



# Fire Detection Camera

User Manual

## Legal Statement

### About this Document

- This Document includes instructions for using and managing the Product. Pictures, charts, images and all other information hereinafter are for description and explanation only.
- The information contained in the Document is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of the Document at the Hikvision website (<https://www.hikvision.com>). Unless otherwise agreed, Hangzhou Hikvision Digital Technology Co., Ltd. or its affiliates (hereinafter referred to as "Hikvision") makes no warranties, express or implied.
- Please use the Document with the guidance and assistance of professionals trained in supporting the Product.

### About this Product

This product can only enjoy the after-sales service support in the country or region where the purchase is made.

### Acknowledgment of Intellectual Property Rights

- Hikvision owns the copyrights and/or patents related to the technology embodied in the Products described in this Document, which may include licenses obtained from third parties.
- Any part of the Document, including text, pictures, graphics, etc., belongs to Hikvision. No part of this Document may be excerpted, copied, translated, or modified in whole or in part by any means without written permission.
- **HIKVISION** and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions.
- Other trademarks and logos mentioned are the properties of their respective owners.

### LEGAL DISCLAIMER

- TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS DOCUMENT AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED "AS IS" AND "WITH ALL FAULTS AND ERRORS". HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.
- YOU ACKNOWLEDGE THAT THE NATURE OF THE INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INFECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.
- YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS

# Fire Detection Camera

---

ABUSES.

- IN THE EVENT OF ANY CONFLICTS BETWEEN THIS DOCUMENT AND THE APPLICABLE LAW, THE LATTER PREVAILS.

© Hangzhou Hikvision Digital Technology Co., Ltd. All rights reserved.

## Introduction

The purpose of this section is to make sure the user can use the product correctly in this manual to avoid risky operation or property damage. Before using this product, please read the product manual carefully and keep it for future reference.

## Pre-Use Description

- Go to our website ([www.hikvision.com](http://www.hikvision.com)) to get manuals, application tools, and development materials.
- Please sync the device before use.
- Part of the web page configuration in the manual is applicable to the latest software version. Please contact technical support to update software.

## Applicable Model

Product Name	Product Model
Fire Detection Camera	HF-VH243

## Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
 <b>Note</b>	Provides additional information to emphasize or supplement important points of the main text.
 <b>Caution</b>	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
 <b>Danger</b>	Indicates a hazardous situation which, if not avoided, will or could result in death or serious injury.

### Safety Instruction

---



- During product installation and use, the electrical safety regulations of the country and area of use should be strictly observed.
  - Please use the power adapter provided by normal manufacturer. See product parameter table for the specific requirements of the power adapter.
  - The plug or socket of the device is the device that disconnects the power supply. Do not block the plug or plug in or unplug.
  - Do not connect more than one product to the same power adapter (it may cause excessive heat or fire if the adapter is overloaded).
  - Make sure to disconnect the product power supply during wiring, disassembling, etc., and do not power on the device.
  - Warning: Battery of incorrect model may cause explosion.
  - Changing batteries with incorrect models (e.g., certain types of lithium batteries) may invalidate safety protection.
  - Do not put the battery in the fire or in the heater. Do not crush, bend, or cut the battery, which may cause explosion.
  - Do not place the battery in extremely high temperature environment. The battery may explode or leak flammable liquid or gas.
  - Do not place the battery in extremely low air pressure environment. The battery may explode or leak flammable liquid or gas.
  - Discarded batteries will pollute the environment. Please follow the instructions to dispose of the used batteries.
  - When installing the product on a wall or ceiling, fix the product firmly.
  - To avoid heat build-up, keep the device ventilated.
  - If the product smokes, it may cause bad taste, or sound noise, please disable the power supply and unplug the power cable. Please contact the distributor or service center.
  - If laser product is used, do not direct the laser of the laser smart dome to avoid possible harm to the human eye.
  - The laser of laser product can expose flammable objects to fire hazards. Please keep a safe distance during installation.
  - If the product is not working normally, please contact the store or nearest service center of the device. Do not disassemble or edit the product in any way. (The Company shall not be responsible for problems caused by unauthorized editing or repair).
- 



- Product functions can only be carried out when the product is installed and maintained. This product is used to help you prevent disaster, but it cannot replace you for on-site inspection, or prevent the accident from happening or expanding. You should still be more vigilant, be safer, and pay careful attention to the safety of your person and property.
  - Please follow the installation method in this guide to install the device.
  - To prevent injury, the device must be secured to the wall or ceiling.
  - The serial port of the device is for debugging only. The user is not allowed.
  - Do not let the object fall on the product or vibrate the product so that the product is away from the point where magnetic field interference exists. Do not install the product in the area of surface vibration or shock
-

## Fire Detection Camera

---

risk (ignoring this item may damage the product).

- Do not use the product in high temperature, low temperature, or high humidity. Please refer to the product parameter table for temperature and humidity requirements.
  - The device's enclosure position temperature may be too hot. It may take about half an hour after powering off.
  - For low-temperature products, preheat before starting. The pre-heating time should be determined according to different environment. Make sure the heat is enough before starting the product.
  - Do not place exposed flame sources on the device, such as lighted candles.
  - Do not target the product lens to strong light source. Otherwise, the camera or thermal imaging detector will be damaged.
  - The product cannot be exposed to rain or humidity.
  - Do not place the product in an environment with corrosive gas, which may cause damage to the device.
  - Avoid placing the product in direct sunshine location, place with poor ventilation, or near heat sources such as heater or heater (ignoring this item may cause fire risk).
  - When cleaning product lens or shield, please use a sufficiently soft dry cloth or other alternative to wipe the outer surface. Do not use basic cleaning agent to wash the lens or shield.
  - When removing the transparent cover, please use randomly carried gloves to avoid direct contact with the transparent cover. The acid sweat of the finger film may corrode the surface coating of the transparent cover. The device may be fuzzy when scratching the transparent cover with hard objects, which may affect the image quality.
  - The product may face network security problems. Please strengthen the protection of personal information and data security. Please contact us when you find that the device may have network security risks.
  - Please understand that it is your responsibility to reasonably configure all password and other related product security settings, and to properly keep your user name and password.
  - Please keep all the original packaging materials of the product properly, so that when the problem persists, the packaging material can be used to package the product and send to the agent or return to the manufacturer. The company shall not be liable for the accidental damage caused by the transportation of non-original packaging material.
- 

### Note

Quality Requirements for Installation and Maintenance Personnel:

- Qualification certificate or experience in video live view system installation, maintenance, and related tasks (such as high-altitude work). You must also have the following knowledge and operation skills.
- Basic knowledge and installation skills of live view system and component.
- Basic knowledge and operation skills of low-voltage wiring and low-voltage electronic wiring.
- It has basic network security knowledge and skills, and is able to read and understand the contents of this manual.

The requirements for lifting devices:

- Use a safe elevator device suitable for installation location and device installation mode.
  - The lifting device has enough lifting and lifting level to reach the installation position.
  - The lifting device has good safety performance.
-

# CONTENTS

Chapter 1 Product Introduction . . . . .	1
1.1 Product Description . . . . .	1
1.2 Product Function . . . . .	1
1.3 Appearance Interface . . . . .	1
Chapter 2 Wiring and Installation . . . . .	5
2.1 Product Wiring . . . . .	5
2.2 Product Installation . . . . .	5
2.2.1 Pre-Installation Description . . . . .	5
2.2.2 Ceiling Installation . . . . .	5
2.2.3 Adjust the Sphere Direction . . . . .	6
2.2.4 Installing Waterproof Tape . . . . .	7
2.2.5 Installing Network Port Waterproof Sleeve . . . . .	8
Chapter 3 Pre-Use Operation Information . . . . .	10
3.1 Network Connection . . . . .	10
3.2 Activate Device . . . . .	10
3.2.1 Activate Device via SADP Software . . . . .	10
3.2.2 Activate via Web Page . . . . .	11
3.3 Access Device . . . . .	12
3.3.1 Access Device via Web Client . . . . .	12
3.3.2 Access Device via EZVIZ Cloud . . . . .	12
3.3.3 Add Device to Hik-Connect Video Mobile Client . . . . .	13
Chapter 4 Web Client Configuration and Operation . . . . .	15
4.1 Live View . . . . .	15
4.2 Video Playback . . . . .	16
4.3 View Picture . . . . .	16
4.4 Parameter Configuration . . . . .	17
4.4.1 System Parameters . . . . .	17
4.4.2 Network Parameters . . . . .	22
4.4.3 Video and Audio Parameters . . . . .	25
4.4.4 Image Parameters . . . . .	28
4.4.5 Event Parameters . . . . .	32
4.4.6 Storage Parameters . . . . .	37

# Chapter 1 Product Introduction

## 1.1 Product Description

The fire detection camera is a new type of integrated surveillance device. It features functions including high-temperature anomaly alerts in indoor environments, local audio-visual alarms, superimposing alarm information on video footage, and video verification. Capable of achieving early fire detection and alarms, as well as visual verification and management of on-site incidents, this camera is widely deployed in fire prevention-critical locations such as hotels, financial institutions, logistics hubs, warehouses, cultural archives, and laboratories, effectively addressing both security monitoring and fire protection requirements.

## 1.2 Product Function

This section provides information about the security camera, and the device is familiar with it.

- High quality imaging with 4 MP resolution.
- Support On/Off Duty Detection.
- Support local alarm indicator.
- Support 30m-infrared / 10m-white light supplemental lighting.
- Water and dust resistant (IP66).
- Supports overlay of OSD alarm events.
- Supports PoE power supply and simple cabling.

## 1.3 Appearance Interface



The product picture in this manual is a picture. Please use the actual device.

---

## Fire Detection Camera

---

### Sphere Appearance and Indicator

- 1. Indicator
- 2. LED
- 3. Microphone
- 4. Visible Light Camera
- 5. Temperature Sensor
- 6. Plastic Base
- 7. Speaker

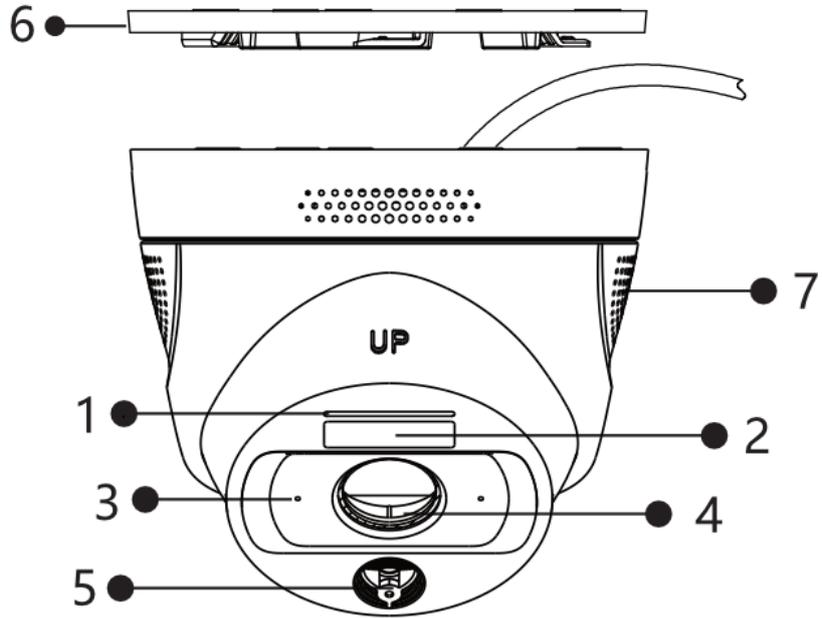


Figure 1-1 Sphere Appearance

Table 1-1 Indicator Description

Indicator	Description
Red/Blue Light	Alarm (Eligible in Red/Blue Light Mode)
Green Light	Normal Operation
Yellow Light	Fault

# Fire Detection Camera

---

## Device Interface Description

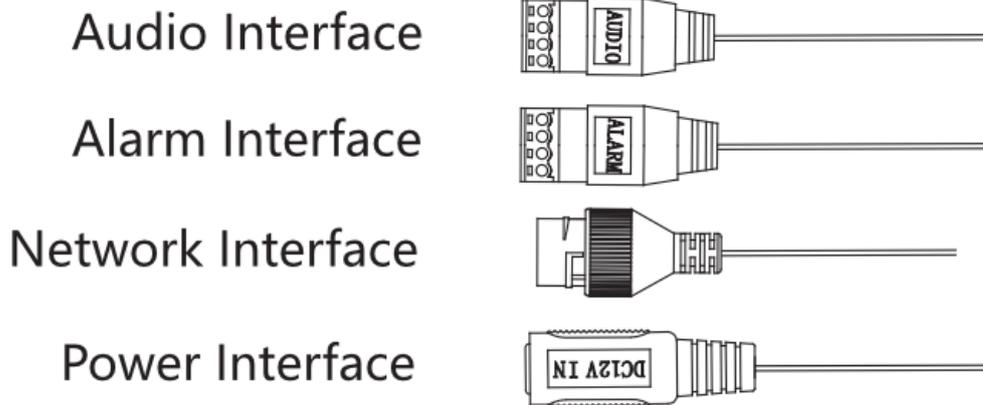


Figure 1-2 Device Interface

### Power Output

DC 12 V.

### Alarm Interface

You can connect to alarm device.

### Audio Interface

You can connect to audio device.



### Note

The model of HF-VH243(B) does not have audio interface and alarm interface.

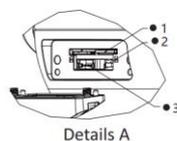
---

### Network Interface

Network Signal Output



View Details A



1. Micro SD Card
2. Reset Button
3. Debug UART

Details A

Figure 1-3 SD Card Interface

### Card Slot

You can plug in microSD card for local storage.

### Reset Button

## Fire Detection Camera

---

Press and hold the key, and then power on the device. Press 10 to 15 seconds to release the key. All parameters will be restored to factory settings.

### Debug UART

Reserved.

---



Note

The serial port of the device is for debugging only. The user is not allowed.

---

## Chapter 2 Wiring and Installation

### 2.1 Product Wiring

The device has external interfaces, including power interface, audio input/output interface (only for HF-VH243), alarm input interface, alarm output interface (only for HF-VH243, and network interface. The alarm interface wiring description is as follows:

Table 2-1 Alarm Interface Description

ID	Description	Wiring Description
IN	Connect Alarm Input Signal Positive Pole	One-Way Access Alarm Input Signal
G	Connect Alarm Input Signal Negative Polarity	
OUT1A, OUT1B	Connect Alarm Output Signal	The alarm output signal of one route is connected, and the positive and negative poles are not distinguished.
OUT2A, OUT2B	Connect Alarm Output Signal	

### 2.2 Product Installation

#### 2.2.1 Pre-Installation Description

- Please make sure the device in the box is intact before installation. All components are complete.
- The wall should be of a certain thickness and be able to withstand at least 4 times the total weight of the device and installation accessories.
- If it is a cement ceiling wall, please install expansion screw (the mounting hole of expansion screw should be the same with the bracket), and then install the bracket.
- If it is a wood wall, the self-tapping screw can be used to directly install the bracket.
- The brackets in the manual are optional. Please select according to actual needs.

#### 2.2.2 Ceiling Installation

The device can be used for ceiling mounting, wall mounting, and lifting. DS-1273ZJ-130-TRL wall mounting bracket is recommended for wall mounting. DS-1271ZJ-130-TRL lifting bracket is recommended for lifting.

Three installation methods are similar. Take ceiling mounted installation as an example.

##### Steps

1. Take out the installation sticker that comes with device, stick the sticker onto the wall of the camera that needs to be installed, and drill holes according to the holes marked on the sticker.

## Fire Detection Camera

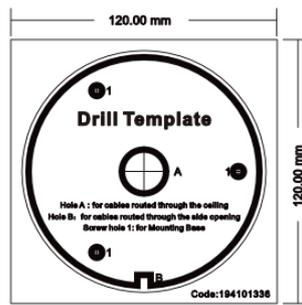


Figure 2-1 Installing Sticker

2. Use three PA4 × 25 screws to secure the device base to the wall.

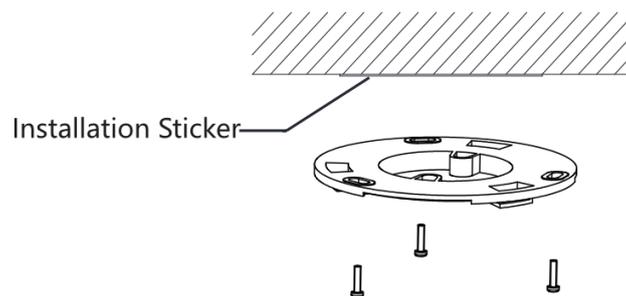


Figure 2-2 Fixed Base

3. Set up and connect the power cables and network cables of the camera, and keep the power cables insulated.
4. Align the camera body with the plastic base, tighten it in the indicated direction.

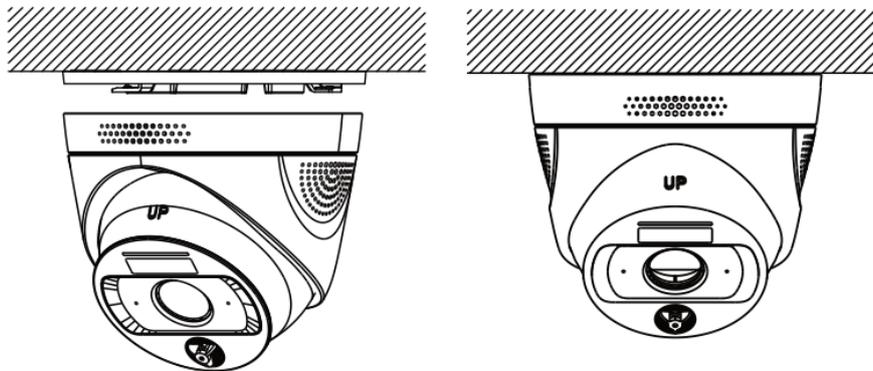


Figure 2-3 Install Device



Note

After installation, the UP ID on the sphere should face up.

### 2.2.3 Adjust the Sphere Direction

Adjust the cover and sphere to the scene.

Compare the video image on the web page and adjust the camera angle by rotating the cover and sphere.

## Fire Detection Camera

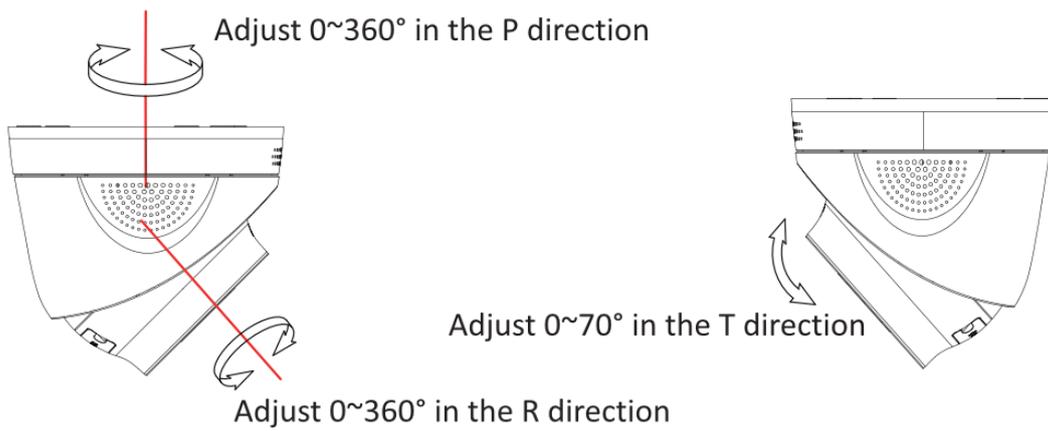


Figure 2 to 4 Adjust Sphere Direction

### 2.2.4 Installing Waterproof Tape

When installing the device outdoors, it is required to install water-proof tape to prevent short circuit of the route.

#### Prerequisite

Set the cable first.

#### Steps

1. Please tear off the release paper on the back of the water-proof tape.
2. Stretch the water-proof tape to the two ends and to about 2 times the initial length.

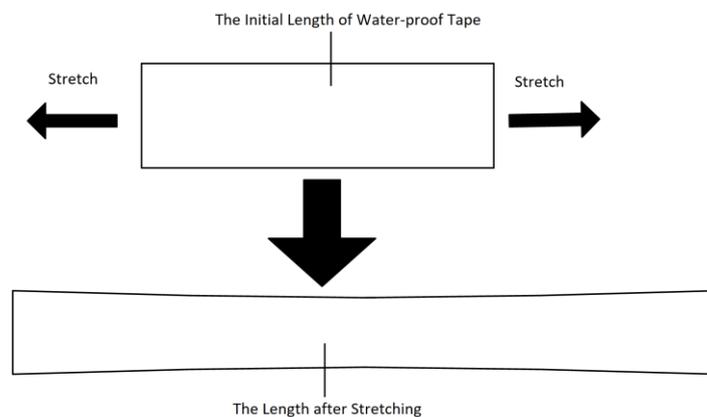


Figure 2-5 Stretch Water-Proof Tape

3. The tensioned waterproof tape should be applied to the terminal and the cable nearby. Keep the adhesive tape tight during the winding.

---

## Fire Detection Camera

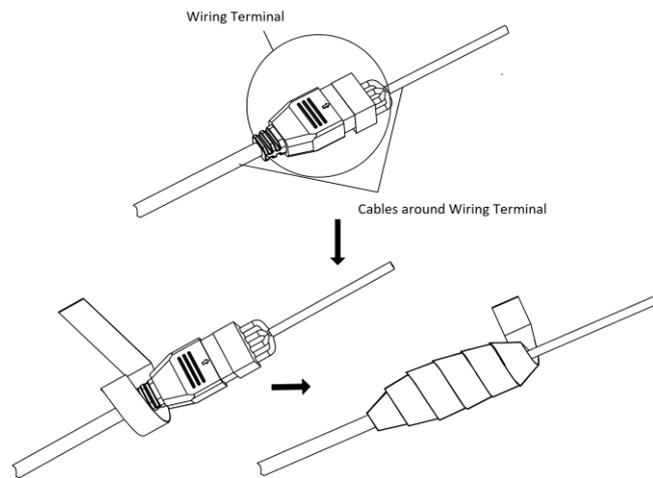


Figure 2-6 Wrapping Waterproof Tape

4. Press the waterproof tape on both sides of the terminal in the direction shown in the picture to achieve the insulation seal.

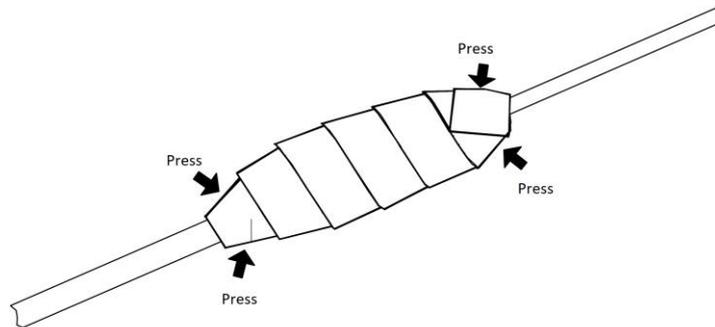


Figure 2-7 Press Water-Proof Tape

### 2.2.5 Installing Network Port Waterproof Sleeve

When the device is in use, it is used to install the network port waterproof sleeve to prevent network cable water entering.

#### Prerequisite

Please set network cable first.

#### Steps

1. Thread the cable through the screw cap and the waterproof sleeve body.
2. Open the water-proof glue ring and connect the cable between the body of the water-proof sleeve and the screw cap.
3. Insert the o-shaped glue ring into the network port, and insert the network cable into the network port.

## Fire Detection Camera

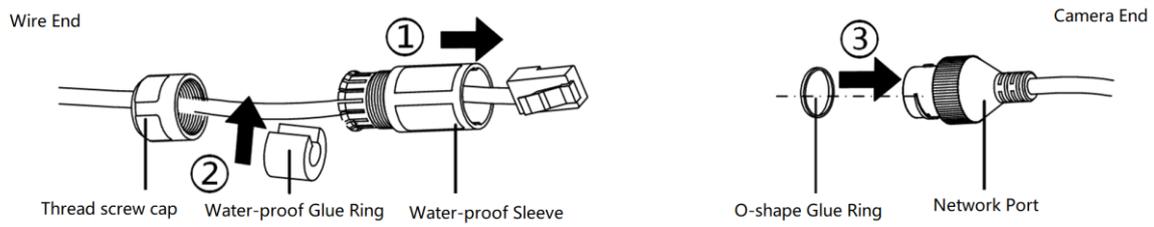


Figure 2-8 Installing Network Cable

4. Align the gap between the network port and the snap of the water barrier body. Connect the water barrier body to the port and turn it clockwise.
5. Put the water-proof glue ring into the body of the water-proof hat.
6. Rotate clockwise to fasten the screw cap, and press the water-proof glue ring.

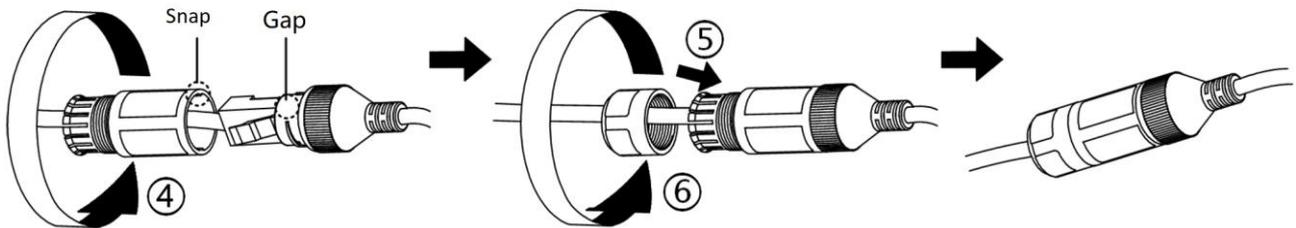


Figure 2-9 Installed

## Chapter 3 Pre-Use Operation Information

### 3.1 Network Connection

---



If you connect the product to the Internet, including but not limited to cyber attack, hacking, virus infection, etc., the company will not be responsible for product work exception, information disclosure, etc., but the company will provide technical support to you.

---

Use network cable to connect the device to Ethernet. After connecting to the network, you can enter the device web page via browser to configure device functions and parameters.

### 3.2 Activate Device

In network access, to protect the security and privacy of personal account, you can set a login password to activate the device, prevent others from logging in to the device, and get the data.

---



Please refer to the latest client software manual for activation method through client software.

---

#### 3.2.1 Activate Device via SADP Software

Download and run SADP software. The SADP software will search for inactive devices or all online devices in the same network segment. The list will display information such as device type, IP address, security status, and device serial No. You can activate the inactive device via SADP software.

##### Prerequisite

Power on the device and connect to the network.

##### Steps

1. Download SADP software from official website and run.
  2. Select the device to activate. Information about the device will be displayed on the right side of the list.
  3. Set the device password in the Activate Device field, and click *OK* to complete the activation.
- 



- In order to protect your privacy and corporate data and avoid network security problems of device products, it is recommended to set strong password that meets security requirements.
  - To improve the security of product network, the password should be between 6 and 16 characters, and it should contain at least 2 of the following types: digits, lowercase letters, and uppercase letters. Special characters are not allowed.
- 

After the device is activated, the activation status in the list will be updated to activated.

4. Optional: Edit device IP address.
-

## Fire Detection Camera

---

- 1) Select the activated device in the device list.
- 2) Enter IP address, subnet mask, gateway, and other information in the modified network parameter on the right.



Edit IP address according to actual needs. For example, when you need to log in to device web page to configure device, set the IP address of the device and the IP address of the computer to log in to device web page to the same network segment.

---

- 3) Enter the password to activate the device after editing, and click *Edit*.  
The parameter settings such as IP address will take effect. The device will reboot after network parameters are edited.

### 3.2.2 Activate via Web Page

Access the device through the web page and activate the device.

#### Steps

1. Connect the device to the network cable for computer.
2. Edit the IP address of the computer and the IP address of the device in the same network segment.



Device IP address: G1 (external network network interface) is 192.168.1.64; G2 (internal network network interface) is 192.10.64. When using external network, the IP address of the computer can be set as any IP address between 192.168.1.2 and 192.168.1.254 (except 192.168.1.64). For example, set the IP address of the computer to 192.168.1.100.

---

3. Enter device IP address in browser to display activation interface.
4. Set device activation password.



- In order to protect your privacy and corporate data and avoid network security problems of device products, it is recommended to set strong password that meets security requirements.
  - The password should contain 8 to 16 characters, including at least 2 of the following types: digits, lowercase letters, uppercase letters, and special characters.
- 

5. Click **OK** to activate the device.

### 3.3 Access Device

Provide access method through web page and Hik-Connect.

#### 3.3.1 Access Device via Web Client

##### Login System

Log in to the device's web page, and configure and operate the device through the web page.

Power on the device and connect to the network. Enter the device IP address in the browser address field to log in.



After logging in, if the installation browser plug-in screen pops up, it is allowed to install.

---

##### Get Help

Quick access to the device through online help.

Click  to open the online help document and view the operating instructions.

##### Exit System

If the device is set or operated, you need to exit the device system safely.

Click  to exit the device system.

#### 3.3.2 Access Device via EZVIZ Cloud

Devices connected to Hik-Connect can receive abnormal information of the site of interest and take security measures in time.



The operation is applicable to gateway only, and not to wireless repeater.

---

##### Enable Hik-Connect

Enable Hik-Connect via SADP or web page.

##### Enable Hik-Connect via SADP

Enable Hik-Connect via SADP software.

##### Prerequisite

Get SADP software via official website and install.

##### Steps

1. Open SADP software.

---

## Fire Detection Camera

---

2. Select the device to enable Hik-Connect.

- Select inactive device. Select *Hik-Connect* to use Hik-Connect to set the verification code to enable Hik-Connect.
- Select the activated device, select *Use Hik-Connect*, set verification code, enter device password, and click *Edit* to enable Hik-Connect.

### Enable Hik-Connect via Web Client

You can enable and set Hik-Connect to access Hik-Connect.

#### Steps

1. On the device web page, go to *Configuration* → *Network* → *Advanced Configuration* → *Platform Access*.
2. The platform access mode is *Hik-Connect*.
3. Select *Enable*.
4. Set Hik-Connect access parameters.

#### Access Server IP Address

By default, the device will automatically assign a server address to the server in the nearest area.

**Custom** means you can set domain name server address manually.

#### Verification Code

For device access security, please customize a verification code or edit the original verification code to add the device to Hik-Connect account.



#### Note

The verification code should contain 6 to 12 characters, including letters and digits, and it is case sensitive. For device security, it is recommended to set a combination of uppercase letters and digits with 8 digits or more.

---

5. Click *Save*.

The registration status is online, meaning the device is registered to Hik-Connect platform.

### 3.3.3 Add Device to Hik-Connect Video Mobile Client

Hik-Connect video mobile client can connect device to Hik-Connect and access device via mobile client.

#### Prerequisite

The device is connected to the router via wired network. Please make sure the router is connected to the WAN normally.

#### Steps

1. Scan Hik-Connect video mobile client and download, install, and register client software.



#### Note

Downloading will consume data. It is recommended to operate in Wi-Fi.

---

## Fire Detection Camera

---



Figure 3-1 EZVIZ Cloud Video QR Code

---



Note

Hik-Connect video QR code supports cell phone scanning and downloading in Android system or iOS system.

---

2. Click + in the upper-left corner of the client software to add the device.
    - Scan the QR code on the device body to add the device.
    - Click in the upper-right corner of the software  to enter the serial No. on the device label to add the device.
  3. Select *non-Hik-Connect device* and connect the device to Hik-Connect according to the prompt.
- 



Note

Adding and configuring should be completed within 3 minutes after the camera is powered on. Otherwise, restart the device and try again.

---

4. Click *Live View*, click Channel, and access device.

# Chapter 4 Web Client Configuration and Operation

## 4.1 Live View



Note

The functions that may be included in the live view page are described below.

### Live View Interface Function

- In the live view page, you can control functions such as live view, recording, picture capture, and audio suppression.
- Select the display mode according to the user's actual needs.
- Select stream of live view.
- When the browser cannot live view normally, you can select different playing plug-in according to the browser to install and preview. The control is related to specific browser. When you use IE core browser, you can select plug-in as Webcomponents and QuickTime. When you use non-IE core browser, you can select plug-in as Webcomponents.

### Live View Screen Icon Function Description

Table 4-1 Icon Function Description

Icon	Function Description
	Select the picture size during live view. 4:3; 16:9; original scale and adaptive display, respectively.
	Select stream type during live view. Main stream and sub-stream, respectively.
	Play plug-in switch selection.
	Two-way audio on button/two-way audio on
	Live view is enabled and disabled.
<i>Clear Sound</i>	Disable the alarm signal of the device.
	Capture picture during live view.
	Local recording is enabled and disabled during live view.
	Enable and disable digital zoom. Drag the left mouse button to zoom in.
	Adjust live view volume.

### 4.2 Video Playback

View video file to perform video playback.

#### Prerequisite

Video file exists. See **Recording Schedule** for recording schedule configuration.

#### Steps

1. Click *Playback* on the device page to enter the video playback page.
2. Select recording date and click *Search*.
3. Select the time point to playback. Drag the time bar below to select playback time.



By default, the system starts playing from the start time of the recording file.

---

4. Click  to start recording playback.
5. Optional: The following actions are allowed during video playback.
  - Set the return visit time point in the Playback Time Point Positioning window, and click  to move the video to the set time.
  - Quick release, slow down, single frame, capture, clipping, zooming in, mute, full screen, etc., are enabled by the function buttons in the video.
6. Optional: Click  to download the recording file to local.

### 4.3 View Picture

Search, view, and download picture files stored on the device.

---



To view the picture file of the event alarm, set the linkage mode in the *event* first. Detailed method: Enter *configuration* → *event*, and then enter corresponding event configuration interface (such as alarm input). Click *Linkage Configuration* and select *Upload FTP*.

---

#### Steps

1. Click *Picture* to enter the picture search page.
2. Set the search condition on the left side of the window, select the file type and start/end time, and click *Search* to list the eligible pictures in the list on the right.
3. Select the line to download locally. Click *Download* to download.



Click *Stop Downloading* to end the download.

---

#### Result Description

The downloaded picture will be stored in the settings of *Parameter* → *Local Settings*.

### 4.4 Parameter Configuration

#### 4.4.1 System Parameters

##### System Settings

---



The system settings are dependent on the actual device. The system settings that the device may support are described below.

---

##### View Basic Information

Basic information includes device model, serial No., version information, channel number, HDD number, and alarm input/output number.

Enter *Configuration* → *System* → *System Settings* → *Basic Information* to edit device name and device No.

##### Set Device Time

Configure device time. Two time sync modes are supported: NTP time sync and manual time sync.

Go to *Configuration* → *System* → *System Settings* → *Time Configuration*.

Select the time zone, and then select time sync mode.

##### NTP Time Sync

Configure NTP server address, server port, and time sync interval.

---



Click *Test* to test if the NTP server is correct.

---

After setting, the device will sync from NTP server periodically according to time sync interval.

##### Manual Time Sync

You can set device time directly or sync with computer time.

##### Set DST

If DST is applied in the area, you can set DST to synchronize the device with local time.

##### Steps

1. Go to *Configuration* → *System* → *System Settings* → *DST*.
2. Select *Enable DST*.
3. Select **start time**, **end time**, and **DST bias** according to the DST of the device.
4. Click *Save*.

### About Device

Go to *Configuration* → *System* → *System Settings* → *About Device*, click *View* to display open source license information.

### System Maintenance

#### Upgrade and Maintenance

Restart device, restore device parameters, export information, import parameters, and upgrade device.

Go to *Configuration* → *System* → *System Maintenance* → *Upgrade Maintenance*.

#### Restart Device

Click *Restart* to restart the device.

#### Restore Default Value

##### Part Restore

Reset all parameters to default settings except for IP address, network, user name, account, and password.

##### Full Restore

Restore all parameters to default settings.

#### Export Information

##### Device Parameters

It is used to export device parameter file. It is used to configure device with the same parameter.

1. Click *Device Parameters* to pop up the file encryption configuration window.
2. Set encryption password to encrypt the exported device parameter file.
3. Click *OK* to select storage path to export.

#### Import Parameter

##### Device Parameters

Importing device parameter file will make it easier for the user to configure the same parameter.

1. Click *Browse* to select the storage path of the device parameter file, and click *Open*.
2. Click *Import*. The prompt will be displayed.
3. Click *OK* to enter the encryption password, and import the device parameter file.

#### Upgrade

##### Upgrade File

When the device needs to be upgraded, you can copy the upgrade program to the local computer, click *Browse* to select the path of saving the upgrade file, and click *Upgrade* to start upgrading.

---

## Fire Detection Camera

---



Upgrading will take about 1 to 10 minutes. Please do not turn off power during the process. Device will restart automatically after upgrading.

---

### Search Log

Log interface can search, display, and export log information that is saved in device storage.

#### Steps

1. Go to *Configuration* → *System* → *System Maintenance* → *Log*.
2. Select log type, set log search date and start/end time, and click *Search*.

The results will be displayed in log list.

---



Only the first 2,000 logs within the search time range are shown in a single search.

---

3. Optional: Click *Export* to save log information to local computer.
- 



The log saving formats are Text (.TXT) files and CSV files.

---

### Search Security Audit Log

It is used to search and manage device security logs.

#### Steps

1. On the device web page, go to *Configuration* → *System* → *System Maintenance* → *Security Audit Log*.
2. Set log major type, minor type, start time, and end time.
3. Click *Search*.

The log list shows all the logs that meet the search condition.

4. Optional: Click *Export* to save the log to the computer.

### Security Management

#### Set Authentication Mode

Set RTSP authentication.

The authentication mode can be set as digest or digest/basic. The information carried varies depending on the

---

## Fire Detection Camera

---

authentication mode. Please refer to the protocol for details.

---



Basic authentication information is relatively simple. If the requirement is high for network security, it is recommended to use digest.

---

### Set IP Address Filter

Used to set access permission of computer or terminal.

---



IP address refers to IPv4 address.

---

#### Steps

1. Enter *Configuration* → *System* → *Security Management* → *IP Address Filtering*.
2. Select *Enable IP Address Filtering*.
3. Set *IP Address Filtering Type*.

**Forbid** Access device is allowed for other IP addresses except those in the list.

**Allow** Only IP address in the list can access the device.

4. Set the IP address to filter.
  - 1) Click *Add* to enter IP address.
  - 2) Optional: Click *Edit* to edit the selected IP address in the list.
  - 3) Optional: Click *Delete* to delete the selected IP address in the list.
5. Click *Save*.

### Set Security Service

Configure SSH and invalid access lock functions.

Enter *Configuration* → *System* → *Security Management* → *Security Service*, enable or disable corresponding security service according to actual situation, and the configuration will take effect after saving.

#### Enable SSH

SSH is a security protocol based on the application layer. After enabling it, it can effectively prevent information leakage in remote management.

Enable *SSH* to provide a secure transmission environment for network service.

---



The function is disabled by default after rebooting.

---

#### Enable Invalid Access Lock

Enable the function. Enter the user name or password at login to the upper limit (seven times, and 5 times after the SSH is enabled). The device will be prompted with lock information and will automatically enter lock status.

---

## Fire Detection Camera

---



For the security of your account, and to prevent unauthorized user login to the device, you are recommended to enable this function. Please set according to the actual situation.

---

### Enable Safe Mode

Select *Enable Safe Mode*, enter administrator password, and enable the function. After enabling the function, the device will use strong password to test. In this mode, some versions of the old NVR will be disabled.

## User Management

### User Management

When you log in to the system using device default user name (admin), you can change admin user password, create and edit other users, and up to 31 users can be created.

### Account Security Settings

Click *Account Security Settings* and set or edit security questions. After setting the security question, click *Forgot Password* in the login page to answer the security question and reset the password.

---



- Please keep the device and computer in the same network segment on the LAN when resetting.
  - The admin is the default user. The user name cannot be edited. Only its password can be edited.
  - When adding, modifying, and deleting admin user, you should enter the admin user password.
- 



- To ensure the security of account information, the password should contain 8 to 16 characters, including at least digits, lowercase letters, uppercase letters, and special characters (! " # \$ % & ' ( ) \* + , - . / : ; < = > ? @ [ \ ] ^ \_ ` { | } ~ space) and cannot contain user name.
  - Password length should be less than 8 characters. Password should contain only one type of character, the same as user name, or the reverse of user name. The above types of passwords are risky. To better protect your privacy and improve product security, it is recommended to change the risky password to high-intensity.
- 

### Add User/Edit User/Delete User

- Click *Add* to add new user. You can set user type, password, and permission. It is divided into strong, medium, and weak according to the complexity of password settings.
  - Select existing user. Click *Edit* to edit user information.
  - Select a user and click *Delete* to delete the user information.
-

### View Online User

It is used to display the list of users logged into the device in the network.

Go to *Configuration* → *System* → *User Management* → *Online User* to view all user information logged in to the device, including user name, user type, IP address, and user operation time. Click *Refresh* to refresh current user information.



- If the IP address and user name are the same, only one user login information will be shown.
  - Up to 30 user logins can be displayed in the online user interface.
- 

## 4.4.2 Network Parameters

### Set TCP/IP Address

TCP/IP is the most basic transmission control protocol of the Internet. TCP/IP configuration is required for network.

Go to *Configuration* → *Network* → *Basic Configuration* → *TCP/IP Address*, set network parameters, and click *Save* to take effect.



The TCP/IP parameters that the device may support are described below. The specific parameters supported by the device are subject to the actual device interface.

---

#### NIC Type

Select according to network environment.

#### IPv4 Address

- Select *Auto Obtain*. The device will automatically get network parameters according to the network environment.
  - Uncheck to get auto information. Manually enter device IPv4 address, IPv4 subnet mask, IPv4 default gateway, and other LAN parameters.
- 



When manually entering IPv4 network parameters, click *Test* to check if the IP address is available, and click *Save*.

---

#### MTU

The max. transmission unit refers to the size of the max. data packet in TCP/UDP protocol network transmission.

#### DNS Server Configuration

The domain name can be parsed when the device has set the correct available DNS server address.

---

## Fire Detection Camera

---

### Configure Port Parameters

You can edit the device port when network access is not available due to port conflict.

---



Do not modify default port parameters at will, otherwise the device will be inaccessible.

---

Enter *Configuration* → *Network* → *Basic Configuration* → *Port*, set port parameters, and save to take effect.

#### HTTP Port

The port of the browser accessing device. For example, when **HTTP port** is changed to 81, you need to enter <http://192.168.1.64:81> to access it when you log in via browser.

#### RTSP Port

The port of the real-time transmission protocol of the device.

#### HTTPS Port

It refers to the port accessed by the browser certificate. When the browser accesses the device, it needs to be verified by certificate, and the security level is high.

#### Server Port

When using the client to log in to the camera, you need to enter the port No. in the login page to log in to the camera normally.

### Set Platform Access Mode

The *Platform Access Mode* enables device registration and access via Hik-Connect.

#### Hik-Connect

Hik-Connect is Hikvision's micro-video service platform that enables access to Hik-Connect devices.

#### Steps

1. Go to *Configuration* → *Network* → *Advanced Configuration* → *Platform Access*.
2. Select *Hik-Connect*.
3. Select *Enable*.
4. Select custom or default *access server IP* address.
  - Custom: Set domain name server IP address manually.
  - Default: The device will automatically assign a server IP address to the nearest area.
5. Click *Save*.



- Refresh the page or restart the device to check *the registration status*. Check if the device is registered.
  - If you log in via administrator, you can view the device's Hik-Connect verification code. If you log in via non-admin user, you cannot view the code.
-

### Set HTTPS

In network access, to improve the security of browser access, you can build secure and encrypted network transmission via HTTPS protocol, and ensure the security of data transmission through identity authentication and encryption communication.

#### Steps

1. Go to *Configuration* → *Network* → *Advanced Configuration* → *HTTPS*.
2. Select *Enable* to access the device via HTTPS protocol.
3. View certificate details.

#### Delete Certificate

You can view the installed certificate and the attributes. Click *Delete* to delete the current certificate.

4. Click *Save*.



- HTTPS port validity range: 1 to 65535. When remote access is via HTTPS, enter `https://IP address` in the browser address bar. If HTTPS sets port other than 443, enter `https://IP address+:(spoof)+port No.`, e.g., `https://192.168.1.64:81.IP address`
  - The user can also apply for *certificate creation*, upload certificate issued by authoritative certificate (CA) for authentication (fee is required for CA organization), and improve the security level of access.
- 

### Configure Open Network Video Interface

When device connection is required through open network video interface protocol, the corresponding user can be configured as needed to enhance device network security.

#### Steps

1. Go to *Configuration* → *Network* → *Advanced Configuration* → *Integration Protocol*.
2. Select *Enable Open Network Video Interface*.
3. Click *Save*.
4. Click *Save*.

### Set HTTP Listening

The device sends alarm information to the IP address or domain name via HTTP protocol. The IP address or domain name should support HTTP protocol transmission.

#### Steps

1. Go to *Configuration* → *Network* → *Advanced Configuration* → *HTTP Listening*.
2. Enter IP address or domain name, URL address, and port to select protocol type.
3. Click *Test*.



Click *Reset* to reset the IP address or domain name.

---

4. Click *Save*.

### 4.4.3 Video and Audio Parameters

---



The content in the audio parameter settings will be determined according to the actual device. The following description refers to the audio settings that the device may support.

---

#### Video Configuration

You can set video parameters according to the quality requirements of the live view image.

Go to *Configuration* → *Video and Audio* → *Video* and configure video parameters.

---



The video parameters of the device are described below. The settings supported by the device are subject to the actual interface of the device.

---

#### Stream Type

##### Main Stream (Scheduled)

Main stream is used for HD storage and live view, resolution, bitrate, and image quality.

##### Sub-Stream

Sub-stream is used for standardizing storage and live view, resolution, bitrate, and image quality when network bandwidth is insufficient.

#### Video Type

##### Video Stream

Video stream only.

##### Video and Audio Stream

Including video stream and audio stream.

#### Resolution

Select according to customer requirements for video clarity. Higher resolution and higher bandwidth requirements.

#### Bit Rate Type and Max. Bit Rate

##### Constant Bit Rate

It means that the bit rate is maintained at the average bit rate for transmission. The compression speed is fast, but video mosaic may occur.

##### Variable Bit Rate

It means adjusting the bit rate on the max. bit rate. The compression speed is relatively slow, but it can ensure the image definition of complex scene.

#### Image Quality

When the bit rate is variable bit rate, you can set the image quality. Select according to customer

---

## Fire Detection Camera

---

requirements for image definition. The higher the image quality, the higher the bandwidth requirement.

### Video Frame Rate

It refers to the number of frames per second of video. The higher the video frame rate, the higher the required bandwidth, and the higher the required storage space.

### Video Encoding

#### H.264

H.264 is a video encoding/decoding technology. It provides high compression, flexible handling, and ultra-low bit rate, saving network transmission bandwidth and storage space.



When the video encoding parameter of sub-stream is set as *MJPEG*, if the live view is stuttered, H.264 encoding format is recommended to ensure smooth picture.

---

#### H.265

H.265 is a video encoding/decoding technology, with high compression, flexible handling, and ultra-low bitrate. Compression performance is twice as high as H.264, saving bandwidth and storage space.

### Profile

Select the profile as *Medium*.

### I Frame Interval

The number of frames between the two key frames. The larger the I frame interval, the smaller the stream fluctuations, but the lower the image quality, the higher the stream fluctuations, and the higher the image quality.

### SVC

It is a scalable video encoding technology that can be used for encoding storage when bandwidth is insufficient. This function should be used with the back-end storage device. The H.264/H.265 encoding device can be configured.

### Stream Smoothing

Drag the progress bar or set stream smoothing value. The higher the value, the better smoothing degree, but the image will be relatively unclear. Otherwise, the smoothness of the image will be poor, and the image is relatively clear.

### Intelligent Information Display Mode

#### Playing Library

Intelligent rule information will be displayed in the special player only when the video is played by the special player of the manufacturer.

#### Video

Intelligent rule information will be displayed in other players when other players are supported to play video.

---

## Fire Detection Camera

---

### Audio Configuration

Go to *Configuration* → *Video and Audio* → *Audio* and configure audio parameters.

#### Audio Encoding

Select audio encoding type according to actual usage requirements, including G.711ulaw, G.711alaw, and ACC. When the encoding type is AAC, set the sampling rate and audio bit rate parameters. Select the sampling rate and audio bit rate parameters from the drop-down list.

#### Audio Input

Select the audio input as *MicIn*.

#### Input Volume

The gain control value of the audio input source. The user can adjust the value from 1 to 100.

### Configure ROI

ROI is the encoding of areas of interest. Enabling ROI will improve the image encoding quality of selected areas, and reduce the encoding quality of selected areas.

#### Prerequisite

ROI is supported when video encoding is set to H.264 or H.265. Check video encoding type.



Note

ROI settings are effective when the bit rate is changed or the bit rate is lower.

---

#### Steps

1. Go to *Configuration* → *Video and Audio* → *ROI*.
2. Select **Stream Type**.
3. Optional: Configure fixed area to be upgraded.
  - 1) Check *Enable*.
  - 2) Select area No. in the fixed area to draw the area of interest.
  - 3) Click to *draw area*, select a fixed area on the live screen with the mouse, and click to *stop drawing*.



Note

Select the fixed area to adjust. Drag the mouse to adjust the position of the fixed area.

---

- 4) Set ROI level and area name.



Note

The higher the level, the clearer the detection area image.

---

- 5) Optional operation: Repeat child steps 2 to 4, and draw multiple areas.
4. Click *Save*.

### 4.4.4 Image Parameters

#### Set Display Parameters

Enter *Configuration* → *Image* → *Display Settings* to set the image quality of the main live view. Click *Restore Default* to restore the default settings.



The display parameter settings that the device may support are described below. The display parameters that the device can configure are subject to the actual interface.

---

#### Image Adjustment

Adjust the brightness, contrast, saturation, and sharpness of the live view by dragging the progress bar. You can also set the value after the progress bar.

#### Exposure

##### Iris Type

Manual by default.

##### Exposure Time

The camera's electronic shutter time, and the longer the exposure time, the better the image display. Different exposure times can be set according to different device scenes. If manual optical circle camera mode is used, the time set here is the longest exposure time.

#### Day/Night Switch

##### Day/Night Switch

###### Auto

The device will automatically switch between daytime and nighttime according to the brightness of the environment.

###### Daytime

When in daytime mode, the device image is forced to be in daytime, without supplement light, and not switched to daytime or night according to actual scene.

###### Night

When in night mode, turn on the supplement light and set the parameters of supplement. Device image is forced to night, and will not be switched to day or night according to actual scene.

##### Scheduled Switch

In scheduled switch mode, the start time and end time of day are set. During this time period, the device will use day mode automatically. During this time period, the device will use night mode automatically.

---

## Fire Detection Camera

---



Start time and end time can be set to the next day when you select *scheduled switch*. Please use the device.

---

### Sensitivity

When day or night mode is selected as *Auto*, 0 to 7 can be adjusted, corresponding to night to day threshold. The lower the sensitivity settings, the higher the device brightness will be required to move from night mode to day mode. The higher the sensitivity settings, the lower the device brightness requirements will be.

### Filtering Time

When the conversion mode is *auto*, the filter time of day and night can be adjusted from 5 to 120 seconds. Day and night will be switched when the environment illumination meets the requirements and the retention time exceeds the set threshold time.

### Smart Supplement Light

Select On or Off according to the actual environment.

### Supplement Light Mode

When the device supports supplementing light, you can select supplement mode.

#### Event Intelligence

The device will supplement light with mobile detection. When the mobile detection alarm occurs during intelligent supplement, the light will be bright in night mode and the filter will be switched to daytime.

#### IR Supplementation

The device will enable IR supplement mode.

#### White Light Supplementation

The device will enable white light supplement mode.

#### Off

Disable supplement light.

### Brightness Adjustment Mode

Set the brightness mode and brightness when supplementing light.

#### Auto

Adjust the brightness automatically according to the brightness of the current channel. When the image reaches a certain darkness, the supplement light will be automatically enabled. When the brightness reaches a certain brightness, the supplement light will be automatically disabled.

#### Manual

The brightness of the supplement light can be adjusted by dragging progress bar or setting value.

### Backlight

#### Backlight Compensation (BLC)

The user can select compensation area according to the actual video scene to avoid the area being too bright or dark. The user can also select custom area.

#### Width Dynamic Range (WDR)

## Fire Detection Camera

---

Wide dynamic is applicable to environments with large differences in light intensity. When high brightness area and areas with relatively low brightness, such as shadow and inverse light under strong light source (such as sunlight, lamps, or reflective light) exist in the picture, you can enable the function of wide dynamic and adjust the level to clear the video picture.

It is used to automatically balance the brightest and darkest parts of the picture, so as to see more details.



Enabling WDR will be mutually exclusive with some functions. Please use the actual device interface.

---

### Highlight Compensation (HLC)

When there is excessive exposure of bright areas and under-occupied areas, the bright areas can be weakened and the dark areas can be highlighted to achieve the light balance of the whole picture.

### White Balance

In different light environments, the color of the object will change according to the projected light color. The color error can be corrected according to the suitable white balance mode in the environment.



- Lock the white balance to lock the current color correction matrix. If the actual scene is of fixed light type, you can select sunlight, incandescent light, hot light, and natural light according to the actual situation.
  - The sunlight is applicable to the color temperature environment of around 6500 K; the incandescent light is applicable to the color temperature environment of around 3000 K; the hotlight is applicable to the color temperature environment of around 4000 K; the natural light is applicable to the color temperature environment of around 5500 K.
- 

### Image Enhancement

#### Digital Noise Reduction

It refers to using advanced 3D image noise reduction technology to reduce the noise of the image and make the image softer and finer.

#### Normal Mode

The noise reduction level is controlled by setting the noise reduction level.

#### Expert Mode

It can be adjusted by two dimensions: airfield noise reduction level and timedomain noise reduction level.

#### Noise Reduction Level

0 to 100 adjustable.

#### Gray Scale

Select the gray range of video encoding according to actual needs.

### Video Adjustment

Optimize image display by setting video adjustment parameters.

#### Mirror

You can adjust video by mirror image as needed, select center, left, right, up, down mirror image, or

## Fire Detection Camera

---

disable mirror image. When the image is inverted, you can flip the image through the menu.

---



- Using mirroring function will cause incorrect positioning of fire points.
  - After enabling mirroring mode, the platform video will be interrupted for a short time.
- 

### Video Standard

It refers to video signal format, and the highest frame rate of different formats (e.g., the highest frame rate of 50 Hz is 25 fps, and the highest frame rate of 60 Hz is 30 fps).

## Set OSD Parameters

OSD refers to the information displayed on the video, and the device name, date, week, and superimposed character can be displayed on the video.

Enter *Configuration* → *Image* → *OSD Settings*, select display item, set channel name, set corresponding parameters, and save to take effect.

### Basic OSD Information Settings

- Select the OSD information to display: Select *the display name, date, and week*, and the corresponding OSD information will be displayed on the live view.
- Enable temperature data overlay: When enabled, the function will overlay the real-time temperature wave chart.
- Edit OSD information display location: Drag the OSD red box on the live view to move to the location you want to display.
- Edited display format: In the channel name/time format/date format, you can edit the channel name displayed on the live view and the time and date format.

### OSD Attribute Settings

Set OSD information properties, font size, color, and alignment method displayed on live view.

## Overlay Custom Characters

Multiple characters can be added to the video. Select and set the characters to be added. The characters in the video will display in red font. You can drag the characters or set the alignment mode to adjust the characters to the position to be displayed. Click *Save* to finish.

---



Some characters are default fire alarm characters, and cannot be edited.

---

## Set Target Mask

Target Mask refers to covering sensitive areas in the video picture, and is not displayed in the image.

### Steps

1. On the device web page, go to *Configuration* → *Image* → *Target Mask*.
-

## Fire Detection Camera

---

2. Select *Enable Target Mask*.
3. Click *Draw Area*, click the left mouse button in the picture, drag the mouse, and release the left mouse button to draw an area.



Up to 4 areas can be drawn in the picture.

---

4. When the area is drawn, click *Stop Drawing* to finish the area drawing.
5. Optional: Click *Clear All* to clear all areas.
6. Click *Save*.

### 4.4.5 Event Parameters

Describe the function configuration of each event supported by the device, and configure the corresponding event according to needs, and trigger device linkage.



The event functions that the device may support are described below. Please refer to the functions supported by the actual device.

---

### Schedule and Linkage Configuration

The device receives alarm information during the scheduled time period. The device is linked to execute corresponding actions.

#### Set Arming Time

Set start time and end time of task execution.

##### Steps

1. Click *Arming Time*.
2. Select a point in the timeline as start point. Hold the left mouse button to drag in the timeline, and release the mouse when dragging to the end point to set the arming time.



8 time periods are supported in one time axis.

---

3. Adjust arming time.
  - Click *Arming Time Period* to enter start time and end time manually to adjust arming time. Click *Save*.
  - Click *Arming Time Period* to display two circles on both ends of the time period. Move the mouse to both ends of the time period, and display the adjustment arrow in the left and right directions. Move the adjustment arrow to adjust the time period.
  - Drag the arming time period to any position on the axis to reset the time period.

**Click to *Delete Time Period*** Delete current time period.

**Click to *Delete*** Delete the selected time period.

## Fire Detection Camera

---

<b>Click to <i>Delete All</i></b>	Delete all time periods.
<b>Click to <i>Copy To...</i></b>	Copy the same schedule to other time.

4. Click *Save*.

### Linkage Configuration

You can enable alarm linkage when there is an event or alarm.

The linkage mode that the device may support is described below. Please configure the linkage mode according to available options on the actual device interface.

### Normal Linkage

#### Notify Surveillance Center

Select and configure surveillance center linkage. When an alarm is triggered, the device sends alarm notifications to the connected surveillance center

#### Upload to Memory Card

Select *Upload to Memory Card* to upload alarm information and pictures to memory card when alarm occurs.

#### Auto Linkage

When the event is triggered, the device will automatically execute the linked actions.



#### Note

The media to be saved is supported by the device. The corresponding configuration path is as follows:

- NAS: *Configuration* → *Storage* → *Storage Management* → *Network HDD*.
  - SD card configuration: *Configuration* → *Storage* → *Storage Management* → *HDD Management*.
- 

### Linkage Alarm Output

A->No.

Select the alarm output channel. If the corresponding alarm output interface of the device is connected to the alarm output device, the alarm output device will output the signal when the alarm is triggered.

### Recording Linkage

Select and configure recording schedule. When alarm is triggered, the channel can be linked to record.

See Recording Schedule for recording schedule configuration. [d112e6a1310](#)

### Configure Basic Event

Describe the basic event configuration of the device.



The event types that the device may support are described below. The actual event types will be determined according to the actual interface.

---

### Configure Motion Detection

The function is used to detect whether an area has moved objects during a certain time period. When there is a moving object, the device will be triggered to execute linkage actions.

#### Steps

1. Enter *Configuration* → *Event* → *Basic Event* → *Motion Detection*.
2. Select *Enable Motion Detection*.
3. Optional: Set the moving object in the picture to green to highlight.  
Select *Enable Dynamic Analysis*.
4. Set arming time and linkage mode. See *Schedule and Linkage Configuration*.
5. Set whether human body is selected for **detection**. When enabling intelligent light supplement, the detection target should be enabled.
6. Set **sensitivity**.
7. Click *Save*.

### Configure Video Tampering Alarm

When the blocked area in the pre-defined video is blocked, the area cannot be viewed normally, and the device will be linked.

#### Steps

1. Enter *configuration* → *Event* → *Basic Event* → *Video Tampering Alarm*.
2. Select *Enable*.
3. The **sensitivity** is set. The higher the sensitivity value, the more sensitive the detection.
4. Set arming time and linkage mode. See ***Schedule and Linkage Configuration***.
5. Click *Save*.

### Configure Alarm Input

The device's alarm input interface is external to the device. When the device generates alarm signal, the device will be triggered to execute linkage actions.

#### Prerequisite

The device's alarm input interface is external to the device.

#### Steps

1. Go to *Configuration* → *Event* → *Basic Event* → *Alarm Input*.

## Fire Detection Camera

---

2. Select alarm input No. and alarm type to customize alarm name.



Set alarm type according to the connected alarm device.

---

3. Optional operation: Select *Enable Alarm Input Handling*. After selecting, event configuration alarm linkage will take effect.
4. Set arming time and linkage mode. See ***Schedule and Linkage Configuration***.
5. Optional: Click *Copy* to copy the alarm input settings to other alarm input channels.



The function is not supported when the device has only one alarm input channel.

---

6. Click *Save*.

### Configure Alarm Output

The device's alarm output interface is external to the device's alarm output. When the device generates alarm signal, the device triggers alarm output.

#### Prerequisite

The device's alarm output interface is external to the device's alarm output.

#### Steps

1. Enter *Configuration* → *Event* → *Basic Event* → *Alarm Output*.
2. Select **alarm output No.** to set its delay time and alarm name.



The delay time is subject to the actual situation. Set the duration between 5 seconds and 10 minutes, or set the duration as *manual*.

---

3. Set arming time. See ***Schedule and Linkage Configuration***.
4. Optional: Click *Copy* to copy the alarm output settings to other alarm output channels.



The function is not supported when the device only has one alarm output channel.

---

5. Optional: Click *Manual Alarm* to control the alarm output device on the alarm output interface of the device.
6. Click *Save*.

### Configure Exception Alarm

When the device is abnormal (such as network disconnection), the configured linkage action can be triggered.

#### Steps

1. Enter *Configuration* → *Event* → *Basic Event* → *Exception*
2. Select exception alarm type.
3. Set linkage mode. See ***Schedule and Linkage Configuration*** for linkage mode settings.
4. Click *Save* to finish the alarm configuration.

### Configure Temperature Measurement

Temperature measurement function is used to detect temperature. When the device detects the temperature exceeded threshold, the device will be triggered to execute linkage action.

#### Steps

1. Go to *Configuration* → *Event* → *Basic Event* → *Temperature Measurement*.
2. Select *Enable*.
3. Set temperature alarm threshold. Adjustable range: 0–120.  
The device will be triggered to execute linkage actions when the detected temperature exceeds the set threshold.
4. Set temperature alarm time threshold. Adjustable range: 1–30.
5. Select differential temperature detection type.
6. Set the alarm threshold of temperature surge. Adjustable range: 1–120.
7. Set the alarm time threshold of temperature surge. Adjustable range: 1–30.
8. Set arming time and linkage mode. See ***Schedule and Linkage Configuration***.
9. Click *Save*.

### Configure Indicator Control

Used to set indicator status and flickering frequency.

#### Steps

1. Go to *Configuration* → *Event* → *Basic Event* → *Indicator Control*.
2. Set *the operation indicator (green light)*.
3. Set *fault indicator (yellow light)*.
4. Set *alarm indicator*.
5. Set the *flashing frequency*, and set the range of 1 to 5.
6. Click *Save*.

### Configure Smart Event

Select and configure Smart Event for specific scene. When there is target triggering rule, the device will execute linkage action.



Note

The event types that the device may support are described below. The actual event types will be determined according to the actual interface.

---

### Configure On/Off Duty Detection

The check-out detection is used to identify whether the person on duty in the control room is on duty. When the number of persons in the recognition area is less than the alarm threshold, or the duration of the check time is longer than the set detection time, the device will be triggered to execute the linked actions.

#### Steps

1. Go to *Configuration* → *Event* → *Smart Event* → *On/Off Duty Detection* on the device web page.
2. Select *Enable Off-duty Detection*.
3. Set detection area and shielded area.
  - 1) Click to *draw detection area/screen area*.
  - 2) Click the left mouse button in the picture to draw any convex quadrilateral shape.

## Fire Detection Camera

---

3) Optional: Repeat child steps 1 to 2, and draw up to 4 detection areas/shielded areas.

4) Optional: Edit drawn area.

- Move the mouse to the area internal. Drag to change the area position.
- Move mouse to area vertex. Click Drag to edit vertex position.
- Click *Clear All* to delete all drawn areas.

The device will intelligently detect and analyze events in the detection area, and ignore the detection results in the shielded area.

4. Set detection parameters.

---



When the number of people in the recognition area is less than the set alarm threshold, or the duration exceeds the set detection time, the alarm will be triggered. The higher the sensitivity, the higher the alarm will be more likely to trigger, and the error recognition rate will increase.

---

5. Set arming time and linkage mode. See ***Schedule and Linkage Configuration***.

6. Click *Save*.

### 4.4.6 Storage Parameters

#### Recording Schedule

Schedule recording is used to automatically execute recording tasks within a set time period.

##### Steps

1. Go to *Configuration* → *Storage* → *Schedule Configuration* → *Recording Schedule*.
  2. Select *Enable* to enable recording schedule.
  3. Select recording type.
- 



The video types of the device are described below. The selected video types will be subject to the actual interface of the device.

---

##### Scheduled

It means recording according to the time configured by the scheduled recording.

##### Motion Detection

Channel recording occurs when motion detection event occurs.

##### Alarm

It means that the alarm input will generate alarm or record the alarm event.

4. Click *Advanced Parameters* to configure the parameters.

##### Overwrite

If you select *Overwrite*, the earliest recording file will be overwritten when the storage space is full. If not, the recording will be stopped when the storage space is full.

##### Pre-Record Time

Pre-recording time before start time node of recording schedule.

---

## Fire Detection Camera

---

### Post-Record

Delay recording time after recording schedule end time node.

### Stream Type

Stream type of video storage.

---



#### Note

The higher the bit rate, the lower the pre-record time.

---

5. Set recording schedule time. See ***Schedule and Linkage Configuration***.

6. Click *Save*.

## Storage Management

The storage space for managing video files and pictures.

---



#### Note

The content in storage management is dependent on the actual device. The following description refers to the storage management that the device may support.

---

## HDD Management

View HDD information and HDD quota.

### Steps

1. Go to *Configuration* → *Storage* → *Storage Management* → *HDD Management*.
2. View disk No., capacity, remaining space, status, type, attribute, and progress.
3. View disk quota, including picture capacity, free size for picture, recording capacity, and free size for record.
4. Set capture picture quota percentage and record quota percentage.
5. Click *Save* to reboot the device.

## Format SD Card

For the first time, please log in to the device web client to format the microSD card.

### Prerequisite

Install the microSD card to the device.

### Steps

1. Go to *Configuration* → *Storage* → *Storage Management* → *HDD Management*.
  2. Select the microSD card to format in the list of HDDs detected.
  3. Set the quota for capture and recording in HDD.
  4. Click *Format*.
- 



#### Note

After formatting, the status of the microSD card is changed from **unformatted** to **normal**. It means that the microSD card can be used normally, and you can check disk capacity and remaining space.

---

## Fire Detection Camera

---

5. Click *Save*.



See Far, Go Further