



Wireless Panic Button(Single)

User 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

Symbols

The following symbols might appear in the manual.

Symbol	Description
 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
V2.0.4	- Revised important safeguards and warnings. - Deleted descriptions about replacing battery.	July 2026
V2.0.3	Optimized the checklist description.	December 2024
V2.0.2	Added precautions for battery use in the important safeguards and warnings.	August 2023
V2.0.1	Revised battery life.	June 2023
V2.0.0	Added battery replacing notes.	April 2022
V1.0.0	First release.	October 2021

Privacy Protection Notice

As the device user, you might collect the personal data of individuals such as their names, email addresses, face images, audio and fingerprints. You shall be fully responsible for any activities associated with processing personal data. You commit to comply with your local privacy protection laws and regulations to protect the legitimate rights and interests of individuals, and shall implement measures which are required by applicable law, including but not limited to, providing clear and comprehensive information to individuals before processing their personal data, obtaining consent from individuals when necessary, informing individuals of the existence of the surveillance area, and providing required contact information.

Intelligent Product Usage Statement

Intelligent products utilize AI technology to effectively enhance security. The intelligent recognition and alarm functions of the product might be affected by factors such as environmental lighting, camera angles, object obstructions, and network delays, potentially leading to false alarms, missed alerts, or response delays. This intelligent product is solely intended to be used as a security assistance tool. The results from performing identification are for reference only and do not constitute absolute guarantee of personal or property safety. Users need to combine these products with necessary physical security measures to enhance overall protection. Except as otherwise provided by laws or in the event of intentional or gross negligence on the part of the company, the company shall not be liable for any losses caused by the aforementioned factors not attributable to the company.

Interface Declaration

This manual mainly introduces the relevant functions of the device. The interfaces used in its manufacture, the procedures for returning the device to the factory for inspection and for locating its faults are not described in this manual. Please contact technical support if you need information on these interfaces.

About the Manual

- This manual is provided for general reference only. Discrepancies might exist between the product and this manual, including but not limited to printed, electronic, or any other editions.
- The manual will be updated according to the latest laws and regulations of related jurisdictions. Specifications and documentation are subject to change without prior notice. For the latest versions, as well as legal notices, consult the printed manual, the product webpage, our official website, or scan the QR code to access the electronic edition.
- The manual will be updated as necessary to reflect product changes and applicable legal requirements. These updates will not diminish your statutory rights, nor will they remove or weaken the safety information or essential instructions provided at the time of purchase.
- Although we make every effort to ensure accuracy, errors or deviations in descriptions of functions, operations, or technical data might occur. If there is any uncertainty or controversy, we reserve the right of final explanation.
- All trademarks, registered trademarks and company names referenced in this manual are the property of their respective owners.

Important Safeguards and Warnings

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

Operation Requirements



The device or remote control contains button batteries. Do not swallow the batteries due to the risk of chemical burns.

Possible result: The swallowed button battery can cause serious internal burns and death within 2 hours.

Preventive measures (including but not limited to):

- Keep new and used batteries out of reach of children.
- If the battery compartment is not securely closed, stop using the product immediately and keep out of reach of children.
- Seek immediate medical attention if a battery is believed to be swallowed or inserted inside any part of the body.



- 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.
- Disassembling the device can reduce performance and create safety hazards. Do not disassemble the device without authorization.

Installation Requirements



- Strictly comply with the local electrical safety code and standards. Make sure that the ambient voltage is stable and meets the power supply requirements of the device.
- The power supply must meet the rated voltage requirements as indicated on the device label.
- If the device uses a power adapter, ensure it meets the following requirements:
 - ◇ If a power adapter was shipped with your device, we recommend you use it. If you need to buy a separate adapter, make sure it meets the following requirements.
 - The power supply must conform to the requirements of IEC 60950-1 and IEC 62368-1 standards.
 - The voltage must meet the SELV (Safety Extra Low Voltage) requirements and not exceed ES-1 standards.
 - When the power of the device does not exceed 100 W, the power supply must meet LPS requirements and be no higher than PS2.

- ◇ Do not connect the power adapter to the device while the adapter is powered on.



- 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.
- Connect class I electrical appliances to a power socket with protective earthing.

Table of Contents

Foreword.....	I
Important Safeguards and Warnings.....	III
1 Introduction.....	1
1.1 Overview.....	1
1.2 Technical Specifications.....	1
2 Checklist.....	3
3 Appearance.....	4
4 Adding the Button to the Hub.....	5
5 Installation.....	6
6 Configuration.....	7
6.1 Viewing Status.....	7
6.2 Configuring the Button.....	8
Appendix 1 Security Commitment and Recommendation.....	10

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	3 years (if used twice a week)	
	Power Supply Mode	Battery (default), 3 VDC	
	Battery Model	1 × CR2032	
	Battery Voltage	3 VDC	

Type	Parameter	Description
	Min. Voltage	2.2 VDC
	Battery Low Threshold	2.6 VDC
	Consumption	- Quiescent current: 4.3 uA - Max. current: 60mA
	PS Type	Type C
	Product Dimensions	55 mm × 36 mm × 14.2 mm (2.17" × 1.42" × 0.56") (L × W × H)
	Packaging Dimensions	95 mm × 59.5 mm × 30.5 mm (3.74" × 2.34" × 1.20") (L × W × H)
	Installation	Wall mount; hand-held
	Net Weight	18 g (0.04 lb)
	Gross Weight	48 g (0.11 lb)
	Certifications	DHI-ARD821-W2 (868): - CE - EN 50131-1:2006+A1:2009+A2:2017+A3:2020 - EN 50131-3:2009 - EN 50131-6:2017 - EN 50131-5-3:2017 - Security Grade 2 - Environmental Class II DHI-ARD821-W2: CE, FCC
Technical	Casing	PC + ABS
	Operating Current	28 mA
	Test Mode	Yes

2 Checklist

Figure 2-1 Checklist

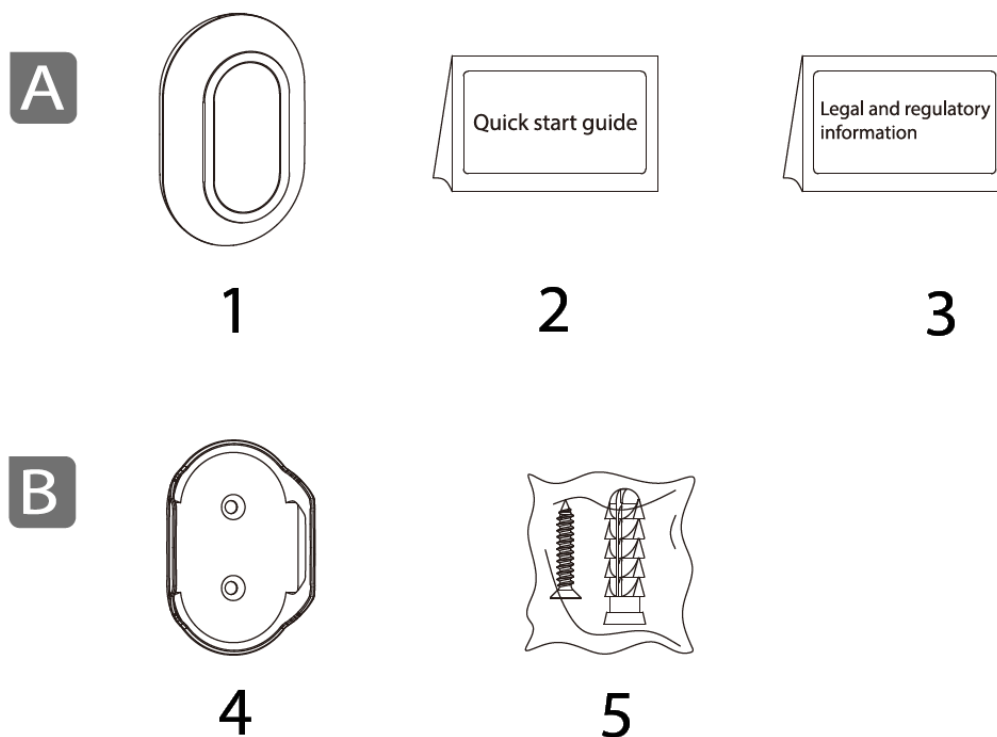


Table 2-1 Checklist

No.	Item Name	Quantity	No.	Item Name	Quantity
A: Standard			B: Optional		
1	Panic button	1	4	Bracket	1
2	Quick start guide	1	5	Screw package	1
3	Legal and regulatory information	1	—	—	—

3 Appearance

Figure 3-1 Appearance

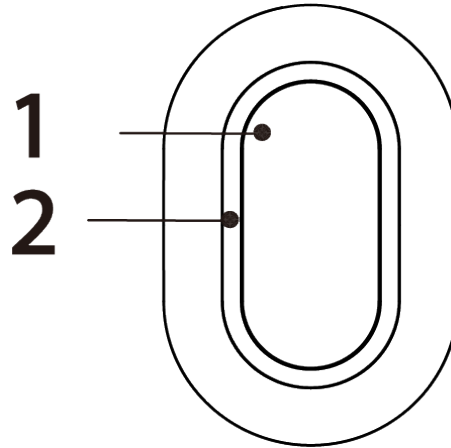


Table 3-1 Structure

No.	Name	Description
1	Button	● Press and hold the button for 8 seconds, and then the system enters pairing mode. ◇ 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.
2	Indicator	 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.

Prerequisites



- 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.

Procedure

- Step 1 Go to the hub screen, and then tap **Peripheral** to add the button
- Step 2 Tap + to scan the QR code at the bottom of the 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

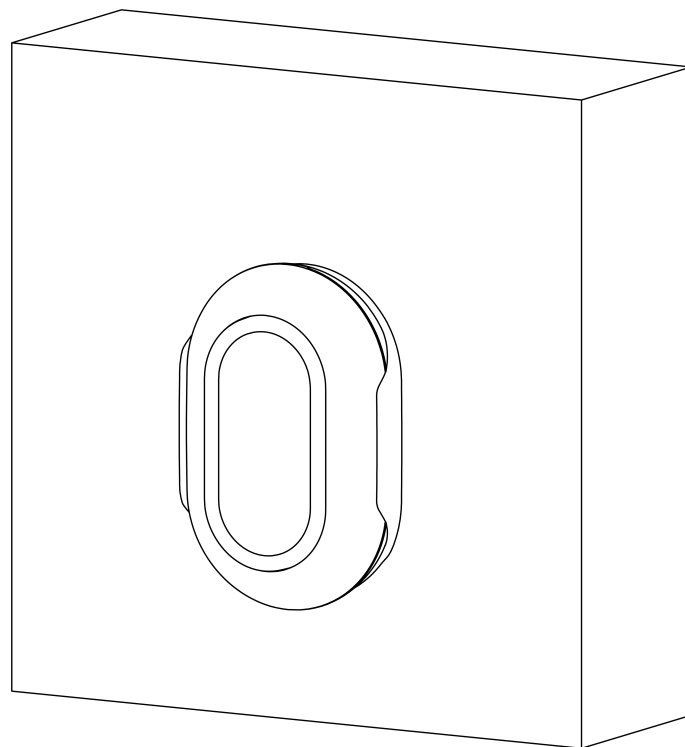
Prior to installation, add the button to the hub and check the signal strength of the installation location. We recommend installing the button in a place with a signal strength of at least 2 bars. The button supports wall mount and can be hand-held. This section uses wall mount as an example.

Background Information



You need to buy a bracket to install the button. Installation height should be less than 2 m.

Figure 5-1 Installation



Procedure

- 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 peripheral list, and then you can view the status of the button.

Table 6-1 Status

Parameter	Value
Permanent Deactivation	The status for whether the permanent deactivation of the button is enabled or turned off.  : Yes. The permanent deactivation is enabled. Alarm information will not be sent to the alarm hub.  : Lid only. All information, except for tamper alarms will be sent to the alarm hub. - No icon appears when the function is configured as No. No means the permanent deactivation is turned off. All information will be sent to the alarm hub.
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 peripheral 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.

Parameter	Value
Program Version	The program version of the button.

6.2 Configuring the Button

On the hub screen, select a button from the peripheral list, and then tap  to configure the parameters of the button.

Table 6-2 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.
Permanent Deactivation	The status for whether the permanent deactivation of the button are enabled or turned off. - Yes: The permanent deactivation is enabled. Alarm information will not be sent to the alarm hub. - Lid only: All information, except for tamper alarms will be sent to the alarm hub. - No icon appears when the function is configured as No. No means the permanent deactivation is turned off. All information will be sent to the alarm hub.
Siren Linkage	When an alarm is triggered, the peripherals will report the alarm events to the hub and alert with siren.
Alarm-video Linkage	When an alarm is triggered, the peripherals will report the alarm events to the hub and then will be linked with videos.
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 .

Parameter	Description
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.
Delete	Delete the button.  Go to the hub screen, select the peripheral from the list, and then swipe left to delete it.

Appendix 1 Security Commitment and Recommendation

Zhejiang Dahua Vision Technology Co., Ltd. (hereinafter referred to as "Dahua") attaches great importance to cybersecurity and privacy protection, and continues to invest special funds to comprehensively improve the security awareness and capabilities of Dahua employees and provide adequate security for products. Dahua has established a professional security team to provide full life cycle security empowerment and control for product design, development, testing, production, delivery and maintenance. While adhering to the principle of minimizing data collection, minimizing services, prohibiting backdoor implantation, and removing unnecessary and insecure services (such as Telnet), Dahua products continue to introduce innovative security technologies, and strive to improve the product security assurance capabilities, providing global users with security alarm and 24/7 security incident response services to better protect users' security rights and interests. At the same time, Dahua encourages users, partners, suppliers, government agencies, industry organizations and independent researchers to report any potential risks or vulnerabilities discovered on Dahua devices to Dahua PSIRT, for specific reporting methods, please refer to the cyber security section of Dahua official website.

Product security requires not only the continuous attention and efforts of manufacturers in R&D, production, and delivery, but also the active participation of users that can help improve the environment and methods of product usage, so as to better ensure the security of products after they are put into use. For this reason, we recommend that users safely use the device, including but not limited to:

Account Management

1. Use complex 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: 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 repeating characters, such as 111, aaa, etc.

2. Change passwords periodically

It is recommended to periodically change the device password to reduce the risk of being guessed or cracked.

3. Allocate accounts and permissions appropriately

Appropriately add users based on service and management requirements and assign minimum permission sets to users.

4. Enable account lockout function

The account lockout function is enabled by default. You are advised to keep it enabled to protect account security. After multiple failed password attempts, the corresponding account and source IP address will be locked.

5. Set and update password reset information in a timely manner

Dahua device supports password reset function. To reduce the risk of this function being used by threat actors, if there is any change in the information, please modify it in time. When setting security questions, it is recommended not to use easily guessed answers.

Service Configuration

1. Enable HTTPS

It is recommended that you enable HTTPS to access Web services through secure channels.

2. Encrypted transmission of audio and video

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

3. Turn off non-essential services and use safe mode

If not needed, it is recommended to turn off some services such as SSH, SNMP, SMTP, UPnP, AP hotspot etc., to reduce the attack surfaces.

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

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

4. Change HTTP and other default service ports

It is recommended that you change the default port of HTTP and other services to any port between 1024 and 65535 to reduce the risk of being guessed by threat actors.

Network Configuration

1. Enable Allowlist

It is recommended that you turn on the allowlist function, and only allow IP in the allowlist to access the device. Therefore, please be sure to add your computer IP address and supporting device IP address to the allowlist.

2. MAC address binding

It is recommended that you bind the IP address of the gateway to the MAC address on the device to reduce the risk of ARP spoofing.

3. Build a secure network environment

In order to better ensure the security of devices and reduce potential cyber risks, the following are recommended:

- Disable the port mapping function of the router to avoid direct access to the intranet devices from external network;
- According to the actual network needs, partition the network: if there is no communication demand between the two subnets, it is recommended to use VLAN, gateway and other methods to partition the network to achieve network isolation;
- Establish 802.1x access authentication system to reduce the risk of illegal terminal access to the private network.

Security Auditing

1. Check online users

It is recommended to check online users regularly to identify illegal users.

2. Check device log

By viewing logs, you can learn about the IP addresses that attempt to log in to the device and key operations of the logged users.

3. **Configure network log**

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

Software Security

1. **Update firmware in time**

According to the industry standard operating specifications, the firmware of devices needs to be updated to the latest version in time in order to ensure that the device has the latest functions and security. If the device is connected to the public network, it is recommended to enable the online upgrade automatic detection function, so as to obtain the firmware update information released by the manufacturer in a timely manner.

2. **Update client software in time**

We recommend you to download and use the latest client software.

Physical Protection

It is recommended that you carry out physical protection for devices (especially storage devices), such as placing the device in a dedicated machine room and cabinet, and having access control and key management in place to prevent unauthorized personnel from damaging hardware and other peripheral equipment (e.g. USB flash disk, serial port).

ENABLING A SMARTER SOCIETY AND BETTER LIVING

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.

Address: No. 1399, Binxing Road, Binjiang District, Hangzhou, P. R. China | Website: www.dahuasecurity.com | Postcode: 310053

Email: dhoverseas@dhvisiontech.com | Tel: +86-571-87688888 28933188