

ZKTECO
X8-BT Bluetooth
ID Card Reader
Access Control
Terminal



ZKTECO X8-BT Bluetooth ID Card Reader Access Control Terminal User Manual

[Home](#) » [ZKTECO](#) » ZKTECO X8-BT Bluetooth ID Card Reader Access Control Terminal User Manual 

Contents

- [1 ZKTECO X8-BT Bluetooth ID Card Reader Access Control Terminal](#)
- [2 Device Installation](#)
- [3 Structure and Function](#)
- [4 Connection with Power](#)
- [5 Instructions](#)
- [6 Administrator Operation](#)
- [7 Registering Access Passwords](#)
- [8 User Deletion](#)
- [9 Technical Specifications](#)
- [10 Documents / Resources](#)
 - [10.1 References](#)

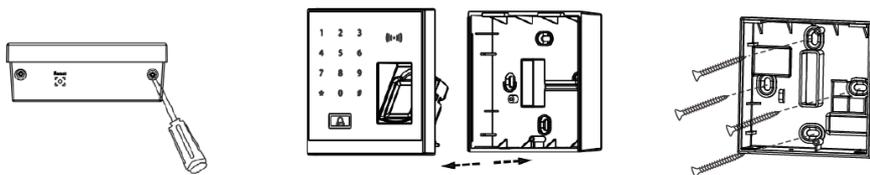


ZKTECO X8-BT Bluetooth ID Card Reader Access Control Terminal



Device Installation

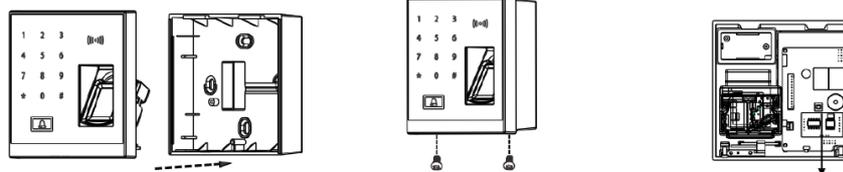
Method 1: Install on the wall



1) Remove the screws 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)

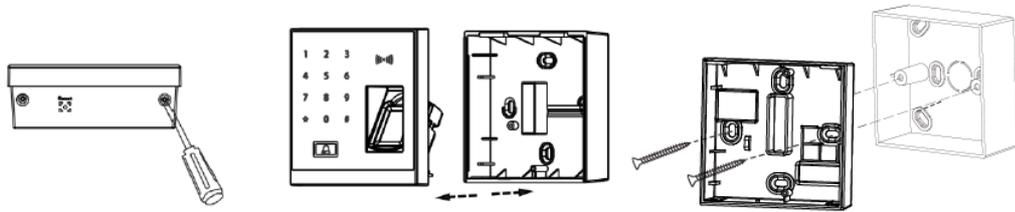


4) Install the device on the fixed back cover.

5) Fix the device on the back cover using screws.

Tamper Alarm Button

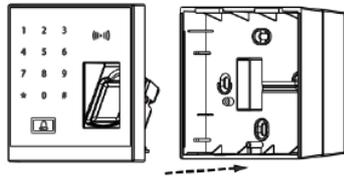
Method 2: Install on the 86 Box



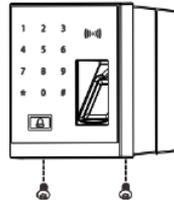
1) Remove the screws from the bottom of the device.

2) Remove the back cover of the device.

3) Fix the back cover to 86 box on the wall.

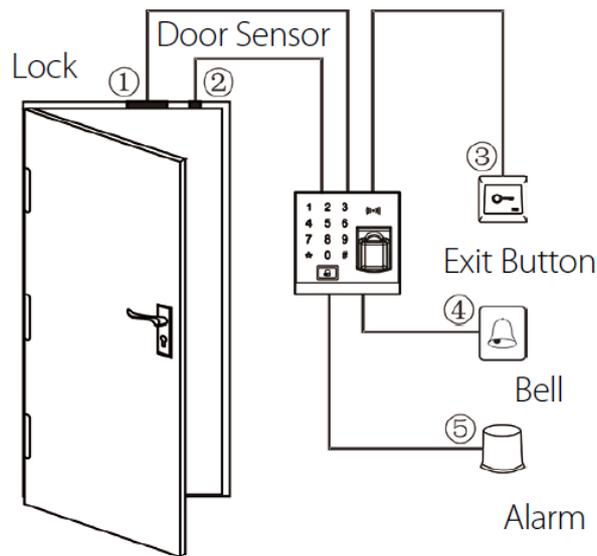


4) Install the device on the back cover. The back cover is fixed on the 86 box.



5) Fix the device on the back cover using screws.

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.

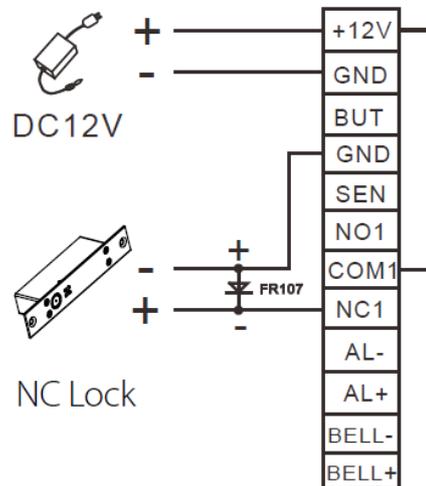
Lock Connection

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

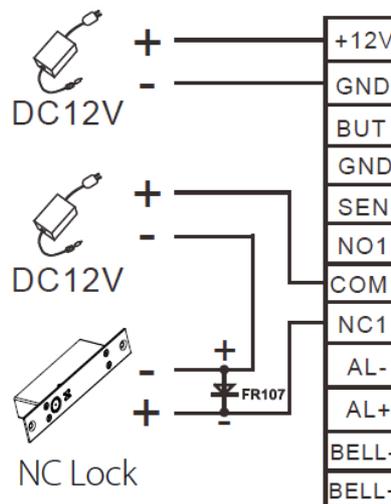
The device shares power with the lock, when $U_{LOCK}=12V$ and $I-I_{LOCK} > 1A$...① and the lock is near to the device.



2. Does not share power with the lock

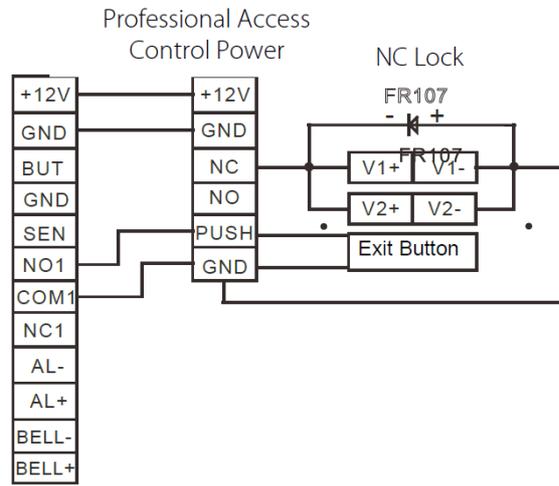
The device does not share power with the lock:

- A. When $U_{LOCK} = 12V$ and $I-I_{LOCK} \leq 1A$;
- B. When $U_{LOCK} \neq 12V$;
- C. When the lock is far apart from the device.



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

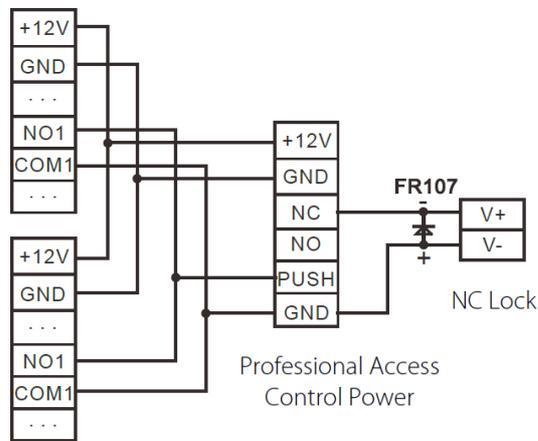
3. One device controls two locks



Access Control Device

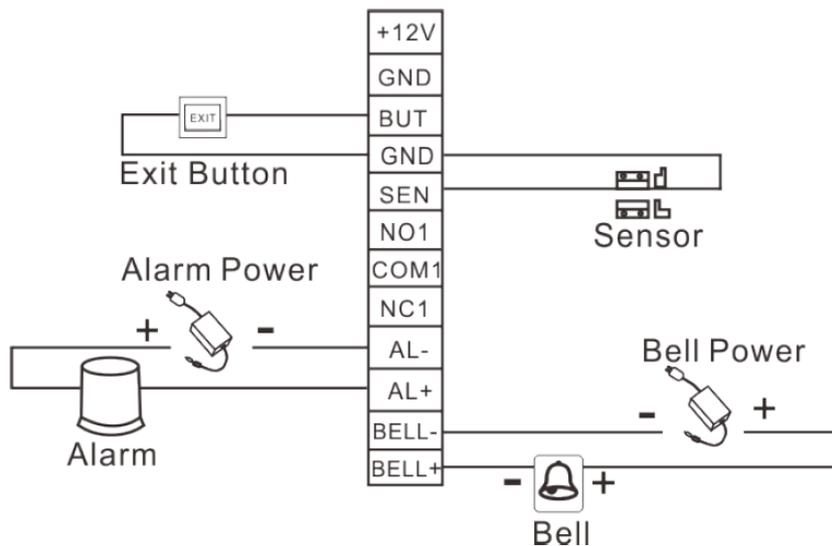
4. Two devices control one lock

Access Control Device 1



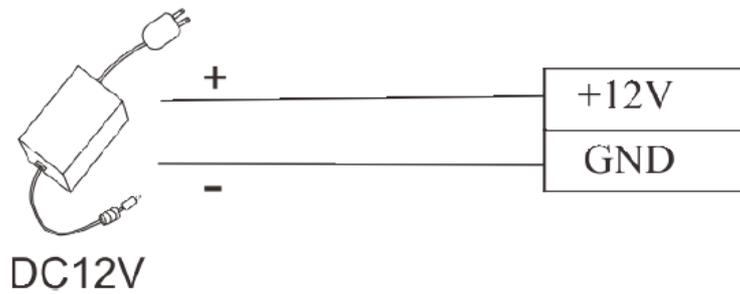
Access Control Device 2

Connection with Other Devices



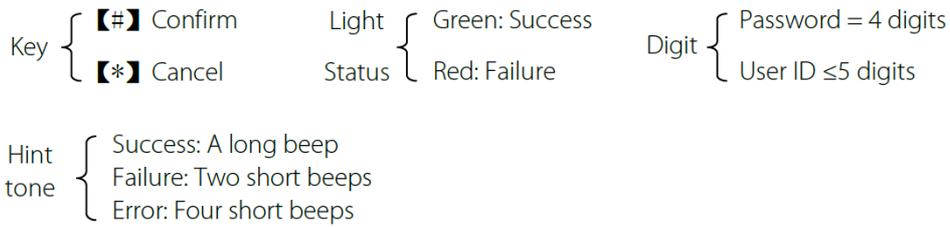
Only devices with an alarm consuming $\leq 12V$ DC can be connected.

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).

Conventions



Note: After entering password/user ID, user must press 【#】 to confirm; press 【*】 to return to initial state.

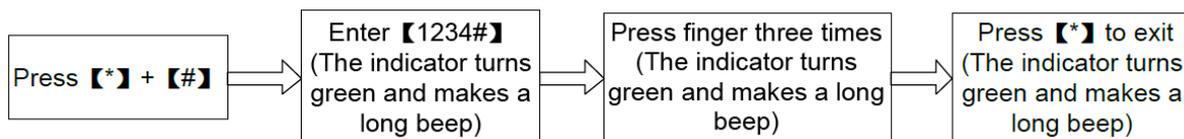
Instructions

- **Step 1:** Power ON after the device is completely installed.
- **Step 2:** Verify administrator using default password and register fingerprint immediately. Adjust access control parameters including 8 passwords, authentication mode, door sensor mode, alarm etc.
- **Step 3:** You can register user, enroll card, fingerprint or 8 passwords.

Administrator Operation

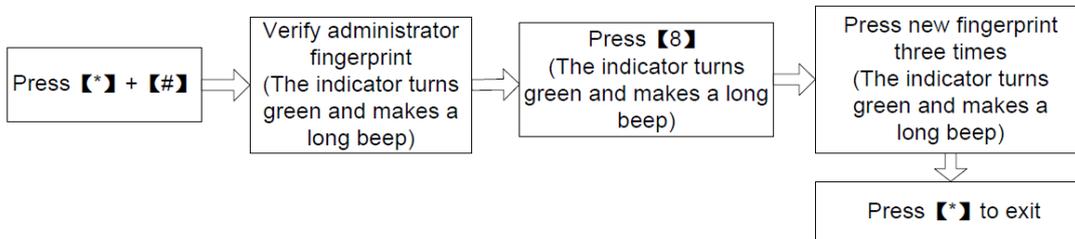
To ensure data security of the device, users can operate the device only after the administrator password is authenticated.

Register Administrator Fingerprint



Note: The default administrator password is 1234. You are advised to change the initial password at the beginning. After administrator fingerprint (only can register one fingerprint) registered successfully, the initial password will become invalid.

Changing Administrator Fingerprint



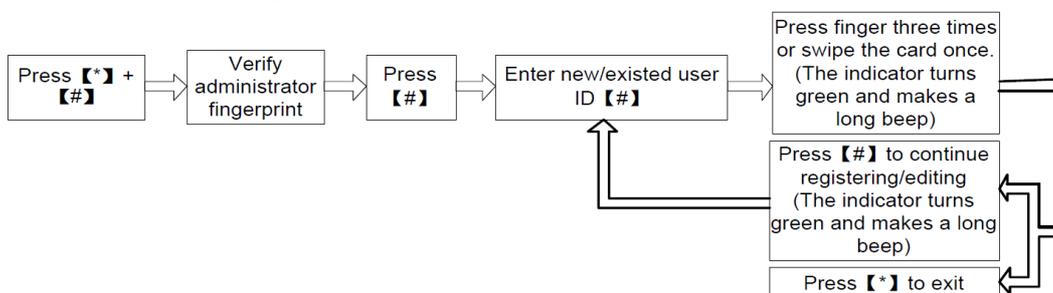
Lost Administrator Fingerprint

If the administrator fingerprint is lost, please dismantle the device and wait 30 seconds when there is a short beep, then press the Tamper Switch three times to reset to the initial administrator password, note this operation must be done within 30 seconds. It makes a long beep after resetting successfully.

Note: The initial administrator password is 1234.

Adding/Editing Users

Each user can register up to 10 fingerprints and 1 card.

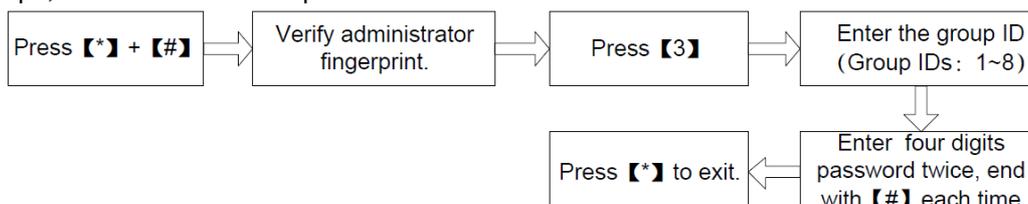


Note:

1. Enter user ID to add new user. If the user ID already exists, the device defaults to edit the user.
2. After registering a fingerprint successfully, the indicator turns green and makes a long beep; you can continue to register other fingerprints, 10 at most.
3. If the fingerprint or the card has been registered already or an error occurred while registering, the indicator turns red and generates four short beeps indicating that the registration fails. You can start registering the user again when the indicator turns green.

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.

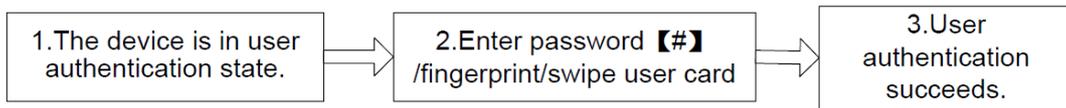


Note: When a password is changed to 0000, the password is disabled. When a password is successfully changed, you can immediately change the next password by entering another group ID.

User Authentication

Fingerprint/ Card /Password Authentication

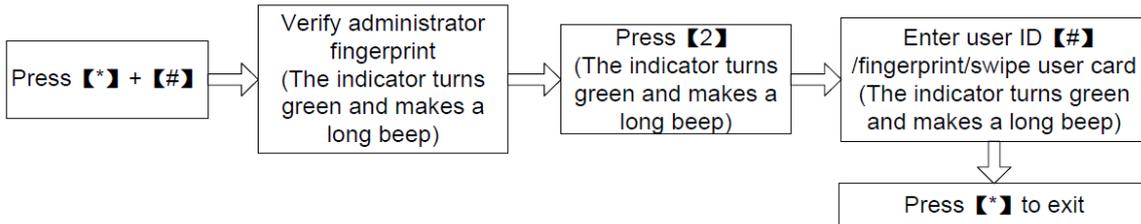
When the device is powered ON, it enters user authentication state (flash blue light).



Note: The door opens only if the entered password matches with one of the 8 passwords. The initial eight passwords for opening the door are set to 0.

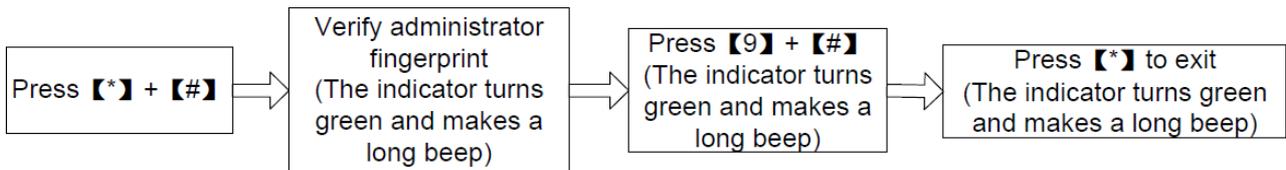
User Deletion

Deleting One User

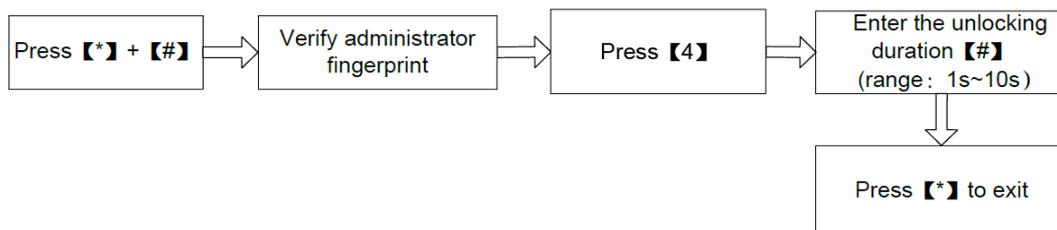


Note: After successful deletion, the device will automatically enter the process of deleting next user. Press [*] to exit.

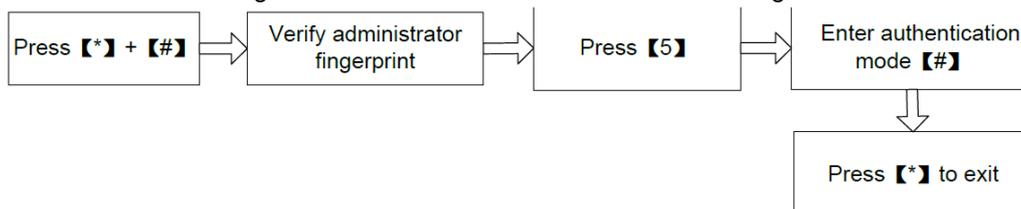
Deleting All Users



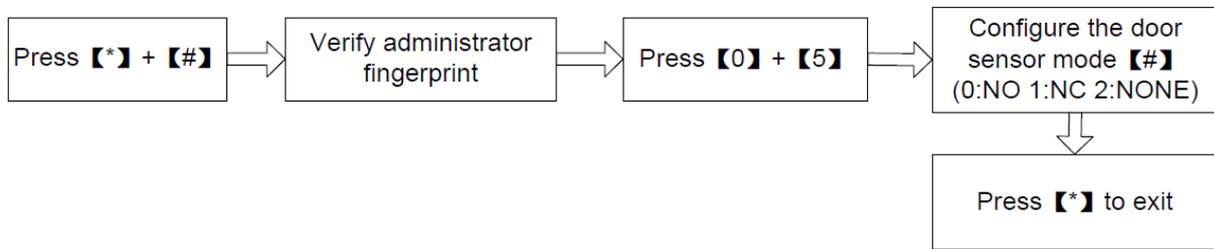
Unlocking Duration Configuration (default duration: 6s)



Note: Values greater than 10 will be considered invalid. The indicator turns red and makes four short beeps. It is recommended to use default settings in access control. User can set according to actual needs.



Authentication Mode Configuration (default mode: FP/PW/RF)



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)

Door Sensor Mode Configuration (default mode: None)

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.

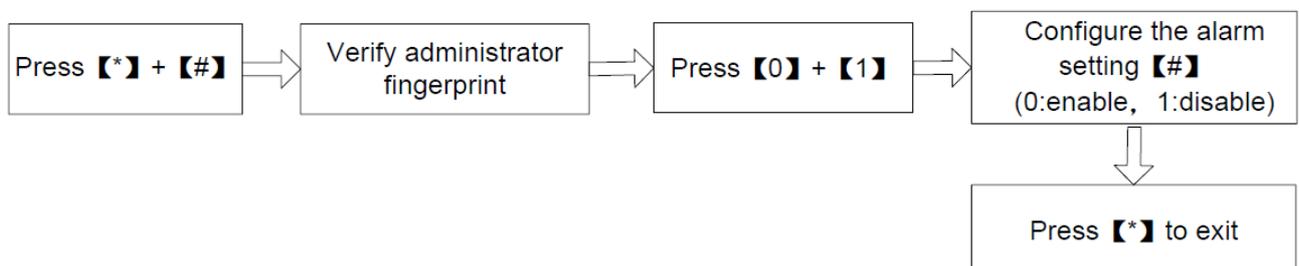
Alarm Configuration

Note: If an alarm is triggered, when the door status is normal, it will be terminated after the user is authenticated; when the door is in abnormal state, it will be terminated only after the administrator is authenticated.

- **Configuring Alarm Switch**

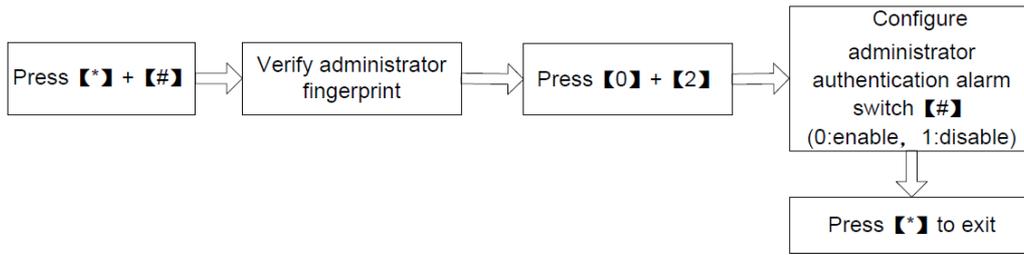
Administrator Authentication Alarm, Tamper Alarm and Door Sensor Alarm will be effective only if the alarm switch is set to ON status.

- **Note:** The default status of the alarm switch is ON. The alarm will not be triggered if the alarm switch is set to OFF status.

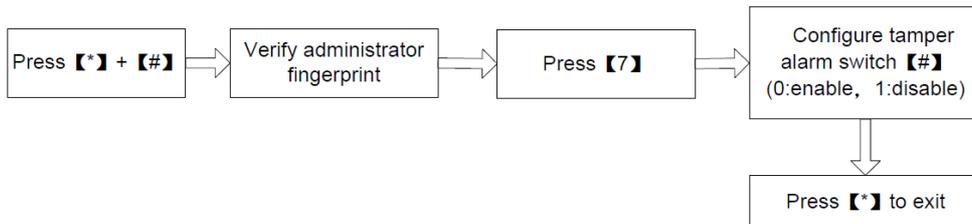


Configuring Administrator Authentication Alarm*

If the administrator fails in authentication in 3 attempts, Administrator Authentication Alarm will be triggered. No authentication can be made within 20 seconds. The default status of the administrator authentication alarm is ON.



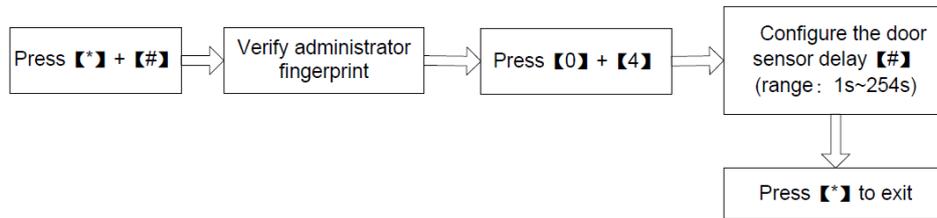
Configuring Tamper Alarm



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

Configuring Door Sensor Delay (default value: 10s)

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. Values greater than 254 are considered invalid. The indicator turns red and makes four short beeps.
2. When an alarm is triggered, the device interior alarm will be triggered first. After 30 seconds, the device exterior alarm will be triggered.

Factory Defaults (Eight passwords for opening the door are set to 0 after reset)

Parameters Type	Defaults
Unlocking Duration	6s
Verification Mode	Fingerprint/Password/RF Card
Door Sensor Type	None
Alarm Switch	enable
Administrator Authentication Alarm	enable
Tamper Alarm	enable
Door Sensor Delay	10s

Technical Specifications

Fingerprint Collector	SilkID Fingerprint Reader
Key Type	Touch key
User Capacity	500
Fingerprint Capacity	500
Card Capacity	500
Access Control Function	Unlocking, Alarm, Lock driver time length
Alarm Function	Tamper Alarm, Failed Authentication Alarm, Door Sensor Alarm
Doorbell	External wired doorbell

ZK Building, Wuhe Road, Gangtou, Bantian, Buji Town,
Longgang District, Shenzhen China 518129.

Tel: +86 755-89602345

Fax: +86 755-89602394

www.zkteco.com

Documents / Resources

	<p>ZKTECO X8-BT Bluetooth ID Card Reader Access Control Terminal [pdf] User Manual 290, X8-BT Bluetooth ID Card Reader Access Control Terminal, X8-BT, Bluetooth ID Card Reader Access Control Terminal, ID Card Reader Access Control Terminal, Reader Access Control Terminal, Access Control Terminal, Control Terminal, Terminal</p>
---	--

References

- [ZKTeco | Biometrics and Computer Vision](#)
- [User Manual](#)

[Manuals+](#), [Privacy Policy](#)

This website is an independent publication and is neither affiliated with nor endorsed by any of the trademark owners. The "Bluetooth®" word mark and logos are registered trademarks owned by Bluetooth SIG, Inc. The "Wi-Fi®" word mark and logos are registered trademarks owned by the Wi-Fi Alliance. Any use of these marks on this website does not imply any affiliation with or endorsement.