Wireless Keyfob

User Manual

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD. V1.1.4

Foreword

General

This manual introduces the installation, functions and operations of the wireless keyfob (hereinafter referred to as the "keyfob"). 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
V1.1.4	Revised important safeguards and warnings.	July 2026
V1.1.3	Revised technical parameters.	July 2025
V1.1.2	Added battery description.	August 2023
V1.1.1	Revised battery life.	June 2023
V1.1.0	• Added technical specifications and field of view. • Updated descriptions of parameters. • Updated images.	January 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 keyfob, hazard prevention, and prevention of property damage. Read carefully before using the keyfob, 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.
- Disassembling the device can reduce performance and create safety hazards. Do not disassemble the device without authorization.

Installation Requirements

WARNING

- 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

1 Introduction

1.1 Overview

Wireless keyfob is a miniature remote that connects to the hub and controls the alarm system in your home. It works by sending wireless communication signals to the alarm system, which will recognize the signal and then perform the function that is assigned to the area.

1.2 Technical Specifications

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

Table 1-1 Technical specifications

Type	Parameter	Description		
Port	Indicator Light	1 × two-color status indicator (green: normal, red: abnormal)		
	Button	4 (Home, Away, Disarm, and SOS)		
Function	Remote Update	Cloud update		
	Low Battery Alarm	Yes		
Wireless Parameters	Carrier Frequency	DHI-ARA24-W2(868): 868.0 MHz–868.6 MHz	DHI-ARA24-W2: 433.1 MHz–434.6 MHz	DHI-ARA24-W2(915): 915MHz-928MHz
	Communication Distance	DHI-ARA24-W2(868): Up to 900 m (2,952.76 ft) in an open space	DHI-ARA24-W2: Up to 500 m (1,640.42 ft) in an open space	DHI-ARA24-W2(915): Up to 900 m (2,952.76 ft) in an open space
	Communication Mechanism	Two-way		
	Encryption Mode	AES128		
	Frequency Hopping	Yes		
General	Power Supply	CR2032 battery		
	Battery Voltage	3 VDC		
	Min. Voltage	1.8 VDC		
	Battery Low Threshold	2.6 VDC		
	Battery Restore Threshold	2.65 VDC		

Type	Parameter	Description		
	Working Current	65 mA(Max) 0.4 uA(Standby)		
	PS Type	Type C		
	Battery Life	3 years		
	Power Consumption	DHI-ARA24-W2(868): Max. 100 mW	DHI-ARA24-W2: Max. 85 mW	DHI-ARA24-W2(915): 195mW(Max) 0.0012mW(Stand by
	Operating Environment	Indoor: –10 °C to +55 °C (+14 °F to +131 °F) Certified temperature: –10°C to +40°C (+14°F to +104 °F)		
	Operating Humidity	10%–90% (RH)		
	Product Dimensions	60.0 mm × 39.5 mm × 15.0 mm (2.36" × 1.56" × 0.59") (L × W × H)		
	Packaging Dimensions	135.0 mm × 98.5 mm × 27.8 mm (5.31" × 3.88" × 1.09")		
	Net Weight	20 g (0.04 lb)		
	Gross Weight	65 g (0.14 lb)		
	Casing	PC + ABS		
	ACE Type	Type B		
Certifications	DHI-ARA24-W2(868): EN 50131-1:2006+A1: 2009+A2:2017+A3:2020 EN 50131-5-3: 2017 EN 50131-6:2017 EN 50131-3: 2009 Security Grade 2 Environmental Class II CE	DHI-ARA24-W2: CE FCC	DHI-ARA24-W2(915): /	

2 Checklist

Figure 2-1 Checklist

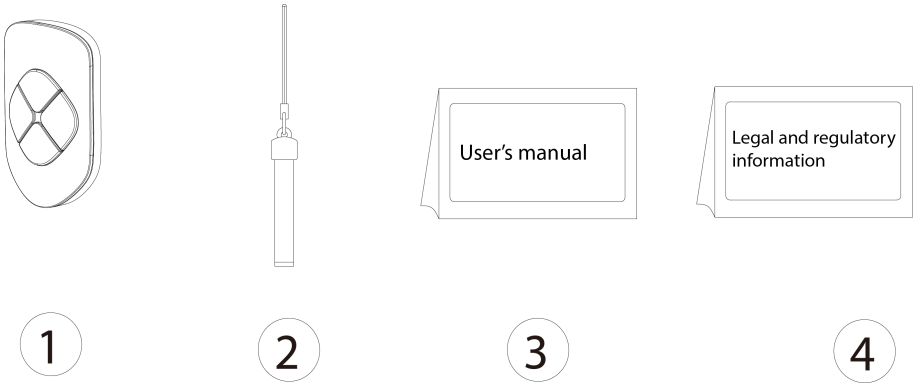


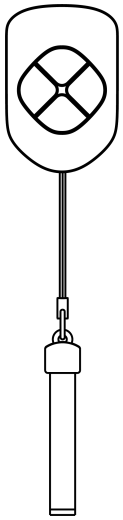
Table 2-1 Checklist

No.	Item Name	Quantity
1	Wireless keyfob	1
2	String	1
3	User's manual	1
4	Legal and regulatory information	1

3 Design

3.1 Appearance

Figure 3-1 Appearance



3.2 Function Key

Figure 3-2 Function key

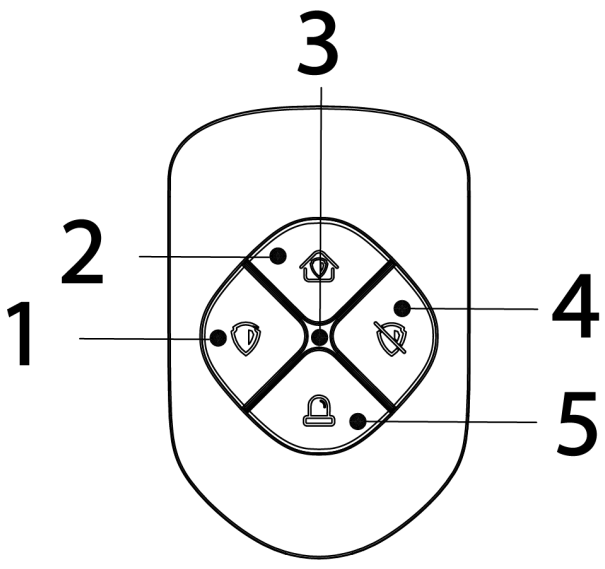


Table 3-1 Description of function button

No.	Name	Description
1	Arming button	Press the home mode, and then the selected peripherals will be armed.
2	Home mode	Press the home mode, and then the selected peripherals will be armed.

No.	Name	Description
3	Indicator	• Flashes green quickly: Pairing mode. • Solid green: Normal. • Solid red: The keyfob is offline. • Flashes green first, and then turns to red: Connection with the hub failed.
4	Disarming button	Press the button once to disarm the system.
5	SOS	Press the panic button, and then the keyfob will send alarm signal to the alarm system.

4 Adding the Keyfob to the Hub

Prerequisites

Device configurations are performed on the DMSS app. Make sure that you have installed the DMSS app, created an account, and added the hub to the app. For details on adding the hub, see the user's manual of the corresponding hub.

- Make sure that the hub has a stable internet connection.
- Make sure that the hub is disarmed.

Background Information

You can add the keyfob to the hub. This user's manual uses the operations on iOS as an example.

Procedure

Step 1 Go to the hub screen, and then tap **Peripheral** to add the keyfob.

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

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

Step 4 Follow the on-screen instructions and press  and  once at the same time, and then tap **Next**.

Step 5 Wait for the pairing.

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

5 Keyfob Configuration

You can view and edit general information of the keyfob.

5.1 Viewing Status

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

Table 5-1 Status

Parameter	Value
Permanent Deactivate	The status for whether the functions of the keyfobs are enabled or disabled. ●  : Enable. ●  : Only disable tamper alarm. ●  : Disable.
Battery Level	The battery level of the keyfob. ●  : Fully charged. ●  : Sufficient. ●  : Moderate. ●  : Insufficient. ●  : Low.
SOS Status	The status of the SOS alarm.
Relay Status	The status of whether the keyfob forwards peripheral messages to the hub through the repeater.
Program Version	The program version of the keyfob.

5.2 Configuring the Keyfob

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

Table 5-2 Keyfob 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	• View the existing area. • Add the area that you want to arm, and then tap **Save** to save configuration.
Permanent Deactivate	• Tap **Enable** , and then the keyfob will not send alarm messages to the hub. **Enable** is set by default. • Tap **Only Disable Tamper Alarm**, and then the system will only ignore tamper alarm messages. • Tap **Disable**, and then the keyfob will send alarm messages to the hub.
LED Indicator	**LED Indicator** is enabled by default on the app. You also need to press any button on the keyfob to enable the function. If **LED Indicator** is disabled, the LED indicator will remain off regardless of whether the keyfob is functioning normally or not.
Control Permissions	Select the area over which the keyfob has control permissions.
SOS Alarm	If enabled, the SOS alarm messages will be pushed when an alarm event is detected.
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.
Cloud Update	Update online. If the latest version is detected, you need to tap **Update** on the app, and then press any button on the keyfob to update the keyfob.
Delete	Delete the online peripheral. Go to the hub screen, select the peripheral from the list, and then swipe left to delete it.

6 Using the Keyfob

Maximum connection distance between the keyfob and the hub is 1,500 meters. This distance is reduced by walls, inserted floors and any objects hindering the signal transmission.

After the accessories have been added on the hub, you can operate on the keyfob.

- Press and once at the same time to connect with the hub.
- Press once to enable the away mode, and then all the accessories in the area will be armed.

  Press twice if the **System Integrity Check** is enabled in the hub.
- Press once to enable the home mode, and then the selected accessories in the area will be armed.
- Press once to enable the disarm mode, and then all the accessories in the area will be disarmed.
- Press once to enable SOS.

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