Wireless Alarm Hub

Quick Start Guide

V1.0.0

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.

Cybersecurity Recommendations

Mandatory actions to be taken towards cybersecurity

1. Change Passwords and Use Strong Passwords:

The number one reason systems get "hacked" is due to having weak or default passwords. It is recommended to change default passwords immediately and choose a strong password whenever possible. A strong password should be made up of at least 8 characters and a combination of special characters, numbers, and upper and lower case letters.

2. Update Firmware

As is standard procedure in the tech-industry, we recommend keeping NVR, DVR, and IP camera firmware up-to-date to ensure the system is current with the latest security patches and fixes.

"Nice to have" recommendations to improve your network security

1. Change Passwords Regularly

Regularly change the credentials to your devices to help ensure that only authorized users are able to access the system.

2. Change Default HTTP and TCP Ports:

● Change default HTTP and TCP ports for systems. These are the two ports used to communicate and to view video feeds remotely.

● These ports can be changed to any set of numbers between 1025-65535. Avoiding the default ports reduces the risk of outsiders being able to guess which ports you are using.

3. Enable HTTPS/SSL:

Set up an SSL Certificate to enable HTTPS. This will encrypt all communication between your devices and recorder.

4. Enable IP Filter:

Enabling your IP filter will prevent everyone, except those with specified IP addresses, from accessing the system.

5. Change ONVIF Password:

On older IP Camera firmware, the ONVIF password does not change when you change the system's credentials. You will need to either update the camera's firmware to the latest revision or manually change the ONVIF password.

6. Forward Only Ports You Need:

● Only forward the HTTP and TCP ports that you need to use. Do not forward a huge range of numbers to the device. Do not DMZ the device's IP address.

● You do not need to forward any ports for individual cameras if they are all connected to a recorder on site; just the NVR is needed.

7. Disable Auto-Login on SmartPSS:

Those using SmartPSS to view their system and on a computer that is used by multiple people should disable auto-login. This adds a layer of security to prevent users without the appropriate credentials from accessing the system.

8. Use a Different Username and Password for SmartPSS:

In the event that your social media, bank, email, etc. account is compromised, you would not want someone collecting those passwords and trying them out on your video surveillance system. Using a different username and password for your security system will make it more difficult for someone to guess their way into your system.

9. Limit Features of Guest Accounts:

If your system is set up for multiple users, ensure that each user only has rights to features and functions they need to use to perform their job.

10. UPnP:

● UPnP will automatically try to forward ports in your router or modem. Normally this would be a good thing. However, if your system automatically forwards the ports and you leave the credentials defaulted, you may end up with unwanted visitors.

● If you manually forwarded the HTTP and TCP ports in your router/modem, this feature should be turned off regardless. Disabling UPnP is recommended when the function is not used in real applications.

11. SNMP:

Disable SNMP if you are not using it. If you are using SNMP, you should do so only temporarily, for tracing and testing purposes only.

12. Multicast:

Multicast is used to share video streams between two recorders. Currently there are no known issues involving Multicast, but if you are not using this feature, deactivation can enhance your network security.

13. Check the Log:

If you suspect that someone has gained unauthorized access to your system, you can check the system log. The system log will show you which IP addresses were used to login to your system and what was accessed.

14. Physically Lock Down the Device:

Ideally, you want to prevent any unauthorized physical access to your system. The best way to achieve this is to install the recorder in a lockbox, locking server rack, or in a room that is behind a lock and key.

15. Connect IP Cameras to the PoE Ports on the Back of an NVR:

Cameras connected to the PoE ports on the back of an NVR are isolated from the outside world and cannot be accessed directly.

16. Isolate NVR and IP Camera Network

The network your NVR and IP camera resides on should not be the same network as your public computer network. This will prevent any visitors or unwanted guests from getting access to the same network the security system needs in order to function properly.

Foreword

General

This Guide introduces the functions, installation wirings and operations of the wireless alarm hub.

Models

H1、H1G、H1F、ARC2000E-SW-imou、G2、DHI-ARC2000E-SW、ARC2000E-SW、ARC2000E-SW-LC

Safety Instructions

The following categorized signal words with defined meaning might appear in the Guide.

Signal Words	Meaning
⚠ DANGER	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
⚠ WARNING	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
⚠ CAUTION	Indicates a potential risk which, if not avoided, could result in property damage, data loss, lower performance, or unpredictable result.
TIPS	Provides methods to help you solve a problem or save you time.
NOTE	Provides additional information as the emphasis and supplement to the text.

Revision History

No.	Version	Revision Content	Release Time
1	V1.0.0	First Release	February 2019

Privacy Protection Notice

As the device user or data controller, you might collect personal data of others, such as face, fingerprints, car plate number, Email address, phone number, GPS and so on. You need to be in compliance with the local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures, including but not limited to: providing clear and visible identification to inform data subject the existence of surveillance area and providing related contact.

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.

Caution: The user is cautioned that 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.

FCC RF Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20cm between the radiator and any part of your body.

FCC Supplier’s Declaration of Conformity

Alarm Hub / H1G， H1, H1F, ARC2000E-SW-imou, G2, DHI-ARC2000E-SW, ARC2000E-SW, ARC2000E-SW-LC

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.

Dahua Technology USA Inc.,

23 Hubble Irvine, CA 92618

(949) 679-7777

About the Guide

- The Guide is for reference only. If there is inconsistency between the Guide and the actual product, the actual product shall prevail.
- We are not liable for any loss caused by the operations that do not comply with the Guide.
- The Guide would be updated according to the latest laws and regulations of related regions. For detailed information, see the User's Manual, CD-ROM, QR code or our official website. If there is inconsistency between User's Manual and the electronic version, the electronic version shall prevail.

- All the designs and software are subject to change without prior written notice. The product updates might cause some differences between the actual product and the Guide. Please contact the customer service for the latest program and supplementary documentation.
- There still might be deviation in technical data, functions and operations description, or errors in print. If there is any doubt or dispute, please refer to our final explanation.
- Upgrade the reader software or try other mainstream reader software if the Guide (in PDF format) cannot be opened.
- All trademarks, registered trademarks and the company names in the Guide are the properties of their respective owners.
- Please visit our website, contact the supplier or customer service if there is any problem occurred when using the device.
- If there is any uncertainty or controversy, please refer to our final explanation.

Important Safeguards and Warnings

The following description is the correct application method of the device. Please read the Guide carefully before use, in order to prevent danger and property loss. Strictly conform to the Guide during application and keep it properly after reading.

Operating Requirement

- Do not place and install the device in an area exposed to direct sunlight or near heat generating device.
- Do not install the device in a humid, dusty or fuliginous area.
- Keep its horizontal installation, or install it at stable places, and prevent it from falling.
- Do not drip or splash liquids onto the device; do not put on the device anything filled with liquids, in order to prevent liquids from flowing into the device.
- Install the device at well-ventilated places; do not block its ventilation opening.
- Use the device only within rated input and output range.
- Do not dismantle the device arbitrarily.
- Transport, use and store the device within allowed humidity and temperature range.

Power Requirement

- Use batteries according to requirements; otherwise, it may result in fire, explosion or burning risks of batteries!
- To replace batteries, only the same type of batteries can be used!
- The product shall use electric wires (power wires) recommended by this area, which shall be used within its rated specification!
- Use standard power adapter matched with this device. Otherwise, the user shall undertake resulting personnel injuries or device damages.
- Use power supply that meets SELV (safety extra low voltage) requirements, and supply power with rated voltage that conforms to Limited Power Source in IEC60950-1. For specific power supply requirements, please refer to device labels.
- Products with category I structure shall be connected to grid power output socket, which is equipped with protective grounding.
- Appliance coupler is a disconnecting device. During normal use, keep an angle that facilitates operation.

Table of Contents

1 Overview

1.1 Profile

Able to connect alarm devices, this alarm hub can communicate with the alarm devices through network, and report alarm information. It supports 2G/4G, Wi-Fi, and wired network. This hub adapts to residences and shops with high security demands, so users manage numerous alarm devices conveniently, and obtain reliable security service.

2G and 4G functions are not standard configurations. H1G matches with 2G module, whereas H1F matches with 4G module.

1.2 Feature

- Support maximum 32 wireless defense zones;
- Prompt with alarm tone;
- Support local alarm, alarm with short message and alarm with APP;
- Support audible and visual alarm linkage, as well as video linkage;
- Support backup battery. The battery can works for more than 4 hours after the power is off.

1.3 Structure

For device structure and description, see Figure 1-1 and Table 1-1.

Figure 1-1 Device structure

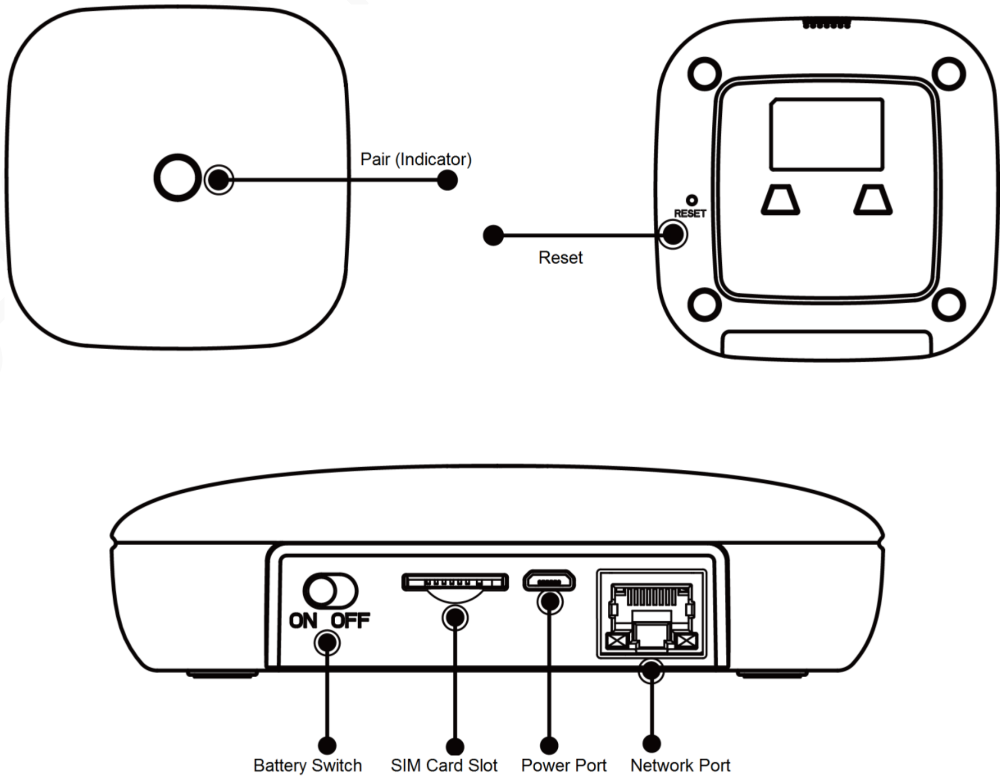


Table 1-1 Button function description

Button	Description
Pair	Pair with alarm devices. ● Press to enter wireless pairing mode. ● Press and hold for more than 5 seconds to enter AP network pairing mode.
Indicator	Indicate the device status. ● Blue light on represents normal operation. ● Slow flashing blue light represents that it enters AP network pairing mode. ● Fast flashing blue light represents that it enters wireless pairing mode. ● Slow flashing red light represents alarm or network error.
Reset	Reset the device to initialized status. During normal operation, press RESET hole for 6s with a needle. The indicator will flash red, the device will restore default status.
Battery switch	Turn on or off the standby battery. 📖 Turn on this switch, the standby battery of the device will automatically charge when the device is connected to power supply, so the device continues to work normally after power failure.
SIM card slot	With SIM card slot, the device goes online. 📖 Basic version H1 does not have SIM card slot.
Power port	5V power port.
Network port	Connect wired network.

1.4 Dimension

For device dimension, see Figure 1-2 and Figure 1-3.

Figure 1-2 Device dimension (1) (unit: mm)

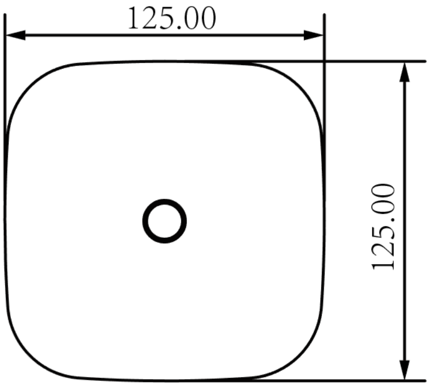
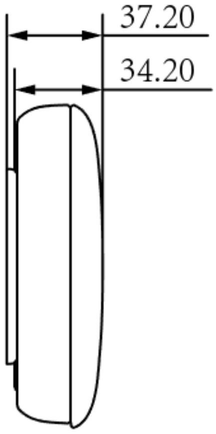


Figure 1-3 Device dimension (2) (unit: mm)

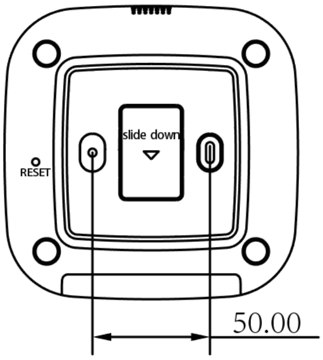


2 Installation

2.1 Installation Dimension

For installation dimension, see Figure 2-1.

Figure 2-1 Installation dimension (unit: mm)



2.2 Installation Procedure

You can install this device with expansion screw.

Step 1 Drill holes in the wall according to hole positions of the bracket.

Step 2 Put expansion tubes into the holes.

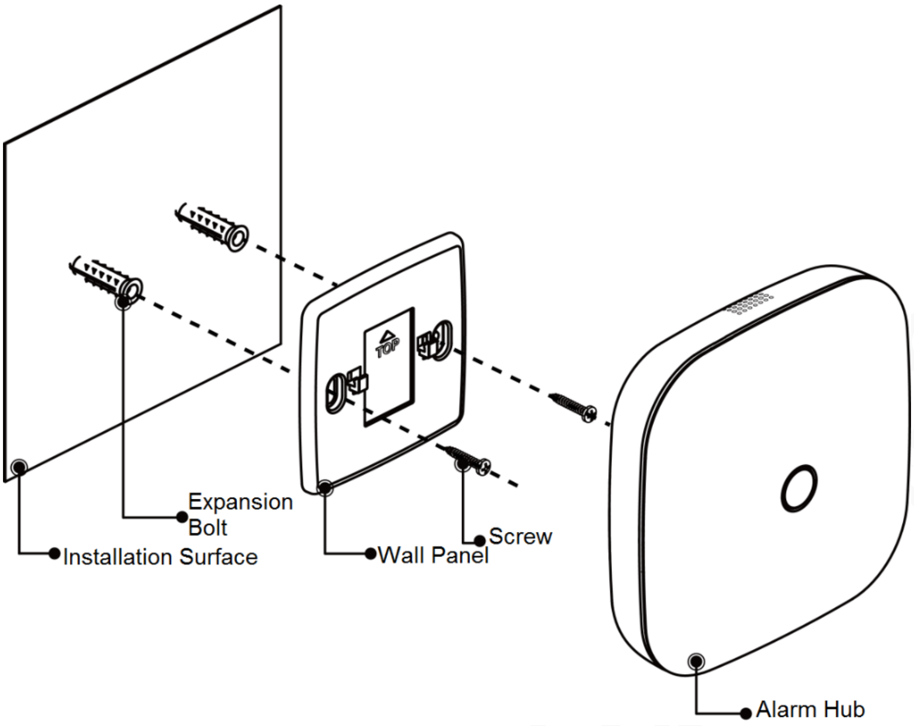
Step 3 Fix the bracket with self-tapping screws.

📖

After installation, insert SIM card or network cable, connect power supply and turn on hub switch, to configure and use the hub conveniently in the future. However, H1 model does not support SIM card.

Step 4 Put the hub into the bracket from top to bottom.

Figure 2-2 Installation with screws



To ensure normal network connection, insert SIM card before power-on.

3 Operation

You can download Imou APP, add the alarm hub, configure network, pair with accessories, arm and delete the accessories.

3.1 Downloading APP

You can search Imou client in APP market, download and login APP. Alternatively, you can scan the QR code as below to download the APP. See Figure 3-1.

Figure 3-1 QR code

- Android users, please go to Android APP market to search and download Imou.
- Apple users, please go to Apple Store to search and download Imou.

3.2 Adding Alarm Hub

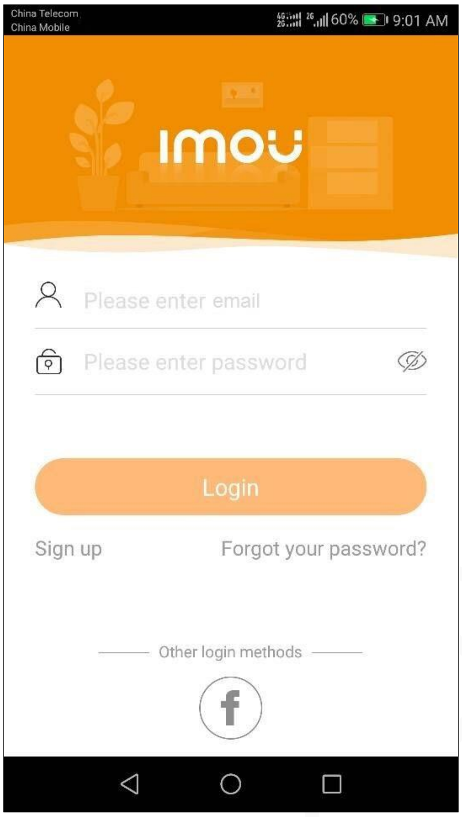
3.2.1 Adding Alarm Hub through Wired Network

- Initialize the hub when you use the hub for the first time.
- Ensure that your mobile phone has enabled Wi-Fi function. Ensure that Wi-Fi of mobile phone is in the same network segment as the network port that is connected by the hub.

Step 1 Tap App icon on your mobile phone, and start the App.

The **Login** interface is displayed. See Figure 3-2.

Figure 3-2 Login

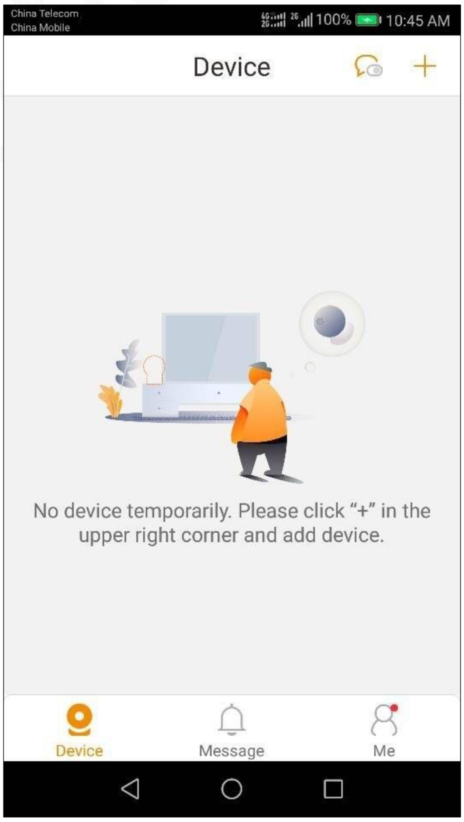


Step 2 Enter your mailbox and password, and then tap **Login**.

The **Device** interface is displayed. See Figure 3-3.

Tap **Sign up** if you have not signed up yet.

Figure 3-3 Device

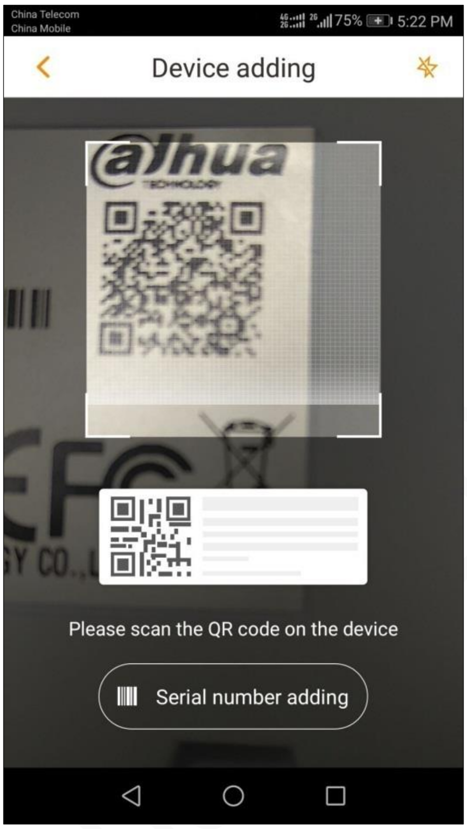


No device temporarily. Please click "+" in the upper right corner and add device.

Step 3 On the **Device** interface, tap + in the upper right corner.

The **Device adding** interface is displayed. See Figure 3-4. Remove the bracket, and then scan QR code at the bottom of the hub.

Figure 3-4 Device adding (QR code)

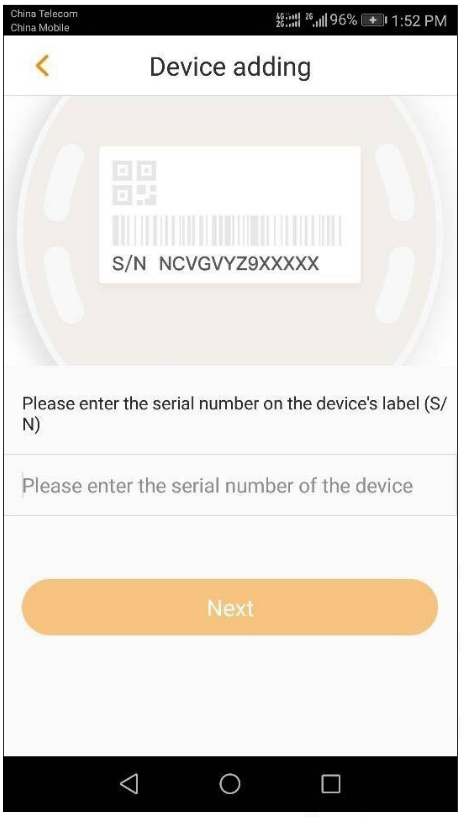


Device adding

Please scan the QR code on the device

Step 4 (Optional) Or tap **Serial number adding** if you fail to scan QR code. The serial number scanning interface is displayed. See Figure 3-5.

Figure 3-5 Device adding (serial number)



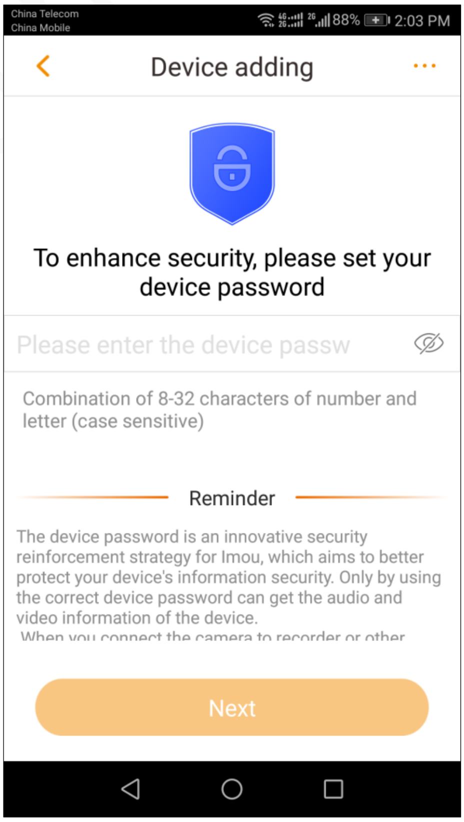
Please enter the serial number on the device's label (S/N)

Please enter the serial number of the device

Enter serial number of the device, select the device in the category of alarm station, and then tap **Next**.

Step 5 On the APP interface, tap **Next**. Enter the device password on the pop-up interface. See Figure 3-6.

Figure 3-6 Enter the device password



To enhance security, please set your device password

Please enter the device passw

Combination of 8-32 characters of number and letter (case sensitive)

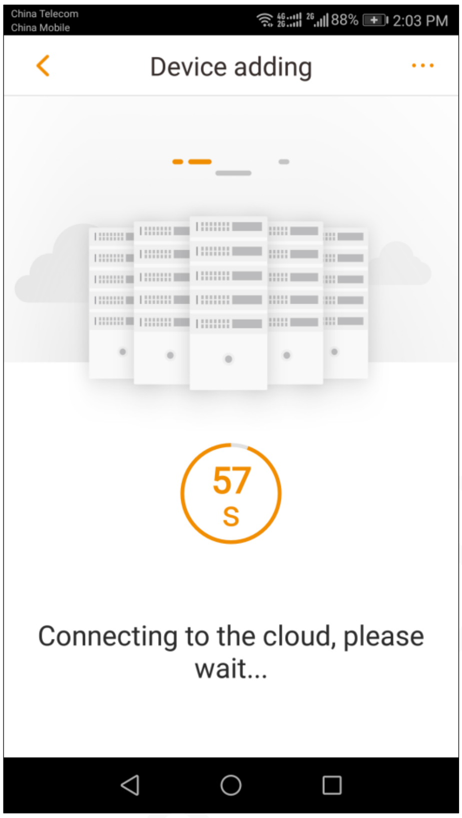
Reminder

The device password is an innovative security reinforcement strategy for Imou, which aims to better protect your device's information security. Only by using the correct device password can get the audio and video information of the device.
When you connect the camera to recorder or other

Step 6 On the APP interface, tap **Next**.

The hub is connecting with cloud. See Figure 3-7.

Figure 3-7 Connect cloud

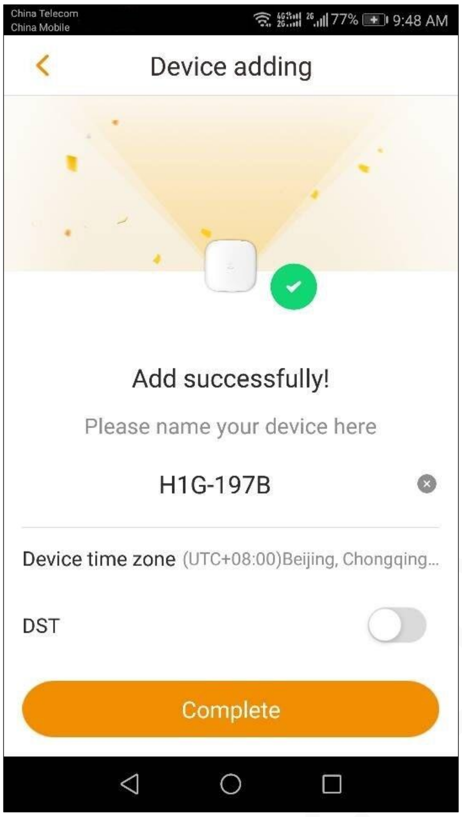


Connecting to the cloud, please wait...

Step 7 Then, the hub prompts that it is connected with router successfully.

The device is added successfully. On this interface, you can name your device, configure time zone and DST. See Figure 3-8.

Figure 3-8 Add successfully



China Telecom
China Mobile
77% 9:48 AM

Device adding

Add successfully!

Please name your device here

H1G-197B

Device time zone (UTC+08:00)Beijing, Chongqing...

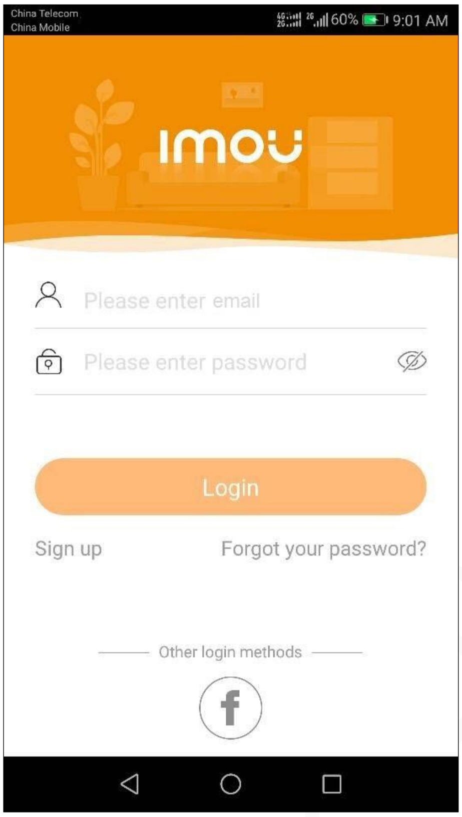
DST

Complete

3.2.2 Adding Alarm Hub through Wi-Fi

Step 1 Tap App icon on your mobile phone, and start the App.
The **Login** interface is displayed. See Figure 3-9.

Figure 3-9 Login

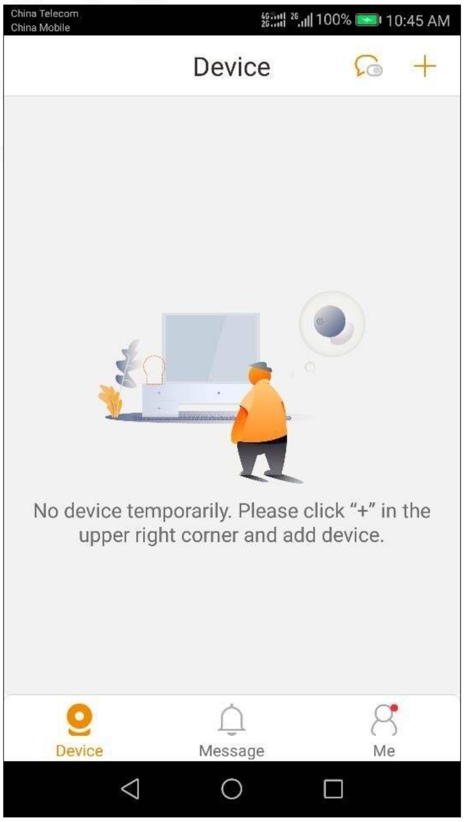


Step 2 Enter your mailbox and password, and then tap **Login**.

The **Device** interface is displayed. See Figure 3-10.

Tap **Sign up** if you have not signed up yet.

Figure 3-10 Device

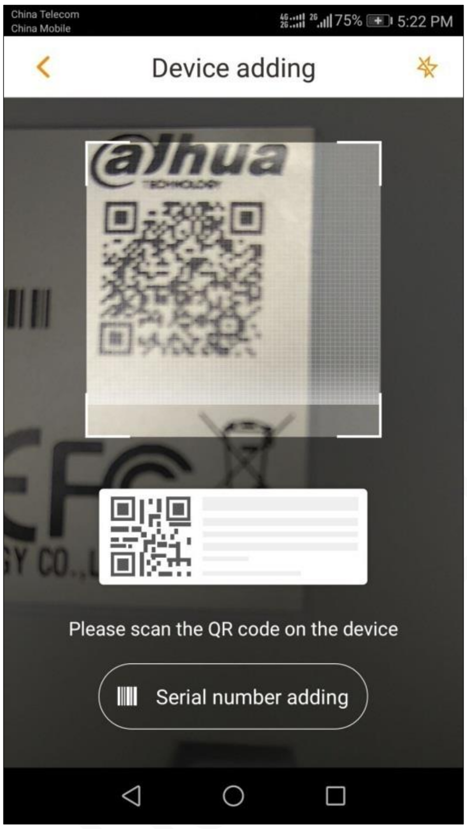


No device temporarily. Please click "+" in the upper right corner and add device.

Step 3 On the **Device** interface, tap + in the upper right corner.

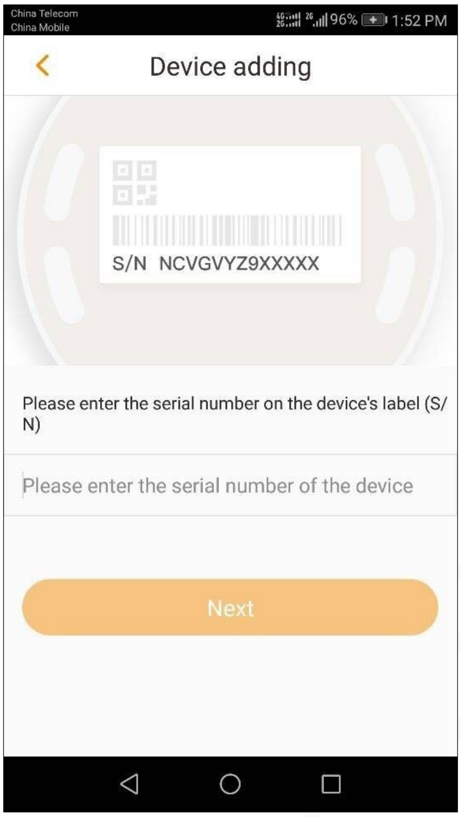
The **Device adding** interface is displayed. See Figure 3-11. Remove the bracket, and then scan QR code at the bottom of the hub.

Figure 3-11 Device adding (QR code)



Step 4 (Optional) Or tap **Serial number adding** if you fail to scan QR code. The serial number scanning interface is displayed. See Figure 3-12.

Figure 3-12 Device adding (serial number)



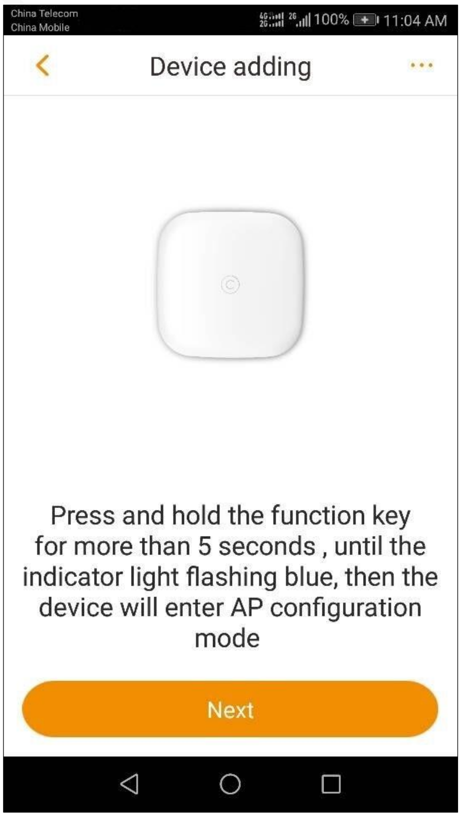
Please enter the serial number on the device's label (S/N)

Please enter the serial number of the device

Enter serial number of the device, select the device in the category of alarm station, and then tap **Next**.

<u>Step 5</u> Press and hold the function key on the top of the hub for more than 5 seconds, until the indicator light flashes blue, then the device will enter AP configuration mode. See Figure 3-13.

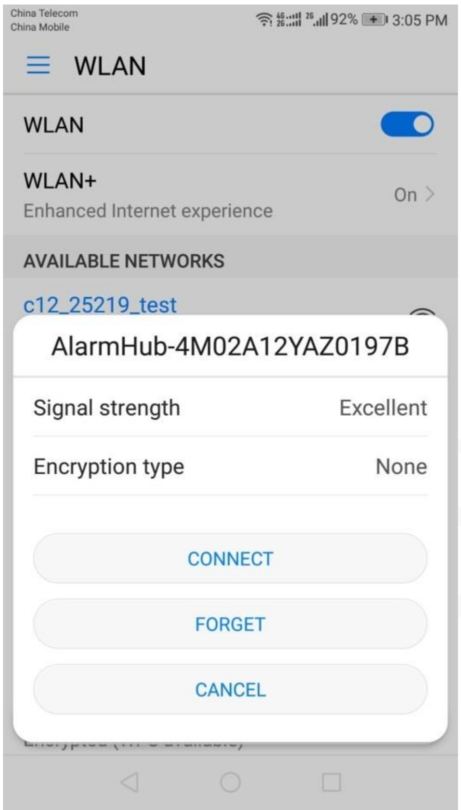
Figure 3-13 Press and hold functional key



Press and hold the function key for more than 5 seconds , until the indicator light flashing blue, then the device will enter AP configuration mode

Step 6 Enable WLAN on your mobile phone, tap hub hotspot (Hotspot Wi-Fi name is AlarmHub-hub serial number), and then tap **Connect** on the pop-up interface. See Figure 3-14.

Figure 3-14 Connect



China Telecom
China Mobile
92% 3:05 PM

WLAN

WLAN

WLAN+
Enhanced Internet experience
On

AVAILABLE NETWORKS

c12_25219_test

AlarmHub-4M02A12YAZ0197B

Signal strength Excellent

Encryption type None

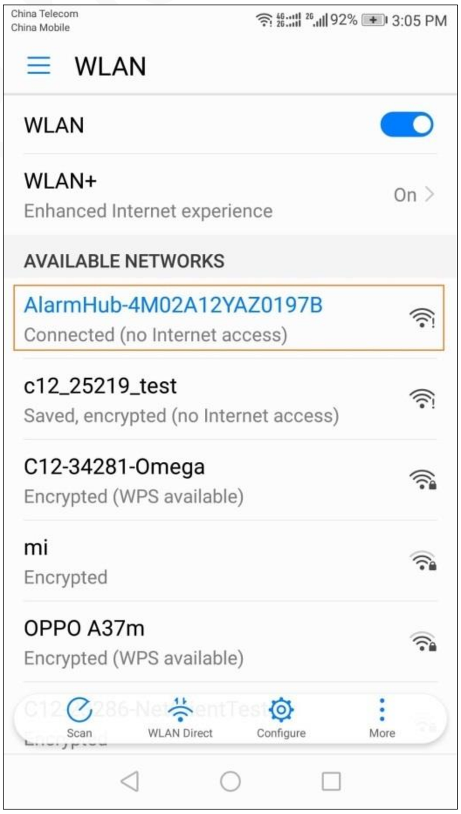
CONNECT

FORGET

CANCEL

The hotspot is connected successfully. See Figure 3-15.

Figure 3-15 Connect successfully



China Telecom
China Mobile
92% 3:05 PM

WLAN

WLAN

WLAN+
Enhanced Internet experience
On

AVAILABLE NETWORKS

AlarmHub-4M02A12YAZ0197B
Connected (no Internet access)

c12_25219_test
Saved, encrypted (no Internet access)

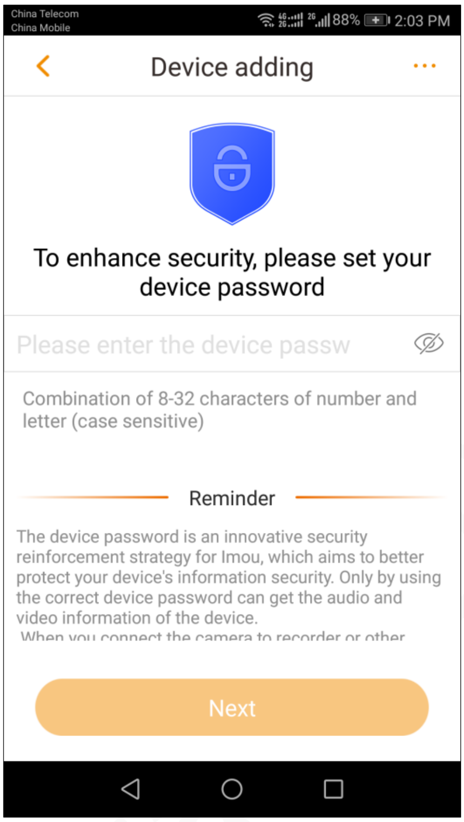
C12-34281-Omega
Encrypted (WPS available)

mi
Encrypted

OPPO A37m
Encrypted (WPS available)

Step 7 Go through Step 1 to Step 6 in 3.2.1 Adding Alarm Hub through Wired Network. On the APP interface, tap **Next**. Enter the device password on the pop-up interface. See Figure 3-16.

Figure 3-16 Enter the device password



China Telecom
China Mobile
88% 2:03 PM

Device adding

To enhance security, please set your device password

Please enter the device passw

Combination of 8-32 characters of number and letter (case sensitive)

Reminder

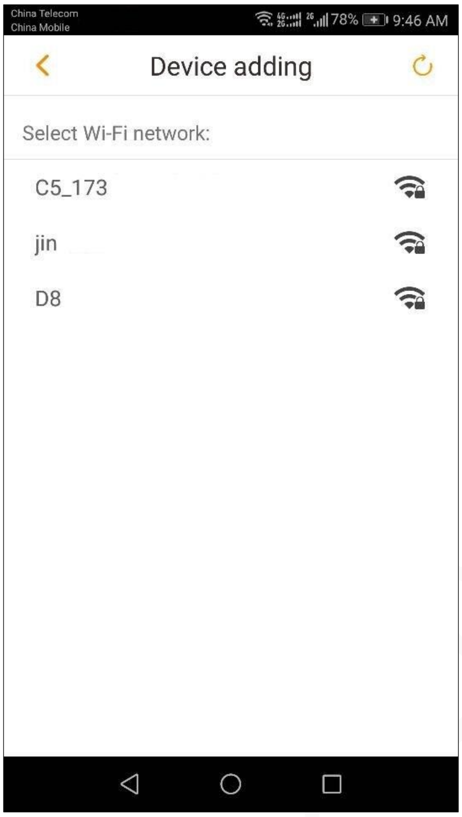
The device password is an innovative security reinforcement strategy for Imou, which aims to better protect your device's information security. Only by using the correct device password can get the audio and video information of the device.
When you connect the camera to recorder or other

Next

Step 8 On the APP interface, tap **Next**.

Select Wi-Fi network, and enter Wi-Fi password according to interface prompts. See Figure 3-17 and Figure 3-18.

Figure 3-17 Select Wi-Fi



China Telecom
China Mobile
78% 9:46 AM

Device adding

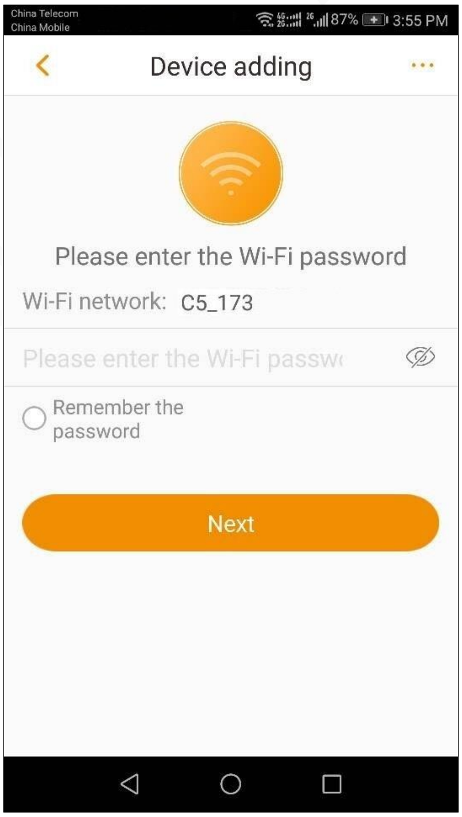
Select Wi-Fi network:

C5_173

jin

D8

Figure 3-18 Enter Wi-Fi password



China Telecom
China Mobile
87% 3:55 PM

Device adding

Please enter the Wi-Fi password

Wi-Fi network: C5_173

Please enter the Wi-Fi passw

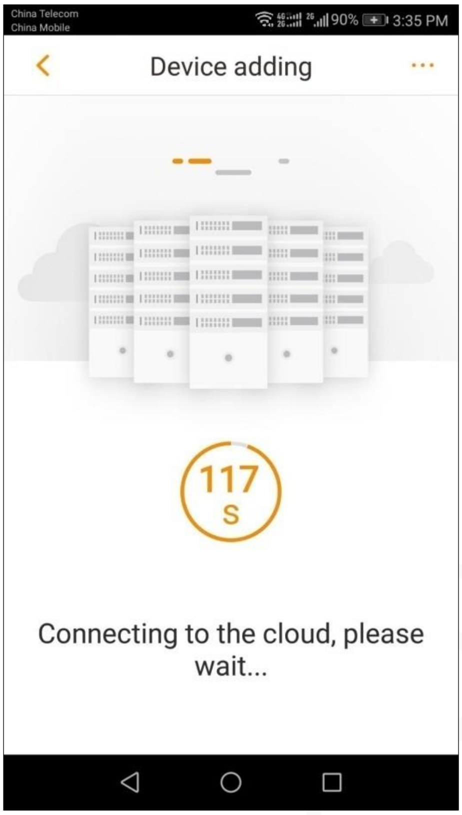
○ Remember the password

Next

Step 9 On the APP interface, tap **Next**.

The hub is connecting with cloud. See Figure 3-19.

Figure 3-19 Connect cloud



Device adding

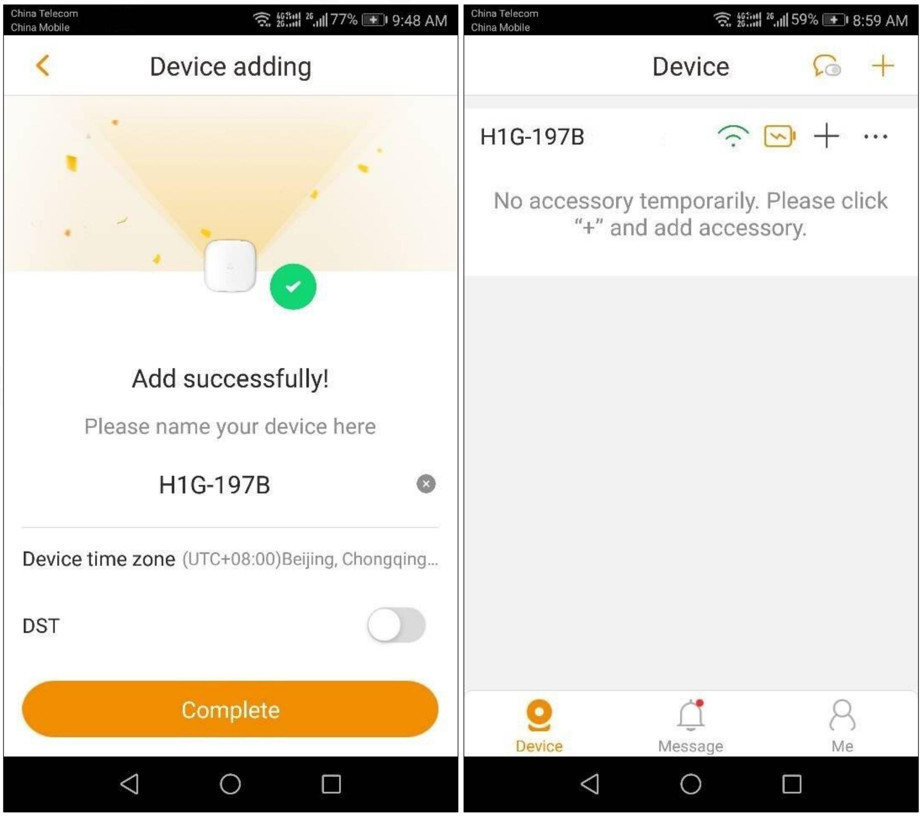
117 S

Connecting to the cloud, please wait...

Step 10 Then, the hub prompts that it is connected with router successfully.

The device is added successfully. On this interface, you can name your device, configure time zone and DST. See Figure 3-20.

Figure 3-20 Add successfully



Device adding

Add successfully!

Please name your device here

H1G-197B

Device time zone (UTC+08:00)Beijing, Chongqing...

DST

Complete

Device

H1G-197B

No accessory temporarily. Please click "+" and add accessory.

Step 11 Tap **Complete**, and the hub is added to the device list.

Table 3-1 Icon description

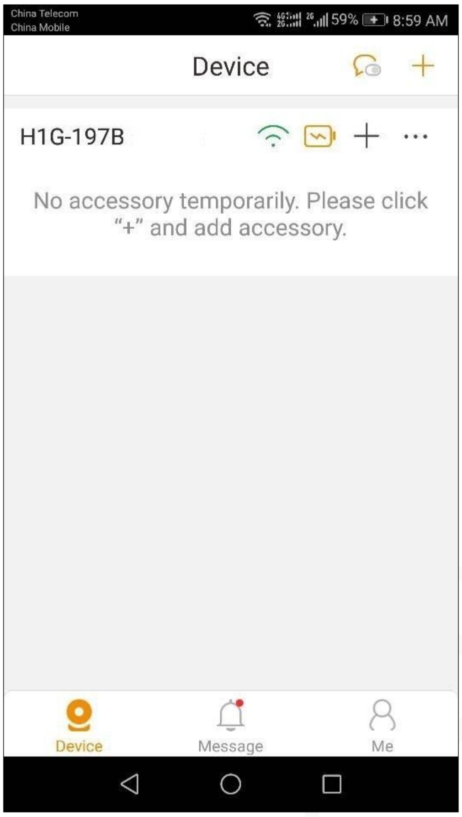
Icon	Description
💬	Tap to enable or disable DND mode. Alarm notification will no longer be received after DND mode is enabled.
+	Tap to add more devices.
📶	Wi-Fi intensity.
🔋	Battery status. 🔋✓: The battery is fully charged. 🟩: The battery has a lot of electricity. 🟧: The battery has moderate electricity. 🟥: The battery has insufficient electricity. ❗: Battery query error. !: The battery is offline. ⚡: The Battery is charging. 🔌: The hub is charging with power adapter.
+	Tap to add more accessories.
···	More settings.

3.3 Pairing with Accessories

You can add multiple detectors, sirens, door contacts and other wireless devices. Take door contact for example.

Step 1 On the **Device** interface, tap + in the upper right corner, scan QR code at the bottom of door contact, and select the device you want to connect. See Figure 3-21.

Figure 3-21 Select hub



China Telecom
China Mobile
59% 8:59 AM

Device

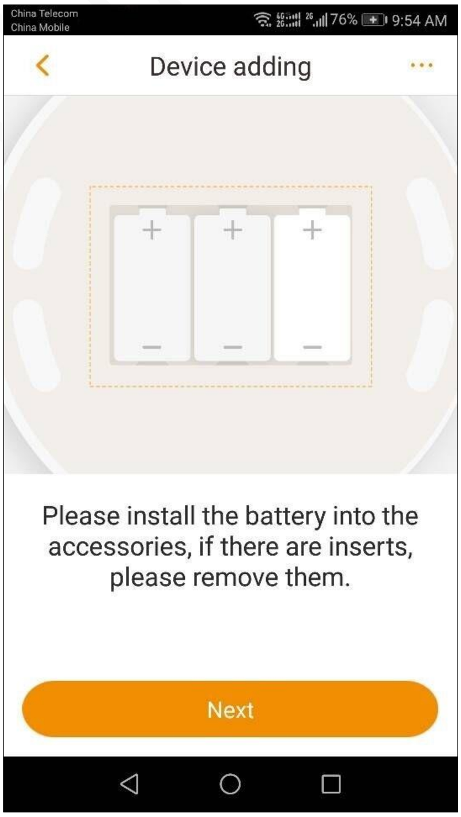
H1G-197B

No accessory temporarily. Please click "+" and add accessory.

Step 2 Tap **Next**.

According to the interface prompts, insert one battery into battery compartment of door contact, and ensure its electrodes are correct. See Figure 3-22.

Figure 3-22 Insert battery



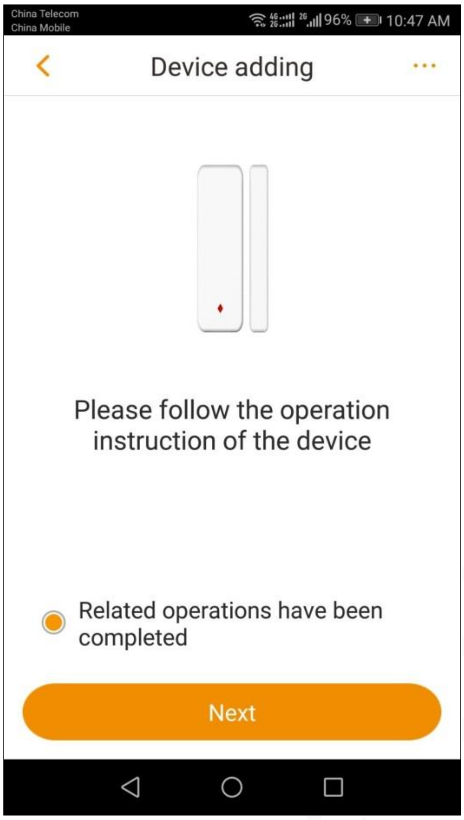
China Telecom
China Mobile
76% 9:54 AM

Device adding

Please install the battery into the accessories, if there are inserts, please remove them.

Step 3 Follow the operation instruction. See Figure 3-23.

Figure 3-23 Operation



Device adding

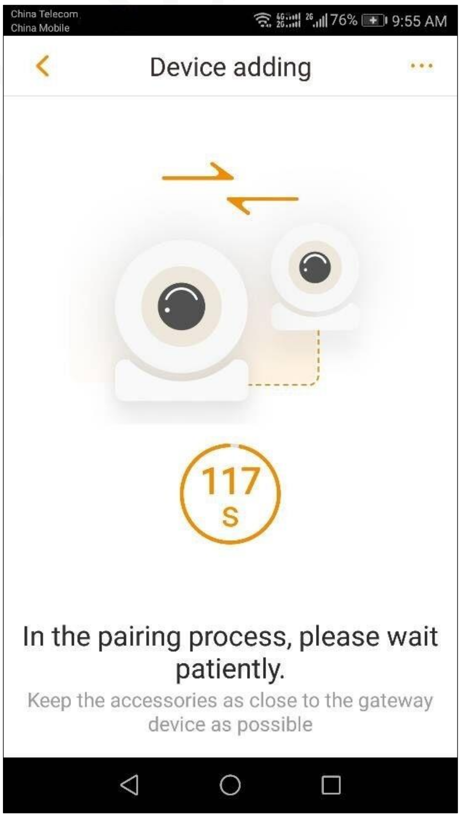
Please follow the operation instruction of the device

○ Related operations have been completed

Next

Step 4 Tick the confirmation that “Related operations have been completed”, and then tap **Next**. The pairing process is going on. See Figure 3-24.

Figure 3-24 Pairing process



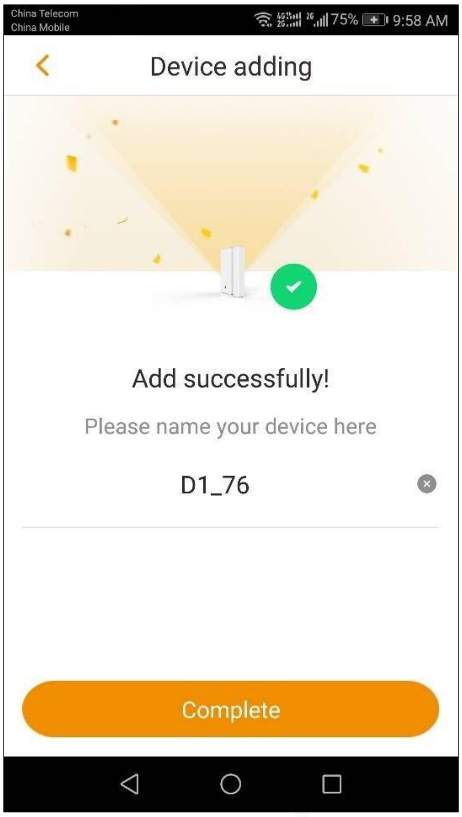
Device adding

In the pairing process, please wait patiently.

Keep the accessories as close to the gateway device as possible

Step 5 After several seconds, the door contact is added successfully. See Figure 3-25. You can name your device on the interface.

Figure 3-25 Add successfully



China Telecom
China Mobile
75% 9:58 AM

Device adding

Add successfully!

Please name your device here

D1_76

Complete

Step 6 Tap **Complete**.

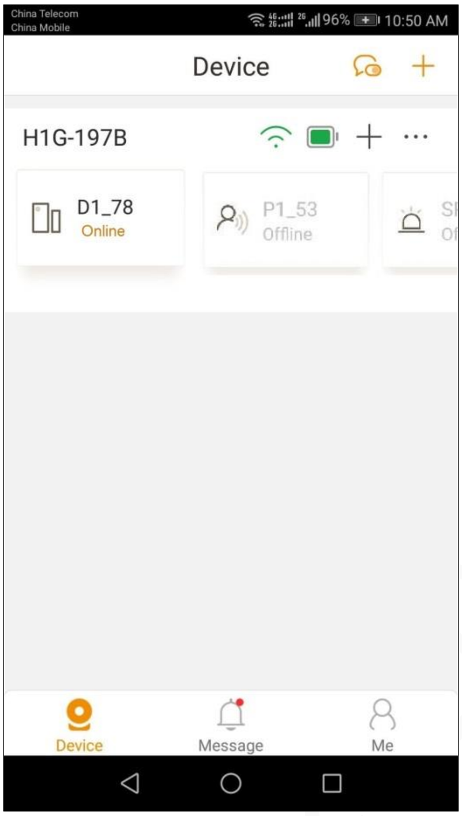
3.4 Arming the Door Contact

After the door contact is added to arming mode, an alarm will be triggered only in armed status.

Step 1 Tap App icon on your mobile phone, and start the App.

The **Device** interface is displayed. See Figure 3-26.

Figure 3-26 Added Device



Step 2 Tap ••• .

Accessory list is displayed. See Figure 3-27.

Figure 3-27 Accessory

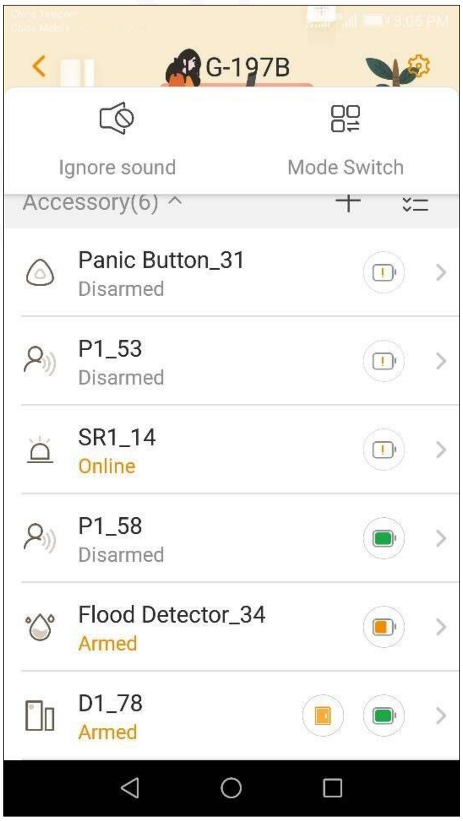


Table 3-2 Opening status description

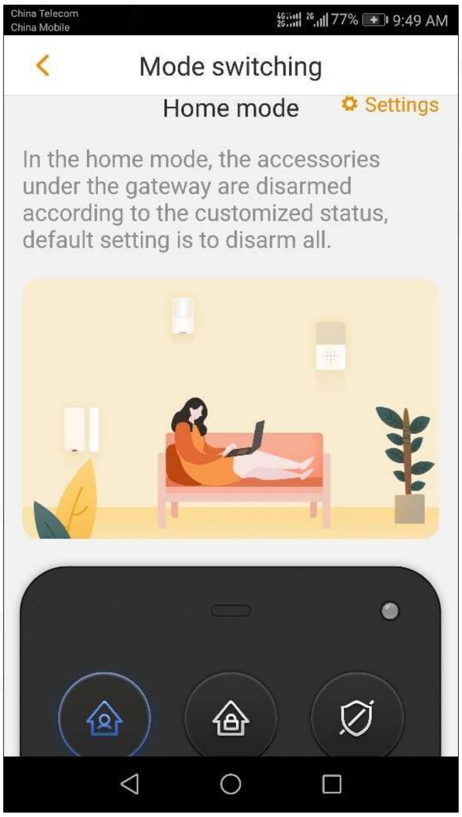
Icon	Description

Icon	Description
🚪	The door is open.
🚪	The door is closed.
!	Offline and unknown status.
!	Query error.

Step 3 Tap **Mode Switch** on the interface.

Switch the mode according to your needs. See Figure 3-28, Figure 3-29 and Figure 3-30.

Figure 3-28 Home mode



China Telecom
China Mobile
77% 9:49 AM

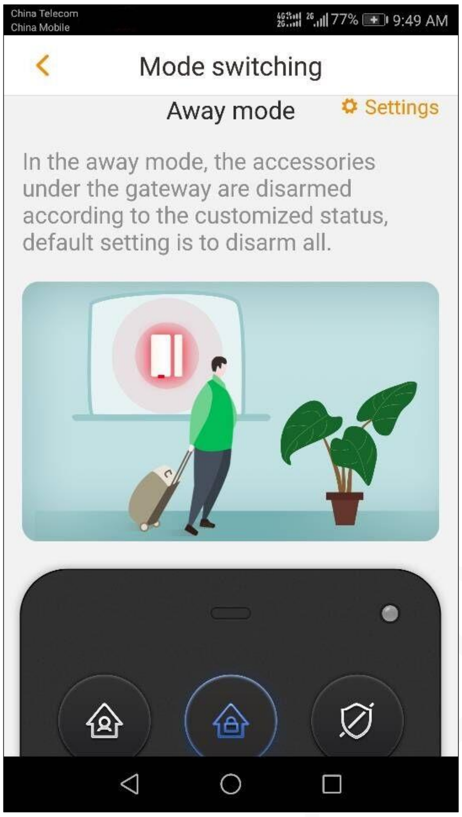
Mode switching

Home mode

Settings

In the home mode, the accessories under the gateway are disarmed according to the customized status, default setting is to disarm all.

Figure 3-29 Away mode



China Telecom
China Mobile
77% 9:49 AM

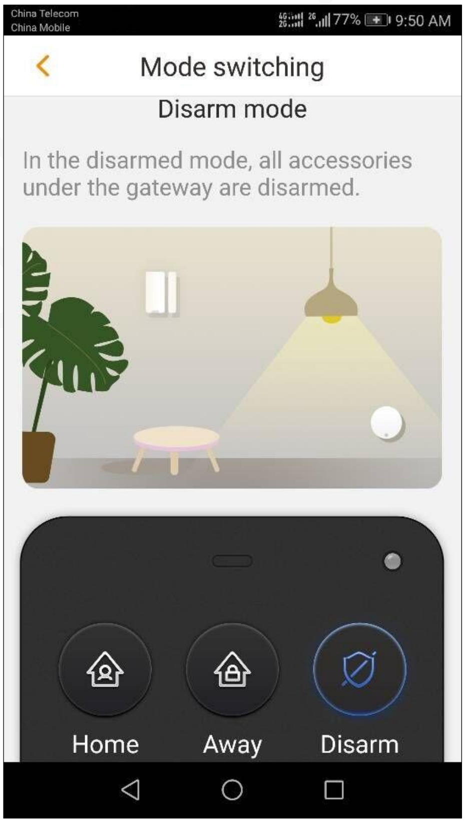
Mode switching

Away mode

Settings

In the away mode, the accessories under the gateway are disarmed according to the customized status, default setting is to disarm all.

Figure 3-30 Disarm mode



China Telecom
China Mobile
77% 9:50 AM

Mode switching

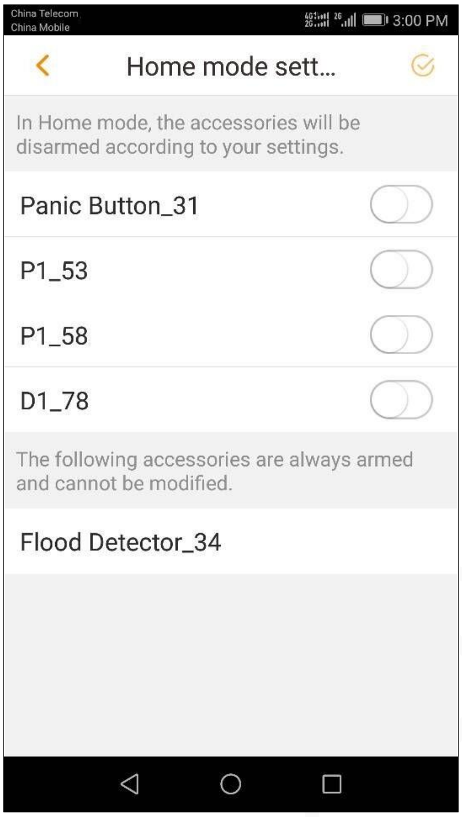
Disarm mode

In the disarmed mode, all accessories under the gateway are disarmed.

Step 4 (Optional) Tap **Settings** in Figure 3-28 home mode.

Home mode setting interface is displayed. See Figure 3-31.

Figure 3-31 Home mode setting



Home mode sett...

In Home mode, the accessories will be disarmed according to your settings.

Panic Button_31 ○

P1_53 ○

P1_58 ○

D1_78 ○

The following accessories are always armed and cannot be modified.

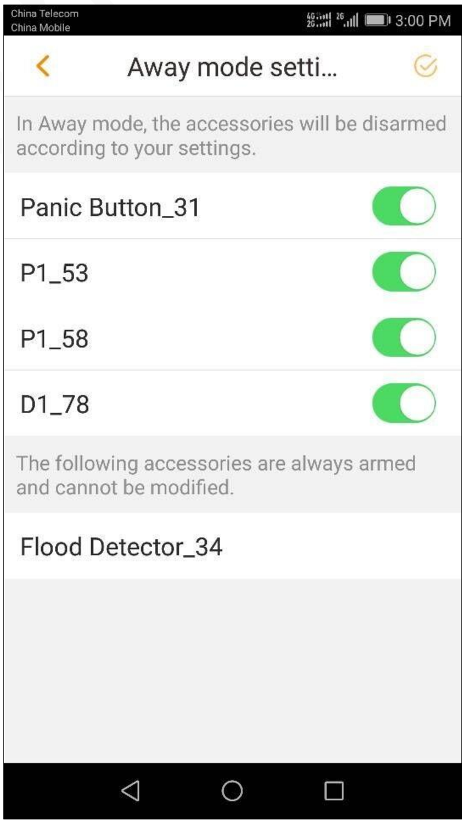
Flood Detector_34

The accessory is disarmed by default in home mode. Tap ○ to arm the accessory.

Step 5 (Optional) Tap **Settings** in Figure 3-29 away mode.

Away mode setting interface is displayed. See Figure 3-32.

Figure 3-32 Away mode setting



Away mode setti...

In Away mode, the accessories will be disarmed according to your settings.

Panic Button_31 ●

P1_53 ●

P1_58 ●

D1_78 ●

The following accessories are always armed and cannot be modified.

Flood Detector_34

The accessory is armed by default in away mode. Tap to disarm the accessory.

Step 6 (Optional) Tap Disarm to disarm all accessories, except 24H alarm devices, such as flood detector and so on.

3.5 Configuration Details

3.5.1 Device Details

Step 1 Tap App icon on your mobile phone, and start the App.

The **Device** interface is displayed. See Figure 3-33.

Figure 3-33 Device

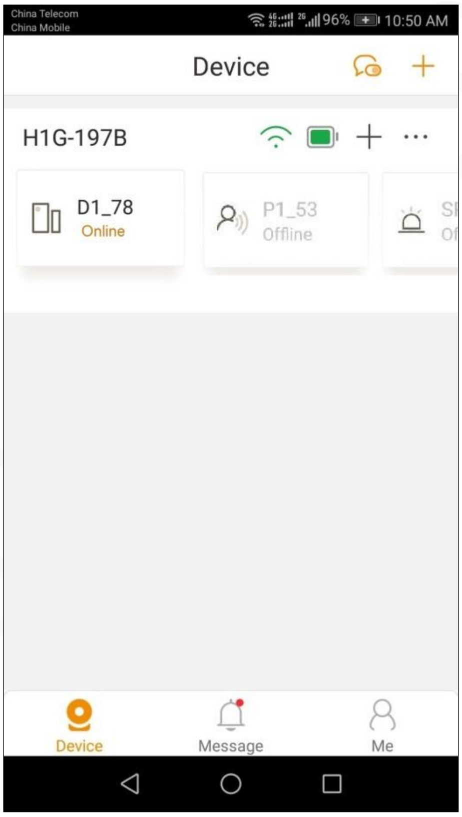


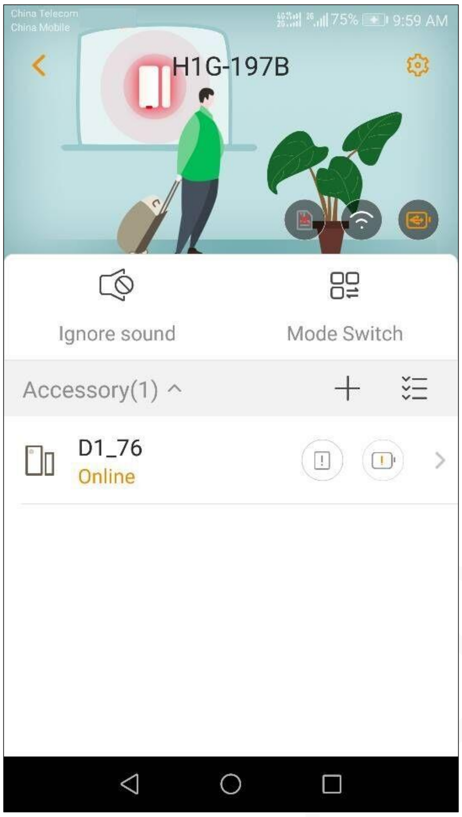
Table 3-3 Accessory status description

Status	Description
Online	The accessory is online and working.
Offline	The accessory is offline and not working.
Armed	The accessory is armed. It will give an alarm when necessary.
Disarmed	The accessory is disarmed. It will not give an alarm.

Step 2 Tap ··· .

Accessory list is displayed. See Figure 3-34.

Figure 3-34 Accessory



H1G-197B

Ignore sound

Mode Switch

Accessory(1)

D1_76

Online

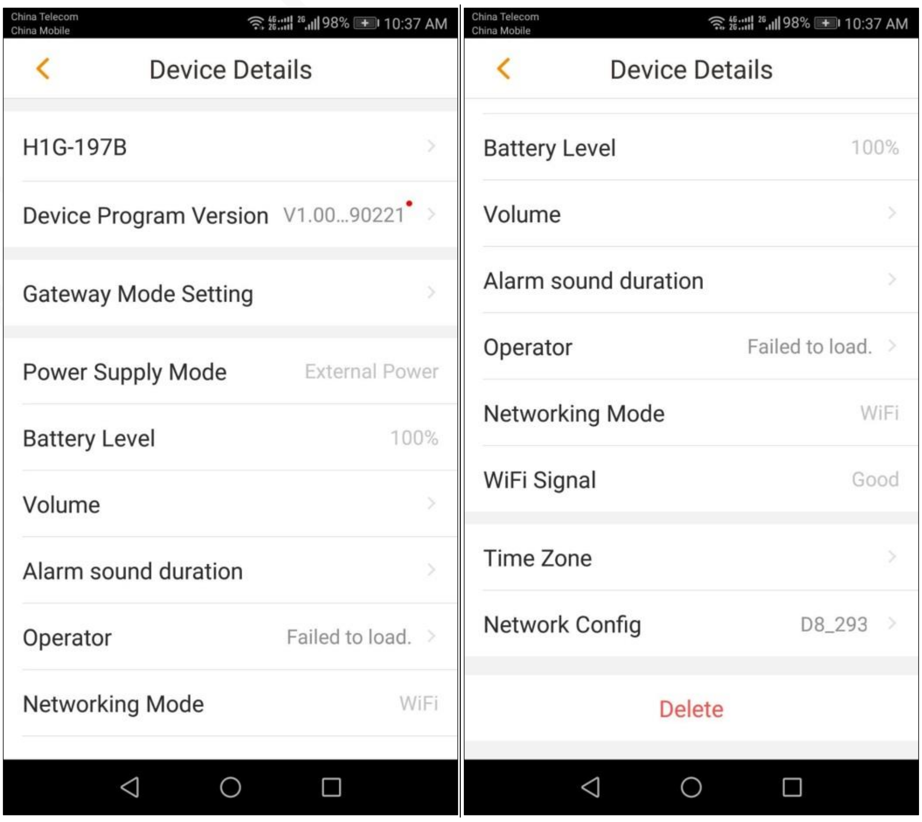
📖

In case of alarm, you can tap **Ignore Sound** to stop the alarm sound.

Step 3 Tap ⚙ in the upper right corner.

Device Details interface is displayed. See Figure 3-35.

Figure 3-35 Device details



Device Details

H1G-197B

Device Program Version V1.00...90221

Gateway Mode Setting

Power Supply Mode External Power

Battery Level 100%

Volume

Alarm sound duration

Operator Failed to load.

Networking Mode WiFi

Device Details

Battery Level 100%

Volume

Alarm sound duration

Operator Failed to load.

Networking Mode WiFi

WiFi Signal Good

Time Zone

Network Config D8_293

Delete

Table 3-4 Description

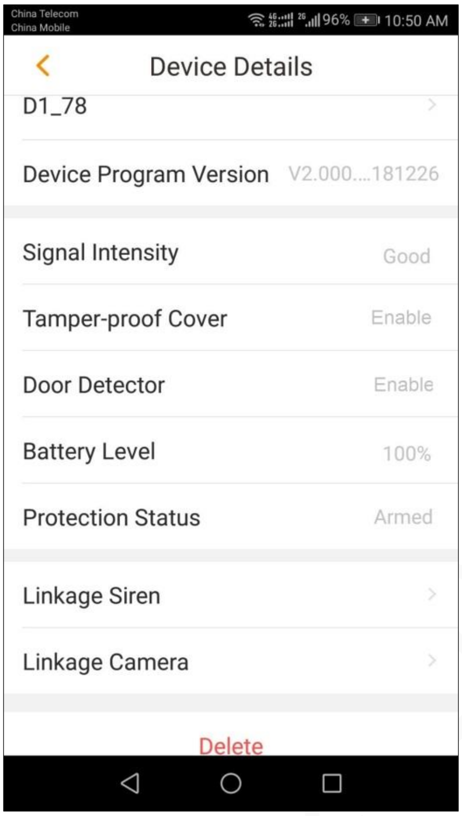
Parameter	Description
Device Program Version	Show the device program version.
Gateway Mode Setting	Tap to switch mode. Refer to “3.4 Arming the Door Contact”.
Power Supply Mode	It includes external power and battery.
Battery Level	Show remaining electricity of the battery.
Volume	You can configure volume to be **Loud**, **Low** and **Mute**.
Alarm sound duration	The alarm sound duration can be from 30 s to 180 s.
Operator	Tap to view signal intensity, operator setting and contact person number. Maximum 8 contact person numbers can be configured. In case of alarm, a message will be sent to all the configured contact person numbers. For operator settings, please contact your operator.
Networking Mode	Show the networking mode, including Wi-Fi, wired network and 2G/4G card.
Wi-Fi Signal	Show the status of Wi-Fi signal.
Time Zone	Tap to select your time zone, and enable DST (daylight saving time) if necessary.
Network Config	Show your present Wi-Fi name. Tap to connect another network.
Delete	Tap **Delete** to delete the device.

3.5.2 Accessory Details

Step 1 Tap › in the line of accessory name as shown in Figure 3-34.

Device Details interface is displayed. See Figure 3-36 and Table 3-5.

Figure 3-36 Device details



China Telecom
China Mobile
96% 10:50 AM

Device Details

D1_78

Device Program Version V2.000....181226

Signal Intensity Good

Tamper-proof Cover Enable

Door Detector Enable

Battery Level 100%

Protection Status Armed

Linkage Siren

Linkage Camera

Delete

Table 3-5 Description

Parameter	Description
Device Program Version	Show the device program version.
Signal Intensity	Show the signal intensity.
Tamper-proof Cover	If tamper-proof cover is enabled, the hub gives an alarm when the tamper-proof cover is moved.
Door Detector	If door detector is enabled, the hub gives an alarm when the door detector is opened.
Battery Level	Show remaining electricity of the battery.
Protection Status	Show protection status, including **Armed** and **Disarmed**.
Linkage Siren	Tap **Linkage Siren**, and then tap ◯ on the interface to enable it. It will activate all the sirens of main device connected to the accessory.
Linkage Camera	Tap **Linkage Camera**, and then tap ◯ on the interface to enable it. The video image of linkage device will be pushed after being enabled.
Delete	Tap **Delete** to delete the device.

3.6 Configuring Network

The hub supports three network connection modes, including 2G/4G, Wi-Fi and wired network. Their priority is wired network > Wi-Fi > 2G/4G.

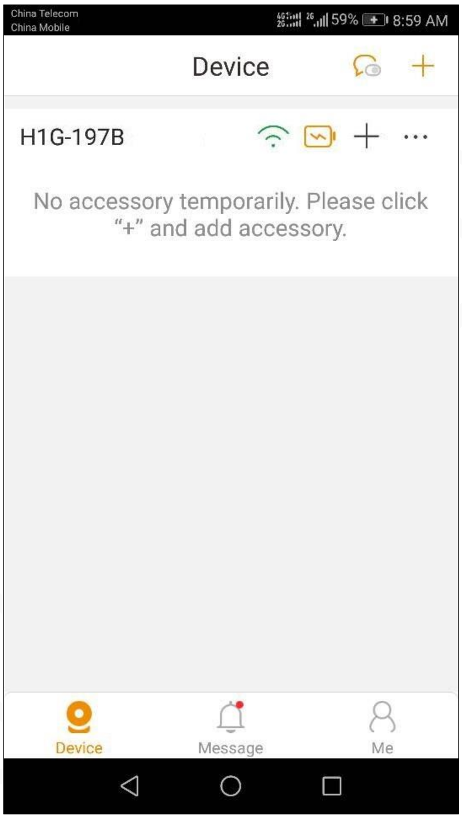
- If there is wired network, and the router distributes IP automatically, the hub gets IP automatically and uses wired network.
- If there is no wired network and there is Wi-Fi, the hub uses Wi-Fi.
- If there is no wired network and Wi-Fi, and 2G/4G card is inserted into the hub, the hub uses 2G/4G network.

This following configuration is valid only when the hub is offline. When the hub is online, you can search nearby Wi-Fi information, and switch Wi-Fi.

Step 1 Tap App icon on your mobile phone, and start the App.

The **Device** interface is displayed. See Figure 3-37.

Figure 3-37 Added device



China Telecom
China Mobile
59% 8:59 AM

Device

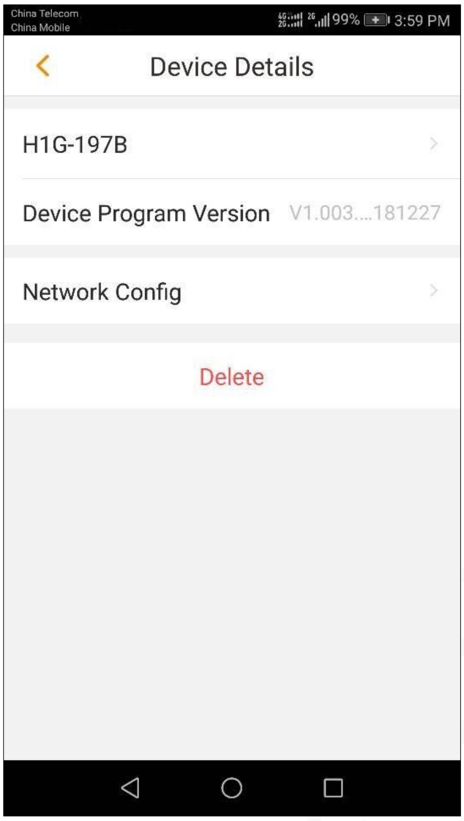
H1G-197B

No accessory temporarily. Please click "+" and add accessory.

Step 2 Tap ⋯ , and then tap ⚙ in the upper right corner of pop-up interface.

The **Device Details** interface is displayed. See Figure 3-38.

Figure 3-38 Device details


China Telecom
China Mobile
99% 3:59 PM

Device Details

H1G-197B

Device Program Version V1.003....181227

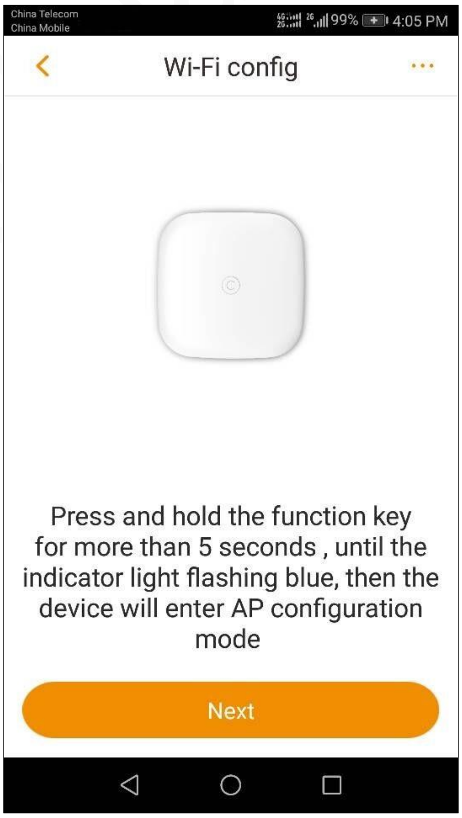
Network Config

Delete

Step 3 Tap **Network Config**.

The **Wi-Fi config** interface is displayed. See Figure 3-39.

Figure 3-39 Wi-Fi config


China Telecom
China Mobile
99% 4:05 PM

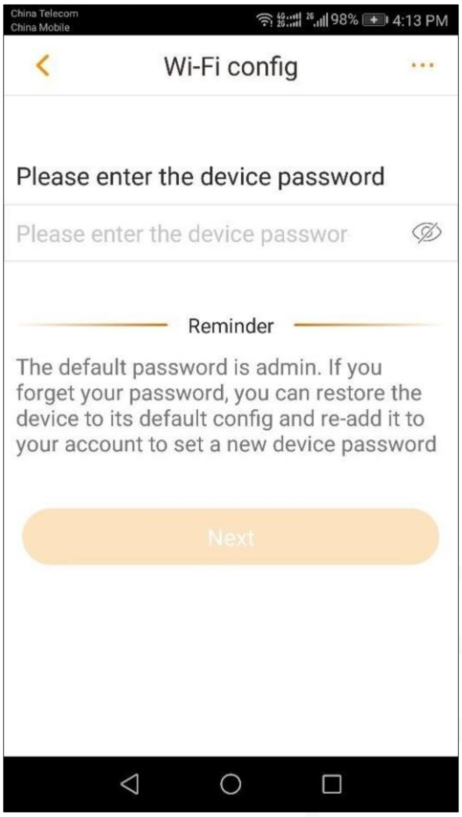
Wi-Fi config

Press and hold the function key for more than 5 seconds , until the indicator light flashing blue, then the device will enter AP configuration mode

Next

Step 4 On the APP interface, tap **Next**. Enter the device password on the pop-up interface. See Figure 3-40.

Figure 3-40 Wi-Fi config—Enter device password



Please enter the device password

Please enter the device passwor

Reminder

The default password is admin. If you forget your password, you can restore the device to its default config and re-add it to your account to set a new device password

Step 5 After entering password, tap **Next**.

Select Wi-Fi network, and enter Wi-Fi password according to interface prompts.

3.7 Deleting the Door Contact

- Method 1: In APP, check accessory details and delete according to prompts.
- Method 2: Press RESET key for 6s when the power is on, restart the hub and restore factory default settings if there is slow pulse red indicator light. All set information has been cleared.

4 FAQ

1. Wireless alarm hub cannot be booted normally.

Solution: Check input power of the hub (including adapter and USB cable).

2. Accessory pairing fails.

Solution:

- Check if electric amount of accessory battery is sufficient.
- Check if the accessory has connected with other hubs. If so, clear configuration and try pairing again.
- Check if the accessory is too far away from the hub and beyond effective distance. Move the detector closer and try pairing again.

3. Accessory is triggered without any response.

Solution:

- Check if electric quantity of accessory battery is sufficient.
- Check if the accessory has been added to arm mode.
- Check if the hub is armed.
- Check if cables of the accessory drop off.
- Check if the accessory exceeds detection scope.

4. Mobile phone client doesn’t receive messages after an alarm is triggered.

Solution:

- Check if network connection of the hub or router is normal.
- Check if alarm subscription of APP is enabled.

5. The accessory goes offline frequently.

Solution:

- Check if the hub or accessory is power-off frequently.
- Check if the hub network is normal.
- Check if the accessory is too far away from the hub and at the critical state of communication.

Appendix 1 Technical Parameters

Appendix table 1-1 Technical parameters

Parameter	Description
Main Processor	MTK7688AN
Wireless Defense Zone	32 channels
Siren Connection	4 sirens
Remote Control	8 remote controls
2G/4G	Support alarm short message function; support mobile data connection.
Wired Network	1-channel 10/100M Ethernet, RJ–45 port
Standby Power Supply	CR18650 battery, 2150 mAh
Supply Voltage	DC5V 2A
Power Consumption	< 10W
Working Temperature	-10 °C to 55 °C
Dimension	125 × 125 × 37.9 mm
Net Weight of Whole Device	0.25 Kg
Installation	Wall-mounted

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.
Address: No.1199, Bin'an Road, Binjiang District, Hangzhou, P.R. China
Postcode: 310053
Tel: +86-571-87688883
Fax: +86-571-87688815
Email: overseas@dahuatech.com
Website: www.dahuasecurity.com