DS-2TD2xxx-xxxx/xx

Thermal and Optical Bi-Spectrum Network Camera

User Manual

Legal Information

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

Trademarks Acknowledgement

Trademarks and logos mentioned are the properties of their respective owners.

LEGAL 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." OUR COMPANY 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 OUR COMPANY 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 OUR COMPANY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.

YOU ACKNOWLEDGE THAT THE NATURE OF INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND OUR COMPANY SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INSPECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, OUR COMPANY WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.

YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.

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

Symbol Conventions

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

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

Safety Instruction

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

Laws and Regulations

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 yourself. Input voltage should meet the Limited Power Source (12 VDC, 24 VAC, or PoE(802.3af)) according to the IEC61010-1 standard. 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 overheating 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.

Environment

- Make sure the running environment meets the device requirement. The operating temperature shall be -40° to 65° C (-40° to 149° F), and the operating humidity shall be 95% or less, non-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.

Contents

Chapter 1 Overview

1.1 Brief Description

Thermal and Optical Bi-Spectrum Network Camera equipped with built-in GPU, which supports intelligent behavior analysis algorithm, can realize high-precision VCA detection and real-time alarms. It is applied to perimeter defense and fire-prevention purposes in critical infrastructures such as community, villa, construction site, factory, automotive dealerships, etc. The pre-alarm system helps you discover unexpected events immediately and protects your property.

Model
DS-2TD2235D-25 DS-2TD2235D-50
DS-2TD2637-10/P DS-2TD2637-15/P DS-2TD2637-25/P DS-2TD2637-35/P
DS-2TD2836-25/V1 DS-2TD2836-50/V1 DS-2TD2866-25/V1 DS-2TD2866-50/V1
DS-2TD2617-3/PA DS-2TD2617-6/PA DS-2TD2617-10/PA

1.2 Functions

This section introduces the main functions of the device.

- **Fire Detection**
  Device can detect the dynamic fire source in the scene and output pre-alarms and alarms 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 smoke behavior and activate an alarm.

Chapter 2 Device Activation and Accessing

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

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

2.1 Activate the Device via SADP

Search and activate the online devices via SADP software.

Before You Start
Get SADP software from the official Website to install.

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

STRONG PASSWORD RECOMMENDED – We highly recommend that you create a strong password of your own choosing (using a minimum of eight 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. We also recommend that you reset your password regularly. Especially in high security systems, resetting the password monthly or weekly can better protect your product.

Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

5. Click **OK** and the **Device Status** changes to **Active**.
6. (Optional): Change the device network parameters in **Modify Network Parameters**.

2.2 Activate the Device via Browser

You can access and activate the device via a Web browser.

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.

STRONG PASSWORD RECOMMENDED – We highly recommend that you create a strong password of your own choosing (using a minimum of eight 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. We also recommend that you reset your password regularly. Especially in high security systems, resetting the password monthly or weekly can better protect your product.

Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

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 a Web browser.

2.3.1 Install Plug-in

You can access the device by installing a plug-in.

1. Input IP address of the device in a 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 the device IP address.

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 security when accessing the device via the Internet.

The admin user can set the number of login attempts with a wrong password. When the login attempts with a wrong password reaches the set number, the device will lock.

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

Chapter 3 Temperature Measurement

When you enable this function, the device measures the actual temperature of the scene. It alarms when the 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.
- Select line thermography or area thermography for a certain area temperature measurement. The point thermography is not recommended in case of deviation occurring during device movement to affect temperature measurement accuracy.

3.2 Thermography Configuration Flow Chart

This section introduces temperature measurement configuration.

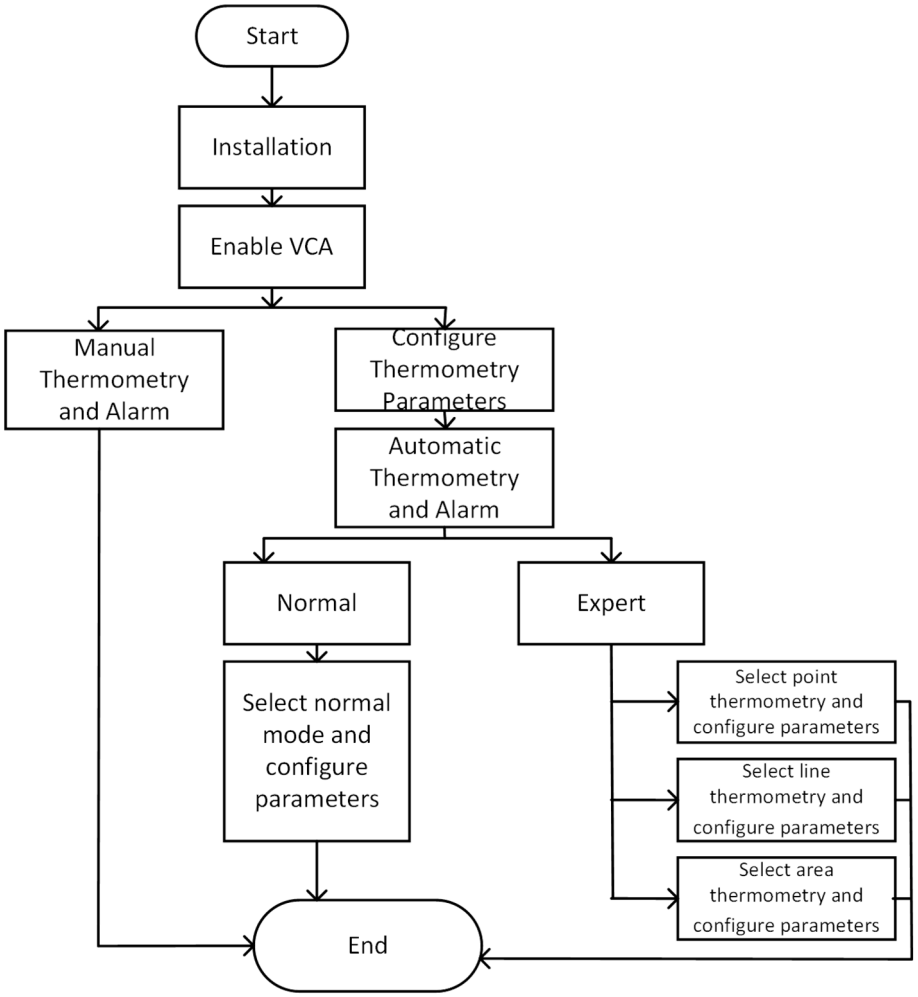

Figure 1, Thermography Configuration Flow Chart

NOTE: Refer to the *Quick Start Guide* for detailed installation information.

3.3 Automatic Thermography

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

3.3.1 Set Thermography Parameters

Configure the temperature measurement parameters.

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

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

1) Display Temperature Info.

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

3) 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 live view when the temperature measurement rule is line or area.
- **Position of Thermometry Info:** Select the position of temperature information shown on 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:** Temperature information refresh interval.
- **Unit:** Display temperature in Celsius (°C)/Fahrenheit (°F)/Kelvin (K).
- **Temperature Range:** Select the temperature measurement range.
- **Version:** View the current algorithm version.

4. Click **Save**.

3.3.2 Set Normal Mode

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

1. Go toConfiguration → 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 (see Appendix).
   - **Distance:** The distance between the target and the device.
   - **Pre-Alarm Threshold:** When the target temperature exceeds the pre-alarm threshold, and this status keeps more than **Filtering Time**, it triggers a 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 live view.

NOTE: Go to **Image → VCA Rules Display** to adjust the font size and the temperature color of normal, alarm, and pre-alarm.

3.3.3 Set Expert Mode

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

1. Go to Configuration → Temperature Measurement → Basic Settings, check **Enable Temperature Measurement**.
2. Refer to ***Set Thermography Parameters*** to set the parameters.
3. Go to Configuration → Temperature Measurement → Advanced Settings, select **Expert**.
4. Select and enable the temperature measurement rules. Refer to ***Set Thermography Rule***.
5. (Optional): Click **Area's Temperature Comparison** to set the alarm rules and the temperature.

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

7. Click **Save**. The maximum temperature and thermography rules will be displayed on live view.

NOTE: Go to **Image → VCA Rules Display** to adjust the font size and the temperature color of normal, alarm, and pre-alarm.

3.3.4 Set Thermography Rule

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 at the position to be measured.

   - **Point:** See ***Point Thermography*** for detailed configuration.
   - **Line:** See ***Line Thermography*** for detailed configuration.
   - **Area:** See ***Area Thermography*** for detailed configuration.

3. Configure the temperature measurement parameters.

   - **Emissivity:** Set the emissivity of the target. The emissivity of the surface of a material is its effectiveness in emitting energy as thermal radiation. Different objects have different emissivity. Refer to ***Common Material Emissivity Reference*** to search for the target emissivity..
   - **Distance:** The distance between the target and the device.
   - **Reflective Temperature:** If there is any object with high emissivity in the scene, check and set the reflective temperature to correct the temperature. The reflective temperature should be set the same as the temperature of the high emissivity object.

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

   - **Alarm Temperature and Pre-Alarm Temperature:** Set the alarm temperature and pre-alarm temperature. E.g., select Alarm Rule as Above (Average Temperature), set the Pre-Alarm Temperature to 50° C, and set the Alarm Temperature to 55° C. The device pre-alarms when its average temperature is higher than 50° C and alarms when its average temperature is higher than 55° C.
   - **Filtering Time:** It refers to the duration after the target temperature reaches or exceeds the pre-alarm temperature/alarm temperature.
   - **Tolerance Temperature:** Set the tolerance temperature to prevent constant temperature changes 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 a pre-alarm when its temperature reaches 50° C and alarms when its temperature reaches 55° C, and only when the device temperature is lower than 52° C will the alarm be cancelled.
   - **Pre-Alarm Output and Alarm Output:** When the target temperature exceeds the pre-alarm or alarm

threshold, it triggers the pre-alarm or alarm output of the connected device.

- **Area's Temperature Comparison:** Select two areas and set the comparison rule, and set the temperature difference threshold. The device alarms when the temperature difference meets the set value.

5. You can shield certain area from being detected. See ***Set Shielded Region*** for detailed settings.
6. Click **Save**.
7. Click **Live View**, and select thermal channel to 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.

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

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.
4. Go to the **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.

1. Click and drag the mouse in live view to draw the area, and right click to finish drawing.
2. Click and move the area to adjust the position.
3. Drag the corners of the area to adjust the size and shape.
4. Go to the **Live View** interface to view the maximum temperature and rule of the area in thermal channel.

3.3.8 Set Shielded Region

You can configure areas from being detected.

1. Check **Enable Shield Area**.

2. Click ⬡.
3. Drag the mouse in live view to draw the area. 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**.

3.4 Manual Thermography

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

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

Chapter 4 Fire Source Detection

The device will trigger and upload an alarm when it detects a 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, tunnels, etc.

- **Fire Detection:** Configure the fire source detection parameters. When a fire source is detected, the alarm actions will be triggered.
- **Smoking Detection:** The device can detect smoking behavior and output an alarm.

4.1 Select Recommended Scene

Introduces the recommended fire source detection scenes and helps you select the appropriate scene.

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

- The installation location 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 location with convenient traffic, well-equipped power, and Internet access. E.g., communication tower, watchtower, high-rise roof, etc.

4.2 Set Fire Detection Parameters

To avoid potential fire damage, configure the fire detection function for certain areas. Detailed configuration steps are shown below.

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

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

will be detected (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**, both detection modes are supported.

6. Check **Display Fire Source Frame on Stream** to display a red frame around the fire source on the stream when a 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 live view to draw the area. Release the mouse to finish drawing.

    4) Drag the corners of the red rectangle area to change its shape and size, or drag the rectangle to a position on 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 demand, and then the shield will appear only 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. See ***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 if a target breaks the VCA rules. The optical camera will track the target or the device and 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.

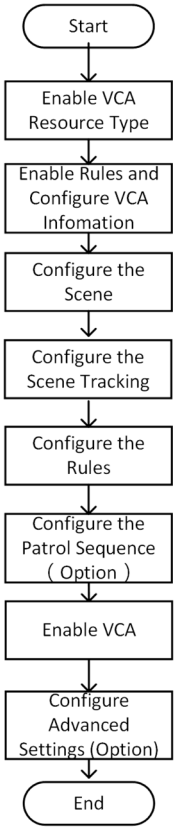

Figure 2, Flow Chart of Behavior Analysis Configuration

5.2 Set VCA Parameters

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 playback by the VS Player.
   - **Display Trajectory:** The target's moving path will be shown in live view.
   - **Target Marking Color:** The frame color of humans is shown as orange, the frame color of vehicles 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 picture quality and resolution separately.

2. Click **Save**.

3. 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 you know the actual height of the target person in the scene.
- Make sure there is no moving object in the view except for the person.

1. Go to Configuration → VCA → Camera Calibration.

2. Check **Camera Calibration**.

3. When the person is entirely 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: Auto Calibration starts when the person is entirely seen in live view and ends when the person is in the endpoint.

The endpoint-to-camera distance (m) equals four times the lens focal length (mm). E.g, for a 7 mm lens, the recommended endpoint is 28 m (7*4).

The person should walk in a zigzag path, and two zigzag paths are required. Make sure the walking route covers the left, middle, and right of image.

The auto calibration duration should be no shorter than 10 seconds, and no longer than 10 minutes. The device will stop calibration automatically if the duration is too long.

If there are moving objecst such as leaves or trees in the scene, you can set the shielded area. See ***Set Shielded Region*** for detailed settings.

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

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

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

5.3.2 Calibrate Manually

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 four vertical lines in the optical-axis direction at the close site, middle, and far site respectively.

Separate four 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, see ***Verify the Calibration Result*** to verify if the calibration is successful.

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

5.3.3 Verify the Calibration Result

This function can verify if the calibrated value is consistent with the actual value.

1. Click .
2. Click , and drag a vertical line in the view.
3. Move the line to the target, then click to calculate the length. Compare the calculated line length to the actual length to verify the calibration settings.

4. Click to exit.

NOTE: Verify not only the person, but also other objects appearing in the view such as car, street lamp, etc.

5.4 Set Rules

The device can detect if a target breaks a VCA rule. The optical camera will track the target or the device will alarm when the VCA rule is triggered.

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 types. Up to eight rules can be set for one scene.

- **Line Crossing:** If a target moves across the setting line, an alarm will be triggered. You can set the crossing direction.
- **Intrusion:** If a target intrudes into the pre-defined region longer than the set duration, the alarm will be triggered.
- **Region Entrance:** If a target enters the pre-defined region, the alarm will be triggered.
- **Region Exiting:** If a target exits the pre-defined region, the alarm will be triggered.

4. Set rule parameters.
   - **Sensitivity:** The higher the value, the easier the alarm will be triggered.
   - **Detection Target:** It is 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 a false or missing alarm.
   - **Background Interference Suppression:** Eliminate the environment interference to reduce false alarms. For example, the wind blowing grass.
5. Draw the rules.
   - When the rule type is set to **Line Crossing**, click ／ to draw a line in live view. You can drag endpoints 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 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 the 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 targets whose size is between the Max. Size and Min. Size values will trigger the alarm.

NOTE: You can draw the max size and min size rectangles according to a real target in the scene. The recommended size is 1.2 times of the target.

- Due to the main difference between humans and animals is height, just consider the animal height.
- Click to copy the same settings to other rules.

7. Click **Save**.
8. (Optional): You can shield certain areas from being detected. See ***Set Shielded Region*** for settings.

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

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

5.5 Advanced Configuration

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

Detection Parameters

- **Detection Sensitivity:** The higher the sensitivity, 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 consider the target as the background automatically. The greater the value, the quicker the target will be counted as the background.
- **Minimum Target Size:** The system will filter out objects smaller than the minimum target size.
- **Displacement Constraint for Target Generation:** The higher the value, the slower the target is generated, and the higher the accuracy.
- **Optical-Axis Movement:** Check this function when the target moves in the direction of the camera's optical axis. When the target is far from the device and the movement is not clear, enable this function to check the movement direction.
- **Single Alarm:** The system sends an alarm only once for each target triggering. Otherwise, the alarm will trigger 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 indoors.

Restore Parameters

- **Restore Default:** Click **Restore** to restore the parameters to the defaults.
- **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 setting is valid for all behavior analysis rules.

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 section introduces event configurations. The device reequires certain responses to triggered alarms.

6.1 Set Motion Detection

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

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

6.1.1 Normal Mode

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

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

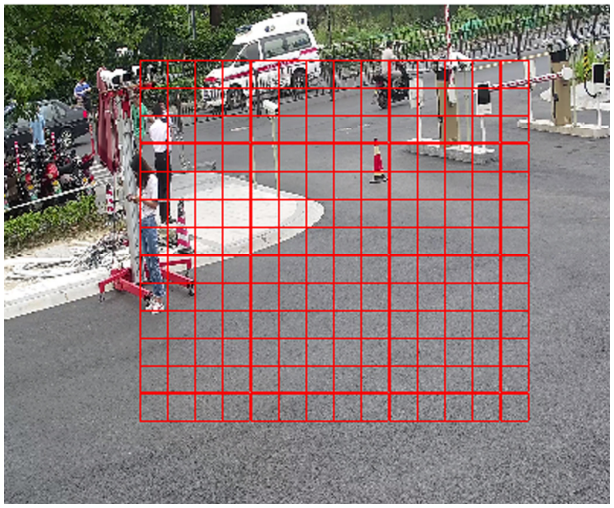

Figure 3, Set Rules

4. (Optional): Set the parameters for multiple areas by repeating the above steps.

6.1.2 Expert Mode

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

1. Select expert mode in **Configuration**.
2. Set expert mode parameters.
   - **Day/Night Switch OFF:** Day/night switch is disabled.
   - **Day/Night Auto-Switch:** The system switches day/night mode automatically according to the environment. It displays a colored image during the day and a 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 sensitivity value, the more sensitive the motion detection. 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.
   - **Stop Drawing:** Finish drawing one area.
   - **Clear All:** Delete all the areas.

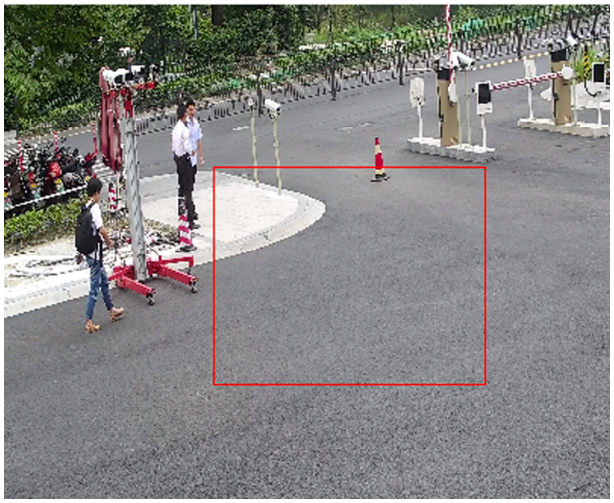

Figure 4, Set Rules

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.

1. Go to Configuration → Event → Basic Event → Video Tampering.
2. Select the channel number.
3. Check **Enable**.
4. Set the **Sensitivity**. The higher the value, the easier to detect the area covering.
5. Click **Draw Area** and drag the mouse in live view to draw the area.
    - **Stop Drawing:** Finish drawing.
    - **Clear All:** Delete all the drawn areas.

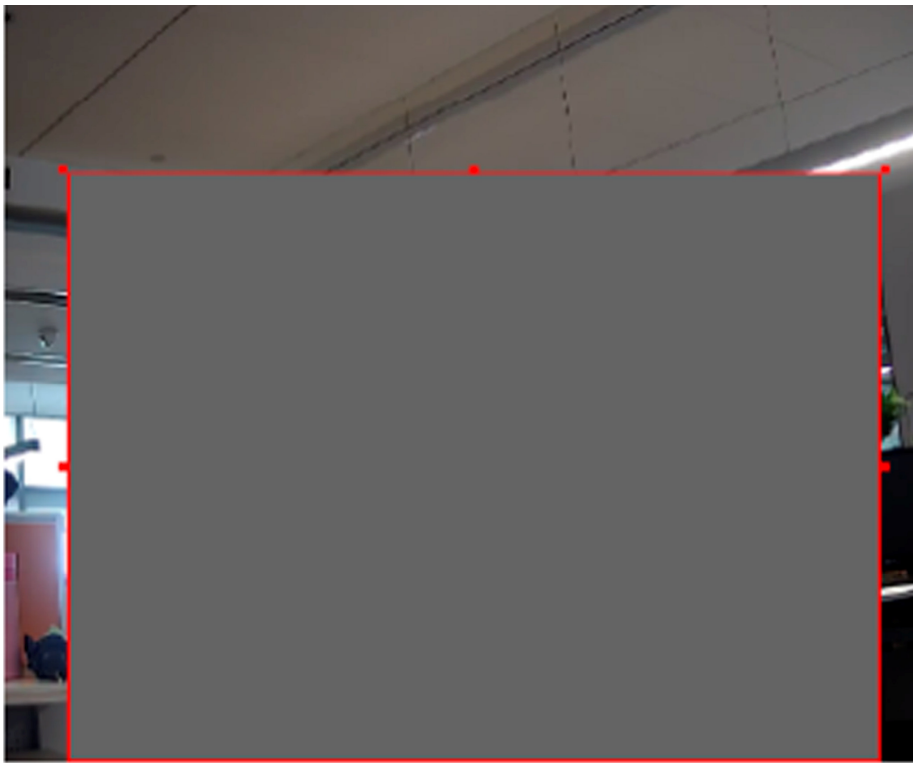

Figure 5, Set Video Tampering Area

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

6.3 Set Alarm Input

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

Before You Start

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

1. Go to Configuration → Event → Basic Event → Alarm Input.
2. Check **Enable Alarm Input Handling**.
3. Select **Alarm Input No.** and **Alarm Type** from the drop-down list. Edit the **Alarm Name**.
4. See ***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

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

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:** Current device IP address is same as that of another device in the network.
   - **Illegal Login:** Incorrect user name or password entered.
3. See ***Linkage Method Settings*** for setting linkage method.
4. Click **Save**.

6.5 Detect Audio Exception

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

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 in Sound Intensity. **Sensitivity** and **Sound Intensity Threshold** are configurable.

NOTE: The lower the sensitivity, the more significant the change must be to trigger detection.

Sound intensity threshold is the detection reference. It is recommended to set as the average sound intensity in the environment. The louder the environment sound, the higher the value should be. Adjust it according to the actual environment.

   - **Sudden Decrease of Sound Intensity Detection:** Detect sudden decrease in sound intensity. Sensitivity is configurable.
3. See ***Set Arming Schedule*** for setting scheduled time and ***Linkage Method Settings*** for linkage methods.
4. Click **Save**.

NOTE: The function varies by model.

Chapter 7 Arming Schedule and Alarm Linkage

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

7.1 Set Arming Schedule

Set the valid time of the device tasks.

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

NOTE: Up to eight 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 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 is 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.

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.

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:** Customize 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 will trigger an alarm output automatically in the set arming schedule.

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:** Customize a name for the alarm output.
   - **Delay:** Refers to the time duration that the alarm output remains after an alarm occurs.
2. Set the alarming schedule. For 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.

- See ***Set FTP*** to set the FTP server.
- See ***Set NAS*** for NAS configuration.
- See ***Set Memory Card*** for memory card storage configuration.

7.2.3 Send Email

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

For e-mail settings, see ***Set Email***.

Set Email
When e-mail is configured and **Send Email** is enabled as a linkage method, the device sends an e-mail 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.

1. Go to the e-mail settings page: Configuration → Network → Advanced Settings → Email.
2. Set e-mail parameters.
    1) Input the sender's e-mail information, including the **Sender's Address**, **SMTP Server**, and **SMTP Port**.
    2) (Optional): If your e-mail 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, e-mails are sent after being encrypted by SSL or TLS. The SMTP port should be set as 465.
        - When you select **SSL** or **TLS** and **Enable STARTTLS**, e-mails are sent after being 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 e-mail server. If you check **Enable STARTTLS** and the protocol is not supported by your e-mail server, your e-mail will be sent with no encryption.

    4) (Optional): To receive notifications with alarm pictures, check **Attached Image**. The notification e-mail has three attached event alarm pictures 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 configured properly.
3. Click **Save**.

7.2.4 Notify Surveillance Center

Check **Notify Surveillance Center** to have the alarm information 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 devices with more than one camera channel, you can set one or more channel recordings if needed.

For recording settings, see ***Video Recording and Picture Capture.***

7.2.6 Set Audible Alarm Output

For devices that support an audible warning as a linkage method, options are open to configure audible alarm parameters.

NOTE: This function is supported only 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. See ***Set Arming Schedule***
4. Click **Save**.

7.2.7 Set Flashing Alarm Light Output

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 this function.

Chapter 8 Live View

Introduction to live view parameters, function icons, and transmission parameters settings.

8.1 Live View Parameters

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

8.1.1 Window Division

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

8.1.2 Live View Stream Type

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

8.1.3 Enable and Disable Live View

Use this function to quickly enable or disable live view of all channels.

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

8.1.4 Start Digital Zoom

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

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 go back to the original image.

8.1.5 View Previous/Next Page

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

Click ← → to switch live view among multiple channels.

8.1.6 Full Screen

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

1. Click to start full screen mode.
2. Press **ESC** button to exit.

8.1.7 Light

1. Click to turn on or turn off the illuminator.

8.1.8 Wiper

For devices that have a wiper, you can control the wiper via a Web browser.

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

8.1.9 Lens Initialization

Lens initialization is used on devices equipped with a motorized lens. This function can reset the lens when a long time zoom or focus results in a blurred image. This function varies by models.

1. Click to operate lens initialization.

8.1.10 Auxiliary Focus

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

8.1.11 Quick Set Live View

Quick setup of PTZ, display settings, OSD, video/audio, and VCA resource settings on the live view page.

1. Click to show the 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 supported only by certain models.

8.1.12 Lens Parameters Adjustment

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.

8.2 Set Transmission Parameters

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

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 a stable network environment.
     - **UDP:** UDP is suitable for an unstable network environment that does not demand high video fluency.
     - **MULTICAST:** Multicast is suitable for situations in which there are multiple clients. You should set the multicast address for them before selection.

NOTE: For detailed information about multicast, see ***Multicast***.

     - **HTTP:** HTTP is suitable for situations in which third-party applications need to get the stream from the device.
   - **Play Performance**
     - **Shortest Delay:** Real-time video image priority over video fluency.
     - **Balanced:** Both real-time video image and video fluency.
     - **Fluent:** Video fluency as priority over real-time video image. In a poor network environment, the device cannot ensure video fluency even if fluency is enabled.

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

- **Auto Start Live View**

  - **Yes**: Live view is started automatically. It requires a high performance monitoring device and a stable network environment.

  - **No:** Live view should be started manually.

3. Click **OK**.

Chapter 9 Video and Audio

This section addresses video and audio related parameter configuration.

9.1 Video Settings

Setting video parameters such as stream type, video encoding, and resolution.

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

NOTE: For devices with multiple camera channels, select a channel before other settings.

9.1.1 Stream Type

For devices that support more than one stream, you can specify parameters for each stream type.

- **Main Stream:** The best stream performance the device supports. It usually offers the device's best resolution and frame rate. But high resolution and frame rate usually means more storage space and higher bandwidth requirements in transmission.
- **Sub Stream:** 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:** Stream is compressed and transmitted at a comparatively fixed bitrate. The compression speed is fast, but image mosaic may occur.
- **Variable Bitrate:** Device automatically adjusts 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 the **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 describes the frequency at which the video stream is updated and is measured in 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 a higher frame rate requires higher bandwidth and more storage space.

9.1.7 Video Encoding

The compression standard the device uses for video encoding.

NOTE: Available compression standards vary by device model.

- **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 a video file more than MJPEG or MPEG-4 Part 2.
- **H.265:** Also known as High Efficiency Video Coding (HEVC) and MPEG-H Part 2 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 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, and the requirement for network bandwidth is also higher.
- **I-Frame Interval:** Defines the number of frames between two 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, a smaller I-frame interval, generates more steady and reliable data bits while requiring more storage space.
- **SVC:** Scalable Video Coding (SVC) is the name for the Annex G extension of the H.264 or H.265 video compression standard.

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

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

to decode high quality video stream.

9.1.8 Smoothing

Refers to the stream smoothness. The higher the smoothing value, the better the stream fluency, though the video quality may not be so satisfactory. The lower the smoothing value, the higher quality of the stream, though it may appear less 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

Sets audio parameters such as audio encoding and 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 by device model.

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

- **Environmental Noise Filter:** Set it to 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

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 a built-in microphone and speaker, two-way audio function can be enabled directly.

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

9.1.12 Set ROI

ROI (Region of Interest) encoding assigns more encoding resources 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.

1. Go to Configuration → Video/Audio → ROI.
2. Check **Enable**.
3. Select the channel No. according to your need.
4. Select **Stream Type**.
5. Select **Region No.** in **Fixed Region** to draw ROI region.
    1) Click **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.

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

NOTE: The higher the ROI level, the clearer the detected region's image.

8. (Optional): Select another region no. and repeat the above steps to draw multiple fixed regions.

9.2 Display Settings

Offers parameter settings to adjust image features.

1. Go to Configuration → Image → Display Settings.

For devices that support multiple channels, display settings of each channel is required.

2. Click **Default** to restore settings.

9.2.1 Image Adjustment

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

9.2.2 Image Adjustment (Thermal Channel)

You can optimize the image display effect of the 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 a 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 normal 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 scenes with obvious WDR and high temperature difference, to improve image contrast and enhance the image. E.g. the scene contains both indoor and outdoor scenes.
  - **Linear:** Choose for scenes with low temperature difference and when the target is not obvious. Improves image contrast and enhances the image. E.g. a bird in a forest.
  - **Self-Adaptive:** Choose AGC mode automatically according to the current scene.

9.2.3 Exposure Settings

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

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

9.2.4 Day/Night Switch

The Day/Night Switch function can provide color images in day mode and black/white images in night mode. Switch mode is configurable.

- **Day:** The image is always in color.
- **Night:** The image is always black/white.
- **Auto:** The camera automatically switches between day mode and the night mode according to the illumination.
- **Scheduled-Switch:** Set the **Start Time** and the **End Time** to define the duration for day mode.

NOTE: Day/Night Switch function varies by model.

9.2.5 Set Supplement Light

1. Go to Configuration → Maintenance → System Service.
2. Check **Enable Supplement Light**.
3. Click **Save**.
4. Go to **Configuration → Image → Display Settings → Day/Night Switch** to set supplement light parameters.
    - **Smart Supplement Light:** Uses smart image processing technology to reduce overexposure caused by supplement light.
    - **IR Light Mode:** When the mode is set to **Auto**, the supplement light is automatically enabled or disabled according to the image brightness.
    - **Brightness Limit:** Adjust the upper limit of IR light power.

9.2.6 BLC

If you focus on an object against a strong backlight, the object will be too dark to be seen clearly. BLC (backlight compensation) compensates light to the object in the front to make it clear. If BLC mode is set to **Custom**, you can draw a red rectangle on the live view image as the BLC area.

9.2.7 WDR

The WDR (Wide Dynamic Range) function helps the camera provide clear images in environments with strong illumination differences.

When there are both very bright and very dark areas simultaneously in the field of view, you can enable the WDR function and set the level. WDR automatically balances the brightness level of the whole image and provides clear images with more details.

NOTE: When WDR is enabled, other functions may be not supported. See the actual interface for details.

9.2.8 White Balance

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

9.2.9 DNR

Digital Noise Reduction reduces the image noise and improves the image quality. **Normal** and **Expert** modes are selectable.

- **Normal:** Sets the DNR level to control the noise reduction degree. A higher level means stronger reduction degree.
- **Expert:** Sets the DNR level for both space DNR and time DNR to control the noise reduction degree. A higher level means stronger reduction degree.

9.2.10 Defog

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

9.2.11 Set Palette

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

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

Result: The live view displays the image with a palette.

9.2.12 Set Target Color

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

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

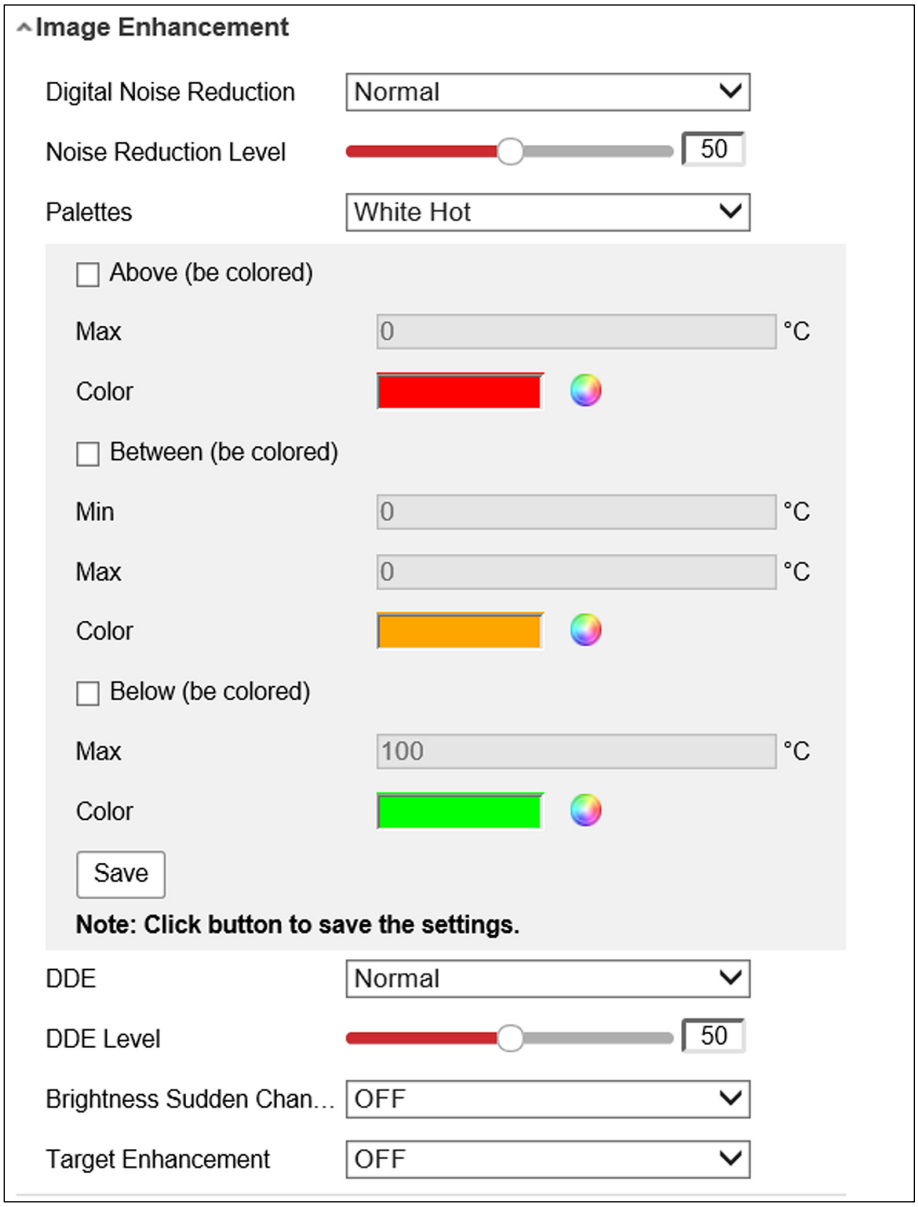

Figure 6, Set the Target's Temperature and Color

- **Above (be colored):** When a high temperature target needs to be colored, set the high temperature color. Targets above the setting temperature will be displayed in the setting color.
- **Between (be colored):** When an interval temperature target needs to be colored, set the interval temperature color. Targets between the minimum and the maximum temperatures will be displayed in the setting color.
- **Below (be colored):** When a low temperature target needs to be colored, set the low temperature color. Targets below the setting temperature will be displayed in the setting color.

5. Click **Save**.

9.2.13 DDE

Digital Detail Enhancement adjusts the image details. **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, the more details show, but the higher the noise.

9.2.14 Brightness Sudden Change

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

9.2.15 Enhance Regional Image

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

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.

9.2.16 Mirror

If 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.

9.2.17 Video Standard

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

9.2.18 Digital Zoom

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

9.2.19 Scene Mode

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

9.3 OSD

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

1. 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 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

Blocks certain areas in live view to protect privacy. Regardless of how the device moves, the blocked areas will never be seen.

1. Go to the privacy mask setting page: **Configuration → Image → Privacy Mask**.
2. Select the channel no.
3. Check **Enable Privacy Mask**.
4. Click **Draw Area**. Drag the mouse in live view to draw a closed area.
   - **Drag the corners of the area:** Adjust the area size.
   - **Drag the area:** Adjust the area position.
   - **Click Clear All:** Clear all the areas you set.
5. Click **Stop Drawing**.
6. Click **Save**.

NOTE: Up to four areas are supported for setting.

9.5 Overlay Picture

Overlay a custom picture on live view.

Before You Start
The picture to overlay has to be in 24-bit BMP format, and the maximum picture size is 128 × 128 pixels.

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

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

4. Check **Enable Picture Overlay**.
5. Drag the picture to adjust its position.
6. 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.

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

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

7. (Optional): Click to cancel defective pixel correction.

9.7 Set Picture-in-Picture

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

1. Select a channel number.
2. Select the **Picture-in-Picture** mode.
   - **Normal Mode:** Disable Picture-in-Picture mode.
   - **Overlay Mode:** Enable Picture-in-Picture mode. You can overlay the image of another channel in the current channel.
3. Click **Save**.

Chapter 10 Video Recording and Picture Capture

This section introduces 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 a memory card, insert and format the memory card in advance.

Before You Start
Insert the memory card into the camera. For detailed installation, see *Quick Start Guide* of the camera.

1. Go to the 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 memory card **Status** turns to **Normal** from **Uninitialized**, which means the memory card can be used normally.
3. (Optional): Define the memory card **Quota**. Input the quota percentage for different contents according to your needs.
4. Click **Save**.

10.1.2 Set NAS

Use a network server as a network disk to store the record files, captured images, etc.

Before You Start
Get the IP address of the network disk.

1. Go to the 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 that are captured by events or a timed snapshot task.

Before You Start
Get the FTP server address.

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 permission to upload pictures.

     If the FTP server supports picture uploading by anonymous users, 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 pictures directly from the cloud for picture and analysis. The function is supported only by certain models.

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

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 section introduces 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***.

1. Go to Configuration → Storage → Schedule Settings → Record Schedule.
2. Select channel no.
3. Check **Enable**.
4. Select a record type.

NOTE: The record type varies by model.

- **Continuous:** The video will be recorded continuously according to the schedule.
- **Motion:** When motion detection is enabled and trigger recording is selected as the linkage method, object movement is recorded.
- **Alarm:** When alarm input is enabled and trigger recording is selected as the linkage method, the video is recorded after receiving alarm signal from an external alarm input device.
- **Motion | Alarm:** Video is recorded when motion is detected or alarm signal is received from an external alarm input device.
- **Motion & Alarm:** Video is recorded only when motion is detected and an alarm signal is received from an external alarm input device.
- **Event:** Video is recorded when a configured event is detected.

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

- **Overwrite:** Enable to overwrite 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 a higher bitrate, the actual time of the pre-record and post-record may be less than the set value.

7. Click **Save**.

10.2.2 Record Manually

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, play back, and download videos stored in local or network storage.

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

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

5. Click on the playback interface to download files.
   1) Set search condition, then click **Search**.
   2) Select the video files, 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 pictures manually or automatically and save them in the 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, configure related linkage methods in event settings. See ***Event and Alarm*** for settings.

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

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 in the live view or playback window to capture a picture manually.

10.3.3 View and Download Picture

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

1. Click **Picture**.
2. Select channel no.
3. Set search condition, and click **Search**. Matching pictures show in the file list.
4. Select the pictures, then click **Download** to download them.

NOTE: Go to **Configuration → Local**, and 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 operating the device over a network. IPv4 and IPv6 are both supported. Both versions can be configured simultaneously without conflicting with each other.

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

   - **NIC Type:** Select a NIC (Network Interface Card) type according to your network.
   - **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 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, and IPv6 Default Gateway. Consult your network administrator for required information.
   - **MTU (Maximum Transmission Unit)**: 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 (Domain Name Server):** Required if you need to visit the device with domain name. It is also required for some applications (e.g., sending e-mail). Set **Preferred DNS Server** and **Alternate DNS Server** properly if needed.

11.1.1 Multicast Discovery

Check **Enable Multicast Discovery**, and then the online network camera will 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.

1. Go to Configuration → Network → Basic Settings → Port for port settings.
    - **HTTP Port:** The port that accesses the device through a browser. Enter the port no. after the IP address. For example, if 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:** The browser certificate access port. Certificate verification is required when accessing the device through a browser and the security level is high.
    - **RTSP Port:** The real time streaming protocol port.
    - **Server Port:** 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 device ports are the same as those of other network devices, see ***Port*** to modify device ports.

1. Go to Configuration → Network → Basic Settings → NAT.
2. Select the port mapping mode.
    - **Auto Port Mapping:** See *Set Auto Port Mapping* for detailed information.
    - **Manual Port Mapping:** Se *Set Manual Port Mapping* for detailed information.
3. Click **Save**.

11.3.1 Set Auto Port Mapping

1. Check **Enable UPnP™**, and choose a friendly name for the camera or 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

1. Check **Enable UPnP™**, and choose a friendly name for the device or use the default name.
2. Set 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 protocol 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.

1. Go to **Configuration** → **Network** → **Basic Settings** → **Multicast** for the multicast settings.
   - **IP Address:** The address of the 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, download the SNMP software and manage to receive the device information via SNMP port.

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.

You also need to use a version according to the security level required. SNMP v1 is not secure and SNMP v2 requires password for access. 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.

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. See ***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. See 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.

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 a dynamic IP, get a domain name from a DDNS provider (e.g., DynDns.com). See ***Access to Device via Domain Name*** for detailed information.

11.8 Enable Guarding Vision Service on Camera

Enable Guarding Vision service on your camera before using the service.

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

11.8.1 Enable Guarding Vision Service via Web Browser

Follow the following steps to enable Guarding Vision Service via a Web Browser.

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

1. Access the camera via a Web browser.
2. Enter the platform access configuration interface, **Configuration → Network → Advanced Settings → Platform Access**
3. Select Guarding Vision as the **Platform Access Mode**.
4. Check **Enable**.
5. Click and read "Terms of Service" and "Privacy Policy" in the 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 Guarding Vision service.

7. Save the settings.

11.8.2 Enable Guarding Vision Service via SADP Software

This section introduces how to enable the Guarding Vision service via SADP software of an activated camera.

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

NOTE: The verification code is required when you add the camera to Guarding Vision service.

5. Click and read “Terms of Service” and “Privacy Policy.”

6. Confirm the settings.

11.8.3 Access Camera via Guarding Vision

Guarding Vision is an application for mobile devices. Using the App, you can view live image, receive alarm notification, etc.

1. Download and install the Guarding Vision app by searching "Guarding Vision" in App Store or Google Play(TM)

2. Launch the app and register for a Guarding Vision 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 Guarding Vision account.

For detailed information, refer to the Guarding Vision app user manual.

11.9 Set ISUP

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

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.

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 HTTP data transmission.

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

This section 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.

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

12.2 Search and Manage Log

Logs help to locate and troubleshoot problems.

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

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

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 a Web browser.
    2) Click **Browse** to select the saved configuration file.
    3) Input the encryption password you set when exporting the configuration file.
    4) Click **Import**.

12.4 Export Diagnose Information

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

1. 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 a Web browser.

1. 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.

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 parameters to the factory defaults.

     Note

     Be careful when using this function. After resetting to the factory defaults, 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. The device reboots automatically after upgrade.

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

12.8 View Open Source Software License

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

12.9 Time and Date

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

12.9.1 Synchronize Time Manually

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 the 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 an NTP server when an accurate and reliable time source is required.

Before You Start
Set up an NTP server or obtain NTP server information.

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 the 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.

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 the device or access a 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 the computer or terminal with an RS-232 cable.

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

12.11 Set RS-485

RS-485 is used to connect the device to an 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 an RS-485 cable.

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

NOTE: Keep all parameters of the device and the computer or terminal 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

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.

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

   - **RTSP Authentication:** Digest and digest/basic are supported, which means authentication information is needed when an 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 supports only 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 log in to 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 supports only 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 log in to 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 the device's 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 to find out illegal intrusion and troubleshoot security events.

NOTE: This function is supported only 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 visits from certain IP addresses.

IP address refers to IPv4.

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 remote login security. This setting is reserved for professional maintenance personnel only.

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 remote access security.

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 Authorized Certificate*

4. Click **Save**.

Create and Install Self-signed Certificate

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

1. Select **Create certificate request** first, then 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 authority for signature.
5. Import certificate to the device.
    - Select **Signed certificate is available**, then start the installation directly. Click **Browse** and **Install** to import the certificate to the device.
    - Select **Create the certificate request** first, then 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 the network device such as router and switch.

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, the higher the priority. You need to set the same value in the router when configuring.

3. Click **Save**.

12.13.7 Set IEEE 802.1X

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

1. Go to Configuration → Network → Advanced Settings → 802.1X and enabling the function.

Select protocol and version according to router information. Server user name and password 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 permissions to different user levels.

CAUTION: To increase security of using the device on the network, change the password of your account regularly. Changing the password every three months is recommended. If the device is used in a high-risk environment, it is recommended that the password be changed monthly or weekly.

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 for all operations and can add users and operators and assign permissions.
   - **User:** Users can be assigned permission to view live video, set PTZ parameters, and change their own passwords, but no permission for other operations.
   - **Operator:** Operators can be assigned all permissions 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