



Wireless External Curtain PIR

User Manual



Foreword

General

This manual introduces the installation, functions and operations of the wireless curtain PIR (hereinafter referred to as the "detector"). Read carefully before using the device, and keep the manual safe for future reference.

Symbols

The following symbols might appear in the manual.

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

Revision History

Version	Revision Content	Release Time
V1.0.0	First release.	June 2026

Privacy Protection Notice

As the device user, you might collect the personal data of individuals such as their names, email addresses, face images, audio and fingerprints. You shall be fully responsible for any activities associated with processing personal data. You commit to comply with your local privacy protection laws and regulations to protect the legitimate rights and interests of individuals, and shall implement measures which are required by applicable law, including but not limited to, providing clear and comprehensive information to individuals before processing their personal data, obtaining consent from individuals when necessary, informing individuals of the existence of the surveillance area, and providing required contact information.

Intelligent Product Usage Statement

Intelligent products utilize AI technology to effectively enhance security. The intelligent recognition and alarm functions of the product might be affected by factors such as environmental lighting, camera angles, object obstructions, and network delays, potentially leading to false alarms, missed alerts, or response delays. This intelligent product is solely intended to be used as a security assistance tool. The results from performing identification are for reference only and do not

constitute absolute guarantee of personal or property safety. Users need to combine these products with necessary physical security measures to enhance overall protection. Except as otherwise provided by laws or in the event of intentional or gross negligence on the part of the company, the company shall not be liable for any losses caused by the aforementioned factors not attributable to the company.

About the Manual

- This manual is provided for general reference only. Discrepancies might exist between the product and this manual, including but not limited to printed, electronic, or any other editions.
- The manual will be updated according to the latest laws and regulations of related jurisdictions. Specifications and documentation are subject to change without prior notice. For the latest versions, as well as legal notices, consult the printed manual, the product webpage, our official website, or scan the QR code to access the electronic edition.
- The manual will be updated as necessary to reflect product changes and applicable legal requirements. These updates will not diminish your statutory rights, nor will they remove or weaken the safety information or essential instructions provided at the time of purchase.
- Although we make every effort to ensure accuracy, errors or deviations in descriptions of functions, operations, or technical data might occur. If there is any uncertainty or controversy, we reserve the right of final explanation.
- All trademarks, registered trademarks and company names referenced in this manual are the property of their respective owners.

Important Safeguards and Warnings

This section introduces content covering the proper handling of the triple-tech detector, hazard protection, and protection of property damage. Read carefully before using the triple-tech detector, and comply with the guidelines when using it.

Operation Requirements



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



- Strictly comply with the local electrical safety code and standards. Make sure that the ambient voltage is stable and meets the power supply requirements of the device.
- The power supply must meet the rated voltage requirements as indicated on the device label.
- If the device uses a power adapter, ensure it meets the following requirements:
 - ◇ If a power adapter was shipped with your device, we recommend you use it. If you need to buy a separate adapter, make sure it meets the following requirements.
 - The power supply must conform to the requirements of IEC 60950-1 and IEC 62368-1 standards.
 - The voltage must meet the SELV (Safety Extra Low Voltage) requirements and not exceed ES-1 standards.
 - When the power of the device does not exceed 100 W, the power supply must meet LPS requirements and be no higher than PS2.
 - ◇ Do not connect the power adapter to the device while the adapter is powered on.



- Observe all safety procedures and wear required protective equipment provided for your use while working at heights.
- Do not expose the device to direct sunlight or heat sources.
- Do not install the device in humid, dusty or smoky places.
- Install the device in a well-ventilated place, and do not block the ventilator of the device.
- Connect class I electrical appliances to a power socket with protective earthing.

Table of Contents

Foreword.....	I
Important Safeguards and Warnings.....	III
1 Introduction.....	1
1.1 Overview.....	1
1.2 Technical Specifications.....	1
2 Checklist.....	4
3 Design.....	5
3.1 Appearance.....	5
3.2 Dimensions.....	7
4 Installation.....	8
4.1 Powering On.....	8
4.2 Adding the Wireless External Curtain PIR to the Hub.....	10
4.3 Field of Detection.....	11
4.4 Installing Detector.....	14
4.4.1 Wall Mount.....	14
4.4.2 Corner Mount.....	15
4.5 Anti-Masking Test.....	15
5 Configuration.....	17
5.1 Viewing Status.....	17
5.2 Configuring the PIR Detector.....	19
Appendix 1 Security Commitment and Recommendation.....	23

1 Introduction

1.1 Overview

The Wireless External Curtain PIR is a motion detector that uses dual motion sensing technology. Its narrow 8° horizontal curtain beam reaches up to 12 meters, providing focused perimeter coverage and reliable intrusion detection. Suited for indoor and outdoor use, it helps protect windows, doorways and other access points.

1.2 Technical Specifications

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

Table 1-1 Technical specifications

Type	Parameter	Description
Function	Indicator Light	1 × three-color alarm light (green, yellow, red)
	Button	1 × power button 1 × Installation height adjustment switch
	Remote Update	Cloud update
	Low Battery Detection	Yes
	Tamper	Tamper alarm
	Moving Detection	Yes
Technical	Detection Mode	PIR + Microwave
	Sensitivity	3 levels adjustable
	Detection Range	Range:5-12 m horizontal: 8° vertical: 58° The angle is 58°at 2.4 m
	Detection Speed	0.3 m/s–2m/s
	Microwave Frequency	24G
	Pet Immunity Level	<50 cm (19.68 ft),about 18 kg (39.68 lb) when installed at height of 2.4m (7.9ft) <80 cm (2.62 ft) when installed at height of 1m (3.3ft)
	White Light Resistance Level	10000 lux
	Anti-masking	Yes. The material and distance of an obstruction can affect the detection results.
	Two-way Digital Temperature Compensation	Yes
	Scenario	Outdoor,indoor

Type	Parameter	Description		
	Operating Current	DHI-ARD2631E-W2: 48 uA	DHI-ARD2631E-W2 (868): 50 uA	DHI-ARD2631E-W2 (915): 52 uA
	Alarm Current	58 mA (Avg); 880 mA (Max)		
Wireless	Carrier Frequency	DHI-ARD2631E-W2: Airfly:433.05 MHz-434.79 MHz RF-HD:433.05 MHz– 434.79 MHz (Device Upgrade)	DHI-ARD2631E-W2 (868): Airfly:868.0 MHz-868.6 MHz RF-HD: 865.0 MHz-867.0 MHz (Device Upgrade)	DHI-ARD2631E-W2 (915): Airfly:915.0 MHz-928.0 MHz RF-HD: 915.0 MHz-928.0 MHz (Device Upgrade)
	Transmitter Power (EIRP)	DHI-ARD2631E-W2: Limit 10 mW	DHI-ARD2631E-W2 (868): Limit 25mW	DHI-ARD2631E-W2 (915): Limit 1W
	Communication Mechanism	Two-way		
	Communication Distance	DHI-ARD2631E-W2: Up to 1,200 m (3937.01 ft) in an open space	DHI-ARD2631E-W2 (868): Up to 1,600 m (5249.34 ft) in an open space	DHI-ARD2631E-W2 (915): Up to 1,600 m (5249.34 ft) in an open space
	Frequency Hopping	Yes		
	Encryption Mode	AES128		
General	Power Supply	CR123A × 2		
	Battery Life	DHI-ARD2631E-W2/DHI-ARD2631E-W2 (868): 4.2 years (triggers 1 alarm a day)		DHI-ARD2631E-W2 (915): 4 years (triggers 1 alarm a day)
	Operating Temperature	–25 °C to +60 °C (–13 °F to +140 °F)		
	Operating Humidity	10%–90% (RH)		
	Product Dimensions	With sunshade: 154.6 mm × 72.3 mm × 81.1 mm (6.09" × 2.85" × 3.19") Without sunshade: 138 mm × 59 mm × 65.57 mm (5.43" × 2.32" × 2.58")		

Type	Parameter	Description
	Packaging Dimensions	181 mm × 142 mm × 111 mm (7.13" × 5.59" × 4.37")
	Installation Height	Low mounting: 0.8 to 1.3 m High mounting: 2 to 2.4 m (the mounting height affects detection range)
	Net Weight	0.35 kg (0.77 lb)
	Gross Weight	0.76 kg (1.68 lb)
	Installation	Wall mount
	Casing	PC + GF
	Protection	IP65
	Anti-corrosion Level	Basic Protection *The products are designed for general use and are applicable even in areas with no specific requirements for anti-corrosion protection.

2 Checklist

Figure 2-1 Checklist

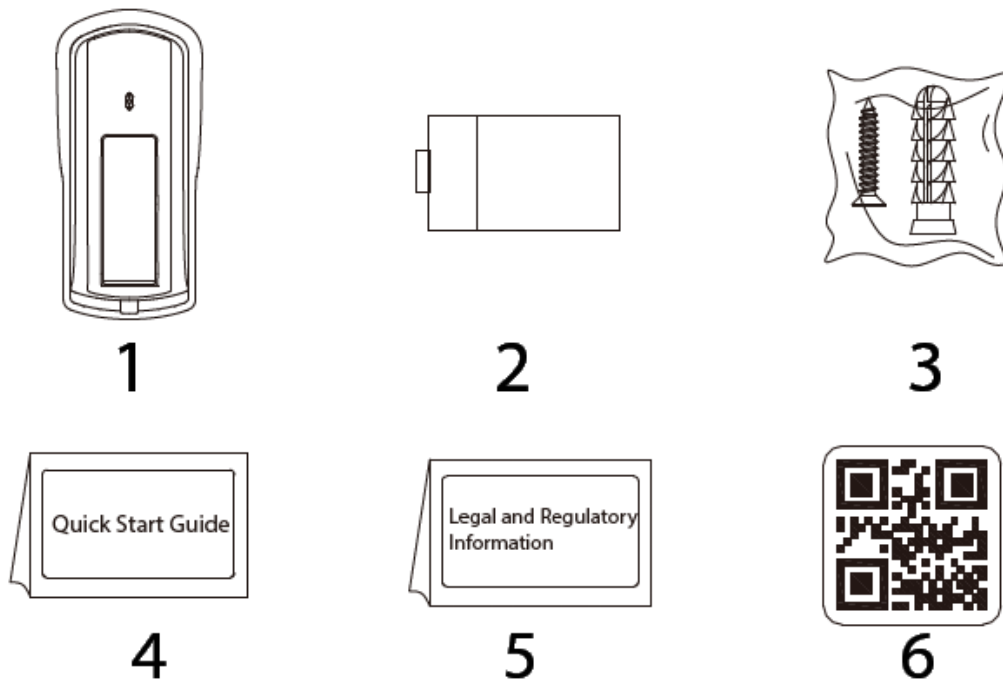


Table 2-1 Checklist

No.	Item Name	Quantity	No.	Item Name	Quantity
1	Wireless external curtain PIR	1	4	Quick start guide	1
2	Battery	2	5	Legal and regulatory information	1
3	Package of screws	1	6	QR code	1

3 Design

3.1 Appearance

Figure 3-1 Appearance

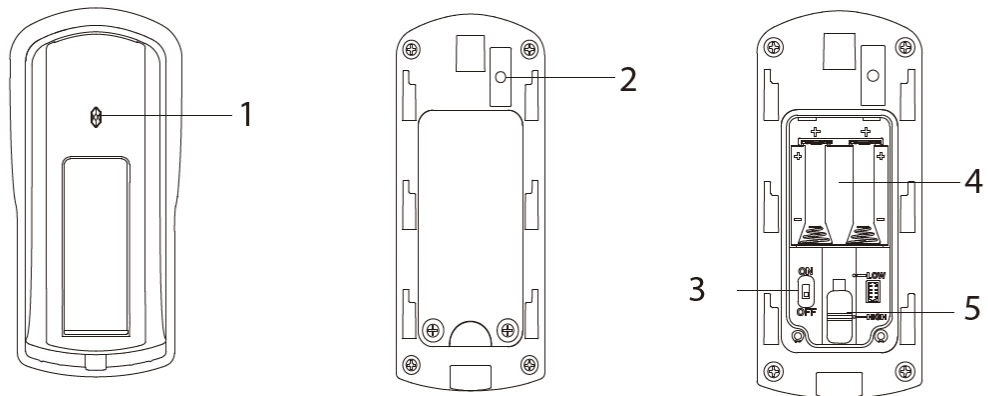
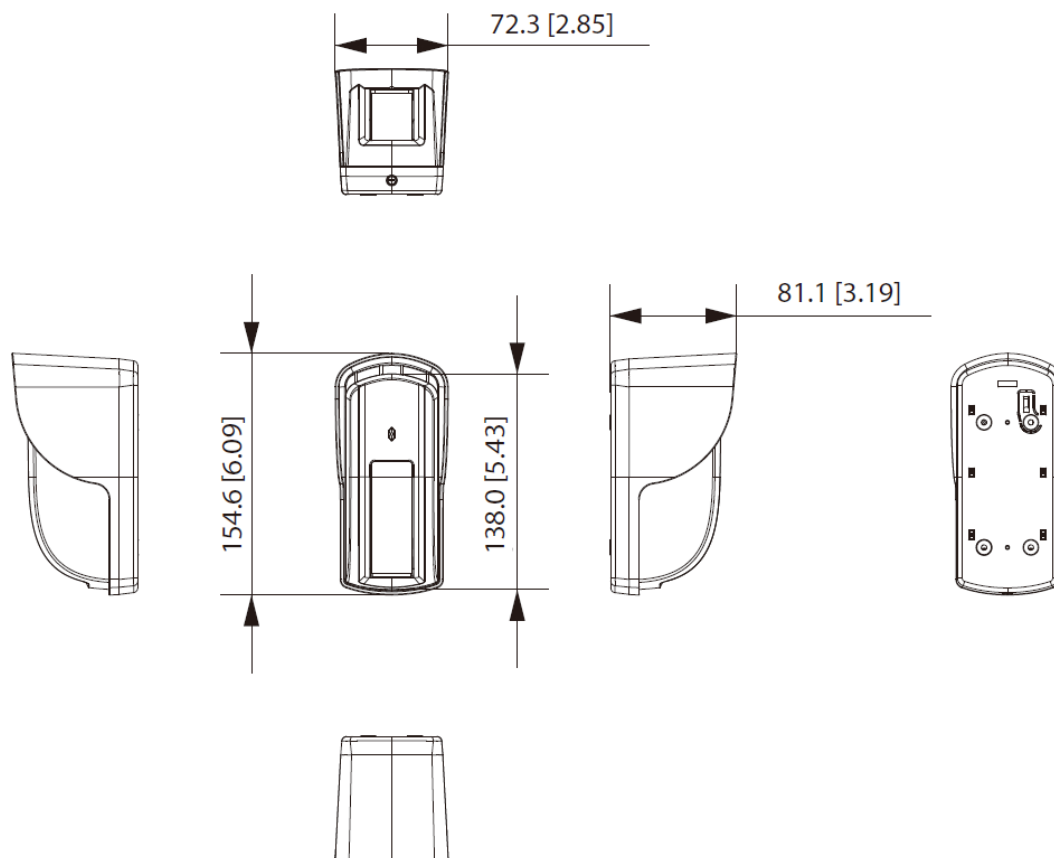


Table 3-1 Structure

No.	Name	Description
1	Indicator	Used to display the working status of the device and provide status feedback through different colors or flashing patterns. ● Power on: Flashes green for 2 seconds after being powered on. ● Pairing: Flashes green quickly (on for 200 ms, off for 200 ms) during pairing. Solid green for 2 seconds if pairing is successfully; Flashes green for 3 seconds if pairing is failed; Solid off if not paired. ● Alarm: Solid green for 0.5 seconds if tamper or device moved alarm is triggered; Solid red for 0.5 seconds if mask alarm is triggered. ● Signal test: Flashes green for when going to signal test. ● Detector test: Solid green for 3 seconds when going to detector test. ● Mask test: Solid red during mask test, until the obstruction is removed. ● Abnormal detection mode: Flashes yellow. ● Attenuation mode: When entering the attenuation mode, it flashes green quickly (on for 100ms, off for 100ms). The indicator only operates for 10 minutes and has the lowest priority; it can be interrupted by other status indications. If interrupted, it resumes indication within the 10-minute period. If the device restarts within 10 minutes, the indication does not resume.
2	Tamper switch	Triggers an alarm when the device is dismantled or moved.
3	Power switch	Used to power on or power off the device.
4	Battery compartment	Used to install batteries.
5	Installation height adjustment switch	Used to adjust the device's height based on the installation environment to optimize monitoring range or detection effectiveness.

3.2 Dimensions

Figure 3-2 Dimensions (mm [inch])



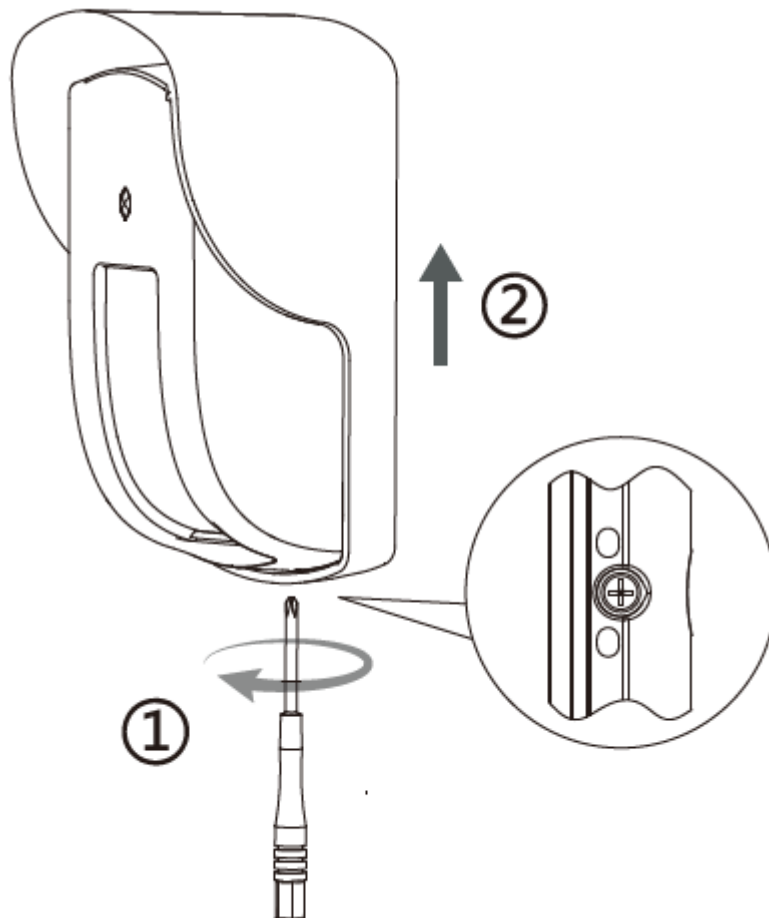
4 Installation

4.1 Powering On

Procedure

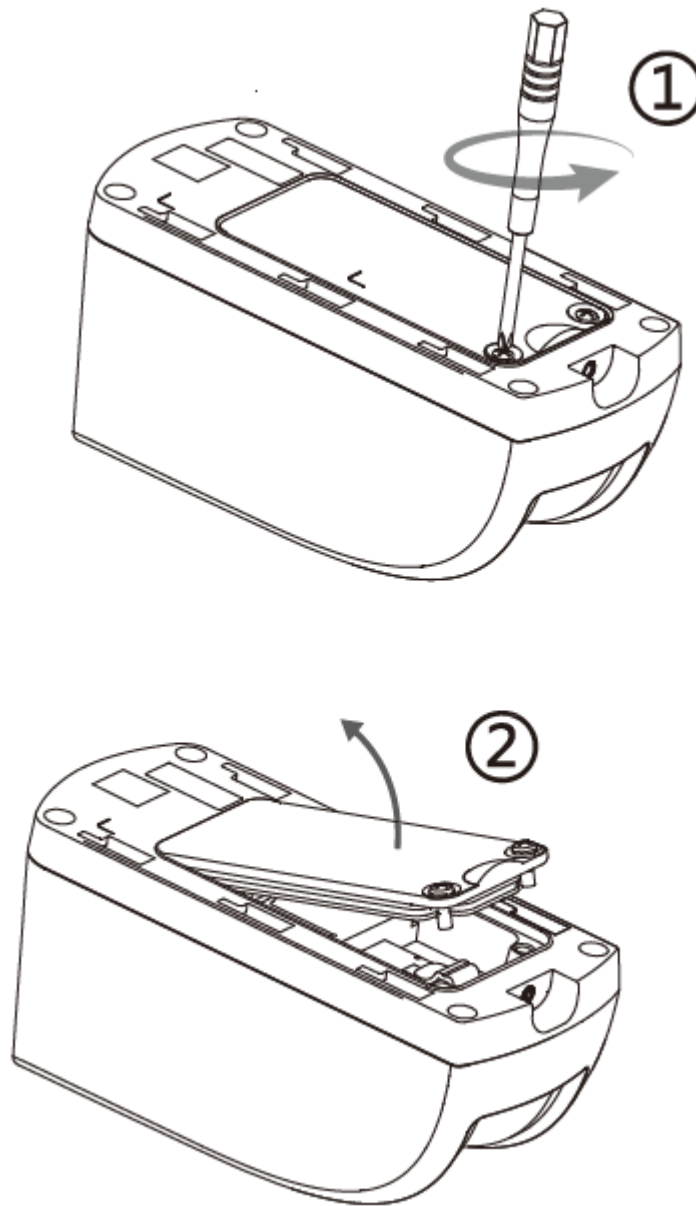
Step 1 Loosen the screw to open the detector.

Figure 4-1 Loosen screw



Step 2 Open the battery compartment.

Figure 4-2 Open compartment

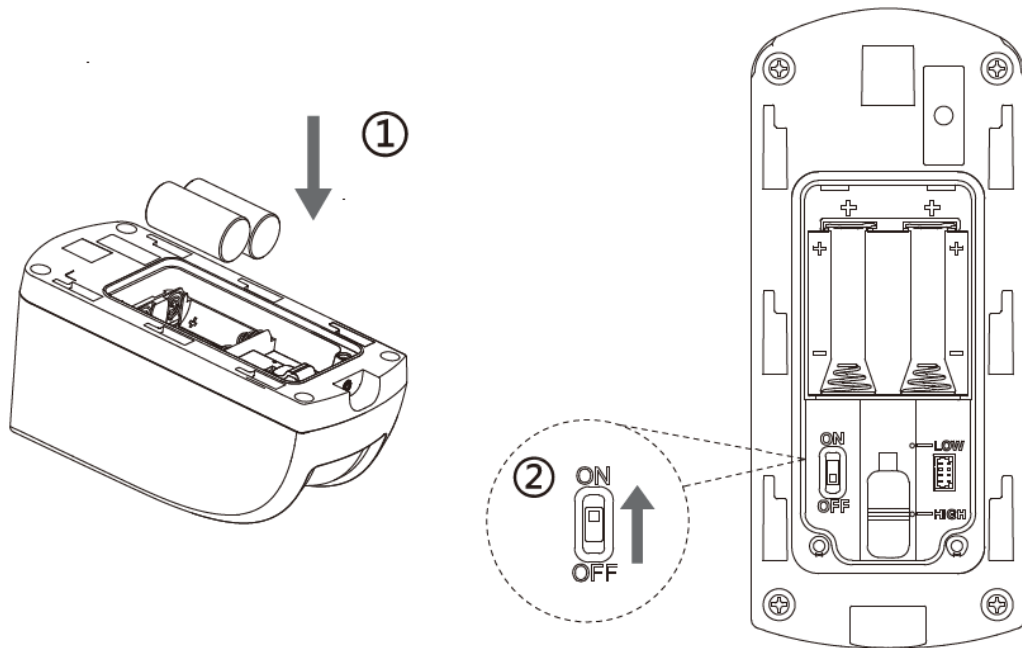


Step 3 Insert batteries into the detector, and then turn on the detector.



- When inserting the batteries, make sure that they are all charged to the same level.
- When inserting the batteries, align the "+" symbols on the batteries to those on the detector.

Figure 4-3 Turn on the detector



4.2 Adding the Wireless External Curtain PIR to the Hub

Background Information

Before you connect the PIR to the hub, install the DMSS app on your phone. This manual uses iOS as an example.



- Make sure that the version of the DMSS app is 2.5.0 or later, and the hub is 2.000.0000010.0.R.260423 or later.
- Make sure that you have already created an account, and added the hub to DMSS.
- Make sure that the hub has a stable internet connection.
- Make sure that the hub is disarmed.

Procedure

- Step 1 Go to the **Devices** screen of the hub, and then select  > **Add Peripheral**.
- Step 2 Scan the QR code at the bottom of the PIR, and then tap **Next**.
- Step 3 Tap **Next** after the PIR has been found.
- Step 4 Configure the device name for the PIR, assign the area for it, and then tap **Next**.
- Step 5 Follow the on-screen instructions to switch the PIR from off to on, and its indicator flashes green, and then tap **Next**.
- Step 6 Wait for the pairing to finish, and then tap **OK**.

4.3 Field of Detection



When installing and using the detector, make sure there are no objects partially or fully obscuring the detector's field of view.

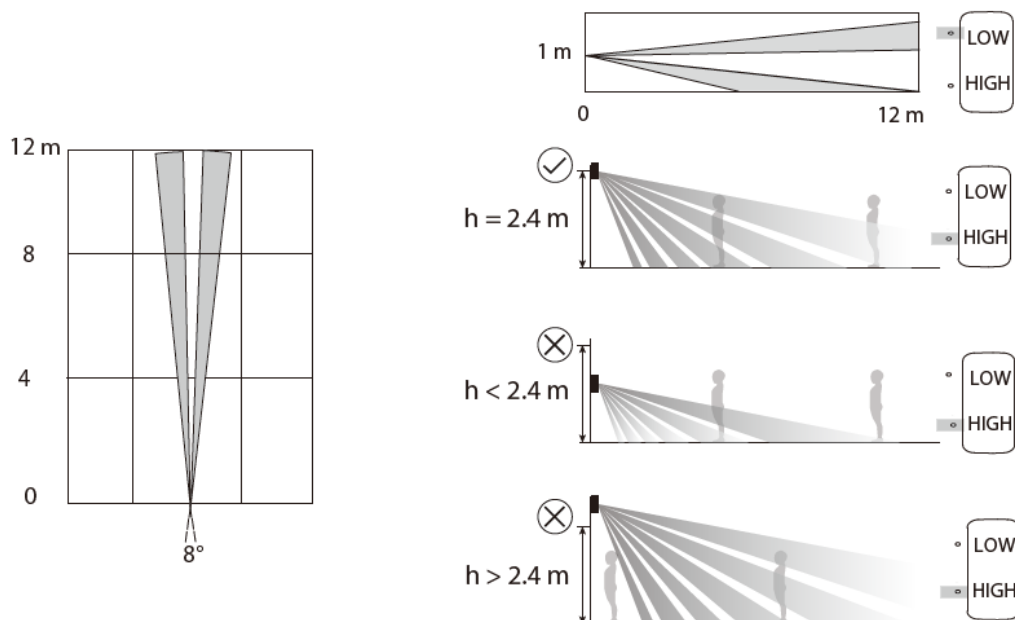
Detection Range

The detection ranges of the detector.



This data is the result of room temperature environmental testing. The actual detection distance might vary due to environmental factors, such as temperature and light exposure.

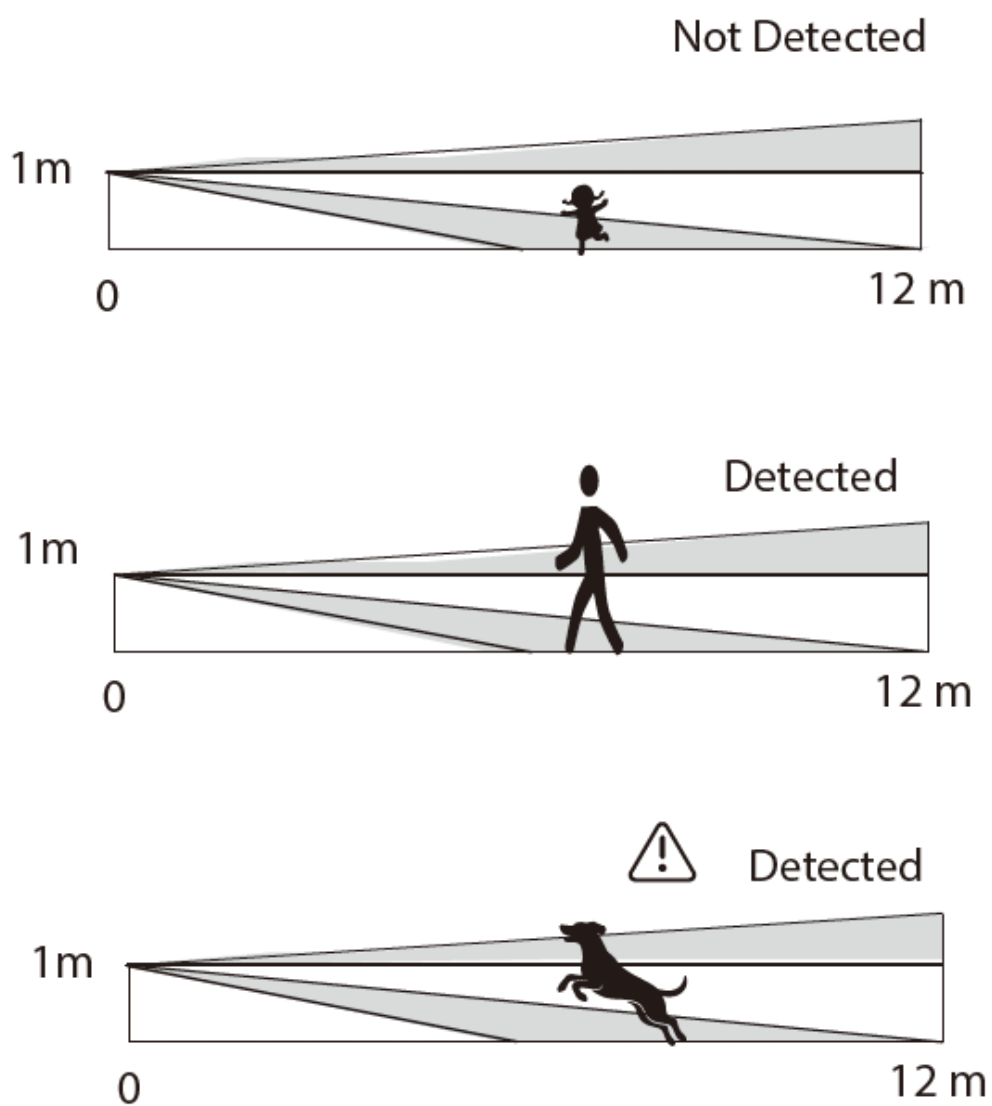
Figure 4-4 Detection range



Effective Detection Trigger

The detection trigger that can effectively trigger the detector. Here are some recommended ones and not recommend objects.

Figure 4-5 Trigger





Installation Position

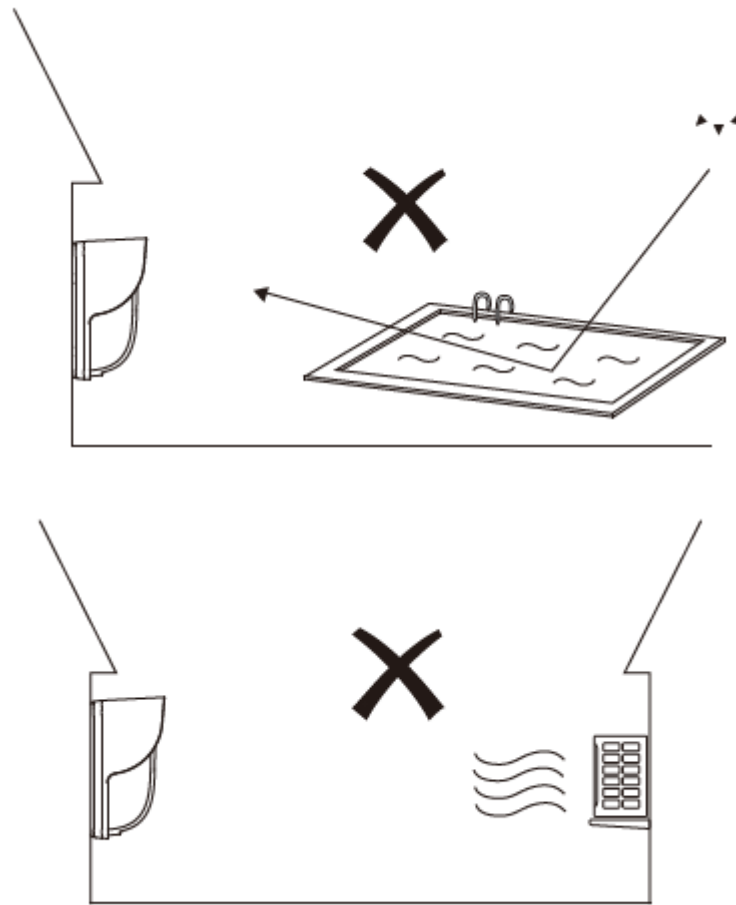
Position not recommended:

- Direct sunlight or reflection.
- Direct heat exposure.
- Areas where pets often jump



For optimal performance, install the detector away from areas with high pet activity. Avoid aiming it at spots where pets frequently jump or where large dogs might stand upright to reduce false alarms.

Figure 4-6 Installation position(not recommended)



4.4 Installing Detector

4.4.1 Wall Mount

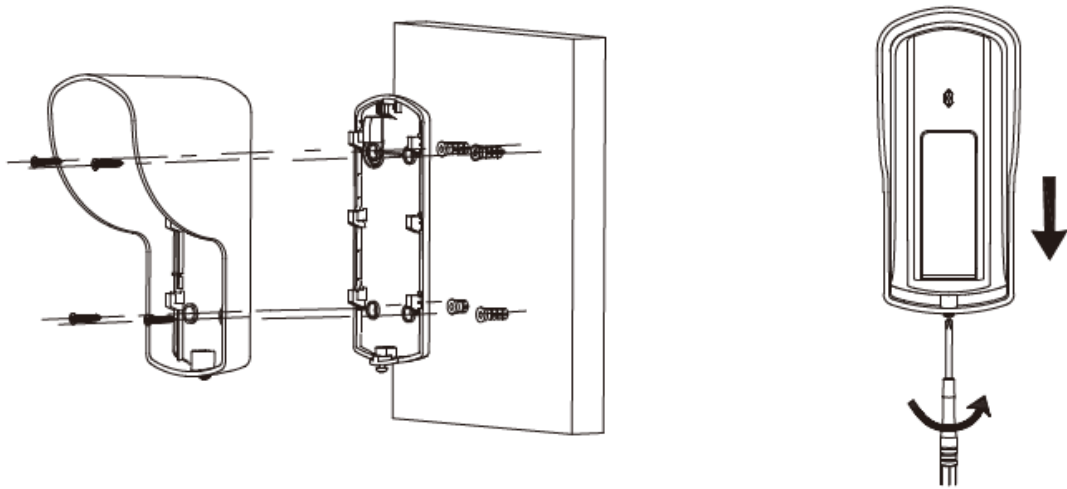
Prerequisites

Prior to installation, add the detector to the hub and test the signal strength (for detectors with camera modules). We recommend that you install the detector in a place with a signal strength of at least 2 bars.

Procedure

- Step 1** Drill 4 holes into the wall according to the hole positions of the detector, and then put the expansion bolts into the holes.
- Step 2** Attach the detector to the back cover.

Figure 4-7 Wall mount

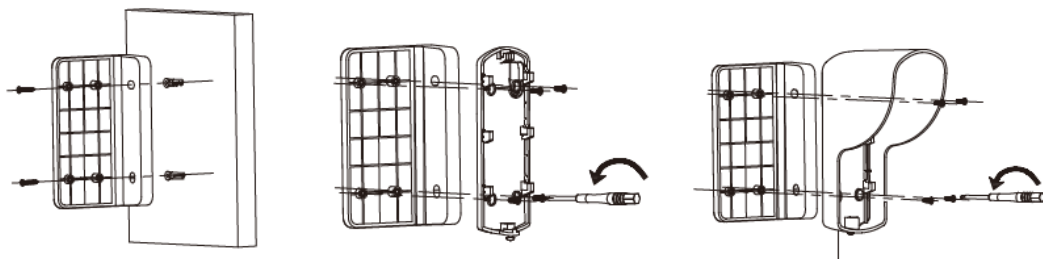


4.4.2 Corner Mount

Procedure

- Step 1 Drill 2 holes into the wall according to the hole positions of bracket and then put the expansion bolts into the holes to fix the bracket onto the wall

Figure 4-8 Drill holes



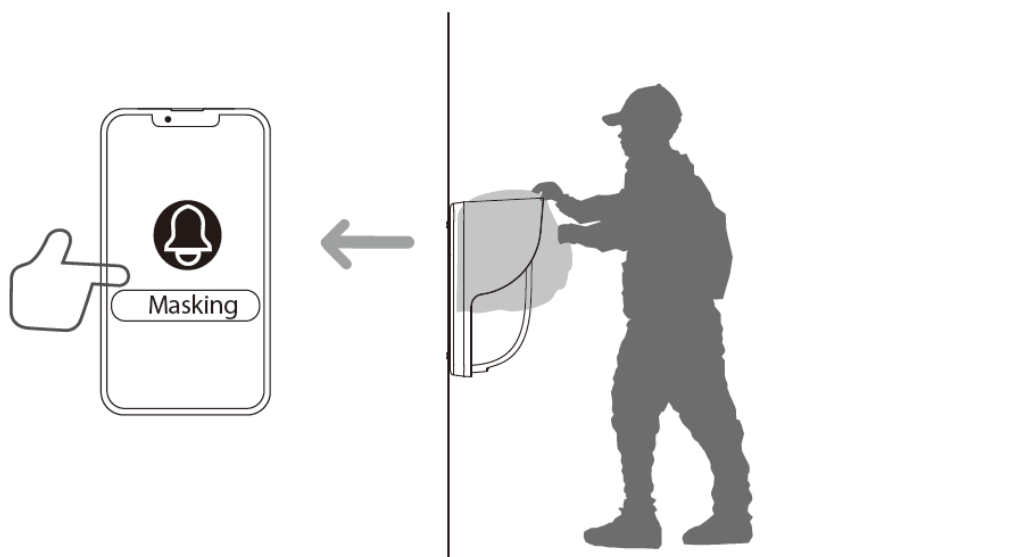
- Step 2 Insert 4 screws or through the mounting holes of the back cover of detector to fix it onto the other side of the bracket.
- Step 3 Fix the detector onto the back cover.

4.5 Anti-Masking Test

Before using the detector, perform anti-masking test.

Make sure that you have tested environment interference before obstruction test.

Figure 4-9 Anti-mask test



5 Configuration

You can view and edit general information of the triple-tech detector.

5.1 Viewing Status

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

Detector Icon Description

Introduces the meaning of icons for the detector. You can view these icons on the hub screen.

Table 5-1 Device icon description

Parameter	Icon	Description
Signal Strength		Low
		Weak
		Good
		Excellent
		No signal
Bypass		Yes
		Lid only
Permanent Deactivation		Yes
		Lid only
Battery Level		100%
		80%
		60%
		40%
		20%
		No battery

Parameter	Icon	Description
Tamper		Opened
Mask Detection		Masked
Home Mode		Home mode enabled
Repeater		Repeater enabled

Detector Status Description

On the **Devices** screen of the hub, select a detector and then select **Overview** to view the information and status.

Table 5-2 Status

Parameter	Description
Device No.	Displays the number of the detector.
Temperature	Displays the temperature of the detector.  The temperature has a tolerance of $\pm 3^{\circ}\text{C}$, and the measurement accuracy is 1°C.
Signal Strength	Displays the signal strength of the detector.
Online Status	Online and offline status of the detector.
Battery Level	Shows the remaining electricity of the battery in the form of percentage.
Permanent Deactivation	The status for whether the permanent deactivation of the detector is enabled or turned off. • Yes • Lid only • No
Bypass	Whether bypass is enabled or not. Once enabled, all information will not be sent to the hub. • Yes • Lid only • No
Tamper	Displays the anti-tamper status of the detector. The types include: • Opened • Disconnected
Masked	Displays the mask status of the detector.

Parameter	Description
Sensitivity	Displays the sensitivity of the detector. The types include: • Low • Medium • High
Detection Mode	Displays the detection status of the detector. • High-point installation • Low-point installation • Abnormal
Zone Type	• Displays Instant when you set Zone Type as Instant in Settings. • Displays 24 hr when you set Zone Type as 24 hr in Settings. • Displays Follow when you set Zone Type as Follow in Settings.
Repeater	The status of whether the detector forwards peripheral messages to the hub through the repeater.
Firmware Version	Displays the latest version of the program.

5.2 Configuring the PIR Detector

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

Table 5-3 Parameter description

Parameter	Description
Device	• View detector name, type, SN and device model. • Edit detector name, and then tap Save to save configuration.
Area	Select the area to which the detector is assigned.
Bypass	• Yes: Bypass is enabled, and information will not be sent to the alarm hub. • Lid only: Tamper only. All information, except for tamper alarms, will be sent to the alarm hub. • No: Bypass is turned off. All information will be sent to the alarm hub.  Bypass will automatically restore after disarming.

Parameter	Description
Permanent Deactivation	The status for whether the permanent deactivation of the detector is enabled or turned off. ● Yes: The permanent deactivation is enabled. Alarm information will not be sent to the alarm hub. ● Lid only: All information, except for tamper alarms will be sent to the alarm hub. ● 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.
Status LED	Status LED is enabled by default.  If Status LED is disabled, the LED indicator will remain off regardless of whether the detector is functioning normally or not.
Zone Type	● Instant: The alarm is triggered immediately upon detection in the armed area. ● Delay: The armed detector starts the countdown and does not report alarms even if the alarms are triggered, until the countdown ends. ◇ 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. ◇ 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. You can select from 0 s to 120 seconds. ● 24 hr: The detector is always in the armed mode, and reports alarms when triggered.. ● 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 selected peripherals under the hub will be armed.
Home Mode Delay  Only available when you select the Zone Type as Delay, and enable Home Mode.	Enable Home Mode Delay. The zone in which the selected PIR-Camera is assigned to will not report alarms even alarms are triggered, until the delay ends.
Crossed Zone	Select crossed zone from the list, or you can also select None.

Parameter	Description
Sensitivity	- Adjust sensitivity level of motion detection. - Select from low, medium and high.
Detection Angle	The detection angle is used to adjust the detection range. You can select from 8° and 15°.  The detection angle you select is only a unilateral angle.
Microwave Detection Distance	The range at which a microwave sensor can detect motion or presence. You can select the detection distance (5 m, 8 m, 12 m) from the list.  Interference between the maximum distance and the set distance can cause the battery to drain quickly.
Fast Discharge Detection	Enable the function, and you can receive notifications when the battery life reduces because of incorrect installation position of the detector.
Mask	Mask Function: Once the detector is masked by other objects, alarms will be sent to the hub. - Tap enable in arming status, and then the mask function is enabled in arming status. - Tap Always On, and then the mask function will always stay enabled. - Tap Disabled, and then the mask function is disabled. Enable Link Mask Alarm to Siren: The mask alarm will be synchronized to the siren.
Over-temperature Alarm	Enable the Over-temperature Alarm function, and then the alarm will be triggered when the temperature of the area where the detector is installed is higher or lower than the defined one. Tap  next to Over-temperature Alarm to enable this function. Scroll left and right on the temperature bar to set the lowest temperature or highest temperature, or tap + or - to set the temperature ranges.
Movement Alarm	Movement Alarm : Enable the function, and then alarms will be sent to the hub once movement is detected. Link Movement Alarm to Siren : The movement alarm will be synchronized to the siren.  - Enabling the movement alarm results in aging of battery life. - We recommend that you enable movement alarm when the detector is pole mounted or installed with extended bracket.
Link Alarm to Siren	When an alarm is triggered, the detector will report the alarm events to the hub and alert with siren.

Parameter	Description
Alarm and Video Linkage	When an alarm is triggered, the detector will report the alarm events to the hub and then will link events.
Signal Strength Detection	Test the signal strength of the detector.
Detector Test	Select the window (bottom window or upper window), and then tap Start Detection for zone test. Make sure that the detector is installed in area with great signal strength.  • The detector test will not begin immediately. It will begin before the end of the heartbeat interval of the hub-detector (60 seconds by default). • You can configure the heartbeat interval on the hub.
Obstruction Test	Checks whether a specific area is blocked, obstructed, or intruded upon by objects.
Environment Interference Test	Checks for the interference in the area and if objects are blocking detection. Tap Start to start the test.  When testing, make sure that the current test environment has no obstructions. If there are obstructions, it might affect subsequent obstruction alarms.
Transmit Power	• Select from high, low, and automatic. • The higher transmission power levels are, the further transmissions can travel, but power consumption increases.  If you select Low, the detector will enter into reduced sensitivity mode.
Firmware Update	Tap to view the current firmware version of the 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 detector.

Appendix 1 Security Commitment and Recommendation

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

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

Account Management

1. Use complex passwords

Please refer to the following suggestions to set passwords:

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

2. Change passwords periodically

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

3. Allocate accounts and permissions appropriately

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

4. Enable account lockout function

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

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

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

Service Configuration

1. Enable HTTPS

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

2. Encrypted transmission of audio and video

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

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

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

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

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

4. Change HTTP and other default service ports

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

Network Configuration

1. Enable Allowlist

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

2. MAC address binding

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

3. Build a secure network environment

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

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

Security Auditing

1. Check online users

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

2. Check device log

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

3. **Configure network log**

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

Software Security

1. **Update firmware in time**

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

2. **Update client software in time**

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

Physical Protection

It is recommended that you carry out physical protection for devices (especially storage devices), such as placing the device in a dedicated machine room and cabinet, and having access control and key management in place to prevent unauthorized personnel from damaging hardware and other peripheral equipment (e.g. USB flash disk, serial port).

ENABLING A SMARTER SOCIETY AND BETTER LIVING

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.

Address: No. 1399, Binxing Road, Binjiang District, Hangzhou, P. R. China | Website: www.dahuasecurity.com | Postcode: 310053

Email: dhoverseas@dhvisiontech.com | Tel: +86-571-87688888 28933188