



# **Wireless Glass Break Detector**

## **User's Manual**








# 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.

## Safety Instructions

The following signal words might appear in the manual.

| Signal Words  | Meaning   |
|---|---|
|  DANGER  | Indicates a high potential hazard which, if not avoided, will result in death or serious injury.  |
|  WARNING | Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.                              |
|  CAUTION | Indicates a potential risk which, if not avoided, could result in property damage, data loss, lower performance, or unpredictable result. |
|  TIPS  | Provides methods to help you solve a problem or save you time.  |
|  NOTE  | Provides additional information as the emphasis and supplement to the text.   |

## Revision History

| Version | Revision Content | Release Time |
|---------|------------------|--------------|
| V1.0.0  | First release.   | June 2023    |

## 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 device, hazard prevention, and prevention of property damage. Read carefully before using the device, and comply with the guidelines when using it.

## Operation Requirements



- Make sure that the power supply of the device works properly before use.
- Do not pull out the power cable of the device while it is powered on.
- Only use the device within the rated power range.
- Transport, use and store the device under allowed humidity and temperature conditions.
- Prevent liquids from splashing or dripping on the device. Make sure that there are no objects filled with liquid on top of the device to avoid liquids flowing into it.
- Do not disassemble the device.

## Installation Requirements



### WARNING

- Connect the device to the adapter before power on.
- Strictly 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 device.
- Do not connect the device to more than one power supply. Otherwise, the device might become damaged.



- 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.
- 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 Design.....                                  | 4   |
| 3.1 Appearance.....                            | 4   |
| 3.2 Dimensions.....                            | 5   |
| 4 Adding Detector to Hub.....                  | 6   |
| 5 Installation.....                            | 7   |
| 5.1 Installing Detector.....                   | 7   |
| 5.2 Field of Installation.....                 | 9   |
| 5.3 Installation Distance and Glass Types..... | 11  |
| 6 Configuration.....                           | 12  |
| 6.1 Viewing Status.....                        | 12  |
| 6.2 Configuring the Detector.....              | 13  |
| Appendix 1 Cybersecurity Recommendations.....  | 18  |

# 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<br>Glass thickness: 2.4 mm–6.4 mm (0.09"–0.25")<br>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   |
|           | Alarm Current          | 50 mA   |

| Type                  | Parameter               | Description  |
|-----------------------|-------------------------|--|
| Wireless              | Carrier Frequency       | <ul style="list-style-type: none"> <li>DHI-ARD512-W2(868): 868.0 MHz–868.6 MHz</li> <li>DHI-ARD512-W2(433): 433.1 MHz–434.6 MHz</li> </ul>     |
|                       | Transmit Power          | <ul style="list-style-type: none"> <li>DHI-ARD512-W2(868): Limit 25 mW</li> <li>DHI-ARD512-W2(433): Limit 10 mW</li> </ul>                     |
|                       | Communication Mechanism | Two-way  |
|                       | Communication Distance  | <ul style="list-style-type: none"> <li>DHI-ARD512-W2(868): 1,600 m (5,249.34 ft)</li> <li>DHI-ARD512-W2(433): 1,200 m (3,937.01 ft)</li> </ul> |
|                       | Encryption Mode         | AES128   |
|                       | Frequency Hopping       | Yes  |
|                       | General                 | Power Supply   |
| Battery Model         |                         | CR123A   |
| Battery Life          |                         | 3 years (The external input type is NO)<br>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  |
| Anti-corrosion        |                         | Basic protection   |

## 2 Checklist

Figure 2-1 Checklist

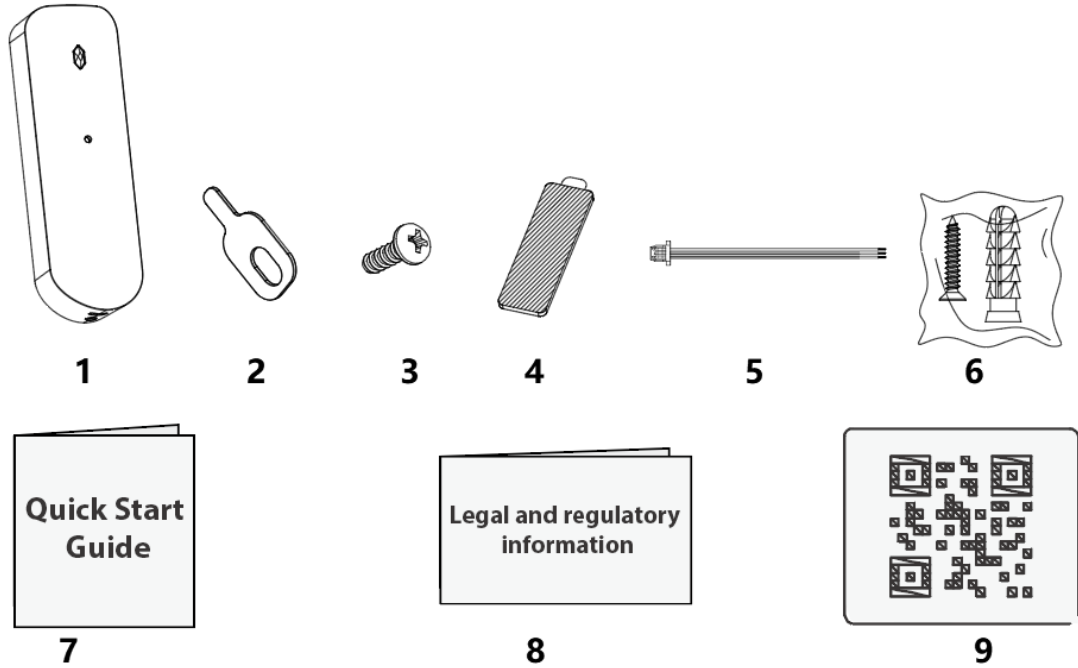


Table 2-1 Checklist

| 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

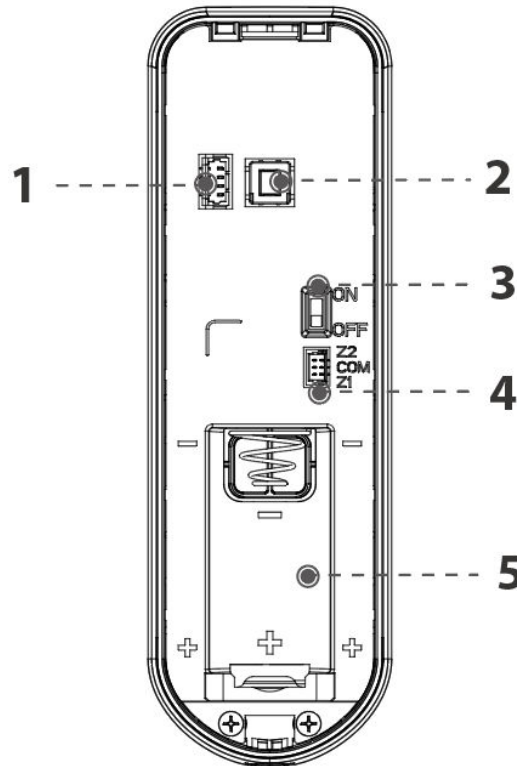

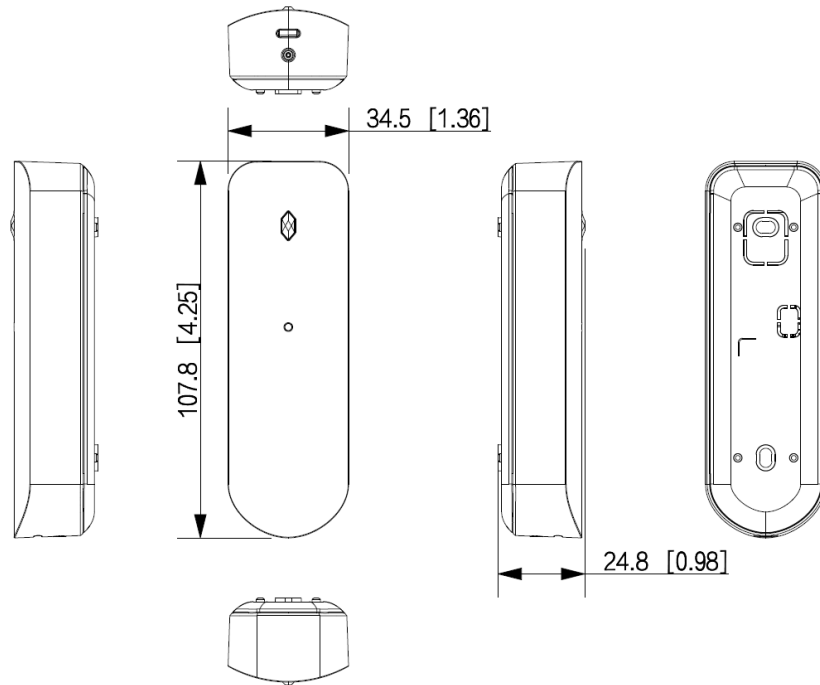


Table 3-1 Port description

| 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         | <p>To connect alarm input devices.</p> <ul style="list-style-type: none"> <li>● Z2 port: Wire to the white cord of the patch cord.</li> <li>● COM: Wire to the black cord of the patch cord.</li> <li>● Z1: Wire to the red cord of the patch cord.</li> </ul> <p></p> <p>The patch cord is included in the package of the device.</p> |
| 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 app is 1.99.420 or later, and the hub is V1.001.0000006.0.R.230404 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**.

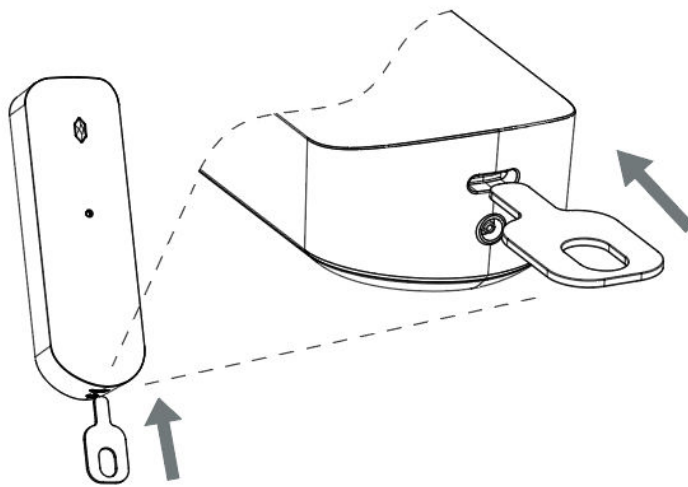
## 5 Installation

### 5.1 Installing Detector

#### Procedure

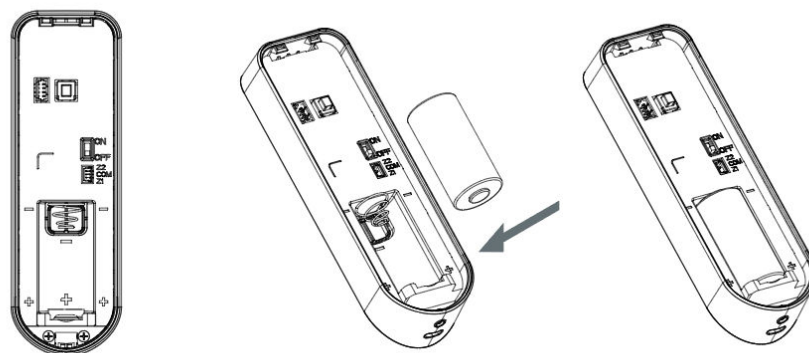
- Step 1 Use an ejection pin to open the back cover.

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 its polarities.

Figure 5-2 Remove battery

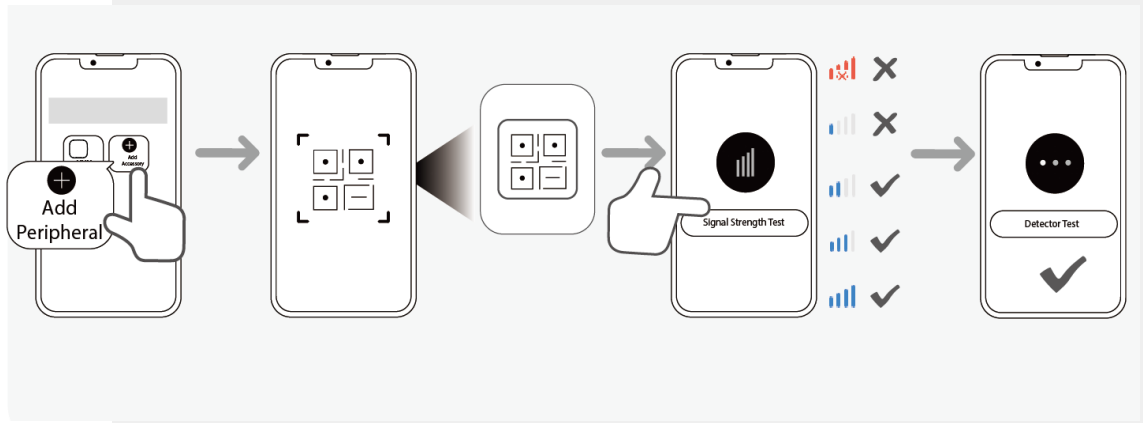


- Step 3 Add the Detector to the Hub, and install the Detector to a recommended location to test the signal strength and detector strength in that place.



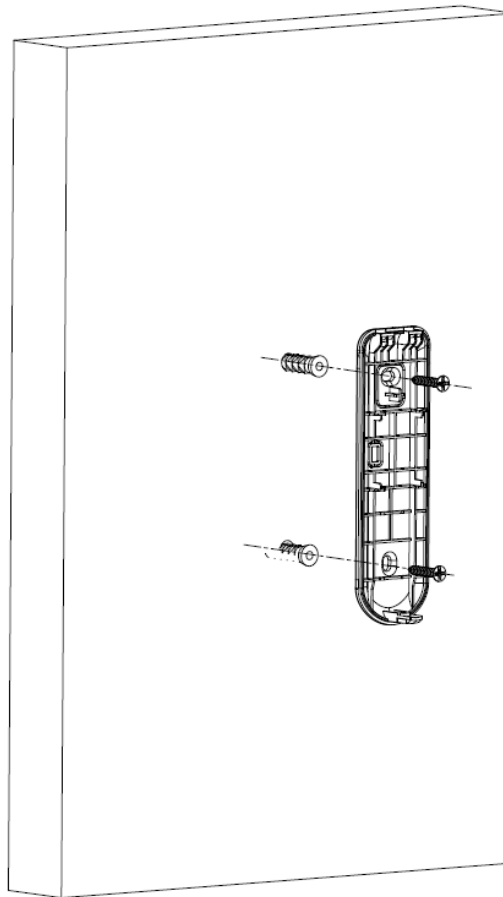
Make sure that the device needs to pass both detector test and signal strength test before going to the next step of installation.

Figure 5-3 Test



**Step 4** Fix the back cover onto the wall.

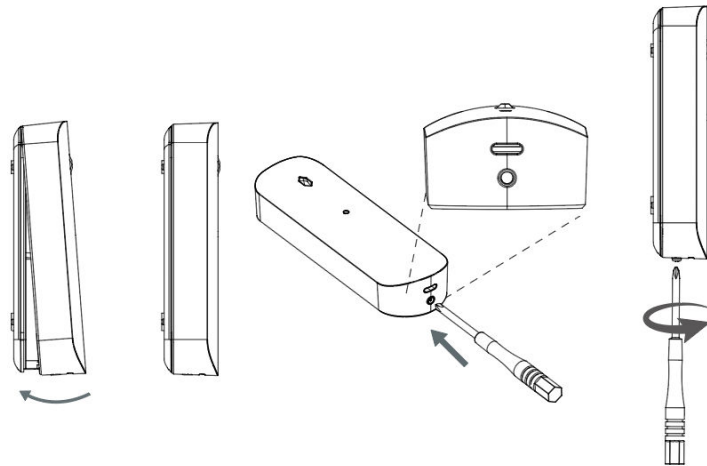
Figure 5-4 Wall-mount



**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 Opposite Wall

Figure 5-6 Opposite

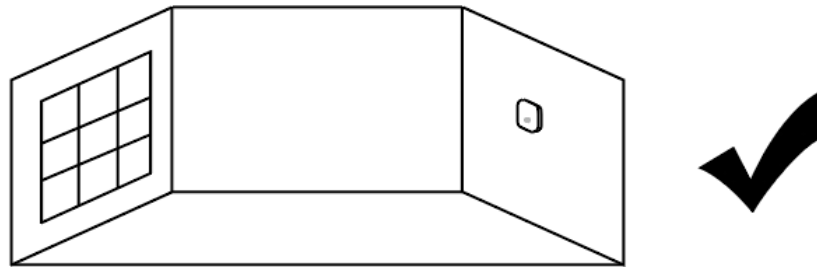
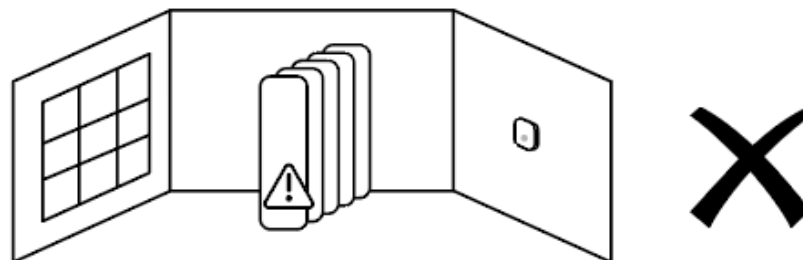
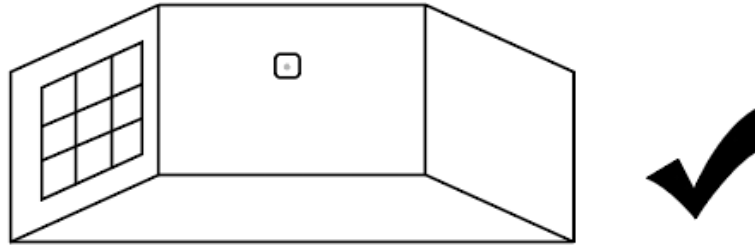


Figure 5-7 Obstacle



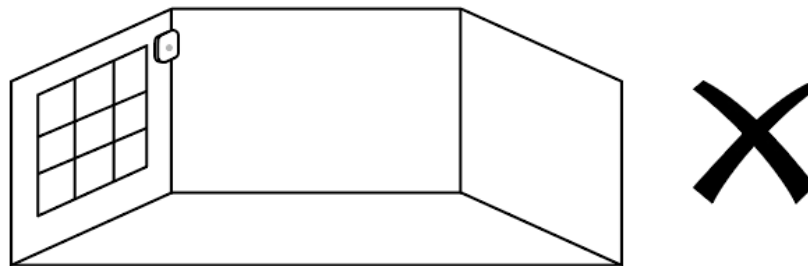
Installed on Adjacent Wall (Recommended)

Figure 5-8 Adjacent



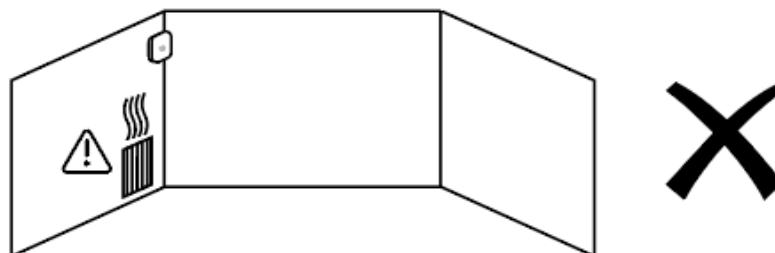
Installed on Same Wall (Not Recommended)

Figure 5-9 Same wall



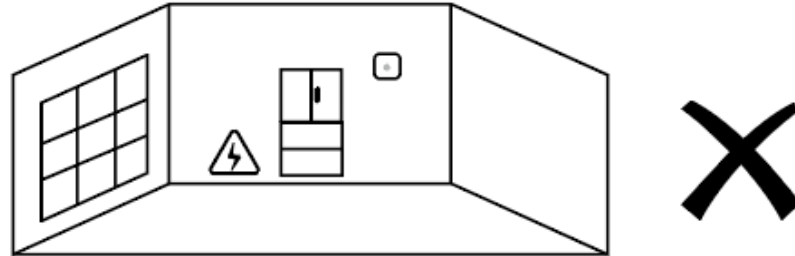
Installed Near Ventilation Devices (Not Recommended)

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. <ul style="list-style-type: none"> <li>●  : Enable.</li> <li>●  : Only disable tamper alarm.</li> <li>●  : Disable.</li> </ul>  |
| Temperature          | The temperature of the environment.  |
| Signal Strength      | The signal strength between the hub and the detector. <ul style="list-style-type: none"> <li>●  : Low.</li> <li>●  : Weak.</li> <li>●  : Good.</li> <li>●  : Excellent.</li> <li>●  : No.</li> </ul>      |
| Battery Level        | The battery level of the detector. <ul style="list-style-type: none"> <li>●  : Fully charged.</li> <li>●  : Sufficient.</li> <li>●  : Moderate.</li> <li>●  : Insufficient.</li> <li>●  : Low.</li> </ul> |
| Tamper Status        | Anti-tampering status of the detector.   |

| Parameter                   | Value  |
|-----------------------------|--|
| Online Status               | Online and offline status of the detector. <ul style="list-style-type: none"> <li> : Online.</li> <li> : Offline.</li> </ul> |
| 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. <ul style="list-style-type: none"> <li> : Enable.</li> <li> : Disable.</li> </ul> |
| 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.<br><br>You need to enable <b>External Detector Config</b> 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 | <ul style="list-style-type: none"> <li>View name, type, SN and device model of the detector.</li> <li>Edit device name, and then tap <b>Save</b> to save configuration.</li> </ul> |
| 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       | <ul style="list-style-type: none"> <li>● Tap <b>Enable</b> , and then the function of the siren will be enabled. <b>Enable</b> is set by default.</li> <li>● Tap <b>Only Disable Tamper Alarm</b>, and then the system will only ignore tamper alarm messages.</li> <li>● Tap <b>Disable</b>, and then the function of the siren will be disabled.</li> </ul>   |
| LED Indicator              | <p><b>LED Indicator</b> is enabled by default.</p>  <p>If <b>LED Indicator</b> is disabled, the LED indicator will remain off regardless of whether the detector is functioning normally or not.</p>   |
| 24 H Protection Zone       | <ul style="list-style-type: none"> <li>● If <b>24 H Protection Zone</b> is enabled, even the system is disarmed, the detector can be armed and detects motion.</li> <li>● If <b>24 H Protection Zone</b> 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).</li> </ul>  <p>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.</p> |
| Home Mode                  | <p>Enable the home mode, and then the selected peripherals under the hub will be armed.</p>   |
| Delay Mode under Home Mode | <p>Enable the <b>Delay Mode under Home Mode</b>, the selected peripheral under the hub will be armed and the alarm will not be triggered until the end of customized delay time.</p>  <p>Only enable <b>Home Mode</b> first can <b>Delay Mode under Home Mode</b> take effect.</p>   |

| Parameter              | Description   |
|------------------------|---|
| Delay Time             | <ul style="list-style-type: none"> <li>● The system provides you with time to leave or enter the protection zone without alarm.               <ul style="list-style-type: none"> <li>◇ <b>Delay Time for Entering Arming Mode</b> : When you enter the zone, if you do not disarm the system before the delay ends, an alarm will be triggered.                   <br/> <br/>Make sure that the delay time for entering arming mode is no longer than 45 seconds in order to comply with EN50131-1.                 </li> <li>◇ <b>Delay Time for Exiting Arming Mode</b> : 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.</li> </ul> </li> <li>● Select from 0 s to 120 s.               <br/> <br/>The arming mode will be effective after the delay time.             </li> </ul>  |
| 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.   |
| External Sensor Config | <p>You can enable or disable the external detectors. After enabling, the external sensor status will be displayed.</p> <ul style="list-style-type: none"> <li>● External Input 1:           <ul style="list-style-type: none"> <li>◇ <b>External Sensor Type</b> : Select from <b>Sensor</b> and <b>Tamper</b>.</li> <li>◇ <b>External Input Type</b> : Select from <b>Normally Open</b>, <b>Normally Closed</b> and <b>Pulse</b>.</li> <li>◇ <b>24 H Protection Zone</b> : 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).               <br/> <br/>The function only applies to detectors whose type is <b>Sensor</b>.             </li> <li>◇ <b>Link to Siren</b> : Alarms will be linked to siren.</li> </ul> </li> <li>● External Input 2: The configuration is the same as that in External Input 1.</li> </ul> |
| Sensitivity            | Select from low, medium and high. The higher the value is, the more likely to alarm will be triggered.  |

| Parameter                 | Description  |
|---------------------------|--|
| Over-temperature Alarm    | <p>Enable the <b>Over-temperature Alarm</b> 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 <input type="checkbox"/> next to <b>Over-temperature Alarm</b> to enable this function.</p> <p>Scroll left and right on the temperature bar to set the lowest temperature or highest temperature, or tap + or - to set the temperature ranges.</p>   |
| Signal Strength Detection | Test the current signal strength.  |
| Detector Test             | <p>Tap <b>Start Detection</b> to test the status of the detector. Make sure that you perform the test in the installation location of the detector.</p> <ol style="list-style-type: none"> <li>1. When the glass breakage detector receives a command to enter the test mode, the indicator flashes for three consecutive times (0.25 second on and 0.25 second off every time) to indicate that the detector has entered the test mode.</li> <li>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 second, 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 second.</li> <li>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.</li> </ol> <p></p> <p>If the test result does not meet your expectation, it is recommended to increase or decrease sensitivity in <b>Sensitivity</b>.</p> |
| Transmit Power            | <ul style="list-style-type: none"> <li>• Select from high, low, and automatic.</li> <li>• The higher the transmission power, the farther the signal can travel, but the greater the power consumption.</li> </ul> <p></p> <ul style="list-style-type: none"> <li>• If you select <b>Low</b>, the detector will enter into reduced sensitivity mode.</li> <li>• We recommend you selecting <b>Low</b> when installing the device to test the signal strength of the installation location, and then adjusting to <b>High</b> or <b>Automatic</b>.</li> <li>• The indicator flashes when setting as <b>Low</b>.</li> </ul>  |
| Cloud Update              | Update online.   |

| Parameter | Description  |
|-----------|--|
| Delete    | <p data-bbox="699 280 933 309">Delete the detector.</p>  <p data-bbox="699 371 1380 436">Go to the hub screen, select the detector from the list, and then swipe left to delete it.</p> |

# 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. 1399, Binxing Road, Binjiang District, Hangzhou, P. R. China | Website: [www.dahuasecurity.com](http://www.dahuasecurity.com) | Postcode: 310053

Email: [dhoverseas@dhvisiontech.com](mailto:dhoverseas@dhvisiontech.com) | Tel: +86-571-87688888 28933188