Qoltec®

Model: 52440, 52441

## INTRODUCTION

Thank you for your trust and for choosing the Qoltec combination lock. We are confident that the product will meet your expectations.

This manual will guide you through the installation and use of the unit. It contains important safety instructions for operation and correct installation. If you have any questions after reading the manual, please contact Customer Service.

## ABOUT THE PRODUCT

The device is a multifunctional access controller for single doors or with Wiegand output.

The operation is very user-friendly and the low-power circuitry ensures a long service life.

The device supports 1,000 users (988 regular users + 2 emergency users + 10 visiting users), all user data can be transferred between users (except for fingerprint users). Supports multiple access modes: access by card, PIN, fingerprint, card + PIN or multiple cards / PIN / fingerprint. It has additional features such as lock storage, Wiegand input and output interface, etc.

### Features

- Capacitive fingerprint sensor, touch button
- Metal housing, vandal-proof
- Waterproof, IP68 compliant
- One relay, 1000 users (988 regular + 2 emergency +10 visitors)
- PIN code length: 4~6 digits
- EM card
- EM card version: Wiegand 26～44 bits input and output
- Can be used as Wiegand reader with LED output and buzzer
- Storage of card blocks

- Three-colour LED status indicator
- Integrated alarm output and buzzer
- Pulse mode, switching mode
- Possibility of transferring user data (except for fingerprint users)
- Possibility to lock 2 devices for 2 doors
- Built-in light dependent resistor (LDR) for tamper protection
- Backlit keypad, can be set to automatically switch off after 20 seconds.

**Contents of the package**

The contents of the package can be seen in Figure 1.

1. combination lock
2. diode IN4004 (for relay protection)
3. mounting pins
4. screws dia. 4*25mm
5. screwdriver

6 Administrator card

| **Simplified instructions** | |
|---|---|
| **Description of functions** | **Operation** |
| Enter programming mode | ***(Admin code) #**<br>Now you can program (123456 is the default Administrator code) |
| Change of admin code | **0 (New code) # (Repeat new code) #**<br>(code: 6 digits) |
| Adding a user card | **1 (Load card) #**<br>(cards can be added continuously) |
| Adding a fingerprint | **1 (fingerprint)(repeat fingerprint)(repeat fingerprint) #** |
| Adding a user PIN | **1 (PIN code) #**<br>(PIN is any 4 ~ 6 digits except |

| | |
|---|---|
| | 8888, which is reserved) |
| User deletion | **2 (fingerprint) #**<br>**2 (load card) #**<br>**2 (PIN code) #** |
| Output | * |
| **With what to open the door** | |
| User fingerprint | Fingerprint |
| Card | Load card |
| PIN code | Enter PIN# |

## TECHNICAL SPECIFICATIONS

**Model: 52448**

| No. | Parameter | Value |
|---|---|---|
| 1 | Type | EM |
| 2 | Transmission type | RFID |
| 3 | Mode of operation | Buetooth / fingerprint / PIN / card / key fob |
| 4 | Degree of protection | IP68 |
| 5 | Nominal voltage | DC 12 - 24V |
| 6 | Frequency | 125kHz |
| 7 | Number of relays | one |
| 8 | Load | 3A |
| 9 | Number of users | 10000 |
| 10 | Proximity reader | Yes |
| 11 | Touch keyboard | Yes |
| 12 | Fingerprint reader | Yes |
| 13 | Opening with a smartphone | Yes |
| 14 | Operating temperature | -30°C~60°C |

**Model 52449**

| N | Parameter | Value |
|---|---|---|

| o. | | |
|---|---|---|
| 1 | Type | EM |
| 2 | Transmission type | RFID |
| 3 | Mode of operation | Fingerprint/PIN code/card/key fob |
| 4 | Degree of protection | IP68 |
| 5 | Nominal voltage | DC 12 - 24V |
| 6 | Frequency | 125kHz |
| 7 | Number of relays | one |
| 8 | Load | 3A |
| 9 | Number of users | 10000 |
| 10 | Proximity reader | Yes |
| 11 | Touch keyboard | Yes |
| 12 | Fingerprint reader | Yes |
| 13 | Otivering via smartphone | Yes |
| 14 | Operating temperature | -30℃~60℃ |

## INSTALLATION

- Remove the back cover of the keyboard using the screwdriver provided

- Drill 2 holes (A, C) in the wall for the screws and one hole for the cable

- Insert the supplied rubber pins into the holes (A, C)

- Fix the back cover firmly to the wall using 4 flat head screws

- Pull the cable through the hole (B)

- Attach the keyboard to the back cover

Markings shown in Figure 2.

### Connection

| No. | Colour | Function | Description |
|---|---|---|---|
| Basic stand-alone wiring | | | |
| 1 | red | DC + | 12 - 18V DC Input voltage |
| 2 | black | GND | Negative pole of DC power input |
| 3 | blue | NO | Door relay NO contact (potential-free) |

| | | | |
|---|---|---|---|
| 4 | violet | Common | Common door relay contact (potential-free) |
| 5 | orange | NC | Door relay NC contact (potential-free) |
| 6 | yellow | OPEN | Output request input (REX) |
| Pass-through cabling (Wiegand reader or controller) | | | |
| 7 | green | Date 0 | Wiegand output (pass-through) Data 0 |
| 8 | white | Date 1 | Wiegand output (pass-through) Data 1 |
| Advanced input and output functions | | | |
| 9 | grey | Alarm output | To control panel GND |
| 10 | brown | Contact input | Door opening sensor (NC) |

**Sound and light signalling**

| STATUS | LED | SOUND |
|---|---|---|
| Vigil | Lights up red | - |
| Enter programming mode | Flashing red | 1 x beep |
| In programming mode | Lights up orange | 1 x beep |
| Failure of surgery | - | 3 x beep |
| Exit programming mode | Flashing red | 1 x beep |
| Unblocking | Lights up green | 1 x beep |
| Alarm | Rapidly flashes red | Continuous beep |

**Basic configuration**

**Entering and exiting programme mode**

| Programming | Key combination |
|---|---|
| 1. Enter programming mode | *** (Admin code) #**<br>(Default is 123456) |
| 2. Exit programming mode | ***** |

**Setting the administrator code**

| Programming | Key combination |
|---|---|

| | |
|---|---|
| 1. Enter programming mode | ***(Admin code) #** |
| 2. Change of admin code | **0 (New admin code) # (Repeat new admin code) #**<br>(The code consists of 6 digits) |
| 3. Exit programming mode | * |

**Set operating mode**

**Notes**: The device has 3 modes of operation: standalone mode, controller mode, Wiegand reader mode, select the mode you use.

| Programming | Key combination |
|---|---|
| 1. Enter programming mode | ***(Admin code) #** |
| 2. Standard operation (access controller)<br>**O**R<br>2. Wiegand reader | **77#** (Factory settings)<br><br>**78#** |
| 3. Exit programming mode | * |

## STAND-ALONE MODE

The unit can operate as a standalone access control for a single door. (Factory default mode) -77#.

**Wiring diagram (figure 3)**

**Common power supply**

**Note:** When using a common power supply, it is necessary to install the IN4004 diode or equivalent, otherwise the keypad may be damaged. (IN4004 is included in the package).

**Access control power supply (Figure 4)**

**Programming**

Programming will vary depending on your access configuration. Follow the instructions appropriate to your access configuration.

**Comments**: User ID number: Assign a user ID to a fingerprint / card / PIN to keep track of the user.

**Common user ID:**

- Fingerprint user ID: 0 ~ 98
- PIN / card: 100 ~ 987
- Primary fingerprint User ID: 99
- Emergency user ID: 988 ~ 989
- Guest user ID: 990 ~ 999

**IMPORTANT: User IDs do not need to be preceded by zeros. Writing down the user ID is crucial.**

**User modifications require the user to be available.**

**- Proximity card**
Proximity card: EM 125kHz
**- PIN**: Can consist of any 4-6 digits, except 8888, which is restricted.

**Adding ordinary users**

(Fingerprint user ID: 0 ~ 98, PIN/card user ID: 100 ~ 987, PIN length: 4 ~ 6 digits except 8888).

| Programming | Key combination |
|---|---|
| 1. Enter programming mode | ***(Admin code) #** |

| | |
|---|---|
| **Add user with fingerprint** | |
| 2. Using the Auto ID function (Allows the device to assign a fingerprint to the next available user ID number).<br>**OR**<br>1. Select a specific ID (allows the Master to define a specific user ID with which to associate the fingerprint) | **1 (Fingerprint) (Fingerprint repeat) (Fingerprint repeat)**<br>Fingerprints can be added continuously.<br><br>**1 (User ID) # (Fingerprint) (Repeat fingerprint) (Repeat fingerprint)**<br>Fingerprints can be added continuously. |
| **Adding a user card** | |
| 2. Using the Auto ID function (Allows the device to assign a card to the next available user ID number).<br>**OR**<br>2. Select a specific ID (Allows the Administrator to define a specific user ID to which the card is to be associated)<br>**OR**<br>2. Add card: Block enrolment (Allows the Administrator to add up to 988 cards to the reader in one step) Programming takes 2 minutes. | **1 (Read card)/**<br>**(Enter card number) #.**<br>Cards can be added continuously.<br><br>**1 (User ID) # (Read card) /.**<br>**Enter card number) #**<br><br>**1 (User ID) # (Number of cards) # (First card number 8/10/17 digit) #**<br>Number of cards = number of cards to be saved. . |
| **Adding a user PIN** | |
| 2. Using Auto ID (Allows the device to assign a PIN to the next available user ID)<br>**OR**<br>2. Select specific ID (allows the manager to specify a specific user ID to which the PIN is to be assigned) | **1 PIN#**<br>PIN can be added continuously<br><br>**1 (User ID) # (PIN) #** |
| **3. Output** | ***** |

**PIN code security instructions (valid for 6-digit PIN code only)**

For added security, we allow the correct PIN to be hidden with other digits, up to a maximum of 10 digits.

Example PIN: 123434)

You can use ** (123434) ** or ** (123434)

("*" can be any number from 0 ~ 9)

**Add primary fingerprint (by specific identifier: 99)**

| Programming | Key combination |
|---|---|
| 1. Enter programming mode | ***(Admin code) #** |
| 2. Add primary fingerprint | **1 (99) # (Fingerprint) (Fingerprint repeat) (Fingerprint repeat)** |
| 3. Output | ***** |

**Adding emergency users (applies to card/PIN users)**

(User ID number is 988, 989; PIN length: 4 ~ 6 digits, except 8888).

| Programming | Key combination |
|---|---|
| 1. Enter programming mode | ***(Admin code) #** |
| 2. Add card<br>**OR**<br>2. Add PIN | **1 (User ID) # (Load card)/(Enter card number) #**<br><br>**1 (User ID) # (PIN) #** |
| 3. Output | ***** |

**Adding guest users (applies to card / PIN users)**

(User ID number is 990 ~ 999; PIN length: 4 ~ 6 digits, except 8888).

Possible for card and PIN users, the master user can specify the exact number of entrances for the guest user (from 1 ~ 10).

| Programming | Key combination |
|---|---|
| 1. Enter programming mode | ***(Admin code) #** |
| 2. Add card<br>**OR**<br><br>2. Add PIN | **1 (user ID) # (0 ~ 9) # (load card/enter card number) #**<br><br>**1 (User ID) # (0 ~ 9) # (PIN) #**<br>(0 ~ 9 indicates the number of guest inputs, where 0 indicates 10 inputs) |
| 3. Output | ***** |

**Change of PIN code of users (length of PIN code: 4 ~ 6 digits except 8988)**

| Programming | Key combination |
|---|---|
| Note: The following steps are performed outside of the programming mode, the user can perform them himself | |
| Changing the PIN code | ***(User ID) # (Old PIN) # (New PIN) # (Repeat new PIN) #** |
| Change of card PIN code, opening with PIN code<br>Automatically assigned PIN: 8888 | ***(Read card) (Old PIN) # (New PIN) # (Repeat new PIN) #** |

**Deletion of users**

| Programming | Key combination |
|---|---|
| 1. Enter programming mode | ***(Admin code) #** |
| 2. User deletion - by fingerprint/card/PIN code<br>**OR**<br><br>2. User deletion - by ID number<br>**OR**<br>2. Deletion of a user - by card number<br>**OR** | **2 (Scan fingerprint)/ (read card)/enter PIN) #**<br>Users can be removed continuously<br><br>**2 (User ID) #**<br><br>**2 (enter card number) #** |

| | |
|---|---|
| 2. Deletion of all users | **2 (Admin code) #** |
| 3. Output | ***** |

**Relay configuration setting**

Adjustment of the door opener release time.

| Programming | Key combination |
|---|---|
| 1. Enter programming mode | ***(Admin code) #** |
| 2. Pulse mode<br>**OR**<br><br><br><br>2. Switchover mode | **3 (1-99) # (factory settings)**<br>1-99 setting of the time for which the electric door strike is released, factory setting is 5 seconds<br><br>**30#**<br>Switching on/off switching mode |
| 3. Output | ***** |

**Access mode setting**

In multi-user access mode, the reading time must not exceed 5 seconds, otherwise the device will automatically enter standby mode.

| Programming | Key combination |
|---|---|
| 1. Enter programming mode | ***(Admin code) #** |
| 2. Using a fingerprint<br>**OR**<br>2. With the card<br>**OR**<br>2. By PIN number<br>**OR**<br>2. With card number + PIN<br>**OR** | **40#**<br><br>**41#**<br><br>**42#**<br><br>**43#**<br><br>**43 (2 ~ 9) #** |

| | |
|---|---|
| 2. Multi-user access<br>**OR**<br>2. Access by fingerprint, card or PIN code | (Only after correct reading of 2 ~ 9) users will the door be opened)<br>**44#**<br>(Factory settings) |
| 3. Output | * |

**Setting the scare alarm**

The alarm sounds after 10 unsuccessful entry attempts (factory disabled). It can be set to prevent access for 10 minutes after activation, or to switch off only when a fingerprint/card/PIN or master code is entered.

| **Programming** | **Key combination** |
|---|---|
| 1. Enter programming mode | ***(Admin code) #** |
| 2. Alarm deactivation<br>**OR**<br>2. Alarm activation<br>**OR**<br>2. Code deletion<br><br>**Setting the alarm time** | **60#** (factory settings)<br><br>**61#** triggers alarm, access locked for 10 minutes<br>**62#**<br><br>**5 (0 ~ 3)** # (#fault alarm duration setting is 1 minute) |
| 3. Output | * |

**Setting door opening detection**

**Door open too long detection (DOTL)**

When using the optional magnetic contact or the built-in magnetic contact of the lock, if the door is normally opened but not closed after 1 minute, the internal buzzer will emit an automatic beep to remind you to close the door. The beep can be stopped by closing the door, otherwise it will sound at the same time as the set alarm time.

**Detection of forced opening of doors**

If the lock is equipped with an optional magnetic contact or built-in magnetic contact, when the door is opened, the internal buzzer and external alarm (if any) will sound and can be interrupted by the administrator or user, otherwise the beep will continue for the duration of the alarm.

| **Programming** | **Key combination** |
|---|---|
| 1. Enter programming mode | ***(Admin code) #** |
| 2. Deactivation of door opening detection<br>**OR**<br>2. Enable door opening detection<br><br>**Setting the alarm time** | **63#** (factory settings)<br><br>64#<br><br>**5 (0 ~ 3)** # (#fault alarm duration setting is 1 minute) |
| 3. Output | * |

**The alarm time setting function also applies to the tamper alarm**

**Setting of tones and LED indication**

| **Programming** | **Key combination** |
|---|---|
| 1. Enter programming mode | ***(Admin code) #** |
| 2. Turn off the sound<br>Turn on the sound<br>**OR**<br><br>2. LED off<br>LED on<br>**OR**<br><br>2. Keyboard backlight off | **70#**<br>**71#** (factory settings)<br><br>72#<br>**73# (**factory settings)<br><br>**74#** |

| | |
|---|---|
| Keyboard backlighting on<br><br>**Keyboard backlighting automatically switched off after 20 seconds** | **75#**<br><br>**76#** (factory settings) |
| 3. Output | * |

**Keyboard backlighting automatically switched off after 20 seconds**

| **Using the master fingerprint/card to add and remove users** | |
|---|---|
| Adding and deleting users with a master fingerprint/master card | 1. Data entry (master fingerprint/card)<br>2. Enter (three times) (fingerprint) or (card) or (PIN #)<br>3. Re-enter (main fingerprint/card) |
| Removal of users' fingerprints/cards/PINs | 1. Enter (master fingerprint/card) twice in 5s)<br>2. Enter (fingerprint) or (card) or (PIN #)<br>Repeat step 2 for additional users<br>3. Enter (main fingerprint/card) again |

**User operation and resetting to factory settings**

**- Open the door:** Read the user's fingerprint or user card or enter a valid user PIN.

**- Delete alarm**: Enter master code # or fingerprint/card/user PIN.

**- To restore the factory settings and add a master card**: Turn off the power, press the * button, hold it down and turn on the power, you will hear two beeps, then release the exit button, the LED will turn yellow, then read any EM 125KHz card, the LED will turn red, indicating a successful factory reset. Of the cards read, this is the Administrator card.

**Notes**:

© If an Administrator card has not been added, press the * button for at least 5 seconds before releasing the button (this will invalidate the previously registered master card).

## CONTROLLER MODE

The unit can operate as a controller connected to an external Wiegand reader. (Factory default mode) - 77#

### Wiring diagram (figure 5)

**Note**: When using a common power supply, it is necessary to install a 1N4004 diode or equivalent, otherwise the reader may be damaged. (1N4004 is included in the package).

### Setting of Wiegand input formats

The Wiegand input formats must be set according to the Wiegand output format of the external reader.

| Programming | Key combination |
|---|---|
| 1. Enter programming mode | ***(Admin code) #** |
| 2. Setting the Wiegand input format | **For EM cards: 8 (26 ~ 44) #**<br>(factory setting is 26bits) |
| 3. Disable the parity bit<br>Enable parity bit | **80#**<br>**81#** (factory settings) |
| 4. Output | ***** |

**Note**: When connecting Wiegand readers with 32, 40, 56 bit output, the parity bits must be switched off.

### Programming

- Basic programming is the same as in stand-alone mode

- There are some exceptions that should be noted:
Device connected to external card reader
-EM cards: users can be added/deleted both on the device and on the external reader.
- HID cards: users can only be added/removed at the external reader.

**Connecting an external fingerprint reader to the device**

1. Connect the fingerprint reader to the device.
2. Add a fingerprint (A) on the external reader according to its operating instructions.
3. Add a fingerprint (A) on the device:

| Programming | Key combination |
|---|---|
| 1. Enter programming mode | ***(Admin code) #** |
| 2. Adding a user by means of a fingerprint - user ID number assigned automatically<br>**OR**<br>Adding a user by means of a fingerprint - User ID number assigned manually | **1 Scan your fingerprint on the external reader #**<br><br>**1 User ID number # Scan fingerprint on external reader #** |
| 3. Output | * |

**Device connected to a keyboard reader**

The keypad reader can have a 4-bit, 8-bit (ASCII) or 10-bit output format. Select the following operation depending on the output format of the reader PIN.

| Programming | Key combination |
|---|---|
| 1. Enter programming mode | ***(Admin code) #** |
| 2. PIN encryption type | **8 (4 /8 /10) #** (factory setting is 4 bits) |

| | |
|---|---|
| 3. Output | * |

**Notes**: 4 means 4 bits, 8 means 8 bits, 10 means 10 bits

**- Adding PIN users:**
To add PIN users, after entering the programming mode on the device, the PIN(s) can be entered/added on both the device and an external keypad reader.
**- Remove PIN users**: in the same way as adding users.

## WIEGAND READER MODE

The device can operate as a standard Wiegand reader, connected to a third-party controller...7 8 #

### Wiring diagram (figure 6)

**Notes:** After switching to Wiegand reader mode, almost all settings in controller mode will become invalid and the brown and yellow wires will be redefined as follows:

- Brown wire: Green LED control
- Yellow wire: Buzzer control

### Setting of Wiegand output formats

Set the reader's Wiegand output formats in accordance with the controller's Wiegand input formats.

| Programming | Key combination |
|---|---|
| 1. Enter programming mode | ***(Admin code) #** |
| 2. Wiegand output format settings | **For EM cards: 8 (26 ~ 44) #**<br>(factory setting is 26bits) |

| | |
|---|---|
| PIN encryption type | **8 (4 /8 /10) #** (factory setting is 4 bits) |
| 3. Disable the parity bit<br>Enable parity bit | **80#**<br>**81# (**factory settings) |
| 4. Output | * |

**Note: When connecting a Wiegand controller with a 32, 40, 56 bit input, the parity bits must be disabled.**

## ADVANCED NETWORK

### Transfer of user information (applies to card/PIN users)

The unit supports User Information Transfer, and registered users (cards, PINs) can be transferred from one (let's call it the Master Unit) to another (let's call it the Acceptance Unit).

### Wiring diagram (Figure 7)

**Notes**:
- Master units and accepting units must be units of the same series.
- The master code of the main unit and the accepting unit must be set the same.
- Program the transfer operation only on the main unit.
- If there are users already enrolled in the Acceptance Unit, this will be taken into account after the transfer.
- With 900 users, the transfer takes about 30 seconds.

### Set the transfer in the main unit

| Programming | Key combination |
|---|---|
| 1. Enter programming mode | ***(Admin code) #** |
| 2. Start data transfer to | **98#** |

| | |
|---|---|
| secondary device | |
| Within 30 seconds, the green LED will light up and after one beep the LED will turn red, indicating that the user data has been transmitted successfully. | |
| 3. Output | * |

**Wiring diagram (figure 8)**

**Note**: The door reed switch must be installed and connected according to the diagram. Let's name the two devices as "A" and "B" for the two doors "1" and "2".

**Step 1:** Register users on device A and then transfer their information to device B using the " Set transfer in the main unit" function.

**Step 2:** Set both devices (A and B) to the lock function.

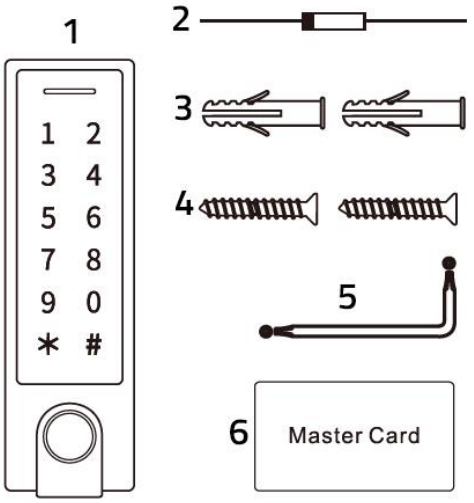
| Programming | Key combination |
|---|---|
| 1. Enter programming mode | ***(Admin code) #** |
| 2. Deactivate the lock function for two electric door openers<br>**OR**<br>2. Activate the lock function for two electric door openers | **90#**<br><br>**91#** |
| 3. Output | * |

With the dual door opener function enabled, if door opener 2 is closed the user can scan a fingerprint/read a card or enter a PIN code on device/reader A, door opener 1 will be released. If electric door strike 1 is

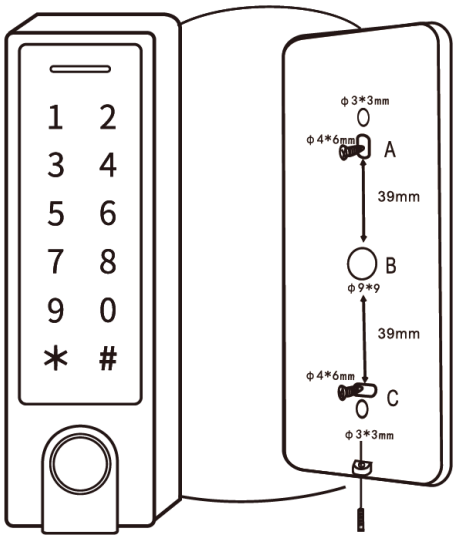
closed the user must scan a fingerprint/read a card or enter a PIN code on device/reader B to release electric door strike 2.

## ATTACHMENT

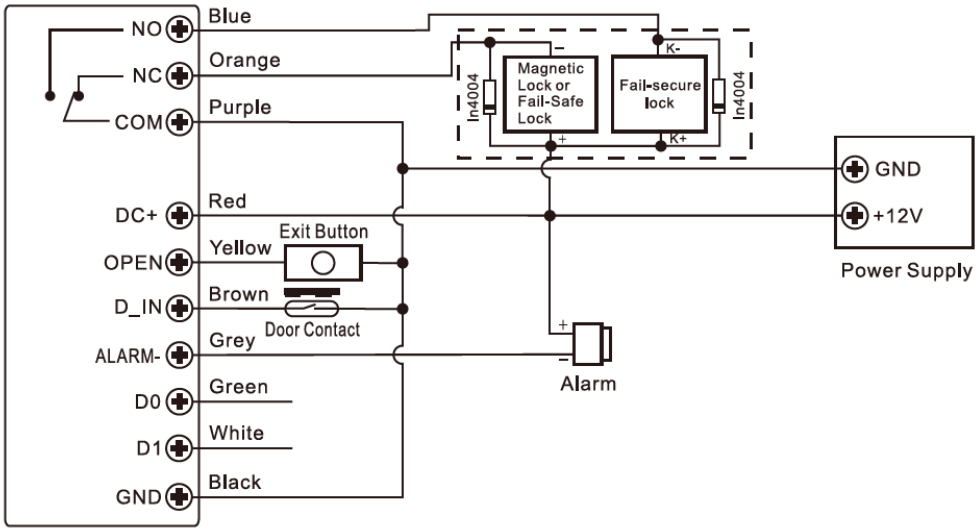
1.



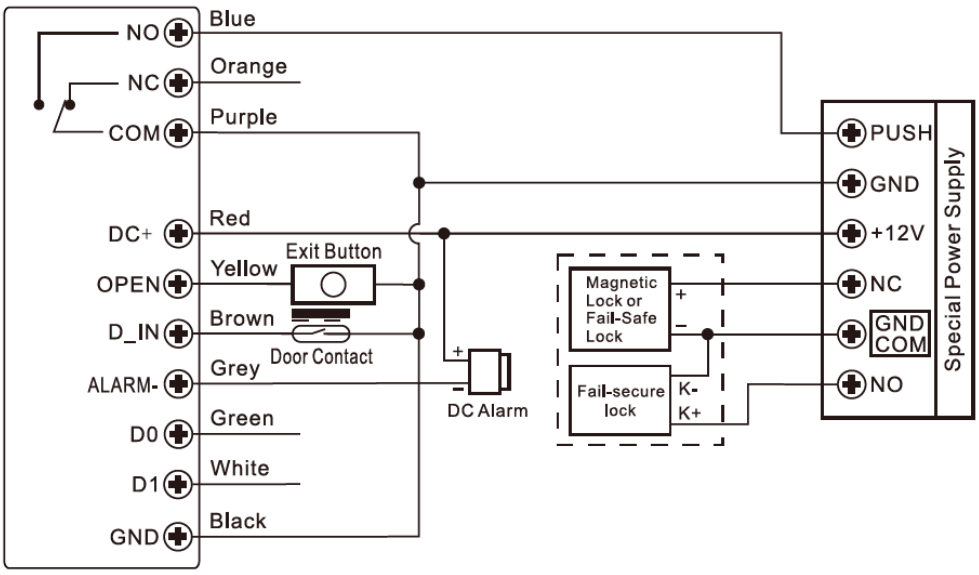

2.



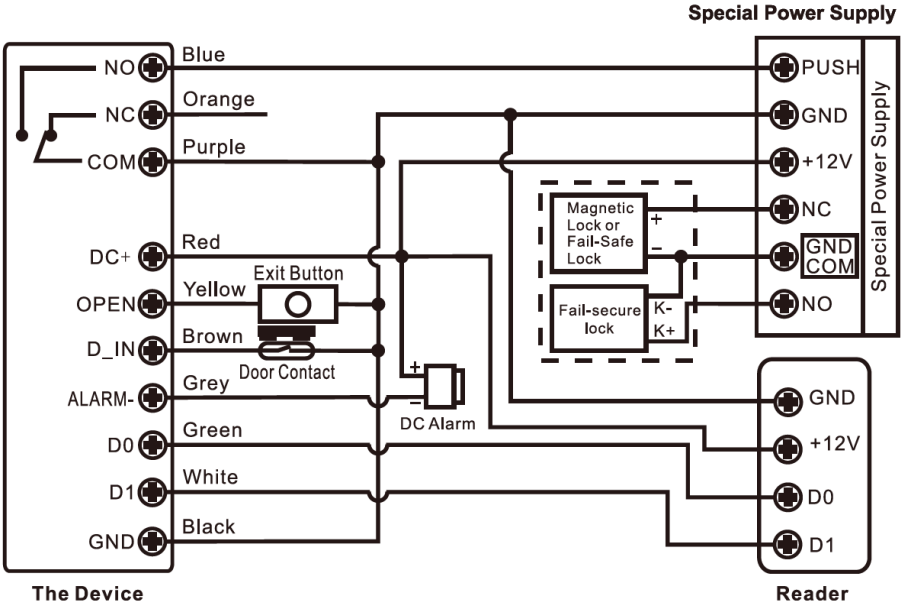

3.



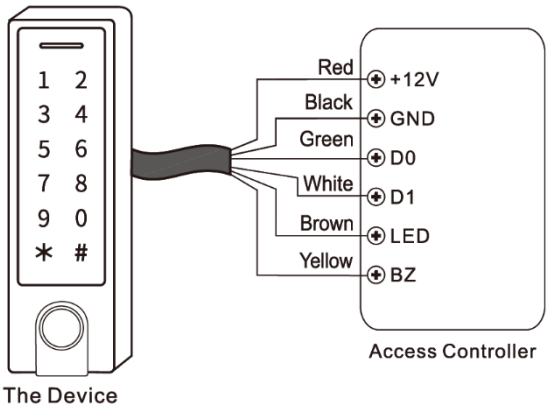

4.



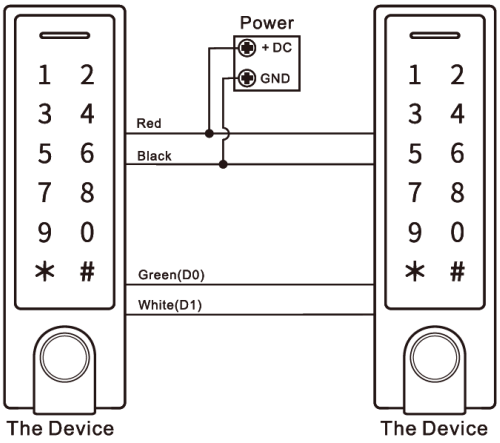
5.


Special Power Supply
NO
NC
COM
DC+
OPEN
D_IN
ALARM-
D0
D1
GND
Blue
Orange
Purple
Red
Yellow
Brown
Grey
Green
White
Black
Exit Button
Door Contact
DC Alarm
Magnetic Lock or Fail-Safe Lock
Fail-secure lock
K-
K+
PUSH
GND
+12V
NC
GND COM
NO
Special Power Supply
GND
+12V
D0
D1
The Device
Reader

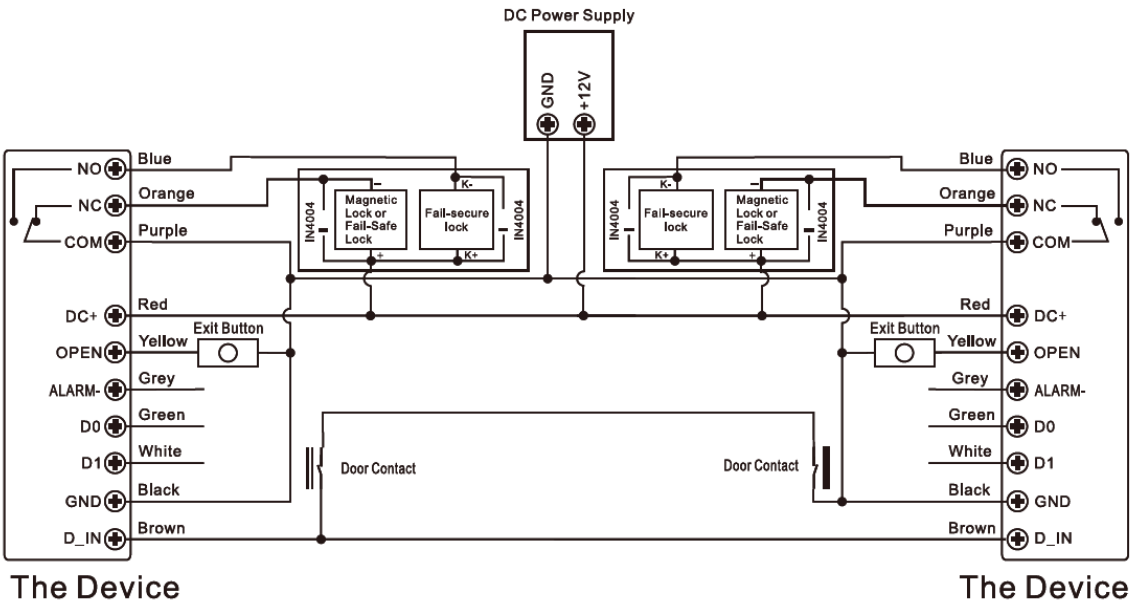
6.


1 2
3 4
5 6
7 8
9 0
* #
Red
Black
Green
White
Brown
Yellow
+12V
GND
D0
D1
LED
BZ
Access Controller
The Device

7.


Power
+ DC
GND
Red
Black
Green(D0)
White(D1)
1 2
3 4
5 6
7 8
9 0
* #
The Device
The Device

8.


DC Power Supply
GND
+12V
NO
NC
COM
DC+
OPEN
ALARM-
D0
D1
GND
D_IN
Blue
Orange
Purple
Red
Yellow
Grey
Green
White
Black
Brown
Exit Button
Door Contact
IN4004
Magnetic Lock or Fail-Safe Lock
Fail-secure lock
K-
K+
The Device
The Device