

User Manual

ML300

Date: October 2020

Doc Version: 1.0

English

Thank you for choosing our product. Please read the instructions carefully before operation. Follow these instructions to ensure that the product is functioning properly. The images shown in this manual are for illustrative purposes only.



For further details, please visit our Company's website
www.zkteco.co.za

Table of Contents

Product Overview	1
Product Features	1
Lock Setup	2
1. Resetting the Lock.....	2
2. Pairing the Lock with App.....	2
3. Programming the Lock in Standlone Mode.....	3
4. *Adding the Smart Gateway.....	5
5. *Connecting to Amazon Alexa or Google Assistant.....	6
How to Use	6
Unlocking Door with Fingerprint.....	6
Unlocking Door with Password.....	6
Unlocking Door with App.....	7
*Unlocking Door with Voice Assistant.....	7

Important Notes

1. Before registration, the new locks can be unlocked by any authentication method by default.
2. An administrator must be registered first, before any other operation in the Standalone Mode.
3. Four alkaline AA batteries (not included) are needed to power the device. Non-alkaline and rechargeable batteries **ARE NOT RECOMMENDED**.
4. Do not remove batteries from the lock when it is operating.
5. Batteries must be replaced when the lock flashes the red light along with 2-second beeps after being turned on.
6. The locks are also equipped with mechanical keys for manual unlocking. Please keep the mechanical keys at a safe place.
7. **Fingerprint positioning tips:**

Recommended fingers: Index, middle, or ring fingers; avoid using the thumb or pinky, as it is difficult to accurately press onto the fingerprint reader using those.



Too low



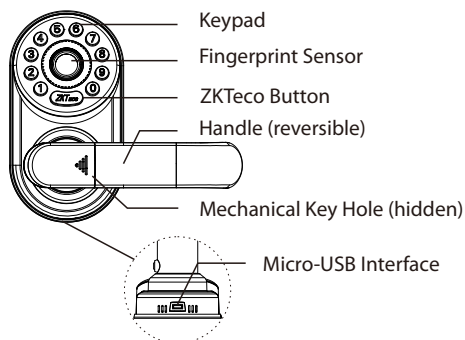
Too close to the edge



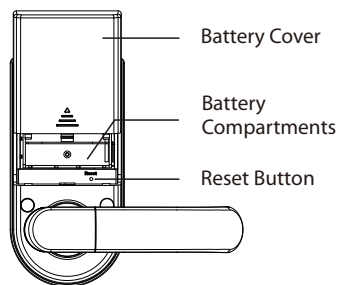
Vertical

Note: Please use the correct method when pressing your fingers onto the fingerprint reader for registration and identification. Our company will assume no liability for recognition issues that may result from incorrect usage of the product. We reserve the right of final interpretation and modification concerning this point.

Product Overview



Outdoor Unit



Indoor Unit

Product Features

User Introduction:

- 1) The **maximum capacity** of all users is 100. The **maximum capacity of each verification method** (fingerprint/password) is 100.
- 2) **Owner** is the person who owns the lock and registers it in **ZSmart App**, and has all the privileges.
- 3) **Admin** can always unlock via fingerprint, password, or App. Admin can add or delete normal users, and control all lock settings.
- 4) **Normal User** can always unlock via fingerprint, password, or App, and check the opening records.

Initialization: All registered user data will be deleted and restored to the factory default setting.

Random Password: To protect the password, users may enter their password with random digits before or after the actual password. The maximum number of entered digits must be less than or equal to 32. For example: If the correct password is 123456, then the random password can be 89123456807, 1234562363, 389123456, etc.

Low Battery Warning: When the battery power is low, the lock will flash the red light along with 2-second beeps after being turned on. Then the batteries need to be replaced.

Illegal Attempts Alert: After 5 failed verification attempts, the lock will flash the red light along with 10-second beeps and the lock will not be operable hereafter.

Emergency Charging: The bottom of the outdoor unit is provided with a Micro-USB interface. Use a power bank to charge the lock when it is out of power.

Emergency Mechanical Key: The mechanical key is used to open the door when the lock has any electronic malfunction. Slide the key cover and insert the key to unlock in emergency situations.

Bluetooth Connectivity: The lock is designed with BLE5.0 communication, you can unlock it via your smart phone when the Bluetooth is connected.

***Remote Access:** This function is only available for the additional Smart Gateway. With the **Smart Gateway** installed, the lock can be controlled remotely via **ZSmart App**.

***Voice Assistant Control:** This function is only available for the additional **Smart Gateway**. The lock can be unlocked using your voice commands through Amazon Alexa and the Google Assistant.

Lock Setup

1 Resetting the Lock

Please note all registered user data will be deleted and restored to the factory default setting.

If Paired with App: Tap the **EDIT** button on the upper right corner of Device Interface, and click "Disconnect and wipe data" to remove the lock from your **ZSmart Account**. Then press and hold the reset button until you hear one long beep and two short beeps.

If Never Paired: Press and hold the reset button until you hear one long beep and two short beeps.

2 Pairing the Lock with App

Step 1

Search for the "ZSmart" App in iOS App Store or Google Play Store, or scan the QR code to download the App.



Step 2

Open the **ZSmart App**, register and sign in to the account.

Step 3

Make sure the lock is in Factory Default Mode. Turn on Bluetooth permission on your smartphone, and stay near the lock (within 10 meters without obstacles).

Step 4

Tap the "+" button on the upper right corner, follow the on-screen instructions to pair the lock automatically, and start to use it.

Note: If you don't want to use the App, please check the next section i.e. "Programming the Lock in Standalone Mode"

3 Programming the Lock in Standalone Mode

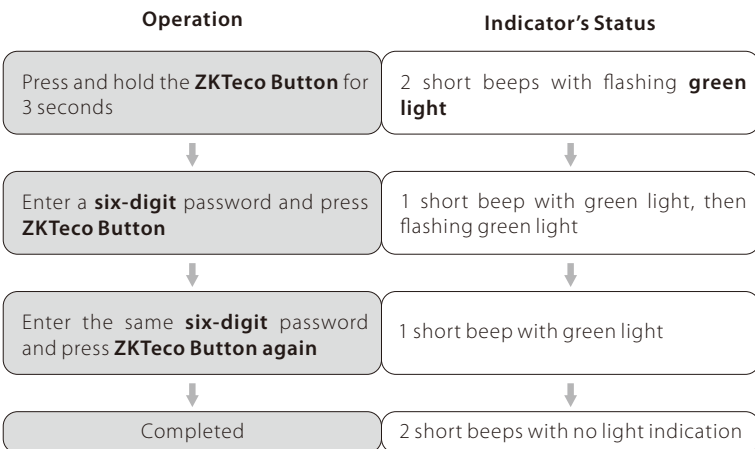
It is recommended to use ZSmart App to program your lock. If you don't have a smartphone or don't want to use the App, you can use the programming instructions below.



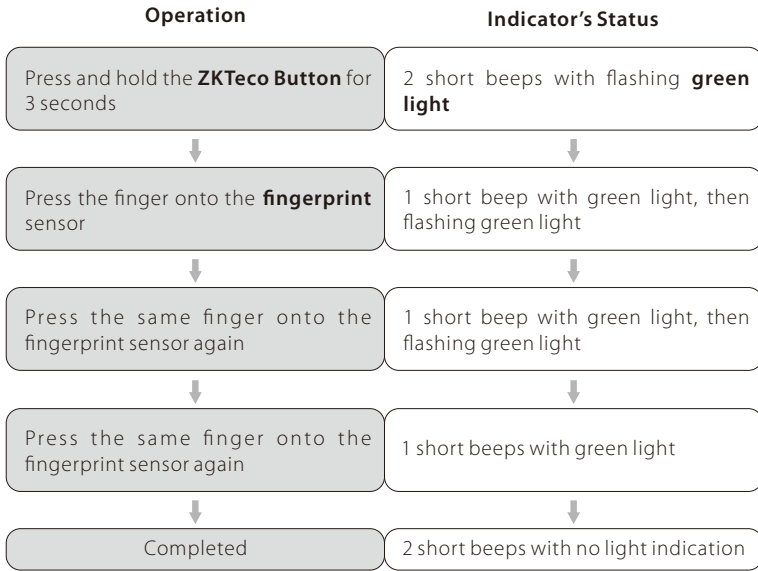
Note:

Standalone Mode is not available after the lock is registered in App! Please reset the lock to Factory Default Mode first to program your lock in Standalone Mode.

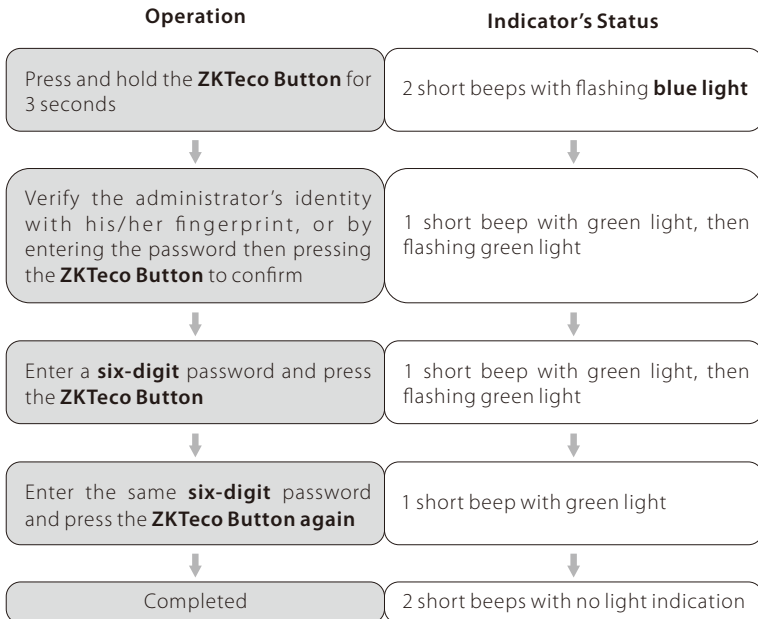
3.1 Add the Admin Password in Standalone Mode



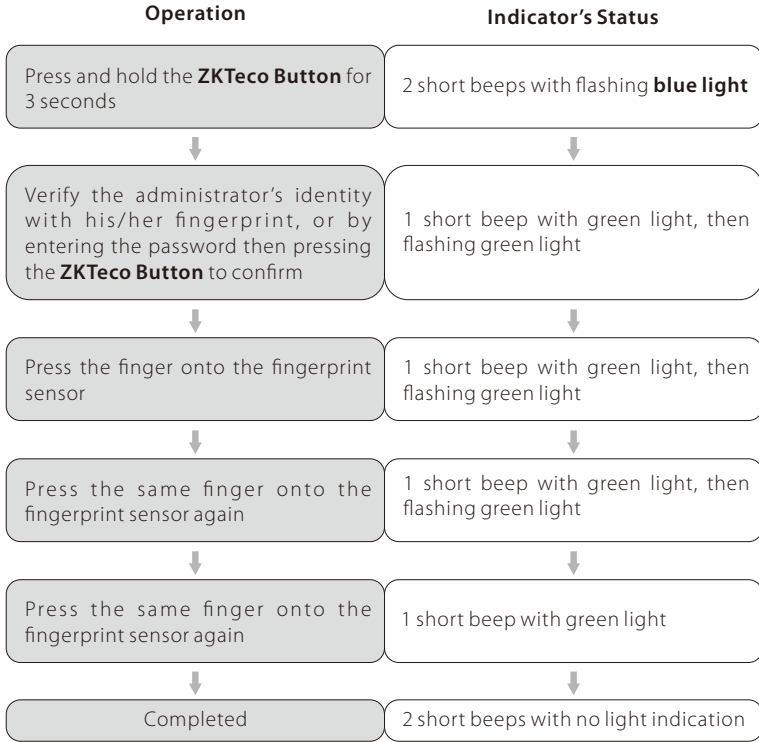
3.2 Add the Admin Fingerprint in Standalone Mode



3.3 Add the User Password in Standalone Mode



3.4 Add the User Fingerprint in Standalone Mode



Note:

- 1) Admin must be created before any other programming. **Only one Admin is available in the Standalone Mode.**
- 2) The verification mode of an admin can be a fingerprint or a passcode.
- 3) The registered password must be six digits.
- 4) If you try to register the same fingerprint/password again, the lock will prompt one long beep with a red light.

4 *Adding the Smart Gateway

Step 1

Plug the Gateway into the outlet using the provided Power Adapter.

Step 2

Open the **ZSmart App**. Tap the "+" button on the upper right corner, and then select the "Smart Lock/Wireless Gateway" category.

Step 3

Follow the on-screen instructions to connect the Gateway to the 2.4GHz Wi-Fi network and complete the setup.

Step 4

Enter the device interface of Gateway, and then follow the on-screen instructions to select the corresponding lock to add.

5 *Connecting to Amazon Alexa or Google Assistant

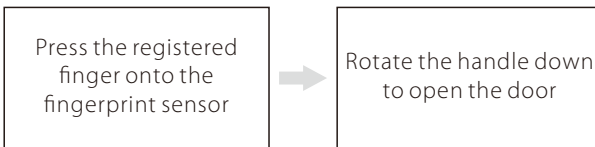
Tap the **EDIT** button on the upper right corner of the device interface. Select the **Alexa or Google Assistant icon**, then follow the on-screen instructions to link your **ZSmart Account** to Amazon Alexa or Google Assistant.

After completing the setup, you can use the supported voice commands that include:

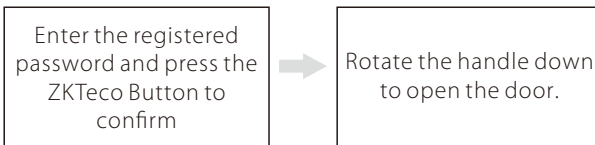
- Alexa, unlock the front door.
- OK Google, unlock the front door.

How to Use

Unlocking Door with Fingerprint



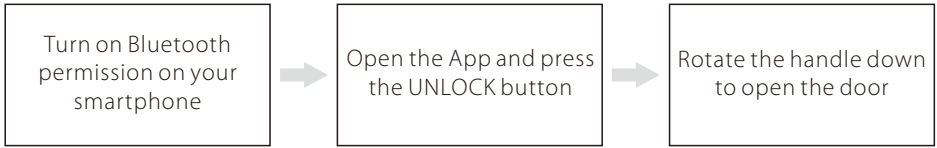
Unlocking Door with Password



Note:

- 1) You can press the ZKTeco Button to turn on the keypad backlight.
- 2) Users may enter a random password to prevent any person from observing the password. The maximum length of a random password is 32 digits.

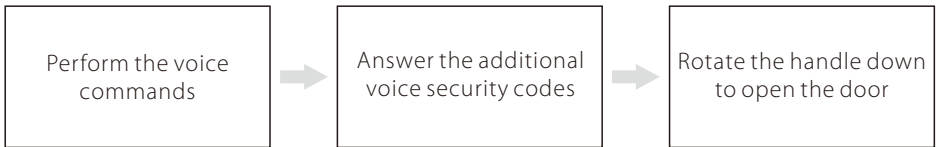
Unlocking Door with App



Note:

- 1) If you have already paired the lock with the gateway, you don't need to turn on Bluetooth.
- 2) When unlocking the lock via Bluetooth, please stay near the lock (within 10 meters without obstacles).

*Unlocking Door with Voice Assistant



Note: Once the Lock and Smart Gateway has been installed and configured correctly, make sure you enable the "ZSmart" Amazon Alexa Skill and Google Home Action first before you can configure your voice to perform voice commands.



Warning:

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC RF Radiation Exposure Statement:

- This Transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
- This equipment complies with RF radiation exposure limits set forth for an uncontrolled environment.

IMPORTANT! Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.