



# Thermographic Cube Camera

User Manual

## Legal Information

© Hangzhou Microimage Software 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 HIKMICRO website ( <http://www.hikmicrotech.com> ).

Please use this Manual with the guidance and assistance of professionals trained in supporting the Product.

### Trademarks



**HIKMICRO**

and other HIKMICRO's trademarks and logos are the properties of HIKMICRO 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". HIKMICRO 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 HIKMICRO 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 HIKMICRO 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 HIKMICRO 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, HIKMICRO WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED. YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING

WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.

IN THE EVENT OF ANY CONFLICTS BETWEEN THIS MANUAL AND THE APPLICABLE LAW, THE 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) 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 -20°C to 50°C (-4°F to 122°F), and the operating humidity shall be 95% or less.
- DO NOT expose the device to high electromagnetic radiation or dusty environments.
- DO NOT aim the lens at the sun or any other bright light.
- The equipment shall not be exposed to dripping or splashing and that no objects filled with liquids, such as vases, shall be placed on the equipment.
- No naked flame sources, such as lighted candles, should be placed on the equipment.
- Provide a surge suppressor at the inlet opening of the equipment under special conditions such as the mountain top, iron tower, and forest.
- Burned fingers when handling the parts with symbol . Wait one-half hour after switching off before handling the parts.

## Emergency

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

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

# Contents

<b>Chapter 1 Overview .....</b>	<b>1</b>
1.1 Brief Description .....	1
1.2 Function .....	1
1.3 Typical Application .....	1
<b>Chapter 2 Device Activation and Accessing .....</b>	<b>4</b>
2.1 Activate the Device via SADP .....	4
2.2 Activate the Device via Browser .....	4
2.3 Login .....	5
2.3.1 Plug-in Installation .....	5
2.3.2 Illegal Login Lock .....	6
2.3.3 Security Reinforcement .....	7
<b>Chapter 3 Temperature Measurement .....</b>	<b>8</b>
3.1 Notice .....	8
3.2 Thermometry Flow Chart .....	8
3.3 Set Shielded Region .....	9
3.4 Automatic Thermography .....	10
3.4.1 Set Thermometry Parameters .....	10
3.4.2 Set Normal Mode .....	12
3.4.3 Set Expert Mode .....	13
3.4.4 Set Thermography Rule .....	14
3.5 External Temperature Sensor .....	17
3.5.1 Set 433 MHz Transmission .....	17
3.5.2 Set External Temperature Sensor .....	18
3.5.3 Connect Temperature Sensors to Device .....	19
3.6 Manual Thermography .....	19
3.7 Upload Temperature Alarm to Center .....	20



3.8 Integration .....	20
3.8.1 Pixel-to-Pixel Thermometry .....	20
3.8.2 Persistent Connection Management .....	21
3.9 Collect Diagnosis Information .....	22
<b>Chapter 4 Event and Alarm .....</b>	<b>23</b>
4.1 Set Video Tampering Alarm .....	23
4.2 Set Exception Alarm .....	24
<b>Chapter 5 Arming Schedule and Alarm Linkage .....</b>	<b>26</b>
5.1 Set Arming Schedule .....	26
5.2 Linkage Method Settings .....	26
5.2.1 Notify Surveillance Center .....	26
5.2.2 Send Email .....	26
5.2.3 FTP/NAS/Memory Card Uploading .....	27
<b>Chapter 6 Live View .....</b>	<b>28</b>
6.1 Live View Parameters .....	28
6.1.1 Select the Third-Party Plug-in .....	28
6.1.2 Window Proportion .....	28
6.1.3 Live View Stream Type .....	28
6.1.4 Enable and Disable Live View .....	28
6.1.5 Start Digital Zoom .....	28
6.1.6 Online Capture .....	29
6.2 Quick Set Live View .....	29
6.3 Set Transmission Parameters .....	29
<b>Chapter 7 Video and Image Settings .....</b>	<b>31</b>
7.1 Video Settings .....	31
7.1.1 Stream Type .....	31
7.1.2 Video Type .....	31
7.1.3 Resolution .....	31

7.1.4 Bitrate Type and Max. Bitrate .....	31
7.1.5 Video Quality .....	32
7.1.6 Frame Rate .....	32
7.1.7 Video Encoding .....	32
7.1.8 Smoothing .....	33
7.1.9 Set ROI .....	33
7.1.10 Display VCA Info .....	34
7.1.11 Metadata .....	34
7.2 Display Settings .....	35
7.2.1 Image Adjustment (Thermal Channel) .....	35
7.2.2 DNR .....	35
7.2.3 Set Palette .....	36
7.2.4 Set Target Enhancement .....	36
7.2.5 Set Palette Range .....	36
7.2.6 DDE .....	37
7.2.7 Mirror .....	37
7.2.8 Rotate .....	37
7.2.9 Digital Zoom .....	37
7.3 OSD .....	38
7.4 Set Privacy Mask .....	38
7.5 Overlay Picture .....	38
7.6 Set Manual DPC (Defective Pixel Correction) .....	39
7.7 VCA Rule Display Settings .....	39
<b>Chapter 8 Video Recording and Picture Capture .....</b>	<b>40</b>
8.1 Storage Settings .....	40
8.1.1 Set Memory Card .....	40
8.1.2 Set NAS .....	40
8.1.3 Set FTP .....	41

8.1.4 Set Cloud Storage .....	41
8.2 Video Recording .....	42
8.2.1 Record Automatically .....	42
8.2.2 Record Manually .....	44
8.2.3 Playback and Download Video .....	44
8.3 Capture Configuration .....	44
8.3.1 Capture Automatically .....	44
8.3.2 Capture Manually .....	45
8.3.3 View and Download Picture .....	45
<b>Chapter 9 Network Settings .....</b>	<b>47</b>
9.1 TCP/IP .....	47
9.1.1 Multicast Discovery .....	48
9.2 Port .....	48
9.3 Port Mapping .....	49
9.3.1 Set Auto Port Mapping .....	50
9.3.2 Set Manual Port Mapping .....	50
9.3.3 Set Port Mapping on Router .....	50
9.4 Multicast .....	51
9.5 SNMP .....	52
9.6 Access to Device via Domain Name .....	52
9.7 Set Alarm Server .....	53
9.8 Set ISUP .....	53
9.9 Set Open Network Video Interface .....	54
9.10 Set Network Service .....	54
9.11 Modbus Communication .....	55
9.11.1 Set Modbus Main Mode .....	55
9.11.2 Set Modbus Subordinate Mode .....	57
9.11.3 Modbus Error Code Description .....	58

<b>Chapter 10 System and Security .....</b>	<b>61</b>
10.1 View Device Information .....	61
10.2 Search and Manage Log .....	61
10.3 Import and Export Configuration File .....	61
10.4 Export Diagnose Information .....	62
10.5 Reboot .....	62
10.6 Restore and Default .....	62
10.7 Upgrade .....	62
10.8 eMMC Protection .....	63
10.9 View Open Source Software License .....	63
10.10 Time and Date .....	63
10.10.1 Synchronize Time Manually .....	63
10.10.2 Set NTP Server .....	64
10.10.3 Set DST .....	64
10.11 Set RS-232 .....	64
10.12 Set RS-485 .....	65
10.13 Set Same Unit .....	65
10.14 Security .....	66
10.14.1 Authentication .....	66
10.14.2 Security Audit Log .....	66
10.14.3 Set IP Address Filter .....	67
10.14.4 Set HTTPS .....	67
10.14.5 Certificate Management .....	68
10.14.6 Set QoS .....	70
10.14.7 Create and Install Self-signed Certificate .....	70
10.14.8 Set IEEE 802.1X .....	71
10.15 User and Account .....	71
10.15.1 Set User Account and Permission .....	71

10.15.2 Online Users ..... 72

**Chapter 11 Appendix ..... 73**

11.1 Common Material Emissivity Reference ..... 73

# Chapter 1 Overview

## 1.1 Brief Description

The Thermographic Cube Camera is a temperature measurement device which is equipped with a thermal lens.

It is equipped with high-sensitivity IR detector and high-performance sensor. The device is able to measure object's temperature at a high accuracy in real time. It is applied to electric system, and industrial automation, etc, for fire prevention. 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.

### Temperature Measurement

Device detects the real-time temperature all the day, and display it on live view.

### Temperature Exception Alarm

Device outputs alarm when the temperature is higher than the setting alarm threshold value.

### Image Adjustment

Device can correct the nonuniformity of the image and improve the image quality.

## 1.3 Typical Application

Thermographic Cube Camera supports 433MHz wireless transmission, which makes it more friendly to use in the application scenarios where cable routing is inconvenient.

The device receives temperature data and alarm from external temperature detectors with 433MHz wireless transmission and uploads the data to the center.

When sending data to the center client (iVMS-4200), the device supports a wireless way (with the help of a gateway that supports 433MHz transmission) and a wired way.

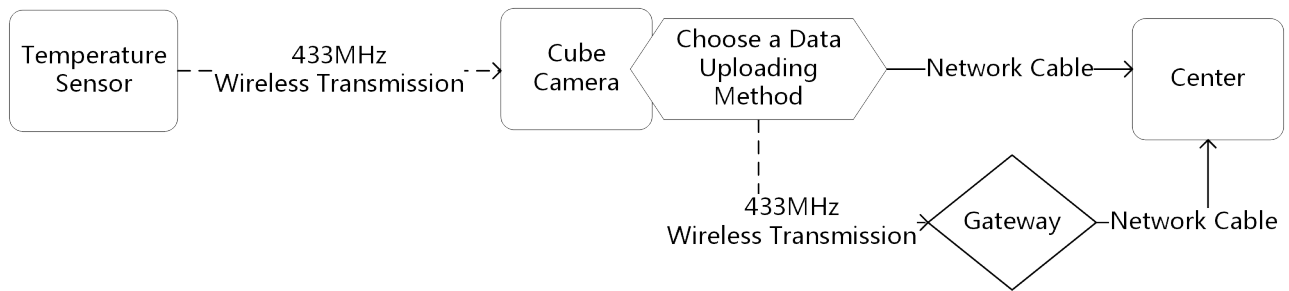




Figure 1-1 Temperature Data Transmission among sensors, Cube Camera, and Center

Table 1-1 Settings for Temperature Data Transmission

Data Transmission	Main Settings
From External Temperature Sensors to Thermographic Cube Camera	<ol style="list-style-type: none"> <li>1. Install sensors and the device. Refer to the installation guide of the sensors and the device.</li> </ol> <p> <b>Note</b> The distance between a sensor and a device should be within the 433MHz transmission distance limitation.</p> <ol style="list-style-type: none"> <li>2. Activate and log in to the device. See <a href="#"><i>Device Activation and Accessing</i></a> for instructions.</li> <li>3. Enable 433MHz data transmission on device. See <a href="#"><i>Set 433 MHz Transmission</i></a> for instructions.</li> <li>4. Connect temperature sensor to device. See <a href="#"><i>Connect Temperature Sensors to Device</i></a> for instructions.</li> <li>5. Set alarm rules for each temperature detector. See <a href="#"><i>Set External Temperature Sensor</i></a> for instructions.</li> </ol>
From Thermographic Cube Camera to Center (Wireless Way)	<ol style="list-style-type: none"> <li>1. Enable 433MHz data transmission on device. See <a href="#"><i>Set 433 MHz Transmission</i></a> for instructions.</li> <li>2. Set up the gateway to connect the device to a network. See the manual of your gateway for instructions.</li> </ol> <p> <b>Note</b> The gateway should support 433MHz transmission.</p> <ol style="list-style-type: none"> <li>3. Set the temperature alarm <b>Transmission Mode</b> to <b>433 Wireless Network Transmission</b> at <b>Configuration &gt; Temperature Measurement &gt; Alarm Settings</b> . See <a href="#"><i>Upload Temperature Alarm to Center</i></a> for instructions.</li> <li>4. Add the device to the center client (iVMS-4200). See the user manual of the client software for instructions.</li> </ol>

Data Transmission	Main Settings
	Access <a href="https://www.hikmicrotech.com/en/download/5">https://www.hikmicrotech.com/en/download/5</a> to get iVMS-4200 software.
From Thermographic Cube Camera to Center (Wired Way)	<ol style="list-style-type: none"><li>1. Connect the device to network with network cable.</li><li>2. Add the device to the center client (iVMS-4200). See the user manual of the client software for instructions.</li></ol> Access <a href="https://www.hikmicrotech.com/en/download/5">https://www.hikmicrotech.com/en/download/5</a> to get iVMS-4200 software.



## 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 <https://www.hikmicrotech.com/en/download/5> 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+ Microsoft Edge 79.0.309+	Click  <b>Download Plug-in</b> to download and install plug-in. Go to <b>Configuration &gt; Network &gt; Advanced Settings &gt; Network Service</b> to enable WebSocket or WebSockets for normal view

Operating System	Web Browser	Operation
		if 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 &gt; Network &gt; Advanced Settings &gt; 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.

### 2.3.3 Security Reinforcement

Security reinforce is a solution to enhance network security. With the function enabled, risky functions, protocols, ports of the device are disabled and more secured alternative functions, protocols and ports are enabled.

Go to **Configuration > System > Security > Advanced Security** . Check **Security Reinforcement**, and click **Save**.

## Chapter 3 Temperature Measurement

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

### 3.1 Notice

This part introduces the notices of configuring temperature measurement function.

- The target surface should be as vertical to the optical axis as possible. It is recommended that the angle of oblique image plane should be less than 45°.
- The target image pixels should be more than  $5 \times 5$ .
- Please select line thermography or area thermography for a certain area temperature measurement. The point thermography is not recommended in case of deviation occurred during device movement to affect the accuracy of temperature measurement.

### 3.2 Thermometry Flow Chart

This part introduces the process of configuring temperature measurement.

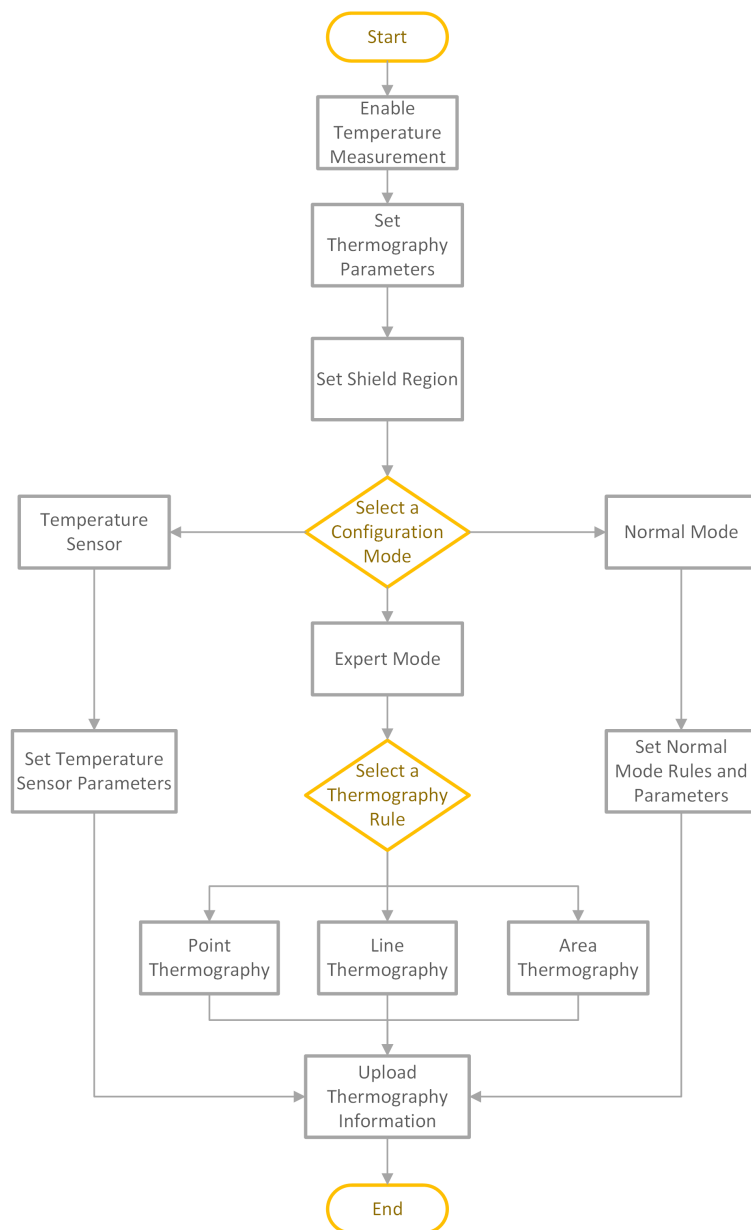


Figure 3-1 Thermometry Flow Chart

## 3.3 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 **X** to delete it.
6. Click **Save**.

### 3.4 Automatic Thermography

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

#### 3.4.1 Set Thermometry Parameters

Configure the parameters of temperature measurement.

##### Steps

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

##### Display Temperature Info.

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

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

2. Click **Save**.

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

##### Enable Temperature Measurement

Check to enable temperature measurement function.

##### Enable Color-Temperature

Check to display Temperature-Color Ruler in live view.

##### Display Temperature Info. on Stream

Check to display temperature information on the stream.

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

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

##### Position of Thermometry Info

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

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

##### Unit

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

## **Temperature Range**

Select the temperature measurement range.

## **Display Pixel-to-Pixel Thermometry Data on Stream**

Add and save real-time pixel-to-pixel thermometry data to stream. The function requires higher network bandwidth.

## **Pixel-to-Pixel Thermometry Data Refresh Interval**

It means the refresh interval of thermometry data added to the stream.

## **Optical Transmissivity**

Set the optical transmissivity of external optical material (e.g.: germanium window) to improve the temperature measuring accuracy.

## **Calibration Coefficient**

Check to enable it and set the value of calibration coefficient to get the temperature of the external window or optical material automatically. The setting range is 0 to 30.



### **Note**

You can get the setting value from SDK software.

---

## **External Optics/Window Correction**

Set the temperature of the external window or optical material (e.g.: germanium window) to correct the measured temperature.

## **Version**

View the version of current algorithm.

## **Calibration File Version**

View the version of calibration file.

## **Alarm Interval**

Set the time interval of alarms.

## **Display Rule Info. on Alarm Picture**

Select the rule information to be added on the alarm capture.

## **Alarm Mode**

Select the desired alarm mode. In temperature measurement alarm mode, the device outputs alarm if the detected temperature is higher than the alarm threshold. In interval temperature measurement alarm mode, the device outputs alarm if the detected temperature is within the set temperature range.

## **Normal Rule Color**

If you select interval temperature measurement alarm as the alarm mode, you can set the color for normal rules.



4. Click **Save**.

## 3.4.2 Set Normal Mode

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

### Steps

1. Go to **Configuration > Temperature Measurement > Basic Settings** , and check **Enable Temperature Measurement**.
2. Refer to ***Set Thermometry Parameters*** to set the parameters.
3. Go to **Configuration > Temperature Measurement > Advanced Settings** , and select **Normal**.
4. Configure the parameters of normal mode.
  - 1) Configure the parameters in **Temperature Measurement Alarm Mode**



### Note

Select **Alarm Mode** as **Temperature Measurement Alarm** first in basic settings.

---

### Emissivity

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

### Distance

The distance between the target and the device.

### Pre-Alarm Temperature

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

### Alarm Temperature

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

### Pre-Alarm Output and Alarm Output

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

### Temperature Sudden Change Alarm

When the temperature change exceeds the set sudden change alarm value within the set cycle, the camera triggers an alarm.

- 2) Configure the parameters in **Interval Temperature Measurement Alarm Mode**



### Note

Select **Alarm Mode** as **Interval Temperature Measurement Alarm** first in basic settings.

---

### Emissivity

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

### Distance

The distance between the target and the device.

### Alarm Rule

Select the alarm rule for interval temperature measurement.

### Alarm Type

If you select **Temperature Range**, the device triggers an alarm when the highest temperature in the scene is lower than the max. temperature, or when the lowest temperature in the scene is not lower than the min. temperature. If you select **Out of Temperature Range**, the device triggers an alarm when the highest temperature in the scene is higher than the max. temperature, or when the lowest temperature in the scene is not higher than the min. temperature.

### Name

Edit the interval name.

### Temperature Range

The device outputs an alarm if the detected temperature is within the set temperature range.

### Alarm Rule Color

Set the rule color in alarm status.

### Alarm Output

Select the alarm output channel.

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

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

---



### Note

- The function varies according to different camera models.
  - Go to **Image > VCA Rules Display** to adjust the fonts size and the temperature colour of normal, alarm and pre-alarm.
- 

### 3.4.3 Set Expert Mode

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

#### Steps

1. Go to **Configuration > Temperature Measurement > Basic Settings**, check **Enable Temperature Measurement**.
2. Refer to ***Set Thermometry Parameters*** to set the parameters.

3. Go to **Configuration > Temperature Measurement > Advanced Settings**, select **Expert**.
4. Select and enable the temperature measurement rules. Please refer to **Set Thermography Rule** for setting the rule.
5. **Optional:** Click **Area's Temperature Comparison** to set the alarm rules and the temperature.
6. Refer to **Set Arming Schedule** for setting scheduled time. Refer to **Linkage Method Settings** for setting linkage method.
7. Click **Save**.

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

---



### Note

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

---

### 3.4.4 Set Thermography Rule

#### Steps

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

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

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

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

3. Configure the temperature measurement parameters.

#### Emissivity


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

#### Distance

The distance between the target and the device.

#### Reflective Temperature

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

4. Click , and refer to **Set Temperature Measurement in Expert Mode** or **Set Interval Temperature Measurement in Expert Mode** to set the Alarm Rule.
5. You can shield certain area from being detected. Refer to **Set Shielded Region** for detailed settings.
6. Click **Save**.

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

### Point Thermography

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

#### Steps

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

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

### Line Thermography

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

#### Steps

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

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

### Area Thermography

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

#### Steps

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

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

## Set Temperature Measurement in Expert Mode

In temperature measurement alarm mode, the device outputs alarm if the detected temperature is higher than the threshold value.

### Before You Start

Select **Alarm Mode** as **Temperature Measurement Alarm** first in basic settings.

### Steps

1. Set the parameters.

#### Alarm Temperature and Pre-Alarm Temperature

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

#### Filtering Time

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

#### Tolerance Temperature

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

#### Area's Temperature Comparison

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

#### Temperature Sudden Change Alarm

**Temperature Sudden Increase** and **OFF** are selectable. When the temperature change value in the drawn area exceeds the set alarm threshold, the device triggers an alarm.

#### Cycle

Set the recording period of the temperature change.

#### Sudden Change Alarm Value

Set the temperature change alarm threshold for the rule. When the difference between the max. temperature and the min. temperature in the recording cycle exceeds the set alarm value, the device triggers an alarm.

2. Save the settings.

## Set Interval Temperature Measurement in Expert Mode

In interval temperature measurement alarm mode, the device will output alarm when the detected temperature triggers the set rule.

### Before You Start

Select **Alarm Mode** as **Interval Temperature Measurement Alarm** first in basic settings.

### Steps

1. Select the alarm rule for interval temperature measurement.
2. Edit the interval name.
3. Select an **Alarm Rule** and **Alarm Type**.
4. Set the temperature range.

---

#### Note

If you select Temperature Range, the device triggers an alarm when the highest temperature in the scene is lower than the max. temperature, or when the lowest temperature in the scene is not lower than the min. temperature. If you select Out of Temperature Range, the device triggers an alarm when the highest temperature in the scene is higher than the max. temperature, or when the lowest temperature in the scene is not higher than the min. temperature.

5. Set the rule color in alarm status.
6. Select the alarm output channel.

---

#### Note

The function varies according to different models.

---

## 3.5 External Temperature Sensor

The device can receive the temperature and alarm information detected by the external temperature sensors.

To receive data from temperature sensors, you should set:

- **Set 433 MHz Transmission**
- **Connect Temperature Sensors to Device**
- **Set External Temperature Sensor**

### 3.5.1 Set 433 MHz Transmission

You can enable the 433 wireless network transmission function to receive and send the thermometry information through the 433 module.

### Steps

1. Go to **Configuration > 433 Module Configuration > Basic Settings** .
2. Check **Enable 433 Wireless Network Transmission**.
3. Confirm the baud rate. The fixed baud rate is 10 k.
4. Set the **Channel Center Frequency**.
5. Select a protocol type.
6. **Optional:** Enter the device address if you select modbus-RTU.
7. Click **Save**.


### 3.5.2 Set External Temperature Sensor

Set alarm rules for the configured sensors. The sensors can measure the temperature in the set area and trigger an alarm if there is any exception.

#### Before You Start

- Enable 433 module configuration. See [\*Set 433 MHz Transmission\*](#) for reference.
- Complete the sensor configuration. See [\*Connect Temperature Sensors to Device\*](#) for reference.

### Steps

1. Go to **Temperature Measurement > Temperature Sensor > Sensor** .
2. Check to select the sensor to be configured.
3. Click  and set the **Alarm Rule**.

#### Alarm Temperature and Pre-Alarm Temperature

Set the alarm temperature and pre-alarm temperature for the sensor. E.g., if you set the **Pre-Alarm Temperature** to **50 °C**, and set the **Alarm Temperature** to **55 °C**, the device triggers pre-alarm actions when its temperature is higher than 50 °C, triggers alarms actions when the temperature is higher than 55 °C.

#### Temperature Sudden Change Alarm


**Temperature Sudden Increase** and **OFF** are selectable. When the temperature change value in the detected area exceeds the set alarm threshold, the device triggers an alarm.

#### Cycle

Set the recording period of the temperature change.

#### Sudden Change Alarm Value

Set the temperature change alarm threshold for the rule. When the difference between the max. temperature and the min. temperature in the recording cycle exceeds the set alarm value, the device triggers an alarm.

4. Click **OK**.
5. Click  , and check the sensor ID as needed to copy the rule to it.

6. Go to **Linkage Method > Arming Schedule** to set the arming schedule for the alarm. See ***Set Arming Schedule*** for reference.
7. Set the linkage method for the alarm. See ***Linkage Method Settings*** for reference.

### 3.5.3 Connect Temperature Sensors to Device

Before starting 433 wireless network transmission, you should configure temperature sensors, and connect the sensors to the device.

#### Before You Start

Go to **Configuration > 433 Module Configuration > Basic Settings** to enable 433 wireless network transmission.

#### Steps

1. Go to **Configuration > 433 Module Configuration > Sensor**.
2. Select the **Type** of the sensor.
3. Enter the **Identification Code**.
4. Enter the **Name** for the sensor.
5. Click **Save**.



#### Note

Please use the sensor models recommended by the manufacturer.

---


#### Result

The configured sensors will be listed in **Temperature Measurement > Temperature Sensor > Sensor**.

## 3.6 Manual Thermography

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

#### Steps

1. Go to **Configuration > Local** and select **Display Temperature Info.** as **Yes**.
2. Go to **Configuration > Temperature Measurement > Basic Settings**.
3. Check **Enable Temperature Measurement**.
4. Click **Save**.
5. Go to live view interface and select thermal channel, click . Click any position on the interface to show the real temperature.



### 3.7 Upload Temperature Alarm to Center

The device can upload thermography information to the surveillance center through 433 wireless module.

#### Before You Start

- Enable the temperature measurement function in **Configuration > Temperature Measurement > Basic Settings**.
- Complete the 433 module configuration. See *Set 433 MHz Transmission* for reference.

#### Steps

1. Go to **Configuration > Temperature Measurement > Alarm Setting**.
2. Confirm that the transmission mode is **433 Wireless Network Transmission**.
3. Configure the parameters for the alarm setting.

##### Normal Interval

The interval of information upload.

##### Display Rule Info. on Alarm

If you select **All Rules**, the uploaded pictures contain all rule information configured in expert mode. If you select **No**, the uploaded pictures do not contain any rule information.

##### Upload Picture

If you select **Upload All**, the device uploads the thermography information and captured thermal pictures at the same time. If you select **No**, the device does not upload any pictures.

4. Click **Save**.

### 3.8 Integration

Users can obtain the pixel-to-pixel thermometry data of the device through the persistent connection management. The data can be used for secondary development and integration.

#### 3.8.1 Pixel-to-Pixel Thermometry

Users can configure general thermometry and data upload parameters to obtain pixel-to-pixel thermometry data, thermometry rule information, and pictures. This function can be used for secondary integration.

#### Steps

1. Go to **Configuration > Temperature Measurement > Integration > Pixel-to-Pixel Thermometry**.

## 2. Configure the parameters.

### Emissivity

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

### Distance

The distance between the target and the device.

### Reflective Temperature

If there is any object reflecting to the target, e.g., a mirror, enter the background temperature value/the reflecting object's temperature value. If not, skip the settings.

### Data Length

It stands for the data length of the detected temperature information of every pixel. 2 means the temperature information type of every pixel is "short", and 4 means the type is "float".

### Max. Frame Rate

The max. frame rate of upload stream for further integration. High frame rate requires more upload bandwidth.

### Refreshing Interval of Temperature Mapping Table

It stands for the frame interval of refreshing the temperature mapping table. Temperature mapping table tells the relation between detected data and the temperature of a pixel. For example, if you set it as 50 (means every 50 frames), and the frame rate as 25 fps, then the table refreshes every 2 seconds, which also means the displayed temperature data refreshes every 2 seconds.

### Upload Thermal Picture

Check this function, then the thermal picture is uploaded together with the pixel-to-pixel thermometry data.



### Note

The parameters above such as Emissivity, Distance, Reflective Temperature, etc. are only applied in integration, which will not affect the configuration in thermometry parameters and rules.

---

## 3. Click **Save**.

### 3.8.2 Persistent Connection Management

This function shows the maximum connections that the device supported for real-time pixel-to-pixel thermometry data uploading and real-time rule thermometry data uploading, and the currently established connections and their parameters. The real-time pixel-to-pixel thermometry data is uploaded using SDK or RTSP protocol, and the real-time rule thermometry data is uploaded using SDK or ISAPI protocol. The real-time rule thermometry data uploaded includes the thermometry rule and the thermometry result.

### Steps

1. Go to **Configuration > Temperature Measurement > Integration > Persistent Connection Management**.
2. Click **Refresh** to obtain the latest connection status of the device.

## 3.9 Collect Diagnosis Information

Collect the temperature measurement original data of the regular frame and superimpose it in the stream to facilitate the export and analysis of subsequent data.

### Steps

1. Access **Configuration > System > System Maintenance > Diagnosis Information Collection**.
2. Check **Add Original Data on Capture** to overlay the raw device data on the temperature alarm capture.
3. Check **Add Original Data on Stream** to overlay the raw data in the corresponding video streams which can subsequently be downloaded along with the video files through the playback download function.
4. Select **Original Data Overlay Rule**.

#### Temperature Measurement Frame

All the raw data used to temperature measurement frame is superimposed on the stream.

#### Temperature Measurement Alarm Frame

The raw data of the frame that triggered the temperature measurement alarm will be superimposed on the stream.

#### By Temperature Range

When the maximum temperature value is detected to exceed the set temperature range, the raw data of that frame will be superimposed in the stream.

#### By Refresh Interval

The raw data of the original data refresh frame is superimposed on the stream.

5. Set parameters.

#### Temperature Range

When the temperature value is out of temperature range, the raw data in the frame will be superimposed in the stream.

#### Data Refresh Interval

Raw data refresh interval.

6. Click **Save**.

## 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 Video Tampering Alarm

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

#### Steps

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

**Stop Drawing**    Finish drawing.

**Clear All**        Delete all the drawn areas.

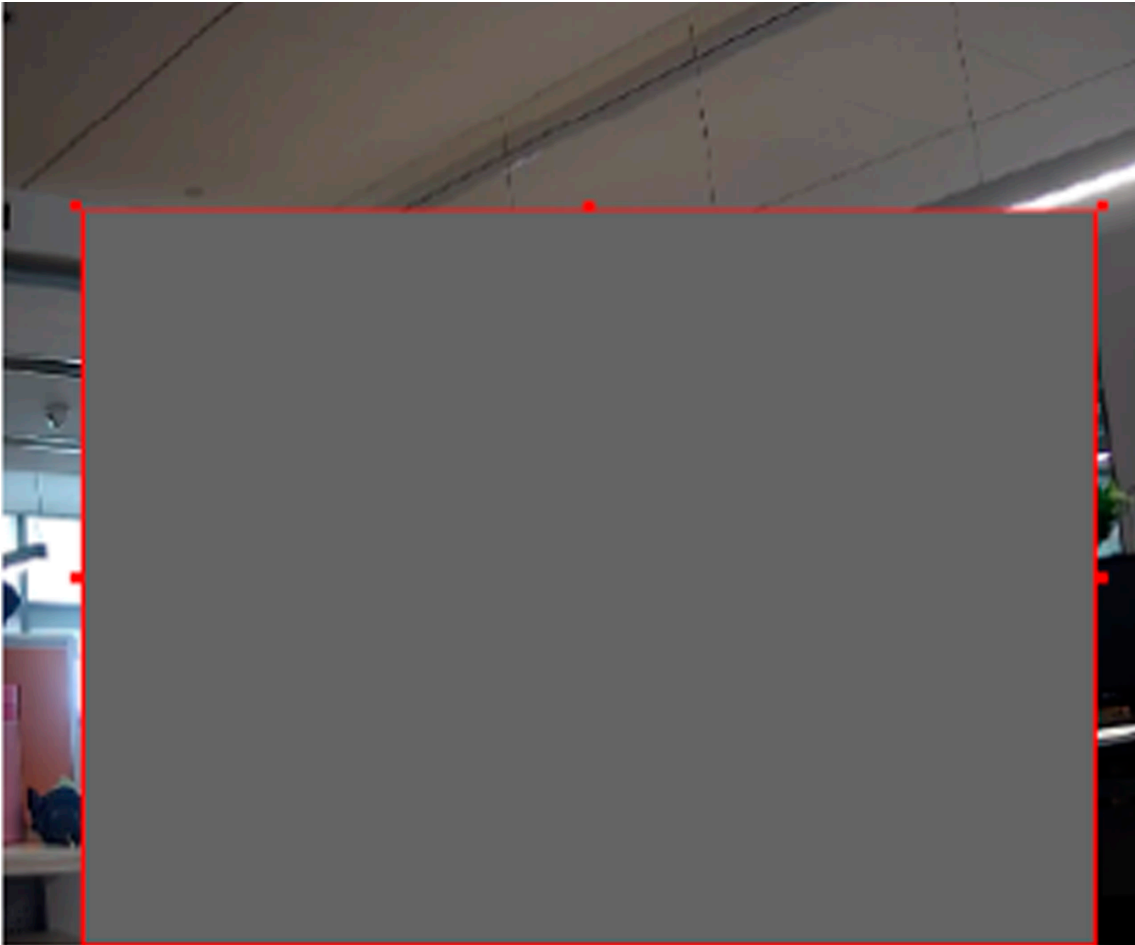


Figure 4-1 Set Video Tampering Area

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

## 4.2 Set Exception Alarm

Exception such as HDD full can trigger the device to take corresponding action.

### Steps

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

HDD Full	The HDD storage is full.
HDD Error	Error occurs in HDD.
Illegal Login	Incorrect user name or password is entered.

**Calibration File Exception** The calibration file is modified. The temperature accuracy may be affected.

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

4. Click **Save**.

## 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.



#### Note

Up to 8 periods can be configured for one day.

---

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

### 5.2 Linkage Method Settings

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

#### 5.2.1 Notify Surveillance Center

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

#### 5.2.2 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

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

### Before You Start

Set the DNS server before using the Email function. Go to **Configuration > Network > Basic Settings > TCP/IP** for DNS settings.

### Steps

1. Go to email settings page: **Configuration > Network > Advanced Settings > Email** .
  2. Set email parameters.
    - 1) Input the sender's email information, including the **Sender's Address**, **SMTP Server**, and **SMTP Port**.
    - 2) **Optional**: If your email server requires authentication, check **Authentication** and input your user name and password to log in to the server.
    - 3) Set the **E-mail Encryption**.
      - When you select **SSL** or **TLS**, and disable **STARTTLS**, emails are sent after encrypted by SSL or TLS. The SMTP port should be set as 465.
      - When you select **SSL** or **TLS** and **Enable STARTTLS**, emails are sent after encrypted by STARTTLS, and the SMTP port should be set as 25.
- 
-  **Note**

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

## 5.2.3 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.



## 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.





#### 6.1.1 Select the Third-Party Plug-in

When the live view cannot display via certain browsers, you can change the plug-in for live view according to the browser.

##### Steps

1. Click **Live View**.
2. Click  to select the plug-in.

#### 6.1.2 Window Proportion



-  refers to the window size is 16 : 9.
-  refers to the window size is 4 : 3.
-  refers to original window size.
-  refers to self-adaptive window size.

#### 6.1.3 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**.

#### 6.1.4 Enable and Disable Live View


This function is used to quickly enable or disable live view of the channel.

- Click  to start the live view.
- Click  to stop the live view.


#### 6.1.5 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.


## 6.1.6 Online Capture

Click  to capture the thermal image (Name: Prefix\_Device IP\_Time.jpeg) with raw data, thermometry information, etc.

## 6.2 Quick Set Live View

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

### Steps

1. Click  to show quick setup page.
2. Set display settings, OSD, video/audio and VCA resource parameters.
  - For display settings, see *[Display Settings](#)*.
  - For OSD settings, see *[OSD](#)*.
  - For audio and video settings, see *[Video and Image Settings](#)*.
  - For VCA settings, see *[Temperature Measurement](#)*.



### Note

The function is only supported by certain models.

---

## 6.3 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.

3. Click OK.

## Chapter 7 Video and Image Settings

This part introduces the configuration of video/audio and image 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** .

#### 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 audio) that should be contained in the stream.

##### Video

Only video content is contained in the 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.

## 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 Set ROI

ROI (Region of Interest) encoding helps to assigns 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 **Stream Type**.
4. Select **Region No.** in **Fixed Region** to draw ROI region.
  - 1) Click **Drawing**.
  - 2) Click and drag the mouse on the view screen to draw the fixed region.
  - 3) Click **Stop Drawing**.

---

### **Note**

Select the fixed region that needs to be adjusted and drag the mouse to adjust its position.

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

---

### **Note**

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

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

## 7.1.10 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.

## 7.1.11 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** .

Click **Default** to restore settings.

### 7.2.1 Image Adjustment (Thermal Channel)

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

#### Background Correction

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

#### Manual Correction

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



#### Note

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

---

#### Thermal AGC Mode

**Linear** mode is for scene with low temperature difference and the target is not obvious. It can improve image contrast and enhance image. E.g. the bird in forest.

### 7.2.2 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.



### 7.2.3 Set Palette

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

#### Steps

1. Go to **Configuration > Image > Display Settings** .
2. Select a palette mode in **Image Enhancement** according to your need.

#### Result

The live view displays the image with palette.

### 7.2.4 Set Target Enhancement

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. Click **Image Enhancement**, select **Palette** as **White Hot** or **Black Hot**.
3. 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.

4. Click **Save**.

### 7.2.5 Set Palette Range

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

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

## Auto

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

## Manual

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

### 7.2.6 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.

### 7.2.7 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.

---

### 7.2.8 Rotate

When enabled, the live view will rotate 90 ° counterclockwise. For example, 1280 × 720 is rotated to 720 × 1280.

Enabling this function can change the effective range of monitoring in the vertical direction.

### 7.2.9 Digital Zoom

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

## 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.

### Character Set

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

### Displayed Information

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

### Text Overlay

Set customized overlay text on image.

### OSD Parameters

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

## 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. Check **Enable Privacy Mask**.
3. Click **Draw Area**. Drag the mouse in the live view to draw a closed area.

<b>Drag the corners of the area</b>	Adjust the size of the area.
<b>Drag the area</b>	Adjust the position of the area.
<b>Click Clear All</b>	Clear all the areas you set.
4. Click **Stop Drawing**.
5. Click **Save**.

## 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. Click **Browse** to select a picture, and click **Upload**.  
The picture with a red rectangle will appear in live view after successfully uploading.
3. Check **Enable Picture Overlay**.
4. Drag the picture to adjust its position.
5. 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 manual mode.
3. Click the defective pixel on the image, then a cursor shows on the live view.
4. Click **Up**, **Down**, **Left**, **Right** to adjust the cursor position to the defective pixel position.
5. 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.
- This function is only supported by certain camera models.

- 
6. **Optional:** Click  to cancel defective pixel correction.

## 7.7 VCA Rule Display Settings

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

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

## Chapter 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. 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.

#### Server Address and Port

The FTP server address and corresponding port.

#### User Name and Password

The FTP user should have the permission to upload pictures.

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

#### Directory Structure

The saving path of snapshots in the FTP server.

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

### 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

---



### Caution

If cloud storage is enabled, the pictures are stored in the cloud storage server preferentially.

---

1. Go to **Configuration > Storage > Storage Management > Cloud Storage** .
2. Check **Enable Cloud Storage**.
3. Set basic parameters.

<b>Protocol Version</b>	The protocol version of the cloud storage server.
<b>Server IP</b>	The IP address of the cloud storage server. It supports IPv4 address.
<b>Serve Port</b>	The port of the cloud storage server. 6001 is the default port and you are not recommended to edit it.
<b>User Name and Password</b>	The user name and password of the cloud storage server.
<b>Picture Storage Pool ID</b>	The ID of the picture storage region in the cloud storage server. 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

1. Go to **Configuration > Storage > Schedule Settings > Record Schedule** .
2. Check **Enable**.
3. Select a record type.

---

## Note

The record type varies according to different models.

---

### Continuous

The video will be recorded continuously according to the schedule.

### Motion

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

### Alarm

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

### Motion | Alarm

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

### Motion & Alarm

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

### Event

The video is recorded when configured event is detected.

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

### Overwrite

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

### Pre-record

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

### Post-record

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

### Stream Type

Select the stream type for recording.

---

## Note

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



---

6. 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  in the live view interface 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. Set search condition and click **Search**.  
The matched video files showed on the timing bar.
3. 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.

- 
4. 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. Set search condition and click **Search**.  
The matched pictures showed in the file list.
3. 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 > Network > Basic Settings > TCP/IP** for parameter settings.

#### NIC Type

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

#### IPv4

Two IPv4 modes are available.

##### DHCP

The device automatically gets the IPv4 parameters from the network if you check **DHCP**. The device IP address is changed after enabling the function. You can use HIKMICRO Studio 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.

## Dynamic Domain Name

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



### Note

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

---

## 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.

### Enhanced SDK Service Port

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

### WebSocket Port

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

### WebSockets Port

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

### ModbusTCP

It refers to the protocol through which the device transmits data, such as the thermometry data.



#### 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.

### 9.3.3 Set Port Mapping on Router

The following settings are for a certain router. The settings vary depending on different models of routers.

#### Steps

1. Select the **WAN Connection Type**.
2. Set the **IP Address**, **Subnet Mask** and other network parameters of the router.
3. Go to **Forwarding > Virtual Servers**, and input the **Port Number** and **IP Address**.
4. Click **Save**.

#### Example

When the cameras are connected to the same router, you can configure the ports of a camera as 80, 8000, and 554 with IP address 192.168.1.23, and the ports of another camera as 81, 8001, 555, 8201 with IP 192.168.1.24.

**108M Wireless Router**  
Model No.:  
TL-WR641G / TL-WR642G

- Status
- Quick Setup
- Basic Settings ---
- + Network
- + Wireless
- Advanced Settings ---
- + DHCP
- Forwarding
  - Virtual Servers
  - Port Triggering
  - DMZ
  - UPnP
- + Security
  - Static Routing
  - Dynamic DNS
- Maintenance ---
- + System Tools

## Virtual Servers

ID	Service Port	IP Address	Protocol	Enable
1	80	192.168.10.23	ALL	<input checked="" type="checkbox"/>
2	8000	192.168.10.23	ALL	<input checked="" type="checkbox"/>
3	554	192.168.10.23	ALL	<input checked="" type="checkbox"/>
4	8200	192.168.10.23	ALL	<input checked="" type="checkbox"/>
5	81	192.168.10.24	ALL	<input checked="" type="checkbox"/>
6	8001	192.168.10.24	ALL	<input checked="" type="checkbox"/>
7	555	192.168.10.24	ALL	<input checked="" type="checkbox"/>
8	8201	192.168.10.24	ALL	<input checked="" type="checkbox"/>

Common Service Port: DNS(53) Copy to ID 1

Previous
Next
Clear All
Save

Figure 9-1 Port Mapping on Router

## Note

The port of the network camera cannot conflict with other ports. For example, some web management port of the router is 80. Change the camera port if it is the same as the management port.

## 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.



## 9.5 SNMP

You can set the SNMP function to get camera status, parameters and alarm related information, and manage the camera remotely when it is connected to the network.

Before setting the SNMP, download the SNMP software and receive the camera information via SNMP port. Set the Trap Address, and the camera can send the alarm event and exception messages to the surveillance center.

The SNMP version you select should be the same as that of the SNMP software.

Use the different version according to the security level you required.

- SNMP v1 provides no security
- SNMP v2 requires password for access.
- SNMP v3 provides encryption. if you use the third version, HTTPS protocol must be enabled. To lower the risk of information leakage, you are suggested to enable SNMP v3 instead of SNMP v1 or v2.



### Note

---

The settings of the SNMP software should be the same as the settings you configure here.

---



### Note

A reboot is required for the settings to take effect.

---

## 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 Set Alarm Server

The device can send alarms to destination IP address or host name through HTTP, HTTPS, or ISUP. 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. Please take the actual product for reference.
- 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**.

### 9.8 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.

## 9.9 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. Select an authentication mode.
  - If you select **Digest**, the device only supports digest authentication.
  - If you select **Digest&ws-username token**, the device supports digest authentication or ws-username token authentication. You can check **Time Verification** to verify the client time based on your needs.
4. 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.
5. Click **Save**.
6. **Optional:** Repeat the steps above to add more Open Network Video Interface users.

## 9.10 Set Network Service

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

### Steps



#### Note

This function varies according to different models.

---

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

#### WebSocket & WebSockets

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

If the device uses HTTP, enable WebSocket.

If the device uses HTTPS, enable WebSockets.

#### TLS (Transport Layer Security)

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

3. Click **Save**.

## 9.11 Modbus Communication

During communicating with Modbus protocol, the Camera can function as the main or the subordinate for transmitting temperature measurement and temperature measurement alarm data, or responding to temperature measurement parameter configuration requests from the main.

Please select the device mode and configure the communication rules and parameters according to the demand to ensure the security of data transmission under the premise of satisfying the data access of the device.

Go to **Configuration > Network > Advanced Configuration > Modbus** , to configure the Modbus.

### 9.11.1 Set Modbus Main Mode

Configure the device as the main server that actively uploads data to the subordinate according to set rules, without sending requests.

#### Steps

1. Select the **Device Mode** as **Main**.

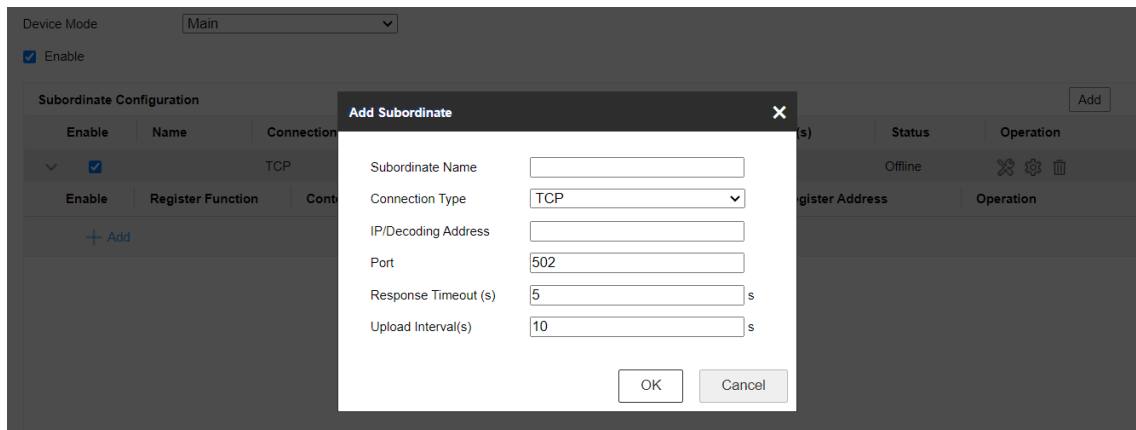


Figure 9-2 Main Mode Configuration

2. Check to enable the function of transmitting data via Modbus.
3. Click **Add** to configure the transmission parameters between the device and the subordinate.

#### Subordinate Name

Customized subordinate for distinguishing between different subordinates.

#### Connection type

---

## Note

Only when **System > System Configuration > RS-485** is selected as main mode, the RS-485 connection type can be supported.

---

## TCP

When connecting the device and the subordinate via the RJ45 interface, the TCP connection type can be selected. Multiple connections can be implemented through the TCP type, but the IP/decoding address and port of the TCP connection cannot be duplicated.

## RS-485

Before selecting an RS-485 connection, make sure that the connection between the device and the subordinate has been established through the RS-485 connector on the body. And only 1 RS-485 connection can be supported.

## Response Timeout(s)

When the response timeout occurs, the device displays the error code **11**, then it will resend the data, and when the response timeout occurs for three consecutive times, it will discard the current data and send the next data.

## Upload Interval(s)

The time interval during the device uploads data to the subordinate.

4. Click **OK** to view the status.

5. Click  to refresh the status.

---

## Note

- If the connection status displays **online**, the device is connected to the subordinate normally; if it displays **offline**, the device is disconnected from the subordinate, which may be caused by the subordinate not being online. If the status shows **Error**, refer to the contents of the error code description below to diagnose the connection problem.
  - Click **Edit** or **Delete** to re-edit the subordinate parameters or delete the added subordinate.
- 

6. Configure the contents to be uploaded to the registers of subordinate.

1) Click **Add**.

2) Check the contents to be uploaded.

3) Select the Rule ID to be uploaded, and the device uploads the temperature measurement information corresponding to the expert temperature measurement rule.

4) Enter the register starting address and register ending address.

---

## Note

In a single subordinate configuration, all register addresses cannot be duplicated or conflicted.

---

5) Click **OK**.

---

**Register Configuration**
✕

*i* There are 123 register addresses, and the number in parentheses indicates the number of register addresses...

Content to Upload      ☒ Max. Temperature...   ☐ Min. Temperature...   ☐ Average Temperature...

☒ Position of Max. Temp...   ☐ Position of Min. Temp...   ☐ Alarm Status(1)

No.	Content	Sorting
1	Max. Temperature	↑ ↓
2	Position of Max. Temperature	↑ ↓

Rule ID                       ~

Register Starting Address    ✔

Number of Occupied Addresses   2\*3=6

Register Ending Address    i

**Figure 9-3 Register Configuration**

7. Click **Save**.

## 9.11.2 Set Modbus Subordinate Mode

Configure the device as the subordinate server, the main can read the temperature measurement data of the device or write the temperature measurement parameters of the device. The form of authorized access can improve data communication security.

### Steps



#### Note

You can set the Modbus TCP port, go to **Configuration > Network > Basic Settings > Port**.

1. Go to **Configuration > Network > Advanced Settings > Modbus**.
2. Select Modbus TCP mode.

#### Device Mode

The device is set as **subordinate**, which means that the device operates as a Modbus server processing the request from the client.

#### Register Mode

In **Read Only**, the client can only read all the register data. In **Read/Write**, the client can read while configure the device using the Modbus TCP protocol.

3. Check **Enable Authorized IP Addresses** and click **Add** to add IP addresses that are allowed to access to the device.



### Note

With regard to the network security risk, it is recommended to limit permission only to trusted IP addresses.

---

### 9.11.3 Modbus Error Code Description

If communication of Modbus is abnormal, an error code will be returned. Please refer to the following table to check the meaning of the error code to help troubleshoot Modbus communication problems.

**Table 9-1 Modbus Error Code Description**

Error Code	Name	Description
01	Illegal Function	The function code received in the query is not an allowable action for the server. This may be because the function code is only applicable to newer devices, and was not implemented in the unit selected. It could also indicate that the server is in the wrong state to process a request of this type, for example because it is unconfigured and is being asked to return register values.
02	Illegal Data Address	The data address received in the query is not an allowable address for the server. More specifically, the combination of reference number and transfer length is invalid. For a controller with 100 registers, the PDU addresses the first register as 0, and the last one as 99. If a request is submitted with a starting register address of 96 and a quantity of registers of 4, then this request will successfully operate (address-wise at least) on registers 96, 97, 98, 99. If a request is submitted with a starting register address of 96 and a quantity of registers of 5, then this request will fail with Exception Code 0x02 "Illegal Data Address" since it attempts to operate on registers 96, 97, 98, 99 and 100, and there is no register with address 100.
03	Illegal Data Value	A value contained in the query data field is not an allowable value for server. This indicates a fault in

Error Code	Name	Description
		the structure of the remainder of a complex request, such as that the implied length is incorrect. It specifically does NOT mean that a data item submitted for storage in a register has a value outside the expectation of the application program, since the Modbus protocol is unaware of the significance of any particular value of any particular register.
04	Server Device Failure	An unrecoverable error occurred while the server was attempting to perform the requested action.
05	Acknowledge	Specialized use in conjunction with programming commands. The server has accepted the request and is processing it, but a long duration of time will be required to do so. This response is returned to prevent a timeout error from occurring in the client. The client can next issue a Poll Program Complete message to determine if processing is completed.
06	Server Device Busy	Specialized use in conjunction with programming commands. The server is engaged in processing a long– duration program command. The client should retransmit the message later when the server is free.
08	Memory Parity Error	Specialized use in conjunction with function codes 20 and 21 and reference type 6, to indicate that the extended file area failed to pass a consistency check. The server attempted to read record file, but detected a parity error in the memory. The client can retry the request, but service may be required on the server device.
10	Gateway Path Unavailable	Specialized use in conjunction with gateways, indicates that the gateway was unable to allocate an intern communication path from the input port to the output port for processing the request. Usually means that the gateway is misconfigured or overload.
11	Gateway Target Device Failed to Response	Specialized use in conjunction with gateways, indicates that no response was obtained from the



Error Code	Name	Description
		target device. Usually means that device is not present on the network.

## 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.

When **Additional Temperature Diagnosis Information** is checked, there is another file for the temperature diagnosis data.

## 10.5 Reboot

You can restart 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.

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

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



### Note

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

---

## 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 restarts 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 eMMC Protection

It is to automatically stop the use of eMMC as a storage media when its health status is poor.



### Note

The eMMC protection is only supported by certain device models with an eMMC hardware.

---

Go to **Configuration > System > Maintenance > System Service** for the settings.

eMMC, short for embedded multimedia card, is an embedded non-volatile memory system. It is able to store the captured images or videos of the device.

The device monitors the eMMC health status and turns off the eMMC when its status is poor. Otherwise, using a worn-out eMMC may lead to device boot failure.

## 10.9 View Open Source Software License

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

## 10.10 Time and Date

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

### 10.10.1 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**.

## 10.10.2 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**.

## 10.10.3 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**.

## 10.11 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**.

## 10.12 Set RS-485

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

### Before You Start

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

### Steps

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

#### Device Mode

The main mode allows the device to actively upload data to subordinate. In subordinate mode, device responses the request from the main.



#### Note

Only one of the modes can be in effect at the same time.

---

#### CRC Response Transmission

Big-endian is an order in which the "big end" is stored first, at the lowest storage address. Little-endian is an order in which the "little end" is stored first.



#### Note

- You should keep the parameters of the device and the computer or terminal all the same.
  - If the **PTZ Protocol** is selected as **modbus-RTU** or **modbus-ASCII**, the temperature information can be transferred by RS-485 interface.
- 

3. Click **Save**.

## 10.13 Set Same Unit

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

### Steps

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

## 10.14 Security

You can improve system security by setting security parameters.

### 10.14.1 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.

---

### 10.14.2 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.

## 10.14.3 Set IP Address Filter

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

IP address refers to IPv4.

### Steps

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

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

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

4. Edit the IP address filter list.

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

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

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

5. Click **Save**.

## 10.14.4 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**.

## 10.14.5 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.

### Install Other Authorized Certificate

If you already has an authorized certificate (not created by the device), you can import it to the device directly.

#### Steps

1. Go to **Configuration > System > Security > Certificate Management** .
2. Click **Import**.
3. Input **Certificate ID**.



## Note

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

- 
4. Click **Browse** to select the certificate file.
  5. Select **Certificate and Key** and select a **Key Type** according to your certificate.

#### Independent Key

If your certificate has a independent key, select this option.  
Browse to select the private key and input the private-key password.

#### PKCS#12

If your certificate has the key in the same certificate file, select this option and input the password.

6. Click **OK**.

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

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

### Install Self-signed Request Certificate

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

## Before You Start

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

## Steps

1. Go to **Configuration > System > Security > Certificate Management**.
2. Select a self-signed certificate from the Server/Client Certificate list.
3. Click **Create Certificate Request**.
4. Input request information.
5. Click **OK**.  
The certificate request details are displayed in a pop-up window.
6. Copy the request content and save it as a request file.
7. Send the file to a trusted-third party for signature.
8. After receiving the certificated sent back from the third-party, install it to the device.
  - 1) Click **Import**.
  - 2) Input **Certificate ID**.



### Note

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

---

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

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

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

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

## Install CA Certificate

### Before You Start

Prepare a CA certificate in advance.

### Steps

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



### Note

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

---

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

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

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

### Enable Certificate Expiration Alarm

#### Steps

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

---

#### Note

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

- 
3. Click **Save**.

### 10.14.6 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**.

### 10.14.7 Create and Install Self-signed Certificate

#### Steps

1. Go to **Maintenance and Security > Security > Certificate Management**.

2. Click **Create Self-signed Certificate**.
3. Input certificate information.



### Note

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

---

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

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

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

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

### 10.14.8 Set IEEE 802.1X

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

Go to **Configuration > Network > Advanced Settings > 802.1X**, and enable the function. Set **Protocol** and **EAPOL Version** according to router information.

#### Protocol

EAP-TLS and EAP-MD5 are selectable

#### EAP-MD5

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

#### EAP-TLS

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

#### EAPOL Version

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

## 10.15 User and Account

### 10.15.1 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**.

## 10.15.2 Online Users

The information of users logging into the device is shown.

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

## Chapter 11 Appendix

### 11.1 Common Material Emissivity Reference

Material	Emissivity
Human Skin	0.98
Printed Curcuit 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



**HIKMICRO**

See the World in a New Way