

Flame Detection Network Camera

User's Manual



V1.0.0

Foreword

This manual introduces the characteristics, basic configurations, daily operation and maintenance of the thermal detector (hereinafter referred to as "the camera"). Read carefully before using the device, and keep the manual safe for future reference.

Safety Instructions

The following signal words might appear in the manual.

Signal Words	Meaning
 DANGER	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
 WARNING	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
 CAUTION	Indicates a potential risk which, if not avoided, could result in property damage, data loss, lower performance, or unpredictable result.
 TIPS	Provides methods to help you solve a problem or save you time.
 NOTE	Provides additional information as the emphasis and supplement to the text.

About the Icon

Icon/Parameter	Meaning
Default	Click the button to restore the configuration to the factory configuration.
Refresh	Click the button to display the latest configuration.
Apply	Click the button to save the current configuration.

Revision History

Version	Revision Content	Release Date
V1.0.0	First Release	2026.07

Statements

About the Manual

To simplify the description, the following conventions are made in this manual for common functions, names, and more.

- This manual is suitable for multiple models of products, and functions and pages vary from models. This manual uses the camera for example. The monocular camera does not support the functions of the visible channel.
- If not specifically stated, "the device" appearing in this document refers to "thermal imaging camera".
- To protect personal privacy and security, personal information such as faces and license plates appearing in this document has been masked.
- To ensure the security of devices, the IP address, MAC address, serial number and other information appearing in this document have been masked.

About the Format

Format	Description	Example
>	Menu cascade.	Select "setting > event > face detection".
“ ”	Interface controls, specific terms and so on.	The interface "smart solutions" is shown on the system.
【 】	Device hardware, keyboard keys and so on.	Press 【Enter】 button.
Italics	Indicating variables, which need to be filled in according to the actual situations.	Open your browser and enter "http://device_IP_address" in the address bar.

About the Mouse Operations

Operation	Meaning
Click	Quickly press and release a button.
Double Click	Quickly press and release a button twice in concession.
Drag	Press and hold a mouse button while moving the mouse.
Scroll	Scroll the wheel in the middle of the mouse.

About the Icon/Button

Icon/Button	Description
	Text box. You can enter numbers, letters, Chinese characters, symbols and other characters.
	Drop-down box. Click the icon to display the drop-down menu.

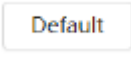
Icon/Button	Description
	Calendar. Click  , and then select the date as needed.
	Click the icon to select the corresponding item.  indicates that the item is selected. Click  to cancel the selection.
	Click the icon to select the corresponding item.  indicates that the item is selected.
	Click  /  to go to the previous or next page.。
	Enter the page and then press the Enter key to go to the specified page.
	Adjust the value. Click  /  or drag  , to adjust the value.
	Click the button to restore the latest configuration.
	Click the button to restore the configuration to the factory configuration.

Table of Contents

Foreword.....	I
Statements.....	II
1 Product Introduction	1
1.1 Overview	1
1.2 Functions	1
2 Configuration Flow	5
3 Device Initialization	6
3.1 Initializing Device.....	6
3.2 Changing IP Address.....	7
3.2.1 Changing One IP Address	7
3.2.2 Changing IP Addresses in Batches.....	8
3.3 Logging in to Web Page	9
3.4 Resetting Password	10
4 Daily Operation	12
4.1 Introduction to Main Page	12
4.2 Live	14
4.2.1 Live Page.....	14
4.2.2 Setting Encode Parameters	15
4.2.3 Quick Toolbar.....	16
4.2.4 Window Adjustment Bar	16
4.2.4.1 Adjustment.....	16
4.2.4.2 Image Adjustment.....	17
4.2.5 Real-time Spot Temperature Monitoring.....	17
4.5 Subscribing Alarm	18
4.5.1 Alarm types.....	18
4.5.2 Subscribing Alarm Information.....	19
5 Smart Operations	21
5.1 Event Management.....	21
5.1.1 Configuring Alarm Linkage.....	21
5.1.1.1 Setting Alarm-in	21
5.1.1.2 Alarm Linkage	23
5.1.1.2.1 Adding Schedule	23
5.1.1.2.2 Record Linkage.....	25
5.1.1.2.3 Snapshot Linkage.....	25
5.1.1.2.4 Alarm-out Linkage.....	25
5.1.1.2.5 Email Linkage.....	26
5.1.1.2.6 Audio Linkage.....	26
5.1.1.2.7 Warning Light.....	26
5.1.2 Configuring Exception	27
5.1.2.1 Configuring SD Card Exception.....	27
5.1.2.2 Configuring Network Exception.....	28
5.1.3 Configuring Video Detection.....	28
5.1.3.1 Configuring Motion Detection	28
5.1.3.2 Configuring Video Tampering	30
5.1.3.3 Configuring Scene Changing.....	31
5.1.4 Configuring Audio Detection	32
5.1.5 Configuring Disarming	33
5.1.6 Configuring Auto Upload	34
5.2 Smart Plan	35
5.2.1 Configuring IVS.....	35
5.2.1.1 Configuration Flow	36
5.2.1.2 Enabling Smart Solutions.....	36
5.2.1.3 Configuring Rules	36
5.2.1.4 Configuring Global Setup	39
5.2.2 Configuring Stereo Behavior Analysis.....	40
5.3 Configuring Smart Thermal.....	40
5.3.1 Configuring Cold Hot Spot Alarm.....	40

5.3.2 Configuring Heat	41
5.3.3 Configuring Temperature Alarm	42
5.3.3.1 Configuring Temperature Measurement Rules	42
5.3.3.2 Configuring Global Configuration	44
5.3.4 Verification	44
6 Record	46
6.1 Playback	46
6.1.1 Playing Back Video	46
6.1.2 Clipping Video	48
6.1.3 Downloading Video	49
6.2 Setting Record Control	50
6.3 Setting Record Plan	50
6.4 Setting Storage	52
7 Picture	55
7.1 Playback	55
7.1.1 Playing Back Picture	55
7.1.2 Downloading Picture	56
7.2 Setting Snapshot Parameters	57
7.3 Setting Snapshot Plan	58
7.4 Setting Snapshot Storage	60
7.5 Setting Auto Upload	62
8 Settings	64
8.1 Setting Local Parameters	64
8.2 Setting Camera Attributes	65
8.2.1 Setting Image Attributes	65
8.2.1.1 Configuring Visible Channel	65
8.2.1.1.1 Setting Working Mode	66
8.2.1.1.2 Adjusting Image	67
8.2.1.1.3 Setting Exposure	68
8.2.1.1.4 Setting Backlight	70
8.2.1.1.5 Setting White Balance	71
8.2.1.1.6 Setting Day/Night Mode	72
8.2.1.1.7 Setting Illuminator	73
8.2.1.1.8 Setting Defog	74
8.2.1.2 Configuring Thermal Channel	75
8.2.3 Setting Video Parameters	79
8.2.3.1 Setting Encode	79
8.2.3.2 Setting Video Overlay	81
8.2.3.2.1 Setting Privacy Masking	81
8.2.3.2.2 Setting Channel Title	82
8.2.3.2.3 Setting Time Title	83
8.2.3.2.4 Setting Location	83
8.2.3.2.5 Setting Font Properties	84
8.2.3.2.6 Setting Picture Overlay	84
8.2.3.2.7 Setting Voltage Information	85
8.2.3.3 Setting ROI	86
8.2.4 Setting Audio Parameters	86
8.2.4.1 Setting Audio	86
8.2.4.2 Setting Alarm Tone	87
8.3 Network Settings	88
8.3.1 Setting TCP/IP	88
8.3.2 Setting Port	91
8.3.3 Setting PPPoE	92
8.3.4 Setting DDNS	93
8.3.5 Setting Email	94
8.3.6 Setting UPnP	96
8.3.7 Setting SNMP	97
8.3.8 Setting Bonjour	99
8.3.9 Setting Multicast	100
8.3.10 Setting Active Registration	101
8.3.11 Setting QoS	102

8.3.12 Platform Access	102
8.3.12.1 Setting National Standard Access.....	102
8.3.12.2 Managing National Standard Certificate.....	104
8.3.12.3 Setting P2P.....	106
8.3.12.4 Setting ONVIF.....	107
8.3.12.5 Setting RTMP.....	107
8.3.13 Setting Basic Service	108
8.4 Storage Management	110
8.5 System Management	110
8.5.1 General	111
8.5.1.1 Setting Basic Parameters.....	111
8.5.1.2 Setting Date.....	111
8.5.1.3 Setting Positioning System.....	113
8.5.2 User Management	113
8.5.2.1 Adding User.....	113
8.5.2.2 Resetting Password.....	116
8.5.2.3 Adding User Group.....	117
8.5.2.4 Adding ONVIF User.....	118
8.5.3 System Upgrade	119
8.5.4 Viewing System Information	119
8.5.4.1 Version.....	119
8.5.4.2 Online User.....	119
8.5.4.3 Legal Information.....	120
8.5.5 Log	120
8.5.5.1 System Log.....	120
8.5.5.2 Remote Log.....	121
8.6 Maintenance	121
8.6.1 Maintenance Requirements	121
8.6.2 Device Maintenance	122
8.6.3 Backup and Restore	123
8.6.3.1 Backup Information.....	123
8.6.3.2 Restore Configuration Information.....	123
8.6.3.3 Restore to Default.....	123
9 Security Management	124
9.1 Scan Security Status.....	124
9.2 System Service	125
9.2.1 802.1x.....	125
9.2.2 HTTPS.....	127
9.3 Attack Defense	127
9.3.1 Firewall.....	127
9.3.2 Account Lockout.....	128
9.3.3 Anti-DoS Attack.....	129
9.4 CA Certificate	130
9.4.1 Installing Device Certificate	130
9.4.1.1 Creating Certificate.....	130
9.4.1.2 Applying for and Importing CA Certificate.....	131
9.4.1.3 Importing the Third-party Certificate.....	132
9.4.2 Installing Trusted CA Certificate	133
9.5 Key Management	134
9.6 A/V Encryption	135
9.7 Security Warning.....	135

1 Product Introduction

1.1 Overview

Flame Detection Network Camera is based on requirements such as temperature measurement, fire prevention, safety protection and night vision. This product can help you view videos, videotape an object, test temperature, warn the potential fire, track a cold/hot spot and analyze a special behavior. This product is widely used in energy industry, transportation, building, power system, public security, government, enterprises, and other fields (such as science, education, culture and health). You can use the product alone or with other storage devices to provide solutions for safety/intelligence city, production safety, safety protection of residential buildings and public area safety.

Its features are as follows:

- Safe and stable
With a full embedded system, this Camera can implement all-day monitoring in a stable way.
- A long detection distance
Wide monitoring range and long detection distance. It can be used for surveillance of wide range and long distance.
- Strong detective ability
With night vision ability, this Camera can clearly distinguish different objects in the dark and can tell camouflage and hidden objects.
- Strong anti-interference ability
This camera can get rid of interference of light intensity under backlight or strong light environment and realize effective detection and recognition.
- Adaptive capacity to complex environment
Applicable to such environment as smoke, smog, rain, snow, and dust which will block your eyes and is very confusing in colors.

1.2 Functions

Live

Table 1-1 Function Description

Function	Description
Live	You can view both the visible images and thermal images. You can use thermal images to identify an object, and then use visible images to view more details of the object.
Voice intercom	• For cameras with voice intercom function, you can talk indoors with a person near the outdoor monitor to solve problems. • Collect the on-site sounds.
Snapshot	During live view, you can capture an abnormal image for further check and handling.
Local recording	During live view, you can record abnormal images for further check and handling.
Real-time reports	For cameras with temperature measurement, you can check the real-time temperature data of your monitoring area.

Function	Description
Real-time temperature measurement	For cameras with temperature measurement, you can check the real-time temperature data of any point in your monitoring area.
Additional functions	• Switch video bit stream. • The visible image will be adjusted to the relevant location when you zoom in or out the thermal image. • Mark information that you need in the surveillance image. • Check whether there is any alarm output. • Magnify part of the surveillance image. Or, scroll the mouse to zoom the whole surveillance image. • Set a smart rule. When an alarm is triggered, you can track the target manually. • Adjust display effect of the surveillance images. • Enable or disable the intelligent rule display.

Record and Picture

Table 1-2 Description of playback function

Function	Description
Manual recording	When playing back a video, you can record the key information of the previous video for further check and handling.
Planned recording	After you set a recording plan, the system will record automatically.
Video playback and download	• Play back a video to find some valuable video fragments. • Download the valuable video fragments for further judgment.
Picture playback	Play back the captured pictures to find something valuable.
Alarm linked recording	When there is an alarm, the system will take videos automatically.

Report

You need to follow certain rules such as time sequence to check history data of temperature saved in the Camera Micro SD card.

Alarm

- Set prompting mode (sound, for example) based on the alarm type.
- Check alarm information.

Account Management

Table 1-3 Function description

Function	Description
Management of user group	• Add, edit or delete an account group. • Manage user permissions based on user groups.
User management	• Add, edit or delete a user account. • Set the user permissions.

Function	Description
ONVIF user management	Add, edit or delete an ONVIF user account.
Change password	Change users' password.

Peripheral Management

You can manage your camera's peripheral such as heater and wiper.

Smart Thermal

Table 1-4 Function description

Function	Description
General Action Analysis	- General actions analysis is available in visible channel, including tripwire intrusion, area intrusion, human-vehicle differentiation. - When an alarm is triggered, the system performs linkages such as recording, alarm output, sending email, and snapshot. - Supports adding detection area and exclusion area.
Stereo Analysis	- Available in visible channel, including smoking detection. - When an alarm is triggered, the system performs linkages such as recording, alarm output, sending email, and snapshot.
Cold/Hot Spot Alarm	- Available in thermal channel only. - According to different colors, displays cold spots and hot spots of the surveillance scene in real time. - When an alarm is triggered, the system performs linkages such as recording, alarm output, sending email, audio, alarm light, and snapshot.
Heat Alarm	- Available in thermal channel. - When an alarm is triggered, the system performs linkages such as recording, alarm output, sending email, audio, alarm light, and snapshot.
Temperature alarm	- When temperature satisfies the alarm conditions of temperature testing rules, an alarm is triggered. - When there is an alarm, the system performs linkage actions such as linkage video recording, alarm output, sending email, PTZ operation and capturing images.

Event

Table 1-5 Function description

Function	Description
Video detection	- Motion detection and video tampering detection. - When an alarm is triggered, the system performs linkages such as recording, alarm output, sending email, and snapshot.

Function	Description
Audio detection	• Audio input abnormal detection and intensity change detection. • When an alarm is triggered, the system performs linkages such as recording, alarm output, sending email, and snapshot.
Alarm settings	• An alarm is triggered when there is an alarm from an external device. • When an alarm is triggered, the system performs linkages such as recording, alarm output, sending email, and snapshot.
Abnormality	• SD card error, network disconnection. • When SD card error or illegal access is triggered, the system links alarm output and sending email. • When network disconnection alarm is triggered, the system links recording and alarm output.

2 Configuration Flow

Figure 2-1 Configuration flow

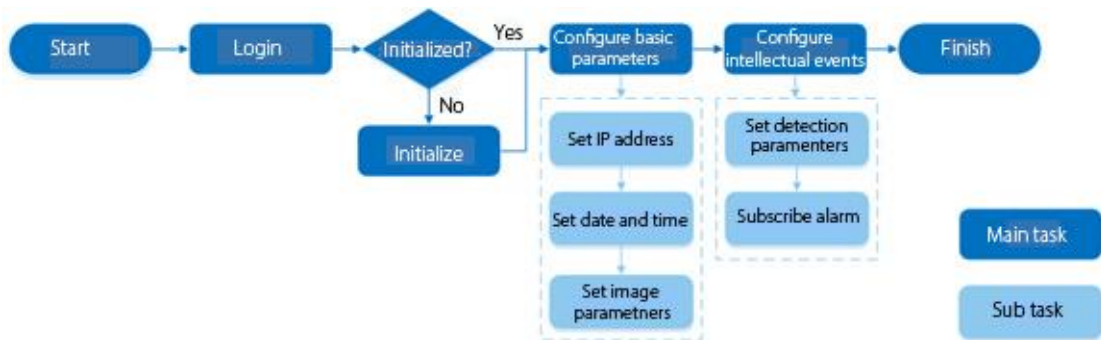


Table 2-1 Configuration introduction

Configuration		Description	Reference
Login		Open IE browser and enter IP address to log in to the web page. The camera IP address is 192.168.1.108 by default.	"3.3 Login WEB" for detailed information
Initialization		When using the device for the first time or restoring factory settings, initialization (such as setting passwords) must be completed before the device can be used normally.	"3.1 Initialization" for detailed information
Basic parameters	IP address	Change IP address according to network planning.	"3.2 change IP address" for detailed information
	Date & time	Set date and time to ensure the recording time is correct and consistent to other devices.	"8.5.1.2 Date & time" for detailed information
	Image	Adjust image parameters according to actual conditions to ensure images appear normal.	"8.2.1 Image"
Intellectual events	Set detection parameters	Set smart solutions or detection parameters.	"5 Smart operations" for detailed information
	Subscribe alarm information	When a user-subscribed alarm event is triggered, the system records the alarm information in the "Alarms" tab.	"4.5 Subscription alarm" for detailed information

3 Device Initialization

3.1 Initializing Device

Device initialization is required for the first-time use. You can initialize the device through ConfigTool or WEB. This manual is based on the operation on the WEB page.



- If not initialized, the device cannot work.
- To ensure the device safety, keep the password properly after initialization and change the password regularly.
- When initializing device, keep the PC IP (192.168.1.108 by default) and device IP in the same network.

Step1 Open IE browser, enter the IP address of the device in the address bar, and then press the Enter key.

Step2 Set password and reserved phone number.

Figure 3-1 Initializing device

Thermal Camera 热成像仪

Set password

User name admin

New password

Confirm password

☒ Number
Used for password reset, please fill in or update timely

Finish

Table 3-1 Description of password configuration

Parameter	Description
New password	The password must consist of 8 to 32 non-blank characters and contain at least two types of characters among upper case, lower case, number, and special character (excluding ' " ; : &). Set a high security level password according to the password security notice.
Confirm password	

Parameter	Description
Reserved phone number	Set a reserved phone number for password reset, selected by default. - Set a reserved phone number for password reset, which is selected by default. When you forget your password, scan the QR code to reset it. You will need to use the reserved phone to receive a security code, which will be used to reset the password for the admin user. - If you didn't set reserved number or plan to change your number, select "  > system management > user management > user" to set phone number. "8.5.2.2 reset password" for detailed information.

Step3 Click "Finish".

3.2 Changing IP Address

The default IP address for all devices is 192.168.1.108. When using the device for the first time or making network adjustments, please modify the device's IP address according to your network planning.

You can use ConfigTool to modify the IP address individually or in batch, or you can log in to the WEB client to change the IP address of the devices.

3.2.1 Changing One IP Address

When there are only a few Cameras or the login passwords of Cameras are different, you can change only one IP address at one time. This section uses changing IP address on WEB page as an example.

Step 1 Log in WEB tab on the camera.



- IP address is 192.168.1.108 by default.
- The default user is admin and the password is the one set during device initialization.

Step 2 In the upper right corner of the interface, click  and select "Network setting > TCP/IP" to configure IP address.

Figure 3-2 Configure IP address

The screenshot shows a configuration window for IP settings. The 'Host Name' field contains 'IPC'. The 'ARP/Ping' toggle is turned on. The 'NIC' dropdown is set to 'Wired(Default)'. The 'Mode' section has 'Static' selected with a radio button. The 'MAC Address' field is empty. The 'IP Version' dropdown is set to 'IPv4'. The 'IP Address', 'Subnet Mask', 'Default Gateway', 'Preferred DNS', and 'Alternate DNS' fields are all empty. At the bottom, there are three buttons: 'Apply' (highlighted with a yellow box), 'Refresh', and 'Default'.

Step 3 Click “Apply”.

3.2.2 Changing IP Addresses in Batches

When there are several Cameras or the login passwords of Cameras are the same, you can modify several IP address at the same time through the ConfigTool.

Prerequisites

- You have obtained the installation package of ConfigTool. To obtain the installation package, you can consult technical support staffs.
- You have achieved network communication between PC (which is with ConfigTool) and the Camera.

Procedure

- Step 1 Open ConfigTool, and click .
- Step 2 Click **Search Settings**.
- Step 3 Set the network segment of the Camera, admin and password. Then click **Save**. After the search, the system displays the searched Cameras.



The default user is admin and the password is the one set during device initialization.

Figure 3-3 Search settings

The 'Settings' window has a title bar with a close button. It contains two checked checkboxes: 'Current network segment search' and 'Other network segment search'. Below these are two IP address ranges: 'Start IP' (192 - 168 - 6 - 67) and 'End IP' (192 - 168 - 6 - 255). There are also fields for 'User name' (admin) and 'Password' (represented by dots). An 'OK' button is at the bottom right.

- Step 4 Choose the device that needs changing and click **Modify IP in Batch**.
- Step 5 Select the mode for setting the IP address based on actual circumstances
- DHCP Mode: When there is a DHCP server in the network, set the Mode as DHCP and the Camera obtains IP addresses from the DHCP server automatically.
 - Manual mode: Set Mode as Static and enter Starting IP, Subnet Mask and Gateway. Then, IP addresses of Cameras are incrementally modified from the start IP address.
- Step 6 Select "Same IP" to set the selected devices to the same IP address.

Figure 3-4 Set IP address

The 'Modify IP Address' window has a title bar with a close button. It shows 'Mode' with 'Static' selected (radio button) and 'DHCP' unselected. Below are input fields for 'Start IP', 'Subnet Mask', and 'Gateway'. To the right of the 'Start IP' field is a checkbox labeled 'Same IP'. At the bottom, it says 'Selected number of devices: 11' and has an 'OK' button.

- Step 7 Click "OK" to finish the modification.

3.3 Logging in to Web Page

After you have changed the IP addresses, you can log in to the web page of the Camera through a browser to operate, configure and maintain. It is recommended to use Internet Explorer 11 or Google Chrome as your browser.

- Step 1 Open the browser, enter the IP address of the camera in the address bar and press the Enter key.
- Step 2 Enter user name and password and click "Login".
The system displays a preview interface.



- The default user is admin and the password is the one set during device initialization.
- When logging into the system for the first time, you will be prompted to install a plugin. Please follow the instructions to save and install the plug in.
- Different devices may show different functions, please refer to the actual interface for accuracy.

Related Operation

Click  in the upper right corner and select “log out” to end the process.

3.4 Resetting Password

After you have provided a reserved phone number, if you forget the password, you can refer to this section to reset the password using the reserved phone number.

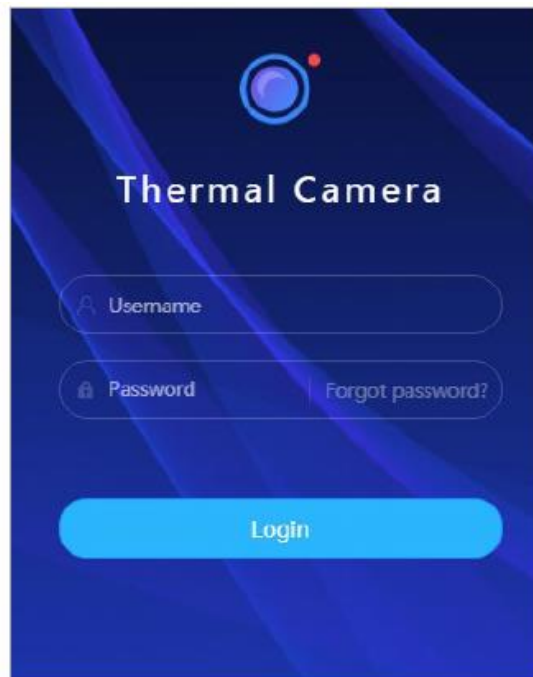
Prerequisite

You have reserved your phone number.

Procedure

- Step 1 Open the IE browse, enter the IP address of the camera in the address bar and press the Enter key.
- Step 2 Click **forgot password?**.

Figure 3-5 Forgot password



- Step 3 According to the instructions on the interface, scan the QR code, and the security code will be sent to the email address you have already fulfilled. Enter the security code.



- Reset the password in time when you receive the security code, because the security code will be invalid within 24 hours.
- If you get security codes twice but do not use them, when you get the security code for the third time, the system will prompt failure. To solve this problem, you need to

restore your Camera to default settings or wait 24 hours to get a new one.

Figure 3-6 Forget password

The screenshot shows a web interface for password reset. At the top, there are two tabs: '1 Enter security code' (active) and '2 Reset password'. The main content area includes a QR code with the text 'Please scan the QR code in the actual page' and 'SN:7L*****Q00012' below it. To the right of the QR code, there is a note for administrators: 'Note (for admin only): Please use any APP with QR scanning , scan the QR code and text the scanning result to 10690067124537. The security code will be sent to your reserved phone: 181****7292'. Below this information is a text input field labeled 'Security code' and a blue 'Next' button at the bottom.

Step 4 Click **Next** to reset and confirm password.

Step 5 Click **OK** to finish resetting password.

The system goes back to "Login" page.

4 Daily Operation

4.1 Introduction to Main Page

Log in to the device's WEB interface via a browser. It is recommended to use Internet Explorer 11 or Google Chrome as the browser.

Prerequisites

- Complete the device initialization before logging in to the device's WEB interface. You can check "3.1 Initializing Device" for reference.
- When logging in to the device, you need to ensure that the IP address of the PC is on the same network as the device IP address.

Procedure

Step 1 Open Chrome browser, enter the IP address of the camera (192.168.1.108 by default) in the address bar and press the Enter key.

Step 2 Enter user name and password.
The default user name is admin.



Click "forgot password?" and reset password through reserved phone number. Check "8.5.2.2 Resetting Password" for detailed information.

Step 3 Click "Login".

The system displays the preview interface by default. Check "4.2.1 Preview Page Layout" for more information. Click  in the upper left corner of the page so the system will show WEB main page.



When logging in to the WEB interface for the first time, the system prompts to install a plug-in. Please download and install the plug-in according to the instructions.

Figure 4-1 WEB main page

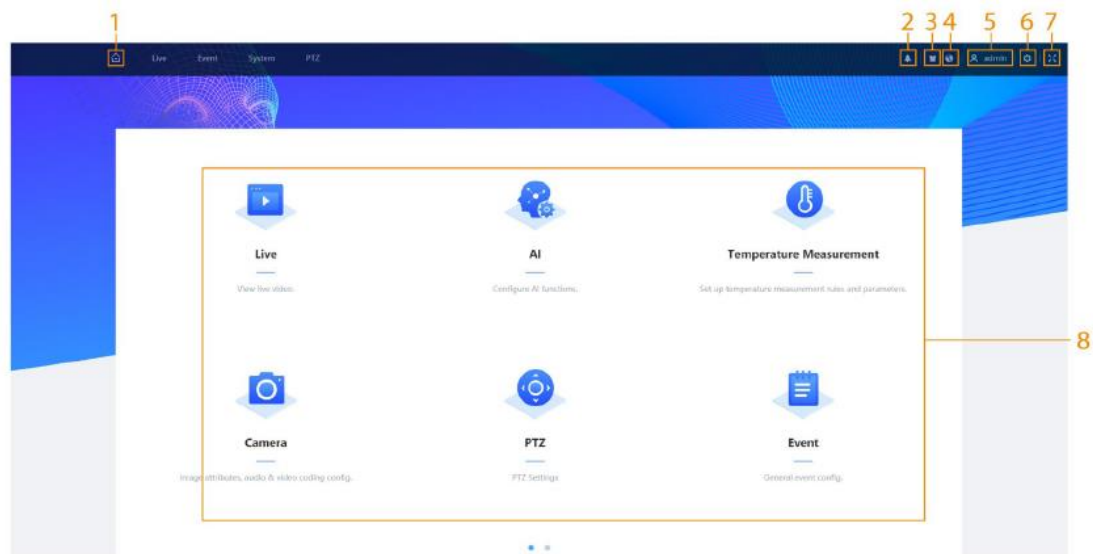


Table 4-1 Description of main page

No.	Name	Description
1		Displays the main page.
2		Subscribe alarm. For details, see "4.5 Subscribing Alarm".
3		Set the skin.
4		Set the language.
5		- Click this button and select "restart" to restart the camera. - Click this button and select "log out" to go back to WEB login page.
6		Set the basic parameters. Check "4 Daily Operation" for detailed information.
7		- Click this button to enter full screen mode. - Click  in the upper right corner to exit full screen mode.

No.	Name	Description
8	Main page	Click   to display more modules. ● Live: View the real-time monitoring image. The preview interface of the multi-channel device displays the monitoring screens of each channel. ● AI: Configure AI functions of the camera. ● Temperature measurement setting: Supports setting temperature measurement rules and temperature comparison. When the temperature meets the set alarm conditions, the system performs linked alarm. ● Camera setting: Set camera properties, including image, video, and audio parameters. ● PTZ setting: Set PTZ (Pan-Tilt-Zoom) functions, including preset points, patrol groups, linear scanning, and tracking. ● Event management: Set alarm linkage parameters for general events. ● System management: Set basic system parameters, user management, external device management, system maintenance, and upgrades. ● Video recording: Set video recording functions, query and play back recorded videos. When playing back videos from a multi-channel device, select the channel number to play back videos from different channels. ● Image: Set image functions, query and play back images. When playing back images from a multi-channel device, select the channel number to play back images from different channels. ● Security center: Check the security status of the device and set security functions. ● Report: query historical temperature data saved on the device's Micro SD card.  Only some devices support temperature measurement settings and reporting functions. Please refer to the actual interface.

4.2 Live

4.2.1 Live Page

Log in to the web page, and the live view page is displayed.

Figure 4-2 Live

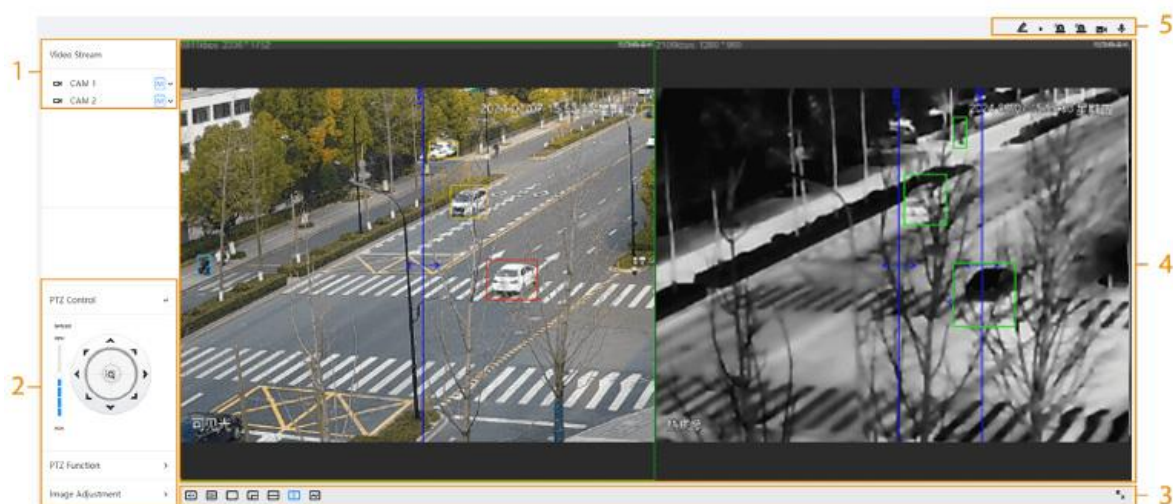


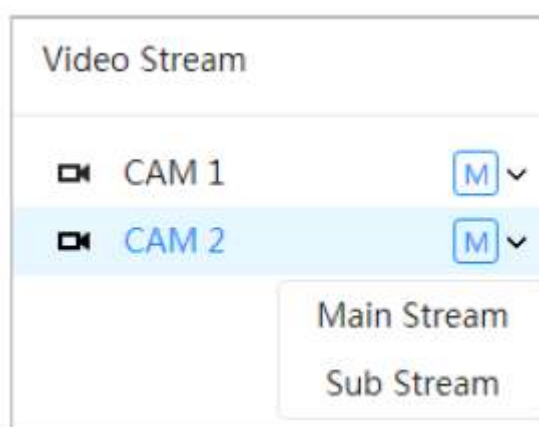
Table 4-2 Live page

No.	Name	Description
1	Channel list	Displays all channels. You can select the channel as needed and set the stream type.
2	Image adjustment	Adjustment operations in live viewing. For details, see "4.2.4 Window A 3 adjustment Bar".
3		
4	Live view	Displays the real-time monitoring image.
5	Quick Toolbar	Display the quick functions supported when viewing real-time footage. Among them, some quick buttons for multi-channel devices are located in the upper right corner of the channel screen. See "4.2.3 Quick Toolbar" for detailed information.

4.2.2 Setting Encode Parameters

In the left part of the live page, click  in the right part of the channel and select the video stream.

Figure 4-3 Video stream



- Main Stream: It has large bit stream value and image with high resolution, but also requires large bandwidth. This option can be used for storage and monitoring. For details, see "8.2.3.1 Setting Encode".
- Sub Stream: It has small bit stream value and smooth image, and requires less bandwidth. This

option is normally used to replace main stream when bandwidth is not enough. For details, see "8.2.3.1 Setting Encode".

-  represents main stream;  represents sub stream.

4.2.3 Quick Toolbar

Introduce the quick functions supported when viewing real-time videos.

Table 4-3 Function description

Icon	Function	Description
	Three consecutive captures	Click this icon to capture three images of the current preview screen at a frequency of one image per second, and save them to the specified storage path. About viewing or configuring storage path, see "8.1 Configuring Local Parameters".
	Partial enlargement	Enlarge the selected area of the screen, and drag the screen while enlarged to view other areas. The following two types of video image scaling operations are supported: • 1: Click this icon to select and enlarge a specific area within the preview screen. Right-click to restore the original state. • 2: Click this icon and scroll the mouse wheel to zoom in or out of the preview screen.
	Force alarm	Display the alarm output status. Click this icon to forcibly turn on or off the alarm. Description of alarm output status: • Red: represents turning on the alarm. • Grey: represents ending the alarm.
	Record	Select the video window, click this icon to record the video, and save it to the set storage path.  About viewing or configuring storage path, see "8.1 Configuring Local Parameters".
	Talk	Click the icon to enable or disable the audio take.

4.2.4 Window Adjustment Bar

4.2.4.1 Adjustment

This section introduces the adjustment of real-time images.

After setting smart rules, click  and select "Enable". The video screen displays smart rules and target detection boxes. To cancel the display, select "Disable".

Table 4-4 Description of adjustment bar

Icon	Function	Description
	Smart rule	After setting smart rules, click this icon to enable or disable the display of information such as smart rule lines and target detection boxes. The default status is "Enabled" each time you log in to the WEB interface.

Icon	Function	Description
	Window layout	This icon is only displayed for multi-channel devices. Click the icon to select the display mode for channel screens. From left to right, they represent: single-channel display only, picture-in-picture display, upper and lower display, left and right display.

4.2.4.2 Image Adjustment

Click Image Adjustment at the lower-left corner of Live page and click “+/-” or drag the slider to adjust the image parameters.



This adjustment does not modify the actual device parameters and only takes effect in the currently open WEB interface.

Figure 4-5 Image Adjustment

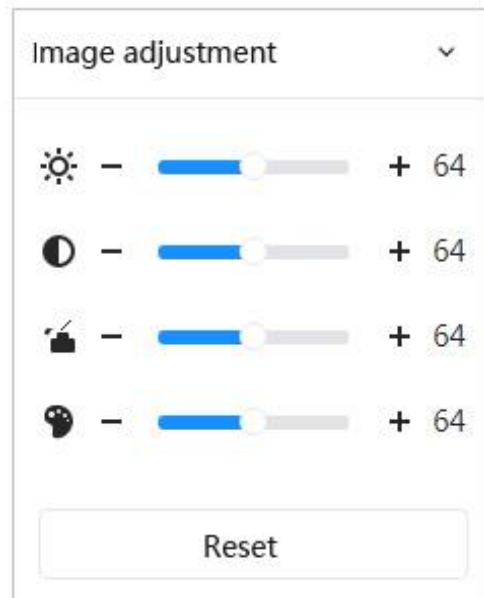


Table 4-6 Description of image adjustment

Icon	Function	Description
	Brightness adjustment	Adjusts the overall image brightness, and changes the value when the image is too bright or too dark. The bright and dark areas will have equal changes.
	Contrast adjustment	Changes the value when the image brightness is proper but contrast is not enough.
	Saturation adjustment	Adjusts the image saturation, this value does not change image brightness.
	Hue adjustment	Makes the color deeper or lighter. The default value is made by the light sensor, and it is recommended.

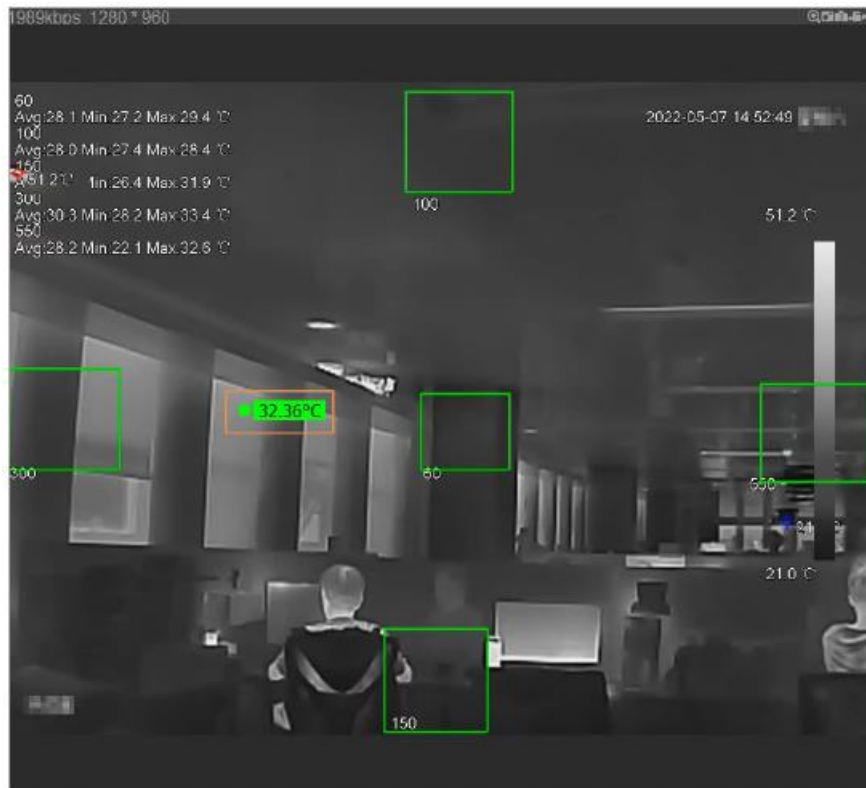
4.2.5 Real-time Spot Temperature Monitoring

View the real-time temperature of any spot on the image. Only Cameras with temperature-

monitoring function support this function.

Log in to the WEB interface of the device, move the mouse cursor to any position on the thermal imaging channel screen in the preview interface and click, the system will display the real-time temperature at that position.

Figure 4-6 Real-time spot temperature monitoring



4.5 Subscribing Alarm

4.5.1 Alarm types

Understand the alarm types of the device and the prerequisites of events.

Table 4-10 Description of alarm types

Alarm type	Description	Prerequisite
Motion Detection	An alarm is triggered when moving object is detected.	Motion detection is enabled. For details, see "5.1.3.1 Configuring Motion Detection".
Disk Full	An alarm is triggered when the free space of SD card is less than the configured value.	The SD card no space function is enabled. For details, see "5.1.2.1 Configuring SD Card Exception".
Disk Error	An alarm is triggered when there is failure or malfunction in the SD card.	SD card failure detection is enabled. For details, see "5.1.2.1 Configuring SD Card Exception".
Video Tampering	An alarm is triggered when the camera lens is covered or there is defocus in video images.	Video tampering is enabled. For details, see "5.1.3.2 Configuring Video Tampering".
External Alarm	An alarm is triggered when there is external alarm input.	The device has alarm input port and external alarm function is enabled. For details, see "5.1.1.1 Setting Alarm-in".

Alarm type	Description	Prerequisite
Safety Warning	The alarm is triggered when the device detects malicious attack.	The safety warning is enabled. See "9.7 Configuring Safety Warning" for more details.
Audio Detection	An alarm is triggered when there is audio connection problem.	Abnormal audio detection is enabled. For details, see "5.1.4 Configuring Audio Detection".
Smart Events	An alarm is triggered when intelligent rule is triggered.	Enable IVS, smoking detection, and other intelligent functions.
Heat (Flame) Detection	An alarm is triggered when the device detects fire.	Enable fire detection. For details, check "5.2.2 Configuring Smoke and Flame Shape Detection".
Temperature Alarm	When temperature satisfies alarm conditions stipulated by temperature testing rules, an alarm is triggered.	You have enabled temperature alarm. For detailed operations, see "5.3.3 Configuring Temperature Alarm".
Hot Spot	When temperature of a hot spot satisfies alarm condition you have set, an alarm is triggered.	You have enabled hot/cold spot tracing. For detailed operations, see "5.3.1 Configuring hot/cold spot alarm".
Cold Spot	When temperature of a cold spot satisfies alarm condition you have set, an alarm is triggered.	

4.5.2 Subscribing Alarm Information

You can subscribe alarm event. When a subscribed alarm event is triggered, the system records detailed alarm information at the right side of the page.



Functions of different devices might be different. Please refer to the actual interface.

- Step 1 Click  at the upper right corner of the interface.
- Step 2 Click  next to "start alarm". The system prompts and records alarm information based on actual conditions.
 - When the subscribed alarm event is triggered and the alarm subscription page is not displayed, a number is displayed on  and the alarm information is recorded automatically. Click  to view the details in the alarm list. You can click Clear to clear the record.
 - When a subscribed alarm event is triggered and the system is on the "Alarm" interface, the corresponding alarm information will be displayed in the alarm list below the alarm interface.
- Step 3 Click "**Subscribing Alarm**" to select the alarm type. For detailed descriptions of alarm types, please refer to "4.5.1 Understanding Alarm Types".
- Step 4 Click  next to **Play Alarm Tone** and select the tone path.
The system will play the selected audio file when the selected alarm is triggered.
- Step 5 (optional) click  next to "**Arming/Disarming**" to start the function.
After disabling alarm, alarm events are not linked and there will be records in the system.

Figure 4-14 Subscribing alarm information

Alarm

☒

Alarm Subscri...

☐ All Types

☐ Motion ...
 ☐ Disk Full
 ☐ Disk Error
 ☐ Video T...

☐ External ...
 ☐ Security ...
 ☐ Audio D...
 ☐ AI Event

☐ Scene C...
 ☒ Temper...
 ☐ Temper...
 ☐ Hot Spot

☐ Cold Spot
 ☐ Heat
 ☐ Burn Ala...
 ☐ Voltage ...

Play Alarm Tone

☒

Disarming

☐

No.	Time	Alarm Type	Source IP ...	Alarm Channel
 No Data				

Clear

5 Smart Operations

5.1 Event Management

You can go to the **Event** page through two ways. Click  to look through the subsequent content.

- Log in to the WEB page, and click "**Event Management**".
- Click  at the upper right corner of the page and select "**Event Management**".

5.1.1 Configuring Alarm Linkage

5.1.1.1 Setting Alarm-in

When an alarm is triggered by the device connected to the alarm-in port, the system performs the defined alarm linkage.

- Step 1 Click  at the upper right corner of the page and select "**Event Management > Alarm Setting**".
- Step 2 Click  next to "**Enable**" to enable alarm linkage.

Figure 5-1 Alarm linkage

The screenshot shows the 'Alarm linkage' configuration page. It includes the following sections and settings:

- General Settings:**
 - Enable: ☒
 - Alarm-in Port: Alarm 1
 - Mode: Alarm
 - Schedule: Full time (with 'Add schedule' button)
 - Anti-dither: 0 (range: sec(0-100))
 - Sensor Type: No
- Event linkage:**
 - Record: Enabled
 - Channel: 1, 2
 - Post-record: 10 (range: sec(10-300))
- Sending Email:** Enabled
- Snapshot:** Enabled
- Alarm-out Port:** Enabled
 - Alarm channel: 1, 2
 - Post-alarm: 3 (range: sec(3-300))
- Audio Linkage:** Enabled
 - Times of play: 5 (range: 1-15)
 - Document: call_ch.wav
- Warning Light:** Enabled
 - Mode: Flash
 - Flashing frequency: Medium
 - Dwell time: 10 (range: 5-30)

At the bottom, there are buttons for 'Time', 'Apply', 'Refresh', and 'Default'.

Step 3 Select an alarm-in port.

Step 4 Select the alarm mode.

- Alarm: When an alarm is triggered by the device connected to the alarm-in port, the system conducts the defined alarm linkage.
 1. Select the schedule and arming periods and alarm linkage actions. For details, see "5.1.1.2 Alarm Linkage". If the exiting schedules cannot meet the scene requirement, you can click Add Schedule to add new schedule. For details, see "5.1.1.2.1 Adding Schedule".
 2. Set the anti-dither time and sensor type.
 - ◇ Anti-Dither: Only record one alarm event during the anti-dither period.
 - ◇ Sensor Type: NO or NC.
- Arming/Disarming: When the camera is directly connected to a third-party alarm platform, and the alarm-in port generates an alarm signal, the system automatically activates one-click disarming.
 1. Select an alarm-in port and sensor type.

2. Click ☐ next to **Arming/Disarming** to enable the arming/disarming mode.

Step 5 Click **"Supply"**.

5.1.1.2 Alarm Linkage

When configuring alarm events, click Event Linkage, and then select alarm linkages (such as record, snapshot). When the corresponding alarm is triggered in the configured arming period, the system will alarm based on alarm linkage set by user .

Figure 5-2 Alarm Linkage

The screenshot displays the 'Alarm Linkage' configuration window. At the top left, there is a '+Event Linkage' button. Below it, there are two main configuration blocks. The first block, 'Record', shows a status of 'Enabled' with a trash icon. It contains a 'Channel' dropdown set to '1', a 'Post-Record' input field with '10', and a range indicator 'sec (10-300)'. The second block, 'Alarm-out Port', also shows a status of 'Enabled' with a trash icon. It contains an 'Alarm Channel' dropdown set to '1', a 'Post-alarm' input field with '3', and a range indicator 'sec (3-300)'. At the bottom of the window are three buttons: 'Apply' (highlighted in blue), 'Refresh', and 'Default'.

5.1.1.2.1 Adding Schedule

Configure arming schedule. The system only performs corresponding linkage actions in the configured period.

Step 1 Click **Add Schedule** next to **Schedule**.

Step 2 Click **Time Plan Table**.

You can add multiple tables, and they will be displayed in the Schedule list.

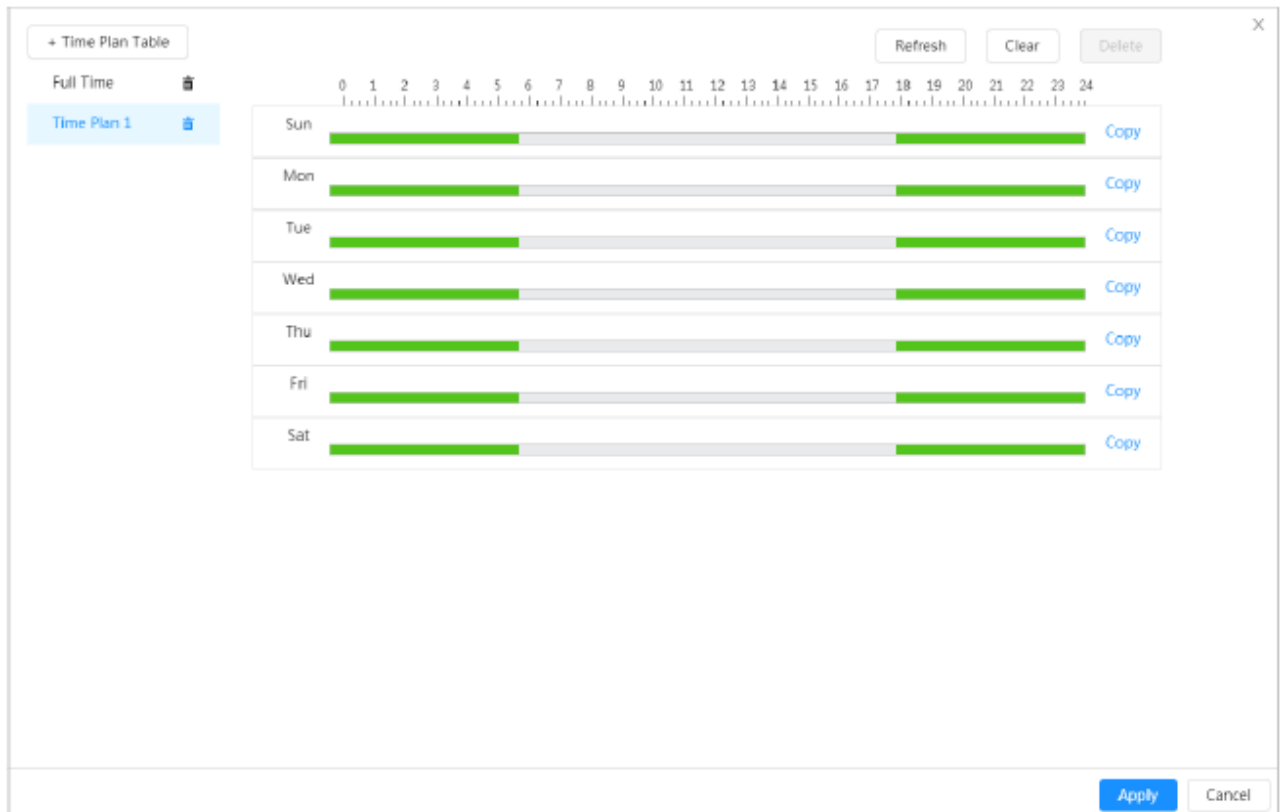
Step 3 Click the table to name to edit the name.

Step 4 Set the arming periods.

Green part on the timeline indicates that the period is armed.

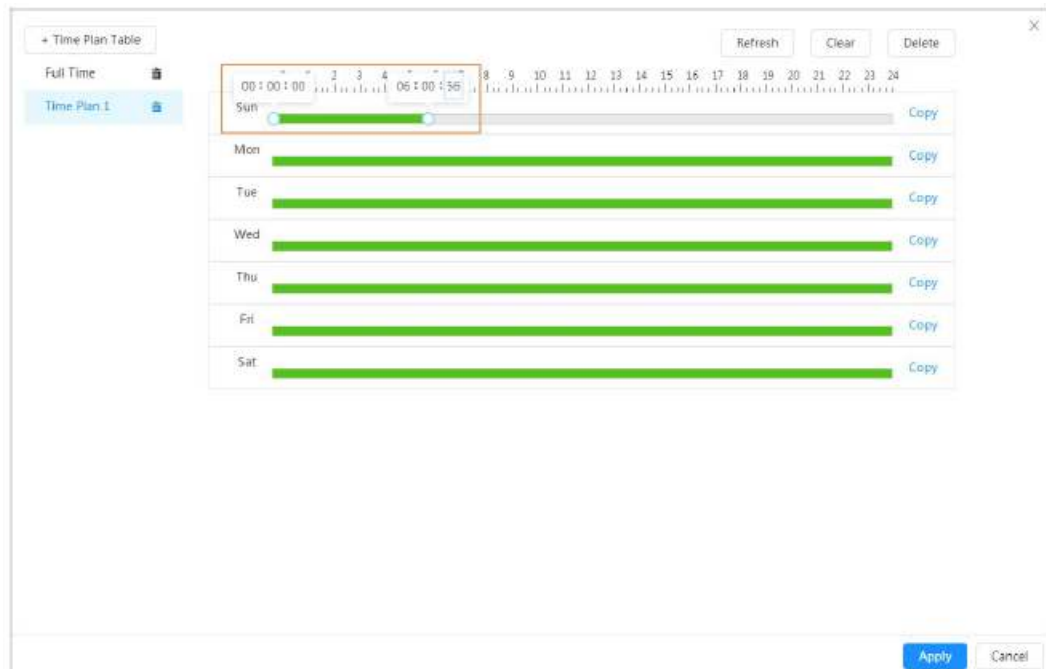
1. Press the left mouse button and drag on the time bar to select the period.

Figure 5-3 Add schedule



2. Click the selected period, enter the specific time in the text box of start time and end time.

Figure 5-4 Set specific time



3. (Optional) Click Copy, select the days, and then click **Apply** to copy the current plan to the selected days.

Step 5 Click "Apply".

5.1.1.2.2 Record Linkage

The system can link record channel when an alarm event occurs. After alarm, the system stops recording after an extended time period according to the Post-Record setting.

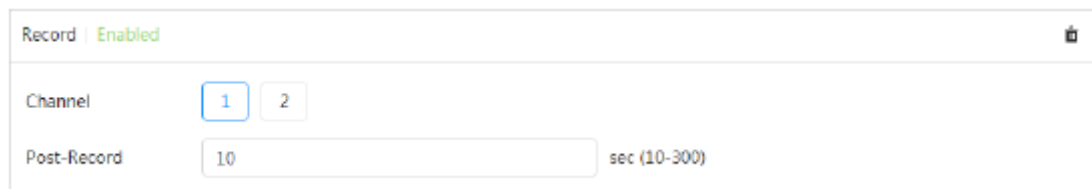
Prerequisites

- After the corresponding alarm type (General, Motion, or Alarm) is enabled, the record channel links recording. For details, see "6.3 Setting Record Plan".
- Enable auto record mode, the record linkage will take effect. For details, see "6.2 Setting Record Control".

Setting Record Linkage

On the **Alarm** page, select **Event Linkage** > **Record** to enable record linkage, select the channel as needed, and set Post-Record to set alarm linkage and record delay. After **Post-Record** is configured, alarm recording continues for an extended period after the alarm ends.

Figure 5-5 Record Linkage



Record	Enabled	
Channel	1 2	
Post-Record	10	sec (10-300)

5.1.1.2.3 Snapshot Linkage

After snapshot linkage is configured, the system can automatically alarm and take snapshots when an alarm is triggered.

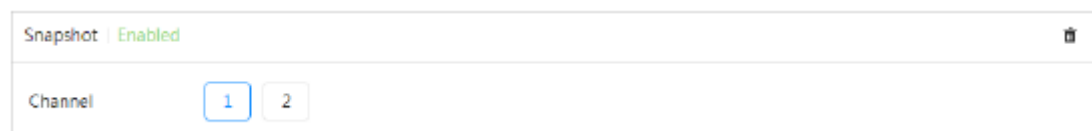
Prerequisite

After the corresponding alarm type (**General**, **Motion**, or **Alarm**) is enabled, the snapshot channel links capturing picture. For details, see "6.3 Setting Record Plan".

Setting Record Linkage

On the **Alarm** page, select **Event Linkage** > **Snapshot** to enable snapshot linkage, and select the channel as needed.

Figure 5-6 Snapshot Linkage



Snapshot	Enabled	
Channel	1 2	

5.1.1.2.4 Alarm-out Linkage

On the **Alarm** page, select **Event Linkage** > **Alarm-out Port** to enable alarm-out linkage, select the channel as needed, and then configure **Post alarm**. When alarm delay is configured, alarm continues for an extended period after the alarm ends.



When a device has multiple alarm output channels, it is necessary to select the linked alarm output channels.

Figure 5-7 Alarm-out Linkage

Alarm-out Port Enabled		🗑️
Alarm Channel	1 2	
Post-alarm	3	sec (3-300)

5.1.1.2.5 Email Linkage

When an alarm is triggered, the system will automatically send an email to users.

Prerequisite

Email linkage takes effect only when SMTP is configured. For details, see "8.3.5 Email".

Setting Email Linkage

On the **Alarm** page, select **Event Linkage**> **Sending Email** to set email linkage.

Figure 5-8 Email linkage

Send Email Enabled	🗑️
----------------------	----

5.1.1.2.6 Audio Linkage

When an alarm is triggered, the system can automatically produce audio for warning.

On the **Alarm** page, select **Event Linkage** > **Audio Linkage** to enable alarm-out linkage, and then set the play count and audio file.

Figure 5-9 Audio Linkage

Audio Linkage Enabled		🗑️
Play Count	5	(1-15)
File	alarm1.pcm	▼

5.1.1.2.7 Warning Light

When an alarm is triggered, the system can automatically start warning light.

On the **Alarm** page, select **Event Linkage** > **Warning Light** to enable alarm-out linkage, set the mode, stay time, and then click time to set the arming periods.

Figure 5-10 Warning light linkage



Warning Light | Enabled

Mode: Always On

Stay Time: 10 (5-30)

Time

5.1.2 Configuring Exception

Abnormality includes SD card, network exception, and voltage detection.



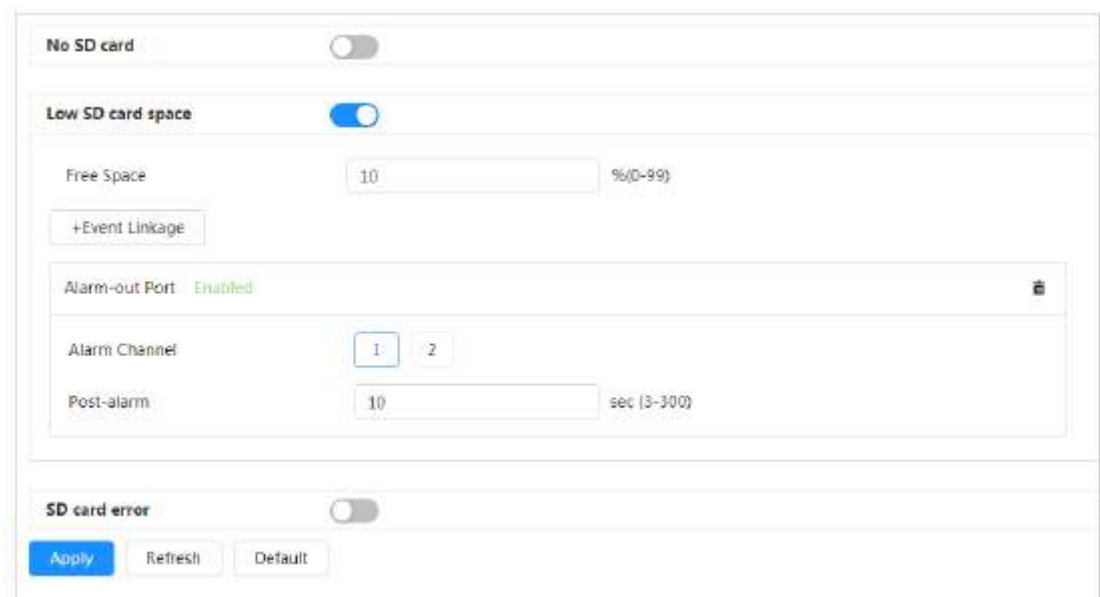
Only the device with SD card has the abnormality functions, including **No SD card**, **Low SD card space**, and **SD card error**.

5.1.2.1 Configuring SD Card Exception

In case of SD card exception, the system performs alarm linkage. The event types include **No SD card**, **Low SD card space**, and **SD card error**. Functions might vary with different models. Please refer to the actual page.

- Step 1 Click  at the upper right corner of the page and select **Event Management > Exception > SD Card Exception**.
- Step 2 Select event type and enable detection of SD card exception.
When the "event type" is set to "SD card capacity insufficient", it supports setting the "available capacity". When the remaining capacity of the SD card is less than this value, an alarm will be triggered.

Figure 5-11 SD card exception



No SD card: ☐

Low SD card space: ☒

Free Space: 10 % (0-99)

+Event Linkage

Alarm-out Port: Enabled

Alarm Channel: 1 2

Post-alarm: 10 sec (3-300)

SD card error: ☐

Apply Refresh Default

- Step 3 Set alarm linkage actions. For details, see "5.1.1.2 Alarm Linkage".
- Step 4 Click **Apply**.

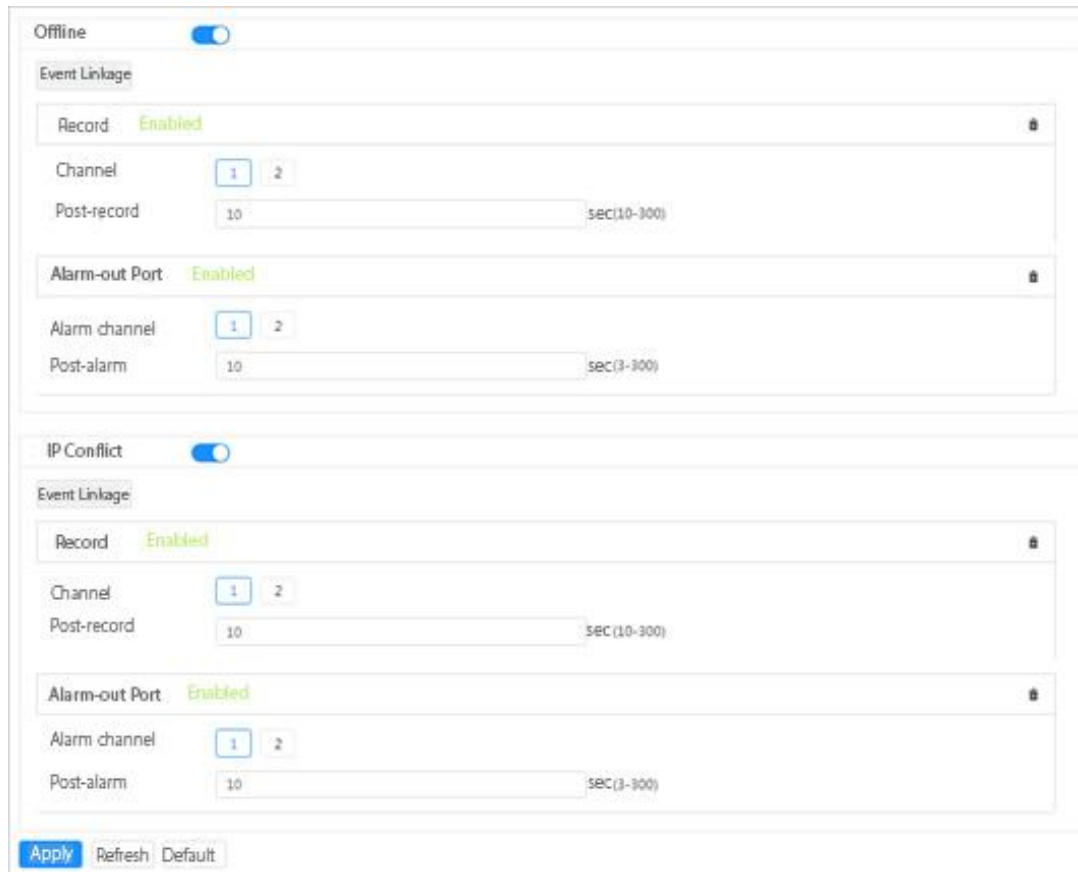
5.1.2.2 Configuring Network Exception

In case of network abnormality, the system performs alarm linkage. The event types include **Offline** and **IP Conflict**.

Step 1 Click  at the upper right corner of the page and select **Event Management > Exception > Network Exception**.

Step 2 Select **Offline** and **IP Conflict** to detect network exception.

Figure 5-12 Network exception



The screenshot displays the configuration interface for network exceptions, divided into two sections: 'Offline' and 'IP Conflict'. Each section has a toggle switch at the top, which is currently turned on (blue). Below each toggle is an 'Event Linkage' section containing three rows of settings: 'Record' (set to 'Enabled'), 'Channel' (with input fields '1' and '2'), and 'Post-record' (set to '10' with a unit of 'sec(10-300)'). A second set of settings follows: 'Alarm-out Port' (set to 'Enabled'), 'Alarm channel' (with input fields '1' and '2'), and 'Post-alarm' (set to '10' with a unit of 'sec(3-300)'). At the bottom of the interface are three buttons: 'Apply' (highlighted in blue), 'Refresh', and 'Default'.

Step 3 Set alarm linkage actions. For details, see "5.1.1.2 Alarm Linkage".

Step 4 Click **Apply**.

5.1.3 Configuring Video Detection

Check whether there are considerable changes on the video by analyzing video images. In case of any considerable change on the video (such as moving object, fuzzy image), the system performs an alarm linkage.

5.1.3.1 Configuring Motion Detection

The system performs an alarm linkage when a moving object appears in the image and its moving

speed reaches the configured sensitivity.



- If you enable motion detection and smart motion detection simultaneously, and configure the linked activities, the linked activities take effect as follows:
 - ◊ When motion detection is triggered, the camera will record and take snapshots, but other configured linkages such as sending emails, PTZ operation will not take effect.
 - ◊ When smart motion detection is triggered, all the configured linkages take effect.
- If you only enable motion detection, all the configured linkages take effect when motion detection is triggered.

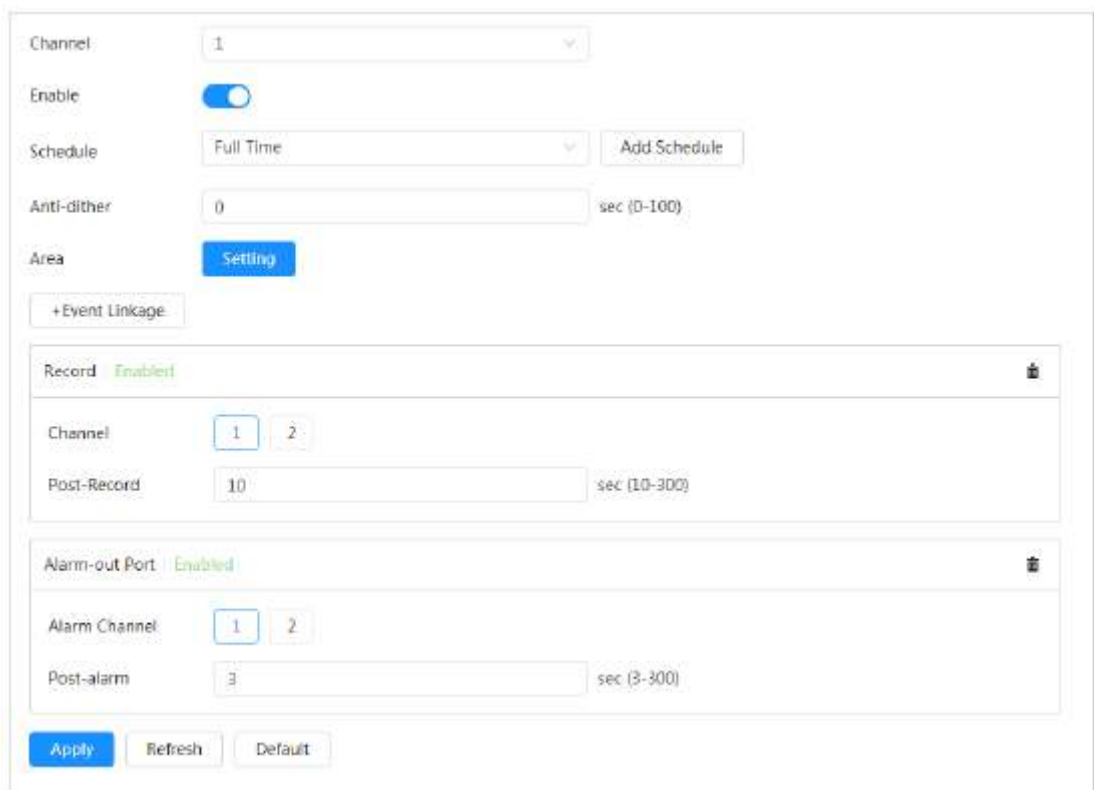
Step 1 Click  at the upper right corner of the page and select **Event Management > Video Detection > Motion Detection**.

Step 2 Select the channel.

When the channel is set to "1", you can set the parameters of visible channel.

Step 3 Click  to enable motion detection.

Figure 5-14 Motion detection



Channel: 1

Enable: ☒

Schedule: Full Time Add Schedule

Anti-dither: 0 sec (0-100)

Area: Setting

+Event Linkage

Record: Enabled

Channel: 1 2

Post-Record: 10 sec (10-300)

Alarm-out Port: Enabled

Alarm Channel: 1 2

Post-alarm: 3 sec (3-300)

Apply Refresh Default

Step 4 Set the area of motion detection.

1. Click **Setting** next to **Area**.
2. Select a color and set the region name. Select an effective area for motion detection in the image and set sensitivity and threshold.
 - The whole image is the detection area by default. Select a color to set different detection parameters for each region.
 - Sensitivity: Sensitive degree of outside changes. It is easier to trigger the alarm with higher sensitivity.
 - Threshold: Effective area threshold for Motion Detection. The smaller the threshold is, the easier the alarm is triggered.
 - The red line in the waveform indicates that the Motion Detection is triggered, and the green one indicates that there is no motion detection. Adjust sensitivity and

threshold according to the waveform.

Figure 5-15 Area



3. Click **OK**.

Step 5 Set arming periods and alarm linkage actions. For details, see "5.1.1.2 Alarm Linkage". If the added schedule doesn't meet the requirements, click "Add Schedule" to add a new Arming schedule. For details, see "5.1.1.2.1 Adding Schedule".
Anti-dither: After the Anti-dither time is set, the system only records one motion detection event in the period.

Step 6 Click **Apply**.

5.1.3.2 Configuring Video Tampering

The system performs alarm linkage when the lens is blocked or video output is mono-color screen caused by light and other reasons.

Step 1 Select "**Event Management > Video Detection > Video Tampering**".

Step 2 Click ☐ to enable the function of video tampering.

Figure 5-16 Video Tampering

Enable ☒

Schedule: Full Time

+Event Linkage

Record: Enabled

Channel:

Post-Record: sec (10-300)

Alarm-out Port: Enabled

Alarm Channel:

Post-alarm: sec (3-300)

Step 3 Select arming time and set alarm linkage actions. For details, see "5.1.1.2 Alarm Linkage". If the added schedule doesn't meet the requirements, click "Add Schedule" to add a new Arming schedule. For details, see "5.1.1.2.1 Adding Schedule".

Step 4 Click **Apply**.

5.1.3.3 Configuring Scene Changing

The system performs alarm linkage when the image switches from the current scene to another one.

Step 1 Click  at the upper right corner of the page and select **Event Management > Video Detection > Scene Changing**.

Step 2 Select **Enable** to detect scene changing.

Figure 5-17 Scene changing

- Step 3 Select arming time and set alarm linkage actions. For details, see “5.1.1.2 Alarm Linkage”. If the added schedule doesn't meet the requirements, click "Add Schedule" to add a new Arming schedule. For details, see “5.1.1.2.1 Adding Schedule”.
- Step 4 Click **Apply**.

5.1.4 Configuring Audio Detection

The system performs alarm linkage when vague voice, tone change, or sudden change of sound intensity is detected.

- Step 1 Click  at the upper right corner of the page and select Event Management > Audio Detection.
- Step 2 Set parameters of audio detection.
- Audio abnormal: click  next to **Audio Abnormal**, and the alarm is triggered when the system detects abnormal sound.
 - Intensity change: click  next to **Intensity Change**, and then set **Sensitivity** and **Threshold**. The alarm is triggered when the system detects that the sound intensity exceeds the configured threshold.
 - ◇ It is easier to trigger the alarm with higher sensitivity or smaller threshold. Set a high threshold for noisy environment.
 - ◇ The red line in the waveform indicates audio detection is triggered, and the green one indicates no audio detection. Adjust sensitivity and threshold according to the waveform.

Figure 5-18 Audio Detection

The screenshot shows the 'Audio Detection' configuration window. At the top, there are four settings: 'Audio Exception' (toggle on), 'Intensity Change' (toggle on), 'Sensitivity' (slider from - to + 50), and 'Threshold' (slider from - to + 50). Below these is a grid for scheduling. Further down, 'Anti-dither' is set to 5 seconds (range 10-100). The 'Event Linkage' section contains two sub-sections: 'Record' and 'Alarm-out Port'. Both are 'Enabled'. 'Record' has 'Channel' set to 1 and 'Post-Record' set to 10 seconds (range 10-300). 'Alarm-out Port' has 'Alarm Channel' set to 1 and 'Post-alarm' set to 3 seconds (range 3-300). At the bottom are 'Apply', 'Refresh', and 'Default' buttons.

- Step 3 Select arming time and set alarm linkage actions. For details, see "5.1.1.2 Alarm Linkage". If the added schedule doesn't meet the requirements, click "Add Schedule" to add a new Arming schedule. For details, see "5.1.1.2.1 Adding Schedule".
Anti-dither: After the Anti-dither time is set, the system only records one motion detection event in the period.
- Step 4 Click **Apply**.

5.1.5 Configuring Disarming

After configuring disarming, the system will not perform any linkage actions, but alarm information will be recorded. One-button control of all events (including regular events and linked events) with a linked switch is supported, as well as control of individual linked items.

- Step 1 Click  at the upper right corner of the page and select **Event Management > One-Button Disarming**.
- Step 2 Based on actual needs, select One-Button Arming/Disarming.
- Click  next to **One-Button Disarming** to enable this function.
After disarming, you can select the linkage between event notification and disarming as Step 4.
 - Click  next to One-Button Disarming to disable this function.
After closing it, please enable disarming by period and set the disarming period as Step 3.

Figure 5-19 One-Button Disarming

Step 3 (optional) Enable disarming by period and set the disarming period.

1. Click  next to Disarming by Period to enable this function.

2. Set disarming period. For more details, see “5.1.1.2.1 Adding Schedule”.

The green area on the timeline indicates that disarming is enabled during that time period.

3. Click **Apply**.

Step 4 (optional) enable or disable **Event Notification**.

After disabling event notification, all supporting clients, including mobile phone, platform, cloud platforms, cannot receive event messages from the Camera (except for network exception, storage exception, security warning, hardware failures) during the disarming period.



This function can only be enabled in the disarming state.

Step 5 Select disarming linkage.

The linkages that support disarming include **Alarm Output**, **Sending Email**, **Audio Linkage**, and **Warning Light**. For the selected linkages, no corresponding linked action will be generated when an alarm occurs; for the unselected linked items, corresponding linked actions will be generated when an alarm occurs.

Step 6 Click **Apply**.

5.1.6 Configuring Auto Upload

After enabling the auto upload function, the Camera will automatically report events to third-party

clients through HTTP.

Step 1 Click  at the upper right corner of the page and select **Event Management > Auto**

Upload.

Step 2 Click  to enable auto upload function.

Step 3 Click **Add**.



You can add 2 servers at most.

Step 4 Configure the server parameters.

Figure 5-20 Auto upload



Table 5-1 Server parameters

Parameters	Description
IP/Domain name	Enter the IP address of the server where the third-party client is located.
Port	Enter the port number of the server where the third-party client is located.
Path	Enter the event or image upload path.
Event Type	Select the corresponding event type.
Test	Click Test to test whether the connection works normally.

Step 5 Click **Apply**.

5.2 Smart Plan

Smart solutions include general behavior analysis, smoke and fire detection, three-dimensional behavior analysis, etc. The corresponding intelligent functions of the device will only take effect after the smart solutions are enabled.



Different devices may support different smart solutions and the specific details should be based on the actual interface.

5.2.1 Configuring IVS

Introduce the requirements for scenario selection, rule configuration operations, and global configuration operations of IVS.

Basic requirements of scenario selection are as follows:

- The target should not exceed 10% of the picture.
- The target in the picture should be no less than 10 pixels by 10 pixels, and the remnant target

should be no less than 15 pixels by 15 pixels (CIF image). The target should not exceed 1/3 of the height and width of the picture. It is suggested that the target should be about 10% of the height of the picture, and the height should not exceed 30% of the image.

- Ensure that the target appears continuously in the field of view for at least 2 seconds, with a movement distance exceeding the width of the target itself and not less than 15 pixels (CIF image).
- When conditions permit, try to reduce the complexity of the monitoring analysis scene; it is not recommended to use intelligent analysis functions in scenes with dense targets and frequent changes in lighting.
- Try to avoid areas such as glass, reflective ground, and water surfaces; try to avoid interference from branches, shadows, and insects; try to avoid backlight scenes and direct sunlight.

5.2.1.1 Configuration Flow

Figure 5-21 Configuration flow



5.2.1.2 Enabling Smart Solutions

You need to enable smart solutions of IVS before setting rules.

Step 1 At the page of WEB, select “**AI > Smart Configuration > Smart Plan**”.

Step 2 Click ☐ next to **IVS** to enable **smart plan**.

- **CAM1** is the visible channel.
- **CAM2** is the thermal channel.

Step 3 Click **Next**.

5.2.1.3 Configuring Rules

Set rule for IVS, including tripwire and intrusion.

Background Information

For the functions and applications of the rules, this section uses configuring tripwire as an example to introduce the configuration rules of IVS.

Table 5-2 Description of IVS functions

Rule	Function	Applicable Scene
Tripwire	When the target crosses tripwire from the defined motion direction, an alarm is triggered, and then the system performs configured alarm linkages.	Scenes with sparse targets and no occlusion among targets, such as the perimeter protection of unattended area.
Intrusion	When the target enters, leaves, or appears in the detection area, an alarm is triggered, and the system performs configured alarm linkages.	

Procedure

Step 1 Click the **Rule Config** tab.

Step 2 Select channel.

When the channel is set to “1”, you can set the rules of visible channel.

Step 3 Click **Add Rule** and select **Tripwire**.

The added rules are displayed in the list below. Click the text box under the name to modify the rule name. The rule is enabled by default.

Figure 5-22 Tripwire

Rule Config

Global Config

Channel

1

Add Rule

No.	Name	Type	On	Delete
1	IVS-1	Tripwire		
2	IVS-2	Intrusion		

Step 4 Click at the right part of the page to draw rule line in the image. Right-click to finish drawing.

The drawing requirements for different rules vary, please follow the drawing instruction table. After drawing, drag each corner of the detection area/detection line to adjust the range.

- Tripwire: draw a detection line.
- Intrusion: draw a detection area.



Click to delete the drawn detection line.

Figure 5-23 Draw line



Step 5 Draw models for filtering target size, etc.

- Click to draw a rectangle. The pixel counter displays the pixel size of the drawn rectangle.
- Click to delete the drawn model.

Step 6 Select **Size Filter**.

This function is only available on the thermal channels.

- Image size: draw a model for filtering targets based on this rule in the monitoring screen. Please note that the entire screen only supports one set of filtering boxes.
 1. Select **Size Filter** in **Size Filter**.

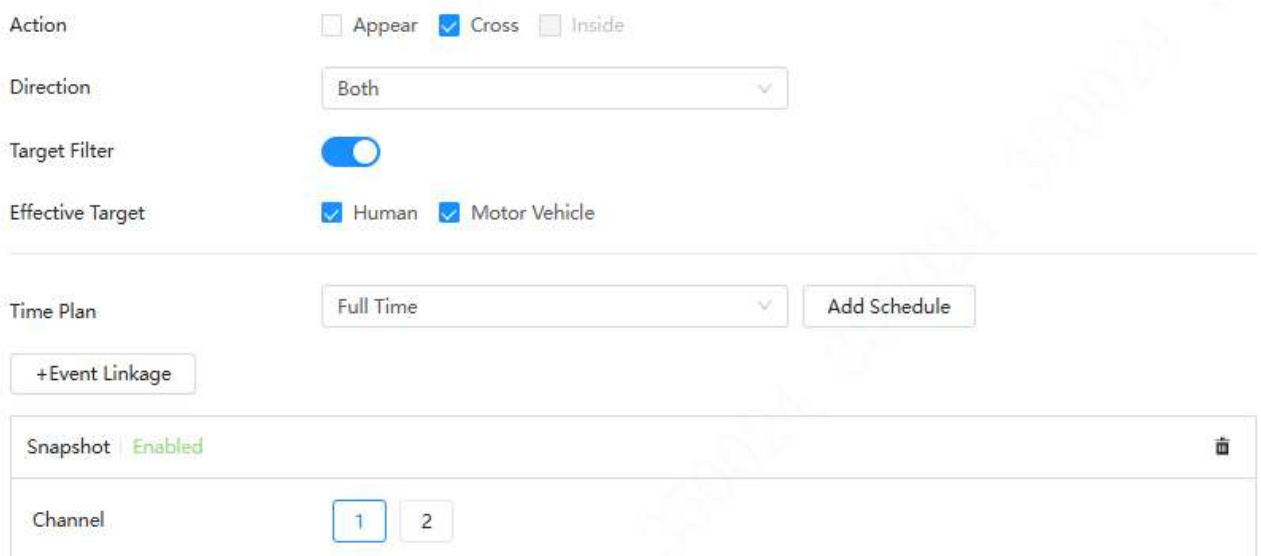
2. Click  to draw the minimum size of the target, and click  to draw the maximum size of the target. Only when the target size is between the maximum size and the minimum size, can the alarm be triggered.
- Image size normalization: you can draw two suits of filter boxes on the image from far to near. According to the size of the drawn filter box, the device scales the filter target proportionally from far to near.
 1. Select **Normalized Size Filter** in **Size Filter**.
 2. Select **Width Or Height** or **Width And Height**, click , and then press and hold the left mouse button to draw rectangle 1; click , and then press and hold the left mouse button to draw rectangle 2. The ratio of width and height of rectangle 2 is the same as that of rectangle 1 by default, and you cannot change it.
 - ◇ **Width or Height**: When the target width or height are smaller than the maximum size and larger than the minimum size, and alarm will be triggered.
 - ◇ **Width and Height**: When both of the target width and height are smaller than the maximum size and larger than the minimum size, and alarm will be triggered.



- Click  to delete all drawn detection lines.
- Click **Copy to all** to copy the configuration to other IVS rules.

Step 7 Configure rule parameters for IVS.

Figure 5-24 Description of IVS parameters



The screenshot shows the IVS rule configuration interface. It includes the following sections:

- Action**: Radio buttons for ☐ Appear, ☒ Cross, and ☐ Inside.
- Direction**: A dropdown menu set to **Both**.
- Target Filter**: A toggle switch that is currently turned on.
- Effective Target**: Checkboxes for ☒ Human and ☒ Motor Vehicle.
- Time Plan**: A dropdown menu set to **Full Time** and an **Add Schedule** button.
- +Event Linkage**: A button to add event linkage.
- Snapshot**: A status indicator showing **Enabled** with a trash icon to the right.
- Channel**: Two buttons labeled **1** and **2**.

Table 5-10 Description of IVS parameters

Parameter	Description
Direction	Set the direction of rule detection. • When setting tripwire, select A->B, B->A, or A<->B. • When setting intrusion, select Enter, Exit, or Both.
Target Filter	

Parameter	Description
Valid target	Enable Target Filter to activate this function. - When you select ppl as the alarm target, an alarm will be triggered when the system detects that person trigger the rule. - When you select Motor Vehicle as the alarm target, alarm will be triggered when the system detects that vehicle triggers the rule.
Action	When setting intrusion action, select Appear or Cross Area .

Step 8 Select the arming time and set the event linkage actions.

- If the added time does not meet the requirements, click **Add Schedule** to add a new arming schedule. For detailed information, see "5.1.1.2.1 Adding Schedule".
- Click **Event Linkage** to add linkage actions and set linkage parameters. For detailed information, see "5.1.1.2 Alarm Linkage".

Step 9 Click **Apply**.

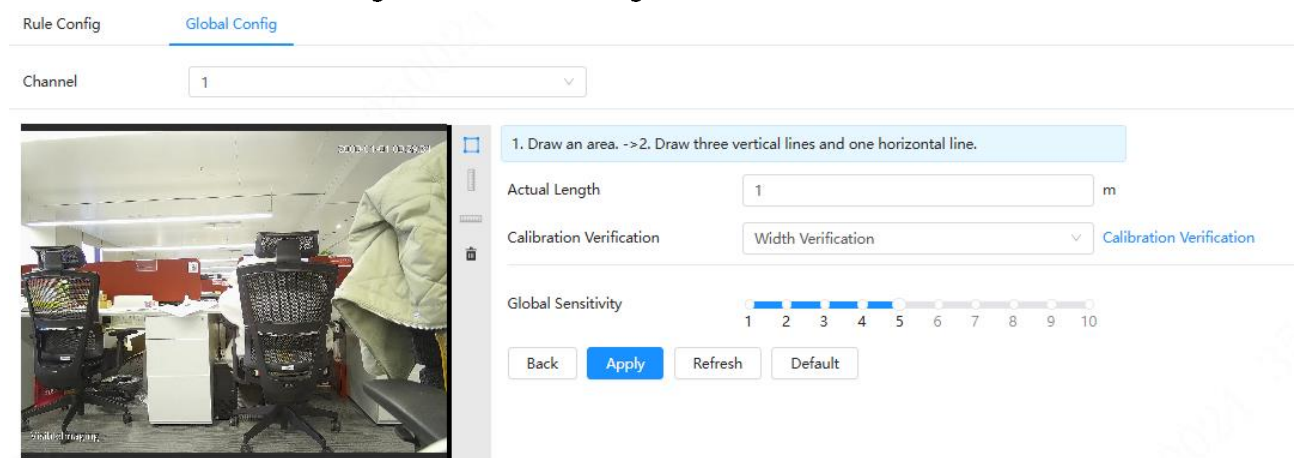
If there is a need, click  at the upper right corner of the page to check alarm information. Please subscribe related alarm events. For detailed information, see "4.5.2 Subscribing Alarm Information".

5.2.1.4 Configuring Global Setup

Configure global rules for IVS. You can draw the detection area. When an alarm is triggered in the detection area, the system will generate an alarm.

Step 1 Click the **Global Config** tab.

Figure 5-41 Global configuration



Step 2 Select the channel.

Select 1 in Channel to set the global parameters of visible channel.

Step 3 Add a detection area.

Click Add Detection Area to draw detection area in the monitoring image. Click the right mouse button to end the drawing.



Click **Add Detection Area** again to draw.

Step 4 Click **Apply**.

5.2.2 Configuring Stereo Behavior Analysis

- Step 1 At the page of WEB, select “**AI > AI Configuration > Smart Plan**”.
- Only one plan can be activated at a time, and other plans will be automatically closed after one is activated.
- Step 2 Click ☐ next to Stereo Behavior Analysis to enable this plan and click **Next** to configure parameters.
- Step 3 Click **Configuring Rules** to add and configure rules for **Smoking Detection** based on actual usage. The added rules will be displayed in the list below. Click on the rule name in the name column to modify it. Rules are enabled by default.

Figure 5-42 Stereo behavior analysis

Table 5-11 Description of smoke detection

Parameter	Description
Sensitivity	The higher the sensitivity value is set, the easier it is to trigger an alarm.
Minimum duration	The time of detecting the smoke and fire alarm.
Repeat alarm time	When an alarm is triggered and the duration of this state reaches the repeated alarm time, another alarm will be activated again.  0 represents disabling the function.

- Step 4 Click **Apply**.

5.3 Configuring Smart Thermal

Select the smart mode of the device based on actual needs, including cold and hot spot alarms, fire alarms, and temperature alarms.

5.3.1 Configuring Cold Hot Spot Alarm

After **Cold Hot Spot Alarm** is enabled, the highest temperature and spot with the lowest temperature are displayed with different colors.

- Step 1 At the main page of WEB, select “**AI > AI Config > Smart Thermal Imaging > Cold Hot Spot**”.
- Step 2 Click **Edit** in **Cold Hot Spot Alarm**.

Figure 5-43 Cold hot spot alarm

The screenshot shows a web-based configuration interface for a 'Cold hot spot alarm'. At the top, there is an 'Enable' toggle switch. Below it, the 'Temperature Unit' is set to 'Fahrenheit degree'. The 'Hot Spot Color' is set to 'rgba(0,255,0,1)' (green) and the 'Cold Spot Color' is set to 'rgba(255,255,0,1)' (yellow). The 'Alarm Condition' is set to 'single'. The 'MaxTempThreshold' is 212.0 (32~392)°F and the 'MinTempThreshold' is 32.0 (32~392)°F. The 'Anti-dither' is set to 3 (0~100)sec. The 'Schedule' is set to 'Full Time'. There is a '+Event Linkage' button. Below these are three sections: 'Record' (Enabled), 'Snapshot' (Enabled), and 'Alarm-out Port' (Enabled). Each of these sections has a 'Channel' dropdown set to '2' and a 'Post-Record' or 'Post-alarm' field set to '10' sec (10~300). At the bottom are 'Apply', 'Refresh', and 'Default' buttons.

- Step 3 Click ☐ to enable the function.
- Step 4 Select the hot spot color and cold spot color.
- Auto: The hot spot color is red, and the cold spot color is blue by default.
 - Manual: You can customize the colors for the hot spot and cold spot.
- Step 5 Click ☐ to enable OSD.
The hot spot or cold spot with temperature value will be displayed on the screen.
- Step 6 Set the alarm condition and anti-dither as needed.
When the alarm condition is met, the system alarms, and only record one alarm event during the anti-dither period.
- Step 7 Set arming periods and alarm linkage actions. For details, see "5.1.1.2.1 Adding Schedule" and "5.1.1.2 Alarm Linkage".
- Step 8 Click **Apply**.

5.3.2 Configuring Heat

Configure fire alarm. When the system determines a fire situation, it will trigger an alarm and activate the configured actions.

- Step 1 At the main page of WEB, select "**AI > AI Config > Smart Thermal Imaging > Heat**".
- Step 2 Click **Edit** to enable the function.

Figure 5-44 Configuring Heat

Step 3 Configure the parameters.

Table 5-12 Configuring Heat

Parameter	Description
Enable	Enable the heat function.
Duration	Duration of heat change. The range of values is 0 to 3600 seconds.
Repeat alarm time	When an alarm is triggered and the duration of this state reaches the repeated alarm time, another alarm will be activated again.  0 represents disabling the function.
Sensitivity	The higher the sensitivity value is set, the easier it is to trigger an alarm.
Composite judgement	If the composite judgment function is enabled, the device will detect the status of visible flame to assess the fire alarm.

Step 4 Click **Apply**.

5.3.3 Configuring Temperature Alarm

After setting the temperature alarm, when the temperature meets the alarm conditions defined by the measurement rules, the system will trigger an alarm and execute the configured actions.

5.3.3.1 Configuring Temperature Measurement Rules

Step 1 At the main page of WEB, select “**AI > AI Configuration > Smart Thermal Imaging >**

Temperature Alarm”

Step 2 Click **Edit** to enable this plan.

Step 3 Select **Configuration Rule** and click **Add Rule** to set detection rules.

1. Select drawing tools, including points, lines, and polygons.
Click names to edit them and click  to disable the corresponding rules which are enabled by default.
2. Drawing rules.
 - When the drawing tool is selected as 'point', click on the target position on the monitoring screen to draw the rule.
 - When the drawing tool is selected as 'line', you can press and hold the left mouse button to draw the rule on the monitoring screen.
 - When the drawing tool is selected as 'polygon', you can press and hold the left mouse button to draw the rule on the monitoring screen, and click the right mouse button to finish drawing.



- Select the drawn rule and click **Redraw Rule** to delete the rule and redraw it.
- Up to 12 rules can be drawn.

Step 4 Configure the parameters.

Figure 5-45 Configuring temperature alarm

Table 5-13 Description of temperature alarm

Parameter	Description
Alarm condition	Set the alarm conditions: Alarm result + Alarm condition + Alarm threshold temperature. • Alarm result: obtaining the temperature that triggers the alarm ◇ When the Measurement Item is selected as Spot, it includes average temperature and temperature slope. ◇ When the Measurement Item is selected as Line or Polygon, it includes maximum temperature, minimum temperature, average temperature, temperature slope, and temperature difference.  ◇ Temperature difference refers to the temperature difference between the maximum and minimum temperatures in the current temperature measurement rules. ◇ Temperature slope refers to the average rate of temperature change in the current temperature measurement rules. • Alarm condition: including below, equal and above. • Alarm Threshold Temperature: the temperature that triggers the alarm. The value range is -40°C to +550°C. When the Alarm Result is set to Maximum Temperature, Minimum Temperature, Average Temperature, or Temperature Difference, this parameter can be set.

Parameter	Description
Temperature error	To prevent temperature fluctuations from affecting the alarm result, an error temperature range is set. As long as the change in the alarm threshold temperature or the temperature gradient falls within this error range, it will be treated as meeting the alarm threshold temperature or temperature gradient conditions. The value range is -10°C to +10°C.
Temperature duration	Duration of temperature or temperature change. The range of values is 0 to 1000 seconds.
Warning threshold temperature	Set a temperature value for warning alarm.
Warning temperature duration	Set a temperature duration for warning alarm. Ranges from 0 to 1000 s.

Step 5 Click **Apply**.

After configuration, you can view the temperature change under the configured rules on the live image.

5.3.3.2 Configuring Global Configuration

You can enable temperature measurement.

Procedure

Step 1 Select **Temperature Measurement > Global Config**.

Step 2 Set the parameters.

Figure5-46 Global configuration

Smart Thermal > Temperature alarm

Rule Config Global Config

Enable ☒

Temperature Unit ☒ centigrade ☐ Fahrenheit degree

Temperature calibr... 1.0 m (0-9)

Schedule Full Time Add Schedule

+Event Linkage

Record Enabled

Channel 1 2

Post-Record 10 sec (10-300)

Snapshot Enabled

Channel 1 2

Apply Refresh Default

Step 5 Click **Apply**.

5.3.4 Verification

After the settings are completed, enable **Temperature Alarm**, **Temperature Difference Alarm**, and

Play Alarm Sound on the alarm tab. When an alarm event is triggered, the system will prompt and record the alarm information based on the actual situation and play the set sound, indicating that the configuration is successful.



Different devices may have different functionalities. Please refer to the actual interface for confirmation.

- Step 1 Click  at the upper right corner of the page.
- Step 2 Click  next to **Enable Alarm** to enable this function.
- Step 3 Click **Subscribe Alarm** and select **Fire Alarm**, **Cold Hot Spot Alarm** and **Temperature Error Alarm**.

Figure 5-47 Subscribe alarm

- Step 4 (Optional) Click  next to **Play Alarm Tone** and select the path of local audio documents.
When a subscribed alarm is triggered, the system plays the selected sound file to notify that an alarm event has been triggered.
 - When a subscribed alarm is triggered and the system is not in the alarm page, there will be number on  like . And the alarm information will be recorded automatically. Click the icon and click **Clear** in the **Alarm** page to clear the number.
 - When a subscribed alarm event is triggered and the system is in the **Alarm** page, the corresponding alarm information is displayed in the alarm list at the bottom of the page.
- Step 5 (Optional) Click  next to **One-Button Disarming** to enable this function.
After enabling one-button disarming, there is no linkage among alarm events and the alarm record will be saved.

6 Record

6.1 Playback

Introduce playback and video file management, support video editing and downloading

6.1.1 Playing Back Video

Check and play back video files stored in the device's SD card

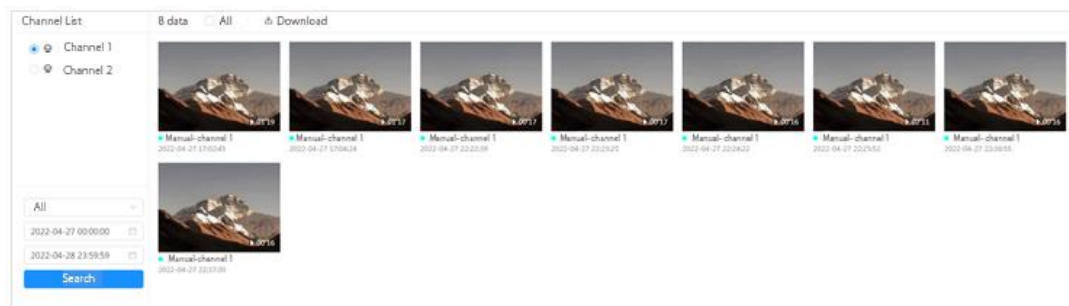
Prerequisite

Before playing back video, make sure SD card is inserted into the device and configure record plan, record control and record storage method. For details, see "6.2 Setting Record Control", "6.3 Setting Record Plan", and "6.4 Setting Storage".

Procedure

- Step 1 At the main page of WEB, select "**Record > Search Video**".
- Step 2 Select the channel, the record type, and record time, and then click **Search**.
 - Click **All**, and select the record type from the drop-down list, you can select from **All**, **General**, **Event**, **Alarm**, and **Manual**.
 - The dates with blue dots indicate there are videos recorded on those days.

Figure 6-1 Search video



- Step 3 Click  to play the video.
The system navigates to the video playback interface.

Figure 6-2 Video playback

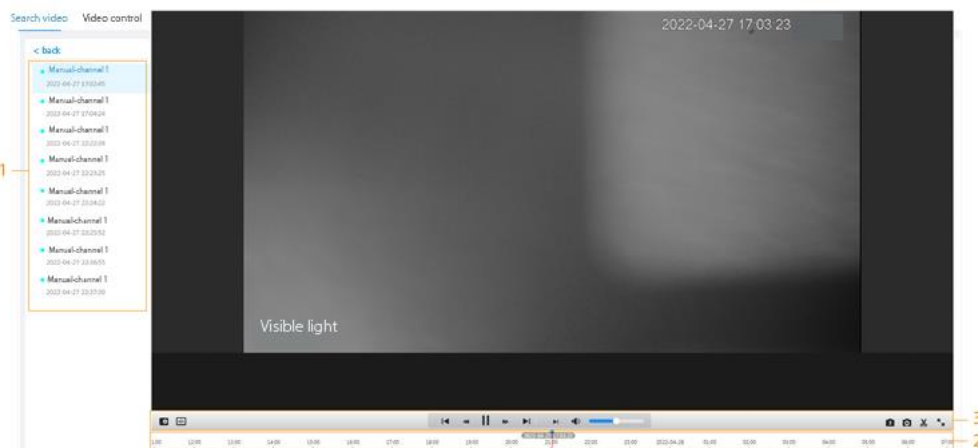


Table 6-1 Description of playback settings

No	Icon	Function	Description
1		Recorded video list	Displays all searched recorded video files. Click any files to play back it. Click Back at the upper-left corner to go to the Search Video page.
2		Zoom in	You can zoom in video image of the selected area. Drag the view to see other areas while zoomed in. The following 2 operations are supported. 1: Click the icon, and then select an area in the video image to zoom in; right-click on the image to resume the original size. 2: Click the icon, and then scroll the mouse wheel in the video image to zoom in or out.
		Smart rules	Click the icon to enable Smart Rules, preview page and detection box. Smart rules are disabled by default.  Smart rules are valid only when you enabled the rules during recording.
		Play control bar	: Click the icon to play back the previous recorded video in the recorded video list. : Click the icon to slow down the playback. : Click the icon to stop playing back recorded videos. The icon changes to , click the icon to play back recorded videos. : Click the icon to speed up the playback. : Click the icon to play back the next recorded video in the recorded video list. : Click the icon to play the next frame.
		Sound control	 : The current sound is in playback mode, and the volume can be adjusted. Click the icon to switch to mute. When the icon changes to  , click the icon to unmute.
		Triple snapshots	Click the icon to capture three images of the current preview screen at a rate of one image per second, and save them to the designated storage path. For details of checking or configuring the storage path, please see "8.1 Setting Local Parameters".
		Snapshot	Click the icon to capture one picture of the current image and it will be saved to the configured storage path. For details of checking or configuring the storage path, please see "8.1 Setting Local Parameters".
		Video clip	Clip a certain recorded video and save it. For details, see "6.1.2 Clipping Video".
		Full Screen	Click the icon and the image is displayed in full-screen mode; double-click the image or press Esc button to exit full-screen mode.

No	Icon	Function	Description
3		Progress bar	Displays the record type and the corresponding period. - Click any point in the colored area, and the system will play back the recorded video from the selected moment. - Each record type has its own color, and you can see their relations in Record Type bar.

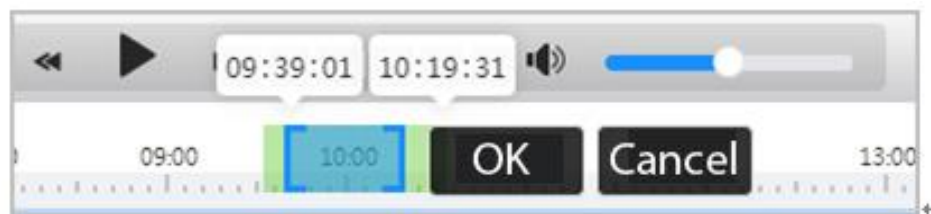
6.1.2 Clipping Video

During video playback, you can clip a segment of the video.

Step 1 During video playback, click  in the bottom of the video.

Step 2 On the progress bar, drag the positions of the start and end clip markers to set the start and end times for the video clip.

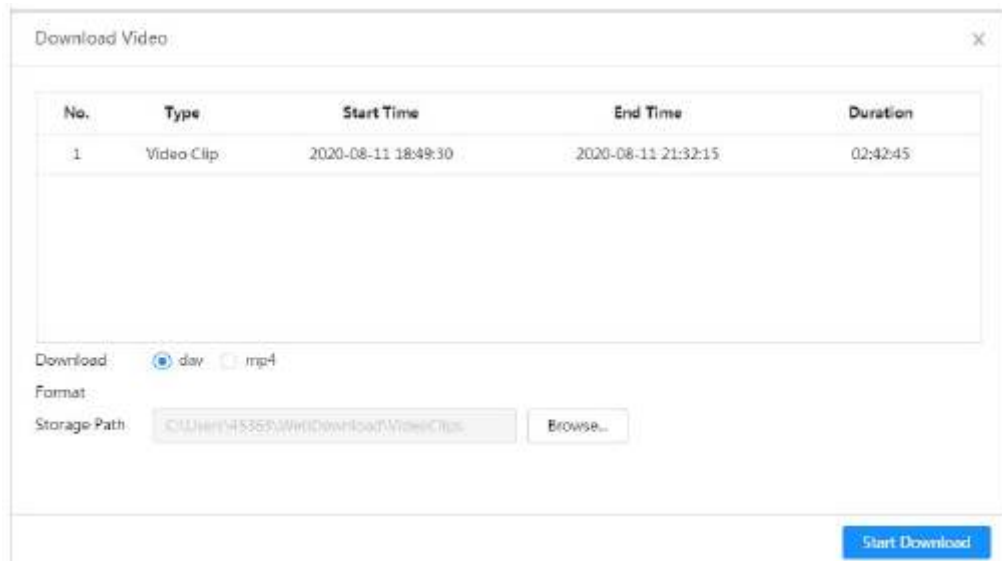
Figure 6-3 Clipping Video



Step 3 Click **OK** to download the video.

Step 4 Select download format and storage path.

Figure 6-4 Download video



Step 5 Click **Start Download**.

Start downloading the edited video and display the download progress. Then, the edited file will be saved to the specified storage path. For details of checking or configuring the storage path, please see "8.1 Setting Local Parameters".

6.1.3 Downloading Video

Download videos to a defined path. You can download a single video, or download them in batches.

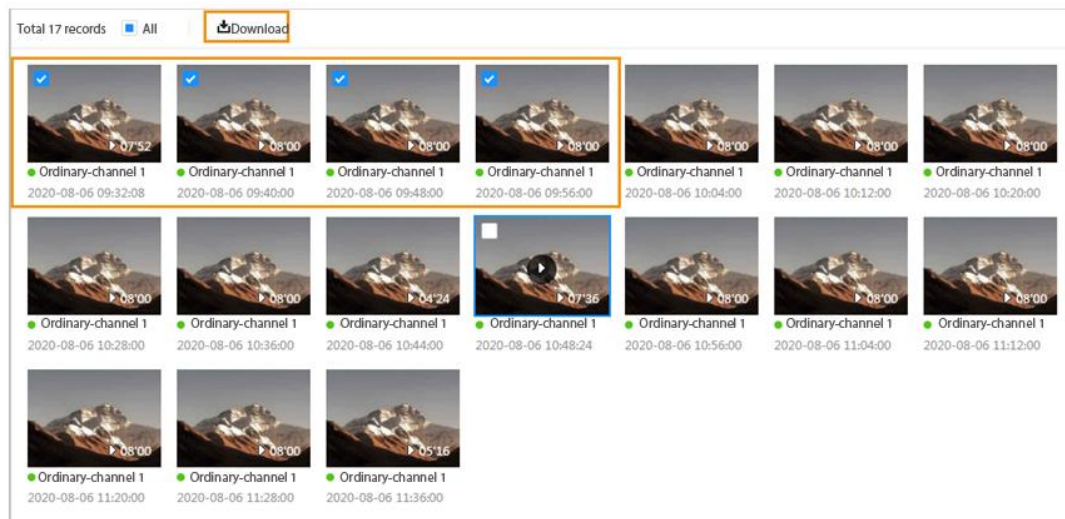
Background information

- Operations might vary with different browsers. Please refer to the actual conditions.
- For details of checking or configuring the storage path, please see "8.1 Setting Local Parameters".

Procedure

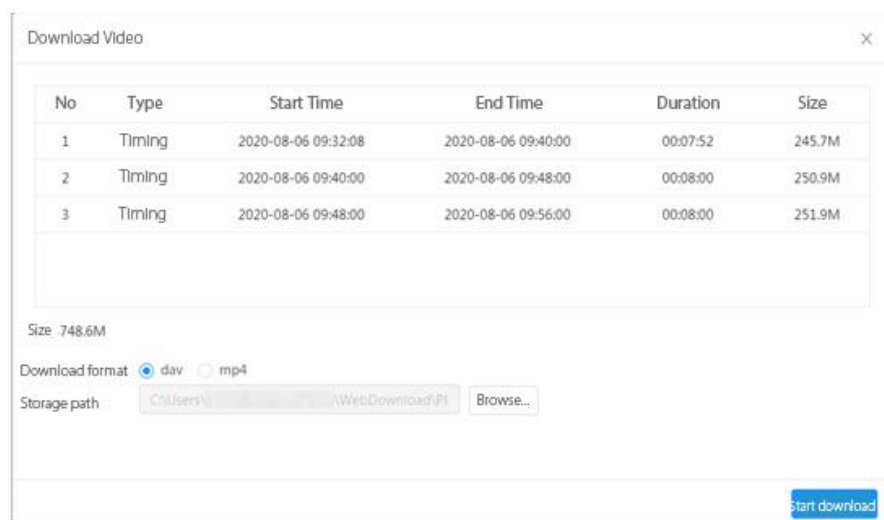
- Step 1 At the page of WEB, select **Record** > **Search Video**.
- Step 2 Select the channel, the record type, and record time, and then click **Search**.
- Step 3 Click ☐ at the upper left corner of the video file to select one or multiple videos. Click **Download**.
- The icon at the upper left corner of the selected document changes to .
 - Click **All** to select all videos.

Figure 6-5 Select video file



- Step 4 Select download format and storage path.

Figure 6-6 Download record



- Step 5 Click **Start Download**.
- Start downloading the video and display the download progress. After a successful download, the video file will be saved to the specified storage path.

6.2 Setting Record Control

Set parameters such as pack duration, pre-event record, disk full, record mode, and record stream.



When a Smart SD Card is inserted into a device that supports the Smart SD Card feature, please ensure that the SD card has been authenticated before you use the recording function.

Step 1 At the page of WEB, select **Record > Record Control**.

Step 2 Set the parameters of record control.

Figure 6-7 Record control

Record duration	30	min (1-120)
Channel	1	
Pre-record	5	sec (0-5)
Record Mode	☒ Auto ☐ Manual ☐ Off	
Record Stream	Main Stream	
Apply Refresh Default		

Table 6-2 Description of record control parameters

Parameter	Description
Record duration	The time for packing each video file.
Pre-record	The time to record the video in advance of a triggered alarm event. For example, if the pre-event record is set to be 5 s, the system saves the recorded video 5 s before the alarm is triggered.  When an alarm or motion detection links recording, and the recording is not enabled, the system saves the video data within the pre-event record time to the video file.
Record Mode	• When you select Manual, the system starts recording. • When you select Auto, the system starts recording in the configured time period of record plan. • When select Off, the system stop recording.
Record Stream	Select record stream, including Main Stream and Sub Stream .

Step 3 Click **Apply**.

6.3 Setting Record Plan

Set daily and holiday recording schedules. Only after enabling ordinary, event, and alarm recording schedules for the recording channel will the channel support alarm linkage recording.

Background information

You can set specific dates as holidays. When the recording for the holiday schedule is activated, the

recording will be done according to the holiday recording plan. If the holiday settings and daily settings are inconsistent, the holiday settings will take precedence over the daily settings. For example, when the holiday setting is enabled, if today is a holiday, recording will follow the holiday settings; otherwise, it will follow the daily settings.

Procedure

Step 1 At the page of WEB, select **Record > Time Plan**.

Step 2 Select recording channel.

Step 3 Set time planning time of daily recording.

Green represents normal record plan (such as timing recording); yellow represents motion record plan (such as recording triggered by intelligent events); red represents alarm record plan (such as recording triggered by alarm-in).

1. Drag the left mouse button on the timeline to select the recording time segments of each event.

The recording schedule is arranged from top to bottom as follows: **Normal Recording**, **Time-Based Recording**, and **Alarm Recording**.

Figure 6-8 Timeline



2. Click on the selected time segment and enter the specific time value in the start time textbox to set the exact start time.

Figure 6-9 Set accurate start time



3. (Optional) Click **Copy**, choose date and click **Apply**.

You can copy the current time plan to the selected days quickly.

Step 4 Click **Holiday** and set record plan.

1. Click ☐ next to **Enable**.
2. Select the days that you need to set as holiday.
 - The selected date is displayed with a blue background.
 - Click **Clear** to cancel the selection and reset date.
3. Click **OK**.

Step 5 Click **Apply**.

6.4 Setting Storage

Set the recording event types for the device corresponding to the hard drive full recording strategy and recording storage method.

Step 1 At the page of WEB, select **Record > Storage**.

Step 2 Select the recording strategy and storage method that you need for different types of recorded videos.

Figure 6-10 Recording storage

Event Type ☒ Scheduled ☒ Motion ☒ Alarm

Disk Full ☒ Overwrite ☐ Stop

Storage Method Local Storage

Apply Refresh Default

Table 6-3 Description of storage parameters

Parameter	Description
Event Type	Including General , Event and Alarm .
Disk Full	Recording strategy when the disk is full. • Stop: Stop recording when the disk is full. • Overwrite: Cyclically overwrite the earliest video when the disk is full.
Storage Method	• Local storage: Save the recorded videos in the internal SD card. • Network storage: Save the recorded videos in the FTP server or NAS.

Step 3 Configure network storage parameters. Do this step when selecting **Network Storage** in **Storage Method**.

- FTP

Figure 6-11 FTP

The screenshot shows a web-based configuration page for FTP. On the left is a sidebar with various settings. The main area contains input fields and controls for each setting. The 'Event Type' section has three checked checkboxes: General, Event, and Alarm. 'Disk Full' has 'Overwrite' selected. 'Storage Method' is set to 'Network Storage'. The 'FTP' section is expanded, showing 'Mode' set to 'SFTP (recommended)'. The 'Enable' toggle is turned on. 'Server IP' is '0.0.0.0', 'Port' is '22', 'Username' is 'anonymity', 'Password' is masked with dots, and 'Storage Path' is 'share'. 'Emergency local storage' is turned off. At the bottom are buttons for 'Test', 'Apply', 'Refresh', and 'Default'.

Table 6-4 FTP Description of FTP parameters

Parameter	Description
Protocol type	SFTP is recommended to safeguard your network safety.
Enable	Click  next to Enable to enable FTP function.
Server IP	The IP address of the FTP server.
Port	The port number of the FTP server.
Username	The username to log in to the FTP server.
Password	The password to log in to the FTP server.
Storage Path	The destination path in the FTP server.
Emergency local storage	When the FTP server does not work, all the files are saved to the internal SD card.
Test	Click Test to test whether FTP works.

- NAS

Figure 6-12 NAS

The screenshot displays a configuration window for Network Attached Storage (NAS). The 'Event Type' section has three checked checkboxes: 'General', 'Event', and 'Alarm'. The 'Disk Full' section has two radio buttons, with 'Overwrite' selected and 'Stop' unselected. The 'Storage Method' section contains two dropdown menus; the first is set to 'Network Storage' and the second is set to 'NAS'. The 'Enable' section features a blue toggle switch that is turned on. The 'Server IP' section has a text input field containing '0.0.0.0'. The 'Storage Path' section has an empty text input field. At the bottom of the window are three buttons: 'Apply' (highlighted in blue), 'Refresh', and 'Default'.

Table 6-5 Description of NAS parameters

Parameter	Description
Enable	Click  next to Enable to enable NAS function.
Server IP	The IP address of NAS server.
Storage path	The destination path in the NAS server.

Step 4 Click **Apply**.

7 Picture

7.1 Playback

This section introduces playback and downloading pictures.

7.1.1 Playing Back Picture

Query and replay the capture files stored on the device's SD card.

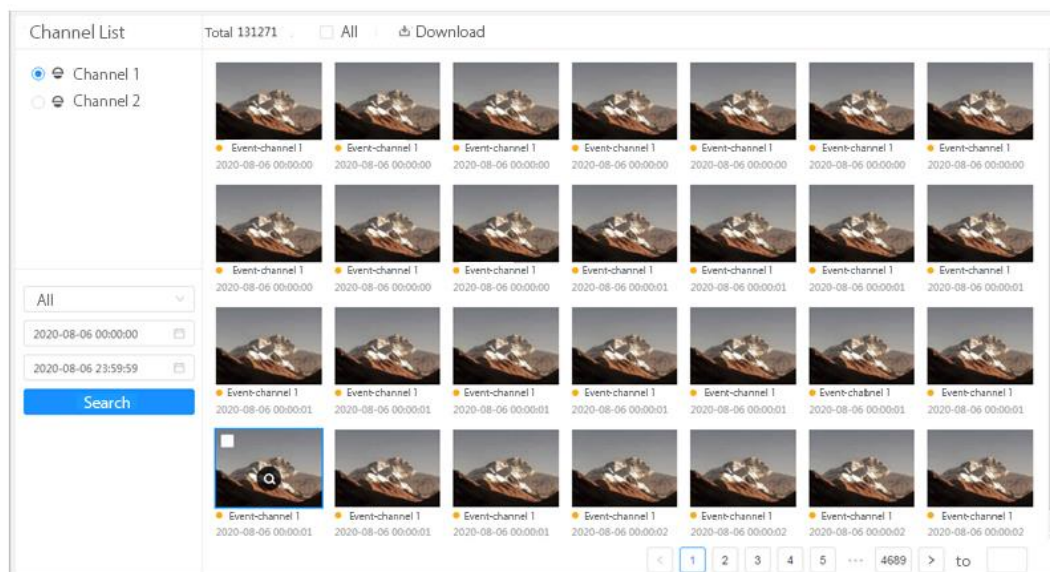
Prerequisite

Before playing back picture, make sure SD card has been inserted into the device and configure snapshot time range, snapshot plan and storage method. For details, see "7.2 Configure Snapshot Parameters, 7.3 Setting Snapshot Plan, 7.4 Configuring Snapshot Storage".

Prerequisite

- Step 1 At the page of WEB, select **Picture > Search Picture**.
- Step 2 Select the channel, the snapshot type, and snapshot time, and then click **Search**.
 - Click **All**, and select the record type from the drop-down list, you can select from **All**, **Normal**, **Event**, and **Alarm**.
 - The dates with blue dots indicate there are snapshots on those days.

Figure 7-1 Search snapshot



- Step 3 Point to the searched picture, and then click  to play back the picture. The system jumps to the snapshot playback page.

Figure 7-2 Snapshot playback page

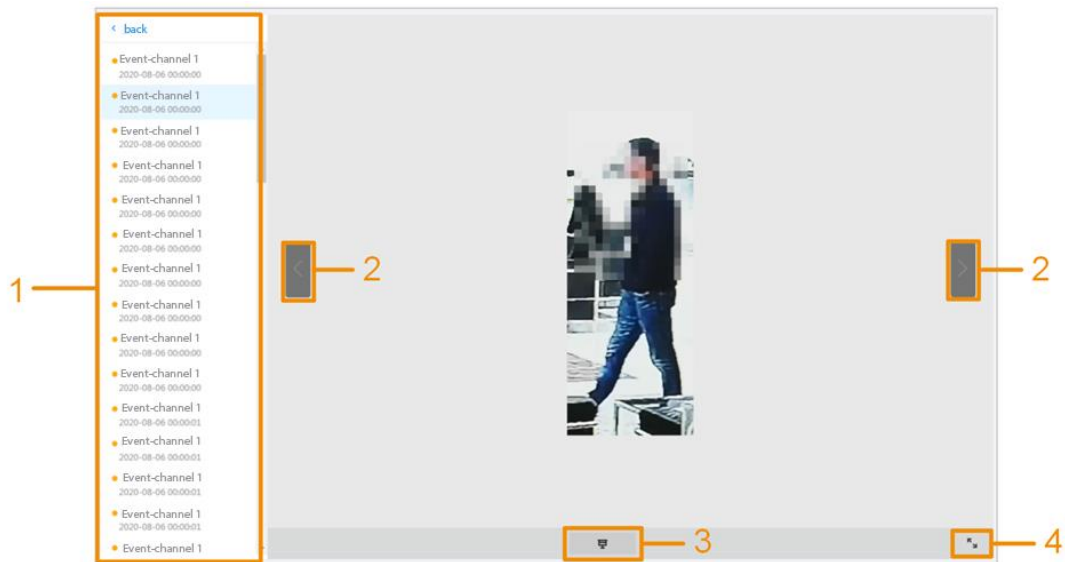


Table 7-1 Description of playback page

No	Icon	Description
1		Display all searched picture files in a list. Clicking on any file will display the picture. Click Back at the upper-left corner to go to the Search Picture page.
2		It displays the previous snapshot in the left picture list.
		It displays the next snapshot in the left picture list.
3		It shows the pictures one by one in slide show mode.
4		Click the icon and the snapshot is displayed in full-screen mode; double-click the image to exit full-screen mode.

7.1.2 Downloading Picture

Download pictures to a defined path. You can download a single picture, or download them in batches.

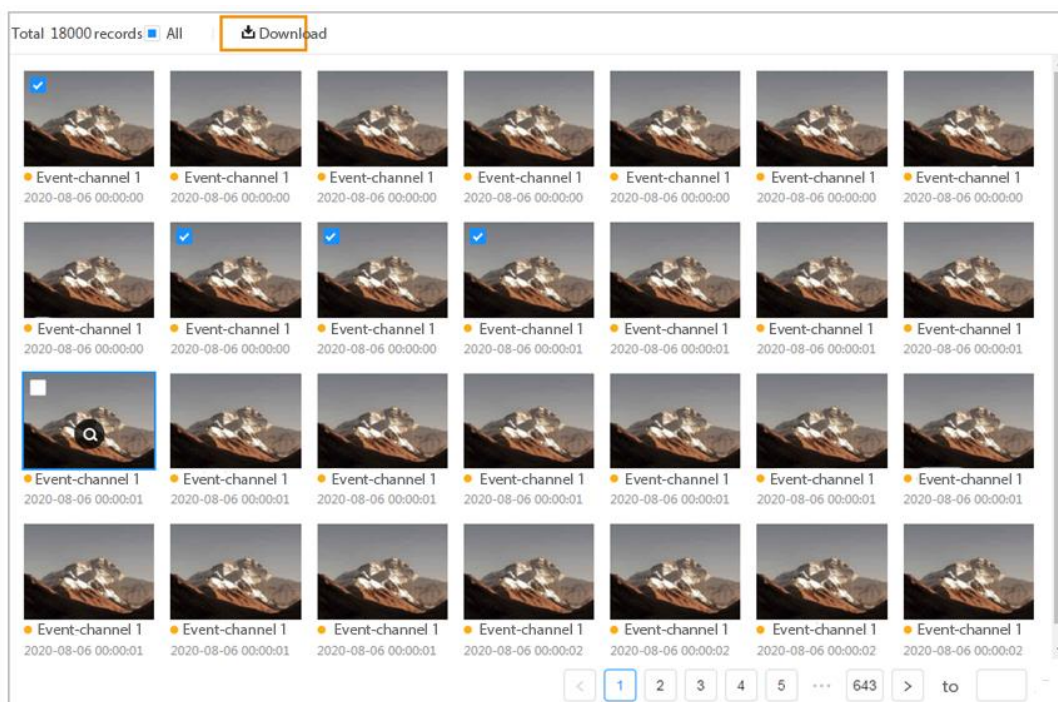
Background information

- Download operations may vary on different browsers. Please refer to actual page.
- For details of checking or setting storage path, see "8.1 Setting Local Parameters".

Prerequisites

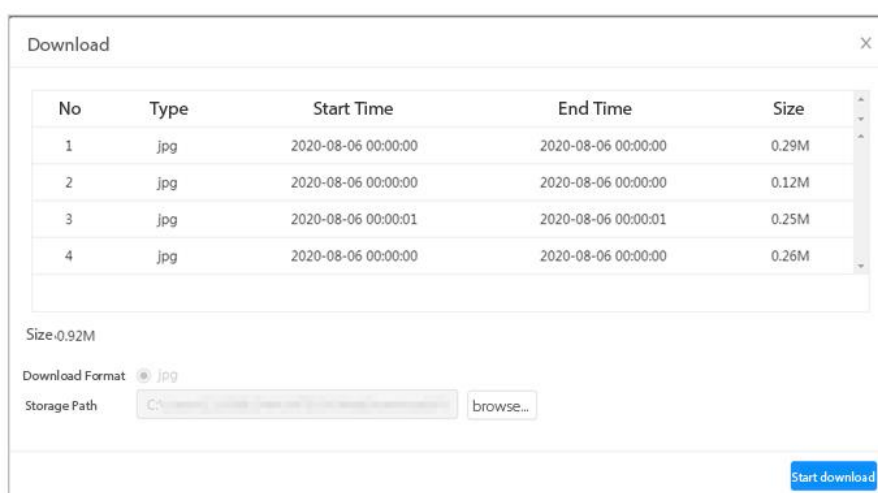
- Step 1 At the page of WEB, select **Picture > Search Picture**.
- Step 2 Select the snapshot channel, snapshot type, and snapshot time, and then click Search.
- Step 3 Click ☐ at the upper left corner of the snapshot file, select one or multiple files and click **Download**.
 - The icon of the selected files changes to ☒.
 - Click **All** to select all files.

Figure 7-3 Select picture file



Step 4 Select storage path.

Figure 7-4 Download picture



Step 5 Click **Start Download**.

It starts downloading the image file and displays the download progress. After the download is finished, the picture file will be saved to the specified storage path.

7.2 Setting Snapshot Parameters

Set the snapshot parameters, including type, size, quality and Interval.

Step 1 At the page of WEB, select **Picture > Snapshot Settings**.

Step 2 Select channel.

- When the channel is set as "1", set parameters of visible channel.
- When the channel is set as "2", set parameters of thermal imaging channel.

Step 3 Set parameters.

Figure 7-5 Set snapshot parameters

The screenshot shows a configuration window for snapshot parameters. It contains the following elements:

- Channel:** A dropdown menu with '1' selected.
- Type:** A dropdown menu with 'General' selected.
- Picture Size:** A text field displaying '2688x1520 (2688*1520)'.
- Quality:** A horizontal slider with markers from 1 to 6. The slider is currently positioned at 5.
- Snapshot Interval:** A dropdown menu with '1 picture/ 1 sec' selected.
- Buttons:** Three buttons at the bottom: 'Apply' (highlighted in blue), 'Refresh', and 'Default'.

Table 7-2 Description of snapshot parameters

Parameter	Description
Type	Including General and Event. • General: Capture images in configured period. For details, see “7.3 Configuring Snapshot Plan”. • Event: Capture images when triggering intelligent events such as video detection, audio detection, smart detection, and alarms, provided that the video detection, audio detection, and corresponding capture functions are enabled.
Picture size	Set the resolution of the captured images.
Quality	Set the quality of the snapshot. The higher the value, the better the quality.
Snapshot interval	Set the frequency of snapshot. You can select Custom to set the frequency as needed.

Step 4 Click **Apply**.

7.3 Setting Snapshot Plan

Set up a daily and holiday snapshot plan. The snapshot channel will only support alarm linkage snapshot after the general, event, and alarm snapshot plans are activated.

Background information

You can set specific dates as holidays. When the snapshot plan of holiday schedule is enabled, it will capture pictures based on the plan. When there is a conflict between the holiday settings and the daily settings, the holiday settings take precedence over daily settings. For example, when holidays are enabled, if today is a holiday, the snapshots will be captured according to the holiday settings; otherwise, they will be captured according to the daily settings.

Procedure

- Step 1 At the page of WEB, select **Picture > Time Plan**.
- Step 2 Select channel.
 - When the channel is set as “1”, set parameters of visible channel.
 - When the channel is set as “2”, set parameters of thermal imaging channel.

Step 3 Set daily snapshot plan.

Green indicates the normal snapshot plan, yellow indicates the event snapshot plan (such as snapshots triggered by smart events), and red indicates the alarm snapshot plan (such as snapshots triggered by alarm inputs)

1. Press and hold the left mouse button on the timeline to drag and select the snapshot time range for each event.

The snapshot time plan includes **Scheduled Snapshot**, **Motion Snapshot** and **Alarm Snapshot** from top to bottom respectively.

Figure 7-6 Timeline



2. Click on the selected time segment and enter the specific time value in the start time textbox to set the exact start time.

Figure 7-7 Set accurate start time



3. (Optional) Click **Copy**, choose date and click **Apply**.

You can copy the current time plan to the selected days quickly.

Step 4 Click **Holiday** and set record plan.

1. Click ☐ next to **Enable**.
2. Select the days that you need to set as holiday.
 - The selected date is displayed with a blue background.
 - Click **Clear** to cancel the selection and reset date.
3. Click **OK**.

Step 5 Click **Apply**.

7.4 Setting Snapshot Storage

Set the snapshot event type corresponding to the hard disk full snapshot strategy and snapshot storage method.

Step 1 At the page of WEB, select **Picture > Storage Settings**.

Step 2 Based on actual conditions, select snapshot strategy and storage method for different event type.

Figure 7-8 Set snapshot storage

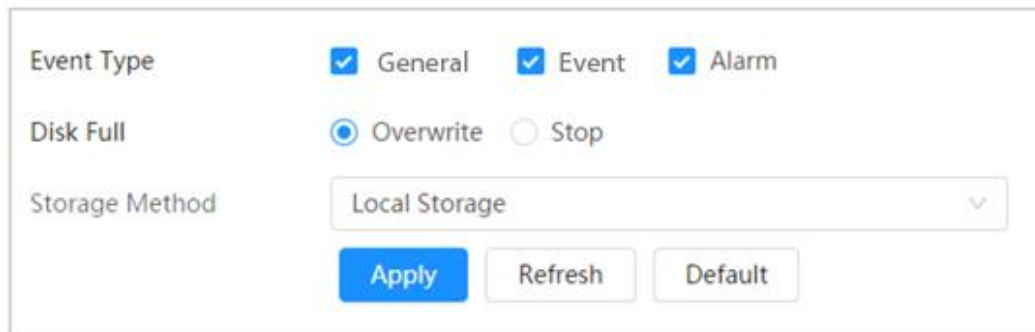


Table 7-3 Description of snapshot storage

Parameter	Description
Event type	Including General , Event and Alarm .
Disk full	The recording strategy when the disk is full. • Stop: Stop capturing when the disk is full. • Overwrite: When the working disk is full, overwrite the oldest capture files in a loop
Storage method	• Local Storage: store in the SD card of the device. • Network Storage: store in FTP or NAS.

Step 3 Configure network storage parameters. Do this step when selecting **Network Storage** in **Storage Method**.

- FTP

Figure 7-9 FTP

The screenshot shows a configuration window for FTP. On the left is a sidebar with a list of settings. The main area contains the following controls:

- Event Type:** Three checkboxes labeled 'General', 'Event', and 'Alarm', all of which are checked.
- Disk Full:** Two radio buttons, 'Overwrite' (selected) and 'Stop'.
- Storage Method:** A dropdown menu currently showing 'Network Storage'.
- FTP:** A dropdown menu currently showing 'FTP'.
- Mode:** A dropdown menu currently showing 'SFTP (recommended)'.
- Enable:** A toggle switch that is currently turned on (blue).
- Server IP:** A text input field containing '0.0.0.0'.
- Port:** A text input field containing '22', with a range '(0~65535)' indicated to the right.
- Username:** A text input field containing 'anonymity'.
- Password:** A text input field filled with dots to mask the password.
- Storage Path:** A text input field containing 'share'.
- Emergency local storage:** A toggle switch that is currently turned off (grey).
- Buttons:** At the bottom, there are three buttons: 'Test' (white), 'Apply' (blue), 'Refresh' (white), and 'Default' (white).

Table 7-4 Description of FTP parameters

Parameter	Description
Protocol type	SFTP is recommended to safeguard your network safety.
Enable	Click  next to Enable to enable FTP function.
Server IP	The IP address of the FTP server.
Port	The port number of the FTP server.
Username	The username to log in to the FTP server.
Password	The password to log in to the FTP server.
Storage Path	The destination path in the FTP server.
Emergency local storage	When the FTP server does not work, all the files are saved to the internal SD card.
Test	Click Test to test whether FTP works.

- NAS

Figure 7-10 NAS

The screenshot shows a configuration window for NAS. On the left is a sidebar with a 'Storage' section. The main area contains the following settings:

- Event Type:** Three checkboxes labeled 'General', 'Event', and 'Alarm', all of which are checked.
- Disk Full:** Two radio buttons, 'Overwrite' (selected) and 'Stop'.
- Storage Method:** Two dropdown menus. The first is set to 'Network Storage' and the second is set to 'NAS'.
- Enable:** A blue toggle switch that is turned on.
- Server IP:** A text input field containing '0.0.0.0'.
- Storage Path:** An empty text input field.
- Buttons:** At the bottom are three buttons: 'Apply' (highlighted in blue), 'Refresh', and 'Default'.

Table 7-5 Description of NAS parameters

Parameter	Description
Enable	Click  next to Enable to enable NAS function.
Server IP	The IP address of NAS server.
Storage path	The destination path in the NAS server.

Step 4 Click **Apply**.

7.5 Setting Auto Upload

Enable the auto upload, so that when an event occurs, the device can proactively report images to a third-party client via HTTP.

Step 1 Click  at the upper right corner of the page and select **Picture > Auto Upload**.

Step 2 Click  next to Enable to enable upload function.

Step 3 Click **Add**.



At most 2 servers can be added.

Step 4 Set server parameters.

Figure 7-11 Auto upload

Upload Mode
HTTP

Enable
☒

Add
Delete

☐	No.	IP/Domain Name	Port	Path	Event Type	Test	Delete
☐	1	Example: 172.168.1.108	Example: 80	Example: /example/	None	Test	

Apply
Refresh
Default

Table 7-6 Server parameters

Parameters	Description
IP/Domain name	Enter the IP address of the server where the third-party client is located.
Port	Enter the port number of the server where the third-party client is located.
Path	Enter the event or image upload path.
Event Type	Select the corresponding event type.
Test	Click Test to test whether the connection works normally.

Step 5 Click **Apply**.

8 Settings

8.1 Setting Local Parameters

The local parameters include playback parameters, recording storage path, and snapshot storage path.

Step 1 At the upper right corner of the page, click  and select **Local**.

Step 2 Set play parameters.

Streaming media protocols: including types of network transmission protocols, TCP (Transmission Control Protocol), UDP (User Datagram Protocol) ports, and multicast.



Before selecting **Multicast**, it is necessary to set the multicast parameters. For detailed information, please see "8.3.9 Set Multicast."

Step 3 Click Browse and set the storage path of recording and snapshots.

Figure 8-1 Set local parameters

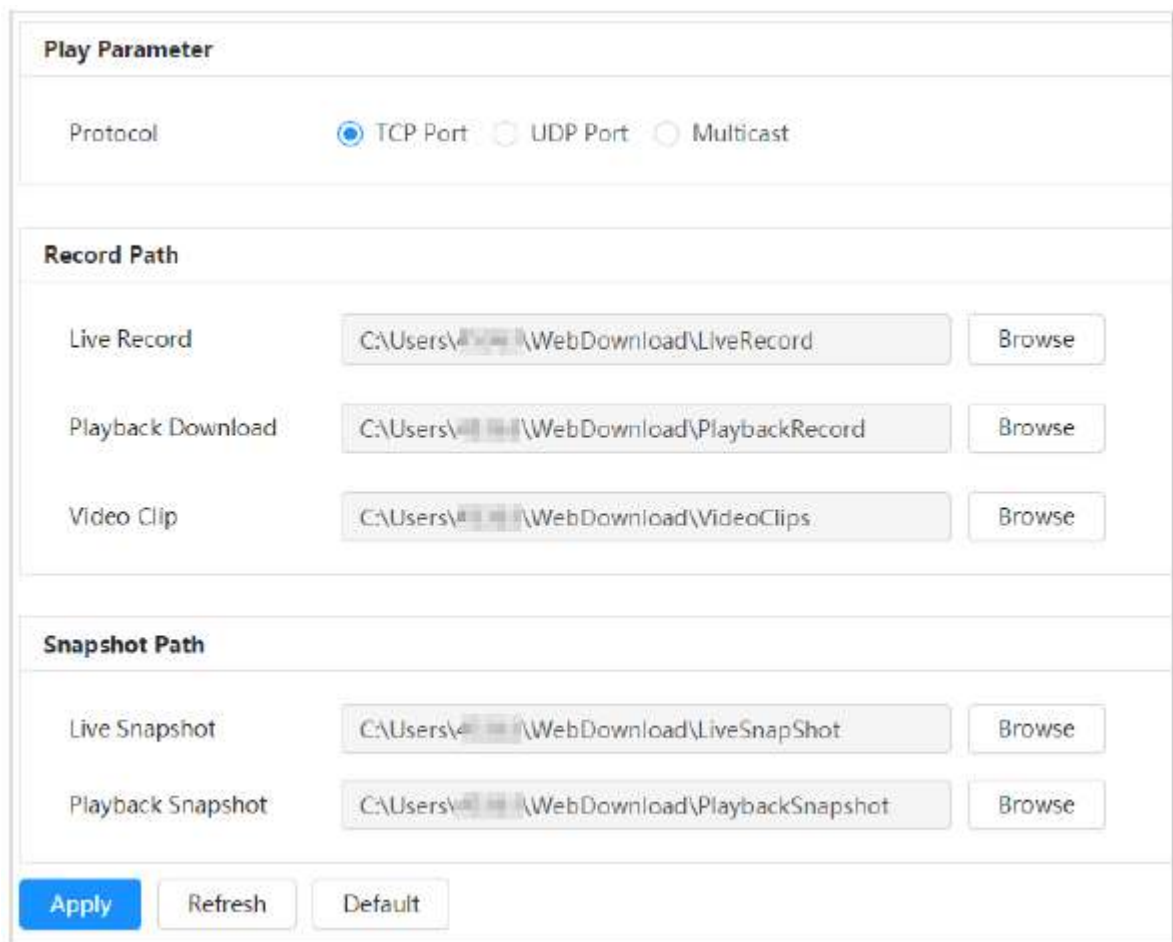


Table 8-1 Description of local parameters

Parameter type	Parameter	Description	
Record path	Preview Recording	It refers to the recording of the preview page. The default path is "C:\Users\admin\WebDownload\LiveRecord"	"Admin" in the path refers to the

Parameter type	Parameter	Description	
	Playback download	Download recording at the page of recording playback page. The default path is "C:\Users\admin\WebDownload\PlaybackRecord".	logged-in PC account.
	Video clip	Video clip at the recording playback page. The default path is "C:\Users\admin\WebDownload\VideoClips".	
Snapshot path	Preview snapshot	Snapshot at the preview page. The default path is "C:\Users\admin\WebDownload\LiveSnapshot".	
	Playback snapshot	Snapshot at the playback page. The default path is "C:\Users\admin\WebDownload\PlaybackSnapshot".	
	Heatmap	Heatmap during collection. The default path is C:\Users\admin\WebDownload\HeatMap.	

Step 4 Click **Apply**.

Click **Refresh** to refresh the parameters of the current page; Click **Default** to restore the default parameters.

8.2 Setting Camera Attributes

This section introduces the camera setting, including camera parameters, video parameters, and audio parameters.

You can go to the Camera page through two ways. The subsequent content will take  button at the upper right corner as an example.

- At the page of WEB, click **Camera Settings**.
- At the upper right corner of the page, click  and select Camera Settings.

8.2.1 Setting Image Attributes

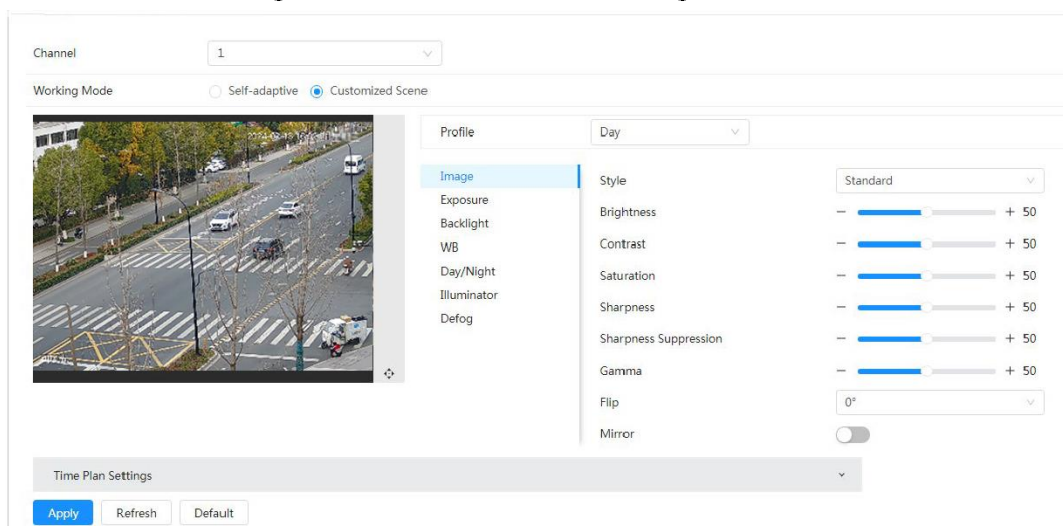
Set parameters for visible light and thermal imaging cameras, and manage camera configuration files.

8.2.1.1 Configuring Visible Channel

Set the visible light image properties of the camera and adjust the image parameters to achieve optimal preview results.

At the upper right corner of the page, click  **Camera Settings > Image > Image Attributes**. When the channel is selected as "1", you can select working mode (self-adaptive or customized scene) and profile(day, night, or general). The system displays the configuration page of visible channel.

Figure 8-2 Camera attribute(visible light)



8.2.1.1.1 Setting Working Mode

Select the working mode of the device based on actual needs, including **Self-adaptive** and **Customized Scene**.

Step 1 At the upper right corner of the page, click  and select **Camera Settings > Image > Image Attributes**.

Step 2 Select the working mode.

- Self-adaptive: The camera automatically matches the appropriate profile for monitoring based on different environments.
If you select **Self-adaptive**, skip to [Step5](#).
- Customized scene: the camera monitors according to the configured profile types at different times.
If you select **Customized Scene**, do [Step3](#).

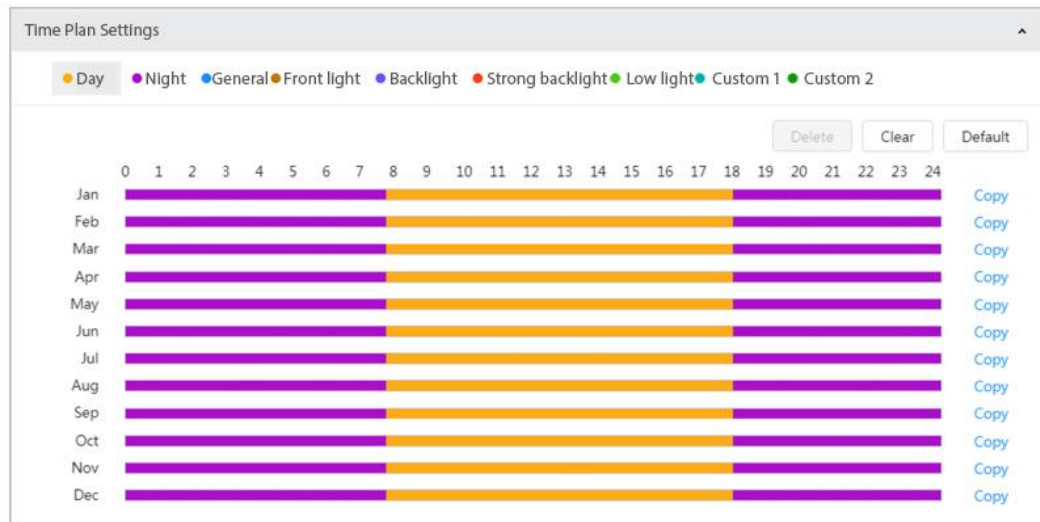
Step 3 Select the file.

You can select the file from **General**, **Day**, and **Night**. After selecting the file type, you can set and view the configuration parameters and corresponding effects.

Step 4 Set time plan.

You can configure the time plan for each day of a month.

Figure 8-3 Setting time plan.



1. Click **Time Plan Settings** or  to unfold time plan image.
2. Click the file type, such as **General**, and the drag the mouse on the time bar to set the period to use general file.
For Day and night, the operations are the same.



General file is set by default, click **Delete** or **Clear**, and then set the time plan as needed.

3. (Optional) Click **Copy**, select months, and then click **Apply**.
The configured time plan can be copied to other selected months.

Step 5 Click **Apply**.

8.2.1.1.2 Adjusting Image

You can adjust the image parameters according to the actual conditions.

Step 1 At the upper right corner of the page, click  and select **Camera Settings > Image > Image Attributes**.

Step 2 Set parameters.

Figure 8-4 Image

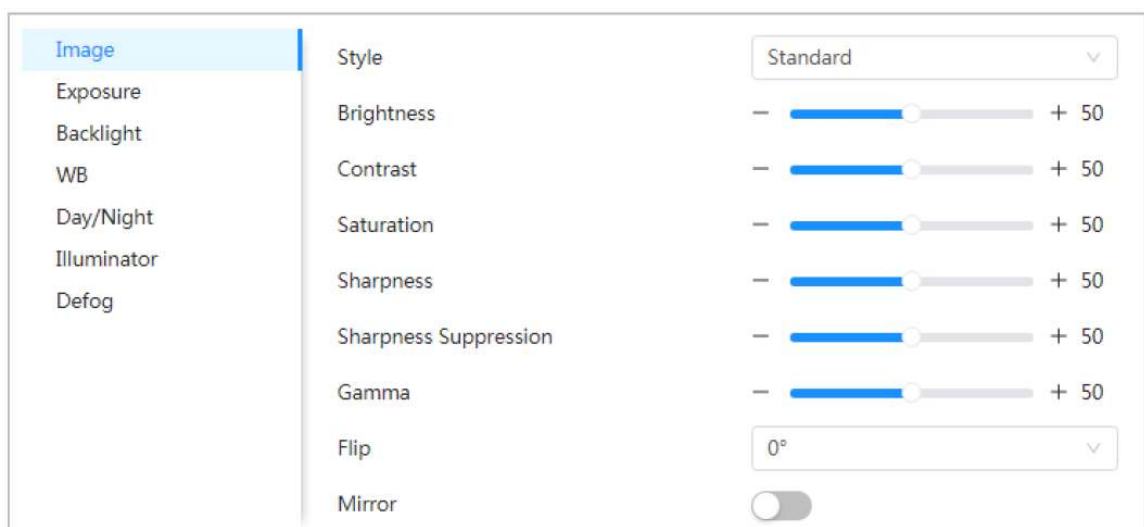


Table 8-2 Description of image parameters

Parameter	Description
Style	Set the style of the image, including soft, standard and vivid. • Soft: the colors in the image are weaker than in the real scene, and the contrast between light and dark is low. • Standard: default image style, displays the actual color of the image. • Vivid: the image is more vivid than the actual one.
Brightness	The overall brightness of the image colors. The higher the value, the brighter the image; conversely, the lower the value, the darker the image. When the value is too high, the image tends to become washed out.
Contrast	The ratio of black to white in the image. The higher the value, the richer and more vibrant the colors in the image; conversely, the lower the value, the less vivid the colors. When the value is too high, the dark areas of the image become too dark, and the bright areas may be prone to overexposure. When the value is too low, the image tends to appear gray.
Saturation	Makes the color deeper or lighter. The higher the value is, the deeper the color will be, and the lower the lighter. Saturation value does not change the overall brightness.
Sharpness	Changes the sharpness of image edges. The higher the value is, the clearer the image edges will be, and if the value is set too big, image noises are more likely to appear.
Color Suppression	The degree of color suppression in an image. The higher the value, the more pronounced the suppression; conversely, the lower the value, the less suppression is observed.
Gamma	Adjust the brightness and contrast of the image through a non-linear adjustment. The larger the value, the brighter the image; conversely, the smaller the value, the darker the image.
Flip	Changes the display direction of the picture, see the options below. • 0°: Normal display. • Corridor Mode 1: The picture rotates 90° clockwise. • Corridor Mode 2: The picture rotates 90° counterclockwise. • Mirror: display the image upside down.  When using corridor mode on certain devices, the video resolution requirements vary for devices with different resolutions. For details of video resolution, see "8.2.3.1 Setting Code". • For devices with a resolution below 4 million (2688×1520), the resolution supported in corridor mode should be consistent with the maximum resolution of the main stream. • For devices with a resolution of 4 million and above, the maximum resolution supported in corridor mode is 4 million.
Mirror	After Mirror is enabled, the image will display with left and right side reversed.

Step 3 Click **Apply**.

8.2.1.1.3 Setting Exposure

By adjusting the lens aperture, shutter, and other settings, the image can be made clearer.



The devices that support true wide dynamic range functionality do not support long exposure when the wide dynamic range is enabled in **Backlight** mode.

Step 1 At the upper right corner of the page, click  and select **Camera Settings > Image > Image Attributes > Exposure**.

Step 2 Set parameters.

Figure 8-5 Exposure

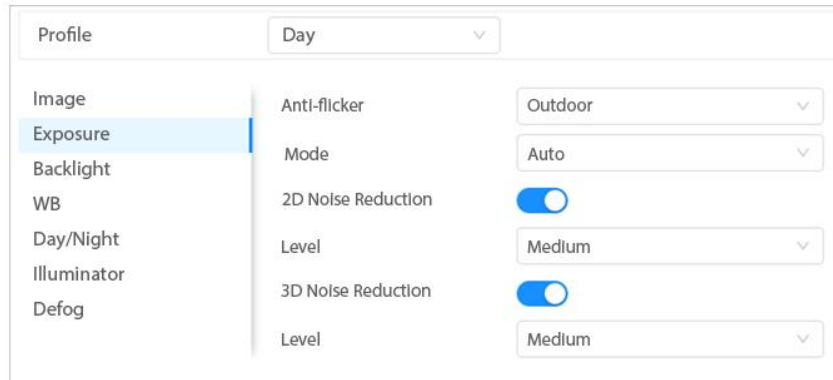


Table 8-3 Description of exposure parameters

Parameter	Description
Anti-flicker	You can select from 50 Hz, 60 Hz and Outdoor. • 50 Hz: When the electric supply is 50 Hz, the system adjusts the exposure according to ambient light automatically to ensure that there is no stripe appears. • 60 Hz: When the electric supply is 60 Hz, the system adjusts the exposure according to ambient light automatically to ensure that there is no stripe appears. • Outdoor: When Outdoor is selected, the exposure mode supports settings for Gain Priority, Shutter Priority, and Aperture Priority. Different devices support different exposure modes.

Parameter	Description
Mode	Device exposure modes. • Auto: Adjusts the image brightness according to the actual condition automatically. • Gain Priority: When the exposure range is normal, the system prefers the configured gain range when auto adjusting according to the ambient lighting condition. If the image brightness is not enough and the gain has reached upper or lower limit, the system adjusts shutter value automatically to ensure the image at ideal brightness. You can configure gain range to adjust gain level when using gain priority mode. • Shutter priority: When the exposure range is normal, the system prefers the configured shutter range when auto adjusting according to the ambient lighting condition. If the image brightness is not enough and the shutter value has reached upper or lower limit, the system adjusts gain value automatically to ensure the image at ideal brightness. • Manual: Configure gain, shutter and aperture value manually to adjust image brightness.  When the Anti-flicker is set to Outdoor, Gain Priority and Shutter Priority are supported in the exposure mode.
Exposure compensation	Set the exposure compensation value, which ranges from 0 to 50; the larger the value, the higher the image brightness.
Shutter	Set the effective exposure time. The smaller the value, the shorter the exposure time will be. The bigger the value, the longer the exposure time will be.
Shutter range	When the mode is set to Shutter Priority or Manual , and Shutter is selected as User Defined Range , it supports setting the shutter range, with the unit in milliseconds (ms).
Gain	When selecting Gain Priority or Manual , you can set Gain . With minimum illumination, the camera increases Gain automatically to get clearer images.
2D NR	Averaging the pixels of a single frame image with surrounding pixels reduces image noise.
Level	
3D NR	Works with multi-frame (no less than 2 frames) images and reduces noise by using the frame information between previous and latter frames. The greater the value of the noise reduction level, the better the noise reduction effect; however, the motion blur in the image will also increase.
Level	

Step 3 Click **Apply**.

8.2.1.1.4 Setting Backlight

The **Backlight** mode includes **Backlight Compensation**, **Wide Dynamic Range**, **High Light Compensation**, and **Scene Adaptation**.

Step 1 At the upper right corner of the page, click  and select **Camera Settings > Image > Image Attributes > Backlight**.

Step 2 Select **Backlight** mode.

Figure 8-6 Backlight

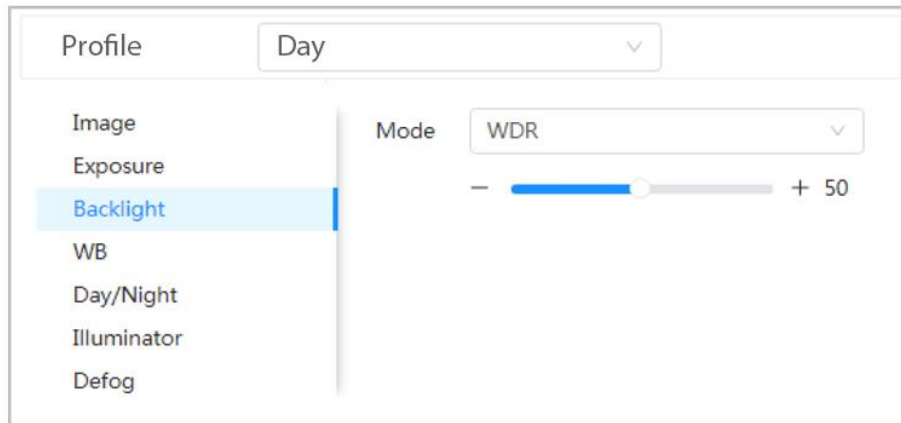


Table 8-4 Description of backlight parameters

Parameter	Description
Off	Turn off the backlight mode.
Backlight compensation	Turning on backlight compensation in backlit environments can help avoid the silhouette effect in the darker areas of the subject being photographed.
WDR	The system dims bright areas and compensates dark areas to ensure the clarity of all the area. The larger the value, the stronger the effect of WDR, making the dark areas brighter; however, this also increases noise.  There might be a few seconds of video loss when the device is switching to WDR mode from other mode.
HLC	Enable HLC when extreme strong light is in the environment (such as toll station or parking lot), the camera will dim strong light, and reduce the size of Halo zone to lower the brightness of the whole image, so that the camera can capture human face or car plate detail clearly. The higher the value is, the more obvious the HLC effect will be.

Step 3 Click **Apply**.

8.2.1.1.5 Setting White Balance

The white balance function can correct color deviations in images caused by lighting conditions, ensuring that white objects appear white in different colored environments.

Step 1 At the upper right corner of the page, click  and select **Camera Settings > Image > Image Attributes > White Balance**.

Step 2 Set **White Balance** mode.

Figure 8-7 White balance

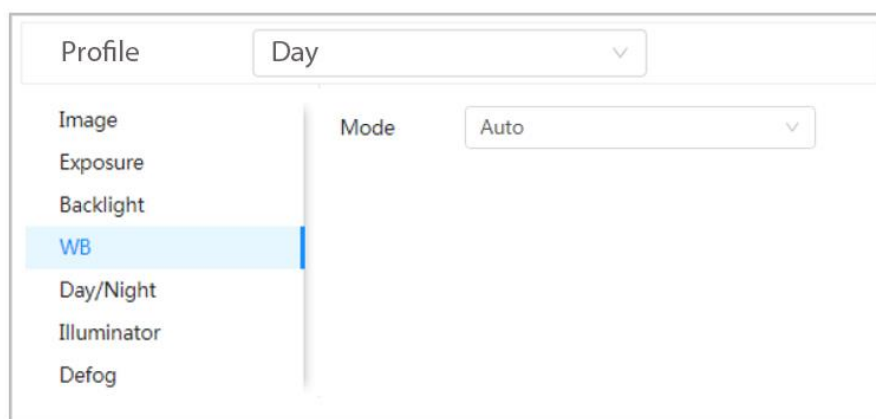


Table 8-5 Description of WB parameters

Parameter	Description
Auto	The system compensates WB according to color temperature to ensure color precision.
Natural light	The system auto compensates WB to environments without artificial light to ensure color precision.
Street Lamp	The system compensates WB to outdoor night scene to ensure color precision.
Indoor	The system auto compensates WB to indoor environments to ensure color precision.
ATW	The system auto compensates WB when the camera is tracking targets.
Outdoor	The system auto compensates WB to most outdoor environments with natural or artificial light to ensure color precision.
Manual	Set red and blue gain manually; the system auto compensates WB according to color temperature.

Step 3 Click **Apply**.

8.2.1.1.6 Setting Day/Night Mode

Set the image display to black and white, color, or switch between color and black and white based on the environment.

Step 1 At the upper right corner of the page, click  and select **Camera Settings > Image > Image Attributes > Day/Night**.

Step 2 Set parameters.

Figure 8-8 Day/Night

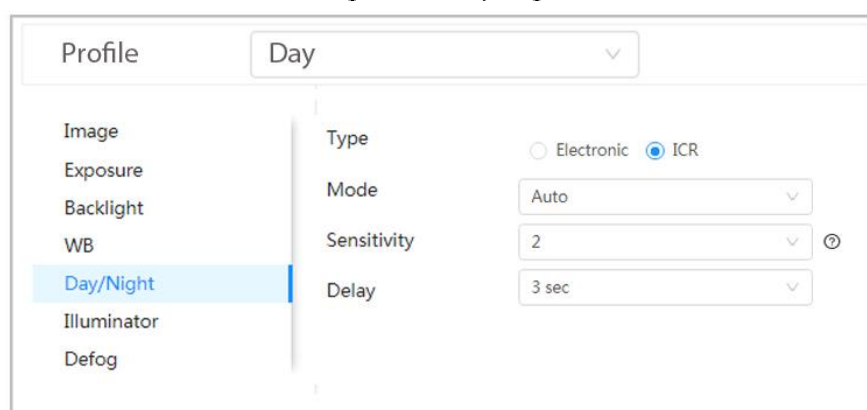


Table 8-6 Description of day and night parameters

Parameter	Description
Type	Select the type from Electronic and ICR. ICR is default. - ICR: The mechanical color-to-black-and-white conversion is accomplished using a filter for day/night switching. - Electronic: Switch day and night through the image processing methods.
Mode	You can select device display mode from Color, Auto, and B/W.  Day/Night configuration is independent from profile management configuration. Color: The system displays color image. Auto: The system switches between color and black-and-white display according to the actual condition. B/W: The system displays black-and-white image.
Sensitivity	This configuration is available only when you set Auto in Mode. You can configure camera sensitivity when switching between color and black-and-white mode. The larger the value, the earlier the color turns to black and white, and the later the black and white turns back to color.
Delay	This configuration is available only when you set Auto in Mode. You can configure the delay when camera switching between color and black-and-white mode. The lower the value is, the faster the camera switches between color and black-and-white mode.

Step 3 Click **Apply**.

8.2.1.1.7 Setting Illuminator

When the device has a built-in fill light, it supports setting the illuminator mode. Different models of the device support different types of fill lights, and the configuration interfaces are also different. Please refer to the actual interface for details.

Step 1 At the upper right corner of the page, click  and select **Camera Settings > Image > Image Attributes > Illuminator**.

Step 2 Set **Illuminator** mode.

Figure 8-9 Illuminator

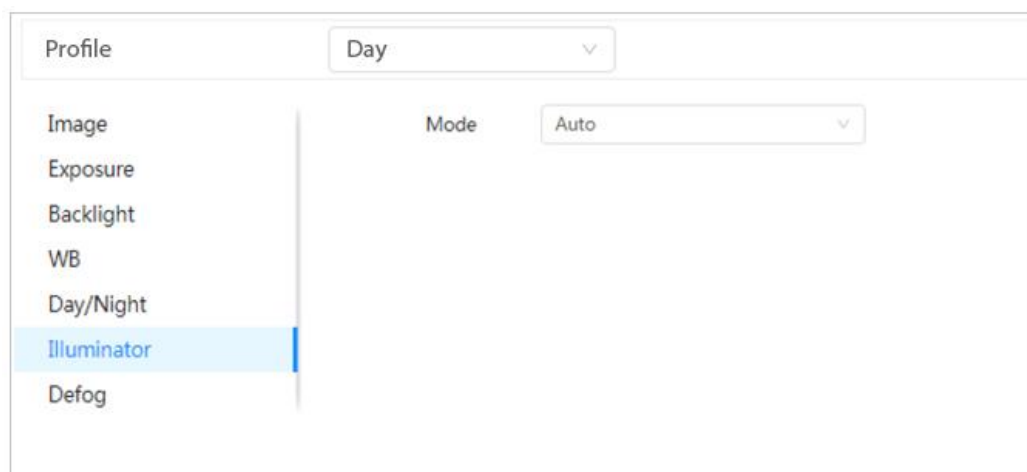


Table 8-7 Description of illuminator parameters

Parameter		Description
Mode	Manual	Adjust the brightness of illuminator manually, and then the system will supply illuminator to the image accordingly.
	Auto	The system adjusts the brightness of the illuminator based on the actual scene. Some devices support setting the sensitivity and brightness limit of the illuminator. • Sensitivity: The higher the sensitivity setting, the fill light will turn on at a higher brightness when the actual scene becomes darker; it will only turn off at a higher brightness when the actual scene becomes brighter. • Brightness Limit: If the fill light is too bright, it may cause overexposure in the center of the image, making it difficult to see the actual picture. In this case, it is recommended to adjust the brightness limit based on the actual scene, with a range of 0 to 100, defaulting to 0.

Step 3 Click **Apply**.

8.2.1.1.8 Setting Defog

When the device is in foggy or hazy environments, image quality will decline. The **Defog** function can be used to adjust the clarity of the image.

Step 1 At the upper right corner of the page, click  and select **Camera Settings > Image > Image Attributes > Defog**.

Step 2 Set **Defog** mode.

Figure 8-10 Defog

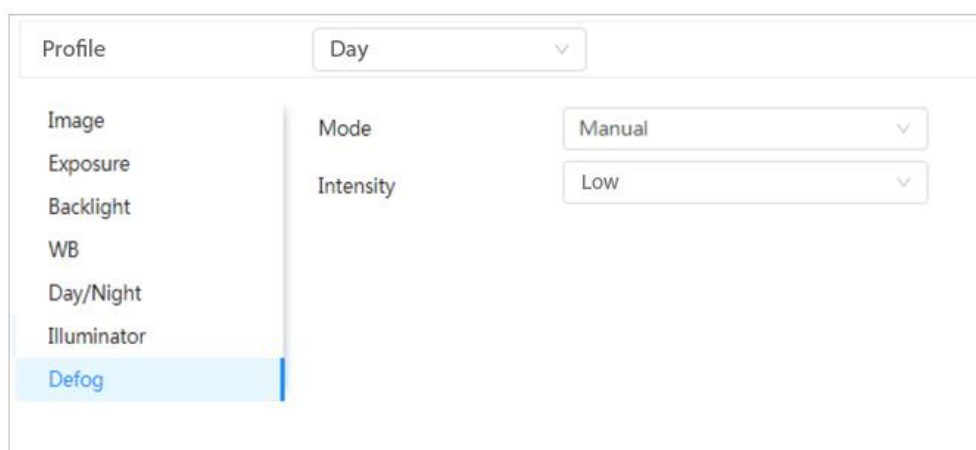


Table 8-8 Description of defog parameters

Parameter	Description
Manual	Configure defog intensity manually, and then the system adjusts image clarity accordingly. Set the intensity higher when the image is not clear.
Auto	The system adjusts image clarity according to the actual condition.
Off	Defog function is disabled.

Step 3 Click **Apply**.

8.2.1.2 Configuring Thermal Channel

You can choose the usage scenario for thermal imaging based on actual shooting requirements, as different scenarios require different parameter settings. You can also customize the parameter values according to your actual needs.

Step 1 At the upper right corner of the page, click  and select **Camera Settings > Image > Image Attributes**.

Step 2 Select **2** in **Channel**.

Step 3 Select the working mode.

- Self-adaptive: The camera will adjust the image according to the environment. If you select **Self-adaptive**, skip to [Step 5](#).
- Customized scene: the camera monitors according to the configured profile type at different times. If you select **Customized Scene**, do [Step 3](#).

Step 4 Select profile, pseudo color, and usage scenario.



The image is for reference only, and might differ from the actual page.

Figure 8-11 Camera(thermal)

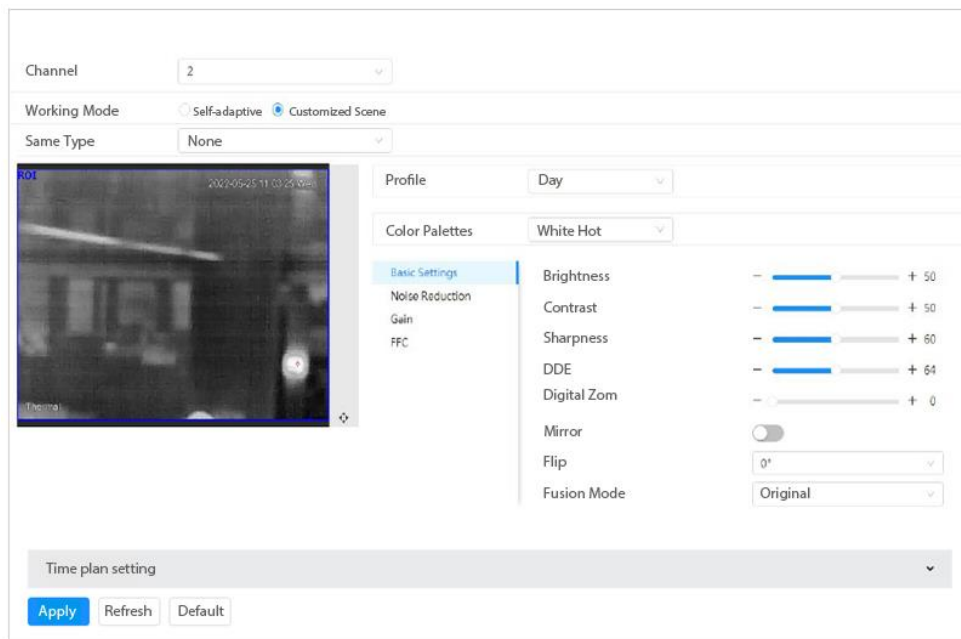


Table 8-9 Description of defog parameters

Parameter	Description
Profile	• Normal, Day and Night can be selected. • After selecting the configuration file, you can configure the relevant parameters for thermal imaging in that file.
Scene Type	Select different scenes according to actual needs. Each scene is automatically associated with different parameter values, making it convenient to quickly set up the thermal imaging display. • Low Dynamic: this scene can be selected when the temperature of the object being captured is too low or too high. After setting it, the object will be displayed more clearly in the thermal imaging picture, but the details in the image may be less pronounced.

Parameter	Description
	● High Dynamic: this scene can be selected when the temperature of the object being captured is normal and there is a high demand for detail in the captured image. ● Self-adaptive: the image quality is automatically adjusted based on the temperature of the object being captured. It is recommended to select this scene.
Colorization	Add color to the thermal image and use color to indicate the temperature. "White glow" is the default color. ● Self-adaptive scene: automatically adjust image quality based on the temperature of the subject being captured. It is recommended to choose this scene. ● Black glow: lighter when the temperature is lower in gray image. ● Fusion: color is concentrated on the range of purple- red-yellow. More purple when the temperature is lower and more yellow when the temperature is higher. ● Rainbow: color is concentrated on the range of blue- green-red- yellow. Bluer when the temperature is lower and more yellow when the temperature is higher. ● Golden autumn: color is concentrated on the range of red- yellow. Redder when the temperature is lower and more yellow when the temperature is higher. ● Midday: color is concentrated on the range of blue- green-red- yellow. Bluer when the temperature is lower and more yellow when the temperature is higher. ● Iron oxide red: its color range is similar to that of Midday, but its brightness is lower than Midday. ● Amber: it's mainly represented as brown. Brighter when the temperature is higher. ● Boulder: color is concentrated on the range of purple - red- yellow- green- blue. More purple when the temperature is lower and bluer when the temperature is higher. ● The setting sun: color is concentrated on the range of blue- red- yellow. Bluer when the temperature is lower and more yellow when the temperature is higher. ● Ice and fire: in color image, high temperature objects show red and low temperature objects show blue. Ice and fire is usually used to give a warning. ● Oil painting: color is concentrated on the range of purple-blue- green- yellow-red. More purple when the temperature is lower and redder when the temperature is higher. ● Pomegranate: it's mainly represented as wine red. Brighter when the temperature is higher. ● Green jade: it's mainly represented as aquamarine. Brighter when the temperature is higher. ● Spring: The colors are predominantly rose red and yellow; the lower the temperature, the more rose red it appears, and the higher the temperature, the more yellow it becomes.

Parameter	Description
	• Summer: The colors are predominantly green and yellow; the lower the temperature, the greener it appears, and the higher the temperature, the more yellow it becomes. • Autumn: The colors are predominantly orange and yellow; the lower the temperature, the more orange it appears, and the higher the temperature, the more yellow it becomes. • Winter: The colors are predominantly blue and yellow; the lower the temperature, the bluer it appears, and the higher the temperature, the more yellow it becomes.

Step 5 (Optional) Configure the advanced parameters.

When the scene cannot meet the scene requirements, configure the advanced parameters manually.

Table 8-10 Description of Advanced parameters

Classification	Parameter	Description
Basic Settings	Brightness	Adjust the overall brightness of the image, generally speaking, you can keep the default settings. The larger the value, the brighter the image will be.
	Contrast	When the grayscale distribution of the image is not clear or appears blurred, you can adjust the contrast of the image. The larger the value, the greater the brightness contrast of the image. However, if this value is set too high, the darker areas of the image may become excessively dark, and the brighter areas may become overexposed.
	Sharpness	Change the sharpness of image edges. The larger the value, the more obvious the image edge.
	DDE	Makes the details of the image clear. The bigger the value is, the clearer the details will be.
	Digital Zoom	Enlarge the thermal image according to the zoom time you have set.
	Mirror	Open the mirror image and the monitor image will reverse from left to right.  After enabling mirroring, the tracking of cold and hot spots will change according to the position of the image.

Classification	Parameter	Description
	Flip	Changes the display direction of the picture. • 0°: Normal display. • Corridor Mode 1: The picture rotates 90° clockwise. • Mirror: The image is displayed upside down. • Corridor Mode 2: The picture rotates 90° counterclockwise.  For some models, please set the resolution to be 1080p or lower when using Corridor Mode.
	Fusion Mode	Overlay the visible light channel data with the thermal imaging channel data, retaining the gray information of the visible light image while using pseudo-color to represent different temperatures, making the thermal imaging video clearer. • Original: Displays the image of the thermal channel. • Warm Color: Combines the data of the visible channel and the thermal channel, and displays the image in warm color. • Cold Color: Combines the data of the visible channel and the thermal channel, and displays the image in cold color. • Thermal Fusion: Overlay the thermal imaging channel data with the visible light channel data and display it in iron red tones. • Fusion Rate: It ranges from 0 to 100. The larger the value, the larger the proportion of the visible channel. • Dual-Lens Calibration Adjustment: You can adjust the misaligned images through direction keys. • Speed: The moving speed of the lens when adjusting the image.  To get a better fusion effect, keep the distance 3 m between the Camera and the targets.
Image Enhancement	2D NR	Remove the 2D noise in the image. As the value increases, the image noise decreases, but the image details become more blurred.
	Basic 3D NR	To remove 3D noise from the image, you can

Classification	Parameter	Description
	Advanced 3D NR	generally keep the default options. As the value increases, the denoising effect improves, but it also ensures that the video output maintains stability, which results in more pronounced motion blur for moving objects. - Basic 3D NR: The module handles noise reduction. - Advanced 3D NR: The back-end program handles noise reduction.  In general, you can choose 2D NR and Basic 3D NR. If the image is still not clear enough at this point, you may select Advanced 3D NR and adjust the parameters.
Gain settings	Auto Gain	The bigger the gain value, the more sensitive the parameters in Basic Settings , resulting in a less stable image.
FFC设置	FFC	When the camera monitors an area for an extended period, there may be abnormalities in the display of image edges. In this case, it is recommended to perform shutter calibration by closing the shutter blade and adjusting the auxiliary lens to correct the error. - Auto: According to the switch period that you have configured, the shutter will be corrected regularly. - Manual: Correct the shutter by yourself.
	FFC Period	You can configure this parameter only when FFC Mode is set to be Auto. Adjust time gap of correcting the shutter automatically.
	Do FFC	Click Do FFC to trigger the shutter correcting for this time.

Step 6 Click **Apply**.

8.2.3 Setting Video Parameters

Set the video parameters, including encoding settings, video overlay, and regions of interest.

8.2.3.1 Setting Encode

Configure the video stream parameters based on the actual network bandwidth, including video encoding, resolution, frame rate, bitrate control, bitrate, I-frame interval, SVC (Scalable Video Coding), and watermark settings.

Step 1 At the upper right corner of the page, click  and select **Camera Settings > Encode > Encode**.

Step 2 Select the channel.

- Select 1 in Channel to set the parameters of visible channel.

- Select 2 in Channel to set the parameters of thermal channel.

Step 3 Set video stream.

The default values for the bitrate on different devices may vary; please refer to the actual interface for specifics.

Figure 8-12 Video stream

The screenshot displays the 'Video Stream' configuration window. At the top, a 'Channel' dropdown is set to '1'. Below this, the interface is divided into two panels: 'Main Stream' and 'Sub Stream'.

Main Stream Settings:

- Compression: H.265
- Resolution: 2336*1752 (2336x...)
- Frame Rate (FPS): 25
- Bit Rate Type: CBR
- Reference Bit Rate: 1536-8192 (Kb/s)
- Bit Rate: 6144 (Kb/s)
- I Frame Interval: 50 (25-150)
- Smooth Stream: A slider set to 50.
- Watermark: Enabled (toggle switch)
- Watermark String: DigitalCCTV

Sub Stream Settings:

- Enable: Enabled (toggle switch)
- Compression: H.265
- Resolution: 352*288 (CIF)
- Frame Rate (FPS): 15
- Bit Rate Type: CBR
- Reference Bit Rate: 81-252 (Kb/s)
- Bit Rate: 192 (Kb/s)
- I Frame Interval: 30 (15-150)
- Smooth Stream: A slider set to 50.

Table 8-11 Description of video stream parameters

Parameter	Description
Enable	Click ☐ to enable sub stream, it is enabled by default. You can enable multiple sub streams simultaneously.
Video Encode	Choose the video encode mode based on the actual bandwidth. ● H.264: H.264 (Main Profile encode mode) . At the same image quality, it occupies more bandwidth than H.264. ● H.264H: 和H.264H (High Profile encode mode) . At the same image quality, it occupies less bandwidth than H.264. ● H.265: Main Profile encode mode. At the same image quality, it occupies less bandwidth than H.264.
Resolution	The resolution of the video. The higher the value is, the clearer the image will be, but the bigger the required bandwidth will be.
Frame Rate (FPS)	The number of frame in one second of video. The higher the value is, the clearer and smoother the video will be.

Parameter	Description
Bit Rate Type	The bit rate control type during video data transmission. ● CBR (Constant Bit Rate): The bit rate keeps close to the defined bit rate value. When the scene is complex, there may be issues with image clarity; when the scene is simple, it may result in wasted bitrate. ● VBR (Variable Bit Rate): The bit rate changes as monitoring scene changes. It ensures that the image is clear in complex scenes while minimizing bandwidth usage in simple scenes.  The Bit Rate Type can only be set as CBR when Encode Mode is set as MJPEG.
Reference Bit Rate	The most suitable bit rate value range recommended to user according to the defined resolution and frame rate.
Bit Rate	This parameter can be configured only when the Bit Rate Type is set as CBR . Select bit rate value in the list according to actual condition and Reference Bit Rate .
I Frame Interval	The number of P frames between two I frames should be as low as possible, as a smaller value results in fewer P frames and higher image quality. The I frame interval varies with the frame rate, and it is recommended to set the I frame interval to twice the frame rate.
Smooth Stream	The larger the smooth stream value is, the larger the I Frame is.
Watermark	After setting a watermark on the video stream, you can verify the watermark to check if the video has been tampered.
Watermark String	1. Select Watermark to enable this function. 2. Enter Watermark String, which is set as Digital CCTV by default.

Step 4 Click Apply.

8.2.3.2 Setting Video Overlay

Set video overlay information, and the preview interface will display the corresponding information.

8.2.3.2.1 Setting Privacy Masking

You can enable this function when you need to protect the privacy of some area on the image.

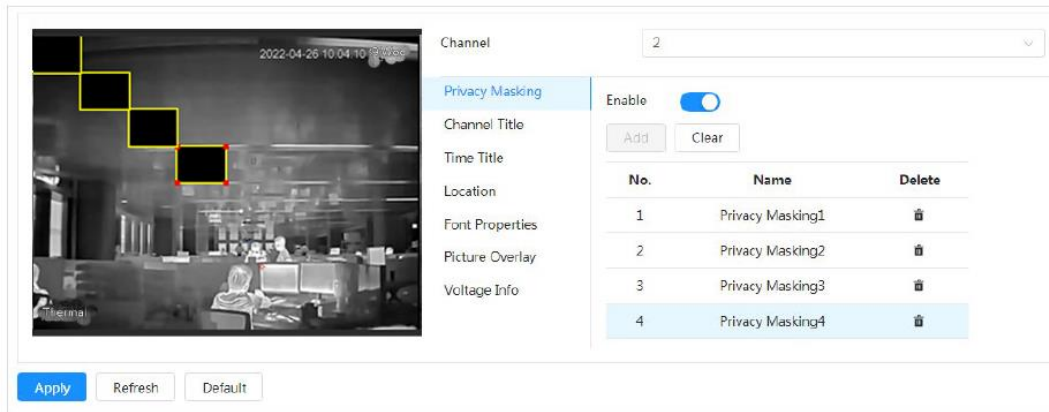
- Step 1 At the upper right corner of the page, click  and select **Camera Settings > Encode > Video Overlay**.
- Step 2 Select the channel.
- Select 1 in Channel to set the parameters of visible channel.
 - Select 2 in Channel to set the parameters of thermal channel.
- Step 3 Click the **Privacy Masking** tab.
- Step 4 Click  next to **Enable**.
- Step 5 Click **Add**, and then drag the block to the area that you need to cover.



- Privacy masking boxes are generated automatically in the image. You can draw four blocks at most.
- Click **Clear** to delete all the area boxes; after selecting privacy masking box, click  to delete it.

Step 6 Adjust the size of the rectangle to protect the privacy.

Figure 8-13 Privacy masking



Step 7 Click **Apply**.

8.2.3.2.2 Setting Channel Title

You can enable this function when you need to display channel title on the image.

Step 1 At the upper right corner of the [age, click  and select **Camera Settings > Encode > Video Overlay**.

Step 2 Select the channel.

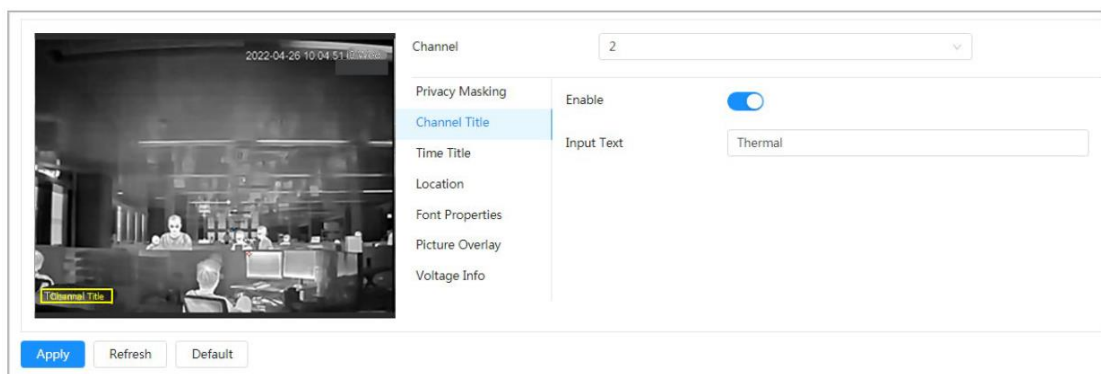
- Select 1 in Channel to set the parameters of visible channel.
- Select 2 in Channel to set the parameters of thermal channel.

Step 3 Click the **Channel Title** tab.

Step 4 Click  next to **Enable**.

Step 5 Set **Channel Title**.

Figure 8-14 Channel title



Step 6 Drag the channel title box to the appropriate position.

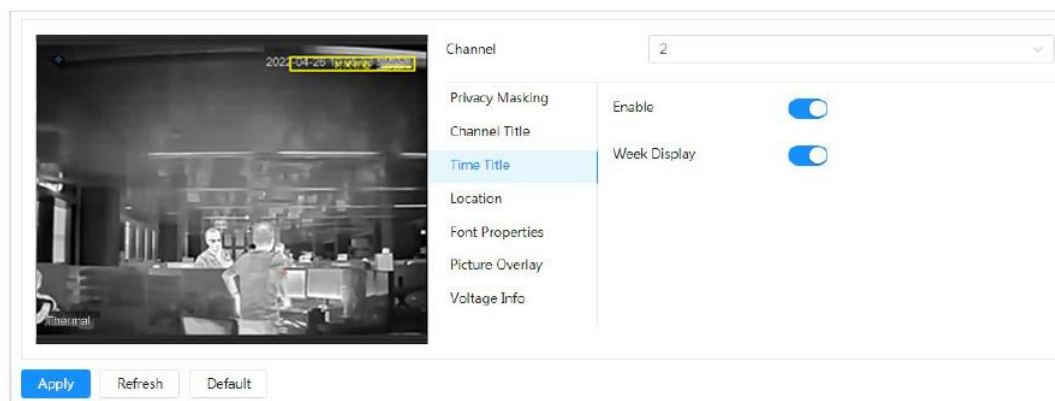
Step 7 Click **Apply**.

8.2.3.2.3 Setting Time Title

You can enable this function when you need to display time on the image.

- Step 1 At the upper right corner of the page, click  and select Camera Settings > Encode > Video Overlay.
- Step 2 Select the channel.
 - Select 1 in Channel to set the parameters of visible channel.
 - Select 2 in Channel to set the parameters of thermal channel.
- Step 3 Click the **Time Title** tab.
- Step 4 Click ☐ next to **Enable**.
- Step 5 (Optional) Select **Week Display** and then the week information displays on the image.
- Step 6 Drag the time box to the position that you want in the image.

Figure 8-15 Time title



- Step 7 Click **Apply**.

8.2.3.2.4 Setting Location

You can enable this function if you need to display text on the image.



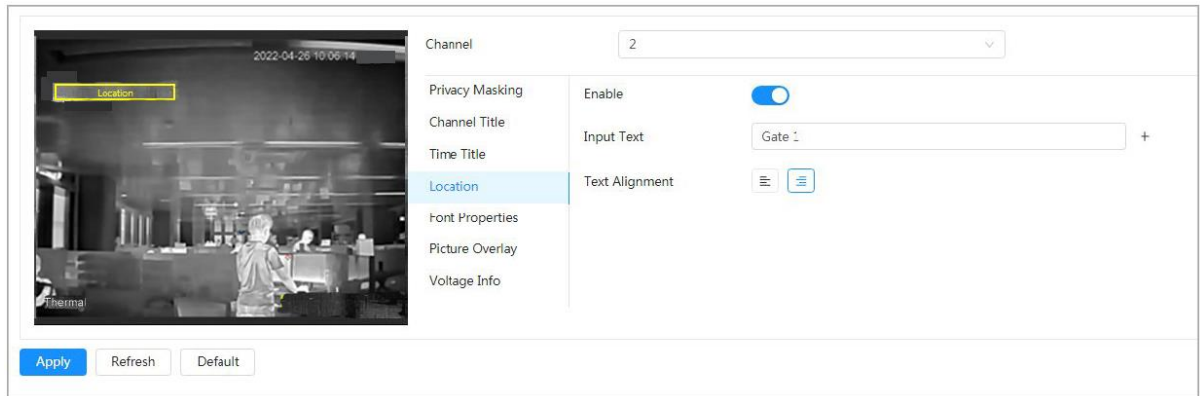
The location and image overlay cannot be enabled simultaneously. When connecting to a network camera with a private protocol on the vehicle-mounted NVR, priority is given to overlaying GPS (Global Positioning System) information.

- Step 1 At the upper right corner of the page, click  and select **Camera Settings > Encode > Video Overlay**.
- Step 2 Select the channel.
 - Select 1 in Channel to set the parameters of visible channel.
 - Select 2 in Channel to set the parameters of thermal channel.
- Step 3 Click the **Location** tab.
- Step 4 Click ☐ next to **Enable**.
- Step 5 Enter the location information, and then select alignment.



Click "+" to add location overlay, and you can add 13 lines at most.

Figure 8-16 Location



Step 6 Drag the location box to the appropriate position.

Step 7 Click **Apply**.

8.2.3.2.5 Setting Font Properties

When you need to adjust the font color or size of the overlay information in the video frame, you can enable this function.

Step 1 At the upper right corner of the page, click  and select **Camera Settings > Encode > Video Overlay**.

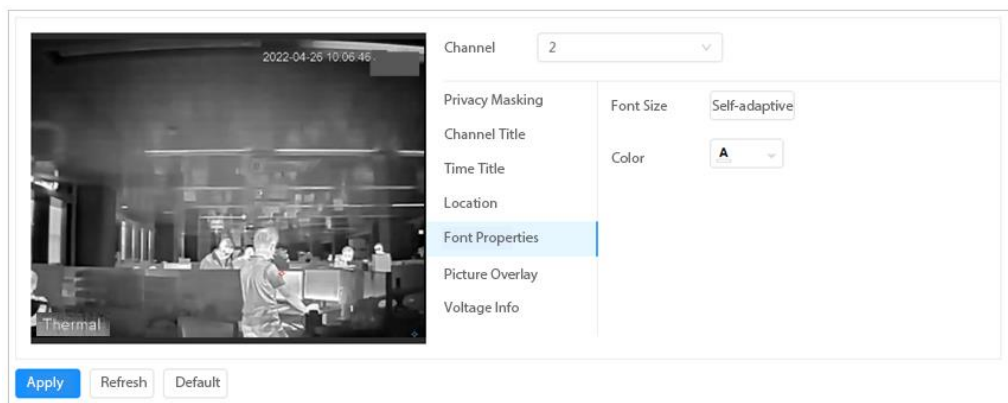
Step 2 Select the channel.

- Select 1 in Channel to set the parameters of visible channel.
- Select 2 in Channel to set the parameters of thermal channel.

Step 3 Click **Font Properties** tab.

Step 4 Select proper font color and size.
Supports custom colors

Figure 8-17 Font Properties



Step 5 Click **Apply**.

After saving the settings, the font properties in the video frame will change to the specified color and size.

8.2.3.2.6 Setting Picture Overlay

You can enable this function if you need to display picture information on the image.



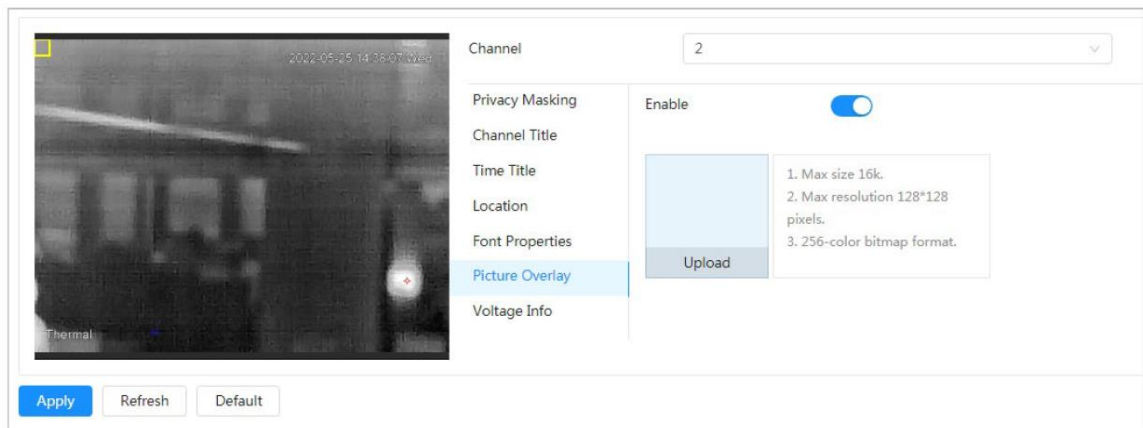
Location and picture overlay cannot work at the same time.

Step 1 At the upper right corner of the page, click  and select **Camera Settings > Encode >**

Video Overlay.

- Step 2 Select the channel.
- Select 1 in Channel to set the parameters of visible channel.
 - Select 2 in Channel to set the parameters of thermal channel.
- Step 3 Click the **Picture Overlay** tab.
- Step 4 Click ☐ next to **Enable**.
- Step 5 Click **Upload**, and then select the picture to be overlaid.
The image is displayed in the **Image Preview**.

Figure 8-18 Picture overlay



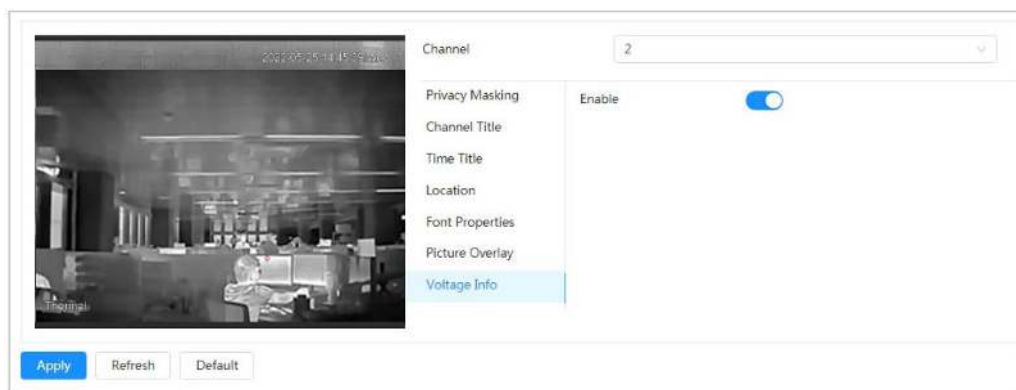
- Step 6 Drag the overlaid image to the appropriate position in the video frame.
- Step 7 Click **Apply**.

8.2.3.2.7 Setting Voltage Information

After enabling voltage information, the image displays the voltage information when the voltage is abnormal.

- Step 1 At the upper right corner of the page, click  and select **Camera Settings > Encode > Video Overlay**.
- Step 2 Select the channel.
- Select 1 in Channel to set the parameters of visible channel.
 - Select 2 in Channel to set the parameters of thermal channel.
- Step 3 Click the **Voltage Info** tab.
- Step 4 Click ☐ next to **Enable**.
After enabling voltage information, picture overlay will be disabled.

Figure 8-19 Voltage information



- Step 5 Click **Apply**.

After enabling the voltage function, the video frame will display overlay when there is an abnormal voltage.

For example, if the device requires a 12V voltage, when the voltage exceeds $\pm 15\%$, the video frame will display an overlay indicating a voltage abnormality, prompting the customer to check the voltage.

8.2.3.3 Setting ROI

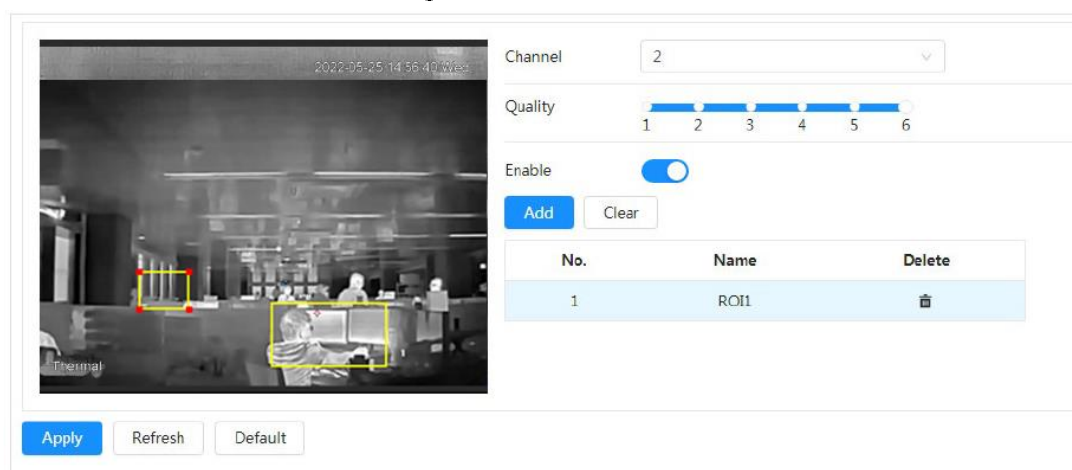
Select ROI (region of interest) on the image and configure the image quality of ROI, and then the selected image is display at defined quality.

- Step 1 At the upper right corner of the page, click  and select **Camera Settings > Encode > ROI**.
- Step 2 Select the channel.
- Select 1 in Channel to set the parameters of visible channel.
 - Select 2 in Channel to set the parameters of thermal channel.
- Step 3 Click ☐ next to Enable.
- Step 4 Click **Add**, and then adjust and drag the rectangle on the image, and then set the image quality of ROI.



- You can draw 4 area boxes at most.
- The higher the image quality value is, the better the quality will be.
- Click **Clear** to delete all the ROI; After selecting ROI, click  to delete it.

Figure 8-20 ROI



- Step 5 Click **Apply**.

8.2.4 Setting Audio Parameters

8.2.4.1 Setting Audio

Set the audio input type, volume, etc. When audio encoding is enabled, the network transmitted stream will be an audio-video composite stream; otherwise, it will only include video.



Before enabling sub-stream audio, click  at the upper right corner of the page and select **Camera Settings > Encode > Encode** to enable video stream of sub-stream.

Step 1 At the upper right corner of the page, click  and select **Camera Settings > Audio > Audio**.

Step 2 Select the enable switch for the main stream or sub-stream region, and turn on audio encoding.



CAUTION

Please carefully decide whether to enable the audio capture function based on the actual usage requirements.

Figure 8-21 Audio

Step 3 Setting parameters.

Table 8-12 Description of audio parameters

Parameter	Description
Audio Input Type	Displays audio input source type of the device. ● LineIn: The device captures audio signals through external audio equipment. ● Mic: The device captures audio signals through its built-in microphone.
Audio Encoding	The configured audio encode mode applies to audio and intercom. You are recommended to use the default mode.
Sampling Frequency	Sampling number per second. The higher the sampling frequency is, the more the sample in a second will be, and the more accuracy the restored signal will be.
Noise Filter	Enable this function, and the system auto filters ambient noise.
Microphone Volume	Adjusts microphone volume.
Speaker Volume	Adjusts speaker volume of the speaker or intercom.

Step 4 Click **Apply**.

8.2.4.2 Setting Alarm Tone

Set the alarm sound so that when an alarm occurs, the corresponding alarm sound is played. Some

devices support recording or uploading custom alarm sounds.

Procedure

- Step 1 At the upper right corner of the page, click  and select **Camera Settings > Audio > Alarm Tone**.
- Step 2 Click **Add**.
- Step 3 Add the audio file of the alarm.
- Select **Record**, enter the file name, click **Record** to record a new audio message, click **Stop** to finish recording, and the file will be automatically added successfully.
 - Select **Upload**, click **Browse** to select the audio file to be uploaded, and then click **Upload**.



- The audio files recorded by the device are in .pcm format, and only some devices support recording.
- The device supports uploading audio files in .pcm, .wav, .mp3, and .aac formats.
- Recorded or uploaded audio files can be edited and deleted.
 - ◇ Edit: Click  to edit the file name in the pop-up interface.
 - ◇ Delete: Click  to delete alarm audio file.

Figure 8-22 Add alarm audio file



Related Operations

- Play audio file.
Click  to play the alarm sound.
- Download audio file.
Click  to download alarm sound to the local to the local system, saving it to the browser's default download path.

8.3 Network Settings

Introduce the device's network configuration and configure it according to actual needs.

8.3.1 Setting TCP/IP

According to the network plan, set the device's IP address, DNS (Domain Name System) server, and

other information to ensure that the device has a normal network connection with other devices.

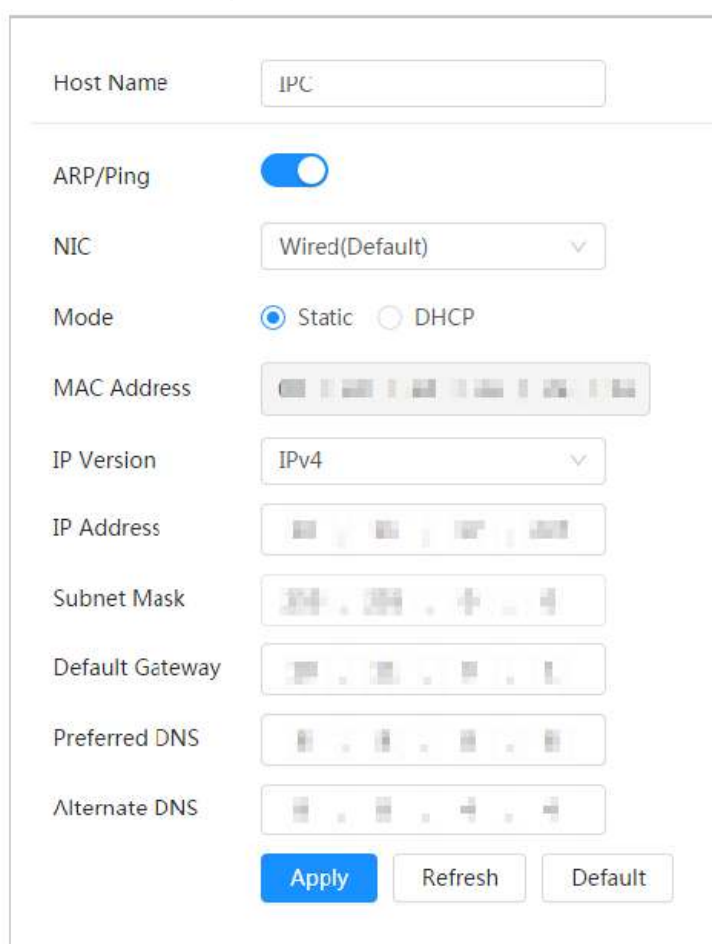
Prerequisite

The camera has connected to the network.

Procedure

- Step 1 At the upper right corner of the page, click  and select **Network > TCP/IP**.
- Step 2 Select the network mode of the device and configure the device's IP address, DNS, and other relevant information.

Figure 8-23 TCP/IP



Host Name: IPC

ARP/Ping: ☒

NIC: Wired(Default)

Mode: ☒ Static ☐ DHCP

MAC Address: [Hexadecimal digits]

IP Version: IPv4

IP Address: [Hexadecimal digits]

Subnet Mask: [Hexadecimal digits]

Default Gateway: [Hexadecimal digits]

Preferred DNS: [Hexadecimal digits]

Alternate DNS: [Hexadecimal digits]

Buttons: Apply, Refresh, Default

Table 8-13 Description of TCP/IP parameters

Parameter	Description
Host Name	Set the current host name, with a maximum length of 32 characters, and reserve functionality.
ARP/Ping	Select 'ARP/Ping' to enable ARP/Ping settings for the device's IP address service. When the MAC address of the device is known, it supports modifying and setting the device's IP address through ARP (Address Resolution Protocol) / ping commands. After enabling this feature, during the device's reboot process, the IP can be set within 2 minutes using a ping packet of a specific length. This service will close after 2 minutes or once the IP is set. A demonstration of setting IP address via ARP/Ping. 1. Keep the camera that needs to be configured and the PC within the same local network, and then get a usable IP address. 2. Get the MAC address of the camera from device label. 3. Open command editor on the PC and enter commands according to the

Parameter	Description
	system. - Windows system (Only some computers are supported) Windows syntax↵ <pre>arp -s <IP Address> <MAC> ↵ ping -l 480 -t <IP Address> ↵</pre> Windows example↵ <pre>arp -s 192.168.0.125 11-40-8c-18-10-11↵ ping -l 480 -t 192.168.0.125↵</pre> - UNIX/Linux/Mac UNIX/Linux/Mac syntax↵ <pre>arp -s <IP Address> <MAC> ↵ ping -s 480 <IP Address> ↵</pre> UNIX/Linux/Mac example↵ <pre>arp -s 192.168.0.125 11-40-8c-18-10-11↵ ping -s 480 192.168.0.125↵</pre> - Restart the camera. - Check the PC command line, if information such as Reply from 192.168.0.125...is displayed, the configuration succeeds. - Turn the command line off. Enter http://(IP address) in the browser address bar to log in.
NIC	Select the Ethernet card that need to be configured, and the default one is Wire .
Mode	The mode that the camera gets IP: - Static: Set IP Address, Subnet Mask, and Default Gateway manually, and then click Apply, the login page with the configured IP address is displayed. - When there is DHCP server in the network, select DHCP, and the camera acquires IP address automatically so that you don't have to set IP address and other information manually.
MAC Address	Displays host MAC (Media Access Control) address.
IP Version	Select IPv4 or IPv6 .
IP Address	When Mode is set to Static, you need to enter the device's IP address, subnet mask, and default gateway according to the network plan.  - IPv6 does not have subnet mask. - The default gateway must be in the same network segment with the IP address.
Subnet Mask	
Default Gateway	
Preferred DNS	IP address of the preferred DNS
Alternate DNS	IP address of the alternate DNS

Step 3 Click Apply.

8.3.2 Setting Port

Configure the maximum number of users that can connect to the device simultaneously (including WEB, platform clients, mobile clients, etc.) and configure the respective port numbers.

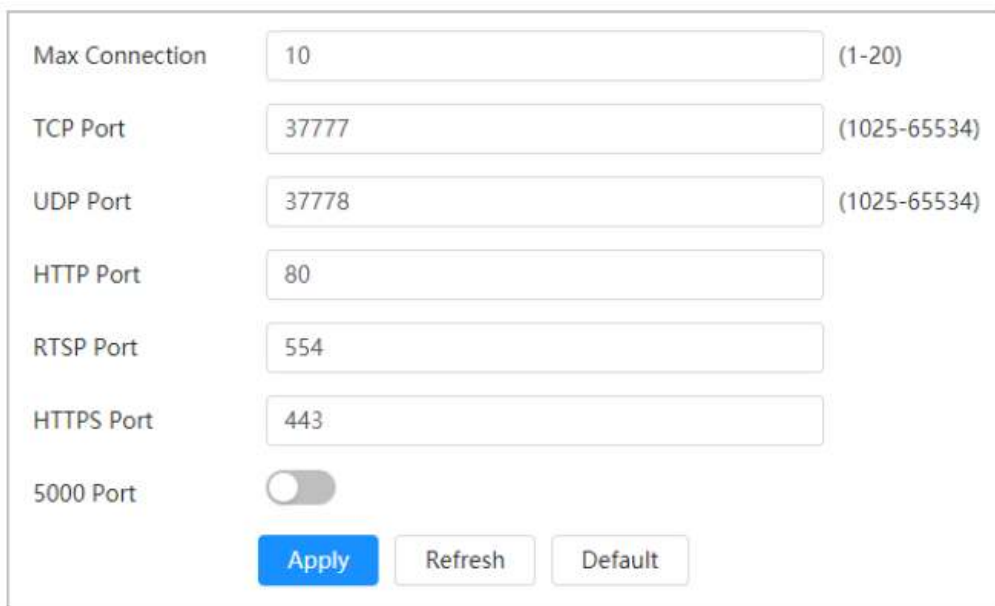
Step 1 At the upper right corner of the page, click  and select **Network > Port**.

Step 2 Set the parameters.



- Changes to parameters other than “maximum connection number, RTSP port, RTMP port, and HTTPS port” will take effect after restarting the device.
- 0~1024, 1900, 3800, 5000, 5050, 9999, 37776, 37780~37880, 39999, 42323 are occupied for specific uses.
- Do not use the default value of any other port during port configuration.

Figure 8-24 Port



Max Connection	10	(1-20)
TCP Port	37777	(1025-65534)
UDP Port	37778	(1025-65534)
HTTP Port	80	
RTSP Port	554	
HTTPS Port	443	
5000 Port	☐	
Apply Refresh Default		

Table 8-14 Description of port parameters

Parameter	Description
Max Connection	The max number of users (web client, platform client or mobile phone client) that can connect to the device simultaneously. The value is 10 by default.
TCP Port	Transmission control protocol port. The value is 37777 by default.
UDP Port	User datagram protocol port. The value is 37778 by default.
HTTP Port	The HTTP (Hyper Text Transfer Protocol) communication port defaults to 80. If set to a different value, you need to append the modified port number to the IP address when logging in with a browser.

Parameter	Description
RTSP Port	- The RTSP (Real Time Streaming Protocol) port number defaults to 554. Users can use the following URL (Uniform Resource Locator) format to stream real-time monitoring when using Apple's QuickTime browser or VLC (Video LAN Client) for playback. - The URL format for real-time monitoring stream: When requesting the real-time monitoring RTSP stream service, you should specify the requested channel number and stream type in the URL. If authentication is required, you must also provide a username and password. - When users access the stream using a BlackBerry phone, they need to set the encoding mode to H.264B, configure the resolution to CIF, and disable the audio. URL format: <code>rtsp://username:password@ip:port/cam/realmonitor?channel=1&subtype=0</code> If no authentication is required, use the following format: <code>rtsp://ip:port/cam/realmonitor?channel=1&subtype=0</code> - Username: The username, such as admin. - Password: The password, such as admin. - Ip: IP of the device, such as 192.168.1.112. - Port: Leave it if the value is 554 by default. - Channel: The channel number, which starts from 1. For example, if you are using channel 2, then the channel=2. - Subtype: The stream type: the main stream is 0 (i.e., subtype=0), sub stream 1 is 1 (i.e., subtype=1), sub stream 2 is 2 (i.e., subtype=2), sub stream 3 is extra3 (i.e., subtype=extra3), and sub stream 4 is extra4 (i.e., subtype=extra4). For example, request sub stream 1 of channel 2 from a device. The URL should be: <code>rtsp://admin:admin@192.168.1.112:554/cam/realmonitor?channel=2&subtype=1</code>
HTTPS Port	HTTPS (Hyper Text Transfer Protocol over Secure Socket Layer) communication port, default is 443.
5000 Port	The service port of Windows XP. It is Off by default.

Step 3 Click **Apply**.

8.3.3 Setting PPPoE

PPPoE (Point to Point Protocol over Ethernet) is one of the protocols that device uses to connect to the internet. Establish a network connection via PPPoE dial-up. After a successful connection, the device automatically obtains a dynamic public IP address.

Prerequisites

- The device is connected to the public internet.
- You have gotten the account and password from Internet Service Provider (Internet Service Provider).

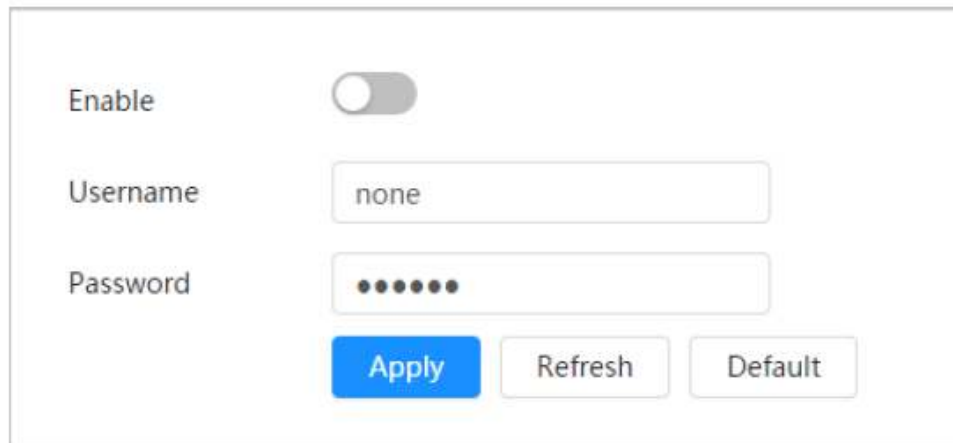


- Disable UPnP while using PPPoE to avoid possible influence.
- After making PPPoE connection, the device IP address cannot be modified through web page.

Procedure

- Step 1 At the upper right corner of the page, click  and select **Network > PPPoE**.
- Step 2 Click ☐ next to Enable.
- Step 3 Enter the username and password of PPPoE.

Figure 8-25 PPPoE



- Step 4 Click **Apply**.
The system prompts that the save was successful and displays the obtained public IP address in real-time. Users can access the device using this IP address.

8.3.4 Setting DDNS

After setting the DDNS (Dynamic Domain Name System) parameters, when the device's IP address changes frequently, the system dynamically updates the relationship between the domain name and the IP address on the DNS server. You can access the device remotely using the domain name without having to keep track of the constantly changing IP address.

Prerequisite

Confirm the type of domain name resolution server supported by the camera.



- Third party server might collect your device information after DDNS is enabled.
- Register and log in to the DDNS website, and then you can view the information of all the connected devices in your account.

Procedure

- Step 1 At the upper right corner of the page, click  and select **Network > DDNS**.
- Step 2 Select **Type** and set parameters of DDNS according to actual conditions.

Figure 8-26 DDNS

Table 8-15 Description of DDNS parameters

Parameter	Description
Type	The name and web address of the DDNS service provider, see the matching relationship below: • CN99 DDNS web address: www.3322.org • NO-IP DDNS web address: dynupdate.no-ip.com • Dyndns DDNS web address: members.dyndns.org
Server Address	
Domain Name	
Test	Only when selecting NO-IP DDNS type, you can click Test to check whether the domain name registration is successful.
Username	Enter the username and password that you got from the DDNS server provider. You need to register an account (includes username and password) on the DDNS server provider's website.
Password	
Interval	The update cycle of the connection between the device and the server.

Step 3 Click **Apply**.

Result

Open the browser on PC, enter the domain name at the address bar, and then press **Enter**, the login page is displayed.

8.3.5 Setting Email

Set email information and enable email linkage. The system sends email to the defined address when the corresponding alarm is triggered.

Step 1 At the upper right corner of the page, click  and select **Network > Email**.

Step 2 Click  next to Enable.

Step 3 Set the parameters.

Figure 8-27 Email

The screenshot shows a configuration window for email settings. The 'Enable' toggle is turned on. 'SMTP Server' is set to 'none' and 'Port' is '25'. 'Anonymous' is turned off, with 'Username' set to 'anonymity' and 'Password' masked with dots. 'Sender' is 'none' and 'Encryption Type' is 'TLS(Recommended)'. The 'Subject' is 'IPC Message' and the 'Attachment' checkbox is checked. The 'Receiver' field is empty with an 'Add' button. 'Health Mail' is turned off. 'Sending Interval' is set to '60' minutes, with a range of 'min.(30-1440)' indicated. At the bottom are 'OK', 'Refresh', and 'Default' buttons.

Table 8-16 Description of email parameters

Parameter	Description	
SMTP Server	SMTP (Simple Mail Transfer Protocol) server address.	 For details, see Table 8-17.
Port	The port number of the SMTP server.	
Username	The account of SMTP server.	
Password	The password of SMTP server.	
Anonymous	Select Anonymous and the sender's information is not displayed in the email.	
Sender	Sender's email address.	
Encryption Type	Select Encryption Type, including None、SSL (Secure Sockets Layer) and TLS (Transport Layer Security).  For details, see Table 8-17.	
Subject	Enter maximum 120 characters in Chinese, English, and Arabic numerals. Click "+" to select type, including Device Name , Device ID , and Event Type , and you can set maximum 2 types.	
Attachment	Select the check box to support attachment in the email.	
Receiver	Receiver's email address. Supports 3 addresses at most.	
Health Mail	Determine whether the email link is successful through the test information automatically sent by the system. Select Health Email and set the sending time interval. The system will send email test information according to the specified interval. 	
Sending interval		
	The sending interval for health emails ranges from 30 minutes to 1440 minutes.	

Table 8-17 Description of common mailbox setting parameters

Email Type	SMTP Server	Encryption Type	Port	Description
QQ	smtp.qq.com	SSL	465	- The encryption type cannot be set as None. - The email must have SMTP service enabled. - The password must use an Authorization Code, and the QQ login password or email login password is invalid.  Authorization Code: The authorization code obtained when the email's SMTP service is enabled.
		TLS	587	
163	smtp.163.com	SSL	465/994	- The email must have SMTP service enabled. - The password must use an Authorization Password; the email login password is invalid.  Authorization password: The authorization password obtained when the SMTP service is enabled for the email.
		TLS	25	
		None	25	
Sina	smtp.sina.com	SSL	465	The email must have SMTP service enabled.
		None	25	
126	smtp.126.com	None	25	The email must have SMTP service enabled.

Step 4 Click **Apply**.

8.3.6 Setting UPnP

Establish a mapping relationship between the local area and wide area networks using the UPnP (Universal Plug and Play) protocol. This function enables you to access local area devices through wide area IP address.

Prerequisites

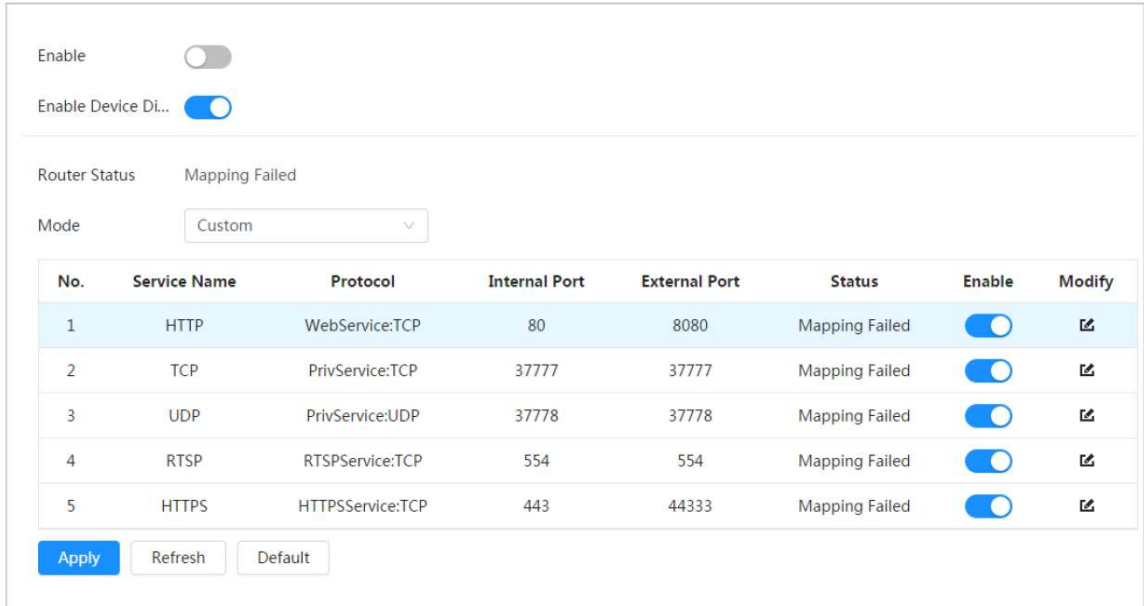
- Make sure the UPnP service is installed in the system.
- Log in the router, and configure WAN IP address to set up external connection.
- Enable UPnP in the router.
- Connect the device to the router's LAN (Local Area Network) port to access the private network.
- At the upper right corner of the page, click  and select **Network > TCP/IP** to set the local area IP address of the router, or select **DHCP** to automatically obtain an IP address.

Procedure

- Step 1 At the upper right corner of the page, click  and select **Network > UPnP**.
- Step 2 Click  next to **Enable**.

- Step 3 Select the mode and the corresponding service name. You can select from **Custom** and **Default**.
- **Custom:** Click  to modify corresponding external port number.
 - **Default:** The system finishes mapping with unoccupied port automatically, and you cannot edit mapping relation.
 - Select **Enable Device Discovery** to support discovering the device through the **Network Neighborhood** on the PC, with the device name being the serial number.

Figure 8-28 UPnP



Enable ☐

Enable Device Di... ☒

Router Status Mapping Failed

Mode Custom

No.	Service Name	Protocol	Internal Port	External Port	Status	Enable	Modify
1	HTTP	WebService:TCP	80	8080	Mapping Failed	☒	
2	TCP	PrivService:TCP	37777	37777	Mapping Failed	☒	
3	UDP	PrivService:UDP	37778	37778	Mapping Failed	☒	
4	RTSP	RTSPService:TCP	554	554	Mapping Failed	☒	
5	HTTPS	HTTPSService:TCP	443	44333	Mapping Failed	☒	

Apply Refresh Default

- Step 4 Click **Apply**.
- Open web browser on PC, enter http:// wide area IP address: external port number, and then you can visit the local area device with corresponding port.

8.3.7 Setting SNMP

SNMP (Simple Network Management Protocol), which can be used to enable software such as MIB Builder and MG-SOFT MIB Browser to connect to the camera and manage and monitor the camera.

Prerequisites

- Install monitoring and managing tools of SNMP such as MIB Builder and MG-SOFT MIB Browser.
- Get the MIB file of the matched version from technical support.

Procedure

- Step 1 At the upper right corner of the page, click  and select **Network > SNMP**.
- Step 2 Select SNMP version to enable SNMP.
- Select **V1**, and the system can only process information of V1 version.
 - Select **V2**, and the system can only process information of V2 version.
 - Select **V3**(recommended). You can set username, password and authentication type. It requires corresponding username, password and authentication type to visit your device from the server. And then V1 and V2 become unavailable
- Step 3 Set the parameters. Enter the IP address of the PC where the MG-SOFT MIB Browser software is installed for the **Trap address**, and keep the other configurations as default.

Figure 8-29 SNMP

Version ☐ V1 ☐ V2 ☒ V3(Recommended)

SNMP Port (1-65535)

Read Community

Write Community

Trap Address

Trap Port (1-65535)

☒ Send Keep-alive Packet Period sec (60-300)

Read-Only User...

Authentication Type ☒ MD5 ☐ SHA

Authentication P...

Encryption Type ☒ CBC-DES

Encryption Passw...

Read/Write User...

Authentication Type ☒ MD5 ☐ SHA

Authentication P...

Encryption Type ☒ CBC-DES

Encryption Passw...

Table 8-18 Description of SNMP parameters

Parameter	Description
SNMP Port	The listening port of the software agent in the device.
Read Community, Write Community	The read and write community string that the software agent supports.  The name can only consist of numbers, letters, underscores, and hyphens.
Trap Address	The target address of the Trap information sent by the software agent in the device.
Trap Port	The target port of the Trap information sent by the software agent in the device.
Send Keep-alive Packet	Select the checkbox, and then set the period. During the configured period, the system checks whether the camera is online.
Read-only Username	Set the read-only username accessing device, and it is public by default. Logging into the device with this username only supports read-only function.

Parameter	Description
	 The name can only consist of numbers, letters and underscores.
Read/Write Username	Set the read/write username access device, and it is private by default. Logging into the device with this username supports only read and write function.  The name can only consist of numbers, letters and underscores.
Authentication Type	You can select from MD5 and SHA . The default type is MD5 .
Authentication Password	It should be no less than 8 digits.
Encryption Type	The default is CBC-DES .
Encryption Password	It should be no less than 8 digits.

Step 4 Click **Apply**.

Result

View device configuration through MIB Builder or MG-SOFT MIB Browser.

1. Run MIB Builder and MG-SOFT MIB Browser.
2. Compile the two MIB files with MIB Builder.
3. Load the compiled module into the MG-SOFT MIB Browser software.
4. Enter the IP address of the device you need to manage in the MG-SOFT MIB Browser, and then select version to search.
5. Unfold all the tree lists displayed in the MG-SOFT MIB Browser.
6. Obtain the configuration information of the device, such as the number of video channels, the number of audio channels, the version number of the program, etc.



Use PC with Windows and disable SNMP Trap service. The MG-SOFT MIB Browser will display prompt when alarm is triggered.

8.3.8 Setting Bonjour

After setting up the Bonjour (zero-configuration networking), operating systems and clients that support Bonjour will automatically detect the device. You can quickly access the device via the Safari browser. When the device is automatically detected by Bonjour, the displayed name will be the **server name**.

Procedure

- Step 1 At the upper right corner of the page, click  and select **Network > Bonjour**.
- Step 2 Click ☐ next to Enable to set the server name.

Figure 8-30 Bonjour

Step 3 Click **Apply**.

Result

In the OS and clients that support Bonjour, follow the steps below to visit the network camera with Safari browser.

1. Click **Show All Bookmarks** in Safari.
2. Enable **Bonjour**.

The OS or client automatically detects the network cameras with Bonjour enabled in the LAN.

3. Click the camera to visit the corresponding web page.

8.3.9 Setting Multicast

When multiple users are viewing the device video image simultaneously through network, it might fail due to limited bandwidth. You can solve this problem by setting up a multicast IP (224.0.0.0~239.255.255.255) for the camera and adopt the multicast protocol.

Procedure

- Step 1 At the upper right corner of the page, click  and select **Network > Multicast**.
- Step 2 Select the channel.
 - Select 1 in Channel to set the parameters of visible channel.
 - Select 2 in Channel to set the parameters of thermal channel.
- Step 3 Click  next to **Enable** to enter multicast address and port.

Figure 8-31 Multicast

Table 8-19 Description of multicast parameters

Parameter	Description
IP Address	The multicast IP address of Main Stream/Sub Stream is 224.1.2.4 by default, and the range is 224.0.0.0~239.255.255.255.

Parameter	Description
Port	Multicast port, the range is 1025~65500. - Single-channel device The main stream is 40000, the sub stream 1 is 40016, and the sub stream 2 is 40032. - Multi-channel device - Channel 1: The main stream is 40000, the sub stream 1 is 40016, and the sub stream 2 is 40032. - Channel 2: The main stream is 40048, the sub stream 1 is 40064, and the sub stream 2 is 40080. - Channel 3: The main stream is 40096, the sub stream 1 is 40112, and the sub stream 2 is 40128. - Channel 4: The main stream is 40144, the sub stream 1 is 40160, and the sub stream 2 is 40176.

Step 4 Click **Apply**.

Result

- At the upper right corner of the WEB page, click  and select **Local**. Select **RTSP** as **Multicast** in the **Playback Parameters** section.
- Click **Live** on the WEB interface, and you can monitor the video image of the corresponding stream via multicast.

8.3.10 Setting Active Registration

The camera actively registers with the user-specified proxy server, which serves as an intermediary, allowing client software to access the device through the proxy server for previewing and monitoring.

Step 1 At the upper right corner of the page, click  and select **Network > Active Register**.

Step 2 Click ☐ next to Enable.

Step 3 Enter server address, port and sub device ID.

Figure 8-32 Active Register

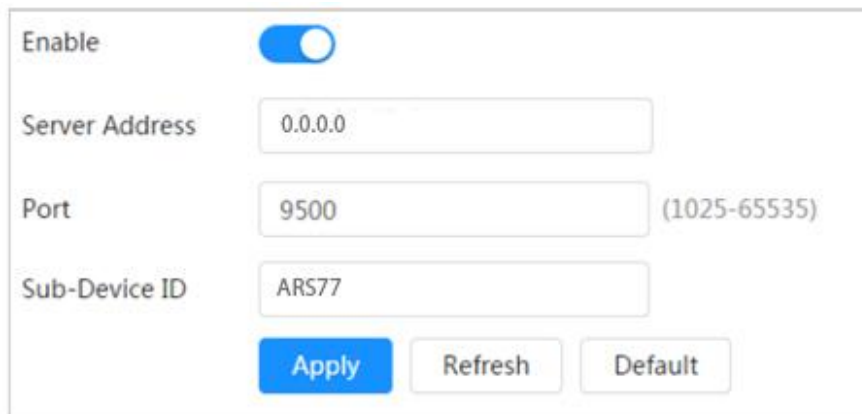


Table 8-20 Description of active register parameters

Parameter	Description
Server Address	The IP address or domain name of the server to be registered.
Port	The port number for registration.

Parameter	Description
Sub-Device ID	The custom ID for the camera.

Step 4 Click **Apply**.

8.3.11 Setting QoS

By implementing QoS (Quality of Service) settings, issues such as network latency and congestion can be addressed. QoS technology enhances service quality by ensuring transmission bandwidth, reducing transmission delay, lowering data packet loss rates, and minimizing delay jitter.

Step 1 At the upper right corner of the page, click  and select **Network > QoS**.

Step 2 Set the parameters.

Figure 8-33 QoS

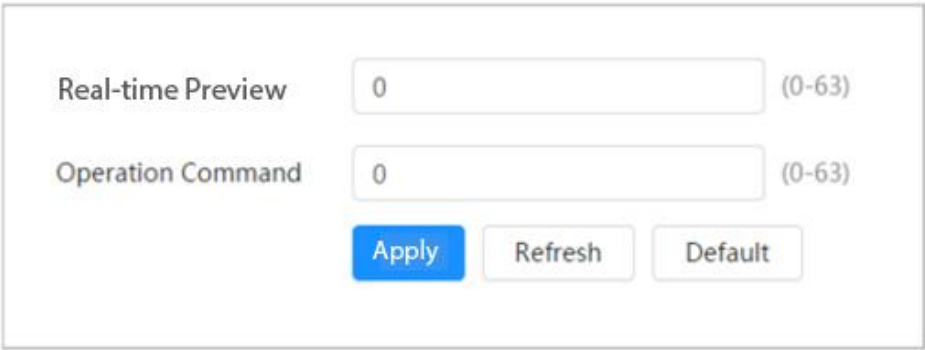


Table 8-21 Description of QoS parameters

Parameter	Description
Real-time Preview	Configure the priority of the data packets that used for network preview. 0 for the lowest and 63 the highest.
Operation Command	Set the priority for non-preview data packets such as device configuration and query, with a range of values from 0 to 63. 0 for the lowest and 63 for the highest.

Step 3 Click **Apply**.

8.3.12 Platform Access

8.3.12.1 Setting National Standard Access.

The device supports access to servers that comply with the National Standards GB/T 28181 protocol or GB/T 35114 protocol (some devices support simultaneous access to two servers). Once connected successfully, real-time monitoring, alarm control, and other operations can be carried out through the server.



- GB/T 28181 Configuration 1 refers to the GB/T 28181 Access configuration in the upper half of the WEB interface, while GB/T 28181 Configuration 2 refers to the GB/T 28181 Access configuration in the lower half of the WEB interface.
- When the device is upgraded from a version that supports single GB access to a version that supports dual GB access, the original GB configuration is synchronized to GB/T 28181 Configuration 1.
- When the device is upgraded from a version that supports dual national standards access to a version that supports only single national standard access, only National Standard 28181 Configuration 1 will be retained.
- Before setting the National Standard 35114, please ensure that all required certificates have been uploaded. For a detailed introduction to the management of national standard certificates, please refer to "8.3.12.2 Management of National Standard Certificates".

Step 1 At the upper right corner of the page, click  and select **Network > Platform Access > National Standard Access**.

Step 2 Select **National Standard 28181 Access** or **National Standard 35114 Access** to set the parameters.

- You can enable two **National Standard Access** functions simultaneously.
- Generally, you only need to set two parameters of SIP Server IP and Device Number. Other parameters should remain consistent with the interfacing device or server side.



Please fill in the parameter settings on this page according to the information provided by the platform during actual use. All parameters must be set correctly; otherwise, you may experience issues such as device registration failure or unresponsive functions.

Figure 8-34 National standard access

Table 8-22 Description of national standard access parameters

Parameter	Description
SIP Server Number	Server platform number, default is 34020000002000000001.
SIP Domain	Server platform domain name identifier, default is 3402000000.

Parameter	Description
SIP Server IP	Server IP, for example, the connected server IP is 192.168.1.112.
SIP Server Port	Server port, default is 5060.
Device Number	The platform assigns a unique number to each device, with each device's number being unique.
SIP Server Password	Default is 12345678.
Device SIP Port	Default is 5060.
Registration Validity Period	Default is 3600. Unit: day.
Heartbeat Cycle	The keep-alive time between the device and the server is set to 60 by default, with the unit being seconds.
Maximum Heartbeat Timeout Count	Count the number of times the device and server exceed the heartbeat timeout. Once this count is exceeded, the device will actively disconnect from communication with the server. The default value is 3 times.
Administrative Division Code	Default is 340200.
Access Module ID	Different values represent the ways in which devices communicate with the server, which are generally agreed upon values between the device side and the server side.
Channel Information	- Channel Type: Select the channel type. 1 for visible light channel; 2 for thermal imaging channel, with the default set to 1. - Channel Number: The default is 34020000001310000001. - Alarm Level: Select the alarm level, with the default set to 1.
Alarm Information	- Alarm Type: Select the alarm type, with the default set to Alarm 1. - Channel Number: The default is 34020000001340000001. - Alarm Level: Select the alarm level, with the default set to 1.

Step 3 Click **Apply**.

The national standard 35114 function requires cooperation with a password module (such as a Micro SD card). If the function is abnormal after activation, please check if the Micro SD card is properly inserted.

8.3.12.2 Managing National Standard Certificate

The National Standard Certificate Management interface supports certificate requests, certificate imports, and certificate management. When the user selects access to National Standard 35114, a certificate request is created through the device, and a request file is downloaded to issue a device certificate from the CA (Certificate Authority).

Prerequisites

- When logging into the WEB interface for the first time, the system prompts to install a plugin. Please follow the instructions to download and install the plugin, and then generate the certificate request and upload the certificate. Otherwise, certificate generation and upload will not be supported.
- The relevant certificates are ready.
 - CA Certificate: The certificate of the Certificate Authority (CA) itself (such as the root CA certificate or sub-CA certificate), used for the trusted validation of other certificates.
 - Local Device Certificate: Generated based on the device number. It is used for the

authentication of the local device, and the corresponding private key is used for VKEK (Video Key Encryption Key) decryption and video signatures.

- ◇ Remote Device Certificate: The server device certificate, used for the authentication of remote devices and the verification of video signatures.
- ◇ User Certificate: Used for user authentication when logging into the web.
- ◇ CRL (Certificate Revocation List): A file that contains the serial numbers and revocation dates of the certificates that have been revoked by the Certificate Authority (CA).

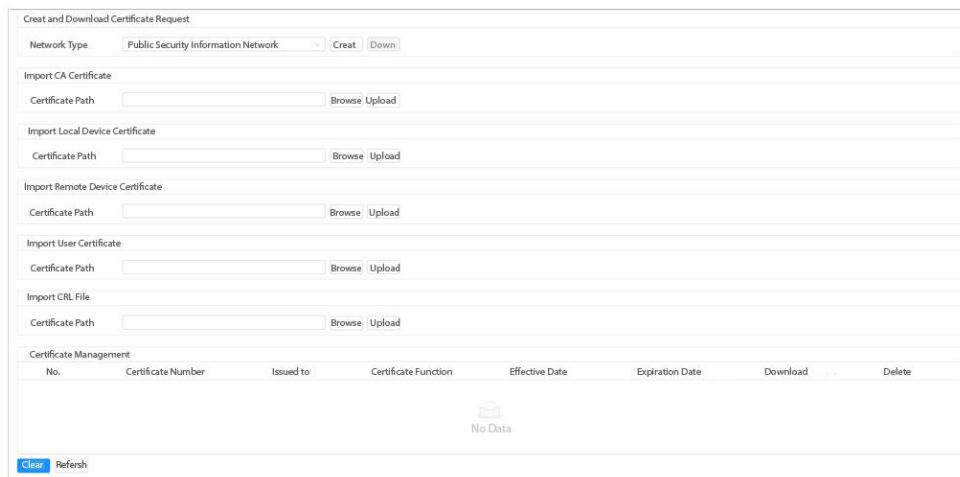


In general, when the certificate authority returns the device identity certificate, it will also provide the CA certificate and the CRL file. If these are not provided, please download them from the certificate authority's website.

Procedure

- Step 1 At the upper right corner of the page, click  and select **Network > Platform Access > Manage National Standard Certificate**.
- Step 2 Create and download a certificate.
1. Select network type.
Support selecting the Public Security Information Network or the Video Private Network.
 - Public Security Information Network: A network specifically established by public security authorities for work-related needs.
 - Video Private Network: A dedicated network established to ensure network bandwidth and the smoothness of video transmission.
 2. Click **Create** to create corresponding certificate request.
The system prompt **Creation successful** indicates that the certificate request has been successfully created.
 3. Click **Download** to download the certificate request to local.

Figure 8-35 Manage national standard certificate



- Step 3 Import the CA certificate, local device certificate, remote device certificate, user certificate, and CRL file in order.



- Please prioritize importing the CA certificate.
- Ensure that the local device certificate number matches the device number entered in “8.3.12.1 Setting the National Standard Access”.
- User certificates need to be generated using a USB security token. Please contact the vendor to obtain the USB security token.

1. Click **Browse**.
2. In the pop-up **Open** dialog, select the certificate you want to upload and click **Open**.
3. Click Upload.

The system prompts **Upload Successful**, and the uploaded certificate is displayed in the certificate list.

Step 4 After all the required certificates have been successfully imported, enable the national standard access feature through the National Standard Access interface. For detailed, please refer to “8.3.12.1 Setting National Standard Access”.

Related Operations

- Check the certificate.
View all the imported certificates in the certificate list.
- Download the certificate.
Click  to download the uploaded certificates.
- Delete the certificate.
Click  to delete uploaded certificates.



- If you need to delete or clear the certificates, please first disable the **GB/T 35114 Access** function in **National Standard Access** interface. After deleting the certificates, you need to upload new certificates; otherwise, the GB/T 35114 Access cannot be enabled.
- If the CA root certificate is deleted, the validation of other certificates will be affected. In this case, you need to re-upload the CA root certificate.

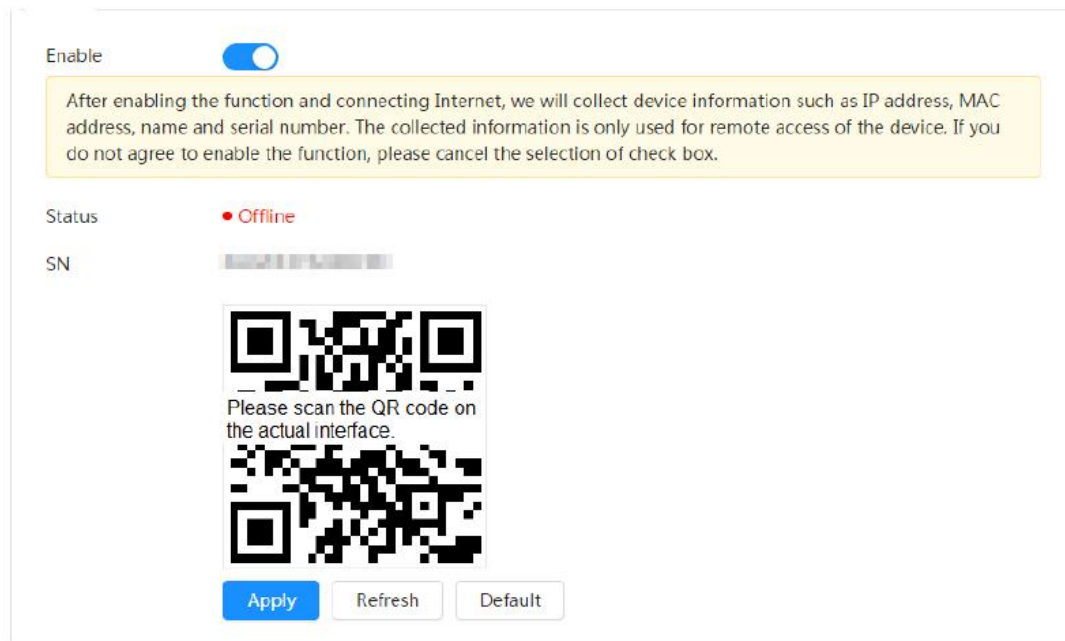
8.3.12.3 Setting P2P

P2P (peer-to-peer) technology enables users to manage devices easily without requiring DDNS, port mapping or transit server. Scan the QR code with your smart phone, and then you can add and manage more devices on the mobile phone client.

Step 1 At the upper right corner of the page, click  and select **Network > Platform Access > P2P**.

- P2P (Peer-to-Peer) is enabled by default, allowing users to remotely manage the device.
- When P2P is enabled and the device accesses to the network, the status shows online. The information of the IP address, MAC address, device name, and device SN will be collected. The collected information is for remote access only. You can cancel Enable selection to reject the collection.

Figure 8-36 P2P



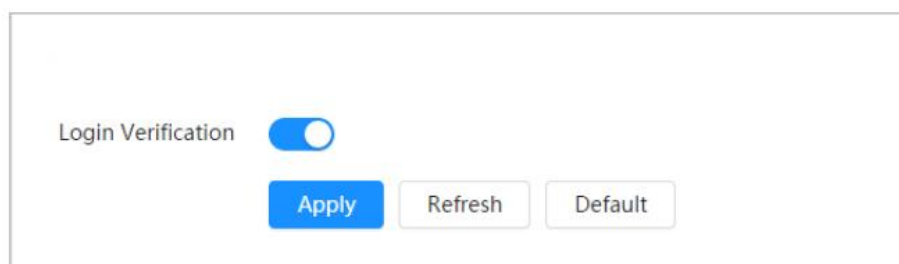
- Step 2 Select **Device Management** on mobile client.
- Step 3 Click "+" at the upper right corner of the page.
- Step 4 Scan the QR code on the **P2P** page.
- Step 5 Follow the instructions to finish the settings.

8.3.12.4 Setting ONVIF

Enable ONVIF, allowing the device to communicate with network video products from other manufacturers (including front-end cameras, recording devices, etc.) through the ONVIF protocol.

- Step 1 At the upper right corner of the page, click  and select **Network > Basic Service**.
- Step 2 Select **ONVIF** to enable this service.
- Step 3 At the upper right corner of the page, click  and select **Network > Platform Access > ONVIF**.
- Step 4 Select **Login Verification** to enable this function.

Figure 8-37 ONVIF



- Step 5 Click **Apply**.

8.3.12.5 Setting RTMP

Through RTMP, you can access a third-party platform (such as Ali and) to realize video live view.

- RTMP can be configured by admin only.
- RTMP supports the H.264, H.264 B and H.264H video formats, and the AAC audio format only.

- Step 1 At the upper right corner of the page, click  and select **Network > Platform Access >**

RTMP.

Step 2 Click  to enable **RTMP**.



Make sure that the IP address is trustable when enabling RTMP.

Step 3 Select the channel.

- Select 1 in Channel to set the parameters of visible channel.
- Select 2 in Channel to set the parameters of thermal channel.

Step 4 Set the parameters.

Figure 8-38 RTMP

The figure shows a configuration window for RTMP. It includes a toggle switch for 'Enable', a dropdown for 'Channel' (set to 1), radio buttons for 'Stream Type' (Main Stream selected) and 'Address Type' (Non-custom selected). Below these are input fields for 'IP Address' (0.0.0.0), 'Port' (1935), and 'Custom Address'. At the bottom are three buttons: 'Apply' (highlighted in blue), 'Refresh', and 'Default'.

Table 8-23 RTMP

Parameter	Description
Stream Type	The stream type for live view. Make sure that the video format is H.264, H.264 B and H.264H, and the audio format is AAC.
Address Type	Including Non-custom and Custom • Non-custom: Enter the server IP and domain name. • Custom: Enter the path allocated by the server.
IP Address	When selecting Non-custom , you need to enter server IP address and port.
Port	• IP address: Support IPv4 or domain name. • Port: Keep the default value.
Custom Address	When selecting Custom , you need to enter the path allocated by the server.

Step 5 Click **Apply**.

8.3.13 Setting Basic Service

Set up basic system services to ensure the security management of the system.

Step 1 At the upper right corner of the page, click  and select **Network > Basic Service**.

Step 2 Enable the basic service according to the actual needs.

Figure 8-43 Basic service

SSH ☐

Multicast/Broadcast Search ☒

CGI ☒

ONVIF ☒

Genetec ☒

Mobile Push Notification ☒

Private Protocol ☒

Private Protocol Authentication Mode

RTSP Login Mode

LLDP ☐

TLSv1.1 ☐

Table 8-24 Description of basic service parameters

Function	Description
SSH	It is disabled by default. You can enable SSH (Secure Shell) authentication to achieve secure management.
Multicast/Broadcast Search	Enabled by default, it supports users to search for devices using multicast/broadcast protocols.
CGI	The device supports interoperability with other video products through this protocol. CGI: Common Gateway Interface.
ONVIF	
Genetec Service	Disabled by default. The Genetec protocol supports access to the Genetec platform.
Mobile Push Notification	Enabled by default, the alarm snapshots triggered by the device are pushed to the mobile end, such as the DMSS client.
Private Protocol	Enabled by default.
Private Protocol Authentication Mode	Select the authentication mode from Security Mode and Compatible Mode .

Function	Description
RTSP Login Mode	You can set the authentication mode for the media stream to ensure the security of data during the transmission of the streaming media. • Digest: Digest Authentication. • None: No Authentication. • Basic: Basic Authentication.
LLDP	Link Layer Discovery Protocol. After enabling LLDP (Link Layer Discovery Protocol), in cloud O&M system, the camera sends the IP addresses to the App for operation and maintenance management and fault diagnosis.  It is recommended to disable the LLDP service. If the service is enabled, the device may have security risks.
TLSv1.1	After enabling TLSv1.1, you can access the camera through TLSv1.1.

Step 3 Click **Apply**.

8.4 Storage Management

Displays information of the local SD card. You can set it as read only or read & write; you can also hot swap and format SD card and set password. Different devices support different functions so please refer to the actual interface.



If the password is entered incorrectly five times in a row during authentication, password modification, or password clearing operations, a wait of 5 minutes is required before unlocking can be attempted again.

Procedure

- Step 1 At the upper right corner of the page, click  and select **Storage Management**.
- Step 2 Select the SD card you need to set, and do the following steps according to actual needs.
- Click **Read-Only**, and then the SD card is set to read only.
 - Click **Read & Write**, and then the SD card is set to read & write.
 - Click **Hot Swap**, and then you can pull out the SD card.
 - Click **Format**, and you can format the SD card.
Click **OK** in the pop-up dialog box to confirm the formatting.
 - Click **Encrypt** to set a password for the SD card.
 - Click **Authenticate**, enter the password for the SD card, and authenticate the unrecognized SD card.
 - Click **Change Password** to modify the password of the SD card.
 - Click **Clear Password** to clear the password of the SD card.

Figure 8-44 Local storage

Format	Read-Only	Read/Write	Hot Swap	Refresh
☒ Name	Status	Properties	Used Space/Total Space	
☒ Local Disk1	Normal	Read/Write		25.86GB / 118.92GB
				General Config

8.5 System Management

Introduce the basic settings of the system, date and time, user management, maintenance

management, and peripheral management operations.

Two methods are available to access **System Management** interface. The subsequent content in this chapter will use the button entry  from the upper right corner as an example.

- Click **System Management** at the page WEB.
- On the upper right corner of the page, click  and select **System Management**.

8.5.1 General

8.5.1.1 Setting Basic Parameters

Set the device name and the video format.

Step 1 At the upper right corner of the page, click  and select **System Management > General > Basic**.

Step 2 Set the parameters.

Figure 8-45 Basic

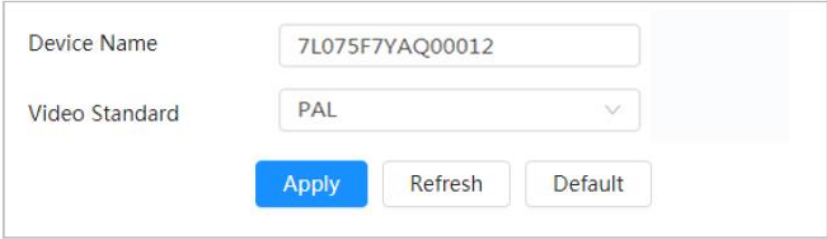


Table 8-25 Description of basic settings

Parameter	Description
Device Name	Set the device name. When the device is searched and added by other devices, the displayed name will be the device name that you have set.  Different devices have different names.
Video Format	Select the video format of the video.

Step 3 Click **Apply**.

8.5.1.2 Setting Date

Set the date and time format, time zone, system time, enable daylight saving time, set the NTP (Network Time Protocol) server, or set GPS time synchronization.

Step 1 At the upper right corner of the page, click  and select **System Management > General > Date**.

Step 2 Set the parameters.

Figure 8-46 Setting date

Table 8-26 Description of date and time parameters

Parameter	Description
Time Setting	Select time setting.
System Time	When Time Setting is set to Manual , set the current system time of the device here. Click Sync with PC to adjust the system time based on the PC time.
Server	When Time Setting is set to NTP , you can enable the NTP server network time synchronization function. Set the IP or domain name of the PC with the installed NTP server, the port number, and the update cycle to configure the network time synchronization with the server.
Port	
Update Cycle	
Time Format	Set the display format for date and time.
Time Zone	Set the time zone that the camera is at.
DST	When the device's location observes DST, DST needs to be enabled. Click next to Enable and set the start and end times for DST based on date or week.
Type	
Start Time	
End Time	

Step 3 Click **Apply**.

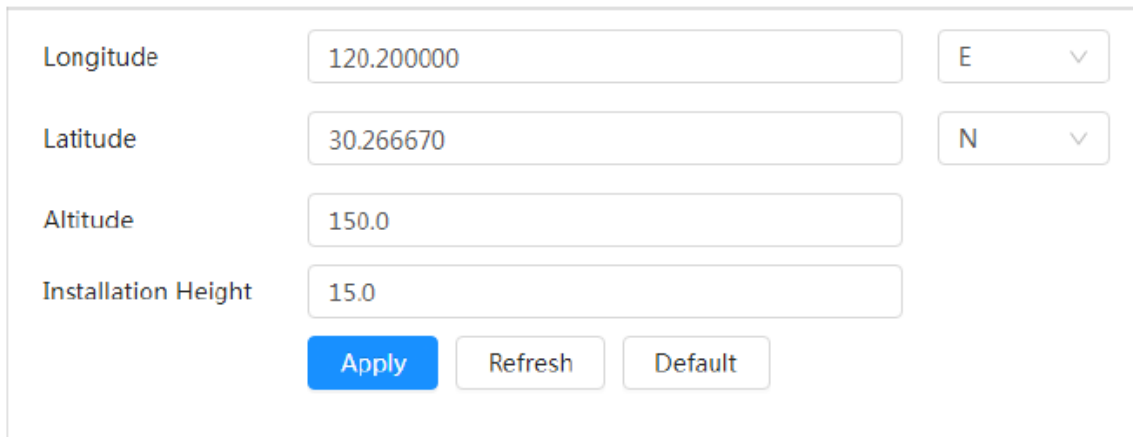
8.5.1.3 Setting Positioning System

Set the device's longitude, latitude, and altitude based on the installation location.

Step 1 At the upper right corner of the page, click  and select System Management > General > Positioning System.

Step 2 Fill in the longitude, latitude, altitude, and camera installation height.

Figure 8-47 Sett positioning system



Longitude	120.200000	E
Latitude	30.266670	N
Altitude	150.0	
Installation Height	15.0	

Buttons: Apply, Refresh, Default

Step 3 Click **Apply**.

8.5.2 User Management

Manage system users, including adding users, deleting users, or modifying user information. System users include admin, added users, and ONVIF users.

User management operations, including adding users or user groups, deleting users or user groups, and modifying user information, can only be performed when the user has user management permissions.

- You can add 18 users (excluding the admin user) and 1 anonymous user, as well as add 6 user groups (excluding the admin and user groups).
- User management is implemented using a two-level structure of user groups and users. Group names must be unique, usernames must be unique, a user can only belong to one group, and a user's permissions can only be a subset of the permissions assigned to that group.
- The currently logged-in user cannot modify their own permissions.
- The default user of the system is admin, who is assigned the highest permissions by default upon factory settings.
- Select **Anonymous Login** and enter the IP to access the WEB interface without needing a username and password, thereby logging into the device anonymously. Users logging in anonymously only have preview permissions as listed in the permissions list. While in anonymous login mode, click  **admin** in the upper right corner of the interface and select **Logout** to log in to the device with another user.

8.5.2.1 Adding User

You are admin user by default. You can add users, and set different authorities.

Procedure

Step 1 At the upper right corner of the page, click  and select **System Management > User**

Management > User.

Step 2 Click **Add**.

Step 3 Add user information.

Figure 8-48 Enter user information(system permission)

The screenshot shows a web-based 'Add' user dialog box. At the top, there's a title bar with 'Add' and a close button. Below it, the form contains several input fields: 'Username' with the value 'user', 'Password' and 'Confirm Password' both masked with dots and a green progress bar below the password field, and a 'Group' dropdown menu set to 'admin'. A 'Remarks' text area is also present. Below these fields are four tabs: 'System' (selected), 'Live', 'Search', and 'Restricted Login'. Under the 'System' tab, there's a list of permissions, each with a checked checkbox: 'All', 'Account', 'Manual Control', 'Event', 'Camera', 'Maintenance', 'System', 'File Backup', 'Network', 'PTZ', 'System Info', 'Storage', 'Peripheral', and 'Security'. At the bottom right, there are 'Apply' and 'Cancel' buttons.

System	Live	Search	Restricted Login
☒ All			
☒ Account		☒ System	☒ System Info
☒ Manual Control		☒ File Backup	☒ Storage
☒ Event		☒ Network	☒ Peripheral
☒ Camera		☒ PTZ	☒ Security
☒ Maintenance			

Figure 8-49 Add user(Restricted Login)

Table 8-27 Description of user parameters

Parameter	Description
Username	User's unique identification. You cannot use existed user name. The username can be up to 31 characters long and can consist of numbers, letters, underscores, hyphens, dots, and the @ symbol.
Password	Enter password and confirm it again.
Confirm Password	The password must be set to a non-empty string of 8 to 32 characters, consisting of at least two of the following three types: numbers, letters, and special characters (excluding '"', "'", ',', '.', and '&'). Please follow the password strength guidelines to set a high-security password.
Group	The group that users belong to. Each group has different authorities.
Remark	Describes the user.
System	Select permissions as needed.  It is recommended to give fewer permissions to normal users than premium users.
Live	Select the live view permission to be enabled.
Playback	Select the playback permissions of recordings and capture images to be enabled.

Parameter	Description
Restricted Login	Set the PC address that allows the defined user to log in to the camera and the validity period and time range. You can log in to web with the defined IP in the defined time range of validity period. • IP address: You can log in to web through the PC with the set IP. • Validity period: You can log in to web in the set validity period. • Time Range: You can log in to web in the set time range. Set as following: 1. Select IP Address, choose the IP type, and set the IP address. • IP Address: Enter the IP address of the host to be added. • IP segment: Enter the start address and end address of the host to be added. 2. Select Validity Period, and then set the start time and end time. 3. Select Period, and then click Time Plan to set the period that allows login. For details, see Step4 in "5.1.1.2.1 Adding Arming Schedule".

Step 4 Click Apply.

The newly added user is displayed in the user name list.

Related Operations

- Edit user information

Click  to modify the password of the added user, the group the user belongs to, notes, system settings, live and playback permissions, and login restrictions, and other information.



For admin user, you can only change the password.

- Delete user information

Click  to delete the added users.



Admin user cannot be deleted.

8.5.2.2 Resetting Password

Step 1 At the upper right corner of the page, click  and select System Management > User Management > User.

Step 2 Click  next to **Enable**.

If the function is not enabled, you can only reset the password by resetting the camera.

Step 3 Set the reserved mobile phone number and password update cycle.

Once the setup is successful, you can reset your password through Forgot Password on the device login interface.

Figure 8-50 Reset password

Step 4 Click **Apply**.

8.5.2.3 Adding User Group

You have two groups named admin and user by default, and you can add new group, and modify user group permissions and remarks.

Procedure

- Step 1 At the upper right corner of the page, click  and select **System Management > User Management > User Group**.
- Step 2 Click **Add**.
- Step 3 Enter the user group name and remarks, and select the system, live, and playback permissions for the user group.
The length of the user group name can be up to 31 characters, consisting of numbers, letters, underscores, hyphens, periods, and @.

Figure 8-51 Add user group

- Step 4 Click **Apply**.
The newly added group displays in the group name list.

Related Operations

- Edit user group information
Click  to modify the remarks and permissions of user group.
- Delete user group

Click  to delete added user group.



The admin group and user group cannot be deleted.

8.5.2.4 Adding ONVIF User

You can add, delete ONVIF user, and change their passwords.

Procedure

- Step 1 At the upper right corner of the page, click  and select **System Management > User Management > ONVIF User**.
- Step 2 Click **Add**.
- Step 3 Set the parameters.

Figure 8-52 Add users (ONVIF)

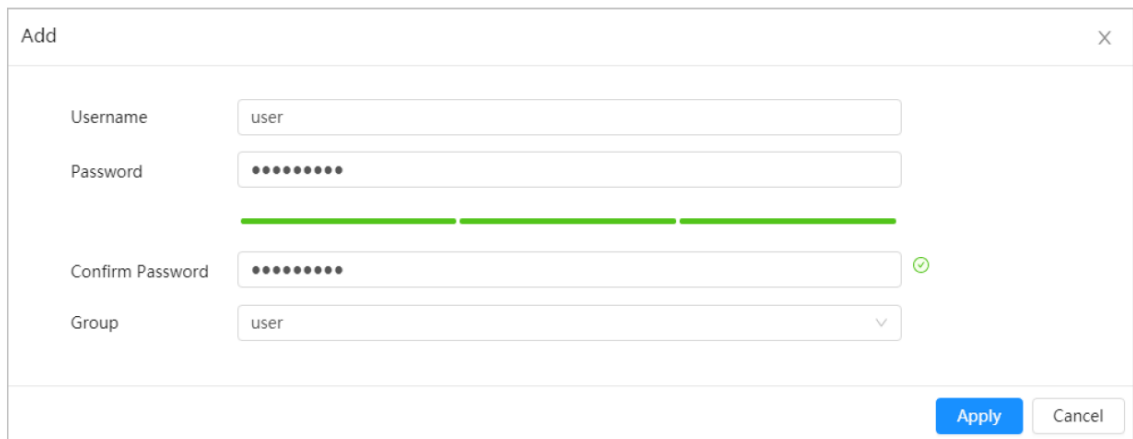


Table 8-28 Description of ONVIF user parameters

Parameter	Description
Username	User's unique identification. You cannot use existed username. The length of the username can be up to 31 characters, consisting of numbers, letters, underscores, hyphens, periods, and @.
Password	The user's password and confirmation password must match. The password must be 8 to 32 characters long and cannot be empty. It must consist of at least two types from the three categories: numbers, letters, and special characters (excluding '"', "'", ',', '.', and '&'). Please set a strong password based on the password strength suggestions.
Confirm Password	
Group Name	The group that users belong to. Each group has different authorities.

- Step 4 Click Apply.

The newly added user displays in the username list.

Related Operations

- Edit user information

Click  to modify the password and the group the added user belong to.



For admin account, you can only change the password.

- Delete user information

Click  to delete added users.



The admin account cannot be deleted.

8.5.3 System Upgrade

Enhance device functions and improve stability through system upgrades.



If wrong upgrade file has been used, restart the device; otherwise some functions might not work properly.

Step 1 At the upper right corner of the page, click  and select **System Management > System Upgrade**.

Step 2 Select upgrade type according actual needs.

- File Upgrade

The upgrade file is of type *.bin. Click **Browse** to import the local upgrade file, then click **Upgrade** to start the firmware upgrade.

- Online upgrade

A new version has been detected through automatic or manual detection. Click **Upgrade Now** to upgrade the system.

- ◇ Auto detection: The system will check for updates automatically once a day and will prompt you when there is a system update available.



To ensure you are promptly notified about firmware updates, we will collect device information such as the device IP address, device name, firmware version, and device serial number. The collected information will only be used to verify the device's legitimacy and to send upgrade notifications.

- ◇ Manual detection: Check for system updates manually.

8.5.4 Viewing System Information

You can view the information, including version, log and online user, and back up or clear log.

8.5.4.1 Version

View system hardware specifications, software version, WEB version, and other version information.

At the upper right corner of the page, click  and select **System Information > Version** to check version information.

8.5.4.2 Online User

View the information of the currently logged-in WEB user.

At the upper right corner of the page, click  and select **System Information > Online User > Online User** to check online user information; Select **System Information > Online User > Platform User** to check platform user information.

8.5.4.3 Legal Information

The legal information to be reviewed includes the software license agreement, privacy policy, and open source software declaration.

At the upper right corner of the page, click  and select **System Information > Legal Information** to check corresponding content in different tabs.

8.5.5 Log

8.5.5.1 System Log

View and back up the system log information.

Background Information

Logs include system operations, data management, alarm events, recording operations, user management, and security center.

- **System:** Includes program start, abnormal close, close, program reboot, device closedown, device reboot, system reboot, and system upgrade.
- **Data:** Includes configuring disk type, clearing data, hot swap, FTP state, and record mode.
- **Event** (records events such as video detection, smart plan, alarm and abnormality): includes event start and event end.
- **Record:** Includes file access, file access error, and file search.
- **Account:** Includes login, logout, adding user, deleting user, editing user, adding group, deleting group, and editing group.
- **Security:** Includes password resetting and IP filter.

Procedure

- Step 1 At the upper right corner of the page, click  and select **System Log > Log**.
- Step 2 Set the start and end time, and select the log types.
The start time can be no earlier than January 1, 2000, and the end time can be no later than December 31, 2037. The log types include system operations, configuration operations, data management, alarm events, recording operations, user management, and security center.
- Step 3 Click **Search**.
- Click each log or  to view log information in **Detailed Information**.
 - Click **Backup**, and then you can back up all found logs to local PC. Select **Log Backup Encryption** to encrypt the backup logs.

Figure 8-57 Log

Start time		2024-03-18 10:41:08	2024-03-19 10:41:08	Type	All	Search
Backup		☐ Log Backup Encryption				
26	2024-03-18 12:11:24	admin	Logout			
27	2024-03-18 11:39:24	admin	Login			
28	2024-03-18 11:32:29	System	Certificate			
29	2024-03-18 11:32:29	System	Certificate			
30	2024-03-18 11:32:29	System	Certificate			
31	2024-03-18 11:32:29	System	Certificate			
32	2024-03-18 11:32:29	System	Certificate			
33	2024-03-18 11:32:29	System	Certificate			
34	2024-03-18 11:31:46	System	Program Start			
35	2024-03-18 11:27:03	admin	Save			
36	2024-03-18 11:27:00	admin	Save			
37	2024-03-18 11:25:58	admin	Save			
38	2024-03-18 11:25:38	admin	Save			
39	2024-03-18 11:24:20	admin	Save			
40	2024-03-18 11:23:46	admin	Save			
41	2024-03-18 11:23:46	admin	Save			
42	2024-03-18 11:23:46	admin	Save			

72 records

8.5.5.2 Remote Log

Configure remote log, and you can get the related log by accessing the set address.

- Step 1 At the upper right corner of the page, click  and select **System Log > Remote Log**.
- Step 2 Click ☐ next to **Enable**.
- Step 3 Set server address, port and device number.

Figure 8-58 Remote log

Enable ☒

Server Address

Port (1-65534)

Device No. (0-23)

EnableTLS ☐

RTSP stream is encrypted by using TLS tunnel before transmission.

Apply

Refresh

Default

- Step 4 Click **Apply**.

8.6 Maintenance

8.6.1 Maintenance Requirements

To ensure the system operates normally and securely, it is recommended to perform system management, backup, and maintenance operations as follows.

- Regularly check the monitoring screens of the devices.
- Regularly clean up unused users and user groups.
- Change user passwords every three months. For detailed instructions on changing passwords, please refer to "8.5.2 User Management".
- Regularly review and analyze system logs, and promptly address any anomalies.
- Regularly back up the system configuration.
- Regularly restart the system and delete old files.
- Promptly upgrade the firmware.

8.6.2 Device Maintenance

Support manual system restart, set the scheduled time for automatic system restart and automatic deletion of old files, with this feature turned off by default.

Step 1 At the upper right corner of the page, click  and select **O&M Center > Maintenance Management**.

Step 2 Set the parameters.

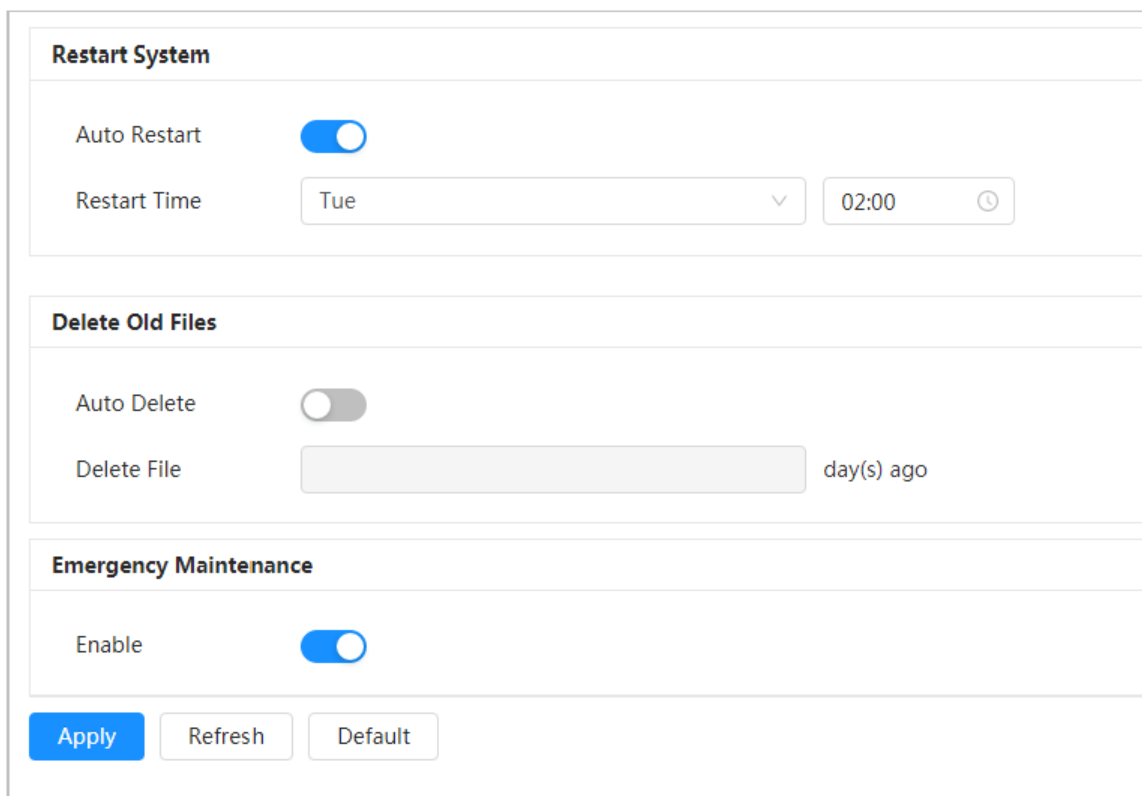
- In the **Restart System** section, click  next to **Automatic Restart**, set the restart time, and the system will automatically restart according to the set time each week.
- In the **Delete Old Files** section, click  next to **Automatic Deletion**, and the system will delete old files based on the customized time, with a range from 1 day to 31 days ago.



Files deleted using the **Automatic Deletion** feature cannot be recovered, please proceed with caution.

- Emergency maintenance
AOL enabled, and you can use the diagnostic tool to fix it.

Figure 8-55 Device maintenance



Restart System	
Auto Restart	☒
Restart Time	Tue 02:00

Delete Old Files	
Auto Delete	☐
Delete File	day(s) ago

Emergency Maintenance	
Enable	☒

Apply Refresh Default

Step 3 Click **Apply**.

8.6.3 Backup and Restore

8.6.3.1 Backup Information

Backup the device's configuration information by exporting the device configuration file.

Step 1 At the upper right corner of the page, click  and select **System Management > Maintenance > Configuration Maintenance**.

Step 2 Click **Export Configuration File**.

The configuration file is saved to the browser's default download location.

8.6.3.2 Restore Configuration Information.

Import a configuration file to quickly configure device information or restore device configuration information.

Step 1 At the upper right corner of the page, click  and select **System Management > Maintenance > Configuration Maintenance**.

Step 2 Click **Select File** to choose the local configuration file.

Step 3 Click **Import File**.

Import the locally backed-up configuration file into the system.

8.6.3.3 Restore to Default

Restore the device to default configuration or factory settings.



Restoring default settings or factory settings will erase device-related information. Please proceed with caution.

At the upper right corner of the page, click  and select **System Management > Maintenance > Restore to Default**.

- Click **Restore to Default** to restore all configurations except for the network IP address, user management, and other related information.
- Click **Factory Defaults** to restore device configurations to factory settings.

Figure 8-56 Restore to default



9 Security Management

9.1 Scan Security Status

Background Information

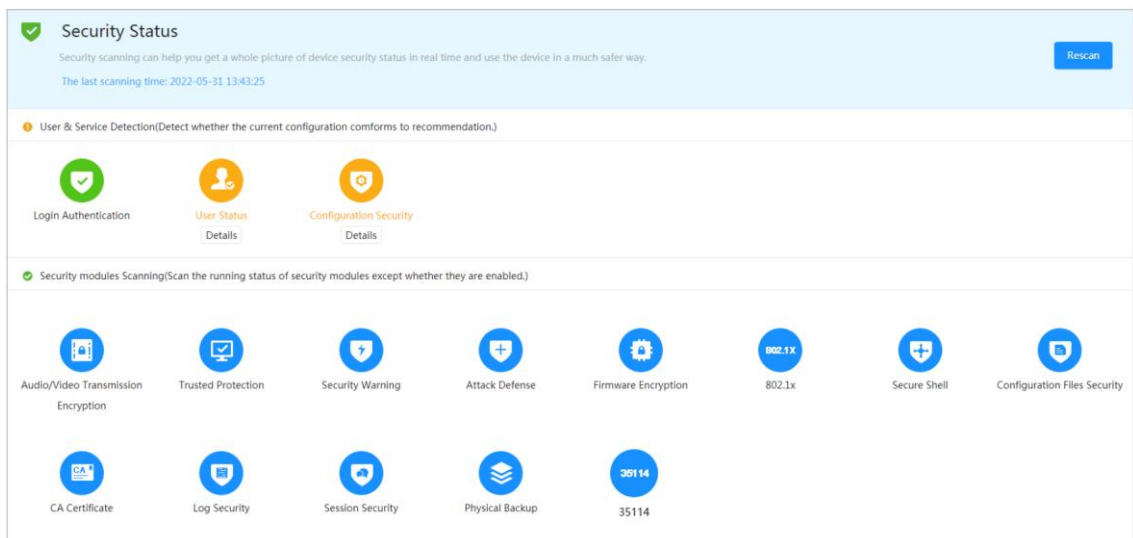
Examine and analyze the current user information, functional configuration, security module features, and other characteristics of the device, providing a comprehensive view of the device's security status to better assist users in strengthening device security.

- User and service detection: Detect login authentication, user status, and configuration security to check whether the current configuration conforms to recommendation.
- Security Module Scan: Detect and check the operating status of security modules such as audio and video transmission encryption, trusted protection, security alerts, attack defense, and firmware encryption, without checking the enabled status.

Procedure

- Step 1 At the WEB page select **Security Center > Security Status**.
- Step 2 Click Rescan to scan the security status of the camera.
During the scanning process, the icon is grayed out. When the icon turns blue, it indicates that the scanning is complete.

Figure 9-1 Security status



Related Operations

After scanning, different results will be displayed with different color. Yellow indicates that the security modules are abnormal, and Green indicates that the security modules are normal.

Click **Details** to view the details of the scanning result.

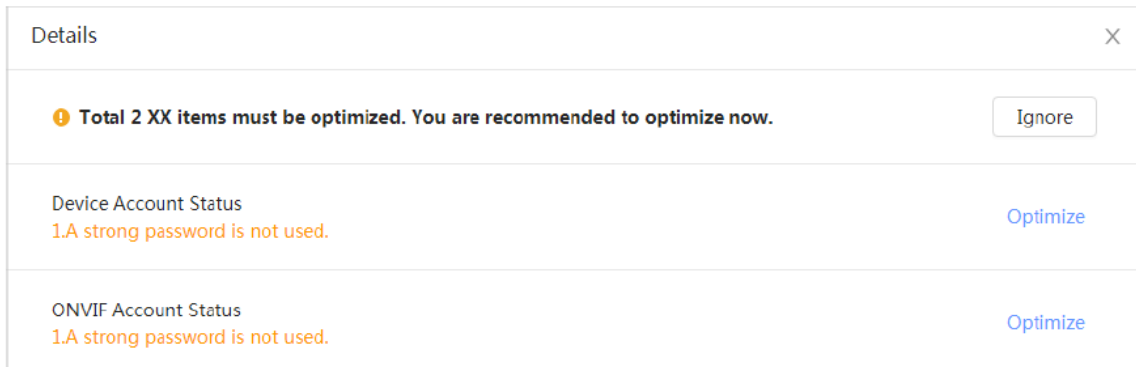
- Click **Ignore** to ignore the exception, and it will not be scanned in next scanning.



In the **Security Status** interface, click **Add to Scan** below the ignored module to re-include the ignored module in the scan content.

- Click **Optimize**, and the corresponding page is displayed, and you can You can modify the abnormal content of this module.

Figure 9-2 Details



9.2 System Service

You can only use the corresponding service functions after enabling the system services.

9.2.1 802.1x

802.1x is a port-based access control and authentication protocol that can restrict unauthorized devices or users from accessing the local area network through the access port. When the switches in the network are configured with 802.1x, devices also need to be configured with 802.1x; otherwise, users will not be able to access the devices through the network.

- Step 1 At the WEB page, select **Security Center > System Service > 802.1x**.
- Step 2 Select the network card name that needs authentication based on the actual situation.
Click ☐ next to **Enable**.
- Step 3 Select the authentication mode and set the corresponding parameters.
 - PEAP: (protected EAP protocol).
 1. Select PEAP as the authentication mode.
 2. Enter the username and password.
You need to enter a username and password that have been authorized on the server side.
 3. (Optional) Select **CA Certificate**, and choose the corresponding certificate from the list on the **Trusted CA Certificates** tab.



If there is no certificate in the list, click Certificate Management at the left navigation bar. For details, see "9.4.2 Installing Trusted CA Certificate".

Figure 9-3 802.1x (PEAP)

802.1x is a network access control protocol which can effectively prevent access from unauthorized hosts.

NIC Name:

Enable: ☐

Authentication Mode:

Username:

Password:

CA Certificate: ☒

Use a trusted CA certificate to verify the validity of peer authentication server (switch or Radius server).

Device Certificate:

Certificate List							Certificate Management
No.	Custom Name	Certificate Serial Number	Validity Period	User	Issued by	Used by	
☐ 1		409-0446-02-00-00-00	2059-05-23 11:05:14	Radius Device Root CA	Radius Device Root CA		
☐ 2		409-0446-02-00-00-00	2049-05-30 13:58:24	Radius Device IPC CA	Radius Device Root CA		

- TLS: Transport Layer Security. It is applied in two communication application programs to guarantee the security and integrity of the data.
 1. Select TLS as the authentication mode.
 2. Enter the username.
 3. Select the corresponding certificate from the list on the **Device Certificate** tab.



If there is no certificate in the list, click Certificate Management at the left navigation bar. For details, see "9.4.2 Installing Trusted CA Certificate".

4. (Optional) Select **CA Certificate** and choose the corresponding certificate from the list on the **Trusted CA Certificates** tab.



If there are no certificates in the list, you need to click **Certificate Management** to import a certificate. For more details, please refer to '9.4.1 Installing Device Certificates'.

Figure 9-4 802.1x (TLS)

802.1x is a network access control protocol which can effectively prevent access from unauthorized hosts.

NIC Name:

Enable: ☐

Authentication Mode:

Username:

CA Certificate: ☒

Device Certificate:

Certificate List							Certificate Management
No.	Custom Name	Certificate Serial Number	Validity Period	User	Issued by	Used by	
☐ 1		409-0446-02-00-00-00	2059-05-23 11:05:14	Radius Device Root CA	Radius Device Root CA		
☐ 2		409-0446-02-00-00-00	2049-05-30 13:58:24	Radius Device IPC CA	Radius Device Root CA		

Step 4 Click Apply.

9.2.2 HTTPS

By creating certificates or uploading signed certificates, PCs can log in via HTTPS properly, ensuring the security of communication data and providing reliable and stable technical means to safeguard user information and device security.



It is recommended to enable the HTTPS service. If this service is disabled, there may be a risk of communication data leakage for the device.

Procedure

- Step 1 At the WEB page, select **Security Center > System Service > HTTPS**.
- Step 2 Click ☐ next to Enable.
- Step 3 Select device certificate.



If there is no certificate in the list, click Certificate Management at the left navigation bar. For details, see “9.4.1 Installing Device Certificate”.

Figure 9-5 HTTPS

No.	Custom Name	Certificate Serial Number	Validity Period	User	Issued by	Used by
1			2054-03-13 10:23:48	9H0701DYAQ00001	Dahua Device TPC CA	HTTPS, RTSP over TLS

- Step 4 Click **Apply**.

Result

Enter “https://IP address” in the browser.

- If the certificate is installed, the normal login interface will be displayed.
- If the certificate is not installed, the browser will display a certificate error.

9.3 Attack Defense

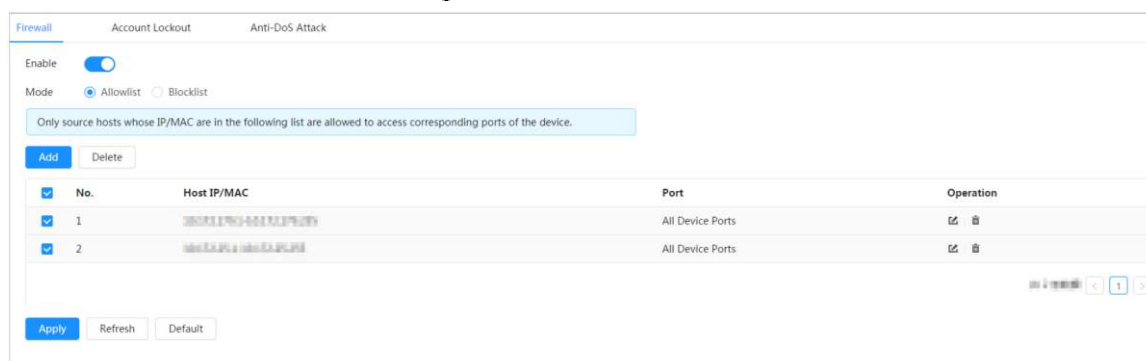
9.3.1 Firewall

Configure firewall to limit access to the camera.

Procedure

- Step 1 At the WEB page, select **Security Center > Attack Defense > Firewall**.
- Step 2 Click ☐ next to **Enable**.

Figure 9-6 Firewall

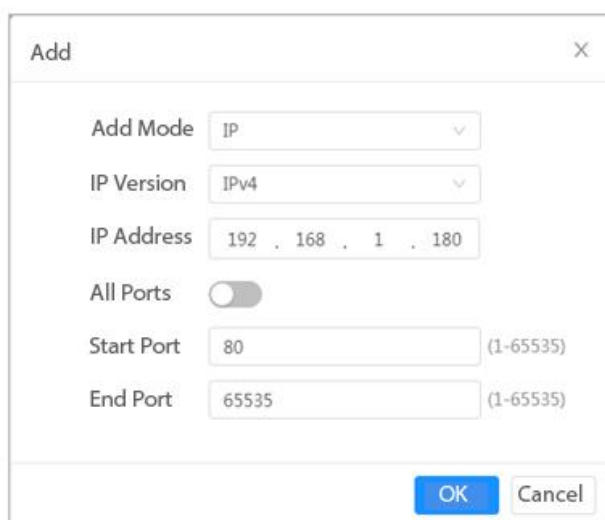


Step 3 Select access mode.

- **Allowlist:** Only when the IP/MAC of your PC in the allow list, can you access the camera. If ports are set simultaneously, users can only access the configured ports.
- **Blocklist:** When the IP/MAC of your PC is in the block list, you cannot access the camera. If ports are set simultaneously, users will not be able to access the specified ports of the device.

Step 4 Click **Add** to add the host IP/MAC address to **Allowlist** or **Blocklist**, and then click **Apply**.

Figure 9-7 Add allowlist/blocklist



Step 5 Click **Apply**.

Related operations

- Edit
Click to edit host information.
- Delete
Click to delete host information.

9.3.2 Account Lockout

If you consecutively enter a wrong password more than the configured value, the account will be locked.

Step 1 At the WEB page, select **Security Center > Attack Defense > Account Lockout**.

Step 2 Configure the login attempt and lock time for device account and ONVIF users.

- Login attempt: Upper limit of login attempts. If you consecutively enter a wrong password more than the configured value, the account will be locked.

- Lock time: The period during which you cannot login after the login attempts reaches upper limit.

Figure 9-8 Account lockout

Firewall **Account Lockout** Anti-DoS Attack

Account

Login Attempts 5

Lock Time 5 min

ONVIF User

Login Attempts 30

Lock Time 5 min

SNMP User

Enable ☐

Login Attempts 30

Lock Time 5 min

Apply Refresh Default

Step 3 Click **Apply**.

9.3.3 Anti-DoS Attack

Defense mode for devices under DoS (Denial of Service) attack.

Step 1 At the WEB page, select **Security Center > Attack Defense > Anti-Dos Attack**.

Step 2 Select to enable the corresponding defense function.

Figure 9-9 Anti-DoS attack

Firewall Account Lockout **Anti-DoS Attack**

SYN Flood Attack Defense ☐

An attacker might send out repeated SYN messages to the device, leaving many half-open TCP connections on the device, which will make the device crash. When hit by an SYN flood attack, the device will defend itself by discarding the first message.

ICMP Flood Attack Defense ☐

An attacker might send out an abnormally large number of ICMP packets to the device, which will use up all computing resources and thus make the device crash. When hit by an ICMP flood attack, the device will defend itself by using the ICMP message filtering tactic.

Apply Refresh Default

Step 3 Click **Apply**.

9.4 CA Certificate

9.4.1 Installing Device Certificate

The device certificate is used to prove the legitimate identity of the device. For example, when a browser accesses the device via HTTPS, it needs to validate the device certificate.

9.4.1.1 Creating Certificate

Create certificate in the device.

Procedure

- Step 1 At the WEB page, select **Security Center > CA Certificate > Device Certificate**.
- Step 2 Click **Install Device Certificate**.
- Step 3 Select **Create Certificate**, and click **Next**.
- Step 4 Enter the certificate information.
IP/Domain: Enter the device's IP address or domain name.

Figure 9-10 Certificate information

Step 2: Fill in certificate information.

Custom Name

* IP/Domain Na...

Organization U...

Organization

* Validity Perio... Days (1~5000)

* Region

Province

City Name

- Step 5 Click **Create and install certificate**.
After the certificate is created successfully, you can view the created certificate on the **Device Certificate** page.

Related Operations

- Edit certificate name.
Click **Enter Edit Mode**, you can edit the custom name of the certificate.
- Download the certificate.
Click  to download certificate.
- Delete the certificate.

Click  to delete certificate.

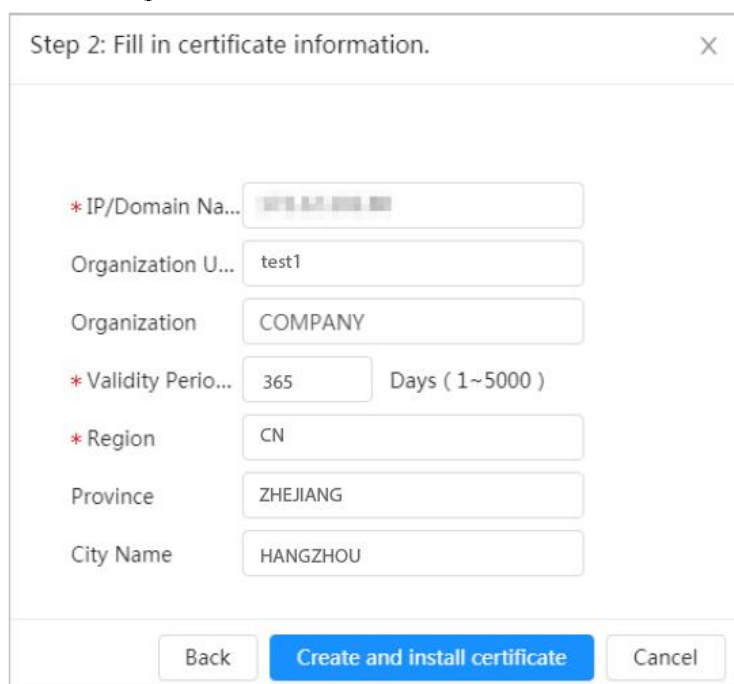
9.4.1.2 Applying for and Importing CA Certificate

Import the third-party CA certificate to the camera.

Procedure

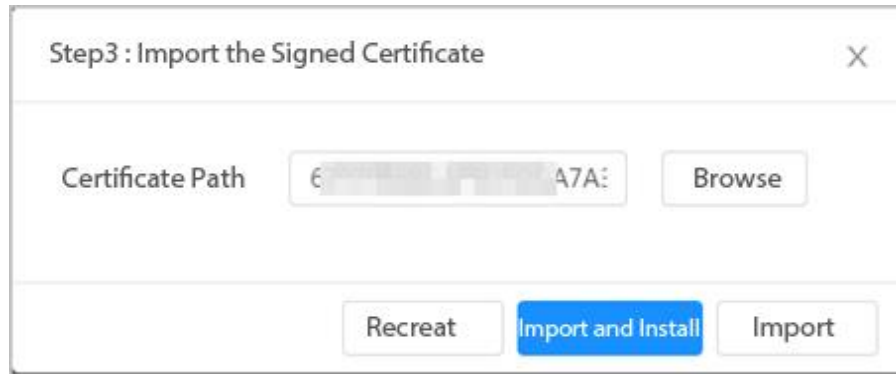
- Step 1 At the WEB page, select **Security Center > CA Certificate > Device Certificate**.
- Step 2 Click **Install Device Certificate**.
- Step 3 Select **Apply for CA Certificate and Import (Recommended)**, and click **Next**.
- Step 4 Enter the certificate information.
IP/Domain: Enter the device's IP address or domain name

Figure 9-11 Certificate information



- Step 5 Click **Create and Download**.
Save the request file to your PC.
- Step 6 Apply the CA certificate from the third-party certificate authority.
- Step 7 Import the signed CA certificate.
 - 1. Save the CA certificate to the PC.
 - 2. Click **Install Device Certificate**, select **Apply for CA Certificate and Import (Recommended)**, and click **Next**.
 - 3. Click **Browse** and select the signed device certificate.

Figure 9-12 Import the signed certificate



4. Click **Import and Install**.

After creation, you can view the created certificates in the **Device Certificate** interface.

- Click **Recreate** to create the request file again.
- Click **Import Later** to import the certificate next time.

Related Operations

- Edit certificate name.
Click **Enter Edit Mode**, you can edit the custom name of the certificate.
- Download the certificate
Click  to download the certificate.
- Delete the certificate.
Click  to delete the certificate.

9.4.1.3 Importing the Third-party Certificate

Import the obtained third-party certificate to the device. When applying for a third-party certificate, you need to request both the private key file and the private key password.

Procedure

- Step 1 At the WEB page, select **Security Center > CA Certificate > Device Certificate**.
- Step 2 Click **Install Device Certificate**.
- Step 3 Select **Install Existing Certificate**, and click **Next**.
- Step 4 Click **Browse** to select the certificate and private key file.
When the private key file is encrypted, you also need to enter the private key password.

Figure 9-13 Certificate and private key

Step 2: Select certificate and private key. X

Certificate Path test.cer Browse

Private Key PrivateKey.jks Browse

Private Key Passw... ●●●●●

Previous Import and Install Cancel

Step 5 Click **Import and Install**.

After the certificate is created successfully, you can view the created certificate on the **Device Certificate** page.

Related Operations

- Edit certificate name.
Click **Enter Edit Mode**, you can edit the custom name of the certificate.
- Download the certificate.
Click  to download certificate file.
- Delete the certificate.
Click  to delete the certificate file.

9.4.2 Installing Trusted CA Certificate

Trusted CA certificate is a digital certificate for the legal identity of the camera. For example, when the camera accesses the LAN through 802.1x, the CA certificate is required.

Procedure

- Step 1 At the WEB page, select Security Center > CA Certificate > Trusted CA Certificate.
- Step 2 Click **Install Trusted Certificate**.

Figure 9-14 Install trust certificate

Device Certificate Trusted CA Certificate

Trusted CA certificate is a digital certificate for the legal identity of the camera. For example, when the camera accesses the LAN through 802.1x, the CA certificate is required.

Install trusted certificate [Enter Edit Mode](#)

No.	Custom Name	Certificate No.	Validity Period	User	Issued by	Operations	Certificate Status	Download	Delete
1		4	2049-06-13 10:57:59	General Device 1 PC CA	General Device Root CA		Normal		
2		6	2059-05-23 11:18:27	General Device Root CA	General Device Root CA		Normal		
3		4	2059-05-23 11:05:14	Dahua Device Root CA	Dahua Device Root CA		Normal		
4		4	2049-05-30 13:58:24	Dahua Device IP C CA	Dahua Device Root CA		Normal		

Step 3 In the pop-up dialog box, click **Browse**, select the certificate file, and click **OK** to import the trusted CA certificate.

After the import is successful, you can view the imported CA certificate in the **Trusted CA Certificates** interface.

Related Operations

- Edit certificate name.
Click **Enter Edit Mode**, you can edit the custom name of the certificate.
- Download the certificate.
Click to download certificates.
- Delete the certificate.
Click to delete certificate file.

9.5 Key Management

When the device activates the 35114 feature and does not have a key, it needs to request a key from the key server and download and install it.

Step 1 At the WEB page, select **Security Center > Key Management**.

Step 2 Set the parameters.

Figure 9-15 Key management

IP Address

Port

Apply Refresh Default

Table 9-1 Description of key parameters

Parameter	Description
IP Address	IP address of key server.
Port	Port of key server.

Step 3 Click **Apply**.

9.6 A/V Encryption

The device supports audio and video encryption during data transmission.



You are recommended to enable A/V Encryption function. There might be safety risk if this function is disabled.

- Step 1
- At the WEB page, select **Security Center > A/V Encryption**.
- Step 2
- Set the parameters.

Figure 9-16 A/V Encryption

Encrypted Transmission

Private Protocol

Enable ☐

Stream transmission is encrypted by using private protocol.

*Please make sure that the corresponding device or software supports video decryption.

Encryption Type AES256-OFB

Update Period of Se... 12 hr (0-720)

RTSP over TLS

Enable ☐

RTSP stream is encrypted by using TLS tunnel before transmission.

*Please make sure that the corresponding device or software supports video decryption.

*Select a device certificate

No.	Custom Name	Certificate Serial Number	Validity Period	User	Issued by	Used by
1			2052-04-24 20:20:54	7L075F7YAQ00015	test	HTTPS, RTSP over TLS

Certificate Management

Apply Refresh Default

Table 9-2 Description of A/V encryption parameters

Encryption Method	Parameter	Description
Private Protocol	Enable	Use a private protocol for the encrypted transmission of audio and video frames. Click ☐ next to Enable . Enable encrypted transmission of audio and video, select Encryption Method , and set the Key Update Interval . - Encryption method: Use default value. - Key update interval: The range is 0 to 720 hours, where 0 means that the key will never be updated.
	Certificate Management	Create or import device certificates. For more details, please refer to '9.4.1 Installing Device Certificates'. The created or imported certificates will be displayed in the Select Device Certificate list, where you can select a certificate from the list.

- Step 3
- Click **Apply**.

9.7 Security Warning

Security warnings help you monitor the security status of your devices in real time. When security

exception event is detected, the camera sends a warning to remind you to process it timely, to avoid security risk.

Step 1 At the WEB page, select **Security Center > Security Warning**.

Step 2 Click ☐ next to Enable.

Figure 9-17 Security warning

Enable ☒

Event Monitoring

☒ Invalid executable programs attempting to run	☒ Session ID bruteforcing
☒ Web directory bruteforcing	☒ Login not in the specified time range.
☒ Number of session connections exceeds limit	☒ Brute force attack of the account.

Security warning can detect device security status in real time, and keep you informed of the security exception events immediately, so that you can deal with them timely and avoid security risks.

+Event Linkage

Alarm-out Port | Enabled

Alarm Channel

Post-alarm sec (3-300)

Step 3 Click **Event Linkage** to add linkage actions and set the linkage parameters. For more details, please refer to “5.1.1.2 Alarm Linkage”.

Step 4 Click **Apply**.