Thermal TandemVu 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.
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 (24 VDC, or 24 VAC) 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 60°C (-40°F to 140°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 TandemVu Camera is integrated by one bi-spectrum bullet camera offering perimeter protection and one optical PTZ camera smartly tracking moving targets to provide details. Thermal TandemVu Camera is popularly applied in infrastructure such as airports, railway, city streets, campus, etc., in which smart tracking and perimeter protection are needed.

Chapter 2 Device Activation and Accessing

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

Note

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

2.1 Activate the Device via SADP

Search and activate the online devices via SADP software.

Before You Start

Access *https://www.hikmicrotech.com* 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 Activate the Device via Browser

You can access and activate the device via the browser.

Steps

1. Connect the device to the PC using the network cables.
2. Change the IP address of the PC and device to the same segment.

Note

The default IP address of the device is 192.168.1.64. You can set the IP address of the PC from 192.168.1.2 to 192.168.1.253 (except 192.168.1.64). For example, you can set the IP address of the PC to 192.168.1.100.

3. Input *192.168.1.64* in the browser.
4. Set device activation password.

Caution

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

5. Click **OK**.
6. Input the activation password to log in to the device.
7. **Optional:** Go to **Configuration > Network > Basic > TCP/IP** to change the IP address of the device to the same segment of your network.

2.3 Login

Log in to the device via Web browser.

2.3.1 Plug-in Installation

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

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

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

2.3.2 Illegal Login Lock

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

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

Illegal Login Attempts

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

Locking Duration

The device releases the lock after the setting duration.

Chapter 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 > Basic Configuration > Network > TCP/IP** for parameter settings.

NIC Type

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

IPv4

Two IPv4 modes are available.

DHCP

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

Note

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

Manual

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

IPv6

Three IPv6 modes are available.

Route Advertisement

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

Note

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

DHCP

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

Manual

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

MTU

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

The valid value range of MTU is 1280 to 1500.

DNS

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

3.1.1 Multicast Discovery

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

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 > Basic Settings > DDNS** .
3. Check **Enable DDNS** and select **DDNS type**.

   DynDNS

   Dynamic DNS server is used for domain name resolution.

   NO-IP

   NO-IP server is used for domain name resolution.
4. Input the domain name information, and click **Save**.
5. Check the device ports and complete port mapping. Refer to *Port* to check the device port, and refer to *Port Mapping* for port mapping settings.
6. Access the device.

By Browsers	Enter the domain name in the browser address bar to access the device.

By Client Software	Add domain name to the client software. Refer to the client manual for specific adding methods.

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 > Basic Settings > PPPoE** .
2. Check **Enable PPPoE**.
3. Set the PPPoE parameters.

   Dynamic IP

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

   User Name

   User name for dial-up network access.

   Password

   Password for dial-up network access.

   Confirm

   Input your dial-up password again.
4. Click **Save**.
5. Access the device.

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

Note

The obtained IP address is dynamically assigned via PPPoE, so the IP address always changes after restarting 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 Port

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

Caution

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

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

HTTP Port

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

HTTPS Port

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

RTSP Port

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

SRTP Port

It refers to the port of secure real-time transport protocol.

Server Port

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

WebSocket Port

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

WebSockets Port

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

Note

- Enhanced SDK Service Port, WebSocket Port, and WebSockets Port are only supported by certain models.
- For device models that support that function, go to **Configuration > Network > Advanced Settings > Network Service** to enable it.

3.5 Port Mapping

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

Before You Start

When the ports in the device are the same as those of other devices in the network, refer to *Port* to modify the device ports.

Steps

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

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

3. Click **Save**.

3.5.1 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.

3.5.2 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.

3.6 Multicast

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

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

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

IP Address

It stands for the address of multicast host.

Stream Type

The stream type as the multicast source.

Video Port

The video port of the selected stream.

Audio Port

The audio port of the selected stream.

3.7 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 > Advanced Settings > SNMP** .
2. Check **Enable SNMPv1**, **Enable SNMP v2c** or **Enable SNMPv3**.

Note

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

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

3.8 Accessing via Mobile Client

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

Note

Hik-Connect service should be supported by the camera.

3.8.1 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 SADP software or 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.

3.8.2 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.

3.8.3 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.

3.9 Set ISUP

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

Steps

1. Go to **Configuration > Network > Advanced Settings > Platform Access** .
2. Select **ISUP** as the platform access mode.

3. Select **Enable**.
4. Select a protocol version and input related parameters.
5. Click **Save**.

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

3.10 Set Alarm Host

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

Steps

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

3.11 Set Open Network Video Interface

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

Steps

1. Go to **Configuration > Network > Advanced Settings > Integration Protocol** .
2. Check **Enable Open Network Video Interface**.
3. Select an authentication mode.
   - If you select **Digest**, the device only supports digest authentication.
   - If you select **Digest&ws-username token**, the device supports digest authentication or ws-username token authentication. You can check **Time Verification** to verify the client time based on your needs.
4. Click **Add** to configure the Open Network Video Interface user.

   Delete Delete the selected Open Network Video Interface user.

   Modify Modify the selected Open Network Video Interface user.
5. Click **Save**.
6. **Optional:** Repeat the steps above to add more Open Network Video Interface users.

3.12 Set Network Service

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

Steps

Note

This function varies according to different models.

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

   WebSocket & WebSockets

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

   If the device uses HTTP, enable WebSocket.

   If the device uses HTTPS, enable WebSockets.

   TLS (Transport Layer Security)

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

   Bonjour

   Bonjour is a zero-configuration protocol used to automatically find devices in a network or create networks between devices. You can disable it when not using the protocol.
3. Click **Save**.

3.13 Set Alarm Server

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

Steps

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

   Note

   HTTP, HTTPS, and ISUP are selectable. It is recommended to use HTTPS, as it encrypts the data transmission during communication.
4. Click **Test** to check if the IP or host is available.
5. Click **Save**.

3.14 Set SRTP

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

Steps

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

Note

Only certain device models support this function.

Chapter 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.

4.1.4 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.

4.1.5 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.

4.1.6 Conduct Regional Focus

You can enable the function to focus on certain area.

Steps

1. Click to enable regional focus.
2. Drag the mouse on the live view to draw a rectangle as the desired focus area.
3. Click to disable this function.

4.1.7 Light

Click to turn on or turn off the illuminator.

4.1.8 Operate Wiper

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

Note

Wiper operation and settings vary on device models.

Steps

1. Go to **Configuration > PTZ > Wiper** .
2. Select a wiper mode.

One Time The wiper wipes one time when you click on live view page.

Cycle The wiper works on schedule at set wiping interval. Click on live view to start wiping.

Duration

The schedule in which the wiper is ready to work.

Interval

The interval between two successive wiping actions.

Auto

Note

Auto mode is only available for device that supports rain-sensing auto wiper.

In auto mode, the wiper works when rain drops on the window.

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.

Manual Lens Initialization

Click to operate lens initialization.

Auto Lens Initialization

Go to **Configuration > System > Maintenance > Lens Correction** to enable this function. You can set the arming schedule, and the device will correct lens automatically during the configured time periods.

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, and video/audio settings on live view page.

Steps

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

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.

PTZ Speed

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

Iris

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

4.1.13 Conduct 3D Positioning

3D positioning is to relocate the selected area to the image center.

Steps

1. Click to enable the function.
2. Select a target area in live image.
   - Left click on a point on live image: the point is relocated to the center of the live image. With no zooming in or out effect.
   - Hold and drag the mouse to a lower right position to frame an area on the live: the framed area is zoomed in and relocated to the center of the live image.
   - Hold and drag the mouse to an upper left position to frame an area on the live: the framed area is zoomed out and relocated to the center of the live image.
3. Click the button again to turn off the function.

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** .

2. Set the transmission parameters as required.

Protocol

TCP

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

UDP

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

MULTICAST

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

Note

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

HTTP

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

Play Performance

Shortest Delay

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

Balanced

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

Fluent

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

Custom

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

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 **OK**.

Chapter 5 Video and Audio

This part introduces the configuration of video and audio 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.

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.

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.

5.2 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** .

5.2.1 Audio Input

If a built-in microphone or an external audio pick-up device is available, audio encoding, audio input mode and input volume are configurable.

Audio Encoding

The device offers several compression standard. Select according to your need.

Audio Input

Select **MicIn** for the built-in microphone, and **LineIn** for external audio pick-up device.

Note

MicIn is only supported by certain models.

Input Volume

Adjust the volume of the audio input.

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.

5.2.2 Two-way Audio

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

Before You Start

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

Steps

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

5.3 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.

5.4 Metadata

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

Go to **Configuration > Video/Audio > Metadata Settings** to enable metadata uploading of the desired function for the camera channels.

5.5 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.

5.5.1 Image Adjustment

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

5.5.2 Image Adjustment (Thermal Channel)

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

Manual Correction

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

Note

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

5.5.3 Exposure Settings

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

Exposure Mode

Auto

The iris, shutter, and gain values are adjusted automatically.

You can limit the changing ranges of iris, shutter and gain by setting **Max. Iris Limit**, **Min. Iris Limit**, **Max. Shutter Limit**, **Min. Shutter Limit** and **Limit Gain** for better exposure effect.

Iris Priority

The value of iris needs to be adjusted manually. The shutter and gain values are adjusted automatically according to the brightness of the environment.

You can limit the changing ranges of the shutter and gain by setting **Max. Shutter Limit**, **Min. Shutter Limit** and **Limit Gain** for better exposure effect.

Shutter Priority

The value of shutter needs to be adjusted manually. The iris and gain values are adjusted automatically according to the brightness of the environment.

You can limit the changing ranges of the iris by setting **Max. Iris Limit**, **Min. Iris Limit** and **Limit Gain** for better exposure effect.

Manual

You need to set **Iris**, **Shutter**, and **Gain** manually.

Slow Shutter

The higher the slow shutter level is, the slower the shutter speed is. It ensures full exposure in underexposure condition.

5.5.4 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 image is black/white or colorful and 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.

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.
- You can turn on the smart supplement light in auto, night, and schedule-switch modes for better image effect.

5.5.5 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.

   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.

5.5.6 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.

5.5.7 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.

WDR Off WDR On

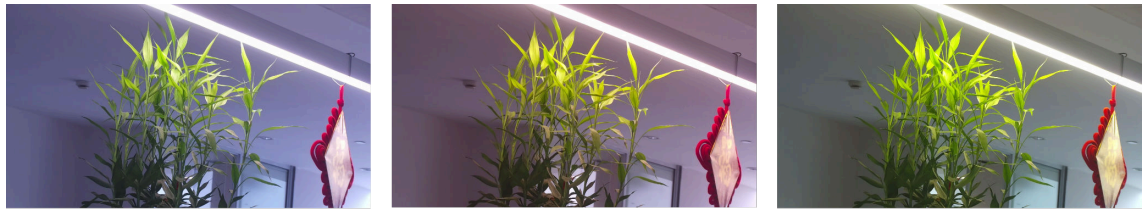
Figure 5-1 WDR

5.5.8 HLC

When the bright area of the image is over-exposed and the dark area is under-exposed, the HLC (High Light Compression) function can be enabled to weaken the bright area and brighten the dark area, so as to achieve the light balance of the overall picture.

5.5.9 White Balance

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



Cold Warm Auto White Balance

Figure 5-2 White Balance

5.5.10 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.

DNR Off

DNR On

Figure 5-3 DNR

5.5.11 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.

Defog Off Defog On

Figure 5-4 Defog

5.5.12 EIS

Increase the stability of video image by using jitter compensation technology.

5.5.13 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].

5.5.14 SuperIR

Resolution of images with SuperIR (Super Image Resolution) is better than the original one.

5.5.15 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.

5.5.16 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.

5.5.17 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.

5.5.18 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.

5.5.19 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.

5.5.20 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.

5.5.21 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.

5.5.22 Digital Zoom

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

5.5.23 Local Video Output

If the device is equipped with video output interfaces, such as BNC, CVBS, HDMI, and SDI, you can preview the live image directly by connecting the device to a monitor screen.

Select the output mode as ON/OFF to control the output.

5.6 OSD

You can customize OSD (On-screen Display) information such as device name, time/date, font, 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 be displayed on screen, select **EUC-KR**. Otherwise, select **GBK**.

Displayed Information

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

Text Overlay

Set customized overlay text on image.

OSD Parameters

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

5.7 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**.

5.8 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. Select manual mode.
4. Click the defective pixel on the image, then a cursor shows on the live view.
5. Click **Up**, **Down**, **Left**, **Right** to adjust the cursor position to the defective pixel position.
6. 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.
7. **Optional:** Click to cancel defective pixel correction.

5.9 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. 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. 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 **Configuration > Network > Advanced Settings > FTP** .
2. Configure FTP settings.

FTP Protocol

FTP and SFTP are selectable. The files uploading is encrypted by using SFTP protocol.

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.

Note

If SFTP is used, logging into the FTP server anonymously is now allowed.

Directory Structure

The saving path of snapshots in the FTP server.

3. Click **Upload Picture** or **Upload Video** to enable uploading snapshots or videos 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 **Record File Size** and saving path to for recorded files.
3. Click **Save**.
4. Click in the live view interface to start recording. Click to stop recording.

6.2.3 Playback and Download Video

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

Steps

1. Click **Playback**.
2. 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 clip video files.
   - Click to play video files in full screen. Press **ESC** to exit full screen.

   Note

   Go to **Configuration > Local** , click **Save clips to** to change the saving path of clipped video files.
5. Click on the playback interface to download files.
   1) Set search condition and click **Search**.
   2) Select the video files and then click **Download**.

Note

Go to **Configuration > Local** , click **Save downloaded files to** to change the saving path of downloaded video files.

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.

Steps

1. Go to **Configuration > Storage > Schedule Settings > Capture > Capture Parameters** .
2. Select a channel to set capture parameters.
3. Set the capture type.

   Timing

   Capture a picture at the configured time interval.

   Event-Triggered

   Capture a picture when an event is triggered. You should configure related linkage methods in event settings first. Refer to ***Event and Alarm*** for event settings.
4. Set the **Format**, **Resolution**, **Quality**, **Interval**, and **Capture Number**.
5. Refer to ***Set Arming Schedule*** for configuring schedule time.
6. 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. Click **Picture**.
2. Select channel No.
3. Set search condition and click **Search**.

   The matched pictures showed in the file list.
4. Select the pictures then click **Download** to download them.

Note

Go to **Configuration > Local** , click **Save snapshots when playback** to change the saving path of pictures.

Chapter 7 Perimeter Protection

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

7.1 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 **Configuration > Perimeter Protection > Rule** .
2. Check **Intelligent Analysis**.
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 **Leaves Interfered View** when there are shaking targets in the scene, such as leaves.

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. *Set Arming Schedule* and *Linkage Method Settings* for each rule.
6. **Optional:** You can shield certain areas from being detected. Refer to *Set Perimeter Protection Shield Region* for detailed settings.
7. **Optional:** Set displayed information on stream or picture. Refer to *Set Overlay & Capture Parameters* for detailed settings.

7.2 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 **Configuration > 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 Set Overlay & Capture Parameters

Steps

1. Go to **Configuration > Perimeter Protection > Overlay & Capture** .

   Display VCA Info. on Stream

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

   Display Trajectory

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

   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.

   Display Size Info. on Alarm Picture

   Select to display the size information of the target on the alarm picture.

   Snapshot Settings

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

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

7.4 Alarm Double Check

When the perimeter protection rule alarm is triggered in camera channel 01/02, the camera channel 03 will be linked to double check the target authenticity and judge to upload the alarm information or not.

Steps

1. Go to **Configuration > Perimeter Protection > Alarm Double Check** .
2. Check **Enable**.
3. Drag the time bar to draw desired valid time.
4. 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.
5. **Optional:** Click **Copy to...** to copy the same settings to other days.
6. Click **Save**.

7.5 Set Advanced Configuration Parameters

Go to **Configuration > 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.

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.

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 **Configuration > Event > 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. Click **Draw Area**. Click and drag the mouse on the live video, then release the mouse to finfish drawing one area.

   Stop Drawing Stop drawing one area.

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

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 **Configuration > Event > 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 **Draw Area** and drag the mouse in the live view to draw the area.

   Stop Drawing Finish drawing.

Clear All Delete all the drawn areas.

Figure 8-1 Set Video Tampering Area

6. Refer to ***Set Arming Schedule*** for setting scheduled time. Refer to ***Linkage Method Settings*** for setting linkage method.
7. 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 **Configuration > Event > Basic Event > Alarm Input** .
2. Check **Enable Alarm Input Handling**.

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

8.4 Set Exception Alarm

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

Steps

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

HDD Full	The HDD storage is full.
HDD Error	Error occurs in HDD.
Network Disconnected	The device is offline.
IP Address Conflicted	The IP address of current device is same as that of other device in the network.
Illegal Login	Incorrect user name or password is entered.
Voltage Instable	The power supply voltage is fluctuating.
PT Locking	The panning and tilting movements are stuck.

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.

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 information to the connected alarm output device when an alarm is triggered.

Steps

Note

This function is only supported by certain models.

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

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

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

3. Click **Save**.

Manual Alarm

You can trigger an alarm output manually.

Steps

1. Set the manual alarm parameters.

   Alarm Output No.

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

   Alarm Name

   Edit a name for the alarm output.

   Delay

   Select **Manual**.

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

Automatic Alarm

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

Steps

1. Set automatic alarm parameters.

   Alarm Output No.

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

   Alarm Name

   Custom a name for the alarm output.

   Delay

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

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

9.2.2 Set Flashing Alarm Light Output

Steps

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

   Flashing Duration

   The time period the flashing lasts when one alarm happens.

   Flashing Frequency

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

   Brightness

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

Note

Only certain camera models support the function.

9.2.3 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.

9.2.4 FTP/NAS/Memory Card Uploading

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

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

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

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

9.2.5 Send Email

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

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

Set Email

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

Before You Start

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

Steps

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

      Note

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

4) **Optional:** If you want to receive notification with alarm pictures, check **Attached Image**. The notification email has 3 attached alarm pictures about the event with configurable image capturing interval.
5) Configure **Alarm E-mail Attachment Settings**.

Image

Select the number of captures of the corresponding channel.

- 0: It will not upload the image of the selected channel.
- 1: It will only upload the image captured when the alarm is triggered.
- 3: It will upload the images captured about 1 s before and after the alarm is triggered, as well as the image captured when the alarm is triggered.

Video

Select the video channel and video duration as required.

- 0 s: It will not upload the video of the selected channel.
- 3 s: Upload the video that is recorded about 1 s before and 2 s after the alarm is triggered.
- 5 s: Upload the video that is recorded about 2 s before and 3 s after the alarm is triggered.
- 7 s: Upload the video that is recorded about 2 s before and 5 s after the alarm is triggered.

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

3. Click **Save**.

9.2.6 Notify Surveillance Center

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

9.2.7 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* .

Chapter 10 PTZ

PTZ is an abbreviation for pan, tilt, and zoom. It means the movement options of the camera.

10.1 PTZ Control

In live view interface, you can use the PTZ control buttons to control the device panning, tilting, and zooming.

PTZ Control Panel

	Click and hold the directional button to pan/tilt the device. **Note** • You can set **Keyboard Control Speed** in **Configuration > PTZ > Basic Settings** . The speed of pan/tilt movement in live view is based on this speed level. • You can set **Max. Tilt-angle** in **Configuration > PTZ > Basic Settings** to limit tilt movement range.
	Click the button, then the device keeps panning. **Note** You can set **Auto Scan Speed** in **Configuration > PTZ > Basic Settings** . The higher the value you set, the faster the device pans.
	Drag the slider to adjust the speed of pan/tilt movement.

Note

- You can set **Manual Control Speed** in **Configuration > PTZ > Basic Settings** .

Compatible	The control speed is same as **Keyboard Control Speed**.
Pedestrian	Choose **Pedestrian** when you monitor the pedestrians.
Non-motor Vehicle	Choose **Non-motor Vehicle** when you monitor the non-motor vehicles.
Motor Vehicle	Choose **Motor Vehicle** when you monitor the motor vehicles.
Auto	You are recommended to set it as **Auto** when the application scene of the speed dome is complicated.

- To avoid blurred image resulted from fast zoom, you can check **Enable Proportional Pan** in **Configuration > PTZ > Basic Settings** . If you enable this function, the pan/tilt speed change according to the amount of zoom. When there is a large amount of zoom, the pan/tilt speed will be slower for keeping the image from moving too fast on the live view image.

Zoom in/out

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

Note

- You can set **Zooming Speed** in **Configuration > PTZ > Basic Settings** . The higher the value is, the faster the zooming speed is.
- You can set **Zoom Limit** in **Configuration > Image > Display Settings > Other** to limit the maximum value of the total zoom (digital zoom and optical zoom).
- You can set **Synchronized Zoom** in **Configuration > PTZ > Basic Settings** to synchronize the zoom settings in the optical channel and the thermal channel.

Focus

	Click the button, then the lens focuses near and the object nearby gets clear.
	Click the button, then the lens focuses far and the object far away gets clear.

Iris

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

10.2 Set Preset

A preset is a predefined image position. For the defined preset, you can call the preset No. to view the position.

Steps

1. Click to show the setting panel, and click .
2. Use the PTZ control buttons to move the lens to the desired position.
3. Select a preset number from the preset list, and click to finish the setting.

Note

Some presets are predefined with special command. You can only call them but not configure them.

4. Repeat the steps above to set multiple presets.

Click the button to call the preset.

Click the button to delete the preset.

Note

You can delete all presets in **Configuration > PTZ > Clear Config** . Click **Clear All Presets**, and click **Save**.

What to do next

Go to **Configuration > PTZ > Basic Settings** to set preset freezing and preset speed.
After enabling preset freezing, the live image switches directly from one preset to another, without showing the areas between these two scenes. It also guarantees the masked area will not be seen when the device is moving.

10.2.1 Special Presets

You can call the following presets with special demands to enable corresponding functions.

Preset No.	Function	Preset No.	Function
33	Auto Flip	92	Set manual limits
34	Back to origin	93	Save manual limits
35	Call patrol 1	94	Remote restart
36	Call patrol 2	95	Call OSD menu
37	Call patrol 3	96	Stop a scan
38	Call patrol 4	97	Start random scan
39	Day mode	98	Start frame scan
40	Night mode	99	Start auto scan
41	Call pattern 1	100	Start tilt scan
42	Call pattern 2	101	Start panorama scan
43	Call pattern 3	102	Call patrol 5
44	Call pattern 4	103	Call patrol 6
45	One-touch patrol	104	Call patrol 7
46	Call area scan	105	Call patrol 8
47	Call area scan 1		

Note

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

10.3 Set Patrol Scan

Patrol scan is a function to automatically move among multiple presets.

Before You Start

Note

This function is only supported by certain models.

Make sure that you have defined more than one presets. See ***Set Preset*** for detailed configuration.

Steps

1. Click to show the setting panel, and click to enter patrol setting interface.
2. Select a patrol number from the list and click .
3. Click + to add presets.

Preset

Select predefined preset.

Speed

Set the speed of moving from one preset to another.

Time

It is the duration staying on one patrol point.

× Delete the presets in patrol.

Adjust the preset order.

Note

A patrol can be configured with 32 presets at most, and 2 presets at least.

4. Click **OK** to finish a patrol setting.
5. Repeat the steps above to configure multiple patrols.
6. Operate patrols.

Call the patrol.

Stop patrolling.

× Delete the patrol.

Set the patrol.

Note

You can delete all patrols in **Configuration > PTZ > Clear Config** . Click **Clear All Patrols**, and click **Save**.

10.3.1 Set One-Touch Patrol

The device automatically adds presets to one patrol path and starts patrol scan.

Steps

1. Set two or more presets except special presets. For setting presets, refer to ***Set Preset*** .
   The device will automatically add presets to patrol path No.8.
2. Choose one of the following methods to enable the function.
   - Click .
   - Call patrol path No.8.
   - Select and call preset No.45.

10.4 Set Pattern Scan

The device can move as the recorded pattern.

Steps

Note

This function is only supported by certain models.

1. Click to show the PTZ control panel, and click .
2. Select one pattern scan path that needs to be set.
3. Click to start recording pattern scan.
4. Click PTZ control buttons as demands.

   Note

   Recording stops when the space for pattern scan is 0%.
5. Click to complete one pattern scan path settings.
6. Click to call pattern scan.

   Stop pattern scan.

   Reset pattern scan path.

   Delete the selected pattern scan.

   Note

   If you need to delete all the pattern scans, go to **Configuration > PTZ > Clear Config** , and check **Clear All Patterns**, and click **Save**.

10.5 Set Linear Scan

The device can perform auto scan in setting area for VCA detection.

Steps

1. Go to **Configuration > PTZ > Linear Scan** .
2. Select the camera channel.
3. Zoom in and zoom out the camera to the appropriate zoom ratio, and click **Save Ratio**.

   Note

   Click **Enable Saved Ratio** to set the camera to the saved zoom ratio.
4. Check **Enter Area Settings**.
5. Set the left/right/up/down limits with the PTZ control panel, and click to confirm settings.
6. **Optional:** Click **Clear** to delete the saved scan area.
7. Click **Save**.
8. Click **Call Linear Scan** to start linear scan, and click **Stop Linear Scan** to stop linear scan.

Note

When setting the linear scan area, make sure the target area is both included in the optical channel and the thermal channel.

10.6 Set Limit

The device can only move within the limited range.

Steps

1. Go to **Configuration > PTZ > Limit** .
2. Select **Limit Type**.

   Manual Stops

   It refers to the movement range limit when you control the device manually.

   Scan Stops

   It refers to the movement range limit when the device scans automatically.

   Note

   Scan limit is only supported by the device that has scan function.
3. Click **Set** and set limits according to the prompt on the live image.
4. **Optional:** Click **Clear** to clear the limit settings of the selected mode.
5. Click **Save**.
6. Check **Enable Limit**.

   Note

   If you need to cancel all the set patrol paths, go to **Configuration > PTZ > Clear Config** , select **Clear All PTZ Limited**, and click **Save**.

Result

The device can only move within the set region after saving the settings.

10.7 Set Initial Position

Initial position refers to the relative initial position of the device azimuth. You can set the initial position if you need to select one point in the scene as the base point.

Steps

1. Go to **Configuration > PTZ > Initial Position** .
2. Move the device to the needed position by manually controlling the PTZ control buttons.
3. Click **Set** to save the information of initial position.

   Call The device moves to the set initial position.

Clear Clear the set initial position.

10.8 Set Park Action

You can set the device to perform an action (for example, preset or patrol) or return to a position after a period of inactivity (park time).

Before You Start

Set the action type first. For example, if you want to select patrol as park action, you should set the patrol. See *Set Patrol Scan* for details.

Steps

1. Go to **Configuration > PTZ > Park Action** .
2. Check **Enable Park Action**.
3. Set **Park Time**: the inactive time before the device starts park action.
4. Select **Action Type** according to your needs.

   Note

   The VCA Type varies according to different action types.
5. Select an **Action Type ID**, if you select patrol or preset as action type.

   When the action type is patrol, action type ID stands for patrol No. When the action type is preset, action type ID stands for preset No.
6. Click **Save**.

10.9 Set Privacy Mask

Privacy masks cover certain areas on the live image to protect personal privacy from being live viewed and recorded.

Steps

1. Go to **Configuration > PTZ > Privacy Mask** .
2. Select a channel.
3. Adjust the live image to the target scene via PTZ control buttons.
4. Draw the area.

Draw Area	Click **Draw Area**, and click on the live view image to determine the boundary of the mask.
Stop Drawing	Click **Stop Drawing** after drawing the mask.

5. Click **Add**.

   It is listed in **Privacy Mask List**.

6. Edit **Name**, **Type**, and **Active Zoom Ratio** on your demand.

   Active Zoom Ratio

   When the actual zoom ratio is less than the set active zoom ratio, the set area cannot be covered. When the actual zoom ratio is greater than the set active zoom ratio, the privacy mask is valid. The maximum value of active zoom ratio depends on the camera module.

   Note

   Active zoom ratio is only supported for the PTZ channel.
7. Repeat the steps above to set other privacy masks.
8. Check **Enable Privacy Masks**.

10.10 Set Scheduled Tasks

You can set the device to perform a certain task during a certain period.

Steps

1. Go to **Configuration > PTZ > Scheduled Tasks** .
2. Check **Enable Scheduled Task**.
3. Select the task type from the drop-down list and draw a time bar on the schedule table.
4. Click the set time bar and set the action ID and smart event or VCA type.

   Note

   Not all task types support the settings of action ID and smart event or VCA function. Please take the actual product for reference.
5. Repeat step 3 and step 4 to set more than one scheduled tasks.
6. Set **Park Time**. During the set task period, if you operate the device manually, the scheduled task will be suspended. When the manual operation is over, the device will continue to perform the scheduled task after the set park time.

   Note

   Up to 30 time periods can be configured per day.
7. Click **Save**.

   Note

   If you want to clear all scheduled tasks, go to **Configuration > PTZ > Clear Config** , check **Clear All Scheduled Tasks**, and click **Save**.

10.11 Set PTZ Priority

The function can set the PTZ priority of different signals.

Steps

1. Go to **Configuration > PTZ > Prioritize PTZ** .
2. Set the priority signal and delayed time.

   Network

   The network signal controls the device with priority.

   RS-485

   The RS-485 signal controls the device with priority.

   Delay

   It refers to the time interval of PTZ operation controlled by different signals. When the operation with high priority is finished, the low priority signal controls the device after the setting interval.
3. Click **Save**.

10.12 Set Device Position

Before You Start

Go to **Configuration > PTZ > Basic Settings > PTZ OSD** to enable **PT Status** display.

Steps

1. Go to the setting page: **Configuration > PTZ > Position Settings** .
2. Select a **PT Mode**.

   Manual Use a direction indicating device to determine the North at the device location, and set the North for the device. For details, see ***Set Manual Compass*** .

   Auto For the device that has built-in e-compass, the compass can automatically tell the north direction for the device. For details, see ***Set Auto Compass*** .
3. **Optional:** Check **Display Position Diagram** to display the position diagram on the live view.
4. Set Vandal-proof alarm.

   After enabling the function, the device triggers alarms once its position changes because of shock or vandalism.

   Sensitivity

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

   Upload Vandal-proof Alarm

   The device uploads the alarm information when the alarm is triggered.
5. Get the device location information in advance, and input the longitude and latitude of the device manually.
6. Click **Save**.

What to do next
If you lost direction when operating the device, you can click **Point to North** to call the north position that is saved in the device.

10.12.1 Set Manual Compass

Use a direction indicating device to determine the North at the device location, and set the North for the device.

Before You Start
Use a direction indicating device to determine the north at the device location.

Steps
1. Select the **PT Mode** as **Manual**.
2. Adjust the tilt position of the device to 0 by controlling the up arrow and down arrow on the PTZ panel.
3. Adjust the pan position to show the live view of the north direction by controlling the left arrow and right arrow on the PTZ panel.
4. Click **Set as North**.

10.12.2 Set Auto Compass

For the device that has built-in e-compass, the compass can automatically tell the north direction for the device.

Before You Start
Electromagnetic interference may affect the accuracy of the e-compass. Use manual compass if electromagnetic interference occurs in the device installation environment.

Steps
1. Select the **PT Mode** as **Auto**.
2. Click **Calibrate** to synchronize the north of the device with that of the e-compass.

10.13 Set Power Off Memory

This function can resume the previous PTZ status of device after it restarting from a power-off.

Steps
1. Go to **Configuration > PTZ > Basic Settings** .
2. Select **Resume Time Point**. When the device stays at one position for the set resume time point or more, the position is saved as a memory point. The device returns to the last memory point when it restarts.
3. Click **Save**.

10.14 Panorama Tracking

This function links panoramic channel with PTZ channel through calibration. The PTZ channel tracks moving objects in panoramic channel and automatically adjusts its PTZ positions to keep the target in the center of PTZ view for more details.

10.14.1 Set Panorama Tracking – Manual Calibration

Steps

1. Go to **Configuration > PTZ > Panorama Tracking > Scene Configuration** . Use the PTZ control buttons to select a scene and click **Save**.
2. Go to **Configuration > PTZ > Panorama Tracking > Calibration** .
3. Check **Track**.
4. Select **Calibration Mode** as **Manual**. Click **Start Calibration**.
5. Add calibration points.
   1) Select a No. in **Calibration Parameter** list. Click + .
      A numbered green cross displayed on the live image.
   2) Drag the green cross to a certain position.
   3) Repeat the steps above to add more calibration points.

   Note

   - It is recommended to add at least 9 calibration points in one scene. For higher tracking precision, up to 12 calibration points can be added. Calibration points should be distributed evenly in live image, for example, 3 points at far range, middle range, and close range each.
   - It is recommended to put calibration points at distinct positions in live image (for example, corners). If no distinct position is available, you can place something (for example, box, stool, or people) to mark the position.
6. Link the PTZ channel to the calibration points in panorama view.
   1) Select a calibration point in panorama view.
   2) Adjust the PTZ channel to set the center of the close-up view at the same position as the calibration point in panorama view by using the PTZ control buttons or by clicking and then clicking or dragging an area on live image.
   3) Click to link the current PTZ positions to the calibration point.
   4) Repeat the steps above to link other calibration points.
7. Click **Start Calibration** to finish the calibration for the current scene.
8. When calibration is completed, click **Complete Manual Calibration** to exit.
9. Set tracking initial position. Use the PTZ buttons to adjust close-up view. Click **Set Tracking Initial Position** to finish setting.

   Tracking Initial Position

When tracking finishes or timed out, PTZ channel returns to the tracking initial position. When tracking initial is not set, PTZ channel stays where tracking finishes or timed out.

10. Set the tracking duration and zooming ratio. Click **Save**.

Tracking Duration

It is used to set the duration of tracking. The PTZ channel switches to next target after the set duration time. When tracking duration is set to 0, tracking continues until the target leaves the scene.

Zooming Ratio

It is used to set the zooming ratio for tracking. The higher the value is, the larger the target is in the close-up view.

10.14.2 Set Panorama Tracking – Auto Calibration

Before You Start

Avoid using auto calibration for vast similar scenes (for example, lake, lawn, or public square) or dark scenes (for example, night scenes).

Steps

1. Go to **Configuration > PTZ > Panorama Tracking > Scene Configuration** . Use the PTZ control buttons to select a scene and click **Save**.
2. Go to **Configuration > PTZ > Panorama Tracking > Calibration** .
3. Check **Track**.
4. Select **Calibration Mode** as **Auto (Fast)**. Click **Start Calibration**.
5. Select a method for auto calibration.

One-touch Calibration	If all scenes in panoramic channel have good stitching effect, it is recommended to use **One-touch Calibration** to calibrate all scenes. Click **One-touch Calibration**. When calibration for all scenes is complete, click **Stop Calibration** to exit.

6. When calibration is completed, click **Auto Calibrating succeeded** to exit.
7. Set tracking initial position. Use the PTZ control buttons to adjust close-up view. Click **Set Tracking Initial Position** to finish setting.

Tracking Initial Position

When tracking finishes or timed out, the PTZ channel returns to the tracking initial position. When tracking initial is not set, PTZ channel stays where tracking finishes or timed out.

8. Set the tracking duration and zooming ratio. Click **Save**.

Tracking Duration

It is used to set the duration of tracking. The PTZ channel switches to next target after the set duration time. When tracking duration is set to 0, tracking continues until the target leaves the scene.

Zooming Ratio

It is used to set the zooming ratio for tracking. The higher the value is, the larger the target is in the close-up view.

Chapter 11 System and Security

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

11.1 View Device Information

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

Enter **Configuration > System > System Settings > Basic Information** to view the device information.

11.2 Time and Date

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

11.2.1 Synchronize Time Manually

Steps

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

11.2.2 Set NTP Server

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

Before You Start

Set up a NTP server or obtain NTP server information.

Steps

1. Go to **Configuration > System > System Settings > Time Settings** .
2. Select **Time Zone**.
3. Click **NTP**.

4. Set **Server Address**, **NTP Port** and **Interval**.

Note

Server Address is NTP server IP address.

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

11.2.3 Set DST

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

Steps

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

11.3 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**.

11.4 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.

Note

You should keep the parameters of the device and the computer or terminal all the same.

3. Click **Save**.

11.5 View Open Source Software License

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

11.6 Set Same Unit

Set the same 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 distance unit.
4. Click **Save**.

11.7 Reboot

You can restart the device via browser.

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

11.8 Restore and Default

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

Steps

1. Go to **Configuration > System > Maintenance > Upgrade & Maintenance** .
2. Click **Restore** or **Default** according to your needs.

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

Default Reset all the parameters to the factory default.

Note

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

11.9 Import and Export Configuration File

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

Steps

1. Export configuration file.
   1) Go to **Configuration > System > Maintenance > Upgrade & Maintenance** .
   2) Click **Device Parameters** and input the encryption password to export the current configuration file.
   3) Click **Device Common Parameters**, check desired common parameters and input the encryption password to export the current configuration file.
   4) **Optional:** Set the saving path to save the configuration file in local computer.
2. Import configuration file.
   1) Access the device that needs to be configured via web browser.
   2) Go to **Configuration > System > Maintenance > Upgrade & Maintenance** .
   3) Select the imported file type from the drop-down list.

      Note

      You can import the exported **Device Common Parameters** to devices of the same series.
   4) Click **Browse** to select the saved configuration file.
   5) Input the encryption password you have set when exporting the configuration file.
   6) Click **Import**.

11.10 Export Diagnose Information

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

Go to **Configuration > System > Maintenance > Upgrade & Maintenance** , and click **Diagnose Information** to export diagnose information of the device.

11.11 Upgrade

Before You Start

You need to obtain the correct upgrade package.

Caution

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

Steps

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

Firmware Locate the exact path of the upgrade file.

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

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

11.12 Device Auto Maintenance

Set the auto maintenance schedule and the device will automatically restart on schedule, which helps avoid problems such as network anomaly and outage during continuous operation, etc.

Steps

1. Go to **Configuration > System > Maintenance > Upgrade & Maintenance** .
2. Check **Enable Auto Maintenance**.
3. Read the prompt information and click **OK**.
4. Select the date and time when the device automatically restart.
5. Click **Save**.

Note

This function is only available for Administrator.

11.13 Search and Manage Log

Log helps locate and troubleshoot problems.

Steps

1. Go to **Configuration > System > Maintenance > Log** .
2. Set search conditions **Major Type**, **Minor Type**, **Start Time**, and **End Time**.
3. Click **Search**.

   The matched log files will be displayed on the log list.
4. **Optional:** Click **Export** to save the log files in your computer.

11.14 Security

You can improve system security by setting security parameters.

11.14.1 Security Audit Log

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

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

Search Security Audit Logs

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

Steps

Note

This function is only supported by certain camera models.

1. Go to **Configuration > System > Maintenance > Security Audit Log** .
2. Select log types, **Start Time**, and **End Time**.
3. Click **Search**.

   The log files that match the search conditions will be displayed on the Log List.
4. **Optional:** Click **Export** to save the log files to your computer.

Set Log Server

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

Before You Start

- Install client and CA certificates before configuration. Refer to ***Certificate Management*** for detailed information.
- Select certificates according to the requirement of the log server. If two-way authentication is required, select the CA certificate and the client certificate. If one-way authentication is required, select the CA certificate only.

Steps

1. Check **Enable Log Upload Server**.
2. **Optional:** Check **Enable Encrypted Transmission** if you want the log data to be encrypted.
3. Input **Log Server IP** and **Log Server Port**.
4. **Optional:** Select client certificate.
5. Select CA certificate to the device.
6. Click **Test** to test the settings.

7. Click **Save**.

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.

11.14.2 Authentication

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

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

RTSP Authentication

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

WEB Authentication

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

Note

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

11.14.3 Set IP Address Filter

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

IP address refers to IPv4.

Steps

Note

IP Address Filter is mutually exclusive with **MAC Address Filter**.

1. Go to **Configuration > System > Security > IP Address Filter** .

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

   Forbidden IP addresses in the list cannot access the device.

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

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

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

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

11.14.4 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

Note

MAC Address Filter is mutually exclusive with **IP Address Filter**.

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

   Forbidden MAC addresses in the list cannot access the device.

   Allowed 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 Modify the selected MAC address in the list.

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

11.14.5 Set SSH

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

Steps

1. Go to **Configuration > System > Security > Security Service** .
2. Check **Enable SSH**.

3. Click **Save**.

11.14.6 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 **Configuration > System > Security > Advanced Security** to complete settings.

11.14.7 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.

Create Self-signed Certificate

Steps

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

   Note

   The certificate ID should be digits or letters and be no more than 64 characters.
3. Click **OK**.
4. **Optional:** Click **Export** to export the certificate, or click **Delete** to delete the certificate to recreate a certificate, or click **Certificate Properties** to view the certificate details.

Create Certificate Request

Before You Start

Select a self-signed certificate.

Steps

1. Click **Create Certificate Request**.
2. Enter the related information.
3. Click **OK**.

Import Certificate

Steps

1. Click **Import**.
2. Click **Create Certificate Request**.
3. Enter the **Certificate ID**.
4. Click **Browser** to select the desired server/client certificate.
5. Select the desired import method and enter the required information.
6. Click **OK**.
7. **Optional:** Click **Export** to export the certificate, or click **Delete** to delete the certificate to recreate a certificate, or click **Certificate Properties** to view the certificate details.

Note

- Up to 16 certificates are allowed.
- If certain functions are using the certificate, it cannot be deleted.
- You can view the functions that are using the certificate in the functions column.
- You cannot create a certificate that has the same ID with that of the existing certificate and import a certificate that has the same content with that of the existing certificate.

Server Certificate/Client Certificate

Note

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

Install CA Certificate

Steps

1. Click **Import**.
2. Enter the **Certificate ID**.
3. Click **Browser** to select the desired server/client certificate.
4. Select the desired import method and enter the required information.
5. Click **OK**.

Note

Up to 16 certificates are allowed.

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**.

11.14.8 Set HTTPS

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

Steps

1. Go to **Configuration > Network > Advanced Settings > HTTPS** .
2. Check **Enable**.
3. **Optional:** Check **HTTPS Browsing** to access the device only via HTTPS protocol.
4. Select a server certificate.

   Note

   - Complete certificate management before selecting server certificate. Refer to *Certificate Management* for detailed information.
   - If the function is abnormal, check if the selected certificate is abnormal in **Certificate Management**.
5. Click **Save**.

11.14.9 Set QoS

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

Note

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

Steps

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

   Note

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

11.14.10 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.

11.15 User and Account

11.15.1 Set User Account and Permission

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

Caution

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

Steps

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

   Administrator

   The administrator has the authority to all operations and can add users/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**.

11.15.2 Online Users

The information of users logging into the device is shown.

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

Chapter 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