

User Manual

Thank you for choosing Keyking products. Please read this manual before using.



Model: FPC3002Q

QR Code & Biometric Fingerprint Reader



KEYKING GROUP

Index

Chapter 1 About FPC3002Q	4
1.1 Introduction	4
1.2 Model Number	5
1.3 FPC Family	6
1.4 Features	7
1.5 Installations instruction	8
1.5.1 FPC3002Q works as a reader (Wiegand)	8
1.5.2 FPC3002Q works as a reader (OSDP)	10
1.5.3 FPC3002Q works as a standalone	10
Chapter 2 Installation	12
2.1 American standard Installation	13
2.2 Europe standard Installation	13
Chapter 3 Wiring Diagram	15
3.1 FPC3002Q Parts.....	15
3.2 Wiring Diagram	16
3.3 Lock Wiring Diagram	17
3.4 TCP/IP Network	18
3.5 Work Mode.....	18
3.5.1 Work as Wiegand reader.....	18
3.5.2 Work as OSDP reader.....	20
3.5.3 Work as Standalone/Terminal	22
Chapter 4 Configuration Menu.....	24
4.1 User Management	25
4.1.1 Add Personnel / Admin	25
4.1.2 Delete Personnel	29
4.1.3 Delete All.....	29
4.1.4 Modify	30
4.2 Network.....	31
4.2.1 Unit ID.....	31
4.2.2 IP Option.....	32
4.2.3 IP Address	33
4.2.4 Subnet Mask.....	34
4.2.5 Gateway.....	35
4.2.6 Host IP	36
4.2.7 Host Port.....	37
4.3 Option.....	38
4.3.1 Language.....	38
4.3.2 Clock Setting	38
4.3.3 Screensaver	38
4.3.4 Door Relay.....	40
4.3.5 Tamper Alarm.....	41
4.3.6 Work Mode	41
4.4 Device	42

4.4.1 FP Level.....	42
4.4.2 Wiegand Setting	42
4.4.3 Card Number Mode.....	44
4.4.4 Display Mode.....	44
4.4.5 Terminal Initial.....	45
4.5 Terminal Info	45
4.6 Quick Operation on terminal.....	47
Chapter 5 Operation in Sphinx.....	48
5.1 Install driver for BioUSB-SC03	48
5.2 Select FPC3002Q Series.....	48
5.3 Search & Setup Unit ID.....	49
5.3.1 Setup Unit ID (work as an OSDP reader).....	49
5.3.2 Change Unit ID (work as an OSDP reader).....	51
5.4 Configure FPC3002Q	53
5.4.1 Parameter	53
5.4.2 Status Schedule	56
5.4.3 Door Access Schedule.....	57
5.4.4 Fingerprint User	57
5.4.5 Flow Control	57
5.4.6 Events Drive.....	57
5.4.7 Alarm Clock.....	57
5.4.8 Wiegand Format.....	57
5.4.9 Channel Mapping.....	58
5.4 Enrolling finger for user.....	58
5.5 Classic application	59
5.5.1 Change Company name	59
5.5.2 Change BackGround picture.....	60
5.5.3 Choose the FPC3002Q location (Work as terminal).....	60
5.5.4 Choose the Unit ID of external OSDP reader (Work as terminal).....	61
5.5.5 To open the door by Temporary PIN	62
5.6 Screen Message.....	65
5.6.1 Biometric Verification.....	65
5.6.2 Card Verification	66
5.6.3 QR Code Verification.....	66
5.6.4 Combination Verification.....	67
Chapter 6 FAQ	68

Chapter 1 About FPC3002Q

1.1 Introduction

KEYKING's FPC3002Q is a Networked/Stand-Alone biometric fingerprint & QR Code access controller.

Multi identify mode of FPC3002Q:

1. Fingerprint,
2. QR Code (Visitor option)
3. PIN
4. Card
5. Card + Fingerprint, Card + Pin, Fingerprint + Pin

Multi-mode operation:

- **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 FPC3002Q 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 allows 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** – Connecting the FPC3002Q OSDP/Wiegand Output to an access control controller, the data will be transferred to Access controller and will bring higher security.
- **QR Code Reader**-Supports QR code scanning, available to visitors;
- **Proximity (Mifare) card Reader**-Supports Proximity & Mifare card;

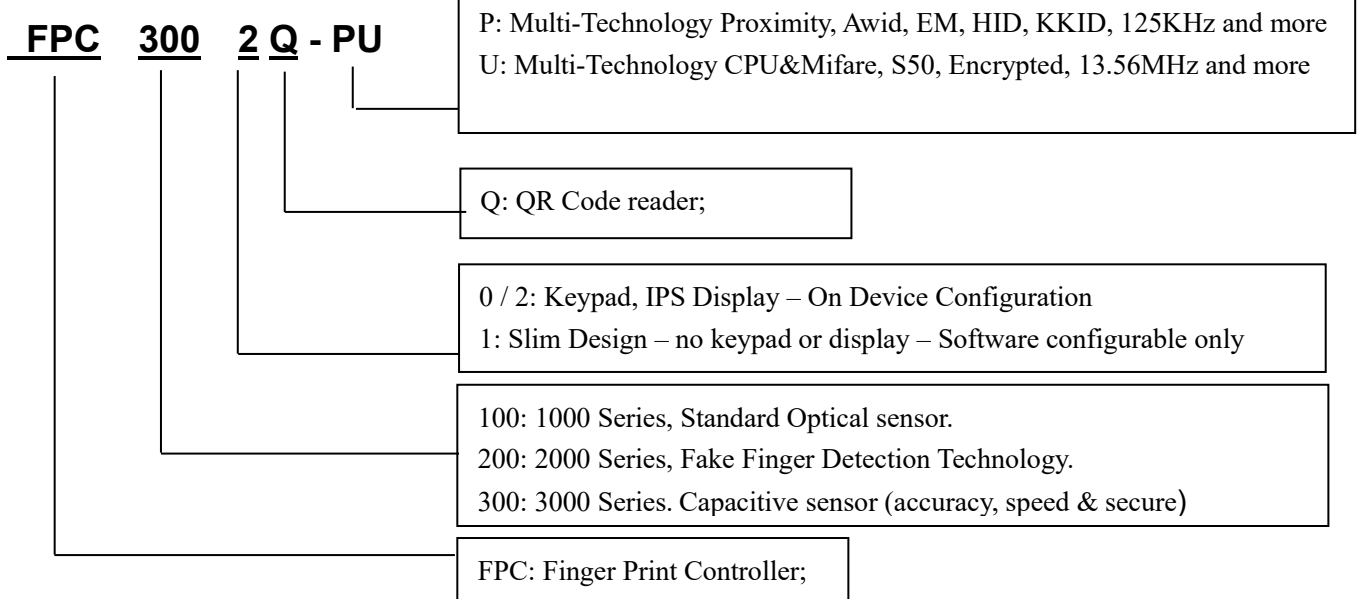
FPC3002Q can be used as Time & Attendance terminal except access control functions. The IPS screen can be customized and show the employee's name when authorized.

FPC3002Q may be installed as Entry device or IN/OUT system where the FPC3002Q is used for entry and for exit, an attached Exit Button or Card Reader or additional FPC3002Q are connected.



1.2 Model Number

Model Options:



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	1 Series Biometric Readers	Picture
FPC1000-P	CPU: 400MHz DSP (4MB Flash memory +8 MB RAM), POE; Capacity: 1,000 templates, 200,000 transactions; 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), POE; Capacity: 1,000 templates, 200,000 transactions; 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: 400MHz DSP (4MB Flash memory +8 MB RAM), POE; Capacity: 1,000 templates, 200,000 transactions; 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: 400MHz DSP (4MB Flash memory +8 MB RAM), POE; Capacity: 1,000 templates, 200,000 transactions; 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	
BioUSB-01	Biometric USB enrollement Finger Print Reader for direct connection to PC. Fully integrated with KEYKING software, No reader	

Card Readers	3 Series Biometric Readers	Picture
FPC3001-P	CPU: 32 bits ARM Cortex-M4 Processor Capacity: 3,000 (5,000 Option) fingerprints with on device memory; Unlimited using SPHINX-4 On-Line Support Card types: Proximity, HD, AWID, EM, KKID. Fingerprint Sensor: Optical Authentication modes: Card / Fingerprint, Fingerprint, Card + Fingerprint Wiegand In & Out Communication Interface: Wiegand In & Out Dimension: W45 xH135xD58 / 490g	
FPC3001-U	CPU: 32 bits ARM Cortex-M4 Processor Capacity: 3,000 (5,000 Option) fingerprints with on device memory; Unlimited using SPHINX-4 On-Line Support Card types: Mifare/DesFire, Mifare Sector, CPU Fingerprint Sensor: Optical Authentication modes: Card / Fingerprint, Fingerprint, Card + Fingerprint Wiegand In & Out Communication Interface: Wiegand In & Out Dimension: W45 xH135xD58 / 490g	
FPC3002Q	Metal case Fingerprint biometric reader; CPU: ARM, 32 Bits, Cortex-M4, 200MHz Fingerprint Capacity: 3,000 (5,000 Option) PCS Support Card types: Proximity, Awid, EM, Hid, KeyKing, 125KHz; S50, Mifare, 13.56MHz Authentication modes: Fingerprint/Card/Qr Code/Bluetooth(Shake), Card + fingerprint... Interface: Wiegand, OSDP, TCP Voltage: 12VDC, POE support Dimension: 161mm L x66mm W x 25mm / 490 g	
FPC3002	Metal case Fingerprint biometric reader; CPU: ARM, 32 Bits, Cortex-M4, 200MHz Fingerprint Capacity: 3,000 (5,000 Option) PCS Support Card types: Proximity, Awid, EM, Hid, KeyKing, 125KHz; S50, Mifare, 13.56MHz Authentication modes: Fingerprint/Card/ No QR Code /Bluetooth(Shake), Card + fingerprint... Interface: Wiegand, OSDP, TCP Voltage: 12VDC, POE support Dimension: 161mm L x66mm W x 25mm / 490 g	
BioUSB-03SC	Biometric USB enrolment Finger Print Reader for direct connection to PC. Fully integrated with KEYKING software, No reader	

1.4 Features

- Capacitive sensor, Live fingerprint check, high security;

- Faster identify: 1 sec searching for 3,000 pcs templates.
- Multi-Core CPU with multithread operation.
- Self-Test, Watchdog Timer for better stability
- No fingerprint image stored – fingerprint converted to mathematical template code.
- Uninterrupted operation on-line and off-line, independent operation.
- IPS (In-Plane Switching) color display – customizable background and employee data.
- 100M Network, PoE (Power over Ethernet) supported;
- Exit Button (REX) and Door Sensor inputs.
- 3A Door Relay.
- AUX Input – programmable, can be used for intercom or alarm operation
- AUX Relay – Default is for DoorBell, programmable, can be used for alarms or other feature
- IP54 Ingress Protection rated.

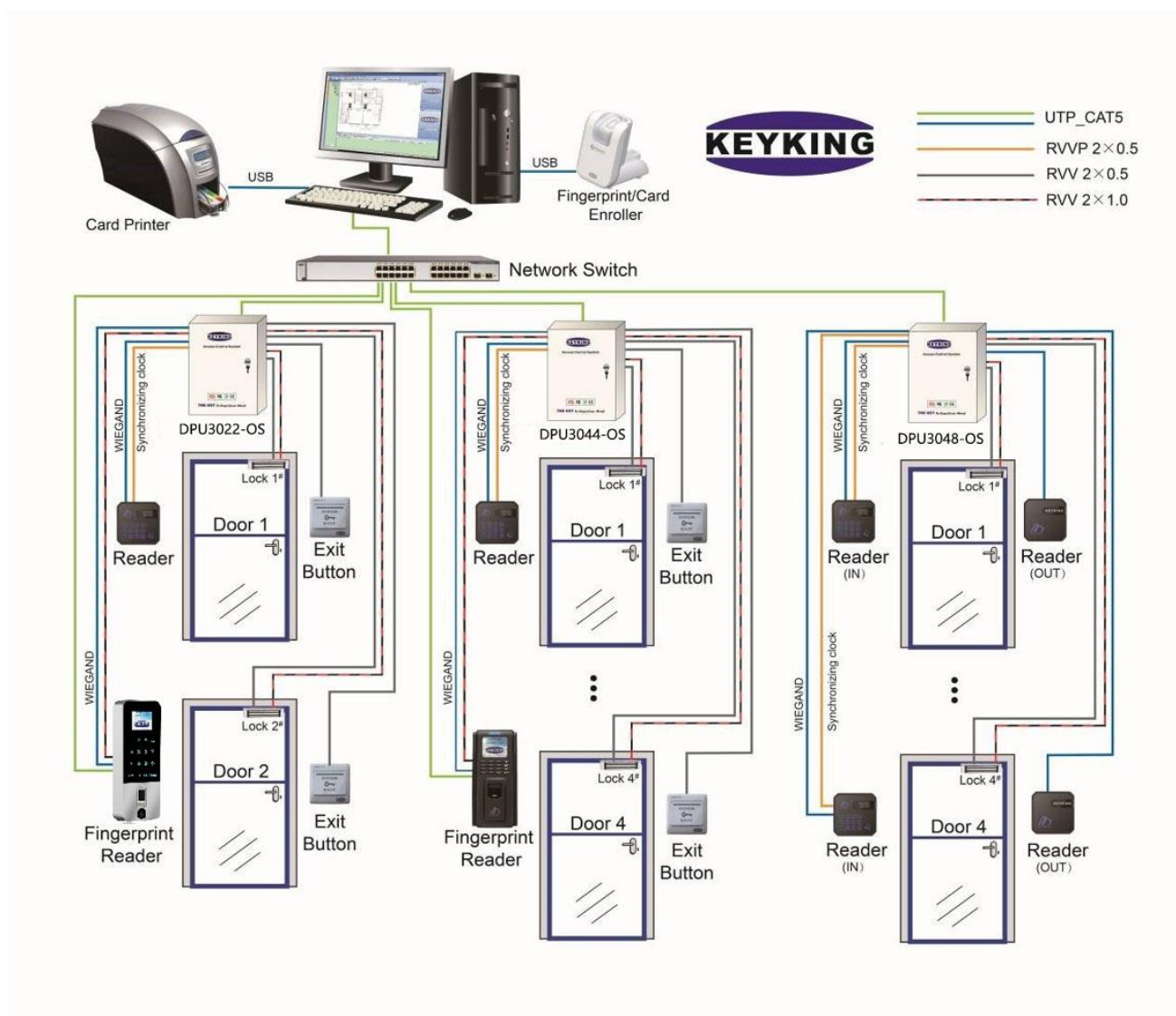
Specification:

- CPU: ARM, 32Bits, Cortex-M4, 200MHz DSP
- Fingerprint capacity: 3,000 pcs templates as default, and 5,000 option
- Identify Modes: FP / Card / QR Code, Card + FP, PIN+FP, Card + PIN;
- Interface:
 - (A) Wiegand: Wiegand Output only, will not support an external reader.
 - (B) OSDP: In & Out;
- Networking: TCP/IP, 100M based
- Power Over Ethernet: IEEE 802.3af (including 12Vdc 500mA output)
- Operating voltage: 12VDC
- Operating current: ≤500mA
- Standby current: ≤260mA
- Temperature: -20°C to 65°C
- Humidity: 0-95%
- Dimension: 161mm L x66mm W x 25mm
- Weight: 490g

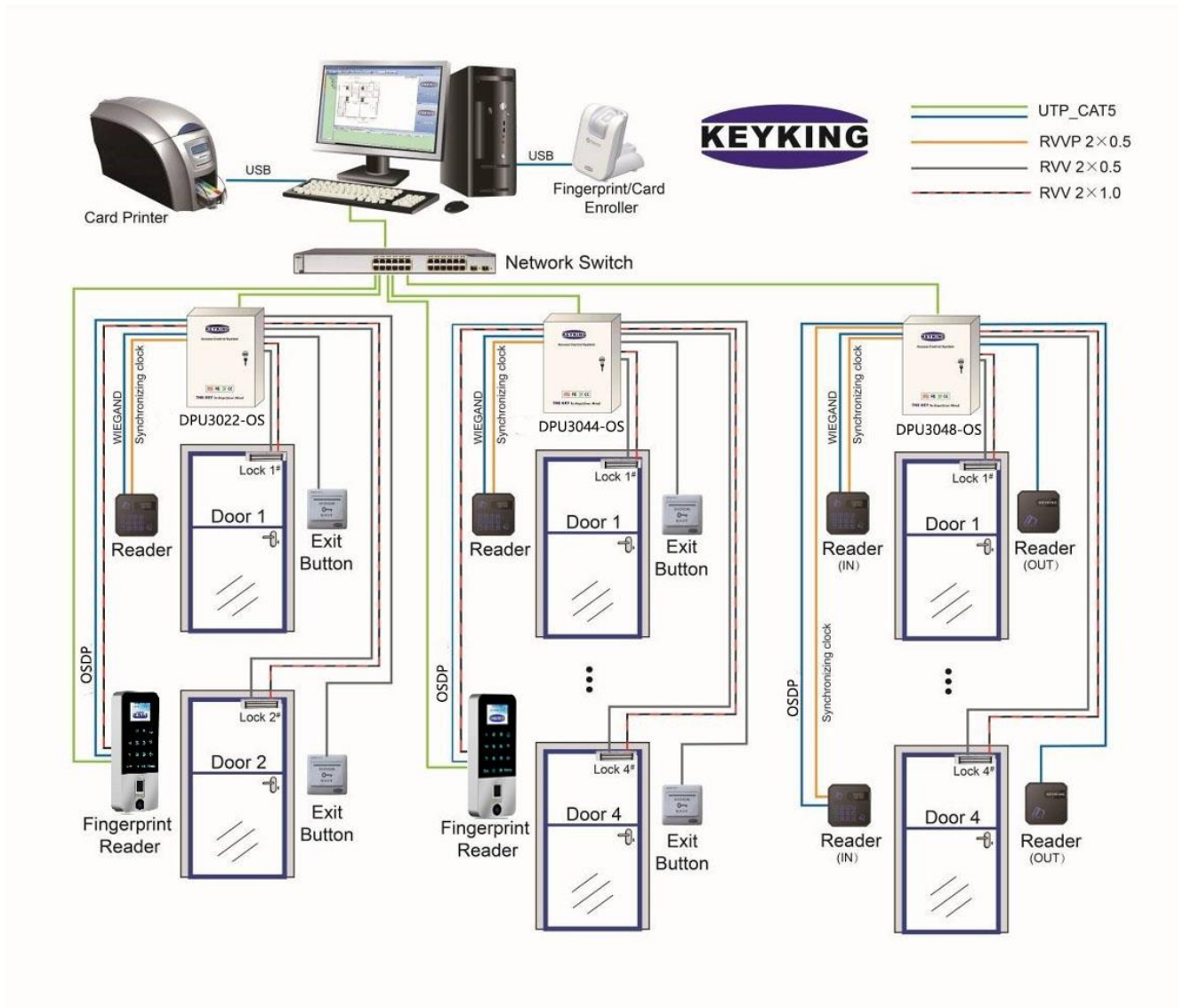
1.5 Installations instruction

1.5.1 FPC3002Q works as a reader (Wiegand)

We suggest to use a separated power supply for FPC3002Q because it requires minimum 500 mA power supply.



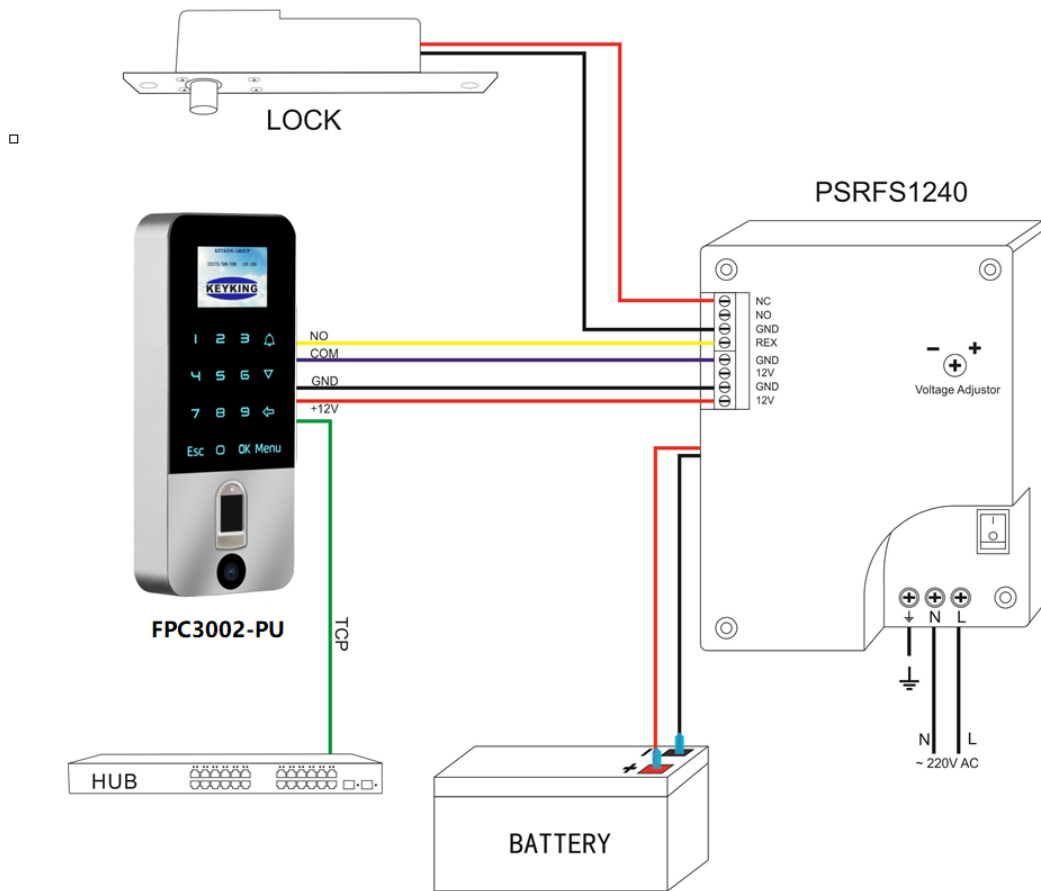
1.5.2 FPC3002Q works as a reader (OSDP)



1.5.3 FPC3002Q works as a standalone

3 options:

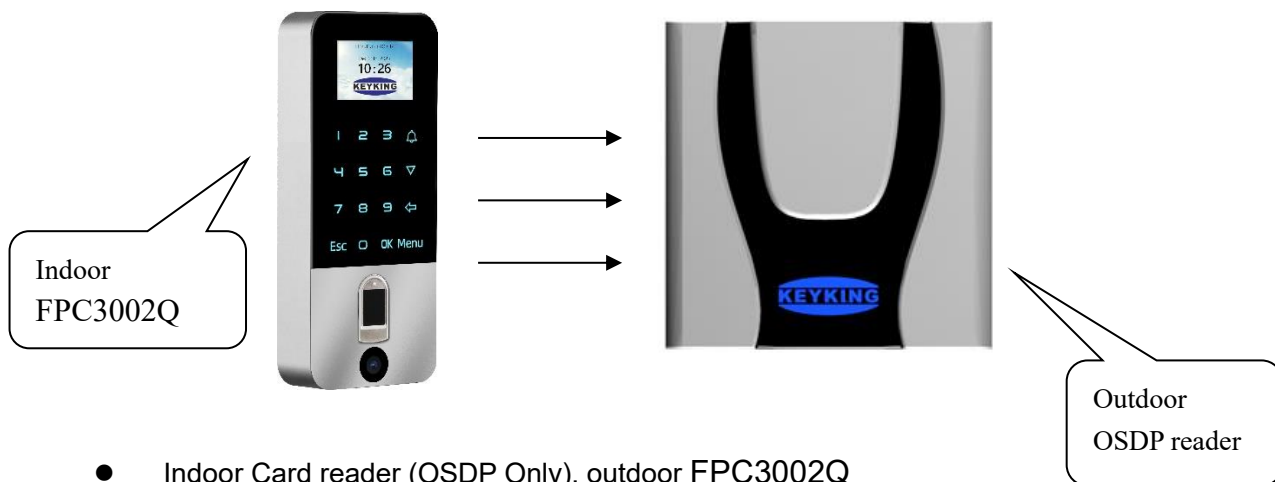
- **Standalone**, no external reader



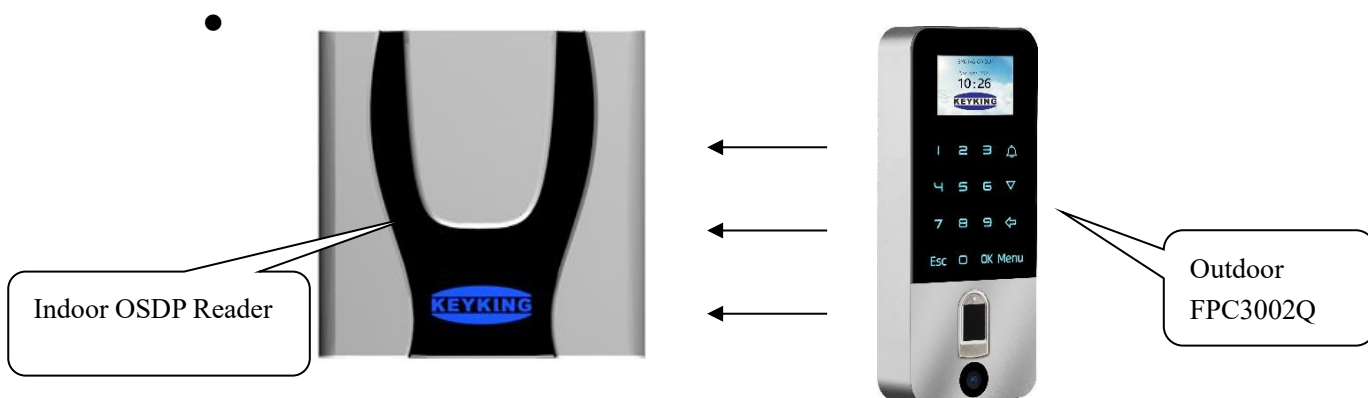
Notes:

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

- Outdoor Card reader (OSDP Only), indoor FPC3002Q



- Indoor Card reader (OSDP Only), outdoor FPC3002Q



Chapter 2 Installation

2.1 American standard Installation

- Mount the back plate on the American electric box by 2 pcs M4 screws. Please refer to picture 2.
- Connect all wires to FPC3002Q.
- Fix FPC3002Q on the back plate. Please refer to picture 3.
- Fasten the fixed screw from the bottom. Please refer to picture 4.

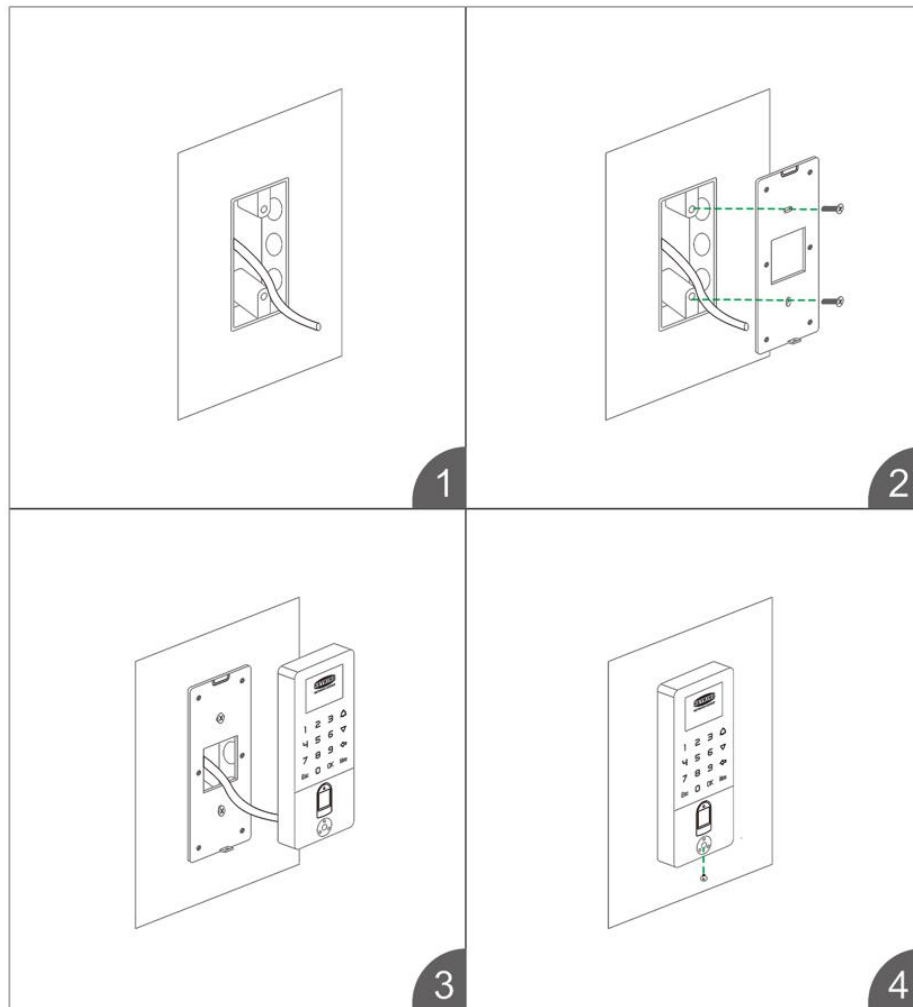


Figure 2-1 American electric standard installation

2.2 Europe standard Installation

- Mount the quadrate back plate on the Europe electric box by 2 pcs M4 screws. Please refer to picture 2.
- Mount the back plate on the quadrate back plate by 2 pcs M4 screws. Please refer to

picture 3.

- Connect all wires to FPC3002Q.
- Fix FPC3002Q on the back plate. Please refer to picture 4.
- Fasten the fixed screw from the bottom. Please refer to picture 5.

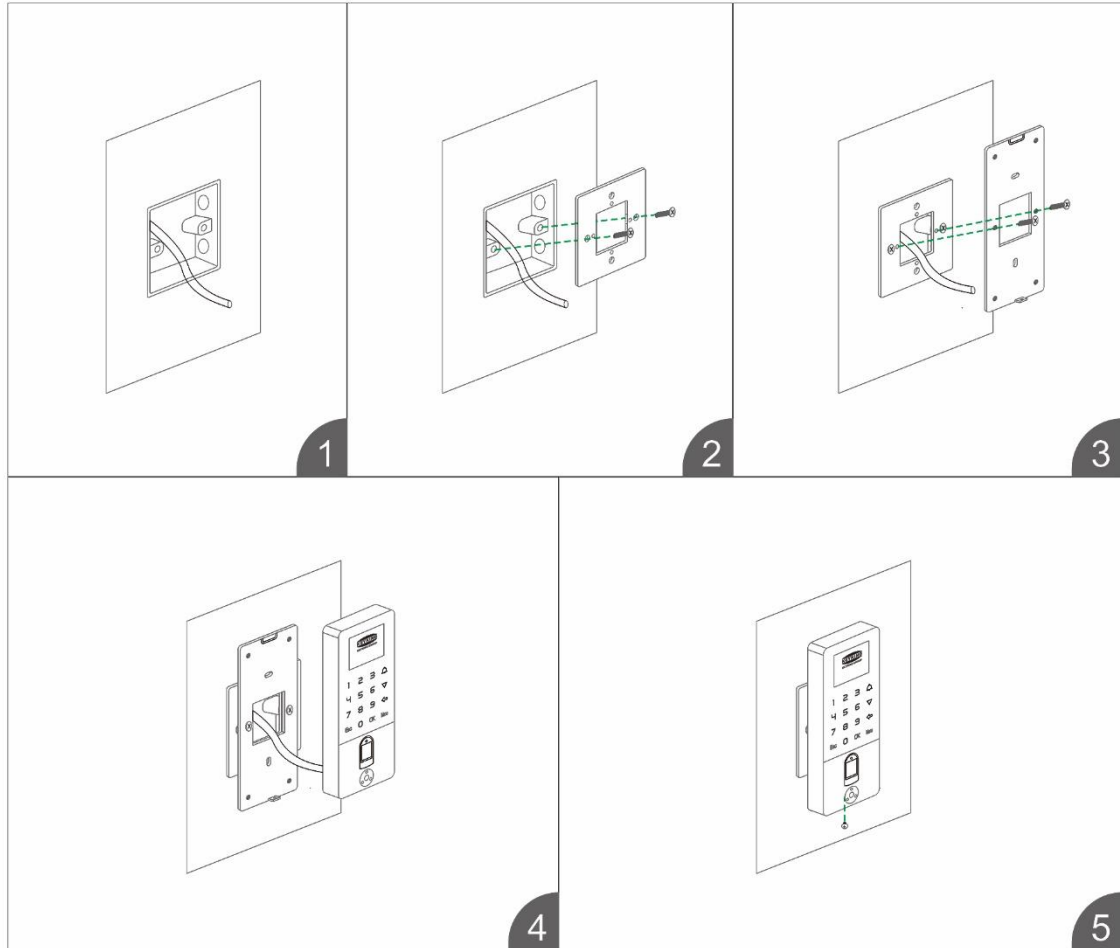


Figure 2-1 [Europe](#) electric standard installation

Chapter 3 Wiring Diagram

3.1 FPC3002Q Parts

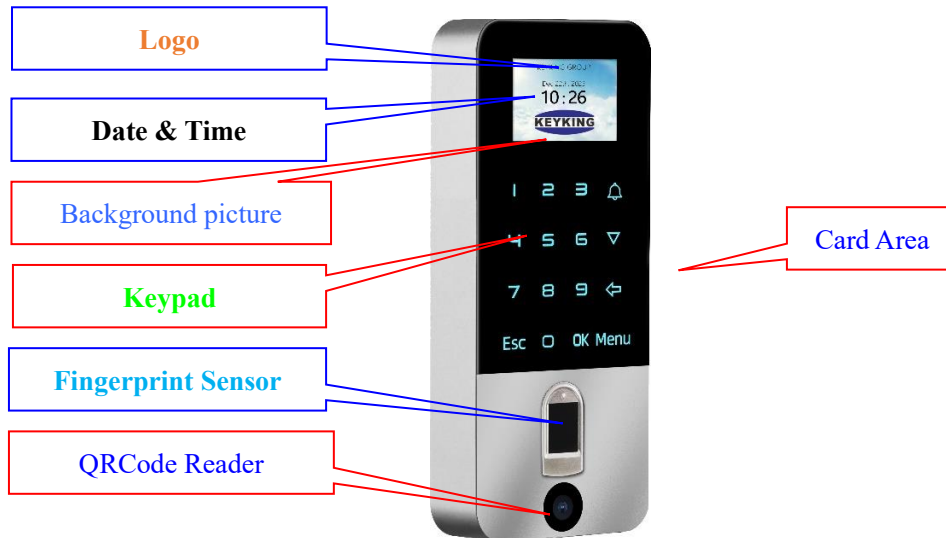





Figure 3-1

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	OK	Confirm Data

3.2 Wiring Diagram

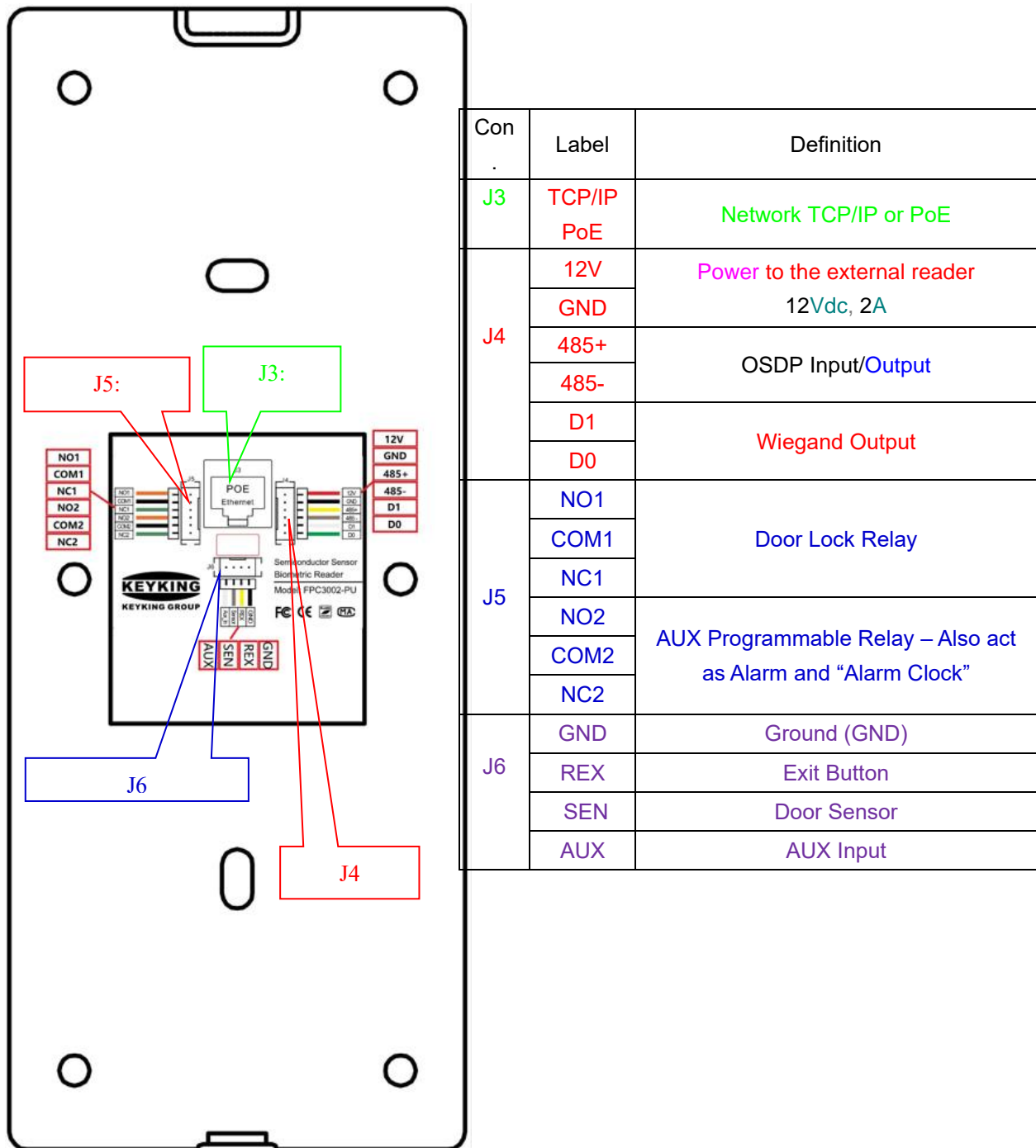


Figure 3-2

Do not connect Power Supply if using PoE!

3.3 Lock Wiring Diagram

J4: Relay Output – Relay 1 (Lock Control)

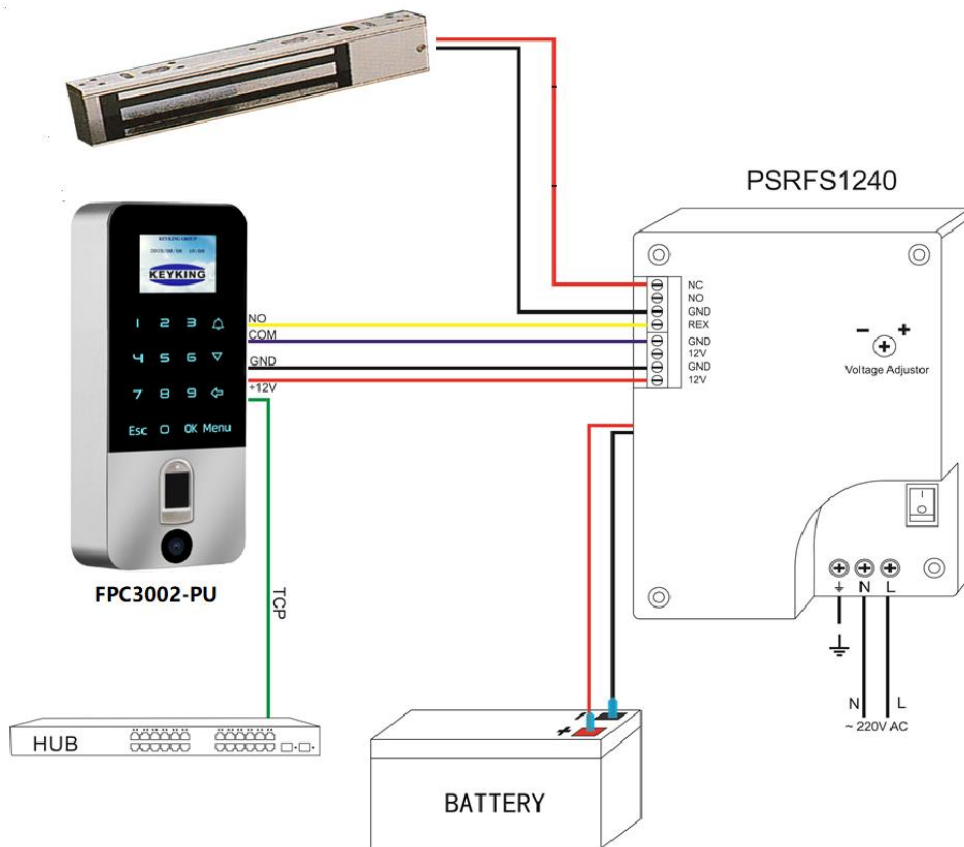


Figure 3-5 MagLock (Fail safe)

Notes:

- ✧ recommended power supply PSRFS1240 – incorporate isolation relay and backup battery support.
- ✧ REX – Exit Button –
 - May be connected via the PSRFS1240 – in such case, do not use Door Sensor to prevent false alarms from the unit.
 - Or direct to the FPC3002Q using GND & SEN connections. If connected directly to FPC3002Q, 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

FPC3002Q TCP/IP network

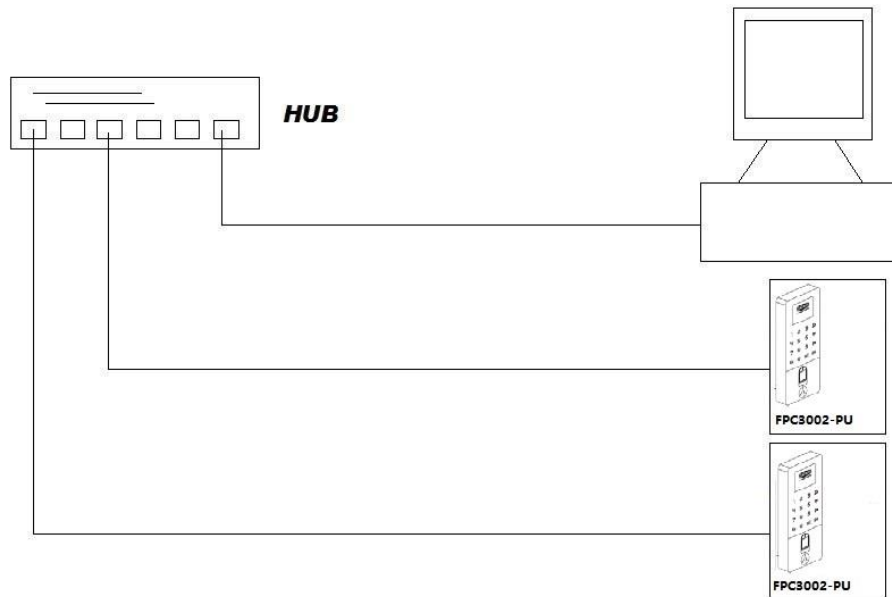


Figure 3-8

TCP/IP crystal head

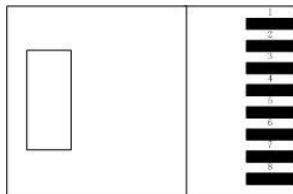


Figure 3-9

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

Figure 3-2

3.5 Work Mode

3.5.1 Work as Wiegand reader.

Wiring stpes:

1. Connect network cable to the RJ45 of TA3002.
2. Connect Wiegand Output of FPC3002Q to Access controller.

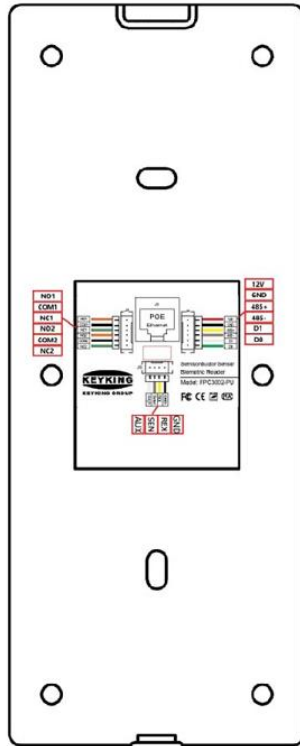
NO.	FPC3002Q	KeyKing Reader		Remark
		Color	Access Controller	
1	+12V	Red	7—14VDC	If using POE, do not power from panel.
2	Data 0	Green	Data0	
3	Data 1	White	Data1	

4	GND	Black	GND	
---	-----	-------	-----	--

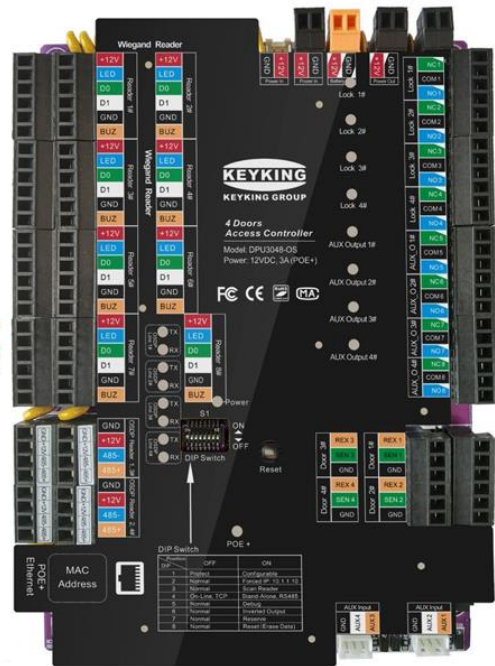
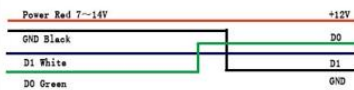
Note:

- If network cable can provide power to FPC3002Q through POE, please do not connect 12VDC to FPC3002Q from access controller.

Wiegand Reader Wiring

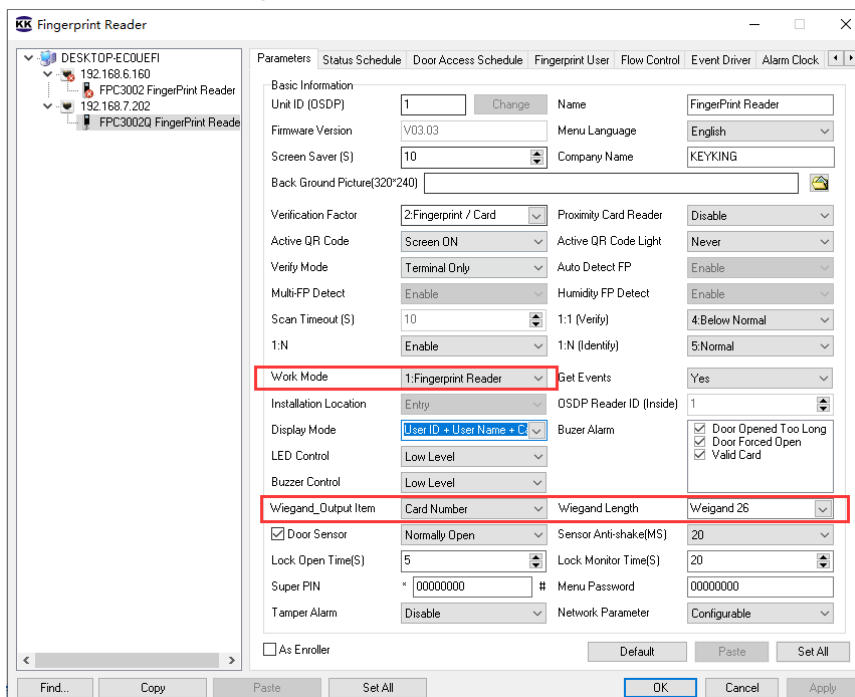


FPC3002

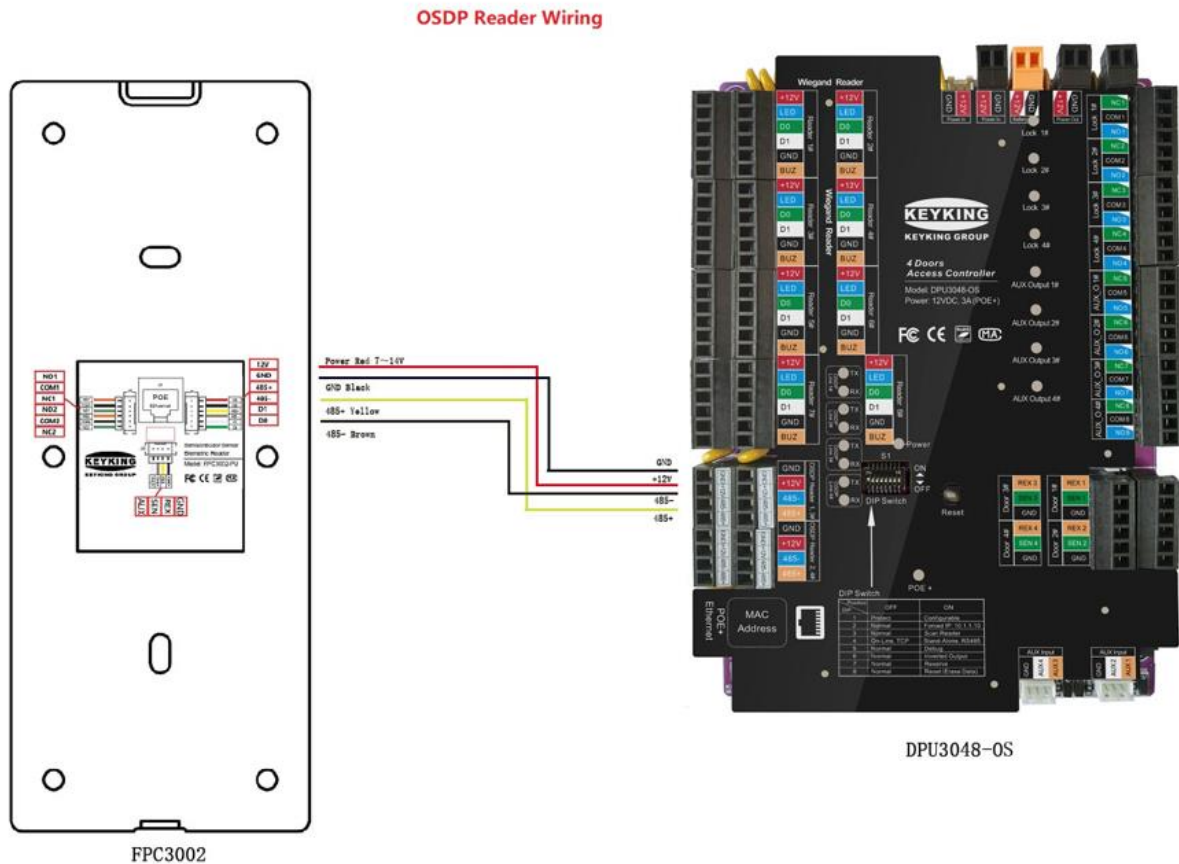


DPU3048-OS

The access control software directly connects to FPC3000 device interface configuration, click Setup/Hardware/Fingerprint Reader/FPC3000:



3.5.2 Work as OSDP reader.



3.5.2.1 Power supply (Wiring steps):

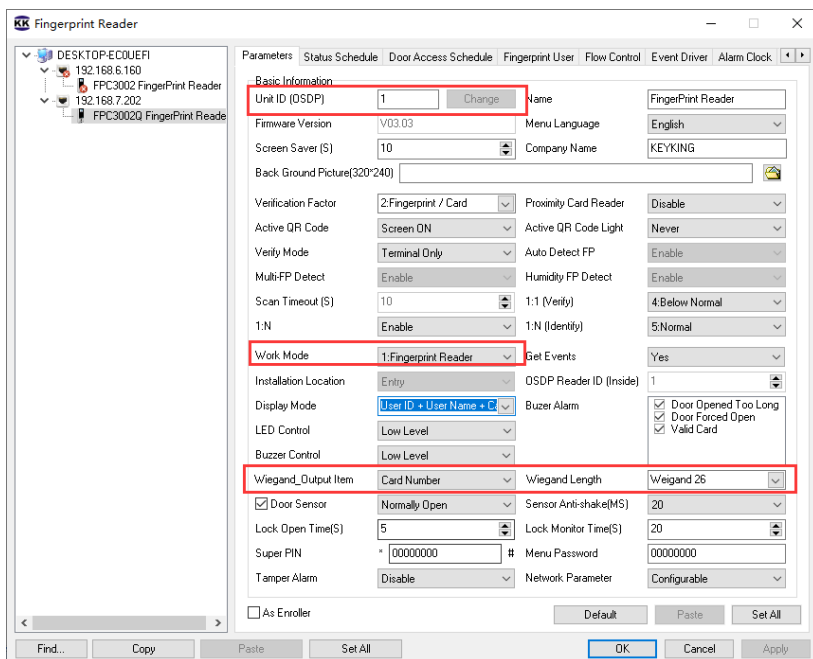
1. Connect network cable to the RJ45 of TA3002.
2. Connect OSDP Output of FPC3002Q to Access controller.

NO.	FPC3002Q	KeyKing Reader		Remark
		Color	Access Controller	
1	GND	Black	GND	
2	+12V	Red	7—14VDC	If using POE, do not power from panel.
3	RS485-	Brown	RS485-	
4	RS485+	Yellow	RS485+	

Note:

- If network cable can provide power to FPC3002Q through POE, please do not connect 12VDC to FPC3002Q from access controller.

The access control software directly connects to FPC3002 device interface configuration, click Setup/Hardware/Fingerprint Reader/FPC3000:



3.5.2.2 Keypad Message

When FPC3002Q work as an osdp reader, it will output the Keypad value to Access Controller through OSDP socket & Wiegand socket.

OSDP socket: It will output the Keypad value only when FPC3002Q work as an OSDP reader.

Wiegand socket: It always output the Keypad value no matter which mode FPC3002Q works as.

Keypad Value Table:

Keypad (FPC3002Q)	KeyKing Common Reader		Remark
	Keypad	Keypad Value	
0	0	0000	
1	1	0001	
2	2	0010	
3	3	0011	
4	4	0100	
5	5	0101	
6	6	0110	
7	7	0111	
8	8	1000	
9	9	1001	
Esc (*)	*	1010	
Ok (#)	#	1011	

The reader will process the keypad entries in the reader and then transmits the data to the host system via the Wiegand data lines. The reader outputs each key as an ASCII encoded hexadecimal digit. The decoding of the message sent through the Wiegand interface is the only processing required of the host system. The user interface has been implemented in the most generic fashion to give the integrator the most flexibility.

The keypad message follows a basic format.

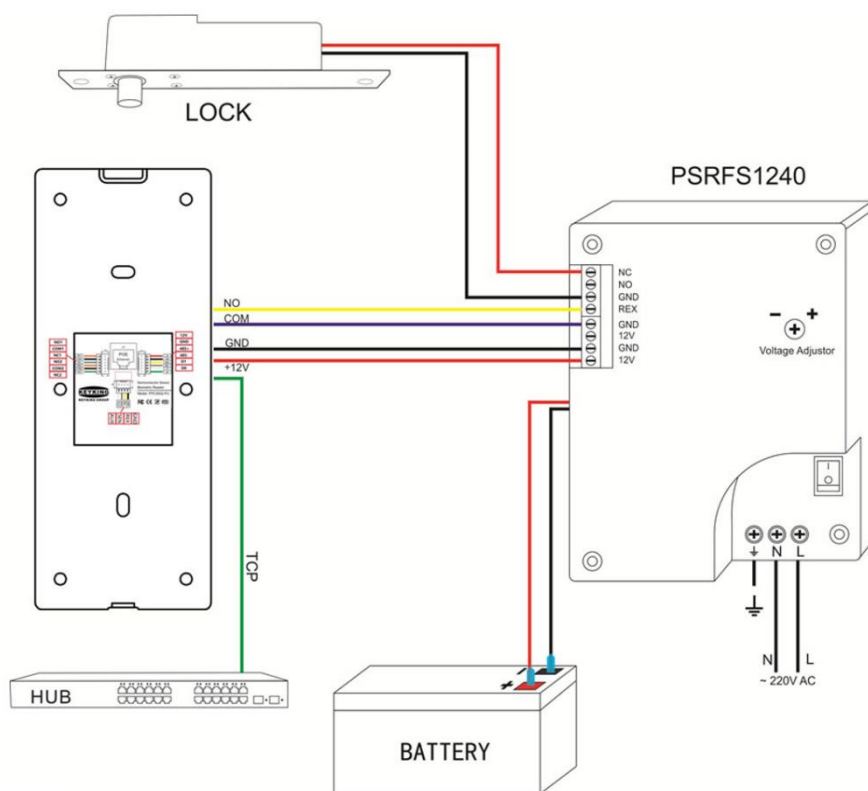
0 = 0000	4 = 0100	8 = 1000
1 = 0001	5 = 0101	9 = 1001
2 = 0010	6 = 0110	* = 1010
3 = 0011	7 = 0111	# = 1011

The reader will transmit every key value individually, after it was pushed.

For example:

- If you push “1”, then the reader will transmit “0001” to the host (Panel or controller).
- If you push “1” and “2”, the reader will transmit “0001” to the host (Panel or controller), then transmit “0010” to the host.

3.5.3 Work as Standalone/Terminal



- The relay of FPC3002Q is not enough strong to control the big current required electronic lock, such as drop bolt or magnetic lock, so we suggest to use a separated power supply to power the lock.
- Only when you use a small current required strike, the relay of FPC3002Q can control the strike.

The access control software directly connects to FPC3002 device interface configuration, click Setup/Hardware/Fingerprint Reader/FPC3000:

KK Fingerprint Reader

Parameters | Status Schedule | Door Access Schedule | Fingerprint User | Flow Control | Event Driver | Alarm Clock

Basic Information

Unit ID (OSDP) Name

Firmware Version Menu Language

Screen Saver (S) Company Name

Back Ground Picture(320*240)

Verification Factor Proximity Card Reader

Active QR Code Active QR Code Light

Verify Mode Auto Detect FP

Multi-FP Detect Humidity FP Detect

Scan Timeout (S) 1:1 (Verify)

1:N 1:N (Identify)

Work Mode Get Events

Installation Location OSDP Reader ID (Inside)

Display Mode Buzzer Alarm

LED Control

Buzzer Control

Wiegand_Output Item Wiegand Length

☒ Door Sensor Sensor Anti-shake(MS)

Lock Open Time(S) Lock Monitor Time(S)

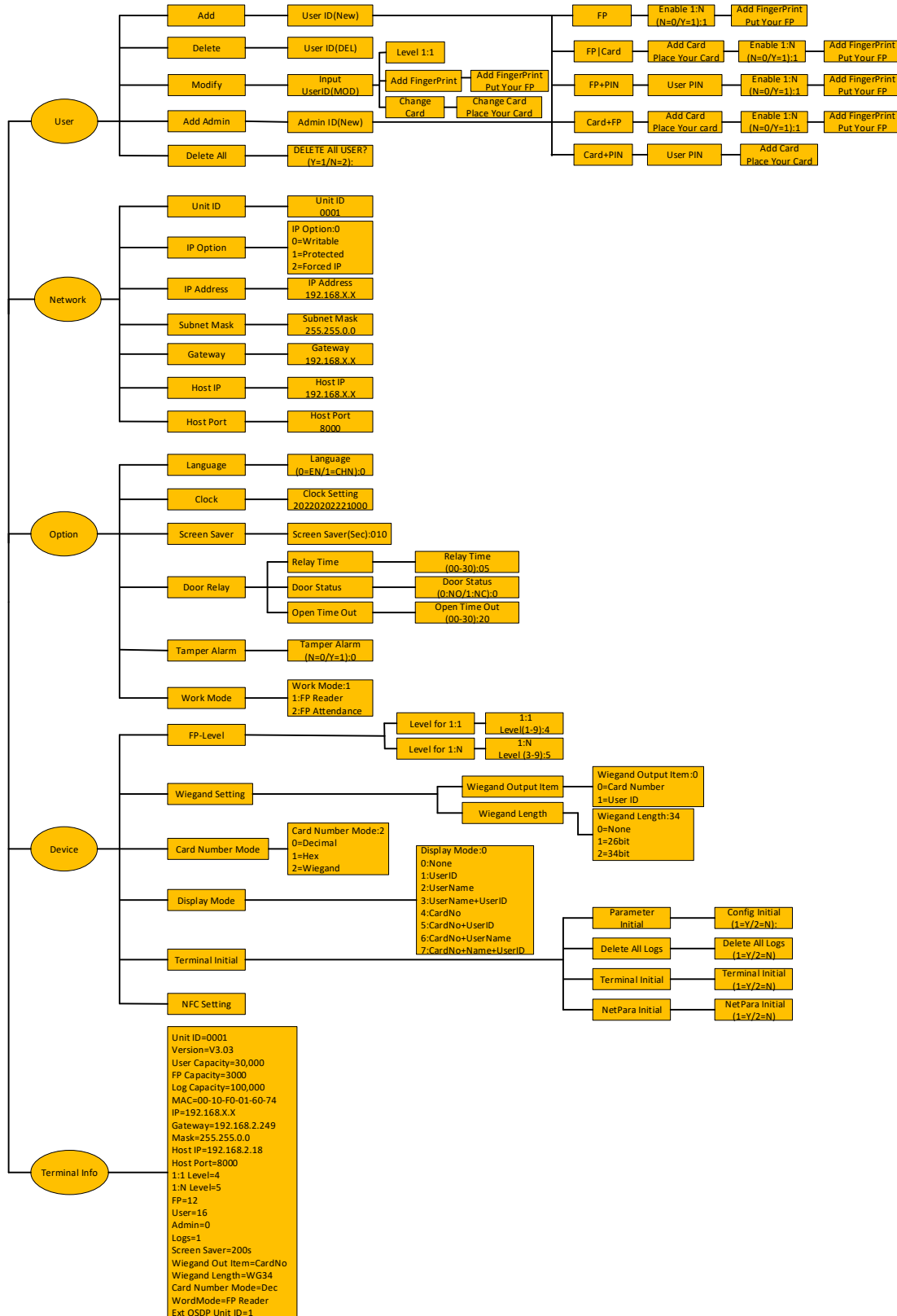
Super PIN # Menu Password

Tamper Alarm Network Parameter

☐ As Enroller

Chapter 4 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 User Management

4.1.1 Add Personnel / Admin

1. Press Menu to enter management menu when FPC3002Q 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 - 1-9 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

Keyking FPC3002Q

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

Keyking FPC3002Q

1. Add
2. Delete
3. Modify
4. Add Admin
5. Delete All

Keyking FPC3002Q

New ID (New)

--123456-----

Keyking FPC3002Q

1. FP
2. FP|Card
3. FP+PIN
4. CARD +FP
5. CARD +PIN

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 PIN+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 three finger scans, let the unit 2 seconds scan time for each finger.

If scan failed, the FPC3002Q will go back to the main menu and the process will begin from the Main Menu 4.2.1

Keyking FPC3002Q

1. **FP**
2. FP|Card
3. FP+PIN
4. CARD +FP
5. CARD +PIN

Keyking FPC3002Q

Enable 1: N

:
(N=0/Y=1) :1

Keyking FPC3002Q

Add FingerPrint

Put Your FP

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

Keyking FPC3002Q

1. FP
2. FP|Card
3. FP+ PIN
4. CARD +FP
5. CARD +PIN

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

Keyking FPC3002Q

Add Card

Place Your Card

3. Hit ENTER to go to the next screen

Level 1:N apply to Card+Fingerprint mode ONLY. The number represent how strict the verification is done. 5 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.

Keyking FPC3002Q

Enable 1: N

:
(N=0/Y=1) :1

4. Hit ENTER to go to the next screen

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

If scan failed, the FPC3002Q will go back to the main menu and the process will begin from Main Menu 4.2.1

Keyking FPC3002Q

Add FingerPrint

Put Your FP

4.2.1.3 FP+PIN

1. Press 3 to enter add FP+PIN 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.

Keyking FPC3002Q

1. FP
2. FP|Card
3. **FP+ PIN**
4. CARD +FP
5. CARD +PIN

2. Enter the PIN; system will enter the next interface after a beep sound

Keyking FPC3002Q

User PIN

3. The number represent how strict the verification is done. 5 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+PIN mode prevent false positive. Hit ENTER to go to the next screen.

Keyking FPC3002Q

Enable 1: N

:
(N=0/Y=1) :1

4. Follow the instructions on the screen, the unit will require three finger scans, let the unit 2 seconds scan time for each finger. If scan failed, the FPC3002Q will go back to the main menu and the process will begin from Main Menu 4.2.1

Keyking FPC3002Q

Add FingerPrint

Put Your FP

4.2.1.4 Card+FP

1. Press 4 to enter add Card+FP interface.

This mode uses Dual-Factor ID. Use this mode in cases where the person fingerprint quality is very low enforcing low 1:N 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 25 seconds after ID entered.

Keyking FPC3002Q

1. FP
2. FP|Card
3. FP+PIN
4. **CARD +FP**
5. CARD +PIN

2. Swipe the card; system will enter the next interface after a beep sound.

Keyking FPC3002Q

Add Card

Place Your Card

3. Follow the instructions on the screen, the unit will require three finger scans, let the unit 2 seconds scan time for each finger. If scan failed, the FPC3002Q will go back to the main menu and the process will begin from Main Menu 4.2.1

Keyking FPC3002Q

Enable 1: N

:
(N=0/Y=1) :1

Keyking FPC3002Q

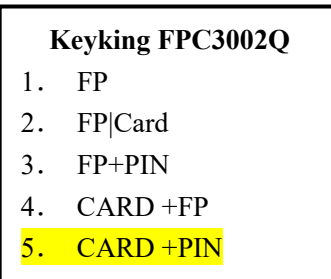
Add FingerPrint

Put Your FP

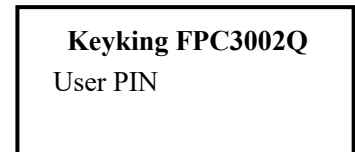
4.2.1.5 Card +PIN

1. Press 5 to enter add Card +PIN.

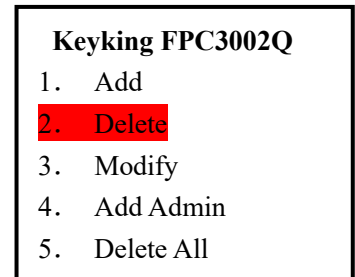
This mode uses Dual-Factor ID, though do not use Fingerprint as one of the identifications. It is not recommended to use this mode, unless, there is a specific problem with an individual that can not use Fingerprint.



2. Enter the PIN; system will enter the next interface after a beep sound

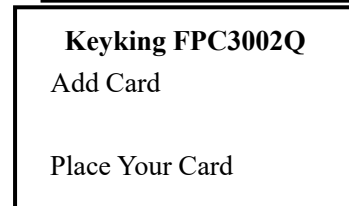


3. Swipe the card in middle of the unit; system will enter the next interface after a beep sound .

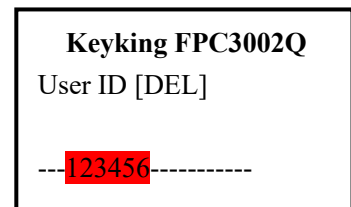
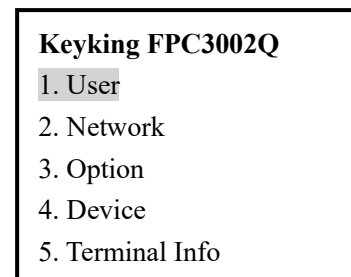


4.1.2 Delete Personnel

1. Enter the main menu and select 1 User



- 2 Press 2 Delete.



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

4.1.3 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

4.1.4 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.

Keyking FPC3002Q

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

Keyking FPC3002Q

1. Add
2. Delete
3. Modify
4. Add Admin
5. Delete All

Keyking FPC3002Q

Input UserID [MOD]

----123456----

Keyking FPC3002Q

1. Level 1:1
2. Add FP
3. Change Card

Keyking FPC3002Q

1. Add
2. Delete
3. Modify
4. Add Admin
5. Delete All

Keyking FPC3002Q

Delete All User?

[Y=1/N=2]:

Keyking FPC3002Q

Add FingerPrint

Put Your FP

Keyking FPC3002Q

Change Card

Place Your Card

4.2 Network

If running FPC3002Q as Stand-Alone without PC Connectivity planned, this chapter can be skipped. In most cases, when FPC3002Q 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 FPC3002Q 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 FPC3002Q will automatically recognize it when connected. Single laptop can be used to configure multiple FPC3002Q units. See SPHINX manual for more information.

4.2.1 Unit ID

1. From the Main Menu, select 2. Network

Keyking FPC3002Q

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

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

Keyking FPC3002Q

1. Unit ID
2. IP Option
3. IP Address
4. Subnet Mask
5. Gateway
6. Host IP
7. Host Port

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

Keyking FPC3002Q

〈Unit ID〉

0001

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

4.2.2 IP Option

1. From the Main Menu, select 2. Network

Keyking FPC3002Q

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

2. Press 2 to enter Network Configuration

Keyking FPC3002Q

1. Terminal ID
2. IP Option
3. IP Address
4. Subnet Mask
5. Gateway
6. Host IP
7. Host Port

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

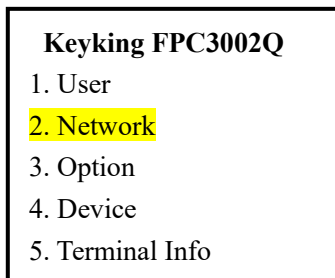
0 = Network parameters configurable.
1 = Network Parameters write-protected
 and can not be changed
2 = force 10.1.1.10 IP Address

Keyking FPC3002Q

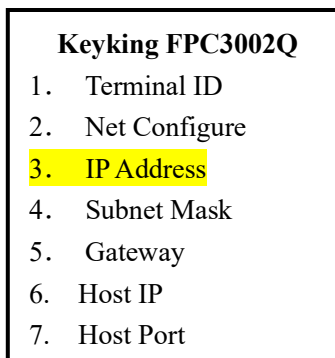
IP Option: **0**
 0=Writable
 1=Protected
 2=Forced IP(10.1.1.10)

4.2.3 IP Address

1. From the Main Menu, select 2. Network



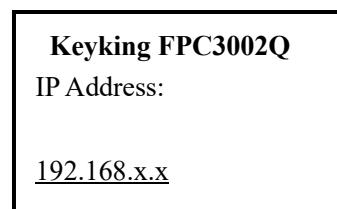
2. Press 3 to enter IP Address



3. Enter IP Address interface. ( button is Delete / Backspace, 

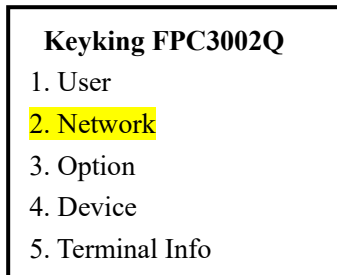
button is .) and ENTER to confirm. Use ESC to go back to previous

“Network Configuration” menu.

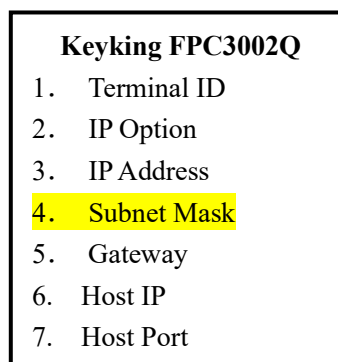




4.2.4 Subnet Mask

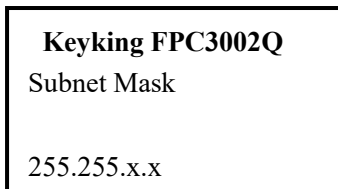
1. From the Main Menu, select 2. Network



2. Press 4 to enter Subnet Mask



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



4.2.5 Gateway

1. From the Main Menu, select 2. Network



Keyking FPC3002Q

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

2. Press 5 to enter Subnet Mask

Keyking FPC3002Q

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 FPC3002Q

Gateway

192.168.X.X

4.2.6 Host IP



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

1. In Main Menu select 2, Network

Keyking FPC3002Q
1. User
2. Network
3. Option
4. Device
5. Terminal Info

3. Select 6 to enter Subnet Mask

Keyking FPC3002Q
1. Terminal ID
2. IP Option
3. IP Address
4. Subnet Mask
5. Gateway
6. Host IP
7. Host Port

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

Keyking FPC3002Q
Host IP:

192.168.X.X

4.2.7 Host Port

1. In Main Menu select 2, Network



Keyking FPC3002Q

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

2. Select 7, Host Port

Keyking FPC3002Q

1. Terminal ID
2. IP Option
3. IP Address
4. Subnet Mask
5. Gateway
6. Host IP
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

Keyking FPC3002Q

Host Port:

8000

4.3 Option

4.3.1 Language

1. In Main Menu, select 3, Option

Keyking FPC3002Q

1. Language
2. Clock
3. Screen Saver
4. Door Relay
5. Tamper Alarm
6. Work Mode

2. Select 1, Language

Keyking FPC3002Q

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

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

Keyking FPC3002Q

1. Language
2. Clock
3. Screen Saver
4. Door Relay
5. Tamper Alarm
6. Work Mode

4.3.2 Clock Setting

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

Keyking FPC3002Q

Language

(0=EN/1=CHN) : 0

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.

Keyking FPC3002Q

1. Language
2. Clock
3. Screen Saver
4. Door Relay
5. Tamper Alarm
6. Work Mode

4.3.3 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.

Keyking FPC3002Q

Clock Setting

20170103130923

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

Keyking FPC3002Q

Screen Saver(Sec): 010

2. Enter the time in Seconds and ENTER to confirm

4.3.4 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.

Keyking FPC3002Q

1. Language
2. Clock
3. Screen Saver
- 4. Door Relay**
5. Tamper Alarm
6. Work Mode

2. Select the parameter to be set

Keyking FPC3002Q

- 1. Relay Time**
- 2. Door Status**
- 3. Open Time Out**

Keyking FPC3002Q

Relay Time

(00-30) : 05

Keyking FPC3002Q

Door Status

[0=NO/1=NC]:0

Keyking FPC3002Q

Open Time Out

(00-30): 20

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
--------------------------------	--	---

4.3.5 Tamper Alarm

FPC3002Q has internal Tamper Switch alerting if the unit is being removed from its mounting bracket. If enabled, removal from the mounting will cause 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 5, Tamper Alarm

Keying FPC3002Q

1. Language
2. Clock Setting
3. Screen Saver
4. Door Relay
5. **Tamper Alarm**
6. Work Mode

2. Select the option and ENTER

Keying FPC3002Q

Tamper Alarm

(N=0/Y=1) :1

4.3.6 Work Mode

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 6, Work Mode

Keying FPC3002Q

1. Language
2. Clock Settings
3. Screen Saver
4. Door Relay
5. Tamper Alarm
6. **Work Mode**

2. Select the option and ENTER

Keying FPC3002Q

Work Mode:1

1. FP Reader
2. FP Attendance

FP Reader: verify and send record to controller, controller open door
 FP Standalone/Terminal: can connect external OSDP reader, open door directly

4.4 Device

4.4.1 FP Level

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

Keyking FPC3002Q

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

2. Select 1, FP-Module

Keyking FPC3002Q

1. **FP-Level**
2. Wiegand Setting
3. Card Number Mode
4. Display Mode
5. Terminal Initial
6. NFC Setting

3. Select the parameter to be changed

Keyking FPC3002Q

1. Level for 1:1
2. Level for 1:N

1. Level for 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 for 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.

Keyking FPC3002Q

1:1

Level (1-9) : 4

Keyking FPC3002Q

1: N

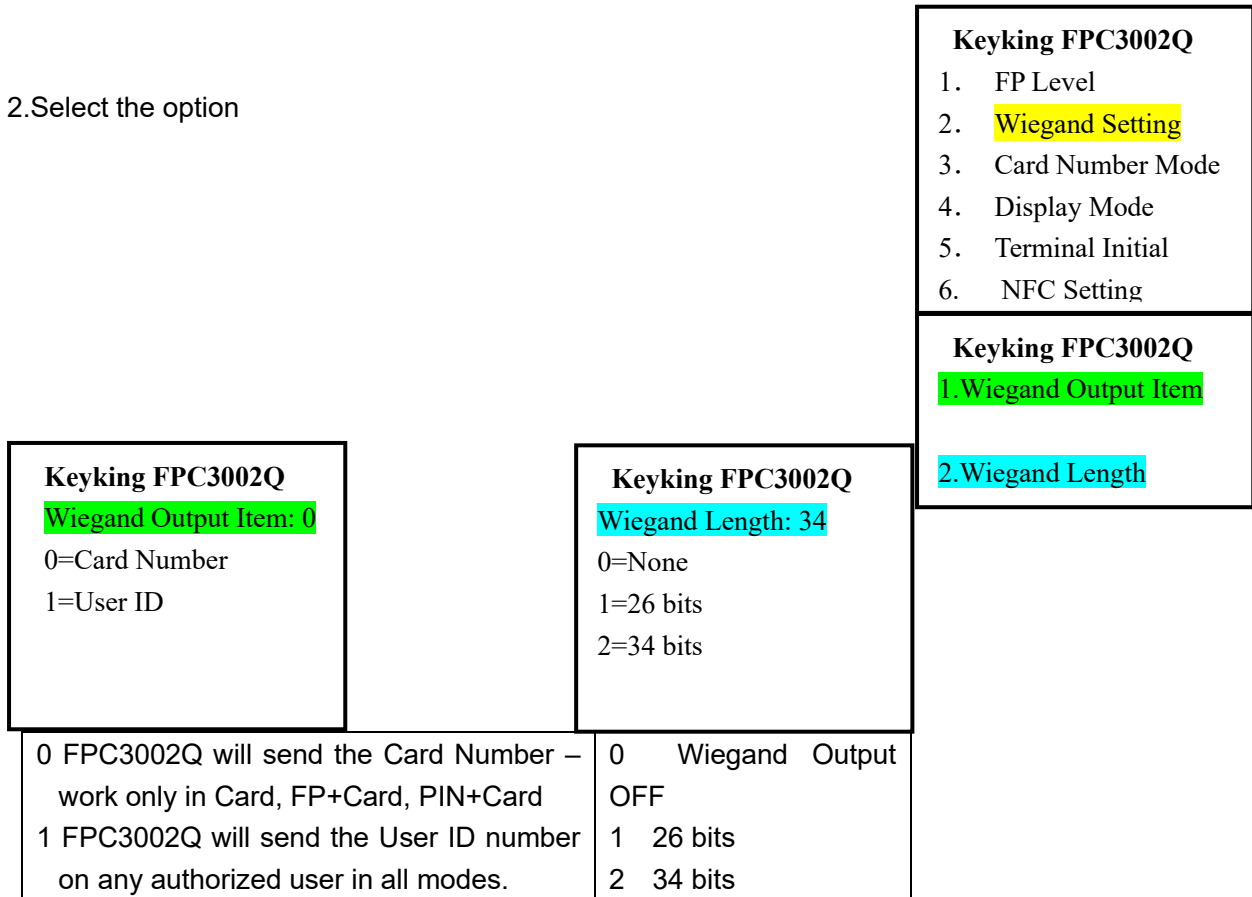
Level (3-9) : 5

4.4.2 Wiegand Setting

Use this setting if connecting the FPC3002Q 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



4.4.3 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 FPC3002Q and it's Weigand Input/Output

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

Keyking FPC3002Q

1. FP-Module
2. Wiegand Setting
3. **Card Number Mode**
4. Display Mode
5. Terminal Initial
6. NFC Setting

2. Select the option and ENTER

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

Keyking FPC3002Q

Card Number Mode:0
 0=Decimal
 1=Hex
 2=Wiegand

4.4.4 Display Mode

1. From Device Menu, select 4, Display Mode

Keyking FPC3002Q

1. FP Level
2. Wiegand Setting
3. Card Number Mode
4. **Display Mode**
5. Terminal Init
6. NFC Setting

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 FPC3002Q

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

4.4.5 Terminal Initial

1. From Device Menu, select 5, Terminal Init

Keyking FPC3002Q

1. FP -evel
2. Wiegand Setting
3. Card Number Mode
4. Display Mode
5. **Terminal Initial**
6. NFC Setting

Keyking FPC3002Q

1. Parameter Initial
2. Delete All Logs
3. Terminal Initial
4. NetPara Initial

2. Select Initialization Type

Keyking FPC3002Q Config Initial	Keyking FPC3002Q Delete All Logs	Keyking FPC3002Q Terminal Initial	Keyking FPC3002Q NetPara Initial
[1=Y/2=N]:	[1=Y/2=N]	[1=Y/2=N]	[1=Y/2=N]


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	Reset net configuration to Default Settings.
---	---	--	--

4.5 Terminal Info

1. From Main Menu, select 5, Terminal Info

Keyking FPC3002Q

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

Press  Down Button to page down to view other information.

Keyking FPC3002Q

Unit ID=0001
 Version=V3.03
 User Capacity=30,000
 FP Capacity=3000
 Log Capacity=100,000
 MAC=00-10-F0-01-60-74
 IP=192.168.X.X
 Gateway=192.168.2.249
 Mask=255.255.0.0
 Host IP=192.168.2.18
 Host Port=8000
 1:1 Level=4
 1:N Level=5
 FP=12
 User=16
 Admin=0
 Logs=1
 Screen Saver=200s
 Wiegand Out Item=CardNo
 Wiegand Length=WG34
 Card Number Mode=Dec
 WordMode=FP Reader
 Ext OSDP Unit ID=1

4.6 Quick Operation on terminal

- 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. Open Time Out --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.

Chapter 5 Operation in Sphinx

5.1 Install driver for BioUSB-SC03

1. If you use FPC3002Q 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 BioUSB-SC03 installation.

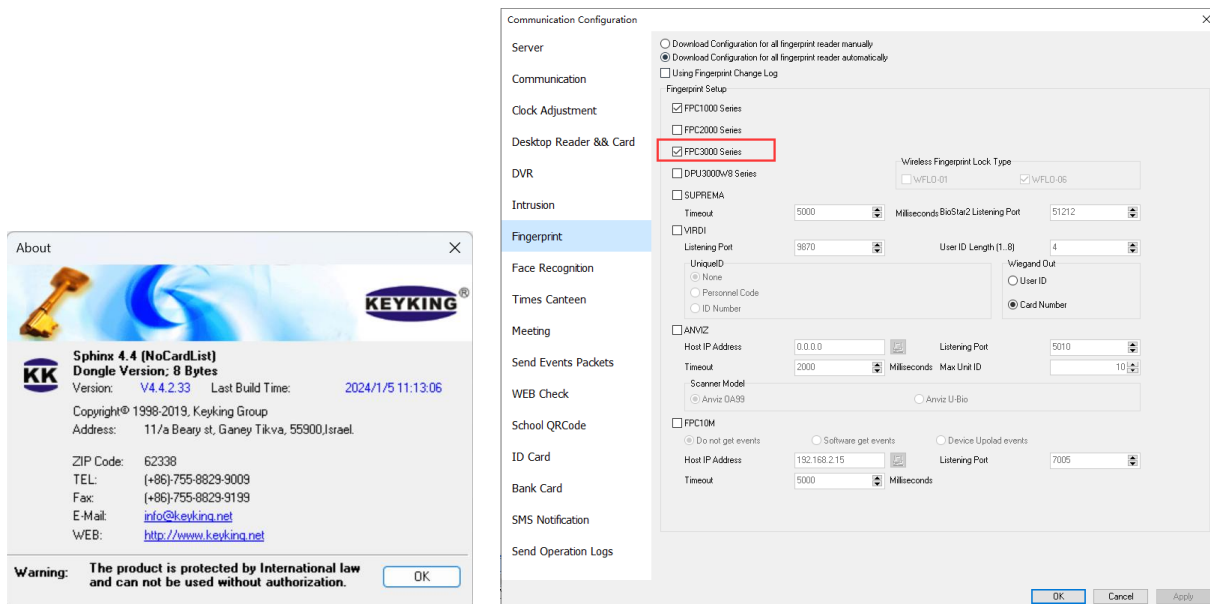


BioUSB-SC03

5.2 Select FPC3002Q Series

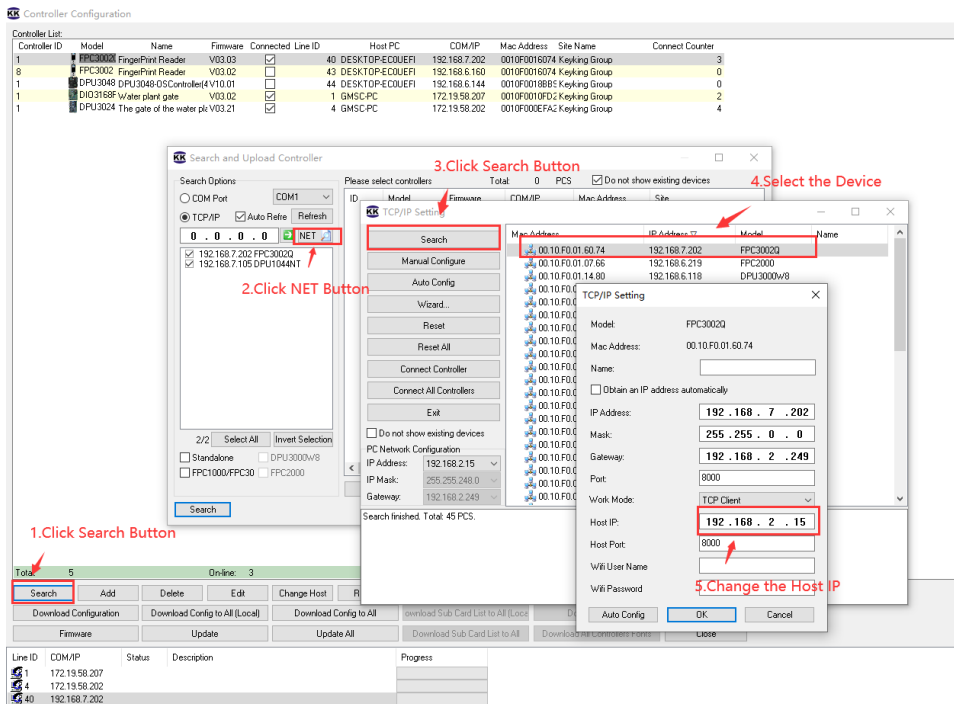
Before you use FPC3002Q, please check the Sphinx version, and make sure the version is after V4.4.2.33.

1. Go to Setup menu and select communication configuration from Sphinx main screen.
2. Select the "Fingerprint", and choose "FPC3000 Series".



5.3 Search & Setup Unit ID

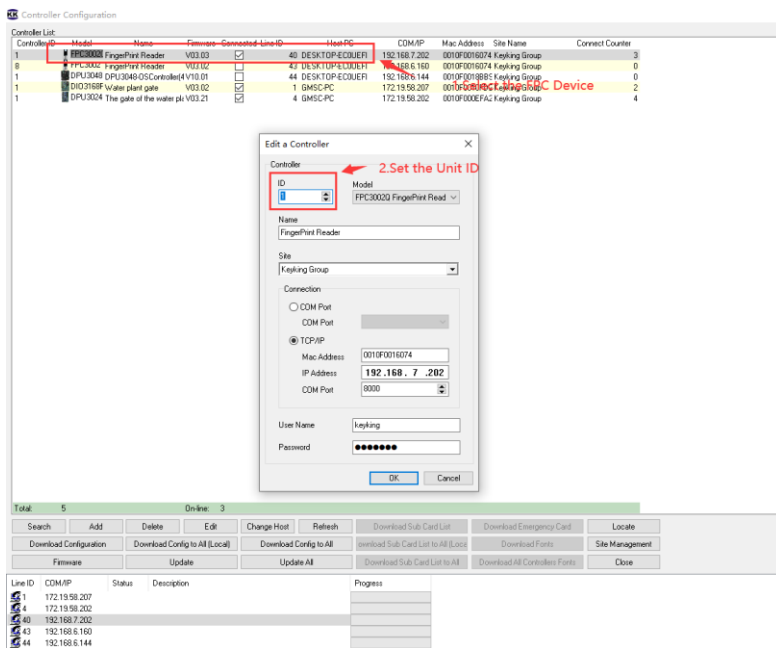
1. Click "Search" in Controller Configuration, and configure FPC3002Q similar as any other Access controller.
2. Click "NET" to search it by TCP/IP.
3. Once you find a lots, just highlight the one you would like to configure. Input the IP, Host IP and so on to configure it.
4. Click ok, to go back TCP/IP setting.
5. Click Exit to go back Search and Upload Controller, choose the FPC3002Q, and click Save to save it into database.
6. Done.



5.3.1 Setup Unit ID (work as an OSDP reader)

Option 1:

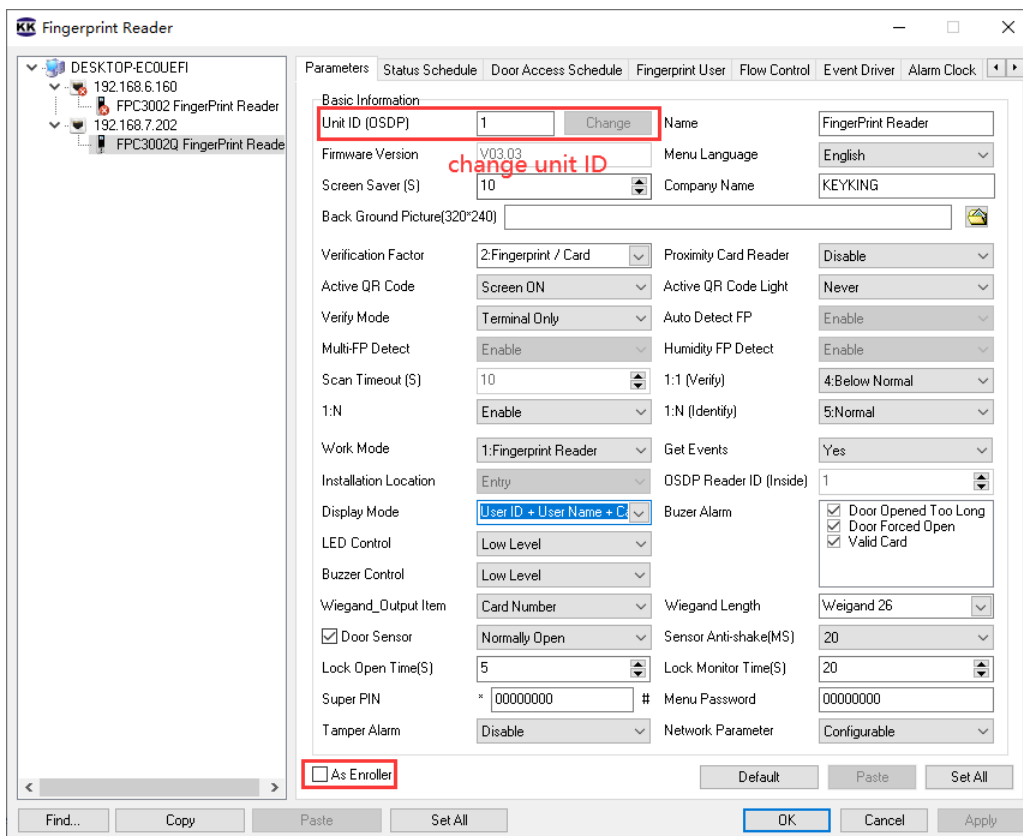
The access control software directly connects to fingerprint device, click Setup/Hardware/Controller Configuration/ and the image below will appear, then set the Unit ID.



Setup Unit ID: The default Unit ID is 1. If you would change it, please input the Unit ID you would like to put, and click “Ok” to make change.

Option 2:

The access control software directly connects to fingerprint device, click Setup/Hardware/Fingerprint Reader/FPC3000 and the image below will appear.



Change Unit ID: Input the Unit ID you would like to put, and click “Change” to make change.

The unit ID should be matched with Reader/door number of Access controller.

For example: Keyking DPU3048-OS (4 doors, 8 readers).

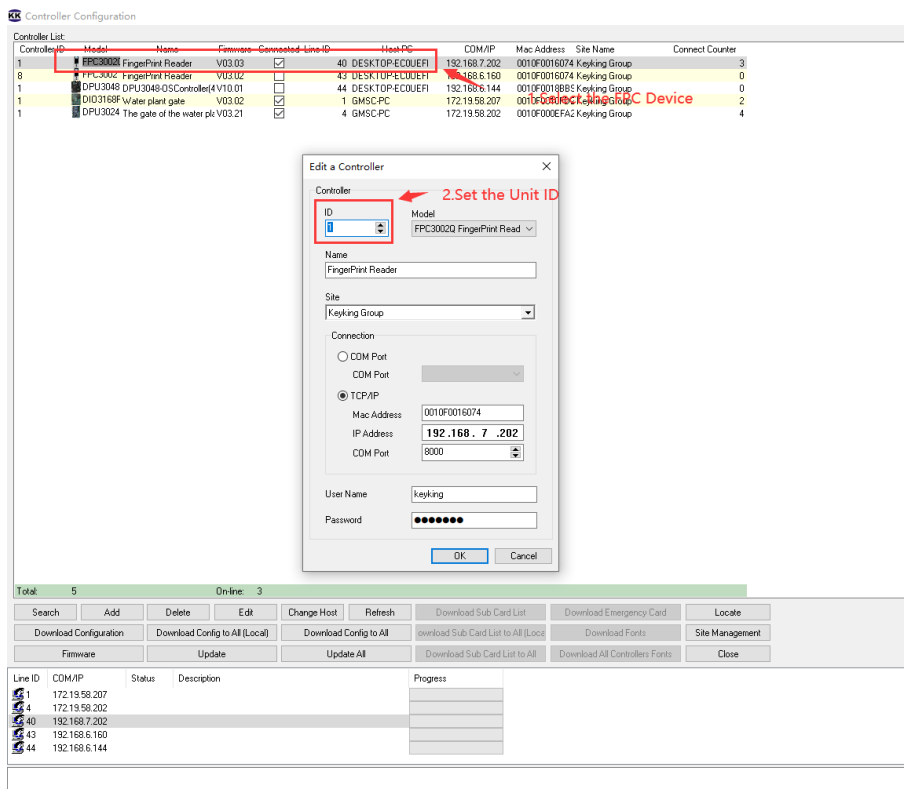
Unit ID (OSDP)	Wiegand Reader		DPU3048-OS Access Controller	
1	Door 1#	In	Door 1#	In
2		Out		Out
3	Door 2#	In	Door 2#	In
4		Out		Out
5	Door 3#	In	Door 3#	In
6		Out		Out
7	Door 4#	In	Door 4#	In
8		Out		Out

5.3.2 Change Unit ID (work as an OSDP reader)

Option 1:

Click Setup/Hardware/Controller Configuration in Sphinx, and the image below will appear.

Setup the Unit ID, and click Ok to confirm.



Option 2:

Click Setup/Hardware/Fingerprint Reader/FPC3000 in Sphinx, and the image below will appear.

Setup the Unit ID, and click Change to confirm.

The screenshot shows the 'Fingerprint Reader' configuration window. The 'Basic Information' tab is active. The 'Unit ID (OSDP)' field is set to '1' and is highlighted with a red box. A red text label 'change unit ID' is placed over the field. The 'Change' button next to the field is also highlighted. The 'As Enroller' checkbox at the bottom left is highlighted with a red box. The software interface includes a tree view on the left, a tabbed menu at the top, and various configuration options in the main area.

Basic Information	
Unit ID (OSDP)	1
Firmware Version	V03.03
Screen Saver (S)	10
Back Ground Picture(320*240)	
Verification Factor	2:Fingerprint / Card
Active QR Code	Screen ON
Verify Mode	Terminal Only
Multi-FP Detect	Enable
Scan Timeout (S)	10
1:N	Enable
Work Mode	1:Fingerprint Reader
Installation Location	Entry
Display Mode	User ID + User Name + C
LED Control	Low Level
Buzzer Control	Low Level
Wiegand Output Item	Card Number
Door Sensor	Normally Open
Lock Open Time(S)	5
Super PIN	* 00000000
Tamper Alarm	Disable
Name	FingerPrint Reader
Menu Language	English
Company Name	KEYKING
Proximity Card Reader	Disable
Active QR Code Light	Never
Auto Detect FP	Enable
Humidity FP Detect	Enable
1:1 (Verify)	4:Below Normal
1:N (Identify)	5:Normal
Get Events	Yes
OSDP Reader ID (Inside)	1
Buzzer Alarm	<input checked="" type="checkbox"/> Door Opened Too Long <input checked="" type="checkbox"/> Door Forced Open <input checked="" type="checkbox"/> Valid Card
Wiegand Length	Weigand 26
Sensor Anti-shake(MS)	20
Lock Monitor Time(S)	20
Menu Password	00000000
Network Parameter	Configurable

☐ As Enroller

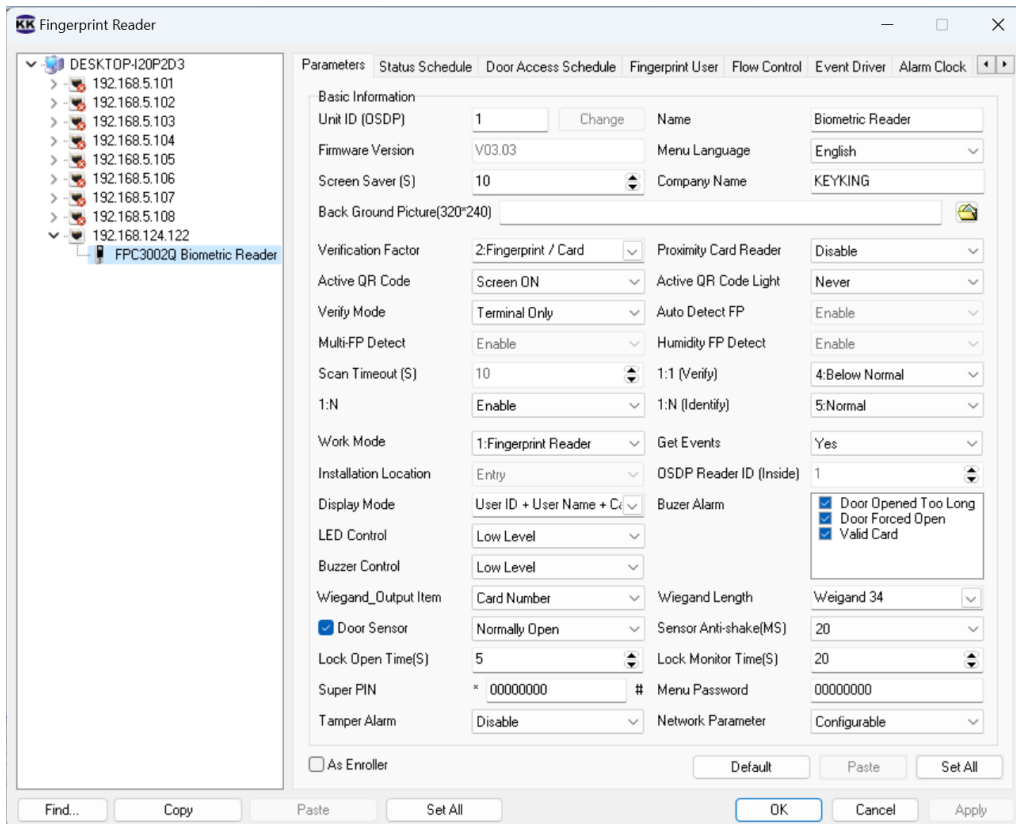
Default Paste Set All

Find... Copy Paste Set All OK Cancel Apply

Change Unit ID: Input the Unit ID you would like to put, and click “Change” to make change.

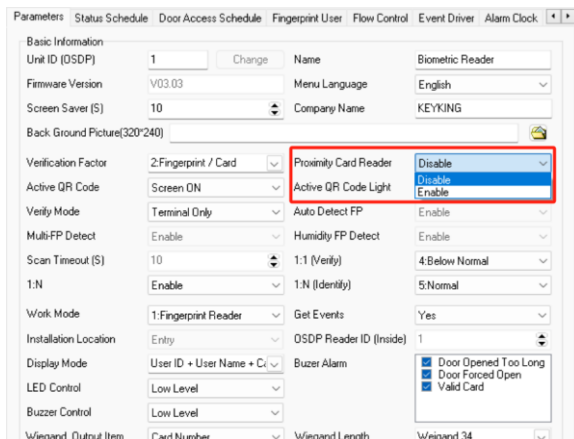
5.4 Configure FPC3002Q

5.4.1 Parameter



Proximity Card Reader:

- “Disable”, will disable proximity card, and will support Mifare card only.
- “Enable”, will support Mifare and Proximity card.



Disable is the default option, because once the proximity reader was enable, it will require more current for FPC3002Q, and FPC3002 will be hotter.

Active QR Code: “Never”, disable; “Screen ON”, when the screen on, active the QR Code function; “Always”, active the QR Code function all the time.

Active QR Code	Screen ON	Active QR Code Light	Never
Verify Mode	Never	Auto Detect FP	Never
Multi-FP Detect	Screen ON	Humidity FP Detect	Object Close to
	Always		Always

Active QR Code Light: “Never”, the light will be always off; “Object Close to”, lights up when an object approaches; “Always”, the light will be always on.

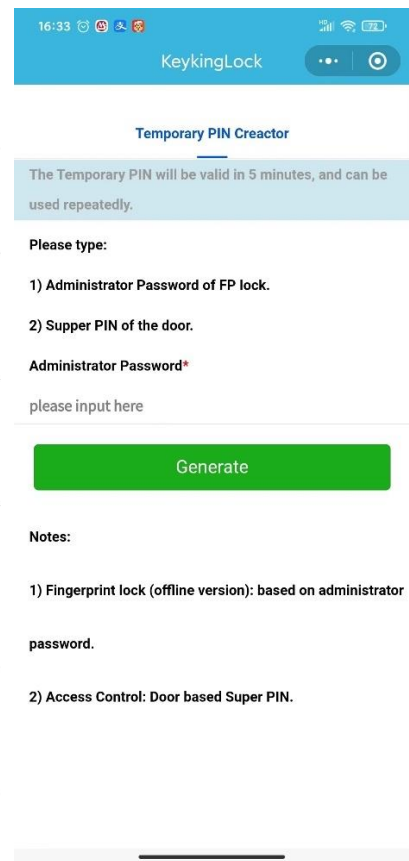
Super PIN: “Super PIN” is the password to open this door, you can put any 8 digitals.

Temporary PIN:

- Temporary PIN will be valid in 5 minutes, and can be used repeatedly.
- Temporary PIN will be created by “Super PIN”.

Steps to make Temporary PIN:

- Run “Wechat” Weixin APP from a smart phone, Android or IOS.
- Search “KeykingLock” *Mini Program* from Wechat.
- Choose “KeykingLock” to run.
- Input the “Super PIN”, you will get “Temporary PIN” for 5 minutes to use.
- The “Temporary PIN” can be used to open the door.



The temporary password is

13898110

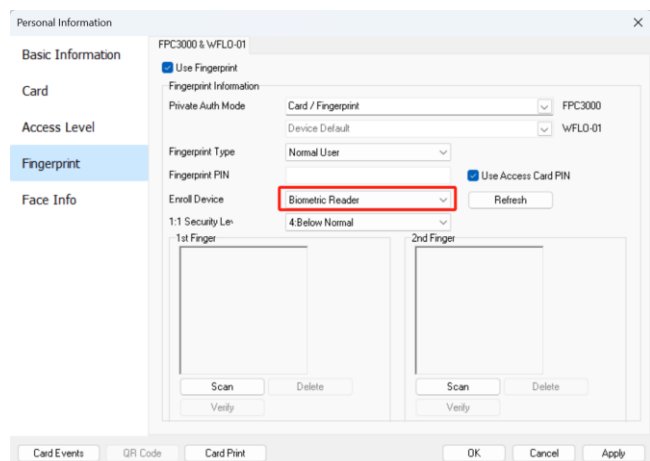
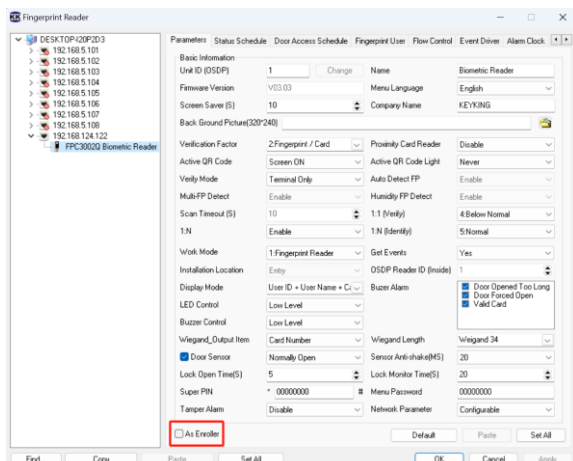
Done

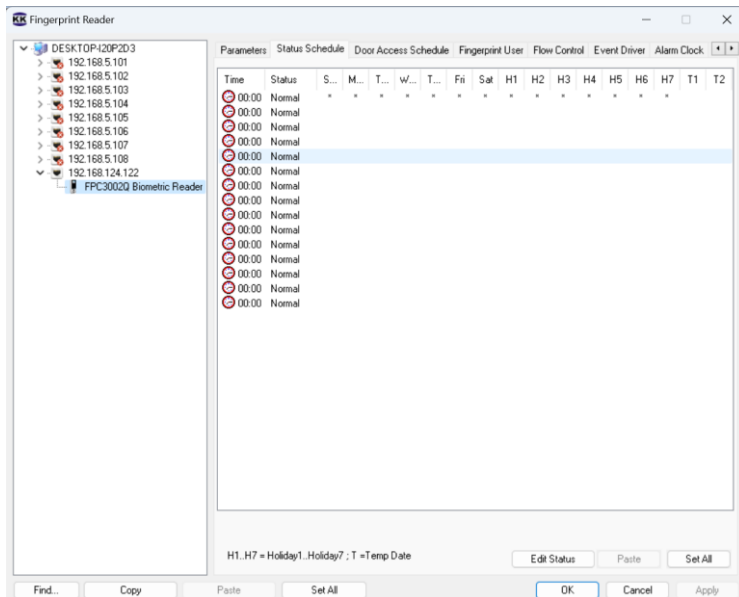
Copy

Menu PIN: “Menu PIN” is the password to manage FPC3002Q, which is as same as “Admin User”. If there is no any “Admin User” or “Menu PIN”, anybody can manage FPC3002Q through Keypads.

- “00000000” is default, invalid also.
- Please setup Menu PIN, and remember it.

As Enroller: Once you choose “As Enrolloer”, this device will be appeared in “Enroller Device” list of Persenal information.





For example, 8:00 am is the time for work, and we can keep the door always open for every employee, and the door will be closed from 8:30.

Door Status Time Set

Status Time

Start Time

8

H

0

M

Entry Status

Always Open

None

In

Out

Valid Date Set

☐ Sunday
☒ Monday
☒ Tuesday
☒ Wednesday
☒ Thursday
☒ Friday
☐ Saturday

☐ H1
☐ H2
☐ H3
☐ H4
☐ H5
☐ H6
☐ H7

☐ T1
☐ T2

Week Days

Weekend

Holidays

OK

Cancel

Door Status Time Set

Status Time

Start Time

8

↓

↑

H

30

↓

↑

M

Entry Status

Normal

▼

None

In

Out

Valid Date Set

☐ Sunday
☒ Monday
☒ Tuesday
☒ Wednesday
☒ Thursday
☒ Friday
☐ Saturday

☐ H1
☐ H2
☐ H3
☐ H4
☐ H5
☐ H6
☐ H7

☐ T1
☐ T2

Week Days

Weekend

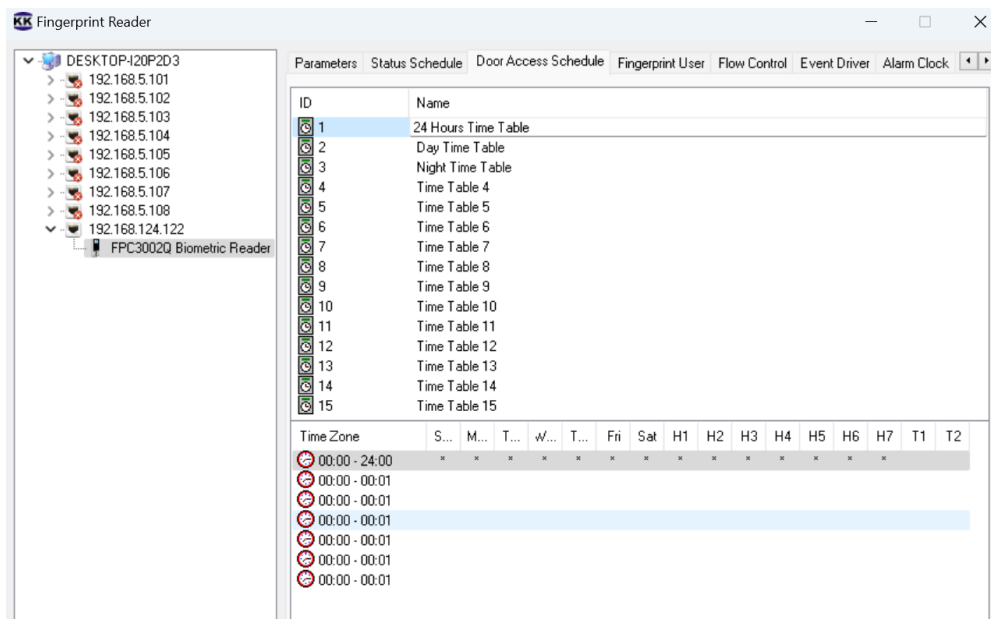
Holidays

OK

Cancel

[illegible]

5.4.3 Door Access Schedule



5.4.4 Fingerprint User

Of course, you can refer to the manual of Sphinx.

5.4.5 Flow Control

You can refer to the manual of Sphinx.

5.4.6 Events Drive

You can refer to the manual of Sphinx.

5.4.7 Alarm Clock

You can refer to the manual of Sphinx.

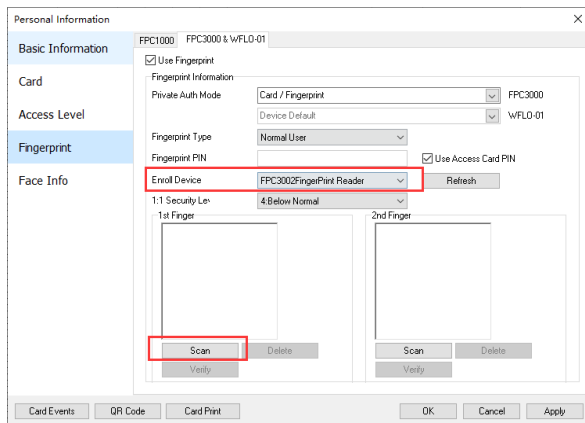
5.4.8 Wiegand Format

5.4.9 Channel Mapping

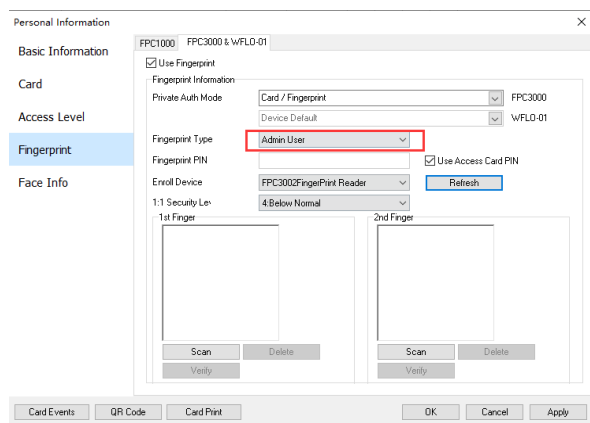
You can refer to the manual of Sphinx.

5.4 Enrolling finger for user

1. Enrolling fingerprint through one of FPC3002Q in "personnel information / Fingerprint".
2. Choose the enroll device: Enroller BioUSB-SC03 or any FPC3000 terminal when it is working as an Enroller.
3. Choose Fingerprint type for this user:
 - (A) **Normal User**: normally most of user should be Normal user.
 - (B) **Admin User**: Admin User can manage the FPC3000 by keypad. If there is no any **Admin User** for the FPC3000, everybody can manage FPC3000 by keypad. Once an "Admin User" was existing, then only **Admin User** can access the menu to manage it.
4. Click Scan to enroll fingerprint for the user.
5. Click Apply or Ok to download Fingerprint to FPC3000.
6. Done.

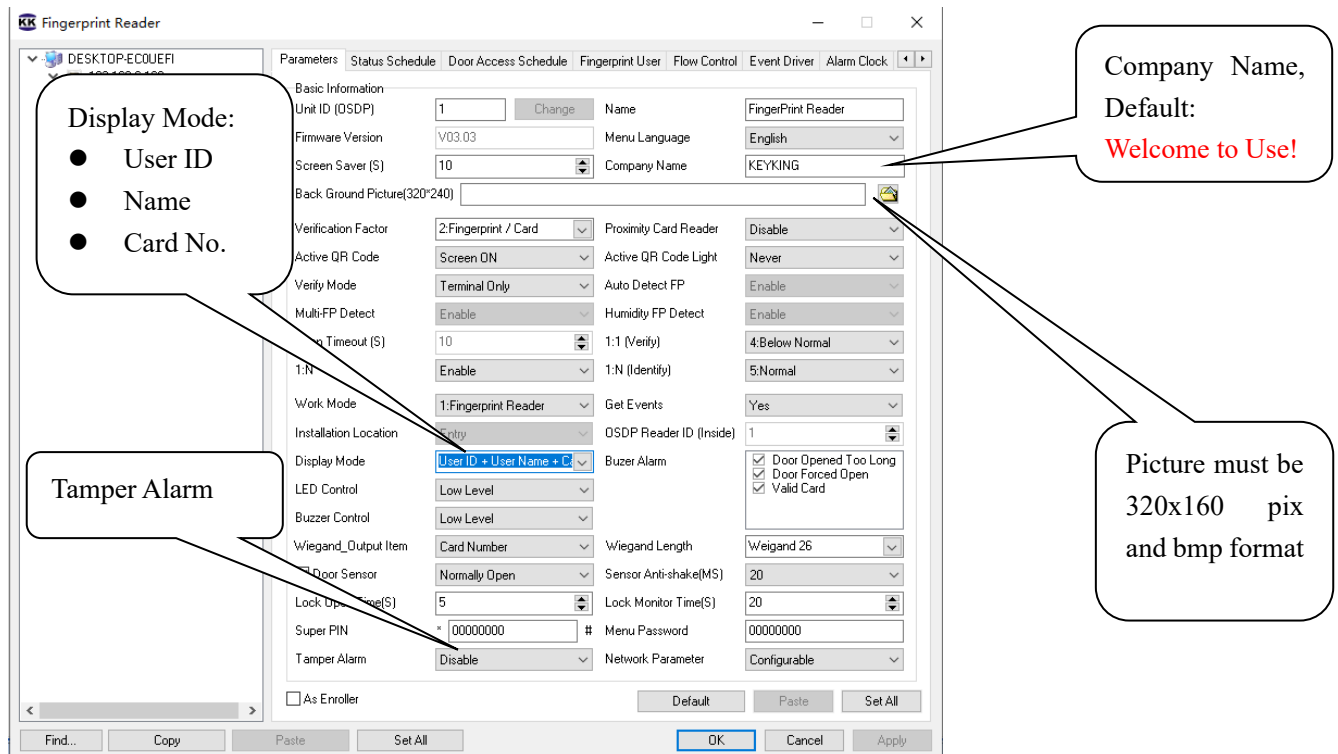


Choose Enroll Device



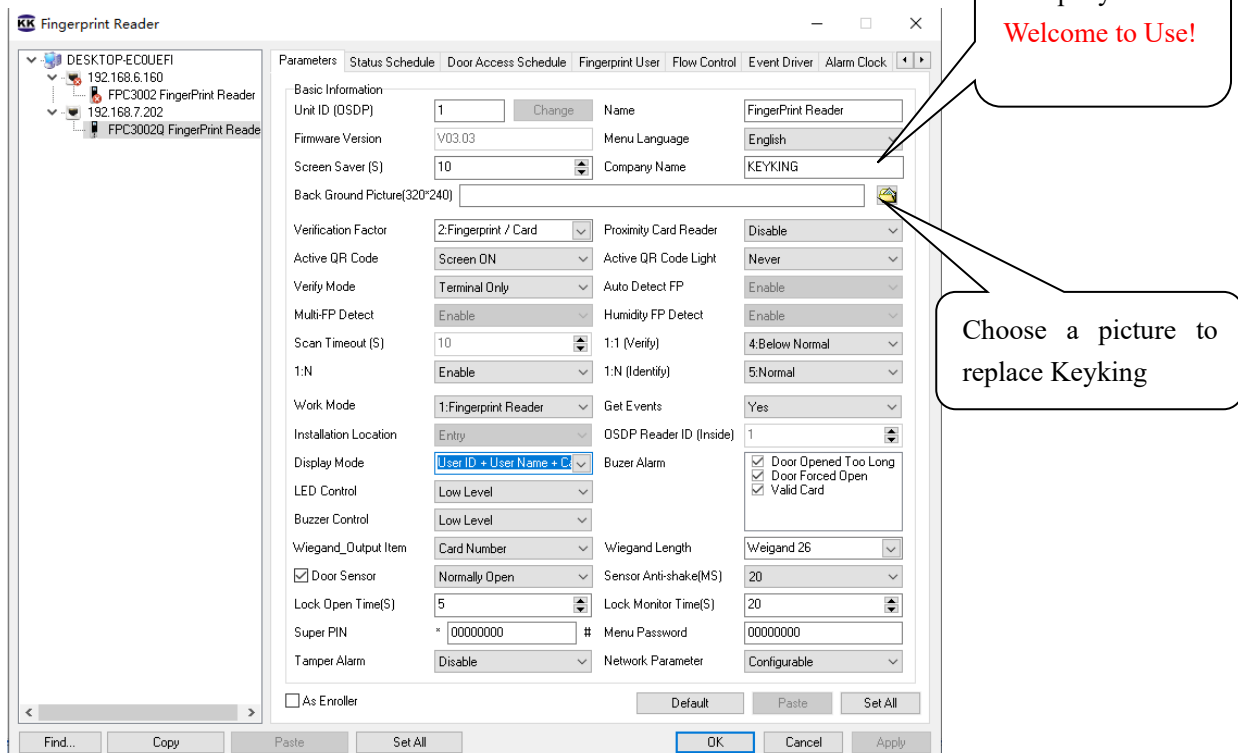
Choose Type

5.5 Classic application



5.5.1 Change Company name

Type the company name you would like to use, like “KEYKING”, then click “Apply”.



5.5.2 Change BackGround picture

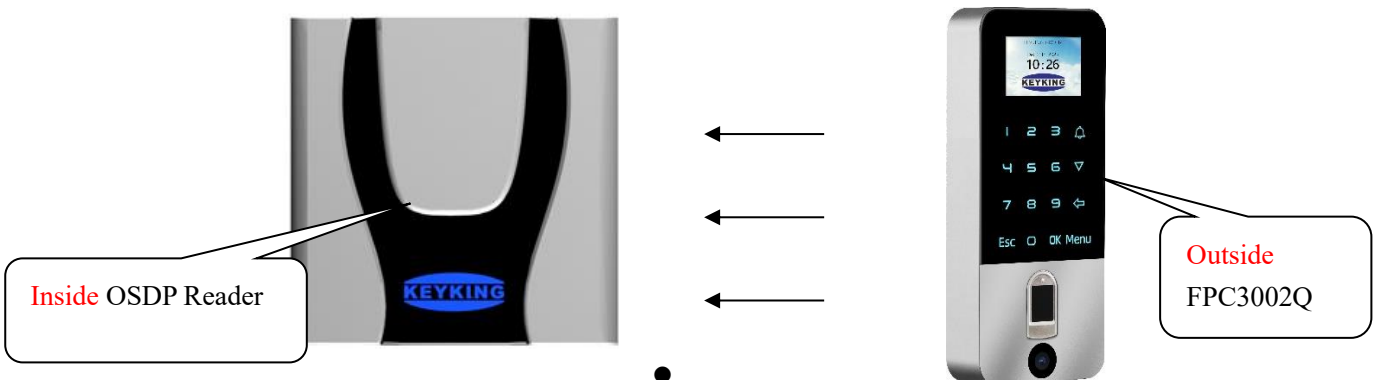
Choose a picture which is 320 * 240 pixels, and click "Apply".

The picture should be Jpg, Bmp format.

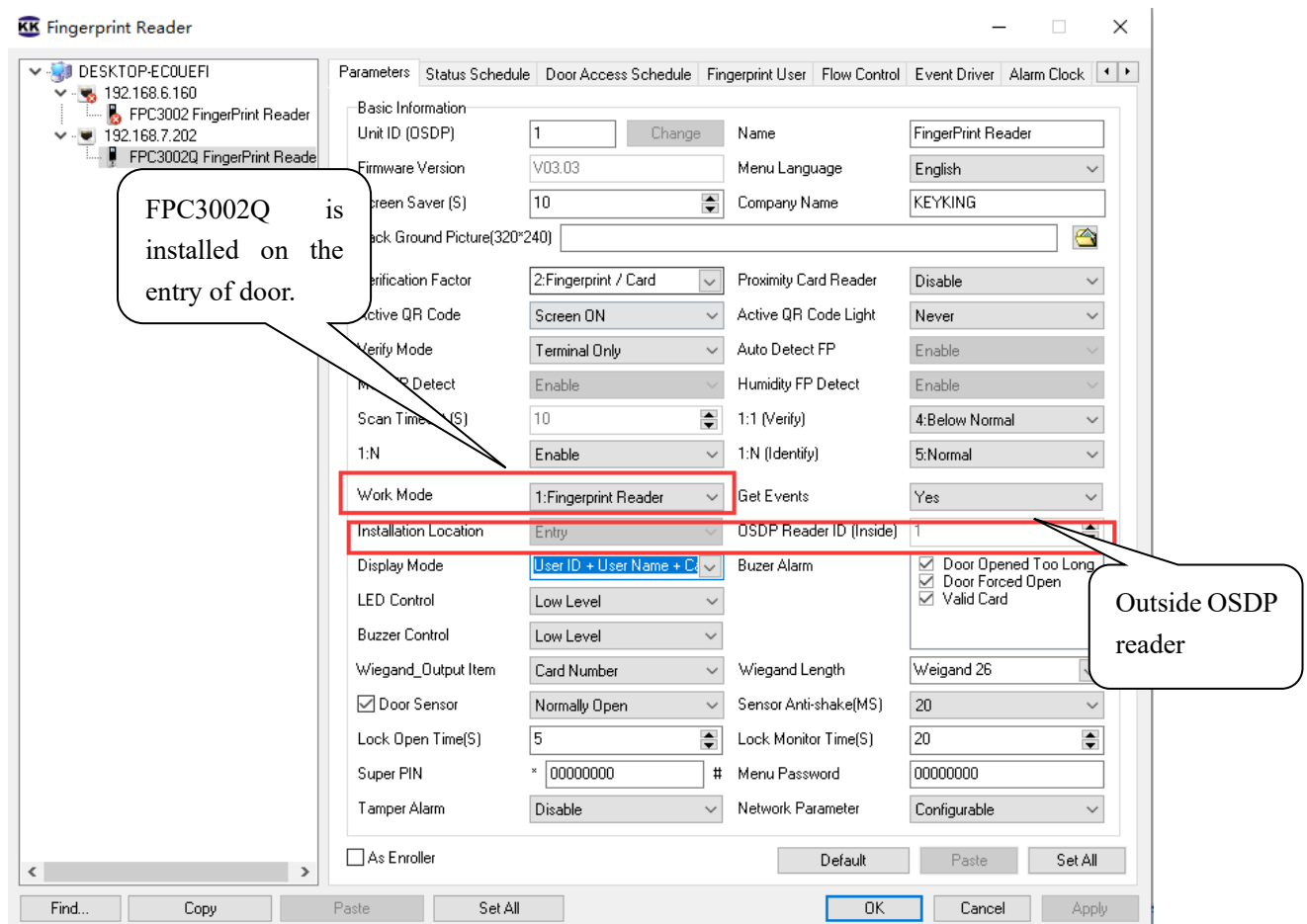
5.5.3 Choose the FPC3002Q location (**Work as terminal**)

FPC3002Q is installed outside of door:

Option 1: Card reader (OSDP Only) is inside of the door, and FPC3002Q is outside.

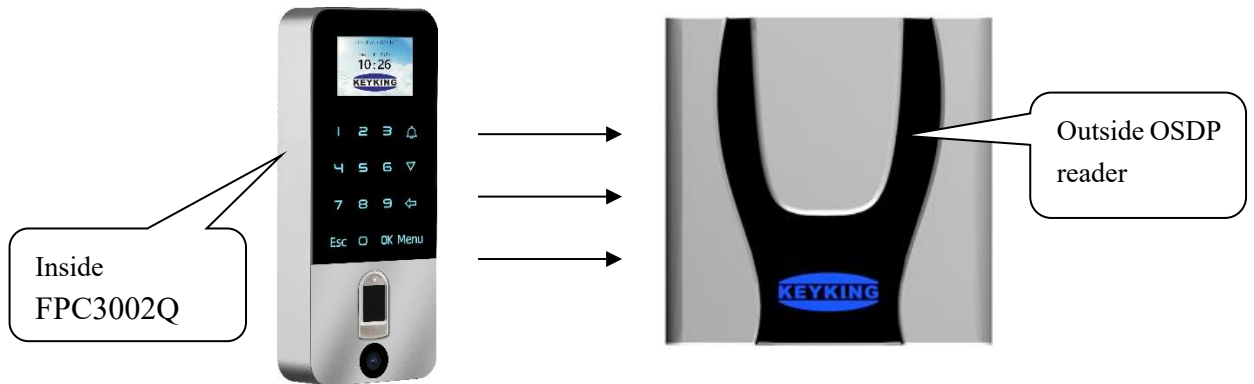


When the FPC3002Q is installed outside the door as below picture, please choose "Entry", and click "Apply".

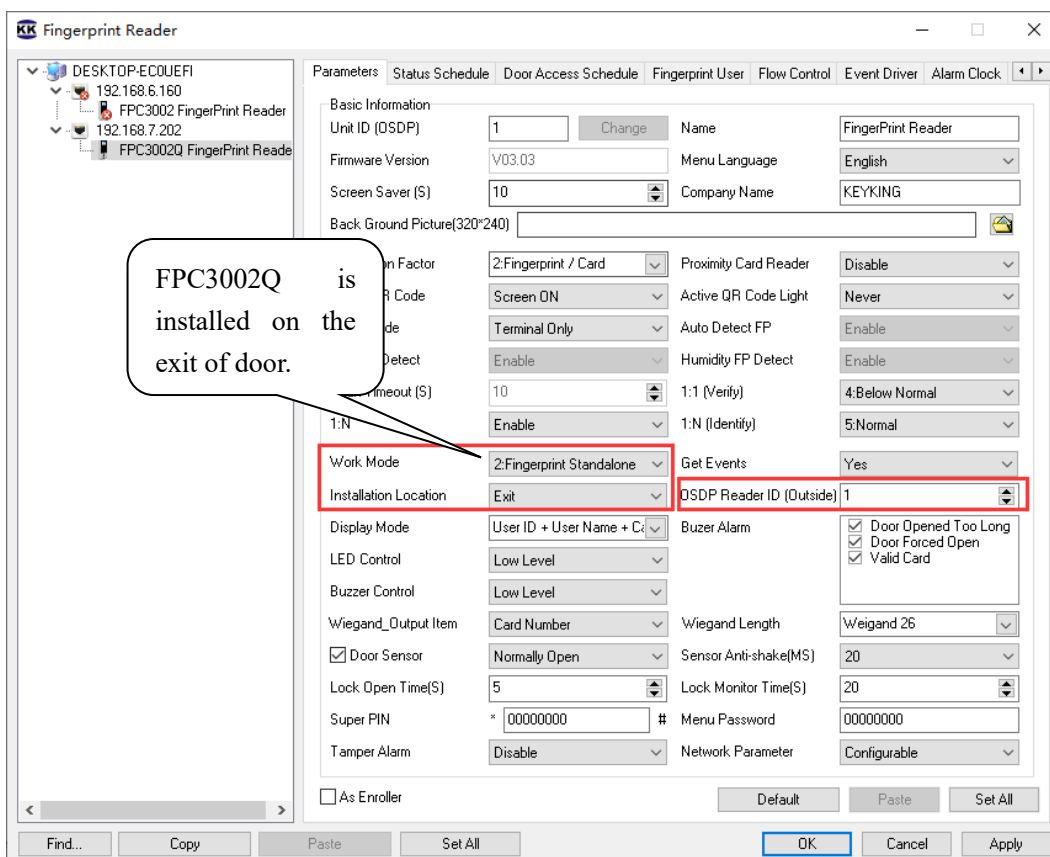


FPC3002Q is installed inside of door:

Option 2: Card reader (OSDP Only) is outside of the door, and FPC3002Q is inside.



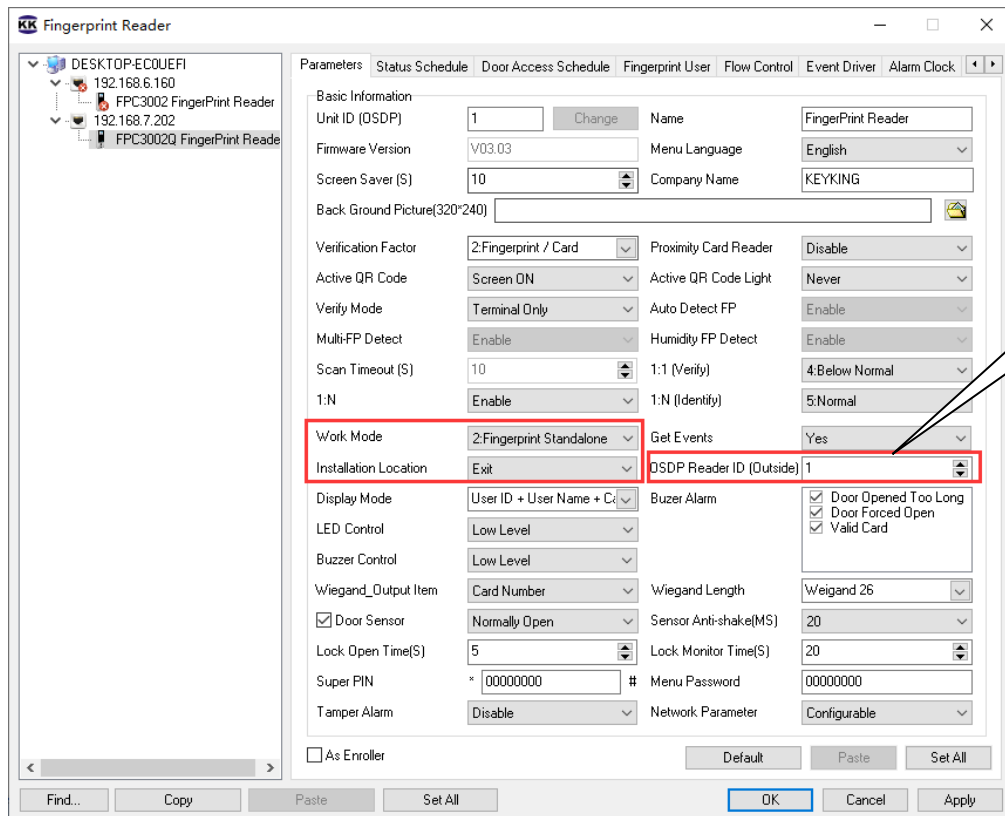
When the FPC3002Q is installed outside the door as below picture, please choose "Entry", and click "Apply".
In case of this, the external OSDP reader become "Outside" automatically.



5.5.4 Choose the Unit ID of external OSDP reader (Work as terminal)

If we will install an external reader work with FPC3002Q standalone, we need know below things:

- FPC3002Q only support OSDP external reader, will not support external Wiegand reader.
- The unit id of OSDP external reader should be in the range 1—126 (From 1 to 126).



- When the FPC3002Q is installed outside the door, we need choose "Entry", then you will see "OSDP Reader (inside)", and please choose the Unit ID of the OSDP reader which is installed on the inside of the door.
- When the FPC3002Q is installed inside the door, we need choose "Exit", then you will see "OSDP Reader (Outside)", and please choose the Unit ID of the OSDP reader which is installed on the outside of the door.

5.5.5 To open the door by Temporary PIN

Super PIN: "Super PIN" is the password to open this door, you can put any 8 digitals.

The screenshot shows the 'Parameters' tab of the KeykingLock software. The 'Super PIN' field is highlighted with a red box and contains the value '00000000'. Other fields include Unit ID (OSDP), Firmware Version, Screen Saver (S), Back Ground Picture(320*240), Verification Factor, Active QR Code, Verify Mode, Multi-FP Detect, Scan Timeout (S), 1:N, Work Mode, Installation Location, Display Mode, LED Control, Buzzer Control, Wiegand_Output Item, Door Sensor, Lock Open Time(S), Tamper Alarm, Name, Menu Language, Company Name, Proximity Card Reader, Active QR Code Light, Auto Detect FP, Humidity FP Detect, 1:1 (Verify), 1:N (Identify), Get Events, OSDP Reader ID (Inside), Buzzer Alarm, Wiegand Length, Sensor Anti-shake(MS), Lock Monitor Time(S), Menu Password, and Network Parameter.

Temporary PIN:

- Temporary PIN will be valid in 5 minutes, and can be used repeatedly.
- Temporary PIN will be created by "Super PIN".

Steps to make Temporary PIN:

- Run "Wechat" Weixin APP from a smart phone, Android or IOS.
- Search "KeykingLock" Mini Program from Wechat.
- Choose "KeykingLock" to run.
- Input the "Super PIN", you will get "Temporary PIN" for 5 minutes to use.
- The "Temporary PIN" can be used to open the door.

The screenshot shows the 'Temporary PIN Creator' screen of the KeykingLock mobile app. The screen displays a message: "The Temporary PIN will be valid in 5 minutes, and can be used repeatedly." and a "Generate" button. Below the message, there is a section for "Please type:" with two options: "1) Administrator Password of FP lock." and "2) Supper PIN of the door." The "Administrator Password*" field is highlighted with a red box and contains the text "please input here".

Notes:

- 1) Fingerprint lock (offline version): based on administrator password.
- 2) Access Control: Door based Super PIN.

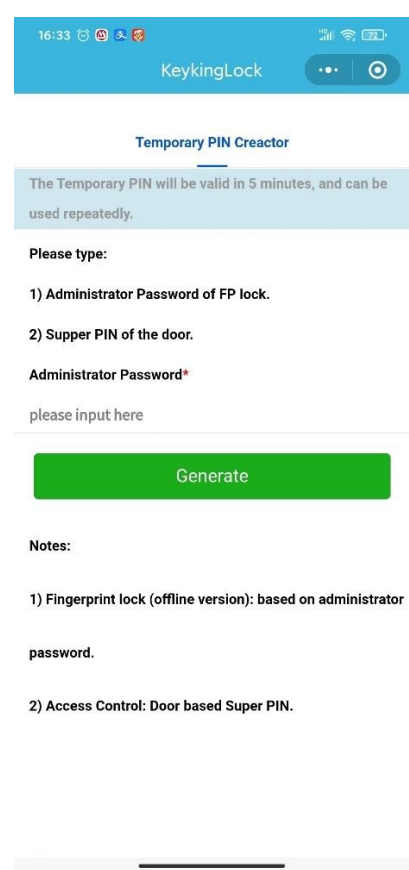


The temporary password is

13898110

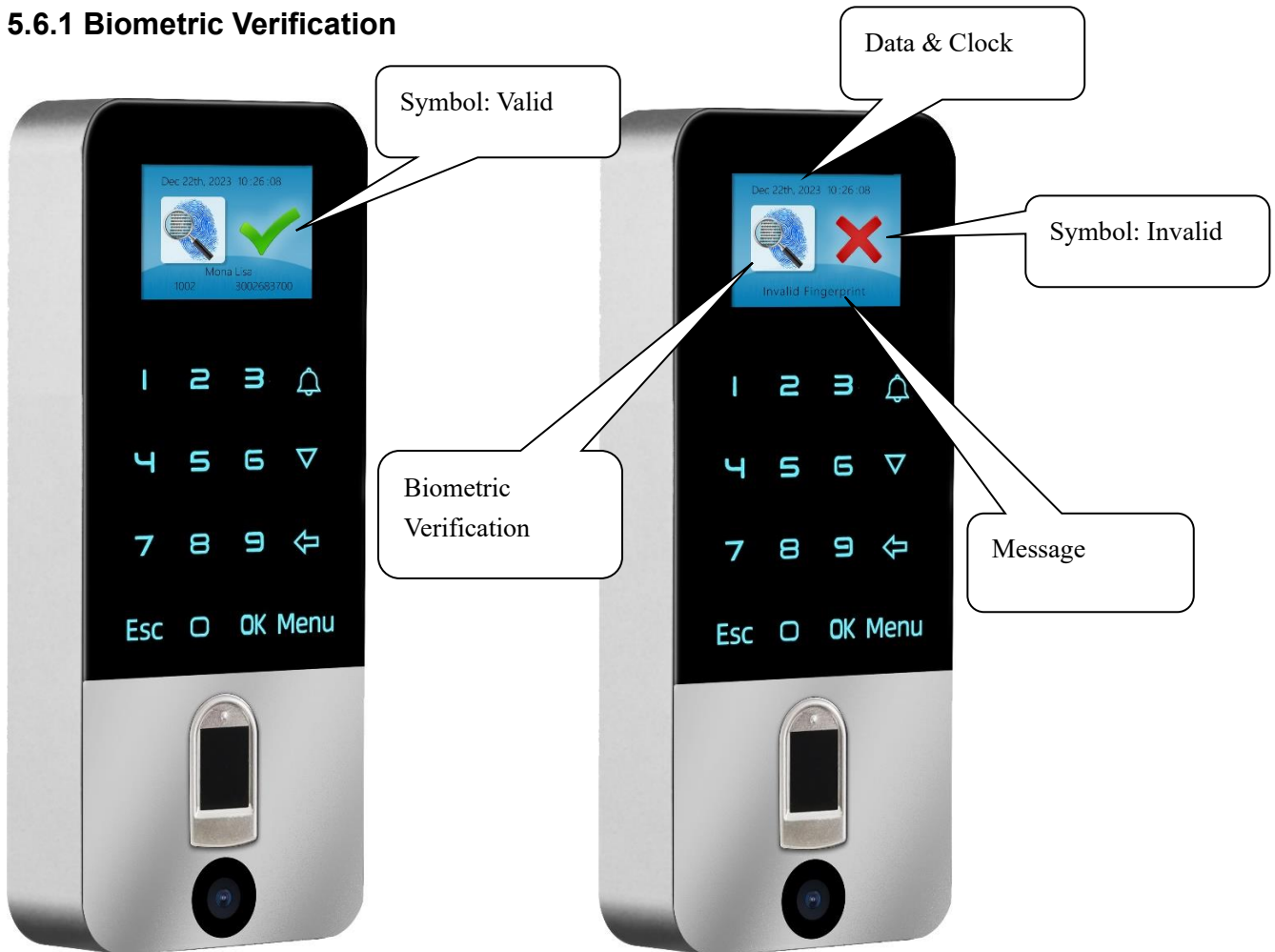
Done

Copy

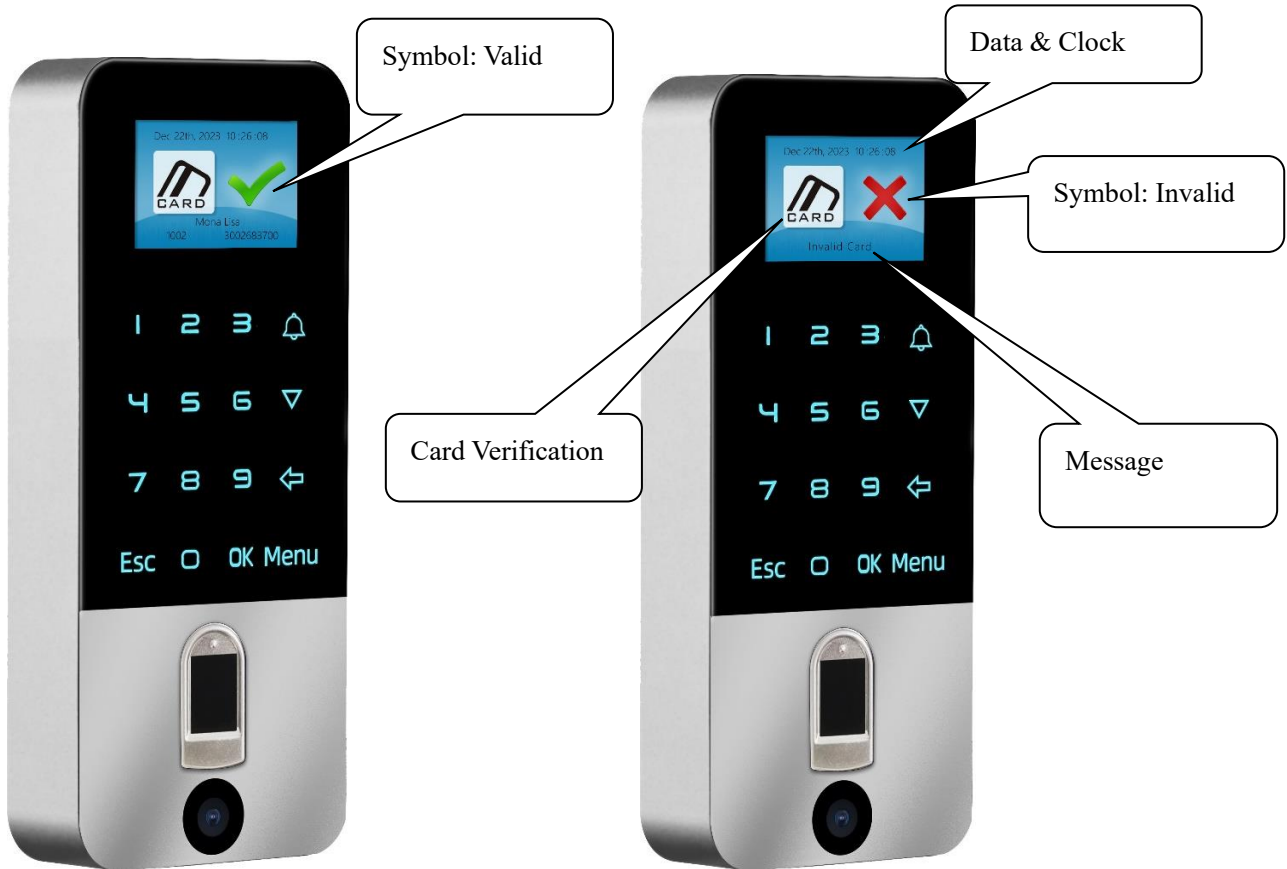


5.6 Screen Message

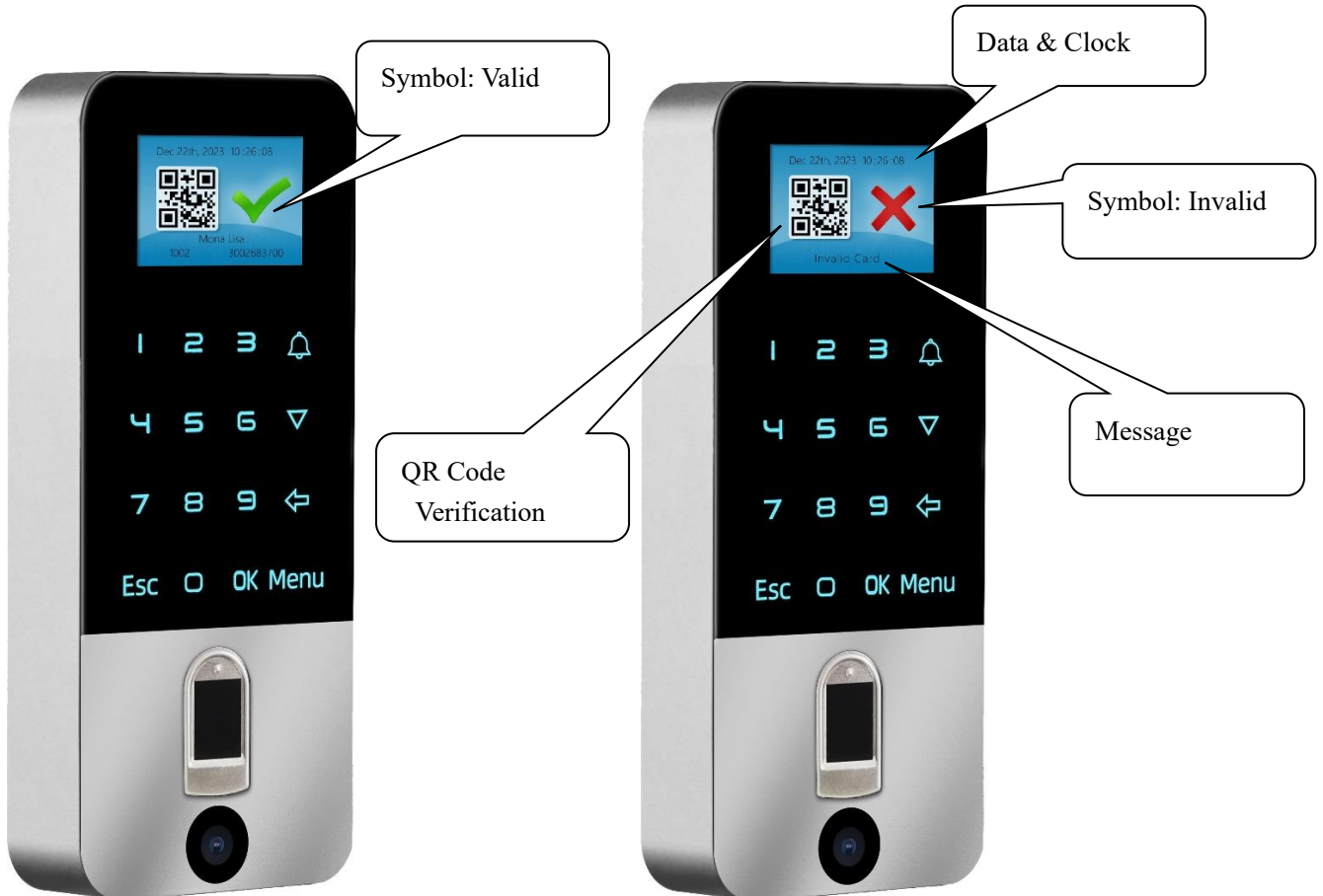
5.6.1 Biometric Verification



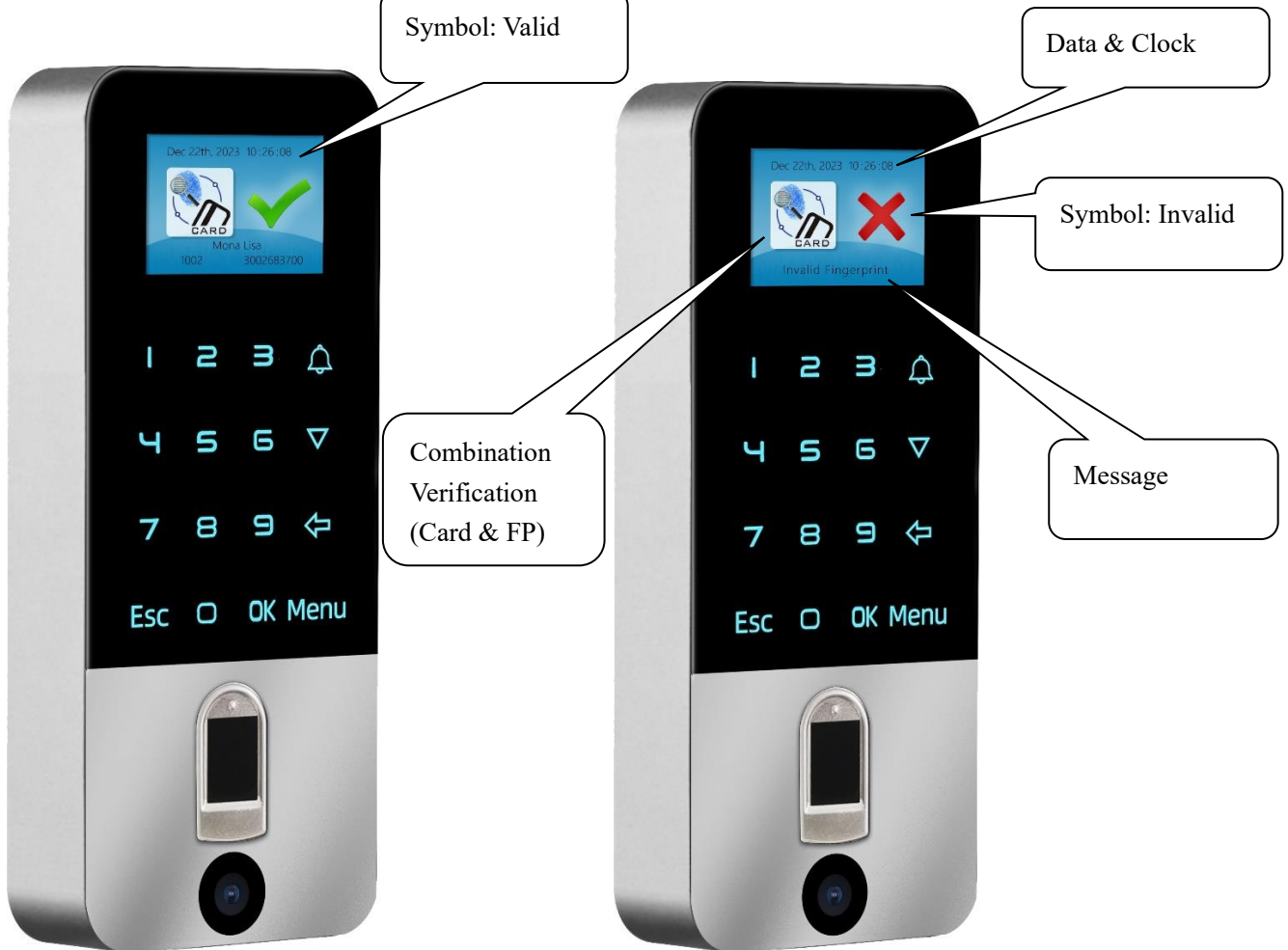
5.6.2 Card Verification



5.6.3 QR Code Verification



5.6.4 Combination Verification



Chapter 6 FAQ

NO	Descriptions	Possible Reason	Solution
1	<ul style="list-style-type: none"> No lights, not responding Lights are ON, card swipe not responsive 	<ul style="list-style-type: none"> Power problem Card technology not compatible 	<ul style="list-style-type: none"> Check power supply replace card
2	<ul style="list-style-type: none"> Lock stays opened 	<ul style="list-style-type: none"> Wrong lock wiring (NC/NO) Lock time too long REX Input configured wrong Exit Button short circuit 	<ul style="list-style-type: none"> Verify wiring Verify lock time Verify REX Configure (NO/NC) Check Exit Button
3	<ul style="list-style-type: none"> FP or card information missing 	<ul style="list-style-type: none"> Missing user information 	<ul style="list-style-type: none"> Verify enrollment Verify network connection
4	<ul style="list-style-type: none"> Can not open door by flashing card or FP. 	<ul style="list-style-type: none"> Lock power problem Enrolment problem Access level not enabled 	<ul style="list-style-type: none"> check lock power and wiring Check enrolment Verify access level
5	<ul style="list-style-type: none"> Can not open the door when it's Card+FP mode 	<ul style="list-style-type: none"> Either card or fingerprint are not enrolled Card and fingerprint not enrolled with same user 	
6	<ul style="list-style-type: none"> Door bell not working 	<ul style="list-style-type: none"> wiring error 	
7	<ul style="list-style-type: none"> Wrong Time/Date 	<ul style="list-style-type: none"> Setting was not complete No PC sync 	<ul style="list-style-type: none"> Set Time/Date in manage menu.
8	<ul style="list-style-type: none"> FPC3002Q does not respond with Fingerprint 	<ol style="list-style-type: none"> The fingerprint is too wet. The fingerprint is too cold. 	<ul style="list-style-type: none"> Wipe dry the fingerprint. Warm the fingerprint to normal.