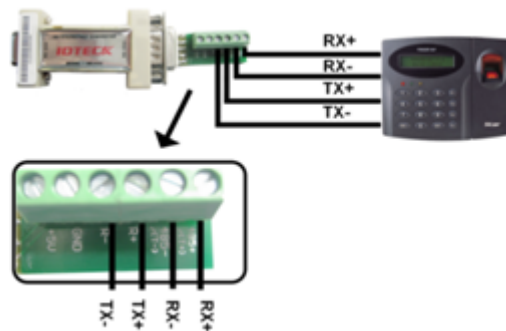
< A Type >

INC400	Unit(RS422)
WHITE	RX+
RED	RX-
BLUE	TX+
BLACK	TX-



< B Type >

INC400	Unit(RS422)
485-/(T-)	RX-
485+/(T+)	RX+
R+	TX+
R-	TX-

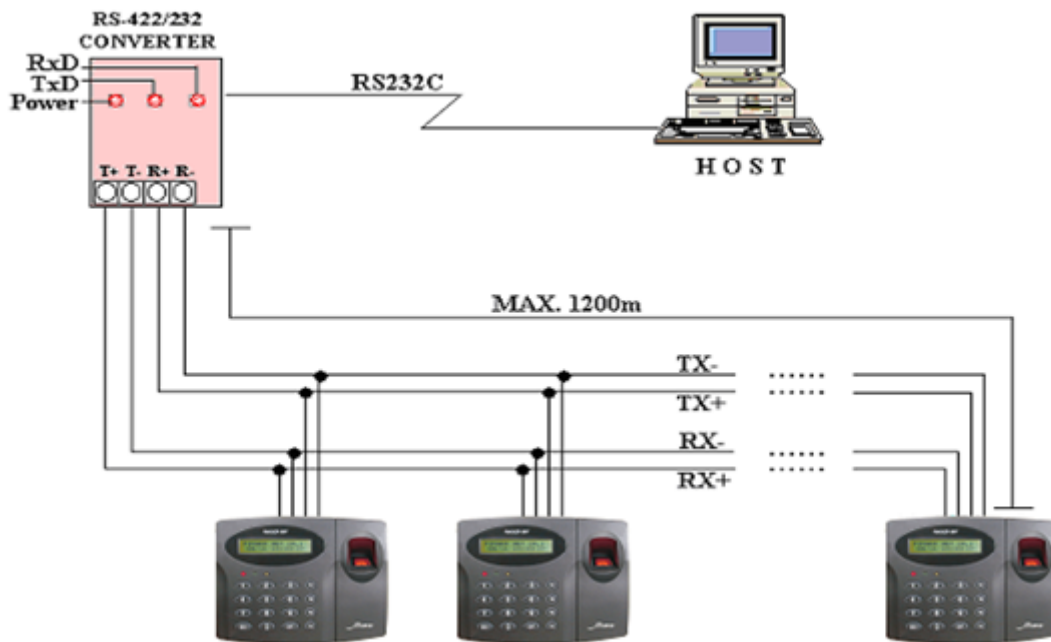


2.2 RS422 Connection (Multiple FINGER006 Connections)

RS422/RS232 converter is required to use RS422 communication between multiple FINGER006 units and a host PC. Please follow the next instructions.

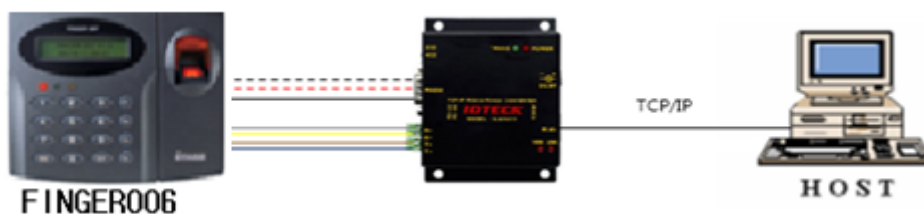
1. First, you have to connect all RS422 port of all FINGER006s in parallel.
 - I. Connect RS422-TX(+) of one FINGER006 to RS422-TX(+) of another FINGER006.
 - II. Connect RS422-TX(-) of one FINGER006 to RS422-TX(-) of another FINGER006.
 - III. Connect RS422-RX(+) of one FINGER006 to RS422-RX(+) of another FINGER006.
 - IV. Connect RS422-RX(-) of one FINGER006 to RS422-RX(-) of another FINGER006.
2. Second, you have to connect one of RS422 port of FINGER006 to RS422/RS232 converter.
 - I. Connect RS422-TX(+) of the one FINGER006 to RX(+) port of the converter.
 - II. Connect RS422-TX(-) of the one FINGER006 to RX(-) port of the converter.

- III. Connect RS422-RX(+) of the one FINGER006 to TX(+) port of the converter.
- IV. Connect RS422-RX(-) of the one FINGER006 to TX(-) port of the converter.
- V. Plug in the RS232 9pin connector of the converter to the COM1 or COM2 port of the PC.
- VI. Install and run FINGER006 Application Software.



3 TCP/IP Converter (External Version)

When you use the TCP/IP converter, choose only one converter between RS232 and RS422.



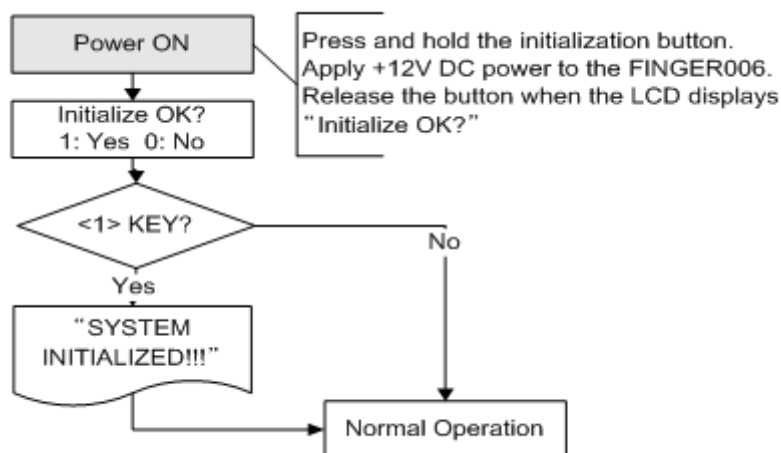
INTERFACE	FINGER006	ILAN422	LINE COLOR
RS232	TX (CON2)	RX (RS232 DSUB9)	BLACK+WHITE
	RX (CON2)	TX (RS232 DSUB9)	RED + WHITE

INTERFACE	FINGER006	ILAN422	LINE COLOR
RS422	GND(CON2)	GND	BLACK
	TX+ (CON3)	X+ (RS422 CONNECTOR)	GRAY
	TX- (CON3)	RX- (RS422 CONNECTOR)	YELLOW
	RX+ (CON3)	TX+ (RS422 CONNECTOR)	BROWN
	RX- (CON3)	TX- (RS422 CONNECTOR)	BLUE

1 Initialization of FINGER006

You must initialize the system prior to first installation or when you can't get into setting mode because of malfunctions etc.

Once power is supplied to the FINGER006, press the initialization switch in the back of the FINGER006 unit. Then, the LCD will first display "Initialize OK? 1: Yes 0: No". Press <1> key if you want to initialize the system or <0> to cancel the initialization procedure. After all the initialization process is completed, the system will be operating in the normal mode and the LCD will display "FINGER006 [F1], MM/DD hh : mm : ss".

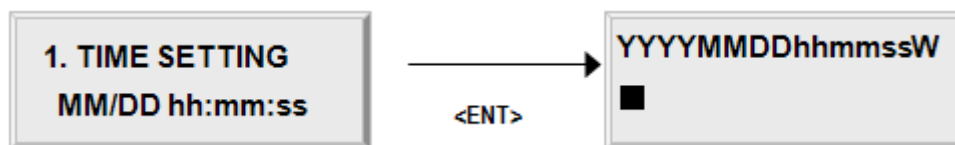


2 How to Enter the Setup Menu

For a setup or FINGER006 setting adjustment, you have to enter the SETUP MENU, first. To do so, press the <0> key 8 times for Master ID (Default “00000000”) and the user can get into the SETUP MENU. There are 4 main SETUP MENUs and you first get into [SETUP MENU F1]. You can move to other SETUP MENUs by pressing <F1> key for [SETUP MENU F1], <F2> key for [SETUP MENU F2], <F3> key for [SETUP MENU F3], and <F4> key for [SETUP MENU F4]. There are several SUB MENUs for each main SETUP MENU and you can scroll up and down the SUB MENU by pressing <4> and <6> key in the main SETUP MENU. You can press the <ESC> key to exit the SETUP MENU and return to the normal operation. You can also change the Master ID in the [SETUP MENU F1]. The Master ID for FINGER006SR is a 10-digit number (Default “0000000000”).

3 Time / Date Setting

After you enter the Setup Mode, you will see the following screen with the current date and time. To adjust the time / date setting, press <ENT>, then enter 15 Digits in a YYYYMMDDhhmmssW format, and then enter <ENT> again to confirm.



For the days of the week (W), 1 : Sun, 2 : Mon, 3 : Tue, 4 : Wed, 5 : Thu, 6 : Fri, 7 : Sat.

e.g. To input August 24, 2009, 13:30:15, Monday, enter 200908241330152.

4 Maximum Number of Cardholder IDs

By default, the FINGER006 is set to store up to 10,000 cardholders and 50,000 events and User can't change Maximum Number of Cardholder IDs because FINGER006 doesn't have the controller inside.

5 Registering Cardholder IDs

To add new cardholder IDs to the FINGER006, enter the Setup Mode (See 10.2 How to Enter Setup Mode), press <F3>. Once the 1.ID registration item appears on the LCD, press <ENT> to begin the ID registration process.

For detailed information on the ID registration process, please refer to "Setting Changes>F3 Setup Menu>Registration".



How to place your finger onto the scanner:

When you register or verify your fingerprint, please place your finger onto the scanner correctly as illustrated below.

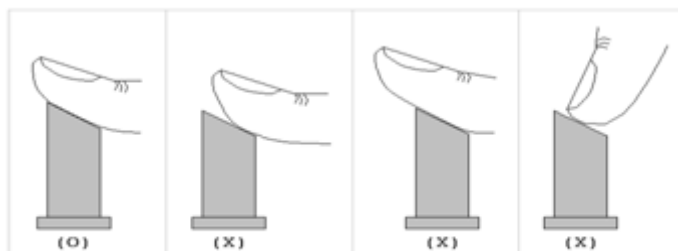


Figure: How to Put Your Finger on the Scanner

1 Normal Operation

Power On

When the power is applied to FINGER006, the “RED LED” is turned on.

Fingerprint Identification

1. If registered card is read by the unit, red LED of fingerprint sensor is on. At this time, you should put your finger and then remove your finger if red LED is off.
2. If fingerprint identification is done, card ID or authorization status appears on the

LCD.

If access has granted by fingerprint, Low Active is generated from OK output wire for 500ms. (Default)

Registered Card Reading

When a registered card (or PIN) is read, the door will open for 3 seconds (Defaults) with the “GREEN LED” on.

Alarms (Unregistered / Password / Fingerprint)

When an unregistered card is read, wrong password is input, wrong fingerprint is input, the access is denied and the alarm will be activated for 3 seconds (Defaults) with “RED LED” on.

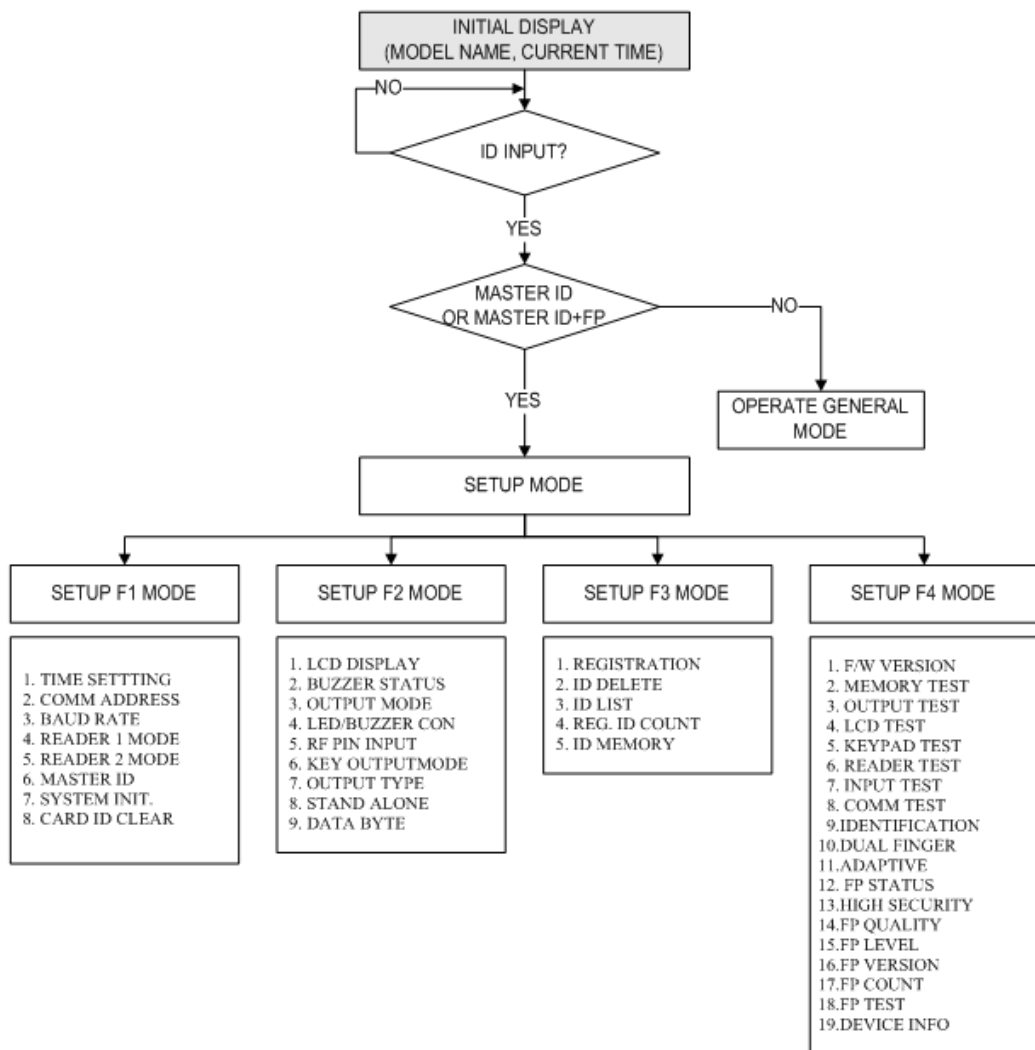
LED turns on for 3 seconds then Low Active is generated from error output wire for 500ms. (Default)

2 Default Setting

When you operate the FINGER006 first time or you initialize the FINGER006, the FINGER006 will set up all values to default settings (Factory Settings). You can change the settings for desired application. Please refer to the “APPENDIX” section at the back of this manual for the default setting values.

Setting Changes

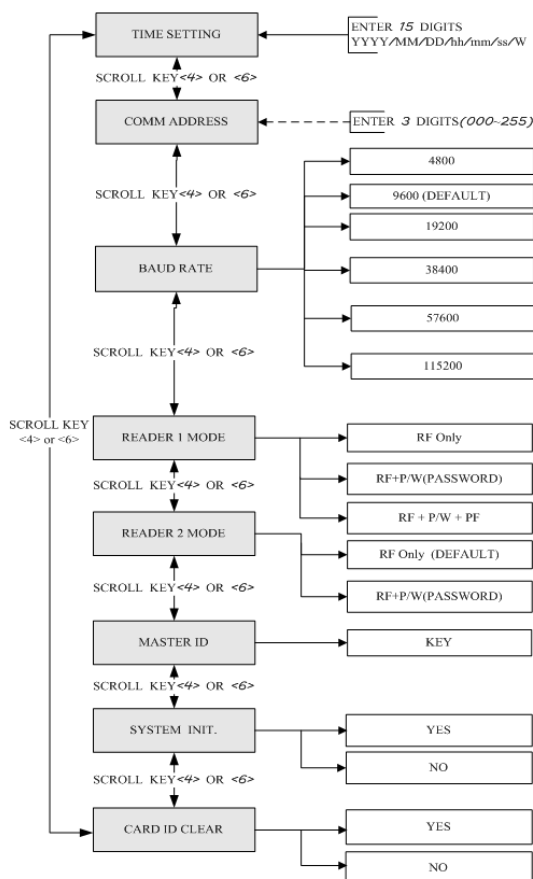
12



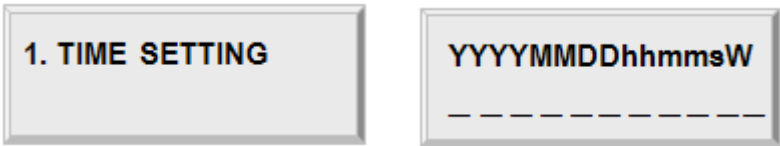


To setup or to change the FINGER006 settings, you have to enter the setup mode first. To do so, enter the Master ID (Default=00000000)* ¹ and press the <ENT> key. There are 4 main Setup menus and you automatically get into “SETUP MENU F1” first. You can move to other setup menus by pressing the <F1> key for “SETUP MENU F1”, <F2> key for “SETUP MENU F2”, <F3> key for “SETUP MENU F3” and <F4> key for “SETUP MENU F4”. There are setting items in the main setup menu and you can scroll up or down the menu by pressing the <4> or <6> key. If you press the <ESC> key then the FINGER006 will exit the Setup Mode and return to normal operation in Reader Mode.

1 Setup Menu F1



1.1 Time Setting

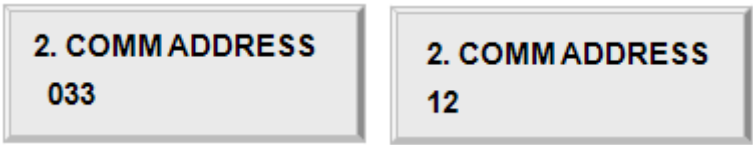


The LCD displays the current time. To change the time, press <ENT>, enter 15 Digits in a “YYMMDDhhmmssW” format, and then enter <ENT> again to confirm.



NOTE: For the days of the week (W),
1 : Sun, 2 : Mon, 3 : Tue, 4 : Wed, 5 : Thu, 6 : Fri, 7 : Sat.
e.g. To input August 24, 2009, 13:30:15, Monday,
enter 200908241330152.

1.2 Communication Address



A communication address is a unique number assigned to each device for communication. The default address is 033.

For proper communication with the PC, it is important that the value you set here should match the value you set on the application software. It is also important to make sure each device on a loop has a unique address.

To change the communication address of the FINGER006, press <ENT>, enter the desired 3-Digit address in the 000-255 range, and then press <ENT> again to confirm.



Comm Address setting depending on application software

1. When using STARWATCH DUAL PRO I, II: Set COMM ADDRESS from “033” to “255”
2. When using STARWATCH iTDC PRO I, II: Set COMM ADDRESS from “128” to “255”

1 The default Master ID for the FINGER006SR is 0000000000 (Press the <0> key 10 times)

55”

3. When using STARWATCH STANDARD: Set COMM ADDRESS from “1” to “255”

1.3 BAUD RATE



Baud Rate is the measure of speed in serial communication. As for the communication address, the baud rate you set here should match the value you set on the software.

Baud Rates of 4800bps, 9600bps, 19200bps, 38400bps, 57600bps and 115200bps are supported, and 9600bps is recommended.

To change the Baud Rate, press <ENT>, select the desired baud rate by pressing <4> or <6>, and then press <ENT> again to confirm.



If a TCP/IP module is being used, the Baud Rate setting must be the same as the TCP/IP module setting.



Troubleshooting Communication Problems

Step 1. Match the communication address between the device and the Application Software.

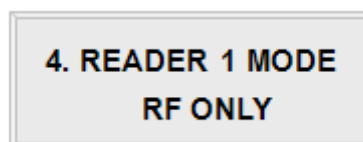
Step 2. Match the Baud Rate between the device and the Application Software.

Step 3. Ensure that the COM port setting in the Application Software is correct.

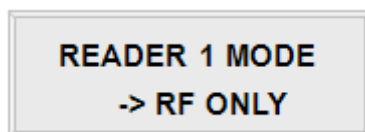
Step 4. Ensure that the communication settings in the Application Software are as follows;

1) Parity Bit: None 2) Data Bit: 8 Bits 3) Stop Bit: 1 Bit

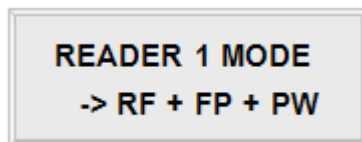
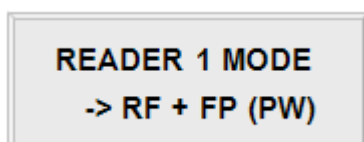
1.4 Reader1 Mode



You can decide which combination of RF card, fingerprint and password verification you wish to use on Reader1 (the FINGER006 device itself).



To change the Access Mode for Reader 1, press <ENT>, select the “DESIRED MODE” by pressing <4> or <6>, and then press <ENT> again to confirm.



RF ONLY

Users can access the door by presenting their card or entering their ID number.

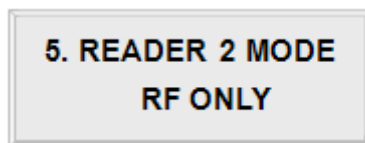
RF+F/P (P/W)

Users can access the door by presenting their card or entering their ID number and then verifying their identity by a fingerprint. For users who did not register their fingerprints, password verification is used instead of fingerprint verification.

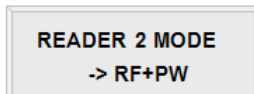
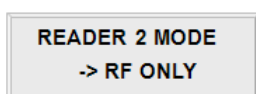
RF+P/W+F/P

Users can access the door by presenting their card or entering their ID number and then verifying their identity by both a fingerprint and a password.

1.5 Reader 2 Mode



If you have an external reader connected to the FINGER006 (referred to herein as Reader 2), you must adjust this setting according to what access mode is used on Reader 2.



To change the Access Mode for Reader 2, press <ENT>, select the desired mode by pressing <4> or <6>, and then press <ENT> again to confirm.

RF ONLY

Select this option if Reader 2 is operating without password verification

RF+ P/W

Select this option if Reader 2 uses password verification.



Proper selection of this setting depends solely on whether Reader 2 uses password verification, but it has nothing to do with whether Reader 2 uses fingerprint verification or not

1.6 Master ID Registration

6. MASTER ID	ENTER MASTER ID —	ID: 25512345 PW: FP:
TO REGISTER FP PUT YOUR FINGER!	REGISTRATION OK!	

Master ID is the number/card that you use to enter the Setup Mode. For security reasons, it is advisable that you change the default Master ID immediately and keep the new Master ID / card confidential.



Beware that if you forget the Master ID, you cannot access the Setup Mode.

To change the Master ID, press <ENT>, and then either enter the desired 8Digit Master ID or present a card to the reader.



For the FINGER006SR, the Master ID is 10Digits long in the range of 0000000000 to 4294967295.

On the next screen, enter the desired 4Digit Master Password in the PW field and, in the FP

field, enter <0> if you wish to access Setup Mode without master fingerprint verification or <1> if you wish to use master fingerprint, in which case you will be asked to place your fingerprint on the scanner twice in the next step. When the Master ID/card registration is successfully completed, the LCD displays the “REGISTRATION OK” message.



The default Master ID for FINGER006 and IP-FINGER006 is 00000000 (Eight zeros), but for the FINGER006SR, it is 0000000000 (Ten zeros)

1.7 System Initialization

7. SYSTEM INIT .

System initialization allows you to initialize the FINGER006. Initialization clears all the user-defined data stored in the device such as card data, input/output setting, Time Schedules, etc.



Prior to system initialization, make sure to check whether or not the data stored in the device is not needed, since it will be deleted after the initialization.

SYSTEM INIT.

1 – Yes, 0 - No

WAITING !!

To initialize the FINGER006, press <ENT>, and then press <1> to confirm. If you wish to cancel and exit without initialization, press <0> instead.

1.8 Card ID Clear

8. CARD ID CLEAR

CARD ID CLEAR

1 - Yes, 0 - No

Card ID clear allows you to delete all the card data from the FINGER006. To clear the card d

ata stored in the memory, press <ENT>, and then press <1> to confirm. If you wish to cancel and exit, press <0> instead.



Before you clear the card memory, make sure you do not need the data stored in the device.

1.9 Event Clear

9. EVENT CLEAR

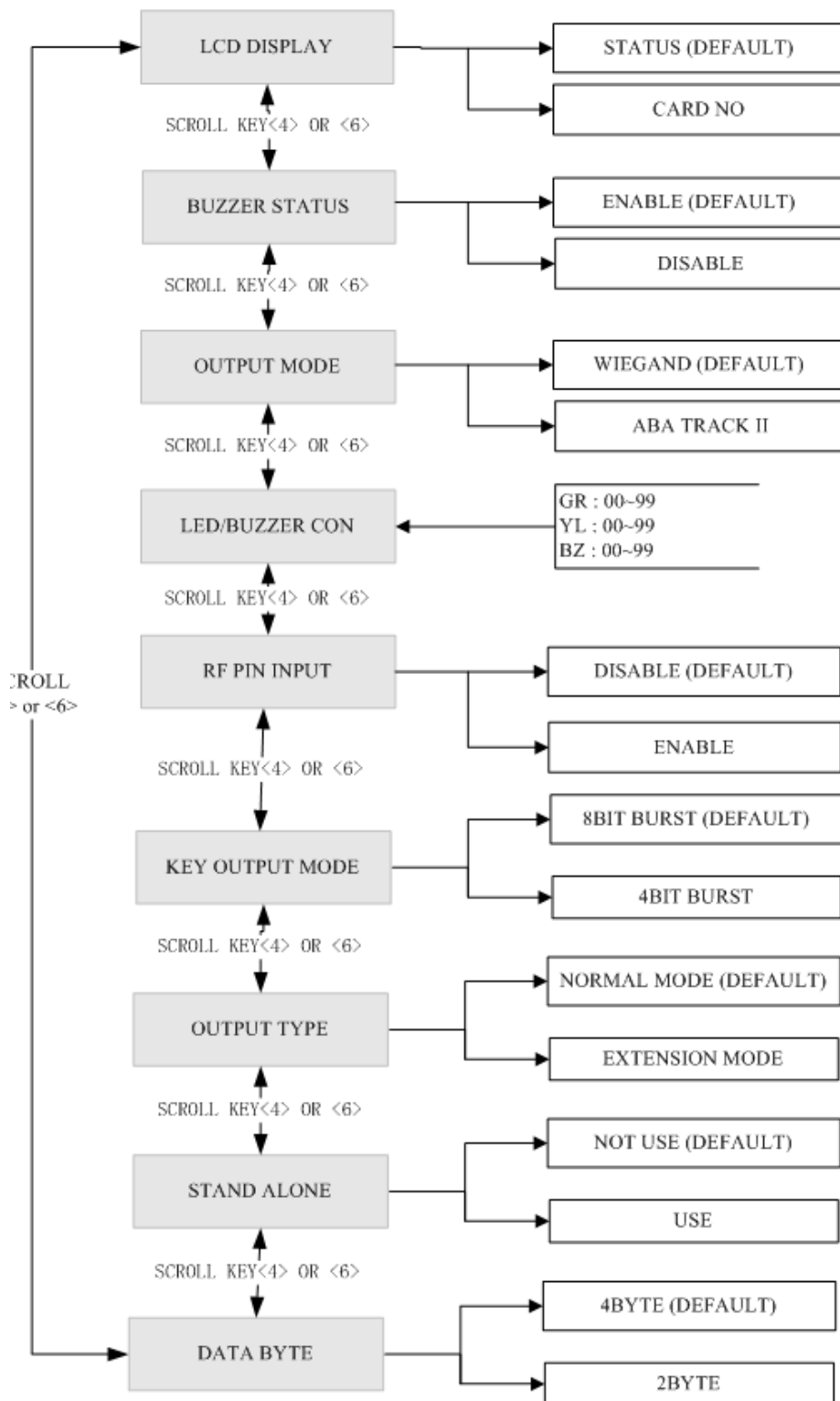
EVENT CLEAR
1 - Yes, 0 - No

Event clear allows you to delete all the event data from the FINGER006. To clear the event data stored in the memory, press <ENT>, and then press <1> to confirm. If you wish to cancel and exit, press <0> instead.



Before you clear the event memory, make sure you do not need the data stored in the device.

2 Setup Menu F2



2.1 LCD DISPLAY



LCD DISPLAY allows you to decide whether to display the card number or the status message on the LCD when access is granted or denied.

STATUS

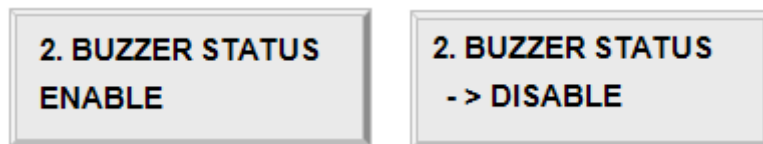
The LCD will display the text message indicating the status, i.e. “ACCESS GRANTED” or “ACCESS DENIED”

CARD NO

Display the number of the card.

To change the setting, press <ENT> and press <4> or <6> to select “STATUS” or “CARD NO” and press <ENT> to confirm.

2.2 BUZZER STATUS



The buzzer generates a beep when a button on the keypad is pressed, when a card is read, when an error occurs, etc.

To enable or disable the buzzer sound, press <ENT> and press <4> or <6> to select “ENABLE” or “DISABLE” and press <ENT> to confirm.



The buzzer beeps regardless of this setting, when you exit the Setup Mode, when a memory alarm is activated, or when Buzzer Output is defined in “In/Output Define”.

2.3 OUTPUT MODE



You can select the output format between WIEGAND or ABA TRACK.

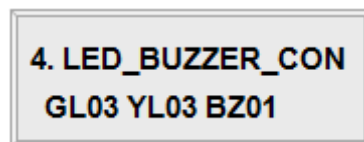
WIEGAND:

Outputs ID data through Wiegand output line.

ABA TRACK II:

Outputs ID data through ABA track output line.(Open collector)

2.4 LED_BUZZER_CONTROL



This function controls the LED and Buzzer of the reader.

GL (Green LED)

controls the card reading status.

YL (Yellow LED)

controls the error indication in case the user's card isn't authorized.

BZ (Buzzer)

It controls the buzzer sound.



e.g.) GL03 YL03 BZ01 : When card is presented to the unit, green LED indicator is lit for 3sec. If a user card isn't authorized, the yellow LED indicator is lit and the buzzer beeps for 1sec.

2.5 RF PIN INPUT

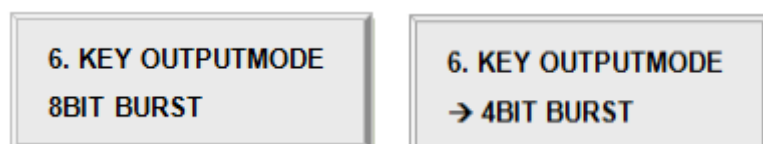


RF Pin Input allows you to decide whether to enable or disable PIN (or RF card number) Input via the keypad. If not configured, PIN Input is enabled by default.



If you choose “Disable”, you cannot gain access via password input when using RF +PW mode.

2.6 KEY OUTPUT MODE



You can change the Output Mode when you press function keys

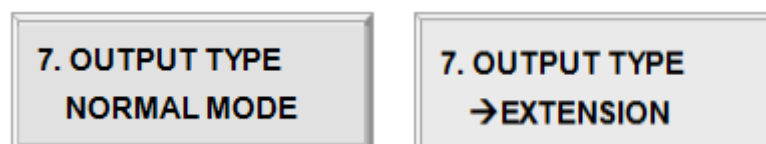
4BIT Burst

4bit burst will be output when you press function keys

8BIT Burst

8bit burst will be output when you press function key

2.7 KEY OUTPUT MODE



You can select the OUTPUT TYPE between NORMAL MODE and EXTENSION MODE.

NORMAL MODE

If a registered ID or/and a fingerprint is entered, FINGER006 outputs ID data only.

EXTENSION MODE

If an ID or/and a fingerprint is entered, FINGER006 outputs OK or ERROR signal and ID data.

2.8 STAND ALONE



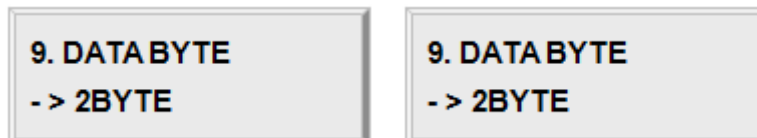
You can choose whether to use a standalone function or not by using <4> or <6> key. After changing set values, press <Enter>key to save the changed values

When the controller is waiting for the verification signal, LCD shows “RD CERTIFYNG” message.



When you select “USE”, FINGER006 waits for a reply of a controller. But if there is no reply after a lag, verification process is denied. (Default is <NOT USE>)

2.9 DATA BYTE (FINGER006SR ONLY)



This feature only applies to FINGER006SR.

By default, the FINGER006SR can read smart card written in the 4BYTE format, but, for advanced applications, you can use 2BYTE format smart cards. To do so, you must change the Data BYTE setting to “2BYTE”. To change the setting, press <ENT> and press <4> or <6> to select “4BYTE” or “2BYTE” and press <ENT> to confirm.

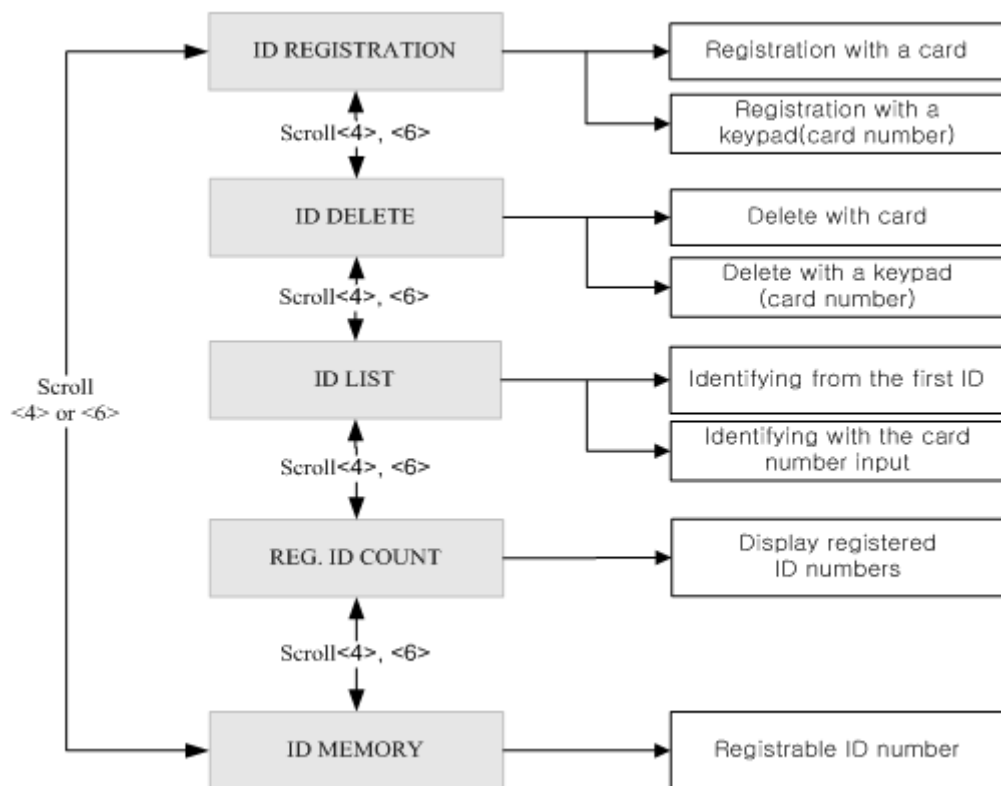


Range of Card Number (FINGER006SR Only)

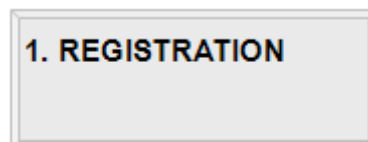
4 Byte (Default): The Card Number can be in the ranges of 00000000 - 4294967295

2 Byte: The first and last 5 digits can each be in the upper ranges of 00000 ~ 65535
5
lower ranges of 00000~65535
The total is in the ranges of 0000000000~6553565535

3 Setup Menu F3



3.1 ID Registration



Registration allows you to add new cardholders to the FINGER006. To add a new cardholder ID, press <ENT>.

ENTER ID NO.



Either present a card you wish to register to the FINGER006 or enter the card number (ID) via the keypad and press <ENT>.



A Card Number (ID) can be 4 to 8 Digits long. For the FINGER006SR, it can be 4 to 10 Digits long.

ID: ***(**)**

PW ____ TS __ RD _ FP

Once the Card Number is entered, enter the Password (PW), Time Schedule (TS), Reader Number (RD) and Use of Fingerprint (FP) and press <ENT>. For more information, see below.

**TO REGISTER F/P
PUT YOUR FINGER!**

If you have entered 1 in the FP field, the fingerprint scanner will be lit up. Then, place the cardholder's fingerprint on the scanner.

**LIFT AND
PUT YOUR FINGER!**

Once the light from the fingerprint scanner is turned off, lift the finger up and put it back on a while later.

**[Q1:3] [Q2:4]
REGISTRATION OK!**

If the registration is successful, the “REGISTRATION OK!” message will be displayed on the LCD. If you have registered the fingerprint, the quality score for the fingerprint will appear as shown on the left. If the registration is not successful, the “REGISTRATION ERR!” Message will be displayed on the LCD.

Description of Fields

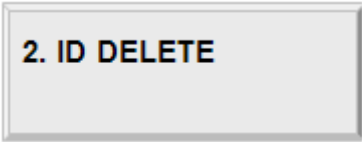
PW (Password)

Enter the 4Digit password. Password verification can be enabled in 11.1.4. Reader1 Mode. This field is compulsory even if you do not use password verification.

FP (Fingerprint)

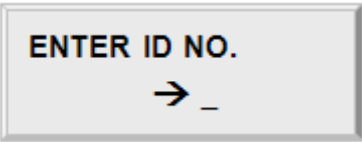
To register the cardholder’s fingerprint, enter 1. If you do not wish to register the cardholder’s fingerprint, enter 0.

3.2 ID Deletion



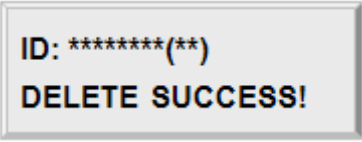
2. ID DELETE

ID Delete allows you to delete existing cards from the FINGER006. To delete an existing card (Or ID), press <ENT>.



ENTER ID NO.
→ _

Either present a card you wish to delete to the FINGER006 or enter the card number (ID) via the keypad and press <ENT>.



ID: ***(**)**
DELETE SUCCESS!

If the card was successfully deleted, the “DELETE SUCCESS!” message will be displayed on the LCD. If the card you presented or the card number you entered is not found, the “UNREGIS

TERED ID” message will be displayed.

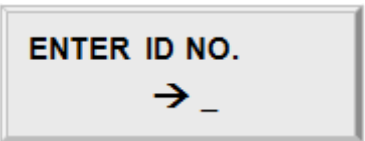
3.3 ID List

3. ID LIST

ID List allows you to search for a certain registered card or view the list of all registered cards. To begin, press <ENT>

3. ID LIST
1: CARD 2: FIRST

To search for a certain registered card, press <1>. To view the entire list of all registered cards, press <2>.



ENTER ID NO.
→ _

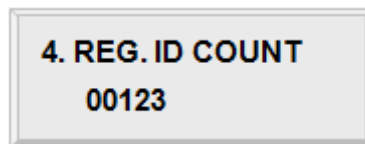
If you have entered <1>, enter the Card Number (ID) or present the card you wish to view the information of.



ID *****
PW1234 TS00 RD3

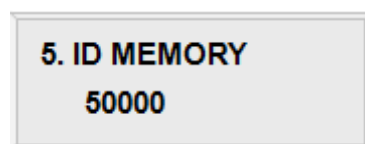
The LCD will show the information of the card you have selected in the previous step or the first card on the list. Press <4> or <6> to view the information of the previous or next card. The “FIRST ID” or “LAST ID” message will appear if you are viewing the first or last ID. If there is no card data, the LCD will display the “MEMORY EMPTY” message.

3.4 Registered ID Count



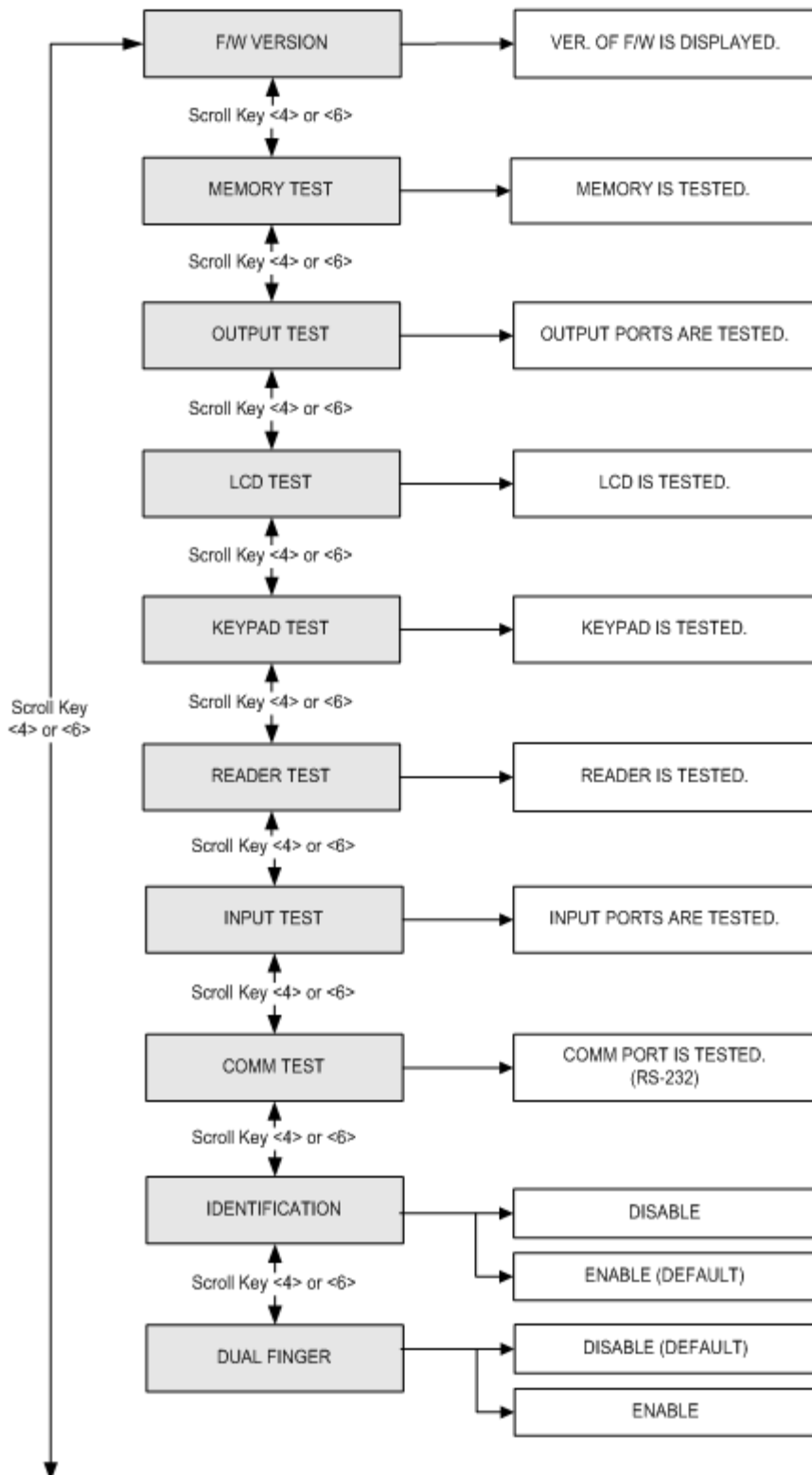
The number of registered user IDs is displayed. This count automatically increases or decreases as IDs are registered or deleted. The LCD on the left shows that the total of 123 user IDs are registered in the memory.

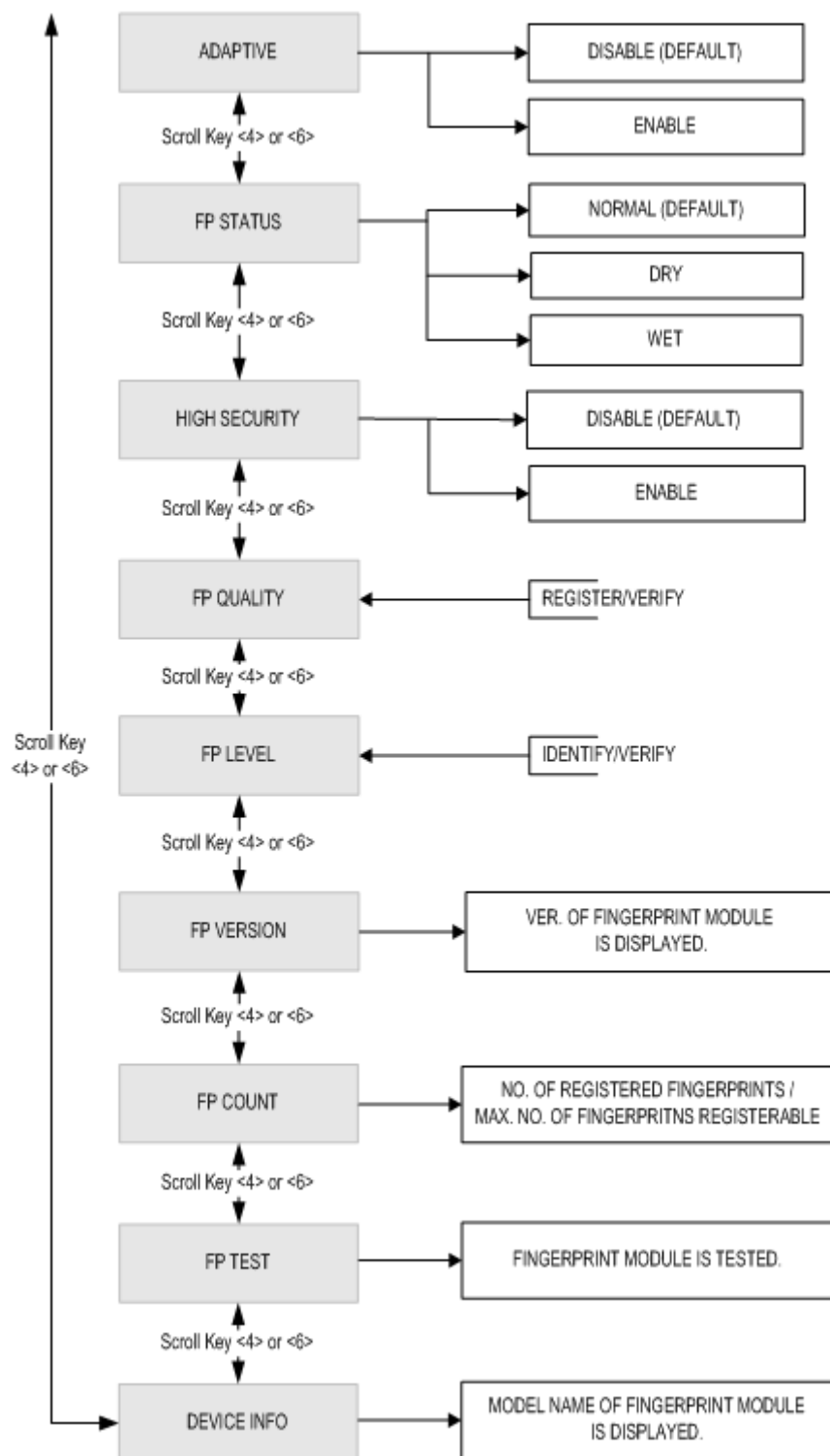
3.5 ID Memory



Show the maximum number of events where you can save.

4 Setup Menu F4



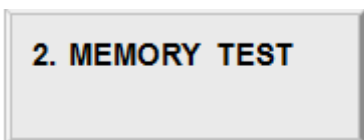


4.1 Firmware Version

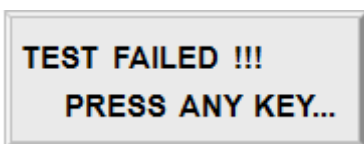


The version of the firmware installed in the FINGER006 is displayed on the LCD.

4.2 Memory Test

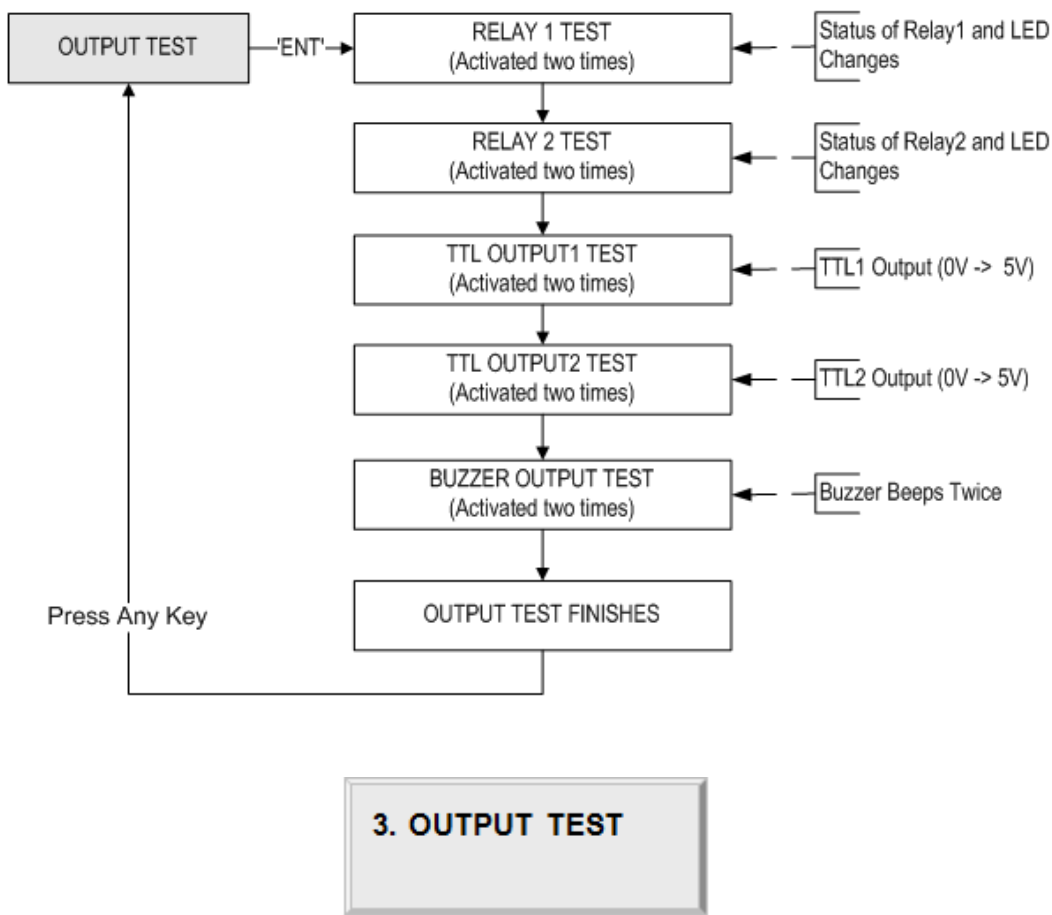


Memory Test allows you to test the memory of the FINGER006. To begin the test, press <ENT>.



If the test is successful, the LCD will display the "TEST PASSED" message. Press any key to finish the test. If the test is unsuccessful, the LCD will display the "TEST FAILED" message. Press any key to finish the test and try again. If the problem persists, please contact your local IDTECK dealer for assistance or service.

4.3 Output Test



Output Test allows you to test the output ports of the FINGER006. To begin the test, press <ENT>.



First, output ports1 and 2 will be tested. During the test, relay outputs are activated and you will hear Tick-Tack sounds with the green LED blinking twice. Second, output oorts3 and 4 will be tested. During the test, TTL outputs are activated and the yellow LED blinks twice. Yo u can check the voltage level of the TTL outputs with appropriate test equipment. Lastly, out put port 5 will be tested. During the test, you will hear 2 beeps. After all the tests are over, p res any key to exit.

4.4 LCD Test

4. LCD TEST

LCD Test allows you to test the LCD of the FINGER006. To begin the test, press <ENT>.

AAAAAAAAAAAAAAAA
CCCCCCCCCCCCCCCC

Once the test begins, the LCD will display a series of different screens. Ensure that all the screens on the LCD are properly displayed. The test ends with the display of the firmware update date (YYYY/MM/DD). After the test is finished, press any key to exit.

4.5 Keypad Test

5. KEYPAD TEST

Keypad Test allows you to test the keys on the keypad. To begin the test, press <ENT>.

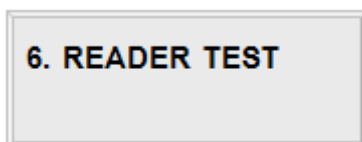
5. KEYPAD TEST
0123456789ABCDEF

Press each key on the keypad, then the number or letter that corresponds to the key pressed will disappear from the screen. After all the keys are pressed, the LCD displays the “TEST PASSED” message.

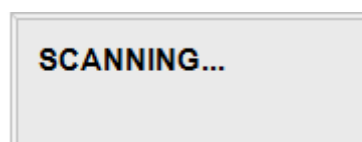


“A”=ESC, “B”=ENT, “C”=F1, “D”=F2, “E”=F3, “F”=F4

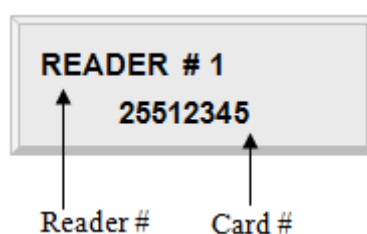
4.6 Reader Test



Reader Test allows you to test the reader(s). To begin the test, press <ENT>.



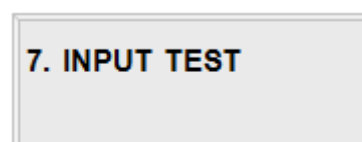
While the LCD displays "SCANNING", present a card to the reader you would like to test, and the LCD will display the reader number and the card number. After the test is finished, press <ESC> to exit.



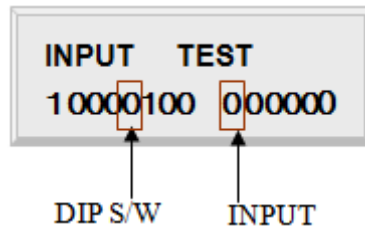
Reader#1 refers to the built-in reader of the FINGER006, and Reader #2 refers to an external reader.

You can also use Reader Test to check the number of a card.

4.7 Input / DIP Switch Test



Input Test allows you to check the status of Input Ports and DIP switches (Communication Address Setting Switches). To begin the test, press <ENT>.



DIP Switch

1=ON, 2=OFF (It shows how the DIP switch on the back of the FINGER006 is set.)

Input 1-4

0=OFF (Disabled)

1=ON (Enabled)

2=Input Disconnected

Input 5

The status of the tamper switch inside the FINGER006 (0=OFF (Disabled), 1=ON (Enabled))

Input 6

The status of the Proximity Sensor

(0=OFF (Disabled), 1=ON (Enabled))

4.8 Communication Test

8. COMM TEST

COMM Test allows you to test communication. Prior to the test, connect the RS232-RX wire (Black wire with White stripe) and the RS232-TX wire (Red wire with Black stripe) together. To begin the test, press <ENT>.

TEST Failed !!!
PRESS ANY KEY

If the test is unsuccessful, the LCD will display the “TEST FAILED” message. Press any key to finish the test and try again after powering the FINGER006 off and back on.

TEST PASSED !!!
PRESS ANY KEY

If the test is successful, the LCD will display the “TEST PASSED” message. Press any key to finish the test.

4.9 Identification Mode

9. IDENTIFICATION

IDENTIFICATION
→ ENABLE

Identification Mode is a feature that allows users to use just fingerprint verification without having to present their cards or enter their ID numbers. If this feature is enabled, a user can just place the fingerprint onto the fingerprint scanner, and then the FINGER006 will perform 1: N authentication for the entire fingerprint templates in the database and grant access if a fingerprint template that matches the user’s fingerprint is found.

4.10 Dual Fingerprint Mode

10. DUAL FINGER

DUAL FINGER
→ DISABLE

The Dual Fingerprint Mode allows one user to register two different fingerprints per ID. This feature is useful when a user’s finger is injured and wishes to use the other registered finger in the verification process.

DUAL FINGER	Number of Templates and Fingers	Authentication Success Ratio	Recommended Authentication Mode
NOT USE	2 Storage Templates for a single finger.	High	Identification Mode
USE	1 Storage Template each for 2 different fingers.	Low	Verification Mode

4.11 ADAPTIVE MODE



The Adaptive Mode is a feature that improves the quality of fingerprint images in the authentication process, guaranteeing a higher likelihood of successful authentication. However, the authentication process may take longer with this feature on.

To enable or disable the Adaptive Mode, press <ENT> and press <4> or <6> to select “ENABLE” or “DISABLE” and press <ENT> to confirm.

4.12 FP STATUS



FP Status is a special feature designed for special environments where the fingers of most employees might be too dry or wet. If you set the FP Status setting to dry or wet, the FINGER 006 will adjust the fingerprint images according to the environment to improve the authentication rate.

To change the setting, press <ENT> and press <4> or <6> to select “NORMAL”, “DRY” or “WET” and press <ENT> to confirm.

4.13 HIGH SECURITY 설정



High Security allows you to enable or disable the latent fingerprint image processing.



Since the image of a latent fingerprint and that of a dry fingerprint are both equally faint, it is hard to tell dry fingerprints from latent images. Therefore, enabling High Security will lower the recognition success rate of dry fingerprints as they might

be mistaken to be latent fingerprints.



In a place where many users have dry fingerprints, a better recognition success rate can be achieved by adjusting the exposure value higher and/or enabling Adaptive Mode.

4.14 FP QUALITY

14. FP QUALITY

REGISTER/VERIFY

40/30

Register Quality and Verify Quality are the threshold values for fingerprint image capture in the fingerprint registration enrollment process (Register Quality) and verification process (Verify Quality). If the quality value for a capture fingerprint image is below the Register Quality threshold, the authentication (registration or verification) is rejected. By adjusting the threshold value, you can control the desired level of fingerprint image quality.



If you want to change this function, please consult with IDTECK. Otherwise the recognition success rate is not guaranteed.

4.15 FP LEVEL

15. FP LEVEL

8/5

IDENTIFY/VERIFY

8/5

Verify / Identify Security Level is the threshold value for fingerprint authentication. By adjusting the setting value, you can achieve either a higher recognition success rate or a higher security level.



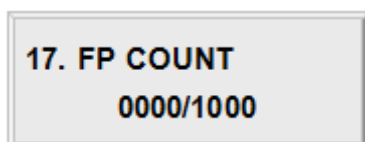
If you want to change this function, please consult with IDTECK. Otherwise the recognition success rate is not guaranteed.

4.16 Fingerprint Module Version



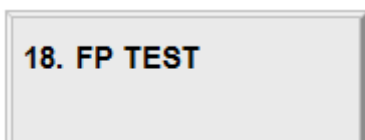
FP Version allows you to check the version of the fingerprint module on your FINGER006.

4.17 Fingerprint Count



FP Count allows you to see how many fingerprints are registered in your FINGER006 and how many can be registered in total. Depending on the specification of the fingerprint module in use, the total fingerprint capacity can be 1000, 2000 or 4000 fingerprints.

4.18 Fingerprint Module Test



FP Test allows you to test the fingerprint module on your FINGER006. To begin the test, press <ENT>. If the test is successful, the "TEST PASSED" message will be displayed. If the test is unsuccessful, the LCD will display the "TEST FAILED" message. If that is the case, try again. If the problem persists, please contact your local IDTECK dealer for assistance or service.

4.19 Fingerprint Device Information Check



Device Info shows you the model name of the fingerprint module on your FINGER006.

1 Default Values for Parameters

No	Parameter	Default Value
1	READER #1 Operation Mode	ID(RF), FP(PW)
2	READER #2 Operation Mode	ID ONLY
3	READER #1 Keypad Input Limit	USE
4	READER #2 Keypad Input Limit	USE
5	Output Mode	WEIGAND
6	Key Output Mode	8BIT BURST
7	Output Type	NOMAL MODE
8	LCD Display	STATUS

2 Output Format

2.1 26bit Wiegand Output Format

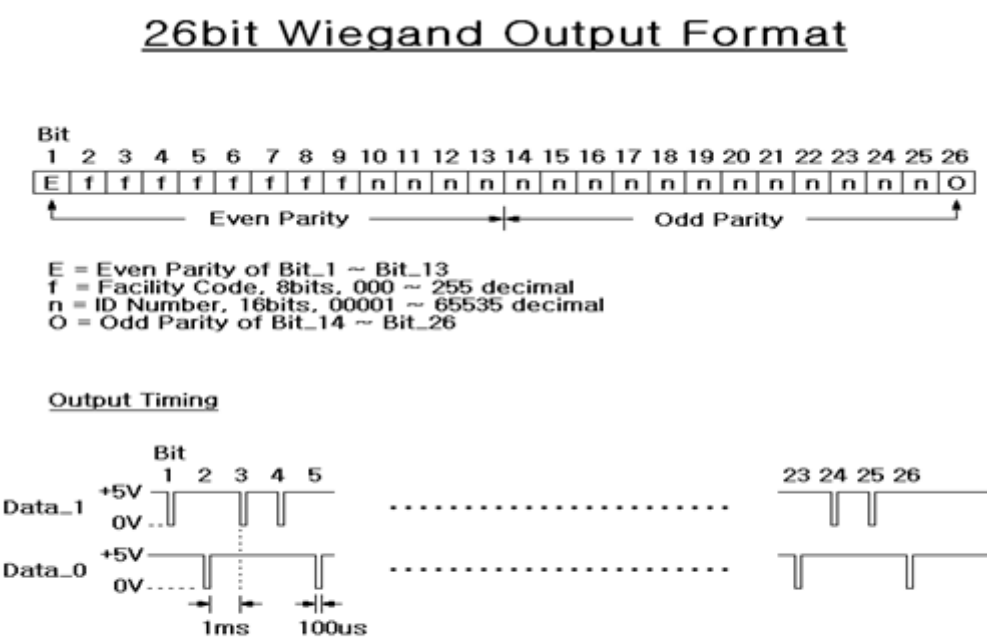
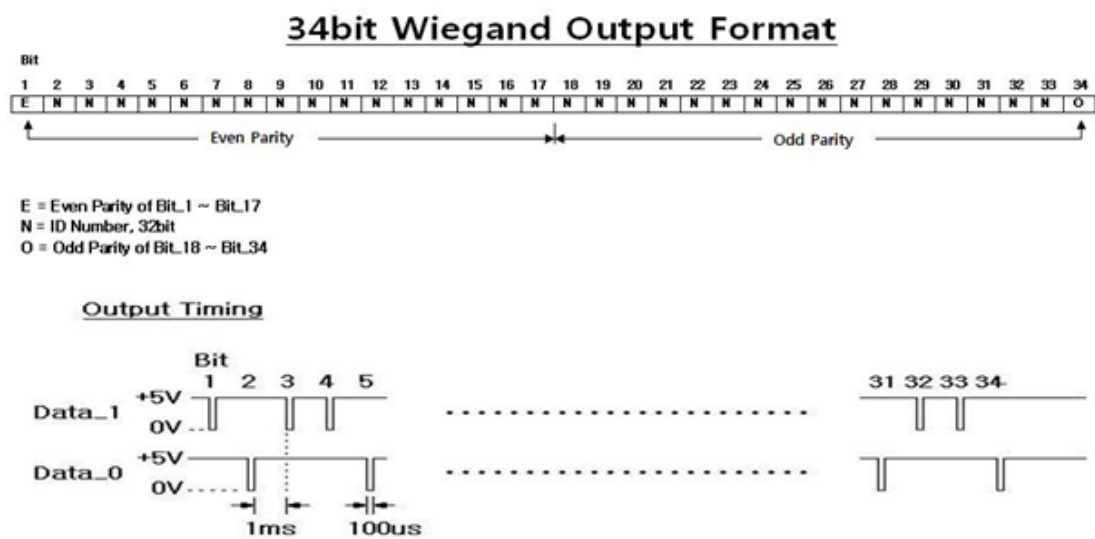


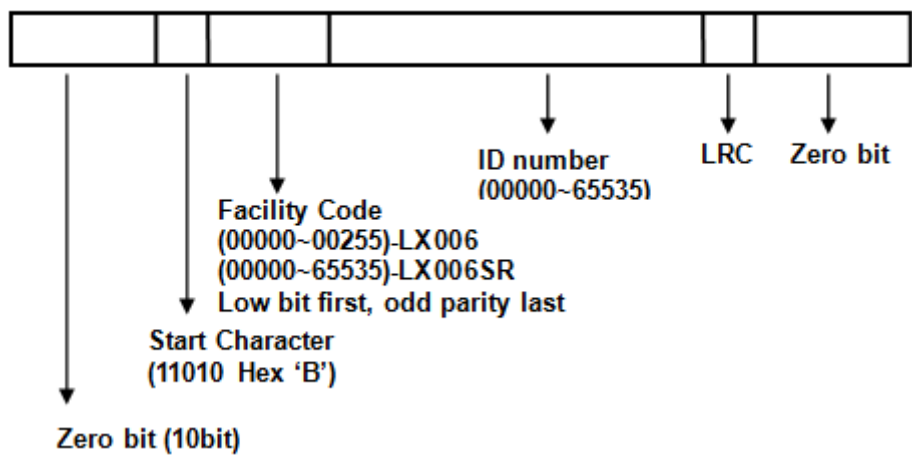
Figure: 26bit Wiegand Output Format

2.2 34bit Wiegand Output Format

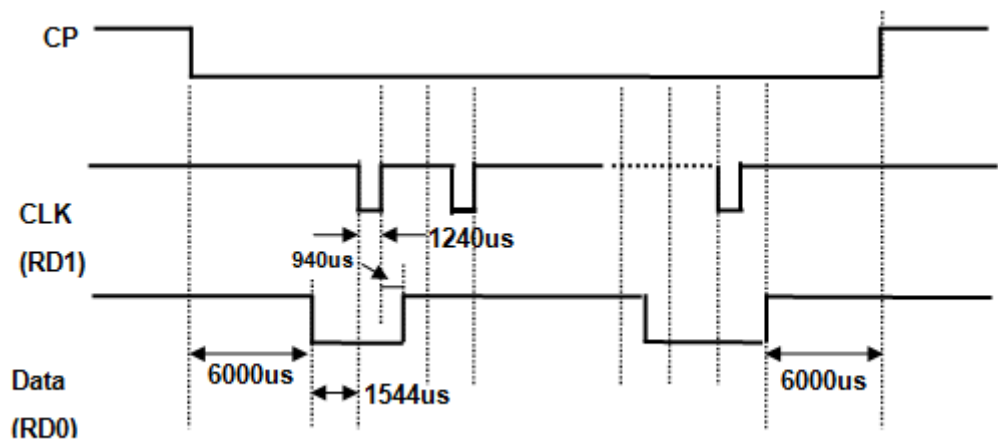


2.3 ABA TRACK II (SELECTABLE USING THE SOFTWARE)

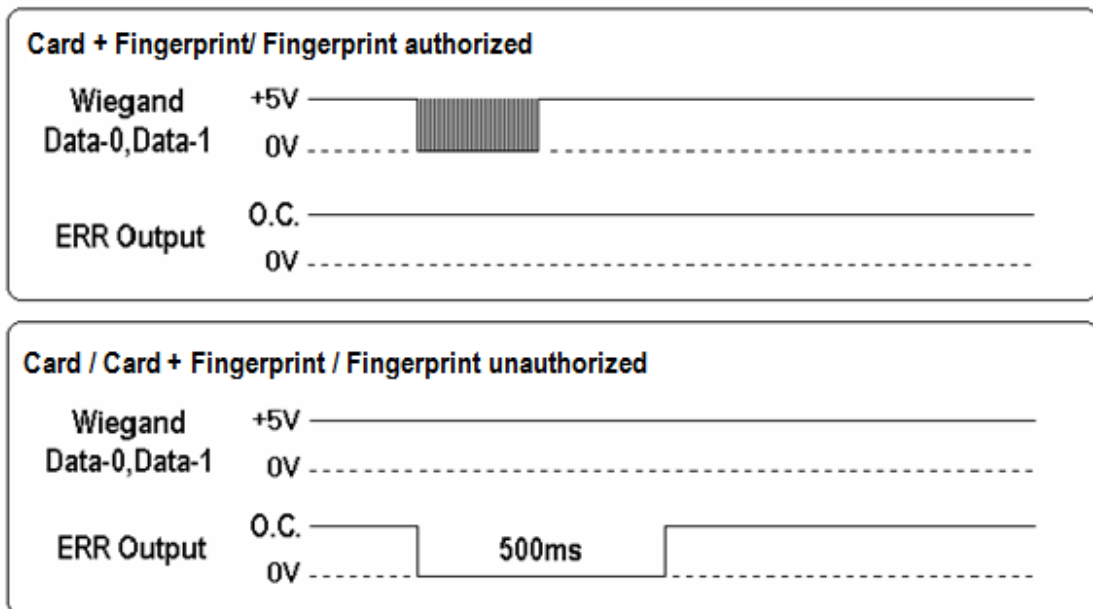
Data format



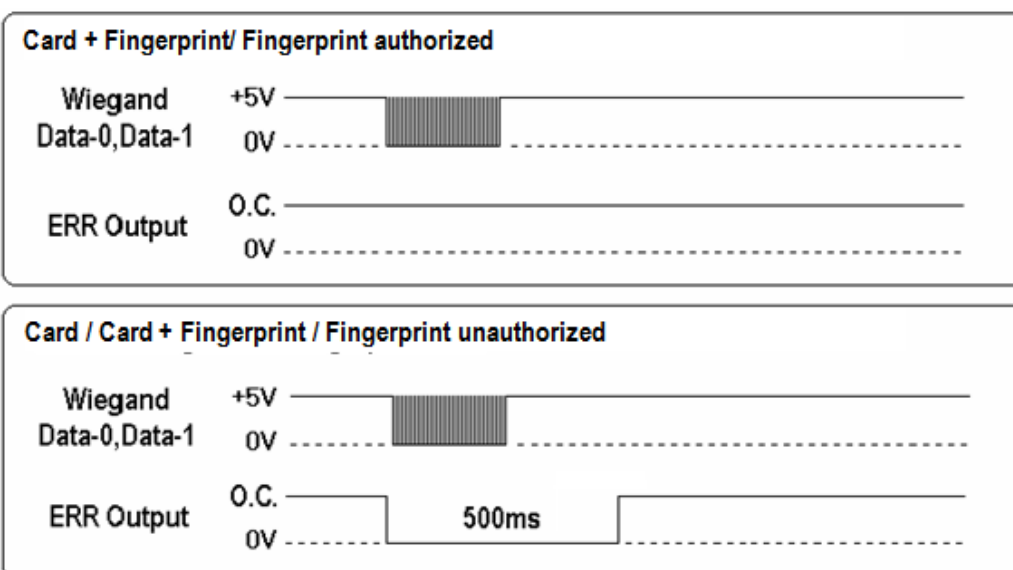
Output timing



3 Normal Output Mode (Default)



4 Extended Output Mode (Selectable using the software)



Before requesting RMA, please check the cases below if your problem is one of them.

1. 1 The device dose not communicate with PC.
2. 2 Cards which were being used are not authenticated after executing batch transmission of IDs from software to the device.
3. 3 When configuring the device using MASTER ID, suddenly the device goes back to the normal mode.
4. 4 The device does not go to setting mode after inputting MASTER ID.
5. 5 The device work well with RF Card, but does not work when inputting card number.
6. 6 A buzzer keeps making sounds. "Bee~~~~~"
7. 7 I want to access with card only, without password.
8. 8 I want to access with fingerprint only, without card or password.
9. 9 A fingerprint is not recognized.
10. 10 I want to register 2 fingerprints for 1 ID.

1 The device dose not communicate with PC.

1.1 Please check wiring.

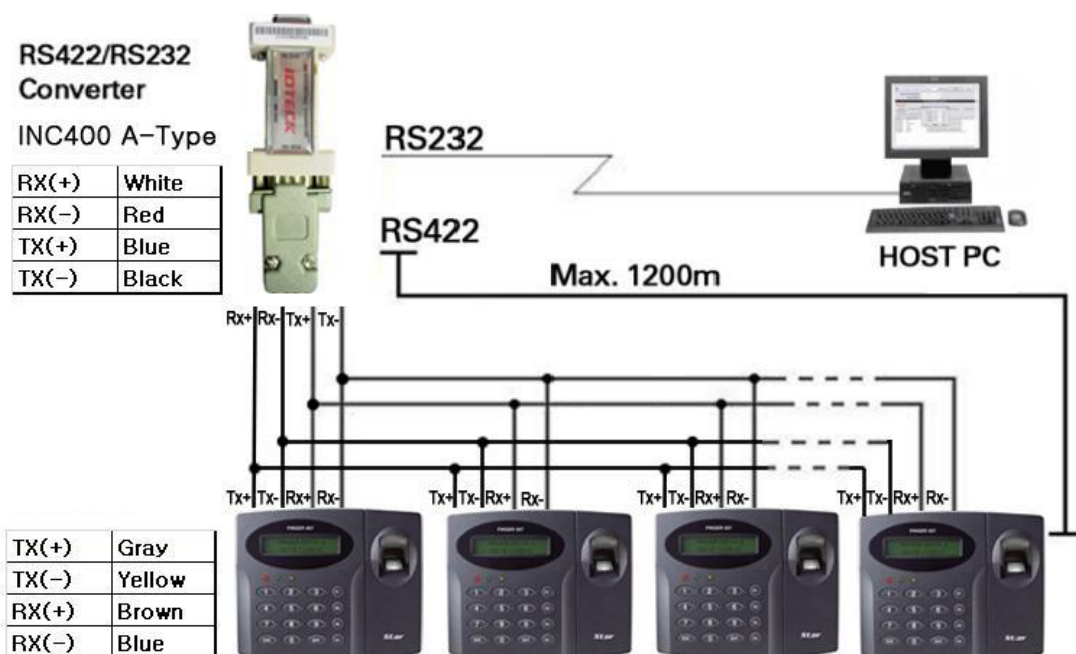
See [Communication] of the manual and check if the wiring is good.

In the case of RS232 communication

See [Communication] > [RS232 Communication Port Connection] of the manual and check if the wiring is good.

In the case of RS422 communication

See [Communication] > [RS422 Communication Port Connection] of the manual and check if the wiring is good.



1.2 Please check if the communication ID is good.

Check communication address setting of software and the device.

1. Check if communication ID set in the device is same with communication ID set in a software.
See [Setting Changes] > [Setup Menu F1] > [COMMUNICATION ADDRESS] and check a communication address set in the device.
2. When you use several devices together, communication addresses set in the devices should be different from each other.
3. See [Setting changes] > [Setup Menu F1] > [Baud Rate] and check if baud rate is same with baud rate set in a software.
* If you initialize the device, baud rate is set to **9,600 bps** which is the default.

1.3 Please check if the communication port setting is good.

Check if communication port set in software is same with communication port set in PC.



If the problem persists, please contact service center.

2 Cards which were being used are not authenticated after executing batch transmission of IDs from software to the device.

2.1 The ID of the card may not be registered to software.

1. Check if the ID is registered to software.
2. If the ID is not registered, register the ID to the software and execute batch transmission of the IDs from software to the device.



If the problem persists, please contact service center.

3 When configuring the device using MASTER ID, suddenly the device goes back to the normal mode.

3.1 If you do not input anything for 60 seconds in setting mode, the device goes back to the normal mode.

To prevent the setting from being changed by one who is not a manager, when the manager leaves the device in setting mode, the device goes back to the normal mode when there is no input for 60 seconds.

4 The device does not go to setting mode after inputting MASTER ID.

4.1 A MASTER ID may have changed.

1. Change the MASTER ID from software and transmit it to the device.
2. If you cannot change MASTER ID using software, see
3. **[Installation of the product] > [System Initialization]** and initialize the device.



Once you initialize the device, MASTER ID of the device goes back to 00000000 (8 digits). In the case of SR model, MASTER ID goes back to 0000000000 (10 digits).



If the problem persists, please contact service center.

5 The device work well with RF Card, but does not work when inputting card number.

5.1 Please check if Keypad is set to "USE".



The default of the keypad input is "NOT USE".

1. See **[Setting Changes] > [Setup Menu F2] > [RF PIN input]** of the manual and set it to "USE".



If the problem persists, please contact service center.

6 A buzzer keeps making sounds. "Bee~~~~~"

6.1 Check if the tamper switch is pressed well.

- The device has a tamper switch on the back to check if the device is fixed on the wall well.
- The tamper switch should be being pressed when and after the installation. If the switch is not pressed, tamper alarm is activated and the buzzer sounds an alarm.
- The tamper switch let you know when someone has taken the device off the wall while attempting trespass or the device has fallen from the wall due to wrong installation.



If the problem persists, please contact service center.

7 I want to access with card only, without password.

By changing reader mode, you can select how to authenticate when accessing.

See **[Setting Changes] > [SETUP MENU F1] > [Reader 1 Mode]** of the manual and select how to authenticate when accessing.



READER#1 refers to the built-in proximity reader in the unit.

ID(PIN) ONLY

In this mode, users can access the door by simply presenting their card or entering their ID number.

ID+F/P(P/W)

In this mode, users can access the door by presenting their card or entering their ID number and then verifying their identity by a fingerprint. For users who did not register their fingerprints, password verification is used instead of fingerprint verification.

ID+P/W+F/P

In this mode, users can access the door by presenting their card or entering their ID number and then verifying their identity by both a fingerprint and a password.



If the problem persists, please contact service center.

8 I want to access with fingerprint only, without card or password.

See **[Setting Changes] > [SETUP MENU F4] > [Identification Mode]** of the manual and set IDENTIFICATION MODE to "USE".



If the problem persists, please contact service center.

9 A fingerprint is not recognized.

9.1 Please check the status of the fingerprint.

- If something is attached to fingerprint, fingerprint recognition may not work properly.
→ Remove it.
- If a fingerprint has a scar, fingerprint recognition may not work properly.
→ Register other fingerprint without a scar.

9.2 If the status of the fingerprint is OK, register your fingerprint again.

If something had been attached to fingerprint or fingerprint had had a scar when you registered, fingerprint recognition may not work properly.



If the problem persists, please contact service center.

10 I want to register 2 fingerprints for 1 ID.

10.1 Please check if Dual Fingerprint Mode is set to "USE".

If you use Dual Fingerprint Mode, you can register 2 fingerprints for 1 ID just in case a fingerprint is injured.

1. See **[Setting Changes] > [SETUP MENU F4] > [Dual Fingerprint Mode]** of the manual and check if Dual Fingerprint mode is set to "USE"
2. If it is not set to "USE", change it to "USE".



If the problem persists, please contact service center.

FCC REGISTRATION INFORMATION

15

FCC Requirements Part 15

***Caution:** Any changes or modifications in construction of this device which are not expressly approved by the responsible for compliance could void the user's authority to operate the equipment.*

***NOTE:** This device complies with **Part 15 of the FCC rules**.*

Operation is subject to the following two conditions:

1. This device may not cause harmful interface, and
2. This device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a **Class A Digital Device**, pursuant to **Part 15 of the FCC rules**. These limits are designed to this equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and receiver.
3. Connect the equipment into an outlet on another circuit.
4. Consult the dealer or an experienced radio/TV technician for help.