GRUNDIG

User Guide

GD-TI-AT26xxT

GD-TI-AT36xxT

www.grundig-security.com

Contents

1 Overview

Thank you for purchasing a **GRUNDIG** product. Before installing or connecting the product, please read first the following documents which you can find in the product package:

- Legal Disclaimer
- Safety Instructions
- Installation Manual for the respective product model

Further information about the product like Data Sheets, CE Documents, etc. can also be found on our homepage www.grundig-security.com.
This User Guide is a user manual for Thermal-cameras.
Please read this User Guide carefully and retain it for future use.

1.1 Brief Description

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

1.2 Function

This section introduces main functions of the device.

Note

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

Fire Detection

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

Temperature Measurement

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

Perimeter Protection

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

2 Device Activation and Accessing

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

Note

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

2.1 Activate Device

For the first-time access, you need to activate the device by setting an admin password. No operation is allowed before activation. You can also activate the device via Web Browser, Grundig IP-Finder or Client Software.

2.1.1 Default User and IP Address

- Default administrator account: admin.
- Default IPv4 address: 192.168.1.100.

2.1.2 Activate via IP-FINDER

IP-FINDER is a tool to detect, activate and modify the IP address of the device over the LAN.

Before You Start

- Get the software from the official website www.grundig-security.com, and install it according to the prompts.
- The device and the PC that runs the IP-FINDER tool should belong to the same subnet.

The following steps show how to activate one device and modify its IP address. For batch activation and IP address modification, refer to *User Manual of IP-FINDER* for details.

Steps

1. Run the IP-FINDER software and search the online devices.
2. Find and select your device in online device list.
3. Input new password (admin password) and confirm the password.

Caution

STRONG PASSWORD RECOMMENDED-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.

4. Click **Activate** to start activation.

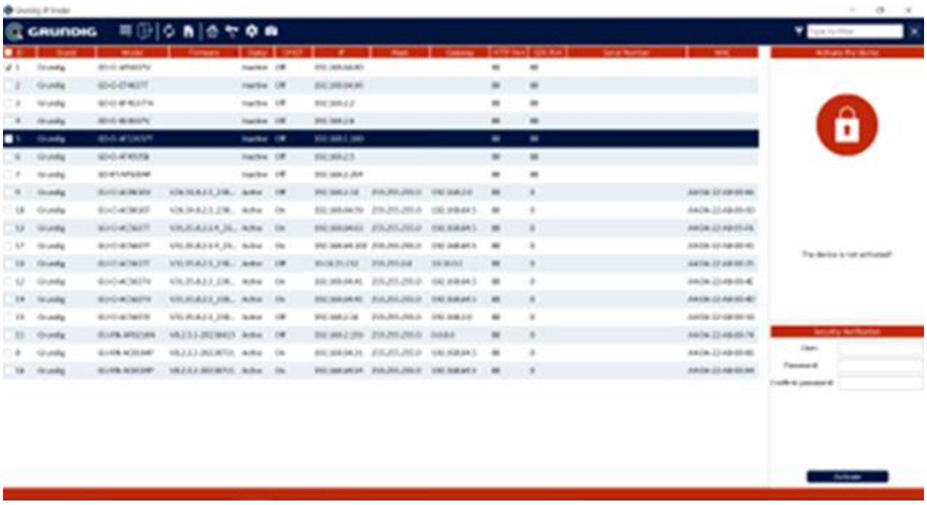


Figure 1.1 Activate via IP-FINDER

Status of the device becomes **Active** after successful activation.

5. Modify IP address of the device.
   1) Select the device.
   2) Change the device IP address to the same subnet as your computer by either modifying the IP address manually or checking **Enable DHCP**.
   3) Input the admin password and click **Modify** to activate your IP address modification.

2.1.3 Activate Camera via SCMS-VMS

SCMS is a PC client to manage and operate your devices. Camera activation is supported by the software.

Before You Start

Get the client software from the official website www.grundig-security.com. Install the software following the prompts.

The camera and the PC that runs the software should be in the same subnet.

Steps

1. Run the client software.
2. Enter **Device Management** or **Online Device**.

3. Check the device status from the device list, and select an inactive camera.
4. Click the **Activate**.
5. Create and confirm the admin password of the camera.

Caution

STRONG PASSWORD RECOMMENDED-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.

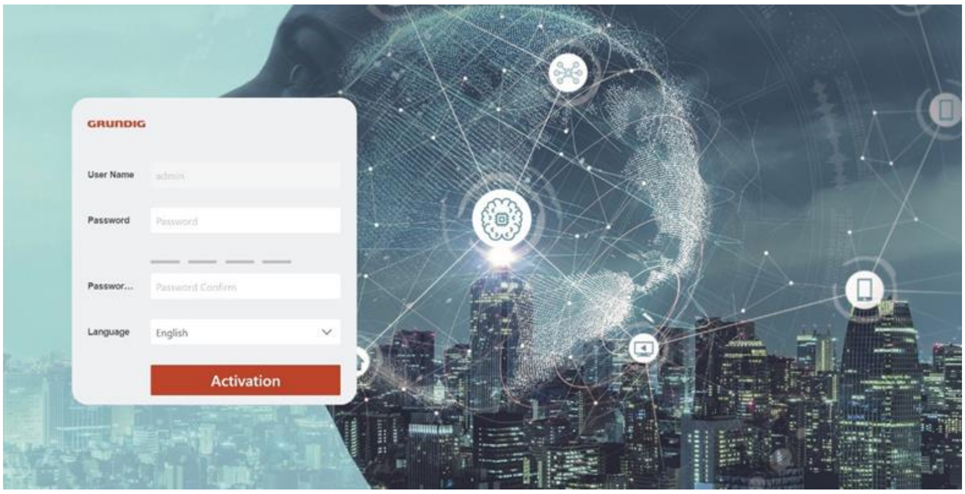
6. Click **OK** to start activation.
   Device status change to **Active** after successful activation.
7. Modify IP address of the device.
   1) Select the device and click **Modify Netinfo** at **Online Device**.
   2) Change the device IP address to the same subnet with your computer by either modifying the IP address manually or checking **DHCP**.
   3) Input the admin password of the device and click **OK** to complete modification.

2.1.4 Activate Device via Web Browser

Use web browser to activate the device. For the device with the DHCP enabled by default, use the IP-FINDER tool or PC client to activate the device.

Before You Start

Make sure your device and your PC connect to the same LAN.



Language English

Figure 1-2 Activation Web-Window

Steps

1. Change the IP address of your PC to the same subnet as the device. The default IP address of the device is 192.168.1.100.

2. Open a web browser and input the default IP address.
3. Create and confirm the admin password.

Caution

STRONG PASSWORD RECOMMENDED-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.

4. Click **OK** to complete activation and enter **Live View** page.
5. Modify IP address of the camera.
   1) Enter IP address modification page. **Configuration** → **Network** → **TCP/IP**
   2) Change IP address.
   3) Save the settings.

2.2 Login

Log in to the device via Web browser.

2.2.1 Plug-in Installation

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

Operating System	Web Browser	Operation
Windows	Internet Explorer 10+	Follow pop-up prompts to complete plug-in installation.
	Google Chrome 57+ Mozilla Firefox 52+ Microsoft Edge 79.0.309+	Click Download Plug-in to download and install plug-in. Go to **Configuration** > **Network** > **Advanced Settings** > **Network Service** to enable WebSocket or WebSockets for normal view if plug-in installation is not required. Display and operation of certain functions are restricted. For example, Playback and Picture are not

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

Note

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

2.2.2 Illegal Login Lock

It helps to improve the security when accessing the device via Internet.
Go to **Configuration** > **System** > **Security** > **Security Service**, and enable **Enable Illegal Login Lock**, **Illegal Login Attempts** and **Locking Duration** are configurable.

Illegal Login Attempts

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

Locking Duration

The device releases the lock after the setting duration.

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 IP-FINDER 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 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.

ModbusTCP

It refers to the protocol through which the device transmits data, such as the thermometry data.

Note

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

3.3 Port Mapping

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

Before You Start

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

Steps

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

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

3. Click **Save**.

3.3.1 Set Auto Port Mapping

Steps

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

Note

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

3.3.2 Set Manual Port Mapping

Steps

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

What to do next

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

3.4 Multicast

Multicast is group communication where data transmission is addressed to a group of destination devices simultaneously. After setting multicast, you can send the source data efficiently to multiple receivers.
Go to **Configuration** > **Network** > **Basic Settings** > **Multicast** for the multicast settings.

IP Address

It stands for the address of multicast host.

Stream Type

The stream type as the multicast source.

Video Port

The video port of the selected stream.

Audio Port

The audio port of the selected stream.

Note

Audio Port varies according to different camera models.

3.5 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**.

3.6 Access to Device via Domain Name

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

Before You Start

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

Steps

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

   DynDNS

   Dynamic DNS server is used for domain name resolution.

   NO-IP

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

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

3.7 Access to Device via PPPoE Dial Up Connection

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

Steps

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

   Dynamic IP

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

   User Name

   User name for dial-up network access.

   Password

   Password for dial-up network access.

   Confirm

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

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

Note

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

3.8 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.

3.9 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.

3.10 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 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**.

3.12 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 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.

3.14 Modbus Communication

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

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

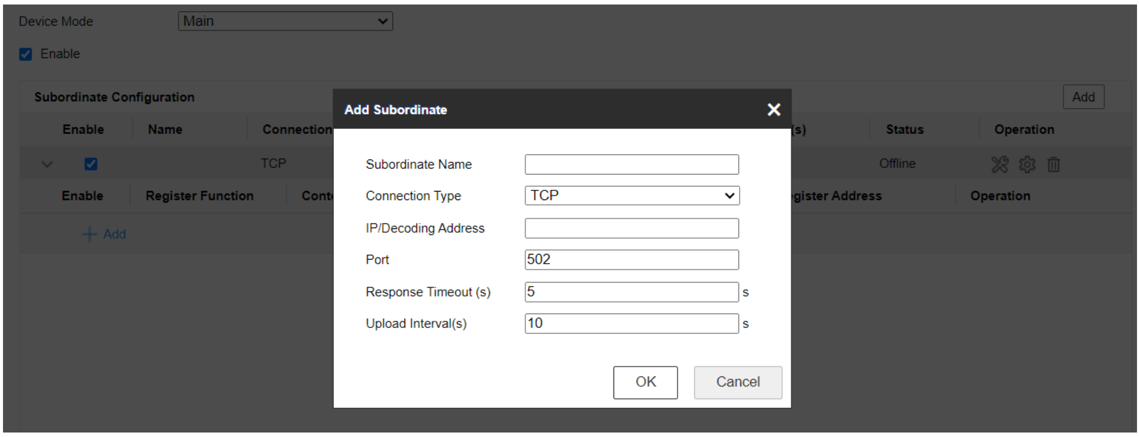
Go to **Configuration** > **Network** > **Advanced Configuration** > **Modbus** to configure the Modbus.

3.14.1 Set Modbus Main Mode

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

Steps

1. Select the **Device Mode** as **Main**.



Device Mode: Main

☑ Enable

Add Subordinate

Subordinate Name:

Connection Type: TCP

IP/Decoding Address:

Port: 502

Response Timeout (s): 5 s

Upload Interval(s): 10 s

Figure 3-1 Main Mode Configuration

2. Check to enable the function of transmitting data via Modbus.
3. Click **Add** to configure the transmission parameters between the device and the subordinate.

Subordinate Name

Customized subordinate for distinguishing between different subordinates.

Connection type

Note

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

TCP

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

RS-485

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

Response Timeout(s)

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

Upload Interval(s)

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

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

Note

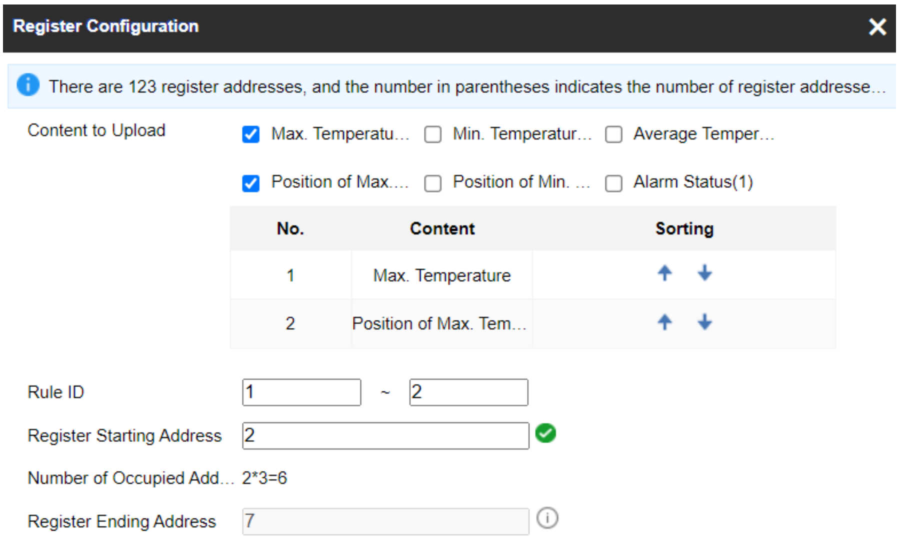
- If the connection status displays **online**, the device is connected to the subordinate normally; if it displays **offline**, the device is disconnected from the subordinate, which may be caused by the subordinate not being online. If the status shows **Error**, refer to the contents of the error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

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

   Note

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

   5) Click **OK**.



Register Configuration

There are 123 register addresses, and the number in parentheses indicates the number of register addresse...

Content to Upload ☑ Max. Temperatu... □ Min. Temperatur... □ Average Temper... ☑ Position of Max.... □ Position of Min. ... □ Alarm Status(1)

No.	Content	Sorting
1	Max. Temperature	↑ ↓
2	Position of Max. Tem...	↑ ↓

Rule ID 1 ~ 2

Register Starting Address 2

Number of Occupied Add... 2*3=6

Register Ending Address 7

Figure 3-2 Register Configuration

7. Click **Save**.

3.14.2 Set Modbus Subordinate Mode

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

Steps

Note

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

1. Go to **Configuration** > **Network** > **Advanced Settings** > **Modbus**.
2. Select Modbus TCP mode.

   Device Mode

   The device is set as **subordinate**, which means that the device operates as a Modbus server processing the request from the client.

   Register Mode

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

Note

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

3.14.3 Modbus Error Code Description

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

Table 3-1 Modbus Error Code Description

Error Code	Name	Description
01	Illegal Function	The function code received in the query is not an allowable action for the server. This may be because the function code is only applicable to newer devices, and was not implemented in the unit selected. It could also indicate that the server is in the wrong state to process a request of this type, for example because it is unconfigured and is being asked to return register values.
02	Illegal Data Address	The data address received in the query is not an allowable address for the server. More specifically, the

Error Code	Name	Description
		combination of reference number and transfer length is invalid. For a controller with 100 registers, the PDU addresses the first register as 0, and the last one as 99. If a request is submitted with a starting register address of 96 and a quantity of registers of 4, then this request will successfully operate (address-wise at least) on registers 96, 97, 98, 99. If a request is submitted with a starting register address of 96 and a quantity of registers of 5, then this request will fail with Exception Code 0x02 “Illegal Data Address” since it attempts to operate on registers 96, 97, 98, 99 and 100, and there is no register with address 100.
03	Illegal Data Value	A value contained in the query data field is not an allowable value for server. This indicates a fault in the structure of the remainder of a complex request, such as that the implied length is incorrect. It specifically does NOT mean that a data item submitted for storage in a register has a value outside the expectation of the application program, since the Modbus protocol is unaware of the significance of any particular value of any particular register.
04	Server Device Failure	An unrecoverable error occurred while the server was attempting to perform the requested action.
05	Acknowledge	Specialized use in conjunction with programming commands. The server has accepted the request and is processing it, but a long duration of time will be required to do so. This response is returned to prevent a timeout error from occurring in the client. The client can next issue a Poll Program Complete message to determine if processing is completed.
06	Server Device Busy	Specialized use in conjunction with programming commands. The server is engaged in processing a long– duration program command. The client should retransmit the message later when the server is free.
08	Memory Parity Error	Specialized use in conjunction with function codes 20 and 21 and reference type 6, to indicate that the extended file area failed to pass a consistency check. The server attempted to read record file, but detected a parity error in the memory. The client can retry the

Error Code	Name	Description
		request, but service may be required on the server device.
10	Gateway Path Unavailable	Specialized use in conjunction with gateways, indicates that the gateway was unable to allocate an intern communication path from the input port to the output port for processing the request. Usually means that the gateway is misconfigured or overload.
11	Gateway Target Device Failed to Response	Specialized use in conjunction with gateways, indicates that no response was obtained from the target device. Usually means that device is not present on the network.

3.15 Operate via Mobile Client

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

Note

SCMS service should be supported by the camera.

3.15.1 Enable SCMS Service on Camera

SCMS service should be enabled on your camera before using the service.
You can enable the service through IP-FINDER software or Web browser.

Enable SCMS Service via Web Browser

Follow the following steps to enable SCMS 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 SCMS 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 SCMS service.

7. Save the settings.

Enable SCMS Service via IP-FINDER Software

This part introduces how to enable SCMS service via IP-FINDER software of an activated camera.

Steps

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

Note

The verification code is required when you add the camera to SCMS service.

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

3.15.2 Set Up SCMS

Steps

1. Get and install SCMS application by searching "SCMS" in App Store or Google Play$^{(TM)}$.
2. Start the application and register for a SCMS user account.
3. Log in after registration.

3.15.3 Add Camera to SCMS

Steps

1. Connect your mobile device to a Wi-Fi.
2. Log into the SCMS 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 SCMS 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 SCMS app.

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.

4.1.1 Window Proportion

- 16:9 refers to the window size is 16 : 9.
- 4:3 refers to the window size is 4 : 3.
- ▭ refers to original ratio window size.▣ refers to self-adaptive window size.

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 the live view.
- Click ■ to stop the live view.

Note

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

4.1.4 Start Digital Zoom

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

Steps

1. Click 🔍 to enable the digital zoom.
2. In live view image, drag the mouse to select the desired region.
3. Click in the live view image to back to the original image.

4.1.5 View Previous/Next Page

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

live view among multiple channels.
Click ← → to switch live view among multiple channels.

4.1.6 Full Screen

This function is used to view the image in full screen mode.
Click to start full screen mode and press ESC button to exit.

4.1.7 Light

Click to turn on or turn off the illuminator.

Caution

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

4.1.8 Wiper

For the device that has a wiper, you can control the wiper via web browser.
Click on live view page. The wiper wipes the window one time.

4.1.9 Lens Initialization

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

4.1.10 Auxiliary Focus

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

4.1.11 Quick Set Live View

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

Steps

1. Click to show quick setup page.
2. Set PTZ, display settings, OSD, video/audio and VCA resource parameters.

- For PTZ settings, see ***Lens Parameters Adjustment*** .
- For display settings, see ***Display Settings***.
- For OSD settings, see ***OSD***.
- For audio and video settings, see ***Video and Image Settings***.
- For VCA settings, see ***Fire Detection***, ***Temperature Measurement***, and ***Perimeter Protection***.

Note

The function is only supported by certain models.

4.1.12 Lens Parameters Adjustment

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

Zoom

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

Focus

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

Iris

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

Note

The function is only supported by certain models.

4.2 Set Transmission Parameters

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

Steps

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

Protocol

TCP

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

UDP

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

MULTICAST

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

Note

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

HTTP

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

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 ensure video fluency even the fluency is enabled.

Custom

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

3. Click **Save**.

5 Video and Image Settings

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

5.1 Video Settings

This part introduces the settings of video parameters, such as, stream type, video encoding, and resolution.
Go to setting page: **Configuration** > **Video/Audio** > **Video**.

5.1.1 Stream Type

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

Main Stream

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

Sub Stream

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

5.1.2 Video Type

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

Video

Only video content is contained in the stream.

Video & Audio

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

Note

Video & Audio varies according to different camera models.

5.1.3 Resolution

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

5.1.4 Bitrate Type and Max. Bitrate

Constant Bitrate

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

Variable Bitrate

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

5.1.5 Video Quality

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

5.1.6 Frame Rate

The frame rate is to describe the frequency at which the video stream is updated and it is measured by frames per second (fps).
A higher frame rate is advantageous when there is movement in the video stream, as it maintains image quality throughout. Note that higher frame rate requires higher bandwidth and larger storage space.

5.1.7 Video Encoding

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

Note

Available compression standards vary according to device models.

H.264

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

H.265

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

MJPEG

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

Profile

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

I-Frame Interval

I-frame interval defines the number of frames between 2 I-frames.
In H.264 and H.265, an I-frame, or intra frame, is a self-contained frame that can be independently decoded without any reference to other images. An I-frame consumes more bits than other frames. Thus, video with more I-frames, in other words, smaller I-frame interval, generates more steady and reliable data bits while requiring more storage space.

SVC

Scalable Video Coding (SVC) is the name for the Annex G extension of the H.264 or H.265 video compression standard.
The objective of the SVC standardization has been to enable the encoding of a high-quality video bitstream that contains one or more subset bitstreams that can themselves be decoded with a complexity and reconstruction quality similar to that achieved using the existing H.264 or H.265 design with the same quantity of data as in the subset bitstream. The subset bitstream is derived by dropping packets from the larger bitstream.
SVC enables forward compatibility for older hardware: the same bitstream can be consumed by basic hardware which can only decode a low-resolution subset, while more advanced hardware will be able decode high quality video stream.

5.1.8 Smoothing

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

5.1.9 Display VCA Info

VCA information can be displayed by Player and Video.

Player

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

Video

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

5.1.10 Audio Settings

It is a function to set audio parameters such as audio encoding, environment noise filtering.
Go to the audio settings page: **Configuration** > **Video/Audio** > **Audio**.

Note

Only certain camera models support the function.

Audio Encoding

Select the audio encoding compression of the audio.

Audio Input

Note

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

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

Environmental Noise Filter

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

5.1.11 Two-way Audio

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

Before You Start

- Make sure the audio input device (pick-up or microphone) and audio output device (speaker) connected to the device is working properly. Refer to specifications of audio input and output devices for device connection.

- If the device has built-in microphone and speaker, two-way audio function can be enabled directly.

Steps

Note

The function varies according to different camera models.

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

5.1.12 Set ROI

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

Before You Start

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

Steps

1. Go to **Configuration** > **Video/Audio** > **ROI**.
2. Check **Enable**.
3. Select **Stream Type**.
4. 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.

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

Note

The higher the ROI level is, the clearer the image of the detected region is.

7. Optional: Select other region No. and repeat the above steps if you need to draw multiple fixed regions.

5.1.13 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.

5.2 Display Settings

It offers the parameter settings to adjust image features.
Go to **Configuration** > **Image** > **Display Settings**.
Click **Default** to restore settings.

5.2.1 Image Adjustment

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

5.2.2 Image Adjustment (Thermal Channel)

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

Manual Correction

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

Note

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

Thermal AGC Mode

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

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

5.2.3 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.

5.2.4 Set Palette

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

Steps

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

Result

The live view displays the image with palette.

5.2.5 Set Target Enhancement

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

Steps

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

   Above (be colored)

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

   Between (be colored)

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

   Below (be colored)

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

5.2.6 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, the more details are shown, but the higher the noise.

5.2.7 Brightness Sudden Change

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

5.2.8 Enhance Regional Image

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

Steps

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

5.2.9 Mirror

When the live view image is the reverse of the actual scene, this function helps to display the image normally.
Select the mirror mode as needed.

Note

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

5.2.10 Video Standard

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

5.2.11 Digital Zoom

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

5.2.12 Scene Mode

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

5.2.13 Local Output

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

5.3 OSD

You can customize OSD (On-screen Display) information such as device name, time/date, font, color, and text overlay displayed on video stream.
Go to OSD setting page: **Configuration** > **Image** > **OSD Settings**. Set the corresponding parameters, and click **Save** to take effect.

Character Set

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

Displayed Information

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

Text Overlay

Set customized overlay text on image.

OSD Parameters

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

5.4 VCA Rule Display Settings

The VCA rule display refers to the function that you can customize the displayed overlay information of the VCA rule, which includes the font size and line and frame color.
You can go to **Configuration** > **Image** > **VCA Rule Display** to select the desired font size, and set the line and frame color.

5.5 Set Privacy Mask

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

Steps

1. Go to privacy mask setting page: **Configuration** > **Image** > **Privacy Mask**.
2. Check **Enable Privacy Mask**.
3. Click **Draw Area**. Drag the mouse in the live view to draw a closed area.

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

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

5.6 Overlay Picture

Overlay a customized picture on live view.

Before You Start

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

Steps

1. Go to picture overlay setting page: **Configuration** > **Image** > **Picture Overlay**.
2. Click **Browse** to select a picture, and click **Upload**.
   The picture with a red rectangle will appear in live view after successfully uploading.
3. Check **Enable Picture Overlay**.
4. Drag the picture to adjust its position.
5. Click **Save**.

5.7 Set Manual DPC (Defective Pixel Correction)

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

Steps

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

Note

- If multiple defective pixels need to be corrected, click 💾 after locating a defective pixel.

Then after locating other pixels, click ⊙ to correct them simultaneously.

- This function is only supported by certain camera models.

---

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

6 Video Recording and Picture Capture

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

6.1 Storage Settings

This part introduces the configuration of several common storage paths.

6.1.1 Set Memory Card

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

Before You Start

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

Steps

1. Go to storage management setting page: **Configuration** > **Storage** > **Storage Management** > **HDD Management**.
2. Select the memory card, and click **Format** to start initializing the memory card.
   The **Status** of memory card turns to **Normal** from **Uninitialized**, which means the memory card can be used normally.
3. Optional: Define the **Quota** of the memory card. Input the quota percentage for different contents according to your need.
4. Optional: Check to enable **POS Information Storage**, then the device will record the POS information forklift filter.

   Note

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

5. Click **Save**.

6.1.2 Set NAS

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

Before You Start

Get the IP address of the network disk first.

Steps

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

   Server Address

   The IP address of the network disk.

   File Path

   The saving path of network disk files.

   Mounting Type

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

6.1.3 Set FTP

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

Before You Start

Get the FTP server address first.

Steps

1. Go to **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. Check **Enable**.
3. Select a record type.

Note

The record type is varied according to different models.

Continuous

The video will be recorded continuously according to the schedule.

Motion

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

Alarm

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

Motion | Alarm

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

Motion & Alarm

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

Event

The video is recorded when configured event is detected.

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

Overwrite

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

Pre-record

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

Post-record

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

Stream Type

Select the stream type for recording.

Note

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

Recording Expiration

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

6. Click **Save**.

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. Set search condition and click **Search**.
   The matched video files showed on the timing bar.
3. Click ▶ to play the video files.
   - Click ✂ to clip video files.
   - Click ⛶ to play video files in full screen. Press **ESC** to exit full screen.

Note

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

4. Click ⤓ on the playback interface to download files.
   1) Set search condition and click **Search**.
   2) Select the video files and then click **Download**.

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

6.3 Capture Configuration

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

6.3.1 Capture Automatically

This function can capture pictures automatically during configured time periods.

Before You Start

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

Steps

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

   Timing

   Capture a picture at the configured time interval.

   Event-Triggered

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

6.3.2 Capture Manually

Steps

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

   JPEG

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

BMP

The picture is compressed with good quality.

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

6.3.3 View and Download Picture

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

Steps

1. Click **Picture**.
2. Set search condition and click **Search**.
   The matched pictures showed in the file list.
3. Select the pictures then click **Download** to download them.

Note

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

7 VCA Resource

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

7.1 Temperature Measurement

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

7.1.1 Thermography Configuration Flow Chart

This part introduces the process of configuring temperature measurement.

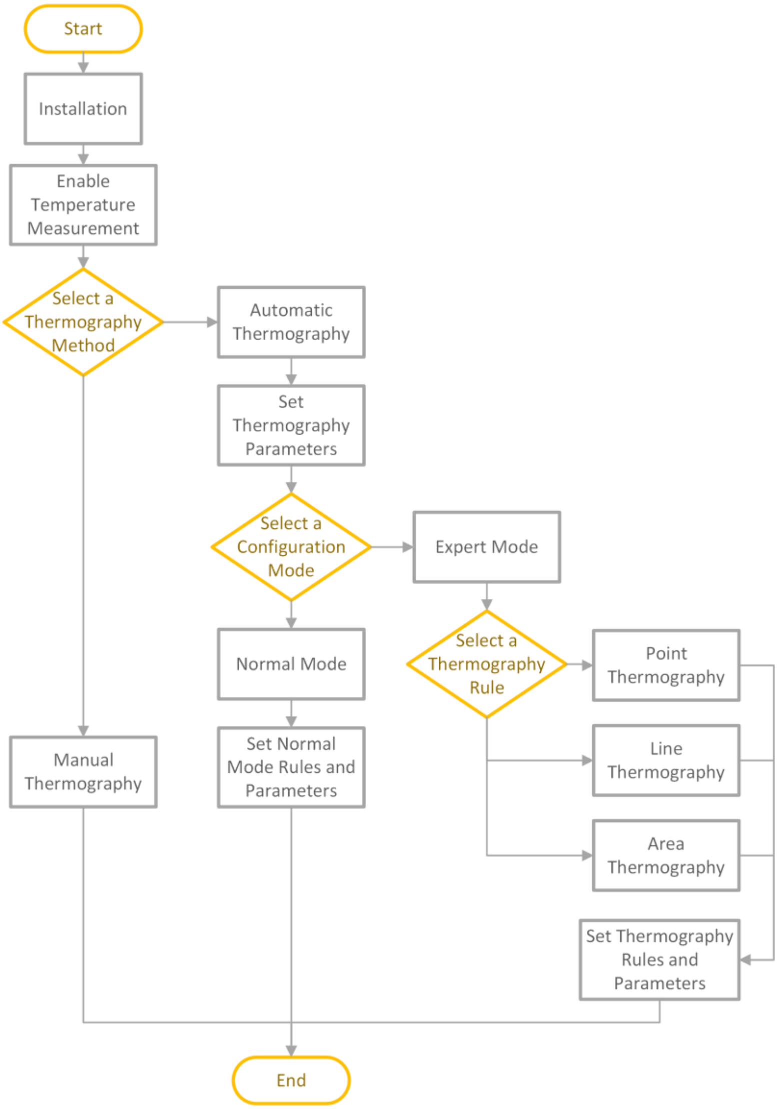

Start
Installation
Enable Temperature Measurement
Select a Thermography Method
Automatic Thermography
Set Thermography Parameters
Select a Configuration Mode
Expert Mode
Normal Mode
Select a Thermography Rule
Point Thermography
Line Thermography
Area Thermography
Manual Thermography
Set Normal Mode Rules and Parameters
Set Thermography Rules and Parameters
End

Figure 7-1 Thermography Configuration Flow Chart

Note

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

7.1.2 Automatic Thermography

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

Set Thermography Parameters

Configure the parameters of temperature measurement.

Steps

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

   Display Temperature Info.

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

   Enable **Rules** to display the rules information on live view.
2. Click **Save**.
3. Go to **Configuration** > **Temperature Measurement & Fire Prevention** > **Basic Settings** to configure parameters.

   Enable Temperature Measurement

   Check to enable temperature measurement function.

   Enable Color-Temperature

   Check to display Temperature-Color Ruler in live view.

   Display Temperature Info. on Stream

   Check to display temperature information on the stream.

   Display Max./Min./Average Temperature

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

   Rule Name

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

   Position of Thermometry Info

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

   Near Target

   Display the information beside the temperature measurement rule.

   Top Left

Display the information on the top left of screen.

Add Original Data on Capture

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

Add Original Data on Stream

Add and save original raw data to stream. The function requires higher network bandwidth.

Picture Quality

Set picture quality as high, medium, or low.

Data Refresh Interval

It means the refresh interval of original data.

Display Pixel-to-Pixel Thermometry Data on Stream

Add and save real-time pixel-to-pixel thermometry data to stream. The function requires higher network bandwidth.
The function varies according to different camera models.

Pixel-to-Pixel Thermometry Data Refresh Interval

It means the refresh interval of thermometry data added to the stream.

Unit

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

Temperature Range

Select the temperature measurement range. The device can adjust the temperature range automatically if you select **Auto**.

Atmospheric Temperature

Set the atmospheric temperature.

Atmospheric Humidity

Set the atmospheric humidity.

Atmospheric Transmissivity

Set the atmospheric transmissivity from 0 to 1.

Distance Mode

Select the distance mode for temperature measurement.

Self-Adaption

This mode is suitable for moving objects. In this mode, device automatically adjusts parameters according to the distance to objects, so as to ensure temperature measurement accuracy.

Fixed Distance

This mode is suitable for fixed objects or objects moving in a very small area.

Optical Transmissivity

Set the optical transmissivity of external optical material (e.g.: germanium window) to improve the temperature measuring accuracy. This parameter varies according to different camera models.

Calibration Coefficient

Check to enable it and set the value of calibration coefficient to get the temperature of the external window or optical material automatically. The setting range is 0 to 30. This parameter varies according to different camera models.

Note

You can get the setting value from SDK software.

External Optics/Window Correction

Set the temperature of the external window or optical material (e.g.: germanium window) to correct the measured temperature. This parameter varies according to different camera models.

Version

View the version of current algorithm.

Calibration File Version

View the version of calibration file.

Alarm Interval

Set the alarm interval between two alarms.

4. Go to **Temperature Measurement** > **Advanced Settings** > **Algorithm Filter** to filter false alarm.

Forklift Filter

Enable this function when there are forklifts or high temperature moving objects, or it may cause false alarm. You can select the filter level to filter out different kinds of objects and set the filtering temperature.

Low

In this level, it only filters the complete forklift.

Medium

In this level, it filters the complete forklift and all moving objects, such as a partially covered but moving forklift in operation.

High

In this level, it filters the complete forklift, all moving objects, and still objects after movement whose temperature are higher than the pre-alarm temperature.

Smoking Filter

Enable this function to filter out high temperature alarms triggered by smoking.

Display Filtering Status

An OSD will be displayed when the function is enabled.

Restart Algorithm Library

Click **Restart** to restart the algorithm library of the corresponding filter function.

Note

- The **Smoking Filter** and **Forklift Filter** vary according to different camera models.
- **Perimeter Protection** and **Forklift Filter** are mutually exclusive.

5. Click **Save**.

Set Normal Mode

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

Steps

1. Go to **Configuration** > **Temperature Measurement & Fire Prevention** > **Basic Settings**, and check **Enable Temperature Measurement**.
2. Refer to ***Set Thermography Parameters*** to set the parameters.
3. Go to **Configuration** > **Temperature Measurement & Fire Prevention** > **Advanced Settings**, and select **Normal**.
4. Configure the parameters of normal mode.

Emissivity

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

Distance

The distance between the target and the device.

Pre-Alarm Threshold and Filtering Time

When the temperature of target exceeds the **Pre-Alarm Threshold** and this status lasts not shorter than the **Filtering Time**, the pre-alarm is triggered.

Alarm Threshold and Filtering Time

When the temperature of target exceeds the **Alarm Threshold**, and this status lasts not shorter than the **Filtering Time**, the alarm is triggered.

Pre-Alarm Output and Alarm Output

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

Temperature Sudden Change Alarm

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

Note

Temperature sudden change alarm is only supported by certain device models.

5. Refer to ***Set Arming Schedule*** for setting scheduled time. Refer to ***Linkage Method Settings*** for setting linkage method.
6. Optional: Set the offsite pre-alarm/alarm specially during off-hours when there are less causes of false alarms. You can set the lower alarm threshold to improve the efficiency of quick alarm.

Note

The function varies according to different camera models.

1) Check **Enable Offsite**.
2) Set the offsite pre-alarm/alarm and follow step 4~5 to adjust the pre-alarm/alarm threshold and arming schedule during working hours.

Note

The same parameters and linkage method apply to the two kinds of pre-alarm/alarm, only the threshold and arming schedule vary.

Offsite Pre-Alarm Threshold

When the temperature of target exceeds the **Offsite Pre-Alarm Threshold** during the **Offsite Arming Schedule**, and this status lasts not shorter than the **Filtering Time**, the pre-alarm is triggered.

Offsite Alarm Threshold

When the temperature of target exceeds the **Offsite Alarm Threshold** during the **Offsite Arming Schedule**, and this status lasts not shorter than the **Filtering Time**, the alarm is triggered.

Offsite Arming Schedule

Click and drag the time bar to select the arming off-hours for offsite pre-alarm and alarm.

7. Click **Save**.
The maximum and minimum temperature will be displayed on the live view.

Note

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

Set Expert Mode

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

Steps

1. Go to **Configuration** > **Temperature Measurement & Fire Prevention** > **Basic Settings**, check **Enable Temperature Measurement**.
2. Refer to ***Set Thermography Parameters*** to set the parameters.
3. Go to **Configuration** > **Temperature Measurement & Fire Prevention** > **Advanced Settings**, select **Expert**.
4. Select and enable the temperature measurement rules. Please refer to ***Set Thermography Rule*** for setting the rule.
5. Optional: Click **Area's Temperature Comparison** to set the alarm rules and the temperature.
6. Click **Save**.
   The maximum temperature and thermography rules will be displayed on the live view.

   Note

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

7. Enable the scan function of device, such as linear scan to monitor the scene.

Set Thermography Rule

Steps

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

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

3. Configure the temperature measurement parameters.

   Emissivity

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

   Distance

   The distance between the target and the device.

   Reflective Temperature

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

Alarm Temperature and Pre-Alarm Temperature

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

Filtering Time

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

Tolerance Temperature

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

Pre-Alarm Output and Alarm Output

When the temperature of target exceeds the pre-alarm or alarm threshold, it triggers the pre-alarm or alarm output of the connected device.

Area's Temperature Comparison

Select two areas and set the comparison rule, and set the temperature difference threshold. The device alarms when the temperature difference meets the setting value.

5. Optional: Check **Enable Forklift Filter**.
6. Refer to ***Set Arming Schedule*** for setting scheduled time. Refer to ***Linkage Method Settings*** for setting linkage method.
7. Optional: Shield certain area from being detected. Refer to ***Set Temperature Measurement Shield Region*** for detailed settings.
8. Optional: Set the offsite pre-alarm/alarm specially during off-hours when there are less causes of false alarms. You can set the lower alarm temperature to improve the efficiency of quick alarm.

Note

The function varies according to different camera models.

1) Click ⚙.
2) Check **Enable Offsite**.
3) Set the offsite pre-alarm/alarm and follow step 4~5 to adjust the pre-alarm/alarm temperature and arming schedule during working hours.

Note

The same parameters and linkage method apply to the two kinds of pre-alarm/alarm, only the threshold temperature and arming schedule vary.

Offsite Pre-Alarm Temperature

When the temperature of target exceeds the **Offsite Pre-Alarm Temperature** during the **Offsite Arming Schedule**, and this status lasts not shorter than the **Filtering Time**, the pre-alarm is triggered.

Offsite Alarm Temperature

When the temperature of target exceeds the **Offsite Alarm Temperature** during the **Offsite Arming Schedule**, and this status lasts not shorter than the **Filtering Time**, the alarm is triggered.

Offsite Arming Schedule

Click and drag the time bar to select the arming off-hours for offsite pre-alarm and alarm.

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

Point Thermography

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

Steps

1. Click in the live view and a cross cursor shows on the interface.
2. Drag the cross cursor to desired position.
   Go to **Live View** interface to view the temperature and rule of the point in thermal channel.

Line Thermography

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

Steps

1. Click and drag the mouse to draw a line in the live view interface.
2. Click and move the line to adjust the position.
3. Click and drag the ends of the line to adjust the length.
   Go to **Live View** interface to view the maximum temperature and rule of the line in thermal channel.

Area Thermography

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

Steps

1. Click and drag the mouse in the live view to draw the area and right click to finish drawing.

2. Click and move the area to adjust the position.
3. Drag the corners of the area to adjust the size and shape.
   Go to **Live View** interface to view the maximum temperature and rule of the area in thermal channel.

Set Temperature Measurement Shield Region

You can configure areas from being detected.

Steps

1. Go to **Configuration** > **Local**, and enable **Display Shield Area**.
2. Check **Enable Shield Area**.
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**.

7.1.3 Manual Thermography

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

Steps

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

7.2 Fire Detection

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

Note

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

7.2.1 Recommended Scene

This part introduces the recommended scenes of fire source detection and helps you select the appropriate scene.
Fire source detection can be applied to indoor and outdoor monitoring with a large detection radius. To achieve the best monitoring effect, please set the installation place as requirements below.

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

7.2.2 Set Dynamic Fire Source Detection

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

Before You Start

Go to **Configuration** > **System** > **Maintenance** > **VCA Resource Type**, select **Temperature Measurement + Perimeter Protection**.

Steps

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

   Fire Source Detection

      Smoking Mode

         Detect smoking behavior in the scene.

      Dynamic Fire

         Detect the dynamic fire source in the scene.

   Sensitivity

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

   Alarm Interval

      Set the alarm interval between two alarms.

   Picture Quality

      Set picture quality as high, medium, or low.

Note

When **VCA Resource Type** is selected as **Temperature Measurement + Perimeter Protection**, only **Smoking Mode** is supported in **Fire Source Detection**. When **VCA Resource Type** is selected as **Temperature Measurement + Fire Detection**, **Dynamic Fire** is also supported in **Fire Source Detection**.

6. Check **Display Fire Source Frame on Stream** to display a red frame around the fire source on stream when fire occurs.
7. Optional: Go to **Smart Event** > **Fire Source Region Shield**. You can shield certain areas from being detected in fire source detection, refer to ***Set Detection Shield Region***.
8. Refer to ***Set Arming Schedule*** for setting scheduled time. Refer to ***Linkage Method Settings*** for setting linkage method.
9. Click **Save**.

7.2.3 Set Detection Shield Region

Steps

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

7.3 Perimeter Protection

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

7.3.1 Set Perimeter Protection Rules

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

Before You Start

Go to **Configuration** > **System** > **Maintenance** > **VCA Resource Type**, select **Temperature Measurement + Perimeter Protection**.

Steps

1. Go to **Configuration** > **Perimeter Protection** > **Rule**.
2. Check **Intelligent Analysis**.
3. 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

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

      Intrusion

      1. Click ⬡ to draw an area in the live view. Right click the mouse to finish drawing.
      2. 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.
      3. Set **Sensitivity**. The higher the value is, the easier the target can be detected.

      Region Entrance and Region Exit

      1. 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**.

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

4) Set other parameters for the rule.

Target Detection

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

Scene Mode

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

Note

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

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**.

4. Optional: Add more rules and set combined event. This function is used to combine multiple events as alarm conditions of the rule and it only triggers alarm when the rule and all the conditions are triggered simultaneously.

1) Check **Alarm Trigger Condition**.
2) Select the condition type. Enable an event first then you can select it as the alarm condition.
3) Select the event according to the selected condition type. Click **Save**.

Note

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

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 VCA information on stream or picture. Refer to ***Set Overlay & Capture Parameters*** for detailed settings.
8. Optional: Calibrate the camera to improve the accuracy. Refer to ***Calibration*** for detailed settings.

7.3.2 Set Perimeter Protection Shield Region

You can configure areas from being detected.

Steps

1. Go to **Configuration** > **Local**, and enable **Display Shield Area**.
2. Go to **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**.

7.3.3 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.

7.3.4 Calibration

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

Note

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

Calibrate Automatically

Before You Start

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

Steps

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

   Note

   The path varies according to different camera models.

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

   Note

   You can set a maximum of two decimal places.

4. Click ▶ to start calibration.

   Caution

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

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

Note

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

Result

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

Calibrate Manually

Steps

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

Note

The path varies according to different camera models.

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

Note

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

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

Caution

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

Result

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

Verify the Calibration Result

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

Steps

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

Note

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

7.3.5 Set Advanced Configuration Parameters

Go to **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.

Activation Period

Set the duration of the alarm with combined events.
Restore Parameters

Restore Default

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

Restart VCA

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

Note

The settings vary according to different models.

7.4 Open Platform

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

Note

Only certain device models support the function.

7.4.1 Set Open Platform

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

Before You Start

Go to **Configuration** > **System** > **Maintenance** > **VCA Resource Type**, select **Temperature Measurement + Open Platform**.

Steps

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

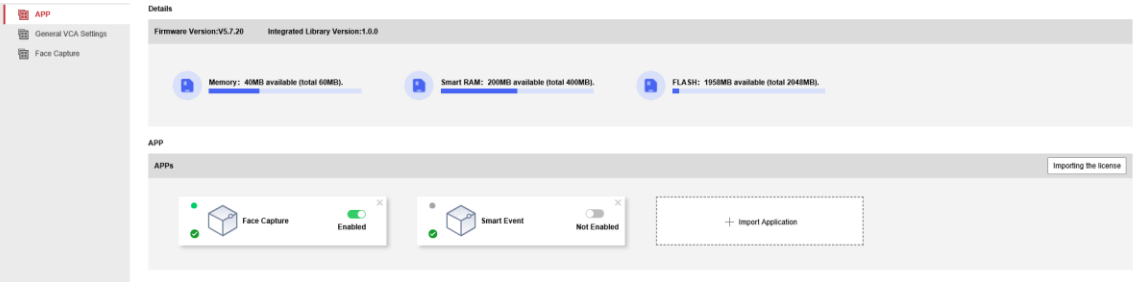
   Note

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

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

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

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



Firmware Version:V5.7.20 Integrated Library Version:1.0.0

Memory: 40MB available (total 60MB).

Smart RAM: 200MB available (total 400MB).

FLASH: 1958MB available (total 2048MB).

Face Capture Enabled

Smart Event Not Enabled

Figure 7-2 Set VCA Resource

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

8.1.1 Normal Mode

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

Steps

1. Select normal mode in **Configuration**.
2. Set the sensitivity of normal mode. The higher the value of sensitivity is, the more sensitive the motion detection is. If the sensitivity is set to ***0***, motion detection and dynamic analysis do not take effect.
3. Set **Detection Target**. Human and vehicle are available. If the detection target is not selected, all the detected targets will be reported, including the human and vehicle.
4. Click **Draw Area**. Click and drag the mouse on the live video, and then release the mouse to finish drawing one area.

Stop Drawing	Stop drawing one area.
Clear All	Clear all the areas.

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

Stop Drawing	Finish drawing.
Clear All	Delete all the drawn areas.

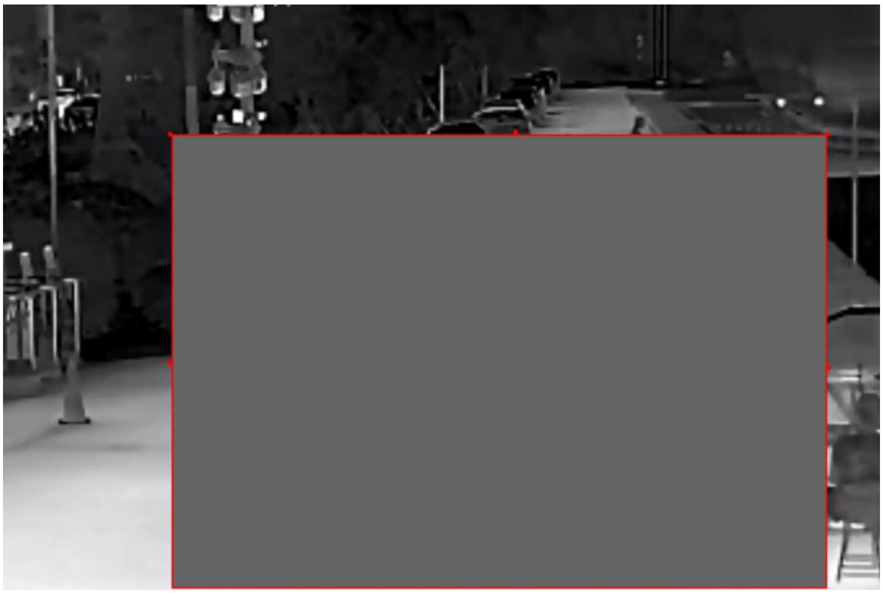


Figure 8-1 Set Video Tampering Area

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

8.3 Set Alarm Input

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

Before You Start

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

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

8.5 Detect Audio Exception

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

Steps

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

Audio Loss Detection

Detect sudden loss of audio track.

Sudden Increase of Sound Intensity Detection

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

Note

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

Sudden Decrease of Sound Intensity Detection

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

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

Note

The function varies according to different models.

8.6 Detect Scene Change

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

Steps

1. Go to **Configuration** > **Event** > **Smart Event** > **Scene Change Detection**.
2. Click **Enable**.
3. Set the **Sensitivity**. The higher the value is, the more easily the change of scene can be detected. But the detection accuracy is reduced.
4. Refer to ***Set Arming Schedule*** for setting scheduled time. Refer to ***Linkage Method Settings*** for setting linkage method.
5. Click **Save**.

Note

The function varies according to different models.

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

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**.

4. Go to **Live View**. You can click ▮ for a quick alarm output configuration and check to enable **Manual Alarm** or turn it off.

Automatic Alarm

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

Steps

1. Set automatic alarm parameters.

   Alarm Output No.

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

   Alarm Name

   Custom a name for the alarm output.

   Delay

   It refers to the time duration that the alarm output remains after an alarm occurs.
2. Set the alarming schedule. For the information about the settings, see ***Set Arming Schedule***.
3. Click **Copy to…** to copy the parameters to other alarm output channels.
4. Click **Save**.

Manual Alarm

You can trigger an alarm output manually.

Steps

1. Set the manual alarm parameters.

   Alarm Output No.

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

   Alarm Name

   Edit a name for the alarm output.

   Delay

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

Alarm Output Self-check

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

Steps

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

9.2.2 FTP/NAS/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.

9.2.3 Send Email

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

Set Email

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

Before You Start

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

Steps

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

Note

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

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

9.2.4 Notify Surveillance Center

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

9.2.5 Trigger Recording

Check **Trigger Recording**, and the device records the video about the detected alarm event.
For recording settings, refer to ***Video Recording and Picture Capture***.

9.2.6 External Alarm Module

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

Steps

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

9.2.7 Module Order

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

Steps

1. Go to **Configuration** > **Event** > **Basic Event** > **Module Order**.
2. Go to **HTTP Order** and check **Enable**.
3. Select the HTTP order from the list and input URL to configure the HTTP server. Up to 10 HTTP orders are supported.
4. Optional: Input the username and password if required.
5. Click **Test** to test the HTTP server connection.
   You can select configured HTTP orders as the linkage method of smart events including **Alarm Input**, **Perimeter Protection**, and **Temperature Measurement**. The alarm or pre-alarm information will upload to the selected HTTP server.

   Note

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

9.2.8 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.

9.2.9 Set Flashing Alarm Light Output

Steps

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

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

3. Set the light action duration and the brightness.

Flashing Duration

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

Brightness

The brightness of the light.

4. Edit the arming schedule.
5. Click **Save**.

Note

Only certain camera models support the function.

10 System and Security

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

10.1 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.

10.2 Search and Manage Log

Log helps locate and troubleshoot problems.

Steps

1. Go to **Configuration** > **System** > **Maintenance** > **Log**.
2. Set search conditions **Major Type**, **Minor Type**, **Start Time**, and **End Time**.
3. Click **Search**.
   The matched log files will be displayed on the log list.
4. Optional: Click **Export** to save the log files in your computer.

10.3 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**.

10.4 Export Diagnose Information

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

10.5 Reboot

You can restart the device via browser.
Go to **Configuration** > **System** > **Maintenance** > **Upgrade & Maintenance**, and click **Reboot**.

10.6 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.

10.7 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.

10.8 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**.

10.9 View Open Source Software License

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

10.10 Time and Date

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

10.10.1 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**.

10.10.2 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**.

10.10.3 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**.

10.11 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**.

10.12 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

The function varies according to different camera models.

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.
- If the **PTZ Protocol** is selected as **modbus-RTU**, the temperature information can be transferred by RS-485 interface.
- In **modbus-RTU**, you can select **CRC Response Transmission** as **Big-Endian** or **Little-Endian**.

3. Click **Save**.

10.13 Set Same Unit

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

Steps

1. Go to **Configuration** > **System** > **System Settings** > **Unit Settings**.
2. Check **Use Same Unit**.

3. Set the temperature unit and distance unit.
4. Click **Save**.

10.14 Security

You can improve system security by setting security parameters.

10.14.1 Authentication

You can improve network access security by setting RTSP and WEB authentication.
Go to **Configuration** > **System** > **Security** > **Authentication** to choose authentication protocol and method according to your needs.

RTSP Authentication

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

RTSP Digest Algorithm

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

WEB Authentication

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

WEB Digest Algorithm

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

Note

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

10.14.2 Security Audit Log

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

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

Search Security Audit Logs

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

Steps

> **Note**
>
> This function is only supported by certain camera models.

1. Go to **Configuration** > **System** > **Maintenance** > **Security Audit Log**.
2. Select log types, **Start Time**, and **End Time**.
3. Click **Search**.
   The log files that match the search conditions will be displayed on the Log List.
4. Optional: Click **Export** to save the log files to your computer.

10.14.3 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**.

10.14.4 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**.

10.14.5 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 function's 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, the camera will remind you the day before the expiration day. 1~30 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**.

10.14.6 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.

10.14.7 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.

10.14.8 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**.

10.14.9 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**.

10.14.10 Set IEEE 802.1X

You can authenticate user permission of the connected device by setting IEEE 802.1X.
Go to **Configuration** > **Network** > **Advanced Settings** > **802.1X**, and enable the function.
Select protocol and version according to router information. User name and password of server are required.

Note

- If you set the **Protocol** to **EAP-TLS**, select the **Client Certificate** and **CA Certificate**.
- If the function is abnormal, check if the selected certificate is abnormal in **Certificate Management**.

10.15 User and Account

10.15.1 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**.

10.15.2 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.

11 Appendix

11.1 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