# Wireless Door Detector

## User Manual

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD. V1.0.0

# Foreword

## General

This manual introduces the installation, functions and operations of the Wireless Door Detector (hereinafter referred to as the "door 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, 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. | August 2025 |

## Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, audio, 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 to: 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 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 door detector, hazard protection, and protection of property damage. Read carefully before using the door 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.
- Do not disassemble the device.

## Installation Requirements

⚠ WARNING

- Connect the device to the adapter before power on.
- Strictly comply with the local electrical safety code and standards, and check whether the power supply is correct before operating the device.
- Do not connect the device to more than one power supply. Otherwise, the device might become damaged.
- Please follow the electrical requirements to power the device.
    - Followings are the requirements for selecting a power adapter.
        - 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.

   - ◇ We recommend using the power adapter provided with the device.
   - ◇ When you select the power adapter, the power supply requirements (such as rated voltage) are subject to the device label.

⚠

- 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

The door detector is a wireless device that includes a sensor. When an armed door is opened, it sends a signal to the hub and triggers an alarm. The device can be easily set up using the DMSS app, available for both iOS and Android phones.

## 1.2 Technical Specifications

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

Table 1-1 Technical specifications

| Type | Parameter | Description | | |
|---|---|---|---|---|
| Port | Indicator Light | 1 × green alarm indicator | | |
| | Button | 1 × power button | | |
| Function | Tamper Alarm | Yes | | |
| | Remote Update | Cloud update | | |
| | Search | Signal strength detection | | |
| | Low Battery Alarm | Yes | | |
| Wireless Parameters | Carrier Frequency | DHI-ARD333-W2 (868S):<br>868.0 MHz–868.6 MHz | DHI-ARD333-W2(S):<br>433.1 MHz–434.6 MHz | DHI-ARD333-W2(915S):<br>915.0-928.0MHz |
| | Communication Distance | DHI-ARD333-W2 (868S):<br>Up to 1,400 m (4,593.18 ft) in an open space | DHI-ARD333-W2 (S):<br>Up to 1,200 m (3,937.01 ft) in an open space | DHI-ARD333-W2 (915S):<br>Up to 1,400 m (4,593.18 ft) in an open space |
| | Communication Mechanism | Two-way | | |
| | Encryption Mode | AES128 | | |
| | Frequency Hopping | Yes | | |
| Peripheral | External Zone | 1-channel external digital input<br>📖<br>1-channel external digital input does not have any certification standards. | | |
| Temperature | Measuring Range | -15 °C to +65 °C (+5 °F to +149 °F) (Indoor) | | |
| | Measuring Precision | ± 1 °C (± 1.8 °F) | | |

<table>
<tr><th>Type</th><th>Parameter</th><th colspan="3">Description</th></tr>
<tr><td></td><td>Resolution</td><td colspan="3">1 °C (33.8 °F)</td></tr>
<tr><td rowspan="4">Technical Parameter</td><td>Sensor</td><td colspan="3">Reed switch</td></tr>
<tr><td>Test Mode</td><td colspan="3">Yes</td></tr>
<tr><td>Scenario</td><td colspan="3">Non-metal doors</td></tr>
<tr><td>Movement Distance</td><td colspan="3">< 40 mm (1.57")</td></tr>
<tr><td rowspan="19">General</td><td>Power Supply</td><td colspan="3">CR123A battery</td></tr>
<tr><td>Battery Voltage</td><td colspan="3">3 VDC</td></tr>
<tr><td>Min. Voltage</td><td colspan="3">1.8 VDC</td></tr>
<tr><td>Battery Low Threshold</td><td colspan="3">2.2 VDC</td></tr>
<tr><td>Battery Restore Threshold</td><td colspan="3">2.6 VDC</td></tr>
<tr><td>Typical Voltage</td><td colspan="3">3 VDC</td></tr>
<tr><td>Low Voltage Value</td><td colspan="3">2.7 VDC</td></tr>
<tr><td>Consumption</td><td colspan="3">Quiescent current 5 uA<br>Max current 60 mA</td></tr>
<tr><td>PS Type</td><td colspan="3">Type C</td></tr>
<tr><td>Battery Life</td><td colspan="3">5 years</td></tr>
<tr><td>Power Consumption</td><td>DHI-ARD333-W2(868S):<br>0.258 W (Max), 0.087 mW (Standby)</td><td>DHI-ARD333-W2(S):<br>0.187 W (Max), 0.072 mW (Standby)</td><td>DHI-ARD333-W2(915S)<br>0.314 W (Max), 0.098 mW (Standby)</td></tr>
<tr><td>Operating Environment</td><td colspan="3">Indoor: –10 °C to +55 °C (+14 °F to +131 °F)<br>Certified temperature: –10°C to +40°C (+14°F to 104 °F)</td></tr>
<tr><td>Operating Humidity</td><td colspan="3">10%–90% (RH)</td></tr>
<tr><td>Product Dimensions</td><td colspan="3">100.2 mm × 20.8 mm × 20.3 mm (3.94" × 0.82" × 0.80")</td></tr>
<tr><td>Packaging Dimensions</td><td colspan="3">110.0 mm × 75.0 mm × 33.0 mm (3.61" × 2.46" × 1.08") (L × W × H)</td></tr>
<tr><td>Installation</td><td colspan="3">Bracket mount</td></tr>
<tr><td>Net Weight</td><td colspan="3">48.7 g (0.11 lb)</td></tr>
<tr><td>Gross Weight</td><td colspan="3">88 g (0.19 lb)</td></tr>
<tr><td>Casing</td><td colspan="3">PC + ABS</td></tr>
<tr><td>Certifications</td><td colspan="2">DHI-ARD333-W2(868S): CE</td><td>DHI-ARD333-W2(S): CE</td><td>DHI-ARD333-W2 (915S): CE</td></tr>
</table>

## 1.3 Detection Performance

An alarm will be triggered when the gap between the door detector and the magnetic stick is wider than the distances shown in the table below.

Figure 1-1 Detection performance

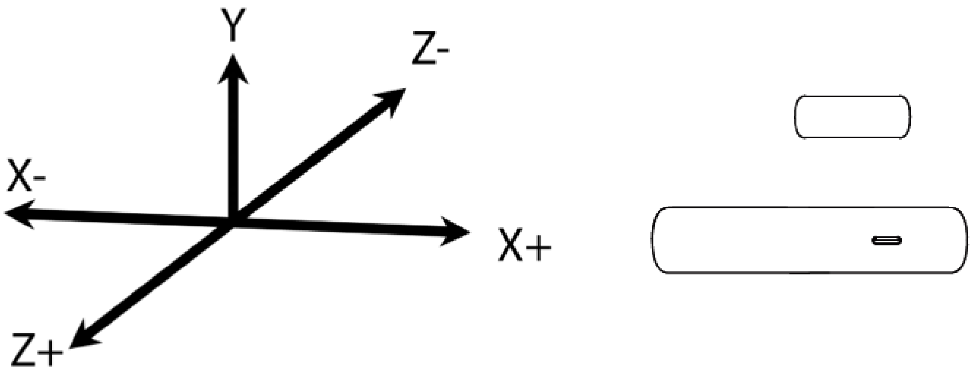


Table 1-2 Detection performance description

| Axes of Operation | Event | Gap between the Door Detector and Magnetic Stick (mm) | Signal Message |
|---|---|---|---|
| Y | Far | 33 | I |
|  | Close | 28 | S |
| X+ | Far | 20 | I |
|  | Close | 18 | S |
| X- | Far | 20 | I |
|  | Close | 18 | S |
| Z+ | Far | 38 | I |
|  | Close | 26 | S |
| Z- | Far | 28 | I |
|  | Close | 26 | S |

- **I** here means intrusion signal; **S** here means stand by signal.
- **Far** means that the door detector is not close to the magnetic stick; **Close** means that the door detector is very close to the magnetic stick.

# 2 Checklist

Figure 2-1 Checklist

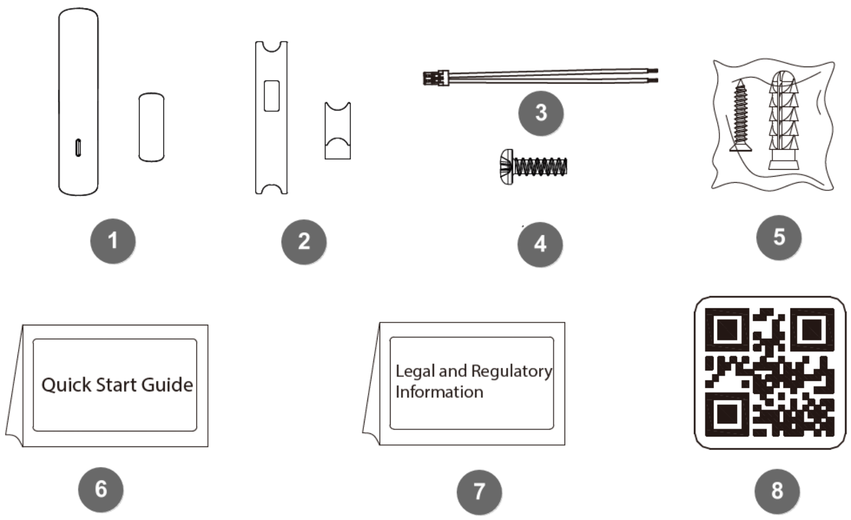


Table 2-1 Checklist

| No. | Item Name | Quantity | No. | Item Name | Quantity |
|---|---|---|---|---|---|
| 1 | Door detector | 1 | 5 | Package of screws | 1 |
| 2 | Double-sided tape | 2 | 6 | Quick Start Guide | 1 |
| 3 | Cable | 1 | 7 | Legal and Regulatory Information | 1 |
| 4 | ST2 × 6 self-tapping screw | 1 | 8 | QR code | 1 |

# 3 Design

## 3.1 Appearance

Figure 3-1 Appearance

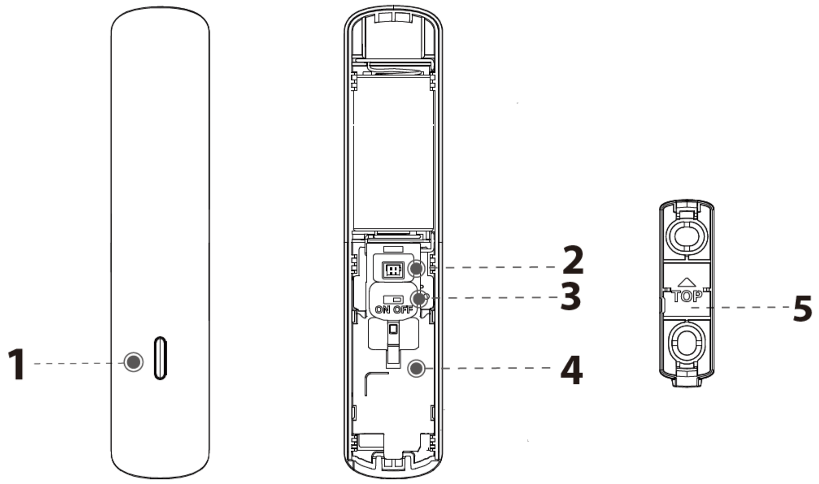
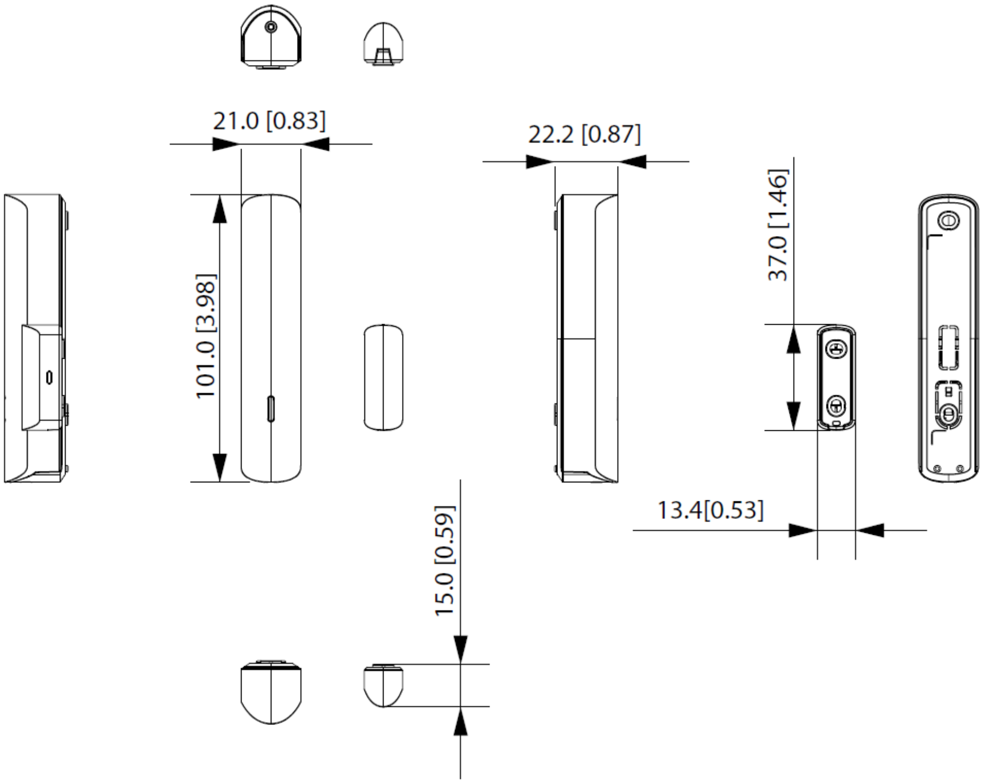


Table 3-1 1

| No. | Name | Description |
|---|---|---|
| 1 | Indicator | ● Flashes green quickly: Pairing mode.<br>● Solid green: Alarm event is triggered. |
| 2 | Peripheral port | Connect the peripheral with the alarm cable. |
| 3 | On/Off switch | Turn on or turn off the door detector. |
| 4 | Tamper switch | When the tamper switch is released, the tamper alarm will be triggered. |
| 5 | Back cover | If the back cover is opened, the tamper alarm will be triggered. |

## 3.2 Dimensions

Figure 3-2 Dimensions (mm [inch])



# 4 Installation

## 4.1 Adding the Door Detector to the Hub

### Background Information

Before you connect door detector to the hub, install the DMSS or DoLynk Care app to 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 version of the DMSS app is V2.00.0030 or later, and the hub is V2.000.0000006.0.R.250603 or later.
- Make sure that the hub has a stable internet connection.
- Make sure that the hub is disarmed.

### Procedure

Step 1 Go to the **Devices** screen of the hub, and then select ⊕ > **Add Peripheral**.

Step 2 Scan the QR code at the bottom of the door detector, and then tap **Next**.

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

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

Step 5 Wait for the pairing.

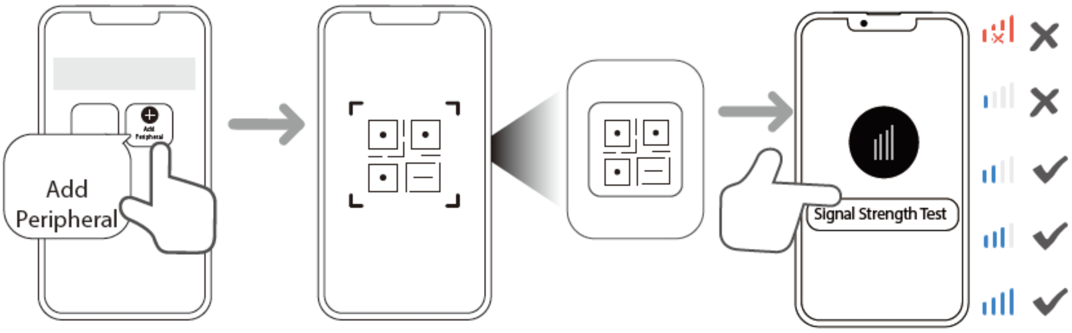
Step 6 Customize the name of the door detector, and select the area, and then tap **Completed**.

## 4.2 Installing the Door Detector

### Prerequisites

Before installation, add the door detector to the hub and check the signal strength of the installation location. We recommend installing the door detector in a place with a signal strength of at least 2 bars.

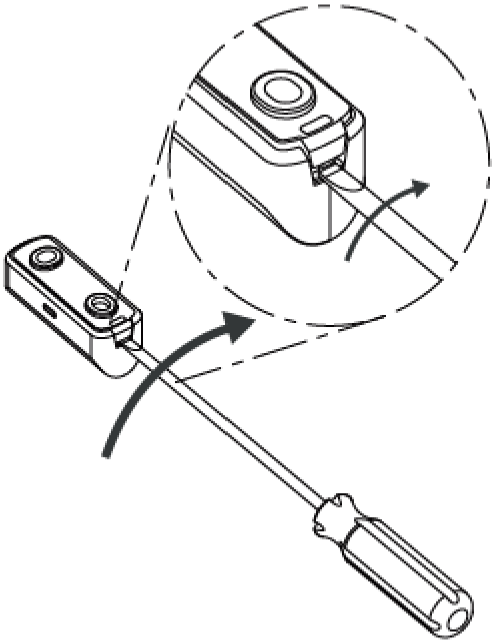
Figure 4-1 Check signal strength



### Procedure

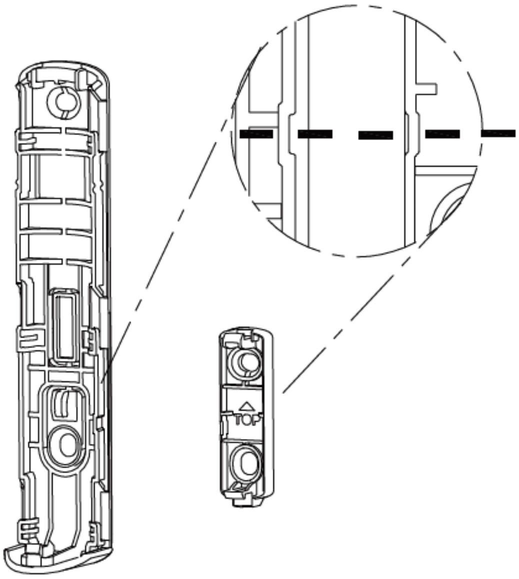
Step 1 Loosen the screw to open the door detector.

Figure 4-2 Open the door detector



Step 2 Take out the attachment panel.

Figure 4-3 Take out attachment panel



Step 3 Drill 4 holes in door 1 and door 2 according to the hole positions of the attachment panel, put the expansion bolts into the holes, and then fix the attachment panels on to the wall with ST3 × 18 mm self-tapping screws.

Figure 4-4 Drill holes

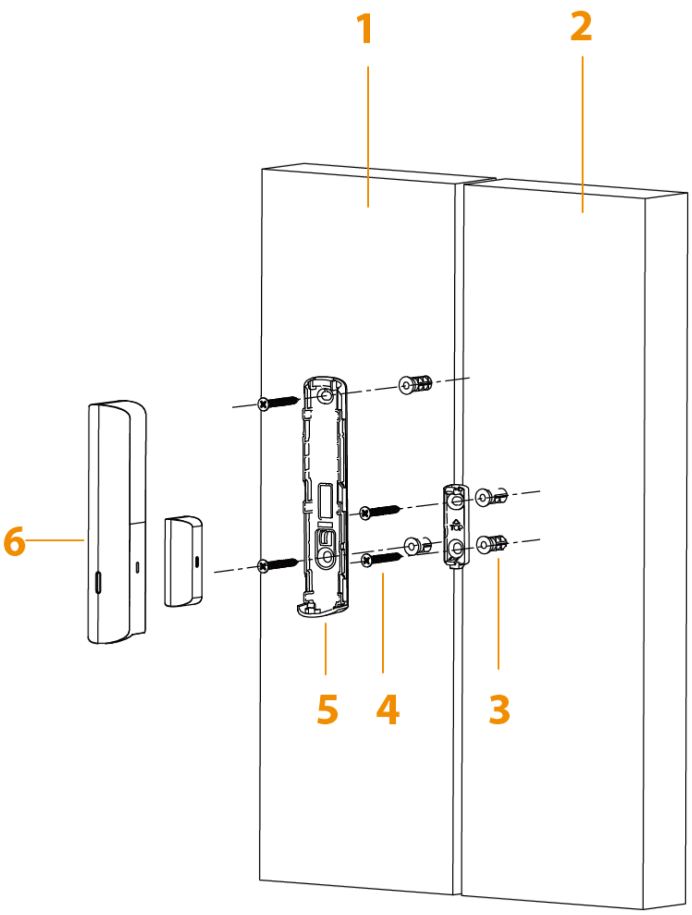
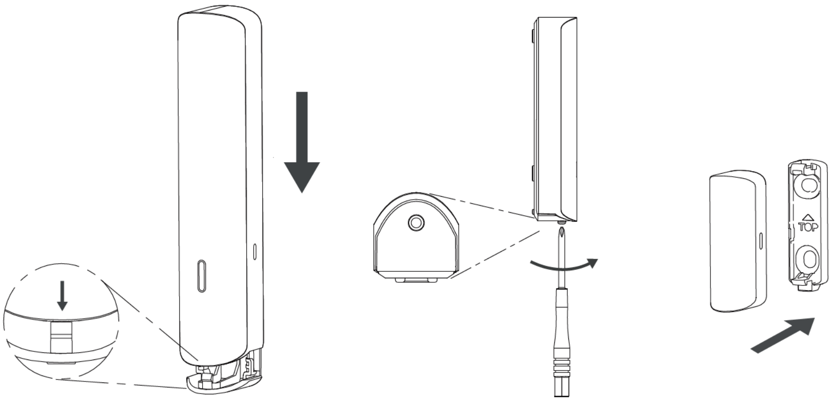


Table 4-1 Installation items

| No. | Item Name | No. | Item Name |
|---|---|---|---|
| 1 | Door 1 | 4 | ST3 × 18 mm self-tapping screw |
| 2 | Door 2 | 5 | Attachment panel |
| 3 | Expansion bolt | 6 | Door detector |

Step 4 Put the door detector into the attachment panel, and then secure it with ST2 × 6 mm self-tapping screws.

Figure 4-5 Fix the detector



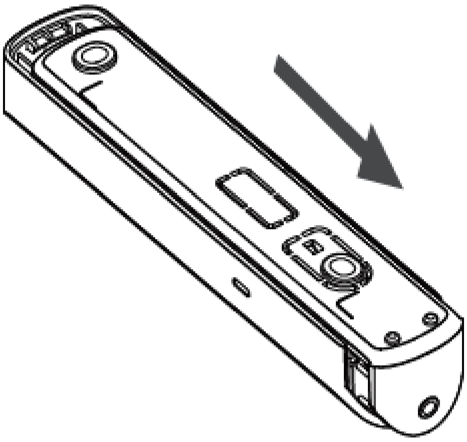
## 4.3 Replacing the battery

If the battery is dead, you need to replace the battery.

### Procedure

Step 1 Open the back cover of the door detector.

Figure 4-6 Open the back cover



Step 2 Replace the battery.

When replacing the battery, make sure that the side marked with "＋" faces the back cover of the devices.

Figure 4-7 Replace the battery

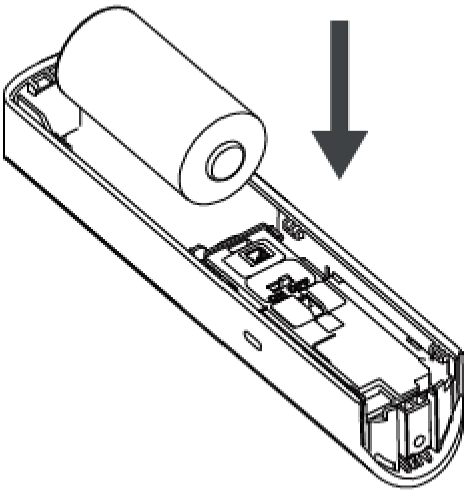
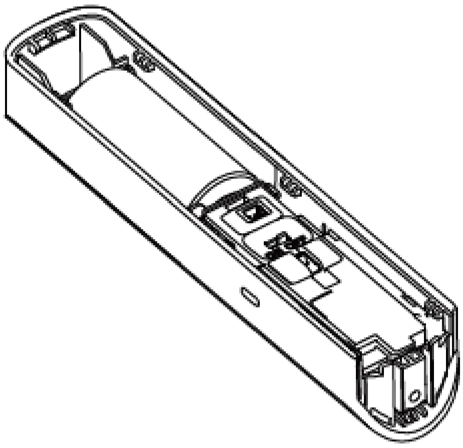


Figure 4-8 Replace completed



Step 3 Close the back cover of the door detector.

# 5 Configuration

You can view and edit general information of the door detector.

## 5.1 Viewing Status

### Detector Icon Description

Introduces the meaning of icons for the door detector. You can view these icons on the **Peripheral** list under the hub screen.

Table 5-1 Device icon description

| Parameter | Icon | Description |
|---|---|---|
| Signal Strength | ▂ | Low |
| | ▂▄ | Weak |
| | ▂▄▆ | Good |
| | ▂▄▆█ | Excellent |
| | 📵 | No signal |
| Battery Level | 🟩 | 100% |
| | 🟩 | 80% |
| | 🟨 | 60% |
| | 🟧 | 40% |
| | 🟥 | 20% |
| Permanent Deactivation | ⊘ | Yes |
| | ⓛ | Lid only |
| Bypass | ⊘ | Yes |
| | ⓛ | Lid only |
| Tamper | ⎿ | Opened. |

## View Detector Status

On the **Devices** screen, select a door detector from the peripheral list to go to the **Overview** screen, and then view the status of the door detector.

Table 5-2 Status

| Parameter | Value |
|---|---|
| + Wired Devices | Click **+ Wired Devices** , and then click **+** to add wired devices.<br>● Device name: Enter the name of the wired device.<br>● Area: Select the area to which the wired device is assigned to.<br>● Type: Select the type of wired device.<br>● Channel: Select the channel of wired device. |
| Device No. | Displays the device number of the door detector. |
| Temperature | Displays the temperature of the environment. |
| Signal Strength | The signal strength between the hub and the door detector. |
| Online Status | Displays online and offline status of the door detector. |
| Battery Level | Displays the remaining battery percentage of the door detector. |
| Permanent Deactivation | The status for whether the permanent deactivation of the door detector is enabled or turned off.<br>● Yes. The permanent deactivation is enabled. Alarm information will not be sent to the alarm hub.<br>● Lid only. All information, except for tamper alarms will be sent to the alarm hub.<br>● No: The permanent deactivation is turned off. All information will be sent to the alarm hub. |
| Bypass | ● Yes. They bypass is enabled.<br>● Lid only. All information, except for tamper alarms will be sent to the alarm hub.<br>● No: All information will be sent to the alarm hub. |
| Tamper | The tamper status of the door detector. The status is triggered when an attempt is made to remove it from its installed position.<br>● Opened.<br>● Closed. |
| Door Status | Open or close status of the door.<br>● Opened.<br>● Closed. |
| Zone Type | ● Displays **Instant** when you set **Zone Type** as **Instant** in **Settings**.<br>● Displays **24 hr** when you set **Zone Type** as **24 hr** in **Settings**.<br>● Displays **Follow** when you set **Zone Type** as **Follow** in **Settings**. |
| Entry Delay Time/Exit Delay Time | Displays the entry and exit delay time when you set **Zone Type** as **Delay** in **Settings**. |

| Parameter | Value |
|---|---|
| Doorbell | - Opened: When the door detector is triggered, the indoor siren gives off a ding dong sound like a doorbell.<br>- Disabled: No sound will be given off when the door detector is triggered. |
| Repeater | The status of whether the door detector forwards peripheral messages to the hub through the repeater. |
| Program Version | The program version of the door detector. |

## 5.2 Configuring the Door Detector

On the **Devices** screen, select a door detector from the peripheral list to go to the **Settings** screen, and then view the status of the door detector.

Table 5-3 Parameter description

| Parameter | Description |
|---|---|
| Device | - View door detector name, type, SN and device model.<br>- Edit door detector name, and then tap **Save** to save configuration. |
| Area | Select the area to which the door detector is assigned. |
| Bypass | - Yes: Bypass is enabled, and information will not be sent to the alarm hub.<br>- Lid only: Tamper only. All information, except for tamper alarms, will be sent to the alarm hub.<br>- No: Bypass is turned off. All information will be sent to the alarm hub.<br>Bypass will automatically restore after disarming. |
| Permanent Deactivation | The status for whether the permanent deactivation of the door detector is enabled or turned off.<br>- Yes: The permanent deactivation is enabled. Alarm information will not be sent to the alarm hub.<br>- Lid only: All information, except for tamper alarms will be sent to the alarm hub.<br>- 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. |
| LED Indicator | **LED Indicator** is enabled by default. Disabling the function will stop the detector from lighting up for alarms, faults, arming, disarming status.<br>If LED Indicator is disabled, the LED indicator will remain off regardless of whether the door detector is functioning normally or not. |

| Parameter | Description |
|---|---|
| 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.<br>Tap ○ next to **Over-temperature Alarm** to enable this function.<br>Scroll left and right on the temperature bar to set the lowest temperature or highest temperature, or tap **+** or **-** to set the temperature ranges. |
| Zone Type | ● Instant: The alarm is triggered immediately upon detection in the armed area.<br>● Delay: The armed detector starts the countdown and does not report alarms even if the alarms are triggered, until the countdown ends.<br>◇ **Delay Time for Entering Arming Mode** : The grace period for entering arming mode. When you enter the zone, and if you do not disarm the system before the delay ends, an alarm will be triggered.<br>◇ **Delay Time for Exiting Arming Mode** : The grace period for exiting arming mode. If you are in the area and do not leave the zone before the delay ends, an alarm will be triggered.<br>You can select from 0 s to 120 seconds.<br>● 24 hr: The detector is always in the armed mode, and reports alarms when triggered..<br>● Follow: Once the area is armed, an immediate alarm will be generated upon detection, provided no delayed zones in the same area have been triggered. If a delayed zone is activated, the alarm will be triggered only after the delay time has expired. When multiple delayed zones are triggered simultaneously within the same area, the alarm follows the shortest delay time among the delayed zones. |
| Home Mode | Enable the **Home Mode**, and then the zone in which the selected detector is assigned to will be armed. |
| Home Mode Delay<br>📖<br>Only available when you select the **Zone Type** as **Delay**, and enable **Home Mode**. | Enable **Home Mode Delay**. The zone in which the selected detector is assigned to will not report alarms even alarms are triggered, until the delay ends. |
| Link Alarm to Siren | When an alarm is triggered, the detector will report the alarm events to the hub and alert with siren. |
| Alarm and Video Linkage | When an alarm is triggered, the detector will report the alarm events to the hub and then will link events. |

| Parameter | Description |
|---|---|
| Video Channel<br>📖<br>It is available after you have enabled **Alarm and Video Linkage**. | Select the linked video channel (s), and these channels store alarm videos when alarms are triggered. |
| Doorbell | When the function is enabled, the indoor siren gives off a ding dong sound like a doorbell. |
| Signal Strength Detection | Test the current signal strength. |
| Detector Test | Detect whether the peripheral works. |
| Transmit Power | ● Select from high, low, and automatic.<br>● The higher the transmission power, the farther the signal can travel, but the greater the power consumption.<br>📖<br>If you select **Low**, and then the door detector will enter reduced sensitivity mode until you select another option. |
| Firmware Update | Tap to view the current firmware version of the door detector. If it is not the latest version, you can update it to the latest. |
| User's Manual | Tap to view the user manual of the door detector. |

# Appendix 1 Security Commitment and Recommendation

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;
   - Stablish 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 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 | Postcode: 310053
Email: dhoverseas@dhvisiontech.com | Tel: +86-571-87688888 28933188