User Manual

Thank you for purchasing Keyking products. Please read before installing.

FPC-1000 Fingerprint stand alone

– networked door controller

KEYKING

Index

1 About FPC-1000

1.1 Introduction

KEYKING's FPC1000 is a Networked/Stand-Alone biometric controller. It can be used in a variety of configurations to fit the customer requirements.

FPC1000 identify personnel by their fingerprint, more reliable technology than card or PIN. If needed, a two-factor ID can be used by adding a card or PIN to the fingerprint.

Installations configurations include:

- **Stand-Alone** – all functions are done on the unit using the keypad and menu on the TFT Color display. This configuration does not require PC or any software for normal operation. Might need the use of SPHINX software for data retrieval. The FPC1000 has all needed to operate the door independently.
- **Networked Door Controller** – Same installation as Stand-Alone with the addition of network connection to the SPHINX. This allow more advanced access control functionalities as well as "sharing" fingerprints with other units on the same network. The unit do support PoE connection as well.
- **Fingerprint Reader** – by connecting the FPC1000 Wiegand Output to an access control controller, the door operation is done by the door controller and not the unit itself. Providing higher security and more functionality.

FPC1000 can be used as Time & Attendance terminal, in addition to it's access control functions. As such, the employee identity is determined by fingerprint, more reliable than card and prevent fraud. The TFT screen can be customized and show the employee name when authorized.

FPC1000 may be installed as Entry device or as IN/OUT system where the FPC1000 is used for entry and for exit, an attached Exit Button or Card Reader or additional FPC1000 are connected.

.

1.2 Model Number

Model Options:

FPC 100 0 - P

P: Multi-Technology 125KHz; Awid, EM, HID Prox., Keyking and more
U: Multi-Technology 13.56MHz: Mifare, DesFire, Encrypted and more

0 / 2: Keypad, TFT Display – On Device Configuration
1: Slim Design – no keypad or display – Software configurable only

100: 1000 Series, Standard Optical sensor.
200: 2000 Series, Fake Finger Detection Technology.

FPC: Finger Print Controller;

Compatible with these types card:

P: 125KHz (LF): EM4100, TK4100, HID1326, 1386, AWID, KK234\250T; and others
U: 13.56MHz (HF): KK1208 M1, Philips S50, Mifare-1 Compatible and others

P models Supports Multi Wiegand Output:

- ✓ AWID: Follow card, up to 58BIT
- ✓ EM, 2308: W26, W34
- ✓ HID, 1326, 1386: According to card configuration, W26/27/34/35/37 and so on
- ✓ KK, KK243\250T: W34 W50

1.3 FPC Family

Model	Description	Picture
FPC1000-P	CPU: 400MHz DSP ((4MB Flash memory +8 MB RAM), Fingerprint capacity: 1,000 PCS, unlimited user identified by PC (Software feature),Fully integrated with SECUSYS software. Support Card types: Awid, EM, HID, Keyking, 125KHz Fingerprint Sensor: 500 dpi optical sensor Authentication modes: fingerprint, proximity card, proximity card + fingerprint, ID + fingerprint etc., Communication Interface: Wiegand output, TCP /IP, Dimension: 197mm L x88mm W x 35mm / 470g	
FPC1000-U	CPU: 400MHz DSP (4MB Flash memory +8 MB RAM) Fingerprint capacity: 1,000 PCS, unlimited user identified by PC (Software feature),Fully integrated with SECUSYS software. Support Card types: S50,Mifare Card, 13.56MHz, KK1208M1 Fingerprint Sensor: 500 dpi optical sensor Authentication modes: fingerprint, proximity card, proximity card + fingerprint, ID + fingerprint etc., Communication Interface: Wiegand output, TCP /IP, Dimension: 197mm L x88mm W x 35mm / 470g	
FPC1001-P	CPU: ARM, 32 Bits, Cortex-M4, 400MHz DSP (16MB Flash memory +4 MB RAM),Fully integrated with SECUSYS software. Fingerprint capacity: 1,000 PCS, unlimited user identified by PC (Software feature. Support Card types: Awid, EM, HID, Keyking, 125KHz Fingerprint Sensor: 500 dpi optical sensor Authentication modes: FingerPrint Only, FingerPrint or Card, FingerPrint + Card Communication Interface: Wiegand output, TCP /IP, Dimension: 135mm L x58mm W x 45mm / 490g	
FPC1001-U	CPU: ARM, 32 Bits, Cortex-M4, 400MHz DSP (16MB Flash memory +4 MB RAM),Fully integrated with SECUSYS software. Fingerprint capacity: 1,000 PCS, unlimited user identified by PC (Software feature). Support Card types: S50,Mifare Card, 13.56MHz, KK1208M1 Fingerprint Sensor: 500 dpi optical sensor Authentication modes: FingerPrint Only, FingerPrint or Card, FingerPrint + Card Communication Interface: Wiegand output, TCP /IP, Dimension: 135mm L x58mm W x 45mm / 490g	
FPC2000-P	CPU: 400MHz DSP (4MB Flash memory +8 MB RAM), Fingerprint capacity: 3000 PCS (Can be expandable to 8000), Support Card types: Awid, EM, HID, Keyking, 125KHz Fingerprint Sensor: 500 dpi optical sensor Authentication modes: fingerprint, proximity card, proximity card + fingerprint, ID + fingerprint etc., Communication Interface: Wiegand output, TCP /IP,Fully integrated with SECUSYS software. Dimension: 197mm L x88mm W x 35mm / 490g	
FPC2000-U	CPU: 400MHz DSP (4MB Flash memory +8 MB RAM), Fingerprint capacity: 3000 PCS (Can be expandable to 8000), Support Card types: S50,Mifare Card, 13.56MHz, KK1208M1 Fingerprint Sensor: 500 dpi optical sensor Authentication modes: fingerprint, proximity card, proximity card + fingerprint, ID + fingerprint etc., Communication Interface: Wiegand output, TCP /IP,Fully integrated with SECUSYS software. Dimension: 197mm L x88mm W x 35mm / 490g	
FPC2001-P	CPU: ARM, 32 Bits, Cortex-M4, 400MHz DSP (16MB Flash memory +4 MB RAM), Wiegand output, TCP /IP,Fully integrated with SECUSYS software. Fingerprint capacity: 480 PCS Support Card types: Awid, EM, HID, Keyking, 125KHz Fingerprint Sensor: 500 dpi optical sensor Authentication modes: FingerPrint Only， FingerPrint or Card， FingerPrint + Card Dimension: 135mm L x58mm W x 45mm / 490g	
FPC2001-U	CPU: ARM, 32 Bits, Cortex-M4, 400MHz DSP (16MB Flash memory +4 MB RAM), Wiegand output, TCP /IP,Fully integrated with SECUSYS software. Fingerprint capacity: 480 PCS Support Card types: S50,Mifare Card, 13.56MHz, KK1208M1 Fingerprint Sensor: 500 dpi optical sensor Authentication modes: FingerPrint Only， FingerPrint or Card， FingerPrint + Card Dimension: 135mm L x58mm W x 45mm / 490g	
FPC2002-P	CPU: 400MHz DSP (4MB Flash memory +8 MB RAM),Wiegand output, TCP /IP,Fully integrated with SECUSYS software. Fingerprint capacity: 480 PCS Support Card types: Awid, EM, HID, Keyking, 125KHz Fingerprint Sensor: 500 dpi optical sensor Authentication modes: fingerprint, proximity card, proximity card + fingerprint, ID + fingerprint etc., Dimension: 197mm L x88mm W x 35mm / 470g	
FPC2002-U	CPU: 400MHz DSP (4MB Flash memory +8 MB RAM),Wiegand output, TCP /IP,Fully integrated with SECUSYS software. Fingerprint capacity: 480 PCS Support Card types: S50,Mifare Card, 13.56MHz, KK1208M1 Fingerprint Sensor: 500 dpi optical sensor Authentication modes: fingerprint, proximity card, proximity card + fingerprint, ID + fingerprint etc., Dimension: 197mm L x88mm W x 35mm / 470g	
BioUSB10P	Biometric USB enrollement Finger Print Reader for direct connection to PC. Fully integrated with SECUSYS software, Built in Multi-Proximity reader	
	Biometric USB enrollement Finger Print Reader for direct connection to PC. Fully integrated with SECUSYS software, Built in CPU	

1.4 Features

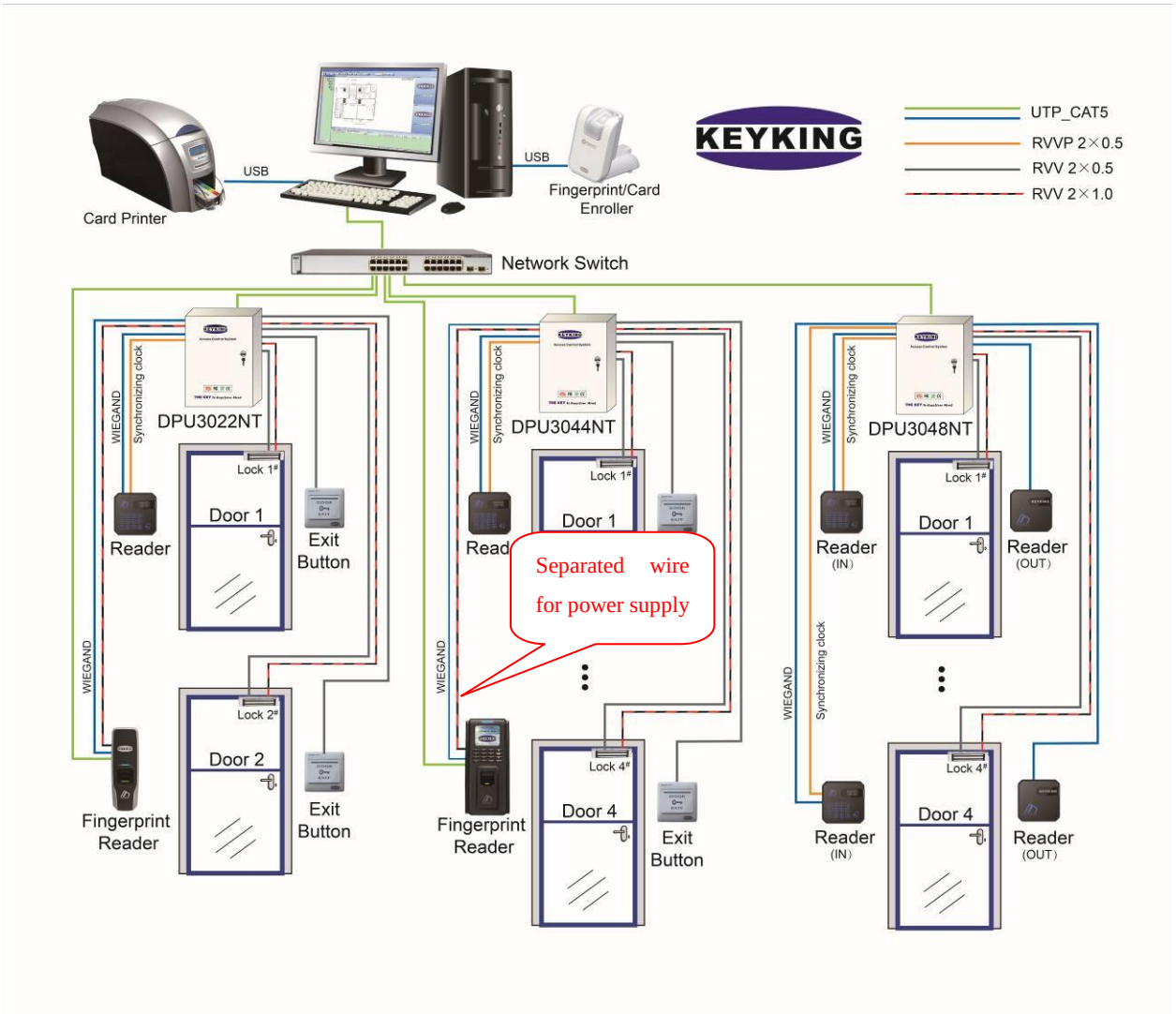
- Scratch resistant 500DPI Fingerprint Sensor
- ~1 sec. response time.
- Multi-Core CPU with multithread operation.
- Self-Test, Watchdog Timer for better stability
- 1,000 fingerprints capacity. Up to 3 fingers / employee.
- No fingerprint image stored – fingerprint converted to mathematical template code.
- Uninterrupted operation on-line and off-line, independent operation.
- TFT color display – customizable background and employee data.
- User Friendly interface in English or Chinese
- On-Device-Configuration for operation as Stand-Alone
- 100MBPS Network connectivity
- PoE supported
- Wiegand 26/34 output, for connection as reader to standard access control controllers.
- Wiegand 26/34 input, for secondary reader as exit device. Can be card reader or another FPC1000 unit.
- Exit Button (REX) and Door Sensor inputs
- 3A Door Relay
- AUX Input – programmable, can be used for intercom or alarm operation
- AUX Relay – programmable, can be used for alarms or other signaling
- IP54 – fit installation in multiple locations.

Specification:

- CPU: ARM, 32Bits, Cortex-M4, 400MHz DSP
- Fingerprint Template: 1,000
- Biometric sensor: 500 dpi 0.5sec. read sensor
- Operation Modes: FP, Card, FP / Card, Card+FP, ID+FP – may personalized by employee
- Wiegand interface: Wiegand input / output
- Networking: TCP/IP 100MBPS – KEYKING Protocol
- Power Over Ethernet: IEEE 802.3af (including 12Vdc 500mA output)
- Operating voltage: 12VDC
- Operating current: ≤500mA
- Standby current: ≤350mA
- Temperature: -20°C to 65°C
- Humidity: 0--95%
- Dimension: 197mm L x88mm W x 35mm
- Weight: 490g

1.5 Installations instruction

1.5.1 FPC1000 works as a reader



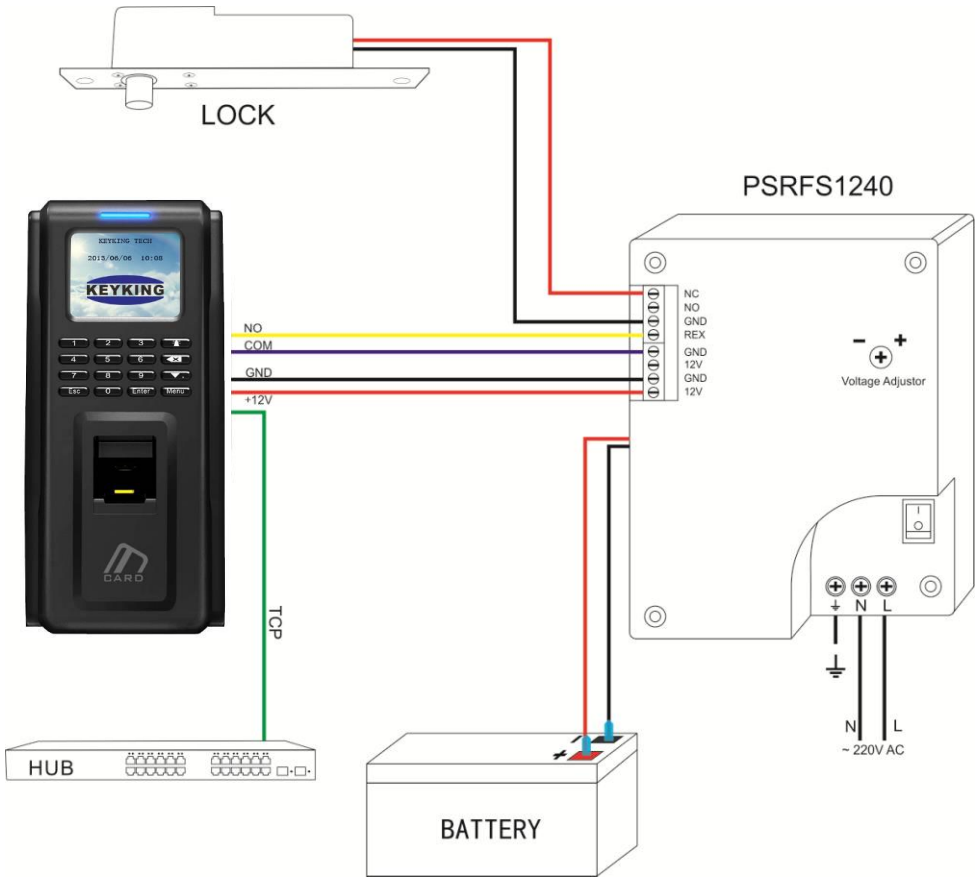
Note:

- Do Not connect FPC to door controller as reader! – connect only Wiegand wires to the controller. Power the FPC from independent power supply (12Vdc 1A)
- Do Not run lock power with Wiegand wires in the same cable!

1.5.2 FPC1000 works as a standalone

3 options:

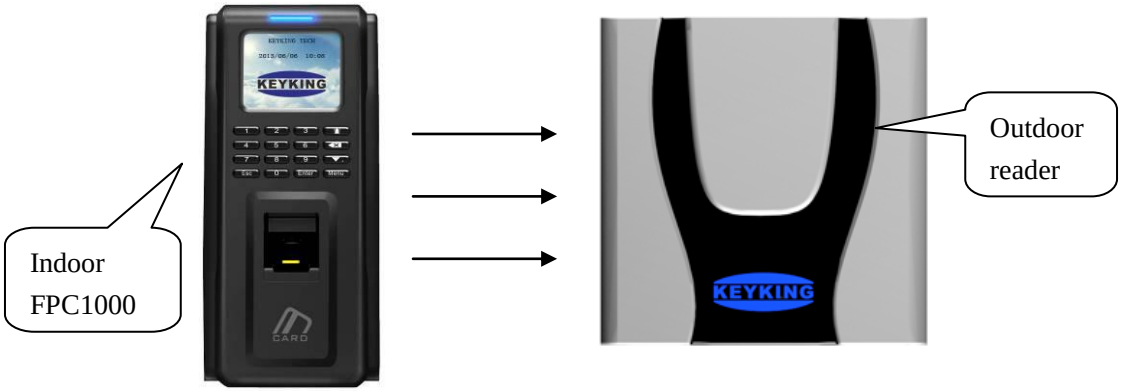
- **Standalone**, no external reader



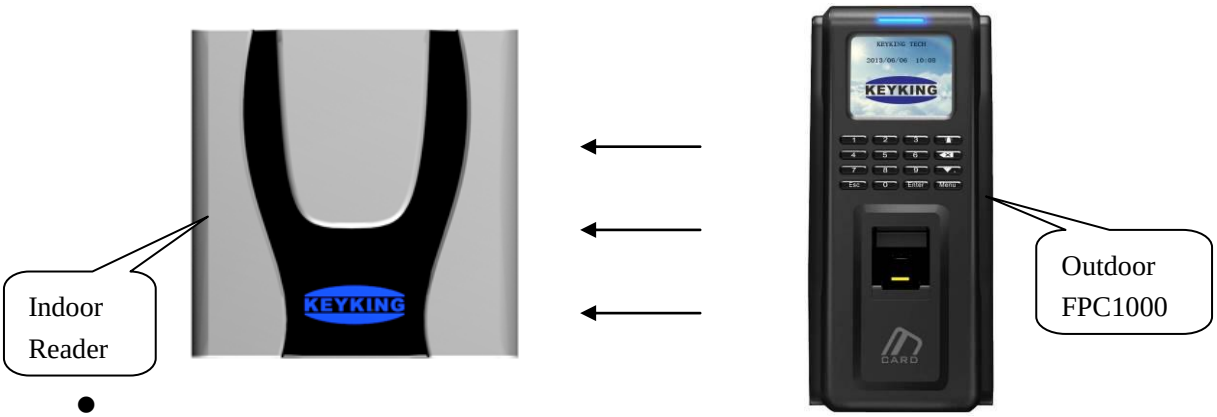
Notes:

- ✧ recommended power supply PSRFS1240 - incorporate isolation relay and backup battery support.
- ✧ .

- Outdoor Card reader, indoor FPC1000



- Indoor Card reader, outdoor FPC1000



-

1.5.3 FPC1000 Location

When selecting the location of installation, make sure the following rules are followed:

- No direct sun - avoid over heating
- Protect from water splashes on the screen and keypad
- Protect back of the unit from water and exposed wires.

Chapter 2 Installation

2.1 Install FPC1000 on the wall

2.1.1. Remove the back plate from the FPC1000 and I by unscrewing the M3 screw at the bottom of the unit.

2.1.2. Identify the mounting location. The unit may be installed directly on the wall or using and electrical mounting box.

2.1.3. Ensure that the wires can go freely and connect to the unit. It is recommended to cut openings the same as on the back-plate to allow the connectors and the wires to be stress-free.

2.1.4. Mount the back-plate to the wall or junction box using 3 x ⌀4mm screws

2.1.5. Run the wires via the connectors openings and connect to the green connectors as described in the Wiring Chapter 2

2.1.6. Attach the FPC1000 to the base plate by hanging it first on the top 2 slots and pushing it against the wall. Use the M3 screw to lock the unit in place from the bottom

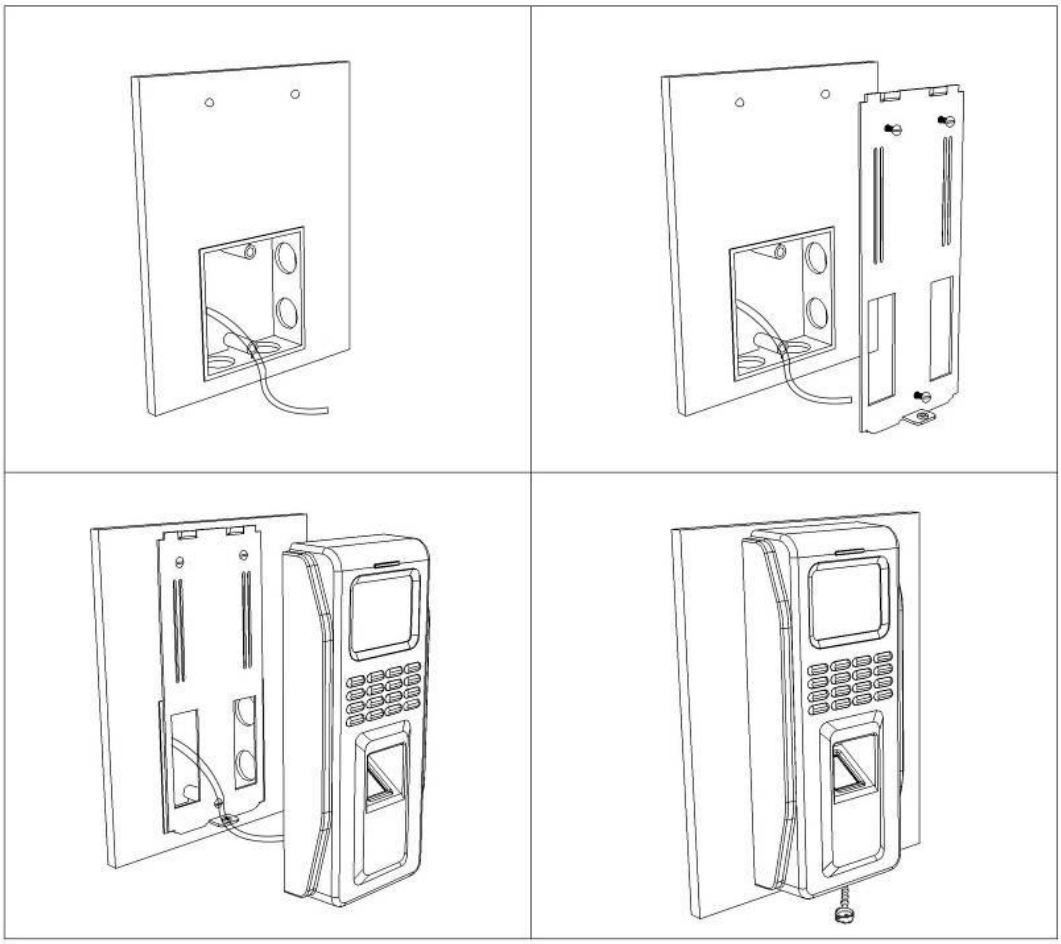


Figure 2-1

Chapter 3 Wiring Diagram

3.1 FPC1000 Parts

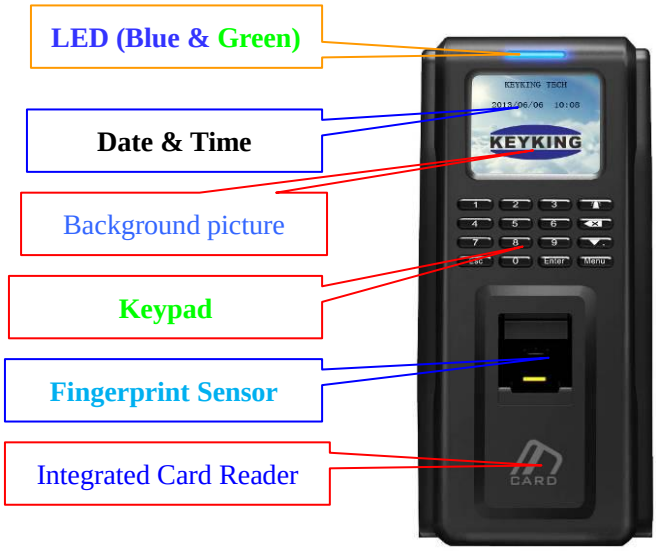


Figure 3-1

LED: **BLUE = Power On** ; **GREEN = Lock Open**

Keypad:

NO.	Key	Description
0-9	0-9	Numerical Keys for menu selection and data entry
2	Esc	Back to previous menu / cancel operation
3		Door Bell – energize Relay 2
4		Delete data entered
5		Scroll down / period (.)
6	Menu	Enter Main Menu
7	Enter	Confirm Data

3.2 Wiring Diagram

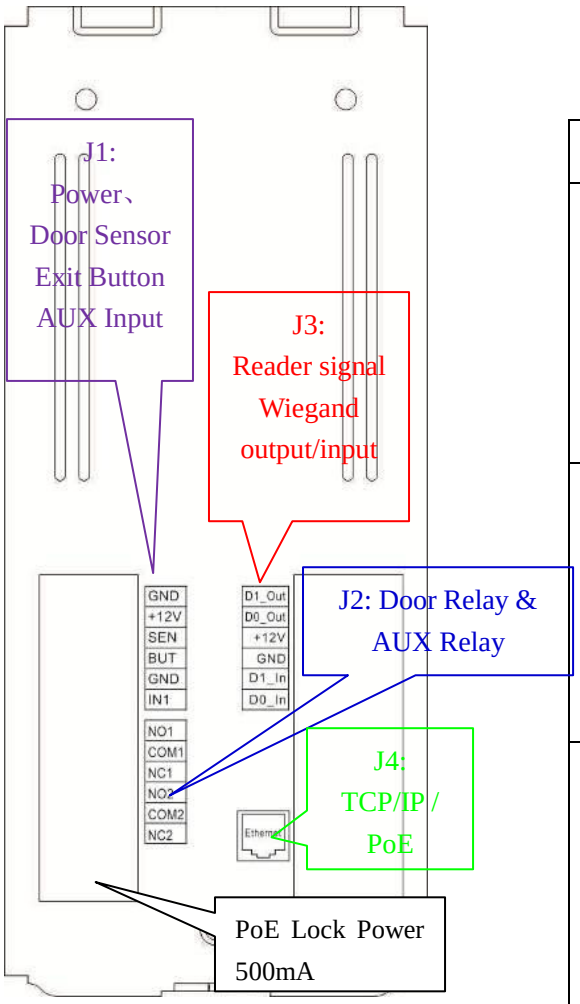


Figure 3-2

Con.	Label	Definition
J1	GND	Power Supply Negative (GND, -)
	+12V	Power Supply Positive (VCC, +)
	SEN	Door Sensor Out Wire
	BUT	Exit Button Out Wire
	GND	Inputs GND – In, COM of all switches
	IN1	AUX Input wire
J2	NO1	Door Lock Relay – See corresponding lock type for wiring
	COM1	
	NC1	
	NO2	AUX Programmable Relay – Also act as Alarm and “Alarm Clock”
	COM2	
	NC2	
J3	D1_Out	Wiegand Output Signal
	D0_ Out	
	+12V	External Reader Power – 12Vdc, 125mA
	GND	
	D1_In	External Reader Wiegand Connection
	D0_In	
J4	RJ45	Network TCP/IP or PoE
J5	GND	PoE Mode Power Output. 12Vdc 500mA
	+12Vdc	

DO NOT Connect Power Supply if using PoE!!

3.3 Lock Wiring Diagram

J4: Relay Output – Relay 1（Lock Control）

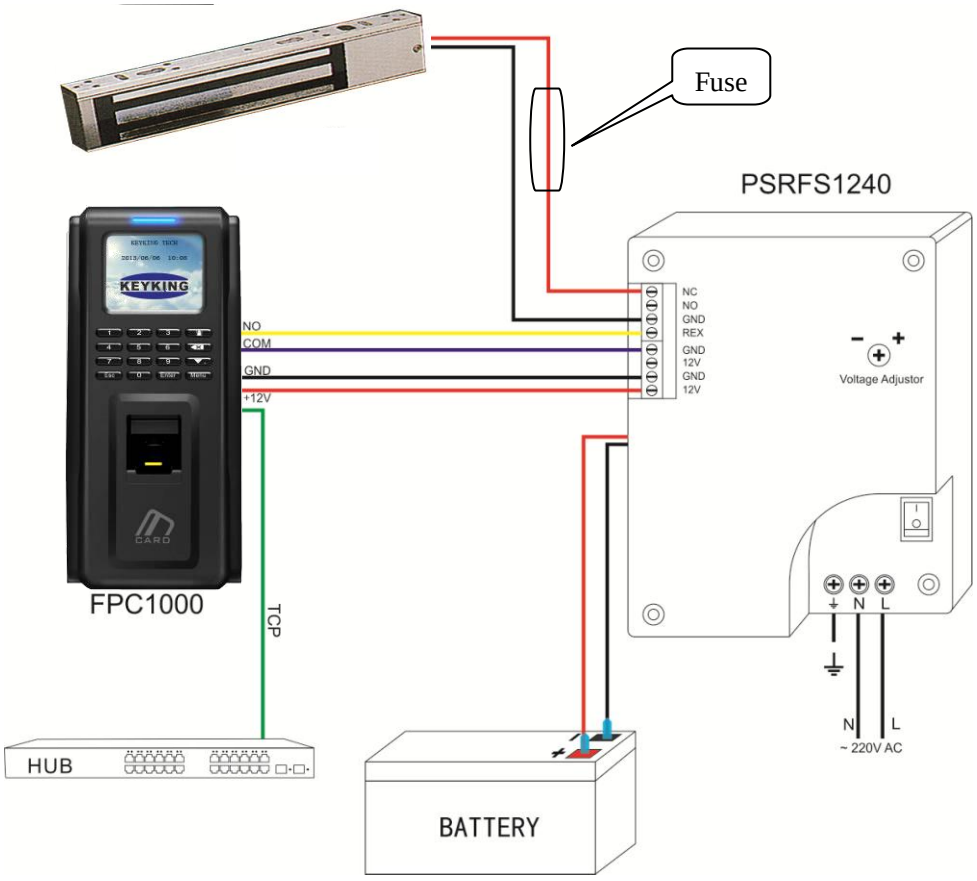


Figure 3-5 MagLock（Fail safe）

Notes:

- ✧ recommended power supply PSRFS1240 – incorporate isolation relay and backup battery support.
- ✧ REX – Exit Button –
  - o May be connected via the PSRFS1240 – in such case, do not use Door Sensor to prevent false alarms from the unit.
  - o Or direct to the FPC1000 using GND & SEN connections. If connected directly to FPC1000, the opening operation will be recorded on the software.
- ✧ If using Fail Secure Strike - Please use NO contact instead of NC.
- ✧ Connect adequate fuse to the lock – protect the power supply

3.4 TCP/IP Network

FPC1000 TCP/IP network

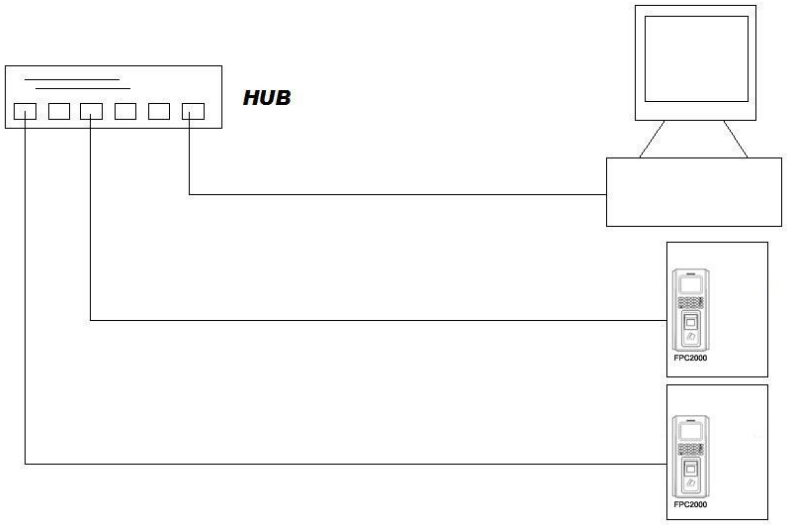


Figure 3-8

TCP/IP crystal head

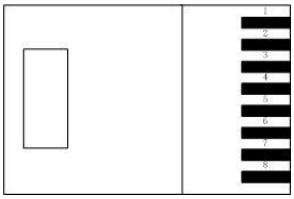


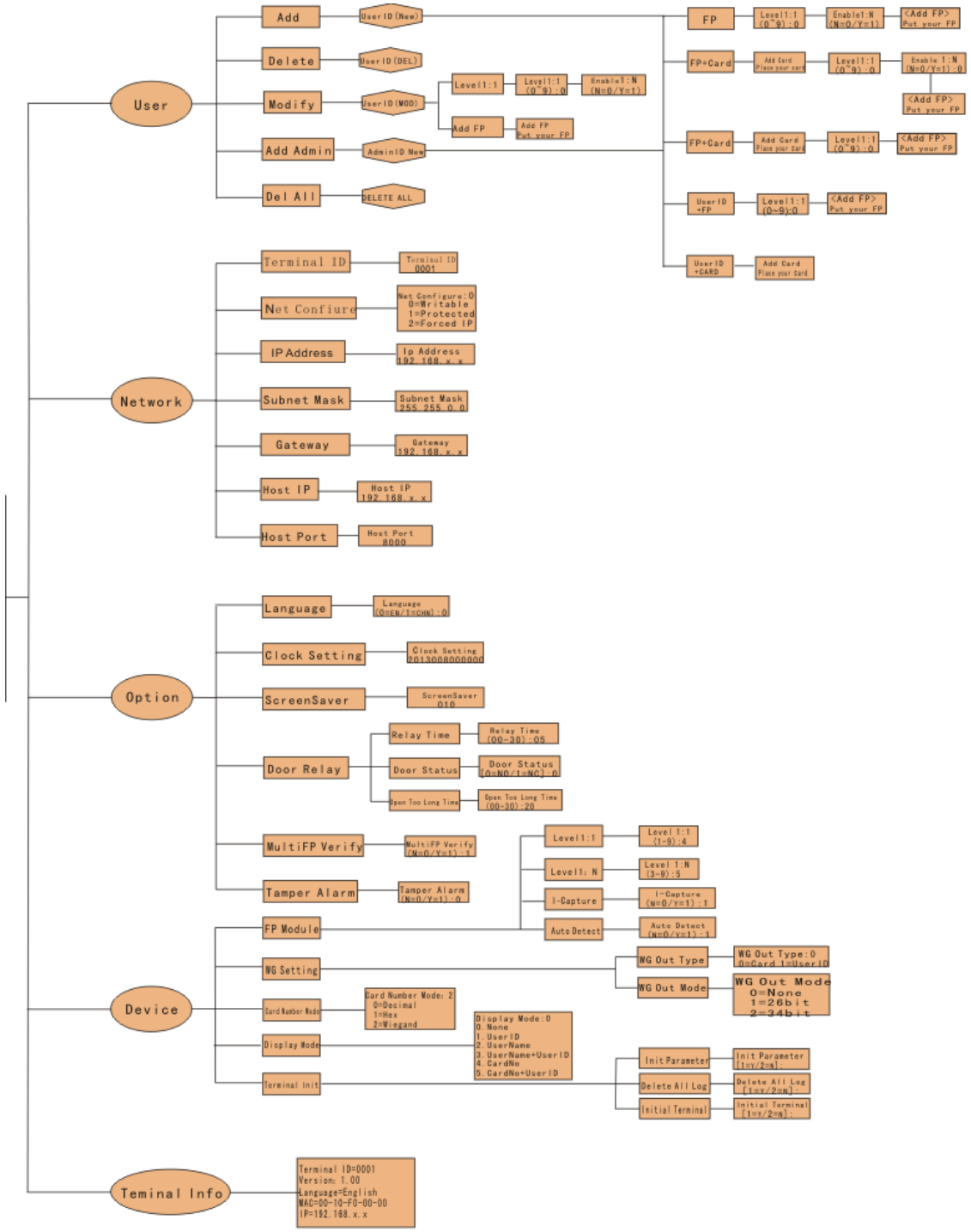
Figure 3-9

RJ45 NO.	Definition
1	TX+
2	TX-
3	RX+
6	RX-

Figure 3-2

Chapter 4 - On Device Configuration Menu

Below is the full configuration menu. New units do not have Administrator and will allow entering the menu without password or 1234. After first Administrator is enrolled, to enter the menu, the unit will require Administrator ID. There is no limit on number of administrators.



4.1. First Installation Procedure – Stand Alone – On Device Configuration

4.1.1. click the MENU button to enter the main menu.

4.1.2. select Options and set the Clock (Date-Time YYYYMMDDHHMMSS)

4.1.3. in Options, set Door Relay

4.1.3.1. Relay Time – set the time of door unlock

4.1.3.2. Door Status – N.O. (0) – normal, N.C. (1) – relay energized to lock door

4.1.3.3. Door Open Too Long time – Time of "Door Held Open" alert (require door sensor)

4.1.4. Click ESC to go to the main menu and select User to enroll Users and Administrators. When enrolling, note the instructions on the screen.

4.1.5. To make changes to other features and functions, see the menu tree on page 15

4.1.6. More options and features are available using the SPHINX software. These include:

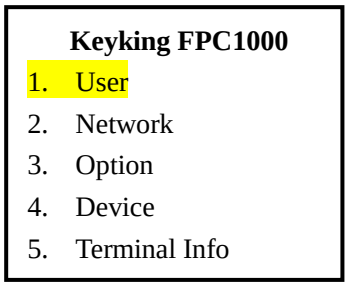
- ✧ Attach name and personnel information to User ID – will display employee name on screen.
- ✧ Screen background change
- ✧ Door Status Schedule – set time when door is open to all, restricted (normal) or locked.
- ✧ Time Zones – set access time restrictions to employees
- ✧ Flow Control – Event and I/O status automated response and configuration
- ✧ Time & Attendance – scheduling and reporting
- ✧ CCTV – link IP Camera to record footage on events direct to SPHINX (require PC connected)
- ✧ Much More…… talk with your supplier for more information.

4.2 Personnel Management

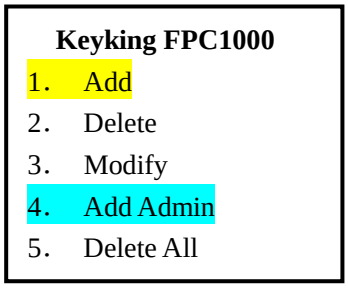
4.2.1 Add Personnel / Administrator

1. Press Menu to enter management menu when FPC1000 is idle. Esc works as cancel while Enter works as confirm.

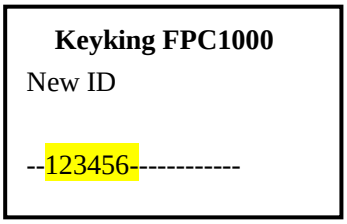
2. Press 1 to enter User interface.



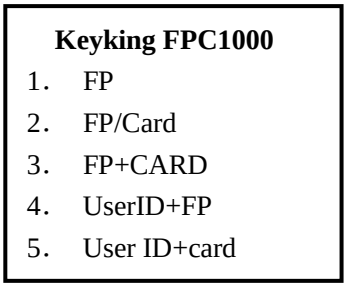
3. Press 1 to Add User or 4 to add Administrator.



4. Type new user ID - 2-6 digits, and press ENTER to confirm.
   It is recommended to keep a list of User ID and the person names. Especially important if not using PC to allow removal from device if needed.

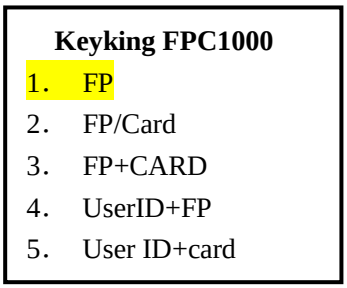


See next pages for instructions on options



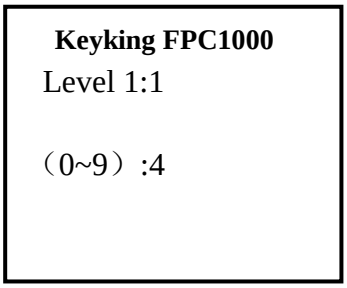
4.2.1.1 Fingerprint Only

1. Press 1 for Fingerprint Only



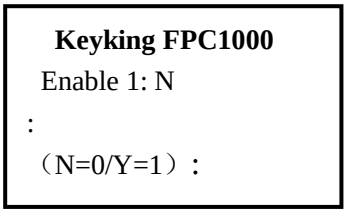
2. Hit ENTER to go to the next screen

Level 1:1 apply to Card+Fingerprint or ID+Fingerprint modes ONLY. The number represent how strict the verification is done. 4 is normal, higher number will provide higher security, but, might result in multiple attempts by authorized users. Lower number will make the unit faster to response and comply with problematic fingers, but, might authorize unauthorized persons.



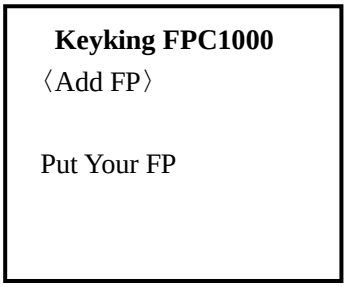
3. Hit ENTER to go to the next screen

If entered 0, the unit will require ID or Card before fingerprint, with 1 (default) the unit will read the finger as it is laid on the sensor.

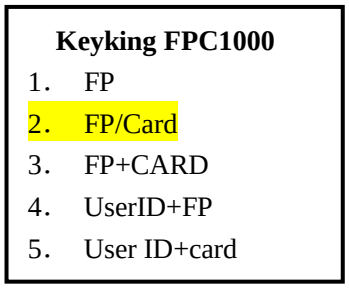


4. Follow the instructions on the screen, the unit will require two finger scans, let the unit 2 seconds scan time for each finger.

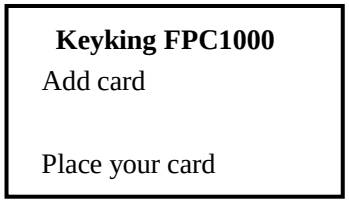
If scan failed, the FPC1000 will go back to the main menu and the process will begin from the Main Menu 4.3.1



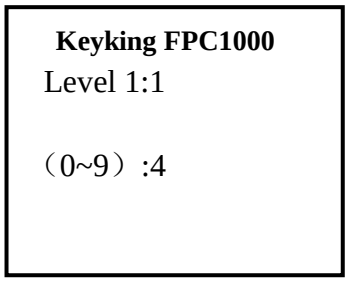
4.2.1.2 FP/Card



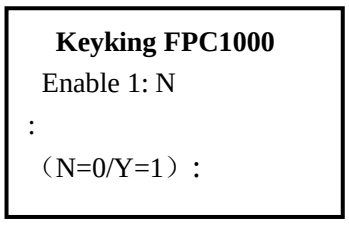
1. Press 2 to enter add FP/Card interface.
   This option will allow a person identity to be either Card or Fingerprint



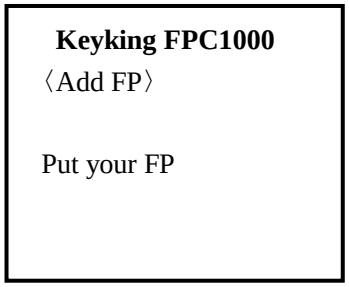
2. Swipe the card in front of the card picture (under the sensor); system will enter the next interface after a beep sound.



3. Hit ENTER to go to the next screen
   Level 1:1 apply to Card+Fingerprint mode ONLY. The number represent how strict the verification is done. 4 is normal, higher number will provide higher security, but, might result in multiple attempts by authorized users. Lower number will make the unit faster to response and comply with problematic fingers, but, might authorize unauthorized persons.



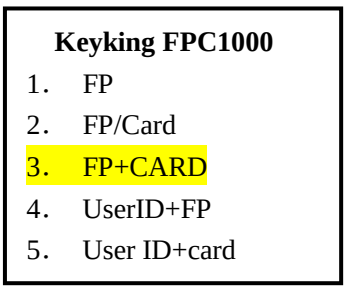
4. Hit ENTER to go to the next screen
   If entered 0, the unit will require ID or Card before fingerprint, with 1 (default) the unit will read the finger as it is laid on the sensor.



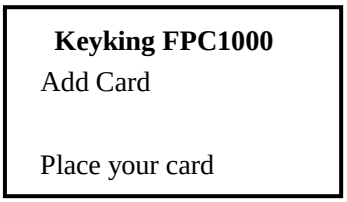
5. Follow the instructions on the screen, the unit will require two finger scans, let the unit 2 seconds scan time for each finger.
   If scan failed, the FPC1000 will go back to the main menu and the process will begin from Main Menu 4.2.1

4.2.1.3 FP+Card

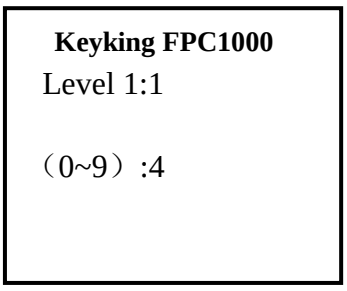
1. Press 3 to enter add FP+Card interface.
   This mode uses Dual-Factor ID. BOTH Card & Fingerprint verification are required and need to match. Use this mode in cases where higher security required or Use this mode in cases where the person fingerprint quality is very low enforcing low 1:n and 1:1 levels. The fingerprint must be read within 4 seconds from Card swipe.



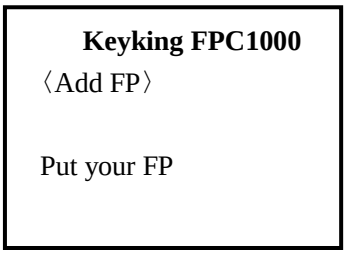
2. Swipe the card in front of the card picture (under the sensor); system will enter the next interface after a beep sound



3. The number represent how strict the verification is done. 4 is normal, higher number will provide higher security, but, might result in multiple attempts by authorized users (False Negative). Lower number will make the unit faster to response and comply with problematic fingers, but, might authorize unauthorized persons (False Positive). FP+Card mode prevent false positive.
   Hit ENTER to go to the next screen.

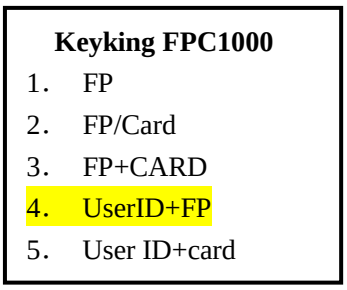


4. Follow the instructions on the screen, the unit will require two finger scans, let the unit 2 seconds scan time for each finger.
   If scan failed, the FPC1000 will go back to the main menu and the process will begin from Main Menu 4.2.1

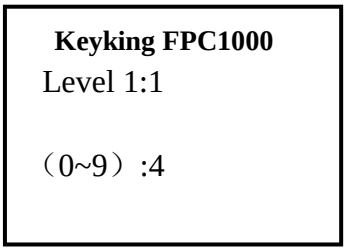


4.2.1.4 UserID+FP

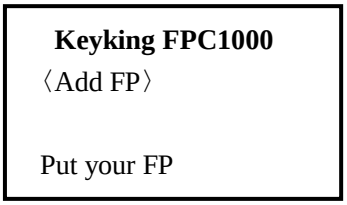
1. Press 4 to enter add UserID+FP interface.
   This mode uses Dual-Factor ID. Use this mode in cases where the person fingerprint quality is very low enforcing low 1:1 level. And there are no cards in use. The User ID (entered at 4.2.1 screen 4) as first identification and then require matching fingerprint within 4 seconds after ID entered.



2. The number represent how strict the verification is done. 4 is normal, higher number will provide higher security, but, might result in multiple attempts by authorized users. Lower number will make the unit faster to response and comply with problematic fingers, but, might authorize unauthorized persons. Hit ENTER to go to the next screen

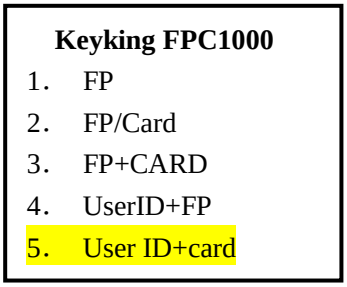


3. Follow the instructions on the screen, the unit will require two finger scans, let the unit 2 seconds scan time for each finger.
   If scan failed, the FPC1000 will go back to the main menu and the process will begin from Main Menu 4.2.1

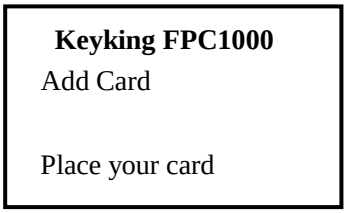


4.2.1.5 User ID+card

1. Press 5 to enter add UserID+Card.
   This mode uses Dual-Factor ID, though do not use Fingerprint as one of the identifications. It is not recommended to use this mode, unless, there is a specific problem with an individual that can not use Fingerprint.

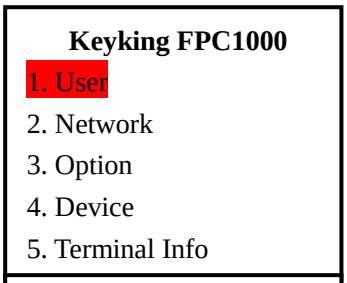


2. Swipe the card in front of the card picture (under the sensor); system will enter the next interface after a beep sound .

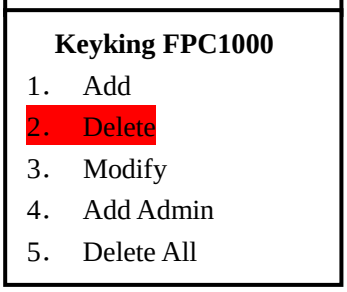


4.2.2 Delete Personnel

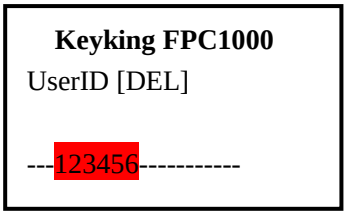
1. Enter the main menu and select 1 User



3 Press 2 Delete.

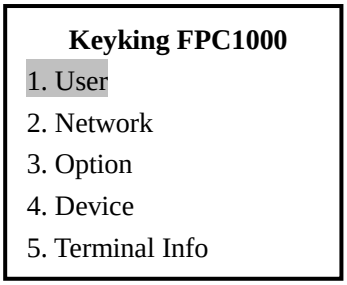


4 Enter the UserID which is to be deleted, then press Enter to confirm.

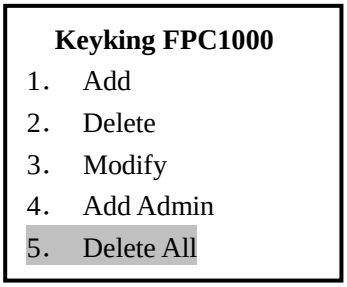


4.2.3 Delete All

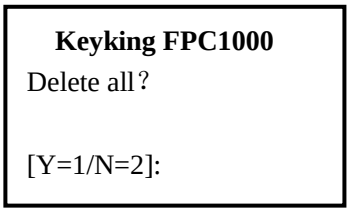
1. Enter main menu and select 1. User



2. Press 5 to enter Delete All interface.

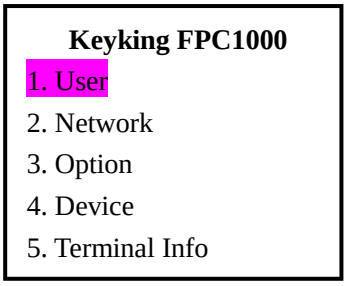


3. Press 1 and Enter to confirm deleting.
4. **NOTE** – this will remove ALL users and administrators credentials but will NOT clear the history

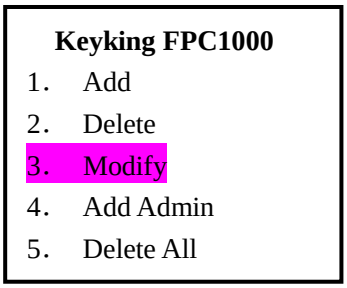


4.2.4 Modify

1. Enter the Main Menu and select 1. User

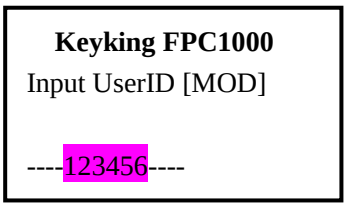


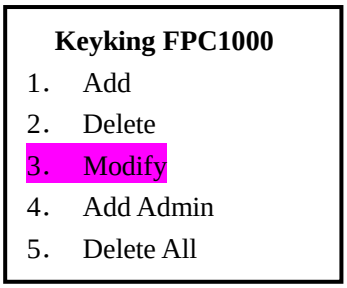
2. Press 3 Modify

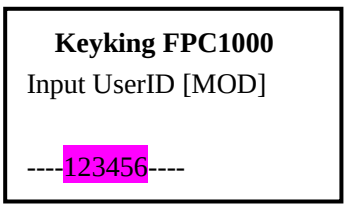


.

3. Enter the UserID to be modified, the same interface as the enrolment will allow to modify specific configurations.





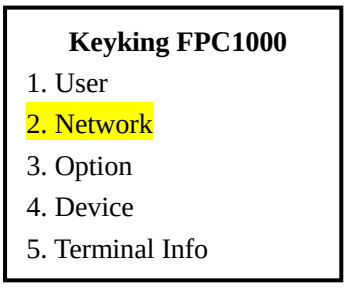


4.3 Network Configuration

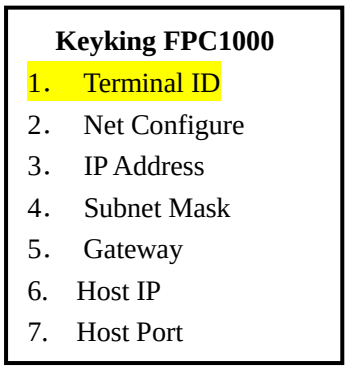
If running FPC1000 as Stand-Alone without PC Connectivity planned, this chapter can be skipped.
In most cases, when FPC1000 may be connected to PC running SPHINX, network configuration may be made On-Device using the following instructions, or, from SPHINX which has very simple and smart controller configuration menu that will allow connection and adaption of the FPC1000 to the local network automatically. If using Lap Top for updates from time to time, make sure the laptop has “static ip” also so the FPC1000 will automatically recognize it when connected. Single laptop can be used to configure multiple FPC1000 units. See SPHINX manual for more information.

4.3. 1 Terminal ID

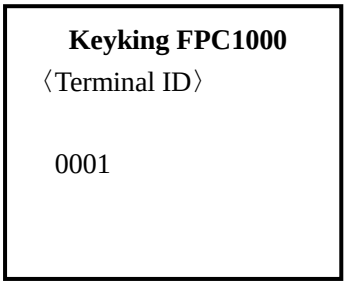
1. From the Main Menu, select 2. Network



2. Press 1 to enter Terminal ID – this is the unit ID number. If using multiple units, make sure it is not duplicated.



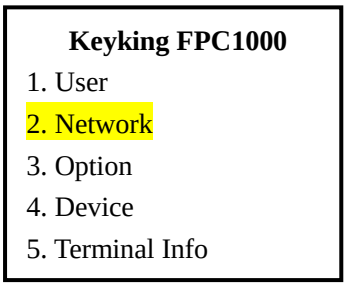
3. Input the Terminal ID by using the keypad and press Enter to confirm.



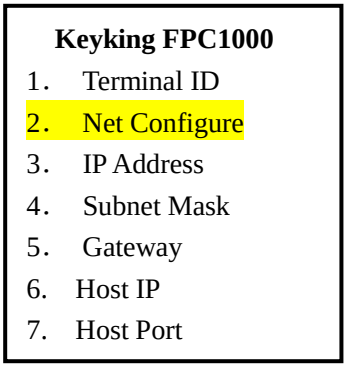
4. Use ESC key to go back to previous menu.

4.3.2 Net Configure

1. From the Main Menu, select 2. Network

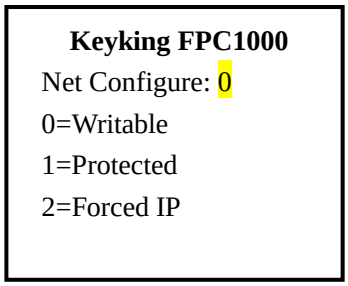


2. Press 2 to enter Network Configuration



3. Make sure Net Configure is **0** and hit ENTER. use ESC key to go back to previous "Network Configuration" menu.

0 = Network parameters configurable.
1 = Network Parameters write-protected and can not be changed
2 = force 10.1.1.10 IP Address



4.3.3 IP Address

1. From the Main Menu, select 2. Network

Keyking FPC1000
1. User
2. Network
3. Option
4. Device
5. Terminal Info

2. Press 3 to enter IP Address

Keyking FPC1000
1. Terminal ID
2. Net Configure
3. IP Address
4. Subnet Mask
5. Gateway
6. Host IP
7. Host Port

3. Enter IP Address interface. ( button is Delete / Backspace,  button is ·) and ENTER to confirm. Use ESC to go back to previous “Network Configuration” menu.

Keyking FPC1000
IP Address:

192.168.x.x

4.3.4 Subnet Mask

1. From the Main Menu, select 2. Network

Keyking FPC1000
1. User
2. Network
3. Option
4. Device
5. Terminal Info

2. Press 4 to enter Subnet Mask

Keyking FPC1000
1. Terminal ID
2. Net Configure
3. IP Address
4. Subnet Mask
5. Gateway
6. Host IP
7. Host Port

3. Enter Subnet Mask. ( button is Delete / Backspace,  button is ·) and ENTER to confirm. Use ESC to go back to previous "Network Configuration" menu.

Keyking FPC1000
Subnet Mask:
255.255.x.x

4.3.5 Gateway

1. From the Main Menu, select 2. Network

Keyking FPC1000
1. User
2. Network
3. Option
4. Device
5. Terminal Info

2. Press 4 to enter Subnet Mask

Keyking FPC1000
1. Terminal ID
2. Net Configure
3. IP Address
4. Subnet Mask
5. Gateway
6. Host IP
7. Host Port

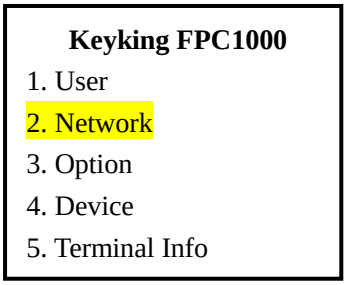
3. Enter Gateway. ( button is Delete / Backspace,  button is ·) and ENTER to confirm. Use ESC to go back to previous “Network Configuration” menu.

Keyking FPC1000
Gateway:
192.168.X.X

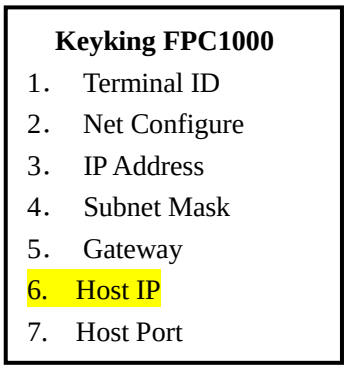
4.3.6 Host IP

The HOST is the computer where the SPHINX software is installed (Server).

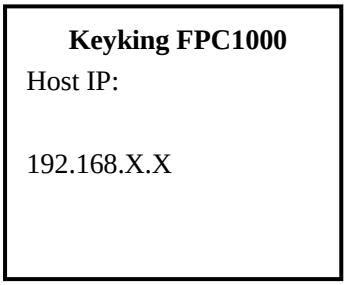
1. In Main Menu select 2, Network



3. Select 4 to enter Subnet Mask

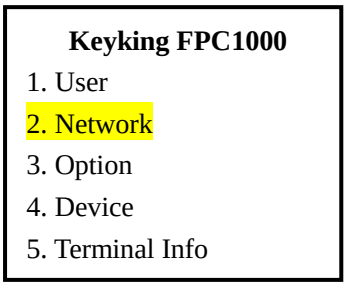


4. Enter Gateway. ( button is Delete / Backspace,  button is ·) and ENTER to confirm. Use ESC to go back to previous “Network Configuration” menu.

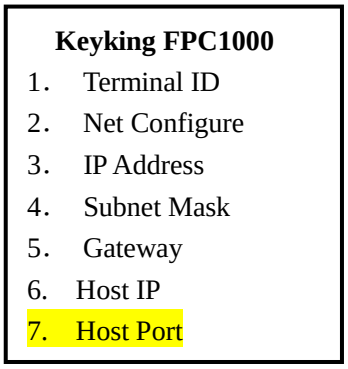


4.3.7 Host Port

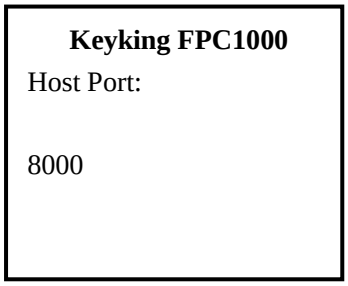
1. In Main Menu select 2, Network



2. Select 7, Host Port



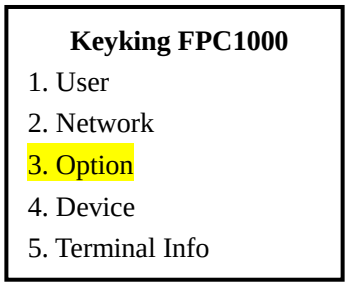
3. Enter Port number. ( button is Delete / Backspace,  button is ·) and ENTER to confirm. Use ESC to go back to previous “Network Configuration” menu



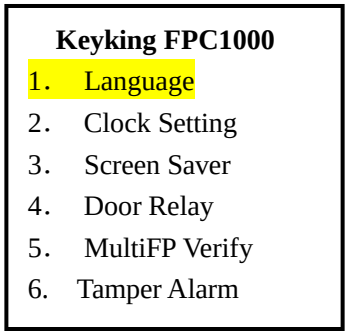
4.4 Option

4.4.1 Language

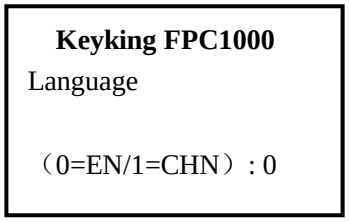
1. In Main Menu, select 3, Option



2. Select 1, Language

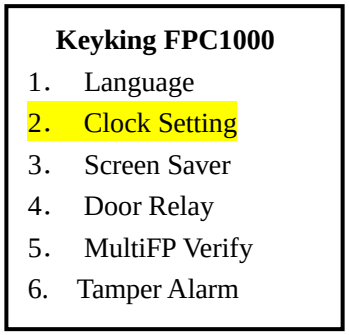


3. Select language (0=English 1=Chinese) and press Enter to confirm.

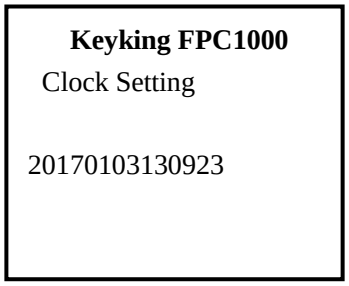


4.4.2 Clock Setting

1. From the Options menu, select 2, Clock Setting



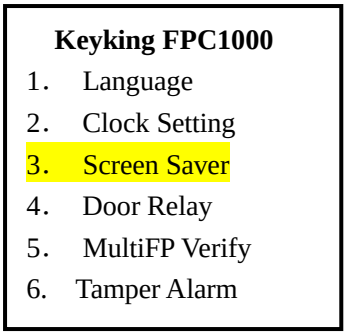
2. Enter date and time in the following format: YYYYMMDDHHMMSS (Year, month in 2 digits, day in 2 digits, hour in 24H format, minutes in 2 digits and seconds in 2 digits)
   For example, 1:09:23 PM on January 3rd. 2017
   Enter to confirm.



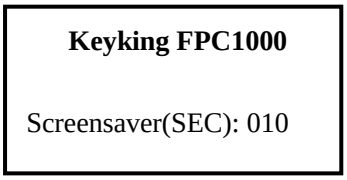
4.4.3 Screensaver

Screen Saver is the time where the LCD screen go dark if no key or finger had been pressed. It is important to select the right time to allow reasonable time to read the screen for users and at the same time to conserve energy by turning off the screen when not needed. The LCD screen had predefined life (like any screen) and keeping the screen on all the time will short the unit usability time. It is recommended to have it at 10-20 seconds.

1. In the Option Menu, select 3, Screen Saver



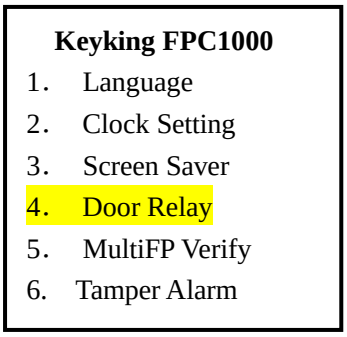
2. Enter the time in Seconds and ENTER to confirm



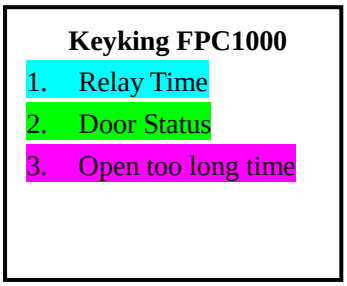
4.4.4 Door Relay

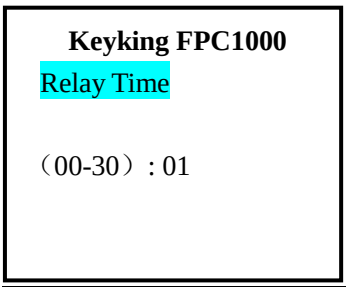
Door Relay time is the time the lock will be open on authorized access (by ID or REX Button or from the software “Grant Access”). Make sure it is a reasonable time. Too short, people will not be able to enter. Too long, others, unauthorized, may be able to enter following authorized entrance (tailgating).
Door Status is the Door Sense input. Usually a “magnet relay” such as used in alarm systems. It is not mandatory for the unit operation, but, provide several important features:
Tailgate Prevention - If using the Door Sensor, the relay will return to Locked position once the door opened and closed regardless the time left.
Door Held Open Alert – The unit can be configured to provide alert if door is not closed within pre-determined time.
Door Status monitoring if the unit is connected to SPHINX

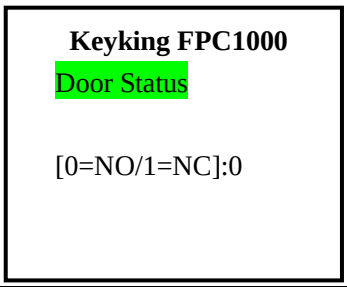
1. From the Option Menu, select 4, Door Relay.

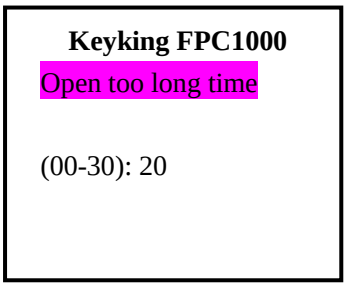


3. Select the parameter to be set









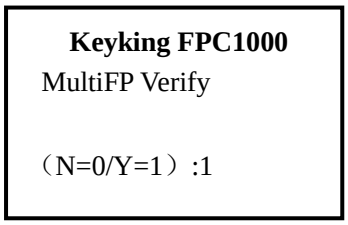
Set Lock Relay time in Seconds	Select Door Sensor Type Leave 0 if not used	Set the time allowed for the door to stay opened before alert

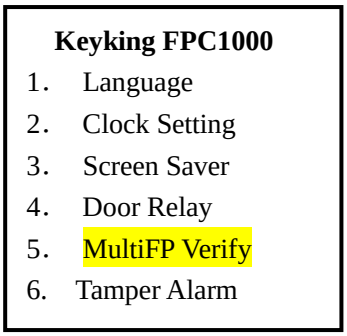
4.4.5 MultiFP Verify

Multi-Fingerprint Verification allow to enroll up to 3 fingerprints for each user. It is recommended since people might have minor cuts (paper cut, cracked skin) on their enrolled finger. having two or more fingers enrolled will allow entrance in such cases. Multiple Fingerprint enrollment is possible only using SPHINX software for enrollment.

1. From the Option Menu, select 5, MultiFP

2. Select the option and ENTER



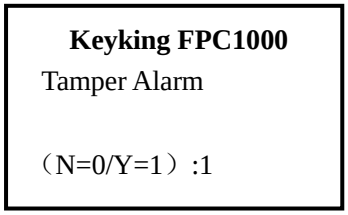


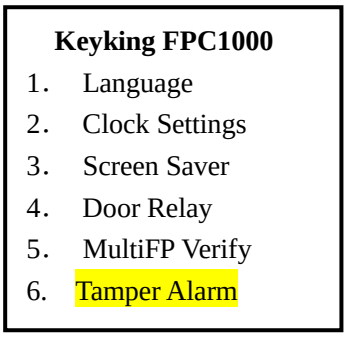
4.4.6 Tamper Alarm

FPC1000 has internal Tamper Switch alerting if the unit is being removed from its mounting bracket. If enabled, removal from the mounting will caused the unit to beep continuously and can also be used to activate alarms using Relay 2 and in the SPHINX software.

1. From the Option Menu, select 6, Tamper Alarm

2. Select the option and ENTER



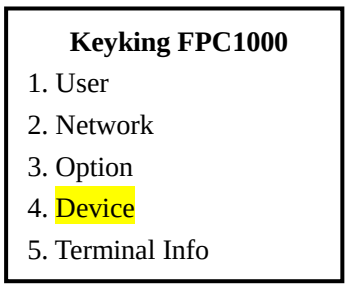


4.5 Device

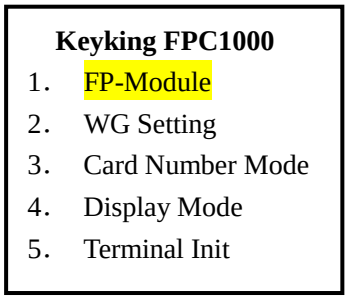
4.5.1 FP-Module

Fingerprint Module configuration allow customization of the fingerprint algorithm to match specific situations. These configurations are affecting the whole unit. Some can be personalized during the enrollment process to match personal conditions. It is recommended to NOT make any changes, unless needed to.

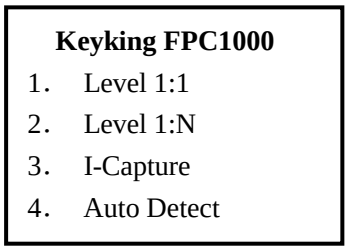
1. From the Main Menu select 4, Device



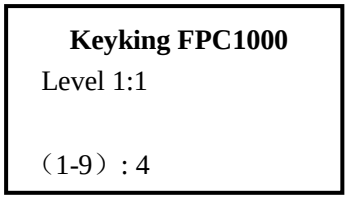
2. Select 1, FP-Module



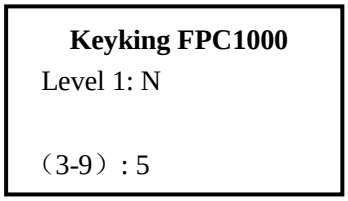
3. Select the parameter to be changed



1. Level 1:1: Algorithm Security Level on Card+FP and PIN+FP. Higher number, more strict may result in multiple attempts to enter. Too low, may result in unauthorized entrances.

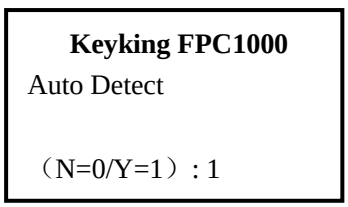


2. Level 1:N: Algorithm Security Level on FP. Higher number, more strict may result in multiple attempts to enter. Too low, may result in unauthorized entrances.



3. I-Capture – Not Functional in FPC1000 models

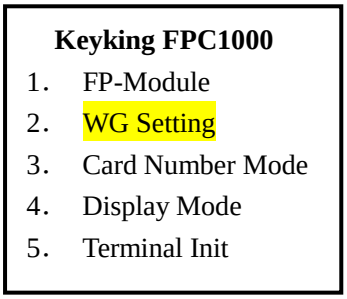
4. AutoDetect – Allow the sensor to initiate search when sensing finger. Disabling will require dual-factor or pressing a key to initiate fingerprint reading.



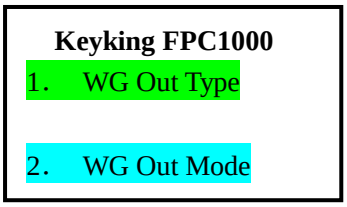
4.5.2 WG Setting

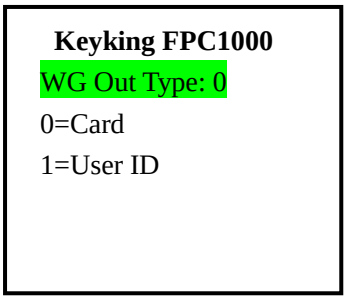
Use this setting if connecting the FTP1000 as Fingerprint Reader to a Door Controller using Wiegand Protocol. This type of connection provides higher security operation where the door is controlled from another controller located in the secured area.

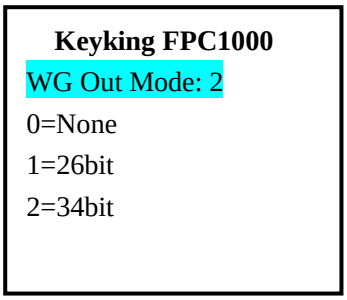
1. From the Device Menu, select 2, WG Setting.



2. Select the option







0 FPC1000 will send the Card Number – work only in Card, FP+Card, UserID+Card 1 FPC1000 will send the User ID number on any authorized user in all modes.	0 Wiegand Output OFF 1 26 BIT Format 2 34 BIT Format

4.5.3 Card Number Mode

Card Number Mode set the display of the card number on the screen (Display Mode 4-7) . It does not affect the operation of the FPC1000 and it's Weigand Input/Output

1. From the Device Menu, select 3, Card Number Mode

Keyking FPC1000
1. FP-Module
2. WG Setting
3. Card Number Mode
4. Display Mode
5. Terminal Init

2. Select the option and ENTER

0 = Decimal – normal number
1 = Hexadecimal – short numbering system
2 = Weigand format - Site Code and Card ID

Keyking FPC1000
Card Number Mode: 2
0=Dec
1=Hex
2=Wiegand

4.5.4 Display Mode

1. From Device Menu, select 4, Display Mode

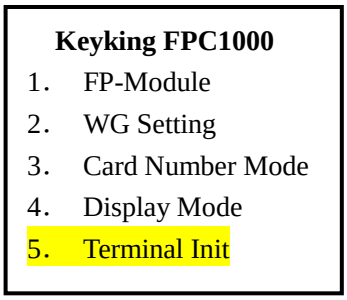
Keyking FPC1000
1. FP-Module
2. WG Setting
3. Card Number Mode
4. Display Mode
5. Terminal Init

2. Select the information to display when authorized ID is detected. Note that User Name can be used only if enrolled by SPHINX software.

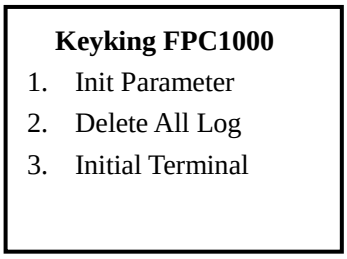
Keyking FPC1000
Display Mode: 3
0. None
1. User ID
2. UserName
3. UserName+UserID
4. CardNo
5. CardNo+UserID
6. CardNo+UserName
7. CardNo+Name+UserID

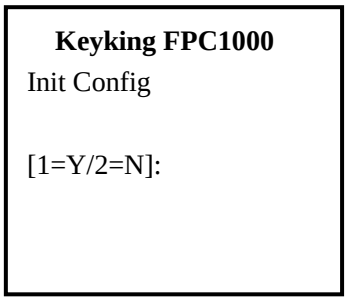
4.5.5 Terminal Initialize

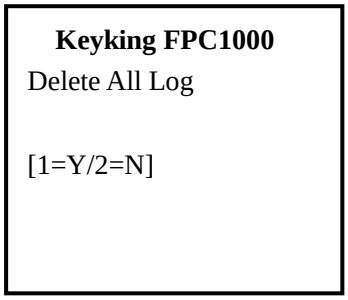
1. From Device Menu, select 5, Terminal Init

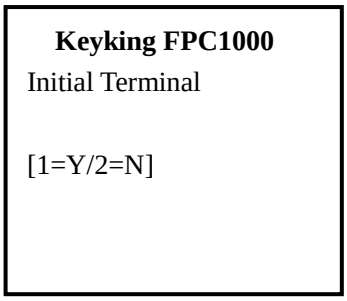


2. Select Initialization Type





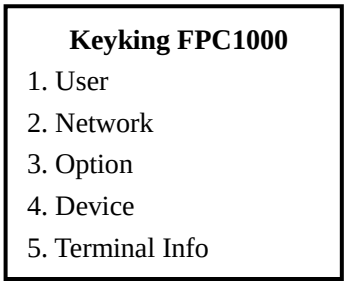


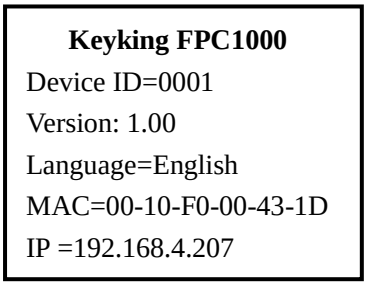


Reset unit configuration to Default Settings. Do NOT delete user data and history	Clear the database including user data and history. Do NOT change configuration	Return the unit to Factory Setting deleting ALL data and configurations – Like New

4.6 Terminal Info

1. From Main Menu, select 5, Terminal Info





3.5 Door Open Mode

1 FP Mode

Application: Put your finger on the biometric reader of FPC1000/2000, if verify passed, the screen will show that verify OK and display User ID, User Name and Card Number. Then the replay will response-door open. If verify failed, then FPC1000/2000 will beep three sounds and display Please try again, door remains closed.

Note: Only the registered personnel can pass verifying.

2 FP/Card

Application: Flash a registered card or FP

FPC1000can control a door by FP/Card

3 FP+Card

Application: Flash a registered card and FP.

Flash a registered card in front of FPC1000/2000. (read range 3-10cm), FPC1000/2000 will beep a long sound and then put your finger on the reader, if verify passed then door will open. The interval time between flashing card and verify FP is 8 seconds.

4 UserID+FP or UserID+Card

Application: Input your User ID by using the keypad and then verify your FP or flash your card to complete access process.

Chapter 5 Operation in Sphinx

5.1 Install driver for BioUSB10

1. If you use FPC1000 for enrollment, please ignore this step.
2. Go to your computer C:\program files (86)\keyking\sphinx4 folder and open Drivers folder.
3. Run the BioUSB10 instalation.

5.2 Select FPC1000 Series

1. **In Sphinx main screen, go to Setup menu and select communication configuration**
2. **Select the fingerprint tab**
3. Select " FPC1000 Series".

5.3 Search & Config FPC1000

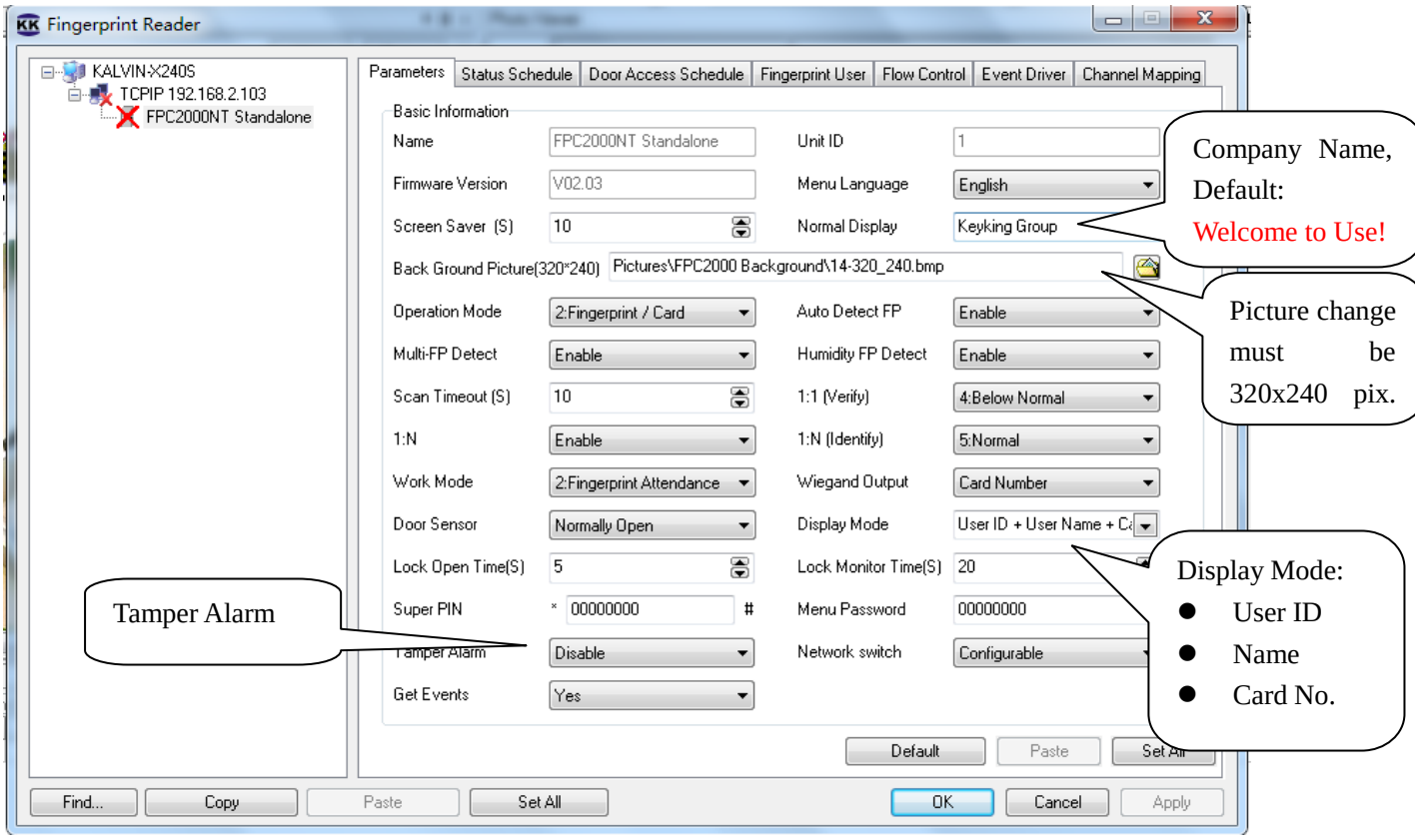
1. run the Controller Configuration process as any other controller
2. To customize the unit, select the fingerprint icon.

5.4 Enrolling finger for user

1. Enrolling fingerprint through one of FPC1000 in "personnel information / Fingerprint".
2. **Admin User**: Setup at least one user as a "Admin", then somebody else can not access the menu to manage it. If you did not setup any "Admin User", everybody can manage FPC1000 to add user or something else.

5.5 Transfer to FPC1000 terminal

5.6 FPC1000 setting



Here you can change the Company name and everything.

When you click Apply, then done.

Chapter 5 FAQ

NO	Descriptions	Possible Reason	Solution
1	● No lights, not responding ● Lights are ON, card swipe not responsive	● Power problem ● Card technology not compatible	● Check power supply ● replace card
2	● Lock stays opened	● Wrong lock wiring (NC/NO) ● Lock time too long ● REX Input configured wrong ● Exit Button short circuit	● Verify wiring ● Verify lock time ● Verify REX Config (NO/NC) ● Check Exit Button
3	● FP or card information missing	● Missing user information	● Verify enrollment ● Verify network connection
4	● Can not open door by flashing card or FP.	● Lock power problem ● Enrolment problem ● Access level not enabled	● check lock power and wiring ● Check enrolment ● Verify access level
5	● Can not open the door when it's Card+FP mode	● Either card or fingerprint are not enrolled ● Card and fingerprint not enrolled with same user	
6	● Door bell not working	● wiring error	
7	● Wrong Time/Date	● Setting was not complete ● No PC sync	● Set Time/Date in manage menu.
8	● FPC1000 does not respond with Fingerprint	1. finger positioned wrong 2. Pressure applied with finger 3. Unit overheating	1. lay finger flat covering the glass 2. Do not apply pressure 3. Cool unit down. Do not install in direct sunlight.