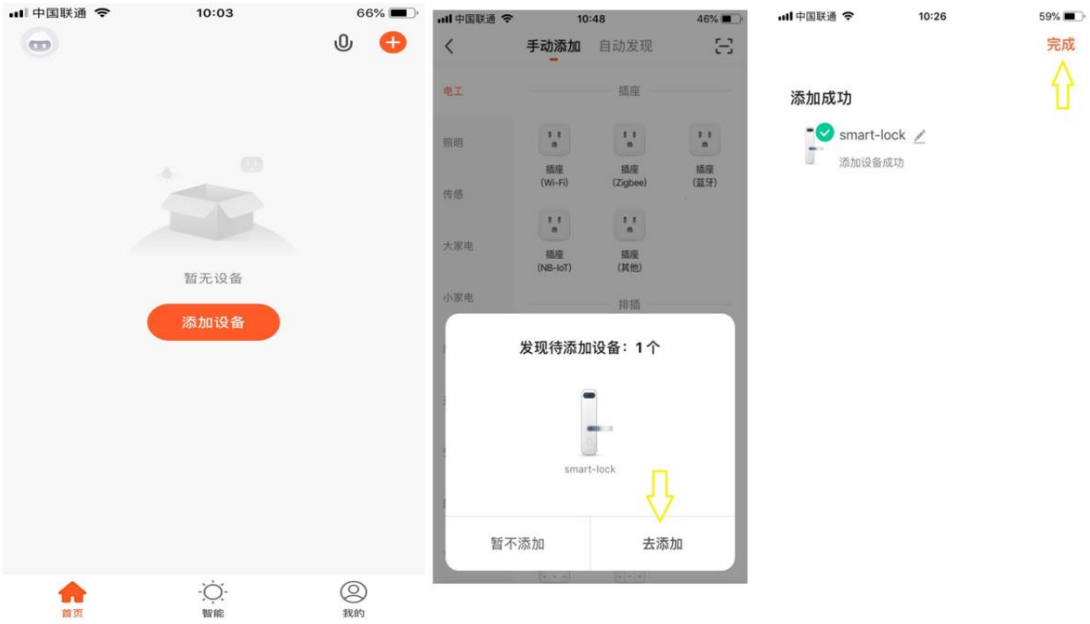
YonevloQ intelligent fingerprint password lock operation instructions

I. APP installation

1、Download and install the "Tuya Smart" APP from the app market.
2、Please register and login after installation.

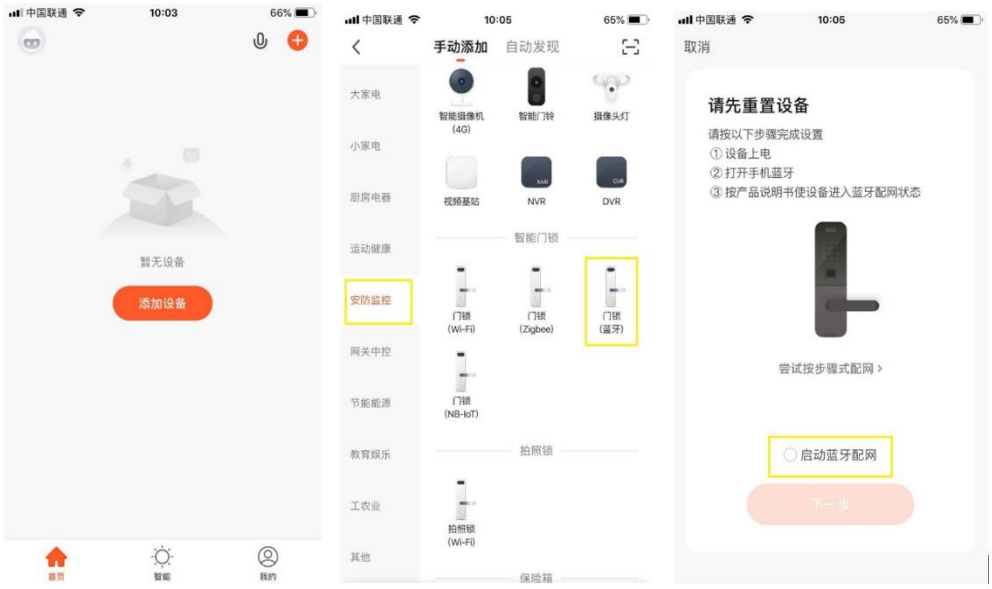
2. Distribution network connection lock

1, Press the fingerprint or the long lock end press the reset key to the red light (about 16S), release the button (if there is a fingerprint input in the lock, use the administrator fingerprint authentication), and the machine automatically enters the distribution network mode;
2, Click Add Device
3, When the phone opens the APP, the device will automatically jump out, the device name is "S mart L ock", and add the device.

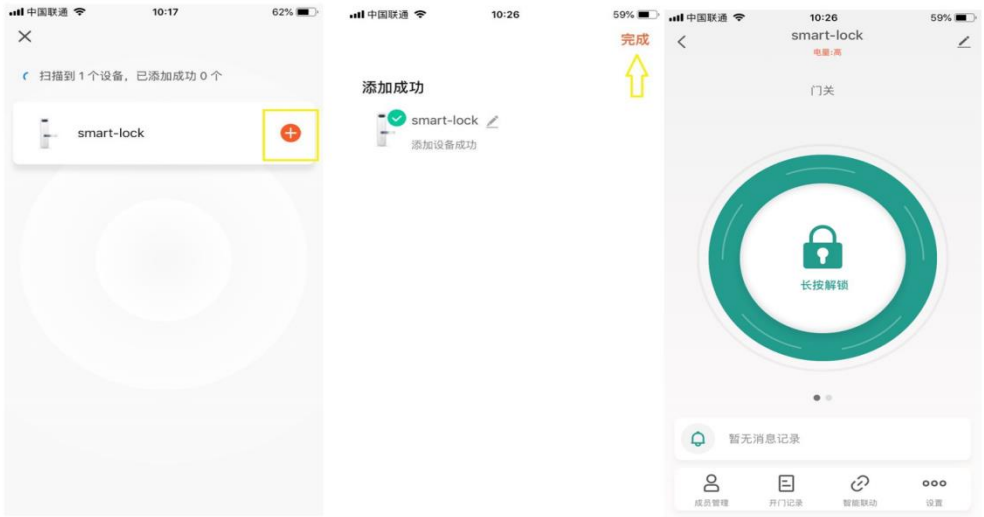


4, If the device does not automatically after the phone opens the A PP, set the device in this way

Open the A PP, click Add the device, select "Security monitoring", "Smart door lock", "Door lock (Bluetooth)", click "Start the Bluetooth distribution



network", and add the device after searching for the device.

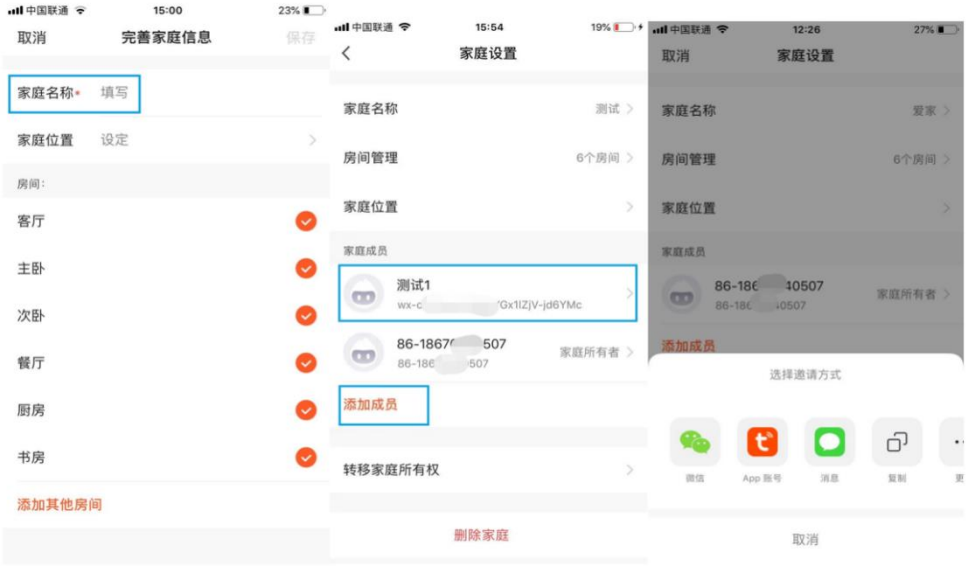


III. Member management

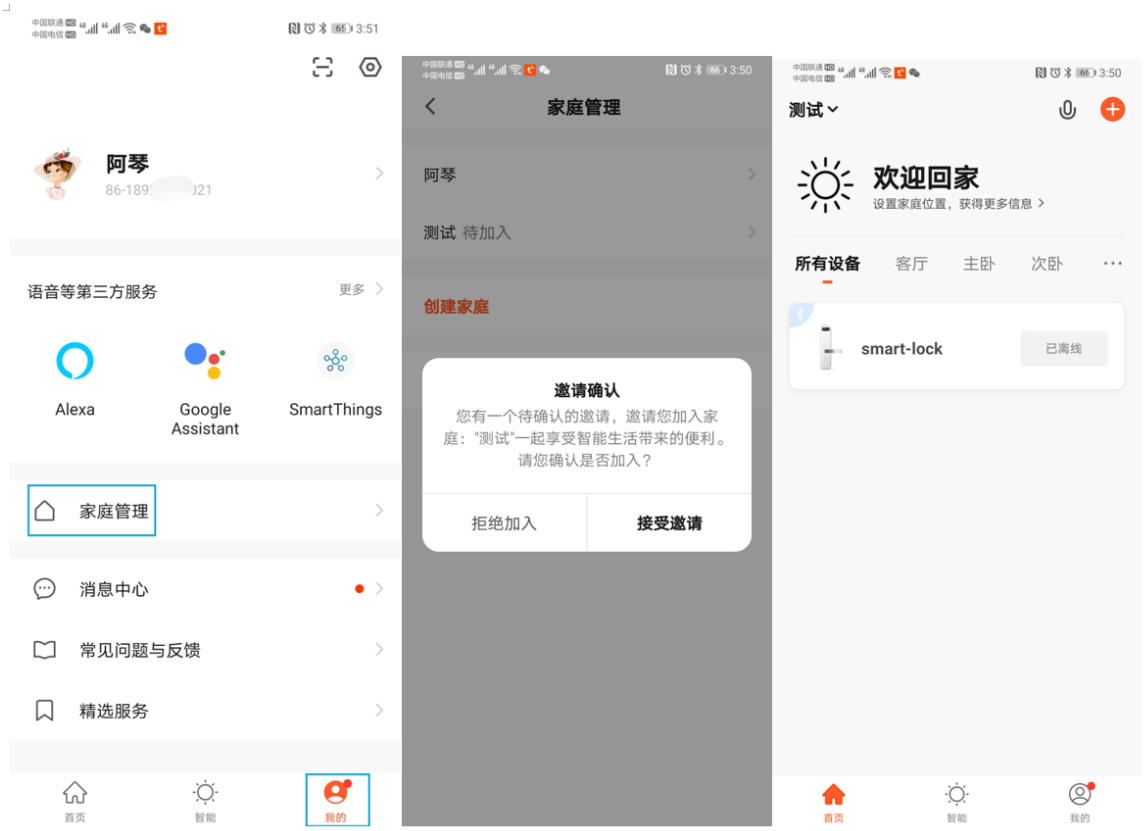
1. Member Management unlocking interface click "Member Management" and select "+" in the upper right corner of the interface

2. member of family

The registered family member for the first time is the administrator, click "Family Member" and "Add Now" to fill in "Family Name" and "Add Member". If you choose the wechat method, the system will automatically transfer to WeChatB 1 interface and send the invitation code to the family members.



After receiving the family members' information about adding members, download and register to log in to the Doodle A PP, find the family in "My" and " Family Management, and receive the invitation to add successfully.

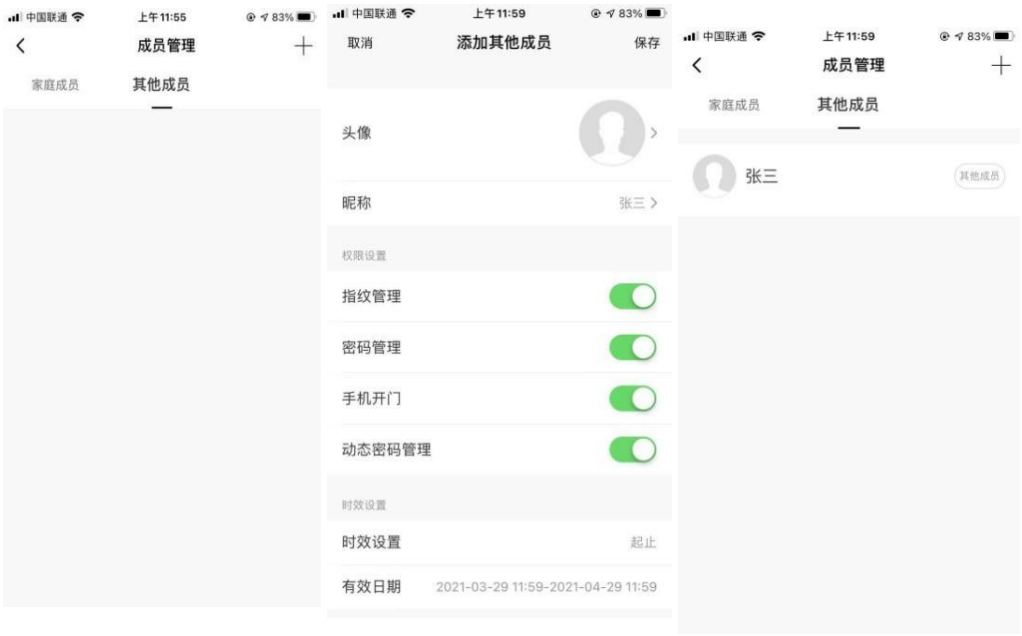


How to delete a family member: My, Family Management, Family Settings. Long. Remove family members on demand, select Remove Members.

3. Other members

Select Member Management and + in the upper right corner of Other Members to add other members. The time limit and valid date must be set.

See Remove Family Members



Four, unlock the way

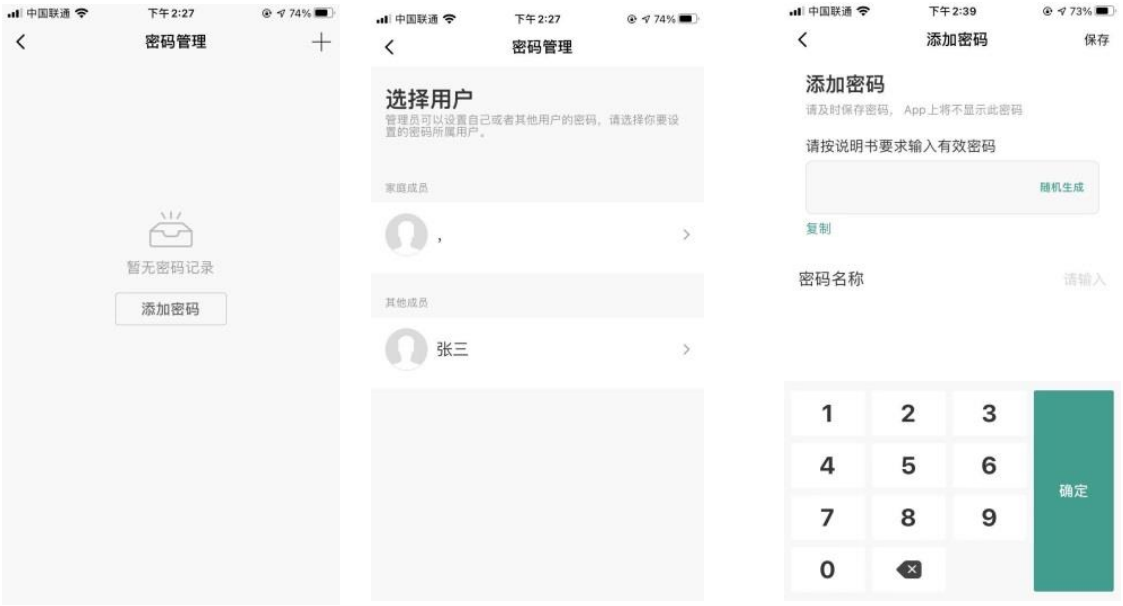
1, The first method: you can add fingerprint, password, card and dynamic password directly in the specific user interface under "Member management".
2, The second method: add to the setup interface.
3, The difference between the two methods: the first is to add an unlock method (such as fingerprint, password) to the user; the second is to correspond to the user under a specific unlock method (for example, fingerprint, password).
4, The second approach is presented below

a) Fingerprint Management:

Add a fingerprint: After selecting the user, press the prompt to input. You can add fingerprint groups: 40 groups (including administrator and ordinary user fingerprints).

Note: Only after entering the administrator fingerprint (at least one) can other user fingerprint (otherwise, prompt "operation fails"), and the administrator's first fingerprint of the administrator cannot be deleted; the fingerprint under the administrator has the administrator attribute (such as factory, verifying the administrator fingerprint).

Password management:



Add password: password can be generated randomly or by user input with 40 groups of passwords (including administrator password and ordinary user password); user password cannot be repeated with temporary password.

[The user password number is related to the number of digital touch buttons on the lock panel: there are 10 (0-9), the user password number is 6,8 or 9, the user password number is 7; the number is only 4 to 7, the user password number is 8. If the number of passwords is not clear, it can be generated randomly, that is, the lock end supports several bits!】

5. If the user has time limit (non-permanent user), the battery or the lock end is cut off. The user cannot unlock the lock and needs to connect the APP update time (APP, and the lock will be automatically update time).

V. Dynamic password

1, This feature only supports a lock body with a touch password.

2, Dynamic password operation process is as follows:

On the interface 1: finger left slide; enter the interface 2; click "get the dynamic password" on the interface 2, to generate the dynamic password;

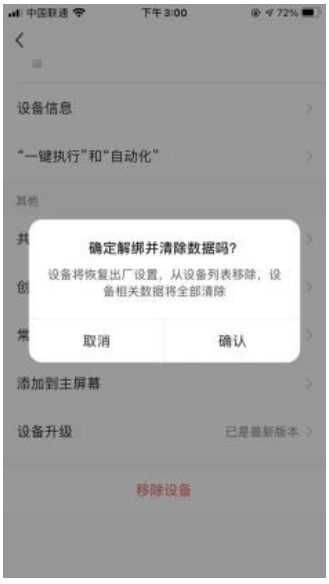
3, Lock terminal to enter the password to unlock the lock.

VI. Restore the factory setting and unbinding

1, Unbinding of the lock end: if the lock and Tuya smart APP must be unconnected, long press the reset key until the red light (about 16S), and then release the button to enter the automatic distribution network, the distribution network will resume the factory settings.Or long press the fingerprint until the red light (about 16S), raise the finger, the system prompt: "restore factory settings" "Please Verify administrator".After verifying the administrator fingerprint, restore the factory setting;

2, The APP end is unbound:

A. Lock and Tuya smart APP are connected:



Finally, the interface can click "Unbind and clear the data", and the device completely restores the factory settings.

B. If the lock and Doodle APP are not connected: untie a lock directly at the APP end, see Doodle FAQ-V1.1.docx for subsequent connection operation.

VII. Regular open mode:

1. Without connecting to the APP, often press the fingerprint head to the green light (about 10s with a user) and release. The system prompt: "Always open mode" and "Please Verify the administrator". System prompted with the administrator finger: Validation Success, Open open mode. This method needs to ensure a user (fingerprint or password).
2. When connecting to the APP,

3、How to cancel open mode: A, APP cancel; B, use valid fingerprint or password cancel.

VIII, System locking function

1, Lock failed 10 consecutive times (fingerprint or password), the system locked for 3 minutes (during any operation will prompt "system locked").
2, Neither the lock and APP operate after system lock.

Nine, temporary password

1, Temporary passwords are independent of the user and do not belong to any user
2, Maximum dynamic real-time (one-time temporary password is deleted) supports 10 sets of temporary passwords
3, Temporary password support 6 to 12 bits (whichever actual input)
4, Temporary passwords do not currently support unopen mode
5, Before the temporary password entry, ensure the administrator fingerprint at the lock
6, Temporary codes are limited by limitation
7, Temporary and user passwords cannot be repeatable

Other questions, reference: <<Tuya FAQ-V1.1.docx>>

burn-in test:

1, Make sure the lock has no user (fingerprint and password).
2, Power must be locked on the end and then press the 35896 # press.
3, The system enters the aging test.
4, After a process (lock-> wait-> lock), a red light will prompt.
5, Cancel aging: A, connect APP automatically cancel; B, enter the password "35896 #" cancel.

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.
Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.
NOTE: 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.
The device has been evaluated to meet general RF exposure requirement. The device can be u sed in portable exposure condition without restriction