



AI-Fire Smoke Sensing Network Camera

Quick Start Guide



Foreword

General






This manual introduces the functions and operations of the 5 MP IR AI-fire Smoke Sensing Network Camera (hereinafter referred to as "the Device").

Models

DHI-HY-SAV849HAP-E
DHI-HY-SAV849HAN-E

Safety Instructions

The following categorized signal words with defined meaning might appear in the manual.

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

Revision History

Version	Revision Content	Release Time
V1.0.2	Modify the alarm interface.	January 2022
V1.0.1	Modify smoke alarm setting.	December 2021
V1.0.0	First release.	September 2021

About the Manual

- The manual is for reference only. If there is inconsistency between the manual and the actual product, the actual product shall prevail.

- We are not liable for any loss caused by the operations that do not comply with the manual.
- The manual would be updated according to the latest laws and regulations of related jurisdictions. For detailed information, refer to the paper manual, CD-ROM, QR code or our official website. If there is inconsistency between paper manual and the electronic version, the electronic version shall prevail.
- All the designs and software are subject to change without prior written notice. The product updates might cause some differences between the actual product and the manual. Please contact the customer service for the latest program and supplementary documentation.
- There still might be deviation in technical data, functions and operations description, or errors in print. 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 the company names in the manual are the properties of their respective owners.
- Please visit our website, contact the supplier or customer service if there is any problem occurring when using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Important Safeguards and Warnings

The manual will help you to use the Device properly. Read the manual carefully before using the Device, and keep it well for future reference.

Operation Requirements

WARNING

Never ignore any alarm. Failure to respond may lead to serious injury or death.



- Make sure that the power supply of the device works properly before use.
- Use the device according to the operating environment.
- 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.

Installation Requirements

WARNING

- 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.
- Failure to properly install and operate this device will prevent proper operation of the Device and will prevent its response to fire hazards.
- All installation and operations shall conform to your local electrical safety regulations, fire protection regulations, and other relevant regulations.
- Make sure that the application scenario conforms to installation requirements. Contact your local retailer or customer service center if there is any problem.
- Use the Device according to the operating environment.
- Keep the original packing material well because you might need it to pack the Device and send it back for repair.



- 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.
- Keep the original packing material well because you might need it to pack the device and send it back for repair.
- Make sure the application scenario conforms to installation requirements. Contact your local retailer or customer service center if there is any problem.

- All installation and operations shall conform to your local electrical safety requirements, fire protection regulations, and other relevant regulations.

Maintenance Requirements

- Do not clean the device with any cleaning products.
- Do not paint the device. Paint will seal the bents and interfere with the sensor's ability to work normally.

Table of Contents

Foreword	II
Important Safeguards and Warnings	IV
1 Product Information	1
1.1 Introduction.....	1
1.2 Dimensions.....	1
1.3 Technical Information.....	1
1.4 Cable.....	2
1.5 Alarm Configuration.....	4
2 Network Configuration	6
2.1 Initializing Device.....	6
2.2 Modifying Device IP Address.....	7
2.3 Logging in to Web Interface.....	8
2.4 Setting Smoke Alarm.....	9
3 Device Installation	10
3.1 Packing List.....	10
3.2 Installation Principle.....	10
3.3 Installation Position.....	11
3.4 Installation Steps.....	11
3.5 Installing SD Card.....	12
4 Test and Operation	13
4.1 Test.....	13
4.2 Status and Operation.....	13
5 FAQ	14
5.1 Green Power indicator light does not flash.....	14
5.2 Press Test button, there is no alarm.....	14
5.3 Alarm sounds continuously.....	14
5.4 Cannot log in to the web interface.....	14
6 Maintenance	15
Appendix 1 Cybersecurity Recommendations	16

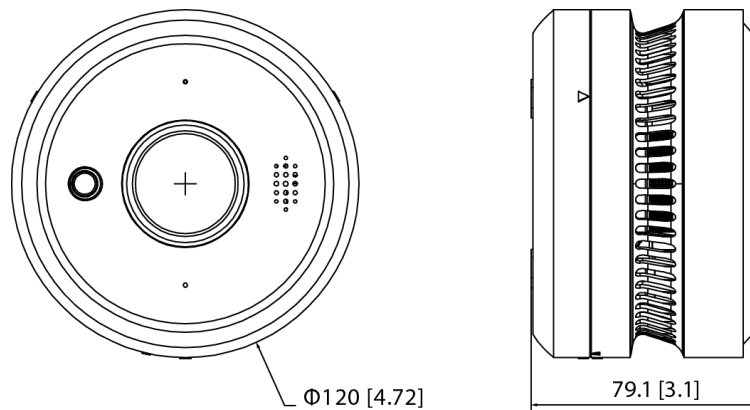
1 Product Information

1.1 Introduction

Together with high-performance microprocessor and advanced electronic technology, the 5 MP IR AI-fire Smoke Sensing Network Camera has the characteristics of high sensitivity and stability. Based on the mounting bracket, it can be easily installed on the ceiling. With built-in high-decibel buzzer, it will send out a sound and light alarm signal in time to remind users to take effective measures immediately when the smoke concentration reaches the alarm setting value. Application scenarios include chain stores, unattended base stations, unmanned power distribution rooms, ATM areas, libraries and places where both fire alarm and video surveillance are needed.

1.2 Dimensions

Figure 1-1 Dimensions (mm[inch])



1.3 Technical Information

Table 1-1 Specification

Specification	Introduction
Model	DHI-HY-SAV849HAP-E, DHI-HY-SAV849HAN-E
Communication	1 RJ-45 PoE 10M/100M Ethernet ports
Indicators	<ul style="list-style-type: none"> Standby: Green indicator flashes once per minute Alarm: Red indicator flashes once per second Fault: Red indicator flashes once per minute Self-test: Red indicator flashes once per second Low voltage: Red indicator flashes once per minute
Protection Area of Smoke Sensor	30 m ² -60 m ²
Operating Principle	Photoelectric
Alarm Method	Sound and LED Indicator
Power Supply	DC12V / PoE and 3V lithium battery

Operating Current	≤30uA (Camera excluded) ≤300mA (Camera included)
Back-up Battery Life	3–5 years
Operating Temperature	–10°C to +55°C (+14°F to +131°F)
Operating Humidity	0%–95% RH (non-condensing)
Alarm Classification	Smoke alarm, fault alarm, undervoltage alarm, AI alarm
Alarm Sound Pressure	≥80 dB (A) @ 3 m (9.84 ft)
Image Sensor	1/2.7" CMOS
Focal Length	2.0mm
Max. Pixel	500W
Day/Night	Auto (ICR)
Video Compression	H.265;H.264;H.264H;H.264B
L:W	16:9
Max. Frame Rate	2592(H)×1944(V)
Bit Rate Control	Variable/Constant
Alarm Linkage	Smoke alarm, AI alarm
Reset	Support
Alarm Input	2 channels in: 5mA 3V–5V DC
Alarm Output	2 channels out: 300mA 12V DC
Temperature Measuring Range	–20°C to +120°C (-4°F to +248°F)
Dimensions	φ120 mm × H79mm (4.72" × 3.11")
Weight (with battery)	420 g (0.93 lb)

1.4 Cable



- Cable type might vary with different devices, and the actual product shall prevail.
- Please waterproof all the cable joints with insulating tape and waterproof tape to avoid short circuit and water damage. For the detailed operation, see the FAQ manual.

Figure 1-2 Cable list

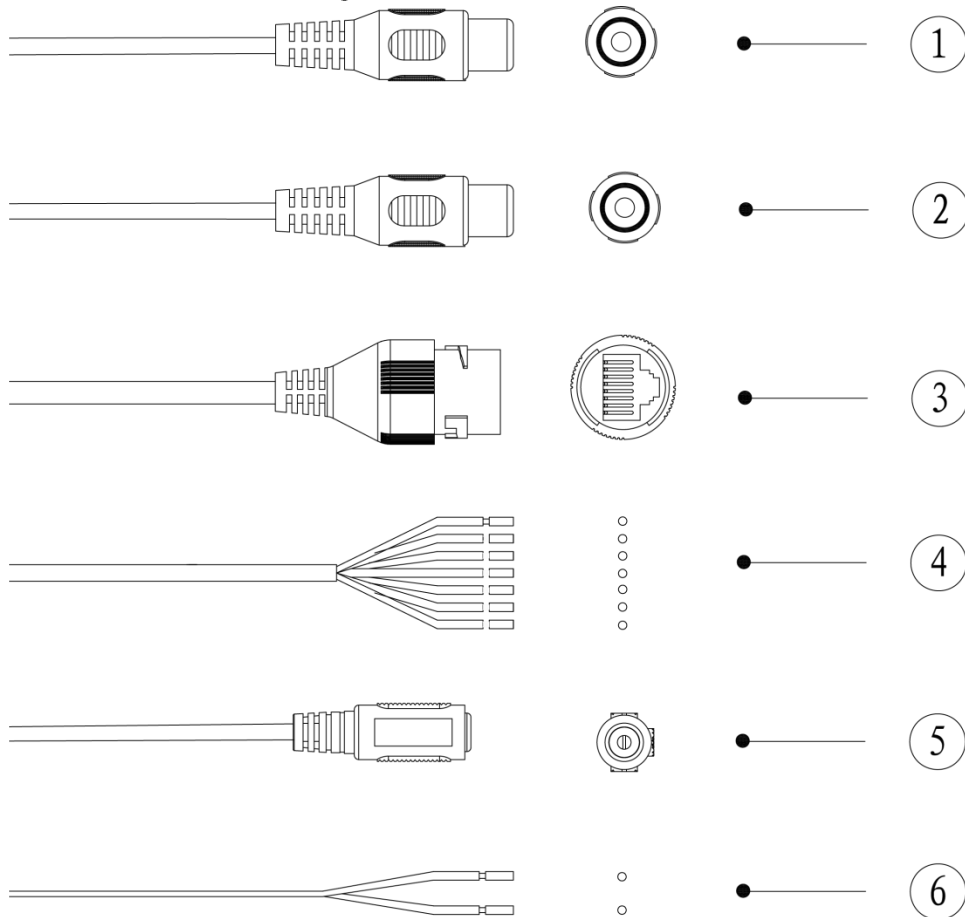




Table 1-2 Cable information

No.	Port name	Description
1	Audio input	RCA port. Connects to sound pickups to receive audio signal.
2	Audio output	RCA port. Connects to speaker to output audio signal.
3	Ethernet port	<ul style="list-style-type: none"> Connects to network with network cable. Provides power to the device with PoE.  PoE is available on select models.
4	Alarm I/O	Includes alarm signal input and output ports, and the number of I/O ports might vary on different devices
5	Power input	Inputs 12 VDC power. Be sure to supply power as instructed in the manual.  Device damage might occur if power is not supplied correctly.
6	RS 485 port	Controls external devices.

For more information about I/O port, see Table 1-3.

Table 1-3 Alarm information

Port	Port Name	Description
Alarm I/O	ALARM_OUT1	Outputs alarm signal to alarm device.
	ALARM_OUT_GND1	
	ALARM_OUT2	When connecting to alarm device, only the ALARM_OUT port and ALARM_OUT_GND port with the same number can be used together.
	ALARM_OUT_GND2	
	ALARM_IN1	Receives the switch signal of external alarm source.
	ALARM_IN2	
	ALM_IN_GND	Connect different alarm input devices to the same ALARM_IN_GND port.

1.5 Alarm Configuration

The Device can connect to external alarm input/output device through input/output port.



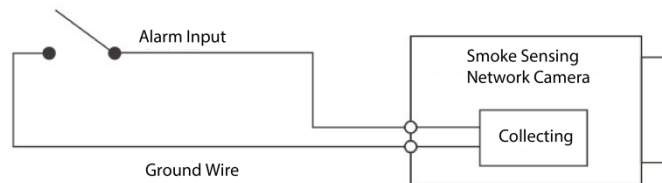
Cut off power before connecting cables.

Step 1 Connect alarm input device to alarm input port of I/O cable.

Device collects different states of alarm input port when the input signal is idling and being grounded.

- When input signal is connecting to +3V to +5V or idling, the Device collects logic "1".
- When input signal is grounded, the Device collects logic "0."

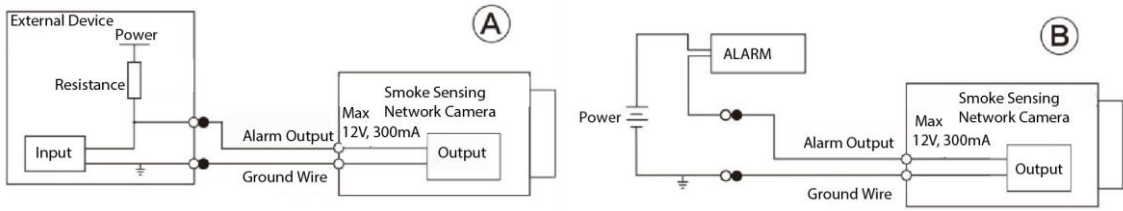
Figure 1-3 Alarm input



Step 2 Connect alarm output device to the alarm output end of the I/O port. The alarm output is open-drain output, which works in the following modes.

- Mode A: Level application. Alarm outputs high and low level, and the alarm outlet is OD, which requires external pull-up resistance (10K Ohm typical) to work. The maximum external pull-up level is 12V, maximum port current is 300mA and the default output signal is high level (external pull-up voltage). The default output signal switches to low level when there is alarm output (As long as the operating current below 300mA, the output low level voltage is lower than 0.8V).
- Mode B: Switch application. Alarm output is used to drive external circuit, the maximum voltage is 12V and the maximum current is 300mA. If the voltage is higher than 12V, please use an additional electric relay.

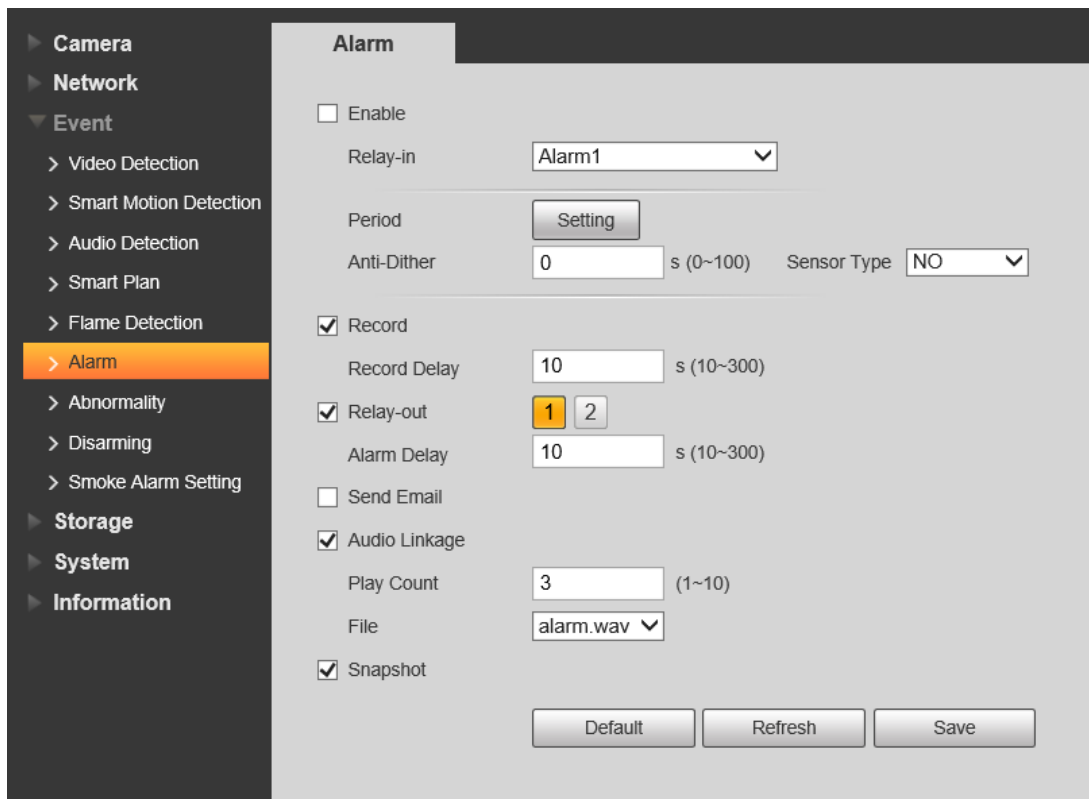
Figure 1-4 Alarm output



Step 3 Log in web interface, and configure alarm input and alarm output in alarm setting.

- The alarm input in the web interface is corresponding to the alarm input end of the I/O port. There will be high level and low level alarm signal generated by the alarm input device when alarm occurs, set the input mode to "NO" (default) if the alarm input signal is logic "0" and to "NC" if the alarm input signal is logic "1".
- The alarm output in the web interface is corresponding to the alarm output end of the device, which is also alarm output end of the I/O port.

Figure 1-5 The alarm interface



2 Network Configuration

Device initialization and IP address setting can be finished with the "ConfigTool" or in web interface. For more information, see the *Web Operation Manual*.



- Device initialization is available on select models, and it is required at first use or after the device being reset.
- Device initialization is available only when the IP addresses of the device (192.168.1.108 by default) and the PC stay in the same network segment.
- Plan useable network segment properly to connect the device to the network.
- The following figures and interfaces are for reference only, and the actual product shall prevail.

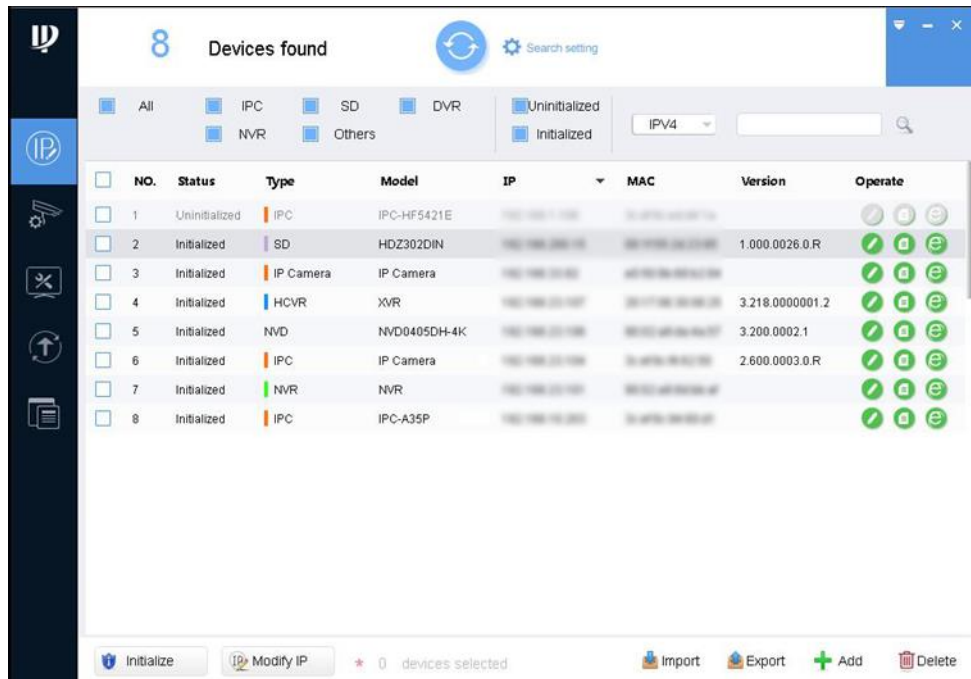
2.1 Initializing Device

Step 1 Double-click "ConfigTool.exe" to open the tool.

Step 2 Click .

The **Modify IP** interface is displayed. See Figure 2-1.

Figure 2-1 Modify IP



Step 3 Click Search setting.

The **Setting** interface is displayed.

Step 4 Enter the start IP address and end IP address of the network segment in which you want to search devices, and then click **OK**.

All the devices found in the network segment are listed.

Step 5 Select one or several devices whose **Status** is **Uninitialized**, and then click **Initialize**. The **Device initialization** interface is displayed.

Step 6 Select the devices that need initialization, and then click **Initialize**.

The password setting interface is displayed. See Figure 2-2.

Figure 2-2 Password setting

Step 7 Set and confirm the password of the devices, then enter a valid email address, and then click **Next**.

The final setting interface is displayed.



Password can be modified or reset in **System Settings**.

Step 8 Select the options according to your needs, and then click **OK**.

The **Initialization** interface is displayed after initialization is completed. Click the success icon (✓) or the failure icon (⚠) for the details.

Step 9 Click **Finish**.

The device status in the **Modify IP** interface (Figure 2-1) turns to **Initialized**.

2.2 Modifying Device IP Address



- You can modify IP address of one or multiple devices in one time. This section is based on modifying IP addresses in batch.
- Modifying IP addresses in batch is available only when the corresponding devices have the same login password.

Step 1 Do "Step 1" to "Step 4" in "2.1 Initializing Device" to search devices in your network segment.



After clicking **Search setting**, enter the username and password, and please make sure they are the same as what you set during initialization, otherwise there will be "wrong password" notice.

Step 2 Select the devices which IP addresses need to be modified, and then click **Modify IP**.

The **Modify IP Address** interface is displayed. See Figure 2-3.

Figure 2-3 Modify IP Address

Modify IP Address

Mode Static DHCP

Start IP Same IP

Subnet Mask

Gateway

Selected number of devices: 11

Step 3 Select **Static** mode, and then enter start IP, subnet mask, and gateway.



- IP addresses of multiple devices will be set to the same if you select the **Same IP** checkbox.
- If DHCP server is available in the network, devices will automatically obtain IP addresses from DHCP server when you select **DHCP**.

Step 4 Click **OK**.

2.3 Logging in to Web Interface

Step 1 Open IE browser, then enter the IP address of the device in the address bar, and then press Enter.

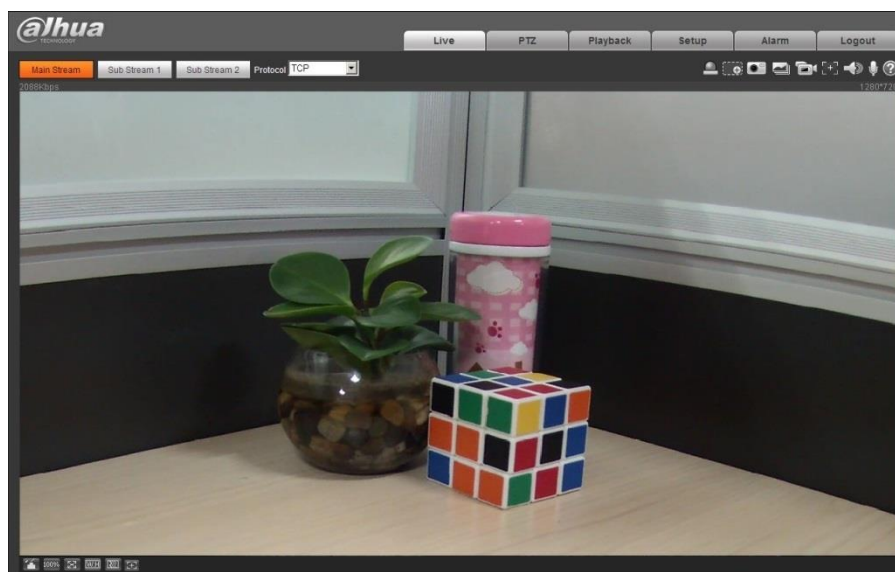
If the setup wizard is displayed, finish the settings as instructed.

Step 2 Enter the user name and password in the login box, and then click **Login**.

Step 3 For first time login, click **Click Here to Download Plugin**, and then install the plugin as instructed.

The main interface is displayed when the installation is finished. See Figure 2-4.

Figure 2-4 Main interface

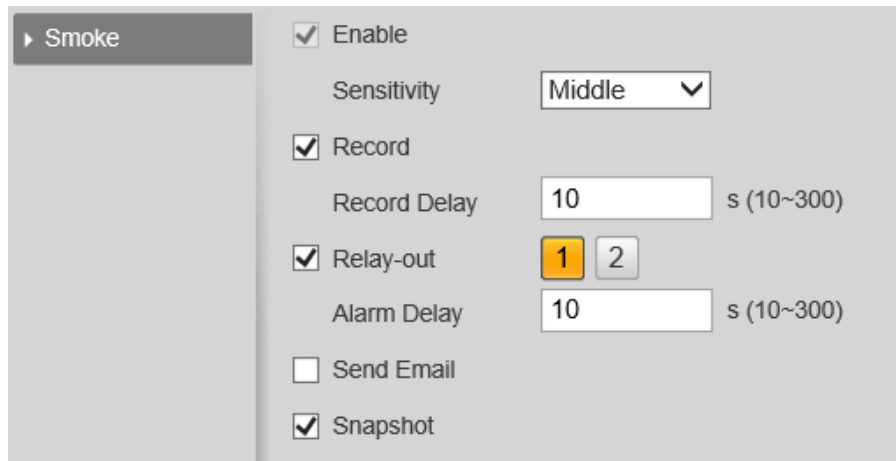


2.4 Setting Smoke Alarm

Step 1 Log in to the web interface and then select **Setting > Event > Smoke Alarm Setting**.

Step 2 Setting smoke alarm.

Figure 2-5 Smoke alarm



The screenshot shows the 'Smoke' settings page in a web interface. On the left, there is a sidebar with a 'Smoke' tab. The main content area contains the following settings:

- Enable
- Sensitivity: Middle (dropdown menu)
- Record
- Record Delay: 10 s (10~300)
- Relay-out: 1 2 (number buttons)
- Alarm Delay: 10 s (10~300)
- Send Email
- Snapshot

Step 3 Click **Save**.

3 Device Installation

3.1 Packing List

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

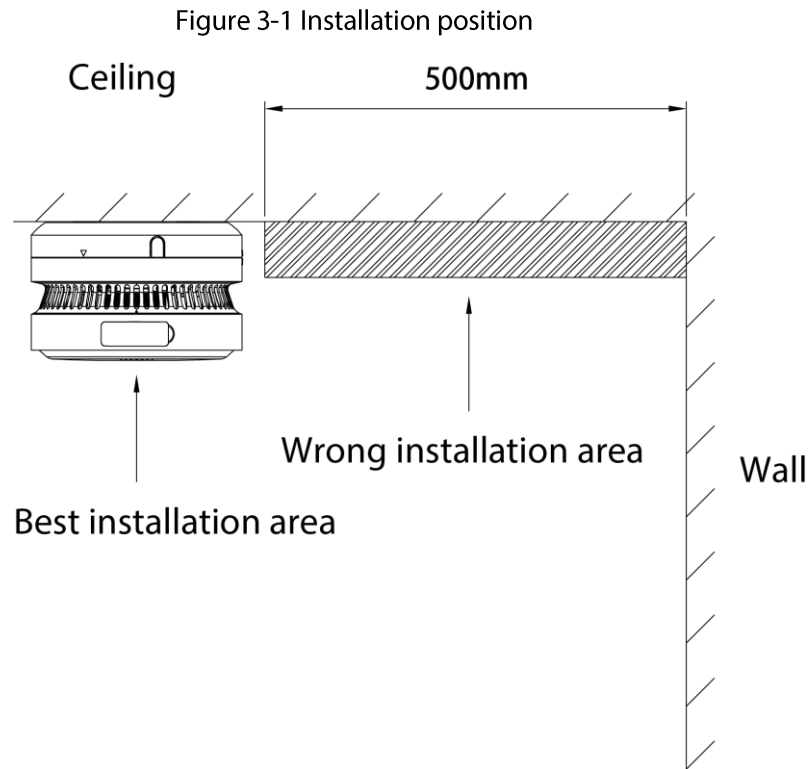
Table 3-1 Checklist

Name	Quantity
Device	1
Positioning Map	1
Screw Package	1
QSG	1

3.2 Installation Principle

- Multiple devices are needed if the length is greater than 10 meters (32.81 ft).
- Make sure the wall is thick enough to install expansion bolts.
- The corresponding signal strength of the device must be above the medium.
- Avoid the installation in following areas:
 - ◇ High-humidity areas such as kitchens, water heaters, and bathrooms.
 - ◇ Areas that are dusty, dirty, or insects frequent.
 - ◇ Areas where the wind speed is too fast such as air conditioner, fan, and heater outlet.
 - ◇ Stoves and other hot and easily polluted places.
 - ◇ Area blocked by other objects.
 - ◇ Within 300 mm (11.81") from the lamp.
 - ◇ In closed spaces such as the upper part of the spire room and the corner of the room.

3.3 Installation Position

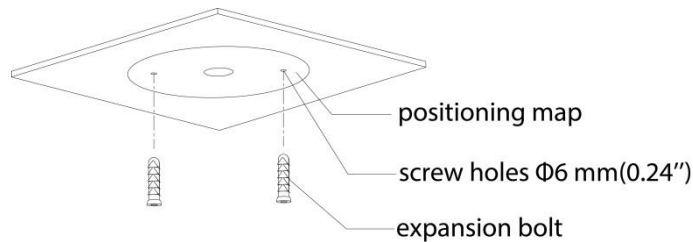


3.4 Installation Steps

Follow below steps to install the device properly.

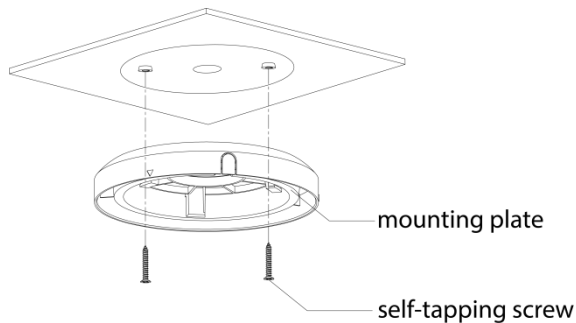
Step 1 Choose suitable place to install positioning map.

Figure 3-2 Installation (1)



Step 2 Drill holes ($\Phi 6$ mm [0.24"]) on the wall as the positioning map shows, and then align the screw holes on the wall with the expansion bolts.

Figure 3-3 Installation (2)



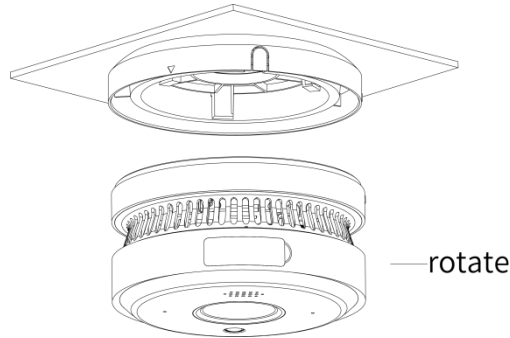
Step 3 Fix the mounting plate with self-tapping screws.

Step 4 Install the battery.

- 1) Correctly insert the battery lead terminals.
- 2) Place the battery in the battery compartment, and arrange the wiring harness.

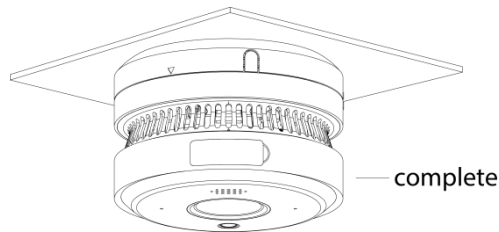
Step 5 Rotate to install the device. Ensure that it is firm and not loose.

Figure 3-4 Installation (3)



Step 6 Complete the installation.

Figure 3-5 Installation (4)

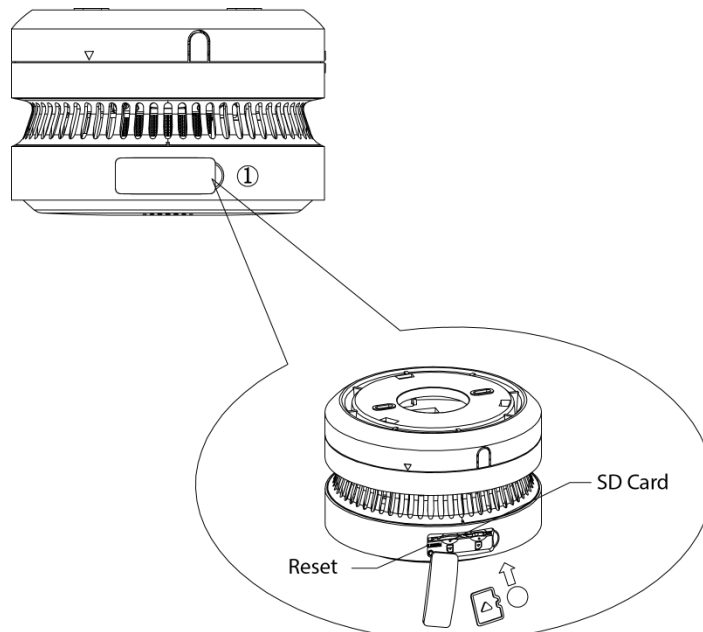


3.5 Installing SD Card



- SD card slot is available on select models.
- Please disconnect the power from the device before installing the SD card.
- Press the reset button for 10 seconds to reset the device.

Figure 3-6 SD Card



4 Test and Operation

4.1 Test

After the installation of the Device or regular maintenance, a test must be carried out to confirm that the Device is operating properly.

During the testing process, the defective Device should be addressed according to "FAQ" and "Maintenance", and then tested again. If it fails to complete the test successfully, please send the Device to the manufacturer for repair.



Do not use real flame for testing in case of detector malfunction or fire.

4.2 Status and Operation

Device self-test

After installing battery, the indicator flashes periodically. Press **Test** button, buzzer beeps and red indicator flashes quickly.

Alarm

When the smoke in the detector reaches a predetermined concentration value or intelligent event is triggered, the indicator light flashes quickly in conjunction with the alarm sound. Press the **Silence** button, the device will temporarily stop emitting the alarm sound. When the smoke concentration decreases to a safe, low level, the device returns to its normal working state.

Sensor fault

When the sensor fails to work, the red indicator light flashes every minute.

Low voltage

When the battery voltage is lower than the certain level, the red indicator light flashes with a short beep every minute. Please replace the battery in time.

5 FAQ

5.1 Green Power indicator light does not flash

Solutions:

- Check the connection of power cable.
- Contact with manufacturer.

5.2 Press Test button, there is no alarm

Solutions:

Disassemble the device to check whether the battery is properly installed.

5.3 Alarm sounds continuously

Solutions:

The battery is low voltage. Please replace the battery.

5.4 Cannot log in to the web interface

Solutions:

- Enter the correct user name and password.
- Check whether the network cable is in good condition, and whether the network configuration is correct; pull out the network cable and plug in again.
- Use the standard power adapter. See the camera label for the power adapter selection.
- Clear the buffer of the browser, check whether the browser permission is enabled, or change the browser.

6 Maintenance

To keep your device in good working condition, please follow these requirements.

- Simulate fire alarm test: once half a year (recommended).
Under normal working conditions, press the **Test** button to ensure that the Device can work normally. If there is a malfunction, please repair it in time. After cleaning, please install the Device and test again.
- Clean the shell: at least once per year (recommended).
Keep the Device free of dust or inserts by gently vacuuming the shell with a soft brush attachment when required. Avoid cleaning solutions on the Device to prevent the possibility of contaminating the sensor.

Appendix 1 Cybersecurity Recommendations

Cybersecurity is more than just a buzzword: it's something that pertains to every device that is connected to the internet. IP video surveillance is not immune to cyber risks, but taking basic steps toward protecting and strengthening networks and networked appliances will make them less susceptible to attacks. Below are some tips and recommendations from Dahua on how to create a more secured security system.

Mandatory actions to be taken for basic device network security:

1. Use Strong Passwords

Please refer to the following suggestions to set passwords.

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

2. Update Firmware and Client Software in Time

- According to the standard procedure in Tech-industry, we recommend to keep your device (such as NVR, DVR, IP camera, etc.) firmware up-to-date to ensure the system is equipped with the latest security patches and fixes. When the device is connected to the public network, it is recommended to enable the "auto-check for updates" function to obtain timely information of firmware updates released by the manufacturer.
- We suggest that you download and use the latest version of client software.

"Nice to have" recommendations to improve your device network security:

1. Physical Protection

We suggest that you perform physical protection to device, especially storage devices. For example, place the device in a special computer room and cabinet, and implement well-done access control permission and key management to prevent unauthorized personnel from carrying out physical contacts such as damaging hardware, unauthorized connection of removable device (such as USB flash disk, serial port), etc.

2. Change Passwords Regularly

We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.

3. Set and Update Passwords Reset Information Timely

The device supports password reset function. Please set up related information for password reset in time, including the end user's mailbox and password protection questions. If the information changes, please modify it in time. When setting password protection questions, it is suggested not to use those that can be easily guessed.

4. Enable Account Lock

The account lock feature is enabled by default, and we recommend you to keep it on to guarantee the account security. If an attacker attempts to log in with the wrong password several times, the corresponding account and the source IP address will be locked.

5. Change Default HTTP and Other Service Ports

We suggest you to change default HTTP and other service ports into any set of numbers between 1024–65535, reducing the risk of outsiders being able to guess which ports you are using.

6. Enable HTTPS

We suggest you to enable HTTPS, so that you visit Web service through a secure communication channel.

7. MAC Address Binding

We recommend you to bind the IP and MAC address of the gateway to the device, thus reducing the risk of ARP spoofing.

8. Assign Accounts and Privileges Reasonably

According to business and management requirements, reasonably add users and assign a minimum set of permissions to them.

9. Disable Unnecessary Services and Choose Secure Modes

If not needed, it is recommended to turn off some services such as SNMP, SMTP, UPnP, etc., to reduce risks.

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

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

10. Audio and Video Encrypted Transmission

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

Reminder: encrypted transmission will cause some loss in transmission efficiency.

11. Secure Auditing

- Check online users: we suggest that you check online users regularly to see if the device is logged in without authorization.
- Check device log: By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.

12. Network Log

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

13. Construct a Safe Network Environment

In order to better ensure the safety of device and reduce potential cyber risks, we recommend:

- Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.
- The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.
- Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.

- Enable IP/MAC address filtering function to limit the range of hosts allowed to access the device.

More information

Please visit Dahua official website security emergency response center for security announcements and the latest security recommendations.