Thermal & 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 HIKMICRO website (*http://www.hikmicrotech.com*).
Please use this Manual with the guidance and assistance of professionals trained in supporting the Product.

Trademarks

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

Disclaimer

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

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

PLEASE FOLLOW ALL THE PROHIBITIONS AND EXCEPTIONAL CAVEATS OF ALL APPLICABLE LAWS AND REGULATIONS, IN PARTICULAR, THE LOCAL FIREARMS AND/OR HUNTING LAWS AND REGULATIONS. PLEASE ALWAYS CHECK NATIONAL PROVISIONS AND REGULATIONS BEFORE PURCHASE OR USE OF THIS PRODUCT. PLEASE NOTE THAT YOU MAY HAVE TO APPLY FOR PERMITS, CERTIFICATES, AND/OR LICENSES BEFORE ANY PURCHASING, SELLING, MARKETING AND/OR USING OF THE PRODUCT. HIKMICRO SHALL NOT BE LIABLE FOR ANY SUCH ILLEGAL OR IMPROPER PURCHASING, SELLING, MARKETING, AND END USES AND ANY SPECIAL, CONSEQUENTIAL,INCIDENTAL, OR INDIRECT DAMAGES ARISING THEREOF.

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

Symbol Conventions

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

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

Safety Instruction

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

Laws and Regulations

- In the use of the product, you must be in strict compliance with the electrical safety regulations of the nation and region.

Transportation

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

Power Supply

- Check the input voltage before powering on the device to avoid damage.
- CAUTION: If the fuse of the device can be replaced, replace it only with the same model to reduce the risk of fire or electric shock.
- If a fuse is connected to the neutral wire and a double pole/neutral fusing occurs, parts of the device that remain energized might represent a hazard during servicing after operation of the fuse.
- If the device uses a 3-prong power supply plug, it must be connected to an earthed mains socket-outlet properly.
- Do not touch the bare components (such as the metal contacts of the inlets) and wait for at least 5 minutes, since electricity may still exist after the device is powered off.
- For the permanently connected device without a disconnect equipment, a readily accessible disconnect equipment shall be incorporated into the electrical installation of the connected building.
- For the permanently connected device without an overcurrent protection equipment, an overcurrent protection equipment shall be incorporated into the electrical installation of the connected building. The specifications of the overcurrent protection equipment shall not exceed that of the building.
- For the permanently connected device without an all-pole mains switch, an all-pole mains switch shall be incorporated into the electrical installation of the connected building.
- If the device is powered by terminals connected to the power cord, ensure correct voltage and wiring of the terminals for connection to mains supply.

- Please purchase the charger by yourself. Input voltage should meet the Limited Power Source (12 VDC, 24 VAC, or PoE(802.3af)) according to the IEC62368 standard. Please refer to technical specifications for detailed information.
- Make sure the plug is properly connected to the power socket.
- The socket-outlet shall be installed near the equipment and shall be easily accessible.
- DO NOT connect multiple devices to one power adapter, to avoid over-heating or fire hazards caused by overload.
- DO NOT touch the bare metal contacts of the inlets after the circuit breaker is turned off. Electricity still exists.
- + identifies the positive terminal(s) of equipment which is used with, or generates direct current. - identifies the negative terminal(s) of equipment which is used with, or generates direct current.

Battery

- Risk of explosion if the battery is replaced by an incorrect type. Dispose of used batteries according to the instructions.
- The built-in battery cannot be dismantled. Please contact the manufacture for repair if necessary.
- For long-term storage of the battery, make sure it is fully charged every half year to ensure the battery quality. Otherwise, damage may occur.
- This equipment is not suitable for use in locations where children are likely to be present.
- Improper replacement of the battery with an incorrect type may defeat a safeguard (for example, in the case of some lithium battery types).
- DO NOT dispose of the battery into fire or a hot oven, or mechanically crush or cut the battery, which may result in an explosion.
- DO NOT leave the battery in an extremely high temperature surrounding environment, which may result in an explosion or the leakage of flammable liquid or gas.
- DO NOT subject the battery to extremely low air pressure, which may result in an explosion or the leakage of flammable liquid or gas.

Installation

- This device is suitable for use above 2 m only.
- Install the device according to the instructions in Quick Start Guide. To prevent injury, this device must be securely attached to the installation surface in accordance with the installation instructions.
- Never place the device in an unstable location. The device may fall, causing serious personal injury or death.
- The additional force shall be equal to three times the weight of the device but not less than 50 N. The device and its associated mounting means shall remain secure during the installation. After the installation, the device, including any associated mounting plate, shall not be damaged.

- Never place the equipment in an unstable location. The equipment may fall, causing serious personal injury or death.
- This equipment is for use only with corresponding brackets. Use with other (carts, stands, or carriers) may result in instability causing injury.
- The interface varies with the models. Please refer to the product datasheet for details.
- If the device needs to be wired by yourself, select the corresponding wire to supply power according to the electric parameters labeled on the device. Strip off wire with a standard wire stripper at corresponding position. To avoid serious consequences, the length of stripped wire shall be appropriate, and conductors shall not be exposed.
- Make sure that the power has been disconnected before you wire, install, or disassemble the device.

System Security

- You acknowledge that the nature of Internet provides for inherent security risks, and our company shall not take any responsibilities for abnormal operation, privacy leakage or other damages resulting from cyber attack, hacker attack, however, our company will provide timely technical support if required.
- Please enforce the protection for the personal information and the data security as the device may be confronted with the network security problems when it is connected to the Internet. Please contact us when the device might exist network security risks.
- Please understand that you have the responsibility to configure all the passwords and other security settings about the device, and keep your user name and password.

Maintenance

- If the product does not work properly, please contact your dealer or the nearest service center. We shall not assume any responsibility for problems caused by unauthorized repair or maintenance.
- Wipe the device gently with a clean cloth and a small quantity of ethanol, if necessary.
- If the equipment is used in a manner not specified by the manufacturer, the protection provided by the device may be impaired.
- To reduce the risk of fire, replace only with the same type and rating of fuse.
- The serial port of the equipment is used for debugging only.

Using Environment

- Make sure the running environment meets the requirement of the device. The operating temperature shall be -40°C to 65°C (-40°F to 149°F), and the operating humidity shall be 95% or less, no condensing.
- DO NOT expose the device to high electromagnetic radiation or dusty environments.
- DO NOT aim the lens at the sun or any other bright light.
- The equipment shall not be exposed to dripping or splashing and that no objects filled with liquids, such as vases, shall be placed on the equipment.
- No naked flame sources, such as lighted candles, should be placed on the equipment.

- For the device with ventilation openings, the ventilation openings should not be impeded by covering the ventilation openings with items, such as newspapers, table-cloths, and curtains. The openings shall never be blocked by placing the device on a bed, sofa, rug, or other similar surface.
- Keep a proper distance around the device for sufficient ventilation.
- This device is suitable for mounting on concrete or other non-combustible surface only to avoid fire hazard.
- This equipment is not suitable for use in locations where children are likely to be present.
- Provide a surge suppressor at the inlet opening of the equipment under special conditions such as the mountain top, iron tower, and forest.
- Burned fingers when handling the parts with symbol  . Wait one-half hour after switching off before handling the parts.

Emergency

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

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

Contents

Chapter 1 Overview

1.1 Brief Description

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

1.2 Function

This section introduces main functions of the device.

Note

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

Fire and Smoke Detection

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

Temperature Measurement

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

Perimeter Protection

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

Chapter 2 Device Activation and Accessing

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

Note

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

2.1 Activate Device

The device needs to be activated by setting a strong password before use. This part introduces activation using different client tools.

2.1.1 Activate the Device via Browser

You can access and activate the device via the browser.

Steps

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

   Note

   The default IP address of the device is 192.168.1.64. You can set the IP address of the computer from 192.168.1.2 to 192.168.1.253 (except 192.168.1.64). For example, you can set the IP address of the PC to 192.168.1.100.
3. Input *192.168.1.64* in the browser.
4. Set device activation password.

   Caution

   We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.
5. Click **OK**.
6. Input the activation password to log in to the device.
7. **Optional:** Go to **Configuration > Network > Basic > TCP/IP** to change the IP address of the device to the same segment of your network.

2.1.2 Activate the Device via SADP

Search and activate the online devices via SADP software.

Before You Start

Access *https://www.hikmicrotech.com* to get SADP software to install.

Steps

1. Connect your computer to the same Wi-Fi network that the device is in.
2. Run SADP software to search the online devices of the LAN.
3. Check **Device Status** from the device list, and select **Inactive** device.
4. Create and input the new password in the password field, and confirm the password.

   Caution

   We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.
5. Click **OK**.

   Device Status changes into **Active**.
6. **Optional:** Change the network parameters of the device in **Modify Network Parameters**.

2.2 Login

Log in to the device via Web browser.

2.2.1 Plug-in Installation

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

Operating System	Web Browser	Operation
Windows	Internet Explorer 10+	Follow pop-up prompts to complete plug-in installation.
	Google Chrome 57+ Mozilla Firefox 52+ Microsoft Edge 79.0.309+	Click Download Plug-in to download and install plug-in. Go to **Configuration > Network > Advanced**

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

Note

The device only supports Windows and Mac OS system and does not support Linux system.

2.2.2 Illegal Login Lock

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

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

Illegal Login Attempts

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

Locking Duration

The device releases the lock after the setting duration.

Chapter 3 Network Settings

3.1 TCP/IP

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

Go to **Configuration > Network > Network Settings > TCP/IP** for parameter settings.

NIC Type

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

IPv4

Two IPv4 modes are available.

DHCP

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

Note

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

Manual

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

IPv6

Three IPv6 modes are available.

Route Advertisement

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

Note

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

DHCP

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

Manual

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

MTU

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

The valid value range of MTU is 1280 to 1500.

DNS

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

Domain Name Settings

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

Note

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

3.1.1 Multicast Discovery

Go to **Configuration > Network > Network Settings > TCP/IP** to enable this function.

Check the **Enable Multicast Discovery**, and then the online network camera can be automatically detected by client software via private multicast protocol in the LAN.

3.2 Access to Device via Domain Name

You can use the Dynamic DNS (DDNS) for network access. The dynamic IP address of the device can be mapped to a domain name resolution server to realize the network access via domain name.

Before You Start

Registration on the DDNS server is required before configuring the DDNS settings of the device.

Steps

1. Refer to *TCP/IP* to set DNS parameters.
2. Go to the DDNS settings page: **Configuration > Network > Network Settings > DDNS** .
3. Check **Enable** and select **DDNS Type**.

DynDNS

Dynamic DNS server is used for domain name resolution.

NO-IP

NO-IP server is used for domain name resolution.

4. Input the domain name information, and click **Save**.
5. Check the device ports and complete port mapping. Refer to *Port Mapping* for port mapping settings.
6. Access the device.

By Browsers	Enter the domain name in the browser address bar to access the device.
By Client Software	Add domain name to the client software. Refer to the client manual for specific adding methods.

3.3 Access to Device via PPPoE Dial Up Connection

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

Steps

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

Dynamic IP

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

User Name

User name for dial-up network access.

Password

Password for dial-up network access.

Confirm

Input your dial-up password again.

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

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

Note

The obtained IP address is dynamically assigned via PPPoE, so the IP address always changes after rebooting the camera. To solve the inconvenience of the dynamic IP, you

need to get a domain name from the DDNS provider (e.g. DynDns.com). Refer to ***Access to Device via Domain Name*** for detail information.

3.4 SNMP

You can set the SNMP (Simple Network Management Protocol) to get device information in network management.

Before You Start

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

Steps

1. Go to **Configuration > Network > Network Settings > SNMP** .
2. Check **Enable SNMPv1**, **Enable SNMP v2c** or **Enable SNMPv3**.

   Note

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

3.5 Set IEEE 802.1X

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

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

Set **Protocol** and **EAPOL Version** according to router information.

Protocol

EAP-TLS and EAP-MD5 are selectable

EAP-MD5

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

EAP-TLS

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

EAPOL Version

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

3.6 Set QoS

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

Note

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

Steps

1. Go to **Configuration > Network > Network Settings > QoS** .
2. Set **Video/Audio DSCP**, **Event/Alarm DSCP** and **Management DSCP**.

   Note

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

3.7 HTTP(S)

HTTP is an application-layer protocol for transmitting hypermedia documents. HTTPS is a network protocol that enables encrypted transmission and identity authentication, which improves the security of remote access.

Steps

1. Go to **Configuration > Network > Network Service > HTTP(S)** .
2. Enter **HTTP Port**.

   Note

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

   Note

   You can click **TLS Settings** to set the TLS version that the device supports. Refer to ***TLS*** or details.
4. Enter **HTTPS Port**.
5. **Optional:** Check **HTTPS Browsing** to access the device only via HTTPS protocol.
6. Select **Server Certificate**.

7. Set **Web Authentication**.

   Authentication

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

   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.
8. Click **Save**.

3.8 Multicast

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

Go to **Configuration > Network > Network Settings > TCP/IP** to set IP address, i.e., the address of multicast host.

For a device with more than one channel, multicast can be set independently for each channel.

3.9 RTSP

RTSP (Real Time Streaming Protocol) is an application-layer controlling protocol for streaming media.

Steps

1. Go to **Configuration > Network > Network Service > RTSP** .
2. Enter **Port**.
3. Set **Multicast** parameters.

   Stream Type

   The stream type as the multicast source.

   Video Port

   The video port of the selected stream.
4. Set **RTSP Authentication**.

   Authentication

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

the device supports digest or basic authentication. If you select **digest**, the device only supports digest authentication.

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.

5. Click **Save**.

3.10 Set SRTP

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

Steps

1. Go to **Configuration > Network > Network Service > SRTP** .
2. Enter the **Port** number.
3. Set **Multicast** parameters.

   Stream Type

   The stream type as the multicast source.

   Video Port

   The video port of the selected stream.
4. Select **Server Certificate**.
5. Select **Encrypted Algorithm**.
6. Click **Save**.

Note

- Only certain device models support this function.
- If the function is abnormal, check if the selected certificate is abnormal in *Certificate Management* .

3.11 Bonjour

It is an implementation of zero-configuration networking (zeroconf), a group of technologies that includes service discovery, address assignment, and hostname resolution. Bonjour locates devices such as printers, other computers, and the services that those devices offer on a local network using multicast Domain Name System (mDNS) service records.

Go to **Configuration > Network > Network Service > Bonjour** to enable the function, and click **Save**.

After enabling the function, the device spread and receive service information in local area network.

3.12 WebSocket(s)

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

Go to **Configuration > Network > Network Service > WebSocket(s)** to set parameters, and click **Save**.

WebSocket

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

WebSockets

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

3.13 Modbus Communication

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

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

Go to **Configuration > Network > Network Service > Modbus** to configure the Modbus.

3.13.1 Set Modbus Main Mode

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

Steps

1. Select the **Device Mode** as **Main**.
2. Check to enable the function of transmitting data via Modbus.
3. Click **Add** to configure the transmission parameters between the device and the subordinate.

Subordinate Name

Customized subordinate for distinguishing between different subordinates.

Connection type

Note

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

TCP

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

RS-485

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

Response Timeout(s)

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

Upload Interval(s)

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

4. Click **OK** to view the status.
5. Click **Test** to refresh the status.

Note

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

6. Configure the contents to be uploaded to the registers of subordinate.
   1) Click **Add**.
   2) Check the contents to be uploaded.
   3) Select the Rule ID to be uploaded, and the device uploads the temperature measurement information corresponding to the expert temperature measurement rule.
   4) Enter the register starting address and register ending address.

Note

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

5) Click **OK**.

7. Click **Save**.

3.13.2 Set Modbus Subordinate Mode

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

Steps

Note

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

1. Select the **Device Mode** as **Subordinate**.
2. Select Register Mode.

   Register Mode

   Read Only
   The client can only read all the register data.

   Read/Write
   The client can read while configure the device using the Modbus TCP protocol.
3. Check **Enable Authorized IP Addresses** and click **Add** to add IP addresses that are allowed to access to the device.

   Note

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

3.13.3 Modbus Error Code Description

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

Table 3-1 Modbus Error Code Description

Error Code	Name	Description
01	Illegal Function	The function code received in the query is not an allowable action for the server. This may be because the function code is only applicable to newer devices, and was not implemented in the unit selected. It could also indicate that the server is in the wrong state to process a request of this type, for example because it is unconfigured and is being asked to return register values.
02	Illegal Data Address	The data address received in the query is not an allowable address for the server. More specifically, the combination of reference number and transfer length is invalid. For a controller with 100 registers, the PDU addresses the first register as 0, and the last one as 99. If a request is submitted with a starting register address of 96 and a quantity of registers of 4, then this request will successfully operate (address-wise at least) on registers 96, 97, 98, 99. If a request is submitted with a starting register address of 96 and a quantity of registers of 5, then this request will fail with Exception Code 0x02 “Illegal Data Address” since it attempts to operate on registers 96, 97, 98, 99 and 100, and there is no register with address 100.
03	Illegal Data Value	A value contained in the query data field is not an allowable value for server. This indicates a fault in the structure of the remainder of a complex request, such as that the implied length is incorrect. It specifically does NOT mean that a data item submitted for storage in a register has a value outside the expectation of the application program, since the Modbus protocol is unaware of the significance of any particular value of any particular register.
04	Server Device Failure	An unrecoverable error occurred while the server was attempting to perform the requested action.

Error Code	Name	Description
05	Acknowledge	Specialized use in conjunction with programming commands. The server has accepted the request and is processing it, but a long duration of time will be required to do so. This response is returned to prevent a timeout error from occurring in the client. The client can next issue a Poll Program Complete message to determine if processing is completed.
06	Server Device Busy	Specialized use in conjunction with programming commands. The server is engaged in processing a long– duration program command. The client should retransmit the message later when the server is free.
08	Memory Parity Error	Specialized use in conjunction with function codes 20 and 21 and reference type 6, to indicate that the extended file area failed to pass a consistency check. The server attempted to read record file, but detected a parity error in the memory. The client can retry the request, but service may be required on the server device.
10	Gateway Path Unavailable	Specialized use in conjunction with gateways, indicates that the gateway was unable to allocate an intern communication path from the input port to the output port for processing the request. Usually means that the gateway is misconfigured or overload.
11	Gateway Target Device Failed to Response	Specialized use in conjunction with gateways, indicates that no response was obtained from the target device. Usually means that device is not present on the network.

3.14 Port Mapping

By setting port mapping, you can access devices through the specified port.

Steps

1. Go to **Configuration > Network > Network Service > NAT** .
2. Select the port mapping mode.

Auto Port Mapping	Refer to ***Set Auto Port Mapping*** for detailed information.
Manual Port Mapping	Refer to ***Set Manual Port Mapping*** for detailed information.

3. Click **Save**.

3.14.1 Set Auto Port Mapping

Steps

1. Check **Enable UPnP™**, and choose a friendly name for the camera, or you can use the default name.
2. Select the port mapping mode to **Auto**.
3. Click **Save**.

Note

UPnP™ function on the router should be enabled at the same time.

3.14.2 Set Manual Port Mapping

Steps

1. Check **Enable UPnP™**, and choose a friendly name for the device, or you can use the default name.
2. Select the port mapping mode to **Manual**, and set the external port to be the same as the internal port.
3. Click **Save**.

What to do next

Go to the router port mapping settings interface and set the port number and IP address to be the same as those on the device. For more information, refer to the router user manual.

3.15 Set OTAP

The device can be accessed to the maintenance platform via OTAP protocol, in order to search and acquire device information, upload device status and alarm information, reboot and update the device.

Steps

1. Go to **Configuration > Network > Advanced Settings > Platform Access** to enable the function.
2. Set related parameters.
3. Click **Test** to check if the device connects to server.
4. Click **Save**.

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

3.16 Set ISUP

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

Steps

1. Go to **Configuration > Network > Platform Access > ISUP** .
2. **Optional:** Select an access center.
3. Check **Enable**.
4. Select a protocol version and enter related parameters.
5. Click **Save**.

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

3.17 Access Camera via Hik-Connect

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

Before You Start

Connect the camera to network with network cables.

Steps

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

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

3.17.1 Enable Hik-Connect Service on Camera

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

You can enable the service through Web browser.

Enable Hik-Connect Service via Web Browser

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

Before You Start

You need to activate the camera before enabling the service.

Steps

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

   Note

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

Enable Hik-Connect Service via SADP Software

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

Steps

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

   Note

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

3.17.2 Set Up Hik-Connect

Steps

1. Download Hik-Connect from *https://www.hik-connect.com* and install it on your mobile device.
2. Start the application and register for a Hik-Connect user account.
3. Log in after registration.

3.17.3 Add Camera to Hik-Connect

Steps

1. Connect your mobile device to a Wi-Fi.
2. Log into the Hik-Connect app.
3. In the home page, tap "+" on the upper-right corner to add a camera.
4. Scan the QR code on camera body or on the *Quick Start Guide* cover.

   Note

   If the QR code is missing or too blur to be recognized, you can also add the camera by inputting the camera's serial number.
5. Input the verification code of your camera.

   Note

   - The required verification code is the code you create or change when you enable Hik-Connect service on the camera.
   - If you forget the verification code, you can check the current verification code on **Platform Access** configuration page via web browser.
6. Tap **Connect to a Network** button in the popup interface.
7. Choose **Wired Connection** or **Wireless Connection** according to your camera function.

Wireless Connection	Input the Wi-Fi password that your mobile phone has connected to, and tap **Next** to start the Wi-Fi connection process. (Locate the camera within 3 meters from the router when setting up the Wi-Fi.)
Wired Connection	Connect the camera to the router with a network cable and tap **Connected** in the result interface.

   Note

   The router should be the same one which your mobile phone has connected to.
8. Tap **Add** in the next interface to finish adding.

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

3.18 Set Open Network Video Interface

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

Steps

1. Go to **Configuration > Network > Platform Access > Open Network Video Interface** .
2. Check **Enable**.
3. Select an authentication mode.
   - If you select **Digest**, the device only supports digest authentication.

- If you select **Digest&ws-username token**, the device supports digest authentication or ws-username token authentication.

4. Click **Add** to configure the Open Network Video Interface user.
5. Click **Save**.
6. **Optional:** Repeat the steps above to add more Open Network Video Interface users.
7. **Optional:** Manage the user.
   - Click to delete the selected Open Network Video Interface user.
   - Click to modify the selected Open Network Video Interface user.

3.19 Set SDK Service

If you want to add the device to the client software, you should enable SDK Service.

Steps

1. Go to **Configuration > Network > Platform Access > SDK Service** .
2. Enter the **Port** number.
3. Click **Save**.

Chapter 4 Live View

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

4.1 Live View Parameters

The supported functions vary depending on the model.

Note

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

4.1.1 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.

4.1.2 Live View Stream Type

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

4.1.3 Enable and Disable Live View

This function is used to quickly enable or disable live view of all channels.

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

Note

Go to **Configuration > Local** , to set **Auto Start Live View**, If **Yes** is selected, live view will start automatically when you go to live view.

4.1.4 Start Digital Zoom

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

Steps

1. Click to enable the digital zoom.

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

4.1.5 View Previous/Next Page

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

Click ← → to switch live view among multiple channels.

4.1.6 Full Screen

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

Click to start full screen mode and press ESC button to exit.

4.1.7 Light

Click to turn on or turn off the illuminator.

Caution

- DO NOT stare at operating light source. May be harmful to the eyes.
- If appropriate shielding or eye protection is not available, turn on the light only at a safe distance or in the area that is not directly exposed to the light.
- When assembling, installing or maintaining the device, DO NOT turn on the light, or wear eye protection.

4.1.8 Wiper

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

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

4.1.9 Lens Initialization

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

Click to operate lens initialization.

4.1.10 Auxiliary Focus

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

4.1.11 Quick Set Live View

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

Steps

1. Click to show quick setup page.
2. Set PTZ, display settings, OSD, video/audio and VCA resource parameters.
   - For PTZ settings, see ***Lens Parameters Adjustment***.
   - For display settings, see ***Display Settings***.
   - For OSD settings, see ***OSD***.
   - For audio and video settings, see ***Video and Image Settings***.
   - For VCA settings, see ***Fire and Smoke Detection***, ***Temperature Measurement***, and ***Perimeter Protection***.

Note

The function is only supported by certain models.

4.1.12 Lens Parameters Adjustment

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

Zoom

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

Focus

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

Iris

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

Note

The function is only supported by certain models.

4.2 Set Transmission Parameters

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

Steps

1. Go to **Configuration > Local > Live View Parameters** .
2. Set the transmission parameters as required.

Protocol

TCP

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

UDP

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

MULTICAST

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

Note

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

HTTP

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

Playing Performance

Shortest Delay

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

Balanced

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

Fluent

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

Custom

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

Auto Start Live View

- **Yes** means the live view is started automatically. It requires a high performance monitoring device and a stable network environment.
- **No** means the live view should be started manually.

3. Click **Save**.

4.3 Set Rule Display

You can set the rule display of target object in live view or captured picture.

Go to **Configuration > Local > Live View Parameter** to set the parameters.

Rules

Display rule info. in live view, such as the rule area of motion detection event and VCA resources.

Display POS Info

Display target ID and attributes in main stream recordings. The attribute type depends on the model and function of different device, and the actual device prevails.

Display Rules Info on Capture

Display rule info (e.g., alarm area and rule area) on captured pictures. The attribute type depends on the model and function of different device, and the actual device prevails.

Display Temperature Info.

Display the highest and lowest as well as the point, line and area temperature value.

Chapter 5 Video and Image Settings

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

5.1 Video Settings

This part introduces the settings of video parameters, such as, stream type, video encoding, and resolution.

Go to setting page: **Configuration > Video/Audio > Video** .

Note

For device with multiple camera channels, select a channel before other settings.

5.1.1 Stream Type

For device supports more than one stream, you can specify parameters for each stream type.

Main Stream

The stream stands for the best stream performance the device supports. It usually offers the best resolution and frame rate the device can do. But high resolution and frame rate usually mean larger storage space and higher bandwidth requirements in transmission.

Sub Stream

The stream usually offers comparatively low resolution options, which consumes less bandwidth and storage space.

5.1.2 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.

Note

Video & Audio varies according to different camera models.

5.1.3 Resolution

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

5.1.4 Bitrate Type and Max. Bitrate

Constant Bitrate

It means that the stream is compressed and transmitted at a comparatively fixed bitrate. The compression speed is fast, but mosaic may occur on the image.

Variable Bitrate

It means that the device automatically adjust the bitrate under the set **Max. Bitrate**. The compression speed is slower than that of the constant bitrate. But it guarantees the image quality of complex scenes.

5.1.5 Video Quality

When **Bitrate Type** is set as Variable, video quality is configurable. Select a video quality according to actual needs. Note that higher video quality requires higher bandwidth.

5.1.6 Frame Rate

The frame rate is to describe the frequency at which the video stream is updated and it is measured by frames per second (fps).

A higher frame rate is advantageous when there is movement in the video stream, as it maintains image quality throughout. Note that higher frame rate requires higher bandwidth and larger storage space.

5.1.7 Video Encoding

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

Note

Available compression standards vary according to device models.

H.264

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

H.265

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

MJPEG

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

Profile

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

I-Frame Interval

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

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

SVC

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

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

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

5.1.8 Smoothing

It refers to the smoothness of the stream. The higher value of the smoothing is, the better fluency of the stream will be, though, the video quality may not be so satisfactory. The lower value of the smoothing is, the higher quality of the stream will be, though it may appear not fluent.

5.1.9 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.

5.1.10 Audio Settings

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

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

Note

Only certain camera models support the function.

Audio Encoding

Select the audio encoding compression of the audio.

Audio Input

Note

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

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

Environmental Noise Filter

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

5.1.11 Two-way Audio

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

Before You Start

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

Steps

Note

The function varies according to different camera models.

1. Click **Live View**.
2. Click on the toolbar to enable two-way audio function of the camera.
3. Click , disable the two-way audio function.

5.1.12 Set ROI

ROI (Region of Interest) encoding helps to assign more encoding resource to the region of interest, thus to increase the quality of the ROI whereas the background information is less focused.

Before You Start

Please check the video coding type. ROI is supported when the video coding type is H.264 or H.265.

Steps

1. Go to **Configuration > Video/Audio > ROI** .
2. Check **Enable**.
3. Select the channel No. according to your need.
4. Select **Stream Type**.
5. Select **Region No.** in **Fixed Region** to draw ROI region.
   1) Click **Draw Area**.
   2) Click and drag the mouse on the view screen to draw the fixed region.
   3) Click **Stop Drawing**.

   Note

   Select the fixed region that needs to be adjusted and drag the mouse to adjust its position.
6. Input the **Region Name** and **ROI Level**.
7. Click **Save**.

   Note

   The higher the ROI level is, the clearer the image of the detected region is.
8. **Optional:** Select other region No. and repeat the above steps if you need to draw multiple fixed regions.

5.2 Display Settings

It offers the parameter settings to adjust image features.

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

For device that supports multiple channels, display settings of each channel is required. The settings for different channels may be different. This part introduces all possible parameters among the channels.

Click **Default** to restore settings.

5.2.1 Image Adjustment

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

Figure 5-1 Saturation

5.2.2 Image Adjustment (Thermal Channel)

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

Manual Correction

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

Note

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

Thermal AGC Mode

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

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

5.2.3 Exposure Settings

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

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

5.2.4 Day/Night Switch

Day/Night Switch function can provide color images in the day mode and turn on fill light in the night mode. Switch mode is configurable.

Day

The image is always in color.

Night

The supplement light will be enabled to ensure clear live view image at night.

Auto

The camera switches between the day mode and the night mode according to the illumination automatically. The higher the **Sensitivity** is, the easier the mode switches. The **Filtering Time** refers to the time interval between the mode switches.

Scheduled-Switch

Set the **Start Time** and the **End Time** to define the duration for day mode.

Note

Day/Night Switch function varies according to models.

5.2.5 Set Supplement Light

Steps

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

   This feature uses smart image processing technology to reduce overexposure caused by supplement light.

   Smart Supplement Light Mode

   Enable or disable the smart supplement light.

   Brightness Limit

   Adjust the upper limit of supplement light power.

   Light Brightness Control

   Control supplement light brightness automatically or manually.

   Auto

   The brightness adjusts according to the actual environment automatically.

Manual

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

Note

The function varies according to device models.

5.2.6 BLC

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

5.2.7 WDR

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

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

Note

When WDR is enabled, some other functions may be not supported. Refer to the actual interface for details.

Figure 5-2 WDR

5.2.8 White Balance

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

Figure 5-3 White Balance

5.2.9 DNR

Digital Noise Reduction is used to reduce the image noise and improve the image quality. **Normal** and **Expert** modes are selectable.

Normal

Set the DNR level to control the noise reduction degree. The higher level means stronger reduction degree.

Expert

Set the DNR level for both space DNR and time DNR to control the noise reduction degree. The higher level means stronger reduction degree.

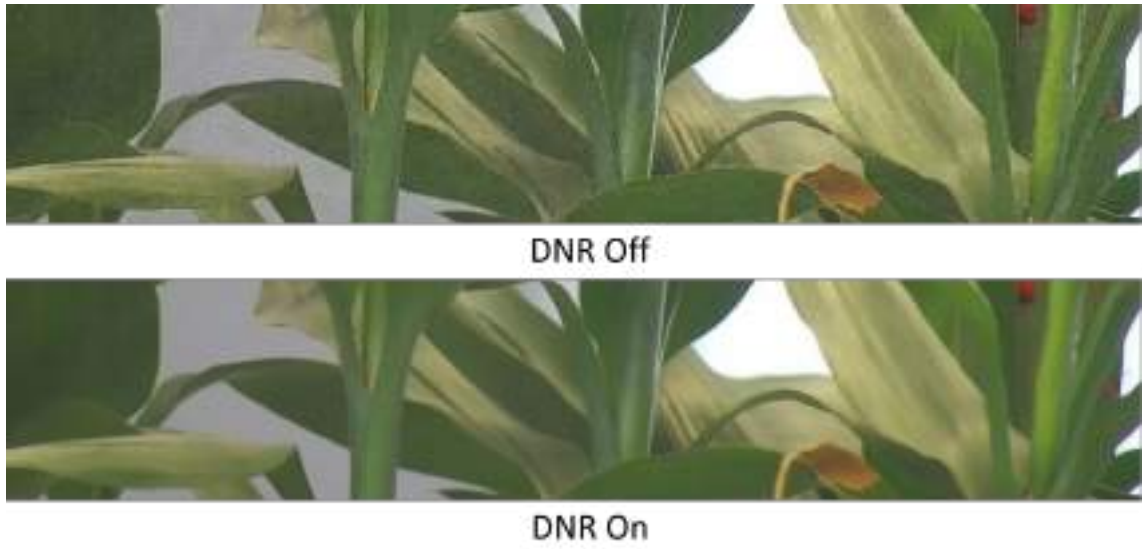

Figure 5-4 DNR

5.2.10 Defog

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

Figure 5-5 Defog

5.2.11 Gray Scale

This section introduces the gray scale function in optical channel.

You can choose the range of the grey scale as [0-255] or [16-235].

5.2.12 Set Palette

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

Steps

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

Result

The live view displays the image with palette.

5.2.13 Set Target Enhancement

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

Steps

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

   Above (be colored)

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

   Between (be colored)

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

   Below (be colored)

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

5.2.14 DDE

Digital Detail Enhancement is used to adjust the details of the image. **OFF** and **Normal** modes are selectable.

OFF

Disable this function.

Normal

Set the DDE level to control the details of the image. The higher the level is, the more details shows, but the higher the noise is.

5.2.15 Brightness Sudden Change

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

5.2.16 Enhance Regional Image

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

Steps

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

5.2.17 Mirror

When the live view image is the reverse of the actual scene, this function helps to display the image normally.

Select the mirror mode as needed.

Note

The video recording will be shortly interrupted when the function is enabled.

5.2.18 Video Standard

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

5.2.19 Digital Zoom

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

5.2.20 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.

5.2.21 Local Output

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

5.3 OSD

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

Go to OSD setting page: **Configuration > Image > OSD Settings** . Set the corresponding parameters, and click **Save** to take effect.

Character Set

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

Displayed Information

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

Text Overlay

Set customized overlay text on image.

OSD Parameters

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

5.4 VCA Rule Display Settings

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

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

5.5 Set Privacy Mask

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

Steps

1. Go to **Configuration > Image > Privacy Mask** .
2. Select the channel No.
3. Check **Enable**.
4. Click . Drag the mouse in the live view to draw a closed area.

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

5. Click **Add** to add a privacy mask and set **Region Name** and **Mask Type**.
6. Click **Save**.

5.6 Overlay Picture

Overlay a customized picture on live view.

Before You Start

The picture to overlay has to be in BMP format with 24-bit, and the maximum picture size is 128 × 128 pixel.

Steps

1. Go to **Configuration > Image > Picture Overlay** .
2. Select a channel to overlay picture.
3. Check **Enable**.
4. Click **Upload** to select a picture and open it.

   The picture with a red rectangle will appear in live view after successfully uploading.
5. Drag the red rectangle to adjust the picture position.
6. Click **Save**.

5.7 Set Manual DPC (Defective Pixel Correction)

If the amount of defective pixels in the image is comparatively small and accurate correction is needed, you can correct these pixels manually.

Steps

1. Go to **Configuration > Image > DPC** .
2. Select the thermal channel.

3. Click the defective pixel on the image, then a cursor shows on the live view.
4. Click **Up**, **Down**, **Left**, **Right** to adjust the cursor position to the defective pixel position.
5. Click , then click to correct defective pixel.

Note

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

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

5.8 Set Picture in Picture

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

Steps

1. Select a channel number.
2. Select the picture in picture mode.

Overlap Mode	Partial image of thermal channel is displayed on the full screen of optical channel. This mode is only supported in **Camera 01**.
Details Overlay	The device displays the details of optical channel on thermal channel. This mode is only supported in **Camera 02**.
Optimized Details Overlay	The device displays more optical details on thermal channel with less palettes color which mainly focuses on the high temperature target. This mode is only supported in **Camera 02**.

Note

The function varies according to different models

3. In **Details Overlay** or **Optimized Details Overlay**, set the **Fusion Distance** of the target to get the best view of bi-spectrum fusion. It is recommended to use the default value.
4. **Optional:** In **Optimized Details Overlay**, set the **Image Fusion Ratio** to adjust the ratio of optical details displayed on thermal channel.
5. Select a **Fusion Type**.

Central Fusion	The device displays the bi-spectrum fusion of scene center. The fusion area is 70% of the whole scene.
Full Screen Fusion	The device displays the bi-spectrum fusion of the whole scene.

6. Click **Save**.

Note

Not all models support this function. Please take the actual product for reference.

Chapter 6 Video Recording and Picture Capture

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

6.1 Storage Settings

This part introduces the configuration of several common storage paths.

6.1.1 Set Memory Card

If you choose to store the files to memory card, make sure you insert and format the memory card in advance.

Before You Start

Insert the memory card to the camera. For detailed installation, refer to *Quick Start Guide* of the camera.

Steps

1. Go to storage management setting page: **Configuration > Storage > Storage Management > HDD Management** .
2. Select the memory card, and click **Format** to start initializing the memory card.

   The **Status** of memory card turns to **Normal** from **Uninitialized**, which means the memory card can be used normally.
3. **Optional:** Define the **Quota** of the memory card. Input the quota percentage for different contents according to your need.
4. **Optional:** Check to enable **POS Information Storage**, then the device will record the POS information of reflect light filter and forklift filter.

   Note

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

6.1.2 Set NAS

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

Before You Start

Get the IP address of the network disk first.

Steps

1. Go to NAS setting page: **Configuration > Storage > Storage Management > Net HDD** .
2. Click **HDD No.**. Enter the server address and file path for the disk.

   Server Address

   The IP address of the network disk.

   File Path

   The saving path of network disk files.

   Mounting Type

   Select file system protocol according to the operation system.

   Enter user name and password of the net HDD to guarantee the security if **SMB/CIFS** is selected.
3. Click **Test** to check whether the network disk is available.
4. Click **Save**.

6.1.3 Set FTP

You can configure the FTP server to save images which are captured by events or a timed snapshot task.

Before You Start

Get the FTP server address first.

Steps

1. Go to **Event Center > Alarm Setting > FTP** .
2. Configure FTP settings.

   Server Address and Port

   The FTP server address and corresponding port.

   User Name and Password

   The FTP user should have the permission to upload pictures.

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

   Directory Structure

   The saving path of snapshots in the FTP server.
3. **Optional:** Check **Upload Picture** to enable uploading snapshots to the FTP server.
4. Click **Test** to verify the FTP server.
5. Click **Save**.

6.1.4 Set Cloud Storage

It helps to upload the captured pictures and data to the cloud. The platform requests picture directly from the cloud for picture and analysis. The function is only supported by certain models.

Steps

Caution

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

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

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

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

6.2 Video Recording

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

6.2.1 Record Automatically

This function can record video automatically during configured time periods.

Before You Start

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

Steps

Note

The function varies according to different models.

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

   Note

   The record type is vary according to different models.

   Continuous

   The video will be recorded continuously according to the schedule.

   Motion

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

   Alarm

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

   Motion | Alarm

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

   Motion & Alarm

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

   Event

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

   Overwrite

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

   Pre-record

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

Post-record

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

Stream Type

Select the stream type for recording.

Note

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

Recording Expiration

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

7. Click **Save**.

6.2.2 Record Manually

Steps

1. Go to **Configuration > Local** .
2. Set the **Video Size** and **Video Saving Path** for recorded video files.
3. Click **Save**.
4. Click in the live view interface to start recording. Click to stop recording.

What to do next

View the recorded video files.
Go to **Configuration > Local** and click **Open** behind **Video Saving Path** to open the saving path and view the files.

6.2.3 Playback and Download Video

You can search, playback, clip and download the videos stored in the local storage or network storage.

Steps

1. Go to **Playback > Video** .
2. Select channel No.
3. Set search condition and click **Search**.

   The matched video files showed on the timing bar.
4. Click to play the video files.
   - Click to play video files in full screen. Press **ESC** to exit full screen.
   - Click to stop video playback for all channels.
5. **Optional:** Click , check the channel, select the time and click to view videos of channel 1 and channel 2 synchronously. Click to view videos asynchronously.

6. **Optional:** Click to clip video files. Click again to stop clipping video files

   Note

   Go to **Configuration > Local > Clip Saving Path** , view and change the saving path of clipped video files.
7. **Optional:** Click on the playback interface to download files.

   Note

   Go to **Configuration > Local > Downloaded File Saving Path** , view and change the saving path of downloaded video files.

6.3 Capture Configuration

The device can capture the pictures manually or automatically and save them in configured saving path. You can view and download the snapshots.

6.3.1 Capture Automatically

This function can capture pictures automatically during configured time periods.

Before You Start

If event-triggered capture is required, you should configure related linkage methods in event settings. Refer to ***Event and Alarm*** for event settings.

Steps

1. Go to **Configuration > Storage > Schedule Settings > Capture > Capture Parameters** .
2. Set the capture type.

   Timing

   Capture a picture at the configured time interval.

   Event-Triggered

   Capture a picture when an event is triggered.
3. Set the **Format**, **Resolution**, **Quality**, **Interval**, and **Capture Number**.
4. Refer to ***Set Arming Schedule*** for configuring schedule time.
5. Click **Save**.

6.3.2 Capture Manually

Steps

1. Go to **Configuration > Local** .
2. Set the **Image Format** and saving path to for snapshots.

   JPEG

The picture size of this format is comparatively small, which is better for network transmission.

BMP

The picture is compressed with good quality.

3. Click **Save**.
4. Click near the live view or play back window to capture a picture manually.

6.3.3 View and Download Picture

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

Steps

1. Go to **Playback > Picture** .
2. Select channel No.
3. Set search condition and click **Search**.

   The matched pictures showed in the file list.
4. Download the pictures.
   - Select the pictures then click **Download** to download them.
   - Click **Download This Page** to download the pictures of this page.
   - Click **Download All** to download all the pictures.

Note

Go to **Configuration > Local > Playback Capture Saving Path** , view and change the saving path of captured pictures when playback.

Chapter 7 VCA Resource

VCA resource is a collection of smart functions supported by the device.

7.1 Temperature Measurement

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

7.1.1 Set Thermography Parameters

Configure the parameters of temperature measurement.

Steps

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

   Display Temperature Info.

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

   Enable **Rules** to display the rules information on live view.
2. Click **Save**.
3. Go to **Event Center > Temperature Measurement > Basic Parameter** to configure parameters.

   Enable Temperature Measurement

   Check to enable temperature measurement function.

   Alarm Mode

   Select an alarm mode as needed, and go to **Temperature Measurement > Temperature Measurement Parameter > Rule** to configure the alarm rules and parameters.

   - Temperature Measurement Alarm: The device sends alarms or pre-alarms when it detects object whose temperature is above the threshold.
   - Interval Temperature Measurement Alarm: The device sends alarms when it detects object whose temperature is within or out of the preset temperature interval.

   Alarm Interval

   Set the alarm interval between two alarms.

   Normal Rule Color

   The color of the interval temperature measurement rule when the rule area is in the normal mode.

   Distance Mode

Set distance mode according to actual application. You can select **Auto** when the target moves in certain area, and select **Fixed** when the target is static.

Enable Color-Temperature

Check to display Temperature-Color Ruler in live view.

Display Temperature Info. on Stream

Check to display temperature information on the stream.

Display Max./Min./Average Temperature

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

Display Position

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

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

Display Rule Name

Display the rule name rather than the rule ID on the live view. You can set the name in expert temperature measurement mode for the rule.

Temperature Unit

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

Temperature Range

Select the temperature measurement range. The device automatically switches its temperature range between available range options according to the measured highest temperature if you select **Auto**.

Overlay & Capture

Go to **Event Center > Temperature Measurement > Temperature Measurement Parameter > Overlay & Capture** to configure whether to enable pixel-to-pixel thermometry data and select alarm rule type..

- Display Pixel-to-Pixel Thermometry Data on Stream: Check to enable pixel-to-pixel thermometry data on stream and select data refresh interval.
- Display Rule Info. on Alarm Picture: Select to display only alarm rule or all rules on alarm pictures, and choose alarm picture quality.

Algorithm Version

Go to **Event Center > Temperature Measurement > Temperature Measurement Parameter > Advanced Configuration** to view the temperature measurement algorithm library and calibration file version.

Note

The settings vary according to different camera models.

4. Click **Save**.

7.1.2 Set Shield Region

You can configure areas from being detected.

Steps

1. Go to **Event Center > Temperature Measurement > Temperature Measurement Parameters > Shield Region** .
2. Check **Enable**.
3. Click . Click and drag the mouse on the live image, and then right click the mouse to finish drawing one area.
4. Drag the mouse in the live view to draw the area. You can drag the corners of the red rectangle area to change its shape and size.
5. **Optional:** Click to clear all the areas.
6. **Optional:** Select one area and click to delete it.
7. Click **Save**.

Note

- Line type thermography rule cannot overlap with shield region.
- If area type thermography rule overlaps with shield region, temperature measurement does not take effect in the overlapped area.
- Shield region cannot contain complete thermography rules.

7.1.3 Automatic Thermography

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

Set Normal Mode

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

Steps

1. Go to **Event Center > Temperature Measurement > Temperature Measurement Parameter > Basic Parameter** , and check **Enable Temperature Measurement**.
2. Refer to ***Set Thermography Parameters*** to set the parameters.
3. Go to **Event Center > Temperature Measurement > Temperature Measurement Parameters > Rule** , and select **Normal**.
4. Configure the thermography parameters.
   1) Set the emissivity of your target.
   2) Set the distance between the target and the device.
5. Configure the alarm parameters of normal mode.

- **Temperature Measurement**: For information about how to configure the parameters, see *Set Temperature Measurement Alarm in Normal Mode* .
- **Interval Temperature Measurement**: For information about how to configure the parameters, see *Set Interval Temperature Measurement Alarm* .

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

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

Note

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

Set Temperature Measurement Alarm in Normal Mode

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

Before You Start

Select **Alarm Mode** as **Temperature Measurement Alarm** first in **Basic Parameter**.

Steps

1. Set the parameters.

Tolerance Temperature

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

Pre-Alarm Temperature

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

Alarm Temperature

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

Pre-Alarm Output and Alarm Output

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

Temperature Sudden Change Alarm

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

2. Save the settings.

Set Interval Temperature Measurement Alarm

In interval temperature measurement alarm mode, the device will output alarm when the detected temperature of the full screen (normal mode) or the thermography rules (expert mode) triggers the set rule.

Before You Start

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

Steps

1. Select an **Alarm Rule** in **Interval Temperature Measurement Alarm** section.
2. Select an **Alarm Type**.

Note

In normal mode, the device measures temperature of the full screen. In expert mode, the device measures the temperature of thermography rules.

3. Check **Alarm Area Rule**, and click **Set** to configure the alarm rule parameters.
4. Edit the interval name, temperature range and alarm rule color.

Note

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

5. Select the alarm output channel.

Note

The function varies according to different models.

6. **Optional:** In expert mode, you can click **Copy to...** to copy current settings for other thermography rules.

Set Expert Mode

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

Steps

1. Go to **Event Center > Temperature Measurement > Temperature Measurement Parameter > Basic Parameter** , check **Enable Temperature Measurement**.
2. Refer to ***Set Thermography Parameters*** to set the parameters.
3. Go to **Configuration > Temperature Measurement > Temperature Measurement Parameter > Rule** , select **Expert**.
4. Select and enable the temperature measurement rules. Please refer to ***Set Thermography Rule*** for setting the rule.
5. Configure the alarm parameters of expert mode.
   - **Temperature Measurement**: For information about how to configure the parameters, see ***Set Temperature Measurement Alarm in Expert Mode*** .
   - **Interval Temperature Measurement**: For information about how to configure the parameters, see ***Set Interval Temperature Measurement Alarm*** .
6. **Optional:** Click **Area's Temperature Comparison** to set the alarm rules and the temperature.
7. Click **Save**.

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

Note

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

Set Thermography Rule

Steps

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

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

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

   Area Please refer to ***Area Thermography*** for detailed configuration.
3. Configure the temperature measurement parameters.

   Emissivity

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

   Distance

   The distance between the target and the device.

   Reflective Temperature

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

4. Click **Save**.

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

Point Thermography

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

Steps

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

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

Line Thermography

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

Steps

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

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

Area Thermography

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

Steps

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

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

Set Temperature Measurement Alarm in Expert Mode

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

Before You Start

Select **Alarm Mode** as **Temperature Measurement Alarm** first in **Basic Parameter**.

Steps

1. Set the parameters.

   Alarm Temperature and Pre-Alarm Temperature

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

   Tolerance Temperature

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

   Filtering Time

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

   Temperature Sudden Change Alarm

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

   Sudden Change Alarm Value

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

   Cycle

   Set the recording period of the temperature change.

2. **Optional:** Set **Area's Temperature Comparison** rules. Select two areas and set the comparison rule, and set the temperature difference threshold. The device alarms when the temperature difference meets the setting value.
3. Save the settings.

Set Interval Temperature Measurement Alarm

In interval temperature measurement alarm mode, the device will output alarm when the detected temperature of the full screen (normal mode) or the thermography rules (expert mode) triggers the set rule.

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

Steps
1. Select an **Alarm Rule** in **Interval Temperature Measurement Alarm** section.
2. Select an **Alarm Type**.

   Note
   In normal mode, the device measures temperature of the full screen. In expert mode, the device measures the temperature of thermography rules.
3. Check **Alarm Area Rule**, and click **Set** to configure the alarm rule parameters.
4. Edit the interval name, temperature range and alarm rule color.

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

   Note
   The function varies according to different models.
6. **Optional:** In expert mode, you can click **Copy to...** to copy current settings for other thermography rules.

7.1.4 Manual Thermography

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

Steps
1. Go to **Configuration > Local** and check **Display Temperature Info.**.
2. Go to **Event Center > Temperature Measurement > Basic Parameter** .
3. Check **Enable Temperature Measurement**.
4. Click **Save**.

5. Go to live view interface and select thermal channel, click . Click any position on the interface to show the real temperature.

7.1.5 Integration

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

Pixel-to-Pixel Thermometry

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

Steps

1. Go to **Event Center > Temperature Measurement > Integration > Pixel-to-Pixel Thermometry** .
2. Configure the parameters.

Emissivity

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

Distance

The distance between the target and the device.

Reflective Temperature

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

Data Length

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

Max. Frame Rate

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

Refreshing Interval of Temperature Mapping Table

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

Display Thermometry Rule Info. on Picture

Check this function, pictures with thermometry rule info will be uploaded.

Upload Thermal Picture

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

Note

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

3. Click **Save**.

Integration Calibration

Integration calibration can improve temperature measurement accuracy. You can configure integration calibration via external optical calibration and temperature rise calibration, depending on whether the integrated device has germanium window. Use **External Optical Calibration** for integrated devices with germanium window, and **Temperature Rise Calibration** for integrated devices without germanium window.

Table 7-1 Integration Calibration

Calibration Type	Calibration Method	
External Optical Calibration	**Optical Transmissivity** Set the optical transmissivity of external optical material (e.g. germanium window) to improve the temperature measuring accuracy. **Calibration Coefficient** Check **Enable Calibration Coefficient** and set the value of calibration coefficient to get the temperature of the external window or optical material automatically. The setting range is 0 to 30. You can obtain the setting value from SDK software. **External Optics/Window Correction** Set the temperature of the external window or optical material (e.g. germanium window) to correct the measured temperature.	
Temperature Rise Calibration You can calibrate the device via temperature	Temperature Calibration	1. Input **Stable Ambient Temperature**. 2. Check **Blackbody Calibration**, and input temperature, emissivity.

Calibration Type	Calibration Method	
calibration or correction file.		3. Check **Enable** to start calibration. 4. Click **Save** to save the settings.
	Correction File	1. Input **Stable Ambient Temperature**. 2. Click , and select the correction file that suits the current mode of the device. 3. Click **Import** and **Enable**. 4. **Optional.** Click **Export** to export the calibration file of the current device mode to apply it to devices used in the same scenarios. 5. Click **Save** to save the settings.

Note

Temperature rise calibration is supported only during the first 30 minutes after the device is powered on.

Persistent Connection Management

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

Steps

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

7.2 Fire and Smoke Detection

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

The detection is applied to fire-prevention purposes in scenic region, forest, tunnel and so on. You can configure the detection parameters. When fire source or smoke is detected, the alarm actions will be triggered.

Note

Not all models support the function. Please take the actual product for reference.

7.2.1 Recommended Scene

This part introduces the recommended scenes of fire source detection and helps you select the appropriate scene.

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

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

7.2.2 Set Fire Detection

To avoid fire source and other potential damage, you can configure the function for certain areas. The detail configuration steps show as below.

Steps

1. Go to **Event Center > Temperature Measurement & Fire Prevention** .
2. Select **Detection Scene**.

   Note

   The auto detection function varies according to different detection scene.
3. Set **Auto Detection**.

Detection Function	Parameter Description
Fire Detection	**Alarm Interval** Set the alarm interval between two alarms. The smaller the value is, the higher the detection frequency is. **Picture Quality** Set quality of the alarm capture. The better the quality is, the sharper the image is, and the larger the file size is. **Display Fire Source Info on Stream** Display a red frame around the fire source on stream when fire occurs. **Sensitivity**

The higher the value is, the more easily the fire source of lower temperature can be detected, and the higher the false alarm rate is.

Smoke Detection

Display Smoke Info on Stream

Display a red frame around the smoke source on stream when smoke occurs.

Sensitivity

The higher the value is, the more easily the smoke can be detected, and the higher the false alarm rate is.

Verification Sensitivity

The higher the value is, the more quickly the device can double-check and identify the smoke, and the higher the false alarm rate is.

Alarm Interval

Set the alarm interval between two alarms. The smaller the value is, the higher the detection frequency is.

Picture Quality

Set quality of the alarm capture. The better the quality is, the sharper the image is, and the larger the file size is.

Smoking Detection

Display Smoking Info on Stream

Display a red frame around the smoking on stream when fire occurs.

Sensitivity

The higher the value is, the more easily the smoking can be detected, and the higher the false alarm rate is.

Verification Sensitivity

The higher the value is, the more quickly the device can double-check and identify the smoking, and the higher the false alarm rate is.

Alarm Interval

Set the alarm interval between two alarms. The smaller the value is, the higher the detection frequency is.

Picture Quality

Set quality of the alarm capture. The better the quality is, the sharper the image is, and the larger the file size is.

4. **Optional:** You can shield certain areas from being detected, refer to ***Set Detection Shield Region*** .
5. Refer to ***Set Arming Schedule*** for setting scheduled time. Refer to ***Linkage Method Settings*** for setting linkage method.

7.2.3 Set Detection Shield Region

Steps

1. Check to enable the function.
2. Click **Draw Area** and drag the mouse in the live view to draw the area. Release the mouse to finish drawing. You can drag the corners of the red rectangle area to change its shape and size or drag the rectangle to the position on your demand.
3. Click **Stop Drawing**. You can click **Clear All** to clear all of the setting areas.
4. Check **Display Shield Area** to show the shield area on the live view.
5. Click **Add** to save the fire detection shield, and it will be listed in the list. You can select a region and click **Delete** to delete it from the list. You can also enable the region or not.
6. Click **Save**.

7.3 Perimeter Protection

The function is used to detect whether there is any target breaking the perimeter protection rules. The device will track the target and alarm when the perimeter protection rule is triggered.

7.3.1 Set Perimeter Protection Rules

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

Steps

1. Go to **Event Center > Perimeter Protection** .
2. Check to enable the function.
3. **Optional:** Check **Enable Fusion** to view optical and thermal image.
4. Set perimeter protection rules.
   1) Click + to add a new rule.
   2) Enter the rule name, and click the drop down menu to select **Rule Type**.

      Line Crossing

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

      Intrusion

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

      Region Entrance

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

      Region Exiting

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

3) Draw the detection rule.

Line Crossing

a. Click to draw a line in the live view.
b. You can drag end points of the line to adjust the position and length.
c. Set the crossing direction. **Bidirectional**, **A-to-B**, or **B-to-A** are selectable.
d. Set **Sensitivity**. The higher the value is, the easier the target can be detected.

Intrusion

a. Click to draw an area in the live view. Right click the mouse to finish drawing.
b. Set **Duration**. When a target intrudes into the set area and stays in the area for more than the set duration, the device triggers an intrusion alarm.
c. Set **Sensitivity**. The higher the value is, the easier the target can be detected.

Region Entrance and Region Exit

a. Click to draw an area in the live view. Right click the mouse to finish drawing. It is recommended to draw three different areas covering the whole detection scene from near to far.

Note

The recommended drawing is optional for some camera models, refer to the pop-up operation guide after you checked **Intelligent Analysis**.

b. Target that enters or exits the set area triggers the region entrance or region exit alarm.

4) Set other parameters for the rule.

Target Detection

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

Scene Mode

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

Note

In distance view, the device cannot classify the target with pixels less than 10*10. The target will be recognized as human directly. So the selection of this item will increase trigger false alarm rate but decrease missing alarm rate.

Background Interference Suppression

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

Note

The parameter is available in optical channel.

Filter by Pixel

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

Note

- The filter configuration is optional for some camera models, refer to the pop-up operation guide after you checked **Intelligent Analysis**.
- You can draw the max. size and min. size rectangles according to the real target in the scene. The recommended size is 1.2 times of the target.

5) Repeat steps above to configure other rules.

Note

You can click to copy the same settings to other rules.

6) Click **Save**.

5. **Optional:** Add more rules and set combined event. This function is used to combine multiple events as alarm conditions of the rule and it only triggers alarm when the rule and all the conditions are triggered simultaneously.
   1) Check **Alarm Trigger Condition**.
   2) Select the condition type. Enable an event first then you can select it as the alarm condition.
   3) Select the event according to the selected condition type. Click **Save**.

Note

- Once a rule has been set as the alarm trigger condition of other rules, it is not supported to set its own trigger condition.
- Alarm trigger conditions cannot be the same of one rule.

6. *Set Arming Schedule* and *Linkage Method Settings* for each rule.
7. **Optional:** You can shield certain areas from being detected. Refer to *Set Perimeter Protection Shield Region* for detailed settings.
8. **Optional:** Set displayed VCA information on stream or picture. Refer to *Set Perimeter Protection Parameters* for detailed settings.
9. **Optional:** Calibrate the camera to improve the accuracy. Refer to *Calibration* for detailed settings.

7.3.2 Set Perimeter Protection Shield Region

You can configure areas from being detected.

Steps

1. Go to **Configuration > Local** , and enable **Display Shield Area**.
2. Go to **Event Center > Perimeter Protection > Shield Region** .
3. Click .

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

7.3.3 Set Perimeter Protection Parameters

Steps

1. Go to **Configuration > Local** .

   Rules

   Enable it to display rules information on live view.

   Display Rules Info. on Capture

   Select **Yes** to display rules information on the capture.
2. Go to **Configuration > Perimeter Protection** .
3. Select the camera channel.
4. Go to **Basic Settings** to configure basic parameters for the channel.

   Display VCA Info. on Stream

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

   Display Target Info. on Alarm Picture

   Select to display the target information on the alarm picture.

   Display Rule Info. on Alarm Picture

   Select to display the rule information on the alarm picture.

   Snapshot Settings

   Select to upload the picture to the surveillance center when the VCA alarm occurs. You can also set the quality of the picture.
5. Click **Save**.

7.3.4 Calibration

You can calibrate the camera first to improve the detection accuracy of perimeter protection. The calibration is optional, take the actual condition for reference.

Note

The function and the path to the calibration page vary according to different camera models.

Calibrate the Camera

Steps

1. Go to **Event Center > Perimeter Protection > Camera Calibration** or **Event Center > Perimeter Protection > Advanced Configuration** .

   Note

   The path varies according to different camera models.
2. Check **Camera Calibration**.
3. Select **Calibration Mode**.
   - For **Self-Learning Calibration**, see *Self-Learning Calibration* .
   - For **Traditional Calibration**, see *Calibrate Automatically* and *Calibrate Manually* .

   Note

   The function varies according to different camera models. If **Calibration Mode** is not supported, see *Calibrate Automatically* and *Calibrate Manually* .

Self-Learning Calibration

The self- learning calibration allows a camera calibration based on the automatic analysis of people height data.

Steps

1. Select **Filter Level**. The higher the level is, the more easily the alarm can be triggered.
2. Check **Camera Calibration**. The device will automatically record and analyze the height range of people at different positions, filtering out the target out of the range.
3. The calibration area is divided into 20 rows. There needs to be a person walking back and forth twice in the white area (uncalibrated) until all the lines turn to green (calibrated). You can pause the calibration process or recalibrate.

Figure 7-1 Calibration Area Lines

4. **Optional:** Check **Manual Correction** and adjust the height range manually.

   Note

   Manual correction requires enough self-learning calibration time or targets.

   1) Select Fig N (1~4).
   2) You can click **Previous** or **Next** to change the target of each figure.
   3) Input the actual height of the target. Click **Save**.

Calibrate Automatically

Before You Start

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

Steps

1. Go to **Event Center > Perimeter Protection > Camera Calibration** or **Event Center > Perimeter Protection > Advanced Configuration** .

   Note

   The path varies according to different camera models.

2. Check **Camera Calibration**.
3. When the person is totally seen in live view, enter the height of person in **Target Height**.

Note

You can set a maximum of two decimal places.

4. Click ▶ to start calibration.

Caution

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

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

Note

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

Result

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

Calibrate Manually

Steps

1. Go to **Event Center > Perimeter Protection > Camera Calibration** or **Event Center > Perimeter Protection > Advanced Configuration** .

Note

The path varies according to different camera models.

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

Note

Draw a calibration line in each figure, and the four calibration lines should be evenly distributed in the same horizontal plane from left to right.

In the four figures, the calibrated object doesn't need to be the same. Select a proper object in each figure.

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

Caution

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

Result

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

Verify the Calibration Result

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

Steps

1. Click .
2. Click , and drag a vertical line in the view.
3. Move the line to the target, then click to 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 person, but also other objects appeared in the view. Such as car, street lamp, etc.

7.3.5 Set Advanced Configuration Parameters

Go to **Event Center > Perimeter Protection > Advanced Configuration** and configure the parameters.

Detection Parameters

Single Alarm

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

Activation Period

Set the duration of the alarm with combined events.

Restore Parameters

Restore Default

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

Restart VCA

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

Note

The settings vary according to different models.

7.4 Open Platform

Open platform allows you to install the application for the third-party to develop and run its function and service.

Note

Only certain device models support the function.

7.4.1 Set Open Platform

You can install the application for the third-party to develop and run its function and service. For the device supporting this function, you can follow the steps to import and run smart applications.

Steps

1. Go to **Open Platform** interface.

   Note

   Before installing the application, make sure that the application you want to install fit the following conditions.

   - Each application has its own exclusive name.
   - The FLASH memory space that the application takes up is less than the available FLASH memory space of the device.
   - The memory and computing power of the application is less than that available memory and computing power of the device.

2. In **Apps**, click **Import Application**.
3. Click **Browse** to select an application package.
4. Click **Import** to import the package. You can click the APP to view relevant details.
5. **Optional:** Set application.

Click	Enable or disable the application.
Click ✕	Delete the application.
Click **Download Logs**	Export log.
Click **Update**	Browse a local path and import an application package to update the application.

Figure 7-2 Set VCA Resource

Chapter 8 Event and Alarm

This part introduces the configuration of events. The device takes certain response to triggered alarm. Certain events may not be supported by certain device models.

8.1 Set Motion Detection

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

Steps

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

8.1.1 Normal Mode

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

Steps

1. Select **Normal Mode** in **Configuration**.
2. Set the **Sensitivity** of normal mode. The higher the value of sensitivity is, the more sensitive the motion detection is. If the sensitivity is set to *0*, motion detection and dynamic analysis do not take effect.
3. Set **Detection Target**. Human and vehicle are available. If the detection target is not selected, all the detected targets will be reported, including the human and vehicle. This function allows alarm triggering by specified target types (human and vehicle).

Note

This function is only available for certain device models under certain settings. Please refer to the actual settings.

4. Click . Click and drag the mouse on the live image, and then right click the mouse to finish drawing one area.
5. **Optional:** Click to clear all the areas.
6. **Optional:** You can set the parameters of multiple areas by repeating the above steps.

8.1.2 Expert Mode

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

Steps

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

   Scheduled Image Settings

   OFF: Switch is disabled.

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

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

   Note

   This function is not supported in the expert mode of thermal channel.

   Sensitivity

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

   Stop Drawing Finish drawing one area.

   Clear All Delete all the areas.
4. **Optional:** Repeat the above steps to set multiple areas.

8.2 Set Video Tampering Alarm

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

Steps

1. Go to **Event Center > Basic Event > Video Tampering** .
2. Select the channel number.

3. Check **Enable**.
4. Set the **Sensitivity**. The higher the value is, the easier to detect the area covering.
5. Click and drag the mouse in the live view to draw the area.

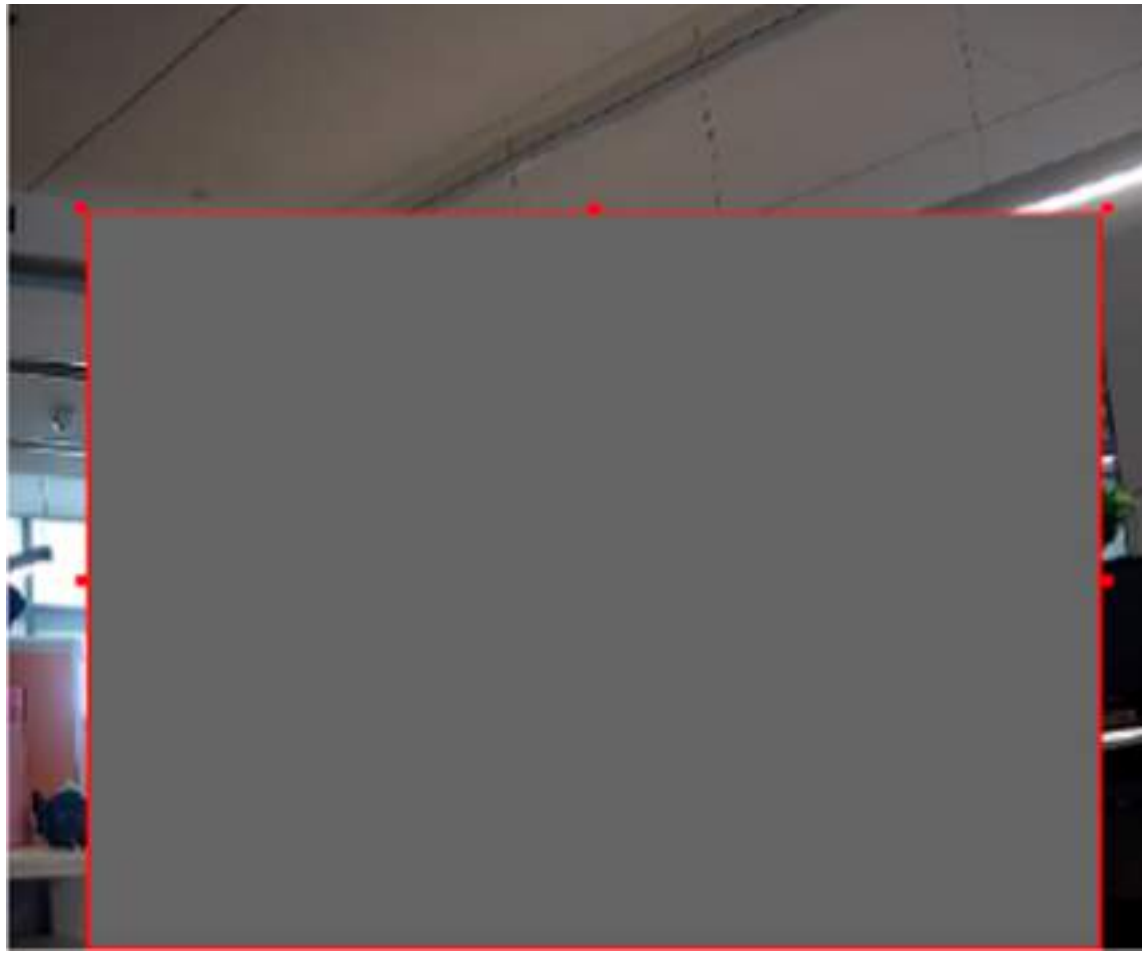

Figure 8-1 Set Video Tampering Area

6. **Optional:** Click to delete all the drawn areas.
7. Refer to ***Set Arming Schedule*** for setting scheduled time. Refer to ***Linkage Method Settings*** for setting linkage method.
8. Click **Save**.

8.3 Set Alarm Input

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

Before You Start

Note

This function is only supported by certain models.

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

Steps

1. Go to **Event Center > Basic Event > Alarm Input** .
2. Select an **Alarm Input NO.** and click to set alarm input.
3. Select **Alarm Type** from the dropdown list. Edit the **Alarm Name**.
4. Check **Enable Alarm Input Handling**.
5. Refer to ***Set Arming Schedule*** for setting scheduled time. Refer to ***Linkage Method Settings*** for setting linkage method.
6. Click **Save**.

8.4 Set Exception Alarm

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

Steps

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

HDD Full	The HDD storage is full.
HDD Error	Error occurs in HDD.
Network Disconnected	The device is offline.
IP Address Conflicted	The IP address of current device is same as that of other device in the network.
Illegal Login	Incorrect user name or password is entered.
Calibration File Exception	The calibration file is modified or deleted. The temperature accuracy may be affected.

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

8.5 Detect Audio Exception

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

Steps

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

   Audio Loss Detection

   Detect sudden loss of audio track.

   Sudden Increase of Sound Intensity Detection

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

   Note

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

   Sudden Decrease of Sound Intensity Detection

   Detect sudden decrease of sound intensity. **Sensitivity** is configurable.
3. Refer to ***Set Arming Schedule*** for setting scheduled time. Refer to ***Linkage Method Settings*** for setting linkage methods.
4. Click **Save**.

Note

The function varies according to different models.

8.6 Set Scene Change Detection

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

Steps

1. Go to **Configuration > Event > Event and Detection > Scene Change Detection** .
2. Select a channel No.
3. Click **Enable**.

4. Set the **Sensitivity**. The higher the value is, the more easily the change of scene can be detected. But the detection accuracy is reduced.
5. Refer to ***Set Arming Schedule*** for setting scheduled time. Refer to ***Linkage Method Settings*** for setting linkage method.
6. Click **Save**.

Note

The function is only supported by certain models. The actual display varies with models.

8.7 Module Order

You can connect the device with the third-party alarm host based on the customized module order, such as HTTP order.

Steps

1. Go to **Event Center > Basic Event > Module Order** .
2. Go to **HTTP Order** and check **Enable**.
3. Select the HTTP order from the list and input URL to configure the HTTP server. Up to 10 HTTP orders are supported.
4. **Optional:** Input the username and password if required.
5. Click **Test** to test the HTTP server connection.

   You can select configured HTTP orders as the linkage method of smart events including **Alarm Input**, **Perimeter Protection**, and **Temperature Measurement**. The alarm or pre-alarm information will upload to the selected HTTP server.

Note

HTTP order linkage is only supported when you check **Enable**.

Chapter 9 Arming Schedule and Alarm Linkage

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

9.1 Set Arming Schedule

Set the valid time of the device tasks.

Steps

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

   Note

   Up to 8 periods can be configured for one day.
3. Adjust the time period.
   - Click on the selected time period, and enter the desired value. Click **Save**.
   - Click on the selected time period. Drag the both ends to adjust the time period.
   - Click on the selected time period, and drag it on the time bar.
4. **Optional:** Click **Copy to...** to copy the same settings to other days.
5. Click **Save**.

9.2 Linkage Method Settings

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

9.2.1 Trigger Alarm Output

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

Steps

1. Go to **Event Center > Alarm Setting > 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*** .

Automatic Alarm

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

Steps

1. Set automatic alarm parameters.
   Alarm Output No.
   Select the alarm output No. according to the alarm interface connected to the external alarm device.
   Alarm Name
   Custom a name for the alarm output.
   Delay
   It refers to the time duration that the alarm output remains after an alarm occurs.
2. Set the alarming schedule. For the information about the settings, see ***Set Arming Schedule***.
3. Click **Copy to...** to copy the parameters to other alarm output channels.
4. Click **Save**.

Manual Alarm

You can trigger an alarm output manually.

Steps

1. Set the manual alarm parameters.
   Alarm Output No.
   Select the alarm output No. according to the alarm interface connected to the external alarm device.
   Alarm Name
   Edit a name for the alarm output.
   Delay
   Select **Manual**.
2. Click **Manual Alarm** to enable manual alarm output.
3. **Optional:** Click **Clear Alarm** to disable manual alarm output.

Alarm Output Self-Check

You can enable the function to regularly self-check the connection between the device and the alarm server.

Steps

1. Check **Enable Auto Trigger**.
2. Set **Trigger Time**, and the device will trigger an alarm output to the alarm server automatically in the set time.
3. Set **Auto Trigger Delay**. It refers to the time duration that the alarm output remains in effect after the auto trigger.
4. Click **Save**.

9.2.2 FTP/NAS Uploading

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

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

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

Refer to ***Set Memory Card*** for disk storage configuration.

9.2.3 Send Email

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

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

Set Email

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

Before You Start

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

Steps

1. Go to email settings page: **Event Center > General Parameter > Alarm Setting > Email** .
2. Set email parameters.
   1) Input the sender's email information, including the **Sender's Address**, **SMTP Server**, and **SMTP Port**.
   2) **Optional:** If your email server requires authentication, check **Authentication** and input your user name and password to log in to the server.
   3) Set the **E-mail Encryption**.

- When you select **TLS**, and disable STARTTLS, emails are sent after encrypted by TLS. The SMTP port should be set as 465.
- When you select **TLS** and check **Enable STARTTLS**, emails are sent after encrypted by STARTTLS, and the **SMTP Port** should be set as 25.

Note

If you want to use STARTTLS, make sure that the protocol is supported by your email server. If you check the **Enable STARTTLS** while the protocol is not supported by your email sever, your email is sent with no encryption.

4) **Optional:** If you want to receive notification with alarm pictures, check **Attached Picture**. The notification email has a certain number of attached alarm pictures about the event with configurable image capturing interval.

Note

The number of alarm pictures may vary according to different device models and different events.

5) Input the recipient's information, including the recipient's name and address.
6) Click **Test** to see if the function is well configured.

3. Click **Save**.

9.2.4 Notify Surveillance Center

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

9.2.5 Trigger Recording

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

For device with more than one camera channels, you can set one or more channels to take recordings if needed.

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

9.2.6 External Alarm Module

You can connect the device with the external alarm module to send alarm to the external device.

Steps

1. Go to **Event Center > Alarm Setting > External Alarm Module** .
2. Click **Add** to add an external device.
3. Select the protocol, and enter **Device IP**, **Management Port**, **Transfer Protocol**. For Arteco protocol, you should enter extra **User Name** and **Password**.

4. Click **OK**.
5. **Optional:** Select the added device, click **Modify** to edit the device information, or click **Delete** to delete it from the list.
6. Click ⚙ to add alarm input and output rules.

9.2.7 Set Audible Alarm Output

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

Steps

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

Note

The function is only supported by certain device models.

9.2.8 Set Flashing Alarm Light Output

Steps

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

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

3. Set the light action duration and the brightness.

   Flashing Duration

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

   Brightness

   The brightness of the light.
4. Edit the arming schedule.

5. Click **Save**.

Note

Only certain camera models support the function.

9.2.9 Metadata

Metadata is the raw data that the device collects before algorithm processing. It is often used for the third party integration.

Go to **Event Center > Alarm Setting > Metadata** to enable metadata uploading of the desired function.

Temperature Measurement

The metadata of temperature measurement includes the target ID, target coordinate, time, etc.

9.2.10 External Alarm Module

You can connect the device with the external alarm module to send alarm to the external device.

Steps

1. Go to **Event Center > Alarm Setting > External Alarm Module** .
2. Click **Add** to add an external device.
3. Select the protocol, and enter **Device IP**, **Management Port**, **Transfer Protocol**. For Arteco protocol, you should enter extra **User Name** and **Password**.
4. Click **OK**.
5. **Optional:** Select the added device, click **Modify** to edit the device information, or click **Delete** to delete it from the list.
6. Click to add alarm input and output rules.

Chapter 10 Device Management

You can add and manage device in **Device Management**.

10.1 Add Audio Device

The device can access and add the alarm speaker through the network protocol. You can view the alarm input/output interface of the speaker.

Steps

1. Click **Add** to add a speaker.
2. Set the parameters of the device, such as the IP address and the description of the alarm speaker.
3. Click **Save**.

Chapter 11 System and Security

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

11.1 System Settings

11.1.1 View Device Information

You can view device information, such as Device No., Model, Serial No. and Firmware Version.

Go to **Configuration > System Settings > Basic Information** to view the device information. You can set **Device Name** and **Device No.**, and click **Save**.

11.1.2 Time and Date

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

Synchronize Time Manually

Steps

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

Set NTP Server

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

Before You Start

Set up a NTP server or obtain NTP server information.

Steps

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

   Note

   Server Address is NTP server IP address.
5. Click **Test** to test server connection.
6. Click **Save**.

Set DST

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

Steps

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

11.1.3 Set RS-232

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

Before You Start

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

Steps

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

11.1.4 Set RS-485

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

Before You Start

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

Steps

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

   Device Mode

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

   Note

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

   CRC Response Transmission

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

   Note

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

11.1.5 Set Same Unit

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

Steps

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

11.2 User and Account

11.2.1 Set User Account and Permission

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

Caution

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

Steps

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

   Administrator

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

   User

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

   Operator

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

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

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

   Note

   The administrator can add up to 31 user accounts.
3. Click **General** to set the allowed number of multi-user simultaneous login.

   Note

   Only the administrator has the authority to the operation.
4. Click **OK**.

11.2.2 Simultaneous Login

The administrator can set the maximum number of users logging into the system through web browser simultaneously.

Go to **Configuration > System > User Management > Online Users** , click **General**, and set **Simultaneous Login**.

11.2.3 Online Users

The information of users logging into the device is shown.

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

11.3 Maintenance

11.3.1 Reboot

You can reboot the device via browser.

Go to **Maintenance and Security > Maintenance > Reboot** , and click **Reboot**.

11.3.2 Upgrade

Before You Start
You need to obtain the correct upgrade package.

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

Steps
1. Go to **Maintenance and Security > Maintenance > Upgrade** .
2. Choose one method to upgrade.

   Firmware Locate the exact path of the upgrade file.

   Firmware Directory Locate the directory which the upgrade file belongs to.
3. Click to select the upgrade file.
4. Click **Upgrade**.

11.3.3 Restore and Default

Restore and Default helps restore the device parameters to the default settings.

Steps
1. Go to **Maintenance and Security > Maintenance > Backup and Restore** .
2. Click **Restore** or **Default** according to your needs.

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

Default Reset all the parameters to the factory default.

Note

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

11.3.4 Import and Export Configuration File

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

Steps

1. Export configuration file.
   1) Go to **Maintenance and Security > Maintenance > Backup and Restore > Backup** .
   2) Click **Export** 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 or calibration file.
   1) Access the device that needs to be configured via web browser.
   2) Go to **Maintenance and Security > Maintenance > Backup and Restore > Reset** .
   3) Click 🗀 to select the saved configuration or calibration file. **Calibration File** is used for device temperature calibration, and **Device Common Parameters** are used for importing system, network or storage related parameters. **Device Parameter** is used for importing parameters except for system, network and storage related ones.
   4) Input the encryption password you have set when exporting the configuration file.
   5) Click **Import**.

11.3.5 Search and Manage Log

Log helps locate and troubleshoot problems.

Steps

1. Go to **Maintenance and Security > 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.

11.3.6 Search Security Audit Logs

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

Steps

Note

This function is only supported by certain camera models.

1. Go to **Maintenance and Security > 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.

11.3.7 SSH

Secure Shell (SSH) is a cryptographic network protocol for operating network services over an unsecured network.

Go to **Maintenance and Security > Maintenance > Device Debugging** , and click **Settings** of **SSH**. You can edit the number of the port. Click **Save**.

Caution

Use the function with caution. The security risk of device internal information leakage exists when the function is enabled.

11.3.8 Export Diagnose Information

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

Go to **Maintenance and Security > Maintenance > Device Debugging > Diagnose Information** . Click **Export**. In the pop-up window, check desired diagnose information and click **Export** to export corresponding diagnose information of the device.

11.4 Security

You can improve system security by setting security parameters.

11.4.1 Set IP Address Filter

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

IP address refers to IPv4.

Steps

1. Go to **Maintenance and Security > Security > IP Address Filter** .

2. Check **Enable**.
3. Select the type of IP address filter.

   Blocklist IP addresses in the list cannot access the device.

   Allowlist Only IP addresses in the list can access the device.
4. Edit the IP address filter list.

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

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

   Delete the selected IP address or IP address range in the list.
5. Click **Save**.

11.4.2 Set MAC Address Filter

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

Steps
1. Go to **Maintenance and Security > Security > MAC Address Filter** .
2. Check **Enable**.
3. Select the type of MAC address filter.

   Blocklist MAC addresses in the list cannot access the device.

   Allowlist Only MAC addresses in the list can access the device.
4. Edit the MAC address filter list.

   Add Add a new MAC address to the list.

   Modify the selected MAC address in the list.

   Delete the selected MAC address in the list.
5. Click **Save**.

11.4.3 Control Timeout Settings

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

Go to **Maintenance and Security > Security > Login Management > Control Timeout Settings** to complete settings.

11.4.4 Certificate Management

It helps to manage the server/client certificates and CA certificate, and to send an alarm if the certificates are close to expiry date, or are expired/abnormal.

Note

The function is only supported by certain device models.

Server Certificate/Client Certificate

Note

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

Create and Install Self-signed Certificate

Steps

1. Go to **Maintenance and Security > Security > Certificate Management** .
2. Click **Create Self-signed Certificate**.
3. Input certificate information.

   Note

   The input certificate ID cannot be the same as the existing ones.
4. Click **Save** to save and install the certificate.

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

   If the certificate is used by certain functions, the function name is shown in the column **Functions**.
5. **Optional:** Click **Property** to see the certificate details.

Install Self-signed Request Certificate

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

Before You Start

Create a self-signed certificate first. See *Create and Install Self-signed Certificate* for instructions.

Steps

1. Go to **Maintenance and Security > Security > Certificate Management** .
2. Select a self-signed certificate from the **Server/Client Certificate** list.

3. Click **Create Certificate Request**.
4. Input request information.
5. Click **Save**.

   The certificate request details are displayed in a pop-up window.
6. Copy the request content and save it as a request file.
7. Send the file to a trusted-third party for signature.
8. After receiving the certificated sent back from the third-party, install it to the device.
   1) Click **Import**.
   2) Input **Certificate ID**.

      Note

      The input certificate ID cannot be the same as the existed ones.
   3) Click to select the certificate file.
   4) Select **Self-signed Request Certificate**.
   5) Click **Save**.

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

   If the certificate is used by certain function, the function name is shown in the column **Functions**.
9. **Optional:** Click **Property** see the certificate details.

Install Other Authorized Certificate

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

Steps

1. Go to **Maintenance and Security > Security > Certificate Management** .
2. Click **Import** in the **Server/Client Certificate** list.
3. Input **Certificate ID**.

   Note

   The input certificate ID cannot be the same as the existed ones.
4. Click to select the certificate file.
5. Select **Certificate and Key** and select a **Key Type** according to your certificate.

Independent Key	If your certificate has an independent key, select this option. Browse to select the private key and input the private-key password.
PKCS#12	If your certificate has the key in the same certificate file, select this option and input the password.

6. Click **Save**.

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

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

Install CA Certificate

Before You Start

Prepare a CA certificate in advance.

Steps

1. Go to **Maintenance and Security > Security > Certificate Management** .
2. Click **Import** in the **CA Certificate** list.
3. Input **Certificate ID**.

   Note

   The input certificate ID cannot be the same as the existing ones.
4. Click to select the certificate file.
5. Click **Save**.

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

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

Enable Certificate Expiration Alarm

Steps

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

   Note

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

11.4.5 TLS

The Transport Layer Security (TLS) protocol aims primarily to provide privacy and data integrity between two or more communicating computer applications. TLS settings are effective for HTTP(S) and enhanced SDK service.

Go to **Maintenance and Security > Security > TLS** , and enable the desired TLS protocol. Click **Save**.

Caution

Use the function with caution. The security risk of device internal information leakage exists when the function is enabled.

Chapter 12 Appendix

12.1 Common Material Emissivity Reference

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

HIKMICRO

See the World in a New Way

UD43694B