Wireless Triple-tech Detector

User Manual



ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD. V1.0.3

Foreword

General

This manual introduces the installation, functions and operations of the wireless triple-tech detector (hereinafter referred to as the "triple-tech 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
V1.0.3	• Updated the technical specification. • Updated the app software and hub software version.	November 2026
V1.0.2	Updated images in "Installation" chapter and description in "Configuration" chapter.	April 2026
V1.0.1	Revised technical parameters and certificate requirements.	June 2024
V1.0.0	First release.	January 2024

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

DANGER

The device or remote control contains button batteries. Do not swallow the batteries due to the risk of chemical burns.

Possible result: The swallowed button battery can cause serious internal burns and death within 2 hours.

Preventive measures (including but not limited to):

- Keep new and used batteries out of reach of children.
- If the battery compartment is not securely closed, stop using the product immediately and keep out of reach of children.
- Seek immediate medical attention if a battery is believed to be swallowed or inserted inside any part of the body.

- Make sure that the power supply of the device works properly before use.
- Do not pull out the power cable of the device while it is powered on.
- Only use the device within the rated power range.
- Transport, use and store the device under allowed humidity and temperature conditions.
- Prevent liquids from splashing or dripping on the device. Make sure that there are no objects filled with liquid on top of the device to avoid liquids flowing into it.
- Disassembling the device can reduce performance and create safety hazards. Do not disassemble the device without authorization.

Installation Requirements

WARNING

- 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 6
4 Installation 7
4.1 Powering On 7
4.2 Adding the Wireless Triple-Tech Detector to the Hub 8
4.3 Field of Detection 9
4.4 Installing Detector 11
4.4.1 Wall Mount 11
4.4.2 Corner Mount 12
4.4.3 Pole Mount 13
4.5 Anti-Masking Test 14
5 Configuration 16
5.1 Viewing Status 16
5.2 Configuring the Triple-tech Detector 18
Appendix 1 Security Commitment and Recommendation 23

1 Introduction

1.1 Overview

Wireless Triple-tech Detector performs high precision detection using PIR, microwave detection technology, optical technology and intelligent algorithms. It also eliminates interference caused by small animals, the ambient temperature and changes in the light to ensure that the detector can recognize objects accurately even when people move, or in complex environments. When combined with the camera module, its expanded capabilities allow you to both monitor your scene through videos and images, and check alarms in real time. You also receive alarm notifications when alarms are triggered, so that you can stay up to date on the situation of your site.

1.2 Technical Specifications

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

Table 1-1 Technical specifications

Type	Parameter	Description
Video	Field of View	110° (H); 60° (V)
	Image Type	JPEG
	Resolution	1280 × 960; 640 × 480; 320 × 240;160 × 120
	Frame Rate	2
	Illumination Mode	Infrared Light
	Illumination Range	15 m (49.21 ft)
	Day/Night Switch	Color/Black & White
Function	Indicator Light	1 × green alarm indicator
	Button	1 × power switch 1 × detection range adjustment switch
	Remote Update	Cloud update
	Low Battery Detection	Yes
	Battery Level Display	Yes
	Tamper	Tamper alarm

Type	Parameter	Description		
	Signal Strength	RF Signal test RF-HD signal test		
Wireless	Carrier Frequency	443 Series: 433.1 MHz–434.6 MHz	868 Series: 868.0 MHz–868.6 MHz	915 Series: 915 MHz–928 MHz
	Communication Mechanism	Two-way		
	Communication Distance	433 Series: RF: Up to 1,200 m (3,937.01 ft) in an open space RF-HD: Up to 1,000 m in an open space	868 Series: RF: Up to 1,600 m (5,249.34 ft) in an open space RF-HD: Up to 1,400 m (4593.18 ft) in an open space	915 Series: RF: Up to 1,600 m (5,249.34 ft) in an open space RF-HD: Up to 1,400 m (4593.18 ft) in an open space
	Transmitter Power (EIRP)	433 Series: Limit 10 mW	868 Series: Limit 25 mW	915 Series: Limit 1 W
	Frequency Hopping	Yes		
	Encryption Mode	AES128		
General	Power Supply	CR123A × 4		
	Battery Life	Without Camera: 5 years (triggers 10 alarms a day) With Camera: 3.5 years (triggers alarms twice a week)		
	Operating Temperature	–25 °C to +60 °C (–13 °F to +140 °F)		
	Operating Humidity	10%–90% (RH)		
	Product Dimensions	Without Camera: 211 mm × 106 mm × 94 mm (8.31" × 4.17" × 3.7") With Camera: 263 mm × 106 mm × 94 mm (10.35" × 4.17" × 3.70")		

Type	Parameter	Description
	Packaging Dimensions	Without Camera: 251 mm × 116 mm × 119 mm (9.88" × 4.57" × 4.69”) With Camera: 297 mm × 146 mm × 120 mm (11.69" × 5.75” × 4.72”)
	Net Weight	Without Camera: 651 g (1.44 lb) With Camera: 763 g (1.68 lb)
	Gross Weight	Without Camera: 890 g (1.96 lb) With Camera: 1.06 kg (2.34 lb)
	Installation	Wall mount, pole mount
	Installation Height	0.8 to 1.3 m
	Casing	PC + GF
	Protection	IP65
	Certifications	CE
Technical	Detection Mode	PIR + Microwave
	Sensitivity	PIR:3 levels adjustable
	Detection Range	15 m (49.21 ft), the installation height is 1 m (3.28 ft)
	Detection Speed	0.3 m/s–2 m/s
	Pet Immunity Level	<80 cm (2.62 ft), about 40 kg (88.19 ft)
	White Light Resistance Level	10000 lux
	Two-way Digital Temperature Compensation	Yes
	Scenario	Outdoor, indoor
	Operating Current	20 uA
	Alarm Current	Without Camera: 26mA (Avg); 250 mA (Max) With Camera in Night: 380 mA (Avg); 1.5 A (Max)

2 Checklist

Figure 2-1 Checklist

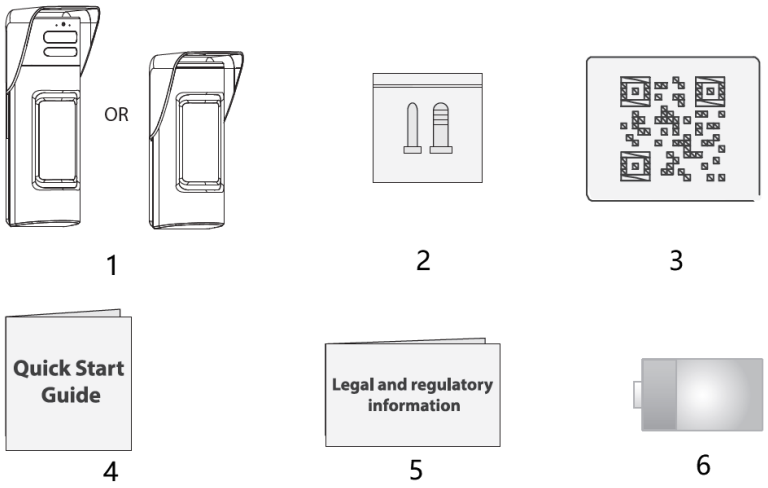


Table 2-1 Checklist

No.	Item Name	Quantity	No.	Item Name	Quantity
1	Wireless triple-tech detector(with/without camera)	1	4	Quick start guide	1
2	Package of screws	1	5	Legal and regulatory information	1
3	QR code	1	6	Battery	4

3 Design

3.1 Appearance

Figure 3-1 Appearance

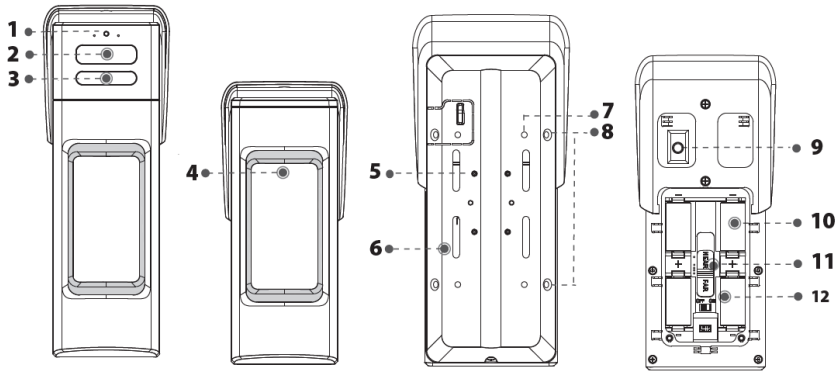


Table 3-1 Structure

No.	Name	Description
1	Photosensitive sensor	Used for detecting the ambient brightness and intensity of the environment.
2	Camera	Captures images when an intrusion alarm is triggered.
3	IR light	Provides IR light for dark environments.
4	Indicator	• Flashes green quickly: Pairing mode or reduced sensitivity mode. • Solid green: An alarm event was triggered. • Solid green for 2 seconds: Pairing successful or the self-detection of camera successful. • Slowly flashes green for 3 seconds: Pairing failed or self-detection of camera failed.
5	Rotation bracket hole	Used to install the rotation bracket.
6	Pole mount bracket hole	Used to install the pole mount bracket.
7	Wall mount screw hole	Used to install the wall mount bracket.
8	Corner mount screw hole	Used to install the corner mount bracket.
9	Tamper switch	When the tamper switch is released, the tamper alarm will be triggered.
10	Battery compartment	The battery receptacle cover on the detector to place batteries.

No.	Name	Description
11	Detection range adjustment switch	Adjust the detecting range of the detector.
12	Power switch	Turn on or off the detector.

3.2 Dimensions

Figure 3-2 Dimensions (mm [inch])

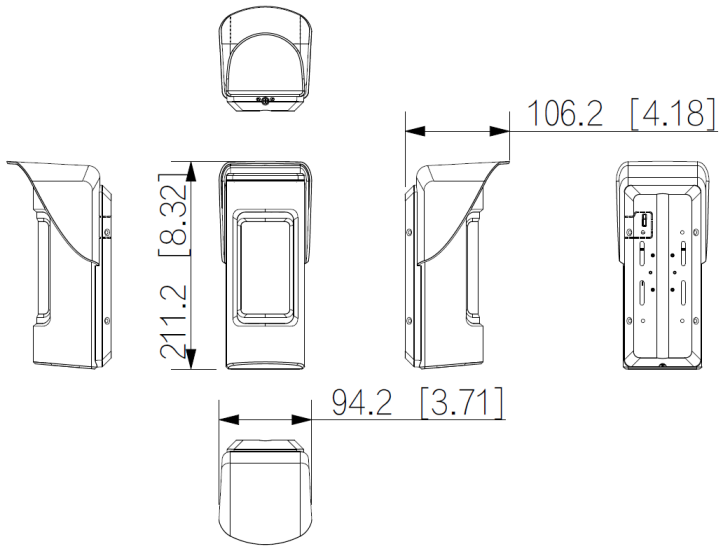
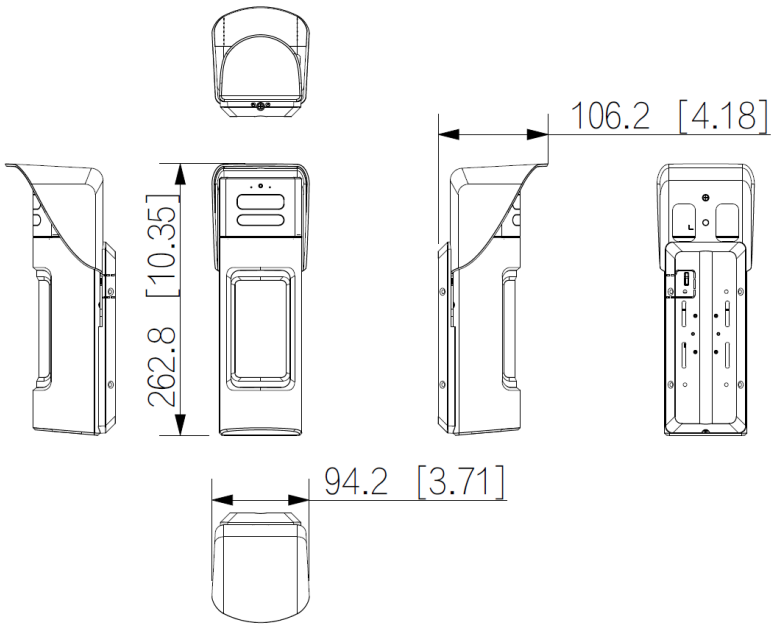


Figure 3-3 Dimensions (mm [inch])



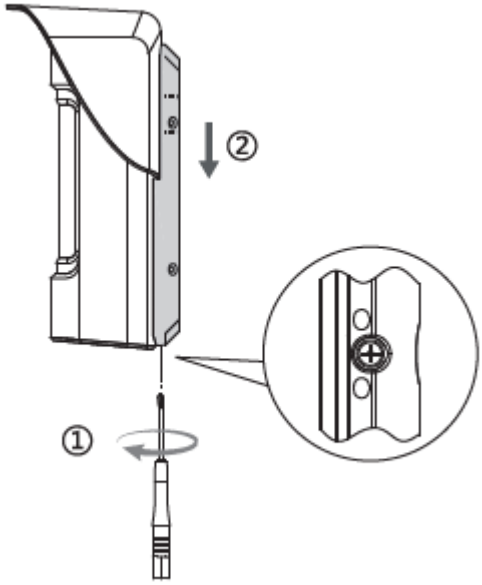
4 Installation

4.1 Powering On

Procedure

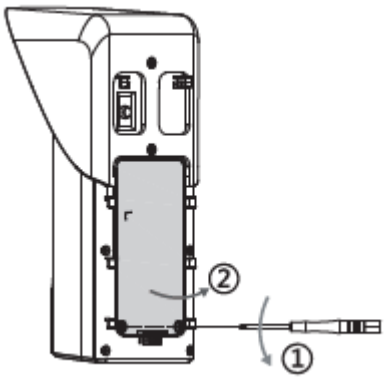
Step 1 Loosen the screw to open the detector.

Figure 4-1 Loosen screw



Step 2 Open the battery compartment.

Figure 4-2 Open compartment

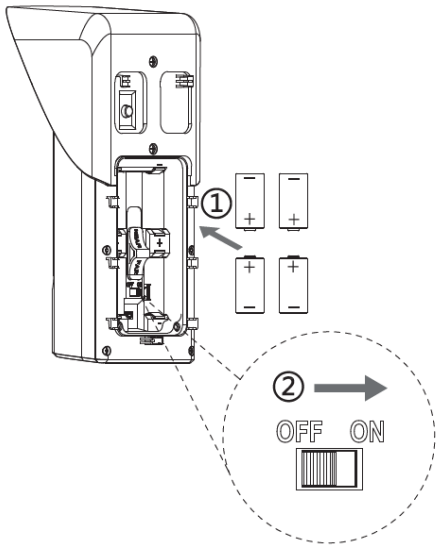


Step 3 Insert batteries into the detector, and then turn on the detector.

- 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 Triple-Tech Detector to the Hub

Background Information

Before you connect the triple-tech detector 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 V2.2.0 or later, and the hub is V2.000.0000006.0.R.250704 or later.
- Make sure that you have already created an account, and added the hub to DMSS.
- Make sure that the hub has a stable internet connection.
- Make sure that the hub is disarmed.

Procedure

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

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

Step 3 Tap **Next** after the triple-tech detector has been found.

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

Step 5 Wait for the pairing.

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

4.3 Field of Detection

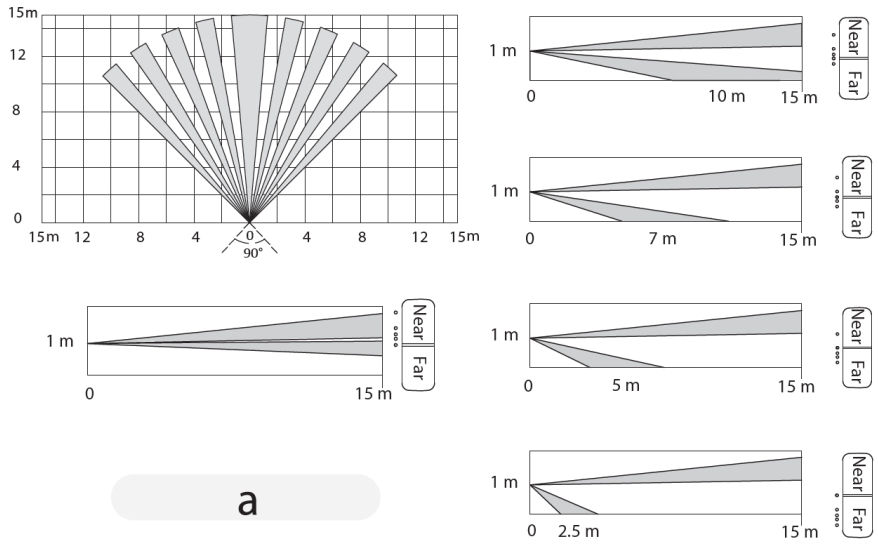
When installing and using the detector, make sure there are no objects partially or fully obscuring the detector's field of view.

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.

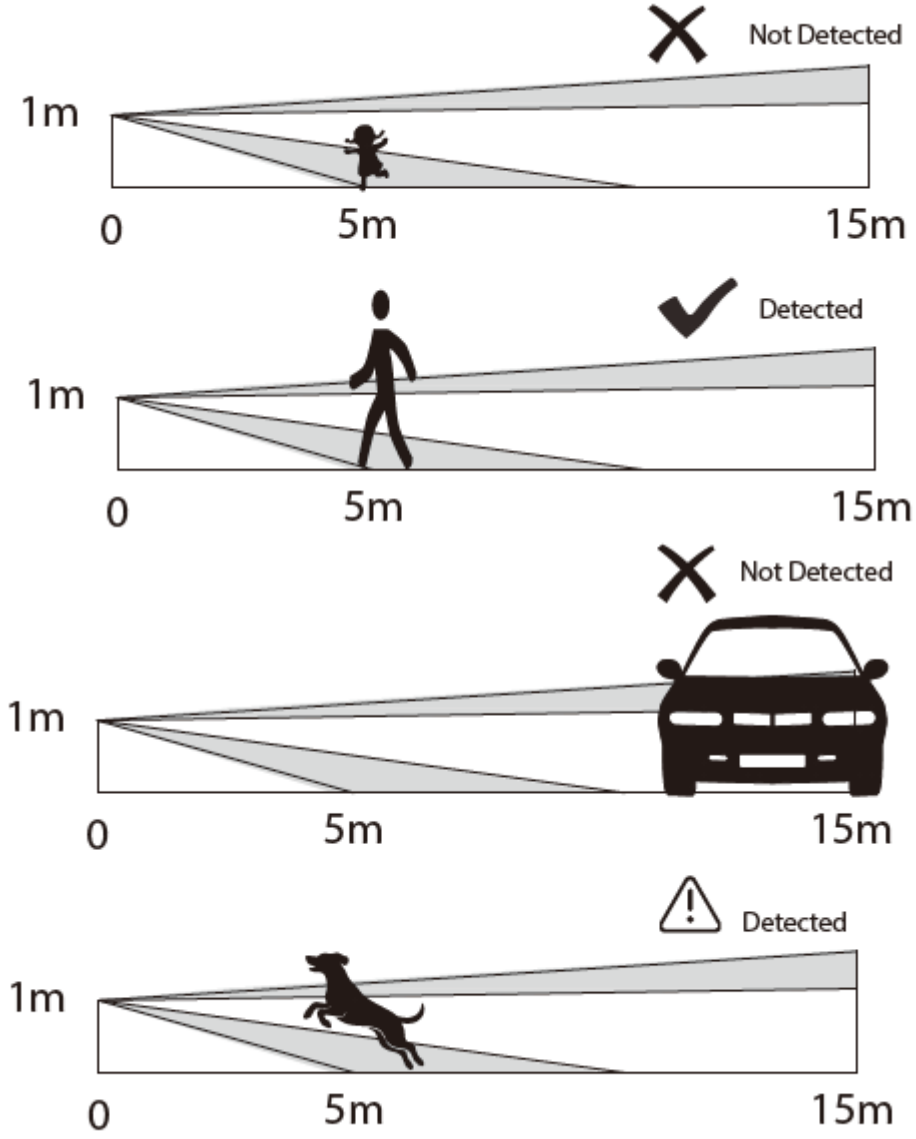
Figure 4-4 Detection range



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



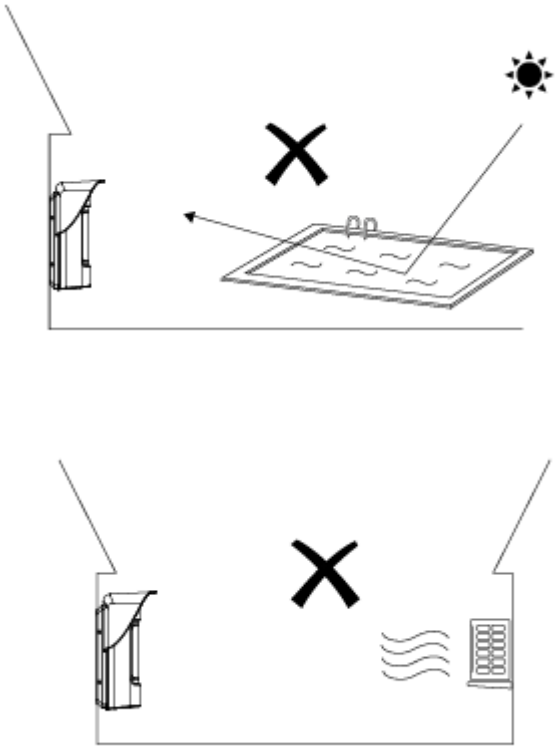
Installation Position

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 and RF-HD test (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 triple-tech detector to the back cover.

Figure 4-7 Wall mount

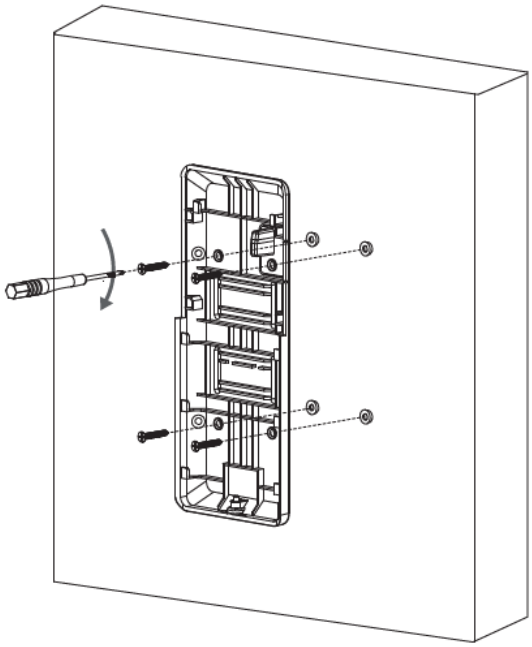
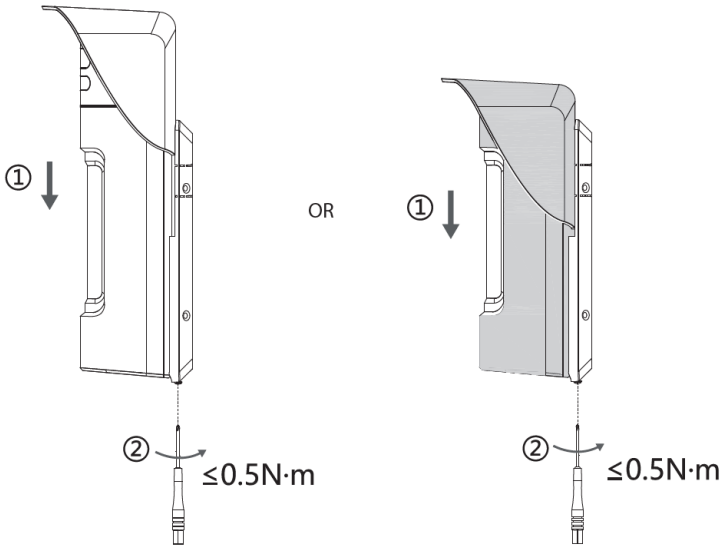


Figure 4-8 Attach the detector to the back cover

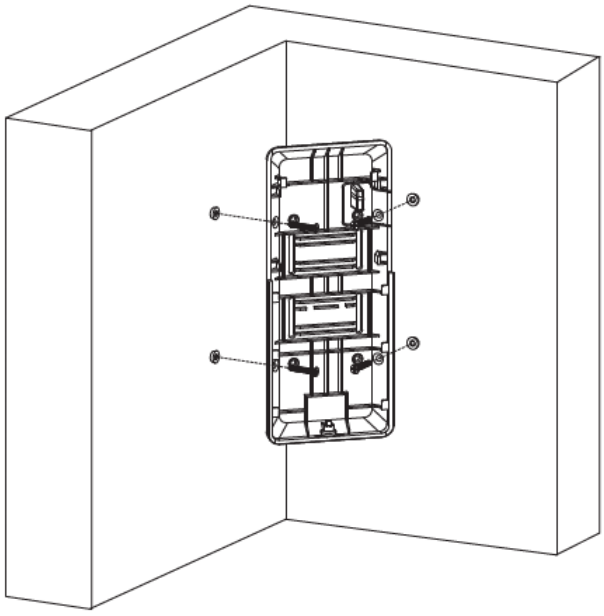


4.4.2 Corner Mount

Procedure

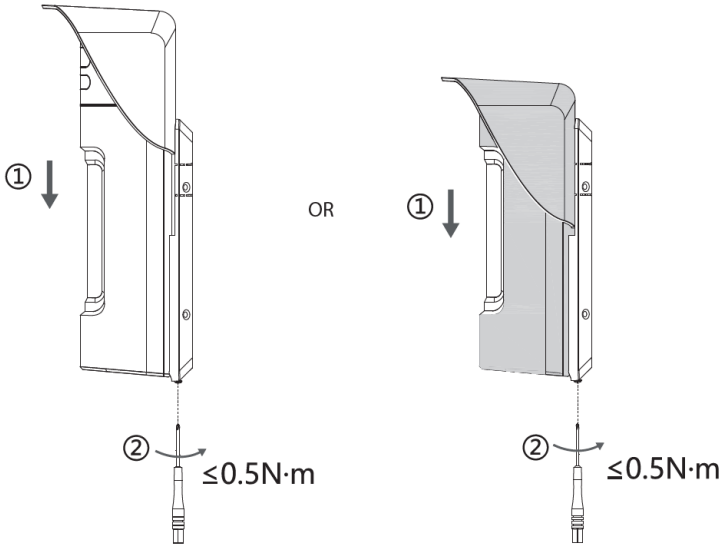
Step 1 Drill 4 holes into the wall according to the hole positions of the detector, and then put the expansion bolts into the holes.

Figure 4-9 Drill holes



Step 2 Attach the detector to the back cover.

Figure 4-10 Attach the detector to the back cover



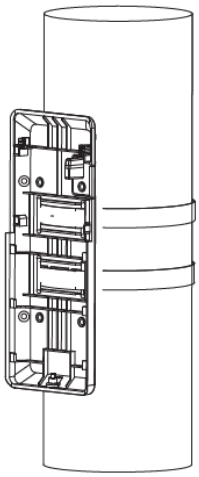
4.4.3 Pole Mount

Procedure

Step 1 Place the bracket on the pipes, cables, or other equipment.

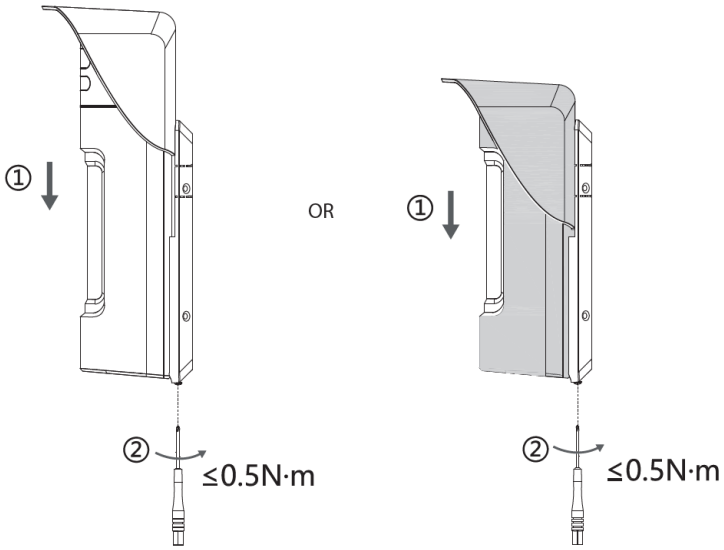
Make sure that the bracket is securely installed.

Figure 4-11 Pole mount



Step 2 Attach the detector to the back cover.

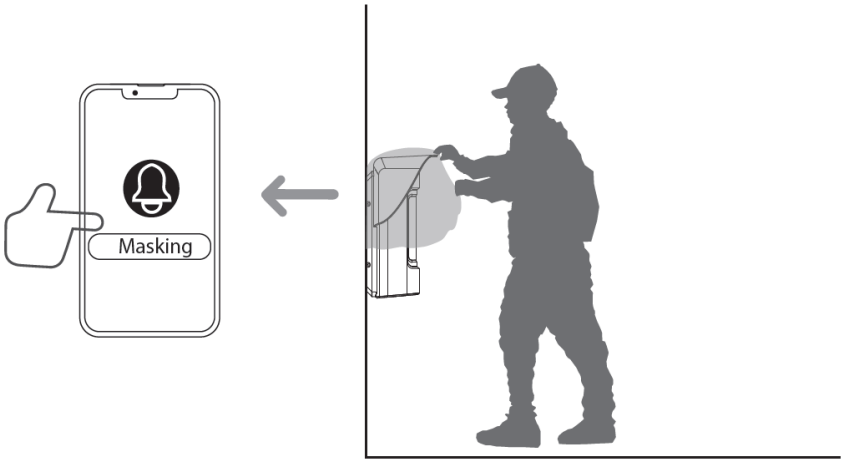
Figure 4-12 Attach the detector to the back cover



4.5 Anti-Masking Test

Before using the detector, perform anti-masking test. Once the detector is masked by other objects, a masking alarm message would be sent to DMSS.

Figure 4-13 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 triple-tech detector 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%

Parameter	Icon	Description
		No battery
Tamper		Opened

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 ± 3 °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. • Online. • Offline.
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

Parameter	Description
Sensitivity	Displays the sensitivity of the detector. The types include: • Low • Medium • High
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.
Program Version	Displays the latest version of the detector program.
Camera Firmware Version	Displays the latest version of the canera program.

5.2 Configuring the Triple-tech Detector

On the hub screen, select a triple-tech 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.
Photos	Only when you add the camera on to the detector can you modify image configuration. • **Image Transmission Speed** : Select from **Fast** and **Normal**. The faster the image transmission speed, the shorter the transmission distance. Select the image transmission rate based on the actual installation scenario. • **Alarms Triggered** : Select the number of alarms that can be triggered within arming/disarming period. • **Image Resolution** : Select from **1280 × 960**, **640 × 480**,**320 × 240** and **160 ×120**. When **Image Transmission Speed** is selected as **Normal**, **1280 × 960**is not supported. • **Alarm Photos** : Select the number of images captured based on your needs. • **Trigger Interval** : Select the trigger interval. • **Snapshot** : Select the number of snapshots from the list. Video is not certificate to IMQ-SISTEMI DI SICUREZZA.
Microwave Detection	• **Microwave Detection** : After being enabled, the detector can start microwave detection. • **Microwave Detection Distance** : Select the detection range.

Parameter	Description
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. Masking function is not certificate to IMQ-SISTEMI DI SICUREZZA.
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.
LED Indicator	**LED Indicator** is enabled by default. If **LED Indicator** is disabled, the LED indicator will remain off regardless of whether the detector is functioning normally or not.
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.

Parameter	Description
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.
Sensitivity	• Adjust sensitivity level of motion detection. • Select from low, medium and high.
Crossed Zone	Select crossed zone from the list, or you can also select **None**.
Link Alarm to Siren	When an alarm is triggered, the detector will report the alarm events to the hub and alert with siren.
Alarm and Video Linkage	When an alarm is triggered, the detector will report the alarm events to the hub and then will link events.
Signal Strength Detection	Test the signal strength of the detector.

Parameter	Description
RF-HD Test	Tap **Start Detection** to perform RF-HD test. • Be advised that you perform RF-HD test when the detector has camera modules. Make sure that the signal has at least 2 bars. • This function is only available when the detector has camera modules.
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.
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