C Prox Ltd (inc Quantek)
Unit 11 Callywhite Business Park, Callywhite Lane, Dronfield, S18 2XP
+44(0)1246 417113 sales@cproxltd.com www.quantek.co.uk

Access Control Proximity Reader

PN10

User Manual

Please read the manual carefully before installing this unit

1. Packing list

Name	Quantity	Remarks
Proximity reader	1	PN10
Infrared remote	1	
Manager add card	1	
Manager delete card	1	
User manual	1	
Self-tapping screws	2	Φ3.5mm×27mm, used for fixing
Screw driver	1	Star

Please ensure that all the above contents are correct. If any are missing please notify us immediately

2. Description

The PN10 is a waterproof standalone or Wiegand access control proximity reader. It uses an advanced microprocessor with a high capacity flash memory for up to 10,000 users. Users can be added and deleted via admin cards making it very simple to operate. The infrared remote control allows settings to be quickly changed, including altering the relay time, applying the anti-passback function or deleting individual lost cards. Two units can also be interlocked. It has low power consumption, anti-theft alarm and door release button, all these make it convenient, safe and reliable.

3. Features

- Zinc alloy, anti-vandal shell
- Waterproof, conforms to IP68
- High capacity memory, 10,000 users
- Wiegand 26 output and Wiegand 26 input
- Besides standalone, it can connect to a controller as a slave reader
- Infrared remote control and manager cards for programming
- Two devices can be interlocked
- Red, yellow and green LEDs display the working status
- Built in buzzer for anti-tamper alarm, and external alarm output
- Adjustable door output, alarm and door open times
- Fast operating speed

4. Specification

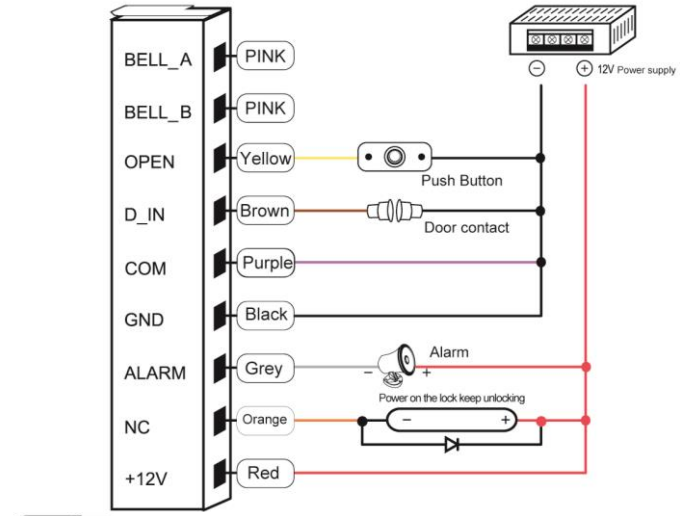
Operating voltage	12-24Vdc
User capacity	10,000
Static consumption	<30mA
Card reading distance	5-8cm
Frequency	125KHz
Operating temperature	-10 to 60^{o}C
Operating humidity	20% to 98% RH
Lock output load	2A
Alarm output load	2A
Waterproof	IP68
Dimensions	115 x 56 x 22 mm

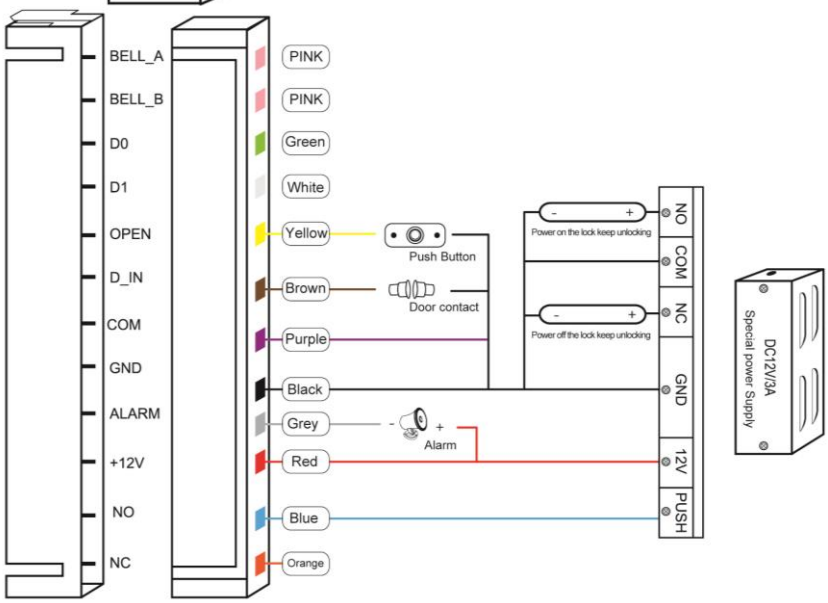
5. Installation

- Remove back plate from the reader using security driver supplied, and use it (or the template) to mark the two fixing holes and one cable hole.
- Secure back plate to the wall using fixing screws provided.
- Thread cable through the hole and connect wires needed, wrap unused wires with insulating tape to prevent short circuit.
- Fit the reader into the back plate and replace retaining screw.

6. Wiring

Colour	Function	Description
Pink	RESET	Reset
Pink	RESET	Reset
Green	D0	WG output D0
White	D1	WG output D1
Grey	ALARM-	Alarm negative (alarm positive connected to 12/24V+)
Yellow	OPEN	Exit button one end (the other end connected to GND)
Brown	D_IN	Magnetic switch one end (the other end connected to GND)
Red	12/24V +	12/24V + DC regulated power input
Black	GND	12/24V – DC regulated power input
Blue	NO	Relay normally open
Purple	COM	Relay common
Orange	NC	Relay normally closed





7. Factory reset & set management cards

Turn off power to the unit. Connect the two pink wires then power on. After the beep, the factory reset is complete and the LED will turn green. Now it is necessary to learn the admin cards again. Read the first card as the admin add card, and the second card as the admin delete card.

Note: Factory reset does not delete user data.

8. Sound & light indication

Operation	LED indicator	Buzzer
Initialisation	Orange	Didi
Standby	Red flash	
Valid button press		Di
Enter programming	Red solid	Di
Setting	Orange	Di
Exit programming	Red flash	Di
Operation failed		Didi
Lock open	Green	Di
Alarm	Quick red flash	Alarm
Add sequential Card No.	Quick green flash	

9. Programming

9.1 Managing users via admin card

9.1.1 Add user via admin card

Read admin add card **Read user card 1** **Read user card 2** **…** **Read admin add card**

9.1.2 Delete user via admin card

Read admin delete card **Read user card 1** **Read user card 2** **…** **Read admin delete card**

9.2 Enter into programming mode (remote control)

***** **Master code** **#** Default master code is 999999

All the steps below must be done after entering into programming mode.

9.3 Change the master code

0 **New master code** **#** **New master code** **#**

9.4 Add users by remote control

9.4.1 Read card to add user

1 **Read card 1** **#** **Read card 2** **#** **…** **#**

9.4.2 Use card number to add user

1 **Card number** **#** **Card number** **#** **…** **#**

Note: Multiple cards can be added without exiting programming mode. Card number digits must be 8 or 10 digits, if the card number is less than 8 or 10 digits, input 0 before the card number.

9.4.3 Add sequential card numbers

1 **Card quantity** **#** **First card number** **#**

Add consecutive number card users, card quantity 1-9999. Fast green flash to confirm.

9.5 Delete users by remote control

9.5.1 Read card to delete user

2 **Read card 1** **#** **Read card 2** **#** **…** **#**

9.5.2 Use card number to delete user

2 Card number # Card number # … #

Multiple cards can be deleted without exiting programming mode.

9.5.3 Delete all users

2 0000 #

Note: This operation will delete all users, but admin card won't be deleted.

9.6 Safe mode setting

9.6.1 Normal mode (Factory default)

3 0 #

9.6.1 Dead mode

3 1 #

Read invalid card 10 times continuously within 10 minutes, the device will be dead for 10 minutes.

9.6.2 Alarm mode

3 2 #

Read invalid card 10 times continuously within 10 minutes, both the built-in buzzer and external alarm sound.

9.7 Door open time setting

4 0 - 99 #

Note: Range is 0 – 99 seconds. 0s equates to 50Ms.

9.8 Alarm time setting

5 0 - 3 #

Note: Range is 0 – 3 minutes. Factory default is 1 minute.

9.9 Red light mode setting

9.9.1 Standby disable mode (red light is off when device is on standby)

6 0 #

9.9.2 Standby normal mode (red light flashes when device is on standby, factory default)

6 1 #

9.10 Interlock mode setting

9.10.1 Interlock disabled (factory default)

7 0 #

9.10.2 Interlock enabled

7 1 #

9.11 Anti-passback mode setting

9.11.1 Anti-passback disabled (factory default)

8 0 #

9.11.2 Anti-passback host mode enabled

8 1 #

9.11.2 Anti-passback subsidiary mode enabled

8 2 #

Note: Details will be illustrated in the advanced application section below.

10. User operation

10.1 User to release the door

Read valid card

Reading a valid card user will unlock the door, admin cards will not unlock the door.

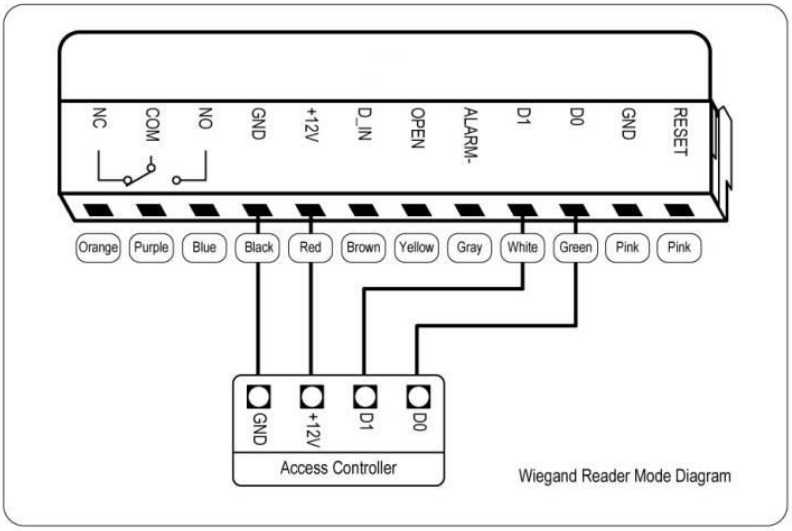
10.2 Remove alarm operation

Read valid card **Or** **Read admin card** **Or** **Input master code**

11. Advanced applications

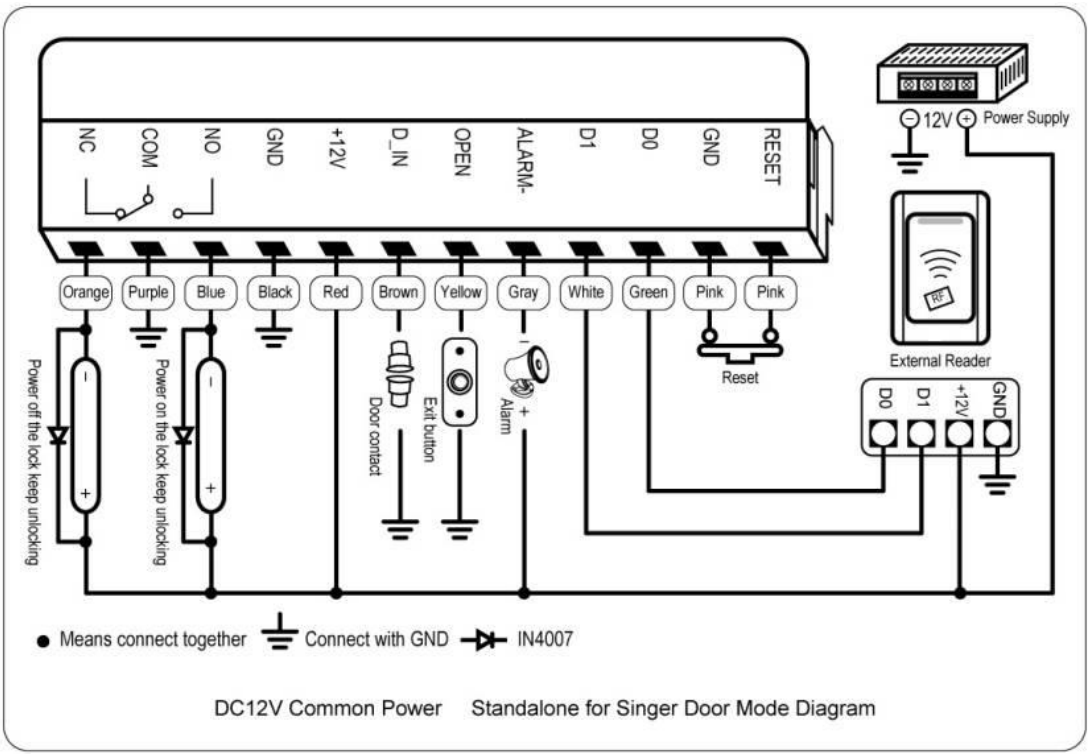
11.1 PN10 works as a slave reader, connecting to a controller

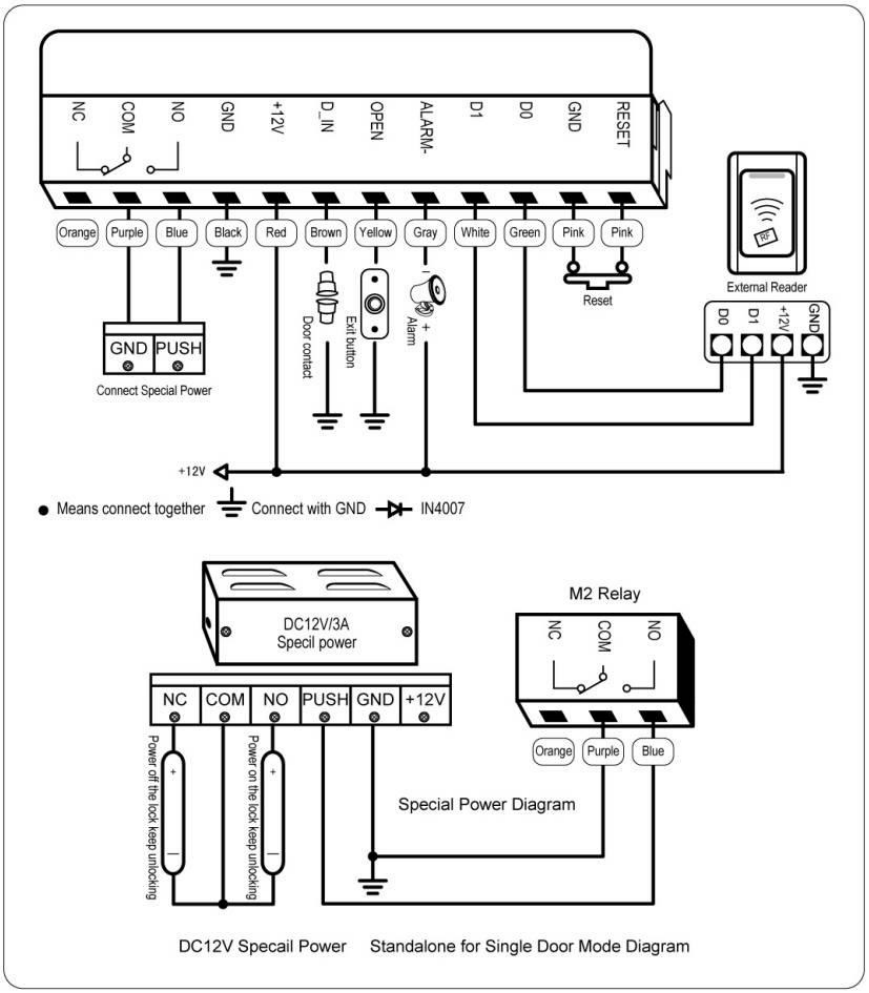
PN10 supports Wiegand output. It can be connected to a controller which supports Wiegand 26 input as its slave reader.



11.2 PN10 works as a controller, connecting to a slave reader

PN10 supports Wiegand input, any card reader which supports Wiegand 26 interface can connect to it as a slave reader. The connections are shown in the below diagram. When adding cards, it is required to do it at the slave reader, not the controller (except EM card reader, which can be added on both the reader and controller).

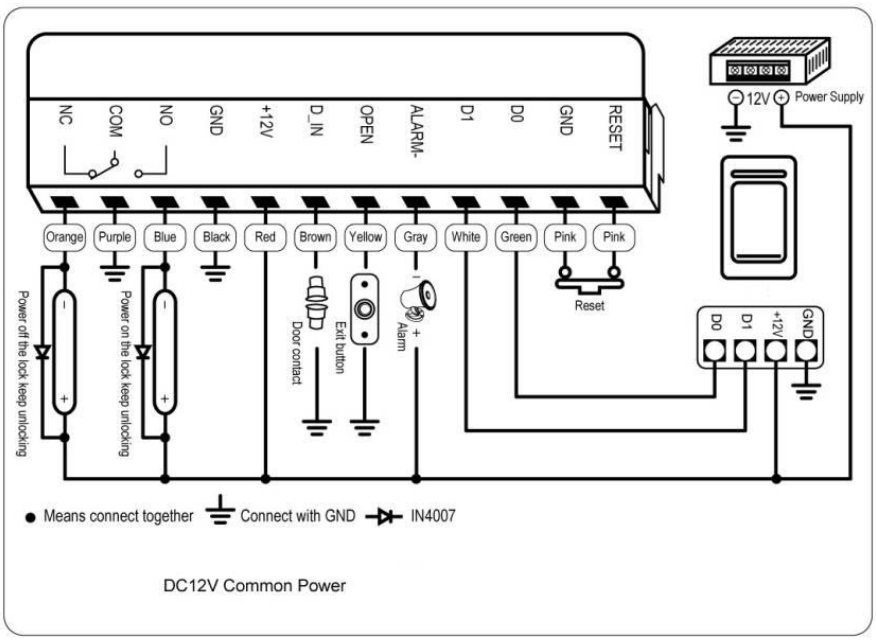




11.3 Two devices interconnected – Single Door

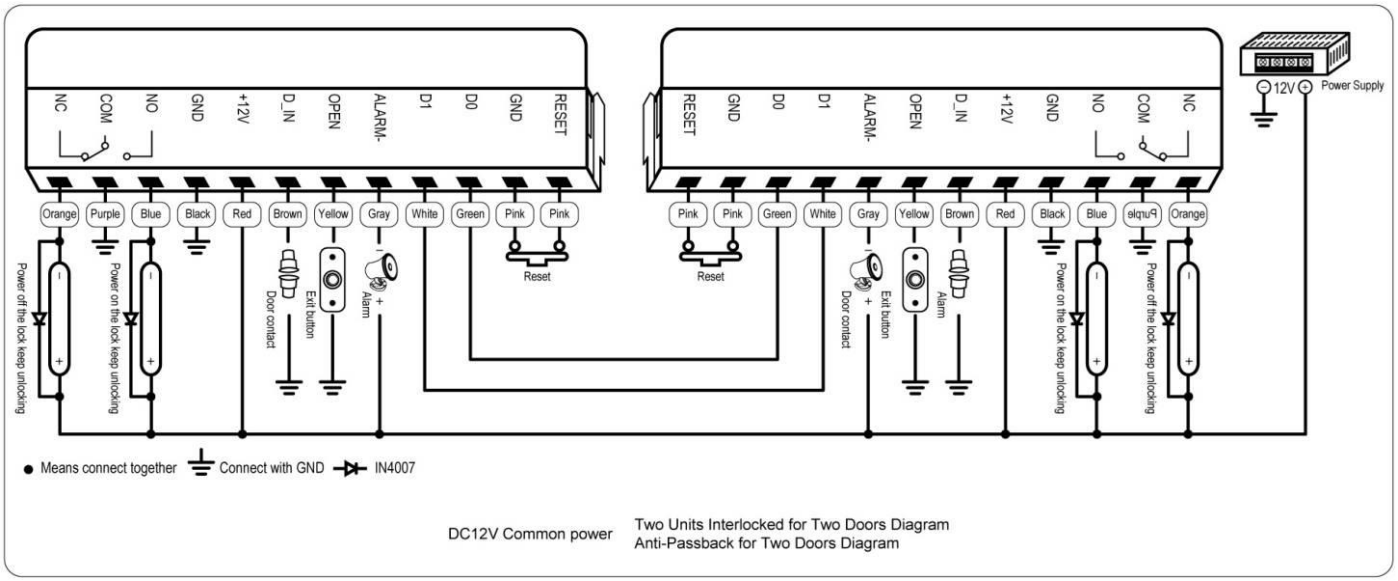
Install one unit indoor and another outdoor, the indoor unit as a controller, the outdoor unit as a reader. This has the following features:

- Users can be enrolled on either device.
- The information on the two devices can be communicated, so in this case the user capacity for one door can be 20,000.
- The setting of both devices must be the same. If the master codes were different, the user enrolled in the outdoor unit can't access from the inside.
- Anti-passback mode can be enabled in host mode. Users must present card on the external reader to enter and internal reader to exit every time, to ensure they enter and exit legally. Users cannot enter or exit 2 times continuously.



11.4 Two devices interconnected and interlocked – Two doors

The connection, as shown below, is for two doors. Each door has one device and one lock. The interlock function must be turned on in the settings. When either door is unlocked and opened, it must be shut before the other door can be opened. This function is mainly used in banks, prisons and other places that require high security, with two doors fitted for one access route.



11.4 Two devices interconnected with anti-passback – Two doors

Install one device on door 1 under anti-passback subsidiary mode. Install one device on door 2 under anti-passback host mode. This function mainly applies for one way in and out systems. Users must present card on the subsidiary device to enter and on the host device to exit every time, to ensure the enter and exit legally. Users cannot enter or exit 2 times continuously.

12. Issue record

Site		Door location	

Card/fob number	User name	Issue date

Please note it is always best to keep a digital copy of the issue record, especially on installations with over 10 users.