



# **Thermal & Optical Bi-spectrum PTZ Network Camera**

**User Manual**

## Legal Information

©2023 Hangzhou Hikvision Digital Technology Co., Ltd. All rights reserved.

### 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

# Thermal & Optical Bi-spectrum PTZ Network Camera User Manual




---

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 LATTER PREVAILS.

## Symbol Conventions

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

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

## Safety Instruction

These instructions are intended to ensure that user can use the product correctly to avoid danger or property loss.

### Laws and Regulations

- In the use of the product, you must be in strict compliance with the electrical safety regulations of the nation and region.

### Transportation

- Keep the device in original or similar packaging while transporting it.
- Keep all wrappers after unpacking 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 the company shall not take any responsibilities.
- Do not drop the product or subject it to physical shock. Keep the device away from magnetic interference.

### Power Supply

- Please purchase the charger by yourself. Input voltage should meet the Limited Power Source (24 VDC, or 24 VAC) according to the IEC62368 standard. Please refer to technical specifications for detailed information.
- Make sure the plug is properly connected to the power socket.
- The socket-outlet shall be installed near the equipment and shall be easily accessible.
- DO NOT connect multiple devices to one power adapter, to avoid over-heating or fire hazards caused by overload.
- DO NOT touch the bare metal contacts of the inlets after the circuit breaker is turned off. Electricity still exists.
- + identifies the positive terminal(s) of equipment which is used with, or generates direct current.  
- identifies the negative terminal(s) of equipment which is used with, or generates direct current.
- Ensure correct wiring of the terminals for connection to an AC mains supply.

### Battery

- Risk of explosion if the battery is replaced by an incorrect type. Dispose of used batteries according to the instructions. Il y a risque d'explosion si la batterie est remplacée par une batterie de type incorrect. Mettre au rebut les batteries usagées conformément aux instructions.
- The built-in battery cannot be dismantled. Please contact the manufacture for repair if necessary.
- For long-term storage of the battery, make sure it is fully charged every half year to ensure the battery quality. Otherwise, damage may occur.
- This equipment is not suitable for use in locations where children are likely to be present.

- 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.

### **Installation**

- Never place the equipment in an unstable location. The equipment may fall, causing serious personal injury or death.
- This equipment is for use only with corresponding brackets. Use with other (carts, stands, or carriers) may result in instability causing injury.


### **System Security**

- You acknowledge that the nature of Internet provides for inherent security risks, and our company shall not take any responsibilities for abnormal operation, privacy leakage or other damages resulting from cyber attack, hacker attack, however, our company will provide timely technical support if required.
- Please enforce the protection for the personal information and the data security as the device may be confronted with the network security problems when it is connected to the Internet. Please contact us when the device might exist network security risks.
- Please understand that you have the responsibility to configure all the passwords and other security settings about the device, and keep your user name and password.

### **Maintenance**

- If the product does not work properly, please contact your dealer or the nearest service center. We shall not assume any responsibility for problems caused by unauthorized repair or maintenance.
- A few device components (e.g., electrolytic capacitor) require regular replacement. The average lifespan varies, so periodic checking is recommended. Contact your dealer for details.
- Wipe the device gently with a clean cloth and a small quantity of ethanol, if necessary.
- If the equipment is used in a manner not specified by the manufacturer, the protection provided by the device may be impaired.
- To reduce the risk of fire, replace only with the same type and rating of fuse.
- The serial port of the equipment is used for debugging only.
- Disconnect the power source during servicing.

## Using Environment

- Make sure the running environment meets the requirement of the device. The operating temperature shall be -40°C to 60°C (-40°F to 140°F), and the operating humidity shall be 95% or less, no condensing.
- DO NOT expose the device to high electromagnetic radiation or dusty environments.
- DO NOT aim the lens at the sun or any other bright light.
- The equipment shall not be exposed to dripping or splashing and that no objects filled with liquids, such as vases, shall be placed on the equipment.
- No naked flame sources, such as lighted candles, should be placed on the equipment.
- Provide a surge suppressor at the inlet opening of the equipment under special conditions such as the mountain top, iron tower, and forest.
- Burned fingers when handling the parts with symbol . Wait one-half hour after switching off before handling the parts.

## Emergency

- If smoke, odor, or noise arises from the device, immediately turn off the power, unplug the power cable, and contact the service center.

COMPLIANCE NOTICE: The thermal series products might be subject to export controls in various countries or regions, including without limitation, the United States, European Union, United Kingdom and/or other member countries of the Wassenaar Arrangement. Please consult your professional legal or compliance expert or local government authorities for any necessary export license requirements if you intend to transfer, export, re-export the thermal series products between different countries.

# Contents

<b>Chapter 1 Overview .....</b>	<b>1</b>
1.1 Brief Description .....	1
1.2 Function .....	1
<b>Chapter 2 Device Activation and Accessing .....</b>	<b>2</b>
2.1 Activate the Device via SADP .....	2
2.2 Activate the Device via Browser .....	2
2.3 Login .....	3
2.3.1 Plug-in Installation .....	3
2.3.2 Illegal Login Lock .....	4
<b>Chapter 3 Temperature Measurement .....</b>	<b>5</b>
3.1 Notice .....	5
3.2 Thermography Configuration Flow Chart .....	5
3.3 Set Thermography Parameters .....	7
3.4 Automatic Thermography .....	8
3.4.1 Set Normal Mode .....	8
3.4.2 Set Expert Mode .....	9
3.4.3 Set Thermography Rule .....	9
3.5 Manual Thermography .....	11
3.6 Search History Temperature .....	12
<b>Chapter 4 Fire Source Detection .....</b>	<b>13</b>
4.1 Fire Detection Flow Chart .....	13
4.2 Recommended Scene .....	14
4.3 Set the Presets .....	14
4.4 Set Fire Detection Parameters .....	16
4.4.1 Set Fire Source Shielded Region .....	17
<b>Chapter 5 Intelligent Analysis .....</b>	<b>19</b>



5.1 Switch the Scene Mode .....	19
5.2 Set VCA Parameters .....	19
5.3 Configure Intelligent Analysis in Panorama View .....	20
5.4 Configure Intelligent Analysis .....	21
5.4.1 Set Detection Scenes and Tracking .....	21
5.4.2 Set Rules .....	22
5.4.3 Set the Scene Auto-Switch .....	23
5.5 Advanced Configuration .....	24
<b>Chapter 6 Event and Alarm .....</b>	<b>26</b>
6.1 Set Motion Detection .....	26
6.1.1 Normal Mode .....	26
6.1.2 Expert Mode .....	27
6.2 Set Video Tampering Alarm .....	28
6.3 Set Exception Alarm .....	29
6.4 Set Burning-Prevention .....	30
6.5 Detect Audio Exception .....	30
<b>Chapter 7 Arming Schedule and Alarm Linkage .....</b>	<b>32</b>
7.1 Set Arming Schedule .....	32
7.2 Linkage Method Settings .....	32
7.2.1 Trigger Alarm Output .....	32
7.2.2 FTP/NAS/Memory Card Uploading .....	34
7.2.3 Send Email .....	34
7.2.4 Notify Surveillance Center .....	35
<b>Chapter 8 PTZ .....</b>	<b>36</b>
8.1 PTZ Control .....	36
8.2 Set Preset .....	38
8.2.1 Special Presets .....	38
8.3 Set Patrol Scan .....	39

8.3.1 Set One-Touch Patrol .....	40
8.4 Set Linear Scan .....	40
8.5 Set Initial Position .....	41
8.6 Set Scheduled Tasks .....	41
8.7 Set Park Action .....	42
8.8 Set Privacy Mask .....	43
8.9 Set Device Position .....	43
8.9.1 Set Manual Compass .....	44
8.9.2 Set Auto Compass .....	44
8.10 Set Power Off Memory .....	45
8.11 Set PTZ Priority .....	45
<b>Chapter 9 Live View .....</b>	<b>46</b>
9.1 Live View Parameters .....	46
9.1.1 Window Division .....	46
9.1.2 Live View Stream Type .....	46
9.1.3 Enable and Disable Live View .....	46
9.1.4 View Previous/Next Page .....	46
9.1.5 Full Screen .....	47
9.1.6 Set Panorama Map .....	47
9.1.7 Conduct Regional Focus .....	47
9.1.8 Light .....	48
9.1.9 Wiper .....	48
9.1.10 Lens Initialization .....	48
9.1.11 Auxiliary Focus .....	48
9.1.12 Quick Set Live View .....	48
9.1.13 Lens Parameters Adjustment .....	49
9.1.14 Conduct 3D Positioning .....	49
9.1.15 Lens Demist .....	49

9.1.16 Synchronize FOV .....	50
9.2 Set Transmission Parameters .....	50
<b>Chapter 10 Video and Audio .....</b>	<b>52</b>
10.1 Video Settings .....	52
10.1.1 Stream Type .....	52
10.1.2 Video Type .....	52
10.1.3 Resolution .....	52
10.1.4 Bitrate Type and Max. Bitrate .....	53
10.1.5 Video Quality .....	53
10.1.6 Frame Rate .....	53
10.1.7 Video Encoding .....	53
10.1.8 Smoothing .....	55
10.1.9 Display VCA Info .....	55
10.2 Audio Settings .....	55
10.2.1 Audio Input .....	56
10.2.2 Two-way Audio .....	56
10.3 Set ROI .....	56
10.4 Display Settings .....	57
10.4.1 Scene Mode .....	57
10.4.2 Image Adjustment .....	57
10.4.3 Image Adjustment (Thermal Channel) .....	58
10.4.4 Exposure Settings .....	58
10.4.5 Focus .....	59
10.4.6 Day/Night Switch .....	59
10.4.7 Set Supplement Light .....	60
10.4.8 BLC .....	60
10.4.9 WDR .....	60
10.4.10 HLC .....	61

10.4.11 White Balance .....	61
10.4.12 DNR .....	61
10.4.13 Defog .....	62
10.4.14 Set Palette .....	62
10.4.15 Set Palette Range .....	62
10.4.16 DDE .....	63
10.4.17 Video Standard .....	63
10.4.18 Mirror .....	63
10.4.19 Digital Zoom .....	63
10.4.20 Zoom Limit .....	63
10.4.21 Local Video Output .....	64
10.5 OSD .....	64
10.6 Overlay Picture .....	64
10.7 Set Manual DPC (Defective Pixel Correction) .....	65
10.8 Set Picture in Picture .....	65
10.9 Metadata .....	66
10.10 VCA Rule Display Settings .....	66
<b>Chapter 11 Video Recording and Picture Capture .....</b>	<b>67</b>
11.1 Storage Settings .....	67
11.1.1 Set Memory Card .....	67
11.1.2 Set NAS .....	67
11.1.3 Set FTP .....	68
11.1.4 Set Cloud Storage .....	68
11.2 Video Recording .....	69
11.2.1 Record Automatically .....	69
11.2.2 Record Manually .....	71
11.2.3 Playback and Download Video .....	71
11.3 Capture Configuration .....	71

11.3.1 Capture Automatically .....	71
11.3.2 Capture Manually .....	72
11.3.3 View and Download Picture .....	72
<b>Chapter 12 Network Settings .....</b>	<b>74</b>
12.1 TCP/IP .....	74
12.1.1 Multicast Discovery .....	75
12.2 Set Wireless Dial .....	75
12.3 Connect Device to Wi-Fi .....	76
12.4 Access to Device via AP .....	76
12.5 Port .....	77
12.6 Port Mapping .....	78
12.6.1 Set Auto Port Mapping .....	78
12.6.2 Set Manual Port Mapping .....	78
12.7 Multicast .....	79
12.8 SNMP .....	79
12.9 Access to Device via Domain Name .....	80
12.10 Access to Device via PPPoE Dial Up Connection .....	80
12.11 Accessing via Mobile Client .....	81
12.11.1 Enable Hik-Connect Service on Camera .....	81
12.11.2 Set Up Hik-Connect .....	82
12.11.3 Add Camera to Hik-Connect .....	83
12.12 Set ISUP .....	84
12.13 Set Open Network Video Interface .....	84
12.14 Set Alarm Server .....	84
12.15 Set SRTP .....	85
<b>Chapter 13 System and Security .....</b>	<b>86</b>
13.1 View Device Information .....	86
13.2 Search and Manage Log .....	86

13.3 Import and Export Configuration File .....	86
13.4 Export Diagnose Information .....	87
13.5 Reboot .....	87
13.6 Restore and Default .....	87
13.7 Upgrade .....	87
13.8 View Open Source Software License .....	88
13.9 Time and Date .....	88
13.9.1 Synchronize Time Manually .....	88
13.9.2 Set NTP Server .....	88
13.9.3 Set DST .....	89
13.10 Set RS-232 .....	89
13.11 Set RS-485 .....	89
13.12 Set Same Unit .....	90
13.13 Security .....	90
13.13.1 Authentication .....	90
13.13.2 Security Audit Log .....	90
13.13.3 Set IP Address Filter .....	91
13.13.4 Set SSH .....	92
13.13.5 Set Network Service .....	92
13.13.6 Set HTTPS .....	93
13.13.7 Set QoS .....	94
13.13.8 Set IEEE 802.1X .....	94
13.13.9 Set Control Timeout .....	95
13.13.10 Certificate Management .....	95
13.14 User and Account .....	97
13.14.1 Set User Account and Permission .....	97
13.14.2 Online Users .....	98
<b>Chapter 14 Appendix .....</b>	<b>99</b>

14.1 Common Material Emissivity Reference .....	99
14.2 Device Command .....	99
14.3 Device Communication Matrix .....	100

# Chapter 1 Overview

## 1.1 Brief Description

Thermal & Optical Bi-spectrum PTZ network camera integrates the function of the decoder, thermal camera, and the high-definition zoom camera. It performs temperature measurement, dynamic fire source detection and other smart detections in the remote video security of the power system, metallurgy system, petrochemical engineering, and so on. It is equipped with high-sensitivity IR detector and high-performance sensor. The device is able to measure object's temperature at a high accuracy in real time. The pre-alarm system helps you discover unexpected events immediately and protects your property.

## 1.2 Function

This section introduces main functions of the device.

### Fire Detection

Device can detect the dynamic fire source in the scene and output pre-alarm and alarm to protect the property.

### Temperature Measurement

Device can measure the actual temperature of the spot being monitored. The device alarms when temperature exceeds the temperature threshold value.

### VCA

Device can perform intelligent analysis. Multiple rules can be configured for different requirements.



## Chapter 2 Device Activation and Accessing

To protect the security and privacy of the user account and data, you should set a login password to activate the device when access the device via network.



Refer to the user manual of the software client for the detailed information about the client software activation.

---

### 2.1 Activate the Device via SADP

Search and activate the online devices via SADP software.

#### Before You Start

Access [www.hikvision.com](http://www.hikvision.com) to get SADP software to install.

#### Steps

1. Connect the device to network using the network cable.
2. Run SADP software to search the online devices.
3. Check **Device Status** from the device list, and select **Inactive** device.
4. Create and input the new password in the password field, and confirm the password.



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.

- 
5. Click **OK**.  
**Device Status** changes into **Active**.
  6. **Optional:** Change the network parameters of the device in **Modify Network Parameters**.

### 2.2 Activate the Device via Browser

You can access and activate the device via the browser.

#### Steps

1. Connect the device to the PC using the network cables.
2. Change the IP address of the PC and device to the same segment.

## Note

The default IP address of the device is 192.168.1.64. You can set the IP address of the PC from 192.168.1.2 to 192.168.1.253 (except 192.168.1.64). For example, you can set the IP address of the PC to 192.168.1.100.

3. Input **192.168.1.64** in the browser.
4. Set device activation password.

## Caution

We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including at least three of the following categories: 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.


5. Click **OK**.
6. Input the activation password to log in to the device.
7. **Optional:** Go to **Configuration** → **Network** → **Basic** → **TCP/IP** to change the IP address of the device to the same segment of your network.

## 2.3 Login

Log in to the device via Web browser.

### 2.3.1 Plug-in Installation

Certain operation systems and web browser may restrict the display and operation of the device function. You should install plug-in or complete certain settings to ensure normal display and operation. For detailed restricted function, refer to the actual device.

Operating System	Web Browser	Operation
Windows	Internet Explorer 10+	Follow pop-up prompts to complete plug-in installation.
	Google Chrome 57+ Mozilla Firefox 52+ Microsoft Edge 79.0.309+	Click  <b>Download Plug-in</b> to download and install plug-in. Go to <b>Configuration</b> → <b>Network</b> → <b>Advanced Settings</b> → <b>Network Service</b> to enable WebSocket or WebSockets for normal view if plug-in installation is not required.

Operating System	Web Browser	Operation
		Display and operation of certain functions are restricted. For example, Playback and Picture are not available. For detailed restricted function, refer to the actual device.
Mac OS 10.13+	Mac Safari 12+	Plug-in installation is not required. Go to <b>Configuration</b> → <b>Network</b> → <b>Advanced Settings</b> → <b>Network Service</b> to enable WebSocket or WebSockets for normal view. Display and operation of certain functions are restricted. For example, Playback and Picture are not available. For detailed restricted function, refer to the actual device.

 **Note**

The device only supports Windows and Mac OS system and does not support Linux system.

---

## 2.3.2 Illegal Login Lock

It helps to improve the security when accessing the device via Internet.

Go to **Configuration** → **System** → **Security** → **Security Service** , and enable **Enable Illegal Login Lock**. **Illegal Login Attempts** and **Locking Duration** are configurable.

### Illegal Login Attempts

When your login attempts with the wrong password reach the set times, the device is locked.

### Locking Duration

The device releases the lock after the setting duration.

## Chapter 3 Temperature Measurement

When you enable this function, the device measures the actual temperature of the scene. It alarms when temperature exceeds the temperature threshold value.

### 3.1 Notice

This part introduces the notices of configuring temperature measurement function.

- The target surface should be as vertical to the optical axis as possible. It is recommended that the angle of oblique image plane should be less than 45°.
- The target image pixels should be more than 5 × 5.
- If multiple presets will be taken for temperature measurement, it is recommended to set the patrol time above 20 s.
- Please select line thermography or area thermography for a certain area temperature measurement. The point thermography is not recommended in case of deviation occurred during device movement to affect the accuracy of temperature measurement.

### 3.2 Thermography Configuration Flow Chart

This part introduces the process of configuring temperature measurement.

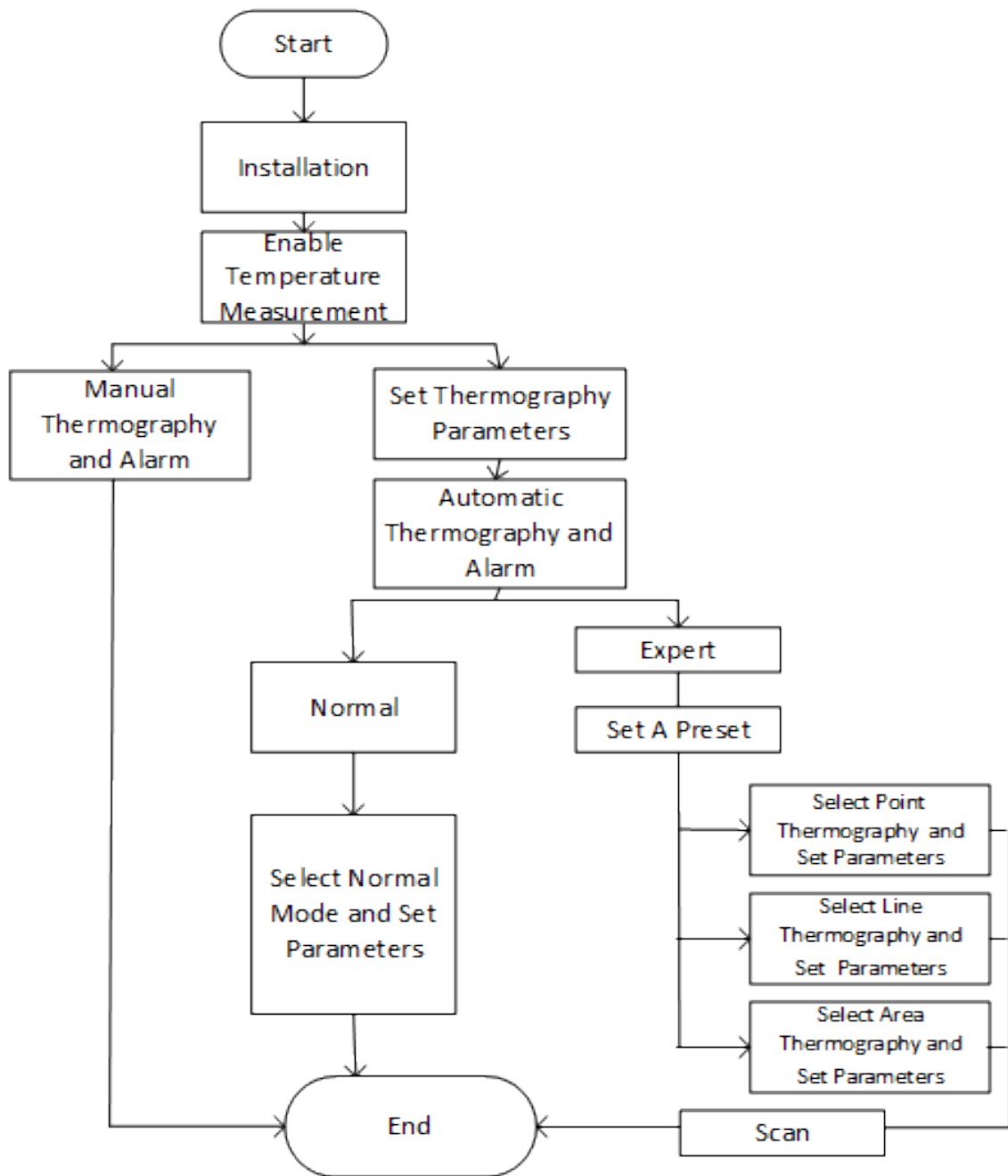


Figure 3-1 Thermography Configuration Flow Chart

**Note**

Please refer to the *Quick Start Guide* for detailed information of Installation part in the flow chart.

### 3.3 Set Thermography Parameters

Configure the parameters of temperature measurement.

#### Steps

1. Go to **Configuration** → **Local** , enable **Display Temperature Info.**

#### **Display Temperature Info.**

Select **Yes** to display temperature information on live view.

Enable **Rules** to display the rules information on live view.

2. Click **Save**.

3. Go to **Configuration** → **Temperature Measurement** → **Basic Settings** to configure parameters.

#### **Enable Temperature Measurement**

Check to enable temperature measurement function.

#### **Enable Color-Temperature**

Check to display Temperature-Color Ruler in live view.

#### **Display Temperature Info. on Stream**

Check to display temperature information on the stream.

#### **Display Temperature in Optical Channel**

Check to display thermal channel temperature information in the optical channel.

#### **Display Max./Min./Average Temperature**

Check to display maximum/minimum/average temperature information on liveview when the temperature measurement rule is line or area.

#### **Position of Thermometry Info**

Select the position of temperature information showed on the live view.

- Near Target: display the information beside the temperature measurement rule.
- Top Left: display the information on the top left of screen.

#### **Add Original Data on Capture**

Check to add data on alarm triggered capture of thermal channel.

#### **Add Original Data on Stream**

Check to add original data on thermal view.

#### **Data Refresh Interval**

It means the refresh interval of temperature information.

#### **Unit**

Display temperature with Degree Celsius (°C)/Degree Fahrenheit (°F)/Degree Kelvin (K).

#### **Temperature Range**

Select the temperature measurement range.

## Version

View the version of current algorithm.

## Reflect Light Filter

Enable this function if there is strong reflect light from sun in the scene. Or it may cause false alarm.

Click **Restart** to restart algorithm library.



## Note

- The settings vary according to different camera models.
- Reflect Light Filter is mutually exclusive with VCA functions.

---

4. Click **Save**.

## 3.4 Automatic Thermography

Configure the temperature measurement parameters and temperature measurement rules. The device can measure the actual temperature and output alarms when temperature exceeds the alarm threshold value.

### 3.4.1 Set Normal Mode

This function is used to measure the temperature of the whole scene and alarm.

#### Steps

1. Go to **Configuration → Temperature Measurement → Basic Settings** , and check **Enable Temperature Measurement**.
2. Refer to **Set Thermography Parameters** to set the parameters.
3. Go to **Configuration → Temperature Measurement → Advanced Settings** , and select **Normal**.
4. Configure the parameters of normal mode.

#### Emissivity

Set the emissivity of your target. The emissivity of each object is different.

#### Distance

The distance between the target and the device.

#### Pre-Alarm Threshold

When the temperature of target exceeds the pre-alarm threshold, and this status keeps more than **Filtering Time**, it triggers pre-alarm.

#### Alarm Threshold

When the temperature of target exceeds the alarm threshold, and this status keeps more than **Filtering Time**, it triggers alarm.

#### Pre-Alarm Output and Alarm Output

Check **Pre-Alarm Output** and **Alarm Output** to link the pre-alarm or alarm with the connected alarm device.

5. Refer to **Set Arming Schedule** for setting scheduled time. Refer to **Linkage Method Settings** for setting linkage method.

6. Click **Save**.

The maximum and minimum temperature will be displayed on the live view.

---



Go to **Image → VCA Rules Display** to adjust the fonts size and the temperature colour of normal, alarm and pre-alarm.

---

### 3.4.2 Set Expert Mode

Select the temperature measurement rules from **Point**, **Line**, or **Area** and configure parameters, the device alarms if the alarm rules are met.

#### Steps

1. Go to **Configuration → Temperature Measurement → Basic Settings**, check **Enable Temperature Measurement**.

2. Refer to **Set Thermography Parameters** to set the parameters.

3. Go to **Configuration → Temperature Measurement → Advanced Settings**, select **Expert**.

4. Refer to **Set Preset** to set a preset.

5. Select and enable the temperature measurement rules. Please refer to **Set Thermography Rule** for setting the rule.

6. **Optional:** Click **Area's Temperature Comparison** to set the alarm rules and the temperature.

7. Refer to **Set Arming Schedule** for setting scheduled time. Refer to **Linkage Method Settings** for setting linkage method.

8. Click **Save**.

The maximum temperature and thermography rules will be displayed on the live view.

---



Go to **Image → VCA Rules Display** to adjust the fonts size and the temperature colour of normal, alarm and pre-alarm.

---

9. **Optional:** Call the preset and check if the rules are efficient.

10. Enable the scan function of device, such as linear scan to monitor the scene.

### 3.4.3 Set Thermography Rule

#### Steps

1. Customize the rule name.

2. Select the rule **type** to Point, Line, or Area. Then draw a point, line, or area on the interface where the position to be measured.



**Point** Please refer to ***Point Thermography*** for detailed configuration.

**Line** Please refer to ***Line Thermography*** for detailed configuration.

**Area** Please refer to ***Area Thermography*** for detailed configuration.

### 3. Configure the temperature measurement parameters.

#### **Emissivity**

Set the emissivity of the target. The emissivity of the surface of a material is its effectiveness in emitting energy as thermal radiation. Different objects have different emissivity. Refer to ***Common Material Emissivity Reference*** to search for the target emissivity..

#### **Distance**

The distance between the target and the device.

#### **Reflective Temperature**

If there is any object with high emissivity in the scene, check and set the reflective temperature to correct the temperature. The reflective temperature should be set the same as the temperature of the high emissivity object.

### 4. Click and set the **Alarm Rule**.

#### **Alarm Temperature and Pre-Alarm Temperature**

Set the alarm temperature and pre-alarm temperature. E.g., select Alarm Rule as Above (Average Temperature), set the Pre-Alarm Temperature to 50 °C, and set the Alarm Temperature to 55 °C. The device pre-alarms when its average temperature is higher than 50 °C and alarms when its average temperature is higher than 55 °C.

#### **Filtering Time**

It refers to the duration time after the target temperature reaches or exceeds the pre-alarm temperature/alarm temperature.

#### **Tolerance Temperature**

Set the tolerance temperature to prevent the constant temperature change to affect the alarm. E.g., set tolerance temperature as 3°C, set alarm temperature as 55°C, and set pre-alarm temperature as 50°C. The device sends pre-alarm when its temperature reaches 50°C and it alarms when its temperature reaches 55°C and only when the device temperature is lower than 52°C will the alarm be cancelled.

#### **Pre-Alarm Output and Alarm Output**

When the temperature of target exceeds the pre-alarm or alarm threshold, it triggers the pre-alarm or alarm output of the connected device.

#### **Area's Temperature Comparison**

Select two areas and set the comparison rule, and set the temperature difference threshold. The device alarms when the temperature difference meets the setting value.

### 5. Click **Save**.

Click **Live View**, and select thermal channel to view the temperature and rules information on live view.

## Point Thermography

Configure the temperature measurement rule and click any point in live view to monitor the temperature.

### Steps

1. Click in the live view and a cross cursor showed on the interface.
2. Drag the cross cursor to desired position.

Go to **Live View** interface to view the temperature and rule of the point in thermal channel.

## Line Thermography

Configure the temperature measurement rule and monitor the maximum temperature of the line.

### Steps

1. Click and drag the mouse to draw a line in the live view interface.
2. Click and move the line to adjust the position.
3. Click and drag the ends of the line to adjust the length.

Go to **Live View** interface to view the maximum temperature and rule of the line in thermal channel.

## Area Thermography

Configure the temperature measurement rule and monitor the maximum temperature of the area.

### Steps

1. Click and drag the mouse in the live view to draw the area and right click to finish drawing.
2. Click and move the area to adjust the position.
3. Drag the corners of the area to adjust the size and shape.


Go to **Live View** interface to view the maximum temperature and rule of the area in thermal channel.

## 3.5 Manual Thermography

After enable the manual thermography function of the device, you can click any position on the live view to show the real temperature.

### Steps

1. Go to **Configuration** → **Local** and select **Display Temperature Info.** as **Yes**.
2. Go to **Configuration** → **Temperature Measurement** → **Basic Settings** .
3. Check **Enable Temperature Measurement**.
4. Click **Save**.

5. Go to live view interface and select thermal channel, click  . Click any position on the interface to show the real temperature.

### 3.6 Search History Temperature

You can search the history temperature and generate the temperature/time graphic.

#### Before You Start

Refer to [Set Memory Card](#) and [Set NAS](#) to set the storage first.

#### Steps

1. Go to **Configuration** → **Temperature Measurement** → **Search History Temperature** .
2. Set the search parameters.

##### Preset

You can search the highest temperature information in normal mode. Or you can search the temperature information of special presets in expert mode.

##### Rule

Select a rule of the special preset.

##### Start Time

Set the searching start time.

##### Display Time Interval

Display the temperature information for every setting time interval.

3. Click **Search** to generate the graphic.
4. Click **Export** to download the graphic.

## Chapter 4 Fire Source Detection

The device will trigger and upload alarm when detect the fire source.

Fire source detection is applied to fire-prevention purposes in scenic region, forest, tunnel and so on. You can configure the fire source detection parameters. When fire source is detected, the alarm actions will be triggered.

### 4.1 Fire Detection Flow Chart

Introduce the process of configuring fire detection.

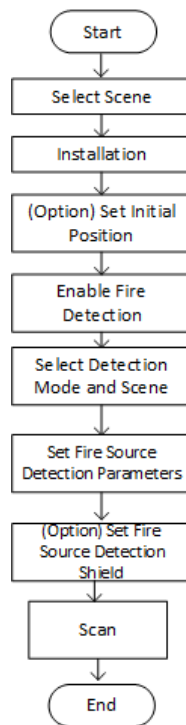


Figure 4-1 Fire Detection Flow Chart

---

 **Note**

Please refer to the Quick Start Guide for detail information of Installation part in the flow chart. Obtain the information of longitude, altitude, direction and so on by device after installation.

---

## 4.2 Recommended Scene

This part introduces the recommended scenes of fire source detection and helps you select the appropriate scene.

Fire source detection can be applied to indoor and outdoor monitoring with a large detection radius. To achieve the best monitoring effect, please set the installation place as requirements below.

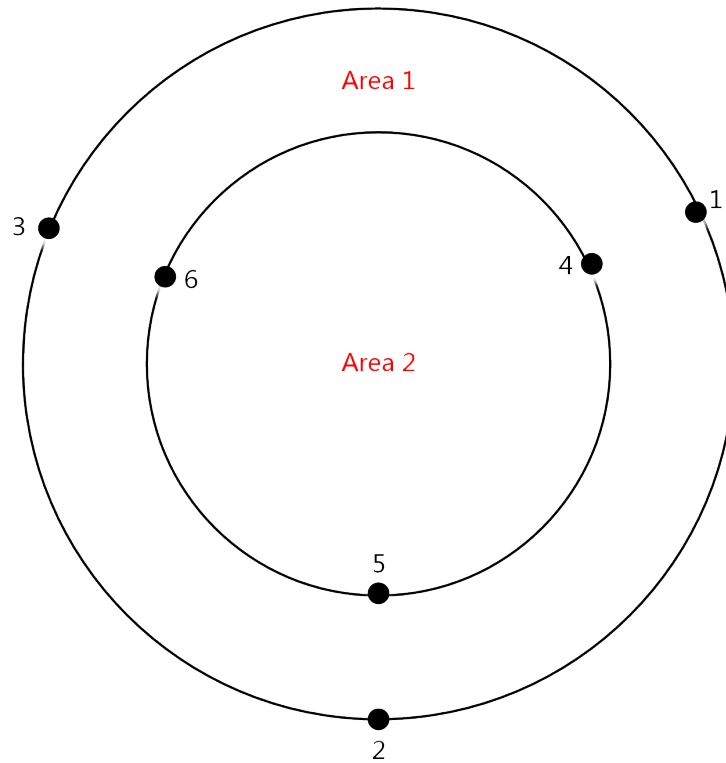
- The installation place should be the highest position within the detection area. The lens should not be covered during movement to detect the maximum area.
- It is better to choose the installation place with convenient traffic, well-equipped power and internet facilities. E.g. communication tower, watchtower, high-rise roof and so on.

## 4.3 Set the Presets

Please set the presets according to steps below to improve the accuracy of fire detection.

### Steps

1. If the presets located in different areas, you can set 6 presets in two areas as the example showed below.



**Figure 4-2 Set the Presets for fire detection**

2. Divide the scan area into three parts and set a preset every 120°. The black numbers are presets, and the red numbers are scan areas.
3. Set the presets according to the sequence of patrol path: 1->2->3->1->4->5->6->4.

---

 **Note**

- When set the presets, you should adjust the zoom ratio to view the image of both optical channel and thermal channel clearly.
- The recommended zoom ratio of optical channel and patrol speed shows in the table below.

**Table 4-1 Table of optical channel zoom ratio and patrol speed**

	16.7-1000 (focus distance)		12.5-775 (focus distance)		15.6-500 (focus distance)		6.7-330 (focus distance)		10-320 (focus distance)		6-240 (focus distance)	
	the left column is optical ratio, the right columns are speed level.											
15 km	15	4	20	4	/	/	/	/	/	/	/	/
10 km	10	5	15	4	12	4	/	/	/	/	/	/
5 km	7	6	10	5	8	5	20	4	13	4	/	/
3 to 5 km	5	6	7	6	6	6	13	4	9	5	15	4

## 4.4 Set Fire Detection Parameters

To avoid the potential fire damage, you should configure the fire detection function for certain areas. The detail configuration steps show as below.

### Before You Start

- The fire detection function can locate the fire source area quickly together with patrol or linear scan. Please refer to **Set Patrol Scan** for configuring patrol. Please refer to **Set the Presets** for presets setting.
- Please refer to **Set Device Position** for locating the fire source position.
- Go to **Configuration → Local** , set the fire point parameters.

### Locate Highest Temperature Point

Click and save to show the position of the highest temperature on the interface.

### Frame Fire Point

Click and save to frame the detected fire source.

### Steps

1. Go to **Configuration → Event → Smart Event** , select **Dynamic Fire Source Detection**.
2. Check **Enable Dynamic Fire Source Detection**.
3. Check **Display Fire Source Frame on Stream** to display a red frame around the fire source on stream when fire occurs.
4. Setting the parameters of fire detection.

### Detection Mode

**by Single Frame**

It can quickly detect fire while moving, but have a high false positive rate.

### by Multiple Frame

The camera stops to check the doubtful fire source after first detection. It alarms with high accuracy when verify the real fire source, but the detection speed is slow.

### Cancel Repeated Alarm

Alarm only one time if fire source detected in the same place during one day. It can be configured when the detection mode is selected as **by Multiple Frame**.

### Sensitivity

The sensitivity of fire detection. The bigger the value is, more easily the fire source can be detected, and the false rate is higher.

### Hold and Alarm Mode

**Auto** and **Manual** are selectable. The system will stop when it detects the fire source. You can set the duration while it keeps still.

#### Auto

You can set the dwell time. During the dwell time the camera stays still where it detects the fire source when performing auto scan, patrol, pattern, scheduled task, and park action.

#### Manual

The device stays still where it detects the fire source, until you manually

### Fire Source Zoom Ratio

#### Auto

The optical channel changes its zoom ratio until the thermal channel have the same field of view.

#### Manual

You can set the optical zoom ratio.

5. **Optional:** you can shield certain areas from being detected in fire source detection. Refer to **Set Fire Source Shielded Region** for details.
6. Refer to **Set Arming Schedule** for setting scheduled time. Refer to **Linkage Method Settings** for setting linkage method.
7. Click **Save**.

### 4.4.1 Set Fire Source Shielded Region

#### Steps

1. Go to **Configuration** → **Local** , and enable **Display Shield Area**.
2. Go to **Configuration** → **Event** → **Smart Event** → **Fire Source Region Shield** .
3. Check **Enable Fire Source Detection Shield** .
4. Select **Drawing Mode**, and draw the area you want to shield.



- In** Select this mode if the shielded area is in the current scene.
- FOV**
- Click the PTZ control buttons to find the area you want to shield from the fire detection.
  - Click **Draw Area**, and drag the mouse in the live view to draw the area.
  - You can drag the corners of the red rectangle area to change its shape and size.
  - Click **Stop Drawing** to finish drawing, or click **Clear All** to clear all of the areas you set without saving them.
- 



### Note

- Set vertexes clockwise or anticlockwise in sequence.
  - Draw four vertexes again if you want to change the shielded area.
- 
5. Check **Display Shield Area** to show the shield area on the live view.
  6. Click **Add** to save the fire detection shield, and it will be listed in the **Fire Source Detection Shield List** area; you can select a region and click **Delete** to delete it from the list; you can also define the color of the regions.
  7. Click **Save**.

## Chapter 5 Intelligent Analysis

**Intelligent Analysis** is used to detect whether there is any target breaks the VCA rules. The system will send alarms when the VCA rule is triggered.

---

### Note

This function is only supported in the thermal channel. Please take the actual product for reference.

---

### 5.1 Switch the Scene Mode

The device provides different scene modes catering to various needs.

Go to **Configuration → VCA → Basic Settings → Scene Mode** to select a scene mode, and follow the prompt to switch **Scene Mode**. Click **Save**.

---

### Note

The individual configuration for each scene mode will not change after switching.

---

#### Basic

In this mode, the device is commonly placed at a specific location, and detects targets in the user-configurable area.

#### Panorama View

In this mode, the device can detect targets in a changing scene when the device is in motion.

### 5.2 Set VCA Parameters

#### Steps

1. Go to **Configuration → Local** .

##### Rules

Enable it to display rules information on live view.

##### Display Rules Info. on Capture

Select **Yes** to display rules information on the capture.

2. Go to **Configuration → VCA → Basic Settings** to configure VCA parameters for the channel..

##### Intelligent Analysis

Check to enable intelligent analysis function.

##### Display VCA Info. on Stream

Select to display target info and rule on stream, the information will be added to the video stream, and the overlay will be displayed if you get live view or play back by the VS Player.

### Display Target Info. on Alarm Picture

Select to display the target information on the alarm picture.

### Display Rule Info. on Alarm Picture

Select to display the rule information on the alarm picture.

### Snapshot Settings

Select to upload the picture to the surveillance center when the VCA alarm occurs. You can also set the quality of the picture.

3. Click **Save**.

## 5.3 Configure Intelligent Analysis in Panorama View

The intelligent analysis of panorama view is used to detect targets and send alarms when the device is in motion.

### Before You Start

Switch the scene mode to **Panorama View**. Please refer to [\*Switch the Scene Mode\*](#) .

### Steps


1. Go to **Configuration** → **VCA** → **Basic Settings** , and check **Intelligent Analysis** to enable the function.
2. Refer to [\*Set VCA Parameters\*](#) to configure VCA parameters.
3. Go to **Configuration** → **VCA** → **Panorama Rule** , Click **+** to add a new rule..
  - 1) Enter the **Rule Name**, and click the drop down menu to select **Rule Type**.

---

### Note

You can only set one rule in **Panorama View** mode.


---

- 2) Click  to draw an area in the live view. Right click the mouse to finish drawing.

**Duration:** The device performs perimeter protection when the target stays in the detection area for more than set value.
- 3) Set parameters of the rule.
- 4) Check to enable **Filter by Pixel**. Then draw max size and min size rectangles to filter the target among human, vehicle, animal, and others. Only the target whose size is between the Max. Size and Min. Size value will trigger the alarm.

---

## Note

- You can draw the max. size and min. size rectangles according to the real target in the scene. The recommended size is 1.2 times of the target.
  - The height of the rectangle is a more important factor as it is the main difference to tell apart a human and an animal.
  - Click  to copy the same settings to other rules.
- 

4. Click **Save**.
5. Refer to **Set Arming Schedule** for setting scheduled time.
6. Refer to **Linkage Method Settings** for setting linkage method.
7. **Optional:** Refer to **Advanced Configuration** to set advanced configuration.

## 5.4 Configure Intelligent Analysis

This section is the detailed instruction of configuring the intelligent analysis rules.

### Before You Start

Switch the scene mode to **Basic** mode. Please refer to **Switch the Scene Mode** .

### Steps

1. Go to **Configuration → VCA → Basic Settings** , and check **Intelligent Analysis** to enable the function.
2. Refer to **Set VCA Parameters** to configure VCA parameters.
3. Add a new scene, and set the scene parameters. Please refer to .
4. Refer to **Set Rules** to set the scene rules.
5. Refer to **Set Arming Schedule** for setting scheduled time.
6. Refer to **Linkage Method Settings** for setting linkage method.
7. Refer to **Set the Scene Auto-Switch** for setting scene patrol.
8. **Optional:** Refer to **Advanced Configuration** to set advanced configuration.

### 5.4.1 Set Detection Scenes and Tracking

Multiple detection scenes are supported for both channels. You can create scenes and set the tracking parameters for better target monitoring performance.

### Steps

1. Go to **Configuration → VCA** .
  2. Click **Scene Configuration** and **New Scene** to create one or more scenes.
  3. Select a numbered scene from the navigation bar on the left and enter a **Scene Name**.
- 

## Note

If you want to show the name on the image, check **Display Scene Name**.

---

4. Check **Track** to enable the target tracking function for the scene.
-

### 5. Set other tracking parameters.

#### Tracking Duration

Set the duration of tracking. If the value is selected as 0, the tracking duration will not be limited.

#### Zooming Ratio

It is the zoomed-in level when the camera channel is tracking a target.

Go to **Configuration → VCA → Zooming Ratio** , select a scene from the drop-down list, and control the zoom in/out buttons to get a desired zooming level, and save the settings.

#### Post-tracking

Set the duration of automatic tracking of the target after it stops.

Go to **Configuration → VCA → Advanced Configuration** , and set parameter.

#### Back to Scene Time

Set the duration of the camera move back to original scene after perimeter protection is started.

Go to **Configuration → VCA → Advanced Configuration** , and set parameter.

### 6. Click **Save**.

## 5.4.2 Set Rules

The device can detect whether there is any target breaking the VCA rules. The optical camera will track the target or the device will alarm when the VCA rule is triggered.

### Steps

1. Go to **Configuration → VCA → Scene Configuration → Scene x → Rule** .
2. Click **+** to add a new rule.
3. Enter the rule name, and click the drop down menu to select **Rule Type**.



#### Note

Each scene can be configured with different rule types. Up to 8 rules can be set for one scene.

---

#### Line Crossing

If any target move across the setting line, the alarm will be triggered. You can set the crossing direction.

#### Intrusion

If any target intrude into the pre-defined region longer than the set duration, the alarm will be triggered.

#### Region Entrance

If any target enters the pre-defined region, the alarm will be triggered.

#### Region Exiting

If any target exits the pre-defined region, the alarm will be triggered.

#### 4. Set parameters of the rule.


##### - Sensitivity

The higher the value is, the more easily the alarm can be triggered.

##### Target Detection


You are recommended to select the target as **Human & Vehicle**. In distant view, the device cannot classify the target with pixels less than 10\*10. The target will be recognized as human directly. So the selection of this item will not trigger false alarm or missing alarm.

#### 5. Draw the rules.

- When the rule type is selected as **Line Crossing**, click  to draw a line in the live view. You can drag end points of the line to adjust the position and length.

##### Line Crossing

You can set the crossing direction. Bidirectional, A-to-B, or B-to-A are selectable.

- When the rule type is selected as **Intrusion, Region Entrance, Region Entrance**, click  to draw an area in the live view. Right click the mouse to finish drawing.

##### Duration

The device performs perimeter protection when the target stays in the detection area for more than set value.




##### Note

Draw three segments of the rule from near to far to cover all of the detection area.

- 
- #### 6. Check to enable **Filter by Pixel**. Then Draw max size and min size rectangles to filter the target among human, vehicle, animal, and others. Only the target whose size is between the Max. Size and Min. Size value will trigger the alarm.



##### Note

- You can draw the max. size and min. size rectangles according to the real target in the scene. The recommended size is 1.2 times of the target.
- The height of the rectangle is a more important factor as it is the main difference to tell apart a human and an animal.
- Click  to copy the same settings to other rules.

---

#### 7. Click **Save**.

- #### 8. Refer to **Set Arming Schedule** for setting scheduled time. Refer to **Linkage Method Settings** for setting linkage method.

### 5.4.3 Set the Scene Auto-Switch

The device support patrol tracking for multiple important scenes. The alarm will be triggered if the rule is broken during patrol sequence.

## Before You Start

Finish scene settings in advance. See ***Set Detection Scenes and Tracking*** for configuration instructions.

## Steps

1. Go to **VCA → Scene Auto-Switch** to configure this function.
2. Set the scene patrol sequence.

### Scene Name

Select a scene name from the drop down list.

### Duration

Set the dwell time of the scene when doing patrol tracking.

3. Click the up, down arrow to adjust the patrol sequence.
4. Click **Save**.

## 5.5 Advanced Configuration

This section introduces the advanced configuration of intelligent analysis.

Go to **Configuration → VCA → Advanced Configuration** and configure the parameters.

## Detection Parameters

### Enable Trajectory Displacement Filter

When this function is turned on, the system will send alarms the moment a target appears in the scene without further movement. When it is turned off, the system only detects a target in the scene after the target has moved a target frame.

### Generation Speed

It refers to the speed of the system to generate targets based on the intelligent analysis. The greater the value is, the faster the system can generate targets.



### Note

It may cause false alarms when the value is too high.

---

### Background Motion Correction

The system will correct the changing positions of the target when the device is in motion to increase detection accuracy. The greater the value is, the better the correction will be.

### Single Alarm

The system only sends alarm once for one target triggering. Otherwise, the alarm will be triggered continuously until the target disappears.

### Scene Modes

The scene mode is set to be **General** or **Distant View** by default. Select **Leaves Interfered View** when there are shaking targets in the scene, such as leaves.

### **Post-tracking**

Set the duration of automatic tracking of the target after it stops.

### **Back to Scene Time**

Set the duration of the camera move back to original scene after perimeter protection is started.

### **Restore Parameters**

#### **Restore Default**

Click **Restore** to restore the parameters to the default.

#### **Restart VCA**

Click **Restart** to restart the VCA function.



## Chapter 6 Event and Alarm

This part introduces the configuration of events. The device takes certain response to triggered alarm. Certain events may not be supported by certain device models.

### 6.1 Set Motion Detection

It helps to detect the moving objects in the detection region and trigger the linkage actions.

#### Steps

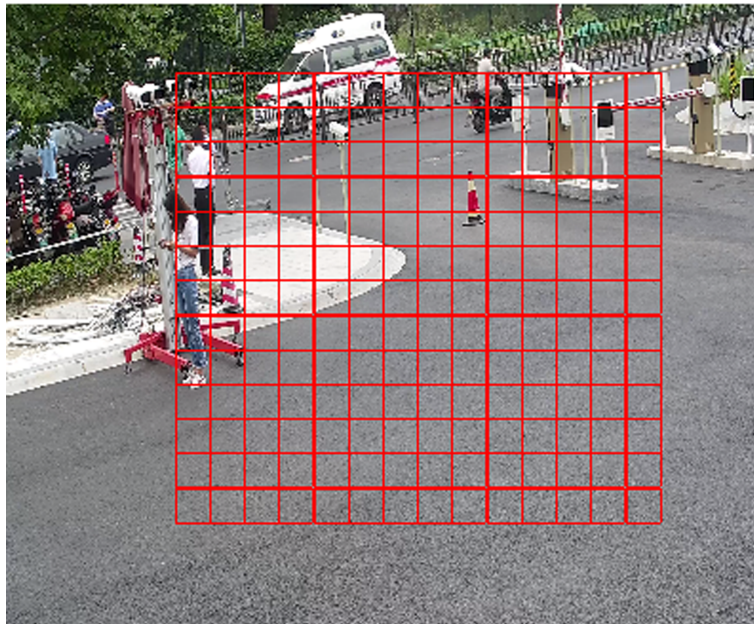
1. Go to **Configuration** → **Event** → **Basic Event** → **Motion Detection** .
2. Select the channel No.
3. Check **Enable Motion Detection**.
4. **Optional**: Highlight to display the moving object in the image in green.
  - 1) Check **Enable Dynamic Analysis for Motion**.
  - 2) Go to **Configuration** → **Local** .
  - 3) Set **Rules** to **Enable**.
5. Select **Configuration Mode**, and set rule region and rule parameters.
  - For the information about normal mode, see ***Normal Mode*** .
  - For the information about expert mode, see ***Expert Mode*** .
6. Set the arming schedule and linkage methods. For the information about arming schedule settings, see ***Set Arming Schedule*** . For the information about linkage methods, see ***Linkage Method Settings*** .
7. Click **Save**.

#### 6.1.1 Normal Mode

You can set motion detection parameters according to the device default parameters.

#### Steps

1. Select normal mode in **Configuration**.
2. Set the sensitivity of normal mode. The higher the value of sensitivity is, the more sensitive the motion detection is. If the sensitivity is set to **0**, motion detection and dynamic analysis do not take effect.
3. Click **Draw Area**. Click and drag the mouse on the live video, then release the mouse to finish drawing one area.



**Figure 6-1 Set Rules**

**Stop Drawing** Stop drawing one area.

**Clear All** Clear all the areas.

**4. Optional:** You can set the parameters of multiple areas by repeating the above steps.

## 6.1.2 Expert Mode

You can configure the motion detection parameters of day/night switch according to the actual needs.

### Steps

1. Select expert mode in **Configuration**.
2. Set parameters of expert mode.

### Day/Night Switch

OFF: Day/Night switch is disabled.

Day/Night Auto-Switch: The system switches day/night mode automatically according to environment. It displays colored image at day and black and white image at night.

Day/Night Scheduled-Switch: The system switches day/night mode according to the schedule. It switches to day mode during the set periods and switches to night mode during the other periods.

---

### **Note**

This function is not supported in the expert mode of thermal channel.

---

## Sensitivity

The higher the value of sensitivity is, the more sensitive the motion detection is. If the sensitivity is set to **0**, motion detection and dynamic analysis do not take effect.

3. Select an **Area** and click **Draw Area**. Click and drag the mouse on the live video, then release the mouse to finish drawing one area.



Figure 6-2 Set Rules

**Stop Drawing** Finish drawing one area.

**Clear All** Delete all the areas.

4. **Optional:** Repeat the above steps to set multiple areas.

## 6.2 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. Select the channel number.
3. Check **Enable**.
4. Set the **Sensitivity**. The higher the value is, the easier to detect the area covering.
5. 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 6-3 Set Video Tampering Area**

6. Refer to **Set Arming Schedule** for setting scheduled time. Refer to **Linkage Method Settings** for setting linkage method.
7. Click **Save**.

### 6.3 Set Exception Alarm

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

#### Steps

1. Go to **Configuration → Event → Basic Event → Exception**.
2. Select **Exception Type**.

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

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

## 6.4 Set Burning-Prevention

This function is used to close the shutter to prevent the lens from high temperature damage.

### Steps

1. Go to **Configuration → Event → Basic Event → Burning-Prevention** .
2. Check **Enable**.
3. Select burning-prevention mode.

### Lens Movement

The lens move automatically to avoid high temperature damage.

4. Set the protection duration.
5. Click **Save**.

## 6.5 Detect Audio Exception

Audio exception detection function detects the abnormal sound in the scene, such as the sudden increase/decrease of the sound intensity, and some certain actions can be taken as response.

### Steps

1. Go to **Configuration → Event → Smart Event → Audio Exception Detection** .
2. Select one or several audio exception detection types.

### Audio Loss Detection

Detect sudden loss of audio track.

### Sudden Increase of Sound Intensity Detection

Detect sudden increase of sound intensity. **Sensitivity** and **Sound Intensity Threshold** are configurable.



### Note

- The lower the sensitivity is, the more significant the change should be to trigger the detection.
- The sound intensity threshold refers to the sound intensity reference for the detection. It is recommended to set as the average sound intensity in the environment. The louder the environment sound, the higher the value should be. You can adjust it according to the real environment.

### Sudden Decrease of Sound Intensity Detection

Detect sudden decrease of sound intensity. **Sensitivity** is configurable.

3. Refer to **Set Arming Schedule** for setting scheduled time. Refer to **Linkage Method Settings** for setting linkage methods.
  4. Click **Save**.
- 



**Note**

The function varies according to different models.

---

## Chapter 7 Arming Schedule and Alarm Linkage

Arming schedule is a customized time period in which the device performs certain tasks. Alarm linkage is the response to the detected certain incident or target during the scheduled time.

### 7.1 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.



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**.

### 7.2 Linkage Method Settings

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

#### 7.2.1 Trigger 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



This function is only supported by certain models.

---

1. Go to **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**.

## 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.

## 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**.



## 7.2.2 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.

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

Refer to **Set NAS** for NAS configuration.

Refer to **Set Memory Card** for memory card storage configuration.

## 7.2.3 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, refer to **Set Email**.

### 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. Go to **Configuration → Network → Basic Settings → TCP/IP** for DNS settings.

#### Steps

1. Go to 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**.

### 7.2.4 Notify Surveillance Center

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




## Chapter 8 PTZ

PTZ is an abbreviation for pan, tilt, and zoom. It means the movement options of the camera.

### 8.1 PTZ Control

In live view interface, you can use the PTZ control buttons to control the device panning, tilting, and zooming.

#### PTZ Control Panel

	<p>Click and hold the directional button to pan/tilt the device.</p> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>You can set <b>Keyboard Control Speed</b> in <b>Configuration → PTZ → Basic Settings</b> . The speed of pan/tilt movement in live view is based on this speed level.</li> <li>You can set <b>Max. Tilt-angle</b> in <b>Configuration → PTZ → Basic Settings</b> to limit tilt movement range.</li> </ul>
	<p>Click the button, then the device keeps panning.</p> <p><b>Note</b></p> <p>You can set <b>Auto Scan Speed</b> in <b>Configuration → PTZ → Basic Settings</b> . The higher the value you set, the faster the device pans.</p>
	<p>Drag the slider to adjust the speed of pan/tilt movement.</p>

**Note**



You can set **Manual Control Speed** in **Configuration → PTZ → Basic Settings** .

<b>Compatible</b>	The control speed is same as <b>Keyboard Control Speed</b> .
<b>Pedestrian</b>	Choose <b>Pedestrian</b> when you monitor the pedestrians.
<b>Non-motor Vehicle</b>	Choose <b>Non-motor Vehicle</b> when you monitor the non-motor vehicles.
<b>Motor Vehicle</b>	Choose <b>Motor Vehicle</b> when you monitor the motor vehicles.
<b>Auto</b>	You are recommended to set it as <b>Auto</b> when the application scene of the speed dome is complicated.

To avoid blurred image resulted from fast zoom, you can check **Enable Proportional Pan** in **Configuration → PTZ → Basic Settings** . If you enable this function, the pan/tilt speed change according to the amount of zoom. When there is a large amount of zoom, the pan/tilt speed will be slower for keeping the image from moving too fast on the live view image.

---



## Zoom in/out

	Click the button, and the lens zooms in.
	Click the button, and the lens zooms out.



### Note

- You can set **Zooming Speed** in **Configuration → PTZ → Basic Settings** . The higher the value is, the faster the zooming speed is.
  - You can set **Zoom Limit** in **Configuration → Image → Display Settings → Other** to limit the maximum value of the total zoom (digital zoom and optical zoom).
  - You can set **Synchronized Zoom** in **Configuration → PTZ → Basic Settings** to synchronize the zoom settings in the optical channel and the thermal channel.
- 

## Focus

	Click the button, then the lens focuses near and the object nearby gets clear.
	Click the button, then the lens focuses far and the object far away gets clear.




## Iris

	When the image is too dark, click the button to enlarge the iris.
	When the image is too bright, click the button to stop down the iris.

## 8.2 Set Preset

A preset is a predefined image position. For the defined preset, you can call the preset No. to view the position.

### Steps



1. Click  to show the setting panel, and click .
2. Use the PTZ control buttons to move the lens to the desired position.
3. Select a preset number from the preset list, and click  to finish the setting.

---

### Note

Some presets are predefined with special command. You can only call them but not configure them.

- 
4. Repeat the steps above to set multiple presets.

-  Click the button to call the preset.
-  Click the button to delete the preset.

---

### Note

You can delete all presets in **Configuration → PTZ → Clear Config**. Click **Clear All Presets**, and click **Save**.

### What to do next

Go to **Configuration → PTZ → Basic Settings** to set preset freezing and preset speed.

After enabling preset freezing, the live image switches directly from one preset to another, without showing the areas between these two scenes. It also guarantees the masked area will not be seen when the device is moving.

### 8.2.1 Special Presets

You can call the following presets with special demands to enable corresponding functions.

Preset No.	Function	Preset No.	Function
33	Auto Flip	92	Set manual limits
34	Back to origin	93	Save manual limits
35	Call patrol 1	94	Remote reboot
36	Call patrol 2	95	Call OSD menu
37	Call patrol 3	96	Stop a scan
38	Call patrol 4	97	Start random scan
39	Day mode	98	Start frame scan
40	Night mode	99	Start auto scan
41	Preset 1	100	Start tilt scan
42	Preset 2	101	Start panorama scan
43	Preset 3	102	Call patrol 5
44	Preset 4	103	Call patrol 6
45	One-touch patrol	104	Call patrol 7
46	Call area scan	105	Call patrol 8
47	Call area scan 1		

 **Note**

Not all models support the presets above. Please take the actual product for reference.

---

## 8.3 Set Patrol Scan

Patrol scan is a function to automatically move among multiple presets.

### Before You Start





 **Note**

This function is only supported by certain models.

---

Make sure that you have defined more than one presets. See ***Set Preset*** for detailed configuration.

### Steps

1. Click  to show the setting panel, and click  to enter patrol setting interface.
2. Select a patrol number from the list and click .
3. Click  to add presets.

## Preset

Select predefined preset.

## Speed

Set the speed of moving from one preset to another.

## Time

It is the duration staying on one patrol point.

✘ Delete the presets in patrol.

⬇ ⬆ Adjust the preset order.



## Note

A patrol can be configured with 32 presets at most, and 2 presets at least.

4. Click **OK** to finish a patrol setting.
5. Repeat the steps above to configure multiple patrols.
6. Operate patrols.
  - ▶ Call the patrol.
  - Stop patrolling.
  - ✘ Delete the patrol.
  - ⚙ Set the patrol.



## Note


You can delete all patrols in **Configuration → PTZ → Clear Config** . Click **Clear All Patrols**, and click **Save**.

---

### 8.3.1 Set One-Touch Patrol

The device automatically adds presets to one patrol path and starts patrol scan.

#### Steps

1. Set two or more presets except special presets. For setting presets, refer to **Set Preset** .  
The device will automatically add presets to patrol path No.8.
2. Choose one of the following methods to enable the function.
  - Click  .
  - Call patrol path No.8.
  - Select and call preset No.45.

### 8.4 Set Linear Scan

The device can perform auto scan in setting area for fire source detection.


## Steps

1. Go to **Configuration → PTZ → Linear Scan** .
2. Select the camera channel.
3. Zoom in and zoom out the camera to the appropriate zoom ratio, and click **Save Ratio**.

---

### Note

Click **Enable Saved Ratio** to set the camera to the saved zoom ratio.

4. Check **Enter Area Settings**.
5. Set the left/right/up/down limits with the PTZ control panel, and click  to confirm settings.
6. **Optional:** Click **Clear** to delete the saved scan area.
7. Click **Save**.
8. Click **Call Linear Scan** to start linear scan, and click **Stop Linear Scan** to stop linear scan.

---

### Note

When setting the linear scan area, make sure the target area is both included in the optical channel and the thermal channel.

---

## 8.5 Set Initial Position

Initial position refers to the relative initial position of the device azimuth. You can set the initial position if you need to select one point in the scene as the base point.

### Steps

1. Go to **Configuration → PTZ → Initial Position** .
2. Move the device to the needed position by manually controlling the PTZ control buttons.
3. Click **Set** to save the information of initial position.

**Call** The device moves to the set initial position.

**Clear** Clear the set initial position.

## 8.6 Set Scheduled Tasks

You can set the device to perform a certain task during a certain period.

### Steps

1. Go to **Configuration → PTZ → Scheduled Tasks** .
2. Check **Enable Scheduled Task**.
3. Select the a task type from the drop-down list and draw a time bar on the schedule table.
4. Click the set time bar and set the action ID and smart event or VCA type.



---

### Note

Not all task types support the settings of action ID and smart event or VCA function. Please take the actual product for reference.

---

- Repeat step 3 and step 4 to set more than one scheduled tasks.
  - Set **Park Time**. During the set task period, if you operate the device manually, the scheduled task will be suspended. When the manual operation is over, the device will continue to perform the scheduled task after the set park time.
- 

### Note

Up to 30 time periods can be configured per day.

---

- Click **Save**.
- 

### Note

If you want to clear all scheduled tasks, go to **Configuration → PTZ → Clear Config**, check **Clear All Scheduled Tasks**, and click **Save**.

---

## 8.7 Set Park Action

You can set the device to perform an action (for example, preset or patrol) or return to a position after a period of inactivity (park time).

### Before You Start

Set the action type first. For example, if you want to select patrol as park action, you should set the patrol. See [Set Patrol Scan](#) for details.

### Steps

- Go to **Configuration → PTZ → Park Action**.
  - Check **Enable Park Action**.
  - Set **Park Time**: the inactive time before the device starts park action.
  - Select **Action Type** according to your needs.
- 

### Note

The VCA Type varies according to different action types.

---

- Select an **Action Type ID**, if you select patrol or preset as action type.  
When the action type is patrol, action type ID stands for patrol No. When the action type is preset, action type ID stands for preset No.
- Click **Save**.

## 8.8 Set Privacy Mask

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

### Steps

1. Go to **Configuration → PTZ → Privacy Mask** .
2. Adjust the live image to the target scene via PTZ control buttons.
3. Draw the area.

Draw Area	Click <b>Draw Area</b> , and click on the live view image to determine the boundary of the mask.
Stop Drawing	Click <b>Stop Drawing</b> after drawing the mask.

4. Click **Add**.

It is listed in **Privacy Mask List**.

5. Edit **Name**, **Type**, and **Active Zoom Ratio** on your demand.

### Active Zoom Ratio

When the actual zoom ratio is less than the set active zoom ratio, the set area can not be covered. When the actual zoom ratio is greater than the set active zoom ratio, the privacy mask is valid. The maximum value of active zoom ratio depends on the camera module.

6. Repeat the steps above to set other privacy masks.
7. Check **Enable Privacy Masks**.

## 8.9 Set Device Position

### Before You Start

Go to **Configuration → PTZ → Basic Settings → PTZ OSD** to enable **PT Status** display.

### Steps

1. Go to the setting page: **Configuration → PTZ → Position Settings** .
2. Select a **PT Mode**.

**Manual** Use a direction indicating device to determine the North at the device location, and set the North for the device. For details, see [Set Manual Compass](#) .

**Auto** For the device that has built-in e-compass, the compass can automatically tell the north direction for the device. For details, see [Set Auto Compass](#) .

3. Check **Installation Angle Calibration** to perform angle calibration one time when the device installation is finished.

It is used for situations where the device is not installed horizontally, to increase the fire source detection accuracy.

4. Set Vandal-proof alarm.

After enabling the function, the device triggers alarms once its position changes because of shock or vandalism.

### **Sensitivity**

The higher the value is, the easier the alarm will be triggered.

### **Upload Vandal-proof Alarm**

The device uploads the alarm information when the alarm is triggered.

5. Get the device location information in advance, and input the longitude and latitude of the device manually.
6. Click **Save**.

### **What to do next**

If you lost direction when operating the device, you can click **Point to North** to call the north position that is saved in the device.

## **8.9.1 Set Manual Compass**

Use a direction indicating device to determine the North at the device location, and set the North for the device.

### **Before You Start**

Use a direction indicating device to determine the north at the device location.

### **Steps**

1. Select the **PT Mode** as **Manual**.
2. Adjust the tilt position of the device to 0 by controlling the up arrow and down arrow on the PTZ panel.
3. Adjust the pan position to show the live view of the north direction by controlling the left arrow and right arrow on the PTZ panel.
4. Click **Set as North**.

## **8.9.2 Set Auto Compass**

For the device that has built-in e-compass, the compass can automatically tell the north direction for the device.

### **Before You Start**

Electromagnetic interference may affect the accuracy of the e-compass. Use manual compass if electromagnetic interference occurs in the device installation environment.

### **Steps**

1. Select the **PT Mode** as **Auto**.
2. Click **Calibrate** to synchronize the north of the device with that of the e-compass.

## 8.10 Set Power Off Memory

This function can resume the previous PTZ status of device after it restarting from a power-off.

### Steps

1. Go to **Configuration** → **PTZ** → **Basic Settings** .
2. Select **Resume Time Point**. When the device stays at one position for the set resume time point or more, the position is saved as a memory point. The device returns to the last memory point when it restarts.
3. Click **Save**.

## 8.11 Set PTZ Priority

The function can set the PTZ priority of different signals.

### Steps

1. Go to **Configuration** → **PTZ** → **Prioritize PTZ** .
2. Set the priority signal and delayed time.

#### Network

The network signal controls the device with priority.

#### RS-485

The RS-485 signal controls the device with priority.

#### Delay

It refers to the time interval of PTZ operation controlled by different signals. When the operation with high priority is finished, the low priority signal controls the device after the setting interval.

3. Click **Save**.

## Chapter 9 Live View

It introduces the live view parameters, function icons and transmission parameters settings.

### 9.1 Live View Parameters





The supported functions vary depending on the model.



For multichannel devices, select the desired channel first before live view settings.

---

#### 9.1.1 Window Division



-  refers to 1 × 1 window division.
-  refers to 2 × 2 window division.
-  refers to 3 × 3 window division.
-  refers to 4 × 4 window division.

#### 9.1.2 Live View Stream Type

Select the live view stream type according to your needs. For the detailed information about the stream type selection, refer to [\*\*\*Stream Type\*\*\*](#).

#### 9.1.3 Enable and Disable Live View

This function is used to quickly enable or disable live view of all channels.

- Click  to start live view of all channels.
- Click  to stop live view of all channels.



Go to **Configuration** → **Local**, to set **Auto Start Live View**, If **Yes** is selected, live view will start automatically when you go to live view.

---


#### 9.1.4 View Previous/Next Page

When the number of channels surpasses that of live view window division, this function can switch live view among multiple channels.

Click   to switch live view among multiple channels.

## 9.1.5 Full Screen

This function is used to view the image in full screen mode.

Click  to start full screen mode and press ESC button to exit.

## 9.1.6 Set Panorama Map

Panorama map is a map generated for the camera to horizontally scan the whole scene. Panorama map is used to quickly locate the presets, patrols, etc.













### Steps

---

#### Note

This function is only supported by certain models.



---

1. Click  to generate the panorama map.
2. Click  to show the tool bar.
  -  Click , and all the valid presets will be shown in the panorama map. Hover on the preset to show its name, and click the preset to move the camera to selected preset.
  -  Click  to enable the 3D positioning.
    - Hold and drag the mouse to a lower right position to frame an area on the live: the framed area is zoomed in and relocated to the center of the live image.
    - Hold and drag the mouse to an upper left position to frame an area on the live: the framed area is zoomed out and relocated to the center of the live image.
  -  Click , and all the saved patrols will be shown in the panorama map. Click a patrol to call the patrol.
  -  Click , and the resolution settings interface shows. Set the panorama map panning angle as 360°, 240°, 120°, or custom. In custom mode, you can set from 1° to 360°.
  -  Download the panorama map and save as picture.
3. Click  to save and exit.


## 9.1.7 Conduct Regional Focus

You can enable the function to focus on certain area.

### Steps

1. Click  to enable regional focus.
2. Drag the mouse on the live view to draw a rectangle as the desired focus area.
3. Click  to disable this function.


## 9.1.8 Light

Click  to turn on or turn off the illuminator.

## 9.1.9 Wiper

For the device that has a wiper, you can control the wiper via web browser.

### Steps

1. Click  on live view page.

The wiper wipes the window one time.

## 9.1.10 Lens Initialization

Lens initialization is used on the device equipped with motorized lens. The function can reset lens when long time zoom or focus results in blurred image. This function varies according to different models.

### Manual Lens Initialization

Click  to operate lens initialization.

### Auto Lens Initialization

Go to **Configuration** → **System** → **Maintenance** → **Lens Correction** to enable this function. You can set the arming schedule, and the device will correct lens automatically during the configured time periods.


## 9.1.11 Auxiliary Focus

Click  to realize automatic focus. This function is subject to the actual device model.

## 9.1.12 Quick Set Live View

It offers a quick setup of PTZ, display settings, OSD, and video/audio settings on live view page.

### Steps

1. Click  to show quick setup page.

2. Set PTZ, display settings, OSD, and video/audio parameters.

- For PTZ settings, see **Lens Parameters Adjustment** .
- For display settings, see **Display Settings** .
- For OSD settings, see **OSD** .
- For audio and video settings, see **Video and Audio** .

---

## Note



The function is only supported by certain models.

---



### 9.1.13 Lens Parameters Adjustment

It is used to adjust the lens focus, zoom and iris.


#### Zoom

- Click  , and the lens zooms in.
- Click  , and the lens zooms out.



#### Focus

- Click  , then the lens focuses far and the distant object gets clear.
- Click  , then the lens focuses near and the nearby object gets clear.

#### PTZ Speed

- Slide  to adjust the speed of the pan/tilt movement.


#### Iris

- When the image is too dark, click  to enlarge the iris.
- When the image is too bright, click  to stop down the iris.

### 9.1.14 Conduct 3D Positioning

3D positioning is to relocate the selected area to the image center.



#### Steps

1. Click  to enable the function.
2. Select a target area in live image.
  - Left click on a point on live image: the point is relocated to the center of the live image. With no zooming in or out effect.
  - Hold and drag the mouse to a lower right position to frame an area on the live: the framed area is zoomed in and relocated to the center of the live image.
  - Hold and drag the mouse to an upper left position to frame an area on the live: the framed area is zoomed out and relocated to the center of the live image.
3. Click the button again to turn off the function.


### 9.1.15 Lens Demist

Lens demist can remove condensation from the lens surface to increase the image quality.



In live view, click  to enable **Lens Demist**. This function will be automatically turned off after 30 min. Or you can click  to turn it off immediately.

## 9.1.16 Synchronize FOV

Click  to synchronize the FOV of optical lens and thermal lens.

## 9.2 Set Transmission Parameters

The live view image may be displayed abnormally according to the network conditions. In different network environments, you can adjust the transmission parameters to solve the problem.

### Steps

1. Go to **Configuration** → **Local** .
2. Set the transmission parameters as required.

#### Protocol

##### TCP

TCP ensures complete delivery of streaming data and better video quality, yet the real-time transmission will be affected. It is suitable for the stable network environment.

##### UDP

UDP is suitable for the unstable network environment that does not demand high video fluency.

##### MULTICAST

MULTICAST is suitable for the situation that there are multiple clients. You should set the multicast address for them before selection.



For detailed information about multicast, refer to ***Multicast*** .

---

##### HTTP

HTTP is suitable for the situation that the third-party needs to get the stream from the device.

### Play Performance

#### Shortest Delay

The device takes the real-time video image as the priority over the video fluency.

#### Balanced

The device ensures both the real-time video image and the fluency.

#### Fluent

The device takes the video fluency as the priority over real-time. In poor network environment, the device cannot ensure video fluency even the fluency is enabled.

### **Custom**

You can set the frame rate manually. In poor network environment, you can reduce the frame rate to get a fluent live view. But the rule information may not display.

### **Auto Start Live View**

- **Yes** means the live view is started automatically. It requires a high performance monitoring device and a stable network environment.
- **No** means the live view should be started manually.

**3.** Click **OK**.

## Chapter 10 Video and Audio

This part introduces the configuration of video and audio related parameters.

### 10.1 Video Settings

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

Go to setting page: **Configuration → Video/Audio → Video** .



For device with multiple camera channels, select a channel before other settings.

---

#### 10.1.1 Stream Type

For device supports more than one stream, you can specify parameters for each stream type.

##### Main Stream

The stream stands for the best stream performance the device supports. It usually offers the best resolution and frame rate the device can do. But high resolution and frame rate usually mean larger storage space and higher bandwidth requirements in transmission.

##### Sub Stream

The stream usually offers comparatively low resolution options, which consumes less bandwidth and storage space.

#### 10.1.2 Video Type

Select the content (video and audio) that should be contained in the stream.

##### Video

Only video content is contained in the stream.

##### Video & Audio

Video content and audio content are contained in the composite stream.

#### 10.1.3 Resolution

Select video resolution according to actual needs. Higher resolution requires higher bandwidth and storage.

## 10.1.4 Bitrate Type and Max. Bitrate

### Constant Bitrate

It means that the stream is compressed and transmitted at a comparatively fixed bitrate. The compression speed is fast, but mosaic may occur on the image.

### Variable Bitrate

It means that the device automatically adjust the bitrate under the set **Max. Bitrate**. The compression speed is slower than that of the constant bitrate. But it guarantees the image quality of complex scenes.

## 10.1.5 Video Quality

When **Bitrate Type** is set as Variable, video quality is configurable. Select a video quality according to actual needs. Note that higher video quality requires higher bandwidth.

## 10.1.6 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. Note that higher frame rate requires higher bandwidth and larger storage space.

## 10.1.7 Video Encoding

It stands for the compression standard the device adopts for video encoding.



### Note

Available compression standards vary according to device models.

---

## H.264

H.264, also known as MPEG-4 Part 10, Advanced Video Coding, is a compression standard. Without compressing image quality, it increases compression ratio and reduces the size of video file than MJPEG or MPEG-4 Part 2.

## H.264+

H.264+ is an improved compression coding technology based on H.264. By enabling H.264+, you can estimate the HDD consumption by its maximum average bitrate. Compared to H.264, H.264+ reduces storage by up to 50% with the same maximum bitrate in most scenes.

When H.264+ is enabled, **Max. Average Bitrate** is configurable. The device gives a recommended max. average bitrate by default. You can adjust the parameter to a higher value if the video quality is less satisfactory. Max. average bitrate should not be higher than max. bitrate.



When H.264+ is enabled, **Video Quality, I Frame Interval, Profile** and **SVC** are not configurable.

---

## H.265

H.265, also known as High Efficiency Video Coding (HEVC) and MPEG-H Part 2, is a compression standard. In comparison to H.264, it offers better video compression at the same resolution, frame rate and image quality.

## H.265+

H.265+ is an improved compression coding technology based on H.265. By enabling H.265+, you can estimate the HDD consumption by its maximum average bitrate. Compared to H.265, H.265+ reduces storage by up to 50% with the same maximum bitrate in most scenes.

When H.265+ is enabled, **Max. Average Bitrate** is configurable. The device gives a recommended max. average bitrate by default. You can adjust the parameter to a higher value if the video quality is less satisfactory. Max. average bitrate should not be higher than max. bitrate.



When H.265+ is enabled, **Video Quality, I Frame Interval, Profile** and **SVC** are not configurable.

---

## Profile

This function means that under the same bitrate, the more complex the profile is, the higher the quality of the image is, and the requirement for network bandwidth is also higher.

## I-Frame Interval

I-frame interval defines the number of frames between 2 I-frames.

In H.264 and H.265, an I-frame, or intra frame, is a self-contained frame that can be independently decoded without any reference to other images. An I-frame consumes more bits than other

frames. Thus, video with more I-frames, in other words, smaller I-frame interval, generates more steady and reliable data bits while requiring more storage space.

### **SVC**

Scalable Video Coding (SVC) is the name for the Annex G extension of the H.264 or H.265 video compression standard.

The objective of the SVC standardization has been to enable the encoding of a high-quality video bitstream that contains one or more subset bitstreams that can themselves be decoded with a complexity and reconstruction quality similar to that achieved using the existing H.264 or H.265 design with the same quantity of data as in the subset bitstream. The subset bitstream is derived by dropping packets from the larger bitstream.

SVC enables forward compatibility for older hardware: the same bitstream can be consumed by basic hardware which can only decode a low-resolution subset, while more advanced hardware will be able to decode high quality video stream.

#### **10.1.8 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.

#### **10.1.9 Display VCA Info**

VCA information can be displayed by Player and Video.

##### **Player**

Player means the VCA info can be displayed by the dedicated player provided by the manufacturer.

##### **Video**

Video means the VCA info can be displayed by any general video player.

### **10.2 Audio Settings**

It is a function to set audio parameters such as audio encoding, environment noise filtering.

Go to the audio settings page: **Configuration → Video/Audio → Audio** .

## 10.2.1 Audio Input

If a built-in microphone or an external audio pick-up device is available, audio encoding, audio input mode and input volume are configurable.

### Audio Encoding

The device offers several compression standard. Select according to your need.

### Audio Input

Select **MicIn** for the built-in microphone, and **LineIn** for external audio pick-up device.



### Note

MicIn is only supported by certain models.

---

### Input Volume

Adjust the volume of the audio input.

### Environmental Noise Filter

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





## 10.2.2 Two-way Audio

It is used to realize the two-way audio function between the monitoring center and the target in the monitoring screen.

### Before You Start

- Make sure the audio input device (pick-up or microphone) and audio output device (speaker) connected to the device is working properly. Refer to specifications of audio input and output devices for device connection.
- If the device has built-in microphone and speaker, two-way audio function can be enabled directly.

### Steps

1. Click **Live View**.
2. Click  on the toolbar to enable two-way audio function of the camera.
3. Click  and select  , move the slider to adjust the volume.
4. Click  , disable the two-way audio function.

## 10.3 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. Go to **Configuration** → **Video/Audio** → **ROI** .
2. Check **Enable**.
3. Select the channel No. according to your need.
4. Select **Stream Type**.
5. 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.

6. Input the **Region Name** and **ROI Level**.
7. Click **Save**.



### Note

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

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

## 10.4 Display Settings

It offers the parameter settings to adjust image features.

Go to **Configuration** → **Image** → **Display Settings** .

For device that supports multiple channels, display settings of each channel is required. The settings for different channels may be different. This part introduces all possible parameters among the channels.

Click **Default** to restore settings.

### 10.4.1 Scene Mode

There are several sets of image parameters predefined for different installation environments. Select a scene according to the actual installation environment to speed up the display settings.

### 10.4.2 Image Adjustment

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



## 10.4.3 Image Adjustment (Thermal Channel)

You can optimize the image display effect of thermal channel by setting background correction and manual correction.

### Background Correction

Fully cover the lens with an object of uniform temperature in front of the lens, such as foam board or paperboard. When you click **DPC (Defective Pixel Correction)**, the device will take the uniform object as the standard and optimize the image once.

### Manual Correction

Click **DPC (Defective Pixel Correction)** to optimize the image once.



### Note

It is a normal phenomenon that short video freezing might occur during the process of **Background Correction** and **Manual Correction**.

---

### Thermal AGC Mode

Choose the AGC mode according to different scenes to balance and improve the image quality.

- Histogram: Choose for scene with obvious WDR and high temperature difference, can improve image contrast and enhance image. E.g. the scene contains both indoor and outdoor scenes.
- Linear: Choose for scene with low temperature difference and the target is not obvious, can improve image contrast and enhance image. E.g. the bird in forest.
- Self-Adaptive: Choose AGC mode automatically according to current scene.

## 10.4.4 Exposure Settings

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

### Exposure Mode

#### Auto

The iris, shutter, and gain values are adjusted automatically.

You can limit the changing ranges of iris, shutter and gain by setting **Max. Iris Limit**, **Min. Iris Limit**, **Max. Shutter Limit**, **Min. Shutter Limit** and **Limit Gain** for better exposure effect.

#### Iris Priority

The value of iris needs to be adjusted manually. The shutter and gain values are adjusted automatically according to the brightness of the environment.

You can limit the changing ranges of the shutter and gain by setting **Max. Shutter Limit**, **Min. Shutter Limit** and **Limit Gain** for better exposure effect.

### Shutter Priority

The value of shutter needs to be adjusted manually. The iris and gain values are adjusted automatically according to the brightness of the environment.

You can limit the changing ranges of the iris by setting **Max. Iris Limit**, **Min. Iris Limit** and **Limit Gain** for better exposure effect.

### Manual

You need to set **Iris**, **Shutter**, and **Gain** manually.

### Slow Shutter

The higher the slow shutter level is, the slower the shutter speed is. It ensures full exposure in underexposure condition.

## 10.4.5 Focus

It offers options to adjust the focus mode, focus range, and the minimum focus distance.

### Focus Mode

#### Semi-auto

The device focuses once after the PTZ and lens zooming. If the image is clear, the focus does not change when the scene changes.

#### Manual

You can adjust the focus manually on the live view page.

### Focus Range

You can set the focus range to **Short**, **Medium**, **Long**. In **Short** mode, the focus range of the device is set to the test range. The device can focus more quickly compared to **Medium**, **Long** mode.

### Min. Focus Distance

When the distance between the scene and lens is shorter than the Min. Focus Distance, the lens does not focus.

## 10.4.6 Day/Night Switch

Day/Night Switch function can provide color images in the day mode and turn on fill light in the night mode. Switch mode is configurable.

### Day

The image is always in color.

### Night

The image is black/white or colorful and the supplement light will be enabled to ensure clear live view image at night.

## 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.
  - You can turn on the smart supplement light in auto, night, and schedule-switch modes for better image effect.
- 

## 10.4.7 Set Supplement Light

### Steps

1. Go to **Configuration** → **Maintenance** → **System Service** .
2. Check **Enable Supplement Light**.
3. Click **Save**.

## 10.4.8 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.

## 10.4.9 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. Refer to the actual interface for details.

---



WDR Off

WDR On

**Figure 10-1 WDR**

### 10.4.10 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.

### 10.4.11 White Balance

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



Cold

Warm

Auto White Balance

**Figure 10-2 White Balance**

### 10.4.12 DNR

Digital Noise Reduction is used to reduce the image noise and improve the image quality. **Normal** and **Expert** modes are selectable.

#### **Normal**

Set the DNR level to control the noise reduction degree. The higher level means stronger reduction degree.

## Expert

Set the DNR level for both space DNR and time DNR to control the noise reduction degree. The higher level means stronger reduction degree.

## OFF

Disable the DNR function.

## 10.4.13 Defog

You can enable the defog function when the environment is foggy and the image is misty. It enhances the subtle details so that the image appears clearer.



**Figure 10-3 Defog**

## 10.4.14 Set Palette

You can select the palette mode to display the thermal grayscale image to colored image.

### Steps

1. Go to **Configuration** → **Image** → **Display Settings** .
2. Select the thermal channel.
3. Select a palette mode in **Image Enhancement** according to your need.

### Result

The live view displays the image with palette.

## 10.4.15 Set Palette Range

The live view can display the palettes effect of the specified temperature range.

Select **Manual** or **Auto** from **By Temp. Range** drop down list.

### Auto

The device detects the max. temperature and min. temperature of the scene automatically and display image of the whole scene with palettes.

## Manual

In this mode, you can enter the temperature upper limit and lower limit manually. And the live view shows the palettes effect of the desired temperature section more detailed.

### 10.4.16 DDE

Digital Detail Enhancement is used to adjust the details of the image. **OFF** and **Normal** modes are selectable.

#### OFF

Disable this function.

#### Normal

Set the DDE level to control the details of the image. The higher the level is, the more details shows, but the higher the noise is.

### 10.4.17 Video Standard

Video standard is an ability of a video card or video display device that defines the amount of colors that are shown and the resolution. The two most common video standard used are NTSC and PAL. In NTSC, 30 frames are transmitted each second. Each frame is made up of 525 individual scan lines. In PAL, 25 frames are transmitted each second. Each frame is made up of 625 individual scan lines. Select video signal standard according to the video system in your country/region.

### 10.4.18 Mirror

When the live view image is the reverse of the actual scene, this function helps to display the image normally.

Select the mirror mode as needed.



#### Note

The video recording will be shortly interrupted when the function is enabled.

---

### 10.4.19 Digital Zoom

You can zoom in the image. The larger the zoom size is, the more blurred the image is.

### 10.4.20 Zoom Limit

You can set a certain value to limit the maximum value of zooming.

### 10.4.21 Local Video Output

If the device is equipped with video output interfaces, such as BNC, CVBS, HDMI, and SDI, you can preview the live image directly by connecting the device to a monitor screen.

Select the output mode as ON/OFF to control the output.

## 10.5 OSD

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

Go to OSD setting page: **Configuration** → **Image** → **OSD Settings** .

Select a channel.

Set the corresponding parameters, and click **Save** to take effect.

### Character Set

Select character set for displayed information. If Korean is required to displayed on screen, select **EUC-KR**. Otherwise, select **GBK**.

### 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**, **Font Color**, and **Alignment**.

## 10.6 Overlay Picture

Overlay a customized picture on live view.

### Before You Start

The picture to overlay has to be in BMP format with 24-bit, and the maximum picture size is 128 × 128 pixel.

### Steps

1. Go to picture overlay setting page: **Configuration** → **Image** → **Picture Overlay** .
2. Select a channel to overlay picture.
3. Click **Browse** to select a picture, and click **Upload**.

The picture with a red rectangle will appear in live view after successfully uploading.



4. Check **Enable Picture Overlay**.

5. Drag the picture to adjust its position.
6. Click **Save**.

### 10.7 Set Manual DPC (Defective Pixel Correction)



If the amount of defective pixels in the image is comparatively small and accurate correction is needed, you can correct these pixels manually.


#### Steps

1. Go to **Configuration** → **Image** → **DPC**.
2. Select the thermal channel.
3. Select manual mode.
4. Click the defective pixel on the image, then a cursor shows on the live view.
5. Click **Up**, **Down**, **Left**, **Right** to adjust the cursor position to the defective pixel position.
6. Click , then click  to correct defective pixel.

---

#### Note

If multiple defective pixels need to be corrected, click  after locating a defective pixel. Then after locating other pixels, click  to correct them simultaneously.

7. **Optional:** Click  to cancel defective pixel correction.

### 10.8 Set Picture in Picture

You can overlay the images of two channels and view the image of two channels at the same time.

#### Steps

1. Select a channel number.
2. Select the picture in picture mode.

**Overlap Mode** Partial image of thermal channel is displayed on the full screen of optical channel. This mode is only supported in optical channel.

**Details Overlay Mode** The device displays the details of optical channel on thermal channel. This mode is only supported in thermal channel.

3. In **Details Overlay Mode**, set the **Fusion Distance** of the target. It is recommended to use the default value.
4. Click **Save**.

---

#### Note

Not all models support this function, take the actual product for reference.

---



### 10.9 Metadata

Metadata is the raw data that the device collects before algorithm processing. It is often used for the third party integration.

Go to **Configuration** → **Video/Audio** → **Metadata Settings** to enable metadata uploading of the desired function for the camera channels.

### 10.10 VCA Rule Display Settings

The VCA rule display refers to the function that you can customize the displayed overlay information of the VCA rule, which includes the font size and line and frame color.

You can go to **Configuration** → **Image** → **VCA Rule Display** to select the desired font size, and set the line and frame color.

## Chapter 11 Video Recording and Picture Capture

This part introduces the operations of capturing video clips and snapshots, playback, and downloading captured files.

### 11.1 Storage Settings

This part introduces the configuration of several common storage paths.

#### 11.1.1 Set Memory Card

If you choose to store the files to memory card, make sure you insert and format the memory card in advance.

##### Before You Start

Insert the memory card to the camera. For detailed installation, refer to *Quick Start Guide* of the camera.

##### Steps

1. Go to storage management setting page: **Configuration** → **Storage** → **Storage Management** → **HDD Management** .
2. Select the memory card, and click **Format** to start initializing the memory card.  
The **Status** of memory card turns to **Normal** from **Uninitialized**, which means the memory card can be used normally.
3. **Optional**: Define the **Quota** of the memory card. Input the quota percentage for different contents according to your need.
4. Click **Save**.

#### 11.1.2 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.** Select **Mounting Type** and set parameters for the disk.

##### Server Address

The IP address of the network disk.

##### File Path

The saving path of network disk files.

### User Name and Password

The user name and password of the net HDD.

3. Click **Test** to check whether the network disk is available.
4. Click **Save**.

### 11.1.3 Set FTP

You can configure the FTP server to save images which are captured by events or a timed snapshot task.

#### Before You Start

Get the FTP server address first.

#### Steps

1. Go to **Configuration → Network → Advanced Settings → FTP** .
2. Configure FTP settings.

#### Server Address and Port

The FTP server address and corresponding port.

#### User Name and Password

The FTP user should have the permission to upload pictures.

If the FTP server supports picture uploading by anonymous users, you can check **Anonymous** to hide your device information during uploading.

#### Directory Structure

The saving path of snapshots in the FTP server.

3. Click **Upload Picture** to enable uploading snapshots to the FTP server.
4. Click **Test** to verify the FTP server.
5. Click **Save**.

### 11.1.4 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 cloud storage is enabled, the pictures are stored in the cloud video manager preferentially.

---

1. Go to **Configuration → Storage → Storage Management → Cloud Storage** .
2. Check **Enable Cloud Storage**.

### 3. Set basic parameters.

<b>Protocol Version</b>	The protocol version of the cloud video manager.
<b>Server IP</b>	The IP address of the cloud video manager. It supports IPv4 address.
<b>Serve Port</b>	The port of the cloud video manager. 6001 is the default port and you are not recommended to edit it.
<b>AccessKey</b>	The key to log in to the cloud video manager.
<b>SecretKey</b>	The key to encrypt the data stored in the cloud video manager.
<b>User Name and Password</b>	The user name and password of the cloud video manager.
<b>Picture Storage Pool ID</b>	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**.

## 11.2 Video Recording

This part introduces the operations of manual and scheduled recording, playback, and downloading recorded files.

### 11.2.1 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](#) for details.

#### Steps

---

#### Note

The function varies according to different models.

---

1. Go to **Configuration** → **Storage** → **Schedule Settings** → **Record Schedule** .
  2. Select channel No.
  3. Check **Enable**.
  4. 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.

5. Set schedule for the selected record type. Refer to **Set Arming Schedule** for the setting operation.
6. 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.

7. Click **Save**.

## 11.2.2 Record Manually




### Steps

1. Go to **Configuration → Local** .
2. Set the **Record File Size** and saving path to for recorded files.
3. Click **Save**.
4. Click  in the live view interface to start recording. Click  to stop recording.

## 11.2.3 Playback and Download Video

You can search, playback and download the videos stored in the local storage or network storage.


### Steps

1. Click **Playback**.
2. Select channel No.
3. Set search condition and click **Search**.  
The matched video files showed on the timing bar.
4. Click  to play the video files.
  - Click  to clip video files.
  - Click  to play video files in full screen. Press **ESC** to exit full screen.

---

### Note

Go to **Configuration → Local** , click **Save clips to** to change the saving path of clipped video files.

5. Click  on the playback interface to download files.
  - 1) Set search condition and click **Search**.
  - 2) Select the video files and then click **Download**.

---

### Note

Go to **Configuration → Local** , click **Save downloaded files to** to change the saving path of downloaded video files.

---

## 11.3 Capture Configuration

The device can capture the pictures manually or automatically and save them in configured saving path. You can view and download the snapshots.

### 11.3.1 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](#) for event settings.

### Steps

1. Go to **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**.

## 11.3.2 Capture Manually

### Steps


1. Go to **Configuration** → **Local** .
2. Set the **Image Format** and saving path to for snapshots.

#### JPEG

The picture size of this format is comparatively small, which is better for network transmission.

#### BMP

The picture is compressed with good quality.

3. Click **Save**.
4. Click  near the live view or play back window to capture a picture manually.

## 11.3.3 View and Download Picture

You can search, view and download the pictures stored in the local storage or network storage.

### Steps

1. Click **Picture**.
2. Select channel No.
3. Set search condition and click **Search**.  
The matched pictures showed in the file list.
4. Select the pictures then click **Download** to download them.



### Note

Go to **Configuration** → **Local** , click **Save snapshots when playback** to change the saving path of pictures.

---



## Chapter 12 Network Settings

### 12.1 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.

Go to **Configuration** → **Network** → **Basic Settings** → **TCP/IP** for parameter settings.

#### 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 changed after enabling the function. You can use SADP to get the device IP address.



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.



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.

## 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.

## Dynamic Domain Name

Check **Enable Dynamic Domain Name** and input **Register Domain Name**. The device is registered under the register domain name for easier management within the local area network.



### Note

**DHCP** should be enabled for the dynamic domain name to take effect.

---

## 12.1.1 Multicast Discovery

Check the **Enable Multicast Discovery**, and then the online network camera can be automatically detected by client software via private multicast protocol in the LAN.

## 12.2 Set Wireless Dial

The built-in wireless module offers dial-up access to the Internet for the device.

### Before You Start

Get a SIM card, and activate 3G/4G services. Insert the SIM card to the corresponding slot.

### Steps

1. Go to **Configuration** → **Network** → **Advanced Settings** → **Wireless Dial** .
2. Check to enable the function.
3. Click **Dial Parameters** to configure and save the parameters.
4. Click **Dial Plan**. See ***Set Arming Schedule*** for detailed information.
5. Click **Dial Status**.

**Click Refresh** Refresh the dial status.

**Click Disconnect** Disconnect the 3G/4G wireless network.

When the **Dial Status** turns to **Connected**, it means a successful dial.

6. Access the device via the **IP Address** of the computer in the network.

- Input the IP address in the browser to access the device.
- Add the device in client application. Select **IP/Domain**, and input IP address and other parameters to access the device.

### 12.3 Connect Device to Wi-Fi

#### Before You Start

Refer to the user manual of wireless router or AP to set SSID, key, and other parameters.

#### Steps

1. Go to TCP/IP settings page: **Configuration → Network → Basic Configuration → TCP/IP** .
2. Select **Wlan** to set the parameters. Refer to **TCP/IP** for detailed configuration.



#### Note

For stable use of Wi-Fi, it is not recommended to use DHCP.

3. Go to Wi-Fi settings page: **Configuration → Network → Advanced Configuration → Wi-Fi** .
4. Set and save the parameters.
  - 1) Click **Search**.
  - 2) Select a **SSID**, which should be the same as that of wireless router or AP.

The parameters of the network is automatically shown in **Wi-Fi**.
  - 3) Select the **Network Mode** as **Manage**.
  - 4) Input the key to connect the wireless network. The key should be that of the wireless network connection you set on the router.

#### What to do next

Go to TCP/IP settings page: **Configuration → Network → Basic Configuration → TCP/IP** , and click **Wlan** to check the **IPv4 Address** and log in the device.

### 12.4 Access to Device via AP

You can access to the device via the device AP when the device cannot connect to the network.

#### Steps

1. Go to **Configuration → Network → Advanced Settings → WLAN AP** to enable WLAN AP function.
2. Search the device WLAN AP in the WLAN list of your phone or PC.
3. Connect your phone or PC to the AP.



#### Note

The AP name is HAP\_Serial Number. The password is the serial number. The serial number can be obtained from **System → System Settings → Basic Information** .

4. Enter the IP address in the browser.

---

## Note

The default IP of the device AP is 192.168.8.1.

---

## 12.5 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.

### 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.

### RTSP Port

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

### SRTP Port

It refers to the port of secure real-time transport protocol.

### Server Port

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

### 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.
-

## 12.6 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**.

### 12.6.1 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.

---

### 12.6.2 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.

## 12.7 Multicast

Multicast is group communication where data transmission is addressed to a group of destination devices simultaneously.

Go to **Configuration → Network → Basic Settings → Multicast** for the multicast settings.

For a device with more than one channel, multicast can be set independently for each channel.

### IP Address

It stands for the address of multicast host.

### Stream Type

The stream type as the multicast source.

### Video Port

The video port of the selected stream.

### Audio Port

The audio port of the selected stream.

## 12.8 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**.

## 12.9 Access to Device via Domain Name

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.

## 12.10 Access to Device via PPPoE Dial Up Connection

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. Go to **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.



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 **[Access to Device via Domain Name](#)** for detail information.

---

## 12.11 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.



Hik-Connect service should be supported by the camera.

---

### 12.11.1 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.

#### Enable Hik-Connect Service via Web Browser

Follow the following steps to enable Hik-Connect Service via Web Browser.

##### Before You Start

You need to activate the camera before enabling the service.

##### Steps

1. Access the camera via web browser.
2. Enter platform access configuration interface. **Configuration** → **Network** → **Advanced Settings** → **Platform Access**
3. Select Hik-Connect as the **Platform Access Mode**.
4. Check **Enable**.



5. Click and read "Terms of Service" and "Privacy Policy" in pop-up window.
6. Create a verification code or change the old verification code for the camera.



The verification code is required when you add the camera to Hik-Connect service.

---

7. Save the settings.

### Enable Hik-Connect Service via SADP Software

This part introduce how to enable Hik-Connect service via SADP software of an activated camera.

#### Steps

1. Run SADP software.
2. Select a camera and enter **Modify Network Parameters** page.
3. Check **Enable Hik-Connect**.
4. Create a verification code or change the old verification code.



The verification code is required when you add the camera to Hik-Connect service.

---

5. Click and read "Terms of Service" and "Privacy Policy".
6. Confirm the settings.

### 12.11.2 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.



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.

### 12.11.3 Add Camera 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.

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

## 12.12 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** → **Platform Access** .
2. Select **ISUP** as the platform access mode.
3. Select **Enable**.
4. Select a protocol version and input related parameters.
5. Click **Save**.

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

## 12.13 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 Open Network Video Interface**.
3. Click **Add** to configure the Open Network Video Interface user.
  - Delete** Delete the selected Open Network Video Interface user.
  - Modify** Modify the selected Open Network Video Interface user.
4. Click **Save**.
5. **Optional:** Repeat the steps above to add more Open Network Video Interface users.

## 12.14 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, HTTPS, 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. Select **Protocol**.



### Note

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

---

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

### 12.15 Set SRTP

The Secure Real-time Transport Protocol (SRTP) is a Real-time Transport Protocol (RTP) internet protocol, intended to provide encryption, message authentication and integrity, and replay attack protection to the RTP data in both unicast and multicast applications.

#### Steps

1. Go to **Configuration → Network → Advanced Settings → SRTP** .
2. Select **Server Certificate**.
3. Select **Encrypted Algorithm**.
4. Click **Save**.



Only certain device models support this function.

---

## Chapter 13 System and Security

It introduces system maintenance, system settings and security management, and explains how to configure relevant parameters.

### 13.1 View Device Information

You can view device information, such as Device No., Model, Serial No. and Firmware Version.

Enter **Configuration** → **System** → **System Settings** → **Basic Information** to view the device information.

### 13.2 Search and Manage Log

Log helps locate and troubleshoot problems.

#### Steps

1. Go to **Configuration** → **System** → **Maintenance** → **Log** .
2. Set search conditions **Major Type**, **Minor Type**, **Start Time**, and **End Time**.
3. Click **Search**.

The matched log files will be displayed on the log list.

4. **Optional**: Click **Export** to save the log files in your computer.

### 13.3 Import and Export Configuration File

It helps speed up batch configuration on other devices with the same parameters.

#### Steps

1. Export configuration file.
  - 1) Go to **Configuration** → **System** → **Maintenance** → **Upgrade & Maintenance** .
  - 2) Click **Device Parameters** and input the encryption password to export the current configuration file.
  - 3) Set the saving path to save the configuration file in local computer.
2. Import configuration file.
  - 1) Access the device that needs to be configured via web browser.
  - 2) Click **Browse** to select the saved configuration file.
  - 3) Input the encryption password you have set when exporting the configuration file.
  - 4) Click **Import**.

## 13.4 Export Diagnose Information

Diagnose information includes running log, system information, hardware information.

Go to **Configuration** → **System** → **Maintenance** → **Upgrade & Maintenance** , and click **Diagnose Information** to export diagnose information of the device.

## 13.5 Reboot

You can reboot the device via browser.

Go to **Configuration** → **System** → **Maintenance** → **Upgrade & Maintenance** , and click **Reboot**.

## 13.6 Restore and Default

Restore and Default helps restore the device parameters to the default settings.

### Steps

1. Go to **Configuration** → **System** → **Maintenance** → **Upgrade & Maintenance** .
2. Click **Restore** or **Default** according to your needs.

**Restore** Reset device parameters, except user information, IP parameters and video format to the default settings.

**Default** Reset all the parameters to the factory default.



### Note

Be careful when using this function. After resetting to the factory default, all the parameters are reset to the default settings.

---

## 13.7 Upgrade

### Before You Start

You need to obtain the correct upgrade package.



### Caution

DO NOT disconnect power during the process, and the device reboots automatically after upgrade.

---

### Steps

1. Go to **Configuration** → **System** → **Maintenance** → **Upgrade & Maintenance** .
2. Choose one method to upgrade.

**Firmware** Locate the exact path of the upgrade file.

**Firmware Directory** Locate the directory which the upgrade file belongs to.

3. Click **Browse** to select the upgrade file.
4. Click **Upgrade**.

### 13.8 View Open Source Software License

Go to **Configuration** → **System** → **System Settings** → **About** , and click **View Licenses**.

### 13.9 Time and Date

You can configure time and date of the device by configuring time zone, time synchronization and Daylight Saving Time (DST).

#### 13.9.1 Synchronize Time Manually

##### Steps

1. Go to **Configuration** → **System** → **System Settings** → **Time Settings** .
2. Select **Time Zone**.
3. Click **Manual Time Sync**.
4. Choose one time synchronization method.
  - Select **Set Time**, and manually input or select date and time from the pop-up calendar.
  - Check **Sync. with computer time** to synchronize the time of the device with that of the local PC.
5. Click **Save**.

#### 13.9.2 Set NTP Server

You can use NTP server when accurate and reliable time source is required.

##### Before You Start

Set up a NTP server or obtain NTP server information.

##### Steps

1. Go to **Configuration** → **System** → **System Settings** → **Time Settings** .
2. Select **Time Zone**.
3. Click **NTP**.
4. Set **Server Address**, **NTP Port** and **Interval**.



Server Address is NTP server IP address.

5. Click **Test** to test server connection.
-

6. Click **Save**.

## 13.9.3 Set DST

If the region where the device is located adopts Daylight Saving Time (DST), you can set this function.

### Steps

1. Go to **Configuration** → **System** → **System Settings** → **DST** .
2. Check **Enable DST**.
3. Select **Start Time**, **End Time** and **DST Bias**.
4. Click **Save**.

## 13.10 Set RS-232

RS-232 can be used to debug device or access peripheral device. RS-232 can realize communication between the device and computer or terminal when the communication distance is short.

### Before You Start

Connect the device to computer or terminal with RS-232 cable.

### Steps

1. Go to **Configuration** → **System** → **System Settings** → **RS-232** .
2. Set RS-232 parameters to match the device with computer or terminal.
3. Click **Save**.

## 13.11 Set RS-485

RS-485 is used to connect the device to external device. You can use RS-485 to transmit the data between the device and the computer or terminal when the communication distance is too long.

### Before You Start

Connect the device and computer or terminal with RS-485 cable.

### Steps

1. Go to **Configuration** → **System** → **System Settings** → **RS-485** .
2. Set the RS-485 parameters.



You should keep the parameters of the device and the computer or terminal all the same.

3. Click **Save**.
-



## 13.12 Set Same Unit

Set the same temperature unit and distance unit. When you enable this function, the unit cannot be configured separately in other setting pages

### Steps

1. Go to **Configuration → System → System Settings → Unit Settings** .
2. Check **Use Same Unit**.
3. Set the temperature unit and distance unit.
4. Click **Save**.

## 13.13 Security

You can improve system security by setting security parameters.

### 13.13.1 Authentication

You can improve network access security by setting RTSP and WEB authentication.

Go to **Configuration → System → Security → Authentication** to choose authentication protocol and method according to your needs.

#### RTSP Authentication

Digest and digest/basic are supported, which means authentication information is needed when RTSP request is sent to the device. If you select **digest/basic**, it means the device supports digest or basic authentication. If you select **digest**, the device only supports digest authentication.

#### WEB Authentication

Digest and digest/basic are supported, which means authentication information is needed when WEB request is sent to the device. If you select **digest/basic**, it means the device supports digest or basic authentication. If you select **digest**, the device only supports digest authentication.



#### Note

Refer to the specific content of protocol to view authentication requirements.

---

### 13.13.2 Security Audit Log

The security audit logs refer to the security operation logs. You can search and analyze the security log files of the device so as to find out the illegal intrusion and troubleshoot the security events.

Security audit logs can be saved on device internal storage. The log will be saved every half hour after device booting. Due to limited storage space, you can also save the logs on a log server.

## Search Security Audit Logs

You can search and analyze the security log files of the device so as to find out the illegal intrusion and troubleshoot the security events.

### Steps



This function is only supported by certain camera models.

---

1. Go to **Configuration** → **System** → **Maintenance** → **Security Audit Log** .
2. Select log types, **Start Time**, and **End Time**.
3. Click **Search**.

The log files that match the search conditions will be displayed on the Log List.

4. **Optional**: Click **Export** to save the log files to your computer.

## Set Log Server

The log server should support syslog (RFC 3164) over TLS.

### Before You Start

- Install client and CA certificates before configuration. Refer to [Certificate Management](#) for detailed information.
- Select certificates according to the requirement of the log server. If two-way authentication is required, select the CA certificate and the client certificate. If one-way authentication is required, select the CA certificate only.

### Steps

1. Check **Enable Log Upload Server**.
2. **Optional**: Check **Enable Encrypted Transmission** if you want the log data to be encrypted.
3. Input **Log Server IP** and **Log Server Port**.
4. **Optional**: Select client certificate.
5. Select CA certificate to the device.
6. Click **Test** to test the settings.
7. Click **Save**.

### 13.13.3 Set IP Address Filter

IP address filter is a tool for access control. You can enable the IP address filter to allow or forbid the visits from the certain IP addresses.

IP address refers to IPv4.

## Steps

1. Go to **Configuration → System → Security → IP Address Filter** .
2. Check **Enable IP Address Filter**.
3. Select the type of IP address filter.

**Forbidden** IP addresses in the list cannot access the device.

**Allowed** Only IP addresses in the list can access the device.

4. Edit the IP address filter list.

**Add** Add a new IP address or IP address range to the list.

**Modify** Modify the selected IP address or IP address range in the list.

**Delete** Delete the selected IP address or IP address range in the list.

5. Click **Save**.

## 13.13.4 Set SSH

SSH is a protocol to ensure security of remote login. This setting is reserved for professional maintenance personnel only.

### Steps

1. Go to **Configuration → System → Security → Security Service** .
2. Check **Enable SSH**.
3. Click **Save**.

## 13.13.5 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, and digital zoom function cannot be used.

If the device uses HTTP, enable WebSocket.

If the device uses HTTPS, enable WebSockets.

#### TLS (Transport Layer Security)

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

3. Click **Save**.

### 13.13.6 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. Click **Delete** to recreate and install certificate.

**Create and install self-signed certificate**

Refer to [\*Create and Install Self-signed Certificate\*](#)

**Create certificate request and install certificate**

Refer to [\*Install Authorized Certificate\*](#)

5. Click **Save**.

### Create and Install Self-signed Certificate

#### Steps

1. Check **Create Self-signed Certificate**.
2. Click **Create**.
3. Follow the prompt to enter **Country/Region, Hostname/IP, Validity** and other parameters.
4. Click **OK**.

#### Result

The device will install the self-signed certificate by default.

### Install Authorized Certificate

If the demand for external access security is high, you can create and install authorized certificate via HTTPS protocol to ensure the data transmission security.

#### Steps

1. Select **Create certificate request first and continue the installation**.
2. Click **Create**.
3. Follow the prompt to input **Country/Region, Hostname/IP, Validity** and other parameters.
4. Click **Download** to download the certificate request and submit it to the trusted authority for signature.

5. Import certificate to the device.
  - Select **Signed certificate is available, start the installation directly**. Click **Browse** and **Install** to import the certificate to the device.
  - Select **Create the certificate request first and continue the installation**. Click **Browse** and **Install** to import the certificate to the device.
6. Click **Save**.

### 13.13.7 Set QoS

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



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**.



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**.

### 13.13.8 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

EAP-TLS and EAP-MD5 are selectable

##### EAP-MD5

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.

##### EAP-TLS

If you use EAP-TLS, input Identify, Private Key Password, and upload CA Certificate, User Certificate and Private Key.

## EAPOL Version

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

### 13.13.9 Set Control Timeout

This function helps to better protect the account information from unauthorized changes.

#### Steps

1. Go to **Configuration → System → Security → Advanced Security** .
2. Check **Enable Control Timeout** to enable the function.
3. Set the timeout duration by adjusting the timeout slider.
4. Click **Save**.

#### Result

You will be logged out if your control session times out due to inactivity. The unsaved parameters will not automatically be saved under this circumstance.

### 13.13.10 Certificate Management

It helps to manage the server/client certificates and CA certificate, and to send an alarm if the certificates are close to expiry date, or are expired/abnormal.



The function is only supported by certain device models.

---

## Create and Install Self-signed Certificate

#### Steps

1. Go to **Configuration → System → Security → Certificate Management** .
2. Click **Create Self-signed Certificate**.
3. Input certificate information.



The input certificate ID cannot be the same as the existing ones.

---

4. Click **OK** to save and install the certificate.

The created certificate is displayed in the **Server/Client Certificate** list.

If the certificate is used by certain functions, the function name is shown in the column **Functions**.

5. **Optional:** Click **Certificate Property** to see the certificate details.

## Install Self-signed Request Certificate

You can send the self-signed certificate to a trusted third-party for the signature, and install the certificate to the device.

### Before You Start

Create a self-signed certificate first. See [\*\*\*Create and Install Self-signed Certificate\*\*\*](#) for instructions.

### Steps

1. Go to **Configuration → System → Security → Certificate Management** .
2. Select a self-signed certificate from the Server/Client Certificate list.
3. Click **Create Certificate Request**.
4. Input request information.
5. Click **OK**.

The certificate request details are displayed in a pop-up window.

6. Copy the request content and save it as a request file.
7. Send the file to a trusted-third party for signature.
8. After receiving the certificated sent back from the third-party, install it to the device.
  - 1) Click **Import**.
  - 2) Input **Certificate ID**.



The input certificate ID cannot be the same as the existed ones.

---

- 3) Click **Browse** to select the certificate file.
- 4) Select **Self-signed Request Certificate**.
- 5) Click **OK**.

The imported certificate is displayed in the **Server/Client Certificate** list.

If the certificate is used by certain function, the function name is shown in the column **Functions**.

9. **Optional:** Click **Certificate Property** see the certificate details.

## Install CA Certificate

### Before You Start

Prepare a CA certificate in advance.

### Steps

1. Go to **Configuration → System → Security → Certificate Management** .
2. Input **Certificate ID**.



The input certificate ID cannot be the same as the existing ones.

---

3. Click **Browse** to select the certificate file.

4. Click **OK**.

The imported certificate is displayed in the **CA Certificate** list.

If the certificate is used by certain functions, the function name is shown in the **Functions** column.

### Enable Certificate Expiration Alarm

#### Steps

1. Check **Enable Certificate Expiration Alarm**. If enabled, you will receive an email or the camera links to the surveillance center that the certificate will expire soon, or is expired or abnormal.
2. Set the **Remind Me Before Expiration (day)**, **Alarm Frequency (day)** and **Detection Time (hour)**.



#### Note

- If you set the reminding day before expiration to 1, then the camera will remind you the day before the expiration day. 1 to 30 days are available. Seven days is the default reminding days.
- If you set the reminding day before expiration to 1, and the detection time to 10:00, and the certificate will expire in 9:00 the next day, the camera will remind you in 10:00 the first day.

---

3. Click **Save**.

## 13.14 User and Account

### 13.14.1 Set User Account and Permission

The administrator can add, modify, or delete other accounts, and grant different permission to different user levels.



#### Caution

To increase security of using the device on the network, please change the password of your account regularly. Changing the password every 3 months is recommended. If the device is used in high-risk environment, it is recommended that the password should be changed every month or week.

---

#### Steps

1. Go to **Configuration → System → User Management → User Management** .
2. Click **Add**. Enter **User Name**, select **Level**, and enter **Password**. Assign remote permission to users based on needs.

#### Administrator

The administrator has the authority to all operations and can add users and operators and assign permission.



## User

Users can be assigned permission of viewing live video, setting PTZ parameters, and changing their own passwords, but no permission for other operations.

## Operator

Operators can be assigned all permission except for operations on the administrator and creating accounts.

**Modify** Select a user and click **Modify** to change the password and permission.

**Delete** Select a user and click **Delete**.

---

## Note

The administrator can add up to 31 user accounts.

---

3. Click **OK**.

## 13.14.2 Online Users

The information of users logging into the device is shown.

Go to **Configuration** → **System** → **User Management** → **Online Users** to view the list of online users.

## Chapter 14 Appendix

### 14.1 Common Material Emissivity Reference

Material	Emissivity
Human Skin	0.98
Printed Circuit Board	0.91
Concrete	0.95
Ceramic	0.92
Rubber	0.95
Paint	0.93
Wood	0.85
Pitch	0.96
Brick	0.95
Sand	0.90
Soil	0.92
Cloth	0.98
Hard Paperboard	0.90
White Paper	0.90
Water	0.96

### 14.2 Device Command

Scan the following QR code to get device common serial port commands.

Note that the command list contains the commonly used serial port commands for Hikvision thermal cameras.



### 14.3 Device Communication Matrix

Scan the following QR code to get device communication matrix.

Note that the matrix contains all communication ports of Hikvision thermal cameras.



