

# TTLock App Manual



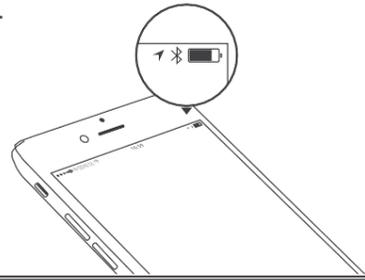
Scan the QR code on the left to download and install APP.

Please read this manual carefully before installation, and save it

- Please consult the dealership store or the installer for installation and testing which are not recorded in the manual. If the problem cannot be solved, please call us for support.
- **Please turn on the phone's Bluetooth function before any operation.**

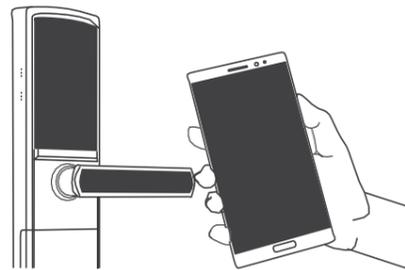


Attention



## Add a smart lock on your phone

- The following operations need to be combined with the [Add & Remove Fingerprint, Password or Bluetooth Manager] section on the back of this manual and follow the instructions to add a smart lock on your phone.



- **When adding devices, operations must be completed near the lock.**



cannot be added without a "+" sign. The interface will jump back to the key list interface after adding successfully. If the adding is unsuccessful, please repeat the above steps and view the device list in step 3.

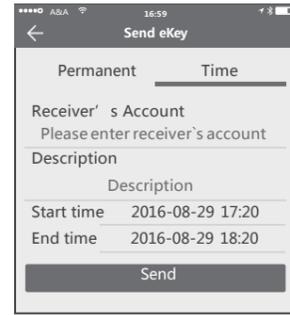
## Send a permanent eKey



Step 1: Click the device name Step 2: Click to send key Step 3: Enter following the prompts

- If you are not the administrator of the device, please contact the device administrator to ask for the secondary authorization function of the device.
- This feature requires the receiver to install the APP in the phone and have an account.

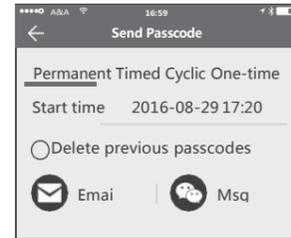
## Send a timed eKey.



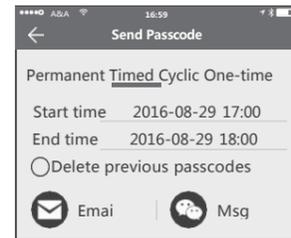
- In the authorized period of time, the receiver can unlock the lock regardless of times. Beyond the limitation of time, it will be invalidated automatically.

## Send a timed passcode

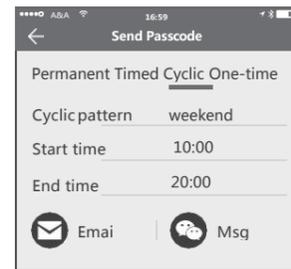
- Passcode is divided into four types: permanent, timed, cyclic and one-time. Please set its attributes accordingly.



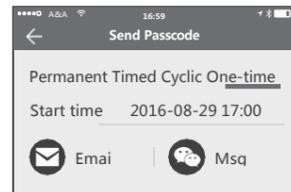
- Permanent passcodes will not expire, but the administrator can delete them in the user list.



- If the [Delete previous passcodes] is checked, all passcodes that have been used on the lock will be deleted while the new generated passcode is used for the first time.
- The passcode needs to be used once within 24 hours after the start time, otherwise it will be invalid.

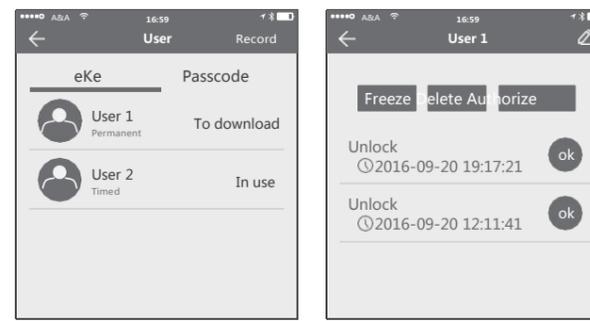


- The cyclic passcode's cycle is a week and can be used cyclically for a defined period of time.
- For example, if the time is valid when setting to 10:00 ~ 20:00 every weekend, the user can only open the door at the set time every weekend, and cannot open the door at other time.
- The passcode needs to be used once within 24 hours after the start time, otherwise it will be invalid.

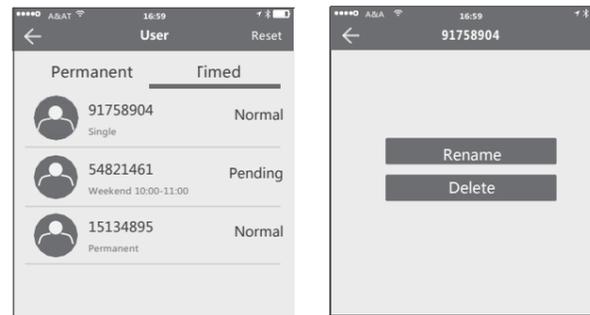


- The one-time passcode is valid for six hours after the start time.

## User management

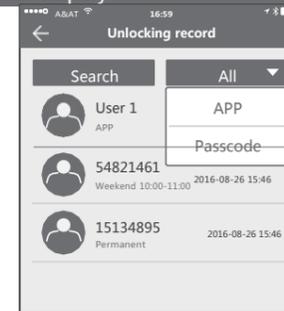


- In the list of eKey user management, click the user to perform the appropriate action:  
 [Modify Validity]: Click to modify the validity period of user's previous eKey.  
 [Freeze]: The user key can be temporarily frozen so that it loses the unlocking function. The function is recovered after freezing is removed.  
 [Authorize]: Authorize the receiver to send an eKey or passcode to other users.  
 In all of the above operations, the phones of two parties need to connect to the Internet, if the users cannot connect the network currently, the administrator's command will be responded after the Internet is connected.



- In the list of passcode user management, you can label the user. Click the user to perform the appropriate action:  
 [Rename]: This function can label the user and facilitate the management of passcodes.  
 [Delete]: This function can delete the user directly (for 3rd-generation lock)

## Unlocking records inquiry

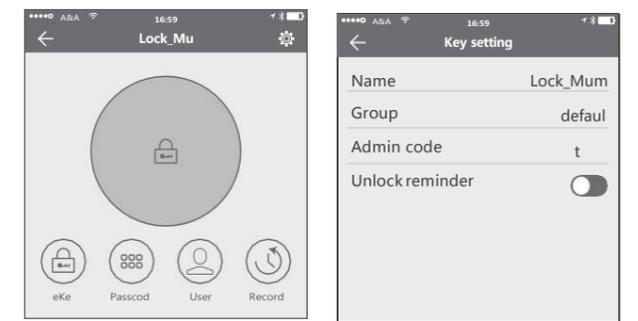


- Each time the ordinary user unlocks the lock with the eKey sent by the administrator, a record containing the user's nickname, eKey attributes and the unlocking time will automatically be generated and pushed to the administrator's APP.

### Attention

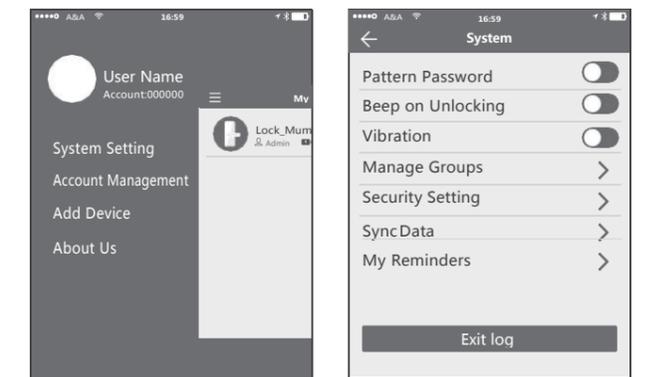
- **If a lock has already been added by a phone, it cannot be added by a new phone unless:**  
 1. The previous administrator delete it from his APP next to the lock.  
 2. The reset button on the lock is pressed.
- **Deleting the passcode must be operated next to the lock.**
- **Enter the software interface and click "≡" button to add locks as the pop-up list suggests.**

## Key setting



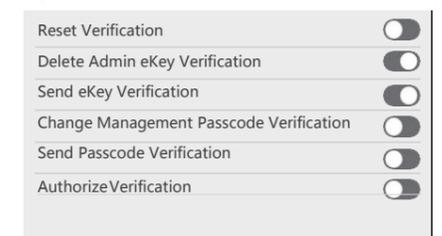
- Enter the device interface and click the button to name the device and view the current administrator's passcode.

## System Setting



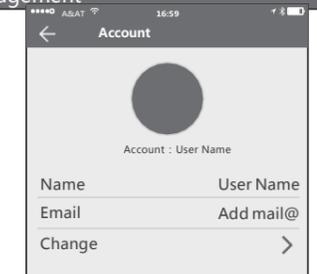
- Enter the software interface and click "≡" button, the appropriate action can be operated in the options of the pop-up users.

## Security Setting



- The verification function in the security settings is to prevent illegal operation on a stolen or lost mobile phone. This function is only activated when the administrator operates the device and manages the users.

## Account Management



- Click on the option to pop out the picture uploading feature and set the image, display your account, mailbox and other information. To modify the password, verification of original password is needed.