

Wireless Door Detector Plus

User's Manual







Foreword

This manual introduces the installation, functions and operations of the Wireless Door Detector Plus (hereinafter referred to as the "door detector plus"). Read carefully before using the device, and keep the manual safe for future reference.

Safety Instructions

The following categorized signs and words with defined meaning might appear in the Manual.

Signal Words	Description
 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, may 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 a supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.1	Updated technical specifications.	March 2023
V1.0.0	First release.	February 2023

Revision History

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



- 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
1.3 Detection Performance	2
1.3.1 Wide Gap	2
1.3.2 Shock	3
1.3.3 Tilt	3
2 Checklist	5
3 Design	6
3.1 Appearance	6
3.2 Dimensions	7
4 Adding the Door Detector Plus to the Hub	8
4.1 Installing the Door Detector Plus	8
4.2 Replacing the Battery	10
5 Wireless Door Detector Plus Configuration	12
5.1 Viewing Status	12
5.2 Configuring the Door Detector Plus	13
Appendix 1 Cybersecurity Recommendations	16

1 Introduction


1.1 Overview

Wireless Door Detector Plus detects the status of doors and windows, recognizing when they are opening, shocking and tilting. It can connect with wired detectors in one of 3 ways: normally open, normally closed, and pulse. Easy to install and use, all the configurations can be done through the app.

1.2 Technical Specifications

This section contains technical specifications of the door detector plus. 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 switch	
Function	Tamper Alarm	Yes	
	Remote Update	Cloud update	
	Search	Signal strength detection	
	Low Battery Alarm	Yes	
Wireless Parameters	Carrier Frequency	ARD324-W2(868S): 868.0 MHz-868.6 MHz	ARD324-W2(S): 433.1 MHz-434.6 MHz
	Communication Distance	ARD324-W2(868S): Up to 1,200 m (3,937.01ft) in	ARD324-W2(S): Up to 1,000 m (3,280.84 ft) in an open space
	Communication Mechanism	Two-way	
	Encryption Mode	AES128	
	Frequency Hopping	Yes	
Peripheral	External Zone	1-channel external digital input  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)	
Technical Parameter	Sensor	Triaxial accelerometer, reed switch	
	Test Mode	Yes	

Type	Parameter	Description	
	Scenario	Non-metal doors	
	Movement Distance	< 40 mm (1.57")	
General	Power Supply	CR123A*1	
	Consumption	Quiescent current 5 uA Max current 60 mA	
	Battery Life	3 years (If triggered twice a day with a battery efficiency of 70%)	
	Power Consumption	ARD324-W2(868S): Max. 167 mW	ARD324-W2(S): Max. 104 mW
	Operating Environment	Indoor: -10 °C to +55 °C (+14 °F to +131 °F) Certified temperature: -10 °C to +40 °C (+14 °F to +104 °F)	
	Operating Humidity	10%-90% (RH)	
	Product Dimensions	100.2 mm× 20.8 mm× 20.3 mm (3.94" × 0.82" × 0.80")	
	Packaging Dimensions	135.0 mm× 98.5 mm× 27.8 mm (5.31" × 3.88" × 1.09")	
	Installation	Bracket mount	
	Net Weight	70 g	
	Gross Weight	115 g	
	Casing	PC + ABS	
Certifications	ARD324-W2(868S): CE	ARD324-W2(S)CE	

1.3 Detection Performance

1.3.1 Wide Gap

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

Figure 1-1 Detection performance

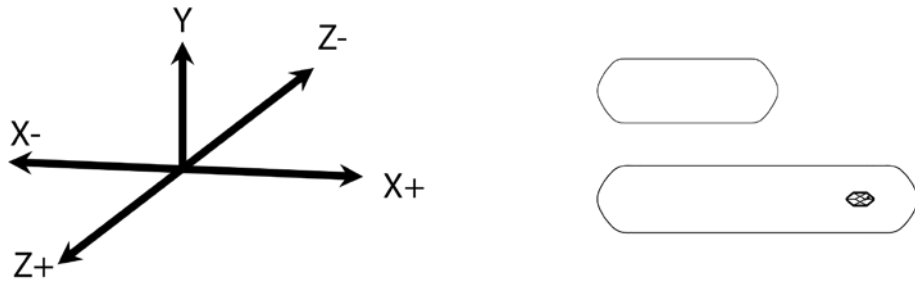


Table 1-2 Detection performance description

Axes of Operation	Event	Gap between the Door Detector Plus 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 plus is not close to the magnetic stick; **Close** means that the door detector plus is very close to the magnetic stick.

1.3.2 Shock

The door detector plus can alarm according to the detected shock intensity. An alarm will be triggered when the shock intensity exceeds the set sensitivity threshold.

After enabling **Ignore Simple Crash Sound**, if the interval between two shocks is less than 1 second, the alarm will be triggered. Otherwise, no alarm will be triggered.

1.3.3 Tilt

An alarm will be triggered if the door detector plus is tilted exceeding the set **Tilted Angle**, and the tilted state is longer than the **Delay Tilt Alarm**. Otherwise, no alarm will be triggered.

Figure 1-2 Tilted angle

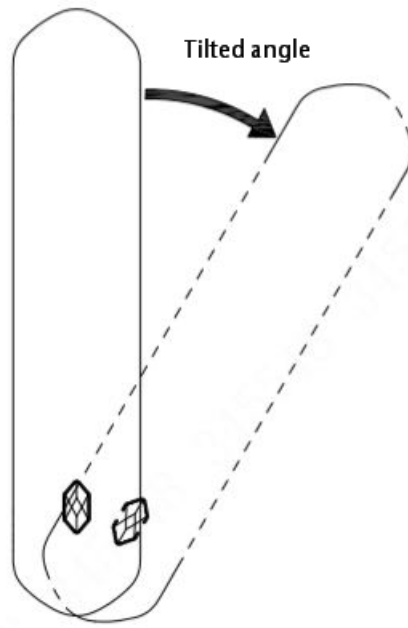
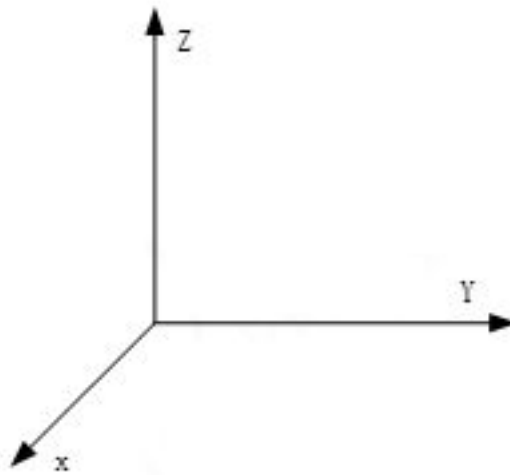


Figure 1-3 Tilt diagram



2 Checklist

Check the package according to the following checklist. If you find device damage or any loss, contact the after-sales service.

Figure 2-1 Checklist

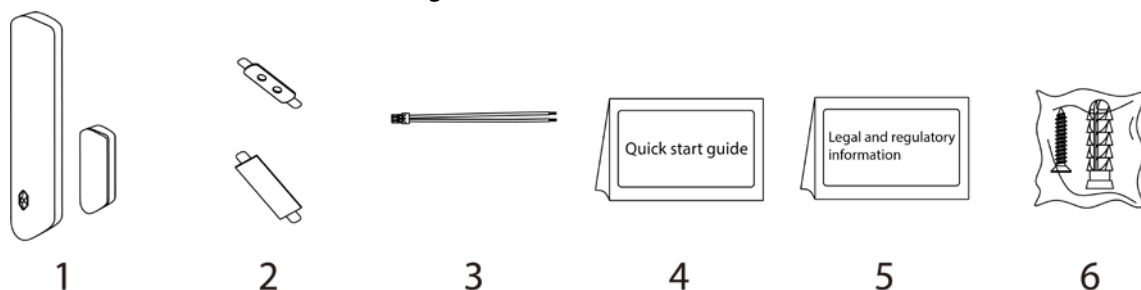


Table 2-1 Checklist

No.	Item Name	Quantity	No.	Item Name	Quantity
1	Door detector plus	1	4	Quick start guide	1
2	Double-sided adhesive tape	2	5	Legal and regulatory information	1
3	Cable	1	6	Screw package	2

3 Design

3.1 Appearance

Figure 3-1 Appearance

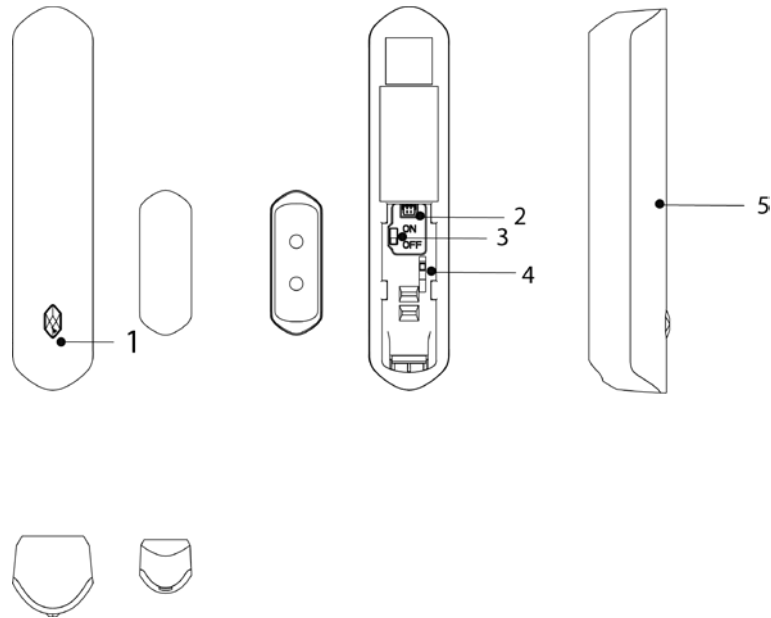
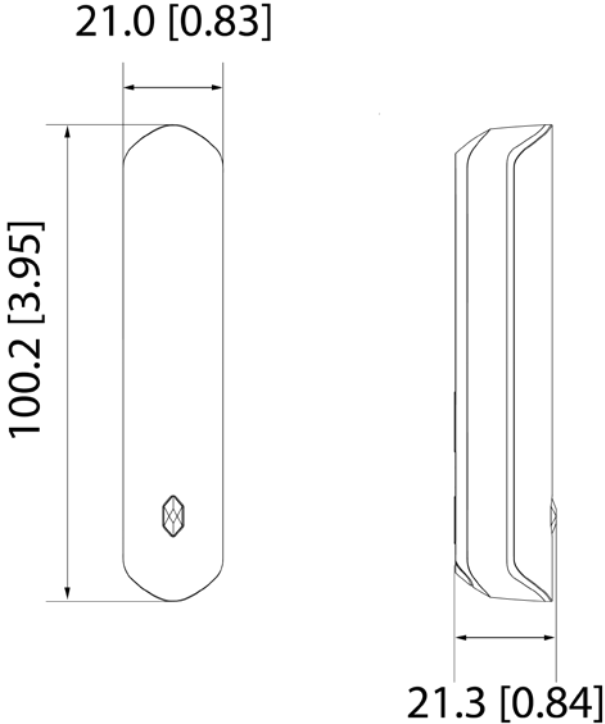


Table 3-1 Structure

No.	Name	Description
1	Indicator	<ul style="list-style-type: none"> Flashes green quickly: Pairing mode or reduced sensitivity mode. Solid green: Alarm event was triggered. Solid green for 2 seconds: Pairing successful. Slowly flashes green for 3 seconds: Pairing failed.
2	Peripheral port	Connect the peripheral with the alarm cable.
3	On/Off switch	Turn on or turn off the door detector plus.
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 Adding the Door Detector Plus to the Hub

Before you connect door detector plus 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 1.99.400 or later, and the hub is V1.001.00000005.0 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.

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

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

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

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

Step 5 Wait for the pairing.

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

4.1 Installing the Door Detector Plus

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.

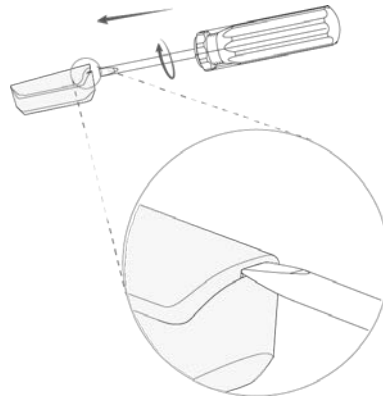


We recommend using expansion screws when installing the door detector. Make sure to align of the magnet with that of the door detector during installation, otherwise normal use of the door detector might be affected.

Procedure

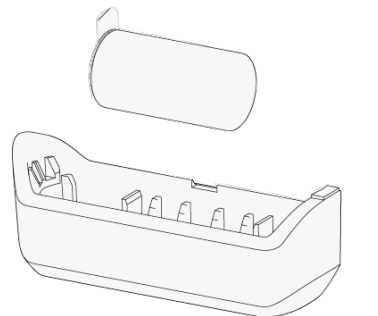
Step 1 Loosen the screw to open the door detector plus.

Figure 4-1 Open the door detector



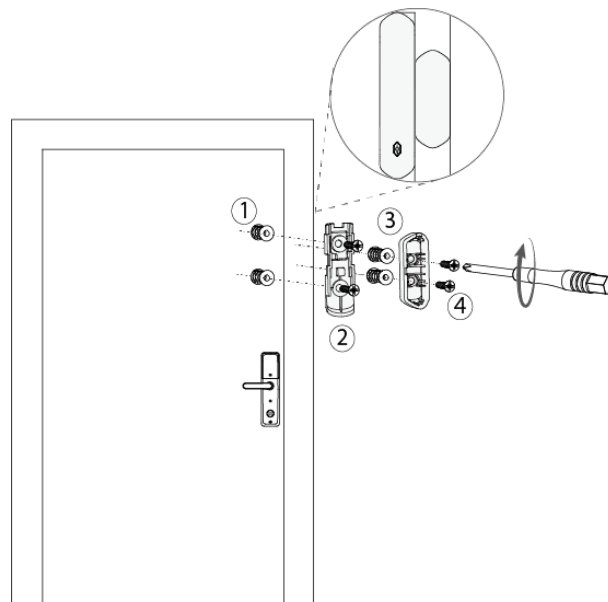
Step 2 Take out the magnet.

Figure 4-2 Take out the magnet



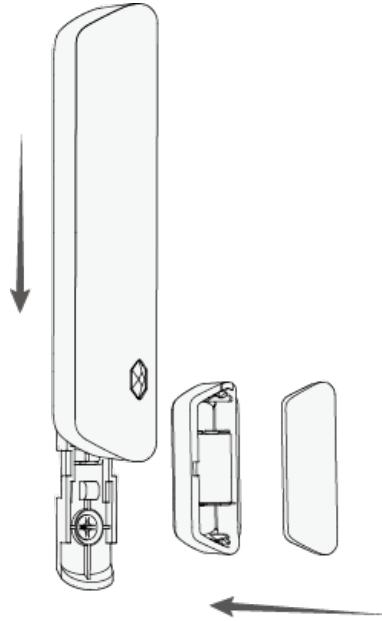
Step 3 Drill 4 holes into the door according to the hole positions of the door detector, and then put the expansion bolts into the holes.

Figure 4-3 Drill holes



Step 4 Close the door detector.

Figure 4-4 Close the door detector

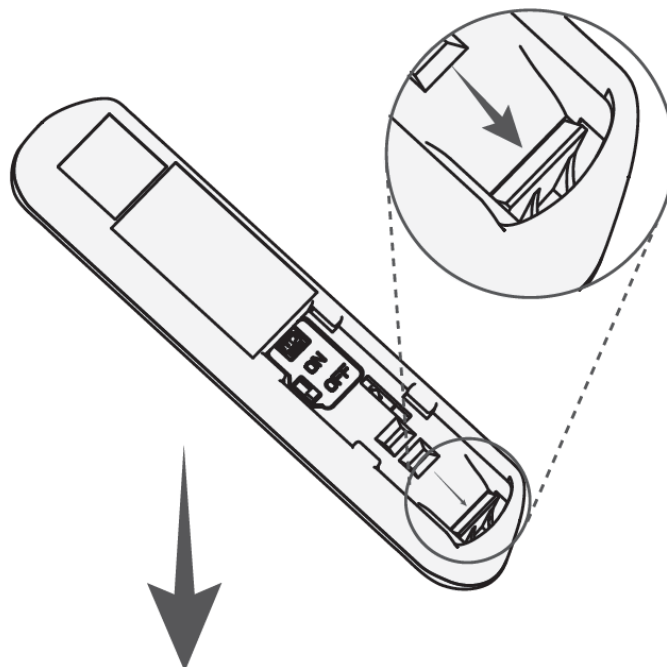


4.2 Replacing the Battery

The battery has been installed when leaving the factory, and the door detector plus can be used directly. If the battery is dead, you need to replace the battery.

Step 1 Open the back cover of the door detector plus.

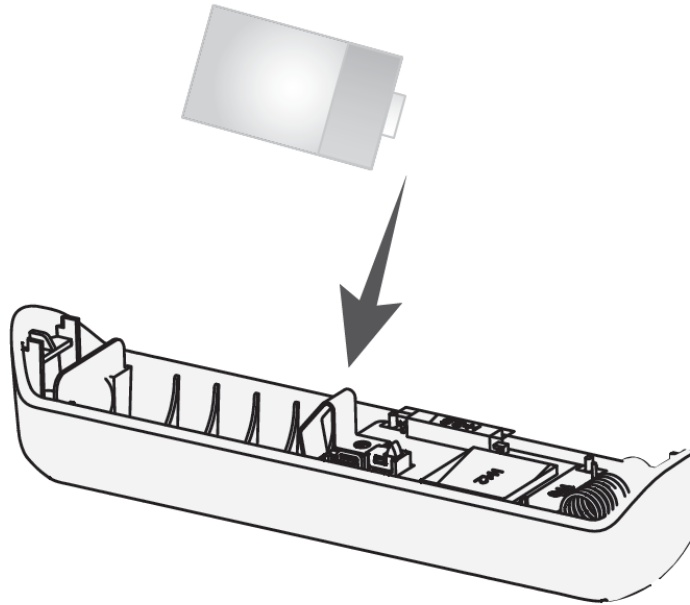
Figure 4-5 Open the back cover



Step 2 Replace the battery.

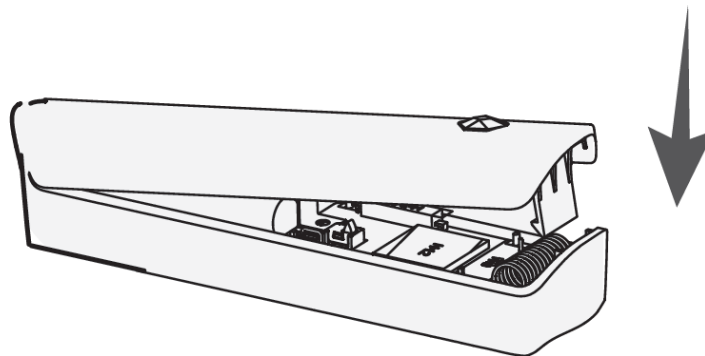
When replacing the battery, make sure that the side marked with "+" faces the back cover of the devices.

Figure 4-6 Replace the battery



Step 3 Close the back cover of the door detector plus.

Figure 4-7 Close the back cover



5 Wireless Door Detector Plus Configuration

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

5.1 Viewing Status








On the hub screen, select a door detector plus from the peripheral list, select **☰** > **Device Details**, and then you can view the status of the door detector plus.



On the hub screen, select a door detector plus from the peripheral list, select **☰** > **Device Channel**, and then you can view the device channel of the door detector plus. You need to enable **External Detector Config** function in advance.

Table 5-1 Status

Parameter	Value
Temporary Deactivate	<p>The status for whether the functions of the repeater are enabled or disabled.</p> <ul style="list-style-type: none"> • : Enable. • : Only disable tamper alarm. • : Disable.
Temperature	The temperature of the environment.
Signal Strength	<p>The signal strength between the hub and the door detector plus.</p> <ul style="list-style-type: none"> • : Low. • : Weak. • : Good. • : Excellent. • : No.
Battery Level	<p>The battery level of the detector.</p> <ul style="list-style-type: none"> • : Fully charged. • : Sufficient. • : Moderate. • : Insufficient. • : Low.
Tamper Status	Tamper status of the door detector plus.
Online Status	<p>Online and offline status of the door detector plus.</p> <ul style="list-style-type: none"> • : Online. • : Offline.
Entering Delay Time	Entrance and exit delay time.
Exiting Delay Time	

Parameter	Value
Door Status	Open or close status of the door. <ul style="list-style-type: none">  : Open.  : Closed.
External Input	On the hub screen, select a door detector plus from the peripheral list, select *** > Device Channel , and then you can view the device channel of the door detector plus.  You need to enable External Detector Config function in advance.
24 H Protection Zone Status	Active status of the 24 h protection zone. <ul style="list-style-type: none">  : Enabled.  : Disabled.
Doorbell Status	Open or close status of the doorbell. <ul style="list-style-type: none">  : Open.  : Close.
Transmit through Repeater	The status of whether the door detector plus forwards peripheral messages to the hub through the repeater.
Program Version	The program version of the door detector plus.

5.2 Configuring the Door Detector Plus








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

Table 5-2 Door detector plus parameters description

Parameter	Description
Device Configuration	<ul style="list-style-type: none"> View device name, type, SN and device model. Edit device name, and then tap Save to save configuration.
Area	Select the area to which the door detector plus is assigned.
Zone No.	The zone No. assigned to the door detector alarm, which cannot be configured.
Temporary Deactivate	<ul style="list-style-type: none"> Tap Enable, and then the function of the door detector plus 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 door detector plus will be disabled.
LED Indicator	LED Indicator is enabled by default. For details on indicator behavior, see "3.1 Appearance". If LED Indicator is disabled, the LED indicator will remain off regardless of whether the door detector is functioning normally or not.
24 H Protection Zone	The peripheral located in the 24 h protection zone is always active whether the security system is configured in the armed mode or not.

Parameter	Description
Home Mode	When the security system is Home armed, the detector will be armed only if its Home Mode is enabled.
Delay Mode under Home Mode	<p>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.</p>  <p>Only enable Home Mode first can Delay Mode under Home Mode take effect.</p>
Delay Time	<ul style="list-style-type: none"> • The system provides you with time to leave or enter the armed zone without alarm. <ul style="list-style-type: none"> ◇ 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.  <p>Make sure that the delay time for entering arming mode is no longer than 45 seconds in order to comply with EN50131-1.</p> <ul style="list-style-type: none"> ◇ 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. <ul style="list-style-type: none"> • Select from 0 s to 120 s.  <p>The arming mode will be effective after the delay time.</p>
Alarm-video Linkage	When an alarm is triggered, the peripherals will report the alarm events to the hub and then will link events.
Video Channel	Select the video channel as needed.
Door Detector Alarm Config	You can enable and disable the door detector alarm. After disabling, no alarm is triggered when the door detector is opened.
External Detector Config	<p>You can enable or disable the external detector. After enabling, the external detector status will be displayed.</p> <ul style="list-style-type: none"> • Link external input to siren • External input type: You can select from Normally Open(default), Normally Closed and Pulse.
Shock Detector Config	<p>You can enable or disable the shock detector. After enabling, you can configure shock detector parameters.</p> <ul style="list-style-type: none"> • Link Shock Alarm to Siren • Sensitivity: You can select from High, Medium (default), and Low. • Ignore Simple Crash Sound: It is disabled by default.  <p>In an installation environment with shock, we recommend you enable Ignore Simple Crash Sound.</p>

Parameter	Description
Tilt Detector Config	<p>You can enable or disable the tilt detector. After enabling, you can configure tilt detector parameters.</p> <ul style="list-style-type: none"> • Link Tilt Alarm to Siren • Tilted Angle: You can select from 5deg, 10deg, 15deg, 20deg, 25deg. The default value is 5deg. When the detector detects the tilted angel exceeds the set value, an alarm is triggered. • Delay Tilt Alarm: You can select from 1s, 2s, 3s, 5s, 10s, 15s, 20s, 30s, 45s, 60s. The default value is 2s. When the detector detects that the tilted angle exceeds the set angle and does not recover beyond the set time, an alarm is triggered.
Chime	After enabling, when the area is disarmed, if the door detector is opened, the indoor siren 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.
Signal Strength Detection	Test the current signal strength.
Detector Test	Detect whether the peripheral works.
Transmit Power	<ul style="list-style-type: none"> • Select from high, low, and automatic. • The higher the transmission power, the farther the signal can travel, but the greater the power consumption.  <ul style="list-style-type: none"> • If you select Low, the door detector plus will enter reduced sensitivity mode until you select another option. • The reduced sensitivity mode is only available when the version of the DMSS app is 1.97 or later, the hub is V1.001.0000000.6.R.211228 or later, and the door detector is V1.000.0000001.0.R.20211203 or later.
Cloud Update	Update online.
Delete	<p>Delete the online peripheral.</p>  <p>Go to the hub screen, select the peripheral 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.