



Fusion Detection Camera

User Manual

Contents

Chapter 1 Product Introduction	1
1.1 Description	1
1.2 Features	1
1.3 Specification	1
1.4 Product Appearance	4
1.5 Cables	5
Chapter 2 Product Installation	6
2.1 Pre-installation Notes	6
2.2 Device Installation	6
2.3 Installation of Waterproof Tape	8
2.4 Installation of Waterproof Network Port Cover	8
Chapter 3 Operation Instructions	10
3.1 System Connection	10
3.2 Device Activation and Configuration	10
3.2.1 Activation via SADP Software	10
3.2.2 Activation via Browser	12
3.2.3 Activation via Client Software	13
3.3 Login and Logout	16
3.4 Main Interface Description	16
Chapter 4 Network Configuration and Access	18
4.1 Setting Basic Network Parameters	18
4.1.1 Setting TCP/IP	18
4.1.2 Setting Ports	19
4.2 Intranet Access	20
4.3 WAN Dynamic IP Access	21
4.3.1 ISUP Access	21
4.3.2 EZVIZ Cloud Access	21
4.3.3 ONVIF Access	23
4.3.4 SDK Service Access	23
Chapter 5 Live View Configuration	24
5.1 Video Parameters	24
5.2 Transmission Parameter Settings	25
Chapter 6 Video, Audio, and Image Settings	26
6.1 Video Settings	26
6.2 Audio Settings	27
6.2.1 Audio Parameter Settings	28
6.2.2 Voice Intercom Settings	28
6.3 ROI Settings	29
6.4 Image Display Settings	30
6.5 OSD Settings	37
6.6 Privacy Mask	37
6.7 Defective Pixel Correction (DPC)	38

Fusion Detection Camera User Manual

6.8 Picture-in-Picture (PIP)	39
Chapter 7 Schedule and Linkage Configuration	39
7.1 Schedule Configuration	39
7.2 Linkage Configuration	40
7.2.1 Upload to Center	41
7.2.2 Upload to Micro SD Card	41
7.2.3 Linked Audible Alarm	41
7.2.4 Linked Alarm Output	42
7.2.5 Linked Recording	43
Chapter 8 Recording and Capture Configuration	44
8.1 Storage Path Configuration	44
8.2 Recording Configuration	45
8.2.1 Scheduled Recording	45
8.2.2 Manual Recording	46
8.2.3 Video Playback and Download	46
8.3 Capture Configuration	48
8.3.1 Event Capture	48
8.3.2 Live View Capture	49
8.3.3 Playback Capture	49
Chapter 9 Event and Alarm Configuration	50
9.1 Algorithm Mode Configuration	50
9.2 Alarm Configuration	50
9.3 General Event Configuration	51
9.3.1 Motion Detection Configuration	51
9.3.2 Occlusion Alarm Configuration	52
9.3.3 Alarm Input Configuration	53
9.3.4 Abnormal Event Alarm Configuration	54
9.3.5 Alarm Simulation Configuration	55
9.3.6 Indicator Control Configuration	55
9.4 Temperature Measurement Configuration	55
9.4.1 Notes on Temperature Measurement	55
9.4.2 Normal Temperature Measurement and Alarm	56
9.4.3 Expert Temperature Measurement and Alarm	58
9.5 Area Intrusion Detection Configuration	60
9.6 Line Crossing Detection Configuration	61
9.7 Flame Detection Configuration	63
9.8 Smoke Detection Configuration	64
Chapter 10 System Parameter Settings	66
10.1 System Maintenance	66
10.1.1 Device Information	66
10.1.2 Log Query	66
10.1.3 Upgrade and Maintenance	67
10.2 System Configuration	67
10.3 Security Management	69

Fusion Detection Camera User Manual

10.3.1 IP Address Filtering	69
10.3.2 Illegal Login Lockout.....	69
10.3.3 HTTPS	69
10.4 User Management	71
Appendix A Installation and Maintenance.	73
A.1 Lens Maintenance.....	73
A.2 Network Security Maintenance	73
Appendix B Common Material Emissivity Table.	74
Appendix C Product Dimension Drawing.	75

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

Fusion Detection Camera User Manual

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.



- **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.

Chapter 1 Product Introduction

1.1 Description

It is a composite high-performance flame detector that integrates thermal imaging sensor and visual AI intelligent detection. It identifies changes in infrared signals and image characteristics of flames in the monitored area, issues warnings and alarms, and supports networked management and visual verification. This product features smoke and fire alarm functions, identification of fire point locations, and video verification for the monitored area, enabling early fire warning and remote visual verification of fire scenes. It is widely used in key units with fire protection and security needs, such as hospitals, schools (laboratories, libraries, warehouses, archives), museums, Taoist monasteries, banks (ATM rooms, equipment rooms), production safety workshops, indoor substations, new energy facilities, and oil and petrochemical sites (gas stations).

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 high-brightness four-color indicator lights to display the running, fault and alarm status.
- Supports flame detection, coverage: 30 meters (burning object: n-heptane, 0.1 m² fire plate).
- Supports high-temperature and temperature-rise exception detection.
- Supports 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.
- Supports access to Hik-Protect or Hik-Connect APP.
- Supports IR fill light, with maximum range up to 30 meters.
- Supports DC 12~24V (±15%) or PoE power supply, with simple wiring.
- Supports 1 channel of alarm input and 3 channels of alarm output.
- IP67 dust and water resistant.

1.3 Specification

Fusion Detection Camera User Manual

Camera	
Sensor Type	1/2.9" Progressive Scan CMOS
Main Stream	30 fps (2560*1440, 1920*1080, 1280*720)
Max. Resolution	2560*1440
Sub Stream	PAL: 25 fps (704*576, 640*480, 352*288) NTSC: 30 fps (704*480, 640*480, 352*240)
Min. Illumination	Color : 0.01 Lux @(F1.6, AGC ON)
Lens	Horizontal: 78°, Vertical: 40°, Diagonal: 93°
Image Settings	Saturation, brightness, contrast, sharpness, AGC and white balance can be adjusted through the client or browser.
WDR	Digital WDR
Shutter	1/25 ~ 1/100,000 s
Image Enhancement	Backlight compensation, 3D digital noise reduction, Grayscale range adjustment
Main Stream Video Compression Standard	Smart265, Smart264, H.265, H.264
Sub Stream Compression Standard	Smart265, Smart264, H.265, H.264
Video Bitrate	256Kbps ~ 8192Kbps
Intelligent Alarm	Smoke alarm, Fire alarm, temperature management alarm
Protocol	TCP/IP, HTTP, HTTPS, DHCP, DNS, RTP, RTSP, RTCP, NTP, IPv4, UDP
Interface Protocol	ONVIF (PROFILE S, PROFILE G), ISAPI, EZVIZ, SDK
General	One-click restoration, Anti-flicker, Heartbeat, Mirroring, Password protection, Video occlusion, IP address filtering
Storage	Micro SD card (Maximum support 512 GB)
Exception Detection	Motion detection, Obstruction alarm, Hard disk full, Hard disk error, Network disconnection, IP address conflict, Illegal access, Peripheral failure
WEB Configuration	Support web preview, configuration and parameter import/export
IR Range	IR: 30m
Detector	
Image Sensor	Vanadium Oxide (VOx) Microbolometer
Pixel Size	120 ×90
Response Waveband	8~14 μm

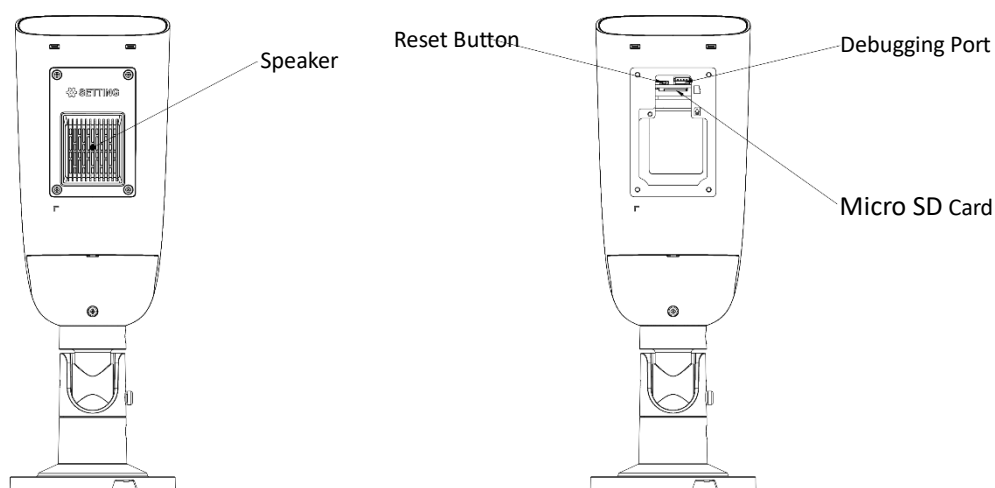
Fusion Detection Camera User Manual

Focal Length of Thermal Imaging Lens	1.2 mm
Thermal Imaging Field of View	90° × 68°
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	-20°C~400°C
Thermography Precision	±8 °C or ±8% of the reading (take the maximum value) (within a distance of 0.3 to 1.5 meters 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	1 way alarm input (Alarm in), 3 ways alarm output (Alarm out)
Ethernet Interface	RJ45 10 M/100 M adaptive Ethernet port × 1
Audio Interface	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, 0.1 m ² fire plate)
Smoke Detection	Yes
General	
Ingress Protection	IP67
Mounting Height	Indoor: higher than 2.5 m Outdoor: higher than 3.5 m
Power Interface Type	DC 12V round head power interface

Fusion Detection Camera User Manual

Power	DC 12V ~ DC 24V, 10W MAX; PoE: 802.3af, CLASS 3 (The power adapter is not included; you will need to configure it yourself). The power source should meet limited power source or PS2 requirements according to IEC 62368-1 standard.
Working Temperature	-20~60°C
Working Humidity	< 95% RH
Dimension (Φ × H)	245.7 mm × 80 mm × 80 mm
Alarm Indicator Light	Red: Alarm Green: Operation indicator light Yellow: Fault Blue: Communication status indicator light
Product Implementation Standard	Q/HKD 054-2024
Power Consumption	Max 10 W
Weight	1.4kg (without packaging)
Installation	Support for hanging and wall mounting

1.4 Product Appearance



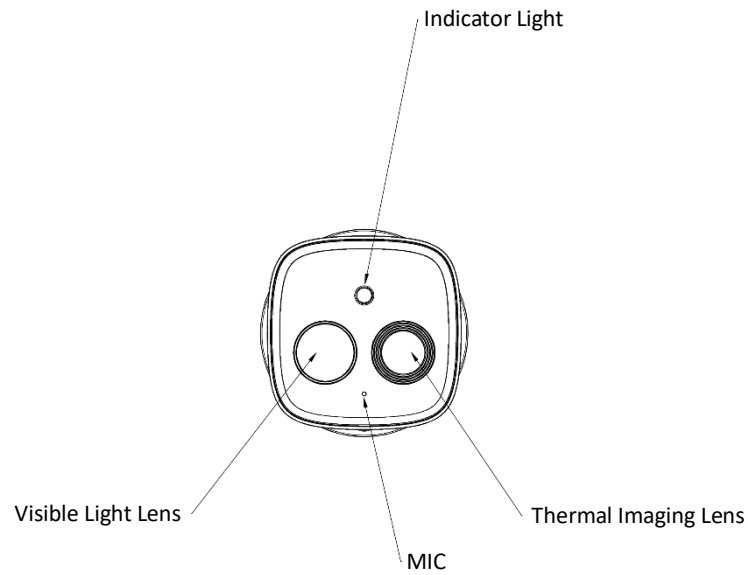


Fig. 1-2 Product Appearance Diagram

1.5 Cables

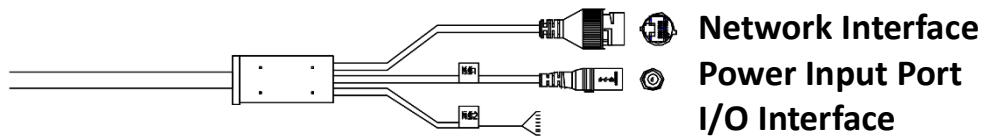


Fig. 1-3 Cables

- Network interface: Network signal output.
- Power input port: Supports DC 12V- DC 24V and PoE power supplies.
- Alarm interface: One channel of alarm input (Alarm in), three channels of alarm output (Alarm out).

Chapter 2 Product Installation

2.1 Pre-installation Notes

- Please install the device in strict accordance with the installation instructions set forth in this guide.
- Prior to installation, please make sure that all the contents in the packaging are intact and that all the parts are present.
- For safety, the device must be securely mounted to a wall or ceiling.
- The installation wall should have a certain thickness and be able to bear at least 4 times the weight of the device and installation accessories.
- For cement walls or ceilings, first install expansion screws (the installation hole positions of the expansion screws need to match the bracket), then install the bracket.
- Self-tapping screws can be used directly when installing the bracket into wooden walls.
- During device installation and use, non-standard wiring operations may affect the device's waterproof performance. Please refer to the content in "2.3 Installation of Waterproof Tape" and "2.4 Installation of Waterproof Network Port Cover" for standard wiring operations.
- 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.

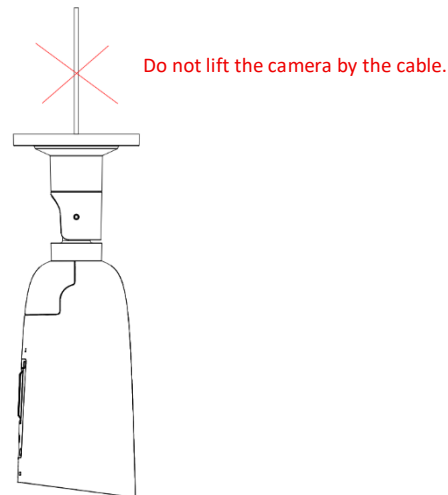


Fig. 2-1 Diagram of Incorrect Handling

2.2 Device Installation

The product comes with a bracket, which supports wall mounting and limited angle adjustments. If other installation forms are required, recommended accessories must be used. Let's take wall mounting as an example.

Wall Mounting

Fusion Detection Camera User Manual

Step 1: Install the Micro SD Card (optional).

- 1) Loosen the screws on the card cover and remove the card cover.
- 2) Insert the Micro SD card correctly in the direction shown in the figure.
- 3) Reinstall the card cover and tighten the screws.

Note: There is a seal ring inside the card cover. Do not leave it out.

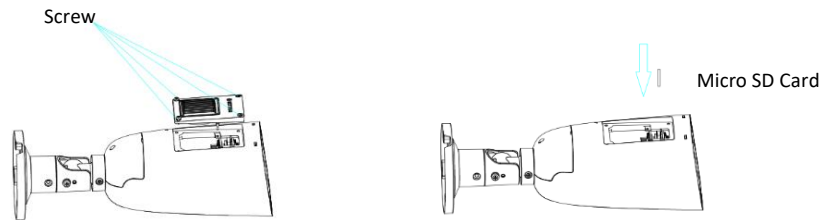


Fig. 2-2 Installing the Micro SD Card

Step 2: Install the device to the mounting surface.

Use three PA4×25 bolts to fix the wall bracket to the wall.

Note: The device can be directly mounted onto a hard wall. For installation on a soft wall, it is necessary to use installation stickers and expansion tubes.

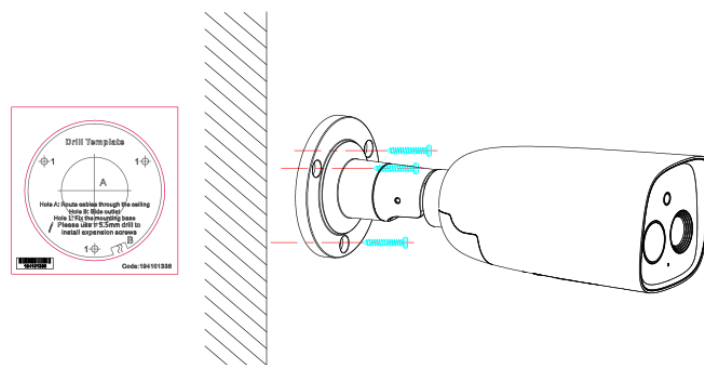


Fig. 2-3 Installing the Device to the Mounting Surface

Step 3: Arrange and connect the detector's power cable, network cable, and other cables, and perform insulation and waterproofing treatments properly (specific methods can be found in the "Installation of Waterproof Tape" and "Installation of Waterproof Network Port Cover" sections).

Step 4: Adjust the bracket to position the device at the desired angle.

Adjust the angle by loosening the corresponding adjustment screws on the bracket. Once the desired field of view for monitoring is achieved, tighten the screws to complete the installation.

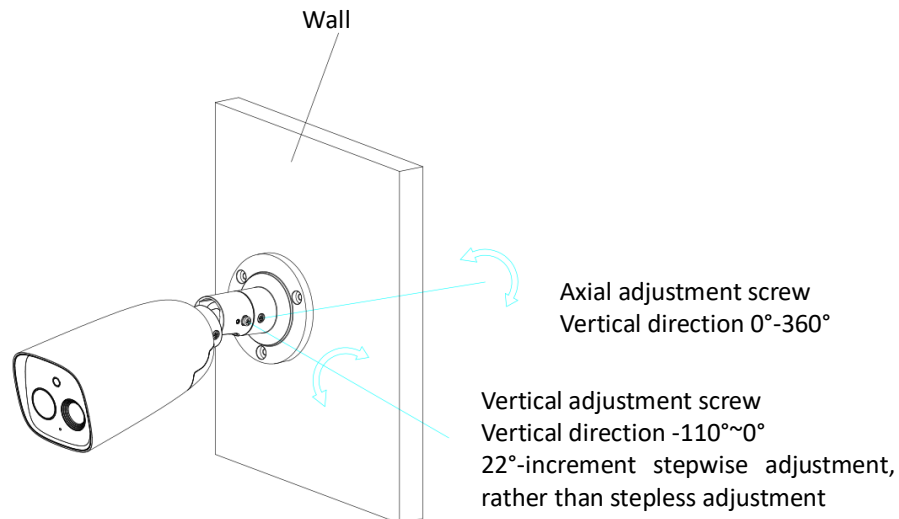


Fig. 2-4 Adjusting the Bracket

2.3 Installation of Waterproof Tape

Some devices already have waterproof tape on them. The instructions for installing waterproof tape are as follows.

Step 1: Please remove the release paper from the back of the supplied waterproof tape.

Step 2: Stretch both ends of the waterproof tape to about twice the initial length.

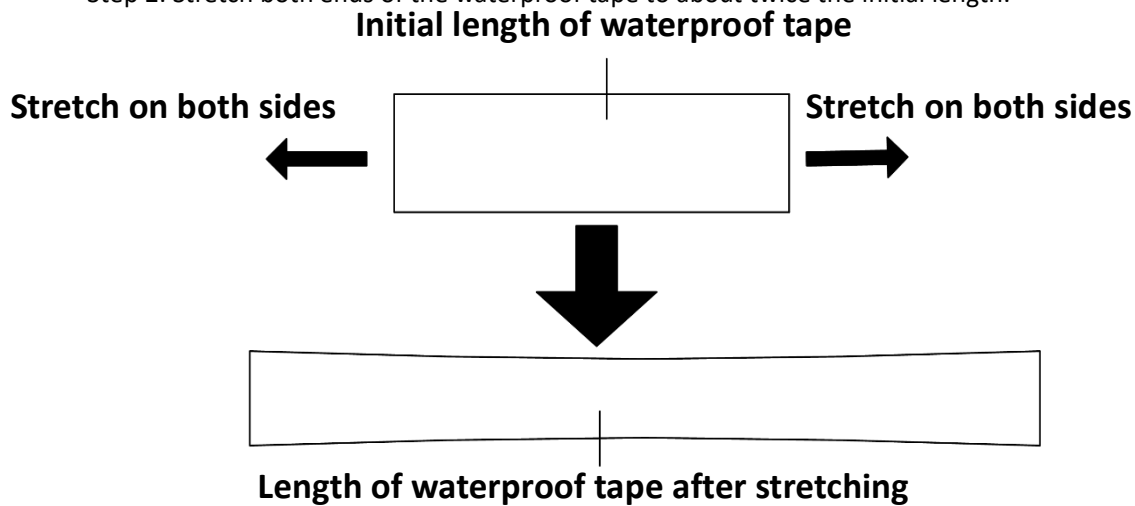


Fig. 2-5 Stretching Waterproof Tape

2.4 Installation of Waterproof Network Port Cover

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.

Step 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.

Step 2: Insert the waterproof rubber ring into the waterproof cap to enhance sealing performance.

Step 3: Terminate the network cable with a crystal head and place the rubber O-ring on the device's network port.

Step 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.

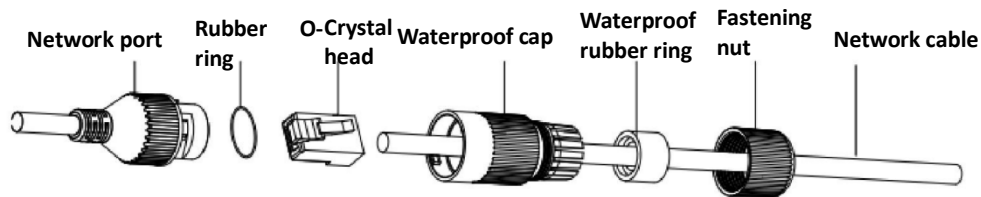


Fig. 2-6 Installing the Waterproof Network Port Cover

Chapter 3 Operation Instructions

3.1 System Connection



- If you connect the product to the Internet, you do so at your own risk. Risks include, but are not limited to, possible cyber-attacks, hacker attacks, viral infections, and so on. Our company shall not be liable for any product malfunction, information leakage, etc., caused by these attacks. However, our company will provide relevant technical support in a timely manner.
 - To ensure the network security of the device, we suggest you perform regular network security evaluations and maintenance on the network equipment system. Our company can provide related professional technical services.
-

After successfully installing the device, you will need to configure the functions and parameters. This can be done through a browser. Before configuration, please confirm that the device and computer are connected and that the device requiring configuration can be accessed.

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 Activation 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.



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

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

Fusion Detection Camera User Manual

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”, as shown in the figure.

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.

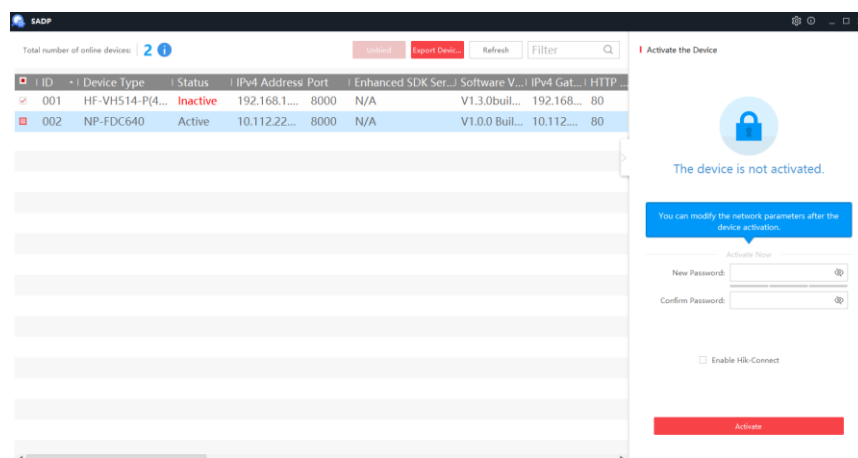


Fig. 3-1 Activating the Device

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.

Fusion Detection Camera User Manual

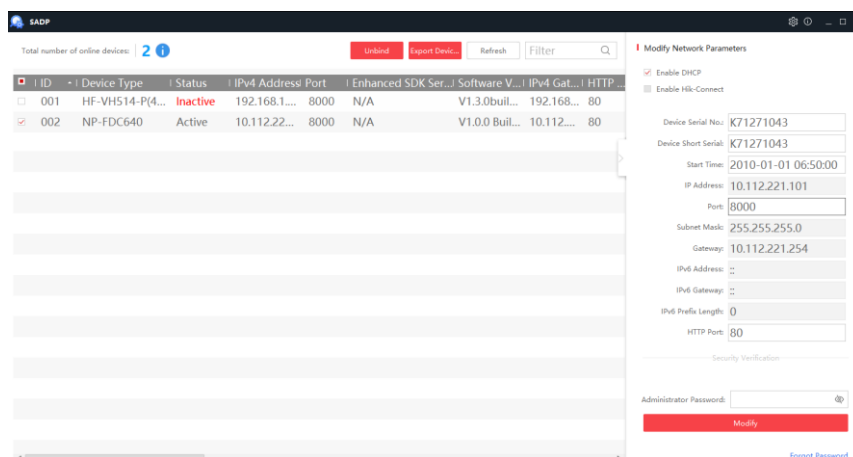


Fig. 3-2 Modifying Device Information



- 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 Activation 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.



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.

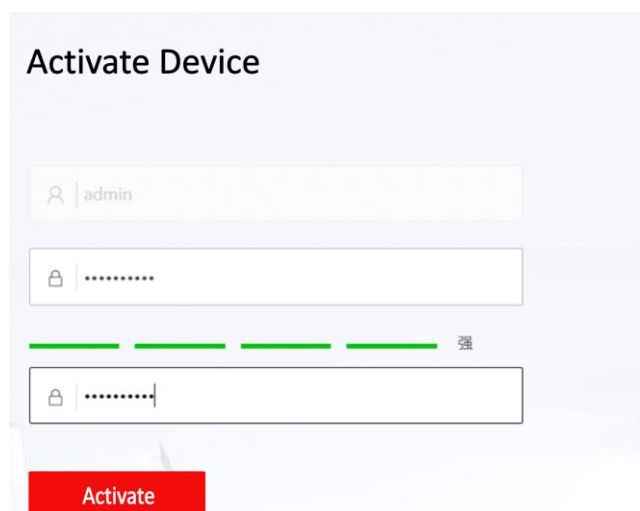


Fig. 3-3 Activation Interface on Browser

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 Configuration - TCP/IP” interface. For specific operations, please refer to the configuration instructions under “Chapter 5 Network Configuration and Access”.

3.2.3 Activation 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

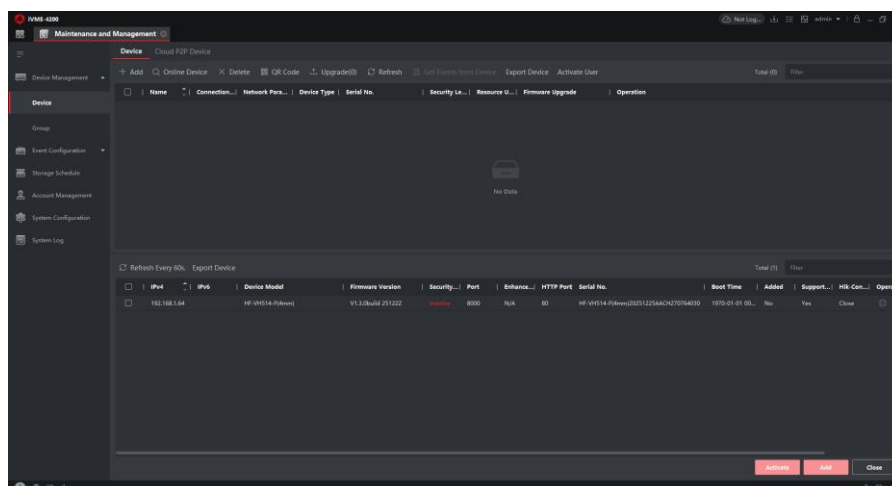


Fig. 3-4 Device List

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.

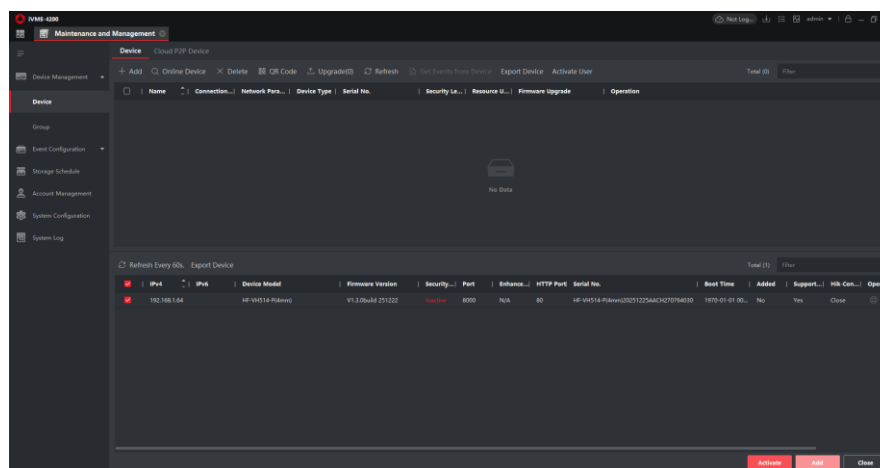


Fig. 3-5 Selected Device Row

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



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

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".



Note

- 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 Login and Logout

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.



Note

- 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 view the device's operating instructions.

Exit System

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

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 Network Configuration and Access

This chapter introduces basic network parameters and device network connections, enabling access to the device over the network.

4.1 Setting Basic Network Parameters

This section introduces the basic parameters that need to be set when the device is connected to the network.

4.1.1 Setting TCP/IP

Step 1: Select “Configuration → Network → Network Configuration”.

Step 2: Set the basic parameters for the device to access the network.

- Network card type: Select according to the network environment.
- There are two ways to set the IPv4 address:
 - Manually fill in the device IPv4 address, IPv4 subnet mask, IPv4 default gateway, and other LAN parameter information.



Note

When filling in the IPv4 address, click [Test] to confirm if the IP address is available, then click "Save" after filling it in.

- Check “Obtain Automatically” to allow the device to automatically obtain network addresses and related network parameters.
- The “MTU” item allows for the setting of the Maximum Transmission Unit, which refers to the largest data packet that can be transmitted in a TCP/UDP protocol network transmission.
- Set DNS Server: Set the device’s DNS server. After the device has a correct and available server address set, the domain name-based access will function properly.

TCP/IP

NIC Type

Self-Adaption

DHCP

☐

* Device IPv4 Address

10.11.51.203

Test

* IPv4 Subnet Mask

255.255.255.0

IPv4 Default Gateway

10.11.51.254

MAC Address

a4:d5:c2:c2:4c:30

* MTU

1500

DNS Server Configuration

Preferred DNS Server

114.114.114.114

Alternate DNS Server

223.5.5.5

Save

Fig. 4-1 TCP/IP Settings

Step 3: Click “Save” after modifying the parameters.

4.1.2 Setting Ports

Step 1: Select “Configuration → Network → Network Service” to set the device’s port parameters. When the device cannot be accessed over the network due to port conflicts, you can modify the device ports.



Do not modify the default port parameters arbitrarily; when it is necessary to modify the port number due to a port conflict, please modify the following information accordingly.

- HTTP Port: The port is used for browser access. 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 to access the device.
- HTTPS Port: When the port is used for browser access, certificate verification is required.
- RTSP Port: The port is used for Real-Time Transport Protocol.

Fusion Detection Camera User Manual

HTTP(S) RTSP

HTTP

* HTTP Port 80

HTTPS

Enable ☒

Please confirm whether the TLS version that the client needs is enabled. [TLS Settings](#)

* HTTPS Port 443

Certificate Management

Server Certificate Without certificate.

Install

Save

HTTP(S) **RTSP**

* Port No. 554

RTSP Authentication

Authentication Mode digest/basic

Save

Fig. 4-2 Port Settings

Step 2: Click “Save” after modifying the parameters.

4.2 Intranet Access

The device is connected to the intranet via a network cable, allowing intranet hosts to access the device. This section takes browser access as an example for explanation.

Step 1: Refer to “4.1.1 Setting TCP/IP” to set the device’s intranet IP address, subnet mask, gateway, and other parameters.

Step 2: Enter the device’s IP address in the browser, then the login screen will pop up. Enter the username and password.



Note

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.

Step 3: Click “Login”.

- After successfully logging into the device, click “Help” to get the online operation guide.
- When entering the device’s main interface, click "Logout" to safely exit the system.

4.3 WAN Dynamic IP Access

4.3.1 ISUP Access

ISUP access refers to registering the device with the ISUP platform by following the platform's relevant technical specifications, thus enabling functions such as remote real-time video streaming, transmission, storage, and management over a broadband network.

Step 1: Go to "Configuration → Network → Platform Access → ISUP" and check "Enable".

Step 2: Set ISUP related parameters according to the ISUP protocol.

ISUP Hik-Connect ONVIF SDK Service

Enable ☐

Protocol Version ISUP5.0

*Server Address 0.0.0.0

*Port No. 7660

*Device ID GK9145230

*Secret Key

Registration Status Offline

Save

Fig. 4-3 ISUP Platform Parameters

Step 3: Click "Save" to complete the setup process.

Step 4: Log in to the ISUP platform for access.



Note

After successfully saving the settings, it is recommended to refresh the web page or restart the device to check the "Registration Status" and see if the device has been successfully registered.

4.3.2 EZVIZ Cloud Access

EZVIZ Cloud is a micro-video service platform under EZVIZ. Devices that support EZVIZ Cloud access can be registered and added to the EZVIZ Cloud platform, so that it can be accessed via EZVIZ Cloud. This section describes how to enable EZVIZ Cloud access using a browser.

Fusion Detection Camera User Manual



Note

- If you need to access the device via the EZVIZ Cloud Video APP and the client software, please download and install the software in advance.
- The availability of EZVIZ Cloud function depends on the device model. Please refer to the actual device for specific capabilities.

Step 1: Go to "Configuration → Network → Platform Access → EZVIZ Cloud" and check "Enable".

Step 2: Set the platform access method.

The device will automatically assign a server address based on the server in nearest region.

Step 3: Set the verification code.

Some devices require the setting of a verification code for the first use. You can set the verification code according to the prompts on the interface.



Note

The verification code must consist of 6 to 12 alphanumeric characters, case-sensitive. For device security, it is recommended to set a combination of uppercase letters, lowercase letters, and numbers with more than 8 characters.

ISUP **Hik-Connect** ONVIF SDK Service

Enable ☐

*Server Address litedev.hik-connect.com

Registration Status ✖ Offline Refresh

*Verification Code

[Create a verification code.](#)

Save

Fig. 4-4 EZVIZ Cloud Platform Parameters

Step 4: Click "Save". The "Registration Status" displayed as "Online" indicates that the device has been successfully registered to the EZVIZ Cloud platform.

Step 5: Configure EZVIZ Cloud access.

- Access via EZVIZ Cloud Video APP
 1. Open the EZVIZ Cloud Video APP and register for an EZVIZ Cloud account.
 2. Click the "+" icon in the upper right corner of the EZVIZ Cloud Video APP to add a device.
 - Scan the QR code on the device body or in the user manual to add the device.
 - Click in the upper right corner of the software and manually enter the serial number on the device label to add the device.
 3. Select a non-EZVIZ device, and connect the device to EZVIZ Cloud according to the instructions on the APP screen.
 4. Go to the live view section of the software, double-click to open the channel for access.



Note

- If the device and router are connected wirelessly, click "wireless device" to complete the Wi-Fi connection, then add the device according to the instructions on the APP screen.
 - The addition and configuration operations must be completed within 3 minutes after the device is powered on. Otherwise, you need to restart the device and repeat the operation.
-

- Access via EZVIZ Cloud website

Log in to the EZVIZ Cloud website via a browser, add the EZVIZ Cloud device, click "Live View", and open the channel for access.

- Access via client software

1. Go to "Control Panel → Device Management" in the client software.
2. Select "EZVIZ Cloud Device", click "Login", and register an EZVIZ Cloud account.
3. Click "Main Live View", double-click to open the channel for access.

4.3.3 ONVIF Access

When you need to connect the device via ONVIF protocol, go to "Configuration → Network → Platform Access → ONVIF", check "Enable", and click "Save" to complete the settings.



Note

ONVIF protocol only supports the addition of devices using 264 encoding.

4.3.4 SDK Service Access

By calling the interfaces provided by SDK, efficient device-platform integration can be achieved.

Step 1: Go to "Configuration → Network → Platform Access → SDK Service".

Step 2: Set SDK service related parameters.

- SDK Protocol Authentication Mode: Compatible mode or secure mode can be selected.
- Enter the port number.

Step 3: Click "Save" to complete the setup process.

Chapter 5 Live View Configuration

This chapter introduces the adjustment of live view parameters and transmission parameters under live view of the device.

5.1 Video Parameters

Click the "Live View" tab on the main interface to enter the device's "Live View" screen.

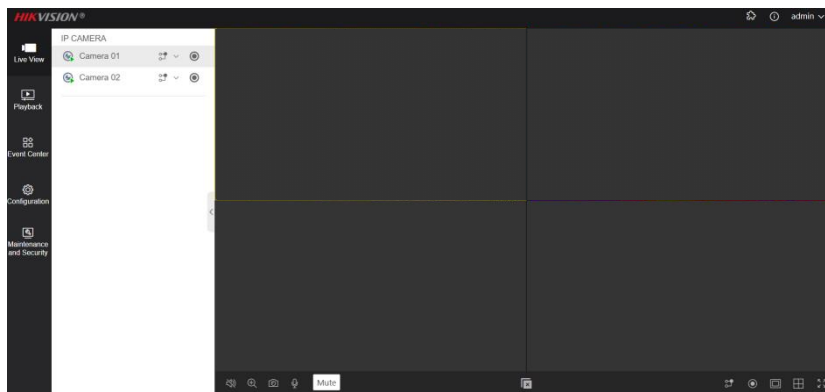


Fig. 5-1 Live View Interface

- Channel Selection: Camera01 is the visible light channel, while Camera02 is the thermal imaging channel.
- Mute : Click this button to turn off the sound.
- Digital Zoom In :
 - If enabled, the button will change to ""; if you click this button again, digital zoom in will be disabled. When the system enables the digital zoom-in function, the following operations can be performed:
 - Hold down the left mouse button and drag to the lower right (upper right) to draw a rectangular area, then the device will move the center of the selected area to the center of the video and zoom in for a close view.
 - Hold down the left mouse button and drag to the upper left (lower left) to draw a rectangular area, then the device will move the center of the selected area to the center of the video and zoom out for wider view.
- Capture : Click this button to capture images.
- Start Intercom : Click this button to start intercom. You need to download and install the web plugin.
- Silence : Click this button to eliminate the sound.
- Start Live view : Click this button to start previewing images.
- Stop Live view : Click this button to stop previewing images.
- Stream : This indicates the main stream and sub-stream respectively; the main stream is the high-definition stream, while the sub-stream is the standard-definition stream.
- Start Recording : Click this button to start recording all screens.
- Screen Size : You can choose 4:3, 16:9, original ratio, and adaptive.

- Split Screen : You can choose from four modes: 1*1, 2*2, 1*2, and 2*1.
- Full Screen : Click this button to preview the image in full screen, and the menu information will be hidden. Press ESC to exit full screen.

5.2 Transmission Parameter Settings

During live view, the preview image may be unstable due to network environment influences. Under different network conditions, this problem can be alleviated by setting transmission protocols and playback parameters.

Step 1: Go to "Configuration → Local", select playback parameters, as shown in the playback parameter settings.

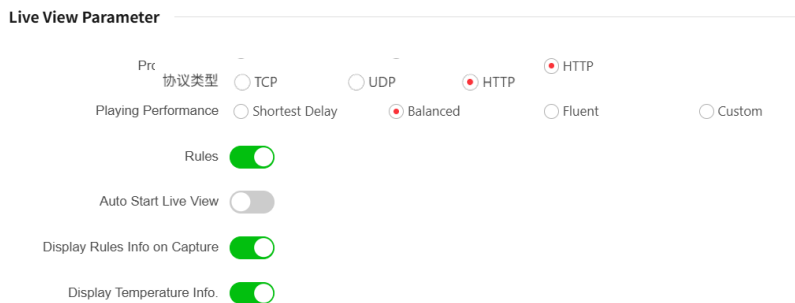


Fig. 5-2 Setting Playback Parameters

Step 2: Set parameters affecting video transmission.

- Transmission Protocol: TCP, UDP, and HTTP protocols are supported.
- Playback Parameters:
 - Shortest Delay: It prioritizes real-time video preview, but may affect video fluency.
 - Balanced: It enables the device to balance both the real-time performance and fluency of video preview.
 - Fluent: It enables the device to prioritize video preview fluency. In case of poor network connection, even setting to "fluent" may not guarantee smooth video preview.
 - Custom: It supports custom frame rate settings.
- Rules: If enabled, rule information will be displayed on the preview image.
- Auto Start Live View: If "Enable" is selected, live view will start automatically. This requires good host performance and a stable network environment.
- Display Rules Info on Capture: If enabled, rule information will be added to the alarm image capture data.
- Display Temperature Info: If enabled, temperature measurement information will be displayed on the preview image.

Step 3: Click "Save".

Chapter 6 Video, Audio, and Image Settings

This chapter introduces the settings of the device's video, audio, and image parameters.

6.1 Video Settings

Select "Configuration → Video & Audio → Video" to adjust video parameters such as stream type, video type, and resolution.

Caution

When the sum of all device connections exceeds the maximum bitrate, the actual bitrate will decrease to ensure normal connection.

- **Channel No.:** Select the channel number that requires the setting of parameters. Video parameters can be set separately for the two channels.
- **Stream Type:** Video parameters for the main stream (scheduled) and sub-stream (network transmission) can be set. The main stream is used for high-definition storage and preview, while the sub-stream is used for standard-definition storage and preview when network bandwidth is insufficient.
- **Video Type:** Video stream and composite stream are available for you to choose.
- **Resolution:** It can be selected according to the customer's requirements for video clarity. The higher the resolution, the higher the network bandwidth requirement.
- **Bitrate Type and Max. Bitrate:** Bitrate type can be set to variable bitrate or constant bitrate. Constant bitrate indicates that the bitrate is maintained at the average bitrate for transmission. It offers fast compression speed but may cause video mosaic artifacts. Variable bitrate indicates dynamic adjustment of bitrate within the defined upper limit of bitrate. While the compression speed is relatively slow, it ensures picture clarity in complex scenes.
- **Image Quality.** When the bitrate type is variable bitrate, the image quality can be set. Selection can be made according to the customer's requirements for image clarity. The higher the image quality, the higher the network bandwidth requirement.
- **Video Frame Rate:** It represents the number of frames per second of the video. You can set it according to the actual bandwidth. The higher the video frame rate, the higher the required bandwidth and storage space.
- **Video Encoding:** All streams can be set to H.264 or H.265 encoding.
- **Smart264/Smart265:** They refer to two ways of Smart encoding.

If Smart264/Smart265 is enabled, in typical scenarios, the average bitrate can save up to 50% of storage space compared to H.264/H.265 bitrate while ensuring image quality, further saving users storage costs.

When the stream type is main stream, both the width and height of the resolution are greater than 512K, and the video encoding is set to H.264/H.265, you can choose "Enable" or "Disable" Smart264/Smart265. A prompt will appear when the status is

switched, and the device needs to be restarted for the change to take effect.

- Below the max. bitrate, an average bitrate field will be displayed. The system automatically adjusts the recommended value of the average bitrate based on the max. bitrate parameter. Users can use this data to calculate storage space or manually set the average bitrate parameter, which must not exceed the max. bitrate.

Manual adjustment of the average bitrate depends on the complexity of the actual monitored scene. If the current scene is complex and the image quality is poor at the default average bitrate, please manually increase the average bitrate value.

- Bitrate type will automatically switch to variable bitrate and cannot be modified.

- Parameters such as image quality, I-frame interval, encoding complexity, and SVC become non-editable.



Note

- In case of preview and playback issues caused by insufficient compatibility with certain player versions, please update to the latest player version.
 - Smart264/Smart265 automatically adjusts bitrate allocation based on scene conditions.
 - After Smart264/Smart265 is enabled, some functions may become unavailable. Please refer to the actual device interface.
-

- 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: It refers to 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 is only applicable to devices using H.264 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: It supports displaying intelligent information through video and playback library.
 - Playback Library: It indicates that videos are playable using the manufacturer's dedicated player.
 - Video: It indicates that videos are playable using other players.

6.2 Audio Settings

Under audio settings, you can configure various basic audio parameters and voice intercom.

6.2.1 Audio Parameter Settings

Audio quality can be optimized by adjusting basic audio parameters.

Step 1: Go to "Configuration → Video & Audio → Audio", as shown in the figure.



The screenshot shows a configuration interface with three tabs: 'Video', 'Audio' (highlighted in red), and 'ROI'. Under the 'Audio' tab, there are three settings: 'Channel' with a value of '1', 'Audio Input' with a dropdown menu showing 'MicIn', and 'Audio Encoding' with a dropdown menu showing 'G.711ulaw'. A red 'Save' button is located at the bottom of the settings area.

Fig. 6-1 Audio Parameters

Step 2: Set audio parameters.

- Audio Input: It represents the audio input method. The default is the built-in MIC input.
- Audio Encoding: You can select the supported audio encoding type based on the system storage, platform, or customer requirements.

Step 3: After completing the setup, click "Save".

6.2.2 Voice Intercom Settings

When you need to communicate with people shown in the video image or issue a warning, you can enable the voice intercom function on the live view page.



Please ensure that the pickup, microphone, or speaker connected to the device functions normally.

Step 1: Go to "Live View".

Step 2: Click "🎤" and select "🎤" to enable intercom. The button will then change to "🗣️". You can now intercom with the device.

Step 3: Adjust the sound volume: Click "🔊" and select "🔊" to enable sound output. The button will then change to "🔊". Drag the progress bar to the right to increase the volume, or to the left to decrease it. Dragging it to the far left will mute the audio, and clicking the button again will stop sound output.

Step 4: Click the "🗣️" button again to stop intercom.

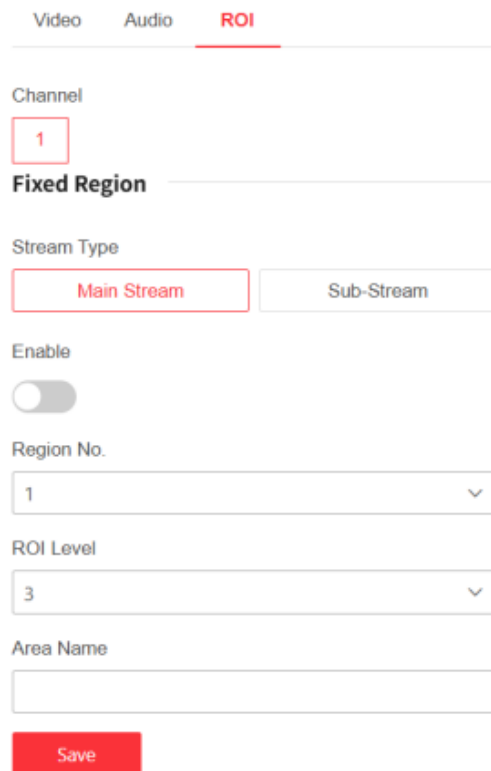
6.3 ROI Settings

Note

The ROI function depends on the specific device model. It is only available under H.264 encoding, and other encodings do not support the ROI function.

The ROI function is designed for Region of Interest encoding. After the ROI function is enabled, the device will improve the image encoding quality of the selected area, so as to ensure the image quality of that area. When the "Fixed Region" mode is enabled, the encoding quality of the selected region will be enhanced, and the encoding quality outside the selected region will be reduced, thereby highlighting the image effect within the selected region. The specific setup steps are as follows.

Step 1: Go to "Configuration → Video & Audio → ROI" to enter the ROI setting interface, as shown in the figure.



The screenshot shows the 'ROI' configuration page. At the top, there are tabs for 'Video', 'Audio', and 'ROI', with 'ROI' being the active tab. Below the tabs, the 'Channel' is set to '1'. The 'Fixed Region' section is expanded. Under 'Stream Type', there are two buttons: 'Main Stream' (highlighted in red) and 'Sub-Stream'. The 'Enable' toggle switch is currently turned off. The 'Region No.' dropdown menu is set to '1'. The 'ROI Level' dropdown menu is set to '3'. There is an empty text field for 'Area Name'. At the bottom, there is a red 'Save' button.

Fig. 6-2 ROI Setting Interface

Step 2: Set stream type: You can choose between the main stream and the sub stream.

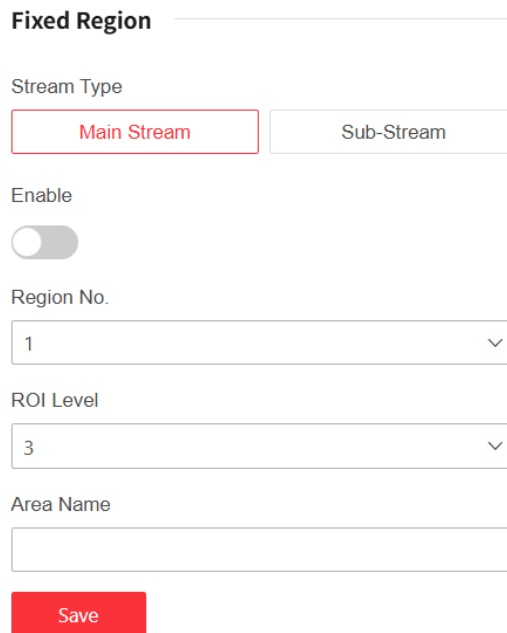
Step 3: Frame the fixed region.

Note

The number of fixed regions supported varies by model. Please refer to the actual device.

Fusion Detection Camera User Manual

The number of fixed regions supported varies by model. Please refer to the actual device. In "Fixed Region" mode, you need to draw an area block. Select the region number to be drawn, and click "Draw Area" to draw an area block on the video image, as shown in the figure.



The figure shows a web-based configuration interface for a "Fixed Region". It includes a title "Fixed Region", a "Stream Type" section with "Main Stream" (highlighted in red) and "Sub-Stream" buttons, an "Enable" toggle switch (currently off), a "Region No." dropdown menu set to "1", an "ROI Level" dropdown menu set to "3", an "Area Name" text input field, and a red "Save" button at the bottom.

Fig. 6-3 Drawing Area Blocks

Step 4: After completing the drawing, set the name and enhancement level of the area block, then click "Save".

The higher the enhancement level is set, the more prominent the image effect in the selected area will be. Other area blocks can be drawn in the same way.

Step 5: Check "Enable" fixed region to enable the fixed region ROI function.

6.4 Image Display Settings

Display settings are used to set the image quality of the video display.



- The device can configure parameters for the two channels separately. The parameters for the two channels are slightly different, and the following will introduce the different parameter items individually.
- The specific parameters displayed depend on the specific device model. Please refer to the actual interface.
- Devices with a laser function can only use the function in "Night" mode.

Step 1: Select "Configuration → Image → Display Settings". The setting interface is shown in the figure.

Fusion Detection Camera User Manual

Step 2: Select a channel. Channel 1 is the visible light channel, while Channel 2 is the thermal imaging channel.

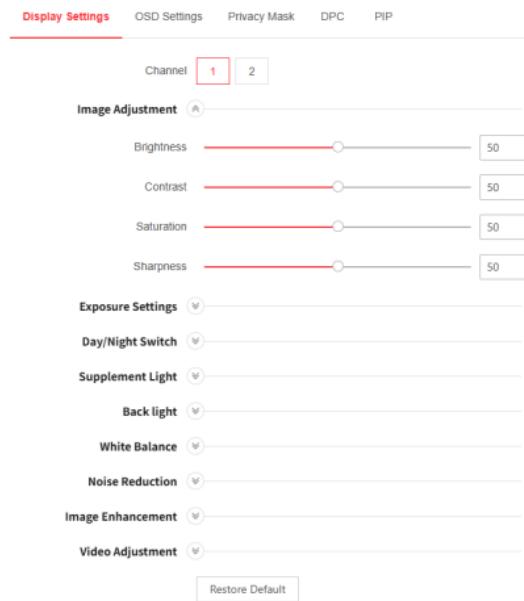


Fig. 6-4 Display Parameter Settings Interface

Step 3: Set display parameters.

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.

- Visible light channel

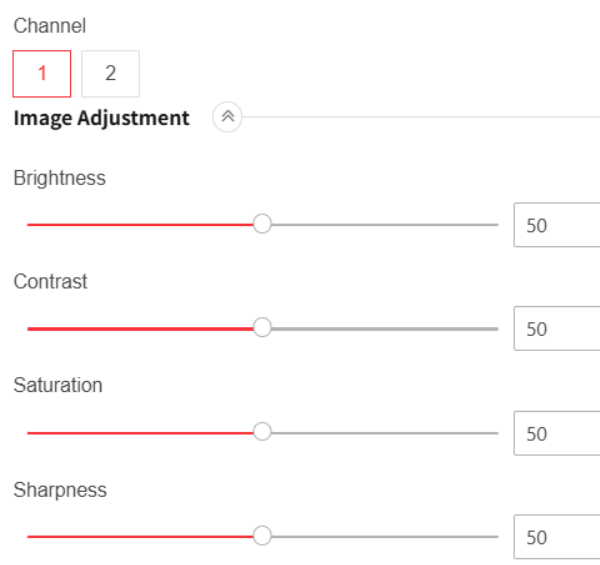


Fig. 6-5 Visible Light Image Adjustment

- Thermal imaging channel
 - Manual Correction: Manually click "Correct" to optimize the image once.

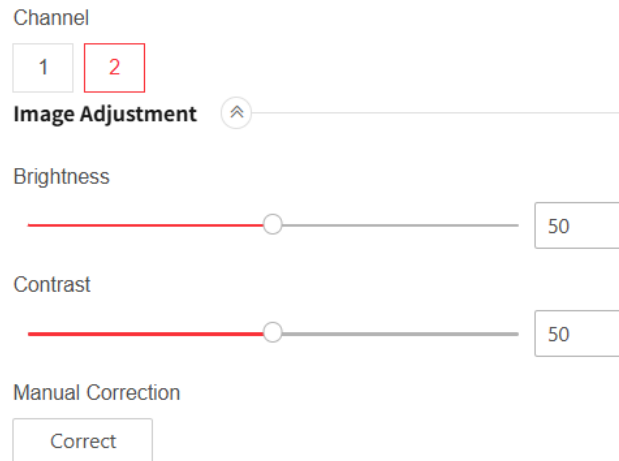


Fig. 6-6 Thermal Image Adjustment



Note

During background correction and manual correction, there may be a brief video freeze, which is normal.

Exposure Parameters (available for visible light channel)

- Iris Type: Fixed.
- Exposure Time: You can select a different exposure time from a drop-down menu.



Fig. 6-7 Exposure Mode

Day/Night Switch (available for visible light channel)



Note

The device supports scheduled mode, meaning that after setting the start time and end time for the scheduled mode, the day/night switch mode will be set to "Day" during this period, and to "Night" at all other times.

Under Day/Night Switch, you can set day/night switch parameters.

The image shows a configuration panel for the Day/Night Switch. At the top, the title 'Day/Night Switch' is followed by an upward-pointing arrow icon. Below this, there are three settings:

- Day/Night Switch:** A dropdown menu currently showing 'Auto'.
- Sensitivity:** A dropdown menu currently showing '4', with an information icon (i) to its left.
- Filtering Time:** A slider control with a circular knob on the left and a numeric input box on the right showing the value '5'.

Fig. 6-8 Day/Night Switch

- **Day/Night Switch:** It can be set to Auto, Day, Night, or Scheduled Switch. When set to Scheduled Switch, the start time and end time for Day mode need to be set. When set to Auto, the day and night scenes will switch automatically; when set to Day or Night, the system will be forced to switch to Day or Night Mode.
- **Sensitivity:** When Day/Night Switch is set to "Auto", the sensitivity can be set. A higher sensitivity makes day/night switch easier, while a lower sensitivity makes it more difficult.
- **Filtering Time:** When Day/Night Switch is set to "Auto", the filtering time can be set. Filtering time refers to the delay duration when switching from day to night. If set to 5, it means that the system will perform a continuous detection for 5 seconds before switching to prevent false switching.

Supplement Light Mode (available for visible light channel)

Caution

Supplement light related parameters are only applicable to devices with a supplement light function. In case of the absence of the function, relevant parameters will not be displayed.

- **Smart Supplement Light**
If enabled, it can alleviate image overexposure caused by supplement light.
- **Supplement Light Mode**
You may select IR Supplement Light.
- **Light Brightness Control**
It can be set to Auto or Manual adjustment. When manual adjustment mode is selected, the IR light value can be set manually.

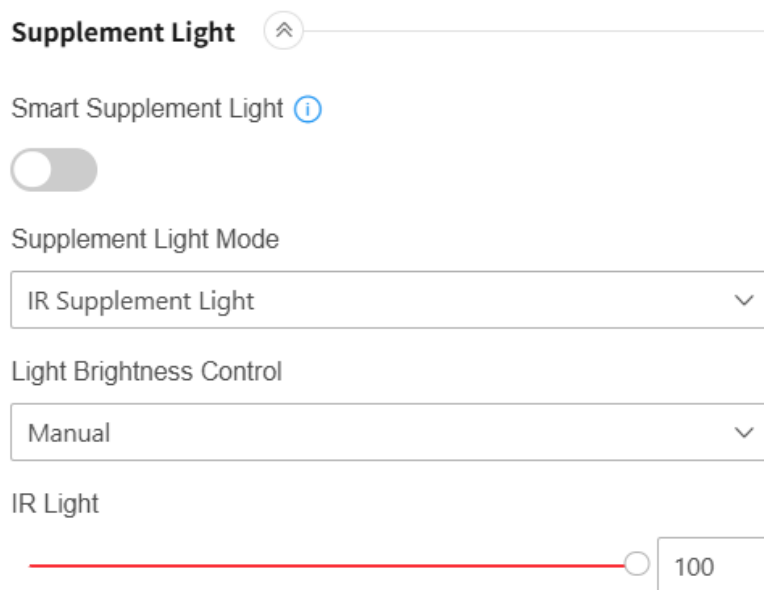


Fig. 5-9 Supplement Light Mode

Back Light Parameters (available for visible light channel)

Backlight parameters include Back Light Compensation Area (BLC Area) , Wide Dynamic Range (WDR), and High Light Compensation (HLC).

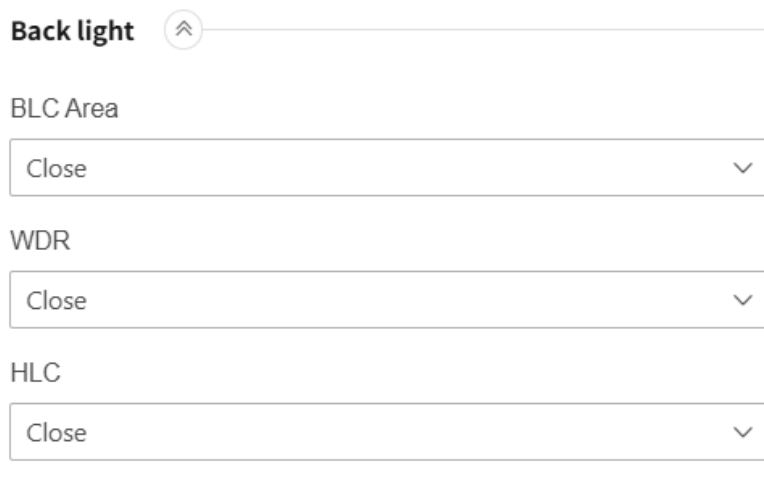


Fig. 6-10 Back Light Parameters

- BLC Area: When the image background is relatively bright, you can enable BLC Area to effectively solve the problem of dark foreground objects caused by underexposure.
- WDR: 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 image, you can enable the WDR function and adjust the level to see the video image clearly.
- HLC: When the video image has overexposed bright areas and underexposed dark areas, you can enable HLC to weaken the bright areas and brighten the dark areas, thus achieving light balance for the overall image.



Note

WDR is mutually exclusive with BLC Area and HLC.

White Balance (available for visible light channel)

When the device operates in different environments, the performance of the video display will vary. White balance can be used to adjust the video image. White Balance can be set to AWB (Auto White Balance), Indoor, Outdoor, MWB (Manual White Balance), Fluorescent Light, or Sodium Lamp, but the specific settings depend on the core module.

Please set White Balance according to the environment where the device is located. For example, if the device operates indoors, you can select "Indoor" white balance mode, and so on.

Noise Reduction Mode

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.

- Noise Reduction Mode

- Normal Mode: You can drag the progress bar or set the noise reduction level value.
- Expert Mode: You can adjust through two dimensions: spatial noise reduction and temporal noise reduction.

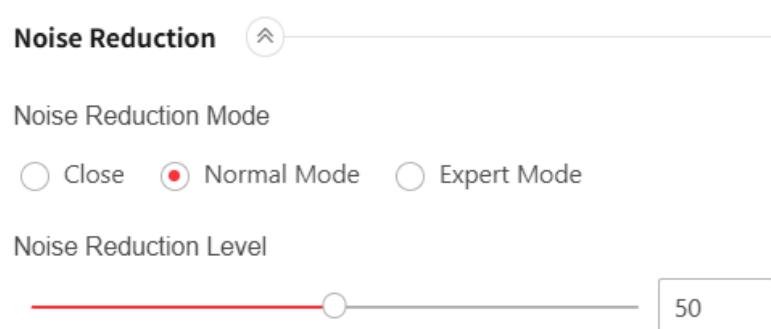


Fig. 6-11 Noise Reduction Mode

Image Enhancement

- Visible light channel

- Gray Scale: You can select gray scale in the drop-down menu.

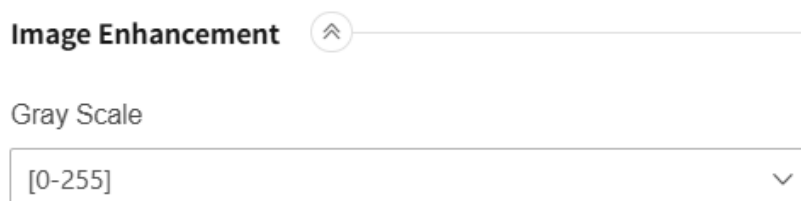


Fig. 6-12 Visible Light Image Enhancement

- Thermal imaging channel

- Palettes: Multiple pseudo-color modes are supported. The target will be highlighted in

pseudo-color for quick identification by users.

- DDE (Digital Detail Enhancement): It allows for manual enhancement of image details. A higher level will result in better details, but also more noise.

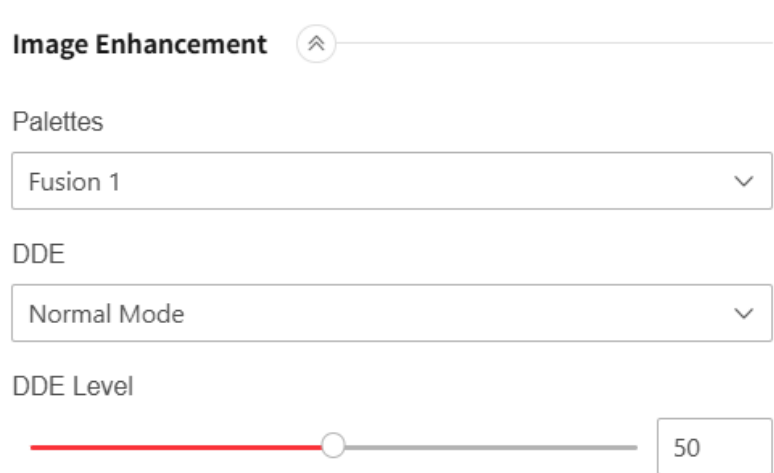


Fig. 6-13 Thermal Image Enhancement

Video Adjustment

- Mirror: You can mirror the video as needed, choose left/right, up/down, and center mirror adjustments, or turn off mirroring. When the image is inverted, you can flip the image through this menu. After the mirror mode is enabled, platform recording will be briefly interrupted.
- Video Standard (available for visible light channel only): PAL (50HZ).
- Digital Zoom (available for thermal imaging channel only): You can set the zoom ratio or disable this function as needed.
- Restore Default: Click "Restore Default" to restore image parameters to their initial state.

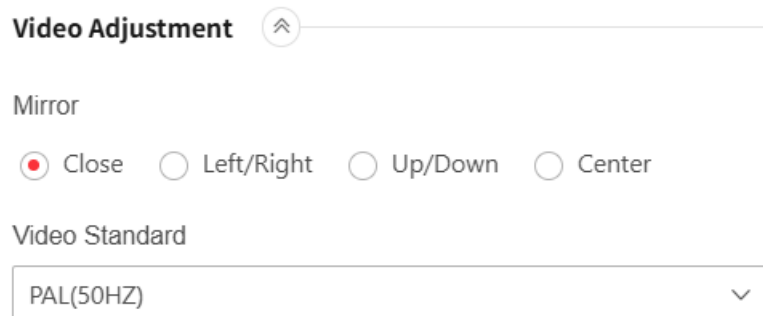


Fig. 6-14 Visible Light Video Adjustment

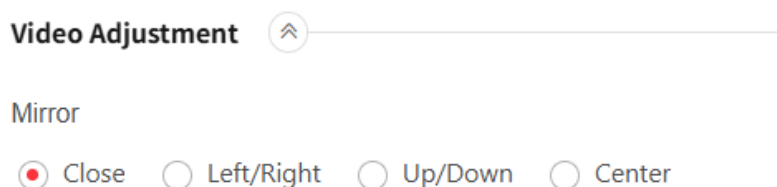


Fig. 6-15 Thermal Imaging Video Adjustment

6.5 OSD Settings

OSD is information displayed on the video image, such as device name, date, day of the week, and channel.

Step 1: Go to "Configuration → Image → OSD Settings".

Step 2: Select a channel and set OSD parameters.

Fig. 6-16 OSD Settings

- Check "Channel Name", "Display Date", "Display Week" to display OSD information. You can then drag the red OSD boxes to change their display position.
- You can modify the channel name, time format, and date format.
- OSD Attributes: OSD attributes include "Transparent, Flashing", "Transparent, Not Flashing", "Flashing, Not Transparent", and "Not Transparent, Not Flashing"; you can also set OSD font size, color, and alignment.
- Text Overlay Settings

The device can overlay up to 8 characters on the video image, and character content can be customized. At this time, the characters in the image will appear in red, and you can drag the characters to the desired display position.

Step 3: After completing the setup, click "Save" to complete the parameter settings.

6.6 Privacy Mask

By configuring Privacy Mask, the set area will not be displayed in the image.

Step 1: Go to "Configuration → Image → Privacy Mask".

Step 2: Select a channel number and check "Enable".

Step 3: Click "Draw Area", then click and hold the left mouse button in the image, drag the mouse, and then release the left mouse button to complete drawing one area.



- You can draw up to 4 areas in the image.
 - Click "Clear All" to clear all drawn areas. A maximum of 4 areas can be drawn in one image.
-

Step 4: Click "Stop Drawing" to end the area drawing.

Step 5: Click "Save" to complete the setup process.

6.7 Defective Pixel Correction (DPC)

DPC is used to correct defective pixels in the image, aiming to maintain image integrity and clarity. This function depends on the actual device and is only supported by the thermal imaging channel.

Step 1: Go to "Configuration → Image → DPC".

Step 2: Click the position of the defective pixel with the mouse. Then, the crosshair in the preview image will move to an approximate position. At this time, you can use the direction keys below the preview image to finely move the crosshair to the precise position.



If there are multiple defective pixels to be corrected in the preview image, after confirming the position of the first defective pixel, click the "💾" save button in the middle of the direction keys. Then, proceed to locate the remaining defective pixels in sequence. Each time after confirming a defective pixel's position, you must click "💾".

Step 3: Click "⌂" to perform correction, as shown in the figure.



- If you need to cancel defective pixel correction, click "↶".
 - Once you click "Save", subsequent attempts to cancel the defective pixel correction will not take effect.
-

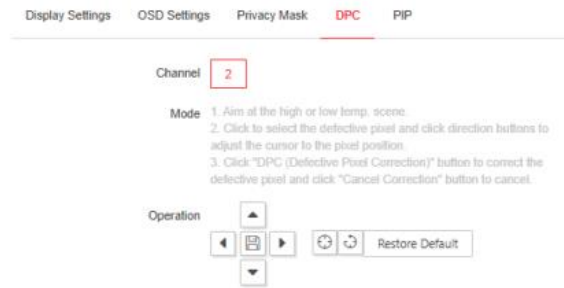


Fig. 6-17 Defective Pixel Correction

6.8 Picture-in-Picture (PIP)

This function enables the blending of images from the visible light channel (Channel 1) and the thermal imaging channel (Channel 2) and allows for preview and storage.

Step 1: Go to "Configuration → Image → PIP".

Step 2: Select PIP mode.

- If "Blending Mode" is selected, the blended image of Channel 1 and Channel 2 will be displayed. By adjusting the edge enhancement sensitivity, you can control the richness of edge details in the image. A higher sensitivity will result in clearer image edges. By adjusting the edge blending ratio, you can control the contour of the blending between visible light and thermal images. By adjusting the blending distance (distance between the device lens and the target scene), the offset of the visible light image relative to the thermal image can be adjusted.
- If "Normal Mode" is selected, only the images from Channel 2 will be displayed.

Step 3: Click "Save" to complete the setup process.

Chapter 7 Schedule and Linkage Configuration

7.1 Schedule Configuration

Set the start time and end time for task execution (taking flame detection as an example).

Step 1: Click "Arming Schedule", as shown in the figure.

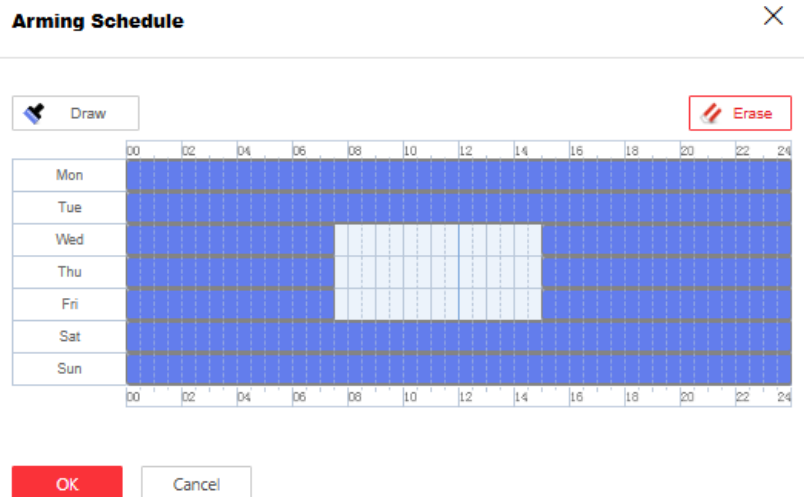


Fig. 7-1 Arming Schedule Settings

Step 2: The arming schedule needs to be set on the timeline. Click “Draw”, “Erase”, or “Arm All” to complete the setting for a specific arming schedule.

Step 3: Adjust the arming schedule.

- Select the set time period, and the setting interface will pop up. You can manually set the start time and end time at this point.
- Draw: Click “Draw”, then click on the timeline and drag the mouse to draw the arming schedule. The blue area is the armed area.
- Erase: Click “Erase”, then click on the timeline and drag the mouse to erase the arming schedule. The white area is the erased area.
- Arm All: Click “Arm All” to make the arming effective at all times.

Step 4: Click "Save".

7.2 Linkage Configuration

When an event or alarm occurs, alarm linkage can be enabled, and there are multiple linkage methods.

Linkage Method

Notify Surveillance Center ☒

Upload to FTP/Memory Card/NAS ☐

Audio Alarm ☒

Trigger Alarm Output ☒ Select All

☒ A->1 ☐ A->2 ☐ A->3

Recording Linkage ☐ Select All

☐ A1

Save

Fig. 7-3 Configuring Linkage Method

7.2.1 Upload to Center

If this option is checked, alarm information will be uploaded to the management center.

7.2.2 Upload to Micro SD Card

If this option is checked and an Micro SD card is configured, alarm information will be sent to the Micro SD card for storage. For Micro SD card configuration, please refer to "8.1.1 Micro SD Card Configuration".

7.2.3 Linked Audible Alarm

This function is used to set the audible alarm output. Its availability depends on the actual device.

Step 1: Go to "Event Center - Alarm Configuration - Audible Alarm Output".

Alarm Output **Audible Alarm Output** Alarm Server

Alarm Type: Flame Alarm

Audio Type: Warning Sound

Warning Sound: Fire alarm, please handle immediately! Test

Alarm Sound Settings

Custom Audio List: Edit

Loudspeaker Volume: 100

Arming Schedule: Draw Erase

	00	02	04	06	08	10	12	14	16	18	20	22	24
Mon													
Tue													
Wed													
Thu													
Fri													
Sat													
Sun													

Save

Fig. 7-3 Audible Alarm

Step 2: Set the alarm type according to usage requirements.

- Audio Type: It represents the sound output by the device after an alarm is triggered.
 - Warning Sound: After a different alarm type is selected, the corresponding warning sound will be automatically associated.
 - Custom Audio List: You can add voice texts to the "Custom Audio List".

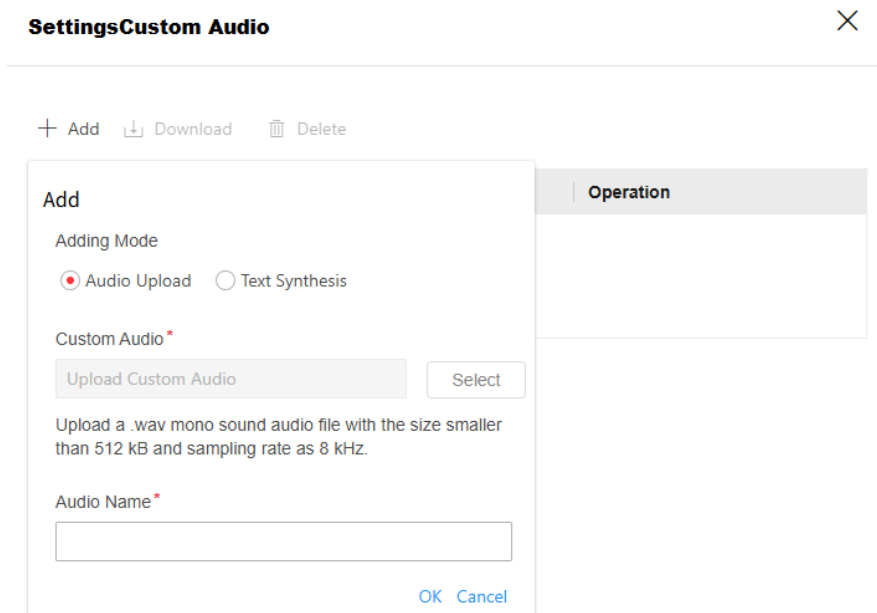


Fig. 7-4 Setting Custom Audio

- Loudspeaker Volume: It is used to adjust the volume of the audio output device.

Step 3: Set arming schedule: Please refer to the arming schedule settings in "Chapter 7 Schedule and Linkage Configuration".

Step 4: Click "Save".

7.2.4 Linked Alarm Output

If this function is checked and the corresponding alarm output channel is configured, alarm information will be output from the connected alarm device.

The device's alarm output interface is connected to an alarm output device (such as a fire alarm controller). When the device generates an alarm, the alarm output device will be triggered to output an alarm.

Step 1: Select "Event Center → General Events", click "Alarm Output" to set basic alarm output parameters.

Fusion Detection Camera User Manual

Alarm Output No.
A->1

IP Address
Local

Alarm Status
Close

Alarm Name

Post-Alarm
5 sec ▾

Arming Schedule

 Draw  Erase

	00	02	04	06	08	10	12	14	16	18	20	22	24
Mon													
Tue													
Wed													
Thu													
Fri													
Sat													
Sun													

Fig. 7-5 Alarm Output Settings

Step 2: Select the set alarm output number. A->1 is the default linked alarm output, A->2 is the linked fault output, and A->3 is the reserved alarm output. Set the alarm name and alarm duration. The specific delay time can be set according to the actual situation. The duration can be set from 1 second to 10 minutes, or it can be set to "Manual", meaning the alarm output is turned off manually.

Step 3: Set arming schedule: Please refer to the arming schedule settings in "Chapter 7 Schedule and Linkage Configuration".

Step 4: If the settings for other alarm outputs are the same, you can click "Copy to...", then click "Save" after completing the setup.

Note

- Click "Manual Alarm" to manually trigger an alarm output. The button will then change to "Clear Alarm". At this time, you need to click "Clear Alarm" to turn off the alarm output.

7.2.5 Linked Recording

If this function is checked and the corresponding device channel is configured, the relevant channel will be linked for recording. For recording configuration, please refer to "8.2.1 Scheduled Recording".

Chapter 8 Recording and Capture Configuration

The device can store recordings, capture images, and other files to storage media such as a Micro SD card and the local host. If recording schedules and capture schedules are configured, the device will automatically perform different recording or capture tasks within the set time frame and save the recording or capture image files to the storage device.

8.1 Storage Path Configuration

Micro SD Card Configuration

To store data on a Micro SD card, you must first install and format the Micro SD card. Once the Micro SD card is in normal status, recording or capture image files can be stored on the Micro SD card.

Step 1: Select "Configuration → Storage → HDD Management" to open the "HDD Management" interface, as shown in the figure.

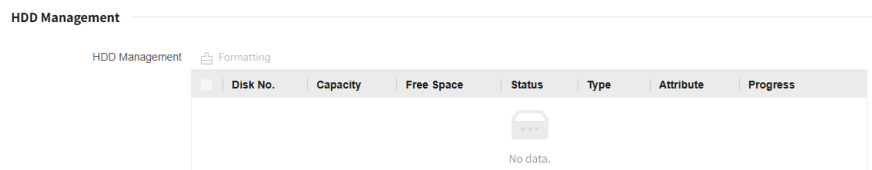


Fig. 8-1 HDD Management

Step 2: Check the detected Micro SD card and click "Formatting". When the Micro SD card status changes from "Unformatted" to "Normal", it means the Micro SD card can be used normally. In this interface, you can view information such as disk capacity, free space, and attributes.

Step 3: (Optional) Configure disk quota: Set the picture quota percentage and recording quota percentage as needed, as shown in the figure.

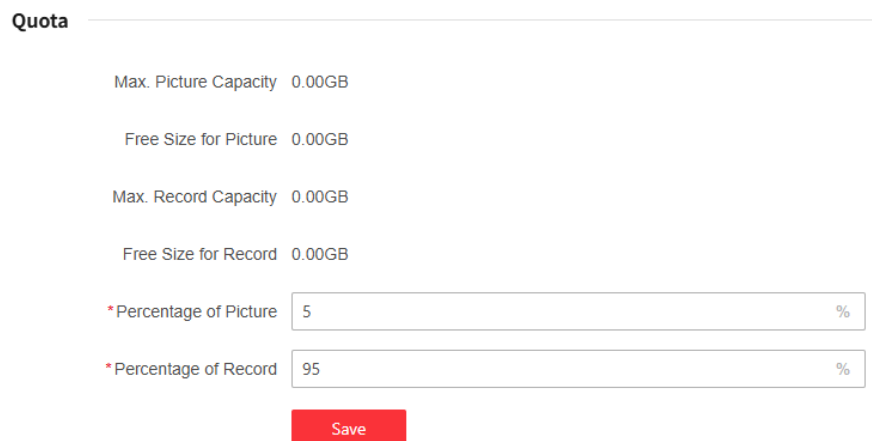


Fig. 8-2 Disk Quota

Step 4: After completing the setup, click "Save".

8.2 Recording Configuration

8.2.1 Scheduled Recording

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

Step 1: Go to Configuration → Storage → Schedule Configuration → Recording Schedule.

Step 2: Check "Enable" to activate the recording schedule.

Step 3: Select a recording type and click the corresponding button to draw the recording schedule time.

- Timed Recording refers to recording according to the time configured in the recording schedule.
- Motion Detection Recording refers to triggering recording on a specified channel when motion detection occurs.
- Alarm Recording refers to triggering recording on a specified channel when any switch signal alarm occurs.



- Motion detection, alarm, and event recording all require the event type to be set in advance. Please refer to "Chapter 9 Event and Alarm Configuration".
 - Channel 2 does not support motion detection-type recording.
-

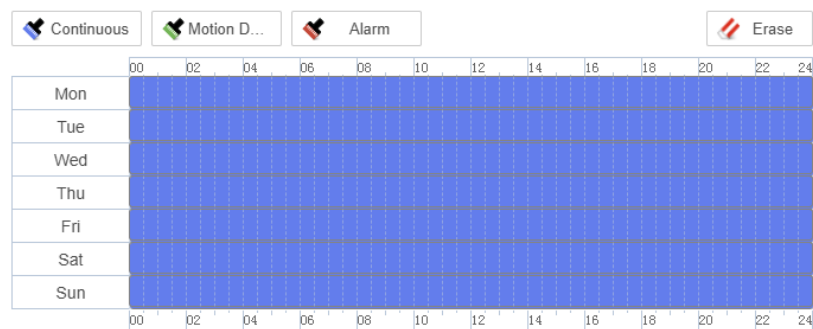


Fig. 8-3 Configuring Scheduled Recording

Step 4: Configure recording parameters.

- Overwrite: If 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-record Time: The pre-record time before the recording schedule start time point.
- Recording Delay: The post-record time after the recording schedule end time point.
- Stream Type: The stream type for recording storage.



Note

- The higher the bitrate selected, the shorter the pre-record time will be.
- The max. pre-record time is calculated based on a bitrate of 2Mbps; as a higher bitrate is selected, the pre-record time will be shortened accordingly.

Step 5: After completing the setup, click "Save".

8.2.2 Manual Recording

You can manually start or stop recording on the Live View interface.

Step 1: Go to "Configuration → Local", and select a video file.

The screenshot shows the 'Video Settings' window. It has three radio buttons for 'Video Size': 256M, 512M (selected), and 1G. Below this are two text input fields for file paths. The first is 'Video Saving Path' with the value 'C:\Users\caoyaoyao\PluginWeb\RecordFiles' and an 'Open' button. The second is 'Downloaded File Saving Path' with the value 'C:\Users\caoyaoyao\PluginWeb\DownloadFiles' and an 'Open' button.

Fig. 8-4 Video File Settings

Step 2: Set manual recording parameters.

- Video File Package Size: Set the size of a single video file stored locally. For example: If 256M is selected, then each video file will be 256M in size.
- Video Saving Path: It indicates the local path where video files are stored. You can click "Browse" to change the path.

Step 3: Click "Save".

Step 4: Go to "Live View" and double-click a channel to open the image of the channel.

Step 5: Click " " to start recording. The button will then change to " ". You can click the button again to stop recording.

8.2.3 Video Playback and Download

You can click "Playback" to search, play back, and download video files stored in the storage path.

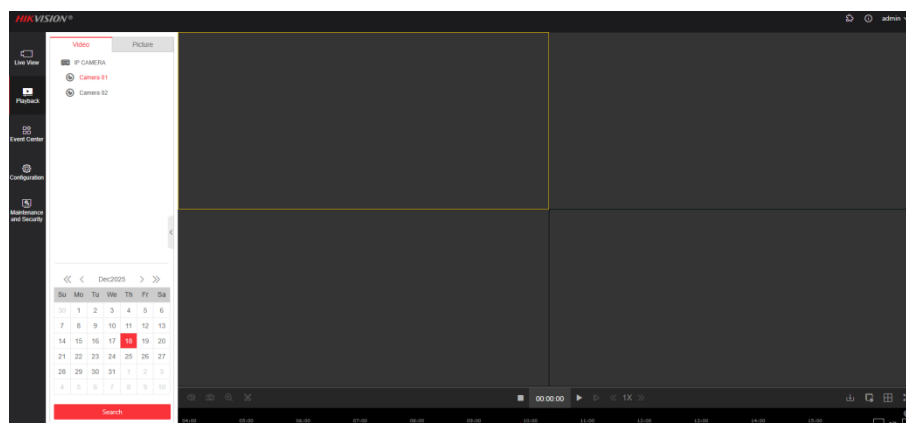


Fig. 8-5 Video Playback

- Channel Selection: Select the specific channel for playback.
- Video Search: Select a date on the calendar on the right, then click "Search". Video files that meet the search criteria will be displayed on the timeline. Drag the timeline to the desired playback position and click the "Play" button to start playing back the video file.
- Capture: Click "  " below the playback interface to capture an image and save it to the local computer.
- Video Clipping: Click "  " on the bottom right of the window to start clipping the video found. Click the icon again to stop clipping. At this time, a notification saying "Clipping Successful" will pop up below the calendar, and the clipped video will be saved locally.



Note

Video files clipped during playback have a default save path. You can go to "Configuration → Local", select "Playback Clip Save Path", and click "Browse" to change the save path.

- Video Search and Download: Click the "  " video download button below the playback interface to open the video download interface.



Note

Video files clipped during playback have a default save path. You can go to "Configuration → Local", select "Playback Download Save Path", and click "Browse" to change the save path.

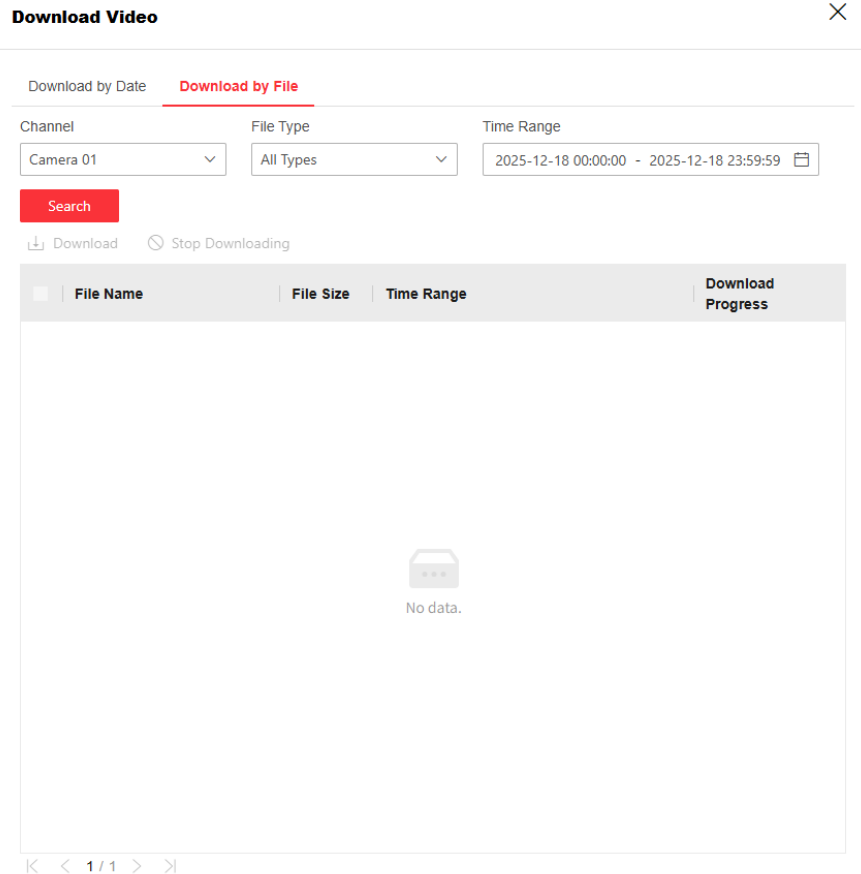


Fig. 8-6 Video Download

- Full Screen Button: Click "⛶" to play back the video file in full screen, and menu information will be hidden. Press ESC to exit full screen.

8.3 Capture Configuration

You can use Capture to record video image information.

8.3.1 Event Capture

Step 1: Click "Configuration → Storage → Schedule Configuration → Picture Capture".

Step 2: Select the channel number for picture capture.

Step 3: Enable "Event Capture". Then a picture will be captured when an event is triggered.



Note

When configuring event capture, you need to set the event type in advance. Please refer to "Chapter 10 Event and Alarm Configuration" for details.

Step 4: Set capture parameters.

- Picture Format: JPEG format is supported.
- Resolution: It refers to the resolution of the configured main/sub stream.

Fusion Detection Camera User Manual

- Picture Quality: You can choose from "Low", "Medium", and "High" three levels.

Video Recording **Picture Capture**

Channel **1** 2

Capture Parameters

Event Triggering

Event Capture ☒

Picture Format **JPEG**

Resolution **1920*1080**

Picture Quality ☐ Low ☒ Medium ☐ High

Save

Fig. 8-7 Configuring Capture Parameters

Step 5: Click "Save".

8.3.2 Live View Capture

You may perform picture capture during live view.

Step 1: Go to "Configuration → Local", and select the picture format.

- JPEG: Compressed files are smaller in size, facilitating network transmission.
- BMP: Compressed pictures are lossless, with better picture quality.

Step 2: Under "Capture and Clip", click "Browse" next to "Live View Capture Save Path" to adjust the storage path of pictures captured during live view, then click "Save".

Step 3: Go to "Live View" and double-click a channel to open the image of the channel.

Step 4: Click "  to capture a picture and save it locally, achieving picture capture during live view.

8.3.3 Playback Capture

You may perform picture capture during video playback.

Step 1: Go to "Configuration → Local".

Step 2: Under "Capture and Clip", click "Browse" next to "Playback Capture Save Path" to adjust the storage path of pictures captured during playback, then click "Save".

Step 3: Go to "Playback", search for video files based on the search criteria, and play them.

Step 4: Click "  to capture a picture and save it locally, achieving picture capture during playback.

Chapter 9 Event and Alarm Configuration

9.1 Algorithm Mode Configuration

The device supports custom selection of algorithm resources to enable corresponding detection and alarm functions. The resource usage ratio must not exceed 100%.

Step 1: Select "Event Center → Algorithm Resource Configuration".

Step 2: Check "Algorithm Resources".



Algorithms of the same category share resources, such as perimeter intrusion.

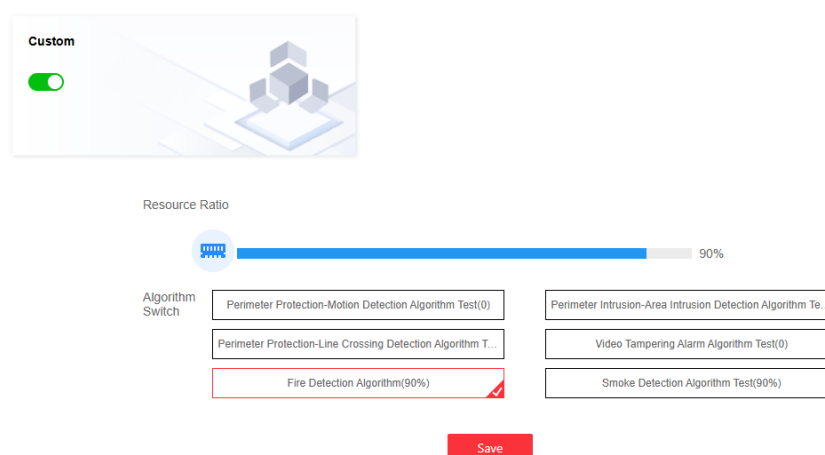


Fig. 9-1 Algorithm Mode Configuration

Step 3: Click "Save".

9.2 Alarm Configuration

Users can configure a custom alarm server.

Step 1: Select "Event Center → Alarm Configuration".

Step 2: Click "Edit", enter IP/domain name, URL, protocol type, and port number to configure the server.

Step 3: Click "Save".

9.3 General Event Configuration

9.3.1 Motion Detection Configuration

The motion detection function is used to detect whether there is a moving object in a certain area over a period of time. When there is a moving object, automatic recording and alarming will be triggered. The specific steps for motion detection configuration are as follows.

Step 1: Select "Event Center → General Events → Motion Detection" to enter the motion detection configuration interface, as shown in the figure.

Channel: 1

Enable: ☐

Parameter Settings

Enable Dynamic Analysis for Motion: ☐

Configuration Mode: Normal Mode

Sensitivity: 60

Arming Schedule

Arming Schedule: Edit

Linkage Method

Notify Surveillance Center: ☒

Upload to FTP/Memory Card/NAS: ☐

Trigger Alarm Output: ☐ Select All

☐ A->1 ☐ A->2 ☐ A->3

Recording Linkage: ☐ Select All

☐ A1

Save

Fig. 9-2 Motion Detection Interface

Step 2: Check "Enable" to activate the device's motion detection function.

If "Enable Dynamic Analysis for Motion" is checked, moving targets in the arming area will be calibrated under the circumstance that both the motion detection function and "Rules" are enabled. When dynamic analysis is set, and there is a moving object on the screen, the detection area will be highlighted with green grids.

Step 3: Area settings

Area settings are used to set the area range for the motion detection function. Only when a moving object is detected within the designated area, will an alarm and video recording be triggered.

- Click "Draw Area", then click and hold the left mouse button in the image, drag the mouse, and then release the left mouse button to complete drawing one area.
 - In "Normal Mode", up to 22*18 square grids can be drawn under PAL Model.
 - In "Expert Mode", you can draw 8 areas and set their day/night switch parameters, sensitivity, and proportion separately. After completing the setup of one area, please save it before drawing another one.
- Clear Area: Click "Clear All" to clear all drawn areas.
- Capture: Click "📷" to capture a picture and save it locally.

Fusion Detection Camera User Manual

- Record: Click "📹" to start recording. The button will then change to "🛑". You can click the button again to stop recording.
- Full Screen: Click "⛶" to enable full screen. Press the Esc key to exit full screen.

The screenshot shows the 'Area Settings' configuration page in 'Expert Mode'. At the top, there is a 'Channel' dropdown set to '1' and an 'Enable' toggle switch. Below this is the 'Parameter Settings' section, which includes an 'Enable Dynamic Analysis for Motion' toggle switch. The 'Configuration Mode' is set to 'Expert Mode' and 'Scheduled Image Settings' is set to 'Close'. The main area is a grid of eight numbered boxes (1-8) representing detection areas; box '1' is highlighted with a red border. Below the grid is a 'Sensitivity' slider set to 50. Further down are sections for 'Arming Schedule' (with an 'Edit' button), 'Linkage Method', 'Notify Surveillance Center' (checked), and 'Upload to FTP/Memory Card/NAS' (unchecked). At the bottom, there are checkboxes for 'Trigger Alarm Output' (with options A->1, A->2, A->3) and 'Recording Linkage' (with option A1). A red 'Save' button is at the very bottom.

Fig. 9-3 Area Settings in "Expert Mode"

Step 4: Parameter configuration

1) Configuration Mode: Configuration mode consists of normal mode and expert mode. In "Normal Mode", you can set motion detection sensitivity; in "Expert Mode", you can set "Day/Night Switch Parameter" and other corresponding parameters. Day/Night Switch parameter can be set to "Off", "Auto Control", and "Scheduled Switch".

- Off: The system will not perform day/night switching.
- Auto Control: The system will automatically switch between day and night modes based on environmental changes. The day mode image is in color, while the night mode image is in black and white.
- Scheduled Switch: Switching is performed according to the set time. It is in "Day" mode during the set time period and in "Night" mode outside the time period.

2) 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.

Step 5: For arming schedule and linkage methods, please refer to "Chapter 7 Schedule and Linkage Configuration".

Step 6: After completing the setup, click "Save" at the bottom of the interface to save the set parameters.

9.3.2 Occlusion Alarm Configuration

An occlusion alarm refers to an alarm generated when an area within the screen is obscured

Fusion Detection Camera User Manual

due to human factors or other elements, preventing normal monitoring of the area. When an occlusion alarm occurs, you can quickly troubleshoot the cause of the alarm and restore the video screen. The setup steps for the occlusion alarm are as follows.

Step 1: Select "Event Center → General Events → Occlusion Alarm" to enter the occlusion alarm setting interface, as shown in the figure.

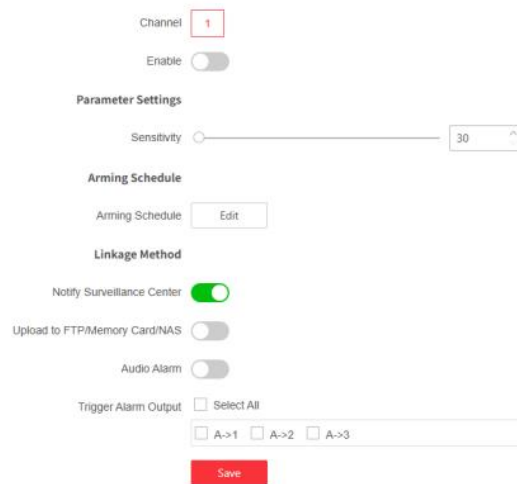
The screenshot shows the 'Occlusion Alarm' configuration interface. At the top, there is a 'Channel' dropdown menu set to '1' and an 'Enable' toggle switch. Below this is the 'Parameter Settings' section, which includes a 'Sensitivity' slider set to 30. The 'Arming Schedule' section has an 'Edit' button. The 'Linkage Method' section contains three toggle switches: 'Notify Surveillance Center' (checked), 'Upload to FTP/Memory Card/NAS' (unchecked), and 'Audio Alarm' (unchecked). At the bottom, there is a 'Trigger Alarm Output' section with a 'Select All' checkbox and three checkboxes for 'A->1', 'A->2', and 'A->3'. A red 'Save' button is located at the bottom right.

Fig. 9-4 Occlusion Alarm Interface

Step 2: Check "Enable" to activate the device's occlusion alarm function.

- Sensitivity: You can drag the progress bar to adjust sensitivity; the further to the right, the higher the sensitivity.
- Capture: Click "📷" to capture a picture and save it locally.
- Record: Click "🔴" to start recording. The button will then change to "🔴". You can click the button again to stop recording.
- Full Screen: Click "⌕" to enable full screen. Press the Esc key to exit full screen.

Step 3: Set arming schedule and linkage method: Please refer to the arming schedule and linkage method settings in "Chapter 7 Schedule and Linkage Configuration".

Step 4: After completing the setup, click "Save" to save the set parameters.

9.3.3 Alarm Input Configuration

Note

When configuring event capture, you need to set the event type in advance. Please refer to "Chapter 10 Event and Alarm Configuration" for details. The alarm input and output devices should first be connected according to the device's alarm input/output interfaces.

The device supports alarm signal input and output. The linked alarm output under other functions refers to the alarm output set here.

After an alarm input device is connected to the device's alarm input interface, the device will be triggered to output an alarm when the alarm input device generates an alarm.

Step 1: Select "Event Center → General Events → Alarm Input" to enter the alarm input setting interface.

Fusion Detection Camera User Manual

Step 2: Select the alarm input number to be set and configure the alarm name and alarm type. The alarm name can be customized, and the alarm type can be set to NO (Normally Open) or NC (Normally Closed), depending on the signal required by the alarm device you are using. Input definition allows you to select either alarm input or alarm output.

Step 3: Check "Enable Alarm Input Handling". Only if this option is checked will subsequent configured alarm linkages take effect; if not checked, the configured alarm linkages will not work.

Step 4: Set arming schedule and linkage method: Please refer to the arming schedule and linkage method settings in "Chapter 7 Schedule and Linkage Configuration".

Alarm Input No.
A < -1

Destination IP or Host Name
Local

Alarm Type
NO

Alarm Name

Enter
Mute

Enable Alarm Input Handling

Arming Schedule

Draw Erase

	00	02	04	06	08	10	12	14	16	18	20	22	24
Mon													
Tue													
Wed													
Thu													
Fri													

Save Cancel

Fig. 9-5 Alarm Linkage

Step 5: After completing the setup, click "Save" to save the set parameters.

9.3.4 Abnormal Event Alarm Configuration

Step 1: Select "Event Center → General Events → Abnormal Events" to enter the abnormal event alarm setting interface. Abnormal events include "full hard disk", "hard disk error", "network disconnection", "IP address conflict", "illegal access", "abnormal subsystem", and "thermal imaging module fault". When the device experiences any of the above situations and the alarm linkage is configured, the device will automatically trigger an abnormal event alarm.

Step 2: Set arming schedule and linkage method: Please refer to the arming schedule and linkage method settings in "Chapter 7 Schedule and Linkage Configuration".

Step 3: After completing the setup, click "Save" to save the set parameters.

9.3.5 Alarm Simulation Configuration

Alarm simulation is provided for developer debugging. It mimics device alarms and is not a real alarm event.

Step 1: Select "Event Center → General Events → Alarm Simulation" to enter the alarm simulation setting interface.

Step 2: Set the event type for alarm simulation, including "Flame Alarm", "Smoke Alarm", and "Distress Call Recognition".

Step 3: After completing the setup, click "Simulate Alarm" to trigger the simulation process.

9.3.6 Indicator Control Configuration

The running, fault, and alarm indicators can be configured.

Step 1: Select "Event Center → General Events → Indicator Control" to enter the indicator control setting interface.

Step 2: Set indicator control.

- Running Indicator: Click to enable.
- Fault Indicator: Click to enable.
- Alarm Indicator: It can be set to solid red, alternating flashing red/blue, chasing light, or off.
- Flash Frequency: When the alarm indicator is set to alternating flashing red/blue or chasing light, the flash frequency is customizable.

Step 3: After completing the setup, click "Save" to save the set parameters.

9.4 Temperature Measurement Configuration

The temperature measurement function is used to monitor the temperature of a site in real-time. When the temperature exceeds the alarm threshold, a prompt or alarm will be triggered.

9.4.1 Notes on Temperature Measurement

- The device should not be more than 50 meters away from the target for temperature measurement.
- The surface of the target should be as perpendicular as possible to the optical axis, with a recommended oblique image plane angle of no more than 45°.
- The target imaging pixels should not be less than 5×5.

9.4.2 Normal Temperature Measurement and Alarm

Normal temperature measurement is designed to perform temperature measurement and alarming for the entire scene.

Step 1: Go to "Event Center → Temperature Measurement → Basic Parameter" and check "Enable".

Step 2: Set basic temperature measurement parameters.

- Display Temperature Info on Stream: If checked, the detected temperature and temperature measurement frame information will be superimposed on the stream of the thermal imaging channel.
- Temperature Display Information: You can select max. temperature, min. temperature, or average temperature. By checking these options, you can view the corresponding temperature information on the "Live View" interface in the thermal imaging channel.
- Temperature Unit: Celsius by default.
- Temperature Range: 0.0-400.0 by default.

The screenshot shows the 'Basic Parameter' tab for temperature measurement. At the top, 'Channel 2' is selected. Below the tabs, there is an 'Enable' toggle switch which is turned on. Under 'Display Parameters', 'Display Temperature Info. on Stream' is also turned on. The 'Temperature Display Information' section contains three checkboxes: 'Max. Tempe...', 'Min. Temper...', and 'Average Te...', all of which are checked. The 'Temperature Parameters' section shows 'Temperature Unit' set to 'Degree Celsius(°C)' and 'Temperature Range' set to '0.0~400.0'. A 'Unit Settings' link is visible next to the unit dropdown. A red 'Save' button is at the bottom.

Fig. 9-6 Temperature Measurement Basic Parameter Settings

Step 3: Go to "Rule Configuration" and select normal configuration mode. Set normal mode parameters, as shown in the figure.

Channel 2

Basic Parameter Rule Configuration Arming Schedule ...

Configuration Mode ☒ Normal Mode ☐ Expert Mode

Emissivity Custom

*Emissivity 0.96

*Distance to Target 1.5 m

Alarm Parameters Settings

Alarm Filter Configuration

Reflect Light Filter

Enable Reflect Light Filter

Save

Fig. 9-7 Setting Normal Mode Parameters

- **Emissivity:** Every object has a specific emissivity. Emissivity can be indicated with a fixed value and varies from rough to smooth surfaces. You can also query the corresponding emissivity for your target and customize the emissivity value.
- **Distance to Target:** It indicates the straight-line distance between the temperature measurement area and the device. Please fill in the actual distance.
- **Alarm Rules**
 - **Pre-alarm/Alarm Temperature:** When the detected temperature exceeds the set pre-alarm/alarm threshold and reaches the set filter time, the device will trigger pre-alarm/alarm.
 - **Pre-alarm/Alarm Filter Time:** It indicates the time during which the temperature of the measured target remains not lower than the temperature threshold for pre-alarm/alarm.
 - **Pre-alarm/Alarm Output:** It indicates the pre-alarm/alarm output linkage set for the pre-alarm rules.

Note

Pre-alarm output and alarm output require connection of an external alarm output device (such as a fire alarm host) to the device's alarm output interface and configuration of alarm output parameters (for configuration details, see Linkage Alarm Output). Pre-alarm and alarm output can be output through different alarm output interfaces.

- **Reflect Light Filter:** If enabled, the algorithm will filter out false alarms caused by sunlight reflection.

Step 4: Set arming schedule and linkage method: Please refer to the arming schedule and linkage method settings in "Chapter 7 Schedule and Linkage Configuration".

Step 5: Click "Save".

9.4.3 Expert Temperature Measurement and Alarm

Expert temperature measurement is designed to perform temperature measurement and alarming for targets that meet the temperature measurement rules.

Step 1: Go to "Event Center → Temperature Measurement → Basic Parameter" and check "Enable".

Step 2: Set basic temperature measurement parameters. Please refer to "9.3.2 Normal Temperature Measurement and Alarm" for details.

Step 3: Go to "Rule Configuration" and select expert configuration mode. Set expert mode parameters, as shown in the figure.

The screenshot shows the 'Rule Configuration' tab in the 'Temperature Measurement' section. At the top, 'Channel 2' is selected. The 'Configuration Mode' is set to 'Expert Mode'. Under 'Temperature Measurement Rule', there is a grid of 8 rule configuration slots, with the first slot containing the number '1'. Below this grid, the 'Enable' toggle is turned on. The 'Rule Name' is set to '1'. The 'Rule Type' is set to 'Area'. The 'Emissivity' is set to 'Custom' with a value of '0.96'. The 'Distance to Target' is set to '1.5 m'. There is an 'Alarm Rule' section with a 'Settings' button. An 'Expand' link is also visible. At the bottom, there is an 'Alarm Filter Configuration' section with a 'Reflect Light Filter' toggle, which is currently turned off. A red 'Save' button is at the bottom right.

Fig. 9-8 Setting Expert Mode Parameters

- Temperature Measurement Area: The device allows you to draw any area, but edges must not intersect. Click "Draw Area" to start drawing, and right-click to finish drawing. The area should be defined by 4-10 points.
- Rule Name: Customize the rule name.
- Temperature Measurement Type: It defaults to area temperature measurement.

Fusion Detection Camera User Manual

- Distance to Target: It indicates the straight-line distance between the temperature measurement area and the device. Please fill in the actual distance.
- Alarm rule configuration
 - Alarm Rules: There are 8 alarm rules: "High Temperature Greater Than", "High Temperature Lower Than", "Low Temperature Greater Than", "Low Temperature Lower Than", "Average Temperature Greater Than", "Average Temperature Lower Than", "Temperature Difference Greater Than", and "Temperature Difference Less Than".
 - Pre-alarm/Alarm Temperature: Set the threshold for pre-alarm and alarm. For example, if "High Temperature Greater Than" is selected as the alarm rule, the pre-alarm temperature is set to "50°C", and the alarm temperature is set to "55°C", a pre-alarm will be triggered when the detected temperature is greater than "50°C" and lasts for the set filter time, and an alarm will be triggered when the temperature is greater than "55°C" and lasts for the set filter time.
 - Temperature Tolerance: A temperature tolerance needs to be set to prevent temperature fluctuations from affecting the alarm result. For example, if the temperature tolerance is set to "3°C" and the alarm temperature is set to "55°C", the device will alarm when the detected temperature is "55°C", and the alarm will only be canceled when the detected temperature is $\leq 52^{\circ}\text{C}$.
 - Pre-alarm/Alarm Filter Time: It indicates the time during which the temperature of the measured target remains not lower than the temperature threshold for pre-alarm/alarm.
 - Pre-alarm/Alarm Output: It indicates the pre-alarm/alarm output linkage set for the pre-alarm rules.
 - Temperature Jump Pre-alarm/Alarm: Set a temperature jump threshold for pre-alarm and alarm. If it is set to a sudden temperature rise alarm with a threshold of 5°C, a pre-alarm/alarm will be triggered when a sudden temperature rise of 5°C is detected.

Note

Pre-alarm output and alarm output require connection of an external alarm output device (such as a fire alarm host) to the device's alarm output interface and configuration of alarm output parameters (for configuration details, see Linkage Alarm Output). Pre-alarm and alarm output can be output through different alarm output interfaces.

- Reflected Temperature: If there is a high-temperature target in the scene, and the emissivity of the measured target is small, and the measured target reflects the high-temperature target, you need to check this option and set the reflected temperature value to the temperature of the high-temperature target.
- Reflect Light Filter: If enabled, the algorithm will filter out false alarms caused by sunlight reflection.

Step 4: Set arming schedule and linkage method: Please refer to the arming schedule and linkage method settings in "Chapter 7 Schedule and Linkage Configuration".

Step 5: Click "Save".

9.5 Area Intrusion Detection Configuration

Area Intrusion Detection is used to detect whether a target enters a warning area. When a target object enters this area, the device can generate an alarm signal and perform related linkage actions.

Step 1: Select "Event Center → Area Intrusion Detection" to enter the area intrusion detection interface.

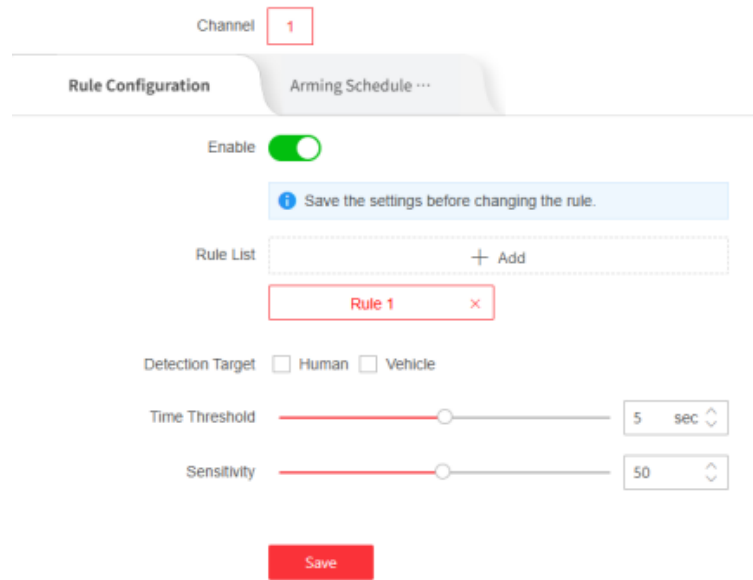


Fig. 9-9 Area Intrusion Detection Configuration

Step 2: Select a channel number and check "Enable".

Step 3: Configure rules, and custom rules are supported.

- Draw the maximum and minimum size.
 - 1) Click "Draw Maximum Size" / "Draw 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.
- Draw warning area
 - 1) Click "Draw Warning Area", and click the mouse to select four vertices to draw a quadrilateral detection area.
 - 2) 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.
- Capture: Click "  " to capture a picture and save it locally.
- Record: Click "  " to start recording. The button will then change to "  ". You can click the button again to stop recording.
- Full Screen: Click "  " to enable full screen. Press the Esc key to exit full screen.

- Set the rule parameters.

- 1) Detection Target

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

- 2) 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.

- 3) 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.

Step 4: Set arming schedule and linkage method: Please refer to the arming schedule and linkage method settings in "Chapter 7 Schedule and Linkage Configuration".

Step 5: After completing the setup, click "Save" to save the set parameters.

9.6 Line Crossing Detection Configuration

Line Crossing 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.

Step 1: Select "Event Center → Line Crossing Detection" to enter the line crossing detection interface.

Channel 1

Rule Configuration Arming Schedule ...

Enable ☒

Save the settings before changing the rule.

Rule List

+ Add

Rule 1 Rule 2

Detection Target

☒ Human ☒ Vehicle

Direction

A<->B

Sensitivity

50

Save

Fig. 9-10 Line Crossing Detection Configuration

Step 2: Select a channel number and check “Enable”.

Step 3: Configure rules, and custom rules are supported.

- Draw the maximum and minimum size.
 - 1) Click "Draw Maximum Size" / "Draw 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.
- Draw warning line
 - 1) Click "Draw Detection Line", then a line segment with an arrow will appear in the image.
 - 2) Optional operation: Click "Clear All" to clear all drawn areas.
 - 3) Click to select the line segment, and 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.
 - 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.

Fusion Detection Camera User Manual

- Capture: Click "  " to capture a picture and save it locally.
 - Record: Click "  " to start recording. The button will then change to "  ". You can click the button again to stop recording.
 - Full Screen: Click "  " to enable full screen. Press the Esc key to exit full screen.
- Set the rule parameters.
 - 1) Detection Target
Used to specify the detection target. The device will detect the specified target.
 - 2) 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.
 - 3) 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.

Step 4: Set arming schedule and linkage method: Please refer to the arming schedule and linkage method settings in "Chapter 7 Schedule and Linkage Configuration".

Step 5: After completing the setup, click "Save" to save the set parameters.

9.7 Flame Detection Configuration

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

Step 1: Select "Event Center → Flame Detection" to enter the flame detection interface.

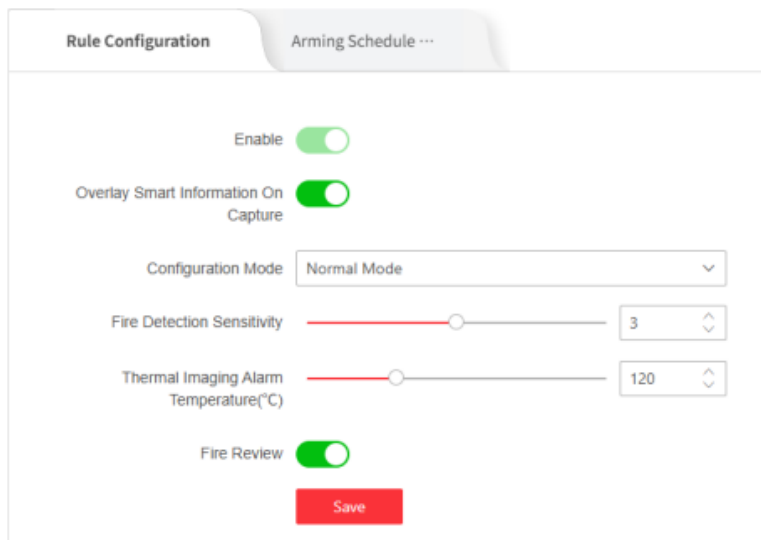


Fig. 9-11 Flame Detection Configuration

Step 2: This event needs to be enabled in "Algorithm Mode Configuration". After it is enabled,

you can decide whether to check "Overlay Smart Information on Capture".

Step 3: Configure rules, and custom rules are supported.

- Draw detection/shield area.
 - 1) The device allows you to draw any area, but edges must not intersect. Click "Draw Area" to start drawing, and right-click to finish drawing. The area should be defined by 4-10 points.
 - 2) 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.
 - Capture: Click "📷" to capture a picture and save it locally.
 - Record: Click "🔴" to start recording. The button will then change to "🔴". You can click the button again to stop recording.
 - Full Screen: Click "⌕" to enable full screen. Press the Esc key to exit full screen.
- Set the rule parameters.
 - 1) Configuration Mode

You may select Normal Mode or Expert Mode. In Expert Mode, you may disable flame/thermal imaging detection.
 - 2) Flame Sensitivity

The higher the sensitivity, the easier it is to trigger an alarm, but the false recognition rate will also increase.
 - 3) Thermal Imaging Alarm Temperature

An alarm will be triggered when the temperature reaches the set threshold.
 - 4) Flame Review

If enabled, a fire alarm will only be triggered when both thermal imaging detection and visual detection trigger an alarm simultaneously.

Step 4: Set arming schedule and linkage method: Please refer to the arming schedule and linkage method settings in "Chapter 7 Schedule and Linkage Configuration".

Step 5: After completing the setup, click "Save" to save the set parameters.

9.8 Smoke Detection Configuration

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

Step 1: Select "Event Center → Smoke Detection" to enter the smoke detection interface.

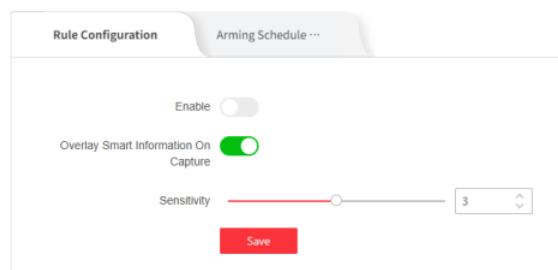


Fig. 9-12 Smoke Detection Configuration

Fusion Detection Camera User Manual

Step 2: This event needs to be enabled in "Algorithm Mode Configuration". After it is enabled, you can decide whether to check "Overlay Smart Information on Capture".

Step 3: Configure rules, and custom rules are supported.

- Draw detection/shield area.

- 1) The device allows you to draw any area, but edges must not intersect. Click "Draw Area" to start drawing, and right-click to finish drawing. The area should be defined by 4-10 points.

- 2) 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.
- Capture: Click "  " to capture a picture and save it locally.
- Record: Click "  " to start recording. The button will then change to "  ". You can click the button again to stop recording.
- Full Screen: Click "  " to enable full screen. Press the Esc key to exit full screen.

- Set sensitivity parameters.

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

Step 4: Set arming schedule and linkage method: Please refer to the arming schedule and linkage method settings in "Chapter 7 Schedule and Linkage Configuration".

Step 5: After completing the setup, click "Save" to save the set parameters.

Chapter 10 System Parameter Settings

10.1 System Maintenance

10.1.1 Device Information

Select "Configuration → System → System Settings", click the "Basic Information" tab to view the device's system information and set the "Device Name" and "Device No."

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

Basic Information

Time Configuration

RS_485

Unit Settings

Device Name

IP CAMERA

* Device No.

88

Device Model

HF-VT342(1mm)

Device Serial No.

HF-VT342(1mm)20251205AAWRGK9145230

Firmware Version

V1.3.0 build 251217 [Upgrade](#)

Encoding Version

V1.0.0 build 251217

Web Version

V5.1.0_R0105 build 251201

Number of Channels

2

Number of HDDs

0

Number of Alarm Inputs

1

Number of Alarm Outputs

3

Algorithm Model

Perimeter Protection-Motion Detection Algorithm Test

Algorithm Version

SMDL Version 3.8.0 2024524

Save

Fig. 10-1 Viewing Basic Device Information

10.1.2 Log Query

Select "Maintenance and Security → System Maintenance → Log/Security Audit Log" to enter the log query interface. The log interface allows you to query, display, and export log information effectively stored on the Micro SD card installed in the device.

The log information can be queried, viewed, and saved normally only when the Micro SD card is

functioning properly.

- Query Logs: Select the log type, set the log query date and start/end time, click "Search" and the log information that meets the criteria will be displayed in the list.
- Click "Export" to save the log information to the local computer.

10.1.3 Upgrade and Maintenance

Reboot

Select "Maintenance and Security → System Maintenance → Reboot" to enter the reboot interface. Click "Reboot" to remotely restart the device.

Upgrade

Select "Maintenance and Security → System Maintenance → Upgrade" to enter the upgrade interface. Select Upgrade 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.

Backup and Reset

Select "Maintenance and Security → System Maintenance → Backup and Reset" to enter the backup and reset interface.

- Backup: Click "Export" to back up device parameters.
- Reset
 - Simple Recovery: Simple recovery means restoring all device parameters except IP address, subnet mask, gateway, etc., to factory settings.
 - Full Recovery: Full recovery means restoring all device parameters to factory settings.
- Parameter Import: Click "Browse" to import device parameters.

Device Debugging

Select "Maintenance and Security → System Maintenance → Device Debugging" to enter the debugging interface. Click "Enable" under SSH Configuration to enable SSH service, and click "Export" to export diagnostic information.

10.2 System Configuration

This section introduces the function for setting device time.

Time Settings

Select "Configuration → System → System Settings → Time Configuration" to set the time zone and conduct time synchronization, as shown in the interface.

Fusion Detection Camera User Manual

Basic Information

Time Configuration

RS_485

Unit Settings

Device Time 2025-12-18 10:23:19

Time Zone (GMT+08:00) Beijing, Urumqi, Singapore, Perth

Time Sync Mode ☒ NTP Time Sync ☐ Manual Time Sync

* Server Address time.windows.com

* NTP Port 123

* Interval 1440 min Test

DST

Enable ☒

Start Time Apr First Sun 02

End Time Oct Last Sun 02

DST Bias ☒ 30min ☐ 60min ☐ 90min ☐ 120min

Save

Fig. 10-2 Time Settings

Set Time Zone

Enter the "Time Configuration" interface to synchronize the device time. "Time Zone" displays the current time zone of the device and can be set according to the actual situation.

Time Sync

The device supports two time synchronization methods: NTP Time Sync and Manual Time Sync. You can choose either method according to your actual needs.

● NTP Time Sync

Step 1: Set the NTP server address, NTP port number, and time synchronization interval. The device will synchronize time at the set interval. After completing the setup, you can click "Test" to check if the connection between the device and the NTP server is normal.

Step 2: After completing the parameter settings, click "Save".

● Manual Time Sync

Step 1: Check "Manual Time Sync" and manually enter the device time. If "Sync with Computer Time" is checked, the device time will remain consistent with the local computer time.

Step 2: After completing the parameter settings, click "Save".

Daylight Saving Time Settings

Daylight saving time is a system where local time is artificially adjusted to save energy. The unified time adopted during the implementation of this system is called "Daylight Saving Time".

10.3 Security Management

This section introduces device security-related parameter settings that can improve system security.

10.3.1 IP Address Filtering

Set IP addresses that are blocked and allowed for access.

Step 1: Select "Maintenance and Security → Security Management → IP Address Filtering".

Step 2: Check "Enable" to activate the IP address filtering function.

Blocklist: Only the IP addresses added to this list cannot access the device.

Allowlist: Only the IP addresses added to this list are allowed to access the device.

Step 3: Click "Save".

10.3.2 Illegal Login Lockout

After a user enters an incorrect password a certain number of times, the account will be locked.

Step 1: Select "Maintenance and Security → Security Management → Login Management".

Step 2: Check "Enable Illegal Login Lock".

If enabled, the device will automatically enter a locked state when the "admin" user enters an incorrect password 7 times, or a non-admin user enters an incorrect password 5 times consecutively. The system will prompt: "The account has been locked, please try again after 30 minutes." During this period, you may log in with another user account.

Step 3: Click "Save".

10.3.3 HTTPS

HTTPS is an HTTP channel with security as its goal, and a security certificate is required for the use of HTTPS. HTTPS allows secure access to web server on insecure networks through authentication.

Step 1: Go to "Configuration → Network → Network Services → HTTPS".

Step 2: Check "Enable" to activate HTTPS and enter the HTTPS port.

Step 3: Create and install a certificate. You can create a private certificate.

1. Check "Create Private Certificate".

2. Fill in parameters such as country/region, domain name/IP, and validity period. The validity period can be set from 1 to 3650 days.

3. Click "OK" to save the settings.

Server Certificate ×

Mounting Type

☒ Create Private Certificate

Country*

Domain/IP*

Validity Period*

 day(s)

Password

Province/State

Locality

Organization

Organization

Email

Create

Cancel

Fig. 10-3 Create Private Certificate

Step 4: Click "Install" to complete the certificate installation.

Step 5: Click "Save".

10.4 User Management

This section introduces device user configuration.

Enter the "Configuration → System → User Management" settings interface to configure the device users. When the current user is the administrator "admin", you can create other users as needed. A maximum of 31 users can be created.

Add User

Click "Add" to display the "Add User" interface, as shown in the figure.

Enter the username and password, select "Operator" or "Normal User" under "User Type", check the user permissions, and then click "OK" to complete user addition.



- To enhance the security of product network usage, please change user passwords regularly. It is recommended to update and maintain them every 3 months. If the device is used in a high-security risk environment, it is recommended to update weekly or monthly.
 - System administrators are advised to effectively manage users and user permissions, promptly delete irrelevant users and permissions, and close unnecessary network ports.
 - If the "admin" user enters an incorrect password 7 times consecutively, or a non-admin user enters an incorrect password 5 times consecutively, the device will automatically enter a locked state. At this time, the device will display a lock message reminder and automatically enter a locked state.
-

Add User ✕

User Name *

User Type

Operator ▼

Admin Password *

Password *

Password Confirm *

Permission Configuration

☒ Select All

☐ Remote: Parameters Settings

☒ Remote: Log Search / Interro...

☐ Remote: Upgrade / Format

☒ Remote: Two-Way Audio

☐ Remote: Shutdown/Reboot

OK

Cancel

Fig. 10-4 Add User

Change User

Select the user row to be modified, click "Change" to enter the "Change User" interface, where you can modify the "Username", "Password", and "User Type".

Delete User

Select the user to be deleted, click "Delete" to bring up a confirmation dialog box, and click "Confirm" to delete the user.

Account Security Settings

Click "Account Security Settings", and you may configure 3 security questions and answers.

View Online Users

Enter "Configuration → System → User Management → Online Users", and click "Refresh" to view currently online users.

Appendix A Installation and Maintenance

A.1 Lens Maintenance

An anti-reflection film is coated on the surface of the lens and it performs less effectively when contaminated with dust, grease, fingerprints, or other substances, which may even lead to scratches, molding, etc. If the lens is found to be dirty, clean it using the following methods.

- Contamination with dust, dirt, etc.: Rinse with water first, or gently wipe with a dry cloth to remove dust. Do not wipe forcefully with a wet cloth, as this may cause permanent damage to the glass.
- Grease contamination, fingerprints, etc.: Gently wipe off water droplets or oil with a soft cloth and allow it to dry. Then gently wipe with oil-free cotton or lens cleaning paper moistened with lens cleaning liquid. If not fully cleaned, repeat the process several times with a fresh cloth.



- Do not use paper to clean the lens, as paper contains hard calcium, which can easily scratch the front cover of the lens. The cloth used must be a sufficiently soft non-woven fabric or long-staple cotton.
 - Ordinary dish soap can be used as cleaning fluid. Do not use alkaline cleaners.
-

A.2 Network Security Maintenance

To ensure the network security of the device, we suggest you perform regular network security evaluations and maintenance on the network equipment system. Our company can provide related professional technical services.

Appendix B Common Material Emissivity Table

Material	Emissivity
Human skin	0.98
Printed circuit board	0.91
Cement concrete	0.95
Ceramics	0.92
Rubber	0.95
Paint	0.93
Wood	0.85
Asphalt	0.96
Brick	0.95
Sand	0.90
Soil	0.92
Cotton fabric	0.98
Cardboard	0.90
White paper	0.90
Water	0.96
Stainless steel (polished)	0.20
Carbon steel (polished)	0.10
Aluminum (polished)	0.05
Copper (polished)	0.05
Titanium (polished)	0.20
Zinc (polished)	0.30

Appendix C Product Dimension Drawing

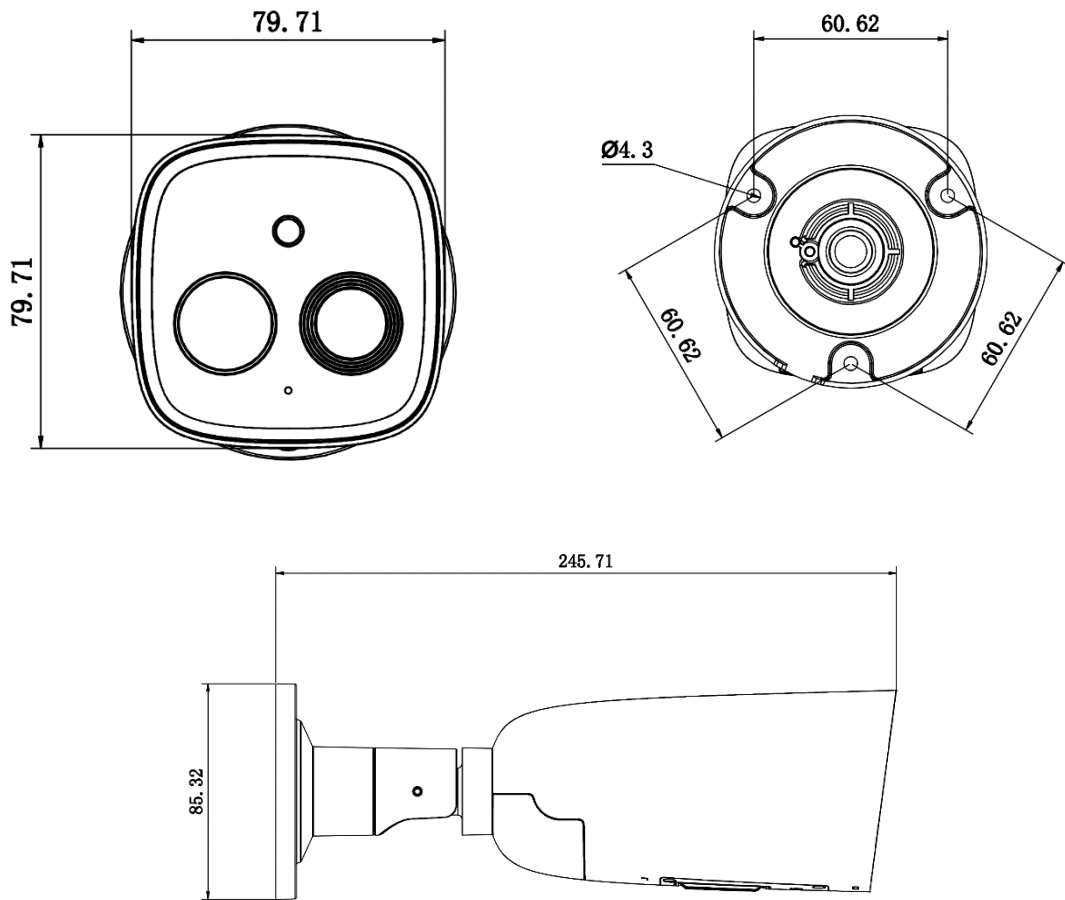


Fig. C-1 Product Dimension Drawing (HF-VT342)

