



Wireless Dual-Channel Relay

User Manual



Foreword

General

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

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
V1.0.0	First release.	April 2026

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.

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 relay, hazard prevention, and prevention of property damage. Read carefully before using the relay, 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.
- Do not disassemble the device.

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 Product Overview.....	1
1.2 Technical Specification.....	1
2 Checklist.....	3
3 Design.....	4
3.1 Appearance.....	4
3.2 Wiring.....	5
3.3 Dimensions.....	7
4 Installation.....	8
4.1 Adding Relay to Hub.....	8
4.2 Installing Relay.....	8
4.2.1 Wall Mount.....	8
4.2.2 Bracket Mount.....	9
4.2.3 Rail Mount.....	10
5 Configuration.....	12
5.1 Viewing Status.....	12
5.2 Configuring the Relay.....	13
5.3 Mode Switching.....	15
Appendix 1 Security Commitment and Recommendation.....	16

1 Introduction

1.1 Product Overview

Wireless dual-channel relay is a compact dual-channel smart switch that monitors power consumption and controls the switching of 100–240 VAC power. The device enables remote control of electrical appliances, such as lights, roller shutters, and blinds, on smartphone or local switch. You can also configure automated scenes for intelligent, hands-free management of connected devices.

1.2 Technical Specification

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
Port	Wired Input	2 switch inputs, used to control 2 relay output respectively.100-240VAC.
	Wired Output	2 relay outputs, 100-240VAC/10 A (single channel), 100-240 VAC/8 A(dual channels)
	Contact Load Condition	Overload:120 VAC, switching inrush 50A, cos(phi)=1, steady state 7.5A cos(phi)=0.75-0.8, duty cycle: 1s:9s, number of times: 50 times Electrical endurance:120 VAC, switching inrush 50 A 2.5ms, steady state 5A, 1s:9s, 25,000 times
Function	Indicator Light	1 for multiple statuses (pairing, power on)
	Button	1
	Remote Update	Cloud update
	Signal Strength	Detects signal strength
Technical	Test Mode	Yes
	Min. Detection Current	> 100 mA
Wireless	Carrier Frequency	DHI-ARM7022-W2(868): 868.0 MHz–868.6 MHz DHI-ARM7022-W2(915): 915.8 MHz–928.0 MHz DHI-ARM7022-W2: 433.05 MHz–434.79 MHz
	Transmitter Power (EIRP)	DHI-ARM7022-W2(868): Limit 25 mW DHI-ARM7022-W2(915): Limit 1 W DHI-ARM7022-W2: Limit 10 mW
	Communication Mechanism	Two-way

Type	Parameter	Description
	Communication Distance	Up to 1,600 m (5,249.34 ft) in an open space
	Encryption Mode	AES128
	Frequency Hopping	Yes
General	Power Supply	100-240 VAC, 50/60 Hz
	Power Consumption	0.5 W
	Operating Temperature	-10 °C to +40 °C (+14 °F to +104 °F)
	Operating Humidity	10%–90% (RH)
	Product Dimensions	47 mm × 47 mm × 24 mm (1.85" × 1.85" × 0.94") (L × W × H)
	Net Weight	57 g (0.13 lb)
	Gross Weight	115 g (0.25 lb)
	Installation	Bracket mount, adhesive mount, 86 junction box mount, 120 junction box mount
	Casing Material	PC + GF
	Appearance Color	White
	Certifications	CE
	Anti-corrosion Level	Basic Protection *The products are designed for general use and are applicable even in areas with no specific requirements for anti-corrosion protection.
	Storage Temperature	-10 °C to +40 °C (+14 °F to +104 °F)
	Storage Humidity	10%–90% (RH)
	Packaging Dimensions	99 mm × 40 mm × 136 mm (3.90" × 1.58" × 5.35") (L × W × H, 1 in inner carton)

2 Checklist

Please check against the following checking list. If any of the items are missing or damaged, contact the local retailer or after-sales engineer immediately.

Figure 2-1 Checklist

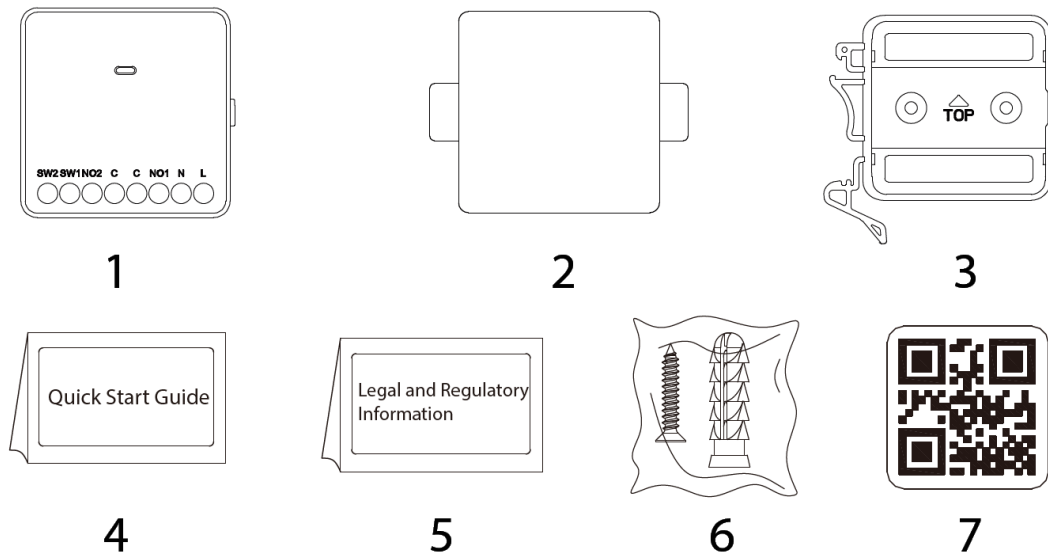


Table 2-1 Checklist

No.	Item Name	Quantity	No.	Item Name	Quantity
1	Wireless dual-channel relay	1	5	Legal and Regulatory information	1
2	Double-sided sticker	1	6	Package of screws	1
3	Bracket and the guide rail	1	7	QR code	1
4	Quick Start Guide	1	—	—	—

3 Design

3.1 Appearance

Figure 3-1 Appearance

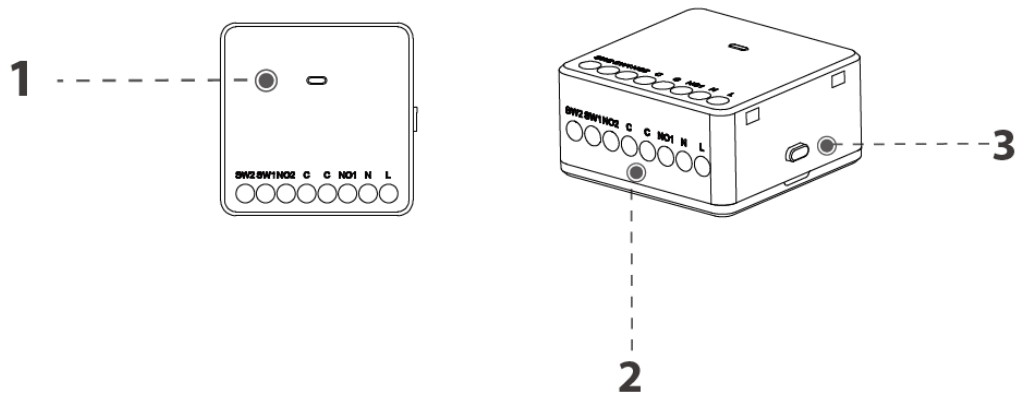


Table 3-1 Description of Structure

No.	Name	Description
1	Indicator	- Press and hold the power button for 2 seconds, and then the relay goes to the pairing mode. - Pairing successful: Solid on for 1 second, then off for 0.5 seconds, and then solid on. - Pairing failed: Flashes slowly for 3 seconds, and then off. - After being powered on, press and hold the power button for 2 seconds, and then the relay is off.

No.	Name	Description
2	Wiring terminal	• L: 100-220 VAC live fire. • N: 100-220 VAC neutral wire. • C: Load common terminal (When relay 1 is toggled, C connects to NO1; when relay 2 is toggled, C connects to NO2).  For single-channel use or when the combined current of both channels is 10 A or less, only one C terminal needs to be connected. If the total current exceeds 10 A, both C terminals must be connected. • NO1: Load 1 connection port. • NO2: Load 2 connection port. • SW1: SW1: Local switch 1 connection port (When SW1 is toggled, NO1 connects to C).  The signal for SW1 must be connected to the live wire. • SW2: Local switch 2 connection port When SW2 is toggled, NO2 connects to C).  The signal for SW2 must be connected to the live wire.
3	Power button	Press the button to power on the relay.

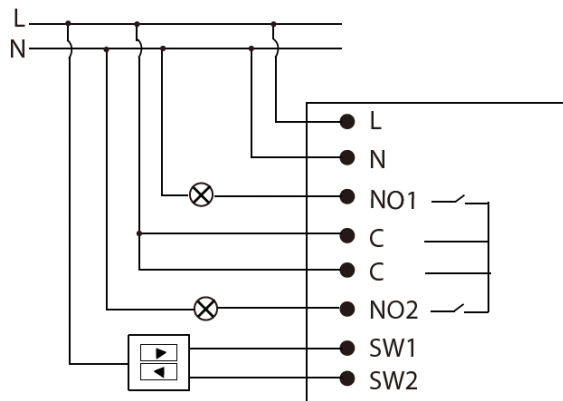
3.2 Wiring

The relay supports 2 distinct modes: General mode and roller shutter mode. In general mode, each channel might be controlled individually. In roller shutter mode, both channels are regarded as a unified device, synchronized by firmware, to provide control of the roller shutter.

General Mode

In general mode, the wiring must be the following:

Figure 3-2 General mode



Roller Shutter Mode

In roller shutter mode, there are 2 ways of wiring.

Figure 3-3 Roller shutter mode (1)

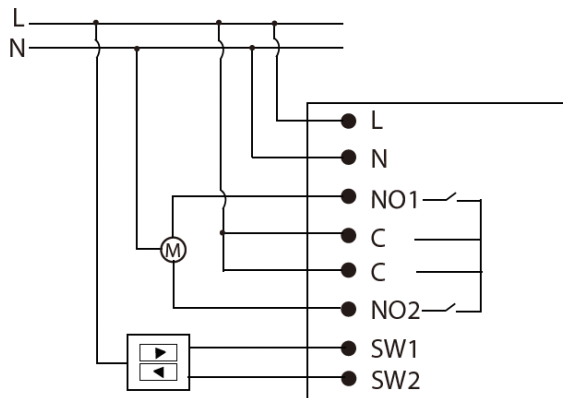
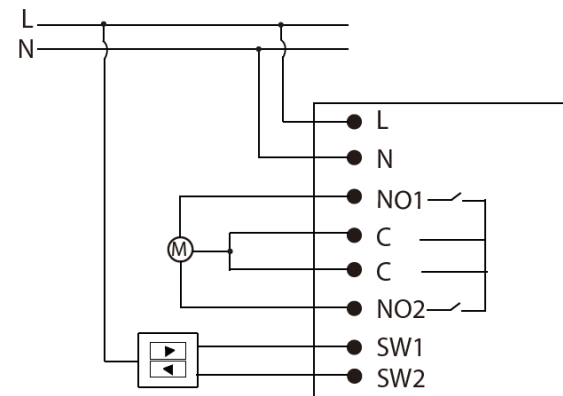
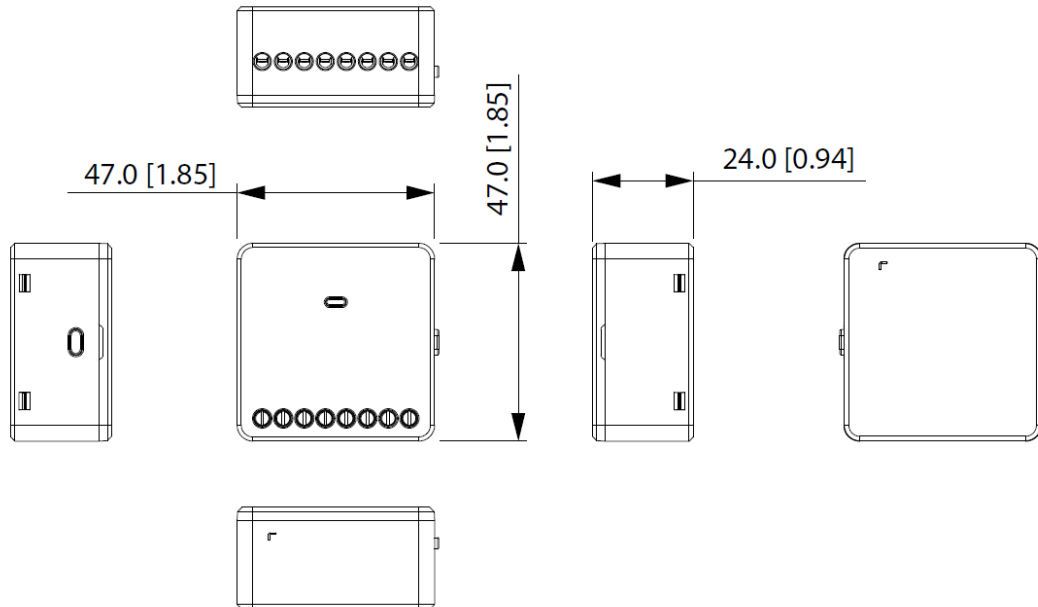


Figure 3-4 Roller shutter mode (2)



3.3 Dimensions

Figure 3-5 Dimensions (mm [inch])



4 Installation

Power on the keypad, connect it to the hub, perform signal strength test, and then install the keypad onto the wall.

4.1 Adding Relay to Hub

Background Information

Before you connect the relay to the hub, install the DMSS or DoLynk Care app on your phone. This manual uses iOS as an example.



- Make sure that you have already created an account, and added the hub to DMSS or DoLynk Care.
- Make sure that the relay has a stable internet connection.
- Make sure that the hub is disarmed.

1. Go to the **Devices** screen of the hub, and then select  > **Add Peripheral**.
2. Scan the QR code at the bottom of the relay, and then tap **Next**.
3. Tap **Next** after the relay has been found.
4. Configure the device name for the relay, assign the area for it, and then tap **Next**.
5. Follow the on-screen instructions to switch the relay from off to on, and its indicator flashes green, and then tap **Next**.
6. Wait for the pairing to finish, and then tap **OK**.

4.2 Installing Relay

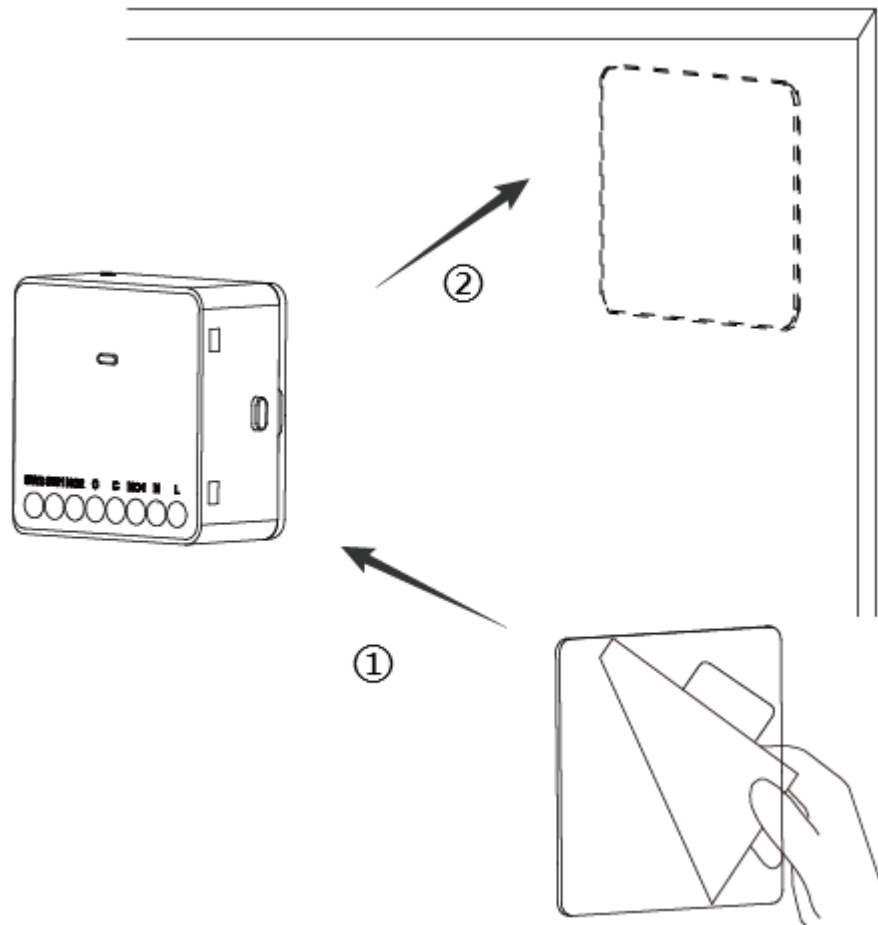
There are 3 methods to install the relay: Wall mount, bracket mount and rail mount.

4.2.1 Wall Mount

Procedure

- Step 1 Peel off the double-sided sticker and then attach one side of the sticker to the back of the relay.
- Step 2 Align the back of the relay (with the double-sided sticker attached) to the designated position on the wall, then press firmly to secure it in place.

Figure 4-1 Wall mount



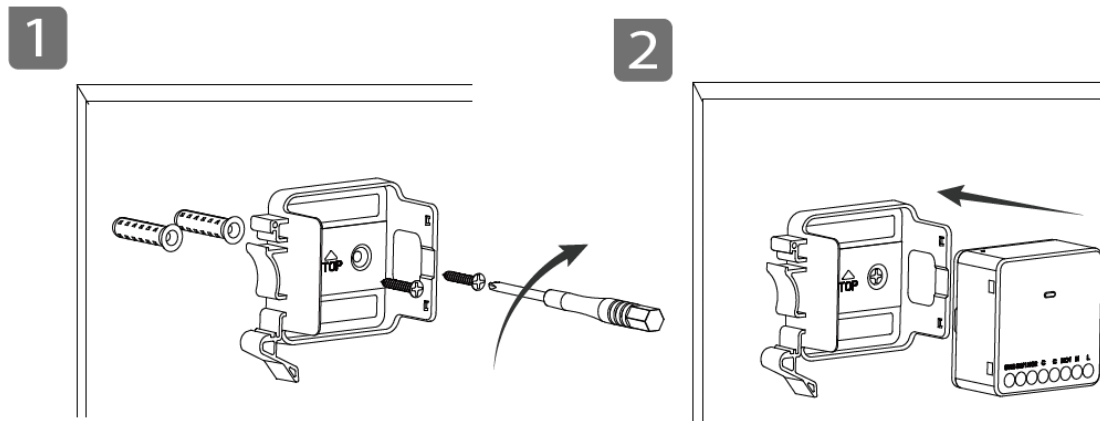
4.2.2 Bracket Mount

Install the relay using the bracket.

Procedure

- Step 1 Drill 2 expansion bolts in to the wall, and then secure the bracket on to the wall using 2 screws.
- Step 2 Insert the relay into the bracket.

Figure 4-2 Bracket mount

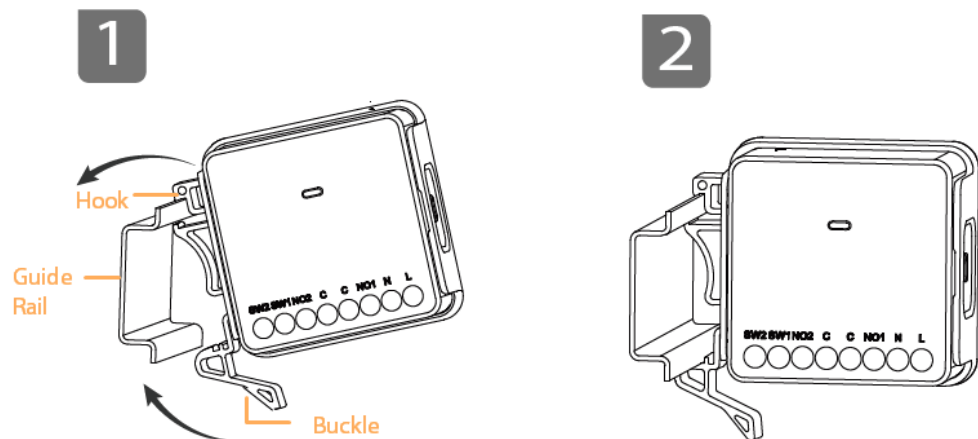


4.2.3 Rail Mount

Procedure

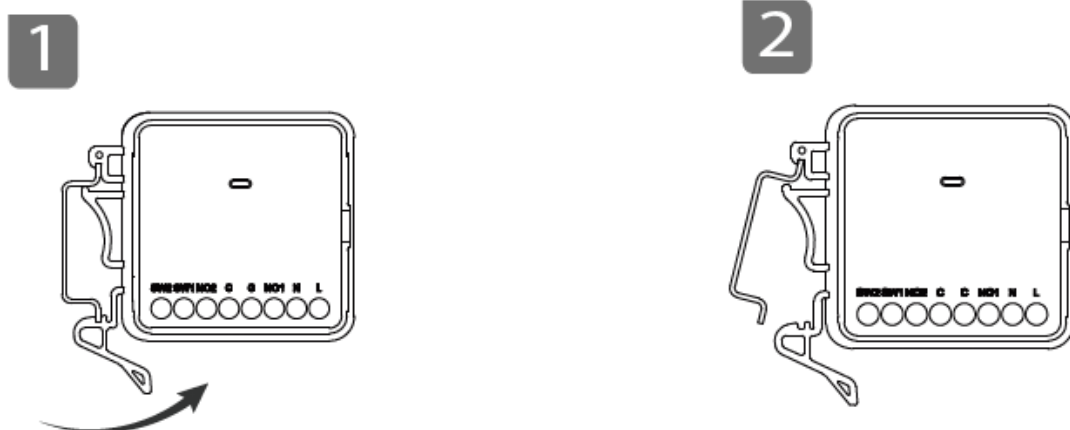
- Step 1 Hang the relay hook on the guide rail, and then press the relay to make the buckle into the guide rail.
- Step 2 Once the relay is fully attached, check whether it is locked in place and will not fall off.

Figure 4-3 Rail mount



- Step 3 (Optional) Remove the rail.
1. Press the buckle in the direction shown in the arrow, and then it would be loose enough to be removed from the rail.
 2. Gently pull the rail away from the relay to complete the removal process.

Figure 4-4 Remove rail



5 Configuration

5.1 Viewing Status

Relay Icon Description

Introduces the meaning of icons for the relay. You can view these icons on the hub screen.

Table 5-1 Device icon description

Parameter	Icon	Description
Signal Strength		Low
		Weak
		Good
		Excellent
		No signal
Permanent Deactivation		Yes
Roller Shutter		Enabled
Bypass		Yes  Only available after the roller shutter function is enabled.

Relay Status Description

On the **Devices** screen of the hub, select a relay and then select **Overview** to view the information and status.

Table 5-2 Status

Parameter	Description
Device No.	Displays the number of the relay.
Temperature	Displays the temperature of the relay.  The temperature has a tolerance of $\pm 3^{\circ}\text{C}$, and the measurement accuracy is 1°C .
Signal Strength	Displays the signal strength of the relay.
Online Status	Online and offline status of the relay.

Parameter	Description
Permanent Deactivation	The status for whether the permanent deactivation of the relay is enabled or turned off.
Opened	The opening degree of the roller shutter installed. It displays in percentage.
Input Voltage	Displays the input voltage of the relay.
Input Current	Displays the input current of the relay.
Power	Displays the power of the relay.
Consumed Electric Energy	Displays the consumed electric energy of the relay.
Program Version	Displays the latest version of the relay program.

5.2 Configuring the Relay

On the **Home** screen, select a hub, and then select a relay on the **Devices** > **Settings** screen of the hub to configure the relay.

Table 5-3 Parameter description

Parameter	Description
Device	- View the name, type, SN of the relay. - Edit the name, and then tap OK to save configuration.
Area	Select the room to which the relay is assigned.
Permanent Deactivation	The status for whether the permanent deactivation of the relay is enabled or turned off. Yes : The permanent deactivation is enabled. Alarm information will not 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.
Over-temperature Alarm	Tap  next to Over-temperature Alarm to enable this function, and then the alarm will be triggered when the temperature of the area where the relay is installed is higher or lower than the defined one. Scroll left and right on the temperature bar to set the lowest temperature or highest temperature, or tap + or - to set the temperature ranges. The range is between -10 and 55°C.
Backlight Brightness	Select from Closed , Low and High to adjust the backlight brightness of the relay operating screen.
LED Indicator	Indicators for alarms, fault and arming/disarming status on the relay.  Turning off the function will stop the indicators of the relay from lighting up for alarms, faults and arming/disarming statuses.

Parameter	Description
Consumed Electric Energy	View the consumed electric energy of the relay. Tap  to set the value to 0.0 kW/h.
Signal Strength Detection	Test the current signal strength to select an area with great signal to install the relay.
Transmit Power	• Select from high, low, and automatic. • The higher the transmission power, the further the signal can travel, but the greater the power consumption.  If you select Low, and then the relay will enter reduced sensitivity mode until you select another option.
Roller Shutter	When you enable the Roller Shutter function, it is necessary to calibrate the roller shutter for initial use. Tap Calibrate, and then the roller shutter starts calibrating. The calibration allows precise control over the roller shutter's opening and closing positions. The system automatically calibrates the full range of the roller shutter's movement. Be advised that do not operate during this process. • Motion Time Limit : Configure the maximum and minimum open time, as well as maximum and minimum close time for the roller shutter. • Idle Time : Configure the delay time required when reversing the shutter's movement direction. For example, If the roller shutter is in the process of opening and you tap Stop and Close in the app, it will continue to open until the configured idle time has elapsed. • Action on Startup : Select from Open, Close and None. ◇ Open : Upon power-up, the roller shutter will automatically open until either the detected power drops below the preset threshold, or the configured maximum opening time is reached. ◇ Close : Upon power-up, the roller shutter will automatically close until either the detected power drops below the preset threshold, or the configured maximum closing time is reached. ◇ None : No actions are performed after the relay is powered up. • Local Control : Enable the function, and then you can control the opening and closing of the roller shutter locally through keyfobs. • Scene Settings : You can create arming/disarming linkage scenes and scheduled linkage scenes for the roller shutter.
User's Manual	View user manual of the relay.
Firmware Update	Update the relay firmware using cloud service.

5.3 Mode Switching

The relay supports 2 distinct modes: General mode and roller shutter mode. In general mode, each channel might be controlled individually. In roller shutter mode, both channels are regarded as a unified device, synchronized by firmware, to provide control of the roller shutter.

Roller Shutter Mode

If you enable **Roller Shutter** function on the app, the relay goes to the roller shutter mode automatically.

General Mode

If you turn off **Roller Shutter** function on the app, the relay goes to the general mode. Configurations about the roller shutter on the app is cleared automatically. You can add other types of output, such as light, for the relay.



You can add up to 2 channels of output in the general mode.

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