KJTECH Fingerprint Verification Technology

User Manual

KJ-3400

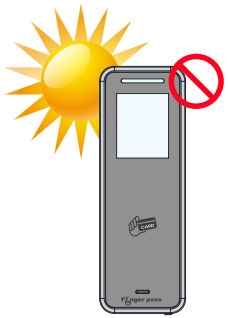
Before using this device, read and follow all instructions for safety

VER. 1.00

CONTENTS

Getting Started

Cautions



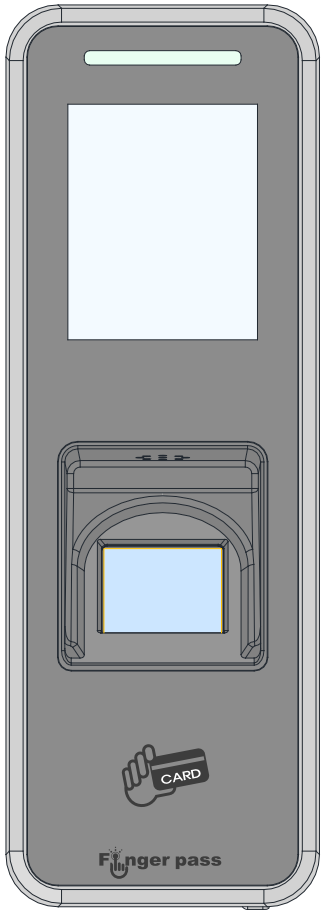
keep out of direct sunlight and heat radiations sources.

Shall not be exposed to dripping or splashing and no objects filled with liquids such as vases, shall be placed on the products.

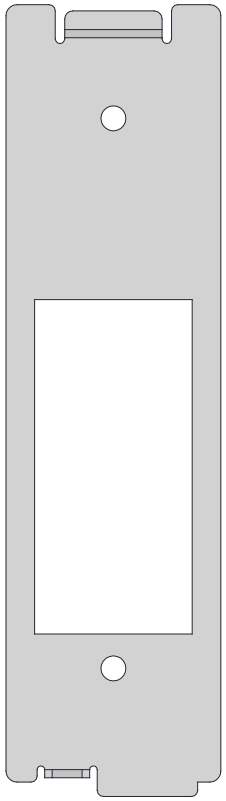
When cleaning, do not use liquid solvent or wet cloth. Wipe with soft cloth.

Never disassemble or modify this device in any way. (KJTECH Co., Ltd is not liable for porblems caused by unauthorized modification or attempted repair)

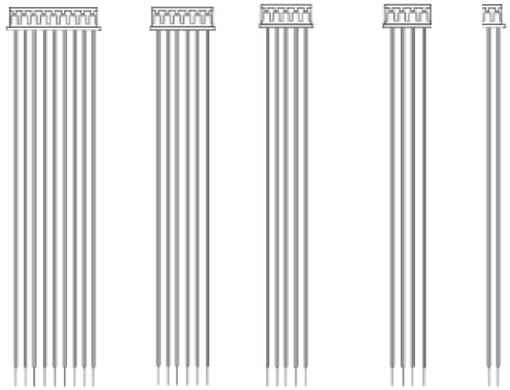
What Include



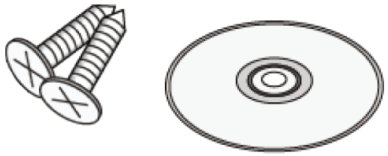
KJ-3400



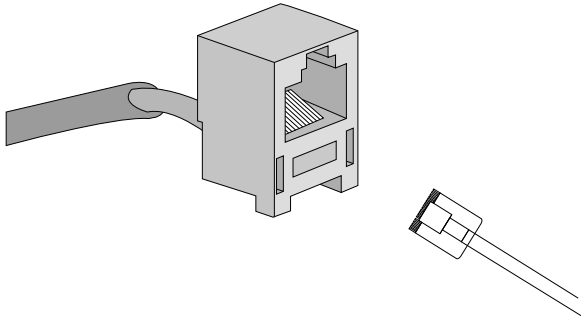
Bracket



Cables

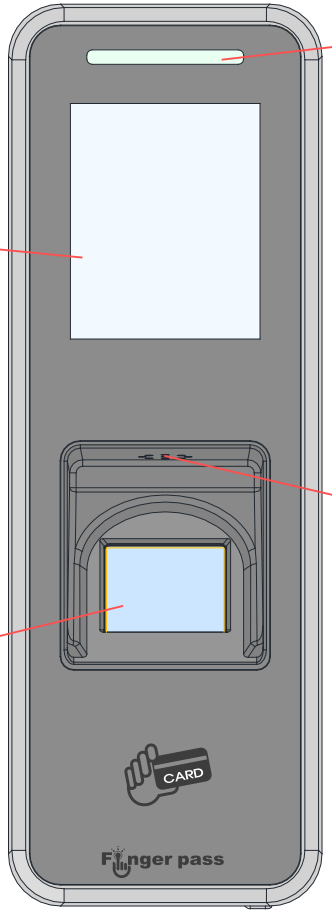


Screw/ Program CD



TCP/IP connector

Parts And Their Functions

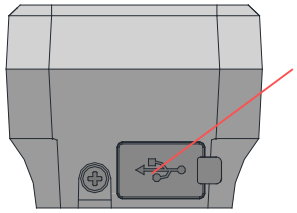


LED
LIghts on for system status

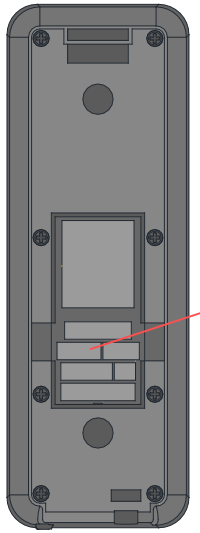
Color TFT LCD
Displays Time, device status, user list and UI for operation.

Speaker
Outputs sounds effect & voice message

Fingerprint Sensor
Registers and Identifys the users

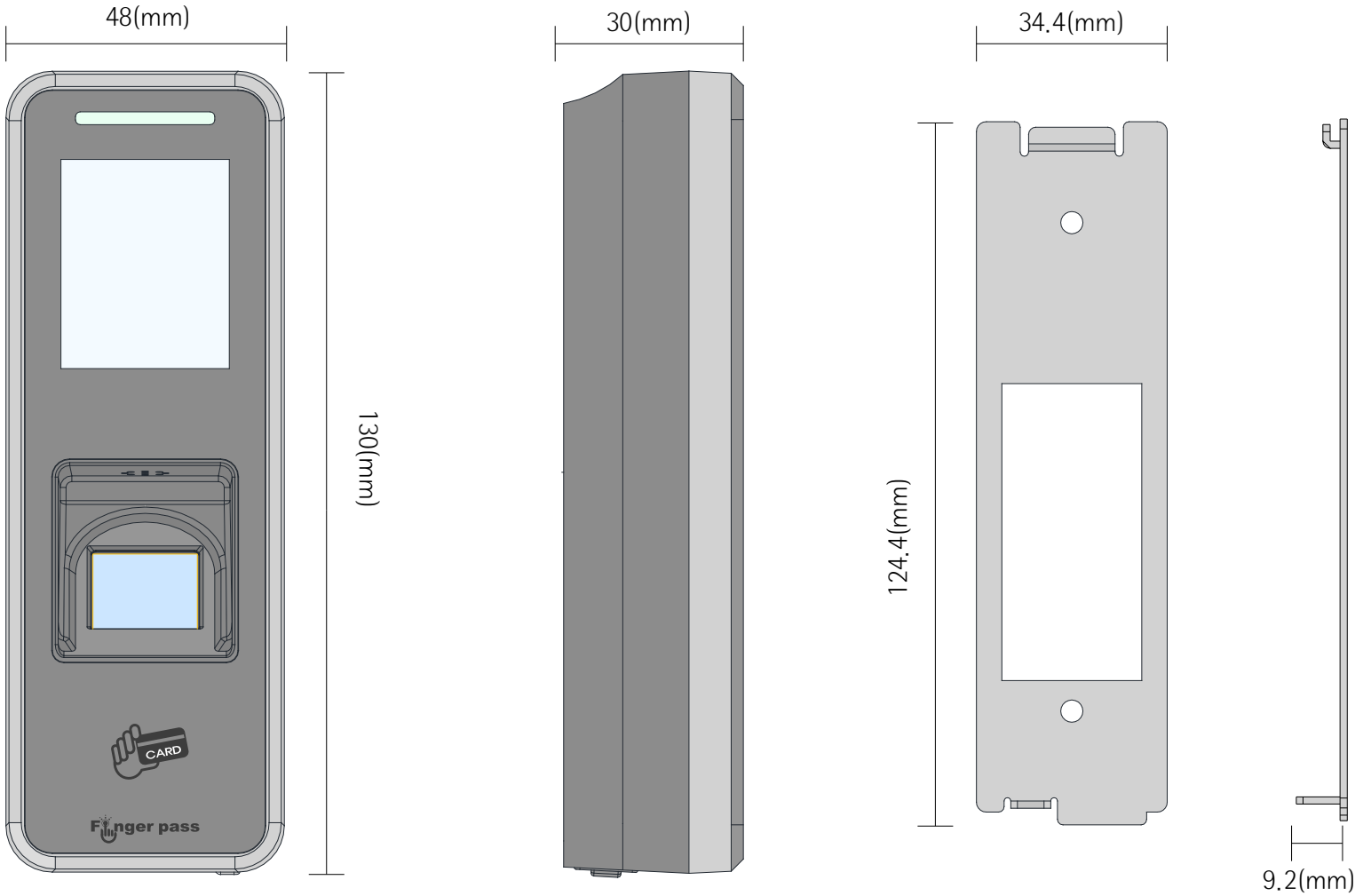


USB
For USB memory



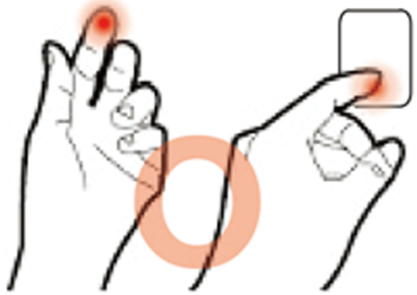
Connector
For Cable Connection

Dimensions



Tips for Registration

Proper way



Improper way

Tips for Finger print registration

To enhance identification, be careful to register fingerprint properly.

Avoid damaged fingerprint and register two fingerprints per user in case.

Verification Mode

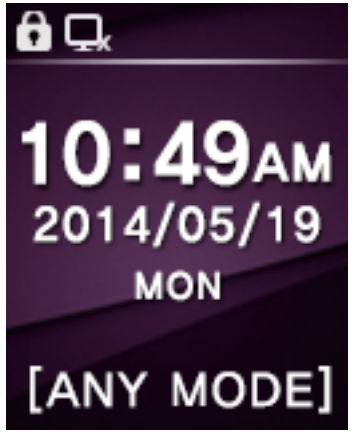
Programable 7 verification modes / Available Settings ==> Advanced ==> Verification mode

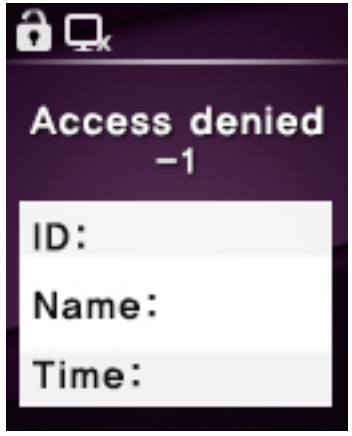
CARD

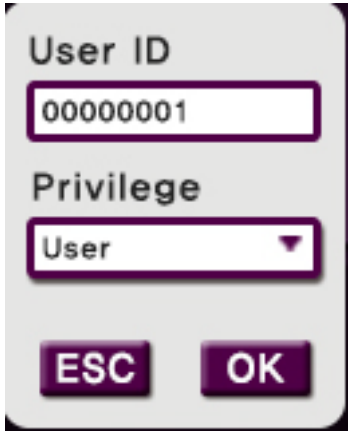
Fingerprint

Displays

These are primary screens

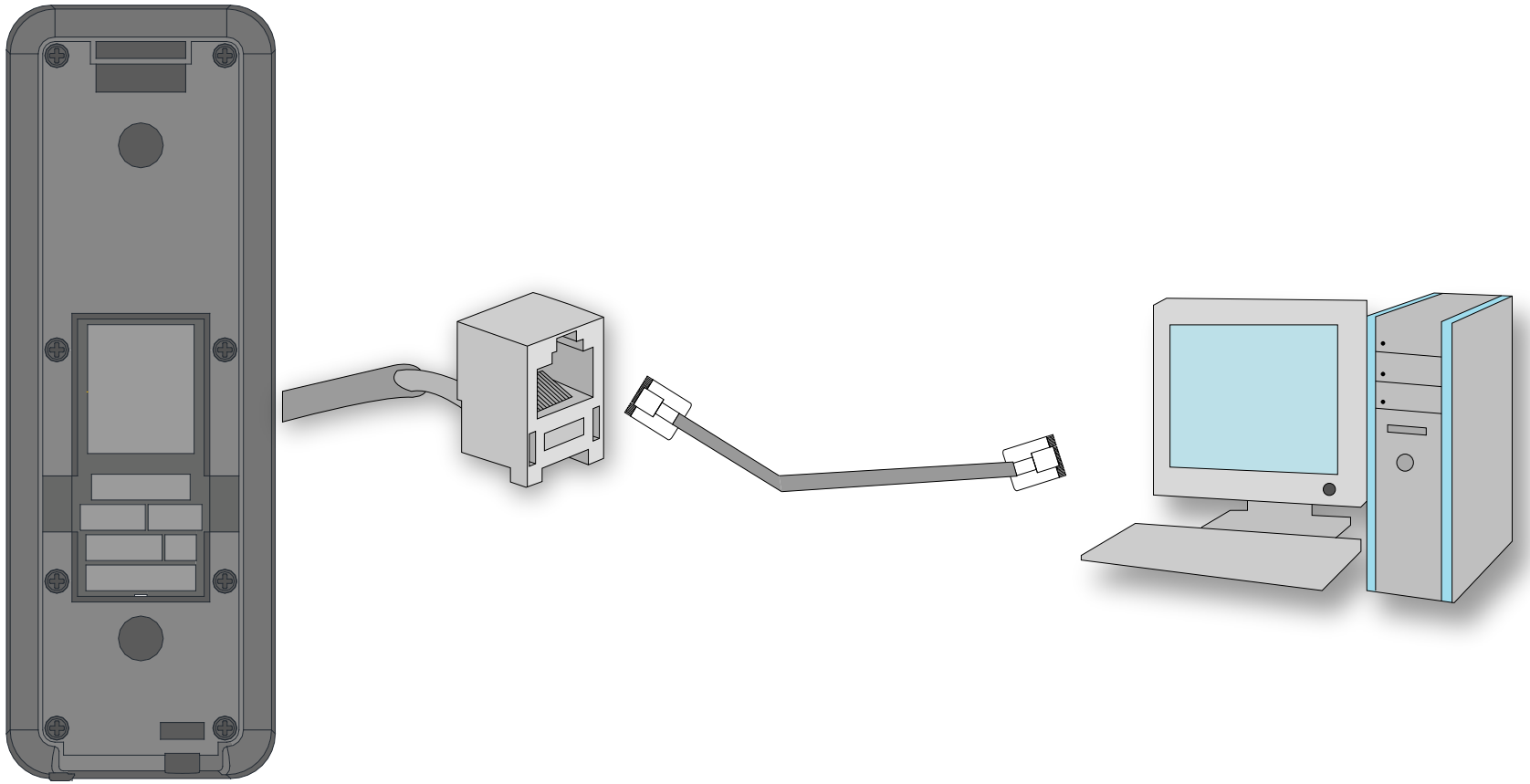




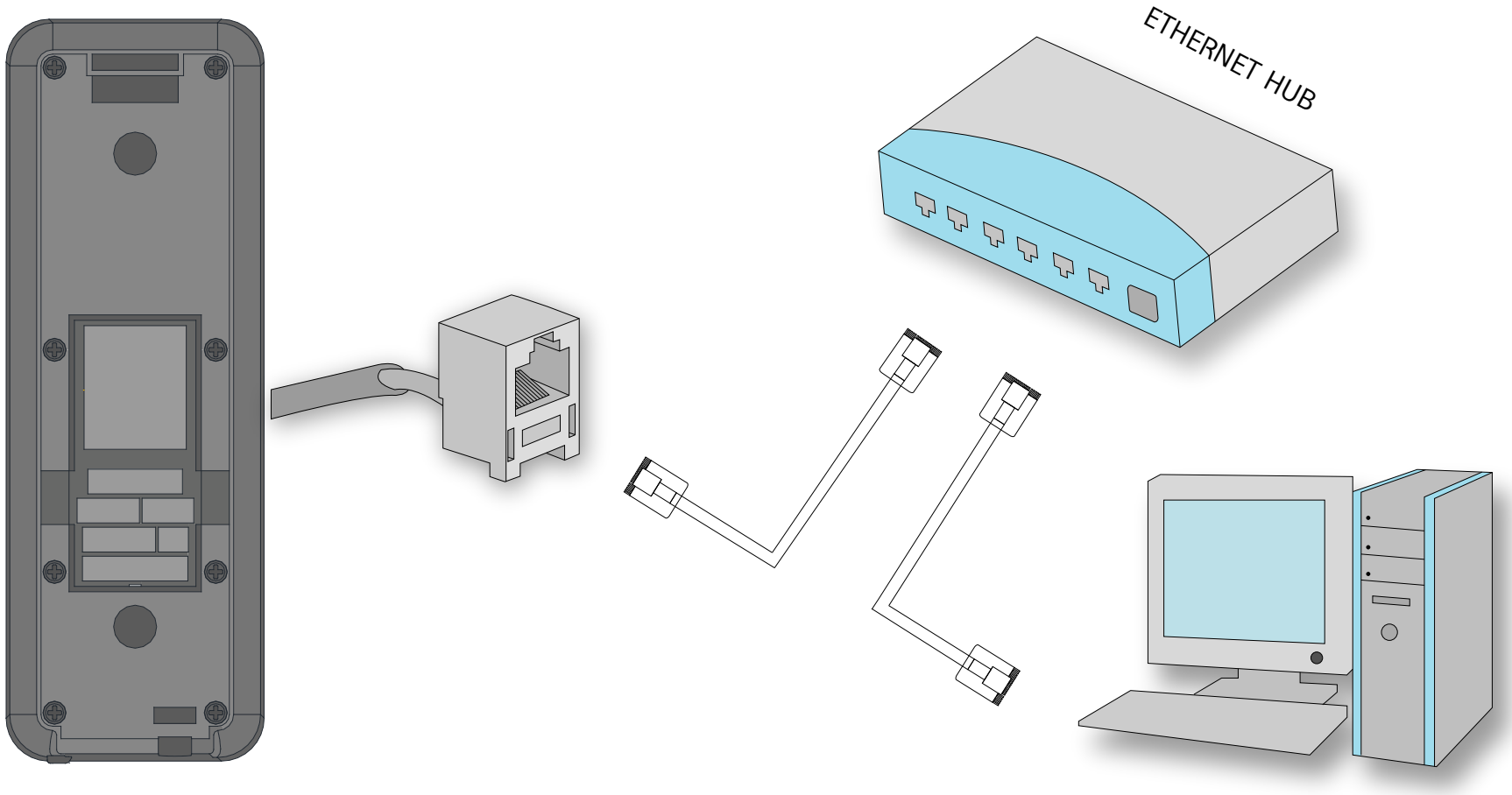


Ethernet Connection (Directly with PC)

KJ-3400 supports MDI/MDIX and can connect with PC using straight CAT-5 cable not cross cable

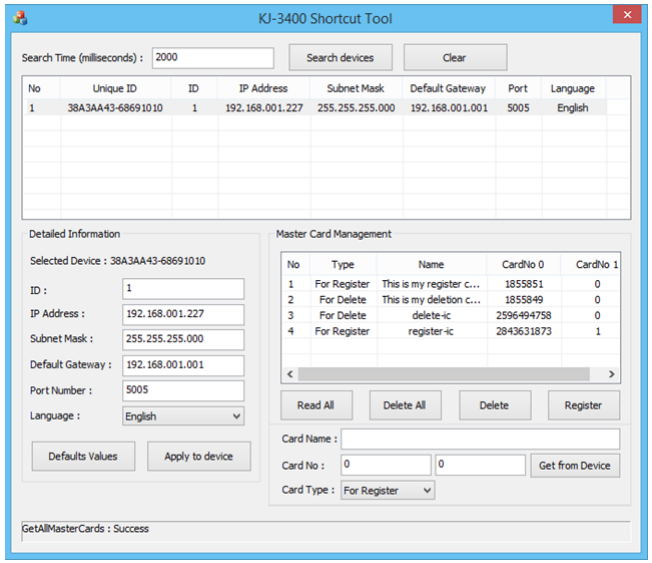


Ethernet Connection (Using HUB)



Using the card type

Using the card type



1. KJ-3400 Shortcut Tool.exe is setup program for card only type without fingerprint.

2. Connect & Setup

1) Run KJ-3400 Shortcut Tool.exe and connect the device by TCP/IP

2) Search Devices : Search the devices connected

Clear : Delete the devices searched

3) Click the device from the list to set up and the data will be linked to the "Detailed Information"

3. Detailed Information

1) Defaults Value: Back to default data

2) Apply to device: Set up data will be applied to the device

4. Master Cad Management

1) Read All : Read the already registered master cards

2) Delete All : Delete all the registered master cards

Using the card type

No	Type	Name	CardNo 0	CardNo 1
1	For Register	This is my register c...	1855851	0
2	For Delete	This is my deletion c...	1855849	0
3	For Delete	delete-ic	2596494758	0
4	For Register	register-ic	2843631873	1

5. Create the master cards

1) Get from Device : Click “Get from Device” button

2) Devices gets stand by to read the card and LED blinks

3) Presents the card and Card no will be read

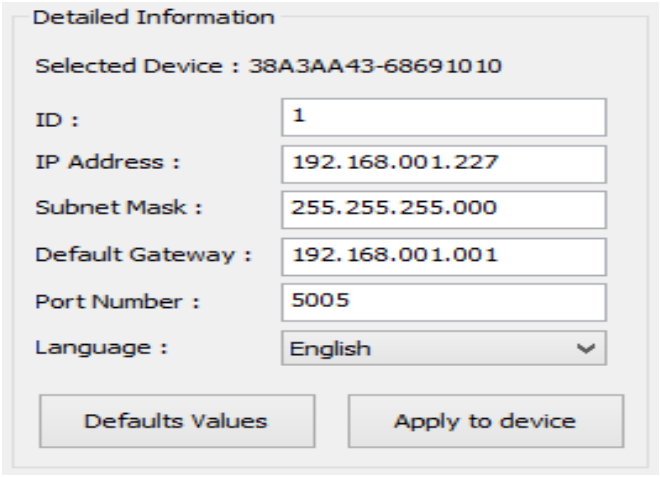
4) Select the card type using drop button : For Register - Register Card / For Delete - Delete Card

5) Click “Register” button to create master card (Register / Delete)

.

Using the card type

No	Unique ID	ID	IP Address	Subnet Mask	Default Gateway	Port	Language
1	38A3AA43-68691010	1	192.168.001.227	255.255.255.000	192.168.001.001	5005	한국어



6. Master Card

5 Master cards are available for Register and Delete in each

1) Register(Delete) the user

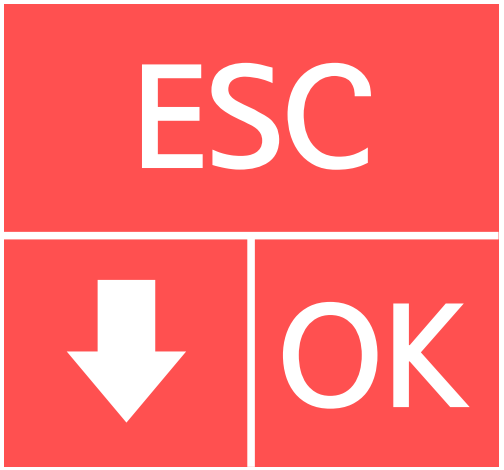
- Present the Register(Delete) card
- KJ-3400 turns to the master mode and Green LED blinks
- Present the user card
- Cards registered to the empty ID in sequence number

  (Corresponding card deleted)
- Present the Register card again to back to normal mode

Note : To register in designated number, please use Guardian software

Using the fingerprint type

Using the fingerprint type



Fingerprint Type

Fingerprint prism implements menu button

Press fingerprint sensor for 3 seconds and access to system menu

If admin user registered, only confirmed admin user has right to access to the system

Note :

Dafult has no admin user and open to access system menu for anyone

Multiple admin user can be reigistered

Using the fingerprint type

Default : No admin user registered

1. Press fingerprint sensor for 3 seconds and access to system menu
2. Move between menus using navigator button

Using the fingerprint type

4.ID (passwords), and how to set up a user or administrator

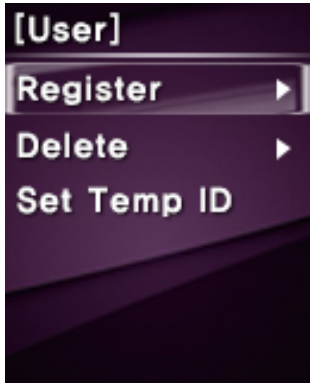
Use the arrows on the arrow on the sensor then

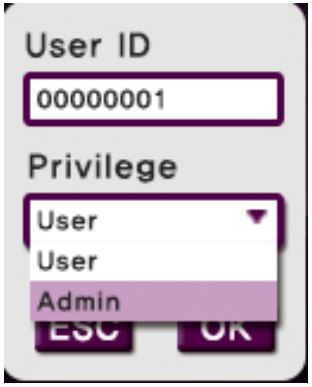
press the OK button ID (password) can be up and down.

Then click OK to set the ID can be set.

User

User - Registration



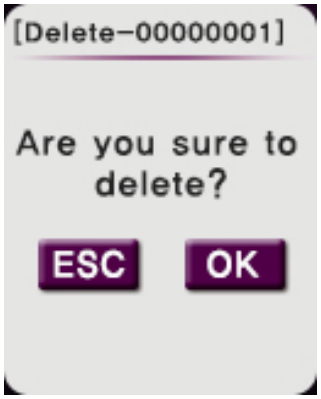


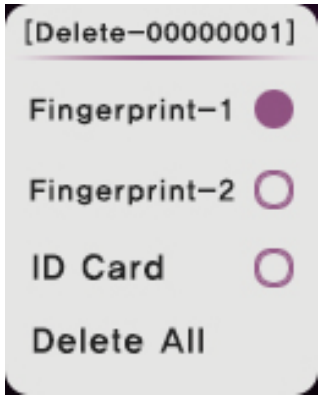
1. Access to system menu
2. Select "User" and press OK button
3. Select "Register" and press OK button
4. Input password (USER ID) and set up the privilege

   User or Admin
5. Register fingerprints and/or card
6. Scan fingerprint 3 times to register and 2 fingerprints are

   available per ID
7. Place user card to read card no.

User - Delete



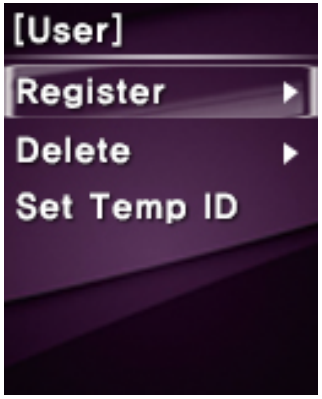


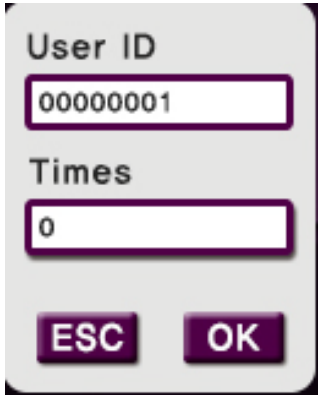
1. Access to system menu
2. Select "User" and press OK button
3. Select "Delete" and press OK button
4. Input password (USER ID) to delete and press OK button
5. Select "Fingerprint" and/or "ID Card" to delete

(If want to delete both fingerprint and card of the relevant ID, select "Delete All")

6. Press OK button after selection
7. Complete the delete

User - TEMP ID

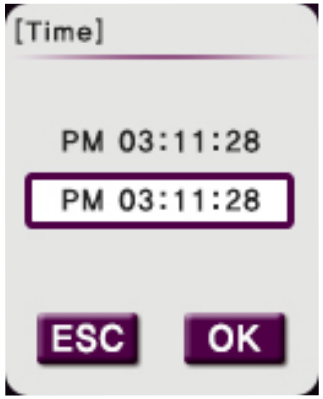


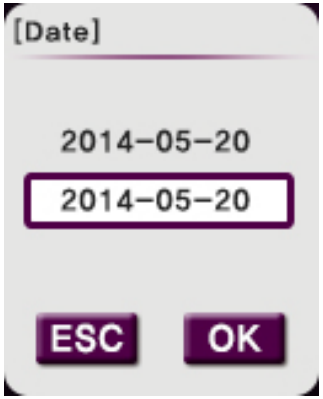


1. Access to system menu
2. Select "User" and press OK button
3. Select "Set Temp IP" and press OK button
4. Input Temp ID (Upto 8 digits) and press OK button
5. Input access admission times (Min. 1, Max. 9) with this them ID and Press OK button)
6. Setup Temp ID completed

Settings

Settings - Basic





1. Time

Set-up the time of the device

Device's time is applied to the time of the event. So it is important the accurate time.

2. Date

Setup the date of the device.

3. Date Format (YYYY-MM-DD)

Define date format at home screen

4. Language

Choose the language

Settings - Advanced

1. Verification Mode

Depends on the security level, it is able to adjust

the verification mode.

2. ID mask

When the user input ID, it hides user ID as XXXXXX and enhance the security.

3. Tamer Alarm

When it detects tamper, it activates alarm.

4. Touch Sensor

If touch sensor is on, sensor lights off in normal condition and lights on

when the user touch the sensor only.

Settings - Advanced

5. Calibrate Sensor

Optical sensor perceive surroundings and optimize the brightness.

When use this function, it has to block external light.

6. Factory Settings

Reset all settings to the default

7. Clear General Log

Delete all general log data

8. Clear Admin Log

Delete all Admin log data

9. Clear User Info

Delete entire user data including fingerprint, card data and it is unrecoverable

Settings - Advanced

1. VERIFICATION MODE

1) **ANY MODE :** Access granted with any form of authorization

2) **FINGER :** Fingerprint only - Not able to access even with the registered ID or Card

3) **CD OR FP :** Card or Fingerprint only - Not able to access even with the registered ID

4) **OPEN :** Always Open (Fail Safe Mode)

5) **CLOSE :** Always Closed (Fail Secure Mode)

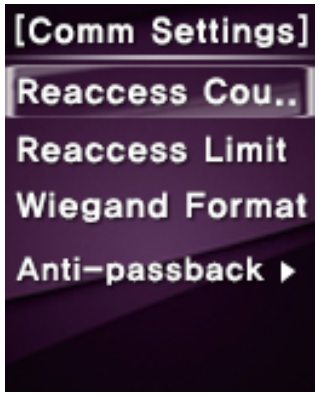
- No access with any form of authorization

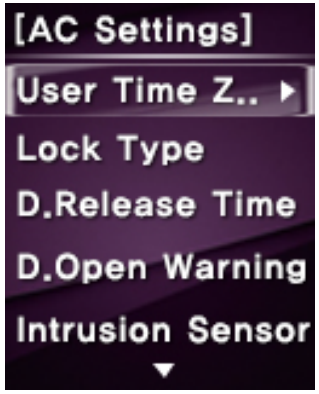
6) **CD :** Card only - Not able to access even with the registered ID or Fingerprint

7) **CD&FP :** Both Card and Fingerprint required for Access

- Card must be authorized before fingerprint authentication

Settings - AC Settings





1.User Time Zone

Able to allocate 2 time zones for each user.

"0" for All Time Access and "257" for Never Access.

2.Lock Type

NC or NO Set up door lock type

3.Door Release Time

Default 3sec. Available to adjust between 1 ~ 99sec.

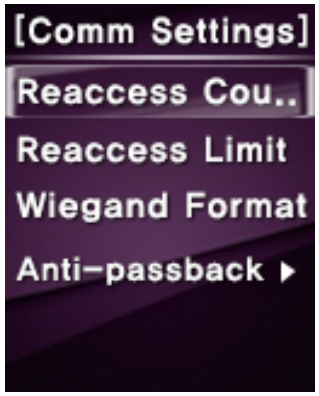
4.Door Open warning

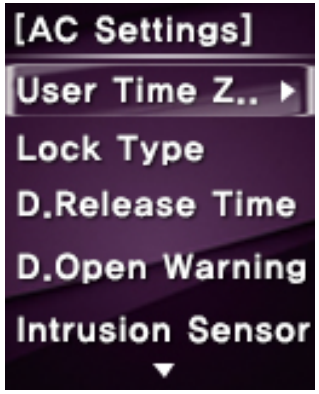
Once door open, if the door remains open over setting condition, it activates alarm

5.Intrusion Sensor (Intrusion/ fire)

This function is connected to a fire alert system. An alert signal is activated when there is a fire or intrusion and all doors are forced open, Intrusion detector closes all doors when an intrusion is detected.

Settings - AC Settings





6 Re-access Count

No, 0~ 9 Limit re-access count between no.0 ~ 9times.

7.Reaccess Limit

Limit re-access time between no. 0 ~ 600minutes.

8.Wiegand Format (26,34,35,37,64)

Designate wiegand output format 26,34,35,37, or 64.

Read all wiegand data regardless of wiegand settings

9.Anti-Passback (No / Yes)

Anti-passback activates through external wiegand input.

If there is two controllers for enter and exit, re-enter is allowed only it has

exit event data (EX : Public Parking lot, Restricted Area, Membership center)

Settings - Communication settings

1 .Device ID (1 ~ 999)

Device ID ranges between 1 ~ 999.

When many devices are connected in one network, each device must have unique address.

2. TCP/IP Settings

1) DHCP : No/ Yes

Choose DHCP on or off

2) IP Address : 192.168.1.224

Setup IP Address

3) Subnet Mask : 255.255.255.000

Setup subnet mask

4) Port : 5005

Setup TCP Port

Settings - Communication settings

5) Default Gateway : 192.168.001.001

Setup default gateway

6) Port : 5005

Setup TCP Port

7) MAC Address

Displays MAC Address of the device.

Cannot set it up from the device

8) Server Settings

7-1. IP Address Port

7-2. Port

7-3 Send Event

3.Com.Password (0~8)

Set the password for the communications equipment. Password is not correct communication the PC program Communication is impossible.

Settings - Log Settings

1. Admin Log Warning (0 ~ 100)

If the management logo exceeds the setting value, it alarms

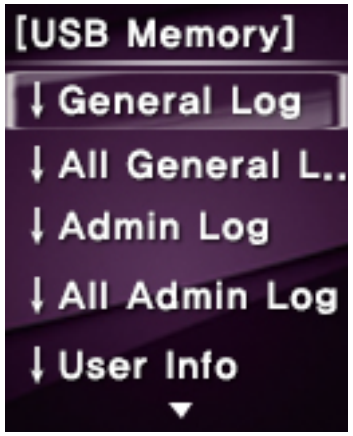
2. General Log Warning (0~2000)

If the management logo exceeds the setting value, it alarms

USB Disk

USB Disk

Insert USB memory into the slot at the bottom of the device and up/download the events data and update the firmware



1. Download General log

Download new general events

2. Download All General log

Download all general events

3. Download Admin log

Download new management events

4. Download All Admin log

Download all management events

5. Download User Info

Download user data

6. Upload User info

Upload user data

7. Upgrade Firmware

Update Firmware

(File Name should be KJ-3400FW.bin)

System Information

System Information - Memory

1. User

User numbers which is enrolled in the device

2. Fingerprint

Template numbers which is enrolled in the device

3. ID Card

ID Card numbers which is enrolled in the device

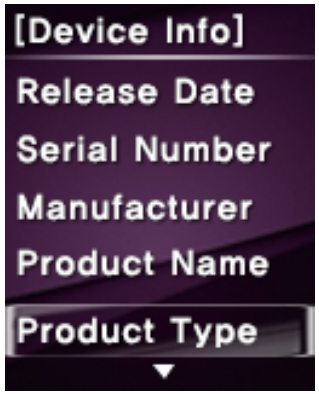
4. General Log

General log (access event) numbers

5. Admin Log

Management log (system event) numbers

System Information - Device Info



1. Release Date

Displays the device release date

2. Serial Number

Displays the device serial number

3. Manufacturer

Displays the device manufacturer

4. Product Name

Displays the device Name

5. Product Type

Displays the device Type

6. Engine Version

Displays the engine version

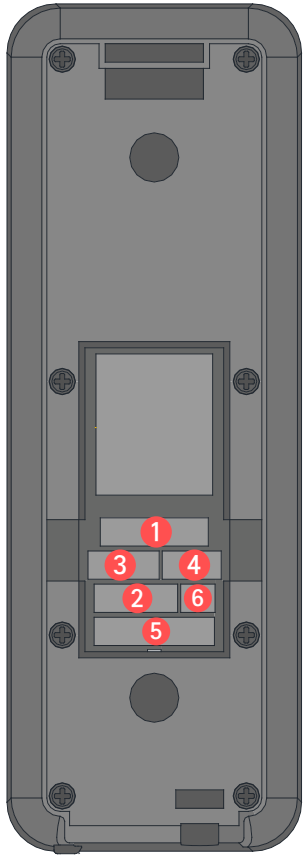
7. Firmware Version

Displays the firmware version

Install Gudie

Connections

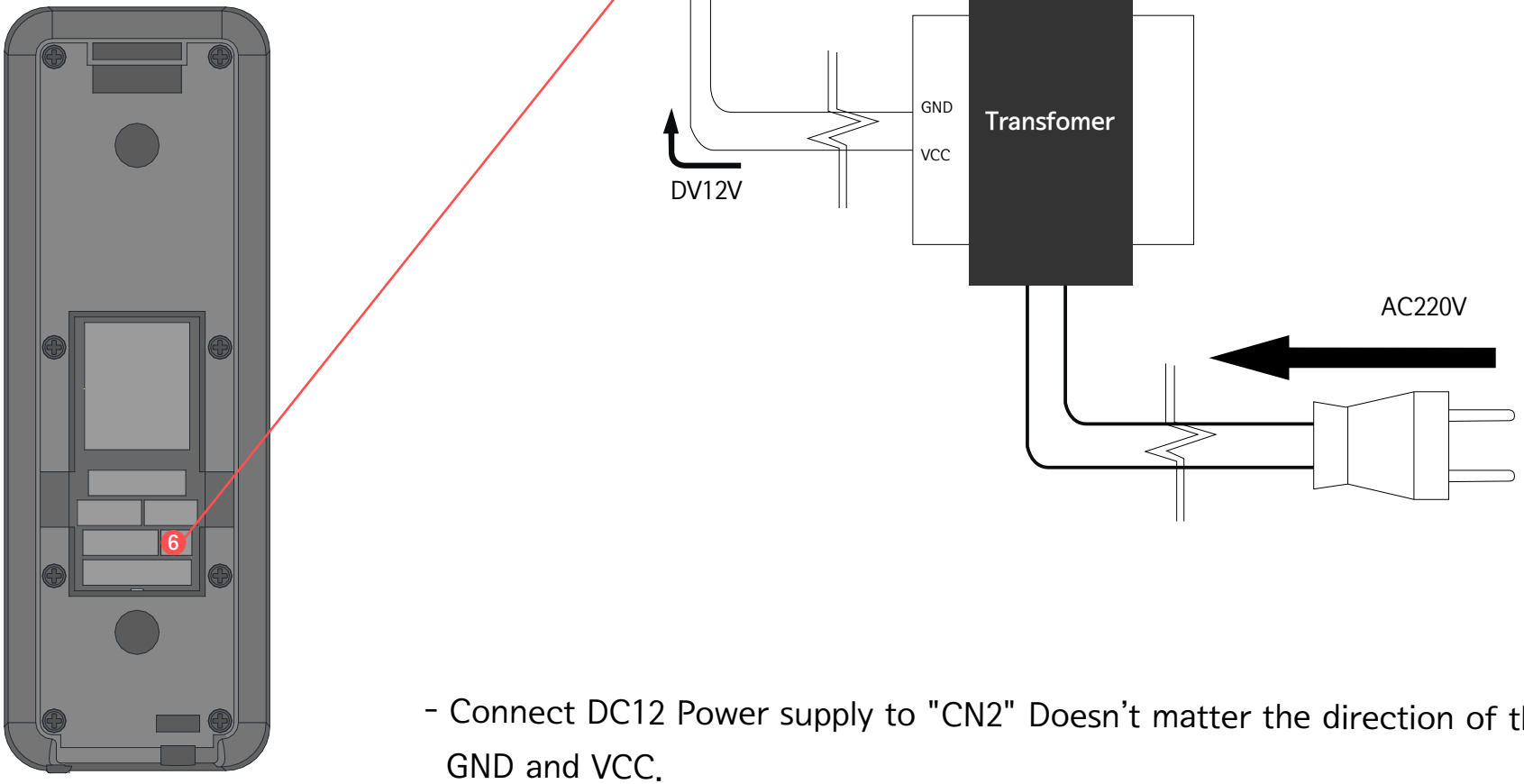
KJ-3400 supports MDI/MDIX and can connect with PC using straight CAT-5 cable not cross cable



1. **CN1)TCP/IP Connector**
   - Using extension cable, communication TCP/IP with PC
2. **CN501) Relay 1,2**
   - Connects with door lock and alarm devices
3. **CN503)Wiegand Input**
   - Connects with external card reader
4. **CN506) Wiegand Output**
   - Outputs CARD data

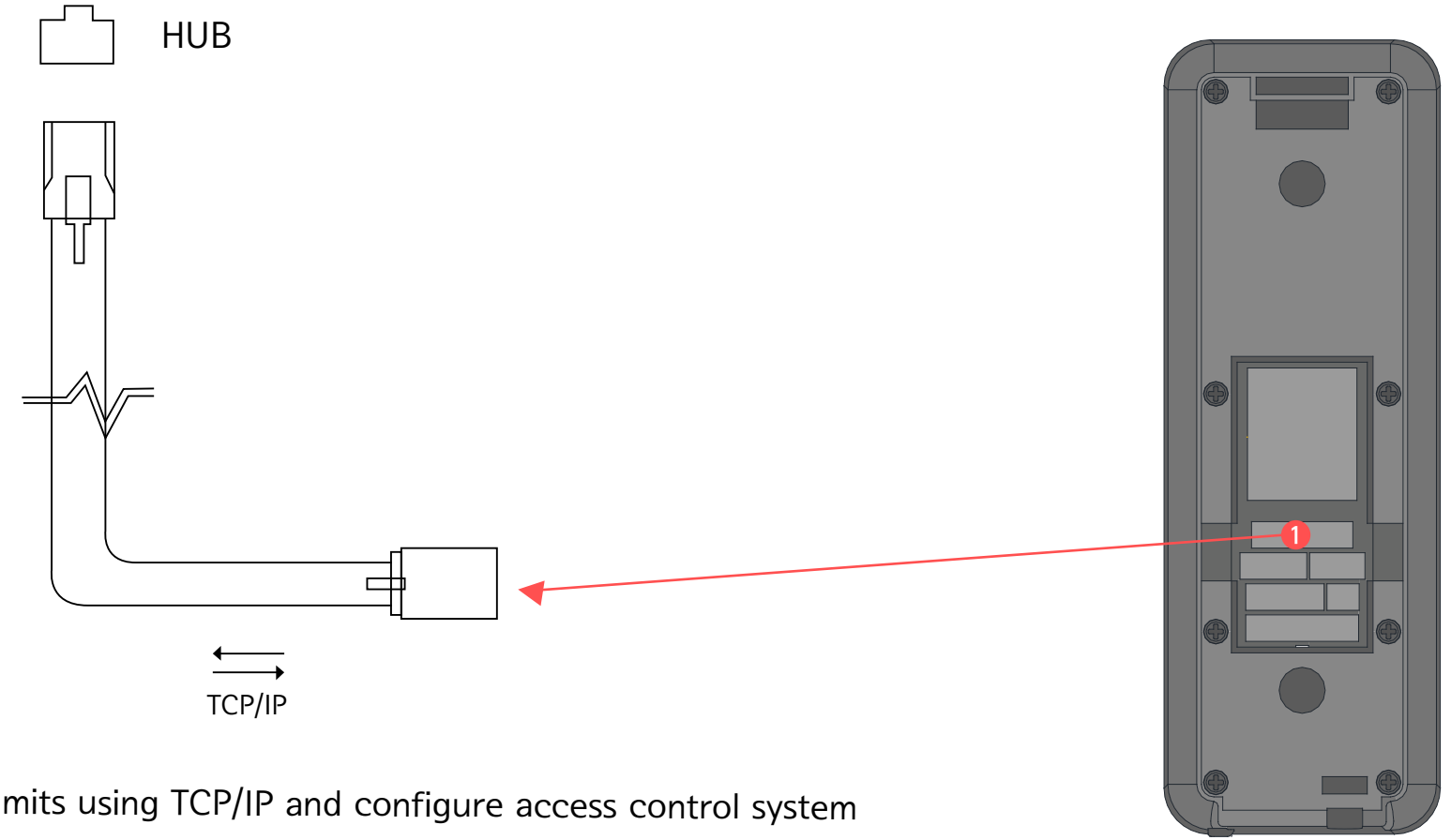
   (Used when it is integrated with other main controller)
5. **CN505) Sensor Input**
   - Connects with various sensors (door contact, alarm sensor etc) and exit button
6. **CN2) Power Input**
   - Supply 12V power to KJ-3500 through power supply

Cable Connection - Power



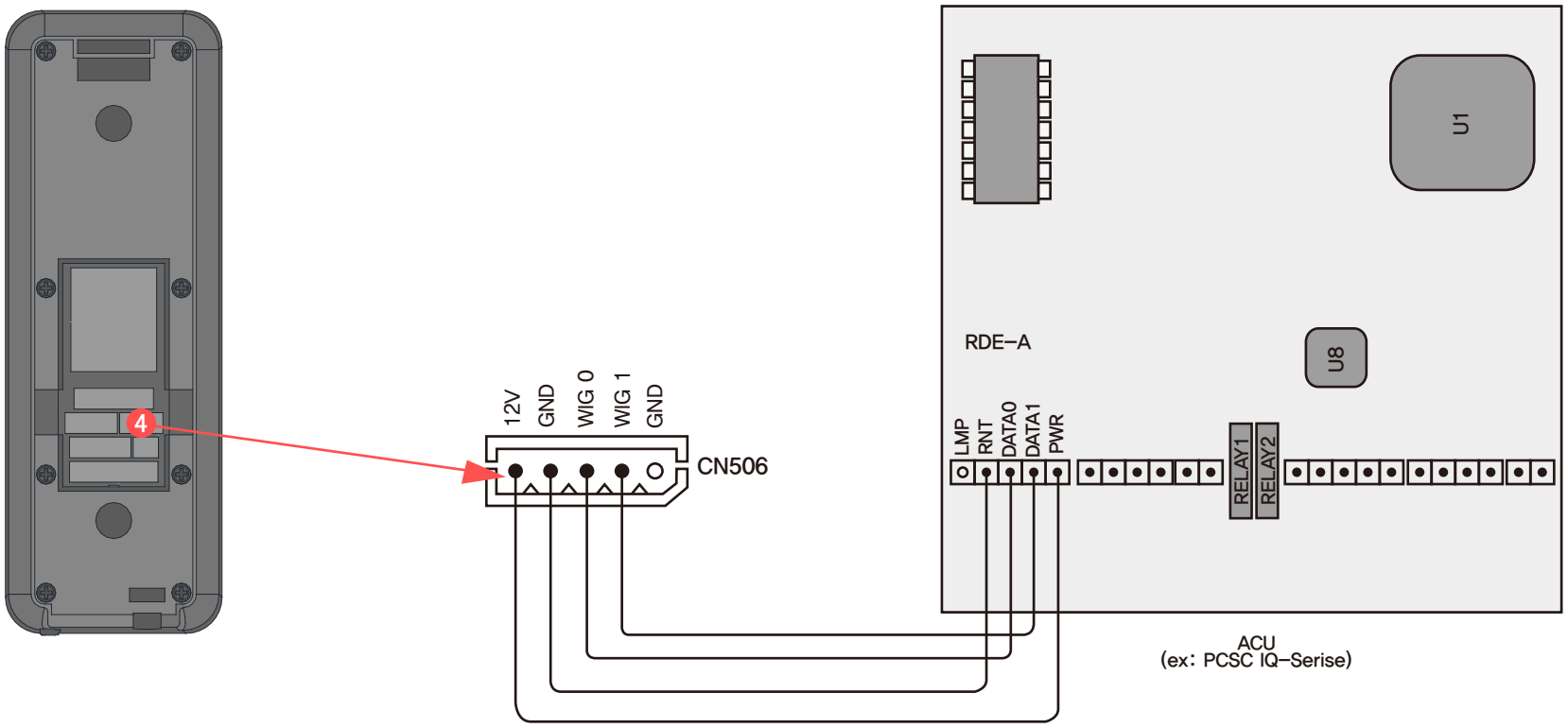
- Connect DC12 Power supply to "CN2" Doesn't matter the direction of the GND and VCC.

Cable Connection - TCP/IP



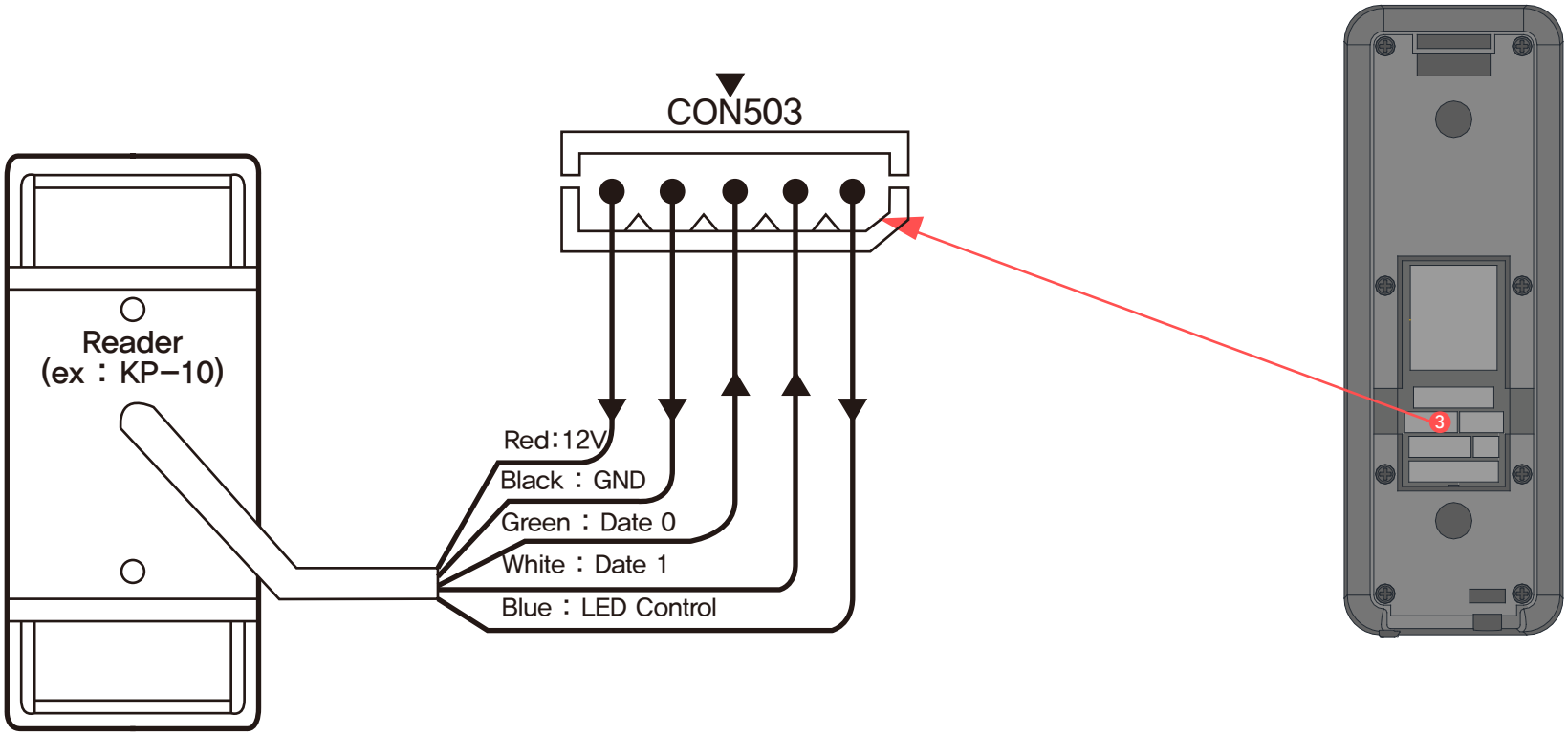
- No distance limits using TCP/IP and configure access control system with LAN or WAN (Refer to manual - " TCP/IP Settings" or guardian software manual for the IP setup) Use enclosed extension cable and plug in "CN1" and connect device with RJ45

Cable Connection - Wiegand Out



- If connected to other main controller, it works as a card reader or fingerprint reader only not controller. CN506(Wiegand out) connects with card reader port of main controller and transmit the data via Wiegand

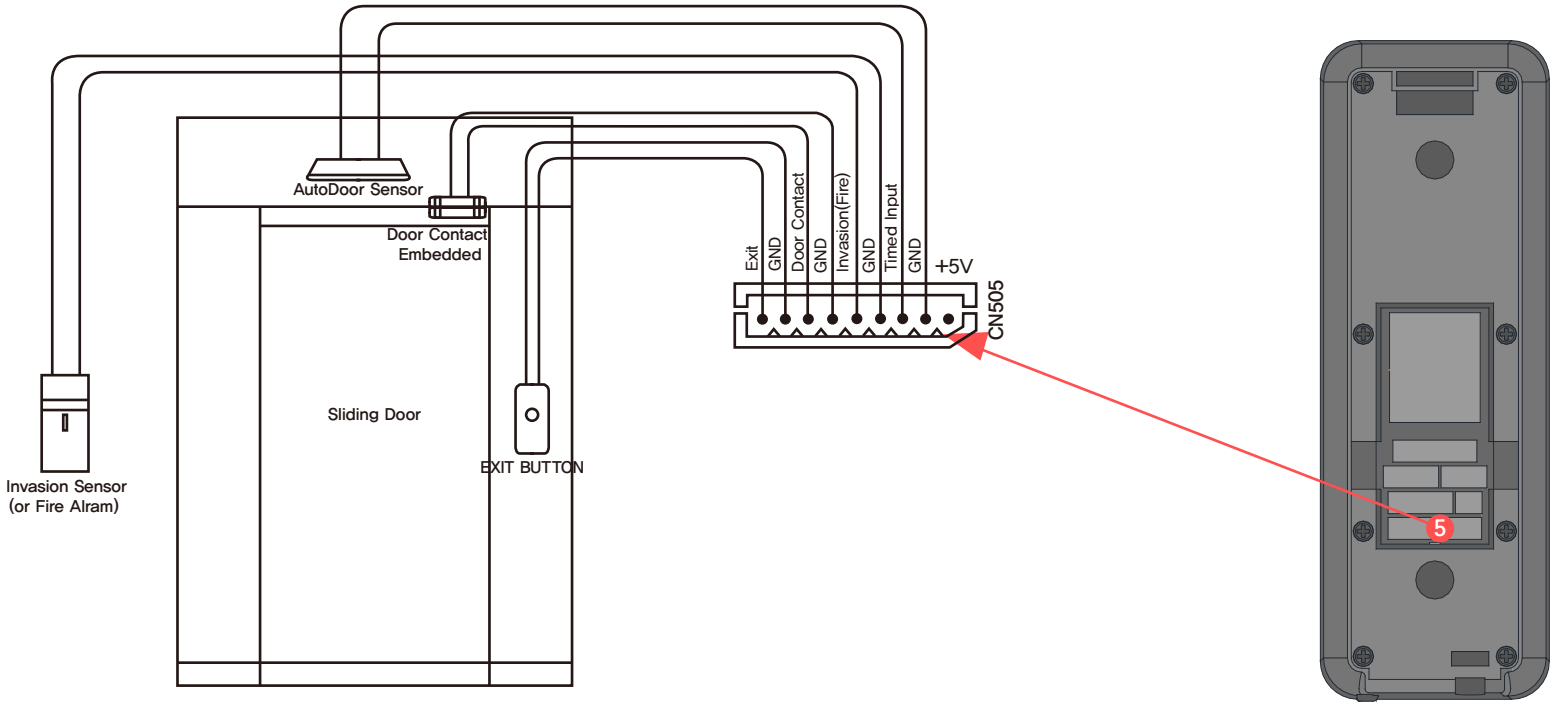
Cable Connection - RF Card Reader



-Connects the cable of the RF card reader to CN503. Connection would be variable for each reader.

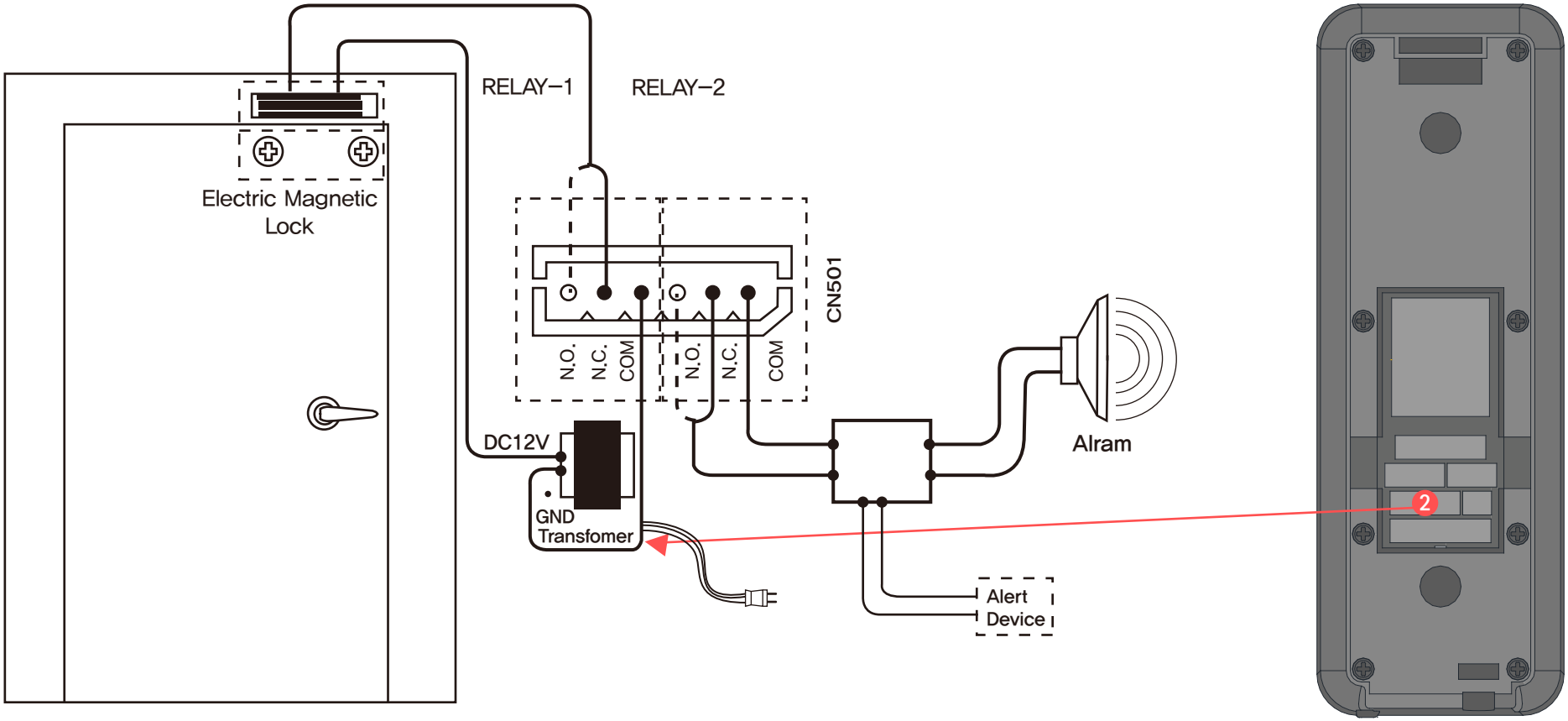
(Follow the manual of each RF card reader)

Cable Connection - Sensor



- Connected with sliding door and relevant controls ; door contact, door sensor, exit button, infrared sensor.

Cable Connection - Relay



-Connected with many devices which detect certain situation through the sensors explained in the above.

Electric strike or alarm devices to be operated with KJ-3400 through CN501.

Fingerprint Verification Technology

KJ TECH

Please keep always in a location that permits a person to use after reading Instruction Manual (CD) to view at any time.

When you receive the product label information required for the service which you may want to reference..

Model _____

S/N _____