



Wireless Relay

User's Manual








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, 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.	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 protection, and protection of property damage. Read carefully before using the relay, and comply with the guidelines when using it.

Operation Requirements



- Make sure that the power supply of the relay works properly before use.
- Do not pull out the power cable of the relay while it is powered on.
- Only use the relay 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 relay to avoid liquids flowing into it.
- Do not disassemble the relay.

Installation Requirements



- Connect the relay 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 relay.
- Do not connect the relay to more than one power supply. Otherwise, the might become damaged.



- Observe all safety procedures and wear required protective equipment provided for your use while working at heights.
- Do not expose the relay to direct sunlight or heat sources.
- Do not install the relay in humid, dusty or smoky places.
- Install the relay 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

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 Wireless Relay to the Hub	5
5 Installation	6
5.1 Wiring	6
5.2 Installing the Wireless Relay	6
6 Configuration	7
6.1 Viewing Status	7
6.2 Configuring the Relay	7
Appendix 1 Cybersecurity Recommendations	10

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)	

Type	Parameter	Description	
	Operating Humidity	10%–90% (RH)	
	Storage Humidity	10%–90% (RH)	
	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

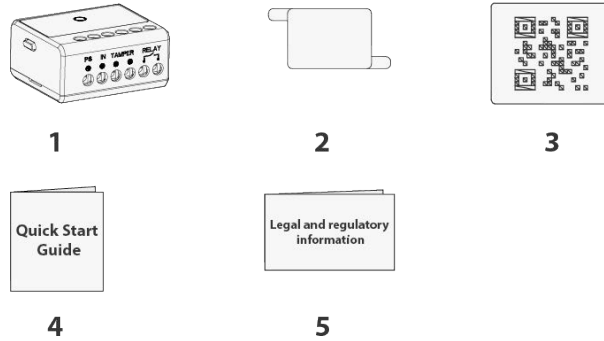


Table 2-1 Checklist

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

3 Appearance

Figure 3-1 Appearance

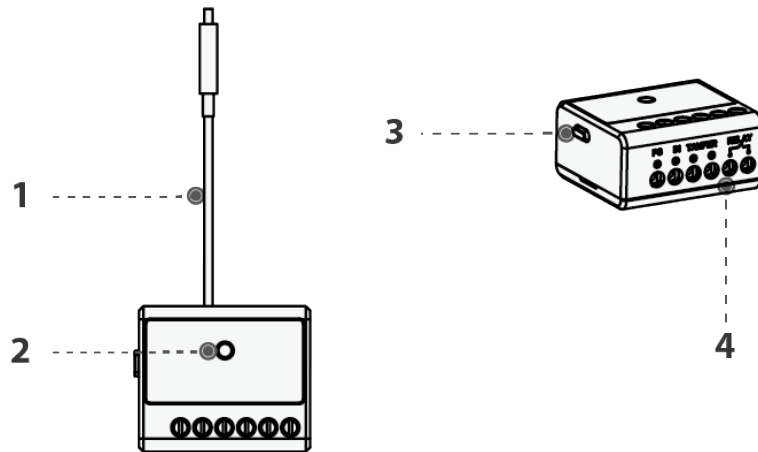


Table 3-1 Structure

No.	Name	Description
1	Antenna	Sends and receives signals.
2	Indicator	<ul style="list-style-type: none"> ● Press and hold the button for 2 seconds, and then the system enters pairing mode. <ul style="list-style-type: none"> ◇ 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. <ul style="list-style-type: none"> ● PS IN: Power input terminal. It is directly connected to the power cable. ● RAMPER: 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.



- 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.

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**.

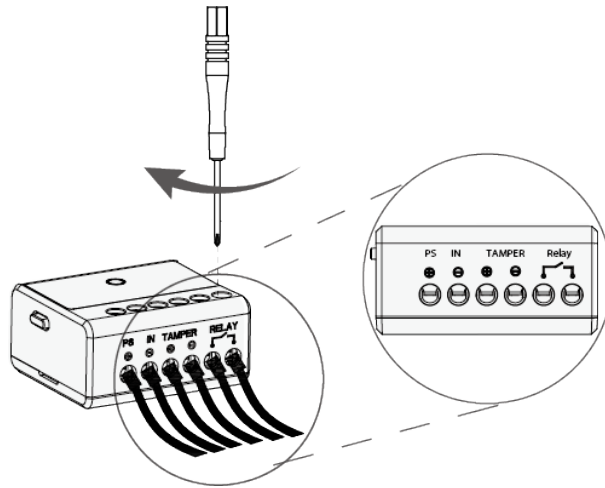
5 Installation

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

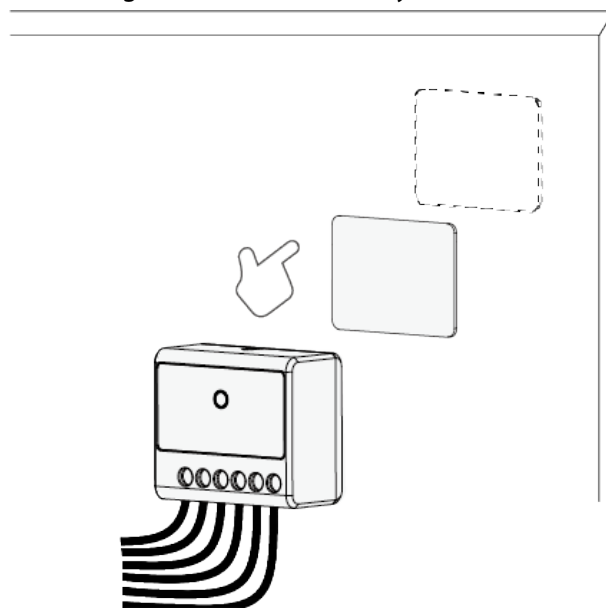
- Relay can be connected to 6.5–36.5 VDC power supply.
- Based on its dimensions, you can install the relay into the deep junction box, inside the electrical appliance enclosure, or in the distribution board.

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 repeater are enabled or disabled. <ul style="list-style-type: none"> ● : Enable. ● : Disable.
Signal Strength	The signal strength between the hub and the relay. <ul style="list-style-type: none"> ● : 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. <ul style="list-style-type: none"> ● : 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	<ul style="list-style-type: none"> ● 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.

Parameter	Description
Temporary Deactivate	Whether send sensor information to the alarm hub. <ul style="list-style-type: none"> • 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 . <ul style="list-style-type: none"> • 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.
Transit Power	<ul style="list-style-type: none"> • Select from high, low, and automatic. • The higher transmission power levels are, the further transmissions can travel, but power consumption increases.  <ul style="list-style-type: none"> • 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.

Parameter	Description
Delete	Delete the relay.  Go to the hub screen, select the relay 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

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.

Address: No.1199 Bin'an Road, Binjiang District, Hangzhou, P. R. China | Website: www.dahuasecurity.com | Postcode: 310053

Email: overseas@dahuatech.com | Fax: +86-571-87688815 | Tel: +86-571-87688883