



Thermal Heat Fire Detection Camera

User Manual

Legal Information

© 2023 Hangzhou Hikfire Technology Co., Ltd. All rights reserved.

Any part of this manual, including text, pictures, and graphics, belongs to Hangzhou Hikfire Technology Co., Ltd. or its affiliates (hereinafter referred to as Hikvision). Without written permission, no entity or person may extract, copy, translate, or edit all or part of this manual in any way. Unless otherwise agreed, Hikvision does not provide any express or implied statements or warranties in this manual.

About the Product

The products described in this manual are for sale and use only in Mainland China. This product can only be used for after-sales service and maintenance in the country or region where the product is purchased.

About this Manual

This manual is only used as guidance for related products. It may be different from actual products. Please use the actual product as the actual product. This manual may be updated by Hikvision due to product version upgrade or other needs. If you need the latest version, please log in to Hikvision website (<http://www.hikvision.com>).

Hikvision recommends that you use this manual under the guidance of a professional.

Trademark Statement

- **HIK FIRE** Registered trademark of Hikvision.
- Other trademarks covered by this manual are owned by their respective owners.

Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS MANUAL AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED "AS IS" AND "WITH ALL FAULTS AND ERRORS". HIKROBOT 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 HIKROBOT 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 HIKROBOT HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.

YOU ACKNOWLEDGE THAT THE NATURE OF INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKROBOT 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, HIKROBOT 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.

THE PERFORMANCE DATA IN THIS PUBLICATION IS BASED ON HIKROBOT'S INTERNAL RESEARCH/EVALUATION. ACTUAL DATA MAY VARY DEPENDING ON SPECIFIC CONFIGURATIONS AND OPERATING CONDITIONS AND HIKROBOT SHALL NOT BEAR THE CONSEQUENCES ARISING THEREFROM.

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

Pre-Use Description

- Go to our website (www.hikvision.com) to get manuals, application tools, and development materials.
- Please sync the device before use. See **Setting Device Time** for details.
- Part of the web page configuration in the manual is applicable to the latest software version. Please contact technical support personnel to update the software.

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 hazardous situation which, if not avoided, will or could result in death or serious injury.

Safety Instruction

Danger

- It is a Class A product. In the living environment, the product may cause radio interference. In this case, the user may be required to take practical steps to interfere.
- During product installation and use, the electrical safety regulations of the country and area must be strictly observed.
- The plug or socket of the device is the device that disconnects the power supply. Do not block the plug or plug it in.
- Do not connect more than one product to the same power adapter (it may cause excessive heat or fire if the adapter is overloaded).
- Make sure to disconnect the product power supply during wiring, disassembling, etc., and do not power on

the device.

- When installing the product on a wall or ceiling, fix the product firmly.
- To avoid heat build-up, keep the device ventilated.
- If product smoke occurs, it may cause odor, or sound noise. Turn off the power supply and unplug the power cable. Please contact the distributor or service center.
- If the product is not working normally, please contact the store or nearest service center of the device. Do not disassemble or edit the product in any way. (The Company shall not be responsible for problems caused by unauthorized editing or repair).

Caution

- Product functions can only be carried out when the product is installed and maintained. This product is used to help you prevent disaster, but it is not a substitute for your on-site inspection, or to stop the accident from happening or expanding. You should still be more vigilant, be safer, and pay careful attention to the safety of your person and property.
- Please follow the installation method in this guide to install the device.
- To prevent injury, the device must be secured to the wall or ceiling.
- The serial port of the device is for debugging only. The user is not allowed.
- The device is only available in areas below 2000 m above sea level.
- Do not let the object fall on the product or vibrate the product so that the product is away from the point where magnetic field interference exists. Do not install the product in the area of surface vibration or shock risk (ignoring this item may damage the product).
- Do not use the product in high temperature, low temperature, or humidity. See the product parameter table for temperature and humidity requirements.
- For low-temperature products, preheat before starting. The pre-heating time should be determined according to different environment. Make sure the heat is enough before starting the product.
- Do not place exposed flame sources, such as lighted candles, on the device.
- Do not target the product lens to strong light source. Otherwise, the camera will be damaged.
- The product cannot be exposed to rain or humidity.
- Do not place the product in an environment with corrosive gas, which may cause damage to the device.
- Avoid placing the product in direct sunshine, in poor ventilation, or near heat sources, such as heaters or heaters (ignoring this item may cause fire hazards).
- When cleaning product lens or shield, use a sufficiently soft dry cloth or other alternative to wipe the outer surface. Do not use basic cleaning agent to wash the lens or shield.
- The product may face network security problems. Please strengthen the protection of personal information and data security. Please contact us as soon as you find the device may have network security risks.
- Please understand that it is your responsibility to reasonably configure all password and other related product security settings, and to properly keep your user name and password.
- Please keep all the original packaging materials of the product properly, so that when the problem persists, the packaging material can be used to package the product and send to the agent or return to the manufacturer. The company shall not be liable for the accidental damage caused by the transportation of non-original packaging material.

Note

Quality requirements for installation and maintenance personnel: Qualification certificate or experience in video system installation and maintenance, and qualification in related work (such as working at height). The following knowledge and operation skills are required.

- Basic knowledge and installation skills of video system and component.
- Basic knowledge and operation skills of low-voltage wiring and low-voltage electronic wiring.
- It has basic network security knowledge and skills, and is able to read the content of this manual.

The requirements of lifting device:

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

Thermal Heat Fire Detection Camera User Manual

- The lifting device has good safety performance.

Contents

Chapter 1 Product Introduction	1
1.1 Product Description	1
1.2 Product Function	1
1.3 Appearance Interface	1
1.4 Indicator and Speaker Status Description	3
Chapter 2 Wiring and Installation	5
2.1 Product Wiring	5
2.2 Product Installation	6
2.2.1 Pre-Installation Description	6
2.2.2 Installation Distance Recommended	7
2.2.3 Installation Method	7
2.2.4 Installing Waterproof Tape	11
2.2.5 Installing Network Port Waterproof Sleeve	12
Chapter 3 Pre-Use Operation Information	14
3.1 Network Connection	14
3.2 Activate Device	14
3.2.1 Activate Device via SADP Software	14
3.2.2 Activate via Web Page	15
3.3 Access Device	16
3.3.1 Access Device via Web Client	16
3.3.2 Access Device via Hik-Connect	16
Chapter 4 Key Functions Configuration Description	19
4.1 Fireworks Detection Function	19
4.2 Temperature Measurement Function	19
Chapter 5 Web Client Configuration and Operation	20
5.1 Live View	20
5.2 Video Playback	21
5.3 View Picture	22
5.4 Parameter Configuration	22
5.4.1 Local Configuration	22
5.4.2 System Parameters	24
5.4.3 Network Parameters	29
5.4.4 Video Audio Parameters	33
5.4.5 Image Parameters	37
5.4.6 Event and Alarm	42
5.4.7 Storage	50
5.4.8 Temperature Measurement	52
A. Communication Matrix and Device Command	55

Chapter 1 Product Introduction

1.1 Product Description

Thermal Heat Fire Detection Camera (the device) uses focal plane temperature detection technology as the main means of detecting the abnormal temperature and fire in the detected area, and provides alarm and alarm for network management and visualization. The device provides fire alarm, temperature detection alarm, and video verification in the detected area. It is used in hospitals, schools (laboratories, libraries, warehouses, archive rooms), museums, monasteries, dorms, ATMs, devices, safe production, indoor substations, new energy, petrochemicals (station stations), and other key fire protection and safety needs.

1.2 Product Function

- New fusion intelligent camera. It can detect temperature and alarm, and can be verified by video.
- High sensitivity, safe and reliable, powerful function, convenient to use, and aesthetically pleasing.
- Dual-light fusion image mode is supported, and the resolution of visible light can be up to $2560 \times 1440@25$ fps. The resolution of thermal image can be up to 160×120 , and the encoding resolution is 1280×720 .
- Support low bitrate, low delay, enhanced coding of areas of interest with ROI, and SVC self-adaptive encoding.
- Support local storage of microSD/SDHC/SDXC card (128 G).
- Support backlight compensation, auto electronic shutter function, and adapt to different monitoring environments.
- The optical channel supports main stream and sub-stream. The thermal imaging channel supports main stream and mobile phone monitoring.
- Fire detection is supported.
- Support 3D digital noise reduction, and 120 dB ultra-width dynamic.
- Temperature exception detection is supported.
- Local alarm indicator, built-in speaker high-decibel alarm, and remote audio suppression.
- PoE power supply is supported.
- Support 10M/100M adaptive network interface.
- IP66 rating is supported.
- Supports 2-channel alarm input, 2-channel alarm output, 1-channel audio input/output, 1-channel RS-485.
- The user shall be able to link alarm pictures and alarm videos during alarm.
- GB28181 access, Hik-Connect platform access.
- Support NTP server test, HTTPS and other security authentication, and certificate creation.

1.3 Appearance Interface



Note

The product pictures in this manual are diagram. Please refer to actual device.

Appearance Description

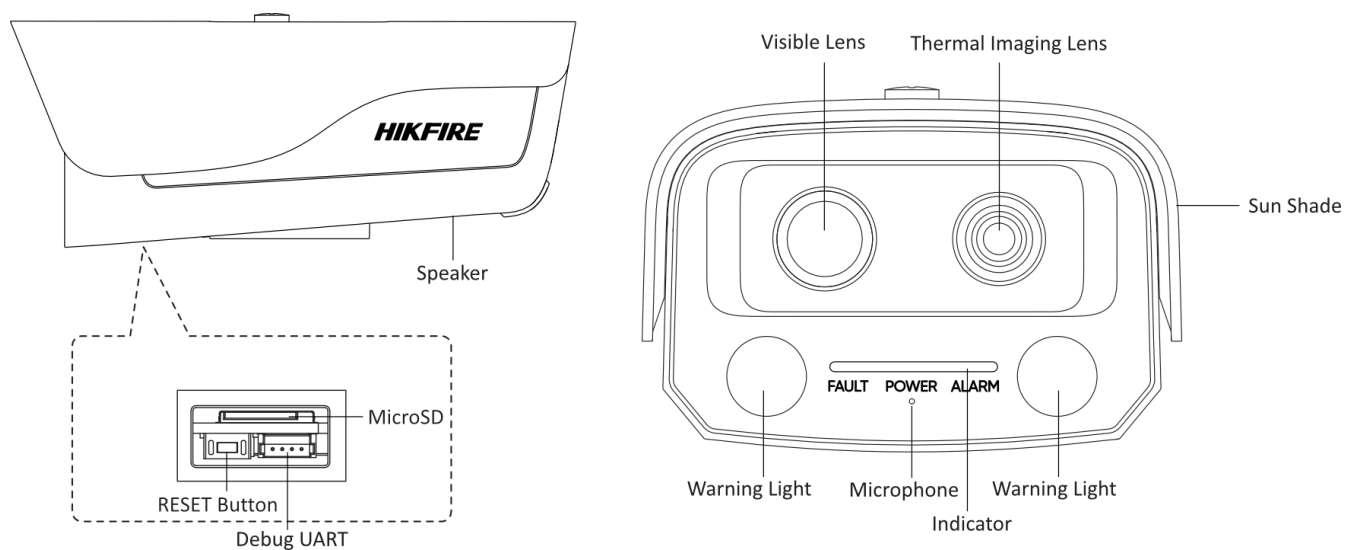


Figure 1-1 Appearance Diagram

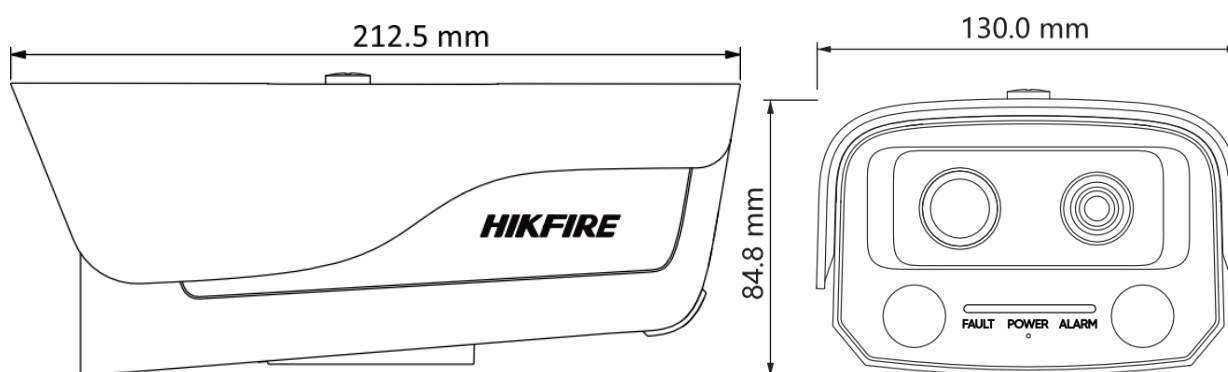


Figure 1-2 Appearance Size

MicroSD Card

You can insert the microSD card for local storage.

RESET Button

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

Debug Serial Port



Caution

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

Interface Description

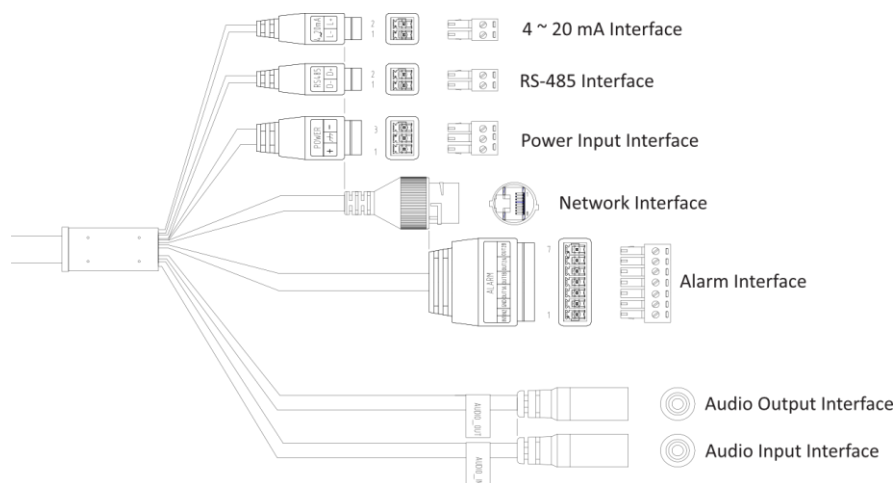


Figure 1-3 Interface

4 ~ 20 mA Interface

Reserved.

RS-485 Interface

Connect the device that supports RS-485 protocol.

Network Interface

Network access, used to configure device, live view, central access platform, etc. The interface supports PoE power supply.

Power Input Interface

DC 12 V input. Please connect to the positive and negative terminals.

Alarm Interface

Alarm interface, which can connect alarm input and alarm output devices.

Audio Output Interface

Connect audio output device, such as audio speaker.

Audio Input Interface

Connect audio input device.

1.4 Indicator and Speaker Status Description

Table 1-1 Status Description

Indicator	Speaker	Status Description
Red Light	Fire and Fire Alarm. Please handle as soon as possible.	Smoke or Fire Alarm
Red Light	Temperature exception. Please	Temperature Exception Alarm

Thermal Heat Fire Detection Camera User Manual

Indicator	Speaker	Status Description
	handle as soon as possible.	
None	"Do Not Block Alarm Device"	Video Tampering Detection
None	"Di...Di...Di..."	Exception (Network disconnected).
Green Light	None	Normal Operation
Yellow Light	None	Fault

Note

If alarm/exceptional event needs to be prompted through the speaker, you can enable sound linkage in **Event**.

Chapter 2 Wiring and Installation

2.1 Product Wiring

The device has five external interfaces, including power input interface, RS-485 interface, alarm interface, audio input/output interface, and network interface. RS-485 interface, alarm interface, and power input interface are described below.

Table 2-1 RS-485 Interface Description

No.	ID	Interface Description	Wiring Description
1.	D-	Connect to B-End of RS-485 Signal	Access RS-485 Signal
2.	D+	Connect the A-End of RS-485 Signal	

Table 2-2 Alarm Interface Description

No.	ID	Interface Description	Wiring Description
1.	IN1	Connect Alarm Input Signal 1 Positive Pole	Access Alarm Input Signal 1
3.	GND	Connect Alarm Input Signal 1 Negative Pole Connect Alarm Input Signal 2 Negative Pole	
2.	IN2	Connect Alarm Input Signal 2 Positive Pole	Access Alarm Input Signal 2
3.	GND	Connect Alarm Input Signal 1 Negative Pole Connect Alarm Input Signal 2 Negative Pole	
4.	OUT1A	Connect Alarm Output Signal	Access alarm output signal 1; positive and negative poles are not distinguished.
5.	OUT1B		
6.	OUT2A	Connect Alarm Output Signal	Access alarm output signal 2, excluding positive and negative poles.
7.	OUT2B		

Table 2-3 Power Input Interface

No.	ID	Interface Description	Wiring Description
1.	+	DC 12 V Power Input Positive	Access DC 12 V to power the

No.	ID	Interface Description	Wiring Description
2.	177	Power Grounding	device.
3.	-	DC 12 V Power Input Negative	

2.2 Product Installation

2.2.1 Pre-Installation Description

- Please follow the installation method in this guide to install the device.
- When installing walls or ceilings, make sure the product is secure.
- Please make sure the device in the box is intact and all components are complete before installation.
- The wall should be of a certain thickness, and should be able to withstand at least 4 times the total weight of the device and installation accessories.
- If it is a cement ceiling wall, please install expansion bolts (the mounting holes of expansion bolts should be the same with the brackets) and then install the brackets.
- If it is a wood wall, you can use self-tapping screws to install the brackets directly.
- In the process of installing and using the device, the connection may affect the device's water resistance. See [Installing Waterproof Tape](#) and [Installing the Water Resistance Cover](#) for the device's cable connection.
- The brackets in the manual are optional. Please select according to actual needs.
- Do not drag the cable on the rear of the device directly when moving the device. Otherwise, the device may cause water resistance or cause route problems.

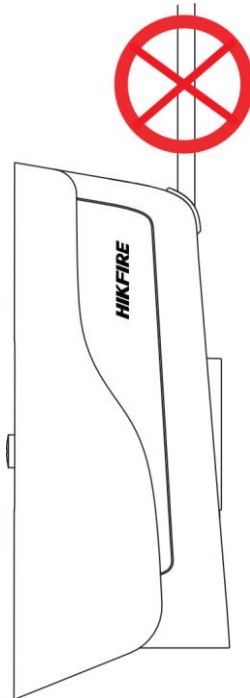


Figure 2-1 Diagram of Moving Notices

2.2.2 Installation Distance Recommended

Before installing the device, select the correct installation location according to actual needs.

Fire Recognition

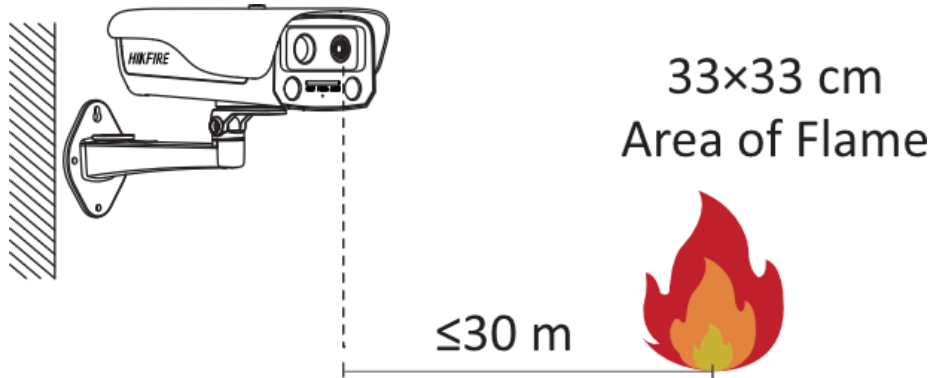


Figure 2-2 Fire Recognition Installation Distance

Smoke Recognition

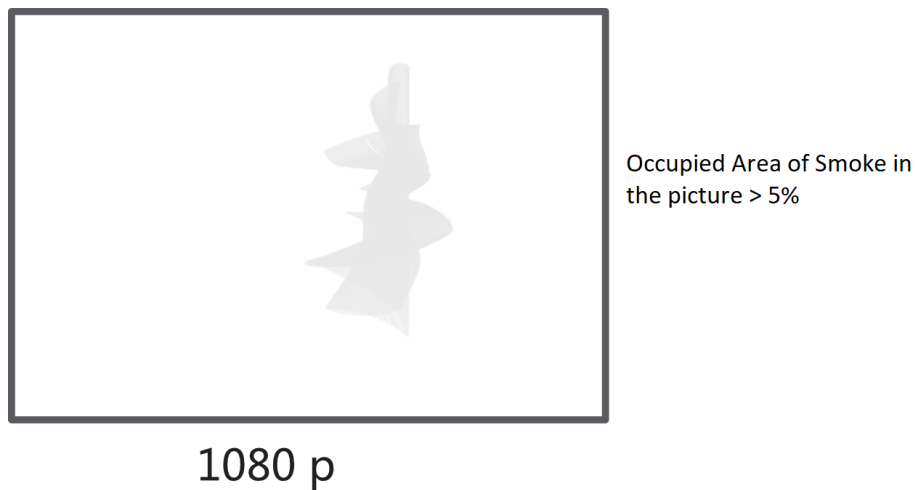


Figure 2-3 Smoke Recognition Ratio

2.2.3 Installation Method

The device can be wall mounted, suspended, and installed in a general section. The three installation methods are similar. The wall installation method and the lifting method are described below.



Note

The device can only be used with the supporting bracket (NP-FP105-B, DS-1299ZJ-P, DS-1232ZJ-XSP, or purchased separately). It can be used with other devices (such as carts, racks, or handling devices).

Wall Mounted

Steps



Note

Speaker exists on the bottom of the device. Please avoid blocking the speaker when installing.

1. Optional Operation: Install the microSD card.
 - 1) Loosen the screws and remove the cover.
 - 2) Insert the microSD card correctly according to the direction shown.
 - 3) Install the cover and tighten the screw.
-



Note

Do not leave the seal ring in the cover.

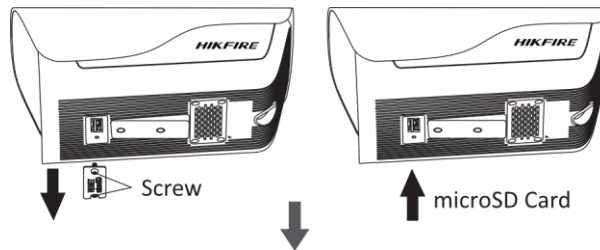


Figure 2-4 Install microSD Card

2. Install the wall mounting bracket. After positioning with the installation sticker, fix the wall mounting bracket to the wall with 4 PA4 × 25 screws.

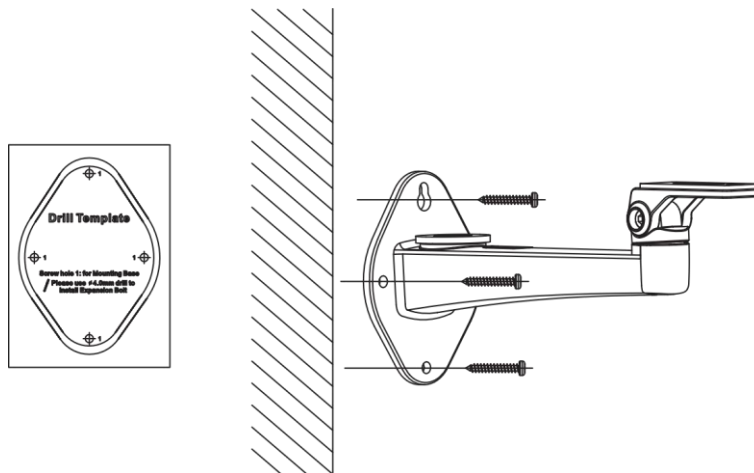


Figure 2-5 Mounting Wall Mount

3. Install the device, and use 2 1/4-20 UNC × 12 screws (with flat-pad bullet) to fasten the device to the wall mounting bracket.

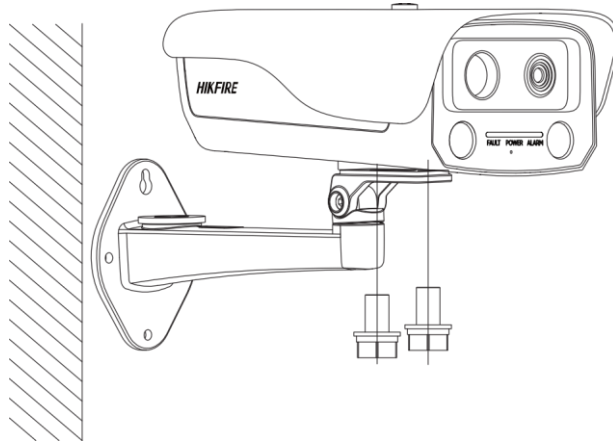


Figure 2-6 Installing Device

4. Set up wiring, arrange and connect power cables, network cables, and other cables, and handle insulation and water repellency. (For handling methods, see [Installing water repellency tape](#) and [installing water repellent sleeve](#).)
5. Adjust the angle. Loosen the vertical or horizontal adjustment screws, and adjust vertically or horizontally. After adjusting the device position, fasten the screws and install.

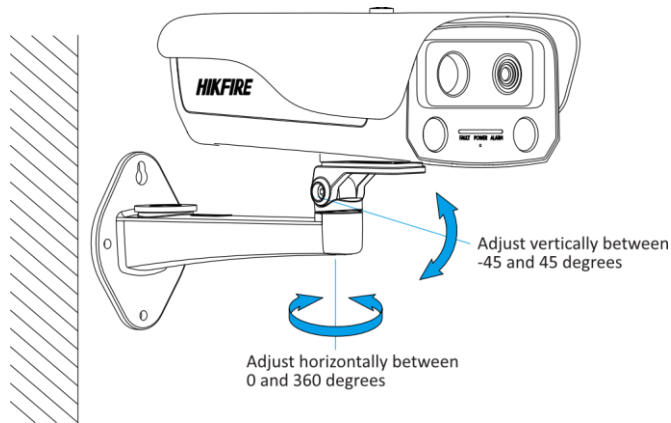


Figure 2-7 Adjusting Angle

Lifting

Steps



Note

Speaker exists on the bottom of the device. Please avoid blocking the speaker when installing.

1. Optional Operation: Install the microSD card.
 - 1) Loosen the screws and remove the cover.
 - 2) Insert the microSD card correctly according to the direction shown.
 - 3) Install the cover and tighten the screw.

Note

Do not leave the seal ring in the cover.

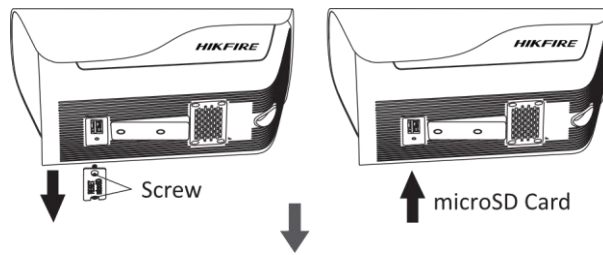


Figure 2-8 Installing microSD Card

2. Install the lifting bracket, and fix the lifting bracket to the wall with 3 PA4 × 25 screws.

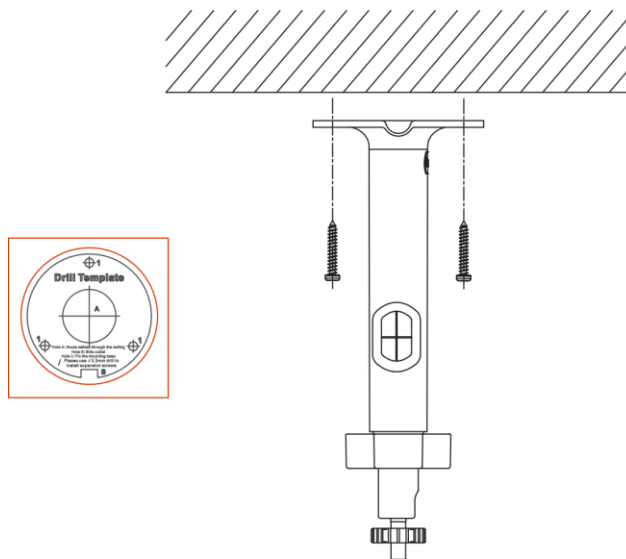


Figure 2-9 Installing Lifting Bracket

3. Install the device, remove the set screw on the device sun visor, align the threaded hole of the body with the bottom end of the bracket, and screw the device into the bracket.

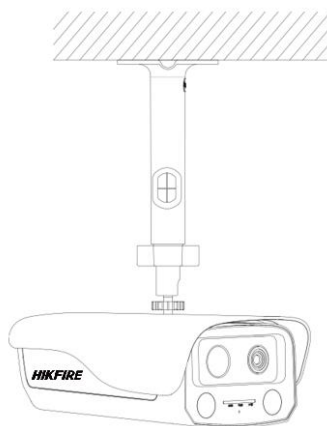


Figure 2-10 Installing Device

4. Set up wiring, arrange and connect power cables, network cables, and other cables, and handle insulation and water repellency. (For handling methods, see [Installing water repellency tape](#) and [installing water repellent sleeve](#).)
5. Adjust the angle. Loosen the adjustment knob of the bracket, and fasten the screws after adjusting the device position.

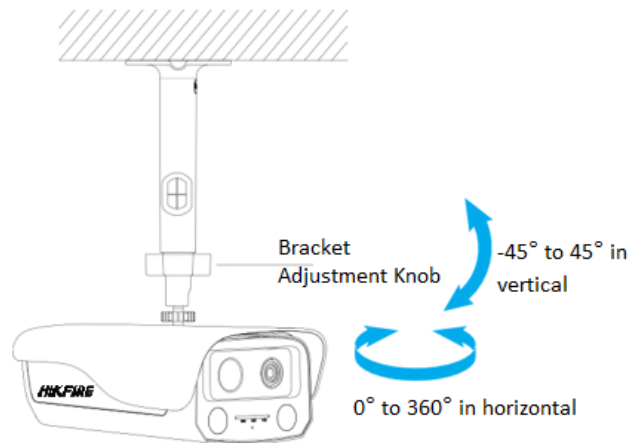


Figure 2-11 Adjusting Angle

2.2.4 Installing Waterproof Tape

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

Prerequisite

Set the cable first.

Steps

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

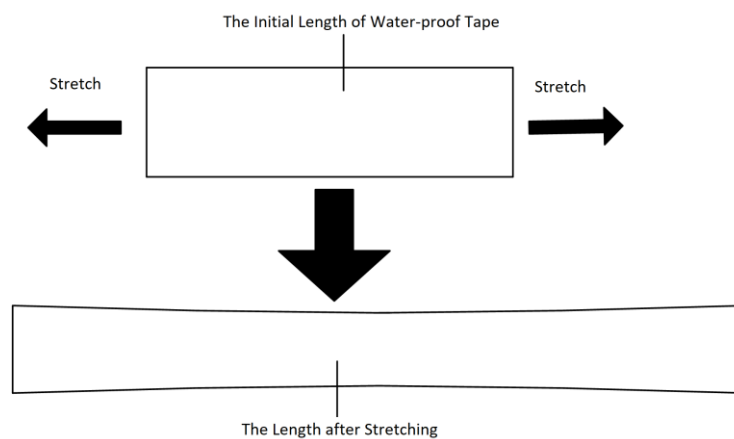


Figure 2-12 Stretch Water-Proof Tape

3. The tensioned waterproof tape is applied to the wiring terminal and the cables nearby. Keep the tape tight during the winding.

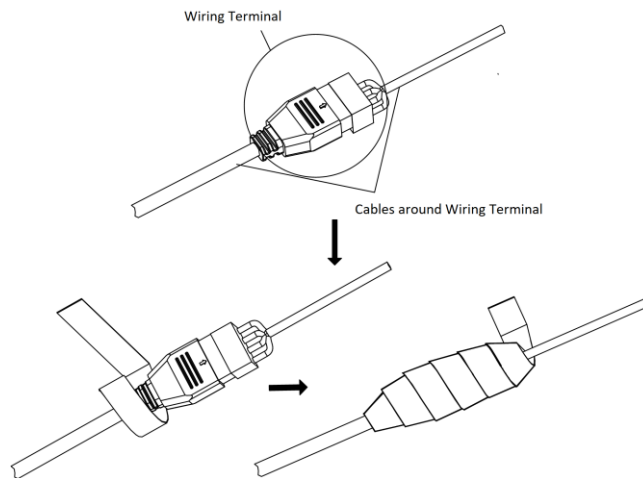


Figure 2-13 Wrapping Water-pool Tape

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

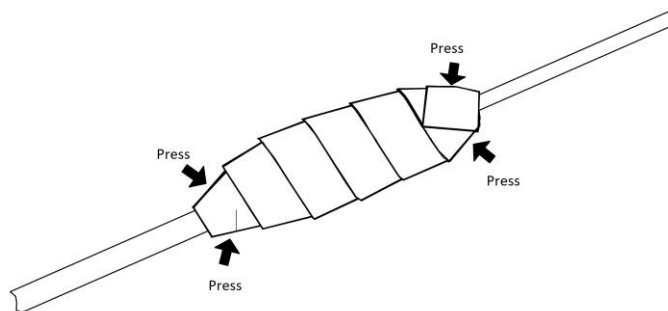


Figure 2-14 Pressing Water-proof Tape

2.2.5 Installing Network Port Waterproof Sleeve

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

Prerequisite

Set up the cable first.

Steps

1. Thread the cable through the screw cap and the waterproof sleeve body.
2. Open the water-proof glue ring and connect the cable between the body of the water-proof sleeve and the screw cap.
3. Insert the O-shaped glue ring into the network port, and insert the network cable into the network port.
4. Align the gap between the network port and the snap of the water barrier body, and connect the water barrier body to the network port, and turn it clockwise.
5. Put the water-proof glue ring into the body of the water-proof hat.

6. Rotate clockwise to fasten the screw cap, and press the water-proof glue ring.

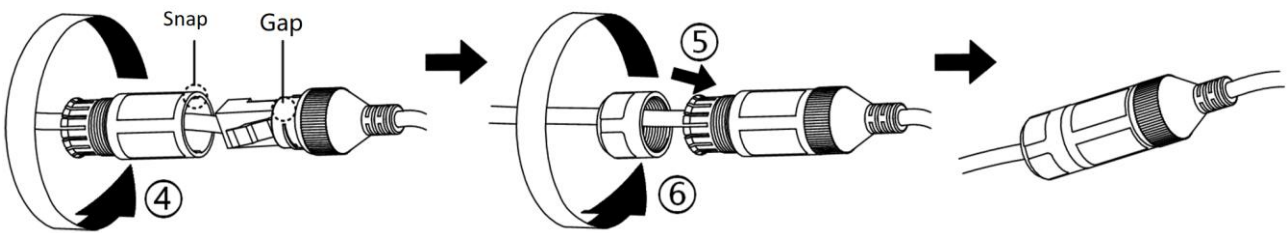


Figure 2-15 Installed

Chapter 3 Pre-Use Operation Information

3.1 Network Connection



Caution

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

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

3.2 Activate Device

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



Note

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

3.2.1 Activate Device via SADP Software

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

Prerequisite

Power on the device and connect to the network.

Steps

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



Caution

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

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

4. Optional: Edit device IP address.

- 1) Select the activated device in the device list.
- 2) Enter IP address, subnet mask, gateway, etc. in **Edit Network Parameter** on the right.



Note

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

3) Enter the password to activate the device after editing, and click **Edit**.

If you are prompted that **Parameters are Edited**, the settings of the IP and other parameters take effect. The device will reboot after network parameters are edited.

3.2.2 Activate via Web Page

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

Steps

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



Note

Device IP address: 192.168.1.64.

3. Enter *192.168.1.64* in the browser, and press Enter to display the activation page.

4. Set device activation password.



Caution

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

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

6. Enter activation password, log in to the device, enter **Configuration → Network → Basic Configuration → TCP/IP**, and change device IP address to make the device IP address in the same network segment as the current network.



Note

See [Set TCP/IP Address](#) to Edit Device Network Parameters.

3.3 Access Device

Provide access method of accessing device via web page and Hik-Connect.

3.3.1 Access Device via Web Client

Login System

Log in to the device's web page, and configure and operate the device through the web page.
Power on the device and connect to the network. Enter the device IP address in the browser address field to log in.



Note

After login, if you pop up the installation browser plug-in interface, please allow installation.

Get Help

You can quickly view and use the device in online help.
Click **Help** to open the online help document and view the operating instructions.

Exit System

If the device is set or operated, you need to exit the device system safely.
Click **Log Out** to exit the device system.

3.3.2 Access Device via Hik-Connect

Devices with Hik-Connect access can view video images and historical videos in real time through Hik-Connect video service. The Hik-Connect alarm service can receive abnormal information of the scene of interest in the first place.

Enable Hik-Connect

Enable Hik-Connect via SADP or web page.

Enable Hik-Connect via SADP

Enable Hik-Connect via SADP software.

Prerequisite

Get SADP software via official website and install.

Steps

1. Open SADP software.
2. Select the device to enable Hik-Connect.
 - Select inactive device. Select Hik-Connect to *use* Hik-Connect to set the verification code to enable Hik-Connect.

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

Enable Hik-Connect via Web Client

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

Steps

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

Access Server IP Address

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

Custom means you can set domain name server address manually.

Verification Code

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



Note

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

5. Click **Save**.

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

Add Device to Hik-Connect Video Mobile Client

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

Prerequisite

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

Steps

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



Caution

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

Hik-Connect - for End user



Scan QR Code to Download

Figure 3-2 Hik-Connect Video QR Code (For Android)

Hik-Connect - for End user



Scan QR Code to Download

Figure 3-3 Hik-Connect Video QR Code (For iOS)

Note

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

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

Note

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

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

Chapter 4 Key Functions Configuration Description

4.1 Fireworks Detection Function

After configuring the function of fire detection, the device can detect whether there is fire or fire in the picture, alarm for fire and fire detection, and link the configured linkage actions.

Configure Entrance

Log in to the device web page and go to **Configuration → Event → Smart Event → Fireworks Detection**.

Configuration Method

See [Configuring Fire and Fire Detection](#) for detailed configuration method.

4.2 Temperature Measurement Function

It is used for real-time temperature measurement of the site. When there is target triggering the configured temperature measurement rule, temperature measurement and alarm will be performed, and alarm actions can be linked.

Temperature Measurement Configuration Notes

- The target surface should be perpendicular to the optical axis. It is recommended that the angle of the angle of the angle should be no more than 45°.
- Target imaging pixel should be no less than 5 × 5.

Configure Entrance

Log in to the device web page and go to **Settings → Temperature Measurement**.

Configuration Method

Select the configuration method of temperature measurement rule according to actual needs: normal temperature measurement or expert temperature measurement.

- Normal temperature measurement: When temperature measurement is applied to the whole picture, the device will recognize the target temperature in the picture according to the configured temperature measurement parameter and set alarm action when triggering temperature alarm.
- Expert temperature measurement: The temperature measurement rule (such as temperature measurement range limit, detailed temperature measurement rule, etc.) should be refined according to actual needs. Select the temperature measurement rule, and the device will identify the corresponding target temperature in the area and set alarm actions when triggering temperature alarm.

See **Normal Temperature Measurement / Expert Temperature Measurement** for details.

Chapter 5 Web Client Configuration and Operation

5.1 Live View

Click to select a live view, and double-click a channel in the channel list on the left to view the live view of the channel in the selected live view.

- In the channel list, you can quickly record and switch channel stream type.



Note

Camera 01 is the visible light channel; Camera 02 is the thermal imaging infrared channel.

- In the live view page, you can control functions such as live view, video recording, picture capture, and audio suppression.
- Select display mode according to the user's actual needs.
- Select stream of live view.



Note

The following features are included in the live view page.

Table 5-1 Icon Function Description

Icon	Function Description
	Select the number of live view pictures. Respectively up to 1 channel and 4 channel live view can be displayed.
	Select the picture size during live view. 4:3, 16:9, original size, original scale, and adaptive display respectively.
	Select stream type during live view. Main stream, sub-stream, and third stream are respectively represented.
	Enable two-way audio button or two-way audio is in progress.
	The pixel value for quick measurement of drawn area height and width. Click the button to draw an area frame in the live view. The left side of the button will display the pixel value of the area's box width and height.

Icon	Function Description
	Enable and disable live view.
Mute	Disable the alarm signal of the device.
	Capture picture during live view.
	Enable and disable local recording during live view.
	Enable and disable digital zoom. Drag the left mouse button to zoom in.
	Switch live view channel.
	Adjust live view volume.
	Display full screen. Click esc to exit the full screen.

5.2 Video Playback

The playback interface provides searching, playback, and downloading of video files stored in the device.

Steps

1. Click **Playback** to enter the video playback page.

Note

Picture division supports 1 and 4 divisions. When using 4 divisions, multi-channel video playback can be played simultaneously.

2. Select the channel and recording date. Click *Search to find* the video file on the timeline.
3. Select playback time.
 - Drag the time axis to the location to play, and click  to start playback.
 - If playback is required, set *the playback time point in the playback time point positioning window*, and click , and the video will go to the set time.

Note

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

4. Optional: During video playback, you can start/stop playback, stop playback, slow down, reverse playback, capture, video clip, zoom in, adjust volume, and download via the function button below the video.

Note

- The capture file is stored in the capture saving path set in **Parameter Configuration → Local Configuration**.
- The clip record file is stored in the clip saving path set in **Parameter Settings → Local Settings**.
- The downloaded video files are stored in the downloaded saving path set in **Parameter Settings → Local Settings**.

5.3 View Picture

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

Prerequisite

To view the picture file of the event alarm, set the linkage mode in the **Event** first. Detailed method: Go to **Configuration** → **Event**, and enter the corresponding event configuration interface (e.g., **Motion Detection**). Click **Linkage Configuration** and select **Upload FTP/SD card/NAS**.



Note

The linkage mode configuration interface will display the specific upload location according to the picture storage mode supported by the current device. When the device supports the storage mode of the microSD card, the **upload SD card** will be displayed only.

Steps

1. Click **Picture** to enter the picture search page.
 2. Set the search condition on the left side of the window, select the picture type and time, and click **Search** to list the picture on the right.
 3. Optional: Select the picture file to download to local. Click **Download** to download the picture.
-



Note

Click **Stop Download** to end the download.

Result Description

The downloaded picture is stored in the downloaded saving path of the visit set in **Parameter** → **Local Configuration**.

5.4 Parameter Configuration

5.4.1 Local Configuration

Enter **Configuration** → **Local** to configure the following parameters.



Note

The parameters that the device may support are described below. The parameters can be configured according to the actual interface.

Playing Parameters

Protocol Type

Set according to actual situation.

Playing Performance

Set according to actual playing requirements.

Display Rule Information

Display rule information of intelligent rule in live view.

Auto Enable Live View

Select **Yes** to automatically display real-time pictures of all channels when you enter the interface of **live view**.
Select **No** to enter the channel of **live view** and preview as needed.

Capture File Format

Set the saving format of captured pictures.

Temperature Measurement Information Display

Select **Yes** to display temperature measurement information in the area triggering temperature alarm rule (e.g., highest temperature, lowest temperature, average temperature, etc.); when selecting **No**, the temperature measurement information will not be displayed in the live view.

Capture Rule Information

Select **Yes** to overlay rule information when capturing picture.

Video File

Video File Package Size

The size of a single video file stored locally.

Video File Saving Path

The video file is stored in the local path. Click **Browse** to change the path. Click **Open Folder** to open the folder in the archive path.

Download and Save Playback Path

The downloaded video file or picture will be stored in the local path. Click **Browse** to change the path. Click **Open Folder** to open the folder in the archive path.

Capture and Clip

Live View Capture Save Path

The captured picture will be stored locally during live view. Click **Browse** to change the path, and **Open Folder** to open the folder under archive path.

Saving path for playback capture.

The captured picture will be stored locally during playback. Click **Browse** to change the path, and **Open Folder** to open the folder under archive path.

Playback Clip Saving Path

When playing back, the edited video files will be stored locally. Click **Browse** to change the path, and *open* the folder under archive path.

5.4.2 System Parameters

System Settings



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

View Basic Device Information

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

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

Set Device Time

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

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

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

NTP Time Sync

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



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

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

Manual Time Sync

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

Set RS-485 Parameters

RS-485 can be used to access control devices that support RS-485 communication protocol.

Prerequisite

Access control device through RS-485 interface.

Steps



When the device has no RS-485 interface, the interface will not be displayed on the web page, and parameters are not required.

1. Go to **Configuration** → **System** → **System Settings** → **RS-485**.
 2. Set RS-485 parameters to make the control device consistent with the device's computer parameters.
 3. Click **Save**.
-

About Device

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

System Maintenance

Upgrade and Maintenance

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

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

Reboot Device

Click **Reboot** to restart the device.

Restore Default Value

Simple Restore

Simply restore device parameters, except IP address, subnet mask, gateway, user information, format, and security question.

Restore All

Restore device parameters to factory settings.

Export Information

Device Parameters

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

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

Import Parameter

Device Parameters

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

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

Upgrade

Upgrade File

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



Caution

The device will reboot automatically after upgrading. Do not power off during upgrading.

Search Log

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

Steps

1. Go to **Configuration → System → System Maintenance → Log**.
 2. Select log type, set date and start/end time of log search, and click **Search**.
The results will be displayed in log list.
-



Note

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

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



Note

The log saving format is Text.files and Excel.files.

Search Security Audit Log

It is used to search and manage device security logs.

Steps

1. Go to **Configuration → System → System Maintenance → Security Audit Log**.
2. Set log type, start time, and end time.
3. Click **Search**.
The log list shows all the logs that meet the search condition.
4. Optional: Click **Export** to save the log to the computer.

Security Management

Set Authentication Mode

Set RTSP authentication.

You can select the authentication mode as “digit” or “digit/basic”. The information to be carried by different

modes of authentication is different. Please refer to the protocol for details.



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

Set IP Address Filter

Used to set access permission of computer or terminal.



IP address refers to IPv4 address.

Steps

1. Go to **Configuration** → **System** → **Security Management** → **IP address Filter**.
2. Select **Enable IP Address Filtering**.
3. Set IP address filtering mode.

Table 5-2 Function Description

Function	Description
Prohibited	Access device is allowed for other IP addresses except those in the list.
Allowed	Only IP address in the list can access the device.

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

Set Security Service

Configure SSH and invalid login lock functions.

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

Enable SSH

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

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



The function is disabled by default after rebooting.

Enable Invalid Login Lock

Enable the function. Enter user name or password at login to the upper limit (seven times, and 5 times after

SSH is enabled). The device will be prompted with lock information and will automatically enter lock status.



Caution

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

User Management

Add User

The administrator user adds operator or normal user, and assigns permission to the user. Up to 31 users can be created.

Steps

1. On the device web page, go to **Configuration → System → User Management → User Management**.
 2. Click **Add**.
 3. Set user name and password, select user type, and confirm password.
-



Caution

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

4. Select permission for the user according to needs.
5. Click **OK** to add the user.

Edit User

Administrator user can change user password, and can change operator and normal user information and permission. Operator and normal user can only change user password.

Steps

1. On the device web page, go to **Configuration → System → User Management → User Management**.
2. Select the user in the user list and click **Edit**.
3. Edit user information.
4. Click **OK**.

Delete User

The administrator can delete the added operator user and normal user.

Steps

1. On the device web page, go to **Configuration → System → User Management → User Management**.
2. Select a user to delete in the user list, and click **Delete**.
3. Pop up prompt to delete the user. Click **OK** to delete the user.

View Online User

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

Go to **Configuration → System → User Management → Online User** to view all user information logged in to the

device, including user name, user type, IP address, and user operation time. Click *Refresh* to refresh current user information.



Caution

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

5.4.3 Network Parameters

Set TCP/IP address

TCP/IP is the most basic transmission control protocol of the Internet. The device used for network monitoring should be configured with TCP/IP for normal use.

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



Note

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

NIC Type

Select according to network environment.

IPv4 Address

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



Note

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

MTU

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

Multicast Address

After multicast address is entered, device data can be sent to multiple devices.

DNS Server Configuration

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

Configure DDNS Parameters

DDNS (Dynamic Domain Name Parsing) is used to access the device. It can map the device's dynamic IP address

to a fixed domain name parsing server to solve network device Internet access problem.

Prerequisite

- The device can be accessed normally in the LAN.
- Get the installation package of client software and IP Server server through the official website, and install IP Server on the computer of public network. Client software is installed on the computer to be monitored.

Steps

1. Set DNS parameters. See *TCP/IP address for details*.
2. Go to **Settings → Network → Basic Settings → DDNS**.
3. Select **Enable DDNS**.
4. Set IP Server Address.
5. Click **Save** to complete the settings.

Result Description

Access device using client software or browser.

- Access via browser: Enter domain name and port No. in browser address field.
- Client software: Add domain name and access device in client software. See Client Manual for details.

Configure Port Parameters

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



Caution

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

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

HTTP Port

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

RTSP Port

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

HTTPS Port

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

Service Port

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

Set Platform Access Function

Platform access function is mainly configured with access 28181 platform, ISUP platform, and Hik-Connect platform.

- 28181 access refers to registering device to public security network platform according to GB/T28181, controlling device through public security network platform, and enabling audio on demand and audio

playback.

- ISUP access means the ISUP platform is accessed.
- Hik-Connect access supports Hik-Connect access device to register to Hik-Connect platform and access via Hik-Connect.

Access Public Security Network Platform

Register device to public security network platform according to GB/T28181 requirements, and realize functions such as remote real-time monitoring and device management.

Steps

1. Go to **Settings** → **Network** → **Advanced Settings** → **Platform Access**.
2. The platform access mode is *28181*.
3. Select **Enable**.
4. Set the parameters of 28181 according to the 28181 protocol. You can find the related information of the protocol and configure it.
5. Click **Save**.

Access ISUP Platform

Register device to ISUP platform according to ISUP platform requirements, and realize functions such as remote real-time monitoring and device management.

Steps

1. Go to **Settings** → **Network** → **Advanced Settings** → **Platform Access**.
2. The platform access mode is *ISUP*.
3. Select **Enable**.
4. Set ISUP parameters.
5. Click **Save**.

Refresh web page or restart device to check registration status.

Hik-Connect

Hik-Connect is the micro-video service platform of Hik-Connect. Devices with Hik-Connect access support can be accessed through Hik-Connect.

Steps

1. Go to **Settings** → **Network** → **Advanced Settings** → **Platform Access**.
2. Select **Hik-Connect**.
3. Select **Enable**.
4. Select **Custom** or **Default** for **Access Server IP Address**.
 - Custom: Set domain name server IP address manually.
 - Default: The device will automatically assign a server IP address of the nearby area.
5. Click **Save**.



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

Set HTTPS

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

Steps

1. Go to **Settings** → **Network** → **Advanced Settings** → **HTTPS**.
2. Create and install certificate.

Table 5-3 Function Description

Function	Description
Create Private Certificate	Select to create private certificate in installation mode. Click Create to open private certificate creation window, enter parameters such as country, domain name/IP address, validity period, and click OK .
Create Certificate Request	Select to create certificate request first, and then continue to install. Click Create to open license certificate creation window, enter country, domain name/IP, and click OK to complete the request. After receiving the valid certificate, you can download or delete the certificate request, or install the applied security certificate.
Install Signed Certificate	Select the already signed certificate in the installation mode. Install it directly. Click Browse to select the existing signed certificate, and click Install . Click Save when finished.
Download Certificate	After creating the certificate request, click Download to download the certificate and send to the authentication authority for authentication.
Delete Certificate	You can view the installed certificate. Click Delete to delete the current certificate.

3. Select **Enable** to access the device via HTTPS protocol.
4. Optional: Select **Auto Redirect to HTTPS** to automatically convert the input IP address to HTTPS address to improve network security.
5. Click **Save**.

Note

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

Configure Open Network Video Interface

Connect device via open network video interface protocol to enhance device network security.

Steps

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

5.4.4 Video Audio Parameters



The content in the audio parameter settings will be determined according to the actual device. The following settings are supported by the device.

Video Configuration

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

Go to **Settings → Audio → Video** to configure video parameters.



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

Channel No.

Select the channel No. to set video parameters.



Only multi-channel devices have this option.

Stream Type

Main Stream (Timed)

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

Sub-Stream

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

Video Type

Video Stream

Video stream only.

Composite Stream

Thermal Heat Fire Detection Camera User Manual

Including video stream and audio stream.

Resolution

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

Bitrate type and bitrate upper limit.

Fixing Rate

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

Bit Change Rate

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

Image Quality

When the bit rate is variable bit rate, you can set the image quality. Select according to the customer's requirements for image clarity. The higher the image quality, the higher the bandwidth requirement.

Video Frame Rate

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

Video Encoding

H.264

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



Caution

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

Smart264

Smart264 is a encoding mode that can further improve compression performance and reduce storage space. Smart264 is supported *when the video code is H.264*. Restart the device when Smart264 is enabled or disabled. After enabling Smart264, image quality, I-frame interval, encoding complexity, and SVC parameters will not be allowed.



Note

After enabling Smart264, the average bit rate will be displayed. The system will automatically give the recommended average bit rate according to the upper limit. In complex monitoring scenes, when the image quality of the default average bit rate is poor, you can set it manually to increase the average bit rate parameter value. The upper limit of the parameter value should be less than the upper limit.

H.265

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

Smart265

Thermal Heat Fire Detection Camera User Manual

Smart265 is a encoding mode that can improve compression performance and reduce storage space. The Smart265 function is only supported when video encoding H.265 is enabled or disabled. Reboot the device. After enabling the Smart265 function, the image quality, I-frame interval, encoding complexity, and SVC parameters will be unavailable.



Note

After Smart265 is enabled, the average bit rate will be displayed. The system will automatically give the recommended average bit rate according to the upper limit. In complex monitoring scenes, when the image quality of the default average bit rate is poor, you can set it manually to increase the average bit rate parameter value. The upper limit of the parameter value should be less than the upper limit.

MJPEG

MJPEG is a video encoding/decoding technology. The compressed image quality is good, and there is no mosaic in the event of image change.

Encoding Complexity

The higher the encoding complexity under the same bitrate, the higher the image quality, but the higher the network bandwidth requirements.

I Frame Interval

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

SVC

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

Stream Smoothing

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

Intelligent Information Display Mode

Playing Library

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

Video

When other players are supported to play video, the intelligent rule information will be displayed in other players.

Audio Configuration

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



Note

- When the device has no audio interface, the interface is not available on the web page.
-

Thermal Heat Fire Detection Camera User Manual

- The audio parameters that the device may contain are described below. The configuration that the device supports is subject to the actual interface of the device.
-

Channel No.

Select the channel No. to set audio parameters.



Note

Only multi-channel devices have this option.

Audio Encoding

Select audio encoding type according to actual usage requirements.

Audio Input

Please connect audio input device according to usage requirements and configure audio input parameters.

- Select audio input as *LineIn* when connecting to *LineIn device*.
It means that the device is connected to devices with high audio output power (such as MP3, synthesizer, and active voice collector).
- Connect *MicIn* device to select *MicIn as the audio input*.
It means that the device is connected to a device with low audio output power (such as microphone and other passive audio input devices).

Input Volume

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

Output Volume

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

Environment Noise Filter

When the monitoring environment is relatively tedious, you can turn on environment noise filtering function. You can filter the environment noise to reduce the noise after filtering.

Configure ROI

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

Prerequisite

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



Note

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

Steps

1. Go to **Configuration** → **Audio View** → **ROI**.
 2. Select **Stream Type**.
 3. Optional: Configure fixed area to be upgraded.
 - 1) Check **Enable**.
 - 2) Select area No. in **Fixed Area** to draw area of interest.
-

Thermal Heat Fire Detection Camera User Manual

3) Click **Draw Area** to select a fixed area on the live view with the mouse, and click **Stop Drawing**.



Note

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

4) Set upgrade level and area name.



Note

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

5) Optional: Repeat steps 2 to 4, and draw multiple areas.

4. Click **Save**.

5.4.5 Image Parameters

Set Display Parameters

Enter **Configuration → Image → Display Settings** to set the image quality of the main live view.



Note

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

Channel No.

Select the channel No. to set audio parameters.



Note

Only multi-channel devices have this option.

Installation Scene

Please select suitable scene according to the device's actual installation environment and usage conditions. After selecting the corresponding scene, the default parameters of the image will be matched accordingly.

Image Adjustment

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

Exposure

Optical Circle Type

Manual by default.

Exposure Time

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

mode is used, the time set here is the longest exposure time.

Exposure

Adjust the zoom in of video signal. The larger the gain, the more obvious the image noise.

Day/Night Conversion

Day/Night Conversion

Auto

In auto mode, the device will automatically switch between daytime mode and night mode according to external environment brightness.

Daytime

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

Night

When in night mode, the supplement light can be enabled, and the parameters of supplement light can be set. The device image is forced to night, and will not be switched to day or night according to actual scene.

Timed Switch

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



Note

The start time and end time can be set to the next day *when* switching time. Please use the device.

Alarm Input Triggered

In the alarm input triggering mode, the open triggering status can be selected as day and night. If the alarm input status of the user is remaining open, the device will remain in the day status. When the alarm input is closed, the device will switch to night status. The option is controlled by the combination of the two.

Sensitivity

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

Filter Time

When the conversion mode *is* auto, the corresponding conversion filter time will be between 5 and 120 seconds. Switching between day and night will take place when the environment light meets the requirements and the retention time exceeds the set threshold time.

Anti-Refining Over-Exposure

Intelligent image processing technology is used to prevent the center area from being exposed to light supplement. The function is invalid when the supplement light is disabled. Select Enable or Disable according to the actual environment.

Supplement Light Mode

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

White Light Mode

White light supplement light will be enabled.

Mixed Light Supplement

White light and IR supplement light will be enabled.

Close

Disable supplement light.

Brightness Mode

Set the brightness mode and brightness when supplementing light.

Auto

Adjust the brightness automatically according to the brightness of the current channel, and turn on the supplement light automatically when the image reaches a certain darkness.

Manual

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

Backlight

Backlight Compensation Area

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

Width Dynamic

Wide dynamic is used for monitoring environment with large difference in light intensity. When the areas with high brightness under strong light source (such as sunlight, lamps, or reflective light) and areas with relatively low brightness, such as shadows and inverse light, can enable the function of wide dynamic and adjust the level to clear the picture.

The brightest and darkest in the video will be automatically balanced in a wide dynamic to see more details.



Note

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

Strong Light Suppression

When there is excessive exposure of bright area and under-occupied dark area, it will enable strong light suppression, weaken bright area, and highlight dark area to achieve the light balance of the whole picture.

White Balance

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



Note

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

environment of around 5500 K.

Image Enhancement

Digital Noise Reduction

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

Normal Mode

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

Expert Mode

It can be adjusted by two dimensions: air domain noise reduction level and time domain noise reduction level.

Grayscale Range

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

Video Adjustment

Optimize image display by setting video adjustment parameters.

Mirror

You can adjust video by mirror image as needed. You can select center, left, right, and up or down mirror image to adjust. You can also disable mirror image. When the image is inverted, you can flip the image through the menu.



Caution

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

Rotate

Enable and disable the function. After enabling the function, video encoding will rotate 90° clockwise, e.g., 1280 × 720 is rotated to 720 × 1280. It is suitable to monitor the valid range of vertical direction, e.g., corridor, road, etc. when the camera is rotated.

Video Format

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

Set OSD Parameters

OSD refers to the information displayed on the camera. The camera can display device name, date, week, channel information, and superimposed characters.

Go to **Configuration** → **Image** → **OSD** and select **Channel No.** to set the corresponding parameters for the channel.

The settings will take effect after saving.



Only multi-channel devices can select channels. Single-channel devices do not need to be selected. Set OSD parameters directly.

Basic OSD Information Settings

- Select the OSD information to display: Select *the display name, date, and week*, and the corresponding OSD information will be displayed on the live view.
- Edit OSD information display location: Drag the OSD red box on the live view to move to the location you want to display.
- Edited display format: In **the channel name/time format/date format**, you can edit the channel name displayed on the live view and the time and date format.

OSD Attribute Settings

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

Overlay Custom Characters

The device can overlay multiple characters to the video monitoring screen. Check and set the required characters. The characters in the screen will be red font. Drag the characters or set **the alignment mode** to adjust the displayed characters to the required position. Click *Save* to finish the settings.



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

Set Video Tampering

Video masking refers to covering sensitive areas in the surveillance image and not displaying them in the image.

Steps

1. On the device web page, go to **Configuration → Image → Video Masking**.
2. Select **Enable Video Masking**.
3. Click **Drawing Area**, click the left mouse button in the picture, drag the mouse, and release the left mouse button to draw an area.



Up to 4 areas can be drawn in the picture.

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

5.4.6 Event and Alarm

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



The event functions supported by the device are described below. Please use the function supported by the actual device.

Schedule and Linkage Configuration

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

Set Arming Time

Set the start time and end time of task execution.

Steps

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



8 time periods are supported in one time axis.

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

Click to Delete Time Period Delete current time period.

Click to Delete Delete the selected time period.

Click to Delete All Delete all time periods.

Click to copy to... Copy the same schedule to other time.

4. Click **Save**.

Linkage Configuration

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

The linkage mode that the device may support is described below. Please configure the linkage mode according

to available options on the actual device interface.

Normal Linkage

Email Linkage

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

Please go to **Settings** → **Network** → **Advanced Settings** → **Email Parameters** to configure the email.

Upload Center

Select **Upload Center** to upload alarm information and pictures to remote central platform when alarm occurs.

Upload center configuration is done in **Configure** → **Network** → **Advanced Settings** → **Platform Access**.

Upload FTP/SD Card/NAS

If you select and configure the FTP/NAS/SD card, the alarm information can be sent to the FTP server, network HDD, and microSD card for saving when alarm is triggered.



Note

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

- FTP Settings: **Configure** → **Network** → **Advanced Settings** → **FTP Settings**.
 - NAS configuration: **Configure** → **Storage** → **Storage Management** → **Network HDD**.
 - SD card configuration: **Configure** → **Storage** → **Storage Management** → **HDD Management**.
-

Flash Alarm

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

Sound Linkage

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

Linkage Alarm Output

A->No.

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

Buzzer

When the alarm is triggered, the buzzer will sound alarm.

Voice Broadcast

When alarm is triggered, the corresponding event alarm is broadcasted.

Video Linkage

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

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

Configure Normal Event

Describe the basic event configuration of the device.



The event types supported by the device are described below. The actual event types will be determined according to the actual interface.

Configure Motion Detection

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

Steps

1. Go to **Configuration → Event → Normal Event → Motion Detection**.
2. Select **Enable Motion Detection**.
3. Optional: Set the moving object in the picture to green to highlight.
 - 1) Check **Enable Dynamic Analysis**.
 - 2) Go to **Configuration → Local** and select **Rule Information** to *enable*.
4. Select **Configuration Mode** to set rule area and rule parameter.
 - See [Normal Mode](#) for details.
 - See details in [Expert Mode](#).
5. Set arming time and linkage mode. See [Schedule and Linkage Configuration](#).
6. Click **Save**.

Normal Mode

Set motion detection according to device default parameters.

Steps

1. Select **Normal Mode** in configuration mode.
2. Set normal mode sensitivity parameters. The higher the sensitivity value, the higher the sensitivity of motion detection. If sensitivity is set to 0, motion detection and dynamic analysis will not work.
3. Click **Draw Area**, hold down the left mouse button in the live picture, drag the mouse, and release the left mouse button to draw an area.

Click to **stop drawing**. End area drawing.

Click **Clear All** Delete the drawn area.



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

Expert Mode

Customize movement detection parameters for daytime and nighttime.

Steps

1. Select **Expert Mode** in configuration mode.
2. Set Expert Mode Parameters.



Note

The parameter configuration items that the device may support are listed here. The parameter items that can be configured will be subject to the actual interface.

Day/Night Parameter Conversion

Close

It means that day or night switch is not allowed.

Auto Switch

The system will automatically switch between daytime and nighttime mode according to changes in environment. The picture of daytime mode is color, and the picture of nighttime mode is black and white.

Timed Switch

Switch according to the set time. The time period is day mode, and the time period is night mode.

Sensitivity

The higher the sensitivity value, the higher the sensitivity of motion detection. If sensitivity is set to 0, motion detection and dynamic analysis will not work.

Ratio

When moving object as a percentage of the area you draw, mobile detection will be triggered when the object exceeds the set percentage.

3. Select an area, click **Draw Area**, click the left mouse button in the live view, drag the mouse, and release the left mouse button to draw an area.

Click to stop drawing. End area drawing.

Click Clear All Delete the drawn area.

Configure Tampering Alarm

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

Steps

1. Go to **Configuration → Event → Normal Event → Block Alarm**.
2. Select **Enable**.
3. The sensitivity is set. The higher the sensitivity value, the more sensitive the detection.
4. Click the **drawing area**, click the left mouse button in the live picture, drag the mouse, and release the left mouse button to draw an area.

Click to stop drawing. End area drawing.

Click **Clear All**

Delete the drawn area.

5. Set arming time and linkage mode. See [Schedule and Linkage Configuration](#).

6. Click **Save**.

Configure Alarm Input

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

Prerequisite

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

Steps

1. Go to **Configuration → Event → Normal Event → Alarm Input**.
2. Select alarm input No. and alarm type to customize alarm name.



Note

Set alarm type according to the connected alarm device.

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



Note

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

6. Click **Save**.

Configure Alarm Output

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

Prerequisite

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

Steps

1. Go to **Configuration → Event → Normal Event → Alarm Output**.
2. Select **Alarm Output No.** to set its delay and alarm name.



Note

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

3. Set arming time. See [Schedule and Linkage Configuration](#).
4. Optional: Click **Copy to** to Copy the alarm output settings to other alarm output channels.



Note

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

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

Configure Exception Alarm

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

Steps

1. Go to **Configuration → Event → Normal Event → Exception**.
2. Select **Exception Alarm Type**.
3. Set linkage mode. See [Schedule and Linkage Configuration](#) for linkage mode settings.
4. Click **Save** to finish the alarm configuration.

Configure Flash Alarm Light Output

Configure the device flash alarm output mode. If the event is triggered when the flash alarm linkage mode is enabled, you can set the flash alarm on the device to warn.

Steps

1. Go to **Configuration → Event → Normal Event → Flash Alarm Output**.
2. Set output parameters.

White Light Mode

Remain Bright

The flash light will remain on during the output.

Flashing

Flash light flashes during output.

Delay Time

After the event of the linked flash alarm disappears, the time of the flash light is disabled.

Flashing Frequency

When the mode is flashing, you can select the flashing frequency. The higher the frequency, the faster the flashing speed.

Brightness

Set the flash brightness.

3. Set arming time. See [Schedule and Linkage Configuration](#).
4. Click **Save**.

Wrap-Up

Enable the event configuration interface of flash alarm, enter *linkage mode*, and select *Flash Alarm*.

Configure Smart Event

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

linkage action.



Note

The event types supported by the device are described below. The actual event types will be determined according to the actual interface.

Configure Area Intrusion Detection

Area intrusion detection is used to detect whether target has entered the alarm area. This function allows the user to build up to 4 four four-sided alarm zones. When target object enters the area, the device can generate alarm signals and interact with each other.

Steps

1. Go to **Configuration → Event → Smart Event → Area Intrusion Detection**.
2. Select **Enable**.
3. Draw the min. size.
 - 1) Click **Max. Size/Min. Size**.
 - 2) Select a point in the live view as start point, and drag to the left mouse button to draw the max. size filter frame/min. size filter frame.
 - 3) Optional: If you need to re-map the filter frame, click **Max. Size/Min. Size** again to draw again.
If there is an object entering the warning area and the object size is within the range of max. and min. size, it can be recognized as the target. Otherwise, it is not the target.
4. Set the alarm area.
 - 1) Select a **Warning Area**, and click **Detection Area**.
 - 2) Click the mouse to select four vertices in the live view to draw the four-way detection area.
 - 3) Optional: Click **Clear** to clear the drawn area.
 - 4) Optional: Repeat child steps 1 to 3. Up to 4 alarm areas can be set.
5. Set alarm parameters.

Time Threshold

It means that the target enters the warning area. The time spent in the area will be exceeded. Alarm will be generated. The larger the time threshold, the longer the target will remain in motion in the detection area. For example, set to 0. The alarm will be triggered immediately after the target intrusion area. Up to 10 seconds are allowed.

Sensitivity

It indicates the degree to which the target enters the arming area. The greater the sensitivity, the easier the alarm will be triggered.

Detection Target

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

6. Set arming time and linkage mode. See [Schedule and Linkage Configuration](#).
7. Click **Save**.

Configure Cross-Border Detection

Line crossing detection is used to detect whether the target crosses the alarm plane in the specified direction. If the target crosses the alarm plane in the specified direction, the device will be triggered to execute linkage action.

Steps

1. Go to **Configuration → Event → Smart Event → Border Crossing Detection**.
2. Select **Enable**.

3. Draw the min. size.
 - 1) Click **Max. Size** or **Min. Size**.
 - 2) Select a point in the live view as start point, and drag to the left mouse button to draw the max. size filter frame or min. size filter frame.
 - 3) Optional: If you need to re-map the filter frame, click **Max. Size** or **Min. Size** again to draw again.
If there is an object entering the warning area and the object size is within the range of max. and min. size, it can be recognized as the target. Otherwise, it is not the target.
4. Set alarm level.
 - 1) Select a **Warning Surface**, and click **Detection Area**. A line segment with arrow will appear in the picture.
 - 2) Click the selected line segment to drag the vertex to edit the line segment length and position, or click **Drag** to move the line segment in parallel.
 - 3) Optional: Click **Clear** to clear the drawn area.
 - 4) Optional: Repeat child steps 1 to 3. Up to 4 alarm areas can be set.
5. Set rule parameters.

Detection Target

After the detection target is selected, the device will detect the specific detection target.

Direction

It indicates the direction of the alarm triggered by the target crossing the alarm surface.

A->B

Alarm will be triggered when the target crosses the line from A to B.

B->A

Alarm will be triggered when the target crosses the line from B to A.

A<->B

It means the alarm is triggered by target two-way.

Sensitivity

The sensitivity value = $100 - S1/ST * 100$. S1 is the area of the target entering the arming area. ST is the actual area of the target. The larger the sensitivity settings, the easier the alarm will be triggered.

6. Set arming time and linkage mode. See [Schedule and Linkage Configuration](#).

7. Click **Save**.

Configure Fire and Fire Detection

Fireworks detection is used to detect whether there is fire or fire in the area. When fire or fire is detected and fire alarm is triggered, the configured linkage will be executed.

Steps

1. On the device web page, go to **Configuration → Event → Smart Event → Fireworks Detection**.
2. Select **Enable**.
3. Set detection area and shielded area.
 - 1) Click **Draw Detection Area/Draw Shielded Area**.
 - 2) Click the left mouse button in the picture to draw any convex quadrilateral shape.
 - 3) Repeat steps 1 to 2, and draw up to 4 detection areas/shielded areas.
 - 4) Optional: Edit the drawn area by the following methods.
 - Move the mouse to the area internal. Drag to change the area position.
 - Move mouse to area vertex. Click **Drag** to edit vertex position.
 - Click **Clear All** to delete all drawn areas.

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

in the shielded area.

4. Select channel alarm mode.

Fire and Fire Alarm The channel is detecting smoke and fire.

Fire Alarm The channel is currently detecting fire.

5. Set detection parameters.

Sensitivity

The higher the sensitivity, the higher the alarm will be triggered, and the error recognition rate will increase.

Fire Check

When you select Fire Check, the recognition accuracy will be improved and false alarm will be reduced. For example, an object in the picture is detected as a fire. The actual temperature is too low through the flame verification function, and it can be determined as false alarm and alarm will not be triggered.

6. Set arming time and linkage mode. See [Schedule and Linkage Configuration](#).

7. Click **Save**.

5.4.7 Storage

Recording Schedule

Schedule recording is used to automatically execute recording tasks during the set time period.

Steps

1. Go to **Configuration → Storage → Schedule Configuration → Recording Schedule**.
2. Select **Channel No.** to configure recording schedule for the channel.
3. Select **Enable** to enable recording schedule.
4. Select recording type.



Note

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

Timed

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

Fire Alarm

Camera recording will occur when fire alarm event is triggered.

Motion Detection

Camera recording occurs when motion detection event occurs.

Alarm

It means that alarm input will generate alarm or record when alarm event is recognized.

Dynamic Detection or Alarm

Channel recording can be triggered when any one of the motion detection or switching alarm occurs.

Dynamic Detection and Alarm

Channel recording will be triggered when motion detection and switching alarm occur simultaneously.

Event

Channel recording is triggered only when an event occurs.



The event type should be set in advance for motion detection or alarm and event recording. See [Event and Alarm](#) for details.

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

Repetition Write

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

Pre-Record Time

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

Recording Delay

Delay recording time after recording schedule end time node.

Stream Type

Stream type of video storage.



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

6. Set recording schedule time. See [Schedule and Linkage Configuration](#).

7. Click **Save**.

8. Optional: Click **Copy to** to copy the recording schedule of the channel to other channels.

Format SD Card

First time using the microSD card. Please log in to the device web client to format the microSD card.

Prerequisite

Install the microSD card to the device.

Steps

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



When formatting, the video partition should be no less than 1 GB. Otherwise, the video function will be affected.

4. Click **Format**.



Note

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

5. Click **Save**.

5.4.8 Temperature Measurement

It is used for real-time temperature monitoring of the site. By setting temperature measurement parameter or temperature measurement rule, temperature measurement and alarm will be automatically performed when the target meets the temperature measurement parameter or the temperature measurement rule is triggered.

Set Temperature Measurement Parameters

Realize the configuration of basic parameters of auto temperature measurement.

Steps

1. Go to **Configuration** → **Temperature Measurement** → **Basic Configuration**.
2. Select **Enable Temperature Measurement**.
3. Set temperature measurement parameters.

Stream Overlay Temperature Information

Select to add the detected temperature and temperature detection frame information in stream.

Max. Temperature, Min. Temperature, Average Temperature

Select to display the temperature measurement data of the highest temperature, lowest temperature, or average temperature in the live picture.

Temperature Measurement Unit

Set the unit of temperature measurement.

Temperature Measurement Range

Set the temperature range of the target.

Algorithm Library Version

Check current temperature measurement algorithm library version.

4. Click **Save**.

Normal Temperature Measurement

Normal temperature measurement is used to measure temperature and alarm the whole scene.

Steps

1. Go to **Configuration** → **Temperature Measurement** → **Basic Configuration**, and select **Enable Temperature Measurement**.
2. Set temperature measurement parameters, see [Setting Temperature Measurement Parameters](#) for details.
3. Go to **Configuration** → **Temperature Measurement** → **Advanced Configuration** and select **Configuration Mode** as **Normal Mode**.
4. Set normal mode parameters.

Transmission Rate

The emission rate of the temperature measurement target.

Distance

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

Warning Threshold and Filtering Time

The device will warn when the temperature exceeds the set warning threshold and the duration exceeds the filter time.

Alarm Threshold and Filtering Time

When the temperature exceeds the set alarm threshold and the duration exceeds the filter time, the device will alarm.

Alarm Output and Alarm Output

When alarm or alarm is generated, the selected alarm output channel actions are linked.

5. Click **Save**.

6. Go to **Configuration → Temperature Measurement → Linkage Mode**, set arming time and linkage mode, and save. See [Setting Arming Time](#) for arming time, and Linkage Mode Configuration for [linkage mode](#).

The live view will show the measured temperature of the highest and lowest temperature in real time.

Expert Temperature Measurement

Set the temperature measurement rule in the scene for temperature measurement and alarm.

Steps

1. Go to **Configuration → Temperature Measurement → Basic Configuration**, and select **Enable Temperature Measurement**.
2. Set temperature measurement parameters, see [Setting Temperature Measurement Parameters](#) for details.
3. Go to **Configuration → Temperature Measurement → Advanced Configuration** and select **Configuration Mode** as **Expert Mode**.
4. Set temperature measurement rule.
 - 1) Select a temperature measurement rule, and select **Enable**.
 - 2) Custom rule name in name field.
 - 3) On the configuration screen, drag the vertex to adjust area range. Click and drag the area border to adjust area position.
 - 4) Select **Alarm Rule**, click , and set alarm rule.

Alarm Rule

Set according to actual needs.

Alarm Temperature and Alarm Temperature

Set temperature threshold of alarm and alarm. For example, if the alarm rule is higher than, the alarm temperature is set to 50 °C, and the alarm temperature is set to 55 °C, the alarm will be warned when the detected temperature is higher than 50 °C, and the alarm will be triggered when the temperature is higher than 55 °C.

Filter Time

The measured target temperature should be no less than the alarm threshold temperature or alarm threshold temperature. If the time is exceeded, the alarm or alarm will be generated.

Tolerance Temperature

Set a tolerance temperature to prevent the temperature from shaking back and forth. For example, if the temperature is 3 °C and the alarm temperature is 55 °C, the device will alarm when the detected temperature is 55 °C. If the detected temperature is less than or equal to 52 °C, the alarm will be canceled.

Warning Output

Link selected output channel actions when alarm is generated.

Alarm Output

Link selected output channel actions when alarm is generated.

Recording Period and Change Warning/Alarm Value

When alarm rule is sudden temperature rise or sudden temperature drop, the recording cycle and mutation alarm/alarm value should be set.

The recording period is the previous time period for calculating time point T temperature change. The time period is (T-Recording Period -1 s) to (T-1 s). The highest temperature per second will be recorded in the recording period.

- Time T temperature surge: T temperature - The minimum temperature in T recording cycle should be $\geq$ the threshold of change warning/alarm.
- Time T temperature drop: Max. temperature in T recording cycle - T temperature $\geq$ change alarm/alarm threshold.



Note

After triggering temperature change warning/alarm, the alarm output will be stopped if no temperature surge/drawing occurs in T during the subsequent time.

5. Optional: Set multiple temperature measurement rules by the method above.
6. Click **Save**.
7. Go to **Configuration** → **Temperature Measurement** → **Linkage Mode**, set arming time and linkage mode, and save. See [Setting Arming Time](#) for arming time, and Linkage Mode Configuration for [linkage mode](#).
The live view will show the measured temperature of the highest and lowest temperature in real time.

A. Communication Matrix and Device Command

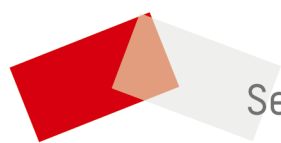
Scan the QR code below to get communication matrix and device command. The communication matrix and device command will be subject to the model and version. The actual device will prevail.



Figure A-1 Communication Matrix



Figure A-2 Device Command



See Far, Go Further