



Network Camera Web 5.0

Operation Manual







Foreword

General

This manual introduces the functions, configuration, general operation, and system maintenance of network camera.

Safety Instructions

The following categorized signal words with defined meaning might appear in the manual.

Signal Words	Meaning
 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, may 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.

Revision History

Version	Revision Content	Release Date
V1.0.0	First release.	September 2020

About the Manual

- The manual is for reference only. If there is inconsistency between the manual and the actual product, the actual product shall prevail.
- We are not liable for any loss caused by the operations that do not comply with the manual.
- The manual would be updated according to the latest laws and regulations of related jurisdictions. For detailed information, refer to the paper manual, CD-ROM, QR code or our official website. If there is inconsistency between paper manual and the electronic version, the electronic version shall prevail.
- All the designs and software are subject to change without prior written notice. The product updates might cause some differences between the actual product and the manual. Please contact the customer service for the latest program and supplementary documentation.
- There still might be deviation in technical data, functions and operations description, or errors in print. If there is any doubt or dispute, we reserve the right of final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and the company names in the manual are the properties of their respective owners.
- Please visit our website, contact the supplier or customer service if there is any problem occurring when using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Important Safeguards and Warnings

Electrical Safety

- All installation and operation shall conform to your local electrical safety codes.
- The power source shall conform to the Safety Extra Low Voltage (SELV) standard, and supply power with rated voltage which conforms to Limited Power Source requirement according to IEC60950-1. Note that the power supply requirement is subject to the device label.
- Make sure that the power supply is correct before operating the device.
- A readily accessible disconnecting device shall be incorporated in the building installation wiring.
- Prevent the power cable from being trampled or pressed, especially the plug, power socket and the junction extruded from the device.

Environment

- Do not aim the device at strong light to focus, such as lamp light and sun light; otherwise it might cause over brightness or light marks, which are not the device malfunction, and affect the longevity of Complementary Metal-Oxide Semiconductor (CMOS).
- Do not place the device in a damp, dusty, extremely hot or cold environment, or the locations with strong electromagnetic radiation or unstable lighting.
- Keep the device away from any liquid to avoid damage to the internal components.
- Keep the indoor device away from rain or damp to avoid fire or lightning.
- Keep sound ventilation to avoid heat accumulation.
- Transport, use and store the device within the range of allowed humidity and temperature.
- Heavy stress, violent vibration or water splash are not allowed during transportation, storage and installation.
- Pack the device with standard factory packaging or the equivalent material when transporting the device.
- Install the device in the location where only the professional staff with relevant knowledge of safety guards and warnings can access. The accidental injury might happen to the non-professionals who enter the installation area when the device is operating normally.

Operation and Daily Maintenance

- Do not touch the heat dissipation component of the device to avoid scald.
- Carefully follow the instructions in the manual when performing any disassembly operation about the device; otherwise, it might cause water leakage or poor image quality due to unprofessional disassembly. Please contact after-sale service for desiccant replacement if there is condensed fog on the lens after unpacking or when the desiccant turns green. (Not all models are included with the desiccant).
- It is recommended to use the device together with lightning arrester to improve lightning protection effect.
- It is recommended to ground the device to enhance reliability.
- Do not touch the image sensor (CMOS) directly. Dust and dirt could be removed with air blower, or you can wipe the lens gently with soft cloth that is moistened with alcohol.
- You can clean the device body with soft dry cloth, and for stubborn stains, use the cloth with

mild detergent. To avoid possible damage on device body coating which could cause performance to decrease, do not use volatile solvent such as alcohol, benzene, diluent and so on to clean the device body, nor can strong, abrasive detergent be used.

- Dome cover is an optical component. Do not touch or wipe the cover with your hands directly during installation or operation. For removing dust, grease or fingerprints, wipe gently with moistened oil-free cotton with diethyl or moisten soft cloth. You can also remove dust with an air blower.

**WARNING**

- Strengthen the protection of network, device data and personal information by adopting measures which include but not limited to using strong password, changing password regularly, upgrading firmware to the latest version, and isolating computer network. For some device with old firmware versions, the ONVIF password will not be modified automatically along with the modification of the system password, and you need to upgrade the firmware or manually update the ONVIF password.
- Use standard components or accessories provided by manufacturer and make sure that the device is installed and maintained by professional engineers.
- The surface of the image sensor should not be exposed to laser beam radiation in an environment where a laser beam device is used.
- Do not provide two or more power supply sources for the device unless otherwise specified. A failure to follow this instruction might cause damage to the device.

Table of Contents

Foreword	I
Important Safeguards and Warnings	II
1 Overview	1
1.1 Introduction	1
1.2 Network Connection	1
1.3 Function	1
1.3.1 Basic Function	1
1.3.2 AI Function	2
2 Configuration Flow	4
3 Device Initialization	5
4 Login	9
4.1 Device Login	9
4.2 Resetting Password	10
5 Main Interface	12
6 Setting	13
6.1 Local	13
6.2 Camera	14
6.2.1 Setting Image Parameters	14
6.2.1.1 Interface Layout	14
6.2.1.2 Image	16
6.2.1.3 Exposure	17
6.2.1.4 Backlight	19
6.2.1.5 WB	20
6.2.1.6 Day/Night	20
6.2.1.7 Illuminator	21
6.2.1.8 Defog	22
6.2.2 Setting Encode Parameters	23
6.2.2.1 Encode	23
6.2.2.2 Overlay	25
6.2.2.2.1 Configuring Privacy Masking	25
6.2.2.2.2 Configuring Channel Title	26
6.2.2.2.3 Configuring Time Title	27
6.2.2.2.4 Configuring Location	27
6.2.2.2.5 Configuring Font Properties	28
6.2.2.2.6 Configuring Picture Overlay	28
6.2.2.2.7 Configuring Custom Title	28
6.2.2.2.8 Configuring Target Statistics	29

6.2.2.2.9 Configuring Face Detection	30
6.2.2.2.10 Configuring Face Recognition.....	30
6.2.2.2.11 Configuring Face Statistics.....	31
6.2.2.3 ROI.....	31
6.2.3 Setting Audio Parameters.....	32
6.3 Network	33
6.3.1 TCP/IP.....	33
6.3.2 Port	36
6.3.3 PPPoE	38
6.3.4 DDNS	38
6.3.5 Email.....	39
6.3.6 UPnP.....	42
6.3.7 SNMP.....	43
6.3.8 Bonjour	46
6.3.9 Multicast.....	46
6.3.10 Register.....	47
6.3.11 QoS.....	47
6.3.12 Platform Access.....	48
6.3.12.1 P2P	48
6.3.12.2 ONVIF.....	49
6.3.12.3 RTMP.....	49
6.3.13 Basic Service.....	50
6.4 Event.....	52
6.4.1 Setting Alarm Linkage.....	52
6.4.1.1 Setting Alarm-in	52
6.4.1.2 Alarm Linkage	53
6.4.1.2.1 Adding Schedule	53
6.4.1.2.2 Record Linkage	54
6.4.1.2.3 Snapshot Linkage	55
6.4.1.2.4 Alarm-out Linkage.....	55
6.4.1.2.5 Email Linkage	55
6.4.1.3 Subscribing Alarm.....	56
6.4.1.3.1 About Alarm Types	56
6.4.1.3.2 Subscribing Alarm Information	56
6.4.2 Setting Exception.....	57
6.4.2.1 Setting SD Card Exception.....	58
6.4.2.2 Setting Network Exception.....	58
6.4.2.3 Setting Voltage Detection	59
6.4.3 Setting Video Detection	60

6.4.3.1 Setting Motion Detection	60
6.4.3.2 Setting Video Tampering	62
6.4.3.3 Setting Scene Changing	62
6.4.4 Setting Audio Detection	63
6.5 Storage	64
6.6 System	65
6.6.1 General	65
6.6.1.1 Basic	65
6.6.1.2 Date & Time	66
6.6.2 Account	67
6.6.2.1 User	67
6.6.2.1.1 Adding User	67
6.6.2.1.2 Resetting Password	70
6.6.2.2 Adding User Group	71
6.6.2.3 ONVIF User	72
6.6.3 Manager	73
6.6.3.1 Requirements	73
6.6.3.2 Maintenance	73
6.6.3.3 Import/Export	74
6.6.3.4 Default	74
6.6.4 Upgrade	75
6.7 System Information	75
6.7.1 Version	75
6.7.2 Online User	76
6.8 Setting Log	76
6.8.1 Log	76
6.8.2 Remote Log	77
7 Live	78
7.1 Live Interface	78
7.2 Setting Encode	79
7.3 Live View Function Bar	79
7.4 Window Adjustment Bar	80
7.4.1 Adjustment	80
7.4.2 Zoom and Focus	81
7.4.3 Image Adjustment	83
7.5 Display Mode	83
8 AI	85
8.1 Setting Crowd Distribution Map	85
8.1.1 Global Configuration	85

8.1.2 Rule Configuration.....	86
8.2 Setting Face Recognition.....	87
8.2.1 Setting Face Detection.....	88
8.2.2 Setting Face Database.....	90
8.2.2.1 Creating Face Database.....	90
8.2.2.2 Adding Face Picture.....	92
8.2.2.2.1 Single Adding.....	92
8.2.2.2.2 Batch Importing.....	94
8.2.2.3 Managing Face Picture.....	95
8.2.2.3.1 Editing Face Information.....	95
8.2.2.3.2 Deleting Face Picture.....	96
8.2.2.4 Face Modeling.....	96
8.2.2.5 Setting Arm Alarm.....	97
8.2.2.6 Viewing Face Recognition Result.....	98
8.3 Setting Face Detection.....	99
8.4 Setting IVS.....	101
8.4.1 Global Configuration.....	102
8.4.2 Rule Configuration.....	103
8.5 Setting Video Metadata.....	107
8.5.1 Global Configuration.....	107
8.5.2 Rule Configuration.....	108
8.5.3 Viewing Video Metadata Result.....	110
9 Camera.....	112
10 Event.....	113
11 System.....	114
12 Security.....	115
12.1 Security Status.....	115
12.2 System Service.....	116
12.2.1 802.1x.....	116
12.2.2 HTTPS.....	117
12.3 Attack Defense.....	118
12.3.1 Firewall.....	118
12.3.2 Account Lockout.....	119
12.3.3 Anti-DoS Attack.....	119
12.4 CA Certificate.....	120
12.4.1 Installing Device Certificate.....	120
12.4.1.1 Creating Certificate.....	120
12.4.1.2 Applying for and Importing CA Certificate.....	121
12.4.1.3 Installing Existing Certificate.....	122

12.4.2 Installing Trusted CA Certificate	123
12.5 A/V Encryption	124
12.6 Security Warning.....	125
13 Record	126
13.1 Playback.....	126
13.1.1 Playing Back Video.....	126
13.1.2 Clipping Video.....	128
13.1.3 Downloading Video	129
13.2 Setting Record Control.....	130
13.3 Setting Record Plan	131
13.4 Storage	132
13.4.1 Local Storage	133
13.4.2 Network Storage	134
13.4.2.1 FTP	134
13.4.2.2 NAS	135
14 Picture	137
14.1 Playback.....	137
14.1.1 Playing Back Picture	137
14.1.2 Downloading Picture	138
14.2 Setting Snapshot Parameters.....	139
14.3 Setting Snapshot Plan	140
14.4 Storage	140
15 Report	141
Appendix 1 Cybersecurity Recommendations	142

1 Overview

1.1 Introduction

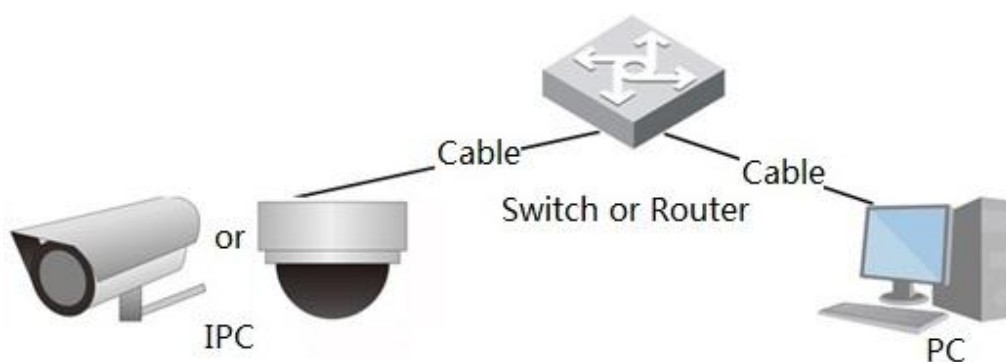
IP camera (Internet Protocol camera), is a type of digital video camera that receives control data and sends image data through internet. They are commonly used for surveillance, requiring no local recording device, but only a local area network.

IP camera is divided into single-channel camera and multi-channel camera according to the channel quantity. For multi-channel camera, you can set the parameters for each channel.

1.2 Network Connection

In the general IPC network topology, IPC is connected to PC through network switch or router.

Figure 1-1 General IPC network



Get IP address by searching on ConfigTool, and then you can start accessing IPC through network.

1.3 Function

Functions might vary with different devices, and the actual product shall prevail.

1.3.1 Basic Function

Real-time Monitoring

- Live view.
- When live viewing the image, you can enable audio, voice talk and connect monitoring center for quick processing on the abnormality.
- Adjust the image to the proper position by PTZ.
- Snapshot and triple snapshot abnormality of the monitoring image for subsequent view and processing.

- Record abnormality of monitoring image for subsequent view and processing.
- Configure coding parameters, and adjust live view image.

Alarm

- Set alarm prompt mode and tone according to alarm type.
- View alarm prompt message.

Exception

- SD card error, network disconnection, illegal access, voltage detection and security exception.
- 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.
- When the input voltage is more or less than the rated voltage, the alarm is triggered and the system links sending email.

Video Detection

- Motion detection, video tampering detection and scene changing detection.
- When an alarm is triggered, the system performs linkages such as recording, alarm output, sending email, PTZ operation, and snapshot.

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, PTZ operation, and snapshot.

Record

- Auto record as schedule.
- Play back recorded video and picture as needed.
- Download recorded video and picture.
- Alarm linked recording.

Account

- Add, edit and delete user group, and manage user authorities according to user group.
- Add, edit and delete user, and configure user authorities.
- Change user password.

1.3.2 AI Function

IVS

- Tripwire, intrusion, abandoned object, moving object, fast moving, parking detection, people gathering, and loitering detection.
- When an alarm is triggered, the system performs linkages such as recording, alarm output, sending email, and snapshot.

Face Detection

- Detect face and display the related attributes on the live interface.
- When an alarm is triggered, the system performs linkages such as recording, alarm output, sending email, PTZ operation, and snapshot.

Face Recognition

- After detecting face, make comparison between the detected face with the face in face database, and activates alarm output.
- Query the recognition result.

Crowd Distribution Map

- View crowd distribution in real time for the timely arm to avoid accidents like stampede.
- When an alarm is triggered, the system performs linkages such as recording, alarm output, sending email, PTZ operation, and snapshot.

Video Metadata

- Capture people, non-motor vehicle and vehicle, and display the related information on the live interface.
- When an alarm is triggered, the system links alarm output.

2 Configuration Flow

For the device configuration flow, see Figure 2-1. For details, see Table 2-1. Configure the device according to the actual situation.

Figure 2-1 Configuration flow

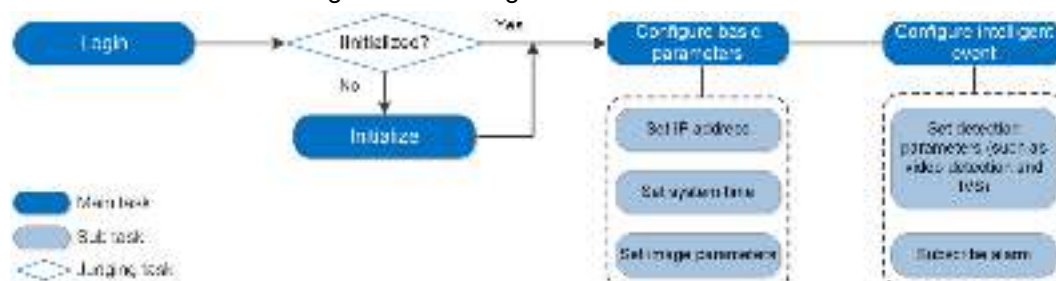


Table 2-1 Description of flow

Configuration		Description	Reference
Login		Open IE browser and enter IP address to log in to the web interface. The camera IP address is 192.168.1.108 by default.	"4 Login".
Initialization		Initialize the camera when you use it for the first time.	"3 Device Initialization"
Basic parameters	Camera Parameters	Configure image parameters, encoder parameters, and audio parameters to ensure the image quality.	"6.2 Camera".
	Date & time	Set date and time to ensure the recording time is correct.	"6.6.1.2 Date & Time"
	IP address	Change IP address according to network planning for the first use or during network adjustment.	"6.3.1 TCP/IP"
	Subscribe alarm	Subscribe alarm event. When the subscribed alarm is triggered, the system will record the alarm on the alarm tab.	"6.4.1.3 Subscribing Alarm"
AI	AI rules	Configure the necessary detection rules, such as face detection and IVS.	"8 AI"

3 Device Initialization

Device initialization is required for the first-time use. This manual is based on the operation on the web interface. You can also initialize device through ConfigTool, NVR, or platform devices.



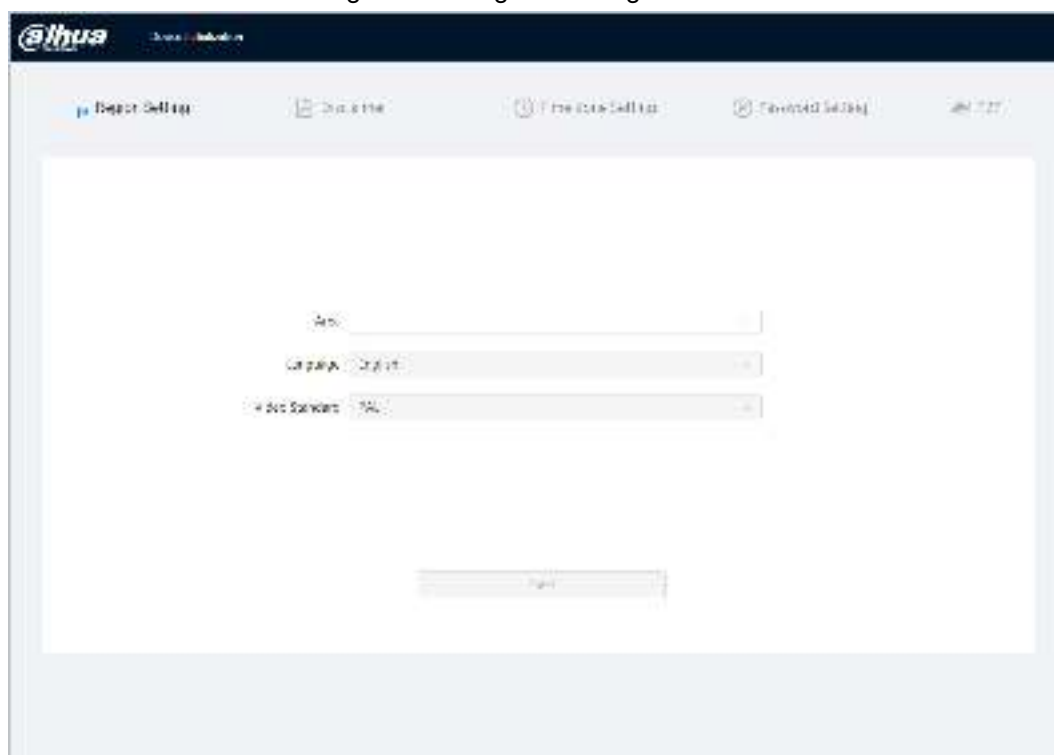
- To ensure the device safety, keep the password properly after initialization and change the password regularly.
- When initializing device, keep the PC IP and device IP in the same network.

Step 1 Open IE browser, enter the IP address of the device in the address bar, and then press the Enter key.



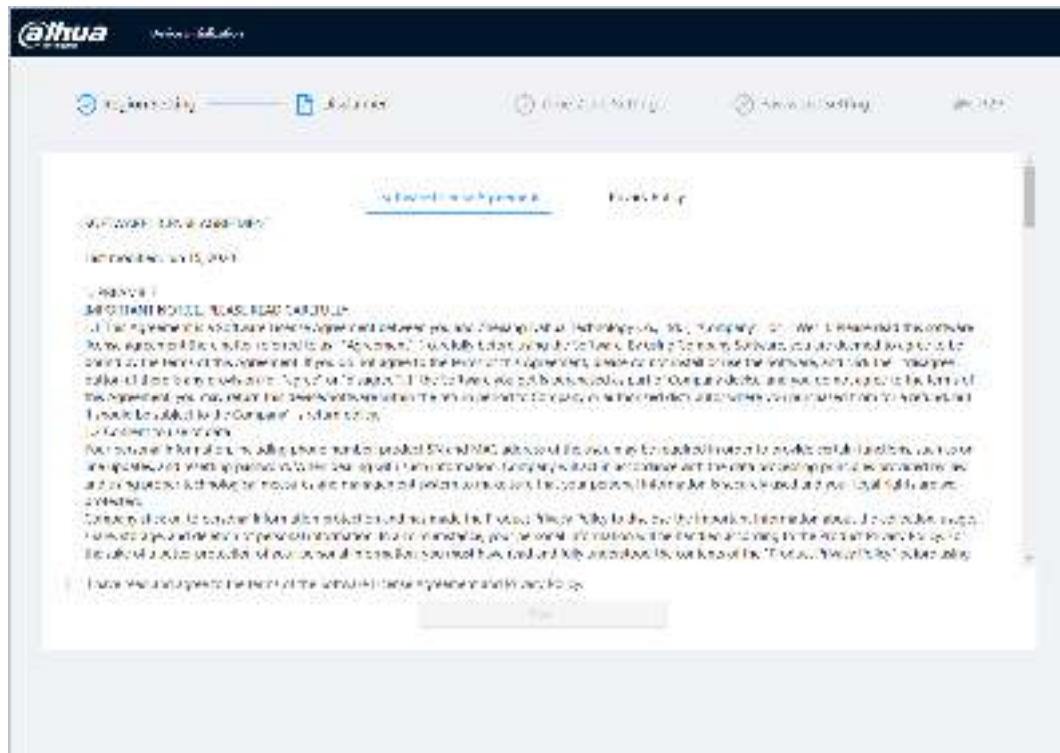
The IP is 192.168.1.108 by default.

Figure 3-1 Region Setting



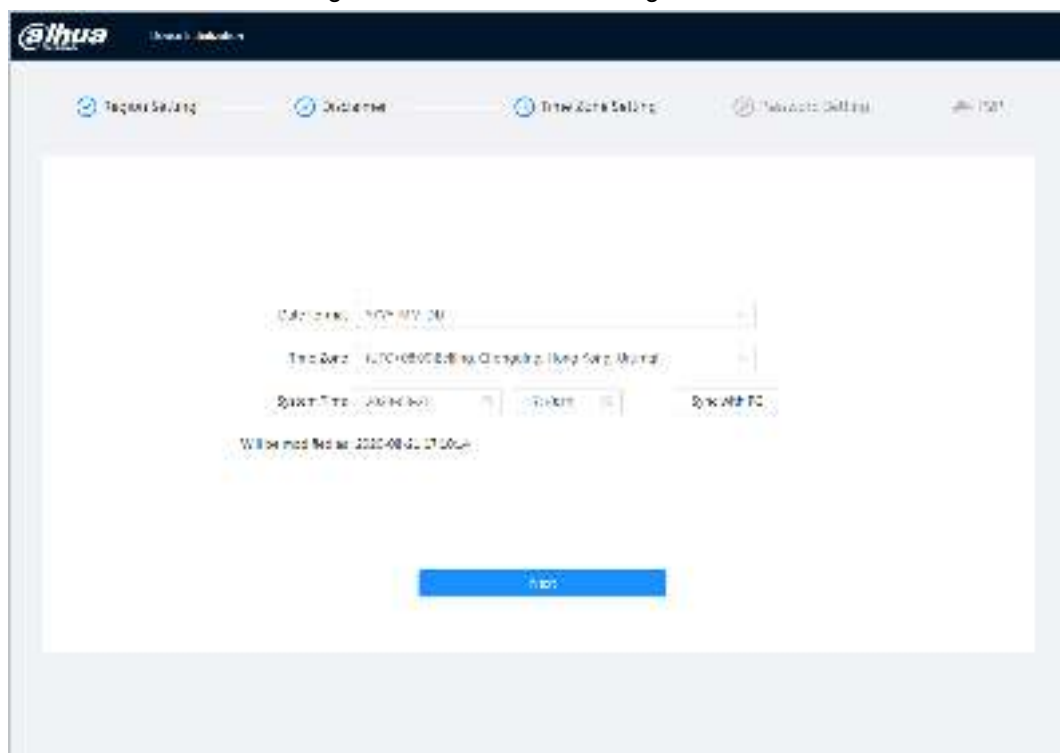
Step 2 Select the area, language, and video standard according to the actual situation, and then click **Next**.

Figure 3-2 Disclaimer



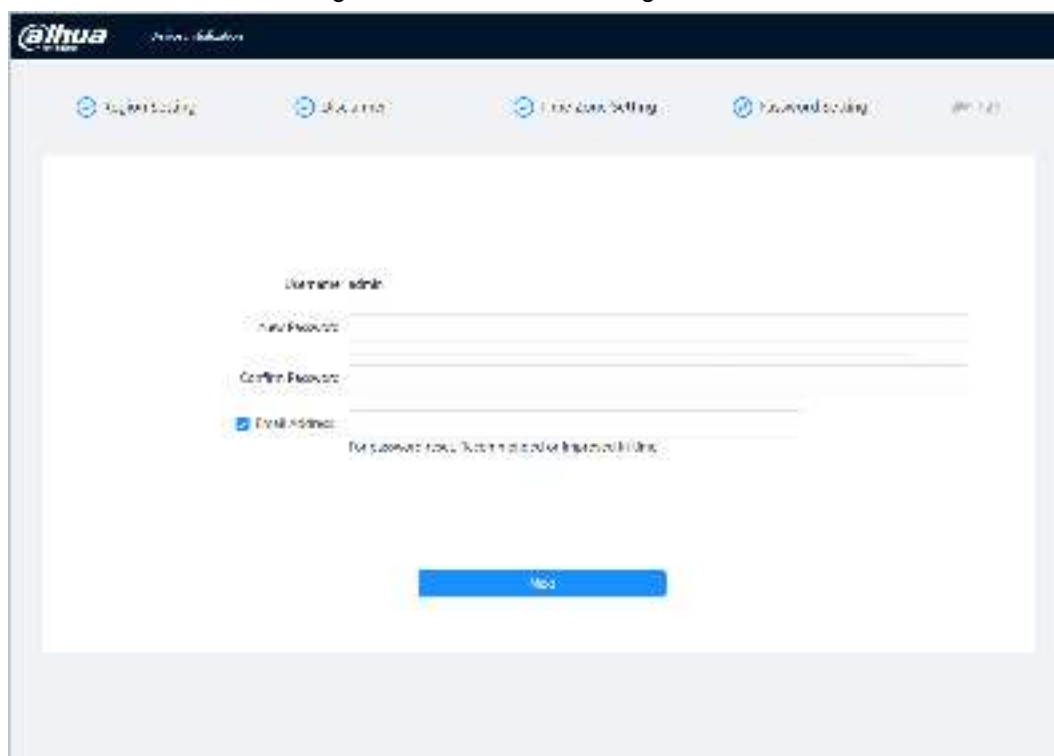
Step 3 Select the **I have read and agree to the terms of the Software License Agreement and Privacy Policy** check box, and then click **Next**.

Figure 3-3 Time zone setting



Step 4 Configure the time parameters, and then click **Next**.

Figure 3-4 Password setting



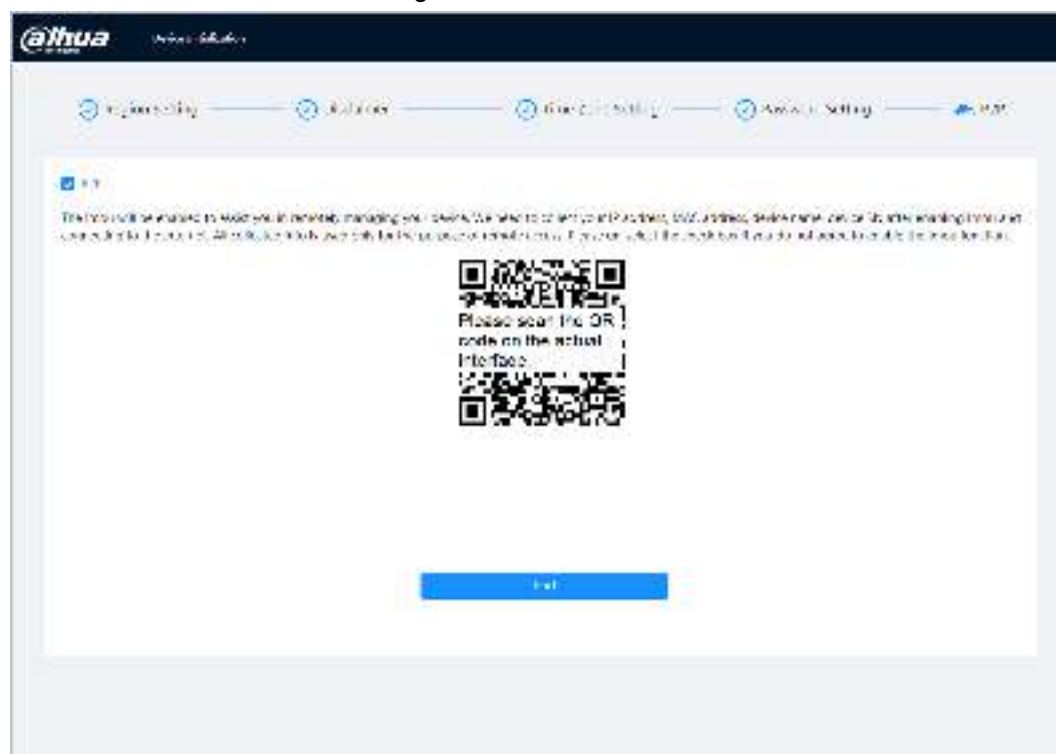
Step 5 Set the password for admin account.

Table 3-1 Description of password configuration

Parameter	Description
Username	The default username is admin.
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	
Reserved email	Enter an email address for password resetting, and it is selected by default. When you need to reset the password of the admin account, a security code for password resetting will be sent to the reserved email address.

Step 6 Click **Next**, and then **P2P** interface is displayed.

Figure 3-5 P2P



4 Login

4.1 Device Login

This section introduces how to log in to and log out of the web interface. This section takes Chrome as an example.



- You need to initialize the camera before logging in to the web interface. For details, see "3 Device Initialization".
- When initializing the camera, keep the PC IP and device IP in the same network.
- Follow the instruction to download and install the plug-in for the first login.

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

Step 2 Enter the username and password.
The username is admin by default.



Click **Forget password?**, and you can reset the password through the email address that is set during the initialization. For details, see "4.2 Resetting Password".

Figure 4-1 Login



Step 3 Click **Login**.

Figure 4-2 Live interface



4.2 Resetting Password

When you need to reset the password for the admin account, there will be a security code sent to the entered email address which can be used to reset the password.

Prerequisites

You have enabled password resetting service. For details, see "6.6.2.1.2 Resetting Password".

Procedure

- Step 1 Open IE browser, enter the IP address of the device in the address bar and press Enter.

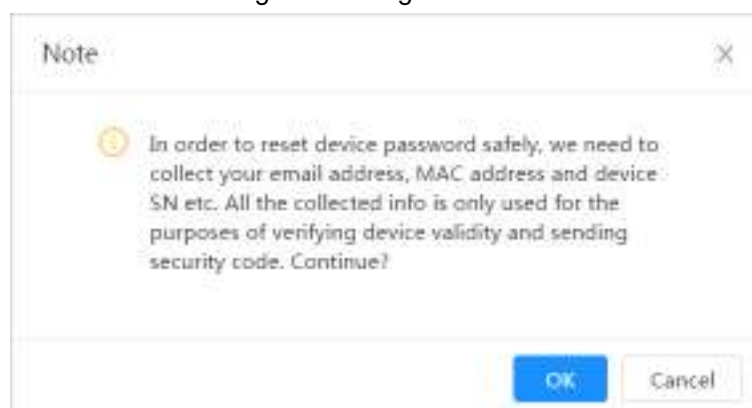
Figure 4-3 Login



- Step 2 Click **Forget password?**, and you can reset the password through the email address

that is set during the initialization.

Figure 4-4 Login



5 Main Interface


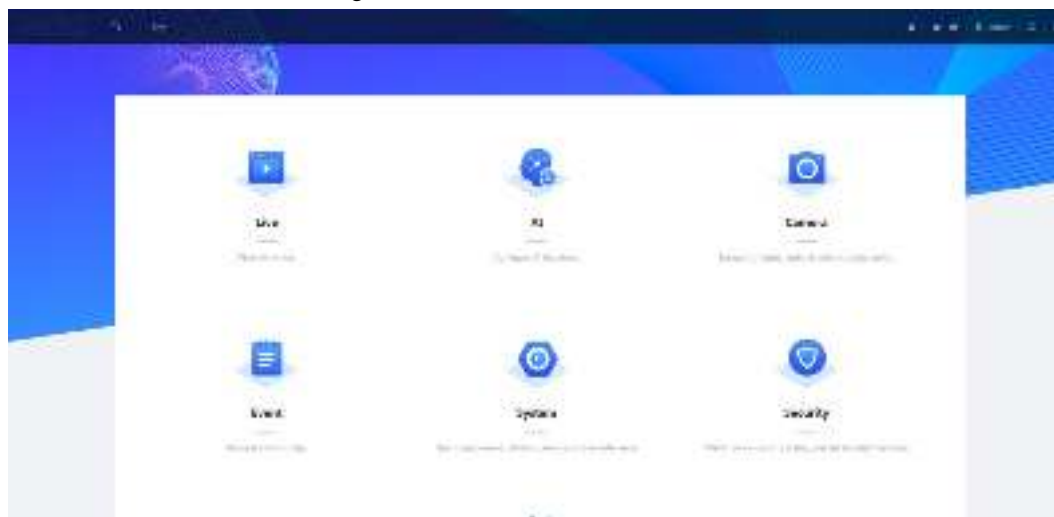





Click  at the left-upper corner of the interface to display the main interface.

Figure 5-1 Main interface



- Live: View the real-time monitoring image.
- AI: Configure AI functions of the camera.
- Camera: Configure camera parameters, including image parameters, encoder parameters, and audio parameters.
- Event: Configure general events, including alarm linkage exception, video detection, and audio detection.
- Event: Configure system parameters, including general, date & time, account, safety, PTZ settings, default, import/export, remote, auto maintain and upgrade.
- Security: Check the device security status and set security functions.
- Record: Play back or download recorded video.
- Picture: Play back or download image files.
- For the camera with multiple channels, through selecting channel numbers, you can set the parameters of the channels.
- Report: Search the AI event report and system report.
- Alarm subscription: Subscribe alarm.
- Skin setting: Set the skin.
- Language setting: Set the language.
- Restart: Click  **admin** at the upper-right corner of the interface, select **Reboot**, and the camera restarts.
- Logout: Click  **admin** at the upper-right corner of the interface, select **Logout** to go to the login interface.
The system will sleep automatically after idling for a period of time.
- Setting: Click  at the upper-right corner of the interface to set the basic parameters.
- Full screen: Click  at the upper-right corner of the interface to enter full screen mode; click  to exit full screen mode.

6 Setting

This section introduces the basic setting of the camera, including the configuration of Local, Camera, Network, Event, Storage, System, System Information and Log.

6.1 Local

You can select protocol and configure the storage path for live snapshot, live record, playback snapshot, playback download, and video clips.


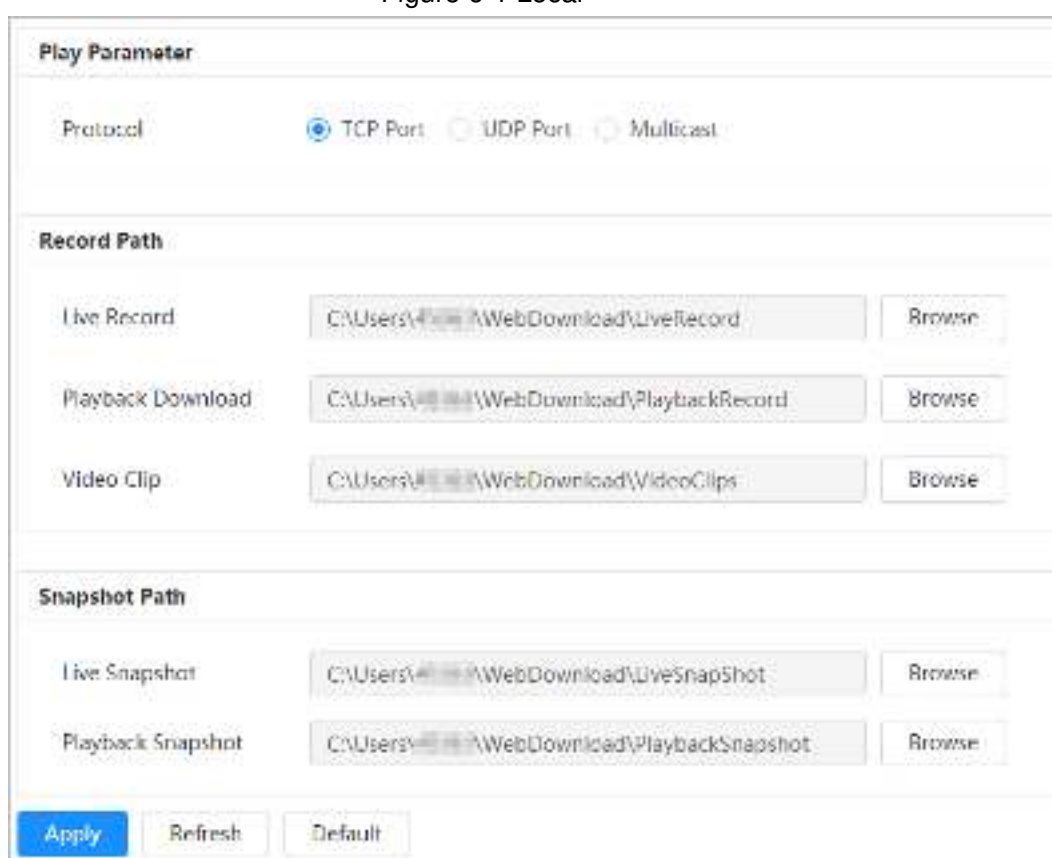

Step 1 Select  > **Local**.


Figure 6-1 Local



Step 2 Click **Browse** to select the storage path for live snapshot, live record, playback snapshot, playback download, and video clips.

Table 6-1 Description of local parameter

Parameter	Description
Protocol	<p>You can select the network transmission protocol as needed, and the options are TCP, UDP and Multicast.</p> <p> Before selecting Multicast, make sure that you have set the Multicast parameters.</p>

Parameter	Description	
Live Record	The recorded video of live interface. The default path is C:\Users\admin\WebDownload\LiveRecord.	 Admin in the path refers to the account being used.
Playback Download	The downloaded video of playback interface. The default path is C:\Users\admin\WebDownload\PlaybackRecord.	
Video Clips	The clipped video of playback interface. C:\Users\admin\WebDownload\VideoClips.	
Live Snapshot	The snapshot of live interface. The default path is C:\Users\admin\WebDownload\LiveSnapshot.	
Playback Snapshot	The snapshot of playback interface. The default path is C:\Users\admin\WebDownload\PlaybackSnapshot.	

Step 3 Click **Save**.

6.2 Camera

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



Camera parameters of different devices might vary, and the actual product shall prevail.

6.2.1 Setting Image Parameters

Configure image parameters according to the actual situation, including image, exposure, backlight, white balance, Day/Night, and light.

6.2.1.1 Interface Layout

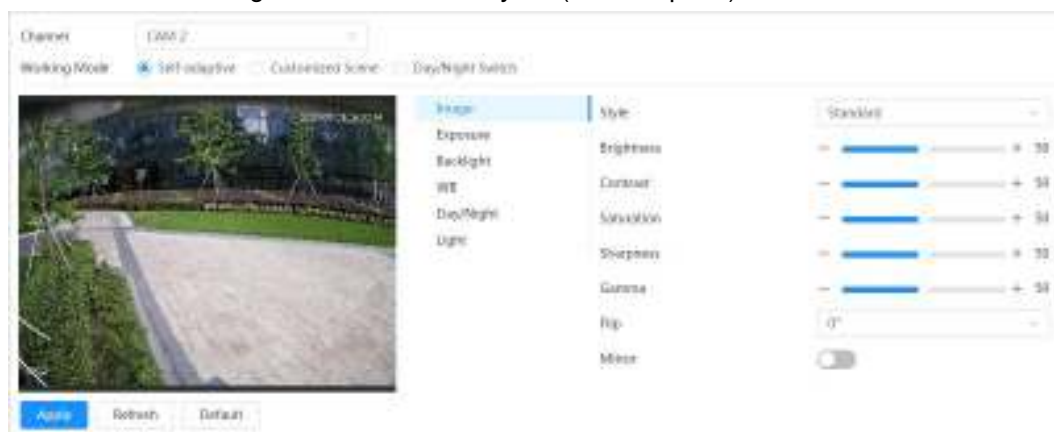
Configure camera parameters to improve the scene clarity, and ensure that surveillance goes properly.

You can select normal mode, day mode, or night mode to view the configuration and the effect of the selected mode, such as picture, exposure, and backlight.

Select the working mode as needed.

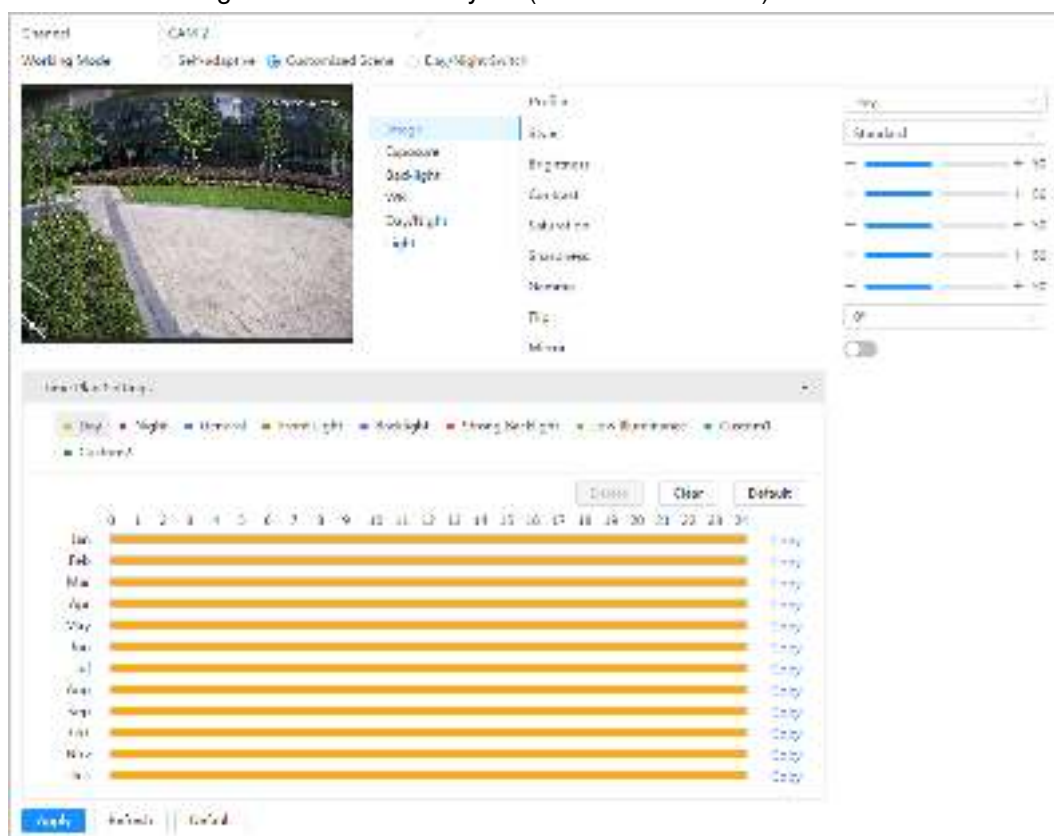
- Self-adaptive: The camera will adjust the image according to the environment.

Figure 6-2 Interface layout (self-adaptive)



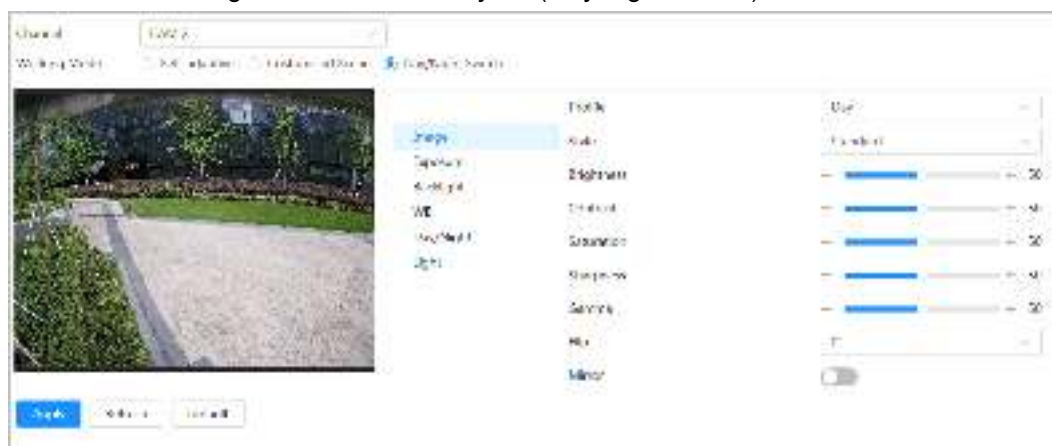
- Customized scene: You can select the profile as needed. Select the profile in **Time Plan Setting** and drag the slide block to set certain time as the selected profile. For example, set 8:00–18:00 as day, and 0:00–8:00 and 18:00–24:00 as night

Figure 6-3 Interface layout (customized scene)



- Day/night switch: You can select **Day** or **night** in **Profile** and the surveillance system works under **Day/Night**.

Figure 6-4 Interface layout (Day/night switch)

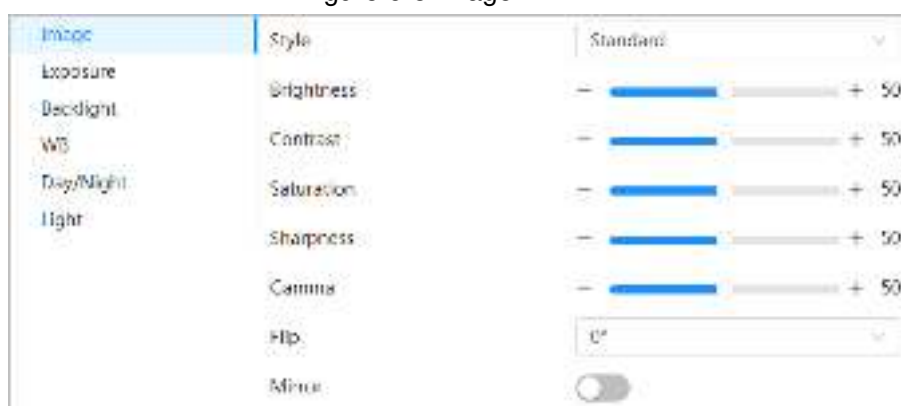


6.2.1.2 Image

You can configure picture parameters as needed.

Step 1 Select > **Camera** > **Image**.



Figure 6-5 Image



Step 2 Configure picture parameters.

Table 6-2 Description of picture parameters

Parameter	Description
Style	<p>Select the picture style from soft, standard and vivid.</p> <ul style="list-style-type: none"> Soft: Default image style, displays the actual color of the image. Standard: The hue of the image is weaker than the actual one, and contrast is smaller. Vivid: The image is more vivid than the actual one.
Brightness	<p>Changes the value to adjust the picture brightness. The higher the value is, the brighter the picture will be, and the smaller the darker. The picture might be hazy if the value is configured too big.</p>
Contrast	<p>Changes the contrast of the picture. The higher the value is, the more the contrast will be between bright and dark areas, and the smaller the less. If the value is set too big, the dark area would be too dark and bright area easier to get overexposed. The picture might be hazy if the value is set too small.</p>

Parameter	Description
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 image brightness.
Sharpness	Changes the sharpness of picture edges. The higher the value is, the clearer the picture edges will be, and if the value is set too big, picture noises are more likely to appear.
Gamma	Changes the picture brightness and improves the picture dynamic range in a non-linear way. The higher the value is, the brighter the picture will be, and the smaller the darker.
Flip	<p>Changes the display direction of the picture, see the options below.</p> <ul style="list-style-type: none"> 0°: Normal display. 90°: The picture rotates 90° clockwise. 180°: The picture rotates 90° counterclockwise. 270°: The picture flips upside down.  <p>For some models, please set the resolution to be 1080p or lower when using 90° and 180°. For details, see "6.2.2 Setting Encode Parameters".</p>
Mirror	Click  , and the picture will display with left and right side reversed.

Step 3 Click **Apply**.

6.2.1.3 Exposure

Configure iris and shutter to improve image clarity.



Cameras with true WDR do not support long exposure when WDR is enabled in **Backlight**.



Step 1 Select  > **Camera** > **Exposure**.

Figure 6-6 Exposure



Step 2 Configure exposure parameters.

Table 6-3 Description of exposure parameters

Parameter	Description
Anti-flicker	<p>You can select from 50 Hz, 60 Hz and Outdoor.</p> <ul style="list-style-type: none"> 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: You can select any exposure mode as needed.
Mode	<p>Device exposure modes.</p> <ul style="list-style-type: none"> 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 and shutter value manually to adjust image brightness.  <p>When the Anti-flicker is set to Outdoor, you can select Auto, Gain priority, Shutter priority or Manual in the Mode list.</p>
Exposure Compensation	Sets the value, and it ranges from 0 to 50. The higher the value is, the brighter the image will be.
Shutter	Set the effective exposure time. The smaller the value, the shorter the exposure time will be.
Gain	When selecting Gain Priority or Manual in Mode , you can set Gain. With minimum illumination, the camera increases Gain automatically to get clearer images.
Auto Iris	<p>This configuration is available only when the camera is equipped with auto-iris lens.</p> <ul style="list-style-type: none"> When auto iris is enabled, the iris size changes automatically according to the ambient lighting condition, and the image brightness changes accordingly. When auto iris is disabled, the iris stays at full size and does not change no matter how ambient lighting condition changes.

Parameter	Description
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.
Level	This configuration is available only when the 3D NR is enabled. The higher the level is, the better the result will be.

Step 3 Click **Apply**.

6.2.1.4 Backlight

You can select backlight mode from Auto, BLC, WDR, and HLS.


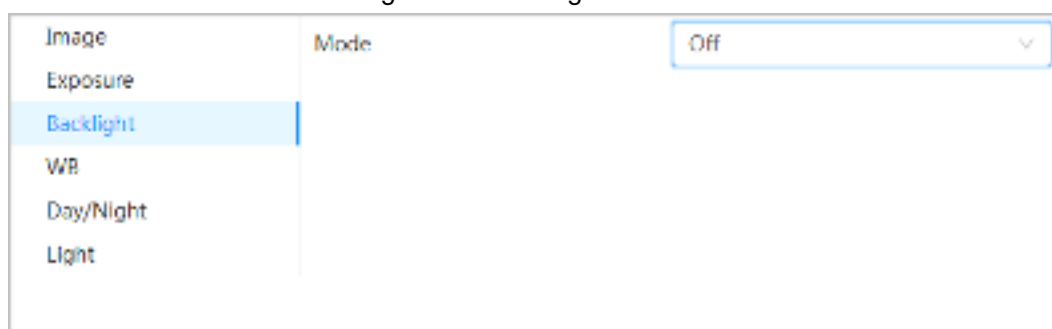

Step 1 Select  > **Camera** > **Backlight**.

Figure 6-7 Backlight



Step 2 Configure backlight parameters.

Table 6-4 Description of backlight parameters

Backlight mode	Description
BLC	<p>Enable BLC, the camera can get clearer image of the dark areas on the target when shooting against light. You can enable or disable Customized mode.</p> <ul style="list-style-type: none"> When you enable Customized mode, the system auto adjusts exposure only to the set area according to ambient lighting condition to ensure the image of the set area at ideal brightness. When you disable Default mode, the system adjusts exposure according to ambient lighting condition automatically to ensure the clarity of the darkest area.
WDR	<p>The system dims bright areas and compensates dark areas to ensure the clarity of all the area. The higher the value is, the brighter the dark will be, but the more the noise will be.</p> <p></p> <p>There might be a few seconds of video loss when the device is switching to WDR mode from other mode.</p>
HLC	<p>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.</p>
SSA	<p>Enable SSA, the system automatically adjusts the image brightness according to the environment to make the objects in the image clearer.</p>

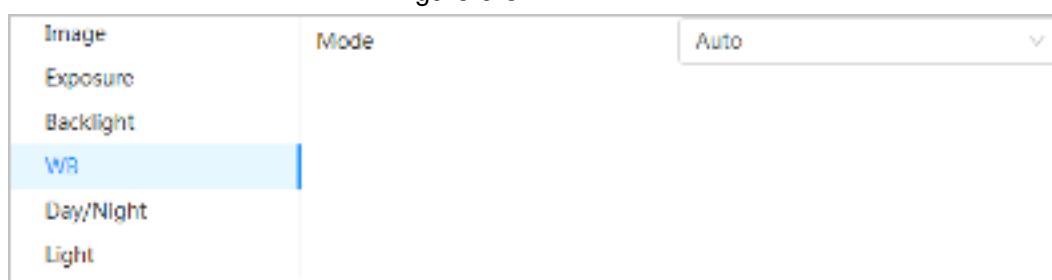
Step 3 Click **Apply**.

6.2.1.5 WB

WB function makes the image color display precisely as it is. When in WB mode, white objects would always display white color in different environments.

Step 1 Select  > **Camera** > **WB**.

Figure 6-8 WB



Step 2 Configure WB parameters.

Table 6-5 Description of WB parameters

WB mode	Description
Auto	The system compensates WB according to color temperature to ensure color precision.
Natural	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.
Outdoor	The system auto compensates WB to most outdoor environments with natural or artificial light to ensure color precision.
Manual	Configure red and blue gain manually; the system auto compensates WB according to color temperature.
Custom Area	The system compensates WB only to the set area according to color temperature to ensure color precision.

Step 3 Click **Apply**.

6.2.1.6 Day/Night

Configure the display mode of the image. The system switches between color and black-and-white mode according to the actual condition.


Step 1 Select  > **Camera** > **WB**.

Figure 6-9 Day/night



Step 2 Configure day and night parameters.

Table 6-6 Description of day and night parameters

Parameter	Description
Mode	<p>You can select device display mode from Color, Auto, and B/W.  Day/Night configuration is independent from profile management configuration.</p> <ul style="list-style-type: none"> • 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	<p>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.</p>
Delay	<p>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.</p>

Step 3 Click **Apply**.

6.2.1.7 Illuminator

This configuration is available only when the device is equipped with illuminator.


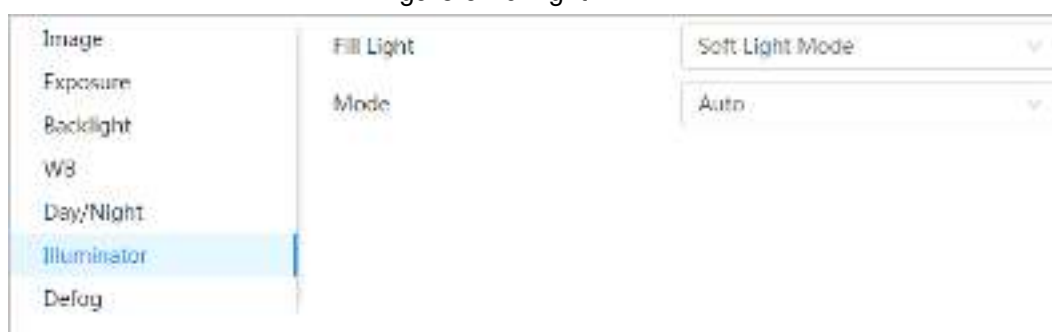
Step 1 Select  > **Camera** > **Illuminator**.

Figure 6-10 Light



Step 2 Configure illuminator parameters.

Table 6-7 Description of illuminator parameters

Parameter	Description	
Fill Light	Set Fill Light for sound and siren cameras. <ul style="list-style-type: none"> IR Mode: Enable the IR illuminator, and the white light is disabled. When an alarm is triggered, the system will link white light. White Light: Enable the white light, and the IR illuminator is disabled. When an alarm is triggered, the system will link white light. Soft Light Mode: Enable IR illuminator and white light at the same time, and adjust the brightness of the two illuminators to get clear images. 	
Mode	Manual	Adjust the brightness of illuminator manually, and then the system will supply illuminator to the image accordingly.
	Auto	The system adjusts the illuminator intensity according to the ambient lighting condition.
	Zoom Priority	The system adjusts the illuminator intensity automatically according to the change of the ambient light. <ul style="list-style-type: none"> When the ambient light turns darker, the system turns on the low beam lights first, if the brightness is still not enough, it turns on the high beam lights then. When the ambient light turns brighter, the system dims high beam lights until they are off, and then the low beam lights. When the focus reaches certain wide angle, the system will not turn on high beam light in order to avoid over-exposure in short distance. In the meantime, you can configure light compensation manually to fine-tune IR light intensity.
	Off	Illuminator is off.

Step 3 Click **Apply**.

6.2.1.8 Defog

The image quality is compromised in foggy or hazy environment, and defog can be used to improve image clarity.

Step 1 Select  > **Camera** > **Defog**.

Figure 6-11 Light



Step 2 Configure defog parameters.

Table 6-8 Description of defog parameters

Defog	Description
Manual	Configure function intensity and atmospheric light mode manually, and then the system adjusts image clarity accordingly. Atmospheric light mode can be adjusted automatically or manually.
Auto	The system adjusts image clarity according to the actual condition.
Off	Defog function is disabled.

Step 3 Click **Apply**.

6.2.2 Setting Encode Parameters

This section introduces video parameters, such as video, snapshot, overlay, ROI (region of interest), and path.



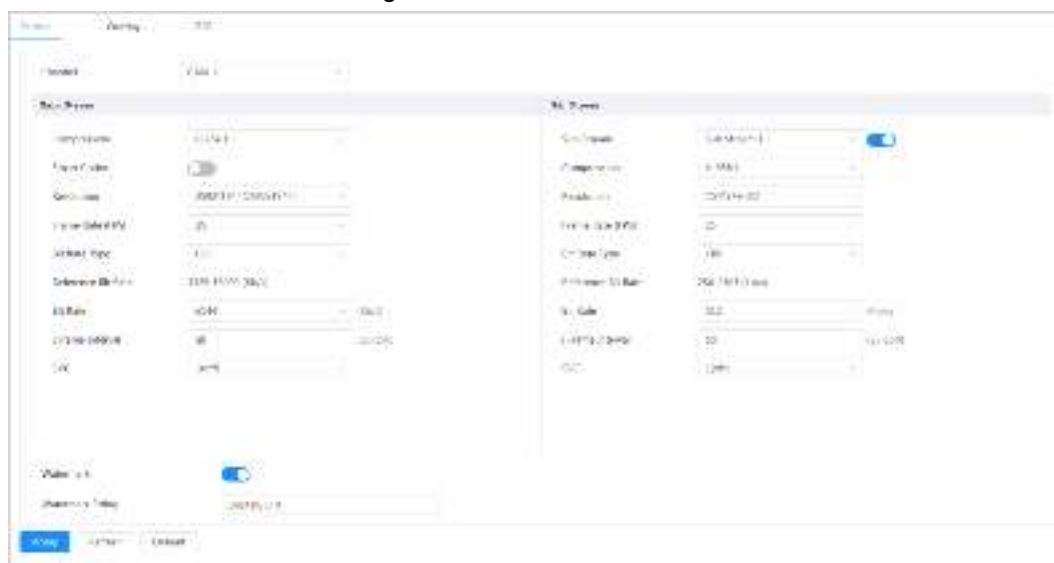
Click **Default**, and the device is restored to default configuration. Click **Refresh** to view the latest configuration.

6.2.2.1 Encode

Configure video stream parameters, such as compression, resolution, frame rate, bit rate type, bit rate, I frame interval, SVC, and watermark.

Step 1 Select  > **Camera** > **Encode** > **Encode**.


Figure 6-12 Encode



Step 2 Configure encode parameters.

Table 6-9 Description of encode parameters

Parameter	Description
Sub Stream	Click to enable sub stream, it is enabled by default. You can enable multiple sub streams simultaneously.
Compression	Select encode mode. <ul style="list-style-type: none"> ● H.264: Main profile encode mode. Compared with H.264B, it requires smaller bandwidth. ● H.264H: High profile encode mode. Compared with H.264, it requires smaller bandwidth. ● H.264B: Baseline profile encode mode. It requires smaller bandwidth. ● H.265: Main profile encode mode. Compared with H.264, it requires smaller bandwidth. ● MJPEG: When under this mode, the image requires high bit rate value to ensure clarity, you are recommended to set the Bit Rate value to the biggest value in the Reference Bit Rate.
Smart Codec	Click to enable smart codec to improve video compressibility and save storage space. After smart codec is enabled, the device would stop supporting the third bit stream, ROI, and smart event detection, and the actual interface shall prevail.
Output Mode	You can select from Single Stream or Flex Stream .
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	<p>The bit rate control type during video data transmission. You can select bit rate type from:</p> <ul style="list-style-type: none"> • CBR (Constant Bit Rate): The bit rate changes a little and keeps close to the defined bit rate value. • VBR (Variable Bit Rate): The bit rate changes as monitoring scene changes.  <p>The Bit Rate Type can be only be set as CBR when Encode Mode is set as MJPEG.</p>
Quality	<p>This parameter can be configured only when the Bit Rate Type is set as VBR.</p> <p>The better the quality is, but the bigger the required bandwidth will be.</p>
Reference Bit Rate	<p>The most suitable bit rate value range recommended to user according to the defined resolution and frame rate.</p>
Max Bit Rate	<p>This parameter can be configured only when the Bit Rate Type is set as VBR.</p> <p>You can select the value of the Max Bit Rate according to the Reference Bit Rate value. The bit rate then changes as monitoring scene changes, but the max bit rate keeps close to the defined value.</p>
Bit Rate	<p>This parameter can be configured only when the Bit Rate Type is set as CBR.</p> <p>Select bit rate value in the list according to actual condition.</p>
I Frame Interval	<p>The number of P frames between two I frames, and the I Frame Interval range changes as FPS changes.</p> <p>It is recommended to set I Frame Interval twice as big as FPS.</p>
SVC	<p>Scaled video coding, is able to encode a high quality video bit stream that contains one or more subset bit streams. When sending stream, to improve fluency, the system will quit some data of related lays according to the network status.</p> <ul style="list-style-type: none"> • 1: The default value, which means that there is no layered coding. • 2, 3 and 4: The lay number that the video stream is packed.
Watermark	<p>You can verify the watermark to check if the video has been tampered.</p>
Watermark String	

Step 3 Click **Apply**.

6.2.2.2 Overlay

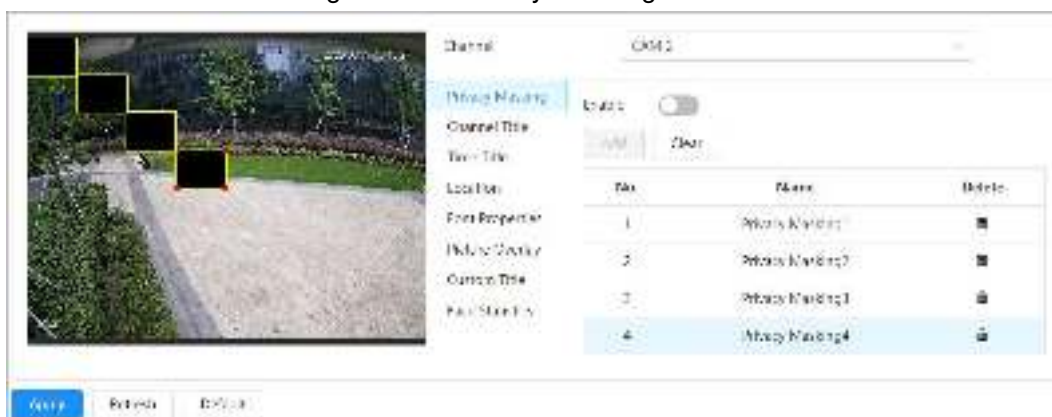
Configure overlay information, and it will be displayed on the **Live** interface.

6.2.2.2.1 Configuring Privacy Masking

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

Step 1 Select > **Camera** > **Encode** > **Overlay** > **Privacy Masking**.

Figure 6-13 Privacy masking



Step 2 Configure privacy masking.

- 1) Click next to **Enable**, and then drag the block to the area that you need to cover.



- You can drag 4 rectangles at most.
- Click **Clear** to delete all the area boxes; select one box, and then click to delete it.

- 2) Adjust the size of the rectangle to protect the privacy.

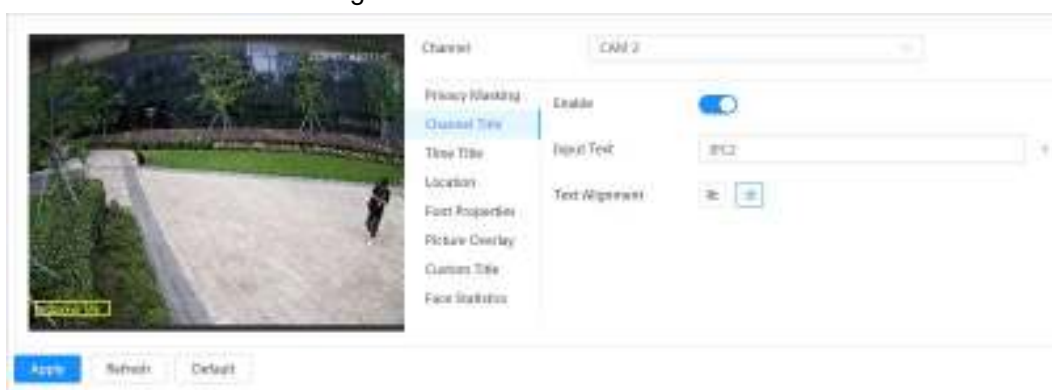
- 3) Click **Apply**.

6.2.2.2.2 Configuring Channel Title

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

Step 1 Select > **Camera** > **Encode** > **Overlay** > **Channel Title**.

Figure 6-14 Channel title



Step 2 Click next to **Enable**, enter the channel title, and select the text alignment.



Click to add the channel title, and you can add 1 line at most.

Step 3 Move the title box to the position that you want in the image.

Step 4 Click **Apply**.

6.2.2.2.3 Configuring Time Title

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


Step 1 Select  > **Camera** > **Encode** > **Overlay** > **Time Title**.

Figure 6-15 Time title



Step 2 Click ☐ next to **Enable**.

Step 3 Click ☐ next to **Week Display** to display the day of week.

Step 4 Move the time box to the position that you want in the image.

Step 5 Click **Apply**.

6.2.2.2.4 Configuring Location

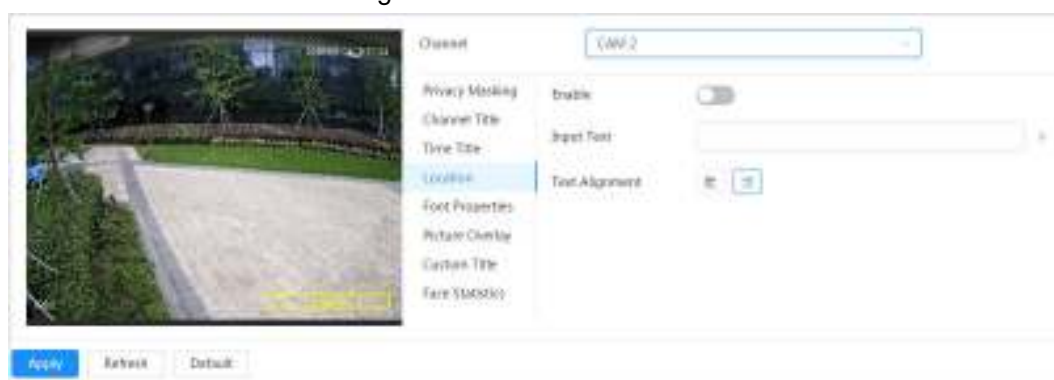
You can enable this function if you need to display text in the video image.



Text overlay and picture overlay cannot work at the same time, and the IPC that connects to mobile NVR with private protocol would display GPS information as priority.

Step 1 Select  > **Camera** > **Encode** > **Overlay** > **Location**.

Figure 6-16 Location



Step 2 Click ☐ next to **Enable**, enter the location information, and then select alignment. The text is displayed in the video image.



Click **+** to add the text overlay, and you can add 13 lines at most.

Step 3 Move the text box to the position that you want in the image.

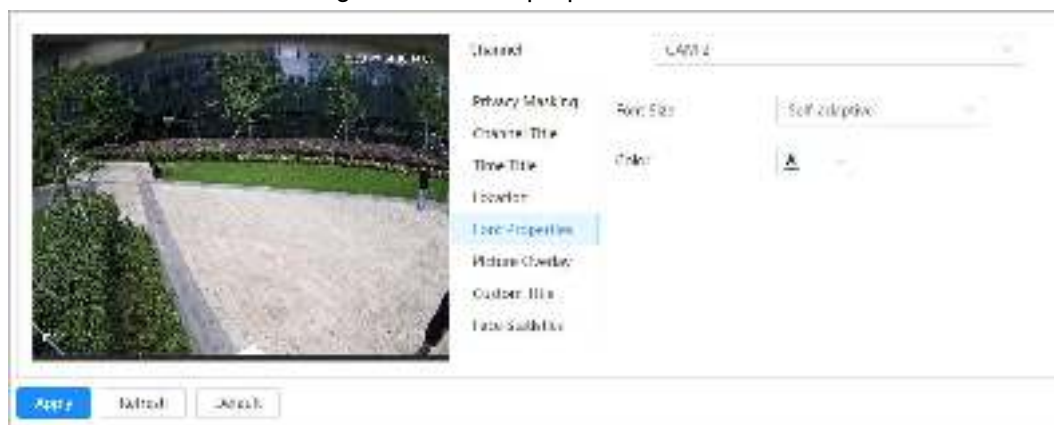
Step 4 Click **Apply**.

6.2.2.2.5 Configuring Font Properties

You can enable this function if you need to adjust the font size in the video image.

Step 1 Select  > **Camera** > **Encode** > **Overlay** > **Font Properties**.

Figure 6-17 Font properties



Step 2 Select the font color and size.

You can set the RGB value to customize the font color.

Step 3 Click **Apply**.

6.2.2.2.6 Configuring Picture Overlay

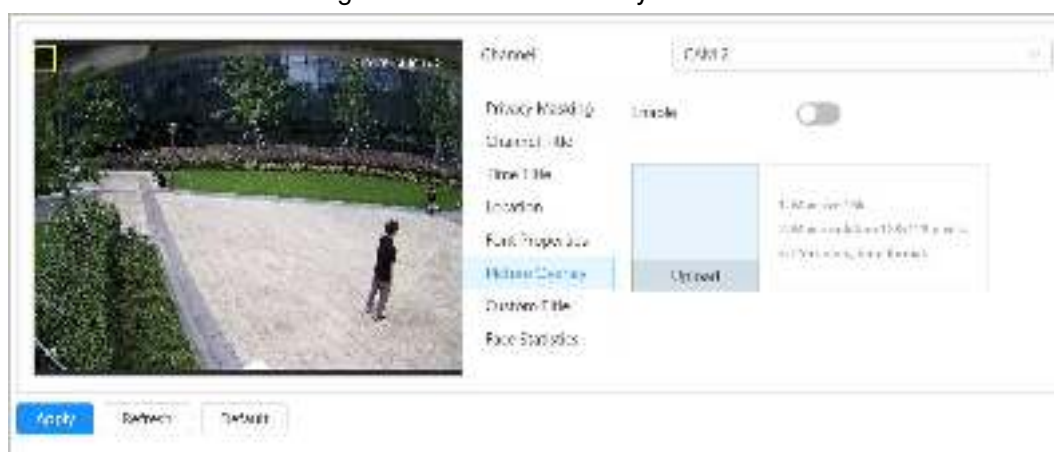
You can enable this function if you need to display picture information on the video image.



Text overlay and picture overlay cannot work at the same time.

Step 1 Select  > **Camera** > **Encode** > **Overlay** > **Picture Overlay**.

Figure 6-18 Picture overlay



Step 2 Click  next to **Enable**, click **Upload**, and then select the picture to be overlaid. The picture is displayed on the video image.

Step 3 Move the overlaid picture to the position that you want in the image.

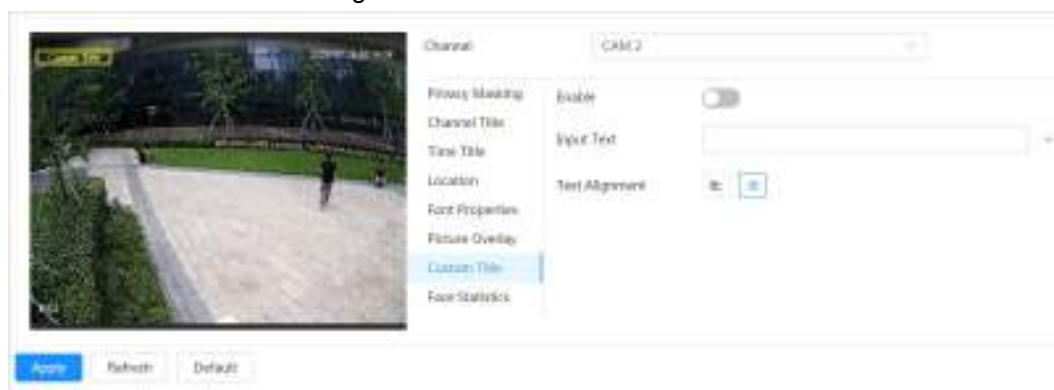
Step 4 Click **Apply**.


6.2.2.2.7 Configuring Custom Title

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


Step 1 Select  > **Camera** > **Encode** > **Overlay** > **Custom Title**

Figure 6-19 Custom Title



Step 2 Click  next to **Enable**, enter the text that you want to display, and then select the text alignment.



Click  to add the text overlay, and you can add 1 line at most.

Step 3 Move the custom box to the position that you want in the image.

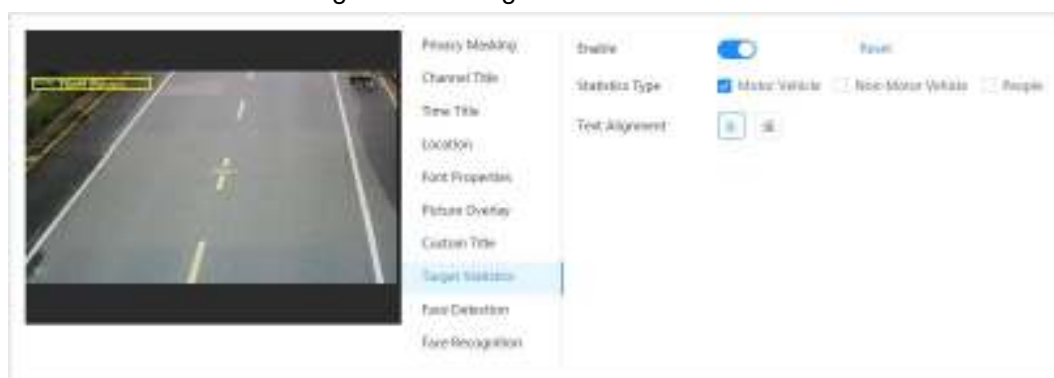
Step 4 Click **Apply**.


6.2.2.2.8 Configuring Target Statistics

After configuring the target statistics, the number of target statistics will be displayed in the image.

Step 1 Select  > **Camera** > **Encode** > **Overlay** > **Target Statistics**.

Figure 6-20 Target statistics



Step 2 Click  next to **Enable**, select the statistics type, and then select the text alignment.



Click **Reset** to clear the statistics data.

Step 3 Move the custom box to the position that you want in the image.

Step 4 Click **Apply**.

The overlaid information will be displayed after enabling video metadata function.

6.2.2.2.9 Configuring Face Detection

The image displays face statistics information. When the overlay function enabled during intelligent rules configuration, this function is enabled simultaneously.

Step 1 Select > **Camera** > **Encode** > **Overlay** > **Face Detection**.

Figure 6-21 Face detection



Step 2 Click next to **Enable**, and select the text alignment.



Click **Reset** to clear the statistics data.

Step 3 Move the statistics box to the position that you want in the image.

Step 4 Click **Apply**.

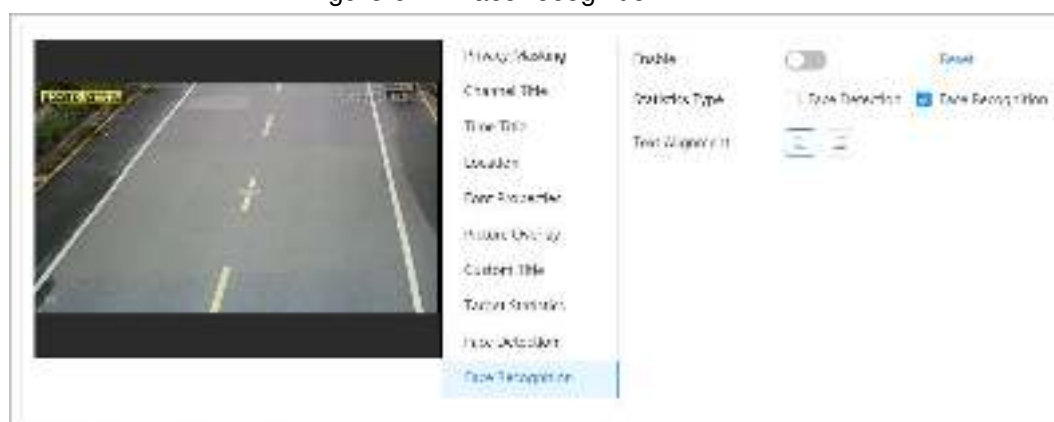
The information will be displayed on the image after the face detection function is enabled.

6.2.2.2.10 Configuring Face Recognition

The image displays face statistics information. When the overlay function enabled during intelligent rules configuration, this function is enabled simultaneously.

Step 1 Select > **Camera** > **Encode** > **Overlay** > **Face Recognition**.

Figure 6-22 Face recognition



Step 2 Click next to **Enable**, select the statistics type, and then select the text alignment.



Click **Reset** to clear the statistics data.

Step 3 Move the statistics box to the position that you want in the image.

Step 4 Click **Apply**.

The information will be displayed on the image after the face recognition function is enabled.

6.2.2.2.11 Configuring Face Statistics

The image displays face statistics information. When the overlay function enabled during intelligent rules configuration, this function is enabled simultaneously.

Step 1 Select  > **Camera** > **Encode** > **Overlay** > **Face Statistics**.

Figure 6-23 Face statistics



Step 2 Click  next to **Enable**, and select the text alignment.



Click **Reset** to clear the statistics data.

Step 3 Move the statistics box to the position that you want in the image.

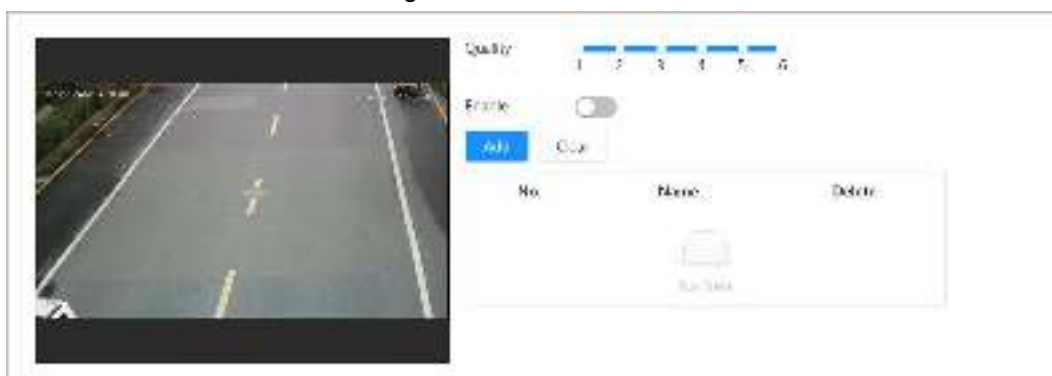
Step 4 Click **Apply**.

6.2.2.3 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 Select  > **Camera** > **Encode** > **ROI**.

Figure 6-24 ROI



Step 2 Click ☐ next to **Enable**, draw an area on the image, and then configure 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 area boxes; select one box, and then click to delete it.

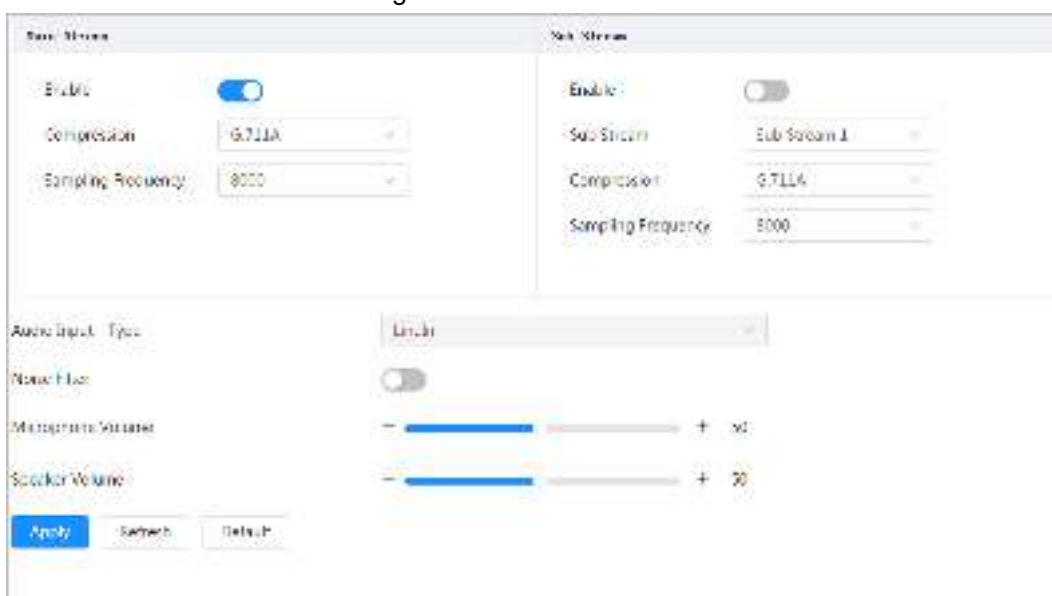
Step 3 Click **Apply**.

6.2.3 Setting Audio Parameters

This section introduces audio parameters, including encode mode, sampling frequency, audio in type, and noise filter.

Step 1 Select > **Camera** > **Audio**.

Figure 6-25 Audio



Step 2 Click ☐ next to **Enable** in **Main Stream** or **Sub Stream**.
For the camera with multiple channels, select the channel number.



Please carefully activate the audio acquisition function according to the actual requirements of the application scenario.

Step 3 Configure audio parameters.

Table 6-10 Description of audio parameters

Parameter	Description
Compression	You can select audio Encode Mode from PCM, G.711A, G.711Mu, G.726, AAC, G.723 . The configured audio encode mode applies to both audio and intercom. The default value is recommended.
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. You can select audio Sampling Frequency from 8000, 16000, 32000, 48000, 64000 .
Audio Input Type	You can select audio input type from: <ul style="list-style-type: none"> • LineIn: Requires external audio device. • Mic: Not require external audio device.
Noise Filter	Enable this function, and the system auto filters ambient noise.
Microphone Volume	Adjusts microphone volume.
Speaker Volume	Adjusts speaker volume.

Step 4 Click **Apply**.

6.3 Network

This section introduces network configuration.

6.3.1 TCP/IP

You can configure IP address and DNS (Domain Name System) server and so on according to network planning.

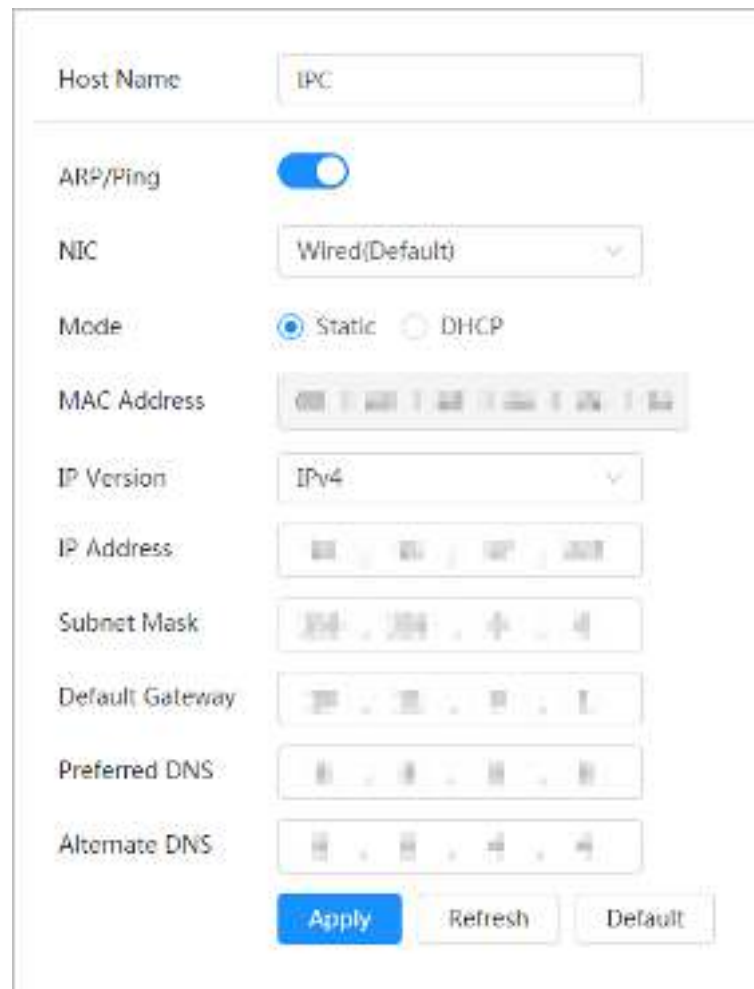
Prerequisites

The camera has connected to the network.

Procedure

Step 1 Select  > **Network** > **TCP/IP**.

Figure 6-26 TCP/IP



Host Name: IPC

ARP/Ping: ☒

NIC: Wired(Default)

Mode: ☒ Static ☐ DHCP

MAC Address: 00:11:22:33:44:55

IP Version: IPv4

IP Address: 192.168.1.100

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.1.1

Preferred DNS: 8.8.8.8


Alternate DNS: 8.8.4.4


Buttons: Apply, Refresh, Default

Step 2 Configure TCP/IP parameters.

Table 6-11 Description of TCP/IP parameters

Parameter	Description
Host Name	Enter the host name, and the maximum length is 15 characters.

Parameter	Description
ARP/Ping	<p>Click  to enable ARP/Ping to set IP address service. Get the camera MAC address, and then you can change and configure the device IP address with ARP/ping command.</p> <p>This is enabled by default. During restart, you will have no more than 2 minutes to configure the device IP address by a ping packet with certain length, the server will be turned off in 2 minutes, or it will be turned off immediately after the IP address is successfully configured. If this is not enabled, the IP address cannot be configured with ping packet.</p> <p>A demonstration of configuring IP address with ARP/Ping.</p> <ol style="list-style-type: none"> 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 the following command. <div data-bbox="657 835 1329 1404" data-label="Code-Block"> <pre> Windows syntax arp -s <IP Address> <MAC> ping -l 480 -t <IP Address> Windows example arp -s 192.168.0.125 11-40-8c-18-10-11 ping -l 480 -t 192.168.0.125 UNIX/Linux/Mac syntax arp -s <IP Address> <MAC> ping -s 480 <IP Address> UNIX/Linux/Mac example arp -s 192.168.0.125 11-40-8c-18-10-11 ping -s 480 192.168.0.125 </pre> </div> <ol style="list-style-type: none"> 4. Restart the camera. 5. Check the PC command line, if information such as Reply from 192.168.0.125... is displayed, the configuration succeeds, and you can turn it off then. 6. Enter <code>http://(IP address)</code> 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	<p>The mode that the camera gets IP:</p> <ul style="list-style-type: none"> • Static Configure IP Address, Subnet Mask, and Default Gateway manually, and then click Save, the login interface with the configured IP address is displayed. • DHCP When there is DHCP server in the network, select DHCP, and the camera acquires IP address automatically.

Parameter	Description
MAC Address	Displays host MAC address.
IP Version	Select IPv4 or IPv6 .
IP Address	When you select Static in Mode , enter the IP address and subnet mask that you need.  <ul style="list-style-type: none"> 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

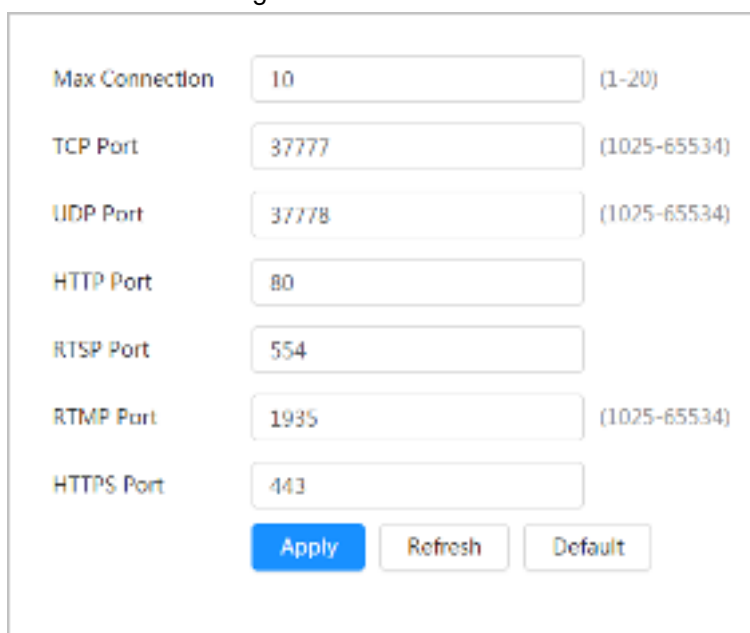
Step 3 Click **Apply**.

6.3.2 Port

Configure the port numbers and the maximum number of users (includes web, platform client, and mobile phone client) that can connect to the device simultaneously.

Step 1 Select  > **Network** > **TCP/IP**.

Figure 6-27 Port



Max Connection	10	(1-20)
TCP Port	37777	(1025-65534)
UDP Port	37778	(1025-65534)
HTTP Port	80	
RTSP Port	554	
RTMP Port	1935	(1025-65534)
HTTPS Port	443	

Step 2 Configure port parameters.



- 0–1024, 1900, 3800, 5000, 5050, 9999, 37776, 37780–37880, 39999, 42323 are occupied for specific uses.
- Do not use the same value of any other port during port configuration.

Table 6-12 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	Hyper text transfer protocol port. The value is 80 by default.
RTSP Port	<ul style="list-style-type: none"> • Real time streaming protocol port, and the value is 554 by default. If you play live view with QuickTime, VLC or Blackberry smart phone, the following URL format is available. • When the URL format requiring RTSP, you need to specify channel number and bit stream type in the URL, and also username and password if needed. • When playing live view with Blackberry smart phone, you need to turn off the audio, and then set the codec mode to H.264B and resolution to CIF. <p>URL format example: rtsp://username:password@ip:port/cam/realmonitor?channel=1&subtype=0</p> <p>Among that:</p> <ul style="list-style-type: none"> • Username: The username, such as admin. • Password: The password, such as admin. • IP: The device IP, 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 bit stream type; 0 means main stream (Subtype=0) and 1 means sub stream (Subtype=1). <p>Example: If you require the sub stream of channel 2 from a certain device, then the URL should be: rtsp://admin:admin@10.12.4.84:554/cam/realmonitor?channel=21&=1</p> <p>If username and password are not needed, then the URL can be: rtsp://ip:port/cam/realmonitor?channel=11&=0</p>
RTMP Port	Real Time Messaging Protocol. The port that RTMP provides service. It is 1935 by default.
HTTPS Port	HTTPS communication port. It is 443 by default.

Step 3 Click **Apply**.



The configuration of **Max Connection** takes effect immediately, and others will take effect after reboot.

6.3.3 PPPoE

Point-to-Point Protocol over Ethernet, is one of the protocols that device uses to connect to the internet. Get the PPPoE username and password from the internet service provider, and then set up network connection through PPPoE, the camera will acquire a WAN dynamic IP address.

Prerequisites


- The camera has connected to the network.
- You have gotten the account and password from Internet Service Provider.

Procedure

Step 1 Select  > **Network** > **PPPoE**.

Figure 6-28 PPPoE



Step 2 Click , and then enter username and password.



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

Step 3 Click **Apply**.

The success prompt box is displayed, and then the real-time WAN IP address is displayed. You can visit camera through the IP address.

6.3.4 DDNS

Properly configure DDNS, and then the domain name on the DNS server matches your IP address and the matching relation refreshes in real time. You can always visit the camera with the same domain name no matter how the IP address changes.

Prerequisites

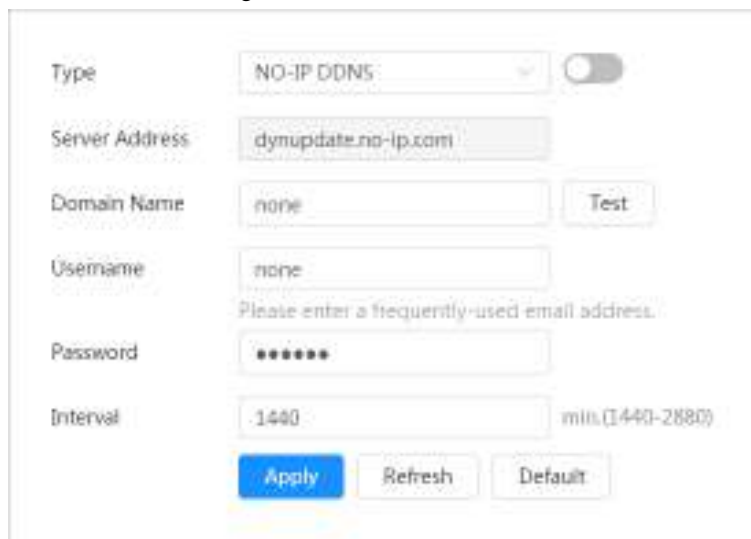
Check the type of DNS server supported by the camera.

Step 1 Select  > **Network** > **DDNS**.



- 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.

Figure 6-29 DDNS



Step 2 Click ☐ to enable the function.

Step 3 Configure DDNS parameters.

Table 6-13 Description of DDNS parameters

Parameter	Description
Type	The name and web address of the DDNS service provider, see the matching relationship below: <ul style="list-style-type: none"> • 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, and the time is 10 minutes by default.

Step 4 Click **Apply**.

Result

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

6.3.5 Email

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





Step 1 Select > **Network** > **Email**.


Figure 6-30 Email

Step 2 Click to enable the function.

Step 3 Configure email parameters.



Table 6-14 Description of email parameters


Parameter	Description	
SMTP Server	SMTP server address	 For details, see Table 6-15.
Port	The port number of the SMTP server.	
Username	The account of SMTP server.	
Password	The password of SMTP server.	
Anonymity	Click  , and the sender's information is not displayed in the email.	
Sender	Sender's email address.	
Encryption Type	Select from None , SSL and TLS .  For details, see Table 6-15.	
Subject	Enter maximum 63 characters in Chinese, English, and Arabic numerals. Click  to select title type, including Device Name , Device ID , and Event Type , and you can set maximum 2 titles.	
Attachment	Select the check box to support attachment in the email.	

Parameter	Description
Receiver	<ul style="list-style-type: none"> Receiver's email address. Supports 3 addresses at most. After entering the receiver's email address, the Test button is display. Click Test to test whether the emails can be sent and received successfully.
Health Mail	The system sends test mail to check if the connection is successfully configured. Click  and configure the Sending Interval , and then the system sends test mail as the set interval.

For the configuration of major mailboxes, see Table 6-15.

Table 6-15 Description of major mailbox configuration

Mailbox	SMTP server	Authentication	Port	Description
QQ	smtp.qq.com	SSL	465	<ul style="list-style-type: none"> The authentication type cannot be None. You need to enable SMTP service in your mailbox. The authentication code is required, the QQ password or email password is not applicable.  Authentication code: The code you receive when enabling SMTP service.
		TLS	587	
163	smtp.163.com	SSL	465/994	<ul style="list-style-type: none"> You need to enable SMTP service in your mailbox. The authentication code is required; the email password is not applicable.  Authentication code: the code you receive when enabling SMTP service.
		TLS	25	


Mailbox	SMTP server	Authentication	Port	Description
		none	25	<ul style="list-style-type: none"> You need to enable SMTP service in your mailbox. The authentication code is required; the email password is not applicable.  Authentication code: the code you receive when enabling SMTP service.
Sina	smtp.sina.com	SSL	465	Enable SMTP service in your mailbox.
		none	25	
126	smtp.126.com	none	25	Enable SMTP service in your mailbox.

Step 4 Click **Apply**.

6.3.6 UPnP

UPnP (Universal Plug and Play), is a protocol that establishes mapping relation between local area and wide area networks. This function enables you to visit local area device 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 internet connection.
- Enable UPnP in the router.
- Connect your device to the LAN port of the router.
- Select  > **Network** > **TCP/IP**, in **IP Address**, enter the local area IP address of the router or select **DHCP** and acquires IP address automatically.

Procedure

Step 1 Select  > **Network** > **UPnP**.

Figure 6-31 UPnP



Step 2 Click ☐ next to **Enable**, and there are two mapping modes: **Custom** and **Default**.

- Select **Custom**, click and then you can change external port as needed.
- Select **Default**, and then the system finishes mapping with unoccupied port automatically, and you cannot edit mapping relation.

Step 3 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.

6.3.7 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.

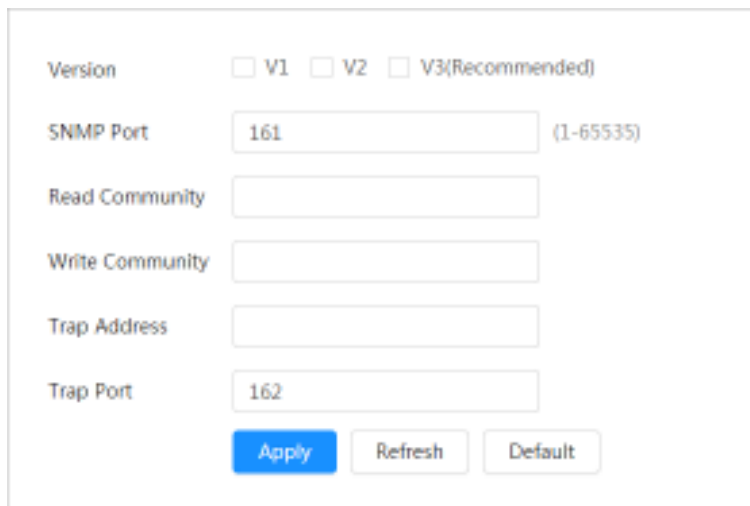
Prerequisites

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

Procedure

Step 1 Select > **Network** > **SNMP**.

Figure 6-32 SNMP (1)



Version ☐ V1 ☐ V2 ☐ V3(Recommended)

SNMP Port (1-65535)

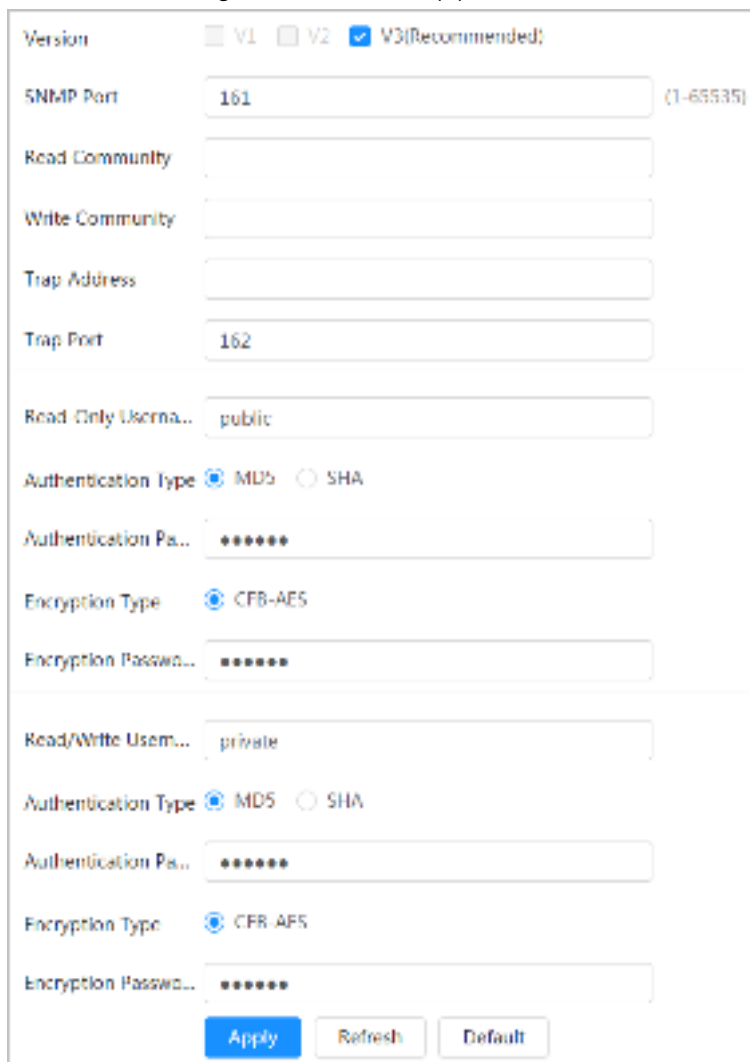
Read Community

Write Community

Trap Address

Trap Port

Figure 6-33 SNMP (2)



Version ☐ V1 ☐ V2 ☒ V3(Recommended)

SNMP Port (1-65535)

Read Community

Write Community

Trap Address

Trap Port

Read Only Userna...

Authentication Type ☒ MD5 ☐ SHA

Authentication Pa...

Encryption Type ☒ CFB-AES

Encryption Passwa...

Read/Write Usen...

Authentication Type ☒ MD5 ☐ SHA

Authentication Pa...

Encryption Type ☒ CFB-AES

Encryption Passwa...

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**, and then **V1** and **V2** become unavailable. You can configure username, password and authentication type. It requires corresponding username, password




and authentication type to visit your device from the server.



Using **V1** and **V2** might cause data leakage, and **V3** is recommended.

Step 3 In **Trap Address**, enter the IP address of the PC that has MIB Builder and MG-SOFT MIB Browser installed, and leave other parameters to the default.

Table 6-16 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.  You can enter number, letter, underline and dash to form the name.
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.
Read-only Username	Set the read-only username accessing device, and it is public by default.  You can enter number, letter, and underline to form the name.
Read/Write Username	Set the read/write username access device, and it is private by default.  You can enter number, letter, and underline to form the name.
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 generated modules with MG-SOFT MIB Browser.
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, and then you can view the configuration information, video channel amount, audio channel amount, and software version.



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

6.3.8 Bonjour

Enable this function, and the OS and clients that support Bonjour would find the camera automatically. You can have quick visit to the camera with Safari browser.



Bonjour is enabled by default.

Procedure

Step 1 Select > **Network** > **Bonjour**.

Figure 6-34 Bonjour



Step 2 Click , and then configure server name.

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 interface.

6.3.9 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 (224.0.1.0–238.255.255.255) for the camera and adopt the multicast protocol.

Step 1 Select > **Network** > **Multicast**.

Figure 6-35 Multicast



Step 2 Click , and enter IP address and port number.

Table 6-17 Description of multicast parameters

Parameter	Description
Multicast 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.
Port	The multicast port of corresponding stream: Main Stream : 40000; Sub Stream1 : 40016; Sub Stream2 : 40032, and all the range is 1025–65500.

Step 3 Click **Apply**.

Result

On the **Live** interface, select **RTSP** in **Multicast**, and then you can view the video image with multicast protocol.

6.3.10 Register

After you enable this function, when the camera is connected into Internet, it will report the current location to the specified server which acts as the transit to make it easier for the client software to access the camera.

Step 1 Select > **Network** > **Register**.

Figure 6-36 Register

Step 2 Click , and then configure server name.

Table 6-18 Description of register parameters

Parameter	Description
Server Address	The IP address or domain name of the server to be registered.
Port	The port for registration.
Sub-Device ID	The custom ID for the camera.

Step 3 Click **Apply**.

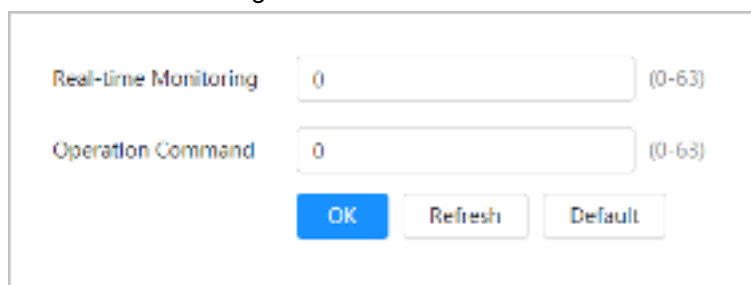
6.3.11 QoS

You can solve problems such as network delay and congestion with this function. It helps to assure bandwidth, reduce transmission delay, packet loss rate, and delay jitter to improve experience.

0–63 means 64 degrees of priority; 0 for the lowest and 63 the highest.

Step 1 Select  > **Network** > **QoS**.

Figure 6-37 QoS



The interface shows two input fields: 'Real-time Monitoring' and 'Operation Command', both with a value of '0' and a range of '(0-63)'. Below the fields are three buttons: 'OK' (blue), 'Refresh' (grey), and 'Default' (grey).

Step 2 Configure QoS parameters.

Table 6-19 Description of QoS parameters

Parameter	Description
Realtime Monitor	Configure the priority of the data packets that used for network surveillance. 0 for the lowest and 63 the highest.
Command	Configure the priority of the data packets that used for configure or checking.

Step 3 Click **Save**.

6.3.12 Platform Access

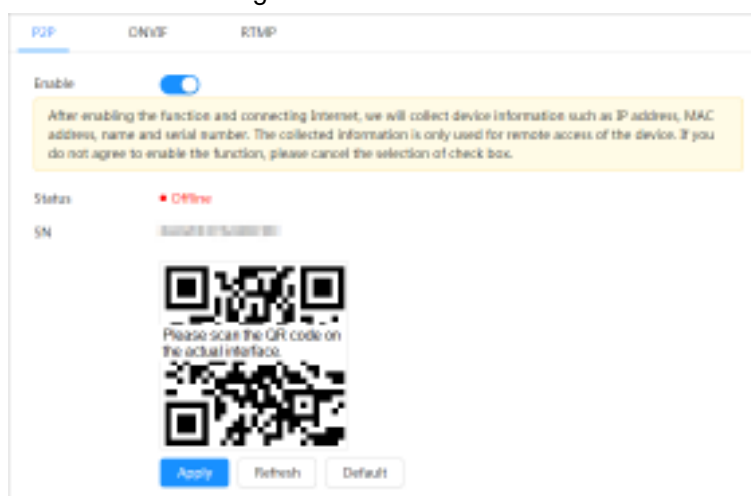
6.3.12.1 P2P

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 smartphone, and then you can add and manage more devices on the mobile phone client.

Step 1 Select  > **Network** > **Platform Access** > **P2P**.

Figure 6-38 P2P



The interface shows the 'P2P' tab selected. There is an 'Enable' toggle switch which is turned on. Below it is a yellow warning box: 'After enabling the function and connecting Internet, we will collect device information such as IP address, MAC address, name and serial number. The collected information is only used for remote access of the device. If you do not agree to enable the function, please cancel the selection of check box.' Below the warning box, the status is shown as 'Offline' with a red dot. The 'SN' field is empty. A large QR code is displayed with the text 'Please scan the QR code on the actual interface.' Below the QR code are three buttons: 'Apply' (blue), 'Refresh' (grey), and 'Default' (grey).

- When P2P is enabled, remote management on device is supported.
- 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.

Step 2 Log in to mobile phone client and tap **Device management**.

Step 3 Tap **+** at the upper-right corner.

Step 4 Scan the QR code on the **P2P** interface.

Step 5 Follow the instructions to finish the settings.

6.3.12.2 ONVIF

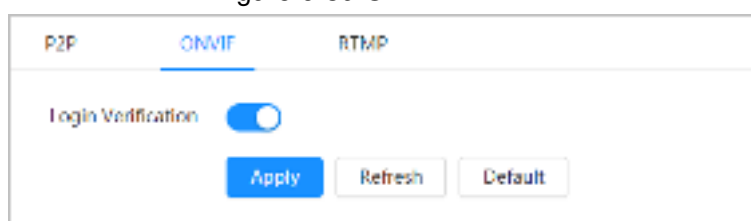
The ONVIF verification is enabled by default, which allows the network video products (including video recording device and other recording devices) from other manufacturers to connect to your device.



ONVIF is enabled by default.

Step 1 Select  > **Network** > **Platform Access** > **ONVIF**.

Figure 6-39 ONVIF



Step 2 Click  next to **ONVIF Verification**.

Step 3 Click **Apply**.

6.3.12.3 RTMP

Through RTMP, you can access a third-party platform (such as Ali and YouTube) 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 Select  > **Network** > **Platform Access** > **RTMP**.

Figure 6-40 RTMP

Step 2 Click .



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

Step 3 Configure RTMP parameters.

Table 6-20 Description of RTMP parameters

Parameter	Description
Stream Type	The stream 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	<ul style="list-style-type: none"> 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. <ul style="list-style-type: none"> IP address: Support IPv4 or domain name. Port: Keep the default value.
Port	
Custom Address	When selecting Custom , you need to enter the path allocated by the server.

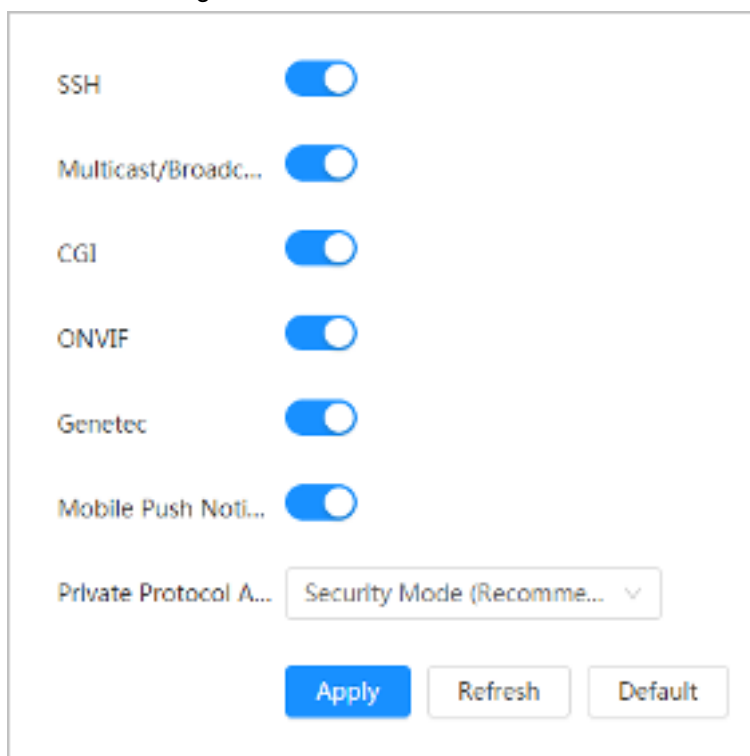
Step 4 Click **Apply**.

6.3.13 Basic Service

Configure the IP hosts (devices with IP address) that are allowed to visit the device. Only the hosts in the trusted sites list can log in to the web interface. This is to enhance network and data security.

Step 1 Select > **Network** > **Basic Service**.

Figure 6-41 Basic service



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

Table 6-21 Description of basic service parameters

Function	Description
SSH	You can enable SSH authentication to perform safety management.
Multicast/Broadcast Search	Enable this function, and then when multiple users are viewing the device video image simultaneously through network, they can find your device with multicast/broadcast protocol.
CGI	Enable the function, and then other devices can access through this service. The function is enabled by default.
Onvif	
Genetec	
Mobile Push Notification	Enable this function, and then the system will send the snapshot that was taken when alarm is triggered to your phone, this is enabled by default.
Private Protocol Authentication Mode	Select the authentication mode from Security Mode and Compatible Mode . Security mode is recommended.

Step 3 Click **Apply**.

6.4 Event

6.4.1 Setting Alarm Linkage

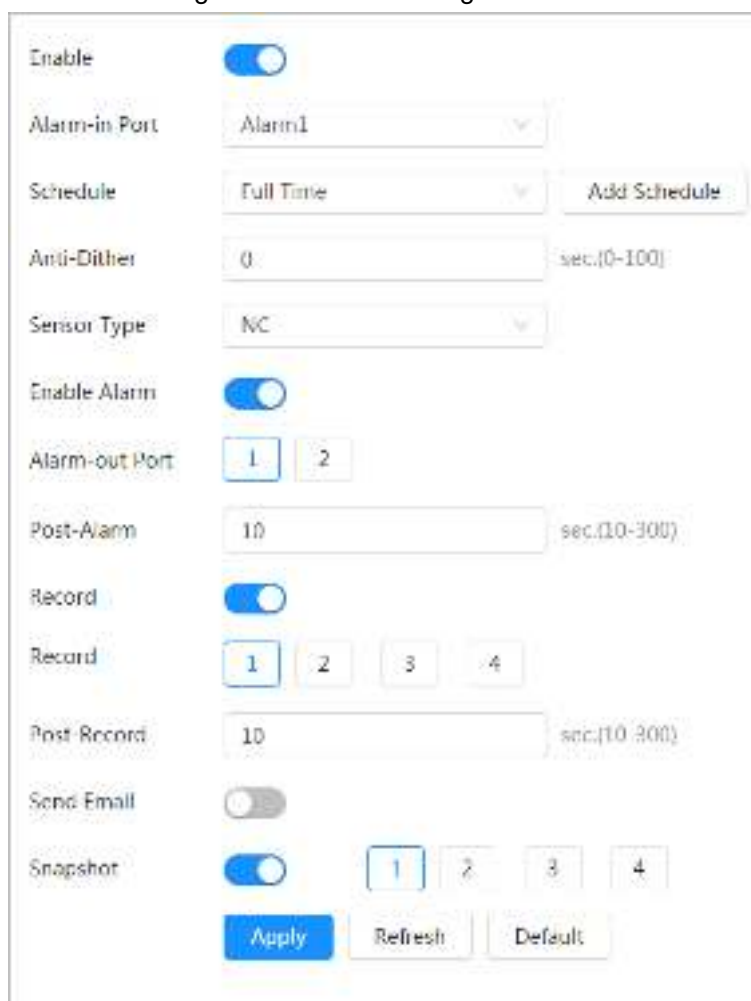
6.4.1.1 Setting Alarm-in

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

Step 1 Select  > **Event** > **Alarm**.

Step 2 Click  next to **Enable** to enable alarm linkage.

Figure 6-42 Alarm linkage



The screenshot shows the 'Alarm Linkage' configuration page. It features a list of settings on the left and their corresponding values on the right. The 'Enable' toggle is turned on. 'Alarm-in Port' is set to 'Alarm1'. 'Schedule' is set to 'Full Time' with an 'Add Schedule' button. 'Anti-Dither' is set to '0' with a range of 'sec.(0-100)'. 'Sensor Type' is set to 'NC'. 'Enable Alarm' is turned on. 'Alarm-out Port' has buttons for '1' and '2'. 'Post-Alarm' is set to '10' with a range of 'sec.(10-300)'. 'Record' is turned on. 'Record' has buttons for '1', '2', '3', and '4'. 'Post Record' is set to '10' with a range of 'sec.(10-300)'. 'Send Email' is turned off. 'Snapshot' is turned on. At the bottom, there are 'Apply', 'Refresh', and 'Default' buttons.

Step 3 Select an alarm-in port and a sensor type.

- Sensor Type: NO or NC.
- Anti-Dither: Only record one alarm event during the anti-dither period.

Step 4 Select the schedule and arming periods and alarm linkage action. For details, see "6.4.1.2 Alarm Linkage".

If the existing schedules cannot meet the scene requirement, you can click **Add Schedule** to add new schedule. For details, see "6.4.1.2.1 Adding Schedule".

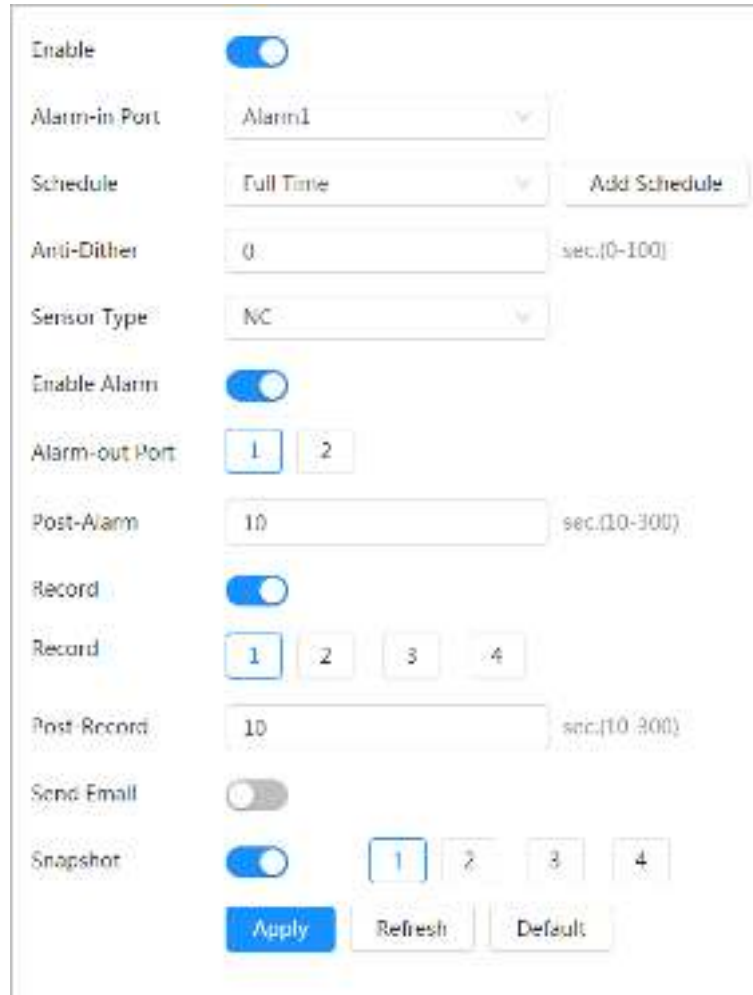
Step 5 Click **Apply**.

6.4.1.2 Alarm Linkage

When configuring alarm events, select alarm linkages (such as record, snapshot). When the corresponding alarm is triggered in the configured arming period, the system will alarm.

Select  > **Event** > **Alarm**, and then click  next to **Enable** to enable alarm linkage.

Figure 6-43 Alarm linkage



The screenshot shows the 'Alarm Linkage' configuration page. It features several settings:

- Enable:** A toggle switch that is currently turned on (blue).
- Alarm-in Port:** A dropdown menu showing 'Alarm1'.
- Schedule:** A dropdown menu showing 'Full Time' and an 'Add Schedule' button.
- Anti-Dither:** A text input field with '0' and a range indicator 'sec.(0-100)'.
- Sensor Type:** A dropdown menu showing 'NC'.
- Enable Alarm:** A toggle switch that is currently turned on (blue).
- Alarm-out Port:** Two buttons labeled '1' and '2', with '1' selected.
- Post-Alarm:** A text input field with '10' and a range indicator 'sec.(10-300)'.
- Record:** A toggle switch that is currently turned on (blue).
- Record:** Four buttons labeled '1', '2', '3', and '4', with '1' selected.
- Post Record:** A text input field with '10' and a range indicator 'sec.(10-300)'.
- Send Email:** A toggle switch that is currently turned off (grey).
- Snapshot:** A toggle switch that is currently turned on (blue).
- Snapshot:** Four buttons labeled '1', '2', '3', and '4', with '1' selected.

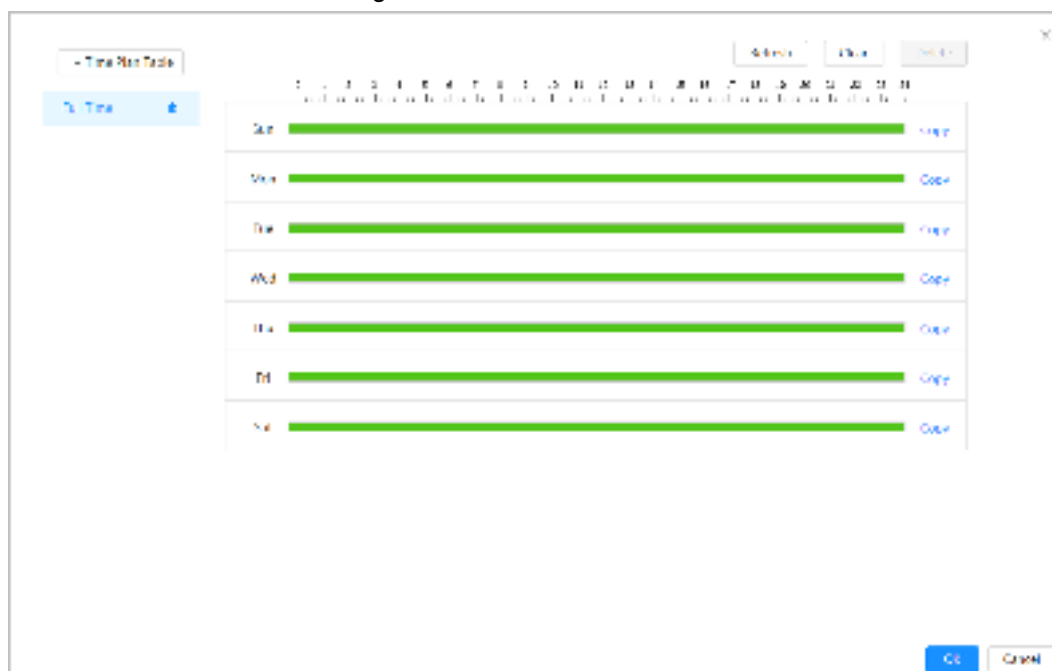
At the bottom of the form, there are three buttons: 'Apply' (blue), 'Refresh' (grey), and 'Default' (grey).

6.4.1.2.1 Adding Schedule

Set arming periods. The system only performs corresponding linkage action in the configured period.

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

Figure 6-44 Schedule




Step 2 Press and drag the left mouse button on the timeline to set arming periods. Alarms will be triggered in the time period in green on the timeline.

- Click **Copy** next to a day, and select the days that you want to copy to in the prompt interface, you can copy the configuration to the selected days. Select the **Select All** check box to select all days to copy the configuration.
- You can set 6 time periods per day.

Step 3 Click **Apply**.

Step 4 (Optional) Click **Time Plan Table** to add a new time plan table.

You can:

- Double-click the table name to edit it.
- Click  to delete the table as needed.


6.4.1.2.2 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

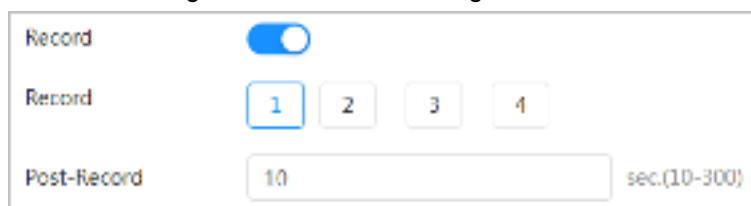
- After the corresponding alarm type (**Normal**, **Motion**, or **Alarm**) is enabled, the record channel links recording. For details, see "13.3 Setting Record Plan".
- Enable auto record mode, the record linkage will take effect. For details, see "13.2 Setting Record Control".

Setting Record Linkage

On the **Alarm** interface, click  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 6-45 Record linkage



6.4.1.2.3 Snapshot Linkage

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

Prerequisites

After the corresponding alarm type (Normal, Motion, or Alarm) is enabled, the snapshot channel links capturing picture. For details, see "13.3 Setting Record Plan".

Setting Record Linkage




On the **Alarm** interface, click  to enable snapshot linkage, and select the channel as needed.

Figure 6-46 Snapshot linkage



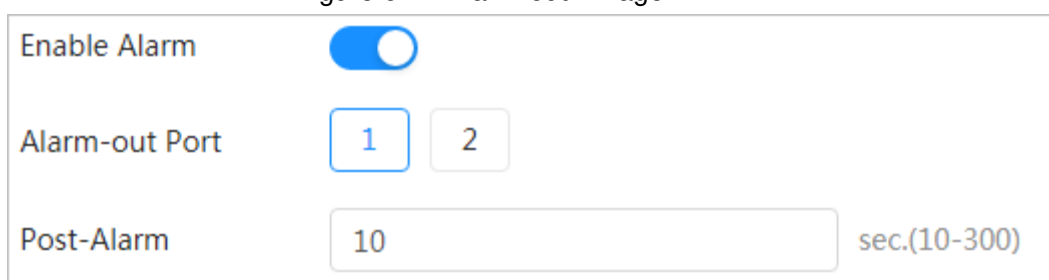
6.4.1.2.4 Alarm-out Linkage

When an alarm is triggered, the system can automatically link with alarm-out device.

On the **Alarm** interface, click  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.

Figure 6-47 Alarm-out linkage



6.4.1.2.5 Email Linkage

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

Email linkage takes effect only when SMTP is configured. For details, see "6.3.5 Email".

Figure 6-48 Email linkage



6.4.1.3 Subscribing Alarm

6.4.1.3.1 About Alarm Types

For alarm types and preparations of alarm events, see Table 6-22.

Table 6-22 Description of alarm types

Alarm Type	Description	Preparation
Motion Detection	The alarm is triggered when moving object is detected.	Motion detection is enabled. For details, see "6.4.3.1 Setting Motion Detection".
Disk Full	The 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 "6.4.2.1 Setting SD Card Exception".
Disk Error	The alarm is triggered when there is failure or malfunction in the SD card.	SD card failure detection is enabled. For details, see "6.4.2.1 Setting SD Card Exception".
Video Tampering	The alarm is triggered when the camera lens is covered or there is defocus in video images.	Video tampering is enabled. For details, see "6.4.3.2 Setting Video Tampering".
External Alarm	The alarm is triggered when there is external alarm input.	The device has alarm input port and external alarm function is enabled. For details, see "6.4.1.1 Setting Alarm-in".
Audio Detection	The alarm is triggered when there is audio connection problem.	Abnormal audio detection is enabled. For details, see "6.4.4 Setting Audio Detection".
IVS	The alarm is triggered when intelligent rule is triggered.	Enable IVS, crowd map, face detection or people counting, and other intelligent functions.
Scene Changing	The alarm is triggered when the device monitoring scene changes.	Scene changing detection is enabled. For details, see "6.4.3.3 Setting Scene Changing".
Voltage Detection	The alarm is triggered when the device detects abnormal voltage input.	Voltage detection is enabled. For details, see "6.4.2.3 Setting Voltage Detection".
Security Exception	The alarm is triggered when the device detects malicious attack.	Voltage detection is enabled. For details, see "12.1 Security Status".

6.4.1.3.2 Subscribing Alarm Information

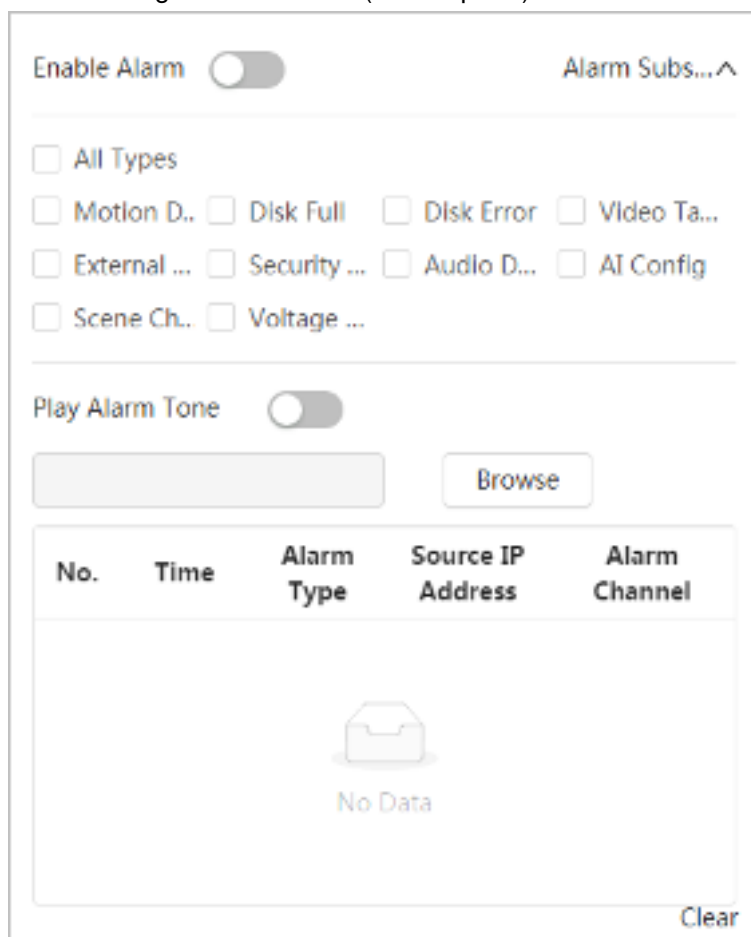
You can subscribe alarm event. When a subscribed alarm event is triggered, the system records detailed alarm information at the right side of the interface.



Functions of different devices might vary, and the actual product shall prevail.

Step 1 Click  at the right-upper corner of the main interface.

Figure 6-49 Alarm (subscription)



Enable Alarm ☐

Alarm Subs...^


☐ All Types

☐ Motion D. ☐ Disk Full ☐ Disk Error ☐ Video Ta...

☐ External ... ☐ Security ... ☐ Audio D... ☐ AI Config



☐ Scene Ch.. ☐ Voltage ...

Play Alarm Tone ☐

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

Step 2 Click ☐ next to **Enable Alarm**.

Step 3 Select alarm type according to the actual need. For details, see "6.4.1.3.2 Subscribing Alarm Information".

The system prompts and records alarm information according to actual conditions. When the subscribed alarm event is triggered and the alarm subscription interface 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.

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.

6.4.2 Setting Exception

Abnormality includes SD card, network, illegal access, voltage detection, and security exception.



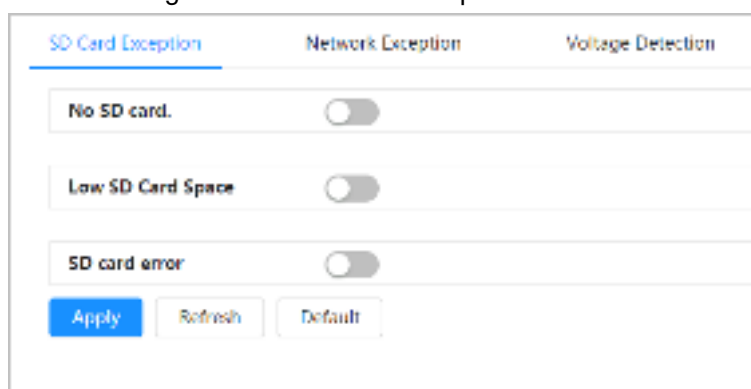
Only the device with SD card has the abnormality functions, including **No SD Card**, **SD Card Error**, and **Capacity Warning**.


6.4.2.1 Setting 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, and the actual interface shall prevail.

Step 1 Select  > **Event** > **Exception** > **SD Card Exception**.

Figure 6-50 SD card exception



Step 2 Click  to enable the SD card detection functions.

When enabling **Low SD Card Space**, set **Capacity Limit**. When the remaining space of SD card is less than this value, the alarm is triggered.

Step 3 Set alarm linkage actions. For details, see "6.4.1.2 Alarm Linkage".

Step 4 Click **Apply**.

6.4.2.2 Setting Network Exception

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

Step 1 Select  > **Event** > **Exception** > **Network Exception**.

Figure 6-51 Network exception

SD Card Exception
Network Exception
Voltage Detection

Offline
☒

Enable Alarm
☐

Alarm-out Port

1

2

Post Alarm

10

sec.(10-300)

Record
☐

Record

1

2

3

4

Post Record

10

sec.(10-300)

IP Conflict
☒

Enable Alarm
☐

Alarm-out Port

1

2

Post Alarm

10

sec.(10-300)

Record
☐

Record

1

2

3

4

Post Record

10

sec.(10-300)

Apply

Refresh

Default

Step 2 Click ☐ to enable the network detection function.

Step 3 Set alarm linkage actions. For details, see "6.4.1.2 Alarm Linkage".

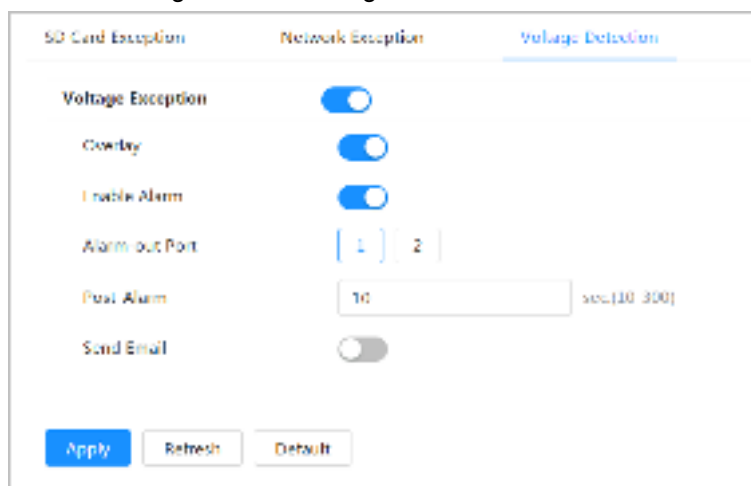
Step 4 Click **Apply**.


6.4.2.3 Setting Voltage Detection

When the input voltage is higher than or lower than the rated value of the device, the system performs alarm linkage.

Step 1 Select  > **Event** > **Exception** > **Voltage Detection**.

Figure 6-52 Voltage detection



- Step 2** Click  to enable the voltage detection function.
When enabling **Overlay**, the alarm icon is displayed by overlapping when the alarm is triggered.
- Step 3** Set alarm linkage actions. For details, see "6.4.1.2 Alarm Linkage".
- Step 4** Click **Apply**.

6.4.3 Setting 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.

6.4.3.1 Setting 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 Select  > **Event** > **Video Detection** > **Motion Detection**.

Figure 6-53 Motion detection

Step 2 Click to enable the motion detection function.

Step 3 Set the area for motion detection.

1) Click **Setting** next to **Area**.

Figure 6-54 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**.

- Select a color on 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 whole video image is the effective area for Motion Detection by default.
- 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.

3) Click **OK**.

Step 4 Set arming periods and alarm linkage action. For details, see "6.4.1.2 Alarm Linkage". If the exiting schedules cannot meet the scene requirement, you can click **Add Schedule** to add a new schedule. For details, see "6.4.1.2.1 Adding Schedule". Anti-dither: After the **Anti-dither** time is set, the system only records one motion detection event in the period.

Step 5 Click **Apply**.

6.4.3.2 Setting Video Tampering

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

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

Figure 6-55 Video tampering

Step 2 Click next to **Video Tampering**, and set arming periods and alarm linkage action. For details, see "6.4.1.2 Alarm Linkage".

If the exiting schedules cannot meet the scene requirement, you can click **Add Schedule** to add a new schedule. For details, see "6.4.1.2.1 Adding Schedule".

Step 3 Click next to **Defocus Detection**: The alarm is triggered when the image is fuzzy.



This function is available on some select models.

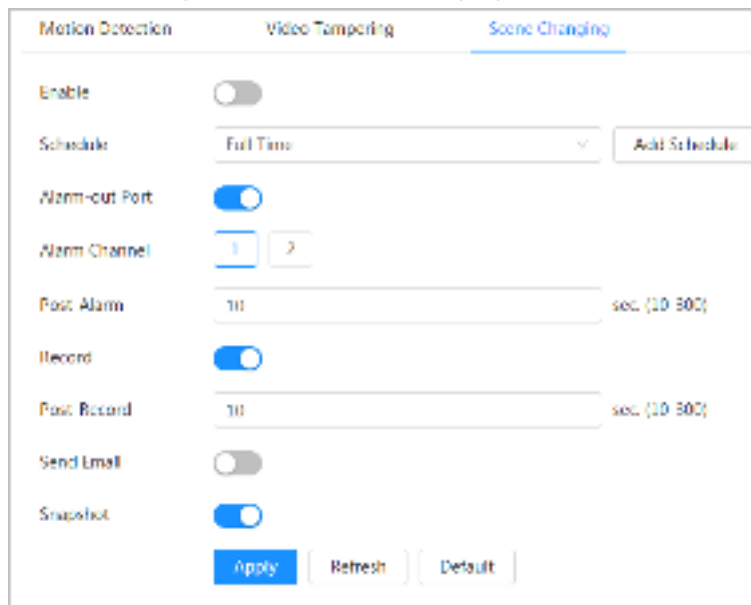
Step 4 Click **Apply**.

6.4.3.3 Setting Scene Changing

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

Step 1 Select  > **Event > Video Detection > Scene Changing.**

Figure 6-56 Scene changing



Step 2 Select the schedule and arming periods and alarm linkage action. For details, see "6.4.1.2 Alarm Linkage".

If the exiting schedules cannot meet the scene requirement, you can click **Add Schedule** to add a new schedule. For details, see "6.4.1.2.1 Adding Schedule".

Step 3 Click **Apply**.

6.4.4 Setting Audio Detection

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

Step 1 Select  > **Event > Video Detection > Audio Detection.**

Figure 6-57 Audio detection



Step 2 Set parameters.

- Input abnormal: Click ☐ next to **Audio Abnormal**, and the alarm is triggered when the system detects abnormal sound input.
- 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.

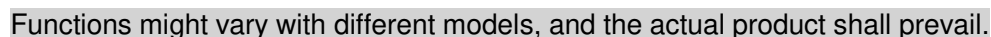
Step 3 Select the schedule and arming periods and alarm linkage action. For details, see "6.4.1.2 Alarm Linkage".

If the existing schedules cannot meet the scene requirement, you can click **Add Schedule** to add a new schedule. For details, see "6.4.1.2.1 Adding Schedule".

Step 4 Click **Apply**.

6.5 Storage

Display the 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.



- 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.

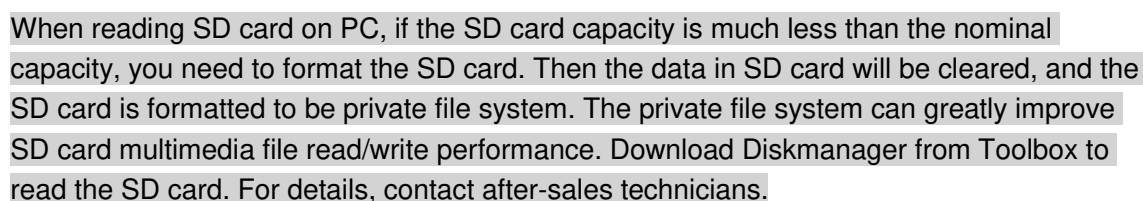


Figure 6-58 Local



6.6 System

This section introduces system configurations, including general, date & time, account, safety, PTZ settings, default, import/export, remote, auto maintain and upgrade.

6.6.1 General

6.6.1.1 Basic

You can configure device name, language and video standard.

Step 1 Select  > **System** > **General** > **Basic**.

Figure 6-59 Basic

Basic

Date & Time

Device Name

Video Standard

PAL

Apply

Refresh

Default

Step 2 Configure general parameters.

Table 6-23 Description of general parameters

Parameter	Description
Name	Enter the device name.

Parameter	Description
Video Standard	Select video standard from PAL and NTSC .

Step 3 Click **Apply**.

6.6.1.2 Date & Time

You can configure date and time format, time zone, current time, DST (Daylight Saving Time) or NTP server.


Step 1 Select > **System** > **General** > **Date & Time**.

Figure 6-60 Date and time

Step 2 Configure date and time parameters.

Table 6-24 Description of date and time parameters

Parameter	Description
Date Format	Configure the date format.
Time	<ul style="list-style-type: none"> Manually Setting: Configure the parameters manually. NTP: When selecting NTP, the system then syncs time with the internet server in real time. You can also enter the IP address, time zone, port, and interval of a PC which installed NTP server to use NTP.
Time Format	Configure the time format. You can select from 12-Hour or 24-Hour .
Time Zone	Configure the time zone that the camera is at.

Parameter	Description
Current Time	Configure system time. Click Sync PC , and the system time changes to the PC time.
DST	Enable DST as needed. Click  , and configure start time and end time of DST with Date or Week .

Step 3 Click **Apply**.

6.6.2 Account

You can manage users, such as add, delete, or edit them. Users include admin, added users and ONVIF users.

Managing users and groups are only available for administrator users.

- The max length of the user or group name is 31 characters which consists of number, letter, underline, dash, dot and @.
- 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 ' " ; : &).
- You can have 18 users and 8 groups at most.
- You can manage users through single user or group, and duplicate usernames or group names are not allowed. A user can only be in one group at a time, and the group users can own authorities within group authority range.
- Online users cannot edit their own authority.
- There is one admin by default which has highest authority.
- Select **Anonymous Login**, and then log in with only IP address instead of username and password. Anonymous users only have preview authorities. During anonymous login, click **Logout**, and then you can log in with other username.

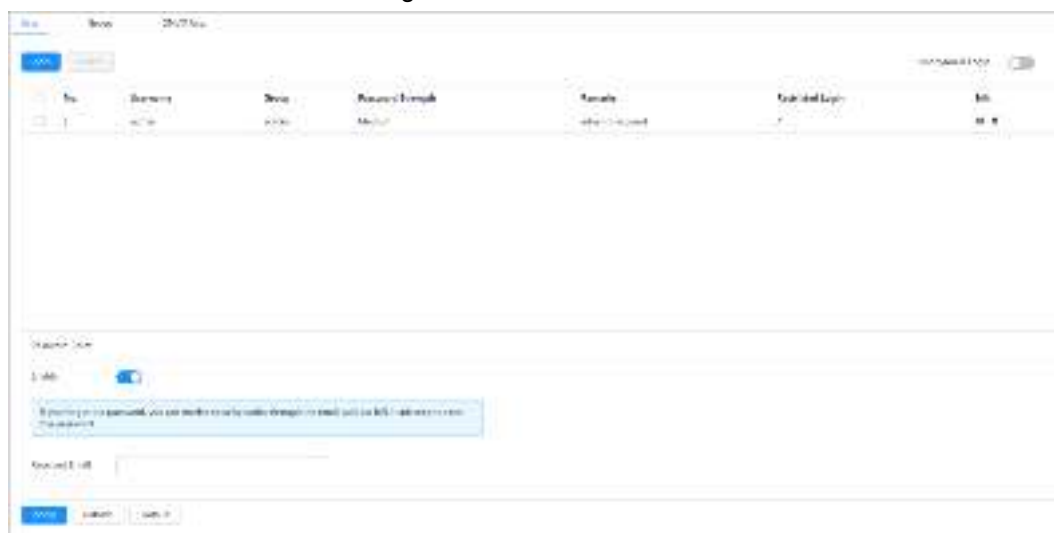
6.6.2.1 User

6.6.2.1.1 Adding User

You are admin user by default. You can add users, and configure different permissions.

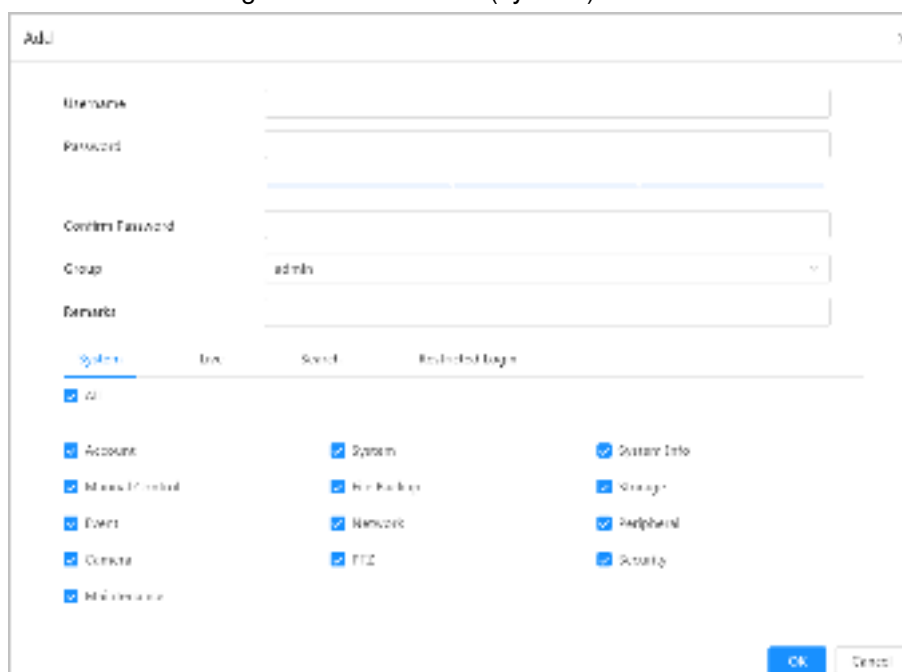
Step 1 Select  > **System** > **Account** > **User**.

Figure 6-61 User



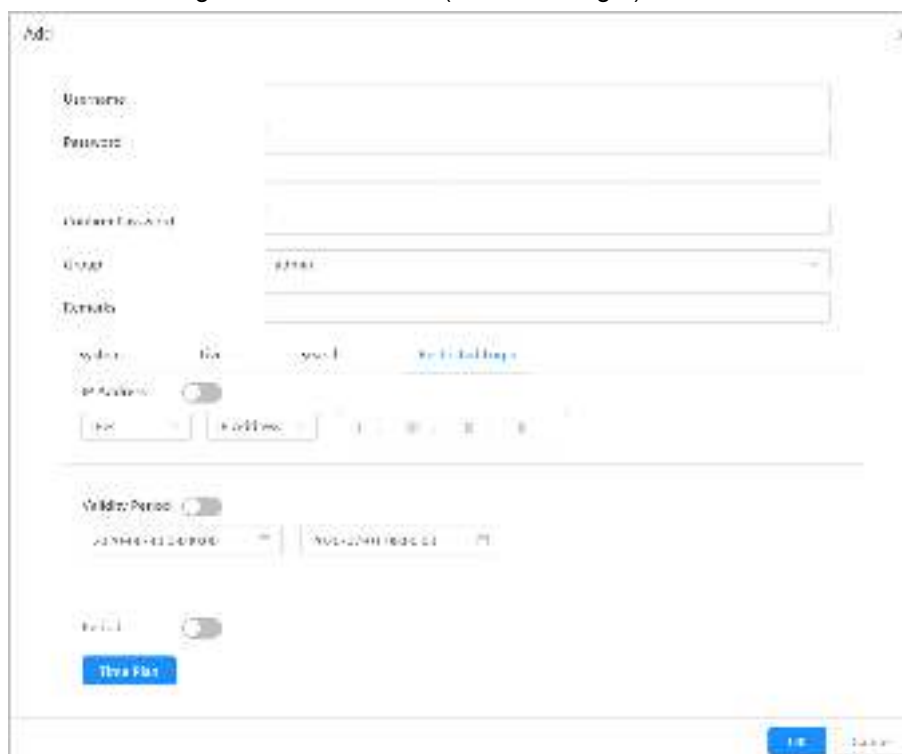
Step 2 Click **Add**.

Figure 6-62 Add user (system)




System		
System	System Info	Storage
<input checked="" type="checkbox"/> All	<input checked="" type="checkbox"/> System	<input checked="" type="checkbox"/> System Info
<input checked="" type="checkbox"/> Account	<input checked="" type="checkbox"/> File Backup	<input checked="" type="checkbox"/> Storage
<input checked="" type="checkbox"/> Manual Download	<input checked="" type="checkbox"/> Network	<input checked="" type="checkbox"/> Peripheral
<input checked="" type="checkbox"/> Event	<input checked="" type="checkbox"/> P2P	<input checked="" type="checkbox"/> Activity
<input checked="" type="checkbox"/> Control		
<input checked="" type="checkbox"/> Initialization		

Figure 6-63 Add user (restricted login)



Step 3 Configure user parameters.

Table 6-25 Description of user parameters (1)

Parameter	Description
Username	User's unique identification. You cannot use existed username.
Password	Enter password and confirm it again.
Confirm 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 ' " ; : &).
Group	The group that users belong to. Each group has different authorities.
Remark	Describe the user.
System	Select authorities as needed.  It is recommended to give fewer authorities to normal users than premium users.
Live	Select the live view authority for the user to be added.
Search	Select the search authority for the user to be added.

Parameter	Description
Restricted Login	<p>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 the web interface with the defined IP in the defined time range of validity period.</p> <ul style="list-style-type: none"> 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. <p>Set as follows</p> <ol style="list-style-type: none"> 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.

Step 4 Click **Apply**.

The newly added user is displayed in the username list.

Related Operations

- click to edit password, group, memo or authorities.



For admin account, you can only edit the password.

- Click to delete the added users. Admin user cannot be deleted.



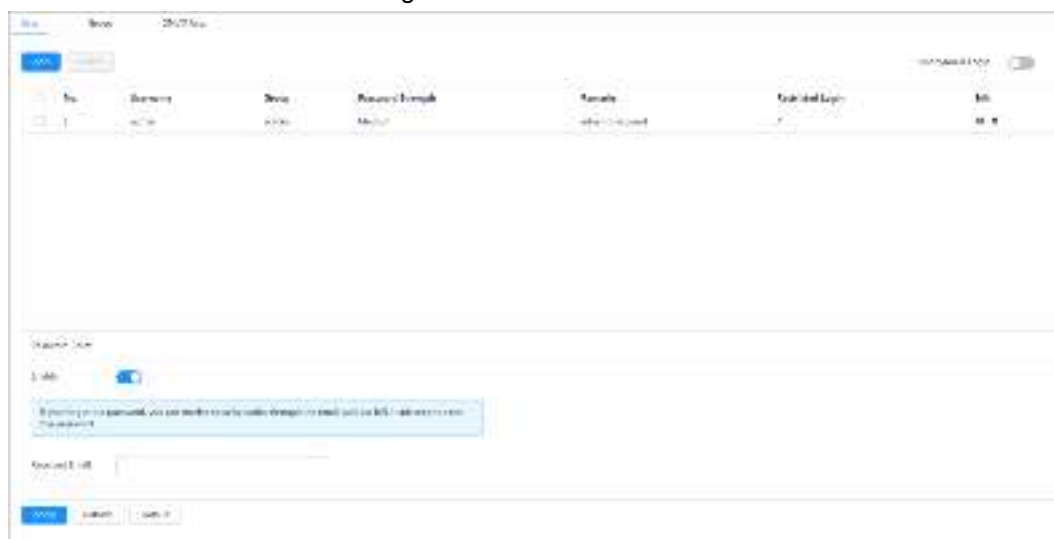
The admin account cannot be deleted.

6.6.2.1.2 Resetting Password

Enable the function, and you can reset password by clicking **Forget password?** on the login interface. For details, see "4.2 Resetting Password".

Step 1 Select > **System** > **Account** > **User**.

Figure 6-64 User



Step 2 Click next to **Enable** in **Password Reset**.

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

camera.

Step 3 Enter the reserved email address.

Step 4 Click **Apply**.

6.6.2.2 Adding User Group

You have two groups named admin and user by default, and you can add new group, delete added group or edit group authority and memo.

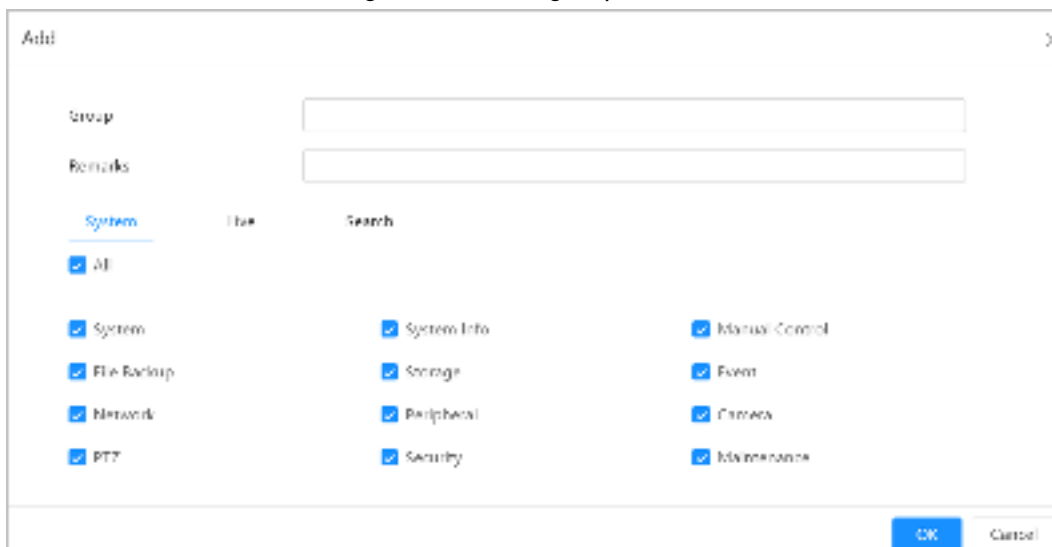
Step 1 Select  > **System** > **Account** > **Group**.

Figure 6-65 Group name



Step 2 Click **Add**.

Figure 6-66 Add group





Step 3 Enter the group name and memo, and then select group authorities.

Step 4 Click **OK** to finish configuration.

The newly added group displays in the group name list.

Related Operations

- click  to edit password, group, memo or authorities.
- Click  to delete the added users. Admin user cannot be deleted.



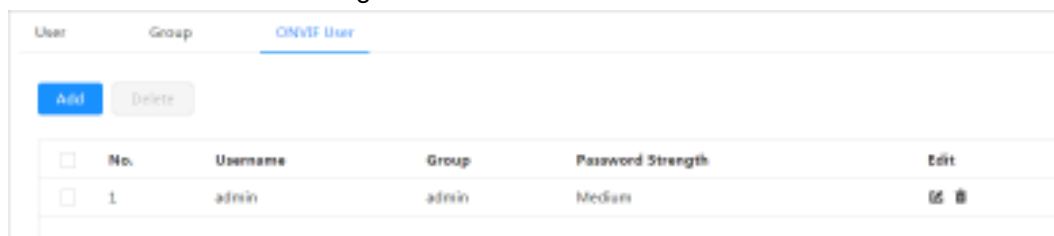
The admin group and user group cannot be deleted.

6.6.2.3 ONVIF User

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

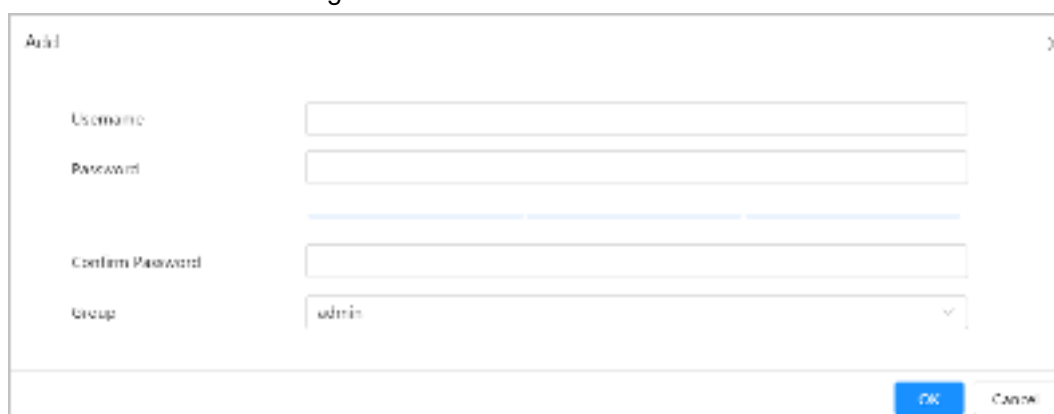
Step 1 Select  > **System** > **Account** > **ONVIF User**.

Figure 6-67 ONVIF user



Step 2 Click **Add**.

Figure 6-68 Add ONVIF user



Step 3 Configure user parameters.

Table 6-26 Description of ONVIF user parameters

Parameter	Description
Username	User's unique identification. You cannot use existed username.
Password	Enter password and confirm it again.
Confirm 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 ' " ; : &).
Group Name	The group that users belong to. Each group has different authorities.

Step 4 Click **OK**.

The newly added user displays in the username list.

Related Operations

- click  to edit password, group, memo or authorities.



For admin account, you can only edit the password.

- Click  to delete the added users. Admin user cannot be deleted.



The admin account cannot be deleted.

6.6.3 Manager

6.6.3.1 Requirements

To make sure the system runs normally, maintain it as the following requirements:

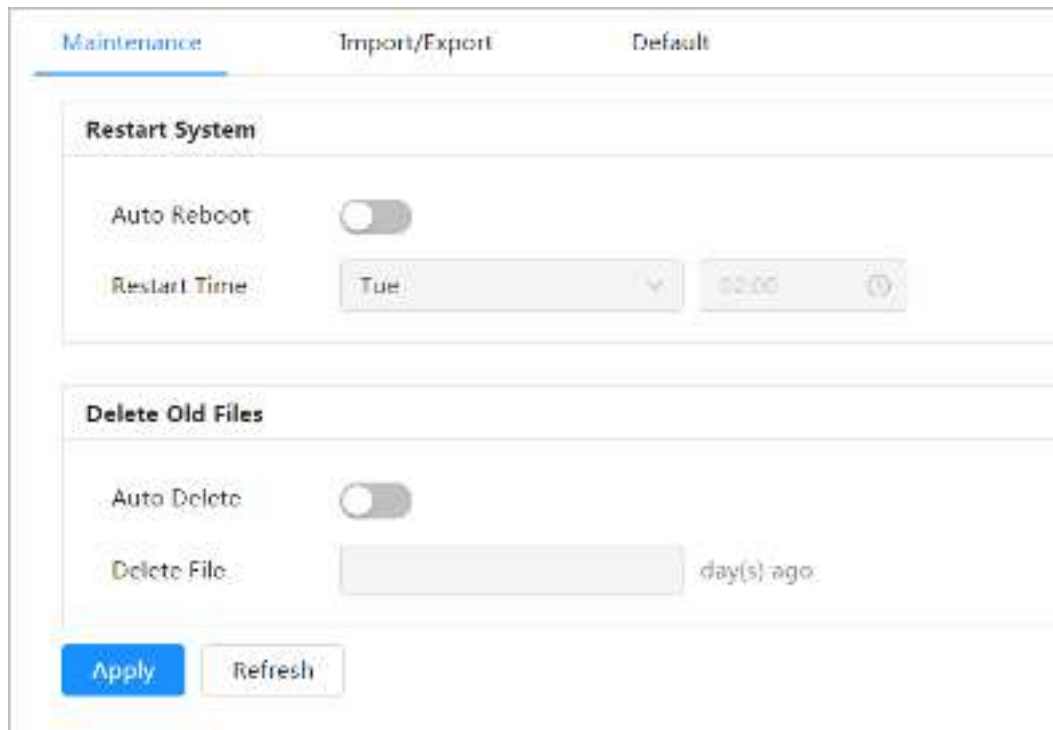
- Check surveillance images regularly.
- Clear regularly user and user group information that are not frequently used.
- Change the password every three months. For details, see "6.6.2 Account".
- View system logs and analyze them, and process the abnormality in time.
- Back up the system configuration regularly.
- Restart the device and delete the old files regularly.
- Upgrade firmware in time.

6.6.3.2 Maintenance



You can restart the system manually, and set the time of auto reboot and auto deleting old files. This function is disabled by default.

Step 1 Select  > **System > Manager > Maintenance**.

Figure 6-69 Maintenance



Step 2 Configure auto maintain parameters.

- Click  next to **Auto Reboot** in **Restart System**, and set the reboot time, the system automatically restarts as the set time every week.
- Click  next to **Auto Delete** in **Delete Old Files**, and set the time, the system automatically deletes old files as the set time. The time range is 1 to 31 days.



When you enable and confirm the **Auto Delete** function, the deleted files cannot be restored. Operate it carefully.

Step 3 Click **Apply**.

6.6.3.3 Import/Export

- Export the system configuration file to back up the system configuration.
- Import system configuration file to make quick configuration or recover system configuration.

Step 1 Select > **System** > **Manager** > **Import/Export**.

Figure 6-70 Import/Export



Step 2 Import and export.

- Import: Select local configuration file, and click **Import File** to import the local system configuration file to the system.
- Export: Click **Export Configuration file** to export the system configuration file to local storage.

6.6.3.4 Default

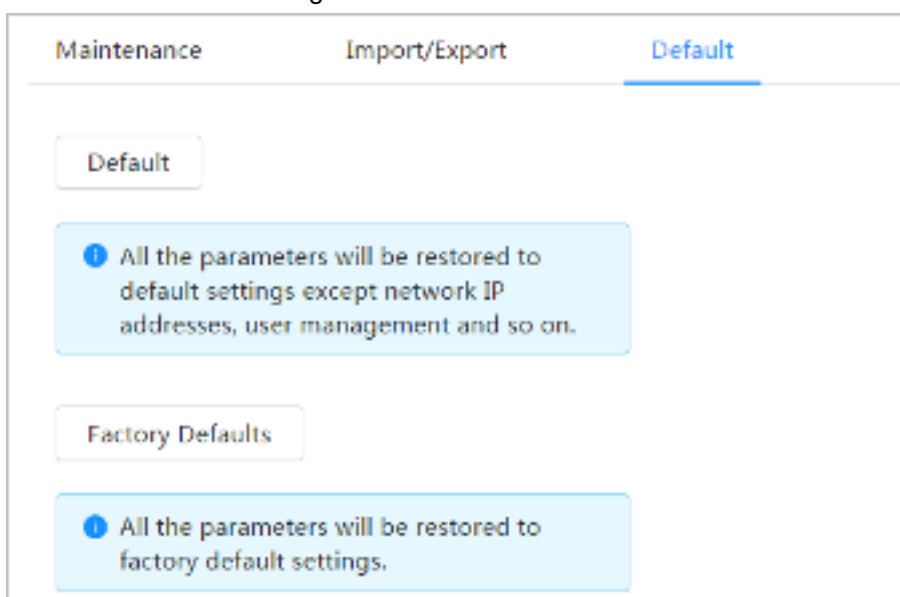
Restore the device to default configuration or factory settings.

This function will restore the device to default configuration or factory setting.

Select > **System** > **Manager** > **Default**

- Click **Default**, and then all the configurations except IP address and account are reset to default.
- Click **Factory Default**, and all the configurations are reset to factory settings.

Figure 6-71 Default



6.6.4 Upgrade

Upgrading to the latest system can refine camera functions and improve stability. If wrong upgrade file has been used, restart the device; otherwise some functions might not work properly.


Step 1 Select  > **System** > **Upgrade**.

Figure 6-72 Upgrade




Step 2 Click **Browse**, and then upload upgrade file.
The upgrade file should be a .bin file.

Step 3 Click **Upgrade**.
The upgrade starts.


6.7 System Information

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

6.7.1 Version

Select  > **System Info** > **Version** to view device information such as hardware, system version, and web version.

6.7.2 Online User

Select  > **System Info** > **Online User** to view all the current users logging in to web.

6.8 Setting Log

6.8.1 Log

You can view and back up logs.

Step 1 Select  > **Log** > **Log**.

Step 2 Configure **Start Time** and **End Time**, and then select the log type.

The start time should be later than January 1st, 2000, and the end time should be earlier than December 31, 2037.

The log type includes All, System, Setting, Data, Event, Record, Account, and Safety.

- **System**: Includes program start, abnormal close, close, program reboot, device closedown, device reboot, system reboot, and system upgrade.
- **Setting**: Includes saving configuration and deleting configuration file.
- **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.

Step 3 Click **Search**.

















- Click  or click a certain log, and then you can view the detailed information in **Details** area.
- Click **Backup**, and then you can back up all found logs to local PC.


Figure 6-73 Log

Start Time		2020-06-29 11:43:32 - 2020-06-30 11:43:32	Type	All	Search	Backup
No.	Time	Username	Type	Details		
1	2020-06-30 11:30:52	admin	Login			
2	2020-06-30 11:26:50	admin	Login			
3	2020-06-30 11:23:13	admin	Logout			
4	2020-06-30 11:23:08	admin	Logout			
5	2020-06-30 11:19:22	admin	Save Config			
6	2020-06-30 11:16:22	admin	Login			
7	2020-06-30 11:15:05	admin	Logout			
8	2020-06-30 11:14:34	admin	Login			
9	2020-06-30 11:10:52	admin	Zoom & Focus			
10	2020-06-30 11:08:25	admin	Zoom & Focus			
11	2020-06-30 11:07:08	admin	Zoom & Focus			
12	2020-06-30 11:07:08	admin	Login			
13	2020-06-30 11:05:46	admin	Zoom & Focus			
14	2020-06-30 11:03:39	admin	Login			
15	2020-06-30 11:01:20	admin	Logout			
171 record(s)					<div> <div><</div> <div>1</div> <div>2</div> <div>></div> <div>Goto</div> <div></div> </div>	

6.8.2 Remote Log

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


Step 1 Select  > **Log** > **Remote Log**.

Step 2 Click  to enable remote log function.

Step 3 Set address, port and device number.

Step 4 Click **Apply**.

Figure 6-74 Remote log

Enable		
Server Address	<input type="text" value="192.168.1.100"/>	
Port	<input type="text" value="514"/>	(1-65534)
Device No.	<input type="text" value="22"/>	(0-23)
	<input type="button" value="Apply"/>	<input type="button" value="Refresh"/> <input type="button" value="Default"/>

7 Live

This section introduces the layout of the interface and function configuration.

7.1 Live Interface

Log in and click the **Live** tab.



Interface might vary with different models, and the actual interface shall prevail.

Figure 7-1 Live (single-channel)

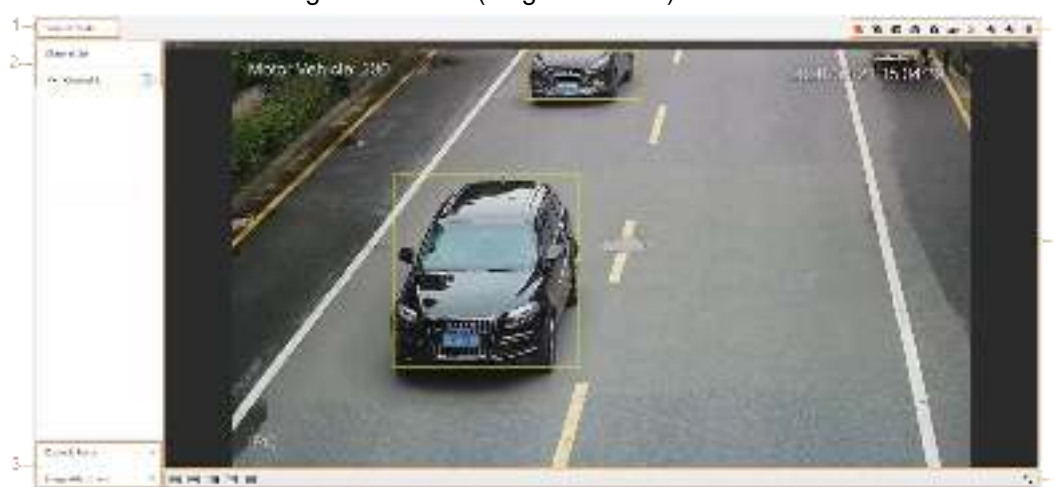


Figure 7-2 Live (multi-channels)

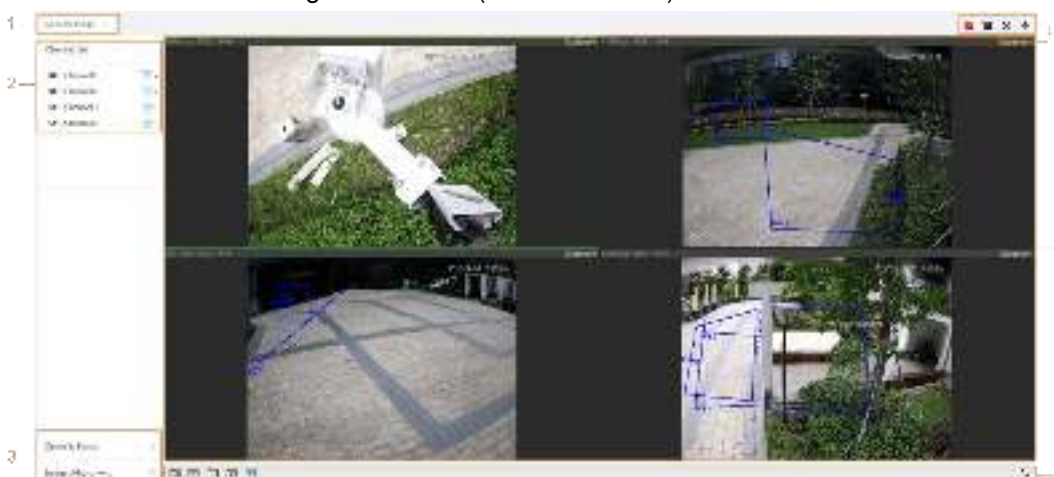


Table 7-1 Description of function bar

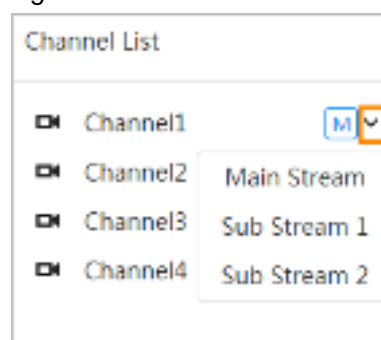
No.	Function	Description
1	Display mode	You can select the display mode from General Mode and Face Mode .
2	Channel list	Displays all channels. You can select the channel as needed and set the stream type.
3	Image adjustment	Adjustment operations in live viewing.




No.	Function	Description
4		
5	Live view	Displays the real-time monitoring image.
6	Live view function bar	Functions and operations in live viewing.

7.2 Setting Encode

Click , and then select the stream as needed.

Figure 7-3 Encode bar















- **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 "6.2.2.1 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 "6.2.2.1 Encode".
-  means the current stream is main stream;  means the current stream is sub stream 1;  means the current stream is sub stream 1.

7.3 Live View Function Bar

For the live view function bar, see Table 7-2.

Table 7-2 Description of live view function bar

Icon	Function	Description
	Force Alarm	Display alarm sound state. Click the icon to enable or disable the alarm sound forcibly.
	Digital Zoom	You can zoom video image through two operations. <ul style="list-style-type: none"> • 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. In zoom in state, drag the image to check other area. • Click the icon, and then scroll the mouse wheel in the video image to zoom in or out.


Icon	Function	Description
	Snapshot	Click the icon to capture one picture of the current image, and it will be saved to the configured storage path.  About viewing or configuring storage path, see "6.1 Local".
	Triple Snapshot	Click the icon to capture three pictures of the current image, and they will be saved to the configured storage path.  About viewing or configuring storage path, see "6.1 Local".
	Record	Click the icon to record video, and it will be saved to the configured storage path.  About viewing or configuring storage path, see "6.1 Local".
	Aux Focus	Click the icon, the AF Peak (focus eigenvalue) and AF Max (max focus eigenvalue) are displayed on the video image. <ul style="list-style-type: none"> AF Peak: The eigenvalue of image definition, it displays during focus. AF Max: The best eigenvalue of image definition. The smaller the difference between AF peak value and the AF max value, the better the focus is.  Aux focus closes automatically after five minutes.
	Audio	Click the icon to enable or disable audio output.
	Talk	Click the icon to enable or disable the audio take.







7.4 Window Adjustment Bar

7.4.1 Adjustment

This section introduces the adjustment of image. For details, see Table 7-3.

Table 7-3 Description of adjustment bar

Icon	Function	Description
	Original Size	Click the icon, and then the video displays with original size.

Icon	Function	Description
	Full Screen	Click the icon to enter full screen mode; double-click or press Esc to exit.
	W:H	Click the icon to resume original ratio or change ratio.
	Fluency Adjustment	Click the icon to select the fluency from Realtime , General and Fluent . <ul style="list-style-type: none"> • Realtime: Guarantees the real time of the image. When the bandwidth is not enough, the image might not be smooth. • General: It is between Realtime and Fluent. • Fluent: Guarantees the fluency of the image. There might be delay between live view image and real-time image.
	AI Rule	Click the icon, and then select Enable to display AI rules and detection box; select Disable to stop the display. It is enabled by default.
	Crowd Distribution Map	Click the icon and select Enable . The Crowd Distribution Map interface is displayed. For details, see "8.1 Setting Crowd Distribution Map".
	Window Layout	When view multi-channel image, you can select display layout.

7.4.2 Zoom and Focus

Click **Zoom and Focus** at the lower-left corner of **Live** interface to adjust focal length to zoom in or out video image; by adjusting focus manually, automatically or within a certain area, you can change image clarity or correct adjusting errors.



The focus would adjust automatically after zooming in or out.

Figure 7-4 Zoom and focus

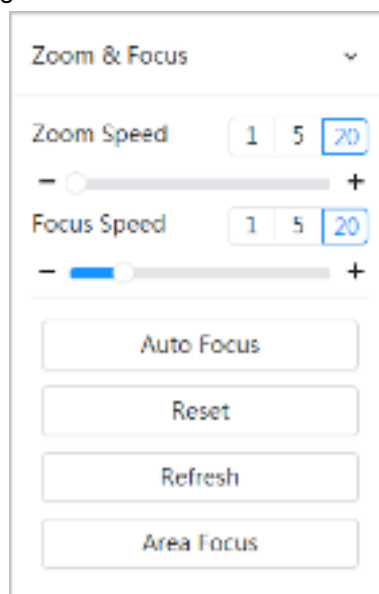




Table 7-4 Description of zoom and focus parameter

Parameter	Description
Zoom Speed	<p>Changes the focal length of the camera to zoom in or out the image.</p> <ol style="list-style-type: none"> 1. Set the speed value. The Zoom Speed is the adjustment range in one click. The larger the value is, the more the image would zoom in or out in one click. 2. Click or hold + or - button, or drag the slider to adjust zoom.
Focus Speed	<p>Adjusts the optical back focal length to make the image clearer.</p> <ol style="list-style-type: none"> 1. Set the speed value. The Focus Speed is the adjustment range in one click. The larger the value is, the more the adjustment in one click. 2. Click or hold + or - button, or drag the slider to adjust focus.
Auto Focus	<p>Adjusts image clarity automatically.</p>  <p>Do not make any other operation during auto focus process.</p>
Reset	<p>Restores focus to default value and corrects errors.</p>  <p>You can restore the focus if the image has poor clarity or has been zoomed too frequently.</p>
Refresh	Get the latest zoom setting of the camera.
Area Focus	<p>Focus on the subject of a selected area.</p> <p>Click Area Focus, and then select an area in the image, the camera performs auto focus in that area.</p>

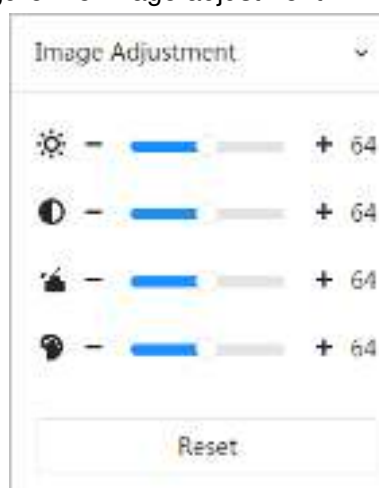
7.4.3 Image Adjustment





Click **Image Adjustment** at the lower-left corner of **Live** interface, and click **+** or **-** button, or drag to adjust image parameters, including brightness, contrast, hue, and saturation.



The adjustment is only available on the web interface, and it does not adjust the camera parameters.

Figure 7-5 Image adjustment



-  (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.

Click **Reset** to restore focus to default value.



You can restore the zoom if the image has poor clarity or has been zoomed too frequently.

7.5 Display Mode

You can select the display mode from **General Mode**, **Face Mode** and **Metadata Mode**. For general mode, see Figure 7-2. This section mainly introduces **Face Mode** and **Metadata Mode**.



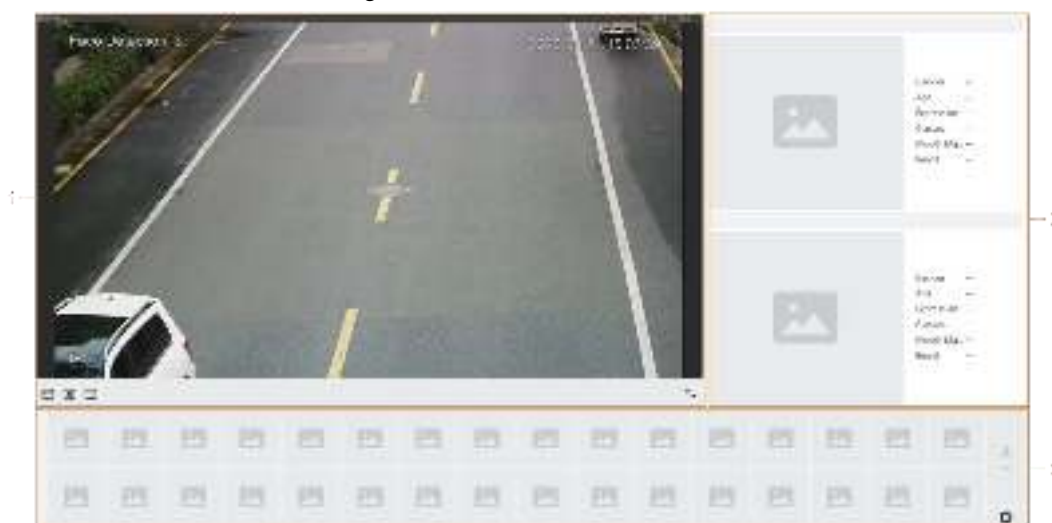
Interface might vary with different models, and the actual interface shall prevail.

- Select **Face Mode** from the display mode drop-down list.



Make sure that you have enabled face detection function.

Figure 7-6 Face mode



- Select **Metadata Mode** from the display mode drop-down list.




Make sure that you have enabled video metadata detection function.

Figure 7-7 Metadata mode



Table 7-5 Description of face mode layout

No.	Function	Description
1	Live view	Displays the real-time monitoring image. For details, see "7.4.1 Adjustment".
2	Details	Displays the captured image and details.
3	Captured image	Displays the captured images. <ul style="list-style-type: none"> • Click a snapshot in the area, and the details of the snapshot are displayed in the Details area. • Click  to set the attributes displayed in the Details area.

8 AI

8.1 Setting Crowd Distribution Map

You can view crowd distribution on the map in real time for timely arming, to prevent stampede and other accidents.

8.1.1 Global Configuration

Set the calibration parameters of panoramic cameras.

Calibration Purpose

Determine corresponding relationship between 2D image captured by the camera and 3D actual object according to one horizontal ruler and three vertical rulers calibrated by the user and the corresponding actual distance.

Notes

When drawing calibration ruler, keep the ruler length consistent with the actual length of the object.

Procedure




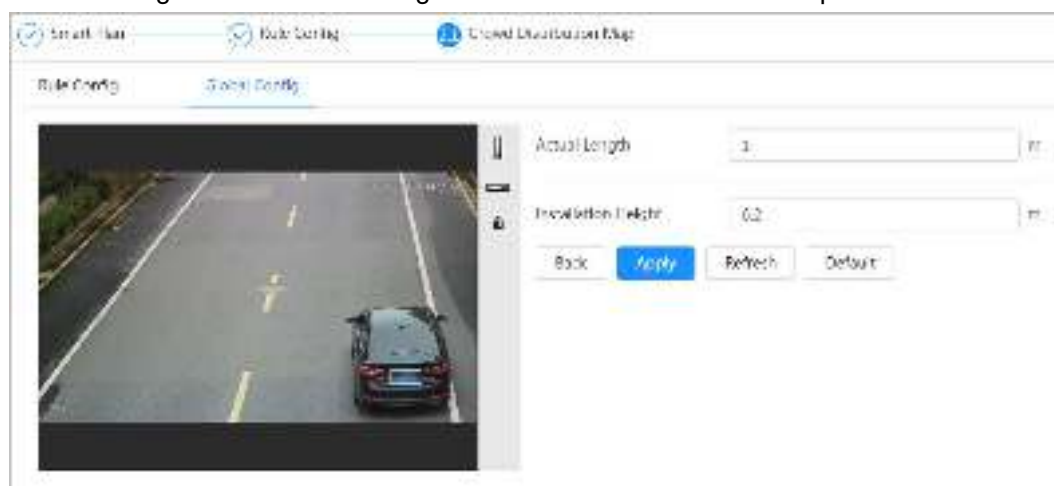
1. Select **AI > Smart Plan**.
2. Click ☐ next to **Crowd Distribution Map** to enable crowd distribution map of the corresponding channel, and then click **Next**.
3. Click the **Global Config** tab.
4. Click the rule icon to draw one horizontal ruler and three vertical rulers on the image.
 -  is the vertical ruler icon, and  is the horizontal ruler icon.
 - Select the added rulers on the image, and click  to delete them.

Figure 8-1 Global configuration of crowd distribution map



5. Select a calibration type and enter the actual length, and then click **Add Rulers**.
6. Click **Apply**.

8.1.2 Rule Configuration

When the number of people or the crowd density in the detection area exceeds the configured threshold, the system performs alarm linkages.

Prerequisites

- Select **AI > Smart Plan**, and enable **Crowd Distribution Map**.
- You have configured the parameters on the **Global Config** interface.

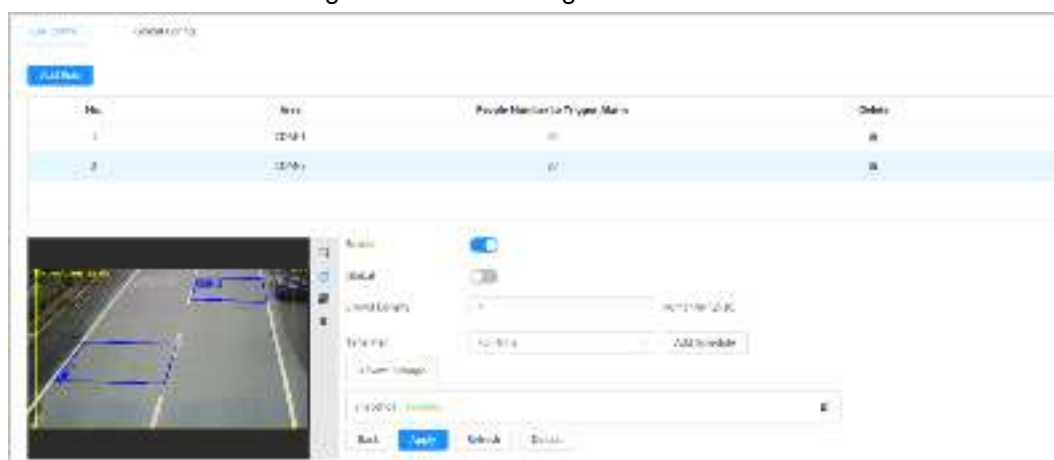
Procedure

Step 1 Select **AI > Smart Plan**


Step 2 Click ☐ next to **Crowd Distribution Map**, and then click **Next**.

Step 3 Click the **Rule Config** tab.

Figure 8-2 Rule configuration



Step 4 Click ☐ next to **Enable**, and then the crowd map function is enabled, and the detection area box is displayed on the image.


Click , and you drag the any corner of the box to adjust the size of the area, and press the left mouse button and move the box to adjust the position.

Step 5 Draw multiple people counting areas in **Detection Area** as needed.



1) Click **Add Rule** to add statistical areas.

2) Set the name of **Area** and **People Number to Trigger Alarm**.

When the number of the people in the area exceeds the configured threshold, the alarm will be triggered, and the system will perform the linkage actions. The people number to trigger alarm is 20 by default.

3) Click  at the right side of the image, draw people counting areas in the detection area, and then right-click to finish the drawing.

4) Repeat the above steps to add more people counting areas.

- Click , and then press and hold the left mouse button to draw a rectangle, and then pixel size is displayed.
- Click  to delete the drawn detection or people counting areas.

Step 6 Configure parameters.

Table 8-1 Description of crowd map parameters

Parameter	Description
Global	Click <input type="checkbox"/> next to Global and set the crowd density threshold.

Parameter	Description
Crowd Density	The system detects crowd distribution in the global area. When the crowd density exceeds the configured threshold, the system performs alarm linkages.

Step 7 Set arming periods and alarm linkage action. For details, see "6.4.1.2 Alarm Linkage". Click **+ Event Linkage** to set the linkage action.

Step 8 Click **Apply**.
To view alarm information on the alarm subscription tab, you need to subscribe relevant alarm event. For details, see "6.4.1.3.2 Subscribing Alarm Information".

Result


Click  on the **Live** interface to view the crowd distribution map.

Figure 8-3 Crowd map (1)



Double-click the rendering area at the lower-right corner in the image to view crowd distribution in the area.

Figure 8-4 Crowd map (2)







8.2 Setting Face Recognition

When a face is detected or recognized in the detection area, the system performs alarm linkage and supports searching face detection and recognition results.






- **Face Detection:** When a face is detected in the area, the system performs alarm linkage, such as recording and sending emails.
- **Face Recognition:** When a face is detected in the area, the system compares the captured face image with the information in the face database, and links alarm according to the comparison result.



For the process of setting face recognition, see Figure 8-5.

- Click  to draw the minimum size of the target, and click  to draw the maximum size of the target. Only when the target size between the maximum size and the minimum size, can the alarm be triggered.
- Click , and then press and hold the left mouse button to draw a rectangle, the pixel size is displayed.
- Click  to delete the detection line.

Step 5 Set parameters.

Table 8-2 Description of face detection parameters

Parameter	Description
OSD Info	Click OSD Info , and the Overlay interface is displayed, and then enable the face statistics function. The number of detected faces is displayed on the Live interface. For details, see "6.2.2.2.11 Configuring Face Statistics".
Face Enhancement	Click  to enable face enhancement, and it can preferably guarantee clear face with low stream.
Non-living Filtering	Filter non-living faces in the image, such as a face picture.
Target Box Overlay	Click  to enable the function, and you can add a bounding box to the face in the captured picture to highlight the face. The captured face picture is saved in SD card or the configured storage path. For the storage path, see "6.1 Local".
Remove Duplicate Faces	During the configured period, the duplicate faces are displayed only once, to avoid repeated counting. Click  , and then click Apply . <ul style="list-style-type: none"> • Time: During the configured time, the function is enabled. • Precision: The larger the precision value, the higher the accuracy.
Face Matting	Set a range for the captured face image, including face, one-inch picture, and custom. When selecting Custom , click  , configure the parameters on the prompt interface, and then click Apply . <ul style="list-style-type: none"> • Customized width: Set snapshot width; enter the times of the original face width. It ranges from 1–5. • Customized face height: Set face height in snapshot; enter the times of the original face height. It ranges from 1–2. • Customized body height: Set body height: in snapshot; enter the times of the original body height. It ranges from 0–4. When the value is 0, it means to cutout the face image only.
Snap Mode	<ul style="list-style-type: none"> • Optimized Snapshot: Capture the clearest picture within the configured time after the camera detects face. • Recognition Priority: Repeatedly compare the captured face to the faces in the armed face database, and capture the most similar face image and send the event. It is recommended to use this mode in access control scene.  Click Advanced to set the optimized time.

Parameter	Description
Properties	Click  next to Properties to enable the properties display.
Face Exposure	Click  next to Face Exposure . When a face is detected, the camera can enhance brightness of the face to make the face image clear.
Face Target Brightness	Set the face target brightness. It is 50 by default.
Face Exposure Detection Interval	Set the face exposure detection interval to prevent image flickering caused by constant adjustment of face exposure. It is five seconds by default.
Advanced	<ul style="list-style-type: none"> • Snapshot Angle Filter: Set snapshot angle to be filtered during the face detection. • Snapshot Sensitivity: Set snapshot sensitivity during the face detection. It is easier to detect face with higher sensitivity. • Optimized Time: Set a time period to capture the clearest picture after the camera detects face.

Step 6 Set arming periods and alarm linkage action. For details, see "6.4.1.2 Alarm Linkage".

Step 7 Click **Apply**.

To view alarm information on the alarm subscription tab, you need to subscribe relevant alarm event. For details, see "6.4.1.3.2 Subscribing Alarm Information".

8.2.2 Setting Face Database

By setting face database, the face database information can be used to compare with the face detected.


Face database configuration includes creating face database, adding face picture, and face modeling.

8.2.2.1 Creating Face Database

Face database includes face picture, face data and other information. It also provides comparison data for the captured face pictures.

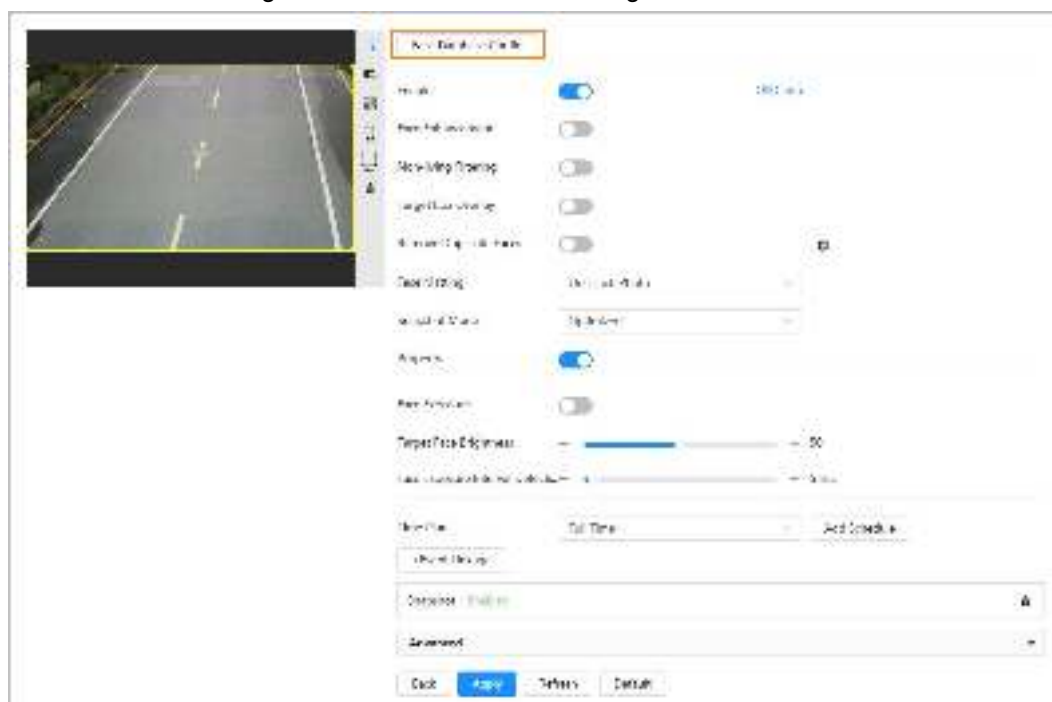
Procedure

Step 1 Select **AI > Smart Plan**.

Step 2 Click  next to **Face Recognition** to enable face recognition of the corresponding channel, and then click **Next**.

Step 3 Click **Face Database Config** on the **Face Recognition** interface.

Figure 8-7 Face database configuration



Step 4 Click **Add Face Database**.

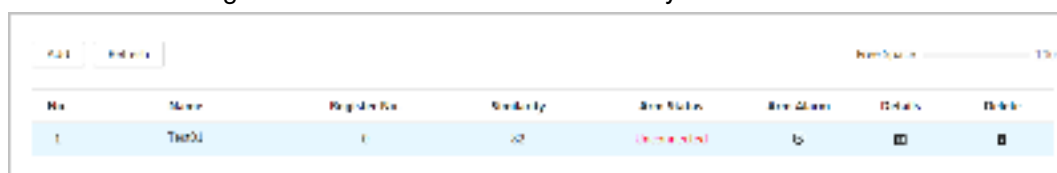
Step 5 Set the name of the face database.




Figure 8-8 Add face database



Step 6 Click **OK**.

Figure 8-9 Face database successfully added



- Edit the name of the face database.
Click the text box under **Name** to edit the name of the face database.
- Arm Alarm
Click  to configure the parameters of arm alarm. For details, see "8.2.2.5 Setting Arm Alarm".
- Manage face database
Click  to manage the face database. You can search face, register, batch register, modeling all, modeling, and delete face.
- Delete face database
Click  to delete the face database.

8.2.2.2 Adding Face Picture


Add face picture to the created face database. Single adding and batch importing are supported.

Requirements on face pictures.

- A single face picture size is 50K–150K in JPEG format. The resolution is less than 1080p.
- Face size is 30%–60% of the whole picture. Pixel should be no less than 100 pixels between the ears.
- Taken in full-face view directly facing the camera without makeup, beautification, glasses, and fringe. Eyebrow, mouth and other face features must be visible.

8.2.2.2.1 Single Adding

Add face pictures one by one. Select this way when you need to add a small number of face pictures.

Step 1 On the **Face Database Config** interface, click  next to the face database to be configured.

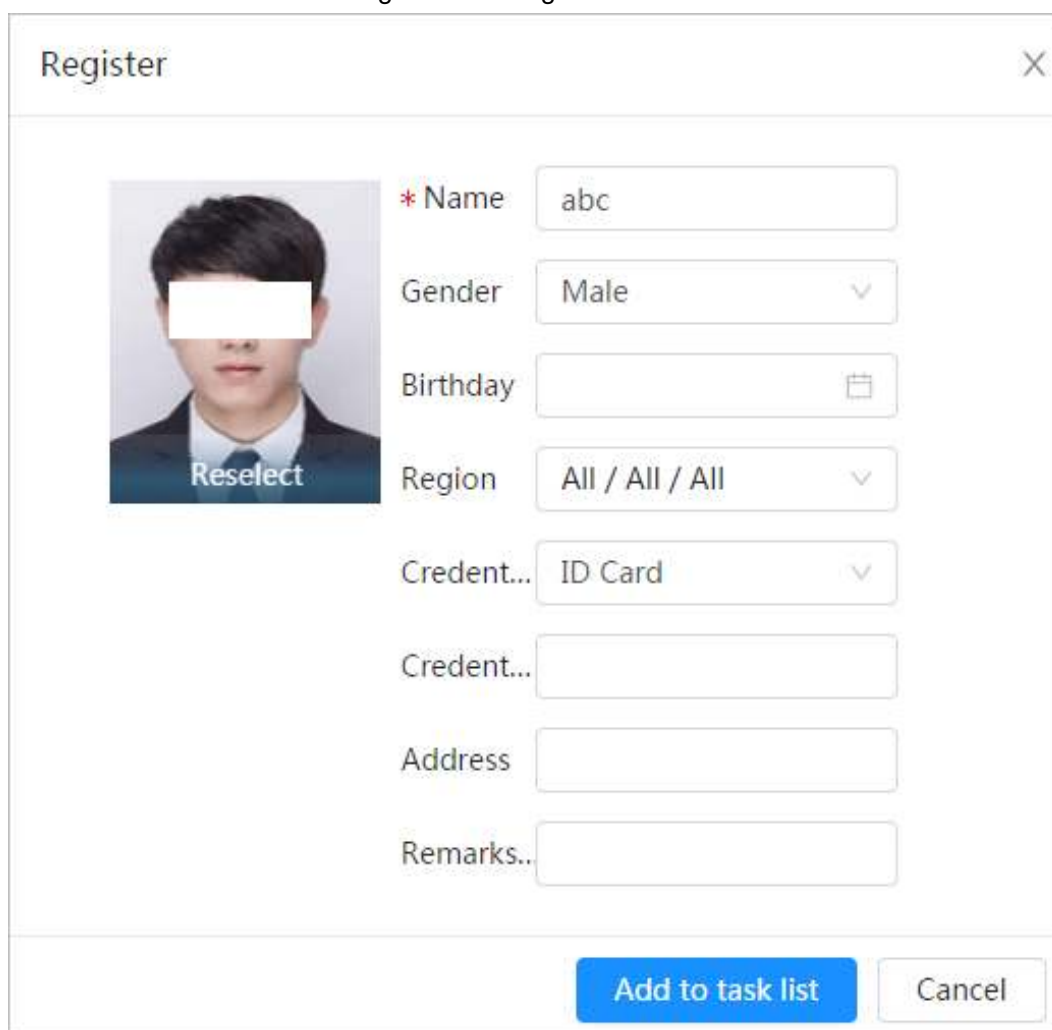
Step 2 Click **Register**.

Step 3 Click **Upload**, select a face picture to be uploaded, and then click **Open**.



You can manually select the area for a face. After uploading picture, select a face and click **Confirm Screen**. When there are multiple faces in a photo, select the target face and click **Confirm Screen** to save face picture.

Figure 8-10 Register



The Register dialog box contains the following fields and controls:

- Name:** A text input field with the value "abc".
- Gender:** A dropdown menu with "Male" selected.
- Birthday:** A date picker control.
- Region:** A dropdown menu with "All / All / All" selected.
- Credent...:** A dropdown menu with "ID Card" selected.
- Credent...:** A text input field.
- Address:** A text input field.
- Remarks..:** A text input field.
- Face Picture:** A preview image of a person's face with a "Reselect" button below it.
- Buttons:** "Add to task list" (blue) and "Cancel" (grey).

Step 4 Enter the information about face picture according to the actual situation.

Step 5 Click **Add to task list**.

Step 6 Click **Task List 1**, and then click **Operation**.

- If the operation is successful, the system prompts that stored successfully, modeled successfully.
- If adding user fails, the error code is displayed on the interface. For details, see Table 8-3. For face modeling operation, see "8.2.2.4 Face Modeling"

Table 8-3 Description of error code

Parameter	Error	Description
0x1134000C	Picture importing error	The picture is too large, and the upper limit is 150K.
0x1134000E		The quality of the added pictures is to the upper limit.
0x11340019		The space of the face database exceeds the upper limit.
1	Picture modeling error	The picture format is not correct. Import the picture in JPG format.
2		No face in the picture or the face is not clear. Change the picture.

Parameter	Error	Description
3		Multiple faces in the picture. Change the picture.
4		Failed to decode the picture. Change the picture.
5		The picture is not suitable to be imported to the face database. Change the picture.
6		The database error. Restart the camera and model faces again.
7		Fails to get the picture. Import the picture again.
8		System error. Restart the camera and model faces again.

8.2.2.2.2 Batch Importing

Import face pictures in batches. Select this way when you need to add a large number of face pictures.


Before importing pictures in batches, name face pictures in a format of "Name#SGender#BDate of Birth#NRegion#TCredentials Type#MID No.jpg" (for example, "John#S1#B1990-01-01#T1#M0000"). For naming rules, see Table 8-4.



- The max. size of a single face picture is 150K, and the resolution is less than 1080p.
- When naming pictures, name is required, and others are optional.

Table 8-4 Description of naming rules for batch import parameters

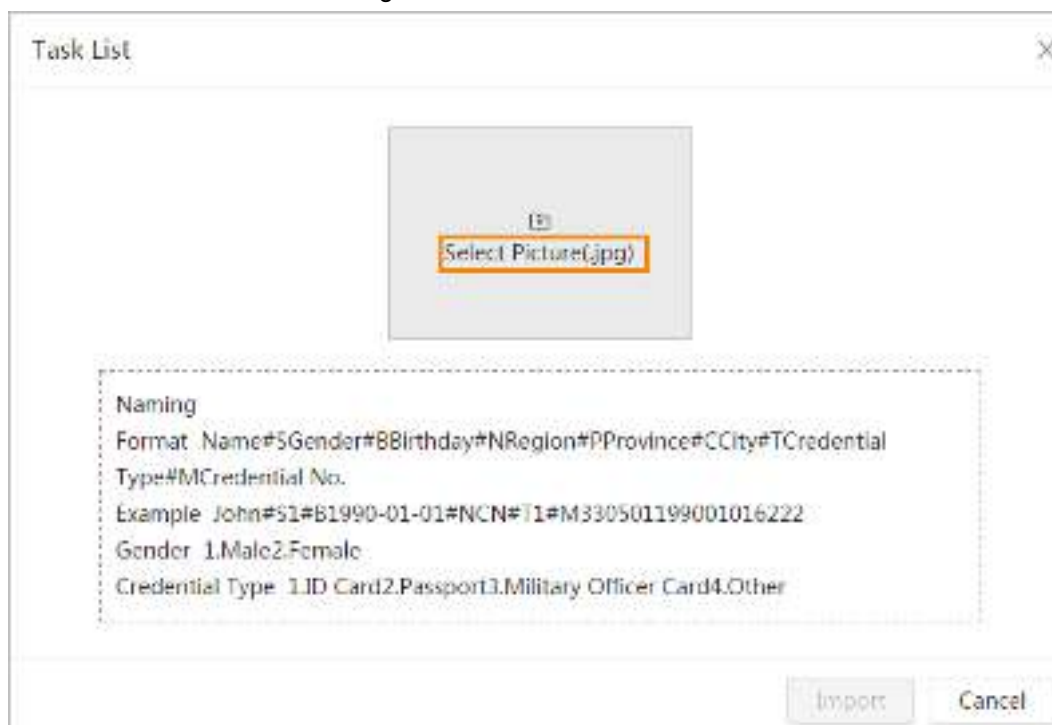
Parameter	Description
Name	Enter a name.
Gender	"1" is male and "2" female.
Date of Birth	Format: yyyy-mm-dd, such as 2020-10-23.
Credentials Type	"1" is ID card and "2" passport.
ID number	Enter ID No.

Step 1 On the **Face Database Config** interface, click  next to the face database to be configured.

Step 2 Click **Batch Register**.

Step 3 Click **Select Picture**, and select storage path of the file.

Figure 8-11 Task list



Step 4 Click **Import** to import the face pictures.

After the importing is completed, the result will be displayed.

- If the picture is imported successfully, click **Next** to do modeling operation.
 - If the picture importing failed, click **Query** to view the details of the pictures and error code. For details, see Table 8-3.
- Click **Export** to export the error details.


Step 5 Click **Next** to do modeling operation.

The modeling result is displayed. If modeling failed, click **Query** and the failure details will be displayed in the list. Point to the modeling status to view the details. Then you can change picture according to the failure reason. For modeling details, see "8.2.2.4 Face Modeling".


8.2.2.3 Managing Face Picture

Add face pictures to face database, and then manage and maintain face pictures to ensure correct information.

8.2.2.3.1 Editing Face Information

Step 1 On the **Face Database Config** interface, click  next to the face database to be configured.


Step 2 Click **Query**, set the criteria as needed, and then click **Search**.

Step 3 Select the row where the face picture or the personnel information is located, and then click .

Step 4 Edit face information according to the actual need. Click **Add to task list**.

Figure 8-12 Face information modification

Register



* Name

Gender

Birthday

Region

Credent...

Credent...

Address


Remarks..




Add to task list

Cancel

Step 5 Click , and then click **Operation**.

8.2.2.3.2 Deleting Face Picture

On the **Face Database Config** interface, click  next to the face database to be configured. Click **Query**, set the search criteria as needed, click **Search**, select the face information that needs to be deleted and delete it.

- Single delete: Select the row where the face picture or the personnel information is located, and click  to delete the face picture.
- Batch delete: Select ☐ at the upper-right corner of the face picture or ☐ of the row where the personnel information is located. Select the information, click **Delete**, then click , and then click **Operation** to delete the selected face pictures.
- Delete all: When viewing face pictures in a list, click ☐ of the row where the serial number is located; when viewing by thumbnail, select **All** to select all face pictures. Click **Delete**, then click , and then click **Operation** to delete all face pictures.


8.2.2.4 Face Modeling

Face modeling extracts face picture information and imports the information to a database to

establish relevant face feature models. Through this function, the face recognition and other intelligent detections can be realized.



- The more the selected face pictures are, the longer time the face modeling takes. Please wait patiently.
- During modeling, some intelligent detection functions (such as face recognition) are not available temporarily, and will be available after modeling.

Step 1 On the **Face Database Config** interface, click  next to the face database to be configured.

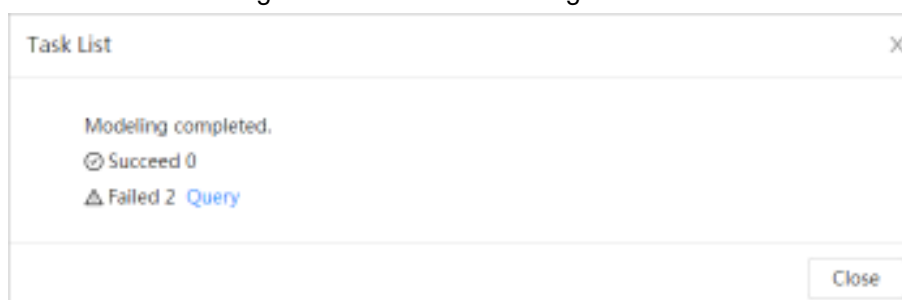
Step 2 Start modeling.



- Selective modeling.
If there are many face pictures in the face database, you can set search criteria to select the pictures that need to be modeled.
 1. Set the search criteria, and click **Search**.
 2. Select the face pictures to be modeled.
 3. Click **Modeling**.
- All modeling.
Click **Modeling All** to complete modeling of all face pictures in the face database.

Step 3 View the modeling result.

When the modeling failed, **Query** will be displayed in the result interface. Click **Query** to view the details.

Figure 8-13 Failed modeling




Click  to view the face picture in list format; click  to view the face picture in thumbnail format.

- When the modeling status is **Valid** in the list or is displayed at the lower-left corner of the thumbnail, it means the modeling succeeded.
- When the modeling status is **Invalid** in the list or is displayed at the lower-left corner of the thumbnail, it means the modeling failed. Point to the modeling status in the list to view the details of the failure. Change the pictures according to the details.

8.2.2.5 Setting Arm Alarm

When face recognition succeeded or failed, the device links alarm out.

Step 1 On the **Face Database Config** interface, click  next to the face database to be configured.

Step 2 Arm face database.

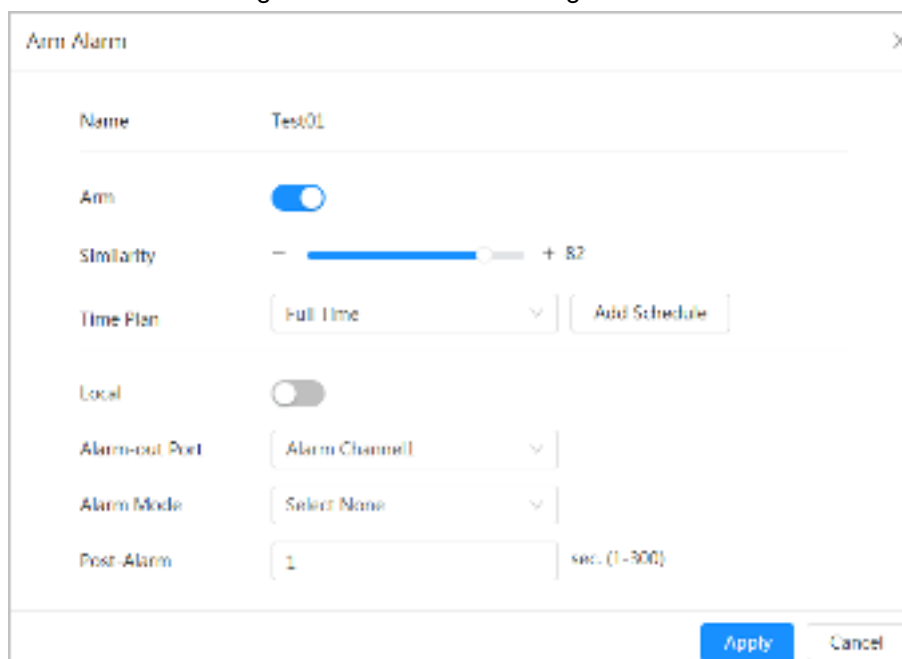
- 1) Click  next to **Arm** to enable the face database arming.

The snapshot will be compared to the pictures in the armed face database.

2) Set the similarity.

The detected face matches the face database only when the similarity between the detected face and the face feature in face database reaches the configured similarity threshold. After successful match, the comparison result is displayed on the **Live** interface.

Figure 8-14 Failed modeling



Step 3 Select alarm mode.

- All: No matter the comparison result of the detected face and that in the face database, the camera links alarm out.
- General: When the detected face matches that in the face database, the camera links alarm out.
- Stranger: When the detected face fails to match that in the face database, the camera links alarm out.
- Select none: No matter the comparison result of the detected face and that in the face database, the camera does not link alarm out.

Step 4 Set arming periods and alarm linkage action. For details, see "6.4.1.2 Alarm Linkage".

Step 5 Click **Apply**.

To view alarm information on the alarm subscription tab, you need to subscribe relevant alarm event. For details, see "6.4.1.3.2 Subscribing Alarm Information".

8.2.2.6 Viewing Face Recognition Result

Select **Face Mode** from the display mode drop-down list at the upper-right corner.


- The live image is displayed at the left side, and the captured face pictures and attribute information are displayed at the right side. When the recognition is successful, the captured face pictures, pictures in the database and the similarity of the face pictures and pictures in the database are displayed at the right side; the snapshot counting result and thumbnails are displayed at the bottom of the live image.
- Click  to set the attributes. For details, see "7.5 Display Mode".

Figure 8-15 Face recognition result



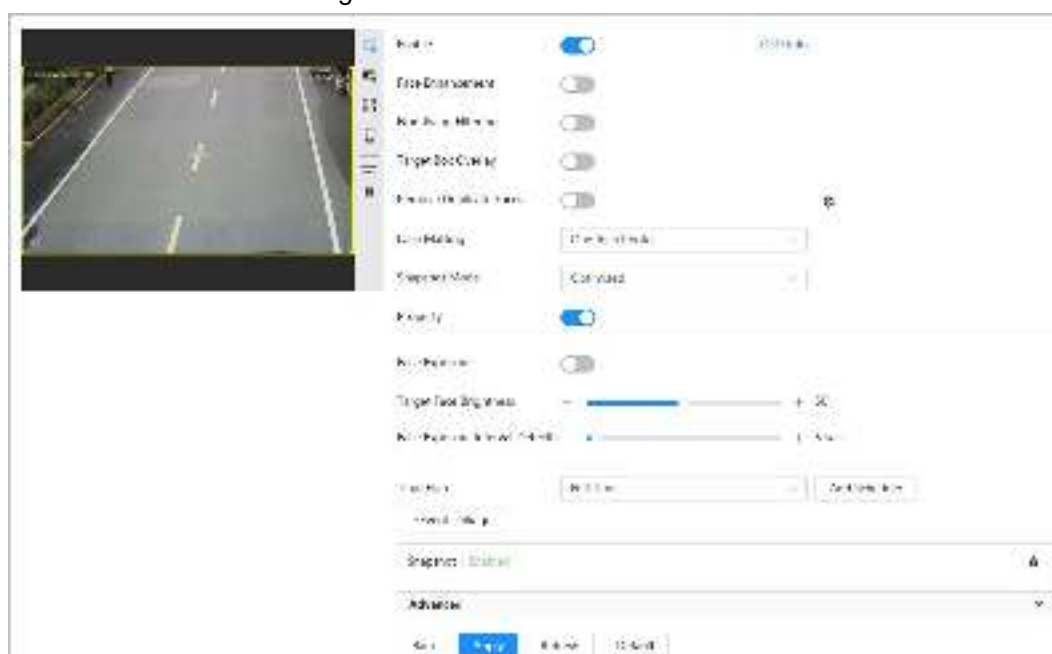
8.3 Setting Face Detection



When a face is detected in the detection area, the system performs an alarm linkage.






Procedure

- Step 1 Select **AI > Smart Plan**.
- Step 2 Click next to **Face Detection** to enable face detection of the corresponding channel, and then click **Next**.

Figure 8-16 Face detection








- Step 3** Click  next to **Enable** to enable the face detection function.
- Step 4** (Optional) Click other icons at the right side of the image to draw detection area, exclusion area, and filter targets in the image.
- Click  to draw a face detection area in the image. The detection area is the whole image by default.

- Click  to draw an exclusion area for face detection in the image.
- Click  to draw the minimum size of the target, and click  to draw the maximum size of the target. Only when the target size between the maximum size and the minimum size, can the alarm be triggered.
- Click , and then press and hold the left mouse button to draw a rectangle, the pixel size is displayed.
- Click  to delete the detection line.

Step 5 Set parameters.

Table 8-5 Description of face detection parameters

Parameter	Description
OSD Info	Click OSD Info , and the Overlay interface is displayed, and then enable the face statistics function. The number of detected faces is displayed on the Live interface. For details, see "6.2.2.2.11 Configuring Face Statistics".
Face Enhancement	Click  to enable face enhancement, and it can preferably guarantee clear face with low stream.
Target Box Overlay	Click  to enable the function, and you can add a bounding box to the face in the captured picture to highlight the face. The captured face picture is saved in SD card or the configured storage path. For the storage path, see "6.1 Local".
Face Matting	During the configured period, the duplicate faces are displayed only once, to avoid repeated counting. When selecting Custom , click  , configure the parameters on the prompt interface, and then click Apply . <ul style="list-style-type: none"> • Customized width: Set snapshot width; enter the times of the original face width. It ranges from 1–5. • Customized face height: Set face height in snapshot; enter the times of the original face height. It ranges from 1–2. • Customized body height: Set body height: in snapshot; enter the times of the original body height. It ranges from 0–4. When the value is 0, it means to cutout the face image only.
Snap Mode	<ul style="list-style-type: none"> • Optimized Snapshot: Capture the clearest picture within the configured time after the camera detects face. • Recognition Priority: Repeatedly compare the captured face to the faces in the armed face database, and capture the most similar face image and send the event. It is recommended to use this mode in access control scene.  Click Advanced to set the optimized time.
Properties	Click  next to Properties to enable the properties display.

Parameter	Description
Advanced	<ul style="list-style-type: none"> • Snapshot Angle Filter: Set snapshot angle to be filtered during the face detection. • Snapshot Sensitivity: Set snapshot sensitivity during the face detection. It is easier to detect face with higher sensitivity. • Optimized Time: Set a time period to capture the clearest picture after the camera detects face.
Face Exposure	Click <input type="checkbox"/> next to Face Exposure . When a face is detected, the camera can enhance brightness of the face to make the face image clear.
Face Target Brightness	Set the face target brightness. It is 50 by default.
Face Exposure Detection Interval	Set the face exposure detection interval to prevent image flickering caused by constant adjustment of face exposure. It is five seconds by default.

Step 6 Set arming periods and alarm linkage action. For details, see "6.4.1.2 Alarm Linkage".

Step 7 Click **Apply**.

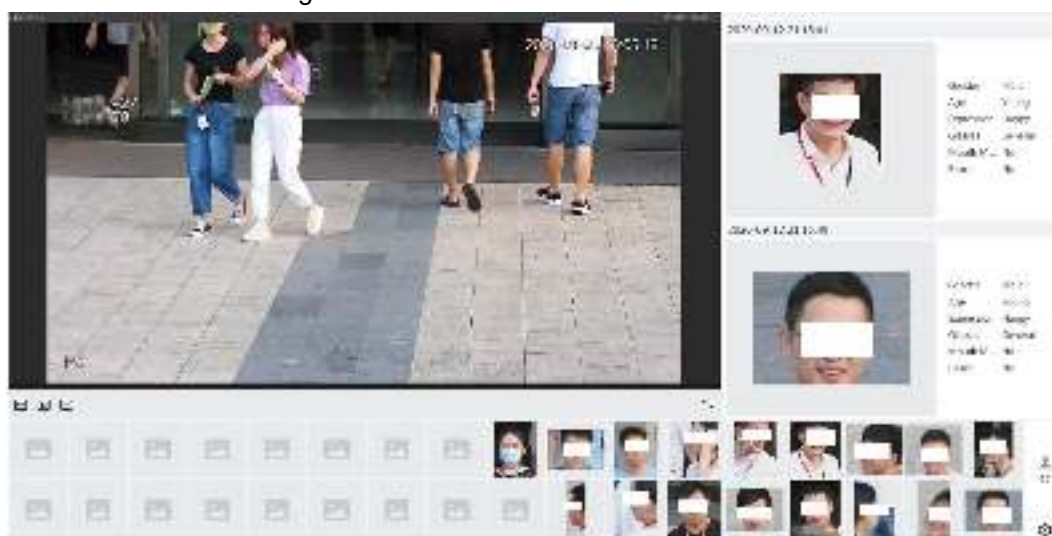
To view alarm information on the alarm subscription tab, you need to subscribe relevant alarm event. For details, see "6.4.1.3.2 Subscribing Alarm Information".

Result

The face detection result is displayed on the live interface.

- The face pictures snapped in real time and their attribute information are displayed.
- Click a face picture in the display area, and the details are displayed.

Figure 8-17 Face detection result



8.4 Setting IVS

This section introduces scene selection requirements, rule configuration, and global configuration for IVS (intelligent video surveillance).

Basic requirements on scene selection are as follows.

- The target should occupy no more than 10% of the whole image.
- The target size in the image should be no more than 10 × 10 pixels. The size of abandoned

object in the image should be no less than 15×15 pixels (CIF image). The target height and width should no more than a third of the image height and width. The recommended target height is 10% of the image height.

- The brightness difference of the target and the background should be no less than 10 gray levels.
- The target should be continuously present in the image for no less than two seconds, and the moving distance of the target should be larger than its width and no less than 15 pixels (CIF image) at the same time.
- Reduce the complexity of surveillance scene as much as you can. Intelligent analysis functions are not recommended to be used in scene with dense targets and frequent illumination change.
- Avoid areas such as glass, reflective ground, water surface, and areas interfered by branch, shadow and mosquito. Avoid backlight scene and direct light.

8.4.1 Global Configuration

Set global rules for IVS, including anti-disturb, depth of field calibration, and valid motion parameter for targets.

Calibration Purpose

Determine corresponding relationship between 2D image captured by the camera and 3D actual object according to one horizontal ruler and three vertical rulers calibrated by the user and the corresponding actual distance.

Applicable Scene

- Medium or distant view with installation height of more than three meters. Scenes with parallel view or ceiling-mounted are not supported.
- Calibrate horizontal plane, not vertical walls or sloping surfaces.
- This function is not applicable to scenes with distorted view, such as the distorted views captured by super wide-angle or fisheye camera.

Notes

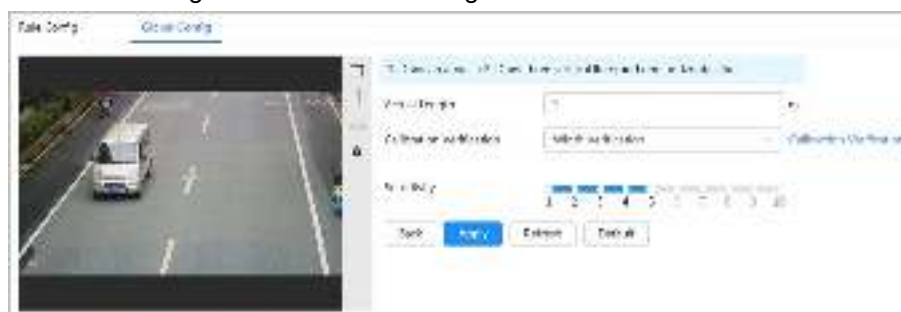
- Calibration Drawing
 - ◇ Calibration area: The calibration area drawn should be on one horizontal plane.
 - ◇ Vertical ruler: The bottom of three vertical rulers should be on the same horizontal plane. Select three reference objects with fixed height in triangular distribution as vertical rulers, such as vehicle parked at roadside or road lamp poles. Arrange three persons to draw at each of the three positions in the monitoring scene.
 - ◇ Horizontal ruler: Select reference object with known length on the ground, such as sign on the road, or use a tape to measure the actual length.
- Calibration Verification





After setting the ruler, draw a straight line on the image, check the estimated value of the straight line, and then compare this value with the value measured in the actual scene to verify calibration accuracy. In case of major difference between the estimated value and the actual one, fine-tune or reset parameters until the error requirement is met.

Procedure

1. Select **AI > Smart Plan**.
2. Click ☐ next to **IVS** to enable IVS of the corresponding channel, and then click **Next**.
3. Click the **Global Config** tab.

Figure 8-18 Global configuration of IVS



4. Set calibration area and ruler.
 - a. Click  and draw a calibration area in the image, and right-click to finish the drawing.
 - b. Click the ruler icon to draw one horizontal ruler and three vertical rulers in the calibration area.
 -  indicates vertical ruler, and  indicates horizontal ruler
 - Select an added ruler, and click  to delete the ruler.
5. Set the sensitivity.
Adjust the filter sensitivity. With higher value, it is easier to trigger an alarm when low-contrast object and small object are captured, and the false detection rate is higher.
6. Click **Apply**.

Result

1. Select the verification type, and then click **Calibration Verification**.
To verify vertical ruler and horizontal ruler, respectively select **Height Verification** and **Width Verification**.
2. Draw a straight line in the image to verify whether the rulers are correctly set.
In case of big difference between the estimated value and the actual one, fine-tune or reset parameters until the error requirement is met.

8.4.2 Rule Configuration

Set rules for IVS, including cross fence detection, tripwire, intrusion, abandoned object, moving object, fast moving, parking detection, crowd gathering, and loitering detection.

- Select **AI > Smart Plan**, and enable **IVS**.
- Select **AI > Smart Plan > Global Config** to finish global configuration.

For the functions and applications of the rules, see Table 8-6.

Table 8-6 Description of IVS functions

Rule	Description	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.	
Abandoned object	When an object is abandoned in the detection area over the configured time, an alarm is triggered, and then the system performs configured alarm linkages.	<p>Scenes with sparse targets and without obvious and frequent light change. Simple scene in the detection area is recommended.</p> <ul style="list-style-type: none"> Missed alarm might increase in the scenes with dense targets, frequent occlusion, and people staying. In scenes with complex foreground and background, false alarm might be triggered for abandoned or missing object.
Missing object	When an object is taken out of the detection area over the defined time, an alarm is triggered, and then the system performs configured alarm linkages.	<p>Scenes with sparse targets and without obvious and frequent light change. Simple scene in the detection area is recommended.</p> <ul style="list-style-type: none"> Missed alarm might increase in the scenes with dense targets, frequent occlusion, and people staying. In scenes with complex foreground and background, false alarm might be triggered for abandoned or missing object.
Fast moving	When the motion speed is higher than the configured speed, an alarm is triggered, and then the system performs configured alarm linkages.	Scene with sparse targets and less occlusion. The camera should be installed right above the monitoring area. The light direction should be vertical to the motion direction.

Rule	Description	Applicable Scene
Parking detection	When the target stays over the configured time, an alarm is triggered, and then the system performs configured alarm linkages.	Road monitoring and traffic management.
Crowd gathering	When the crowd gathers or the crowd density is large, an alarm is triggered, and then the system performs configured alarm linkages.	Scenes with medium or long distance, such as outdoor plaza, government entrance, station entrance and exit. It is not suitable for short-distance view analysis.
Loitering detection	When the target loiters over the shortest alarm time, an alarm is triggered, and then the system performs configured alarm linkages. After alarm is triggered, if the target stays in the area within the time interval of alarm, then alarm will be triggered again.	Scenes such as park and hall.

Configure IVS rules. This section takes tripwire as an example.

Step 1 Select **AI > Smart Plan**.

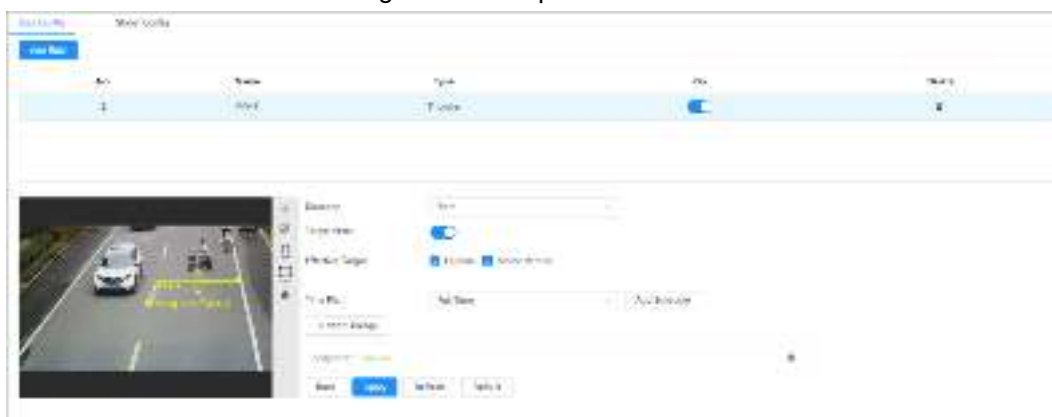
Step 2 Click ☐ next to **IVS** to enable IVS of the corresponding channel, and then click **Next**.


Step 3 Click the **Rule Config** tab.

Step 4 Click **Add Rule** on the **Rule Config** interface, and then select **Tripwire** from the drop-down list.

Double-click the name, and you can edit the rule name; the rule is enabled by default.

Figure 8-19 Tripwire



Step 5 Click  to draw rule line in the image. Right-click to finish drawing.






For requirements of drawing rules, see Table 8-6. After drawing rules, drag corners of the detection area to adjust the area range.

Table 8-7 Description of IVS analysis

Rule	Description
Tripwire	Draw a detection line.
Intrusion	Draw a detection area.
Abandoned object	<ul style="list-style-type: none"> During the detection of abandoned object, the alarm is also


Rule	Description
Missing object	<p>triggered if pedestrian or vehicle stays for a long time. If the abandoned object is smaller than pedestrian and vehicle, set the target size to filter pedestrian and vehicle or properly extend the duration to avoid false alarm triggered by transient staying of pedestrian.</p> <ul style="list-style-type: none"> During the detection of crowd gathering, false alarm might be triggered by low installation height, large percentage of single person in an image or obvious target occlusion, continuous shaking of the camera, shaking of leaves and tree shade, frequent opening or closing of retractable door, or dense traffic or people flow.
Fast moving	
Parking detection	
Crowd gathering	
Loitering detection	

Step 6 (Optional) Click other icons at the right side of the image to filter targets in the image.

- Click  to draw the minimum size of the target, and click  to draw the maximum size of the target. Only when the target size between the maximum size and the minimum size, can the alarm be triggered.
- When the rule of crowd gathering is configured, you do not need to set target filter, but draw the minimum gathering area. Click  to draw the minimum gathering area in the scene. The alarm is triggered when the number of people in the detection area exceeds the minimum area and the duration.
- Click , and then press and hold the left mouse button to draw a rectangle, the pixel size is displayed.
- Click  to delete the detection line.

Step 7 Set rule parameters for IVS.

Table 8-8 Description of IVS parameters

Parameter	Description
Direction	<p>Set the direction of rule detection.</p> <ul style="list-style-type: none"> When setting tripwire, select A->B, B->A, or A<->B. When setting intrusion, select Enter, Exit, or Both.
Action	<p>When setting intrusion action, select Appears or Cross.</p>
Target Filter	<p>Click  to enable this function.</p> <ul style="list-style-type: none"> When you select Human as the alarm target, an alarm will be triggered when the system detects that persons 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.
Duration	<ul style="list-style-type: none"> For abandoned object, the duration is the shortest time for triggering an alarm after an object is abandoned. For missing object, the duration is the shortest time for triggering an alarm after an object is missing. For parking detection, crowd gathering, or loitering detection, the duration is the shortest time for triggering an alarm after an object appears in the area.

Parameter	Description
Sensitivity	<ul style="list-style-type: none"> For fast moving, sensitivity is related to the triggering speed. Lower sensitivity requires faster moving speed to trigger the alarm. For crowd gathering, sensitivity is related to the alarm triggering time. It is easier to trigger the alarm with higher sensitivity.

Step 8 Set arming periods and alarm linkage action. For details, see "6.4.1.2 Alarm Linkage". Click **+ Event Linkage** to set the linkage action.

Step 9 Click **Apply**.
To view alarm information on the alarm subscription tab, you need to subscribe relevant alarm event. For details, see "6.4.1.3.2 Subscribing Alarm Information".


8.5 Setting Video Metadata

Classify people, non-motor vehicles and motor vehicles in the captured video, and display the relevant attributes on the live interface.

8.5.1 Global Configuration

Set the global configuration of video metadata, including face parameter and scene parameter.

Step 1 Select **AI > Smart Plan**.

Step 2 Click  next to **Video Metadata** to enable video metadata of the corresponding channel, and then click **Next**.

Step 3 Click the **Global Config** tab.

Step 4 Set parameters.

Figure 8-20 Global configuration of video metadata

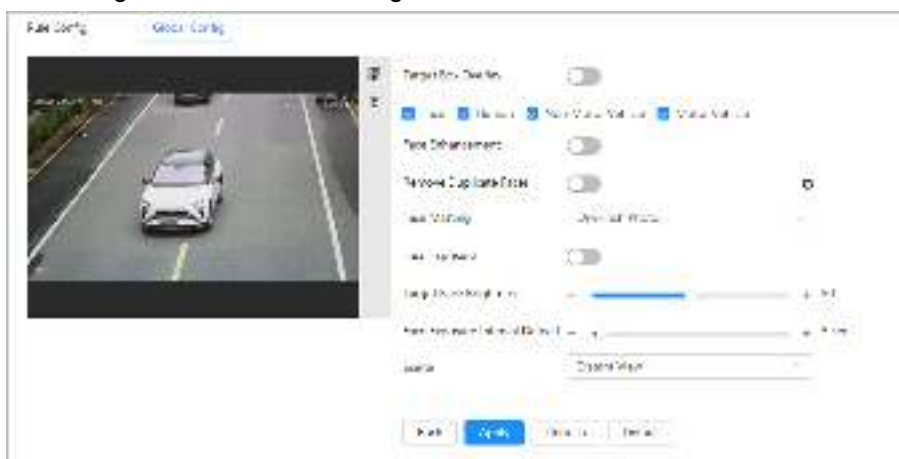



Table 8-9 Description of scene set parameters (video metadata)

Parameter	Description
Target Box Overlay	<p>Overlay target box on the captured pictures to mark the target position.</p> <p>Four types of target boxes are supported. Select the target box as needed.</p> <p>The captured pictures are stored in SD card or the configured storage path. For details, see "6.1 Local".</p>
Face Enhancement	<p>Click <input type="checkbox"/> next to Face Enhancement to preferably guarantee clear face with low stream.</p>
Remove Duplicate Faces	<p>During the configured period, the face that detected several times is displayed only once, to avoid repeated counting.</p> <p>Click  to set the parameters, and then click Apply.</p> <ul style="list-style-type: none"> Time: During the configured period, the function is valid. Precision: The larger the value is, the higher the accuracy will be.
Face Matting	<p>Set a range for matting face image, including face picture and one-inch picture.</p>
Face Exposure	<p>Click <input type="checkbox"/> next to Face Exposure to make face clearer by adjusting lens aperture and shutter.</p>
Target Face Brightness	<p>Set the face target brightness, and it is 50 by default.</p>
Face Exposure Interval Detection Time	<p>Set the face exposure interval detection time to prevent image flickering caused by constant adjustment of face exposure. It is 5 seconds by default.</p>
Scene	<p>Set scene as Distant View or Close View.</p>

Step 5 Click **Apply**.

8.5.2 Rule Configuration

Set the detection scene and rules, including people, non-motor vehicle, and motor vehicle.

Prerequisites

- Select **AI > Smart Plan**, and enable **Video Metadata**.
- You have configured the parameters on the **Global Config** interface.

Procedure

Step 1 Select **AI > Smart Plan**

Step 2 Click ☐ next to **Video Metadata**, and then click **Next**.

Step 3 Click the **Rule Config** tab.

Step 4 Click **Add Rule** to select rules.

The added rules will be display in the list. Click the text box under **Name** to edit the rule name. The rule is enabled by default.

Figure 8-21 Rule Configure (Video Metadata)

ID	Name	Type	On	Picture	Alarm
1	Rule 1	Vehicle Detection	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2	Rule 2	Non-Motor Vehicle Detection	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
3	Rule 3	Video Motion Detection	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

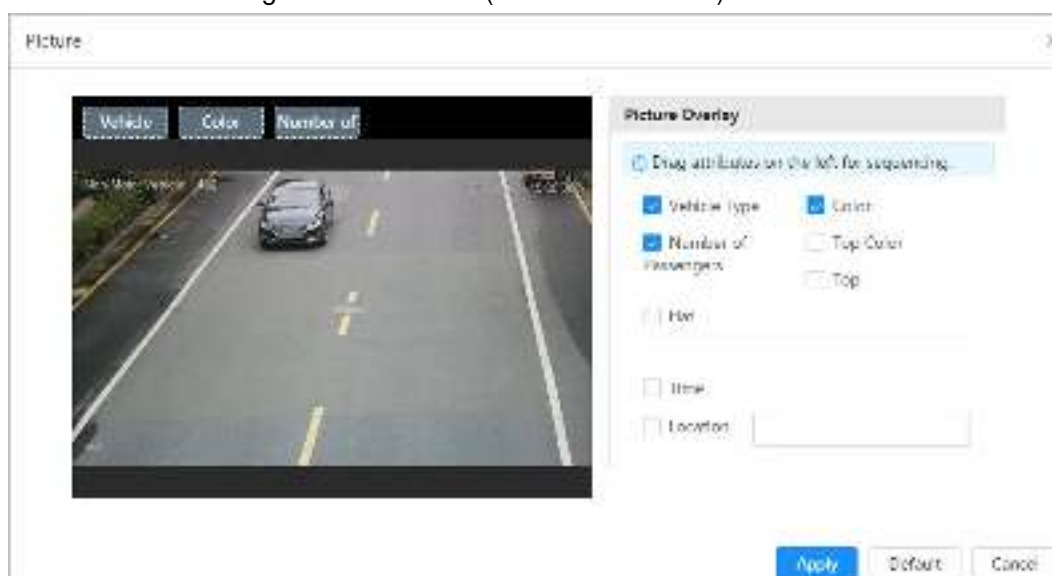
Step 5 Configure **Picture**.

1) Click .

2) Set overlay of motor vehicle, non-motor vehicle and people and the box position.

This section takes the configuration of non-motor vehicle overlay as an example.

Figure 8-22 Picture (non-motor vehicle)







3) Click **Apply**.

Step 6 (Optional) Click the icons at the right side of the image to filter targets in the image.

- After the rule is enabled, the detection area is displayed. Click , and you drag the any corner of the box to adjust the size of the area, and press the left mouse button and move the box to adjust the position.
- Click to draw an area exclusion area for face detection in the image, and right-click to finish the drawing..
- Click to draw the minimum size of the target, and click to draw the maximum size of the target. Only when the target size between the maximum size and the minimum size, can the alarm be triggered.
- Click , and then press and hold the left mouse button to draw a rectangle, the pixel size is displayed.
- Click to delete the detection line.

Step 7 Set parameters.

Table 8-10 Description of crowd map parameters

Parameter	Description
People Flow Statistics	Click  next to People Flow Statistics to count the number of people in the detection area.
Flow Statistics (Non-motor Vehicle)	Click  next to Flow Statistics (Non-motor Vehicle) to count the number of non-motor vehicles in the detection area.
Traffic Flow Stat	Click  next to Traffic Flow Statistics to count the number of motor vehicles in the detection area.
OSD	Click OSD Info , and the Overlay interface is displayed. Click  next to Enable to enable the target statistics function. For details, see "6.2.2.2.8 Configuring Target Statistics".
Snapshot Mode	<ul style="list-style-type: none"> Optimized: Capture the pictures until the vehicle disappears from the image, and report the clearest picture. Tripwire: Capture the pictures when the vehicle triggers tripwire as the configured direction. <ol style="list-style-type: none"> Select Tripwire. Select the direction from A to B, B to A, and Both. Adjust the position of rule line as needed..

Step 8 Set arming periods and alarm linkage action. For details, see "6.4.1.2 Alarm Linkage".
Click **+ Event Linkage** to set the linkage action.

Step 9 Click **Apply**.

To view alarm information on the alarm subscription tab, you need to subscribe relevant alarm event. For details, see "6.4.1.3.2 Subscribing Alarm Information".

8.5.3 Viewing Video Metadata Result

Generate data of video metadata recognition in report form.

Step 1 Select **Setting > Event > Video Metadata > Report**.

The **Report** interface is displayed.

Step 2 Select the report type, start time, end time, and other parameters.

Step 3 Click **Search** to complete the report.

The statistical results are displayed. Click **Export** to export the statistical report.

Figure 8-23 Video metadata report



9 Camera

Click **Camera** to configure camera parameters, including image parameters, encoder parameters, and audio parameters. For details, see "6.2 Camera".

10 Event

Click **Event** to configure general events, including alarm linkage exception, video detection, and audio detection. For details, see "6.4 Event".

11 System

Click **System**, and you can configure system parameters, including general, date & time, account, safety, PTZ settings, default, import/export, remote, auto maintain and upgrade. For details, see "6.6 System".

12 Security

12.1 Security Status

Background Information

Detect the user and service, and scan the security modules to check the security status of the camera, so that when abnormality appears, you can process it timely.

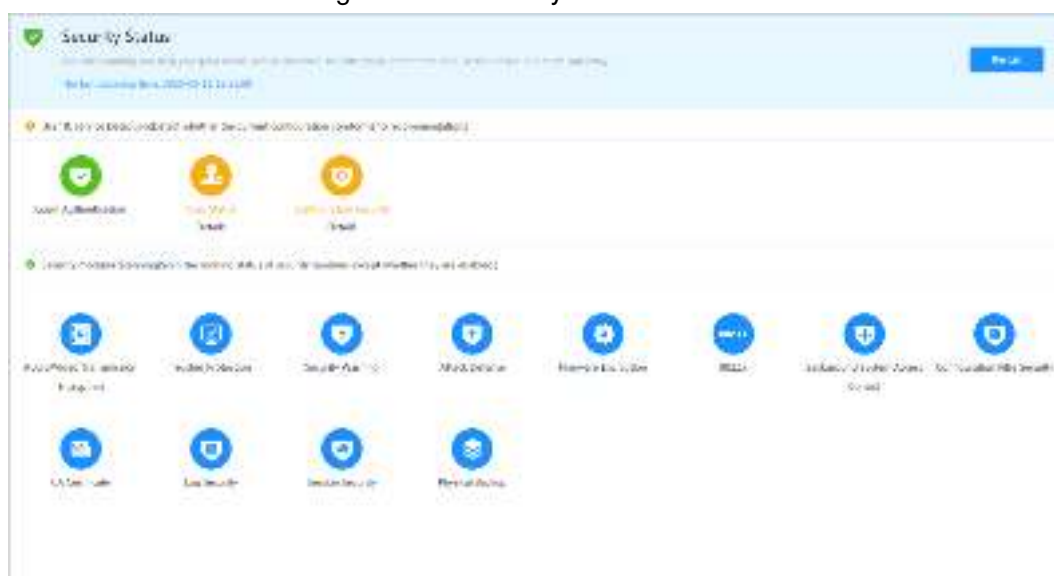
- User and service detection: Detect login authentication, user status, and configuration security to check whether the current configuration conforms to recommendation.
- Security modules scanning: Scan the running status of security modules, such as audio/video transmission, trusted protection, securing warning and attack defense, not detect whether they are enabled.

Procedure

Step 1 Select **Security > Security Status**.

Step 2 Click **Rescan** to scan the security status of the camera.

Figure 12-1 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.

1. Click **Details** to view the details of the scanning result.
2. Click **Ignore** to ignore the exception, and it will not be scanned in next scanning.
Click **Joint Detection**, and the exception will be scanned in next scanning.
3. Click **Optimize**, and the corresponding interface is displayed, and you can edit the configuration to clear the exception.

Figure 12-2 Security Status



12.2 System Service

12.2.1 802.1x

Cameras can connect to LAN after passing 802.1x authentication.

Step 1 Select **Security > System Service > 802.1x**.

Step 2 Select the NIC name as needed, and click ☐ to enable it.

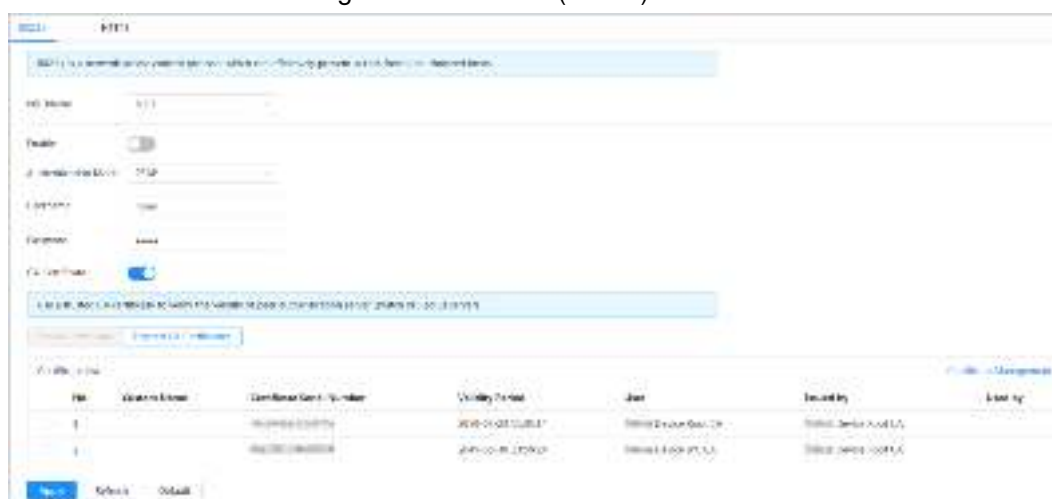
Step 3 Select the authentication mode, and then configure parameters.

- PEAP: Protected EAP protocol.
 1. Select PEAP as the authentication mode.
 2. Enter the username and password that has been authenticated on the server.
 3. Click ☐ next to CA certificate, and select the trusted CA certificate in list.



If there is no certificate in the list, click **Certificate Management** at the left navigation bar. For details, see "12.4.2 Installing Trusted CA Certificate".

Figure 12-3 802.1x (PEAP)



- 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. Click ☐ next to CA certificate, and select the trusted CA certificate in list.



If there is no certificate in the list, click **Certificate Management** at the left navigation bar. For details, see "12.4.2 Installing Trusted CA Certificate".

Figure 12-4 802.1x (TLS)



Step 4 Click **Apply**.

12.2.2 HTTPS

Create a certificate or upload an authenticated certificate, and then you can log in through HTTPS with your PC. The HTTPS can protect page authenticity on all types of websites, secure accounts, and keep user communications, identity, and web browsing private.

Procedure

Step 1 Select **Security > System Service > HTTPS**.

Step 2 Click ☐ to enable it.

Step 3 Select the certificate.



If there is no certificate in the list, click **Certificate Management** at the left navigation bar. For details, see

Figure 12-5 HTTPS



Step 4 Click **Apply**.

12.3 Attack Defense

12.3.1 Firewall

Configure firewall to limit access to the camera.

Step 1 Select **Security > Attack Defense > Firewall**.


Step 2 Click  to enable the firewall function.

Figure 12-6 Firewall

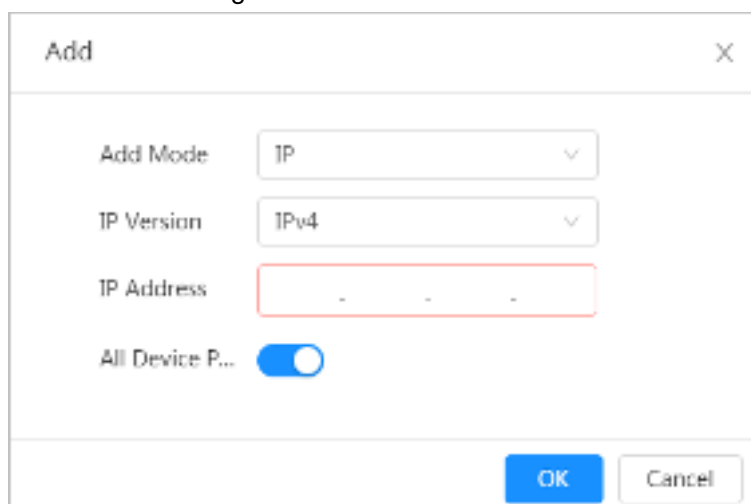


Step 3 Select the mode: **Allowlist** and **Blocklist**.

- **Allowlist**: Only when the IP/MAC of your PC in the allow list, can you access the camera. Ports are the same.
- **Blocklist**: When the IP/MAC of your PC is in the block list, you cannot access the camera. Ports are the same.



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

Figure 12-7 Firewall



Step 5 Click **Apply**.

Related Operations

- Click  to edit the host information.
- Click  to delete the host information.

12.3.2 Account Lockout

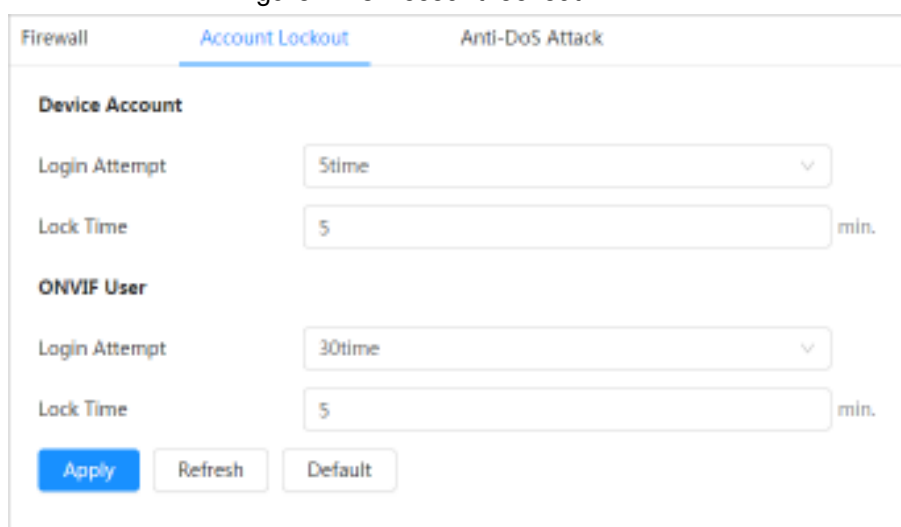
If you consecutively enter a wrong password more than the configured value, the account will be locked.

Step 1 Select **Security > Attack Defense > Account Lockout**.

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

- 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 12-8 Account lockout



Account Type	Login Attempt	Lock Time
Device Account	5	5 min.
ONVIF User	30	5 min.

Buttons: Apply, Refresh, Default

Step 3 Click **Apply**.

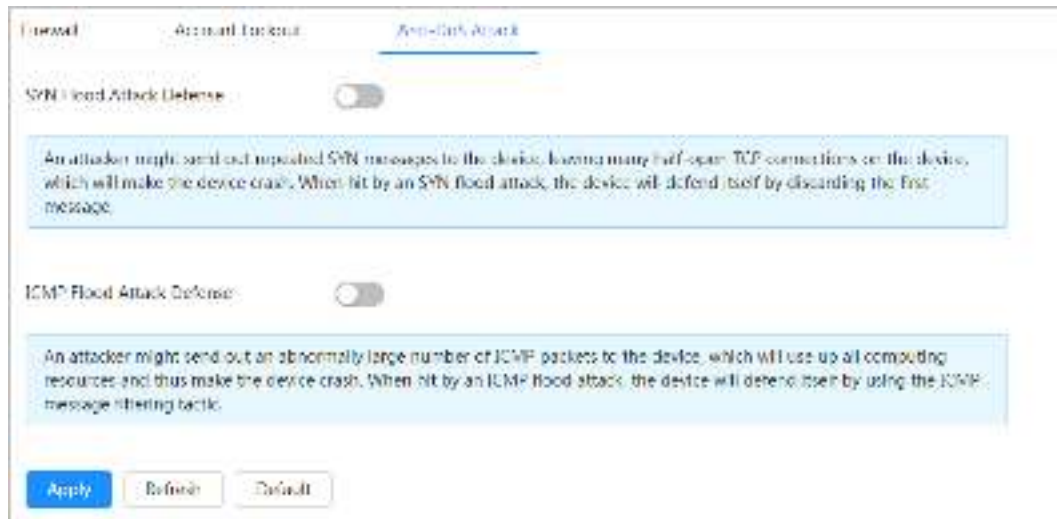
12.3.3 Anti-DoS Attack

You can enable **SYN Flood Attack Defense** and **ICMP Flood Attack Defense** to defend the device against Dos attack.

Step 1 Select **Security > Attack Defense > Anti-DoS Attack**.

Step 2 Select **SYN Flood Attack Defense** or **ICMP Flood Attack Defense** to defend the device against Dos attack.

Figure 12-9 Anti-DoS attack



12.4 CA Certificate

12.4.1 Installing Device Certificate

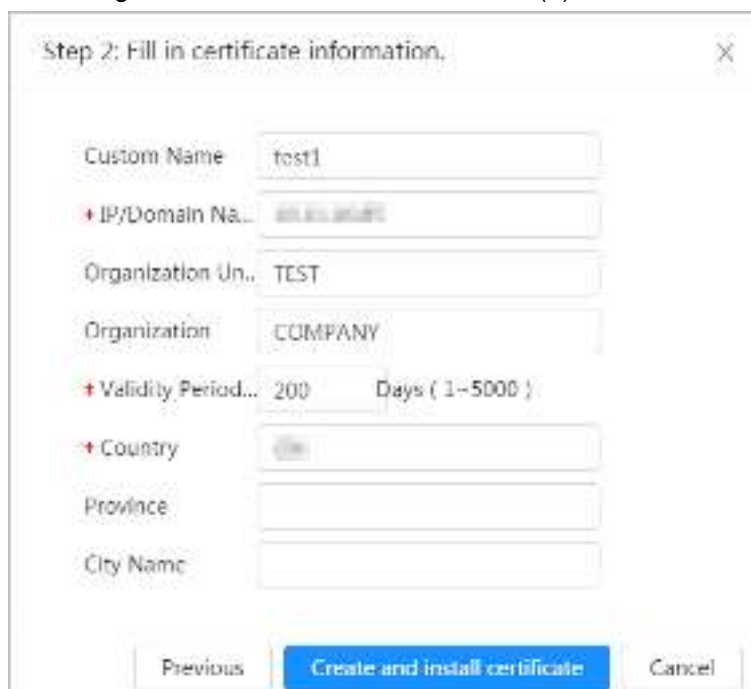
Create a certificate or upload an authenticated certificate, and then you can log in through HTTPS with your PC.

12.4.1.1 Creating Certificate

Creating certificate in the device.

- Step 1 Select **Security > CA Certificate > Device Certificate**.
- Step 2 Select **Installing Device Certificate**.
- Step 3 Select **Create Certificate**, and click **Next**.
- Step 4 Enter the certificate information.



Figure 12-10 Certificate information (1)



Step 5 Click **Create and install certificate**.

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

Related Operations

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

12.4.1.2 Applying for and Importing CA Certificate

Import the third-party CA certificate to the camera.

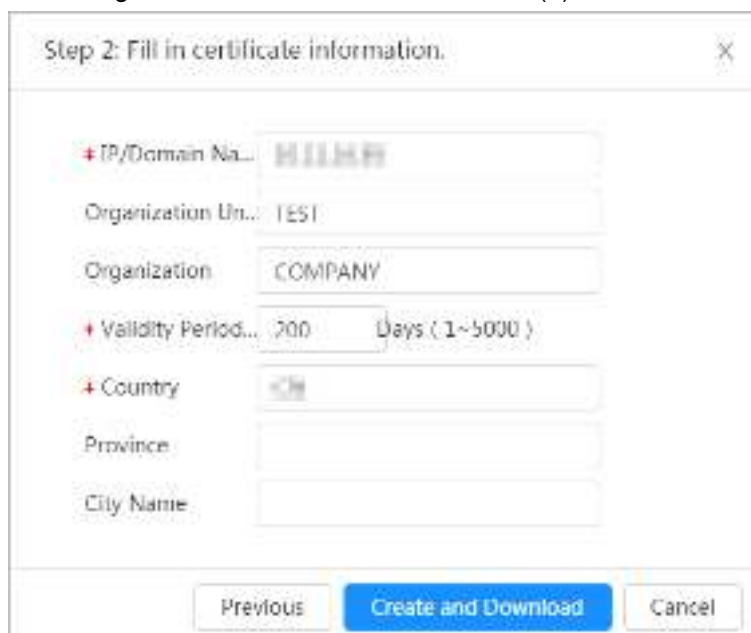
Step 1 Select **Security > CA Certificate > Device Certificate**.

Step 2 Select **Installing Device Certificate**.

Step 3 Select **Apply for CA Certificate and Import (Recommended)**, and click **Next**.

Step 4 Enter the certificate information.

Figure 12-11 Certificate information (2)



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) Do **Step1** to **Step3**, and click **Browse** to select the signed CE certificate.

3) Click **Install and Import**.

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

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

Related Operations

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

12.4.1.3 Installing Existing Certificate

Import the existing third-party certificate to the camera. When apply for the third-party certificate, you also need to apply for the private key file and private key password.

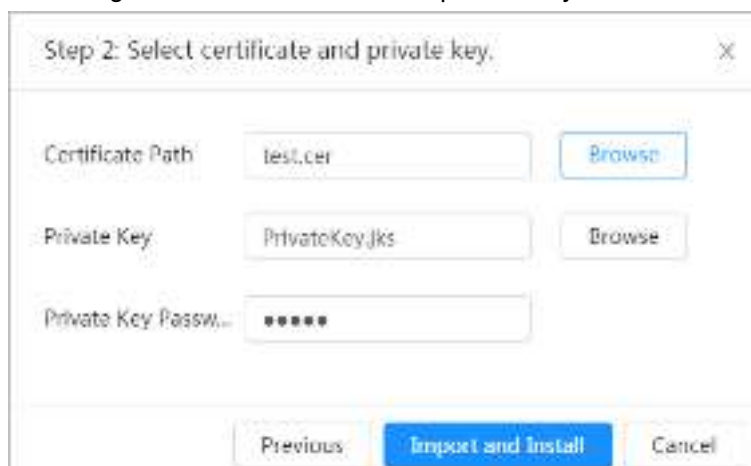
Step 1 Select **Security > CA Certificate > Device Certificate**.

Step 2 Select **Installing Device Certificate**.

Step 3 Select **Install Existing Certificate**, and click **Next**.

Step 4 Click **Browse** to select the certificate and private key file, and enter the private key password.



Figure 12-12 Certificate and private key



Step 5 Click **Import and Install**.

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

Related Operations

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

12.4.2 Installing Trusted CA Certificate

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.

Step 1 Select **Security > CA Certificate > Trusted CA Certificates**.

Step 2 Select **Installing Trusted Certificate**.

Step 3 Click **Browse** to select the certificate.



Figure 12-13 Installing trusted certificate



Step 4 Click **OK**.

After the certificate is created successfully, you can view the created certificate on the **Trusted CA Certificate** interface.

Related Operations

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

12.5 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 Select **Security > A/V Encryption**.

Step 2 Configure the parameters.

Figure 12-14 A/V encryption



Table 12-1 A/V encryption parameter

Area	Parameter	Description
Private Protocol	Enable	Enables stream frame encryption by using private protocol.  There might be safety risk if this service is disabled.
	Encryption Type	Use the default setting.
	Update Period of Secret Key	Secret key update period. Value range: 0–720 hours. 0 means never update the secret key. Default value: 12.
RTSP over TLS	Enable	Enables RTSP stream encryption by using TLS.  There might be safety risk if this service is disabled.
	Select a device certificate	Select a device certificate for RTSP over TLS.
	Certificate Management	For details about certificate management, see "12.4.1 Installing Device Certificate".

Step 3 Click **Apply**.

12.6 Security Warning

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

Step 1 Select **Security** > **Security Warning**.

Step 2 Click ☐ next to **Enable** to enable security warning.

Step 3 Configure the parameters.

Figure 12-15 Security warning



Step 4 Set arming periods and alarm linkage action. For details, see "6.4.1.2 Alarm Linkage". Click **+ Event Linkage** to set the linkage action.

Step 5 Click **Apply**.

13 Record

This section introduces the functions and operations of video playback.

13.1 Playback

13.1.1 Playing Back Video

This section introduces the operation of video playback.

Prerequisites

- This function is available on the camera with SD card.
- Before playing back video, configure record time range, record storage method, record schedule and record control. For details, see "13.2 Setting Record Control", "13.3 Setting Record Plan", and "13.4 Storage".

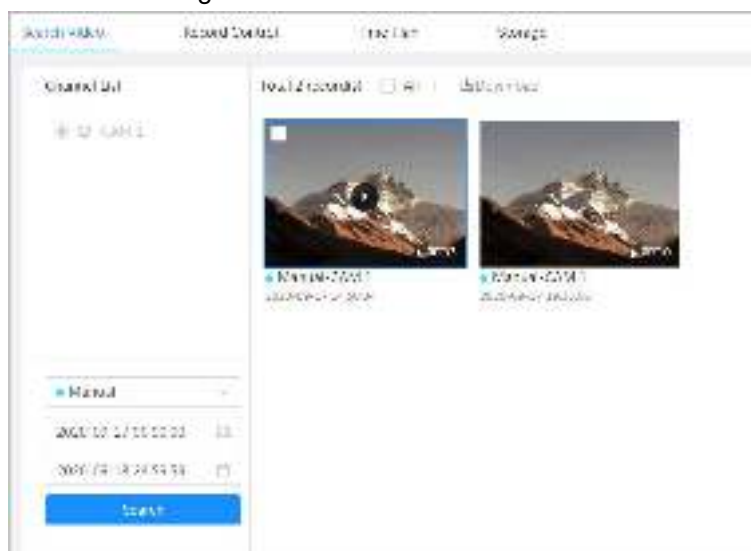
Procedure

Step 1 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**.
When selecting **Event** as the record type, you can select the specific event types, such as **Motion Detection**, **Video Tamper** and **Scene Changing**.
- The dates with blue dots indicate there are videos recorded on those days.

Figure 13-1 Search video



















Step 3 Point to the searched video, and then click  to play back the selected video. The video playback interface is displayed.

Figure 13-2 Video playback



Table 13-1 Description of video playback interface

No	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 interface.
2	Digital Zoom	You can zoom video image of the selected area through two operations. <ul style="list-style-type: none"> 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. In zoom in state, drag the image to check other area. Click the icon, and then scroll the mouse wheel in the video image to zoom in or out.
	AI Rule	Click  , and then select Enable to display AI rules and detection box; select Disable to stop the display. It is enabled by default.  AI rules is valid only when you enabled the rule during recording.
	Play control bar	Controls playback. <ul style="list-style-type: none"> : 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. <ul style="list-style-type: none"> : 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.

No	Function	Description
	Sound	Controls the sound during playback. <ul style="list-style-type: none"> : Mute mode. : Vocal state. You can adjust the sound.
	Snapshot	Click  to capture one picture of the current image, and it will be saved to the configured storage path.  About viewing or configuring storage path, see "6.1 Local".
	Video clip	Click  , and clip a certain recorded video and save it. For details, see "13.1.2 Clipping Video".
	Full Screen	Click  , and the image is displayed in full-screen mode; double-click the image or press Esc button to exit full-screen mode.
3	Progress bar	Displays the record type and the corresponding period. <ul style="list-style-type: none"> 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

13.1.2 Clipping Video

Step 1 Click .

Step 2 Drag the clipping box on the progress bar to select the start time and end time of the target video

Figure 13-3 Clipping video



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

Step 4 Select the download format and storage path.

Figure 13-4 Clipping video



Step 5 Click **Start Download**.

The playback stops and the clipped file is saved in the configured storage path. For details of storage path, see "6.1 Local".

13.1.3 Downloading Video

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



- Playback and downloading at the same time is not supported.
- Operations might vary with different browsers, and the actual product shall prevail.
- For details of viewing or setting storage path, see "6.1 Local".

Step 1 Select **Record > Search Video**.

Step 2 Select the channel, the record type, and record time, and the click **Search**.

Step 3 Select the videos to be downloaded.

- Select ☐ at the upper-right corner of each video file to select one or multiple videos.
- Select ☐ next to **Select All** to select all searched videos.

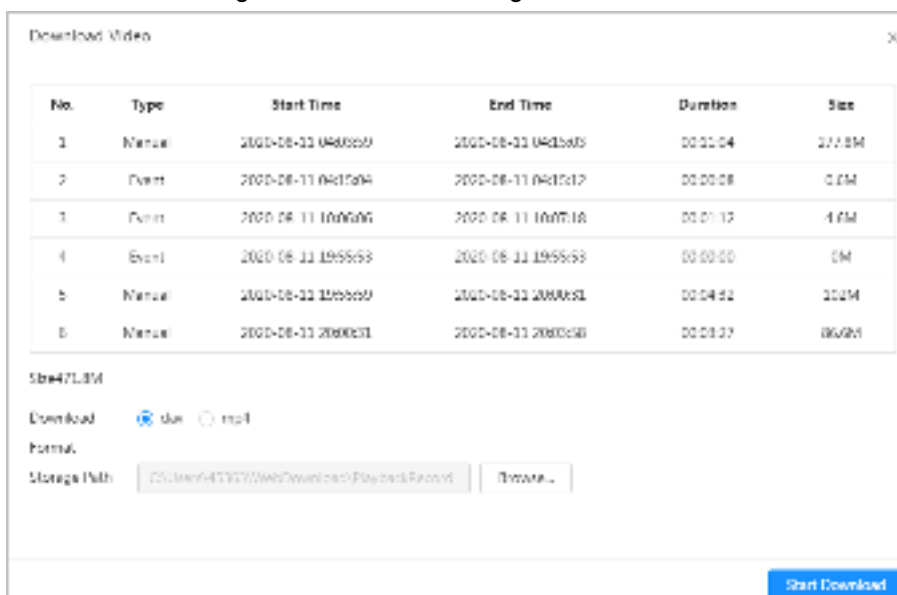
Figure 13-5 Selecting video file



Step 4 Click **Download**.

Step 5 Select the download format and storage path.

Figure 13-6 Downloading video



No.	Type	Start Time	End Time	Duration	Size
1	Manual	2020-08-11 04:00:00	2020-08-11 04:15:00	00:15:04	277.8M
2	Event	2020-08-11 04:15:04	2020-08-11 04:15:12	00:00:08	0.0M
3	Event	2020-08-11 10:00:00	2020-08-11 10:00:10	00:00:10	4.0M
4	Event	2020-08-11 19:55:53	2020-08-11 19:55:53	00:00:00	0M
5	Manual	2020-08-11 20:00:00	2020-08-11 20:00:01	00:00:01	10.0M
6	Manual	2020-08-11 20:00:01	2020-08-11 20:00:03	00:00:02	10.0M

Size: 471.8M

Download: ☒ all ☐ part

Format:

Storage Path: C:\Users\Administrator\AppData\Local\Temp\Download\Record\ [Browse...]

Start Download

Step 6 Click **Start Download**.

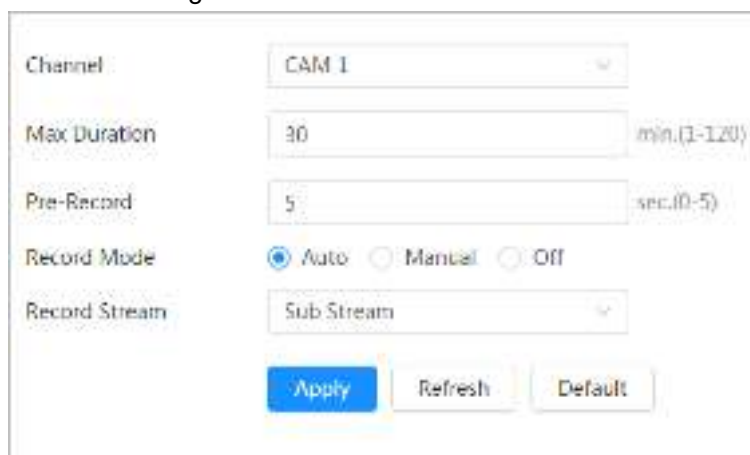
The downloaded files are saved in the configured storage path. For details of storage path, see "6.1 Local".

13.2 Setting Record Control

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

Step 1 Click **Record** in the main interface, and then click the **Record Control** tab.

Figure 13-7 Record control



Channel: CAM 1

Max Duration: 30 min (1-120)

Pre-Record: 5 sec (0-5)

Record Mode: ☒ Auto ☐ Manual ☐ Off


Record Stream: Sub Stream

Apply Refresh Default

Step 2 Set parameters.

Table 13-2 Description of record control parameters

Parameter	Description
Max Duration	The time for packing each video file.

Parameter	Description
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.
Record Stream	Select record stream, including Main Stream and Sub Stream .

Step 3 Click **Apply**.

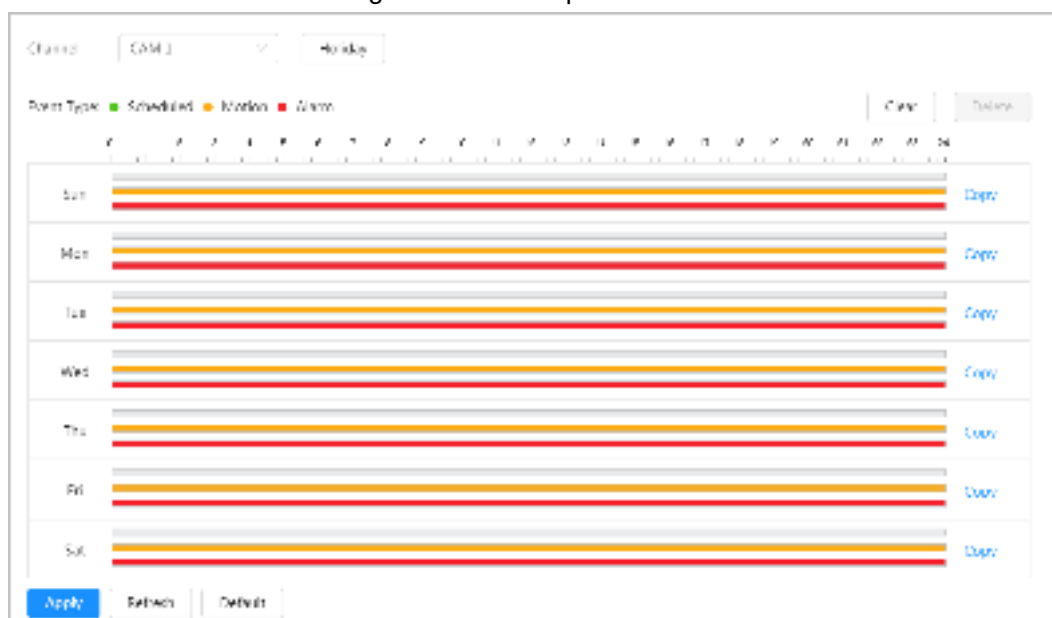
13.3 Setting Record Plan

After the corresponding alarm type (**Normal**, **Motion**, and **Alarm**) is enabled, the record channel links recording.

Set certain days as holiday, and when the **Record** is selected in the holiday schedule, the system records video as holiday schedule defined.

Step 1 Click **Record** on the main interface, and then click the **Time Plan** tab.

Figure 13-8 Time plan



Step 2 Set record plan.

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). Select a record type, such as **Normal**, and directly press and drag the left mouse button to set the time period for normal record on the timeline.

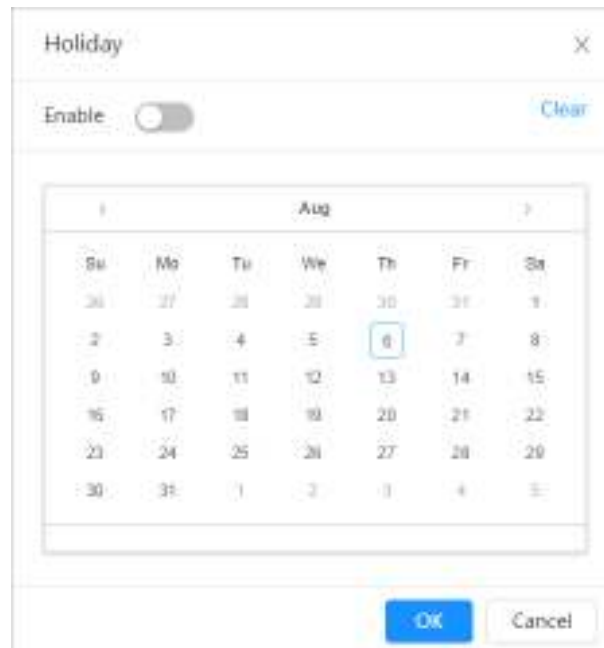



- Click **Copy** next to a day, and select the days that you want to copy to in the prompt interface, you can copy the configuration to the selected days. Select the **Select All** check box to select all day to copy the configuration.
- You can set 6 time periods per day.

Step 3 Click **Apply**.

Step 4 Click **Holiday** to set holidays.

Figure 13-9 Time plan



Step 5 Click  to enable the holiday configuration, and select the days that you need to set as holiday
Click **Clear** to cancel the selection.



When holiday schedule setting is not the same as the general setting, holiday schedule setting is prior to the general setting. For example, with holiday schedule enabled, if the day is holiday, the system snapshots or records as holiday schedule setting; otherwise, the system snapshots or records as general setting.

Step 6 Click **OK**.

13.4 Storage

This section introduces the configuration of the storage method for the recorded videos.

Step 1 Select **Record > Storage**.

Figure 13-10 Live

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

Table 13-3 Description of storage parameters

Parameter	Description
Event Type	Select from Scheduled , Motion Detection and Alarm .
Disk Full	Recording strategy when the disk is full. <ul style="list-style-type: none"> Overwrite: Cyclically overwrite the earliest video when the disk is full. Stop: Stop recording when the disk is full.
Storage Method	Select from Local storage and Network storage <ul style="list-style-type: none"> Local storage: Save the recorded videos in the internal SD card. <div> </div> Local storage is displayed only on models that support SD card. Network storage: Save the recorded videos in the FTP server or NAS.

Step 3 Click **Apply**.

13.4.1 Local Storage

Step 1 Select **Record > Storage**.

Step 2 Select the recording strategy in **Disk Full**.

- Overwrite**: Cyclically overwrite the earliest video when the disk is full.
- Stop**: Stop recording when the disk is full.

Step 3 Select **Local storage** in **Storage Method** to save the recorded videos in the internal SD card.

Figure 13-11 Local storage

Step 4 Click **Apply**.

13.4.2 Network Storage

You can select from **FTP** and **NAS**.

When the network does not work, you can save all the files to the internal SD card for emergency.

13.4.2.1 FTP

Enable this function, and you can save all the files in the FTP server.

Step 1 Select **Record > Storage**.

Step 2 Select the recording strategy in **Disk Full**.

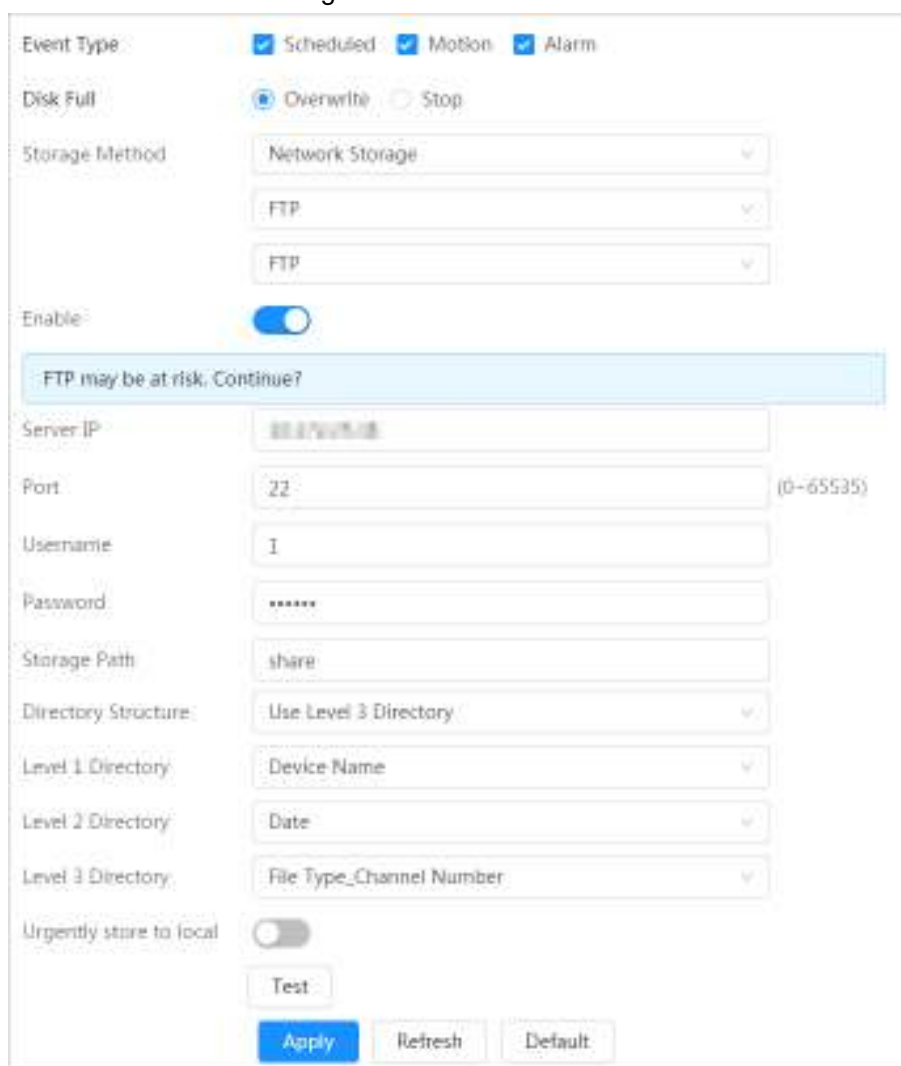
- **Overwrite**: Cyclically overwrite the earliest video when the disk is full.
- **Stop**: Stop recording when the disk is full.

Step 3 Select **Network storage** in **Storage Method**, and select **FTP** to save the recorded videos in FTP server.

You select **FTP** or **SFPT** from the drop-down list. **SFPT** is recommended to enhance network security.

Step 4 Click ☐ next to **Enable** to enable the FTP function.

Figure 13-12 FTP



Event Type: ☒ Scheduled ☒ Motion ☒ Alarm

Disk Full: ☒ Overwrite ☐ Stop

Storage Method: Network Storage

FTP

FTP

Enable: ☒

FTP may be at risk. Continue?

Server IP: 192.168.1.100

Port: 22 (0-65535)

Username: I

Password: *****

Storage Path: share

Directory Structure: Use Level 3 Directory

Level 1 Directory: Device Name

Level 2 Directory: Date

Level 3 Directory: File Type_Channel Number


Urgently store to local: ☐

Test

Apply Refresh Default

Step 5 Configure FTP parameters.

Table 13-4 Description of FTP parameters

Parameter	Description
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.
Directory Structure	Set the directory structure, and you can select Use Level 1 Directory , Use Level 2 Directory , and Use Level 3 Directory
Level 1 Directory	Set the Level 1 directory name, and you can select from Device name , Device IP , and Custom . When you select Custom , please enter the custom directory.
Level 2 Directory	Set the Level 2 directory name, and you can select from File Type , Date , File Type_Channel Number , and Custom . When you select Custom , please enter the custom directory.
Level 3 Directory	
Urgently store to local	Click  , and when the FTP server does not work, all the files are saved to the internal SD card.

Step 6 Click **Save**.

Step 7 Click **Test** to test whether FTP function works normally.

13.4.2.2 NAS

Enable this function, and you can save all the files in the NAS.

Step 1 Select **Record > Storage**.

Step 2 Select the recording strategy in **Disk Full**.

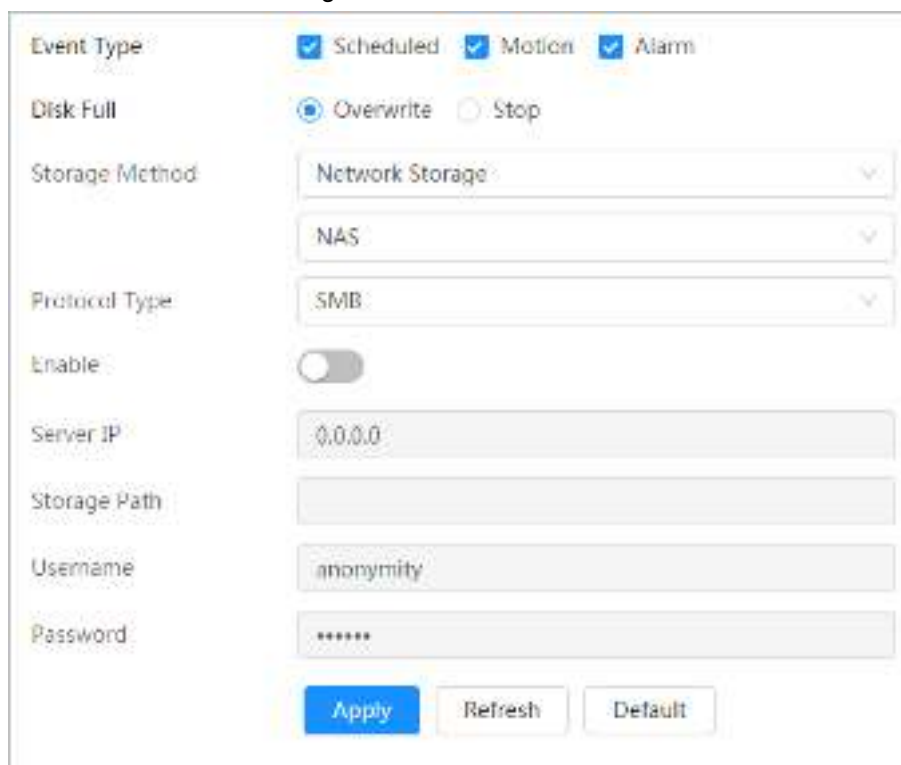
- **Overwrite**: Cyclically overwrite the earliest video when the disk is full.
- **Stop**: Stop recording when the disk is full.

Step 3 Select **Network storage** in **Storage Method**, and select **NAS** to save the recorded videos in NAS server.

Step 4 Select NAS protocol type.

- **NFS** (Network File System): A file system which enables computers in the same network share files through TCP/IP.
- **SMB** (Server Message Block): Provides shared access for clients and the server.

Figure 13-13 FTP



Event Type ☒ Scheduled ☒ Motion ☒ Alarm

Disk Full ☒ Overwrite ☐ Stop

Storage Method Network Storage

NAS

Protocol Type SMB

Enable ☐

Server IP 0.0.0.0

Storage Path

Username anonymity

Password *****

Apply Refresh Default

Step 5 Configure NAS parameters.

Table 13-5 Description of NAS parameters

Parameter	Description
Server IP	The IP address of the NAS server.
Storage Path	The destination path in the NAS server.
Username	When selecting SMB protocol, you are required to enter username and password. Enter them as needed.
Password	

Step 6 Click **Apply**.

14 Picture

This section introduces the related functions and operations of picture playback.

14.1 Playback

14.1.1 Playing Back Picture

This section introduces the operation of picture playback.

Prerequisites

- This function is available on the camera with SD card.
- Before playing back picture, configure snapshot time range, snapshot storage method, snapshot plan. For details, see "14.3 Setting Snapshot Plan".

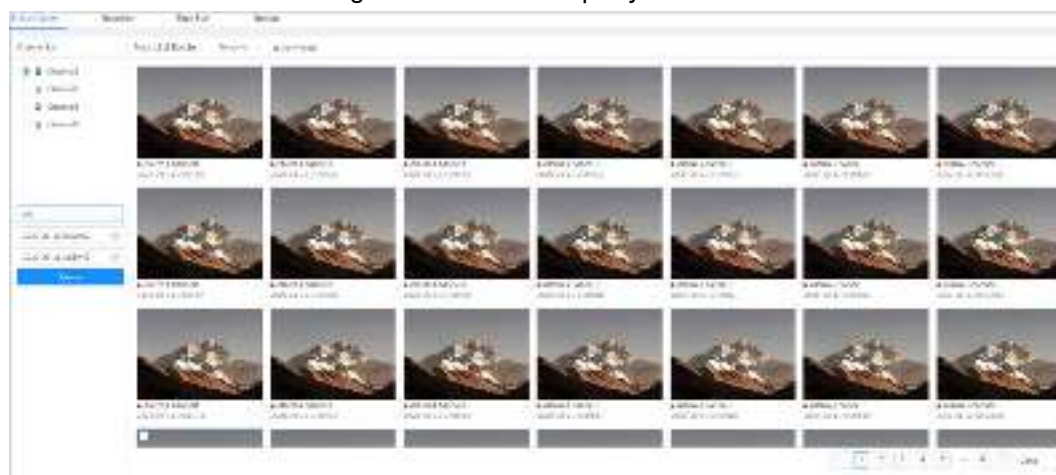
Procedure

Step 1 Select **Record > Picture Query**.

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**, **General**, **Event**, and **Alarm**.
When selecting **Event** as the snapshot type, you can select the specific event types, such as **Motion Detection**, **Video Tamper** and **Scene Changing**.
- The dates with blue dots indicate there are snapshots on those days.

Figure 14-1 Picture query








Step 3 Point to the searched picture, and then click  to play back the selected picture. The picture playback interface is displayed.

Figure 14-2 Picture playback



Table 14-1 Description of playback interface

No	Function	Description
1	Snapshot list	Displays all searched snapshots. Click any files to play back it. Click Back at the upper-left corner to go to the Picture Query interface.
2	Manual display	<ul style="list-style-type: none"> Click  to display the previous snapshot in the snapshot list. Click  to display the next snapshot in the snapshot list.
3	Slide show	Click  to display the snapshots list one by one in slide show mode.
4	Full Screen	Click  , and the snapshot is displayed in full-screen mode; double-click the image or press Esc button to exit full-screen mode.

14.1.2 Downloading Picture

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



- Operations might vary with different browsers, and the actual product shall prevail.
- For details of viewing or setting storage path, see "6.1 Local".

Step 1 Select **Picture > Picture Query**.

Step 2 Select the channel, the snapshot type, and snapshot time, and then click **Search**.

Step 3 Select the pictures to be downloaded.

- Select ☐ at the upper-right corner of each picture file to select one or multiple pictures.
- Select ☐ next to **Select All** to select all searched pictures.

Figure 14-3 Selecting picture file



Step 4 Click **Download**.

Step 5 Select the download format and storage path.

Figure 14-4 Downloading picture



Step 6 Click **Start Download**.

The downloaded pictures are saved in the configured storage path. For details of storage path, see "6.1 Local".

14.2 Setting Snapshot Parameters

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

Step 1 Select **Picture > Snapshot**.

Step 2 Select the channel and set the parameters.

Figure 14-5 Snapshot

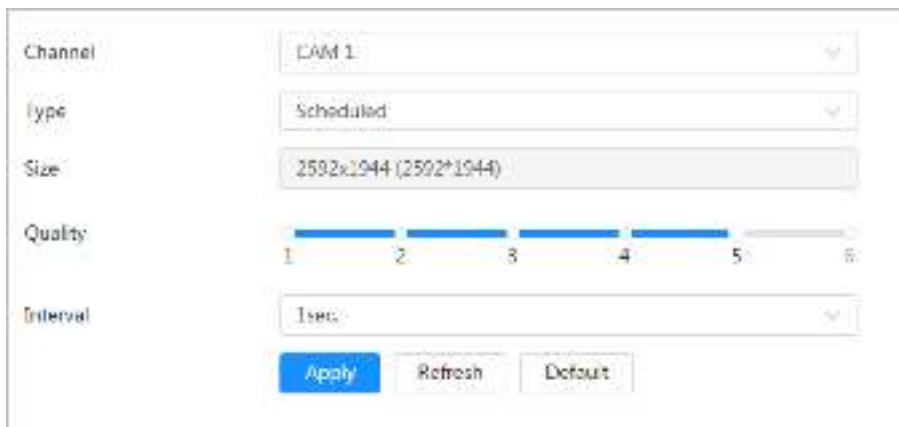



Table 14-2 Description of snapshot parameters

Parameter	Description
Type	<p>You can select from Scheduled and Event.</p> <ul style="list-style-type: none"> • Scheduled: Capture images in configured period. For details, see • Event: Capture images when configured event is triggered, such as Motion Detection, Video Tamper and Scene Changing.  <p>Make sure that you have enable the corresponding event detection and the snapshot function.</p>
Size	It is same with the resolution of the main stream.
Quality	Set the quality of the snapshot. The higher the value, the better the quality.
Interval	Set the frequency of snapshot. You can select Custom to set the frequency as needed.

Step 3 Click **Apply**.

14.3 Setting Snapshot Plan

According to the configured snapshot plan, the system enables or disables snapshot at corresponding time. For detailed operation, see "13.3 Setting Record Plan".

14.4 Storage

Set the storage method for the snapshot. For detailed operation, see "13.4 Storage".

15 Report

You can search the result of face detection.

Step 1 Select **Report > Face Detection**.

Step 2 Select the channel, and set the time.

Click **Advance**, and you can set face attributes.

Step 3 Click **Search**.

Figure 15-1 Face detection Report



Step 4 Click the picture, and you can view the details.

Figure 15-2 Details



Appendix 1 Cybersecurity Recommendations

Cybersecurity is more than just a buzzword: it's something that pertains to every device that is connected to the internet. IP video surveillance is not immune to cyber risks, but taking basic steps toward protecting and strengthening networks and networked appliances will make them less susceptible to attacks. Below are some tips and recommendations on how to create a more secured security system.

Mandatory actions to be taken for basic equipment network security:

1. Use Strong Passwords

Please refer to the following suggestions to set passwords:

- The length should not be less than 8 characters;
- Include at least two types of characters; character types include upper and lower case letters, numbers and symbols;
- Do not contain the account name or the account name in reverse order;
- Do not use continuous characters, such as 123, abc, etc.;
- Do not use overlapped characters, such as 111, aaa, etc.;

2. Update Firmware and Client Software in Time

- According to the standard procedure in Tech-industry, we recommend to keep your equipment (such as NVR, DVR, IP camera, etc.) firmware up-to-date to ensure the system is equipped with the latest security patches and fixes. When the equipment is connected to the public network, it is recommended to enable the "auto-check for updates" function to obtain timely information of firmware updates released by the manufacturer.
- We suggest that you download and use the latest version of client software.

"Nice to have" recommendations to improve your equipment network security:

1. Physical Protection

We suggest that you perform physical protection to equipment, especially storage devices. For example, place the equipment in a special computer room and cabinet, and implement well-done access control permission and key management to prevent unauthorized personnel from carrying out physical contacts such as damaging hardware, unauthorized connection of removable equipment (such as USB flash disk, serial port), etc.

2. Change Passwords Regularly

We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.

3. Set and Update Passwords Reset Information Timely

The equipment supports password reset function. Please set up related information for password reset in time, including the end user's mailbox and password protection questions. If the information changes, please modify it in time. When setting password protection questions, it is suggested not to use those that can be easily guessed.

4. Enable Account Lock

The account lock feature is enabled by default, and we recommend you to keep it on to guarantee the account security. If an attacker attempts to log in with the wrong password several times, the corresponding account and the source IP address will be locked.

5. Change Default HTTP and Other Service Ports

We suggest you to change default HTTP and other service ports into any set of numbers

between 1024~65535, reducing the risk of outsiders being able to guess which ports you are using.

6. **Enable HTTPS**

We suggest you to enable HTTPS, so that you visit Web service through a secure communication channel.

7. **MAC Address Binding**

We recommend you to bind the IP and MAC address of the gateway to the equipment, thus reducing the risk of ARP spoofing.

8. **Assign Accounts and Privileges Reasonably**

According to business and management requirements, reasonably add users and assign a minimum set of permissions to them.

9. **Disable Unnecessary Services and Choose Secure Modes**

If not needed, it is recommended to turn off some services such as SNMP, SMTP, UPnP, etc., to reduce risks.

If necessary, it is highly recommended that you use safe modes, including but not limited to the following services:

- SNMP: Choose SNMP v3, and set up strong encryption passwords and authentication passwords.
- SMTP: Choose TLS to access mailbox server.
- FTP: Choose SFTP, and set up strong passwords.
- AP hotspot: Choose WPA2-PSK encryption mode, and set up strong passwords.

10. **Audio and Video Encrypted Transmission**

If your audio and video data contents are very important or sensitive, we recommend that you use encrypted transmission function, to reduce the risk of audio and video data being stolen during transmission.

Reminder: encrypted transmission will cause some loss in transmission efficiency.

11. **Secure Auditing**

- Check online users: we suggest that you check online users regularly to see if the device is logged in without authorization.
- Check equipment log: By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.

12. **Network Log**

Due to the limited storage capacity of the equipment, the stored log is limited. If you need to save the log for a long time, it is recommended that you enable the network log function to ensure that the critical logs are synchronized to the network log server for tracing.

13. **Construct a Safe Network Environment**

In order to better ensure the safety of equipment and reduce potential cyber risks, we recommend:

- Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.
- The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.
- Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.
- Enable IP/MAC address filtering function to limit the range of hosts allowed to access the

device.

ENABLING A SAFER SOCIETY AND SMARTER LIVING