

Thermal Presence Detector

User Manual

Legal Information

©2021 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
Danger	Indicates a hazardous situation which, if not avoided, will or could result in death or serious injury.
Caution	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
Note	Provides additional information to emphasize or supplement important points of the main text.

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 (16 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 45°C (-4°F to 113°F), and the operating humidity shall be 95% or less, no condensing.
- DO NOT expose the device to high electromagnetic radiation or dusty environments.
- DO NOT aim the lens at the sun or any other bright light.

- The equipment shall not be exposed to dripping or splashing and that no objects filled with liquids, such as vases, shall be placed on the equipment.
- No naked flame sources, such as lighted candles, should be placed on the equipment.
- Provide a surge suppressor at the inlet opening of the equipment under special conditions such as the mountain top, iron tower, and forest.
- Burned fingers when handling the parts with symbol . Wait one-half hour after switching off before handling the parts.

Emergency

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

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

Contents

Chapter 1 Overview 1
1.1 Introduction 1
1.2 Application 2
Chapter 2 Wi-Fi 3
2.1 Connect to Wi-Fi via Web Browser 3
Chapter 3 Device Activation and Accessing 5
3.1 Activate the Device via SADP 5
3.2 Activate the Device via Browser 5
3.3 Login 6
3.3.1 Plug-in Installation 6
3.3.2 Illegal Login Lock 7
Chapter 4 People Number Management 8
4.1 Set People Number Management Rule 8
Chapter 5 Temperature Measurement 10
5.1 Notice 10
5.2 Set Normal Mode 10
5.3 Set Thermography Parameters 11
5.4 VCA Rule Display Settings 12
5.5 Set Shielded Region 12
Chapter 6 Event and Alarm 13
6.1 Set Exception Alarm 13
Chapter 7 Arming Schedule and Alarm Linkage 14
7.1 Set Arming Schedule 14
7.2 Linkage Method Settings 14
7.2.1 Trigger Alarm Output 14
7.2.2 FTP/NAS/Memory Card Uploading 15

7.2.3 Send Email 16
7.2.4 Notify Surveillance Center 17
7.2.5 Trigger Recording 17
7.2.6 Set Audible Alarm Output 17
Chapter 8 Live View 18
8.1 Live View Parameters 18
8.1.1 Start and Stop Live View 18
8.1.2 Window Proportion 18
8.1.3 Live View Stream Type 18
8.1.4 Select the Third-Party Plug-in 18
8.1.5 Start Digital Zoom 18
8.2 Quick Set Live View 19
8.3 Set Transmission Parameters 19
Chapter 9 Video and Audio 21
9.1 Video Settings 21
9.1.1 Stream Type 21
9.1.2 Video Type 21
9.1.3 Resolution 21
9.1.4 Bitrate Type and Max. Bitrate 21
9.1.5 Video Quality 22
9.1.6 Frame Rate 22
9.1.7 Video Encoding 22
9.1.8 Smoothing 23
9.1.9 Display VCA Info 24
9.2 Display Settings 24
9.2.1 Image Adjustment 24
9.2.2 Image Adjustment (Thermal Channel) 24
9.2.3 DNR 25

9.2.4 Set Palette 25
9.2.5 DDE 25
9.2.6 Brightness Sudden Change 26
9.2.7 Mirror 26
9.3 OSD 26
9.4 Overlay Picture 26
Chapter 10 Video Recording and Picture Capture 28
10.1 Storage Settings 28
10.1.1 Set Memory Card 28
10.1.2 Set NAS 28
10.1.3 Set FTP 29
10.1.4 Set Cloud Storage 30
10.2 Video Recording 30
10.2.1 Record Automatically 30
10.2.2 Record Manually 32
10.2.3 Playback and Download Video 32
10.3 Capture Configuration 33
10.3.1 Capture Automatically 33
10.3.2 Capture Manually 33
10.3.3 View and Download Picture 33
Chapter 11 Network Settings 35
11.1 TCP/IP 35
11.1.1 Multicast Discovery 36
11.2 Change Wi-Fi Parameters 36
11.3 Port 37
11.4 Port Mapping 37
11.4.1 Set Auto Port Mapping 38
11.4.2 Set Manual Port Mapping 38

11.5 Multicast 38
11.6 SNMP 39
11.7 Access to Device via Domain Name 39
11.8 Access to Device via PPPoE Dial Up Connection 40
11.9 Enable Hik-Connect Service on Camera 41
11.9.1 Enable Hik-Connect Service via Web Browser 41
11.9.2 Enable Hik-Connect Service via SADP Software 41
11.9.3 Access Camera via Hik-Connect 42
11.10 Set ISUP 42
11.11 Set Open Network Video Interface 42
11.12 Set Alarm Host 43
11.13 Set Alarm Server 43
11.14 Set Network Service 43
11.15 Set SRTP 44
Chapter 12 System and Security 45
12.1 View Device Information 45
12.2 Search and Manage Log 45
12.3 Import and Export Configuration File 45
12.4 Export Diagnose Information 46
12.5 Reboot 46
12.6 Restore and Default 46
12.7 Upgrade 46
12.8 View Open Source Software License 47
12.9 Time and Date 47
12.9.1 Synchronize Time Manually 47
12.9.2 Set NTP Server 47
12.9.3 Set DST 48
12.10 Set RS-232 48

12.11 Set RS-485 48
12.12 Set Same Unit 49
12.13 Security 49
12.13.1 Authentication 49
12.13.2 Security Audit Log 49
12.13.3 Set IP Address Filter 50
12.13.4 Set SSH 51
12.13.5 Set HTTPS 51
12.13.6 Set QoS 52
12.14 User and Account 53
12.14.1 Set User Account and Permission 53
Chapter 13 Appendix 54
13.1 Common Material Emissivity Reference 54
13.2 Device Command 54
13.3 Device Communication Matrix 55
13.4 FAQ 55

Chapter 1 Overview

1.1 Introduction

Thermal Presence Detector is a detector based on thermal imaging technology.

Due to the advantages of thermal imaging, the detector is able to achieve the detection tasks without the influence of changing light condition.

The device supports network connection by web browser on a mobile phone or on a computer with Wi-Fi function. Data transmission, live view and device configuration are available with web browser and mobile application.

The detector can be used for people number detection, people existence detection, and abnormal temperature monitoring in meeting rooms, libraries, etc.

Table 1-1 Function and Settings

Function	Descriptions	Main Settings
People Number Detection and People Existence Detection	Detector detects the people number in a region. When abnormal number is detected, the device triggers alarms. The people existence status is able to be uploaded continuously when the people existence detection is enabled. The function is ideal to use in the situation where people number should be restricted to a certain quantity.	Enable **Number of People Exception Detection**, **People Existence Detection** and complete related settings. See ***People Number Management*** for instructions. Voice warning is supported when you select **Audible Warning** as the alarm linkage of detected exceptions and complete the related settings. See ***People Number Management*** and ***Set Audible Alarm Output*** for instructions. The device also supports outputting alarm signals to a connected peripheral device. See *Quick Start Guide* of the detector for alarm cable connection, and see ***Trigger***

Function	Descriptions	Main Settings
		Alarm Output for device settings.
Temperature Measurement and Abnormal Temperature Alarm	Detect the temperatures in the detection scene. When abnormal temperature is detected, the device triggers and upload alarm information. The function is often used for fire prevention in places such as, warehouse, laboratory, museum, meeting room.	Enable **Temperature Measurement** and complete related settings. See ***Temperature Measurement*** for instructions. Voice warning is supported when you select **Audible Warning** as the alarm linkage of detected exceptions and complete the related settings. See ***People Number Management*** and ***Set Audible Alarm Output*** for instructions.

1.2 Application

The mobile client Hik-Connect or PC client iVMS-4200 is used to configure the detector and to receive alarm information.

Table 1-2 Applications

Main Parts	Usage	Main Setting Procedure
• Thermal Presence Detector • PC Client iVMS-4200	Use PC client to configure and manage the device, and receive alarm notifications.	1. Connect the device to a Wi-Fi network. See ***Wi-Fi*** . 2. Activate and add the device to PC client iVMS-4200. See *User Manual of iVMS-4200* for instructions.
• Thermal Presence Detector • Mobile Client Hik-Connect	Use your mobile client to configure and manage the device, and receive alarm notifications.	• Connect the device to a Wi-Fi network. See ***Wi-Fi*** . • Activate and configure the device. See ***Device Activation and Accessing*** . • Add the device to your mobile client. See ***Enable Hik-Connect Service on Camera*** .

Chapter 2 Wi-Fi

Connect the device to wireless network by setting Wi-Fi parameters.

Note

This function is only supported by certain device models.

2.1 Connect to Wi-Fi via Web Browser

Use a web browser on you smart phone or your computer (with Wi-Fi function) to connect the device to a Wi-Fi network.

Before You Start

Install and power on the device.

Steps

1. Enable the Wi-Fi function on your mobile phone/computer.
2. Select the device wireless AP (Access Point) from the Wi-Fi list.

   Note

   Every device has a unique AP SSID, HM-AP_ABCDEF. ABCDEF stands for the verification code of your device, which you can find on the device label.
3. Enter the password of your device AP.

   Note

   The password is the last eight characters of the device serial number.
   For example, if the device serial number is D12345678, then the AP password is 12345678.
4. Open the browser on mobile phone/computer, tap **Refresh** to select the Wi-Fi network that the device needs to connect to, and enter password of the selected Wi-Fi network.
5. Check the device indicator to see if the connection is successful.

Table 2-1 Indicator Status

Indicator Status	Description
Flash about every 2 seconds.	Network connected.
Flash about every 0.2 second.	Network connection failed. **Note** If the connection fails, please try again.

What to do next

You can change the Wi-Fi parameters at **Configuration → Network Settings → Advanced Settings → Wi-Fi** . See ***Change Wi-Fi Parameters*** for instructions.

Chapter 3 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.

3.1 Activate the Device via SADP

Search and activate the online devices via SADP software.

Before You Start

Access www.hikvision.com to get SADP software to install.

Steps

1. Connect your computer to the same Wi-Fi network that the device is in.
2. Run SADP software to search the online devices of the LAN.
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**.

3.2 Activate the Device via Browser

You can access and activate the device via the browser.

Steps

1. Connect your computer to the same Wi-Fi network that the device is in.
2. Change the IP address of the computer 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 computer 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.

3.3 Login

Log in to the device via Web browser.

3.3.1 Plug-in Installation

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

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

Operating System	Web Browser	Operation
		Display and operation of certain functions are restricted. For example, Playback and Picture are not available. For detailed restricted function, refer to the actual device.
Mac OS 10.13+	Mac Safari 12+	Plug-in installation is not required. Go to **Configuration → Network → Advanced Settings → Network Service** 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.

3.3.2 Illegal Login Lock

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

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

Illegal Login Attempts

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

Locking Duration

The device releases the lock after the setting duration.

Chapter 4 People Number Management

People number management is used to detect the people number in a predefined area. When the number is abnormal, the device triggers alarms.

4.1 Set People Number Management Rule

Draw the detection area and set detection rule for people number management.

Steps

1. Go to **Configuration → People Number Management → Rule** .
2. Click + to add a region and enter a region name.

   Note

   Click ✕ to clear the selected region.
3. Click ⬡ ,and click on the live image to draw a region.
4. Set detection parameters for the region.

   People Number OSD

   Check the item to display the real-time people number of the region on live image.

   Drag the yellow OSD frame to adjust the display position.

   Alarm Times Per Exception

   Check the item to enable the function and enter a desired **Times**.

   The **Times** stands for the maximum times of uploading alarm information for one exception incident. If the parameter is not set, the device uploads the alarm information continuously until the exception disappears.

   Alarm Interval

   It is the minimum time interval for the device to upload alarms for a different exception incident. If the interval between two exceptions is less the set value, the second exception will not trigger alarm uploading.

   First Alarm Delay

   It is the time the device waits before it triggers alarm and uploads information.

   This parameter helps to filter out the interference caused by people moving around the edge of the detection region.
5. **Optional:** Check **Number of People Exception Detection**, and set the **Alarm Trigger Condition**.
6. **Optional:** Check **Enable People Existence Detection**.

   The device will detect whether there are people in the region and upload the result. The alarm information that contains people existence status and people number will be uploaded according to the set alarm interval.

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

Chapter 5 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.

5.1 Notice

This part introduces the notices of configuring temperature measurement function.

- The target surface should be as vertical to the optical axis as possible. It is recommended that the angle of oblique image plane should be less than 45°.
- The target image pixels should be more than 5 × 5.

5.2 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 Thermography Parameters*** to set the parameters.
3. Go to **Configuration → Temperature Measurement → Advanced Settings** , and select **Normal**.
4. Configure the parameters of normal mode.

   Emissivity

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

   Distance

   The distance between the target and the device.

   Pre-Alarm Threshold

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

   Alarm Threshold

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

   Pre-Alarm Output and Alarm Output

   Check **Pre-Alarm Output** and **Alarm Output** to link the pre-alarm or alarm with the connected alarm device.
5. Refer to ***Set Arming Schedule*** for setting scheduled time. Refer to ***Linkage Method Settings*** for setting linkage method.
6. Click **Save**.

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

Note

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

5.3 Set Thermography Parameters

Configure the parameters of temperature measurement.

Steps

1. Go to **Configuration → Local** , and 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.

   Add Original Data on Capture

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

   Add Original Data on Stream

   Check to add original data on thermal view.

   Data Refresh Interval

   It means the refresh interval of temperature information.

   Unit

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

Temperature Range

Select the temperature measurement range.

Version

View the version of current algorithm.

4. Click **Save**.

5.4 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.

5.5 Set Shielded Region

You can configure areas from being detected.

Steps

1. Check **Enable Shield Area**.
2. Click ⬡ .
3. Drag the mouse in the live view to draw the area. You can drag the corners of the red rectangle area to change its shape and size.
4. Right click the mouse to stop drawing.
5. **Optional:** Select one area and click ✕ to delete it.
6. Click **Save**.

Chapter 6 Event and Alarm

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

6.1 Set Exception Alarm

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

Steps

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

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

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

Chapter 7 Arming Schedule and Alarm Linkage

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

7.1 Set Arming Schedule

Set the valid time of the device tasks.

Steps

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

   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**.

7.2 Linkage Method Settings

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

7.2.1 Trigger Alarm Output

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

Steps

1. Go to **Configuration → Event → Basic Event → Alarm Output** .
2. Set alarm output parameters.

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

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

Manual Alarm

You can trigger an alarm output manually.

Steps

1. Set the manual alarm parameters.

   Alarm Output No.

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

   Alarm Name

   Edit a name for the alarm output.

   Delay

   Select **Manual**.

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

Automatic Alarm

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

Steps

1. Set automatic alarm parameters.

   Alarm Output No.

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

   Alarm Name

   Custom a name for the alarm output.

   Delay

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

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

7.2.2 FTP/NAS/Memory Card Uploading

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

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

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

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

7.2.3 Send Email

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

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

Set Email

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

Before You Start

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

Steps

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

      Note

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

7.2.4 Notify Surveillance Center

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

7.2.5 Trigger Recording

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

For recording settings, refer to ***Video Recording and Picture Capture***

7.2.6 Set Audible Alarm Output

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

Steps

1. Go to **Configuration → Event → Basic Event → Audible Alarm Output** .
2. Select a **Alarm Type**.
3. Select **Sound Type** and set related parameters.
   - Select **Warning** and its contents. Set the alarm times you need.
   - Select **Custom Audio**. You can select a custom audio file from the drop-down list. If no file is available, you can click **Add** to upload an audio file that meets the requirement. Up to three audio files can be uploaded.
4. **Optional:** Click **Test** to play the selected audio file on the device.
5. Set arming schedule for audible alarm. See ***Set Arming Schedule*** for details.
6. Click **Save**.

Note

The function is only supported by certain device models.

Chapter 8 Live View

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

8.1 Live View Parameters

The supported functions vary depending on the model.

8.1.1 Start and Stop Live View

Click **Live View**. Click ▶ to start live view. Click ■ to stop live view.

8.1.2 Window Proportion

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

8.1.3 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*** .

8.1.4 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.

8.1.5 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.

8.2 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 Audio*** .
   - For VCA settings, see ***Temperature Measurement*** .

Note

The function is only supported by certain models.

8.3 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 teal-time. In poor network environment, the device cannot ensures video fluency even the fluency is enabled.

3. Click **OK**.

Chapter 9 Video and Audio

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

9.1 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** .

9.1.1 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 means 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.

Other Streams

Steams other than the main stream and sub stream may also be offered for customized usage.

9.1.2 Video Type

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

Video

Only video content is contained in the stream.

9.1.3 Resolution

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

9.1.4 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.

9.1.5 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.

9.1.6 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.

9.1.7 Video Encoding

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

Note

Available compression standards vary according to device models.

H.264

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

H.265

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

MJPEG

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

Profile

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

I-Frame Interval

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

In H.264 and H.265, an I-frame, or intra frame, is a self-contained frame that can be independently decoded without any reference to other images. An I-frame consumes more bits than other frames. Thus, video with more I-frames, in other words, smaller I-frame interval, generates more steady and reliable data bits while requiring more storage space.

SVC

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

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

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

9.1.8 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.

9.1.9 Display VCA Info

VCA information can be displayed by Player and Video.

Player

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

Video

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

9.2 Display Settings

It offers the parameter settings to adjust image features.

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

Click **Default** to restore settings.

9.2.1 Image Adjustment

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

9.2.2 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 **Correct**, the device will take the uniform object as the standard and optimize the image once.

Manual Correction

Click **Correct** to optimize the image once.

Note

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

Thermal AGC Mode

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

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

9.2.3 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.

9.2.4 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.

9.2.5 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.

9.2.6 Brightness Sudden Change

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

9.2.7 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.

9.3 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 displayed on screen, select **EUC-KR**. Otherwise, select **GBK**.

Displayed Information

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

Text Overlay

Set customized overlay text on image.

OSD Parameters

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

9.4 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**.

Chapter 10 Video Recording and Picture Capture

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

10.1 Storage Settings

This part introduces the configuration of several common storage paths.

10.1.1 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**.

10.1.2 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**.

10.1.3 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.

Picture Filling Interval

For better picture management, you can set the picture filing interval from 1 day to 30 days. Pictures captured in the same time interval will be saved in one folder named after the beginning date and ending date of the time interval.

Picture Name

Set the naming rule for captured pictures. You can choose **Default** in the drop-down list to use the default rule, that is, IP address_channel number_capture time_event type.jpg (e.g., 10.11.37.189_01_20150917094425492_FACE_DETECTION.jpg). Or you can customize it by adding a **Custom Prefix** to the default naming rule.

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

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

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

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

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

10.2 Video Recording

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

10.2.1 Record Automatically

This function can record video automatically during configured time periods.

Before You Start

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

Steps

Note

The function varies according to different models.

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

   Note

   The record type is vary according to different models.

   Continuous

   The video will be recorded continuously according to the schedule.

   Motion

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

   Alarm

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

   Motion | Alarm

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

   Motion & Alarm

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

   Event

   The video is recorded when configured event is detected.
4. Set schedule for the selected record type. Refer to ***Set Arming Schedule*** for the setting operation.
5. Click **Advanced** to set the advanced settings.

   Overwrite

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

   Pre-record

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

   Post-record

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

   Stream Type

Select the stream type for recording.

Note

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

Recording Expiration

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

6. Click **Save**.

10.2.2 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.

10.2.3 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.

10.3 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.

10.3.1 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**.

10.3.2 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.

10.3.3 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 11 Network Settings

11.1 TCP/IP

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

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

NIC Type

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

IPv4

Two IPv4 modes are available.

DHCP

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

Note

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

Manual

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

IPv6

Three IPv6 modes are available.

Route Advertisement

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

Note

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

DHCP

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

Manual

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

MTU

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

The valid value range of MTU is 1280 to 1500.

DNS

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

11.1.1 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.

11.2 Change Wi-Fi Parameters

Before You Start

The device should be connected to a Wi-Fi network. See ***Connect to Wi-Fi via Web Browser*** for instructions.

Steps

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

Note

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

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

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

What to do next

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

11.3 Port

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

Caution

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

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

HTTP Port

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

RTSP Port

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

HTTPS Port

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

Server Port

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

WebSocket Port

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

WebSockets Port

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

Note

- 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.

11.4 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**.

11.4.1 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.

11.4.2 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.

11.5 Multicast

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

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

IP Address

It stands for the address of multicast host.

Stream Type

The stream type as the multicast source.

Video Port

The video port of the selected stream.

Audio Port

The audio port of the selected stream.

11.6 SNMP

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

Before You Start

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

Steps

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

Note

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

3. Configure the SNMP settings.
4. Click **Save**.

11.7 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.

11.8 Access to Device via PPPoE Dial Up Connection

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

Steps

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

Dynamic IP

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

User Name

User name for dial-up network access.

Password

Password for dial-up network access.

Confirm

Input your dial-up password again.

4. Click **Save**.
5. Access the device.

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

Note

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

11.9 Enable Hik-Connect Service on Camera

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

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

11.9.1 Enable Hik-Connect Service via Web Browser

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

Before You Start
You need to activate the camera before enabling the service.

Steps
1. Access the camera via web browser.
2. Enter platform access configuration interface. **Configuration → Network → Advanced Settings → Platform Access**
3. Select Hik-Connect as the **Platform Access Mode**.
4. Check **Enable**.
5. Click and read "Terms of Service" and "Privacy Policy" in pop-up window.
6. Create a verification code or change the old verification code for the camera.

   Note

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

11.9.2 Enable Hik-Connect Service via SADP Software

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

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

   Note

   The verification code is required when you add the camera to Hik-Connect service.
5. Click and read "Terms of Service" and "Privacy Policy".
6. Confirm the settings.

11.9.3 Access Camera via Hik-Connect

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

Before You Start
Connect the camera to network with network cables.

Steps
1. Download Hik-Connect from ***https://www.hikmicrotech.com/en/download/5*** and install it on your mobile device.
2. Start the application and register for a Hik-Connect user account.
3. Log in after registration.
4. In the app, tap "+" on the upper-right corner and then scan the QR code of the camera to add the camera. You can find the QR code on the camera or on the cover of the Quick Start Guide of the camera in the package.
5. Follow the prompts to set the network connection and add the camera to your Hik-Connect account.

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

11.10 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.

11.11 Set Open Network Video Interface

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

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

Delete Delete the selected Open Network Video Interface user.

Modify Modify the selected Open Network Video Interface user.

4. Click **Save**.
5. **Optional:** Repeat the steps above to add more Open Network Video Interface users.

11.12 Set Alarm Host

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

Steps

1. Go to **Configuration → Network → Other** .
2. Enter the alarm host IP and port.
3. Click **Save**.

11.13 Set Alarm Server

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

Steps

1. Go to **Configuration → Network → Advanced Settings → Alarm Server** .
2. Enter **Destination IP or Host Name**, **URL**, and **Port**.
3. Select **Protocol**.

Note

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

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

11.14 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**.

11.15 Set SRTP

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

Steps

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

Note

Only certain device models support this function.

Chapter 12 System and Security

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

12.1 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.

12.2 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.

12.3 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**.

12.4 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.

12.5 Reboot

You can reboot the device via browser.

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

12.6 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.

12.7 Upgrade

Before You Start

You need to obtain the correct upgrade package.

Caution

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

Steps

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

Firmware Locate the exact path of the upgrade file.

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

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

12.8 View Open Source Software License

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

12.9 Time and Date

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

12.9.1 Synchronize Time Manually

Steps

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

12.9.2 Set NTP Server

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

Before You Start

Set up a NTP server or obtain NTP server information.

Steps

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

Note

Server Address is NTP server IP address.

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

6. Click **Save**.

12.9.3 Set DST

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

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

12.10 Set RS-232

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

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

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

12.11 Set RS-485

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

Before You Start
Connect the device and computer or termial with RS-485 cable.

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

   Note

   You should keep the parameters of the device and the computer or terminal all the same.
3. Click **Save**.

12.12 Set Same Unit

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

Steps

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

12.13 Security

You can improve system security by setting security parameters.

12.13.1 Authentication

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

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

RTSP Authentication

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

WEB Authentication

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

Note

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

12.13.2 Security Audit Log

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

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

Search Security Audit Logs

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

Steps

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.

Set Log Server

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

Steps

1. Check **Enable Log Upload Server**.
2. Input **Log Server IP** and **Log Server Port**.
3. Click **Test** to test the settings.
4. Install client certificate.
   1) Click **Create** to create the certificate request. Fill in the required information in the pop-up window.
   2) Click **Download** to download the certificate request and submit it to the trusted certificate authority for signature.
   3) Install the signed certificate to the device.
5. Install the CA certificate to the device.

12.13.3 Set IP Address Filter

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

IP address refers to IPv4.

Steps

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

Forbidden IP addresses in the list cannot access the device.

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

4. Edit the IP address filter list.

Add Add a new IP address to the list.

Modify Modify the selected IP address in the list.

Delete Delete the selected IP address in the list.

5. Click **Save**.

12.13.4 Set SSH

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

Steps

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

12.13.5 Set HTTPS

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

Steps

1. Go to **Configuration → Network → Advanced Settings → HTTPS** .
2. Check **Enable** .
3. **Optional:** Check **HTTPS Browsing** to access the device only via HTTPS protocol.
4. Click **Delete** to recreate and install certificate.

Create and install self-signed certificate Refer to ***Create and Install Self-signed Certificate***

Create certificate request and install certificate Refer to ***Install Authorized Certificate***

5. Click **Save**.

Create and Install Self-signed Certificate

Steps

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

4. Click **OK**.

Result

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

Install Authorized Certificate

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

Steps

1. Select **Create certificate request first and continue the installation**.
2. Click **Create**.
3. Follow the prompt to input **Country/Region**, **Hostname/IP**, **Validity** and other parameters.
4. Click **Download** to download the certificate request and submit it to the trusted authority for signature.
5. Import certificate to the device.
   - Select **Signed certificate is available, start the installation directly**. Click **Browse** and **Install** to import the certificate to the device.
   - Select **Create the certificate request first and continue the installation**. Click **Browse** and **Install** to import the certificate to the device.
6. Click **Save**.

12.13.6 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**.

12.14 User and Account

12.14.1 Set User Account and Permission

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

Caution

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

Steps

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

   Administrator

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

   User

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

   Operator

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

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

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

   Note

   The administrator can add up to 31 user accounts.
3. Click **OK**.

Chapter 13 Appendix

13.1 Common Material Emissivity Reference

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

13.2 Device Command

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

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

13.3 Device Communication Matrix

Scan the following QR code to get device communication matrix.
Note that the matrix contains all communication ports of HikMicro thermal cameras.

13.4 FAQ

Scan the following QR code to get device common FAQ.



HIKMICRO

See the World in a New Way