

Wireless Door Detector Plus(Big)

User's Manual



ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.

V1.0.2



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	Meaning
	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
	Indicates a potential risk which, if not avoided, could result in property damage, data loss, reductions in performance, or unpredictable results.
©— [™] TIPS	Provides methods to help you solve a problem or save time.
NOTE	Provides additional information as a supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.2	Revised technical specifications and certificate requirements.	June 2024
V1.0.1	Updated technical specifications.	March 2023
V1.0.0	First release.	February 2023

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: 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
Important Safeguards and WarningsIII
1 Introduction
1.1 Overview
1.2 Technical Specifications
1.3 Detection Performance
1.3.1 Wide Gap
1.3.2 Shock
1.3.3 Tilt
2 Checklist
3 Design
3.1 Appearance
3.2 Dimensions
4 Adding the Door Detector Plus to the Hub
4.1 Installing the Door Detector Plus
4.2 Replacing the Battery 9
5 Wireless Door Detector Plus Configuration
5.1 Viewing Status
5.2 Configuring the Door Detector Plus13
Appendix 1 Security Commitment and Recommendation



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.

Туре	Parameter	Description		
Port	Indicator Light	$1 \times green alarm indicator$		
FUIL	Button	$1 \times power switch$		
	Tamper Alarm	Yes		
Function	Remote Update	Cloud update		
runction	Search	Signal strength detection		
	Low Battery Alarm	Yes		
	Carrier Frequency	DHI-ARD324-W2(868):	DHI-ARD324-W2:	
	Carrier Frequency	868.0 MHz-868.6 MHz	433.1 MHz-434.6 MHz	
	Communication	DHI-ARD324-W2(868):	DHI-ARD324-W2:	
Wireless Parameters	Distance	Up to 1,200 m (3,937.01ft) in an open space	Up to 1,000 m (3,280.84 ft) in an open space	
	Communication Mechanism	Two-way		
	Encryption Mode	AES128		
	Frequency Hopping	Yes		
		1-channel external digital input		
Dawina ka swa l	External Zone			
Peripheral	External Zone	The 1-channel external digital input does not have any		
		certification standards.		
Temperatu	Measuring Range	-15 °C to +65 °C (+5 °F to +14	9 °F) (indoor)	
re	Measuring Precision	± 1 °C (± 1.8 °F)		

Table 1-1 Technical specifications



Туре	Parameter	Description		
	Sensor	Triaxial accelerometer, reed s	switch	
Technical	Test Mode	Yes		
Parameter	Scenario	Non-metal doors		
	Movement Distance	< 40 mm (1.57")		
	Power Supply	CR123A*1		
	Consumption	Quiescent current 5 uA		
	Consumption	Max. current 60 mA		
	Battery Life	3 years (If triggered twice a d of 70%)	ay with a battery efficiency	
	PS Type	Type C		
	Battery Low Threshold	2.6 V		
	Battery Restore Threshold	3 V		
		DHI-ARD324-W2(868):	DHI-ARD324-W2:	
General	Power Consumption	Max. 167 mW	Max. 104 mW	
		Indoor: -10 °C to +55 °C (+14 °F to +131 °F)		
	Operating Environment	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+ABC		
	DHI-ARD324-W2(868)			
	CE			
	EN 50131- 1:2006+A1:2009+A2:2 017+A3:2020			
Certificatio	EN 50131- 6:2017/A1:2021	DHI-ARD324-W2: FCC		
ns	EN 50131-5-3:2017			
	EN 50131-2-6:2008			
	Security Grade 2 (IMQ- SISTEMI DI SICUREZZA)			
	Environmental Class II			



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.

Sample No. Grade	Axes of Operation	Distances In Air		Distances In Iron		Signal	Verdict		
		Lvent	Declared	Verified	Declared	Verified	Message		
		V	Removal	34	34	—	_	I	
		Y	Approach	28	28	—	_	S	
		X+	Removal	20	20	—	—	I	
		X +	Approach	18	18	—		S	
1	2	X-	Removal	20	20	—		I	Р
1	2	^-	Approach	18	18	_		S	
		Z+	Removal	46	46	—		I	
		Ζ+	Approach	40	40	—		S	
		7	Removal	46	46	_		I	
	Z-	Ζ-	Approach	39	39	—		S	
$X \rightarrow X \rightarrow$									
Z+						<u></u>			
		sion signal; S DHI-ARD324-	here means sta W2(868).	and by signa	al.				

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.

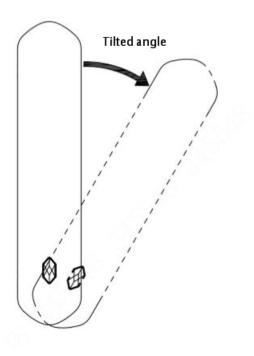
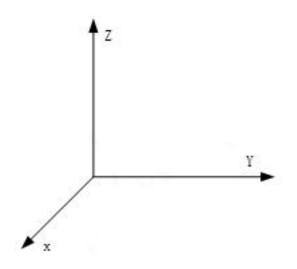


Figure 1-1 Tilted angle







2 Checklist

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

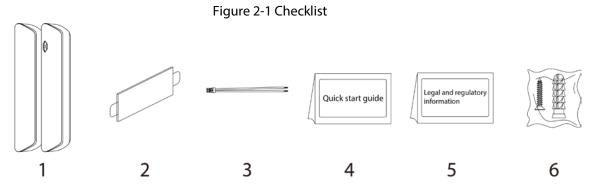


Table 2-1 Checklist

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



3 Design

3.1 Appearance

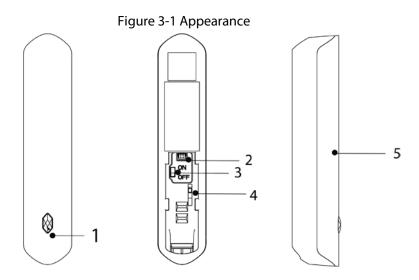


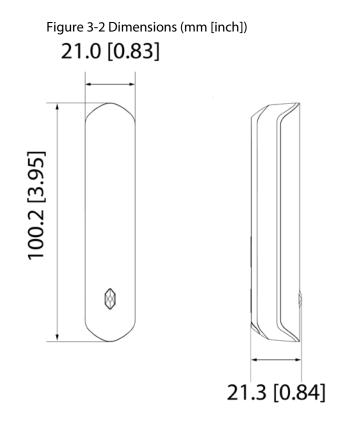


Table 3-1 Structure

No.	Name	Description	
1	Indicator	 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





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.

Background Information

- 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.

Procedure

- <u>Step 1</u> Go to the hub screen, and then tap **Peripheral** to add the door detector.
- <u>Step 2</u> Tap "+" to scan the QR code at the bottom of the door detector, and then tap **Next**.
- <u>Step 3</u> Tap **Next** after the door detector plus has been found.
- <u>Step 4</u> Follow the on-screen instructions and switch the door detector plus to on, and then tap **Next**.
- Step 5 Wait for the pairing.
- <u>Step 6</u> Customize the name of the door detector plus, and select the area, and then tap **Completed**.

4.1 Installing the Door Detector Plus

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

Background Information

 \square

We recommend you use expansion screws when installing the door detector plus.

Procedure

- <u>Step 1</u> Drill 4 holes in door 1 and door 2 according to the hole positions of the attachment panel.
- <u>Step 2</u> Put the expansion bolts into the holes.
- <u>Step 3</u> Align the screw holes on the plate with the expansion bolts.
- <u>Step 4</u> Secure the attachment panels with ST3 \times 18 mm self-tapping screws.
- <u>Step 5</u> Put the door detector plus into the attachment panel.



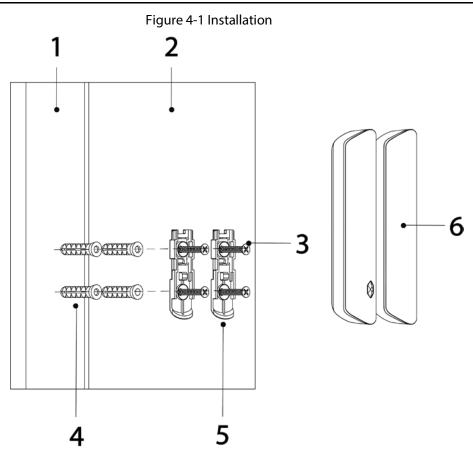


Table 4-1 Installation items

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

4.2 Replacing the Battery

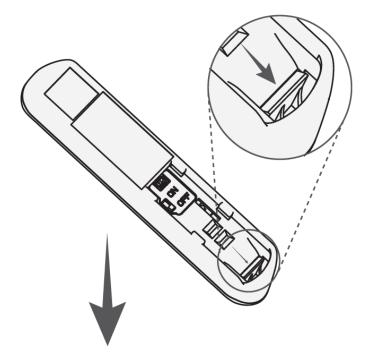
The battery has been installed when leaving the factory, and the door detector plus can be used directly. If the battery is dead, you need to replace the battery.

Procedure

<u>Step 1</u> Open the back cover of the door detector plus.

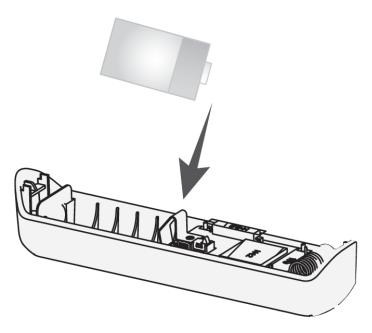


Figure 4-2 Open the back cover



Step 2 Replace the battery.
 When replacing the battery, make sure that the side marked with "+" faces the back cover of the devices.

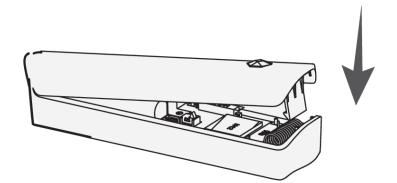
Figure 4-3 Replace the battery



<u>Step 3</u> Close the back cover of the door detector plus.



Figure 4-4 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.

 \square

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.

Parameter	Value		
	The status for whether the functions of the repeater are enabled or disabled.		
Temporary Deactivate	• (1) : Enable.		
	• (1) : Only disable tamper alarm.		
	• 🚫 : Disable.		
Temperature	The temperature of the environment.		
	The signal strength between the hub and the door detector plus.		
	• []]: Low.		
Signal Strength	• III : Weak.		
Signal Strength	• III : Good.		
	• III : Excellent.		
	• 👷 : No.		
	The battery level of the detector.		
	• 🔲: Fully charged.		
Dattory Loyal	• 🔲 : Sufficient.		
Battery Level	• 🔲 : Moderate.		
	• Insufficient.		
	• 🕒: Low.		
Tamper Status	Tamper status of the door detector plus.		
	Online and offline status of the door detector plus.		
Online Status	• 🕞: Online.		
	• CD: Offline.		

Table 5-1 Status



Parameter	Value		
Entering Delay Time			
Exiting Delay Time	Entrance and exit delay time.		
	Open or close status of the door.		
Door Status	• 📘 : 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.		
	Active status of the 24 h protection zone.		
24 H Protection Zone Status	• 24: Enabled.		
	• 24: Disabled.		
	Open or close status of the doorbell.		
Doorbell Status	• 🔲 : 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 \Box to configure the parameters of the door detector plus.

Parameter	Description
Device Configuration	 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 number assigned to the door detector alarm, which cannot be configured.
Permanent Deactivate	 Tap Enable, and the permanent deactivate 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 permanent deactivate function door detector
	plus will be disabled.

Table 5-2 Door detector plus parameters description



Parameter	Description
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.
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	Enable the Delay Mode under Home Mode , the selected peripheral under the hub will be armed and the alarm will not be triggered until the end of customized delay time. Only enable Home Mode first can Delay Mode under Home Mode take effect.
Delay Time	 The system provides you with time to leave or enter the armed zone without alarm. Delay Time for Entering Arming Mode: When you enter the zone, if you do not disarm the system before the delay ends, an alarm will be triggered. Make sure that the delay time for entering arming mode is no longer than 45 seconds in order to comply with EN50131-1. Delay Time for Exiting Arming Mode: When you are in the zone and arm the system, if you do not leave the zone before the delay ends, an alarm will be triggered. Select from 0 s to 120 s. The arming mode will be effective after the delay time.
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	 You can enable or disable the external detector. After enabling, the external detector status will be displayed. Link external input to siren. External input type: You can select from Normally Open(default), Normally Closed and Pulse. External input Alarm functions not certificate IMQ- SISTEMI DI SICUREZZ.



Shock Detector ConfigYou can enable or disable the shock detector. After enabling, you can configure shock detector parameters.Shock Detector Config Link Shock Alarm to SirenSensitivity: You can select from High, Medium (default), and Low.Ignore Simple Crash Sound: It is disabled by default.In an installation environment with shock, we recommend that you enable Ignore Simple Crash Sound.Shock function not certificate IMQ- SISTEMI DI SICUREZZA. You can enable or disable the tilt detector. After enabling, you can configure tilt detector parameters.Link Tilt Alarm to SirenTilt Detector ConfigTilt Detector ConfigConfigTilt detector ConfigTilt det
Shock Detector • Sensitivity: You can select from High, Medium (default), and Low. • Ignore Simple Crash Sound: It is disabled by default. • • Ignore Simple Crash Sound: It is disabled by default. • • In an installation environment with shock, we recommend that you enable Ignore Simple Crash Sound. • • Shock function not certificate IMQ- SISTEMI DI SICUREZZA. You can enable or disable the tilt detector. After enabling, you can configure tilt detector parameters. • 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. • Delay Tilt function not certificate IMQ- SISTEMI DI SICUREZZA.
Shock Detector Config • Ignore Simple Crash Sound: It is disabled by default. In an installation environment with shock, we recommend that you enable Ignore Simple Crash Sound. Shock function not certificate IMQ- SISTEMI DI SICUREZZA. You can enable or disable the tilt detector. After enabling, you can configure tilt detector parameters. • 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. Image: Tilt function not certificate IMQ- SISTEMI DI SICUREZZA.
Shock Detector Config In an installation environment with shock, we recommend that you enable Ignore Simple Crash Sound. Image: Shock function not certificate IMQ- SISTEMI DI SICUREZZA. You can enable or disable the tilt detector. After enabling, you can configure tilt detector parameters. Image: Interpret of tilt Alarm to Siren Tilt Detector Config Delay Tilt Alarm: 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. Tilt function not certificate IMQ- SISTEMI DI SICUREZZA. After enabling, when the area is disarmed, if the door detector is opened, the
Config In an installation environment with shock, we recommend that you enable Ignore Simple Crash Sound. Image: Interpret term Image: Ima
Tilt Detector • Link Tilt Alarm to Siren • Link Tilt Alarm to Siren • Tilted Angle: You can select from 5deg, 10deg, 15deg, 20deg, 25deg. • 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. • Delay Tilt function not certificate IMQ- SISTEMI DI SICUREZZA. • After enabling when the area is disarmed if the door detector is opened the
Shock function not certificate IMQ- SISTEMI DI SICUREZZA.You can enable or disable the tilt detector. After enabling, you can configure tilt detector parameters.• 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.Image: Tilt function not certificate IMQ- SISTEMI DI SICUREZZA.
You can enable or disable the tilt detector. After enabling, you can configure tilt detector parameters.• 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.Image: Tilt function not certificate IMQ- SISTEMI DI SICUREZZA.
You can enable or disable the tilt detector. After enabling, you can configure tilt detector parameters.• 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.Image: Tilt function not certificate IMQ- SISTEMI DI SICUREZZA.
Tilt Detector ConfigLink Tilt Alarm to SirenTilt Detector ConfigTilted 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.Image: Tilt function not certificate IMQ- SISTEMI DI SICUREZZA.After enabling, when the area is disarmed if the door detector is opened, the
Tilt Detector Config• 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.Image: Tilt function not certificate IMQ- SISTEMI DI SICUREZZA.
Tilt Detector ConfigThe 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.Image: Tilt function not certificate IMQ- SISTEMI DI SICUREZZA.
Tilt Detector Configexceeds 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.Tilt function not certificate IMQ- SISTEMI DI SICUREZZA.After enabling, when the area is disarmed, if the door detector is opened, the
 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. Tilt function not certificate IMQ- SISTEMI DI SICUREZZA.
 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. Tilt function not certificate IMQ- SISTEMI DI SICUREZZA.
tilted angle exceeds the set angle and does not recover beyond the set time, an alarm is triggered. Tilt function not certificate IMQ- SISTEMI DI SICUREZZA.
time, an alarm is triggered. Tilt function not certificate IMQ- SISTEMI DI SICUREZZA. After enabling, when the area is disarmed, if the door detector is opened, the
Tilt function not certificate IMQ- SISTEMI DI SICUREZZA. After enabling, when the area is disarmed, if the door detector is opened, the
After enabling when the area is disarmed if the door detector is opened the
After enabling when the area is disarmed if the door detector is opened the
After enabling, when the area is disarmed, if the door detector is opened, the
Chime indoor siren will be triggered.
Over-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.
temperature
Alarm Over-temperature Alarm function not certificate IMQ- SISTEMI DI
SICUREZZA.
Signal Strength Detection Test the current signal strength.
Detector Test Detect whether the peripheral works.



Parameter	Description
Transmit Power	 Select from high, low, and automatic. The higher the transmission power, the farther the signal can travel, but the greater the power consumption. If you select Low, the 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 V1.000.000001.0.R.20211203 or later.
Cloud Update	Update online.
Delete	Delete the online peripheral. Go to the hub screen, select the peripheral from the list, and then swipe left to delete it.



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 Allow list

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

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