Thermal Network Camera

User Manual

Legal Information

©2019 Hangzhou Hikvision Digital Technology Co., Ltd. All rights reserved.

About this Manual

The Manual includes instructions for using and managing the Product. Pictures, charts, images and all other information hereinafter are for description and explanation only. The information contained in the Manual is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of this Manual at the Hikvision website (***https://www.hikvision.com/***).
Please use this Manual with the guidance and assistance of professionals trained in supporting the Product.

Trademarks

HIKVISION and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions.
Other trademarks and logos mentioned are the properties of their respective owners.

Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS MANUAL AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED “AS IS” AND “WITH ALL FAULTS AND ERRORS”. HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.
YOU ACKNOWLEDGE THAT THE NATURE OF INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INSPECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.
YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR

PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.

IN THE EVENT OF ANY CONFLICTS BETWEEN THIS MANUAL AND THE APPLICABLE LAW, THE LATER PREVAILS.

Symbol Conventions

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

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

Safety Instruction

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

Laws and Regulations

- Use of the product must be in strict compliance with the local electrical safety regulations.

Transportation

- Keep the device in original or similar packaging while transporting it.
- Keep all wrappers after unpacking them for future use. In case of any failure occurred, you need to return the device to the factory with the original wrapper. Transportation without the original wrapper may result in damage on the device and the company shall not take any responsibilities.
- Do not drop the product or subject it to physical shock. Keep the device away from magnetic interference.

Power Supply

- Please purchase the charger by yourself. Input voltage should meet the Limited Power Source (12 VDC, 24 VAC, or PoE(802.3af)) according to the IEC61010-1 standard. Please refer to technical specifications for detailed information.
- Make sure the plug is properly connected to the power socket.
- DO NOT connect multiple devices to one power adapter, to avoid over-heating or fire hazards caused by overload.

Battery

- Improper use or replacement of the battery may result in explosion hazard. Replace with the same or equivalent type only. Dispose of used batteries in conformance with the instructions provided by the battery manufacturer.
- 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.

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.

Using Environment

- Make sure the running environment meets the requirement of the device. The operating temperature shall be -40°C to 65°C (-40°F to 149°F), and the operating humidity shall be 95% or less, no condensing.
- DO NOT expose the device to high electromagnetic radiation or dusty environments.
- DO NOT aim the lens at the sun or any other bright light.

Emergency

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

Manufacture Address

No.555 Qianmo Road, Binjiang District, Hangzhou 310052, China
Hangzhou Hikvision Digital Technology Co.,Ltd

Contents

Chapter 1 Overview 1
1.1 Brief Description 1
1.2 Function 1
Chapter 2 Device Activation and Accessing 2
2.1 Activate the Device via SADP 2
2.2 Activate the Device via Browser 2
2.3 Login 3
2.3.1 Install Plug-in 3
2.3.2 Illegal Login Lock 3
Chapter 3 Temperature Measurement 5
3.1 Notice 5
3.2 Thermography Configuration Flow Chart 5
3.3 Automatic Thermography 6
3.3.1 Set Thermography Parameters 7
3.3.2 Set Normal Mode 8
3.3.3 Object Missing 9
3.3.4 Set Thermography Rule 9
3.3.5 Point Thermography 9
3.3.6 Line Thermography 10
3.3.7 Area Thermography 10
3.4 Set Shielded Region 10
3.5 Manual Thermography 10
Chapter 4 Fire Source Detection 12
4.1 Select Recommended Scene 12
4.2 Set Fire Detection Parameters 12
Chapter 5 Behavior Analysis 14

5.1 Flow Chart of Behavior Analysis 14
5.2 Set VCA Parameters 15
5.3 Calibration 15
5.3.1 Calibrate Automatically 15
5.3.2 Calibrate Manually 16
5.3.3 Verify the Calibration Result 17
5.4 Set Rules 17
5.5 Advanced Configuration 19
5.6 Set Global Size Filter 20
Chapter 6 Event and Alarm 21
6.1 Set Motion Detection 21
6.1.1 Normal Mode 21
6.1.2 Expert Mode 22
6.2 Set Video Tampering Alarm 23
6.3 Set Alarm Input 24
6.4 Set Exception Alarm 25
6.5 Detect Audio Exception 25
Chapter 7 Arming Schedule and Alarm Linkage 27
7.1 Set Arming Schedule 27
7.2 Linkage Method Settings 27
7.2.1 Trigger Alarm Output 27
7.2.2 FTP/NAS/Memory Card Uploading 28
7.2.3 Send Email 29
7.2.4 Notify Surveillance Center 30
7.2.5 Trigger Recording 30
7.2.6 Set Audible Alarm Output 30
7.2.7 Set Flashing Alarm Light Output 30
Chapter 8 Live View 32

8.1 Live View Parameters 32
8.1.1 Window Proportion 32
8.1.2 Live View Stream Type 32
8.1.3 Start Digital Zoom 32
8.1.4 Quick Set Live View 32
8.1.5 Lens Parameters Adjustment 33
8.1.6 Light 33
8.1.7 Wiper 33
8.1.8 Lens Initialization 33
8.1.9 Auxiliary Focus 34
8.2 Set Transmission Parameters 34
Chapter 9 Video and Audio 36
9.1 Video Settings 36
9.1.1 Stream Type 36
9.1.2 Video Type 36
9.1.3 Resolution 36
9.1.4 Bitrate Type and Max. Bitrate 37
9.1.5 Video Quality 37
9.1.6 Frame Rate 37
9.1.7 Video Encoding 37
9.1.8 Smoothing 39
9.1.9 Display VCA Info 39
9.1.10 Audio Settings 39
9.1.11 Two-way Audio 40
9.1.12 Set ROI 40
9.2 Display Settings 41
9.2.1 Image Adjustment (Thermal Channel) 41
9.2.2 DNR 42

9.2.3 Set Palette 42
9.2.4 Set Target Color 42
9.2.5 DDE 44
9.2.6 Brightness Sudden Change 44
9.2.7 Enhance Regional Image 44
9.2.8 Mirror 44
9.2.9 Video Standard 45
9.2.10 Digital Zoom 45
9.2.11 Scene Mode 45
9.3 OSD 45
9.4 Set Privacy Mask 45
9.5 Overlay Picture 46
9.6 Set Manual DPC (Defective Pixel Correction) 46
Chapter 10 Video Recording and Picture Capture 48
10.1 Storage Settings 48
10.1.1 Set Memory Card 48
10.1.2 Set NAS 48
10.1.3 Set FTP 49
10.1.4 Set Cloud Storage 49
10.2 Video Recording 50
10.2.1 Record Automatically 50
10.2.2 Record Manually 51
10.2.3 Playback and Download Video 51
10.3 Capture Configuration 52
10.3.1 Capture Automatically 52
10.3.2 Capture Manually 53
10.3.3 View and Download Picture 53
Chapter 11 Network Settings 54

11.1 TCP/IP 54
11.1.1 Multicast Discovery 55
11.2 Port 55
11.3 Port Mapping 56
11.3.1 Set Auto Port Mapping 56
11.3.2 Set Manual Port Mapping 56
11.4 Multicast 57
11.5 SNMP 57
11.6 Access to Device via Domain Name 58
11.7 Access to Device via PPPoE Dial Up Connection 58
11.8 Enable Hik-Connect Service on Camera 59
11.8.1 Enable Hik-Connect Service via Web Browser 59
11.8.2 Enable Hik-Connect Service via SADP Software 60
11.8.3 Access Camera via Hik-Connect 60
11.9 Set ISUP 60
11.10 Set ONVIF 61
11.11 Set HTTP Listening 61
Chapter 12 System and Security 62
12.1 View Device Information 62
12.2 Search and Manage Log 62
12.3 Import and Export Configuration File 62
12.4 Export Diagnose Information 63
12.5 Reboot 63
12.6 Restore and Default 63
12.7 Upgrade 63
12.8 View Open Source Software License 64
12.9 Time and Date 64
12.9.1 Synchronize Time Manually 64

12.9.2 Set NTP Server 64
12.9.3 Set DST 65
12.10 Set RS-232 65
12.11 Set RS-485 65
12.12 Set Same Unit 66
12.13 Security 66
12.13.1 Authentication 66
12.13.2 Security Audit Log 67
12.13.3 Set IP Address Filter 67
12.13.4 Set SSH 68
12.13.5 Set HTTPS 68
12.13.6 Set QoS 69
12.13.7 Set IEEE 802.1X 69
12.14 User and Account 70
12.14.1 Set User Account and Permission 70
Chapter 13 Appendix 71
13.1 Common Material Emissivity Reference 71
13.2 Device Command 71
13.3 Device Communication Matrix 72

Chapter 1 Overview

1.1 Brief Description

Thermal network bullet camera equipped with built-in GPU which supports intelligent behavior analysis algorithm, can realize high-precision VCA detection and real-time alarm. It is applied to perimeter defense and fire-prevention purposes in critical infrastructures such as community, villa, construction site, factory, 4S stores, and so on. The pre-alarm system helps you discover unexpected events immediately and protects your property.

1.2 Function

This section introduces main functions of the device.

Fire Detection

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

Temperature Measurement

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

VCA

Device can do behavior analysis. Multiple rules can be configured for different requirements.

Smoking Detection

Device can detect the smoking behavior and alarm.

Chapter 2 Device Activation and Accessing

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

Note

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

2.1 Activate the Device via SADP

Search and activate the online devices via SADP software.

Before You Start

Access www.hikvision.com 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 Install Plug-in

You can access the device by installing plug-in.

Steps

1. Input IP address of the device in web browser and the login window will pop up.
2. Install the plug-in according to the prompt.
3. Open the web browser again and input IP address of the device.
4. Input user name and password, and click **Login**.

Help	Get online help document of the device.
Logout	You can exit safely.

2.3.2 Illegal Login Lock

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

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

Go to **Configuration → System → Security → Security Service** , and enable **Enable Illegal Login Lock**, and set the illegal login attempts.

Chapter 3 Temperature Measurement

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

3.1 Notice

This part introduces the notices of configuring temperature measurement function.

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

3.2 Thermography Configuration Flow Chart

This part introduces the process of configuring temperature measurement.

Figure 3-1 Thermography Configuration Flow Chart

Note

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

3.3 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.

3.3.1 Set Thermography Parameters

Configure the parameters of temperature measurement.

Before You Start
Go to **Configuration → System → Maintenance → VCA Resource Type** , select **Temperature Measurement+Behavior Analysis**.

Steps

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

   Display Temperature Info.

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

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

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

   Enable Temperature Measurement

   Check to enable temperature measurement function.

   Enable Color-Temperature

   Check to display Temperature-Color Ruler in live view.

   Display Temperature Info. on Stream

   Check to display temperature information on the stream.

   Display Temperature in Optical Channel

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

   Display Max./Min./Average Temperature

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

   Position of Thermometry Info

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

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

   Add Original Data on Capture

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

   Add Original Data on Stream

   Check to add original data on thermal view.

   Data Refresh Interval

   It means the refresh interval of temperature information.

   Unit

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

Temperature Range

Select the temperature measurement range.

Version

View the version of current algorithm.

4. Click **Save**.

3.3.2 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.

3.3.3 Object Missing

This object is not available in the repository.

3.3.4 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. Click ⚙ and set the **Alarm Rule**.

   Alarm Temperature and Pre-Alarm Temperature

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

   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 canceled.
4. Click **Save**.

   Click **Liveview**, and you can view the temperature and rules information on live view.

3.3.5 Point Thermography

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

Steps

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

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

3.3.6 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.

3.3.7 Area Thermography

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

Steps

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

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

3.4 Set Shielded Region

You can configure areas from being detected.

Steps

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

3.5 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.

Chapter 4 Fire Source Detection

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

Fire source detection includes fire source detection and smoking detection. It is applied to fire-prevention purposes in scenic region, forest, tunnel and so on.

Fire Detection

Configure the fire source detection parameters. When fire source is detected, the alarm actions will be triggered.

Smoking Detection

The device can detect the smoking behavior and output alarm.

4.1 Select Recommended Scene

Introduce the recommended scenes of fire source detection and help you select the appropriate scene.

Fire source detection can be applied to indoor and outdoor monitoring with a maximum detection radius 15 km. To achieve the best monitoring effect, please set the installation place as requirements below.

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

4.2 Set Fire Detection Parameters

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

Before You Start

Go to **Configuration → System → Maintenance → VCA Resource Type** , select **Temperature Measurement+Behavior Analysis** or **Temperature Measurement+Fire Detection**.

Steps

1. Go to **Configuration → Local** .
2. Check **Locate Highest Temperature Point** to display the position of highest temperature. Check **Frame Fire Point** to frame the fire source on live view.
3. Go to **Configuration → Event → Smart Event** , select **Dynamic Fire Source Detection**.
4. Check **Enable Dynamic Fire Source Detection**.
5. Set the parameters of fire detection.

Fire Source Detection Mode

Smoking Mode

Detect smoking behavior in the scene.

Dynamic Fire

Detect the fire source in the scene.

Sensitivity

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

Note

When **VCA Resource Type** is selected as **Temperature Measurement+Behavior Analysis**, only smoking detection is supported. When **VCA Resource Type** is selected as **Temperature Measurement+Fire Detection**, two detection modes are both supported.

6. Check **Display Fire Source Frame on Stream** to display a red frame around the fire source on stream when fire occurs.
7. **Optional:** you can shield certain areas from being detected in fire source detection.
   1) Go to **Configuration → Event → Smart Event → Fire Source Detection Shield** .
   2) Check **Enable Fire Source Detection Shield** .
   3) Click **Draw Area** and drag the mouse in the live view to draw the area. Release the mouse to finish drawing.
   4) You can drag the corners of the red rectangle area to change its shape and size. Or drag the rectangle to the position on your demand.
   5) Click **Stop Drawing**.
   6) Click **Clear All** to clear all of the setting areas.
   7) Set the value of **Active Zoom Ratio** on your demand, and then the shield will only appear when the zoom ratio is greater than the predefined value
   8) Click **Add** to save the smoke detection shield, and it will be listed in the **Fire Source Detection Shield List** area; you can select a region and click **Delete** to delete it from the list; you can also define the color of the regions.
   9) Check **Display Shield Region** to show the shielded area in live view.
8. Refer to ***Set Arming Schedule*** for setting scheduled time. Refer to ***Linkage Method Settings*** for setting linkage method.
9. Click **Save**.

Chapter 5 Behavior Analysis

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

5.1 Flow Chart of Behavior Analysis

The process of configuraing the behavior analysis function is decribed below.

Figure 5-1 Flow Chart of Behavior Analysis Configuration

5.2 Set VCA Parameters

Steps

1. Go to **Configuration → VCA → Basic Settings** .

   Display VCA Info. on Stream

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

   Display Trajectory

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

   Target Marking Color

   The frame color of human is shown as orange, the frame color of vehicle is shown as purple.

   Display Target Info. on Alarm Picture

   Select to display the target information on the alarm picture.

   Display Rule Info. on Alarm Picture

   Select to display the rule information on the alarm picture.

   Snapshot Settings

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

2. Click **Save**.

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

5.3 Calibration

5.3.1 Calibrate Automatically

Before You Start

- Make sure that we have known the actual height of the target person in the scene.
- Make sure there is no moving objects in the view except for the person.

Steps

1. Go to **Configuration → VCA → Camera Calibration** .
2. Check **Camera Calibration**.
3. when the person is totally seen in live view, enter the height of person in **Target Height**.

   Note

   You can set a maximum of two decimal places.

4. Click ▶ to start calibration.

Caution

- The auto calibration starts when the person is totally seen in live view, and ends when the person is in the endpoint.
- The endpoint-to-camera distance (m) equals 4 times the lens focal length (mm). E.g, for 7mm lens, the recommended endpoint is 28m (7*4).
- The person should walk in zigzag path. And two zigzag paths are required. Make sure the walking route covers the left, middle, right of image.
- The auto calibration duration should be no shorter than 10 sec, and no longer than 10 min. The device will stop calibration automatically if the duration is too long.
- If there is moving object such as leave or tree in the scene, you can set the shielded area . Refer to ***Set Shielded Region*** for detail settings.

5. When the person exits, click ■ to stop calibration.

Note

After auto calibration, refer to ***Verify the Calibration Result*** to verify if the calibration is successful. Set manual calibration if the auto calibration failed, or the verified result turns bad.

Result

After calibration, the height and angle of camera will be shown in live view.

5.3.2 Calibrate Manually

Steps

1. Go to **Configuration → VCA → Camera Calibration** .
2. Check **Manual Calibration**.
3. Click **Fig 1**. Click and drag the vertical line until it fits the target.
4. Enter the actual length of the calibration line.
5. Repeat steps above to set **Fig 2**, **Fig 3**, and **Fig 4**.

Note

Draw a calibration line in each figure, and the four calibration lines should be evenly distributed in the same horizontal plane from left to right.
In the four figures, the calibrated object doesn't need to be the same. Select a proper object in each figure.

6. **Optional:** Click ✕ to delete the calibration line.
7. Click **Save**.

Caution

- Separate 4 vertical lines in the optical-axis direction at the close site, middle and far site respectively.
- Separate 4 vertical lines at the left, middle and right of the image respectively.
- If manual calibration's result is incorrect, select another target to recalibrate.
- After manual calibration, refer to ***Verify the Calibration Result*** to verify if the calibration is successful.

Result

After calibration, the height and angle of camera will be shown in live view.

5.3.3 Verify the Calibration Result

The function can verify whether the calibrated value is consistent with the actual value.

Steps

1. Click .
2. Click , and drag a vertical line in the view.
3. Move the line to the target, then click to caculate the length.

   Compare the calculated line length to the actual length to verify the calibration settings.
4. Click to exit.

Note

Verify not only person, but also other objects appeared in the view. Such as car, street lamp, etc.

5.4 Set Rules

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

Steps

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

Note

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

Line Crossing

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

Intrusion

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

Region Entrance

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

Region Exiting

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

4. Set parameters of the rule.
   - **Sensitivity**

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

     Detection Target

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

     Background Interference Suppression

     Eliminate the environment interference to reduce the false alarm. For example, the wind blow grass.
5. Draw the rules.
   - When the rule type is selected as **Line Crossing**, click to draw a line in the live view. You can drag end points of the line to adjust the position and length.

     Line Crossing

     You can set the crossing direction. Bidirectional, A-to-B, or B-to-A are selectable.
   - When the rule type is selected as **Intrusion**,**Region Entrance**, **Region Entrance**, click to draw an area in the live view. Right click the mouse to finish drawing.

     Duration

     The device performs behavior analysis when the target stays in the detection area for more than setting value.

Note

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

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

Note

- You can draw the max size and min size rectangles according to the real target in the scene. The recommended size is 1.2 times of the target.
- Due to the main difference between human and animal is the height. Just concern the height of animal.
- Click to copy the same settings to other rules.

7. Click **Save**.
8. **Optional:** you can shield certain areas from being detected. Refer to ***Set Shielded Region*** for detailed settings.

Note

Repeat steps above to configure multiply rules. Set the arming schedule and linkage method for each rule.

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

5.5 Advanced Configuration

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

Detection Parameters

Detection Sensitivity

The higher the sensitivity is, the easier the target will be detected.

Background Update Rate

if a detected target remains in the monitoring scene for a certain time, the system will count the target as the background automatically. The greater the value is, the faster the target will be counted as the background.

Minimum Target Size

The system will filter out the object smaller than the minimum target size.

Displacement Constraint for Target Generation

The higher the value is, the slower the target is generated, and the higher accuracy the analysis will get.

Optical-axis Movement

Check the function when the target moves in the direction of camera's optical -axis.

When the target is far from the device and the movement is not clear, enable this function to check the move direction.

Single Alarm

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

Scene Modes

The scene mode is set to be **General** by default. Select **Distant View** when you are far from the targets. Select **Indoor** when you are indoor.

Restore Parameters

Restore Default

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

Restart VCA

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

5.6 Set Global Size Filter

Targets larger or smaller than the set size range are filtered out. The settings is valid for all behavior analysis rules.

Steps

1. Go to **Configuration → Behavior Analysis → Advanced Configuration** to enable the function.
2. Click to draw a maximum size frame on live image.
3. Click to draw a minimum size frame on live image.
4. 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 Motion Detection

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

Steps

1. Go to **Configuration → Event → Basic Event → Motion Detection** .
2. Check **Enable Motion Detection**.
3. **Optional:** Highlight to display the moving object in the image in green.
   1) Check **Enable Dynamic Analysis for Motion**.
   2) Go to **Configuration → Local** .
   3) Set **Rules** to **Enable**.
4. Select **Configuration Mode**, and set rule region and rule parameters.
   - For the information about normal mode, see ***Normal Mode*** .
   - For the information about expert mode, see ***Expert Mode*** .
5. Set the arming schedule and linkage methods. For the information about arming schedule settings, see ***Set Arming Schedule*** . For the information about linkage methods, see ***Linkage Method Settings*** .
6. Click **Save**.

6.1.1 Normal Mode

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

Steps

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

Figure 6-1 Set Rules

Stop Drawing Stop drawing one area.

Clear All Clear all the areas.

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

6.1.2 Expert Mode

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

Steps

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

   Day/Night Switch

   OFF: Day/night switch is disabled.

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

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

   Sensitivity

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

Figure 6-2 Set Rules

Stop Drawing Finish drawing one area.

Clear All Delete all the areas.

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

6.2 Set Video Tampering Alarm

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

Steps

1. Go to **Configuration → Event → Basic Event → Video Tampering** .
2. 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 6-3 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**.

6.3 Set Alarm Input

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

Before You Start

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

Steps

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

6.4 Set Exception Alarm

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

Steps

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

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**.

6.5 Detect Audio Exception

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

Steps

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

Audio Loss Detection

Detect sudden loss of audio track.

Sudden Increase of Sound Intensity Detection

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

Note

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

Sudden Decrease of Sound Intensity Detection

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

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

Note

The function varies according to different models.

Chapter 7 Arming Schedule and Alarm Linkage

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

7.1 Set Arming Schedule

Set the valid time of the device tasks.

Steps

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

   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

   Custom a name for the alarm output.

   Delay

   Select **Manual**.

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

Automatic Alarm

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

Steps

1. Set automatic alarm parameters.

   Alarm Output No.

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

   Alarm Name

   Custom a name for the alarm output.

   Delay

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

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

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

For device that supports audible warning as a linkage method, options are open to configure audible alarm parameters.

Steps

Note

The function is only supported by certain camera models.

1. Go to the setting page: **Configuration → Event → Basic Event → Audible Alarm Output** .
2. Select desired alarm sound type and alarm times.
3. Set arming schedule for audible alarm. Refer to ***Set Arming Schedule***
4. Click **Save**.

7.2.7 Set Flashing Alarm Light Output

Steps

1. Go to **Configuration → Event → Basic Event → Flashing Alarm Light Output** .
2. Set **Flashing Duration**, **Flashing Frequency** and **Brightness**.

   Flashing Duration

   The time period the flashing lasts when one alarm happens.

   Flashing Frequency

   The flashing speed of the light. High, Medium, and Low are selectable.

   Brightness

   The brightness of the light.
3. Edit the arming schedule.
4. Click **Save**.

Note

Only certain camera models support the function.

Chapter 8 Live View

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

8.1 Live View Parameters

8.1.1 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.

8.1.2 Live View Stream Type

Select the live view stream type according to your needs. For the detailed information about the stream type selection, refer to ***Stream Type*** .

8.1.3 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.

8.1.4 Quick Set Live View

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

Steps

1. Click to show quick setup page.
2. Set PTZ, display settings, OSD, video/audio and VCA resource parameters.
   - For PTZ settings, see ***Lens Parameters Adjustment*** .
   - For display settings, see ***Display Settings*** .
   - For OSD settings, see ***OSD*** .
   - For audio and video settings, see ***Video and Audio*** .

- For VCA settings, see ***Fire Source Detection*** , ***Temperature Measurement*** , and ***Behavior Analysis*** .

Note

The function is only supported by certain models.

8.1.5 Lens Parameters Adjustment

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

Zoom

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

Focus

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

PTZ Speed

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

Iris

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

8.1.6 Light

Click to turn on or turn off the illuminator.

8.1.7 Wiper

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

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

8.1.8 Lens Initialization

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

Click to operate lens initialization.

8.1.9 Auxiliary Focus

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

8.2 Set Transmission Parameters

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

Steps

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

Protocol

TCP

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

UDP

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

MULTICAST

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

Note

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

HTTP

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

Play Performance

Shortest Delay

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

Balanced

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

Fluent

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

Custom

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

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 and audio) that should be contained in the stream.

Video

Only video content is contained in the stream.

Video & Audio

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

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.

9.1.10 Audio Settings

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

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

Audio Encoding

Select the audio encoding compression of the audio.

Audio Input

Note

- Connect the audio input device as required.
- The audio input display varies with the device models.

LineIn	Set **Audio Input** to **LineIn** when the device connects to the audio input device with the high output power, such as MP3, synthesizer or active pickup.
MicIn	Set **Audio Input** to **MicIn** when the device connects to the audio input device with the low output power, such as microphone or passive pickup.

Environmental Noise Filter

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

9.1.11 Two-way Audio

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

Before You Start

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

Steps

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

9.1.12 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.

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 (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.

9.2.2 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.

9.2.3 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.

9.2.4 Set Target Color

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

Steps

1. Go to **Configuration → Image → Display Settings** .
2. 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.

Figure 9-1 Set the Temperature and Color of Target

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**.

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 Enhance Regional Image

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

Steps

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

9.2.8 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.

9.2.9 Video Standard

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

9.2.10 Digital Zoom

You can zoom in the image

The larger the zoom size is, the more blurred the image is.

9.2.11 Scene Mode

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

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.

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**, and **Font Color**.

9.4 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.

Drag the corners of the area	Adjust the size of the area.
Drag the area	Adjust the position of the area.
Click Clear All	Clear all the areas you set.

4. Click **Stop Drawing**.
5. Click **Save**.

Note

Up to 4 areas are supported for setting.

9.5 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**.

9.6 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.

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

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

   Server Address

   The IP address of the network disk.

   File Path

The saving path of network disk files.

User Name and Password

The user name and password of the net HDD.

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

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.
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 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.

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

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

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.

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 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 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 unaccessible.

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

HTTP Port

It refers to the port that access the device through the browser. You should enter the port No. after the IP address. For example, when the **HTTP port** is modified to 81, you need to enter ***http://192.168.1.64:81*** in the browser for browser login.

HTTPS Port

It refers to the port of browser certificate access. Certificate verification is required when accessing the device through the browser, and the security level is high.

RTSP Port

It refers to the port of real time streaming protocol.

Server Port

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

11.3 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**.

11.3.1 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.

11.3.2 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.

11.4 Multicast

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

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

IP Address

It stands for the address of multicast host.

Stream Type

The stream type as the multicast source.

Video Port

The video port of the selected stream.

Audio Port

The audio port of the selected stream.

11.5 SNMP

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

Before You Start

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

Steps

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

   Note

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

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

11.6 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.

11.7 Access to Device via PPPoE Dial Up Connection

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

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

   Dynamic IP

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

   User Name

   User name for dial-up network access.

   Password

Password for dial-up network access.

Confirm

Input your dial-up password again.

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

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

Note

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

11.8 Enable Hik-Connect Service on Camera

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

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

11.8.1 Enable Hik-Connect Service via Web Browser

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

Before You Start

You need to activate the camera before enabling the service.

Steps

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

Note

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

7. Save the settings.

11.8.2 Enable Hik-Connect Service via SADP Software

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

Steps

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

   Note

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

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

11.8.3 Access Camera via Hik-Connect

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

Steps

1. Download and install the Hik-Connect app by searching "Hik-Connect" in App Store or ™
2. Launch the app 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.

11.9 Set ISUP

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

Steps

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

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

11.10 Set ONVIF

If you need to access to the device through ONVIF protocol, you can configure the ONVIF user to enhance the network security.

Steps

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

   Delete Delete the selected ONVIF user.

   Modify Modify the selected ONVIF user.
4. Click **Save**.
5. **Optional:** Repeat the steps above to add more ONVIF users.

11.11 Set HTTP Listening

The device can send alarms to destination IP or host name through HTTP protocol. The destination IP or host name should support the HTTP data transmission

Steps

1. Go to **Configuration → Network → Advanced Settings → HTTP Listening** .
2. Input **Destination IP** or **Host Name**, **URL**, and **Port**.
3. Click **Test**.

   Note

   Click **Default** to reset the destination IP or host name.
4. Click **Save**.

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.

RTSP Digest Algorithm

MD5, SHA256 and MD5/SHA256 encrypted algorithm in RTSP authentication. If you enable the digest algorithm except for MD5, the third-party platform might not be able to login the device or enable live view because of compatibility. The encrypted algorithm with high strength is recommended.

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.

WEB Digest Algorithm

MD5, SHA256 and MD5/SHA256 encrypted algorithm in WEB authentication. If you enable the digest algorithm except for MD5, the third-party platform might not be able to login the device or enable live view because of compatibility. The encrypted algorithm with high strength is recommended.

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.

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. 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 CA Certificate***

4. 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**, **Hostname/IP**, **Validity** and other parameters.
4. Click **OK**.

Result

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

Install CA 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**, **Hostname/IP**, **Validity** and other parameters.
4. Click **Download** to download the certificate request and submit it to the trusted certificate 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**.

12.13.7 Set IEEE 802.1X

You can authenticate user permission of the connected device by setting IEEE 802.1X.

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

Select protocol and version according to router information. User name and password of server are required.

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 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

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 Hikvision 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 Hikvision thermal cameras.

See Far, Go Further