



# Thermal & Optical Bi-spectrum 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 DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR

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




---

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 (12 VDC, 24 VAC, or PoE(802.3af)) 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.

### 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.

### Using Environment

- Make sure the running environment meets the requirement of the device. The operating temperature shall be -40°C to 65°C (-40°F to 149°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>
<b>1.1 Brief Description</b> .....	<b>1</b>
<b>1.2 Function</b> .....	<b>1</b>
<b>Chapter 2 Device Activation and Accessing</b> .....	<b>2</b>
<b>2.1 Activate the Device via SADP</b> .....	<b>2</b>
<b>2.2 Activate the Device via Browser</b> .....	<b>2</b>
<b>2.3 Login</b> .....	<b>3</b>
<b>2.3.1 Plug-in Installation</b> .....	<b>3</b>
<b>2.3.2 Illegal Login Lock</b> .....	<b>4</b>
<b>Chapter 3 Perimeter Protection</b> .....	<b>5</b>
<b>3.1 Flow Chart of Perimeter Protection</b> .....	<b>5</b>
<b>3.2 Set VCA Parameters</b> .....	<b>6</b>
<b>3.3 Set Rules</b> .....	<b>6</b>
<b>3.4 Set Shielded Region</b> .....	<b>8</b>
<b>3.5 Advanced Configuration</b> .....	<b>9</b>
<b>Chapter 4 Event and Alarm</b> .....	<b>10</b>
<b>4.1 Set Motion Detection</b> .....	<b>10</b>
<b>4.1.1 Normal Mode</b> .....	<b>10</b>
<b>4.1.2 Expert Mode</b> .....	<b>11</b>
<b>4.2 Set Video Tampering Alarm</b> .....	<b>12</b>
<b>4.3 Set Alarm Input</b> .....	<b>13</b>
<b>4.4 Set Exception Alarm</b> .....	<b>14</b>
<b>4.5 Detect Scene Change</b> .....	<b>14</b>
<b>Chapter 5 Arming Schedule and Alarm Linkage</b> .....	<b>15</b>
<b>5.1 Set Arming Schedule</b> .....	<b>15</b>
<b>5.2 Linkage Method Settings</b> .....	<b>15</b>
<b>5.2.1 Trigger Alarm Output</b> .....	<b>15</b>
<b>5.2.2 FTP/NAS/Memory Card Uploading</b> .....	<b>16</b>
<b>5.2.3 Send Email</b> .....	<b>17</b>



5.2.4 Notify Surveillance Center .....	18
5.2.5 Trigger Recording .....	18
5.2.6 Set Audible Alarm Output .....	18
5.2.7 Set Flashing Alarm Light Output .....	19
<b>Chapter 6 Live View .....</b>	<b>20</b>
6.1 Live View Parameters .....	20
6.1.1 Window Division .....	20
6.1.2 Live View Stream Type .....	20
6.1.3 Enable and Disable Live View .....	20
6.1.4 Start Digital Zoom .....	20
6.1.5 View Previous/Next Page .....	21
6.1.6 Full Screen .....	21
6.1.7 Light .....	21
6.1.8 Wiper .....	21
6.1.9 Lens Initialization .....	21
6.1.10 Auxiliary Focus .....	21
6.1.11 Quick Set Live View .....	21
6.1.12 Lens Parameters Adjustment .....	22
6.2 Set Transmission Parameters .....	22
<b>Chapter 7 Video and Audio .....</b>	<b>24</b>
7.1 Video Settings .....	24
7.1.1 Stream Type .....	24
7.1.2 Video Type .....	24
7.1.3 Resolution .....	24
7.1.4 Bitrate Type and Max. Bitrate .....	25
7.1.5 Video Quality .....	25
7.1.6 Frame Rate .....	25
7.1.7 Video Encoding .....	25
7.1.8 Smoothing .....	26
7.1.9 Display VCA Info .....	26
7.1.10 Set ROI .....	27

7.1.11 Metadata.....	27
7.2 Display Settings.....	28
7.2.1 Image Adjustment.....	28
7.2.2 Image Adjustment (Thermal Channel) .....	28
7.2.3 Exposure Settings.....	29
7.2.4 Day/Night Switch .....	29
7.2.5 Supplement Light Settings.....	29
7.2.6 BLC .....	30
7.2.7 WDR .....	30
7.2.8 White Balance .....	31
7.2.9 DNR .....	31
7.2.10 Defog.....	31
7.2.11 Gray Scale.....	31
7.2.12 Set Target Color.....	32
7.2.13 DDE.....	32
7.2.14 Brightness Sudden Change .....	32
7.2.15 Enhance Regional Image .....	32
7.2.16 Mirror.....	33
7.2.17 Video Standard.....	33
7.2.18 Digital Zoom .....	33
7.2.19 Scene Mode.....	33
7.2.20 Local Output.....	33
7.3 OSD .....	34
7.4 Set Privacy Mask.....	34
7.5 Overlay Picture .....	35
7.6 Set Manual DPC (Defective Pixel Correction).....	35
7.7 Set Picture in Picture.....	35
<b>Chapter 8 Video Recording and Picture Capture .....</b>	<b>37</b>
8.1 Storage Settings .....	37
8.1.1 Set Memory Card .....	37
8.1.2 Set NAS.....	37

8.1.3 Set FTP.....	38
8.1.4 Set Cloud Storage .....	39
8.2 Video Recording.....	39
8.2.1 Record Automatically .....	40
8.2.2 Record Manually .....	41
8.2.3 Playback and Download Video.....	41
8.3 Capture Configuration .....	42
8.3.1 Capture Automatically .....	42
8.3.2 Capture Manually.....	43
8.3.3 View and Download Picture .....	43
<b>Chapter 9 Network Settings .....</b>	<b>44</b>
9.1 TCP/IP .....	44
9.1.1 Multicast Discovery.....	45
9.2 Port .....	45
9.3 Port Mapping .....	46
9.3.1 Set Auto Port Mapping.....	46
9.3.2 Set Manual Port Mapping .....	47
9.4 Multicast.....	47
9.5 SNMP .....	47
9.6 Access to Device via Domain Name .....	48
9.7 Access to Device via PPPoE Dial Up Connection .....	48
9.8 Enable Hik-Connect Service on Camera .....	49
9.8.1 Enable Hik-Connect Service via Web Browser.....	49
9.8.2 Enable Hik-Connect Service via SADP Software .....	50
9.8.3 Access Camera via Hik-Connect.....	50
9.9 Set ISUP.....	51
9.10 Set Open Network Video Interface .....	51
9.11 Set Alarm Host .....	52
9.12 Set Alarm Server .....	52
9.13 Set Network Service.....	53
9.14 Set SRTP .....	53

<b>Chapter 10 System and Security</b> .....	<b>54</b>
<b>10.1 View Device Information</b> .....	54
<b>10.2 Search and Manage Log</b> .....	54
<b>10.3 Import and Export Configuration File</b> .....	54
<b>10.4 Export Diagnose Information</b> .....	55
<b>10.5 Reboot</b> .....	55
<b>10.6 Restore and Default</b> .....	55
<b>10.7 Upgrade</b> .....	55
<b>10.8 View Open Source Software License</b> .....	56
<b>10.9 Time and Date</b> .....	56
<b>10.9.1 Synchronize Time Manually</b> .....	56
<b>10.9.2 Set NTP Server</b> .....	56
<b>10.9.3 Set DST</b> .....	57
<b>10.10 Set RS-232</b> .....	57
<b>10.11 Security</b> .....	57
<b>10.11.1 Authentication</b> .....	57
<b>10.11.2 Security Audit Log</b> .....	58
<b>10.11.3 Set IP Address Filter</b> .....	58
<b>10.11.4 Certificate Management</b> .....	59
<b>10.11.5 Control Timeout Settings</b> .....	61
<b>10.11.6 Set SSH</b> .....	61
<b>10.11.7 Set HTTPS</b> .....	61
<b>10.11.8 Set QoS</b> .....	62
<b>10.11.9 Set IEEE 802.1X</b> .....	62
<b>10.12 User and Account</b> .....	63
<b>10.12.1 Set User Account and Permission</b> .....	63
<b>Chapter 11 Appendix</b> .....	<b>64</b>
<b>11.1 Common Material Emissivity Reference</b> .....	64
<b>11.2 Device Command</b> .....	64
<b>11.3 Device Communication Matrix</b> .....	65
<b>11.4 FAQ</b> .....	65

# Chapter 1 Overview

## 1.1 Brief Description

Thermal & Optical Bi-spectrum network camera equipped with built-in GPU which supports intelligent perimeter protection algorithm, can realize high-precision VCA detection and real-time alarm. It is applied to perimeter protection and fire-prevention purposes in critical infrastructures such as community, villa, construction site, factory, 4S stores, and so on. 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.

---

### Note

Not all models support the configurations below. Take the actual product for reference.

---

### VCA

Device can do perimeter protection. Multiple rules can be configured for different requirements.

### Motion Detection

Device detects the moving objects in the configured video security area, and triggers the certain action as a respond to detection.

## 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.

---

### Note

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.

---

### Caution

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+	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

Operating System	Web Browser	Operation
		plug-in installation is not required. 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 Perimeter Protection

The perimeter protection function is used to detect whether there is any target break the VCA rules. The optical camera will track the target or the device will alarm when the VCA rule is triggered.

### 3.1 Flow Chart of Perimeter Protection

The process of configuring the perimeter protection function is described below.

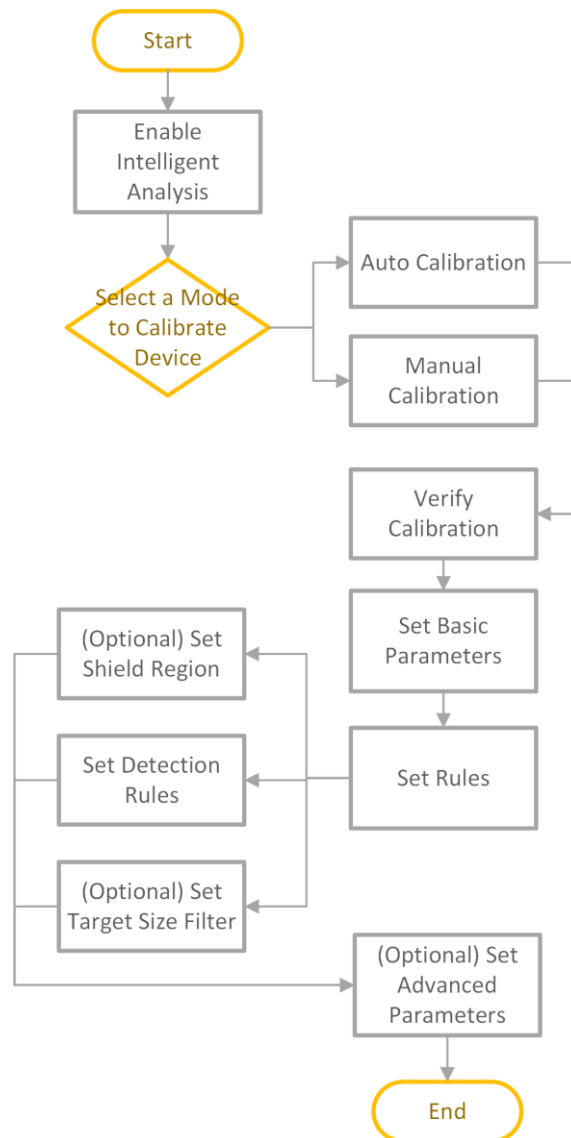


Figure 3-1 Flow Chart of Perimeter Protection Configuration

## 3.2 Set VCA Parameters

### Steps

1. Go to **Configuration** → **VCA** → **Overlay & Capture**.

#### 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 Trajectory

The target's moving path will be shown in live view.

#### 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.

#### Display Size Info. on Alarm Picture

Select to display the size information of the target 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 and resolution of the picture separately.

2. Click **Save**.

Go to **Configuration** → **Local**, check **Enable** rules to display rules information on the live view.

## 3.3 Set Rules

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

### Steps

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

#### Line Crossing

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

#### Intrusion

If any target intrudes 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. Draw the detection rule.

**Table 3-1 Configure VCA Rules**

<b>Rule Type</b>	<b>How to Draw and What Parameters to Set</b>
Line Crossing	<ol style="list-style-type: none"><li>1. Click  to draw a line in the live view.</li><li>2. You can drag end points of the line to adjust the position and length.</li><li>3. Set the crossing direction. <b>Bidirectional</b>, <b>A-to-B</b>, or <b>B-to-A</b> are selectable.</li><li>4. Set <b>Sensitivity</b>. The higher the value is, the easier the target can be detected.</li></ol>
Intrusion	<ol style="list-style-type: none"><li>1. Click  to draw an area in the live view. Right click the mouse to finish drawing.</li><li>2. Set <b>Duration</b>. When a target intrudes into the set area and stays in the area for more than the set duration, the device triggers an intrusion alarm.</li><li>3. Set <b>Sensitivity</b>. The higher the value is, the easier the target can be detected.</li></ol>
Region Entrance and Region Exit	<p>Click  to draw an area in the live view. Right click the mouse to finish drawing.</p> <p>Target that enters or exits the set area triggers the region entrance or region exit alarm.</p>

5. Set other parameters for the rule.

## Detection Target

You are recommended to select the target as **Human & Vehicle**.

## Scene Mode

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

### Note

In distance 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 increase trigger false alarm rate but decrease missing alarm rate.

---

### Background Interference Suppression

Eliminate the environment interference to reduce the false alarm. For example, the false alarms caused by wind blowing grass.

---

### Note

The parameter is available in optical channel.

---


### Filter by Pixel

Check to enable **Filter by Pixel**. 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.
  - Due to the main difference between human and animal is the height. Just concern the height of animal.
- 

6. Optional: Repeat steps above to configure other rules.
7. Optional: Click  to copy the same settings to other rules.
8. Click **Save**.
9. Optional: you can shield certain areas from being detected. Refer to ***Set Shielded Region*** for detailed settings.
10. ***Set Arming Schedule*** and ***Linkage Method Settings*** for each rule.

## 3.4 Set Shielded Region

You can configure areas from being detected.

### Steps

1. Check **Enable Shield Area**.
  2. Click .
  3. 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.
  4. Right click the mouse to stop drawing.
  5. Optional: Select one area and click  to delete it.
  6. Click **Save**.
-

## 3.5 Advanced Configuration

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

Detection Parameters

### Single Alarm

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

Restore Parameters

### Restore Default

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

### Restart VCA

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

---

### Note

The settings vary according to different models.

---

## Chapter 4 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.

### 4.1 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**.

#### 4.1.1 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 4-1 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.

### 4.1.2 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 4-2 Set Rules**

**Stop Drawing**                      Finish drawing one area.

**Clear All**                              Delete all the areas.

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

## 4.2 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 4-3 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**.

### 4.3 Set Alarm Input

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

#### Before You Start

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

#### Steps

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

## 4.4 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.

3. Refer to [Linkage Method Settings](#) for setting linkage method.
4. Click **Save**.

## 4.5 Detect Scene Change

Scene change detection function detects the change of the scene. Some certain actions can be taken when the alarm is triggered.

### Steps

1. Go to **Configuration** → **Event** → **Smart Event** → **Scene Change Detection**.
2. Click **Enable**.
3. Set the **Sensitivity**. The higher the value is, the more easily the change of scene can be detected. But the detection accuracy is reduced.
4. Refer to [Set Arming Schedule](#) for setting scheduled time. Refer to [Linkage Method Settings](#) for setting linkage method.
5. Click **Save**.

---

### Note

The function varies according to different models.

---

## Chapter 5 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.

### 5.1 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**.

### 5.2 Linkage Method Settings

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

#### 5.2.1 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

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

Custom 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**.

### 5.2.2 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.

### 5.2.3 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) Configure **Alarm E-mail Attachment Settings**.

#### Image

Select the number of captures of the corresponding channel.

- 0: It will not upload the image of the selected channel.
- 1: It will only upload the image captured when the alarm is triggered.
- 3: It will upload the images captured about 1 s before and after the alarm is triggered, as

well as the image captured when the alarm is triggered.

### Video

Select the video channel and video duration as required.

- 0 s: It will not upload the video of the selected channel.
- 3 s: Upload the video that is recorded about 1 s before and 2 s after the alarm is triggered.
- 5 s: Upload the video that is recorded about 2 s before and 3 s after the alarm is triggered.
- 7 s: Upload the video that is recorded about 2 s before and 5 s after the alarm is triggered.

6) Input the receiver's information, including the receiver's name and address.

7) Click **Test** to see if the function is well configured.

3. Click **Save**.

### 5.2.4 Notify Surveillance Center

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

### 5.2.5 Trigger Recording

Check **Trigger Recording**, and the device records the video about the detected alarm event. For device with more than one camera channels, you can set one or more channels to take recordings if needed.

For recording settings, refer to [\*Video Recording and Picture Capture\*](#).

### 5.2.6 Set Audible Alarm Output

When the device detects targets in the detection area, audible alarm can be triggered as a warning.

#### Steps

1. Go to **Configuration** → **Event** → **Basic Event** → **Audible Alarm Output**.
2. Select an **Alarm Type**.
3. Select **Sound Type** and set related parameters.
  - Select **Warning** and its contents. Set the alarm times you need.
  - Select **Custom Audio**. You can select a custom audio file from the drop-down list. If no file is available, you can click **Add** to upload an audio file that meets the requirement. Up to six audio files can be uploaded, and each audio file shall not exceed 512 KB.
4. Optional: Click **Test** to play the selected audio file on the device.
5. Set arming schedule for audible alarm. See [\*Set Arming Schedule\*](#) for details.
6. Click **Save**.

 **Note**

The function is only supported by certain device models.

---

## 5.2.7 Set Flashing Alarm Light Output

### Steps

1. Go to **Configuration** → **Event** → **Basic Event** → **Flashing Alarm Light Output**.
2. Select a **White Light Mode**.

<b>Mode</b>	<b>Description</b>
<b>Flashing</b>	Alarm triggers the light to flash for a certain duration. Set the flashing speed in <b>Flashing Frequency</b> .
<b>Solid</b>	Alarm triggers the light to turn on for a certain duration.

3. Set the light action duration and the brightness.

### **Flashing Duration**

The time period of light on or light flashing when one alarm happens.

### **Brightness**

The brightness of the light.

4. Edit the arming schedule.
5. Click **Save**.

 **Note**

Only certain camera models support the function.

---

## Chapter 6 Live View

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

### 6.1 Live View Parameters

The supported functions vary depending on the model.







**Note**

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

---

#### 6.1.1 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.

#### 6.1.2 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\*](#).

#### 6.1.3 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.

#### 6.1.4 Start Digital Zoom

It helps to see a detailed information of any region in the image.

##### Steps

1. Click  to enable the digital zoom.
2. In live view image, drag the mouse to select the desired region.
3. Click in the live view image to back to the original image.



### 6.1.5 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.

### 6.1.6 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.

### 6.1.7 Light

Click  to turn on or turn off the illuminator.

### 6.1.8 Wiper

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

Click  on live view page. The wiper wipes the window one time.

### 6.1.9 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.

Click  to operate lens initialization.


### 6.1.10 Auxiliary Focus

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

### 6.1.11 Quick Set Live View

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

#### Steps

1. Click  to show quick setup page.
2. Set PTZ, display settings, OSD, video/audio and VCA resource 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](#).

– For VCA settings, see *Perimeter Protection*.

---

### Note



The function is only supported by certain models.

---



## 6.1.12 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.

### Iris

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

### Note

The function is only supported by certain models.

---

## 6.2 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.

### **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.

### **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 7 Video and Audio

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

### 7.1 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.

---

#### 7.1.1 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.

#### 7.1.2 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.

#### 7.1.3 Resolution

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

and storage.

### 7.1.4 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.

### 7.1.5 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.

### 7.1.6 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.

### 7.1.7 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.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.

### **MJPEG**

Motion JPEG (M-JPEG or MJPEG) is a video compression format in which intraframe coding technology is used. Images in a MJPEG format is compressed as individual JPEG images.

### **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 decode high quality video stream.

## **7.1.8 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.

## **7.1.9 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.

### 7.1.10 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.

### 7.1.11 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.

## 7.2 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.

### 7.2.1 Image Adjustment

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



Low Saturation



High Saturation

Figure 7-1 Saturation

### 7.2.2 Image Adjustment (Thermal Channel)

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

#### 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 **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.

### 7.2.3 Exposure Settings

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

In manual mode, you need to set **Exposure Time**, **Gain** and **Slow Shutter**.

### 7.2.4 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 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.

---

### 7.2.5 Supplement Light Settings

You can set supplement light and refer to the actual device for relevant parameters.

#### Smart Supplement Light

Smart supplement light avoids over exposure when the supplement light is on.

#### Supplement Light Mode

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

#### IR Supplement Light

IR light is enabled.

#### White Light

White light is enabled.

### Mixed Light

Both IR light and white light are enabled.

### Smart

When you select this mode after enabling certain smart events or motion detection, in the night state, the default supplement light mode is IR supplement light mode. When the alarm is triggered, the white light is enabled and the device captures the target. After the alarm ends, the supplement light mode will switch to IR supplement light mode.

Only device models with IR and white light or hybrid supplement light with IR and white light support this function.

### Off

Supplement light is disabled.

---

### Note

The supplement light mode may vary according to different device models.

---

## Brightness Adjustment Mode

### Auto

The brightness adjusts according to the actual environment automatically.

### Manual

You can drag the slider or set value to adjust the brightness.

## 7.2.6 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.

## 7.2.7 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.

---

## 7.2.8 White Balance

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

## 7.2.9 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.

## 7.2.10 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 7-2 Defog

## 7.2.11 Gray Scale

This section introduces the gray scale function in optical channel. You can choose the range of the gray scale as [0-255] or [16-235].

## 7.2.12 Set Target Color

You can set the color of the targets in different temperature ranges to identify the target quickly.

### Steps

1. Go to **Configuration** → **Image** → **Display Settings**.
2. Select the thermal channel.
3. Click **Image Enhancement**, select **Palette** as **White Hot** or **Black Hot**.
4. Set the temperature value and color of **High Temperature**, **Interval Temperature**, or **Low Temperature** targets.

#### **Above (be colored)**

When the target of high temperature needs to be colored, you can set the high temperature color. Target above the setting temperature will be displayed in setting color.

#### **Between (be colored)**

When the target of an interval temperature needs to be colored, you can set the interval temperature color. Target between the minimum and the maximum temperatures will be displayed in setting color.

#### **Below (be colored)**

When the target of low temperature needs to be colored, you can set the low temperature color. Target below the setting temperature will be displayed in setting color.

5. Click **Save**.

## 7.2.13 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.

## 7.2.14 Brightness Sudden Change

When the brightness of target and the background is hugely different (the temperature difference of target and background is huge), the system reduces the difference for viewing.

## 7.2.15 Enhance Regional Image

You can select the desired area of image to improve the coding quality. The regional image will be

more detailed and clear.

### Steps

1. Go to **Configuration** → **Image** → **Display Settings** → **Image Enhancement**.
2. Select the area of regional image enhancement. You can select **OFF** to disable this function, or select **Custom Area** to draw a desired area.  
A red rectangle shows on the display, in which the image quality is improved.

### 7.2.16 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.

---

### 7.2.17 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.

### 7.2.18 Digital Zoom

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

### 7.2.19 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.

### 7.2.20 Local Output

Enter a short description of your concept here (optional).

Some camera models support CVBS, SDI, or HDMI output. Set the local output ON or OFF according to the actual device. This is the start of your concept.

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

Select a channel.

### Displayed Information

Check to display camera name, date, week, laser ranging info, image center on the screen. You can set the time and date formats.

### Text Overlay

Set customized overlay text on image.

### OSD Parameters

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

## 7.4 Set Privacy Mask

The function blocks certain areas in the live view to protect privacy. No matter how the device moves, the blocked scene will never be seen.

### Steps

1. Go to privacy mask setting page: **Configuration** → **Image** → **Privacy Mask**.
2. Select the channel No.
3. Check **Enable Privacy Mask**.
4. Click **Draw Area**. Drag the mouse in the live view to draw a closed area.

**Drag the corners of the area**      Adjust the size of the area.

**Drag the area**      Adjust the position of the area.

**Click Clear All**      Clear all the areas you set.

5. Click **Stop Drawing**.

6. Click **Save**.



Up to 4 areas are supported for setting.

---

## 7.5 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**.

## 7.6 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.

## 7.7 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.

**Normal Mode**

Disable picture in picture mode.

**Details Overlay Mode**

Enable picture in picture mode. You can overlay the image of another channel in the current channel.

3. Click **Save**.



## Chapter 8 Video Recording and Picture Capture

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

### 8.1 Storage Settings

This part introduces the configuration of several common storage paths.

#### 8.1.1 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. Optional: Check to enable **POS Information Storage**, then the device will record the POS information of reflect light filter and forklift filter.

---

##### Note

The function is supported when your memory card capacity is 32 GB or above. Formatting the memory card manually is required to reserve 16 GB for POS information.

---

5. Click **Save**.

#### 8.1.2 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.**. Enter the server address and file path for the disk.

#### Server Address

The IP address of the network disk.

#### File Path

The saving path of network disk files.

#### Mounting Type

Select file system protocol according to the operation system.

Enter user name and password of the net HDD to guarantee the security if **SMB/CIFS** is selected.

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

### 8.1.3 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.

#### FTP Protocol

FTP and SFTP are selectable. The files uploading is encrypted by using SFTP protocol.

#### 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.

---

#### Note

If SFTP is used, logging into the FTP server anonymously is now allowed.

---

#### Directory Structure

The saving path of snapshots in the FTP server.

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

### 8.1.4 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



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

---

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. You are recommended to use the default port.
<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**.

## 8.2 Video Recording

This part introduces the operations of manual and scheduled recording, playback, and

downloading recorded files.

### 8.2.1 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.



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**.

## 8.2.2 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  to start recording. Click  to stop recording.

## 8.2.3 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.

---

## 8.3 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.

### 8.3.1 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**.

### 8.3.2 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.

### 8.3.3 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 9 Network Settings

### 9.1 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** → **Basic Configuration** → **Network** → **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.

---

#### Note

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

---

#### Manual

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

#### IPv6

Three IPv6 modes are available.

##### Route Advertisement

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

---

#### Note

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

---

##### DHCP

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



### Manual

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

### MTU

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

The valid value range of MTU is 1280 to 1500.

### 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.

## 9.1.1 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.

## 9.2 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.
- 

## 9.3 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**.

### 9.3.1 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.

---

## 9.3.2 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.

## 9.4 Multicast

Multicast is group communication where data transmission is addressed to a group of destination devices simultaneously. After setting multicast, you can send the source data efficiently to multiple receivers.

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

### 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.

## 9.5 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**.

## 9.6 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.

## 9.7 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.

---

### Note

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

---

## 9.8 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.

### 9.8.1 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.
- 

#### **Note**

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

---

7. Save the settings.

### 9.8.2 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.
- 

#### **Note**

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.

### 9.8.3 Access Camera via Hik-Connect

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

#### **Before You Start**

Connect the camera to network with network cables.

### 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** → **Hikvision App Store**. Scan

the QR code below to download the application.



---

### Note

If errors like "Unknown app" occur during the installation, solve the problem in two ways. Visit <https://appstore.hikvision.com/static/help/index.html> to refer to the troubleshooting. Visit <https://appstore.hikvision.com/>, and click **Installation Help** at the upper right corner of the interface to refer to the troubleshooting.

---

2. Start the application and register for a Hik-Connect user account.
3. Log in after registration.
4. In the app, tap "+" on the upper-right corner and then scan the QR code of the camera to add the camera. You can find the QR code on the camera or on the cover of the Quick Start Guide of the camera in the package.
5. Follow the prompts to set the network connection and add the camera to your Hik-Connect account.

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

## 9.9 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.

## 9.10 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.

## 9.11 Set Alarm Host

The device can send the alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software.

### Steps

1. Go to **Configuration** → **Network** → **Other**.

2. Enter the alarm host IP and port.

3. Click **Save**.

## 9.12 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**.



## 9.13 Set Network Service

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

### Steps



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**.

## 9.14 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 10 System and Security

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

### 10.1 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.

### 10.2 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.

### 10.3 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**.

## 10.4 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.

## 10.5 Reboot

You can reboot the device via browser. Go to **Configuration** → **System** → **Maintenance** → **Upgrade & Maintenance**, and click **Reboot**.

## 10.6 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.

<b>Restore</b>	Reset device parameters, except user information, IP parameters and video format to the default settings.
----------------	---

<b>Default</b>	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.

---

## 10.7 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**.

## 10.8 View Open Source Software License

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

## 10.9 Time and Date

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

### 10.9.1 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**.

### 10.9.2 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**.

### Note

Server Address is NTP server IP address.

---

5. Click **Test** to test server connection.
6. Click **Save**.

### 10.9.3 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**.

### 10.10 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**.

### 10.11 Security

You can improve system security by setting security parameters.

#### 10.11.1 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.

---

## 10.11.2 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



#### Note

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.

## 10.11.3 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 to the list.

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

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

5. Click **Save**.

### 10.11.4 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.



#### Note

The function is only supported by certain device models.

---

### Create Self-signed Certificate

#### Steps

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



#### Note

The certificate ID should be digits or letters and be no more than 64 characters.

---

3. Click **OK**.
4. Optional: Click **Export** to export the certificate, or click **Delete** to delete the certificate to recreate a certificate, or click **Certificate Properties** to view the certificate details.

## Create Certificate Request

### Before You Start

Select a self-signed certificate.

### Steps

1. Click **Create Certificate Request**.
2. Enter the related information.
3. Click **OK**.

## Import Certificate

### Steps

1. Click **Import**.
2. Click **Create Certificate Request**.
3. Enter the **Certificate ID**.
4. Click **Browser** to select the desired server/client certificate.
5. Select the desired import method and enter the required information.
6. Click **OK**.
7. Optional: Click **Export** to export the certificate, or click **Delete** to delete the certificate to recreate a certificate, or click **Certificate Properties** to view the certificate details.

---

### Note

- Up to 16 certificates are allowed.
  - If certain functions are using the certificate, it cannot be deleted.
  - You can view the functions that are using the certificate in the functions column.
  - You cannot create a certificate that has the same ID with that of the existing certificate and import a certificate that has the same content with that of the existing certificate.
- 

## Server Certificate/Client Certificate

---

### Note

The device has default self-signed server/client certificate installed. The certificate ID is **default**.

---

## Install CA Certificate

### Steps

1. Click **Import**.
  2. Enter the **Certificate ID**.
  3. Click **Browser** to select the desired server/client certificate.
-



4. Select the desired import method and enter the required information.
5. Click **OK**.

---

### **Note**

Up to 16 certificates are allowed.

---

## 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**.

## 10.11.5 Control Timeout Settings

If this function is enabled, you will be logged out when you make no operation (not including viewing live image) to the device via web browser within the set timeout period.

Go to **Configuration** → **System** → **Security** → **Advanced Security** to complete settings.

## 10.11.6 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**.

## 10.11.7 Set HTTPS

HTTPS is a network protocol that enables encrypted transmission and identity authentication,

which improves the security of remote access.

### Steps

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

---

#### Note

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

- 
5. Click **Save**.

### 10.11.8 Set QoS

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

---

#### Note

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

### Steps

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

---

#### Note

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

- 
3. Click **Save**.

### 10.11.9 Set IEEE 802.1X

You can authenticate user permission of the connected device by setting IEEE 802.1X. Go to **Configuration** → **Network** → **Advanced Settings** → **802.1X**, and enable the function. Select protocol and version according to router information. User name and password of server are required.

## 10.12 User and Account

### 10.12.1 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**.

## Chapter 11 Appendix

### 11.1 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

### 11.2 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.



### 11.3 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.



### 11.4 FAQ

Scan the following QR code to get device common FAQ.





See Far, Go Further