



Panoramic Fisheye Network Camera

Quick Start Guide






Foreword

General

This manual introduces the functions, installation and operations of the 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, could result in property damage, data loss, lower performance, or unpredictable result.
 NOTE	Provides additional information as supplement to the text.

Revision History

Version	Revision Content	Release Date
V1.0.0	First release.	November, 2021

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, fingerprints, and license plate number. You need to be in compliance with your local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures which include but are not limited: Providing clear and visible identification to inform people of the existence of the surveillance area and provide required contact information.

About the Manual

- The manual is for reference only. Slight differences might be found between the manual and the product.
- We are not liable for losses incurred due to operating of the product in ways that are not in compliance with the manual.
- The manual will be updated according to the latest laws and regulations of related jurisdictions. For detailed information, see the paper User Manual, use our CD-ROM, scan the QR code or visit our official website. The manual is for reference only. Slight differences might be found between the electronic version and the paper version.
- All the designs and software are subject to change without prior written notice. Product updates might result in some differences appearing between the actual product and the

manual. Please contact customer service for the latest program and supplementary documentation.

- There might be deviations in the description of the technical data, functions and operations, or errors in the 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 any problems occur while 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 should conform to your local electrical safety codes.
- The power supply must conform to the requirements of ES1 in IEC 62368-1 standard and be no higher than PS2. Note that the power supply requirements are subject to the device label.
- Make sure the power supply is correct before operating the device.
- A readily accessible disconnect 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 or dusty environment, extremely hot or cold temperatures, 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 disassembling operation about the device; otherwise, it might cause water leakage or poor image quality due to unprofessional operations. Make sure that the gasket ring is flat and properly installed in the groove before installing the cover. Contact after-sales 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).
- We recommend using the device together with lightning arrester to improve lightning protection effect.
- We recommend grounding 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 decrease, do not use volatile solvent such as alcohol, benzene, diluent 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 moistened soft cloth. You can also remove dust with an air blower.

**WARNING**

- Please 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 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	III
1 Introduction	1
1.1 Cable	1
1.2 Connecting Alarm Input/output	2
2 Network Configuration	4
2.1 Initializing Device.....	4
2.2 Changing Device IP Address	6
2.3 Logging in Web Page	7
3 Installation	8
3.1 Packing List.....	8
3.2 Dimension.....	8
3.3 Installing Device	9
3.3.1 Installation Method.....	9
3.3.2 Installing SD Card (Optional)	10
3.3.3 Attaching Device.....	10
3.3.4 Installing Waterproof Connector.....	14

1 Introduction

1.1 Cable



Waterproof all the cable joints with insulating tape and waterproof tape to avoid short circuit and water damage. For detailed operation, see FAQ manual.

Figure 1-1 Cables

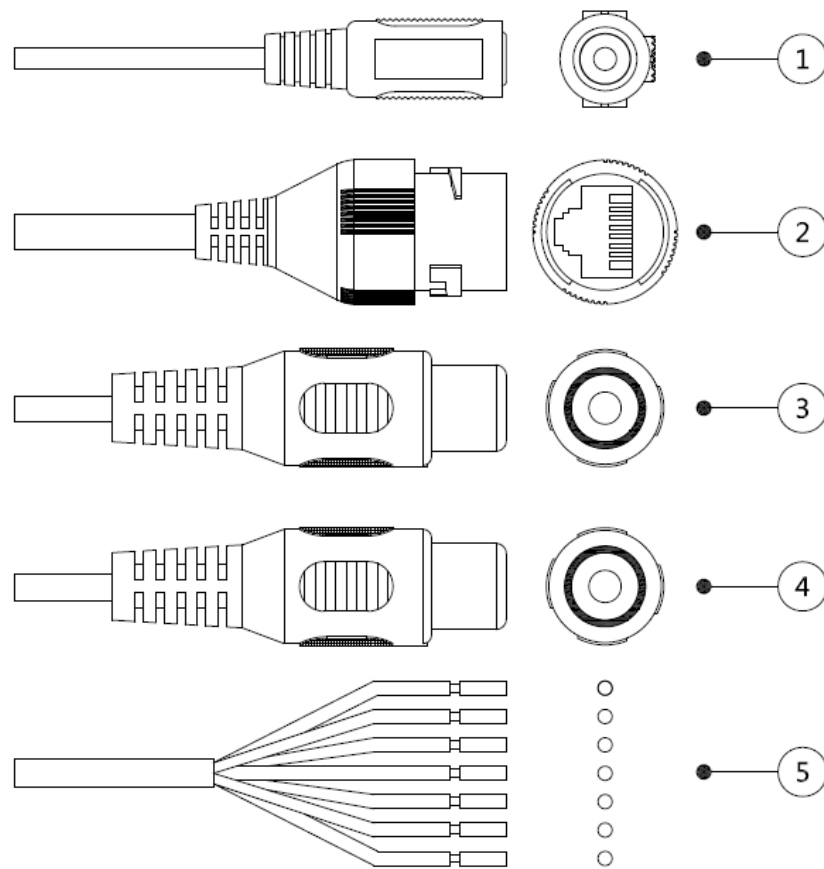



Table 1-1 Cable information

No.	Port Name	Description
1	Power input	<p>Inputs 12 VDC power. Please be sure to supply power as instructed in the Guide.</p> <p></p> <p>Device abnormality or damage could occur if power is not supplied correctly.</p>




No.	Port Name	Description
2	Ethernet Port	<ul style="list-style-type: none"> Connects to network with network cable. Provides power to the device with PoE.  PoE is available on select model.
3	Audio input	Connects to sound-pick-up device to receive audio signal.
4	Audio output	Connects to speaker to output audio signal.
5	Alarm I/O	Includes alarm signal input and output ports, the number of I/O ports might vary on different devices. For detailed information, see Table 1-2.

Table 1-2 Alarm I/O port information

Port name	No.	Connector name	Description
I/O port	1	ALARM_OUT1	Alarm output port 1 outputs alarm signal to alarm device.
	2	ALM_OUT_GND1	 When connecting to alarm device, only the ALARM_OUT 1 port and ALARM_OUT_GND 1 port with the same number can be used together.
	3	ALARM_IN1	Alarm input port 1 receives the switch signal of external alarm source.
	4	ALARM_IN2	Alarm input port 2 receives the switch signal of external alarm source.
	5	ALM_IN_GND	Alarm input GND.
	6	ALARM_OUT2	Alarm output port 2 outputs alarm signal to alarm device.
	7	ALM_OUT_GND2	 When connecting to alarm device, only the ALARM_OUT 2 port and ALARM_OUT_GND 2 port with the same number can be used together.

1.2 Connecting Alarm Input/output

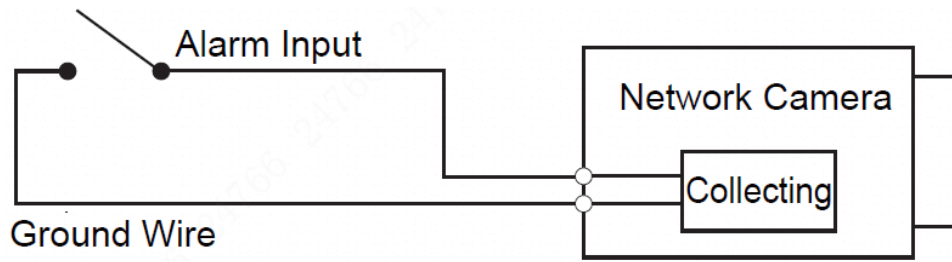


Alarm input/output is available on select models.

Step 1 Connect alarm input device to the alarm input end of the I/O port.

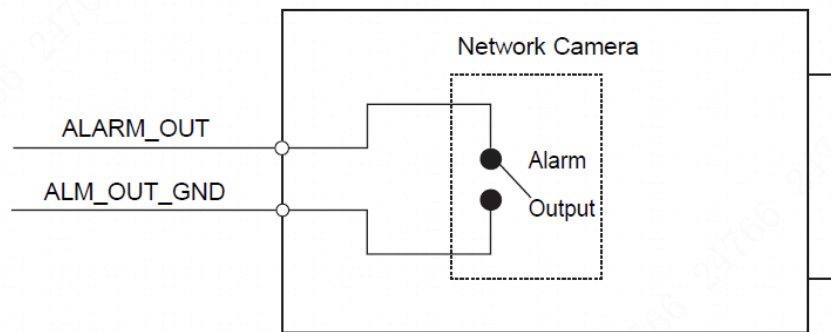
Device collects different states of alarm input port when the input signal is idling and being grounded. Device collects logic "1" when input signal connecting to 3.3 V or idling; device collects logic "0" when input signal being grounded.

Figure 1-2 Alarm input



- Step 2** Connect alarm output device to the alarm output end of the I/O port. The alarm output is relay switch output, which can only connect to NO alarm devices. The ALARM_OUT port and the ALM_OUT_GND port with the same number constitute a switch for alarm output. The switch is open normally and closes when there is alarm output.

Figure 1-3 Alarm output



- Step 3** Log in web page, and configure alarm input and alarm output in alarm setting.
- The alarm input on the web page is corresponding to the alarm input end of the I/O port. There will be high level and low level alarm signal generated by the alarm input device when alarm occurs, set the input mode to "NO" (default) if the alarm input signal is logic "0" and to "NC" if the alarm input signal is logic "1".
 - The alarm output in the web page is corresponding to the alarm output end of the device, which is also the alarm output end of the I/O port.

2 Network Configuration

Device initialization and IP setting can be finished with the ConfigTool or in web page. For more information, see web operation manual.



- Device initialization is available on select models, and it is required at first use and after device is being reset.
- Device initialization is available only when the IP addresses of the device (192.168.1.108 by default) and the PC stays in the same network segment.
- Planning useable network segment properly to connect the device to the network.
- The following figures and interfaces are for reference only.

2.1 Initializing Device

Step 1 Double-click ConfigTool.exe to open the tool.

Step 2 Click **Modify IP**.

Step 3 Click **Search Setting**.

Figure 2-1 Setting

Step 4 Select the searching way.

- **Current Segment Search (default)**
Select the **Current Segment Search** checkbox. Enter the username in the **Username** box and the password in the **Password** box. The system will search for devices accordingly.
- **Other Segment Search**
Select the **Other Segment Search** checkbox. Enter IP address in the **Start IP** box and **End IP** box respectively. Enter username and password. The system will search for the devices accordingly.



- If you select the **Current Segment Search** checkbox and the **Other Segment Search** checkbox together, the system searches for devices under both conditions.

- Enter username and password when you want to change IP, configure the system, update the device, restart the device, and more.

Step 5 Click **OK**.

Step 6 Select one or several devices in uninitialized status, and then click **Initialize**.

Step 7 Select the devices to be initialized, and then click **Initialize**.

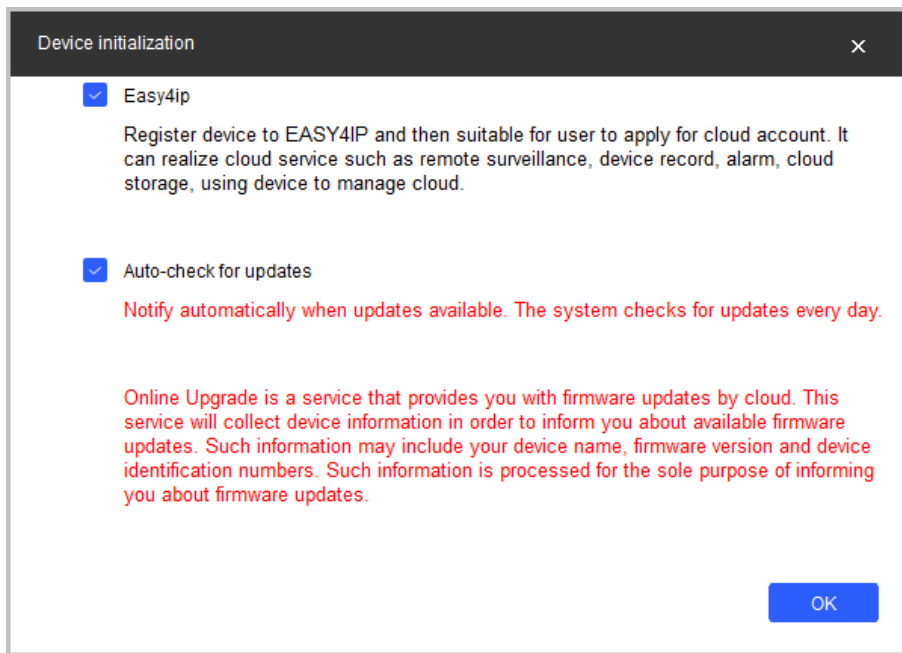


- If you do not provide the linked information for password reset, you can reset the password only through XML file.
- When initializing multiple devices, ConfigTool initializes all devices based on the password reset mode of the first selected device.

Figure 2-2 Password setting

Step 8 Set and confirm the password of the devices, then enter a valid email address, and then click **Next**.

Figure 2-3 Device initialization



Step 9 Select **Easy4ip** or select **Auto-check for updates** as needed. If neither, leave them unselected.

Step 10 Click **OK** to initialize the device.

Click the success icon (✓) or the failure icon (⚠) for the details.

Step 11 Click **Finish**.

2.2 Changing Device IP Address

- You can change IP address of one or multiple devices in one time. This section is based on changing IP addresses in batches.
- Changing IP addresses in batches is available only when the corresponding devices have the same login password.

Step 1 Follow Step 1 to Step 4 in "2.1 Initializing Device" to search devices in your network segment.



After clicking **Search setting**, please make sure the **username** and **password** are the same as what you set during initialization, otherwise there will be "wrong password" notice.

Step 2 Select the devices whose IP addresses need to be modified, and then click **Batch Modify IP**.

Figure 2-4 Change IP address

Step 3 Select **Static** mode and enter start IP, subnet mask and gateway.



- IP addresses of multiple devices will be set to the same if you select **Same IP**.
- If DHCP server is available in the network, devices will automatically obtain IP addresses from DHCP server when you select **DHCP**.

Step 4 Click **OK**.

2.3 Logging in to Web Page

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

If the setup wizard is displayed, follow the instructions to finish the settings.

Step 2 Enter the username and password in the login box, and then click **Login**.

Step 3 For the first-time login, click **Click Here to Download Plugin** and install the plugin as instructed.

The home page is displayed when the installation is finished.

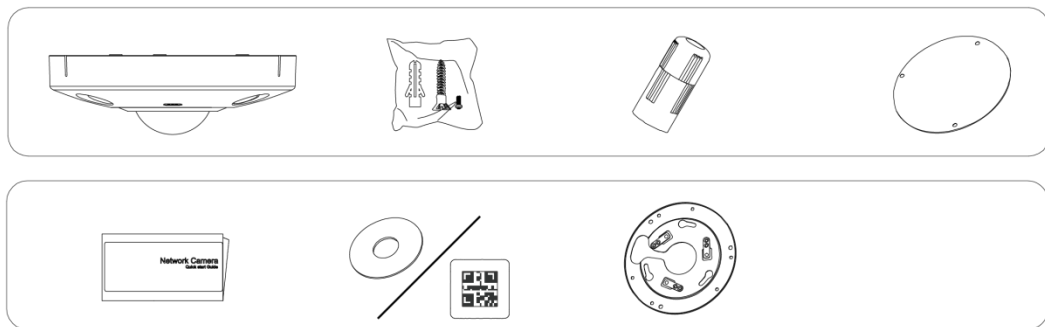
3 Installation

3.1 Packing List



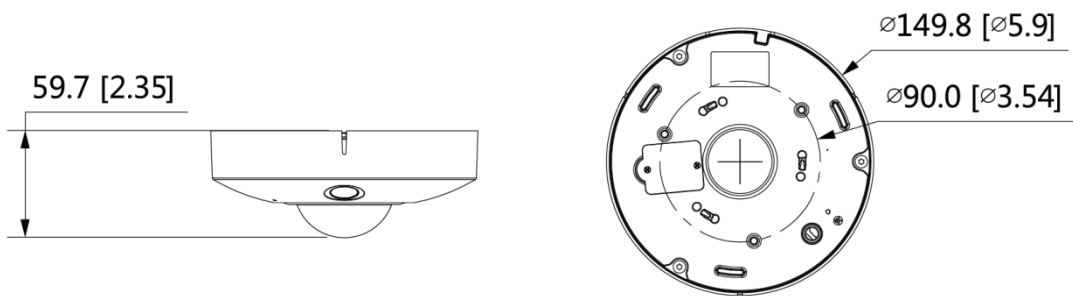
- The tools required for the installation including electric drill are not provided in the packing.
- The operation manual and related tool are contained in the disk or the QR code.

Figure 3-1 Packing list



3.2 Dimension

Figure 3-2 Dimensions (mm[inch])



3.3 Installing Device

3.3.1 Installation Method

Figure 3-3 Installation Type

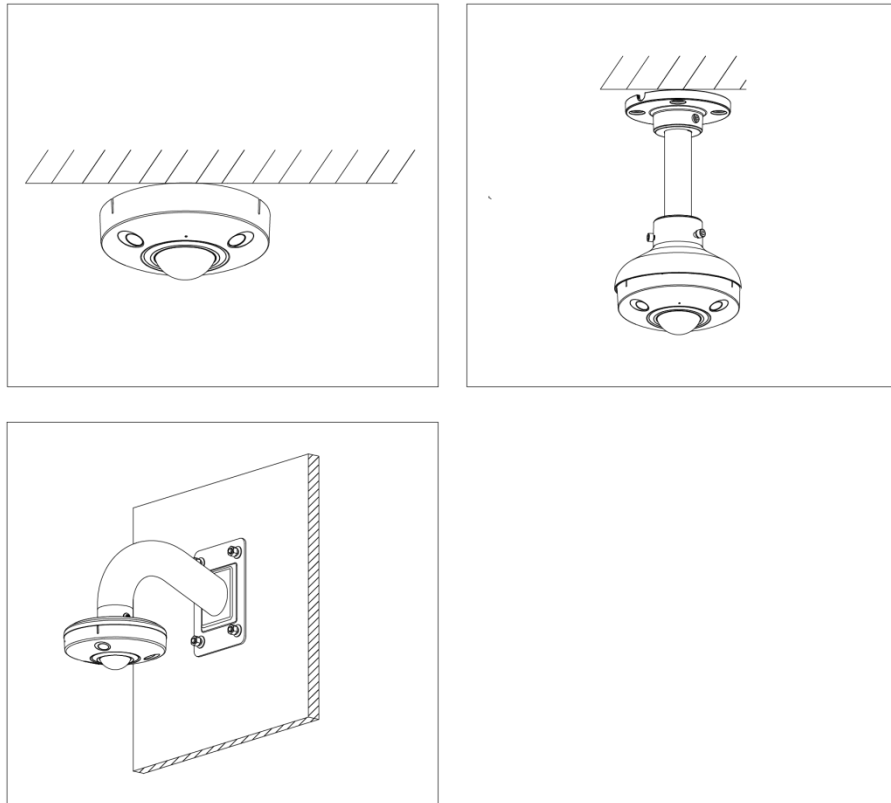
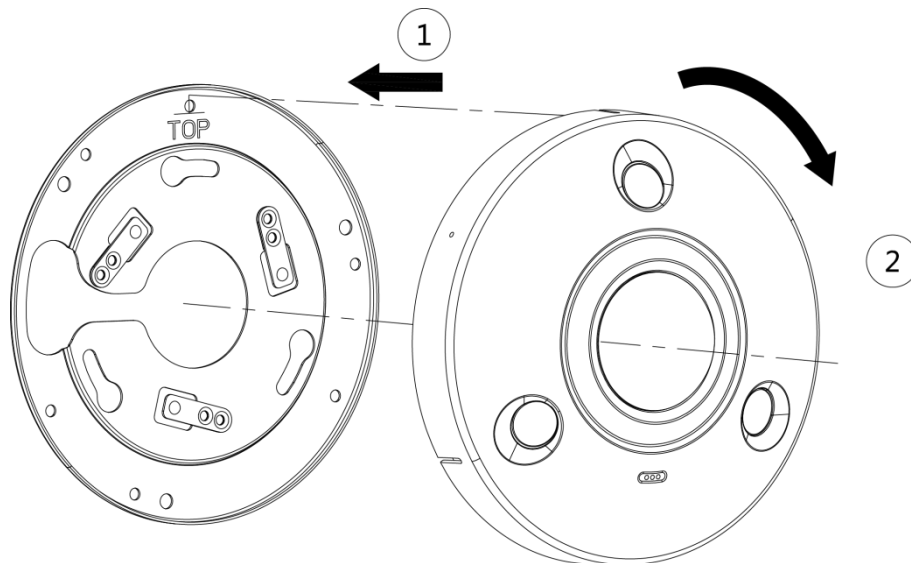


Figure 3-4 Covering Mode



Find the gap on the camera body; align it with the "TOP" on the corresponding quick mounting board, rotate the camera body clockwise to complete installation.

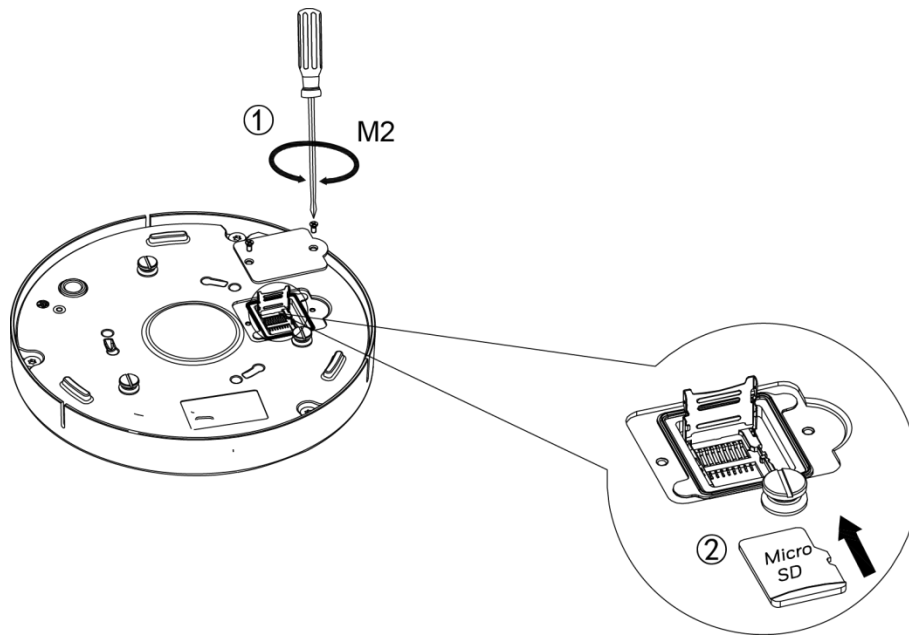
3.3.2 Installing SD Card (Optional)

- SD card slot is available on select models.
- Please disconnect the power from the device before installing the SD card.



Press the reset button for 10 seconds to reset the device.

Figure 3-5 Install SD card



3.3.3 Attaching Device




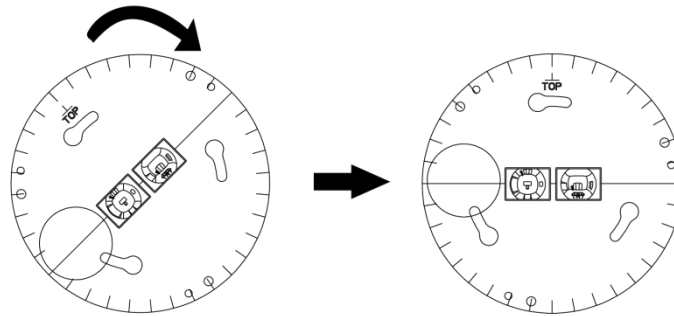
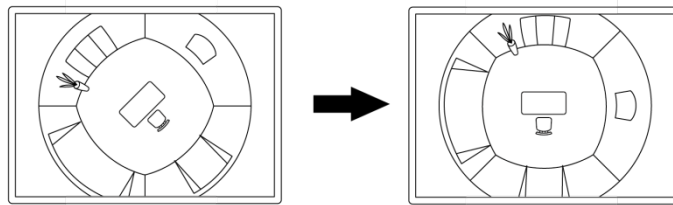
- Make sure the mounting surface is strong enough to hold at least three times of the total weight of device and bracket.
- Connect the host grounding hole () to ground wire, which can improve device reliability effectively. The ground hole is located next to the cable exit hole which is on the back of the bottom cover; the specification of grounding screw is M2.5.

Figure 3-6 Attach device

Positioning Map



Ceiling-mount



Wall-mount

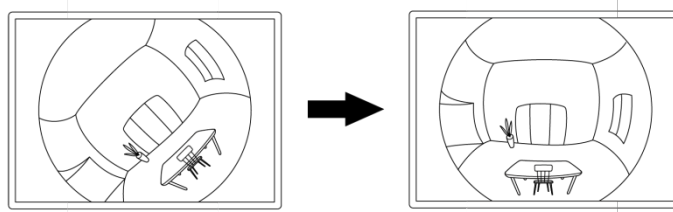


Figure 3-7 Cable going through ceiling-mount

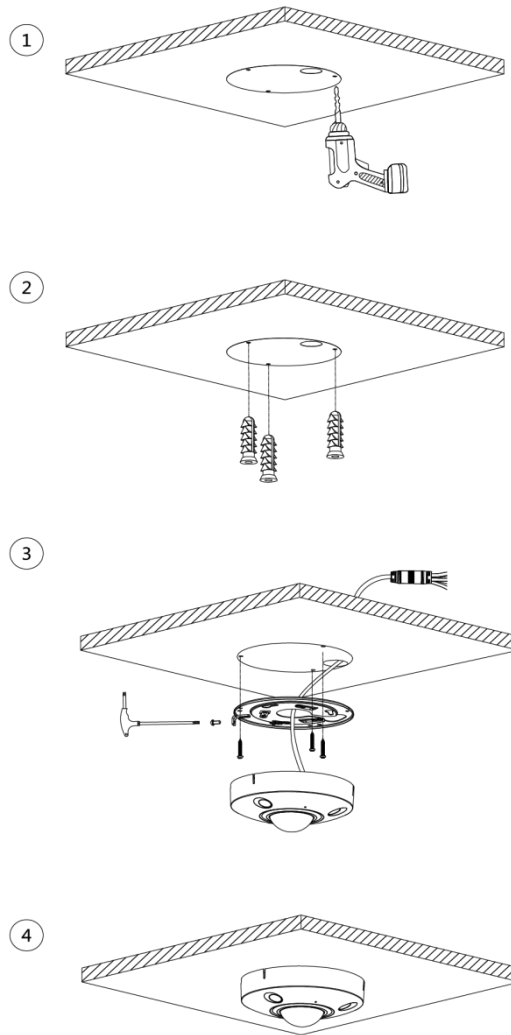
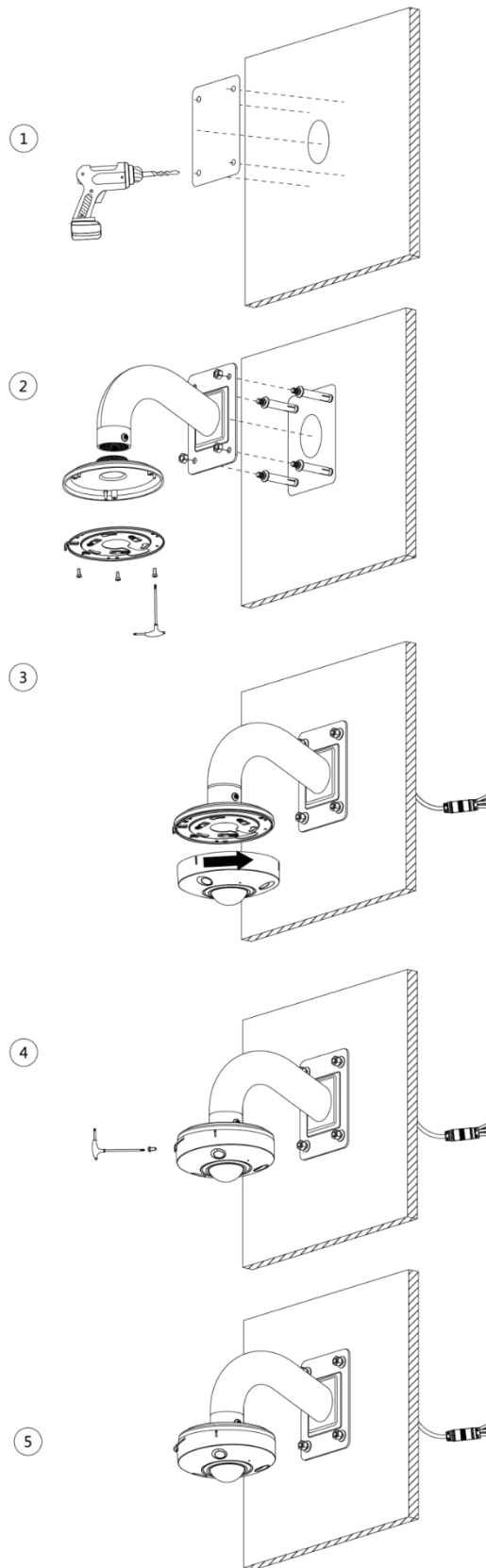


Figure 3-8 Cable going through wall-mount

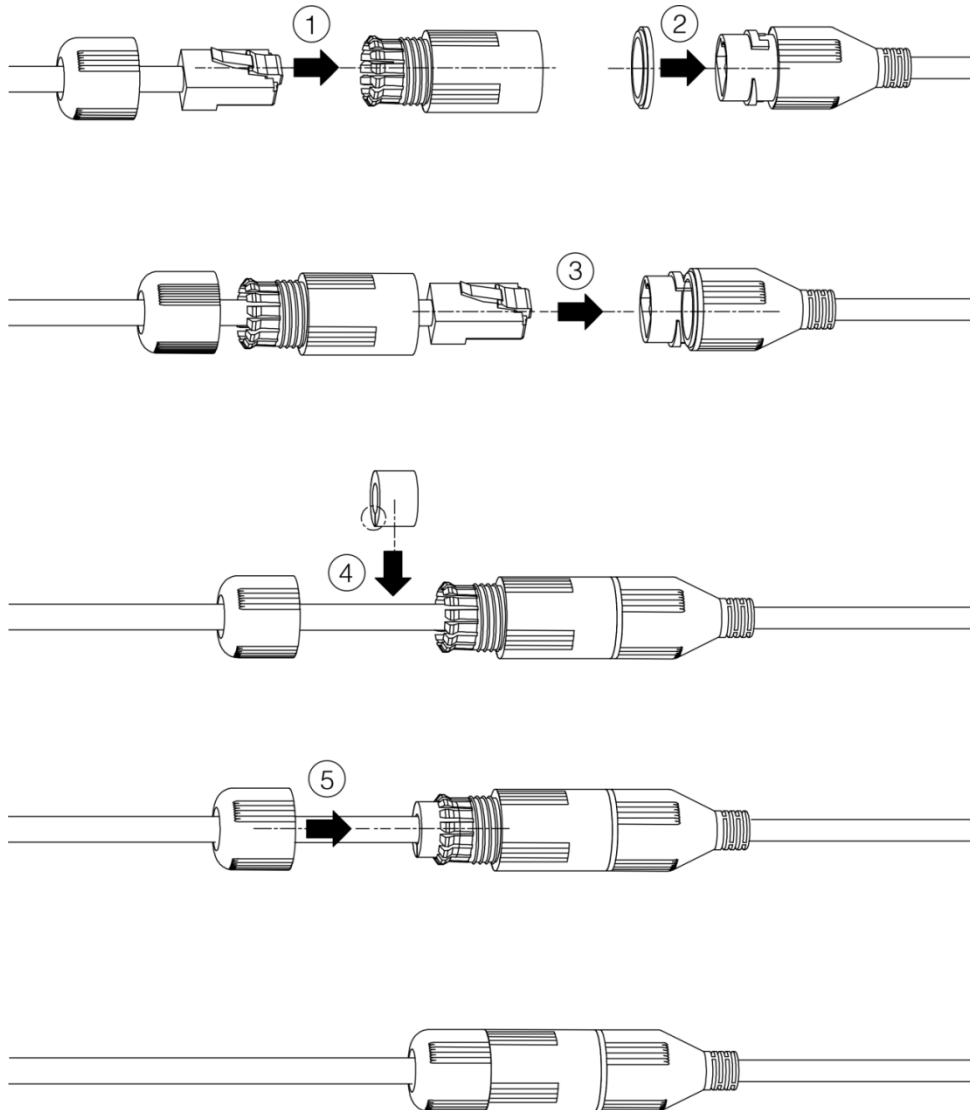


3.3.4 Installing Waterproof Connector



This part is only needed when a waterproof connector comes with the device and the device is used outdoors.

Figure 3-9 Install waterproof connector



ENABLING A SAFER SOCIETY AND SMARTER LIVING

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.

Address: No.1199 Bin'an Road, Binjiang District, Hangzhou, P. R. China | Website: www.dahuasecurity.com | Postcode: 310053

Email: overseas@dahuatech.com | Fax: +86-571-87688815 | Tel: +86-571-87688883



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 signal words 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, could result in property damage, data loss, reductions in performance, or unpredictable results.
 TIPS	Provides methods to help you solve a problem or save time.
 NOTE	Provides additional information as a supplement to the text.

Revision History

Version	Revision Content	Release Date
V1.0.2	<ul style="list-style-type: none"> Added "6.2.2.2.14 Configuring Parking Space". Added "8.5 Setting Vehicle Density". Added "8.6 Setting Parking Space". Added "12.1.4 Crowd Distribution". Added "12.1.5 Vehicle Density". Updated "8.11 Setting ANPR". 	July 2021
V1.0.1	<ul style="list-style-type: none"> Added "8.8 Setting People Counting" and "8.10 Setting Heat Map". Added "6.2.1.9 Fisheye" and "7.4.4 Fisheye". Updated "8.2 Setting Face Recognition". Updated "12 Report". 	May 2021
V1.0.0	First release.	September 2020

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, fingerprints, and car plate number. You need to be in compliance with your local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures which include but are not limited: Providing clear and visible identification to inform people of the existence of the surveillance area and provide required contact information.

About the Manual

- The manual is for reference only. Slight differences might be found between the manual and the product.
- We are not liable for losses incurred due to operating the product in ways that are not in compliance with the manual.
- The manual will be updated according to the latest laws and regulations of related jurisdictions. For detailed information, see the paper user's manual, use our CD-ROM, scan the QR code or visit our official website. The manual is for reference only. Slight differences might be found between the electronic version and the paper version.
- All designs and software are subject to change without prior written notice. Product updates might result in some differences appearing between the actual product and the manual. Please contact customer service for the latest program and supplementary documentation.
- There might be errors in the print or deviations in the description of the functions, operations and technical data. 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 company names in the manual are properties of their respective owners.
- Please visit our website, contact the supplier or customer service if any problems occur while 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.
- Use power supply that meets ES1 but does not exceed PS2 limits defined in IEC 62368-1. For specific power supply requirements, refer to device labels.
- 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.....	III
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	5
3 Device Initialization	6
4 Login	10
4.1 Device Login.....	10
4.2 Resetting Password	11
5 Main Interface	13
6 Setting.....	14
6.1 Local	14
6.2 Camera.....	15
6.2.1 Setting Image Parameters.....	15
6.2.1.1 Interface Layout	15
6.2.1.2 Image	17
6.2.1.3 Exposure.....	18
6.2.1.4 Backlight	20
6.2.1.5 WB.....	21
6.2.1.6 Day/Night.....	22
6.2.1.7 Illuminator.....	22
6.2.1.8 Defog.....	24
6.2.1.9 Fisheye	24
6.2.2 Setting Encode Parameters	25
6.2.2.1 Encode.....	25
6.2.2.2 Overlay	27
6.2.2.2.1 Configuring Privacy Masking.....	27
6.2.2.2.2 Configuring Channel Title	28
6.2.2.2.3 Configuring Time Title.....	29
6.2.2.2.4 Configuring Location	29
6.2.2.2.5 Configuring Font Properties	30

6.2.2.2.6 Configuring Picture Overlay.....	30
6.2.2.2.7 Configuring Custom Title.....	31
6.2.2.2.8 Configuring Target Statistics	31
6.2.2.2.9 Configuring ANPR.....	32
6.2.2.2.10 Configuring Face Detection	33
6.2.2.2.11 Configuring Face Recognition	33
6.2.2.2.12 Configuring Face Statistics.....	34
6.2.2.2.13 Configure Face&Body Counting	34
6.2.2.2.14 Configuring Parking Space	35
6.2.2.3 ROI.....	36
6.2.3 Audio.....	36
6.2.3.1 Setting Audio Parameters	36
6.2.3.2 Setting Alarm Tone	37
6.3 Network.....	39
6.3.1 TCP/IP.....	39
6.3.2 Port.....	41
6.3.3 PPPoE.....	43
6.3.4 DDNS	43
6.3.5 Email.....	44
6.3.6 UPnP	46
6.3.7 SNMP	47
6.3.8 Bonjour	49
6.3.9 Multicast.....	50
6.3.10 Register	51
6.3.11 QoS.....	51
6.3.12 Platform Access.....	52
6.3.12.1 P2P.....	52
6.3.12.2 ONVIF	53
6.3.12.3 RTMP.....	53
6.3.13 Basic Service	54
6.4 Event	56
6.4.1 Setting Alarm Linkage.....	56
6.4.1.1 Setting Alarm-in	56
6.4.1.2 Alarm Linkage.....	57
6.4.1.2.1 Adding Schedule	57
6.4.1.2.2 Record Linkage.....	58
6.4.1.2.3 Snapshot Linkage	59

6.4.1.2.4 Alarm-out Linkage.....	59
6.4.1.2.5 Email Linkage.....	59
6.4.1.3 Subscribing Alarm	60
6.4.1.3.1 About Alarm Types.....	60
6.4.1.3.2 Subscribing Alarm Information	60
6.4.2 Setting Exception	61
6.4.2.1 Setting SD Card Exception	61
6.4.2.2 Setting Network Exception.....	62
6.4.2.3 Setting Voltage Detection.....	63
6.4.3 Setting Video Detection	64
6.4.3.1 Setting Motion Detection	64
6.4.3.2 Setting Video Tampering.....	66
6.4.3.3 Setting Scene Changing	67
6.4.4 Setting Audio Detection.....	67
6.5 Storage.....	68
6.6 System.....	69
6.6.1 General.....	69
6.6.1.1 Basic.....	69
6.6.1.2 Date & Time.....	70
6.6.2 Account.....	71
6.6.2.1 User	71
6.6.2.1.1 Adding User	71
6.6.2.1.2 Resetting Password	74
6.6.2.2 Adding User Group	75
6.6.2.3 ONVIF User	76
6.6.3 Peripheral Management	77
6.6.3.1 Configuring Serial Port	77
6.6.3.2 Configuring External Light.....	77
6.6.3.3 Configuring Wiper	78
6.6.4 Manager	79
6.6.4.1 Requirements	79
6.6.4.2 Maintenance.....	79
6.6.4.3 Import/Export.....	80
6.6.4.4 Default.....	81
6.6.5 Upgrade.....	81
6.7 System Information.....	82
6.7.1 Version	82

6.7.2 Online User.....	82
6.8 Setting Log.....	82
6.8.1 Log.....	82
6.8.2 Remote Log.....	83
7 Live.....	84
7.1 Live Interface.....	84
7.2 Setting Encode.....	85
7.3 Live View Function Bar.....	85
7.4 Window Adjustment Bar.....	87
7.4.1 Adjustment.....	87
7.4.2 Zoom and Focus.....	87
7.4.3 Image Adjustment.....	88
7.4.4 Fisheye.....	89
7.5 Display Mode.....	93
8 AI.....	97
8.1 Setting Crowd Distribution Map.....	97
8.1.1 Global Configuration.....	97
8.1.2 Rule Configuration.....	98
8.2 Setting Face Recognition.....	99
8.2.1 Setting Face Detection.....	100
8.2.2 Setting Face Database.....	103
8.2.2.1 Creating Face Database.....	103
8.2.2.2 Adding Face Picture.....	105
8.2.2.2.1 Single Adding.....	105
8.2.2.2.2 Batch Importing.....	107
8.2.2.3 Managing Face Picture.....	108
8.2.2.3.1 Editing Face Information.....	108
8.2.2.3.2 Deleting Face Picture.....	109
8.2.2.4 Face Modeling.....	110
8.2.3 Setting Arm Alarm.....	110
8.2.4 Viewing Face Recognition Result.....	113
8.3 Setting Face Detection.....	114
8.4 Setting IVS.....	116
8.4.1 Global Configuration.....	117
8.4.2 Rule Configuration.....	118
8.5 Setting Vehicle Density.....	122
8.6 Setting Parking Space.....	124

8.6.1 Rule Configuration.....	124
8.6.2 Global Configuration	128
8.7 Setting Video Metadata	128
8.7.1 Global Configuration	128
8.7.2 Rule Configuration.....	129
8.7.3 Viewing Video Metadata Report.....	131
8.8 Setting People Counting.....	132
8.8.1 People Counting.....	132
8.8.2 Queuing.....	135
8.8.3 Global Configuration	137
8.9 Face & Body Detection	138
8.9.1 Global Configuration	138
8.9.2 Rule Configuration.....	139
8.10 Setting Heat Map	141
8.11 Setting ANPR.....	141
8.11.1 Lane Configuration	142
8.11.2 Rule Configuration	143
8.11.3 Picture.....	144
8.11.4 Allowlist.....	145
8.11.5 Blocklist.....	148
9 Security.....	149
9.1 Security Status	149
9.2 System Service	150
9.2.1 802.1x.....	150
9.2.2 HTTPS.....	151
9.3 Attack Defense.....	152
9.3.1 Firewall.....	152
9.3.2 Account Lockout	153
9.3.3 Anti-DoS Attack	153
9.4 CA Certificate.....	154
9.4.1 Installing Device Certificate	154
9.4.1.1 Creating Certificate.....	154
9.4.1.2 Applying for and Importing CA Certificate.....	155
9.4.1.3 Installing Existing Certificate.....	156
9.4.2 Installing Trusted CA Certificate	157
9.5 A/V Encryption	158
9.6 Security Warning	159

10 Record	160
10.1 Playback	160
10.1.1 Playing Back Video	160
10.1.2 Clipping Video	162
10.1.3 Downloading Video	163
10.2 Setting Record Control	164
10.3 Setting Record Plan	165
10.4 Storage	166
10.4.1 Local Storage	167
10.4.2 Network Storage	168
10.4.2.1 FTP	168
10.4.2.2 NAS	169
11 Picture	171
11.1 Playback	171
11.1.1 Playing Back Picture	171
11.1.2 Downloading Picture	172
11.2 Setting Snapshot Parameters	173
11.3 Setting Snapshot Plan	174
11.4 Storage	174
11.5 Setting Upload Method	174
12 Report	176
12.1 Viewing Report	176
12.1.1 Face Recognition	176
12.1.2 Video Metadata	177
12.1.3 People Counting	178
12.1.4 Crowd Distribution	181
12.1.5 Vehicle Density	182
12.1.6 Heat Map	182
12.1.7 ANPR	184
12.2 Searching for Face Picture	185
12.3 Auto Upload	186
Appendix 1 Cybersecurity Recommendations	191

1 Overview

1.1 Introduction

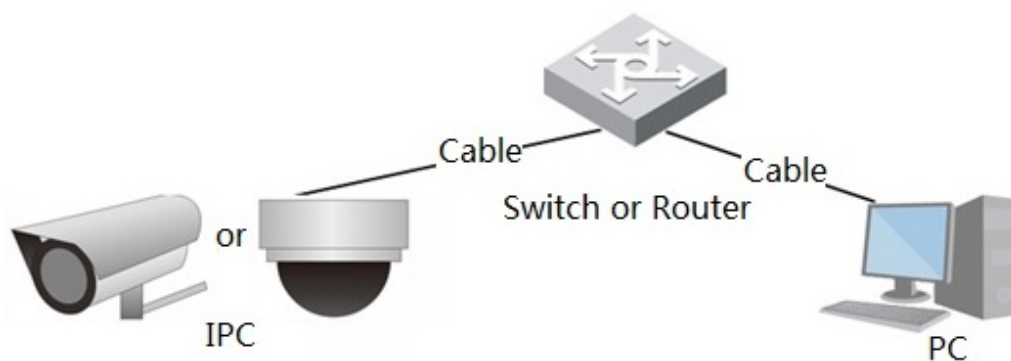
IP camera (Internet Protocol camera), is a type of digital video camera that receives control data and sends image data through internet. They are commonly used for surveillance, requiring no local recording device, but only a local area network.

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.

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

- Detects 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

- Displays the recognition result on the live view interface.
- In general mode, makes comparison between the detected face with the faces in face database after detecting face,. You can set the alarm mode and reporting mode for each face database separately, and set linkages for each reporting mode.
- In counting mode, does precise face counting after detecting face.
- When an alarm is triggered, the system performs linkages such as recording, alarm output, sending email, PTZ operation, and snapshot.

Crowd Distribution Map

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

Video Metadata

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

People Counting

- Counts the people flow in/out the detection area, and generates report.
- When the number of counted number of people in the detection area or the stay duration exceeds the configured value, an alarm will be triggered.
- When an alarm is triggered, the system performs linkages such as recording, alarm output, sending email, PTZ operation, and snapshot.

Heat Map

- Counts cumulative density of moving objects, and displays the result in different colors..
- View report of heat map, which includes heat map and track map (track map is not available on economic fisheye cameras).

ANPR

- Recognizes plate number in detection area, and displays the related information on live interface.
- When an alarm is triggered, the system links alarm output and snapshot.

Face & Body Detection

- Detects faces and human body separately, and then correlates the face and the body.
- When select compliant mode, the camera can detect attributes including face masks, helmets, glasses, safety vests, top color, and bottom color, and determine whether PPE requirements are met. PPE compliance or non-compliance alarms can be triggered according to the alarm settings.
- When an alarm is triggered, the system links alarm output and snapshot.

Parking Space

- Supports planned parking space and open parking space.
- When an alarm is triggered, the system performs linkages such as recording, alarm output, sending email, and snapshot.

Vehicle Density

- Includes road congestion and parking limit, and supports to view vehicle statistics through the live interface.
- When the counted vehicle exceeds the configured vehicle number and the congestion time exceeds the configured time, an alarm will be triggered.
- When an alarm is triggered, the system performs linkages such as recording, alarm output and sending email.

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.

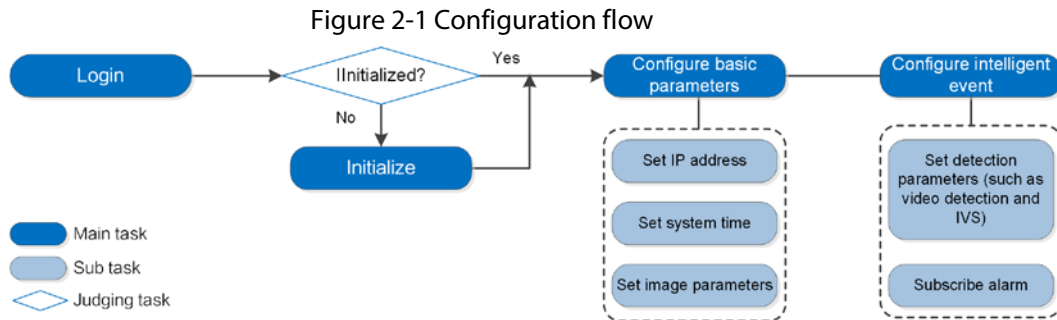


Table 2-1 Description of flow

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.



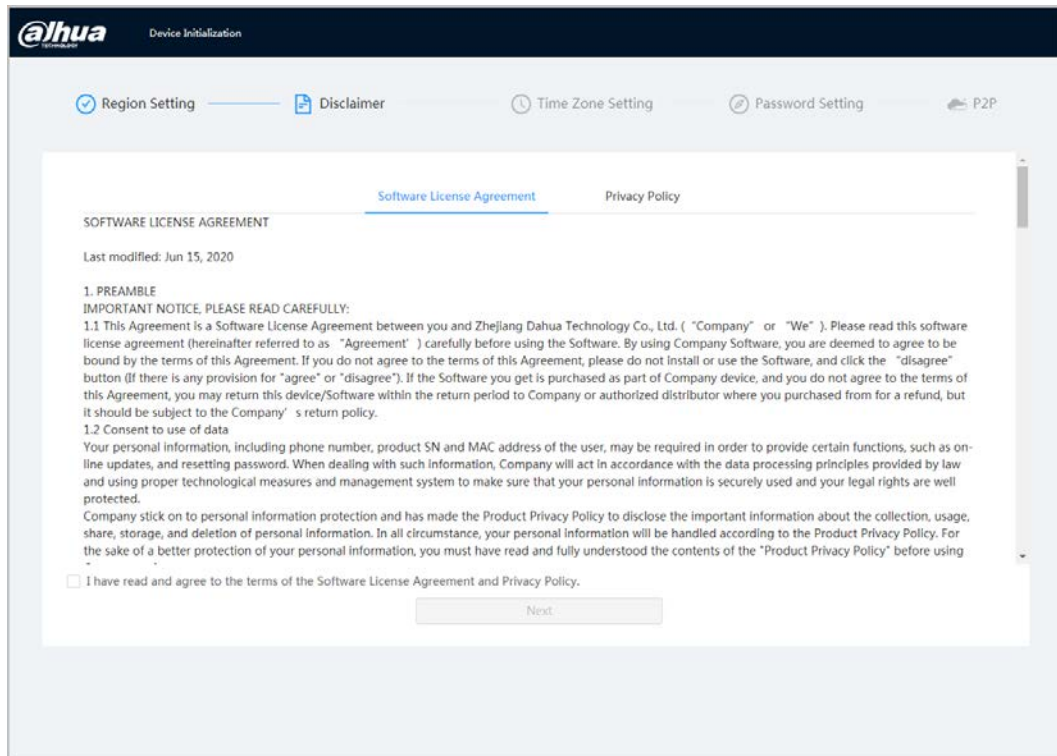
The IP is 192.168.1.108 by default.

Figure 3-1 Region Setting

The screenshot shows the 'aHua Device Initialization' web interface. At the top, there is a dark blue header with the 'aHua' logo and 'Device Initialization' text. Below the header is a light blue navigation bar with five items: 'Region Setting' (active), 'Disclaimer', 'Time Zone Setting', 'Password Setting', and 'P2P'. The main content area is white and contains three dropdown menus: 'Area', 'Language' (set to 'English'), and 'Video Standard' (set to 'PAL'). At the bottom center of the main content area is a 'Next' button.

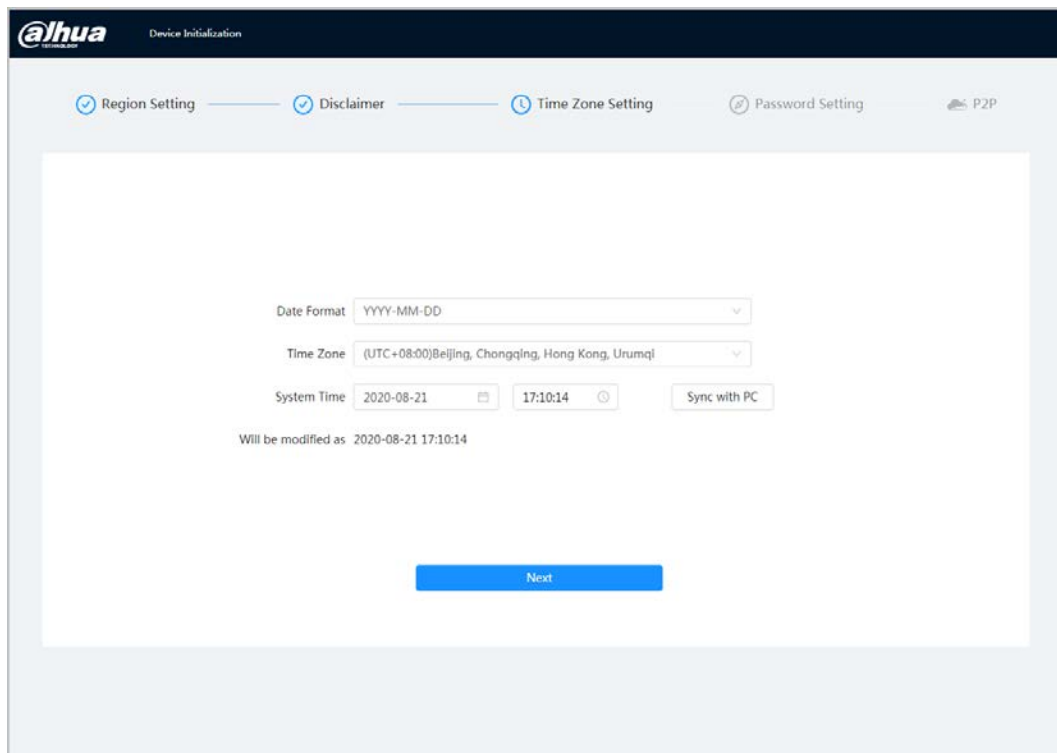
Step 2 Select the area, language, and video standard according to the actual situation, and then click **Next**.

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

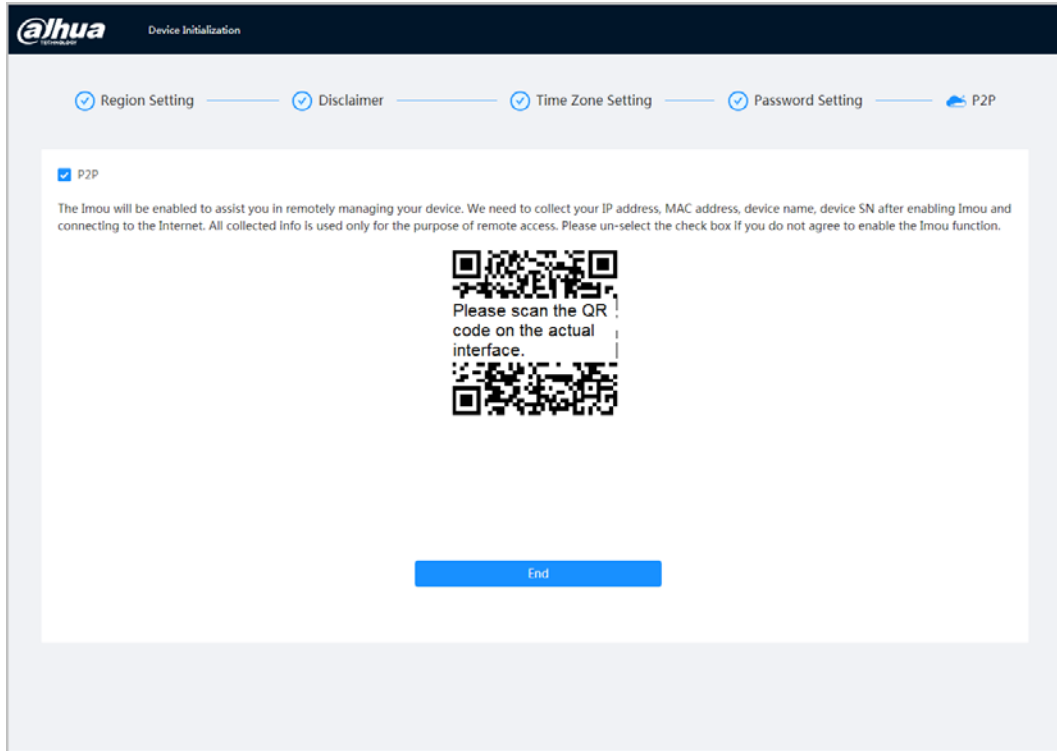
Step 5 Set the password for admin account.

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.

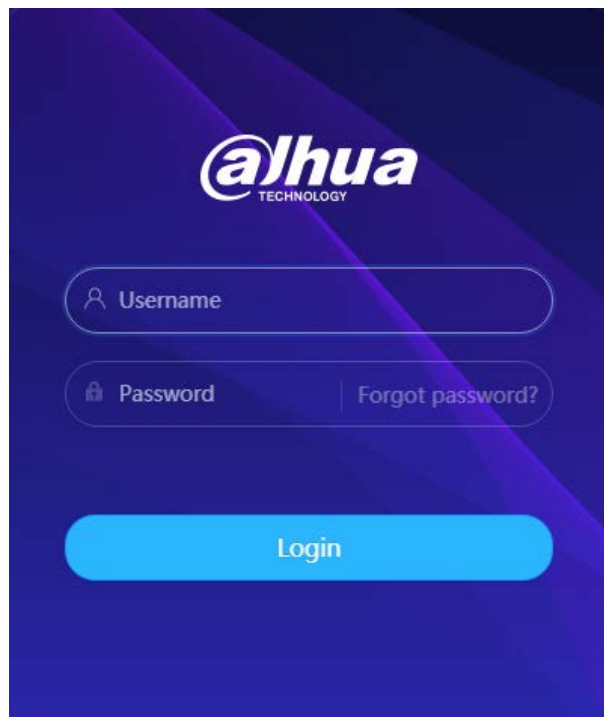
Step 1 Open IE browser, enter the IP address of the camera (192.168.1.108 by default) in the address bar and press Enter.

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



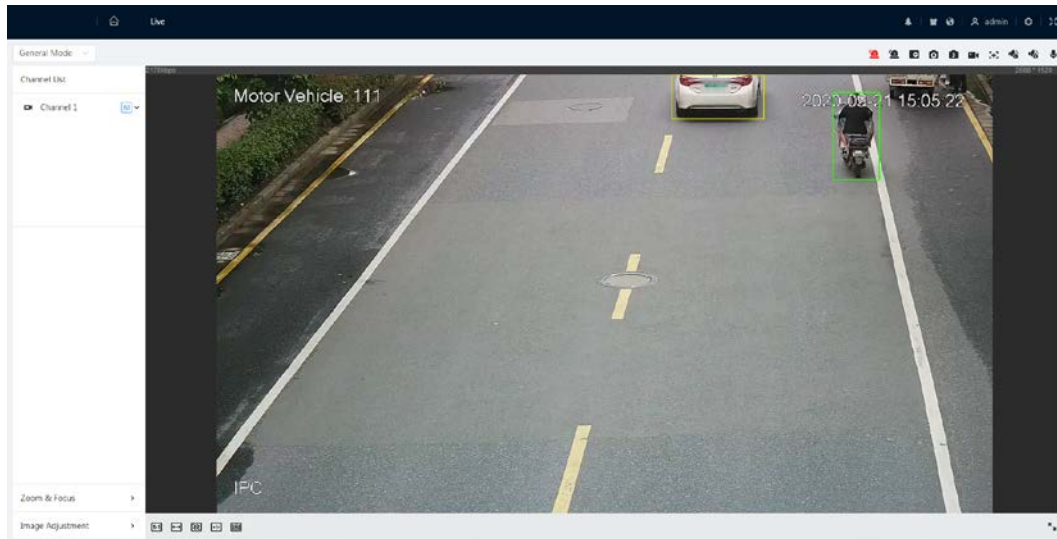
Click **Forget password?**, and you can reset the password through the email address that is set during the initialization. For details, see "4.2 Resetting Password".

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.

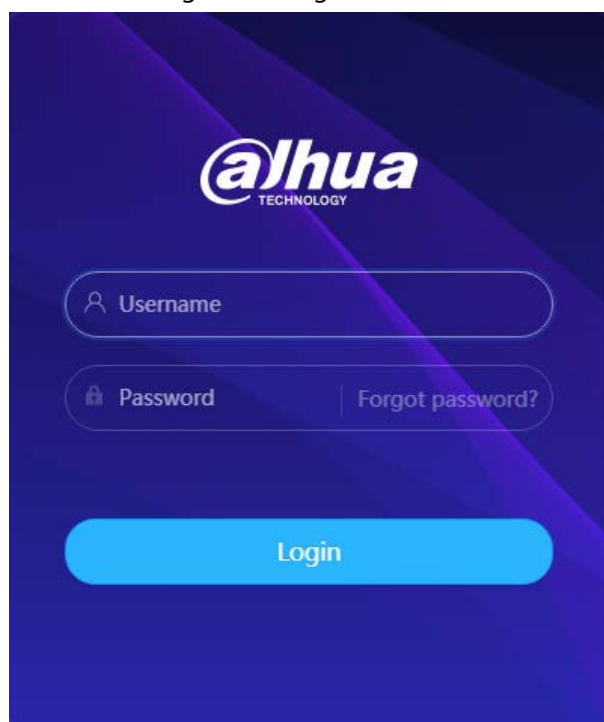
Prerequisites

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

Procedure

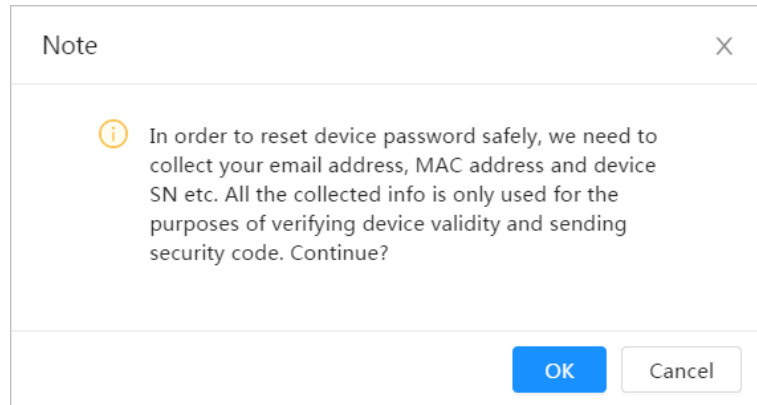
Step 1 Open IE browser, enter the IP address of the device in the address bar and press Enter.

Figure 4-3 Login



Step 2 Click **Forgot password?**, and you can reset the password through the email address that is set during the initialization.

Figure 4-4 Login



5 Main Interface


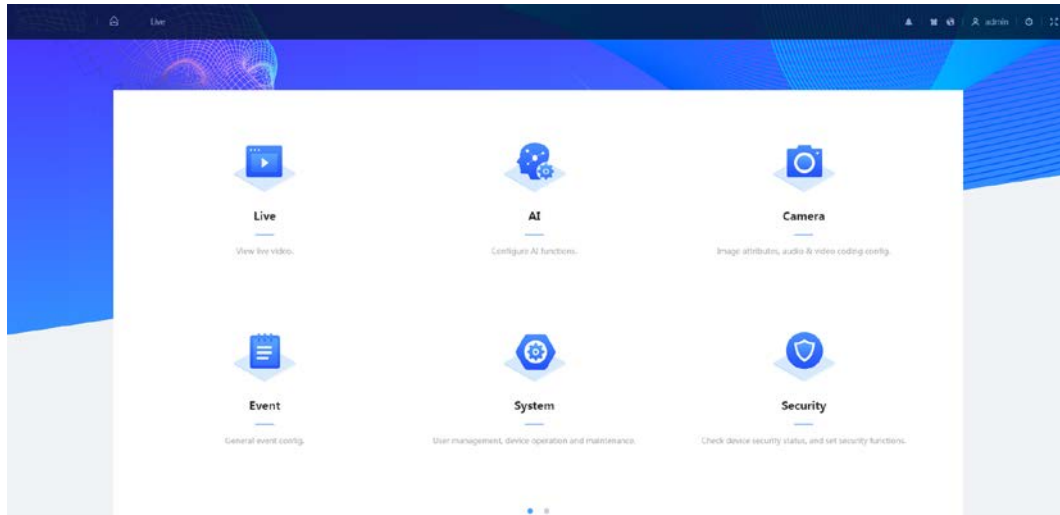





Click  at the left-upper corner of the interface to display the main interface.

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.

For **Camera**, **Event** and **System**, you can go to the configuration interface through two methods.

This section takes method 1 as an example.

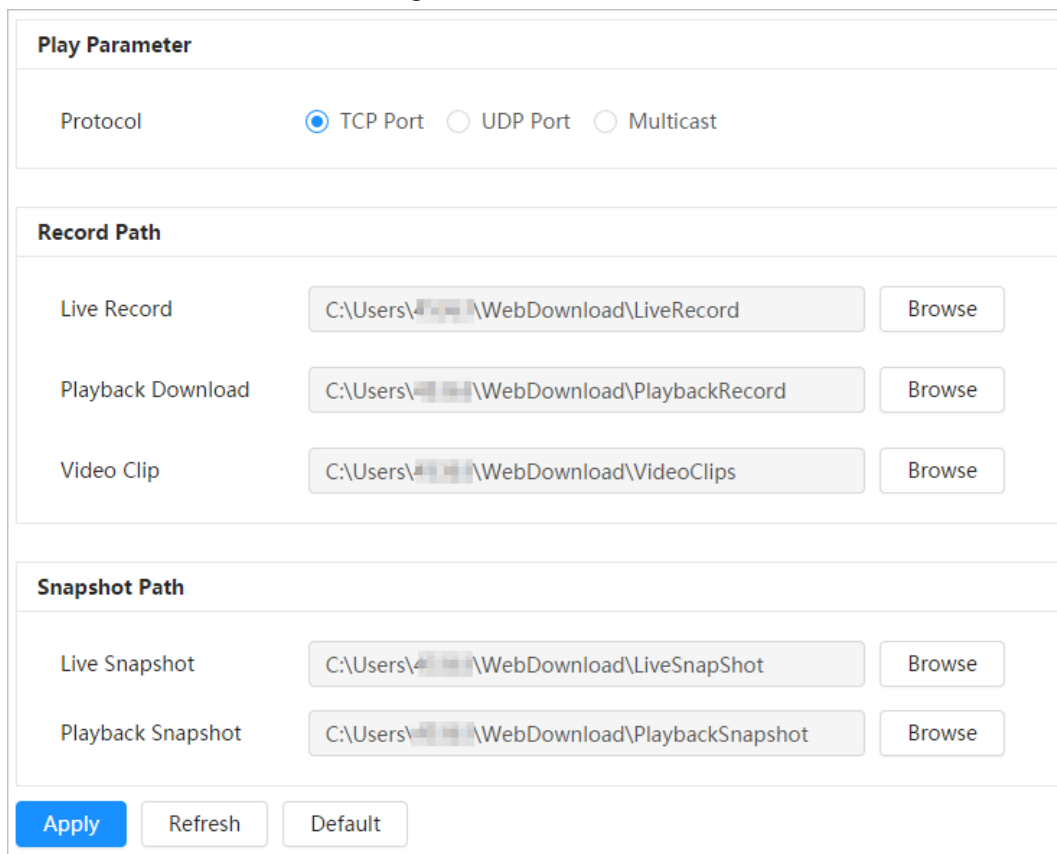
- Method 1: Click , and then select the corresponding item.
- Method 2: Click the corresponding icon on the main interface.

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




The screenshot shows the 'Local' configuration interface with the following sections:

- Play Parameter:** Protocol is set to TCP Port (selected), with options for UDP Port and Multicast.
- Record Path:**
 - Live Record: C:\Users\... \WebDownload\LiveRecord (Browse)
 - Playback Download: C:\Users\... \WebDownload\PlaybackRecord (Browse)
 - Video Clip: C:\Users\... \WebDownload\VideoClips (Browse)
- Snapshot Path:**
 - Live Snapshot: C:\Users\... \WebDownload\LiveSnapShot (Browse)
 - Playback Snapshot: C:\Users\... \WebDownload\PlaybackSnapshot (Browse)

At the bottom, there are three buttons: Apply (highlighted in blue), Refresh, and Default.

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>
Live Record	<p>The recorded video of live interface. The default path is C:\Users\admin\WebDownload\LiveRecord.</p>
Playback Download	<p>The downloaded video of playback interface. The default path is C:\Users\admin\WebDownload\PlaybackRecord.</p>
Video Clips	<p>The clipped video of playback interface. C:\Users\admin\WebDownload\VideoClips.</p>
Live Snapshot	<p>The snapshot of live interface. The default path is C:\Users\admin\WebDownload\LiveSnapshot.</p>
Playback Snapshot	<p>The snapshot of playback interface. The default path is C:\Users\admin\WebDownload\PlaybackSnapshot.</p>



Admin in the path refers to the account being used.

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.

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

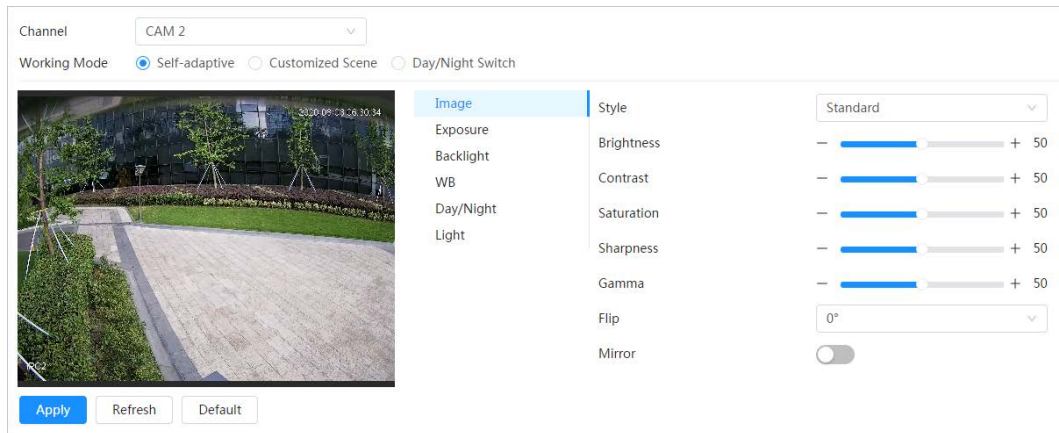
Configure camera parameters to improve the scene clarity, and ensure that surveillance goes properly.

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.

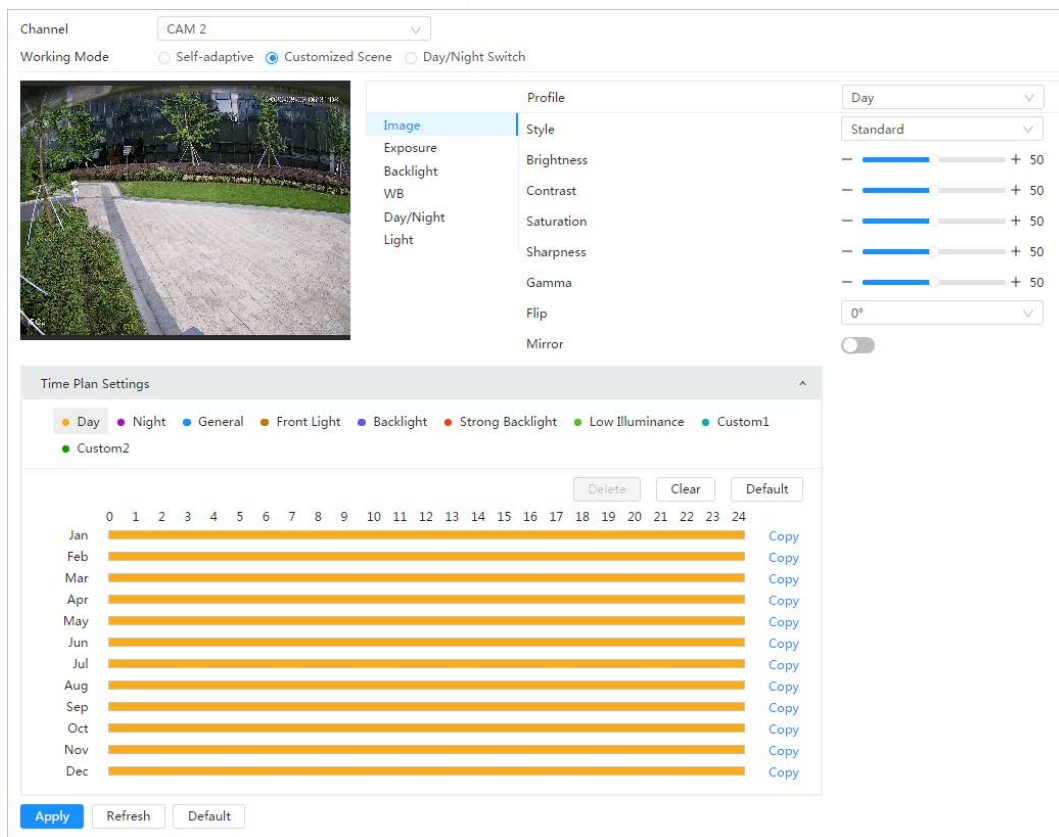
- Self-adaptive: The camera will adjust the image according to the environment.

Figure 6-2 Interface layout (self-adaptive)



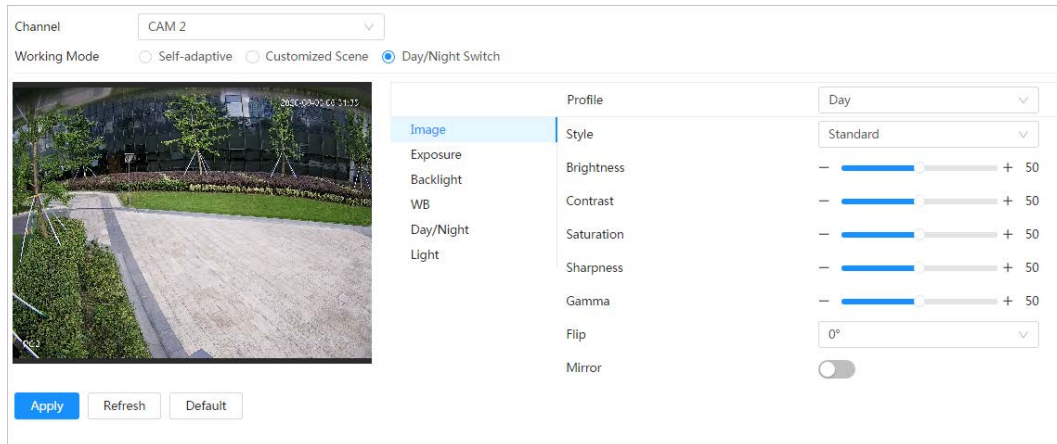
- Customized scene: You can select the profile as needed. Select the profile in **Time Plan Setting** and drag the slide block to set certain time as the selected profile. For example, set 8:00–18:00 as day, and 0:00–8:00 and 18:00–24:00 as night

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)

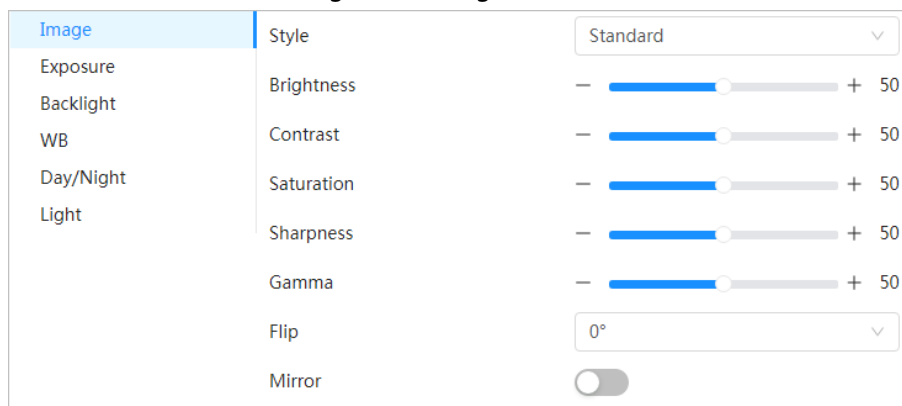


6.2.1.2 Image

You can configure picture parameters as needed.

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


Figure 6-5 Image



Step 2 Configure picture parameters.

Table 6-2 Description of picture parameters

Parameter	Description
Style	Select the picture style from soft, standard and vivid. <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	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.
Contrast	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.

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 <input type="checkbox"/> , and the picture will display with left and right side reversed.

Step 3 Click **Apply**.

6.2.1.3 Exposure

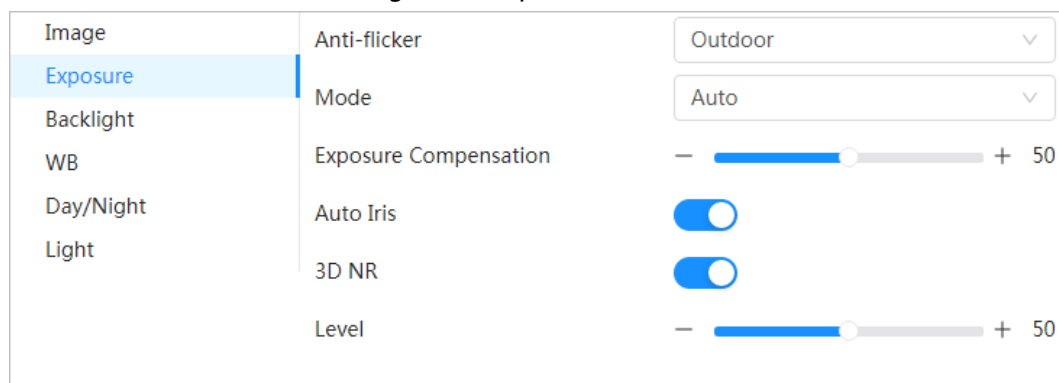
Configure iris and shutter to improve image clarity.



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


Step 1 Select  > **Camera** > **Image** > **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	<p>Sets the value, and it ranges from 0 to 50. The higher the value is, the brighter the image will be.</p>
Shutter	<p>Set the effective exposure time. The smaller the value, the shorter the exposure time will be.</p>
Gain	<p>When selecting Gain Priority or Manual in Mode, you can set Gain. With minimum illumination, the camera increases Gain automatically to get clearer images.</p>

Parameter	Description
Auto Iris	This configuration is available only when the camera is equipped with auto-iris lens. <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.
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.

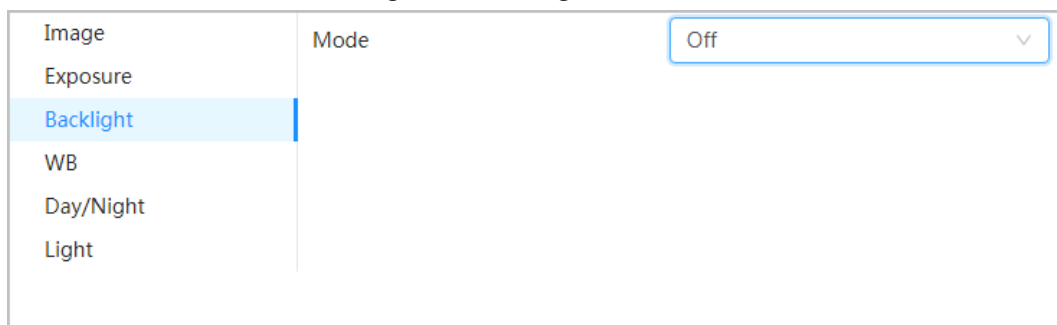
Step 3 Click **Apply**.

6.2.1.4 Backlight

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

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


Figure 6-7 Backlight



Step 2 Configure backlight parameters.

Table 6-4 Description of backlight parameters

Backlight mode	Description
BLC	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. <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.

Backlight mode	Description
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>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.


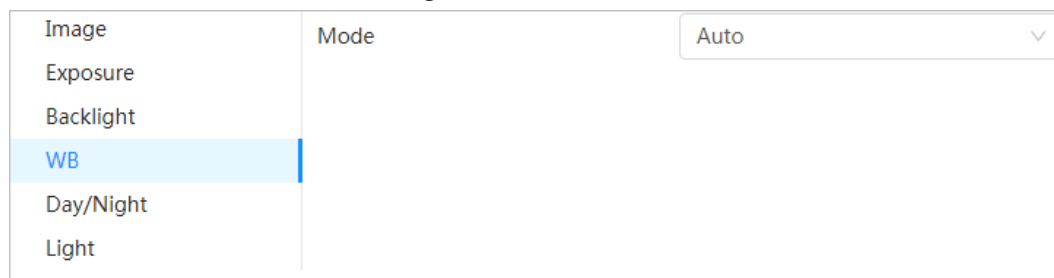
Step 1 Select  > **Camera** > **Image** > **WB**.

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.


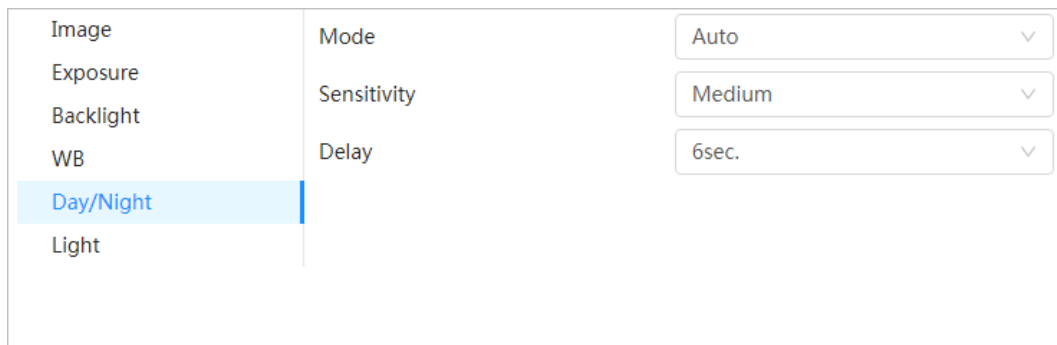

Step 1 Select  > **Camera** > **Image** > **WB**.

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.</p> <p> 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.</p> <p>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.</p> <p>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** > **Image** > **Illuminator**.

Figure 6-10 Light

Image	Fill Light	Soft Light Mode
Exposure	Mode	Auto
Backlight		
WB		
Day/Night		
Illuminator		
Defog		

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 > Image > 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**.

6.2.1.9 Fisheye

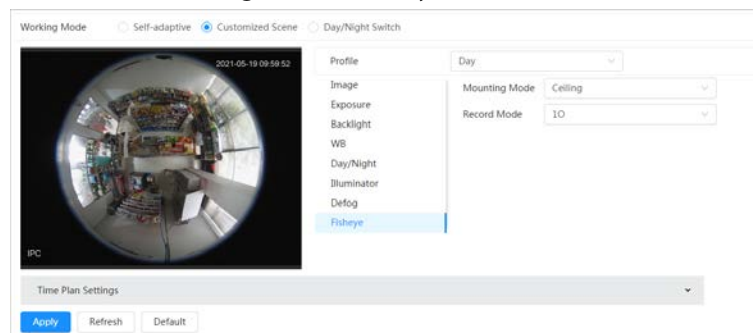
Select installation mode and record mode according to the actual installation scene. When the camera accesses the platform with corrective stream, the platform displays the corrective image.



This function is only available on fisheye device.

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

Figure 6-12 Fisheye



Step 2 Set installation mode and record mode.

Table 6-9 Description of fisheye parameters

Parameter	Description
installation Mode	You can select Ceiling , Wall , or Ground .
Record Mode	<ul style="list-style-type: none"> • 1O: The original image before correction. • 1P: 360° rectangular panoramic image. • 2P: When the installation mode is Ceiling or Ground, you can set this mode. Two associated 180° rectangular image screens; at any time, the two screens form a 360° panoramic image. • 1R: Original image screen + independent sub-screen. You can zoom or drag the image in all the screens. • 2R: Original image screen + two independent sub-screens. You can zoom or drag the image in all the screens. • 4R: Original image screen + four independent sub-screens. You can zoom or drag the image in all the screens. • 1O + 3R: Original image screen + three independent sub-screens. You can zoom or drag the image in original image screen, and move the image (upper and lower) in sub-screens to adjust the vertical view.

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 6-13 Encode

The screenshot shows the 'Encode' configuration page for 'CAM 1'. It is divided into two main sections: 'Main Stream' and 'Sub Stream'. Both sections have identical settings: Compression (H.264H), Smart Codec (disabled), Resolution (2592*1944), Frame Rate (FPS) (25), Bit Rate Type (CBR), Reference Bit Rate (3329-16093 Kbps), Bit Rate (6144 Kbps), I Frame Interval (50), and SVC (1(off)). The Sub Stream section also includes a 'Sub Stream' dropdown set to 'Sub Stream 1' and an enabled toggle switch. At the bottom, there is a 'Watermark' section with a toggle switch (enabled) and a 'Watermark String' field containing 'DigitalCCTV'. Buttons for 'Apply', 'Refresh', and 'Default' are located at the bottom left.

Step 2 Configure encode parameters.

Table 6-10 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.
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

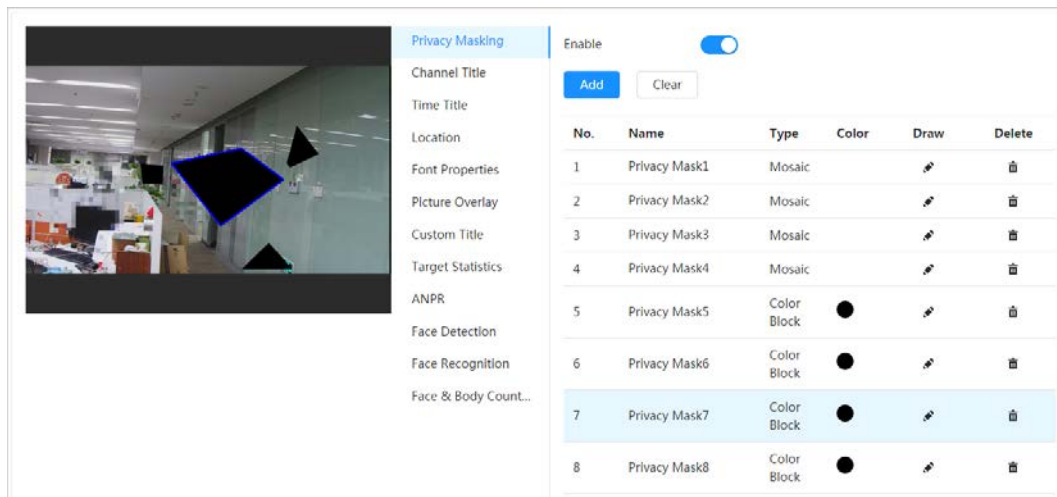
You can enable this function when you need to protect the privacy of some area on the video image.

You can select the type of the masking from **Color Block** and **Mosaic**.


- When selecting **Color Block** only, you can draw triangles and convex quadrilaterals as blocks. You can drag 8 blocks at most, and the color is black.
- When selecting **Mosaic**, you can draw rectangles as blocks with mosaic. You can draw 4 blocks at most.
- **Color Block + Mosaic**: You can draw 8 blocks at most.

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


Figure 6-14 Privacy masking



Step 2 Configure privacy masking.

- 1) Click  next to **Enable**.
- 2) Click **Add**, and then drag the block to the area that you need to cover.
- 3) Adjust the size of the rectangle to protect the privacy.
- 4) Click **Apply**.

Related Operations

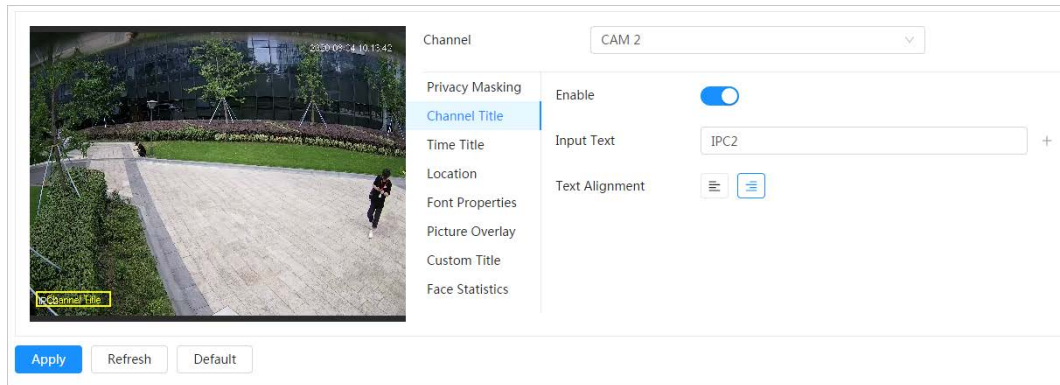
- View and edit the block
Select the privacy masking rule to be edited in the list, then the rule is highlighted, and the block frame is displayed in the image. You can edit the selected block as needed, including moving the position, and adjusting the size.
- Edit the block name
Double-click the name in **Name** to edit the block name.
- Delete the block
 - ◇ Click  to delete blocks one by one.
 - ◇ Click **Clear** to delete all blocks.

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 6-15 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.

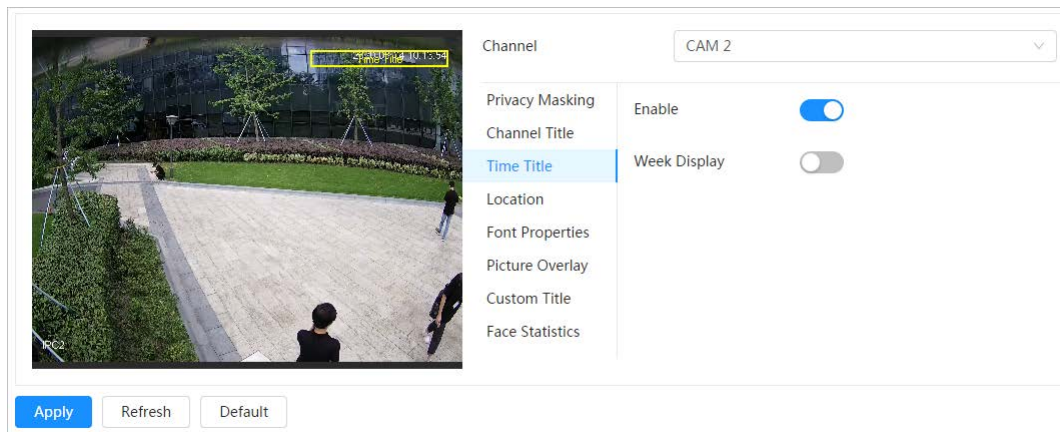
Step 4 Click **Apply**.

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 6-16 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.


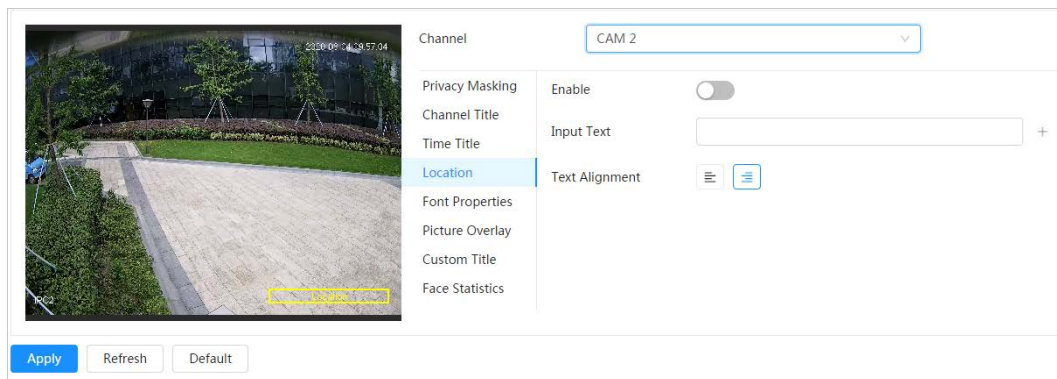
Step 1 Select  > **Camera > Encode > Overlay > Location.**

Figure 6-17 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.

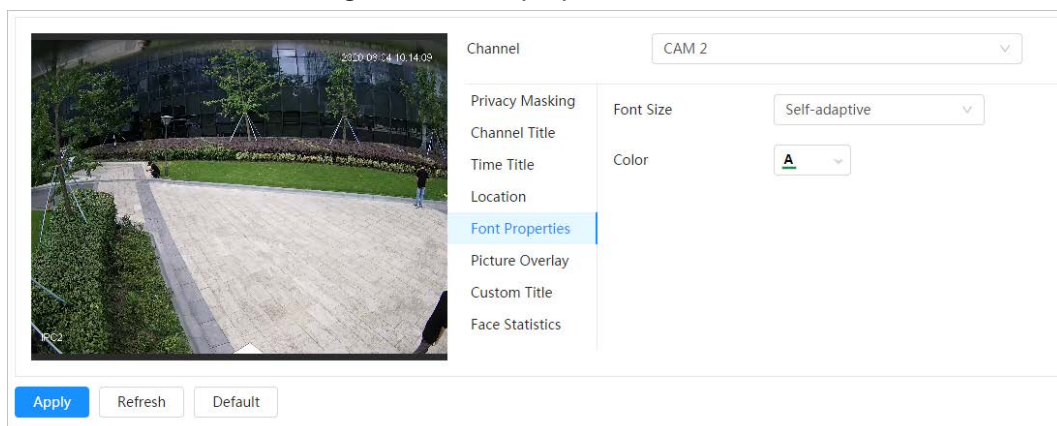
Step 4 Click **Apply**.

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 6-18 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

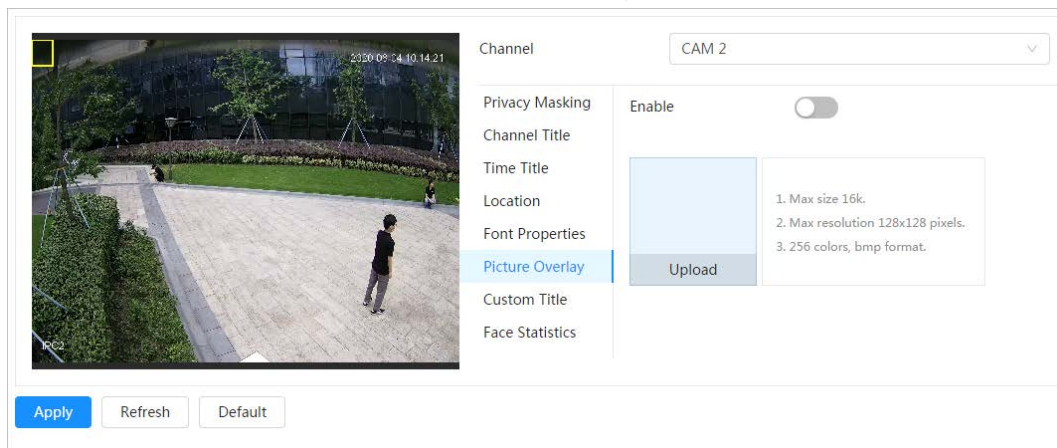
You can enable this function if you need to display picture information on the video image.



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

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

Figure 6-19 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.

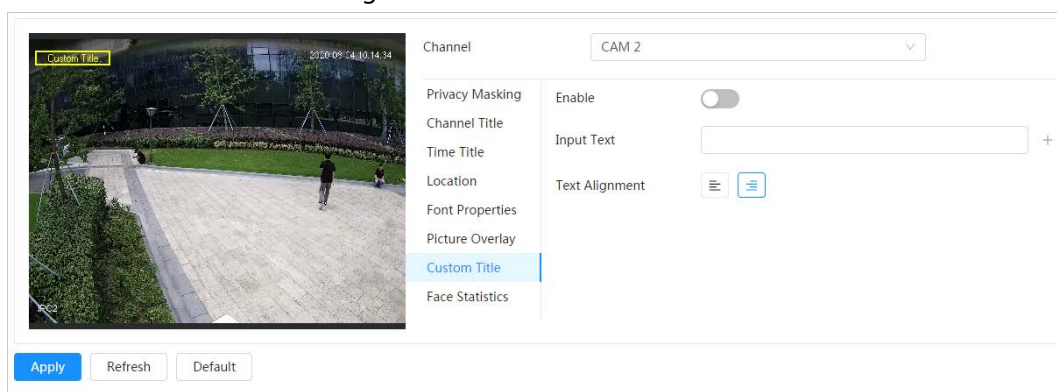
Step 4 Click **Apply**.

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 6-20 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.

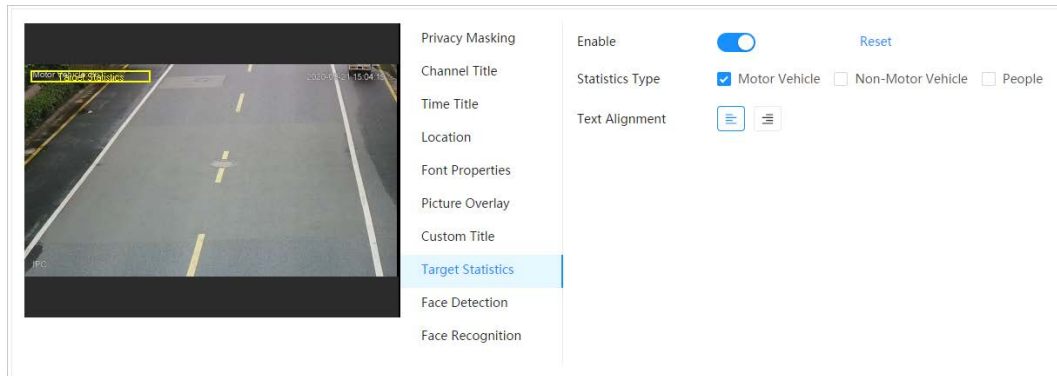
Step 4 Click **Apply**.

6.2.2.2.8 Configuring Target Statistics

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

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

Figure 6-21 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**.

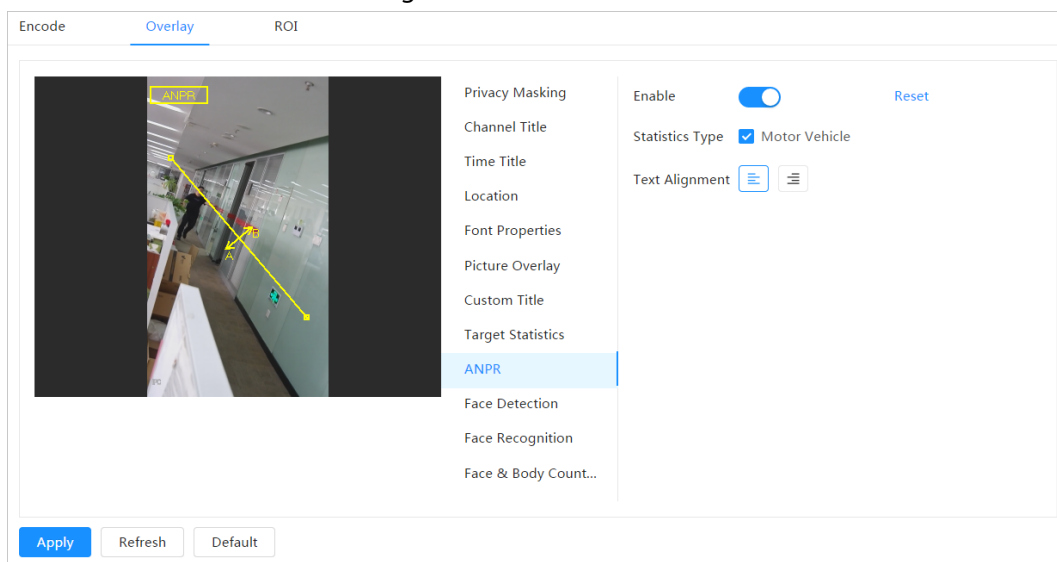
The overlaid information will be displayed after enabling video metadata function.

6.2.2.2.9 Configuring ANPR

After enabling this function, ANPR statistics information will be displayed on the image. When the overlay function is enabled during intelligent rules configuration, this function is enabled simultaneously.

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

Figure 6-22 ANPR



Step 2 Select the **Enable** check box, select the statistics type, and then select text alignment.



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

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

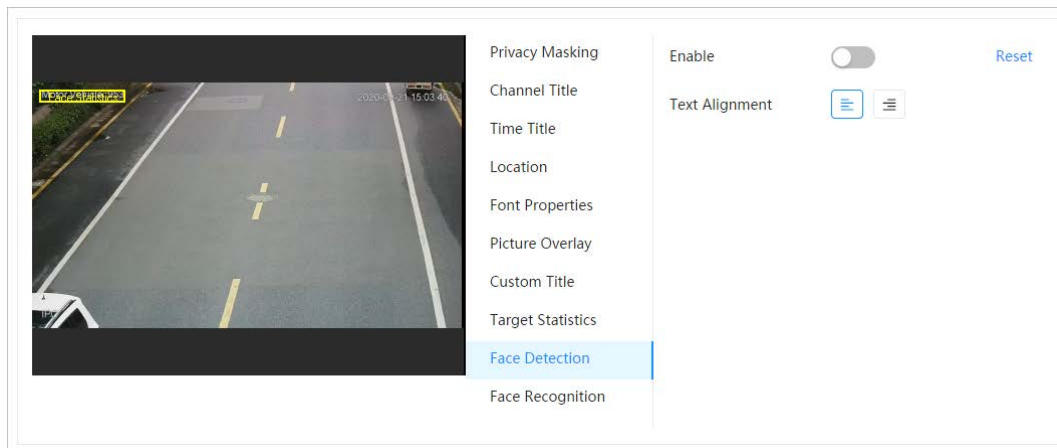
Step 4 Click **Apply**.

6.2.2.2.10 Configuring Face Detection

After enabling this function, face statistics information will be displayed on the image. When the overlay function is enabled during intelligent rules configuration, this function is enabled simultaneously.

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

Figure 6-23 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**.

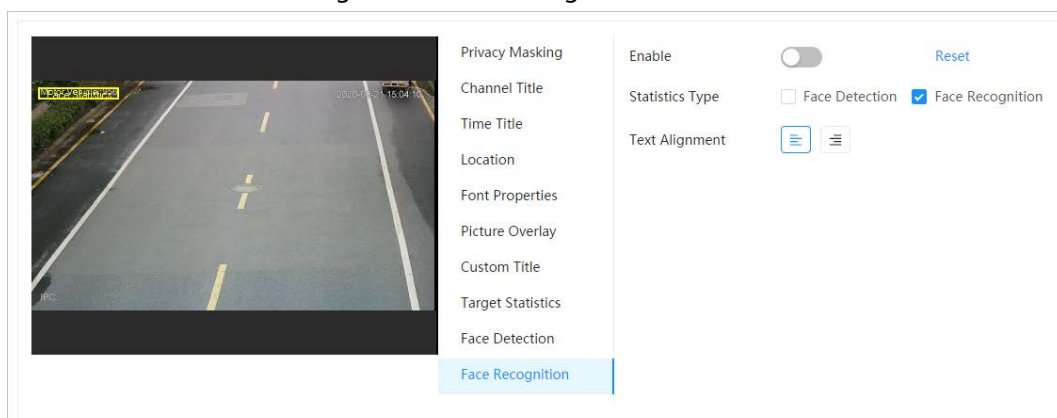
The information will be displayed on the image after the face detection function is enabled.

6.2.2.2.11 Configuring Face Recognition

After enabling this function, face statistics information will be displayed on the image. When the overlay function is enabled during intelligent rules configuration, this function is enabled simultaneously.

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

Figure 6-24 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**.

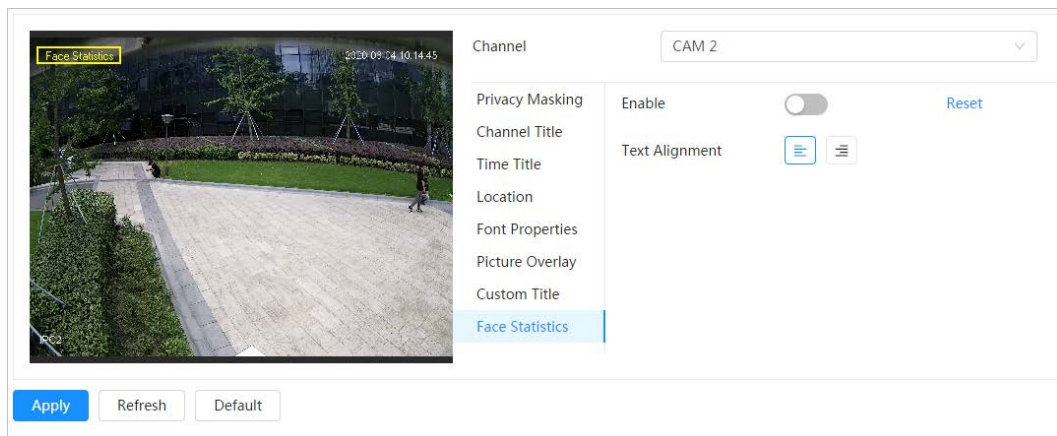
The information will be displayed on the image after the face recognition function is enabled.

6.2.2.2.12 Configuring Face Statistics

After enabling this function, face statistics information will be displayed on the image. When the overlay function is enabled during intelligent rules configuration, this function is enabled simultaneously.

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

Figure 6-25 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.

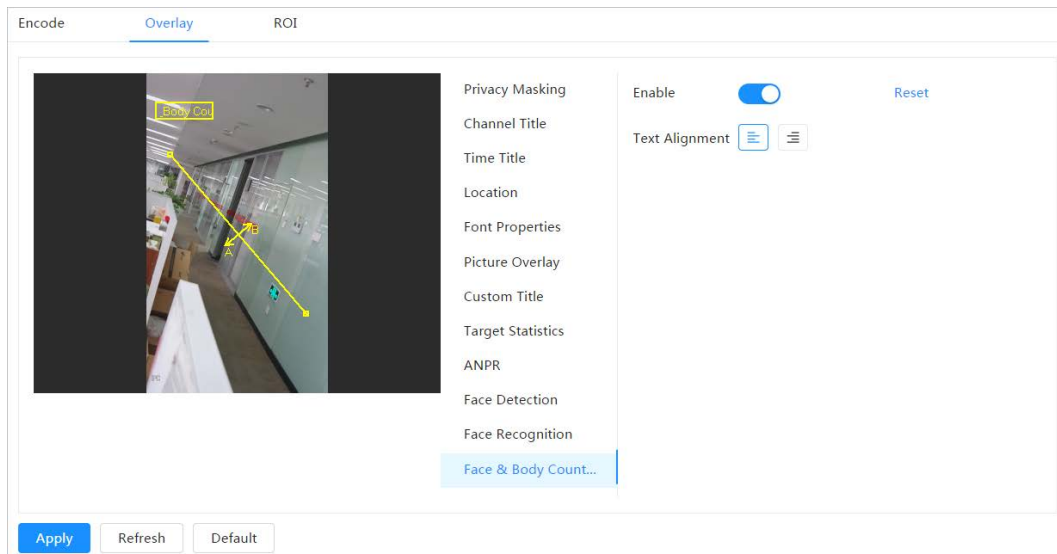
Step 4 Click **Apply**.

6.2.2.2.13 Configure Face&Body Counting

After enabling this function, face&body counting information will be displayed on the image. When the overlay function is enabled during intelligent rules configuration, this function is enabled simultaneously.

Step 1 Select  > **Camera** > **Encode** > **Overlay** > **Face&Body Counting**.

Figure 6-26 Face&body counting



Step 2 Select the **Enable** check box, and then select text alignment.



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

Step 3 Move the face&body counting box to the position that you want in the image.

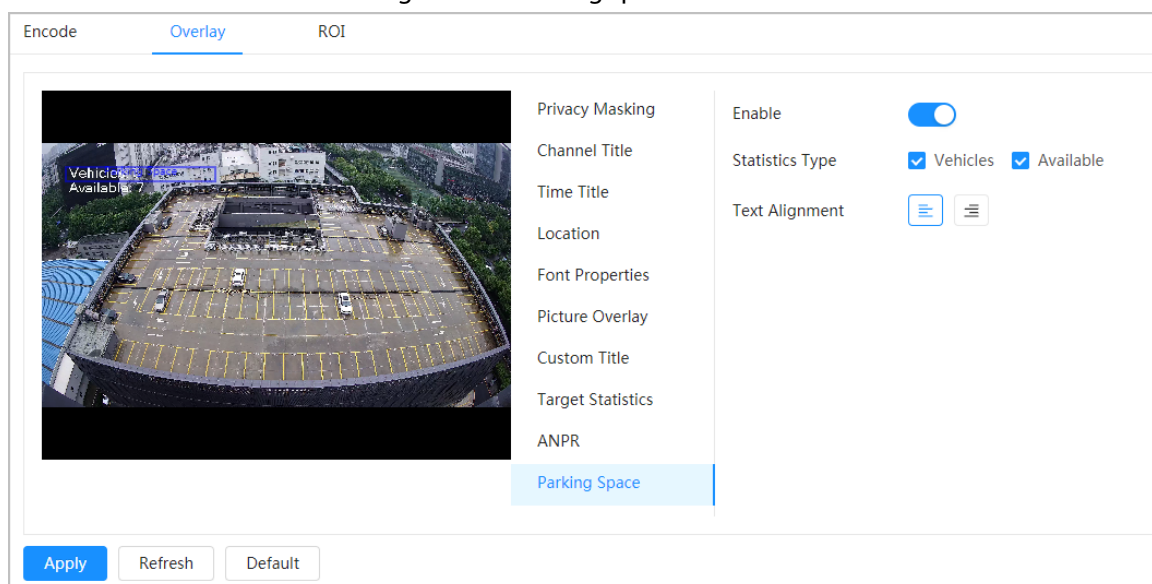
Step 4 Click **Apply**.

6.2.2.2.14 Configuring Parking Space

After enabling this function, parking space information will be displayed on the image. When the overlay function is enabled during intelligent rules configuration, this function is enabled simultaneously.

Step 1 Select  > **Camera** > **Encode** > **Overlay** > **Parking Space**.

Figure 6-27 Parking space



Step 2 Select the **Enable** check box.

Step 3 Select statistic type and text alignment.

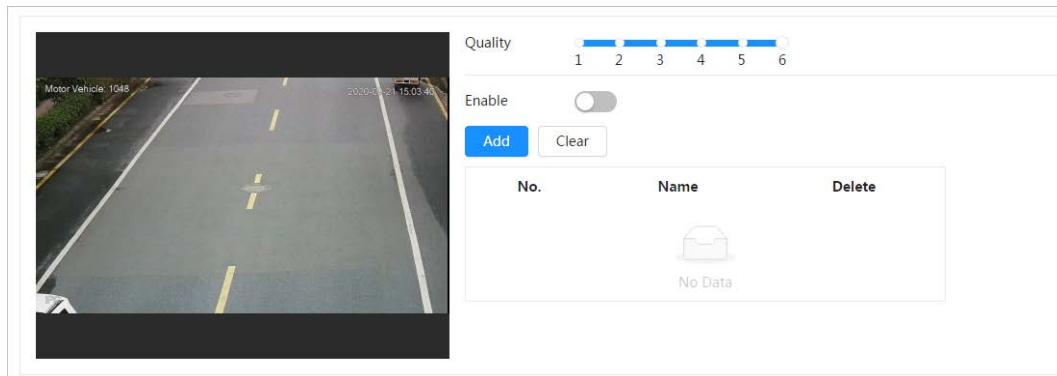
Step 4 Click **Apply**.

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 6-28 ROI



Step 2 Click next to **Enable**, draw an area on the image, and then configure the image quality of ROI.



- 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**.

Step 4 (optional) Click **Add** to add more ROI. You can draw 4 area boxes at most.

6.2.3 Audio

You can configure audio parameters and alarm audio.

6.2.3.1 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 6-29 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 6-11 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**.

6.2.3.2 Setting Alarm Tone

You can record or upload alarm audio file. The audio file will be played when the alarm is triggered.

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

Figure 6-30 Audio tone

Main Stream	Sub Stream
Enable <input checked="" type="checkbox"/>	Enable <input type="checkbox"/>
Compression <input type="text" value="G.711A"/>	Sub Stream <input type="text" value="Sub Stream 1"/>
Sampling Frequency <input type="text" value="8000"/>	Compression <input type="text" value="G.711A"/>
	Sampling Frequency <input type="text" value="8000"/>
Audio Input Type <input type="text" value="LineIn"/>	
Noise Filter <input type="checkbox"/>	
Microphone Volume <input type="range" value="50"/>	
Speaker Volume <input type="range" value="50"/>	
<input type="button" value="Apply"/> <input type="button" value="Refresh"/> <input type="button" value="Default"/>	

Step 2 Click **Add**.

Step 3 Configure the audio file.

- Select **Record**, enter the audio name in the input box, and then click **Record**.
- Select **Upload**, click **Browse** to select the audio file to be uploaded, and then click **Upload**.



- The camera supports recording audio file in .pcm format only. Recording is only supported by select models.
- You can upload audio files in .pcm, .wav2, .mp3, or .aac format.

Figure 6-31 Add alarm tone

Add
×

Record
 Upload

File .pcm

Step 4 Select the file that you need.

Related Operations

- Edit audio file
Click to edit the file name.
- Delete audio file
Click to delete the file name.
- Play audio file
Click to play the file name.
- Download audio file
Click to download the file name.

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 6-32 TCP/IP

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

Step 2 Configure TCP/IP parameters.

Table 6-12 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="659 824 1337 1391" style="border: 1px solid black; padding: 5px;"> <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 http://(IP address) in the browser address bar to log in.
NIC	<p>Select the Ethernet card that need to be configured, and the default one is Wire.</p>
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 6-33 Port

Max Connection	<input type="text" value="10"/>	(1-20)
TCP Port	<input type="text" value="3777"/>	(1025-65534)
UDP Port	<input type="text" value="3778"/>	(1025-65534)
HTTP Port	<input type="text" value="80"/>	
RTSP Port	<input type="text" value="554"/>	
RTMP Port	<input type="text" value="1935"/>	(1025-65534)
HTTPS Port	<input type="text" value="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 6-13 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: <code>rtsp://username:password@ip:port/cam/realmonitor?channel=1&subtype=0</code></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: <code>rtsp://admin:admin@10.12.4.84:554/cam/realmonitor?channel=2&subtype=1</code></p> <p>If username and password are not needed, then the URL can be: <code>rtsp://ip:port/cam/realmonitor?channel=1&subtype=0</code></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.

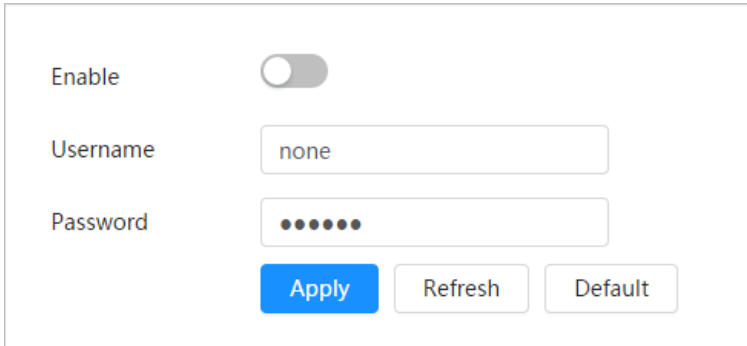
Prerequisites


- 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 6-34 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 access 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 6-35 DDNS

Step 2 Click to enable the function.

Step 3 Configure DDNS parameters.

Table 6-14 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 • Dyn dns DDNS web address: members.dyndns.org
Server Address	
Domain Name	The domain name you registered on the DDNS website.
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, then enter the domain name at the address bar and 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 6-36 Email

Step 2 Click to enable the function.

Step 3 Configure email parameters.

Table 6-15 Description of email parameters

Parameter	Description
SMTP Server	SMTP server address
Port	The port number of the SMTP server.
Username	The account of SMTP server.
Password	The password of SMTP server.
Anonymous	Click <input type="checkbox"/> , 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 6-16.
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.
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.

Parameter	Description
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 6-16.

Table 6-16 Description of major mailbox configuration

Mailbox	SMTP server	Authentication	Port	Description
gmail	smtp.gmail.com	SSL	465	You need to enable SMTP service in your mailbox.
		TLS	587	

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 access 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 6-37 UPnP

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

Buttons: **Apply**, Refresh, Default

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.

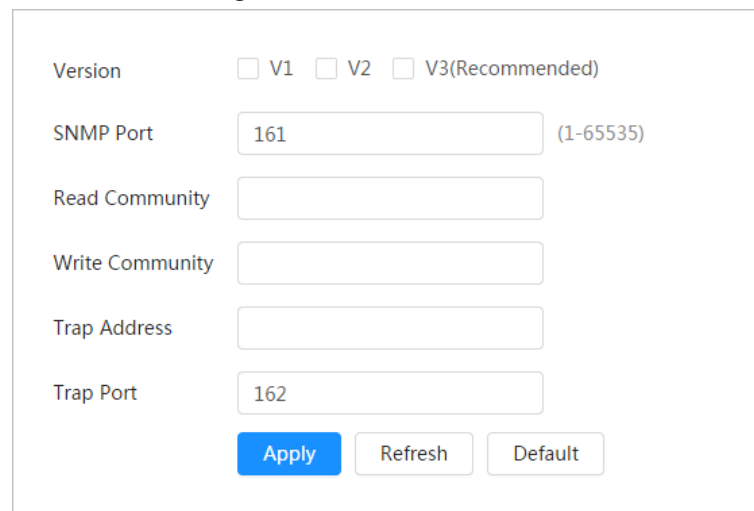
Prerequisites

- 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 6-38 SNMP (1)



The screenshot shows the SNMP configuration page with the following fields and options:

- Version:** Radio buttons for V1, V2, and V3(Recommended).
- SNMP Port:** Text input field containing '161' with a range indicator '(1-65535)' to its right.
- Read Community:** Empty text input field.
- Write Community:** Empty text input field.
- Trap Address:** Empty text input field.
- Trap Port:** Text input field containing '162'.
- Buttons:** 'Apply' (blue), 'Refresh', and 'Default' (grey).

Figure 6-39 SNMP (2)

Version	<input type="checkbox"/> V1 <input type="checkbox"/> V2 <input checked="" type="checkbox"/> V3(Recommended)
SNMP Port	<input type="text" value="161"/> (1-65535)
Read Community	<input type="text"/>
Write Community	<input type="text"/>
Trap Address	<input type="text"/>
Trap Port	<input type="text" value="162"/>
Read-Only Userna...	<input type="text" value="public"/>
Authentication Type	<input checked="" type="radio"/> MD5 <input type="radio"/> SHA
Authentication Pa...	<input type="text" value="....."/>
Encryption Type	<input checked="" type="radio"/> CFB-AES
Encryption Passwo...	<input type="text" value="....."/>
Read/Write Usern...	<input type="text" value="private"/>
Authentication Type	<input checked="" type="radio"/> MD5 <input type="radio"/> SHA
Authentication Pa...	<input type="text" value="....."/>
Encryption Type	<input checked="" type="radio"/> CFB-AES
Encryption Passwo...	<input type="text" value="....."/>
<input type="button" value="Apply"/> <input type="button" value="Refresh"/> <input type="button" value="Default"/>	

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 6-17 Description of SNMP parameters

Parameter	Description
SNMP Port	The listening port of the software agent in the device.

Parameter	Description
Read Community, Write Community	<p>The read and write community string that the software agent supports.</p>  <p>You can enter number, letter, underline and dash to form the name.</p>
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	<p>Set the read-only username accessing device, and it is public by default.</p>  <p>You can enter number, letter, and underline to form the name.</p>
Read/Write Username	<p>Set the read/write username access device, and it is private by default.</p>  <p>You can enter number, letter, and underline to form the name.</p>
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.

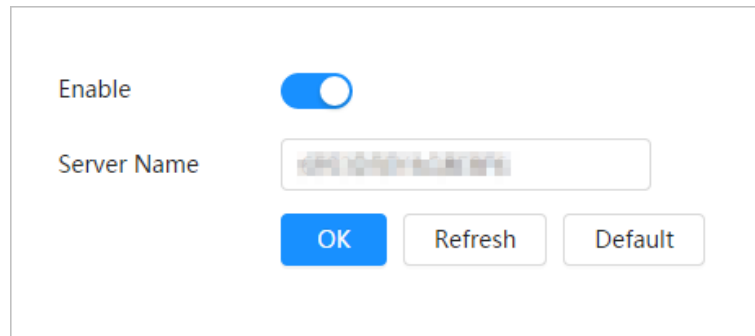



Bonjour is enabled by default.

Procedure

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

Figure 6-40 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.


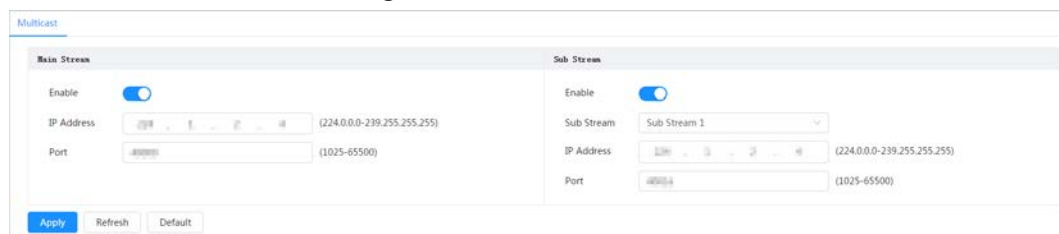
Step 1 Select  > **Network** > **Multicast**.

Figure 6-41 Multicast



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

Table 6-18 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.

Parameter	Description
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

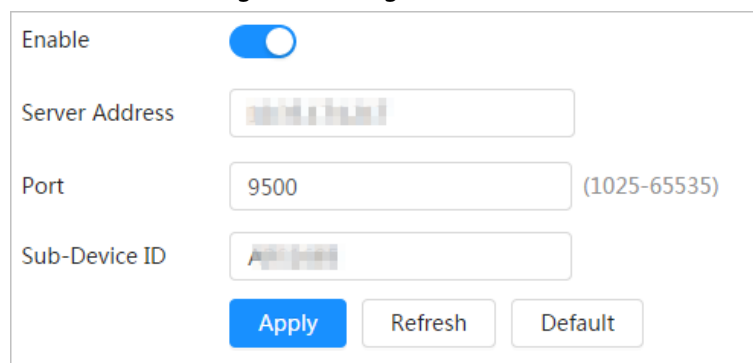
On the **Live** interface, select **RTSP** in **Multicast**, and then you can view the video image with multicast protocol.

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 6-42 Register




Step 2 Click , and then configure server name.

Table 6-19 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 6-43 QoS

Step 2 Configure QoS parameters.

Table 6-20 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 6-44 P2P

- 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

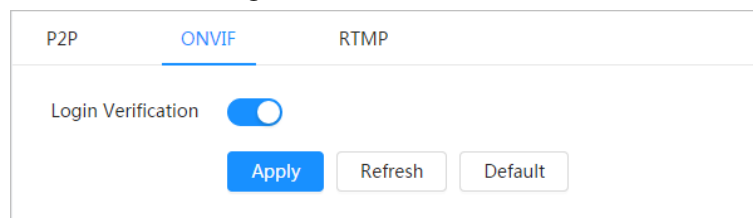
The ONVIF verification is enabled by default, which allows the network video products (including video recording device and other recording devices) from other manufacturers to connect to your device.



ONVIF is enabled by default.

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

Figure 6-45 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 6-46 RTMP

Step 2 Click .



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

Step 3 Configure RTMP parameters.

Table 6-21 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.

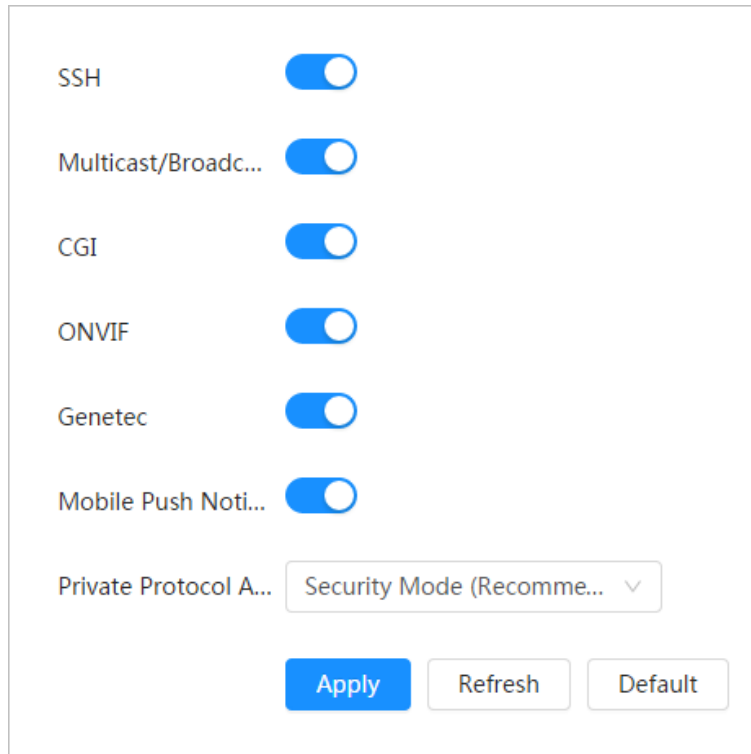
Step 4 Click **Apply**.

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 6-47 Basic service



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

Table 6-22 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 6-48 Alarm linkage

The screenshot shows the 'Alarm Linkage' configuration page. It features a list of settings on the left and their corresponding input fields or controls on the right. The 'Enable' toggle is turned on. The 'Alarm-in Port' is set to 'Alarm1'. The 'Schedule' is set to 'Full Time', with an 'Add Schedule' button next to it. '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 two buttons labeled '1' and '2'. 'Post-Alarm' is set to '10' with a range of 'sec.(10-300)'. 'Record' is turned on, and there are four buttons labeled '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, and there are four buttons labeled '1', '2', '3', and '4'. At the bottom, there are three buttons: 'Apply' (highlighted in blue), 'Refresh', and 'Default'.

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. If the exiting 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".

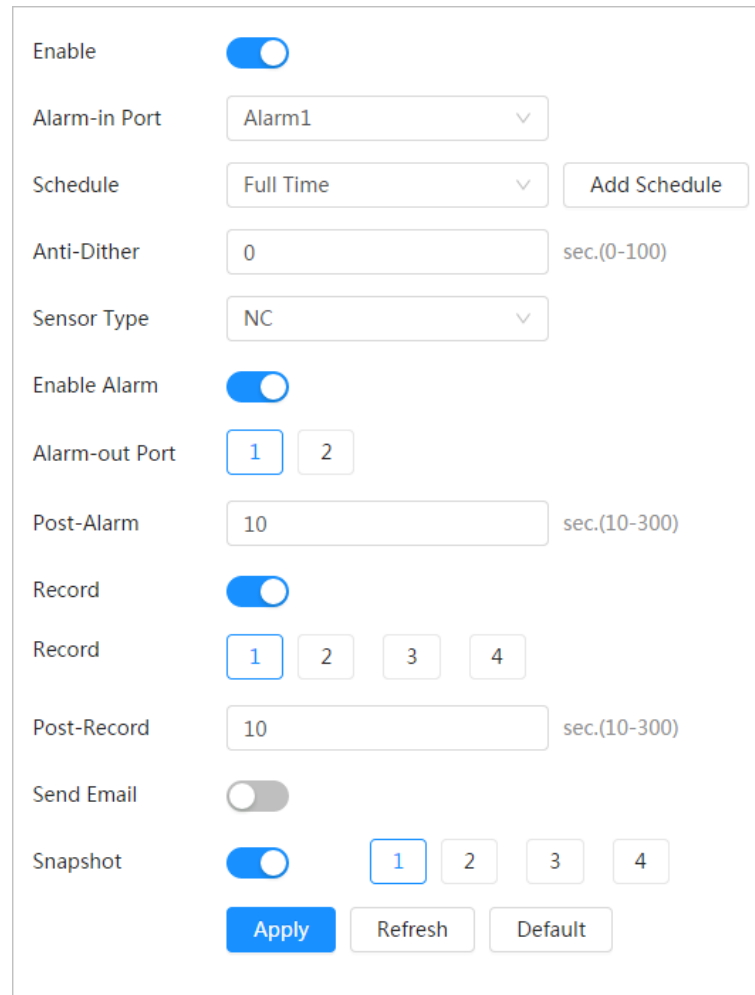
Step 5 Click **Apply**.

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 6-49 Alarm linkage



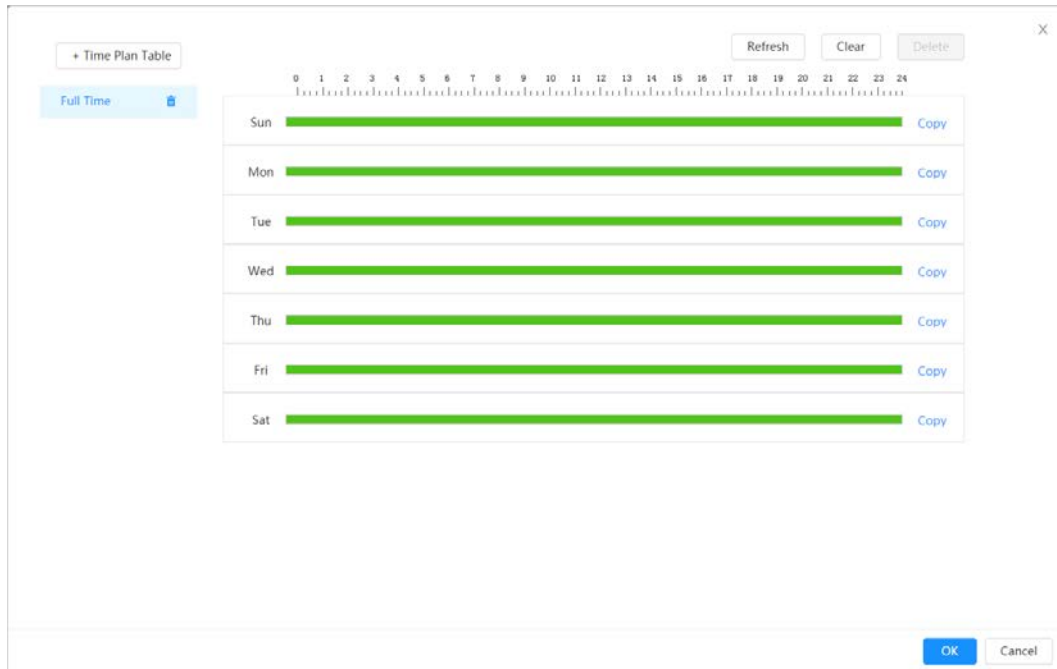
Enable	<input checked="" type="checkbox"/>
Alarm-in Port	Alarm1
Schedule	Full Time
Anti-Dither	0
Sensor Type	NC
Enable Alarm	<input checked="" type="checkbox"/>
Alarm-out Port	1 2
Post-Alarm	10
Record	<input checked="" type="checkbox"/>
Record	1 2 3 4
Post-Record	10
Send Email	<input type="checkbox"/>
Snapshot	<input checked="" type="checkbox"/>
	1 2 3 4
	Apply Refresh Default

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 6-50 Schedule




Step 2 Press and drag the left mouse button on the timeline to set arming periods. Alarms will be triggered in the 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 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 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 "10.3 Setting Record Plan".
- Enable auto record mode, the record linkage will take effect. For details, see "10.2 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 6-51 Record linkage

Record	<input checked="" type="checkbox"/>
Record	<input checked="" type="button" value="1"/> <input type="button" value="2"/> <input type="button" value="3"/> <input type="button" value="4"/>
Post-Record	<input type="text" value="10"/> sec.(10-300)

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 "10.3 Setting Record Plan".

Setting Record Linkage

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

Figure 6-52 Snapshot linkage

Snapshot	<input checked="" type="checkbox"/> <input type="button" value="1"/> <input type="button" value="2"/> <input type="button" value="3"/> <input type="button" value="4"/>
----------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------

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 6-53 Alarm-out linkage

Enable Alarm	<input checked="" type="checkbox"/>
Alarm-out Port	<input checked="" type="button" value="1"/> <input type="button" value="2"/>
Post-Alarm	<input type="text" value="10"/> sec.(10-300)

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 6-54 Email linkage

Send Email	<input type="checkbox"/>
------------	--------------------------

6.4.1.3 Subscribing Alarm

6.4.1.3.1 About Alarm Types

For alarm types and preparations of alarm events, see Table 6-23.

Table 6-23 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 "9.1 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.


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

Figure 6-55 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

Browse

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

Clear

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**.

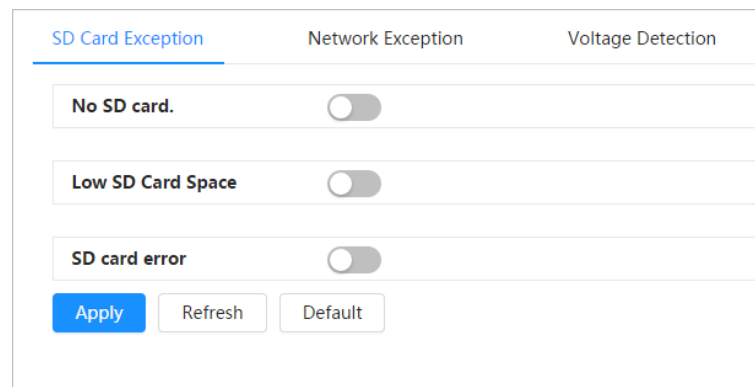
6.4.2.1 Setting SD Card Exception


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.

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

Figure 6-56 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 6-57 Network exception

SD Card Exception
Network Exception
Voltage Detection

Offline

Enable Alarm

Alarm-out Port

Post-Alarm sec.(10-300)

Record

Record

Post-Record sec.(10-300)

IP Conflict

Enable Alarm

Alarm-out Port

Post-Alarm sec.(10-300)

Record

Record

Post-Record 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 6-58 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 and 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 6-59 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 6-60 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**.

Step 2 Select the event type.

- **Video Tampering:** When the percentage of the tampered image and the duration exceed the configured values, an alarm will be triggered.
- **Defocus Detection:** When the image is blurred, an alarm will be triggered. This function is available on some select models.

Figure 6-61 Video tampering

Motion Detection	Video Tampering	Scene Changing
Event Type	Video Tampering	
Enable	<input type="checkbox"/>	
Covered Area	100	% (1-100)
Duration	1	sec. (1-300)
Anti-Dither	1	sec. (0-100)
Schedule	Full Time	<input type="button" value="Add Schedule"/>
Alarm-out Port	<input checked="" type="checkbox"/>	
Alarm Channel	<input type="text" value="1"/> <input type="text" value="2"/>	
Post-Alarm	10	sec. (10-300)
Record	<input checked="" type="checkbox"/>	
Post-Record	10	sec. (10-300)
Send Email	<input type="checkbox"/>	
Snapshot	<input checked="" type="checkbox"/>	
	<input type="button" value="Apply"/>	<input type="button" value="Refresh"/> <input type="button" value="Default"/>

Table 6-24 Description of video temper parameter

Parameter	Description
Covered Area	When the percentage of the tampered image and the duration exceed the configured values, an alarm will be triggered.
Duration	
Anti-Dither	Only record one alarm event during the anti-dither period.

Step 3 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 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 6-62 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 6-63 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

Displays 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.



Functions might vary with different models.

Select > **Storage**.

- 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.



When reading SD card on PC, if the SD card capacity is much less than the nominal capacity, you need to format the SD card. Then the data in SD card will be cleared, and the SD card is formatted to be private file system. The private file system can greatly improve SD card multimedia file read/write performance. Download Diskmanager from Toolbox to read the SD card. For details, contact after-sales technicians.

Figure 6-64 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.

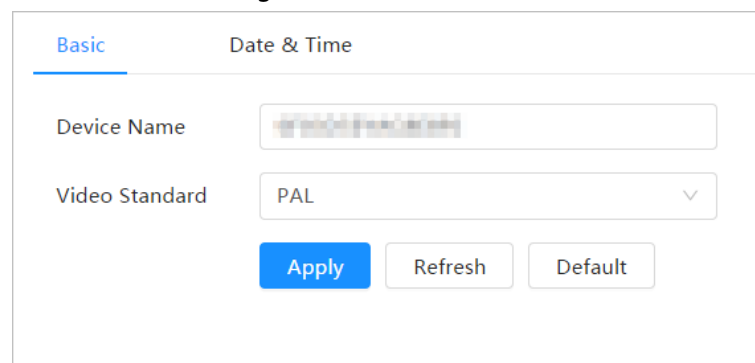
6.6.1 General

6.6.1.1 Basic

You can configure device name, language and video standard.

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

Figure 6-65 Basic



Step 2 Configure general parameters.

Table 6-25 Description of general parameters

Parameter	Description
Name	Enter the device name.
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 6-66 Date and time

Step 2 Configure date and time parameters.

Table 6-26 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.

Parameter	Description
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.
Current Time	Configure system time. Click Sync PC , and the system time changes to the PC time.
DST	Enable DST as needed. Click <input type="checkbox"/> , 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.

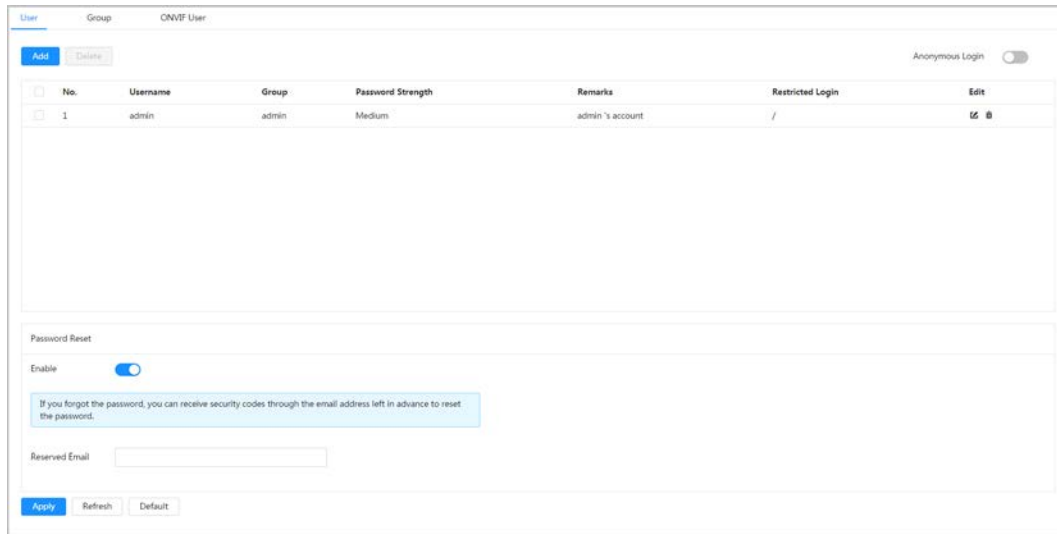
6.6.2.1 User

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 6-67 User



Step 2 Click **Add**.

Figure 6-68 Add user (system)

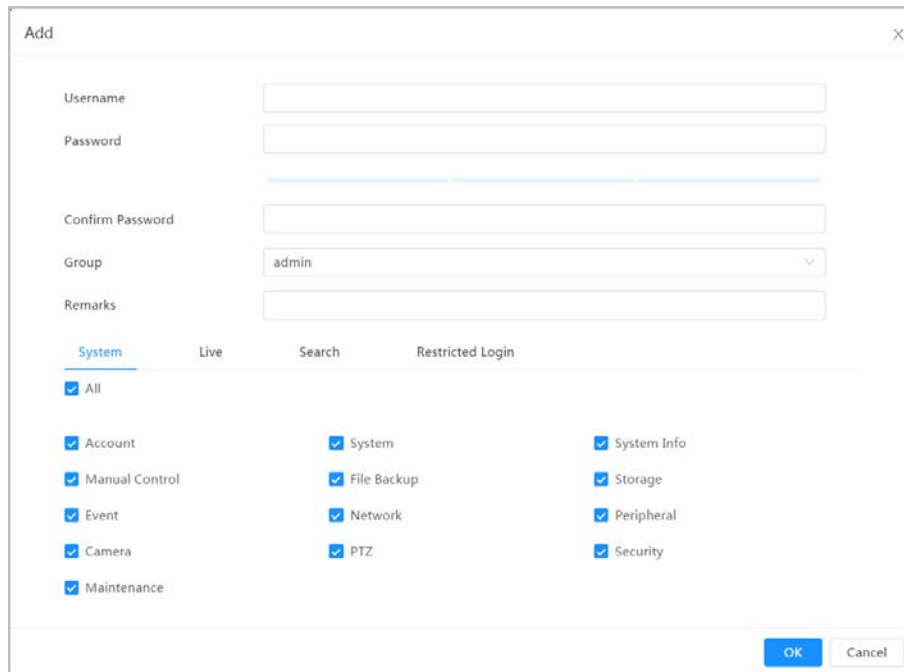



Figure 6-69 Add user (restricted login)

Step 3 Configure user parameters.

Table 6-27 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.  We recommend giving fewer permissions 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"> 1. IP address: Enter the IP address of the host to be added. 2. 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 6-70 User

The screenshot shows the 'User' management page. At the top, there are tabs for 'User', 'Group', and 'ONVIF User'. Below the tabs are 'Add' and 'Delete' buttons. On the right, there is an 'Anonymous Login' toggle. The main area contains a table with the following columns: No., Username, Group, Password Strength, Remarks, Restricted Login, and Edit. The table has one row for the 'admin' user. Below the table is a 'Password Reset' section with an 'Enable' toggle (currently turned on), a text box for 'Reserved Email', and 'Apply', 'Refresh', and 'Default' buttons.

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 6-71 Group name

No.	Group	Remarks	Operation
1	admin	administrator group	
2	user	user group	

Step 2 Click **Add**.

Figure 6-72 Add group

Group:

Remarks:

System | Live | Search

- All
- System
- File Backup
- Network
- PTZ
- System Info
- Storage
- Peripheral
- Security
- Manual Control
- Event
- Camera
- Maintenance



OK Cancel

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 6-73 ONVIF user

No.	Username	Group	Password Strength	Edit
1	admin	admin	Medium	

Step 2 Click **Add**.

Figure 6-74 Add ONVIF user

Step 3 Configure user parameters.

Table 6-28 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 change the password.

- Click to delete the added users.



The admin account cannot be deleted.

6.6.3 Peripheral Management

6.6.3.1 Configuring Serial Port

Set the serial port of the external device.


Step 1 Select  > **System** > **Peripheral** > **Serial Port**.

Step 2 Configure parameters.

Figure 6-75 Serial port settings

Serial Port	External Light	Wiper
Address	<input type="text" value="1"/>	
Baud Rate	<input type="text" value="9600"/>	▼
Data Bit	<input type="text" value="8"/>	▼
Stop Bit	<input type="text" value="1"/>	▼
Parity	<input type="text" value="None"/>	▼
<input type="button" value="Apply"/> <input type="button" value="Refresh"/> <input type="button" value="Default"/>		

Table 6-29 Description of serial port settings parameters

Parameter	Description
IP Address	Enter the corresponding device address. It is 1 by default.  Make sure that the address is the same as the device address; otherwise you cannot control the device.
Baud Rate	Configure device baud rate. It is 9600 by default.
Data Bits	It is 8 by default.
Stop Bits	It is 1 by default.
Test	It is none by default.

Step 3 Click **Apply**.


6.6.3.2 Configuring External Light

You need to configure external light mode when the external light is used.

Prerequisites

- Connect external light with RS-485 port.
- You have configured serial port parameters. For details, see "6.6.3.1 Configuring Serial Port".

Procedure

Step 1 Select  > **System** > **Peripheral** > **External Light**.

Step 2 Select working mode as needed.

Figure 6-76 External light

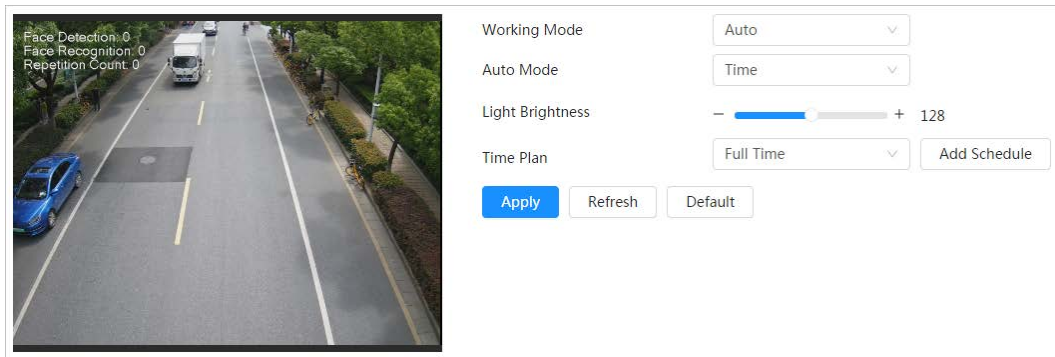



Table 6-30 Lamp parameters

Parameter	Description
Work Mode	<ul style="list-style-type: none"> ● Off: The external light is disabled. ● Manual: Set the light brightness manually. ● Auto: The camera turns on or turns off the light according to the light time and photoresistor automatically.
Auto Mode	<ul style="list-style-type: none"> ● Time: When selecting Time in Auto Mode, set the arming period. During the arming period, the external light is on. Select the added time plan table in the Time Plan list. Click Add Schedule to add new time plan table. For details, see "6.4.1.2 Alarm Linkage". ● Photoresistor: When you select Photoresistor in Auto Mode, the camera turns on the external light according to the brightness automatically.
Light Brightness	Set the brightness of the external light.  For some models, you can set the brightness of each external light separately.

Step 3 Click **OK**.

6.6.3.3 Configuring Wiper

Step 1 Select  > **System** > **Peripheral** > **Wiper**.

Step 2 Configure working mode of wipers.

Figure 6-77 Wiper

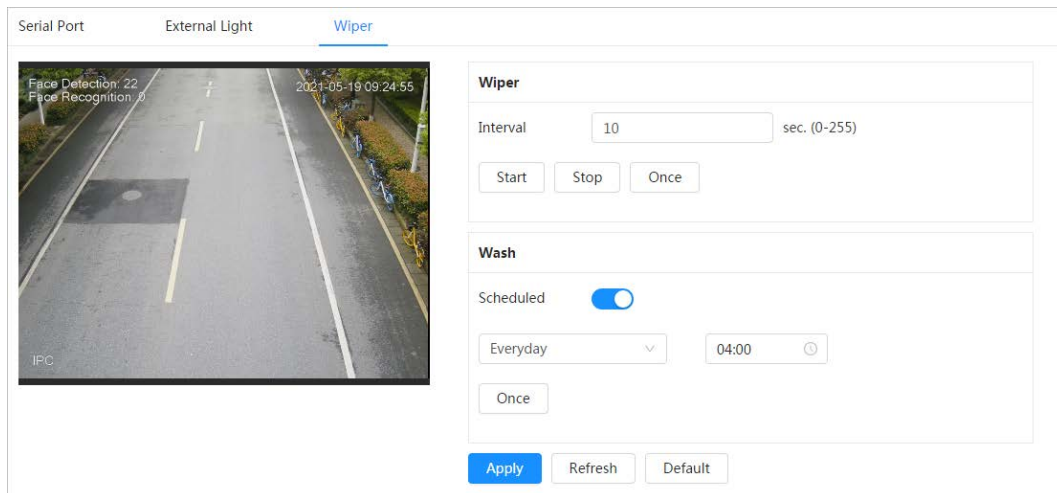


Table 6-31 Wiper parameter description

Parameter	Description
Interval	The interval between stop mode and start mode. For example, set the time to 10 s, and the wiper will work every 10 s.
Start, Stop, Once	Configure working mode of the wiper. <ul style="list-style-type: none"> Click Start, and the wiper works as the set interval time. Click Stop, and the wiper stops working. Click Once, and the wiper works once.
Wash	Select the Schedule check box and set the time, and then the wiper will work as the configured time. Click Once , and the wiper works once. It can be used to check whether the wiper works normally.

Step 3 Click **Apply**.

6.6.4 Manager

6.6.4.1 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.

6.6.4.2 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 6-78 Maintenance

Step 2 Configure auto maintain parameters.

- Click next to **Auto Reboot** in **Restart System**, and set the reboot time, then the system will automatically restarts at the set time every week.
- Click next to **Auto Delete** in **Delete Old Files**, and set the time, then the system will automatically deletes old files at 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**.

6.6.4.3 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 6-79 Import/Export

Step 2 Import or export the file.

- 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.

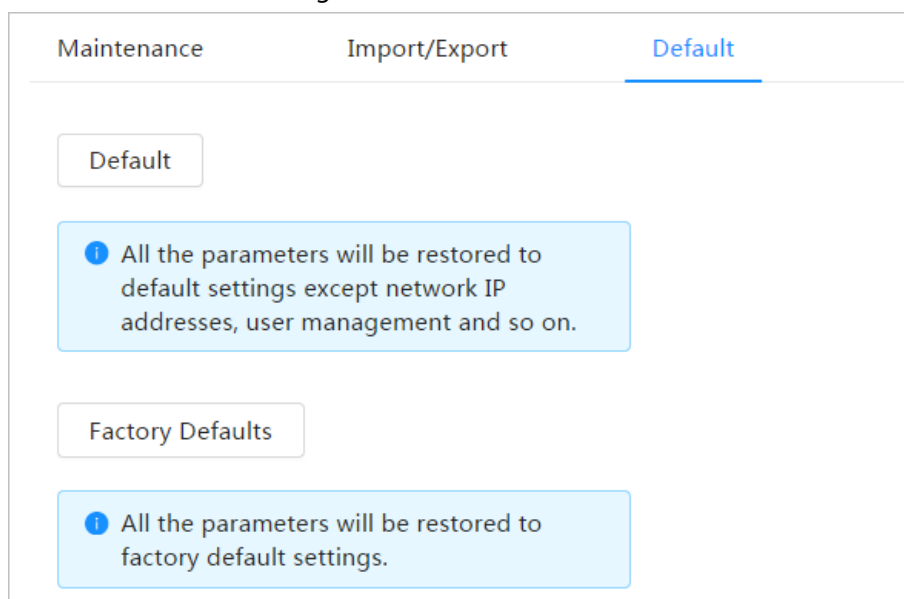
6.6.4.4 Default

Restore the device to default configuration or factory settings.

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 6-80 Default



6.6.5 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 6-81 Upgrade




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

Step 3 Click **Update**.


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 online 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 1, 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 6-82 Log

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 11:08:23	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) < 1 2 > Goto

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 6-83 Remote log

Enable	<input type="checkbox"/>
Server Address	<input type="text"/>
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 chapter introduces the layout of the interface and function configuration.

7.1 Live Interface

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



Interfaces might vary with different models.

Figure 7-1 Live (single-channel)

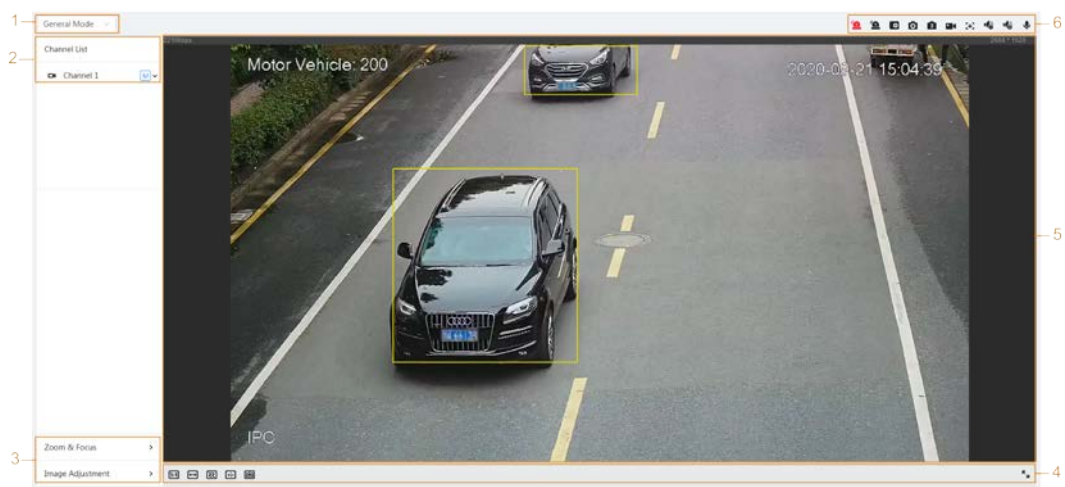


Figure 7-2 Live (multi-channels)

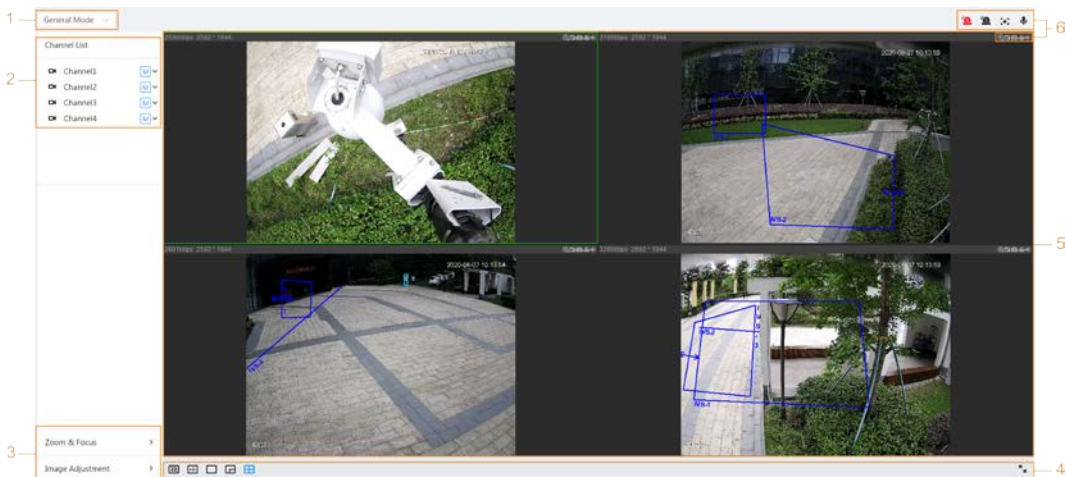


Table 7-1 Description of function bar

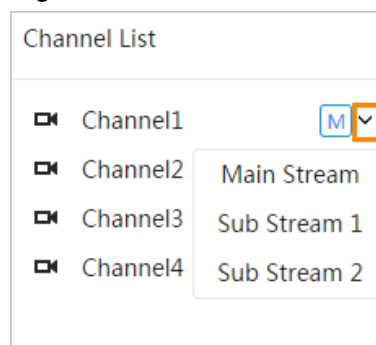
No.	Function	Description
1	Display mode	You can select the display mode from General Mode , Face Mode , Metadata Mode , ANPR and Face & Body Detection . For details, see "7.5 Display Mode".
2	Channel list	Displays all channels. You can select the channel as needed and set the stream type.




No.	Function	Description
3	Image adjustment	Adjustment operations in live viewing.
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	Displays alarm sound state. Click the icon to enable or disable the alarm sound forcibly.








Icon	Function	Description
	Digital Zoom	<p>You can zoom video image through two operations.</p> <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.
	Snapshot	<p>Click the icon to capture one picture of the current image, and it will be saved to the configured storage path.</p> <p> For details on viewing or configuring storage path, see "6.1 Local".</p>
	Triple Snapshot	<p>Click the icon to capture three pictures of the current image, and they will be saved to the configured storage path.</p> <p> For details on viewing or configuring storage path, see "6.1 Local".</p>
	Record	<p>Click the icon to record video, and it will be saved to the configured storage path.</p> <p> For details on viewing or configuring storage path, see "6.1 Local".</p>
	Aux Focus	<p>Click the icon, the AF Peak (focus eigenvalue) and AF Max (max focus eigenvalue) are displayed on the video image.</p> <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. <p> Aux focus closes automatically after five minutes.</p>
	Audio	Click the icon to enable or disable audio output.
	Talk	Click the icon to enable or disable the audio talk.

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.
	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	<p>Click the icon to select the fluency from Realtime, General and Fluent.</p> <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 viewing 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

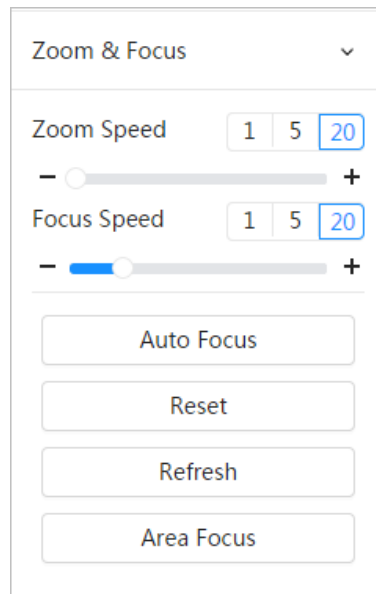




Table 7-4 Description of zoom and focus parameter

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	<p>Get the latest zoom setting of the camera.</p>
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>

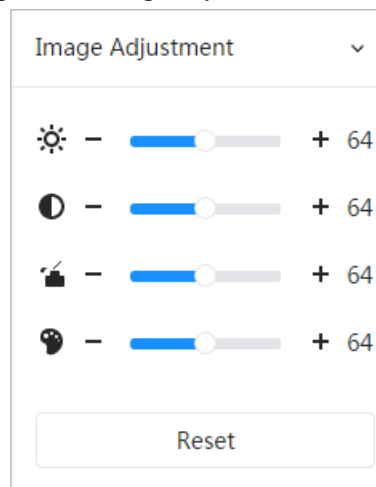
7.4.3 Image Adjustment

Click **Image Adjustment** at the lower-left corner of **Live** interface, and click + or- button, or drag the slider 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.

7.4.4 Fisheye

You can select the installation mode, display mode and VR mode of fisheye devices as needed. For details, see Table 7-5.

- **Install Mode:** Select the installation mode according to the actual situation.
- **Display Mode:** Select the display mode of live view.
- **VR Mode:** Select VR mode to display images in stereo mode.

Figure 7-6 Fisheye-ceiling mount

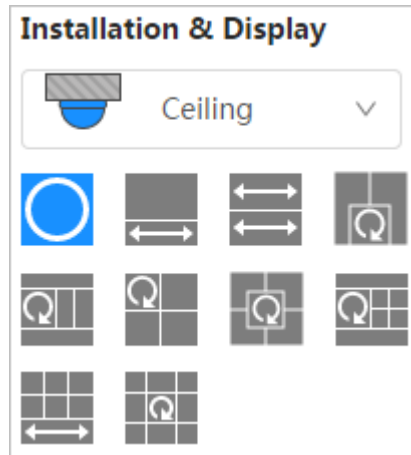


Figure 7-7 Fisheye-wall mount

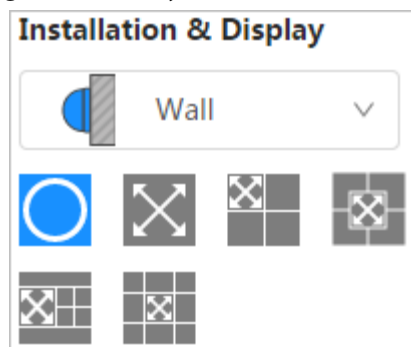


Figure 7-8 Fisheye-ground mount

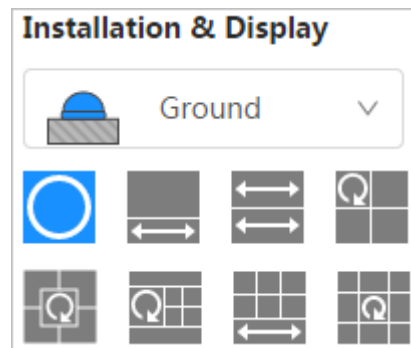













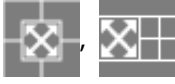


Figure 7-9 Fisheye-VR mode






Table 7-5 Description of fisheye configuration

Parameter	Description
Installation mode	Includes ceiling mount, wall mount, and ground mount.

Parameter	Description	
Display mode	<p>The display model of the current image. There are different display modes for each installation mode.</p> <ul style="list-style-type: none"> ● Ceiling: 1P+1, 2P, 1+2, 1+3, 1+4, 1P+6, 1+8. ● Wall: 1P, 1P+3, 1P+4, 1P+8. ● Ground: 1P+1, 2P, 1+3, 1+4, 1P+6, 1+8.  <p>The image will be the original size by default when switching installation mode.</p>	
Ceiling/Wall/Ground mount	 Original image	The original image before correction.
Ceiling/Ground mount	 1P+1	<p>360° rectangular panoramic image screen + independent sub-screens.</p> <ul style="list-style-type: none"> ● You can zoom or drag the image in all the screens. ● You can move the start point (left and right) on rectangular panoramic image screen.
	 2P	<p>Two associated 180° rectangular image screens; at any time, the two screens form a 360° panoramic image. It is also called dual-panoramic image.</p> <p>You can move the start point (left and right) on the two rectangular panoramic image screens, and the two screens link each other.</p>
	 1+2	<p>Original image screen + two independent sub-screens. Ground mount does not support this display mode.</p> <ul style="list-style-type: none"> ● You can zoom or drag the image in all the screens. ● You can rotate the image on the original image screen to change the start point.
	 1+3	<p>Original image screen + three independent sub-screens.</p> <ul style="list-style-type: none"> ● You can zoom or drag the image in all the screens. ● You can rotate the image on the original image screen to change the start point.
	 1+4	<p>Original image screen + four independent sub-screens.</p> <ul style="list-style-type: none"> ● You can zoom or drag the image in all the screens. ● You can rotate the image on the original image screen to change the start point.

Parameter	Description
	 1P+6 360° rectangular panoramic screen + six independent sub-screens. <ul style="list-style-type: none"> You can zoom or drag the image in all the screens. You can move the start point (left and right) on rectangular panoramic image screen.
	 1P+8 Original image screen + eight independent sub-screens. <ul style="list-style-type: none"> You can zoom or drag the image in all the screens. You can rotate the image on the original image screen to change the start point.
Wall mount	 1P 180° rectangular panoramic image screen (from left to right). You can drag the image in all the screens (up and down) to adjust the vertical view.
	 1P+3 180° rectangular panoramic image screen + three independent sub-screens. <ul style="list-style-type: none"> You can zoom or drag the image in all the screens. You can drag the image in all the screens (upper and lower) to adjust the vertical view.
	 1P+4 180° rectangular panoramic image screen + four independent sub-screens. <ul style="list-style-type: none"> You can zoom or drag the image in all the screens. You can drag the image in all the screens (upper and lower) to adjust the vertical view.
	 1P+8 180° rectangular panoramic image screen + eight independent sub-screens. <ul style="list-style-type: none"> You can zoom or drag the image in all the screens. You can drag the image in all the screens (upper and lower) to adjust the vertical view.
VR mode	 Panorama Drag or cross the screen 360° to unfold the distortion panorama, and you can drag the image in left/right direction.

Parameter	Description	
	 Semi-circle	<ul style="list-style-type: none"> You can drag the image in upper/lower/left/right direction. Press I to display the panorama, and press O to resume the original size. Press S to rotate the image in anticlockwise direction, and press E to stop the rotation. Scroll the mouse wheel to zoom the image.
	 Cylinder	<p>Display the distortion panorama in 360° circularity.</p> <ul style="list-style-type: none"> You can drag the image in upper/lower/left/right direction. Press I to display the panorama, and press O to return to the original size. Press S to rotate the image in anticlockwise direction, and press E to stop the rotation. Scroll the mouse wheel to zoom the image.
	 Asteroid	<ul style="list-style-type: none"> You can drag the image in upper/lower/left/right direction. Press I to display the panorama, and press O to return to the original size. Press the left mouse-button to slide down to display the image on the plane surface. Scroll the mouse wheel to zoom the image.

7.5 Display Mode

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



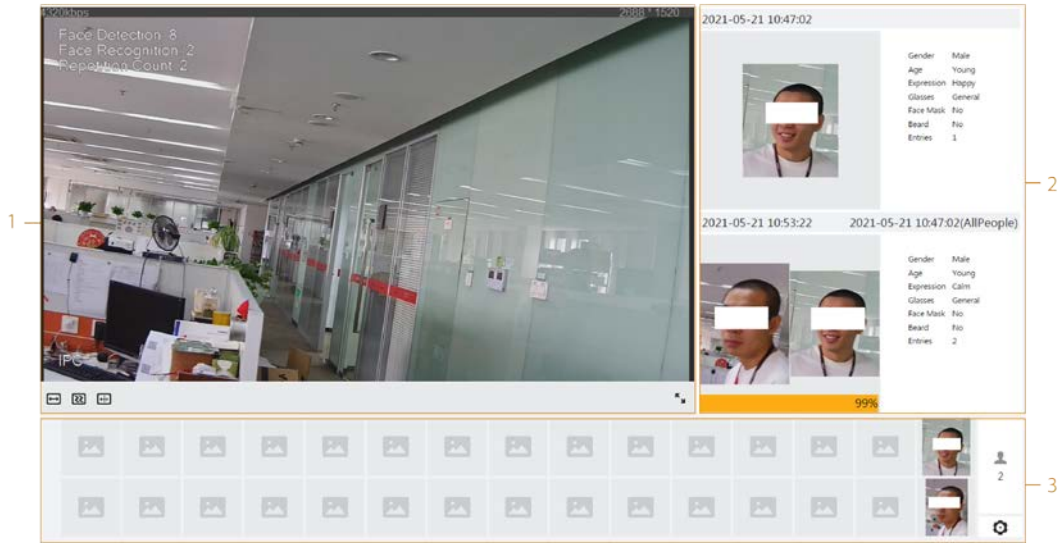
Interfaces might vary with different models.

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



Make sure that you have enabled face detection function.

Figure 7-10 Face mode

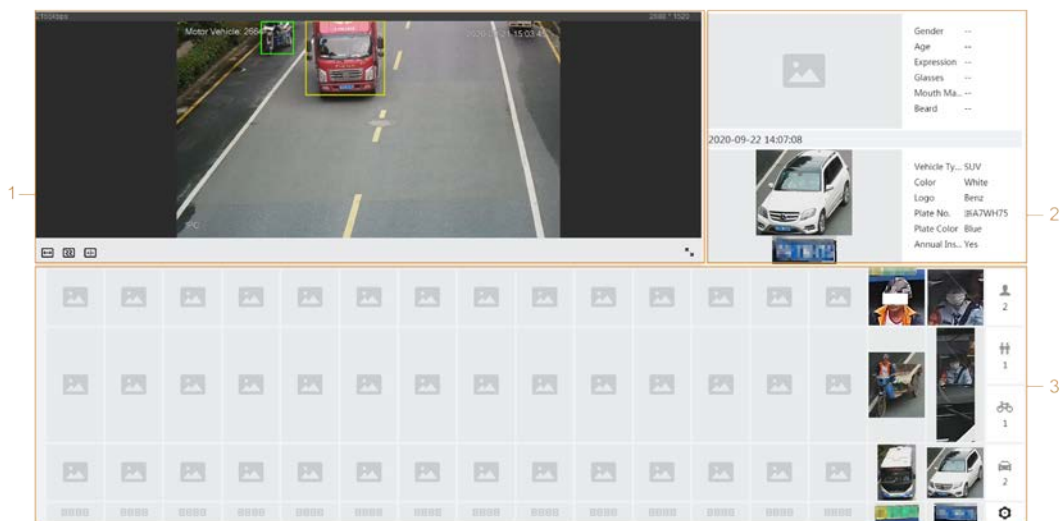


- Select **Metadata Mode** from the display mode drop-down list.



Make sure that you have enabled video metadata detection function.

Figure 7-11 Metadata mode

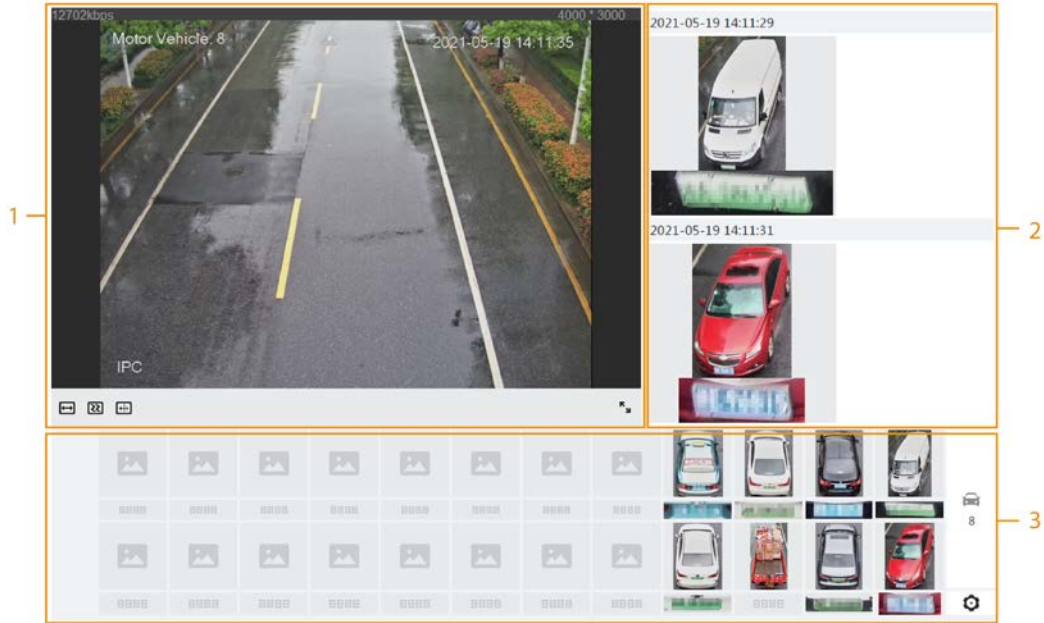


- Select **ANPR** from the display mode drop-down list.



Make sure that you have enabled ANPR function.

Figure 7-12 ANPR



- Select **Face & Body Detection** from the display mode drop-down list.



Make sure that you have enabled face & body detection function.

Figure 7-13 Face & body detection

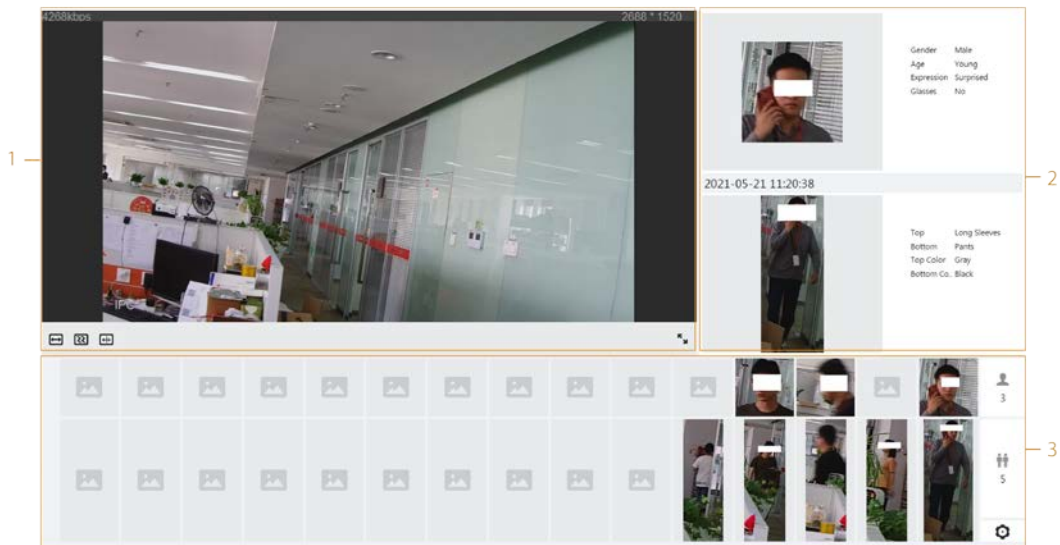



Table 7-6 Description of layout

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.

No.	Function	Description
3	Captured image	<p>Displays the captured images.</p> <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




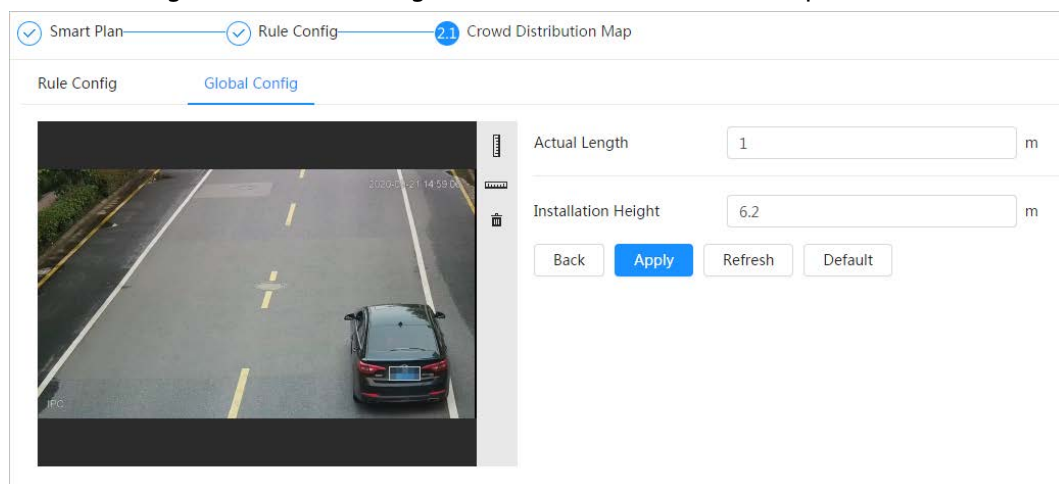
1. Select **AI > Smart Plan**.
2. Click next to **Crowd Distribution Map** to enable crowd distribution map of the corresponding channel, and then click **Next**.
3. Click the **Global Config** tab.
4. Click the rule icon to draw one horizontal ruler and three vertical rulers on the image.
 -  is the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

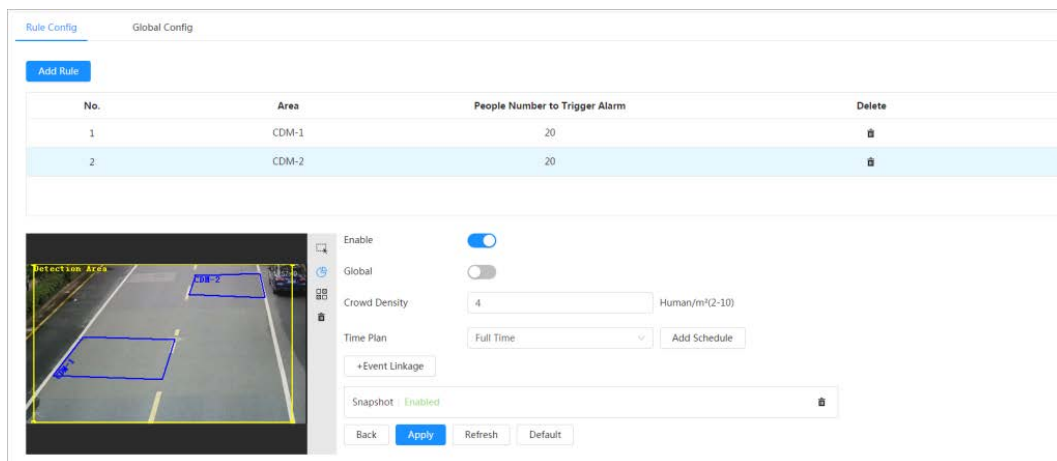
Procedure

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

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)



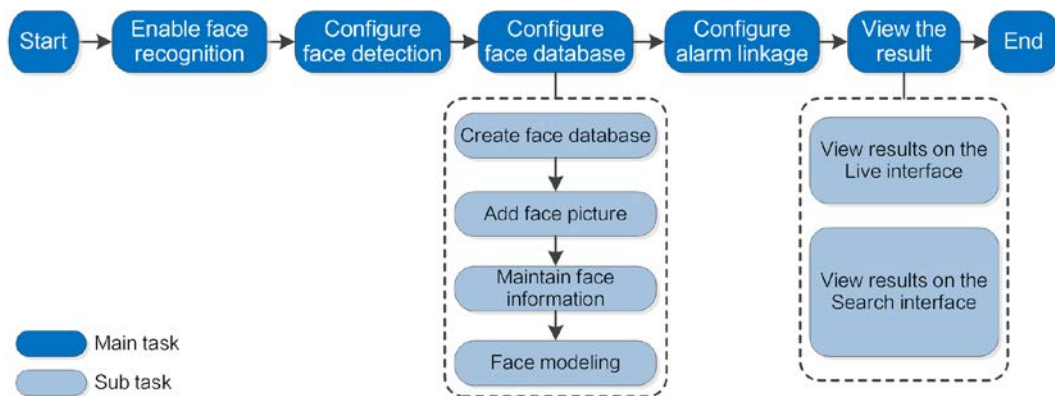
8.2 Setting Face Recognition

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.

Figure 8-5 Face recognition flowchart



8.2.1 Setting Face Detection

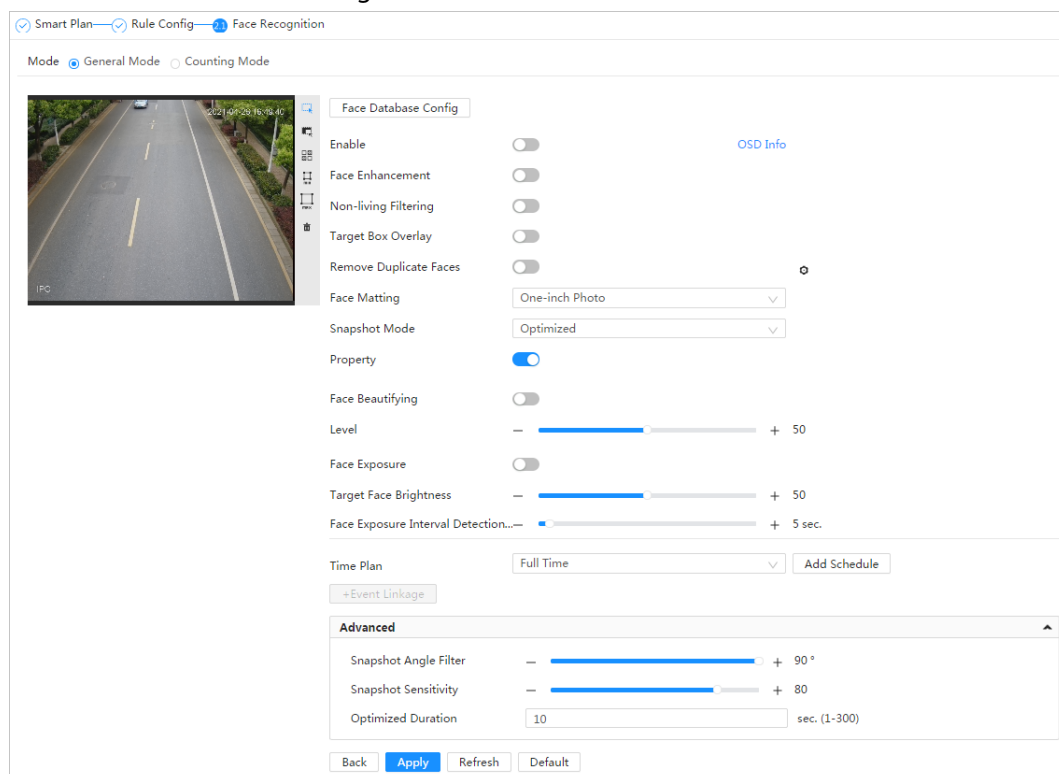
When a face is recognized in the detection area, the system performs alarm linkage.

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**.

Figure 8-6 Face detection



Step 3 Select the detection mode.

- **General Mode:** When a face is detected in the detection area, the system performs alarm linkage, such as recording and sending emails.
- **Counting Mode:** You can do precise face counting with two default function databases (all people database and exclude people database). The faces detected by the camera will be uploaded to the all people database automatically; the face in the exclude

people database will not be counted. Add faces that you do not want to count (such as repeating faces and loitering faces) into the exclude people database so that the system will not count the faces after detecting them.

Step 4 Click next to **Enable** to enable the face detection function.

Step 5 (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 rule line in the image.

When targets enter or leave the detection area along the direction line, their face images will be uploaded to the all people database, and then the system will determine whether to count it after comparing with that in the exclude database.






This icon is only available in counting mode.

- Click to draw a face detection area in the image, and right-click to finish the drawing.
- Click to draw an 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 is 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 6 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 "6.2.2.2.12 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 to configure the parameter, 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.

Parameter	Description
Face Matting	<p>Set a range for the captured face image, including face, one-inch picture, and custom.</p> <p>When selecting Custom, click , configure the parameters on the prompt interface, and then click Apply.</p> <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 cuts out the face image only.
Snap Mode	<ul style="list-style-type: none"> • General 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. We recommend you using this mode in access control scene. <p></p> <p>Click Advanced to set the optimized time.</p> <ul style="list-style-type: none"> • Counting mode: The snapshot mode is tripwire by default, and you cannot change it.
Property	Click  next to Property to enable the properties display.
Face Beautifying	Enable Face Beautifying to make face details clearer at night. After enabling this function, you can adjust the level. The higher the level, the higher the beautifying level.
Face Exposure	Enable 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 5 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 period to capture the clearest picture after the camera detects face.

Step 7 Set arming periods and alarm linkage action. For details, see "6.4.1.2 Alarm Linkage".

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".

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.

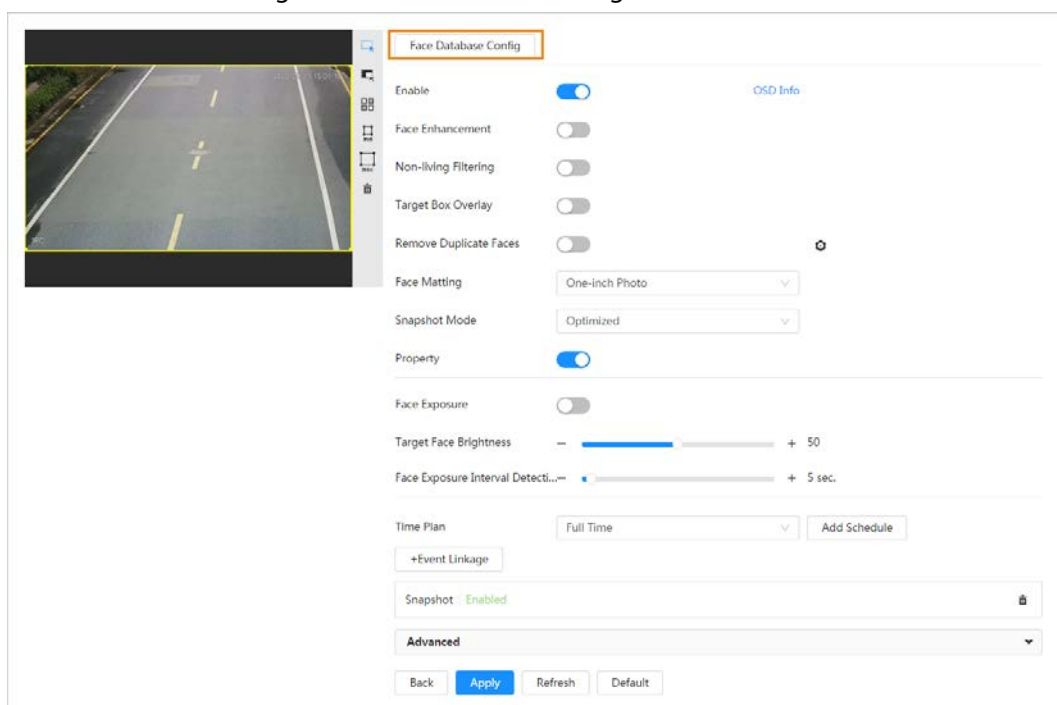
8.2.2.1 Creating Face Database

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 Select the detection mode.
- Step 4 Click **Face Database Config** on the **Face Recognition** interface.

Figure 8-7 Face database configuration



- Step 5 Click **Add Face Database**.
- Step 6 Set the name of the face database.

Figure 8-8 Add face database

Step 7 Click **OK**.

- General mode: You can add 5 databases at most as needed.

Figure 8-9 Face database successfully added (general mode)

No.	Name	Register No.	Similarity	Arm Status	Arm Alarm	Details	Delete
1	VIP	0	82	Unconnected			
2	Employees	0	82	Unconnected			
3	5	0	82	Unconnected			
4	6	0	82	Unconnected			
5	test01	0	82	Unconnected			

- Counting mode: Except two default function databases (all people database and exclude people database), you can add 5 databases at most. Add faces that you do not want to count (such as repeating faces and loitering faces) into the exclude people database so that the system will not count the faces face after detecting them.

Figure 8-10 Face database successfully added (counting mode)

No.	Name	Register No.	Similarity	Arm Status	Arm Alarm	Details	Delete
1	AllPeople	0	82	Connected			
2	ExcludePeople	0	82	Connected			
3	VIP	0	82	Unconnected			
4	Employees	0	82	Unconnected			
5	5	0	82	Unconnected			
6	6	0	82	Unconnected			
7	test01	0	82	Unconnected			

- Edit the name of the face database

Click the text box under **Name** to edit the name of the face database.



- ◇ You cannot change the name of all people database and exclude database.
- ◇ Do not name the newly added database as **AllPeople** or **ExcludePeople**.

- Arm alarm

Click to configure the parameters of arm alarm. For details, see "8.2.3 Setting Arm Alarm".

- Manage face database

Click to manage the face database. You can search face, register, batch register, modeling all, modeling, and delete faces.



The all people database only supports modeling all, modeling, and delete faces.

- Delete face database

Click to delete the face database.



The all people database and exclude database cannot be deleted.


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 8-11 Register

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.

Parameter	Error	Description
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.
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

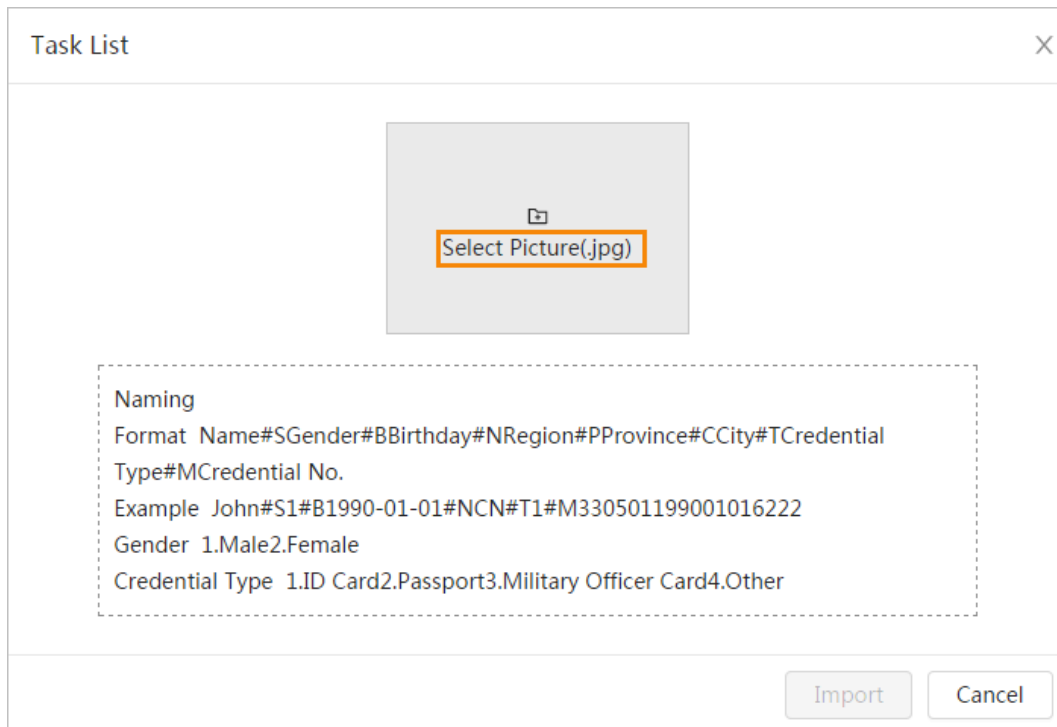
Parameter	Description
Name	Enter a name.
Gender	"1" is male and "2" female.
Date of Birth	Format: yyyy-mm-dd, such as 2020-10-23.
Credentials Type	"1" is ID card and "2" passport.
ID number	Enter ID No.

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 8-12 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





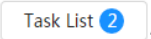
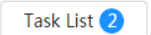
- Step 1** On the **Face Database Config** interface, click  next to the face database to be configured.
- Step 2** Click **Query**, set the criteria as needed, and then click **Search**.
- Step 3** Select the row where the face picture or the personnel information is located, and then click .
- Step 4** Edit face information according to the actual need. Click **Add to task list**.

Figure 8-13 Face information modification

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**.

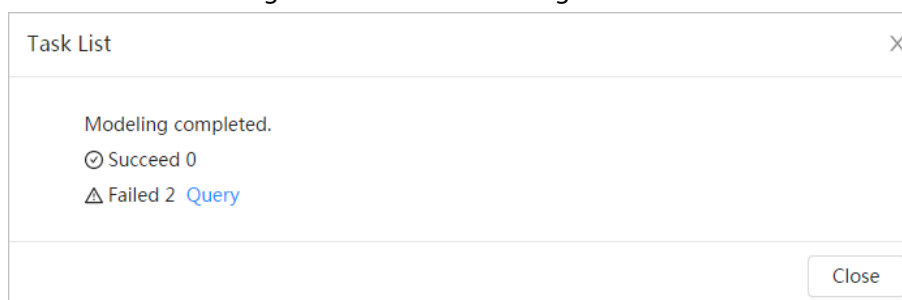
- All modeling.

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 8-14 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.

8.2.3 Setting Arming 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 8-15 Arm alarm

Arm Alarm

Name 1

Arm

Similarity - + 82

Time Plan Full Time

Local

Alarm-out Port Alarm Channel1

Alarm Mode Select None ⓘ

Post-Alarm 1 sec. (1-300)

Report Mode All ⓘ

General Mode	Stranger Mode
Record <input type="checkbox"/>	Record <input type="checkbox"/>
Post-Record 10 sec. (10-300)	Post-Record 10 sec. (10-300)
Audio Linkage <input type="checkbox"/>	Audio Linkage <input type="checkbox"/>
Send Email <input type="checkbox"/>	Send Email <input type="checkbox"/>
Snapshot <input checked="" type="checkbox"/>	Snapshot <input checked="" type="checkbox"/>

Figure 8-16 Arm alarm (all people)

Arm Alarm

Name: AllPeople

Arm:

Similarity: + 82

Time Plan: Full Time

Local:

Alarm-out Port: Alarm Channel1

Alarm Mode: Select None ⓘ

Post-Alarm: 1 sec. (1-300)

Report Mode: All ⓘ

General Mode	Stranger Mode
Record: <input type="checkbox"/>	Record: <input type="checkbox"/>
Post-Record: 10 sec. (10-300)	Post-Record: 10 sec. (10-300)
Audio Linkage: <input type="checkbox"/>	Audio Linkage: <input type="checkbox"/>
Send Email: <input type="checkbox"/>	Send Email: <input type="checkbox"/>
Snapshot: <input checked="" type="checkbox"/>	Snapshot: <input checked="" type="checkbox"/>

Auto Delete:

Delete Old Files: 7 day(s) ago (1-30)

Figure 8-17 Arm alarm (exclude people)

Arm Alarm

Name: ExcludePeople

Arm:

Similarity: + 82

Time Plan: Full Time

Step 3 Set arming periods.

Step 4 Click next to **Local** to enable local alarm output.

Table 8-5 Local alarm output

Parameter	Description
Alarm-out Port	For the device with multiple alarm-out channels, select the channels as needed.

Parameter	Description
Alarm Mode	<ul style="list-style-type: none"> • All: No matter the comparison result of the detected face and that in the face database, the camera links alarm out. • General: The camera links alarm out when the detected face matches that in the face database, the camera links alarm out. • Stranger: The camera links alarm out when the detected face fails to match that in the face database, the camera links alarm out. • Select none: the camera does not link alarm out no matter the comparison result of the detected face and that in the face database, the camera does not link alarm out.
Post-Alarm	When alarm delay is configured, alarm continues for the defined period after the alarm ends.

Step 5 Select the report mode and alarm linkage action.

- There are four report modes:
 - ◇ All: The camera reports events no matter the comparison result of the detected face and that in the face database, and then configure the linkage action in **General Mode** and **Stranger Mode**.
 - ◇ General: The camera reports events when the detected face matches that in the face database, and then configure the linkage action in **General Mode**.
 - ◇ Stranger: The camera reports events when the detected face fails to match that in the face database, and then configure the linkage action in **Stranger Mode**.
 - ◇ Select none: The camera does not report events no matter the comparison result of the detected face and that in the face database. You do not need to configure any linkage action.
- Set alarm linkage action. For details, see "6.4.1.2 Alarm Linkage".

Step 6 Enable **Auto Delete**, set the time.

When the database is full, the camera will delete the old files according to the configured time, and it is 7 days by default.



This function is only available on the all people database.

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".

8.2.4 Viewing Face Recognition Result

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


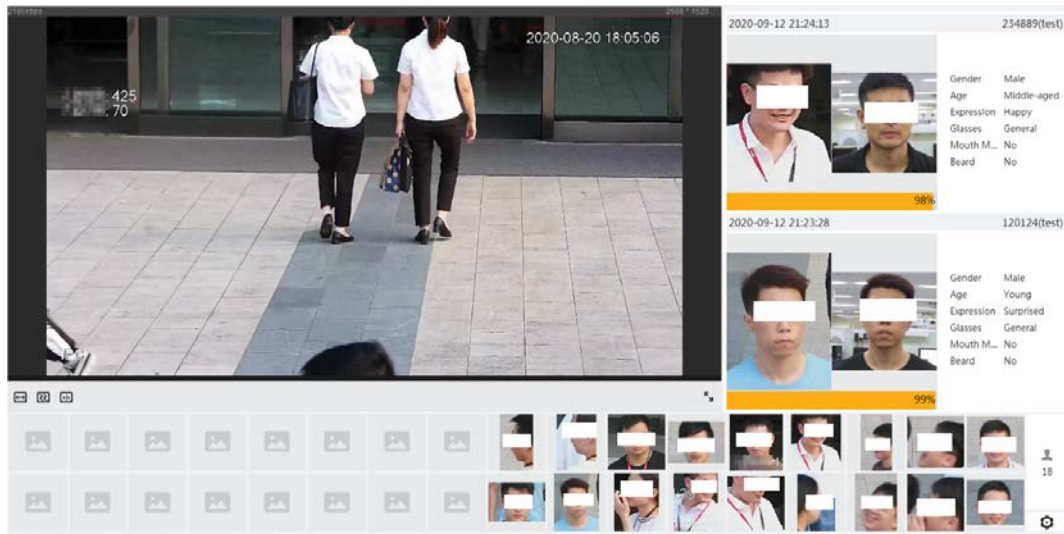
- The live image is displayed at the left side, and the captured face pictures and attribute information are displayed at the right side. When the recognition is successful, the captured face pictures, pictures in the database and the similarity of the face pictures and pictures in the database are displayed 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 8-18 Face recognition result



8.3 Setting Face Detection

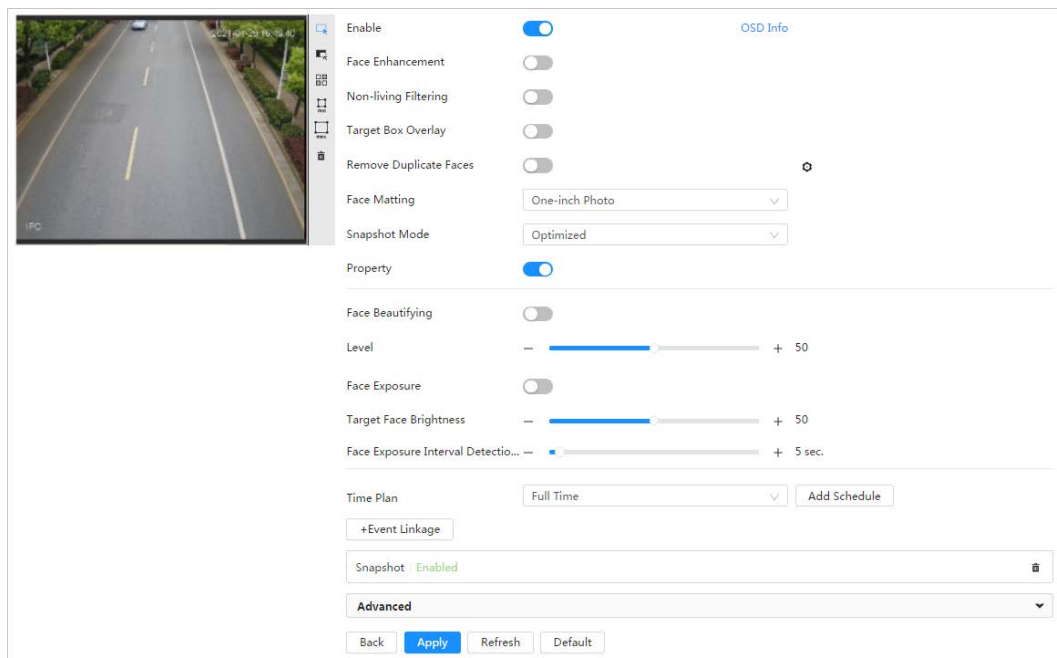
When a face is detected in the detection area, the system performs an alarm linkage.

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 8-19 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 is 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 8-6 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 "6.2.2.2.12 Configuring Face Statistics".
Face Enhancement	Click <input type="checkbox"/> to enable face enhancement, and it can preferably guarantee clear face with low stream.
Target Box Overlay	Click <input type="checkbox"/> 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.
Property	Click <input type="checkbox"/> next to Property 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 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**.

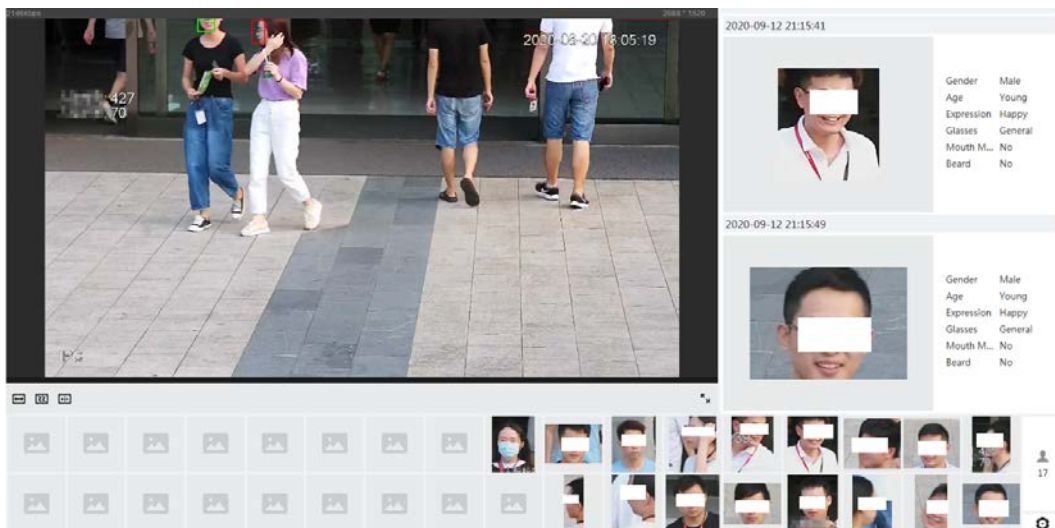
To view alarm information on the alarm subscription tab, you need to subscribe relevant alarm event. For details, see "6.4.1.3.2 Subscribing Alarm Information".

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 8-20 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

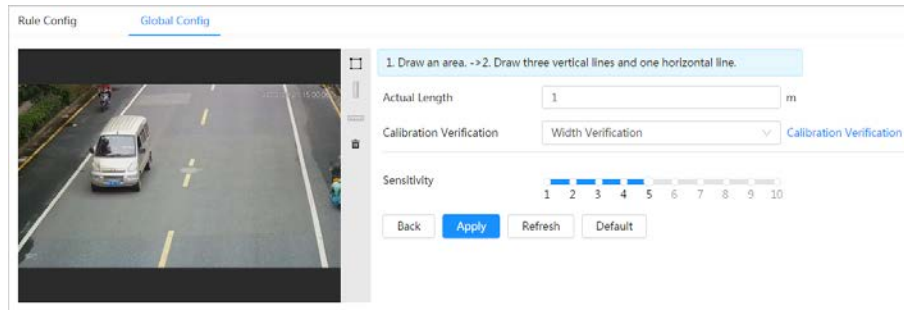
- Calibration Drawing
 - ◇ Calibration area: The calibration area drawn should be on one horizontal plane.
 - ◇ Vertical ruler: The bottom of three vertical rulers should be on the same horizontal plane. Select three reference objects with fixed height in triangular distribution as vertical rulers, such 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 8-21 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 8-7.

Table 8-7 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.	Scenes with sparse targets and without obvious and frequent light change. Simple scene in the detection area is recommended. <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.	Scenes with sparse targets and without obvious and frequent light change. Simple scene in the detection area is recommended. <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.

Rule	Description	Applicable Scene
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.
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**.

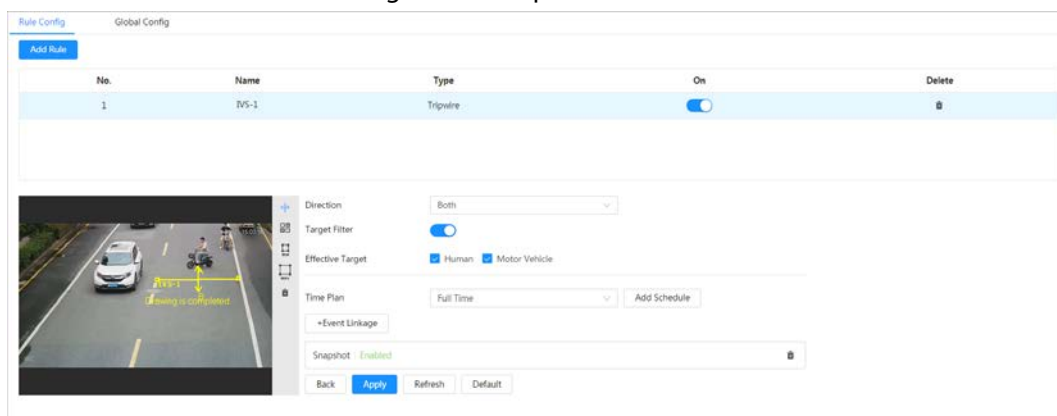
Step 2 Click next to **IVS** to enable IVS of the corresponding channel, and then click **Next**.

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 8-22 Tripwire








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

For requirements of drawing rules, see Table 8-7. After drawing rules, drag corners of the detection area to adjust the area range.

Table 8-8 Description of IVS analysis


Rule	Description
Tripwire	Draw a detection line.
Intrusion	Draw a detection area. <ul style="list-style-type: none"> During the detection of abandoned object, the alarm is also 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. 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.
Abandoned object	
Missing object	
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 is 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 8-9 Description of IVS parameters

Parameter	Description
Direction	Set the direction of rule detection. <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	When setting intrusion action, select Appears or Cross .
Target Filter	Click  to enable this function. <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.

Parameter	Description
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.
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 Vehicle Density

Configure rules for vehicle density, including road congestion and parking upper limit, and you can view vehicle statistics through the live interface.

Background Information

Configure rules for traffic congestion and parking upper limit. When the counted vehicle exceeds the configured vehicle number and the congestion time exceeds the configured time, an alarm will be triggered.

Procedure

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

Step 2 Click next to **Vehicle Density**, and then click **Next**.

Step 3 Click **Add Rule** to select rules.

Figure 8-23 Add rules

No.	Name	Type	On	Delete
1	VD-1	Traffic Congestion	<input checked="" type="checkbox"/>	
2	VD-2	Parking Upper Limit	<input checked="" type="checkbox"/>	

Step 4 (Optional) Click other icons at the right side of the image to draw detection area on the image.

- Click to draw a detection area in the image. The detection area is the whole image by default.
- 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.

Repeat step 1-4 to add multiple statistical areas. You can add up to 9 rules at most.

Figure 8-24 Vehicle density (traffic congestion)

The screenshot shows the 'Add Rule' configuration interface. At the top, there is a table with columns: No., Name, Type, On, and Delete. Two rules are listed: Rule 1 (VD-1, Traffic Congestion) and Rule 2 (VD-2, Parking Upper Limit). Below the table, there is a video feed on the left showing a parking area with a blue detection line. On the right, the configuration parameters are: Repeat Alarm Time (0 sec), Vehicle Congestion Alarm (checked), Threshold (10 vehicles), Duration (1 min), Time Plan (Full Time), and Snapshot (Enabled). Buttons for Back, Apply, Refresh, and Default are at the bottom.


Figure 8-25 Vehicle density (parking upper limit)

The screenshot shows the 'Add Rule' configuration interface. The table at the top is identical to Figure 8-24. The video feed on the left shows a parking area with a yellow detection line. The configuration parameters on the right are: Repeat Alarm Time (0 sec), Upper Limit Vehicle Qua... (unchecked), Threshold (20 vehicles), Time Plan (Full Time), and Snapshot (Enabled). Buttons for Back, Apply, Refresh, and Default are at the bottom.

Step 5 Set parameters.

Table 8-10 Description of parameters

Parameter		Description
Traffic Congestion	Repeat Alarm Time	When the alarm is triggered and this state lasts for repetitive alarm time, the alarm will be triggered again. 0 means repeat alarm function disabled.
	Vehicle Congestion Alarm	Enable vehicle congestion alarm to set the upper threshold and duration of vehicles in the area. When the number of vehicles exceeds the threshold and the congestion time exceeds the configured continuous congestion time, an alarm will be triggered.

Parameter		Description
Parking Upper Limit	Repeat Alarm Time	When the alarm is triggered and this state lasts for repetitive alarm time, the alarm will be triggered again.  0 means Repeat Alarm function disabled.
	Upper Limit Vehicle Quantity Alarm	Enable upper limit vehicle quantity alarm to set the upper threshold and duration of vehicles in the area. When the number of vehicles exceeds the threshold and the congestion time exceeds the configured continuous congestion time, an alarm will be triggered. The upper threshold of vehicles that trigger an alarm is 20 vehicles by default.

Step 6 Select time plan and click + **Event Linkage**.

- If the added time plan cannot meet your requirements, click **Add Schedule** to add an arming schedule. For details, see "6.4.1.2.1 Adding Schedule".
- Click **Event Linkage** to add linked event and set linkage parameters. For details, see "6.4.1.2 Alarm Linkage".

Step 7 Click **Apply**.

8.6 Setting Parking Space

This section introduces rule configuration and global configuration for parking space.

8.6.1 Rule Configuration

Set planned or open type for parking space.

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

Step 2 Click next to **Parking Space**, and then click **Next**.

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

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.


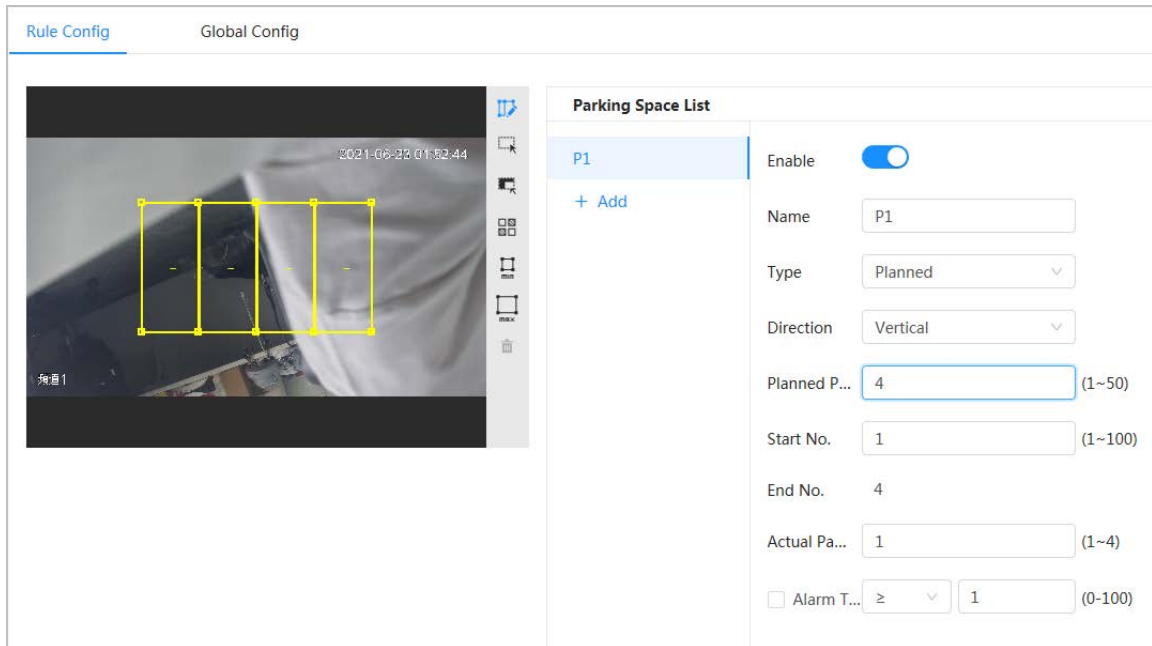
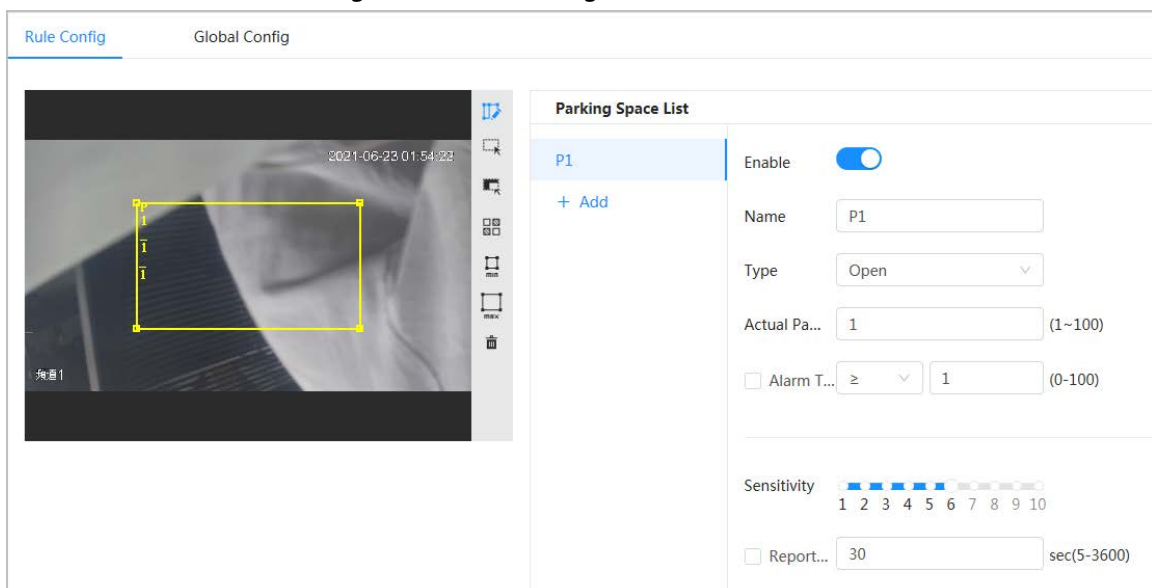
- Click  to draw the rectangle area.
 - ◇ If you select planned parking space, the rectangle area will be divided equally according to the planned parking spaces number that you configured.

Figure 8-26 Rule configuration (1)



- ◇ If you select open parking space, the rectangle area will not be divided.

Figure 8-27 Rule configuration (2)



- Click to draw a parking space detection area in the image. The detection area is the whole image by default.
- Click to draw an exclusion area for parking space 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 is 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 Select **Planned/Open** in **Type**.

- Planned Parking Space

It is used for parking management of planned parking lots (with clearly delineated parking spaces). When there is a car parked in the parking space, a red dot is drawn. And a parking space without a car is drawn a green dot.

Figure 8-28 Planned parking space

Table 8-11 Description of planned parking space parameters

Parameter	Description
Name	Enter the name of the added parking space.
Direction	You can select Vertical or Horizontal direction.
Planned Parking Space	It can be used to divide the initial quadrilateral equally, which is convenient for you to draw the rule box
Start No.	Associates with the name of parking spaces.
End No.	Associates with Planned Parking Space .
Actual Parking Space	It ranges from 1 to the configured value of planned parking space. Actual Parking Space is 1 by default.
Alarm Threshold	You can set it from 0 through 100. When alarm is triggered, the frame of related statistic area will flash red. And the threshold number is 0 by default.
Sensitivity	Adjust the false alarm and miss alarm of the system. And the sensitivity is 6 by default.
Report Period	The report period is 30 seconds by default. And you can set it between 5 to 3600 seconds. It will only upload related data but not pictures or videos.

- Open Parking Space

It is used for parking management of open parking lots in a large area. When there is a car parked in the parking space, a red dot is drawn. And a parking space without a car will not show any dot.

Figure 8-29 Open parking space parameters

Table 8-12 Description of open parking space parameters


Parameter	Description
Name	Enter the name of the added parking space.
Actual Parking Space	Actual Parking Space is 1 by default. When you change the planned parking space, the input range would change into 1 - the number of planned parking space.
Alarm Threshold	The threshold number is 0 by default. And you can set it between 0 to 100. When alarm is triggered, the frame of related statistic area will flash in red.
Sensitivity	It is designed to adjust the false alarm and miss alarm of the system. And the sensitivity is 6 by default.
Report Period	The report period is 30 seconds by default. And you can set it between 5 to 3600 seconds. It will only upload related data but not pictures or videos.

Step 6 Select time plan and click + **Event Linkage**

- If the added time plan cannot meet your requirements, click **Add Schedule** to add an arming schedule. For details, see "6.4.1.2.1 Adding Schedule".
- Click **+Event Linkage** to add linked event and set linkage parameters. For details, see "6.4.1.2 Alarm Linkage".

Step 7 Click **Apply**.

8.6.2 Global Configuration

- Step 1** (Optional) Set OSD information.
Click **OSD Info**, and the **Overlay** interface is displayed, and then enable the **Parking Space** function. The statistical result is displayed on the **Live** interface. For details, see "6.2.2.2.14 Configuring Parking Space".
- Step 2** Adjust confidence level.
- 
- Confidence level is used for algorithm adjustment of false alarm and detection.
- Step 3** Click **Apply**.

8.7 Setting Video Metadata

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

8.7.1 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 8-30 Global configuration of video metadata

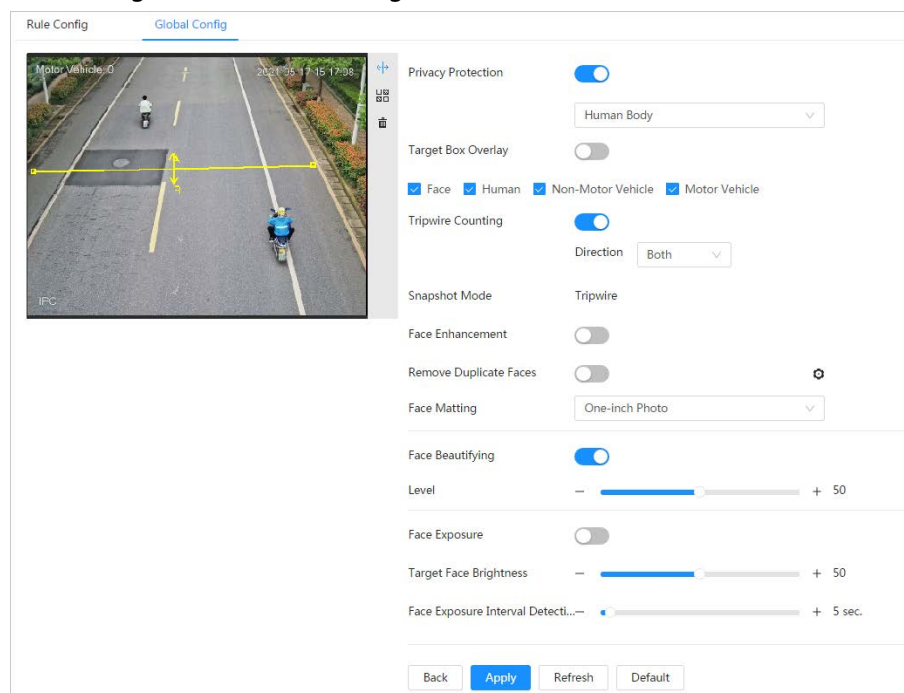





Table 8-13 Description of scene set parameters (video metadata)

Parameter	Description
Privacy Protection	Enable this function, and the faces and bodies will be blurred by mosaic or color blocks when they are detected.
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>
Tripwire Counting	<p>Enable this function, and set the tripwire direction. The snapshot mode is Tripwire by default, and you cannot change it.  will be displayed beside the image on the Rule Config interface. You can draw the rule as needed.</p>
Face Enhancement	Click  next to Face Enhancement to preferably guarantee clear face with low stream.
Remove Duplicate Faces	<p>During the configured period, the face that detected several times is displayed only once, to avoid repeated counting. Click  to set the parameters, and then click Apply.</p> <ul style="list-style-type: none"> • Time: The function is valid within the configured period. • Precision: The larger the value is, the higher the accuracy will be.
Face Matting	Set a range for matting face image, including face picture and one-inch picture.
Face Beautifying	Enable Face Beautifying to make face details clearer at night. After enabling this function, you can adjust the level. The higher the level, the higher the beautifying level.
Face Exposure	Enable Face Exposure to make face clearer by adjusting lens aperture and shutter.
Target Face Brightness	Set the face target brightness, and it is 50 by default.
Face Exposure Interval Detection Time	Set the face exposure interval detection time to prevent image flickering caused by constant adjustment of face exposure. It is 5 seconds by default.
Scene	Set scene as Distant View or Close View .

Step 5 Click **Apply**.

8.7.2 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 8-31 Rule configure (video metadata)

No.	Name	Type	On	Picture	Delete
1	VM-1	People Detection	<input checked="" type="checkbox"/>		
2	VM-2	Non-motor Vehicle Detection	<input checked="" type="checkbox"/>		
3	VM-3	Motor Vehicle Detection	<input checked="" type="checkbox"/>		

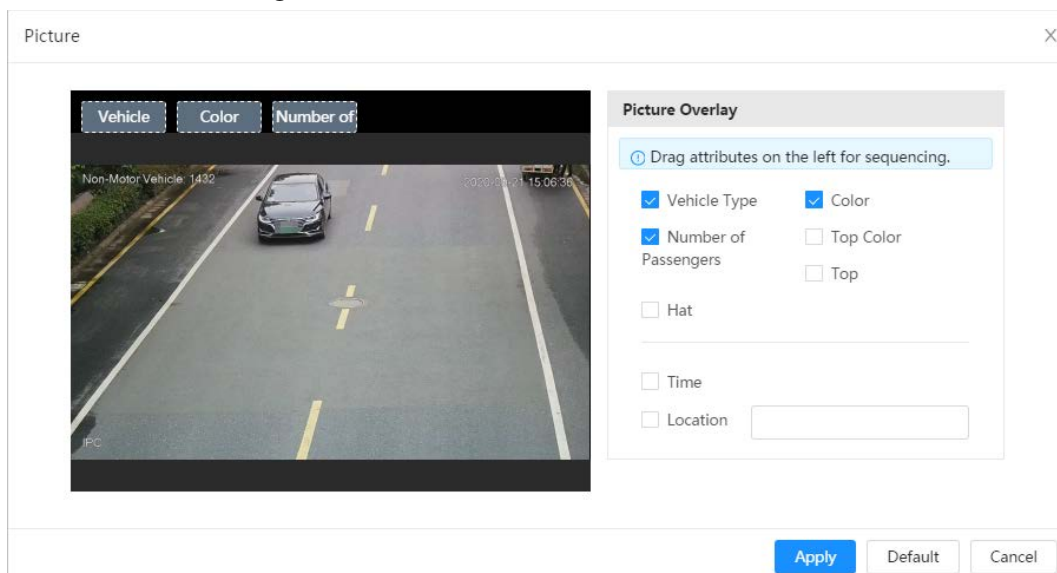
Step 5 Configure **Picture**.

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 8-32 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.

- Click to draw rule line in the image.

When targets pass the tripwire along the configured direction line, they will be counted.

- 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 is 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 8-14 Description of crowd map parameters

Parameter	Description
People Flow Statistics	Click <input type="checkbox"/> next to People Flow Statistics to count the number of people in the detection area.
Flow Statistics (Non-motor Vehicle)	Click <input type="checkbox"/> next to Flow Statistics (Non-motor Vehicle) to count the number of non-motor vehicles in the detection area.
Traffic Flow Stat	Click <input type="checkbox"/> 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 <input type="checkbox"/> 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"> 1. Select Tripwire. 2. Select the direction from A to B, B to A, and Both. 3. 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".

8.7.3 Viewing Video Metadata Report

Generate data of video metadata recognition in report form.

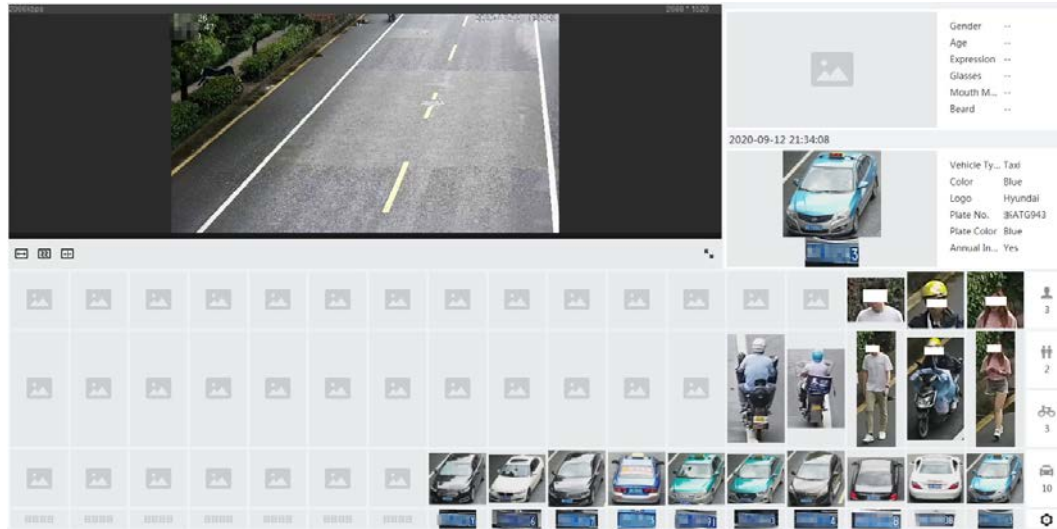
Step 1 Select **Setting > Event > Video Metadata > Report**.

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 8-33 Video metadata report



8.8 Setting People Counting

People counting (including entry number, exit number and stay number in area), queuing number, and view the people counting data in report form.

8.8.1 People Counting

The system counts the people entering and leaving the detection area. When the number of counted people exceeds the configured value, an alarm is triggered and the system performs an alarm linkage.

Background Information

There are two types of people counting rules.

- **People Counting:** The system counts the people entering and leaving the detection area. When the number of counted number of people who enter, leave, or stay in the area exceeds the configured value, an alarm is triggered, and the system performs an alarm linkage.
- **Area People Counting:** The system counts the people in the detection area and the duration that people stay in the area. When the number of counted number of people in the detection area or the stay duration exceeds the configured value, an alarm is triggered, and the system performs an alarm linkage. This function is available on some select models.

Procedure

Step 1 Select **AI > Smart Plan**

Step 2 Click next to **People Counting**, and then click **Next**.

Step 3 Click the **People Counting** tab.

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

- The added rules will be displayed in the list. Click the text box under **Name** to edit the rule name. The rule is enabled by default.
- For the models that support multiple counting rules, different detection areas can be overlapped. It supports at most 4 people counting rules and 4 area people counting



rules.

Figure 8-34 Add rule



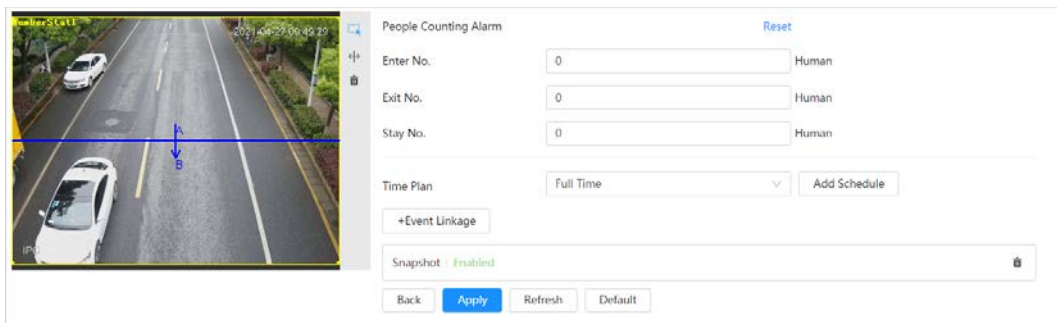
Step 5 Draw a detection area in the image.

- People counting

1. Click , and drag the any corner of the box to adjust the size of the area, and press the right mouse button and move the box to adjust the position.
2. Click  to draw rule line in the image.

When targets enter or leave the detection area along the direction line, they will be counted.

Figure 8-35 People counting (1)



- Area people counting


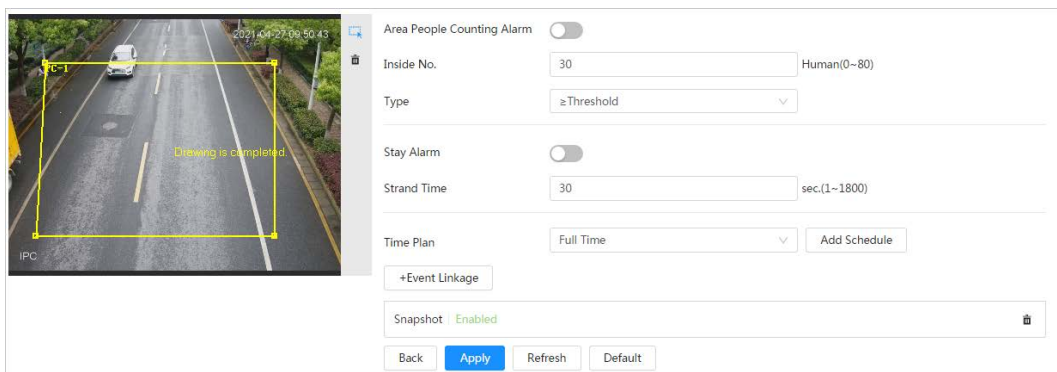
Click , and drag the any corner of the box to adjust the size of the area, and press the right mouse button and move the box to adjust the position.

Figure 8-36 People counting (2)



Step 6 Set parameters.

Table 8-15 Description of people counting parameters

Parameter	Description	
People counting	Enter No.	Counts the number of people entering in the direction A-->B. When the number exceeds the configured value, an alarm will be triggered.

Parameter	Description	
	Exit No.	Counts the number of people entering in the direction B-->A. When the number exceeds the configured value, an alarm will be triggered.
	Stay No.	It is the difference between the Enter No. and Exit No. . When the number exceeds the configured value, an alarm will be triggered.
	Clear	Clears the counted number.
Area people counting	Area people counting	Enable the area people counting function.
Inside Number	Set the number of people in the people counting region. When the people count reaches the configured value, an alarm will be triggered. When you set inside number to 0, and select \geq Threshold in Type , the system will not perform the alarm linkage.	
Type		
Stay Alarm	Select the Stay Alarm check box, and then set the stay time, when the stay duration exceeds the configured value, an alarm will be triggered.	
Strand Time		

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

You can view the counting results on the **Live** interface.

- For **People Counting** rule, the entry and exit numbers are displayed.
- For **Area People Counting** rule, the inside number is displayed.

Figure 8-37 Counting result



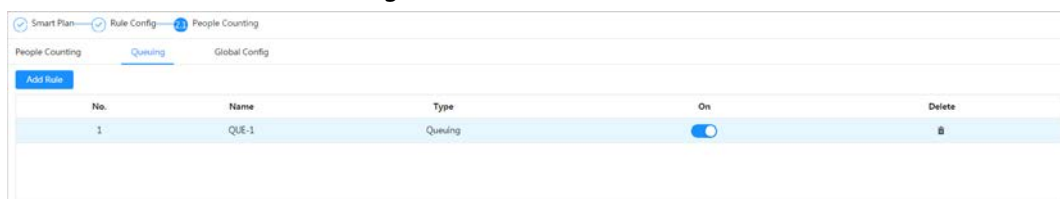
8.8.2 Queuing

The system counts the queue people in the detection area. When the queue people number exceeds the configured number or the queue time exceeds the configured time, an alarm will be triggered, and the system performs an alarm linkage.

Procedure

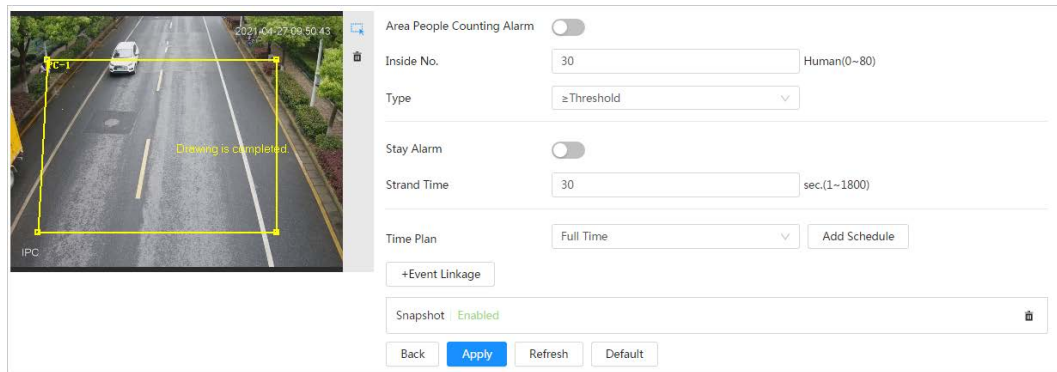
- Step 1** Select **AI > Smart Plan**
- Step 2** Click next to **People Counting**, and then click **Next**.
- Step 3** Click the **Queuing** tab.
- Step 4** Click **Add Rule > Queuing** to select rules.
- The added rules will be display in the list. Click the text box under **Name** to edit the rule name. The rule is enabled by default.
 - For the models that support multiple counting rules, different detection areas can be overlapped. It supports at most 4 queuing rules.

Figure 8-38 Add rule



- Step 5** Draw a detection area in the image.
Click to draw the detection area, and press the right mouse button to complete the drawing.

Figure 8-39 Queuing



Step 6 Set parameters.

Table 8-16 Description of queuing

Parameter	Description
Queue People No. Alarm	Enable the queue people No. alarm function.
Queue People No.	
Type	Set the queue people number for triggering the alarm and counting type. When the queue people number reaches the configured value, an alarm will be triggered.
Queue Time Alarm	Enable the queue time alarm function.
Queue Time	Set the queue time. When the queue time reaches the configured value, the alarm is triggered.

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.

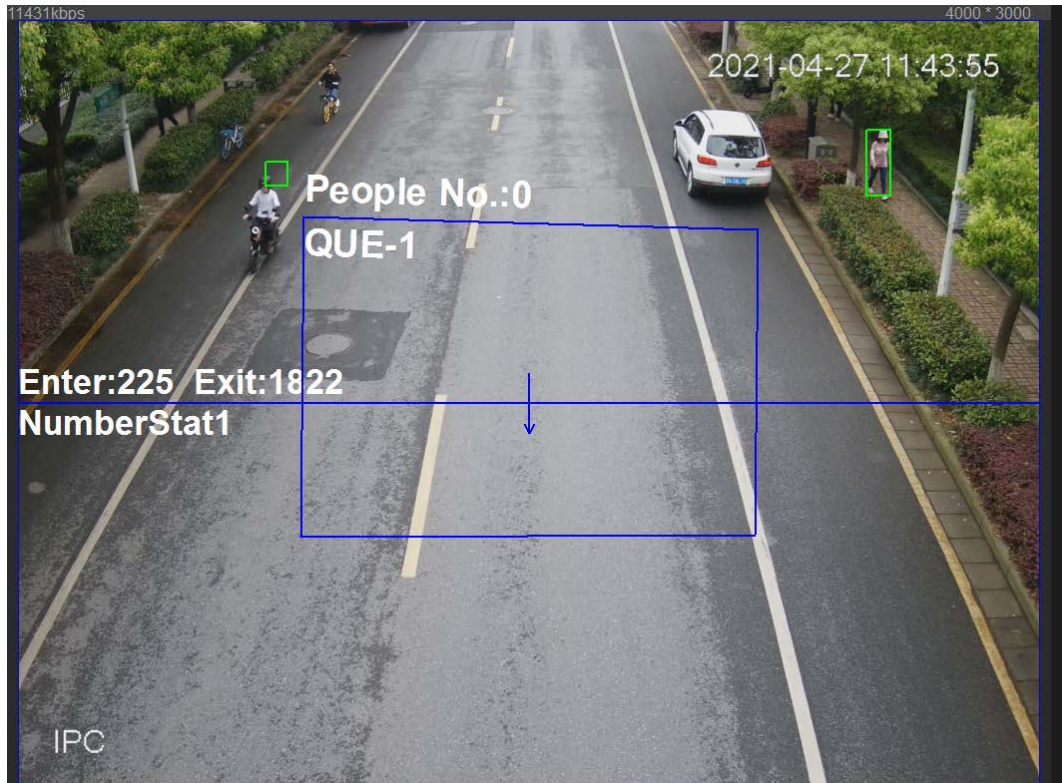
Step 8 Click **Apply**.
To view alarm information on the alarm subscription tab, you need to subscribe relevant alarm event. For details, see "6.4.1.3.2 Subscribing Alarm Information".

Result

You can view the queuing results on the **Live** interface.

The queuing number and the stay time of each target are displayed on the interface.

Figure 8-40 Queuing result



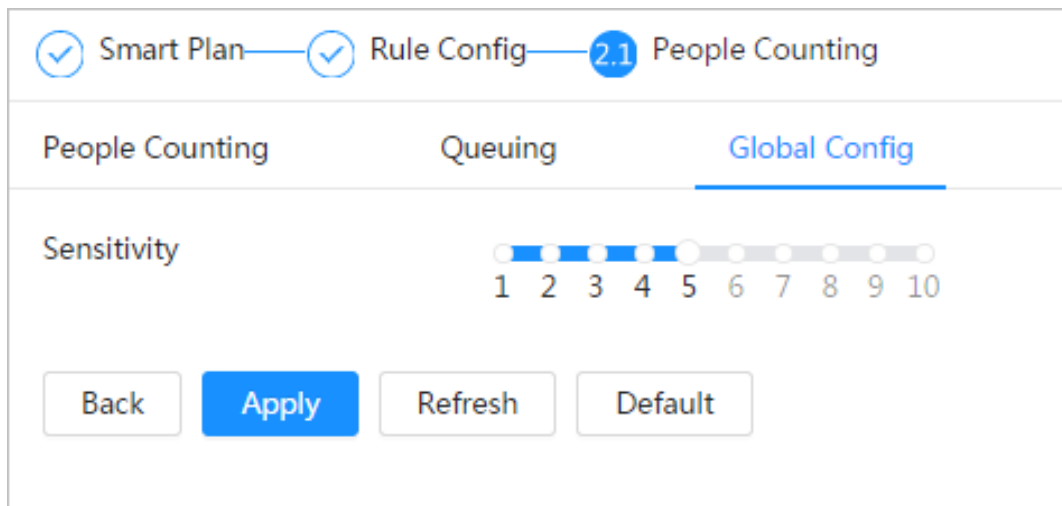
8.8.3 Global Configuration

Set the sensitivity of each people counting rule.

Procedure

- Step 1 Select **AI > Smart Plan**
- Step 2 Click next to **People Counting**, and then click **Next**.
- Step 3 Click the **Global Config** tab.
- Step 4 Set the sensitivity.
The higher the sensitivity, the easier the detection, but the more the false detections.

Figure 8-41 Global configuration



- Step 5 Click **Apply**.

8.9 Face & Body Detection

After enabling this function, the camera detects faces and human body separately, and then correlates the face and the body. When selecting compliant mode, the camera can detect attributes including face masks, helmets, glasses, safety vests, top color, and bottom color, and determine whether PPE requirements are met. PPE compliance or non-compliance alarms can be triggered according to the alarm settings.

8.9.1 Global Configuration

Set the global configuration of face & body detection, including face parameter and scene parameter.

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

Step 2 Click next to **Face & Body Detection** to enable face & body detection of the corresponding channel, and then click **Next**.

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

Step 4 Set parameters.

Figure 8-42 Global configuration of face & body detection

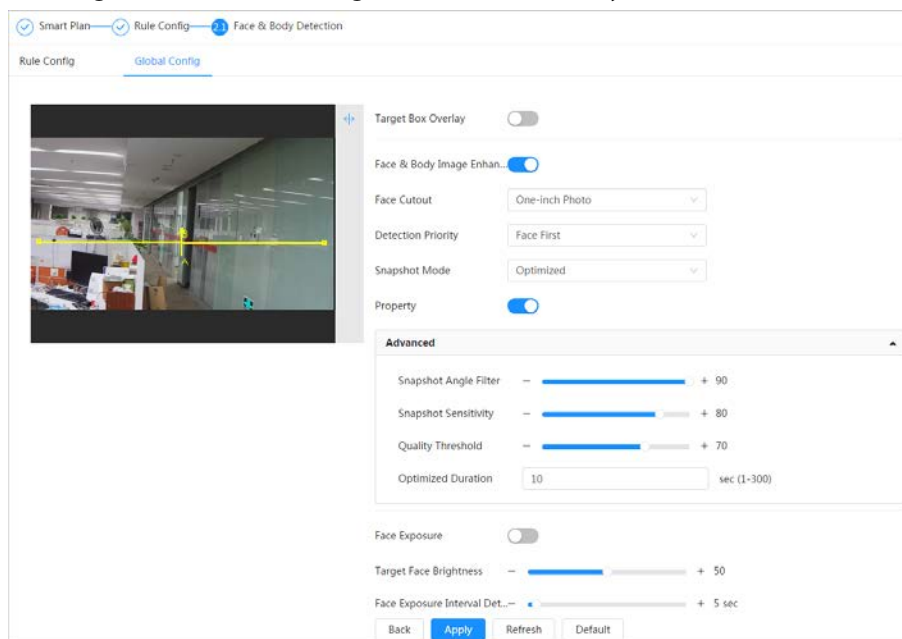



Table 8-17 Description of scene set parameters (face & body detection)

Parameter	Description
Target Box Overlay	Overlay target box on the captured pictures to mark the target position.
Face & Body Image Enhancement	Click <input type="checkbox"/> next to Face & Body Image Enhancement to preferably guarantee clear face and body with low stream.
Face Cutout	Set a range for matting face image, including face, one-inch photo, and custom.
Detection Priority	Select from Face First or Human Body First .

Parameter	Description
Snapshot Mode	<ul style="list-style-type: none"> • Real-time: Capture the image when the camera detects a face. • Optimized: Capture the clearest image within the configured time after the camera detects face. • Quality Priority: After detecting the face image quality is higher than the quality threshold, the camera captures the image. • Tripwire: This snapshot is available in PPE Detection Mode.  <p>Click Advanced to set the optimized time and quality threshold.</p>
Property	Click next to Property to enable the properties display.
Advance	<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 period to capture the clearest picture after the camera detects face.
Face Exposure	Click <input type="checkbox"/> next to Face Exposure to make face clearer by adjusting lens aperture and shutter.
Target Face Brightness	Set the face target brightness, and it is 50 by default.
Face Exposure Interval Detection Time	Set the face exposure interval detection time to prevent image flickering caused by constant adjustment of face exposure. It is 5 seconds by default.

Step 5 Click **Apply**.

8.9.2 Rule Configuration

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

Prerequisites

- Select **AI > Smart Plan**, and enable **Face & Body Detection**.
- You have configured the parameters on the **Global Config** interface.

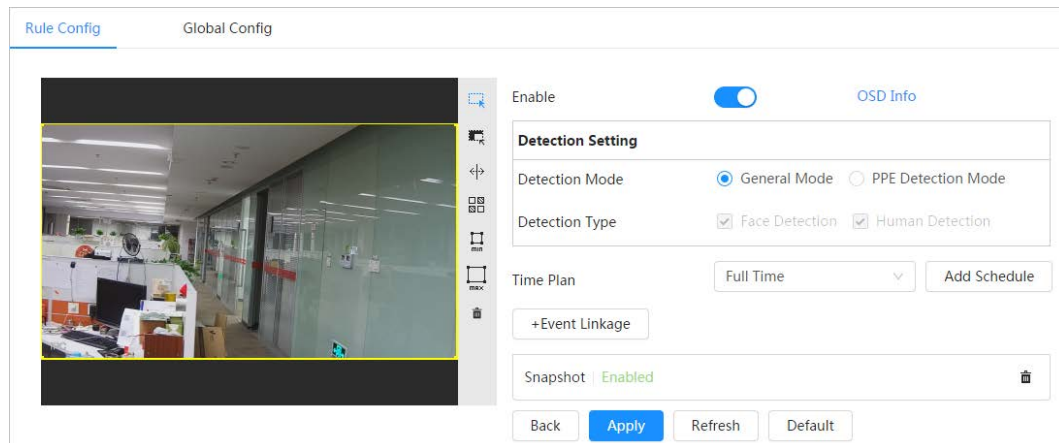
Procedure

Step 1 Select **AI > Smart Plan**

Step 2 Click next to **Face & Body Detection**, and then click **Next**.

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

Figure 8-43 Rule configuration



Step 4 Click next to **Enable** to enable the face detection function.

Step 5 (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, and right-click to finish the drawing.
- Click to draw an exclusion area for face detection in the image, and right-click to finish the drawing.
- Click to draw rule line 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 is 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 6 (Optional) Set OSD information.

Click **OSD Info**, and the **Overlay** interface is displayed, and then enable the face & body counting function. The number of detected faces and bodies is displayed on the **Live** interface. For details, see "6.2.2.2.12 Configuring Face Statistics".

Step 7 Select the detection mode.

- **General Mode** (selected by default): The system will perform an alarm linkage when the camera detects a face or a person.
- **PPE Detection Mode:**
 1. Click + next to **AI Attributes**.
 2. Select AI attributes that you want to detect.
The AI attributes include mouth mask, vest, safety helmet, glasses, top color, and bottom color. For glasses, you need to select the glass type; for safety helmet, top color, and bottom color, you need to select colors.
 3. Click **Apply** to go back to the **Rule Config** interface.
 4. Select the alarm mode.
 - ◇ **Match Attributes Alarm:** When the target's properties are compliant with the configured properties, an alarm will be triggered, and the system performs an alarm linkage.

- ◇ **Mismatch Attributes Alarm:** When the target's properties are not compliant with the configured properties, an alarm will be triggered, and the system performs an alarm linkage..

Step 8 Set arming periods and alarm linkage action. For details, see "6.4.1.2 Alarm Linkage".

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".

8.10 Setting Heat Map

Detect the distribution of dynamically moving objects in the target area within a certain period and displays the distribution on a heat map. Color varies from blue to red. The lowest heating value is in blue, and the highest heating value is in red.

Background Information

When mirroring occurs on the camera or the viewing angle changes, original data on the heat map will be cleared.

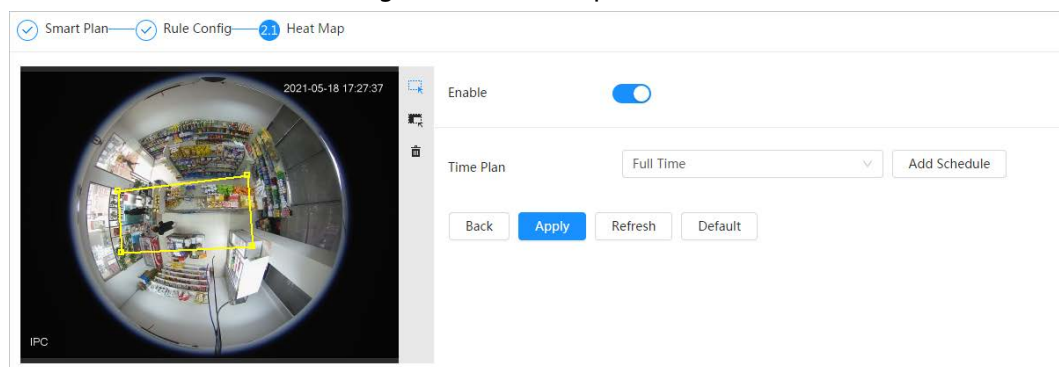
Procedure

Step 1 Select **AI > Smart Plan**

Step 2 Click next to **Heat Map**, and then click **Next**.

Step 3 Select the **Enable** check box, and then the heat map function is enabled.

Figure 8-44 Heat Map



Step 4 Draw detection area and exclusion area.

- Click to draw a detection area on the image. Right-click to finish drawing.
- Click to draw an exclusion area on the image. Right-click to finish drawing.
- Click to clear the existing detection area or exclusion area.

Step 5 Set arming periods and alarm linkage action. For details, see "6.4.1.2 Alarm Linkage".

Step 6 Click **Apply**.

8.11 Setting ANPR

When a motor vehicle triggers the rule line in the detection area, it will capture the license plate and report the attributes of the motor vehicle.

8.11.1 Lane Configuration


Configure lane configuration including detection area, lane line, detection line and lane direction.

Procedure

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

Step 2 Click next to **ANPR**, and then click **Next**.

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

Step 4 Click  and draw the detection area.

Press the left mouse button to draw the detection area, and press the right mouse button to finish.

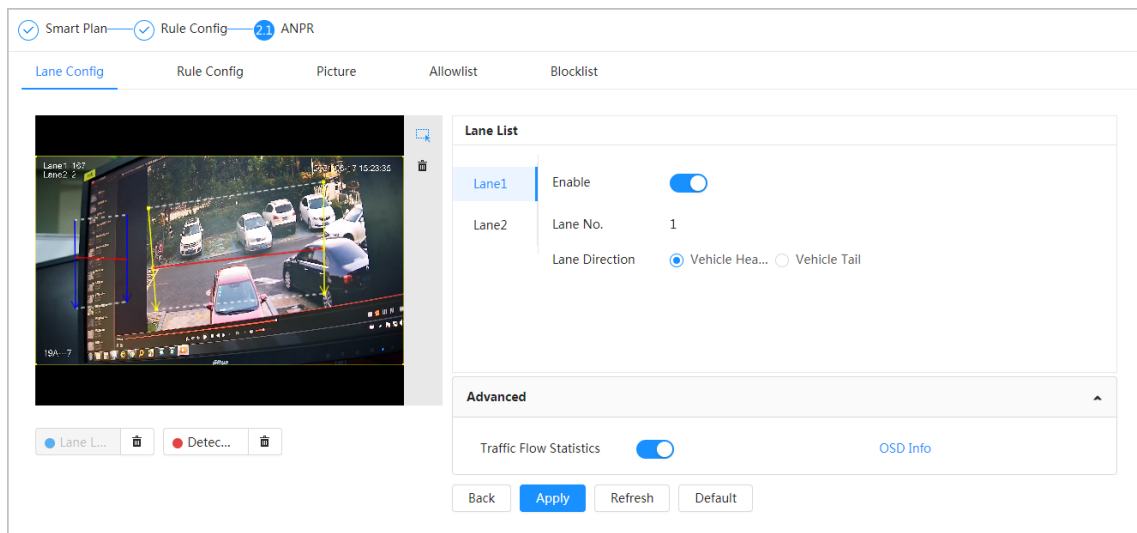
Step 5 Configure lane line information.

- One lane line is composed of two lane lines with an arrow, and the arrow represents the direction of the lane.
- The lane is enabled by default after drawing. If you do not select a lane, the track frame will be displayed on the screen, but the event of license plate recognition will not be reported.
- The lane number of each lane is unique and unchangeable.

Step 6 Select the lane direction.

- **Vehicle Head:** The driving direction of the vehicle in the lane is from top to bottom ↓ .
- **Vehicle Tail:** The driving direction of the vehicle in the lane is from bottom to top ↑ .

Figure 8-45 ANPR



Step 7 Configure detection line information.

- The detection line is displayed in red and it only available in the drawn lane line.
- When a motor vehicle triggers the detection line, a snapshot will be taken. Also the license plate and its vehicle attributes will be reported.

Step 8 (optional) You can repeat step 4-7 to draw more lane lines and detection lines. You can add two lane lines at most.

Step 9 (optional) Click **Advanced**.

- Click next to **Traffic Flow Statics**. The system only detects the number of motor vehicle and generates report after you enable this function.

- Click **OSD Info**, and the **Overlay** interface is displayed, and then enable the **Parking Space** function. The statistical result is displayed on the **Live** interface. For details, see "6.2.2.2.9 Configuring ANPR".

Step 10 Click **Apply**.

8.11.2 Rule Configuration

When a motor vehicle trigger the lane line associated , the system performs the defined alarm linkage.

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

Step 2 Click next to **ANPR**, and then click **Next**.

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

Step 4 Click lane line to select the line that you configured. If no line is configured, click **Add Lane Line**.

Figure 8-46 Rule configuration (1)

The screenshot shows a web interface for rule configuration. At the top, there is a breadcrumb trail: 'Smart Plan' (checked), 'Rule Config' (checked), and 'ANPR' (2.1). Below this is a tabbed interface with five tabs: 'Lane Config', 'Rule Config' (active), 'Picture', 'Allowlist', and 'Blocklist'. Under the 'Rule Config' tab, there is a 'Lane Line' label followed by an empty dropdown menu. In the lower right area of the interface, there is a drawing icon, the text 'Please draw lane line.', and a blue button labeled 'Add Lane Line'.

Figure 8-47 Rule configuration (2)

Time Plan

Full Time ▼

Add Schedule

+Event Linkage

Record | Enabled 🗑️

Post-Record

sec (10-300)

Snapshot | Enabled 🗑️

Alarm-out Port | Enabled 🗑️

Alarm Channel

1

2

Post-alarm

sec (10-300)

Audio Linkage | Enabled 🗑️

Play Count

(1-10)

File

You are under surveillance.wav
▼

Back

Apply

Refresh

Default

Step 5 Select time plan and click + **Event Linkage**

- If the added time plan cannot meet your requirements, click **Add Schedule** to add an arming schedule. For details, see "6.4.1.2.1 Adding Schedule".
- Click **+Event Linkage** to add linked event, which support record, send email, snapshot, alarm-out port and audio linkage.

Step 6 Set related alarm linkage.

Step 7 Set audio linkage. For more information, see "6.2.3.2 Setting Alarm Tone"

- Set play count period.
- Select the file needed.

Step 8 (optical) Click 🗑️ to delete related linkage as needed.

Step 9 Click **Apply**.

8.11.3 Picture

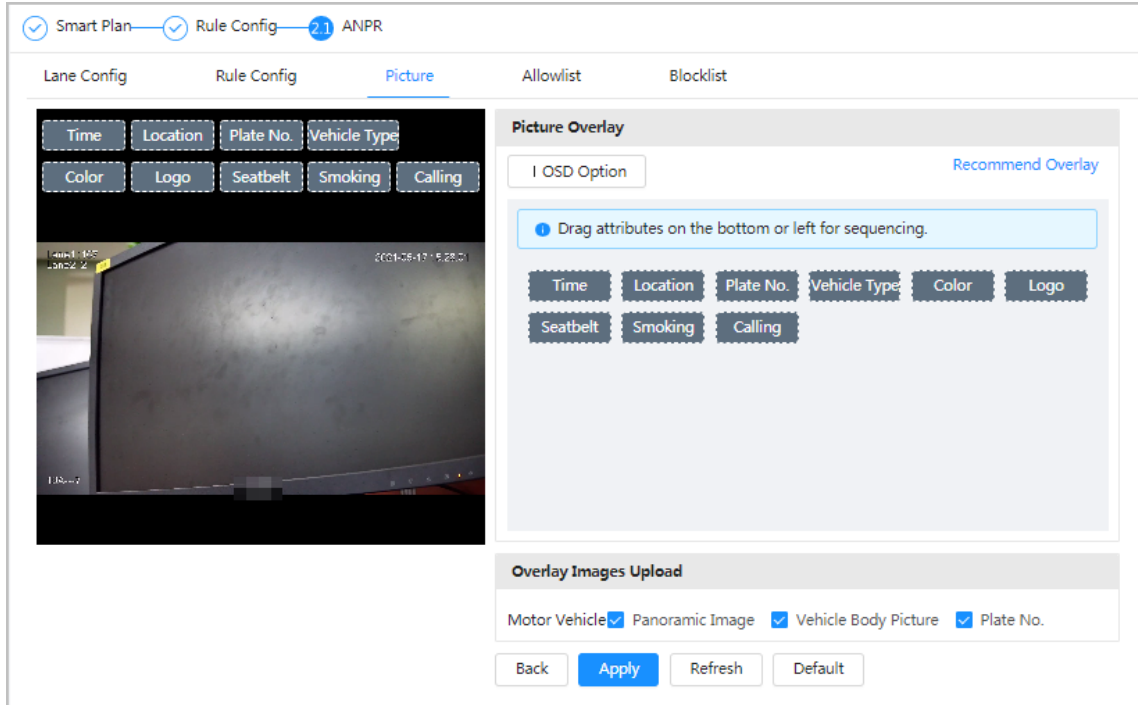
Set overlay information and image display position, such as plate number, time, vehicle type, and vehicle logo.

Procedure

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

- Step 2** Click next to **ANPR**, and then click **Next**.
- Step 3** Click the **Picture** tab.
- Step 4** Click + **OSD Option** to select the type of overlay information that needs to capture. You can adjust the position of the information displayed.

Figure 8-48 Picture



- Step 5** Select the overlay images upload type(s).
- Step 6** Click **Apply**.

8.11.4 Allowlist

After enabling allowlist, the camera will upload allowlist event and trigger linkage alarm when it detects the plate number in the allowlist.

Background Information

You can add 10,000 plate information in allowlist at most.

Procedure

- Step 1** Select **AI > Smart Plan > Allowlist**
- Step 2** Click next to **Enable** to enable the allowlist function.

Figure 8-49 Enable allowlist



- Step 3** Add allowlist.
 - Add allowlist one by one.

1. Click **Add**.
2. Set plate information.

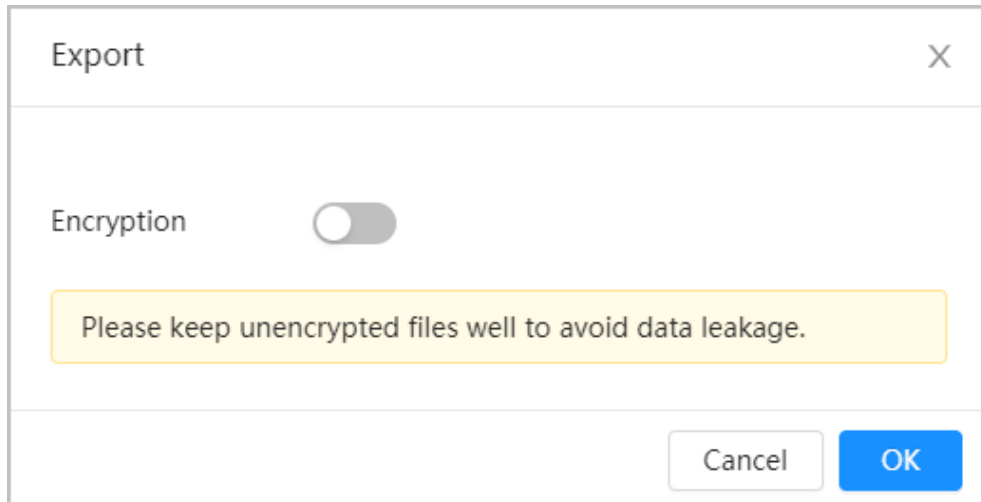
Figure 8-50 Add allowlist plate

Table 8-18 Description of parameters

Parameter	Description
Plate No.	Enter the complete plate number.
Start Time/End Time	Set the validity of allowlist for the plate number. After this time range, the vehicle will not be detected even within allowlist.
Owner Name	Enter the name of car owner.

3. Click **OK**.
 Click **Add Continuously** to add more plate number.
- Add allowlist in batches.
 1. Refer to the steps "Add allowlist one by one".
 2. Click **Export**.
 3. Do not select **Encryption** and then click **OK** to export the unencrypted allowlist file.

Figure 8-51 Encryption settings (1)



4. Add the license plate information according to the sample of the exported file, and then save the table.

Figure 8-52 Template

Start Time	End Time	Owner Name	Plate No.
2017-1-1 0:00	2037-12-5 23:59	xxx	xxx

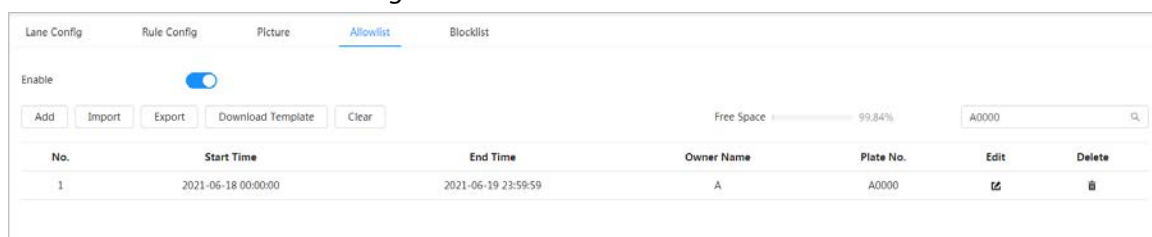
5. Click **Import** to upload allowlist table.
 - ◇ If the table is encrypted, you need to enter the password when uploading.
 - ◇ If the table is unencrypted, you can upload directly.

Related Operations

- Search plate number.

Enter the plate number in and then click . The search result is as below:

Figure 8-53 Search allowlist

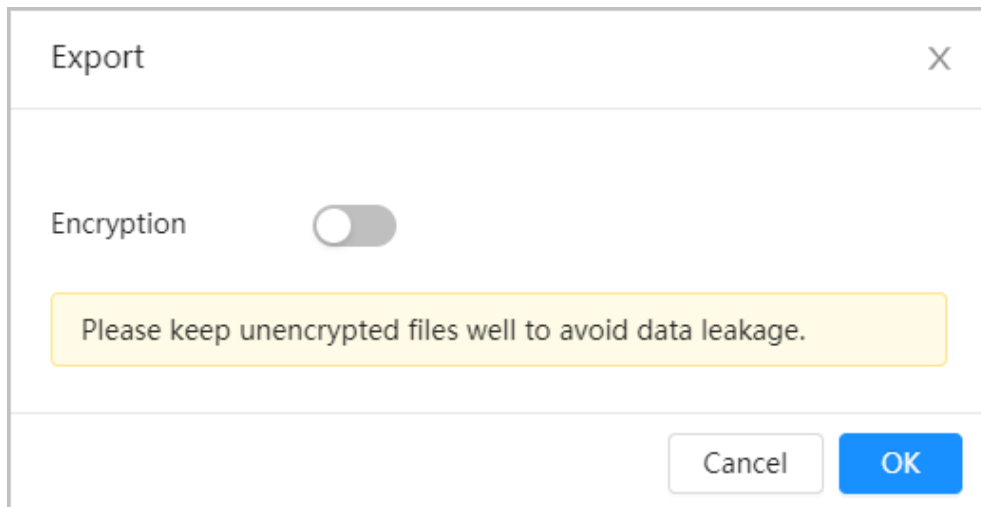


If you do not enter anything, it will show all the allowlist plate numbers added.

- Edit allowlist information.
 - Click to edit **Start Time/End Time** and **Owner Name**.
- Delete allowlist.
 - ◇ Click to delete specific allowlist number.
 - ◇ Click **Clear** to delete all allowlist number.
- Export allowlist.
 - Click **Export**. Enable encrypted or unencrypted file as needed and then export it to your PC.

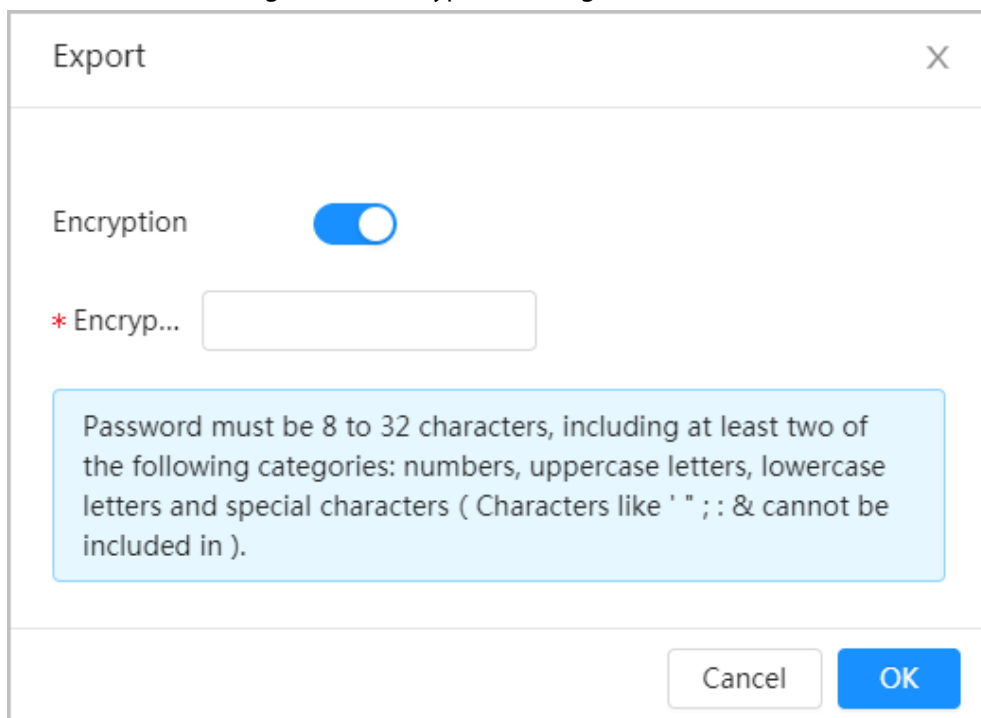
- ◇ Export the file in .csv format if not encrypted, and you can edit the file.

Figure 8-54 Encryption settings (2)



- ◇ Export the file in .backup format if encrypted, and you cannot edit the file.

Figure 8-55 Encryption settings (3)



8.11.5 Blocklist

After enabling blocklist, an alarm will be triggered when a plate number in blocklist is detected.

An alarm will be triggered when a plate number in the block list is detected.

You can add 10,000 plate information in blocklist at most.

The operation of blocklist is same as allowlist. For details, see "8.11.4 Allowlist".

9 Security

9.1 Security Status

Background Information

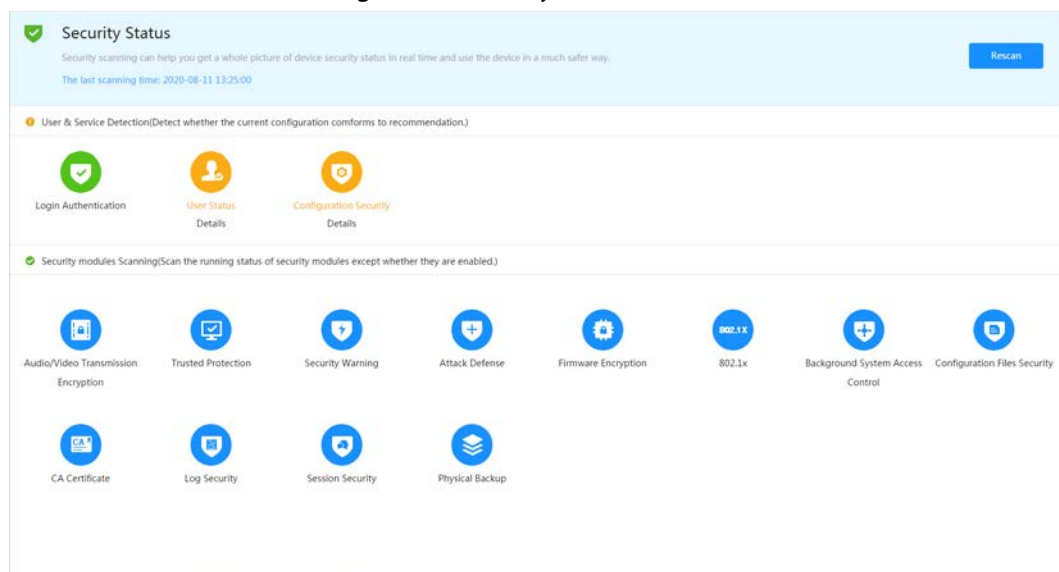
Detect the user and service, and scan the security modules to check the security status of the camera, so that when abnormality appears, you can process it timely.

- 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 9-1 Security Status

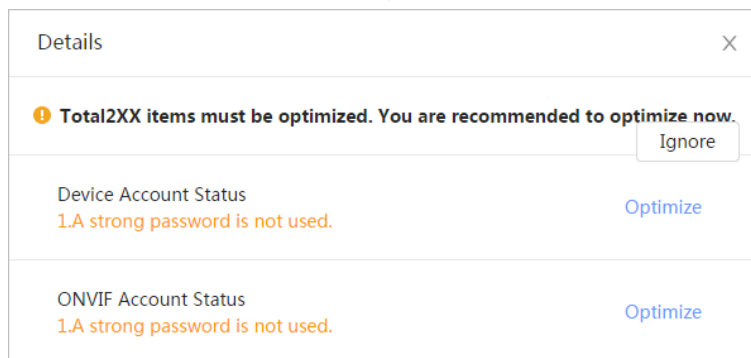


Related Operations

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

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 9-2 Security Status



9.2 System Service

9.2.1 802.1x

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.

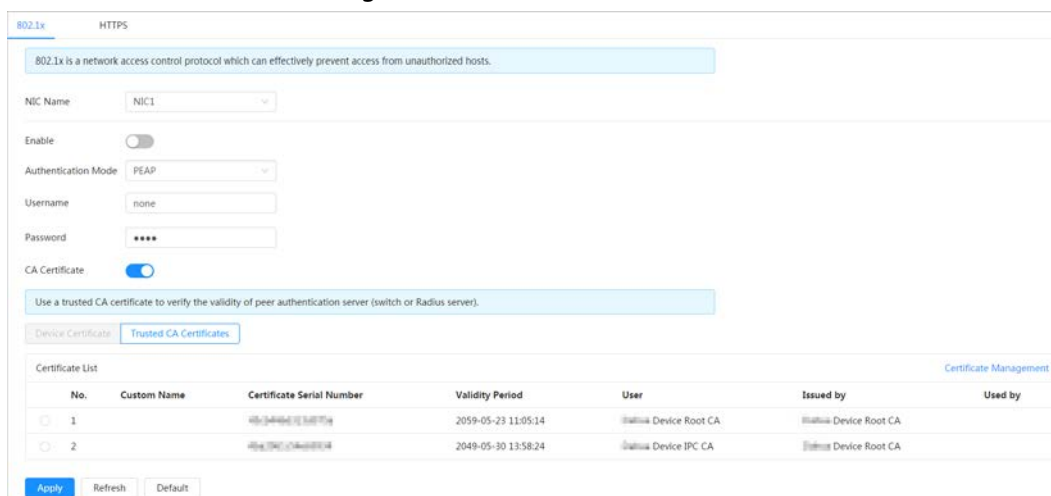
Step 3 Select the authentication mode, and then configure parameters.

- 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 "9.4.2 Installing Trusted CA Certificate".

Figure 9-3 802.1x (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.

- 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 "9.4.2 Installing Trusted CA Certificate".

Figure 9-4 802.1x (TLS)

No.	Custom Name	Certificate Serial Number	Validity Period	User	Issued by	Used by
<input checked="" type="radio"/> 1		00000000000000000000000000000000	2059-05-23 11:05:14	Dahua Device Root CA	Dahua Device Root CA	
<input type="radio"/> 2		00000000000000000000000000000000	2049-05-30 13:58:24	Dahua Device IPC CA	Dahua Device Root CA	

Step 4 Click **Apply**.

9.2.2 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 "9.4.2 Installing Trusted CA Certificate".

Figure 9-5 HTTPS

No.	Custom Name	Certificate Serial Number	Validity Period	User	Issued by	Used by
<input checked="" type="radio"/> 1		00000000000000000000000000000000	2050-07-15 15:37:32	6F03D5EYAG9E43B	Dahua Device IPC CA	HTTPS, RTSP over TLS

Step 4 Click **Apply**.

9.3 Attack Defense

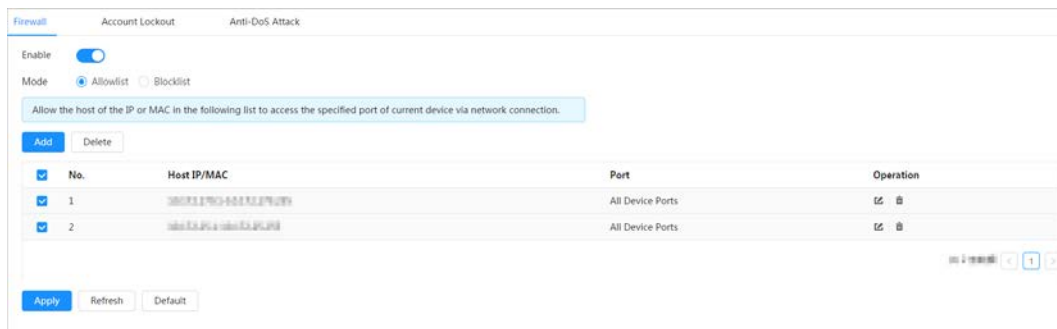
9.3.1 Firewall

Configure firewall to limit access to the camera.

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

Step 2 Click to enable the firewall function.

Figure 9-6 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 9-7 Firewall

Add ✕

Add Mode

IP Version

IP Address

All Device P...

Step 5 Click **Apply**.

Related Operations

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

9.3.2 Account Lockout

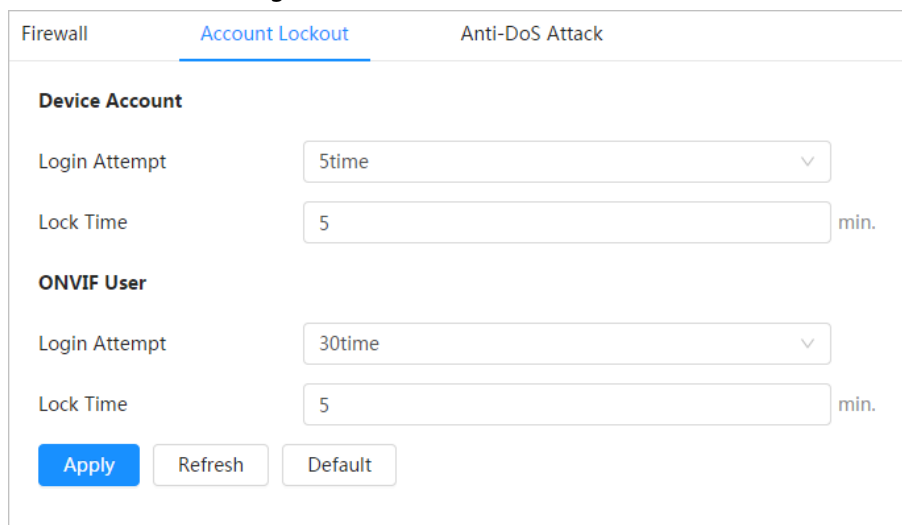
If you consecutively enter a wrong password more than the configured value, the account will be locked.

Step 1 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 9-8 Account lockout



Section	Field	Value	Unit
Device Account	Login Attempt	5time	
	Lock Time	5	min.
ONVIF User	Login Attempt	30time	
	Lock Time	5	min.

Buttons: **Apply**, Refresh, Default

Step 3 Click **Apply**.

9.3.3 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 9-9 Anti-DoS attack

Firewall
Account Lockout
Anti-DoS Attack

SYN Flood Attack Defense

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

ICMP Flood Attack Defense

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

Apply
Refresh
Default

9.4 CA Certificate

9.4.1 Installing Device Certificate

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

9.4.1.1 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 9-10 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.

9.4.1.2 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 9-11 Certificate information (2)

The screenshot shows a web form titled "Step 2: Fill in certificate information." with a close button (X) in the top right corner. The form contains the following fields and buttons:

- * IP/Domain Na...: Input field containing "111111"
- Organization Un..: Input field containing "TEST"
- Organization: Input field containing "COMPANY"
- * Validity Period...: Input field containing "200" and a label "Days (1~5000)"
- * Country: Input field with a dropdown arrow and a small flag icon
- Province: Input field
- City Name: Input field
- Buttons: "Previous", "Create and Download" (highlighted in blue), and "Cancel"

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.

9.4.1.3 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 9-12 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.

9.4.2 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 9-13 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.

9.5 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 9-14 A/V encryption

Table 9-1 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.

Area	Parameter	Description
	Certificate Management	For details about certificate management, see "9.4.1 Installing Device Certificate".

Step 3 Click **Apply**.

9.6 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 9-15 Security warning

The screenshot displays the 'Security Warning' configuration page. At the top, there is an 'Enable' toggle switch. Below it is the 'Event Monitoring' section, which lists four security events: 'Invalid executable programs attempting to run', 'Web Path Brute Force Attack', 'Session ID Brute Force Attack', and 'Session connection number exceeds limit.' A blue informational box states: 'Security warning can detect device security status in real time, and keep you informed of the security exception events immediately, so that you can deal with them timely and avoid security risks.' Below this is a '+ Event Linkage' button. The 'Enable Alarm' toggle is set to 'Enabled'. The 'Alarm-out Port' is set to '1' and the 'Post-Alarm' is set to '10' seconds. At the bottom, there are 'Apply', 'Refresh', and 'Default' buttons.

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**.

10 Record

This section introduces the functions and operations of video playback.

10.1 Playback

10.1.1 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 "10.2 Setting Record Control", "10.3 Setting Record Plan", and "10.4 Storage".

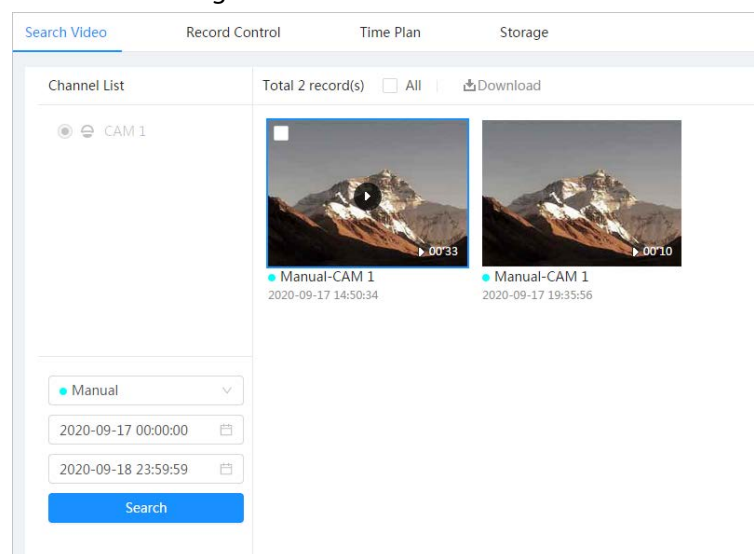
Procedure

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 10-1 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 10-2 Video playback

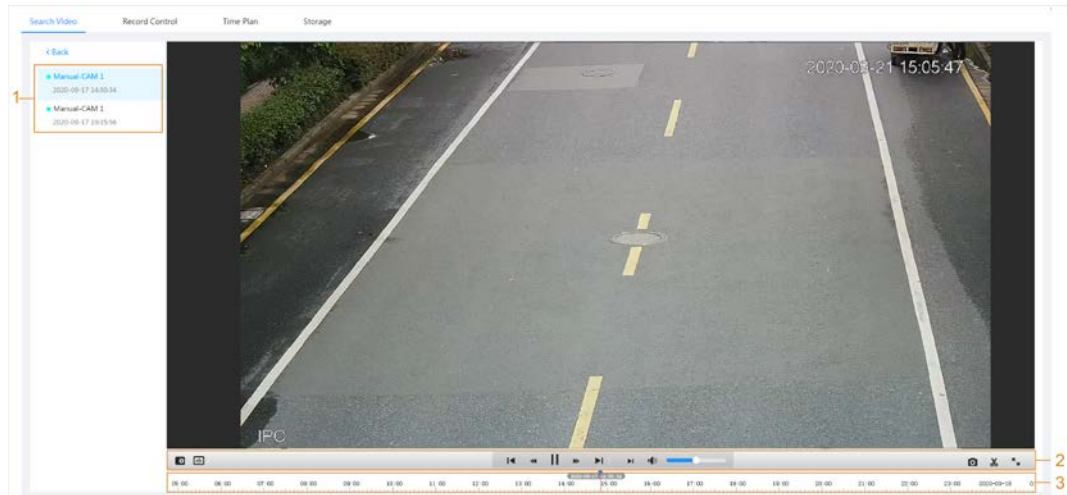





Table 10-1 Description of video playback interface

No	Function	Description
1	Recorded video list	<p>Displays all searched recorded video files. Click any files to play back it.</p> <p>Click Back at the upper-left corner to go to the Search Video interface.</p>
2	Digital Zoom	<p>You can zoom video image of the selected area through two operations.</p> <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	<p>Click , and then select Enable to display AI rules and detection box; select Disable to stop the display. It is enabled by default.</p> <p></p> <p>AI rules is valid only when you enabled the rule during recording.</p>

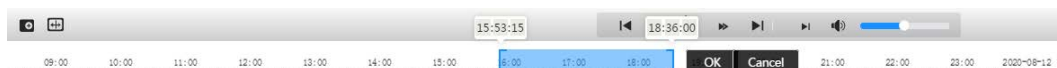
No	Function	Description
	Play control bar	Controls playback. <ul style="list-style-type: none"> ◀: Click the icon to play back the previous recorded video in the recorded video list. ⏪: Click the icon to slow down the playback. ⏸: Click the icon to stop playing back recorded videos. The icon changes to ▶, click the icon to play back recorded videos. ⏩: Click the icon to speed up the playback. ▶: Click the icon to play back the next recorded video in the recorded video list. ▶: Click the icon to play the next frame.
	Sound	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 "10.1.2 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

10.1.2 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

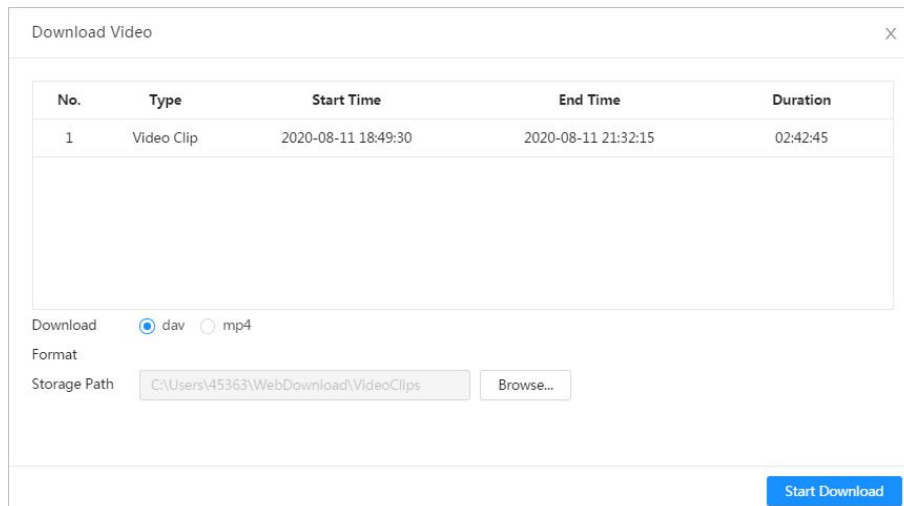
Figure 10-3 Clipping video



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

Step 4 Select the download format and storage path.

Figure 10-4 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".

10.1.3 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.
- For details of viewing or setting storage path, see "6.1 Local".

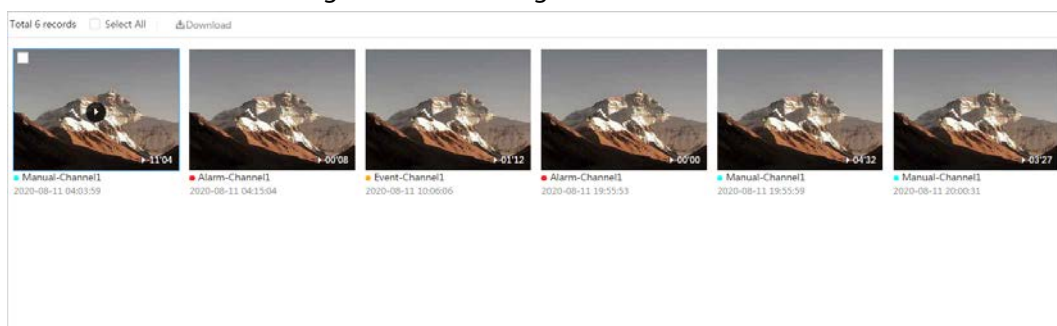
Step 1 Select **Record** > **Search Video**.

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 10-5 Selecting video file



Step 4 Click **Download**.

Step 5 Select the download format and storage path.

Figure 10-6 Downloading video

No.	Type	Start Time	End Time	Duration	Size
1	Manual	2020-08-11 04:03:59	2020-08-11 04:15:03	00:11:04	277.8M
2	Event	2020-08-11 04:15:04	2020-08-11 04:15:12	00:00:08	0.6M
3	Event	2020-08-11 10:06:06	2020-08-11 10:07:18	00:01:12	4.6M
4	Event	2020-08-11 19:55:53	2020-08-11 19:55:53	00:00:00	0M
5	Manual	2020-08-11 19:55:59	2020-08-11 20:00:31	00:04:32	102M
6	Manual	2020-08-11 20:00:31	2020-08-11 20:03:58	00:03:27	86.6M

Size 471.8M

Download dav mp4

Format

Storage Path

Step 6 Click **Start Download**.

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

10.2 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 10-7 Record control

Channel

Max Duration min.(1-120)

Pre-Record sec.(0-5)


Record Mode Auto Manual Off

Record Stream

Step 2 Set parameters.

Table 10-2 Description of record control parameters

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

Parameter	Description
Pre-Record	<p>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.</p>  <p>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.</p>
Record Mode	When you select Manual , the system starts recording; when you select Auto , the system starts recording in the configured period of record plan.
Record Stream	Select record stream, including Main Stream and Sub Stream .

Step 3 Click **Apply**.

10.3 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 10-8 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 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 periods per day.

Step 3 Click **Apply**.

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

Figure 10-9 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**.

10.4 Storage


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

Step 1 Select **Record > Storage**.

Figure 10-10 Live

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

Table 10-3 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.  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**.

10.4.1 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 10-11 Local storage

Step 4 Click **Apply**.

10.4.2 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.

10.4.2.1 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 10-12 FTP

The screenshot shows the FTP configuration interface with the following settings:

- Event Type**: Scheduled, Motion, Alarm
- Disk Full**: Overwrite, Stop
- Storage Method**: Network Storage (dropdown)
- FTP**: FTP (dropdown)
- FTP**: FTP (dropdown)
- Enable**:
- Warning**: FTP may be at risk. Continue?
- Server IP**: [Redacted]
- Port**: 22 (0~65535)
- Username**: 1
- Password**: [Redacted]
- Storage Path**: share
- Directory Structure**: Use Level 3 Directory (dropdown)
- Level 1 Directory**: Device Name (dropdown)
- Level 2 Directory**: Date (dropdown)
- Level 3 Directory**: File Type_Channel Number (dropdown)
- Urgently store to local**:
- Buttons**: Test, Apply, Refresh, Default

Step 5 Configure FTP parameters.

Table 10-4 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 <input type="checkbox"/> , 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.

10.4.2.2 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**.

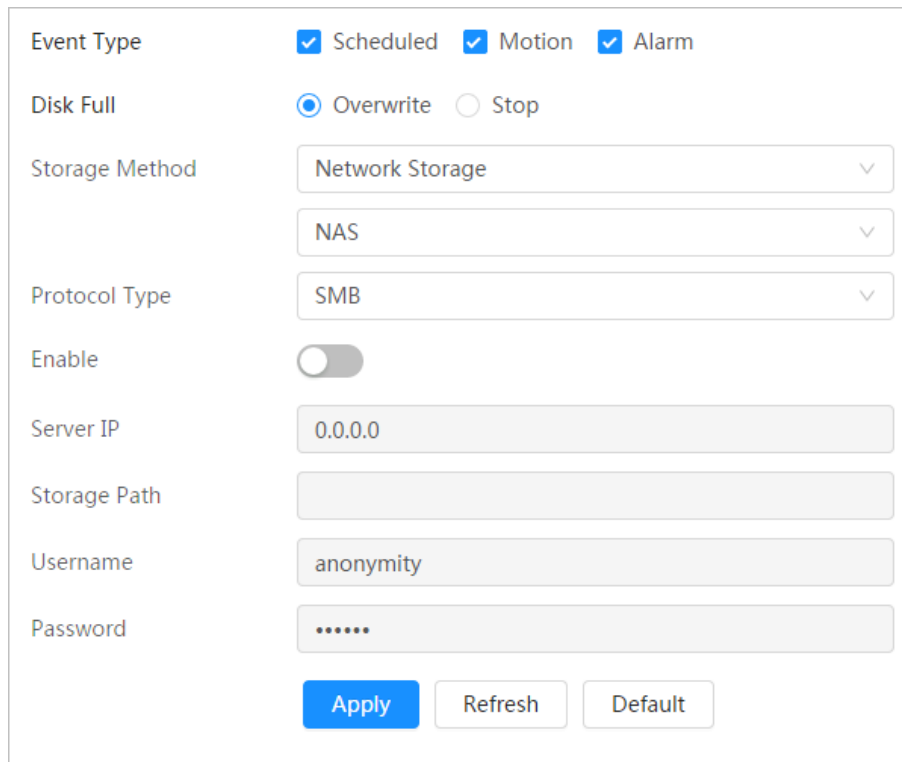
- **Overwrite**: Cyclically overwrite the earliest video when the disk is full.
- **Stop**: Stop recording when the disk is full.

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 10-13 FTP



The screenshot shows the FTP configuration interface with the following settings:

- Event Type:** Scheduled Motion Alarm
- Disk Full:** Overwrite Stop
- Storage Method:** Network Storage
- Protocol Type:** SMB
- Enable:** (disabled)
- Server IP:** 0.0.0.0
- Storage Path:** (empty)
- Username:** anonymity
- Password:** (masked with dots)

Buttons at the bottom: **Apply** (blue), **Refresh** (grey), **Default** (grey).

Step 5 Configure NAS parameters.

Table 10-5 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**.

11 Picture

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

11.1 Playback

11.1.1 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 "1.3 Setting Snapshot Plan".

Procedure

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

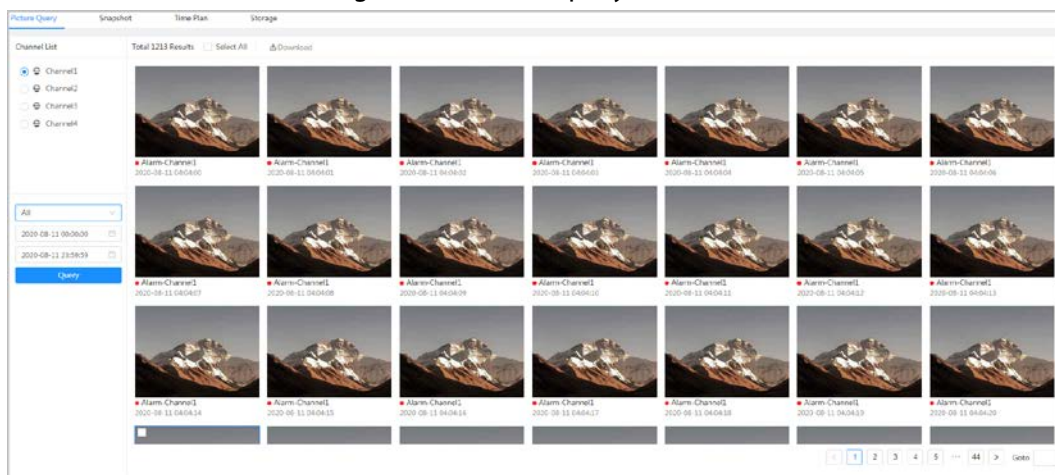
Step 2 Select the channel, the snapshot type, and snapshot time, and then click **Search**.

- 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 11-1 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 11-2 Picture playback



Table 11-1 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.

11.1.2 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.
- 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.



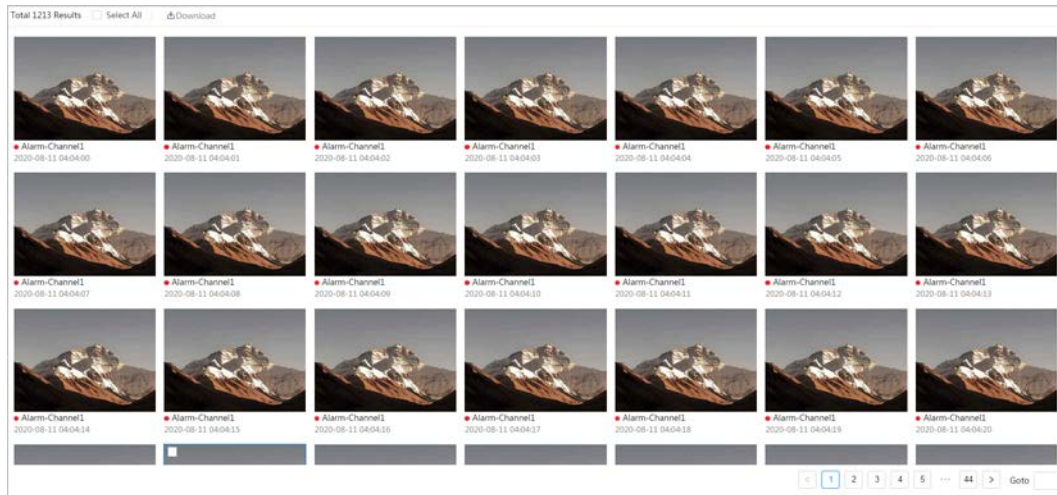
- Select  at the upper-right corner of each picture file to select one or multiple pictures.
- Select  next to **Select All** to select all searched pictures.

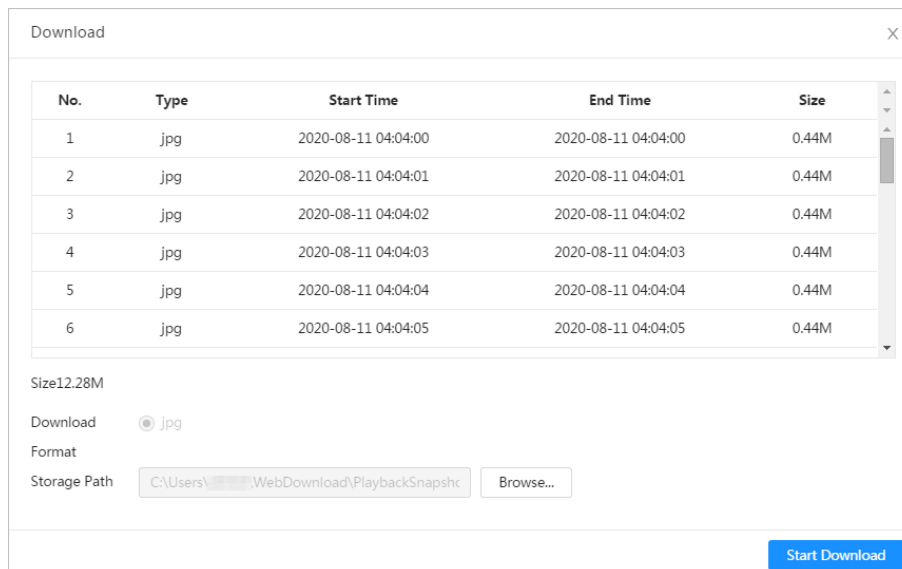
Figure 11-3 Selecting picture file



Step 4 Click **Download**.

Step 5 Select the download format and storage path.

Figure 11-4 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".

11.2 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 11-5 Snapshot

Table 11-2 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. • 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**.

11.3 Setting Snapshot Plan

According to the configured snapshot plan, the system enables or disables snapshot at corresponding time. For detailed operation, see "10.3 Setting Record Plan".

11.4 Storage

Set the storage method for the snapshot. For detailed operation, see "10.4 Storage".

11.5 Setting Upload Method

Automatically upload images to the defined server through HTTP protocol, and configure parameters.

Background Information

You do not need to set upload period. When an alarm is triggered, images will be automatically uploaded to the defined server.

Procedure

- Step 1** On the web interface, select **Picture > Auto Upload**.
- Step 2** Enable the function.
- Step 3** Click **Add**, and then configure parameters of HTTP upload method.
You can add two server information at most.

Figure 11-6 Image Upload

No.	IP/Domain Name	Port	Path	Event Type	Test	Delete
1	Example : 172.16.1.1	Example : 80	Example : /example/	None	Test	
2	Example : 172.16.1.1	Example : 80	Example : /example/	None	Test	

Table 11-3 Description of HTTP mode Parameter

Parameter	Description
IP/Domain name	The IP address and port number of the server which the report will be uploaded to.
Port	
Path	The storage path of the server for the report.
Event type	Select the event type form the drop-down list. You can select more than one types at the same time. The event types in the drop-down list are the same with that of picture playback.
Test	Test the network connection between the camera and the server.

- Step 4** Click **Apply**.

12 Report

12.1 Viewing Report

View the statistics results of AI functions in report form.

Figure 12-1 Report

- The period for the report is the latest 24 hours by default.
- Click to customize the period for the report.
- Click **Today**, **This Week**, **This Month**, or **This Year**. The start time of the period is 0 o'clock of the first day, and the end time is the current time.

12.1.1 Face Recognition

View the statistics result of face recognition in report form.

Procedure

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

Step 2 Set the period for the report.



For multi-channel camera, select the channel first.

Step 3 Select the gender and age.

Step 4 Click **Search**.

Figure 12-2 Face Recognition report



Related Operations

- Select the report form
Click to display the report in line chart; click to display the report in bar chart.
- Select the statistics type on the upper-right corner.
The statistics result of unselected types will not be displayed.
- Export reports
Select the file format, and then click **Export**.
 - ◇ Select **png**: Displays the report in picture format.
 - ◇ Select **csv**: Displays the report in list format.

12.1.2 Video Metadata

View the statistics result of video metadata in report form.

Procedure

- Step 1 Select **Report > Report > Video Metadata**.
- Step 2 Set the period for the report.

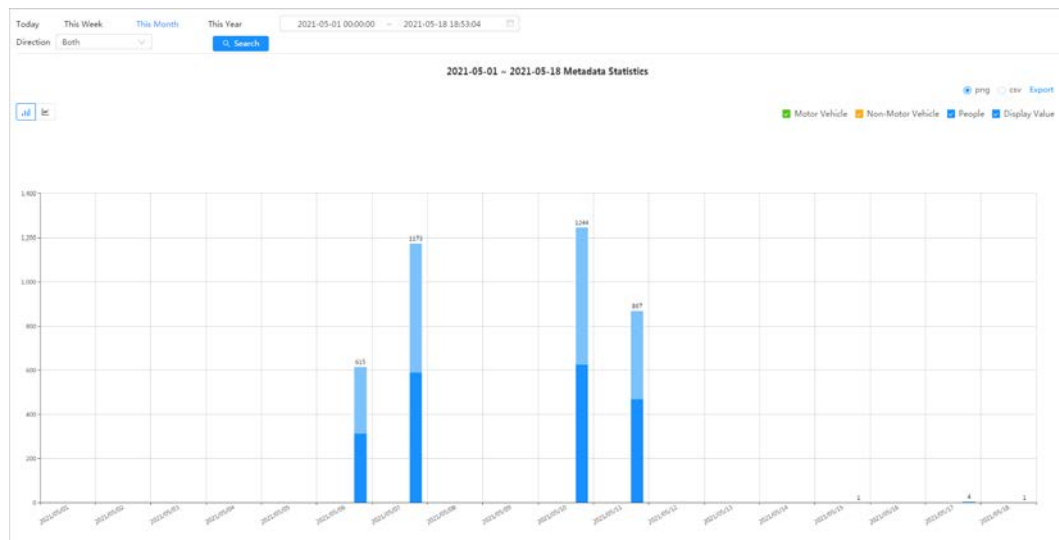


For multi-channel camera, select the channel first.

Step 3 Select the tripwire direction.

Step 4 Click **Search**.

Figure 12-3 Video metadata report



Related Operations

- Select the report form
Click to display the report in line chart; click to display the report in bar chart.
- Select the statistics type on the upper-right corner
The statistics result of unselected types will not be displayed.
- Export reports
Select the file format, and then click **Export**.
 - ◇ Select **png**: Displays the report in picture format.
 - ◇ Select **csv**: Displays the report in list format.

12.1.3 People Counting

Search for the counting results with different rules and counting methods.

Prerequisites

Make sure that you have configured the rule before searching for the report.

Procedure

Step 1 Select **Report > Report > People Counting**.

Step 2 Set search conditions.



For multi-channel camera, select the channel first.

Table 12-1 Set search conditions

Parameter	Description
Rule	Select the rule as needed, and then you need to select the statistics type according to the select rule.
Statistics Type	<p>The statistics type of the people counting report.</p> <ul style="list-style-type: none"> • People No.: Displays the report of the number of people that meet the configured condition. • Strand Time: Displays the report of the average stranding time in the detection area during a certain period. It is available when the rule of Area People Counting is selected.
Stay Time	<p>When selecting rule to Area People Counting, and statistics type to People No., you need to configure this parameter.</p> <p>The report displays the number of people whose stay time < the stay time threshold and ≥ the stay time threshold</p>
Queue Time	<p>When selecting rule to Queuing, and statistics type to People No., you need to configure this parameter.</p> <p>The report displays the number of people whose stay time < Queuing Time and ≥ Queuing Time.</p>
Period for the report	<p>Set the period for the report.</p> <ul style="list-style-type: none"> • When selecting rule to People Counting, you can view the daily, weekly, monthly and yearly report, and you can also customize the period. • When selecting rule to Area People Counting or Queuing, you can view the daily, weekly, and monthly report, and you can also customize the period.
Report	Select the rule name of the report that you want to search. You can select multiple rule names at the same time.

Step 3 Click **Search**.

Figure 12-4 People counting

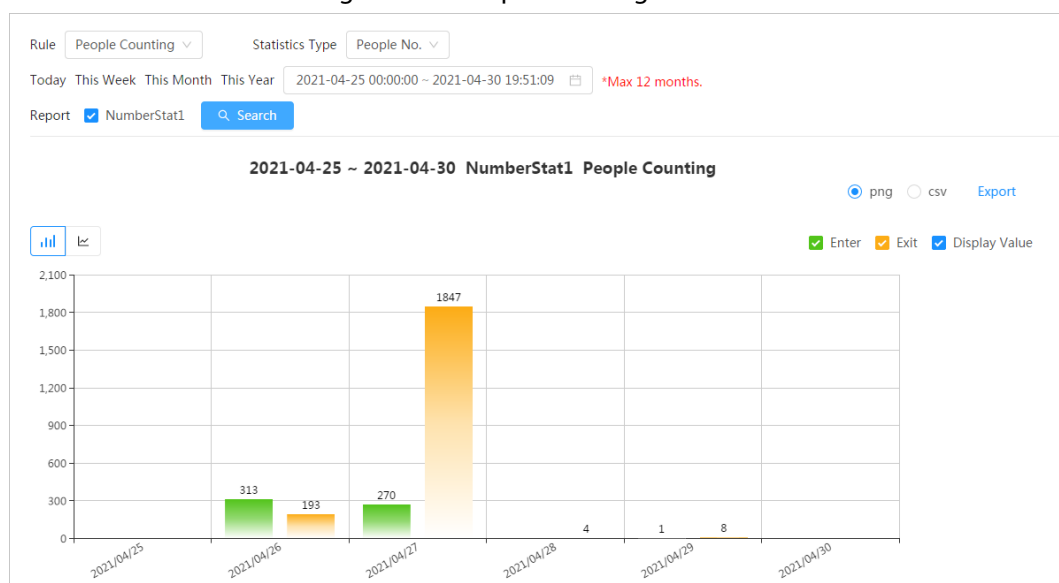


Figure 12-5 Area People Counting (number of people)

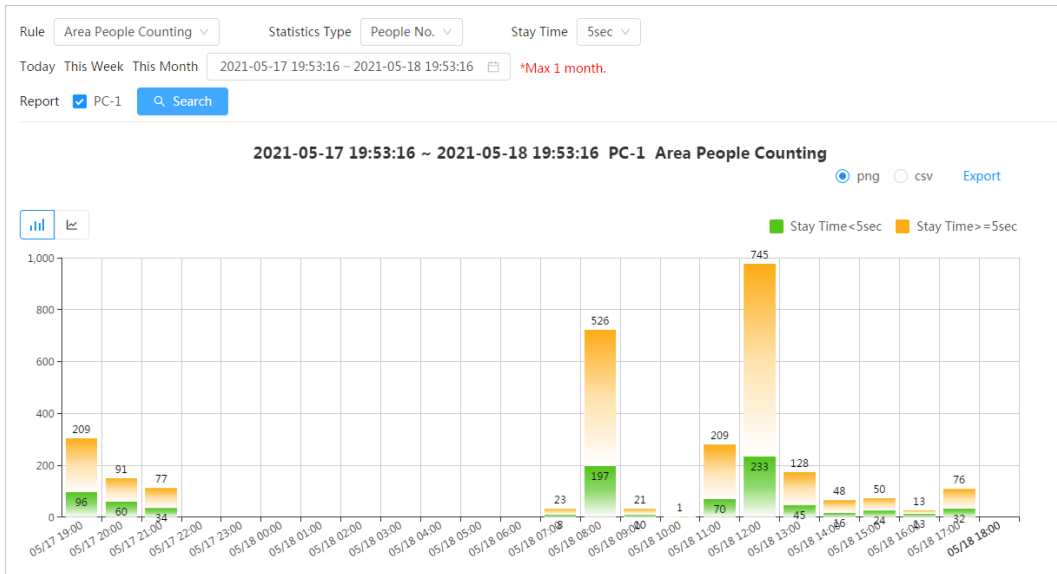


Figure 12-6 Region People Counting (stay time)

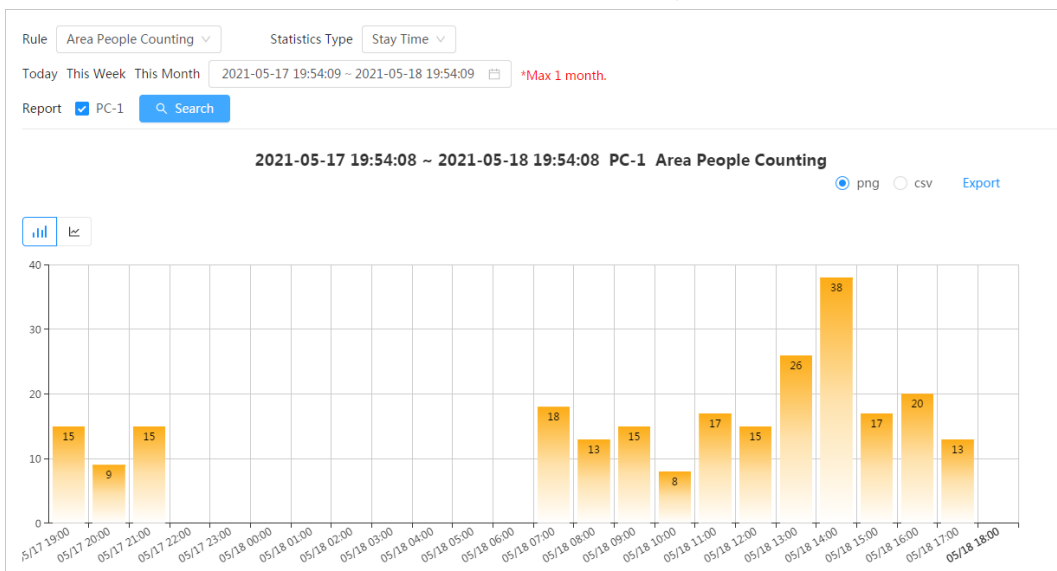
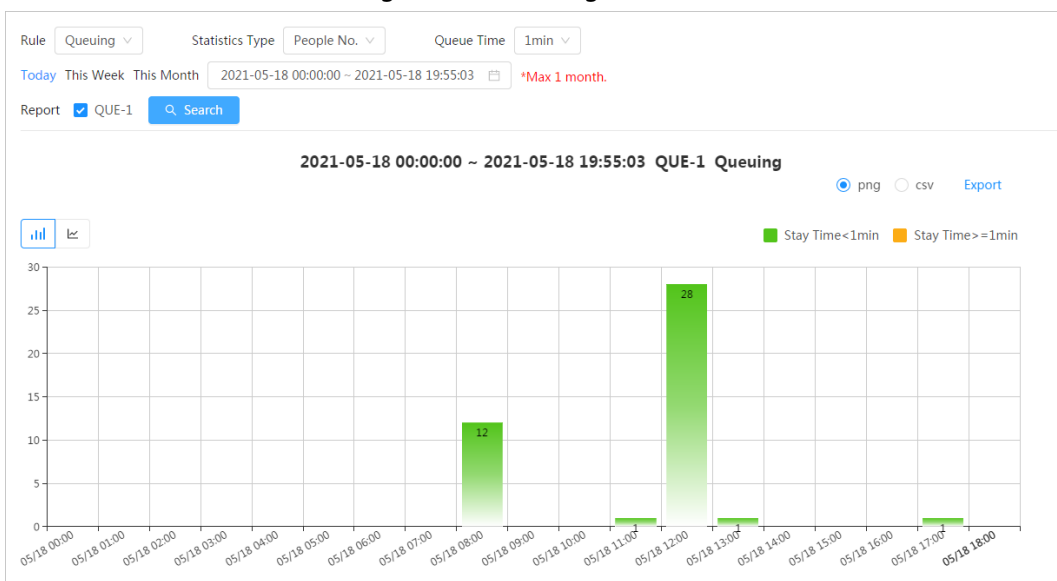


Figure 12-7 Queuing



Related Operations

- Select the report form
Click to display the report in line chart; click to display the report in bar chart.
- Select the statistics type on the upper-right corner
The statistics result of unselected types will not be displayed.
- Export reports
Select the file format, and then click **Export**.
 - ◇ Select **png**: Displays the report in picture format.
 - ◇ Select **csv**: Displays the report in list format.

12.1.4 Crowd Distribution

You can search for the number of people at a certain moment and get daily/weekly/monthly reports.

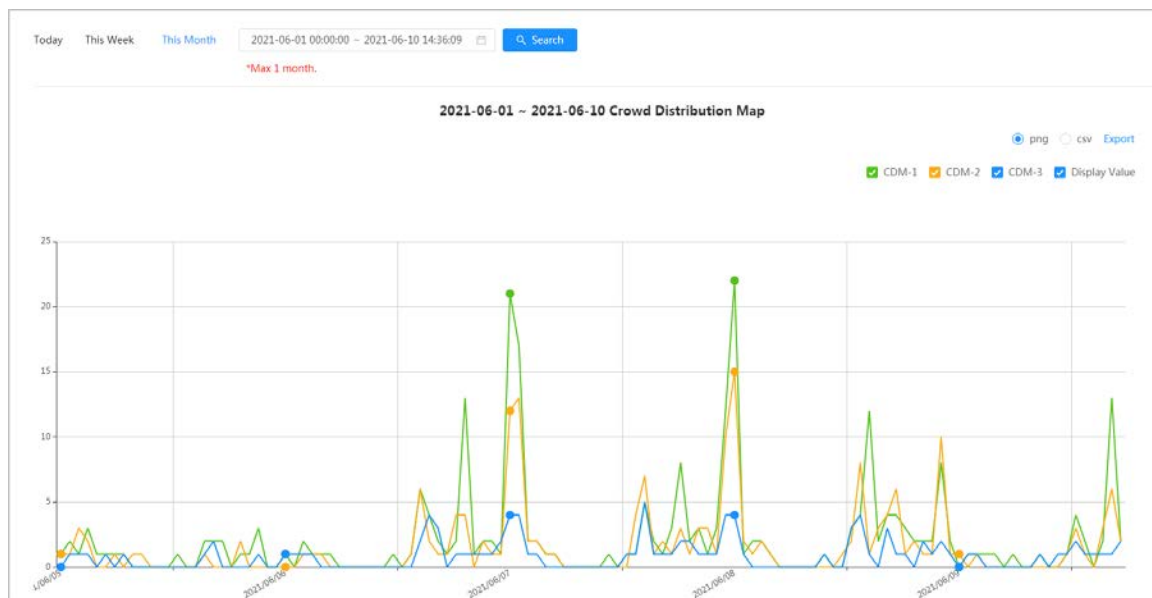
Prerequisites

Confirm that crowd distribution map function has already set; otherwise the corresponding report cannot be searched.

Procedure

- Step 1 Select **Report > Report > Crowd Distribution Map**.
- Step 2 Select the period for report statistics. You can view daily reports, weekly reports and monthly reports, or customize the period.
- Step 3 Click **Search**.

Figure 12-8 Crowd distribution map



Related Operations

- Select statistics type
Click CDM-1 CDM-2 CDM-3 Display Value and select the type needed.
- Export statistic report
Select the exact format and click **Export**, the report will be saved to the storage path of your browser.

- ◇ Select **png**: Displays the report in picture format.
- ◇ Select **csv**: Displays the report in list format.

12.1.5 Vehicle Density

Search for the number of cars at a certain moment in each statistical area.

Procedure

- Step 1 Select **Report > Report > Vehicle Density**.
- Step 2 Select the period for report statistics. You can view daily reports, weekly reports and monthly reports, or customize the period.
- Step 3 Click **Search**.

Figure 12-9 Vehicle density map



Related Operations

- Select statistics type
Click VD-1 VD-2 Display Value to select the type as needed.
- Export statistic report
Select the exact format and click **Export**, the report will be saved to the save path of your browser.
 - ◇ Select **png**: Displays the report in picture format.
 - ◇ Select **csv**: Displays the report in list format.

12.1.6 Heat Map

View heat map and track map. You can search the detection results by number of people and stay time, and then generate the heat map. Heat map is not available on economic fisheye cameras.

Procedure

- Step 1 Select **Report > Report > Heat Map**.
- Step 2 Set search conditions.



For multi-channel camera, select the channel first.

Table 12-2 Set search conditions

Parameter	Description
Channel	For multi-channel camera, select the channel first.
Type	You can select report type form Heat Map and Track Map .
People No.	When selecting type as Heat Map , select People No. , and then set the threshold. The system will display the heat map for people density.
Threshold	
Time	When selecting type as Heat Map , select Time and then set the threshold. The system will display the heat map for stay time.
Threshold	
Period for the report	Set the period for the report. You can view the daily and weekly report, and you can also customize the period.

Step 3 Click **Search**.

Figure 12-10 Heat map (people No.)

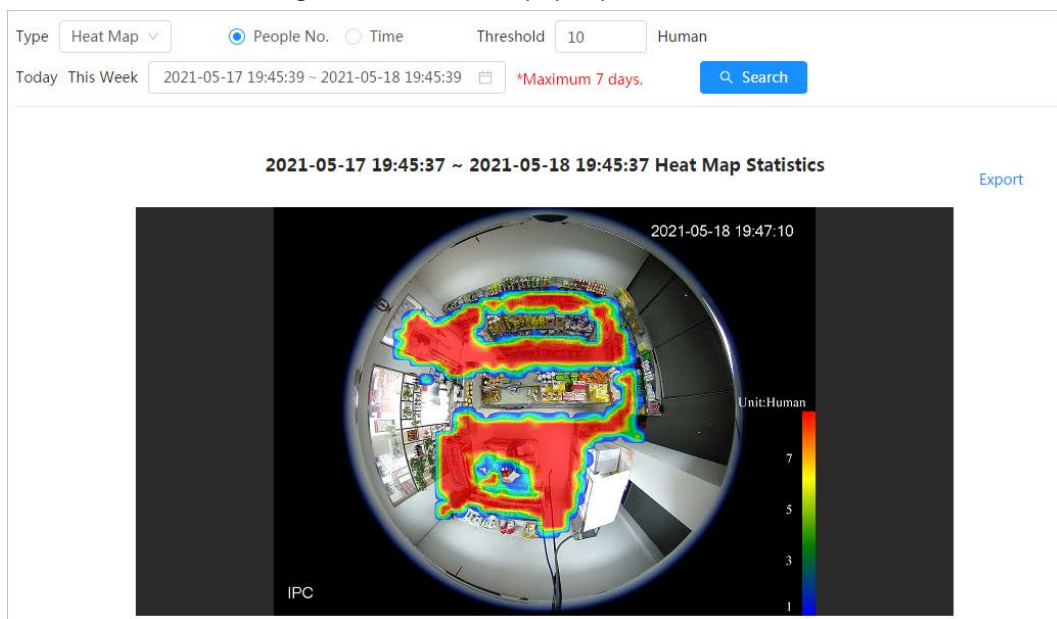


Figure 12-11 Heat map (time)

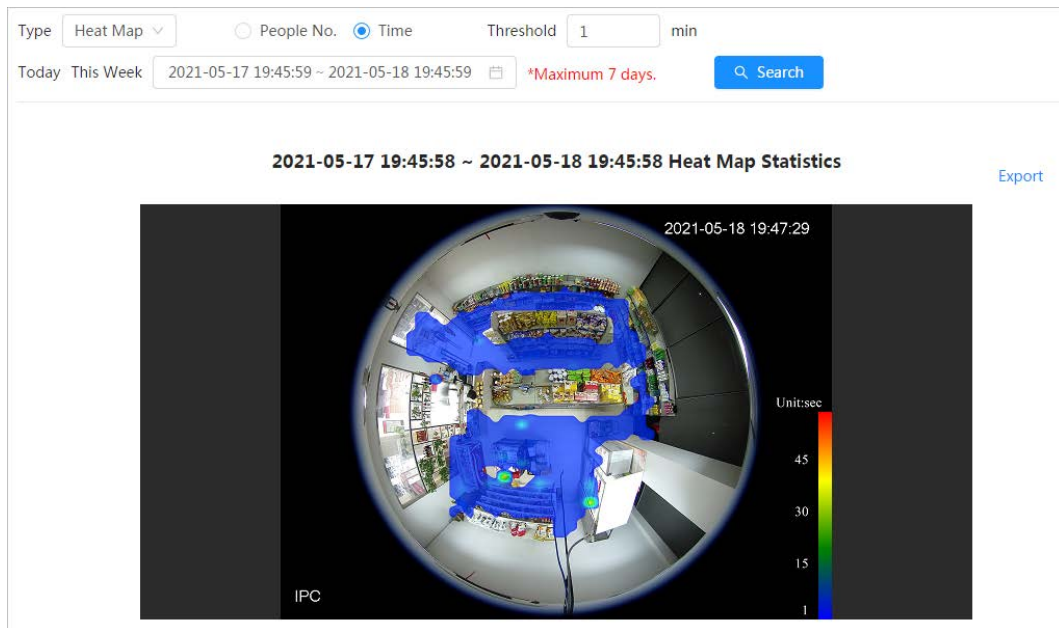
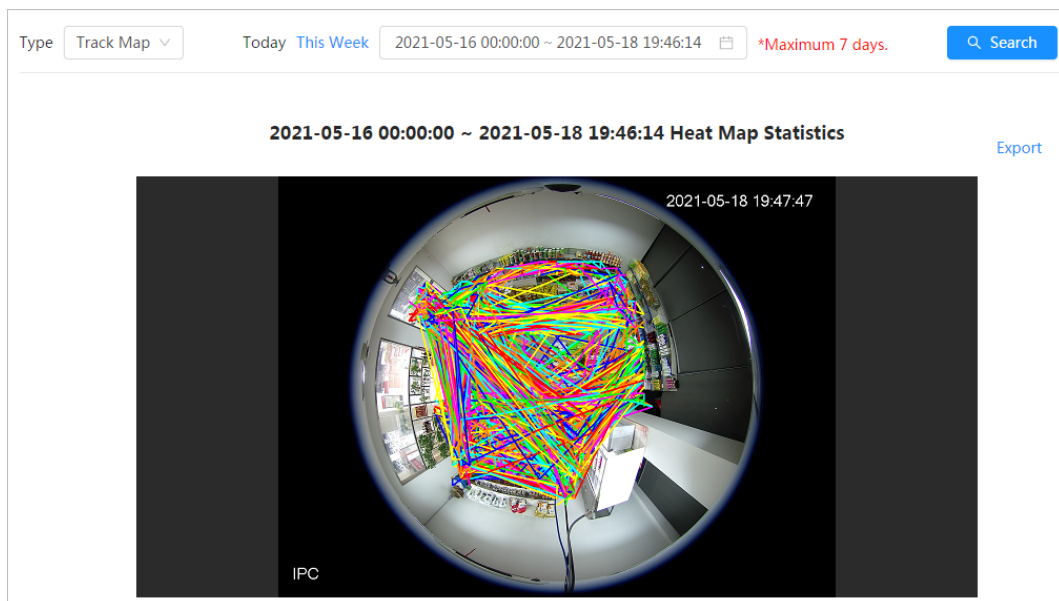


Figure 12-12 Track map



Related Operations

Click **Export**, and select the storage path for the exported report in .bmp format.

12.1.7 ANPR

View the statistics result of ANPR in report form.

Step 1 Select **Report** > **Report** > **ANPR**.

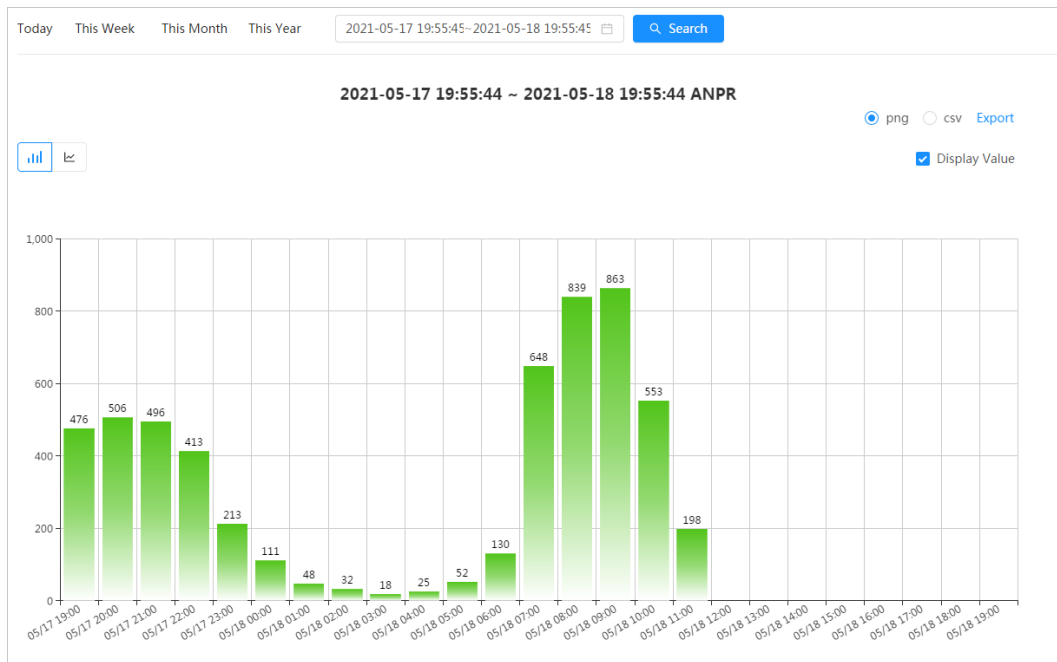
Step 2 Set the period for the report.



For multi-channel camera, select the channel first.

Step 3 Click **Search**.

Figure 12-13 ANPR report



- Select the report form
Click to display the report in line chart; click to display the report in bar chart.
- Select the **Display Value** check box to display the value in the report.
- Export reports
Select the file format, and then click **Export**.
 - ◇ Select **png**: Displays the report in picture format.
 - ◇ Select **csv**: Displays the report in list format.

12.2 Searching for Face Picture

Search for the face recognition or snapshot results by pictures.

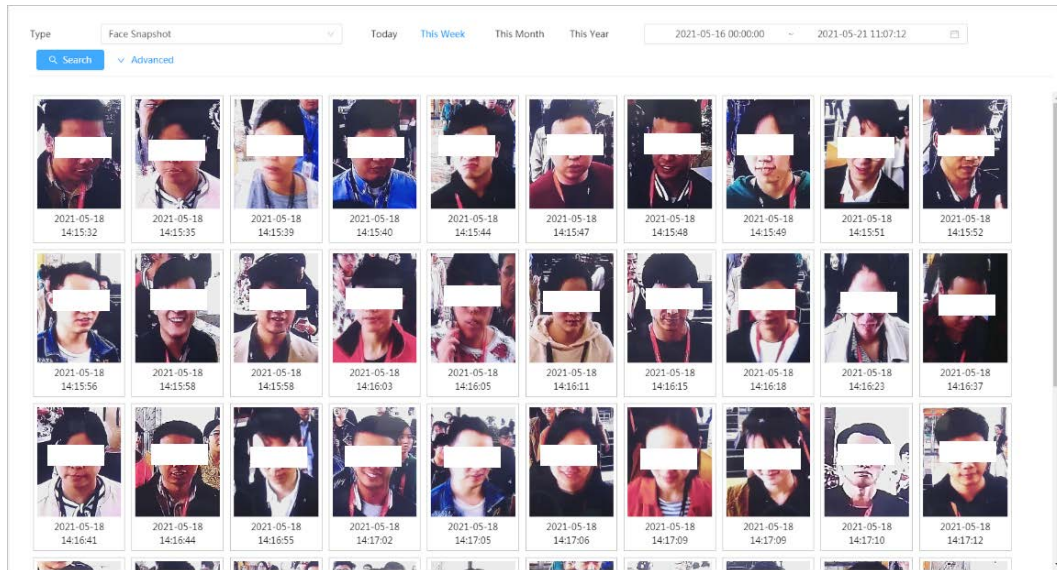
Prerequisites

Make sure that you have installed SD card.

Procedure

- Step 1 Select **Report** > **Picture Query** > **Face**.
- Step 2 Select the type and set the period for the report.
Click **Advance** to set face attributes for precise search.
- Step 3 Click **Search**. The search result is displayed.

Figure 12-14 Face report



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

12.3 Auto Upload

Select the upload mode, enable it, and configure the parameters. The camera will upload reports of AI functions to a defined server periodically.

Background Information

There are three upload methods:

- HTTP: Upload reports to a server through HTTP protocol.
- FTP: Upload reports to a server through FTP protocol. You need to set the parameters, such as the server IP, username, password, and storage path.
- Email: Send reports to receivers through emails. You need to set the parameters, such as the username, password, sender and receiver.

Procedure

Step 1 Select **Report > Auto Upload**.

Step 2 Select the upload method, and then enable it.

Step 3 Set parameters.


Parameters of different upload methods are different.

- **HTTP**

Click **Add**, and then add the information of server. You can add two server information at most.

Figure 12-15 HTTP upload method


Table 12-3 Description of HTTP mode parameter

Parameter	Description
Report Period	Select the report period from the drop-down list. It is 1 hour by default, which indicates that upload the report every 1 hour.
IP/Domain name	The IP address and port number of the server which the report will be uploaded to.
Port	
Path	The storage path of the server for the report.
Report type	Select the report type form the drop-down list. You can select more than one types at the same time.  The report types in the drop-down list are the same with that supported AI function. For example: If the camera supports people counting, heat map, and video metadata, the 3 report types are displayed in the drop-down list.
Test	Test the network connection between the camera and the server.

- **FTP** upload method

Figure 12-16 FTP upload method

Table 12-4 Description of FTP mode parameter



Parameter	Description
Report Period	Select the report period from the drop-down list. It is 1 hour by default, which indicates that upload the report every 1 hour.
Report type	Select the report type form the drop-down list. You can select more than one types at the same time.  The report types in the drop-down list are the same with that supported AI function. For example: If the camera supports people counting, heat map, and video metadata, the 3 report types are displayed in the drop-down list.
Server IP	The IP address and port number of the FTP server which the report will be uploaded to.
Port	
Username	Username and password for logging in to FTP server.
Password	
Storage Path	Username and password for logging in to FTP server.
Test	Test the network connection between the camera and the server.

- Email upload method

Figure 12-17 Email upload method

Upload Mode	Email
Enable	<input checked="" type="checkbox"/>
Report Period	1hr
Report Type	People Counting x
SMTP Server	none
Port	25
Anonymous	<input type="checkbox"/>
Username	anonymity
Password
Sender	none
Encryption Type	TLS(Recommended)
Subject	IPC Message
Receiver	<input type="text"/> <input type="button" value="Add"/>
<input type="button" value="Apply"/> <input type="button" value="Refresh"/> <input type="button" value="Default"/>	

Table 12-5 Description of email mode parameter

Parameter	Description
Report Period	Select the report period from the drop-down list. It is 1 hour by default, which indicates that upload the report every 1 hour.
Report Type	Select the report type form the drop-down list. You can select more than one types at the same time.  <ul style="list-style-type: none"> The report types in the drop-down list are the same with that supported AI function. For example: If the camera supports people counting, and video metadata the 2 report types are displayed in the drop-down list. Heat map report will not be uploaded when you select email upload method, so heat map will not be displayed in the drop-down list.
SMTP server	SMTP (Simple Mail Transfer Protocol) server IP address and port number.
Port	 See Table 12-6 for details.
Anonymous	Select Anonymous , and the sender's information is not displayed in the email.
Username	Username and password used to log in server.



Parameter	Description
Password	 See Table 12-6 for details.
Sender	Sender's email address.
Encryption Type	Select the encryption type from None, SSL (Secure Sockets Layer) and TLS (Transport Layer Security).  See Table 12-6 for details.
Subject	Email subject. You can enter up to 120 characters in Chinese, English, and Arabic numerals.
Receiver	Email addresses of receivers. Click add to set more than one receivers. Supports 3 addresses at most.

Table 12-6 Description of major mailbox configuration

Mailbox	SMTP server	Authentication	Port	Description
gmail	smtp.gmail.com	SSL	465	You need to enable SMTP service in your mailbox.
		TLS	587	

Step 4 Click **Apply**.

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

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.

Address: No.1199 Bin'an Road, Binjiang District, Hangzhou, P. R. China | Website: www.dahuasecurity.com | Postcode: 310053

Email: overseas@dahuatech.com | Fax: +86-571-87688815 | Tel: +86-571-87688883



Network Camera Web 3.0

Operation Manual







Foreword

General

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

Safety Instructions

The following signal words 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
V2.1.3	Updated the description of encode bar.	November 2021
V2.1.2	<ul style="list-style-type: none"> Updated "4.2.4.1 Adjustment". Updated "4.5.1.1.1 Interface Layout". Updated "4.5.1.1.2 Picture". Updated "4.5.1.1.11 Image Correction". Updated "4.5.1.4 Splicing". Updated "4.5.2.1 Video". Updated "4.8.2 Date & Time". 	September 2021
V2.1.1	<ul style="list-style-type: none"> Updated "4.8.3.2 Adding User Group". Updated "5.18 Setting Relay-in". 	July 2021
V2.1.0	Updated "5.7 Setting Smart Plan"	July 2021
V2.0.9	Updated "4.5.2.1 Video".	May 2021
V2.0.8	<ul style="list-style-type: none"> Updated "4.5.2.3.1 Configuring Privacy Masking". Updated "4.7.3.3 FTP". Updated "4.8.3.1 Adding a User" and "4.8.3.3 ONVIF User". Updated "5.4.2 Setting Video Tampering". Updated "5.11 Setting Face Detection". Updated "5.15 Setting Stereo Analysis". Updated "5.19.5 Setting Security Exception". 	December 2020

Version	Revision Content	Release Date
V2.0.7	<ul style="list-style-type: none"> • Modify "5.1.1.7 Warning Light Linkage". • Add "4.6.12 5G". • Modify "4.7.3.2 Local". 	July 2020
V2.0.6	<ul style="list-style-type: none"> • Added "4.5.2.3.11 Configuring GPS Position". • Updated "5.2 Setting Smart Track". 	July 2020
V2.0.5	<ul style="list-style-type: none"> • Updated "4.5.1.1.8 Illuminator". • Updated "4.7.3.2 Local". • Added "5.19.6 Setting Disarming". 	June 2020
V2.0.4	<ul style="list-style-type: none"> • Updated "4.5.1.4 Splicing". • Updated "5.14 Setting Vehicle Density". • Updated "5.12 Setting People Counting". 	May 2020
V2.0.3	Added note in "4.7.3.2 Local".	May 2020
V2.0.2	<ul style="list-style-type: none"> • Modified the contents of "5.16 Setting ANPR". • Added modeling in "5.11 Setting Face Detection". 	December 2019
V2.0.1	Added "5.5 Setting Smart Motion Detection".	August 2019
V2.0.0	<ul style="list-style-type: none"> • Consolidated the outline, and added baseline and safety contents, and some intelligent functions such as face recognition and ANPR. • Deleted some old function such as stereo vision. 	July 2019
V1.0.4	<ul style="list-style-type: none"> • Updated the chapters of "5.12 Setting People Counting" and "5.13.1 Heat Map". • Add VR mode of Fisheye device. • Add video metadata function. 	March 2019
V1.0.3	Added Stereo Analysis function.	November 2018
V1.0.2	<ul style="list-style-type: none"> • Added chapters of "3 Device Initialization". and "Stereo vision." • Updated the chapters of "4.8.3 Account", and "4.6.7 SNMP". 	October 2017
V1.0.1	First release.	September 2016

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, fingerprints, and license plate number. You need to be in compliance with your local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures which include but are not limited: Providing clear and visible identification to inform people of the existence of the surveillance area and provide required contact information.

About the Manual

- The manual is for reference only. Slight differences might be found between the manual and the product.
- We are not liable for losses incurred due to operating the product in ways that are not in compliance with the manual.

- The manual will be updated according to the latest laws and regulations of related jurisdictions. For detailed information, see the paper user's manual, use our CD-ROM, scan the QR code or visit our official website. The manual is for reference only. Slight differences might be found between the electronic version and the paper version.
- All designs and software are subject to change without prior written notice. Product updates might result in some differences appearing between the actual product and the manual. Please contact customer service for the latest program and supplementary documentation.
- There might be errors in the print or deviations in the description of the functions, operations and technical data. 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 company names in the manual are properties of their respective owners.
- Please visit our website, contact the supplier or customer service if any problems occur while 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 supply must conform to the requirements of ES1 in IEC 62368-1 standard and be no higher than PS2. Note that the power supply requirements are 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 device malfunctions, 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 disassembling operation about the device; otherwise, it might cause water leakage or poor image quality due to unprofessional operations. Make sure that the gasket ring is flat and properly installed in the groove before installing the cover. Contact after-sales 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).
- We recommend using the device together with lightning arrester to improve lightning protection effect.
- We recommend grounding 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 decrease, do not use volatile solvent such as alcohol, benzene, diluent 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 moistened 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 devices with old firmware versions, the ONVIF password will not be changed automatically along with changing the system password, and you need to upgrade the firmware or manually change the ONVIF password.
- Use standard components or accessories provided by manufacturer and make sure that the device is installed and maintained by professional engineers.
- Do not expose the surface of the image sensor 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.....	IV
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 Intelligent Function	2
2 Configuration Flow	5
3 Device Initialization	6
4 Basic Configuration	9
4.1 Login	9
4.2 Live.....	10
4.2.1 Live Interface	10
4.2.2 Encode bar.....	11
4.2.3 Live View Function Bar.....	11
4.2.4 Window Adjustment Bar.....	14
4.2.4.1 Adjustment	14
4.2.4.2 Zoom and Focus.....	17
4.2.4.3 Fisheye	18
4.3 PTZ Operation	22
4.3.1 Configuring External PTZ Protocol.....	22
4.3.2 Configuring PTZ Function	22
4.3.2.1 Preset	22
4.3.2.2 Tour.....	23
4.3.2.3 Scan.....	24
4.3.2.4 Pattern.....	25
4.3.2.5 Pan.....	26
4.3.2.6 PTZ Speed	27
4.3.2.7 Idle Motion	27
4.3.2.8 PowerUp.....	28
4.3.2.9 PTZ Limit.....	29
4.3.2.10 Time Task.....	29
4.3.2.11 PTZ Restart	30
4.3.2.12 Default.....	31

4.3.3 Calling PTZ	32
4.3.3.1 PTZ Control	32
4.3.3.2 PTZ Function	34
4.4 Playback	34
4.4.1 Playback Interface	35
4.4.2 Playing back Video or Picture	37
4.4.3 Clipping Video	39
4.4.4 Downloading Video or Picture	40
4.4.4.1 Downloading A Single File	40
4.4.4.2 Downloading Files in Batches	40
4.5 Camera	41
4.5.1 Conditions	41
4.5.1.1 Conditions	41
4.5.1.1.1 Interface Layout	41
4.5.1.1.2 Picture	43
4.5.1.1.3 Exposure	44
4.5.1.1.4 Backlight	46
4.5.1.1.5 WB	47
4.5.1.1.6 Day & Night	48
4.5.1.1.7 Zoom and Focus	49
4.5.1.1.8 Illuminator	50
4.5.1.1.9 Defog	51
4.5.1.1.10 Fisheye	52
4.5.1.1.11 Image Correction	53
4.5.1.1.12 Splicing Mode	54
4.5.1.2 Profile Management	54
4.5.1.3 Zoom and Focus	55
4.5.1.4 Splicing	55
4.5.2 Setting Video Parameters	56
4.5.2.1 Video	56
4.5.2.2 Snapshot	59
4.5.2.3 Overlay	60
4.5.2.3.1 Configuring Privacy Masking	60
4.5.2.3.2 Configuring Channel Title	63
4.5.2.3.3 Configuring Time Title	63
4.5.2.3.4 Configure Text Overlay	64
4.5.2.3.5 Configure Font Attribute	65

4.5.2.3.6 Configure Picture Overlay	65
4.5.2.3.7 Configure Custom Overlay	66
4.5.2.3.8 Configuring OSD Info	67
4.5.2.3.9 Configuring Counting	68
4.5.2.3.10 Configuring Structured Statistics	68
4.5.2.3.11 Configuring GPS Position	69
4.5.2.3.12 Configuring Ranging	69
4.5.2.3.13 Configuring ANPR	70
4.5.2.3.14 Configuring Face Statistics	71
4.5.2.4 ROI	71
4.5.2.5 Path	72
4.5.3 Audio	73
4.5.3.1 Configuring Audio Parameter	73
4.5.3.2 Configuring Alarm Audio	74
4.6 Network	75
4.6.1 TCP/IP	75
4.6.2 Port	78
4.6.3 PPPoE	79
4.6.4 DDNS	80
4.6.5 SMTP (Email)	81
4.6.6 UPnP	84
4.6.7 SNMP	85
4.6.8 Bonjour	88
4.6.9 Multicast	88
4.6.10 802.1x	89
4.6.11 QoS	90
4.6.12 5G	90
4.6.12.1 Dialing Setting	90
4.6.12.2 Mobile Setting	92
4.6.13 Access Platform	92
4.6.13.1 P2P	92
4.6.13.2 ONVIF	93
4.6.13.3 RTMP	94
4.7 Storage	95
4.7.1 Setting Storage Plan	95
4.7.2 Setting Schedule	95
4.7.3 Setting Destination	96

4.7.3.1 Path.....	96
4.7.3.2 Local.....	97
4.7.3.3 FTP.....	98
4.7.3.4 NAS.....	100
4.8 System.....	101
4.8.1 General.....	101
4.8.2 Date & Time.....	102
4.8.3 Account.....	103
4.8.3.1 Adding a User.....	103
4.8.3.2 Adding User Group.....	108
4.8.3.3 ONVIF User.....	110
4.8.4 Safety.....	113
4.8.4.1 System Service.....	113
4.8.4.2 HTTPS.....	114
4.8.4.3 Firewall.....	118
4.8.5 Peripheral.....	120
4.8.5.1 Serial Port Settings.....	120
4.8.5.2 External Light.....	121
4.8.5.3 Wiper.....	122
5 Event.....	124
5.1 Setting Alarm Linkage.....	124
5.1.1 Alarm Linkage.....	124
5.1.1.1 Setting Period.....	125
5.1.1.2 Record Linkage.....	125
5.1.1.2.1 Setting Record Plan.....	126
5.1.1.2.2 Setting Record Control.....	127
5.1.1.2.3 Setting Record Linkage.....	127
5.1.1.3 Snapshot Linkage.....	128
5.1.1.3.1 Setting Snapshot Plan.....	128
5.1.1.3.2 Setting Snapshot Linkage.....	129
5.1.1.4 Relay-out Linkage.....	129
5.1.1.5 Email Linkage.....	129
5.1.1.6 PTZ Linkage.....	130
5.1.1.7 Warning Light Linkage.....	130
5.1.1.8 Audio Linkage.....	130
5.1.2 Subscribing Alarm.....	131
5.1.2.1 About Alarm Types.....	131

5.1.2.2 Subscribing Alarm Information	131
5.2 Setting Smart Track	132
5.2.1 Setting Calibration Parameters for Smart Track	132
5.2.2 Enabling Alarm Track	134
5.3 Setting Panoramic Calibration	135
5.4 Setting Video Detection	137
5.4.1 Setting Motion Detection	137
5.4.2 Setting Video Tampering	139
5.4.3 Setting Scene Changing	140
5.5 Setting Smart Motion Detection	141
5.6 Setting Audio Detection	142
5.7 Setting Smart Plan	144
5.7.1 Basic Smart Plan	144
5.7.2 Schedule	145
5.8 Setting IVS	147
5.8.1 Global Configuration	147
5.8.2 Rule Configuration	149
5.9 Setting Crowd Map	153
5.9.1 Global Configuration	153
5.9.2 Rule Configuration	154
5.10 Setting Face Recognition	157
5.10.1 Setting Face Detection	157
5.10.2 Setting Face Database	159
5.10.2.1 Creating Face Database	160
5.10.2.2 Adding Face Picture	161
5.10.2.2.1 Single Adding	161
5.10.2.2.2 Batch Importing	164
5.10.2.3 Managing Face Picture	165
5.10.2.3.1 Modifying Face Information	166
5.10.2.3.2 Deleting Face Picture	166
5.10.2.4 Face Modeling	166
5.10.3 Setting Face Recognition Alarm Linkage	168
5.10.4 Viewing Face Recognition Result	169
5.10.4.1 Viewing Result in the Live Interface	169
5.10.4.2 Viewing Result by Search Function	170
5.11 Setting Face Detection	171
5.12 Setting People Counting	174

5.12.1 People Counting	174
5.12.2 Calibration Configuration.....	178
5.12.3 Queuing	179
5.12.4 Viewing People Counting Diagram.....	181
5.12.5 Viewing People Counting Report	182
5.13 Setting Heat Map	184
5.13.1 Heat Map	184
5.13.2 Viewing Heat Map Report.....	184
5.14 Setting Vehicle Density.....	185
5.15 Setting Stereo Analysis.....	188
5.15.1 Setting Rules for Stereo Analysis	188
5.15.2 Calibration Configuration.....	193
5.15.3 Zoom Calibration	193
5.15.4 Viewing Report.....	194
5.16 Setting ANPR.....	195
5.16.1 Scene Configuration	195
5.16.2 Setting Picture Overlay	197
5.16.3 Viewing ANPR Report	198
5.17 Setting Video Metadata.....	198
5.17.1 Scene Configuration	199
5.17.2 Setting Picture Information	201
5.17.3 Viewing Video Metadata Report	202
5.18 Setting Relay-in.....	202
5.18.1 Relay-in (1).....	202
5.18.2 Relay-in (2).....	203
5.19 Setting Abnormality	204
5.19.1 Setting SD Card	204
5.19.2 Setting Network.....	205
5.19.3 Setting Illegal Access.....	206
5.19.4 Setting Voltage Detection	206
5.19.5 Setting Security Exception	207
5.19.6 Setting Disarming.....	208
6 Maintenance	210
6.1 Requirements	210
6.2 Auto Maintain.....	210
6.3 Resetting Password	210
6.4 Backup and Default	213

6.4.1 Import/Export	213
6.4.2 Default	213
6.5 Upgrade	214
6.6 Information	214
6.6.1 Version	215
6.6.2 Log	215
6.6.3 Remote Log	216
6.6.4 Online User	216
Appendix 1 Cybersecurity Recommendations	218

1 Overview

1.1 Introduction

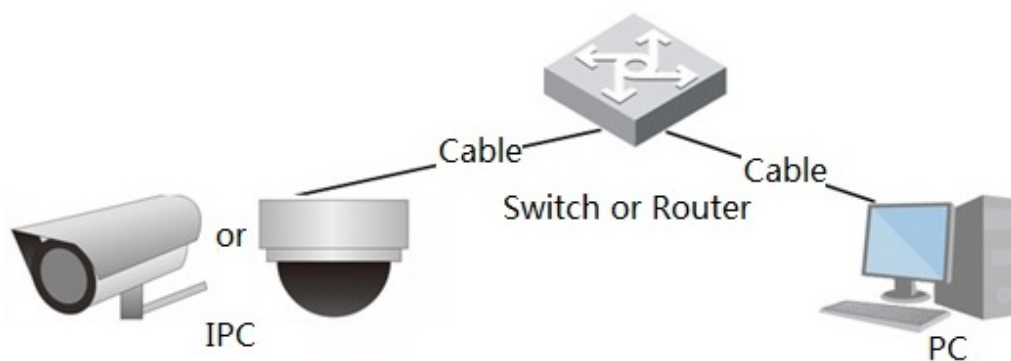
IP camera (Internet Protocol camera), is a type of digital video camera that receives control data and sends image data through internet. They are commonly used for surveillance, requiring no local recording device, but only a local area network.

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.

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.

Record

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

Account

- Add, modify and delete user group, and manage user authorities according to user group.
- Add, modify and delete user, and configure user authorities.
- Modify user password.

1.3.2 Intelligent Function

Alarm

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

Smart Track

- Set calibration and parameters for smart track and enable alarm track.
- Switch between smart track and speed dome auto track.

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.

Smart Motion Detection

- Avoid the alarms triggered by the environment changes.
- 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.

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.

Crowd 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.

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.

People Counting

- Count the people flow in/out the detection area, and generate report.
- When an alarm is triggered, the system performs linkages such as recording, alarm output, sending email, PTZ operation, and snapshot.

Heat Map

- Count cumulative density of moving objects.
- View report of heat map.

Vehicle Density

- Supports traffic congestion detection and parking upper limit detection.
- View the statistic data on the live interface.
- When an alarm is triggered, the system performs linkages such as recording, alarm output, sending email, and snapshot.

Stereo Analysis

- Include Activation Analysis, Back Detection, Fall Detection, Walking Detection, Blackboard Writing Detection, Violence Detection, People No. Error, Stand Detection, Running Detection, People Approaching Detection, and Strand Detection.
- When an alarm is triggered, the system performs linkages such as recording, alarm output, sending email, PTZ operation, and snapshot.

ANPR

- Recognize plate number in detection area, and display the related information on live interface.
- When an alarm is triggered, the system links alarm output and snapshot.

Video Metadata

- Snap 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.

Alarm Setting

- The alarm is triggered when an external alarm input device inputs alarm.
- When an alarm is triggered, the system performs linkages such as recording, alarm output, sending email, PTZ operation, and snapshot.

Abnormality

- 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.

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.

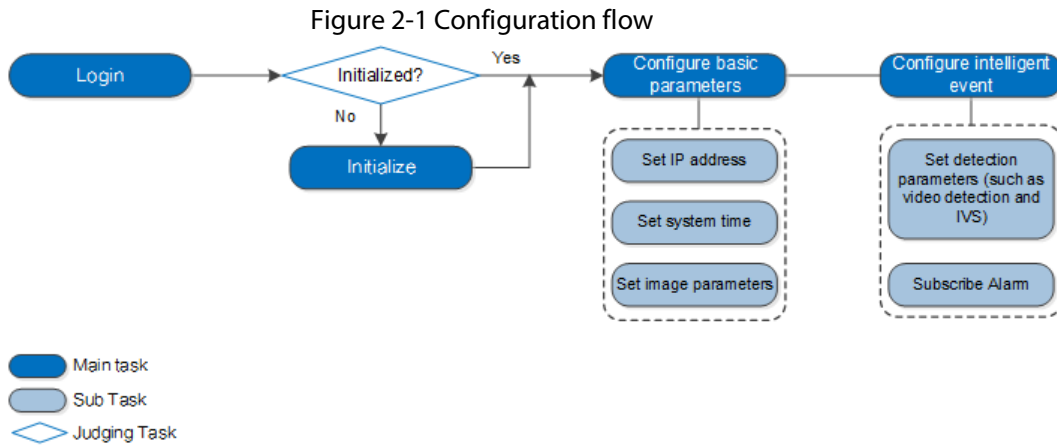


Table 2-1 Description of flow

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.	"4.1 Login"
Initialization		Initialize the camera when you use it for the first time.	"3 Device Initialization"
Basic parameters	IP address	Modify IP address according to network planning for the first use or during network adjustment.	"4.6.1 TCP/IP"
	Date & time	Set date and time to ensure the recording time is correct.	"4.8.2 Date & Time"
	Image parameters	Adjust image parameters according to the actual situation to ensure the image quality.	"4.5.1 Conditions"
Intelligent Event	Detection rules	Configure the necessary detection rules, such as video detection and IVS.	"5 Event"
	Subscribe alarm	Subscribe alarm event. When the subscribed alarm is triggered, the system will record the alarm on the alarm tab.	"5.1.2 Subscribing Alarm"

3 Device Initialization

Device initialization is required for the first 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 Enter key.



The IP is 192.168.1.108 by default.

Figure 3-1 Device initialization

The screenshot shows a web interface titled "Device Initialization". It contains the following elements:

- Username:** A text field with "admin" entered.
- Password:** A text field with a red error message: "The minimum pass phrase length is 8 characters". Below it are three buttons: "Weak", "Middle", and "Strong".
- Confirm Password:** An empty text field.
- Instructions:** "Use a password that has 8 to 32 characters, it can be a combination of letter(s), number(s) and symbol(s) with at least two kinds of them.(please do not use special symbols like '*'; : &)"
- Email Address:** A checked checkbox labeled "Email Address" and an empty text field. Below it is the text: "To reset password, please input properly or update in time."
- Save:** A button at the bottom center.

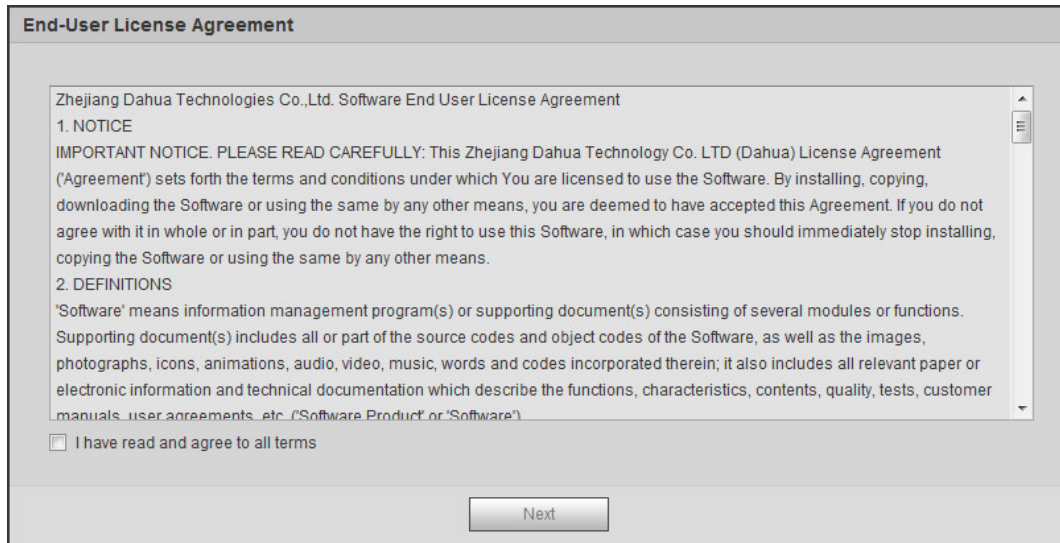
Step 2 Set the password for admin account.

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	
email	Enter an email address for password reset, 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.

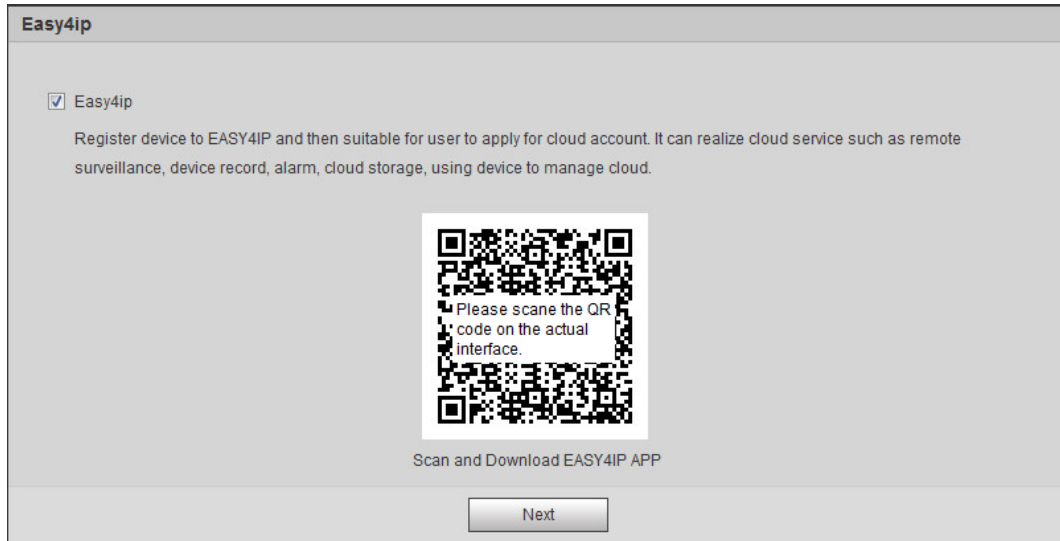
Step 3 Click **Save**.

Figure 3-2 End-user license agreement



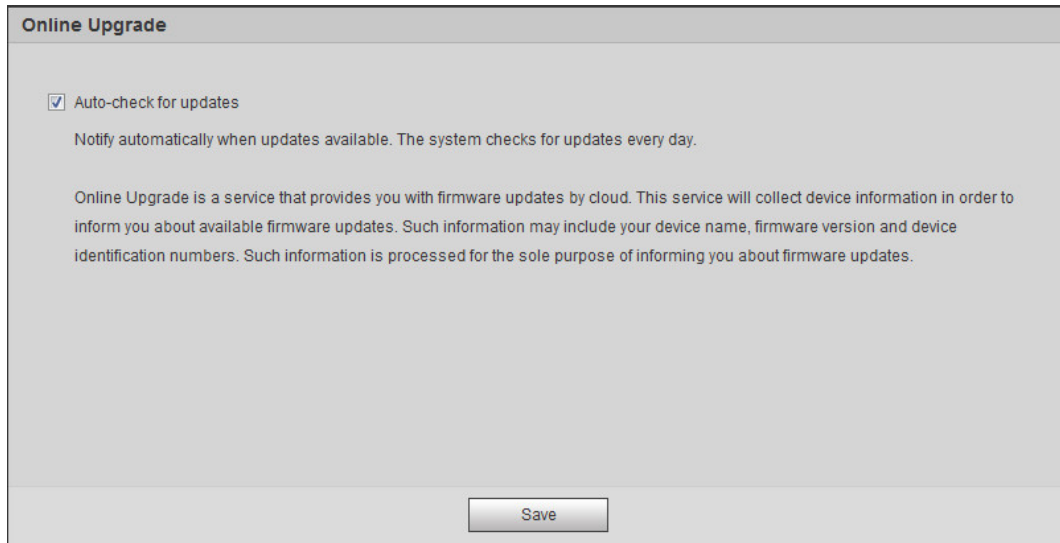
Step 4 Select the **I have read and agree to all terms** checkbox, and then click **Next**.

Figure 3-3 Easy4ip



Step 5 You can register the camera to Easy4ip, select the checkbox as needed, and then click **Next**.

Figure 3-4 Online upgrade



Step 6 Select the upgrading method as needed.

If you select **Auto-check for updates**, the system checks new version once a day automatically. There will be system notice on **Upgrade** interface and **Version** interface if any new version is available.



Select **Setting > System > Upgrade > Online Upgrade**, and you can enable the auto-check function.

Step 7 Click **Save**.

4 Basic Configuration

The chapter introduces the basic configuration, including login, live view, PTZ operation, playback, camera configuration, network configuration, storage configuration and system configuration.

4.1 Login


This section introduces how to log in to and log out of the web interface. This section takes IE Explorer 9 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.

Figure 4-1 Login



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



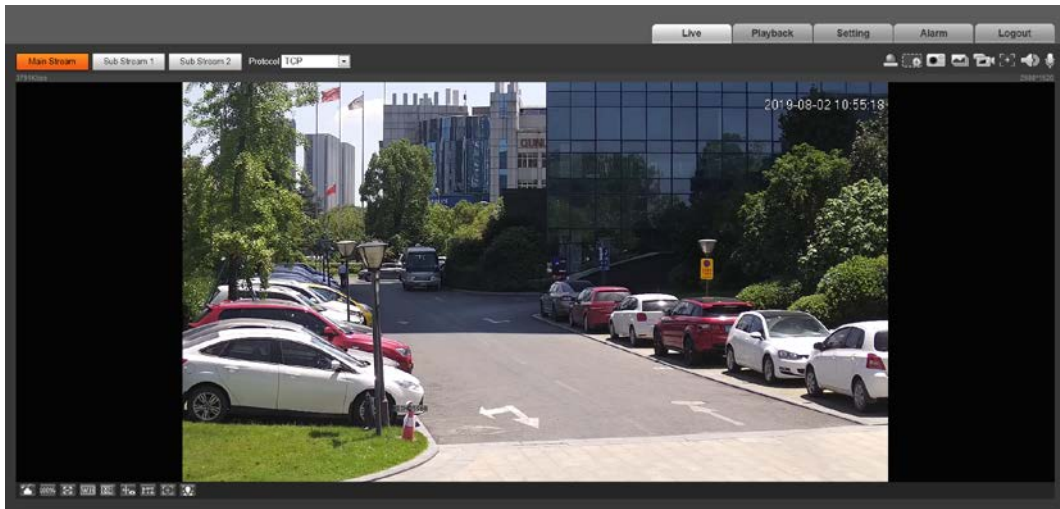
Click **Forget password?**, and you can reset the password through the email address that is set during the initialization. For details, see "6.3 Resetting Password".

Step 3 Click **Login**.

- Live: Click **Live**, and you can view the real-time monitoring image.
- Playback: Click **Playback**, and you can play back or download recorded video or image files.
- Setting: Click **Setting**, and you can configure the basic and intelligent functions of the camera.
- For the camera with multiple channels, through selecting channel numbers, you can set the parameters of the channels.

- Alarm: Click **Alarm**, and you can subscribe and view alarm information.
- Logout: Click **Logout** to go to login interface.
- The system will sleep automatically after idling for a period of time.

Figure 4-2 Live



4.2 Live

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

4.2.1 Live Interface

This section introduces system menu, encode bar, live view function bar, and window adjustment bar.

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



The functions and interfaces of different models might vary.

Figure 4-3 Live

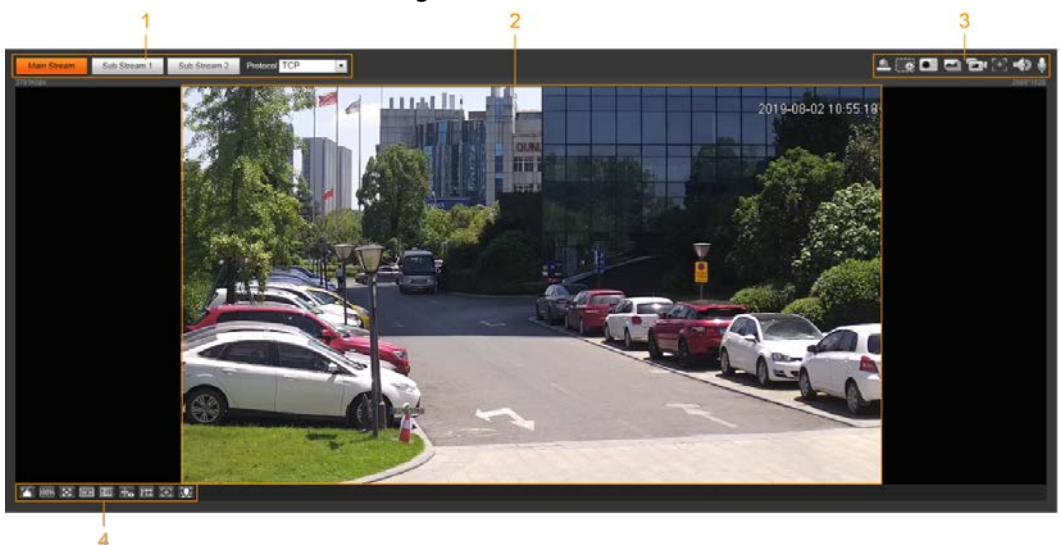
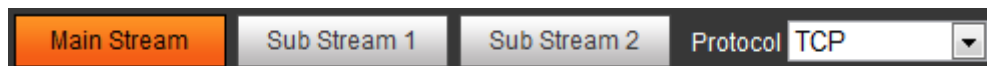


Table 4-1 Description of function bar

No.	Function	Description
1	Encode bar	Sets stream type and protocol.
2	Live view	Displays the real-time monitoring image.
3	Live view function bar	Functions and operations in live viewing.
4	Window adjustment bar	Adjustment operations in live viewing.

4.2.2 Encode Bar

Figure 4-4 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 "4.5.2.1 Video".
- **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 "4.5.2.1 Video".
- **Protocol:** You can select the network transmission protocol as needed, and the options are **TCP**, **UDP** and **Multicast**.














Before selecting **Multicast**, make sure that you have set the **Multicast** parameters.







4.2.3 Live View Function Bar

For the live view function bar, see Table 4-2.

Table 4-2 Description of live view function bar

Icon	Function	Description
	Manual Position	<p>Manually position the tracking speed dome to the selected location of corresponding panoramic camera.</p> <p>Click the icon and click or select randomly on the image of panoramic camera channel, the tracking speed dome will automatically position the selected location.</p> <p></p> <ul style="list-style-type: none"> For multi-sensor panoramic network camera + PTZ camera, before enabling manual position, make sure that you have enabled alarm track and smart track calibration. For details, see "5.2 Setting Smart Track". For panoramic network camera, before enabling manual position, make sure that you have enabled panoramic linkage. For details, see "5.3 Setting Panoramic Calibration".
	Regional Focus	<p>Select channel image of the tracking speed dome, click the icon and click or select randomly on the channel image of the tracking speed dome, and then the speed dome can realize auto focus upon the selected region.</p>
	Wiper	<p>Controls the wiper of the camera.</p> <p>Click the icon to enable or disable wiper function.</p>
	Ranging	<p>Click the icon, select a point on the ground, and the distance between the camera and the selected point will be displayed.</p> <p></p> <p>Before using this function, you need to set the installation of device first. For details, see "4.5.2.3.12 Configuring Ranging".</p>
	Gesture	<p>Controls PTZ by operating the mouse on the live view of tracking speed dome.</p> <p>Select the live view of tracking speed dome, click the icon, press left-button and drag image to control PTZ. And you can zoom in or out the image through rolling mouse wheel.</p>
	Manual Track	<p>Click the icon, and select tracking target on the live view of tracking speed dome, the camera tracks the selected target automatically.</p>

Icon	Function	Description
	Vehicle Density	Click the icon, and select an area on the live image, the camera will automatically count the number of the vehicles in the selected area, and display the number on the Live interface.
	Relay-out	Displays alarm output state. Click the icon to force to enable or disable alarm output. Alarm output state description: <ul style="list-style-type: none"> ● Red: Alarm output enabled. ● Grey: Alarm output disabled.
	Warning Light	Displays the warning light state. Click the icon to enable or disable the warning light forcibly.
	Alarm	Displays alarm sound state. Click the icon to enable or disable the alarm sound forcibly.
	Crowd Map	Click the icon to display the crowd map on the Live interface.  <ul style="list-style-type: none"> ● Only after enabling the function, can you see the icon on the Live interface. ● The positions of the icon might vary depending on models.
	Digital Zoom	You can zoom in or out 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.
	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 "4.5.2.5 Path".
	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 "4.5.2.5 Path".












Icon	Function	Description
	Record	<p>Click the icon to record video, and it will be saved to the configured storage path.</p> <p> About viewing or configuring storage path, see "4.5.2.5 Path".</p>
	Easy Focus	<p>Click the icon, the AF Peak (focus eigenvalue) and AF Max (max focus eigenvalue) are displayed on the video image.</p> <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. <p> Easy focus closes automatically after five minutes.</p>
	Audio	Click the icon to enable or disable audio output.
	Talk	Click the icon to enable or disable the audio talk.








4.2.4 Window Adjustment Bar




4.2.4.1 Adjustment

This section introduces the adjustment of image.

Table 4-3 Description of adjustment bar

Icon	Function	Description
	Image Adjustment	<p>Click the icon, and then the Image Adjustment interface is displayed at the right side of the Live interface. You can adjust brightness, contrast, hue, and saturation.</p> <p></p> <p>The adjustment is only available on the web interface, and it does not adjust the camera parameters.</p> <ul style="list-style-type: none">  (Brightness adjustment): Adjusts the overall image brightness, and change the value when the image is too bright or too dark. The bright and dark areas will have equal changes.  (Contrast adjustment): Change the value when the image brightness is proper but contrast is not enough.  (Hue adjustment): Makes the color deeper or lighter. The default value is made by the light sensor, and it is recommended.  (Saturation adjustment): Adjusts the image saturation. This value does not change image brightness.
	Original Size	<p>Click the icon, and it changes to , and then the video displays with original size; click , and the video displays with adapted size.</p>
	Full Screen	<p>Click the icon to enter full screen mode; double-click or press Esc to exit.</p>
	Width : Height	<p>Click the icon to resume original ratio or change ratio.</p>

Icon	Function	Description
	Fluency	<p>Click the icon to select the fluency from Realtime, Fluency and Normal.</p> <ul style="list-style-type: none"> • Realtime: Guarantees the real-time display of the image. When the bandwidth is not enough, the image might not be smooth. • Fluency: Guarantees the fluency of the image. There might be delay between live view image and real-time image. • Normal: It is between Realtime and Fluency.
	Rule Info	<p>Click the icon, and then select Enable to display smart rules and detection box; select Disable to stop the display. It is enabled by default.</p>
	PTZ	<p>Click the icon, and the PTZ control panel is displayed at the right side of the Live interface. You can control and call PTZ function. For details, see "4.3.3 Calling PTZ".</p>
	Zoom and Focus	<p>Adjust focal length to zoom in and out video image. Click the icon, and the Zoom and Focus configuration interface is displayed at the right side of the Live interface. You can control and call PTZ function. For details, see "4.2.4.2 Zoom and Focus".</p>
	Fisheye	<p>Click the icon, and then the Fisheye configuration interface is displayed at the right side of the Live interface. For details, see "4.2.4.3 Fisheye".</p>
	Face	<ul style="list-style-type: none"> • Click the icon, and the face detection or face recognition results are displayed on the Live interface. • For face recognition, see "5.10.1 Setting Face Detection". • For face detection: see "5.11 Setting Face Detection".
	ANPR	<p>Click the icon, and the ANPR results are displayed on the Live interface. For details, see "5.16 Setting ANPR".</p>
	Video Metadata	<p>Click the icon, the video metadata results are displayed on the Live interface. For details, see "5.17 Setting Video Metadata".</p>

Icon	Function	Description
	Window Layout	<p>When viewing the multi-channel image, you can select display layout.</p> <p>For Multi-Sensor Panoramic + PTZ Camera:</p> <ul style="list-style-type: none"> The live interface will show Panorama 1 and Panorama 2 by default if you choose dual-channel mode. If you switch from three-channel mode or dual-channel mode to single-channel mode, the live window will show Panorama 1 by default. Click  Panorama 1 Panorama 2 PTZ Camera and select the camera you want to view.
	Crowd Map	<p>Click the icon and select the Enable checkbox. The Crowd Map interface is displayed. For details, see "5.9 Setting Crowd Map".</p>

4.2.4.2 Zoom and Focus

You can adjust focal length to zoom in or out video image and the image clarity.



The focus would adjust automatically after zooming in or out.

Figure 4-5 Zoom and focus

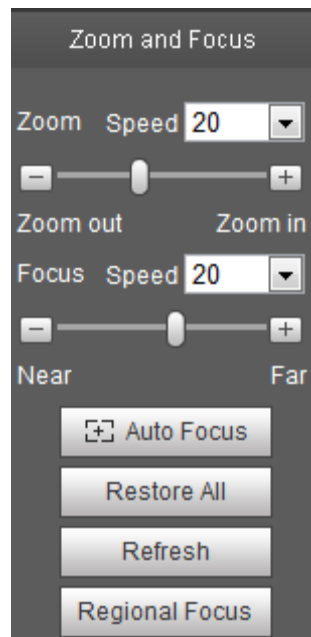




Table 4-4 Description of zoom and focus

Parameter	Description
Zoom	<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 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	<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 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>
Restore All	<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>
Regional Focus	<p>Focus on the subject of a selected area.</p> <p>Click Regional Focus, and then select an area in the image, the camera performs auto focus in that area.</p>
Refresh	<p>Get the latest zoom setting of the device.</p>

4.2.4.3 Fisheye

You can select the installation mode, display mode and VR mode of fisheye devices as needed. For details, see Table 4-5.








- **Install Mode:** Select the installation mode according to the actual situation.
- **Display Mode:** Select the display mode of live view.
- **VR Mode:** Select VR mode to display images in stereo mode.








Figure 4-6 Fisheye




Table 4-5 Description of fisheye configuration

Parameter	Description		
Installation mode	Includes ceiling mount, wall mount, and ground mount.		
Display mode	<p>The display mode of the current image. There are different display modes for each installation mode.</p> <ul style="list-style-type: none"> • Ceiling: 1P+1, 2P, 1+2, 1+3, 1+4, 1P+6, 1+8. • Wall: 1P, 1P+3, 1P+4, 1P+8. • Ground: 1P+1, 2P, 1+3, 1+4, 1P+6, 1+8. <p> The image will be on original size by default when switching installation mode.</p>		
Ceiling/Wall/Ground mount	<table border="1"> <tr> <td> Original image</td> <td>The original image before correction.</td> </tr> </table>	Original image	The original image before correction.
Original image	The original image before correction.		

Parameter	Description	
Ceiling/Ground mount	 1P+1	360° rectangular panoramic image screen + independent sub-screens. <ul style="list-style-type: none"> You can zoom or drag the image in all the screens. You can move the start point (left and right) on rectangular panoramic image screen.
	 2P	Two associated 180° rectangular image screens, and at any time, the two screens form a 360° panoramic image. It is also called dual-panoramic image. You can move the start point (left and right) on the two rectangular panoramic image screens, and the two screens link each other.
	 1+2	Original image screen + two independent sub-screens. Ground Mount does not support this display mode. <ul style="list-style-type: none"> You can zoom or drag the image in all the screens. You can rotate the image on the original image screen to change the start point.
	 1+3	Original image screen + three independent sub-screens. <ul style="list-style-type: none"> You can zoom or drag the image in all the screens. You can rotate the image on the original image screen to change the start point.
	 1+4	Original image screen + four independent sub-screens. <ul style="list-style-type: none"> You can zoom or drag the image in all the screens. You can rotate the image on the original image screen to change the start point.
	 1P+6	360° rectangular panoramic screen + six independent sub-screens. <ul style="list-style-type: none"> You can zoom or drag the image in all the screens. You can move the start point (left and right) on rectangular panoramic image screen.
	 1P+8	Original image screen + eight independent sub-screens. <ul style="list-style-type: none"> You can zoom or drag the image in all the screens. You can rotate the image on the original image screen to change the start point.

Parameter	Description
Wall mount	 1P <p>180° rectangular panoramic image screen (from left to right). You can drag the image in all the screens (up and down) to adjust the vertical view.</p>
	 1P+3 <p>180° rectangular panoramic image screen + three independent sub-screens.</p> <ul style="list-style-type: none"> You can zoom or drag the image in all the screens. You can drag the image in all the screens (upper and lower) to adjust the vertical view.
	 1P+4 <p>180° rectangular panoramic image screen + four independent sub-screens.</p> <ul style="list-style-type: none"> You can zoom or drag the image in all the screens. You can drag the image in all the screens (upper and lower) to adjust the vertical view.
	 1P+8 <p>180° rectangular panoramic image screen + eight independent sub-screens.</p> <ul style="list-style-type: none"> You can zoom or drag the image in all the screens. You can drag the image in all the screens (upper and lower) to adjust the vertical view.
VR mode	 <p>Panorama</p> <p>Drag or cross the screen 360° to unfold the distortion panorama, and you can drag the image in left/right direction.</p>
	 <p>Semi-circle</p> <ul style="list-style-type: none"> You can drag the image in upper/lower/left/right direction. Press I to display the panorama, and press O to resume the original size. Press S to rotate the image in anticlockwise direction, and press E to stop the rotation. Scroll the mouse wheel to zoom the image.
	 <p>Cylinder</p> <p>Display the distortion panorama in 360° circularity.</p> <ul style="list-style-type: none"> You can drag the image in upper/lower/left/right direction. Press I to display the panorama, and press O to return to the original size. Press S to rotate the image in anticlockwise direction, and press E to stop the rotation. Scroll the mouse wheel to zoom the image.

Parameter	Description
	 Asteroid <ul style="list-style-type: none"> You can drag the image in upper/lower/left/right direction. Press I to display the panorama, and press O to return to the original size. Press the left mouse-button to slide down to display the image on the plane surface. Scroll the mouse wheel to zoom the image.

4.3 PTZ Operation

This section introduces PTZ parameter configuration, PTZ control and PTZ function configuration.

4.3.1 Configuring External PTZ Protocol

You need to configure PTZ protocol when accessing external PTZ camera; otherwise the camera cannot control external PTZ camera.

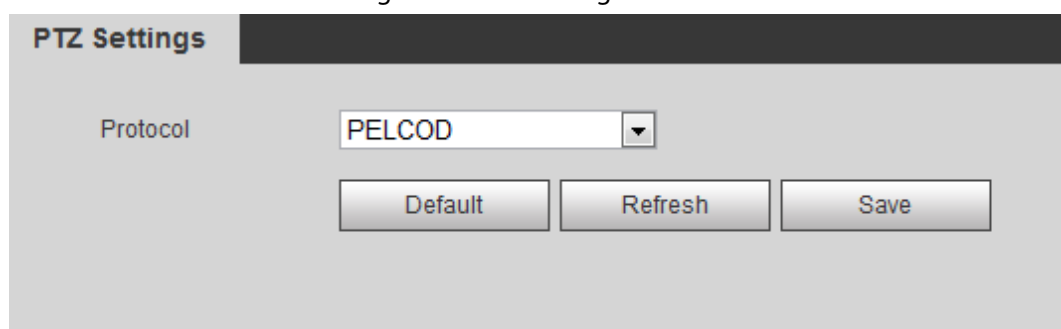
Prerequisites

- Access external PTZ through RS-485.
- You have configured the parameters of serial port. For details, see "4.8.5.1 Serial Port Settings".

Procedure

Step 1 Select **Setting** > **PTZ Setting** > **Protocol**.

Figure 4-7 PTZ setting



Step 2 Select the PTZ protocol.

Step 3 Click **OK**.

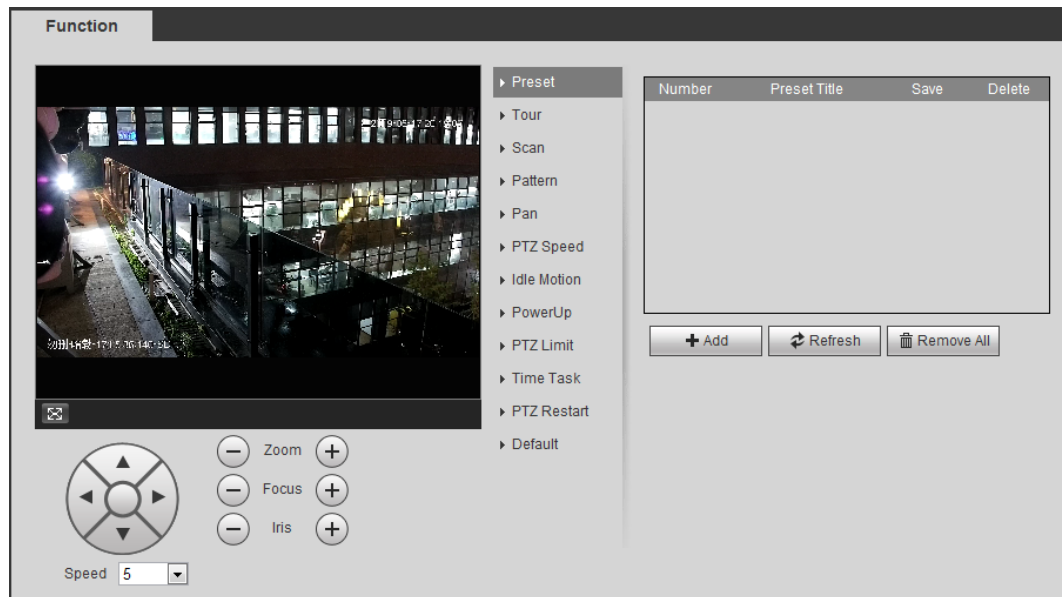
4.3.2 Configuring PTZ Function

4.3.2.1 Preset

Preset means a certain position that the camera can make quick orientation to. It includes PTZ pan and tilt angles, camera focus, and location.

Step 1 Select **Setting** > **PTZ Settings** > **Function** > **Preset**.

Figure 4-8 Preset



- Step 2** Set the speed, and click , and to adjust the parameters of direction, zoom, focus and iris, to move the camera to the position you need.
- Step 3** Click **Add** to add the current position to be a preset, and the preset is displayed in preset list.
- Step 4** Double-click the preset title to edit it.
- Step 5** Click to save the preset.

Related Operations

- Click to delete the preset.
- Click **Remove All** to remove all presets.

4.3.2.2 Tour

Tour means a series of movements that the camera makes along several presets.

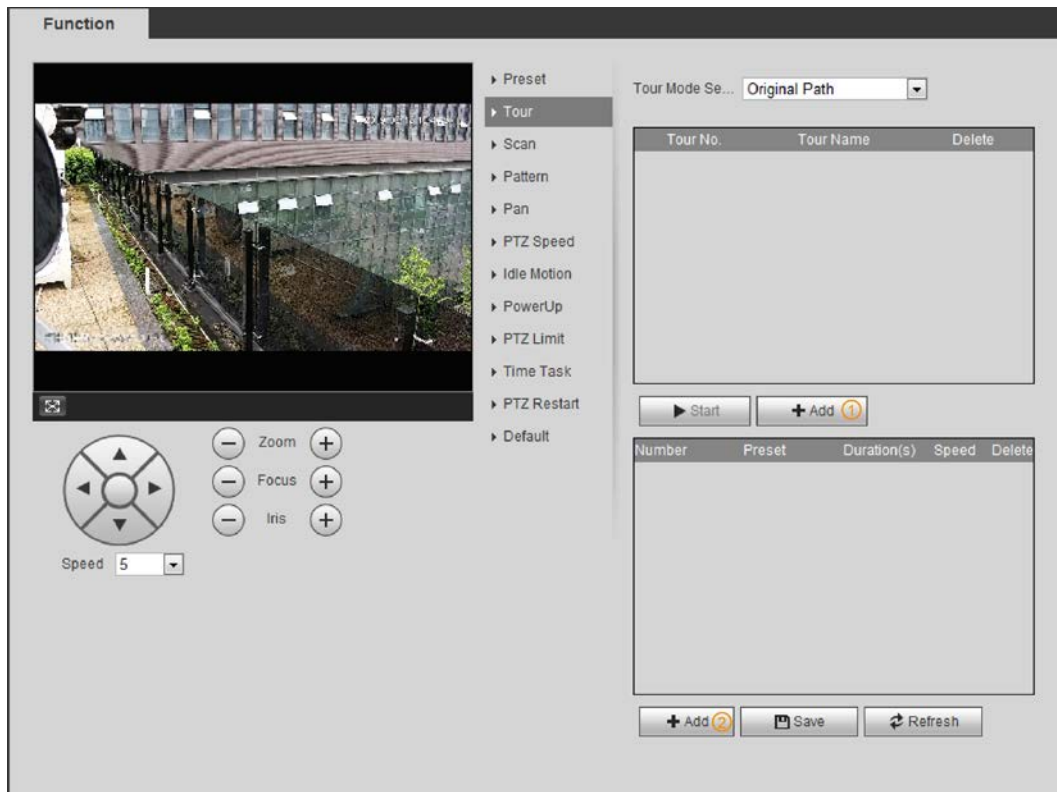
Prerequisites

You have set several presets.

Procedure

- Step 1** Select **Setting > PTZ settings > Function > Tour**.

Figure 4-9 Tour



Step 2 Click **Add**① to add tour.

Double-click the tour name to edit the name.

Step 3 Click **Add**② to add preset.

Double-click the duration to set the duration.

Step 4 Select the tour mode.

- Original path: The PTZ camera moves in the order of the selected presets.
- Shortest path: The PTZ camera ranks presets by distance, and moves in the optimal path.

Step 5 Click **Save**.

Step 6 Click **Start** to start touring.



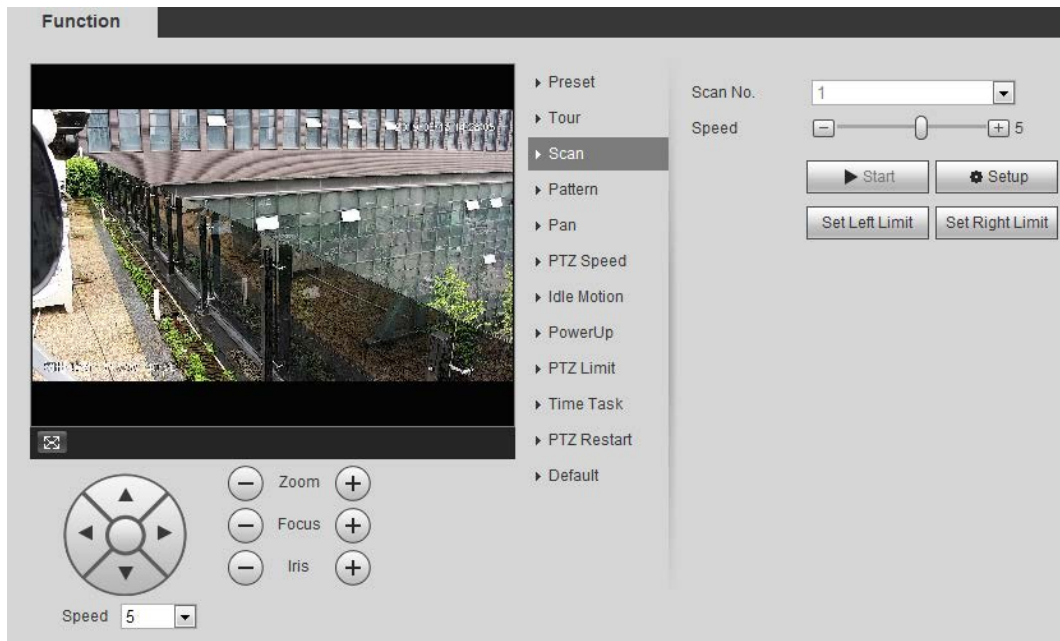
- If you operate PTZ during tour, the camera will stop tour.
- Click **Stop** to stop touring.

4.3.2.3 Scan

Scan means the camera moves horizontally at a certain speed between the configured left and right limits.

Step 1 Select **Setting > PTZ settings > Function > Scan**.

Figure 4-10 Scan



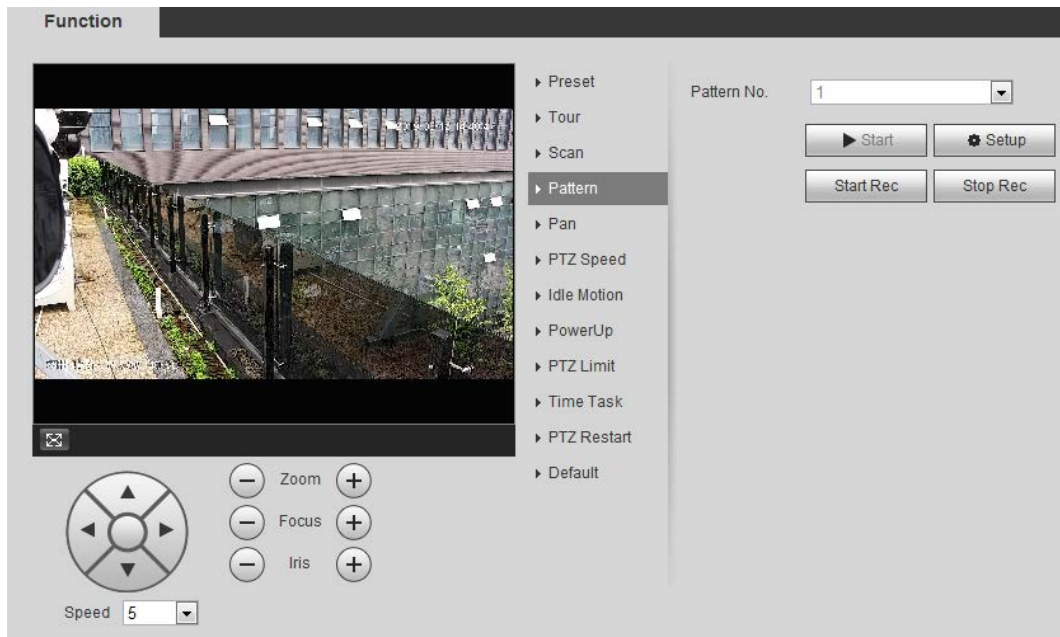
- Step 2** Select the scan number, and set the speed.
- Step 3** Click **Setup** to set left limit and right limit.
- 1) Click **Set Left Limit** to set the current position to be the left limit.
 - 2) Click **Set Right Limit** to set the current position to be the right limit.
- Step 4** Click **Start** to start scanning.
- Click **Stop** to stop scanning.

4.3.2.4 Pattern

Pattern means a recording of a series of operations that you make to the camera, and when pattern starts, the camera performs the operations repeatedly. The operations include horizontal and vertical movements, zoom and preset calling. Record and save the operations, and then you can call the pattern path directly.

- Step 1** Select **Setting > PTZ settings > Function > Pattern**.

Figure 4-11 Pattern



Step 2 Select the pattern number.

Step 3 Click **Setup**, and then click **Start Rec**. Adjust the parameters of direction, zoom, focus and iris according to the actual situation.

Step 4 Click **Stop Rec** to stop recording.

Step 5 Click **Start** to start patterning.

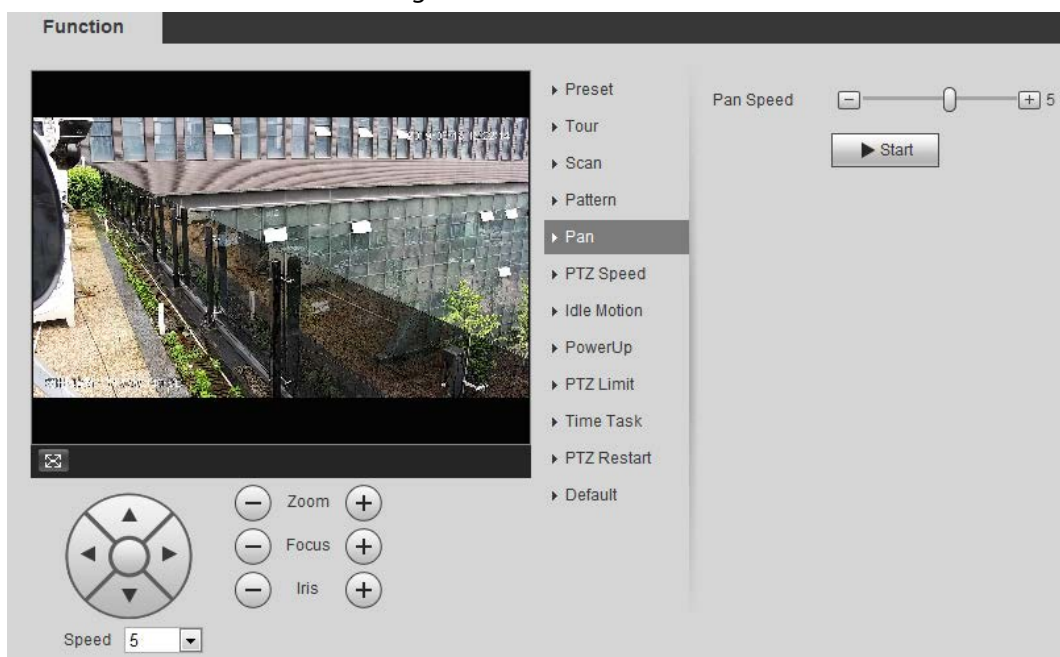
Step 6 Click **Stop** to stop patterning.

4.3.2.5 Pan

Enable Pan, the camera can realize continuous 360° horizontal rotation at a certain speed.

Step 1 Select **Setting** > **PTZ settings** > **Function** > **Pan**.

Figure 4-12 Pan



Step 2 Set the pan speed and click **Start**, and the camera starts horizontal rotation.

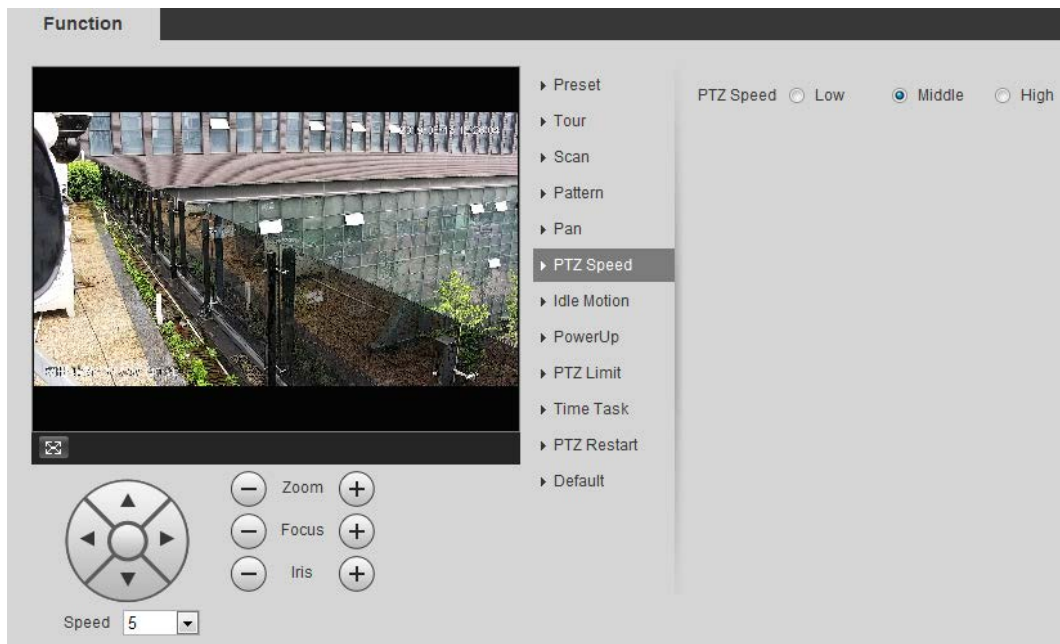
Click **Stop** to stop rotation.

4.3.2.6 PTZ Speed

PTZ speed means the rotation speed of the PTZ camera during touring, pattern, or auto tracking.

Step 1 Select **Setting > PTZ settings > Function > PTZ Speed**.

Figure 4-13 PTZ speed



Step 2 Select the PTZ speed: **Low**, **Middle**, and **High**.



Speed under the direction buttons refers to the rotation angle of the PTZ camera for each press of the direction button.

4.3.2.7 Idle Motion

Idle motion means that the PTZ camera implements the operation which is configured in advance when it does not receive any valid command within the set time.

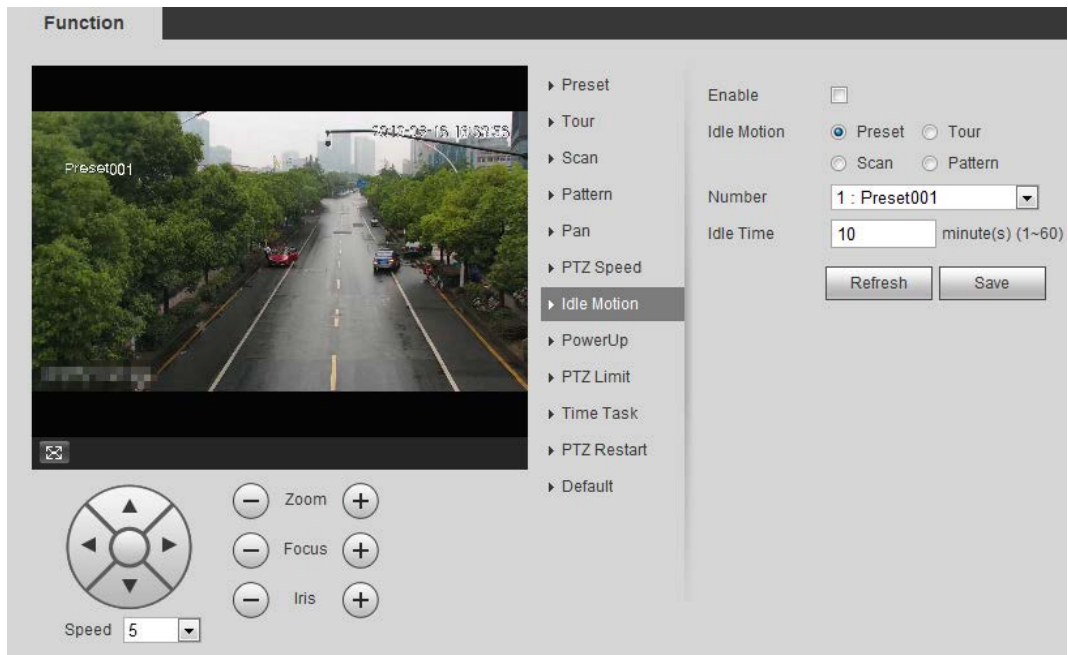
Prerequisites

You have configured the PTZ motions, including preset, scan, tour, or pattern.

Procedure

Step 1 Select **Setting > PTZ settings > Function > Idle Motion**.

Figure 4-14 Idle motion



Step 2 Select the **Enable** checkbox to enable the idle motion function.

Step 3 Select the idle motion and set the idle time.

You need to select the corresponding number for some selected idle motions, such as **Preset001**.

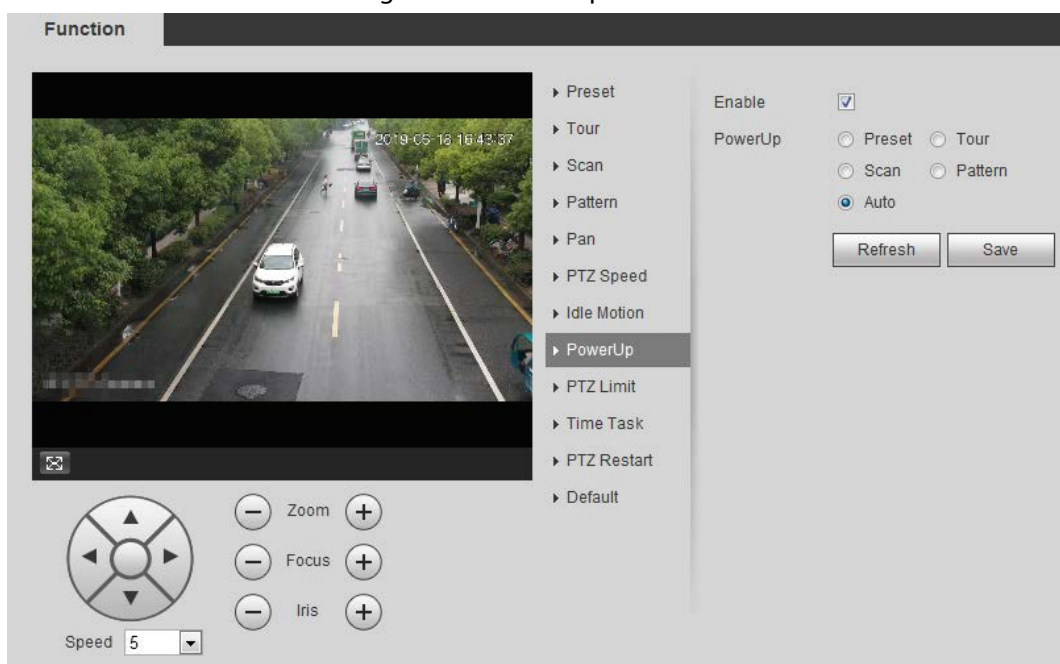
Step 4 Click **Save**.

4.3.2.8 PowerUp

After setting Powerup motion, the camera will perform the configured motion after it is powered on.

Step 1 Select **Setting > PTZ settings > Function > PowerUp**.

Figure 4-15 PowerUp



Step 2 Select the **Enable** checkbox to enable the power up function.

Step 3 Select the power up motion.



When you select **Auto**, the system will perform the last motion that is executed for more than 20 s before power-off.

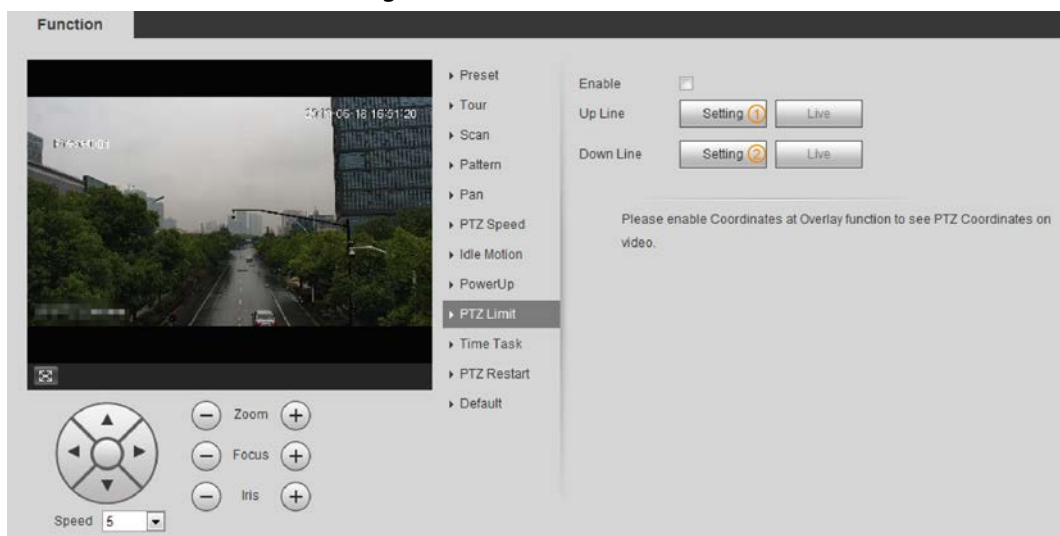
Step 4 Click **OK**.

4.3.2.9 PTZ Limit

After setting PTZ limit, the camera can only rotate within the configured area.

Step 1 Select **Setting > PTZ settings > Function > PTZ Limit**.

Figure 4-16 PTZ limit



Step 2 Adjust the direction buttons, and then click **Setting** ① to set the up line; click **Setting** ② to set the down line.

Click **Live** to view the configured up line and down line.

Step 3 Select the **Enable** checkbox to enable the PTZ limit function.

4.3.2.10 Time Task

After setting time task, the camera performs the motions during the configured period.

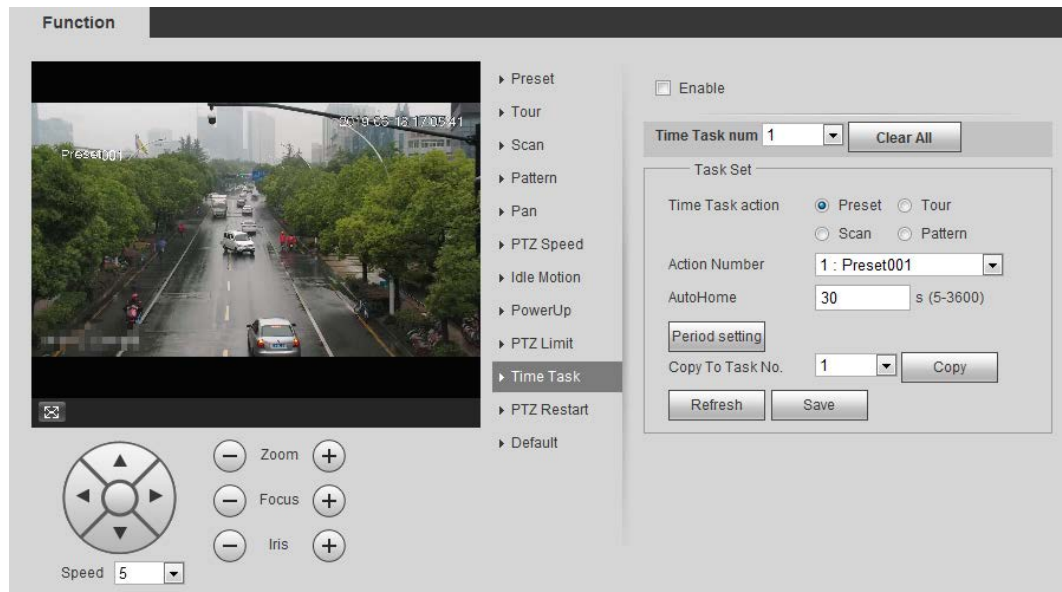
Prerequisites

You have configured the PTZ motions, including preset, scan, tour, and pattern.

Procedure

Step 1 Select **Setting > PTZ settings > Function > Time Task**.

Figure 4-17 Time task



Step 2 Select the **Enable** checkbox to enable time task function.

Step 3 Select the time task number.

Step 4 Select the time task action.

You need to select the corresponding action number for some selected time task actions.

Step 5 Set the auto home time in **AutoHome**.

AutoHome: When you call PTZ, the time task will be interrupted. After setting **AutoHome** time, the camera will resume the time task automatically.

Step 6 Click **Period setting** to set the time of the task, and then click **Save**.

For setting arm time, see "5.1.1.1 Setting Period".

Step 7 Click **Save**.

Related Operations

You can copy the configurations of existing task number to other task number.

1. Select the existing task number in **Time Task num**.
2. Select the task number to be configured in **Copy To Task No**.
3. Click **Copy**.
4. Click **Save**.

4.3.2.11 PTZ Restart

Step 1 Select **Setting > PTZ settings > Function > PTZ Restart**.

Figure 4-18 PTZ restart



Step 2 Click **PTZ Restart** to restart PTZ.

4.3.2.12 Default



Be careful when doing this operation. It will restore the camera to default configuration, and result in data loss.

Step 1 Select **Setting > PTZ settings > Function > Default**.

Figure 4-19 Default



Step 2 Click **Default** and the PTZ function is restored to default.

4.3.3 Calling PTZ

Click **PTZ** on **Live** interface, and the PTZ configuration panel is displayed. You can control PTZ and call PTZ function.

4.3.3.1 PTZ Control







You can rotate device, zoom image, and adjust iris through PTZ control or virtual joystick. See Figure 4-20 and Figure 4-21.

Figure 4-20 PTZ control



Figure 4-21 Joystick



- : Rotate PTZ direction through direction button. PTZ supports eight directions: left/right/up/down/upper left/upper right/bottom left/bottom right. Click , and draw a box in the image, PTZ will rotate, focus and quickly position the defined scene.
- : Rotate PTZ direction through joystick. Select and hold , and drag it to the direction that you need, then PTZ will move to the defined direction.
- Speed: Measure the rotation speed. The higher the speed value is, the faster the speed becomes.
- Zoom, focus and iris: Click  or  to adjust zoom, focus and iris.

4.3.3.2 PTZ Function

Select the PTZ function from the drop-down list to call the corresponding functions, including Scan, Preset, Tour, Pattern, Pan, Go to, Assistant and Light Wiper. See Figure 4-22. For details, see Table 4-6. Before calling PTZ function, see "4.3.2 Configuring PTZ Function" to configure PTZ function.



- If an external PTZ is connected to the camera, the configurations are valid only when the corresponding functions are available on the external PTZ.
- The range of PTZ function (such as preset and tour) depends on the PTZ protocol.

Figure 4-22 PTZ function

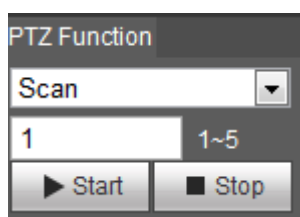


Table 4-6 Description of PTZ function

Parameter	Description
Scan	Set the scan number and click Start , the camera moves horizontally at a certain speed between the set left and right limit. Click Stop to stop scanning.
Preset	Set the preset number and click Go to , the camera quickly positions the corresponding preset.
Tour	Set the tour number and click Start , the camera moves in the order of the selected presets. Click Stop to stop touring.
Pattern	Set the pattern number and click Start , the camera moves continuously according to the operation recording. Click Stop to stop patterning. Operation recording includes the information of manual operation, focus and zoom.
Pan	Click Start , and the camera rotates 360° at a certain speed in horizontal direction.
Go to	Set the horizontal angle, vertical angle, and zoom. Click Go to to position a certain point accurately.
Assistant	Set the assistant number and click Aux On to enable the corresponding assistant function, and then you can adjust the camera. Click Aux Off to disable the corresponding assistant function.
Light/Wiper	Set the light or wiper of the camera. <ul style="list-style-type: none"> • Click Enable to enable light/wiper function. • Click Disable to disable light/wiper function.

4.4 Playback

This section introduces playback related functions and operations, including video playback and picture playback.



- Before playing back video, configure record time range, record storage method, record schedule and record control. For details, see "5.1.1.2.1 Setting Record Plan".
- Before playing back picture, configure snapshot time range, snapshot storage method, snapshot plan. For details, see "5.1.1.3.1 Setting Snapshot Plan".

4.4.1 Playback Interface

Click the **Playback** tab, and the **Playback** interface is displayed.

Figure 4-23 Video playback

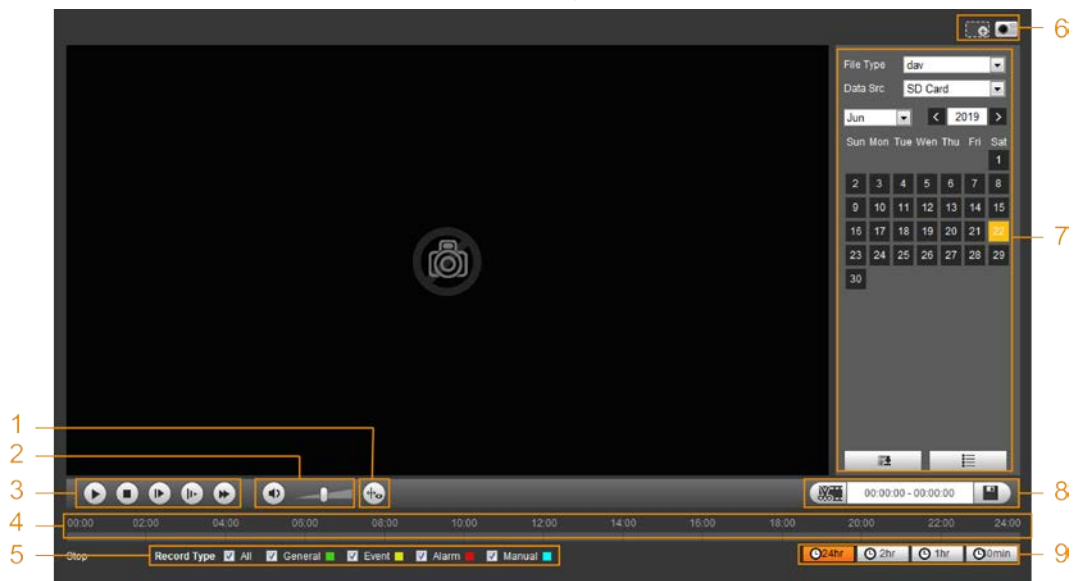


Figure 4-24 Picture playback

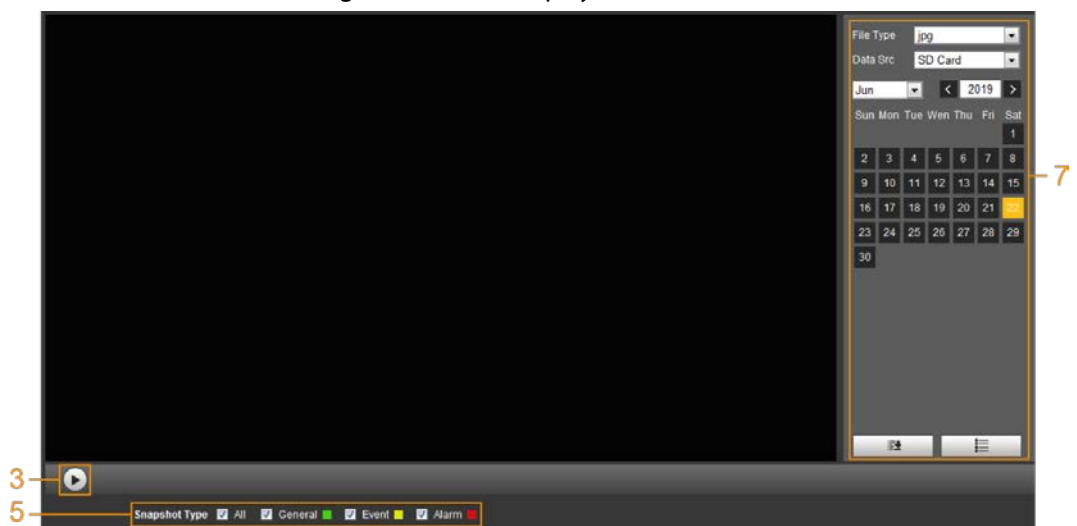















Table 4-7 Playback interface description

No.	Function	Description
1	Fisheye	Click  , you can select display mode according to the installation mode during playback.  This function is only available on fisheye cameras.
	Rules Info	Click  , intelligent rules and object detection box are displayed. It is enabled by default.  Rules Info is valid only when you enabled the rule during recording.
2	Sound	Controls the sound during playback. <ul style="list-style-type: none"> : Mute mode. : Vocal state. You can adjust the sound.
3	Play control bar	Controls playback. <ul style="list-style-type: none"> : Click the icon to play back recorded videos. : Click the icon to stop playing back recorded videos. : Click the icon to play the next frame. : Click the icon to slow down the playback. : Click the icon to speed up the playback.
4	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.
5	Record/Snapshot Type	Select the record type or snapshot type. <ul style="list-style-type: none"> Record type includes General, Event, Alarm, Manual. Snapshot type includes General, Event, Alarm.
6	Assistant	<ul style="list-style-type: none"> : You can zoom in or out video image of the selected area through two operations. : Click the icon to capture one picture of the current video, and it will be saved to the configured storage path.
7	Playback video	You can select the file type, data source, and record date.
8	Video clip	Clip a certain recorded video and save it. For details, see "4.4.3 Clipping Video".

No.	Function	Description
9	Time format of progress bar	Includes 4 time formats: . Take as an example, the whole progress stands for 24 hours.

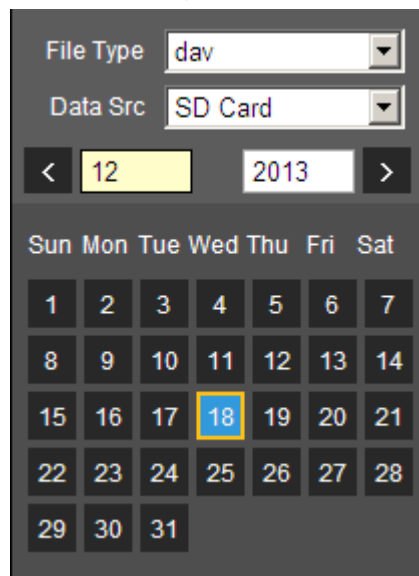
4.4.2 Playing back Video or Picture

This section introduces the operation of video playback and picture playback. This section takes video playback as an example.

Step 1 Select **dav** from the **Record Type** drop-down list and **SD card** from the **Data Src** drop-down list.

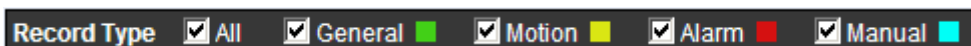
Select **jpg** from **Record Type** drop-down list when playing back pictures, and you do not need to select data source.

Figure 4-25 File type selection



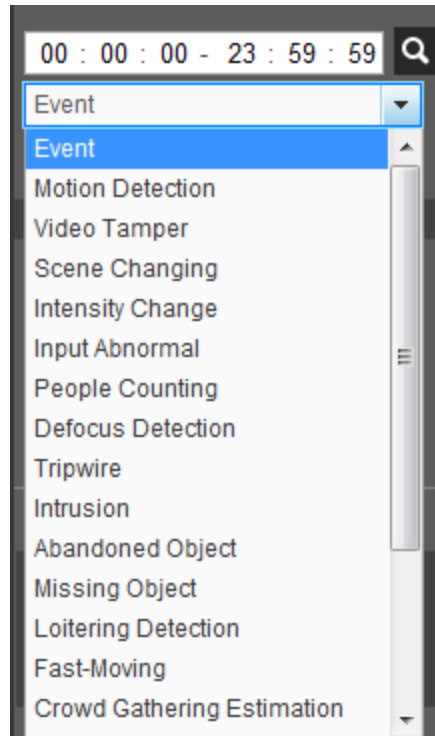
Step 2 Select the record type in **Record Type**.

Figure 4-26 Record type selection



When selecting **Event** as the record type, you can select the specific event types from the playback file list, such as **Motion Detection**, **Video Tamper** and **Scene Changing**.

Figure 4-27 Specific event types



Step 3 Select the month and year of the video that you want to play.



Those dates with blue color indicate there were videos recorded in those days.

Step 4 Play video.


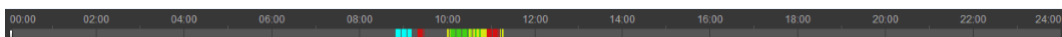
- Click  in the control bar.
The system plays the recorded video of the selected date (in the order of time).
- The system plays the recorded video of the selected date (in the order of time).
- Click any point in the colored area on the progress bar.
The playback starts from that moment.

Figure 4-28 Progress bar





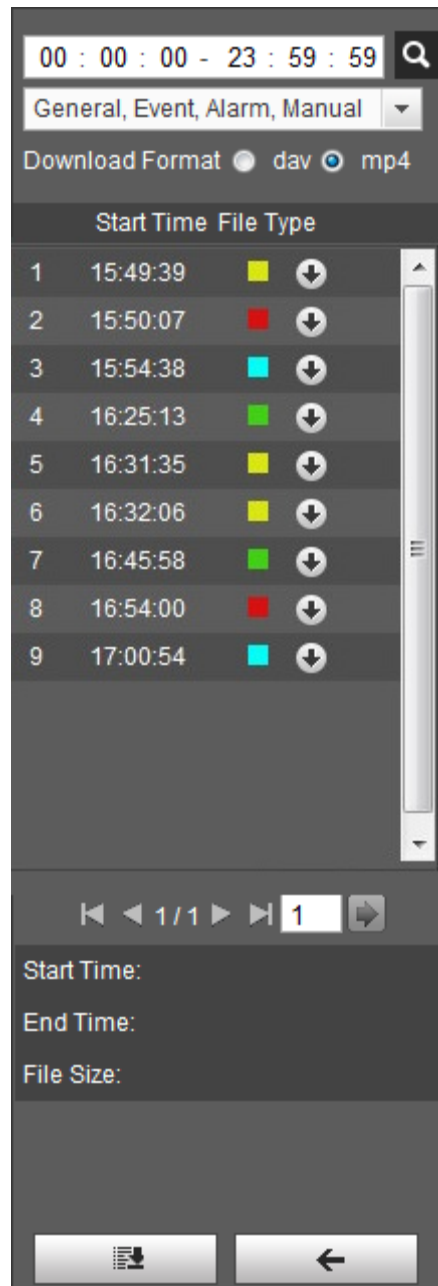
- Click , the video files of the selected date would be listed. Enter the start time and end time, and then click  to search all files between the start time and end time. Double-click the file in the list, and the system plays the video and displays file size, starting time, and ending time.

Figure 4-29 Playback file list



4.4.3 Clipping Video



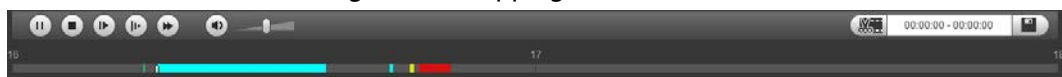


- Step 1 Click , the video files of the selected date are listed.
- Step 2 Select **dav** or **mp4** in **Download Format**.
- Step 3 Click on the progress bar to select the start time of the target video, and then click . See Figure 4-30.

Figure 4-30 Clipping video



- Step 4 Click again on the progress bar to select the end time of the target video, and then click .

- Step 5** Click  to download the video.
The system will prompt that it cannot play back and download at the same time.
- Step 6** Click **OK**.
The playback stops and the clipped file is saved in the configured storage path. For the configuration of storage path, see "4.5.2.5 Path".



4.4.4 Downloading Video or Picture

Download video or picture to a defined path. You can download single video or picture file, or download them in batches. This section takes downloading video as an example.



- Playback and downloading at the same time is not supported.
- Operations might vary with different browsers.
- For details of viewing or setting storage path, see "4.5.2.5 Path".

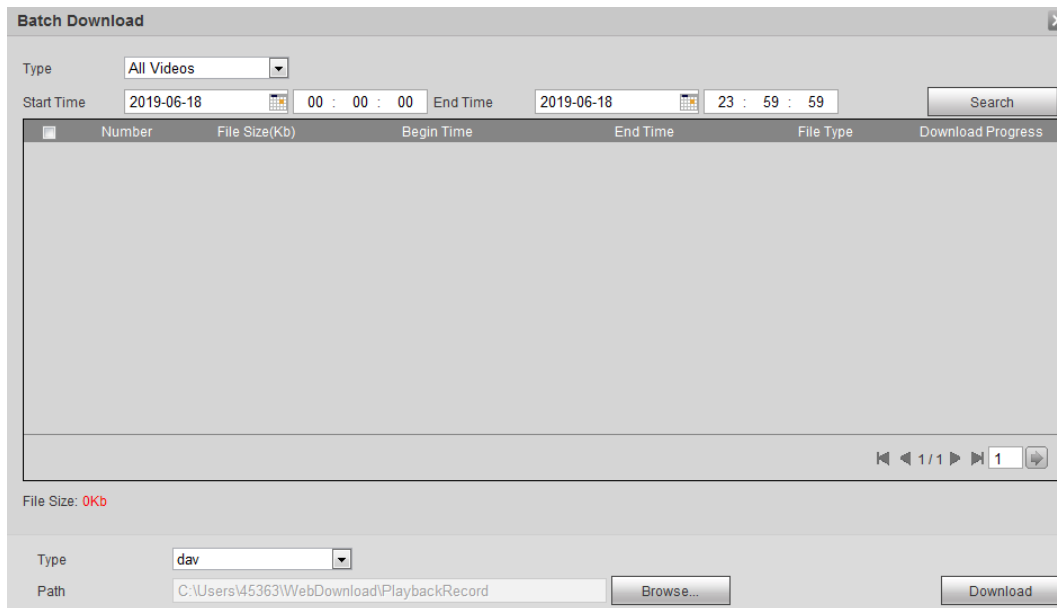
4.4.4.1 Downloading a Single File

- Step 1** Select **dav** from the **Record Type** drop-down list and **SD card** from the **Data Src** drop-down list.
Select **jpg** from **Record Type** drop-down list when playing back pictures, and you do not need to select data source.
- Step 2** Click , the video files of the selected date are listed. See Figure 4-29.
- Step 3** Select **dav** or **mp4** in **Download Format**. Click  next to the file to be download.
The system starts to download the file to the configured path. When downloading pictures, you do not need to select the download format.

4.4.4.2 Downloading Files in Batches

- Step 1** Click  on the playback interface.

Figure 4-31 Batch download



- Step 2** Select the record type, set the start time and end time, and then click **Search**.
The searched files are listed.
- Step 3** Select the files to be downloaded, select **dav** or **mp4** from the **Format** drop-down list, and then set the storage path. Click **Download**.
The system starts to download the file to the configured path. When downloading picture, you do not need to select the download format.

4.5 Camera

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



Camera parameters of different devices might vary.

4.5.1 Conditions

Configure camera parameters of the camera to ensure surveillance goes properly.

4.5.1.1 Conditions

Configure camera parameters according to the actual situation, including picture, exposure, backlight and white balance.

4.5.1.1.1 Interface Layout

Configure camera parameters to improve the scene clarity, and ensure that surveillance goes properly. See Figure 4-32.

- Under profile, you can select between 9 different styles, such as normal, day, night or flowing light mode. Parameters (such as contrast and saturation) will change to match the style. You can

also further modify the configurations for select modes (such as picture, exposure and backlight) after changing the main style. Flowing light is suitable for situations where there is slight light, and the panoramic function is unable to effectively detect targets.



- ◇ After switching to flowing light, the mode in the exposure menu is automatically set to manual. The shutter time is adaptive, working at a maximum speed of 333 ms.
- ◇ By default the backlight is off. The wide dynamic effect start or not can be determined by identifying the overexposure in the picture. This gives you control over overexposure in the picture.
- Camera with PTZ function supports zoom, focus and iris operations. See Figure 4-33. Configure speed, click direction button, **−** and **+** to adjust the direction, zoom, focus and iris and so on, to adjust the camera to the proper position.

Figure 4-32 Camera conditions

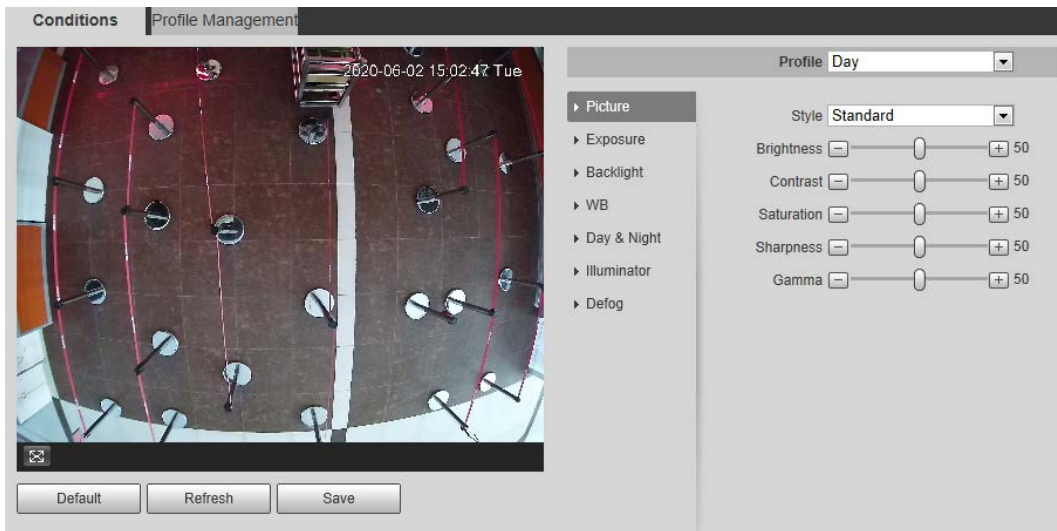
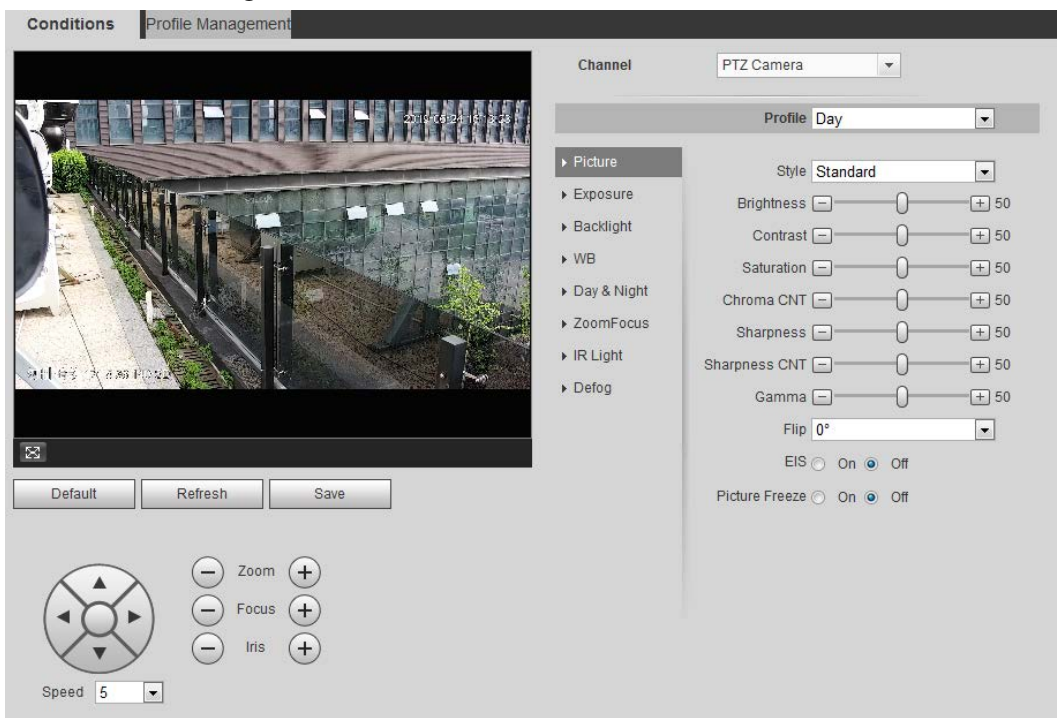


Figure 4-33 Camera conditions (PTZ camera)

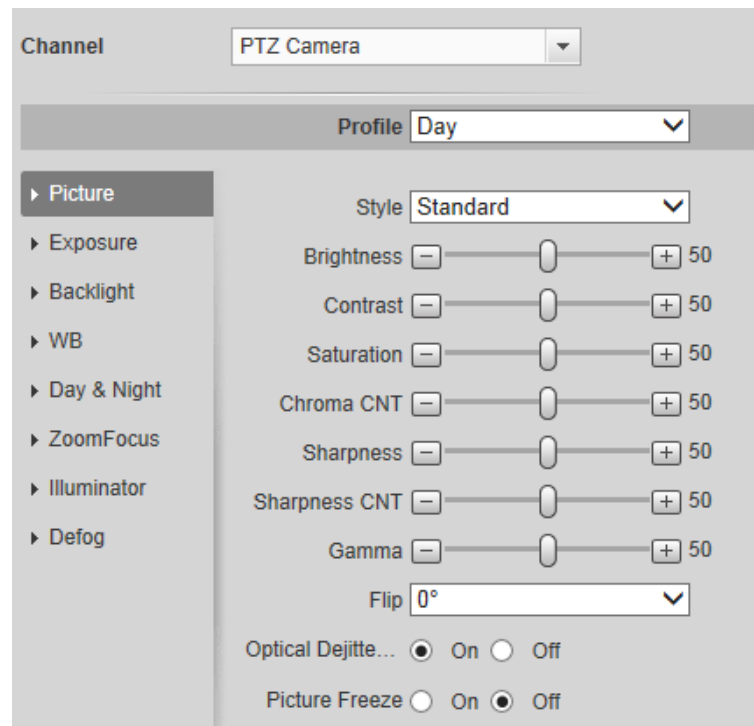


4.5.1.1.2 Picture

You can configure picture parameters as needed.

Step 1 Select **Setting > Camera > Conditions > Conditions > Picture**.


Figure 4-34 Picture



Step 2 Configure picture parameters.

Table 4-8 Description of picture parameters

Parameter	Description
Style	Select the picture style from soft, standard and vivid. <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	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.
Contrast	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.
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.

Parameter	Description
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.
Mirror	Select On , and the picture would display with left and right side reversed.
Flip	Changes the display direction of the picture, see the options below. <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.  For some models, please set the resolution to be 1080p or lower when using 90° and 180°. For details, see "4.5.2.1 Video".
EIS	Corrects the device shaking with difference comparison algorithm and improves the image clarity, effectively solves the picture shaking problem.
Optical Dejitering	The lens vibration is sensed by the gyroscope sensor, and the corresponding compensation is calculated using the intelligent anti-shake algorithm. The movable parts inside the lens are driven to offset the vibration, which greatly reduces blurring of the image caused by the vibration.
Picture Freeze	When you call a preset, the image displays the preset location, not the rotation image.

Step 3 Click **Save**.

4.5.1.1.3 Exposure

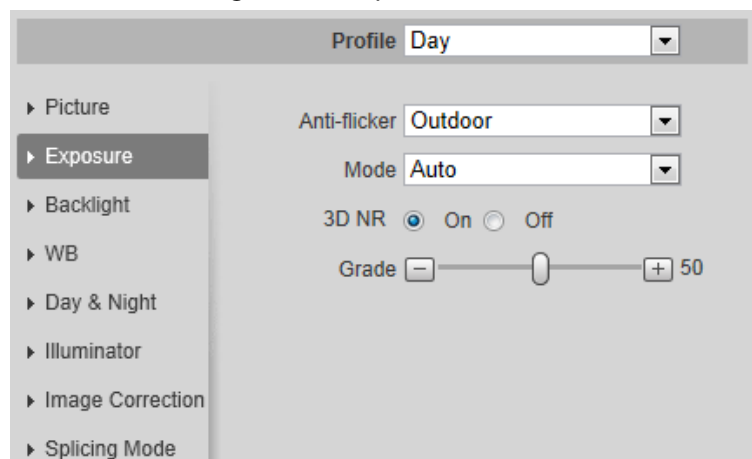
Configure iris and shutter to improve image clarity.



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


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

Figure 4-35 Exposure



Step 2 Configure exposure parameters.

Table 4-9 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. ● Iris priority: The iris value is set to a fixed value, and the device adjusts shutter value then. 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 Gain priority or Shutter priority in the Mode list.</p>
Exposure Comp	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.

Parameter	Description
Shutter range	When selecting Shutter Priority or Manual in Mode , and setting Customized Range in Shutter , you can set shutter range, and the unit is ms.
Gain	When selecting Gain Priority or Manual in Mode , you can set shutter range. With minimum illumination, the camera increases Gain automatically to get clearer images.
Iris	When selecting Aperture Priority in Mode , you can set iris range.
Auto Iris	This configuration is available only when the camera is equipped with auto-iris lens. <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.
2D NR	Average single-frame dots and other dots around to reduce noise.
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.
Grade	This configuration is available only when the 3D DNR is enabled. The higher the DNR level is, the better the result will be.

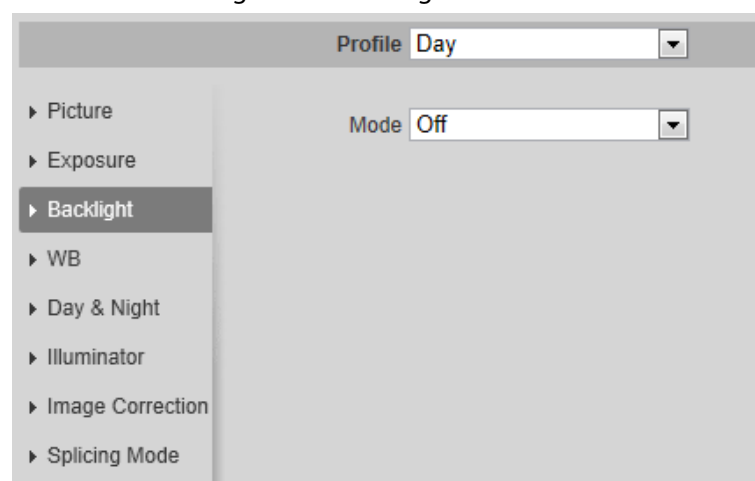
Step 3 Click **Save**.

4.5.1.1.4 Backlight

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


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

Figure 4-36 Backlight



Step 2 Configure backlight parameters.

Table 4-10 Description of backlight parameters

Backlight mode	Description
Auto	The system adjusts image brightness according to ambient lighting condition automatically to ensure image clarity.
BLC	<p>Enable BLC, the camera can get clearer image of the dark areas on the target when shooting against light. You can select Default mode or Customized mode.</p> <ul style="list-style-type: none"> When in Default mode, the system adjusts exposure according to ambient lighting condition automatically to ensure the clarity of the darkest area. When in 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.
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>There might be a few seconds of video loss when the device is switching to WDR mode from other mode.</p>
HLS	Enable HLS 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 HLS effect will be.

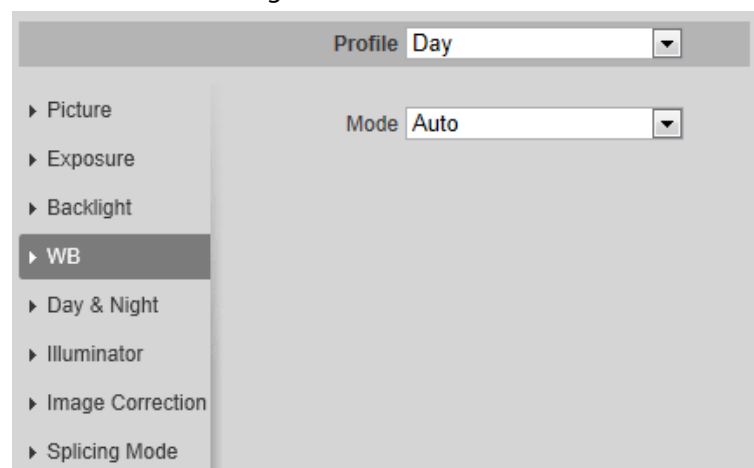
Step 3 Click **Save**.

4.5.1.1.5 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 **Setting** > **Camera** > **Conditions** > **Conditions** > **WB**.

Figure 4-37 WB



Step 2 Configure WB parameters.

Table 4-11 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.
Regional Custom	The system compensates WB only to the set area according to color temperature to ensure color precision.

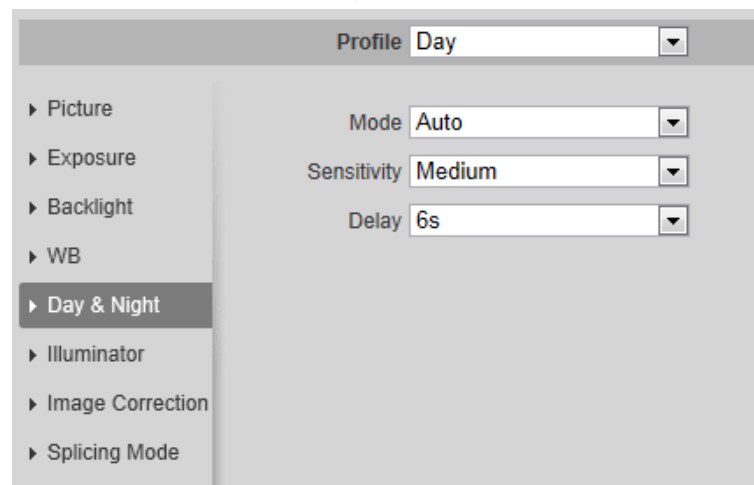
Step 3 Click **Save**.

4.5.1.1.6 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 **Setting > Camera > Conditions > Conditions > Day & Night**.

Figure 4-38 Day and night



Step 2 Configure day and night parameters.

Table 4-12 Description of day and night parameters

Parameter	Description
Mode	<p>You can select device display mode from Color, Auto, and B/W.</p>  <p>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.</p> <p>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.</p> <p>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>

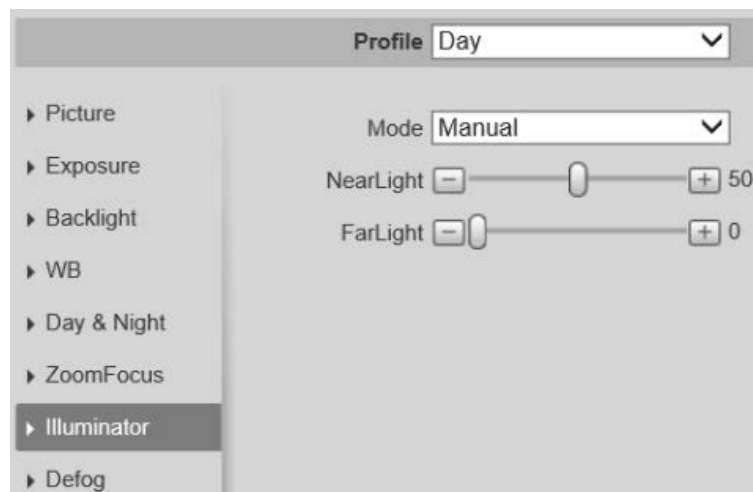
Step 3 Click **Save**.

4.5.1.1.7 Zoom and Focus

Initialize lens to adjust zoom and focus. Only PTZ camera supports lens initialization.

Step 1 Select **Setting** > **Camera** > **Conditions** > **Conditions** > **ZoomFocus**.

Figure 4-39 Zoom and focus



Step 2 Configure zoom and focus parameters.

Table 4-13 Description of zoom and focus parameters

Parameter	Description
Digital Zoom	<p>Select On to enable digital zoom function.</p> <p>After the optical zoom reached the upper limit, enable digital zoom function, you still can do digital zoom operation.</p>

Parameter	Description
Zoom Speed	Adjusts zoom speed. The higher the value is, the higher the speed will be.
Mode	Sets focus mode. <ul style="list-style-type: none"> • Auto: When image moves or object changes in the scene, the camera will focus automatically. • Semi Auto: Click or corresponding to Focus or Zoom, the camera will focus. Calling preset, positioning accurately or rotating PTZ also will trigger focus. • Manual: Click or corresponding to Focus to adjust the focus.
Focus Limit	When the focus length is too short, the camera will focus on the dome cover. Sets the shortest focus distance to avoid focusing on the dome cover. You can also change the focus speed by changing focus length.
Sensitivity	The sensitivity of triggering focus. The higher the value is, the easier the focus will be triggered.

Step 3 Click **Save**.



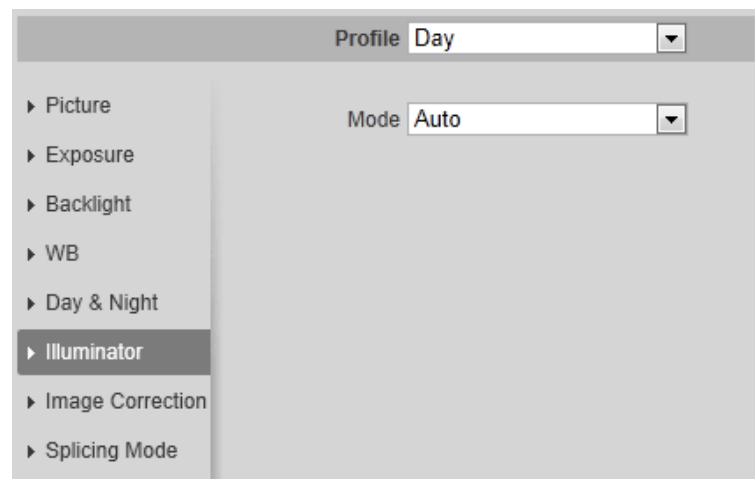
Click **Lens Initialization**, the lens will adjust the zoom and focus parameters.

4.5.1.1.8 Illuminator

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

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

Figure 4-40 Illuminator



Step 2 Configure illuminator parameters.

Table 4-14 Description of illuminator parameters

Illuminator	Description	
Fill Light	<p>Set Fill Light for sound and siren cameras.</p> <ul style="list-style-type: none"> IR Mode: Enable the IR illuminator, and the white light is disabled. White Light: Enable the white light, and the IR illuminator is disabled. Smart illumination. They system will switch the illuminators according to the actual condition. When the ambient light reaches the threshold of IR illuminator, the IR illuminator is enabled. The white light is enabled when the target appears in surveillance area, disabled when the target is out of the surveillance area, and then the IR illuminator is enabled according to the ambient light. <p>When selecting Smart Illumination as Fill Light, you need to set the illuminator delay. It is 60 seconds by default, and the range is 30–300 seconds.</p>	
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.
	Smart IR	
	ZoomPrio	<p>The system adjusts the illuminator intensity automatically according to the change of the ambient light.</p> <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 **Save**.

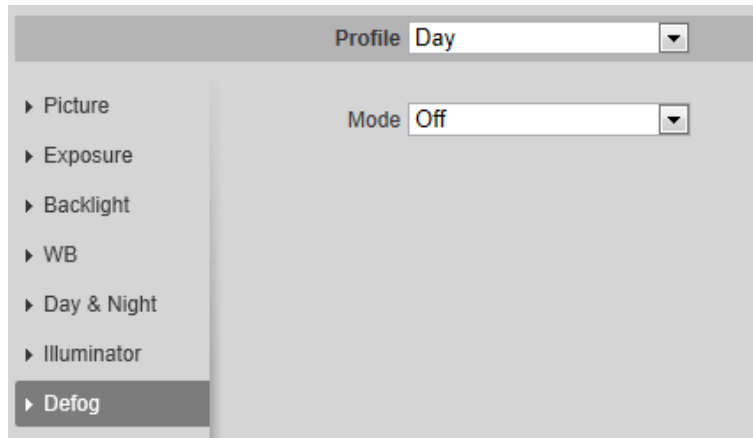
4.5.1.1.9 Defog

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

image clarity.

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

Figure 4-41 Defog



Step 2 Configure defog parameters.

Table 4-15 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 **Save**.

4.5.1.1.10 Fisheye

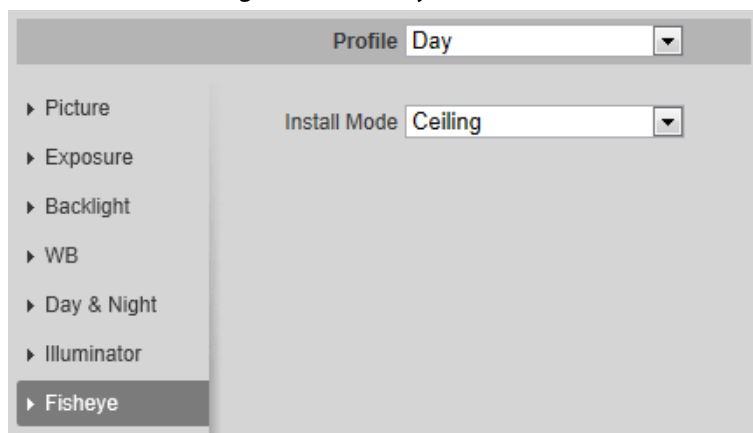
Select install mode and record mode according to the actual installation scene. When the camera accesses the platform with corrective stream, the platform displays the corrective image.



This function is only available on fisheye device.

Step 1 Select **Setting > Camera > Conditions > Conditions > Fisheye.**

Figure 4-42 Fisheye



Step 2 Set install mode and record mode.

Table 4-16 Description of fisheye parameters

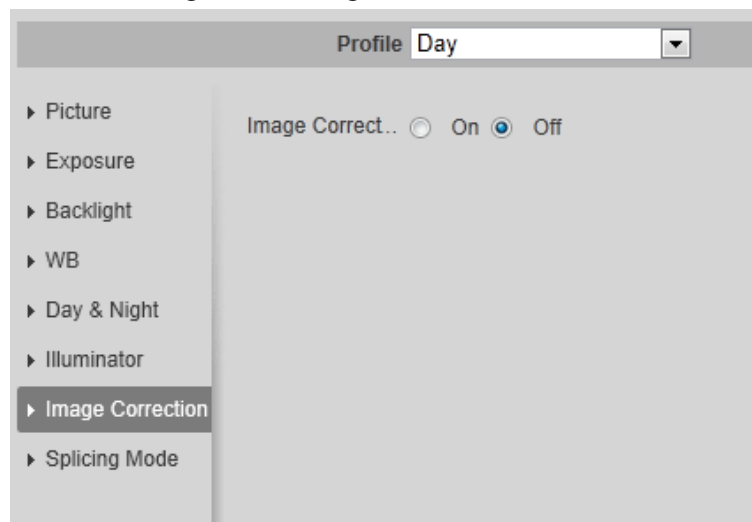
Parameter	Description
Install Mode	You can select Ceiling , Wall , or Ground .
Record Mode	<ul style="list-style-type: none"> • 1O: The original image before correction. • 1P: 360°rectangular panoramic image. • 2P: When the install mode is Ceiling or Ground, you can set this mode. Two associated 180° rectangular image screens, and at any time, the two screens form a 360° panoramic image. • 1R: Original image screen + independent sub-screen. You can zoom or drag the image in all the screens. • 2R: Original image screen + two independent sub-screens. You can zoom or drag the image in all the screens. • 4R: Original image screen + four independent sub-screens. You can zoom or drag the image in all the screens. • 1O + 3R: Original image screen + three independent sub-screens. You can zoom or drag the image in original image screen, and move the image (upper and lower) in sub-screens to adjust the vertical view.

Step 3 Click **Save**.

4.5.1.1.11 Image Correction

Enable the image correction function to correct some bent objects (such as roads) in the image of panoramic splicing cameras, but it will influence the field of view.

Figure 4-43 Image correction

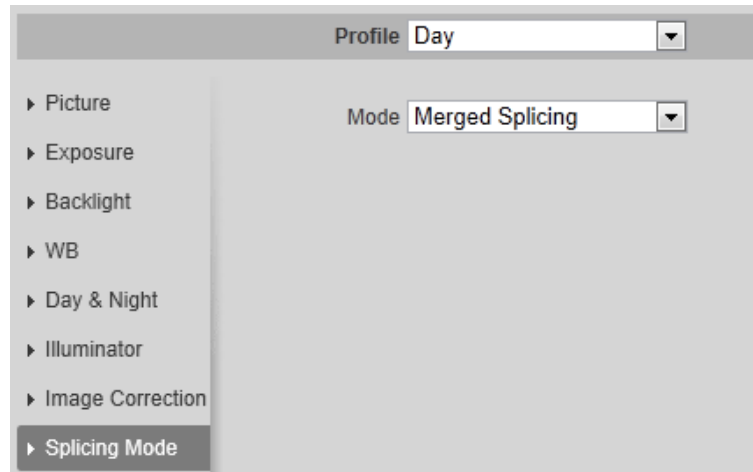


- If the camera has multiple sensors, the image correction function will only displayed when the number of splicing sensors is 4 or less.
- When the device enables image correction, intelligent event and sub stream 2 are closed automatically.

4.5.1.1.12 Splicing Mode

Select the splicing mode to splice several images of different lens to a panoramic image. You can select **Merged Splicing** or **Splicing for Mode**.

Figure 4-44 Splicing mode



4.5.1.2 Profile Management

The surveillance system works in different ways as profile configured in different time.

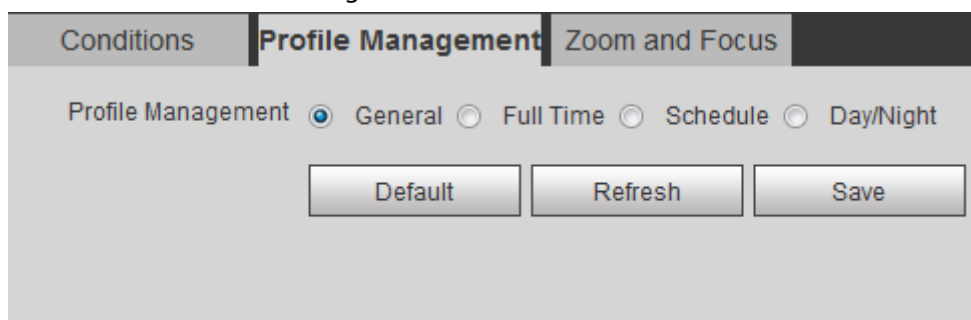
Step 1 Select **Setting > Camera > Conditions > Profile Management**.

The **Profile Management** interface is displayed.

Step 2 Manage profile.

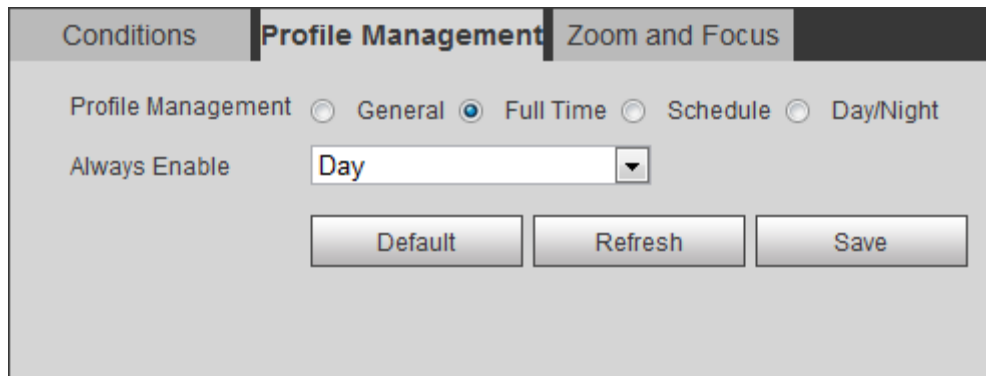
- When **Profile Management** is set as **General**, the surveillance system works under **General** configuration.

Figure 4-45 General



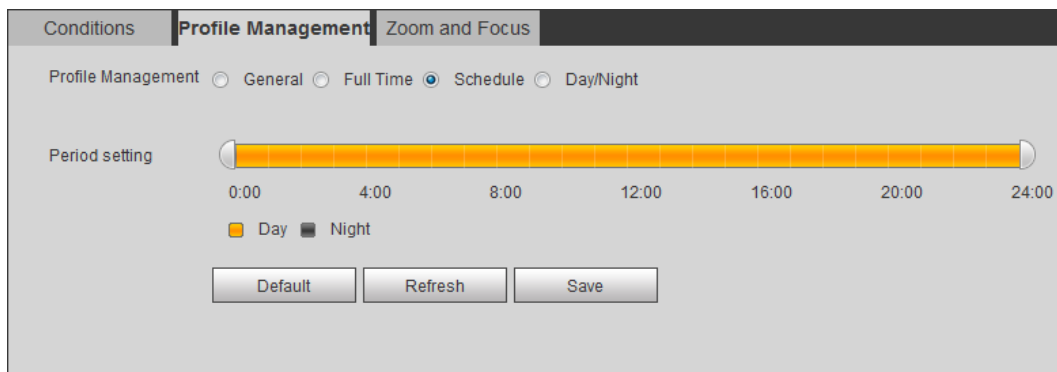
- When **Profile Management** is set as **Full Time**, you can select **Day** or **Night** in the **Always Enable** list, the surveillance system works under **Always Enable** configuration.

Figure 4-46 Full time



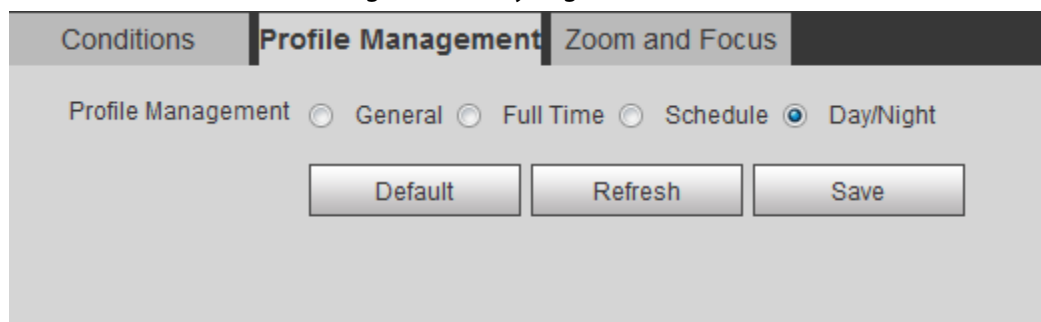
- When **Profile Management** is set as **Schedule**, you can drag the slide block to set certain time as **Day** or **Night**. For example, set 8:00–18:00 as day, and 0:00–8:00 and 18:00–24:00 as night.

Figure 4-47 Schedule



- When **Profile Management** is set as **Day & Night**, the surveillance system works under **Day & Night** configuration.

Figure 4-48 Day/Night



Step 3 Click **Save**.

4.5.1.3 Zoom and Focus

You can adjust image clarity through auto or manual focus; and adjust the image size through zoom. For details, see "4.2.4.2 Zoom and Focus".

4.5.1.4 Splicing

When the panorama contains multiple images captured by different lenses, enable this function. Before splicing, make sure that the surveillance scene is large and there are no objects blocking the


camera from taking a clear picture, otherwise, the splicing might fail.

Step 1 Select **Setting > Camera > Conditions > Splicing**.

Figure 4-49 Splicing



Step 2 Select the lenses that need to be spliced.

When splicing the image through selecting lenses, you need to select the continuous splicing screens. The screen with the icon  (deeper color) is the first screen of the splicing. You can select any screen as the first one, and then select the following screens continuously. The system supports the splicing of 2 lenses to 8 lenses.



- This function is available on select models. And it is all sensors splicing by default.
- For Multi-Sensor Panoramic + PTZ Camera, the 4-sensor device supports 2 to 4 lenses splicing; the 6-sensor device supports 2 to 6 lenses splicing; the 8-sensor device supports 2-8 lenses splicing.

Step 3 Click **Start**.

The system starts to splice the image.

- Some cameras restart automatically after splicing is complete, You can view the results of the splicing in the **Live** window.
- Some cameras display splicing live window after splicing is complete. Click **OK**, and then the default window appears. Click **OK** and the splicing will take effect.

4.5.2 Setting Video 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.

4.5.2.1 Video

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

Step 1 Select **Setting > Camera > Video > Video**.

Figure 4-50 Video

The screenshot shows a configuration window with tabs for Video, Snapshot, Overlay, and Path. The Video tab is active, displaying settings for Main Stream and Sub Stream.

Main Stream Settings:

- Encode Mode: H.265
- Encoding Strategy: AI Codec
- Resolution: 3840*2160(3840x2160)
- Frame Rate(FPS): 20
- Bit Rate Type: CBR
- Reference Bit Rate: 1441-8192Kb/S
- Bit Rate: Customized
- I Frame Interval: 40
- Watermark Settings: (Watermark Character: DigitalCCTV)
- Stream Smooth: Slider (46)

Sub Stream Settings:





- Enable: (Sub Stream 1)
- Encode Mode: H.265
- Resolution: 704*576(D1)
- Frame Rate(FPS): 20
- Bit Rate Type: CBR
- Reference Bit Rate: 156-1280Kb/S
- Bit Rate: 512 (Kb/S)
- I Frame Interval: 40 (20-150)
- Stream Smooth: Slider (46)





Buttons at the bottom: Default, Refresh, Save.

Step 2 Configure video parameters.

Table 4-17 Description of video parameters

Parameter	Description
Enable	<p>Select the Enable checkbox to enable sub stream. It is enabled by default.</p> <ul style="list-style-type: none"> You can enable multiple sub streams simultaneously. When the device enables image correction, intelligent event and sub stream 2 are closed automatically.
Encode Mode	<p>Select encode mode.</p> <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.

Parameter	Description
Encoding Strategy	<p>Select the encoding strategy as needed.</p> <ul style="list-style-type: none"> • General: Disable smart codec. • Smart Codec: Enable smart codec to improve video compressibility and save storage space. It is applicable to static scenes. • AI Code: When the bandwidth and storage space are restricted, the camera will select the encoding strategy with lower bit rate to save storage space. It is applicable to dynamic scenes. <p>After AI codec is enabled, Bit Rate Type is CBR, and it cannot be changed. Comparing with general mode, AI codec has lower bite rate. This function is only available on cameras with AI functions.</p> <p> After smart codec and AI codec are enabled, the camera would stop supporting the third stream, ROI, and smart event detection, and the actual interface shall prevail.</p>
Resolution	<p>The resolution of the video. The higher the value is, the clearer the image will be, but the bigger the bandwidth will be required.</p>
Video Clip	<p>This function is available only for sub stream 2 of some select models.</p> <ul style="list-style-type: none"> • Main stream <ol style="list-style-type: none"> 1. Select the resolution as needed, and click  next to Resolution. The Area interface is displayed. 2. Clip the image on the Area interface, and then click Save. View the clipped video on Live interface. • Sub stream 2 <ol style="list-style-type: none"> 1. Select Video Clip, and click . 2. View the clipped video on Live interface (only the live interface of sub stream 2 displays the clipped area).
Frame Rate (FPS)	<p>The number of frame in one second of video. The higher the value is, the clearer and smoother the video will be.</p>
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. The better the quality is, the larger the bandwidth will be requested.</p>

Parameter	Description
Reference Bit Rate	The most suitable bit rate value range recommended to user according to the defined resolution and frame rate.
Max Bit Rate	This parameter can be configured only when the Bit Rate Type is set as VBR . 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.
Bit Rate	This parameter can be configured only when the Bit Rate Type is set as CBR . Select bit rate value in the list according to actual condition. You can also customize the value.
I Frame Interval	This parameter can be configured only when Encoding Strategy is set as General or AI Codec . The number of P frames between two I frames. The smaller the value, the higher the image quality, and the range changes as Frame Rate(FPS) changes. It is recommended to set I Frame Interval twice as big as Frame Rate(FPS) . When selecting AI Codec in Encoding Strategy , you can only select the value same as or twice as big as Frame Rate(FPS) .
SVC	Scaled video coding, 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. <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 Settings	You can verify the watermark to check if the video has been tampered. <ol style="list-style-type: none"> 1. Select the checkbox to enable watermark function. 2. The default character is DigitalCCTV.
Watermark Character	
Stream Smooth	Click  ,  or drag  to set the value of Stream Smooth . The higher the value is, the less smooth the stream, but the higher the image definition; the lower the value is, the more smooth the stream, but the lower the image definition.  The value of Stream Smooth is 100 by default.

Step 3 Click **Save**.

4.5.2.2 Snapshot

You can configure snapshot parameters, including snapshot type, image size, quality and interval.

Step 1 Select **Setting** > **Camera** > **Video** > **Snapshot**.

Figure 4-51 Snapshot

Step 2 Configure snapshot parameters.

Table 4-18 Description of snapshot parameter

Parameter	Description
Snapshot Type	You can select General and Event . <ul style="list-style-type: none"> • General: The system takes snapshot as scheduled. For details, see "4.7.2 Setting Schedule". • Event: The system takes snapshot when the video detection, audio detection, event, or alarm is triggered. This function requires the corresponding snapshot being enabled.
Image Size	The same resolution with main stream.
Quality	Configures the snapshot quality. There are six levels of Image quality, and the sixth is the best.
Interval	Configures the snapshot frequency. Select Customized , and then you can configure snapshot frequency manually.

Step 3 Click **Save**.

4.5.2.3 Overlay

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

4.5.2.3.1 Configuring Privacy Masking

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



Functions might vary with different models.

Privacy Masking (1)

Step 1 Select **Setting > Camera > Video > Overlay > Privacy Masking**.

Figure 4-52 Privacy masking (1)

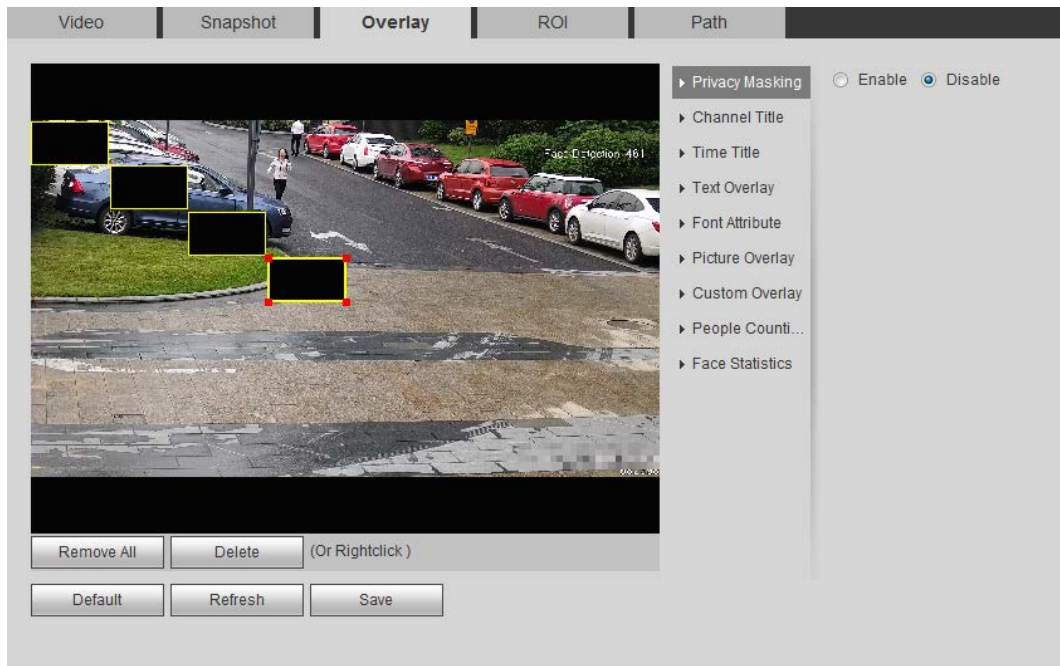
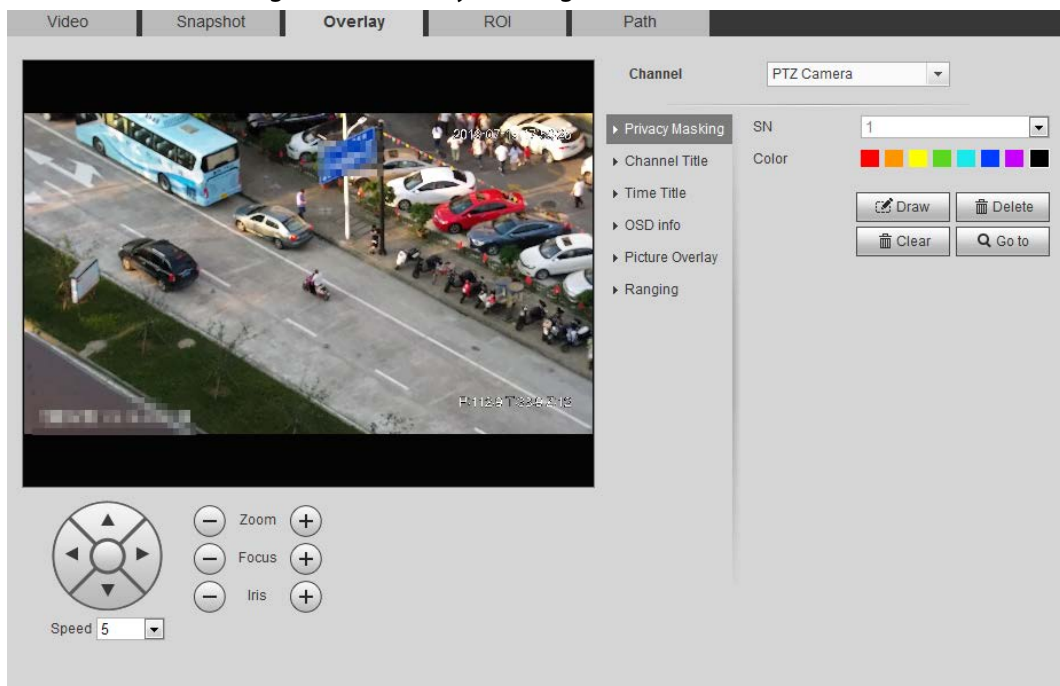


Figure 4-53 Privacy masking (PTZ dome)



Step 2 Configure privacy masking.

- PTZ dome
 1. Select the SN.
 2. Adjust the live image to the proper location through PTZ, select the color, and then click **Draw**. Press the mouse button to draw rectangles. The configuration takes effect immediately.
 3. Other operations:
 - ◇ Select the SN, and click **Go to**, the speed dome rotates to the masked area.
 - ◇ Select the SN, and click **Delete** to delete the masking rectangles.
 - ◇ Click **Clear**, and the click **OK** to clear all masking rectangles.

- Other cameras
 1. Select **Enable**, and then drag the block to the area that you need to cover.



- ◇ You can drag 4 rectangles at most.
- ◇ Click **Remove All** to delete all the area boxes; select one box, and then click **Delete** or right-click to delete it.

2. Adjust the size of the rectangle to protect the privacy.
3. Click **Save**.

Privacy Masking (2)

You can select the type of the masking from **Color Lump** and **Mosaic**.

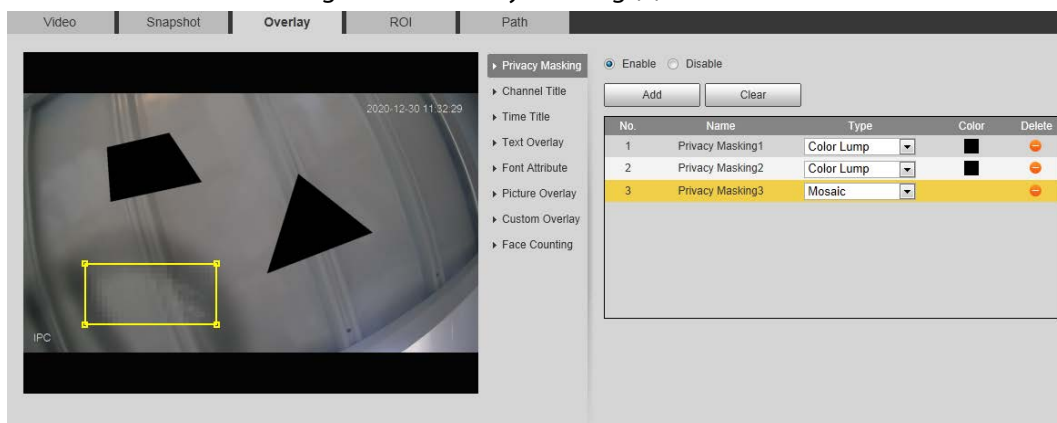
- When selecting **Color Lump** only, you can draw triangles and convex quadrilaterals as blocks. You can drag 8 blocks at most, and the color is black.
- When selecting **Mosaic**, you can draw rectangles as blocks with mosaic. You can draw 4 blocks at most.
- **Color Lump + Mosaic** (≤ 4): You can draw 8 blocks at most.

Step 1 Select **Setting > Camera > Video > Overlay > Privacy Masking**.

Step 2 Select **Enable**.

Step 3 Click **Add**, select the masking type, and then draw blocks in image as needed.

Figure 4-54 Privacy masking (2)



Related Operations

- View and edit the block

Select the privacy masking rule to be edited in the list, then the rule is highlighted, and the block frame is displayed in the image. You can edit the selected block as needed, including moving the position, and adjusting the size.
- Edit the block name

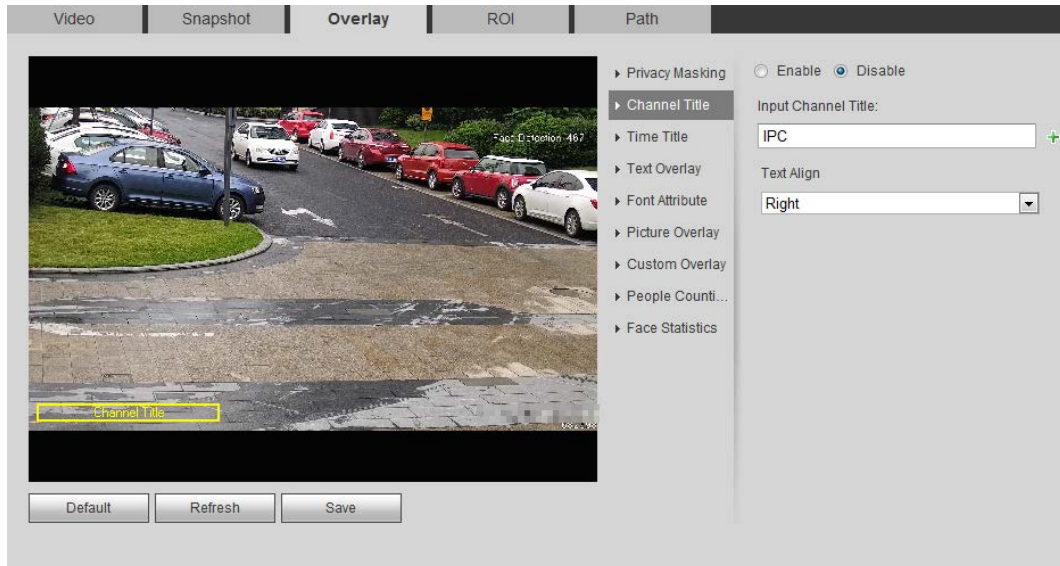
Double-click the name in **Name** to edit the block name.
- Delete the block
 - ◇ Click to delete blocks one by one.
 - ◇ Click **Clear** to delete all blocks.

4.5.2.3.2 Configuring Channel Title

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

Step 1 Select **Setting > Camera > Video > Overlay > Channel Title**.

Figure 4-55 Channel title



Step 2 Select the **Enable** checkbox, enter the channel title, and then select the text align.



Click **+** to expand the channel title, and you can expand 1 line at most.

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

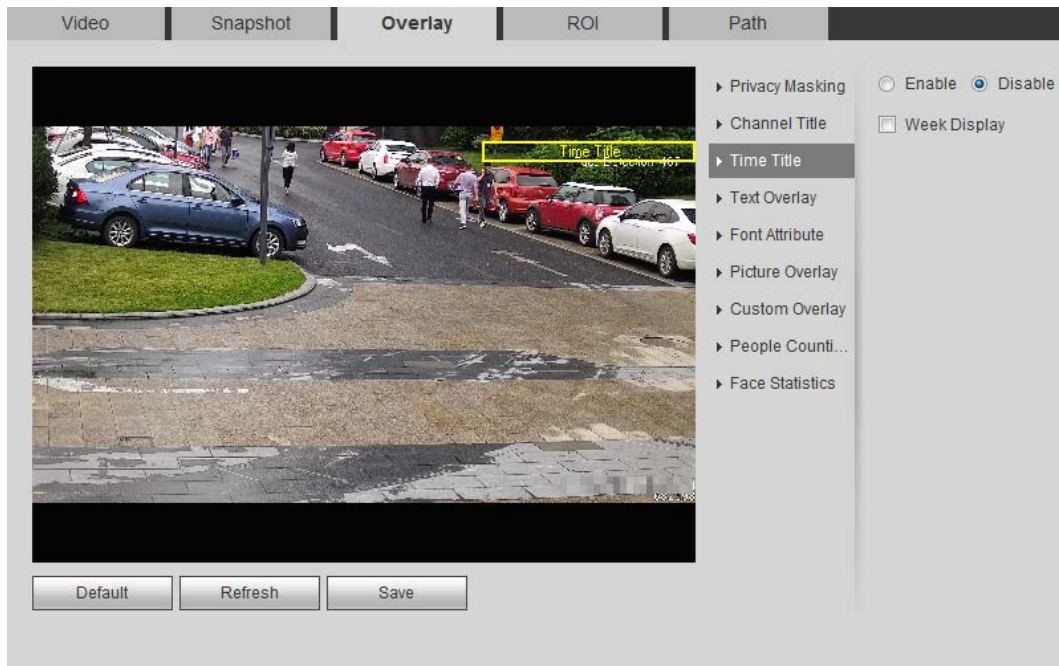
Step 4 Click **Save**.

4.5.2.3.3 Configuring Time Title

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

Step 1 Select **Setting > Camera > Video > Overlay > Time Title**.

Figure 4-56 Time title



- Step 2** Select the **Enable** checkbox.
- Step 3** Select the **Week Display** checkbox.
- Step 4** Move the time box to the position that you want in the image.
- Step 5** Click **Save**.

4.5.2.3.4 Configure Text Overlay

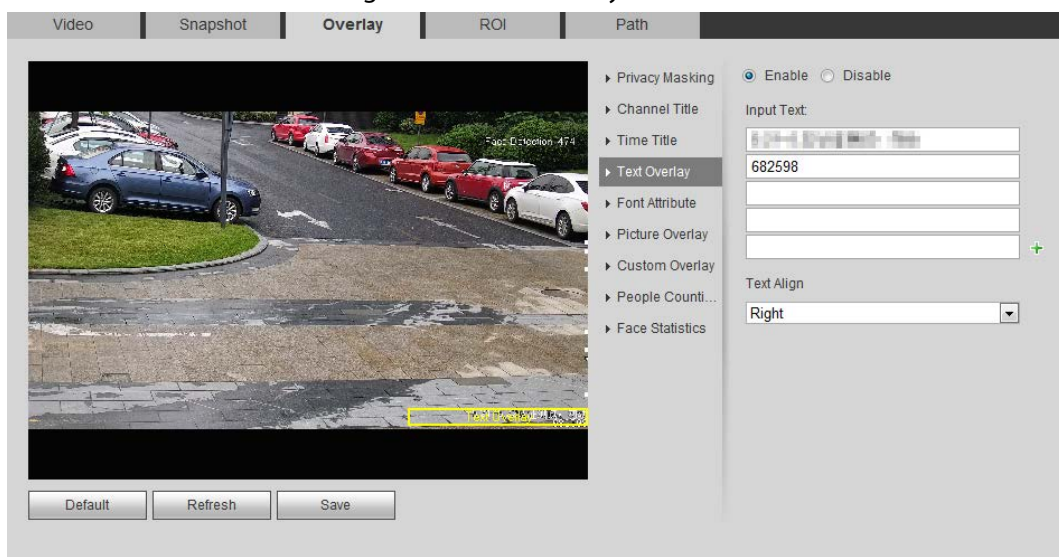
You can enable this function if you need to display text in the video image.



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 **Setting > Camera > Video > Overlay > Text Overlay**.

Figure 4-57 Text overlay



- Step 2** Select the **Enable** checkbox, enter the text you need, and then select alignment. The text is

displayed in the video image.



Click **+** to expand the text overlay, and you can expand 9 lines at most.

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

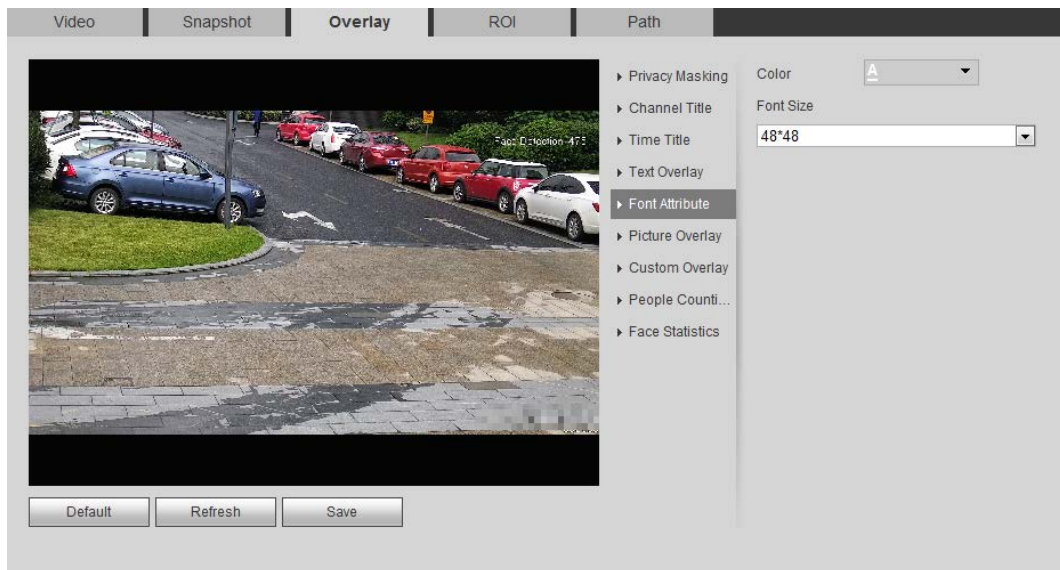
Step 4 Click **Save**.

4.5.2.3.5 Configure Font Attribute

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

Step 1 Select **Setting > Camera > Video > Overlay > Font Attribute**.

Figure 4-58 Font attribute



Step 2 Select the font color and size.

Click **More Color** to customize the font color.

Step 3 Click **Save**.

4.5.2.3.6 Configure Picture Overlay

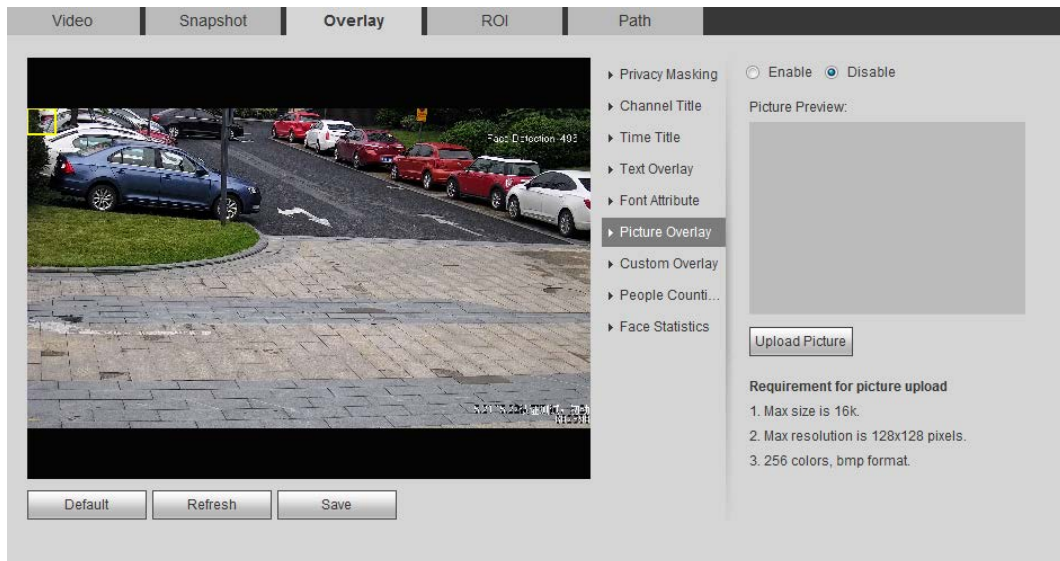
You can enable this function if you need to display picture information on the video image.



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

Step 1 Select **Setting > Camera > Video > Overlay > Picture Overlay**.

Figure 4-59 Picture overlay



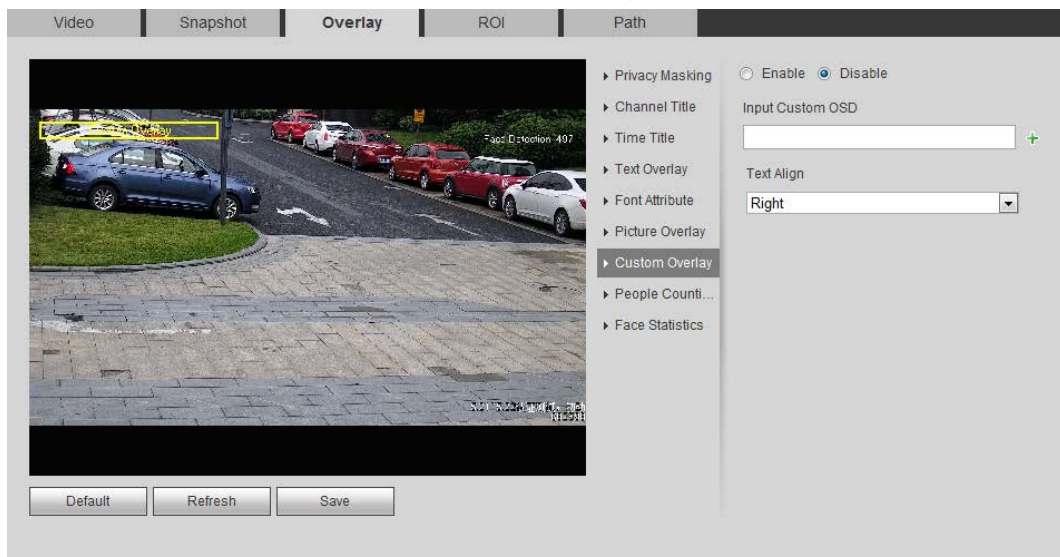
- Step 2** Select the **Enable** checkbox, click **Upload Picture**, and then select the picture to be overlaid.
The picture is displayed on the video image.
- Step 3** Move the overlaid picture to the position that you want in the image.
- Step 4** Click **Save**.

4.5.2.3.7 Configure Custom Overlay

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

- Step 1** Select **Setting > Camera > Video > Overlay > Custom Overlay**.

Figure 4-60 Custom overlay



- Step 2** Select the **Enable** checkbox, and then select the text align.



Click **+** to expand the custom overlay, and you can expand 1 line at most.

- Step 3** Move the custom box to the position that you want in the image.
- Step 4** Click **Save**.

4.5.2.3.8 Configuring OSD Info

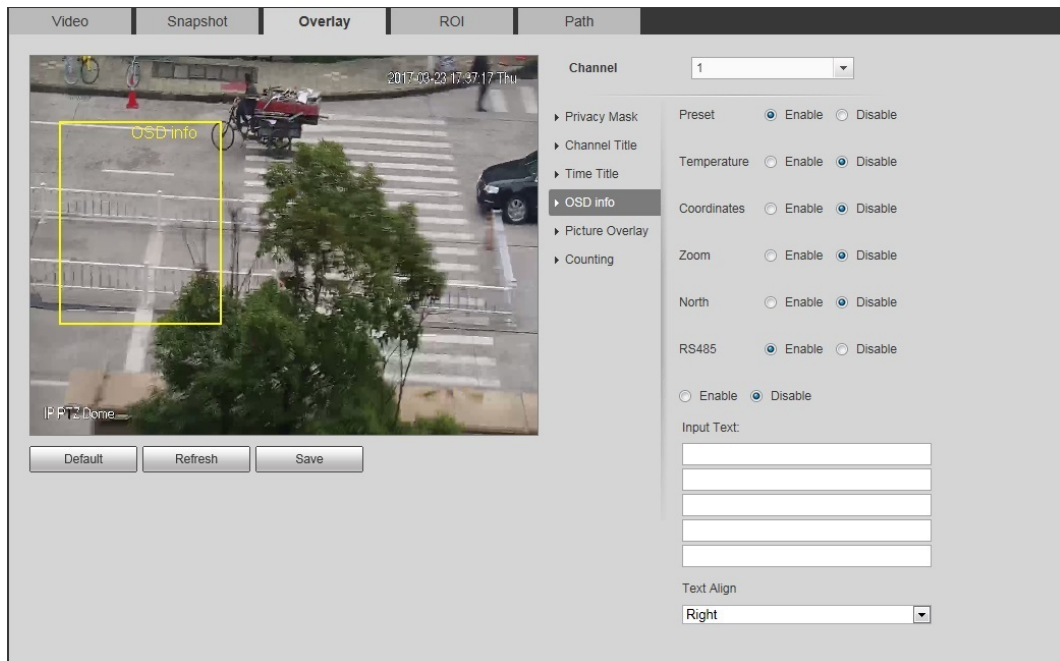
You can enable this function if you want to display the information of preset, PTZ coordinates, zoom, tour and location on the video image.



Only tracking speed dome supports OSD info function.

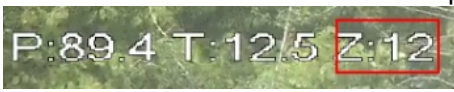
Step 1 Select **Setting > Camera > Video > Overlay > OSD Info**.

Figure 4-61 OSD information



Step 2 Configure OSD information.

Table 4-19 Description of OSD information

Parameter	Description
Preset	Select Enable , and the preset name is displayed in the image when the camera turns to the preset, and it will disappear 3 s later.
Temperature	Select Enable and the internal temperature of the current device is displayed.
Coordinates	Select Enable and the PTZ coordinates info is displayed in the image.
Zoom	Select Enable and the zoom info is displayed in the image. such as  , which means 12x zoom rate.
North	Select Enable and the north direction is displayed in the image.
RS485	Select Enable and it will enable RS-485 communication function.
Text	Select Enable and set text, and the text is displayed in the image.
Input Text	
Text Align	Alignment mode of the displayed information in the image.

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

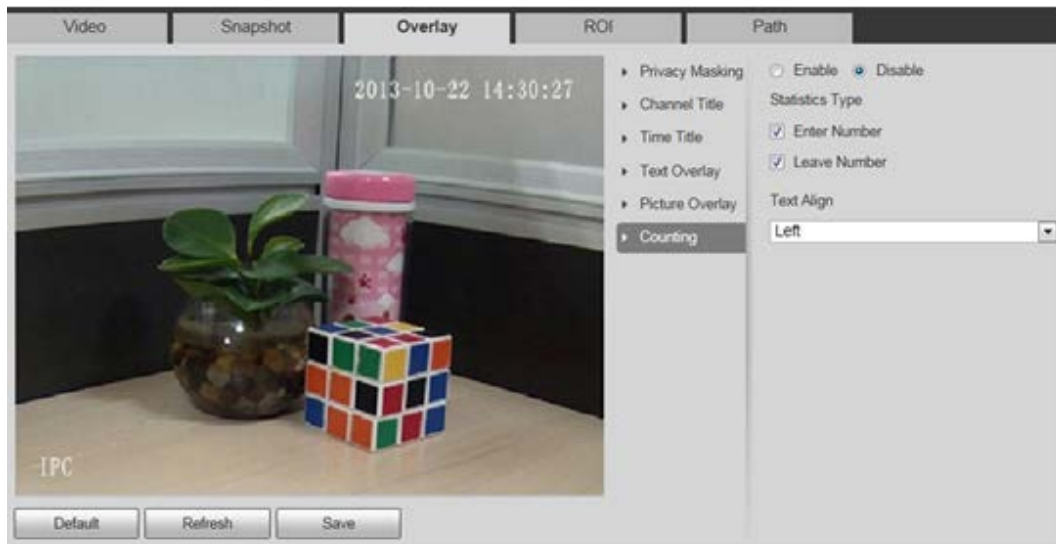
Step 4 Click **Save**.

4.5.2.3.9 Configuring Counting

The image displays statistics of the enter number and leave number. When the overlay function is enabled during intelligent rules configuration, this function is enabled simultaneously.

Step 1 Select **Setting > Camera > Video > Overlay > Counting**.

Figure 4-62 Counting



Step 2 Select the **Enable** checkbox, and then configure counting method and alignment.

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

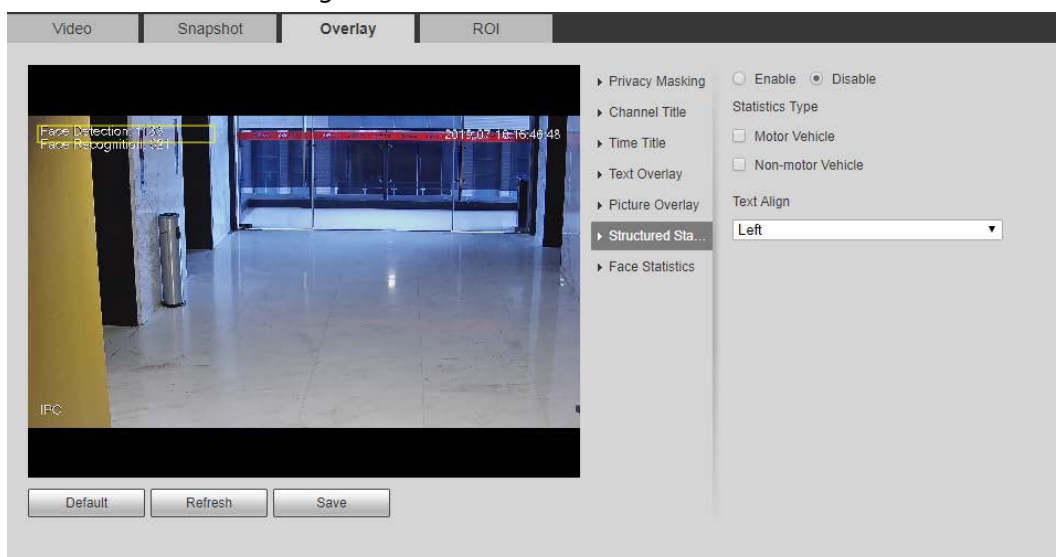
Step 4 Click **Save**.

4.5.2.3.10 Configuring Structured Statistics

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

Step 1 Select **Setting > Camera > Video > Overlay > Structured Statistics**.

Figure 4-63 Structured statistics



Step 2 Select the **Enable** checkbox, select the statistics type, and then select text align.

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

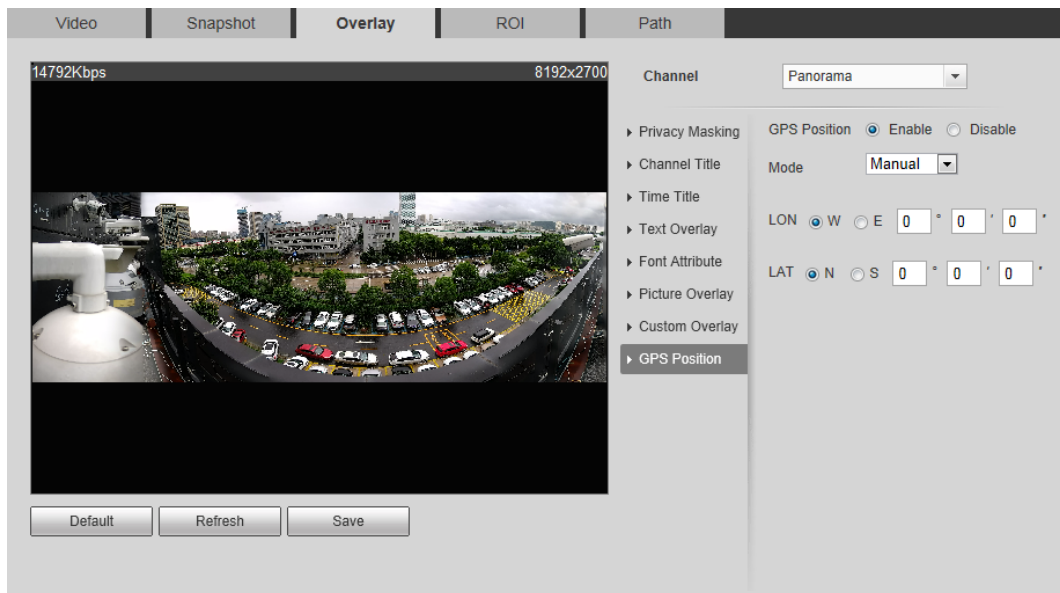
Step 4 Click **Save**.

4.5.2.3.11 Configuring GPS Position

The image displays GPS position. When the overlay function enabled during intelligent rules configuration, this function is enabled simultaneously.

Step 1 Select **Setting > Camera > Video > Overlay > GDP Position**.

Figure 4-64 GDP position



Step 2 Select the **Enable** checkbox, and then select the **Mode** to **Auto** or **Manual**.

- Auto: The GPS positions the longitude and latitude automatically.
- Manual: Enter the longitude and latitude manually.

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

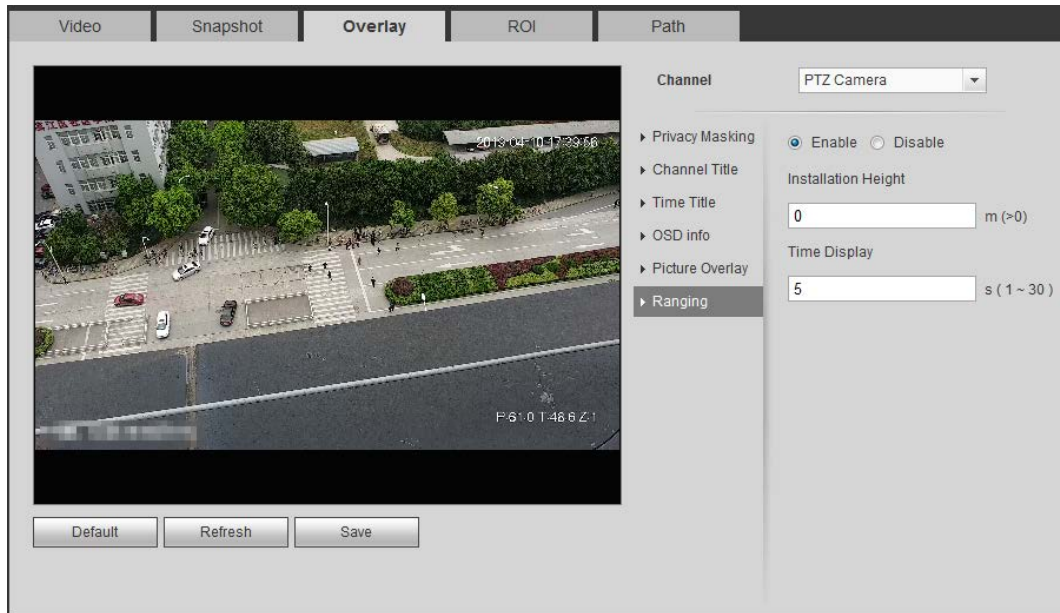
Step 4 Click **Save**.

4.5.2.3.12 Configuring Ranging

Configure camera height and the display time of overlay information. Click any point on the ground that the pole is installed on the image, and the overlay information between camera and the selected point is displayed.

Step 1 Select **Setting > Camera > Video > Overlay > Ranging**.

Figure 4-65 Ranging



Step 2 Select the **Enable** checkbox, and then set the installation height and time display.
Time display: The display time of the ranging information on live image.

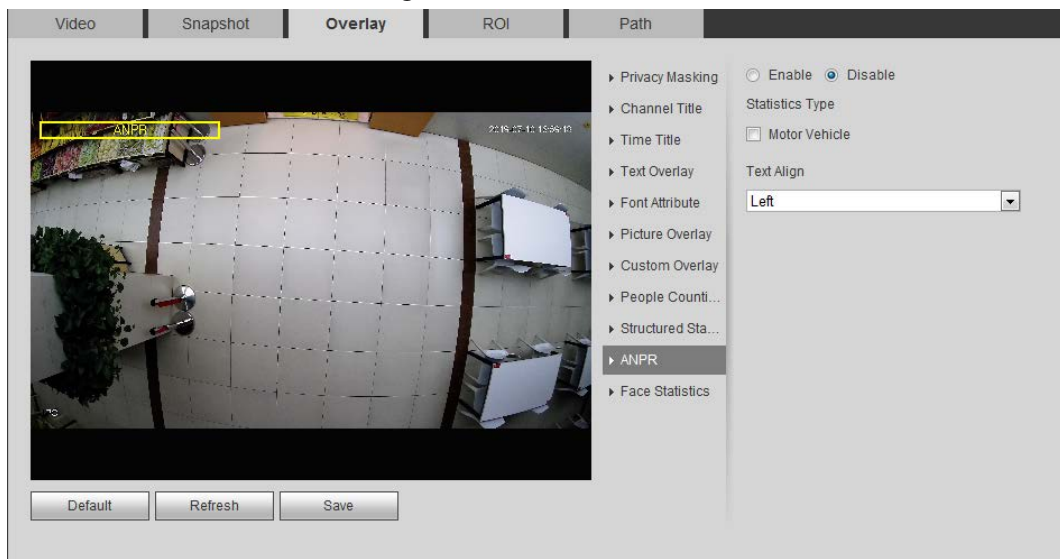
Step 3 Click **Save**.

4.5.2.3.13 Configuring ANPR

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

Step 1 Select **Setting > Camera > Video > Overlay > ANPR**.

Figure 4-66 ANPR



Step 2 Select the **Enable** checkbox, select the statistics type, and then select text align.

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

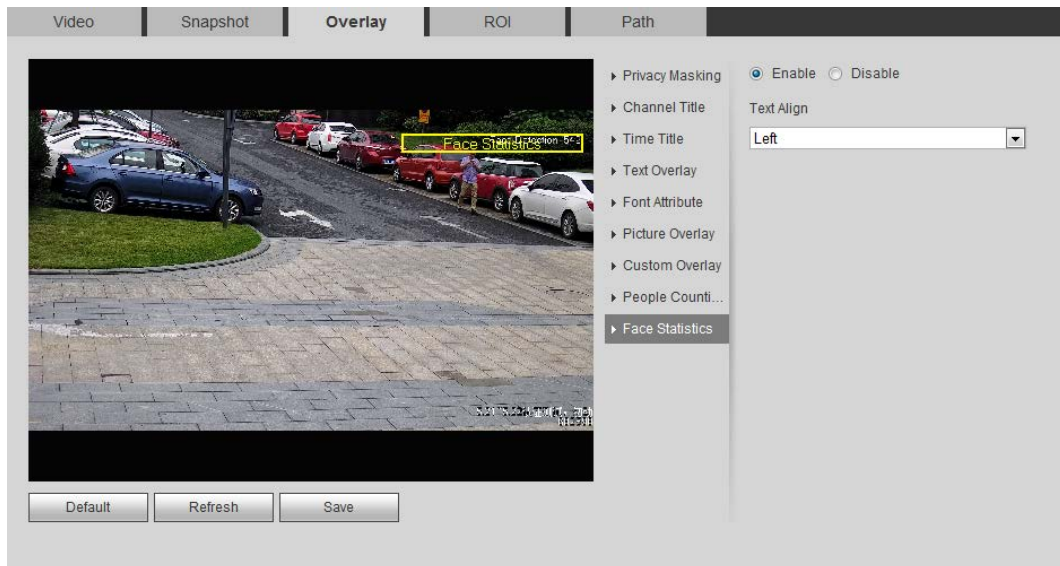
Step 4 Click **Save**.

4.5.2.3.14 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 **Setting > Camera > Video > Overlay > Face Statistics**.

Figure 4-67 Face statistics



Step 2 Select the **Enable** checkbox, and select text align.

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

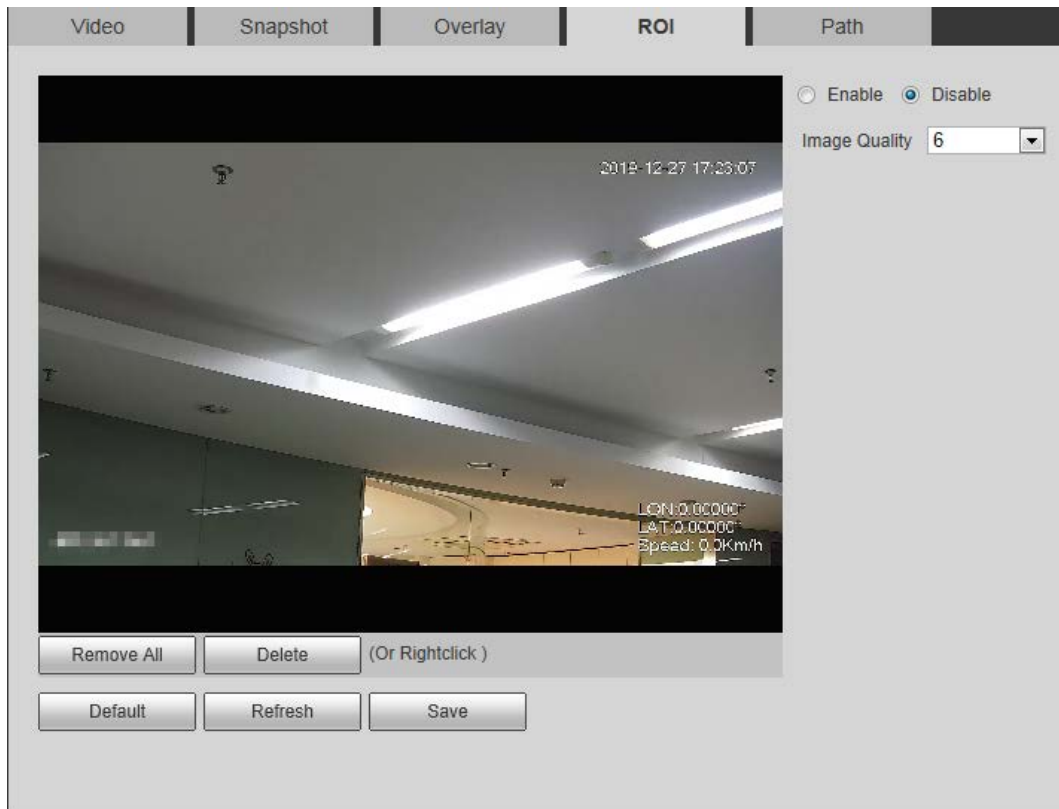
Step 4 Click **Save**.

4.5.2.4 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 **Setting > Camera > Video > ROI**.

Figure 4-68 ROI



Step 2 Select the **Enable** checkbox, draw the area on the image, and then configure the image quality of ROI.



- You can draw four area boxes at most.
- The higher the image quality value is, the better the quality will be.
- Click **Remove All** to delete all the area boxes; select one box, and then click **Delete** or right-click to delete it.

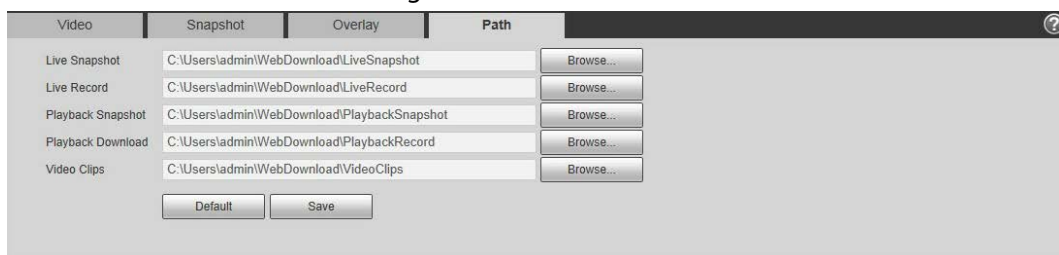
Step 3 Click **Save**.

4.5.2.5 Path

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

Step 1 Select **Setting > Camera > Video > Path**.


Figure 4-69 Path



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

Table 4-20 Description of path

Parameter	Description
Live Snapshot	The snapshot of live interface. The default path is C:\Users\admin\WebDownload\LiveSnapshot.
Live Record	The recorded video of live interface. The default path is C:\Users\admin\WebDownload\LiveRecord.
Playback Snapshot	The snapshot of playback interface. The default path is C:\Users\admin\WebDownload\PlaybackSnapshot.
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. The default path is C:\Users\admin\WebDownload\VideoClips.



Admin in the path refers to the account being used.

Step 3 Click **Save**.

4.5.3 Audio

You can configure audio parameters and alarm audio.

4.5.3.1 Configuring Audio Parameter

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

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

Figure 4-70 Audio

- Step 2** Select the **Enable** checkbox 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 4-21 Description of audio parameters

Parameter	Description
Encode Mode	You can select audio Encode Mode from G.711A , G.711Mu , AAC , G.726 . 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 accurate the restored signal will be. You can select audio Sampling Frequency from 8K , 16K , 32K , 48K , 64K .
Audioin Type	You can select audioin 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 **Save**.

4.5.3.2 Configuring Alarm Audio

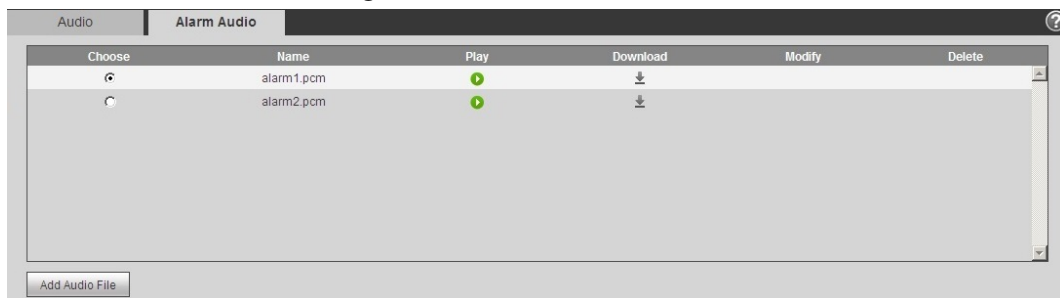
You can record or upload alarm audio file. The audio file will be played when the alarm is triggered.

- Click to play the selected audio.

- Click to download the audio to local storage.

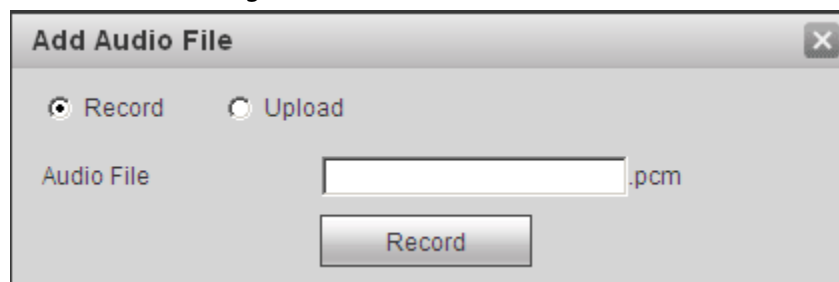
Step 1 Select **Setting > Camera > Audio > Alarm Audio**.

Figure 4-71 Alarm audio



Step 2 Click **Add Audio File**.

Figure 4-72 Add audio file



Step 3 Configure the audio file.

- Select **Record**, enter the audio name in the input box, and then click **Record**.
- Select **Upload**, click to select the audio file to be uploaded, and then click **Upload**.



The camera supports audio file with .pcm format only, and you can upload audio files with .pcm or .wav2 formats.

Step 4 Select the file that you need.

4.6 Network

This section introduces network configuration.

4.6.1 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 **Setting > Network > TCP/IP**.

Figure 4-73 TCP/IP

Step 2 Configure TCP/IP parameters.

Table 4-22 Description of TCP/IP parameters

Parameter	Description
Host Name	Enter the host name, and the maximum length is 15 characters.
Ethernet Card	Select the Ethernet card that need to be configured, and the default one is Wire .
Mode	The mode that the camera gets IP: <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.
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.
Subnet Mask	

Parameter	Description
Default Gateway	 <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.
Preferred DNS	IP address of the preferred DNS.
Alternate DNS	IP address of the alternate DNS.
Enable ARP/Ping to set IP address service	<p>Select the checkbox, get the camera MAC address, and then you can modify and configure the device IP address with ARP/ping command. This is enabled by default. During reboot, 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"> Keep the camera that needs to be configured and the PC within the same local network, and then get a usable IP address. Get the MAC address of the camera from device label. Open command editor on the PC and enter the following command. <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <p>Windows syntax↵</p> <pre>arp -s <IP Address> <MAC> ↵ ping -l 480 -t <IP Address> ↵</pre> </div> <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <p>Windows example↵</p> <pre>arp -s 192.168.0.125 11-40-8c-18-10-11↵ ping -l 480 -t 192.168.0.125↵</pre> </div> <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <p>UNIX/Linux/Mac syntax↵</p> <pre>arp -s <IP Address> <MAC> ↵ ping -s 480 <IP Address> ↵</pre> </div> <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <p>UNIX/Linux/Mac example↵</p> <pre>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"> Restart the camera. 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. Enter <code>http://(IP address)</code> in the browser address bar to log in.

Step 3 Click **Save**.

4.6.2 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 **Setting > Network > Port**.

Figure 4-74 Port

Parameter	Value	Range
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 4-23 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.

Parameter	Description
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 user name 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 user name, 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=2&subtype=1</p> <p>If user name and password are not needed, then the URL can be: rtsp://ip:port/cam/realmonitor?channel=1&subtype=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 **Save**.



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

4.6.3 PPPoE

Point-to-Point Protocol over Ethernet, it 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 **Setting** > **Network** > **PPPoE**.

Figure 4-75 PPPoE



Step 2 Select the **Enable** checkbox, and then enter user name 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 **Save**.

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

4.6.4 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.

Procedure

Step 1 Select **Setting** > **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 4-76 DDNS

Step 2 Select **Type**, and configure the parameters as needed.

Table 4-24 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
Web Address	
Domain Name	The domain name you registered on the DDNS website.
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 3 Click **Save**.

Result

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

4.6.5 SMTP (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 **Setting > Network > SMTP (Email)**.

Figure 4-77 SMTP (Email)

Step 2 Configure SMTP (Email) parameters.



Table 4-25 Description of SMTP (Email) parameters




Parameter	Description
SMTP Server	SMTP server address
Port	The port number of the SMTP server.
Username	The account of SMTP server.
Password	The password of SMTP server.
Anonymity	Select the checkbox, and the sender's information is not displayed in the email.
Sender	Sender's email address.
Authentication	Select Authentication from None , SSL and TLS . For details, see Table 4-26.
Title	Enter maximum 63 characters in Chinese, English, and Arabic numerals. Click to select title type, including Name , Device ID , and Event Type , and you can set maximum 2 titles.
Attachment	Select the checkbox to support attachment in the email.
Mail Receiver	Receiver's email address. Supports 3 addresses at most.

Parameter	Description
Health Mail	The system sends test mail to check if the connection is successfully configured. Select Health Mail and configure the Update Period , and then the system sends test mail as the set interval.

For the configuration of major mailboxes, see Table 4-26.

Table 4-26 Description of major mailbox configuration

Mailbox	SMTP server	Authenticat ion	Port	Description
QQ	smtp.qq.co m	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.  <p>Authentication code: The code you receive when enabling SMTP service.</p>
		TLS	587	<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.  <p>Authentication code: The code you receive when enabling SMTP service.</p>

Mailbox	SMTP server	Authenticat ion	Port	Description
163	smtp.163.co m	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.  <p>Authentication code: the code you receive when enabling SMTP service.</p>
		TLS	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.  <p>Authentication code: the code you receive when enabling SMTP service.</p>
		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.  <p>Authentication code: the code you receive when enabling SMTP service.</p>
Sina	smtp.sina.co m	SSL	465	Enable SMTP service in your mailbox.
		none	25	
126	smtp.126.co m	none	25	Enable SMTP service in your mailbox.

Step 3 Click **Save**.

Step 4 Click **Test** to test whether the emails can be sent and received successfully.

4.6.6 UPnP

UPnP (Universal Plug and Play), 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

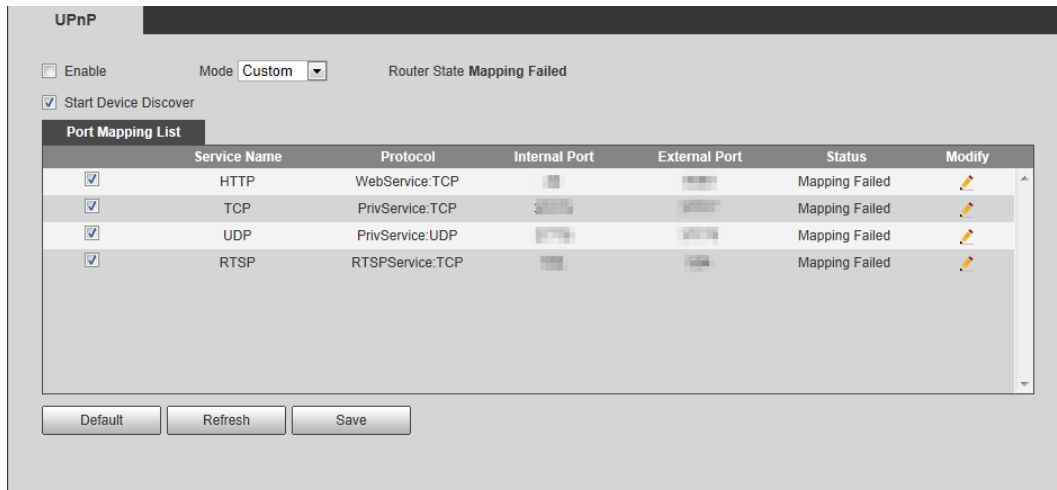
- Make sure the UPnP service is installed in the system.
- Log in the router, and configure WAN IP address to set up internet connection.
- Enable UPnP in the router.
- Connect your device to the LAN port of the router.

- Select **Setting > 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 **Setting > Network > UPnP**.

Figure 4-78 UPnP



- Step 2 Select the **Enable** checkbox, and there are two mapping modes: **Custom** and **Default**.

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

- Step 3 Click **Save**.

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.

4.6.7 SNMP

SNMP (Simple Network Management Protocol) 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 **Setting > Network > SNMP**.

Figure 4-79 SNMP (1)

The interface shows the following configuration:

- Version: v1, v2, v3
- SNMP Port: (1~65535)
- Read Community:
- Write Community:
- Trap Address:
- Trap Port:
- Buttons: Default, Refresh, Save

Figure 4-80 SNMP (2)

The interface shows the following configuration:

- Version: v1, v2, v3 (Recommen...)
- SNMP Port: (1~65535)
- Read Community:
- Write Community:
- Trap Address:
- Trap Port:
- Read-only Username:
- Authentication Type: MD5, SHA
- Authentication Pas...: The minimum pass phrase length is 8 characters
- Encryption Type: CBC-DES
- Encryption Password: The minimum pass phrase length is 8 characters
- Read&write Userna...:
- Authentication Type: MD5, SHA
- Authentication Pas...: The minimum pass phrase length is 8 characters
- Encryption Type: CBC-DES
- Encryption Password: The minimum pass phrase length is 8 characters
- Buttons: Default, Refresh, Save

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 user name,




password and authentication type. It requires corresponding user name, password and authentication type to visit your device from the server.



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

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 4-27 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 public 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 3 Click **Save**.

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 OS and disable SNMP Trap service. The MG-SOFT MIB Browser will display prompt when alarm is triggered.

4.6.8 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 **Setting > Network > Bonjour**.

Figure 4-81 Bonjour

Step 2 Select the **Enable** checkbox, and then configure server name.

Step 3 Click **Save**.

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.

4.6.9 Multicast

When multiple users are previewing 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 **Setting > Network > Multicast**.

Figure 4-82 Multicast

Step 2 Select the **Enable** checkbox, and enter IP address and port number.

Table 4-28 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 **Save**.

Result

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

4.6.10 802.1x

Cameras can connect to LAN after passing 802.1x authentication.

Step 1 Select **Setting > Network > 802.1x**.

Figure 4-83 802.1x

Step 2 Select the **Enable** checkbox, and then configure parameters.

Table 4-29 Description of 802.1x parameters

Parameter	Description
Authentication	PEAP (protected EAP protocol).
Username	The user name that was authenticated on the server.
Password	Corresponding password.

Step 3 Click **Save**.

4.6.11 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 **Setting > Network > QoS**.

Figure 4-84 QoS

Step 2 Configure QoS parameters.

Table 4-30 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**.

4.6.12 5G

5G configuration includes dialing configuration and mobile configuration. Install SIM card (Subscriber Identification Module) to the camera, and connect it to 5G network through dialing configuration and mobile configuration.

- Dialing configuration: Connect the camera to 5G network in a specific period.
- Mobile configuration: Configure the mobile phone to receive the linkage message. When an alarm is triggered, the system sends an alarm message to the receiver, and then the receiver can active the camera and connect it to 5G network through message or call.

4.6.12.1 Dialing Setting

Configure the camera to connect it to 5G network.

Step 1 Select **Setting > Network > 5G > Dialing Setting**.

Step 2 Select the **Enable** checkbox, and configure the parameters.

Figure 4-85 Dialing setting

Table 4-31 Dialing setting parameters

Parameter	Description
Wireless Net Type	Select the wireless net type according to the carrier.
APN	Acquired from the carrier.
Authentication Mode	Select the authentication mode according to different carrier.
Dial-up Number	The number is different according to different carrier, and it can be acquired from carrier.
Username	Acquired from the carrier.
Password	Acquired from the carrier.
Interval	It is the period beyond the dial-up period which has been configured, it is 30 s by default, during which means the camera can auto connect to 5G network. After the period is over, the camera automatically cuts off the connection to save flow.
Time Range	The camera can connect to 5G network during the configured period. For details, see "5.1.1.1 Setting Period".
Wireless Network State	When the dialing is successful, the wireless network status is displayed.
Wireless Signal	When the dialing is successful, the wireless net type and signal strength are displayed.

Step 3 Click **Save**.

4.6.12.2 Mobile Setting

Configure the mobile phone, and all alarm messages support sending message the configured receiver. After receiving a message, the receiver can active the camera and connect it to 5G network through message or call.

- **Message send:** Set the receiver's phone number, and when an alarm is triggered, the system will send message to the receiver.
- **Message activation:** Set the sender's phone number, the sender can send command message to active the camera. The commands are as following:
 - ◇ On: Make the camera online.
 - ◇ Off: Make the camera offline.
 - ◇ Reboot: Restart the camera.
- **Phone activation:** Set the receiver's phone number, the caller can call the camera to active the camera, and make it online.

Step 1 Select **Setting > Network > 5G > Mobile Setting**.

Step 2 Select **Message send, Message activation, or Phone activation** as needed.

Step 3 Enter the phone numbers of receiver, sender, or caller, and click to add it to the list.



- Select a phone number, and click to delete it.
- You can edit the message in **Title** during configuration.

Figure 4-86 Mobile setting

The screenshot shows the 'Mobile Settings' configuration page. It is divided into three columns: 'Message Send', 'Message Activation', and 'Phone Activation'. Each column has a checked checkbox at the top. Below each checkbox is a 'Receiver' field containing a phone number (partially masked) and a '+' button to the right. Underneath each 'Receiver' field is a list box containing several phone numbers, with a '-' button to the right of the list. At the bottom of each column is a 'Title' text input field. In the 'Message Send' section, the title is 'Event Message'. At the bottom of the entire page are three buttons: 'Default', 'Refresh', and 'Save'.

4.6.13 Access Platform

4.6.13.1 P2P

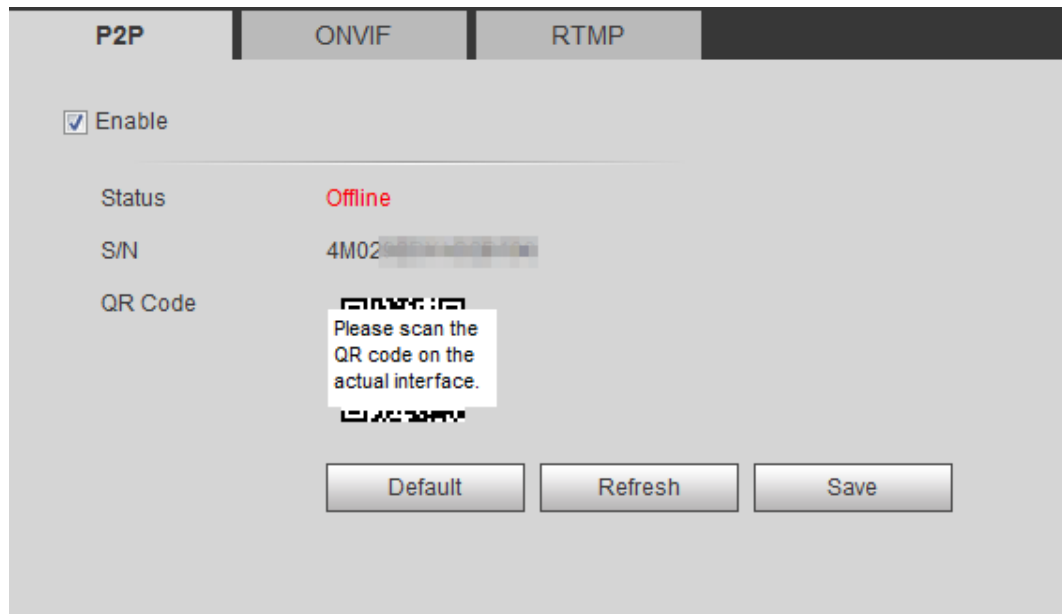
P2P is a private network traversal technology which enables users to manage devices easily without requiring DDNS, port mapping or transit server.

Scan the QR code with your smart phone, and then you can add and manage more devices on the

mobile phone client.

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

Figure 4-87 P2P



- 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 the + at the upper right corner.

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

Step 5 Follow the instructions to finish the settings.

4.6.13.2 ONVIF

The ONVIF authentication is **On** 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 **Setting > Network > Port > ONVIF**.

Figure 4-88 ONVIF

Step 2 Select **On** in **Authentication**.

Step 3 Click **Save**.

4.6.13.3 RTMP

Through RTMP, you can access the 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 **Setting > Network > Port > RTMP**.

Figure 4-89 RTMP

Step 2 Select the **Enable** checkbox.



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

Step 3 Configure RTMP parameters. .

Table 4-32 Description of RTMP parameters

Parameter	Description
Stream Type	The stream for live view. Make sure that the video format is the H.264, H.264 B and H.264H, and the audio format is AAC.

Parameter	Description
Address Type	Includes Non-custom and Custom . <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: We recommend that you use the default one.
Port	
Custom Address	When selecting Custom , you need to enter the path allocated by the server.

Step 4 Click **Save**.

4.7 Storage

This section introduces how to manage saved resources (such as recorded video) and storage space. The storage management helps to make best use of storage space.

4.7.1 Setting Storage Plan

- Setting record plan and record control to achieve all-time recording, recording in specific period or alarm linked recording. For details, see "5.1.1.2.1 Setting Record Plan" and "5.1.1.2.2 Setting Record Control".
- Set the snapshot schedule as needed. For details, see "5.1.1.3.1 Setting Snapshot Plan".

4.7.2 Setting Schedule

You can configure record schedule, snapshot schedule and holiday schedule. Set certain days as holiday, and when the **Record** or **Snapshot** is selected in the holiday schedule, the system takes snapshot or records video as holiday schedule defined.

Prerequisites

- Set the record mode to be **Auto** in **Record Control**. For details, see "5.1.1.2.1 Setting Record Plan".
- Configure holiday record and snapshot schedule. For details, see "5.1.1.2.1 Setting Record Plan" and "5.1.1.3.1 Setting Snapshot Plan".

Procedure

Step 1 Select **Setting** > **Storage** > **Schedule** > **Holiday Schedule**.

Figure 4-90 Holiday schedule

Step 2 Select **Record** or **Snapshot**.

Step 3 Select the days you need to set as holiday.

Those days with yellow color indicates that they were set as holidays.



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 4 Click **Save**.

4.7.3 Setting Destination

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

4.7.3.1 Path

You can select different storage paths for the recorded videos and snapshots according to event type. You can select from SD card, FTP and NAS.



Local is displayed only on models that support SD card.

Step 1 Select **Setting > Storage > Destination > Path**.

Figure 4-91 Path

Record				Snapshot			
Event Type	Scheduled	Motion Detection	Alarm	Event Type	Scheduled	Motion Detection	Alarm
Local	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Local	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
FTP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	FTP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
NAS	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	NAS	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Buttons: Default, Refresh, Save

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

Table 4-33 Description of path parameters

Parameter	Description
Event Type	Select from Scheduled , Motion Detection and Alarm .
Local	Save in the internal SD card.
FTP	Save in the FTP server.
NAS	Save in the NAS (network attached storage).

Step 3 Click **Save**.

Step 4 Configure other path parameters on **Destination**, **FTP** or **NAS** interface. For details, see "4.7.3 Setting Destination", "4.7.3.3 FTP" or "4.7.3.4 NAS".

4.7.3.2 Local

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.



Functions might vary with different models.

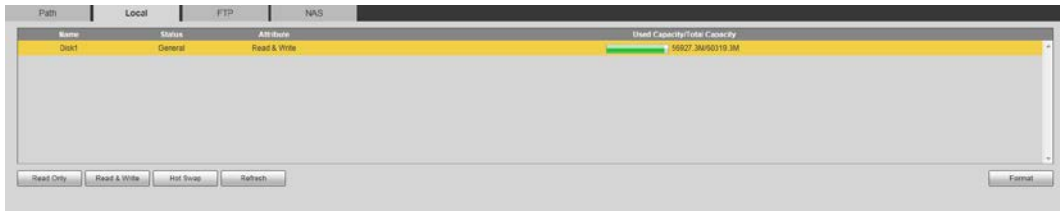
Select **Setting** > **Storage** > **Destination** > **Local**.

- 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 **Refresh**, and then you can format the SD card.
- Click **Format**, and you can format the SD card.



When reading SD card on PC, if the SD card capacity is much less than the nominal capacity, you need to format the SD card. Then the data in SD card will be cleared, and the SD card is formatted to be private file system. The private file system can greatly improve SD card multimedia file read/write performance. Download Diskmanager from Toolbox to read the SD card. For details, contact aftersales technicians.

Figure 4-92 Local



4.7.3.3 FTP

FTP can be enabled only when it was selected as a destination path. When the network does not work, you can save all the files to the internal SD card for emergency.

Step 1 Select **Setting > Storage > Destination > FTP**.

Step 2 Select the **Enable** checkbox, and select the FTP type.



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

Step 3 Configure FTP parameters.

Figure 4-93 FTP

Figure 4-94 Picture name settings

<input type="checkbox"/>	No.	Picture Name Content	Separator	Ordering
<input checked="" type="checkbox"/>	1	Date&Time		<input type="checkbox"/> ↑ ↓
<input checked="" type="checkbox"/>	2	Millisecond	-	<input type="checkbox"/> ↑ ↓
<input checked="" type="checkbox"/>	3	Name	-	<input type="checkbox"/> ↑ ↓
<input checked="" type="checkbox"/>	4	IP Address	-	<input type="checkbox"/> ↑ ↓
<input type="checkbox"/>	5	Channel NO.	-	<input type="checkbox"/> ↑ ↓
<input type="checkbox"/>	6	Snapshot Type	-	<input type="checkbox"/> ↑ ↓
<input type="checkbox"/>	7	Custom	-	<input type="checkbox"/> ↑ ↓


Date&TimeMillisecond_Name_IP Address_

Separator can only be a dash, underline or space.

Save Cancel

Table 4-34 Description of FTP parameters

Parameter	Description
Server Address	The IP address of the FTP server.
Port	The port number of the FTP server.
Username	The user name to log in to the FTP server.
Password	The password to log in to the FTP server.
Remote Directory	The destination path in the FTP server, and it is shared by default.
Directory Structure	Set the directory structure, which supports three levels at most.
Level 1 Directory	Set the directory name, and you can customize the name.
Level 2 Directory	When you select Custom , enter the custom directory name, which supports numbers, English letters, underlines and dashes.
Level 3 Directory	

Parameter	Description
Customized Picture Name	<p>Click Setting to set picture name.</p> <ul style="list-style-type: none"> • Date&Time is required, and it is selected by default. • Select the other fields of the name, and the corresponding instruction will be displayed on the screen. • Double-click the symbols under Separator, you can customize the separator. • Double-click Custom, you can customize the files of the picture name. • Click the arrow under Ordering, and you can adjust the ordering of the file.  <p>Date&Time and Millisecond is a whole, click the arrow of any one of the two fields, the two moves together.</p> <ul style="list-style-type: none"> • The real-time value of Millisecond will be displayed for precise snapshot, and for schedule and normal event, the millisecond displays 0000.
Emergency (Local)	Select Emergency (Local) , and when the FTP server does not work, all the files are saved to the internal SD card.

Step 4 Click **Save**.

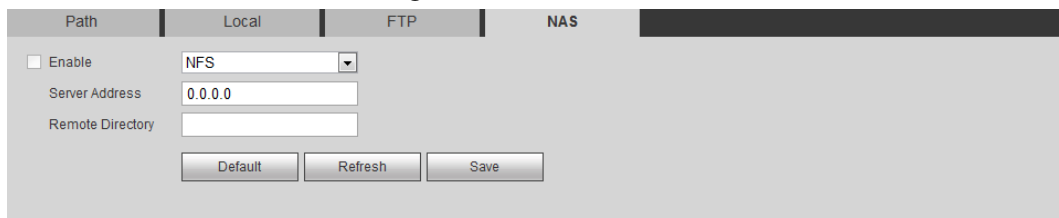
Step 5 Click **test** to test whether FTP function works normally.

4.7.3.4 NAS

This function can be enabled only when NAS was selected as a destination path. Enable this function, and you can save all the files in the NAS.

Step 1 Select **Setting > Storage > Destination > NAS**.

Figure 4-95 NAS



Step 2 Select the **Enable** checkbox to enable NAS function, and select NAS protocol type.

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

Step 3 Configure NAS parameters.

Table 4-35 Description of NAS parameters

Parameter	Description
Server Address	The IP address of the NAS server.
Username	When selecting SMB protocol, you are required to enter user

Parameter	Description
Password	name and password. Enter them as needed.
Remote Directory	The destination path in the NAS server.

Step 4 Click **Save**.

4.8 System

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

4.8.1 General

You can configure device name, language and video standard.

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

Figure 4-96 General

Step 2 Configure general parameters.

Table 4-36 Description of general parameters

Parameter	Description
Name	The name of the device. Each device has its own name.
Language	Select system language.
Video Standard	Select video standard from PAL and NTSC .
TVOut	Select On or Off . This function is available on models with analog output. <ul style="list-style-type: none"> If the TV out is On, smart plans will be disabled; if the smart plans are enabled, the TV out will be set as Off. SDI and HDCVI are available on select models.

Step 3 Click **Save**.

4.8.2 Date & Time

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

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

Figure 4-97 Date and time

Step 2 Configure date and time parameters.

Table 4-37 Description of date and time parameters

Parameter	Description
Date Format	Configure the date format.
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.
Current Time	Configure system time. Click Sync PC , and the system time changes to the PC time.

Parameter	Description
DST	Enable DST as needed. Select the checkbox, and configure start time and end time of DST with Date or Week .
NTP	Select the checkbox, and then NTP (network time protocol) is enabled, 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.
NTP Server	
Time Zone	
Port	
Interval	
Positioning System	Supports both GPS and BeiDou.
Positioning System Time Synchronization	Select Position System Time Synchronization and configure Interval to enable this function. After enabling this function, the device will synchronize the system time according to the interval you set.
Interval	

Step 3 Click **Save**.

4.8.3 Account

Manage all the users. You can add, delete, or modify users. 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 consisted of number, letters, 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 user names or group names are not allowed. A user can be in only one group at a time, and the group users can own authorities within group authority range.
- Online users cannot modify 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 user name and password. Anonymous users only have preview authorities. During anonymous login, click **Logout**, and then you can log in with other username.

4.8.3.1 Adding a User

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

Step 1 Select **Setting** > **System** > **Account** > **Account** > **Username**.

Figure 4-98 Username

The screenshot shows the 'Account' management interface with the 'Onvif User' tab selected. At the top, there is an 'Anonymous Login' checkbox. Below it is a table with columns for 'Username' and 'Group Name'. The main table lists users with columns: No., Username, Group Name, Memo, Restricted Login, Modify, and Delete. Below the table is an 'Authority' section with a grid of permissions. At the bottom is an 'Add User' button.

No.	Username	Group Name	Memo	Restricted Login	Modify	Delete
1	admin	admin	admin's account	/	[Edit]	[Delete]
2	admin1	admin		[Search]	[Edit]	[Delete]

Authority	Live	Playback	System	System Info
User				
Manual Control	File Backup	Storage	Event	Network
Peripheral	AV Parameter	PTZ	Security	Maintenance

Step 2 Click **Add User**.


Figure 4-99 Add user (operation permission)

The screenshot shows the 'Add User' dialog box. It contains input fields for Username (with a 'Must' label), Password, Confirm Password, Group Name (set to 'admin'), and Memo. Below the password fields is a strength indicator with 'Weak', 'Middle', and 'Strong' buttons, and a note: 'The minimum pass phrase length is 8 characters'. The 'Operation Permission' section is active, showing a list of permissions with checkboxes: All, User, Live, Playback, System, System Info, Manual Control, File Backup, Storage, Event, Network, Peripheral, AV Parameter, PTZ, Security, and Maintenance. At the bottom are 'Save' and 'Cancel' buttons.

Figure 4-100 Add user (restricted login)

Step 3 Configure user parameters.

Table 4-38 Description of user parameters (1)

Parameter	Description
Username	User's unique identification. You cannot use existed user name.
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.
Memo	Describe the user.
Operation Permission	Select authorities as needed.  We recommend you giving fewer authorities to normal users than advance users.


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 web 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 following:</p> <ol style="list-style-type: none"> 1. Select IP Address: Select IP type and set IP address. <ul 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. 2. Select Validity Period: Set the begin time and end time. 3. Select Time Range: Set the time range that allow user to log in. For details, see "5.1.1.1 Setting Period".

Step 4 Click **Save**.

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

Related Operations

- Edit user information

Click  to change password, group, memo, operation authorities, and login authorities.



You can only change the password of the admin.

The methods of changing password vary with different accounts.

- ◇ Login with the admin account, you can change password through **Old Password** and **Admin Account**.
- ◇ Login with non-admin account (an added account with the permission of user management), you can change password through **Old Password**.
- ◇ **Old Password**: Change the password through entering the old password to be changed, and then the new password.

Figure 4-101 Change password through old password (login with non-admin account)

Modify User

Username: 11

Modify Password

Old Password: []

New Password: []

The minimum pass phrase length is 8 characters

Weak Medium Strong

Confirm Password: []

Group Name: user

Memo: []

Authority: All

Live

Playback

Save Cancel

- ◇ **Admin Account:** Change the password through entering the admin password, and then the new password for the non-admin account to be changed.

Figure 4-102 Change password through admin password (login with admin account)

Modify User

Username: 11

Modify Password

Modification Mode: Admin Account

Admin Username: admin

Admin Password: []

New Password: []

The minimum pass phrase length is 8 characters

Weak Medium Strong

Confirm Password: []

Group Name: user

Memo: []


Save Cancel

- Delete users
Click  to delete the added users.



Admin account cannot be deleted.

- View the authorities

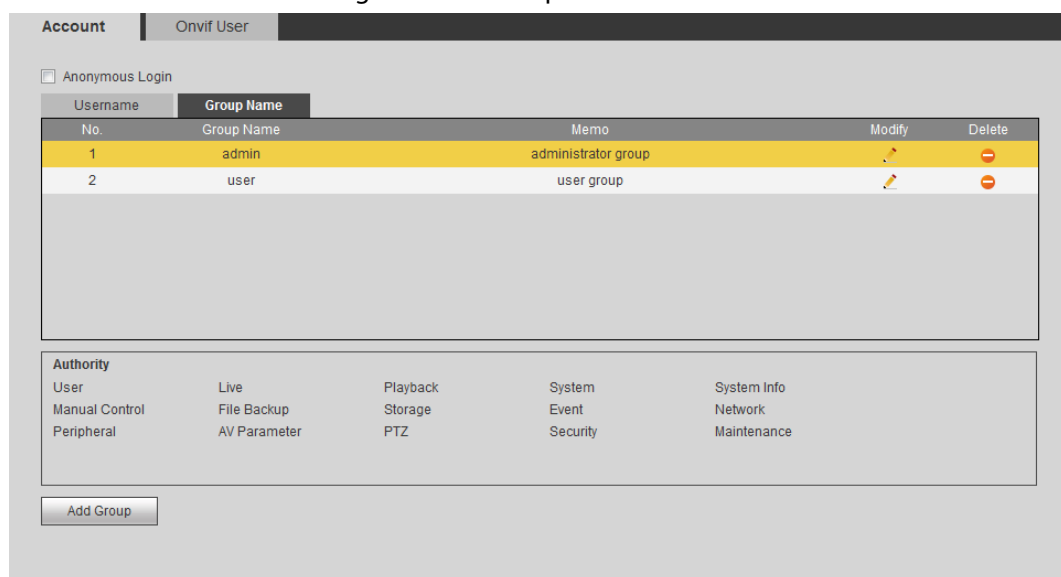
If the current account has with the permission of user management, click  to view the login authorities of other accounts. If not, you can only view the login authorities of the current account.

4.8.3.2 Adding User Group

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

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

Figure 4-103 Group name



Step 2 Click **Add Group**.

Figure 4-104 Add group

- Step 3** Enter the group name and memo, and then select group authorities.
 The default authorities of Admin group includes live, playback, storage, file backup, user, system, system info, manual control, maintenance, peripheral, PTZ, security, network, event and AV parameters; the default authorities of User group include live and playback.

Table 4-39 Description of user group parameters

Group Authority	Admin	User	Functions
User	YES	NA	Add, delete and check user/user group.
Live	YES	YES	Real-time stream view.
Playback	YES	YES	Playback view.
System	YES	NA	System time setting and more.
System Info	YES	NA	Version information, system logs and more.
Manual Control	YES	NA	PTZ settings.
File Backup	YES	NA	File backup.
Storage	YES	NA	Storage point configuration, snapshot recording time configuration, SFTP configuration and more.
Event	YES	NA	Video detection settings, audio detection settings, alarm settings and more.
Network	YES	NA	IP settings, SMTP settings, SNMP settings, AP Hotspot settings and more.




Group Authority	Admin	User	Functions
Peripheral	YES	NA	External light, wiper and serial port settings.
AV Parameter	YES	NA	Camera property settings, audio and video settings and more.
PTZ	YES	NA	Preset settings, tour settings and more.
Security	YES	NA	HTTPS settings, RTSP over TLS settings and more.
Maintenance	YES	NA	Automatic maintenance settings and more.



- Any user in the **Admin** group has **User** authorities to modify group authorities. The **User** group does not have this authorities.
- The function of the device correspond to the authority control respectively. Only user with specified authority can use corresponding function; the **Admin** group has all the authorities.

Step 4 Click **Save** to finish configuration.
The newly added group displays in the group name list.



- After adding group, click  to modify group memo or authorities; click  to delete the added group, admin group and user group cannot be deleted.
- Click  in the row of admin group or user group to modify group memo.

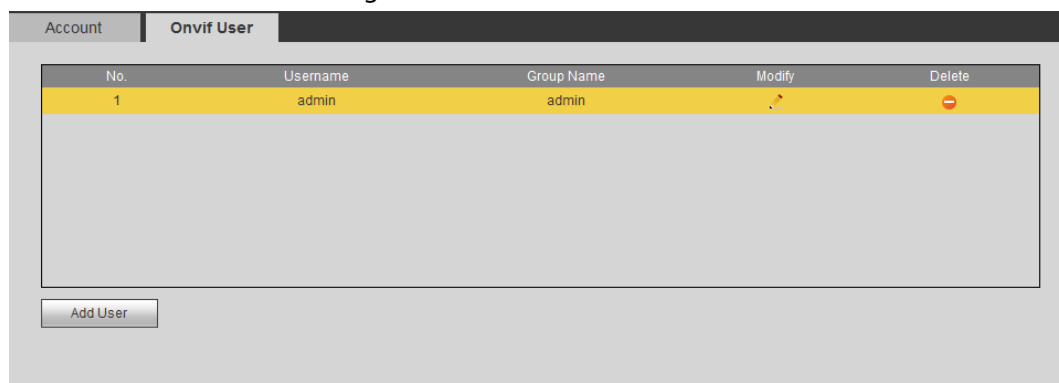
4.8.3.3 ONVIF User

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

Procedure

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

Figure 4-105 ONVIF user



Step 2 Click **Add User**.

Figure 4-106 Add user

Step 3 Configure user parameters.

Table 4-40 Description of user parameters

Parameter	Description
Username	User's unique identification. You cannot use existed user name.
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 **Save**.

The newly added user displays in the user name list.

Related Operations

- Edit user information

Click to change password, group, memo, operation authorities, and login authorities.



You can only change the password of the admin.

The methods of changing password vary with different accounts.

- ◇ Log in with admin account, you can change password through **Old Password** and **Admin Account**.
The password of admin account can be changed through **Old Password** only.
- ◇ Login with non-admin account (an added account with the permission of user management), you can change password through **Old Password**.
- ◇ **Old Password**: Change the password through entering the old password to be changed, and then the new password.

Figure 4-107 Change password through old password (login with non-admin account)

Modify User

Username: 11

Modify Password

Old Password: []

New Password: []

The minimum pass phrase length is 8 characters

Weak Medium Strong

Confirm Password: []

Group Name: user

Memo: []

Authority: All

Live

Playback

Save Cancel

- ◇ **Admin Account:** Change the password through entering the admin password, and then the new password for the non-admin account to be changed.

Figure 4-108 Change password through admin password (login with admin account)

Modify User

Username: 11

Modify Password

Modification Mode: Admin Account

Admin Username: admin

Admin Password: []

New Password: []

The minimum pass phrase length is 8 characters

Weak Medium Strong

Confirm Password: []

Group Name: user

Memo: []

- Delete users
Click  to delete the added users.



Admin account cannot be deleted.

- View the authorities
 - If the current account has the permission of user management, click to view the login authorities of other accounts. If not, you can only view the login authorities of the current account.

4.8.4 Safety

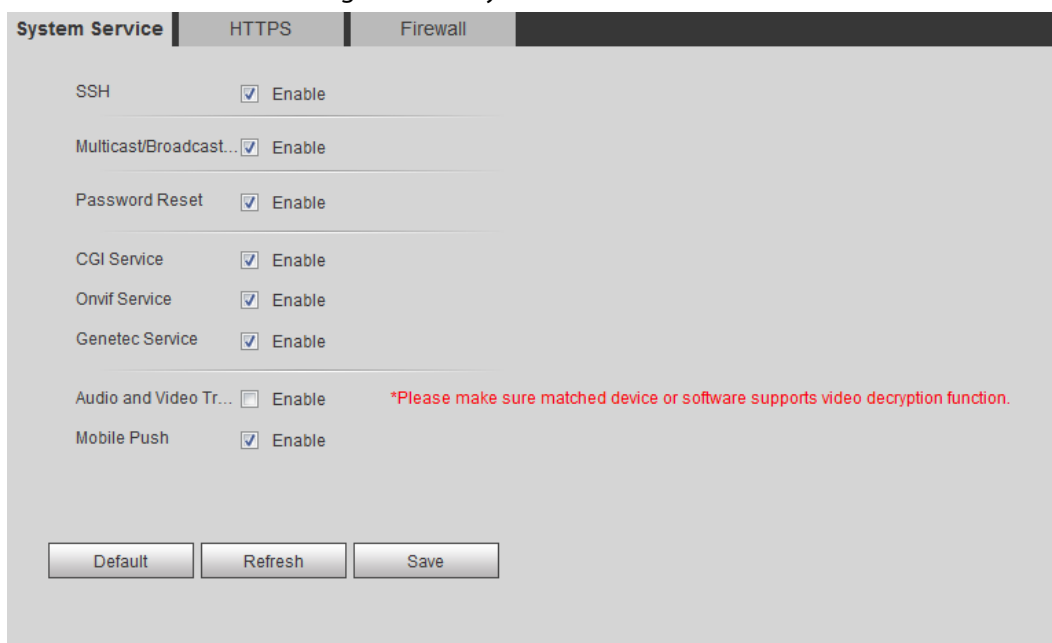
You can configure system service, HTTPS, and firewall.

4.8.4.1 System 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 **Setting > System > Safety > System Service**.


Figure 4-109 System service



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

Table 4-41 Description of system 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 previewing the device video image simultaneously through network, they can find your device with multicast/broadcast protocol.
Password Reset	Manage system security with this function.

Function	Description
CGI Service	Enable this function, and then other devices can access through this service.
Onvif Service	Enable this function, and then other devices can access through this service.
Genetec Service	Enable this function, and then other devices can access through this service.
Audio and Video Transmission Encryption	Enable to encrypt audio/video transmission.  Make sure that the other devices and software that working together with the camera support video decryption.
Mobile Push	Enable this function, and then the system would send the snapshot that was taken when alarm is triggered to your phone, this is enabled by default.

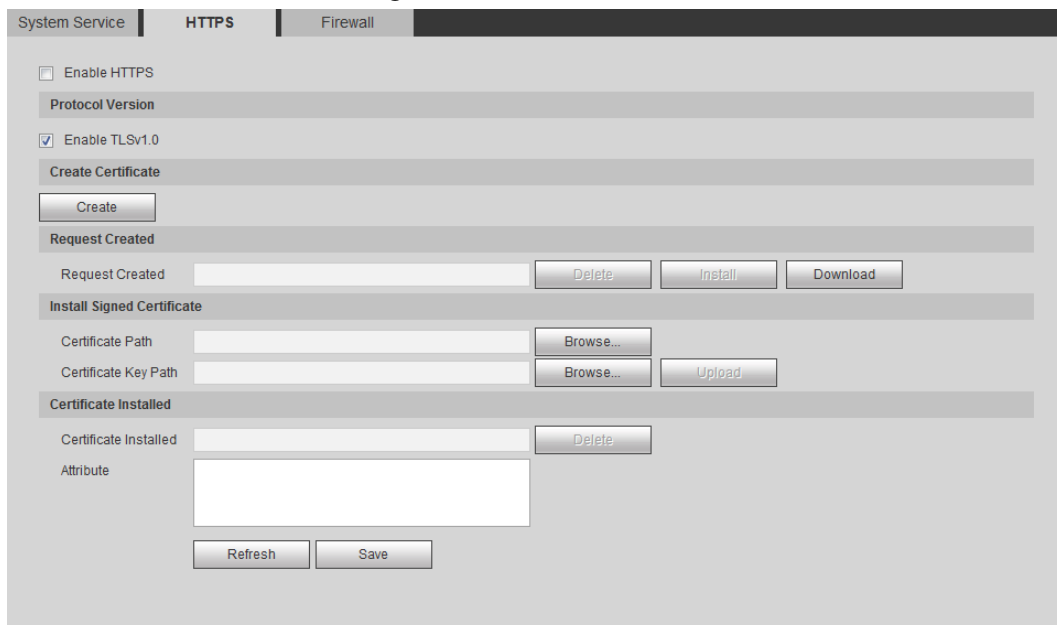
Step 3 Click **Save**.

4.8.4.2 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.

Step 1 Select **Setting > Network > HTTPS**.

Figure 4-110 HTTPS



Step 2 Create a certificate or upload an authenticated certificate.

- For creating a certificate, click **Create**.

Figure 4-111 HTTPS dialog box

- For uploading the authenticated certificate, click **Browse** to select the certificate and certificate key, click **Upload** to upload them, and then skip to Step5.

Step 3 Enter the required information and then click **Create**.



The entered **IP or Domain name** must be the same as the IP or domain name of the device.

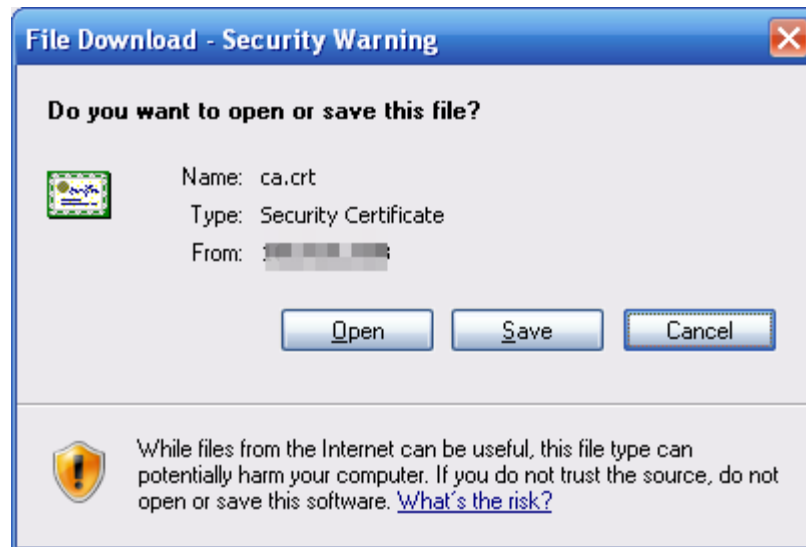
Step 4 Click **Install**.

Figure 4-112 Certificate installation

Step 5 Click **Download** to download root certificate.

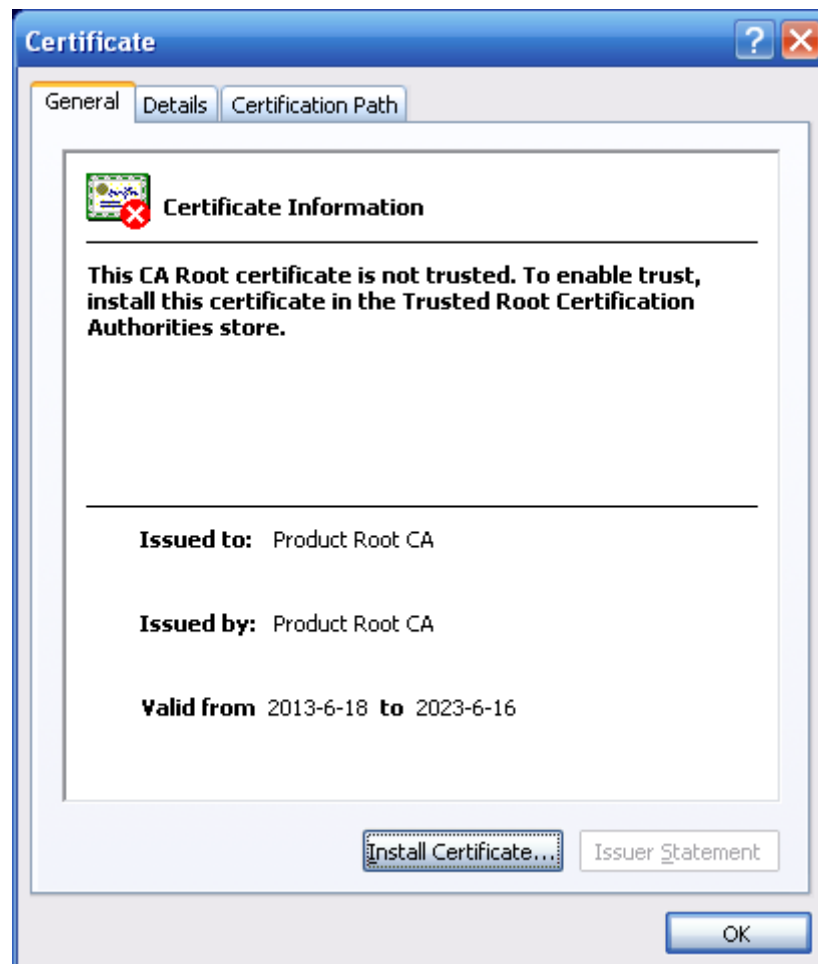
Step 6 Click **Download Root Certificate**.

Figure 4-113 File download



Step 7 Click **Open**.

Figure 4-114 Certificate information



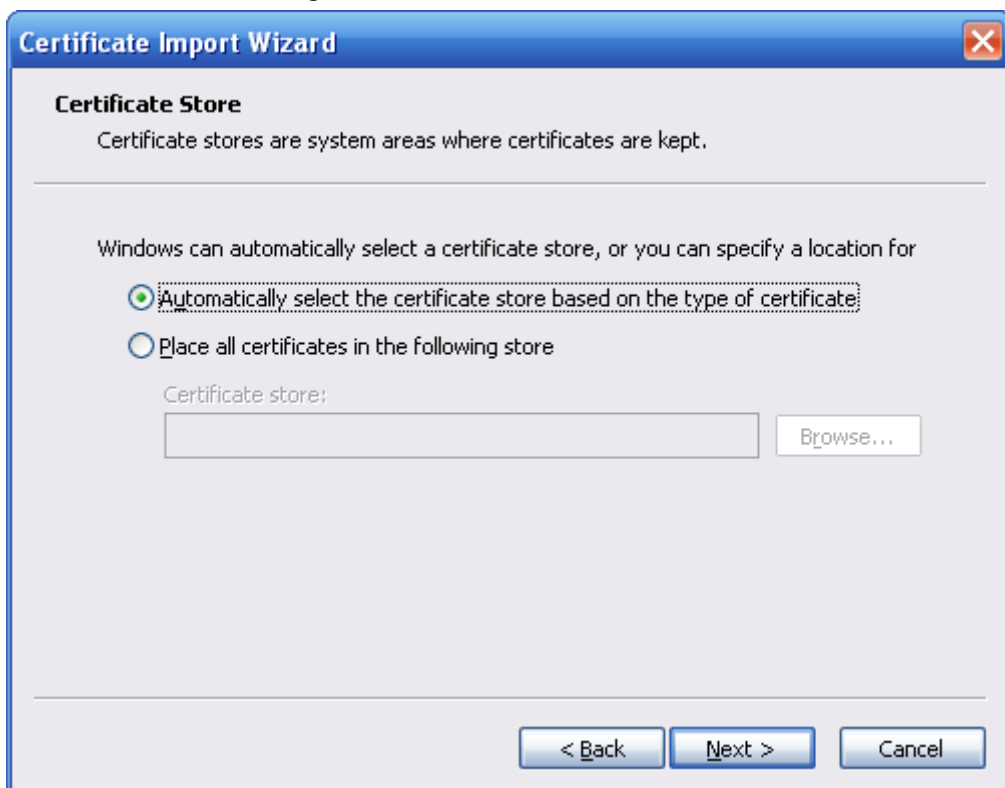
Step 8 Click **Install Certificate**.

Figure 4-115 Certificate import wizard (1)



Step 9 Click **Next**.

Figure 4-116 Certificate store



Step 10 Select the storage location and click **Next**.

Figure 4-117 Certificate import wizard (2)



Step 11 Click **Finish** and a dialog box showing **The import was successful** pops up.

Figure 4-118 Import succeeds



4.8.4.3 Firewall

Configure **Network Access**, **PING prohibited** and **Prevent Semijoin** to enhance network and data security.

- **Network Access:** Set trusted list and restricted list to limit access.
 - ◇ **Allowlist:** Only when the IP/MAC of your PC in the allowlist, can you access the camera. Ports are the same.
 - ◇ **Blocklist:** When the IP/MAC of your PC is in the blocklist, you cannot access the camera. Ports are the same.
- **PING prohibited:** Enable **PING prohibited** function, and the camera will not respond to the ping request.
- **Prevent Semijoin:** Enable **Prevent Semijoin** function, and the camera can provide service normally under Semijoin attack.



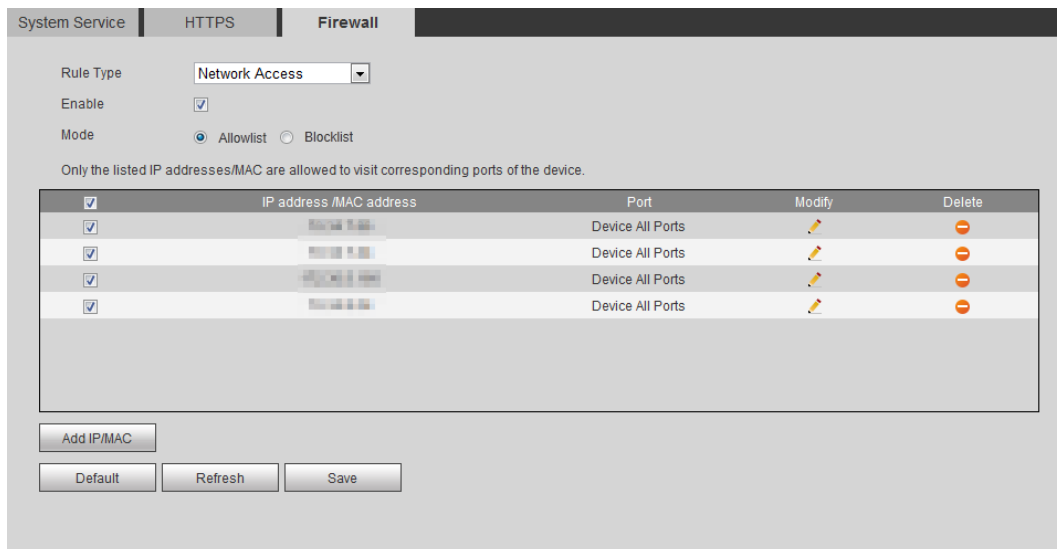
- You cannot set allowlist or blocklist for camera IP or MAC addresses.

- You cannot set allowlist or blocklist for port MAC addresses.
- When the IP addresses of the camera and your PC are in the same LAN, MAC verification takes effect.
- When you access the camera through internet, the camera verifies the MAC address according to the router MAC.

This section takes **Network Access** as an example.

Step 1 Select **Setting > System > Safety > Firewall**.

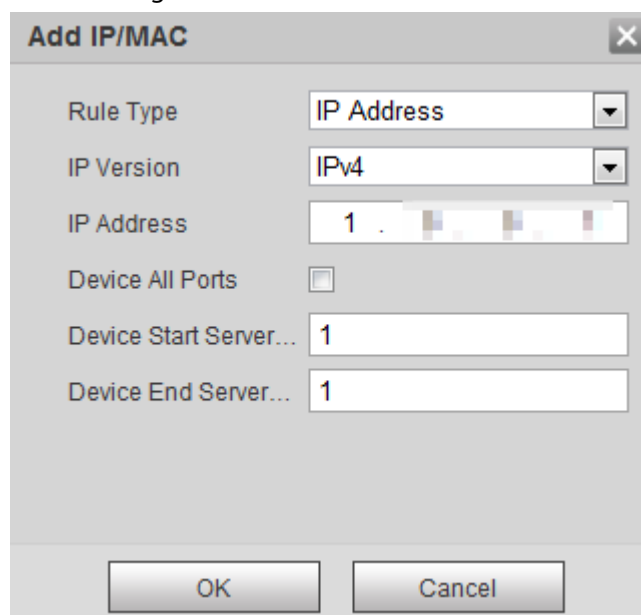
Figure 4-119 Firewall



Step 2 Select **Network Access** from **Rule Type** list, and then select the **Enable** checkbox.

- Enable **PING prohibited** and **Prevent Semijoin**, and click **Save**. You do not need to configure parameters.
- Enable **Network Access**, and configure allowlist and blocklist.
 - ◇ Select the mode: **Allowlist** and **Blocklist**.
 - ◇ Click **Add IP/MAC**.

Figure 4-120 Add IP/MAC



Step 3 Configure parameters.

Table 4-42 Description of adding IP/MAC parameters

Parameter	Description
Rule Type	Select IP address, IP segment, MAC address or all IP addresses. <ul style="list-style-type: none"> IP address: Select IP version and enter the IP address of the host to be added. IP segment: Select IP version and enter the start address and end address of the segment to be added. MAC address: Enter MAC address of the host to be added. All IP addresses: Set all IP addresses in allowlist or restricted list.
Device All Ports	Set access ports. You can select all ports or the ports in defined areas. <ul style="list-style-type: none"> Device all ports: Set all IP port in allowlist or Blocklist. When selecting BlockList in Mode, and All IP Address in Rule Type, you cannot select the Device All Ports checkbox. Device start server port and Device end server port: Set Device start server port and device end server port, and the range is 1–65535.
Device Start Server Port	
Device End Server Port	

Step 4 Click **OK**, and the **Firewall** interface is displayed.

Step 5 Click **Save**.

4.8.5 Peripheral

4.8.5.1 Serial Port Settings


Set the serial port of the external device.

Step 1 Select **Setting > System > Peripheral > Serial Port Setting**.

Figure 4-121 Serial port settings

Step 2 Configure serial port settings parameters.

Table 4-43 Description of serial port settings parameters

Parameter	Description
Address	The corresponding device address. It is 1 by default.  Make sure that the address is the device address; otherwise you cannot control the device.
Baud Rate	Select the baud rate for the camera. It is 9600 by default.
Date Bit	It is 8 by default.
Stop Bit	It is 1 by default.
Parity	It is None by default.

Step 3 Click **Save**.

4.8.5.2 External Light

You need to configure external light mode when the external light is used.

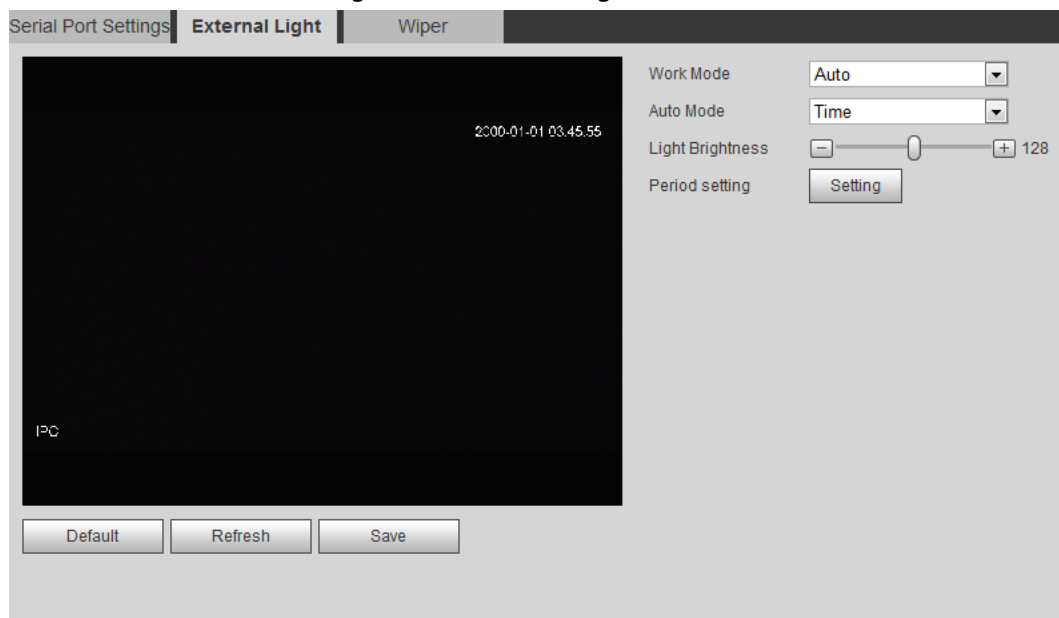
Prerequisites

- Connect external light with RS-485 port.
- You have configured serial port parameters. For details, see "4.8.5.1 Serial Port Settings".

Procedure

Step 1 Select **Setting** > **System** > **Peripheral** > **External Light**.

Figure 4-122 External light



Step 2 Configure external light work mode.

Table 4-44 Description of external light parameters

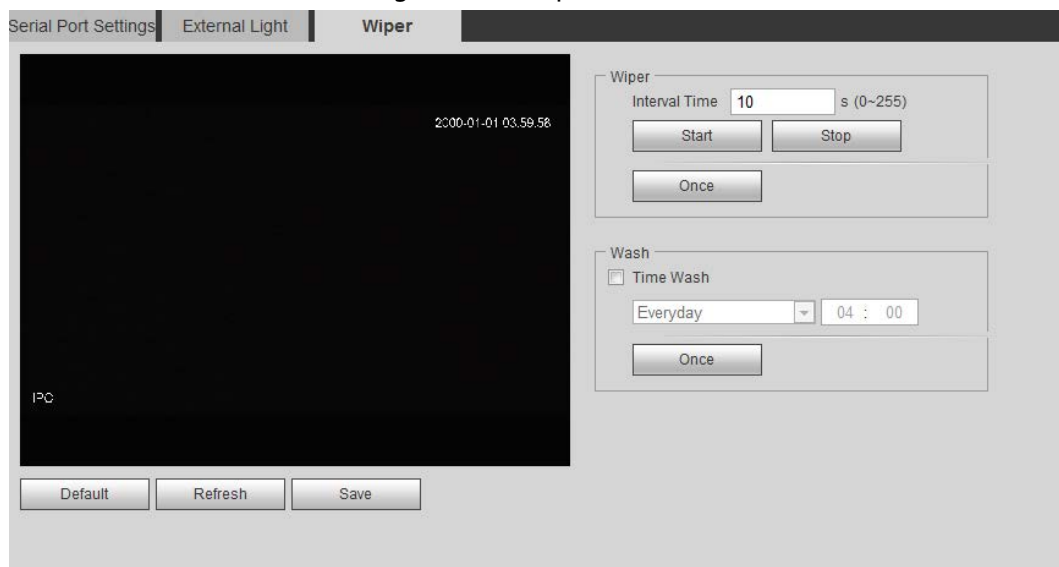
Parameter	Description
Work Mode	<ul style="list-style-type: none"> • Off: Turn off the external light. • Manual: Set the light brightness manually. • Auto: The camera turns on or turns off the light according to the light time and photoresistor automatically.
Auto Mode	<ul style="list-style-type: none"> • Time: When selecting Time in Auto Mode, click Setting to set the arming period. During the arming period, the external light is on. For details of arming period setting, see "5.1.1.1 Setting Period". • Photoresistor: When you select Photoresistor in Auto Mode, the system turns on the external light according to the brightness automatically.
Light Brightness	Set the brightness of the external light.

Step 3 Click **Save**.

4.8.5.3 Wiper

Step 1 Select **Setting** > **System** > **Peripheral** > **Peripheral** > **Wiper**.

Figure 4-123 Wiper



Step 2 Configure wiper work mode.

Table 4-45 Description of wiper parameters

Parameter	Description
Interval Time	The interval time between stop mode and start mode. For example, set the time to 10 s, and the wiper will work every 10 s.
Start	Set the work status of the wiper.
Stop	<ul style="list-style-type: none"> • Start: Click Start, and the wiper works as the set interval time. • Stop: Click Stop, and the wiper stops working.
Once	<ul style="list-style-type: none"> • Once: Click Once, and the wiper works once.

Parameter	Description
Time Wash	Select the Time Wash checkbox and set the time, and then the wiper will work as the set time. Click Once , and the wiper works once. It can be used to check whether the wiper can work normally.

Step 3 Click **Save**.

5 Event

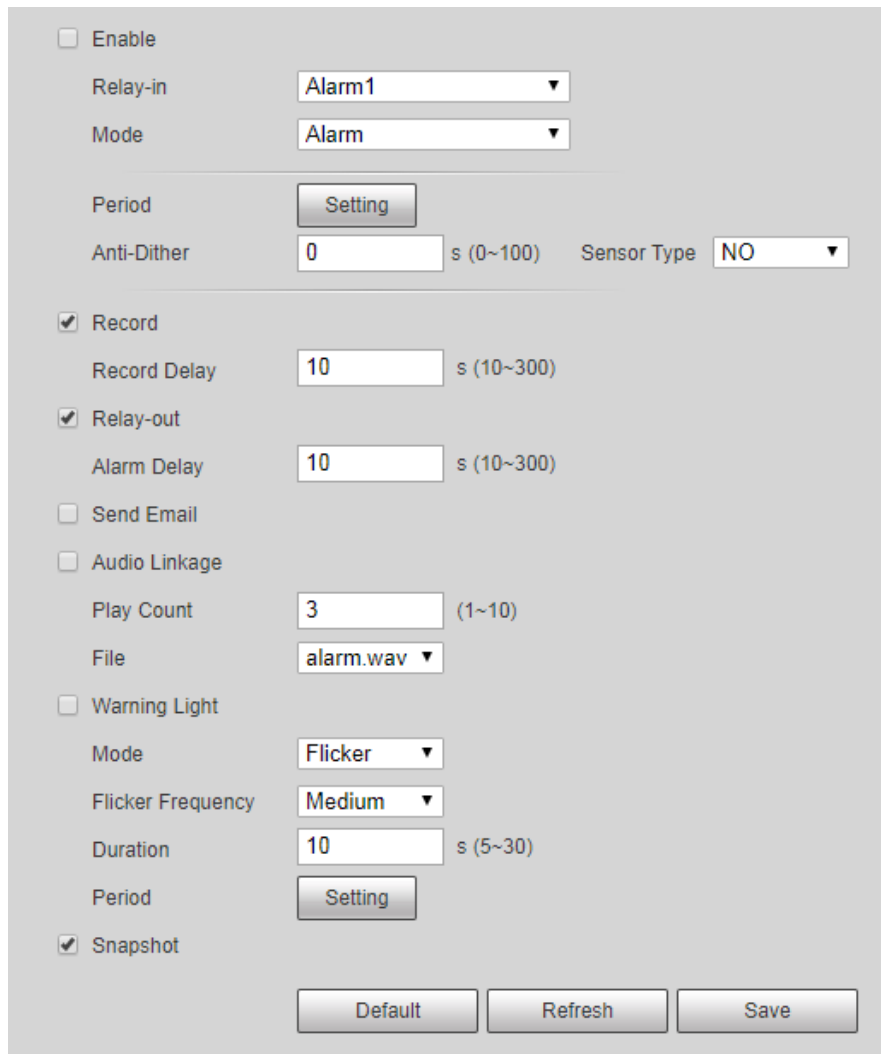
This chapter introduces intelligent event settings, including smart track, panoramic calibration, video detection, audio detection, smart plan, IVS, face detection, face recognition, people counting, heat map, video Metadata, alarm, and abnormality.

5.1 Setting Alarm Linkage

5.1.1 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. Interfaces might vary with different events, and the actual interface shall prevail.

Figure 5-1 Alarm linkage



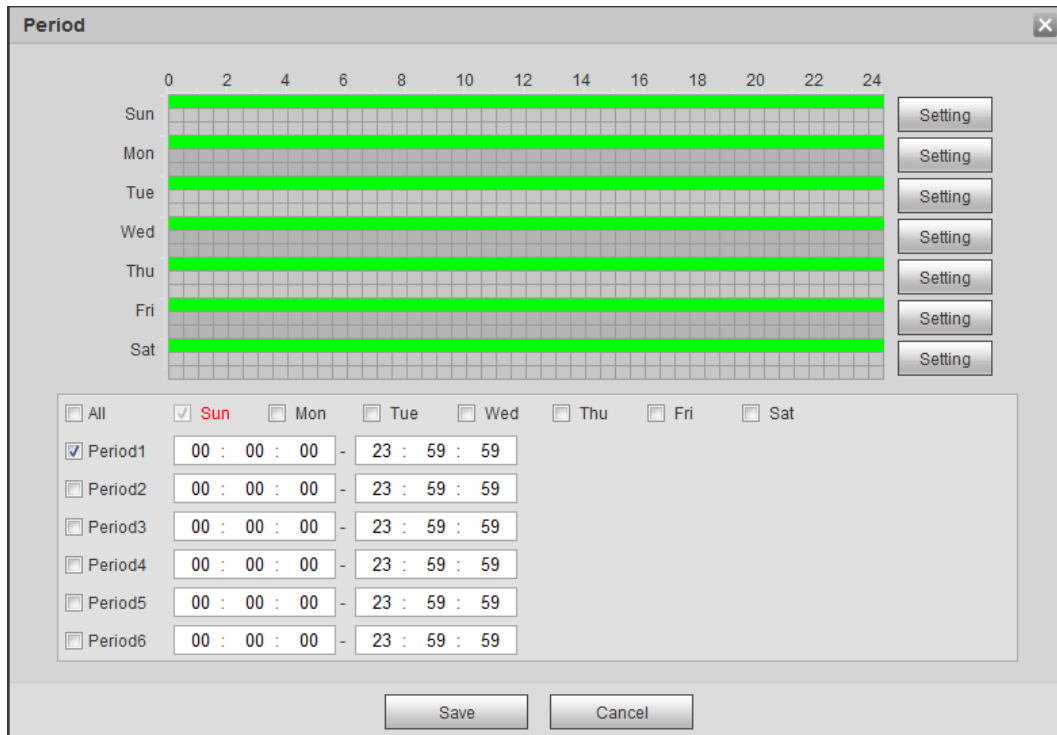
Enable
 Relay-in: Alarm1
 Mode: Alarm
 Period: Setting
 Anti-Dither: 0 s (0~100) Sensor Type: NO
 Record
 Record Delay: 10 s (10~300)
 Relay-out
 Alarm Delay: 10 s (10~300)
 Send Email
 Audio Linkage
 Play Count: 3 (1~10)
 File: alarm.wav
 Warning Light
 Mode: Flicker
 Flicker Frequency: Medium
 Duration: 10 s (5~30)
 Period: Setting
 Snapshot
 Default Refresh Save

5.1.1.1 Setting Period

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

Step 1 Click **Setting** next to **Period**.

Figure 5-2 Period



Step 2 Set arming periods. Alarms will be triggered in the time period in green on the timeline.

- Method 1: Directly press and drag the left mouse button on the timeline.
- Method 2: Enter an actual time period.
 1. Click **Setting** next to a day.
 2. Select a time period to be enabled.
 3. Enter start time and end time of a time period.



- ◇ Select **All** or checkboxes of some days to set the time period of multiple days at one time.
- ◇ You can set 6 time periods per day.

Step 3 Click **Save**.

5.1.1.2 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 **Record Delay** setting.

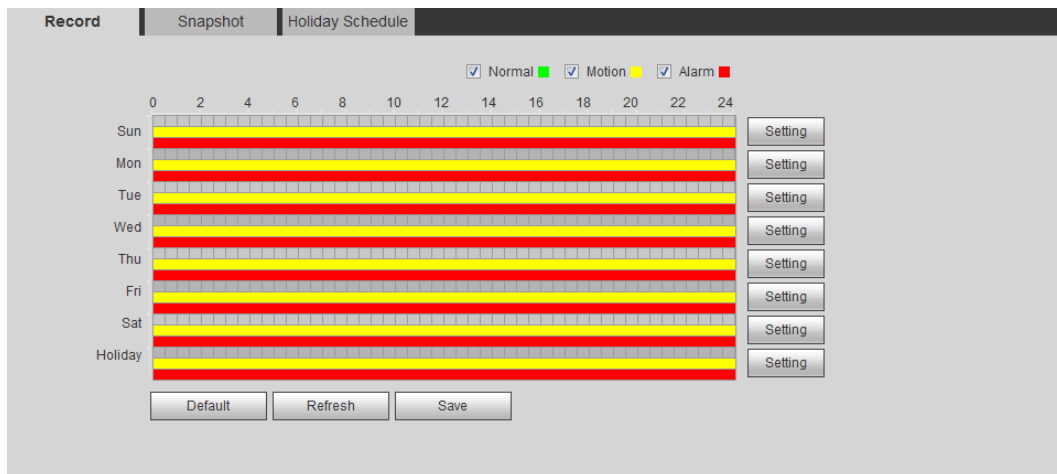
To use the record linkage function, set record plan for motion detection alarm and enable auto recording in record control.

5.1.1.2.1 Setting Record Plan

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

Step 1 Select **Setting** > **Storage** > **Schedule** > **Record**.

Figure 5-3 Record

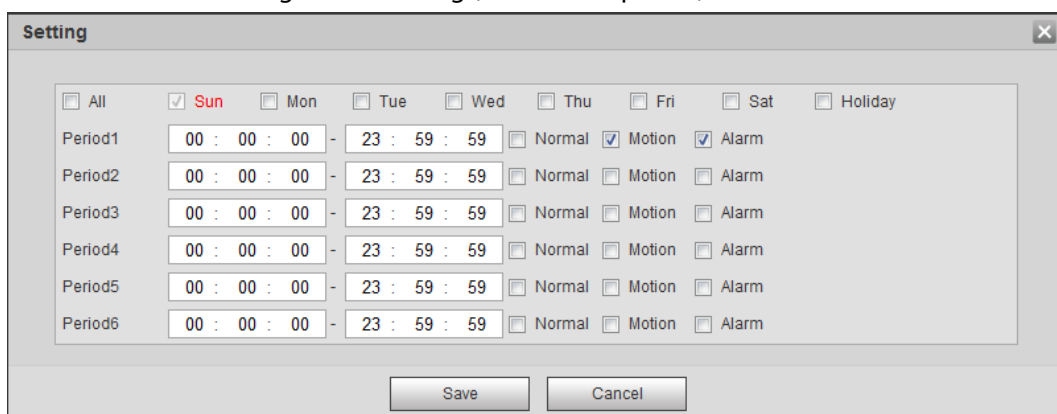


Step 2 Set record plan.

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).

- Method one: 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.
- Method two: Enter an actual time period.
 1. Click **Setting** next to a day.

Figure 5-4 Setting (record time period)



2. Select a day, and the alarm type next to a period, and then set the period.



- ◇ Select **All** or checkboxes of some days to set the time period of multiple days at one time.
- ◇ You can set 6 time periods per day.

Step 3 Click **Save**.

5.1.1.2.2 Setting Record Control

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



Make sure that the SD card is authenticated before recording if you use Dahua smart card. For details, see "4.5.2.5 Path".

Step 1 Select **Setting** > **Storage** > **Record Control**.

Figure 5-5 Record control

Step 2 Set parameters.

Table 5-1 Description of record control parameters

Parameter	Description
Pack Duration	The time for packing each video file.
Pre-event Record	<p>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 of 5 s before the alarm is triggered.</p> <p>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.</p>
Disk Full	<p>Recording strategy when the disk is full.</p> <ul style="list-style-type: none"> • Stop: Stop recording when the disk is full. • Overwrite: Cyclically overwrite the earliest video when the disk is full.
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 **Save**.

5.1.1.2.3 Setting Record Linkage

On the alarm event setting interface (such as the motion detection interface), select **Record** and set **Record Delay** to set alarm linkage and record delay.

After **Record Delay** is configured, alarm recording continues for an extended period after the alarm ends.

Figure 5-6 Record linkage



5.1.1.3 Snapshot Linkage

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

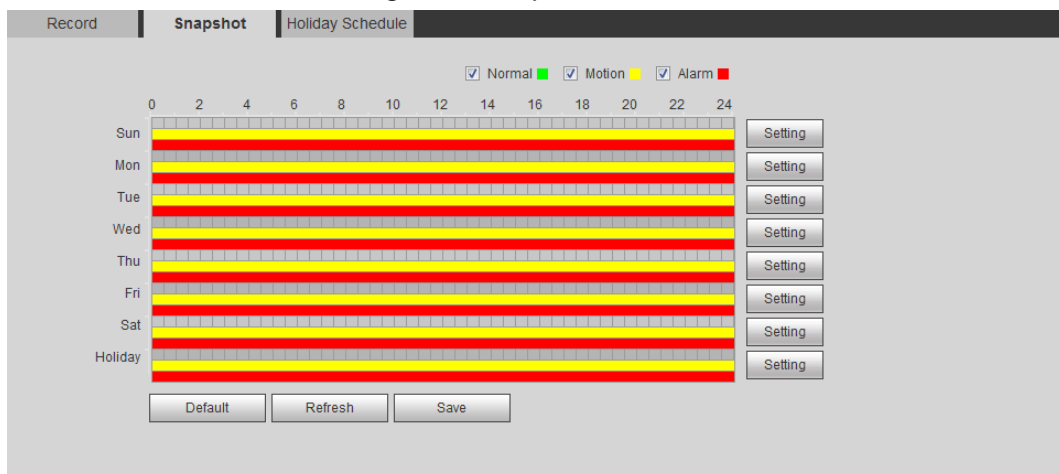
After **Motion** is enabled in **Snapshot**, the system takes snapshots when an alarm is triggered. For querying and setting snapshot storage location, see "4.5.2.5 Path".

5.1.1.3.1 Setting Snapshot Plan

According to the configured snapshot plan, the system enables or disables snapshot at corresponding time.

Step 1 Select **Setting** > **Storage** > **Schedule** > **Snapshot**.

Figure 5-7 Snapshot



Step 2 Select snapshot type and set time period.

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

- Method one: Select snapshot type, such as **Normal**, and directly press and drag the left mouse button to set time period for normal snapshot on the timeline.
- Method two: Enter an actual time period.
 1. Click **Setting** next to a day.

Figure 5-8 Setting (snapshot time period)

2. Select a day, and the alarm type next to a period. Then set the period.



- ◇ Select **All** or checkboxes of some days to set the time period of multiple days at one time.
- ◇ You can set 6 time periods per day.

3. You can set 6 time periods per day.

Step 3 Click **Save**.

5.1.1.3.2 Setting Snapshot Linkage

On the alarm event setting interface (such as the motion detection interface), select **Snapshot** and set alarm linkage snapshot.

Figure 5-9 Snapshot linkage

Snapshot

5.1.1.4 Relay-out Linkage

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

On the alarm event setting interface (such as the motion detection interface), select **Alarm** and set **Alarm Delay**.

When alarm delay is configured, alarm continues for an extended period after the alarm ends.

Figure 5-10 Relay-out linkage

Relay-out
Alarm Delay s (10~300)

5.1.1.5 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 "4.6.5 SMTP (Email)".

Figure 5-11 Email linkage

Send Email

5.1.1.6 PTZ Linkage

When an alarm is triggered, the system links PTZ to do some operations. For example, the system links PTZ to rotate to the preset X.

Figure 5-12 PTZ linkage

PTZ Activation No. (1~255)

5.1.1.7 Warning Light Linkage

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

Set **Mode**, **Flicker Frequency**, **Duration**, and **Period**.

- **Mode:** The display mode of the warning light when an alarm is triggered. It includes **Normally on** and **Flicker**. When setting **Flicker** as the mode, you need to set the flicker frequency.



For the camera with red and blue alarm light, you can only select **Flicker** in **Mode**.

- **Duration:** After setting warning light duration, the warning light is turned off after an extended time of period after an alarm. It is 5 seconds–30 seconds.
- **Period:** The period for using warning light. When an alarm triggered during the configured period, the system links warning light. For the configuration, see "5.1.1.1 Setting Period".

Figure 5-13 Warning light linkage

Warning Light

Mode

Flicker Frequency

Duration s (5~30)

Period

5.1.1.8 Audio Linkage

The system broadcasts alarm audio file when an alarm event occurs. Select **Setting** > **Camera** > **Audio** > **Alarm Audio** to set alarm audio file.

Figure 5-14 Audio linkage

Audio Linkage

Play Duration s

5.1.2 Subscribing Alarm

5.1.2.1 About Alarm Types

For alarm types and preparations of alarm events, see Table 5-2.

Table 5-2 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 "5.4.1 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 "5.19.1 Setting SD Card".
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 "5.19.1 Setting SD Card".
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 "5.4.2 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 "5.18 Setting Relay-in".
Illegal Access	The alarm is triggered when the number of consecutive login password error is up to the allowable number.	Illegal access detection is enabled. For details, see "5.19.3 Setting Illegal Access".
Audio Detection	The alarm is triggered when there is audio connection problem.	Abnormal audio detection is enabled. For details, see "5.6 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 "5.4.3 Setting Scene Changing".
Voltage Detection	The alarm is triggered when the device detects abnormal voltage input.	Voltage detection is enabled. For details, see "5.19.4 Setting Voltage Detection".
Security Exception	The alarm is triggered when the device detects malicious attack.	Voltage detection is enabled. For details, see "5.19.5 Setting Security Exception".

5.1.2.2 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.

Step 1 Click the **Alarm** tab.

Figure 5-15 Alarm (subscription)

No.	Time	Alarm Type	Source IP	Alarm Channel

Alarm Type

Motion Detection Disk Full

Disk Error Video Tampering

External Alarm Illegal Access

Audio Detection IVS

Scene Changing Security Exception

Operation


Prompt

Alarm Tone

Play Alarm Tone

Tone Path:

Step 2 Select **Alarm Type** according to the actual need.

- Select **Prompt**. The system prompts and records alarm information according to actual conditions.
 - ◇ When the subscribed alarm event is triggered and the **Alarm** interface is not displayed, the  is displayed on the **Alarm** tab and the alarm information is recorded automatically. Click the **Alarm** tab, and this icon disappears.
 - ◇ When the subscribed alarm event is triggered and the **Alarm** interface is displayed, the corresponding alarm information is displayed in the alarm list at the right side of the **Alarm** interface.
- Select **Play Alarm Tone**, and select the tone path.
The system would play the selected audio file when the selected alarm is triggered.

5.2 Setting Smart Track

After setting calibration and parameters for smart track, the tracking speed dome can automatically link to a corresponding position and track an object till it is out of the monitoring range or the set tracking time is reached when the intelligent rules for panoramic camera triggers an alarm.

5.2.1 Setting Calibration Parameters for Smart Track

The camera has calibration parameters by default, and you can modify the parameters manually when the effect is not good with default setting.



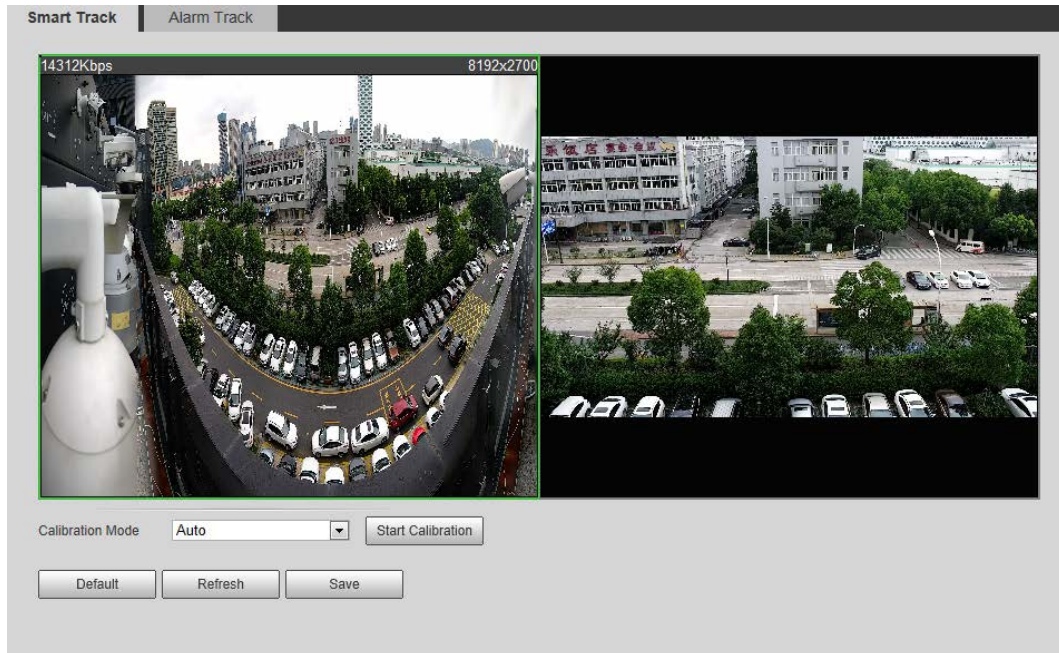
Auto calibration mode is available on some select models.

Step 1 Select **Setting > Event > Smart Track > Smart Track**.

Step 2 Configure calibration parameters.

- Auto calibration
Select **Auto** in **Calibration Mode**, and then click **Start Calibration**.

Figure 5-16 Auto calibration



- Manual calibration
Select **Manual** in **Calibration Mode**, select the channel that you need, and then add calibration point for it in the live image.

Figure 5-17 Manual calibration (1)

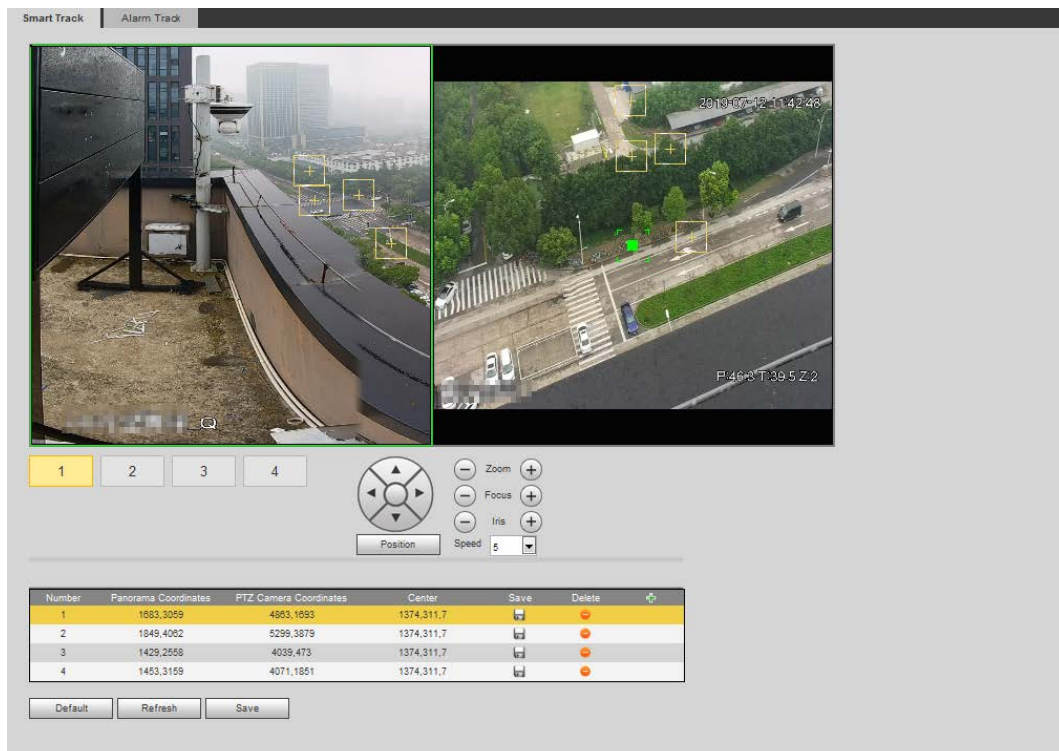
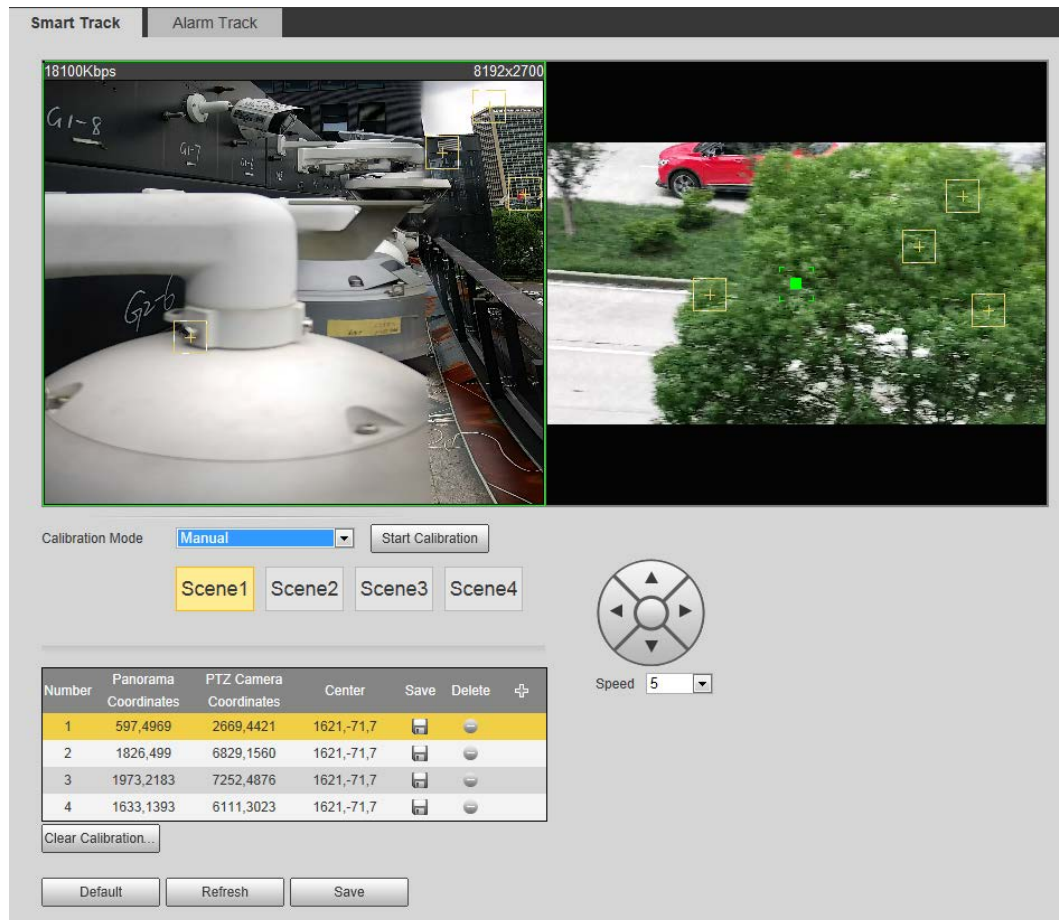


Figure 5-18 Manual calibration (2)



- 1) Adjust the speed dome lens and turn it to the same view as the chosen lens, and then click . The calibration boxes are displayed in both images.
- 2) Pair each box in the two images, and keep the paired boxes at the same spot of the live view.
- 3) Click . You need at least 4 pairs of calibration boxes to ensure the views of the speed dome and the panoramic camera as similar as possible.

Step 3 Click **Save**.

5.2.2 Enabling Alarm Track

Alarm Track is disabled by default. Smart Track is enabled only after Alarm Track is enabled and intelligent rules of the panoramic camera are configured. Smart Track is supported only when rules of crowd map, intrusion and tripwire are triggered. See "5.8 Setting IVS" and "5.9 Setting Crowd Map".

Step 1 Select **Setting > Event > Smart Track > Alarm Track**.

Figure 5-19 Alarm track

Step 2 Select the **Enable** checkbox to enable track linkage.

After enabling the function, manual positioning, manual tracking and auto tracking take effect.

Step 3 Set parameters.

Table 5-3 Description of alarm track parameters

Parameter	Description
Auto Track	Select On , and the speed dome automatically links to a corresponding position and tracks an object when the intelligent rules of the panoramic camera trigger alarms.
Track Time	Set the alarm track time. <ul style="list-style-type: none"> Before an object disappears: The speed dome would automatically link to a corresponding position and tracks an object until the object moves out of the monitoring range when the intelligent rules of the panoramic camera trigger alarms. Custom: Set the auto alarm track time of the speed dome.
Idle Time	It is an interval from the end of alarm track of the speed dome to the start of idle mode.
Idle Position	Set Idle Time and Idle Position . If no event needs to be tracked after the configured idle time, the device automatically rotates to the set idle position. For example, the Idle Time is set to be five seconds and the Idle Position is set to be preset point 1. When the speed dome does not start tracking after five seconds, it automatically rotates to preset 1. To set Idle Position , first set a preset point. For preset point, see "4.3.2.1 Preset".

Step 4 Click **Save**.

5.3 Setting Panoramic Calibration

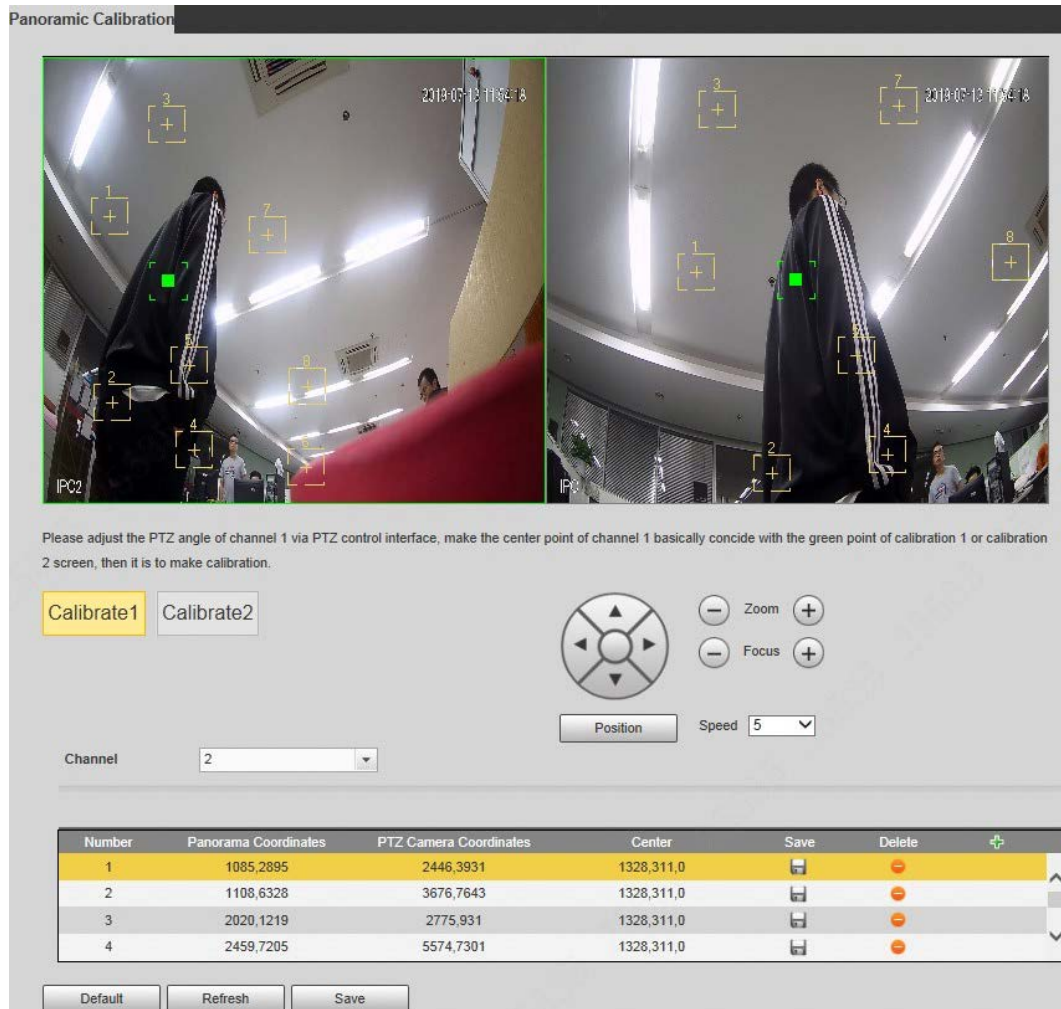
The device has calibration parameters by default, and you can modify the parameters manually

when the effect is not good with default setting. Before manually calibrating a channel, clear all default calibration parameters.

Channel 1 is a PTZ camera. You should calibrate the scene coordinates of **Channel 1** and other channels. Take **Channel 2** as an example.

Step 1 Select **Setting > Event > Panoramic Calibration**.

Figure 5-20 Panoramic calibration



Step 2 Select channel 2, and then select a calibration number under the video images in turns (See Figure 5-21) to add calibration points to the corresponding video images. Take **Calibrate 1** as an example.

Figure 5-21 Select a calibration number



- 1) Adjust the PTZ angle of channel 1 through the PTZ control interface to rotate the center of channel 1 to a position aligned with the green point in **Calibrate 1** image, and then click .

Calibration box is displayed in images of **Channel 1** and **Calibrate 1**

- 2) Respectively drag calibration boxes on images of **Channel 1** and **Calibrate 1** to the corresponding positions. Click to save this pair of calibration boxes.

You are recommended to drag calibration box to a static position with clear edges in

the image. This can ensure the edges can be accurately distinguished by the camera.

After the calibration record is saved, the calibration box is displayed in yellow.

Repeat 1) to 2) to add at least 4 pairs of calibration points to each calibration picture.

Step 3 Click **Save**.

5.4 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.

5.4.1 Setting Motion Detection

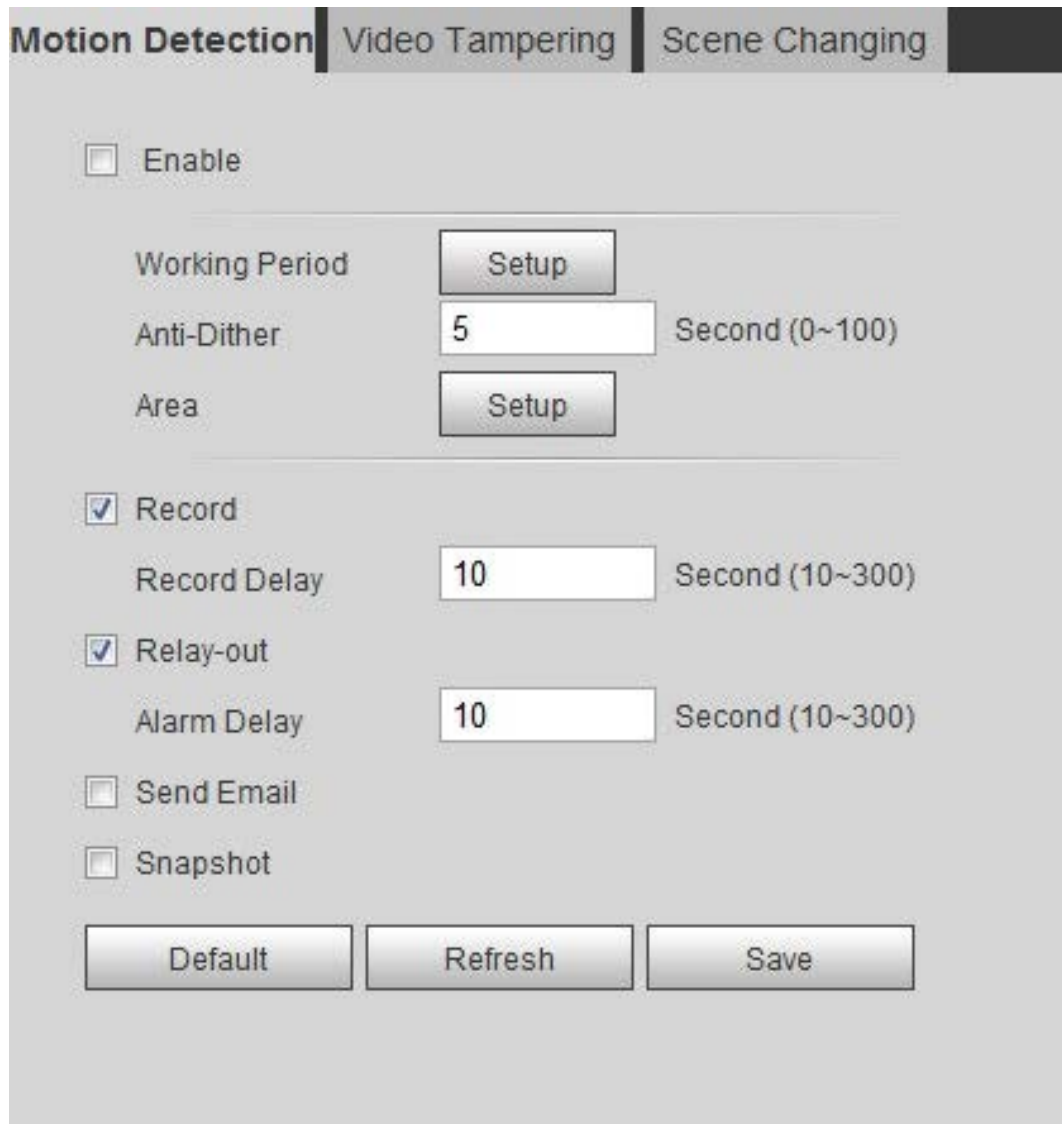
The system performs an alarm linkage when the moving object appears on the image and its moving speed reaches the preset sensitivity.



- If you enable motion detection and smart motion detection simultaneously, and configure the linked activities, the linked activities take effect as following:
 - ◇ 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 **Setting > Event > Video Detection > Motion Detection**.

Figure 5-22 Motion detection



Motion Detection | Video Tampering | Scene Changing

Enable

Working Period

Anti-Dither Second (0~100)

Area

Record

Record Delay Second (10~300)

Relay-out

Alarm Delay Second (10~300)

Send Email

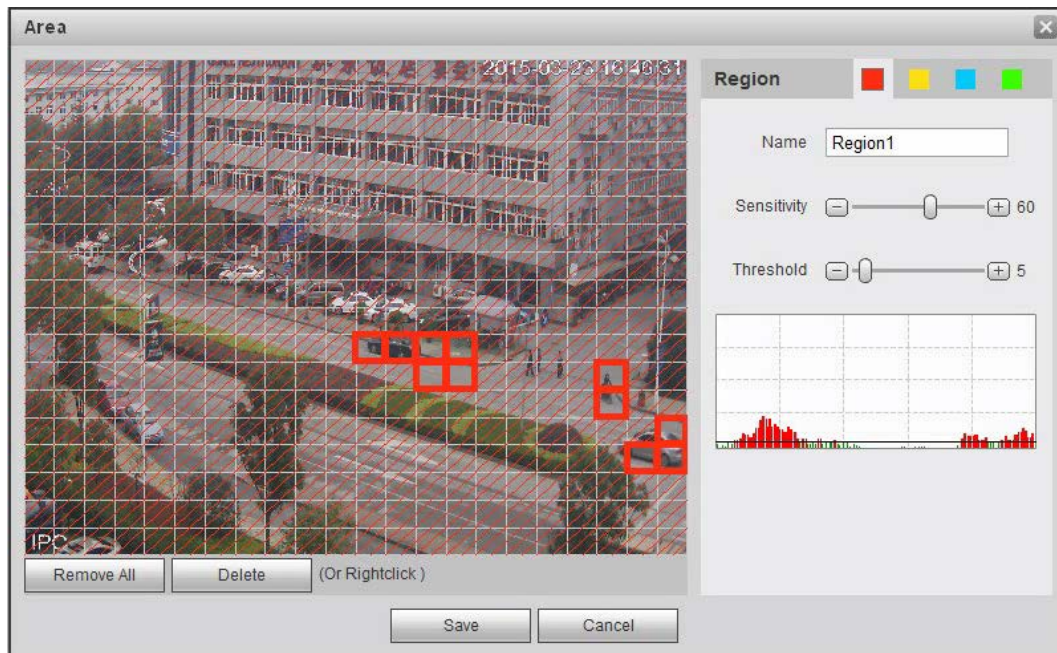
Snapshot

Step 2 Select the **Enable** checkbox to enable motion detection function.


Step 3 Set the area for motion detection.

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

Figure 5-23 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 **Save**.

Step 4 Set arming periods and alarm linkage action. For details, see "5.1.1 Alarm Linkage".
Anti-dither: After the **Anti-dither** time is set, the system only records one motion detection event in the period.

Step 5 Click **Save**.

5.4.2 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 **Setting > Event > Video Detection > Video Tamper**.

Step 2 Select the event type.

- **Video Tampering**: When the percentage of the tampered image and the duration exceed the configured values, an alarm will be triggered.
- **Defocus Detection**: When the image is blurred, an alarm will be triggered. This

function is available on some select models.

Figure 5-24 Video tampering

Table 5-4 Description of video temper parameter

Parameter	Description
Tamper Area	When the percentage of the tampered image and the duration exceed the configured values, an alarm will be triggered. The tamper area is 30% and the duration is 5 s by default.
Duration	
Anti-Dither	Only record one alarm event during the anti-dither period.

Step 3 Set arming periods and alarm linkage action. For details, see "5.1.1 Alarm Linkage".

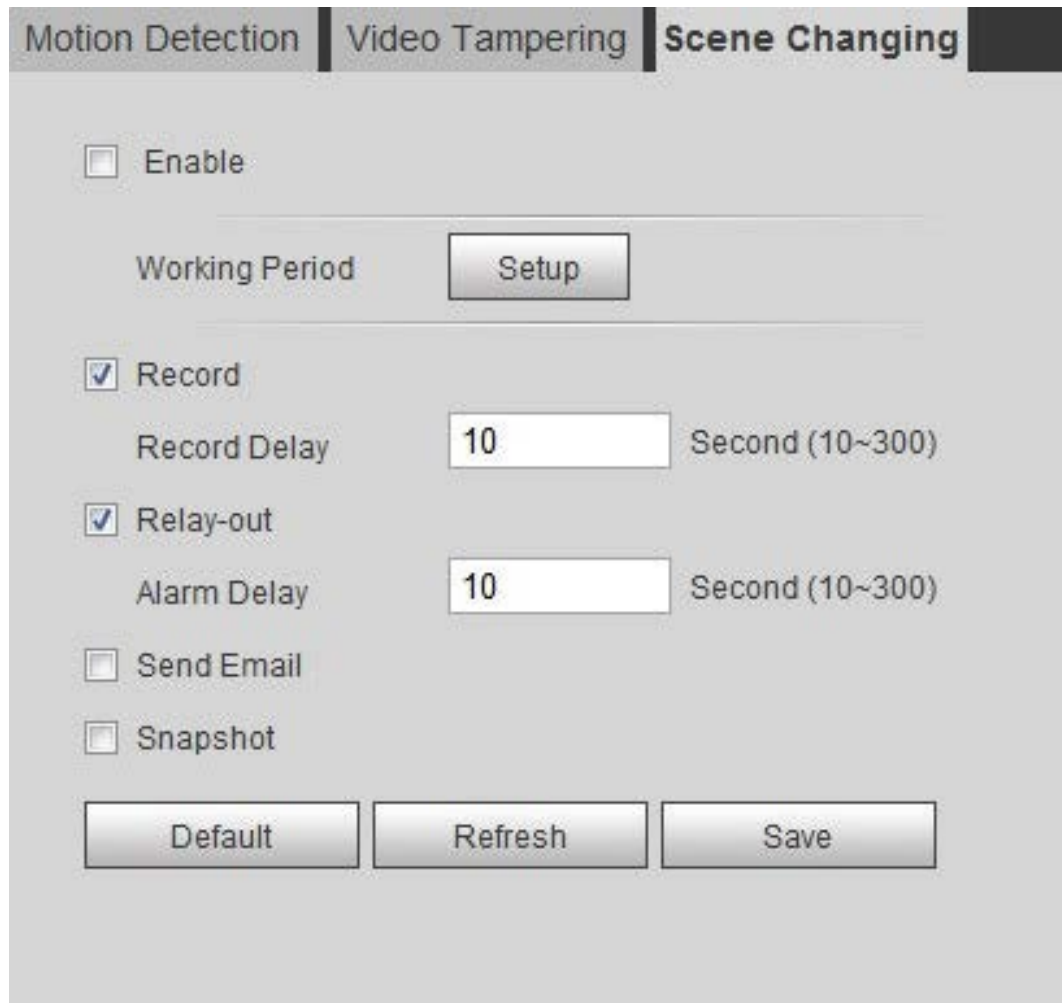
Step 4 Click **Save**.

5.4.3 Setting Scene Changing

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

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

Figure 5-25 Scene changing



Step 2 Set arming periods and alarm linkage action. For details, see "5.1.1 Alarm Linkage".

Step 3 Click **Save**.

5.5 Setting Smart Motion Detection

The system performs alarm linkage when human, non-motorized vehicle, or motor vehicle appear on the image and its moving speed reaches the preset sensitivity. Enabling smart motion detection can avoid the alarms triggered by the environment changes, and the function is enabled by default.

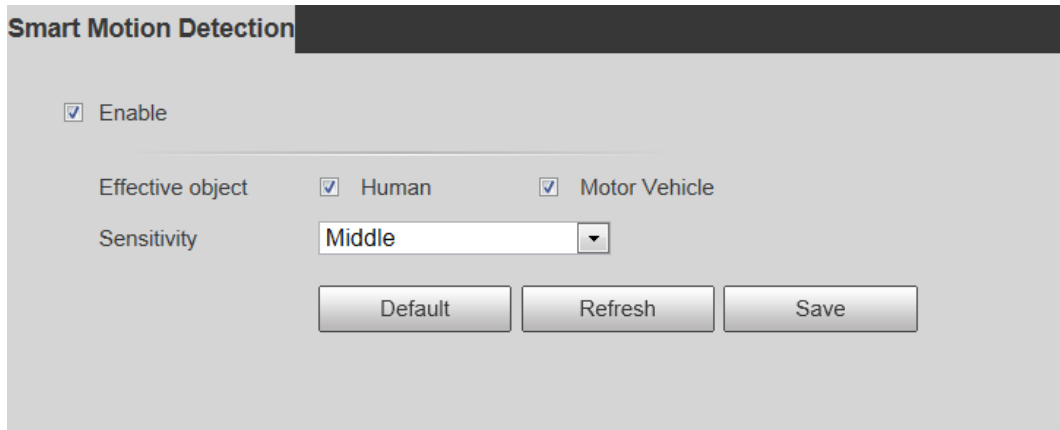
Prerequisites

- Select **Setting > Event > Video Detection > Motion Detection** to enable the motion detection function.
- You have set **Period** and **Area** in **Motion Detection**, and make sure that the sensitivity value is larger than 0, and the threshold value is smaller than 100.

Procedure

Step 1 Select **Setting > Event > Smart Motion Detection**.

Figure 5-26 Smart motion detection



- Step 2 Select the **Enable** checkbox to enable the smart motion detection function.
- Step 3 Set effective object and sensitivity.
- Effective object: Includes **Human** and **Motor vehicle**. When you select **Human**, the camera will detect human and non-motorized vehicle.
 - Sensitivity: Includes **Low**, **Middle**, and **High**. The higher the sensitivity is, the easier the alarm will be triggered.
- Step 4 Click **OK**.

5.6 Setting Audio Detection

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

- Step 1 Select **Setting > Event > Audio Detection**.

Figure 5-27 Audio detection

Audio Detection

Enable Input Abnormal

Enable Intensity Change

Sensitivity -
-
+
50

Threshold -
-
+
50

Working Period Setup

Anti-Dither Second (0~100)

Record

Record Delay Second (10~300)

Relay-out

Alarm Delay Second (10~300)

Send Email

Snapshot

Default
Refresh
Save

Step 2 Set parameters.

- Input abnormal: Select the **Enable Input Abnormal** checkbox, and the alarm is triggered when the system detects abnormal sound input.
- Intensity change: Select the **Enable Intensity Change** checkbox and then set **Sensitivity** and **Threshold**. The alarm is triggered when the system detects that the sound intensity exceeds the set 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 Set arming periods and alarm linkage action.

Step 4 Click **Save**.

5.7 Setting Smart Plan

Smart plan includes face detection, heat map, IVS, people counting, face detection, video metadata, stereo analysis and schedule. The intelligent function can be enabled only after the corresponding smart plan is enabled.

5.7.1 Basic Smart Plan

Step 1 Select **Setting > Event > Smart Plan**.

The **Smart Plan** interface is displayed. For smart plan icon, see the table below.

Table 5-5 Description of smart plan icon

Icon	Description	Icon	Description	Icon	Description
	Face detection		Stereo vision		Heat map
	Stereo analysis		IVS		Face recognition
	People counting		Video metadata		Crowd map
	ANPR		Vehicle density	—	—

Step 2 Enable smart functions as need.

Different cameras support different ways to enable smart functions. Select corresponding ways to enable these functions according to the actual interface.

- Select an icon to enable the corresponding smart plan.

Click an icon to enable it, and the selected smart function is highlighted. Click it again to cancel the selection.

If the icon  on the interface, click it to enable the smart function switch.

- Enable smart plan through **Add Plan**.

1. Select a preset point from the **Add Plan** the interface.
The smart plan for the point is displayed.
2. Click the corresponding icon to enable a smart function.
The selected smart function is highlighted. Click it again to cancel the selection.

Step 3 Click **Save**.

5.7.2 Schedule

After enabling this function, you can configure different smart plans at different periods for your camera.

Step 1 Select **Setting > Event > Smart Plan**.

Step 2 Enable **Schedule**.

Figure 5-28 Schedule

Smart Plan

Schedule

Plan

No.	Color	Name	Channel 1	Modify	Delete

Time Settings

	0	2	4	6	8	10	12	14	16	18	20	22	24	
Sun														<input type="button" value="Setting"/>
Mon														<input type="button" value="Setting"/>
Tue														<input type="button" value="Setting"/>
Wed														<input type="button" value="Setting"/>
Thu														<input type="button" value="Setting"/>
Fri														<input type="button" value="Setting"/>
Sat														<input type="button" value="Setting"/>

No Plans

Step 3 Click **Add Plan**.

1. Rename the plan as needed.
2. Select smart plan. Other plans which are incompatible with the one that you selected would turn gray.
3. Click **Save**.
4. (Optional) Follow Step1 to Step3 to add more plans. You can add 10 plans at most.
 - Click to modify the plan added.
 - Click to delete the plan.

Figure 5-29 Add plan (1)

Figure 5-30 Add plan (2)

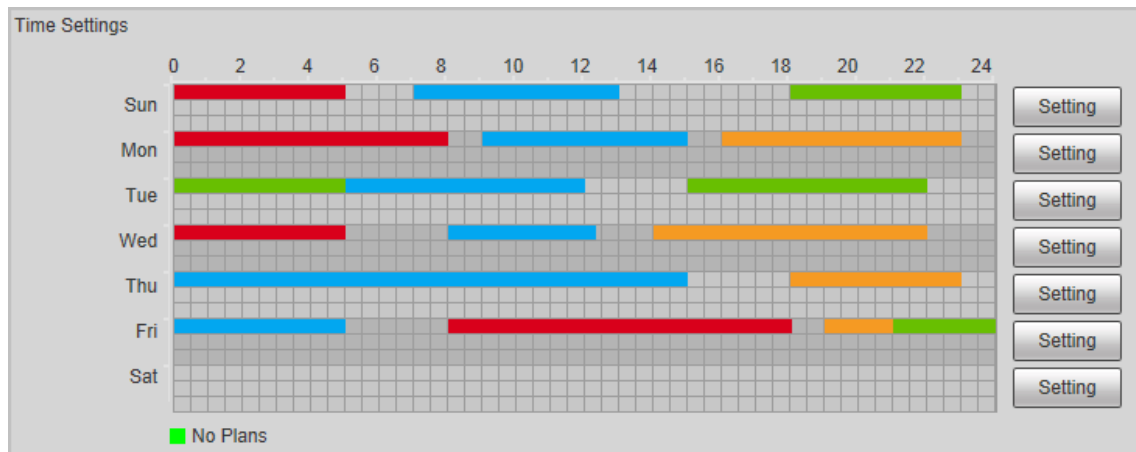
No.	Color	Name	Channel 1	Modify	Delete
1	Red	Plan1	Face Detection		
2	Blue	Plan2	Heat Map		
3	Orange	Plan3	IVS		
4	Green	Plan4	People Counting		

Step 4 Configure the time settings.

1. Click **Settings**.
2. Configure the period. In the **Smart Plan** list, select the type as needed.
3. Click **Save**.
4. (Optional) Repeat step 1-4 to add more plans for different time.
 - You can set up to 6 different plans for one day.
 - One period can only add one smart plan.

Figure 5-31 Time settings (1)

Figure 5-32 Time settings (2)



Step 5 Click **Save**.



Schedule function is only available on single-channel cameras.

5.8 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 less 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.

5.8.1 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

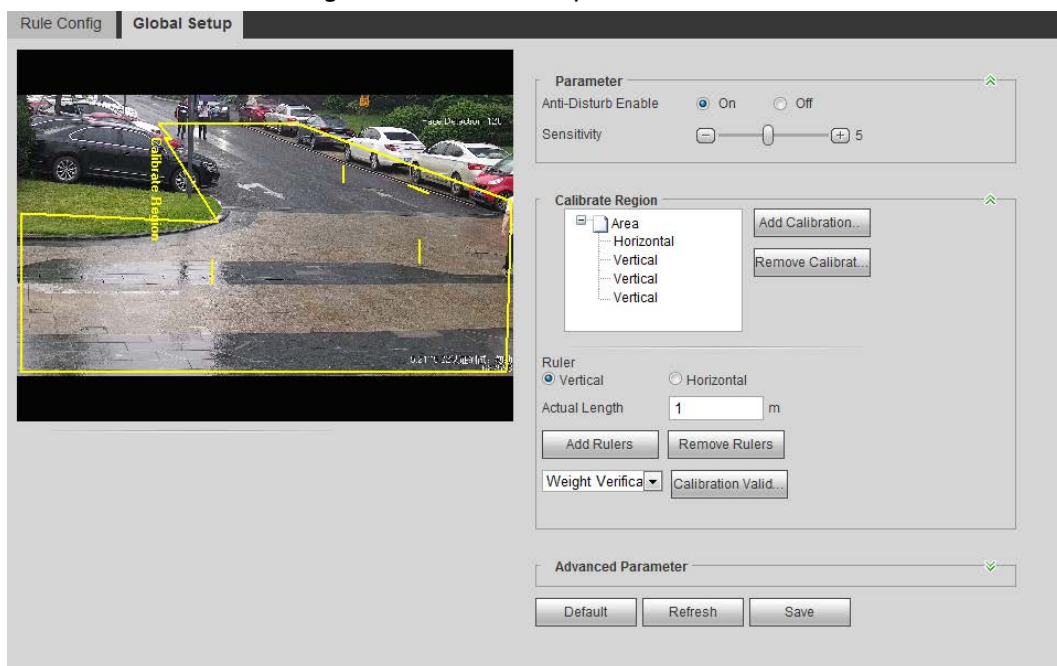
- Calibration Drawing
 - ◇ Calibration area: The calibration area drawn should be on one horizontal plane.
 - ◇ Vertical ruler: The bottom of three vertical rulers should be on the same horizontal plane. Select three reference objects with fixed height in triangular distribution as vertical rulers, such 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 **Setting > Event > IVS > Global Setup**.

Figure 5-33 Global setup of IVS



2. Set parameters.

Table 5-6 Description of global setup (IVS) parameters

Parameter	Description
Anti-Disturb Enable	A reserved function.
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.
Tracking Overlap Rate	Reserved functions.
Valid Tracking Distance	
Valid Tracking Time	

3. Set calibration area and ruler.
 - a. Click **Add Calibration Area** and draw a calibration area in the image.
 - b. Select a calibration type and enter the actual length, and then click **Add Rulers**.
 - c. Draw one horizontal ruler and three vertical rulers in the calibration area.
4. Click **Save**.

Result

1. Select the verification type, and then click **Calibration Valid**.
 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.

5.8.2 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 **Setting > Event > Smart Plan**, and enable **IVS**.
- Select **Setting > Event > IVS > Global Setup** to finish global configuration, and then configure **Fast Moving** rule.

Table 5-7 Description of IVS functions

Rule	Description	Applicable Scene
Tripwire	When the target crosses tripwire from the defined motion direction, the system performs 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, the system performs alarm linkages.	

Rule	Description	Applicable Scene
Abandoned object	When an object is abandoned in the detection area over the set time, the system performs alarm linkages.	Scenes with sparse targets and without obvious and frequent light change. Simple scene in the detection area is recommended. <ul style="list-style-type: none"> ● Missed alarms 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, the system performs alarm linkages.	Scenes with sparse targets and without obvious and frequent light change. Simple scene in the detection area is recommended. <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, the system performs 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.
Parking detection	When the target stays over the configured time, the system performs alarm linkages.	Road monitoring and traffic management.

Rule	Description	Applicable Scene
Crowd gathering	When the crowd gathers or the crowd density is large, the system performs 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, the system performs 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.

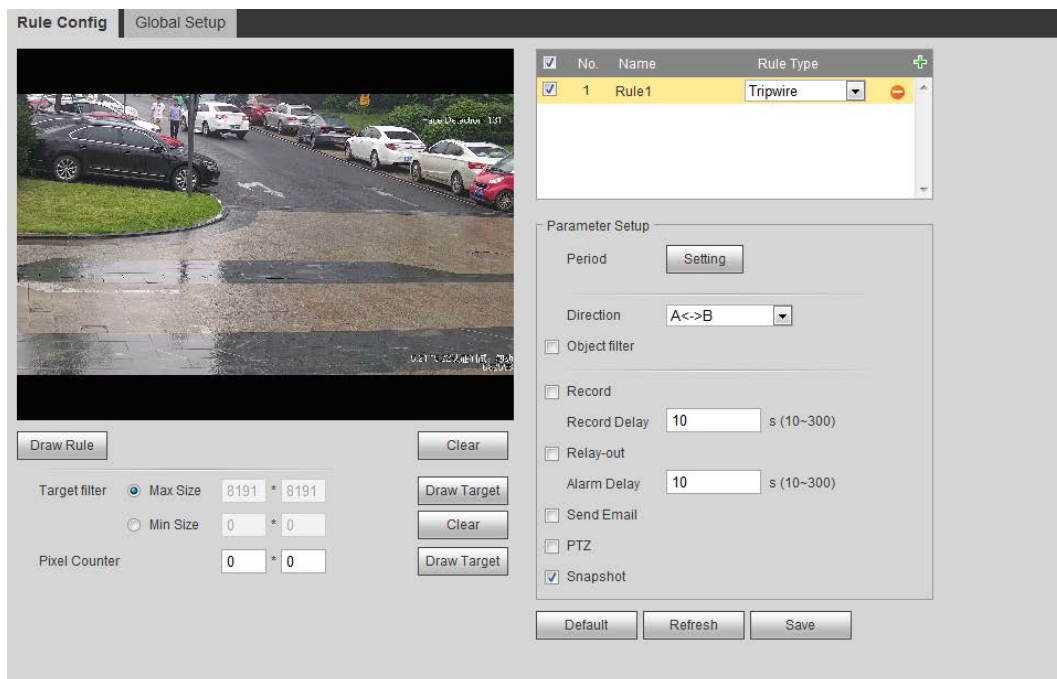


Go to the **Rule Config** interface of the speed dome, and the PTZ lock function is automatically enabled. The locking time is 180 seconds. You can only manually control the PTZ during the locking time. Click **Unlock** at lower left corner of the **Rule Config** interface to manually unlock the PTZ, and click **Lock** again to relock the PTZ.

Step 1 Select **Setting > Event > IVS > Rule Config**.

Step 2 Click **+** on the **Rule Config** interface, double-click the name to modify the rule name, and then select **Tripwire** from the **Rule Type** drop-down list.

Figure 5-34 Tripwire



Step 3 Click **Draw Rule** to draw rule line in the image. Right-click to finish drawing.

For requirements of drawing rules, see Table 5-7. After drawing rules, drag corners of the detection area to adjust the area range.

Table 5-8 Description of IVS analysis


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


Step 4 (Optional) Click **Draw Target** at the right side of **Target Filter**, and then draw the target in the image.

- When the rule of crowd gathering is configured, you do not need to set target filter, but draw the minimum gathering area. Click **Draw Target** 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 **Clear** to delete all drawn detection lines.
- Click **Draw Target** at the right side of **Pixel Counter**, and then press and hold the left mouse button to draw a rectangle, the **Pixel Counter** then displays its pixel.

Step 5 Set rule parameters for IVS.

Table 5-9 Description of IVS parameters

Parameter	Description
Direction	Set the direction of rule detection. <ul style="list-style-type: none"> When setting cross fence detection and tripwire, select A->B, B->A, or A<->B. When setting intrusion, select Enters, Exits, or Enter&Exit.
Action	When setting intrusion action, select Appears or Cross .
Object tracking	Select Object Tracking to enable this function. When alarm is triggered by a moving object, select 1P+3 or 1P+5 as the object tracking display mode in the Live interface. Then the tracking scene follows the moving object until the object is out of the camera range. For details, see "4.2.4 Window Adjustment Bar".  This function is available on some select models.
Track linkage	Select AlarmTrack and set the tracking time. When alarm is

Parameter	Description
Track Time	<p>triggered, the camera automatically tracks the person or object that triggers the alarm. Tracking time is the duration that the camera automatically tracks the object.</p>  <p>Before enabling this function, you need to enable or disable the Alarm Track function under Smart Track as needed.</p> <ul style="list-style-type: none"> • When the Channel is set as 1, disable Alarm Track under Smart Track. • When the Channel is set as 2 or 3, enable Alarm Track under Smart Track.
AI Recognition	<p>Select AI Recognition to enable this function.</p> <ul style="list-style-type: none"> • When you select Person as the alarm target, an alarm will be triggered when the system detects that persons trigger the rule. • When you select Vehicle as the alarm target, alarm will be triggered when the system detects that vehicle trigger 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.
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 6 Set arming periods and alarm linkage action. For details, see "5.1.1 Alarm Linkage".

Step 7 Click **Save**.

To view alarm information on the **Alarm** tab, you need to subscribe relevant alarm event.

For details, see "5.1.2 Subscribing Alarm".

5.9 Setting Crowd Map

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

5.9.1 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.

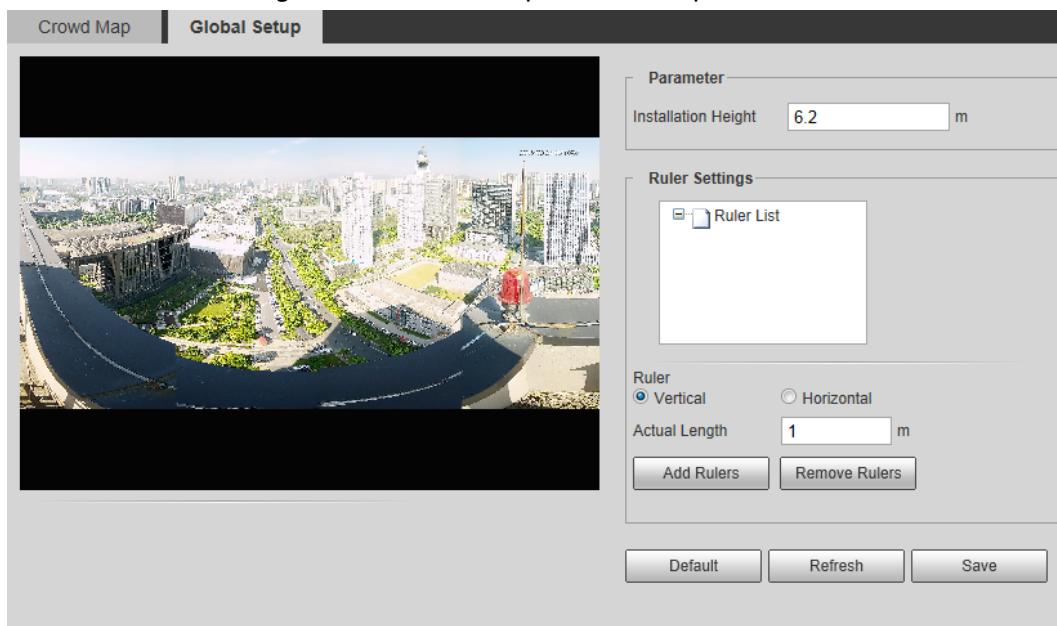
Notes

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

Procedure

1. Select **Setting > Event > Crowd Map > Global Setup**

Figure 5-35 Global setup of crowd map



2. Set calibration area and ruler.
 - a. Click **Add Calibration Area** and draw a calibration area in the image.
 - b. Select a calibration type and enter the actual length, and then click **Add Rulers**.
 - c. Draw one horizontal ruler and three vertical rulers in the calibration area.
3. Click **Save**.

5.9.2 Rule Configuration

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

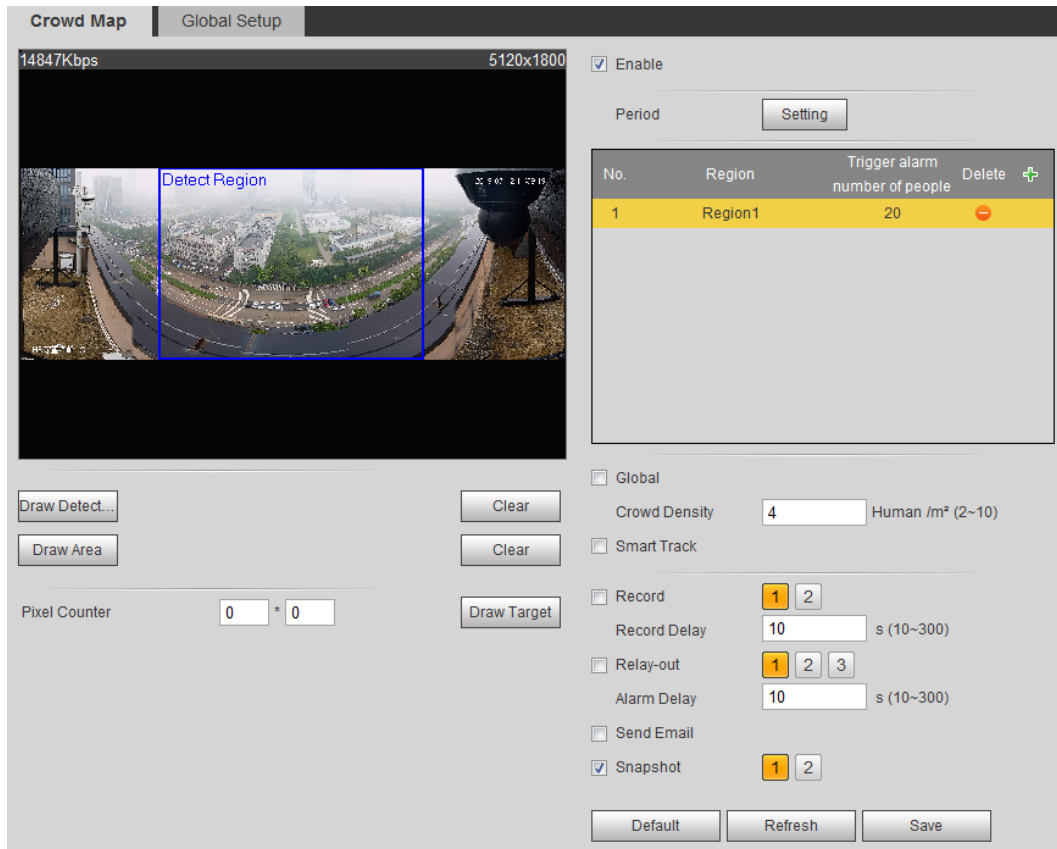
Prerequisites

- Select **Setting > Event > Smart Plan**, and enable **Crowd Map**.
- Select **Setting > Event > Crowd Map > Global Setup** to configure the crowd map.

Procedure

Step 1 Select **Setting > Event > Crowd Map > Crowd Map**.


Figure 5-36 Crowd map



Step 2 Select the **Enable** checkbox, and then the crowd map function is enabled.

Step 3 Click **Draw Detection Area** to draw global area for detecting crowd distribution in the image.

After drawing a global area, you can draw multiple local statistical areas in the global area as needed.

1) Click , and then click **Draw Area** to draw local statistical area in global detection area.

You can draw up to eight local statistical areas.


2) Double-click the area name and the alarm people amount to set the area name of local statistical area and the threshold of the alarm people amount.

When the number of people in the statistical area exceeds the alarm people amount, the system performs alarm linkages. The default alarm people amount is 20.

Step 4 Set parameters.

Table 5-10 Description of crowd map parameters

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

Parameter	Description
Smart track	<p>Select the Smart Track checkbox, and when alarm is triggered by the panoramic camera, the speed dome automatically turns to the position where alarm is triggered. The tracking time is "idle time + five seconds." For the details of idle time configuration, see "5.2.2 Enabling Alarm Track"</p> <p>Linkage rules:</p> <ul style="list-style-type: none"> • Detect global alarm only: Turns to crowd with highest density. • Detect local alarm only: Turns to local area that triggers alarm first. • Detect global alarm + one local alarm: First turns to local area, and then the crowd with highest density when there is no alarm in local area. • Detect global alarm + multiple local alarms: First turns to local area that triggers alarm first, and then the crowd with highest density when there is no alarm in local area. <p> Before enabling this function, you need to configure Smart Track. For details, see "5.2 Setting Smart Track".</p>
Pixel Counter	<p>Click Draw Target next to Pixel Counter, and then press and hold the left mouse button to draw a rectangle, the Pixel Counter then displays its pixel.</p>

Step 5 Set arming periods and alarm linkage actions. For details, see "5.1.1 Alarm Linkage"

Step 6 Click **Save**.

Result

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

Figure 5-37 Crowd map (1)



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

Figure 5-38 Crowd map (2)

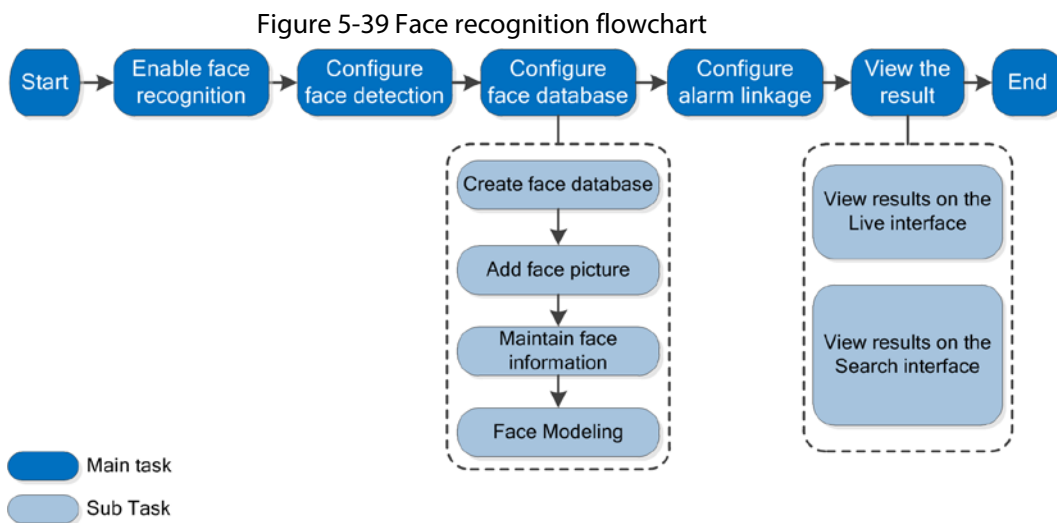


5.10 Setting Face Recognition

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 5-39.



5.10.1 Setting Face Detection

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

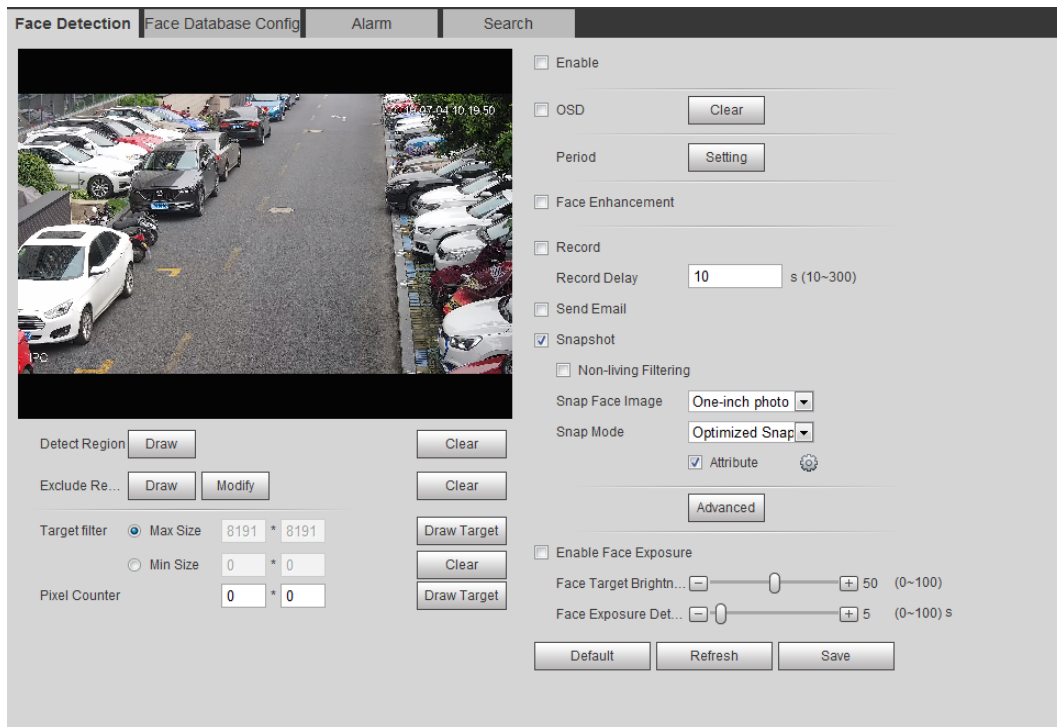
Prerequisites

Select **Setting > Event > Smart Plan**, and then enable **Face Recognition**.

Procedure

Step 1 Select **Setting > Face Recognition > Face Detection**.



Figure 5-40 Face detection



- Step 2** Select the **Enable** checkbox to enable the face detection function.
- Step 3** (Optional) Click **Draw** next to **Detect Region** to draw a face detection area in the image.
- Step 4** (Optional) Click **Draw** next to **Exclude Region** to draw a non-face detection area in the **Detect Region**.
- Step 5** (Optional) Select **Max Size** or **Min Size**, click **Draw Target** at the right side of **Target filter**, and then draw the target in the image.
- Step 6** Set parameters.

Table 5-11 Description of face detection parameters

Parameter	Description
OSD	Select the OSD checkbox, and the number of people with face detected and recognized is displayed on the Live interface. Click Reset to recount.
Face Enhancement	Select the Face Enhancement checkbox to preferably guarantee clear face with low stream.
Non-living Filtering	Filter non-living faces in the image, such as a face picture.

Parameter	Description
Snap Face Image	<p>Set a range for snapping face image, including face picture, one-inch picture, and custom.</p> <p>When selecting Custom, click Setting, configure the parameters on the prompt interface, and then click OK.</p> <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. <p>When the value is 0, it means to cutout the face image only.</p>
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 alarm. It is recommended to use this mode in access control scene. <p> Click Advanced to set the optimized time.</p>
Attribute	<p>Select the Attribute checkbox, and click  to set the display of face attribute during the face detection.</p>
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.
Enable Face Exposure	<p>Select the Enable Face Exposure checkbox. When a face is detected, the camera can enhance brightness of the face to make the face image clear.</p>
Face Target Brightness	<p>Set the face target brightness. It is 50 by default.</p>
Face Exposure Detection Interval	<p>Set the face exposure detection interval to prevent image flickering caused by constant adjustment of face exposure. It is five seconds by default.</p>
Pixel Counter	<p>Click Draw Target next to Pixel Counter, and then press and hold the left mouse button to draw a rectangle, the Pixel Counter then displays its pixel.</p>

Step 7 Set arming periods and alarm linkage actions. For details, see "5.1.1 Alarm Linkage".

Step 8 Click **Save**.

5.10.2 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.

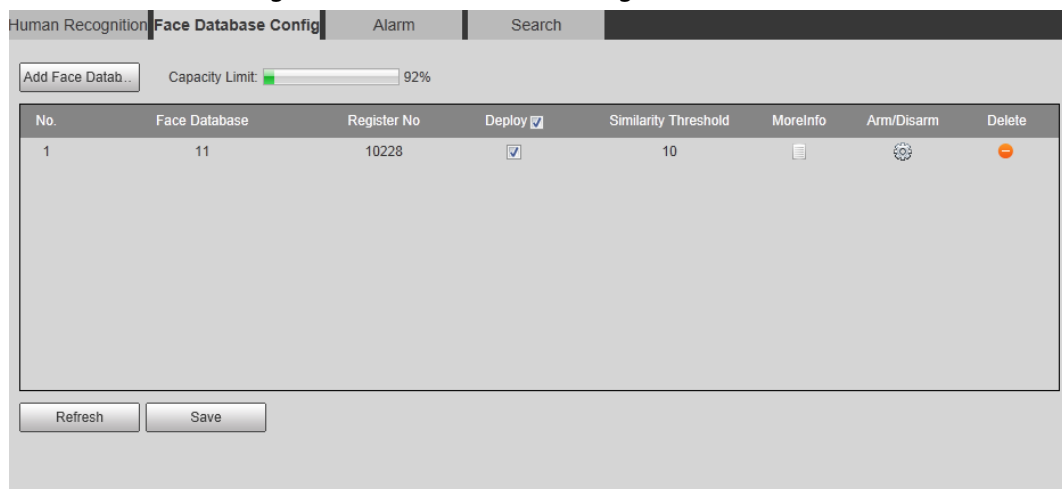
5.10.2.1 Creating Face Database

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

Step 1 Select **Setting > Event > Face Recognition > Face Database Config**.

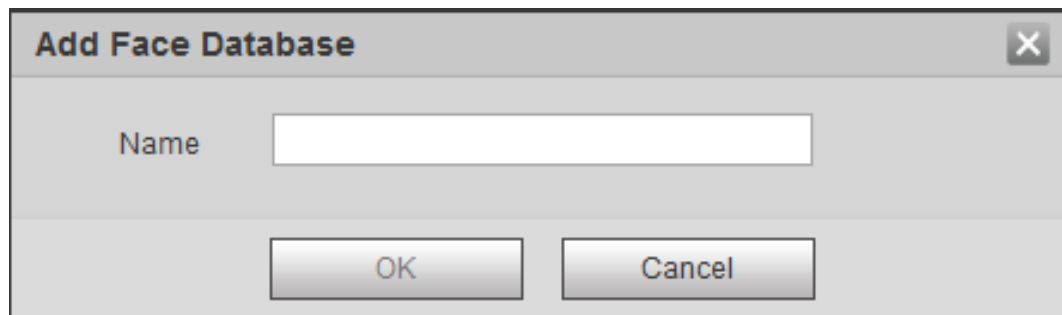
Capacity Limit: Shows the usage of the memory.

Figure 5-41 Face database configuration



Step 2 Click **Add Face Database**.

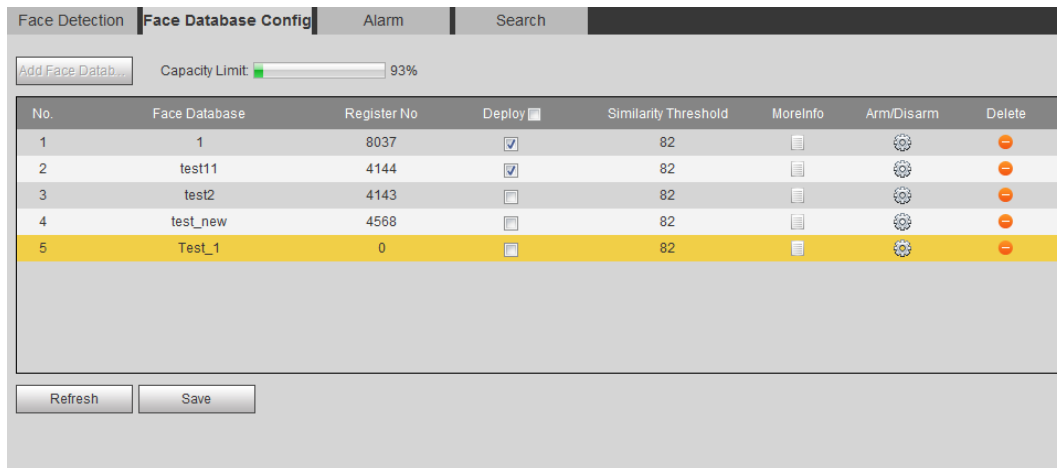
Figure 5-42 Add face database



Step 3 Set the name of the face database.

Step 4 Click **OK**.

Figure 5-43 Face database successfully added



Step 5 Set parameters.

Table 5-12 Description of face database parameters

Parameter	Description
Deploy	Select the Deploy checkbox, and the face database deployment is enabled. The captured face picture is compared to the armed face database.
Similarity Threshold	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.
MoreInfo	Click MoreInfo to manage face database. You can search face images by setting search conditions, register personnel, and modify personnel information.
Arm/Disarm	Set the alarm time period. Alarm event will be triggered only within the defined time. See "5.1.1.1 Setting Period".
Delete	Delete the selected face database.

5.10.2.2 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.

5.10.2.2.1 Single Adding

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

Step 1 Select **Setting** > **Event** > **Face Recognition** > **Face Database Config**.

Step 2 Click next to the face database to be set.

Figure 5-44 Face database configuration

Step 3 Click **Registration**.

Figure 5-45 Registration (1)

Step 4 Click **Upload Picture**, select a face picture to be uploaded, and then click **Open**.



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

Figure 5-46 Registration (2)



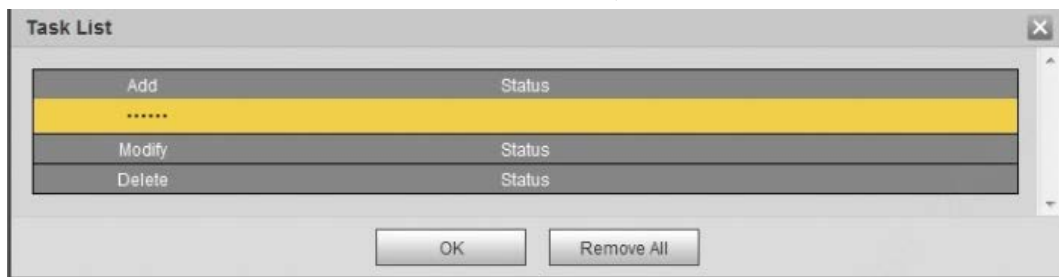
Step 5 Enter the information about face picture according to the actual situation.

Step 6 Click **Add to task list**.

Step 7 Click **Task List1**, and then click **OK**.

The **Task List** interface is displayed. See Figure 5-47. Click **Remove All** to remove all tasks by one click.

Figure 5-47 Task list (manually add)



If adding user fails, the error code is displayed on the interface. For details, see Table 5-13. For face modeling operation, see "5.10.2.4 Face Modeling".

Table 5-13 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.

Parameter	Error	Description
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.
3		Multiple faces in the picture. Change the picture.
4		Fails 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.

5.10.2.2.2 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 5-14.



- 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 5-14 Description of naming rules for batch import parameters

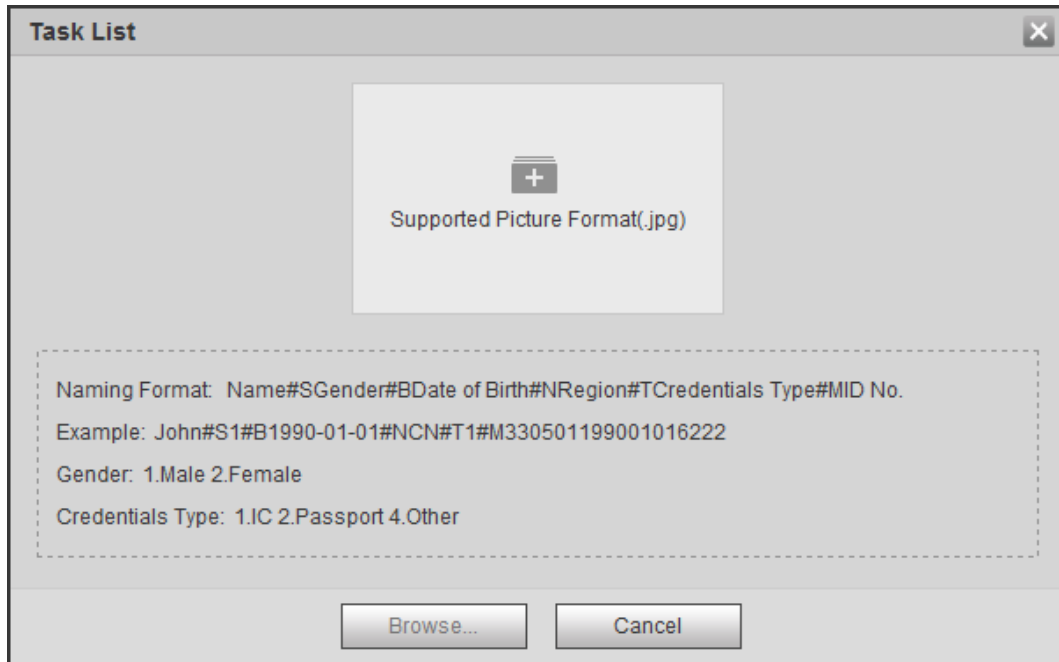
Parameter	Description
Name	Enter a name.
Gender	Enter a figure. "1" is male and "2" is female.
Date of Birth	Enter a figure. Format: yyyy-mm-dd, such as 2017-11-23.
Credentials Type	Enter a figure. "1" is ID card and "2" passport.
ID number	Enter ID No.

Step 1 Select **Setting > Event > Face Recognition > Face Database Config.**

Step 2 Click  next to the face database that you want to set.

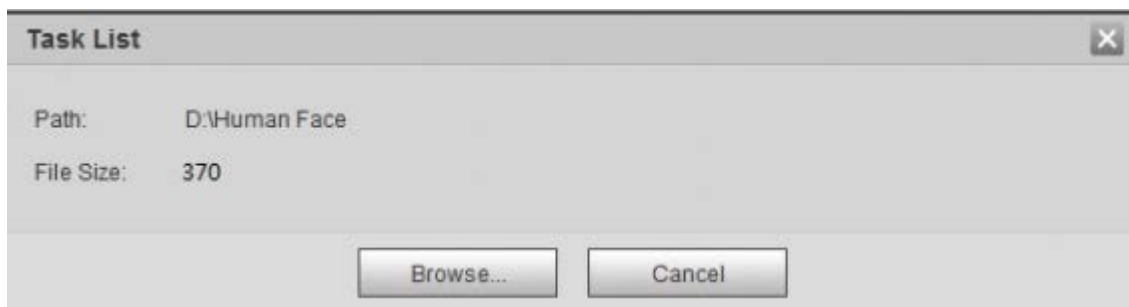
Step 3 Click **Batch Registration.**

Figure 5-48 Batch add



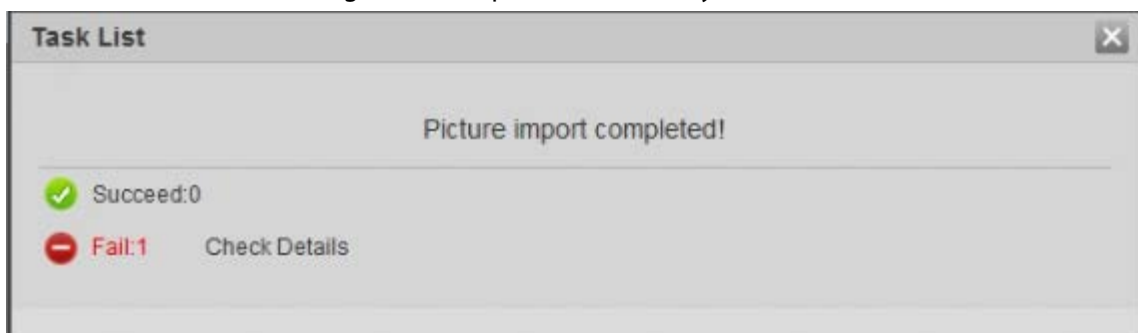
Step 4 Click  to select file path.

Figure 5-49 Batch import



Step 5 Click **Browse**.
The interface shows import process. After finishing the import, the interface shown as Figure 5-50 is displayed.

Figure 5-50 Imported successfully



5.10.2.3 Managing Face Picture

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

5.10.2.3.1 Modifying Face Information





- Step 1** Go to the **Face Database Config** interface, set filtering condition as needed, and click **Search**.
The search result is displayed.
- Step 2** Select the row where the face picture or the personnel information is located, and then click  or .

Figure 5-51 Face information modification

- Step 3** Modify face information according to the actual need. Click **Add to task list**.
- Step 4** Click **Task List1**, and then click **OK**.

5.10.2.3.2 Deleting Face Picture

Go to the **Face Database Config** interface, and delete the created face picture.

- Single delete: Select the row where the face picture or the personnel information is located, and click  or  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 **Add to Deletion List**, **Task List1**, and then click **OK** to delete the selected face picture.
- 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 **Add to Deletion List**, **Task List1**, and then click **OK** to delete all face pictures.

5.10.2.4 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 Select **Setting > Event > Face Recognition > Face Database Config**.

The **Face Database Config** interface is displayed.


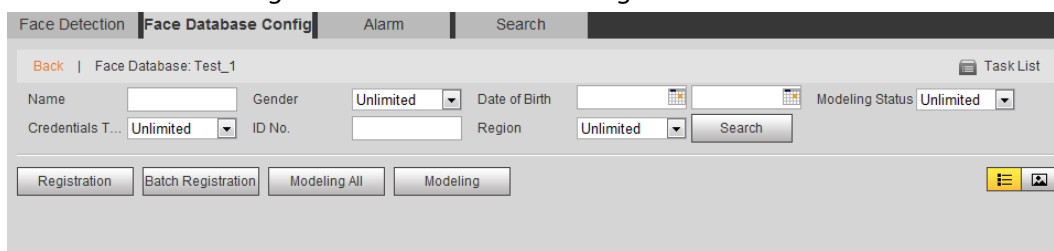
Step 2 Click  next to the face database to be set.

Figure 5-52 Face database configuration



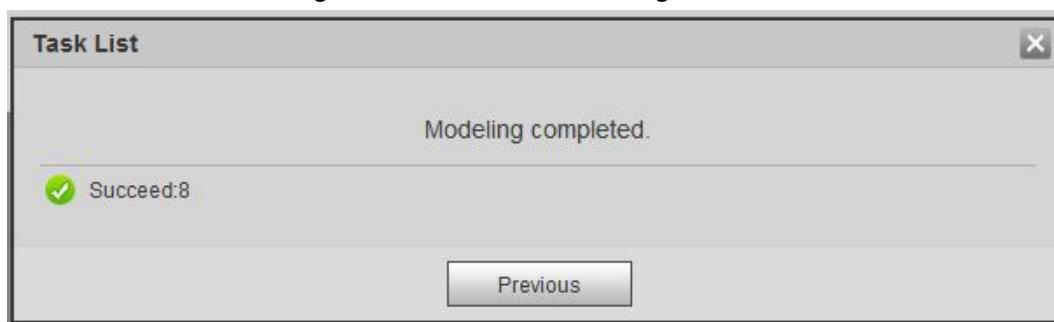
Step 3 Start modeling.

- 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 4 View the modeling result.

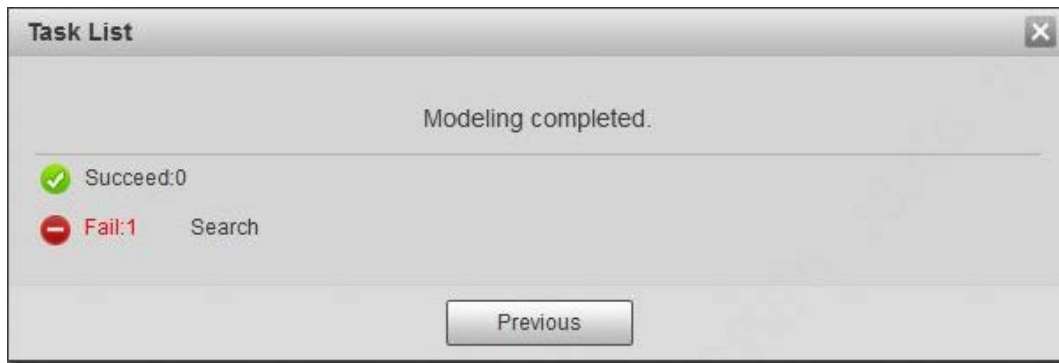
- Successful modeling.

Figure 5-53 Successful modeling



- Failed modeling.

Figure 5-54 Failed modeling



Click **Search**, and the face details are displayed. Click to view the face picture in list format. See Figure 5-55. Click to view the face picture in thumbnail format. See Figure 5-56.

- ◇ When the modeling status is **Valid** in the list or is displayed on the left corner of the thumbnail, it means the modeling succeeded.
- ◇ When the modeling status is **Invalid** in the list or is not displayed on the left corner of the thumbnail, it means the modeling failed. Point to the modeling status in the list or the pictures without to view the details of the failure. Change the pictures according to the details.

Figure 5-55 Modeling status (list)

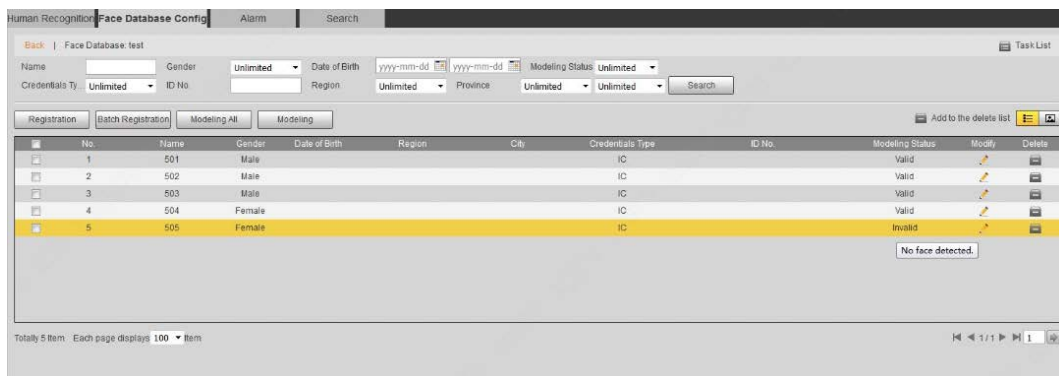
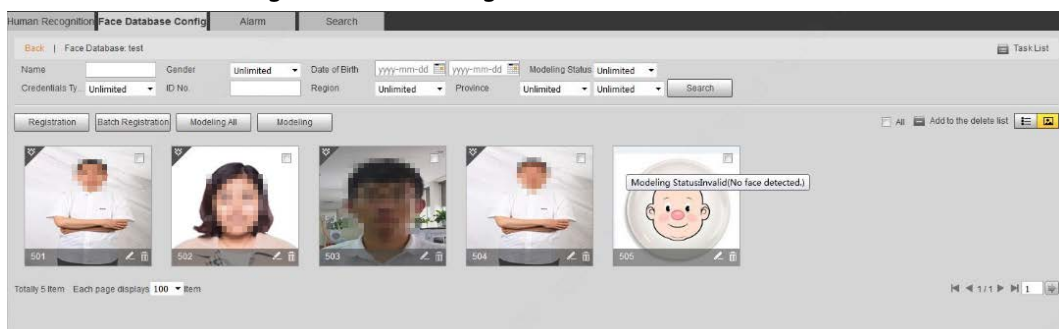


Figure 5-56 Modeling status (thumbnail)

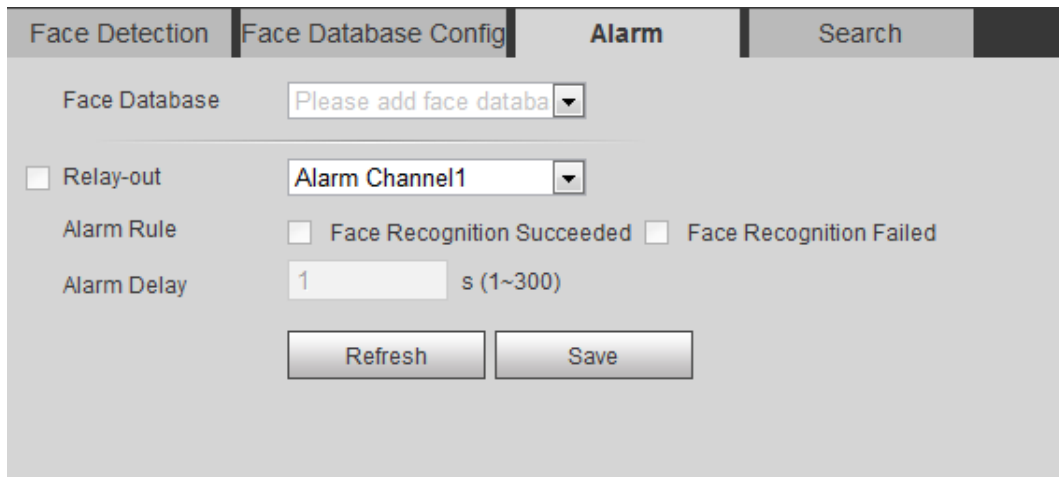


5.10.3 Setting Face Recognition Alarm Linkage

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

Step 1 Select **Setting** > **Event** > **Face Recognition** > **Alarm**.

Figure 5-57 Alarm (face recognition)



Step 2 Select a face database and an alarm rule.

- Face recognition succeeded: When the detected face matches that in the face database, the device links alarm out.
- Face recognition failed: When the detected face fails to match that in the face database, the device links alarm out.

Step 3 Set alarm linkage actions. For details, see "5.1.1 Alarm Linkage"

Step 4 Click **Save**.

5.10.4 Viewing Face Recognition Result

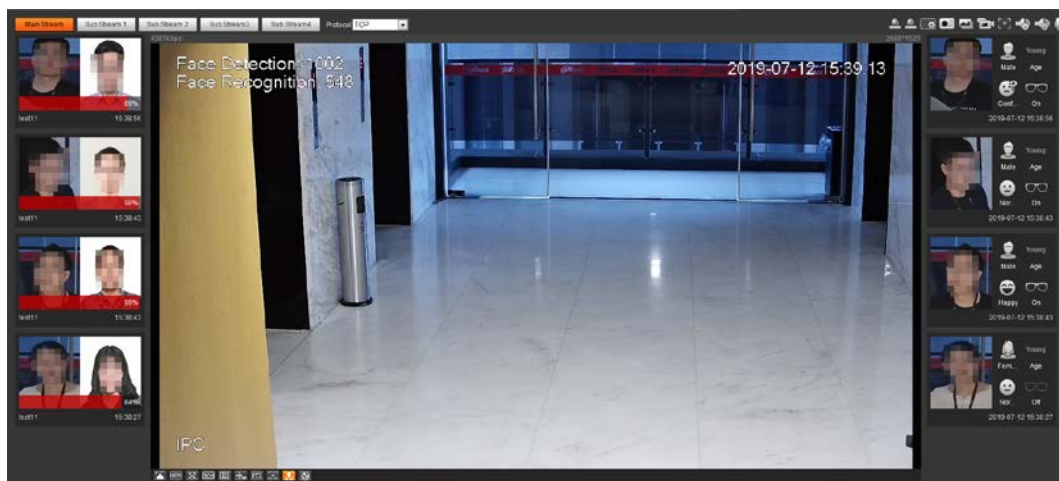
View face recognition result on the **Live** interface or by the search function.

5.10.4.1 Viewing Result in the Live Interface

View face recognition result on the **Live** interface. See Figure 5-58.

- Face recognition result is displayed at the left side and the captured face pictures and attribute information at the right side.
- Click a face picture in the display area, and the information is displayed.

Figure 5-58 Face recognition result



5.10.4.2 Viewing Result by Search Function

View face recognition or face snapshot result. Take face recognition search as an example.

Prerequisites

You have installed a SD card in the camera.

Procedure

Step 1 Select **Setting** > **Event** > **Face Recognition** > **Search**.

Figure 5-59 Face recognition search

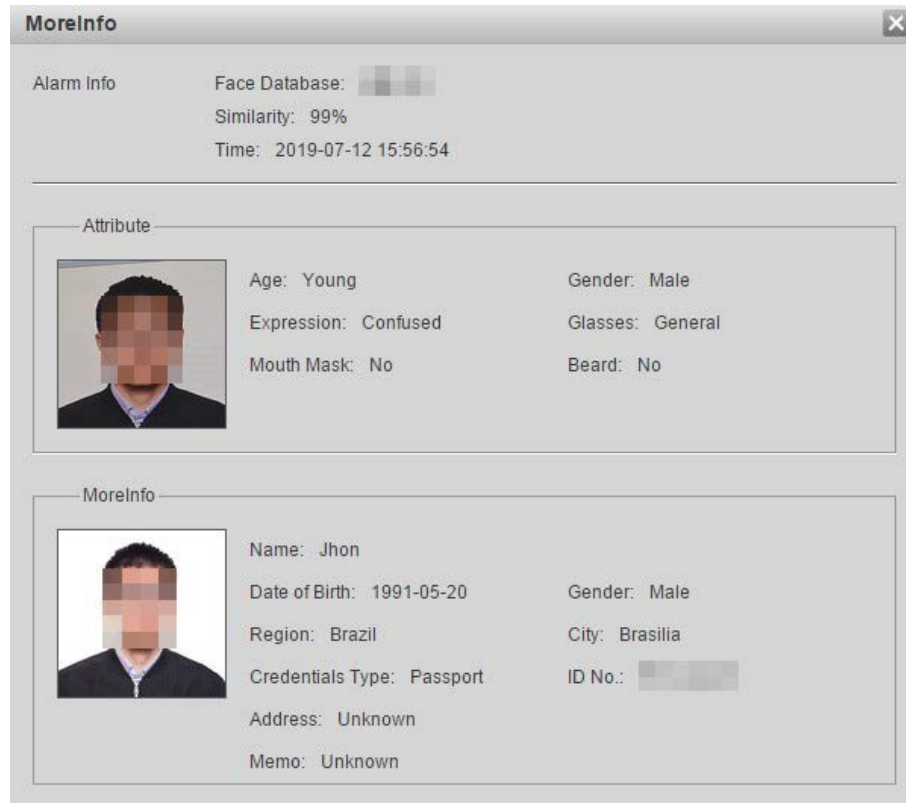
Step 2 Select **Face Recognition** for **Type**, enter the start time and the end time, and then click **Search**.

The result is displayed. See Figure 5-60.

- Click **Advanced Parameters** to set more search conditions.
- Click a search result to view details. See Figure 5-61.

Figure 5-60 Search results (face recognition)

Figure 5-61 MoreInfo (face recognition)



5.11 Setting Face Detection

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

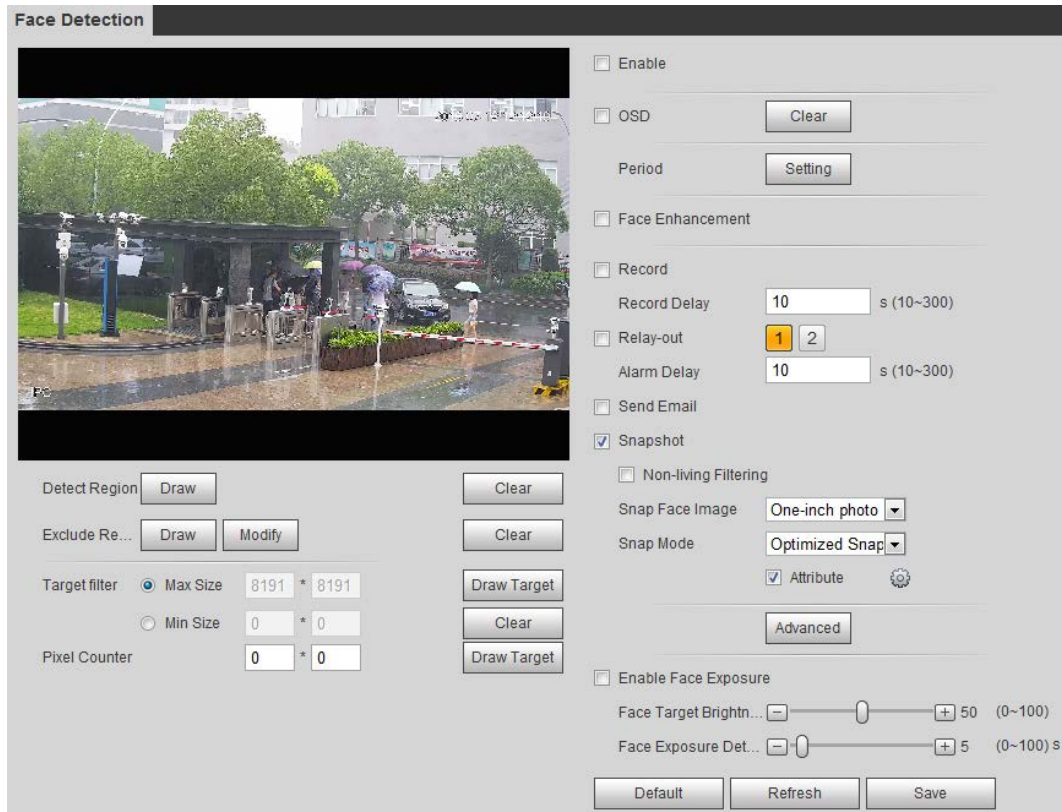
Prerequisites

Select **Setting** > **Event** > **Smart Plan**, and then enable **Face Detection**.

Procedure

Step 1 Select **Setting** > **Event** > **Face Detection**.



Figure 5-62 Face detection



- Step 2** Select the **Enable** checkbox to enable the face detection function.
- Step 3** (Optional) Click **Draw** next to **Detect Region** to draw a face detection area in the image.
- Step 4** (Optional) Click **Draw** next to **Exclude Region**, and then draw an area excluding face detection in the image.
- Step 5** (Optional) Select **Max Size** or **Min Size**, click **Draw Target** at the right side of **Target filter**, and then draw the target in the image.
- Step 6** Set parameters.

Table 5-15 Description of face detection parameters

Parameter	Description
OSD	Select the OSD checkbox, and the number people with face detected and recognized is displayed on the Live interface. Click Clear to recount.
Face Enhancement	Select the Face Enhancement checkbox to preferably guarantee clear face with low stream.
Target Box Overlay	Select the Non-living Filtering checkbox to add a target box to the face in the captured picture to highlight the face. The captured face picture is saved in SD card. Click the Snap Face Image tab to view the captured picture.
Non-living Filtering	Filter non-living faces in the image, such as a face picture.

Parameter	Description
Snap Face Image	<p>Set a range for snapping face image, including face picture, one-inch picture, and custom.</p> <p>When selecting Custom, click Setting, configure the parameters on the prompt interface, and then click OK.</p> <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. <p>When the value is 0, it means to cutout the face image only.</p>
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. <p> Click Advanced to set the optimized time.</p>
Attribute	<p>Select the Attribute checkbox, and click  to set the display of face attribute during the face detection.</p>
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.
Enable Face Exposure	<p>Select the Enable Face Exposure checkbox. When a face is detected, the camera can enhance brightness of the face to make the face image clear.</p>
Face Target Brightness	<p>Set the face target brightness. It is 50 by default.</p>
Face Exposure Detection Interval	<p>Set the face exposure detection interval to prevent image flickering caused by constant adjustment of face exposure. It is five seconds by default.</p>
Pixel Counter	<p>Click Draw Target next to Pixel Counter, and then press and hold the left mouse button to draw a rectangle, the Pixel Counter then displays its pixel.</p>

Step 7 Set arming periods and alarm linkage actions. For details, see "5.1.1 Alarm Linkage".

Step 8 Click **Save**.

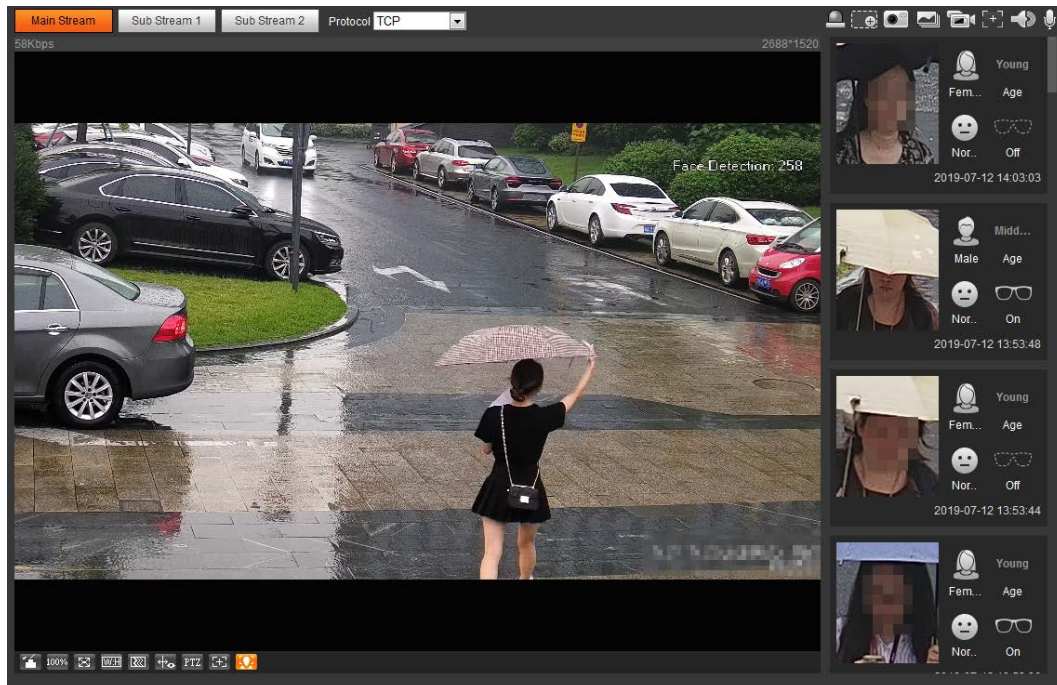
To view alarm information on the **Alarm** tab, subscribe relevant alarm event. For details, see "5.1.2 Subscribing Alarm".

Result

The face detection result is displayed on the live interface.

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

Figure 5-63 Face detection result



5.12 Setting People Counting

People counting (including enter number, leave number and strand number in area), calibration configuration, queuing number, and view the people counting data in report form.

5.12.1 People Counting

The system counts the people entering and leaving the detection area. When the number of counted people exceeds the configured value, the system performs an alarm linkage.

Prerequisites


Select **Setting** > **Event** > **Smart Plan**, and then enable **People Counting**.

Procedure

Step 1 Select **Setting** > **Event** > **People Counting**.

Figure 5-64 People counting

People Counting
Calibration Config
Queuing
Report



2020-05-27 10:38:09 Wed

Draw Rule
Clear

Draw Line
Clear

<input checked="" type="checkbox"/>	No.	Name	Rule Type	+
<input checked="" type="checkbox"/>	1	1	People Counting	-
<input checked="" type="checkbox"/>	2	PC-1	In Area No.	-

Parameter Setup

OSD Clear

Period Setting

Flowrate Alarm

Enter No.

Leave No.

Stranded No.

Record

Record Delay s (10~300)

Relay-out

Alarm Delay s (10~300)

Send Email

Snapshot

Global Setup

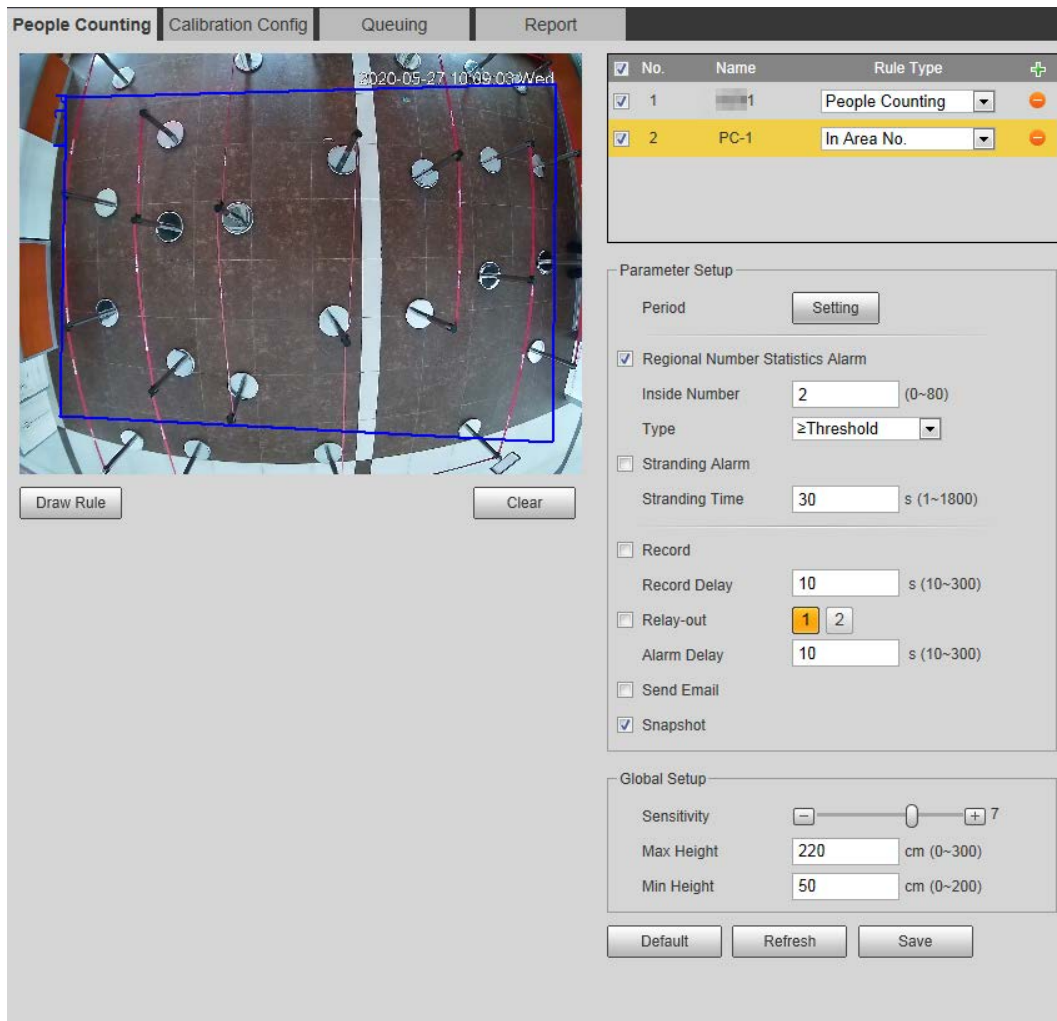
Sensitivity - +

Max Height cm (0~300)

Min Height cm (0~200)

Default
Refresh
Save

Figure 5-65 In area No.



Step 2 Click to add the people counting function.

Step 3 Double-click the name to modify the rule name. Select **People Counting** or **In Area No.**

- **People Counting:** The system counts the people entering and leaving the detection area. When the number of counted number of people who enter, leave, or stay in the area exceeds the configured value, the system performs an alarm linkage.
- **In Area No.:** The system counts the people in the detection area and the duration that people stay in the area. When the number of counted number of people in the detection area or the stay duration exceeds the configured value, the system performs an alarm linkage. This function is available on some select models.

Step 4 Click **Draw Area** to draw a detection area in the image.

- When setting **People Counting**, you need to draw direction lines. When targets enter or leave along the direction line, they will be counted.
- For the models that support multiple counting rules, different detection areas can be overlapped.

Step 5 Set parameters.

Table 5-16 Description of people counting parameters

Parameter	Description
OSD	Select the OSD checkbox or select the Enter No. or Leave No. checkbox under OSD to display the people counting data in the image. Click Clear to clear the count.
Flip	Set the viewing angle of the image as Inclined or Vertical .
Flowrate Alarm	Set Enter No. , Leave No. , and Stranded No. The alarm is triggered when the configured value is reached.
Regional People Number Statistics Alarm	Set the number of people in the people counting region. When the people count reaches the threshold or the stay duration exceeds the configured value, the alarm is triggered.
Inside Number	When you set inside number to be 0, and select the type to be \geq Threshold , the system will not perform the alarm linkage.
Type	
Stranding Alarm	Select the Stranding Alarm checkbox, and then set the stranding time, when the stay duration exceeds the configured value, the alarm will be triggered.
Stranding Time	
Sensitivity	Set the alarm-triggered sensitivity. The higher the sensitivity is, the easier the alarm will be triggered.
Max Height	Set the maximum height of the people in detection area. The unit is cm, and the range is 0–300.
Min Height	Set the minimum height of the people in detection area. The unit is cm, and the range is 0–200.

Step 6 Set arming periods and alarm linkage actions. For details, see "5.1.1 Alarm Linkage".

Step 7 Click **Save**.

To view alarm information on the **Alarm** tab, subscribe relevant alarm event. For details, see "5.1.2 Subscribing Alarm".

Result

You can view the counting results on the **Live** interface.

- For **People Counting** rule, the entry and exit numbers are displayed.
- For **In Area No.** rule, the inside number is displayed.

Figure 5-66 Counting result



5.12.2 Calibration Configuration

After configuring the rule for people counting, set the installation height and angle of the camera through calibration configuration.

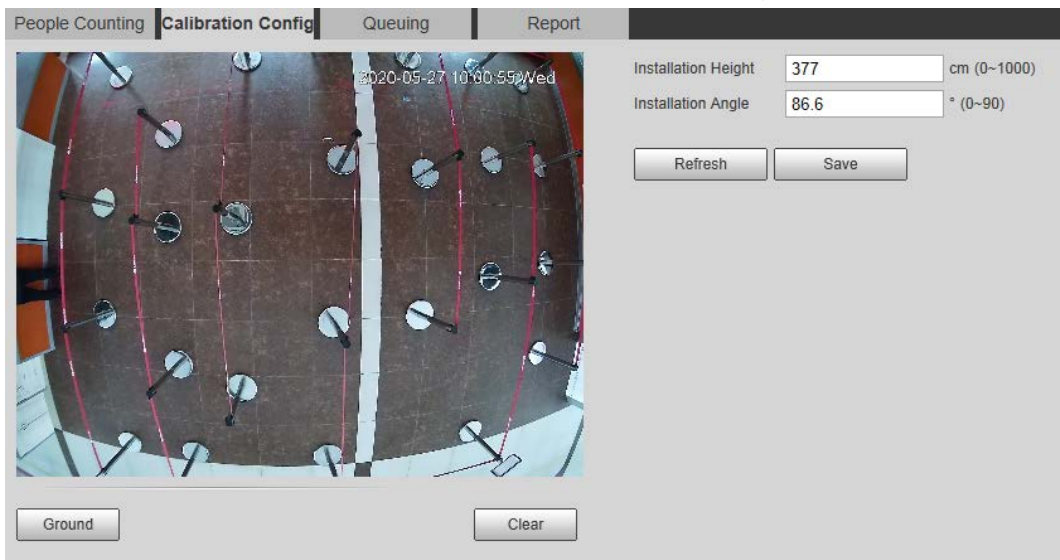
Prerequisites

You have set at least one rule in **Setting > Event > People counting > People Counting**.

Procedure

Step 1 Select **Setting > Event > People Counting > Calibration Config**.

Figure 5-67 Calibration configuration (stereo analysis)



- Step 2 Click **Clear** to clear the default calibration box.
- Step 3 Click **Ground** to draw a rectangular box in the image.
Ground should be on the same plane and as big as possible for calibration.
- Step 4 Click **Save**, and then the camera calculates its height above the ground and the angle it forms with the ground.
If the height and angle are quite different from the actual situation, repeat Step2 and Step3.

5.12.3 Queuing

The system counts the queue people in the detection area. When the queue people number exceeds the configured number or the queue time exceeds the configured time, the alarm is triggered, and the system performs an alarm linkage.

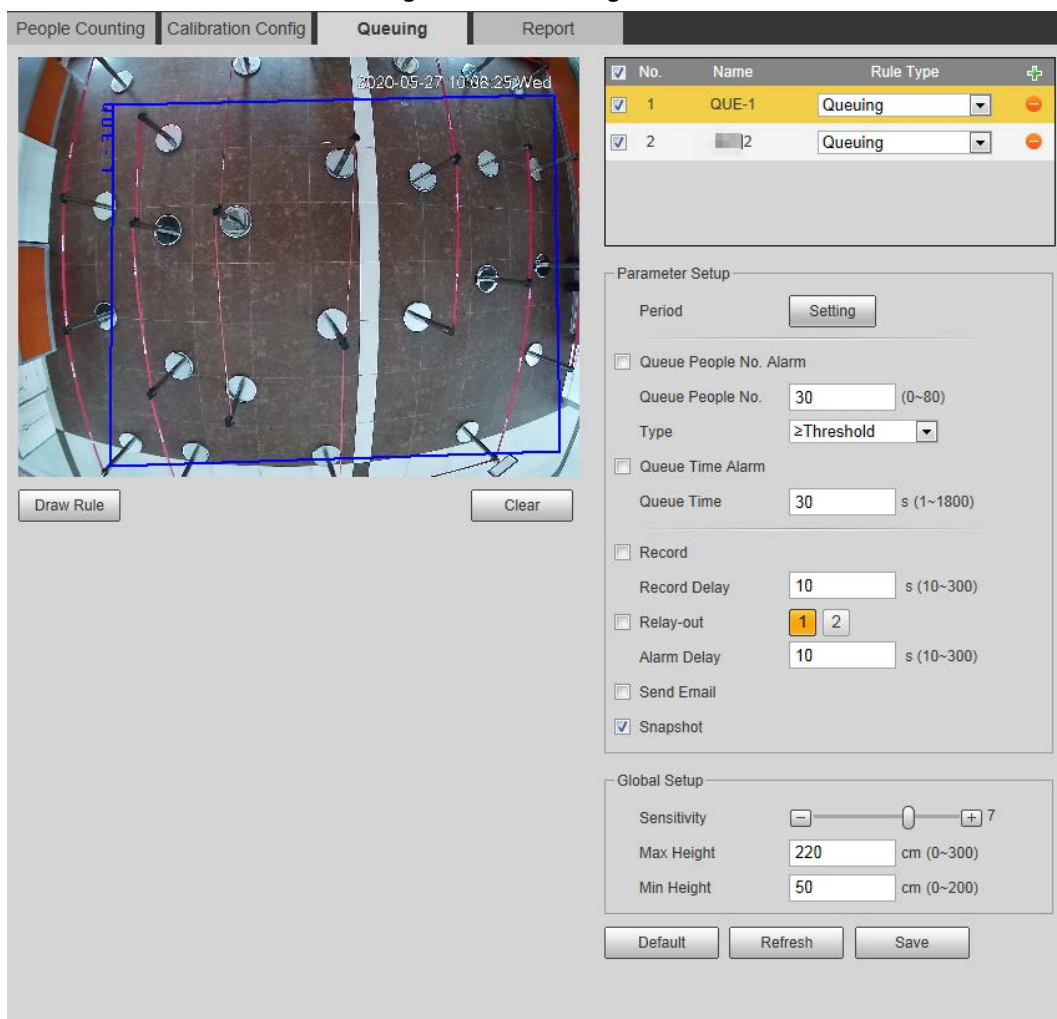
Prerequisites


Select **Setting > Event > Smart Plan**, and then enable **People Counting**.

Procedure

- Step 1 Select **Setting > Event > Queuing**.

Figure 5-68 Queuing



- Step 2 Click  to add the queuing function.



You can add 4 rules at most.

- Step 3** Double-click the name to modify the rule name. Click **Draw Rule** to draw a detection area in the image, and right-click to complete the drawing.
- Step 4** Set parameters.

Table 5-17 Description of people queuing

Parameter	Description
Queue People No. Alarm	Set the queue people number for triggering the alarm and counting type. When the queue people number reaches the configured value, the alarm is triggered.
Queue People No.	
Type	
Queue Time Alarm	Set the queue time. When the queue time reaches the configured value, the alarm is triggered.
Queue Time	
Sensitivity	Set the alarm-triggered sensitivity. The higher the sensitivity is, the easier the alarm will be triggered.
Max Height	Set the maximum height of the people in detection area. The unit is cm, and the range is 0–300.
Min Height	Set the minimum height of the people in detection area. The unit is cm, and the range is 0–200.

Step 5 Set arming periods and alarm linkage actions. For details, see "5.1.1 Alarm Linkage".

Step 6 Click **Save**.

To view alarm information on the **Alarm** tab, subscribe relevant alarm event. For details, see "5.1.2 Subscribing Alarm".

Result

You can view the queuing result on the **Live** interface.

The queuing number and the stranding time of each target are displayed on the interface.

Figure 5-69 Queuing result

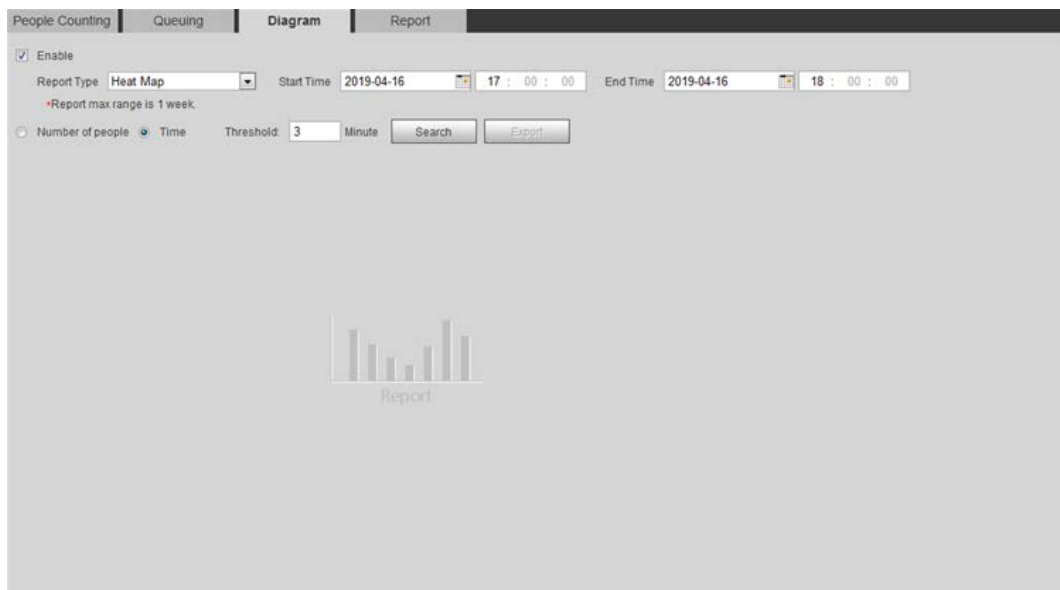


5.12.4 Viewing People Counting Diagram

You can search and export the heat map and tracking map according to the set searching criteria. This function is available on some fisheye cameras.

Step 1 Select **Setting > Event > People Counting > Diagram**.

Figure 5-70 Diagram



Step 2 Select the **Enable** checkbox to enable diagram function. And then you can search the

diagram during the set period.

Step 3 Set the searching criteria.

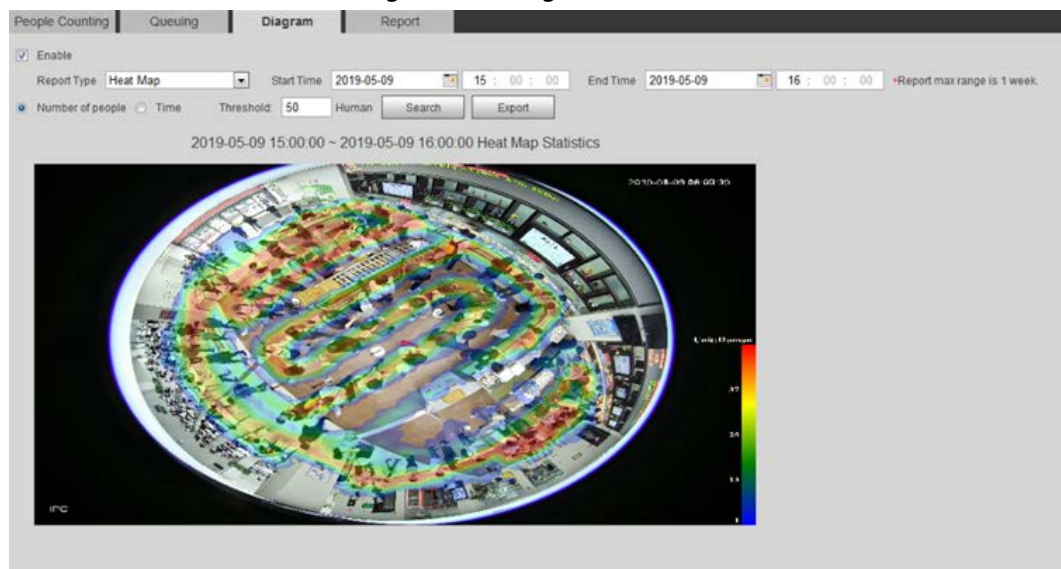
Table 5-18 Description of searching criteria

Parameter	Description
Report Type	Select the report type from the following two types: <ul style="list-style-type: none"> • Heat Map: Density statistics of moving object, the color range is from blue to red, blue means the minimum heat value and red means the maximum heat value. • Track Map: Tendency statistics of moving object.
Start Time	The start time of the report.
End Time	The end time of the report.
Number of People	When selecting heat map as the report type, you can select Number of People , and set the threshold. The system searches the diagram according to the number of people in the area, and shows the heat map.
Threshold	
Time	When selecting heat map as the report type, you can select Time , and set the threshold. The system searches the diagram according to the queuing time in the area and shows the heat map.
Threshold	

Step 4 Click **Search** to complete the diagram.

Click **Export** to export the report.

Figure 5-71 Diagram



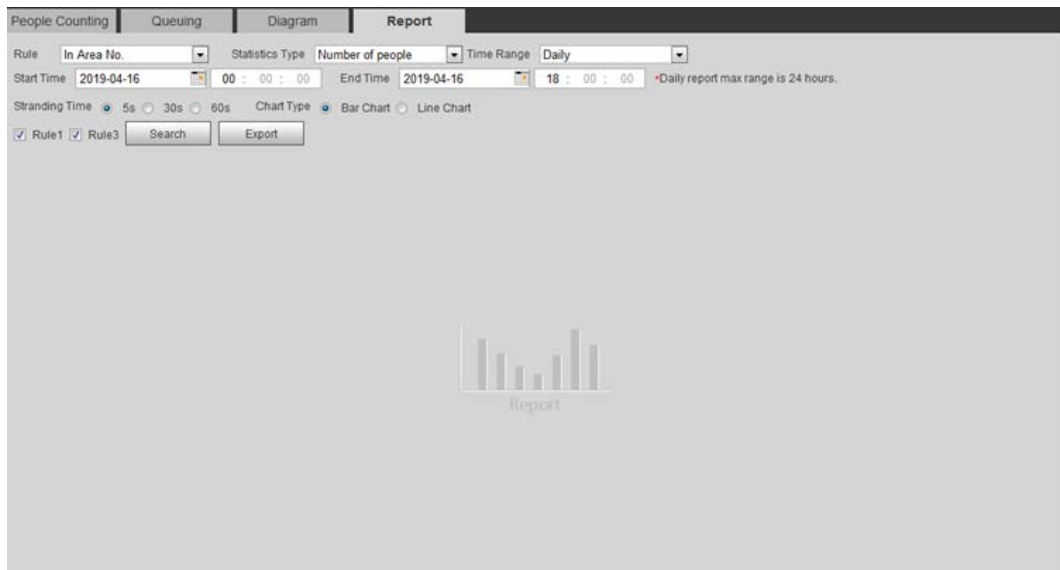
With the ruler on the right, you can read the diagram clearly.

5.12.5 Viewing People Counting Report

Generate people counting data in report form.

Step 1 Select **Setting > Event > People Counting > People Counting Report**.

Figure 5-72 People counting report



Step 2 Set search conditions.

Table 5-19 Description of people counting report parameters

Parameter	Description
Rule	Select the rule of the report from In Area No and Queuing .
Statistics Type	The statistical type of people counting report. <ul style="list-style-type: none"> When you select Number of people, the system generates the report of the number of people that exceeds the configured number of people. When you select Average stranding time, the system generates the report of the average stranding time that exceeds the average stranding time.
Time Range	Select the period for the report. <ul style="list-style-type: none"> When selecting People Counting, you can view daily report, monthly report and annual report. When selecting In Area No., you can view daily report and monthly report.
Begin Time	The begin time and the end time of people counting.
End Time	
People Counting Direction	In and out directions of people counting report. You can select Entrance or Leave . Select Display Data , and the statistical quantity is displayed on the report.
Stranding Time	Count the stay time, select 5 s, 30 s, or 60 s.
Queue Time	Count the queuing time, select 1 minute, 5 minutes, or 10 minutes.
Report Type (Bar Chart/Line Chart)	Includes bar chart and line chart.
Rule 1, Rule 2...	Select the checkbox to search the report of the corresponding rule.

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

Click **Export** to export the report in .bmp or .csv format.

5.13 Setting Heat Map

Make statistics on the cumulative density of object movement and view heat map in report.

5.13.1 Heat Map

Detect the distribution of dynamically moving objects in the target area within a certain period and displays the distribution on a heat map. Color varies from blue to red. The lowest heating value is in blue, and the highest heating value is in red. When mirroring occurs on the camera or the viewing angle changes, original data on the heat map will be cleared.

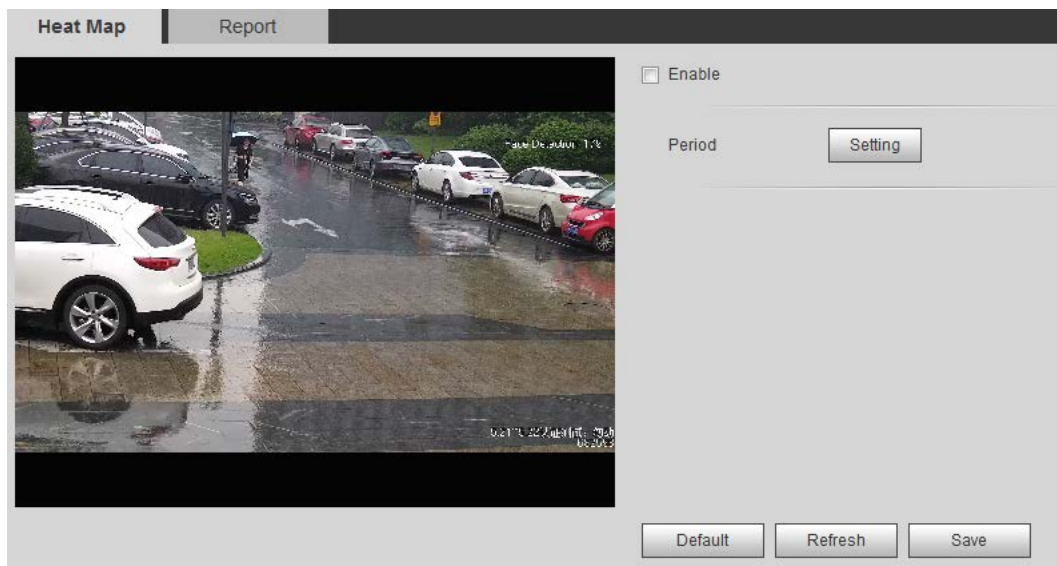
Prerequisites

Select **Setting > Setting > Event > Smart Plan**, and then enable **Heat Map**.

Procedure

Step 1 Select **Setting > Event > Heat Map > Heat Map**.

Figure 5-73 Heat map



Step 2 Select the **Enable** checkbox to enable the heat map function.

Step 3 Set the arming period. For details, see "5.1.1.1 Setting Period".

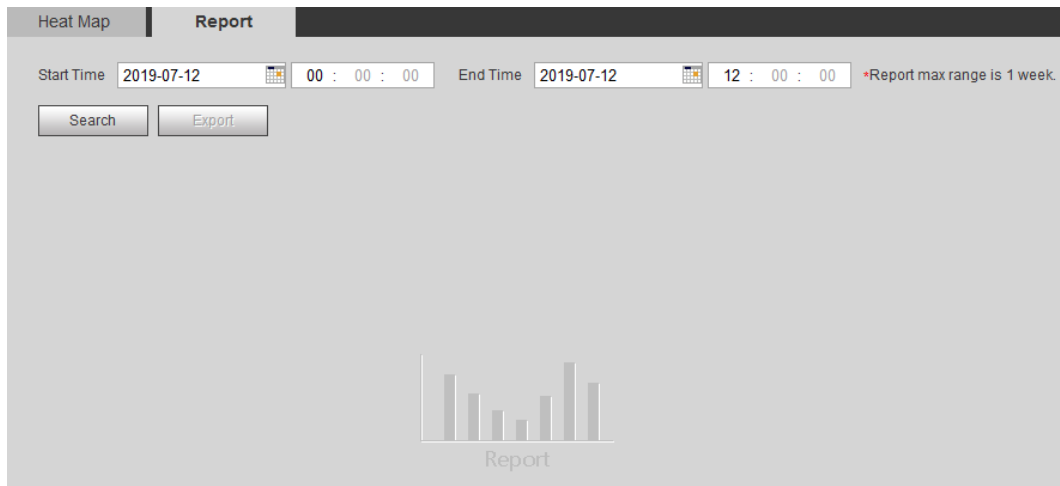
Step 4 Click **Save**.

5.13.2 Viewing Heat Map Report

The system can export heat map data as a report.

Step 1 Select **Setting > Event > Heat Map > Report**.

Figure 5-74 Heat map report



- Step 2** Set the start time and end time.
Only some devices support heat map sequence numbers.
- Step 3** Click **Search** to complete the report.
Click **Export** to export the statistical report.

5.14 Setting Vehicle Density

Configure the rules for traffic congestion and parking upper limit, and view the counting data on the **Live** interface.

Prerequisites

Select **Setting** > **Event** > **Smart Plan**, and then enable **Vehicle Density**.

Procedure

- Step 1** Select **Setting** > **Event** > **Vehicle Density**.

Figure 5-75 Vehicle density (traffic congestion)

The screenshot shows the 'Vehicle Density' configuration window. On the left is a video feed of a city street with a red bounding box around a vehicle. Below the video are 'Draw Area', 'Clear', and 'Pixel Counter' (0 * 0) with a 'Draw Target' button. On the right is a table of rules:

<input checked="" type="checkbox"/>	No.	Region	Scene	Delete
<input checked="" type="checkbox"/>	1	VD-1	Traffic Cong	
<input checked="" type="checkbox"/>	2	VD-2	Parking Upp	

Below the table is the 'Parameter Setup' panel with the following settings:

- Period: Setup
- Repeat Alarm Time: 0 s (0~300)
- Vehicle Congestio...
- Threshold: 50 vehicles (10~1000)
- Continuous Cong...: 10 Min. (1~100)
- Record
- Record Delay: 10 s (10~300)
- Relay-out: 1 2
- Alarm Delay: 10 s (10~300)
- Send Email
- Snapshot

Buttons at the bottom: Default, Refresh, Save.

Figure 5-76 Vehicle density (parking upper limit)

The screenshot shows the 'Vehicle Density' configuration window. The video feed and 'Draw Area' controls are the same as in Figure 5-75. The table of rules is:

<input checked="" type="checkbox"/>	No.	Region	Scene	Delete
<input checked="" type="checkbox"/>	1	VD-1	Traffic Cong	
<input checked="" type="checkbox"/>	2	VD-2	Parking Upp	

The 'Parameter Setup' panel has the following settings:

- Period: Setup
- Repeat Alarm Time: 0 s (0~300)
- Upper Limit Vehicl...
- Threshold: 20 vehicles (10~1000)
- Record
- Record Delay: 10 s (10~300)
- Relay-out: 1 2
- Alarm Delay: 10 s (10~300)
- Send Email
- Snapshot

Buttons at the bottom: Default, Refresh, Save.

Step 2 Click to add the vehicle density function.


Step 3 Double-click the name to modify the rule name. Select **Traffic Congestion** or **Parking Upper Limit**.

- **Traffic Congestion:** The system counts the vehicles in the detection area. When the counted vehicle number and the continuous congestion time exceed the configured values, an alarm is triggered and the system performs an alarm linkage.
- **Parking Upper Limit:** The system counts the vehicles in the detection area. When the counted vehicle number exceeds the configured value, an alarm triggered and the system performs an alarm linkage.

Step 4 Click **Draw Area** to draw a detection area in the image.

Step 5 Set parameters.

Table 5-20 Description of people counting parameters

Parameter	Description
Repeat Alarm Time	After the alarm is triggered, if the status lasts for the configured time in Repeat Alarm Time , the alarm will be triggered again.  0 indicates that the function is disabled.
Vehicle Congestion Alarm	Select the checkbox, and set the Threshold and Continuous Congestion Time . When the counted vehicle and the continuous congestion time exceed the configured values, an alarm is triggered.
Upper Limit Vehicle Quantity Alarm	Select the checkbox, and set the Threshold . When the counted vehicle exceeds the configured values, an alarm is triggered.
Pixel Counter	Click Draw Target next to Pixel Counter , and then press and hold the left mouse button to draw a rectangle, the Pixel Counter then displays its pixel.

Step 6 Set arming periods and alarm linkage actions. For details, see "5.1.1 Alarm Linkage".

Step 7 Click **Save**.

To view alarm information on the **Alarm** tab, subscribe relevant alarm event. For details, see "5.1.2 Subscribing Alarm".

Result

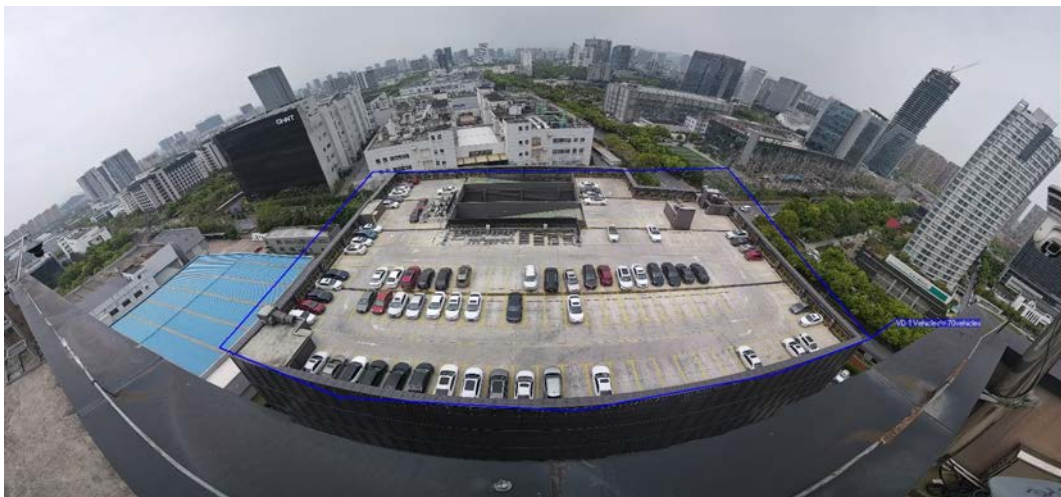
You can view the counting result on the **Live** interface.

- For **Traffic Congestion** rule, the entry and exit numbers are displayed.
- For **Parking Upper Limit** rule, the inside number is displayed.

Figure 5-77 Traffic congestion



Figure 5-78 Parking upper limit



5.15 Setting Stereo Analysis

Stereo analysis includes rule configuration and calibration configuration.

5.15.1 Setting Rules for Stereo Analysis


The rules for stereo analysis include **Activation Analysis**, **Back Detection**, **Fall Detection**, **Walking Detection**, **Blackboard Writing Detection**, **Violence Detection**, **People No. Error**, **Stand Detection**, **Running Detection**, **People Approaching Detection**, and **Strand Detection**.

Prerequisites

Select **Setting** > **Event** > **Smart Plan**, and then enable **Stereo Analysis**

For the functions and applications of the rules, see Table 5-21.

Table 5-21 Description of stereo analysis function

Rule	Function	Applicable Scene
Activation Analysis	Working with a recording & broadcasting server, the camera monitors the target's positions in the front of the classroom and analyzes the data, and then generates a report.	Classrooms
Back Detection	When the camera monitors the front of the classroom works with a recording & broadcasting server, and detects a target with back to the camera, an alarm will be triggered.	Classrooms
Fall Detection	When walking or standing people in the detection area suddenly fall down on the ground, the alarm will be triggered.	Park and hall
Walking Detection	When the camera that monitors the front of the classroom works with a recording & broadcasting server, and detects a working target, an alarm will be triggered.	Classrooms
Blackboard Writing Detection	<p>When the camera that monitors the front of the classroom works with a recording & broadcasting server, and detect blackboard writing actions, an alarm will be triggered.</p>  <p>When configuring the rule, click Draw Close-up Area to draw the blackboard as the close-up area, and then the image of sub stream 3 switches to close-up image from the global image.</p>	Classrooms
Violence Detection	When people walking or standing inside or outside the self-service hall or ATM protection cabin have violent movement (such as smashing ATM machine) or fighting, an alarm will be triggered.	Bank halls and ATM protection cabins
People No. Error (vary from devices.)	The camera can recognize the real-time number of people in the detection area. When the number of people exceeds the configured value, an alarm will be triggered.	Scenic spots and banks

Rule	Function	Applicable Scene
	When a recording & broadcasting server is used, the camera that monitors the front of a classroom needs to be configured this function. With this function, the teacher's actions can be traced and enlarged. When the number of people in the image is not 1, the global image is displayed.	Classrooms
Stand Detection	When a recording & broadcasting server is used, the camera that monitors the area where the students stay needs to be configured with this function. When only 1 standing person in the image, an alarm will be triggered, and enlarge the person; when the number of people in the image is not 1, or the stand time is longer than the defined time, the global image is displayed.	Classrooms
Running Detection	When the camera detects a running person, an alarm will be triggered.	Classrooms
People Approaching Detection	When the distance between two walking/standing people reaches the configured value, an alarm will be triggered.	Banks and educational institutions
Strand Detection	When people in the detection area stay longer than the configured stranding time, an alarm will be triggered.	Banks and parks

This section takes Fall Detection as an example to introduce the configuration of stereo analysis rule.

Procedure

Step 1 Select **Setting > Event > Stereo Analysis > Stereo Analysis**.


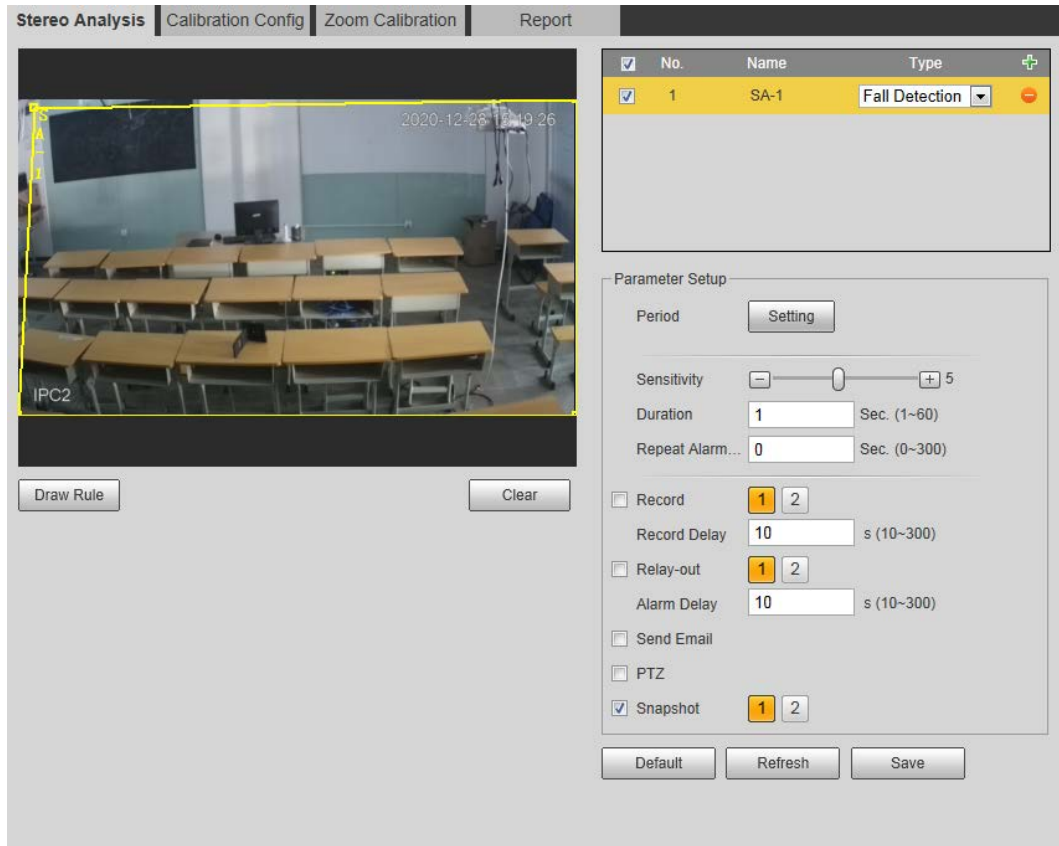
Step 2 Click , double-click the name to modify the rule name, and then select **Fall Detection** as **Rule Type**.

Figure 5-79 Fall detection





- Step 3** (Optional) Click **Clear** to delete the default rule box, and then click **Draw Rule** to draw a detection area in the image.
- When configuring **People No. Error** for a recording & broadcasting device, draw the front of a classroom as the detection area.
 - When configuring **Stand Detection** for a recording & broadcasting device, draw the area where the students stay as the detection area.
 - When configuring **Activation Analysis**, draw the front of a classroom as the detection area.
 - When configuring **Back Detection**, draw the front of a classroom as the detection area.
 - When configuring **Blackboard Writing Detection**, draw the blackboard as the detection area, and make sure that the detection area is larger than the blackboard. Click **Draw Close-up Area** to draw the blackboard as the close-up area.
 - For other devices without special requirements, use the default box of the system (draw the full screen as the detection area).

Step 4 Set parameters.
Parameters for recording device and common device are different. The actual interface shall prevail.

Table 5-22 Description of stereo analysis parameters

Parameter	Description
Sensitivity	Set the alarm-triggered sensitivity. The higher the sensitivity is, the easier the alarm will be triggered.
Alarm People Amount	When configuring People No. Error , set the alarm people amount

Parameter	Description
Alarm Type	<p>and alarm type. Alarm type includes Greater than, Equal to, Less than, and Unequal to.</p> <p>When the real-time number of people in the detection area is greater than, equal to, less than, or unequal to Alarm People Amount, the alarm is triggered.</p>
Duration	<ul style="list-style-type: none"> • For People Approaching Detection, when the time for people approaching reaches the configured value, the alarm is triggered. • For Fall Detection, when the time of people falling down on the ground reaches the configured value, the alarm is triggered. • For People No. Error, when the number of people in the area reaches the configured value of alarm people amount and alarm type, and the time reaches the configured value, the alarm is triggered.
Close-up Mode	<ul style="list-style-type: none"> • For people No. error function for a recording device, select Tracking Mode as Close-up Mode. Then the camera traces the teacher's walking trajectory. You can view the tracking effect through sub stream 1 of the live interface. When the number of people on the image is not 1, the full screen is displayed. • When setting the stand detection function for a recording device, select Fixed Mode as Close-up Mode. Then sub stream 1 enlarges and displays the image of standing people. When the number of standing people is not 1, the full screen is displayed. <p> Before viewing the tracking or enlargement effect through sub stream 1, ensure that sub stream 1 is enabled and the resolution of the main stream and sub stream is 1080p. For configuration details of the main and sub streams, see "4.5.2.1 Video".</p>
Repeat Alarm Time	<p>After the alarm is triggered, if the status lasts for the configured time in Repeat Alarm Time, the alarm will be triggered again.</p> <p> 0 indicates that the function is disabled.</p>
Strand Time Threshold	<p>When configuring Strand Detection, you need to set the strand time threshold. When people in the area stay longer than the configured strand time threshold, the alarm is triggered.</p>

Step 5 Set arming periods and alarm linkage actions. For details, see "5.1.1 Alarm Linkage".

Step 6 Click **Save**.

- Select **Setting > Event > Stereo Analysis > Calibration Config** to finish calibration configuration for other devices, and then the detection rule becomes valid. For details, see "5.15.2 Calibration Configuration".
- To view alarm information on the **Alarm** tab, you should subscribe relevant alarm

event. For details, see "5.1.2 Subscribing Alarm".

5.15.2 Calibration Configuration

After configuring the rule for stereo analysis, set the installation height and angle of the camera through calibration configuration. There are two calibration modes: Calibration mode 1: Directly enter the installation height and angle according to the actual conditions; calibration mode 2: Draw an area in the image to automatically calculate the installation height and the angle. This section takes calibration mode 2 as an example.

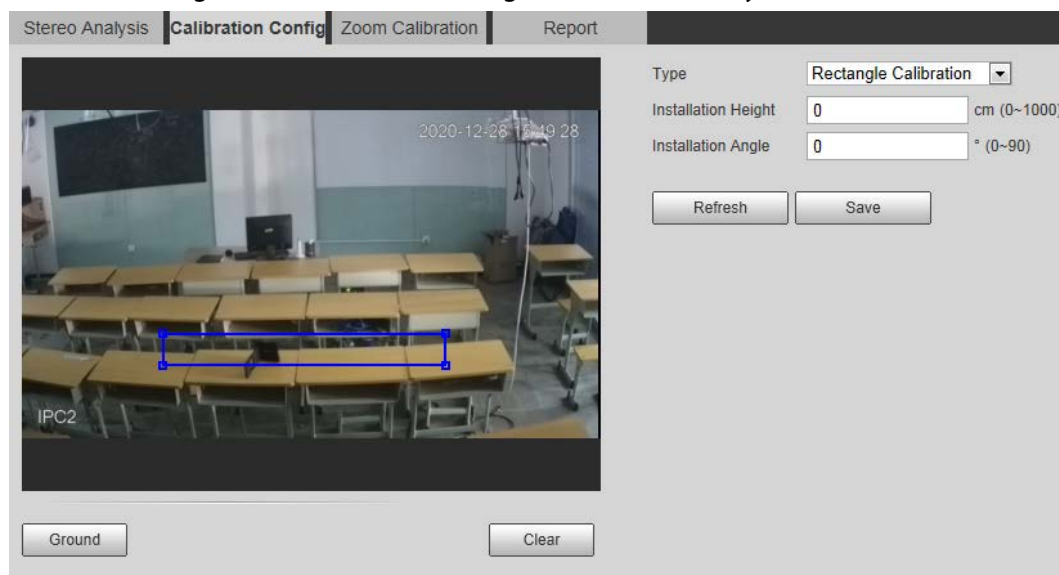
Prerequisites

You have set at least one rule in **Setting > Event > Stereo Analysis > Stereo Analysis**.

Procedure

Step 1 Select **Setting > Event > Stereo Analysis > Calibration Config**.

Figure 5-80 Calibration configuration (stereo analysis)



Step 2 Click **Clear** to clear the default calibration box.

Step 3 Click **Ground** to draw a rectangular box in the image.

Ground should be on the same plane and as big as possible for calibration.

Step 4 Click **Save**, and then the camera calculates its height above the ground and the angle it forms with the ground.

If the height and angle are quite different from the actual situation, repeat Step2–Step4.

5.15.3 Zoom Calibration

When configuring People No. Error and Stand Detection rule, you need to configure the enlarging zoom in the image of sub stream 1. When the number of people in the image is not 1, the global image (sub stream 1) is displayed.

Prerequisites

You have set at least one rule in **Setting > Event > Stereo Analysis > Stereo Analysis**.



Zoom configuration is only available on recording & broadcasting devices.

Procedure

Step 1 Select **Setting > Event > Stereo Analysis > Zoom Configuration**.

Step 2 Configure the zoom.

- Method 1: Click **Calibration Area**, and then draw a rectangular box in the image, which is size of the enlarged image of sub stream 1.
- Method 2: Set the zoom value. For example, if you want the target to be 1/5 of the image, set the zoom value to 5.



- When calibrating the zoom for Stand Detection, make sure that there is 1 person in the image at least.
- When calibrating the zoom for People No. Error, make the calibration box in the center of the image, and the zoom value larger than 3. Some models only support calibration by drawing calibration area.

Figure 5-81 Calibration configuration (stereo analysis)



Step 3 Click **Save**.

5.15.4 Viewing Report

Working with a recording & broadcasting server, the camera monitors the target's positions in the front of the classroom and analyzes the data, and then generates a report.

Prerequisites

You have set at least one rule in **Setting > Event > Stereo Analysis > Stereo Analysis**.

Procedure

Step 1 Select **Setting > Event > Stereo Analysis > Report**.

Step 2 Select the start time and end time.

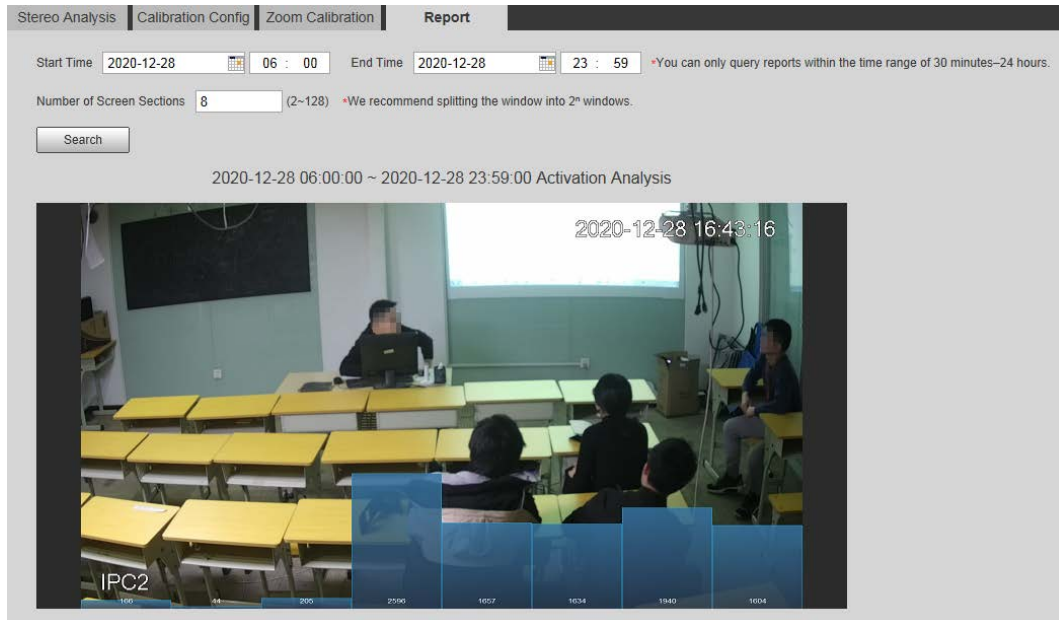
You can search for reports within the time range of 30 minutes–24 hours.

Step 3 Set the number of screen sections.

We recommend splitting the window into 2ⁿ windows.

Step 4 Click **Search**.

Figure 5-82 Report



5.16 Setting ANPR

Extract information of motor vehicles and display related attributes on the live interface.

5.16.1 Scene Configuration

Configure non-motor vehicle detection.

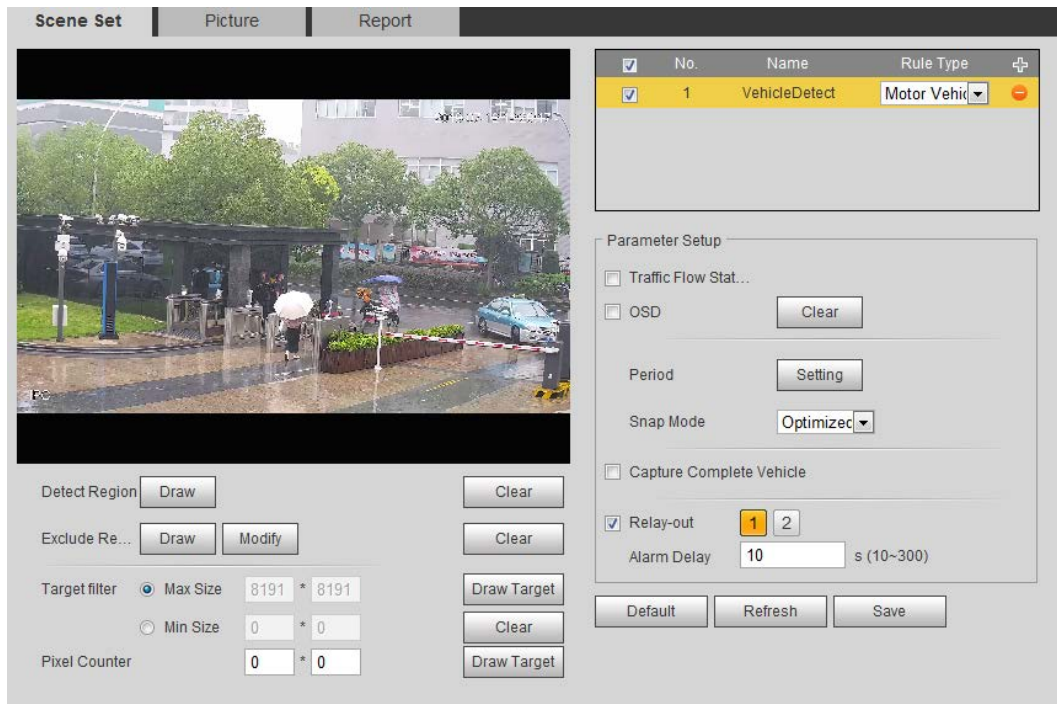
Prerequisites

Select **Setting** > **Event** > **Smart Plan**, and then enable **ANPR**.

Procedure

Step 1 Select **Setting** > **Event** > **ANPR** > **Scene Set**.

Figure 5-83 Scene set (ANPR)



- Step 2** Click **Draw** to draw a detect region and an exclude region in the image.
- Detect region: The region that needs to be detected.
 - Exclude region: The region that does not need to be detected. Click **Modify** to modify the drawn region.
- Click **Clear** at the right side to draw the detection area again.
- Step 3** Click **Draw Target** next to **Target Filter** to draw the maximum size and minimum size for the detection target in the image.
- Step 4** Configure parameters.

Table 5-23 Description of scene set parameters (ANPR)

Parameter	Description
Traffic Flow Statistics	Select Traffic Flow Stat , and the device detects the number of motor vehicles and non-motor vehicles in the detection area and generates the statistical report. If Traffic Flow Stat is disabled, the report has no statistical data.
OSD	Select OSD to display the statistical result on the preview interface. To clear the statistical result, click Clear .
Snap Mode	Select the snap mode: Optimized Snap and Tripwire .
Relay-out	Select the Relay-out checkbox, and when alarm is triggered, the system interacts with the linked alarm devices.
Alarm Delay	The Alarm linkage keeps running for the configured time after alarm is ended.

Step 5 Set arming periods and alarm linkage action. For details, see "5.1.1 Alarm Linkage".

Step 6 Click **Save**.

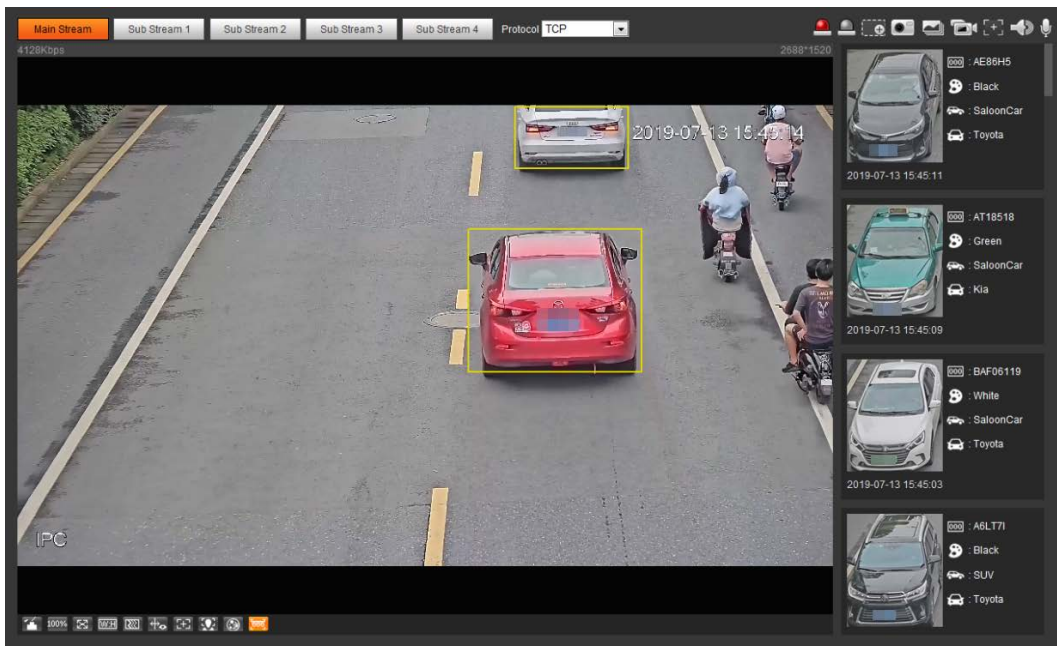
Result

The ANPR result is displayed on the live interface.

- The plate no. and attribute information of vehicle are displayed at the right side.

- Click the picture in the display area, and the detailed information is displayed.

Figure 5-84 ANPR result

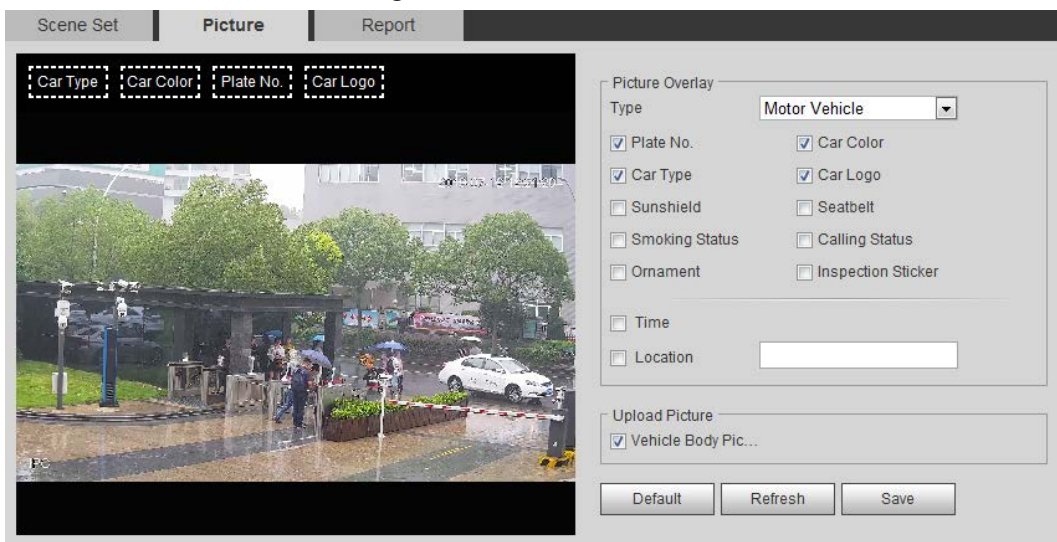


5.16.2 Setting Picture Overlay

Set overlay of motor vehicle.

Step 1 Select **Setting > Event > ANPR > Picture**.

Figure 5-85 Picture



Step 2 Select **Motor Vehicle** from the **Type** drop-down list.

Step 3 Set overlay information and box position, such as plate no., time, car color, car type, and car logo.

Step 4 Click **Save**.

5.16.3 Viewing ANPR Report

Generate data of ANPR in report form.

Step 1 Select **Setting > Event > ANPR > Report**.

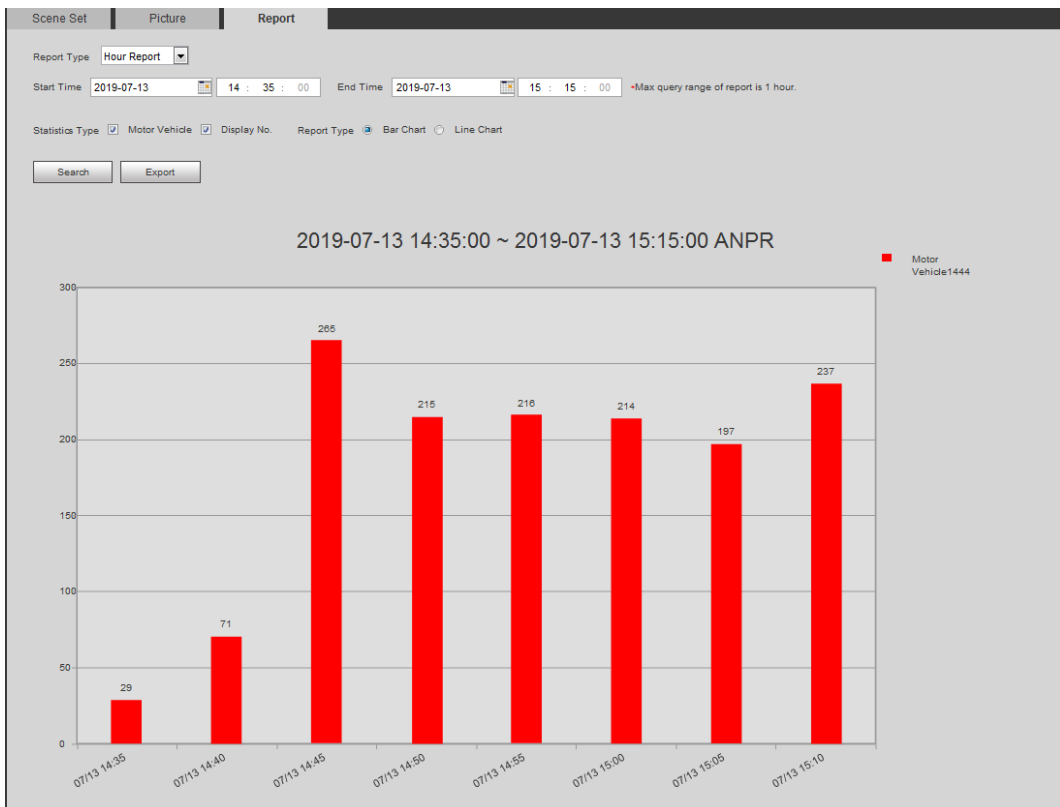
Figure 5-86 Report

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

Step 3 Click **Search**.

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

Figure 5-87 Statistical results



5.17 Setting Video Metadata

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

5.17.1 Scene Configuration

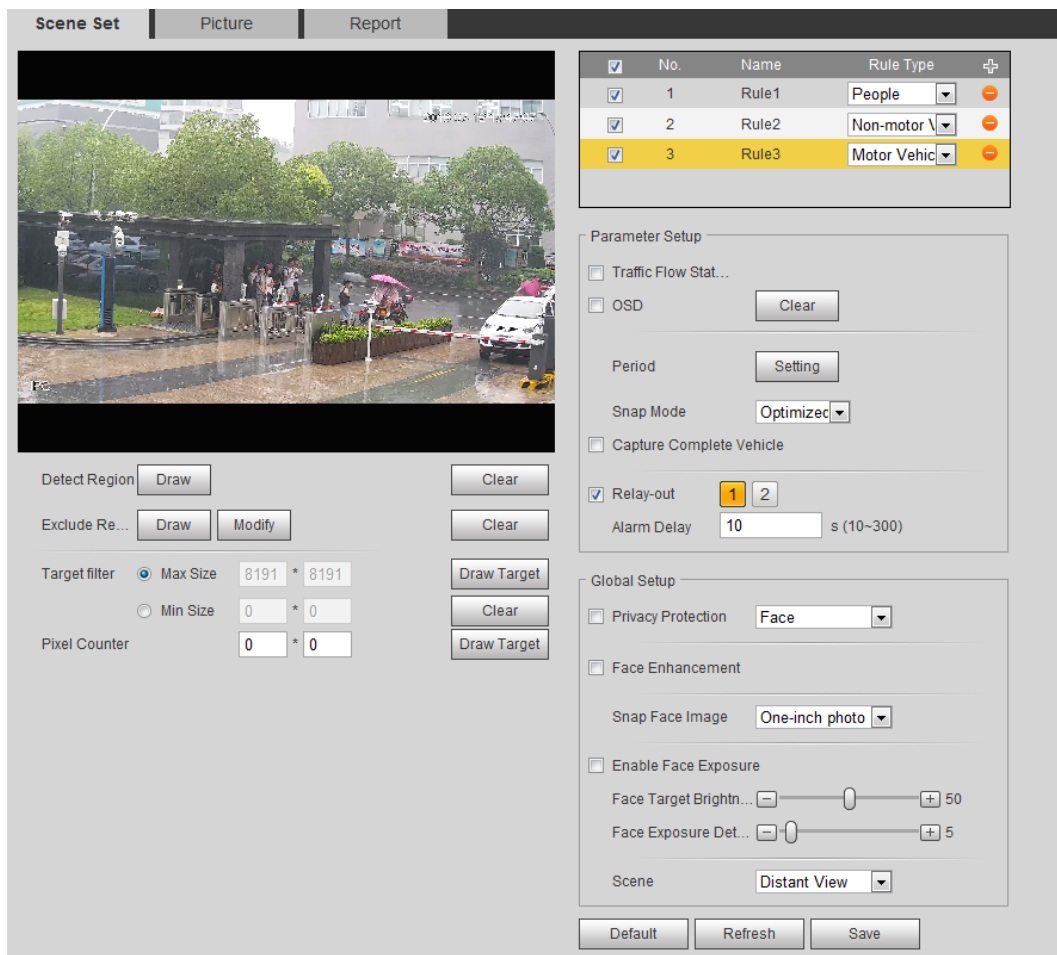
Set the detection scenes and rules, including rules for people, non-motor vehicles and motor vehicles.


Select **Setting > Event > Smart Plan**, and then enable **Video Metadata**.

Take setting of the People Detection rules as an example.

Step 1 Select **Setting > Event > Video Metadata > Scene Set**.

Figure 5-88 Scene set (video metadata)



Step 2 Click , and double-click the name to modify the rule name, and select **People** in **Rule Type** list.


Step 3 Click **Draw** to draw a detect region and an exclude region in the image.

Step 4 Click **Draw Target** next to **Target Filter** to draw the maximum size and minimum size for the detection target in the image.

Step 5 Set parameters.

Table 5-24 Description of scene set parameters (video metadata)


Parameter	Description
People Flow Statistics	Select the People Flow Statistics checkbox to count the number of people in the detection area.
Traffic Flow Stat	Select the Traffic Flow Statistics checkbox to count the number of motor vehicles in the detection area.

Parameter	Description
Capture whole vehicle	Select the Capture Whole Vehicle checkbox to capture whole vehicle. The snapshot is saved in the preset path for monitoring snapshots. For details, see "4.5.2.5 Path".
Non-motor Vehicle Flow Statistics	Select the Non-motor Vehicle Flow Statistics checkbox to count the number of non-motor vehicles in the detection area.
OSD	Select the OSD checkbox, and the numbers of motor vehicles, non-motor vehicles and people in the detection area are displayed.  Click Reset to recount.
Pixel Counter	Click Draw Target next to Pixel Counter , and then press and hold the left mouse button to draw a rectangle, the Pixel Counter then displays its pixel.
Privacy Protection	Select the Privacy Protection checkbox and then select Face or Human body from the drop-down list to blur faces or human bodies in the image.
Face Enhancement	Select the Face Enhancement checkbox to preferably guarantee clear face with low stream.
Snap Face Image	Set a range for snapping face image, including face picture and one-inch picture.
Enable Face Exposure	Select the Enable Face Exposure checkbox to make face clearer by adjusting lens aperture and shutter.
Face Target Brightness	Set the face target brightness, and 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 5 seconds by default.
Scene	Set scene as Distant View or Close View .

Step 6 Set arming periods and alarm linkage actions. For details, see "5.1.1 Alarm Linkage".

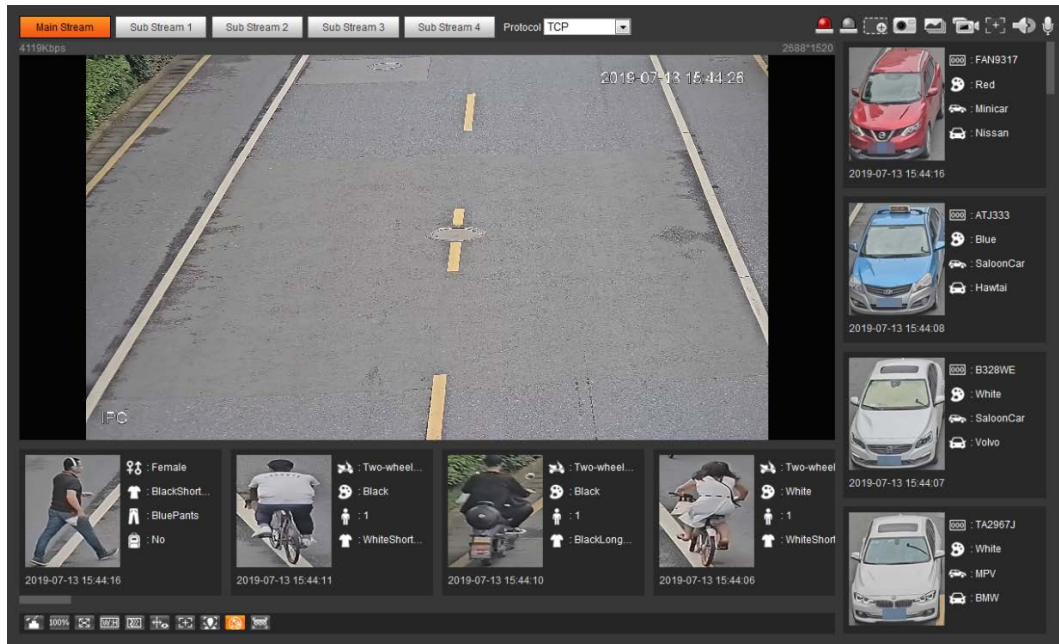
Step 7 Click **Save**.

Result

Click  on the live interface to view the detection results of video metadata.

- The plate no. and attributes of motor vehicle are displayed at the right side, and pictures of people and non-motor vehicles and their attributes at the bottom.
- Click the picture in the display area, and the detailed information is displayed.

Figure 5-89 Video metadata result

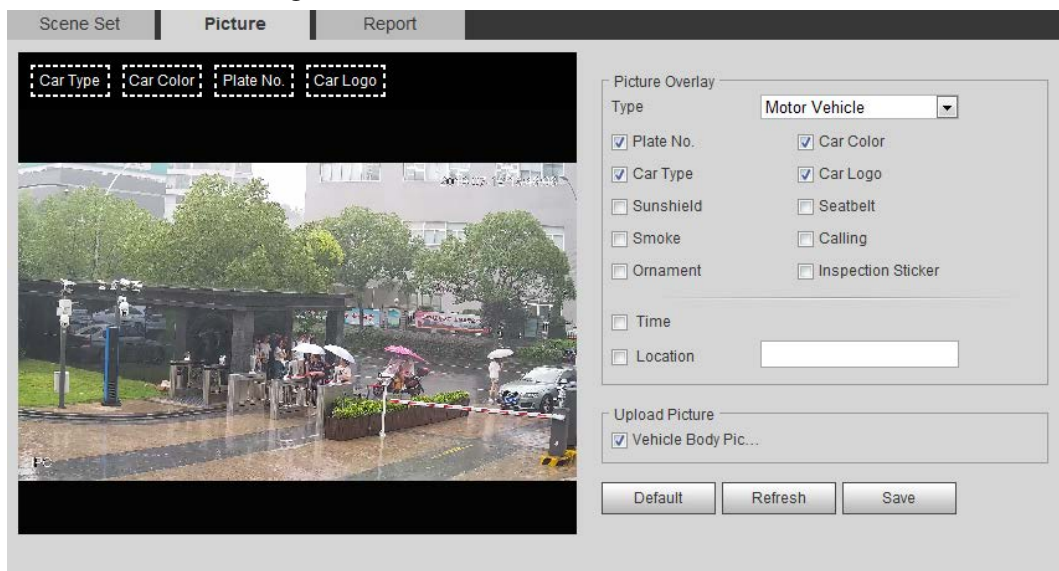


5.17.2 Setting Picture Information

Set overlay of motor vehicle, non-motor vehicle and people and the box position. This section takes the configuration of motor vehicle overlay as an example.

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

Figure 5-90 Picture (video metadata)



Step 2 Select **Motor Vehicle** from the **Type** drop-down list.

Select **Non-motor Vehicle** or **People**, and set non-motor vehicle and people overlay.

Step 3 Set overlay information and box position, such as plate no., time, car color, car type, and car logo.

Step 4 Click **Save**.

5.17.3 Viewing Video Metadata Report

Generate data of video metadata recognition in report form.

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

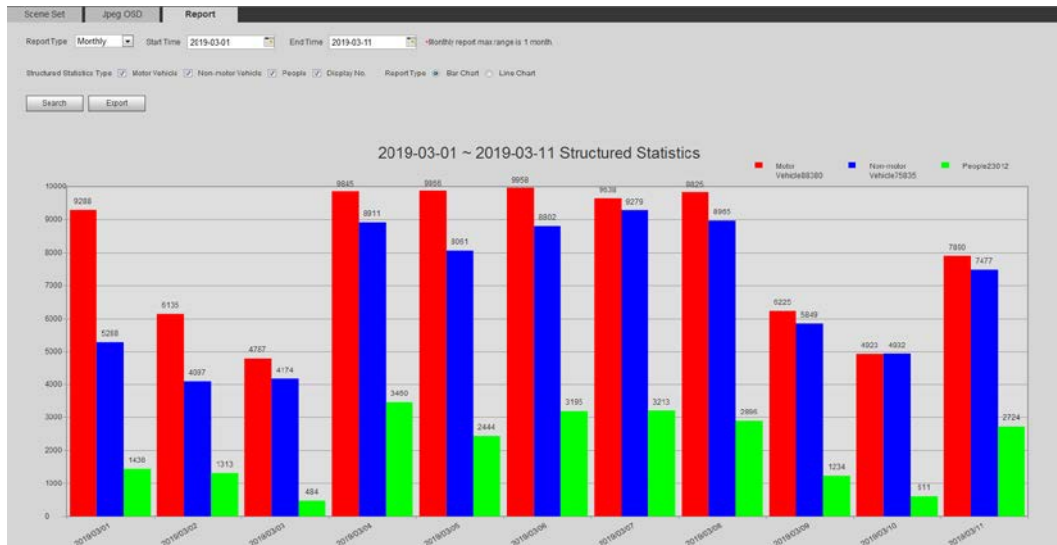
The **Report** interface is displayed.

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 5-91 Video metadata report



5.18 Setting Relay-in

When an alarm is triggered at the alarm-in port, the system performs alarm linkage.



Functions might vary with different models.

5.18.1 Relay-in (1)

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

Figure 5-92 Alarm linkage

Step 2 Select the **Enable** checkbox to enable the alarm linkage function.

Step 3 Select a relay-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 Set arming periods and alarm linkage action. For details, see "5.1.1 Alarm Linkage".

Step 5 Click **Save**.

5.18.2 Relay-in (2)

You can select the mode from **Alarm** and **Arming/Disarming**.

Figure 5-93 Select the mode

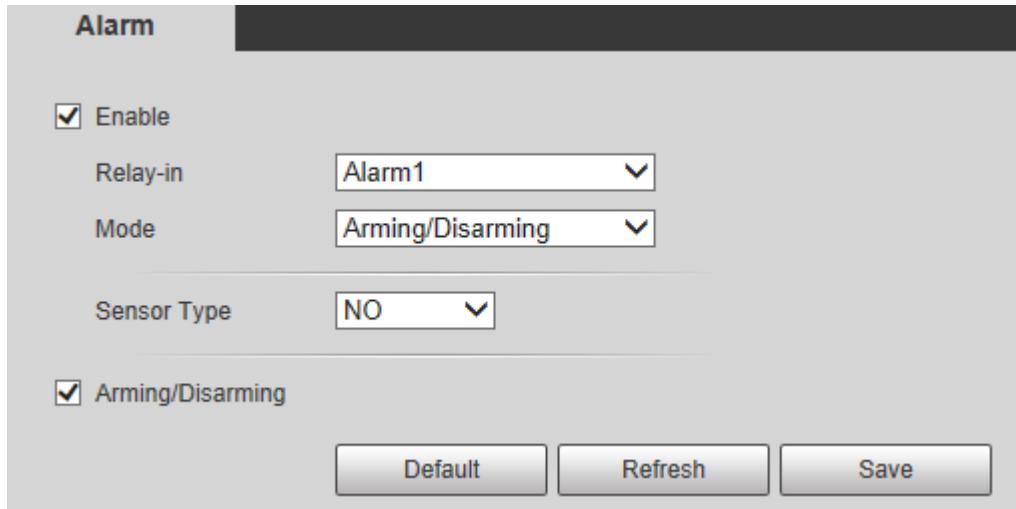
- When selecting **Alarm**, the function is same as Relay-in (1). For details, see "5.18.1 Relay-in (1)".
- When selecting **Arming/Disarming**, you can enable arming or disarming mode through one press on an external alarm system.

Step 1 Select **Enable** checkbox to enable the alarm function.

Step 2 Select a relay-in port, for details, see "5.18.1 Relay-in (1)".

Step 3 In the **Mode** list, select **Arming/Disarming**.

Figure 5-94 Arming/Disarming




The arming/disarming checkbox is selected by default. Do not cancel the selection; otherwise the configuration is invalid.

Step 4 Select the sensor type from **NO** and **NC**.

Step 5 Click **Save**.

5.19 Setting Abnormality

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**.

5.19.1 Setting SD Card

In case of SD card abnormality, the system performs alarm linkage. The event types include **No SD Card**, **Capacity Warning**, and **SD Card Error**. The introduction is for reference only, and may differ from the actual interface.

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

Figure 5-95 SD card

Step 2 Select the event type from the **Event Type** drop-down list, and then select the **Enable** checkbox to enable the SD card detection function.

When setting **Capacity Warning** as **Event Type**, 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 "5.1.1 Alarm Linkage".

Step 4 Click **Save**.

5.19.2 Setting Network

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

Step 1 Select **Setting > Event > Abnormality > Network**.

Figure 5-96 Network

Step 2 Select the event type from the **Event Type** drop-down list, and then select the **Enable** checkbox to enable the network detection function.

Step 3 Set alarm linkage actions. For details, see "5.1.1 Alarm Linkage".

Step 4 Click **Save**.

5.19.3 Setting Illegal Access

When you enter a wrong login password more than the set times, the system performs alarm linkage.

Step 1 Select **Setting** > **Event** > **Abnormality** > **Illegal Access**.

Figure 5-97 Illegal access

Step 2 Select the **Enable** checkbox to enable the illegal access detection function.

Step 3 Set **Login Error**.

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

Step 4 Set alarm linkage actions. For details, see "5.1.1 Alarm Linkage".



Step 5 Click **Save**.

5.19.4 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 **Setting** > **Event** > **Abnormality** > **Voltage Detection**.

Figure 5-98 Voltage detection

- Step 2** Select the **Enable** checkbox to enable the voltage detection function.
 Select **Overlay**, and the alarm icon is displayed by overlapping when the alarm is triggered.
 indicates undervoltage and  indicates overvoltage.
- Step 3** Set alarm linkage actions. For details, see "5.1.1 Alarm Linkage".
- Step 4** Click **Save**.

5.19.5 Setting Security Exception

When a hostile attack is detected, the system performs alarm linkage.

- Step 1** Select **Setting > Event > Abnormality > Security Exception**.
- Step 2** Select the **Enable** checkbox.

Figure 5-99 Security exception

- Step 3** Select the event to be monitored as needed.

Table 5-25 Security exception description

Parameter	Description
Trusted environment detected program	Monitors the programs that run in trusted environment to detect whether there are program running without trusted signature. Select it to prevent the program with trojan and virus.
Account login exceeds the set time range	The account tries to login during the period that does not allow user to log in. Configure Restricted Login in Setting > System > Account > Account > Username , including the IP address, validity period, and time range.
Session ID Brute Force Attack	When sessionid false reaches the configured threshold in the defined period, an alarm will be triggered. Select it to monitor attacks in real time, so that attacks can be prevented timely.
Brute force attack of web path	Generates the web serve directory and send a request through enumeration. When URL false reaches the configured threshold in the defined period, an alarm will be triggered. Select it to monitor attacks in real time, so that attacks can be prevented timely.
Session connection exceeds limit	The number of users (web, platform or mobile phone client) exceeds the max number of users that can connect to the device simultaneously. Configure the Max Connection in Setting > Network > Port .

Step 4 Set alarm linkage actions. For details, see "5.1.1 Alarm Linkage".

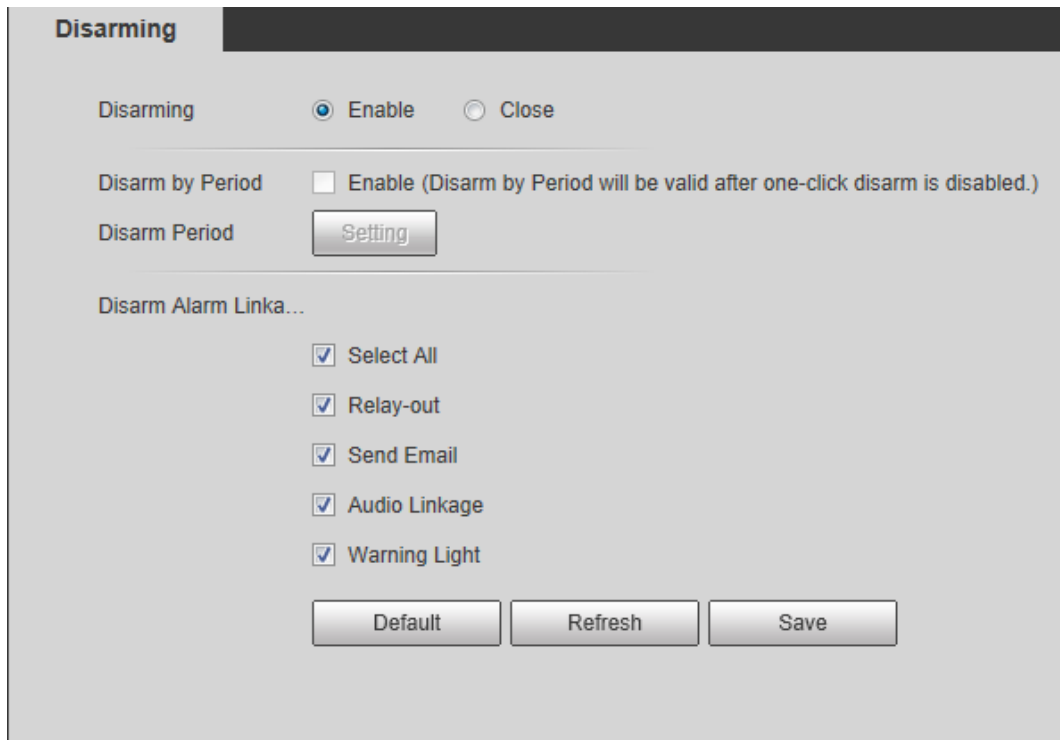
Step 5 Click **Save**.

5.19.6 Setting Disarming

You can disable the linkage actions through the app on your smart phone, and then the system will not perform any linkage action, but alarm records will still be generated.

Step 1 Select **Setting > Event > Disarming**.

Figure 5-100 Disarming



Step 2 Select the **Enable** checkbox to disarm.

Step 3 (Optional) Select the **Enable** checkbox next to **Disarm by Period** to enable the Disarm by Period function, and then you can disarm by period. For setting disarm period, see "5.1.1.1 Setting Period".



This function is only valid when **Disarming** is disabled.

Step 4 Select alarm linkage actions as needed.

Step 5 Click **Save**.

6 Maintenance

6.1 Requirements

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

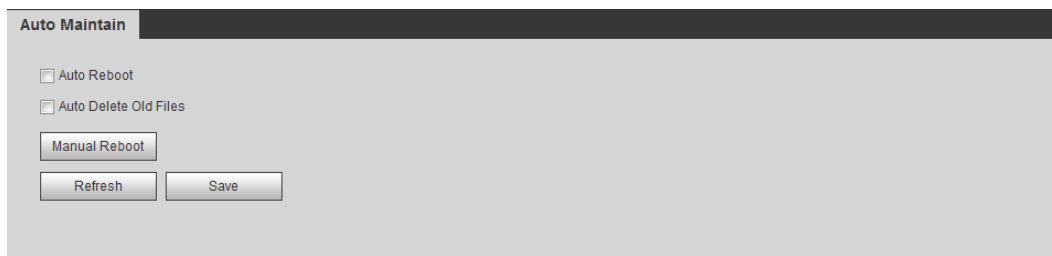
- Check surveillance images regularly.
- Clear regularly user and user group information that are not frequently used.
- Modify the password every three months. For details, see "4.8.3 Account".
- View system logs and analyze them, and process the abnormality in time.
- Back up the system configuration regularly.
- Restart the device and delete the old files regularly.
- Upgrade firmware in time.

6.2 Auto Maintain

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 **Setting** > **System** > **Auto Maintain**.

Figure 6-1 Auto maintain



Step 2 Configure auto maintain parameters.

- Select the **Auto Reboot** checkbox, and set the reboot time, the system automatically restarts as the set time every week.
- Select the **Auto Delete Old Files** checkbox, 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 Old Files** function, The **The deleted files cannot be restored, are you sure?** notice is displayed. Operate it carefully.

- Click **Manual Reboot**, and then click **OK** on the displayed interface, the camera will restart.

Step 3 Click **OK**.

6.3 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 reset service. For details, see "4.8.4.1 System Service".

Procedure

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

Figure 6-2 Login



Step 2 Click **Forgot password?**

Figure 6-3 Prompt

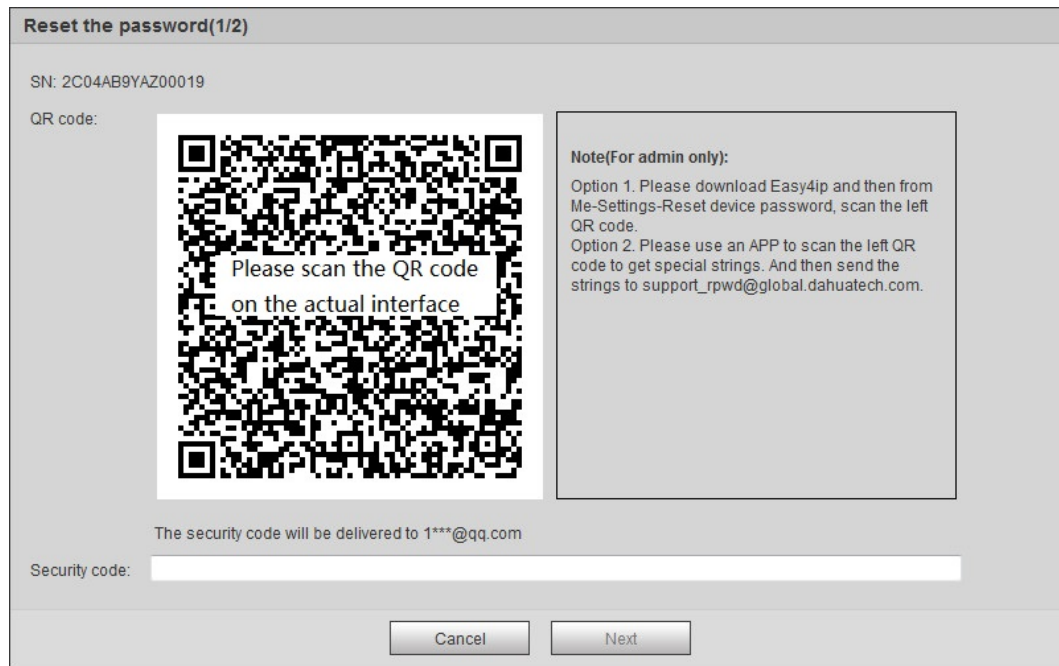


Step 3 Click **OK**.



Clicking **OK** means that you are informed that some of your personal data might be collected to help reset the password, such as phone number, MAC address, and device serial number. Read the prompt carefully to decide whether to authorize the collection activity.

Figure 6-4 Reset the password (1)



Reset the password(1/2)

SN: 2C04AB9YAZ00019

QR code:

Please scan the QR code on the actual interface

Note(For admin only):

Option 1. Please download Easy4ip and then from Me-Settings-Reset device password, scan the left QR code.

Option 2. Please use an APP to scan the left QR code to get special strings. And then send the strings to support_rpwd@global.dahuatech.com.

The security code will be delivered to 1***@qq.com

Security code:

Cancel Next

Step 4 Reset the password.

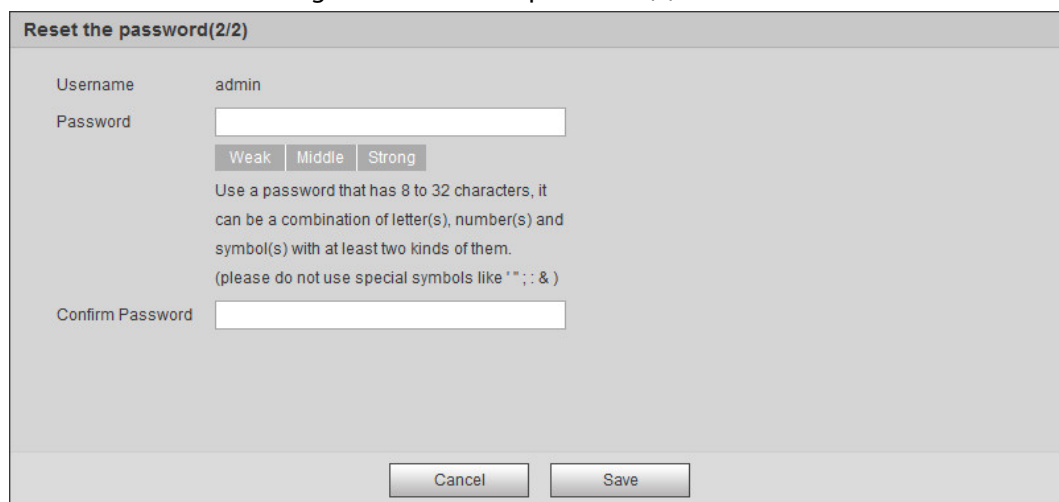
Step 5 Scan the QR code, and there will be a security code sent to the email address you entered. Enter the security code as instructed.



- Please use the security code within 24 hours after you receive it. Otherwise, it will become invalid.
- If you fail to use the security code for two times continuously, there will be fail notice when you try to get a security code for the third time. You have to reset the device to get a security code or wait 24 hours to get it again.

Step 6 Click **Next**.

Figure 6-5 Reset the password (2)



Reset the password(2/2)

Username admin

Password

Weak Middle Strong

Use a password that has 8 to 32 characters, it can be a combination of letter(s), number(s) and symbol(s) with at least two kinds of them. (please do not use special symbols like * ; : &)

Confirm Password

Cancel Save

Step 7 Reset and confirm the 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 ' " ; : &).

Step 8 Click **Save**.

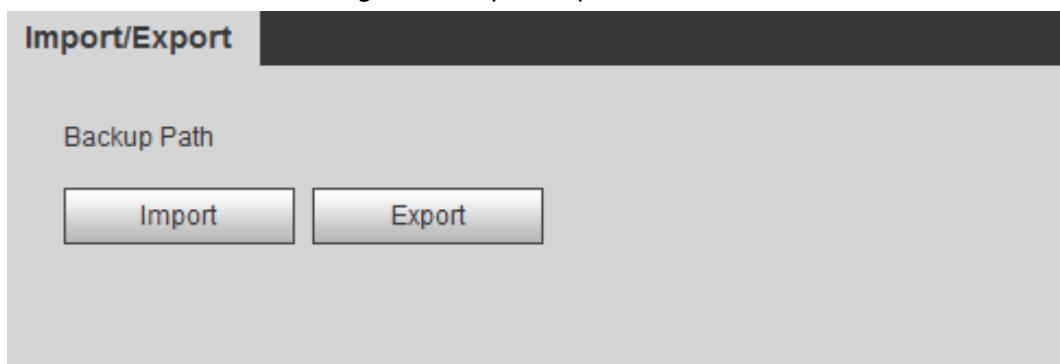
6.4 Backup and Default

6.4.1 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 **Setting > System > Import/Export**.

Figure 6-6 Import/Export



Step 2 Click **Import** or **Export**.

- Import: Select local configuration file, and click **Open** to import the local system configuration file to the system.
- Export: Select the storage path, and click **Save** to export the system configuration file to local storage.

Step 3 Click **Save** to finish configuration.

6.4.2 Default

Restore the device to default configuration or factory settings.

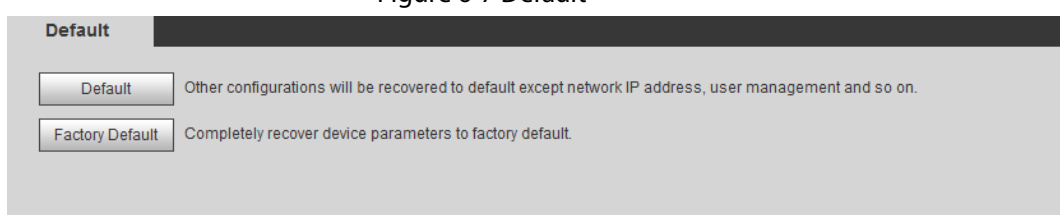


This function will restore the device to default configuration or factory setting.

Select **Setting > System > 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 6-7 Default



6.5 Upgrade

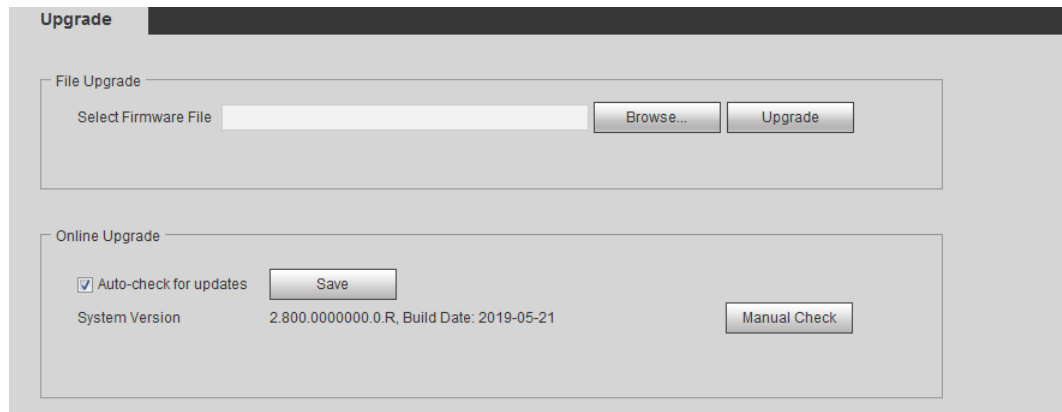
Upgrading to the latest system can perfect camera functions and improve stability.



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

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

Figure 6-8 Upgrade



Step 2 Select upgrading method according to the actual needs.

- File Upgrade
 1. Click **Browse**, and then upload upgrade file.
 2. The upgrade file should be a .bin file.
 3. Click **Upgrade**.
The upgrade starts.
- Online Upgrade
 1. Select the **Auto-check for updates** checkbox.
The system checks for upgrade once a day automatically, and there will be system notice if any upgrade is available.



We need to collect the data such as device name, firmware version, and device serial number to proceed auto-check. The collected information is only used for verifying the legality of cameras and upgrade notice.

2. If there is any upgrade available, click **Upgrade**, and then the system starts upgrading.



Click **Manual Check** to check for upgrade manually.

6.6 Information

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

6.6.1 Version

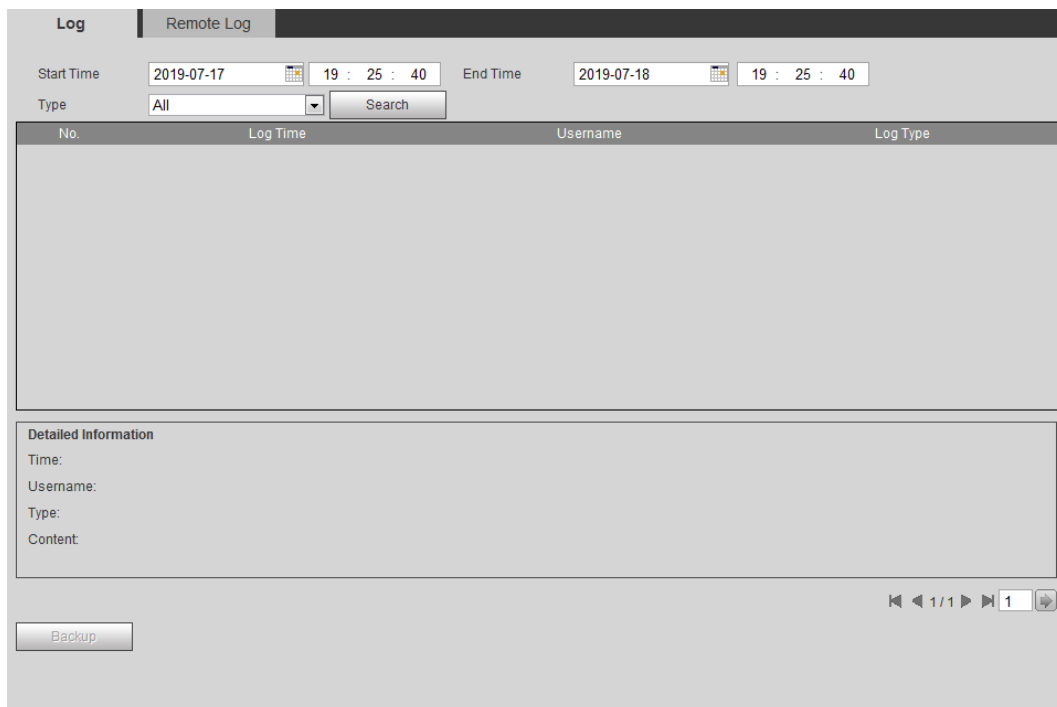
You can view device information such as hardware, system version, and web version.
 Select **Setting > Information > Version** to view the version information.

6.6.2 Log

You can view and back up logs.

Step 1 Select **Setting > Information > Log**.

Figure 6-9 Log



The screenshot shows the 'Log' interface with the following elements:

- Navigation tabs: 'Log' (selected) and 'Remote Log'.
- Search filters: 'Start Time' (2019-07-17 19:25:40), 'End Time' (2019-07-18 19:25:40), and 'Type' (All).
- A 'Search' button.
- A table with columns: 'No.', 'Log Time', 'Username', and 'Log Type'.
- A 'Detailed Information' section with fields for 'Time:', 'Username:', 'Type:', and 'Content:'.
- A 'Backup' button.
- Navigation controls at the bottom right: '1 / 1' and a '1' page indicator.

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, modifying user, adding group, deleting group, and modifying group.
- **Safety:** Includes password resetting and IP filter.

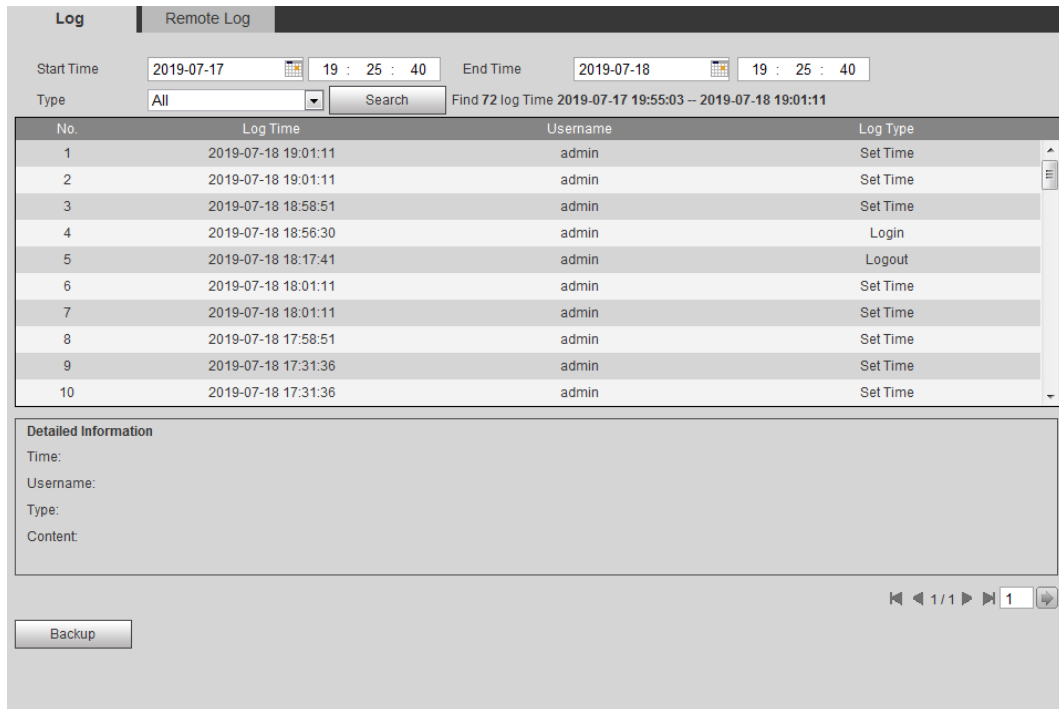
Step 3 Click **Search**.

- Click a certain log, and then you can view the detailed information in **Detailed**

Information area.

- Click **Backup**, and then you can back up all found logs to local PC.

Figure 6-10 Log (details)

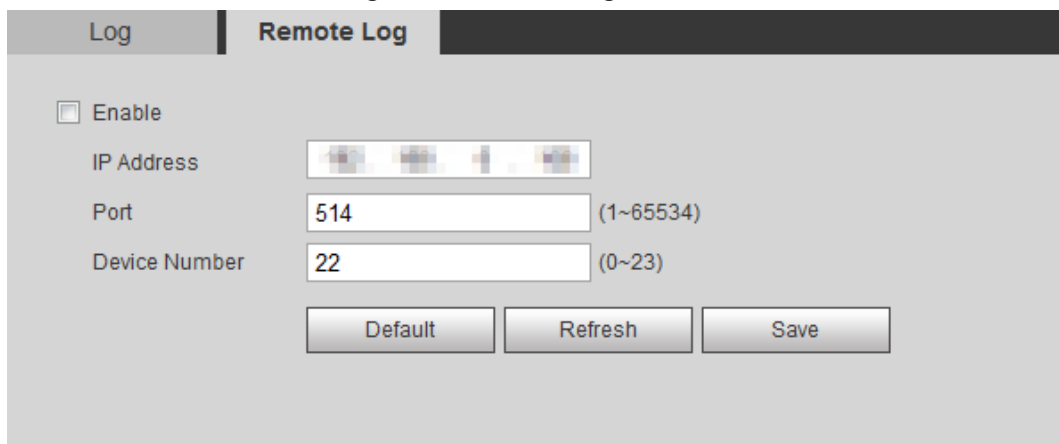


6.6.3 Remote Log

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

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

Figure 6-11 Remote log



Step 2 Select the **Enable** checkbox to enable remote log function.

Step 3 Set address, port and device number.

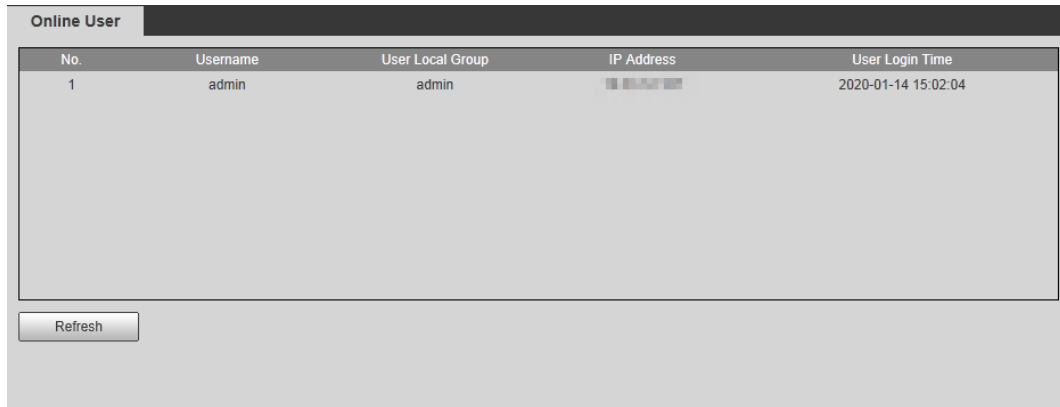
Step 4 Click **Save**.

6.6.4 Online User

View all the current users logging in to web.

Select **Setting** > **Information** > **Online User**.

Figure 6-12 Online user



The screenshot displays a web interface titled "Online User". It features a table with the following columns: "No.", "Username", "User Local Group", "IP Address", and "User Login Time". A single row of data is visible, representing the user "admin" with a login time of "2020-01-14 15:02:04". Below the table is a "Refresh" button.

No.	Username	User Local Group	IP Address	User Login Time
1	admin	admin	192.168.1.1	2020-01-14 15:02:04

Refresh

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 from Dahua 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.

More information

Please visit Dahua official website security emergency response center for security announcements and the latest security recommendations.

ENABLING A SAFER SOCIETY AND SMARTER LIVING

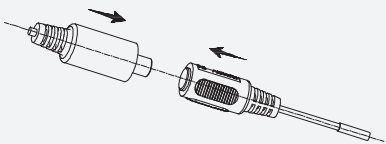
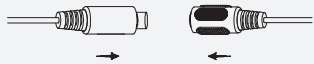
ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.

Address: No.1199 Bin'an Road, Binjiang District, Hangzhou, P. R. China | Website: www.dahuasecurity.com | Postcode: 310053

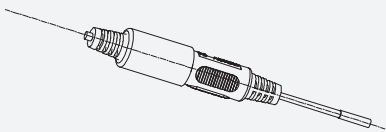
Email: overseas@dahuatech.com | Fax: +86-571-87688815 | Tel: +86-571-87688883

B

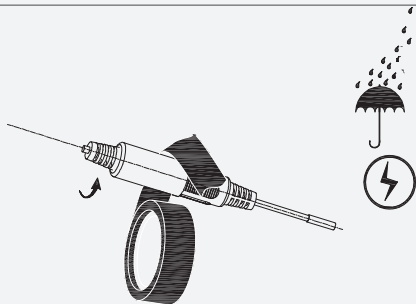
1



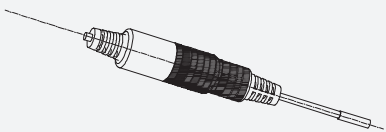
2



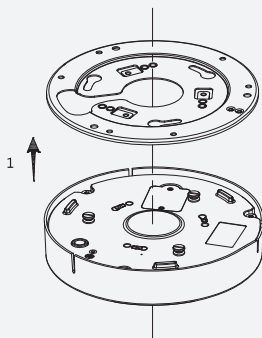
3



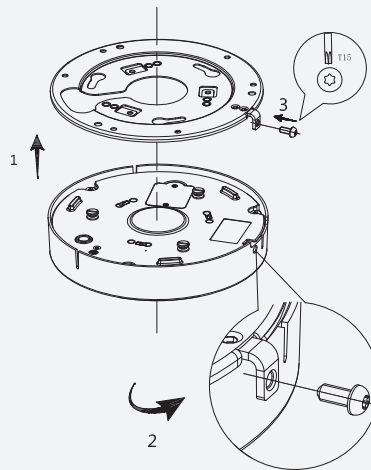
4



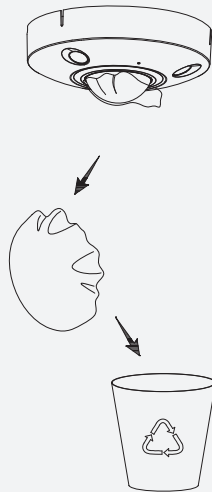
3.1a



3.1b












3.2



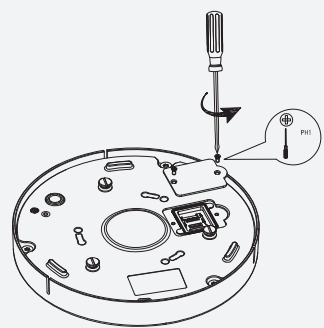
Fisheye Network Camera

Installation Guide

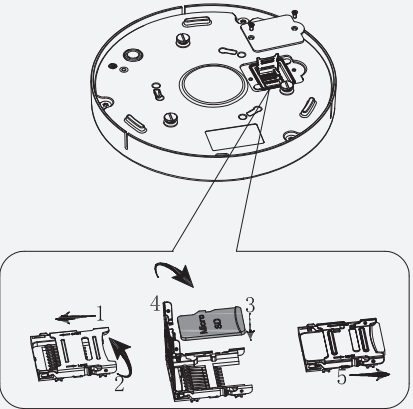
V1.0.0

-  × 1
-  × 1
-  × 2
-  × 1
-  × 1
-  × 1
-  × 1
-  × 1 (Optional)
-  × 1 (Optional)

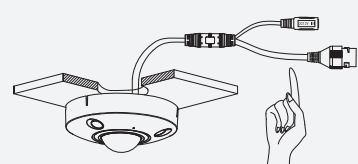
1.1 Optional



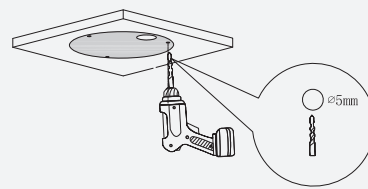
1.2



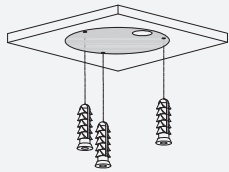
2.1



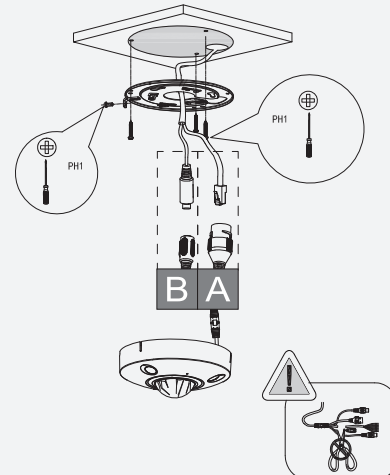
2.2




2.3



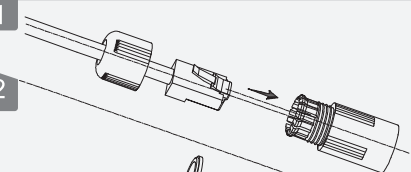
2.4



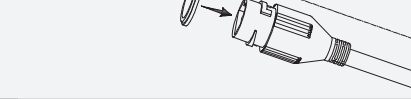
A Optional



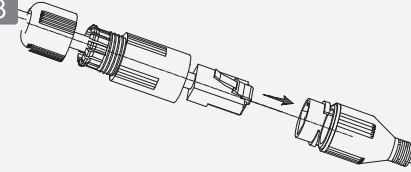
1



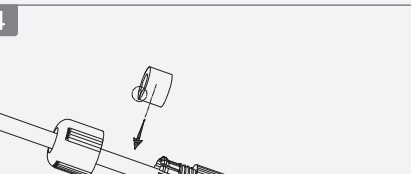
2



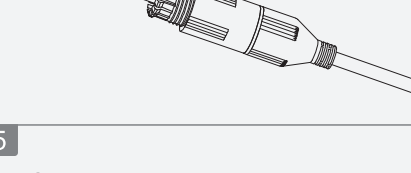
3



4



5



6

