Wireless Glass Break Detector

User Manual



ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD. V1.0.2

Foreword

General

This manual introduces the installation, functions and operations of the wireless glass break detector (hereinafter referred to as the "detector"). 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
V1.0.2	• Updated the technical specification. • Updated the app software and hub software version.	November 2026
V1.0.1	Added EN certifications	March 2024
V1.0.0	First release.	June 2023

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 detector, hazard prevention, and prevention of property damage. Read carefully before using the detector, 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

Foreword I
Important Safeguards and Warnings III
1 Introduction 1
1.1 Overview 1
1.2 Technical Specifications 1
2 Checklist 4
3 Design 5
3.1 Appearance 5
3.2 Dimensions 6
4 Adding Detector to Hub 7
5 Installation 8
5.1 Installing Detector 8
5.2 Field of Installation 10
5.3 Installation Distance and Glass Types 12
6 Configuration 13
6.1 Viewing Status 13
6.2 Configuring the Detector 14
Appendix 1 Security Commitment and Recommendation 19

1 Introduction

1.1 Overview

The wireless glass break detector detects breakage and triggers alarm for multiple types of glasses. It triggers alarm when the detector recognizes the required frequency of broken glass (low-frequency and subsequent high-frequency glass break sounds). The detector can therefore reduce false positives caused by noise interference in the environment. It is also sufficient to keep families safe from more intrusion scenarios, through the use of 2 external extension inputs for connecting third-party wired detectors.

1.2 Technical Specifications

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

Table 1-1 Technical specifications

Type	Parameter	Description
Port	Alarm Input	2 (NO/NC)
	Microphone	Highly-sensitive omnidirectional microphone
Function	Button	1 × power button
	Remote Update	Cloud update
	Low Battery Detection	Yes
	Battery Level Display	Yes
	Tamper	Yes
	Signal Strength	Signal strength detection
Technical	Detection Range	Max. 9 m (29.53 ft)
	Specification	Glass type: Tempered, double-glazed, laminated, wired, plate and float Glass thickness: 2.4 mm–6.4 mm (0.09"–0.25") Glass size: 0.3 m × 0.3 m to 3 m × 3 m (0.98 ft × 0.98 ft to 9.84 ft × 9.84 ft)
	Test Mode	Yes
	LED Indicator	1 × green alarm indicator
	Scenario	Indoor
	Max. Operating Current	45 uA

Type	Parameter	Description
	Alarm Current	50 mA
Wireless	Carrier Frequency	• DHI-ARD512-W2(868): 868.0 MHz–868.6 MHz • DHI-ARD512-W2(433): 433.1 MHz–434.6 MHz • DHI-ARD512-W2(915): 915 MHz–928 MHz
	Transmitter Power (EIRP)	• DHI-ARD512-W2(433): Limit 10 mW • DHI-ARD512-W2(868): Limit 25 mW • DHI-ARD512-W2(915): Limit 1 W
	Communication Mechanism	Two-way
	Communication Distance	• DHI-ARD512-W2(433): 1,200 m (3,937.01 ft) • DHI-ARD512-W2(868): 1,600 m (5,249.34 ft) • DHI-ARD512-W2(915): 1,600 m (5,249.34 ft)
	Encryption Mode	AES128
	Frequency Hopping	Yes
General	Power Supply	1 × CR123A battery
	Battery Model	CR123A
	Battery Life	3 years (The external input type is NO) 1 year (Both external sensors are enabled, and the input type is NC)
	Power Consumption	Max. 150 mW
	Operating Temperature	–10 °C to +55 °C (+14 °F to +131 °F) (indoor)
	Operating Humidity	10%–90% (RH)
	Product Dimensions	107.8 mm × 34.5 mm × 24.8 mm (4.24" × 1.36" × 0.98")
	Net Weight	45 g (0.10 lb)
	Gross Weight	130 g (0.29 lb)
	Installation	Surface mount
	Certifications	CE
	Casing	PC and ABS
	Packaging Dimensions	95 mm × 43 mm × 139 mm (3.74" × 1.69" × 5.47")
	Color	White

Type	Parameter	Description		
	Anti-corrosion	Basic protection		
	Certifications	DHI-ARD512-W2(433): CE	DHI-ARD512-W2(868): EN 50131-1:2006+A1:2009+A2:2017+A3:2020 EN 50131-6:2017 EN 50131-5-3:2017 EN 50131-2-7:2012 Security Grade 2 Environmental Class II	DHI-ARD512-W2(915): CE

2 Checklist

Figure 2-1 Checklist

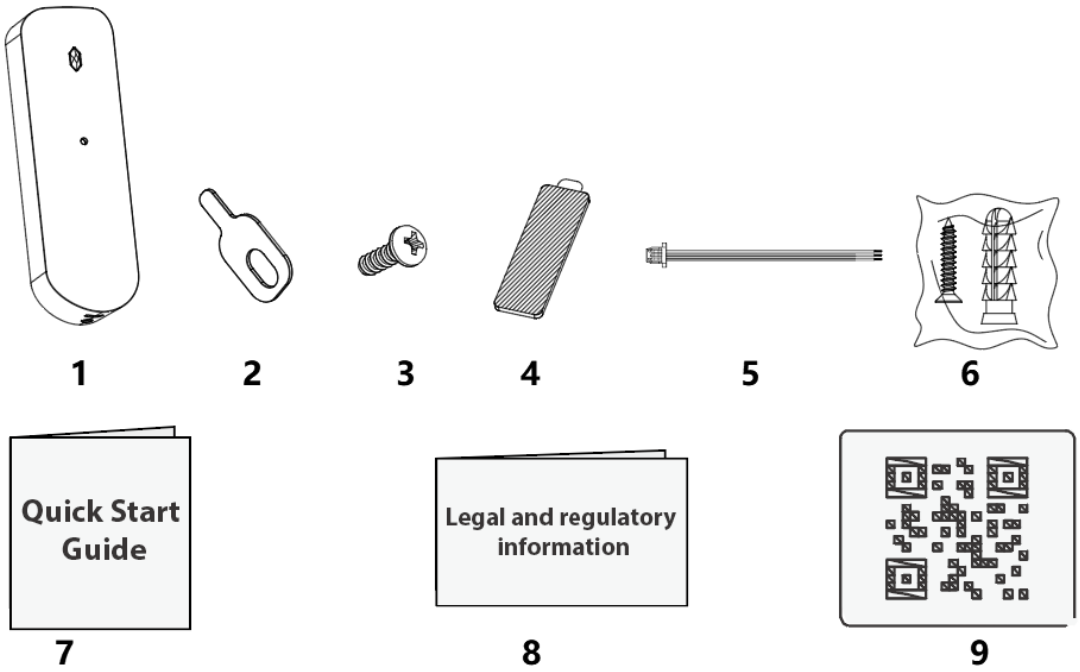


Table 2-1 Checklist

No.	Item Name	Quantity	No.	Item Name	Quantity
1	Wireless glass break detector	1	6	Screw kit	1
2	Ejection pin	1	7	Quick start guide	1
3	Screw	1	8	Legal and regulatory information	1
4	Double-faced tape	1	9	QR code	1
5	Patch cord	1	—	—	—

3 Design

3.1 Appearance

Figure 3-1 Appearance

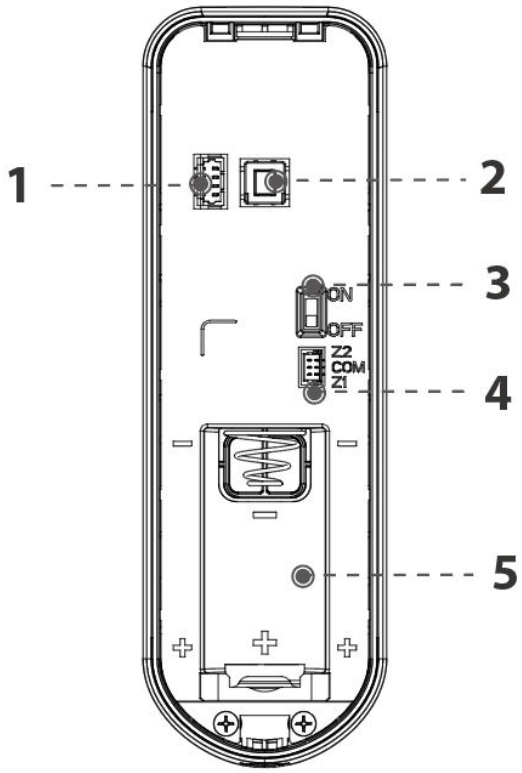


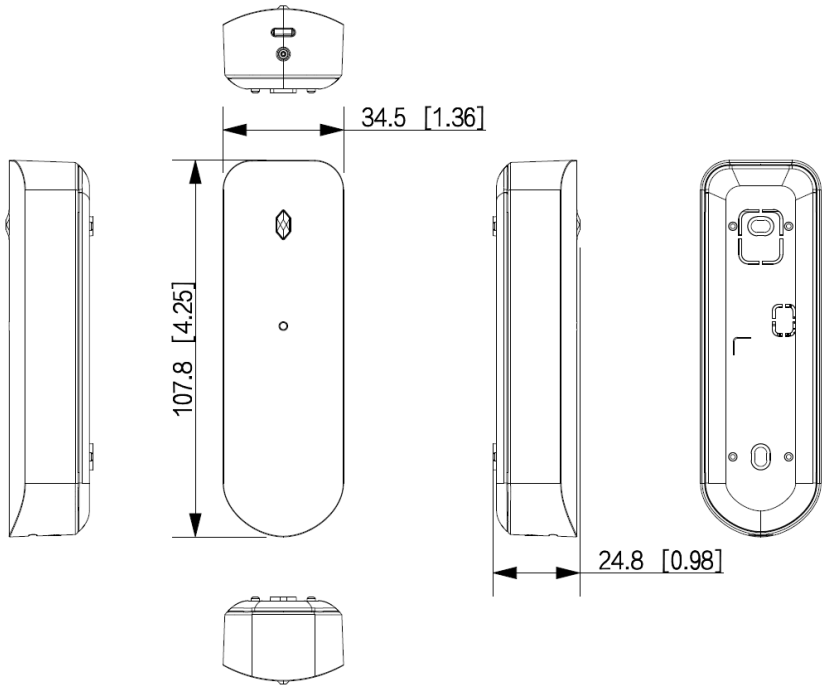
Table 3-1 Port description

No.	Name	Description
1	Serial Port	Used for serial port commissioning.
2	Tamper Switch	The alarm is activated when the device is detached.
3	On/Off Switch	Turn on or turn off the device.
4	Alarm Input	To connect alarm input devices. • Z2: Wire to the white cord of the patch cord. • COM: Wire to the black cord of the patch cord. • Z1: Wire to the red cord of the patch cord. The patch cord is included in the package of the device.

No.	Name	Description
5	Battery Compartment	Holds the cells securely and powers the device it is attached to.

3.2 Dimensions

Figure 3-2 Dimensions (Unit:mm [inch])



4 Adding Detector to Hub

Background Information

Before you connect detector 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 2.2.0 or later, and the hub is V2.000.0000006.0.R.250704 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 detector.

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

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

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

Step 5 Wait for the pairing.

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

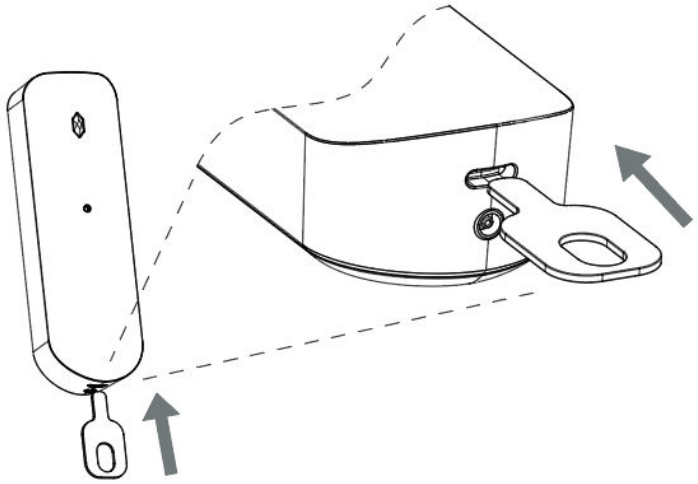
5 Installation

5.1 Installing Detector

Procedure

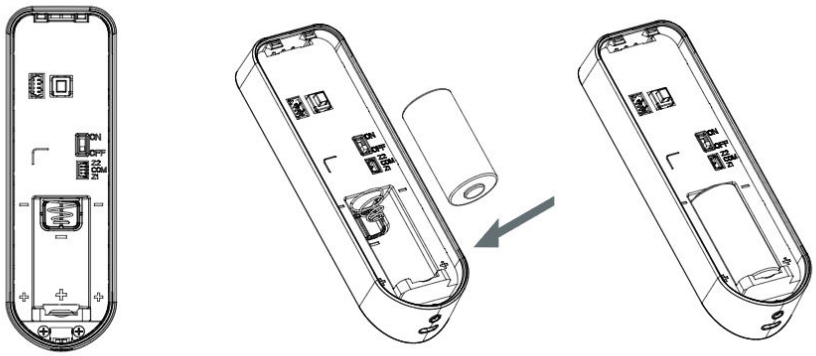
Step 1 Use an ejection pin to open the back cover.

Figure 5-1 Open back-cover



Step 2 Remove the protective film of the battery, and insert the battery into the compartment in a manner that matches it polarities.

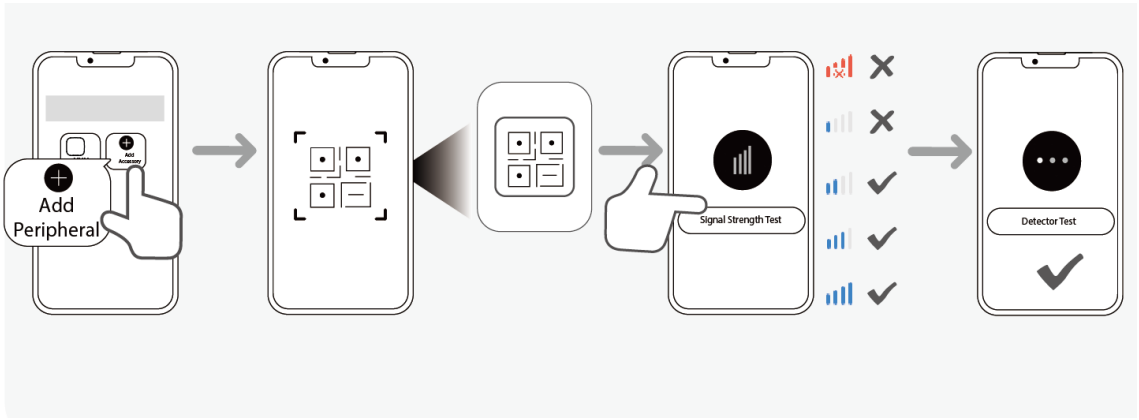
Figure 5-2 Remove battery



Step 3 Add the Detector to the Hub, and install the Detector to a recommended location to test the signal strength and detector strength in that place.

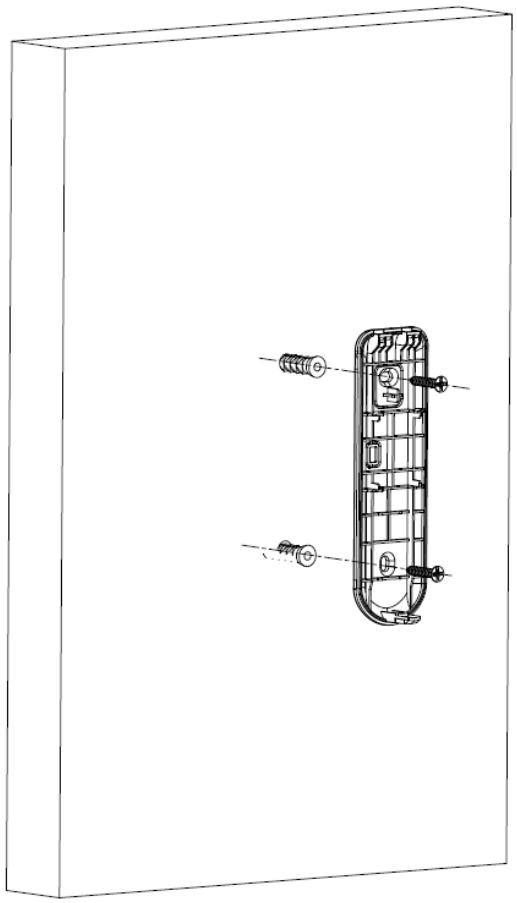
Make sure that the device needs to pass both detector test and signal strength test before going to the next step of installation.

Figure 5-3 Test



Step 4 Fix the back cover onto the wall.

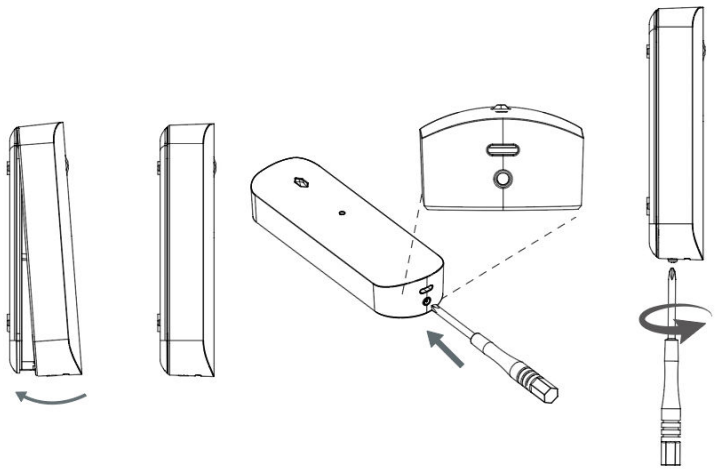
Figure 5-4 Wall-mount



Step 5 Fix the entire Detector onto the wall.

Step 6 (Optional) Tighten the screws.

Figure 5-5 Integrated device



5.2 Field of Installation

Make sure that there is no object in between that partially or fully obscuring the detector and the glass.

Installed on the Opposite Wall

Figure 5-6 Opposite wall

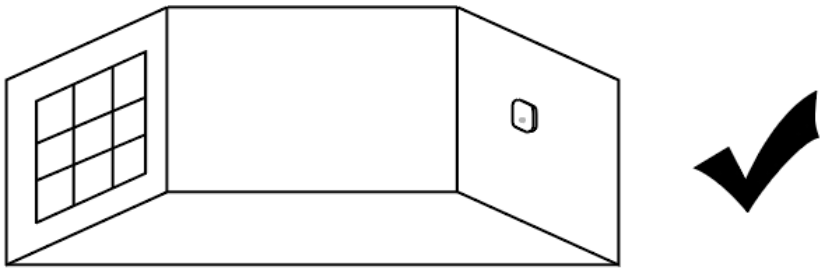
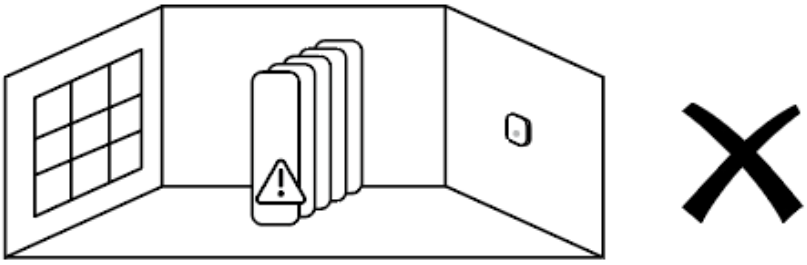
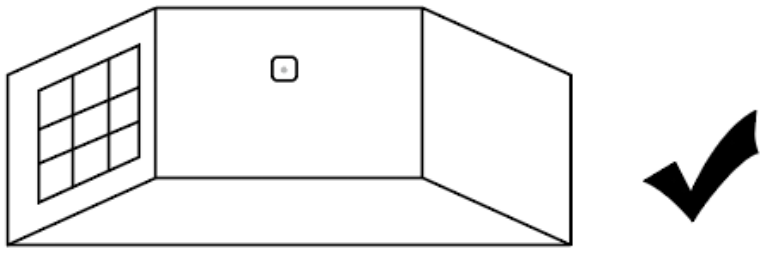


Figure 5-7 Obstacle



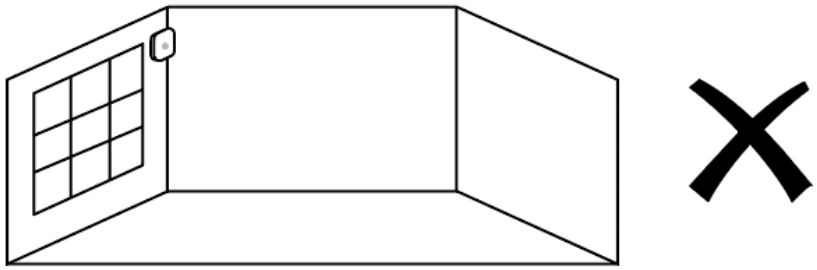
Installed on the Adjacent Wall (Recommended)

Figure 5-8 Adjacent wall



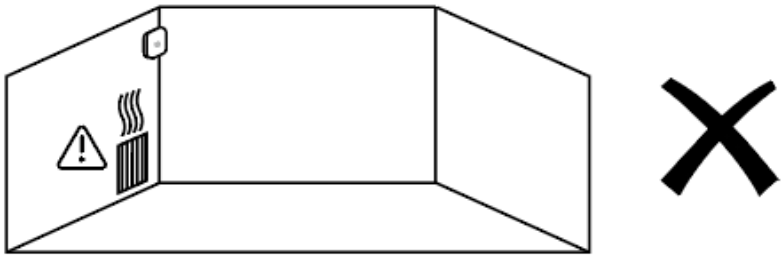
Installed on the Same Wall (Not Recommended)

Figure 5-9 Same wall



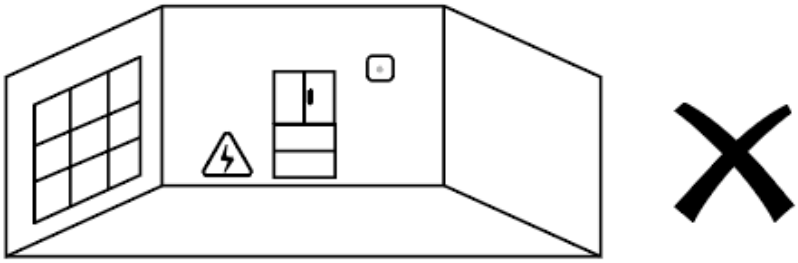
Installed Near Ventilation Devices (Not Recommended)

Figure 5-10 Ventilation



Installed Near Strong Current Devices (Not Recommended)

Figure 5-11 Strong current devices



5.3 Installation Distance and Glass Types

- For ordinary glass with a dimension of 3 m × 3 m, the recommended installation distance between the detector and the tested glass should be less than 6 m.
- For plate glass, the recommended installation distance between the detector and the tested glass should be less than 6 m.

6 Configuration

6.1 Viewing Status

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

Table 6-1 Status

Parameter	Value
Temporary Deactivate	The status for whether the functions of the detector are enabled or disabled. •  : Enable. •  : Only disable tamper alarm. •  : Disable.
Temperature	The temperature of the environment.
Signal Strength	The signal strength between the hub and the detector. • : Low. •  : Weak. •  : Good. •  : Excellent. •  : No.
Battery Level	The battery level of the detector. •  : Fully charged. •  : Sufficient. •  : Moderate. •  : Insufficient. •  : Low.

Parameter	Value
Tamper Status	Anti-tampering status of the detector.
Online Status	Online and offline status of the detector. • : Online. • : Offline.
Entering Delay Time	Entrance delay time.
Exiting Delay Time	Exit delay time.
Sensitivity	The sensitivity level of glass break detection. The higher the value, the easier the breaking is detected.
24 H Protection Zone Status	Active status of the 24 h protection zone. • : Enable. • : Disable.
Transmit through Repeater	The status of whether the detector forwards its messages to the hub through the repeater.
External Input	View device channel status of external input 1 and external input 2. You need to enable **External Detector Config** function in advance.
Program Version	The program version of the detector.

6.2 Configuring the Detector

On the hub screen, select the detector from the peripheral list, and then tap on the **Device Details** screen to configure the parameters.

Table 6-2 Parameter description

Parameter	Description
Device Configuration	• View name, type, SN and device model of the detector. • Edit device name, and then tap **Save** to save configuration.
Area	Select the area to which the detector is assigned.
Zone No.	The zone number assigned to the door detector alarm, which cannot be configured.

Parameter	Description
Temporary Deactivate	• Tap **Enable** , and then the function of the siren will be enabled. **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 function of the siren will be disabled.
LED Indicator	**LED Indicator** is enabled by default. If **LED Indicator** is disabled, the LED indicator will remain off regardless of whether the detector is functioning normally or not.
24 H Protection Zone	• If **24 H Protection Zone** is enabled, even the system is disarmed, the detector can be armed and detects motion. • If **24 H Protection Zone** is disabled, only when the system is armed, the detector can be armed and detects motion. The detector will not be armed immediately, it will begin before the end of the ping interval of the hub-detector (60 seconds by default). You can go to the hub's screen to configure the ping interval of the hub-detector. For details, see the user's manual of the hub.
Home Mode	Enable the home mode, and then the selected peripherals under the hub will be armed.
Delay Mode under Home Mode	Enable the **Delay Mode under Home Mode**, the selected peripheral under the hub will be armed and the alarm will not be triggered until the end of customized delay time. Only enable **Home Mode** first can **Delay Mode under Home Mode** take effect.

Parameter	Description
Delay Time	• The system provides you with time to leave or enter the protection zone without alarm. ◇ **Delay Time for Entering Arming Mode** : When you enter the zone, if you do not disarm the system before the delay ends, an alarm will be triggered. Make sure that the delay time for entering arming mode is no longer than 45 seconds in order to comply with EN50131-1. ◇ **Delay Time for Exiting Arming Mode** : When you are in the zone and arm the system, if you do not leave the zone before the delay ends, an alarm will be triggered. • Select from 0 s to 120 s. The arming mode will be effective after the delay time.
Siren Linkage	When an alarm is triggered, the detector will report the alarm events to the hub and alert with siren.
Alarm-video Linkage	When an alarm is triggered, the detector will report the alarm events to the hub and then will be linked with videos.
Video Channel	Select the video channel as needed.

Parameter	Description
External Sensor Config	You can enable or disable the external detectors. After enabling, the external sensor status will be displayed. • External Input 1: ◇ **External Sensor Type** : Select from **Sensor** and **Tamper**. ◇ **External Input Type** : Select from **Normally Open**, **Normally Closed** and **Pulse**. ◇ **24 H Protection Zone** : If is enabled, even the system is disarmed, the detector can be armed and detects motion; If is disabled, only when the system is armed, the detector can be armed and detects motion. The detector will not be armed immediately, it will begin before the end of the ping interval of the hub-detector (60 seconds by default). The function only applies to detectors whose type is **Sensor**. ◇ **Link to Siren** : Alarms will be linked to siren. • External Input 2: The configuration is the same as that in External Input 1.
Sensitivity	Select from low, medium and high. The higher the value is, the more likely to alarm will be triggered.
Over-temperature Alarm	Enable the **Over-temperature Alarm** function, and then the alarm will be triggered when the temperature of the area where the water leak detector is installed is higher or lower than the defined one. Tap next to **Over-temperature Alarm** to enable this function. Scroll left and right on the temperature bar to set the lowest temperature or highest temperature, or tap **+** or **-** to set the temperature ranges.
Signal Strength Detection	Test the current signal strength.

Parameter	Description
Detector Test	Tap **Start Detection** to test the status of the detector. Make sure that you perform he test in the installation location of the detector. 1. When the glass breakage detector receives a command to enter the test mode, the indicator flashes for three consecutive times (0.25 seconds on and 0.25 seconds off every time) to indicate that the detector has entered the test mode. 2. In the test mode, use your fist or rubber ball to pound on the glass (do not break it), and when the LED indicator flashes for 0.5 seconds, indicating that the low-frequency is triggered. If the low-frequency signal is detected again after the indicator lights off, it will be lighted on for another 0.5 seconds. 3. In the test mode, within 10 seconds after low-frequency was triggered, use a metal to pound on the glass (do not break it), or use a simulator to simulate the sound of glass breaking. The LED indicator lights up for 3 seconds to indicate that the high-frequency is triggered. If the test result does meet your expectation, it is recommended to increase or decrease sensitivity in **Sensitivity**.
Transmit Power	• Select from high, low, and automatic. • The higher the transmission power, the farther the signal can travel, but the greater the power consumption. • If you select **Low**, the detector 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**.
Cloud Update	Update online.
Delete	Delete the detector. Go to the hub screen, select the detector from the list, and then swipe left to delete it.

Appendix 1 Security Commitment and Recommendation

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

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

Account Management

1. **Use complex passwords**

   Please refer to the following suggestions to set passwords:

   - The length should not be less than 8 characters;
   - Include at least two types of characters: upper and lower case letters, numbers and symbols;
   - Do not contain the account name or the account name in reverse order;
   - Do not use continuous characters, such as 123, abc, etc.;
   - Do not use repeating characters, such as 111, aaa, etc.

2. **Change passwords periodically**

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

3. **Allocate accounts and permissions appropriately**

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

4. **Enable account lockout function**

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

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

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

Service Configuration

1. **Enable HTTPS**

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

2. **Encrypted transmission of audio and video**

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

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

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

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

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

4. **Change HTTP and other default service ports**

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

Network Configuration

1. **Enable Allowlist**

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

2. **MAC address binding**

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

3. **Build a secure network environment**

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

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

Security Auditing

1. **Check online users**

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

2. **Check device log**

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

3. **Configure network log**

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

Software Security

1. **Update firmware in time**

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

2. **Update client software in time**

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

Physical Protection

It is recommended that you carry out physical protection for devices (especially storage devices), such as placing the device in a dedicated machine room and cabinet, and

having access control and key management in place to prevent unauthorized personnel from damaging hardware and other peripheral equipment (e.g. USB flash disk, serial port).

ENABLING A SMARTER SOCIETY AND BETTER LIVING

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.
Address: No. 1399, Binxing Road, Binjiang District, Hangzhou, P. R. China | Website: www.dahuasecurity.com | Postcode: 310053
Email: dhoverseas@dhvisiontech.com | Tel: +86-571-87688888 28933188