HF-VS409 Smoke Detected Camera

User Manual

Legal Information

About this Manual

The Manual 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 Manual is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of this Manual at the Hikvision website (***https://www.hikvision.com/***).
Please use this Manual with the guidance and assistance of professionals trained in supporting the Product.

Trademarks

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.

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". 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 MANUAL AND THE APPLICABLE LAW, THE LATER PREVAILS.

Symbol Conventions

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

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

Contents

Chapter 1 Safety Instruction

Warning

- All the electronic operation should be strictly compliance with the electrical safety regulations, fire prevention regulations and other related regulations in your local region.
- Do not connect several devices to one power adapter as adapter overload may cause over-heat or fire hazard.
- Please make sure that the power has been disconnected before you wire, install or dismantle the device.
- When the product is installed on wall or ceiling, the device shall be firmly fixed.
- If smoke, odors or noise rise from the device, turn off the power at once and unplug the power cable, and then please contact the service center.
- If the product does not work properly, please contact your dealer or the nearest service center. Never attempt to disassemble the device yourself. (We shall not assume any responsibility for problems caused by unauthorized repair or maintenance.
- In the use of the product, you must be in strict compliance with the electrical safety regulations of the nation and region.

Caution

- Do not drop the device or subject it to physical shock,and do not expose it to high electromagnetism radiaon. Avoid the equipment installation on vibrations surface or places subject to shock(ignorance can cause equipment damage).
- Do not place the device in entremely hot (refer to specification of the device for detailed operating temperature), cold, dusty or damp locations, and do not expose it to high electromagnetic radiation.
- The device cover for indoor use shall be kept from rain and moisture.
- Exposing the equipment to direct sun light, low ventilation or heat source such as heater or radiator is forbidden (ignorance can cause fire danger).
- Do not aim the device at the sun or extra bright places. A blooming or smear may occur otherwise (which is not a malfunction however), and affecting the endurance of sensor at the same time.
- Please use the provided glove when open up the device cover, avoid direct contact with the device cover, because the acidic sweat of the fingers may erode the surface coating of the device cover.
- Please use a soft and dry cloth when clean inside and outside surfaces of the device cover, do not use alkaline detergents.
- Please keep all wrappers after unpack them for future use. In case of any failure occurred, you need to return the device to the factory with the original wrapper. Transportation without the original wrapper may result in damage on the device and lead to additional costs.

- CAUTION: Risk of explosion if the battery is replaced by an incorrect type.
- Improper replacement of the battery with an incorrect type may defeat a safeguard (for example, in the case of some lithium battery types).
- Do not dispose of the battery into fire or a hot oven, or mechanically crush or cut the battery, which may result in an explosion.
- Do not leave the battery in an extremely high temperature surrounding environment, which may result in an explosion or the leakage of flammable liquid or gas.
- Do not subject the battery to extremely low air pressure, which may result in an explosion or the leakage of flammable liquid or gas.
- Dispose of used batteries according to the instructions.

Chapter 2 Regulatory Information

FCC Information

Please take attention that changes or modification not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.
FCC compliance: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
—Reorient or relocate the receiving antenna.
—Increase the separation between the equipment and receiver.
—Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
—Consult the dealer or an experienced radio/TV technician for help
FCC Conditions
This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:
1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

EU Conformity Statement

CE

This product and - if applicable - the supplied accessories too are marked with "CE" and comply therefore with the applicable harmonized European standards listed

under the EMC Directive 2014/30/EU, LVD Directive 2014/35/EU, the RoHS Directive 2011/65/EU

2012/19/EU (WEEE directive): Products marked with this symbol cannot be disposed of as unsorted municipal waste in the European Union. For proper recycling, return this product to your local supplier upon the purchase of equivalent new equipment, or dispose of it at designated collection points. For more information see: www.recyclethis.info

2006/66/EC (battery directive): This product contains a battery that cannot be disposed of as unsorted municipal waste in the European Union. See the product documentation for specific battery information. The battery is marked with this symbol, which may include lettering to indicate cadmium (Cd), lead (Pb), or mercury (Hg). For proper recycling, return the battery to your supplier or to a designated collection point. For more information see:www.recyclethis.info

Industry Canada ICES-003 Compliance

This device meets the CAN ICES-3 (B)/NMB-3(B) standards requirements.

Chapter 3 Overview

3.1 Introduction

HF-VS409 series visual smoke detection camera integrates smoke detection, temperature detection and video perception as well as video intelligent analysis. The camera can detect heat and smoke in the early stage of a fire hazard, facilitate intelligent video analysis and provide warnings by sending out audible and visual alarm signals and showing alarm information and relevant images and video clips in the video surveillance system. The camera can also verify potential security hazards based on intelligent analysis. It can be widely used in various scenes including nine types of small places, shops, nursing homes, family dwellings, hotels and tall buildings.

3.2 Features

- Smoke detection, temperature detection, VaaS (Intruder Verification as a Service) approved
- High sensitivity, safe, reliable and handy
- 4 million HD resolution, wide angle lens
- Configurable intelligent video analysis to facilitate fire source detection and fire hazards verification
- Real-time video prompts, showing alarm information, real-time alarm prompts to mobile APP
- Upload alarm events and device status information
- External 12 VDC power supply, battery power supply in the event of power failure to ensure normal operation of the alarm
- 1-ch alarm input and 1-ch alarm output
- Link alarm images and videos when alarm is triggered
- Maximum resolution: 4 megapixels (2560 × 1440@25 fps), real-time image output
- Low bit rate, low latency, ROI enhanced coding, SVC adaptive coding technology, smart 265 coding
- IR lamp, long service life, irradiation distance up to 15 meters
- Automatic switch of ICR infrared filter to achieve 24/7 monitoring
- microSD/SDHC/SDXC card (128 G) local storage
- 3D digital noise reduction, backlight compensation, automatic electronic shutter function, adapt to different monitoring environments

3.3 Appearance

Note

The appearance may vary according to different device models. Refer to the actual device for details.

Dimensions

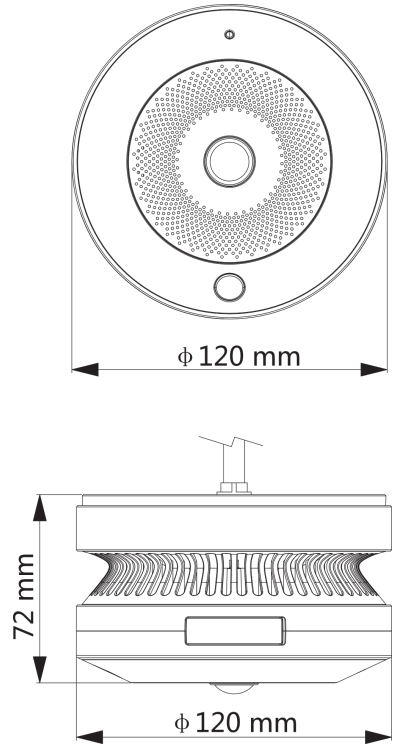


Figure 3-1 Dimensions

Appearance and Interface

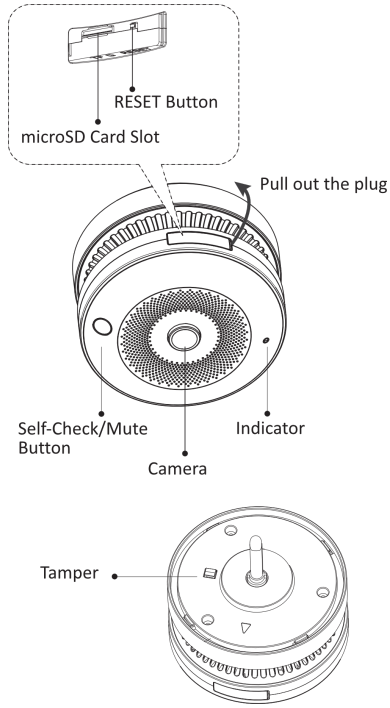


Figure 3-2 Appearance

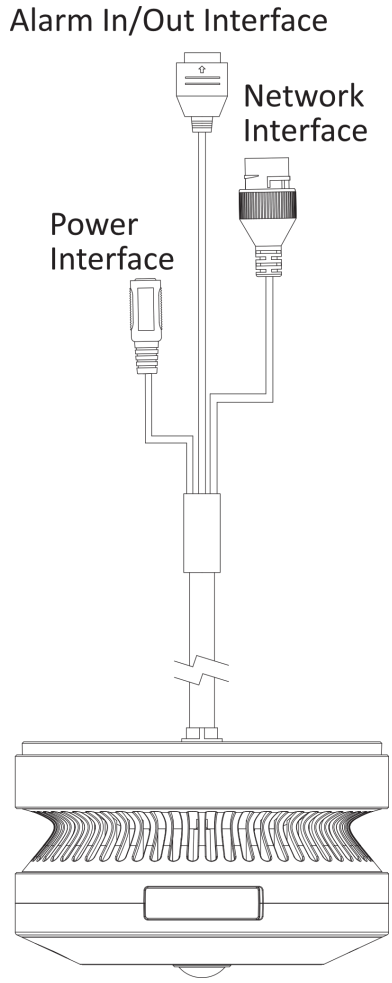


Figure 3-3 Interface

MicroSD Card Slot

Insert microSD card for local storage.

RESET Button

Hold the RESET button and power on the device. Hold the button for 10 to 15 seconds while the device is powered on. Release the button and the device will be restored to default settings.

TEST/SILENCE Button

The button controls functions including test, muting the alarm and resetting. Refer to ***TEST*** / ***Mute*** for details.

Camera

Fisheye camera

Indicator

Refer to ***Indicator & Buzzer Status*** for details.

TAMPER

If the device is pulled off its base by force, the button will pop out to trigger the tampering alarm.

Power Interface

12 VDC power supply

Note

Make sure the power supply connect correctly.

Network Interface

Connect to Ethernet.

Alarm In/Out Interface

Pull out the green connector inside the Alarm In/Out Interface. Loosen the screws with a mini slotted screrwdriver, put in the cable and tighten the screws. Plug the connector into the green base.

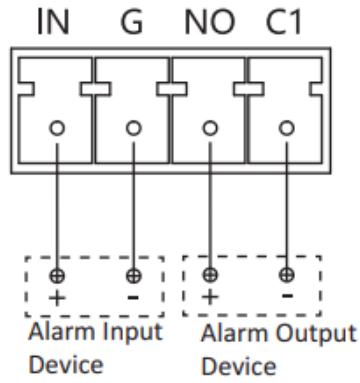


Figure 3-4 Alarm In/Out Interface Illustration

3.4 Indicator & Buzzer Status

Table 3-1 Indicator & Buzzer Status Description

Indicator	Buzzer	Status
Flashing green every 90 seconds	Disable	Standby
Solid red	Squeal	Smoke/Temperature alarm

Indicator	Buzzer	Status
Flashing red every 40 seconds	Beeping every 40 seconds	Low voltage
Quick flashing green 3 times	Disable	Tampering alarm
Flashing yellow every 40 seconds	Beeping every 40 seconds	Maze pollution
Flashing red every 100 seconds	Disable	Temperature sensor fault

Note

If pollution alarm is triggered, please contact the supplier.

Chapter 4 Installation

4.1 Installation Description

- Install the alarm according to the instructions in this manual.
- To prevent injury, please ensure the alarm is securely attached to the wall or the ceiling.
- Before installation, confirm that the alarm is intact and the mounting parts in the box are all ready.
- Do not install the alarm within 30 cm (11.81'') away from power lines to avoid maze pollution and alarm caused by the gathering of phototactic insects.
- Install multiple devices if the installation location (such as ceiling) is longer than 10 meters (32.81 ft).
- Do not install the alarm at the following locations:
  - Humid areas including kitchens, water heaters, or bathrooms.
  - Areas affeted by strong air flow, such as places right in front of air conditioners, fans or heatings.
  - Dusty, dirty, or insect infested areas.
  - Hot and greasy areas such as stoves.
  - Where the sensor might be blocked.
  - Within 1.5 meters (4.92 ft) from lights.
  - Blind spots such as apexes of ceilings and corners of the rooms.
  - Areas affected by vibrations, shocks or EMI (the product might be damaged).
  - Areas exposed to spraying water or ther liquids.

4.2 Mounting Location

When mounting the alarm on flat ceilings, locate it at a minimum distance of 500 mm (19.69'') from the side wall.

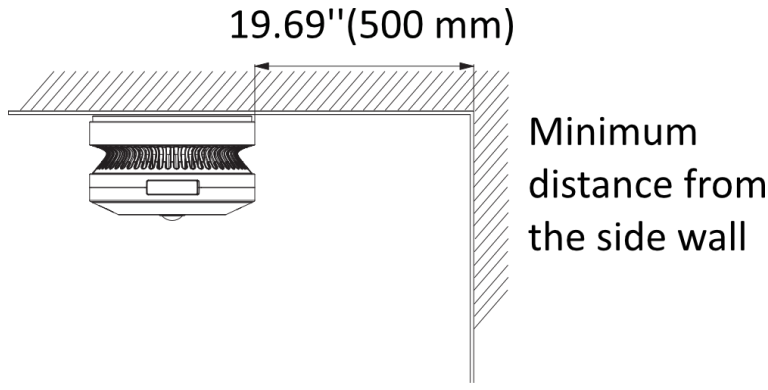


Figure 4-1 Mounting Locations

4.3 Ceiling Mounting without Junction Box

Steps

1. Drill 4 screw holes on the ceiling according to the mounting template.
2. Insert the plastic expansion sleeves into the screw holes, and fix the mounting base with screws.
3. Smooth the cables and turn the smoke detector clockwise until it snaps in place.

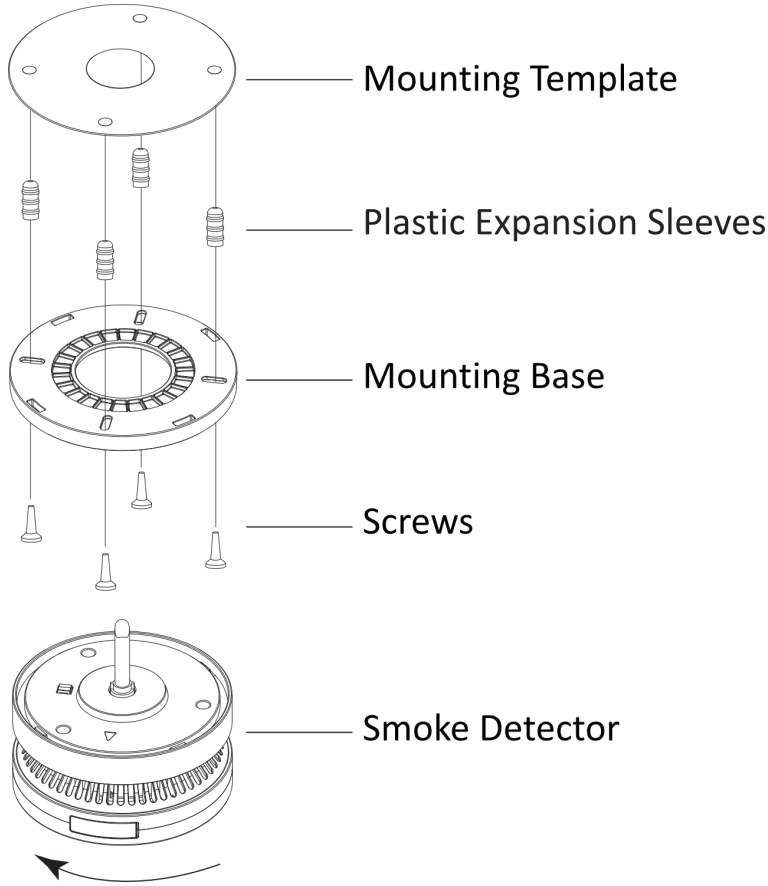


Figure 4-2 Installation Illustration

4.4 Ceiling Mounting with Junction Box

Steps

Note

Accessories that you need to prepare for installation: Junction box (Optional). Ask our technique supports and sales and purchase the junction box.

1. Drill 4 holes on the ceiling according to the mounting template.
2. Insert the plastic expansion sleeves into the screw holes, and fix the junction box with screws.

3. Fix the mounting base to the junction box with screws.
4. Smooth the cables and turn the smoke detector clockwise until it snaps in place.

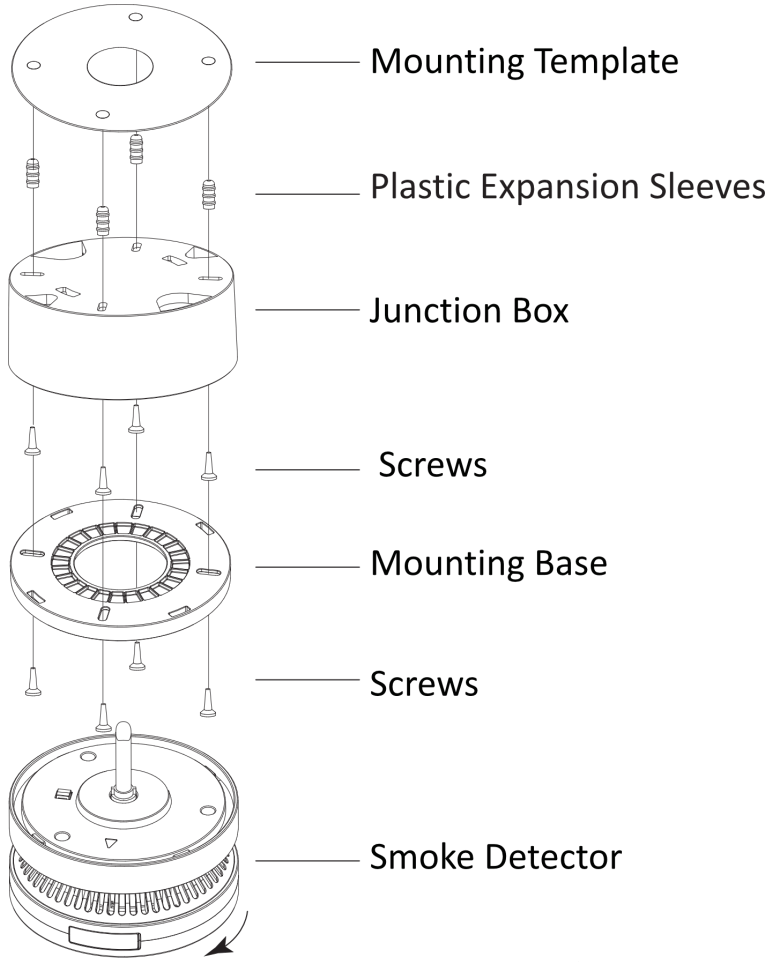


Figure 4-3 Installation Illustration

Chapter 5 Quick Operation

5.1 Connect Device to Network

Connect your device to Ethernet, and you can configure parameters of the device via browser.

5.2 Activation

The device need to be activated by settings a strong password before use. This part introduces activation using different client tools.

5.2.1 Activate via SADP

SADP is a tool to detect, activate and modify the IP address of the device over the LAN.

Before You Start

- Get the SADP software from the supplied disk or the official website ***http://www.hikvision.com/*** , and install the SADP according to the prompts.
- The device and the PC that runs the SADP tool should belong to the same subnet.

The following steps show how to activate one device and modify its IP address. For batch activation and IP address modification, refer to *User Manual of SADP* for details.

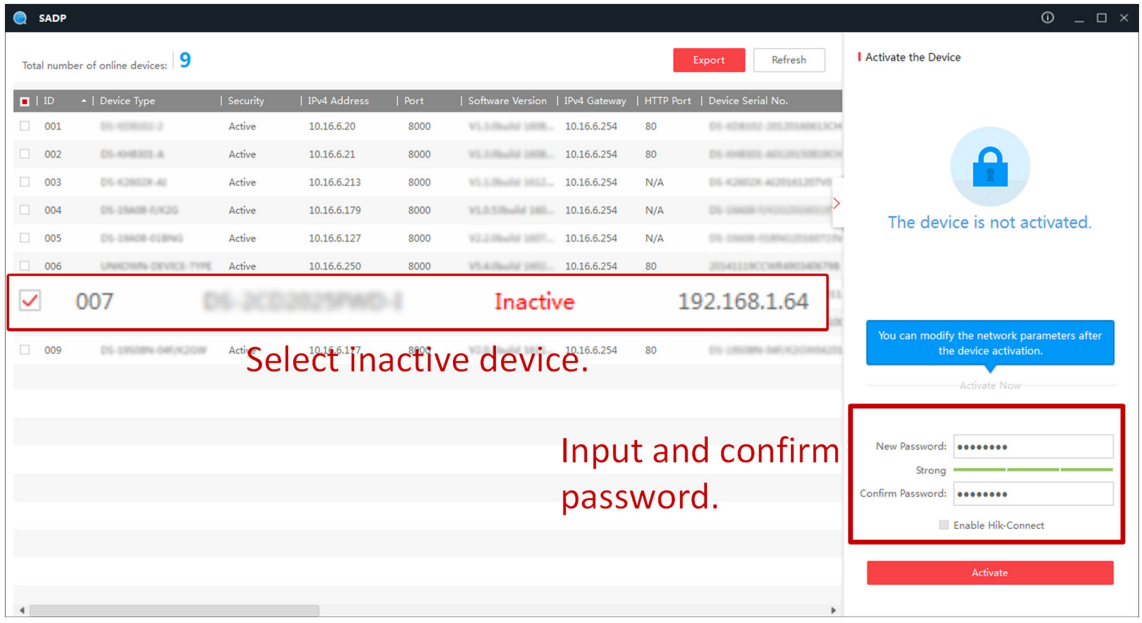
Steps

1. Run the SADP software and search the online devices.
2. Find and select your device in online device list.
3. Input new password (admin password) and confirm the password.

Caution

STRONG PASSWORD RECOMMENDED-We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

4. Click **Activate** to start activation.



Status of the device becomes **Active** after successful activation.

5. Modify IP address of the device.
   1) Select the device.
   2) Change the device IP address to the same subnet as your computer by either modifying the IP address manually or checking **Enable DHCP**.
   3) Input the admin password and click **Modify** to activate your IP address modification.

5.2.2 Activate Device via Web Browser

Use web browser to activate the device. For the device with the DHCP enabled by default, use SADP software or PC client to activate the device.

Before You Start

Make sure your device and your PC connect to the same LAN.

Steps

1. Change the IP address of your PC to the same subnet as the device.

   The default IP address of the device is 192.168.1.64.
2. Open a web browser and input the default IP address.
3. Create and confirm the admin password.

Caution

STRONG PASSWORD RECOMMENDED-We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And

we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

4. Click **OK** to complete activation and enter **Live View** page.
5. Modify IP address of the camera.
   1) Enter IP address modification page. **Configuration → Network → TCP/IP**
   2) Modify IP address.
   3) Save the settings.

5.3 Access Device via Web Browser

Before You Start

Check the system requirement to confirm that the operating computer and web browser meets the requirements.

Steps

1. Open the web browser.
2. Input IP address of the device to enter the login interface.
3. Input user name and password.

   Note

   Illegal login lock is activated by default. If admin user performs seven failed password attempts (five attempts for user/operator), the IP address is blocked for 30 minutes.
   If illegal login lock is not needed, go to **Configuration → System → Security → Security Service** to turn it off.

4. Click **Login**.
5. Download and install appropriate plug-in for your web browser.

   For IE based web browser, webcomponents and QuickTime™ are optional. For non-IE based web browser, webcomponents, QuickTime™, VLC and MJEPG are optional.
6. **Optional:** Click **Help** on the right-bottom of the page to get the web help manual online.
7. **Optional:** When you finished the operation and configuration, click **Exit** to log out.

Chapter 6 Local Settings

6.1 Smoke/Temperature Alarm

In standby mode, when smoke particles or the temperature reach the settings, the alarm will be triggered.
The buzzer will beep and the indicator keeps red.

Note

You can enable the function via web to upload the alarm records, smoke concentration and pollution data to platforms and FTP. Refers to ***Set Smoke Detection*** for details.

6.2 TEST

Make sure the buzzer and indicator work properly.

In standby mode, press the 【TEST/SILENCE】 button, and the device will enter test mode. After testing, the device will exit the test mode automatically.

Test Mode: The buzzer beeps for 10 times, and the indicator keeps red.

6.3 Mute

In alarm mode, hold the 【TEST/SILENCE】 button to mute the alarm (the mute period is 10 minutes).

Mute Mode: The buzzer stops beeping, and the indicator keeps red.

Mute Period: After the alarm is mute, if the smoke concentration or the temperature still reach the settings, the alarm will be triggered in 10 minutes.

6.4 Reset

When the alarm is in mute mode(when the red light keeps red and the buzzer stops beeping), press the 【TEST/SILENCE】 button again to reset the device.

In alarm mode, if the smoke dissipates or the temperature declines, the alarm will automatically resume to standby mode.

6.5 Restore

Hold the 【RESET】 button and power on the alarm. Hold the button for 10 to 15 seconds while the device is powered on. Release the button and the device will be restored to default settings.

Chapter 7 Remote Configuration via Web

7.1 Live View

The live view page allows you to view the real-time video, capture images, realize PTZ control, set/call presets and configure video parameters.

Log in the device to enter the live view page, or click **Live View** on the menu bar of the main page to enter the live view page.

Note

You can also visit the fisheye camera to get the live view in different live view modes via iVMS-4200 client software. Refers to the User Manual of iVMS-4200 Client Software for details.

Live View Page

The Live View Page is mainly composed of two parts, the live view screen and a PTZ panel which can be shown or hidden on the right.

Figure 7-1 Live View Page (PTZ Control)

Figure 7-2 Live View Page (General Settings)

Manu Bar

Click the tab to enter Live View, Playback, Picture and Configuration page respectively.

Live View Window

Display the live video on the display window of live view.

Tool Bar

Start/Stop the live view, enable/disable the two-way audio, adjust volume, capture pictures, record the video files, etc.

PTZ Control

Realize the pan/tilt/zoom function of PTZ view via the navigation box, and set the PTZ moving speed.

Preset/Patrol Settings

Set and call the preset/patrol for the device.

Start Live View

Live Video will be automatically displayed when you click Live View on menu bar.

Figure 7-3 Live View Page

Table 7-1 Descriptions of Live Icons

Icon	Description
▶	Start all live view.
■	Stop all live view.
Clear	Clear
📷	Capture images.
📹 / 📹	Manually start/stop recording.
🔍 / 🔍	Start/Stop digital zoom.
🔇	Mute
🔊	Audio on and adjust the volume.
4:3	Set aspect ratio as 4:3.
16:9	Set aspect ratio as 16:9.
1×	Window size for iriginal video stream.
⛶	Self-adaptive window size.
	Main stream
	Sub stream

Icon	Description
	Webcomponents
M	MJPEG

Digital Zoom:
1. Click to start the function.
2. Click the mouse on the live view image and drag it to a lower right position. The area in the red rectangle will be zoomed in after you release the mouse.
3. Click the mouse on the zoomed-in image, drag it to a higher left position and release the mouse to zoom out.
4. Click to stop the function.

Record and Capture Pictures Manually

In the live view page, click on the toolbar to capture the live pictures or click to record the live video. The saving paths of the captured pictures and record files can be set on **Configuration → Local Settings** page.

Note

The captured image will be saved as JPEG file or BMP file in your computer.

PTZ Control

A PTZ View is a close-up view of some defined area on the panoramic and fisheye view, and it supports digital PTZ Control.
When PTZ View is selected for live view, you can use the PTZ control panel on the right of the window to realize pan/tilt zoom control of the PTZ View.
On the live view page, you can click to show the PTZ control panel, and click to hide it.

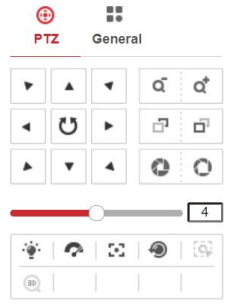


Figure 7-4 PTZ Control Panel

Table 7-2 Descriptions of PTZ Control Panel

Icon	Description
	Direction buttons
/	Start/Stop auto scan
/	Zoom in/Zoom out
/	Focus -/Focus +
/	Iris -/Iris +
4	Adjust speed of pan/tilt movements
	Enable/disable light
	Auxiliary focus
	Enable/disable wiper
	Lens initialization
	Start manual tracking
	Start 3D zoom
	Click to set presets
	Click to set patrol

Note

The page may vary according to different device models. Refers to the actual page for details.

General Parameters

Click **General** to edit the display, OSD and video/audio parameters.

- Refers to ***Set Display Parameters*** for editing display parameters.
- Refers to ***Set OSD*** for editing display parameters.
- Refers to ***Set Video Parameters*** for editing video/audio parameters.

7.2 Playback

You can search, play and download the video files saved in the device at the playback page.

Steps

1. Click **Playback** to view the playback page.
2. Filter by **Date** and click **Search**. The qualified recordings will be displayed on the timeline.
3. Play a recording on a specific time.

1) Drag the timeline to a specific time and click ▶ to play the recording.
2) If you need to play the recordings on a specific time, set **Time** at **Locate Play Time** and click ↵ . The recordings will play on the time you set.

Note

Default play time starts from when the video was recorded.

4. **Optional:** During recording playing, you can click the icons below to realize operations including start/pause, stop, speed up, slow down, play backwards, capture images, edit recording, zoom in, adjust volume and download.

Note

- The pictures will be saved at the **Visit the Save Path of Captured Images** you set at **Configuration → Local** .
- The clips will be saved at the **Visit the Save Path of Clips** you set at **Configuration → Local** .
- The downloaded files will be saved at the **Visit the Save Path of Downloaded Files** you set at **Configuration → Local** .

7.3 Picture

You can search, view and download valid pictures saved in the device.

Before You Start

Note

If you want to view pictures of event alarms, you need to click **Event** to set Linkage Method. Steps: Click **Configuration → Event** to view the configuration page of the selected event, such as Alarm Input, click **Linkage Method**, and check **Upload to FTP**.

Steps

1. Click **Picture** to view the picture search page.
2. Set search condition on the left to filter by file type, star time or end time, click **Search**, and the qualified pictures will be displayed on the list to the right.
3. Select the pictures you need by check the checkboxes, click **Download** to download the pictures.

Note

If you need to stop downloading, click **Stop Downloading**.

Result

The downloaded pictures will be saved according to the **Save downloaded path** you set at **Configuration → Local** .

7.4 Parameter Settings

7.4.1 Local

Click **Configuration → Local** to enter the settings page.

Video Parameters

Protocol

configure settings according to actual practice.

Play Performance

configure settings according to actual practice.

Rule Information

You can click to **Enable** or **Disable** the rule information. If the function is enabled, the preview interface will display info boxes, such as dynamic analysis of motion detection.

Display POS Information

You can click to **Enable** or **Disable** POS information. If the function is enabled, alarm target in the rule-triggering zones will be displayed as regtangular boxes.

Image Format

Set save format for captured images.

Record Files Settings

Record File Size

The size of a single file saved locally.

Save Record File

Click **Browse** to change the path. Click **Open** to open the folders that save the Record files.

Save Downloaded File

Click **Browse** to change path. Click **Open** to open the folders that save the downloaded files.

Picture and Clip Settings

Save Snapshots in Live View

Click **Browse** to change path. Click **Open** to open the folders that save the snapshots in live view.

Save Snapshots When Playback

Click **Browse** to change path. Click **Open** to open the folders that save the snapshots when playback.

Save Clips

Click **Browse** to change path. Click **Open** to open the folders that save the clips.

7.4.2 System

System Settings

Note

system settings may vary according to different device models and the followings are possible system settings supported by the device.

View Basic Information

System info includs device model, serial No., version info, number of camera, number of HDDs and number of alarm input/output.

Click **Configutarion → System → System Settings → Basic Information** to change your device name and number.

Set Time

Set time for the device. NTP and Manual Time Sync. are supported.

Click **Configuration → System → System Settings → Time Settings** to select your time zone and time synchronizing mode.

NTP

The function requires configuration of NTP server address, NTP port and time synchronizing interval.

Manual Time Sync.

You can set time for the device manually or check **Sync. with computer time**.

Set RS-232 Parameters

RS-232 can be used o test the device or connect to peripherals. Data transmition between the device and computer or other terminals can be realized through RS-232 when the communication distance is short.

Note

Connect the device to your PC with a RS-232 cable before settings.

Steps: Click **Configuration → System → System Settings → RS-232** . Set RS-232 Settings to ensure the device matches with your PC or other terminals. Click **Save**.

RS-485

Steps: Click **Configuration → System → System Settings → RS-485** . Set RS-485 Settings to ensure the device matches with your PC or other terminals. Click **Save**.

About Device

Click **Configuration → System → System Settings → About** and click **View** to view open source software licenses.

Maintenance

Upgrade and Maintenance

Click **Configuration → System → Maintenance → Upgrade and Maintenance** to reboot device, set parameters, import/export and upgrade.

Reboot

Click **Reboot** to reboot the device.

Default

Restore

Reset all the parameters, except the IP parameters and user information, to the default settings.

Default

Restore all parameters to default settings.

Information Export

Device Parameter

Export parameter files for configuration reference.

1. Click **Device Parameter**, the file encryption configuration window will pop up.
2. Set an encryption password for parameter files exported.
3. Click **OK** to save the export path.

Note

The OSD parameter is not included in the parameter files.

Diagnosis Information

Download operation logs, system information, hardware information, etc.

Import Configuration File

Import parameter files for configuration reference.

1. Click **Browse** to choose the save path for parameter files imported. Click **Open**.
2. Click **Import**.
3. Click **OK** and enter the encryption password. Click **OK** to import the files.

Note

The OSD parameter is not included in the parameter files.

Upgrade

Upgrade Files

If the device needs upgrading, you can copy the upgrade program to your PC, click**Browse** to choose the save path, and click **Upgrade**.

Note

The upgrading process will be 1 to 10 minutes, please do not power off. The device will restart automatically after upgrading.

Log

You can view, display and export valid logs saved in the device on the Log page.

1. Click **Configuration → System → Maintenance → Log** .

2. Select log type. Set start time and end time. Click **Search**. The qualified files will be displayed on the list.

Note

Up to 2,000 results will be displayed for a single search.

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

Note

The save formats of Text. files and Excel. files are supported.

Security Audit Log

Faults caused by illegal intrusion and security events can be identified through searches for and analysis on security logs. The storage is limited, and it is recommended you set a log server and upload security logs.

Note

The security audit log function may vary according to different device models. Refer to the actual device for details.

Search

Search and manage the security logs.

1. Click **Configuration → System → Maintenance → Security Audit Log** .

2. Select log type. Set start time and end time. Click **Search**. The qualified files will be displayed on the list.

3. Optional: Click **Export** to save the logs on the computer.

Server Configuration

Upload and store the security logs to log servers.

Note

If mutual-authentification is required for the server, the device needs to install both client certificate and CA certificate. If not, the device needs to install CA certificate.

1. Click **Configuration → System → Maintenance → Security Audit Log** .
2. Install client certificate.
1. Click **Create** to create certificate request.
2. Click **Download** to download certificate request.
3. Optional: Click **Delete** and repeat step1 and step 2 to create new certificates.
4. Send the certificate to institution for authentification.
5. Click **Browse** to select authenticated certificate and click **Install**.
3. Install CA certificate
1. Obtain CA certificate.
2. Click **Browse** to select CA certificate and click **Install**.
4. Configure log server.
1. Check **Enable Log Upload Server**.
2. Check**Enable Encrypted Transmission**.

Note

Enctypted transmission will be disabled when the device is not equipped with client certificate and CA certificate.

3. Set server parameters.

Log Server Address

Server address, e.g., IP address.

Log Server Port

Data port of log server.

4. Click **Test**. Test success means the device is connected to the log server.
5. Click **Save**.

Result: The device will upload security audit logs to the server regularly.

The function may vary according to different device models. Refer to the actual device for details.

Security

Authentication

Set RTSP and WEB authentication.

Digest, digest/basic authentication are supported. Different authencitation mode requires different information. Refer to the protocol for details.

Note

Requirement for basic authentication is rather simple. To ensure high-level cyber security, the digest authentication is recommended.

IP Address Filter

Set permissions for visits from computers or other terminals.

Note

IP address refers to IPv4 address.

1. Click **Configuration → System → Security → IP Address Filter**
2. Check **Enable IP Address Filter**.
3. Set IP address filter type.

Forbidden

Allow all IP address, except that on the list, to visit the device.

Allow

Allow the IP address on the list only to visit the device.

4. Set IP address filter.

1. Click **Add** to input IP address.
2. Optional: Click **Edit** to edit selected IP address.
3. Optional: Click **Delete** to delete selected IP address.

5. Click **Save**.

Security Service

If an admin user makes 7 login attempts (5 for non-admin users) with incorrect password, the device will send a message and be locked automatically.

Click **Configuration → System → Security → Security Service** to check **Enable Illegal Login Lock**

Note

For security concern, it is recommended that you enable the function according to actual practice to avoid illegal login.

User Management

User Management

When logging in with default admin account, you can change password and add (no more than 31 user accounts) or edit other user accounts.

Account Security Settings

Click **Account Security Settings** and input password for the admin user account to set or change security questions. After configuration, click **Forget Password** on the login page and answer the security questions to reset your password.

Note

- Ensure your device and computer are connected to the same LAN segment.
- You are not allowed to change the username of the default admin user account. Password reset is allowed.
- You need to input password for admin user account when adding, editting and deleting other user accounts.

Caution

- For account security, ensure the password is 8 to 16 characters of at least 2 types, including numbers, lower case letters, upper case letters and symbols (! ''#$%&'()*□,□./:; □=□?@[\]^_`{|}~blank). The password can not contain the username.
- Password shorter than 8 characters, consisted of one type of character or same with the username is risky. For privacy protection and product security, we recommend you change your password to high-level secure password.

Add/Edit/Delete User Account

Click **Add** to add new user account. You can set user type, password and other permissions. Password can be identified strong, medium or weak depending on its complexity.

Select a user account, click **Edit** to modify user information.

Select a user account, click **Delete** to delete user information.

Online Users

Online users that log in to the device will be displayed on the list.

Click **Configuration → System → User Management → Online Users** to view information of users that log in to the device, including username, user type, IP address and user operation time. Click **Refresh** to refresh all user information.

Caution

Only one piece of user login information will be displayed if the IP addresses and usernames are respectively the same.
Up to 30 pieces of user login information will be displayed on the online users page.

7.4.3 Network Settings

TCP/IP

TCP/IP settings must be properly configured before you operate the device over network. IPv4 and IPv6 are both supported. Both versions can be configured simultaneously without conflicting to each other.

Click **Configuration → Network → Basic Settings → TCP/IP** to enter the settings page.

NIC Type

Select a NIC (Network Interface Card) type according to your network condition.

IPv4

Two IPv4 modes are available.

DHCP

The device automatically gets the IPv4 parameters from the network if you check **DHCP**. The device IP address is modified after enabling the function. You can use SADP to get the device IP address.

Note

The network that the device is connected to should support DHCP (Dynamic Host Configuration Protocol).

Manual

You can set the device IPv4 parameters manually. Input **IPv4 Address**, **IPv4 Subnet Mask**, and **IPv4 Default Gateway**, and click **Test** to see if the IP address is available.

IPv6

Three IPv6 modes are available.

Route Advertisement

The IPv6 address is generated by combining the route advertisement and the device Mac address.

Note

Route advertisement mode requires the support from the router that the device is connected to.

DHCP

The IPv6 address is assigned by the server, router, or gateway.

Manual

Input **IPv6 Address**, **IPv6 Subnet**, **IPv6 Default Gateway**. Consult the network administrator for required information.

MTU

It stands for maximum transmission unit. It is the size of the largest protocol data unit that can be communicated in a single network layer transaction.

The valid value range of MTU is 1280 to 1500.

Multicast

Check the **Enable Multicast Discovery**, and input **Multicast Address**, the online device can be automatically detected by client software via private multicast protocol in the LAN.

DNS

It stands for domain name server. It is required if you need to visit the device with domain name. And it is also required for some applications (e.g., sending email). Set **Preferred DNS Server** and **Alternate DNS server** properly if needed.

DDNS

You can use the Dynamic DNS (DDNS) for network access. The dynamic IP address of the device can be mapped to a domain name resolution server to realize the network access via domain name.

Before You Start

Registration on the DDNS server is required before configuring the DDNS settings of the device.

Steps

1. Refer to ***TCP/IP*** to set DNS parameters.
2. Go to the DDNS settings page: **Configuration → Network → Basic Settings → DDNS** .
3. Check **Enable DDNS** and select **DDNS type**.

   DynDNS

   Dynamic DNS server is used for domain name resolution.

   NO-IP

   NO-IP server is used for domain name resolution.
4. Input the domain name information, and click **Save**.
5. Check the device ports and complete port mapping. Refer to ***Port*** to check the device port , and refer to ***Port Mapping*** for port mapping settings.
6. Access the device.

By Browsers	Enter the domain name in the browser address bar to access the device.
By Client Software	Add domain name to the client software. Refer to the client manual for specific adding methods.

Set PPPoE

This device supports the PPPoE auto dial-up function. The device gets a public IP address by ADSL dial-up after the device is connected to a modem. You need to configure the PPPoE parameters of the device.

Steps

1. Click **Configuration → Network → Basic Settings → PPPoE** .
2. Check **Enable PPPoE**.
3. Set the PPPoE parameters.

   Dynamic IP

   After successful dial-up, the dynamic IP address of the WAN is displayed.

   User Name

   User name for dial-up network access.

   Password

   Password for dial-up network access.

   Confirm

   Input your dial-up password again.
4. Click **Save**.
5. Access the device.

By Browsers	Enter the WAN dynamic IP address in the browser address bar to access the device.
By Client Software	Add the WAN dynamic IP address to the client software. Refer to the client manual for details.

Note

The obtained IP address is dynamically assigned via PPPoE, so the IP address always changes after rebooting the camera. To solve the inconvenience of the dynamic IP, you need to get a domain name from the DDNS provider (e.g. DynDns.com). Refer to ***DDNS*** for detail information.

Port

The device port can be modified when the device cannot access the network due to port conflicts.

Caution

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

Go to **Configuration → Network → Basic Settings → Port** for port settings.

HTTP Port

It refers to the port through which the browser accesses the device. For example, when the **HTTP Port** is modified to 81, you need to enter ***http://192.168.1.64:81*** in the browser for login.

RTSP Port

It refers to the port of real-time streaming protocol.

HTTPS Port

It refers to the port through which the browser accesses the device with certificate. Certificate verification is required to ensure the secure access.

Server Port

It refers to the port through which the client adds the device.

Enhanced SDK Service Port

It refers to the port through which the client adds the device. Certificate verification is required to ensure the secure access.

WebSocket Port

TCP-based full-duplex communication protocol port for plug-in free preview.

WebSockets Port

TCP-based full-duplex communication protocol port for plug-in free preview. Certificate verification is required to ensure the secure access.

Note

- Enhanced SDK Service Port, WebSocket Port, and WebSockets Port are only supported by certain models.
- For device models that support that function, go to **Configuration → Network → Advanced Settings → Network Service** to enable it.

Port Mapping

By setting port mapping, you can access devices through the specified port.

Before You Start

When the ports in the device are the same as those of other devices in the network, refer to ***Port*** to modify the device ports.

Steps

1. Go to **Configuration → Network → Basic Settings → NAT** .
2. Select the port mapping mode.

   Auto Port Mapping Refer to ***Set Auto Port Mapping*** for detailed information.

   Manual Port Mapping Refer to ***Set Manual Port Mapping*** for detailed information.
3. Click **Save**.

Set Auto Port Mapping

Steps

1. Check **Enable UPnP™**, and choose a friendly name for the camera, or you can use the default name.
2. Select the port mapping mode to **Auto**.
3. Click **Save**.

Note

UPnP™ function on the router should be enabled at the same time.

Set Manual Port Mapping

Steps

1. Check **Enable UPnP™**, and choose a friendly name for the device, or you can use the default name.
2. Select the port mapping mode to **Manual**, and set the external port to be the same as the internal port.
3. Click **Save**.

What to do next

Go to the router port mapping settings interface and set the port number and IP address to be the same as those on the device. For more information, refer to the router user manual.

SNMP

You can set the SNMP network management protocol to get the alarm event and exception messages in network transmission.

Before You Start

Before setting the SNMP, you should download the SNMP software and manage to receive the device information via SNMP port.

Steps

1. Go to the settings page: **Configuration → Network → Advanced Settings → SNMP** .
2. Check **Enable SNMPv1**, **Enable SNMP v2c** or **Enable SNMPv3**.

Note

The SNMP version you select should be the same as that of the SNMP software.
And you also need to use the different version according to the security level required. SNMP v1 is not secure and SNMP v2 requires password for access. And SNMP v3 provides encryption and if you use the third version, HTTPS protocol must be enabled.

3. Configure the SNMP settings.

4. Click **Save**.

Set FTP

Set FTP parameters if you want to upload the captured pictures to the FTP server.

Before You Start
Set the FTP server, and ensure the device can communicate normally with the server.

Steps
1. Go to **Configuration → Device Configuration → Encoding and Storage → FTP** .
2. **Optional:** Check **Upload Additional Information to FTP**, and then the related information can be attached when uploading.
3. Enable the FTP server.
4. Set FTP parameters.
   1) Enter **Server Address** and **Port**.
   2) Enter **User Name** and **Password**, and confirm the password.
   3) Select **Directory Structure**.

   Note
   If multiple directories are needed, you can customize the directory name.
5. Set the name rule and separator according to the actual needs.
6. **Optional:** Edit OSD information which can be uploaded to the FTP server with the pictures to make it convenient to view and distinguish the data.
7. **Optional:** Click **Test** to test the FTP server connection.

   Note
   The test is single-use. You cannot test the connection repeatedly.
8. Click **Save**.

Set Email

When the email is configured and **Send Email** is enabled as a linkage method, the device sends an email notification to all designated receivers if an alarm event is detected.

Before You Start
Set the DNS server before using the Email function. Click **Configuration → Network → Basic Settings → TCP/IP** for DNS settings.

Steps
1. Click email settings page: **Configuration → Network → Advanced Settings → Email** .
2. Set email parameters.
   1) Input the sender's email information, including the **Sender's Address**, **SMTP Server**, and **SMTP Port**.

2) **Optional:** If your email server requires authentication, check **Authentication** and input your user name and password to log in to the server.
3) Set the **E-mail Encryption**.
   - When you select **SSL** or **TLS**, and disable STARTTLS, emails are sent after encrypted by SSL or TLS. The SMTP port should be set as 465.
   - When you select **SSL** or **TLS** and **Enable STARTTLS**, emails are sent after encrypted by STARTTLS, and the SMTP port should be set as 25.

   Note

   If you want to use STARTTLS, make sure that the protocol is supported by your email server. If you check the **Enable STARTTLS** while the protocol is not supported by your email sever, your email is sent with no encryption.
4) **Optional:** If you want to receive notification with alarm pictures, check **Attached Image**. The notification email has 3 attached alarm pictures about the event with configurable image capturing interval.
5) Input the receiver's information, including the receiver's name and address.
6) Click **Test** to see if the function is well configured.

3. Click **Save**.

Accessing via Mobile Client

Hik-Connect is an application for mobile devices. Using the App, you can view live image, receive alarm notification and so on.

Note

Hik-Connect service should be supported by the device.

Enable Hik-Connect Service on Camera

Hik-Connect service should be enabled on your camera before using the service.

You can enable the service through SADP software or Web browser.

Set Up Hik-Connect

Steps

1. Get and install Hik-Connect application by the following ways.
- Visit ***https://appstore.hikvision.com*** to download the application according to your mobile phone system.
- Visit the official site of our company. Then go to **Support → Tools → Hikvision App Store** .
- Scan the QR code below to download the application.

Note

If errors like "Unknown app" occur during the installation, solve the problem in two ways.

- Visit ***https://appstore.hikvision.com/static/help/index.html*** to refer to the troubleshooting.
- Visit ***https://appstore.hikvision.com/*** , and click **Installation Help** at the upper right corner of the interface to refer to the troubleshooting.

2. Start the application and register for a Hik-Connect user account.
3. Log in after registration.

Add Device to Hik-Connect

Steps

1. Connect your mobile device to a Wi-Fi.
2. Log into the Hik-Connect app.
3. In the home page, tap "+" on the upper-right corner to add a camera.
4. Scan the QR code on camera body or on the *Quick Start Guide* cover.

Note

If the QR code is missing or too blur to be recognized, you can also add the camera by inputting the camera's serial number.

5. Input the verification code of your camera.

Note

- The required verification code is the code you create or change when you enable Hik-Connect service on the camera.
- If you forget the verification code, you can check the current verification code on **Platform Access** configuration page via web browser.

6. Tap **Connect to a Network** button in the popup interface.
7. Choose **Wired Connection** or **Wireless Connection** according to your camera function.

Wireless Connection	Input the Wi-Fi password that your mobile phone has connected to, and tap **Next** to start the Wi-Fi connection process. (Locate the camera within 3 meters from the router when setting up the Wi-Fi.)
Wired Connection	Connect the camera to the router with a network cable and tap **Connected** in the result interface.

Note

The router should be the same one which your mobile phone has connected to.

8. Tap **Add** in the next interface to finish adding.

   For detailed information, refer to the user manual of the Hik-Connect app.

Set ISUP

When the device is registered on ISUP platform (formerly called Ehome), you can visit and manage the device, transmit data, and forward alarm information over public network.

Steps

1. Go to **Configuration → Network → Advanced Settings → Access Platform** .
2. Select **ISUP** as the platform access mode.
3. Check **Enable**.
4. Select a protocol version and input related parameters.
5. Click **Save**.

   Register status turns to **Online** when the function is correctly set.

Set HTTPS

HTTPS is a network protocol that enables encrypted transmission and identity authentication, which improves the security of remote access.

Steps

1. Go to **Configuration → Network → Advanced Settings → HTTPS** .
2. Check **Enable**.
3. **Optional:** Check **HTTPS Browsing** to access the device only via HTTPS protocol.
4. Select a server certificate.

   Note

   - Complete certificate management before selecting server certificate.
   - If the function is abnormal, check if the selected certificate is abnormal in **Certificate Management**.

5. Click **Save**.

Set QoS

QoS (Quality of Service) can help improve the network delay and network congestion by setting the priority of data sending.

Note

QoS needs support from network device such as router and switch.

Steps

1. Go to **Configuration → Network → Advanced Configuration → QoS** .
2. Set **Video/Audio DSCP**, **Alarm DSCP** and **Management DSCP**.

Note

Network can identify the priority of data transmission. The bigger the DSCP value is, the higher the priority is. You need to set the same value in router while configuration.

3. Click **Save**.

Set IEEE 802.1X

IEEE 802.1x is a port-based network access control. It enhances the security level of the LAN/ WLAN. When devices connect to the network with IEEE 802.1x standard, the authentication is needed.

Go to **Configuration → Network → Advanced Settings → 802.1X** , and enable the function.

Set **Protocol** and **EAPOL Version** according to router information.

Protocol

If you use EAP-MD5, the authentication server must be configured. Register a user name and password for 802.1X in the server in advance. Input the user name and password for authentication.

EAPOL Version

The EAPOL version must be identical with that of the router or the switch.

Set Open Network Video Interface

If you need to access the device through Open Network Video Interface protocol, you can configure the user settings to enhance the network security.

Steps

1. Go to **Configuration → Network → Advanced Settings → Integration Protocol** .
2. Check **Enable Hikvision-CGI**.
3. Check **Enable ONVIF**.
4. Click **Add** to configure the Open Network Video Interface user.

   Delete Delete the selected Open Network Video Interface user.

   Edit Edit the selected Open Network Video Interface user.
5. Click **Save**.
6. **Optional:** Repeat the steps above to add more Open Network Video Interface users.

Set Network Service

You can control the ON/OFF status of certain protocol as desired.

Steps

Note

This function varies according to different models.

1. Go to **Configuration → Network → Advanced Settings → Network Service** .
2. Set network service.

WebSocket & WebSockets

WebSocket or WebSockets protocol should be enabled if you use Google Chrome 57 and its above version or Mozilla Firefox 52 and its above version to visit the device. Otherwise, live view, image capture, digital zoom, etc. cannot be used.

If the device uses HTTP, enable WebSocket.

If the device uses HTTPS, enable WebSockets.

When you use WebSockets, select the **Server Certificate**.

Note

Complete certificate management before selecting server certificate.

SDK Service & Enhanced SDK Service

Check **Enable SDK Service** to add the device to the client software with SDK protocol.

Check **Enable Enhanced SDK Service** to add the device to the client software with SDK over TLS protocol.

When you use Enhanced SDK Service, select the **Server Certificate**.

Note

- Complete certificate management before selecting server certificate.
- When set up connection between the device and the client software, it is recommended to use Enhanced SDK Service and set the communication in Arming Mode to encrypt the data transmission. See the user manual of the client software for the arming mode settings.

TLS (Transport Layer Security)

The device offers TLS1.1, TLS1.2 and TLS1.3. Enable one or more protocol versions according to your need.

3. Click **Save**.

Set Alarm Server

The device can send alarms to destination IP address or host name through HTTP, HTTPS, or ISUP protocol. The destination IP address or host name should support HTTP, HTTP, or ISUP data transmission.

Steps

1. Go to **Configuration → Network → Advanced Settings → Alarm Server** .
2. Enter **Destination IP or Host Name**, **URL**, and **Port**.
3. **Optional:** Check **Enable** to enable ANR.
4. Select **Protocol**.

Note

HTTP, HTTPS, and ISUP are selectable. It is recommended to use HTTPS, as it encrypts the data transmission during communication.

5. Click **Test** to check if the IP or host is available.
6. Click **Save**.

7.4.4 Video/Audio Settings

Follow the instructions below to configure the video setting, audio settings, ROI, Display info. on Stream, etc.

Set Video Parameters

This part introduces the settings of video parameters, such as, stream type, video encoding, and resolution.

Click **Configuration → Video/Audio → Video** to enter the settings page.

Stream Type

Select the stream type as **Main Stream** or **Sub Stream**.

Video Type

Select the stream type to video stream, or video & audio composite stream. The audio signal will be recorded only when the **Video Type** is **Video & Audio**.

Resolution

Select the resolution of the video output.

Bitrate Type

Select the bitrate type to constant or variable.

Video Quality

When bitrate type is selected as Variable, 6 levels of video quality are selectable.

Video Frame Rate

Set the frame rate. The frame rate is to describe the frequency at which the video stream is updated and it is measured by frames per second (fps). A higher frame rate is advantageous when there is movement in the video stream, as it maintains image quality throughout.

Max. Bitrate

Set the max. bitrate from 32 to 16384 Kbps. The higher value corresponds to the higher video quality, but the better bandwidth is required.

Video Encoding

The device supports H.264 and H.265.

Smart264 and Smart265

Smart264

If you set the main stream as the stream type, and H.264 as the video encoding, you can see Smart264 available. Smart264 is an improved compression coding technology based on H. 264. By enabling Smart264, users can estimate the HDD consumption by its maximum average bitrate. Compared to H.264, Smart264 reduces storage by up to 50% with the same maximum bitrate in most scenes.

Smart265

If you set the main stream as the stream type, and H.265 as the video encoding, you can see Smart265 available. Smart265 is an improved compression coding technology based on H. 265. By enabling Smart265, users can estimate the HDD consumption by its maximum average bitrate. Compared to H.265, Smart265 reduces storage by up to 50% with the same maximum bitrate in most scenes.

I Frame Interval

Set I Frame Interval from 1 to 400.

SVC

Scalable Video Coding is an extension of the H.264/AVC and H.265 standard. Select OFF/ON to disable/enable the SVC function. Select Auto and the device will automatically extract frames from the original video when the network bandwidth is insufficient.

Bitstream Smoothing

It refers to the smoothness of the stream. The higher value of the smoothing is, the better fluency of the stream will be, though, the video quality may not be so satisfactory. The lower value of the smoothing is, the higher quality of the stream will be, though it may appear not fluent.

Click **Save** to enable the settings.

Set Audio Parameters

You can configure the audio settings for the camera on the Web.

Note

Audio settings may vary with the camera models.

Click **Configuration → Video/Audio → Audio** to configure the audio settings.

The audio settings includes the audio encoding, audio input, input volume and the environment noise filter.

Audio Encoding

G.722.1, G.711 ulaw, G.711alaw, G.726, MP2L2 and PCM are selectable. For MP2L2, the Sampling Rate and Audio Stream Bitrate are configurable. For PCM, the Sampling Rate can be set.

Audio Input

LineIn is selectable for the pickup respectively.

Input Volume

0 to 100 adjustable.

Environmental Noise Filter

Set it as **Disable** or **Enable**. When the function is enabled, the noise in the environment can be filtered to some extent.

Click **Save** to enable the settings.

Set ROI

ROI (Region of Interest) encoding helps to assign more encoding resource to the region of interest, thus to increase the quality of the ROI whereas the background information is less focused.

Before You Start

Please check the video coding type. ROI is supported when the video coding type is H.264 or H. 265.

Steps

1. Click **Configuration → Video/Audio → ROI** .
2. Check **Enable**.
3. Select **Stream Type**.
4. Select **Region No.** in **Fixed Region** to draw ROI region.
   1) Click **Draw Area**.
   2) Click and drag the mouse on the view screen to draw the fixed region.
   3) Click **Stop Drawing**.

   Note

   Select the fixed region that needs to be adjusted and drag the mouse to adjust its position.
5. Input the **Region Name** and select **ROI Level**.
6. Click **Save**.

   Note

   The higher the ROI level is, the clearer the image of the detected region is.

7. **Optional:** Select other region No. and repeat the above steps if you need to draw multiple fixed regions.

Display Info. on Stream

The information of the objects (e.g. human, vehicle, etc.) is marked in the video stream. You can set rules on the connected rear-end device or client software to detect the events including line crossing, intrusion, etc.

Steps

1. Click the setting page: **Configuration → Video/Audio → Display Info. on Stream** .
2. Check **Enable Smart Post Retrieval**.
3. Click **Save**.

7.4.5 Image Settings

Set Display Parameters

It offers the parameter settings to adjust image features.

Click **Configuration → Image → Display Settings** to enter the settings page.

Image Adjustment

By adjusting the **Brightness**, **Saturation**, **Contrast** and **Sharpness**, the image can be best displayed.

Exposure Settings

Exposure is controlled by the combination of iris. You can adjust image effect by setting exposure parameters.

Day/Night Switch

Day/Night Switch function can provide color images in the day mode and black/white images in the night mode. Switch mode is configurable.

Day

The image is always in color.

Night

The image is always black/white.

Auto

The camera switches between the day mode and the night mode according to the illumination automatically.

Scheduled-Switch

Set the **Start Time** and the **End Time** to define the duration for day mode.

Note

Day/Night Switch function varies according to models.

Supplement Light

Smart Supplement Light

This feature uses smart image processing technology to reduce overexposure caused by supplement light.

IR Light Mode

When the mode is set to Auto, the supplement light is automatically turned in or off according to the image brightness.

Brightness Limit

Adjust the upper limit of supplement light power.

Blacklight

BLC

If you focus on an object against strong backlight, the object will be too dark to be seen clearly. BLC (backlight compensation) compensates light to the object in the front to make it clear. If BLC mode is set as **Custom**, you can draw a red rectangle on the live view image as the BLC area.

WDR

The WDR (Wide Dynamic Range) function helps the camera provide clear images in environment with strong illumination differences. When there are both very bright and very dark areas simultaneously in the field of view, you can enable the WDR function and set the level. WDR automatically balances the brightness level of the whole image and provides clear images with more details.

Note

When WDR is enabled, some other functions may be not supported. Refers to the actual page for details.

HLC

When the bright area of the image is over-exposed and the dark area is under-exposed, the HLC (High Light Compression) function can be enabled to weaken the bright area and brighten the dark area, so as to achieve the light balance of the overall picture.

White Balance

White balance is the white rendition function of the camera. It is used to adjust the color temperature according to the environment.

Image Enhancement

Digital Noise Reduction

DNR reduces the noise in the video stream. OFF, Normal Mode and Expert Mode are selectable. Under normal mode, set the DNR level from 0 to 100, and the default value is 50. Under expert mode, you can set Space DNR Level and Time DNR Level separately.

Gray Scale

You can choose the range of the grey scale as [0 to 255] or [16 to 235].

Video Adjustment

Adjust the **Mirror** and **Video Standard** of the video to fit the environment.

Click **Default** to restore settings.

Set OSD

You can customize OSD (On-screen Display) information such as device name, time/date, font, color, and text overlay displayed on video stream.

Click **Configuration → Image → OSD Settings** . Set the corresponding parameters, and click **Save** to enable the settings.

Displayed Information

Set camera name, date, week, and their related display format.

Text Overlay

Set customized overlay text on image.

OSD Parameters

Set OSD parameters, such as **Display Mode**, **OSD Size**, **OSD Color**, and **Alignment**.

Set Privacy Mask

Privacy mask enables you to cover certain areas on the live video to prevent certain spots in the surveillance area from being live viewed and recorded.

Steps

Note

Privacy Mask function may not be supported by certain display modes, refer to the actual interface for detailed information.

1. Click **Configuration → Image → Privacy Mask** .
2. Check **Enable Privacy Mask** to enable the function.
3. Draw the mask area.
   1) Click **Draw Area** to start drawing.
   2) Click and drag the mouse in the live video window to draw the mask area.

3) Click **Stop Drawing** to finish drawing.

4. **Optional:** Click **Clear All** to clear all the configured privacy masks.
5. Click **Save**.

Image Parameters Switch

The device automatically switches image parameters in set time periods.

Click **Configuration → Image → Image Parameters Switch** , and set parameters as needed.

7.4.6 Event and Alarm Settings

This part introduces the configuration of events. The device takes certain response to triggered alarm.

Schedule and Linkage Settings

Set Arming Schedule

Set the valid time of the device tasks.

Steps

1. Click **Arming Schedule**.
2. Drag the time bar to draw desired valid time.

Note

Up to 8 periods can be configured for one day.

3. Adjust the time period.
   - Click on the selected time period, and enter the desired value. Click **Save**.
   - Click on the selected time period. Drag the both ends to adjust the time period.
   - Click on the selected time period, and drag it on the time bar.
4. **Optional:** Click **Copy to...** to copy the same settings to other days.
5. Click **Save**.

Linkage Method Settings

You can enable the linkage functions when an event or alarm occurs.

Send Email

Check **Send Email**, and the device sends an email to the designated addresses with alarm information when an alarm event is detected.

For email settings, refers to ***Set Email*** .

Notify Surveillance Center

Check **Notify Surveillance Center**, the alarm information is uploaded to the surveillance center when an alarm event is detected.

FTP/NAS/Memory Card Uploading

If you have enabled and configured the FTP/NAS/memory card uploading, the device sends the alarm information to the FTP server, network attached storage and memory card when an alarm is triggered.

Refers to ***Set FTP*** to set the FTP server.

Refers to ***Set NAS*** for NAS configuration.

Refers to ***Set Encrypted Memory Card*** for memory card storage configuration.

Trigger Recording

Check **Trigger Recording**, and the device records the video about the detected alarm event.

Basic Event

Set Motion Detection

This function detects moving objects in the detection region and trigger linkage actions.

Steps

1. Click **Configuration → Event → Basic Event → Motion Detection** .
2. Check **Enable Motion Detection**.
3. **Optional:** Highlight moving objects in green.
   1) Check **Enable Dynamic Analysis for Motion**.
   2) Click **Configuration → Local** to enable **Rules**.
4. Select **Configuration Mode**. Normal mode and expert mode are selectable.
5. Set the arming schedule. See ***Set Arming Schedule*** for details.
6. Set linkage methods. See ***Linkage Method Settings*** for details.

7. Click **Save**.

Set Video Tampering Alarm

When the configured area is covered and cannot be monitored normally, the alarm is triggered and the device takes certain alarm response actions.

Steps

1. Go to **Configuration → Event → Basic Event → Video Tampering** .
2. Check **Enable**.
3. Set the **Sensitivity**. The higher the value is, the easier to detect the area covering.
4. Click **Draw Area** and drag the mouse in the live view to draw the area.

Stop Drawing	Finish drawing.
Clear All	Delete all the drawn areas.

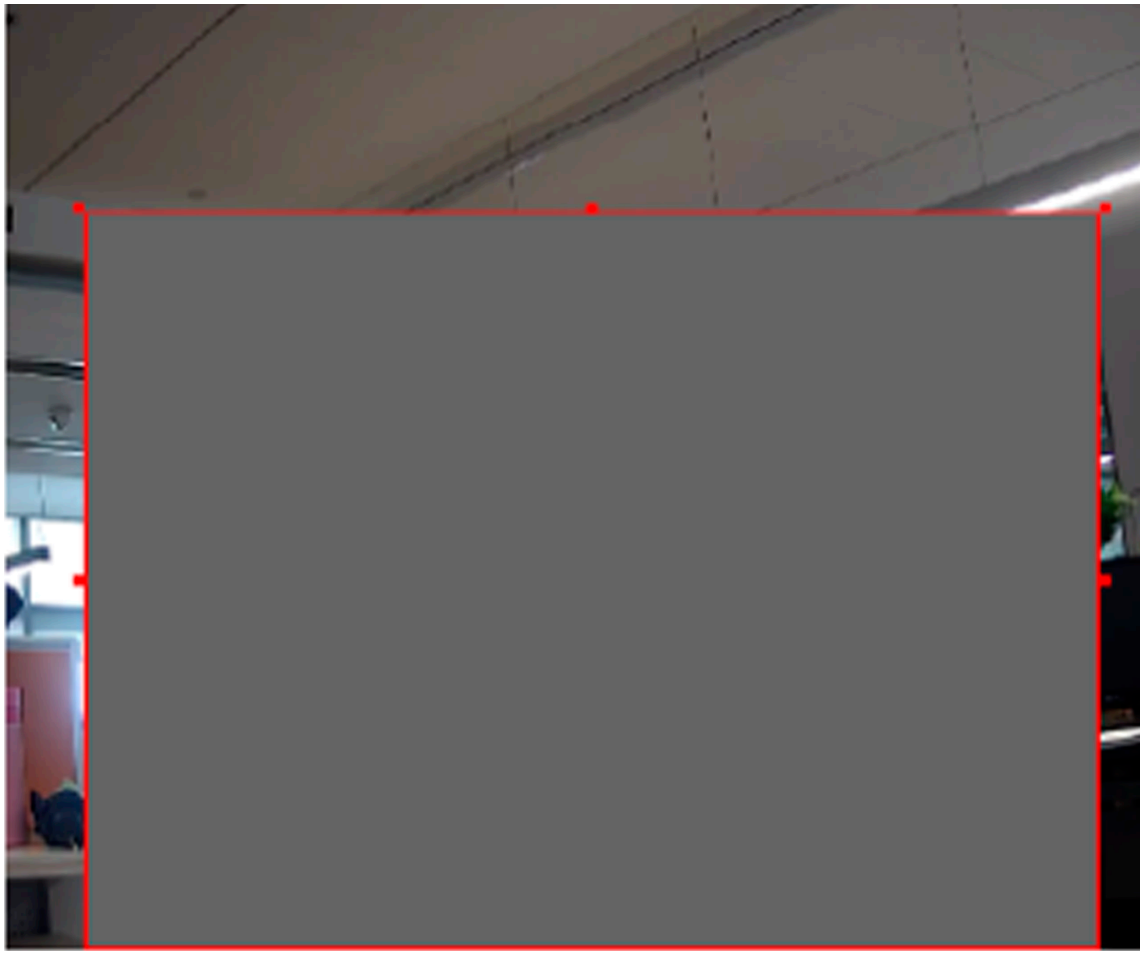


Figure 7-5 Set Video Tampering Area

5. Refers to for setting scheduled time. Refers to ***Set Arming Schedule*** for setting linkage method.

6. Click **Save**.

Set Alarm Input

Alarm signal from the external device triggers the corresponding actions of the current device.

Before You Start
Make sure the external alarm device is connected. See *Quick Start Guide* for cable connection.

Steps
1. Click **Configuration → Event → Basic Event → Alarm Input** .
2. Check **Enable Alarm Input Handling**.
3. Select **Alarm Input NO.** and **Alarm Type** from the dropdown list. Edit the **Alarm Name**.
4. Refers to ***Set Arming Schedule*** for setting scheduled time. Refers to ***Linkage Method Settings*** for setting linkage method.
5. Click **Copy to...** to copy the settings to other alarm input channels.
6. Click **Save**.

Set Alarm Output

If the device has been connected to an alarm output device, and the alarm output No. has been configured, the device sends alarm information to the connected alarm output device when an alarm is triggered.

Steps
1. Click **Configuration → Event → Basic Event → Alarm Output** .
2. Set alarm output parameters.

   Automatic Alarm For the information about the configuration, see ***Automatic Alarm*** .

   Manual Alarm For the information about the configuration, see ***Manual Alarm*** .
3. Click **Save**.

Automatic Alarm

Set the automatic alarm parameters, then the device triggers an alarm output automatically in the set arming schedule.

Steps
1. Set automatic alarm parameters.

   Alarm Output No.

   Select the alarm output No. according to the alarm interface connected to the external alarm device.

   Alarm Name

Custom a name for the alarm output.

Delay

It refers to the time duration that the alarm output remains after an alarm occurs.

2. Set the alarming schedule. For the information about the settings, see ***Set Arming Schedule*** .
3. Click **Copy to…** to copy the parameters to other alarm output channels.
4. Click **Save**.

Manual Alarm

You can trigger an alarm output manually.

Steps

1. Set the manual alarm parameters.

Alarm Output No.

Select the alarm output No. according to the alarm interface connected to the external alarm device.

Alarm Name

Edit a name for the alarm output.

Delay

Select **Manual**.

2. Click **Manual Alarm** to enable manual alarm output.
3. **Optional:** Click **Clear Alarm** to disable manual alarm output.

Set Exception Alarm

Exception such as network disconnection can trigger the device to take corresponding action.

Steps

1. Click **Configuration → Event → Basic Event → Exception** .
2. Select **Exception Type**.

HDD Full	The HDD storage is full.
HDD Error	Error occurs in HDD.
Network Disconnected	The device is offline.
IP Address Conflicted	The IP address of current device is same as that of other device in the network.
Illegal Login	Incorrect user name or password is entered.
Voltage Instable	The power supply voltage is fluctuating.

3. Refers to ***Linkage Method Settings*** for setting linkage method.
4. Click **Save**.

Set Smoke Detection

Smoke detection function detects the concentration of the smoke. When the concentration of the smoke is over the limit, the alarm will be triggered.

Steps

1. Click **Configuration → Event → Normal Event → Smoke Detection** .
2. Check **Enable Smoke Alarm Report**.

   When smoke alarm is triggered, the alarm information and image will be uploaded to the center and FTP.
3. Check **Pollution Data Upload**.

   When smoke alarm is triggered, the pollution data will be uploaded to the center periodically by settings reporting interval.
4. Slide to adjust **Smoke Detector Sensitivity** and **Reporting Interval**.
5. Set arming schedule. See ***Set Arming Schedule*** .
6. Set linkage method. See ***Linkage Method Settings*** .
7. Click **Save**.

Set Tampering Alarm

Steps

1. Click **Configuration → Event → Normal Event → Tampering Alarm** .
2. Check **Enable** to enable the function.
3. Set arming schedule. See ***Set Arming Schedule*** .
4. Set linkage method. See ***Linkage Method Settings*** .
5. Click **Save**.

Set Temperature Measurement

Temperature measurement function detects the temperature of the environment. When the temperature of the environment is over the limit, the alarm will be triggered.

Steps

1. Click **Configuration → Event → Normal Event → Temperature Measurement** .
2. Check **Enable** to enable the function.
3. Slide to adjust **Temperature Threshold**.

   When the temperature of environment is over the threshold, the alarm will be triggered.
4. Set arming schedule. See ***Set Arming Schedule*** .
5. Set linkage method. See ***Linkage Method Settings*** .
6. Click **Save**.

Smart Event

Set Intrusion Detection

Intrusion detection function detects people, vehicle or other objects which enter and loiter in a pre-defined virtual region, and some certain actions can be taken when the alarm is triggered.

Steps

1. Click **Configuration → Event → Smart Event → Intrusion Detection** .
2. Check **Enable**.
3. Select a region No. from the drop-down list of **Region**.
4. Set the **Max. Size** and **Min. Size** for valid targets. Targets smaller or larger than the valid target size are not able to trigger detection.

   Max. Size

   The maximum size of a valid target. Targets with larger sizes would not trigger detection.

   Min. Size

   The minimum size of a valid target. Targets with smaller sizes would not trigger detection.
5. Set the time threshold for intrusion detection.
6. Drag the slider to set the sensitivity value.
7. Set arming schedule. See ***Set Arming Schedule*** .
8. Set linkage method. See ***Linkage Method Settings*** .
9. Click **Save**.

Set Line Crossing Detection

Line crossing detection is used to detect the object movement of crossing a predefined line. When it occurs, the device takes linkage actions as response.

Steps

1. Click **Configuration → Event → Smart Event → Line Crossing Detection** .
2. Check **Enable**.
3. **Optional:** Click **Lock** to lock PTZ control to prevent the interruption from other PTZ related action during configuration.

   Normally, the PTZ control is automatically locked when you enter the configuration interface. You can manually resume the lock when the countdown is over.
4. Adjust the live image to the desired scene by using PTZ control buttons.
5. Draw detection line.

   1) Select a **Line No.**. Up to 4 lines can be set in the scene.

   2) Click **Detection Area**.

   A yellow line is displayed on live image.

3) Click on the line, and drag its end points to adjust the length and position.
4) Select the **Direction** for the detection line.

Direction

It stands for the direction from which the object goes across the line.

A<->B

The object going across the line from both directions can be detected and alarms are triggered.

A->B

Only the object crossing the configured line from side A to side B can be detected.

B->A

Only the object crossing the configured line from side B to side A can be detected.

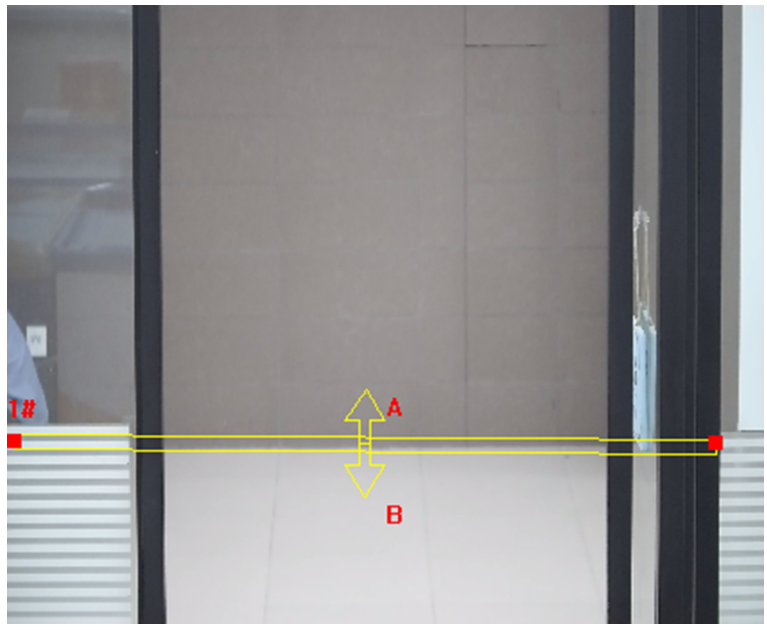


Figure 7-6 Draw Line

6. **Optional:** Set the minimum size and the maximum size for the target to improve detection accuracy. Only targets whose size are between the maximum size and the minimum size trigger the detection.
   1) Click **Max. Size**, and drag the mouse on live image. If you want to change the size, click the button and draw again.
   2) Click **Min. Size**, and drag the mouse on the live image. If you want to change the size, click the button and draw again.
7. Set detection parameters.

Sensitivity	It stands for the sensitivity of detecting an target. The higher the value is, the more easily the target is detected.

Detection Target You can specify the object type, and the device only detects the selected type of objects.

8. Click **Save**.
9. Repeat above steps to set other lines.
10. Set arming schedule. See ***Set Arming Schedule*** .
11. Set linkage method. See ***Linkage Method Settings*** .

Set Indoor Channel Blockage Detection

The function is developed to detect whether the indoor passages are blocked by old junk. If the duration reaches the setting, the fire alarm will be triggered and a series of operations will be executed.

Before You Start

Note

Fire Source Detection and On/Off Work Detection will be out of service when Indoor Channel Blockage Detection is enabled.

Steps

1. Click **Configuration → Event → Smart Event → Indoor Channel Blockage Detection** .
2. Click **Enable**.
3. Set detection area and disabled area.
   1) Click **Draw Detection Area**/**Draw Disabled Area**.
   2) Left-click to draw a convex quadrilateral.
   3) Repeat step a and step b to draw less than 4 detection areas/disabled areas.
   4) **Optional:** You can edit the areas you draw as follows.
      - Hover mouse inside an area and drag to change its location.
      - Hover mouse on the vertexes of an area and drag to adjust the their locations.
      - Click **Clear All** to delete all areas exist.

   Device will process smart detection and analysis on events in detection areas and neglect feedbacks from disabled areas.
4. Set detection parameters.

   Time Threshold(s)

   If the indoor channels are blocked by old junk and the duration reaches the setting, the fire alarm will be triggered.
5. Set arming schedule. See ***Set Arming Schedule*** .
6. Set linkage method. See ***Linkage Method Settings*** .
7. Click **Save**.

Fire Source Detection

The function is developed to detect the fire source in the detection area. If fire sources are spotted and the duration reaches the setting, the fire alarm will be triggered and a series of operations will be executed.

Before You Start

Note

Indoor Channel Blockage Detection and On/Off Work Detection will be out of service when Fire Source Detection is enabled.

Steps

1. Click **Configuration → Event → Smart Event → Fire Source Detection** .
2. Check **Enable**.
3. Set detection area and disabled area.
   1) Click **Draw Detection Area** /**Draw Disabled Area**.
   2) Left-click to draw a convex quadrilateral.
   3) Repeat step a and step b to draw less than 4 detection areas/disabled areas.
   4) **Optional:** You can edit the areas you drew as follows.
      - Hover mouse inside an area and drag to change its location.
      - Hover mouse on the vertexes of an area and drag to adjust the their locations.
      - Click **Clear All** to delete all areas exist.

   Device will process smart detection and analysis on events in detection areas and neglect feedbacks from desabled areas.
4. Set detection parameters.

   Time Threshold(s)

   If fire sources are spotted and the duration reaches the time setting, the fire alarm will be triggered.

   Sensitivity

   The more sensitive the detecting function is, the more easily the alarm will be triggered and the more likely to misidentify.
5. Set arming schedule. See ***Set Arming Schedule*** .
6. Set linkage method. See ***Linkage Method Settings*** .
7. Click **Save**.

Set On/Off Work Detection

The function is developed to detect whether the staff are on duty. If the number of detected persons in the zones does not reach the settings and the duration reaches the time settings, a series of operations will be executed.

Before You Start

Note

Indoor Passage Blockage Detection and Fire Source Detection will be out of service when On/Off Duty Detection is enabled.

Steps

1. Click **Configuration → Event → Smart Event → On/Off Work Detection** .
2. Check **Enable**.
3. Set detection area and disabled area.
   1) Click **Draw Detection Area**/**Draw Disabled Area**.
   2) Left-click to draw a convex quadrilateral.
   3) Repeat step a and step b to draw less than 4 detection areas/disabled areas.
   4) **Optional:** You can edit the areas you draw as follows.
      - Hover mouse inside a zone and drag to change its location.
      - Hover mouse on the vertexes of an area and drag to adjust the their locations.
      - Click **Clear All** to delete all areas exist.

   Device will process smart detection and analysis on events in detection areas and neglect feedbacks from disabled areas.
4. Set detection parameters.

   Number of Alarm People Threshold

   If the detected number of staff in the detection zone is less than the lower limit settings, the alarm will be triggered.

   Off Work Detection Time (s)

   If the number of off-work staff is under the settings and the duration reaches the time settings, the fire alarm will be triggered.

   Sensitivity

   The more sensitive the detecting function is, the more easily the alarm will be triggered and the more likely to misidentify.
5. Set arming schedule. See ***Set Arming Schedule*** .
6. Set linkage method. See ***Linkage Method Settings*** .
7. Click **Save**.

7.4.7 Storage Settings

Memory Card

You can view the capacity, free space, status, type, and property of the memory card. Encryption of memory card is supported to ensure data security.

Set New or Unencrypted Memory Card

Before You Start

Insert a new or unencrypted memory card to the device. For detailed installation, refer to *Quick Start Guide* of the device.

Steps

1. Click **Configuration → Storage → Storage Management → HDD Management** .
2. Select the memory card.

   Note

   If an **Unlock** button appears, you need to unlock the memory card first. See ***Detect Memory Card Status*** for details.
3. Click **Format** to initialize the memory card.

   When the **Status** of memory card turns from **Uninitialized** to **Normal**, the memory card is ready for use.
4. **Optional:** Encrypt the memory card.
   1) Click **Encrypted Format**.
   2) Set the encryption password.
   3) Click **OK**.

      When the **Encryption Status** turns to **Encrypted**, the memory card is ready for use.

   Note

   Keep your encryption password properly. Encryption password cannot be found if forgotten.
5. **Optional:** Define the **Quota** of the memory card. Input the percentage for storing different contents according to your needs.
6. Click **Save**.

Set Encrypted Memory Card

Before You Start

- Insert an encrypted memory card to the device. For detailed installation, refers to *Quick Start Guide* of the device.
- You need to know the correct encryption password of the memory card.

Steps

1. Click **Configuration → Storage → Storage Management → HDD Management** .
2. Select the memory card.

   Note

   If an **Unlock** button appears, you need to unlock the memory card first. See ***Detect Memory Card Status*** for details.

3. Verify the encryption password.
   1) Click **Parity**.
   2) Enter the encryption password.
   3) Click **OK**.

   When the **Encryption Status** turns to **Encrypted**, the memory card is ready for use.

Note

If the encryption password is forgotten and you still want to use this memory card, see ***Set New or Unencrypted Memory Card*** to format and set the memory card. All existing contents will be removed.

4. **Optional:** Define the **Quota** of the memory card. Input the percentage for storing different contents according to your needs.
5. Click **Save**.

Detect Memory Card Status

The device detects the status of Hikvision memory card. You receive notifications when your memory card is detected abnormal.

Before You Start

The configuration page only appears when a Hikvision memory card is installed to the device.

Steps

1. Click **Configuration → Storage → Storage Management → Memory Card Detection** .
2. Click **Status Detection** to check the **Remaining Lifespan** and **Health Status** of your memory card.

   Remaining Lifespan

   It shows the percentage of the remaining lifespan. The lifespan of a memory card may be influenced by factors such as its capacity and the bitrate. You need to change the memory card if the remaining lifespan is not enough.

   Health Status

   It shows the condition of your memory card. There are three status descriptions: good, bad, and damaged. You will receive a notification if the health status is anything other than good when the **Arming Schedule** and **Linkage Method** are set.

Note

It is recommended that you change the memory card when the health status is not "good".

3. Click **R/W Lock** to set the permission of reading and writing to the memory card.
   - Add a Lock
     a. Select the **Lock Switch** as ON.
     b. Enter the password.
     c. Click **Save**
   - Unlock

- If you use the memory card on the device that locks it, unlocking will be done automatically and no unlocking procedures are required on the part of users.
- If you use the memory card (with a lock) on a different device, you can go to **HDD Management** to unlock the memory card manually. Select the memory card, and click **Unlock**. Enter the correct password to unlock it.

- Remove the Lock
  a. Select the **Lock Switch** as OFF.
  b. Enter the password in **Password Settings**.
  c. Click **Save**.

Note

- Only admin user can set the **R/W Lock**.
- The memory card can only be read and written when it is unlocked.
- If the device, which adds a lock to a memory card, is restored to the factory settings, you can go to **HDD Management** to unlock the memory card.

4. Set **Arming Schedule** and **Linkage Method**. See ***Set Arming Schedule*** and ***Linkage Method Settings*** for details.
5. Click **Save**.

Set NAS

Take network server as network disk to store the record files, captured images, etc.

Before You Start
Get the IP address of the network disk first.

Steps
1. Go to NAS setting page: **Configuration → Storage → Storage Management → Net HDD** .
2. Click **HDD No.**. Enter the server address and file path for the disk.

   Server Address

   The IP address of the network disk.

   File Path

   The saving path of network disk files.

   Mounting Type

   Select file system protocol according to the operation system.

   Enter user name and password of the net HDD to guarantee the security if **SMB/CIFS** is selected.
3. Click **Test** to check whether the network disk is available.
4. Click **Save**.

Set Cloud Storage

It helps to upload the captured pictures and data to the cloud. The platform requests picture directly from the cloud for picture and analysis. The function is only supported by certain models.

Steps

Caution

If the cloud storage is enabled, the pictures are stored in the cloud video manager firstly.

1. Click **Configuration → Storage → Storage Management → Cloud Storage** .
2. Check **Enable Cloud Storage**.
3. Set basic parameters.

Protocol Version	The protocol version of the cloud video manager.
Server IP	The IP address of the cloud video manager. It supports IPv4 address.
Serve Port	The port of the cloud video manager. You are recommended to use the default port.
AccessKey	The key to log in to the cloud video manager.
SecretKey	The key to encrypt the data stored in the cloud video manager.
User Name and Password	The user name and password of the cloud video manager.
Picture Storage Pool ID	The ID of the picture storage region in the cloud video manager. Make sure storage pool ID and the storage region ID are the same.

4. Click **Test** to test the configured settings.
5. Click **Save**.

Record Automatically

This function can record video automatically during configured time periods.

Before You Start

Select **Trigger Recording** in event settings for each record type except **Continuous**. See ***Event and Alarm Settings*** for details.

Steps

1. Click **Configuration → Storage → Schedule Settings → Record Schedule** .
2. Check **Enable**.
3. Select a record type.

Note

The record type is vary according to different models.

Continuous

The video will be recorded continuously according to the schedule.

Motion

When motion detection is enabled and trigger recording is selected as linkage method, object movement is recorded.

Alarm

When alarm input is enabled and trigger recording is selected as linkage method, the video is recorded after receiving alarm signal from external alarm input device.

Motion | Alarm

Video is recorded when motion is detected or alarm signal is received from the external alarm input device.

Motion & Alarm

Video is recorded only when motion is detected and alarm signal is received from the external alarm input device.

Event

The video is recorded when configured event is detected.

4. Set schedule for the selected record type. Refer to ***Set Arming Schedule*** for the setting operation.
5. Click **Advanced** to set the advanced settings.

Overwrite

Enable **Overwrite** to overwrite the video records when the storage space is full. Otherwise the camera cannot record new videos.

Pre-record

The time period you set to record before the scheduled time.

Post-record

The time period you set to stop recording after the scheduled time.

Stream Type

Select the stream type for recording.

Note

When you select the stream type with higher bitrate, the actual time of the pre-record and post-record may be less than the set value.

Recording Expiration

The recordings are deleted when they exceed the expired time. The expired time is configurable. Note that once the recordings are deleted, they can not be recovered.

6. Click **Save**.

Capture Automatically

This function can capture pictures automatically during configured time periods.

Before You Start

If event-triggered capture is required, you should configure related linkage methods in event settings. Refer to ***Event and Alarm Settings*** for event settings.

Steps

1. Click **Configuration → Storage → Schedule Settings → Capture → Capture Parameters** .
2. Set the capture type.

   Timing

   Capture a picture at the configured time interval.

   Event-Triggered

   Capture a picture when an event is triggered.
3. Set the **Format**, **Resolution**, **Quality**, **Interval**, and **Capture Number**.
4. Refer to ***Set Arming Schedule*** for configuring schedule time.
5. Click **Save**.

7.4.8 The Third-Party Platform

Manage the Third-Party Software

Steps

Note

The open platform function may vary according to different device models. Refer to the actual device for details.

1. Click **Configuration → Open Platform → Application** .

   The installed programs and related information will be displayed on the **Application List**, including application name, operation, version, used memory, used flash, company, status and license.
2. **Optional:** The following operations can be launched on the **Application List**.
   - Click to export log files.
   - Click to configure permissions.
   - Click to start or stop applications.


See Far, Go Further