

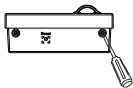
User Manual

X8s Access Control System

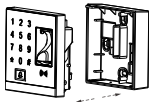
Version: 1.0



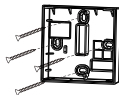
1. Equipment Installation



- (1) Remove the screw from the bottom of the device.



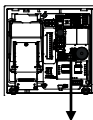
- (2) Remove the back cover of the device.



- (3) Fix the back cover on the wall.
(Drill the wiring hole and fixing holes according to the back cover)

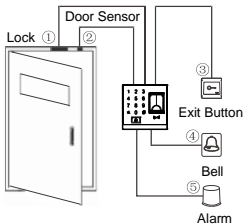


- (4) Fix the device on the back cover using screws.



Tamper Alarm Button

2. Structure and Function



Access Control System Function:

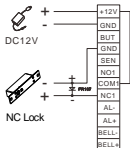
- (1) When a registered user's identity is verified, the Access Control device will send out signal to unlock the door.
- (2) The door sensor will detect the status of the lock. If the door is unexpectedly opened or improperly closed, an alarm will be triggered.
- (3) It supports the exit button for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

3. Lock Connection

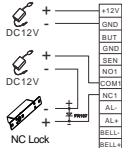
⚠ Warning: No operation when power on!

- (1) The system supports NO LOCK and NC LOCK. The NO LOCK (normally open at 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.

- (1) Device shares power with the lock
The device shares power with the lock, when $U_{LOCK}=12V$ and $I_{LOCK} > 1A \dots$ ① and the lock is near to the device.

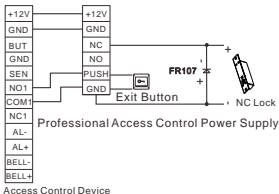


- (2) Does not share power with the lock
The device does not share power with the lock:
A. When $U_{LOCK}=12V$ $I_{LOCK} \leq 1A$;
B. When $U_{LOCK} \neq 12V$;
C. When the lock is far apart from the device.

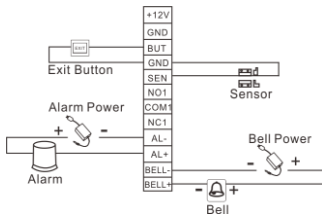


① I: device' current output, U_{LOCK} : lock voltage, I_{LOCK} : lock current.

- (3) Professional Access Control Power Supply Connection

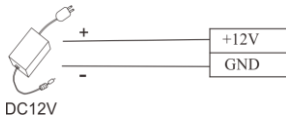


4. Connection with Other Devices



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

5. Connection with Power



Input 12V DC, 500mA (50mA in idle status). Positive is connected with **+12V**, negative is connected with **GND** (do not reverse the polarities).

Instructions

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 including password change for door opening, setting unlocking duration, authentication mode, concealed mode, door sensor mode, etc.

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

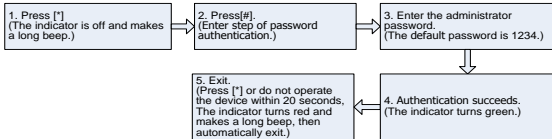
Operation Instructions

1. User Management

1.1 Administrator Operation

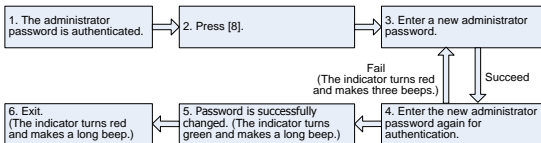
To ensure data security of the device, users can operate the device only after the administrator password is authenticated.

❖ Administrator Authentication



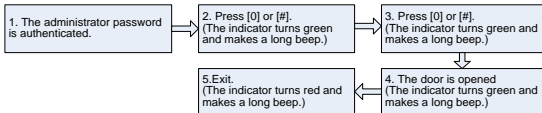
☺Note: The default administrator password is 1234. You are advised to change the initial password at the beginning.

❖ Changing Administrator Password



☺Note: Four-digit passwords are automatically verified. If the password length is less than four digits, then press [#] to confirm the password.

❖ Opening Door by Entering Administrator Password



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

❖ Forgot Administrator Password

If the administrator password is lost, you can reset the password to default by using tamper switch.

Operation:

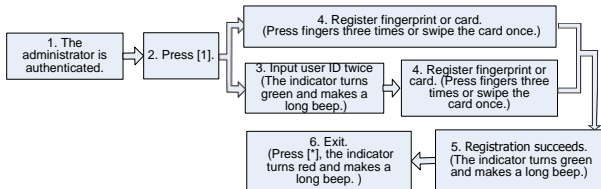
1. Dismantle the device and wait for 30 seconds until a short beep is heard.
2. Press the Tamper Switch thrice to reset to the initial administrator password.

☺Note: This operation must be done within 30 seconds; the default administrator password is 1234.

1.2 Adding Users

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

❖ Adding a User



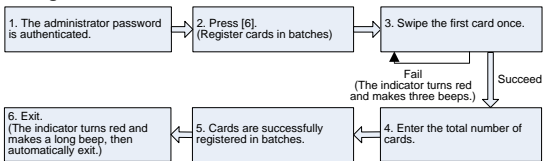
☺Note:

1. First-digit user ID is automatically verified, if the user ID is less than five digits, press [#] to confirm the user ID.
2. If the user ID is not available, the device automatically increases the ID number and

continues to register a new user once the user is successfully registered.

3. If the user ID, fingerprint or the card has been registered already, the indicator turns red and generates three short beeps indicating that the registration fails. You can start registering the user again when the indicator turns green. Note: If you fail to register the card, then press fingerprint or enter user ID thrice to set the device in idle state.

❖ Registering Cards in Batches

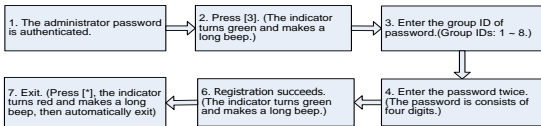


☺Note:

1. While registering the card number, three-digit card numbers are automatically verified. For card number less than or greater than three digits, press [#] to confirm and then press [*] to register the card number.
2. You must clear all the registered users before registering the cards in batches. IDs of the to-be-registered cards must be in consecutive numbers.

1.3 Registering 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.



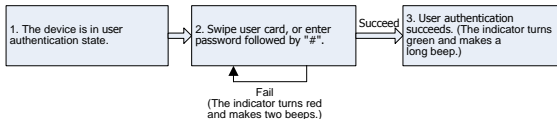
☺Note:

1. When a password is changed to 0, 00, 000, or 0000, the password is disabled.
2. When a password is successfully changed, you can immediately change the next password by entering another group ID.

1.4 User Authentication

Card / Fingerprint / Password Authentication

When the device is powered ON, it enters user authentication state.

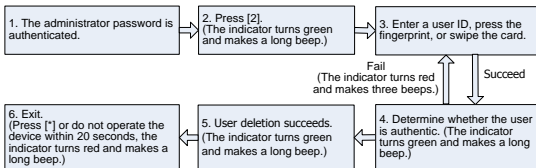


☺Note: Press [#] after entering the password for authentication. The door opens only if the entered password matches with one of the 8 passwords. The initial eight passwords for opening the door is set to 0.

1.5 User Deletion

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

❖ Deleting One User



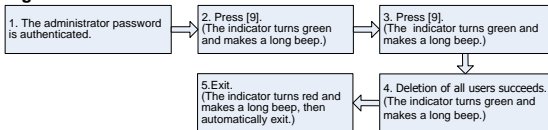
☺Note:

1. You can either swipe the card, press fingerprint or input user ID to delete a user.

Five-digit user ID will be automatically verified. If user ID is less than five digits, press [#] to confirm.

- After successful deletion, the device will automatically enter the process of deleting next user. Press [*] to exit.

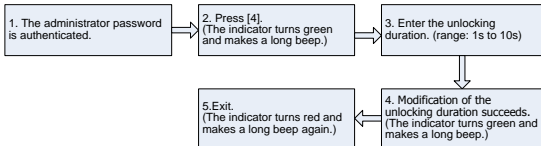
❖ Deleting All Users



☺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 makes three short beeps, then makes a long beep and exits the process.

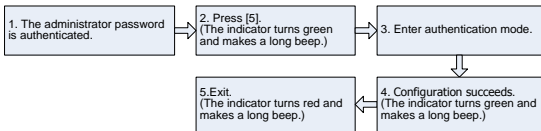
2. Access Control Management

2.1 Unlocking Duration Configuration



☺Note: Press [10] for automatic confirmation. For values with less than 10, press [#] to confirm. Values greater than 10 will be considered invalid.

2.2 Authentication Mode Configuration

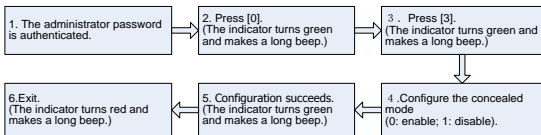


☺Note: Details of authentication modes are as follows:

Authentication Mode	Value	Description
PW	1	Only password verification
RF	2	Only RF Card verification
FP	3	Only fingerprint verification
FP/PW/RF	4	fingerprint or password or RF Card verification
RF&PW	5	RF Card and password verification (swipe card before entering password)
FP&PW	6	fingerprint and password verification (fingerprinting before entering password)

2.3 Concealed Mode Configuration

In standby mode, when the Concealed Mode is ON, the indicator will be turned OFF.

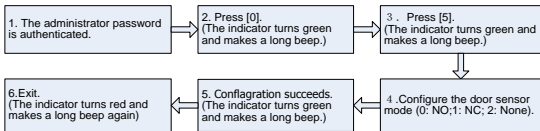


☺Note: When user is authenticating the card or fingerprints or password in Concealed Mode, the indicator will still blink correspondingly to denote process status.

2.4 Door Sensor Mode Configuration

The door sensor has three modes:

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

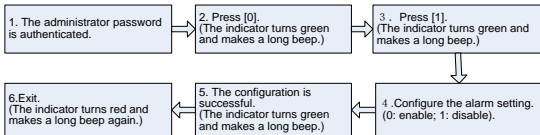


2.5 Alarm Configuration

©Note: If an alarm is triggered, it will be terminated only after the user is authenticated.

❖ Configuring Alarm Switch

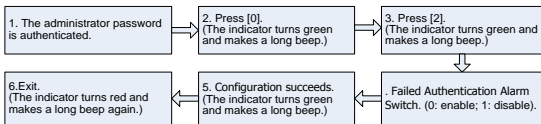
Failed Authentication Alarm and Door Sensor Alarm will be effective only if the alarm switch is set to ON status. Note: The default status of the alarm switch is ON.



©Note: The Tamper Alarm will be effective even if the alarm switch is set to OFF.

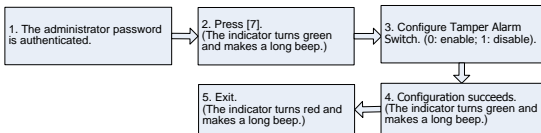
❖ Configuring Failed Authentication Alarm

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



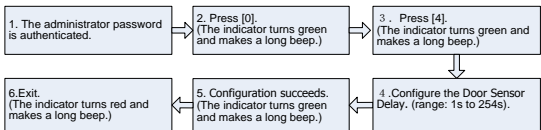
❖ Configuring Tamper Alarm

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 the set time period, the Door Sensor Alarm will generate an alarm signal to alert the users.



☺Note:

1. 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. When an alarm is triggered, the device interior alarm will be triggered first. After 30 seconds, the device exterior alarm will be triggered.