Wireless Panic Button

User's Manual

Foreword

General

This manual introduces the installation, functions and operations of the Wireless Panic Button (hereinafter referred to as the "button"). Read carefully before using the device, and keep the manual safe for future reference.

Model

DHI-ARD821-W2 (868); DHI-ARD821-W2

Safety Instructions

The following signal words 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, reductions in performance, or unpredictable results.
⊙━ **TIPS**	Provides methods to help you solve a problem or save time.
📖 **NOTE**	Provides additional information as a supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.0	First release.	March 2022

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, fingerprints, and license plate number. You need to be in compliance with your local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures which include but are not limited: Providing clear and visible identification to inform people of the existence of the surveillance area and provide required contact information.

About the Manual

- The manual is for reference only. Slight differences might be found between the manual and the product.
- We are not liable for losses incurred due to operating the product in ways that are not in compliance with the manual.

- The manual will be updated according to the latest laws and regulations of related jurisdictions. For detailed information, see the paper user's manual, use our CD-ROM, scan the QR code or visit our official website. The manual is for reference only. Slight differences might be found between the electronic version and the paper version.
- All designs and software are subject to change without prior written notice. Product updates might result in some differences appearing between the actual product and the manual. Please contact customer service for the latest program and supplementary documentation.
- There might be errors in the print or deviations in the description of the functions, operations and technical data. If there is any doubt or dispute, we reserve the right of final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and company names in the manual are properties of their respective owners.
- Please visit our website, contact the supplier or customer service if any problems occur while using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Important Safeguards and Warnings

This section introduces content covering the proper handling of the device, hazard protection, and protection of property damage. Read carefully before using the device, and comply with the guidelines when using it.

Operation Requirements

⚠

- Make sure that the power supply of the device works properly before use.
- Do not pull out the power cable of the device while it is powered on.
- Only use the device within the rated power range.
- Transport, use and store the device under allowed humidity and temperature conditions.
- Prevent liquids from splashing or dripping on the device. Make sure that there are no objects filled with liquid on top of the device to avoid liquids flowing into it.
- Do not disassemble the device.

Installation Requirements

⚠ WARNING

- Connect the device to the adapter before power on.
- Strictly abide by local electrical safety standards, and make sure that the voltage in the area is steady and conforms to the power requirements of the device.
- Do not connect the device to more than one power supply. Otherwise, the device might become damaged.

⚠

- Observe all safety procedures and wear required protective equipment provided for your use while working at heights.
- Do not expose the device to direct sunlight or heat sources.
- Do not install the device in humid, dusty or smoky places.
- Install the device in a well-ventilated place, and do not block the ventilator of the device.
- Use the power adapter or case power supply provided by the device manufacturer.
- The power supply must conform to the requirements of ES1 in IEC 62368-1 standard and be no higher than PS2. Note that the power supply requirements are subject to the device label.
- Connect class I electrical appliances to a power socket with protective earthing.

Table of Contents

1 Introduction

1.1 Overview

Wireless panic button is a wireless button transmitter that sends a panic alarm signal to the hub of the alarm security system. By just the press of the button, alarm signals and events are sent to the monitoring company to ensure a prompt response, and to keep you up to date via the DMSS app. It is suitable for use with security in homes, banks and more. It is also easy to carry around.

1.2 Technical Specifications

This section contains technical specifications of the button. Please refer to the ones that correspond with your model.

Table 1-1 Technical specifications

Type	Parameter	Description	
Function	Indicator Light	1 for multiple statuses (pairing, communication, and more)	
	Button	1	
	Remote Update	Cloud update	
	Signal Strength Detection	Yes	
	Low Battery Detection	Yes	
	Battery Level Display	Displays battery level on app	
Wireless	Carrier Frequency	DHI-ARD821-W2 (868): 868.0 MHz–868.6 MHz	DHI-ARD821-W2: 433.1 MHz–434.6 MHz
	Communication Distance	DHI-ARD821-W2 (868): Up to 1,400 m (4,593.18 ft) in an open space	DHI-ARD821-W2: Up to 1,300 m (4,065.09 ft) in an open space
	Power Consumption	Limit 14 mW	
	Communication Mechanism	Two-way	
	Encryption Mode	AES128	
	Frequency Hopping	Yes	
General	Operating Temperature	−10 °C to +55 °C (+14 °F to +131 °F) (indoor)	
	Operating Humidity	10%–90% (RH)	
	Battery Life	5 years (if used twice a week)	
	Product Dimensions	55 mm × 36 mm × 14.2 mm (2.17" × 1.42" × 0.56") (L × W × H)	

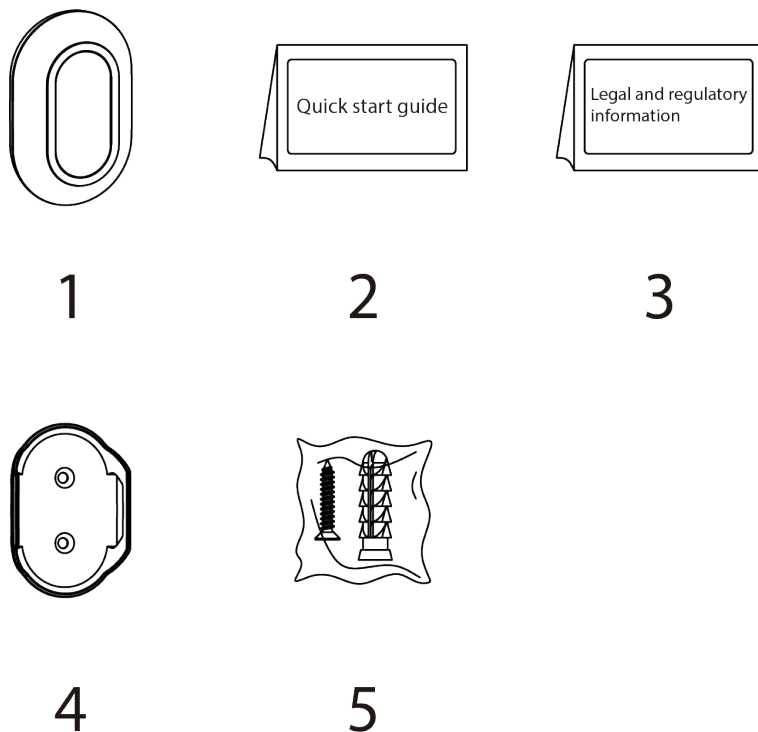| Type	Parameter	Description	
	Packaging Dimensions	95 mm × 59.5 mm × 30.5 mm (3.74" × 2.34" × 1.20") (L × W × H)	
	Installation	Wall mount; handheld	
	Net Weight	18 g (0.04 lb)	
	Gross Weight	48 g (0.11 lb)	
	Certifications	DHI-ARD821-W2 (868): CE	DHI-ARD821-W2: CE, FCC
	Casing	PC + ABS	
	Protection	IP54	
Technical	Operating Current	28 mA	
	Test Mode	Yes	

2 Checklist

Figure 2-1 Checklist

| 1 | 2 | 3 |

| 4 | 5 |

Table 2-1 Checklist

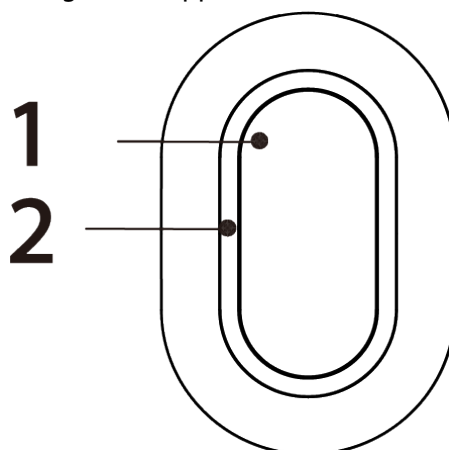| No.	Item Name	Quantity	No.	Item Name	Quantity
1	Panic button	1	4	Bracket (optional)	1
2	Quick start guide	1	5	Screw package (optional)	1
3	Legal and regulatory information	1	—	—	—

3 Appearance

Figure 3-1 Appearance

Table 3-1 Structure

No.	Name	Description
1	Button	● Press and hold the button for 8 seconds, and then the system enters pairing mode.
2	Indicator	◇ Flashes green quickly: Pairing. ◇ Solid green for 2 seconds: Pairing successful. ◇ Slowly flashes green for 3 seconds: Pairing failed. ● On the normal status, press the button once, and then the button sends alarm messages to the hub. ◇ Flashes green once: Sending messages to the hub. ◇ Flashes green for 0.5 seconds: Successfully sent messages to the hub. ◇ Flashes red for 0.5 seconds: Failed to send messages to the hub. ● In accidental press protection mode, press and hold the button for 2 seconds, or double-press it, and then alarm messages will be sent to the hub. The indicator status in accidental press protection mode is the same as that of the normal status. 📖 Make sure that you have enabled the accidental press protection function on the DMSS app.

4 Adding the Button to the Hub

Before you connect it to the hub, install the DMSS app to your phone. This manual uses iOS as an example.

- Make sure that the version of the DMSS app is 1.97 or later, and the hub is V1.001.0000000.7.R.220106 or later.
- Make sure that the hub has a stable internet connection.
- Make sure that the hub is disarmed.

Step 1   Go to the hub screen, and then tap [Accessory] to add the button.

Step 2   Tap ⊕ to scan the QR code at the bottom of the panic button, and then tap **Next**.

Step 3   Tap **Next** after the button has been found.

Step 4   Follow the on-screen instructions and switch the button to on, and then tap **Next**.

Step 5   Wait for the pairing.

Step 6   Customize the name of the button, and select the area, and then tap **Completed**.

5 Installation

Prior to installation, add the button to the hub and check the signal strength of the installation location. We recommend installing the button in a place with a signal strength of at least 2 bars. The button supports wall mount and can be handheld. This section uses wall mount as an example.

You need to buy a bracket to install the button.

Figure 5-1 Installation
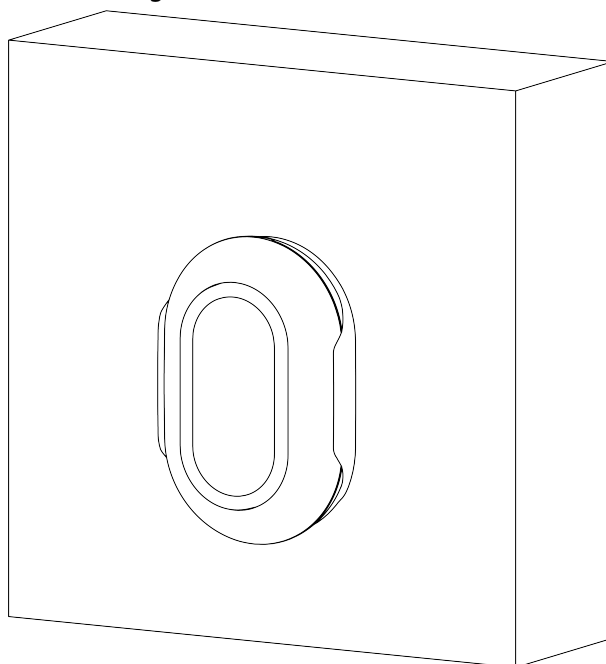
Step 1   Drill 2 holes in the wall according to the hole positions of the bracket.

Step 2   Put the expansion bolts into the holes.

Step 3   Align the screw holes on the bracket with the expansion bolts, and then secure the bracket with screws.

Step 4   Fix the button to the bracket.

6 Configuration

You can view and edit general information of the button.

6.1 Viewing Status

On the hub screen, select a button from the accessory list, and then you can view the status of the button.

Table 6-1 Status

Parameter	Value
Temporary Deactivate	The status for whether the functions of the repeater are enabled or disabled. ● 🔵 : Enable. ● 🟠 : Only disable tamper alarm. ● 🚫 : Disable. 📖 The function is only available when the version of the DMSS app is 1.96 or later, the hub is V1.001.0000000.6.R.211215 or later, and the button is V1.000.0000001.0.R.20211203 or later.
Battery Level	The battery level of the button. ● ▬: Fully charged. ● ▬: Sufficient. ● ▭: Moderate. ● ▭: Insufficient. ● ▭: Low.
Operation Mode	The working mode of the button.
LED Brightness	The brightness of LED lights.
Accidental Press Protection	The status for whether the accidental press protection function is enabled or disabled.
Transmit through Repeater	The status of whether the button forwards accessory messages to the hub through the repeater. 📖 The function is only available when the version of the DMSS app is 1.96 or later, the hub is V1.001.0000000.6.R.211215 or later, and the button is V1.000.0000001.0.R.20211203 or later.
Program Version	The program version of the button.

6.2 Configuring the Button

On the hub screen, select a button from the accessory list, and then tap ☑ to configure the

parameters of the button.

Table 6-2 Panic button parameter description

Parameter	Description
Device Configuration	• View device name, type, SN and device model. • Edit device name, and then tap **Save** to save configuration.
Area	Select the area to which the button is assigned.
Temporary Deactivate	Whether send sensor information to the alarm hub. • Tap **Enable**, and then the button will send alarm messages to the hub. **Enable** is set by default. • Tap **Disable**, and then the button will not send alarm messages to the hub.
Siren Linkage	When an alarm is triggered, the accessories will report the alarm events to the hub and alert with siren.
Alarm-video Linkage	When an alarm is triggered, the accessories will report the alarm events to the hub and then will link events.
Video Channel	Select the video channel as needed.
Alarm Type	Select an alarm event type, and then tap **OK**. • **Intrusion**: Intrusion alarm. • **Fire Alarm**: Fire alarm. • **Medical Help**: Medical alarm. • **Panic Button**: Panic alarm. Set by default. • **Gas Alarm**: Gas leak alarm. 📖 If you select an alarm type as **Intrusion**, the button will send intrusion event messages to the hub.
LED Brightness	Configure the brightness of LED lights. You can select from **Off**, **Low** and **High**.
Accidental Press Protection	Enable **Accidental Press protection** to avoid triggering unintended operations by accidentally pressing the button. • **Off**: Disable the accidental press protection function. • **Press and Hold**: Select **Press and Hold** to enable the accidental press protection function. Once enabled, you have to press and hold the button to send alarm messages to the hub. • **Double-press**: Select **Double-press** to enable the accidental press protection function. Once enabled, you have to double-press the button to send alarm messages to the hub.
Signal Strength Detection	Test the current signal strength.
Button Test	Detect whether the button works.
Cloud Update	Update online.

Parameter	Description
Delete	Delete the online accessory. 📖 Go to the hub screen, select the accessory from the list, and then swipe left to delete it.

Appendix 1 Cybersecurity Recommendations

Cybersecurity is more than just a buzzword: it's something that pertains to every device that is connected to the internet. IP video surveillance is not immune to cyber risks, but taking basic steps toward protecting and strengthening networks and networked appliances will make them less susceptible to attacks. Below are some tips and recommendations from Dahua on how to create a more secured security system.

Mandatory actions to be taken for basic device network security:

1. **Use Strong Passwords**

   Please refer to the following suggestions to set passwords:
   - The length should not be less than 8 characters.
   - Include at least two types of characters; character types include upper and lower case letters, numbers and symbols.
   - Do not contain the account name or the account name in reverse order.
   - Do not use continuous characters, such as 123, abc, etc.
   - Do not use overlapped characters, such as 111, aaa, etc.

2. **Update Firmware and Client Software in Time**
   - According to the standard procedure in Tech-industry, we recommend to keep your device (such as NVR, DVR, IP camera, etc.) firmware up-to-date to ensure the system is equipped with the latest security patches and fixes. When the device is connected to the public network, it is recommended to enable the "auto-check for updates" function to obtain timely information of firmware updates released by the manufacturer.
   - We suggest that you download and use the latest version of client software.

"Nice to have" recommendations to improve your device network security:

1. **Physical Protection**

   We suggest that you perform physical protection to device, especially storage devices. For example, place the device in a special computer room and cabinet, and implement well-done access control permission and key management to prevent unauthorized personnel from carrying out physical contacts such as damaging hardware, unauthorized connection of removable device (such as USB flash disk, serial port), etc.

2. **Change Passwords Regularly**

   We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.

3. **Set and Update Passwords Reset Information Timely**

   The device supports password reset function. Please set up related information for password reset in time, including the end user's mailbox and password protection questions. If the information changes, please modify it in time. When setting password protection questions, it is suggested not to use those that can be easily guessed.

4. **Enable Account Lock**

   The account lock feature is enabled by default, and we recommend you to keep it on to guarantee the account security. If an attacker attempts to log in with the wrong password several times, the corresponding account and the source IP address will be locked.

5. **Change Default HTTP and Other Service Ports**

   We suggest you to change default HTTP and other service ports into any set of numbers between

1024–65535, reducing the risk of outsiders being able to guess which ports you are using.

6. **Enable HTTPS**

   We suggest you to enable HTTPS, so that you visit Web service through a secure communication channel.

7. **MAC Address Binding**

   We recommend you to bind the IP and MAC address of the gateway to the device, thus reducing the risk of ARP spoofing.

8. **Assign Accounts and Privileges Reasonably**

   According to business and management requirements, reasonably add users and assign a minimum set of permissions to them.

9. **Disable Unnecessary Services and Choose Secure Modes**

   If not needed, it is recommended to turn off some services such as SNMP, SMTP, UPnP, etc., to reduce risks.

   If necessary, it is highly recommended that you use safe modes, including but not limited to the following services:

   ● SNMP: Choose SNMP v3, and set up strong encryption passwords and authentication passwords.
   ● SMTP: Choose TLS to access mailbox server.
   ● FTP: Choose SFTP, and set up strong passwords.
   ● AP hotspot: Choose WPA2-PSK encryption mode, and set up strong passwords.

10. **Audio and Video Encrypted Transmission**

    If your audio and video data contents are very important or sensitive, we recommend that you use encrypted transmission function, to reduce the risk of audio and video data being stolen during transmission.

    Reminder: encrypted transmission will cause some loss in transmission efficiency.

11. **Secure Auditing**

    ● Check online users: we suggest that you check online users regularly to see if the device is logged in without authorization.
    ● Check device log: By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.

12. **Network Log**

    Due to the limited storage capacity of the device, the stored log is limited. If you need to save the log for a long time, it is recommended that you enable the network log function to ensure that the critical logs are synchronized to the network log server for tracing.

13. **Construct a Safe Network Environment**

    In order to better ensure the safety of device and reduce potential cyber risks, we recommend:

    ● Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.
    ● The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.
    ● Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.
    ● Enable IP/MAC address filtering function to limit the range of hosts allowed to access the

device.

More information

Please visit Dahua official website security emergency response center for security announcements and the latest security recommendations.

ENABLING A SAFER SOCIETY AND SMARTER LIVING