



Fusion Detection Camera

User Manual

Legal Information

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.
- If the product you choose is a video product, please scan the following QR code to obtain the "Initiatives on the Use of Video Products", and read it carefully.



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 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.

Foreword

The purpose of this instruction manual is to ensure that users will use this product safely and correctly, without causing property damage. Before using this product, please carefully read the product instruction manual and retain the manual for future reference.

Data Acquisition

Visit our official website (www.hikvision.com) to obtain manuals, application tools, and development materials.

Scan the product QR code with WeChat to get the user manual, application tools, and online services.

Introduction

This manual applies to thermal imaging heat detectors and describes the installation steps, installation precautions, and functional operations of visual thermal imaging heat detectors.

Symbol Conventions

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

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

Precautions for Safe Usage

Danger

- Regional and national electrical full regulations must be strictly adhered to during the installation and operation of this product.
- Please use the power adapter provided by a regular manufacturer. For specific requirements of the power adapter, please refer to the product parameter table.
- To reduce the risk of fire or electric shock, do not expose the product to rain or moisture.
- When installing the device on a wall or on the ceiling, please ensure that the product is firmly secured.

- If the product isn't working properly, please contact the nearest service center or product dealer.
- Do not disassemble or modify the product in any way. (The company will not assume responsibility for any issues that arise due to unauthorized modification or repair.)



Caution

- The product functions can be normally achieved only when the product is correctly installed and effectively maintained. This product is designed to assist you in disaster prevention, but it cannot replace on-site inspection by you, nor can it prevent the occurrence or expansion of accidents. In daily use, you should still remain vigilant, strengthen safety awareness, and carefully pay attention to your personal and property safety.
- Do not drop objects onto the product or shake the product vigorously. Keep the product away from locations with magnetic interference. Avoid installing the product in a place where the surface vibrates or where the product is vulnerable to impact. Otherwise, the product may be damaged.
- This is a Class A product. In a residential environment, this product may cause radio interference. In such cases, the user may be required to take practical measures against the interference.
- The serial port on the device is only used for debugging and is not intended for users.
- Please do not use the product in environments with high temperatures, low temperatures, or high humidity. For specific temperature and humidity requirements, please refer to the product's parameter table.
- Do not aim the product's lens at strong light sources, such as the sun, incandescent lamp, or other high-temperature targets, as this may damage the lens or thermal imaging detector.
- Do not expose the device to dripping or splashing, nor place items such as vases containing liquid on the top.
- Do not place the device in an environment with corrosive gases, as corrosive gases can damage the device.
- Do not place an exposed flame source, for example, a lit candle, on the device.
- Avoid placing the product in direct sunlight, poorly ventilated locations, or near heat sources such as heaters or heating sources (Neglecting this may lead to a fire hazard).
- When cleaning the device lens or cover, use a sufficiently soft dry cloth or other substitute to wipe the inner and outer surfaces. Do not use alkaline cleaners. Avoid scratching the lens or cover with hard objects.
- Network security issues may arise when the device is connected to the Internet. Please enhance your personal information and data security protection. When you discover potential network security risks, please contact us immediately.
- Please understand that you are responsible for the configurations, all passwords, and relevant security issues of the product. You are also responsible for keeping your username and password safe.
- Keep all of the original packaging materials of the device safe, so that it can be used to re-package the device to be sent back to the distributor or manufacturer should any issues arise. The company assumes no responsibility for accidental damage caused by the use of non-original packaging materials during transportation.



Note

- **Qualifications for installation and maintenance personnel**
 - Must possess qualifications or experience in installing and maintaining video preview systems, and have the qualifications for related work (such as working at heights). Additionally, must have the following knowledge and operational skills.
 - Have basic knowledge and installation skills for video preview systems and their components.
 - Basic knowledge and operational skills in low-voltage wiring and low-voltage circuit connections.
 - Basic knowledge and skills in network security, with the ability to understand the contents of this manual.
- **Lifting equipment requirements**
 - Use safe lifting equipment suitable for the installation site and equipment installation method.
 - The lifting equipment should be able to reach the height required for installation.
 - The lifting equipment should be safe to operate.

Button Battery Safety

1. Do not ingest battery. Chemical Burn Hazard!
2. This product contains a coin/button cell battery. If the coin/button cell battery is swallowed, it can cause severe internal burns in just 2 hours and can lead to death.
3. Keep new and used batteries away from children.
4. If the battery compartment does not close securely, stop using the product and keep it away from children.
5. If you think batteries might have been swallowed or placed inside any part of the body, seek immediate medical attention.
6. CAUTION: Risk of explosion if the battery is replaced by an incorrect type.
7. Improper replacement of the battery with an incorrect type may defeat a safeguard (for example, in the case of some lithium battery types).
8. Do not dispose of the battery into fire or a hot oven, or mechanically crush or cut the battery, which may result in an explosion.
9. Do not leave the battery in an extremely high temperature surrounding environment, which may result in an explosion or the leakage of flammable liquid or gas.
10. Do not subject the battery to extremely low air pressure, which may result in an explosion or the leakage of flammable liquid or gas.
11. Dispose of used batteries according to the instructions.

Contents

Chapter 1 Product Introduction	1
1.1 Description	1
1.2 Features	1
1.3 Specification	2
Chapter 2 Wiring and Installation	7
2.1 Product Wiring	7
2.2 Product Installation	7
2.2.1 Pre-installation Description	7
2.2.2 Ceiling Installation	8
2.2.3 Adjusting Sphere Direction	9
2.2.4 Installing Waterproof Tape	10
2.2.5 Installing Network Port Waterproof Sleeve	11
Chapter 3 Operation Instructions	13
3.1 Network Connection	13
3.2 Device Activation and Configuration	13
3.2.1 Activating via SADP Software	13
3.2.2 Activating via Browser	15
3.2.3 Activating via Client Software	16
3.3 Accessing Device	19
3.3.1 Accessing Device via Web Client	19
3.3.2 Accessing Device via EZVIZ Cloud	19
3.3.3 Adding Device to Hik-Connect Video Mobile Client	21
3.4 Main Interface Description	22
Chapter 4 Web Client Configuration and Operation	23
4.1. Preview	23
4.2 Playback	24
4.3 Viewing Pictures	24
4.4 Parameter Configuration	25
4.4.1 Local Configuration	25
4.4.2 System Parameters	26
4.4.3 Network Parameters	31
4.4.4 Video and Audio Parameters	35
4.4.5 Image Parameters	38
4.4.6 Events and Alarms	42
4.4.7 Storage	53
4.4.8 Temperature Measurement	55

Chapter 1 Product Introduction

1.1 Description

It is a flame detector with focal plane array thermometry, which can detect abnormal object temperature and flame in the detection area, and issue early warning and alarms. It supports visual review and networked management. This product features functions such as temperature measurement alarm, identification of fire point locations, and video review for the monitored area, enabling early fire warning and remote visual verification of fire scenes. It is widely applied to hospitals, schools (laboratories, libraries, warehouses, archives), museums, Taoist temples, banks (ATM rooms, equipment rooms), production workshops, substations, oil and petrochemicals (petrol stations) and other organizations with key fire protection and security needs.

1.2 Features

- New fusion smart camera, which can sense the temperature for alarm and can be rechecked via video
- 400W Fixed Focus Intelligent Camera
- Equipped with local alarm indicators
- Support flame detection, coverage: 30 meters (burning object: n-heptane, 0.1 m² fire plate)
- Support high-temperature and temperature-rise exception detection
- Support local alarm indicator light, high-decibel alarm through an internal speaker, and remote muting
- 1 internal speaker, 1 internal microphone, supports bidirectional voice intercom
- OSD alarm event overlay support
- Support access to Hik-Connect
- Support white/IR fill light
- Support PoE power supply
- Support DC12V (1W) external power output, providing power for sensors such as smoke detectors and gas sensors
- Support 2 alarm input/output channels and 1 audio input/output channel
- IP67 dust and water resistant

1.3 Specification

Camera	
Sensor Type	1/3" Progressive Scan CMOS
Max. Resolution	2688×1520
Main Stream	50Hz: 25 fps (2560 × 1440, 1920 × 1080, 1280 × 720) 60Hz: 30 fps (2560 × 1440, 1920 × 1080, 1280 × 720)
Sub Stream	50Hz: 25 fps (704 × 576, 640 × 480, 352 × 288) 60Hz: 30 fps (704 × 480, 640 × 480, 352 × 240)
Min. Illumination	Color : 0.01 Lux @ (F1.6, AGC ON)
Lens	Horizontal: 83°, Vertical: 43°, Diagonal: 100°
Image Settings	Saturation, brightness, contrast, sharpness, AGC and white balance can be adjusted through the client or browser.
WDR	WDR
Shutter	1/25 ~ 1/100,000 s
Image Enhancement	BLC, 3D DNR
Main Stream Video Compression Standard	H.265,H.264
Sub Stream Compression Standard	H.265,H.264
Video Bitrate	256Kbps ~ 8192Kbps
Intelligent Alarm	Intrusion detection, line crossing detection, smoke and flame detection, Fire and Smoke Detection, Indoor Access Blocked Detection, On/Off Duty Detection, Detection of Dangerous Goods in Elevator, Dangerous Behavior Detection, Fire Extinguisher Detection
Protocol	TCP/IP, HTTP, HTTPS, DHCP, DNS, RTP, RTSP, RTCP, NTP, IPv4, UDP
Interface Protocol	ONVIF(PROFILE S, PROFILE G), ISAPI, EZVIZ, ISUP
General	Anti flicker, heartbeat, image, password protection, video occlusion
Storage	Micro SD/SDHC/SDXC card (256 G) disconnection local storage
Exception Detection	Motion Detection, video tampering alarm, network cable disconnection, IP address conflict, invalid access, full memory, memory error
WEB Configuration	Support web preview, configuration and parameter import/export

Fusion Detection Camera User Manual

IR Range	White: 10 m IR: 30m
Accessory Type	Wall mounted support, pendent support, universal joint
Detector	
Image Sensor	Vanadium Oxide (VOx) Microbolometer
Max. Resolution	HF-VT343(1mm):120 × 90 HF-VT343(3mm):256 × 192
Pixel Size	HF-VT343(1mm):17 μm HF-VT343(3mm):12 μm
Response Waveband	8~14 μm
Focal Length of Thermal Imaging Lens	HF-VT343(1mm):1.2 mm HF-VT343(3mm):3.2 mm
Thermal Imaging Field of View	HF-VT343(1mm):90° × 68° HF-VT343(3mm):56.2° × 42.2°
Palette Mode	Support 15 modes including white hot, black hot, fusion 1, rainbow, fusion 2, iron red 1, iron red 2, etc.
Fire and Smoke Detection	Yes
Temperature Exception Detection	Yes
Temperature Measurement Range	HF-VT343(1mm):-20 °C ~ 400 °C HF-VT343(3mm):-20 °C~550 °C
Thermography Precision	HF-VT343(1mm):Max (± 8 °C, ± 8 %) , within the range of 0.5 ~ 1.2 m from the device HF-VT343(3mm):Max (± 8 °C, ± 8 %) , within the range of 0.4 ~ 2.5 m from the device
Noise Equivalent Temperature Difference (NETD)	≤50 mK(@25 °C,F1.0)
Temperature Sensing Mode	Support non-contact temperature sensing
High Temperature Alarm	Yes
Interface	
Alarm Interface	2 way alarm input (Alarm in), 2 way alarm output (Alarm out, support DC 30 V/2 or AC 125 V/0.5 A)

Fusion Detection Camera User Manual

Ethernet Interface	RJ45 10 M/100 M adaptive Ethernet port × 1
Audio Interface	1 way audio input (Line in), 1 way audio output (Line out), 1 way built-in microphone, 1 way built-in speaker
Professional Intelligence (Deep Learning Algorithm)	
Flame Detection	Yes coverage: 30 meters (burning object: n-heptane, 0.1m ² fire plate)
Smoke Detection	Yes
General	
Ingress Protection	IP 67
Mounting Height	Indoor: higher than 2.5 m Outdoor: higher than 3.5 m
Power Interface Type	3pin industrial terminal, spacing: 3.81
Power	DC 9V ~ DC 30V, 24W MAX; PoE: 802.3at; CLASS 4 (The power adapter is not included; you will need to configure it yourself)
Working Temperature	-20~60°C
Working Humidity	<95% RH
Dimension (Φ × H)	Φ 130 × H 101 mm
Alarm Indicator Light	Red/blue: Alarm Green: Normal Yellow: Fault
Product Implementation Standard	Q/HKD 054-2024
Power Consumption	< 10W
Weight	677g (without packaging)

1.4 Product Appearance



Note

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

Sphere Appearance and Indicator

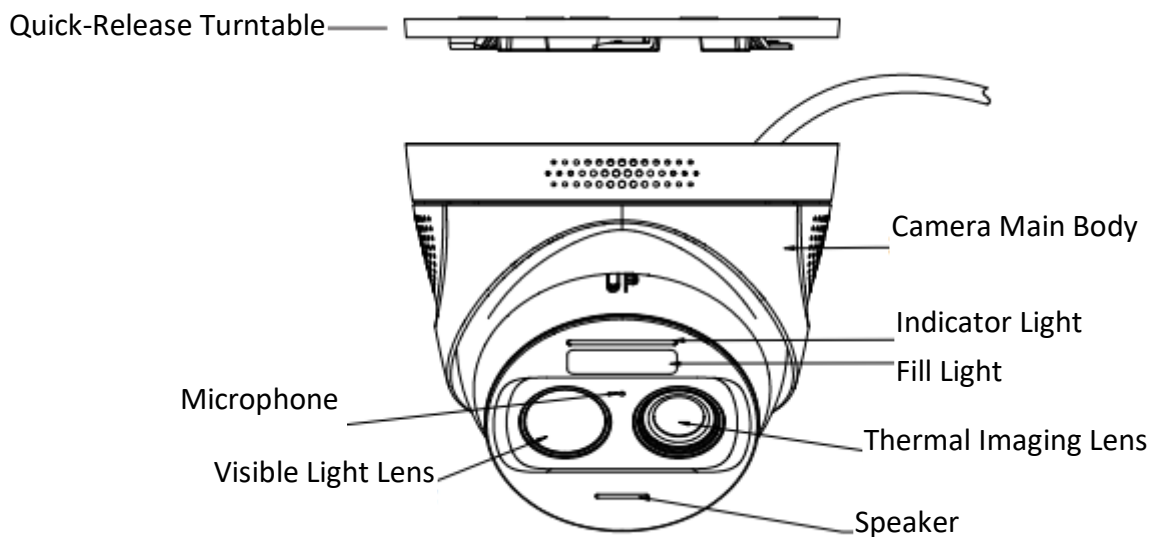


Fig. 1-1 Sphere Appearance

Table 1-1 Indicator Description

Indicator	Description
Red	Alarm
Green Light	Normal Operation
Yellow Light	Fault

1.5 Cables

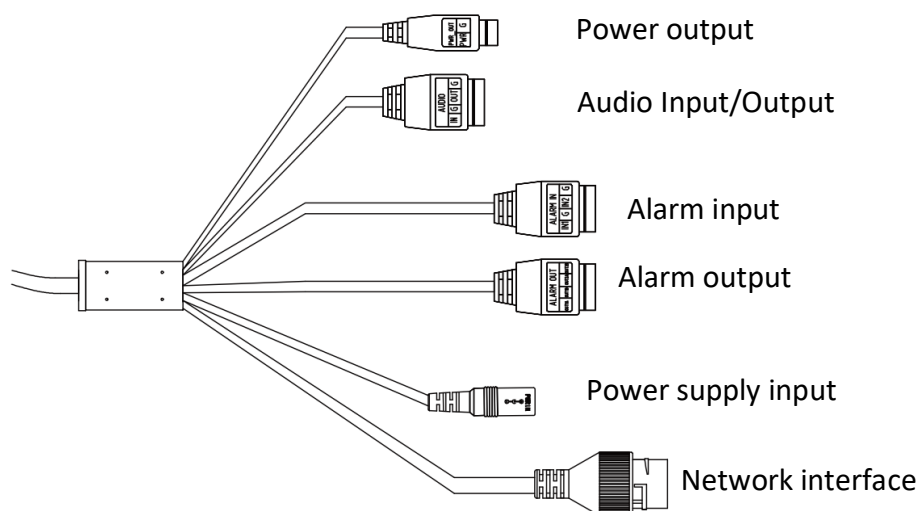


Fig. 1-2 Cables

- Power Out
DC 9~30 V。

- Alarm In

Connect to alarm input device.

- Alarm Out

Connect to alarm input device.

- Audio In/Out

Connect to audio input/output device

- Network Interface

Network signal output.

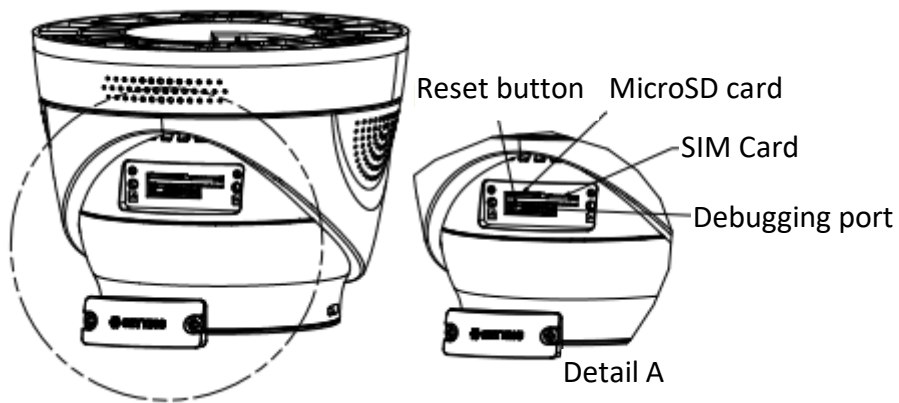


Figure 1-5 SD Card Interface

- Card Slot

You can plug in micro SD card and SIM card (for 4G version only) for local storage.

- Reset Button

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 is equipped with six external interfaces in total, including the power interface, audio input/output interface, alarm input interface, alarm output interface, and network interface. The wiring instructions for the alarm interface and audio interface are provided below:

Table 2-1 Alarm Interface Description

ID	Description	Wiring Instructions
IN	Connect to the positive terminal of the alarm input signal	Connect to one alarm input signal
G	Connect to the negative terminal of the alarm input signal	
NO	Connect to the alarm output signal	Connect to one alarm output signal; polarity is not distinguished.
C1	Connect to the alarm output signal	

Table 2-2 Audio Interface Description

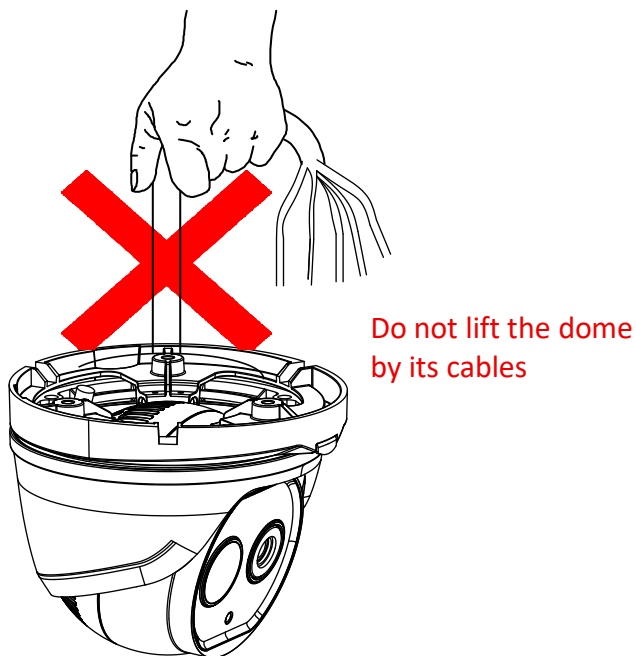
ID	Description	Wiring Instructions
IN	Connect to the positive terminal of the audio input signal	Connect to one Line-in audio signal
G	Connect to the negative terminal of the audio input signal	
OUT	Connect to the positive terminal of the audio output signal	Connect to one Line-out audio signal.
G	Connect to the negative terminal of the audio 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.
- When moving the device, do not pull on the cables behind the device, otherwise, this may affect the device's waterproof performance or lead to wiring problems, as shown in the figure below.



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.

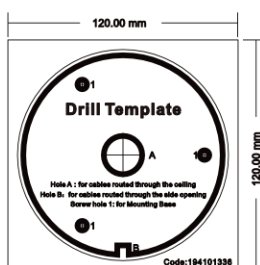


Figure 2-1 Installing Sticker

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

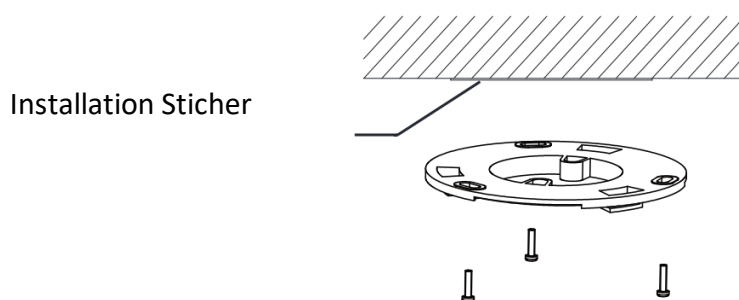


Figure 2-2 Fixed Base

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.

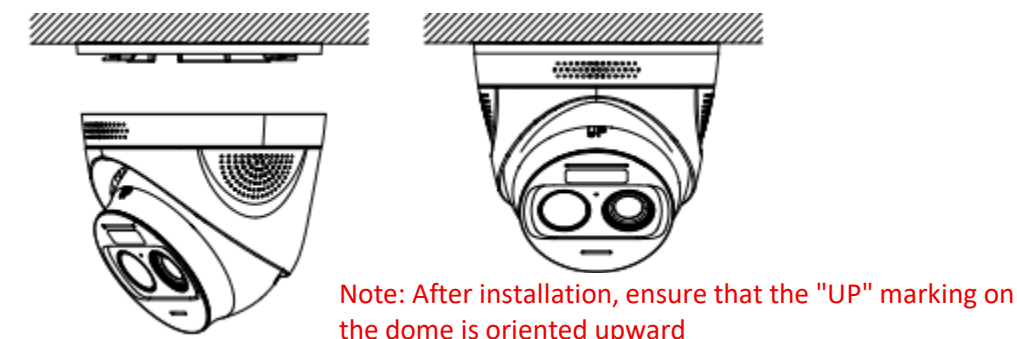


Figure 2-3 Install Device

Note

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

2.2.3 Adjusting 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.

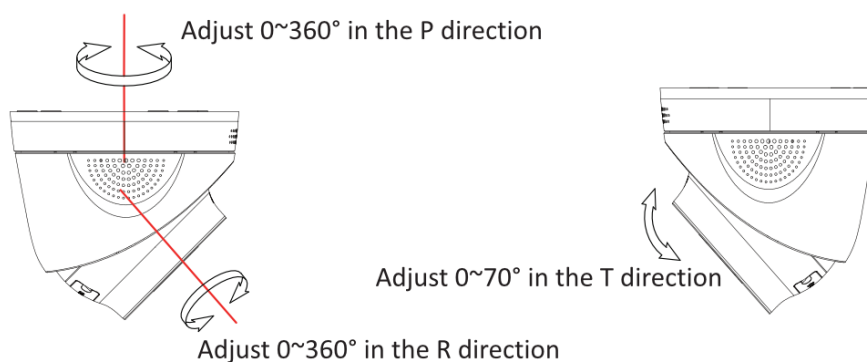


Figure 2-4 Adjust Sphere Direction

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.

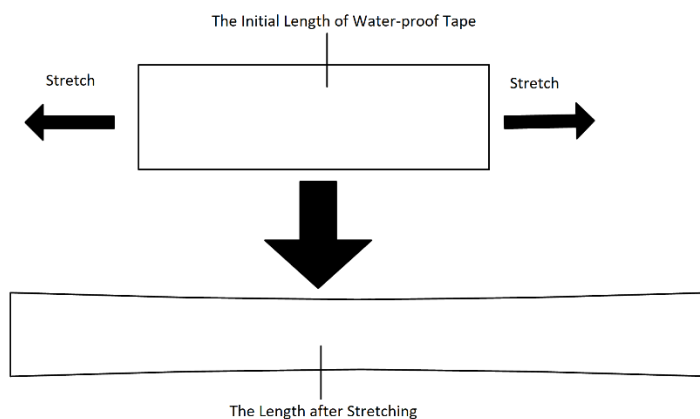


Figure 2-5 Stretch Water-Proof Tape

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

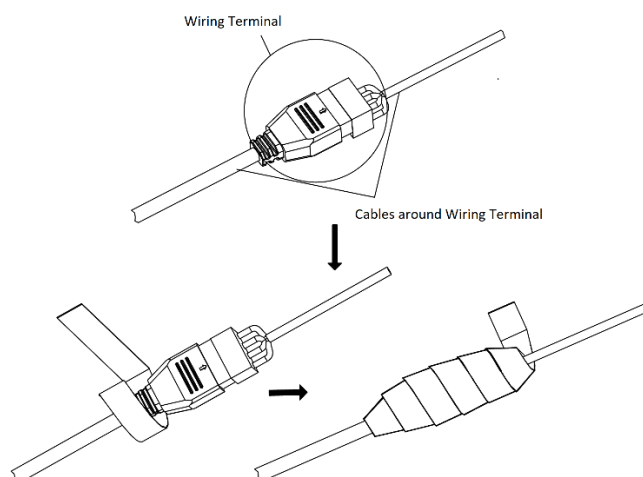


Figure 2-6 Wrapping Waterproof Tape

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

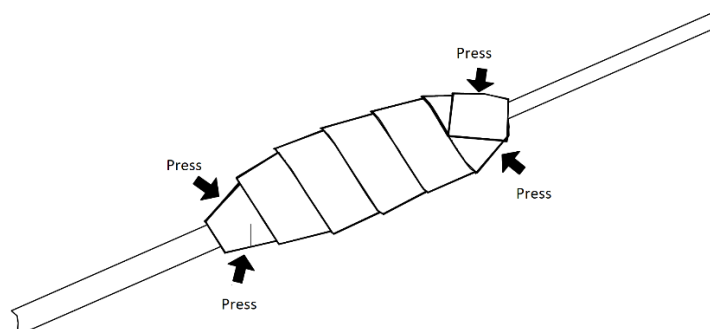


Figure 2-7 Press Water-Proof Tape

2.2.5 Installing Network Port Waterproof Sleeve

Some devices come with a waterproof network port cover. For outdoor installation and use, the supplied waterproof network port cover must be installed to prevent short circuits due to water ingress. Please install it as needed. The installation steps for waterproof network port cover are as follows.

Steps

1. If the network cable has already been laid, cut the crystal head at the end connected to the device, and thread the network cable through the fastening nut, waterproof rubber ring, and waterproof cap as shown in the figure.
2. Insert the waterproof rubber ring into the waterproof cap to enhance sealing performance.
3. Terminate the network cable with a crystal head and place the rubber O-ring on the device's network port.
4. Insert the prepared network cable into the network port, fit the waterproof cap over the network port end, and screw the fastening nut clockwise into the waterproof cap. When screwing the waterproof cap into the network port, keep the network port's latch aligned with the notch on the waterproof cap to complete the installation of the waterproof network port cover properly.

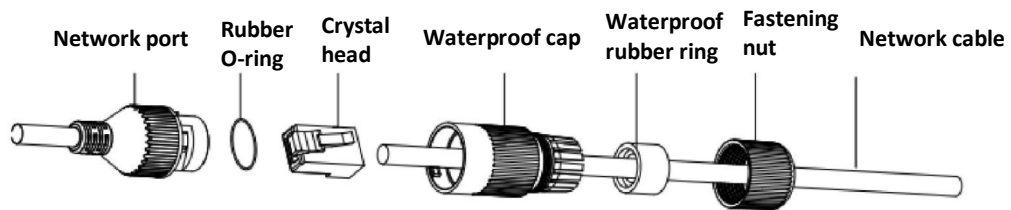


Fig. 2-8 Installing the Waterproof Network Port Cover

Chapter 3 Operation Instructions

3.1 Network Connection



Note

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 Device Activation and Configuration

The device must first be activated and a login password must be set before it can be logged into and used. You can activate the device using SADP software, client software, or a browser.

The factory default values are as follows:

Default IP: 192.168.1.64.

Default port: 8000.

Default username (administrator): admin.

3.2.1 Activating via SADP Software

Activation via SADP refers to the process of activating the device using the SADP software. This method requires the installation of the SADP software, after which certain network parameters of the device can be modified through the SADP software. The software has relatively simple functions.



Note

Visit www.hikvision.com to obtain the SADP software and complete the installation.

Step 1: Connect the device and computer with a network cable.

Step 2: After running, the SADP software will automatically search for all online devices in the LAN.

Step 3: Select the device in the list that needs to be activated and whose security status is displayed as “Inactive”.

Step 4: Set the device activation password under “Activate Device”.

Caution

- To protect your personal privacy and corporate data, and to avoid network security issues with the device, create a strong password that complies with security protocols.
- To enhance security while using the product on the network, the device password set must be 8-16 characters long and consist of at least two or more types of characters from numbers, lowercase letters, uppercase letters, and special characters.

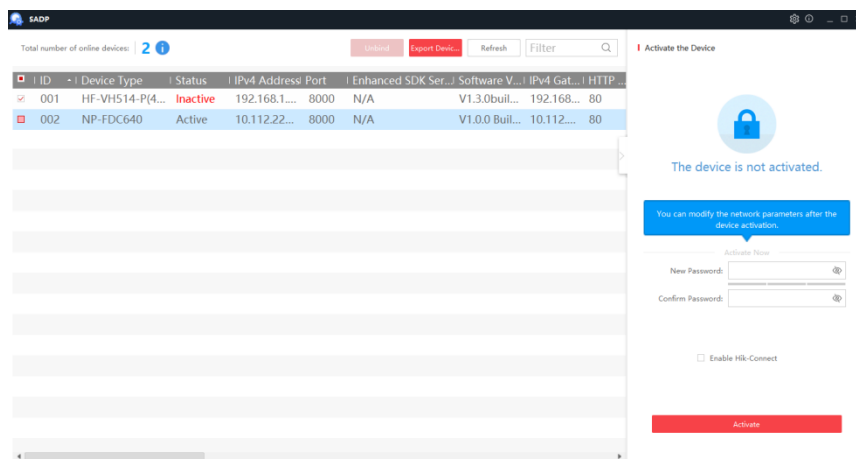


Fig. 3-1 Activating the Device

Step 5: Click “OK”.

Note

The device’s security status will update to “Activated”.

Step 6: Modify the device IP address.

Check the activated device, set the device’s IP address, subnet mask, gateway, and other information under “Modify Network Parameters”, enter the activation password, and click “Modify”, as shown in the figure.

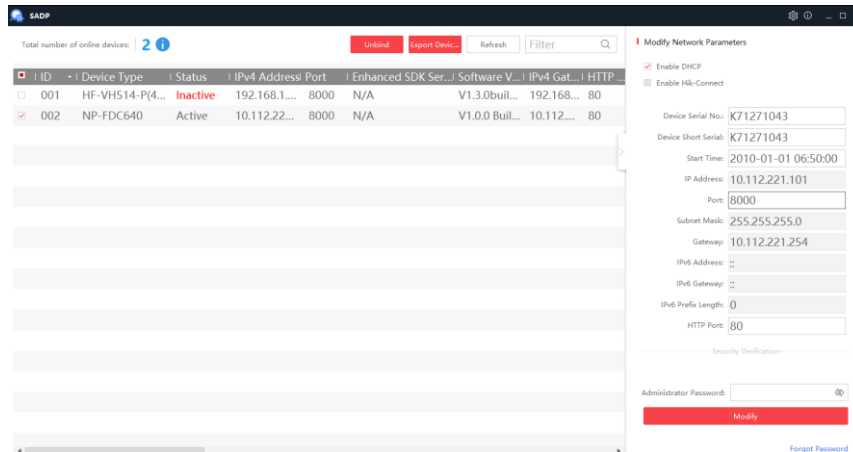


Fig. 3-2 Modifying Device Information

Note

- When setting the IP address of the device, ensure that the device IP address and the computer IP address are in the same LAN network segment.
- “admin” is the system administrator user. For the sake of system security, you are suggested to conduct all operations under a newly created user account. For specific steps to add a user, please refer to “11.4 User Management”.

3.2.2 Activating via Browser

Activation via browser refers to the process of logging into the device through a browser to activate it. This method requires the IP addresses of the device and the computer to be in the same network segment.

Step 1: Connect the device and computer with a network cable.

Step 2: Modify the computer's IP address and the device's IP address to be in the same network segment.

Note

The device default IP address is 192.168.1.64. The computer IP address can be set to any IP address between 192.168.1.2 and 192.168.1.254 (excluding 192.168.1.64).

Step 3: Enter 192.168.1.64 in the browser to display the activation interface.

Step 4: Set the device activation password on the device activation interface, as shown in the figure.

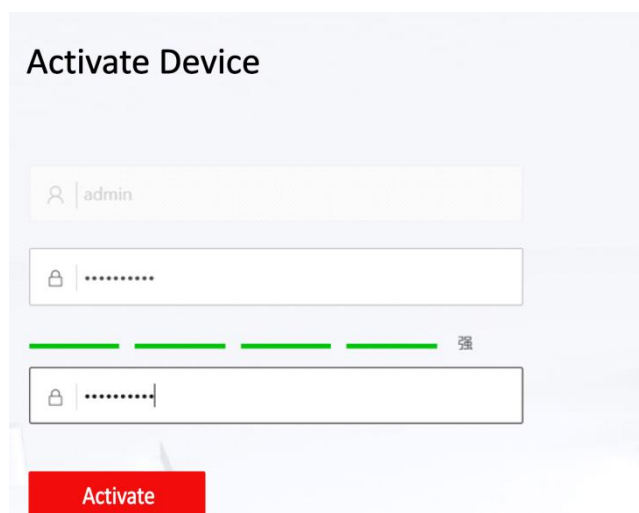


Fig. 3-3 Activation Interface on Browser

 Caution

- To protect your personal privacy and corporate data, and to avoid network security issues with the device, create a strong password that complies with security protocols.
 - To enhance security while using the product on the network, the password set must be 8-16 characters long and consist of at least two or more types of characters from numbers, lowercase letters, uppercase letters, and special characters.
-

Step 5: Click “OK”.

Step 6: Open the browser, enter 192.168.1.64 in the browser, and log in to the device.

Step 7: After logging into the device, you can modify such parameters as the device's IP address, subnet mask, and gateway on the “Network Settings - TCP/IP” interface. For specific operations, please refer to the configuration instructions under “Chapter 5 Network Settings and Access”.

3.2.3 Activating via Client Software

Activation via client refers to the process of logging into the client software to activate the device. This method requires the installation of the client software, after which the device can be managed through the client software with complete functionality.

 Note

Visit www.hikvision.com to obtain the iVMS-4200 client software and complete the installation.

Step 1: Connect the device and computer with a network cable.

Step 2: Run the client software, click the “Device Management” icon under “Control Panel” to display all online devices found in the LAN, as shown in the figure.

Fusion Detection Camera User Manual

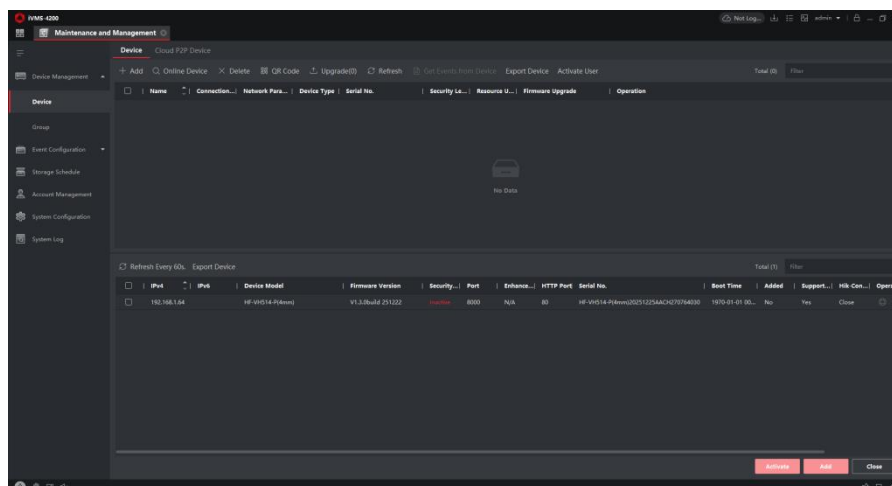


Fig. 3-4 Device List

Step 3: Select the device in the list that needs to be activated and whose "Security Status" is displayed as "Inactive".

Step 4: Click "Activate", as shown in the figure.

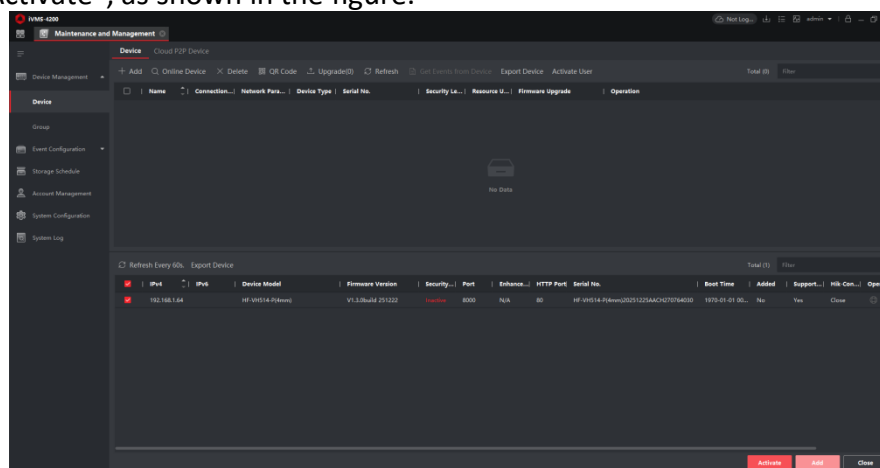
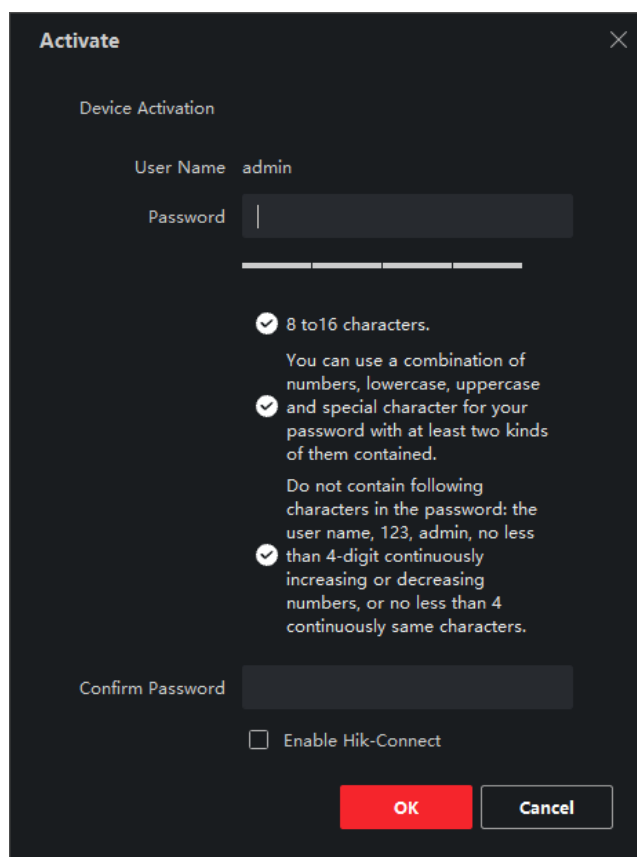


Fig. 3-5 Selected Device Row

Step 5: Set the device activation password on the activation page and click "OK". as shown in the figure.

Note

The device's security status will update to "Activated".



Activate [X]

Device Activation

User Name admin

Password []

8 to 16 characters.

You can use a combination of numbers, lowercase, uppercase and special character for your password with at least two kinds of them contained.

Do not contain following characters in the password: the user name, 123, admin, no less than 4-digit continuously increasing or decreasing numbers, or no less than 4 continuously same characters.

Confirm Password []

☐ Enable Hik-Connect

OK Cancel

Fig. 3-6 Activating the Device

 Caution

- To protect your personal privacy and corporate data, and to avoid network security issues with the device, create a strong password that complies with security protocols.
 - To enhance security while using the product on the network, the password set must be 8-16 characters long and consist of at least two or more types of characters from numbers, lowercase letters, uppercase letters, and special characters.
-

Step 6: Modify the device IP address.

Select the activated device, click "Modify Network Parameters", and modify the device's IP address, gateway, and other information in the pop-up page. After modification, enter the password set during device activation and click "OK".



- When setting IP address, ensure that the device IP address and the computer IP address are in the same network.
 - “admin” is the system administrator user, who has the authority to create system users. For the sake of system security, you are suggested to perform operations under a newly created user account. For specific steps to add a new user, please refer to “Adding a User”.
 - After logging into the device via the client software, you can configure the device's parameters and functions (temperature measurement, dynamic fire spot search, etc.). The configuration method is the same as that used in the browser.
-

3.3 Accessing Device

Provide access method through web page and Hik-Connect.

3.3.1 Accessing Device via Web Client

Login System

After the device is successfully connected to the computer, you can enter the device's IP address in the browser's address bar to log in. After entering the device's IP address, the login screen will pop up. Then, you can enter the username and password to log in to the system.



- If you have modified the IP address, please use the new IP address to log into the system.
 - An interface for installing browser plugin will automatically pop up during the first access. Please save the plugin, then close the browser and proceed with plugin installation. After the plugin is installed, you can log in to the device for related operations.
-

Get Help

After successfully logging into the device, you can click “Help” to see the device's operating instructions.

Exit System

When entering the device's interface menu, you can click “Cancel” in the upper-right corner to safely exit the system.

3.3.2 Accessing Device via EZVIZ Cloud

Devices connected to Hik-Connect can receive abnormal information of the site of interest and

take security measures in time.



Note

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.
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.



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 Adding 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.
-



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



Figure 3-7 EZVIZ Cloud Video QR Code



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.

3.4 Main Interface Description

The main interface of the device allows you to preview, playback, perform and configure various functions.

- Live View: Used for video image preview and operation control.
- Playback: Search, play back, and download recordings stored on the Micro SD card by time.
- Event Center: Configure algorithm modes and alarm events.
- Configuration: Perform system configuration and function configuration.
- Maintenance and Security: Enable maintenance functions and security configuration.

Chapter 4 Web Client Configuration and Operation

4.1. Preview



Note

The following describes functions that may be included on the preview interface. Please refer to the actual device's preview interface for the specific functions available.

Preview Interface Functions

- On the preview interface, you can control functions such as preview, recording, snapshot, and silencing.
- The preview image size can be selected according to the user's actual needs.
- It supports selecting the stream type for the live view during preview.
- When the browser cannot preview normally, you can select and install different playback plugins according to the browser for preview. Control selection is related to the specific browser. When using an IE-core browser, you can choose Webcomponents and QuickTime as plugins; when using a non-IE-core browser, you can choose Webcomponents as the plugin.

Preview Interface Icon Function Description

Table 4--1 Icon Function Description

Map icon	Function Description
	Preview screen display size selection. Represent 4:3, 16:9, Original Ratio, and Adaptive Display respectively.
	Preview stream type selection. Represent Main Stream and Sub Stream respectively.
	Playback plugin switch selection.
	Voice Intercom On Button / Voice Intercom Active
	Preview screen on and off.
<i>Silence</i>	Silence button, eliminates the device's alarm sound signal.
	Take snapshot during preview.
	Local recording during preview on and off.
	Electronic zoom on and off. Drag the left mouse button on the preview screen for electronic zoom.
	Adjust preview volume.

4.2 Playback

View recorded video files and perform playback operations.

Prerequisites

Recorded video files must already exist. For recording schedule configuration, refer to the [Recording Schedule](#) section.

Operating Procedure

1. On the device web client, click *Playback* to enter the video playback interface.
2. Select the recording date and click *Search*.
3. Select the time point for playback. Drag the time bar below to select the playback time.



The system defaults to playing from the start time of the video file.

4. Click ▶ to start video playback.
5. Optional: During video playback, the following operations can be performed.
 - Set the playback time point in the "Playback Time Point Location" window, then click ↶. The video will jump to the set time.
 - Use the function buttons below the video for fast forward, slow motion, single frame, snapshot, clip, zoom, mute, full screen, etc.
6. Optional: Click ⬇ to download the video file to the local computer.

4.3 Viewing Pictures

Query, view, and download picture files effectively stored on the device.



To view picture files during event alarms, you need to configure the linkage method in the *event* first. Specific method: Go to *Configuration* → *Event*, then enter the corresponding event configuration interface (e.g., enter *Alarm Input*), click *Linkage Configuration*, and check *Upload to FTP*.

Operating Procedure

1. Click *Picture* to enter the picture query interface.
2. Set the query conditions on the left side of the window, select the file type and start/end time, and click *Search*. The pictures that meet the criteria will be listed in the right-hand list.
3. Check the picture rows you want to download locally, and click *Download* to download the pictures.



If you need to terminate the download, click *Stop Download*.

Result Description

The downloaded pictures are stored in the **playback download save path** set in *Parameters* → *Local Configuration*.

4.4 Parameter Configuration

4.4.1 Local Configuration

Go to *Configuration* → *Local*, you can configure the following parameters.

Playback Parameters

Protocol type

Set according to the actual situation.

Playback Performance

Set according to actual playback requirements.

Display Rule Information

Can choose **Yes** or **No**. When Display Rule Information is enabled, an information box will appear on the preview interface, including the dynamic analysis frame for motion detection, etc.

Snapshot File Format

Set the save format for captured pictures.

Snapshot Overlay Rule Information

Can choose **Yes** or **No**.

Video File

Video File Package Size

Indicates the size of a single video file stored locally.

Video File Save Path

The local path where video files are stored. Click *Browse* to change the path. Click *Open Folder* to open the folder under the archive path.

Playback Download Save Path

The local path where playback downloaded video files or pictures are stored. Click *Browse* to change the path. Click *Open Folder* to open the folder under the archive path.

Snapshot and Clip

Preview Snapshot Save Path

The local path where pictures captured during preview are stored. Click *Browse* to change the path. Click *Open Folder* to open the folder under the archive path.

Playback Snapshot Save Path

The local path where pictures captured during playback are stored. Click *Browse* to change the path. Click *Open Folder* to open the folder under the archive path.

Playback Clip Save Path

The local path where video files clipped during playback are stored. Click *Browse* to change the path. Click *Open Folder* to open the folder under the archive path.

4.4.2 System Parameters

System settings



Note

The content in System Settings depends on the actual device. The following describes system settings that the device may support.

Viewing Basic Device Information

Device system information includes device model, serial number, version information, number of channels, number of hard disks, number of alarm inputs and outputs.

Go to *Configuration* → *System* → *System Settings* → *Basic Information* to modify the device name and device number.

Setting the Time on the Terminal

Configure device time, supports two time calibration methods: NTP time calibration and manual time calibration.

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

Select your time zone, then select the time calibration method.

NTP timing

You need to configure the NTP server address, server port, and time calibration interval.



Note

Click *Test* to check if the set NTP server is correct.

After setup, the device will periodically synchronize time from the NTP server according to the calibration interval.

Manual Timing

You can choose to set the device time directly or calibrate by checking *Synchronize with Computer Time*.

Setting Daylight Saving Time

If the device is located in a region that observes Daylight Saving Time (DST), you can configure DST to keep the device synchronized with local time.

Operating Procedure

1. Go to *Configuration* → *System* → *System Settings* → *Daylight Saving Time*.
2. Check *Enable Daylight Saving Time*.
3. Select the **Start Time**, **End Time**, and **Offset Time** according to the DST system of the device's location.
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, upgrade device.

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

Reboot Device

Click *Restart* to restart the device.

Restore Default Value

Partially Restore

Simple Restore Device Parameters means restoring all parameters except IP address, subnet mask, gateway, user information, system standard, security questions, etc., to factory settings.

Fully Restore

Fully restore device parameters to factory settings.

Information Export

Device Parameter

Used to export device parameter files, which can facilitate configuring the same parameters on devices.

1. Click *Device Parameters* to pop up the *File Encryption Configuration* window.
2. Set an encryption password to encrypt the exported device parameter file.
3. Click *OK*, select the storage path for export.

Parameter Import

Device Parameter

Import device parameter files, which can facilitate users to configure the same parameters on devices.

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

Upgrade

Upgraded File

When the device needs an upgrade, you can copy the upgrade program to the local computer, click *Browse* to select the path where the upgrade file is stored, and click *Upgrade* to start the upgrade.



Caution

After a successful upgrade, the device will automatically restart. Do not power off during the upgrade process.

Querying Logs

The log interface allows you to query, display, and export log information effectively stored on the device storage.

Operating Procedure

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

The results that meet the criteria will be displayed in the log list.



Note

A single query only displays the first 2000 logs within the query time range.

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



Note

There are two log save formats: Text.files and Excel.files.

Querying Security Audit Logs

Used to query and manage the device's security logs.

Operating Procedure

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

The log list displays all log information that meets the query criteria.

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

Security management

Setting Authentication Method

Set RTSP authentication.

Authentication methods available: digest, digest/basic. Different authentication modes require different information to be carried. Refer to the specific protocol for the required information.



Basic authentication information is simpler. If higher network security is required, it is recommended to use digest.

Setting IP Address Filtering

Used to set the access permissions for computers or terminals to access the device.



IP addresses refer to IPv4 addresses.

Operating Procedure

1. Go to *Configuration* → *System* → *Security Management* → *IP Address Filtering*.
2. Check *Enable IP Address Filtering*.
3. Set the IP address filtering method.

Prohibit	Except for the IP addresses in the list, other IP addresses are allowed to access the device.
-----------------	---

Allowed	Only IP addresses in the list are allowed to access the device.
----------------	---

4. Set the IP addresses to be filtered.
 - 1) Click *Add*, enter the IP address.
 - 2) Optional: Click *Modify* to modify the selected IP address in the list.
 - 3) Optional: Click *Delete* to delete the selected IP address in the list.
5. Click *Save*.

Setting Security Services

Configure SSH and illegal login lock function.

Go to *Configuration* → *System* → *Security Management* → *Security Services*. Enable or disable the corresponding security services according to the actual situation. The configuration takes effect after saving.

Enable SSH

SSH is a security protocol based on the application layer. Enabling it can effectively prevent information leakage during remote management.

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



After the device restarts, this function is not enabled by default.

Enable Illegal Login Lock

When this function is enabled, if the number of incorrect username or password entries during login reaches the upper limit (7 times, or 5 times when SSH is enabled), the device will display a lock message reminder and automatically enter a locked state.



Caution

For your account security and to prevent unauthorized users from logging into the device, it is recommended to enable this function. Please set it according to the actual situation.

Enable Security Mode

Check *Enable Security Mode*, enter the administrator password, and confirm to complete enabling. After enabling this function, the device will use strong password verification. In this mode, some older version NVRs may not be able to connect.

User Management

User Management

When logging into the system using the device default username (admin), you can modify the admin user password, create and edit other users, up to a maximum of 31 users.

Account Security Settings

Click *Account Security Settings*, enter the admin user password, you can set or modify security questions. After setting security questions, click *Forgot Password* on the login interface, answer the security questions to reset the password.



Note

- During reset, please ensure the device and the computer are on the same subnet of the local area network.
 - admin is the default user. This username cannot be modified, only its password can be changed.
 - When the admin user adds, modifies, or deletes other users, the admin user's password needs to be entered.
-



Caution

- To ensure the security of account information, it is recommended that the set password length be 8--16 characters, and consist of at least two or more types of characters from numbers, lowercase letters, uppercase letters, and special characters (! " # \$ % & ' () * + , - . / : ; < = > ? @ [\] ^ _ ` { | } ~ space) , and it must not contain the username.
 - Passwords with a length less than 8 characters, passwords containing only one type of character, passwords that are the same as the username, or passwords that are the reverse of the username are considered risky passwords. To better protect your privacy and enhance product security, it is recommended to change risky passwords to high-strength passwords.
-

Add User / Modify User / Delete User

- Click *Add* to add a new user. You can set the user's type, password, and permissions. The password strength is divided into Strong, Medium, and Weak based on the complexity of the password setting.
 - Select an existing user, click *Modify* to modify user information.
-

- Select an existing user, click *Delete* to delete obsolete user information.

Viewing Online Users

Used to display the list of users logged into the device on the network.

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



Caution

- If the IP address and username are the same, only one user login information will be displayed.
 - The online users interface can display up to 30 user login entries.
-

4.4.3 Network Parameters

Setting TCP/IP

TCP/IP is the most basic transmission control protocol on the Internet. TCP/IP configuration is required for the network to function properly.

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



Note

The following describes the TCP/IP parameter configurations that the device may support. For the specific parameters supported by the device, please refer to the actual device interface.

Network Card Type

Select according to the network environment.

IPv4 Address

- Check *Obtain automatically*, the device will automatically obtain network parameters based on the network environment.
 - Uncheck *Obtain automatically*, manually fill in the device IPv4 address, IPv4 subnet mask, IPv4 default gateway, and other LAN parameter information.
-



Note

When manually filling in IPv4 network parameters, click *Test* to confirm if the IP address is available. After confirming it is available, click *Save*.

MTU

Represents the Maximum Transmission Unit, which is the size of the largest data packet that can be transmitted in a TCP/UDP protocol network transmission.

DNS Server Configuration

When the device has a correct and available DNS server address set, domain name resolution can be performed.

Configuring Port Parameters

When the device cannot be accessed over the network due to port conflicts, you can modify the device ports.



Caution

Do not modify the default port parameters arbitrarily, otherwise, the device may become inaccessible.

Go to *Configuration* → *Network* → *Basic Configuration* → *Port*, set the port parameters, and they will take effect after saving.

HTTP Port

Represents the port for browser access to the device. For example, if the **HTTP port** is modified to 81, when logging in via a browser, you need to enter *http://192.168.1.64:81* in the browser.

RTSP Port

Represents the port for the device's Real-time Transport Protocol.

HTTPS Port

Represents the port for browser certificate access. When a browser accesses the device, certificate verification is required for access, providing a high level of security.

Service Port

When using a client to log in to the network camera, if you modify the service port, you need to enter the port number on the login interface to log in to the network camera normally.

Setting Platform Access Function

The platform access function mainly configures access to the 28181 platform, ISUP platform, and Ezviz Cloud platform.

- 28181 platform access means registering the device to the public security network platform in accordance with GB/T28181 requirements, controlling the device through the public security network platform to achieve operations such as audio and video on-demand, historical audio and video playback, etc.
- ISUP access refers to connecting to the ISUP platform.
- Ezviz Cloud access means that devices supporting Ezviz Cloud access can be accessed via Ezviz Cloud after being registered to the Ezviz Cloud platform.

Accessing Public Security Network Platform

Follow the requirements of GB/T28181 to register the device to the public security network platform, enabling functions such as remote real-time viewing and device management.

Operating Procedure

1. Go to *Configuration* → *Network* → *Advanced Configuration* → *Platform Access*.
2. Select *28181* as the **Platform Access Method**.
3. Check *Enable*.

4. Set the relevant 28181 parameters according to the 28181 protocol. You can find relevant information about the protocol for configuration.
5. Click *Save*.

Accessing ISUP Platform

Follow the requirements of the ISUP platform to register the device to the ISUP platform, enabling functions such as remote real-time viewing and device management.

Operating Procedure

1. Go to *Configuration* → *Network* → *Advanced Configuration* → *Platform Access*.
2. Select *ISUP* as the **Platform Access Method**.
3. Check *Enable*.
4. Set ISUP parameters.
5. Click *Save*.

Refresh the web page or restart the device to check the registration status.

Accessing Ezviz Cloud

Ezviz Cloud is a micro-video service platform under Ezviz. Devices supporting Ezviz Cloud access can be accessed via Ezviz Cloud after being registered to the Ezviz Cloud platform.

Operating Procedure

1. Go to *Configuration* → *Network* → *Advanced Configuration* → *Platform Access*.
2. Select *Ezviz Cloud* as the *Platform Access Method*.
3. Check *Enable*.
4. For *Access Server IP*, select *Custom* or *Default*.
 - Custom: Manually set the domain name server IP address.
 - Default: The device automatically assigns a server IP address from the nearest region.
5. Click *Save*.

Note

- After completion, refresh the web page or restart the device to check the *Registration Status* and see if the device registered successfully.
 - If logged in as an administrator user, you can view the device's Ezviz Cloud verification code. If logged in as a non-administrator user, you cannot view it.
-

Setting HTTPS

In network access, to improve the security of browser access, you can use the HTTPS protocol to build a secure, encrypted network transmission, ensuring the security of transmitted data through authentication and encrypted communication.

Operating Procedure

1. Go to *Configuration* → *Network* → *Advanced Configuration* → *HTTPS*.
2. Create and install certificates.

Create Private Certificate

In the Installation Method, select *Create Private Certificate*, click *Create*, open the private certificate creation window, fill in parameters such as Country, Domain Name/IP, Validity Period, etc., and click *OK*.

Create Certificate Request	In the Installation Method, select <i>Create Certificate Request first, then continue installation</i> , click <i>Create</i> , open the authorization certificate creation window, fill in parameters such as Country, Domain Name/IP, etc., and click <i>OK</i> to complete the request. After receiving the signed valid certificate, you can download or delete the certificate request, and you can also install the downloaded security certificate.
Install Signed Certificate	In the Installation Method, select <i>Already have a signed certificate, install directly</i> , click <i>Browse</i> to select the existing signed certificate, then click <i>Install</i> , and click <i>Save</i> after completion.
Download Certificate	After creating a certificate request, click <i>Download</i> to download the certificate and send it to the certification authority for authentication.
Delete Certificate	You can view the installed certificate. Click <i>Delete</i> to delete the current certificate.

3. Check *Enable* to access the device via the HTTPS protocol.
4. Optional: Check *Auto Redirect to HTTPS* to automatically convert the entered IP address to an HTTPS address, enhancing network security.
5. Click *Save*.



Note

- The valid range for the HTTPS port is: 1~65535. When accessing remotely via HTTPS, enter *https://IP address* in the browser address bar; if the HTTPS port is set to a port other than 443, enter *https://IP address +: (colon) + port number* in the browser address bar, for example, *https://192.168.1.64:81*.
 - Users can also choose to *create a certificate request* and upload a certificate issued by an authoritative Certificate Authority (CA) for authentication (usually authoritative CAs charge a fee) to improve the security level of access.
-

Configuring Open Network Video Interface

When you need to connect to the device using the Open Network Video Interface protocol, you can configure the corresponding users as needed to enhance the device's network security.

Operating Procedure

1. Go to *Configuration* → *Network* → *Advanced Configuration* → *Integration Protocol*.
2. Check *Enable Open Network Video Interface*.
3. Configure users.
 - 1) Click *Add* to customize an Open Network Video Interface user according to the protocol.
 - 2) Optional: Click *Delete* to delete this user.
 - 3) Optional: Click *Modify* to modify user information.
4. Click *Save*.
5. Optional: Repeat the above steps to add multiple users as needed.

Setting HTTP Listening

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

Operating Procedure

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



Click *Reset* to re-enter the destination IP address or domain name information.

4. Click *Save*.

4.4.4 Video and Audio Parameters



The content in the Video and Audio parameter settings depends on the actual device. The following describes the video and audio settings that the device may support.

Video Configuration

You can set video parameters according to the quality requirements of the desired preview image.

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



The following describes video parameters that the device may include. For the specific configurations supported by the device, please refer to the actual device interface.

Channel No.

Select the channel number for which you want to set video parameters.



Only multi-channel devices have this option.

Bit Stream Types

Main Stream (Scheduled)

The main stream is used for HD storage and preview, with relatively high resolution, bitrate, and image quality.

Sub-Stream

The sub stream is used for standard definition storage and preview when network bandwidth is insufficient, with relatively low resolution, bitrate, and image quality.

Video Type

Video Stream

Video Stream Only.

Composite Stream

Includes video stream and audio stream.

Resolution

Select according to the customer's requirements for video clarity. The higher the resolution, the higher the network bandwidth requirement.

Bitrate Type and Max. Bitrate

Constant Bitrate

Indicates that the bitrate is maintained at the average bitrate for transmission. Compression speed is fast, but it may cause video mosaic artifacts.

Variable Bitrate

Indicates that the bitrate adjusts itself without exceeding the maximum bitrate. Compression speed is relatively slow, but it ensures picture clarity in complex scenes.

Image Quality

When the bitrate type is Variable Bitrate, the image quality can be set. Select according to the customer's requirements for image clarity. The higher the image quality, the higher the network bandwidth requirement.

Video Frame Rate

Represents the number of frames per second of the video. Set according to the actual bandwidth. The higher the video frame rate, the higher the required bandwidth and storage space.

Video Encoding

H.264

H.264 is a video codec technology with high compression ratio, flexible processing, ultra-low bitrate, saving network transmission bandwidth and storage space.



Caution

When the sub stream's **video encoding** parameter is set to *MJPEG*, if the preview screen appears stuttering, it is recommended to use the *H.264* encoding format to ensure smooth video.

H.265

H.265 is a video codec technology with high compression ratio, flexible processing, and ultra-low bitrate. Compression performance is doubled compared to the current H.264, further saving bandwidth and storage space.

Encoding Complexity

At the same bitrate, the higher the encoding complexity, the higher the image quality, but the higher the requirement for network bandwidth.

I Frame Interval

The number of frames between two consecutive keyframes. The larger the I-frame interval, the smaller the bitstream fluctuation, but the image quality is relatively poor; conversely, the smaller the interval, the greater the bitstream fluctuation, and the higher the image quality.

SVC

It is a scalable video coding technology that can be used for encoding and storage when bandwidth is insufficient. This function needs to be implemented in conjunction with backend storage devices and can be set for devices with H.264/H.265 encoding.

Stream Smoothing

You can drag the progress bar or set the stream smoothing value. The higher the value, the better the smoothness, but the image will be relatively less clear; conversely, the image smoothness will be poor, and the image will be relatively clear.

Intelligent Information Display Method

Playback Library

When only the manufacturer's dedicated player is used to play the video, intelligent rule information will be displayed in the dedicated player.

Video

When other players are supported for playing video, intelligent rule information will be displayed in those players.

Audio Configuration

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

Audio Encoding

Set the type of audio encoding. Types include G.722.1, G.711ulaw, G.711alaw, MP2L2, AAC, and PCM.

When the encoding type is selected as *MP2L2* or *AAC*, you need to set the sampling rate and audio bitrate parameters. The sampling rate and audio bitrate parameters can be selected via the drop-down list.

When the encoding type is selected as *PCM*, you need to set the sampling rate parameter. The sampling rate parameter can be selected via the drop-down list.

Audio Input

Represents the audio input method. You can choose *LineIn* or *MicIn*. If using an active pickup, select *LineIn*; if using a passive microphone, select *MicIn*.

Input Volume

The gain control value for the audio input source. Users can adjust it from 1 to -100 according to actual volume requirements.

ROI Configuration

ROI is Region of Interest encoding. After enabling the ROI function, the device will improve the image encoding quality of the selected area and reduce the encoding quality outside the selected area, making the image within the selected area clearer during image preview or recording.

Prerequisites

The ROI function is supported when the video encoding is set to H.264 or H.265. Please check the video encoding type.



Note

ROI configuration is more effective when using variable bitrate or when the bitrate setting is low.

Operating Procedure

1. Go to *Configuration* → *Video & Audio* → *ROI*.
 2. Select the **stream type**.
 3. Optional: Configure fixed area enhancement.
 - 1) Check *Enable*.
 - 2) In *Fixed Area*, select the **area number** and draw the region of interest.
 - 3) Click *Draw Area*, use the mouse to frame the fixed area on the live picture, and click *Stop Drawing*.
-



Note

Select the fixed area to be adjusted, you can adjust the position of the fixed area by dragging with the mouse.

- 4) Set the Enhancement Level and Area Name.
-



Note

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

- 5) Optional: Repeat sub-steps 2~4 to draw multiple areas.
4. Click *Save*.

4.4.5 Image Parameters

Sets the display parameters.

Go to *Configuration* → *Image* → *Display Settings* to set the image quality of the main preview screen. Click *Restore Defaults* to restore the factory default settings.



Note

The following describes the display parameter settings that the device may support. For the specific display parameters configurable on the device, please refer to the actual interface.

Image adjustment

Adjust the brightness, contrast, saturation, and sharpness of the preview image by dragging the progress bar, or set the value after the progress bar.

Exposure

Iris Type

The default setting is *Manual*.

Exposure Time

Camera electronic shutter time. The longer the exposure time, the better the image presentation effect. Different exposure times can be set according to different device scenes. If using manual iris lens mode, the time set here is the maximum exposure time.

Day/Night Switch

Day/Night Switch

Auto

In Auto mode, the device automatically switches between Day mode and Night mode based on the ambient brightness.

Day

In Day mode, the device image is forced to day, the supplemental light is not turned on, and day/night switching is not performed based on the actual scene.

Night

In Night mode, the supplemental light is turned on, and related parameters can be set. The device image is forced to night, and day/night switching is not performed based on the actual scene.

Scheduled Switch

In Scheduled Switch mode, the user needs to set the start time and end time for the day. During this period, the device will automatically use Day mode; outside this period, the device will automatically use Night mode.



Note

When selecting *Scheduled Switch*, the start time and end time can be set to span across days. Please refer to the specific device.

Sensitivity

When the **Day/Night Switch mode** is set to *Auto*, adjustable from 0-7, corresponding to the night-to-day switch threshold. The lower the sensitivity setting, the higher the brightness required for the device to switch from Night mode to Day mode. The higher the sensitivity setting, the lower the brightness requirement for the device to switch from Night mode to Day mode.

Filtering Duration

When the **Day/Night Switch mode** is set to *Auto*, the corresponding day/night switch filter time is adjustable from 5 seconds to 120 seconds. Day/night switching will only occur when the ambient illumination meets the switching requirements and remains for longer than the set threshold time.

Anti-Supplemental Light Overexposure

Uses intelligent image processing technology to prevent overexposure of the central area due to the device turning on supplemental light. This function is invalid when the supplemental light is off. Choose to enable or disable according to the actual environment.

Supplemental Light Mode

When the device supports supplemental light, you can select the supplemental light mode.

White Light Mode

The device will enable the white supplemental light for illumination.

Mixed Supplemental Light

The device will enable both white and infrared supplemental lights for illumination.

Shutdown

Turn off the supplemental light.

Brightness Adjustment Mode

When supplemental light is enabled, you can set the brightness adjustment mode and brightness.

Auto

Automatically adjust the brightness according to the picture brightness of the current channel. Automatically turn on the supplemental light when the picture reaches a certain darkness, and automatically turn it off when it reaches a certain brightness.

Manual

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

Backlight

Backlight Compensation Area

Users can select the compensation area according to the actual video scene to avoid this area being too bright or too dark. Users can also choose a custom area.

Wide Dynamic Range

Wide Dynamic Range is suitable for use environments with large differences in light intensity. When high-brightness areas under strong light sources (such as sunlight, lamps, or reflections) and relatively low-brightness areas such as shadows or backlighting coexist in the picture, you can enable the Wide Dynamic Range function and adjust the level to see the video picture clearly.

Wide Dynamic Range automatically balances the brightest and darkest parts of the picture to see more picture details.



Note

Enabling Wide Dynamic Range may conflict with some functions. Please refer to the actual device interface.

Strong Light Suppression

When the video picture has overexposed bright areas and underexposed dark areas, enabling Strong Light Suppression can weaken the bright areas and brighten the dark areas to achieve light balance for the overall picture.

White Balance

In different lighting environments, object colors change due to the color of the projected light. Selecting the appropriate white balance mode according to the use environment can correct color errors.



Note

- Lock White Balance locks the current color correction matrix. If the actual use scenario has fixed lighting types, you can select Fluorescent, Incandescent, Warm Light, or Natural Light according to the situation.
 - Fluorescent is suitable for an environment with a color temperature of about 6500K; Incandescent is suitable for about 3000K; Warm Light is suitable for about 4000K; Natural Light is suitable for about 5500K.
-

Image Enhancement

Digital Noise Reduction

Refers to the use of advanced 3D image noise reduction technology to effectively reduce image noise and make the image softer and more detailed.

Normal Mode

Control the degree of noise reduction by setting the noise reduction level.

Expert Mode

Can be adjusted through two dimensions: spatial noise reduction level and temporal noise reduction level.

Noise Reduction Level

Adjustable from 0-100.

Grayscale Range

Select the grayscale range for video encoding according to actual needs.

Video Adjustment

Optimize the image display effect by setting video adjustment parameters.

Mirror

You can mirror the video as needed, choose center, left-right, and up-down mirror adjustments, or turn off mirroring. When the image is inverted, you can flip the image through this menu.



Caution

- Using the mirror function will cause inaccurate fire point positioning.
 - After enabling mirror mode, platform recording will be briefly interrupted.
-

Video Standard

Represents the video signal standard. Different standards correspond to different maximum frame rates (e.g., 50 Hz corresponds to a maximum frame rate of 25 fps, 60 Hz corresponds to 30 fps).

Setting OSD Parameters

OSD refers to the information displayed on the video screen. The device name, date, day of the week, and overlay characters can be displayed on the video screen.

Go to *Configuration* → *Image* → *OSD Settings*, check the display items, set the channel name, set the corresponding parameters, and it will take effect after saving.

Basic OSD Information Settings

- Select the OSD information to be displayed: Check *Display Name* / *Display Date* / *Display Week*, and the corresponding OSD information will be displayed on the preview screen.
- Enable Temperature Data Overlay: Check to enable this function to overlay a real-time temperature waveform.
- Edit OSD information display position: Use the mouse to drag the red OSD box on the preview screen to the desired display position.
- Edit display format: At **Channel Name** / **Time Format** / **Date Format**, you can modify the channel name displayed on the preview screen, as well as the time and date display format.

OSD Attribute Settings

Set the attributes, font size, color, and alignment of the OSD information displayed on the preview screen.

Overlay Custom Characters

The device can overlay multiple characters onto the video image. Check and set the characters to be overlaid. The characters in the image will appear in red. You can drag the characters or set the **alignment** to adjust the overlaid characters to the desired display position. Click *Save* to complete the setup.



Some characters are default fire alarm characters and cannot be modified by users.

Setting Video Masking

Video masking refers to covering sensitive areas in the video image so that they are not displayed.

Operating Procedure

1. On the device web client, go to *Configuration* → *Image* → *Video Masking*.
2. Check *Enable Video Masking*.
3. Click *Draw Area*, then click and hold the left mouse button in the image, drag the mouse, and release the left mouse button to complete drawing one area.



You can draw up to 4 areas in the image.

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

4.4.6 Events and Alarms

Introduces the functional configuration of various events supported by the device. Configure corresponding events as needed to trigger the device to perform linkage actions.



The following describes event functions that the device may support. Please refer to the functions actually supported by the device.

Schedule and Linkage Configuration

The device receives alarm information during the set scheduled time period and links the device to perform corresponding actions.

Setting Arming Time

Set the start time and end time for task execution.

Operating Procedure

1. Click *Arming Time*.
2. Select a point on the timeline as the starting point, hold down the left mouse button and drag on the timeline, release the mouse button at the end point to complete the arming time setting.



Note

One timeline supports setting up to 8 time periods.

3. Adjust the arming time.
 - Click on the arming time period, you can manually enter the start time and end time to adjust the arming time, then click *Save*.
 - Click on the arming time period, two circles will appear at both ends of the time period. Move the mouse to either end of the time period, adjustment angles in the left and right directions will appear. Move the adjustment angles to adjust the time period.
 - Drag the arming time period with the mouse to any position on the timeline to reset the time period.

Click the *delete* icon on the time period Delete the current time period.

Click *Delete* Delete the selected time period.

Click *Delete All* Delete all set time periods.

Click *Copy to...* Copy the same schedule to other times.

4. Click *Save*.

Linkage Configuration

Alarm linkage can be enabled when an event or alarm occurs.

The following describes the linkage methods that the device may support. Please configure the linkage method according to the options available on the actual device interface.

Regular Linkage

Email Linkage

Check and configure email linkage. When an alarm is triggered, the device will send the alarm information to the configured mailbox.

For email configuration, go to *Configuration* → *Network* → *Advanced Configuration* → *Email Parameters* to complete.

Upload Center

Check *Upload to Center*. When an alarm occurs, alarm information, pictures, etc., can be uploaded to the remote central platform.

For upload center configuration, go to *Configuration* → *Network* → *Advanced Configuration* → *Platform Access* to complete.

Upload to FTP/SD Card/NAS

If FTP/NAS/SD Card is checked and configured, when an alarm is triggered, the alarm information can be sent to the FTP server, network hard drive, or microSD card for storage.



The storage media available depend on the device support. The corresponding configuration paths are as follows:

- FTP Configuration: *Configuration → Network → Advanced Configuration → FTP Settings.*
 - NAS Configuration: *Configuration → Storage → Storage Management → Network Hard Drive.*
 - SD Card Configuration: *Configuration → Storage → Storage Management → Hard Disk Management.*
-

Flash Alarm

When an event is triggered, the device will emit an alarm light signal.

Sound Linkage

When an event is triggered, the device will emit an alarm sound signal.

Linked Alarm Output

A->Number

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

Buzzer

After checking, when an alarm is triggered, the buzzer will sound an alarm prompt.

Voice broadcast

When an alarm is triggered, the corresponding event alarm voice will be broadcast.

Video Linkage

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

For recording schedule configuration, refer to the [Recording Schedule](#) section.

Configuring General Events

Introduces the basic event configuration of the device.



The following describes event types that the device may support. The actual supported event types depend on the actual interface.

Configuring Motion Detection

The motion detection function is used to detect whether there is a moving object in a certain area over a period of time. When a moving object is detected, it triggers the device to perform linkage actions.

Operating Procedure

1. Go to *Configuration → Event → General Event → Motion Detection.*
2. Check *Enable Motion Detection.*

- Optional: Set moving objects in the image to be highlighted in green.
 - 1) Check *Enable Dynamic Analysis*.
 - 2) Go to *Configuration* → *Local*, and check *Enable Rule Information*.
- Select the **Configuration mode**, set the rule area and rule parameters.
 - For Normal Mode settings, refer to the *Normal Mode* section.
 - For Expert Mode settings, refer to the *Expert Mode* section.
- Set the arming time and linkage method. Please refer to the *Schedule and Linkage Configuration* section.
- Set the **sensitivity**.
- Click *Save*.

Normal Mode

Set motion detection according to the device's default parameters.

Operating Procedure

- In **Configuration Mode**, select *Normal Mode*.
- Set the Normal Mode sensitivity parameter. The higher the sensitivity value, the more sensitive the motion detection; if the sensitivity is set to 0, motion detection and dynamic analysis will not work.
- Click *Draw Area*, hold down the left mouse button in the live image and drag the mouse, then release the left mouse button to complete drawing one area.

Click Stop Drawing End area drawing.

Click Clear All Delete the drawn area.



Multiple rule areas and rule parameters can be set using the above method.

Expert Mode

Customize motion detection parameters for day and night according to requirements.

Operating Procedure

- In **Configuration Mode**, select *Expert Mode*.
- Set Expert Mode parameters.



The parameter configuration items that the device may support are listed here. The specific configurable parameter items are subject to the actual interface.

Day/Night Parameter Switch

Shutdown

Indicates no day/night switching.

Auto Switch

The system will automatically switch between day and night modes based on environmental changes. The day mode image is in color, and the night mode image is in black and white.

Scheduled Switch

Switch according to the set time. It is in day mode during the set time period and in night mode outside the time period.

Sensitivity

The higher the sensitivity value, the more sensitive the motion detection; if the sensitivity is set to 0, motion detection and dynamic analysis will not work.

Proportion

Refers to the percentage of the moving object occupying the area you drawn. Motion detection is triggered only when the object exceeds the set percentage.

3. Select an **area**, click *Draw Area*, click and hold the left mouse button in the live image and drag the mouse, then release the left mouse button to complete drawing one area.

Click *Stop Drawing* End area drawing.

Click *Clear All* Delete the drawn area.

Configuring Masking Alarm

When the predefined masking area in the video image is blocked, preventing normal viewing of that area, it triggers the device to perform linkage actions.

Operating Procedure

1. Go to *Configuration* → *Event* → *General Event* → *Masking Alarm*.
2. Check *Enable*.
3. Set the **Sensitivity**. The higher the sensitivity value, the more sensitive the detection.
4. Set the arming time and linkage method. Please refer to the [Schedule and Linkage Configuration](#) section.
5. Click *Save*.

Configuring Alarm Input

The device's alarm input interface connects to an external alarm device. When the external alarm device generates an alarm signal, the device triggers the configured linkage actions.

Prerequisites

An external alarm device is connected to the alarm input interface of the device.

Operating Procedure

1. Go to *Configuration* → *Event* → *General Event* → *Alarm Input*.
2. Select the alarm input number and alarm type, and customize the alarm name as needed.



Note: Set the alarm type according to the connected alarm device.

3. Optional: Check *Process Alarm Input*. Once checked, the alarm linkage configured for the event will take effect.
4. Set the arming time and linkage method. Please refer to the [Schedule and Linkage Configuration](#) section.
5. Optional: Click *Copy to* to copy the alarm input information to other alarm input channels.



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

6. Click *Save*.

Configuring Alarm Output

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

Prerequisites

The device's alarm output interface is connected to an external alarm output device.

Operating Procedure

1. Go to *Configuration* → *Event* → *General Event* → *Alarm Output*.
 2. Select the **alarm output number**, set its delay and alarm name.
-



The specific delay time can be set according to the actual situation. The duration can be set from 5 seconds to 10 minutes, or it can be set to *Manual*, meaning the alarm output is turned off manually.

3. Set the arming time. Please refer to the *Schedule and Linkage Configuration* section.
 4. Optional: Click *Copy to* to copy this alarm output setting information to other alarm output channels.
-



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

5. Optional: Click *Manual Alarm* to control the alarm output device on the device's alarm output interface and trigger the alarm linkage.
6. Click *Save*.

Abnormal Event Alarm Configuration

When an abnormality occurs on the device (such as network disconnection, etc.), it can trigger the configured linkage actions.

Operating Procedure

1. Go to *Configuration* → *Event* → *General Event* → *Exception*
2. Select the exception alarm type.
3. Configure the linkage method. For linkage method settings, please refer to the *Schedule and Linkage Configuration* section.
4. Click *Save* to complete the exception alarm configuration.

Configuring Smart Events

Select and configure Smart events for specific scenarios. When a target triggers the rule, the device will perform linkage actions.



Note

The following describes event types that the device may support. The actual supported event types depend on the actual interface.

Algorithm Resource Configuration

Supports configuring whether the device's overall algorithm is enabled.

On the web client interface, go to *Configuration* → *Event* → *Smart Event* → *Algorithm Resource Configuration*. You can view the resource usage and check the desired algorithm resource configuration. Click *Save* to complete the setup.

Configuring Fire Detection

Fire detection is used to detect whether there is smoke, fire, or flames in an area. When smoke, fire, or flames are detected and a fire alarm is triggered, the configured linkage actions will be executed.

Operating Procedure

1. On the device web client, go to *Configuration* → *Event* → *Smart Event* → *Fire Detection*.
2. Check *Enable*.
3. Set the detection area and masking area.

- 1) Click *Draw Detection Area / Draw Masking Area*.

- 2) Click the left mouse button in the image to draw any convex quadrilateral.

- 3) Repeat substeps 1~2 to draw up to 4 detection areas / masking areas.

- 4) Optional: Edit the drawn area using the following methods.

- Move the mouse inside the area and drag to change the area position.
- Move the mouse to a vertex of the area, click and drag to modify the vertex position.
- Click *Clear All* to delete all drawn areas.

The device will intelligently detect and analyze events within the detection area and will ignore detection results within the masking area.

4. Select the channel alarm mode.

Smoke and Fire Alarm The channel currently detects smoke and flames.

Flame Alarm The channel currently detects flames.

5. Set the detection parameters.

Sensitivity

The higher the sensitivity, the easier it is to trigger an alarm, but the false recognition rate will also increase.

6. Set the arming time and linkage method. Please refer to the [Schedule and Linkage Configuration](#) section.
7. Click *Save*.

Configuring Indoor Passageway Blockage Detection

Indoor passageway blockage detection is used to detect whether there are obstructions occupying an indoor passageway and if the duration exceeds the set trigger alarm time. When the conditions are met, it will trigger the device to perform linkage actions.

Operating Procedure

1. On the device web client, go to *Configuration* → *Event* → *Smart Event* → *Indoor Passageway Blockage Detection*.
2. Check *Enable*.
3. Set the detection area and masking area.
 - 1) Click *Draw Detection Area / Draw Masking Area*.
 - 2) Click the left mouse button in the image to draw any convex quadrilateral.
 - 3) Optional: Repeat substeps 1~2 to draw up to 4 detection areas / masking areas.
 - 4) Optional: Edit the drawn area.
 - Move the mouse inside the area and drag to change the area position.
 - Move the mouse to a vertex of the area, click and drag to modify the vertex position.
 - Click *Clear All* to delete all drawn areas.

The device will intelligently detect and analyze events within the detection area and will ignore detection results within the masking area.

4. Set the detection parameters.

Time Threshold(s)

When there are obstructions in the detection area and the duration exceeds the set time threshold, an alarm is triggered.

5. Set the arming time and linkage method. Please refer to the [Schedule and Linkage Configuration](#) section.
6. Click *Save*.

Configuring Duty Status Detection

The off-post detection function is used to identify whether duty personnel in the fire control room are absent from their post, sleeping on duty, or using mobile phones. When the number of people in the detection area falls below the set alarm threshold, or when the duration exceeds the configured detection time, the device triggers the configured linkage actions.

Operating Procedure

1. On the device web client, go to *Configuration* → *Event* → *Smart Event* → *Duty Status Detection*.
2. Check to *enable Off-Post Detection, Mobile Phone Usage Detection, or Sleeping-on-Duty Detection* as needed.
3. Set the detection area and masking area.
 - 1) Click *Draw Detection Area / Draw Masking Area*.
 - 2) Click the left mouse button in the image to draw any convex quadrilateral.
 - 3) Optional: Repeat substeps 1~2 to draw up to 4 detection areas / masking areas.
 - 4) Optional: Edit the drawn area.
 - Move the mouse inside the area and drag to change the area position.
 - Move the mouse to a vertex of the area, click and drag to modify the vertex position.
 - Click *Clear All* to delete all drawn areas.

The device will intelligently detect and analyze events within the detection area and will ignore detection results within the masking area.

4. Set the detection parameters.



An alarm is triggered when the number of people in the detection area falls below the configured alarm threshold or when the duration exceeds the set detection time. Higher sensitivity makes the alarm easier to trigger, but may also increase the rate of false detections.

5. Set the arming time and linkage method. Please refer to the [Schedule and Linkage Configuration](#) section.
6. Click *Save*.

Configuring Elevator Hazardous Object Detection

This function is used to detect whether electric bicycles and gas cylinders enter the elevator area. This function allows users to set up to 4 quadrilateral warning zones. When a target object enters these zones, the device can generate an alarm signal and perform related linkage actions.

Operating Procedure

1. Go to *Configuration* → *Event* → *Smart Event* → *Elevator Hazardous Object Detection*.
2. Check *Electric Bicycle Detection* or *Gas Cylinder Detection* as required.
3. Draw the maximum and minimum size.
 - 1) Click *Maximum Size / Minimum Size*.
 - 2) Select a point in the preview image as the starting point, hold down the left mouse button and drag arbitrarily until a quadrilateral maximum size filter box / minimum size filter box is drawn.
 - 3) Optional: If you need to redraw the filter box, click *Maximum Size / Minimum Size* again to redraw.When an object enters the elevator and its size is within the range of the maximum and minimum sizes, it can be identified as a target; otherwise, it is not considered a target. This function can improve detection accuracy.
4. Set the detection parameters.

Mode

Select the mode according to the actual scenario.

Sensitivity

Indicates the degree to which the target enters the armed area. The larger the sensitivity setting, the easier it is to trigger an alarm.

Alarm Trigger Time

Set the duration required to trigger the alarm.

5. Set the arming time and linkage method. Please refer to the [Schedule and Linkage Configuration](#) section.
6. Click *Save*.

Configuring Hazardous Behavior Detection

This function is used to detect smoking and phone-calling behaviors in the monitored area. When a hazardous behavior is detected and an alarm is triggered, the configured linkage actions will be executed.

Operating Procedure

1. On the device web client, go to *Configuration* → *Event* → *Smart Event* → *Hazardous Behavior Detection*.
2. Check *Enable Smoking Detection* or *Enable Phone Call Detection* as required.
3. Set the detection area and masking area.
 - 1) Click *Draw Detection Area / Draw Masking Area*.
 - 2) Click the left mouse button in the image to draw any convex quadrilateral.
 - 3) Repeat substeps 1~2 to draw up to 4 detection areas / masking areas.
 - 4) Optional: Edit the drawn area using the following methods.
 - Move the mouse inside the area and drag to change the area position.
 - Move the mouse to a vertex of the area, click and drag to modify the vertex position.
 - Click *Clear All* to delete all drawn areas.

The device will intelligently detect and analyze events within the detection area and will ignore detection results within the masking area.

4. Set the detection parameters.

Sensitivity

The higher the sensitivity, the easier it is to trigger an alarm, but the false recognition rate will also increase.

Test Time

Set a value between 1 and 5 seconds. An alarm will be triggered upon exceeding the detection value.

5. Set the arming time and linkage method. Please refer to the [Schedule and Linkage Configuration](#) section.
6. Click *Save*.

Configuring Fire Extinguisher Detection

Used to detect whether there is a lack of fire extinguishers in an area. When no fire extinguisher is detected and an alarm is triggered, the configured linkage actions will be executed.

Operating Procedure

1. On the device web client, go to *Configuration* → *Event* → *Smart Event* → *Fire Extinguisher Detection*.
2. Check *Enable*.
3. Set the detection area and masking area.
 - 1) Click *Draw Detection Area / Draw Masking Area*.
 - 2) Click the left mouse button in the image to draw any convex quadrilateral.
 - 3) Repeat substeps 1~2 to draw up to 4 detection areas / masking areas.
 - 4) Optional: Edit the drawn area using the following methods.
 - Move the mouse inside the area and drag to change the area position.
 - Move the mouse to a vertex of the area, click and drag to modify the vertex position.
 - Click *Clear All* to delete all drawn areas.

The device will intelligently detect and analyze events within the detection area and will ignore detection results within the masking area.

4. Set the detection parameters.

Fire Extinguisher Quantity Threshold

An alarm is triggered if the detected number does not reach the set threshold.

Fire Extinguisher Detection Time

Can be set from 1--3600 seconds. If no fire extinguisher is detected for longer than this value, an alarm is triggered.

Fire Extinguisher Sensitivity

Indicates the degree of detection for the presence or absence of fire extinguishers. The larger the sensitivity setting, the easier it is to detect the corresponding result.

5. Set the arming time and linkage method. Please refer to the [Schedule and Linkage Configuration](#) section.
6. Click *Save*.

Configuring Call-for-Help Detection

This function is used to detect whether someone in the monitored area is calling for help. It can recognize specific call-for-help keywords. Currently, the system supports detection of the following three keywords: "Fire", "Help", and "Put out the fire". When a call-for-help keyword is detected and an alarm is triggered, the configured linkage actions will be executed.

Operating Procedure

1. On the device web client, go to *Configuration* → *Event* → *Smart Event* → *Call-for-Help Detection*.
2. Check *Enable*.
3. Set the detection parameters.

Sensitivity

Higher sensitivity makes it easier to recognize calls and trigger alarms, but may also increase the rate of false detections.

4. Set the arming time and linkage method. Please refer to the [Schedule and Linkage Configuration](#) section.
5. Click *Save*.

Configuring Intrusion Detection

Area Intrusion Detection is used to detect whether a target enters a warning area. This function allows users to set up to 4 quadrilateral warning zones. When a target object enters these zones, the device can generate an alarm signal and perform related linkage actions.

Operating Procedure

1. Go to *Configuration* → *Event* → *Smart Event* → *Intrusion Detection*.
2. Check *Enable*.
3. Draw the maximum and minimum size.
 - 1) Click *Maximum Size / Minimum Size*.
 - 2) Select a point in the preview image as the starting point, hold down the left mouse button and drag arbitrarily until a quadrilateral maximum size filter box / minimum size filter box is drawn.
 - 3) Optional: If you need to redraw the filter box, click *Maximum Size / Minimum Size* again to redraw.When an object enters the warning area and its size is within the range of the maximum and minimum sizes, it can be identified as a target; otherwise, it is not considered a target. This function can improve detection accuracy.
4. Set the warning area.
 - 1) Select a **Warning Area**, click *Detection Area*.
 - 2) In the preview image, click the mouse to select four vertices to draw a quadrilateral detection area.
 - 3) Optional: Click *Clear* to clear the drawn area.
 - 4) Optional: Repeat substeps 1~3 to set up to 4 warning areas.
5. Set the warning parameters.

Time Threshold

Indicates the time a target stays in the warning area after entering. An alarm will be generated if this time is exceeded. The larger the time threshold setting, the longer the target needs to be moving continuously within the detection area to trigger. For example, if set to 0, the alarm is triggered immediately after the target invades the area. The maximum is 10 seconds.

Sensitivity

Indicates the degree to which the target enters the armed area. Sensitivity value = $100 - S1/ST*100$, where S1 is the area of the target entering the armed area, and ST is the actual area of the target. The larger the sensitivity setting, the easier it is to trigger an alarm.

Proportion

This defines the percentage of the target that occupies the user-drawn region. A regional intrusion alarm will be triggered only when the target object exceeds the configured proportion.

Detection Target

Used to specify the detection target. The device will detect the specified target.

6. Set the arming time and linkage method. Please refer to the [Schedule and Linkage Configuration](#) section.
7. Click *Save*.

Configuring Line Intrusion Detection

Line Intrusion Detection is used to detect whether a target crosses a warning line in a specified direction. If a target crosses in the specified direction, it triggers the device to perform linkage actions.

Operating Procedure

1. Go to *Configuration* → *Event* → *Smart Event* → *Line Intrusion Detection*.
2. Check *Enable*.
3. Draw the maximum and minimum size.
 - 1) Click *Maximum Size* or *Minimum Size*.
 - 2) Select a point in the preview image as the starting point, hold down the left mouse button and drag arbitrarily until a quadrilateral maximum size filter box or minimum size filter box is drawn.
 - 3) Optional: If you need to redraw the filter box, click *Maximum Size* or *Minimum Size* again to redraw. When an object enters the warning area and its size is within the range of the maximum and minimum sizes, it can be identified as a target; otherwise, it is not considered a target. This function can improve detection accuracy.
4. Set the warning line.
 - 1) Select a **warning line**, click *Detection Area*, a line segment with an angle will appear in the image.
 - 2) Click to select the line segment, you can drag the vertices to edit the length and position of the line segment, or click and drag the line segment to move it parallelly.
 - 3) Optional: Click *Clear* to clear the drawn area.
 - 4) Optional: Repeat substeps 1~3 to set up to 4 warning areas.
5. Set the rule parameters.

Detection Target

After selecting the detection target, the device will detect the specific target.

Direction

Indicates the direction in which the target crossing the warning line triggers the alarm.

A->B

Indicates that an alarm will be triggered when the target crosses from A to B.

B->A

Indicates that an alarm will be triggered when the target crosses from B to A.

A<->B

Indicates that the target triggers the alarm in both directions.

Sensitivity

Indicates the degree to which the target enters the armed area. Sensitivity value = $100 - S1/ST*100$, where S1 is the area of the target entering the armed area, and ST is the actual area of the target. The larger the sensitivity setting, the easier it is to trigger an alarm.

6. Set the arming time and linkage method. Please refer to the [Schedule and Linkage Configuration](#) section.
7. Click *Save*.

4.4.7 Storage

Recording Schedule

Scheduled recording means automatically executing recording tasks during set time periods.

Operating Procedure

1. Go to *Configuration* → *Storage* → *Schedule Configuration* → *Recording Schedule*.
2. Check *Enable* to activate the recording schedule.

3. Select the recording type.



The following describes recording types that the device may include. The specific selectable recording types are subject to the actual device interface.

Schedule

Indicates recording according to the time configured in the recording schedule.

Motion Detection

Channel recording when a motion detection event occurs.

Alarm

Indicates recording when an alarm input generates an alarm or an alarm event is recognized.

4. Click *Advanced Parameters* to configure parameters.

Overwrite

If *Overwrite* is checked, when the storage is full, the earliest recording files will be overwritten; if not checked, recording will stop when the storage is full.

Pre-Recording Time

Pre-record time before the recording schedule start time point.

Video Delay

Post-record time after the recording schedule end time point.

Bit Stream Types

The stream type for recording storage.



The higher the bitrate selected, the shorter the pre-record time will be.

5. Set the recording schedule time. Please refer to the [Schedule and Linkage Configuration](#) section.

6. Click *Save*.

Storage Management

Used to manage the storage space for video files and snapshots.



The content in Storage Management depends on the actual device. The following describes storage management that the device may support.

Hard Disk Management

View hard disk information and hard disk quotas.

Operating Procedure

1. Go to *Configuration* → *Storage* → *Storage Management* → *Hard Disk Management*.
2. View Disk Number, Capacity, Free Space, Status, Type, Attribute, and Progress.
3. View hard disk quotas, including Picture Capacity, Picture Free Space, Video Capacity, Video Free Space.
4. Set the Snapshot Quota Percentage and Recording Quota Percentage.
5. Click *Save* to complete device restart.

Format SD Card

When using a microSD card for the first time, please log in to the device Web client and format the microSD card.

Prerequisites

Please install the microSD card into the device.

Operating Procedure

1. Go to *Configuration* → *Storage* → *Storage Management* → *Hard Disk Management*.
2. In the detected hard disk list, check the microSD card that needs to be formatted.
3. Configure the snapshot and recording quotas on the disk.
4. Click *Format*.



After formatting, the microSD card status changes from **Unformatted** to **Normal**, indicating that the microSD card can be used normally, and you can view disk capacity, free space, and other information.

5. Click *Save*.

4.4.8 Temperature Measurement

This function is used for real-time temperature monitoring of a location. By configuring temperature measurement parameters or rules, the device will automatically perform temperature measurement and trigger alarms when a target meets the specified parameters or triggers the configured rules.

Configuring Temperature Measurement Parameters

This covers the basic parameter configuration for automatic temperature measurement.

Operating Procedure

1. Go to *Configuration* → *Temperature Measurement* → *Basic Configuration*.
2. Check the *Enable Temperature Measurement* box.
3. Configure the temperature measurement parameters.

Overlay Temperature Information on Stream

When checked, the detected temperature data and measurement frame information will be overlaid.

Maximum Temperature, Minimum Temperature, Average Temperature

When checked, the temperature data (max, min, or average) will be overlaid and displayed on the live view of the thermal imaging channel.

Temperature Unit

Set the unit for temperature measurement.

Temperature Measurement Range

Set the temperature range for the target to be measured.

Algorithm Library Version

View the current version of the temperature measurement algorithm library.

4. Click *Save*.

Normal Temperature Measurement

Normal temperature measurement performs temperature measurement and alarm triggering for the entire scene as a whole.

Operating Procedure

1. Go to *Configuration* → *Temperature Measurement* → *Basic Configuration*, and check the *Enable Temperature Measurement* box.
2. Configure the temperature measurement parameters. For details, please refer to the [Configuring Temperature Measurement Parameters](#) section.
3. Go to *Configuration* → *Temperature Measurement* → *Advanced Configuration*, and select *Normal Mode* as the **configuration mode**.
4. Configure the normal mode parameters.

Emissivity

The emissivity of the temperature measurement target.

Distance

The straight-line distance between the temperature measurement scene and the device.

Pre- Alarm Threshold and Filtering Time

When the detected temperature exceeds the configured pre- alarm threshold and the duration exceeds the filtering time, the device will issue a pre- alarm.

Alarm Threshold and Filtering Time

When the detected temperature exceeds the configured alarm threshold and the duration exceeds the filtering time, the device will issue an alarm.

Pre- Alarm Output and Alarm Output

When a pre- alarm or alarm is triggered, the selected alarm output channel(s) will be activated as linkage actions.

5. Click *Save*.
6. Go to *Configuration* → *Temperature Measurement* → *Linkage Method*, configure the arming schedule and linkage method, and save. For arming schedule settings, please refer to the [Configuring Arming Schedule](#) section; for linkage method settings, please refer to the [Linkage Configuration](#) section.
The live view will display the measured real- time maximum and minimum temperature points along with their temperature readings.

