Wireless Relay

User Manual

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD. V1.0.1

Foreword

General

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

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, 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

Version	Revision Content	Release Time
V1.0.1	Revised Appearance chapter.	August 2025
V1.0.0	First release.	November 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 relay, hazard prevention, and prevention of property damage. Read carefully before using the relay, and comply with the guidelines when using it.

Operation Requirements

DANGER

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.
- Do not disassemble the device.

Installation Requirements

WARNING

- Connect the device to the adapter before power on.
- Strictly comply with the local electrical safety code and standards, and check whether the power supply is correct before operating the device.
- Do not connect the device to more than one power supply. Otherwise, the device might become damaged.
- Please follow the electrical requirements to power the device.
  - Followings are the requirements for selecting a power adapter.
    - 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.

- ◇ We recommend using the power adapter provided with the device.
- ◇ When you select the power adapter, the power supply requirements (such as rated voltage) are subject to the device label.

- 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

1 Introduction

1.1 Overview

Wireless Relay is a dry contact device that is used to remotely control 0–36 VDC power. The dry contact of the relay is electrically isolated from the power supply circuit of the device. Relay can be used in low-voltage to control the supply of power to other devices. The device comes with overvoltage protection and overheating protection.

1.2 Technical Specifications

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

Table 1-1 Technical specification

Type	Parameter	Description	
Function	Indicator Light	1 for multiple statuses (pairing, power status, and alarm)	
	Button	1	
	Remote Update	Cloud update	
	Signal Strength	Detects signal strength	
Wireless	Carrier Frequency	DHI-ARM7011-W2(868): 868.0 MHz–868.6 MHz	DHI-ARM7011-W2: 433.1 MHz–434.6 MHz
	Communication Distance	DHI-ARM7011-W2(868): Up to 1,200 m (3937.01 ft) in an open space	DHI-ARM7011-W2: Up to 800 m (2624.67 ft) in an open space
	Transmit Power	DHI-ARM7011-W2(868): Limit 25 mW	DHI-ARM7011-W2: Limit 15.8 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)	
	Storage Temperature	–10 °C to +55 °C (+14 °F to +131 °F)	
	Operating Humidity	10%–90% (RH)	
	Storage Humidity	10%–90% (RH)	

Type	Parameter	Description	
	Power Supply	DHI-ARM7011-W2(868) and DHI-ARM7011-W2: 7–24 VDC	
	Product Dimensions	39 mm × 33 mm × 19 mm (1.54" × 1.30" × 0.75")	
	Packaging Dimensions	95 mm × 59.5 mm × 30.5 mm (3.74" × 2.34" × 1.20")	
	Installation	Wall mount	
	Net Weight	45 g (0.10 lb)	
	Gross Weight	60 g (0.13 lb)	
	Certifications	DHI-ARM7011-W2(868): CE	DHI-ARM7011-W2: CE, FCC
	Casing Material	PC + ABS	
Technical	Test Mode	Yes	
Port	Alarm Input	1 for tamper, NO/NC	
	Relay Output	1, NO/NC (0–36 VAC, Max 5A）	

2 Checklist

Figure 2-1 Checklist

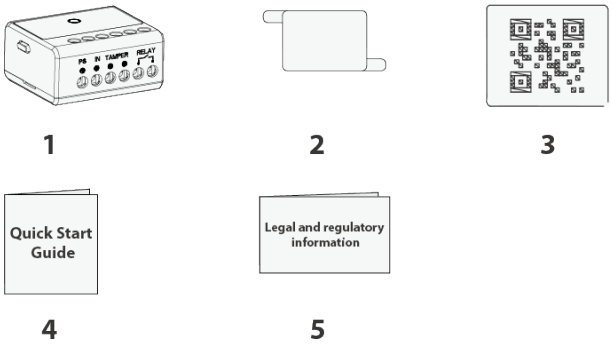


Table 2-1 Checklist

No.	Item Name	Quantity	No.	Item Name	Quantity
1	Relay	1	4	Quick start guide	1
2	Double-sided tape	1	5	Legal and regulatory information	1
3	QR code	1	–	–	–

3 Appearance

Figure 3-1 Appearance

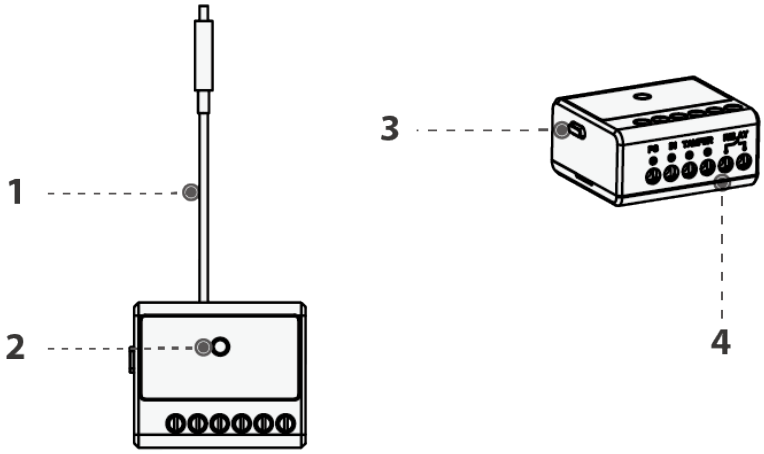


Table 3-1 Structure

No.	Name	Description
1	Antenna	Sends and receives signals.
2	Indicator	• Press and hold the button for 2 seconds, and then the system enters pairing mode. ◇ Solid on for 1 second, then off for 0.5 seconds, and then solid on: Pairing successful. ◇ Slowly flashes for 3 seconds, and then off: Pairing failed. • After being powered on, press and hold the button for 2 seconds, and then the device is off.
3	Power button	
4	Wiring terminal	Relay can be connected to 6.5–36.5 VDC power supply. • PS IN: Power input terminal. It is directly connected to the power cable. • TAMPER: Input terminal for external device. It is connected to the external device to trigger tamper alarm. • RELAY: The connection between the output terminal and the power input terminal is controlled through opening and closing of the built-in relay.

4 Adding the Wireless Relay to the Hub

Before you connect relay 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 1.99.200 or later, and the hub is V1.001.0000004.0.R.221104 or later.
- Make sure that you have already created an account, and added the hub to DMSS.
- 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 relay.

Step 2 Tap **+** to scan the QR code at the bottom of the relay, and then tap **Next**.

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

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

Step 5 Wait for the pairing.

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

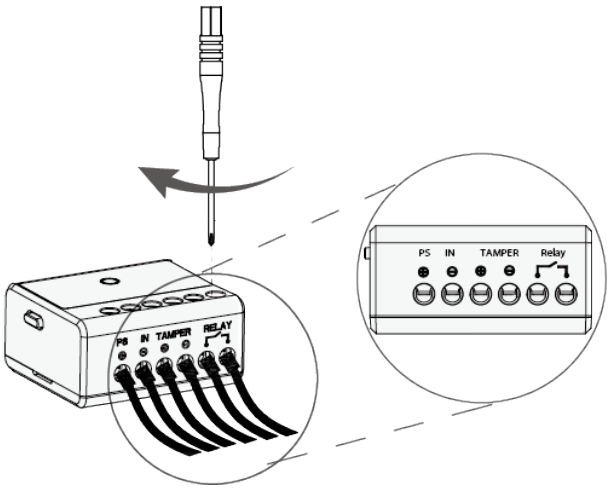
5 Installation

Before installation, add the relay to the hub and check the signal strength of the installation location. We recommend installing the relay in a place with a signal strength of at least 2 bars.

5.1 Wiring

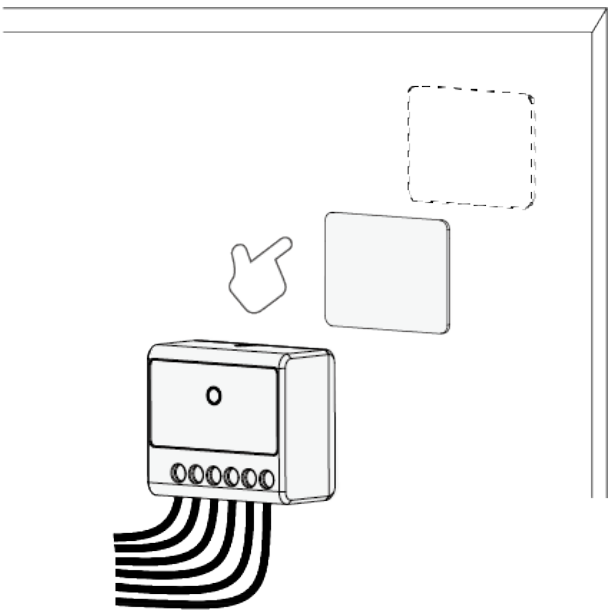
- Relay can be connected to 6.5–36.5 VDC power supply.
- Based on its dimensions, you can install the relay into the deep junction box, inside the electrical appliance enclosure, or in the distribution board.

Figure 5-1 Wire



5.2 Installing the Wireless Relay

Figure 5-2 Attach the relay



6 Configuration

You can view and edit general information of the relay.

6.1 Viewing Status

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

Table 6-1 Status

Parameter	Value
Temporary Deactivate	The status for whether the functions of the relay are enabled or disabled. ●  : Enable. ●  : Disable.
Signal Strength	The signal strength between the hub and the relay. ● : Low. ●  : Weak. ●  : Good. ●  : Excellent. ●  : No.
Input Voltage	Voltage value of the power input.
Output Status	Output status of the relay.
Online Status	Online and offline status of the relay. ●  : Online. ●  : Offline.
Transmit through Repeater	The status of whether the relay forwards its messages to the hub through the repeater.
Program Version	The program version of the relay.

6.2 Configuring the Relay

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

Table 6-2 Parameter description

Parameter	Description
Device Configuration	• View relay name, type, SN and device model. • Edit relay name, and then tap **Save** to save configuration.
Area	Select the area to which the relay is assigned.
Temporary Deactivate	Whether send sensor information to the alarm hub. • Tap **Enable** , and then the relay will send alarm messages to the hub. **Enable** is set by default. • Tap **Disable**, and then the relay will not send alarm messages to the hub.
Output Type	Select form **Normally Open** or **Normally Closed**. **Normally Closed** is set by default.
Output Mode	Select form **Steady State** or **Pulse**. **Pulse** is set by default. When selecting as **Pulse**, you can set pulse duration.
LED Indicator	LED Indicator is enabled by default. If LED Indicator is disabled, the LED indicator will remain off regardless of whether the relay is functioning normally or not.
Scenario Setting	Configure scenarios to associate the relay to perform the corresponding action. Click **Create Scenario** , you can select from **Arming/Disarming Linkage Scenario**, **Alarm Linkage Scenario**, or **Scheduled Linkage Scenario**. • **Arming/Disarming Linkage Scenario** : After customizing scenario name and selecting linkage area, you can enable or disable **Arming Linkage Output Module**, **Disarming Linkage Output Module**, or **Home Mode Linkage Output Module**. • **Alarm Linkage Scenario** • **Scheduled Linkage Scenario** : After customizing scenario name and enabling **Scheduled Linkage Output Module**, you can set time and repeat periods.
External Tamper	After enabling **External Tamper**, external tamper alarm will be triggered.
Signal Strength Detection	Test the current signal strength.

Parameter	Description
Transit Power	• Select from high, low, and automatic. • The higher transmission power levels are, the further transmissions can travel, but power consumption increases. • If you select **Low**, the relay will enter into reduced sensitivity mode. • We recommend you selecting **Low** when installing the device to test the signal strength of the installation location, and then adjusting to **High** or **Automatic**. • The indicator flashes when setting as **Low**.
Delete	Delete the relay. Go to the hub screen, select the relay from the list, and then swipe left to delete it.

Appendix 1 Security Commitment and Recommendation

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;
   - Stablish 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