

# DS11 Wireless Chime

User's Manual

**V1.0.0**

# 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.

## FCC Information



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

### **FCC conditions:**

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operation.

### **FCC compliance:**

This equipment has been tested and found to comply with the limits for a digital device, pursuant to part 15 of the FCC Rules. This equipment generate, uses and can radiate radio frequency energy and, if not installed and used in accordance with the guide, may cause harmful interference to radio communication.

- For class A device, these limits are designed to provide reasonable protection against harmful interference in a commercial environment. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.
- For class B device, these limits are designed to provide reasonable protection against harmful interference in a residential installation. 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.

## General

This document elaborates introduction, installation, device adding and FAQ of wireless chime.

## Model






DS11

## Operation Definition

Italic Content	Note
<i>Device Name</i>	It represents modifiable parameter name. Specific contents are different depending on settings. Default device name is its serial number and default channel name is Channel 1.
<i>Channel Name</i>	

## Safety Instructions

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

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	2018.3.30

## 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 include but not limited to: providing clear and visible identification to inform data subject the existence of surveillance area and providing related contact.

## About the Manual

- The Manual is for reference only. If there is inconsistency between the Manual 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 Manual.
- The Manual would be updated according to the latest laws and regulations of related regions. For detailed information, see the paper User's Manual, CD-ROM, QR code or our official website. If there is inconsistency between paper 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 Manual. 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 Manual 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 manual carefully before use, in order to prevent danger and property loss. Strictly conform to the manual during application and keep it properly after reading.

## Operating Requirement

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

## Power Requirement

- The product shall use electric cables (power cables) recommended by this area, which shall be used within its rated specification.
- Please use standard power adapter supplied with this device; otherwise, resulting personal injury or device damage shall be borne by the user.
- Please 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; please keep its convenient operation during use.

# Table of Contents

<b>Cybersecurity Recommendations</b> .....	<b>I</b>
<b>Regulatory Information</b> .....	<b>III</b>
<b>Foreword</b> .....	<b>IV</b>
<b>Important Safeguards and Warnings</b> .....	<b>VI</b>
<b>1 Packing List</b> .....	<b>1</b>
<b>2 Device Introduction</b> .....	<b>2</b>
2.1 Front Panel .....	2
2.1.1 State Description of Indicator Light .....	2
2.1.2 Description of Button .....	2
2.2 Rear Panel .....	3
2.3 Side Panel.....	3
<b>3 Get Started</b> .....	<b>4</b>
3.1 Download Lechange Client .....	4
3.2 Add Device .....	4
3.3 Link Chime.....	11
3.4 Ring Setup .....	13
3.5 Doorbell Call .....	15
<b>4 APP Operation</b> .....	<b>16</b>
4.1 Modify Device Info .....	16
4.2 Volume.....	17
4.3 View Linked Doorbell.....	17
4.4 Cloud Update.....	18
4.5 Wi-Fi Config.....	19
4.6 Delete Device .....	21
<b>5 FAQ</b> .....	<b>22</b>
<b>Appendix 1 Technical Parameter</b> .....	<b>23</b>



# 1

## Packing List

- Check whether device appearance shows obvious damages.
- Check whether all accessories are supplied. Packing list is as follows:
  - ◇ Wireless chime
  - ◇ User's manual
  - ◇ Installation accessories package

## 2.1 Front Panel

Front panel includes loudspeaker, indicator light and call button, as shown in Figure 2-1.

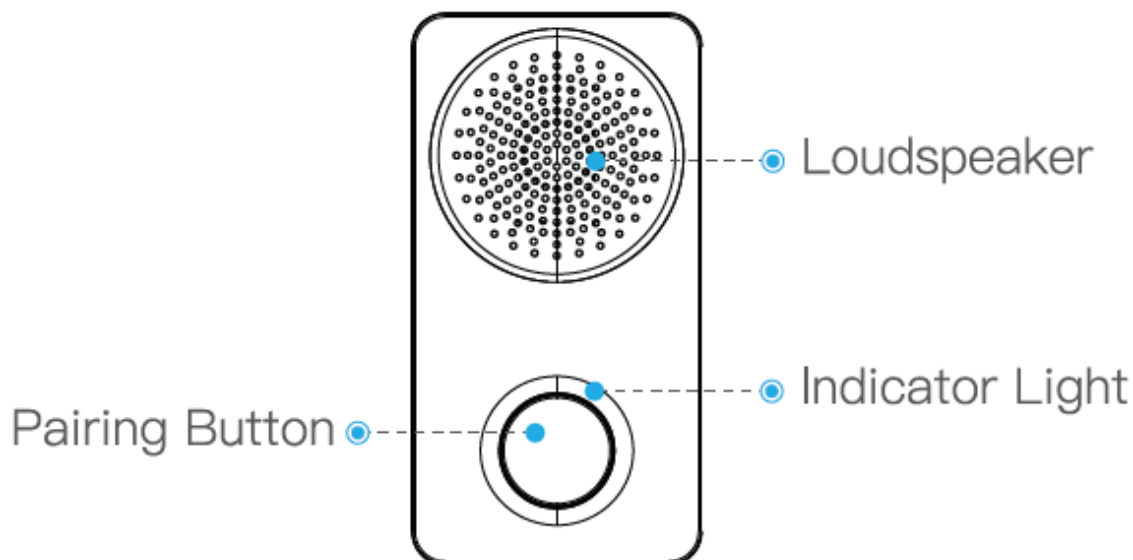


Figure 2-1

### 2.1.1 State Description of Indicator Light

State description of indicator light is shown in Table 2-1.



State	Icon	Description
Blue Flashing		<ul style="list-style-type: none"> <li>• Wireless router is not connected;</li> <li>• Cloud service is not connected;</li> <li>• Enable hotspot.</li> </ul>
Blue Solid		Cloud service is connected successfully.


Table 2-1

### 2.1.2 Description of Button

Long press the button for 5s to enter pairing mode.

## 2.2 Rear Panel

Rear panel includes power plug and switch, as shown in Figure 2-2.

 Note

Power plug of the device varies depending on your local security requirements and relevant standards. Please refer to actual model.

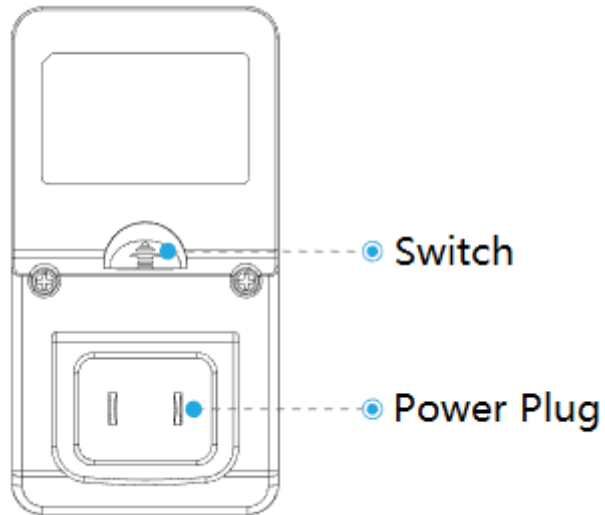


Figure 2-2

## 2.3 Side Panel

Reset hole on the side panel is used to restore factory defaults, as shown in Figure 2-3.

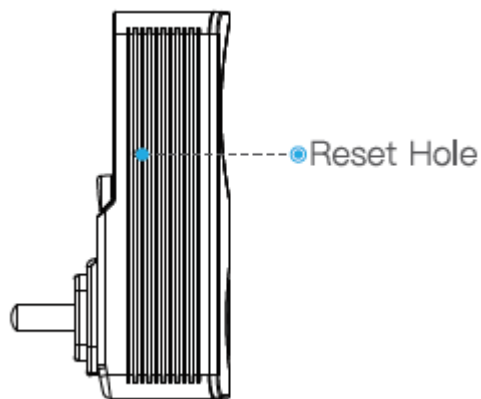


Figure 2-3

## 3.1 Download Lechange Client

Please ensure that your smartphone has connected with Wi-Fi. Scan QR code below, or search “Lechange” in APP market, download and log onto APP client. For specific operation, please refer to relevant Lechange user’s manual.



Figure 3-1



Note

This document takes iOS system as an example and explains operations.

## 3.2 Add Device

- Step 1 At device list interface, press + to enter “QR Code Scanning” interface.
- Step 2 Scan QR code to get the SN, or you can also manually enter the SN on the next page. The system reminds you to enable device hotspot, as shown in Figure 3-2.



Note

Scan QR code to obtain serial number, and it will display serial number confirmation interface. Press [Next] to enter the interface as shown in Figure 3-2.



Figure 3-2

- Step 3 Connect power socket, and press reset button (pinhole) at the side of the device. If the chime beeps and blue indicator light flashes, it means that the device hotspot has been enabled.

 TIPS

Long press the button in the front of the device for 5s, and the hotspot can be enabled too.

- Step 4 At APP interface, press [Next].  
The system displays “Connect device hotspot” interface, as shown in Figure 3-3.

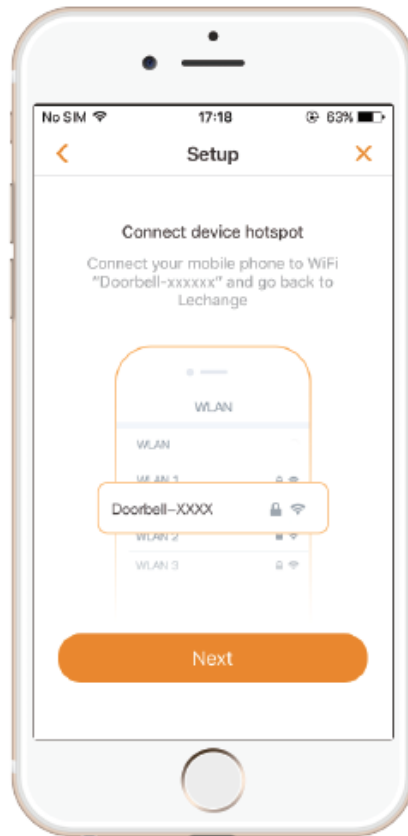


Figure 3-3

Step 5 Connect your smartphone with hotspot. Hotspot Wi-Fi name is Doorbell-device serial number.



Figure 3-4

Step 6 At APP interface, press [Next].

The system displays device password setting interface, as shown in Figure 3-5.

 Note

If this device is not used for the first time, the interface is to enter device password, rather than setting the password, as shown in Figure 3-6.

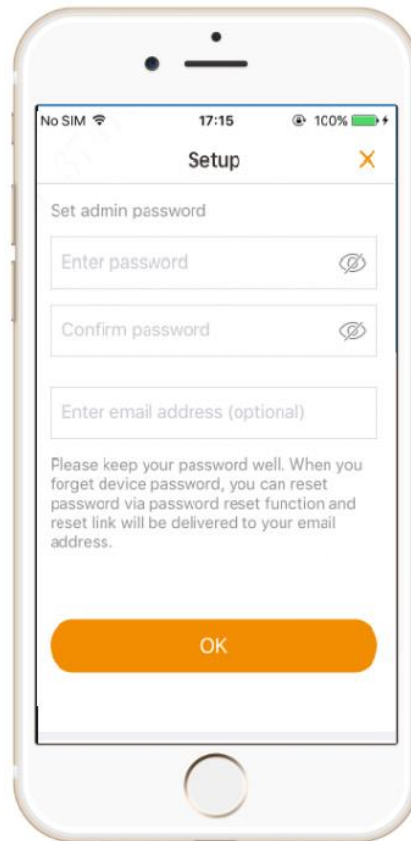


Figure 3-5

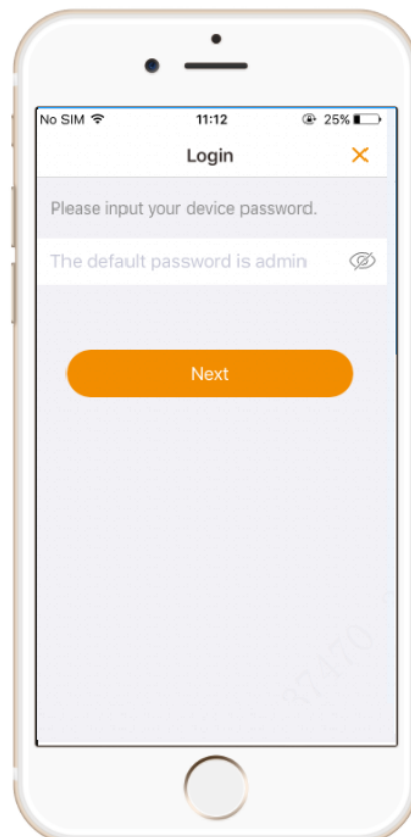


Figure 3-6

Step 7 Set device password and email, and press [Next].

The system displays available Wi-Fi list, as shown in Figure 3-7.

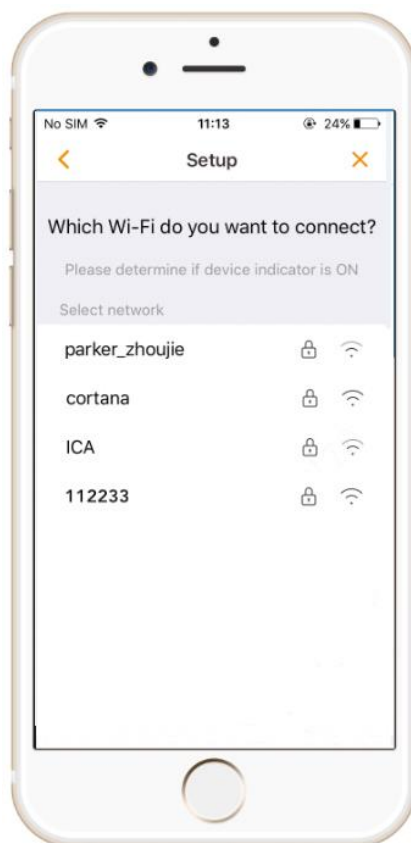


Figure 3-7

Step 8 Choose the Wi-Fi network to be connected.

The system displays Wi-Fi connection interface, as shown in Figure 3-8.



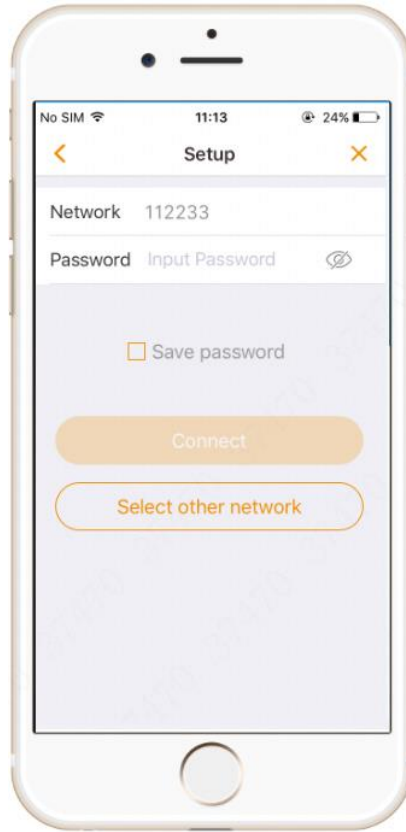


Figure 3-8

Step 9 Input Wi-Fi network password and press [Connect].

The system displays indicator light judgment interface, as shown in Figure 3-9.

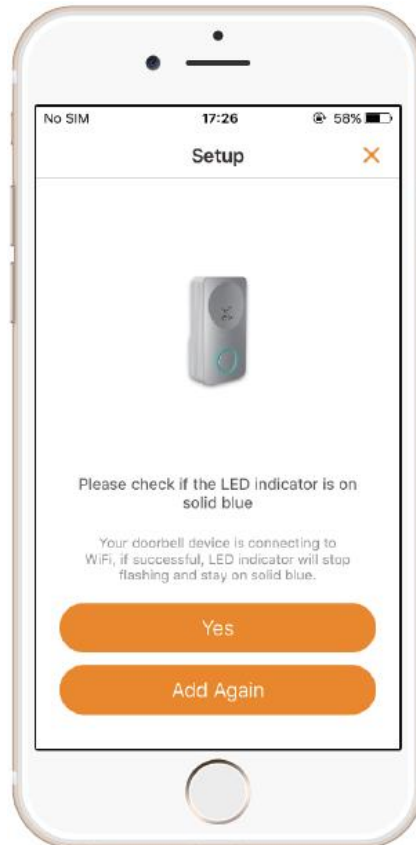


Figure 3-9

Step 10 Please check if device indicator light is blue ON.

- If the blue indicator light doesn't turn on, press [Add again], repeat above steps to add it again.
  - If blue light turns on, it means that the connection is successful.
1. Press [Yes] to add the device to APP.  
Start to add the device to APP, as shown in Figure 3-10. After adding it successfully, display a time zone setup interface, as shown in Figure 3-11.

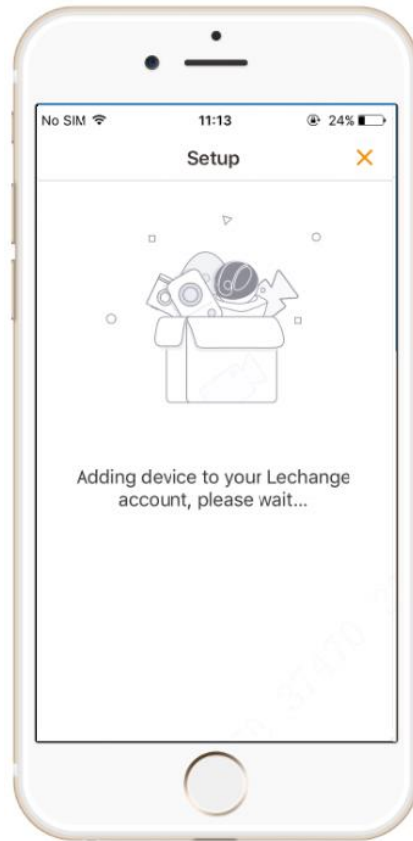


Figure 3-10

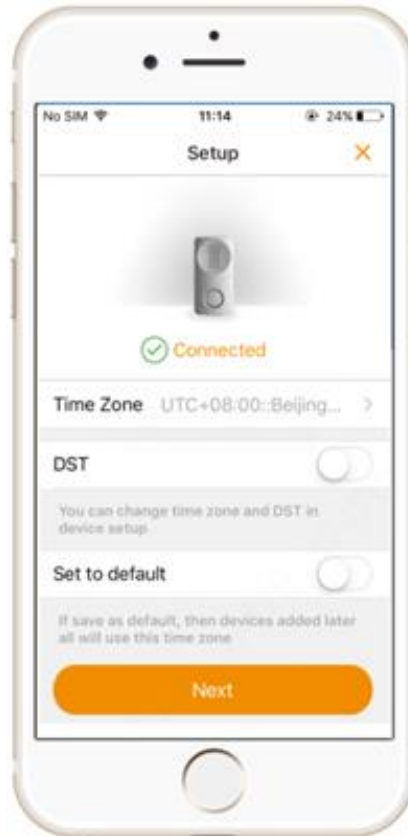


Figure 3-11

2. Set “Time Zone” and “DST”.
3. Press [Next] to enter real-time monitoring interface.

Step 11 Set the local time zone and press [Next] to complete adding.

### 3.3 Link Chime

Link the chime with doorbell.

Step 1 Select “Me > My Device > Device Name > Link Chime” or click  in device menu.

The system displays “Link Chime” interface, as shown in Figure 3-12.

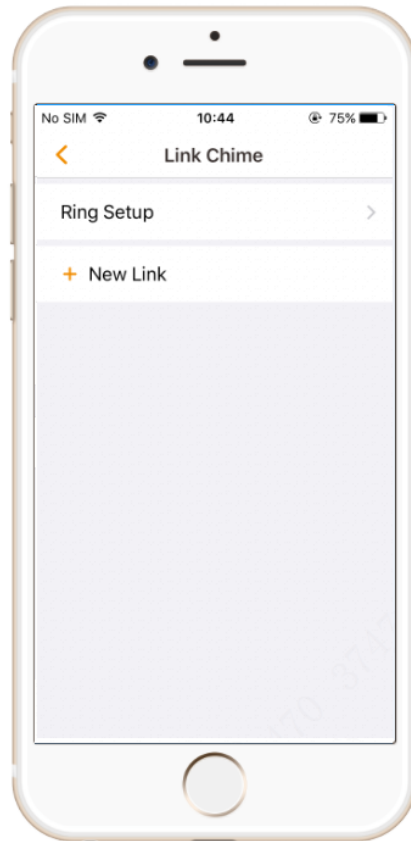


Figure 3-12

Step 2 Select "New Link".

The system displays wireless chime list, as shown in Figure 3-13.

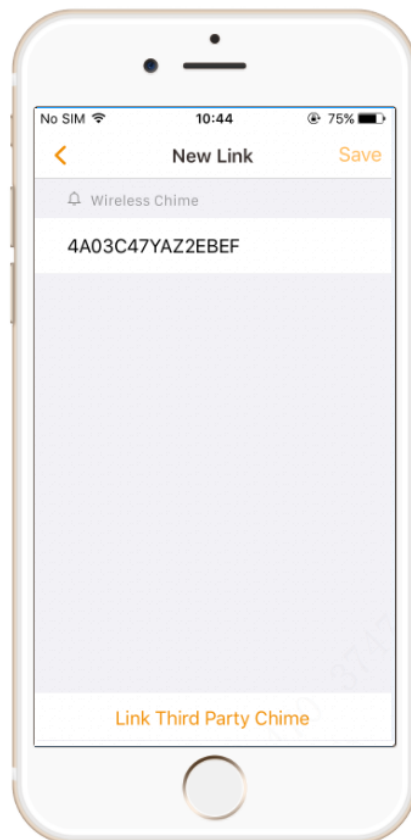


Figure 3-13

- To link wireless chime, select it from the list.

- To link third-party chime, press [Link Third Party Chime], and the system displays chime type selection interface, as shown in Figure 3-14. Select a type, press [OK], and the system will automatically read the connected chime info.

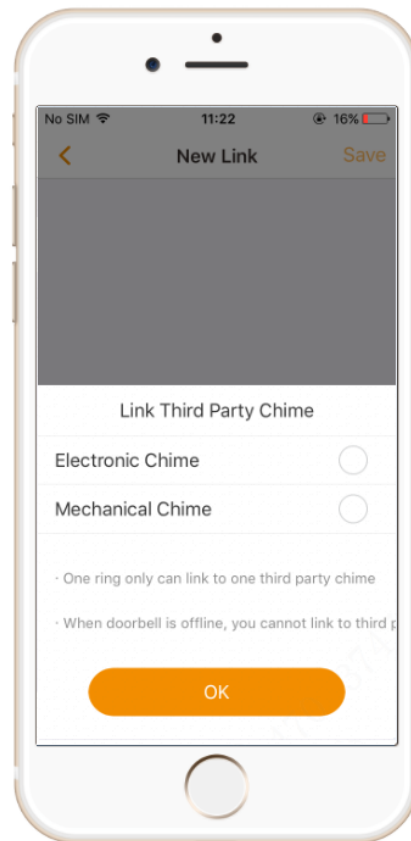


Figure 3-14

Step 3 Press [Save] to complete adding.

## 3.4 Ring Setup

Set the chime ring on the paired doorbell.

Step 1 Select “Me > My Device > Device Name > Link Chime” or click  in device menu.

The system displays “Link Chime” interface, as shown in Figure 3-15.

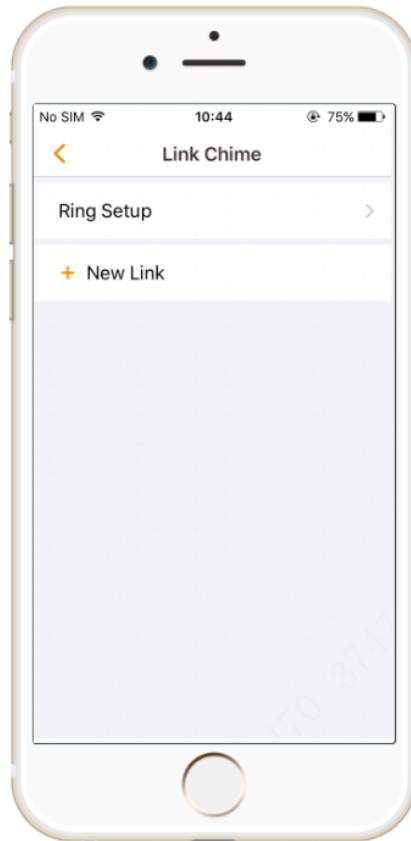


Figure 3-15

Step 2 Select “Ring Setup”.

The system displays ring list, as shown in Figure 3-16. A, B and C represent ring A, ring B and ring C.

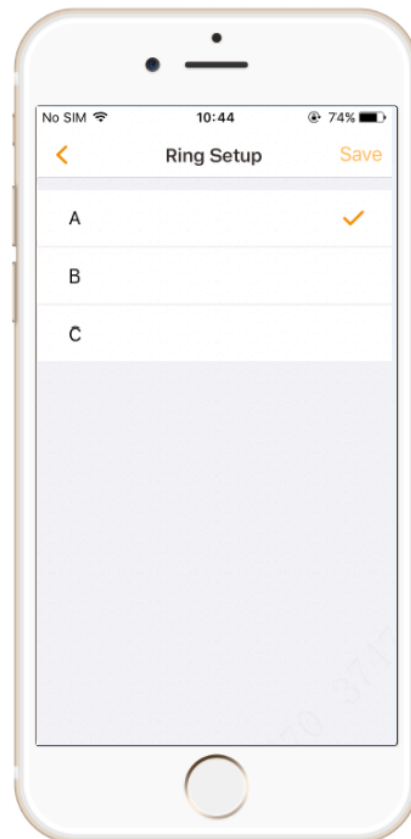


Figure 3-16

Step 3 Select a ring, and press [Save] to complete adding.

## 3.5 Doorbell Call

When someone presses call button on the doorbell to call, the chime rings and informs about the call.

# 4

## APP Operation

### 4.1 Modify Device Info

Modify device name and channel name; view its SN.

Step 1 Select “Me > My Device > Device Info”.

The system displays “Device Info” interface, as shown in Figure 4-1.

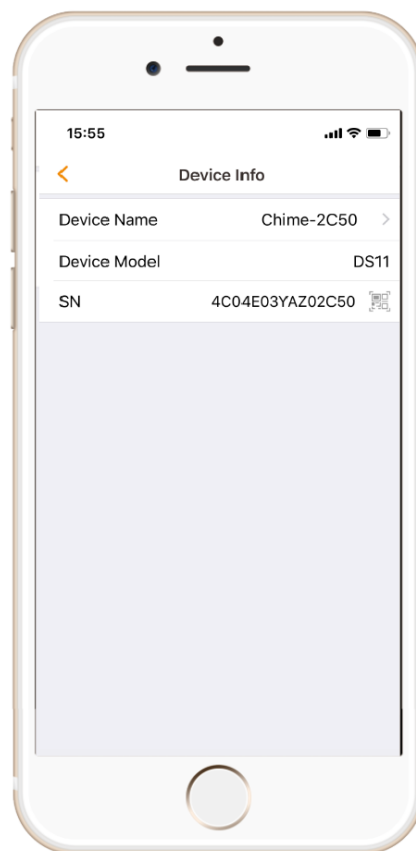




Figure 4-1

Step 2 Modify device name or view its QR code.

- Select “Device Name” to set chime name, and press  to save the setup.
- Press  to view QR code of the chime.

 Note

By default, “Device Name” is serial number of the device.



## 4.2 Volume

Set volume of the chime.

Modify device cover, device name and channel name; view device S.N. and set device password.

Step 1 Select “Me > My Device > Device Name > Device Info”.

The system displays “Volume” interface, as shown in Figure 4-2.

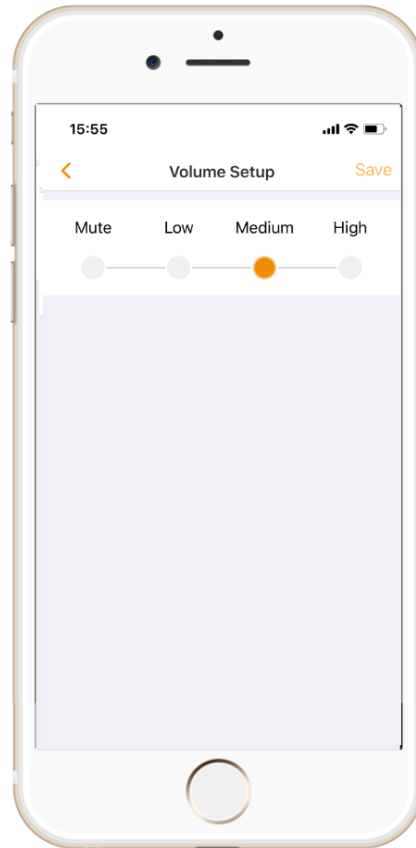


Figure 4-2

Step 2 Select the volume and press [Save].

## 4.3 View Linked Doorbell

View the doorbell that is linked with this chime.

Select “Me > My Device > Device Name > Linked Doorbell”. The system displays “Linked Doorbell” interface, as shown in Figure 4-3. All linked doorbell info is displayed.



Figure 4-3

## 4.4 Cloud Update

After entering the update interface, update the device to the latest version.

Step 1 Select “Me > My Device > Device Name > Cloud Update”.

The system displays “Update” interface, as shown in Figure 4-4.

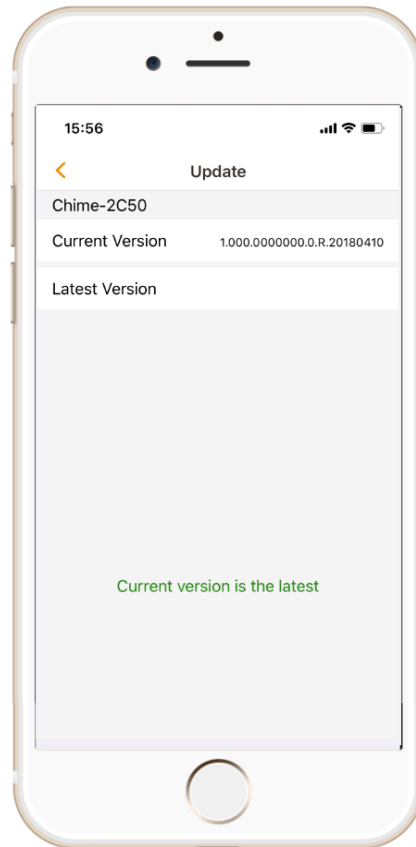


Figure 4-4

Step 2 Press [Update].

Update the device according to interface prompt. The device reboots automatically after successful update.

## 4.5 Wi-Fi Config

Modify Wi-Fi config of the device, in order to connect with other Wi-Fi networks.

Step 1 Select "Me > My Device > Device Name > Wi-Fi Config".

The system displays "Wi-Fi Config" interface, as shown in Figure 4-5.

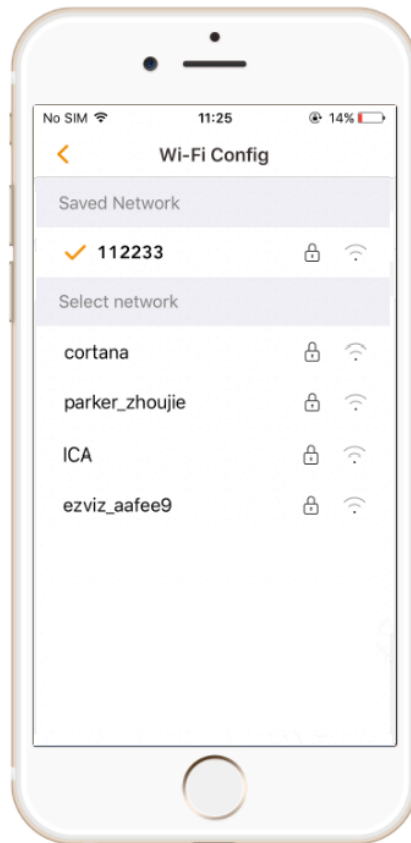


Figure 4-5

Step 2 Select new Wi-Fi and enter the password.

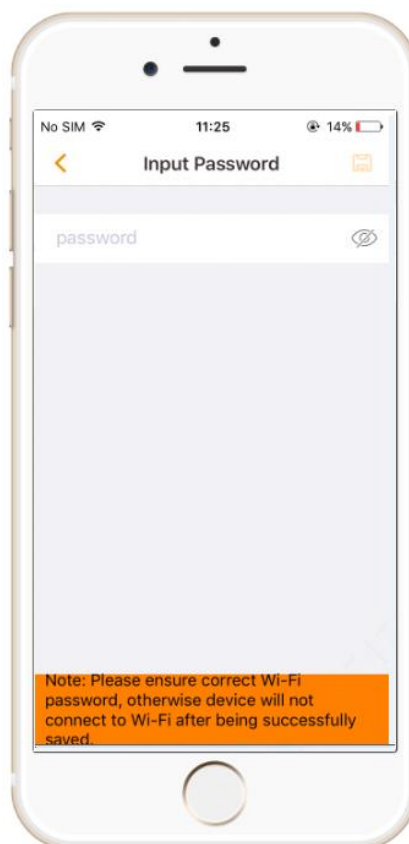



Figure 4-6

Step 3 Press  to connect new Wi-Fi network.

## 4.6 Delete Device

Select “Me > My Device > Device Name > Delete Device”, press [Delete], so as to unbind the device.

### **Question 1**

Q: How to restore factory settings?

A: Please press Reset Button on the side panel of the device for 10s. Blue light will be on for 3s and then turn off; the device will reboot automatically and restore factory default settings.

### **Question 2**

Q: The device cannot work normally?

A: Please restore factory settings, and configure the device again.

### **Question 3**

Q: How to enter wireless config mode?

A: Short press Reset Button at the side panel of the device, until the indicator light turns to be green flashing light, it means that the hotspot has been enabled.

### **Question 4**

Q: The device is not online?

A: Please check the state of device indicator light. If blue light flickers all the time, it means that the device fails to connect the network. Please check whether wireless router can connect the network; connect your smartphone with this wireless network to test it. If it can connect the network, please reset the device and configure again.

### **Question 5**

Q: Connection is overtime?

A: a. After the device has enabled hotspot, your smartphone doesn't connect the hotspot for a long time, and thus leads to overtime.

b. The device starts configuration without reminder of waiting to connect the network.

# Appendix 1 Technical Parameter

Parameter		Description
Audio	Output	Built-in loudspeaker, clear ring
	Ring	Switch built-in ring through Lechange
Network	Wi-Fi	1-channel, 802.11b/g/n, 2.4GHz frequency band
Man-machine interaction	Pairing button	At the side panel of the device
	State indicator light	Blue indicator light
Others	Power input	90Vac~240Vac
	Working environment	-10°C~+50°C, 20%RH~95%RH
	Dimension (length × width × height)	99mm×52mm×33.7mm
	Weight	0.2kg

Appendix Table 1-1