

Installation & User Guide

Standalone Metal RFID Series

Version: 2.2

Date: May, 2015





Important Statement

Copyright Statement

Thank you for choosing our product. Before use, please read our Installation and User Guide (the guide) carefully to ensure high effectiveness and authentication speed under proper use, avoiding unwanted damages caused.

It is informed that without our company's written consent, no copy or any other forms of distribution of the guide's content may be allowed.

Disclaimer

Our company does not guarantee that the information and technical parameters of the guide are exactly consistent with the actual product, nor make prior notice on any updates of the product. The rights of final amendment and interpretation are reserved for our company.



Contents

Installation Guide

1. Equipment Installation.....	I
2. Structure and Function.....	II
3. Lock Connection.....	III
4. Connect with Other Devices	IV
5. Connect with Power.....	IV

User Guide

1. User Management.....	1
1.1 Administrator Operation	1
1.2 Adding Users.....	2
1.3 Register Access Passwords	3
1.4 User Authentication	4
1.5 User Deletion	4
2. Access Control Management	5
2.1 Unlocking Duration Configuration.....	5
2.2 Authentication Mode Configuration.....	6
2.3 Concealed Mode Configuration	6
2.4 Door Sensor Mode Configuration.....	7
2.5 Alarm Configuration.....	7
2.6 SRB	9
2.7 Factory Default Restoration.....	9
3. Switching Working Mode.....	9
3.1 Switching to Reader Mode	10
3.2 Switching to Controller Mode	10
Appendix.....	11
Packing List	11

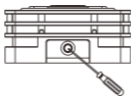


1. Equipment Installation



Optical Tamper Switch

①



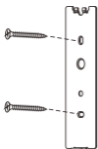
Remove the screw on the bottom of device.

②



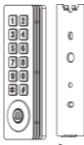
Take away the back cover.

③



Fix the back cover on the wall.

④



Fix the device to the back cover.

⑤



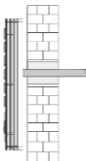
Fix the screw.

⑥



Exposed wiring

⑥



Buried wire

Please remove the plastic when installing exposed wire

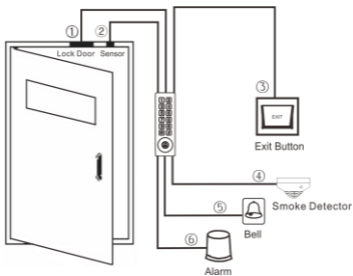




2. Structure and Function

Access Control System Function

- (1) When a registered user's identity is verified, the Access Control device will send out signal to unlock the door.
- (2) The door sensor will detect the status of the lock. If the door is unexpectedly opened or improperly closed, the alarm will be triggered.
- (3) It supports the exit button for opening the door from inside.
- (4) It supports smoke detector and infrared sensor etc.. If the Access Control device receives signal from detector, the alarm will be triggered, and the door is set as normally open.
- (5) It supports door bell.
- (6) If the Access Control device is dismantled, the alarm will be triggered.



④ Linkage Function

This device has an Auxiliary Input interface (AUX+) which allows it to be connected with an external source, for instance, a smoke detector, gas detector, infrared sensor or emergency switch.

Trigger Linkage

When the device receives a signal from detectors or sensors connected to AUX+, the alarm will be triggered, switching the door to normally open state.

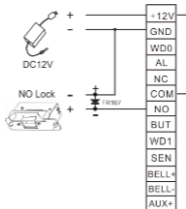
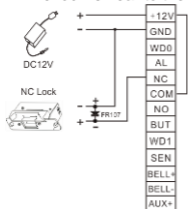
Cancel Linkage

Alarm and normally open state will be canceled after user verification or administrator entering password. The Access Control device will resume to ready mode.

3. Lock Connection

Warning: No operation when power on!

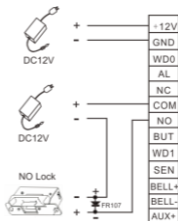
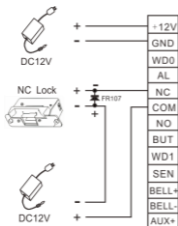
- (1) The system supports NO LOCK and NC LOCK. The NO LOCK (normally open by power on) is connected with **NO** terminal, and the NC LOCK is connected with **NC** terminal.
 - (2) To prevent the generation of self-inductance EMF which would affect the system, when the electrical lock is linked to the Access Control System, it is required to connect one FR107 diode (equipped in the package, do not reverse the polarities) in parallel in order to release the self-inductance EMF.
- (I) Under following two situations, device shares power with the lock:
- ① $U_{LOCK}=12V$, $I \geq I_{Device} + I_{Lock}$ (The maximum operating current of device is 100mA, and the rated current is 60mA);
 - ② The lock is near to the device.



(II) Under following situations, device does NOT share power with the lock:

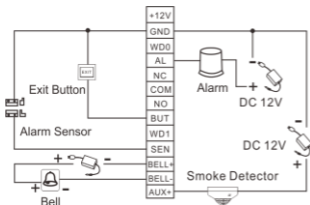
Device does not share power with the lock:

- ① When $U_{\text{Lock}}=12\text{V}$, $I < I_{\text{Device}} + I_{\text{Lock}}$ (The maximum operating current of device is 100mA, and the rated current is 60mA);
- ② When $U_{\text{Lock}} \neq 12\text{V}$;
- ③ When the lock is far from the device.



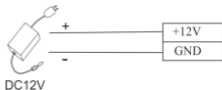
I: device's current output; U_{Lock} : lock voltage; I_{Lock} : lock current.

4. Connect with Other Devices



Only devices with an alarm \leq DC 12V can be connected

5. Connect with Power



Input DC12V, $\leq 110\text{mA}$ ($\leq 80\text{mA}$ standby) Positive is connected with **+12V**, negative is connected with **GND** (do not reverse the polarities).

Recommended procedure

Step 1: Power on after the device is completely installed on the wall.

Step 2: Authenticate administrator password and change it immediately. Adjust access control parameters, which include changing passwords for door opening, and setting unlocking duration, authentication mode, concealed mode, door sensor mode and alarm etc.

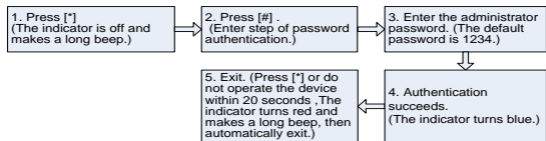
Step 3: You may register and authenticate user accounts, cards or passwords.

1. User Management

1.1 Administrator Operation

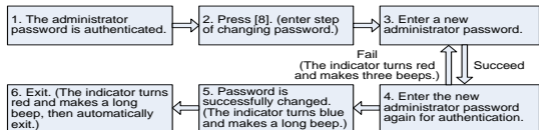
To ensure data security of the device, users can operate the device only after the administrator password is authenticated.

❖ Authenticate Administrator Password



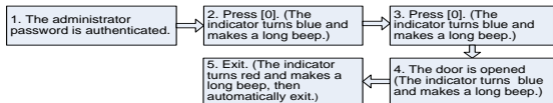
☺Note: The default administrator password is 1234.

❖ Change Administrator Password



☺Note: Four-digit passwords are automatically verified. For passwords with less than four digits, press [#] to enter the verification process.

❖ Open Door by Entering Administrator Password



😊Note: This function can be used to open the door.

❖ Forgot Administrator Password

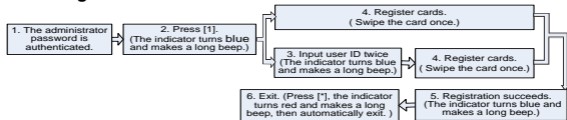
If administrator password is lost, you may reset the password to default through tamper switch. Dismantle the device and wait for 30 seconds until the blue light is on and a long beep is heard. Press the optical tamper switch for 2 to 5 seconds and repeat this step for 3 times. The administrator password is successfully reset to default when the blue light is on and a long beep is heard. The red light is then on and the operation is quit automatically.

😊Note: The default administrator password is 1234.

1.2 Adding Users

Register the card of a user or register cards in batches.

❖ Adding Users

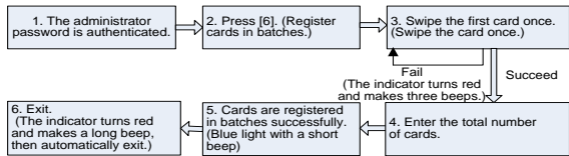


😊Note:

1. Nine-digit user ID is automatically verified. For user ID with less than nine digits, press [#] to confirm.
2. If the user ID is not available, the ID number increases automatically. It continues to register new one once a user is successfully registered.
3. The registration fails if the user ID or the card has been registered (the indicator turns

red and makes three short beeps). When the indicator turns blue, you can register the user again. If you fail to swipe card or enter user ID for three times, the device will enter the standby state.

❖ Registering Cards in Batches

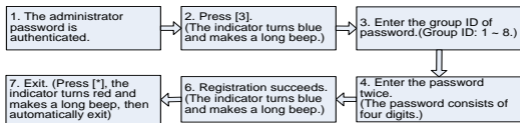


☺Note:

1. In the process of entering the total number of cards, three-digit numbers are automatically verified. For numbers with less than three digits, press [#] to enter the verification process. Press [*] to enter the total number of cards again.
2. IDs of the to-be-registered cards must be consecutive numbers.

1.3 Register Access Passwords

This device supports 8 passwords, each password has a Group ID ranged from 1~8. The default password value is 0 for all groups, which means those passwords are disabled. You can modify the passwords under 8 groups to open the door.

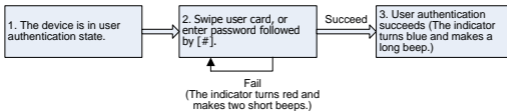


☺Note: When a password is successfully changed, you can immediately change the next password by entering another group ID.

1.4 User Authentication

Card / Password Authentication

When the device is power-on, it enters user authentication state.

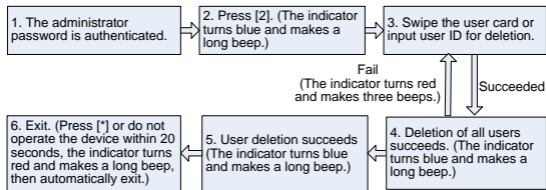


☺Note: Press [#] after entering a password for authentication. The door opens if the entered password is identical with one of the eight passwords for opening the door.

1.5 User Deletion

Delete one, multiple or all registered user(s).

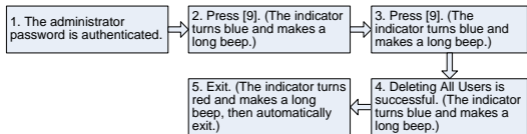
❖ Deleting One User



☺Note:

1. You can either swipe the card or input user ID to delete a user. Nine-digit user ID will be automatically verified. For user ID with less than nine digits, press [#] to confirm.
2. After successful deletion, the device will automatically enter the process of deleting next user. Press [*] to exit.

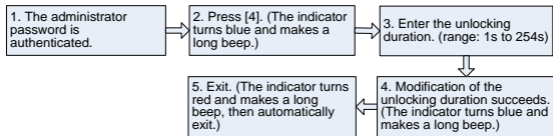
❖ Deleting All Users



☺Note: In step 3, press [9] for automatic confirmation. Other numbers are considered invalid. If an invalid number is entered, the device indicator turns red, and the device makes a long beep and exits the process.

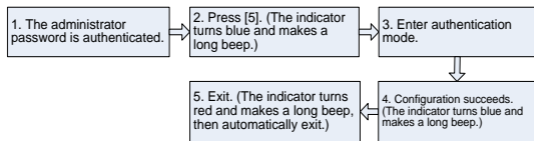
2. Access Control Management

2.1 Unlocking Duration Configuration



☺Note: The unit of unlocking duration is “second”. Three-digit values will be automatically verified. For values with less than three digits, press [#] to enter verification process.

2.2 Authentication Mode Configuration



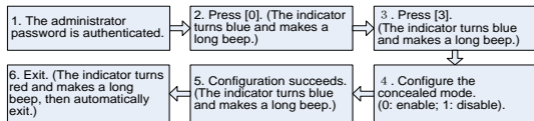
☺Note:

- When the authentication mode is **RF card & password**, user must swipe card first and then enter the password.
- Details about the authentication modes are as follows:

Authentication Mode	Value	Description
PW	1	Only password verification
RF	2	Only RF Card verification
RF/PW (default)	3	RF Card or password verification
RF&PW	4	RF Card and password verification

2.3 Concealed Mode Configuration

Under standby mode, when the Concealed Mode is on, the indicator will be turned off.

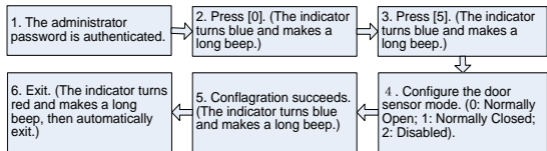


☺Note: When user is authenticating the card or password under Concealed Mode, the indicator will still blink correspondingly to denote process status.

2.4 Door Sensor Mode Configuration

The door sensor has three modes:

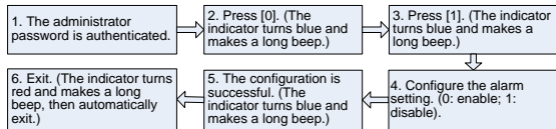
- **NONE**: The door sensor is disabled.
- **Normal Open (NO)**: The door sensor will send an alarm signal if it detects the door is closed.
- **Normal Closed (NC)**: The door sensor will send an alarm signal if it detects the door is open.



2.5 Alarm Configuration

❖ Configuring Alarm Switch

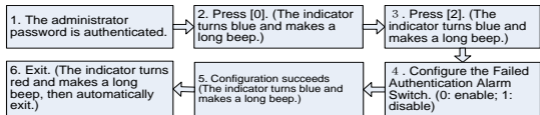
Only if the alarm switch is set to be ON will the Failed Authentication Alarm and Door Sensor Alarm be effective. The default status of the alarm switch is ON.



Note: The Temper Alarm is still effective even if the alarm switch is OFF.

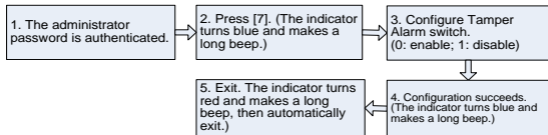
❖ Configuring Failed Authentication Alarm

If the administrator fails in authentication in 3 attempts, Failed Authentication Alarm will be triggered. No authentication can be made within 20 seconds.



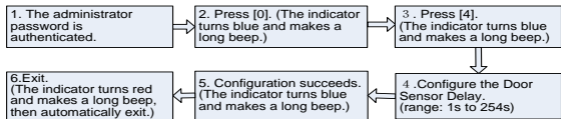
❖ Configuring Tamper Alarm

If this function is enabled, alarms will be raised when the device is dismantled from the wall.



❖ Configuring Door Sensor Delay

When the door is not closed well after a time period, the Door Sensor Delay will raise an alarm to alert users. Its configured value is the time period denoting how long after the door is opened will the alarm ring.



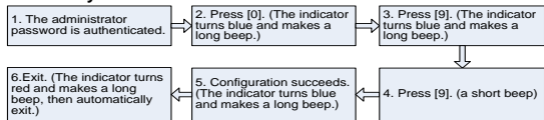
☺Note: Three-digit values will be automatically verified. For values with less than three digits, press [#] to confirm. Values greater than 254 are considered invalid.

2.6 SRB

Security Relay Box (SRB) is a relay switch controlling electric lock. When it receives the Wiegand signal sent from the Access Control device, it will send a (unlock/lock) signal to trigger the relay switch to operate, so as to provide a higher security level for access control.

☺Note: For the detailed parameters and wiring guide of SRB, please consult the SRB Access Controller Wiring Guide.

2.7 Factory Default Restoration



The Factory Default Settings

Unlock Authentication Mode	RF/PW
Door Sensor Mode	None
Alarm Switch	Enabled
Failed Authentication Alarm Switch	Enabled
Tamper Alarm Switch	Enabled
Concealed Mode	Disabled
Unlocking Duration	5 seconds
Door Sensor Delay	15 seconds

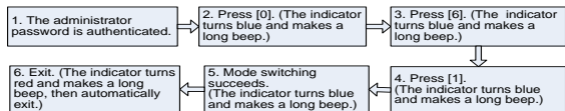
3. Switching Working Mode

This device can work as either a standalone controller or a wiegand reader, which offering high flexibility to use depending on actual needs. It is a standalone controller in default setting, but user can switch the working mode by the following instruction.

If the indicator stays in red, this indicates that the device is set to Reader Mode. If the indicator blinks in blue, this indicates that the device is set to Controller Mode.

☺Note: For wiring diagram of reader mode, please consult [Appendix](#).

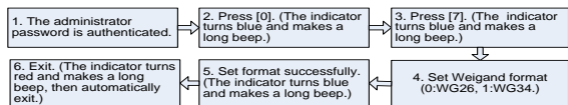
3.1 Switching to Reader Mode



☺Note: When mode switching fails, the device will give 3 short beeps, followed by the indicator turning to red with a long beep, and then automatically exits.

Setting Weigand Format

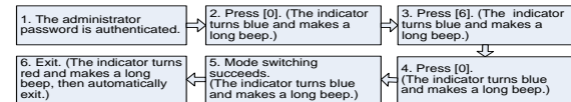
When the device is in Reader Mode, press and hold [*] for five seconds. Press [#] when the red indicator is off, and then input administrator password. The Wiegand format can be set to Wiegand 26 or Wiegand 34.



☺Note: When mode switching fails, the device will give 3 short beeps, followed by the indicator turning to red with a long beep, and then automatically exits.

3.2 Switching to Controller Mode

When the device is in Reader Mode, press and hold [*] for five seconds. Press [#] when the red indicator is off, and then input administrator password.



☺Note: When mode switching fails, the device will give 3 short beeps, followed by the indicator turning to red with a long beep, and then automatically exits.

Appendix

Wiring Diagram of Controller Mode

Red: DC 12V	Light Blue: SEN
Black: GND	Gray: BUT
Yellow: NC	Purple: BELL+ (Bell)
Pink: COM	Brown: BELL- (Bell)
Blue: NO	

Weigand Output Linkage Function

Green: WD0	Orange: AL (Alarm)
White: WD1	Light Green: AUX+

Wiring Diagram of Reader Mode

Red: DC 12V	Black: GND
Green: WD0	White: WD1
Gray: BEEP	Light Blue: LED
Purple: BELL+ (Bell)	
Brown: BELL- (Bell)	

Packing List



Access Control
Device & Mounting



Card



4 Diodes (FR107)



Screwdriver



4 Screws



4 Wall Plugs



Star-shaped Screw



Installation Guide