PNI DK350

Access Control Keyboard

Contents

Basic Features

Fingerprint sensor.

Touch keys.

Waterproof metal housing (IP66).

Supports 1000 local users (988 common users, 2 panic users, 10 temporary users).

Supports 500 users via app.

Supports 125KHz EM card.

Alarm and buzzer output.

Anti-vandalism function.

Multiple access methods: fingerprint, card, PIN, app.

Supports temporary password (one-time or period-long).

Supports adding/deleting users via app.

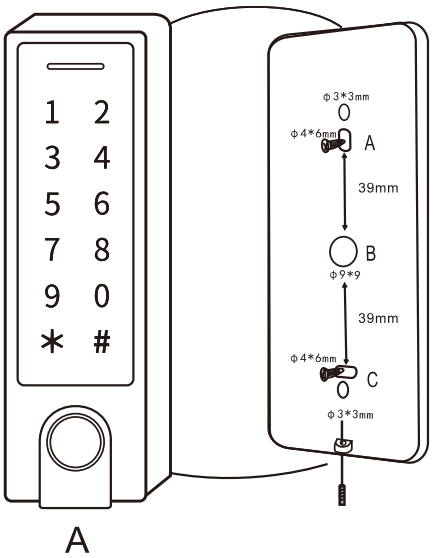
Supports setting time restrictions for users.

Technical specifications

Operating voltage	12-18V DC
Standby power	≤60mA
Operating power	≤150mA
Compatible RFID card	EM 125 KHz

RFID card reading distance	2-6 cm
Output connections	Relay, access button, alarm, door contact, Wiegand card reader
Input connections	Wiegand card reader
Relay	One ralay NO, NC, COM
Relay operation time	0-99 s. (5s. default)
Lock output load	Max. 2A
PIN output	4 bits, 10-character virtual number
Protection grade	IP66
Operating temperature	-26 ~ 80°C
Housing material	Zinc alloy
Dimensions	148 x 44 x 22 mm
Wi-Fi	2.4 GHz/100mW
Bluetooth	2.4 GHz/2.5mW

Installation



A

Remove the bracket from the back of the unit.

Fix the bracket to the wall using the screws provided.

Pass the connection cable through the hole marked B in the drawing below.

Fix the unit to the bracket.

Connections

Wire color	Function	Notes
Red	DC+	DC 12-18V input
Black	GND	DC negative pole input
Blue	NO	NO relay output (connect the diode in the package)
Purple	COM	COM relay output
Orange	NC	NC relay output (connect the diode in the package)

Yellow	OPEN	Access button input
Connections via a Wiegand reader or controller		
Green	Data 0	Wiegand output (pass-through)
White	Data 1	Wiegand output (pass-through)
Special connections		
Gray	Alarm output	Negative contact for alarm
Brown	Input	Door contact input

Audio and light warnings

Status	**LED**	**Buzzer**
Standby	Red LED	-
Entering programming mode	Red LED flashing	One beep
Programming mode	Orange LED	One beep
Operation error	-	Three beeps

Exit programming mode	Red LED	One beep
Opening the door	Green LED	One beep
Alarm	Red LED flashing quickly	Beeps

Enter and exit programming mode

Enter programming mode: *master code#

Note: the default master code is 123456.

Exit programming mode: *

Set master code

1. Enter programming mode: *master code#

2. Change master code: 0 (new master code)# (repeat new master code)#

Note: master code must contain 6 characters.

3. Exit programming mode: *

Example: change master code 123456 with 654321: *123456#0654321#654321#*

Keypad behavior: *(LED flashes red and waits for master code) 123456 # (beep/LED lights up green briefly and then red) 0 (LED lights up orange) 654321#654321# Press the “star” key to exit

programming mode.

Test the set code.

Setting the operating mode

There are 3 operating modes: standalone mode, controller mode and Wiegand reader mode. The default mode is standalone/controller mode.

1. Enter programming mode: *master code#

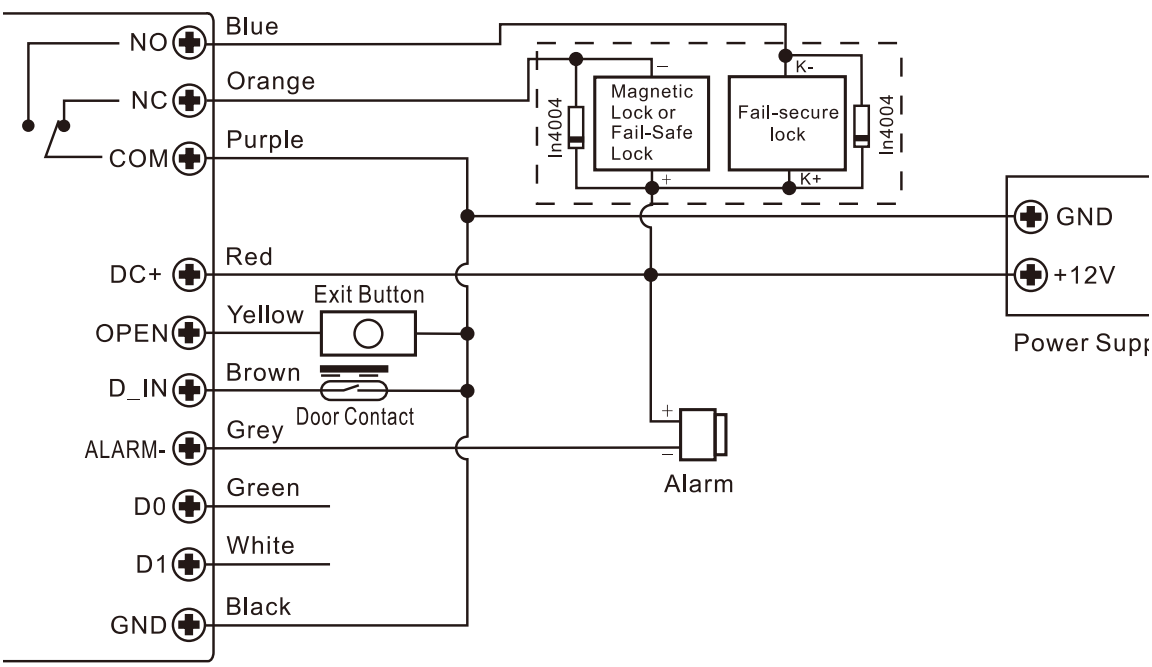
2. Enter 7 7# (default mode) or 7 8# (Wiegand mode).

3. Exit programming mode: *

1. Standalone mode

Connection diagram

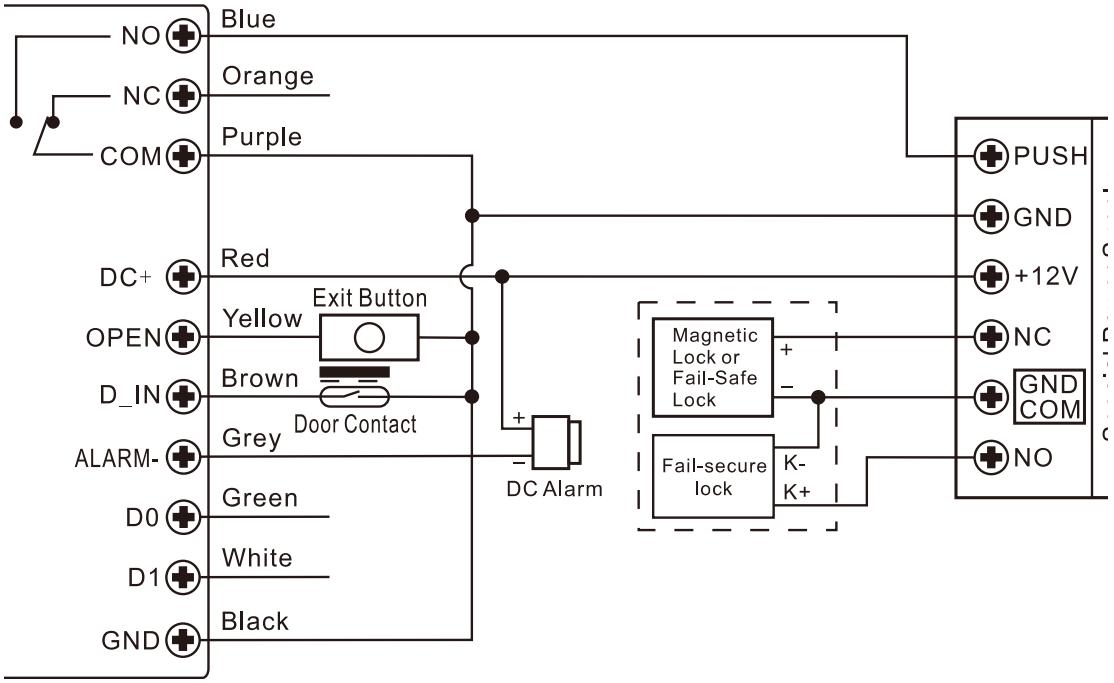
Common power supply:



Attention: it is necessary to install the included 1N4004 diode or equivalent if you are using a power supply to

which other devices are connected.

Separate power supply:



Programming

Programming differs depending on the access mode.

1. User ID: Assign a user ID for each fingerprint, PIN or access card for better management of access information.

Common User ID:

Fingerprint User ID: 0-98

PIN or card User ID: 100-987

Master User ID: 99

Panic User ID: 988-989

Visitor User ID: 990-999

Important: The user ID must not be preceded by 0

(zero). The registration of user IDs is very important. Changing a user requires knowing the user ID.

2. Card: The system only supports 125 KHz EM RFID cards.

3. PIN: Can contain 4-6 characters, except for the sequence 8888 which is reserved.

Add regular user fingerprint

1. Enter programming mode: *master code#

2.1. Add user fingerprint using automatically assigned ID: 1 (read fingerprint)(repeat fingerprint reading) (repeat fingerprint reading again)

Note: fingerprints can be added continuously.

2.2 Add user fingerprint using customized ID: 1 (user ID) # (read fingerprint) (repeat fingerprint reading) (repeat fingerprint reading again). Note: fingerprints can be added continuously.

3. Exit programming mode: *

Add regular user card

1. Enter programming mode: *master code#

2.1. Add user card using automatically assigned ID: 1 (read card or manually enter card number) #

Note: fingerprints can be added continuously.

2.2 Add user card using a personalized ID: 1 (user ID) (scan card or manually enter card number) #

2.3 Add cards in bulk: allows the Master user to add up to 888 cards in one step. The procedure takes up to 2 minutes: 1 (user ID) # (card quantity) # (manually enter the first card number) #

Notes:

1. The card quantity represents the number of cards that you want to add to the system.

2. The card numbers must be consecutive.

Add regular user PIN

1. Enter programming mode: *master code#

2.1. Add user PIN using automatically assigned ID: 1 (PIN) #

2.2 Add user PIN using customized ID: 1 (user ID) # (PIN) #

3. Exit programming mode: *

Example: add opening PIN 4321: *123456#1 4321#

Keypad behavior: *(LED flashes red and waits for master code) 123456 # (beep/LED lights up green briefly and then red) 1 (LED lights up orange) 4321# Press the “star” key to exit programming mode. Test the set code: 4321# The keypad will confirm opening. The LED will light up green.

For increased security, you can hide the PIN (max. 6 characters) by typing up to 10 characters.

For example:

If the correct PIN is: 123434

Type: **123434** or **123434, where ** can be any number from 0 to 9.

Add master user fingerprint

1. Enter programming mode: *master code#

2. Add fingerprint: 1 (99) # (read fingerprint) (repeat fingerprint reading) (repeat fingerprint reading again)

3. Exit programming mode: *

Add panic user

1. Enter programming mode: *master code#

2.1. Add card: 1 (user ID) # (read card or manually enter card number) #

2.2 Add PIN: 1 (user ID) # (PIN) #

3. Exit programming mode: *

Add visitor user

A maximum of 10 visitors can be added with PIN or card. Visitors can use the PIN or card a maximum of 10 times. After a maximum of 10 uses, the PIN or card will automatically become invalid.

1. Enter programming mode: *master code#

2.1. Add card: 1 (user ID) # (0~9) # (read card or manually enter card number) #

2.2 Add PIN: 1 (user ID) # (0~9) # (PIN) #

3. Exit programming mode: *

Delete user

1. Enter programming mode: *master code#

2.1. Delete user by fingerprint, card or PIN: 2 (read fingerprint/read card/enter PIN) #

2.2 Delete user by ID number: 2 (user ID) #

2.3 Delete user by card number: 2 (enter card number) #

2.4. Delete all users: 2 (master code) #

3. Exit programming mode: *

Relay activation mode configuration

The relay configuration influences its behavior after entering the access code.

1. Enter programming mode: *master code#

2.1. Impulse mode (default mode): 3 (1~99) #

The relay is activated for a period of time between 0-99 seconds (default 5 seconds) after entering the code, then it deactivates automatically.

The relay activation time is 1-99 seconds. Default: 5 seconds.

2.2. Alternating mode: 3 0 #

The relay changes its state each time the code is entered correctly:

If it is off (open), it activates (closes the contact). If it is activated, it deactivates.

Useful for gates or doors that must remain open until they are manually closed again.

3. Exit programming mode: *

Access mode setting

For multi-user access mode, the time interval in which the access codes are read should not exceed 5 seconds. After 5 seconds, the unit automatically enters standby.

1. Enter programming mode: *master code#

2.1. Fingerprint access: 4 0 #

2.2. Card access: 4 1 #

2.3. PIN access: 4 2 #

2. 4. Multi-user access: 4 3 (2~9) #

Only after 2~9 users are validated, the door will open.

2.5. Fingerprint or Card or PIN (default): 4 4 #

3. Exit programming mode: *

Alarm for repeated failed attempts

Refers to an alarm that is activated after a consecutive number of 10 incorrect access attempts (inputting a wrong code, invalid card, etc.). It can be set to deny access for 10 minutes or to allow access only after entering a valid code or card or fingerprint.

1. Enter programming mode: *master code#

2.1. Function disabled (default): 6 0 #

2.2. Function enabled: 6 1 # (access will be prohibited for 10 minutes)

2.3. Function enabled (Alarm): 6 2 #

Alarm duration setting: 5 (0~3) #. Default 1 minute.

To stop the alarm, enter the master code # or scan the master fingerprint/card or enter the PIN or scan a user fingerprint/card.

3. Exit the programming mode: *

Door open warning

If you have connected a wired magnetic door contact to the access control keypad and the door remains open for more than 1 minute, the built-in buzzer will sound to remind the user to close the door. The sound can be stopped by closing the door or entering a valid access code (master or user). Otherwise, the sound will continue as long as it is set.

Forced door warning

If you have connected a wired magnetic door contact to the access control keypad and the door is forced open, the built-in buzzer and external siren (if any) will sound the alarm. The sound can be stopped by closing the door or entering a valid access code (master or user). Otherwise, the sound will continue as long as it is set.

1. Enter programming mode: *master code#

2.1. Function disabled (default): 6 3 #

2.2. Function enabled” 6 4 #

Set alarm duration: 5 (0~3) #. Default 1 minute.

3. Exit programming mode: *

Buzzer and LED Setting

1. Enter programming mode: *master code#

2.1. Disable buzzer: 7 0 #

2.2. Enable buzzer (default): 7 1 #

3.1. LED off: 7 2 #

3.2. LED on (default): 7 3 #

4.1. Keypad light off: 7 4 #

4.2. Keypad light on all the time: 7 5 #

4.3. Keypad light off automatically (default): 7 6 #. After 20 seconds from the last operation, the keypad turns off automatically. By touching any key, the keypad lights up.

3. Exit programming mode: *

Adding user fingerprint/card/PIN with master card/fingerprint

1. Read the master card/fingerprint.

2. Scan the user’s fingerprint 3 times or scan the user’s card or PIN #

Repeat step 2 to add more users consecutively.

3. Scan the master card/fingerprint again.

Deleting a user's fingerprint/card/PIN with a master card/fingerprint

1. Scan the master card/fingerprint twice within a maximum of 5 seconds.

2. Scan the fingerprint/card or enter the user's PIN #

Repeat step 2 to delete more users consecutively.

3. Scan the master card/fingerprint again.

Reset and add a master card

If you have connected an access button to the access control keypad, proceed as follows to reset the keypad:

1. Turn off the power.

2. Press and hold the access button while turning the power back on.

3. 2 beeps will be heard.

4. Remove your finger from the access button.

5. The yellow LED lights up.

6. Read any 125KHz EM card.

7. The LED lights up red.

8. The keypad has been reset.

9. The read card has become the master card.

Notes:

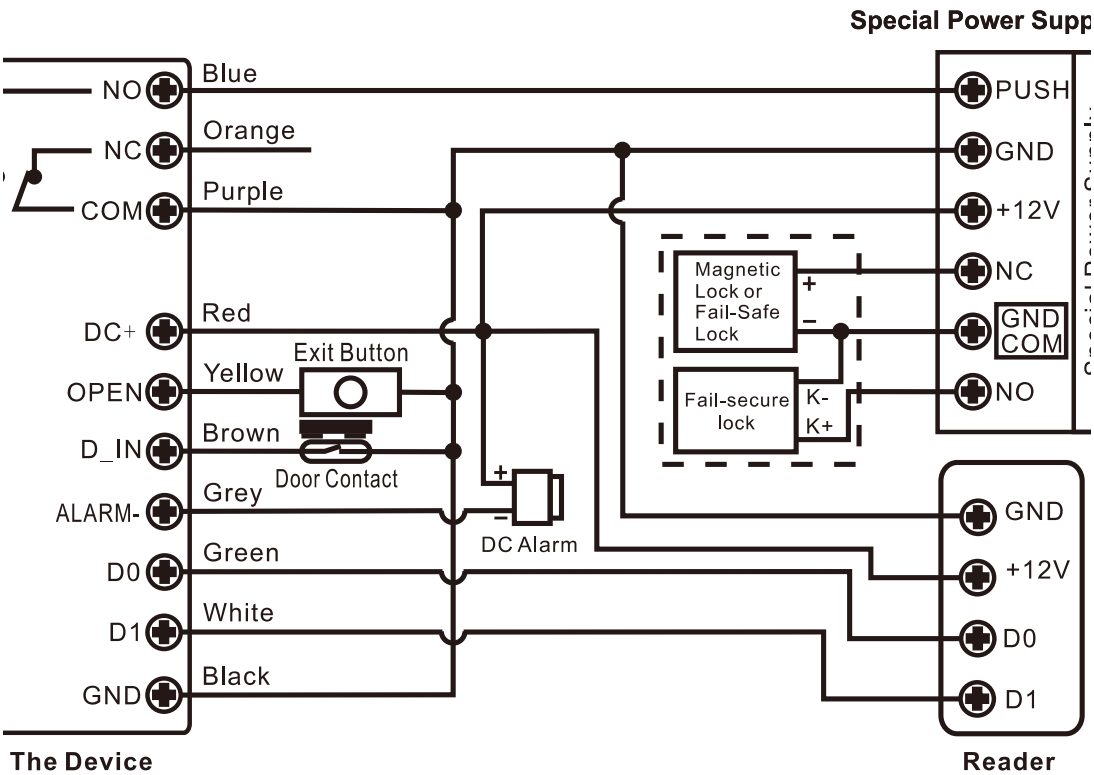
1. If you do not want to add a master card, you must hold down the access button for at least 5 seconds before releasing it. This procedure will invalidate the former master card.

2. By resetting, the user information will not be deleted.

2. Controller Mode

The keyboard will operate as a controller if connected to a Wiegand reader.

Connection Diagram



Attention: it is necessary to install the included 1N4004 diode or equivalent if you use a power supply to which other devices are connected.

Wiegand input format setting

1. Enter programming mode: *master code#

2. Set Wiegand input bits for EM card:

8 (26~44) # (default 26bits)

3.1. Disable parity bit: 8 0 #

3.2. Enable parity bit: 8 1 #

3. Exit programming mode: *

Programming

The basic programming is the same as in standalone mode.

Connecting to an external card reader

In case of an EM or Mifare card reader, users can be added/deleted on both the keypad and the external reader.

In case of an HID card reader, users can be added/deleted only on the external reader.

Connecting to a fingerprint reader

Connect the fingerprint reader to the keypad.

1. Enter programming mode: *master code#

2.1. Type 1 (read the fingerprint on the fingerprint reader) #. The ID is automatically assigned.

2.2. Type 1 (user ID) # (read the fingerprint on the fingerprint reader) #

3. Exit programming mode: *

Connecting to a keypad reader

The keypad reader can be 4 Bits, 8 Bits (ASCII) or 10 Bits.

1. Enter programming mode: *master code#

2.1. Enter the number of bits: 8 (4 or 8 or 10) #. The default is 4 Bits.

3. Exit programming mode: *

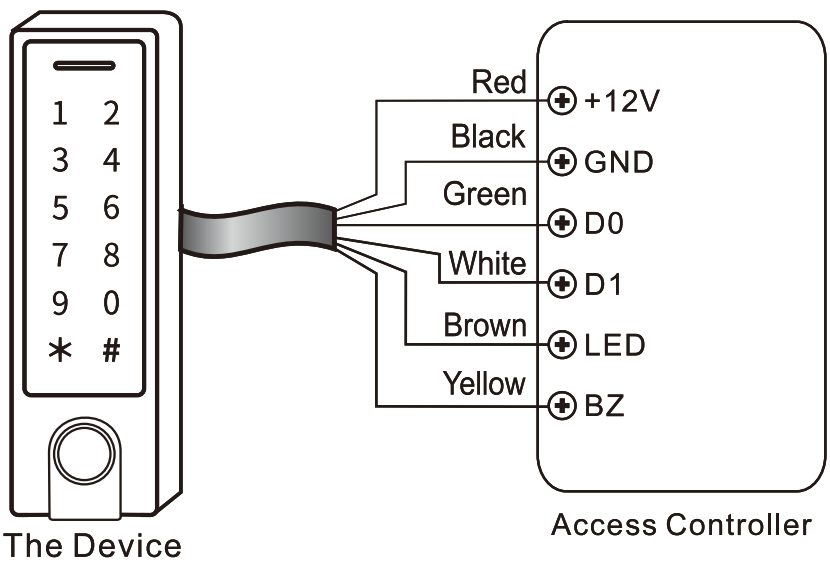
Add/Delete User PIN

User PIN can be added/deleted on both the access control keypad and the external keypad reader.

3. Wiegand reader mode

The keyboard can also operate as a standard Wiegand reader connected to an external controller.

Connection diagram



When the keypad is in Wiegand reader mode, all settings made in Controller mode become invalid. The big and yellow wires will be redefined as follows:

Brown wire: Green LED control

Yellow wire: Buzzer control.

Wiegand output format setting

1. Enter programming mode: *master code#

2. Set Wiegand bits for EM card: 8 (26~44) #

3.1. Disable parity bit: 8 0 #

3.2. Enable parity bit: 8 1 # (default)

3. Exit programming mode: *

Note: to connect a Wiegand controller, you need to disable parity bit.

All card access

After activating this mode, all cards can open the door. At the same time, the card is added to the system.

1. Enter programming mode: *master code#

2.1. Disable function: 9 2 # (default)

2.2. Enable function: 9 3 #

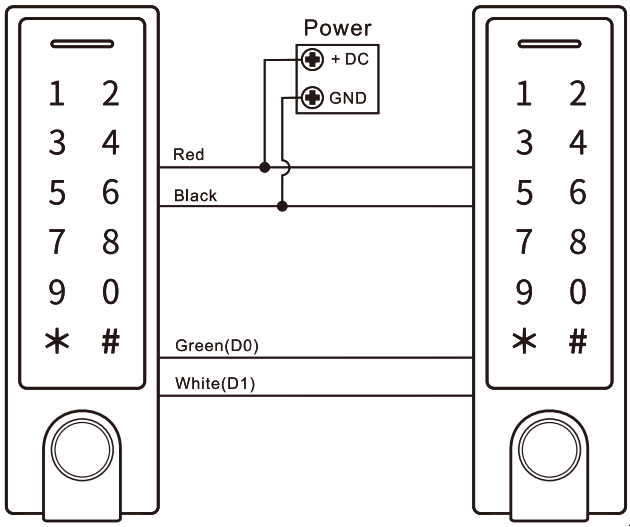
3. Exit programming mode: *

Transfer user information

For users registered with PIN/card.

User information can be transferred from one keypad to another.

Connection diagram



Notes:

Both keypads must be from the same series.

The master code of both keypads must be identical.

Activate the transfer function only on the main keypad (master keypad).

If the secondary keypad already has registered users, they will be overwritten during the transfer.

For a number of 900 users, the transfer could take up to 30 seconds.

Activate transfer mode on the master keypad

1. Enter the programming mode: *master code#

2. Type 9 8 #

For 30 seconds, the maximum transfer duration, the green LED is on. When the data transfer is finished, a

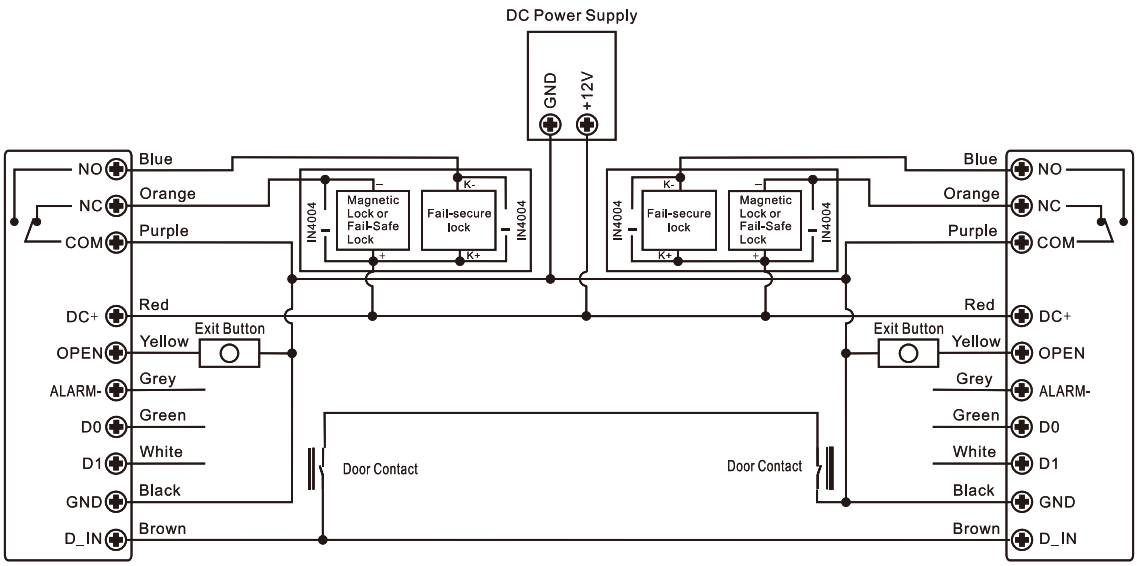
beep is heard and the red LED lights up.

3. Exit the programming mode: *

Interconnecting keypads

This mode means interconnecting two keypads to control two doors. The function is especially useful in prisons, banks and other locations where a higher level of security is required.

Connection diagram



Register users on keypad A, then transfer them to keypad B.

Enable Interlock mode on both keypads:

1. Enter programming mode: *master code#

2.1. Disable function: 9 0 # (default)

2.2. Enable function: 9 1 #

3. Exit programming mode: *

When the function is active, when door 2 needs to stay

closed, the user can scan the fingerprint/card or enter the PIN on keypad A. Door 1 will open. When door 1 needs to stay closed, the user can scan the fingerprint/card or enter the PIN on keypad B. Door 2 will open.

When the function is active, the user can scan the fingerprint/card or enter the PIN on keypad A to open door 1. Or scan the fingerprint/card or enter the PIN on keypad B to open door 2.

Keyboard control from Tuya Smart app

Note: Due to frequent updates of the Tuya Smart app, the images and information presented in this manual may differ from those in the version installed on your device.

Accesati Google Play sau App Store sau scanati codul QR de mai jos si instalati aplicatia Tuya Smart.

Connect your phone to the WiFi network, activate Location and Bluetooth.

Open the app and log in.

Press “+“ - “Add device“.

The app will automatically identify your device.

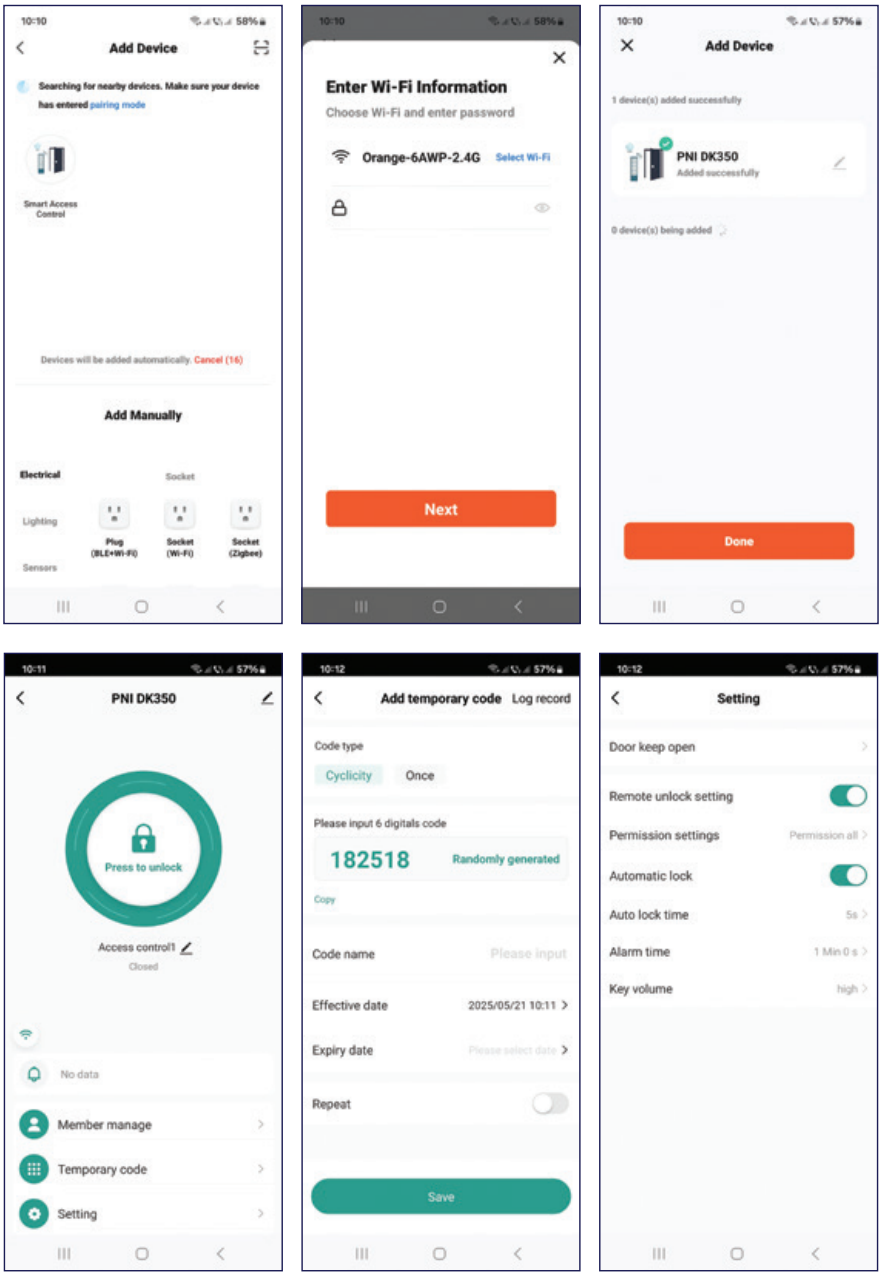
Press the keyboard icon and follow the on-screen steps.

Note: you can also manually add the keyboard to the

app by accessing the Cameras & Lock - Lock (Wi-Fi) category.

Reset WiFi

* master code # 9 master code #



The application allows you to unlock the door, add and manage users, and generate a temporary access code.

Основни характеристики

Сензор за пръстови отпечатъци.

Сензорни бутони.

Водоустойчив метален корпус (IP66).

Поддържа 1000 локални потребители (988 обикновени потребители, 2 потребители за паника, 10 временни потребители).

Поддържа 500 потребители чрез приложение. Поддържа 125KHz EM карта.

Изход за аларма и зумер.

Функция против вандализъм. Множество методи за достъп: пръстов отпечатък, карта, ПИН, приложение.

Поддържа временна парола (еднократна или за период от време).

Поддържа добавяне/изтриване на потребители чрез приложение.

Поддържа задаване на времеви ограничения за потребителите.

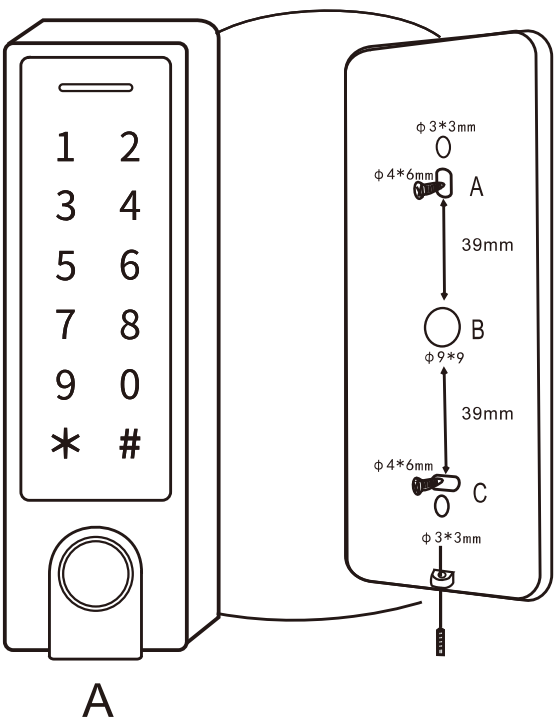
Технически спецификации

Работно напрежение	12-18V DC
Мощност в режим на готовност	≤60mA

Работна мощност	≤150mA
Съвместима RFID карта	EM 125 KHz
Разстояние на четене на RFID карта	2-6 cm
Изходни връзки	Реле, бутон за достъп, аларма, контакт за врата, четец на карти Wiegand
Входни връзки	Четец на карти Wiegand
Реле	Едно реле NO, NC, COM
Време за работа на релето	0-99 сек. (5 сек. по подразбиране)
Натоварване на изхода за заключване	Макс. 2A
ПИН изход	4 бита, 10-символен виртуален номер
Степен на защита	IP66
Работна температура	-26 ~ 80°C

Материал на корпуса	Цинкова сплав
Размери	148 x 44 x 22 mm
Wi-Fi	2.4 GHz/100mW
Bluetooth	2.4 GHz/2.5mW

Инсталация



A

Отстранете скобата от задната страна на устройството. Фиксирайте скобата към стената с помощта на предоставените винтове. Прекарайте свързващия кабел през отвора, маркиран с B на чертежа по-долу. Фиксирайте устройството към скобата.

Свързване на проводници

Цвят	**Функция**	**Бележки**
Червено	DC+	DC вход 12-18V

Черен	GND	DC вход с отрицателен полюс
Син	NO	NO релеен изход (свържете диода в опаковката)
Лилаво	COM	COM релеен изход
Оранжево	NC	NC релеен изход (свържете диода в опаковката)
Жълто	OPEN	Вход за бутон за достъп
Връзки чрез Wiegand четец или контролер		
Зелено	Data 0	Wiegand изход (pass-through)
Бяло	Data 1	Wiegand изход (pass-through)
Специални връзки		
Сиво	Изход за аларма	Отрицателен контакт за аларма
Кафяво	Вход	Вход за контакт на вратата

Звукови и светлинни предупреждения

Състояние	**LED**	**Buzzer**
В готовност	Червен светодиод	-
Влизане в режим на програмиране	Червен светодиод мига	Едно бипкане
Режим на програмиране	Оранжев светодиод	Едно бипкане
Грешка в работата	-	Три бипкания
Изход от режим на програмиране	Червен светодиод	Едно бипкане
Отваряне на вратата	Зелен светодиод	Едно бипкане
Аларма	Червеният светодиод мига бързо	Beeps

Влизане и излизане от режим на програмиране

Влизане в режим на програмиране: * мастер код

#

Забележка: главният код по подразбиране е 123456.

Излизане от режим на програмиране: *

Задаване на мастер код

1. Влезте в режим на програмиране: * мастер код #

2. Промяна на мастер кода: 0 (нов мастер код)# (повторете новия мастер код)#

Забележка: мастер кодът трябва да съдържа 6 знака.

3. Излезте от режим на програмиране: *

Настройка на режима на работа

Има 3 режима на работа: самостоятелен режим, режим на контролер и режим на Wiegand четец. Режимът по подразбиране е самостоятелен/контролер.

1. Влезте в режим на програмиране: * мастер код #

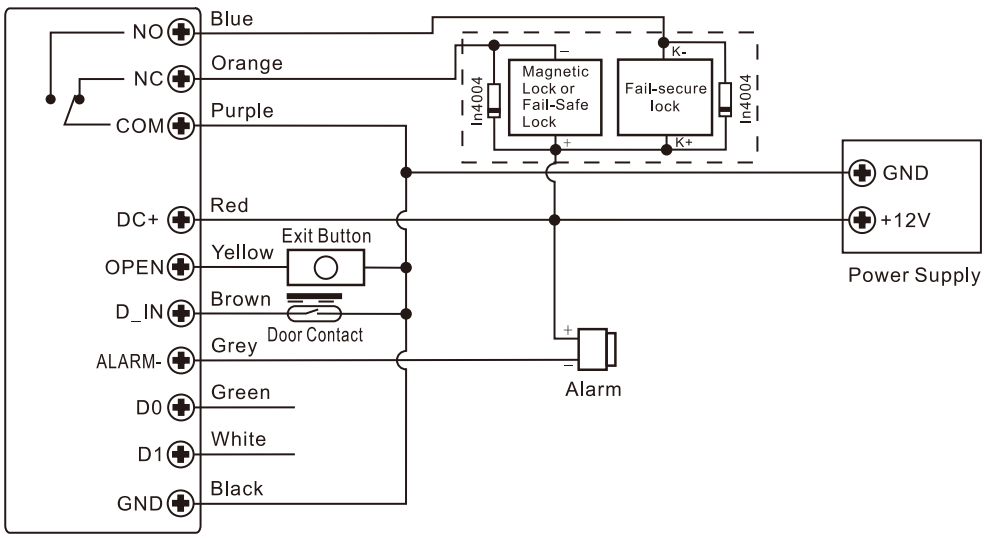
2. Въведете 7 7# (режим по подразбиране) или 7 8# (режим Wiegand).

3. Излезте от режим на програмиране: *

1. Самостоятелен режим

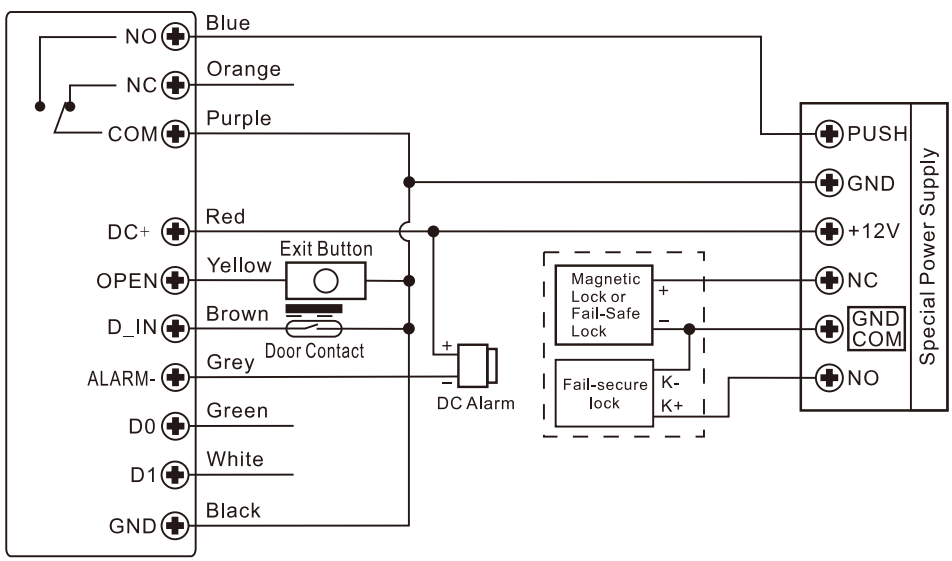
Схема на свързване

Общо захранване:



Внимание: необходимо е да инсталирате включения диод 1N4004 или еквивалентен, ако използвате захранване, към което са свързани други устройства.

Отделно захранване:



Програмиране

Програмирането се различава в зависимост от режима на достъп.

Бележки:

1. Потребителски ID: Задайте потребителски ID за всеки пръстов отпечатък, ПИН или карта за достъп за по-добро управление на информацията за достъп.

Общ потребителски ID:

Потребителски ID с пръстов отпечатък: 0-98

Потребителски ID с ПИН или карта: 100-987

Главен потребителски ID: 99

Паник потребителски ID: 988-989

Потребителски ID за посетители: 990-999

Важно: Потребителският ID не трябва да се предшества от 0 (нула). Регистрацията на потребителски ID е много важна. Промяната на потребител изисква познаване на потребителския ID.

2. Карта: Системата поддържа само 125 KHz EM RFID карти.

3. ПИН: Може да съдържа 4-6 знака, с изключение на последователността 8888, която е запазена.

Добавяне на пръстов отпечатък на обикновен потребител

1. Влезте в режим на програмиране: * мастер код #

2.1. Добавете пръстов отпечатък на потребител, използвайки автоматично зададен идентификатор: 1 (четене на пръстов отпечатък) (повторете отчитането на пръстов отпечатък) (повторете отчитането на пръстов отпечатък отново)

Забележка: пръстовите отпечатъци могат да се добавят непрекъснато.

2.2 Добавяне на пръстов отпечатък на потребител, използвайки персонализиран идентификатор: 1 (потребителски идентификатор) # (четене на пръстов отпечатък) (повторете отчитането на пръстов отпечатък) (повторете отчитането на пръстов отпечатък отново). Забележка: пръстовите отпечатъци могат да се добавят непрекъснато.

3. Излезте от режим на програмиране: *

Добавяне на карта на обикновен потребител

1. Влезте в режим на програмиране: * мастер код #

2.1. Добавяне на карта на потребител, използвайки

автоматично зададен идентификатор: 1 (прочетете картата или въведете ръчно номера на картата) #

Забележка: пръстовите отпечатъци могат да се добавят непрекъснато.

2.2 Добавяне на карта на потребител, използвайки персонализиран идентификатор: 1 (идентификатор на потребителя) (сканирайте картата или въведете ръчно номера на картата) #

2.3 Добавяне на карти наведнъж: позволява на главния потребител да добави до 888 карти наведнъж. Процедурата отнема до 2 минути: 1 (идентификатор на потребителя) # (брой карти) # (ръчно въведете първия номер на картата) #

Забележки:

1. Броят карти представлява броя карти, които искате да добавите към системата.

2. Номерата на картите трябва да са последователни.

Добавяне на обикновен потребителски ПИН

1. Влезте в режим на програмиране: * мастер код #

2.1. Добавете потребителски ПИН, използвайки автоматично зададен идентификатор: 1 (ПИН) #

2.2 Добавяне на потребителски ПИН, използвайки персонализиран идентификатор: 1 (Потребителски идентификатор) # (ПИН) #

3. Излезте от режим на програмиране: *

За повишена сигурност можете да скриете ПИН кода (макс. 6 знака), като въведете до 10 знака.

Например:

Ако правилният ПИН е: 123434

Въведете: **123434** или **123434, където ** може да бъде всяко число от 0 до 9.

Добавяне на пръстов отпечатък на главен потребител

1. Влезте в режим на програмиране: * мастер код #

2. Добавяне на пръстов отпечатък: 1 (99) # (прочетете пръстов отпечатък) (повторете отчитането на пръстов отпечатък) (повторете отчитането на пръстов отпечатък отново)

3. Излезте от режим на програмиране: *

Добавяне на паник потребител

1. Влезте в режим на програмиране: * мастер код #

2.1. Добавяне на карта: 1 (потребителски ID) # (прочетете картата или въведете ръчно номера

на картата) #

2.2 Добавяне на ПИН: 1 (потребителски ID) # (ПИН) #

3. Излезте от режим на програмиране: *

Добавяне на посетител потребител

Могат да бъдат добавени максимум 10 посетители с ПИН или карта. Посетителите могат да използват ПИН или картата максимум 10 пъти. След максимум 10 употреби, ПИН или картата автоматично ще станат невалидни.

1. Влезте в режим на програмиране: * мастер код #

2.1. Добавяне на карта: 1 (ID на потребител) # (0~9) # (прочетете картата или въведете ръчно номера на картата) #

2.2 Добавяне на ПИН: 1 (ID на потребител) # (0~9) # (ПИН) #

3. Изход от режим на програмиране: *

Изтриване на потребител

1. Влизане в режим на програмиране: * мастер код #

2.1. Изтриване на потребител по пръстов отпечатък, карта или ПИН: 2 (прочетете пръстов отпечатък/прочетете картата/въведете ПИН) #

2.2 Изтриване на потребител по ID номер: 2 (ID на потребител) #

2.3 Изтриване на потребител по номер на карта: 2 (въведете номера на картата) #

2.4. Изтриване на всички потребители: 2 (главен код) #

3. Изход от режим на програмиране: *

Конфигурация на режима на активиране на релето

Конфигурацията на релето влияе върху поведението му след въвеждане на кода за достъп.

1. Влезте в режим на програмиране: * мастер код #

2.1. Импулсен режим (режим по подразбиране): 3 (1~99) #

Релето се активира за период от време между 0-99 секунди (по подразбиране 5 секунди) след въвеждане на кода, след което се деактивира автоматично.

Времето за активиране на релето е 1-99 секунди. По подразбиране: 5 секунди.

2.2. Алтернативен режим: 3 0 #

Релето променя състоянието си всеки път, когато кодът е въведен правилно:

Ако е изключено (отворено), то се активира

(затваря контакта). Ако е активирано, то се деактивира.

Полезно за порти или врати, които трябва да останат отворени, докато не бъдат затворени отново ръчно.

3. Излезте от режим на програмиране: *

Настройка на режима на достъп

За режим на достъп за много потребители, интервалът от време, в който се четат кодовете за достъп, не трябва да надвишава 5 секунди. След 5 секунди устройството автоматично влиза в режим на готовност.

1. Влезте в режим на програмиране: * мастер код #

2.1. Достъп с пръстов отпечатък: 4 0 #

2.2. Достъп с карта: 4 1 #

2.3. Достъп с ПИН: 4 2 #

2. 4. Достъп за множество потребители: 4 3 (2~9) #

Само след като 2~9 потребители бъдат валидирани, вратата ще се отвори.

2.5. Пръстов отпечатък, карта или ПИН (по подразбиране): 4 4 #

3. Излезте от режим на програмиране: *

Аларма за многократни неуспешни опити

Отнася се за аларма, която се активира след последователни 10 неправилни опита за достъп (въвеждане на грешен код, невалидна карта и др.). Може да се настрои да откаже достъп за 10 минути или да разреши достъп само след въвеждане на валиден код, карта или пръстов отпечатък.

1. Влезте в режим на програмиране: * мастер код #

2.1. Функция деактивирана (по подразбиране): 6 0 #

2.2. Функция активирана: 6 1 # (достъпът ще бъде забранен за 10 минути)

2.3. Функция активирана (Аларма): 6 2 #

Настройка на продължителността на алармата: 5 (0~3) #. По подразбиране 1 минута.

За да спрете алармата, въведете главния код # или сканирайте главния пръстов отпечатък/картата, или въведете ПИН кода, или сканирайте потребителски пръстов отпечатък/карта.

3. Излезте от режим на програмиране: *

Предупреждение за отворена врата

Ако сте свързали кабелен магнитен контакт за врата към клавиатурата за контрол на достъпа и вратата остане отворена за повече от 1 минута,

вграденият зумер ще прозвучи, за да напомни на потребителя да затвори вратата. Звукът може да бъде спрян чрез затваряне на вратата или въвеждане на валиден код за достъп (главен или потребителски). В противен случай звукът ще продължи, докато е зададен.

Предупреждение за насилствено отваряне на врата

Ако сте свързали кабелен магнитен контакт за врата към клавиатурата за контрол на достъпа и вратата е насилствено отворена, вграденият зумер и външната сирена (ако има такава) ще задействат алармата. Звукът може да бъде спрян чрез затваряне на вратата или въвеждане на валиден код за достъп (главен или потребителски). В противен случай звукът ще продължи, докато е зададен.

1. Влезте в режим на програмиране: * мастер код #

2.1. Функцията е деактивирана (по подразбиране): 6 3 #

2.2. „Функция активирана“ 6 4 #

Задаване на продължителност на алармата: 5 (0~3) #. По подразбиране 1 минута.

3. Изход от режим на програмиране: *

Настройка на зумера и светодиода

1. Влизане в режим на програмиране: * мастер код #

2.1. Деактивиране на зумера: 7 0 #

2.2. Активиране на зумера (по подразбиране): 7 1 #

3.1. Изключен светодиод: 7 2 #

3.2. Включен светодиод (по подразбиране): 7 3 #

4.1. Изключена светлина на клавиатурата: 7 4 #

4.2. Светлината на клавиатурата е включена постоянно: 7 5 #

4.3. Автоматично изключване на светлината на клавиатурата (по подразбиране): 7 6 #. 20 секунди след последната операция клавиатурата се изключва автоматично. При докосване на произволен клавиш, клавиатурата светва.

3. Изход от режим на програмиране: *

Добавяне на потребителски пръстов отпечатък/карта/ПИН с мастер карта/ пръстов отпечатък

1. Прочетете мастер картата/пръстовия отпечатък.

2. Сканирайте пръстовия отпечатък на потребителя 3 пъти или сканирайте картата или ПИН кода на потребителя.

Повторете стъпка 2, за да добавите още потребители последователно.

3. Сканирайте отново мастер картата/пръстовия отпечатък.

Изтриване на потребителски пръстов отпечатък/карта/ПИН с мастер карта/ пръстов отпечатък

1. Сканирайте мастер картата/пръстовия отпечатък два пъти в рамките на максимум 5 секунди.

2. Сканирайте пръстовия отпечатък/картата или въведете ПИН кода на потребителя.

Повторете стъпка 2, за да изтриете още потребители последователно.

3. Сканирайте отново мастер картата/пръстовия отпечатък.

Нулиране и добавяне на мастер карта

Ако сте свързали бутон за достъп към клавиатурата за контрол на достъпа, продължете както следва, за да нулирате клавиатурата:

1. Изключете захранването.

2. Натиснете и задръжте бутона за достъп, докато включвате захранването отново.

3. Ще се чуят 2 звукови сигнала.

4. Махнете пръста си от бутона за достъп.

5. Жълтият светодиод светва.

6. Прочетете всяка 125KHz EM карта.

7. Светодиодът светва червено.

8. Клавиатурата е нулирана.

9. Прочетената карта е станала главна карта.

Бележки:

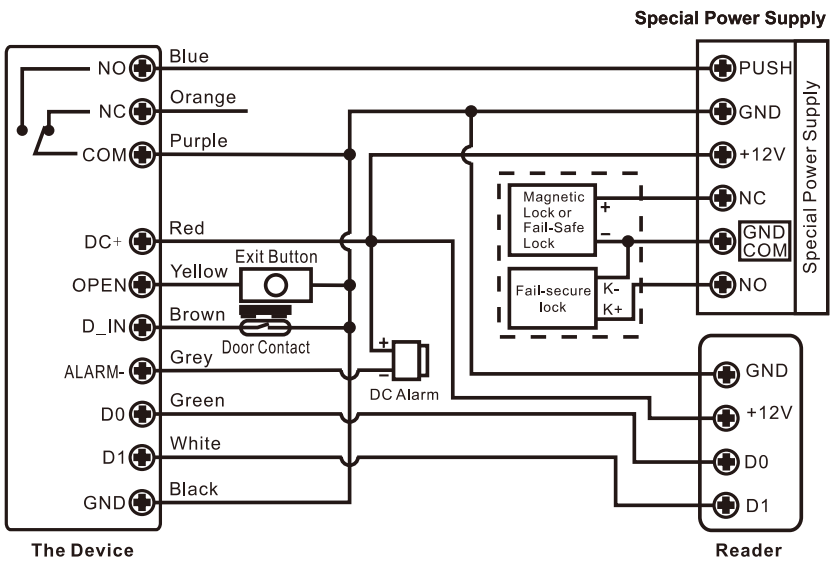
1. Ако не искате да добавяте главна карта, трябва да задържите бутона за достъп поне 5 секунди, преди да го освободите. Тази процедура ще анулира предишната главна карта.

2. Чрез нулиране, потребителската информация няма да бъде изтрита.

2. Режим на контролер

Клавиатурата ще работи като контролер, ако е свързана към Wiegand четец.

Диаграма на свързване



Внимание: необходимо е да инсталирате включения диод 1N4004 или еквивалентен, ако използвате захранване, към което са свързани други устройства.

Настройка на входния формат на Wiegand

1. Влезте в режим на програмиране: * мастер код #

2. Задайте входните битове на Wiegand за EM карта:

8 (26~44) # (по подразбиране 26 бита)

3.1. Деактивирайте бита за паритет: 8 0 #

3.2. Активирайте бита за паритет: 8 1 #

3. Излезте от режим на програмиране: *

Програмиране

Основно програмиране е същото като в самостоятелен режим.

Свързване към външен четец на карти

В случай на четец на EM или Mifare карти, потребители могат да бъдат добавяни/изтривани както на клавиатурата, така и на външния четец.

В случай на четец на HID карти, потребители могат да бъдат добавяни/изтривани само на външния четец.

Свързване към четец на пръстови отпечатъци

Свържете четеца на пръстови отпечатъци към клавиатурата.

1. Влезте в режим на програмиране: * мастер код #

2.1. Въведете 1 (прочетете пръстовия отпечатък на четеца на пръстови отпечатъци) #. Идентификаторът се задава автоматично.

2.2. Въведете 1 (потребителски ID) # (прочетете пръстовия отпечатък на четеца на пръстови отпечатъци) #

3. Излезте от режим на програмиране: *

Свързване към четец на клавиатура

Четецът на клавиатура може да бъде 4-битов, 8-битов (ASCII) или 10-битов.

1. Влезте в режим на програмиране: * мастер код #

2.1. Въведете броя битове: 8 (4 или 8 или 10) #. Стойността по подразбиране е 4 бита.

3. Излезте от режим на програмиране: *

Добавяне/Изтриване на потребителски ПИН

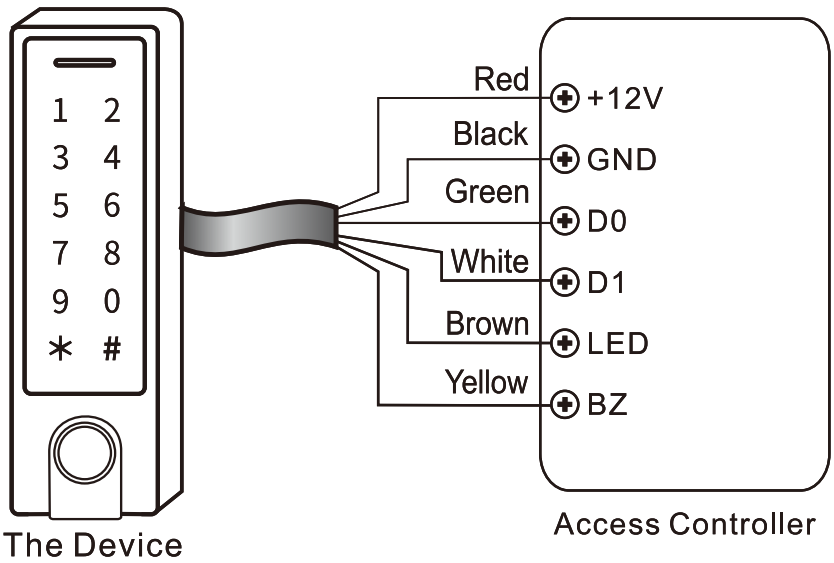
Потребителският ПИН може да бъде добавян/изтриван както на клавиатурата за контрол на

достъпа, така и на външния четец на клавиатура.

3. Режим на Wiegand четец

Клавиатурата може да работи и като стандартен Wiegand четец, свързан към външен контролер.

Диаграма на свързване



Когато клавиатурата е в режим Wiegand четец, всички настройки, направени в режим Контролер, стават невалидни. Големият и жълтият проводник ще бъдат предефинирани, както следва:

Кафяв проводник: Управление на зелен светодиод

Жълт проводник: Управление на зумер.

Настройка на Wiegand изходния формат

1. Влезте в режим на програмиране: * мастер код #

2. Задайте Wiegand битове за EM карта: 8 (26~44) #

3.1. Деактивирайте бита за паритет: 8 0 #

3.2. Активирайте бита за паритет: 8 1 # (по подразбиране)

3. Излезте от режим на програмиране: *

Забележка: за да свържете Wiegand контролер, трябва да деактивирате бита за паритет.

Разширени приложения

Достъп с всички карти

След активиране на този режим, всички карти могат да отварят вратата. Едновременно с това картата се добавя към системата.

1. Влезте в режим на програмиране: * мастер код #

2.1. Деактивиране на функцията: 9 2 # (по подразбиране)

2.2. Активиране на функцията: 9 3 #

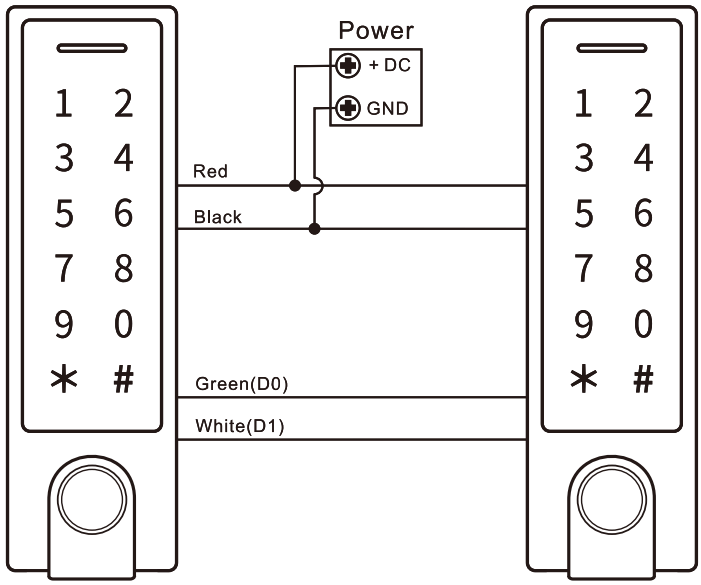
3. Излезте от режим на програмиране: *

Прехвърляне на потребителска информация

За потребители, регистрирани с ПИН/карта.

Потребителска информация може да се прехвърля от една клавиатура на друга.

Диаграма на свързване



Бележки:

И двете клавиатури трябва да са от една и съща серия.

Главният код на двете клавиатури трябва да е идентичен.

Активирайте функцията за прехвърляне само на основната клавиатура (главна клавиатура).

Ако вторичната клавиатура вече има регистрирани потребители, те ще бъдат презаписани по време на прехвърлянето.

За 900 потребители, прехвърлянето може да отнеме до 30 секунди.

Активиране на режим на прехвърляне на главната клавиатура

1. Влезте в режим на програмиране: * мастер код #

2. Въведете 9 8 #

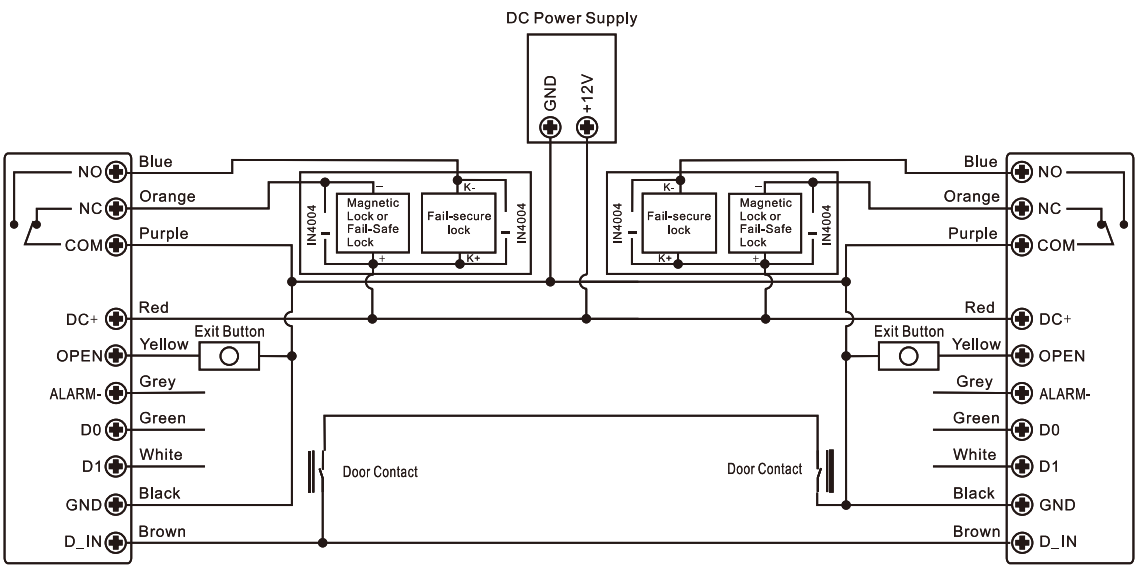
За 30 секунди, максималната продължителност на прехвърлянето, зеленият светодиод свети. Когато прехвърлянето на данни приключи, се чува звуков сигнал и червеният светодиод светва.

3. Излезте от режим на програмиране: *

Свързване на клавиатури

Този режим означава свързване на две клавиатури за управление на две врати. Функцията е особено полезна в затвори, банки и други места, където се изисква по-високо ниво на сигурност.

Диаграма на свързване



Регистрирайте потребители на клавиатура A, след което ги прехвърлете към клавиатура B.

Активиране на режим на блокиране и на двете клавиатури:

1. Влезте в режим на програмиране: * мастер код

#

2.1. Деактивиране на функцията: 9 0 # (по подразбиране)

2.2. Активиране на функцията: 9 1 #

3. Излезте от режим на програмиране: *

Когато функцията е активна, когато врата 2 трябва да остане затворена, потребителят може да сканира пръстовия си отпечатък/картата или да въведе ПИН кода на клавиатура A. Врата 1 ще се отвори. Когато врата 1 трябва да остане затворена, потребителят може да сканира пръстовия си отпечатък/картата или да въведе ПИН кода на клавиатура B. Врата 2 ще се отвори.

Когато функцията е активна, потребителят може да сканира пръстовия си отпечатък/картата или да въведе ПИН кода на клавиатура A, за да отвори врата 1. Или да сканира пръстовия си отпечатък/картата или да въведе ПИН кода на клавиатура B, за да отвори врата 2.

Управление с клавиатура от приложението Tuya Smart

Забележка: Поради честите актуализации на приложението Tuya Smart, изображенията и информацията, представени в това ръководство, може да се различават от тези във версията, инсталирана на вашето устройство.

Отидете в Google Play или App Store или сканирайте QR кода по-долу и инсталирайте приложението Tuya Smart.

Свържете телефона си към WiFi мрежата, активирайте „Местоположение“ и Bluetooth.

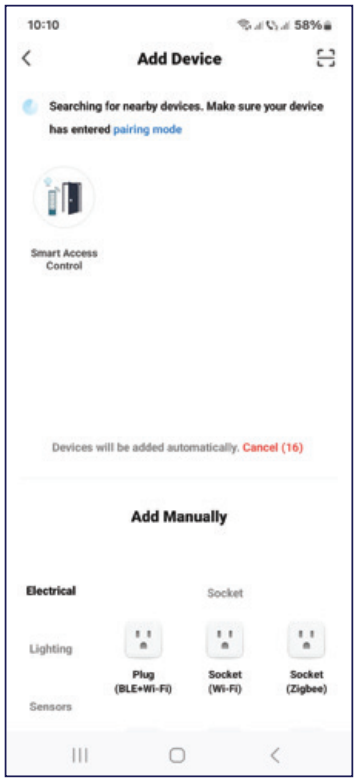
Отворете приложението и влезте.

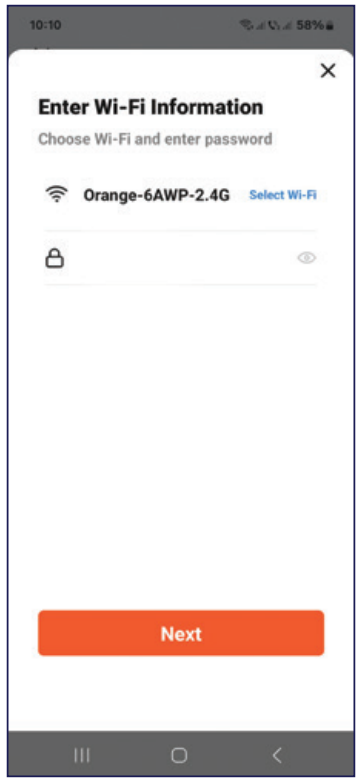
Натиснете „+“ - „Добавяне на устройство“.

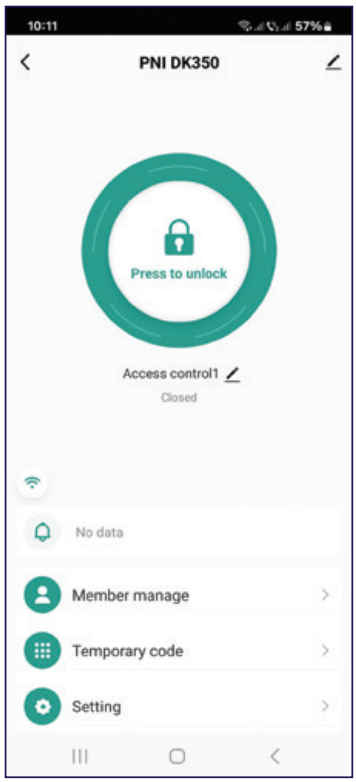
Приложението автоматично ще разпознае вашето устройство.

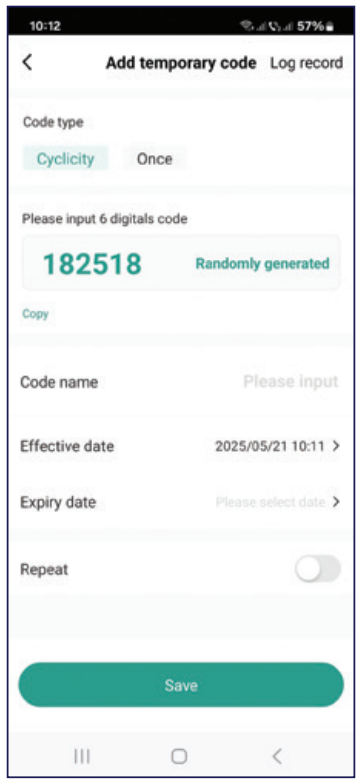
Натиснете иконата на клавиатура и следвайте стъпките на екрана.

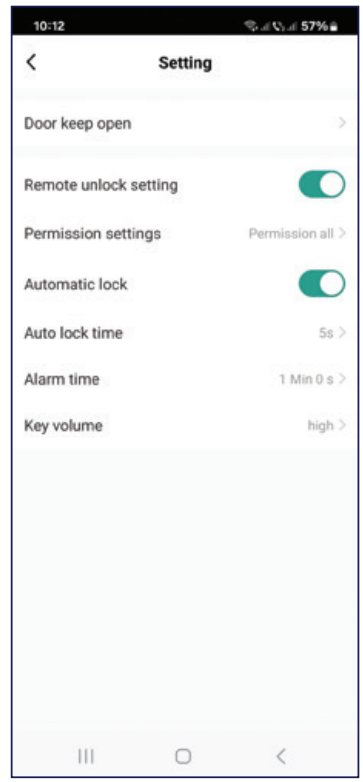
Забележка: Можете също така ръчно да добавите клавиатурата към приложението, като отворите категорията „Камери и заключване“ - „Заключване (Wi-Fi)“..











Приложението ви позволява да отключвате вратата, да добавяте и управлявате потребители и да генерирате временен код за достъп.

Grundfunktionen

Fingerabdrucksensor.

Touch-Tasten.

Wasserdichtes Metallgehäuse (IP66).

Unterstützt 1000 lokale Benutzer (988 normale Benutzer, 2 Panikbenutzer, 10 temporäre Benutzer).

Unterstützt 500 Benutzer über die App.

Unterstützt 125-kHz-EM-Karten.

Alarm- und Summerausgang.

Vandalismusschutz.

Verschiedene Zugriffsmethoden: Fingerabdruck, Karte, PIN, App.

Unterstützt temporäre Passwörter (einmalig oder zeitlich begrenzt).

Unterstützt das Hinzufügen/Löschen von Benutzern über die App.

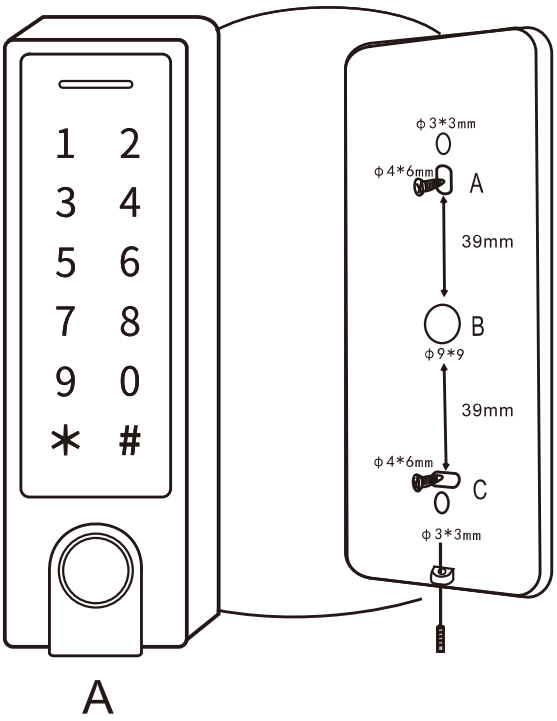
Unterstützt die Festlegung zeitlicher Beschränkungen für Benutzer.

Technische Daten

Betriebsspannung	12-18V DC
Standby-Leistung	≤60mA
Betriebsleistung	≤150mA

Kompatible RFID-Karte	EM 125 KHz
Lesereichweite der RFID-Karte	2-6 cm
Ausgangsanschlüsse	Relais, Zugangstaste, Alarm, Türkontakt, Wiegand-Kartenleser
Eingangsanschlüsse	Wiegand-Kartenleser
Relais	Ein Relais (NO, NC, COM)
Relaislaufzeit	0–99 s (Standard: 5 s)
Sperrausgangslast	Max. 2 A
PIN-Ausgang	Virtuelle 4-Bit-Nummer (10 Zeichen)
Schutzart	IP66
Betriebstemperatur	-26 °C ~ 80 °C
Gehäusematerial	Zinklegierung
Abmessungen	148 x 44 x 22 mm
WLAN	2.4 GHz/100mW
Bluetooth	2.4 GHz/2.5mW

Installation



A

Entfernen Sie die Halterung von der Geräterückseite.

Befestigen Sie die Halterung mit den mitgelieferten Schrauben an der Wand.

Führen Sie das Anschlusskabel durch die in der Abbildung unten mit B markierte Öffnung.

Befestigen Sie das Gerät an der Halterung.

Anschlüsse

Kabelfarbe	Funktion	Hinweise
Rot	DC+	DC 12–18 V Eingang
Schwarz	GND	DC Minuspol-Eingang
Blau	NO	NO-Relaisausgang (Diode im Gehäuse anschließen)

Lila	COM	COM-Relaisausgang
Orange	NC	NC-Relaisausgang (Diode im Gehäuse anschließen)
Gelb	OPEN	Zugriffstasteneingang
Verbindungen über einen Wiegand-Leser oder Controller		
Grün	Data 0	Wiegand-Ausgang (pass-through)
Weiß	Data 1	Wiegand-Ausgang (pass-through)
Spezielle Verbindungen		
Grau	Alarmausgang	Minuskontakt für Alarm
Braun	Eingang	Türkontakteingang

Akustische und visuelle Warnungen

Status	**LED**	**Summer**
Standby	Rote LED	-
Programmiermodus wird gestartet	Rote LED blinkt	Ein Piepton

Programmiermodus	Orange LED	Ein Piepton
Bedienungsfehler	-	Drei Pieptöne
Programmiermodus beenden	Rote LED	Ein Piepton
Tür wird geöffnet	Grüne LED	Ein Piepton
Alarm	Rote LED blinkt schnell	Pieptöne

Programmiermodus aufrufen und beenden

Programmiermodus aufrufen: * Mastercode #

Hinweis: Der Standard-Mastercode lautet 123456.

Programmiermodus beenden: *

Mastercode einstellen

1. Programmiermodus aufrufen: * Mastercode #

2. Mastercode ändern: 0 (neuer Mastercode)# (neuen Mastercode wiederholen)#

Hinweis: Der Mastercode muss 6 Zeichen lang sein.

3. Programmiermodus beenden: *

Betriebsmodus einstellen

Es gibt drei Betriebsmodi: Standalone-Modus, Controller-Modus und Wiegand-Lesegerät-Modus. Der Standardmodus ist Standalone/Controller-Modus.

1. Programmiermodus aufrufen: * Mastercode #

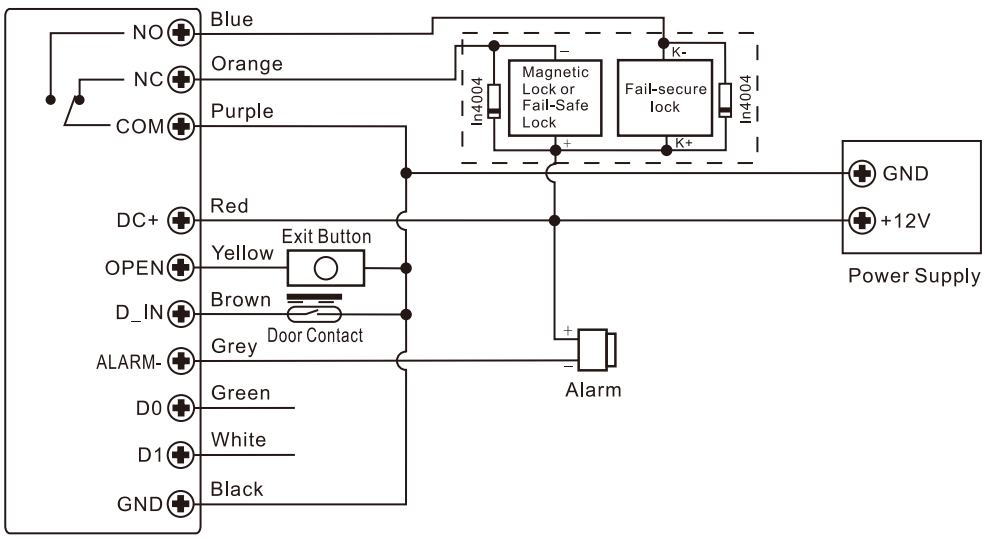
2. 7 7# (Standardmodus) oder 7 8# (Wiegand-Modus) eingeben.

3. Programmiermodus beenden: *

1. Standalone-Modus

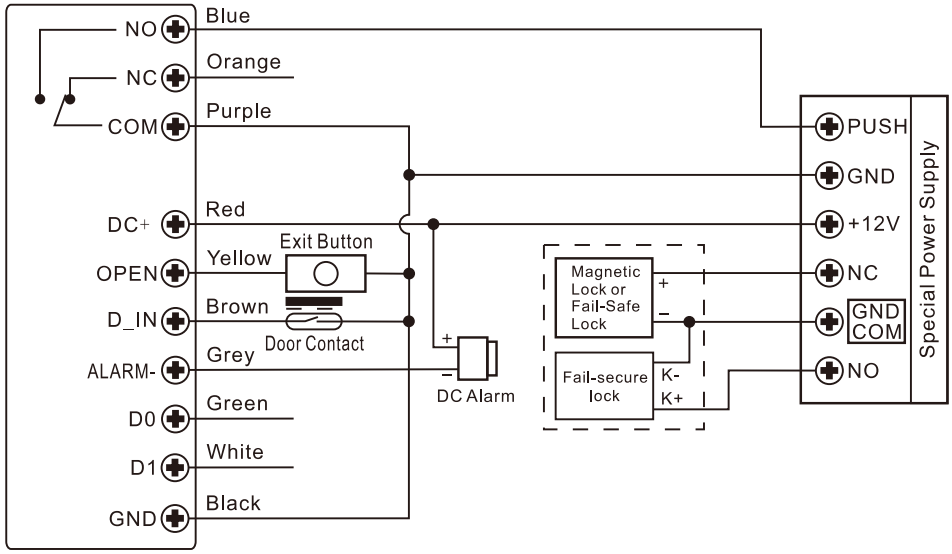
Anschlussplan

Gemeinsame Stromversorgung:



Achtung: Es ist notwendig, die mitgelieferte 1N4004-Diode oder ein gleichwertiges Produkt zu installieren, wenn Sie ein Netzteil verwenden, an das andere Geräte angeschlossen sind.

Separate Stromversorgung:



Programmierung

Die Programmierung ist je nach Zutrittsmodus unterschiedlich.

Hinweise:

1. Benutzer-ID: Weisen Sie jedem Fingerabdruck, jeder PIN oder jeder Zutrittskarte eine Benutzer-ID zu, um die Zutrittsinformationen besser verwalten zu können.

Allgemeine Benutzer-ID:

Fingerabdruck-Benutzer-ID: 0–98

PIN- oder Karten-Benutzer-ID: 100–987

Master-Benutzer-ID: 99

Panik-Benutzer-ID: 988–989

Besucher-Benutzer-ID: 990–999

Wichtig: Der Benutzer-ID darf keine 0 (Null) vorangestellt sein. Die Registrierung der Benutzer-IDs

ist sehr wichtig. Zum Ändern eines Benutzers ist die Kenntnis der Benutzer-ID erforderlich.

2. Karte: Das System unterstützt nur 125-kHz-EM-RFID-Karten.

3. PIN: Kann 4–6 Zeichen enthalten, mit Ausnahme der reservierten Ziffernfolge 8888.

Normalen Benutzer-Fingerabdruck hinzufügen

1. Programmiermodus aufrufen: * Mastercode #

2.1. Benutzerfingerabdruck mit automatisch zugewiesener ID hinzufügen: 1 (Fingerabdruck lesen) (Fingerabdruck erneut lesen) (Fingerabdruck erneut lesen)

Hinweis: Fingerabdrücke können kontinuierlich hinzugefügt werden.

2.2 Benutzerfingerabdruck mit benutzerdefinierter ID hinzufügen: 1 (Benutzer-ID) # (Fingerabdruck lesen) (Fingerabdruck erneut lesen) (Fingerabdruck erneut lesen). Hinweis: Fingerabdrücke können kontinuierlich hinzugefügt werden.

3. Programmiermodus beenden: *

Benutzerkarte hinzufügen

1. Programmiermodus aufrufen: * Mastercode #

2.1. Benutzerkarte mit automatisch zugewiesener ID hinzufügen: 1 (Karte lesen oder Kartennummer manuell eingeben) #

Hinweis: Fingerabdrücke können kontinuierlich hinzugefügt werden.

2.2 Benutzerkarte mit personalisierter ID hinzufügen: 1 (Benutzer-ID) (Karte scannen oder Kartennummer manuell eingeben) #

2.3 Karten gleichzeitig hinzufügen: Ermöglicht dem Masterbenutzer, bis zu 888 Karten in einem Schritt hinzuzufügen. Der Vorgang dauert bis zu 2 Minuten: 1 (Benutzer-ID) # (Kartenanzahl) # (Erste Kartennummer manuell eingeben) #

Hinweise:

1. Die Kartenanzahl gibt die Anzahl der Karten an, die Sie dem System hinzufügen möchten.

2. Die Kartennummern müssen fortlaufend sein.

Reguläre Benutzer-PIN hinzufügen

1. Programmiermodus aufrufen: * Mastercode #

2.1. Benutzer-PIN mit automatisch zugewiesener ID hinzufügen: 1 (PIN) #

2.2. Benutzer-PIN mit benutzerdefinierter ID hinzufügen: 1 (Benutzer-ID) # (PIN) #

3. Programmiermodus beenden: *

Zur Erhöhung der Sicherheit können Sie die PIN (max. 6 Zeichen) verbergen, indem Sie bis zu 10 Zeichen eingeben.

Beispiel:

Wenn die korrekte PIN 123434 lautet, geben Sie Folgendes ein: **123434** oder **123434, wobei ** eine beliebige Zahl zwischen 0 und 9 sein kann.

Fingerabdruck des Masterbenutzers hinzufügen

1. Programmiermodus aktivieren: * Mastercode #

2. Fingerabdruck hinzufügen: 1 (99) # (Fingerabdruck lesen) (Fingerabdruck erneut lesen) (Fingerabdruck erneut lesen)

3. Programmiermodus beenden: *

Panikbenutzer hinzufügen

1. Programmiermodus aktivieren: * Mastercode #

2.1. Karte hinzufügen: 1 (Benutzer-ID) # (Karte lesen oder Kartennummer manuell eingeben) #

2.2 PIN hinzufügen: 1 (Benutzer-ID) # (PIN) #

3. Programmiermodus beenden: *

Besucher hinzufügen

Maximal 10 Besucher können mit PIN oder Karte hinzugefügt werden. Besucher können die PIN oder Karte maximal 10 Mal verwenden. Nach maximal 10 Verwendungen verfällt die PIN oder Karte automatisch.

1. Programmiermodus aktivieren: * Mastercode #

2.1. Karte hinzufügen: 1 (Benutzer-ID) # (0–9) # (Karte lesen oder Kartennummer manuell eingeben) #

2.2 PIN hinzufügen: 1 (Benutzer-ID) # (0–9) # (PIN) #

3. Programmiermodus beenden: *

Benutzer löschen

1. Programmiermodus aufrufen: * Mastercode #

2.1. Benutzer per Fingerabdruck, Karte oder PIN löschen: 2 (Fingerabdruck lesen/Karte lesen/PIN eingeben) #

2.2. Benutzer per ID-Nummer löschen: 2 (Benutzer-ID) #

2.3. Benutzer per Kartennummer löschen: 2 (Kartennummer eingeben) #

2.4. Alle Benutzer löschen: 2 (Mastercode) #

3. Programmiermodus beenden: *

Konfiguration des Relaisaktivierungsmodus

Die Konfiguration des Relais beeinflusst dessen Verhalten nach Eingabe des Zugangscodes.

1. Programmiermodus aufrufen: * Mastercode #

2.1. Impulsmodus (Standardmodus): 3 (1~99) #

Das Relais wird nach Eingabe des Codes für einen Zeitraum zwischen 0 und 99 Sekunden (Standard: 5 Sekunden) aktiviert und deaktiviert sich anschließend automatisch.

Die Aktivierungszeit des Relais beträgt 1 bis 99 Sekunden. Standard: 5 Sekunden.

2.2. Wechselmodus: 3 0 #

Das Relais ändert seinen Zustand bei jeder korrekten Codeeingabe:

Ist es ausgeschaltet (offen), wird es aktiviert (schließt den Kontakt). Ist es aktiviert, wird es deaktiviert.

Nützlich für Tore oder Türen, die geöffnet bleiben müssen, bis sie manuell wieder geschlossen werden.

3. Programmiermodus beenden: *

Zugangsmodus-Einstellung

Im Mehrbenutzermodus sollte das Zeitintervall, in dem die Zugangscodes gelesen werden, 5 Sekunden nicht überschreiten. Nach 5 Sekunden wechselt das Gerät automatisch in den Standby-Modus.

1. Programmiermodus starten: * Mastercode #

2.1. Fingerabdruck-Zugang: 4 0 #

2.2. Karten-Zugang: 4 1 #

2.3. PIN-Zugang: 4 2 #

2. 4. Mehrbenutzer-Zugang: 4 3 (2~9) #

Erst nach der Validierung von 2~9 Benutzern öffnet sich die Tür.

2.5. Fingerabdruck oder Karte oder PIN (Standard): 4 4 #

3. Programmiermodus beenden: *

Alarm bei wiederholten Fehlversuchen

Dieser Alarm wird nach zehn aufeinanderfolgenden

Fehlversuchen (Eingabe eines falschen Codes, einer ungültigen Karte usw.) ausgelöst. Er kann so eingestellt werden, dass der Zutritt für 10 Minuten gesperrt oder erst nach Eingabe eines gültigen Codes, einer gültigen Karte oder eines gültigen Fingerabdrucks freigegeben wird.

1. Programmiermodus aufrufen: * Mastercode #

2.1. Funktion deaktiviert (Standard): 6 0 #

2.2. Funktion aktiviert: 6 1 # (Zutritt für 10 Minuten gesperrt)

2.3. Funktion aktiviert (Alarm): 6 2 #

Alarmdauer: 5 (0–3) #. Standard: 1 Minute.

Um den Alarm zu beenden, geben Sie den Mastercode # ein, scannen Sie den Master-Fingerabdruck/die Master-Karte, geben Sie die PIN ein oder scannen Sie einen Benutzer-Fingerabdruck/eine Benutzer-Karte.

3. Programmiermodus beenden: *

Tür-offen-Warnung

Wenn Sie einen kabelgebundenen magnetischen Türkontakt an die Zutrittskontrolltastatur angeschlossen haben und die Tür länger als eine Minute geöffnet bleibt, ertönt der eingebaute Summer, um den Benutzer daran zu erinnern, die Tür zu schließen. Der Ton kann durch Schließen der Tür oder Eingabe eines gültigen Zugangscodes (Master- oder Benutzercode) gestoppt werden. Andernfalls läuft

der Ton so lange weiter, wie er eingestellt ist.

Türaufbruch-Warnung

Wenn Sie einen kabelgebundenen magnetischen Türkontakt an die Zutrittskontrolltastatur angeschlossen haben und die Tür aufgebrochen wird, lösen der eingebaute Summer und die externe Sirene (falls vorhanden) den Alarm aus. Der Ton kann durch Schließen der Tür oder Eingabe eines gültigen Zugangscodes (Master- oder Benutzercode) gestoppt werden. Andernfalls läuft der Ton so lange weiter, wie er eingestellt ist.

1. Programmiermodus aufrufen: * Mastercode #

2.1. Funktion deaktiviert (Standard): 6 3 #

2.2. Funktion aktiviert“ 6 4 #

Alarmdauer einstellen: 5 (0–3) #. Standard: 1 Minute.

3. Programmiermodus beenden: *

Summer- und LED-Einstellung

1. Programmiermodus aufrufen: * Mastercode #

2.1. Summer deaktivieren: 7 0 #

2.2. Summer aktivieren (Standard): 7 1 #

3.1. LED aus: 7 2 #

3.2. LED an (Standard): 7 3 #

4.1. Tastenbeleuchtung aus: 7 4 #

4.2. Tastenbeleuchtung dauerhaft an: 7 5 #

4.3. Tastenbeleuchtung automatisch aus (Standard): 7 6 #. 20 Sekunden nach der letzten Bedienung schaltet sich die Tastatur automatisch aus. Durch Berühren einer beliebigen Taste leuchtet die Tastatur wieder auf.

3. Programmiermodus beenden: *

Fingerabdruck/Karte/PIN eines Benutzers mit Masterkarte/Fingerabdruck hinzufügen

1. Masterkarte/Fingerabdruck einlesen.

2. Fingerabdruck des Benutzers dreimal scannen oder Karte oder PIN des Benutzers scannen.

Schritt 2 wiederholen, um weitere Benutzer hinzuzufügen.

3. Masterkarte/Fingerabdruck erneut scannen.

Fingerabdruck/Karte/PIN eines Benutzers mit Masterkarte/Fingerabdruck löschen

1. Masterkarte/Fingerabdruck zweimal innerhalb von maximal 5 Sekunden scannen.

2. Fingerabdruck/Karte scannen oder PIN des Benutzers eingeben.

Schritt 2 wiederholen, um weitere Benutzer zu löschen.

3. Masterkarte/Fingerabdruck erneut scannen.

Masterkarte zurücksetzen und hinzufügen

Wenn Sie eine Zutrittstaste an die

Zutrittskontrolltastatur angeschlossen haben, gehen Sie wie folgt vor, um die Tastatur zurückzusetzen:

1. Stromversorgung ausschalten.

2. Zutrittstaste gedrückt halten, während Sie die Stromversorgung wieder einschalten.

3. Es ertönen zwei Signaltöne.

4. Nehmen Sie Ihren Finger von der Zugangstaste.

5. Die gelbe LED leuchtet.

6. Lesen Sie eine beliebige 125-kHz-EM-Karte.

7. Die LED leuchtet rot.

8. Die Tastatur wurde zurückgesetzt.

9. Die gelesene Karte ist nun die Masterkarte.

Hinweise:

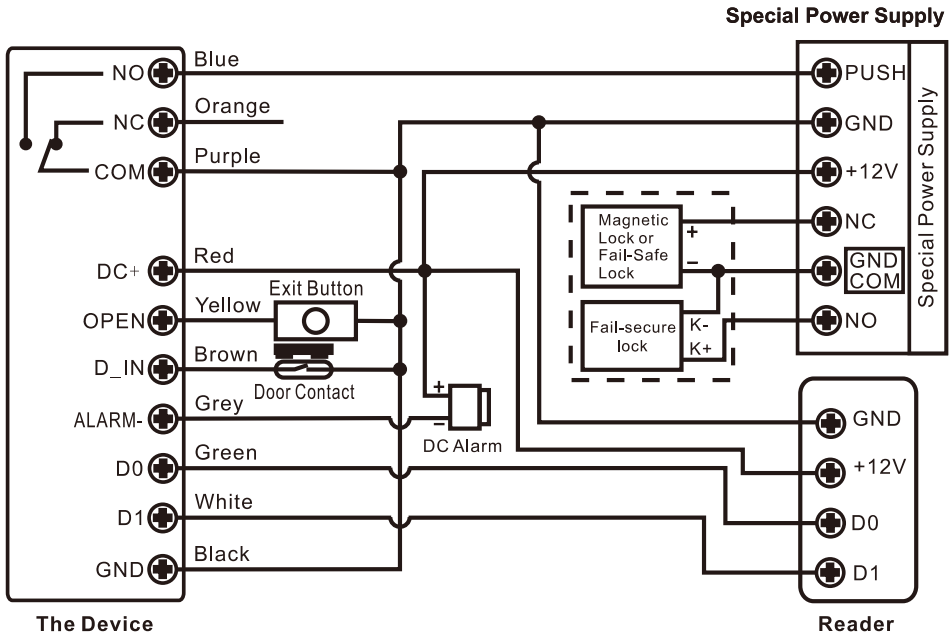
1. Wenn Sie keine Masterkarte hinzufügen möchten, müssen Sie die Zugangstaste mindestens 5 Sekunden lang gedrückt halten, bevor Sie sie loslassen. Dadurch wird die vorherige Masterkarte ungültig.

2. Durch das Zurücksetzen werden die Benutzerinformationen nicht gelöscht.

2. Controller-Modus

Die Tastatur fungiert als Controller, wenn sie an ein Wiegand-Lesegerät angeschlossen ist.

Anschlussdiagramm



Achtung: Bei Verwendung eines Netzteils, an das andere Geräte angeschlossen sind, muss die mitgelieferte Diode 1N4004 oder eine gleichwertige Diode installiert werden.

Wiegand-Eingabeformat einstellen

1. Programmiermodus aktivieren: * Mastercode #

2. Wiegand-Eingabebits für EM-Karte einstellen:

8 (26–44) # (Standard: 26 Bit)

3.1. Paritätsbit deaktivieren: 8 0 #

3.2. Paritätsbit aktivieren: 8 1 #

3. Programmiermodus beenden: *

Programmierung

Die grundlegende Programmierung erfolgt wie im Standalone-Modus.

Anschluss an einen externen Kartenleser

Bei einem EM- oder Mifare-Kartenleser können Benutzer sowohl über die Tastatur als auch über den externen Leser hinzugefügt/gelöscht werden.

Bei einem HID-Kartenleser können Benutzer nur über den externen Leser hinzugefügt/gelöscht werden.

Anschluss an einen Fingerabdruckleser

Schließen Sie den Fingerabdruckleser an die Tastatur an.

1. Programmiermodus aktivieren: * Mastercode #

2.1. Geben Sie 1 ein (Fingerabdruck am Fingerabdruckleser lesen). # Die ID wird automatisch zugewiesen.

2.2. Geben Sie 1 ein (Benutzer-ID). # (Fingerabdruck am Fingerabdruckleser lesen). #

3. Programmiermodus beenden: *

Verbindung mit einem Tastaturleser herstellen

Der Tastaturleser kann 4 Bit, 8 Bit (ASCII) oder 10 Bit unterstützen.

1. Programmiermodus aufrufen: * Mastercode #

2.1. Anzahl der Bits eingeben: 8 (4, 8 oder 10) #. Die Standardeinstellung ist 4 Bit.

3. Programmiermodus beenden: *

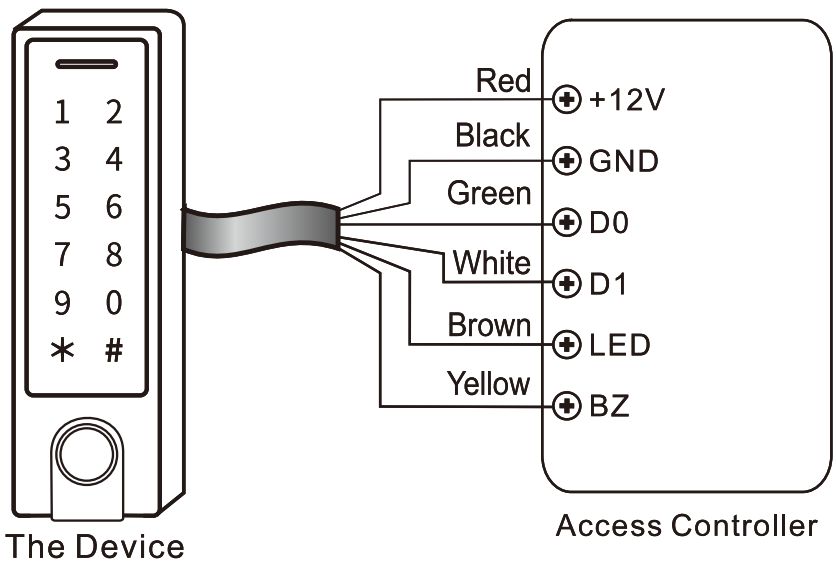
Benutzer-PIN hinzufügen/löschen

Die Benutzer-PIN kann sowohl am Tastaturleser für die Zutrittskontrolle als auch am externen Tastaturleser hinzugefügt/gelöscht werden..

3. Wiegand-Lesegerät-Modus

Die Tastatur kann auch als Standard-Wiegand-Lesegerät an einen externen Controller angeschlossen werden.

Anschlussplan



Befindet sich die Tastatur im Wiegand-Lesemodus, sind alle im Controller-Modus vorgenommenen Einstellungen ungültig. Die großen und gelben Kabel werden wie folgt neu definiert:

Braunes Kabel: Grüne LED-Steuerung

Gelbes Kabel: Summer-Steuerung

Einstellung des Wiegand-Ausgabeformats

1. Programmiermodus aktivieren: * Mastercode #

2. Wiegand-Bits für EM-Karte einstellen: 8 (26–44) #

3.1. Paritätsbit deaktivieren: 8 0 #

3.2. Paritätsbit aktivieren: 8 1 # (Standard)

3. Programmiermodus beenden: *

Hinweis: Um einen Wiegand-Controller anzuschließen, muss das Paritätsbit deaktiviert werden.

Erweiterte Anwendungen

Zugriff mit allen Karten

Nach Aktivierung dieses Modus können alle Karten die Tür öffnen. Gleichzeitig wird die Karte dem System hinzugefügt.

1. Programmiermodus aktivieren: * Mastercode #

2.1. Funktion deaktivieren: 9 2 # (Standard)

2.2. Funktion aktivieren: 9 3 #

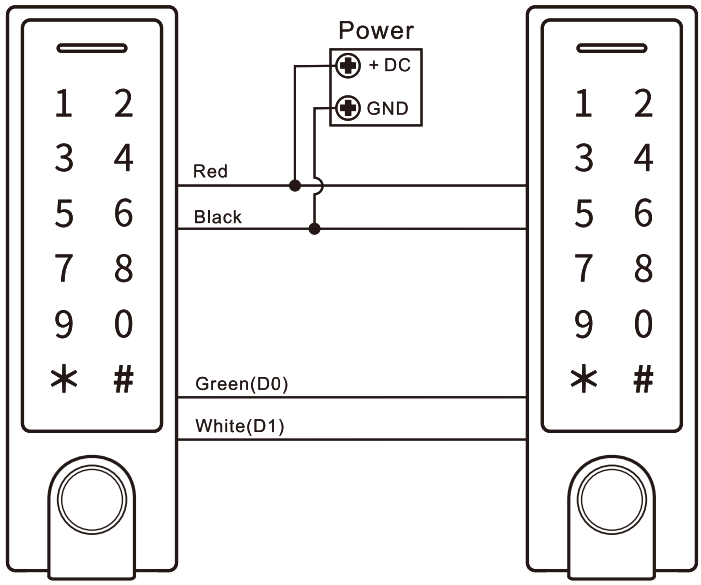
3. Programmiermodus beenden: *

Benutzerdaten übertragen

Für mit PIN/Karte registrierte Benutzer.

Benutzerdaten können von einer Tastatur auf eine andere übertragen werden.

Anschlussplan



Hinweise:

Beide Tastaturen müssen aus derselben Serie stammen.

Der Mastercode beider Tastaturen muss identisch sein.

Aktivieren Sie die Übertragungsfunktion nur auf der Haupttastatur (Mastertastatur).

Falls auf der Nebentastatur bereits Benutzer registriert sind, werden diese bei der Übertragung überschrieben.

Bei einer Anzahl von 900 Benutzern kann die Übertragung bis zu 30 Sekunden dauern.

Aktivieren Sie den Übertragungsmodus auf der Mastertastatur.

1. Rufen Sie den Programmiermodus auf: * Mastercode #

2. Geben Sie 9 8 # ein.

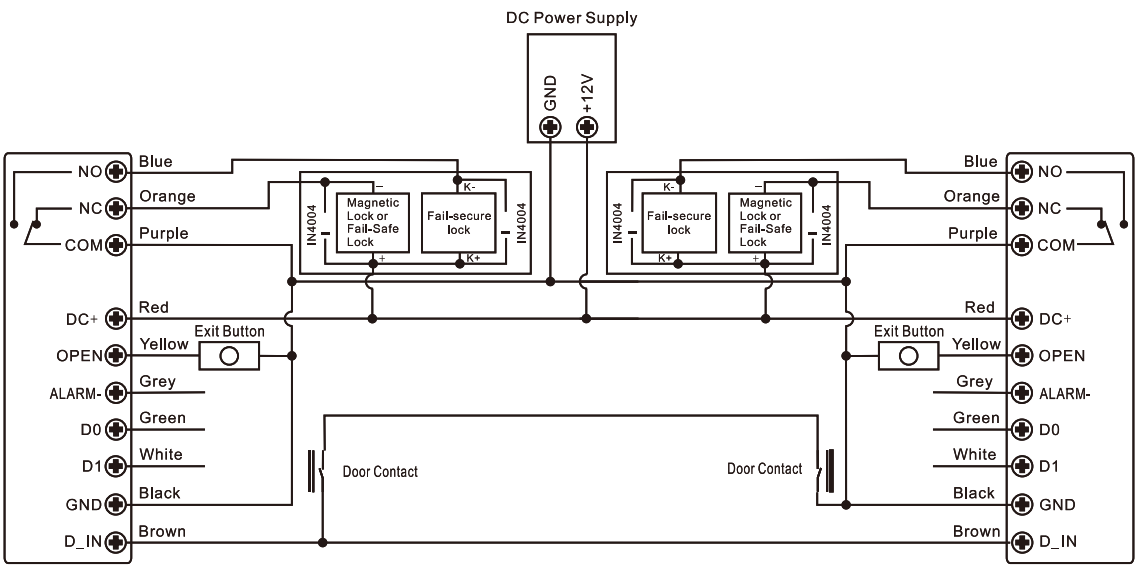
Für 30 Sekunden, die maximale Übertragungsdauer, leuchtet die grüne LED. Sobald die Datenübertragung abgeschlossen ist, ertönt ein Signalton und die rote LED leuchtet.

3. Beenden Sie den Programmiermodus: *

Tastaturen verbinden

In diesem Modus können zwei Tastaturen miteinander verbunden werden, um zwei Türen zu steuern. Diese Funktion ist besonders nützlich in Gefängnissen, Banken und anderen Orten, an denen ein höheres Sicherheitsniveau erforderlich ist.

Anschlussplan



Benutzer an Tastatur A registrieren und anschließend auf Tastatur B übertragen.

Verriegelungsmodus auf beiden Tastaturen aktivieren:

1. Programmiermodus aktivieren: * Mastercode #

2.1. Funktion deaktivieren: 9 0 # (Standard)

2.2. Funktion aktivieren: 9 1 #

3. Programmiermodus beenden: *

Wenn die Funktion aktiviert ist und Tür 2 geschlossen bleiben soll, kann der Benutzer seinen Fingerabdruck/ seine Karte scannen oder die PIN an Tastatur A eingeben. Tür 1 öffnet sich. Wenn Tür 1 geschlossen bleiben soll, kann der Benutzer seinen Fingerabdruck/ seine Karte scannen oder die PIN an Tastatur B eingeben. Tür 2 öffnet sich.

Wenn die Funktion aktiviert ist, kann der Benutzer seinen Fingerabdruck/seine Karte scannen oder die PIN an Tastatur A eingeben, um Tür 1 zu öffnen. Oder er scannen seinen Fingerabdruck/seine Karte oder geben die PIN an Tastatur B ein, um Tür 2 zu öffnen..

Tastatursteuerung über die Tuya Smart App

Hinweis: Aufgrund häufiger Updates der Tuya Smart App können die in diesem Handbuch dargestellten Bilder und Informationen von denen in der auf Ihrem Gerät installierten Version abweichen..

Gehen Sie zu Google Play oder App Store oder scannen Sie den untenstehenden QR-Code und installieren Sie die Tuya Smart-App.

Verbinden Sie Ihr Smartphone mit dem WLAN und

aktivieren Sie Standort und Bluetooth.

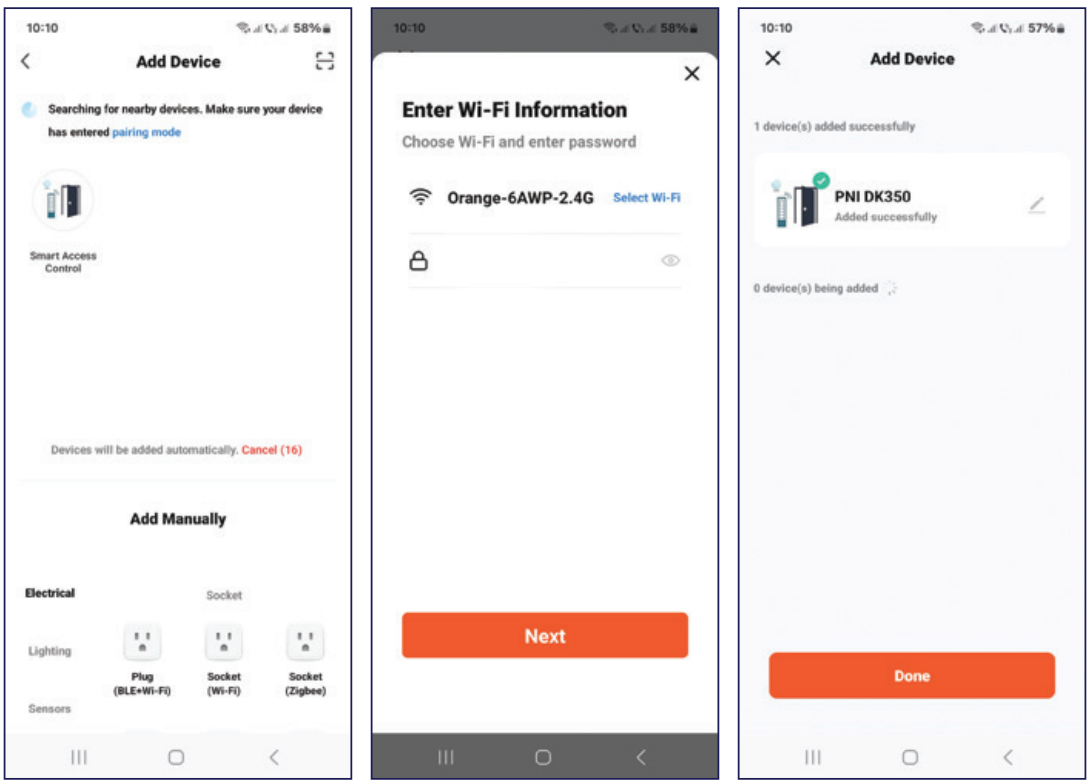
Öffnen Sie die App und melden Sie sich an.

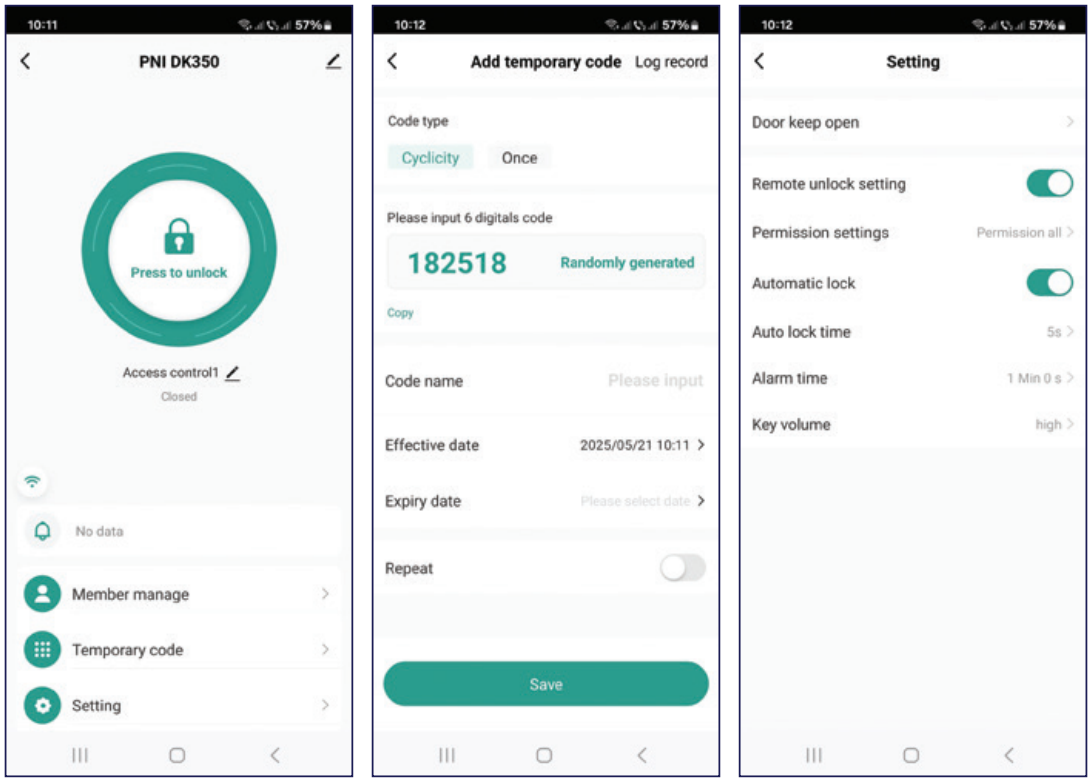
Drücken Sie „+“ – „Gerät hinzufügen“.

Die App erkennt Ihr Gerät automatisch.

Drücken Sie auf das Tastatursymbol und folgen Sie den Anweisungen auf dem Bildschirm.

Hinweis: Sie können die Tastatur auch manuell zur App hinzufügen, indem Sie auf die Kategorie „Kameras & Sperren – Sperren (WLAN)“ zugreifen..





Mit der Anwendung können Sie die Tür öffnen, Benutzer hinzufügen und verwalten sowie einen temporären Zugangscode generieren.

Características básicas

Sensor de huellas dactilares.

Teclas táctiles.

Carcasa metálica resistente al agua (IP66).

Admite 1000 usuarios locales (988 usuarios comunes, 2 usuarios de pánico y 10 usuarios temporales).

Admite 500 usuarios mediante la aplicación.

Admite tarjeta EM de 125 KHz.

Salida de alarma y zumbador.

Función antivandálica.

Múltiples métodos de acceso: huella dactilar, tarjeta, PIN y aplicación.

Admite contraseña temporal (de un solo uso o temporal).

Admite añadir/eliminar usuarios mediante la aplicación.

Admite la configuración de restricciones horarias para los usuarios.

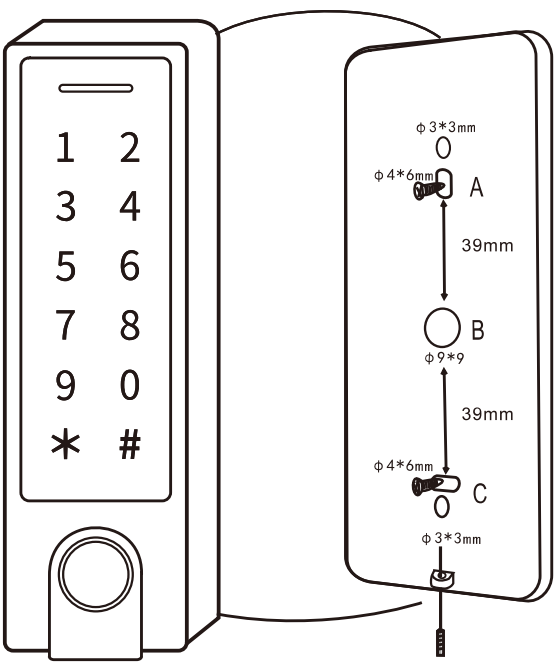
Especificaciones técnicas

Voltaje de funcionamiento	12-18V DC
Consumo en espera	≤60mA

Consumo de funcionamiento	≤150mA
Tarjeta RFID compatible	EM 125 KHz
Distancia de lectura de la tarjeta RFID	2-6 cm
Conexiones de salida	Relé, botón de acceso, alarma, contacto de puerta, lector de tarjetas Wiegand
Conexiones de entrada	Lector de tarjetas Wiegand
Relé	Un relé NO, NC, COM
Tiempo de funcionamiento del relé	0-99 s (5 s por defecto)
Carga de salida de bloqueo	Máx. 2 A
Salida PIN	4 bits, número virtual de 10 caracteres
Grado de protección	IP66

Temperatura de funcionamiento	-26 ~ 80°C
Material de la carcasa	Aleación de zinc
Dimensiones	148 x 44 x 22 mm
Wi-Fi	2.4 GHz/100mW
Bluetooth	2.4 GHz/2.5mW

Instalación



A

Retire el soporte de la parte trasera de la unidad.

Fije el soporte a la pared con los tornillos incluidos.

Pase el cable de conexión por el orificio marcado con una B en el dibujo inferior.

Fije la unidad al soporte.

Conexiones

Color del cable	**Función**	**Notas**
Rojo	DC+	Entrada de CC 12-18 V
Negro	GND	Entrada de CC con polo negativo
Azul	NO	Salida de relé NO (conecte el diodo incluido en el paquete)
Morado	COM	Salida de relé COM
Naranja	NC	Salida de relé NC (conecte el diodo incluido en el paquete)
Amarillo	OPEN	Entrada de botón de acceso
Conexiones a través de un lector o controlador Wiegand		
Verde	Data 0	Salida Wiegand (pass-through)
Blanco	Data 1	Salida Wiegand(pass-through)

Conexiones especiales		
Gris	Salida de alarma	Contacto negativo para alarma
Marrón	Entrada	Entrada de contacto de puerta

Advertencias sonoras y luminosas

Estado	**LED**	**Zumbador**
En espera	LED rojo	-
Entrando al modo de programación	LED rojo parpadeando	Un pitido
Modo de programación	LED naranja	Un pitido
Error de funcionamiento	-	Tres pitidos
Saliendo del modo de programación	LED rojo	Un pitido
Abriendo la puerta	LED verde	Un pitido

Alarma	LED rojo parpadeando rápidamente	Pitidos

Entrar y salir del modo de programación

Entrar al modo de programación: * código maestro #

Nota: El código maestro predeterminado es 123456.

Salir del modo de programación: *

Establecer código maestro

1. Entrar al modo de programación: * código maestro #

2. Cambiar código maestro: 0 (nuevo código maestro)# (repetir nuevo código maestro)#

Nota: El código maestro debe contener 6 caracteres.

3. Salir del modo de programación: *

Configuración del modo de funcionamiento

Existen 3 modos de funcionamiento: modo autónomo, modo controlador y modo lector Wiegand. El modo predeterminado es modo autónomo/controlador.

1. Entrar al modo de programación: * código maestro #

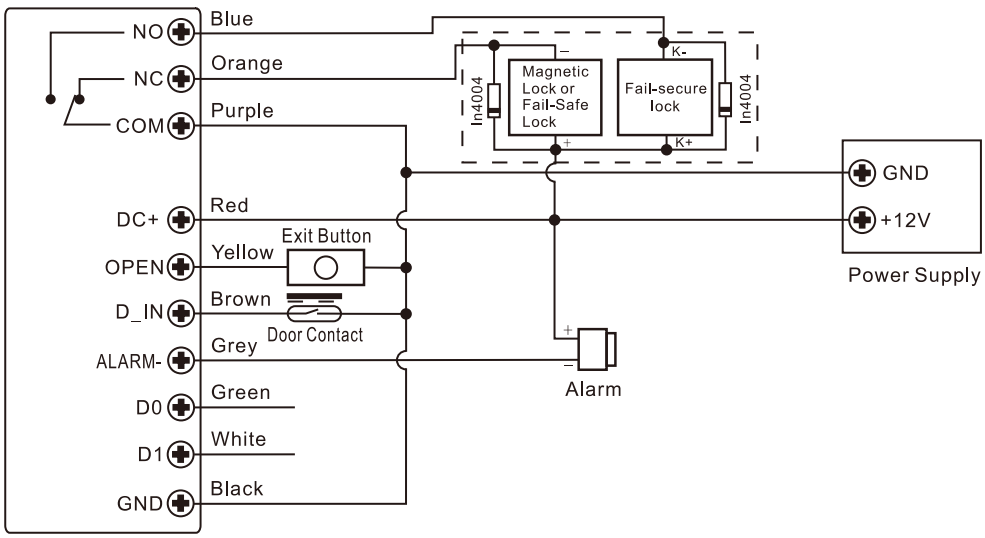
2. Introducir 7 7# (modo predeterminado) o 7 8# (modo Wiegand).

3. Salir del modo de programación: *

1. Modo autónomo

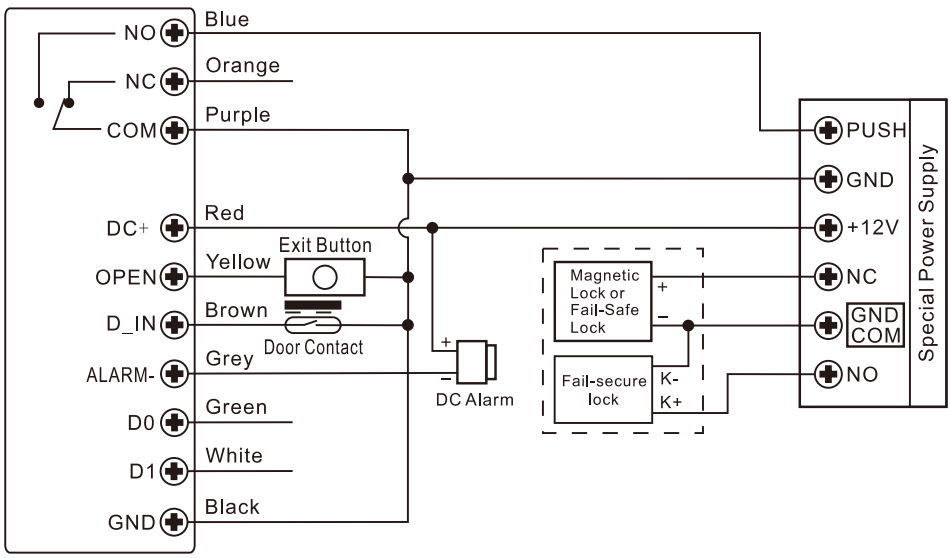
Diagrama de conexión

Alimentación común:



Atención: Es necesario instalar el diodo 1N4004 incluido o equivalente si se utiliza una fuente de alimentación con otros dispositivos conectados.

Fuente de alimentación independiente:



Programación

La programación varía según el modo de acceso.

Notas:

1. ID de usuario: Asigne un ID de usuario a cada huella dactilar, PIN o tarjeta de acceso para una mejor gestión de la información de acceso.

ID de usuario común:

ID de usuario de huella dactilar: 0-98

ID de usuario de PIN o tarjeta: 100-987

ID de usuario maestro: 99

ID de usuario de pánico: 988-989

ID de usuario de visitante: 990-999

Importante: El ID de usuario no debe ir precedido de 0 (cero). El registro de los ID de usuario es muy importante. Para cambiar un usuario, es necesario conocer el ID de usuario.

2. Tarjeta: El sistema solo admite tarjetas RFID EM de 125 KHz.

3. PIN: Puede contener de 4 a 6 caracteres, excepto la secuencia 8888, que está reservada.

Añadir huella dactilar de usuario normal

1. Acceda al modo de programación: * código maestro #

2.1. Añadir huella de usuario usando el ID asignado automáticamente: 1 (leer huella) (repetir lectura de huella) (repetir lectura de huella)

Nota: Se pueden añadir huellas continuamente.

2.2 Añadir huella de usuario usando el ID personalizado: 1 (ID de usuario) # (leer huella) (repetir lectura de huella) (repetir lectura de huella). Nota: Se pueden añadir huellas continuamente.

3. Salir del modo de programación: *

Añadir tarjeta de usuario

1. Acceda al modo de programación: * código maestro #

2.1. Añadir tarjeta de usuario con ID asignado automáticamente: 1 (leer tarjeta o introducir manualmente el número) #

Nota: Se pueden añadir huellas dactilares de forma continua.

2.2. Añadir tarjeta de usuario con ID personalizado: 1 (ID de usuario) (escanear tarjeta o introducir manualmente el número) #

2.3. Añadir tarjetas en bloque: permite al usuario maestro añadir hasta 888 tarjetas en un solo paso. El procedimiento tarda hasta 2 minutos: 1 (ID de usuario) # (cantidad de tarjetas) # (introducir manualmente el primer número de tarjeta) #

Notas:

1. La cantidad de tarjetas representa la cantidad de tarjetas que desea añadir al sistema.

2. Los números de tarjeta deben ser consecutivos.

Añadir PIN de usuario

1. Acceda al modo de programación: * código maestro #

2.1. Agregar PIN de usuario usando el ID asignado automáticamente: 1 (PIN) #

2.2 Agregar PIN de usuario usando el ID personalizado: 1 (ID de usuario) # (PIN) #

3. Salir del modo de programación: *

Para mayor seguridad, puede ocultar el PIN (máximo 6 caracteres) escribiendo hasta 10 caracteres.

Por ejemplo:

Si el PIN correcto es: 123434

Escriba: **123434** o **123434, donde ** puede ser cualquier número del 0 al 9.

Añadir huella de usuario maestro

1. Acceder al modo de programación: * código maestro #

2. Añadir huella: 1 (99) # (leer huella) (repetir lectura de huella) (repetir lectura de huella)

3. Salir del modo de programación: *

Añadir usuario de pánico

1. Acceder al modo de programación:* código maestro #

2.1. Añadir tarjeta: 1 (ID de usuario) # (leer tarjeta o introducir manualmente el número de tarjeta) #

2.2. Añadir PIN: 1 (ID de usuario) # (PIN) #

3. Salir del modo de programación: *

Añadir usuario visitante

Se puede añadir un máximo de 10 visitantes con PIN o tarjeta. Los visitantes pueden usar el PIN o la tarjeta un máximo de 10 veces. Después de un máximo de 10 usos, el PIN o la tarjeta quedarán invalidados automáticamente.

1. Acceder al modo de programación: * código maestro #

2.1. Añadir tarjeta: 1 (ID de usuario) # (0~9) # (leer tarjeta o introducir manualmente el número de tarjeta) #

2.2 Añadir PIN: 1 (ID de usuario) # (0~9) # (PIN) #

3. Salir del modo de programación: *

Eliminar usuario

1. Entrar al modo de programación: * código maestro #

2.1. Eliminar usuario por huella dactilar, tarjeta o PIN: 2 (leer huella dactilar/leer tarjeta/introducir PIN) #

2.2 Eliminar usuario por número de ID: 2 (ID de usuario) #

2.3 Eliminar usuario por número de tarjeta: 2 (introducir el número de tarjeta) #

2.4. Eliminar todos los usuarios: 2 (código maestro) #

3. Salir del modo de programación: *

Configuración del modo de activación del relé

La configuración del relé influye en su comportamiento tras introducir el código de acceso.

1. Entrar en el modo de programación: * código maestro #

2.1. Modo de impulso (predeterminado): 3 (1~99) #

El relé se activa durante un periodo de entre 0 y 99 segundos (predeterminado: 5 segundos) tras introducir el código y, a continuación, se desactiva automáticamente.

El tiempo de activación del relé es de 1 a 99 segundos. Predeterminado: 5 segundos.

2.2. Modo alterno: 3 0 #

El relé cambia de estado cada vez que se introduce el código correctamente:

Si está apagado (abierto), se activa (cierra el contacto). Si está activado, se desactiva.

Útil para portones o puertas que deben permanecer abiertos hasta que se vuelvan a cerrar manualmente.

3. Salir del modo de programación: *

Configuración del modo de acceso

En el modo de acceso multiusuario, el intervalo de tiempo de lectura de los códigos de acceso no debe superar los 5 segundos. Después de 5 segundos, la unidad entra automáticamente en modo de espera.

1. Entrar en modo de programación: * código maestro #

2.1. Acceso con huella dactilar: 4 0 #

2.2. Acceso con tarjeta: 4 1 #

2.3. Acceso con PIN: 4 2 #

2.4. Acceso multiusuario: 4 3 (2-9) #

Solo después de que se validen de 2 a 9 usuarios, la puerta se abrirá.

2.5. Huella dactilar, tarjeta o PIN (predeterminado): 4 4 #

3. Salir del modo de programación: *

Alarma por intentos fallidos repetidos

Se refiere a una alarma que se activa después de 10 intentos de acceso incorrectos consecutivos (introducción de un código erróneo, tarjeta no válida, etc.). Se puede configurar para denegar el acceso durante 10 minutos o para permitir el acceso solo después de introducir un código, tarjeta o huella dactilar válidos.

1. Entrar en modo de programación: * código maestro

#

2.1. Función deshabilitada (predeterminado): 6 0 #

2.2. Función habilitada: 6 1 # (el acceso estará prohibido durante 10 minutos)

2.3. Función habilitada (Alarma): 6 2 #

Duración de la alarma: 5 (0-3) #. Predeterminado: 1 minuto.

Para detener la alarma, introduzca el código maestro #, escanee la huella dactilar/tarjeta maestra, introduzca el PIN o escanee la huella dactilar/tarjeta de usuario.

3. Salga del modo de programación: *

Aviso de puerta abierta

Si ha conectado un contacto magnético cableado al teclado de control de acceso y la puerta permanece abierta durante más de un minuto, el zumbador integrado sonará para recordarle al usuario que cierre la puerta. El sonido se puede detener cerrando la puerta o introduciendo un código de acceso válido (maestro o de usuario). De lo contrario, el sonido continuará mientras esté configurado.

Aviso de puerta forzada

Si ha conectado un contacto magnético cableado al teclado de control de acceso y se fuerza la puerta, el zumbador integrado y la sirena externa (si la hay)

activarán la alarma. El sonido se puede detener cerrando la puerta o introduciendo un código de acceso válido (maestro o de usuario). De lo contrario, el sonido continuará mientras esté configurado.

1. Acceda al modo de programación: * código maestro #

2.1. Función deshabilitada (predeterminado): 6 3 #

2.2. Función habilitada" 6 4 #

Configurar duración de alarma: 5 (0~3) #. Predeterminado: 1 minuto.

3. Salir del modo de programación: *

Configuración de zumbador y LED

1. Entrar al modo de programación: * código maestro #

2.1. Desactivar zumbador: 7 0 #

2.2. Activar zumbador (predeterminado): 7 1 #

3.1. LED apagado: 7 2 #

3.2. LED encendido (predeterminado): 7 3 #

4.1. Apagado de la luz del teclado: 7 4 #

4.2. Encendido permanente de la luz del teclado: 7 5 #

4.3. Apagado automático de la luz del teclado (predeterminado): 7 6 #. Transcurridos 20 segundos desde la última operación, el teclado se apaga

automáticamente. Al tocar cualquier tecla, se enciende.

3. Salir del modo de programación: *

Añadir huella/tarjeta/PIN de usuario con tarjeta maestra

1. Lea la tarjeta maestra.

2. Escanee la huella del usuario 3 veces o escanee su tarjeta o PIN.

Repita el paso 2 para añadir más usuarios consecutivamente.

3. Escanee de nuevo la tarjeta maestra.

Eliminar huella/tarjeta/PIN de un usuario con tarjeta maestra

1. Escanee la tarjeta maestra dos veces en un máximo de 5 segundos.

2. Escanee la huella o tarjeta o introduzca el PIN.

Repita el paso 2 para eliminar más usuarios consecutivamente.

3. Escanee de nuevo la tarjeta maestra.

Reiniciar y añadir una tarjeta maestra

Si ha conectado un botón de acceso al teclado de control de acceso, proceda de la siguiente manera para reiniciarlo:

1. Apague el dispositivo.

2. Mantenga pulsado el botón de acceso mientras lo vuelve a encender.

3. Se oirán 2 pitidos. 4. Retire el dedo del botón de acceso.

5. El LED amarillo se ilumina.

6. Lea cualquier tarjeta EM de 125 KHz.

7. El LED se ilumina en rojo.

8. El teclado se ha reiniciado.

9. La tarjeta leída se ha convertido en la tarjeta maestra.

Notas:

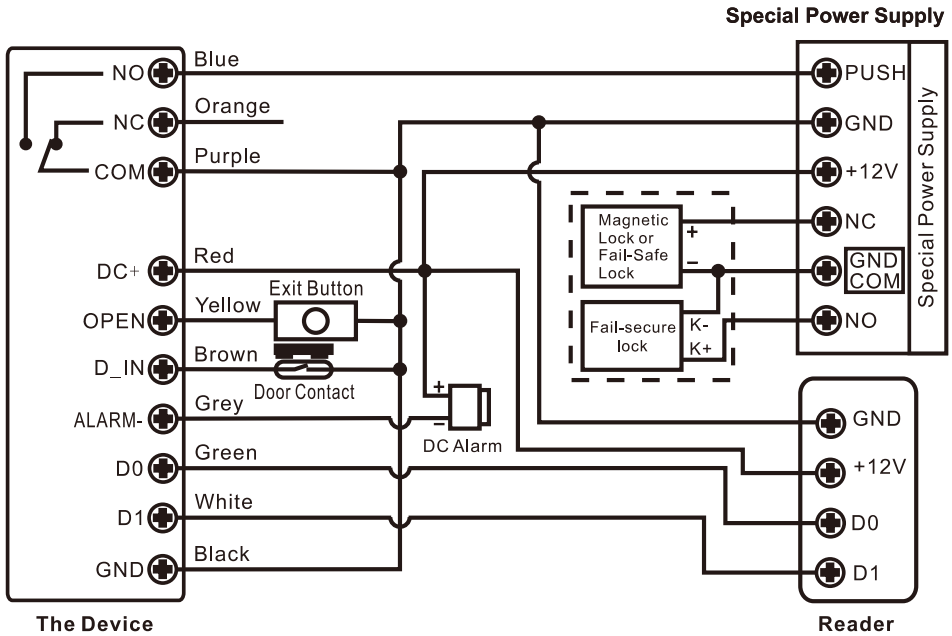
1. Si no desea agregar una tarjeta maestra, mantenga presionado el botón de acceso durante al menos 5 segundos antes de soltarlo. Este procedimiento invalidará la tarjeta maestra anterior.

2. Al reiniciar, no se eliminará la información del usuario.

2. Modo controlador

El teclado funcionará como controlador si se conecta a un lector Wiegand.

Diagrama de conexión



Atención: Es necesario instalar el diodo 1N4004 incluido o equivalente si utiliza una fuente de alimentación a la que se conectan otros dispositivos.

Configuración del formato de entrada Wiegand

1. Acceder al modo de programación: * código maestro #

2. Configurar los bits de entrada Wiegand para la tarjeta EM:

8 (26~44) # (predeterminado: 26 bits)

3.1. Desactivar el bit de paridad: 8 0 #

3.2. Activar el bit de paridad: 8 1 #

3. Salir del modo de programación: *

Programación

La programación básica es la misma que en el modo

autónomo.

Conexión a un lector de tarjetas externo

En el caso de un lector de tarjetas EM o Mifare, se pueden añadir o eliminar usuarios tanto en el teclado como en el lector externo.

En el caso de un lector de tarjetas HID, solo se pueden añadir o eliminar usuarios en el lector externo.

Conexión a un lector de huellas dactilares

Conecte el lector de huellas dactilares al teclado. 1. Acceder al modo de programación: * código maestro #

2.1. Introducir 1 (leer la huella dactilar en el lector) #. El ID se asigna automáticamente.

2.2. Introducir 1 (ID de usuario) # (leer la huella dactilar en el lector) #

3. Salir del modo de programación: *

Conexión a un lector de teclado

El lector de teclado puede ser de 4 bits, 8 bits (ASCII) o 10 bits.

1. Acceder al modo de programación: * código maestro #

2.1. Introducir el número de bits: 8 (4, 8 o 10) #. El valor predeterminado es 4 bits.

3. Salir del modo de programación: *

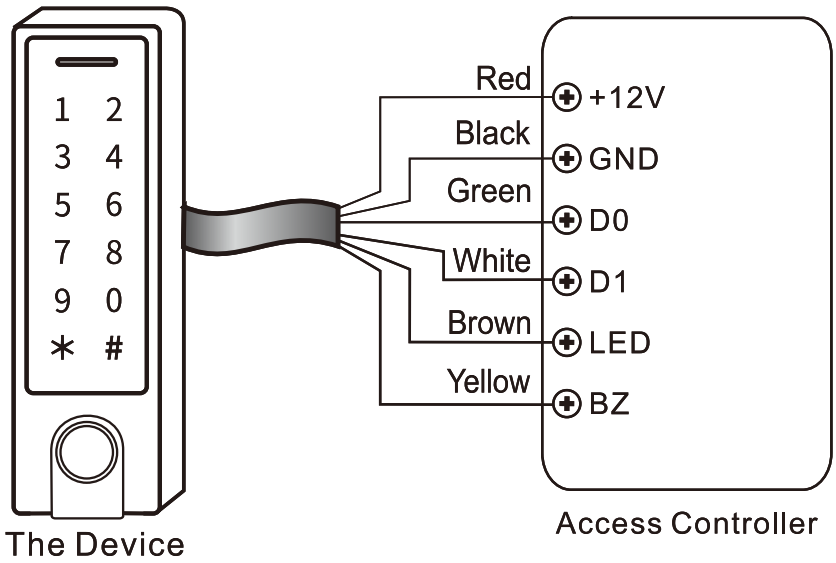
Añadir/Eliminar PIN de usuario

El PIN de usuario se puede añadir/eliminar tanto en el teclado de control de acceso como en el lector de teclado externo.

3. Modo lector Wiegand

El teclado también puede funcionar como un lector Wiegand estándar conectado a un controlador externo.

Diagrama de conexión



Cuando el teclado está en modo lector Wiegand, todos los ajustes realizados en el modo controlador se invalidan. Los cables grande y amarillo se redefinirán de la siguiente manera:

Cable marrón: Control del LED verde

Cable amarillo: Control del zumbador.

Ajuste del formato de salida Wiegand

1. Acceder al modo de programación: * código maestro

#

2. Configurar los bits Wiegand para la tarjeta EM: 8 (26~44) #

3.1. Desactivar el bit de paridad: 8 0 #

3.2. Activar el bit de paridad: 8 1 # (predeterminado)

3. Salir del modo de programación: *

Nota: Para conectar un controlador Wiegand, debe desactivar el bit de paridad.

Aplicaciones avanzadas

Acceso a todas las tarjetas

Tras activar este modo, todas las tarjetas pueden abrir la puerta. La tarjeta se añade simultáneamente al sistema.

1. Acceder al modo de programación: * código maestro #

2.1. Desactivar la función: 9 2 # (predeterminado)

2.2. Habilitar función: 9 3 #

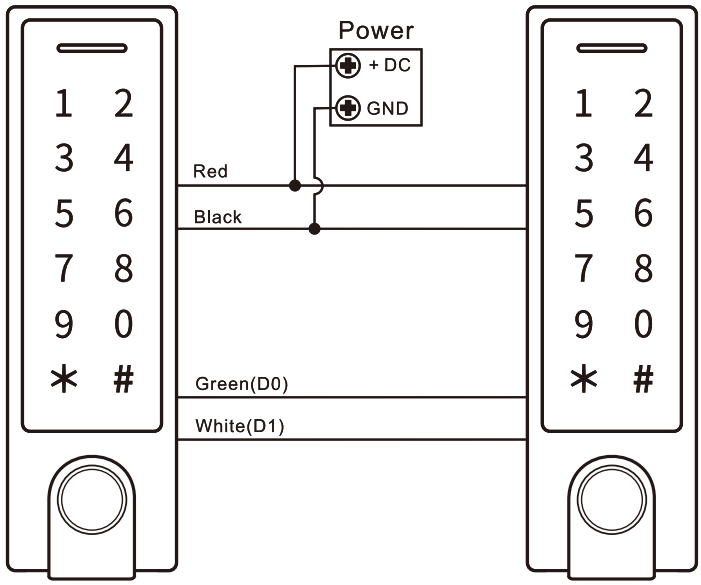
3. Salir del modo de programación: *

Transferir información de usuario

Para usuarios registrados con PIN/tarjeta.

La información del usuario se puede transferir de un teclado a otro.

Diagrama de conexión



Notas:

Ambos teclados deben ser de la misma serie.

El código maestro de ambos teclados debe ser idéntico.

Active la función de transferencia solo en el teclado principal (teclado maestro).

Si el teclado secundario ya tiene usuarios registrados, se sobrescribirán durante la transferencia.

Para un número de 900 usuarios, la transferencia podría tardar hasta 30 segundos.

Active el modo de transferencia en el teclado maestro.

1. Acceda al modo de programación: * código maestro #

2. Marque 9 8 #

Durante 30 segundos, la duración máxima de la

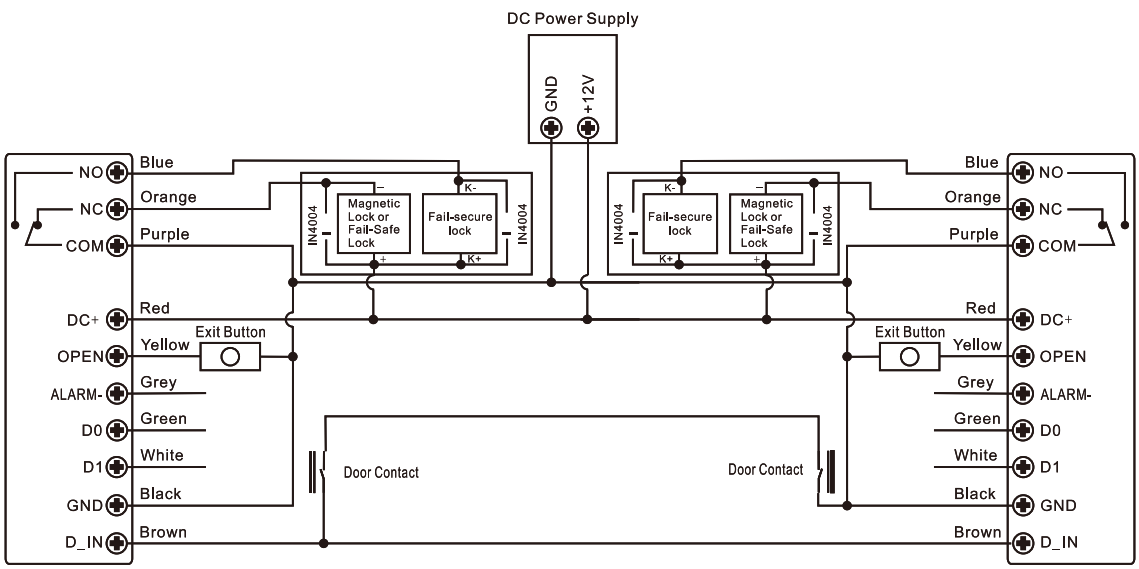
transferencia, el LED verde se enciende. Al finalizar la transferencia de datos, se oye un pitido y se enciende el LED rojo.

3. Salga del modo de programación: *

Interconexión de teclados

Este modo implica interconectar dos teclados para controlar dos puertas. Esta función es especialmente útil en prisiones, bancos y otros lugares donde se requiere un mayor nivel de seguridad.

Diagrama de conexión



Registre a los usuarios en el teclado A y luego transfiéralos al teclado B.

Habilite el modo de interbloqueo en ambos teclados:

1. Ingrese al modo de programación: * código maestro #

2.1. Deshabilitar función: 9 0 # (predeterminado)

2.2. Habilitar función: 9 1 #

3. Salir del modo de programación: *

Cuando la función está activa, si la puerta 2 necesita permanecer cerrada, el usuario puede escanear la huella dactilar/tarjeta o ingresar el PIN en el teclado A. La puerta 1 se abrirá. Si la puerta 1 necesita permanecer cerrada, el usuario puede escanear la huella dactilar/tarjeta o ingresar el PIN en el teclado B. La puerta 2 se abrirá.

Cuando la función está activa, el usuario puede escanear la huella dactilar/tarjeta o introducir el PIN en el teclado A para abrir la puerta 1. O bien, puede escanear la huella dactilar/tarjeta o introducir el PIN en el teclado B para abrir la puerta 2.

Control mediante teclado desde la app Tuya Smart

Nota: Debido a las frecuentes actualizaciones de la app Tuya Smart, las imágenes y la información de este manual pueden diferir de las de la versión instalada en su dispositivo.

Vaya a Google Play o App Store o escanee el código QR a continuación e instale la aplicación Tuya Smart.

Conecta tu teléfono a la red wifi, activa la ubicación y el Bluetooth.

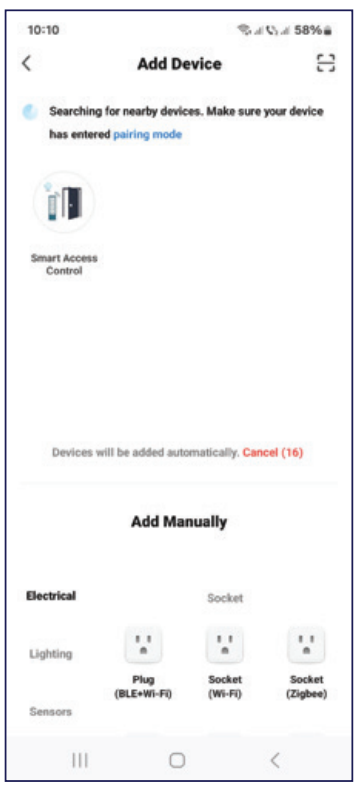
Abre la app e inicia sesión.

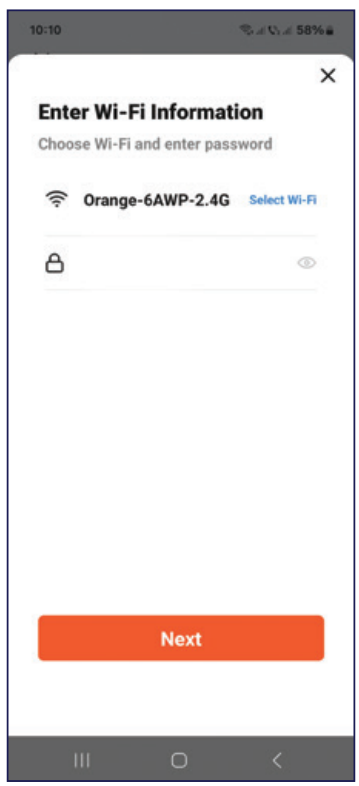
Pulsa “+” - “Añadir dispositivo” .

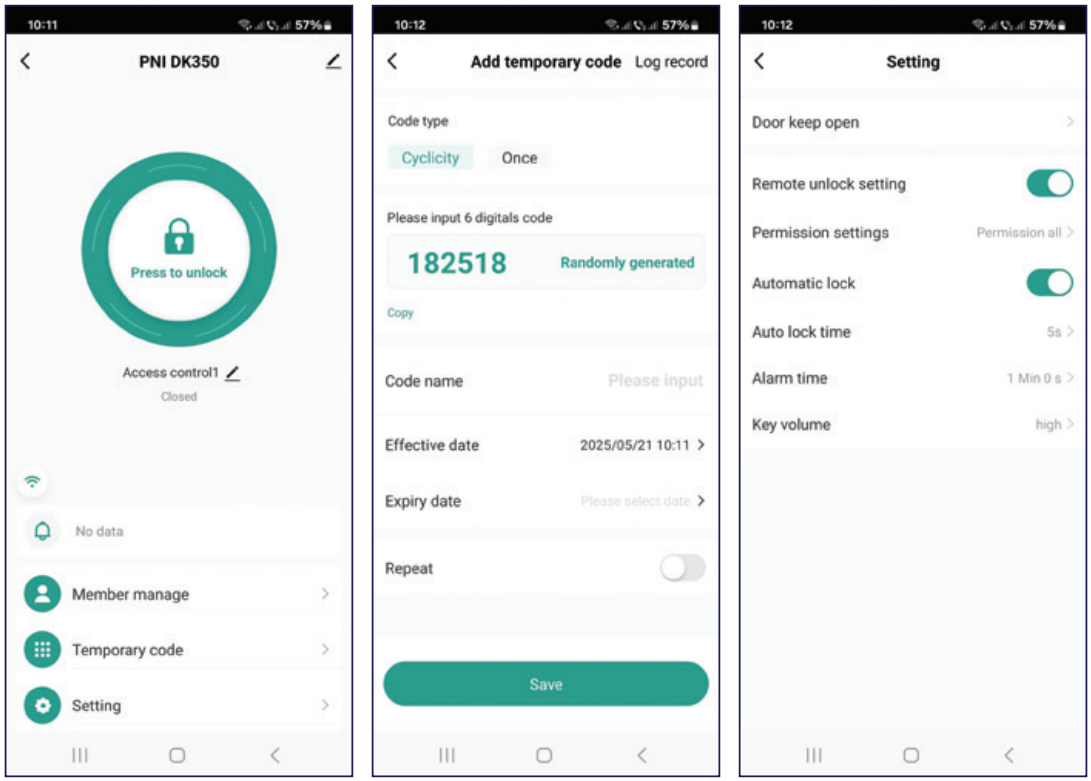
La app identificará tu dispositivo automáticamente.

Pulsa el icono del teclado y sigue las instrucciones en pantalla.

Nota: También puedes añadir el teclado manualmente a la app accediendo a la categoría Cámaras y Bloqueo - Bloqueo (Wi-Fi).







La aplicación permite desbloquear la puerta, agregar y administrar usuarios y generar un código de acceso temporal.

Fonctionnalités de base

Capteur d'empreintes digitales.

Touches tactiles.

Boîtier métallique étanche (IP66).

Prend en charge 1000 utilisateurs locaux (988 utilisateurs communs, 2 utilisateurs d'urgence, 10 utilisateurs temporaires).

Prend en charge 500 utilisateurs via l'application.

Prend en charge les cartes EM 125 kHz.

Sortie alarme et buzzer.

Fonction anti-vandalisme.

Plusieurs méthodes d'accès : empreinte digitale, carte, code PIN, application.

Prise en charge des mots de passe temporaires (à usage unique ou temporaire).

Prise en charge de l'ajout/suppression d'utilisateurs via l'application.

Prise en charge de la définition de restrictions horaires pour les utilisateurs.

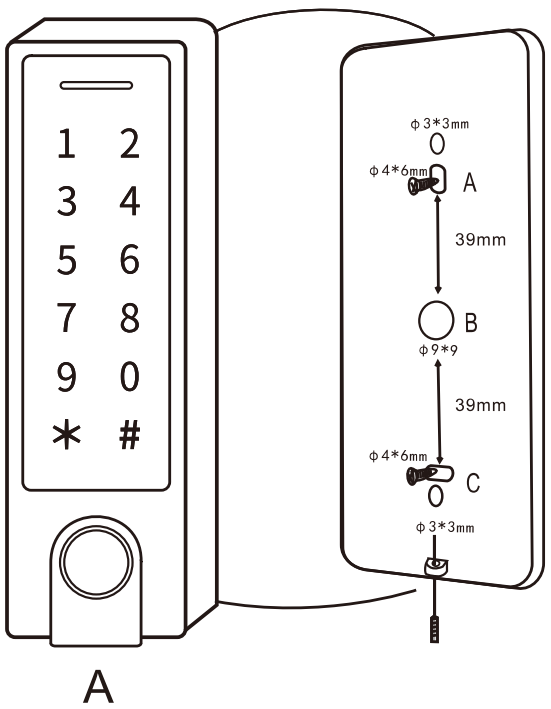
Spécifications techniques

Tension de fonctionnement	12-18V DC

Consommation en veille	≤60mA
Consommation de fonctionnement	≤150mA
Carte RFID compatible	EM 125 KHz
Distance de lecture de la carte RFID	2-6 cm
Connexions de sortie	Relais, bouton d'accès, alarme, contact de porte, lecteur de carte Wiegand
Connexions d'entrée	Lecteur de carte Wiegand
Relais	Un relais NO, NC, COM
Durée de fonctionnement du relais	0-99 s (5 s par défaut)
Charge de sortie de verrouillage	Max. 2 A
Sortie code PIN	4 bits, numéro virtuel de 10 caractères
Indice de protection	IP66

Température de fonctionnement	-26 ~ 80 °C
Matériau du boîtier	Alliage de zinc
Dimensions	148 x 44 x 22 mm
Wi-Fi	2.4 GHz/100mW
Bluetooth	2.4 GHz/2.5mW

Installation



Retirez le support à l'arrière de l'appareil.

Fixez le support au mur à l'aide des vis fournies.

Faites passer le câble de connexion par le trou marqué B sur le schéma ci-dessous.

Fixez l'appareil au support..

Connexions

Couleur du fil	**Function**	**Remarques**

Rouge	DC+	Entrée CC 12-18 V
Noir	GND	Entrée CC pôle négatif
Bleu	NO	Sortie relais NO (connecter la diode du boîtier)
Violet	COM	Sortie relais COM
Orange	NC	Sortie relais NF (connecter la diode du boîtier)
Jaune	OPEN	Entrée bouton d'accès
Connexions via un lecteur ou un contrôleur Wiegand		
Vert	Data 0	Sortie Wiegand (pass-through)
Blanc	Data 1	Sortie Wiegand (pass-through)
Connexions spéciales		
Gris	Sortie d'alarme	Contact négatif pour alarme
Marron	Entrée	Entrée contact de porte

Avertissements sonores et lumineux

État	LED	Buzzer
Veille	LED rouge	-
Entrée en mode programmation	LED rouge clignotante	Un bip
Mode programmation	LED orange	Un bip
Erreur de fonctionnement	-	Trois bips
Sortie du mode programmation	LED rouge	Un bip
Ouverture de la porte	LED verte	Un bip
Alarme	LED rouge clignotante rapidement	Bips

Entrée et sortie du mode programmation

Entrée en mode programmation : * code maître #

Remarque : le code maître par défaut est 123456.

Sortie du mode programmation : *

Définition du code maître

1. Entrée en mode programmation : * code maître #

2. Modification du code maître : 0 (nouveau code maître) # (répéter le nouveau code maître) #

Remarque : le code maître doit contenir 6 caractères.

3. Sortie du mode programmation : *

Réglage du mode de fonctionnement

Il existe 3 modes de fonctionnement : le mode autonome, le mode contrôleur et le mode lecteur Wiegand. Le mode par défaut est le mode autonome/ contrôleur.

1. Entrée en mode programmation : * code maître #

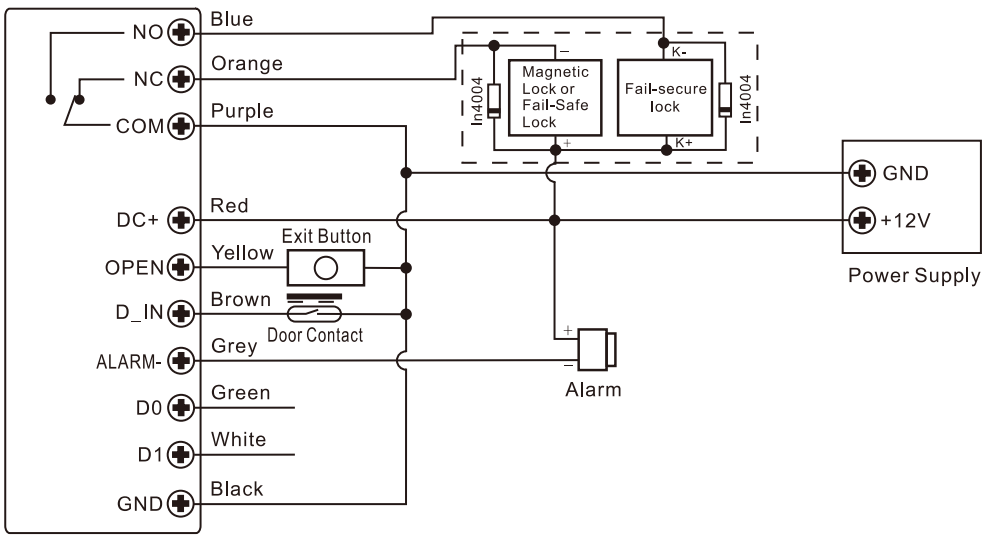
2. Saisissez 7 7# (mode par défaut) ou 7 8# (mode Wiegand).

3. Sortie du mode programmation : *

1. Mode autonome

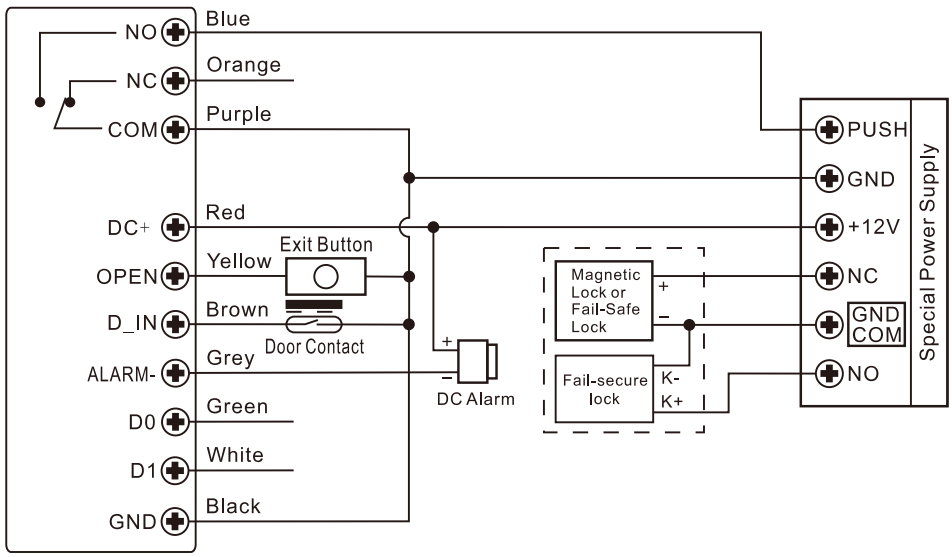
Schéma de raccordement

Alimentation commune :



Attention: it is necessary to install the included 1N4004 diode or equivalent if you are using a power supply to which other devices are connected.

Separate power supply:



Programmation

La programmation diffère selon le mode d'accès.

Remarques :

1. Identifiant utilisateur : Attribuez un identifiant utilisateur à chaque empreinte digitale, code PIN ou carte d'accès pour une meilleure gestion des informations d'accès.

Identifiant utilisateur commun :

Identifiant utilisateur par empreinte digitale : 0-98

Identifiant utilisateur par code PIN ou carte : 100-987

Identifiant utilisateur maître : 99

Identifiant utilisateur en cas d'urgence : 988-989

Identifiant utilisateur visiteur : 990-999

Important : L'identifiant utilisateur ne doit pas être précédé de 0 (zéro). L'enregistrement des identifiants utilisateur est très important. Pour modifier un utilisateur, il est nécessaire de connaître son identifiant.

2. Carte : Le système prend uniquement en charge les cartes EM RFID 125 kHz.

3. Code PIN : Peut contenir de 4 à 6 caractères, à l'exception de la séquence 8888 qui est réservée.

Ajouter une empreinte digitale utilisateur standard

1. Accéder au mode de programmation : * code maître #

2.1. Ajout d'empreintes digitales à l'aide de l'identifiant automatiquement attribué : 1 (lecture de l'empreinte digitale) (relecture répétée de l'empreinte digitale) (relecture répétée de l'empreinte digitale)

Remarque : les empreintes digitales peuvent être ajoutées en continu.

2.2 Ajout d'empreintes digitales à l'aide de l'identifiant personnalisé : 1 (identifiant utilisateur) # (lecture de l'empreinte digitale) (relecture répétée de l'empreinte digitale) (relecture répétée de l'empreinte digitale). Remarque : les empreintes digitales peuvent être ajoutées en continu.

3. Sortie du mode programmation : *

Ajout d'une carte utilisateur standard

1. Accès au mode programmation : * code maître #

2.1. Ajout d'une carte utilisateur à l'aide de l'identifiant automatiquement attribué : 1 (lecture de la carte ou saisie manuelle du numéro de carte) #

Remarque : les empreintes digitales peuvent être ajoutées en continu.

2.2 Ajout d'une carte utilisateur à l'aide d'un identifiant personnalisé : 1 (identifiant utilisateur) (scanner la carte ou saisie manuelle du numéro de carte) #

2.3 Ajout groupé de cartes : permet à l'utilisateur maître d'ajouter jusqu'à 888 cartes en une seule étape. La procédure prend jusqu'à 2 minutes : 1 (identifiant utilisateur) # (nombre de cartes) # (saisir manuellement le premier numéro de carte) #

Remarques :

1. Le nombre de cartes correspond au nombre de cartes que vous souhaitez ajouter au système.

2. Les numéros de carte doivent être consécutifs.

Ajouter un code PIN utilisateur standard

1. Accéder au mode programmation : * code maître #

2.1. Ajouter un code PIN utilisateur à l'aide de l'identifiant attribué automatiquement : 1 (code PIN)

#

2.2. Ajouter un code PIN utilisateur à l'aide de l'identifiant personnalisé : 1 (identifiant utilisateur) # (code PIN) #

3. Quitter le mode programmation : *

Pour plus de sécurité, vous pouvez masquer le code PIN (6 caractères maximum) en saisissant jusqu'à 10 caractères.

Par exemple :

Si le code PIN correct est : 123434

Saisissez : **123434** ou **123434, où ** peut être un nombre compris entre 0 et 9.

Ajouter l'empreinte digitale de l'utilisateur principal

1. Entrer en mode programmation : * code maître #

2. Ajouter l'empreinte digitale : 1 (99) # (lecture de l'empreinte) (répéter la lecture de l'empreinte) (répéter la lecture de l'empreinte)

3. Quitter le mode programmation : *

Ajouter un utilisateur en mode panique

1. Entrer en mode programmation : * code maître #

2.1. Ajouter une carte : 1 (identifiant utilisateur) # (lecture de la carte ou saisie manuelle du numéro de carte) #

2.2 Ajouter un code PIN : 1 (identifiant utilisateur) # (code PIN) #

3. Quitter le mode programmation : *

Ajouter un utilisateur visiteur

Un maximum de 10 visiteurs peuvent être ajoutés avec un code PIN ou une carte. Les visiteurs peuvent utiliser le code PIN ou la carte un maximum de 10 fois. Après un maximum de 10 utilisations, le code PIN ou la carte devient automatiquement invalide. 1. Accéder au mode de programmation : * code maître #

2.1. Ajouter une carte : 1 (identifiant utilisateur) # (0~9) # (lire la carte ou saisir manuellement le numéro de carte) #

2.2. Ajouter un code PIN : 1 (identifiant utilisateur) # (0~9) # (code PIN) #

3. Quitter le mode de programmation : *

Supprimer un utilisateur

1. Accéder au mode de programmation : * code maître #

2.1. Supprimer un utilisateur par empreinte digitale, carte ou code PIN : 2 (lire l'empreinte digitale/lire la carte/saisir le code PIN) #

2.2 Supprimer un utilisateur par numéro d'identifiant : 2 (identifiant utilisateur) #

2.3 Supprimer un utilisateur par numéro de carte : 2

(saisir le numéro de carte) #

2.4. Supprimer tous les utilisateurs : 2 (code maître) #

3. Quitter le mode programmation : *

Configuration du mode d'activation du relais

La configuration du relais influence son comportement après la saisie du code d'accès.

1. Entrer en mode programmation : * code maître #

2.1. Mode impulsion (mode par défaut) : 3 (1 à 99) #

Le relais est activé pendant une durée comprise entre 0 et 99 secondes (5 secondes par défaut) après la saisie du code, puis se désactive automatiquement.

La durée d'activation du relais est comprise entre 1 et 99 secondes. Par défaut : 5 secondes.

2.2. Mode alterné : 3 0 #

Le relais change d'état à chaque saisie correcte du code :

S'il est éteint (ouvert), il s'active (ferme le contact). S'il est activé, il se désactive.

Utile pour les portails ou portes qui doivent rester ouverts jusqu'à leur fermeture manuelle.

3. Sortie du mode programmation : *

Paramètres du mode d'accès

En mode multi-utilisateurs, l'intervalle de lecture des

codes d'accès ne doit pas dépasser 5 secondes. Après 5 secondes, l'appareil se met automatiquement en veille.

1. Entrée en mode programmation : * code maître #

2.1. Accès par empreinte digitale : 4 0 #

2.2. Accès par carte : 4 1 #

2.3. Accès par code PIN : 4 2 #

2. 4. Accès multi-utilisateurs : 4 3 (2 à 9) #

La porte ne s'ouvre qu'après la validation de 2 à 9 utilisateurs.

2.5. Empreinte digitale, carte ou code PIN (par défaut) : 4 4 #

3. Sortie du mode programmation : *

Alarme pour tentatives infructueuses répétées

L'alarme se déclenche après 10 tentatives d'accès incorrectes consécutives (saisie d'un code erroné, carte non valide, etc.). Elle peut être configurée pour refuser l'accès pendant 10 minutes ou pour l'autoriser uniquement après la saisie d'un code, d'une carte ou d'une empreinte digitale valide.

1. Accéder au mode programmation : * code maître #

2.1. Fonction désactivée (par défaut) : 6 0 #

2.2. Fonction activée : 6 1 # (accès interdit pendant 10 minutes)

2.3. Fonction activée (alarme) : 6 2 #

Durée de l'alarme : 5 (0 à 3) #. Par défaut : 1 minute.

Pour arrêter l'alarme, saisissez le code maître #, scannez l'empreinte/la carte du maître, le code PIN ou scannez l'empreinte/la carte d'un utilisateur.

3. Quitter le mode programmation : *

Avertissement de porte ouverte

Si vous avez connecté un contact magnétique filaire au clavier de contrôle d'accès et que la porte reste ouverte plus d'une minute, le buzzer intégré retentit pour rappeler à l'utilisateur de fermer la porte. Le signal sonore peut être arrêté en fermant la porte ou en saisissant un code d'accès valide (maître ou utilisateur). Sinon, le signal sonore continue tant qu'il est activé.

Alerte porte forcée

Si vous avez connecté un contact magnétique filaire au clavier de contrôle d'accès et que la porte est forcée, le buzzer intégré et la sirène extérieure (le cas échéant) déclencheront l'alarme. L'alarme peut être interrompue en fermant la porte ou en saisissant un code d'accès valide (maître ou utilisateur). Sinon, l'alarme continuera tant qu'elle sera activée.

1. Entrer en mode programmation : * code maître #

2.1. Fonction désactivée (par défaut) : 6 3 #

2.2. Fonction activée 6 4 #

Réglage de la durée de l'alarme : 5 (0~3) #. Par défaut : 1 minute.

3. Sortie du mode programmation : *

Réglage du buzzer et des voyants

1. Accès au mode programmation : * code maître #

2.1. Désactivation du buzzer : 7 0 #

2.2. Activation du buzzer (par défaut) : 7 1 #

3.1. Voyant éteint : 7 2 #

3.2. Voyant allumé (par défaut) : 7 3 #

4.1. Clavier éteint : 7 4 #

4.2. Clavier allumé en permanence : 7 5 #

4.3. Clavier éteint automatiquement (par défaut) : 7 6 #. 20 secondes après la dernière utilisation, le clavier s'éteint automatiquement. Appuyez sur n'importe quelle touche pour rallumer le clavier.

3. Sortie du mode programmation : *

Ajout d'une empreinte digitale/carte/code PIN avec une carte principale/empreinte digitale

1. Lisez la carte principale/empreinte digitale.

2. Scannez l'empreinte digitale de l'utilisateur trois fois ou scannez sa carte ou son code PIN.

Répétez l'étape 2 pour ajouter d'autres utilisateurs

consécutivement.

3. Scannez à nouveau la carte principale/empreinte digitale.

Suppression d'une empreinte digitale/carte/code PIN avec une carte principale/empreinte digitale

1. Scannez la carte principale/empreinte digitale deux fois en 5 secondes maximum.

2. Scannez l'empreinte digitale/carte ou saisissez le code PIN de l'utilisateur.

Répétez l'étape 2 pour supprimer d'autres utilisateurs consécutivement.

3. Scannez à nouveau la carte principale/empreinte digitale.

Réinitialisation et ajout d'une carte principale

Si vous avez connecté un bouton d'accès au clavier de contrôle d'accès, procédez comme suit pour réinitialiser le clavier :

1. Éteignez l'appareil.

2. Maintenez le bouton d'accès enfoncé tout en le rallumant.

3. Deux bips sonores retentissent. 4. Retirez votre doigt du bouton d'accès.

5. La LED jaune s'allume.

6. Lisez n’importe quelle carte EM 125 kHz.

7. La LED s’allume en rouge.

8. Le clavier a été réinitialisé.

9. La carte lue est devenue la carte maître.

Remarques :

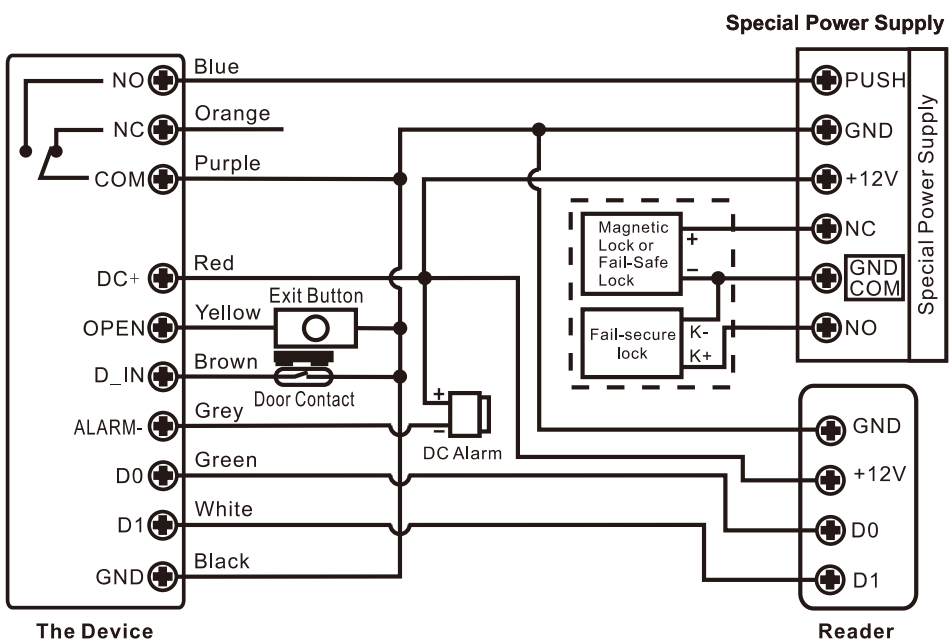
1. Si vous ne souhaitez pas ajouter de carte maître, maintenez le bouton d’accès enfoncé pendant au moins 5 secondes avant de le relâcher. Cette procédure invalidera l’ancienne carte maître.

2. La réinitialisation ne supprime pas les informations utilisateur.

2. Mode contrôleur

Le clavier fonctionnera comme un contrôleur s’il est connecté à un lecteur Wiegand..

Schéma de connexion



Attention : il est nécessaire d'installer la diode 1N4004 fournie ou équivalente si vous utilisez une alimentation à laquelle d'autres appareils sont connectés.

Paramétrage du format d'entrée Wiegand

1. Accéder au mode de programmation : * code maître #

2. Définir les bits d'entrée Wiegand pour la carte EM :

8 (26~44) # (par défaut : 26 bits)

3.1. Désactiver le bit de parité : 8 0 #

3.2. Activer le bit de parité : 8 1 #

3. Quitter le mode de programmation : *

Programmation

La programmation de base est la même qu'en mode autonome.

Connexion à un lecteur de cartes externe

Avec un lecteur de cartes EM ou Mifare, l'ajout/la suppression d'utilisateurs peut se faire à la fois sur le clavier et sur le lecteur externe.

Avec un lecteur de cartes HID, l'ajout/la suppression d'utilisateurs peut se faire uniquement sur le lecteur externe.

Connexion à un lecteur d'empreintes digitales

Connecter le lecteur d'empreintes digitales au clavier.

1. Accéder au mode de programmation : * code maître

#

2.1. Type 1 (lecture de l'empreinte digitale sur le lecteur d'empreintes digitales) #. L'identifiant est automatiquement attribué.

2.2. Type 1 (identifiant utilisateur) # (lecture de l'empreinte digitale sur le lecteur d'empreintes digitales) #

3. Quitter le mode programmation : *

Connexion à un lecteur à clavier

Le lecteur à clavier peut être de 4 bits, 8 bits (ASCII) ou 10 bits.

1. Entrer en mode programmation : * code maître #

2.1. Saisir le nombre de bits : 8 (4, 8 ou 10) #. La valeur par défaut est 4 bits.

3. Quitter le mode programmation : *

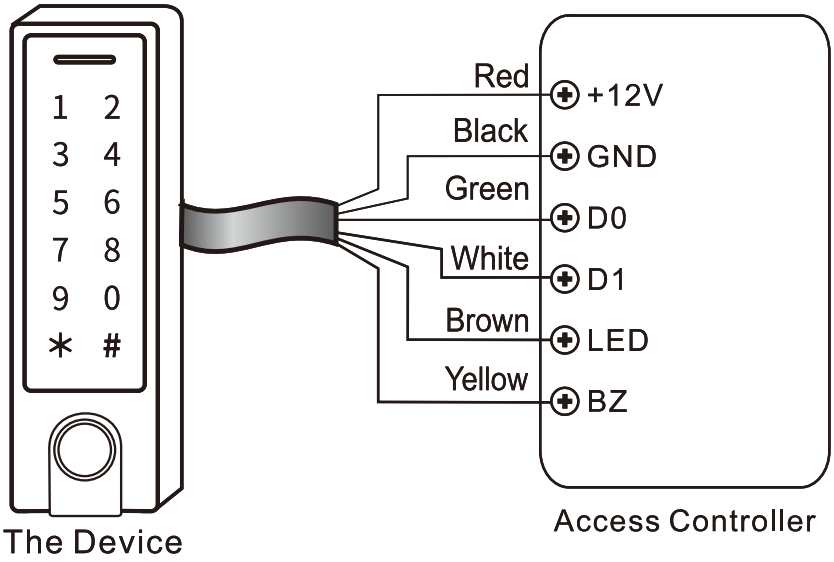
Ajouter/Supprimer un code PIN utilisateur

Le code PIN utilisateur peut être ajouté/supprimé sur le clavier de contrôle d'accès et sur le lecteur à clavier externe.

3. Mode lecteur Wiegand

Le clavier peut également fonctionner comme un lecteur Wiegand standard connecté à un contrôleur externe.

Schéma de connexion



Lorsque le clavier est en mode lecteur Wiegand, tous les réglages effectués en mode contrôleur deviennent invalides. Les fils jaune et gros seront redéfinis comme suit :

Fil marron : Contrôle de la LED verte

Fil jaune : Contrôle du buzzer

Paramètre du format de sortie Wiegand

1. Accéder au mode programmation : * code maître #

2. Définir les bits Wiegand pour la carte EM : 8 (26~44) #

3.1. Désactiver le bit de parité : 8 0 #

3.2. Activation du bit de parité : 8 1 # (par défaut)

3. Quitter le mode programmation : *

Remarque : pour connecter un contrôleur Wiegand, vous devez désactiver le bit de parité.

Applications avancées

Accès toutes cartes

Après activation de ce mode, toutes les cartes peuvent ouvrir la porte. La carte est ajoutée simultanément au système.

1. Accéder au mode programmation : * code maître #

2.1. Désactiver la fonction : 9 2 # (par défaut)

2.2. Activation de la fonction : 9 3 #

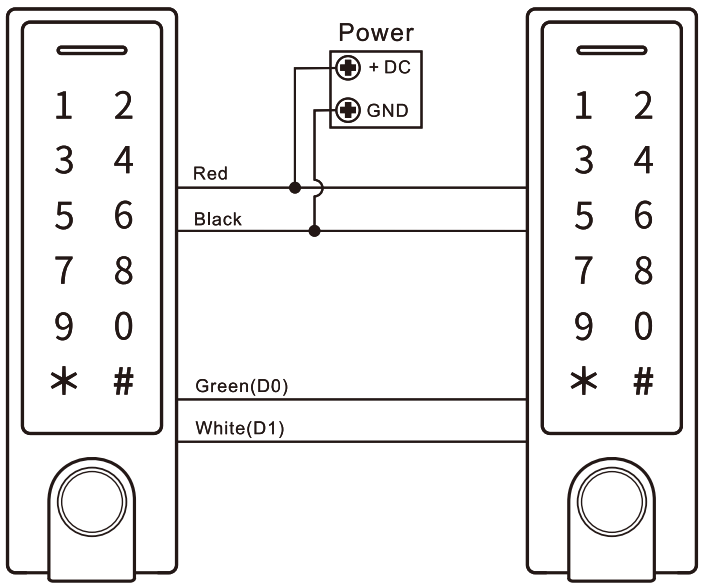
3. Quitter le mode programmation : *

Transfert des informations utilisateur

Pour les utilisateurs enregistrés avec code PIN/carte.

Les informations utilisateur peuvent être transférées d'un clavier à un autre.

Schéma de connexion



Remarques :

Les deux claviers doivent être de la même série.

Le code maître des deux claviers doit être identique.

Activez la fonction de transfert uniquement sur le clavier principal (clavier maître).

Si des utilisateurs sont déjà enregistrés sur le clavier secondaire, ils seront écrasés lors du transfert.

Pour un nombre d'utilisateurs supérieur à 900, le transfert peut prendre jusqu'à 30 secondes.

Activez le mode transfert sur le clavier maître

1. Entrez en mode programmation : * code maître #

2. Tapez 9 8 #

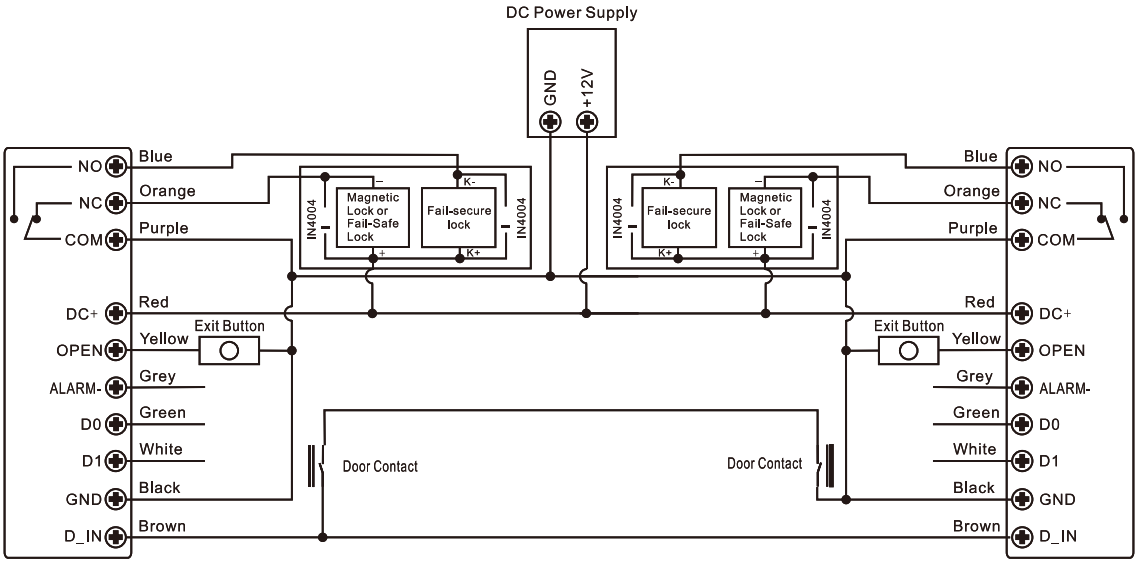
Pendant 30 secondes, durée maximale du transfert, la LED verte est allumée. Une fois le transfert terminé, un bip retentit et la LED rouge s'allume.

3. Quittez le mode programmation : *

Interconnexion de claviers

Ce mode permet d'interconnecter deux claviers pour contrôler deux portes. Cette fonction est particulièrement utile dans les prisons, les banques et autres lieux exigeant un niveau de sécurité élevé..

Schéma de connexion



Enregistrez les utilisateurs sur le clavier A, puis transférez-les sur le clavier B.

Activez le mode verrouillage sur les deux claviers :

1. Entrez en mode programmation : * code maître #

2.1. Désactivez la fonction : 9 0 # (par défaut)

2.2. Activez la fonction : 9 1 #

3. Quittez le mode programmation : *

Lorsque la fonction est activée, lorsque la porte 2 doit rester fermée, l'utilisateur peut scanner son empreinte digitale/carte ou saisir son code PIN sur le clavier A. La porte 1 s'ouvre. Lorsque la porte 1 doit rester fermée, l'utilisateur peut scanner son empreinte digitale/carte ou saisir son code PIN sur le clavier B. La porte 2 s'ouvre.

Lorsque la fonction est activée, l'utilisateur peut scanner son empreinte digitale/carte ou saisir son

code PIN sur le clavier A pour ouvrir la porte 1. Ou scanner son empreinte digitale/carte ou saisir son code PIN sur le clavier B pour ouvrir la porte 2.

Contrôle du clavier depuis l'application Tuya Smart

Remarque : En raison des mises à jour fréquentes de l'application Tuya Smart, les images et les informations présentées dans ce manuel peuvent différer de celles de la version installée sur votre appareil..

Accédez à Google Play ou à l'App Store ou scannez le code QR ci-dessous et installez l'application Tuya Smart.

Connectez votre téléphone au Wi-Fi, activez la localisation et le Bluetooth.

Ouvrez l'application et connectez-vous.

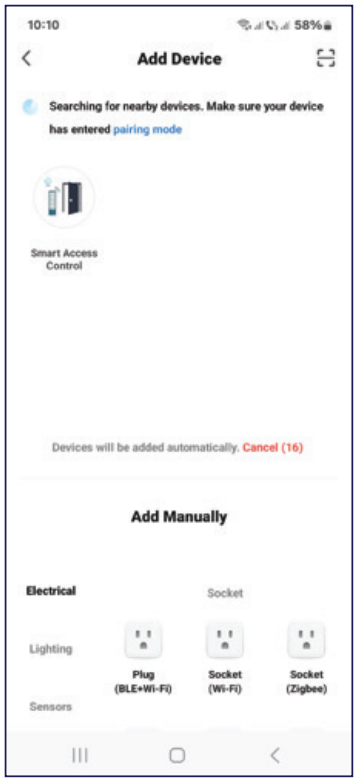
Appuyez sur « + » - « Ajouter un appareil » .

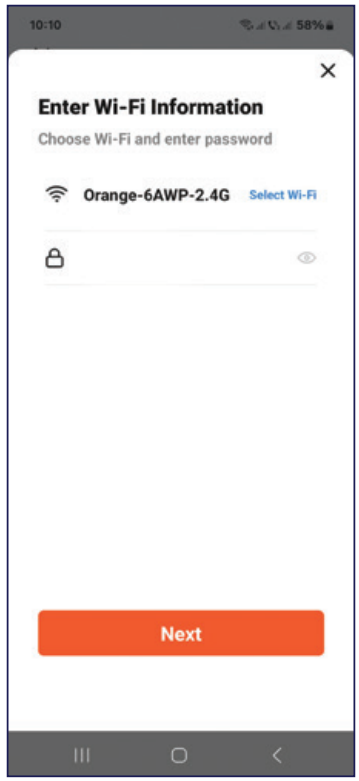
L'application identifiera automatiquement votre appareil.

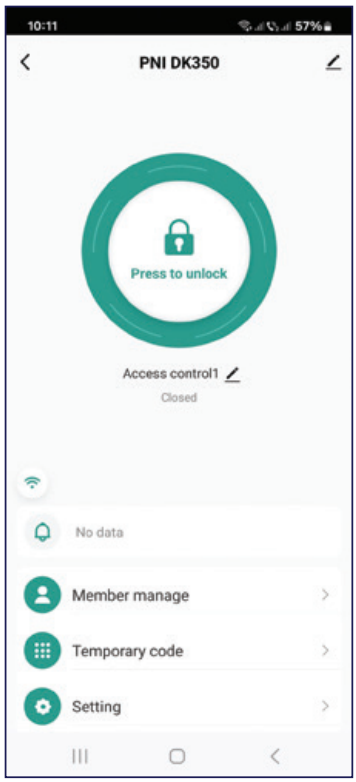
Appuyez sur l'icône du clavier et suivez les étapes à l'écran.

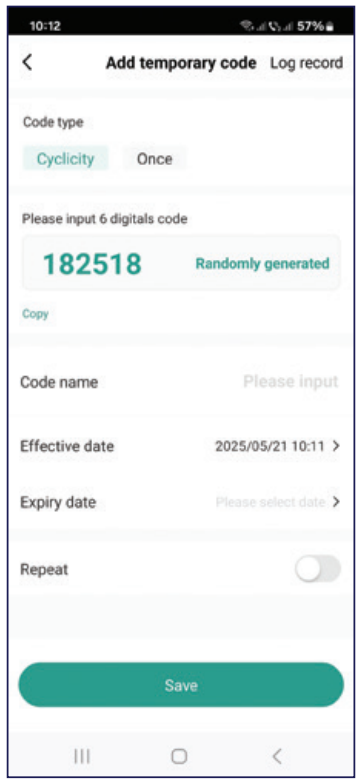
Remarque : vous pouvez également ajouter manuellement le clavier à l'application en accédant

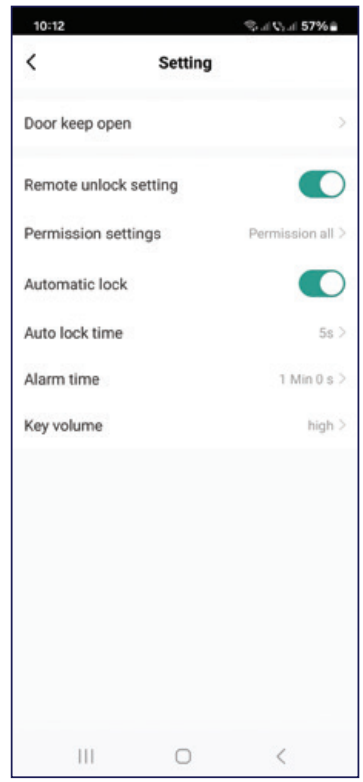
à la catégorie « Caméras et verrouillage » - « Verrouillage (Wi-Fi) ».











L’application vous permet de déverrouiller la porte,

d’ajouter et de gérer les utilisateurs et de générer un code d’accès temporaire.

Alapvető jellemzők

Ujjlenyomat-érzékelő.

Érintőgombok.

Vízálló fémház (IP66).

1000 helyi felhasználót támogat (988 közös felhasználó, 2 pánikfelhasználó, 10 ideiglenes felhasználó).

500 felhasználót támogat alkalmazáson keresztül.

125 kHz-es EM kártyát támogat.

Riasztási és berregő kimenet. Vandalizmus elleni funkció. Több hozzáférési mód: ujjlenyomat, kártya, PIN, alkalmazás.

Ideiglenes jelszó támogatása (egyszeri vagy időszakos).

Felhasználók hozzáadásának/törlésének támogatása alkalmazáson keresztül.

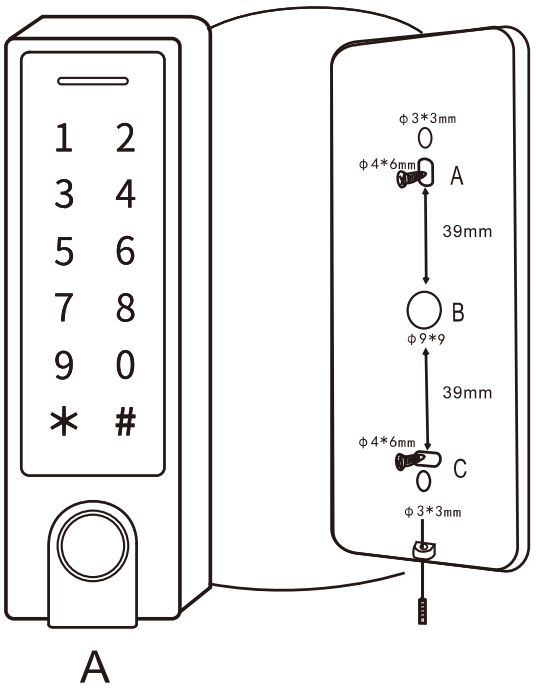
Időbeli korlátozások beállításának támogatása a felhasználók számára.

Műszaki adatok

Üzemi feszültség	12-18V DC
Készenléti teljesítmény	≤60mA
Üzemi teljesítmény	≤150mA
Kompatibilis RFID kártya	EM 125 KHz

RFID kártya olvasási távolsága	2-6 cm
Kimeneti csatlakozók	Relé, hozzáférési gomb, riasztó, ajtónyitás-érzékelő, Wiegand kártyaolvasó
Bemeneti csatlakozók	Wiegand kártyaolvasó
Relé	Egy relé NO, NC, COM
Relé működési ideje	0-99 s. (5 s. alapértelmezett)
Zár kimenet terhelése	Max. 2A
PIN kimenet	4 bit, 10 karakteres virtuális szám
Védettségi fokozat	IP66
Üzemi hőmérséklet	-26 ~ 80°C
Ház anyaga	Cinkötvözet
Méretek	148 x 44 x 22 mm
Wi-Fi	2.4 GHz/100mW
Bluetooth	2.4 GHz/2.5mW

Telepítés



A

Távolítsa el a konzolt az egység hátuljáról.

Rögzítse a konzolt a falhoz a mellékelt csavarokkal. Vezesse át a csatlakozókábelt az alábbi rajzon B-vel jelölt lyukon.

Rögzítse az egységet a konzolhoz.

Kapcsolatok

Vezeték színe	**Funkció**	**Megjegyzések**
Piros	DC+	12–18 V-os egyenáramú bemenet
Fekete	GND	Negatív pólusú egyenáramú bemenet
Kék	NO	NO relé kimenet (csatlakoztassa a csomagban található diódát)
Lila	COM	COM relé kimenet

Naran cssárga	NC	NC relé kimenet (csatlakoztassa a csomagban található diódát)
Sárga	OPEN	Hozzáférés gomb bemenet
Csatlakozások Wiegand olvasón vagy vezérlőn keresztül		
Zöld	Data 0	Wiegand kimenet (pass-through)
Fehér	Data 1	Wiegand kimenet (pass-through)
Speciális kapcsolatok		
Szürke	Riasztás kimenet	Negatív érintkező riasztáshoz
Barna	Bemenet	Ajtóérintkező bemenet

Hang- és fényjelzések

Állapot	**LED**	**Csengő**
Készenlét	Piros LED	-

Belépés programozási módba	Piros LED villog	Egy sípolás
Programozási mód	Narancssárga LED	Egy sípolás
Működési hiba	-	Három sípolás
Kilépés programozási módból	Piros LED	Egy sípolás
Ajtónyitás	Zöld LED	Egy sípolás
Riasztás	Piros LED gyorsan villog	Sípolás

Belépés és kilépés a programozási módból

Belépés a programozási módba: * mesterkód #

Megjegyzés: az alapértelmezett mesterkód 123456.

Kilépés a programozási módból: *

Mesterkód beállítása

1. Belépés a programozási módba: * mesterkód #

2. Mesterkód módosítása: 0 (új mesterkód)# (ismételje meg az új mesterkódot)#

Megjegyzés: a mesterkódnak 6 karakterből kell állnia.

3. Kilépés a programozási módból: *

Az üzemmód beállítása

3 üzemmód létezik: önálló mód, vezérlő mód és Wiegand olvasó mód. Az alapértelmezett mód az önálló/vezérlő mód.

1. Lépjen be programozási módba: * mesterkód #

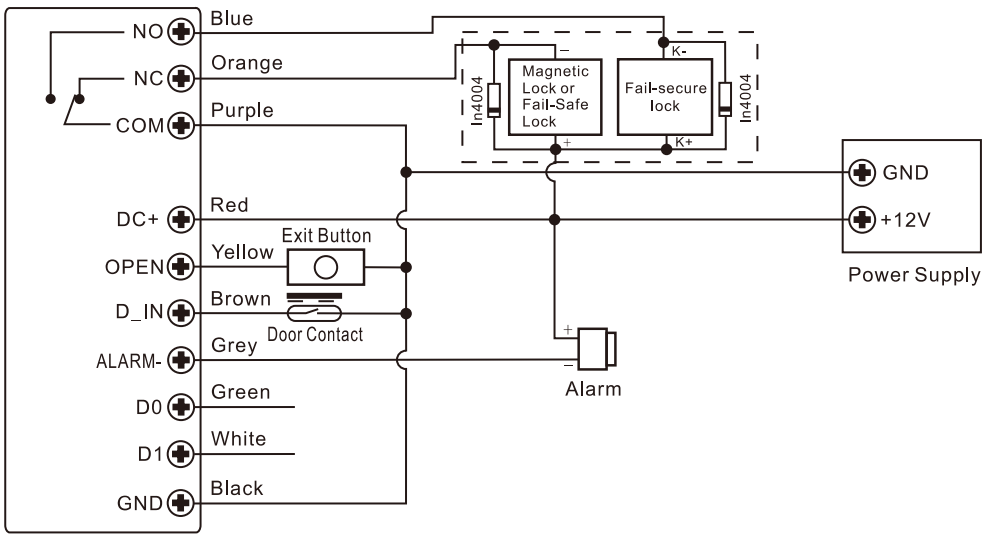
2. Írja be a 7 7# (alapértelmezett mód) vagy a 7 8# (Wiegand mód) kódot.

3. Lépjen ki a programozási módból: *

1. Önálló mód

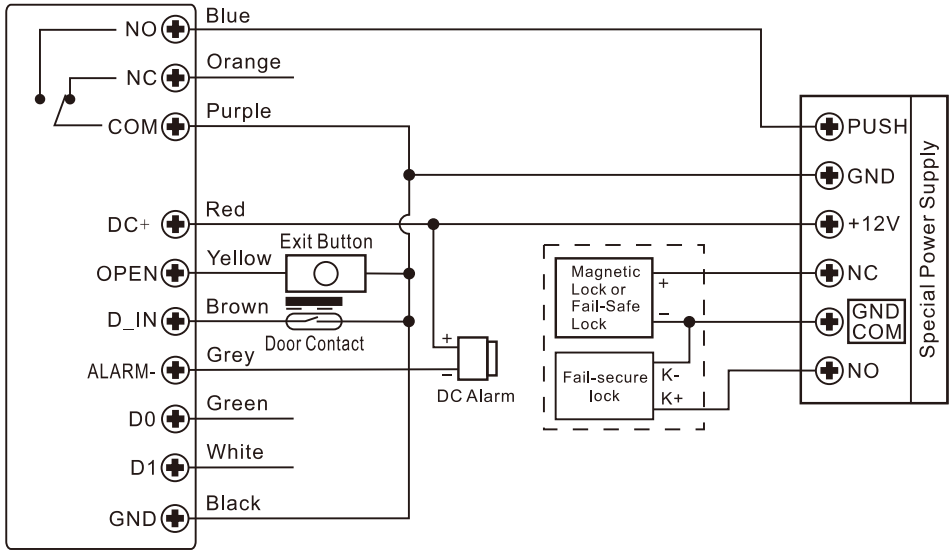
Csatlakoztatási rajz

Közös tápegység:



Figyelem: ha olyan tápegységet használ, amelyhez más eszközök is csatlakoznak, akkor a mellékelt 1N4004 dióda vagy azzal egyenértékű dióda beszerelése szükséges.

Külön tápegység:



Programozás

A programozás a hozzáférési módtól függően eltérő.

Megjegyzések:

1. Felhasználói azonosító: Rendeljen felhasználói azonosítót minden ujjlenyomathoz, PIN-kódhoz vagy belépőkártyához a hozzáférési információk jobb kezelése érdekében.

Közös felhasználói azonosító:

Ujjlenyomat felhasználói azonosító: 0-98

PIN-kód vagy kártya felhasználói azonosító: 100-987

Fő felhasználói azonosító: 99

Pánik felhasználói azonosító: 988-989

Látogató felhasználói azonosító: 990-999

Fontos: A felhasználói azonosító előtt nem állhat 0 (nulla). A felhasználói azonosítók regisztrálása nagyon

fontos. A felhasználó módosításához ismerni kell a felhasználói azonosítót.

2. Kártya: A rendszer csak 125 kHz-es EM RFID kártyákat támogat.

3. PIN: 4-6 karaktert tartalmazhat, kivéve a 8888-as sorozatot, amely foglalt.

Normál felhasználói ujjlenyomat hozzáadása

1. Lépjen be a programozási módba: * mesterkód #

2.1. Felhasználói ujjlenyomat hozzáadása automatikusan hozzárendelt azonosítóval: 1 (ujjlenyomat olvasása) (ujjlenyomat-olvasás ismétlése) (ujjlenyomat-olvasás ismétlése)

Megjegyzés: az ujjlenyomatok folyamatosan hozzáadhatók.

2.2 Felhasználói ujjlenyomat hozzáadása testreszabott azonosítóval: 1 (felhasználói azonosító) # (ujjlenyomat olvasása) (ujjlenyomat-olvasás ismétlése) (ujjlenyomat-olvasás ismétlése). Megjegyzés: az ujjlenyomatok folyamatosan hozzáadhatók.

3. Kilépés a programozási módból: *

Normál felhasználói kártya hozzáadása

1. Lépjen be a programozási módba: * mesterkód #

2.1. Felhasználói kártya hozzáadása automatikusan hozzárendelt azonosítóval: 1 (kártya olvasása vagy a kártyaszám manuális megadása) #

Megjegyzés: az ujjlenyomatok folyamatosan hozzáadhatók.

2.2 Felhasználói kártya hozzáadása személyre szabott azonosítóval: 1 (felhasználói azonosító) (kártya beolvasása vagy a kártyaszám manuális megadása) #

2.3 Kártyák tömeges hozzáadása: lehetővé teszi a mester felhasználó számára, hogy akár 888 kártyát is hozzáadjon egy lépésben. Az eljárás legfeljebb 2 percig tart: 1 (felhasználói azonosító) # (kártya mennyisége) # (manuálisan adja meg az első kártyaszámot) #

Megjegyzések:

1. A kártya mennyisége a rendszerhez hozzáadni kívánt kártyák számát jelöli.

2. A kártyaszámoknak egymást követőnek kell lenniük.

Normál felhasználói PIN-kód hozzáadása

1. Lépjen be programozási módba: * mesterkód #

2.1. Felhasználói PIN-kód hozzáadása automatikusan hozzárendelt azonosítóval: 1 (PIN) #

2.2 Felhasználói PIN-kód hozzáadása egyéni azonosítóval: 1 (felhasználói azonosító) # (PIN) #

3. Kilépés a programozási módból: *

A fokozott biztonság érdekében elrejtheti a PIN-kódot (max. 6 karakter) legfeljebb 10 karakter beírásával.

Például:

Ha a helyes PIN-kód: 123434

Írja be: **123434** vagy **123434, ahol a ** 0 és 9 közötti szám lehet.

Add mester felhasználó ujjlenyomata

1. Lépjen be programozási módba: * mester kód #

2. Ujjlenyomat hozzáadása: 1 (99) # (ujjlenyomat olvasása) (ujjlenyomat-olvasás ismétlése) (ujjlenyomat-olvasás ismétlése)

3. Kilépés a programozási módból: *

Pánik felhasználó hozzáadása

1. Lépjen be programozási módba: * mester kód #

2.1. Kártya hozzáadása: 1 (felhasználói azonosító) # (kártya olvasása vagy kártyaszám manuális megadása) #

2.2 PIN-kód hozzáadása: 1 (felhasználói azonosító) # (PIN) #

3. Kilépés a programozási módból: *

Látogató felhasználó hozzáadása

Maximum 10 látogató adható hozzá PIN-kóddal vagy kártyával. A látogatók maximum 10 alkalommal használhatják a PIN-kódot vagy a kártyát. Maximum 10 használat után a PIN-kód vagy a kártya automatikusan érvénytelenné válik.

1. Lépjen be programozási módba: * mester kód #

2.1. Kártya hozzáadása: 1 (felhasználói azonosító) # (0~9) # (kártya olvasása vagy kártyaszám manuális megadása) #

2.2 PIN-kód hozzáadása: 1 (felhasználói azonosító) # (0~9) # (PIN) #

3. Kilépés a programozási módból: *

Felhasználó törlése

1. Belépés a programozási módba: * mesterkód #

2.1. Felhasználó törlése ujjlenyomat, kártya vagy PIN-kód alapján: 2 (ujjlenyomat olvasása/kártya olvasása/PIN-kód megadása) #

2.2 Felhasználó törlése azonosítószám alapján: 2 (felhasználói azonosító) #

2.3 Felhasználó törlése kártyaszám alapján: 2 (kártyaszám megadása) #

2.4. Összes felhasználó törlése: 2 (mesterkód) #

3. Kilépés a programozási módból: *

Relé aktiválási mód konfigurációja

A relé konfigurációja befolyásolja a viselkedését a hozzáférési kód megadása után.

1. Lépjen be programozási módba: * mesterkód #

2.1. Impulzus mód (alapértelmezett mód): 3 (1~99) #

A relé a kód megadása után 0-99 másodpercig

(alapértelmezett 5 másodperc) aktiválódik, majd automatikusan deaktiválódik.

A relé aktiválási ideje 1-99 másodperc. Alapértelmezett: 5 másodperc.

2.2. Váltakozó mód: 3 0 #

A relé minden alkalommal megváltoztatja az állapotát, amikor a kódot helyesen megadja:

Ha ki van kapcsolva (nyitva), aktiválódik (zárja az érintkezőt). Ha aktiválva van, deaktiválódik.

Hasznos kapuk vagy ajtók esetén, amelyeknek nyitva kell maradniuk, amíg manuálisan be nem zárják őket.

3. Kilépés a programozási módból: *

Hozzáférés mód beállítása

Többfelhasználós hozzáférési mód esetén a hozzáférési kódok beolvasásának időtartama nem haladhatja meg az 5 másodpercet. 5 másodperc elteltével a készülék automatikusan készenléti állapotba lép.

1. Lépjen be programozási módba: * mesterkód #

2.1. Ujjlenyomat-hozzáférés: 4 0 #

2.2. Kártyás hozzáférés: 4 1 #

2.3. PIN-kódos hozzáférés: 4 2 #

2. 4. Többfelhasználós hozzáférés: 4 3 (2~9) #

Csak 2~9 felhasználó érvényesítése után nyílik ki az ajtó.

2.5. Ujjlenyomat vagy kártya vagy PIN (alapértelmezett): 4 4 #

3. Kilépés a programozási módból: *

Riasztás ismételt sikertelen kísérletek esetén

Olyan riasztásra utal, amely 10 egymást követő helytelen hozzáférési kísérlet (rossz kód megadása, érvénytelen kártya stb.) után aktiválódik. Beállítható úgy, hogy 10 percre tiltsa a hozzáférést, vagy csak érvényes kód, kártya vagy ujjlenyomat megadása után engedélyezze a hozzáférést.

1. Lépjen be programozási módba: * mesterkód #

2.1. Funkció letiltva (alapértelmezett): 6 0 #

2.2. Funkció engedélyezve: 6 1 # (a hozzáférés 10 percig tiltott)

2.3. Funkció engedélyezve (Riasztás): 6 2 #

Riasztás időtartamának beállítása: 5 (0~3) #. Alapértelmezett 1 perc.

A riasztás leállításához adja meg a mesterkódot #, vagy olvassa be a mester ujjlenyomatát/kártyáját, vagy adja meg a PIN-kódot, vagy olvassa be a felhasználói ujjlenyomatát/kártyáját.

3. Lépjen ki a programozási módból: *

Ajtónyitás figyelmeztetés

Ha vezetékes mágneses ajtóérintkezőt csatlakoztatott

a beléptetőrendszer billentyűzetéhez, és az ajtó több mint 1 percig nyitva marad, a beépített hangjelzés figyelmezteti a felhasználót az ajtó bezárására. A hangjelzés az ajtó bezárásával vagy érvényes hozzáférési kód (master vagy felhasználói) megadásával állítható le. Ellenkező esetben a hangjelzés addig hallható, amíg be van állítva.

Kényszerített ajtónyitás figyelmeztetés

Ha vezetékes mágneses ajtóérintkezőt csatlakoztatott a beléptetőrendszer billentyűzetéhez, és az ajtót kényszerítik kinyitni, a beépített hangjelzés és a külső sziréna (ha van) megszólaltatja a riasztást. A hangjelzés az ajtó bezárásával vagy érvényes hozzáférési kód (master vagy felhasználói) megadásával állítható le. Ellenkező esetben a hangjelzés addig hallható, amíg be van állítva.

1. Lépjen be programozási módba: * mesterkód #

2.1. Funkció letiltva (alapértelmezett): 6 3 #

2.2. „Funkció engedélyezve” 6 4 #

Riasztás időtartamának beállítása: 5 (0~3) #. Alapértelmezett 1 perc.

3. Kilépés a programozási módból: *

Zümmögő és LED beállítások

1. Lépjen be programozási módba: * mesterkód #

2.1. Zümmögő letiltása: 7 0 #

2.2. Zümmögő engedélyezése (alapértelmezett): 7 1 #

3.1. LED kikapcsolva: 7 2 #

3.2. LED bekapcsolva (alapértelmezett): 7 3 #

4.1. Billentyűzet világítás kikapcsolva: 7 4 #

4.2. Billentyűzet világítás folyamatosan világít: 7 5 #

4.3. Billentyűzet világítás automatikus kikapcsolása (alapértelmezett): 7 6 #. Az utolsó művelet után 20 másodperc elteltével a billentyűzet automatikusan kikapcsol. Bármelyik gomb megérintésére a billentyűzet világít.

3. Kilépés a programozási módból: *

Felhasználói ujjlenyomat/kártya/PIN-kód hozzáadása mesterkártyával/ujjlenyomattal

1. Olvassa le a mesterkártyát/ujjlenyomatot.

2. Olvassa be a felhasználó ujjlenyomatát 3-szor, vagy olvassa be a felhasználói kártyát vagy PIN-kódot.

Ismételje meg a 2. lépést további felhasználók egymást követő hozzáadásához.

3. Olvassa be újra a mesterkártyát/ujjlenyomatot.

Felhasználó ujjlenyomatának/kártyájának/PIN-kódjának törlése mesterkártyával/ujjlenyomattal

1. Olvassa be a mesterkártyát/ujjlenyomatot kétszer,

legfeljebb 5 másodpercen belül.

2. Olvassa be az ujjlenyomatot/kártyát, vagy adja meg a felhasználó PIN-kódját.

Ismételje meg a 2. lépést további felhasználók egymást követő törléséhez.

3. Olvassa be újra a mesterkártyát/ujjlenyomatot.

Alaphelyzetbe állítás és mesterkártya hozzáadása

Ha hozzáférés-vezérlő billentyűzethez csatlakoztatott hozzáférés-vezérlő gombot, a billentyűzet alaphelyzetbe állításához az alábbiak szerint járjon el:

1. Kapcsolja ki a készüléket.

2. Nyomja meg és tartsa lenyomva a hozzáférés-vezérlő gombot, miközben visszakapcsolja a készüléket.

3. 2 sípoló hang hallatszik.

4. Vegye le az ujját a hozzáférés-vezérlő gombról. 5. A sárga LED világít.

6. Olvasson be egy 125 kHz-es EM kártyát.

7. A LED pirosan világít.

8. A billentyűzet visszaállítása megtörtént.

9. A beolvasott kártya lett a mesterkártya.

Megjegyzések:

1. Ha nem szeretne mesterkártyát hozzáadni, legalább 5 másodpercig lenyomva kell tartania a hozzáférés

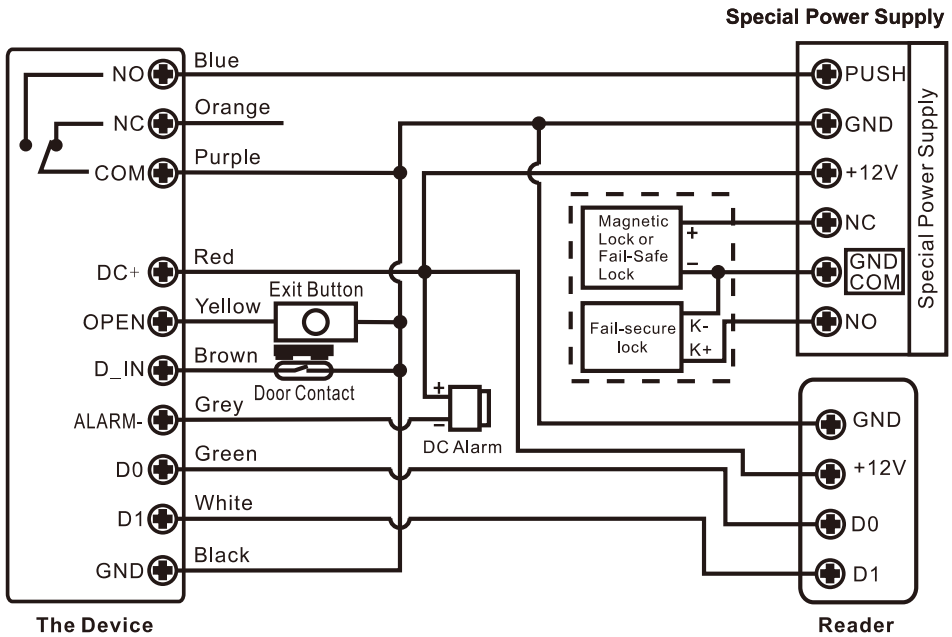
gombot, mielőtt elengedné. Ez az eljárás érvényteleníti a korábbi mesterkártyát.

2. A visszaállítással a felhasználói adatok nem törlődnek.

2. Vezérlő mód

A billentyűzet vezérlőként működik, ha Wiegand olvasóhoz csatlakozik

Csatlakozási rajz



Figyelem: a mellékelt 1N4004 dióda vagy azzal egyenértékű dióda beszerelése szükséges, ha olyan tápegységet használ, amelyhez más eszközök is csatlakoznak.

Wiegand bemeneti formátum beállítása

1. Lépjen be programozási módba: * mesterkód #

2. Állítsa be az EM kártya Wiegand bemeneti bitjeit:

8 (26~44) # (alapértelmezett 26 bit)

3.1. Paritásbit letiltása: 8 0 #

3.2. Paritásbit engedélyezése: 8 1 #

3. Kilépés a programozási módból: *

Programozás

Az alapvető programozás megegyezik az önálló móddal.

Külső kártyaolvasóhoz való csatlakoztatás

EM vagy Mifare kártyaolvasó esetén a felhasználók mind a billentyűzeten, mind a külső olvasón hozzáadhatók/törölhetők.

HID kártyaolvasó esetén a felhasználók csak a külső olvasón hozzáadhatók/törölhetők.

Ujjlenyomat-olvasóhoz való csatlakoztatás

Csatlakoztassa az ujjlenyomat-olvasót a billentyűzethez.

1. Lépjen be programozási módba: * mesterkód #

2.1. Írja be az 1-es számot (ujjlenyomat beolvasása az ujjlenyomat-olvasón) #. Az azonosító automatikusan kiosztódik.

2.2. Írja be az 1-es számot (felhasználói azonosító) # (olvassa le az ujjlenyomatot az ujjlenyomat-olvasón) #

3. Lépjen ki a programozási módból: *

Csatlakozás billentyűzet-olvasóhoz

A billentyűzet-olvasó lehet 4 bites, 8 bites (ASCII) vagy 10 bites.

1. Lépjen be a programozási módba: * mesterkód #

2.1. Adja meg a bitek számát: 8 (4 vagy 8 vagy 10) #. Az alapértelmezett érték 4 bit.

3. Lépjen ki a programozási módból: *

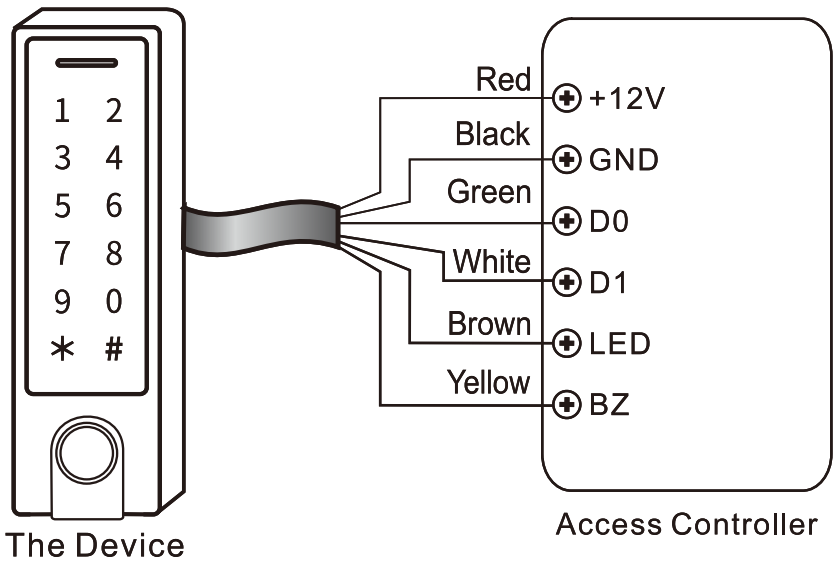
Felhasználói PIN-kód hozzáadása/törlése

A felhasználói PIN-kód hozzáadható/törölhető mind a beléptető billentyűzeten, mind a külső billentyűzet-olvasón.

3. Wiegand olvasó mód

A billentyűzet standard Wiegand olvasóként is működhet, külső vezérlőhöz csatlakoztatva.

Csatlakozási rajz



Amikor a billentyűzet Wiegand olvasó módban van, a Vezérlő módban végrehajtott összes beállítás érvényét veszti. A nagy és sárga vezetékek a

következőképpen lesznek újradefiniálva:

Barna vezeték: Zöld LED vezérlés

Sárga vezeték: Zümmer vezérlés.

Wiegand kimeneti formátum beállítása

1. Lépjen be programozási módba: * mesterkód #

2. Állítsa be az EM kártya Wiegand bitjeit: 8 (26~44) #

3.1. Paritásbit letiltása: 8 0 #

3.2. Paritásbit engedélyezése: 8 1 # (alapértelmezett)

3. Kilépés a programozási módból: *

Megjegyzés: Wiegand vezérlő csatlakoztatásához le kell tiltani a paritásbitet.

Speciális alkalmazások

Összes kártya hozzáférése

A mód aktiválása után minden kártya kinyithatja az ajtót. Ezzel egyidejűleg a kártya hozzáadódik a rendszerhez.

1. Lépjen be programozási módba: * mesterkód #

2.1. Funkció letiltása: 9 2 # (alapértelmezett)

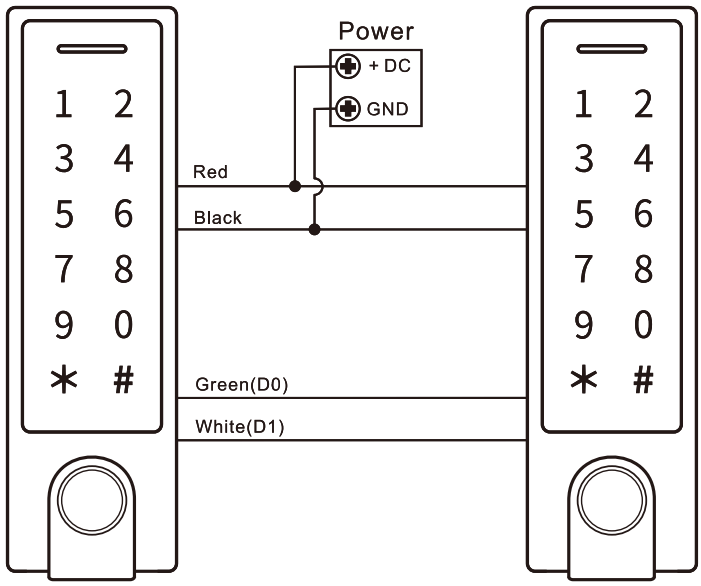
2.2. Funkció engedélyezése: 9 3 #

3. Kilépés a programozási módból: *

Felhasználói adatok átvitele

PIN-kóddal/kártyával regisztrált felhasználók számára.

A felhasználói adatok átvihetők egyik billentyűzetről a másikra.Csatlakozási rajz



Megjegyzések:

Mindkét billentyűzetnek ugyanabból a sorozatból kell származnia.

Mindkét billentyűzet mesterkódjának azonosnak kell lennie.

Az átviteli funkciót csak a fő billentyűzeten (master billentyűzet) aktiválja.

Ha a másodlagos billentyűzeten már vannak regisztrált felhasználók, akkor azok felülírásra kerülnek az átvitel során.

900 felhasználó esetén az átvitel akár 30 másodpercig is eltarthat.

Átviteli mód aktiválása a fő billentyűzeten

1. Lépjen be a programozási módba: * mesterkód #

2. Írja be a 9 8 # kódot

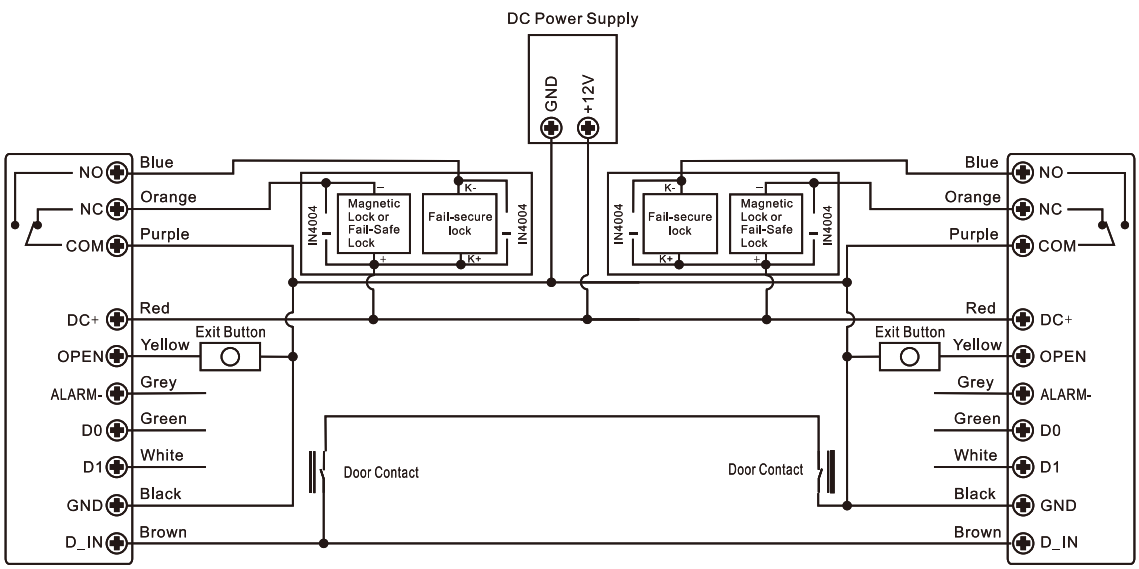
30 másodpercig, a maximális átviteli időtartamig, a zöld LED világít. Amikor az adatátvitel befejeződött, sípoló hang hallatszik, és a piros LED kigyullad.

3. Lépjen ki a programozási módból: *

Kezelőegységek összekapcsolása

Ez a mód két billentyűzet összekapcsolását jelenti két ajtó vezérléséhez. A funkció különösen hasznos börtönökben, bankokban és más olyan helyeken, ahol magasabb szintű biztonságra van szükség.

Csatlakozási rajz



Regisztrálja a felhasználókat az A billentyűzeten, majd adja át őket a B billentyűzetre.

Engedélyezze a reteszelés módot mindkét billentyűzeten:

1. Lépjen be programozási módba: * mesterkód #

2.1. Funkció letiltása: 9 0 # (alapértelmezett)

2.2. Funkció engedélyezése: 9 1 #

3. Kilépés a programozási módból: *

Amikor a funkció aktív, és a 2. ajtónak zárva kell maradnia, a felhasználó beolvashatja az ujjlenyomatát/kártyát, vagy megadhatja a PIN-kódot az A billentyűzeten. Az 1. ajtó kinyílik. Amikor az 1. ajtónak zárva kell maradnia, a felhasználó beolvashatja az ujjlenyomatát/kártyát, vagy megadhatja a PIN-kódot a B billentyűzeten. A 2. ajtó kinyílik.

Amikor a funkció aktív, a felhasználó beolvashatja az ujjlenyomatát/kártyát, vagy megadhatja a PIN-kódot az A billentyűzeten az 1. ajtó kinyitásához. Vagy beolvashatja az ujjlenyomatát/kártyát, vagy megadhatja a PIN-kódot a B billentyűzeten a 2. ajtó kinyitásához.

Billentyűzetvezérlés a Tuya Smart alkalmazásból

Megjegyzés: A Tuya Smart alkalmazás gyakori frissítései miatt a jelen kézikönyvben bemutatott képek és információk eltérhetnek az eszközére telepített verzióban találhatóktól.

Látogass el a Google Play vagy az App Store áruházba, vagy olvasd be az alábbi QR-kódot, és telepítsd a Tuya Smart alkalmazást..

Csatlakoztassa telefonját a WiFi hálózathoz, aktiválja a Helymeghatározás és a Bluetooth funkciókat.

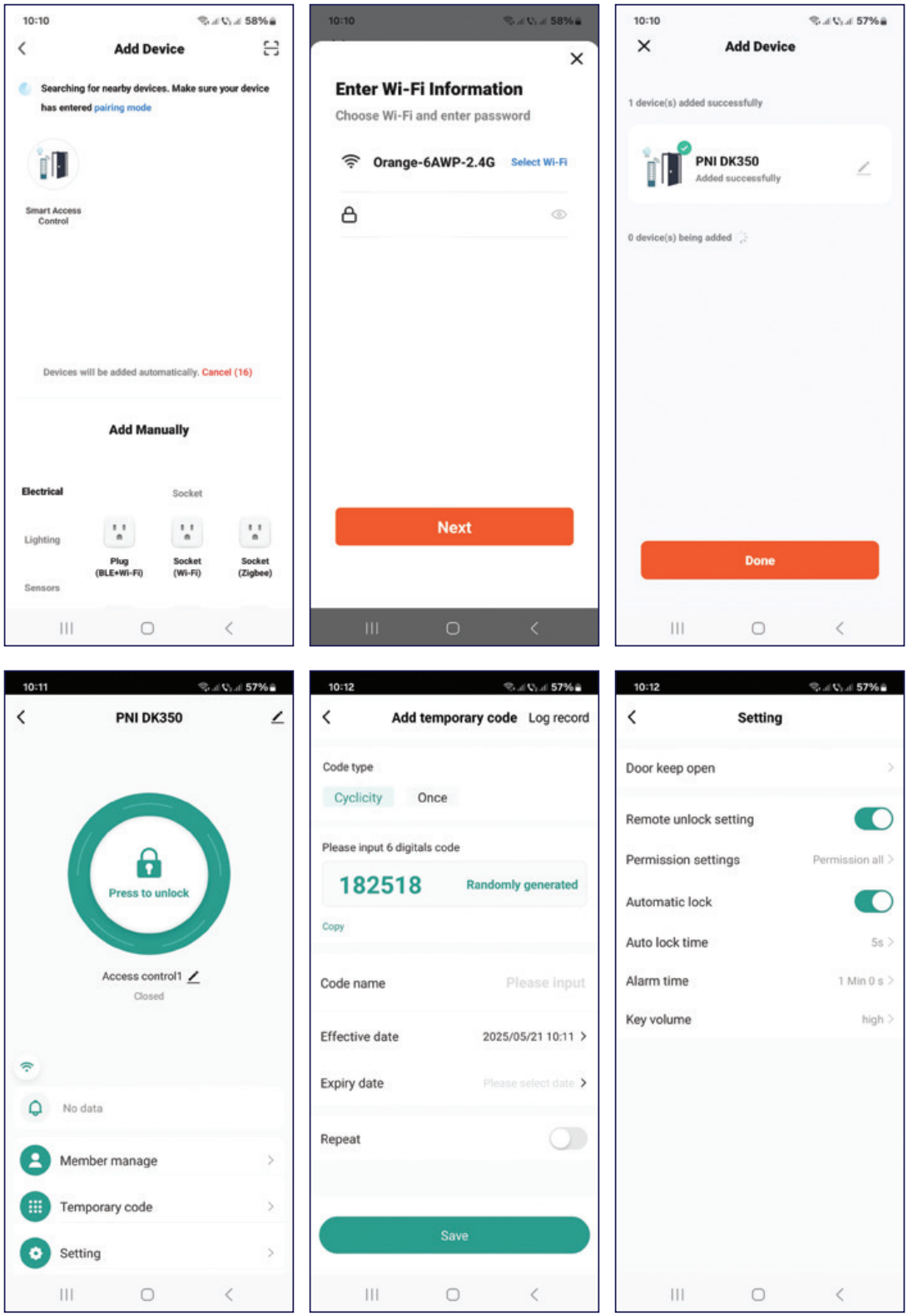
Nyissa meg az alkalmazást, és jelentkezzen be.

Nyomja meg a „+” - „Eszköz hozzáadása” gombot.

Az alkalmazás automatikusan azonosítja az eszközét.

Nyomja meg a billentyűzet ikont, és kövesse a képernyőn megjelenő lépéseket.

Megjegyzés: a billentyűzetet manuálisan is hozzáadhatja az alkalmazáshoz a Kamerák és zárolás - Zárolás (Wi-Fi) kategóriában.



Az alkalmazás lehetővé teszi az ajtó kinyitását, felhasználók hozzáadását és kezelését, valamint ideiglenes hozzáférési kód létrehozását.

Caratteristiche di base

Sensore di impronte digitali.

Tasti touch.

Custodia in metallo impermeabile (IP66).

Supporta 1000 utenti locali (988 utenti comuni, 2 utenti di emergenza, 10 utenti temporanei).

Supporta 500 utenti tramite app.

Supporta tessera EM a 125 kHz.

Uscita allarme e buzzer.

Funzione antivandalismo.

Molteplici metodi di accesso: impronta digitale, tessera, PIN, app.

Supporta password temporanea (monouso o a lungo termine).

Supporta l'aggiunta/eliminazione di utenti tramite app.

Supporta l'impostazione di restrizioni temporali per gli utenti.

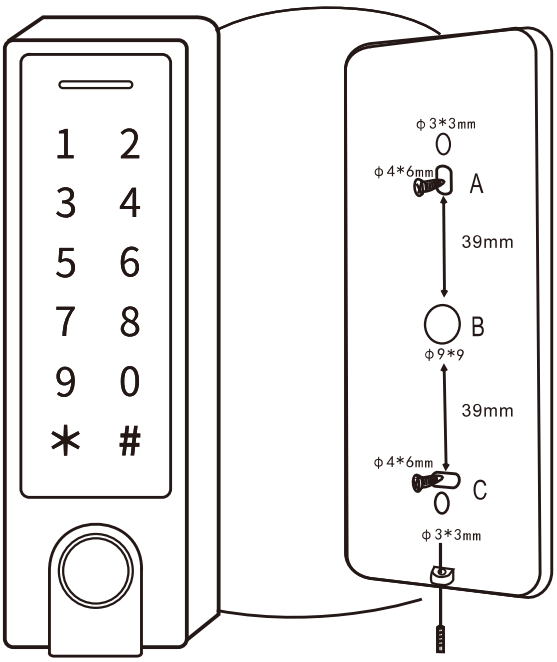
Specifiche tecniche

Tensione di esercizio	12-18V DC
Potenza in standby	≤60mA
Potenza di esercizio	≤150mA

Scheda RFID compatibile	EM 125 KHz
Distanza di lettura della scheda RFID	2-6 cm
Connessioni di uscita	Relè, pulsante di accesso, allarme, contatto porta, lettore di schede Wiegand
Connessioni di ingresso	Lettore di schede Wiegand
Relè	Un relè NO, NC, COM
Tempo di funzionamento del relè	0-99 s. (5 s. predefinito)
Carico di uscita di blocco	Max. 2 A
Uscita PIN	4 bit, numero virtuale di 10 caratteri
Grado di protezione	IP66
Temperatura di esercizio	-26 ~ 80 °C
Materiale dell'alloggiamento	Lega di zinco

Dimensioni	148 x 44 x 22 mm
Wi-Fi	2.4 GHz/100mW
Bluetooth	2.4 GHz/2.5mW

Installazione



A

Rimuovere la staffa dal retro dell'unità.

Fissare la staffa alla parete utilizzando le viti in dotazione.

Fare passare il cavo di collegamento attraverso il foro contrassegnato con B nel disegno sottostante.

Fissare l'unità alla staffa.

Connessioni

Colore del filo	**Funzioni**	**Note**
Rosso	DC+	Ingresso CC 12-18 V
Nero	GND	Ingresso CC polo negativo

Blu	NO	Uscita relè NO (collegare il diodo incluso nella confezione)
Viola	COM	Uscita relè COM
Arancione	NC	Uscita relè NC (collegare il diodo incluso nella confezione)
Giallo	OPEN	Ingresso pulsante di accesso
Connessioni tramite lettore o controller Wiegand		
Verde	Data 0	Uscita Wiegand (pass-through)
Bianco	Data 1	Uscita Wiegand (pass-through)
Collegamenti speciali		
Grigio	Uscita allarme	Contatto negativo per allarme
Marrone	Ingresso	Ingresso contatto porta

Avvisi acustici e luminosi

Stato	LED	Cicalino
Standby	LED rosso	-
Accesso alla modalità di programmazione	LED rosso lampeggiante	Un bip
Modalità di programmazione	LED arancione	Un bip
Errore di funzionamento	-	Tre bip
Uscita dalla modalità di programmazione	LED rosso	Un bip
Apertura porta	LED verde	Un bip
Allarme	LED rosso lampeggiante velocemente	Bip

Accesso e uscita dalla modalità di programmazione

Accesso alla modalità di programmazione: * codice master #

Nota: il codice master predefinito è 123456.

Uscita dalla modalità di programmazione: *

Impostazione del codice master

1. Accesso alla modalità di programmazione: * codice master #

2. Modifica del codice master: 0 (nuovo codice master) # (ripeti il nuovo codice master) #

Nota: il codice master deve contenere 6 caratteri.

3. Uscita dalla modalità di programmazione: *

Impostazione della modalità di funzionamento

Sono disponibili 3 modalità di funzionamento: modalità standalone, modalità controller e modalità lettore Wiegand. La modalità predefinita è la modalità standalone/controller.

1. Accesso alla modalità di programmazione: * codice master #

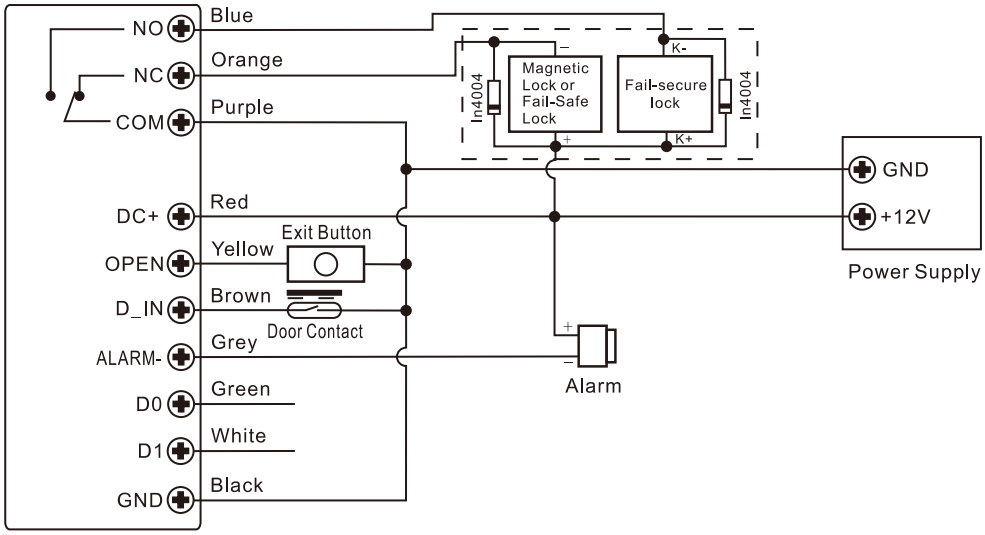
2. Inserire 7 7 # (modalità predefinita) o 7 8 # (modalità Wiegand).

3. Uscita dalla modalità di programmazione: *

1. Modalità standalone

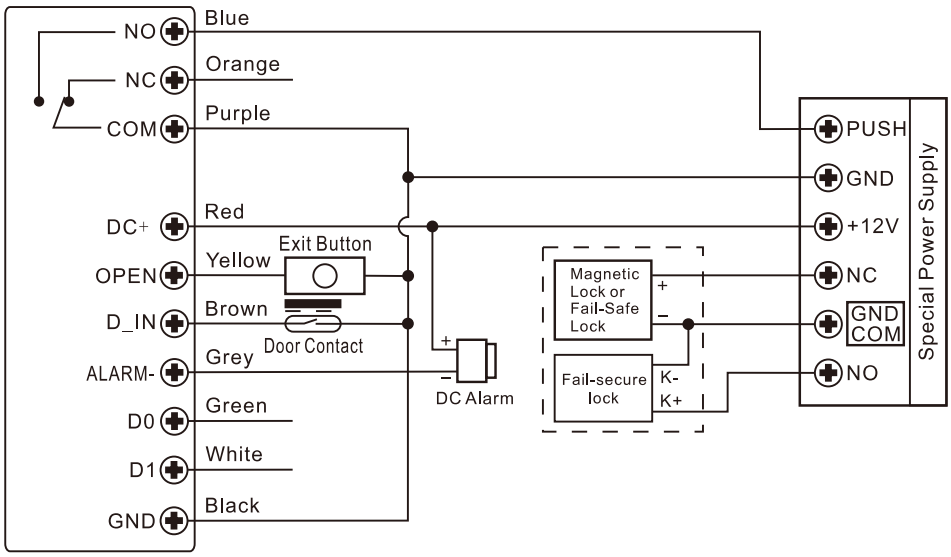
Schema di collegamento

Alimentazione comune:



Attenzione: è necessario installare il diodo 1N4004 incluso o un equivalente se si utilizza un alimentatore a cui sono collegati altri dispositivi.

Alimentatore separato:



Programmazione

*La pro*grammazione varia a seconda della modalità di accesso.

Note:

1. ID utente: Assegnare un ID utente per ogni impronta

digitale, PIN o tessera di accesso per una migliore gestione delle informazioni di accesso.

ID utente comune:

ID utente impronta digitale: 0-98

ID utente PIN o tessera: 100-987

ID utente master: 99

ID utente antipanico: 988-989

ID utente visitatore: 990-999

Importante: L'ID utente non deve essere preceduto da 0 (zero). La registrazione degli ID utente è molto importante. Per modificare un utente è necessario conoscere l'ID utente.

2. Tessera: Il sistema supporta solo tessere RFID EM a 125 KHz.

3. PIN: Può contenere da 4 a 6 caratteri, ad eccezione della sequenza 8888 che è riservata.

Aggiunta dell'impronta digitale utente standard

1. Accedere alla modalità di programmazione: * codice master #

2.1. Aggiungi l'impronta digitale utente utilizzando l'ID assegnato automaticamente: 1 (leggi impronta digitale) (ripeti lettura impronta digitale) (ripeti lettura impronta digitale)

Nota: le impronte digitali possono essere aggiunte in modo continuo.

2.2 Aggiungi l’impronta digitale utente utilizzando l’ID personalizzato: 1 (ID utente) # (leggi impronta digitale) (ripeti lettura impronta digitale) (ripeti lettura impronta digitale) Nota: le impronte digitali possono essere aggiunte in modo continuo.

3. Esci dalla modalità di programmazione: *

Aggiungi tessera utente standard

1. Entra in modalità programmazione: * codice master #

2.1. Aggiungi tessera utente utilizzando l’ID assegnato automaticamente: 1 (leggi tessera o inserisci manualmente il numero tessera) #

Nota: le impronte digitali possono essere aggiunte in modo continuo.

2.2 Aggiungi tessera utente utilizzando un ID personalizzato: 1 (ID utente) (scansiona tessera o inserisci manualmente il numero tessera) #

2.3 Aggiungi tessere in blocco: consente all’utente master di aggiungere fino a 888 tessere in un unico passaggio. La procedura richiede fino a 2 minuti: 1 (ID utente) # (quantità tessera) # (inserisci manualmente il primo numero tessera) #

Note:

1. La quantità tessera rappresenta il numero di tessere che si desidera aggiungere al sistema.

2. I numeri tessera devono essere consecutivi.

Aggiungi PIN utente standard

1. Entra in modalità programmazione: * codice master #

2.1. Aggiungi PIN utente utilizzando l'ID assegnato automaticamente: 1 (PIN) #

2.2 Aggiungi PIN utente utilizzando l'ID personalizzato: 1 (ID utente) # (PIN) #

3. Esci dalla modalità di programmazione: *

Per una maggiore sicurezza, è possibile nascondere il PIN (max. 6 caratteri) digitando fino a 10 caratteri.

Ad esempio:

Se il PIN corretto è: 123434

Digitare: **123434** o **123434, dove ** può essere un numero qualsiasi da 0 a 9.

Aggiungi impronta digitale utente master

1. Entra nella modalità di programmazione: * codice master #

2. Aggiungi impronta digitale: 1 (99) # (leggi impronta digitale) (ripeti lettura impronta digitale) (ripeti nuovamente lettura impronta digitale)

3. Esci dalla modalità di programmazione: *

Aggiungi utente antipanico

1. Entra nella modalità di programmazione: * codice master #

2.1. Aggiungi tessera: 1 (ID utente) # (leggi tessera o inserisci manualmente il numero della tessera) #

2.2 Aggiungi PIN: 1 (ID utente) # (PIN) #

3. Esci dalla modalità di programmazione: *

Aggiungi utente visitatore

È possibile aggiungere un massimo di 10 visitatori con PIN o tessera. I visitatori possono utilizzare il PIN o la tessera al massimo 10 volte. Dopo un massimo di 10 utilizzi, il PIN o la tessera diventeranno automaticamente non validi.

1. Accedi alla modalità di programmazione: * codice master #

2.1. Aggiungi tessera: 1 (ID utente) # (0~9) # (leggi tessera o inserisci manualmente il numero della tessera) #

2.2 Aggiungi PIN: 1 (ID utente) # (0~9) # (PIN) #

3. Esci dalla modalità di programmazione: *

Elimina utente

1. Entrare in modalità programmazione: * codice master #

2.1. Eliminare utente tramite impronta digitale, tessera o PIN: 2 (leggere impronta digitale/leggere tessera/inserire PIN) #

2.2 Eliminare utente tramite numero ID: 2 (ID utente)

#

2.3 Eliminare utente tramite numero tessera: 2 (inserire numero tessera) #

2.4. Eliminare tutti gli utenti: 2 (codice master) #

3. Uscire dalla modalità programmazione: *

Configurazione della modalità di attivazione del relè

La configurazione del relè ne influenza il comportamento dopo l'inserimento del codice di accesso.

1. Entrare in modalità programmazione: * codice master #

2.1. Modalità impulsi (modalità predefinita): 3 (1~99) #

Il relè si attiva per un periodo di tempo compreso tra 0 e 99 secondi (impostazione predefinita 5 secondi) dopo l'inserimento del codice, dopodiché si disattiva automaticamente.

Il tempo di attivazione del relè è compreso tra 1 e 99 secondi. Impostazione predefinita: 5 secondi.

2.2. Modalità alternata: 3 0 #

Il relè cambia stato ogni volta che il codice viene inserito correttamente:

Se è spento (aperto), si attiva (chiude il contatto). Se è attivato, si disattiva.

Utile per cancelli o porte che devono rimanere aperti finché non vengono richiusi manualmente.

3. Uscita dalla modalità di programmazione: *

Impostazione della modalità di accesso

Per la modalità di accesso multiutente, l'intervallo di tempo per la lettura dei codici di accesso non deve superare i 5 secondi. Dopo 5 secondi, l'unità entra automaticamente in standby.

1. Accesso alla modalità di programmazione: * codice master #

2.1. Accesso tramite impronta digitale: 4 0 #

2.2. Accesso tramite tessera: 4 1 #

2.3. Accesso tramite PIN: 4 2 #

2. 4. Accesso multiutente: 4 3 (2~9) #

Solo dopo la convalida di 2~9 utenti, la porta si aprirà.

2.5. Impronta digitale o tessera o PIN (predefinito): 4 4 #

3. Uscita dalla modalità di programmazione: *

Allarme per tentativi ripetuti non riusciti

Si riferisce a un allarme che si attiva dopo un numero consecutivo di 10 tentativi di accesso errati (inserimento di un codice errato, tessera non valida, ecc.). Può essere impostato per negare l'accesso per 10 minuti o per consentire l'accesso solo dopo

l’inserimento di un codice, di una tessera o di un’impronta digitale validi. 1. Entrare in modalità programmazione: * codice master #

2.1. Funzione disabilitata (impostazione predefinita): 6 0 #

2.2. Funzione abilitata: 6 1 # (l’accesso sarà vietato per 10 minuti)

2.3. Funzione abilitata (Allarme): 6 2 #

Impostazione durata allarme: 5 (0~3) #. Impostazione predefinita: 1 minuto.

Per interrompere l’allarme, inserire il codice master # o scansionare l’impronta digitale/tessera master, oppure inserire il PIN o scansionare l’impronta digitale/tessera utente.

3. Uscire dalla modalità programmazione: *

Avviso porta aperta

Se è stato collegato un contatto magnetico cablato alla tastiera di controllo accessi e la porta rimane aperta per più di 1 minuto, il cicalino integrato suonerà per ricordare all’utente di chiudere la porta. Il suono può essere interrotto chiudendo la porta o inserendo un codice di accesso valido (master o utente). In caso contrario, il suono continuerà finché rimarrà impostato.

Allarme porta forzata

Se è stato collegato un contatto magnetico cablato alla tastiera del controllo accessi e la porta viene forzata, il buzzer integrato e la sirena esterna (se presente) emetteranno l'allarme. Il suono può essere interrotto chiudendo la porta o inserendo un codice di accesso valido (master o utente). In caso contrario, il suono continuerà finché rimarrà impostato.

1. Accedere alla modalità di programmazione: * codice master #

2.1. Funzione disabilitata (default): 6 3 #

2.2. Funzione abilitata" 6 4 #

Imposta durata allarme: 5 (0~3) #. Predefinito 1 minuto.

3. Uscita dalla modalità di programmazione: *

Impostazione buzzer e LED

1. Entrare in modalità di programmazione: * codice master #

2.1. Disabilitare buzzer: 7 0 #

2.2. Abilitare buzzer (predefinito): 7 1 #

3.1. LED spento: 7 2 #

3.2. LED acceso (predefinito): 7 3 #

4.1. Luce tastiera spenta: 7 4 #

4.2. Luce tastiera sempre accesa: 7 5 #

4.3. Luce tastiera spenta automaticamente

(predefinito): 7 6 #. Dopo 20 secondi dall'ultima operazione, la tastiera si spegne automaticamente. Toccando un tasto qualsiasi, la tastiera si illumina.

3. Uscita dalla modalità di programmazione: *

Aggiunta impronta digitale/tessera/PIN utente con tessera/impronta digitale master

1. Leggere la tessera/impronta digitale master.

2. Scansionare l'impronta digitale dell'utente 3 volte o Scansiona la scheda dell'utente o il pin #

Ripeti il passaggio 2 per aggiungere più utenti consecutivamente.

3. Scansiona nuovamente la scheda principale/ impronta digitale.

Eliminazione di impronte digitali/scheda/perno di un utente con una scheda/impronta digitale

1. Scansionare due volte la scheda principale/impronta digitale entro un massimo di 5 secondi.

2. Scansiona l'impronta digitale/scheda o immettere il pin dell'utente #

Ripeti il passaggio 2 per eliminare più utenti consecutivamente.

3. Scansiona nuovamente la scheda principale/ impronta digitale.

Ripristina e aggiungi una scheda principale

Se hai collegato un pulsante di accesso alla tastiera di controllo Access, procedi come segue per ripristinare la tastiera:

1. Spegnere il potere.

2. Premere e tenere premuto il pulsante di accesso mentre si riaccende.

3. 2 Segnali acustici saranno ascoltati.

4. Rimuovere il dito dal pulsante di accesso.

5. Il LED giallo si illumina.

6. Leggi qualsiasi scheda EM da 125khz.

7. Il LED si illumina di rosso.

8. La tastiera è stata ripristinata.

9. La carta letta è diventata la carta master.

Note:

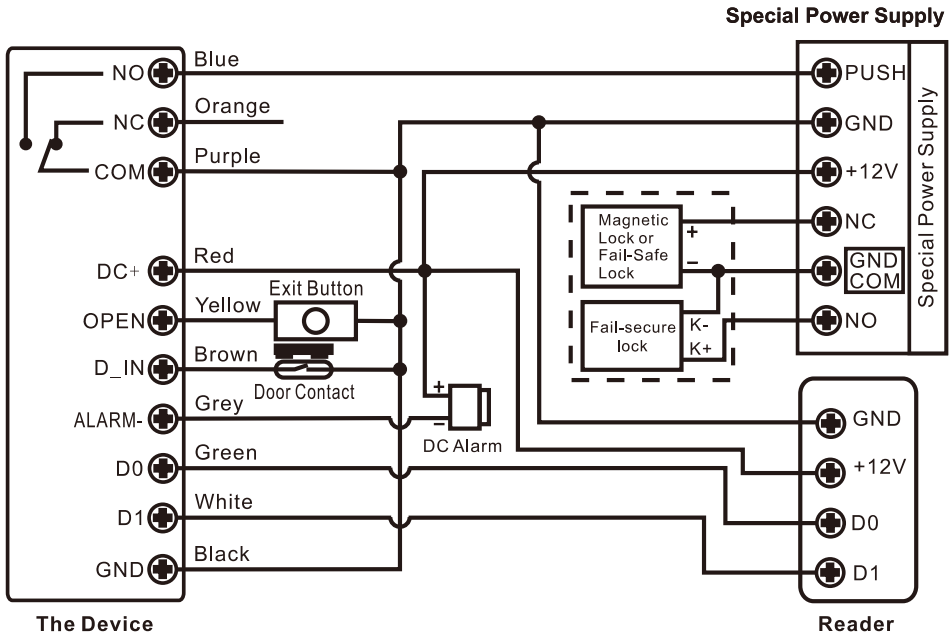
1. Se non si desidera aggiungere una carta master, è necessario tenere premuto il pulsante di accesso per almeno 5 secondi prima di rilasciarlo. Questa procedura invaliderà la precedente carta master.

2. Con il reset, le informazioni utente non verranno eliminate.

2. Modalità Controller

La tastiera funzionerà come controller se collegata a un lettore Wiegand.

Schema di collegamento



Attenzione: è necessario installare il diodo 1N4004 incluso o un equivalente se si utilizza un alimentatore a cui sono collegati altri dispositivi.

Impostazione del formato di ingresso Wiegand

1. Accedere alla modalità di programmazione: * codice master #

2. Impostare i bit di ingresso Wiegand per la tessera EM:

8 (26~44) # (predefinito 26 bit)

3.1. Disabilitare il bit di parità: 8 0 #

3.2. Abilitare il bit di parità: 8 1 #

3. Uscire dalla modalità di programmazione: *

Programmazione

La programmazione di base è la stessa della modalità

standalone.

Collegamento a un lettore di tessere esterno

In caso di lettore di tessere EM o Mifare, è possibile aggiungere/eliminare utenti sia sulla tastiera che sul lettore esterno.

In caso di lettore di tessere HID, è possibile aggiungere/eliminare utenti solo sul lettore esterno.

Collegamento a un lettore di impronte digitali

Collegare il lettore di impronte digitali alla tastiera.

1. Accedere alla modalità di programmazione: * codice master #

2.1. Tipo 1 (leggere l'impronta digitale sul lettore di impronte digitali) #. L'ID viene assegnato automaticamente.

2.2. Tipo 1 (ID utente) # (leggere l'impronta digitale sul lettore di impronte digitali) #

3. Uscita dalla modalità di programmazione: *

Connessione a un lettore di tastiera

Il lettore di tastiera può essere a 4 bit, 8 bit (ASCII) o 10 bit.

1. Entrare in modalità di programmazione: * codice master #

2.1. Inserire il numero di bit: 8 (4 o 8 o 10) #. Il valore predefinito è 4 bit.

3. Uscita dalla modalità di programmazione: *

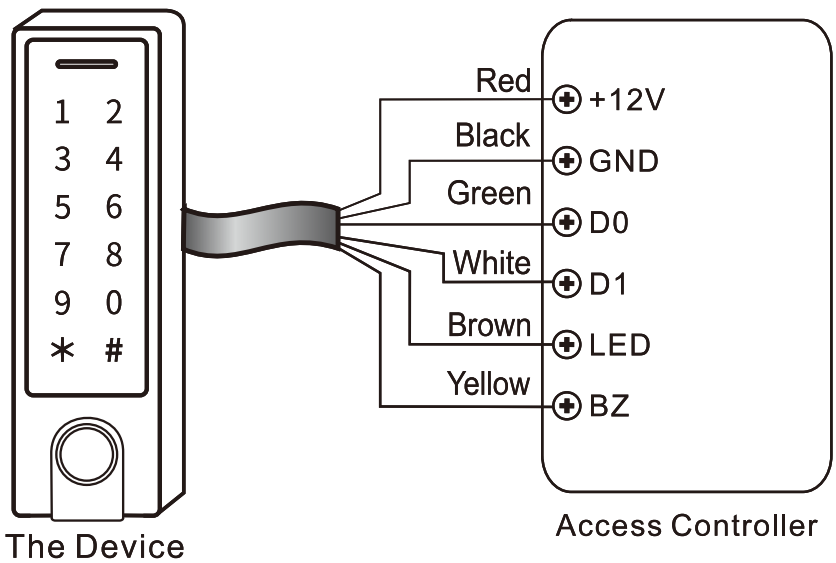
Aggiungere/Eliminare PIN utente

Il PIN utente può essere aggiunto/eliminato sia sulla tastiera di controllo accessi che sul lettore di tastiera esterno.

3. Modalità lettore Wiegand

La tastiera può anche funzionare come un lettore Wiegand standard collegato a un controller esterno.

Schema di collegamento



Quando la tastiera è in modalità lettore Wiegand, tutte le impostazioni effettuate in modalità Controller non sono più valide. I fili grande e giallo verranno ridefiniti come segue:

Filo marrone: controllo LED verde

Filo giallo: controllo buzzer.

Impostazione del formato di uscita Wiegand

1. Accedere alla modalità di programmazione: * codice master #

2. Impostare i bit Wiegand per la tessera EM: 8 (26~44) #

3.1. Disabilitare il bit di parità: 8 0 #

3.2. Abilitare il bit di parità: 8 1 # (predefinito)

3. Uscire dalla modalità di programmazione: *

Nota: per collegare un controller Wiegand, è necessario disabilitare il bit di parità.

Applicazioni avanzate

Accesso a tutte le tessere

Dopo aver attivato questa modalità, tutte le tessere possono aprire la porta. Contemporaneamente, la tessera viene aggiunta al sistema.

1. Accedere alla modalità di programmazione: * codice master #

2.1. Disabilitare la funzione: 9 2 # (predefinito)

2.2. Abilita funzione: 9 3 #

3. Esci dalla modalità di programmazione: *

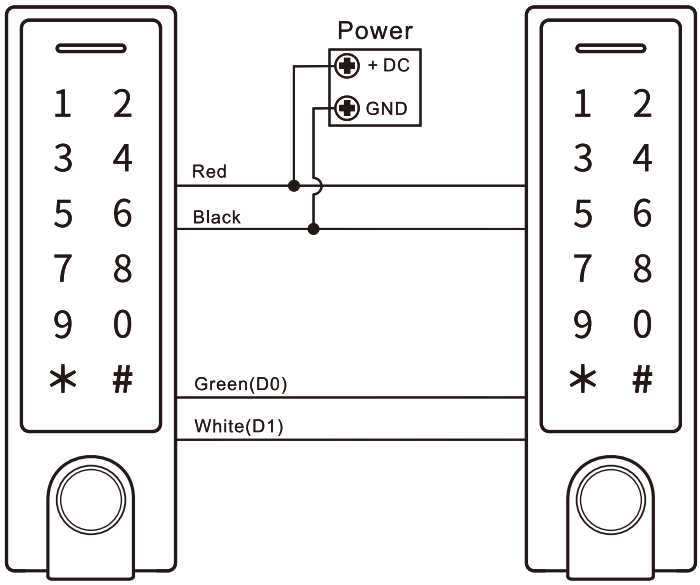
Trasferisci informazioni utente

Per gli utenti registrati con PIN/tessera.

Le informazioni utente possono essere trasferite da

una tastiera all’altra.

Schema di collegamento



Note:

Entrambe le tastiere devono appartenere alla stessa serie.

Il codice master di entrambe le tastiere deve essere identico.

Attivare la funzione di trasferimento solo sulla tastiera principale (tastiera master).

Se sulla tastiera secondaria sono già presenti utenti registrati, questi verranno sovrascritti durante il trasferimento.

Per un numero di 900 utenti, il trasferimento potrebbe richiedere fino a 30 secondi.

Attivare la modalità di trasferimento sulla tastiera master

1. Accedere alla modalità di programmazione: * codice master #

2. Digitare 9 8 #

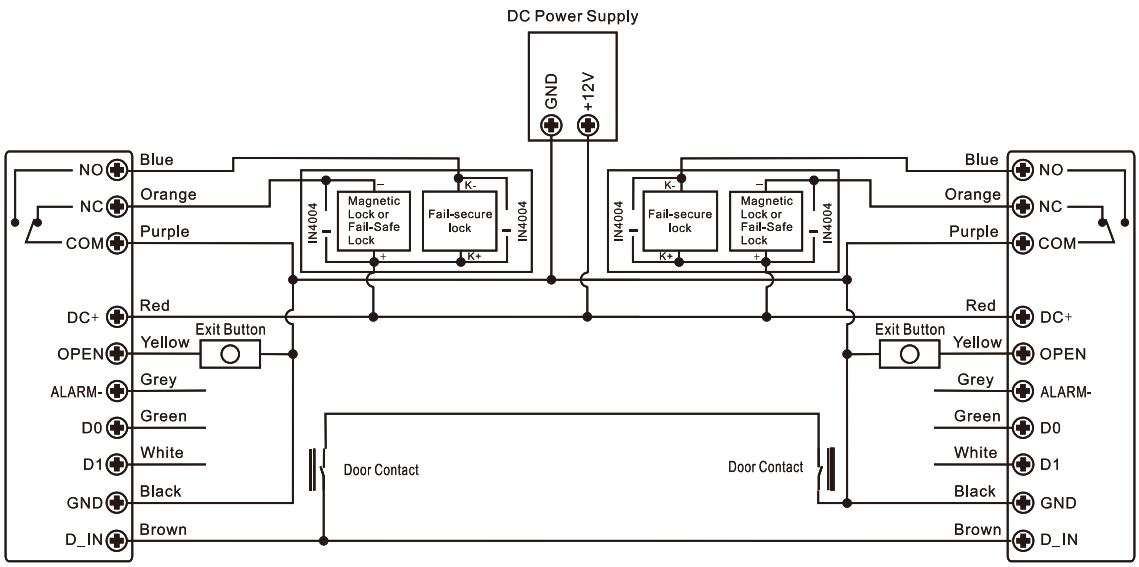
Per 30 secondi, la durata massima del trasferimento, il LED verde è acceso. Al termine del trasferimento dati, viene emesso un segnale acustico e il LED rosso si accende.

3. Uscire dalla modalità di programmazione: *

Interconnessione delle tastiere

Questa modalità consente di interconnettere due tastiere per controllare due porte. La funzione è particolarmente utile in carceri, banche e altri luoghi in cui è richiesto un livello di sicurezza più elevato..

Schema di collegamento



Registrare gli utenti sulla tastiera A, quindi trasferirli

sulla tastiera B.

Abilitare la modalità interblocco su entrambe le tastiere:

1. Entrare in modalità programmazione: * codice master #

2.1. Disabilitare la funzione: 9 0 # (predefinito)

2.2. Abilitare la funzione: 9 1 #

3. Uscire dalla modalità programmazione: *

Quando la funzione è attiva, se la porta 2 deve rimanere chiusa, l'utente può scansionare l'impronta digitale/la tessera o inserire il PIN sulla tastiera A. La porta 1 si aprirà. Quando la porta 1 deve rimanere chiusa, l'utente può scansionare l'impronta digitale/la tessera o inserire il PIN sulla tastiera B. La porta 2 si aprirà.

Quando la funzione è attiva, l'utente può scansionare l'impronta digitale/la tessera o inserire il PIN sulla tastiera A per aprire la porta 1. Oppure scansionare l'impronta digitale/la tessera o inserire il PIN sulla tastiera B per aprire la porta 2.

Controllo della tastiera dall'app Tuya Smart

Nota: a causa dei frequenti aggiornamenti dell'app Tuya Smart, le immagini e le informazioni presentate in questo manuale potrebbero differire da quelle della versione installata sul dispositivo.

Vai su Google Play o App Store oppure scansiona il codice QR qui sotto e installa l’app Tuya Smart.

Connetti il telefono alla rete Wi-Fi, attiva la posizione e il Bluetooth.

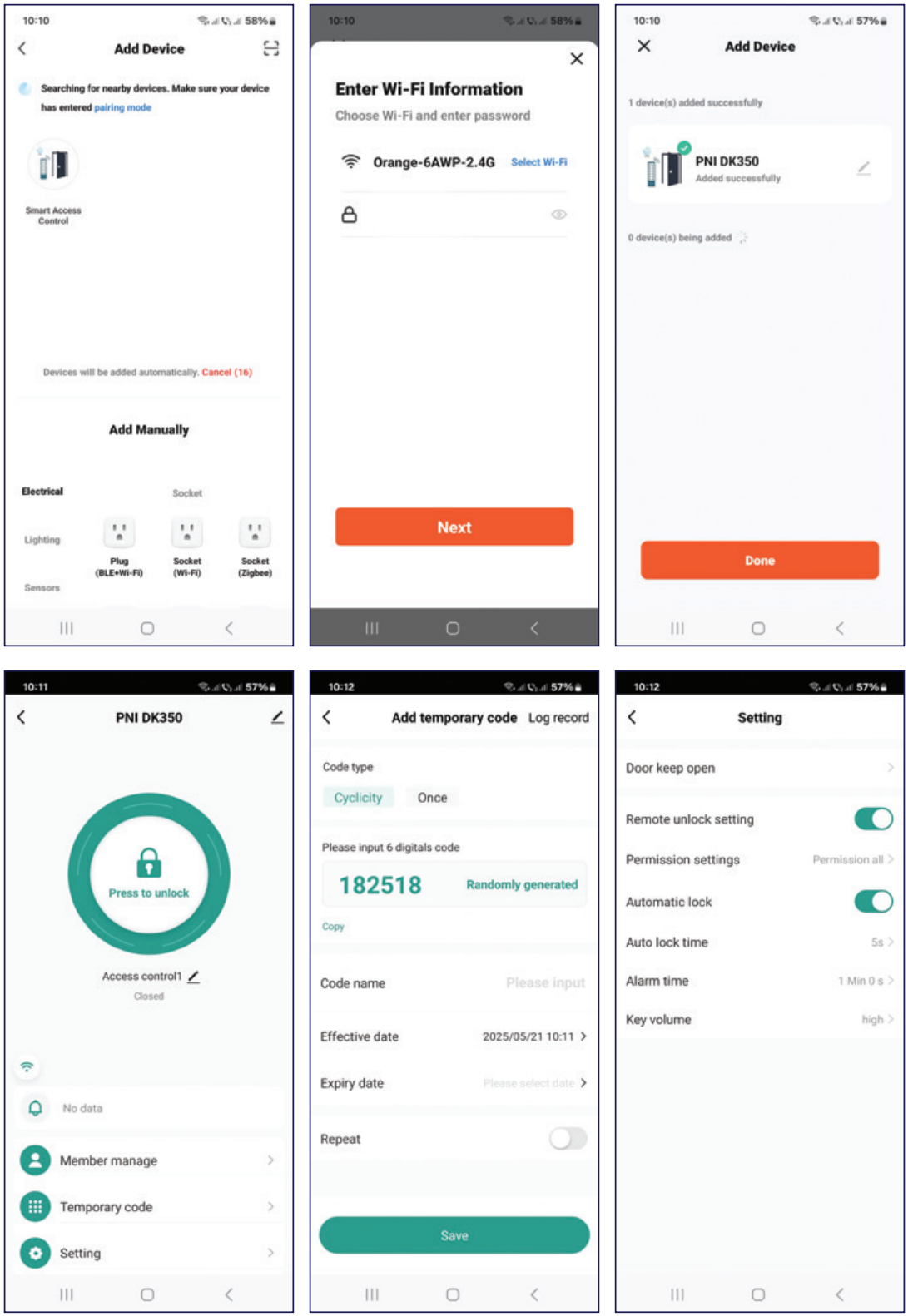
Apri l’app e accedi.

Premi “+” - “Aggiungi dispositivo” .

L’app identificherà automaticamente il tuo dispositivo.

Premi l’icona della tastiera e segui le istruzioni sullo schermo.

Nota: puoi anche aggiungere manualmente la tastiera all’app accedendo alla categoria Fotocamere e blocco - Blocco (Wi-Fi).



L’applicazione consente di sbloccare la porta, aggiungere e gestire gli utenti e generare un codice di accesso temporaneo.

Basisfuncties

Vingerafdruksensor.

Aanraaktoetsen.

Waterdichte metalen behuizing (IP66).

Ondersteunt 1000 lokale gebruikers (988 algemene gebruikers, 2 paniekgebruikers, 10 tijdelijke gebruikers).

Ondersteunt 500 gebruikers via de app.

Ondersteunt 125 kHz EM-kaart.

Alarm- en zoemeruitgang.

Anti-vandalismefunctie.

Meerdere toegangsmethoden: vingerafdruk, kaart, pincode, app.

Ondersteunt tijdelijk wachtwoord (eenmalig of voor een bepaalde periode).

Ondersteunt het toevoegen/verwijderen van gebruikers via de app.

Ondersteunt het instellen van tijdsbeperkingen voor gebruikers.

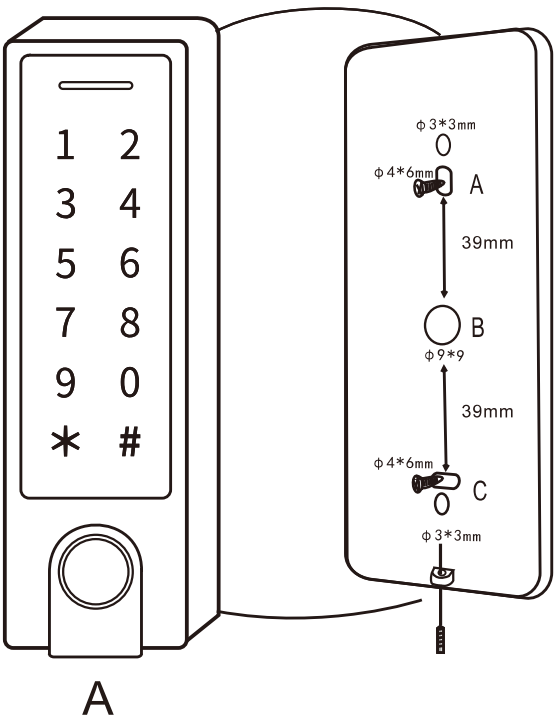
Technische specificaties

Bedrijfsspanning	12-18V DC
Stand-byvermogen	≤60mA

Bedrijfsvermogen	≤150mA
Compatibele RFID-kaart	EM 125 KHz
Leesafstand RFID-kaart	2-6 cm
Uitgangsaansluitingen	Relais, toegangsknop, alarm, deurcontact, Wiegand-kaartlezer
Ingangsaansluitingen	Wiegand-kaartlezer
Relais	Eén relay NO, NC, COM
Bedrijfstijd relais	0-99 s. (standaard 5 s.)
Uitgangsbelasting slot	Max. 2A
PIN-uitgang	4 bits, virtueel nummer van 10 tekens
Beschermingsklasse	IP66
Bedrijfstemperatuur	-26 ~ 80 °C
Materiaal behuizing	Zinklegering
Afmetingen	148 x 44 x 22 mm
Wifi	2.4 GHz/100mW

Bluetooth	2.4 GHz/2.5mW

Installatie



A

Verwijder de beugel aan de achterkant van het apparaat.

Bevestig de beugel aan de muur met de meegeleverde schroeven.

Leg de aansluitkabel door het gat met de letter B in de onderstaande tekening.

Bevestig het apparaat aan de beugel.

Verbindingen

Draadkleur	**Functie**	**Opmerkingen**
Rood	DC+	DC 12-18V-ingang
Zwart	GND	DC-ingang met negatieve pool

Blauw	NO	NO-relaisuitgang (sluit de diode in de behuizing aan)
Paars	COM	COM-relaisuitgang
Oranje	NC	NC-relaisuitgang (sluit de diode in de behuizing aan)
Geel	OPEN	Ingang voor toegangsknop
Verbindingen via een Wiegand-lezer of controller		
Groen	Data 0	Wiegand-uitgang (pass-through)
Wit	Data 1	Wiegand-uitgang (pass-through)
Speciale verbindingen		
Grijs	Alarmuitgang	Negatief contact voor alarm
Bruin	Ingang	Deurcontactingang

Audio- en lichtwaarschuwingen

Status	LED	Zoemer
Stand-by	Rode LED	-
Programmeermodus openen	Rode LED knippert	Eén piep
Programmeermodus	Oranje LED	Eén piep
Bedieningsfout	-	Drie piepjes
Programmeermodus verlaten	Rode LED	Eén piep
Deur openen	Groene LED	Eén piep
Alarm	Rode LED knippert snel	Piepjes

Programmeermodus openen en sluiten

Programmeermodus openen: * Mastercode #

Opmerking: de standaard mastercode is 123456.

Programmeermodus verlaten: *

Mastercode instellen

1. Programmeermodus openen: * Mastercode #

2. Mastercode wijzigen: 0 (nieuwe mastercode)# (nieuwe mastercode herhalen)#

Opmerking: de mastercode moet 6 tekens bevatten.

3. Programmeermodus verlaten: *

De bedrijfsmodus instellen

Er zijn 3 bedrijfsmodi: stand-alonemodus, controllermodus en Wiegand-lezermodus. De standaardmodus is stand-alone/controllermodus.

1. Programmeermodus openen: * Mastercode #

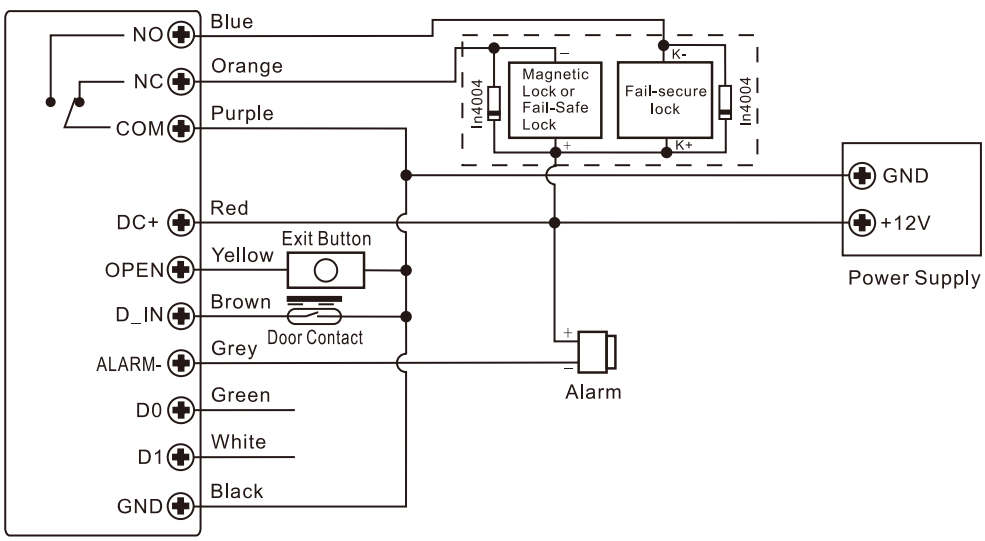
2. Voer 7 7# (standaardmodus) of 7 8# (Wiegand-modus) in.

3. Programmeermodus verlaten: *

1. Stand-alonemodus

Aansluitschema

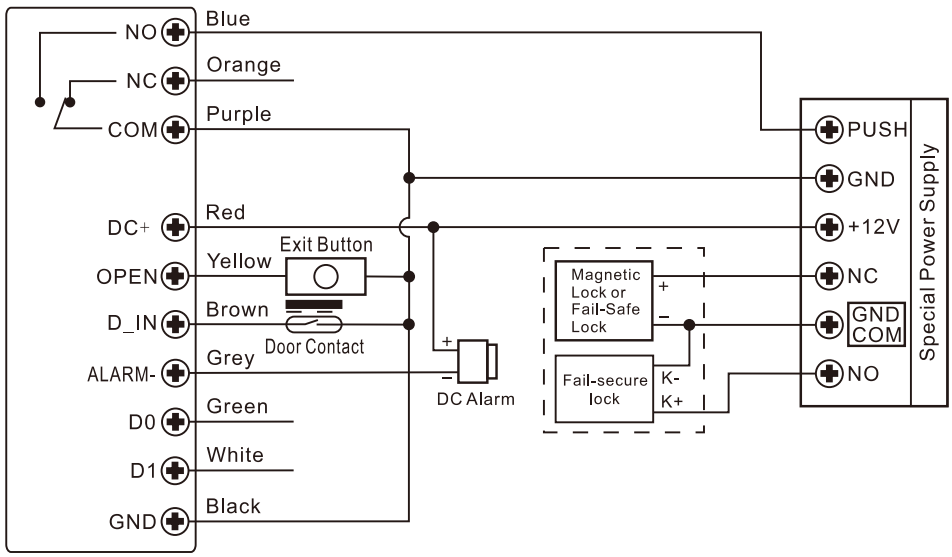
Gemeenschappelijke voeding:



Let op: het is noodzakelijk om de meegeleverde

1N4004-diode of een gelijkwaardige diode te installeren als u een voeding gebruikt waarop andere apparaten zijn aangesloten.

Aparte voeding:



Programmeren

De programmering verschilt afhankelijk van de toegangsmodus.

Opmerkingen:

1. Gebruikers-ID: Wijs een gebruikers-ID toe voor elke vingerafdruk, pincode of toegangskaart voor een beter beheer van de toegangsgegevens.

Algemene gebruikers-ID:

Vingerafdrukgebruikers-ID: 0-98

PIN- of kaartgebruikers-ID: 100-987

Mastergebruikers-ID: 99

Paniekgebruikers-ID: 988-989

Bezoekergebruikers-ID: 990-999

Belangrijk: De gebruikers-ID mag niet worden voorafgegaan door een 0 (nul). Het registreren van gebruikers-ID's is erg belangrijk. Om een gebruiker te wijzigen, moet u de gebruikers-ID kennen.

2. Kaart: Het systeem ondersteunt alleen 125 kHz EM RFID-kaarten.

3. PIN: Kan 4-6 tekens bevatten, met uitzondering van de reeks 8888, die is gereserveerd.

Voeg een gewone gebruikersvingerafdruk toe

1. Programmeermodus openen: * Mastercode #

2.1. Voeg een gebruikersvingerafdruk toe met behulp van de automatisch toegewezen ID: 1 (vingerafdruk lezen) (vingerafdruk opnieuw lezen) (vingerafdruk opnieuw lezen)

Opmerking: vingerafdrukken kunnen doorlopend worden toegevoegd.

2.2 Voeg een gebruikersvingerafdruk toe met behulp van een aangepaste ID: 1 (gebruikers-ID) # (vingerafdruk lezen) (vingerafdruk opnieuw lezen) (vingerafdruk opnieuw lezen). Opmerking: vingerafdrukken kunnen doorlopend worden toegevoegd.

3. Verlaat de programmeermodus: *

Voeg een gewone gebruikerskaart toe

1. Ga naar de programmeermodus: * Mastercode #

2.1. Voeg een gebruikerskaart toe met behulp van de automatisch toegewezen ID: 1 (kaart lezen of handmatig kaartnummer invoeren) #

Opmerking: vingerafdrukken kunnen doorlopend worden toegevoegd.

2.2 Voeg een gebruikerskaart toe met behulp van een gepersonaliseerde ID: 1 (gebruikers-ID) (kaart scannen of handmatig kaartnummer invoeren) #

2.3 Kaarten in bulk toevoegen: hiermee kan de hoofdgebruiker tot 888 kaarten in één stap toevoegen. De procedure duurt maximaal 2 minuten: 1 (gebruikers-ID) # (kaartnummer) # (voer handmatig het eerste kaartnummer in) #

Opmerkingen:

1. Het kaartnummer geeft het aantal kaarten aan dat u aan het systeem wilt toevoegen.

2. De kaartnummers moeten opeenvolgend zijn.

Voeg een normale gebruikerspincode toe

1. Ga naar de programmeermodus: * Mastercode #

2.1. Voeg een gebruikerspincode toe met behulp van de automatisch toegewezen ID: 1 (PIN) #

2.2. Voeg een gebruikerspincode toe met behulp van een aangepaste ID: 1 (gebruikers-ID) # (PIN) #

3. Verlaat de programmeermodus: *

Voor extra beveiliging kunt u de pincode (max. 6 tekens) verbergen door maximaal 10 tekens in te voeren. Bijvoorbeeld:

Als de juiste pincode 123434 is, typ dan: **123434** of **123434, waarbij ** een willekeurig getal van 0 tot en met 9 kan zijn.

Voeg vingerafdruk van hoofdgebruiker toe

1. Ga naar de programmeermodus: * hoofdcode *

2. Voeg vingerafdruk toe: 1 (99) # (vingerafdruk lezen) (herhaal vingerafdruk lezen) (herhaal vingerafdruk lezen)

3. Verlaat de programmeermodus: *

Voeg paniekgebruiker toe

1. Ga naar de programmeermodus: * hoofdcode *

2.1. Voeg kaart toe: 1 (gebruikers-ID) # (kaart lezen of handmatig kaartnummer invoeren) #

2.2 Voeg pincode toe: 1 (gebruikers-ID) # (PIN) #

3. Verlaat de programmeermodus: *

Voeg bezoeker toe

Er kunnen maximaal 10 bezoekers worden toegevoegd met pincode of kaart. Bezoekers kunnen de pincode of kaart maximaal 10 keer gebruiken. Na maximaal 10 keer gebruiken wordt de pincode of kaart automatisch

ongeldig.

1. Ga naar de programmeermodus: * hoofdcode *

2.1. Kaart toevoegen: 1 (gebruikers-ID) # (0~9) # (kaart lezen of handmatig kaartnummer invoeren) #

2.2 PIN toevoegen: 1 (gebruikers-ID) # (0~9) # (PIN) #

3. Programmeermodus verlaten: *

Gebruiker verwijderen

1. Programmeermodus openen: * Mastercode #

2.1. Gebruiker verwijderen met vingerafdruk, kaart of pincode: 2 (vingerafdruk lezen/kaart lezen/pincode invoeren) #

2.2 Gebruiker verwijderen op ID-nummer: 2 (gebruikers-ID) #

2.3 Gebruiker verwijderen op kaartnummer: 2 (kaartnummer invoeren) #

2.4. Alle gebruikers verwijderen: 2 (mastercode) #

3. Programmeermodus verlaten: *

Configuratie relaisactiveringsmodus

De relaisconfiguratie beïnvloedt het gedrag na het invoeren van de toegangscode.

1. Programmeermodus openen: * Mastercode #

2.1. Impulsmodus (standaardmodus): 3 (1~99) #

Het relais wordt geactiveerd gedurende een periode

van 0-99 seconden (standaard 5 seconden) na het invoeren van de code en wordt vervolgens automatisch gedeactiveerd.

De activeringstijd van het relais is 1-99 seconden. Standaard: 5 seconden.

2.2. Wisselmodus: 3 0 #

Het relais verandert van status telkens wanneer de code correct wordt ingevoerd:

Als het uit is (open), activeert het (sluit het contact). Als het geactiveerd is, deactiveert het.

Handig voor poorten of deuren die open moeten blijven totdat ze handmatig weer worden gesloten.

3. Programmeermodus verlaten: *

Instelling toegangsmodus

Voor de toegangsmodus voor meerdere gebruikers mag het tijdsinterval waarin de toegangscodes worden gelezen niet langer zijn dan 5 seconden. Na 5 seconden gaat het apparaat automatisch in de stand-bymodus.

1. Programmeermodus openen: * Mastercode #

2.1. Toegang met vingerafdruk: 4 0 #

2.2. Toegang met kaart: 4 1 #

2.3. Toegang met pincode: 4 2 #

2. 4. Toegang voor meerdere gebruikers: 4 3 (2~9) #

Pas nadat 2~9 gebruikers zijn gevalideerd, gaat de

deur open.

2.5. Vingerafdruk of kaart of pincode (standaard): 4 4 #

3. Programmeermodus verlaten: *

Alarm voor herhaalde mislukte pogingen

Verwijst naar een alarm dat wordt geactiveerd na een opeenvolgend aantal van 10 onjuiste toegangspogingen (het invoeren van een verkeerde code, ongeldige kaart, enz.). De toegang kan 10 minuten worden geweigerd of pas na het invoeren van een geldige code, kaart of vingerafdruk.

1. Programmeermodus openen: * Mastercode #

2.1. Functie uitgeschakeld (standaard): 6 0 #

2.2. Functie ingeschakeld: 6 1 # (toegang is 10 minuten geblokkeerd)

2.3. Functie ingeschakeld (Alarm): 6 2 #

Instelling alarmduur: 5 (0~3) #. Standaard 1 minuut.

Om het alarm te stoppen, voert u de mastercode in of scant u de mastervingerafdruk/kaart, voert u de pincode in of scant u een gebruikersvingerafdruk/kaart.

3. Programmeermodus verlaten: *

Waarschuwing deur open

Als u een bedraad magnetisch deurcontact op het

toegangscontroletoetsenbord hebt aangesloten en de deur langer dan 1 minuut open blijft staan, klinkt de ingebouwde zoemer om de gebruiker eraan te herinneren de deur te sluiten. Het geluid kan worden gestopt door de deur te sluiten of een geldige toegangscode (master- of gebruikerscode) in te voeren. Anders blijft het geluid aanhouden zolang het is ingesteld.

Waarschuwing voor geforceerde deur

Als u een bedraad magnetisch deurcontact hebt aangesloten op het toegangscontroletoetsenbord en de deur wordt geforceerd geopend, laten de ingebouwde zoemer en de externe sirene (indien aanwezig) het alarm afgaan. Het geluid kan worden gestopt door de deur te sluiten of een geldige toegangscode in te voeren (master- of gebruikerscode). Anders blijft het geluid aanhouden zolang het is ingesteld.

1. Ga naar de programmeermodus: * Mastercode #

2.1. Functie uitgeschakeld (standaard): 6 3 #

2.2. Functie ingeschakeld” 6 4 #

Stel de alarmduur in: 5 (0~3) #. Standaard 1 minuut.

3. Programmeermodus verlaten: *

Instelling zoemer en led

1. Programmeermodus openen: * Mastercode #

2.1. Zoemer uitschakelen: 7 0 #

2.2. Zoemer inschakelen (standaard): 7 1 #

3.1. Led uit: 7 2 #

3.2. Led aan (standaard): 7 3 #

4.1. Toetsenbordverlichting uit: 7 4 #

4.2. Toetsenbordverlichting altijd aan: 7 5 #

4.3. Toetsenbordverlichting automatisch uit (standaard): 7 6 #. 20 seconden na de laatste bediening schakelt het toetsenbord automatisch uit. Door een toets aan te raken, licht het toetsenbord op.

3. Programmeermodus verlaten: *

Vingerafdruk/kaart/pincode van gebruiker toevoegen met mastercard/vingerafdruk

1. Lees de mastercard/vingerafdruk.

2. Scan de vingerafdruk van de gebruiker 3 keer of scan de kaart of pincode van de gebruiker.

Herhaal stap 2 om meer gebruikers achter elkaar toe te voegen.

3. Scan de mastercard/vingerafdruk opnieuw.

Vingerafdruk/kaart/pincode van een gebruiker verwijderen met een mastercard/vingerafdruk

1. Scan de mastercard/vingerafdruk twee keer binnen maximaal 5 seconden.

2. Scan de vingerafdruk/kaart of voer de pincode van de gebruiker in.

Herhaal stap 2 om meer gebruikers achter elkaar te verwijderen.

3. Scan de mastercard/vingerafdruk opnieuw.

Resetten en een mastercard toevoegen

Als u een toegangsknop op het toegangscontroletoetsenbord hebt aangesloten, gaat u als volgt te werk om het toetsenbord te resetten:

1. Schakel de stroom uit.

2. Houd de toegangsknop ingedrukt terwijl u de stroom weer inschakelt.

3. U hoort 2 pieptonen.

4. Haal uw vinger van de toegangsknop.

5. De gele led gaat branden.

6. Lees een 125 kHz EM-kaart.

7. De led gaat rood branden.

8. Het toetsenbord is gereset.

9. De gelezen kaart is nu de masterkaart.

Opmerkingen:

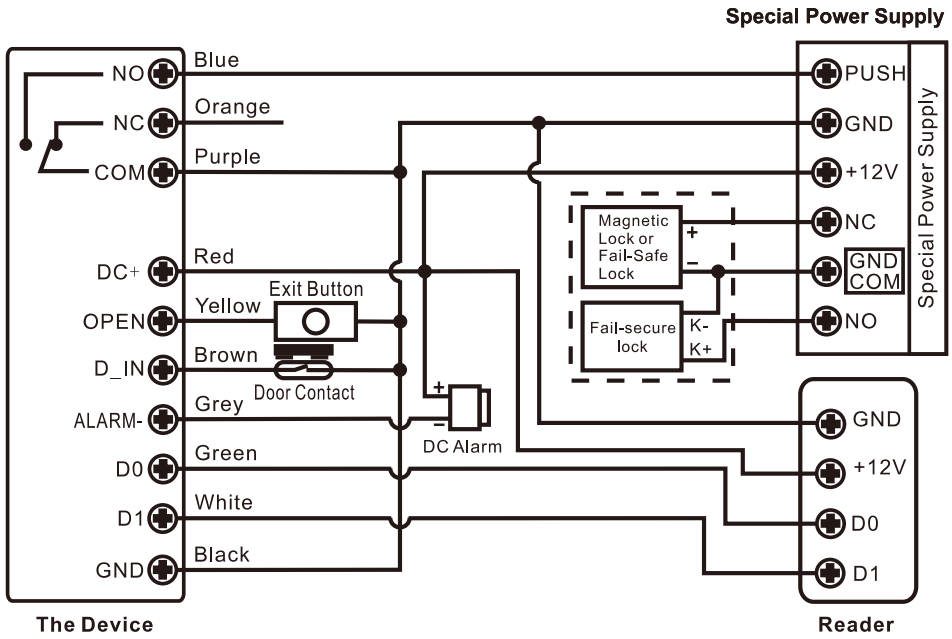
1. Als u geen masterkaart wilt toevoegen, moet u de toegangsknop minimaal 5 seconden ingedrukt houden voordat u deze loslaat. Deze procedure maakt de vorige masterkaart ongeldig.

2. Door te resetten worden de gebruikersgegevens niet verwijderd.

2. Controllermodus

Het toetsenbord functioneert als controller als het is aangesloten op een Wiegand-lezer.

Verbindingsschema



Let op: het is noodzakelijk om de meegeleverde 1N4004-diode of een gelijkwaardige module te installeren als u een voeding gebruikt waarop andere apparaten zijn aangesloten.

Instelling Wiegand-ingangsformaat

1. Programmeermodus openen: * Mastercode #

2. Wiegand-ingangsbits voor EM-kaart instellen:

8 (26~44) # (standaard 26 bits)

3.1. Pariteitsbit uitschakelen: 8 0 #

3.2. Pariteitsbit inschakelen: 8 1 #

3. Programmeermodus verlaten: *

Programmeren

De basisprogrammering is hetzelfde als in de standalone-modus.

Aansluiten op een externe kaartlezer

In het geval van een EM- of Mifare-kaartlezer kunnen gebruikers zowel op het toetsenbord als op de externe lezer worden toegevoegd/verwijderd.

In het geval van een HID-kaartlezer kunnen gebruikers alleen op de externe lezer worden toegevoegd/verwijderd.

Aansluiten op een vingerafdruklezer

Sluit de vingerafdruklezer aan op het toetsenbord.

1. Programmeermodus openen: * Mastercode #

2.1. Type 1 (lezen van de vingerafdruk op de vingerafdruklezer) #. De ID wordt automatisch toegewezen.

2.2. Type 1 (gebruikers-ID) # (lezen van de vingerafdruk op de vingerafdruklezer) #

3. Programmeermodus verlaten: *

Aansluiten op een keypadlezer

De keypadlezer kan 4 bits, 8 bits (ASCII) of 10 bits zijn.

1. Programmeermodus openen: * Mastercode #

2.1. Voer het aantal bits in: 8 (4, 8 of 10) #. De standaardwaarde is 4 bits.

3. Programmeermodus verlaten: *

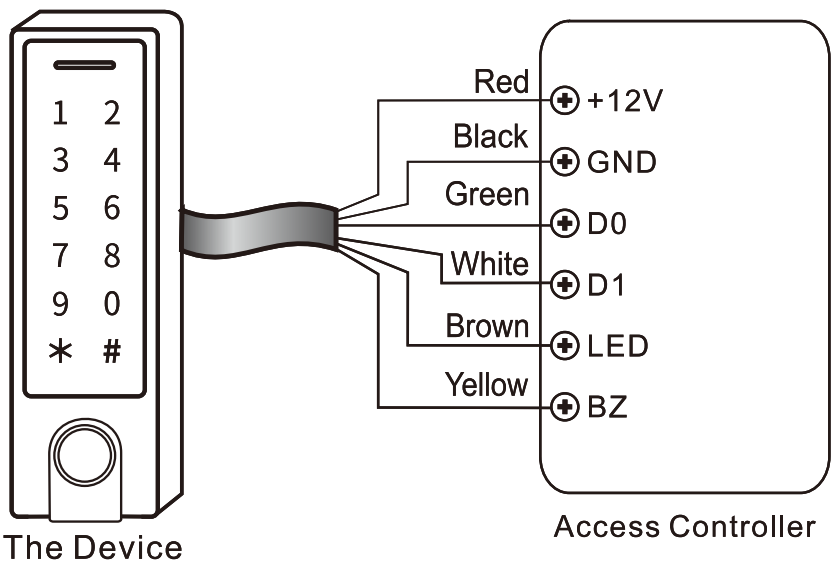
Gebruikerspincode toevoegen/verwijderen

De gebruikerspincode kan worden toegevoegd/verwijderd op zowel het toegangscontrolekeyboard als de externe keypadlezer.

3. Wiegand-lezermodus

Het keyboard kan ook functioneren als een standaard Wiegand-lezer die is aangesloten op een externe controller.

Verbindingsschema



Wanneer het toetsenbord in de Wiegand-lezermodus staat, worden alle instellingen die in de controllermodus zijn gemaakt ongeldig. De dikke en gele draden worden als volgt opnieuw gedefinieerd:

Bruine draad: Groene LED-bediening

Gele draad: Zoemerbediening.

Instelling Wiegand-uitvoerformaat

1. Programmeermodus openen: * Mastercode #

2. Wiegand-bits voor EM-kaart instellen: 8 (26~44) #

3.1. Pariteitsbit uitschakelen: 8 0 #

3.2. Pariteitsbit inschakelen: 8 1 # (standaard)

3. Programmeermodus verlaten: *

Opmerking: om een Wiegand-controller aan te sluiten, moet u de pariteitsbit uitschakelen.

Geavanceerde toepassingen

Toegang voor alle kaarten

Na activering van deze modus kunnen alle kaarten de deur openen. Tegelijkertijd wordt de kaart aan het systeem toegevoegd.

1. Programmeermodus openen: * Mastercode #

2.1. Functie uitschakelen: 9 2 # (standaard)

2.2. Functie inschakelen: 9 3 #

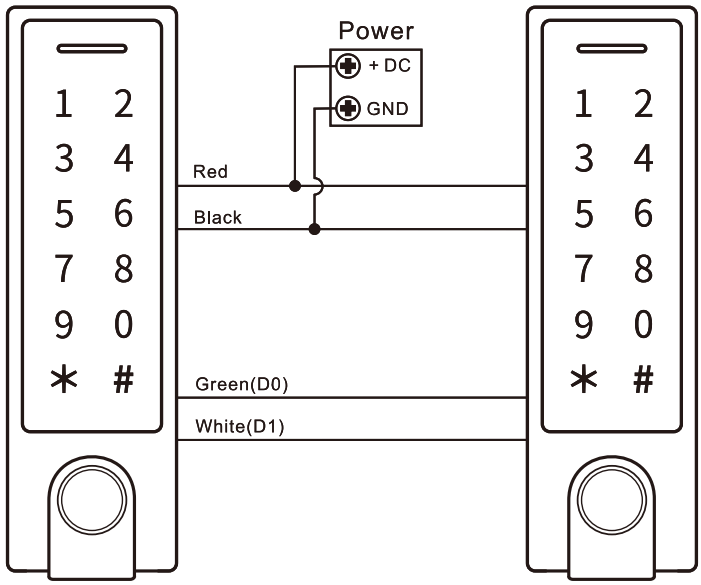
3. Programmeermodus verlaten: *

Gebruikersgegevens overdragen

Voor gebruikers die geregistreerd zijn met een pincode/kaart.

Gebruikersgegevens kunnen van het ene toetsenbord naar het andere worden overgedragen.

Verbindingsschema



Opmerkingen:

Beide toetsenborden moeten uit dezelfde serie komen.

De mastercode van beide toetsenborden moet identiek zijn.

Activeer de overdrachtsfunctie alleen op het hoofdtoetsenbord (mastertoetsenbord).

Als het secundaire toetsenbord al geregistreerde gebruikers heeft, worden deze tijdens de overdracht overschreven.

Bij een aantal van 900 gebruikers kan de overdracht tot 30 seconden duren.

Activeer de overdrachtsmodus op het mastertoetsenbord

1. Ga naar de programmeermodus: * Mastercode #

2. Typ 9 8 #

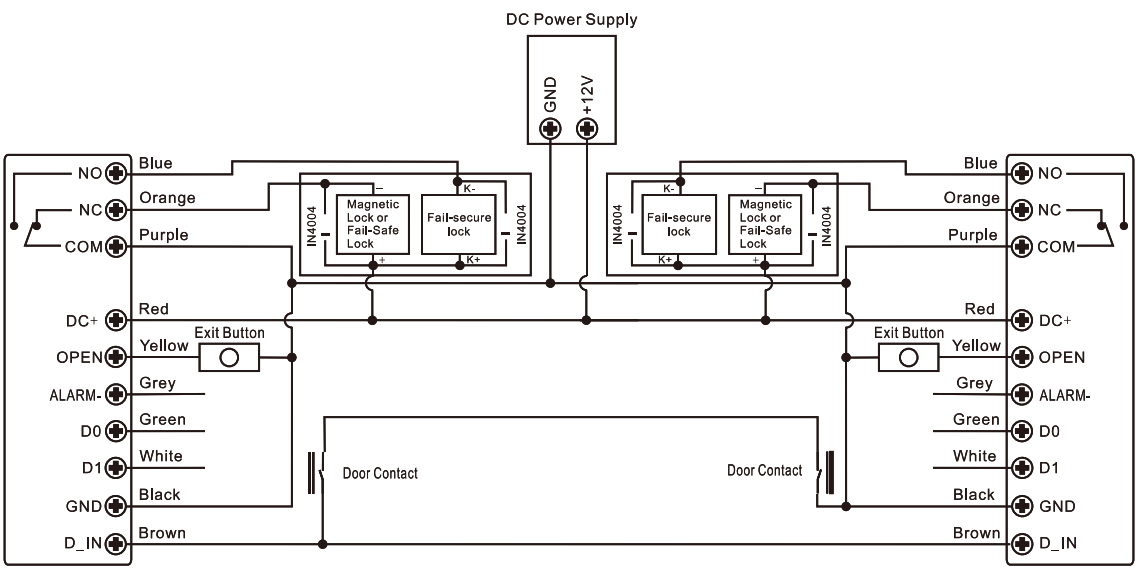
Gedurende 30 seconden, de maximale overdrachtsduur, brandt de groene LED. Wanneer de gegevensoverdracht is voltooid, klinkt er een pieptoon en gaat de rode LED branden.

3. Verlaat de programmeermodus: *

Toetsenborden met elkaar verbinden

Deze modus houdt in dat twee toetsenborden met elkaar worden verbonden om twee deuren te bedienen. Deze functie is met name handig in gevangenissen, banken en andere locaties waar een hoger beveiligingsniveau vereist is..

Verbindingsschema



Registreer gebruikers op toetsenbord A en verplaats ze vervolgens naar toetsenbord B.

Schakel de interlockmodus in op beide toetsenborden:

1. Ga naar de programmeermodus: * Mastercode #

2.1. Functie uitschakelen: 9 0 # (standaard)

2.2. Functie inschakelen: 9 1 #

3. Programmeermodus verlaten: *

Wanneer de functie actief is en deur 2 gesloten moet blijven, kan de gebruiker de vingerafdruk/kaart scannen of de pincode invoeren op toetsenbord A. Deur 1 gaat open. Wanneer deur 1 gesloten moet blijven, kan de gebruiker de vingerafdruk/kaart scannen of de pincode invoeren op toetsenbord B. Deur 2 gaat open.

Wanneer de functie actief is, kan de gebruiker de vingerafdruk/kaart scannen of de pincode invoeren op toetsenbord A om deur 1 te openen. Of scan de vingerafdruk/kaart of voer de pincode in op toetsenbord B om deur 2 te openen.

Toetsenbordbediening via de Tuya Smart-app

Let op: Vanwege frequente updates van de Tuya Smart-app kunnen de afbeeldingen en informatie in deze handleiding afwijken van die in de versie die op uw apparaat is geïnstalleerd.

Ga naar Google Play of App Store of scan de onderstaande QR-code en installeer de Tuya Smart-app.

Verbind je telefoon met het wifi-netwerk en activeer Locatie en Bluetooth.

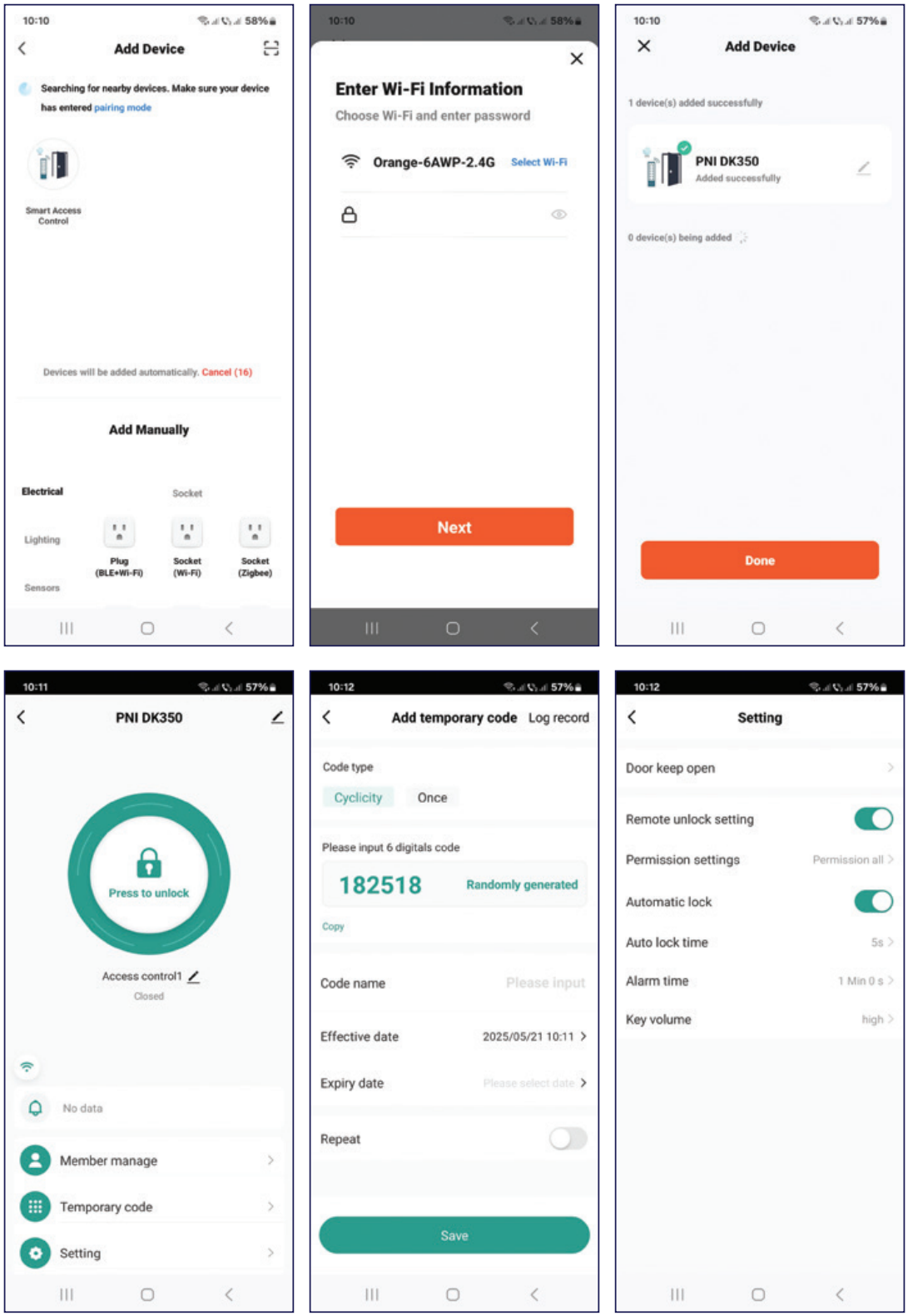
Open de app en log in.

Druk op “+” - “Apparaat toevoegen”.

De app herkent je apparaat automatisch.

Druk op het toetsenbordpictogram en volg de stappen op het scherm.

Opmerking: je kunt het toetsenbord ook handmatig aan de app toevoegen via de categorie Camera’s & Vergrendeling - Vergrendeling (wifi).



Met de applicatie kunt u de deur ontgrendelen, gebruikers toevoegen en beheren en een tijdelijke toegangscode genereren.

Podstawowe funkcje

Czujnik odcisku palca.

Klawisze dotykowe.

Wodoodporna obudowa metalowa (IP66).

Obsługuje 1000 użytkowników lokalnych (988 zwykłych użytkowników, 2 użytkowników paniki, 10 użytkowników tymczasowych).

Obsługuje 500 użytkowników za pośrednictwem aplikacji.

Obsługuje kartę EM 125 kHz.

Wyjście alarmu i brzęczyka.

Funkcja antywandalizmu.

Wiele metod dostępu: odcisk palca, karta, PIN, aplikacja.

Obsługuje tymczasowe hasło (jednorazowe lub okresowe).

Obsługuje dodawanie/usuwanie użytkowników za pośrednictwem aplikacji.

Obsługuje ustawianie ograniczeń czasowych dla użytkowników.

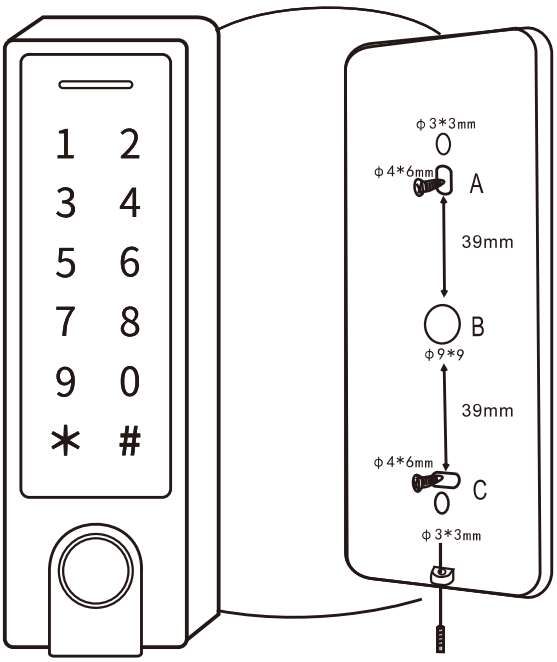
Dane techniczne

Napięcie robocze	12-18V DC
Moc czuwania	≤60mA

Moc robocza	≤150mA
Kompatybilna karta RFID	EM 125 KHz
Odległość odczytu karty RFID	2-6 cm
Połączenia wyjściowe	Przekaźnik, przycisk dostępu, alarm, czujnik drzwiowy, czytnik kart Wiegand
Połączenia wejściowe	Czytnik kart Wiegand
Przekaźnik	Jeden przekaźnik NO, NC, COM
Czas działania przekaźnika	0-99 s. (5 s. domyślnie)
Obciążenie wyjścia blokady	Maks. 2 A
Wyjście PIN	4 bity, 10-znakowy wirtualny numer
Stopień ochrony	IP66
Temperatura robocza	-26 ~ 80°C
Materiał obudowy	Stop cynku

Wymiary	148 x 44 x 22 mm
Wi-Fi	2.4 GHz/100mW
Bluetooth	2.4 GHz/2.5mW

Instalacja



A

Zdejmij wspornik z tyłu urządzenia.

Przymocuj wspornik do ściany za pomocą dostarczonych śrub.

Przeprowadź kabel połączeniowy przez otwór oznaczony literą B na poniższym rysunku.

Przymocuj urządzenie do wspornika.

Znajomości

Kolor przewodu	**Funkcjonować**	**Uwagi**
Czerwony	DC+	Wejście DC 12-18V
Czarny	GND	Wejście bieguna ujemnego DC

Niebieski	NO	Wyjście przekaźnika NO (podłącz diodę w pakiecie)
Fioletowy	COM	Wyjście przekaźnika COM
Pomarań czowy	NC	Wyjście przekaźnika NC (podłącz diodę w pakiecie)
Żółty	OPEN	Wejście przycisku dostępu
Połączenia za pomocą czytnika Wiegand lub kontrolera		
Zielony	Data 0	Wyjście Wieganda (pass-through)
Biały	Data 1	Wyjście Wieganda (pass-through)
Połączenia specjalne		
Szary	Wyjście alarmowe	Styk ujemny dla alarmu
Brązowy	Wejście	Wejście styku drzwi

Ostrzeżenia dźwiękowe i świetlne

Status	LED	Buzzer
Czuwanie	Czerwona dioda LED	-
Wchodzenie w tryb programowania	Czerwona dioda LED miga	Jeden sygnał dźwiękowy
Tryb programowania	Pomarańczowa dioda LED	Jeden sygnał dźwiękowy
Błąd działania	-	Trzy sygnały dźwiękowe
Wyjście z trybu programowania	Czerwona dioda LED	Jeden sygnał dźwiękowy
Otwieranie drzwi	Zielona dioda LED	Jeden sygnał dźwiękowy
Alarm	Czerwona dioda LED miga szybko	Sygnały dźwiękowe

Wejście i wyjście z trybu programowania

Wejście do trybu programowania: * kod główny #

Uwaga: domyślny kod główny to 123456.

Wyjście z trybu programowania: *

Ustawienie kodu głównego

1. Wejście do trybu programowania: * kod główny #

2. Zmiana kodu głównego: 0 (nowy kod główny)# (powtórz nowy kod główny)#

Uwaga: kod główny musi zawierać 6 znaków.

3. Wyjście z trybu programowania: *

Ustawianie trybu pracy

Dostępne są 3 tryby pracy: tryb samodzielny, tryb kontrolera i tryb czytnika Wiegand. Domyślnym trybem jest tryb samodzielny/kontrolera.

1. Wejście do trybu programowania: * kod główny #

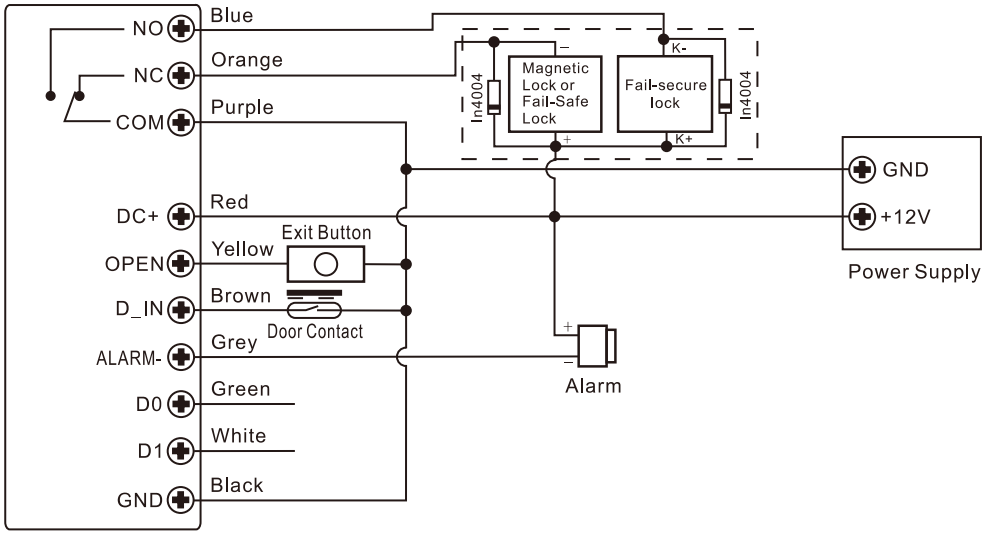
2. Wprowadź 7 7# (tryb domyślny) lub 7 8# (tryb Wiegand).

3. Wyjście z trybu programowania: *

1. Tryb samodzielny

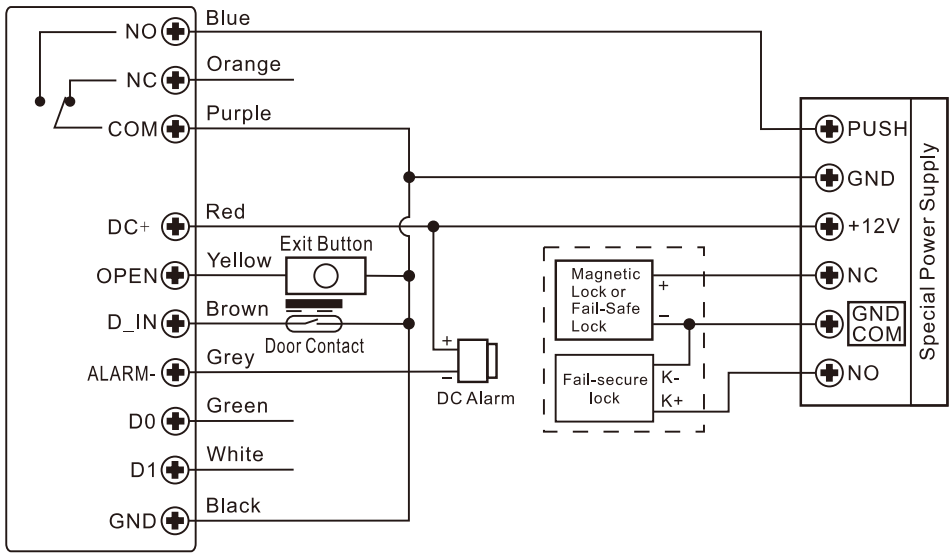
Schemat połączeń

Wspólne zasilanie:



Uwaga: należy zainstalować dołączoną diodę 1N4004 lub jej odpowiednik, jeśli używasz zasilacza, do którego podłączone są inne urządzenia.

Oddzielne źródło zasilania:



Programowanie

Programowanie różni się w zależności od trybu dostępu.

Uwagi:

1. Identyfikator użytkownika: Przypisz identyfikator

użytkownika dla każdego odcisku palca, kodu PIN lub karty dostępu, aby lepiej zarządzać informacjami o dostępie.

Wspólny identyfikator użytkownika:

Identyfikator użytkownika odcisku palca: 0-98

Identyfikator użytkownika PIN lub karty: 100-987

Identyfikator użytkownika głównego: 99

Identyfikator użytkownika paniki: 988-989

Identyfikator użytkownika gościa: 990-999

Ważne: Identyfikator użytkownika nie może być poprzedzony cyfrą 0 (zero). Rejestracja identyfikatorów użytkowników jest bardzo ważna. Zmiana użytkownika wymaga znajomości identyfikatora użytkownika.

2. Karta: System obsługuje tylko karty 125 KHz EM RFID.

3. PIN: Może zawierać od 4 do 6 znaków, z wyjątkiem sekwencji 8888, która jest zarezerwowana.

Dodaj zwykły odcisk palca użytkownika

1. Wejdź w tryb programowania: * kod główny #

2.1. Dodaj odcisk palca użytkownika, używając automatycznie przypisanego ID: 1 (odczyt odcisku palca) (powtórz odczyt odcisku palca) (powtórz odczyt odcisku palca ponownie)

Uwaga: odciski palców można dodawać w sposób ciągły.

2.2 Dodaj odcisk palca użytkownika, używając niestandardowego ID: 1 (ID użytkownika) # (odczyt odcisku palca) (powtórz odczyt odcisku palca) (powtórz odczyt odcisku palca ponownie). Uwaga: odciski palców można dodawać w sposób ciągły.

3. Wyjdź z trybu programowania: *

Dodaj kartę zwykłego użytkownika

1. Wejdź w tryb programowania: * kod główny #

2.1. Dodaj kartę użytkownika, używając automatycznie przypisanego ID: 1 (odczytaj kartę lub ręcznie wprowadź numer karty) #

Uwaga: odciski palców można dodawać w sposób ciągły.

2.2 Dodaj kartę użytkownika, używając spersonalizowanego ID: 1 (ID użytkownika) (zeskanuj kartę lub ręcznie wprowadź numer karty) #

2.3 Dodaj karty zbiorczo: umożliwia użytkownikowi głównemu dodanie do 888 kart w jednym kroku. Procedura trwa do 2 minut: 1 (ID użytkownika) # (liczba kart) # (ręcznie wprowadź numer pierwszej karty) #

Uwagi:

1. Liczba kart oznacza liczbę kart, które chcesz dodać do systemu.

2. Numery kart muszą być kolejne.

Dodaj zwykły kod PIN użytkownika

1. Wejdź w tryb programowania: * kod główny #

2.1. Dodaj kod PIN użytkownika, używając automatycznie przypisanego identyfikatora: 1 (kod PIN) #

2.2 Dodaj kod PIN użytkownika, używając niestandardowego identyfikatora: 1 (identyfikator użytkownika) # (kod PIN) #

3. Wyjdź z trybu programowania: *

Aby zwiększyć bezpieczeństwo, możesz ukryć kod PIN (maks. 6 znaków), wpisując do 10 znaków.

Na przykład:

Jeśli prawidłowy kod PIN to: 123434

Wpisz: **123434** lub **123434, gdzie ** może być dowolną liczbą od 0 do 9.

Dodaj odcisk palca użytkownika głównego

1. Wejdź w tryb programowania: * kod główny #

2. Dodaj odcisk palca: 1 (99) # (odczyt odcisku palca) (powtórz odczyt odcisku palca) (ponownie powtórz odczyt odcisku palca)

3. Wyjdź z trybu programowania: *

Dodaj użytkownika paniki

1. Wejdź w tryb programowania: * kod główny #

2.1. Dodaj kartę: 1 (ID użytkownika) # (odczytaj kartę lub ręcznie wprowadź numer karty) #

2.2 Dodaj PIN: 1 (ID użytkownika) # (PIN) #

3. Wyjdź z trybu programowania: *

Dodaj użytkownika-gościa

Maksymalnie 10 gości może zostać dodanych z PIN-em lub kartą. Goście mogą użyć PIN-u lub karty maksymalnie 10 razy. Po maksymalnie 10 użyciach PIN lub karta automatycznie staną się nieważne.

1. Wejdź do trybu programowania: * kod główny #

2.1. Dodaj kartę: 1 (ID użytkownika) # (0~9) # (odczytaj kartę lub ręcznie wprowadź numer karty) #

2.2 Dodaj PIN: 1 (ID użytkownika) # (0~9) # (PIN) #

3. Wyjdź z trybu programowania: *

Usuń użytkownika

1. Wejdź do trybu programowania: * kod główny #

2.1. Usuń użytkownika za pomocą odcisku palca, karty lub kodu PIN: 2 (odczytaj odcisk palca/odczytaj kartę/ wprowadź kod PIN) #

2.2 Usuń użytkownika za pomocą numeru ID: 2 (ID użytkownika) #

2.3 Usuń użytkownika za pomocą numeru karty: 2 (wprowadź numer karty) #

2.4. Usuń wszystkich użytkowników: 2 (kod główny)#

3. Wyjdź z trybu programowania: *

Konfiguracja trybu aktywacji przekaźnika

Konfiguracja przekaźnika wpływa na jego zachowanie po wprowadzeniu kodu dostępu.

1. Wejdź do trybu programowania: * kod główny #

2.1. Tryb impulsowy (tryb domyślny): 3 (1~99) #

Przekaźnik jest aktywowany na okres czasu od 0 do 99 sekund (domyślnie 5 sekund) po wprowadzeniu kodu, a następnie automatycznie się dezaktywuje.

Czas aktywacji przekaźnika wynosi 1-99 sekund. Domyślnie: 5 sekund.

2.2. Tryb naprzemienny: 3 0 #

Przekaźnik zmienia swój stan za każdym razem, gdy kod zostanie wprowadzony poprawnie:

Jeśli jest wyłączony (otwarty), aktywuje się (zamyka styk). Jeśli jest aktywowany, dezaktywuje się.

Przydatne w przypadku bram lub drzwi, które muszą pozostać otwarte, dopóki nie zostaną ponownie ręcznie zamknięte.

3. Wyjście z trybu programowania: *

Ustawienie trybu dostępu

W przypadku trybu dostępu dla wielu użytkowników odstęp czasu, w którym odczytywane są kody dostępu, nie powinien przekraczać 5 sekund. Po 5 sekundach

urządzenie automatycznie przechodzi w tryb czuwania.

1. Wejście do trybu programowania: * kod główny #

2.1. Dostęp za pomocą odcisku palca: 4 0 #

2.2. Dostęp za pomocą karty: 4 1 #

2.3. Dostęp za pomocą kodu PIN: 4 2 #

2. 4. Dostęp dla wielu użytkowników: 4 3 (2~9) #

Drzwi otworzą się dopiero po zatwierdzeniu 2~9 użytkowników.

2.5. Odcisk palca lub karta lub kod PIN (domyślnie): 4 4 #

3. Wyjście z trybu programowania: *

Alarm przy powtarzających się nieudanych próbach

Odnosi się do alarmu, który jest aktywowany po kolejnych 10 nieudanych próbach dostępu (wprowadzenie błędnego kodu, nieważnej karty itp.). Można go ustawić tak, aby odmawiał dostępu przez 10 minut lub zezwalał na dostęp tylko po wprowadzeniu prawidłowego kodu, karty lub odcisku palca.

1. Wejście do trybu programowania: * kod główny #

2.1. Funkcja wyłączona (domyślnie): 6 0 #

2.2. Funkcja włączona: 6 1 # (dostęp będzie zabroniony przez 10 minut)

2.3. Funkcja włączona (Alarm): 6 2 #

Ustawienie czasu trwania alarmu: 5 (0~3) #. Domyślnie 1 minuta.

Aby zatrzymać alarm, wprowadź kod główny # lub zeskanuj odcisk palca/kartę główną lub wprowadź kod PIN lub zeskanuj odcisk palca/kartę użytkownika.

3. Wyjdź z trybu programowania: *

Ostrzeżenie o otwartych drzwiach

Jeśli podłączyłeś przewodowy magnetyczny kontaktron drzwiowy do klawiatury kontroli dostępu i drzwi pozostają otwarte przez ponad 1 minutę, wbudowany brzęczyk wyda dźwięk przypominający użytkownikowi o zamknięciu drzwi. Dźwięk można zatrzymać, zamykając drzwi lub wprowadzając prawidłowy kod dostępu (główny lub użytkownika). W przeciwnym razie dźwięk będzie trwał tak długo, jak długo jest ustawiony.

Ostrzeżenie o wymuszonych drzwiach

Jeśli podłączyłeś przewodowy magnetyczny kontaktron drzwiowy do klawiatury kontroli dostępu i drzwi zostaną wymuszone, wbudowany brzęczyk i zewnętrzna syrena (jeśli jest) wyemitują alarm. Dźwięk można zatrzymać, zamykając drzwi lub wprowadzając prawidłowy kod dostępu (główny lub użytkownika). W przeciwnym razie dźwięk będzie trwał tak długo, jak długo jest ustawiony.

1. Wejdź w tryb programowania: * kod główny #

2.1. Funkcja wyłączona (domyślnie): 6 3 #

2.2. Funkcja włączona” 6 4 #

Ustaw czas trwania alarmu: 5 (0~3) #. Domyślnie 1 minuta.

3. Wyjdź z trybu programowania: *

Ustawienie brzęczyka i diody LED

1. Wejdź do trybu programowania: * kod główny #

2.1. Wyłącz brzęczyk: 7 0 #

2.2. Włącz brzęczyk (domyślnie): 7 1 #

3.1. Dioda LED wyłączona: 7 2 #

3.2. Dioda LED włączona (domyślnie): 7 3 #

4.1. Podświetlenie klawiatury wyłączone: 7 4 #

4.2. Podświetlenie klawiatury włączone przez cały czas: 7 5 #

4.3. Podświetlenie klawiatury wyłączone automatycznie (domyślnie): 7 6 #. Po 20 sekundach od ostatniej operacji klawiatura automatycznie się wyłączy. Dotknięcie dowolnego klawisza spowoduje podświetlenie klawiatury.

3. Wyjdź z trybu programowania: *

Dodawanie odcisku palca/karty/kodu PIN użytkownika za pomocą karty głównej/odcisku palca

1. Odczytaj kartę główną/odcisk palca.

2. Zeskanuj odcisk palca użytkownika 3 razy lub zeskanuj kartę użytkownika lub numer PIN

Powtórz krok 2, aby dodać kolejnych użytkowników.

3. Ponownie zeskanuj kartę główną/odcisk palca.

Usuwanie odcisku palca/karty/PIN użytkownika za pomocą karty głównej/odcisku palca

1. Zeskanuj kartę główną/odcisk palca dwa razy w ciągu maksymalnie 5 sekund.

2. Zeskanuj odcisk palca/kartę lub wprowadź numer PIN użytkownika

Powtórz krok 2, aby usunąć kolejnych użytkowników.

3. Ponownie zeskanuj kartę główną/odcisk palca.

Zresetuj i dodaj kartę główną

Jeśli podłączyłeś przycisk dostępu do klawiatury kontroli dostępu, wykonaj następujące czynności, aby zresetować klawiaturę:

1. Wyłącz zasilanie.

2. Naciśnij i przytrzymaj przycisk dostępu, włączając ponownie zasilanie.

3. Usłyszysz 2 sygnały dźwiękowe.

4. Zdejmij palec z przycisku dostępu.

5. Zaświeci się żółta dioda LED.

6. Odczytaj dowolną kartę EM 125 kHz.

7. Dioda LED zaświeci się na czerwono.

8. Klawiatura została zresetowana.

9. Odczytana karta stała się kartą główną.

Uwagi:

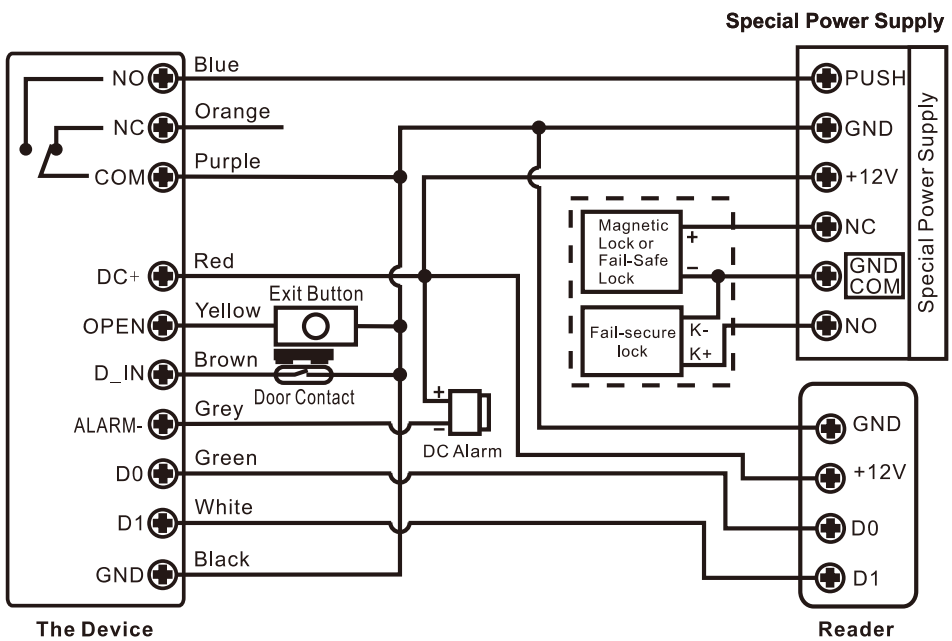
1. Jeśli nie chcesz dodać karty głównej, musisz przytrzymać przycisk dostępu przez co najmniej 5 sekund przed jego zwolnieniem. Ta procedura unieważni poprzednią kartę główną.

2. Po zresetowaniu informacje o użytkowniku nie zostaną usunięte.

2. Tryb kontrolera

Klawiatura będzie działać jako kontroler, jeśli zostanie podłączona do czytnika Wiegand.

Schemat połączeń



Uwaga: konieczne jest zainstalowanie dołączonej diody 1N4004 lub jej odpowiednika, jeśli używasz zasilacza, do którego podłączone są inne urządzenia.

Ustawienie formatu wejściowego Wiegand

1. Wejdź do trybu programowania: * kod główny #

2. Ustaw bity wejściowe Wiegand dla karty EM:

8 (26~44) # (domyślnie 26 bitów)

3.1. Wyłącz bit parzystości: 8 0 #

3.2. Włącz bit parzystości: 8 1 #

3. Wyjdź z trybu programowania: *

Programowanie

Podstawowe programowanie jest takie samo, jak w trybie autonomicznym.

Podłączanie do zewnętrznego czytnika kart

W przypadku czytnika kart EM lub Mifare, użytkowników można dodawać/usuwać zarówno na klawiaturze, jak i na czytniku zewnętrznym.

W przypadku czytnika kart HID, użytkowników można dodawać/usuwać tylko na czytniku zewnętrznym.

Podłączanie do czytnika linii papilarnych

Podłącz czytnik linii papilarnych do klawiatury.

1. Wejdź w tryb programowania: * kod główny #

2.1. Wpisz 1 (odczytaj odcisk palca na czytniku linii

papilarnych) #. ID jest automatycznie przypisywane.

2.2. Wpisz 1 (ID użytkownika) # (odczytaj odcisk palca na czytniku linii papilarnych) #

3. Wyjdź z trybu programowania: *

Podłączanie do czytnika klawiatury

Czytnik klawiatury może być 4-bitowy, 8-bitowy (ASCII) lub 10-bitowy.

1. Wejdź w tryb programowania: * kod główny #

2.1. Wpisz liczbę bitów: 8 (4 lub 8 lub 10) #. Domyślnie jest to 4 bity.

3. Wyjdź z trybu programowania: *

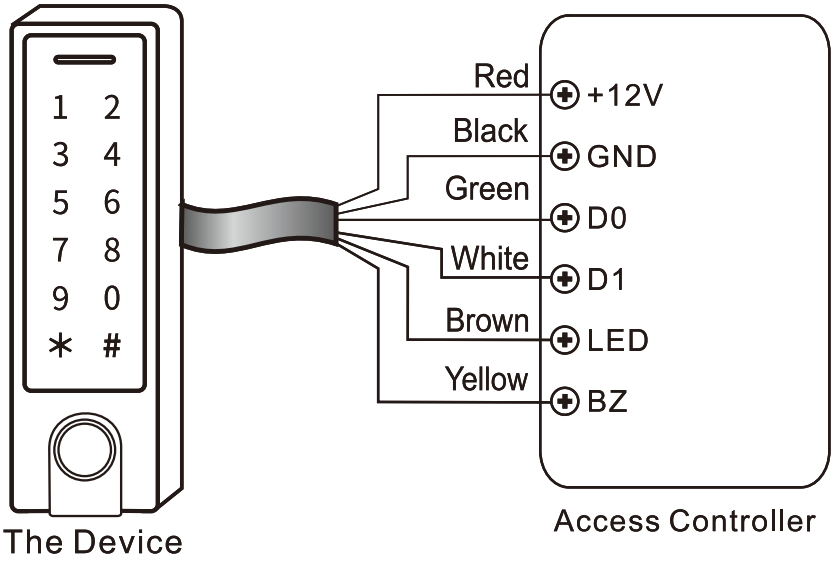
Dodaj/usuń kod PIN użytkownika

Kod PIN użytkownika można dodać/usunąć zarówno na klawiaturze kontroli dostępu, jak i na zewnętrznym czytniku klawiatury.

3. Tryb czytnika Wiegand

Klawiatura może również działać jako standardowy czytnik Wiegand podłączony do zewnętrznego kontrolera.

Schemat połączeń



Gdy klawiatura jest w trybie czytnika Wiegand, wszystkie ustawienia dokonane w trybie kontrolera stają się nieważne. Duży i żółty przewód zostaną zdefiniowane ponownie w następujący sposób:

Brązowy przewód: sterowanie zieloną diodą LED

Żółty przewód: sterowanie brzęczykiem.

Ustawienie formatu wyjściowego Wiegand

1. Wejdź do trybu programowania: * kod główny #

2. Ustaw bity Wiegand dla karty EM: 8 (26~44) #

3.1. Wyłącz bit parzystości: 8 0 #

3.2. Włącz bit parzystości: 8 1 # (domyślnie)

3. Wyjdź z trybu programowania: *

Uwaga: aby podłączyć kontroler Wiegand, musisz wyłączyć bit parzystości.

Zaawansowane aplikacje

Dostęp do wszystkich kart

Po aktywacji tego trybu wszystkie karty mogą otwierać drzwi. Jednocześnie karta jest dodawana do systemu.

1. Wejdź do trybu programowania: * kod główny #

2.1. Wyłącz funkcję: 9 2 # (domyślnie)

2.2. Włącz funkcję: 9 3 #

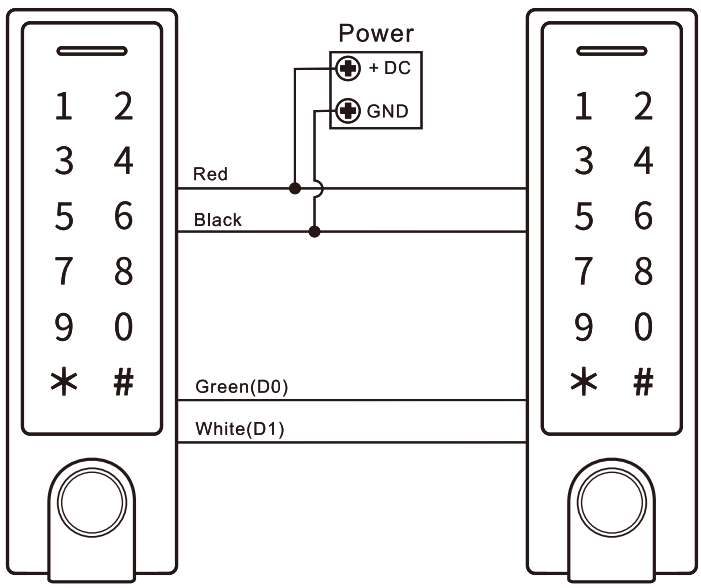
3. Wyjdź z trybu programowania: *

Przenieś informacje o użytkowniku

Dla użytkowników zarejestrowanych za pomocą kodu PIN/karty.

Informacje o użytkowniku można przenieść z jednej klawiatury na drugą.

Schemat połączeń



Uwagi:

Obie klawiatury muszą być z tej samej serii.

Kod główny obu klawiatur musi być identyczny.

Funkcję transferu należy aktywować tylko na klawiaturze głównej (klawiatura główna).

Jeśli klawiatura pomocnicza ma już zarejestrowanych użytkowników, zostaną oni nadpisani podczas transferu.

W przypadku liczby 900 użytkowników transfer może potrwać do 30 sekund.

Aktywuj tryb transferu na klawiaturze głównej

1. Wejdź w tryb programowania: * kod główny #

2. Wpisz 9 8 #

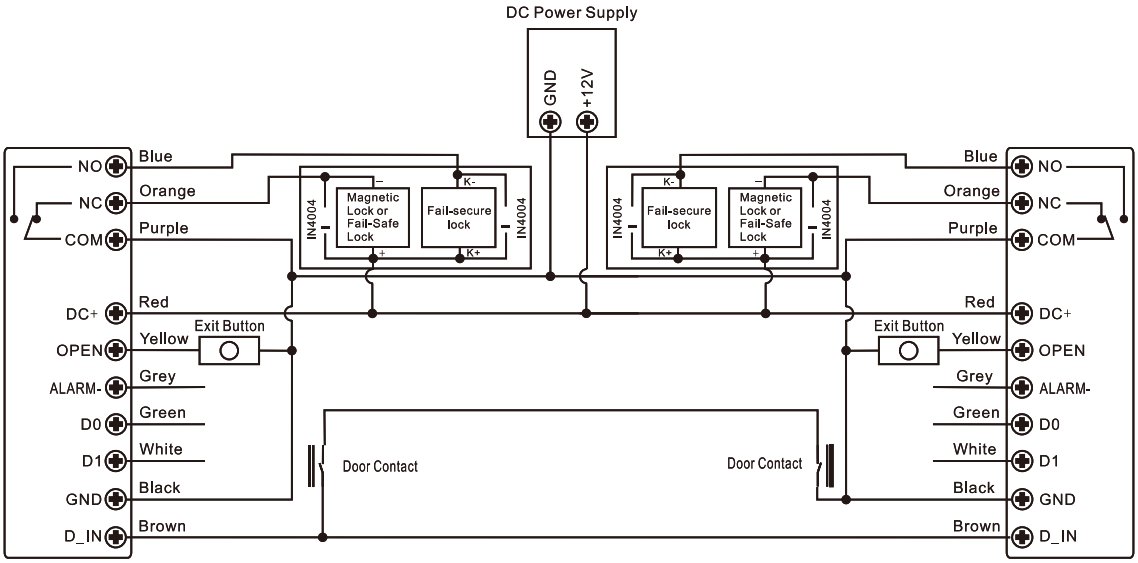
Przez 30 sekund, czyli maksymalny czas transferu, świeci się zielona dioda LED. Po zakończeniu transferu danych rozlegnie się sygnał dźwiękowy i zaświeci się czerwona dioda LED.

3. Wyjdź z trybu programowania: *

Łączenie klawiatur

Ten tryb oznacza łączenie dwóch klawiatur w celu sterowania dwoma drzwiami. Funkcja ta jest szczególnie przydatna w więzieniach, bankach i innych miejscach, w których wymagany jest wyższy poziom bezpieczeństwa.

Schemat połączeń



Zarejestruj użytkowników na klawiaturze A, a następnie przenieś ich na klawiaturę B.

Włącz tryb blokady na obu klawiaturach:

1. Wejdź w tryb programowania: * kod główny #

2.1. Wyłącz funkcję: 9 0 # (domyślnie)

2.2. Włącz funkcję: 9 1 #

3. Wyjdź z trybu programowania: *

Gdy funkcja jest aktywna, gdy drzwi 2 muszą pozostać zamknięte, użytkownik może zeskanować odcisk palca/kartę lub wprowadzić kod PIN na klawiaturze A. Drzwi 1 zostaną otwarte. Gdy drzwi 1 muszą pozostać zamknięte, użytkownik może zeskanować odcisk palca/kartę lub wprowadzić kod PIN na klawiaturze B. Drzwi 2 zostaną otwarte.

Gdy funkcja jest aktywna, użytkownik może zeskanować odcisk palca/kartę lub wprowadzić kod

PIN na klawiaturze A, aby otworzyć drzwi 1. Lub zeskanować odcisk palca/kartę lub wprowadzić kod PIN na klawiaturze B, aby otworzyć drzwi 2.

Sterowanie klawiaturą z aplikacji Tuya Smart

Uwaga: Ze względu na częste aktualizacje aplikacji Tuya Smart, obrazy i informacje przedstawione w tej instrukcji mogą różnić się od tych w wersji zainstalowanej na Twoim urządzeniu..

Przejdź do sklepu Google Play lub App Store lub zeskanuj poniższy kod QR i zainstaluj aplikację Tuya Smart.

Podłącz telefon do sieci WiFi, aktywuj Lokalizację i Bluetooth.

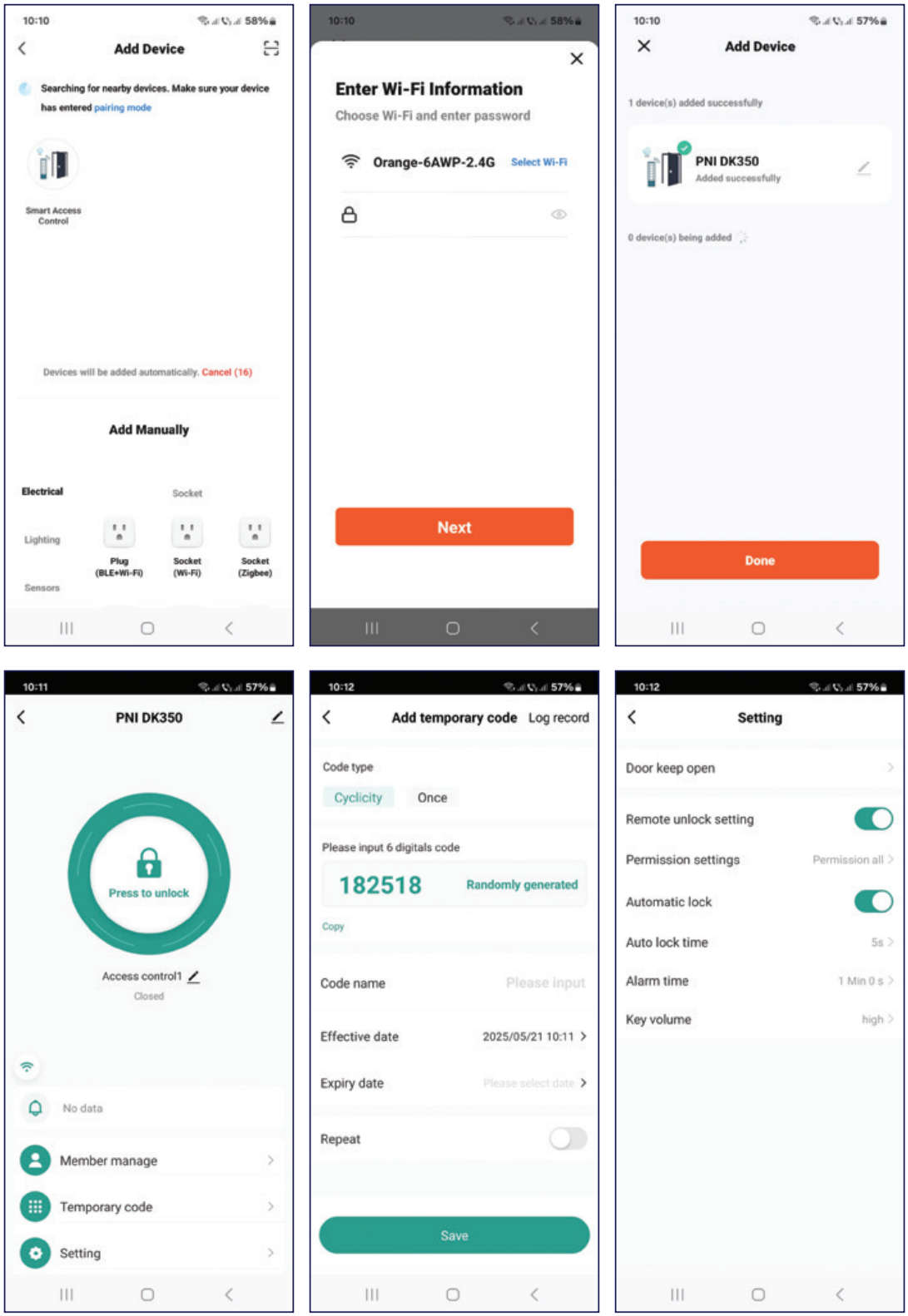
Otwórz aplikację i zaloguj się.

Naciśnij „+“ - „Dodaj urządzenie“.

Aplikacja automatycznie zidentyfikuje Twoje urządzenie.

Naciśnij ikonę klawiatury i postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.

Uwaga: możesz również ręcznie dodać klawiaturę do aplikacji, uzyskując dostęp do kategorii Aparaty i blokada - Blokada (Wi-Fi).



Aplikacja umożliwia otwieranie drzwi, dodawanie i zarządzanie użytkownikami oraz generowanie tymczasowego kodu dostępu.

Caracteristici de baza

Senzor de amprenta.

Taste tactile.

Carcasa metalica rezistenta la apa (IP66).

Suporta 1000 utilizatori locali (988 utilizatori comuni, 2 utilizatori de panica, 10 utilizatori temporari).

Suporta 500 de utilizatori prin aplicatie.

Suporta card RFID EM 125KHz.

Iesire pentru alarma si buzzer.

Functie antivandalism.

Multiple metode de acces: amprenta, card, PIN, aplicatie.

Suporta parola temporara (cu utilizare unica sau pe o perioada).

Suporta adaugare/stergere utilizatori prin aplicatie.

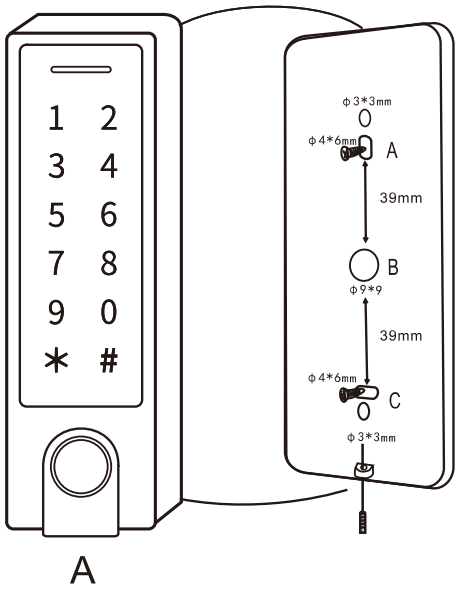
Suporta setare restrictii orare pentru utilizatori.

Specificatii tehnice

Tensiune de operare	12-18V DC
Consum in standby	≤60mA
Consum in lucru	≤150mA
Card RFID compatibil	EM 125 KHz

Distanta citire card RFID	2-6 cm
Conexiuni de iesire	Releu, buton de acces, alarma, senzor de usa, cititor de card Wiegand
Conexiuni de intrare	Cititor de card Wiegand
Releu	Un releu NO, NC, COM
Durata actionare releu	0-99 sec. (5 sec. implicit)
Sarcina iesire yala electromagnetica	Max. 2A
Iesire PIN	4 bits, numar virtual din 10 caractere
Clasa de protectie la apa	IP66
Temperatura de lucru	-26 ~ 80°C
Material carcasa	Aliaj de zinc
Dimensiuni	148 x 44 x 22 mm
Wi-Fi	2.4 GHz/100mW
Bluetooth	2.4 GHz/2.5mW

Instalare



Scoateti suportul de pe spatele unitatii.
Fixati suportul pe perete cu ajutorul suruburilor incluse.
Treceti cablul de conexiuni prin gaura marcata cu B in desenul alaturat.
Fixati unitatea pe suport.

Conexiuni

Fir	Functie	Note
Rosu	DC+	Intrare DC 12-18V
Negru	GND	Intrare DC pol negativ
Albastru	NO	Iesire NO releu (conectati dioda din pachet)
Violet	COM	Iesire COM releu
Orange	NC	Iesire NC releu (conectati dioda din pachet)
Galben	OPEN	Intrare buton de acces

Conexiuni printr-un cititor sau controller Wiegand		
Verde	Data 0	Iesire Wiegand (pass-through)
Alb	Data 1	Iesire Wiegand (pass-through)
Conexiuni speciale		
Gri	Iesire alarma	Contact negativ pentru alarma
Maro	Intrare	Intrare senzor de usa cablat

Avertizari audio si luminoase

Status	LED	Buzzer
Standby	LED rosu	-
Intrare in mod programare	LED rosu clipeste	Un beep
Mod programare	LED orange	Un beep
Eroare operare	-	Trei beep-uri

Iesire mod programare	LED rosu	Un beep
Deschidere yala	LED verde	Un beep
Alarma	LED rosu clipeste des	Beep-uri

Intrare si iesire din modul de programare

Intrare mod programare: *cod master#

Nota: codul master implicit este 123456.

Iesire mod programare: *

Setare cod master

1. Intrati in modul de programare: *cod master#

2. Schimbati codul master: 0 (codul master nou)# (repetati codul master nou)#

Nota: codul master trebuie sa contina 6 caractere.

3. Iesiti din modul de programare: *

Exemplu: schimbare cod master 123456 cu 654321: *123456#0654321#654321#*

Comportament tastatura: *(LED-ul clipeste rosu si asteapta codul master) 123456 # (beep/LED-ul se aprinde verde scurt si apoi rosu) 0 (LED-ul se aprinde portocaliu) 654321#654321# Apasati tasta “steluta“ pentru a iesi din modul programare.

Testati codul setat.

Setare mod de operare

Sunt 3 moduri de operare: mod standlone, mod controller si mod cititor Wiegand. Modul implicit este modul standalone/controller.

1. Intrati in modul de programare: *cod master#

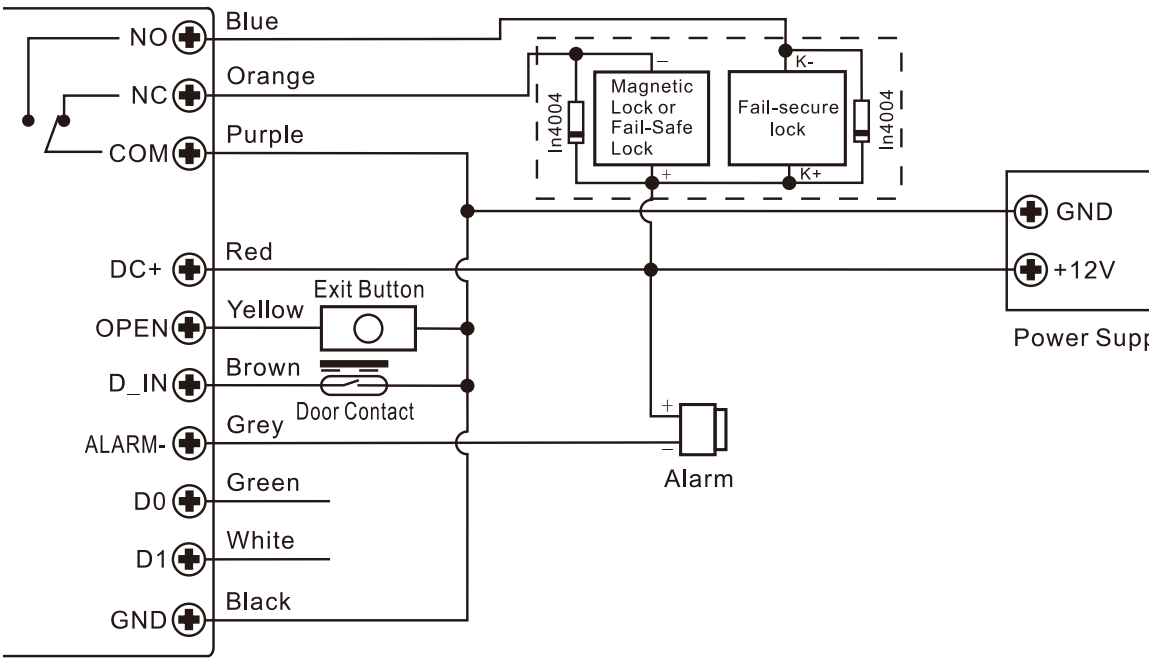
2. Tastati 7 7 # (modul implicit) sau 7 8 # (modul Wiegand).

3. Iesiti din modul de programare: *

1. Modul Standalone (operare independenta)

Diagrama conexiuni

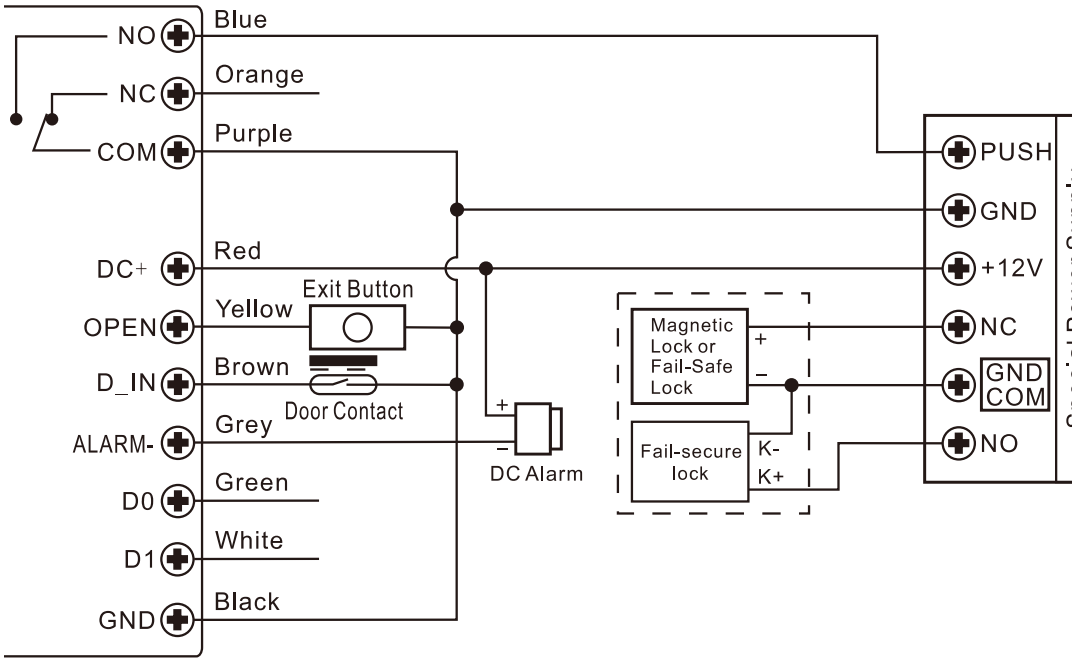
Alimentare comuna:



Atentie: este necesar sa instalati dioda 1N4004 inclusa sau una echivalenta daca folositi o sursa de alimentare

la care mai sunt conectate si alte dispozitive.

Alimentare separata:



Programare

Programarea difera in functie de modul de acces.

Note:

1. ID utilizator: alocati un ID utilizator pentru fiecare amprenta, PIN sau card de acces pentru o gestionare mai buna a informatiilor de acces.

ID utilizator comune:

ID utilizator pentru amprenta: 0-98

ID utilizator pentru PIN sau card: 100-987

ID utilizator pentru master: 99

ID utilizator pentru panica: 988-989

ID utilizator pentru vizitator: 990-999

Important: ID-ul de utilizator nu trebuie sa fie precedat de 0 (zero). Inregistrarea ID-urilor de utilizator este foarte importanta. Modificarea unui utilizator necesita cunoasterea ID-ului utilizatorului.

2. Card: sistemul suporta doar carduri RFID EM 125 KHz.

3. PIN: poate contine 4-6 caractere, cu exceptia secventei 8888 care este rezervata.

Adaugare amprenta utilizator obisnuit

1. Intrati in modul de programare: *cod master#

2.1. Adaugati amprenta utilizator folosind ID-ul alocat automat: 1 (cititi amprenta)(repetati citirea amprentei) (repetati din nou citirea amprentei)

Nota: amprentele pot fi adaugate in continuu.

2.2 Adaugati amprenta utilizator folosind un ID personalizat: 1 (ID utilizator) # (cititi amprenta) (repetati citirea amprentei) (repetati din nou citirea amprentei). Nota: amprentele pot fi adaugate in continuu.

3. Iesiti din modul de programare: *

Adaugare card utilizator obisnuit

1. Intrati in modul de programare: *cod master#

2.1. Adaugati card utilizator folosind ID-ul alocat automat: 1 (cititi cardul sau introduceti manual numarul cardului) #

Nota: amprentele pot fi adaugate in continuu.

2.2 Adaugati card utilizator folosind un ID personalizat: 1 (ID utilizator) (cititi cardul sau introduceti manual numarul cardului) #

2.3 Adaugati carduri in bloc: permite utilizatorului Master sa adauge pana la 888 de carduri intr-un singur pas. Procedura dureaza pana la 2 minute: 1 (ID utilizator) # (cantitatea de carduri) # (introduceti manual numarul primului card) #

Note:

1. Cantitatea de carduri reprezinta numarul de carduri care se doreste a fi adaugate in sistem.

2. Numerele cardurilor trebuie sa fie consecutive.

Adaugare PIN utilizator obisnuit

1. Intrati in modul de programare: *cod master#

2.1. Adaugati PIN utilizator folosind ID-ul alocat automat: 1 (PIN) #

2.2 Adaugati PIN utilizator folosind un ID personalizat: 1 (ID utilizator) # (PIN) #

3. Iesiti din modul de programare: *

Exemplu: adaugare PIN deschidere 4321: *123456#1 4321#

Comportament tastatura: *(LED-ul clipeste rosu si asteapta codul master) 123456 # (beep/LED-ul se aprinde verde scurt si apoi rosu) 1 (LED-ul se aprinde

portocaliu) 4321# Apasati tasta “steluta“ pentru a iesi din modul programare. Testati codul setat: 4321# Tastatura va confirma deschiderea. LED-ul se va aprinde verde.

Pentru o securitate sporita, puteti ascunde PIN-ul (max. 6 caractere) tastand pana la 10 caractere.

De exemplu:

Daca PIN-ul corect este: 123434

Tastati: **123434** sau **123434, unde ** poate fi orice numar de la 0 la 9.

Adaugare amprenta utilizator Master

1. Intrati in modul de programare: *cod master#

2. Adaugati amprenta: 1 (99) # (cititi amprenta) (repetati citirea amprentei) (repetati din nou citirea amprentei)

3. Iesiti din modul de programare: *

Adaugati utilizator de panica

1. Intrati in modul de programare: *cod master#

2.1. Adaugati card: 1 (ID utilizator) # (cititi cardul sau introduceti manual numarul cardului) #

2.2 Adaugati PIN: 1 (ID utilizator) # (PIN) #

3. Iesiti din modul de programare: *

Adaugare utilizator vizitator

Pot fi adaugati maxim 10 vizitatori cu PIN sau card. Vizitatorii pot folosi PIN-ul sau cardul de maxim 10 ori. Dupa maxim 10 utilizari, PIN-ul sau cardul devin automat invalide.

1. Intrati in modul de programare: *cod master#

2.1. Adaugati card: 1 (ID utilizator) # (0~9) # (cititi cardul sau introduceti manual numarul cardului) #

2.2 Adaugati PIN: 1 (ID utilizator) # (0~9) # (PIN) #

3. Iesiti din modul de programare: *

Stergere utilizator

1. Intrati in modul de programare: *cod master#

2.1. Stergeti utilizator pe baza de amprenta, card sau PIN: 2 (cititi amprenta/cititi cardul/introduceti PIN-ul) #

2.2 Stergeti utilizator pe baza de numar ID: 2 (ID utilizator) #

2.3 Stergeti utilizator pe baza de numar card: 2 (introduceti numarul cardului) #

2.4. Stergeti toti utilizatorii: 2 (cod master) #

3. Iesiti din modul de programare: *

Configurare mod activare releu

Configurarea releului influenteaza comportamentul acestuia dupa introducerea codului de acces.

1. Intrati in modul de programare: *cod master#

2.1. Mod impuls (modul implicit): 3 (1~99) #

Releul este activat pentru o perioada de timp cuprinsa intre 0-99 secunde (implicit 5 secunde) dupa introducerea codului, apoi se dezactiveaza automat.

Timpul de actionare a releului este de 1-99 secunde. Implicit: 5 secunde.

2.2. Mod alternant: 3 0 #

Releul isi schimba starea de fiecare data cand codul este introdus corect:

Daca este oprit (deschis), se activeaza (inchide contactul). Daca este activat, se dezactiveaza.

Util pentru porti sau usi care trebuie sa ramana deschise pana cand sunt inchise manual din nou.

3. Iesiti din modul de programare: *

Setare mod acces

Pentru modul de acces pentru multipli utilizatori, intervalul de timp in care are loc citirea codurilor de acces nu trebuie sa depaseasca 5 secunde. Dupa 5 secunde, unitatea intra automat in standby.

1. Intrati in modul de programare: *cod master#

2.1. Acces cu amprenta: 4 0 #

2.2. Acces cu card: 4 1 #

2.3. Acces cu PIN: 4 2 #

2. 4. Acces utilizatori multipli: 4 3 (2~9) #

Doar dupa 2~9 utilizatori validati, usa se va deschide.

2.5. Amprenta sau Card sau PIN (implicit): 4 4 #

3. Iesiti din modul de programare: *

Alarma la incercari esuate repetate

Se refera la o alarma care se activeaza dupa un numar consecutiv de 10 incercari gresite de acces (introducere cod gresit, card invalid etc.).Se poate seta ca timp de 10 minute sa fie refuzat accesul sau accesul sa fie permis doar dupa introducerea unui cod sau card sau amprenta valida.

1. Intrati in modul de programare: *cod master#

2.1. Functie dezactivata (implicit): 6 0 #

2.2. Functie activata: 6 1 # (accesul va fi interzis timp de 10 minute)

2.3. Functie activata (Alarma): 6 2 #

Setare durata alarma: 5 (0~3) #. Implicit 1 minut.

Pentru a opri alarma, introduceti codul master # sau cititi amprenta/cardul master sau introduceti PIN-ul sau cititi amprenta/cardul unui utilizator.

3. Iesiti din modul de programare: *

Avertizare usa deschisa

Daca ati conectat la tastatura de conrol acces un contact magnetic cablat pentru usa si usa ramane

deschisa mai mult de 1 minut, buzzer-ul incorporat va emite un sunet pentru a aminti utilizatorului sa inchida usa. Sunetul poate fi oprit inchizand usa sau introducand un cod de acces valid (master sau utilizator). Altfel, sunetul va continua atat timp cat este setat.

Avertizare usa fortata

Daca ati conectat la tastatura de conrol acces un contact magnetic cablat pentru usa si usa este deschisa cu forta, buzzer-ul incorporat si sirena externa (daca exista) vor suna alarma. Sunetul poate fi oprit inchizand usa sau introducand un cod de acces valid (master sau utilizator). Altfel, sunetul va continua atat timp cat este setat.

1. Intrati in modul de programare: *cod master#

2.1. Functie dezactivata (implicit): 6 3 #

2.2. Functie activata” 6 4 #

Setare durata alarma: 5 (0~3) #. Implicit 1 minut.

3. Iesiti din modul de programare: *

Setare buzzer si LED

1. Intrati in modul de programare: *cod master#

2.1. Dezactivati buzzer-ul: 7 0 #

2.2. Activati buzzer-ul (implicit): 7 1 #

3.1. LED stins: 7 2 #

3.2. LED aprins (implicit): 7 3 #

4.1. Lumina tastatura stinsa: 7 4 #

4.2. Lumina tastatura aprinsa tot timpul: 7 5 #

4.3. Lumina tastatura stinsa in mod automat (implicit): 7 6 #. Dupa 20 de secunde de la ultima operatiune, tastatura se stinge automat. Atingand orice tasta, tastatura se aprinde.

3. Iesiti din modul de programare: *

Adaugare amprenta/card/PIN utilizator cu card/amprenta master

1. Cititi cardul/amprenta master.

2. Cititi amprenta utilizatorului de 3 ori sau cititi cardul sau PIN-ul utilizatorului #

Repetati pasul 2 pentru adaugarea mai multor utilizatori consecutiv.

3. Cititi din nou cardul/amprenta master.

Stergere amprenta/card/PIN utilizator cu card/amprenta master

1. Cititi cardul/amprenta master de doua ori intr-un timp de maxim 5 secunde.

2. Cititi amprenta/cardul sau introduceti PIN-ul utilizatorului #

Repetati pasul 2 pentru stergerea mai multor utilizatori

consecutiv.

3. Cititi din nou cardul/amprenta master.

Resetare si adaugare card master

Daca ati conectat la tastatura de control acces un buton de acces, procedati dupa cum urmeaza pentru a reseta tastatura:

1. Intrerupeti alimentarea.

2. Tineti apasat butonul de acces in timp ce reporniti alimentarea.

3. Se aud 2 beep-uri.

4. Luati degetul de pe butonul de acces.

5. LED-ul galben se aprinde.

6. Cititi orice card EM 125KHz.

7. LED-ul se aprinde rosu.

8. Tastatura a fost resetata.

9. Cardul citit a deventi card master.

Note:

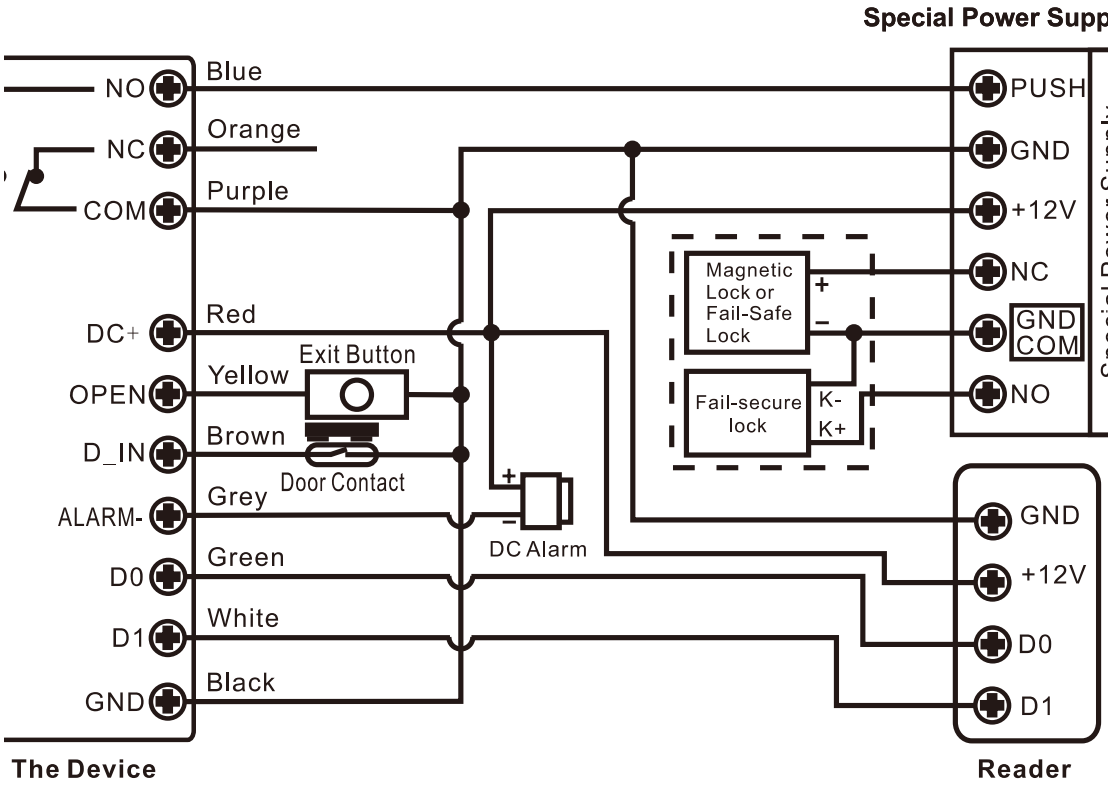
1. Daca nu vreti sa adaugati card master, trebuie sa tineti apasat butonul de acces cel putin 5 secunde inainte de a-l elibera. Aceasta procedura va face invalid fostul card master.

2. Prin resetare, informatiile despre utilizatori nu vor fi sterse.

2. Modul Controller

Tastatura va opera ca un controller daca este conectata la un cititor Wiegand.

Diagrama conexiuni



Atentie: este necesar sa instalati dioda 1N4004 inclusa sau una echivalenta daca folositi o sursa de alimentare la care mai sunt conectate si alte dispozitive.

Setare format intrare Wiegand

1. Intrati in modul de programare: *cod master#

2. Setati biti intrare Wiegand pentru card EM:

8 (26~44) # (implicit 26bits)

3.1. Dezactivare paritate bit: 8 0 #

3.2. Activare paritate bit: 8 1 #

3. Iesiti din modul de programare: *

Programare

Programarea de baza este aceeasi ca la modul standalone.

Conectarea la un cititor de card extern

In cazul unui cititor de card EM sau Mifare, utilizatorii pot fi adaugati/stersi atat pe tastatura cat si pe cititorul extern.

In cazul unui cititor de card HID, utilizatorii pot fi adaugati/stersi doar de pe cititorul extern.

Conectarea la un cititor de amprenta

Conectati cititorul de amprenta la tastatura.

1. Intrati in modul de programare: *cod master#

2.1. Tastati 1 (cititi amprenta pe cititorul de amprenta) #. ID-ul se aloca automat.

2.2. Tastati 1 (ID utilizator) # (cititi amprenta pe cititorul de amprenta) #

3. Iesiti din modul de programare: *

Conectarea la un cititor cu tastatura

Cititorul cu tastatura poate fi de 4 Bits, 8 Bits (ASCII) sau de 10 Bits.

1. Intrati in modul de programare: *cod master#

2.1. Introduceti numarul de biti: 8 (4 sau 8 sau 10) #. Implicit este 4 Bits.

3. Iesiti din modul de programare: *

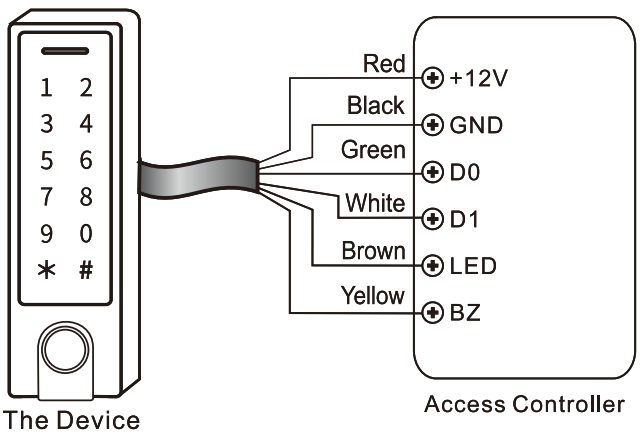
Adaugare/Stergere PIN utilizator

PIN utilizator poate fi adaugat/sters atat pe tastatura de control acces cat si pe cititorul cu tastatura extern.

3. Modul cititor Wiegand

Tastatura poate opera si ca un cititor Wiegand standard conectat la un controller extern.

Diagrama conexiuni



Cand tastatura este pe modul cititor Wiegand, toate setarile facute in modul Controller devin invalide. Firele maro si galben vor fi redefinite dupa cum urmeaza:

Firul maro: control LED verde

Firul galben: control buzzer.

Setare format iesire Wiegand

1. Intrati in modul de programare: *cod master#

2. Setare biti Wiegand pentru card EM: 8 (26~44) #

3.1. Dezactivare paritate biti: 8 0 #

3.2. Activare paritate biti: 8 1 # (implicit)

3. Iesiti din modul de programare: *

Nota: pentru conectarea unui controller Wiegabd, trebuie sa dezactivati paritate biti.

Aplicatii avansate

Acces al tuturor cardurilor

Dupa activarea acestui mod, toate cardurile pot deschide usa. In acelasi timp, cardul este adaugat in sistem.

1. Intrati in modul de programare: *cod master#

2.1. Dezactivare functie: 9 2 # (implicit)

2.2. Activare functie: 9 3 #

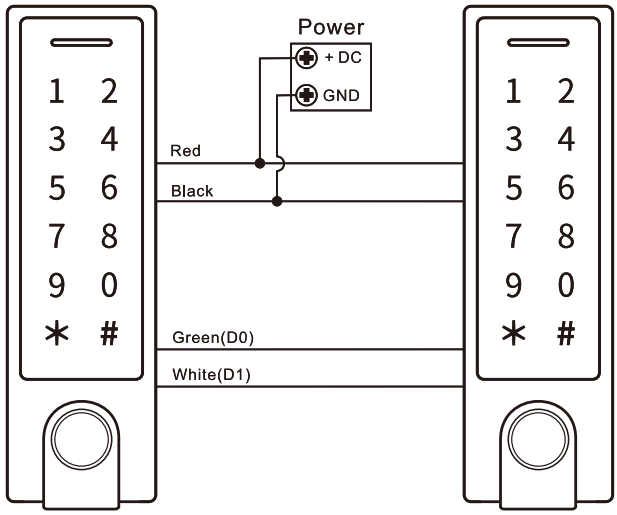
3. Iesiti din modul de programare: *

Transfer informatii utilizator

Pentru utilizatorii inregistrati cu PIN/card.

Informatiile despre utilizatori pot fi transferate de la o tastatura la alta.

Diagrama conexiuni



Ambele tastaturi trebuie sa fie din aceeasi serie.

Codul master al ambelor tastaturi trebuie sa fie identic.

Activati functia de transfer doar pe tastatura principala (tastatura master).

Daca tastatura secundara are deja utilizatori inregistrati, acestia vor si suprascrisi in timpul transferului.

Pentru un numar de 900 utilizatori, transferul ar putea dura pana la 30 secunde.

Activare mod transfer pe tastatura master

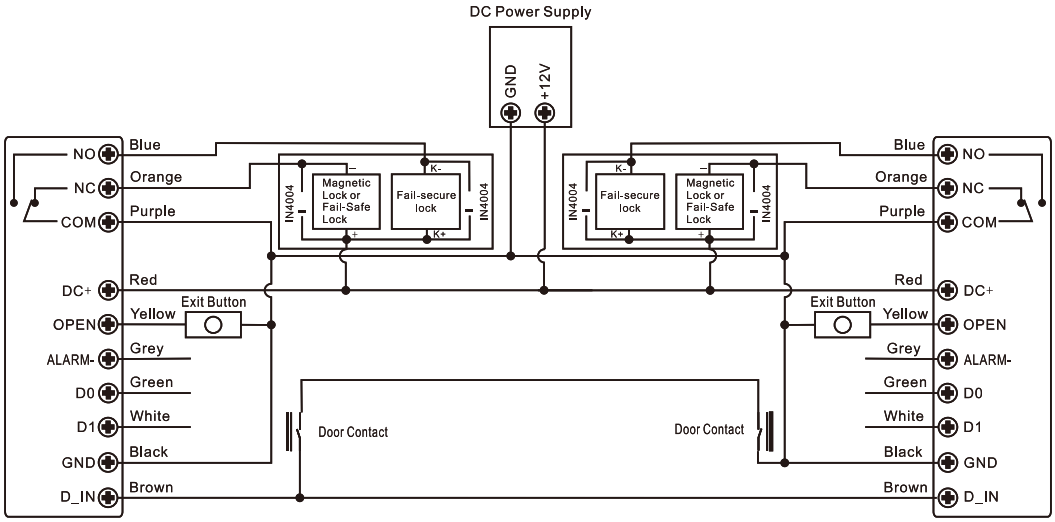
1. Intrati in modul de programare: *cod master#

2. Tastati 9 8 #

Timp de 30 de secunde, durata maxima a transferului, LED-ul verde este arprins. Cand s-a terminat transferul datelor, se aude un beep si se aprinde LED-ul rosu.

3. Iesiti din modul de programare: *

Interconectare tastaturi



Acest mod inseamna interconectarea a doua tastaturi pentru controlul a doua usi. Functia este utila in special in inchisori, banci si alte locatii unde se cere un nivel de securitate mai ridicat.

Diagrama conexiuni

Inregistrati utilizatorii pe tastatura A, apoi transferati-i pe tastatura B.

Activati modul Interconectare pe ambele tastaturi:

1. Intrati in modul de programare: *cod master#

2.1. Dezactivare functie: 9 0 # (implicit)

2.2. Activare functie: 9 1 #

3. Iesiti din modul de programare: *

Cand functia este activa, cand usa 2 trebuie sa ramana inchisa, utilizatorul poate citi amprenta/cardul sau poate introduce PIN-ul pe tastatura A. Usa 1 se va deschide. Cand usa 1 trebuie sa ramana inchisa,

utilizatorul poate citi amprenta/cardul sau poate introduce PIN-ul pe tastatura B. Usa 2 se va deschide.

Cand functia este activa, utilizatorul poate citi amprenta/cardul sau poate introduce PIN-ul pe tastatura A pentru a deschide usa 1. Sau poate citi amprenta/cardul sau poate introduce PIN-ul pe tastatura B pentru a deschide usa 2.

Control tastatura din aplicatia Tuya Smart

Nota: Din cauza actualizarilor frecvente ale aplicatiei Tuya Smart, este posibil ca imaginile si informatiile prezentate in acest manual sa difere de cele din versiunea instalata pe dispozitivul dumneavoastra.

Accesati Google Play sau App Store sau scanati codul QR de mai jos si instalati aplicatia Tuya Smart.

Conectati telefonul la reteaua WiFi, activati Locatia si functia Bluetooth.

Deschideti aplicatia si autentificati-va.

Apasati “+“ - “Add device“.

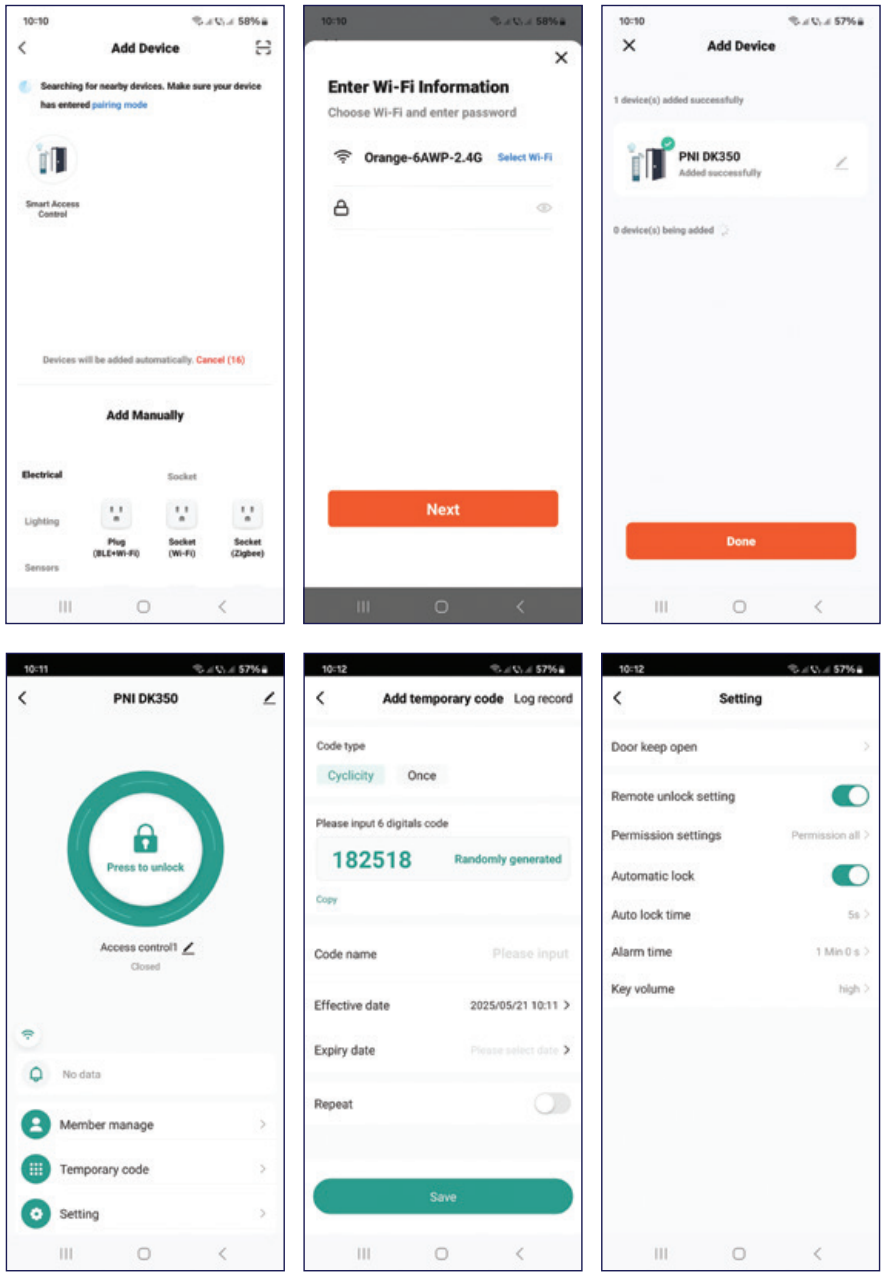
Aplicatia va identifica automat dispozitivul dumneavoastra.

Apasati pe pictograma tastaturii si urmati pasii de pe ecran.

Nota: puteti adauga si manual tastatura in aplicatie, accesand categoria Camera & Lock - Lock (Wi-Fi).

Resetare WiFi

Tastati: * cod master # 9 cod master #



Aplicatia permite deblocarea usii, adaugarea si gestionarea utilizatorilor si generarea unui cod temporar de acces.