Fire Detection Camera

User Manual

Legal Statement

About this Document

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

About this Product

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

Acknowledgment of Intellectual Property Rights

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

LEGAL DISCLAIMER

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

ABUSES.

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

Introduction

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

Pre-Use Description

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

Applicable Model

Product Name	Product Model
Thermal Imaging Thermal Fire Detector	HF-VR343

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

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

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

risk (ignoring this item may damage the product).

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

Note

Quality Requirements for Installation and Maintenance Personnel:

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

The requirements for lifting devices:

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

CONTENTS

Chapter 1 Product Introduction

1.1 Product Description

It is a composite flame detector that integrates dual-band infrared pyroelectric sensors, AI visual fire hazard recognition, and local audio-visual alarms. It identifies changes in infrared signals and image characteristics of flames in the monitored area, achieving early fire warning and alarm, as well as remote visual verification of fire scenes. It is widely used in key units with fire and security needs, such as hospitals, schools (laboratories, libraries, warehouses, archives), museums, temples, banks (ATM rooms, equipment rooms), production safety workshops, indoor substations, new energy facilities, and oil and petrochemical sites (gas stations).

1.2 Product Function

This section provides information about security and safety cameras. You can get to know and get familiar with the device more quickly.

- New intelligent fusion camera, supporting flame detection by sensing changes in infrared signals around the flame, and capable of video verification.
- Built-in infrared pyroelectric flame detector, further enhancing the accuracy of flame alarms.
- Support AI intelligent detection: Smoke and flame detection, Indoor access blocked alarm, On/off duty alarm, Dangerous goods detection, Dangerous behavior detection, Fire Extinguisher Detection, Area Invasion Detection.
- Equip with local alarm indicators
- The maximum resolution can reach 2560 × 1440@25 fps
- Supports 30m infrared illumination
- Support 3D digital noise reduction and wide dynamic range
- Supports backlight compensation and automatic electronic shutter function, adaptable to various usage environments.
- Supports linkage local alarm indicator lights.
- 1 built-in speaker, 1 built-in microphone, supports two-way voice intercom
- Supports OSD alarm event overlay
- Support access to Hik-Connect
- Support PoE power supply
- Supports DC12V (1W) external power output, for powering smoke, gas, and other sensors
- Supports 2 alarm input/output channels, 1 audio input/output channel
- IP67 dust and water resistant
-

1.3 Appearance Interface

Note

The product picture in this manual is a picture. Please refer to actual device.

Sphere Appearance and Indicator

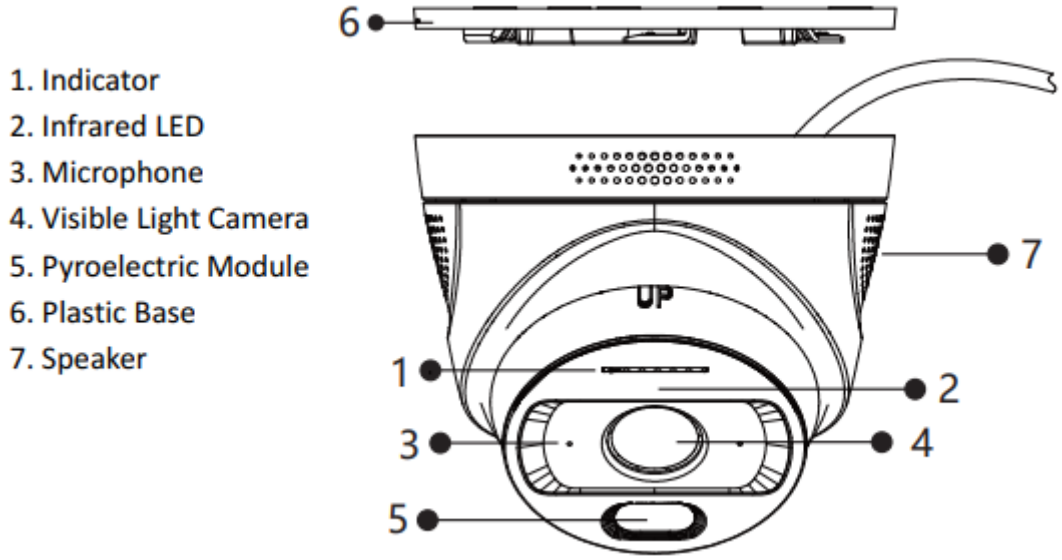

Figure 1-1 Sphere Appearance Figure

Table 1-1 Indicator Description

Indicator	Description
Red Light	Alarm
Green Light	Normal Operation
Yellow Light	Fault

Device Interface Description

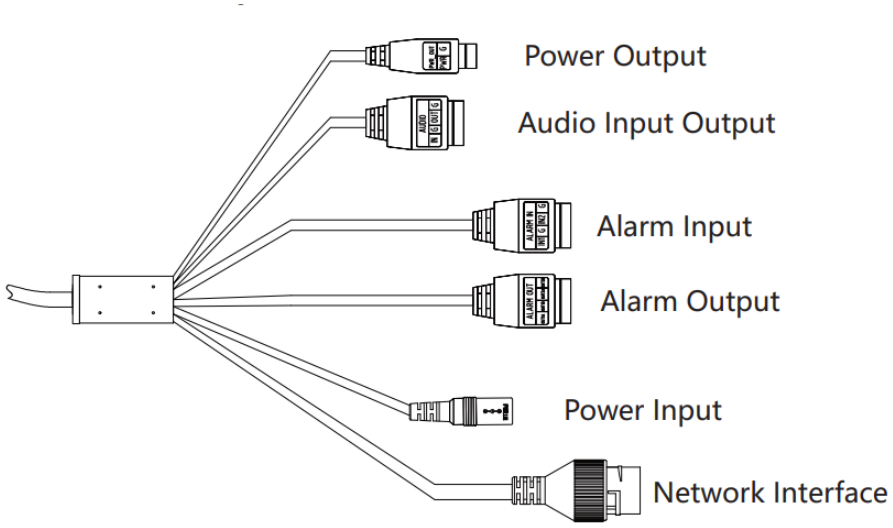

Figure 1 - 2 Device Interface

Power Output

DC 9 to 30 V.

Alarm Input

You can connect to alarm input device.

Alarm Output

The device can be connected to alarm output.

Audio Input Output

Connect audio input and audio output devices.

Network Interface

Network Signal Output

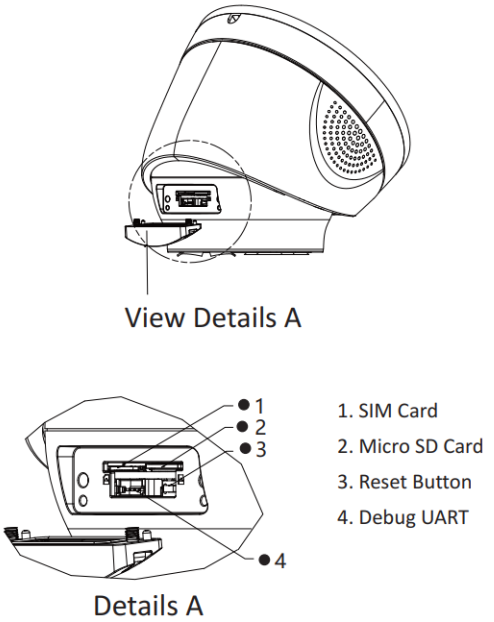

Figure 1 to 3 SD Card Interface

SIM Card/Micro SD Card

You can plug in SIM card (4G version has SIM card slot) and microSD card for local storage.

Reset Button

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

Debug UART

Reserved.

Note

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

Chapter 2 Wiring and Installation

2.1 Product Wiring

The device has six external interfaces, including power interface, audio input/output interface, alarm input interface, alarm output interface, and network interface. The alarm interface wiring and audio wiring are described below.

Table 2-1 Alarm Interface Description

ID	Description	Wiring Description
IN	Connect Alarm Input Signal Positive Pole	One-Way Access Alarm Input Signal
G	Connect Alarm Input Signal Negative Pole	
NO	Connect Alarm Output Signal	The alarm output signal of one route is not separated between positive and negative.
C1	Connect Alarm Output Signal	

Table 2-2 Audio Interface Description

ID	Description	Wiring Description
IN	Connect Audio Input Signal Positive Pole	One-Way Audio Linein Signal
G	Connect Audio Input Signal Negative Pole	
OUT	Connect Audio Output Signal Positive Pole	One-way audio lineout signal.
G	Connect Audio Output Signal Negative Pole	

2.2 Product Installation

2.2.1 Pre-Installation Description

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

2.2.2 Ceiling Mounted Installation

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

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

Steps

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

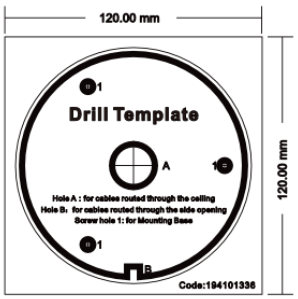

Figure 2-1 Installing Sticker

2. Use 3 PA4 × 25 screws to secure the device base to the wall.

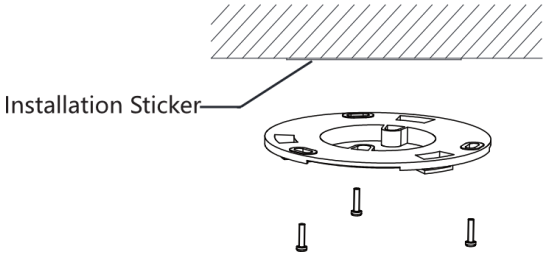

Figure 2-2 Fixed Base

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

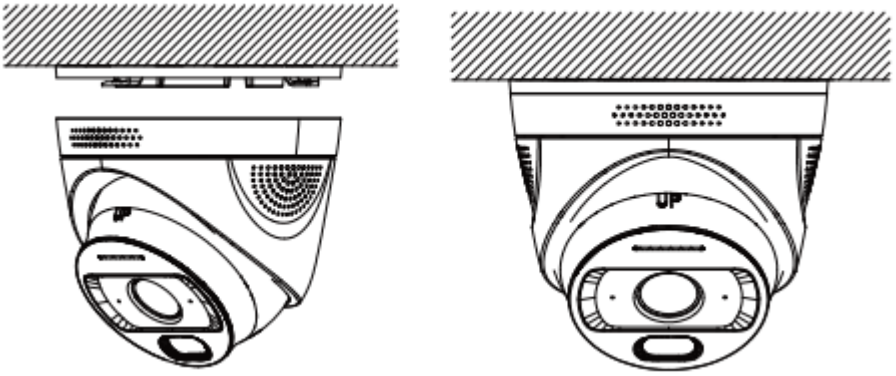

Figure 2-3 Installation Device

Note

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

2.2.3 Adjust the Sphere Direction

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

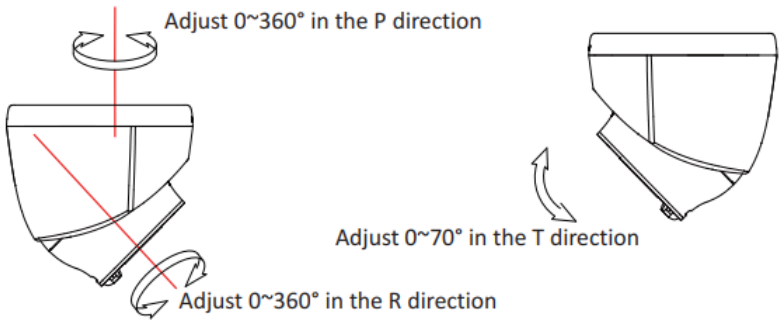

Figure 2-4 Adjust Sphere Direction

2.2.4 Installing Waterproof Tape

When installing the device outdoors, it is necessary 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 water-proof tape to the two ends and to about 2 times the initial length.

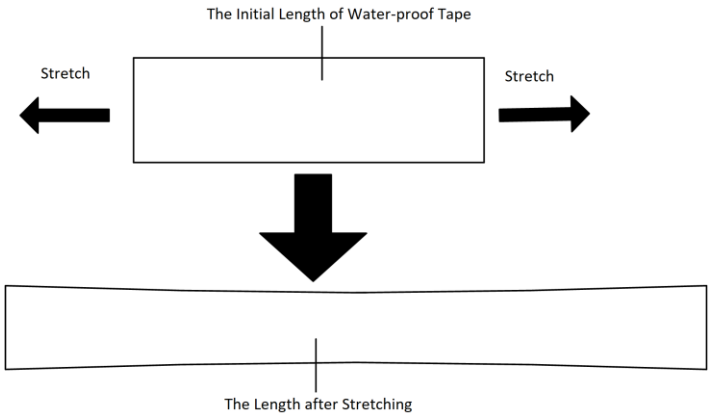

Figure 2-5 Stretching Waterproof Tape

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

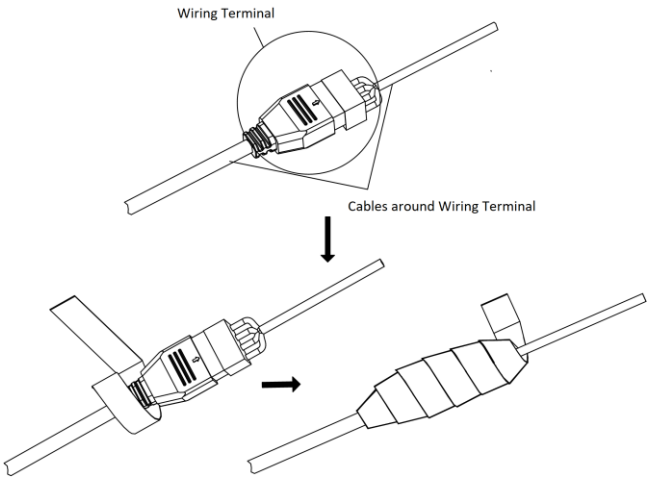

Figure 2-6 Wrapping Waterproof Tape

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

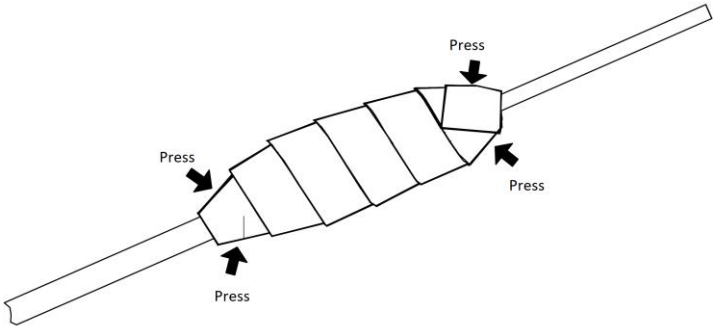

Figure 2-7 Press Water-Proof Tape

2.2.5 Installing Network Port Waterproof Sleeve

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. Put the o-shaped glue ring into the network port, and plug the network cable into the network port.

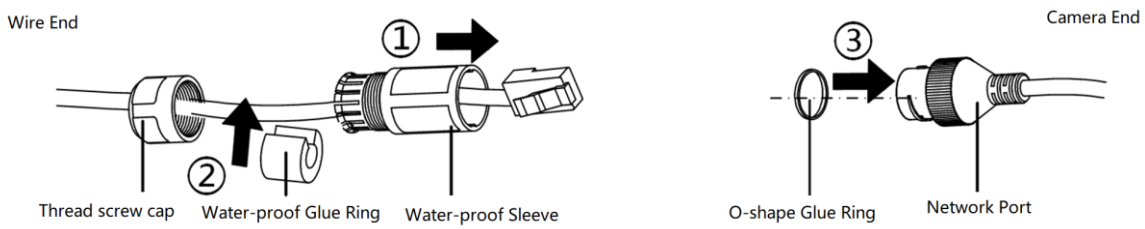

Figure 2-8 Installing Network Cable

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

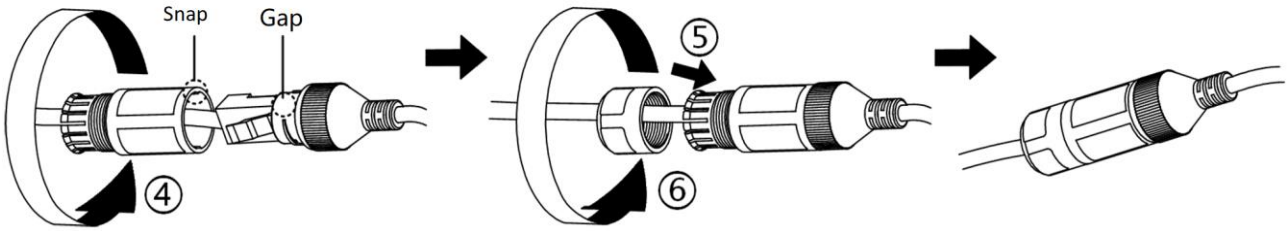

Figure 2-9 Installed

Chapter 3 Pre-Use Operation Information

3.1 Network Connection

Note

If you connect the product to the Internet, including but not limited to cyber attack, hacking, virus infection, etc., the company will not be responsible for the abnormal work and information disclosure of the product, 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 your account, you can set a login password to activate the device, prevent others from logging in to the device, and get information.

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. The list will display information such as device type, IP address, security status, and device serial No. You can activate the inactive device via SADP software.

Prerequisite

Power on the device and connect to the network.

Steps

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

   Note

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

   After the device is activated, the activation status in the list will be updated to activated.
4. Optional: Edit device IP address.

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

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 that needs 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*.
The parameter settings such as IP address will take effect. The device will reboot after network parameters are edited.

3.2.2 Activate via Web Client

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 IP address of the device in the same network segment.

Note

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

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

Note

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

5. Click *OK* to activate the device.

3.3 Access Device

Provide access method through web page and Hik-Connect.

3.3.1 Access Device via Web Client

Login System

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

Note

After logging in, if the interface of installing browser plug-in pops up, please allow installation.

Get Help

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

Exit System

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

3.3.2 Access Device via EZVIZ Cloud

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

Note

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

Enable Hik-Connect

Enable Hik-Connect via SADP or web page.

Enable Hik-Connect via SADP

Enable Hik-Connect via SADP software.

Prerequisite

Get SADP software via official website and install.

Steps

1. Open SADP software.

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

Enable Hik-Connect via Web Client

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

Steps

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

   Access Server IP Address

   By default, the device will automatically assign a server address to the server in the nearest area. **Custom** means you can set domain name server address manually.

   Verification Code

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

   Note

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

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

3.3.3 Add Device to Hik-Connect Video Mobile Client

You can connect the device to Hik-Connect via Hik-Connect Video Mobile Client, and access the device via Hik-Connect Mobile Client.

Prerequisite

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

Steps

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

   Note

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

Figure 3-2 EZVIZ Cloud Video QR Code

Note

EZVIZ Cloud video QR code supports cell phone scanning and downloading in Android system or iOS system.

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

Note

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

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

Chapter 4 Web Client Configuration and Operation

4.1 Live View

Note

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

Live View Screen Function

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

Live view interface icon function description.

Table 4-1 Icon Function Description

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

4.2 Video Playback

View video file to perform video playback.

Prerequisite

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

Steps

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

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

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

4.3 View Picture

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

Note

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

Steps

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

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

Result Description

The downloaded picture will be stored in the settings of *parameter* → *local settings*.

4.4 Parameter Configuration

4.4.1 Local Configuration

Enter *Configuration* → *Local*. You can configure the following parameters.

Playing Parameters

Protocol Type

Set according to actual situation.

Playing Performance

Set according to actual playing requirements.

Display Rule Information

Select **Yes** or **No**. When the display rule information is enabled, the information box will be displayed on the live view page, including dynamic analysis box of mobile detection.

Capture File Format

Set the saving format of captured pictures.

Capture Rule Information

You can select **Yes** or **No**.

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 the archive path.

Playback Capture Save Path

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.

4.4.2 System Parameters

System Settings

Note

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.

Note

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

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

Manual Time Sync

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

Set DST

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

Steps

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

About Device

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

information.

System Maintenance

Upgrade and Maintenance

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

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

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.

Restored completely.

Restore device parameters to factory settings.

Export Information

Device Parameters

It is used to export device parameter file. It can be 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 same parameter.

1. Click *Browse* to select the storage path of the device parameter file. 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.

Note

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 log search date and start/end time, 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. On the device web page, go to *Configuration* → *System* → *System Maintenance* → *Security Audit Log*.
2. Set log main type, minor type, start time, and end time.
3. Click *Search*.
   All log information that meets the search condition is displayed in log list.
4. Optional: Click *Export* to save log to computer.

Security Management

Set Authentication Mode

Set RTSP authentication.

You can select the authentication modes of bigest and bigest/basic. The information to be carried by different

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

Note

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

Set IP Address Filter

Set permission for access to computer or terminal.

Note

IP address refers to IPv4 address.

Steps

1. Enter *configuration → System → Security Management → IP address filtering*.
2. Select *Enable IP Address Filtering*.
3. Set IP address filtering mode.

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

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

Set Security Service

Configure SSH and invalid login lock functions.

Enter *configuration → system → security management → security service*. 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 information leakage in remote management.
Enable *SSH* to provide a secure transmission environment for network service.

Note

The function is disabled by default after rebooting the device.

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.

Note

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

Enable Security Mode

Select *Enable Security Mode*, enter administrator password, and enable the function. After enabling the function, the device will verify with strong password. In this mode, some versions of older NVRs will be disabled.

User Management

User Management

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

Account Security Settings

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

Note

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

Caution

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

Add User/Edit User/Delete User

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

View Online User

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

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

Note

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

4.4.3 Network Parameters

Set TCP/IP address

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

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

Note

The TCP/IP parameters that the device may support are described below. The specific parameters that the device supports 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.
- If *auto-getting* is not selected, manually enter device IPv4 address, IPv4 subnet mask, IPv4 default gateway, and other LAN parameters.

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.

DNS Server Configuration

You can parse the domain name when the device has set the correct available DNS server address.

Configure Port Parameters

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

Note

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

Enter *the 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 ISUP access.
- 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 the device to public security network platform according to GB/T28181 requirements for remote real-time viewing and device management.

Steps

1. Go to *Configuration → Network → Advanced Configuration → Platform Access*.
2. The platform access mode is 28*181*.
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 the device to ISUP platform according to ISUP platform requirements to realize functions such as remote real-time viewing and device management.

Steps

1. Go to *Configuration → Network → Advanced Configuration → Platform Access*.
2. **The platform access mode** is ISUP*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 Hik-Connect micro-video service platform, and the device that supports Hik-Connect access can be accessed through Hik-Connect.

Steps

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

Note

- Refresh the page or restart the device to check *the registration status*. Check if the device is registered.
- If you log in as administrator, you can view the device's Hik-Connect verification code. If you log in as a non-administrator, 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.

Create Private Certificate	Select *Create Private Certificate* in Installation Mode, click *Create*, open Private Certificate Creation Window, enter parameters such as country, domain name/IP address, and 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 existing signed certificate in the installation mode. Install it directly. Click *Browse* to select the existing signed certificate, click *Install*, and click Save when finished.
Download Certificate	After creating the certificate request, click *Download* to download the certificate and send it 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 IP address to HTTPS 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 is set to a port other than 443, enter https://IP address+:(spoof)+port No. in the browser address bar, e.g., *https://192.168.1.64:81.IP address*
- You can also apply for *certificate creation*, upload the certificate issued by the authority certificate (CA) for authentication (fee is required for CA organization), and improve the security level of access.

Configure Open Network Video Interface

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

Steps

1. Go to *Settings* → *Network* → *Advanced Settings* → *Integration Protocol*.
2. Select *Enable Open Network Video Interface*.
3. Configure user.
   1) Click *Add* to customize open network video interface user according to protocol.
   2) Optional: Click *Delete* to delete the user.
   3) Optional: Click *Edit* to edit user information.
4. Click *Save*.
5. Optional: Repeat the steps above to add multiple users according to actual needs.

Set HTTP Listening

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

Steps

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

Note

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

4. Click *Save*.

4.4.4 Video Audio Parameters

Note

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

Set video parameters according to the quality requirements of the live view image.

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

Note

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.

Note

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

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 be caused.

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

Video Frame Rate

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

Video Encoding

H.264

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

Note

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

H.265

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

Encoding Complexity

The higher the encoding complexity under the same bit rate, 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, the poorer the image quality, the larger 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 progress bar or set stream smoothing value. The higher the value, the better smoothing degree, but the image will be less clear. The other way, the smoothness of the image will be poor.

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* View → *Audio* → and configure audio parameters.

Audio Encoding

Set audio encoding type, including G.722.1, G.711ulaw, G.711alaw, MP2L2, AAC, and PCM.
When the encoding type is *MP2L2* or *AAC*, set sampling rate and audio bit rate parameter. Select sampling rate and audio bit rate parameter through the drop-down list.
When the encoding type is PCM, the sampling rate parameter should be set. Select the sampling rate parameter through the drop-down list.

Audio Input

Select *LineIn* and *MicIn* for audio input mode. Select LineIn for active picker, and *MicIn* for passive microphone.

Input Volume

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

Configure ROI

ROI is the encoding of areas of interest. Enabling ROI will improve the image encoding quality of selected areas, reduce the encoding quality of selected areas, and make the image clearer in selected areas during live view or recording.

Prerequisite

ROI function 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 settings are lower.

Steps

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

Note

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

4) Set upgrade level and area name.

Note

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

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

4. Click *Save*.

4.4.5 Image Parameters

Set Display Parameters

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

Note

The display parameters that the device may support are described below. The display parameters of the device should be subject to the actual interface.

Image Adjustment

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

Exposure

Optical Circle Type

Manual by default.

Exposure Time

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

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

without switching day or night according to actual scene.

Night

When in night mode, turn on the supplement light and set the parameters of supplement. The device image is forced to night, and will not be switched to day or night according to the 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 you select *the scheduled switch*. Please set the start time and end time to the next day.

Sensitivity

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

Filtering 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-Light Over-Aeration

Intelligent image processing technology is used to prevent over-aeration of center area due to supplement light of device. 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 Supplementation

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. When the image reaches a certain darkness, the supplement light will be automatically enabled. When the brightness reaches a certain level, the supplement light will be automatically disabled.

Manual

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

Backlight

Backlight Compensation 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 applicable to environments with large differences in light intensity. When high brightness area under strong light source (driving sunlight, lamps or reflective light, etc.) and areas with relatively low brightness, such as shadows and inverse light, you can enable wide dynamic function and adjust the level to view the video picture.
It is used to automatically balance the brightest and darkest parts of the picture 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 areas and under-occupied areas, the bright areas can be weakened and the dark areas can be highlighted to achieve the light balance of the whole picture.

White Balance

In different light environments, the color of the object will change according to the projected light color. You can select a suitable white balance mode according to the environment to correct the color error.

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.

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.

Noise Reduction Level

0 to 100 adjustable.

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.

Note

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

Video Format

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

Set OSD Parameters

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

Enter *configuration → image → OSD settings*, select display item, set channel name, set corresponding parameters, and save to take effect.

Basic OSD Information Settings

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

OSD Attribute Settings

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

Overlay Custom Characters

Multiple characters can be added to the video. Select and set the characters to be added. The characters in the video will be red. Drag the characters or set **the alignment mode** to adjust the characters to the displayed

position. Click *Save* to finish the settings.

Note

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

Set Video Tampering

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

Steps

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

   Note

   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.
6. Click *Save*.

4.4.6 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.

Note

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

Schedule and Linkage Configuration

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

Set Arming Time

Set start time and end time of task execution.

Steps

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

Note

8 time periods are supported in one time axis.

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

Click to Delete Time Period	Delete current time period.
Click to *Delete*	Delete the selected time period.
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 sends 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.
Please go to Configure → Network → Advanced Settings → Platform Access to configure the upload center.

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: *Configure → Network → Advanced Settings → FTP Settings*.
- NAS: *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 will be 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.

Note

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

Configure Motion Detection

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

Steps

1. Enter *configuration → event → basic event → motion detection*.
2. Select *Enable Motion Detection*.
3. Optional: Set the moving object in the picture to green to highlight.
   1) Select *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 general mode settings.
   - See **Expert Mode** for the settings.
5. Set arming time and linkage mode. See *Schedule and Linkage Configuration*.
6. Set **sensitivity**.
7. Click *Save*.

Normal Mode

Set mobile 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 the *drawing 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.

Note

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

Expert Mode

Customize movement detection parameters for daytime and nighttime according to needs.

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 the *area to draw*, 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 drawn area.

Configure Video Tampering Alarm

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

Steps

1. Enter *configuration → event → basic event → video tampering alarm*.
2. Select *Enable*.
3. The sensitivity is set. The higher the sensitivity value, the more sensitive the detection.
4. Set arming time and linkage mode. See *Schedule and Linkage Configuration*.
5. Click *Save*.

Configure Alarm Input

The device's alarm input interface is external to the device. When the alarm signal is generated by the device, the device will be linked.

Prerequisite

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

Steps

1. Enter *configuration → event → basic event → alarm input*.
2. Select alarm input No. and alarm type, and customize alarm name.

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

3. Optional operation: Select *Handling Alarm Input* to select the event configuration alarm linkage to take effect.
4. Set arming time and linkage mode. See *Schedule and Linkage Configuration*.
5. Optional: Click *Copy* to Copy 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. Enter *configuration → event → basic 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 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. Enter *Configuration → Event → Basic Event → Exception*
2. Select exception alarm type.
3. Set linkage mode. See Schedule and Linkage Configuration for linkage mode settings.
4. Click *Save* to finish the alarm configuration.

Configure Smart Event

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

Note

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

Configure Algorithm Resource Allocation

Configure whether to enable the device general algorithm.

Go to Configuration → Event → Smart Event → Algorithm Resource Allocation on the web page to check resource proportion, and select the required algorithm resource configuration. Click *Save* to complete the configuration.

Configure Fire and Smoke Detection

Fire and smoke detection is used to detect whether there is fire or fire in the area. When the fire or smoke 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 → Fire and Smoke Detection.*
2. Select *Enable*.

3. Set detection area and shielded area.
   1) Click to *draw detection area*/*screen area*.
   2) Click the left mouse button in the picture to draw any convex quadrilateral shape.
   3) Repeat steps 1 to 2, and draw up to 4 detection areas/shielded areas.
   4) Optional: Edit the drawn area by following methods.
      - Move the mouse to the internal area. 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 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.

6. Set arming time and linkage mode. See *Schedule and Linkage Configuration*.
7. Click *Save*.

Configure Indoor Access Blocked Detection

The indoor channel is blocked to detect whether the indoor channel has occupied debris and the duration exceeded the set triggering alarm time. When the condition is met, the device will be triggered to execute the linkage action.

Steps

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

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

Time Threshold (s)

Alarm is triggered when there are debris in detection area and the duration exceeds the set time threshold.

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

Configure On/Off Duty Detection

The check-out detection is used to check whether the person on duty in the control room is on duty, sleeping

duty, and cell phone detection. When the number of people in the recognition area is less than the alarm threshold, or the duration of the detection time is longer than the set detection time, the device will execute linkage action.

Steps

1. Go to Configuration → Event → Smart Event → On/Off Duty Detection on the device web page.
2. Select *Enable Absence Detection*, *Play Mobile Detection*, or *Sleep Detection*.
3. Set detection area and shielded area.
   1) Click to *draw detection area/screen area*.
   2) Click the left mouse button in the picture to draw any convex quadrilateral shape.
   3) Optional: Repeat child steps 1 to 2, and draw up to 4 detection areas/shielded areas.
   4) Optional: Edit drawn area.
      - Move the mouse to the internal area. Drag to change the area position.
      - Move mouse to area vertex. Click Drag to edit vertex position.
      - Click *Clear All* to delete all drawn areas.

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

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

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

Configure Detection of Dangerous Goods in Elevator

This function is used to detect whether electric battery and gas tank enter elevator area. It can set up to 4 four four-sided alarm zones. When target object enters the area, the device can generate alarm signal and act as a linkage.

Steps

1. Go to *Configuration → Event → Smart Event → Detection of Dangerous Goods in Elevator*.
2. Check *the battery or gas tank* detection.
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 elevator and the object size is within the max. and min. size range, it can be recognized as the target. Otherwise, it is not the target. This function can improve detection accuracy.
4. Set detection parameters.

Mode

Select mode according to actual situation.

Sensitivity

The degree of target entering arming area. The larger the sensitivity settings, the easier the alarm will be triggered.

Trigger Alarm Time

Alarm Triggering Duration Settings.

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

Configure Dangerous Behavior Detection

Detects whether there is smoke and call behavior in the area. When risky behavior is detected and alarm triggered, the configured linkage will be executed.

Steps

1. On the device web page, go to *Configuration → Event → Smart Event → Dangerous Behavior Detection*.
2. Select *Enable Smoking Detection* or *Enable Phone Detection*.
3. Set detection area and shielded area.
   1) Click to *draw detection area/screen area*.
   2) Click the left mouse button in the picture to draw any convex quadrilateral shape.
   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 internal area. Drag to change the area position.
      - Move mouse to area vertex. Click Drag to edit vertex position.
      - Click *Clear All* to delete all drawn areas.

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

Sensitivity

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

Detection Time

You can set the alarm for 1 to 5 seconds. Alarm will be triggered if the detection value is exceeded.

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

Configure Fire Extinguisher Detection

Detect whether fire extinguisher is missing in area. When no fire extinguisher is detected and alarm triggered, the configured linkage will be executed.

Steps

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

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

Fire Extinguisher Quantity Threshold

Alarm triggered when detection failed to reach the set number.

Fire Extinguisher Detection Time

You can set the alarm for 1 to 600 seconds. Alarm will be triggered if no fire extinguisher device exceeds the detection value.

Fire Extinguisher Sensitivity

The sensitivity settings of fire extinguisher device is larger, and the corresponding results are easier to detect.

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

Configure Call and Rescue Recognition

It is used to detect whether there are people calling for help. It is used to detect three keywords: fire, life, and fire suppression. When the keyword is detected and alarm triggered, the configured linkage will be executed.

Steps

1. On the device web page, go to *Configuration → Event → Smart Event → Call and Rescue Recognition*.
2. Select *Enable*.
3. Set detection parameters.

Sensitivity

Higher sensitivity will make it easier to recognize and trigger alarm, and the error recognition rate will increase.

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

Configure Intrusion Detection

Area intrusion detection is used to detect whether target has entered the warning area. This function can create up to 4 four four-sided warning areas. When target object has entered the area, the device can generate alarm signal and interact with the function.

Steps

1. Enter *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, and draw the four-way detection area.
   3) Optional: Click *Clear* to clear the drawn area.
   4) Optional operation: Repeat child steps 1 to 3. Up to 4 warning areas can be set.
5. Set alarm parameters.

Time Threshold

It means that the target enters the alarm area. The duration of the time is set to stay in the area. Alarm will be generated if the time exceeded the time limit. 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

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.

Ratio

The detection target is the percentage of the area you draw. When the object exceeds the set percentage, the area intrusion 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 Line Crossing 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. Enter *configuration → Event → Smart Event → Line 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 operation: 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 triggering alarm when the target crosses the alarm surface.

A->B

The 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 that 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*.

4.4.7 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 *Enable* to enable recording schedule.
3. Select recording type.

Note

The video type of the device may be included. The selected video type will be subject to the actual interface of the device.

Timed

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

Motion Detection

Channel recording when mobile detection event occurs.

Alarm

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

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

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-Recording Time

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

Video Delay

Delay recording time after recording schedule end time node.

Stream Type

Stream type of video storage.

Note

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

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

Storage Management

The storage space for managing video files and pictures.

Note

The content in storage management is dependent on the actual device. The following information describes the storage management that the device may support.

HDD Management

View HDD information and HDD quota.

Steps

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

Format SD Card

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

Prerequisite

Install the microSD card to the device.

Steps

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

Note

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

5. Click *Save*.

UD00000B