



Network Speed Dome & PTZ Camera Web 3.0

User Manual









Foreword

General

This manual introduces the functions and operations of the network speed dome and PTZ camera (hereinafter referred to as "the Device").

Safety Instructions

The following signal words might appear in the manual.

Signal Words	Meaning
 DANGER	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
 WARNING	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
 CAUTION	Indicates a potential risk which, if not avoided, could result in property damage, data loss, reductions in performance, or unpredictable results.
 ESD	Electrostatic Sensitive Devices. Indicates a device that is sensitive to electrostatic discharge.
 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	Release Content	Revision Time
V3.0.4	Updated illuminator function.	September 2023
V3.0.3	Added sleep mode function.	February 2022
V3.0.2	<ul style="list-style-type: none">Updated illuminator function.Added legal information function.	September 2021
V3.0.1	Added Configuring User Group function.	July 2021
V3.0.0	<ul style="list-style-type: none">Modified overlay, audio, network settings, and destination sections.Added Bluetooth settings, construction monitoring, battery exception, screen-off settings, emergency maintenance, life statistics, and battery status sections.	March 2021
V2.0.2	Added the note to provide international calling codes for 4G models.	June 2020

Version	Release Content	Revision Time
V2.0.1	Updated OSD info, TCP/IP and smart plan, and delete life statistics.	April 2020
V2.0.0	Added some functions of the Baseline, and refine the whole manual.	January 2020
V1.1.1	Updated some functions of the Security Baseline.	September 2019
V1.0.0	First release.	May 2018

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.

Interface Declaration

This manual mainly introduces the relevant functions of the device. The interface used in its manufacture, the procedures for returning the device to the factory for inspection and for locating its faults are not described in this manual. Please contact technical support if you need information on these interfaces.

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

This section introduces content covering the proper handling of the device, hazard prevention, and prevention of property damage. Read carefully before using the device, and comply with the guidelines when using it

Transportation Requirements



- Pack the device with packaging provided by its manufacturer or packaging of the same quality before transporting it.
- Avoid heavy stress, violent vibration, and immersion during transportation.
- Transport the device under allowed humidity and temperature conditions. Refer to the technical parameters for requirements on the transporting temperature and humidity of the device

Storage Requirements



- Store the device under allowed humidity and temperature conditions. Refer to the technical parameters for requirements on the storing temperature and humidity of the device.
- Avoid heavy stress, violent vibration, and immersion during storage.

Installation Requirements



- Make sure that the power is off when you connect the cables, install or disassemble the device.
- For devices with earthing systems, make sure they are grounded to avoid being damaged by static electricity or induced voltage, and prevent electrocution from occurring.
- All installation and operations must conform to local electrical safety regulations.
- Use accessories suggested by the manufacturer, and installed by professionals.
- Do not block the ventilator of the device, and install the device in a well-ventilated place.
- Do not expose the device to heat sources or direct sunlight, such as radiator, heater, stove or other heating equipment, which is to avoid the risk of fire.
- Do not place the device in explosive, humid, dusty, extremely hot or cold sites with corrosive gas, strong electromagnetic radiation or unstable illumination.
- Avoid heavy stress, violent vibration, and immersion during installation.



Safe and stable power supply is a prerequisite for proper operation of the device.

- Make sure that the ambient voltage is stable and meet the power supply requirements of the device.
- Prevent the power cord from being trampled or pressed, especially the plug, power socket and the junction from the device.
- For devices that can be powered by multiple supplies, do not connect them to two or more kinds of power supplies; otherwise, the device might be damaged.

- Refer to the specific user's manual for the power requirements of single device.



It is recommended to use the device with a lightning protector for better lightning-proof effect.

Operation Requirements



A suitable operating environment is the foundation for the device to work properly. Confirm whether the following conditions have been met before use.

- Use the device under allowed humidity and temperature conditions. Refer to the technical parameters for requirements on the operating temperature and humidity of the device.
- Use the device on a stable base.
- Do not let any liquid flow into the device to avoid damage to internal components. When liquid flows into the device, immediately disconnect the power supply, unplug all cables connected to it, and contact after-sales service.
- Do not plug or unplug RS-232, RS-485 and other ports with the power on, otherwise, the ports will be easily damaged.
- Back up data in time during deployment and use, in an effort to avoid data loss caused by abnormal operation. The company is not liable for data security.
- The company is not responsible for damages to the device or other product problems caused by excessive use or other improper use.

Maintenance Requirements



WARNING

- Contact professionals for regular inspection and maintenance of the device. Do not disassemble or dismantle the device without a professional present.
- Use accessories suggested by the manufacturer, and maintain the device by professionals.

Table of Contents

Foreword.....	I
Important Safeguards and Warnings.....	III
1 Network Configuration.....	1
1.1 Network Connection.....	1
1.2 Log in to the Webpage.....	1
1.2.1 Device Initialization.....	1
1.2.2 First-time Login.....	4
1.2.3 Device Login.....	6
1.2.4 Resetting Password.....	6
2 Live.....	10
2.1 Encoding Setting.....	10
2.2 Video Window Adjustment.....	11
2.3 System Menu.....	15
2.4 Video Window Functions.....	15
2.5 PTZ Configuration.....	18
2.6 PTZ Status.....	22
3 AI Live.....	24
3.1 AI Live Page.....	24
3.1.1 Information Display Area of Detected Targets.....	24
3.1.2 Snapshot Display Area.....	25
3.1.3 Statistics Area of the Detected Targets.....	25
3.2 AI Live Settings.....	26
4 Playback.....	28
4.1 Video Playback.....	28
4.1.1 Video Play Function Bar.....	29
4.1.2 Recording Type.....	29
4.1.3 Auxiliary Functions.....	30
4.1.4 Video Playback File Search and Display Area.....	30
4.1.5 Video Clipping Area.....	34
4.1.6 Progress Bar Time Formats.....	34
4.2 Image Playback.....	35
4.2.1 Image Playing Functions.....	35
4.2.2 Image Playback File Search and Display Area.....	36
4.2.3 Snapshot Types.....	37
5 Setting.....	38
5.1 Camera.....	38
5.1.1 Conditions Settings.....	38

5.1.2	Video.....	56
5.1.3	Audio.....	69
5.2	Network Settings.....	72
5.2.1	TCP/IP.....	72
5.2.2	Port.....	76
5.2.3	PPPoE.....	78
5.2.4	DDNS.....	78
5.2.5	SMTP (Email).....	80
5.2.6	UPnP.....	82
5.2.7	Bonjour.....	83
5.2.8	SNMP.....	84
5.2.9	Multicast.....	87
5.2.10	Auto Register.....	88
5.2.11	Wi-Fi.....	89
5.2.12	802.1x.....	92
5.2.13	QoS.....	93
5.2.14	4G/5G.....	94
5.2.15	Access Platform.....	97
5.3	Bluetooth Settings.....	100
5.4	PTZ Settings.....	102
5.4.1	Protocol.....	102
5.4.2	Function.....	103
5.5	Event Management.....	116
5.5.1	Video Detection.....	116
5.5.2	Smart Motion Detection.....	122
5.5.3	Audio Detection.....	123
5.5.4	Smart Plan.....	125
5.5.5	IVS.....	126
5.5.6	Construction Monitoring.....	133
5.5.7	Face Recognition.....	138
5.5.8	People Counting.....	148
5.5.9	Heat Map.....	150
5.5.10	Video Metadata.....	152
5.5.11	Alarm.....	156
5.5.12	Abnormality.....	157
5.6	Storage.....	162
5.6.1	Schedule.....	162
5.6.2	Snapshot by Location.....	165
5.6.3	Destination.....	166
5.6.4	Record Control.....	169

5.7 System Management.....	171
5.7.1 Device Settings.....	171
5.7.2 Account Settings.....	175
5.7.3 Safety.....	182
5.7.4 Peripheral.....	194
5.7.5 Default.....	195
5.7.6 Import/Export.....	195
5.7.7 System Maintenance.....	196
5.7.8 Upgrade.....	197
5.8 Information.....	198
5.8.1 Version.....	198
5.8.2 Log Information.....	199
5.8.3 Online User.....	201
5.8.4 Life Statistics.....	201
5.8.5 Battery Status.....	201
5.8.6 Legal Information.....	202
6 Alarm.....	203
7 Logout.....	205
Appendix 1 Security Recommendation.....	206
Appendix 2 Security Commitment and Recommendation.....	209

1 Network Configuration

1.1 Network Connection

To view the webpage on your computer, connect the Device to the computer first. There are mainly two connection modes between the Device and computer.



The models presented in the figures are for reference only, and the actual product shall prevail.

Figure 1-1 Direct connection by using a network cable

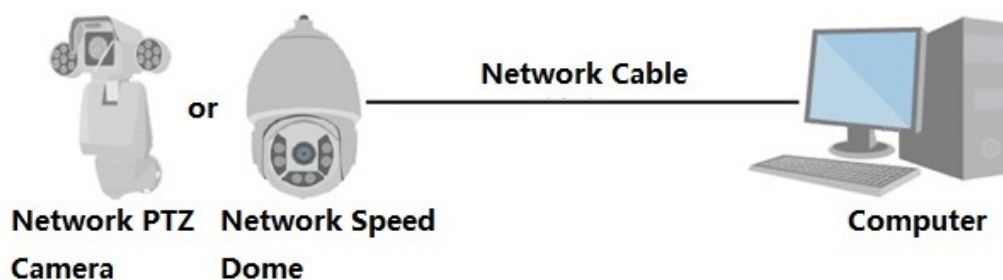
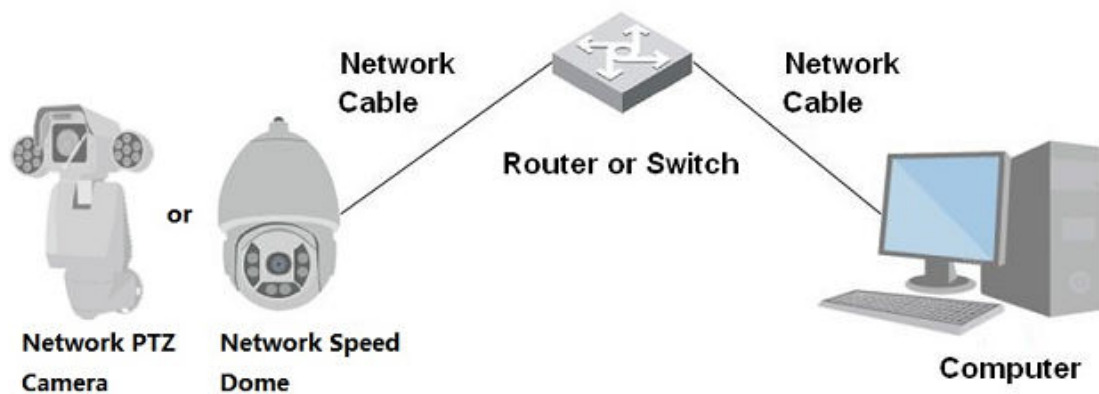


Figure 1-2 Connection by using a switch or router



All devices have the same IP address (192.168.1.108 by default) when they are delivered out of factory. To make the Device get access to network smoothly, plan available IP segment reasonably according to practical network environment.

1.2 Log in to the Webpage

1.2.1 Device Initialization

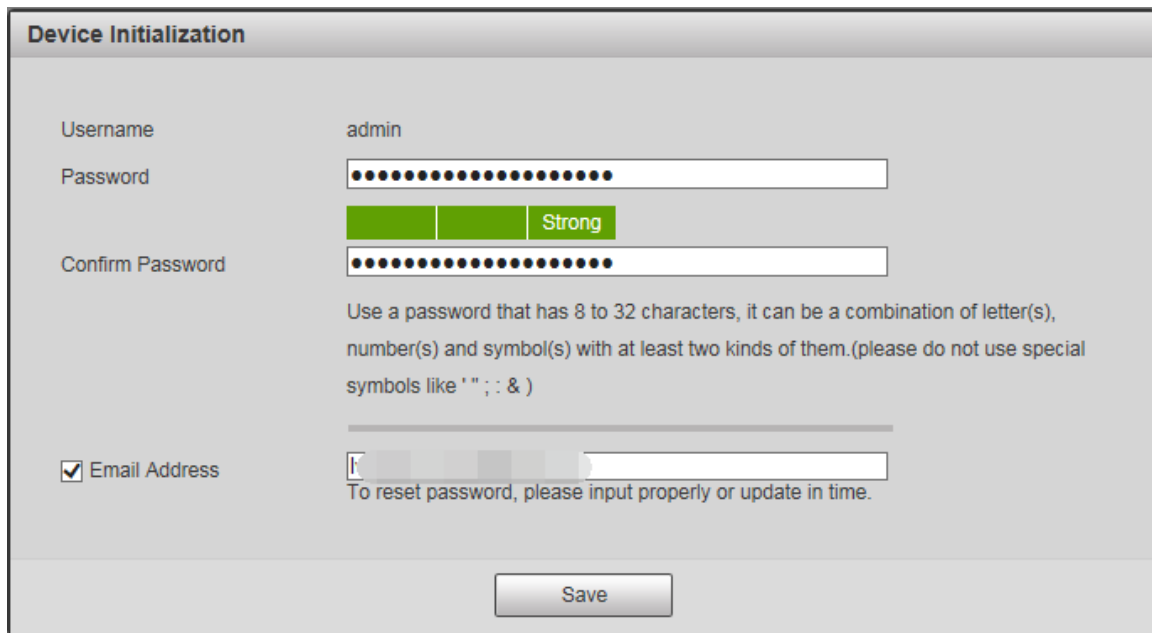
Background Information

For first-time use or after you have restored the Device to defaults, you need to initialize the Device by performing the following steps.

Procedure

- Step 1** Open the browser, enter the IP address of the Device in the address bar, and then press the Enter key.
- Step 2** Set the **Country/Region** , **Language** and **Video Standard**, and then click **Save**.
- Step 3** Configure time parameters, and then click **Next**.
- Step 4** Set the password for admin account, and then click **Save**.

Figure 1-3 Device initialization



Device Initialization

Username: admin

Password: [Masked] Strong


Confirm Password: [Masked]

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 [Masked]
To reset password, please input properly or update in time.

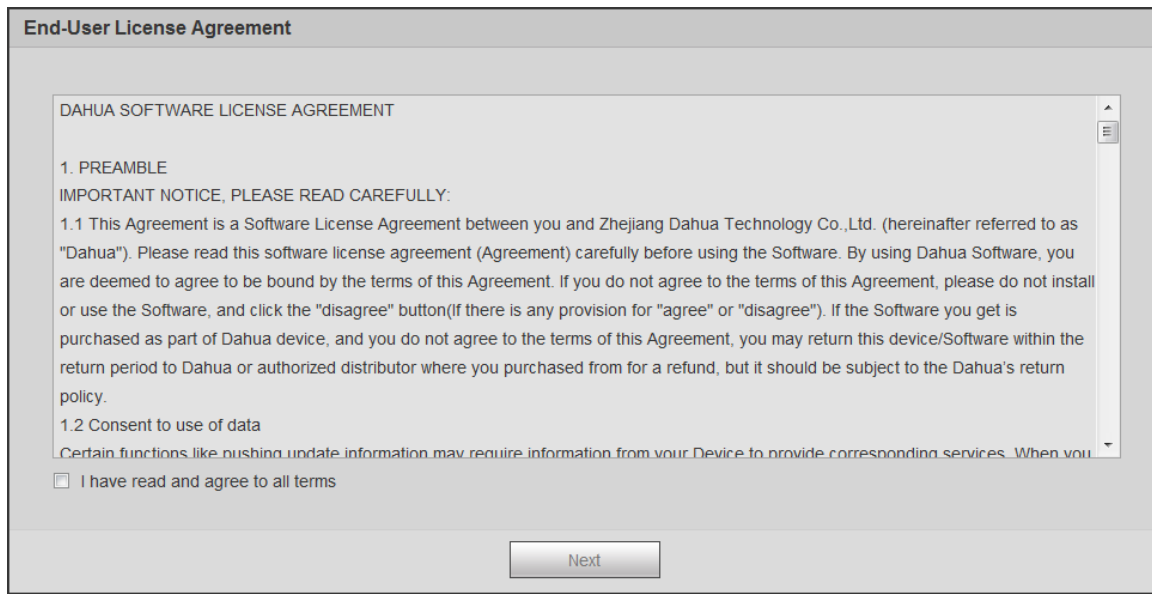
Save

Table 1-1 Device initialization parameter description

Parameter	Description
Username	It is admin by default.
Password	The password should consist of 8 to 32 non-blank characters and contain at least two types of characters among upper case, lower case, number, and special characters (excluding ' " ; : &). Set a high security password according to the prompt of password strength. Make sure that the new password is the same as the confirming password.
Confirm Password	Enter the confirming password that shall be the same as the password you entered.
Email Address	Set the email address which is used to reset password.  Email address is enabled by default. You can disable the function as needed.

- Step 5** Select **I have read and agree to all terms** checkbox, and then click **Next**.

Figure 1-4 End-user license agreement



The image shows a window titled "End-User License Agreement". Inside, there is a text area with the following content:

DAHUA SOFTWARE LICENSE AGREEMENT

1. PREAMBLE
IMPORTANT NOTICE, PLEASE READ CAREFULLY:

1.1 This Agreement is a Software License Agreement between you and Zhejiang Dahua Technology Co.,Ltd. (hereinafter referred to as "Dahua"). Please read this software license agreement (Agreement) carefully before using the Software. By using Dahua Software, you are deemed to agree to be bound by the terms of this Agreement. If you do not agree to the terms of this Agreement, please do not install or use the Software, and click the "disagree" button(if there is any provision for "agree" or "disagree"). If the Software you get is purchased as part of Dahua device, and you do not agree to the terms of this Agreement, you may return this device/Software within the return period to Dahua or authorized distributor where you purchased from for a refund, but it should be subject to the Dahua's return policy.

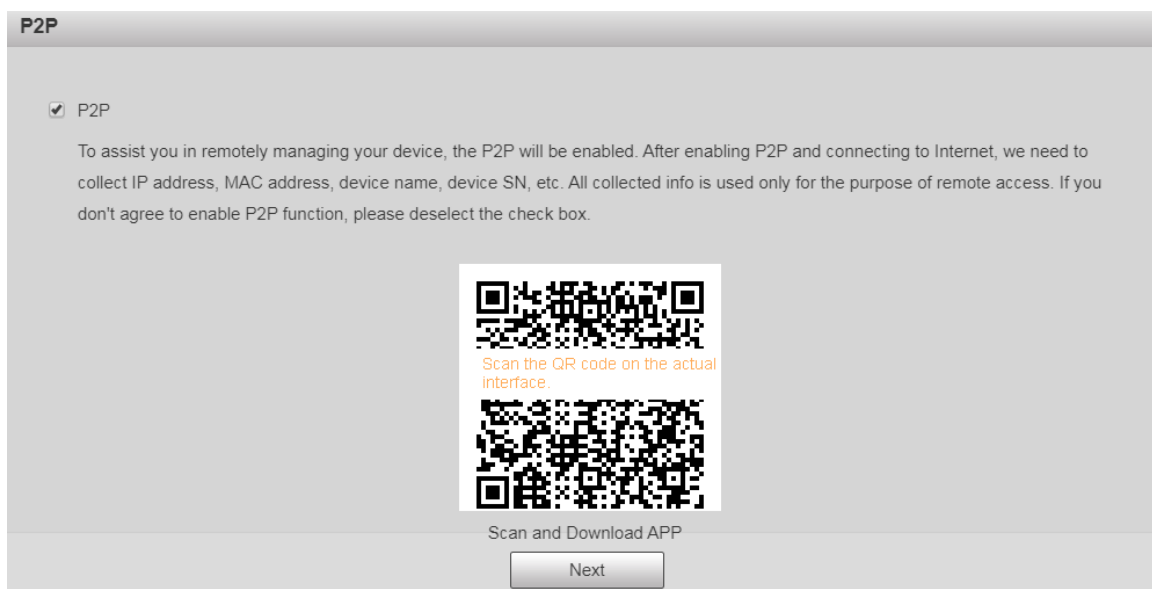
1.2 Consent to use of data
Certain functions like pushing update information may require information from your Device to provide corresponding services. When you

☐ I have read and agree to all terms

At the bottom right, there is a "Next" button.

Step 6 Select **P2P** checkbox, and then click **Next**.

Figure 1-5 P2P page



The image shows a window titled "P2P". Inside, there is a checkbox labeled "P2P" which is checked. Below it, there is a paragraph of text:

To assist you in remotely managing your device, the P2P will be enabled. After enabling P2P and connecting to Internet, we need to collect IP address, MAC address, device name, device SN, etc. All collected info is used only for the purpose of remote access. If you don't agree to enable P2P function, please deselect the check box.

Below the text, there are two QR codes. Between them, there is a text label: "Scan the QR code on the actual interface."

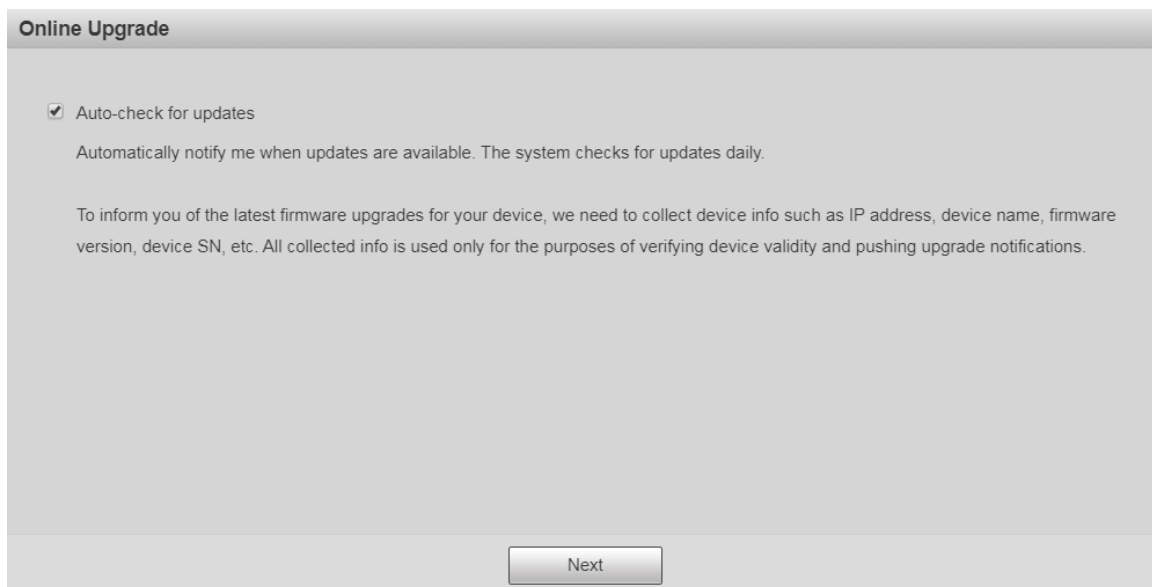
Below the QR codes, there is a text label: "Scan and Download APP".

At the bottom right, there is a "Next" button.

Step 7 Scan the QR code on the page, download the app, and then finish configurations according to the instructions on your mobile device. After that, click **Next**.

The **Online Upgrade** page is displayed.

Figure 1-6 Online upgrade



The 'Online Upgrade' dialog box has a title bar with the text 'Online Upgrade'. Inside, there is a checked checkbox labeled 'Auto-check for updates'. Below this, a paragraph states: 'Automatically notify me when updates are available. The system checks for updates daily.' Another paragraph follows: 'To inform you of the latest firmware upgrades for your device, we need to collect device info such as IP address, device name, firmware version, device SN, etc. All collected info is used only for the purposes of verifying device validity and pushing upgrade notifications.' At the bottom center is a 'Next' button.

Step 8 Select **Auto-check for updates** checkbox.

After the function is enabled, the Device will check for updates once a day automatically. There will be system notice if any update is available.

Step 9 Click **Next**, and the login page is displayed.

Figure 1-7 Login page



The login page features the 'alhua TECHNOLOGY' logo and a camera lens icon at the top. It contains two input fields: 'Username:' and 'Password:'. The 'Password:' field has a small icon for password visibility. To the right of the password field is a link that says 'Forgot password?'. At the bottom are two buttons: 'Login' and 'Cancel'.

1.2.2 First-time Login

Background Information

You need to download and install the plug-in for the first-time login.

Procedure

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

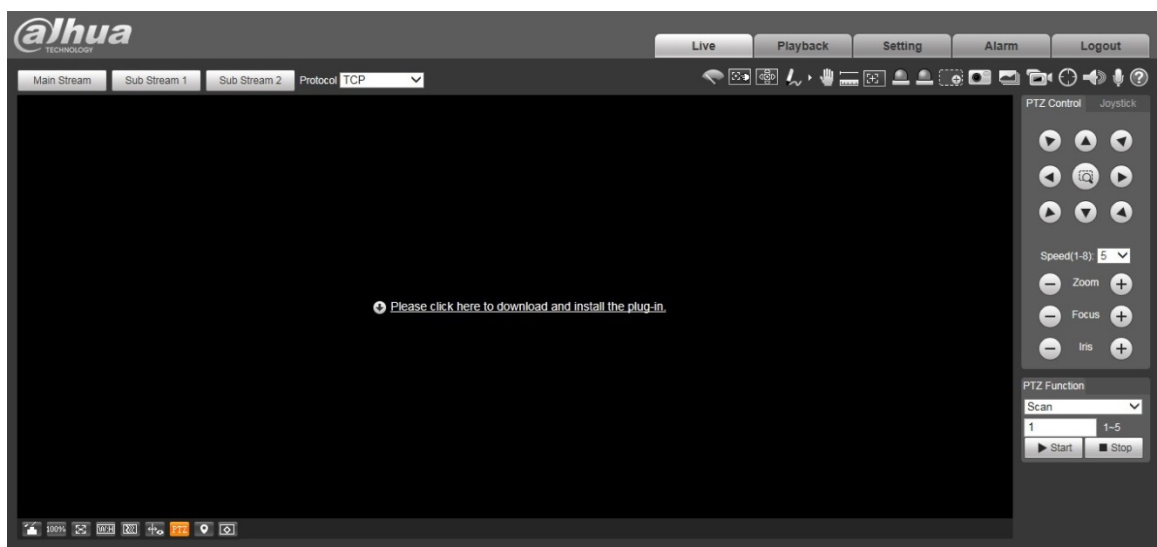
Step 2 Enter the username and password, and then click **Login**.



- If you enter the wrong password for 5 times, the account will be locked for 5 minutes. After the locked time, you can log in to the webpage again.
- You can set the number of allowed password attempts and locked time in "5.5.12.3 Illegal Access".

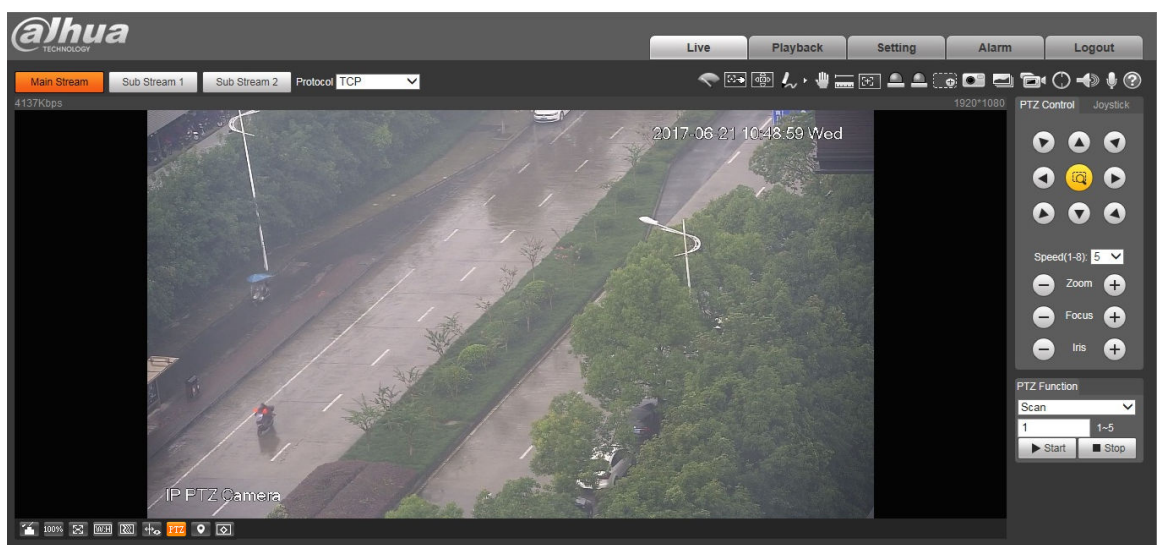
Step 3 Download and install the plug-in according to the on-screen instruction after logging in to the webpage.

Figure 1-8 Install the plug-in



Step 4 After the plug-in is installed, the webpage will be refreshed automatically, and the video is displayed on the **Live** page.

Figure 1-9 Live page





The **Live** page shown in the manual is for reference only, and functions might be different depending on the model.

1.2.3 Device Login

Procedure

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

Figure 1-10 Device login



- Step 2 Enter the username and password, and then click **Login**.

The video is displayed on the **Live** page.



- If you enter the wrong password for 5 times, the account will be locked for 5 minutes. After the locked time, you can log in to the webpage again.
- You can set the number of allowed password attempts and locked time. For details, see "5.5.12.3 Illegal Access".

1.2.4 Resetting Password

Background Information

If you forget the password of the admin user, you can set the password through the provided email address.



Before resetting the password, you need to provide the email address in advance. For details, see "1.2.1 Device Initialization" or "5.7.3.2 System Service".

Procedure

- Step 1** Open the browser, enter the IP address of the Device in the address bar, and then press Enter.

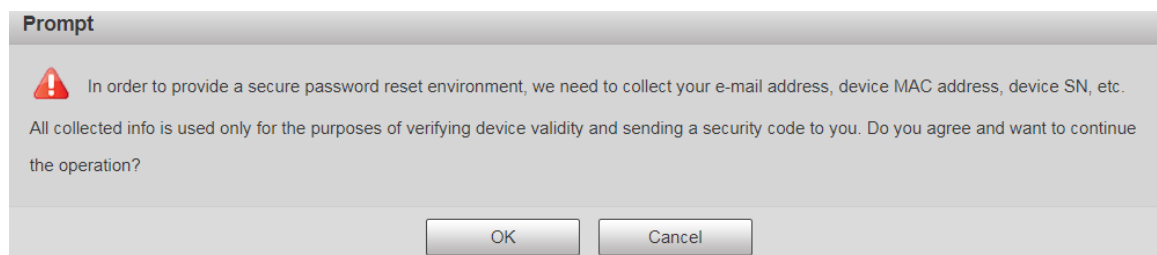
The **Login** page is displayed.

Figure 1-11 Login



- Step 2** Click **Forgot password?**, and the **Prompt** page is displayed.

Figure 1-12 Prompt



- Step 3** Click **OK** to reset the password.

The **Reset the password (1/2)** page is displayed.



If you click **OK**, your email address, MAC address, device serial number, and other information might be collected.

Figure 1-13 Reset the password (1)



Reset the password(1/2)

SN: 51-00000000000000000000

QR code:

Scan the QR code on the actual interface.

Note(For admin only):

Option 1. Please download DMSS and then from More-Reset Device Password, scan the left QR code.

Option 2. Please use an APP to scan the left QR code to get encryption strings. And then send the strings to support_pwd@global.dahuatech.com.

The security code will be delivered to 17702000000000000000

Security code:

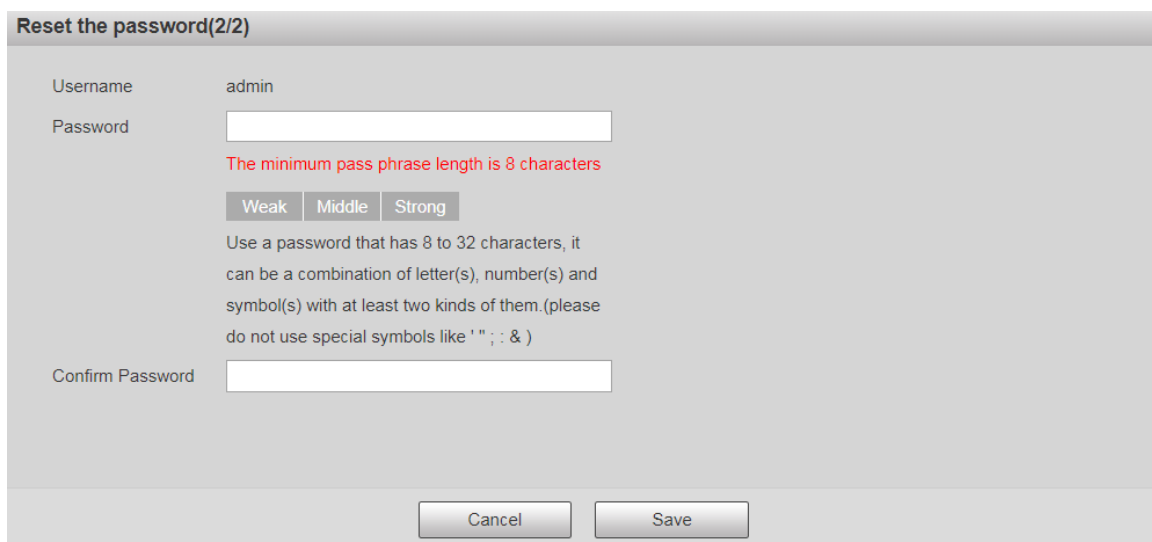
- Step 4** Scan the QR code on the actual page according to the instructions, and then enter the security code received in the mailbox.



Reset the password with the security code you received within 24 hours, otherwise the code will be invalid.

- Step 5** Click **Next**.
The **Reset the password (2/2)** page is displayed.

Figure 1-14 Reset the password (2)



Reset the password(2/2)

Username: admin

Password:

The minimum pass phrase length is 8 characters

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:

- Step 6** Set the password of the admin user again.



The password should consist of 8 to 32 non-blank characters and contain at least two types of characters among upper case, lower case, number, and special characters (excluding ' " ; : &). Set a high security password according to the prompt of password strength.

Step 7 Click **Save**.

2 Live

Click the **Live** tab, and the **Live** page is displayed.

Figure 2-1 Live page

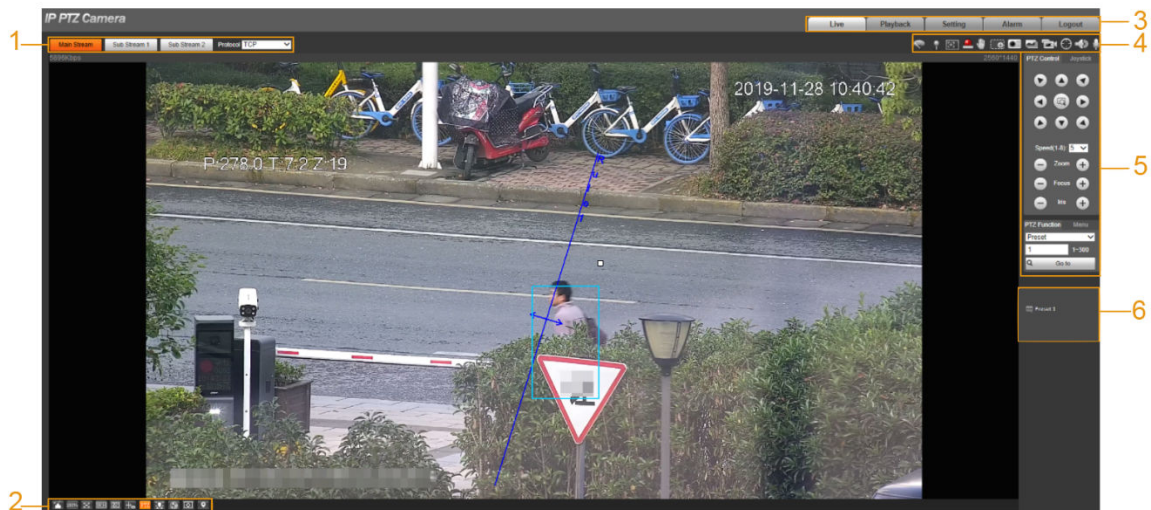


Table 2-1 Function bars description

No.	Description
1	Encoding setting
2	Video window adjustment
3	System menu
4	Video window functions
5	PTZ configuration
6	PTZ status

2.1 Encoding Setting

Click , and then select the stream as needed.



Some devices do not support two sub streams.

Figure 2-2 Encoding setting



Table 2-2 Description of encoding setting parameter

Parameter	Description
Main Stream	It has large bit stream value and image with high resolution, but requires large bandwidth. This option can be used for storage and monitoring.

Parameter	Description
Sub Stream 1	It has small bit stream value and smooth image, and requires little bandwidth. This option is normally used to replace main stream when bandwidth is not enough.
Sub Stream 2	
Protocol	Select a protocol for video monitoring. The supported protocols include TCP (Transmission Control Protocol), UDP (User Datagram Protocol), and Multicast .

2.2 Video Window Adjustment

This section introduces the adjustment of video window.

Figure 2-3 Video window adjustment

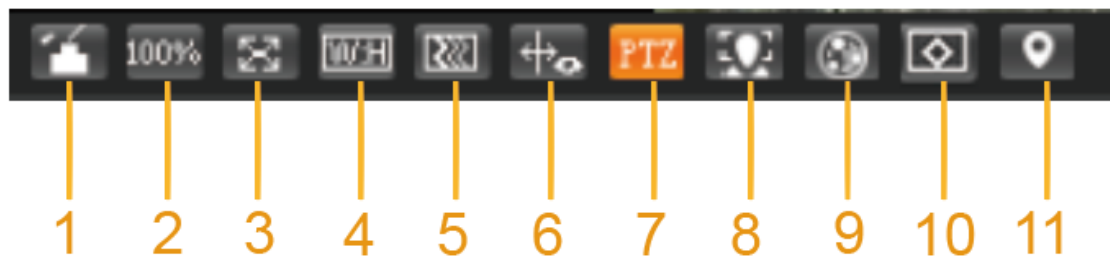


Table 2-3 Description of Video window adjustment parameter

No.	Parameter	Description
1	Image Adjustment	Click this button, and the Image Adjustment page is displayed on the right side of the Live page. You can adjust parameters such as brightness, contrast, hue, and saturation on the page.
2	Original Size	Adjust the video image to original size.
3	Full Screen	Click this button, and the video is displayed in full screen. To exit full screen, double-click the screen or press the Esc key.
4	W:H	Adjust the video image to original ratio or a proper window.
5	Fluency	Click this button, and you can select Realtime , General , or Fluent . General is selected by default.
6	Rules Info	Click this button, and smart rules are displayed on the Live page after the function is enabled. The function is enabled by default.
7	PTZ	Click this button, and PTZ configurations are displayed on the Live page after the function is enabled.
8	Face	Click this button, and images are displayed on the screen. See Figure 2-8.
9	Video Metadata	Click this button, and information about motor vehicles, non-motor vehicles, and people is displayed on the screen in real time. See Figure 2-11.

No.	Parameter	Description
10	Anti-aliasing	Click this button to enable anti-aliasing, and then aliasing can be avoided when video windows are small.
11	Panorama	Click this button, and a panorama window is displayed on the Live page. You can perform operations such as positioning, calling presets, and setting tours.

Image Adjustment

This section introduces the adjustment of image.

Figure 2-4 Image adjustment

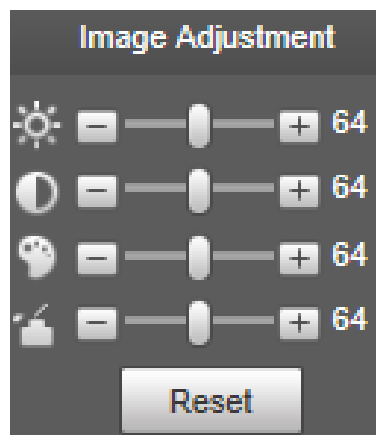







Table 2-4 Image adjustment parameter description

Parameter	Description
	Adjust the image brightness.
	Adjust the image contrast.
	Adjust the image hue.
	Adjust the image saturation.
	Restore brightness, contrast, saturation and hue to default values.



Only brightness, contrast, hue, and saturation of live view image on the web page can be adjusted with this function. To adjust the brightness, contrast, hue, and saturation of the Device, you can go to **Setting > Camera > Conditions**.

Panorama

Figure 2-5 Panorama page





- You can perform positioning in this window by drawing a box with the left mouse button. The located area is displayed on the **Live** page and enlarged.
- After you click **Refresh**, the Device rotates from 0 to 360 degrees horizontally and from 6 to 65 degrees vertically to obtain a new panoramic image.
- You can adjust the size of the panoramic image by dragging the screen ratio bar .
- You can click  to call a corresponding preset on the right side of the window. For how to set a preset, see "5.4.2.1 Preset".

Figure 2-6 Preset




- You can click  to call a corresponding tour on the right side of the window. For how to set a tour, see "5.4.2.2 Tour".

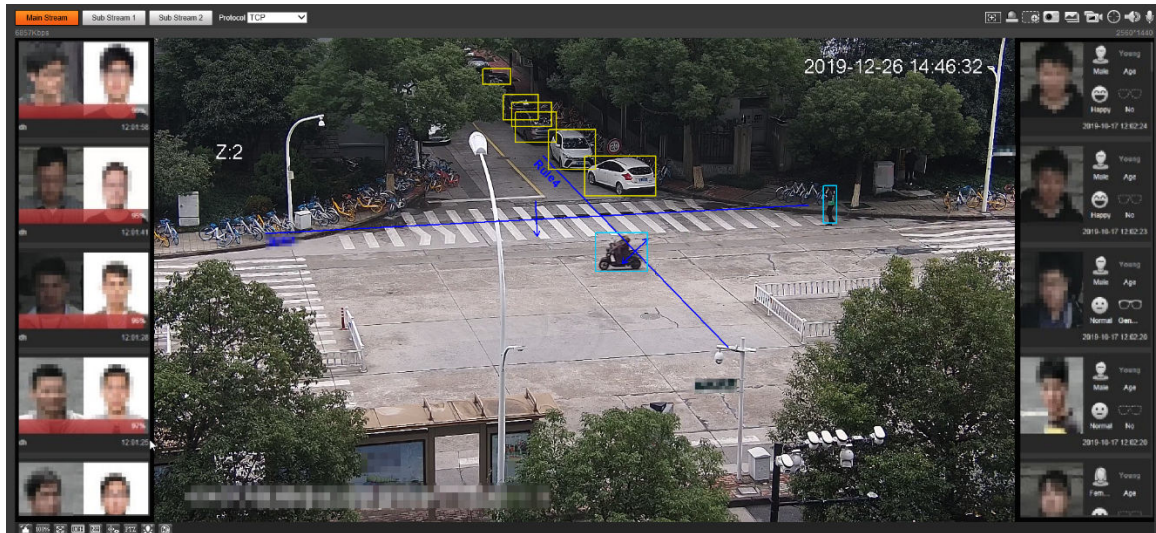
Figure 2-7 Tour



Face

Face recognition result is displayed on the left side, and the captured face image and attributes are displayed on the right side.

Figure 2-8 Face



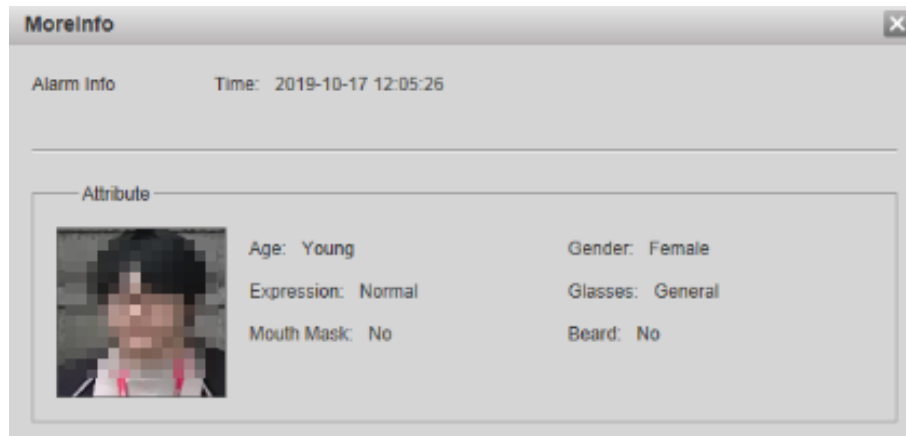
- Face recognition result display area: Displays the captured small face images, the corresponding face images in the database, and the similarities between them. After you click the image the attributes and details are displayed.

Figure 2-9 Face recognition result display



- Face and attributes display area: Displays the captured small face pictures and information such as gender, age, and expression. After you click the picture, the details are displayed.

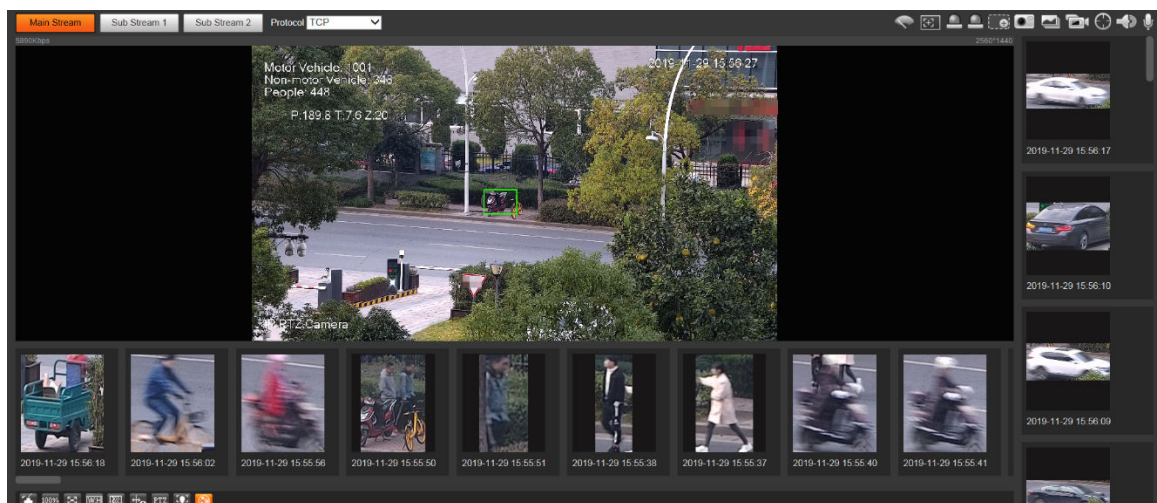
Figure 2-10 Face and attributes display



Video Metadata

Motor vehicle information is displayed on the right side, and the information about human and non-motor vehicles is at the bottom of the page. For details, see "5.5.10 Video Metadata".

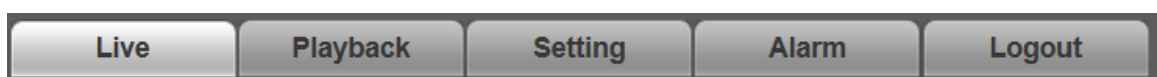
Figure 2-11 Video metadata



2.3 System Menu

To access a page, click the corresponding tab on the system menu.

Figure 2-12 System menu



2.4 Video Window Functions

This section introduces the function of video window.

Figure 2-13 Video window function buttons

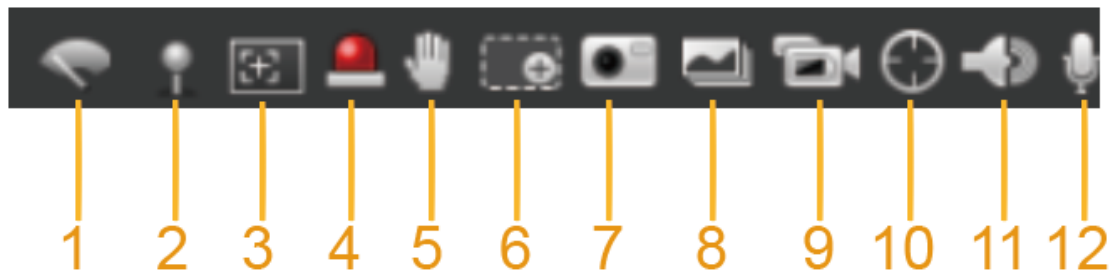


Table 2-5 Description of video window function button

No.	Parameter	Description
1	Wiper Control	<p>Click this button to select wiper operation.</p> <ul style="list-style-type: none"> ● Start : Click this button, and the wiper starts and waves continuously. ● Stop : Click this button, and the wiper is turned off and stops waving. ● Once : Click this button, and the wiper starts and waves from left to right for one time.
2	Mark	<p>Click this button, right-click on the Live page, and the function menu is displayed. See Figure 2-14 . You can add information on the Live page, and also manage added comments.</p> <ul style="list-style-type: none"> ● Add info: Select Add Info from the pop-up menu, and enter the comment. For the page, see Figure 2-15 . ● Manage comments: Select Info Management from the pop-up menu to display, hide, or delete added comments. For the page, see Figure 2-16 .
3	Regional Focus	<p>Click the button, draw a box with the mouse on the live view, and then the Device will automatically focus on the area in the box.</p>
4	Relay-out	<p>Click the button, and an alarm will be triggered. When an alarm is triggered, the icon turns red; and when an alarm is canceled, the icon turns grey.</p>
5	Gesture Control	<p>Click the button, and you can drag the live view by pressing and holding the left mouse button to control PTZ; and you can also zoom in or out through the mouse wheel.</p>
6	Digital Zoom	<ul style="list-style-type: none"> ● Click the button, and then select an area in the live view to zoom in; right-click on the image to restore to the original status. In enlarged status, drag the image to check other area. ● Click the button, and then scroll the mouse wheel in the live view to zoom in or out.
7	Snapshot	<p>Click the button to capture one image of the current image, and it will be saved to the live snapshot storage path set in "5.1.2.5 Path."</p>


No.	Parameter	Description
8	Triple Snapshot	Click the button, and three images of the current image are captured with one snapshot per second. These snapshots will be saved to the live snapshot storage path set in "5.1.2.5 Path."
9	Record	Click the button to record videos. The recording will be saved to the live recording storage path set in "5.1.2.5 Path."
10	Manual Track	Click the button and select any area by dragging the left mouse button in the video window; the Device tracks objects in this area intelligently.
11	Audio	Click the button to enable or disable audio output of the monitoring stream.  Before using the function, you need to enable the audio of the corresponding stream in Setting > Camera > Audio first.
12	Talk	Click the button to enable or disable the two-way audio.

Figure 2-14 Mark—menu

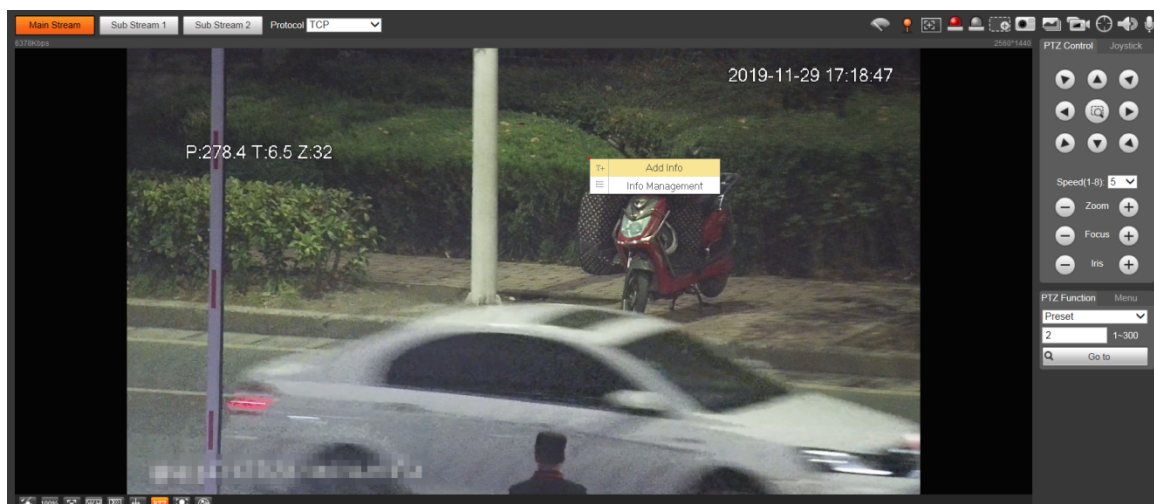


Figure 2-15 Mark—add comments

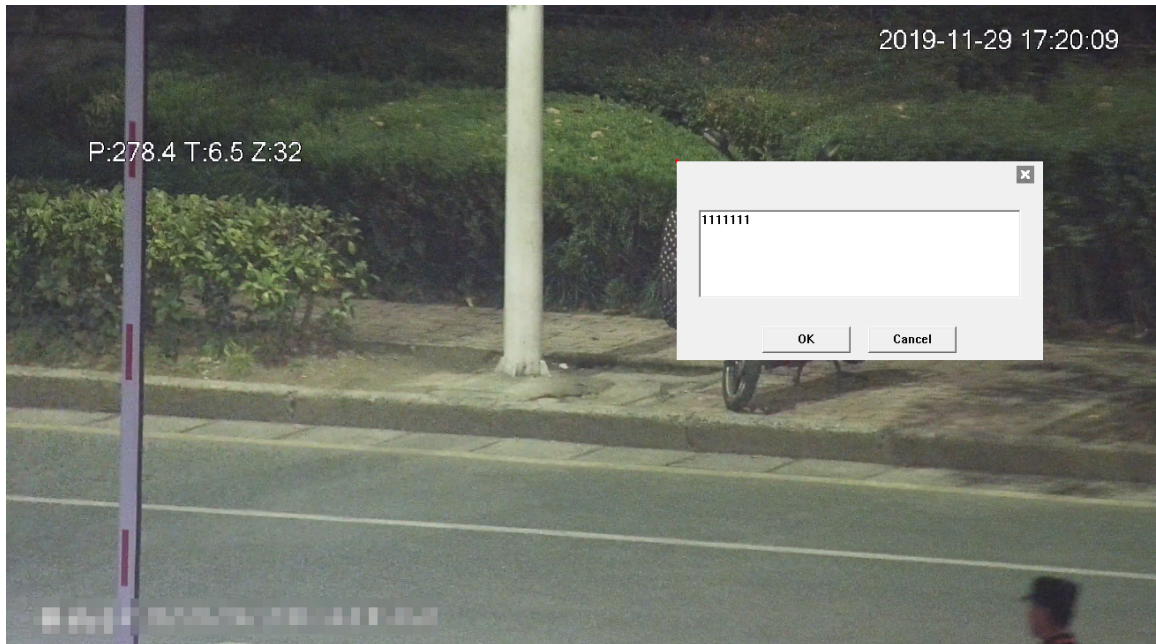
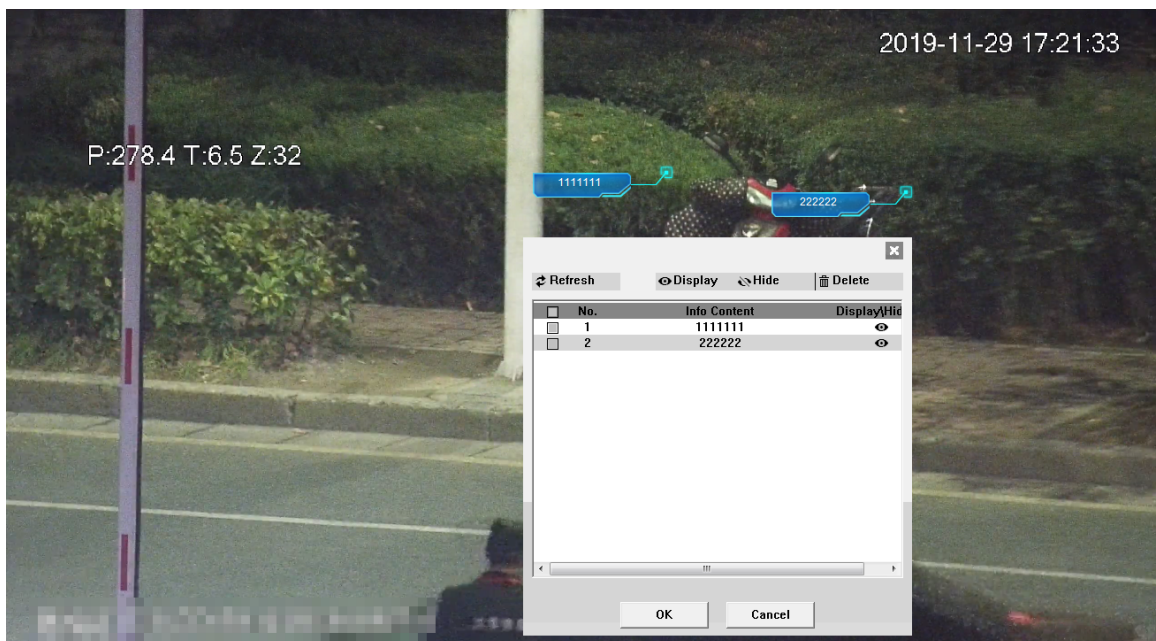


Figure 2-16 Mark—manage comments



2.5 PTZ Configuration

You can control PTZ by using the **PTZ Control** panel or joystick. You can also set preset, scanning, and other functions in the **PTZ Function** area.

PTZ Control



Before using the **PTZ Control** panel, you need to set the PTZ protocol by selecting **Setting > PTZ > Protocol**.

Figure 2-17 PTZ control

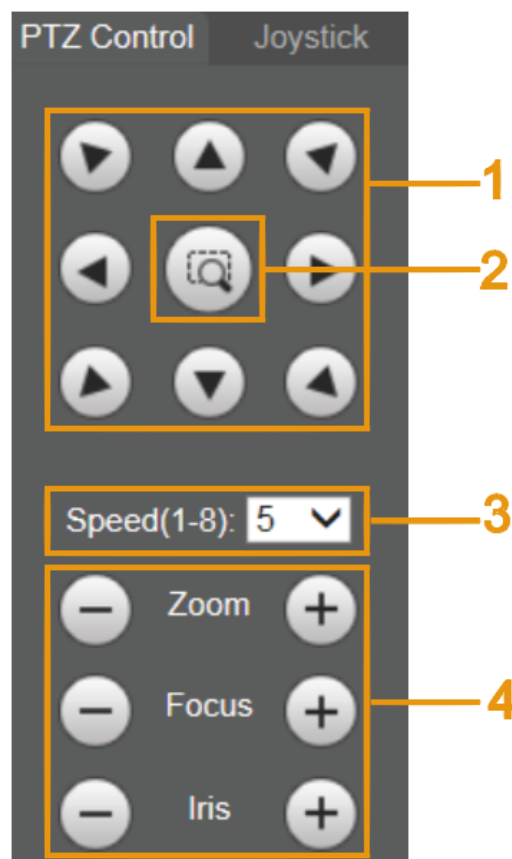




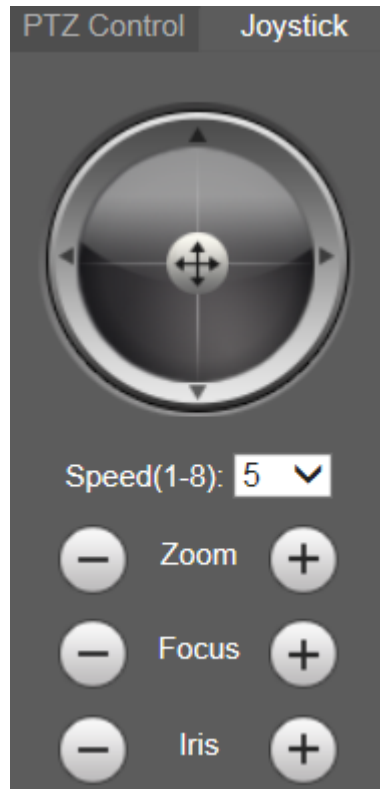
Table 2-6 Description of PTZ control parameter

No.	Parameter	Description
1	Direction Buttons	There are 8 directions: Up, down, left, right, upper left, upper right, lower left, and lower right.
2	Position	Provides quick positioning function. Draw a box in the live view with the mouse, and then the PTZ rotates to and focuses on the selected area rapidly.
3	Speed	The changing speed of PTZ direction. The higher the value, the faster the speed.
4	Zoom/Focus/Iris	Click  to increase the value, and click  to decrease the value.

Joystick

You can drag the middle button to simulate joystick operations to control device rotation. Speed, zoom, focus, and iris configurations are the same as that of **PTZ Control** panel.

Figure 2-18 Joystick



PTZ Functions

The PTZ supports multiple functions. Select a function, click or to start using the function, and then click to stop using the function.

Figure 2-19 PTZ functions

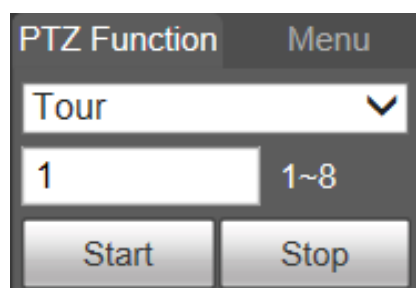



Table 2-7 Description of PTZ function

Parameter	Description
Scan	Select Scan from the list, enter a scan number, and then click Start . The PTZ starts scanning, and the default number is 1.

Parameter	Description
Preset	Select Preset from the list, enter a preset number, and then click Go to . The PTZ will rotate to the preset position.
Tour	Select Tour from the list, enter a tour number, and then click Start . The PTZ starts to tour.
Pattern	Select Pattern from the list, enter a pattern number, and then click Start . The PTZ starts to pattern.
Assistant	Reserved for special requirements.  If necessary, enable this function under the guidance of professionals.
Pan	Select Pan from the list, and then click Start . The PTZ starts to pan.
Go to	<ul style="list-style-type: none"> Select Go to from the list, enter horizontal angle value, vertical angle value and zoom, and then click Go to. The Device will turn to the position you want. One unit of the horizontal angle value or vertical angle value you enter equals 0.1 degree.

Menu

Figure 2-20 Menu page

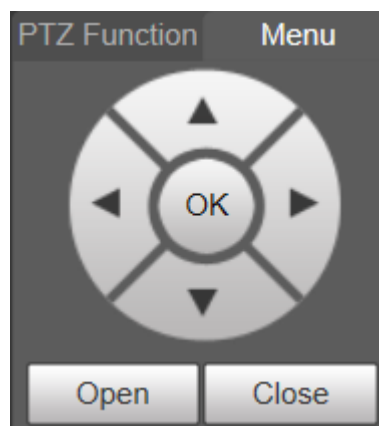
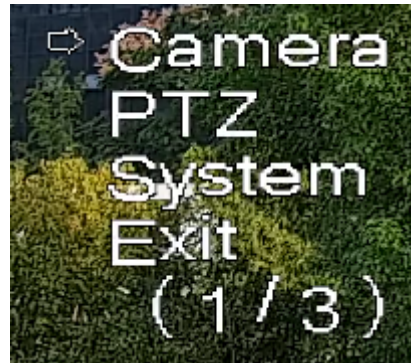


Table 2-8 Description of menu parameter

Parameter	Description
Direction Buttons	Click the up and down buttons to select parameters, and click the left and right buttons to select parameter values.
OK	Confirmation button.
Open	Open the OSD menu.
Close	Close the OSD menu.

Click **Open** to open the OSD menu. The OSD menu is displayed on the live view.

Figure 2-21 OSD menu



You can finish the following settings through the menu.

- Camera settings: For details, see "5.1 Camera".
- PTZ settings: For details, see "5.4 PTZ Settings".
- System management: For details, see "5.7 System Management".

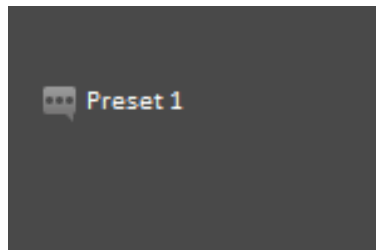
2.6 PTZ Status

On the **Live** page, the PTZ status is displayed at the lower right corner.



The function is available on select models.

Figure 2-22 PTZ status



When the PTZ lifespan is close to the threshold, a warning will be displayed on the **Live** page.

Figure 2-23 Warning (1)

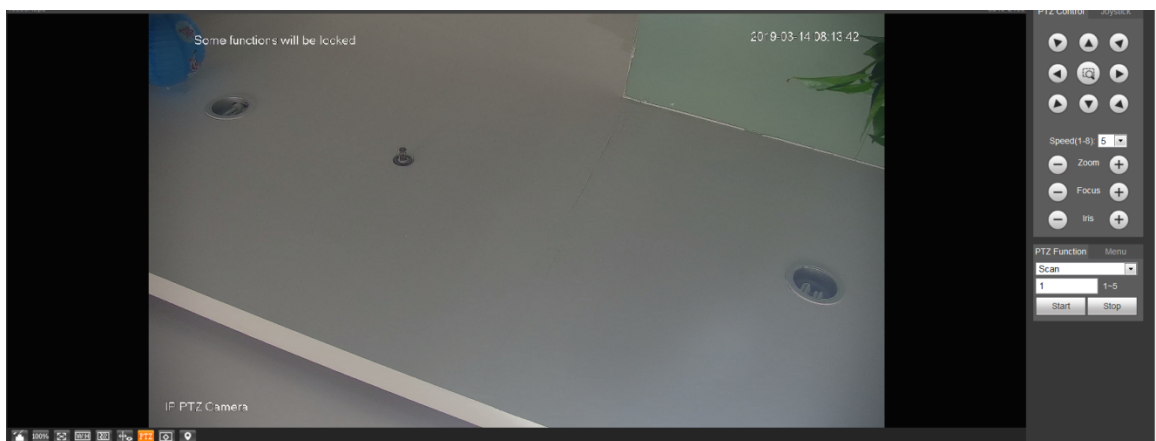


Figure 2-24 Warning (2)



3 AI Live

You can check the information of the detected human faces, human bodies, motor vehicles, and non-motor vehicles.



This function is available on select models.

3.1 AI Live Page

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

Page might vary with different models.

Figure 3-1 AI live page

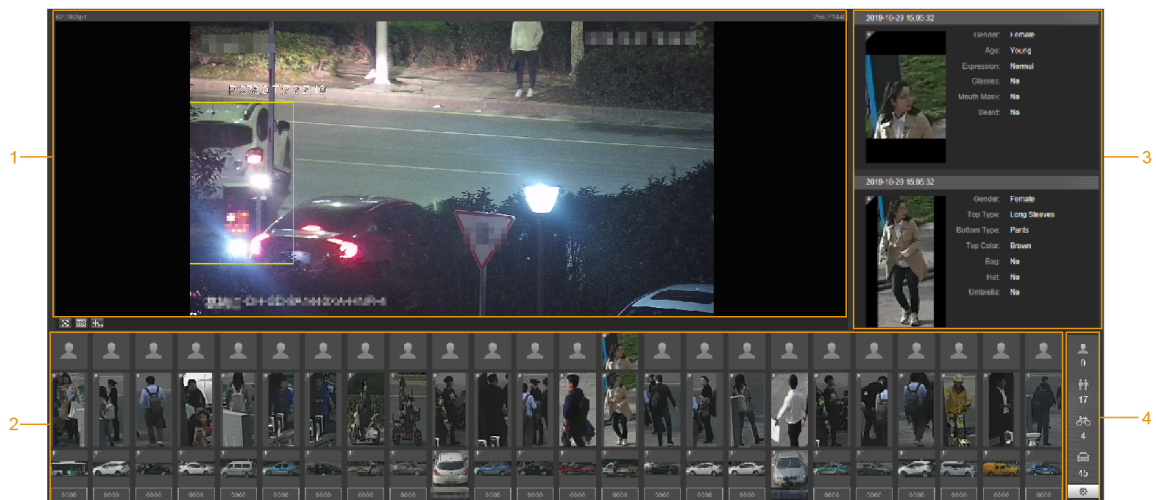


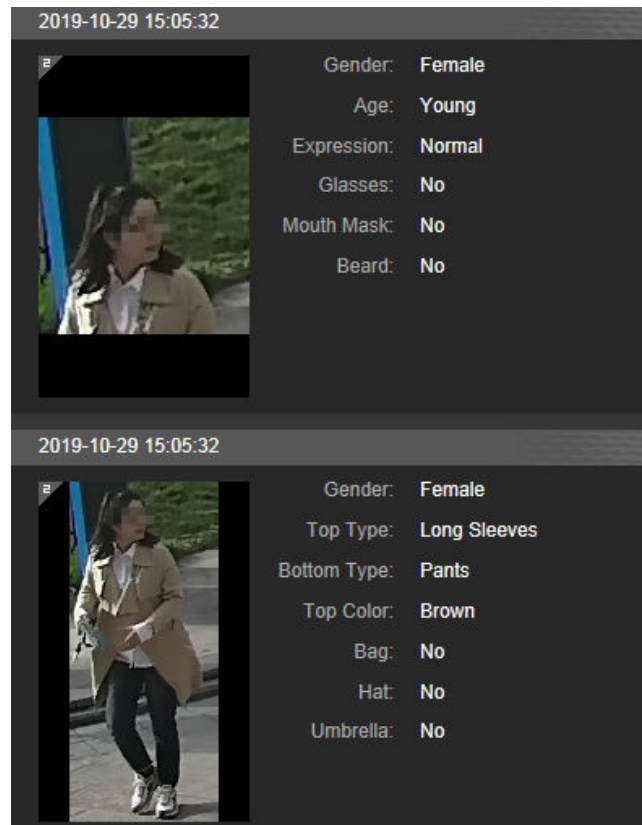
Table 3-1 Description of AI live page

No.	Function
1	Live view
2	Snapshot display area
3	Information display area of detected targets
4	Statistics area of the detected targets

3.1.1 Information Display Area of Detected Targets

This area displays the information of the captured targets in real time.

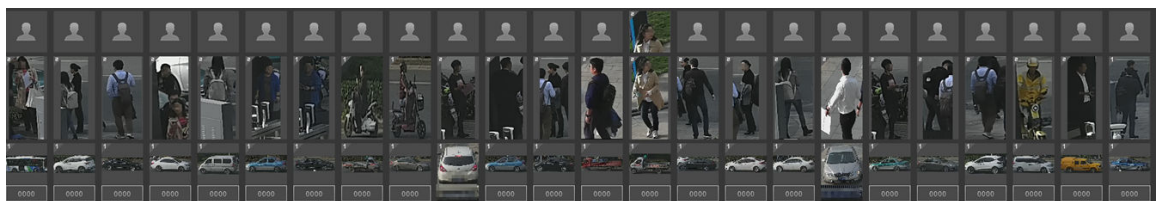
Figure 3-2 Information display of the detected targets



3.1.2 Snapshot Display Area

This area displays the snapshots of the detected targets. Click any snapshot to view the information of the detected target in information display area.

Figure 3-3 Snapshot display area



3.1.3 Statistics Area of the Detected Targets

This area displays the number of the captured target in real time.

Figure 3-4 Statistics area of the detected targets

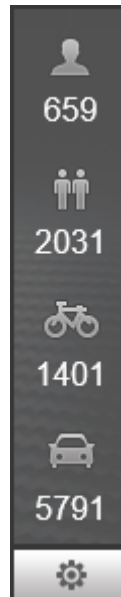








Table 3-2 Statistics area description of the detected targets

Icon	Detected Target	Description
	Face	Available detection items: Gender, age, expression, glasses, mouth mask, and beard.
	Human	Available detection items: Top, bottom, top color, bottom color, bag, hat, and umbrella.
	Non-motor vehicle	Available detection items: Vehicle type, vehicle body color, top, top color, occupancy, and hat.
	Motor vehicle	<p>Available detection items: License plate, vehicle body color, vehicle type, vehicle logo, vehicle series, sunshield, seatbelt, smoking, calling, ornament, and annual inspection mark.</p> <p></p> <p>Up to 7 items can be selected at the same time for motor vehicle detection.</p>
	Settings	Click the button to select the detection items.

3.2 AI Live Settings

Prerequisites

Select **Setting** > **Event** > **Smart Plan**, and then enable **Face Detection**, **Face Recognition** or **Video Metadata**.

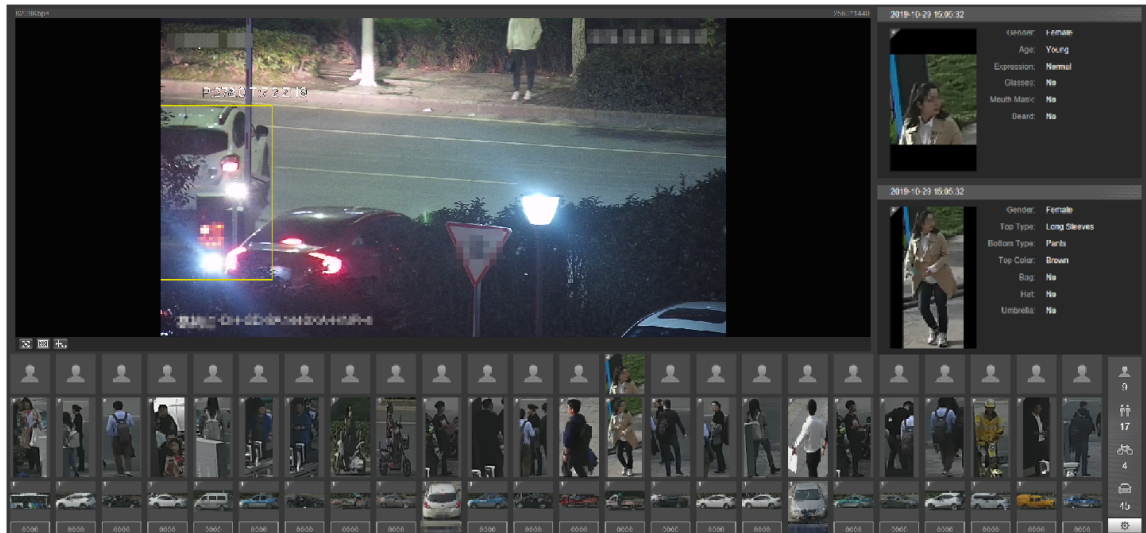
For the method to enable the function, see "5.5.4 Smart Plan". For the operations, see "5.5.7 Face Recognition" or "5.5.10 Video Metadata".

Procedure

Step 1 Click the **AI Live** tab.

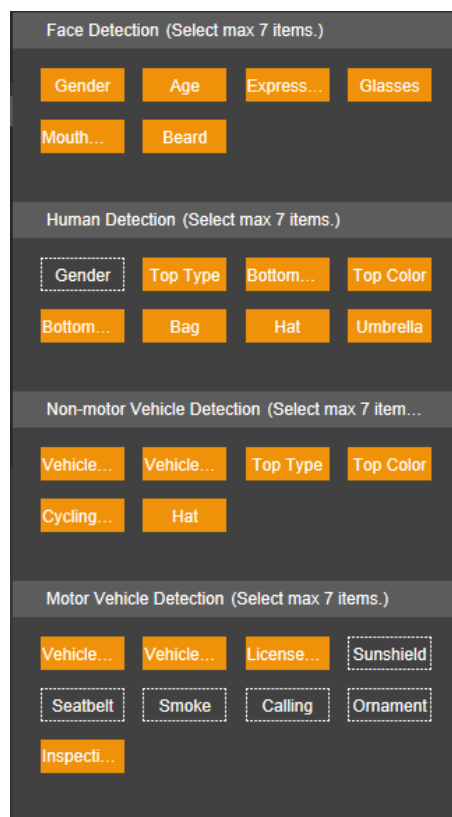
The information display area of detected targets is on the right side; the snapshot display area is on the bottom; the statistics area of the detected targets is on the lower right corner.

Figure 3-5 AI live page



Step 2 Click to set the detection items of the targets.

Figure 3-6 Detection items selection page



Step 3 Click to complete the configuration.

4 Playback

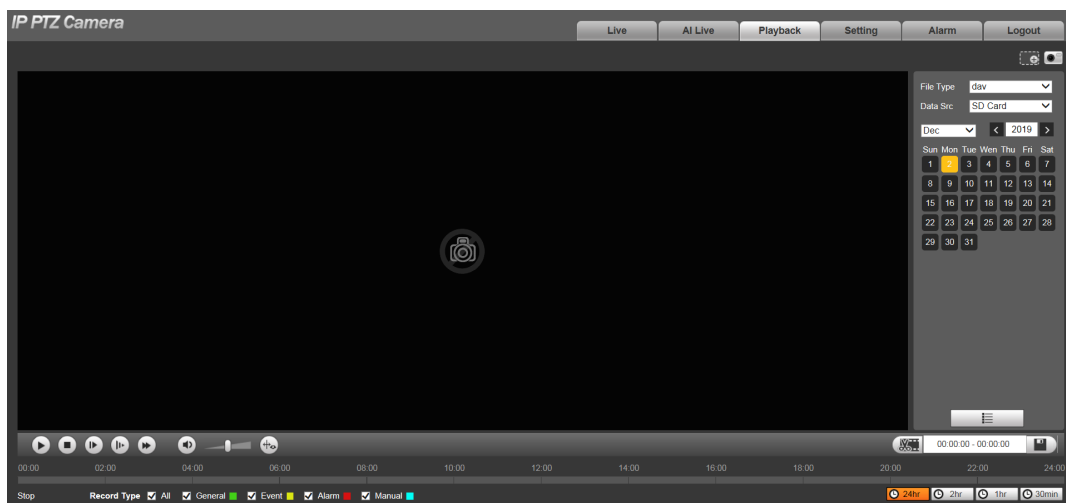
You can view the saved images and videos on the **Playback** page



Before using the function, you need to set the period, storage method, and record control of recording and snapshot first. For details, see "5.6 Storage".

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

Figure 4-1 Playback page



4.1 Video Playback

Select **dav** from the **File Type** list, and the video playback page is displayed.

Figure 4-2 Video playback

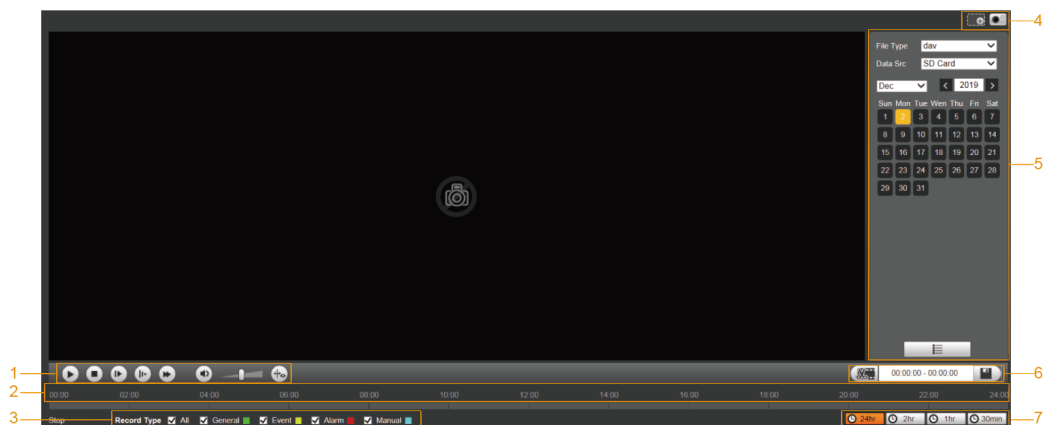


Table 4-1 Description of video playback parameter

No.	Description
1	Video playing function bar

No.	Description
2	Progress bar
3	Recording types
4	Auxiliary functions
5	Video playback file search and display area
6	Video clipping area
7	Progress bar time formats

4.1.1 Video Play Function Bar

This section introduces the function of video play function bar.

Figure 4-3 Video playing function bar

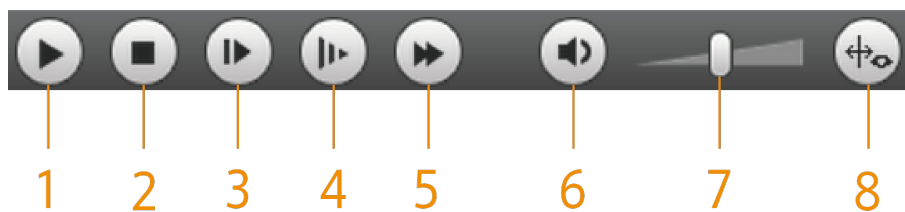



Table 4-2 Description of video play function bar

No.	Parameter	Description
1	Play	Play the video.
2	Stop	Stop playing the video.
3	Next Frame	Play the next frame.  You need to pause the playback before playing the next frame.
4	Slow	Slow down video playing.
5	Fast	Speed up video playing.
6	Sound	Mute or unmute the sound.
7	Volume	Adjust the volume.
8	Rules Info	Click this button, and smart rules will be displayed on the video playback page if the smart rules are enabled.

4.1.2 Recording Type

Select a recording type, and then only files of the selected types will be displayed in the progress bar and file list.

Figure 4-4 Recording type



4.1.3 Auxiliary Functions

This section introduces auxiliary function.

Figure 4-5 Auxiliary functions

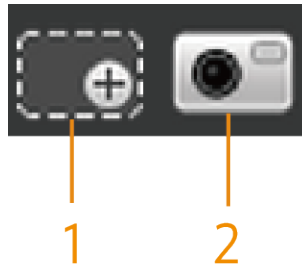


Table 4-3 Description of auxiliary functions parameter

No.	Parameter	Description
1	Digital Zoom	<ul style="list-style-type: none"> Click the button, and then select an area in the live view to zoom in; right-click on the image to restore to the original status. In zoomed-in status, drag the image to check other areas. Click the button, and then scroll the mouse wheel in the live view to zoom in or out.
2	Snapshot	Click the button, and then you can take snapshots of the video in playback, and save them in the playback snapshot path set in "5.1.2.5 Path".

4.1.4 Video Playback File Search and Display Area

Background Information

This section introduces the operation of searching video playback file. There are videos and snapshots on days with blue shading.

Figure 4-6 Playback file (1)

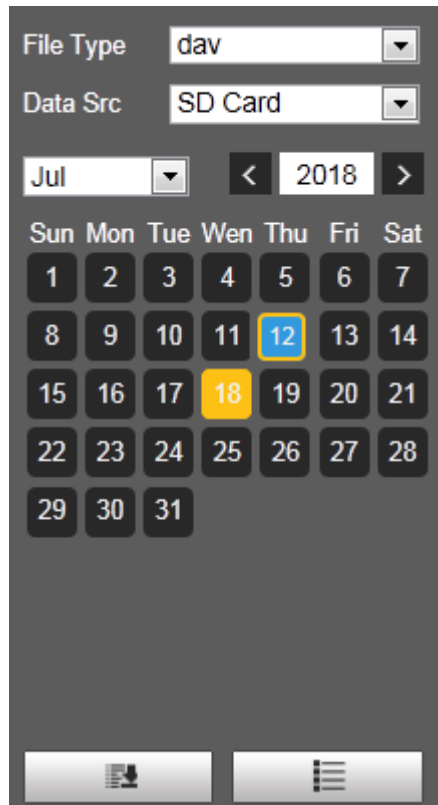





Table 4-4 Description of playback file parameter (1)

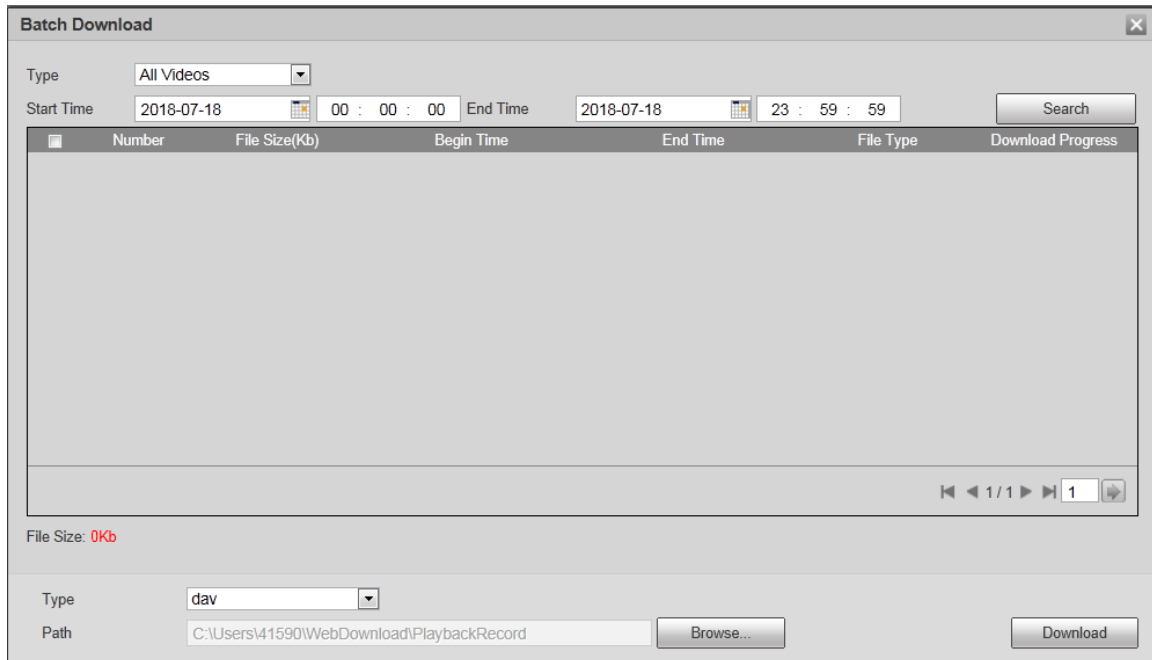
Parameter	Description
File Type	<ul style="list-style-type: none"> To play back a recording, select dav. To play back an image, select jpg.
Data Src	The SD Card is used by default.
	Click this button, and recordings or images of a certain type on specific dates can be downloaded in batches.  The function is available on select models.
	File list. Click this button, and the recording files on the selected day will be displayed in the list.

4.1.4.1 Downloading Files in Batches

Procedure

- Step 1 Click .
- The **Batch Download** page is displayed.

Figure 4-7 Batch download



Step 2 Configure batch download parameters.

Table 4-5 Description of batch download parameter

Parameter	Description
Type	Select the event type that triggers video recording. All Videos , General , Event , Alarm , Manual , and Snapshot are selectable. It is All Videos by default.
Start Time/End Time	Select the start time and end time for video searching.
File Type	Select the video type dav and mp4 are selectable. It is dav by default.
Path	Click Browse , and set the saving path for video files. The default path is C:\Users\admin\WebDownload\PlaybackRecord.

Step 3 Click **Search** to search for the video files that meets the requirements.

Step 4 Select the video, and then click **Download**.

The video files are downloaded and saved in the saving path.



You can select multiple files to download them.

4.1.4.2 Displaying File List

Procedure

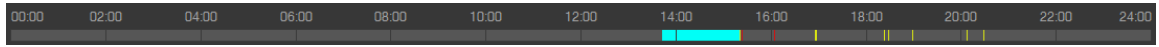
Step 1 Click a day with blue shading, and recording file progress bar with different colors is displayed on the time axis.


- Green: Represents general videos.
- Yellow: Represents motion detection videos.
- Red: Represents alarm videos.

- Blue: Represents manually recorded videos.

Step 2 Click anywhere on the progress bar, and the video will be played from that time.

Figure 4-8 Progress bar



Step 3 Click , and videos recorded on the selected day will be displayed in a list.



To play back a file in the list, double-click the file.

Figure 4-9 Playback file (2)

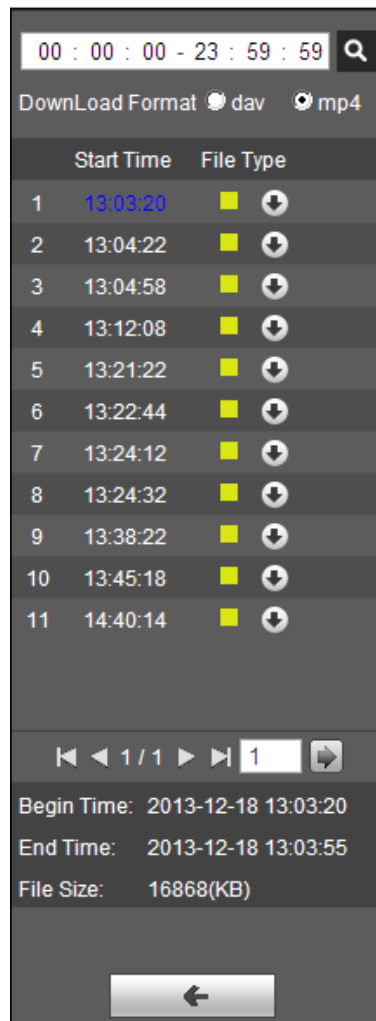






Table 4-6 Description of playback file parameter (2)

Parameter	Description
	Search all the recorded files from the start time to the end time on the selected date.
Download Format	There are two options: dav and mp4 .

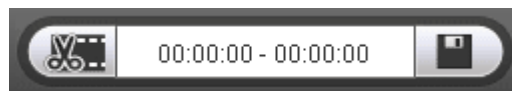
Parameter	Description
	Click the download button, and the files will be saved to the storage path set in "5.1.2.5 Path".  Downloading and playing video at the same time is not supported.
	Click the button to go back to the calendar page.

4.1.5 Video Clipping Area

Background Information


You can clip the videos in this area.


Figure 4-10 Video clipping



Procedure

Step 1 Click the time axis to select the start time for video clipping. The time must be within the progress bar range.


Step 2 Hover over , and then **Select start time** is displayed.


Step 3 Click  to set the start time for video clipping.


Step 4 Click the time axis to select the end time for video clipping.



The time must be within the progress bar range.

Step 5 Hover over , and then **Select end time** is displayed.

Step 6 Click  to set the end time for video clipping.

Step 7 Click , and the clipped video will be saved in the path set in "5.1.2.5 Path".


4.1.6 Progress Bar Time Formats




This section introduces the time format of progress bar.

Figure 4-11 Progress bar time formats



Table 4-7 Description of progress bar time format

Parameter	Description
	Click the button, and then the progress bar displays the recordings in 24-hour mode.

Parameter	Description
	Click the button, and then the video within the selected 2-hour period is displayed.
	Click the button, and then the video within the selected 1-hour period is displayed.
	Click the button, and then the video within the selected 30-minute period is displayed.

4.2 Image Playback

This section introduces the operations of image playback.

Select **jpg** from the **File Type** list.

Figure 4-12 Image playback

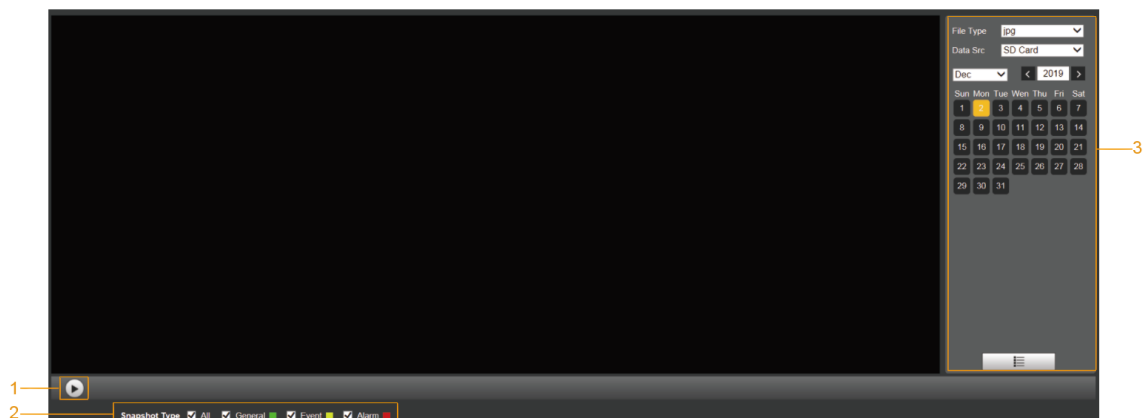


Table 4-8 Description of image playback parameter


No.	Description
1	Image playing functions
2	Snapshot types
3	Image playback file search and display area




4.2.1 Image Playing Functions

This section introduces the function of image playing.

Figure 4-13 Image playing buttons



The status button is displayed as  by default, indicating the image play is paused or no image is being played.

- To play the image, click , and the button is switched to .
- To pause the image play, click .

4.2.2 Image Playback File Search and Display Area

Background Information

This section introduces the operation of searching video playback file. There are videos and snapshots on days with blue shading.

Figure 4-14 Playback file (1)

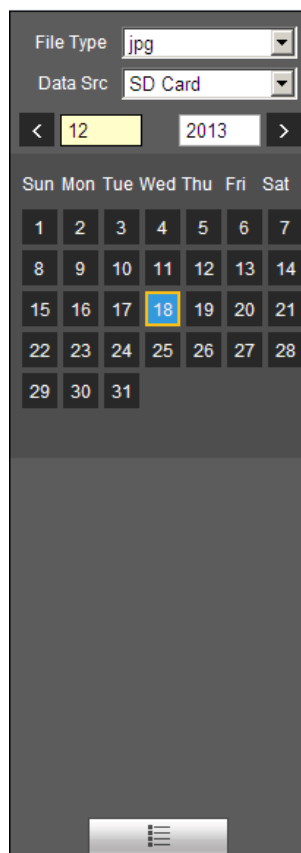


Table 4-9 Description of playback file parameter


Parameter	Description
File Type	Select jpg from the File Type list, and the image will be played in jpg..
Data Src	The SD Card is selected by default.
	File list. Click this button, and the recording files on the selected day will be displayed in the list.

Figure 4-15 Playback file (2)



Procedure





- Step 1** Click , and the snapshots on a selected day will be displayed in a list.
- Step 2** To play back a snapshot, double-click the corresponding file.

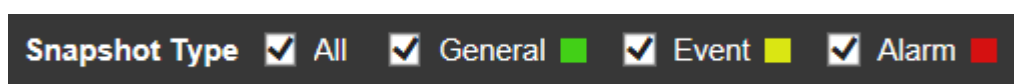
Table 4-10 Description of playback file parameter

Parameter	Description
	Search all the snapshots from the start time to the end time on the selected date.
	Click the button to download the snapshot to local storage.
	Click the button to go back to the calendar page.

4.2.3 Snapshot Types

After you select a snapshot type, only the files of the selected type are displayed in the file list.

Figure 4-16 Snapshot types



5 Setting

5.1 Camera

5.1.1 Conditions Settings

This section describes how to set camera attributes and manage profiles.

5.1.1.1 Conditions

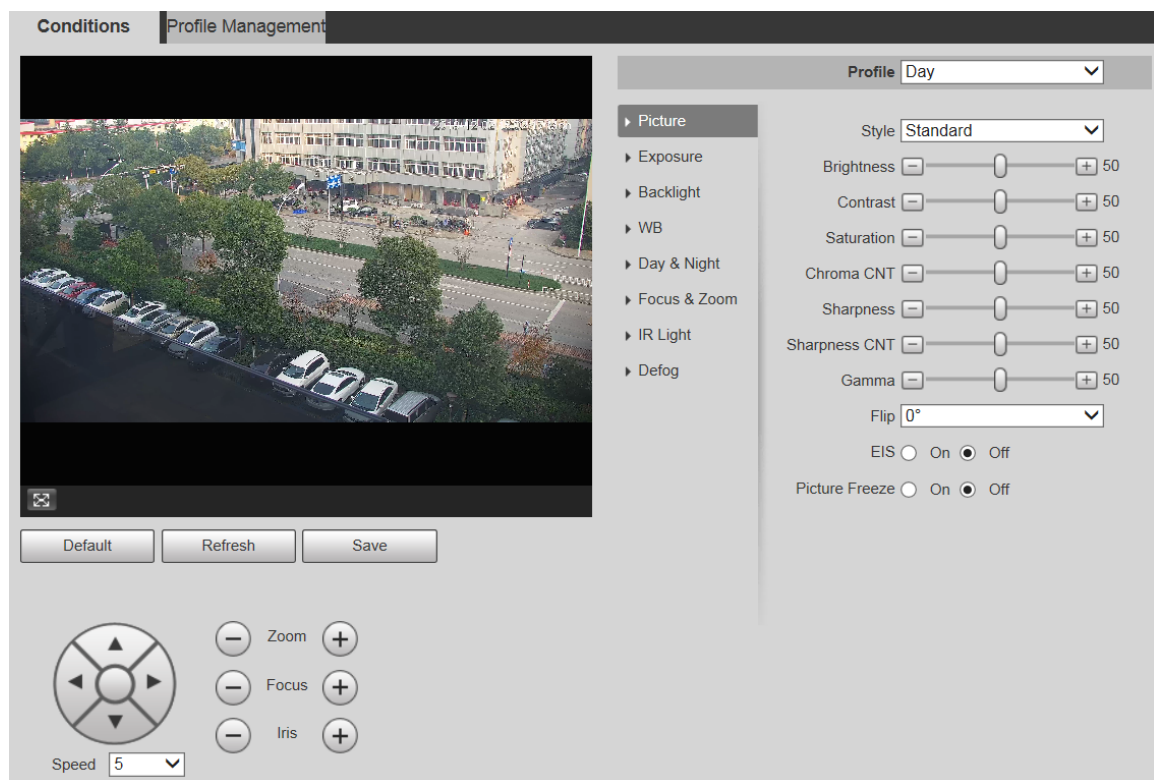
5.1.1.1.1 Picture

You can set camera attributes and picture parameters to achieve the best display effect.

Procedure

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





Figure 5-1 Picture page



Step 2 Configure image setting parameter.

Table 5-1 Description of image setting parameter

Parameter	Description
Profile	There are three options: General , Day , and Night . You can view the configurations and the effect of the selected mode. Day is selected by default.
Style	Set the image display style. There are three options: Soft , Standard , and Vivid . Standard is selected by default.

Parameter	Description
Brightness	Set the overall image brightness. The larger the value is, the brighter the image will be. The value ranges from 0 to 100.
Contrast	Set the image contrast. The larger the value is, the greater the contrast will be. The value ranges from 0 to 100.
Saturation	Set the intensity of colors. The larger the value is, the brighter the colors will be. The value ranges from 0 to 100.
Chroma CNT	<p>The larger the value, the higher suppression on image colors. The value ranges from 0 to 100.</p>  <p>This parameter takes effect only when the Device is in the environment with low luminance.</p>
Sharpness	<p>Set the sharpness of picture edges. The larger the value is, the more obvious the edge will be. The value ranges from 0 to 100.</p>  <p>If the value is too large, there might be image noise. Set the value according to the actual condition.</p>
Sharpness CNT	<p>The larger the value, the stronger the sharpness CNT will be. The value ranges from 0 to 100.</p>  <p>This parameter takes effect only when the Device is in the environment with low luminance.</p>
Gamma	Change image brightness through non-linear tuning to expand the dynamic display range of images. The larger the value is, the brighter the image will be. The value ranges from 0 to 100.
Flip	<p>Monitoring videos can be flipped over. There are two options.</p> <ul style="list-style-type: none"> ● 0° : The monitoring video is normally displayed. It is 0° by default. ● 180° : The monitoring video is flipped over.
EIS	<p>Electronic image stabilization (EIS) is used to effectively solve the problem of image shaking during use, thus presenting clearer images. It is Off by default.</p>  <ul style="list-style-type: none"> ● This function is available on select models. ● This parameter takes effect only when the Device is in the environment with low luminance. ● Optical image stabilization and electronic image stabilization cannot be enabled at the same time.
Picture Freeze	After you select On , the image at the called preset is displayed directly if you call a preset or tour, and no images during the rotation of the Device are displayed.

Step 3 Click **Save**.

5.1.1.1.2 Exposure

You can control the amount of light per unit area reaching the electronic image sensor by adjusting parameters on the **Exposure** page.

Procedure

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

Figure 5-2 Exposure—auto mode

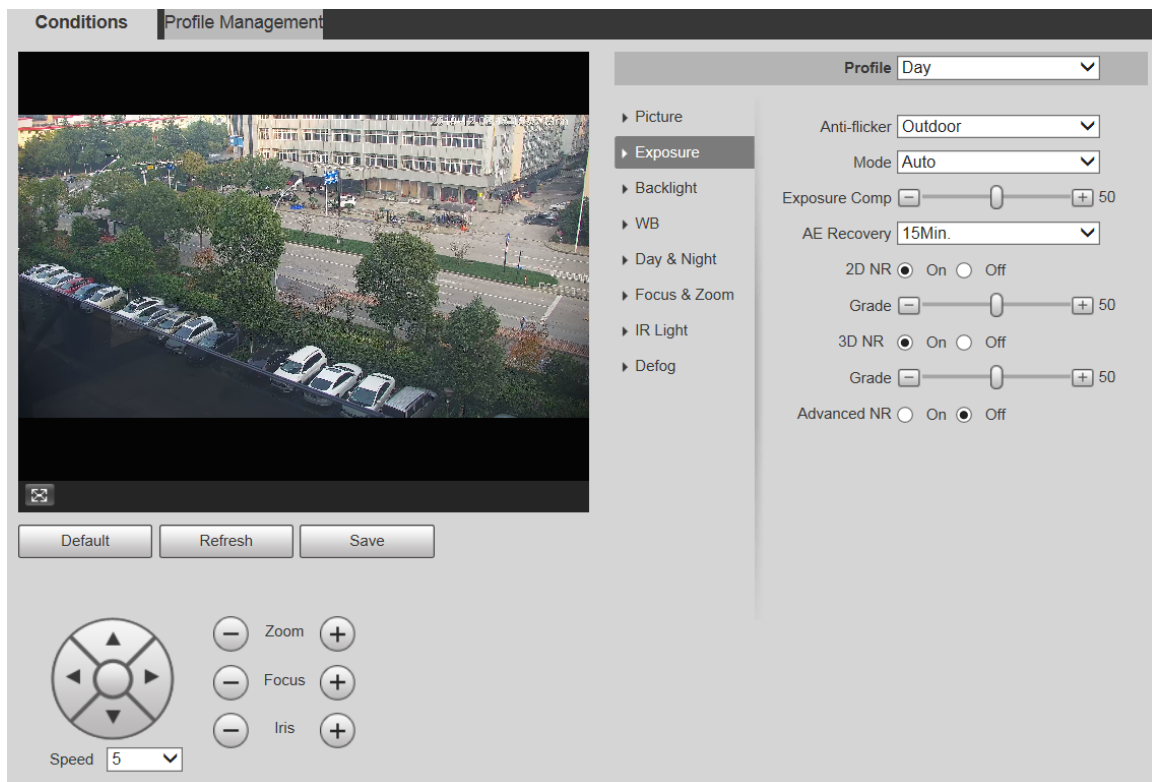


Figure 5-3 Exposure—aperture priority mode

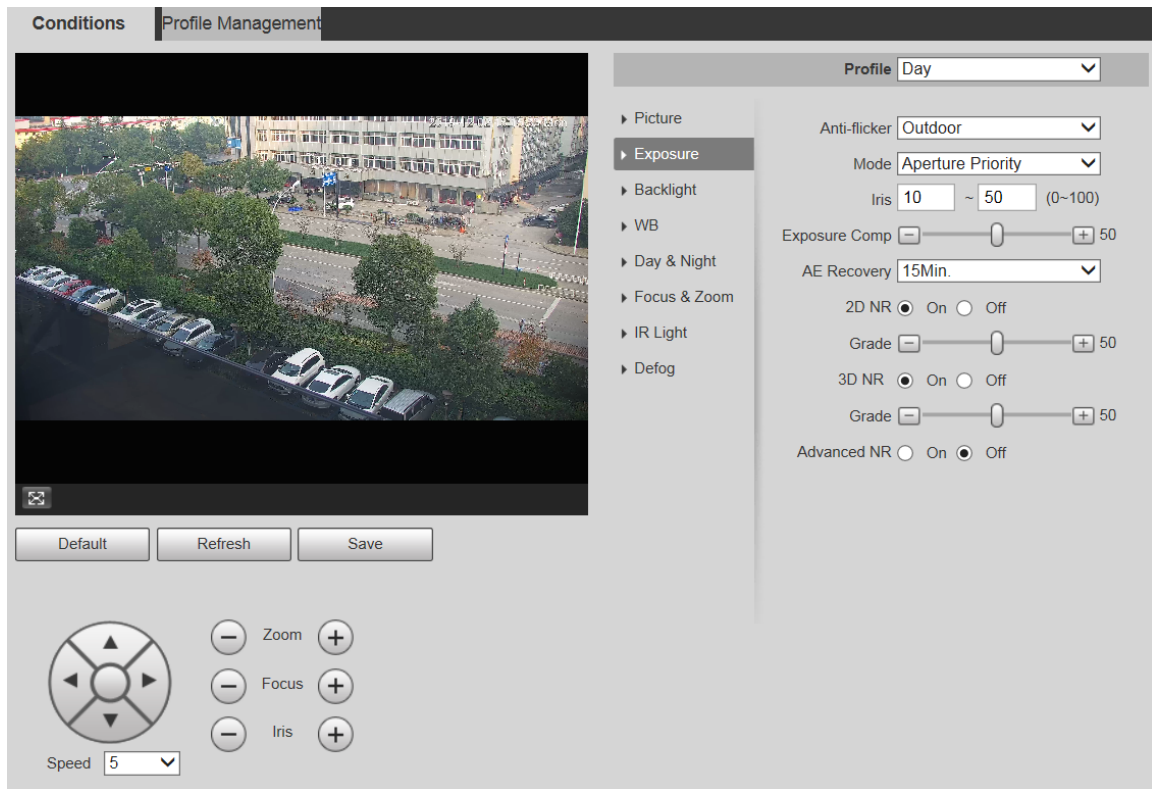


Figure 5-4 Exposure—shutter priority mode

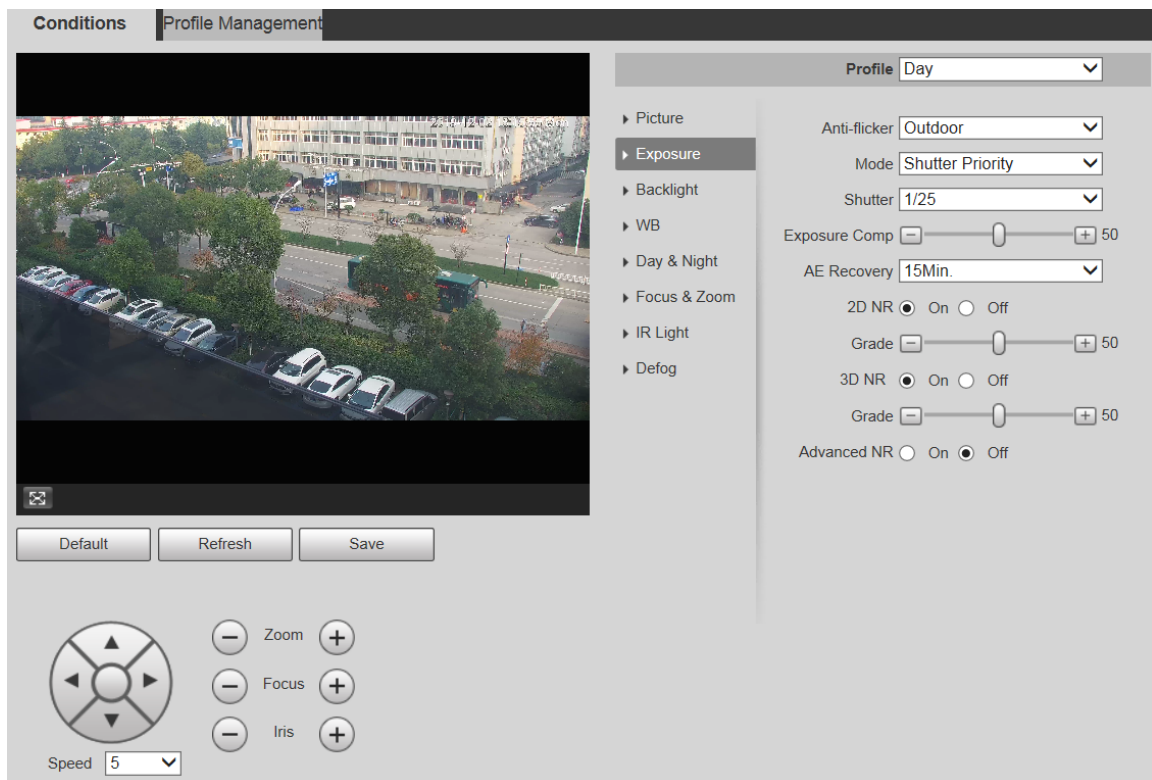


Figure 5-5 Exposure—gain priority mode

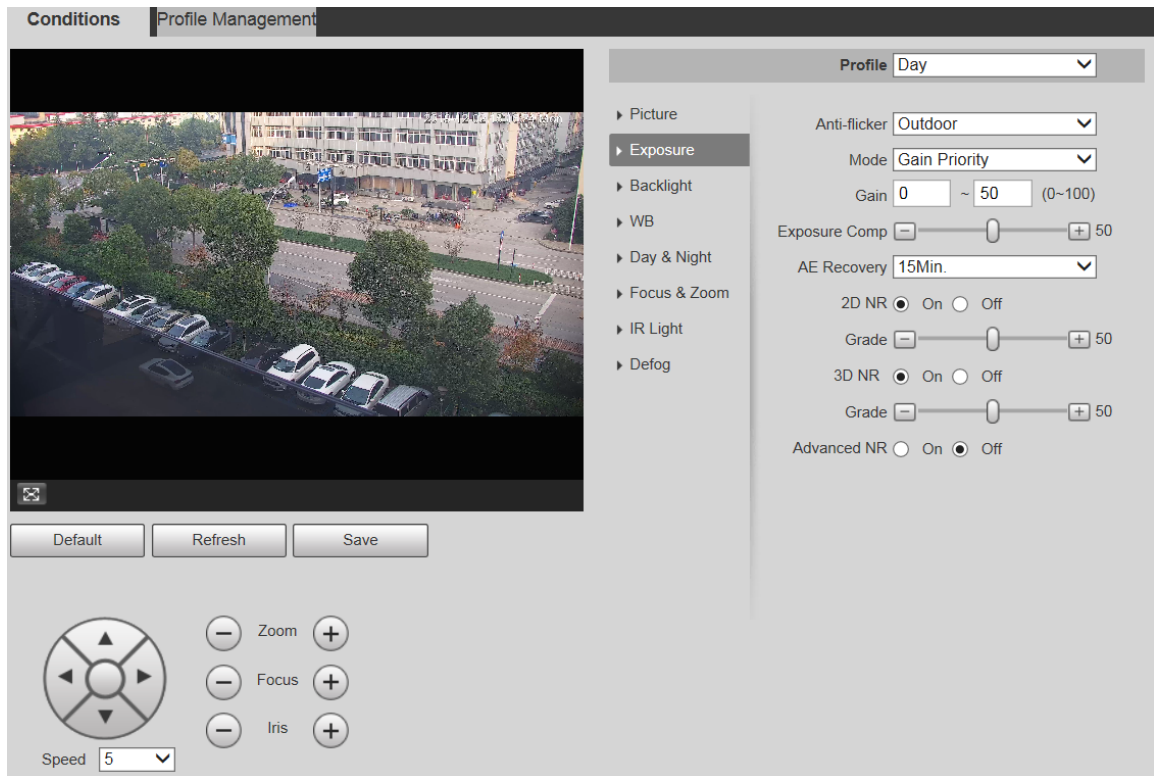
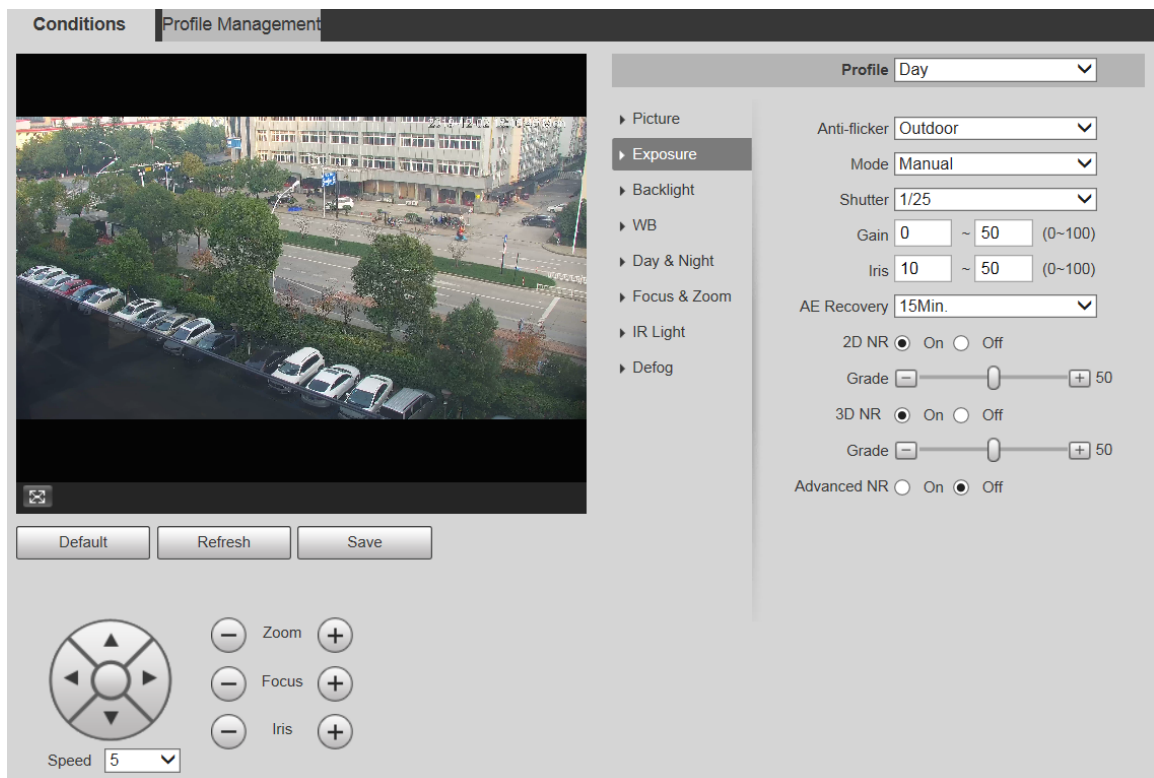



Figure 5-6 Exposure—manual mode



Step 2 Configure exposure setting parameter.

Table 5-2 Description of exposure setting parameter

Parameter	Description
Anti-flicker	<p>You can select 50Hz, 60Hz, or Outdoor from the list.</p> <ul style="list-style-type: none"> • 50Hz : When the alternating current is 50Hz, the exposure is automatically adjusted to make sure that there are no stripes on images. • 60Hz : When the alternating current is 60Hz, the exposure is automatically adjusted to make sure that there are no stripes on images. • Outdoor : You can switch the modes to achieve the effect you want.
Mode	<p>Set the exposure modes. You can select Auto, Manual, Aperture Priority, Shutter Priority, or Gain Priority. The Auto mode is selected by default.</p> <ul style="list-style-type: none"> • Auto : Exposure is automatically adjusted according to scene brightness if the overall brightness of images is in the normal exposure range. • Manual : You can adjust the Gain, Shutter, and Iris value manually. • Aperture Priority : You can set the iris 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 is at ideal brightness. • Shutter Priority : You can customize the shutter range. The Device automatically adjusts the aperture and gain according to the scene brightness. • Gain Priority : Gain value and exposure compensation value can be adjusted manually.
Gain	You can set the exposure gain. The value ranges from 0 to 100.
Shutter	You can adjust the exposure time of the Device. The larger the shutter value, the brighter the image.
Iris	You can set the Device luminous flux. The larger the iris value, the brighter the image.
Exposure Comp	You can set the exposure compensation value. The value ranges from 0 to 100.
AE Recovery	Automatic exposure is an automated digital camera system that adjusts the aperture and shutter speed, based on the external lighting conditions for images and videos. If you have selected an AE Recovery time, the exposure mode will be restored to the previous mode after you adjust the iris value. There are five options: Off , 5Min , 15Min , 1Hour , and 2Hour .
2D NR	2D noise reduction is the process of removing noise from a signal. The higher the grade is, the less the noise will be, and images appear to be blurrier.
3D NR	3D noise reduction is the process of removing noise from a signal. The higher the grade is, the less the noise will be, and images appear to be blurrier.
Grade	Noise reduction grade. The value ranges from 0 to 100. The larger the value is, the less the noise will be.

Parameter	Description
Advanced NR	Realize noise suppression effect through 3D and 2D video filtering method.  The function is available on select models.

Step 3 Click **Save**.

5.1.1.1.3 Backlight

Background Information



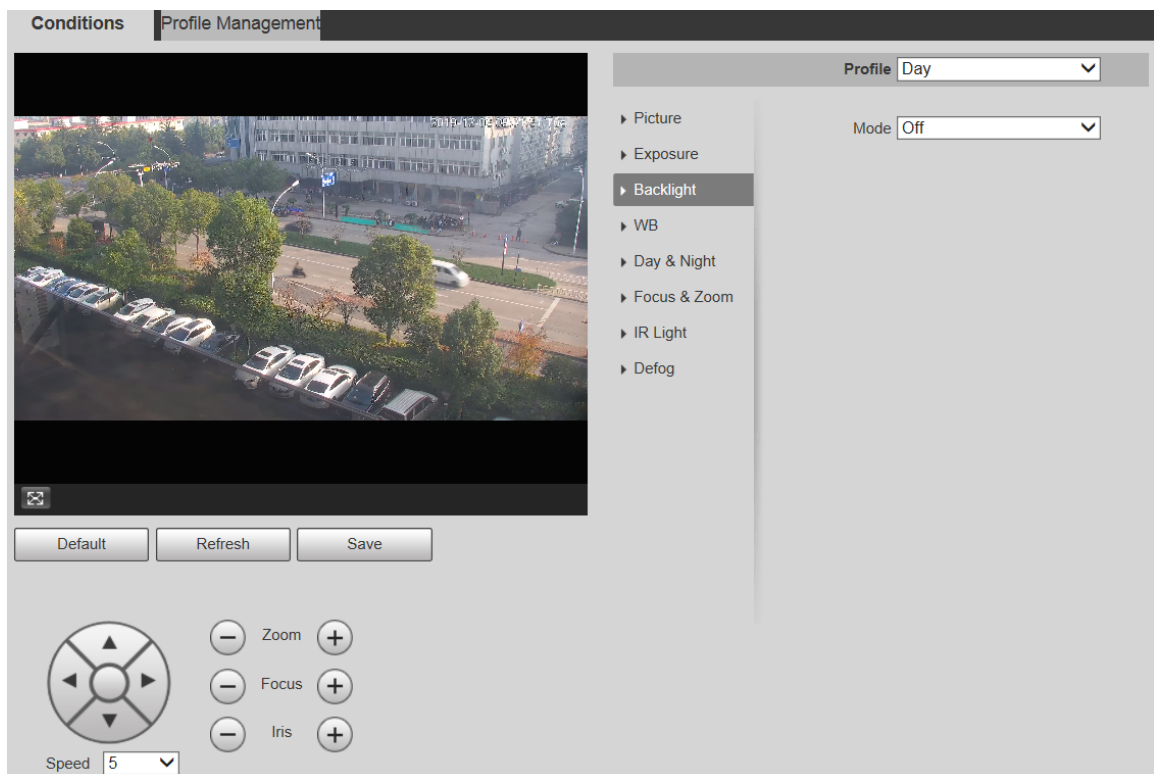
The backlight function cannot be configured if defog function is enabled. There will be a prompt on the page.

You can use this function to adjust the backlight compensation mode of the monitoring screen.

Procedure

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

Figure 5-7 Backlight settings



Step 2 Select a backlight mode from the list.

There are 4 options: **Off**, **BLC**, **HLC**, and **WDR**.

- **Off** : Backlight is disabled.
- **BLC** : Backlight compensation corrects regions with extremely high or low levels of light to maintain a normal and usable level of light for the object in focus.
- **HLC** : Highlight compensation dims strong light, so that the Device can capture details of faces and license plates in extreme light conditions. It is applicable to the entrance and exit of toll stations or parking lots.

- **WDR** : When in WDR (Wide Dynamic Range) mode, the Device constrains over bright areas and compensates dark areas to improve the image clarity.

Step 3 Click **Save**.



If you select **Off**, other backlight mode configurations will not be effective.

5.1.1.1.4 WB

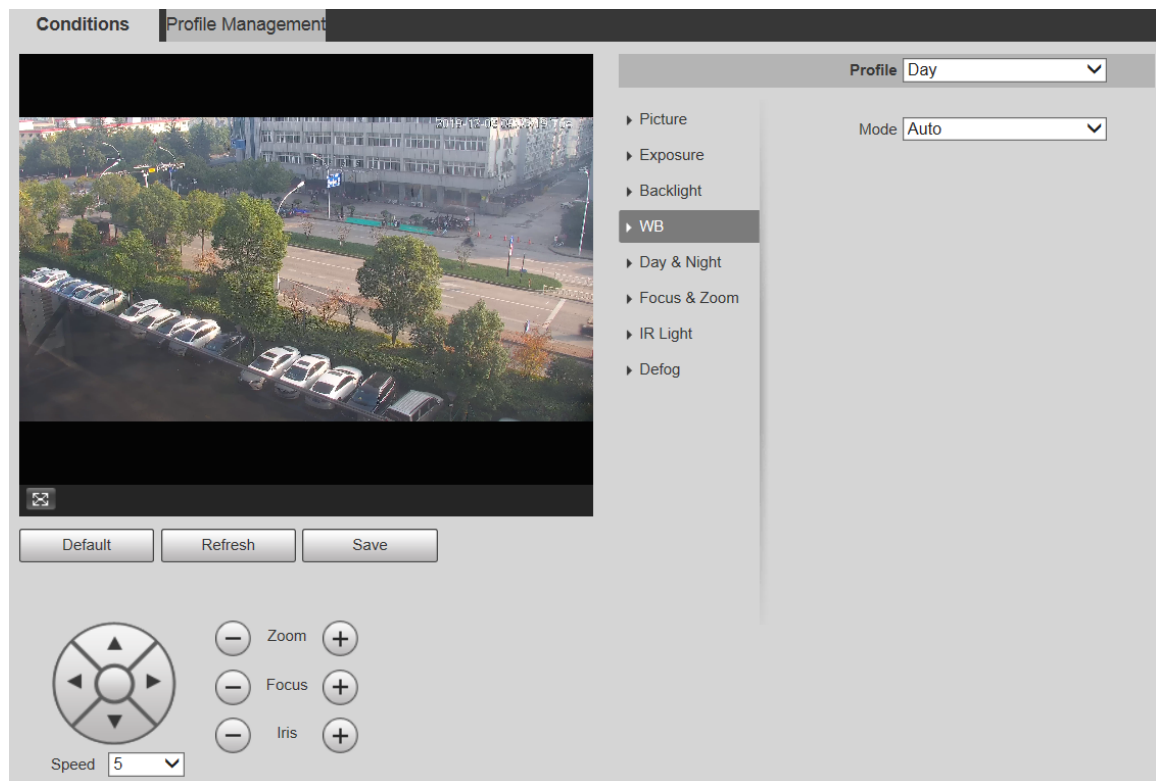
Background Information

In this mode, you can make a white object displaying itself clearly on the video image in all environments.

Procedure

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

Figure 5-8 WB settings



Step 2 Select WB mode from the list.

You can select from **Auto**, **Indoor**, **Outdoor**, **ATW**, **Manual**, **Sodium Lamp**, **Natural**, and **Street Lamp**. **Auto** is selected by default.

Step 3 Click **Save**.

5.1.1.1.5 Day & Night

Background Information

This function allows you to switch between the color mode and the black & white mode, ensuring clear monitoring screen in a dim environment.

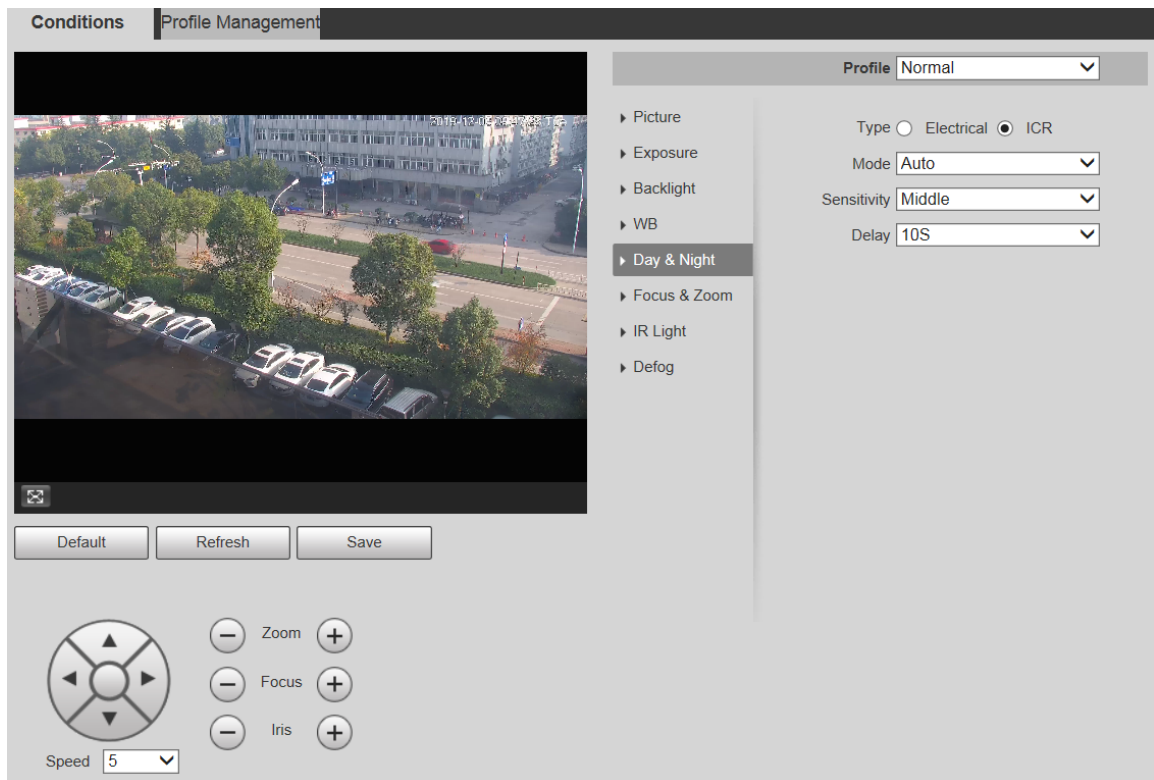


Defog function cannot be configured if **Day & Night** function is enabled. There will be a prompt on the page.

Procedure


Step 1 Select **Setting** > **Camera** > **Conditions** > **Conditions** > **Day & Night**.


Figure 5-9 Day & night settings



Step 2 Configure day & night parameter.

Table 5-3 Description of day & night parameter

Parameter	Description
Type	There are two options: Electrical and ICR . ICR is selected by default. <ul style="list-style-type: none"> ● Electrical Image processing method is used for day & night switch. ● ICR : IR filter is used for day & night switch.
Mode	Select a mode from the list (Your selection is independent from the profile). Auto is selected by default. <ul style="list-style-type: none"> ● Color : The Device only outputs color images. ● Auto : The Device outputs color images or black-and-white images according to ambient conditions. ● B/W : The Device only outputs black-and-white images.
Sensitivity	Adjust the sensitivity to switch between different modes. There are three options: Low , Middle , and High . <div>  <p>You can set sensitivity only when Day & Night mode is set to Auto.</p> </div>

Parameter	Description
Delay	Adjust the delay time to switch between different modes. The value ranges from 2 s to 10 s.  You can set Delay only when Day & Night mode is set to Auto .

Step 3 Click **Save**.

5.1.1.1.6 Focus & Zoom

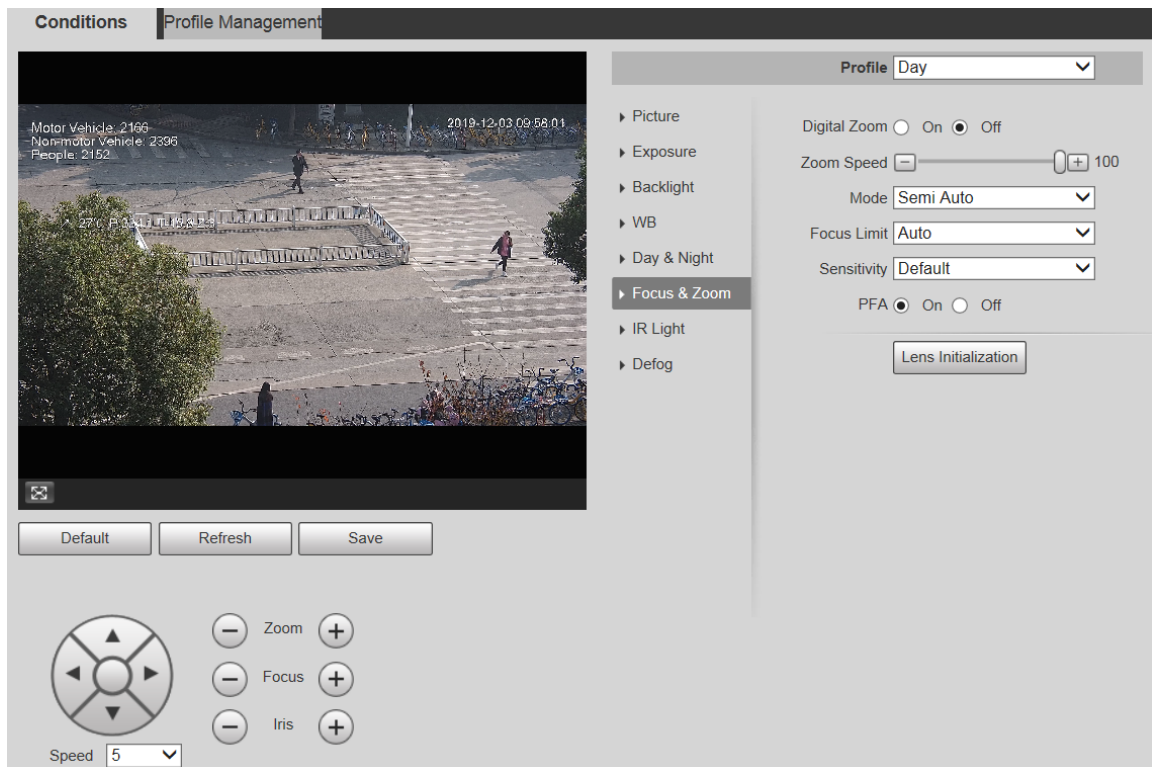
Background Information

Digital zoom refers to capturing a part of the image to magnify it. The higher the magnification is, the blurrier the images will become.

Procedure

Step 1 Select **Setting** > **Camera** > **Conditions** > **Conditions** > **Focus & Zoom**.

Figure 5-10 Focus & zoom settings



Step 2 Configure focus & zoom parameter.

Table 5-4 Description of focus & zoom parameter

Parameter	Description
Digital Zoom	Select On or Off to enable or disable digital zoom. Off is selected by default.
Zoom Speed	The larger the value is, the faster the Device zooms.

Parameter	Description
Mode	<p>Select the focus triggering mode. There are three options: Semi Auto , Auto, and Manual. Semi Auto is selected by default.</p> <ul style="list-style-type: none"> ● Semi Auto : The Device focuses automatically when zoom or ICR switch is detected. ● Auto : The Device focuses automatically when scene changes, zoom, or ICR switch are detected. ● Manual : The Device cannot focus automatically. You need to adjust the focus manually.
Focus Limit	<p>You can select the shortest focus distance, which means the Device will focus on objects farther than the shortest focus distance. If you select Auto, the Device will select an appropriate shortest distance according to the zoom value.</p>
Sensitivity	<p>Sensitivity is the capacity of resisting interference of the Device when focusing. The smaller the value is, the more capable the Device can resist interference when focusing.</p>
PFA	<p>If you enable this function, the image is relatively clear during zoom. If you disable this function, the speed is relatively high during zoom.</p>
Lens Initialization	<p>Click this button, and the lens will be initialized automatically. The lens will be extended to calibrate the zoom and focus.</p>

Step 3 Click **Save**.

5.1.1.1.7 Illuminator (IR Light/White Light)

This configuration is available only when the Device is equipped with illuminators. Some models support IR lights, white lights, and others. This section is for reference only, and might differ from the actual page.

Background Information

These are the conditions for using IR light and white light.

- When the day & night mode is set to **B/W**, the monitoring screen is black and white. In this case, IR light is used.
- When the day & night mode is set to **Color**, the monitoring screen is colored. In this case, white light is used.
- When the day & night mode is set to **Auto** , the monitoring screen color changes with the ambient light condition, and the illuminator varies with the monitoring screen. In **B/W** mode, the IR light is turned on; in **Color** mode, the white light is turned on.
- Full-spectrum IR light supports the infrared IR light and white-light IR light at the same time.



Some models are equipped with photoresistor that can turn on different types of illuminators based on the ambient brightness.

Procedure

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

Figure 5-11 Illuminator settings (1)

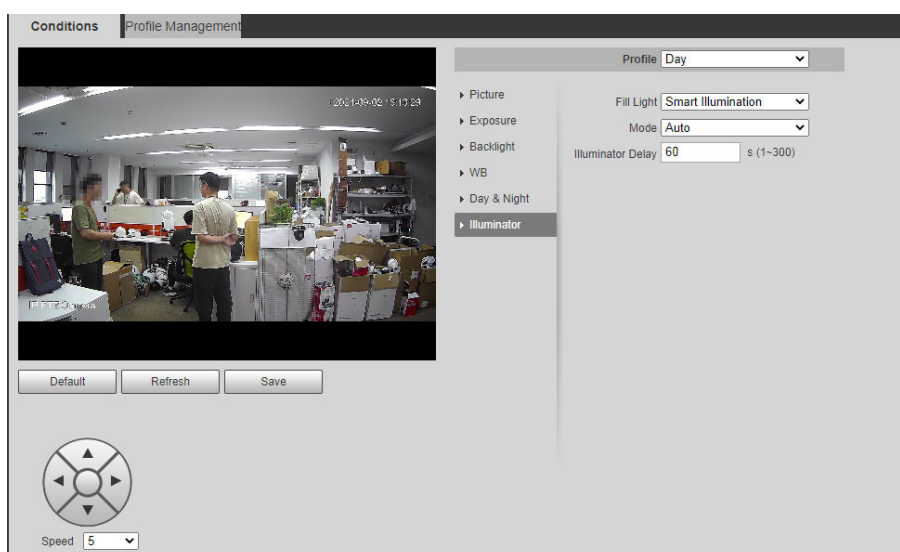


Figure 5-12 Illuminator settings (2)

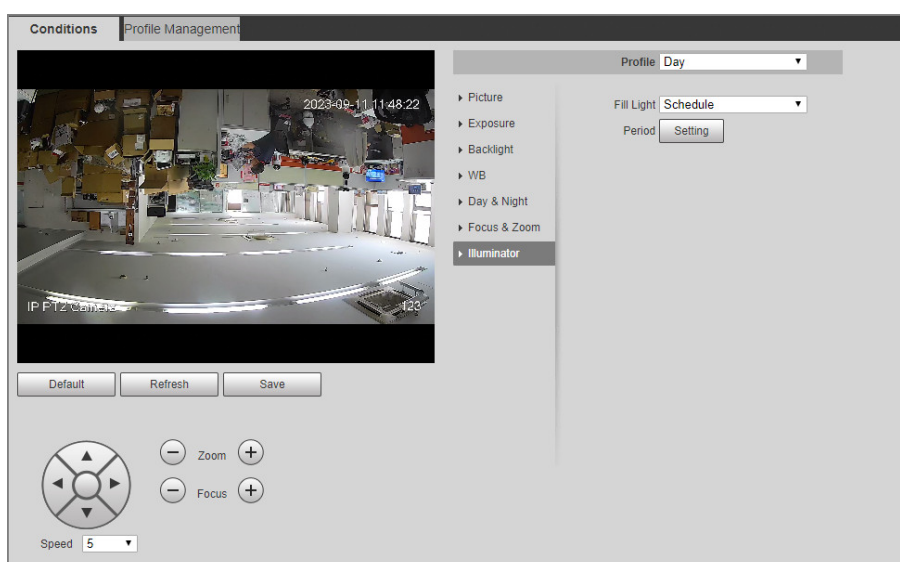
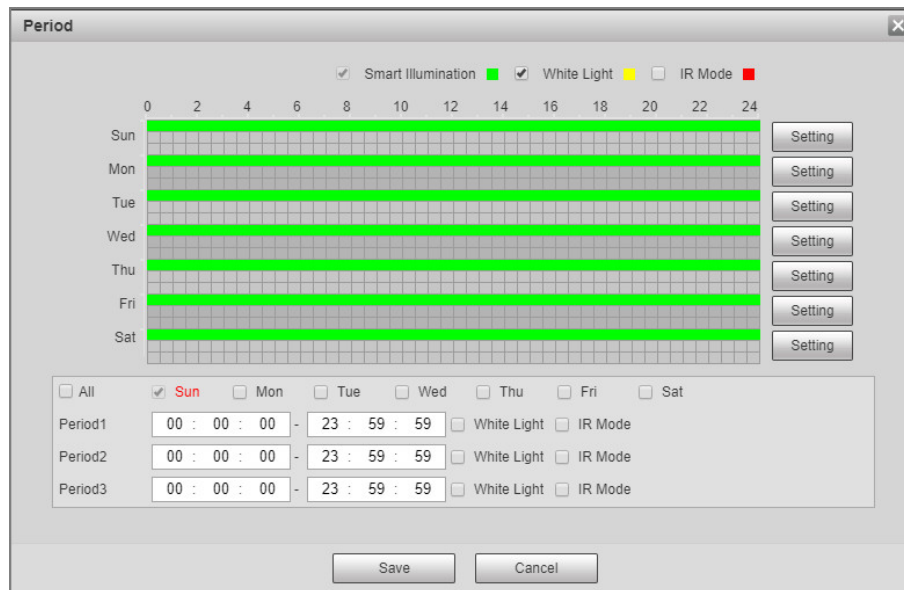



Figure 5-13 Period plan



Step 2 Configure illuminator.





1. Select **Fill Light** as needed.

Table 5-5 Description of fill light

Parameter	Description
IR Mode	<p>When the device is equipped with illuminators, you can configure the fill light mode, including IR mode, white light and smart illumination.</p> <ul style="list-style-type: none"> ● IR Mode: Enable the IR light, and then the white light is disabled. You can only capture black and white images after enabling this function. <p>The IR light is turned off for cameras with low power consumption by default. Turn on the IR light if necessary.</p> <ul style="list-style-type: none"> ● White Mode: Enable the white light, and the IR light is disabled. You can capture clear scene image after enabling this function. ● Smart Illumination: This function is mainly used at night. <p>Smart illumination applies IR mode in most situations. When an event occurs (for example, motion detection and human detection), the camera automatically switches to white light mode to link image capturing and video recording under the full color mode. The white light turns off when the event stops, and then the mode switches to IR mode according to the ambient brightness.</p> <p></p> <p>The status of the illuminator mainly depends on time and environment. If the smart illumination is triggered at night and the event continues during the day, the illuminator configured for the daytime will be turned off.</p> <ul style="list-style-type: none"> ● Schedule: Set the illumination solution according to the time period and use different solutions at different time periods.
White Mode	
Smart Illumination	
Schedule	

2. Select **Mode** as needed.



Table 5-6 Description of mode

Manual	<p>Adjust the brightness of illuminator manually, and then the system will supply illumination to the image accordingly.</p>  <p>This function is available on select models.</p>
Timing	<p>Enable different light types in different time periods according to actual condition. You can set four periods with different light types.</p>  <p>This function is available on select models.</p>
Auto	<p>The system adjusts the illuminator intensity according to the ambient lighting condition. Some devices support setting the brightness upper limit and sensitivity of the illuminator.</p> <ul style="list-style-type: none"> ● Sensitivity: The higher the sensitivity setting, the higher the brightness can turn on the illuminator when the actual scene darkens. When the actual scene becomes bright, a higher brightness is required to turn off the illuminator. ● Brightness upper limit: If the filling light is too bright, the center of the image might be overexposed, and the actual image cannot be seen clearly. It is suggested to adjust the brightness upper limit according to the actual scene. The value range is 0-100, and the default is 100.
Smart IR	<p>The system adjusts the illuminator intensity according to the ambient lighting condition.</p>  <p>Only infrared IR light supports the Smart IR mode.</p>
Zoom Priority	<p>The system adjusts the illuminator intensity automatically according to the change of the ambient light. You can configure light compensation manually to fine-tune the brightness of the illuminator.</p> <ul style="list-style-type: none"> ● When the ambient light turns darker, the system turns on the near light first, if the brightness is still not enough, then it turns on the far light. ● When the ambient light turns brighter, the system dims far light until they are off, and then the near light. ● When the focus reaches certain wide angle, the system will not turn on far light in order to avoid over-exposure in short distance.  <p>In ZoomPrio mode, IR light and white light are supported, and IR light is selected by default.</p>
Off	<p>Illuminator is off.</p>

3. Configure illumination parameters.

You can configure different illuminator parameters based on the selected fill light and mode.

Table 5-7 Description of illuminator parameters

Parameter	Description
Light Type	You can select IR Light or White Light .
Brightness	Change the overall brightness of the illuminator. The higher the value is, the brighter the illuminator will be, and the weaker its darker. The value ranges from 0 to 100.
Correction	Compensate for the brightness of the IR light. The value ranges from 0 to 100.
Illuminator Delay	The duration of the illuminator.  When selecting Smart Illumination in the drop-down list next to Fill Light , you need to set Illuminator Delay .
Period	When selecting Schedule in the drop-down list next to Fill Light , you need to set Period . The Device uses different illumination solutions at different time periods based on the time. a. Click Setting next to Period , and then select an illumination solution. b. Set a period corresponding to the illumination solution. Smart illumination is default for all periods. Different colors represent different illumination solutions on the timeline, as shown in Figure 5-13 . <ul style="list-style-type: none">● Method 1: You can directly drag on the timeline to set the period.● Method 2: You can click Setting corresponding to a week, select an illumination solution, and then set an accurate start and end time.  <ul style="list-style-type: none">● You can set 3 periods per day.● You can select All to set periods simultaneously.
Near Light	Set the brightness of the short-range light. The value ranges from 0 to 100.
Far Light	Set the brightness of the long-range light. The value ranges from 0 to 100.

Step 3 Click **Save**.

5.1.1.1.8 Illuminator (Laser Light)

This configuration is available only when the Device is equipped with illuminators. Some models support laser lights. This section is for reference only, and might differ from the actual page.

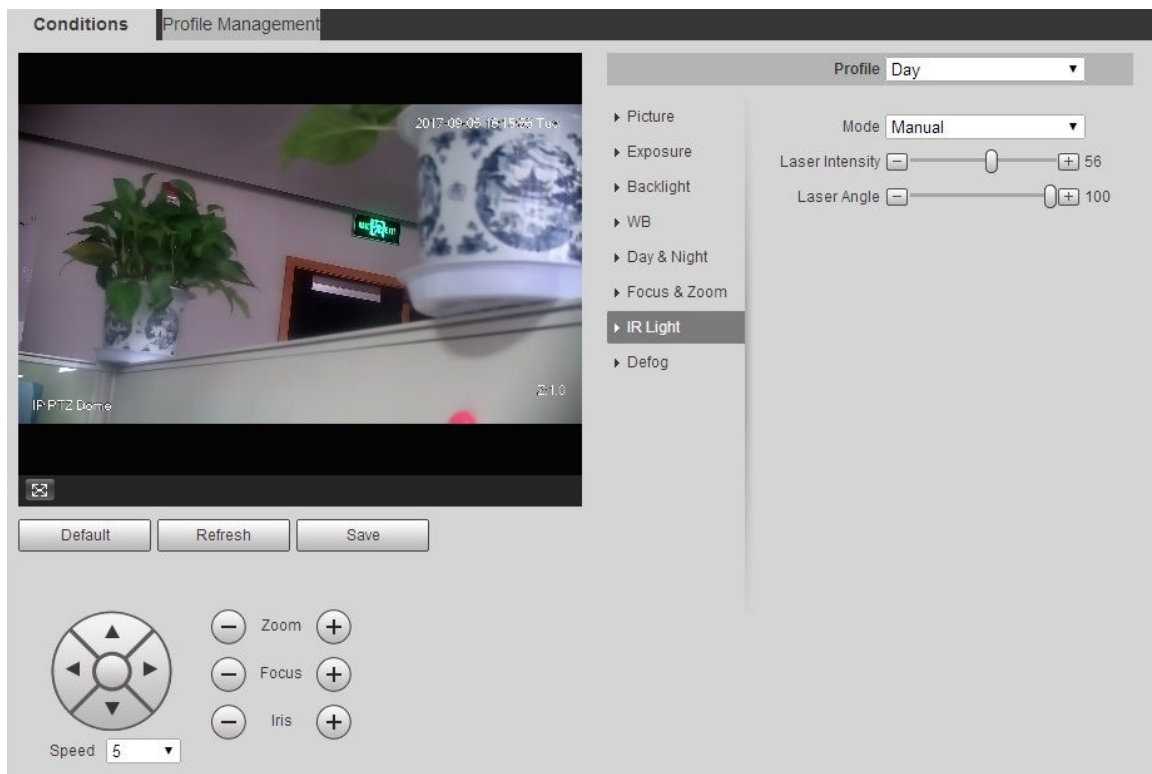
Background Information

Laser light makes compensation for the ambient environment when it is used for long-distance monitoring.

Procedure

Step 1 Select **Setting** > **Camera** > **Conditions** > **Conditions** > **IR Light**.

Figure 5-14 Laser light settings



Step 2 Configure laser light setting parameter.

Table 5-8 Description of laser light setting parameter

Parameter	Description
Mode	Select the laser light mode from ZoomPrio and Manual . It is ZoomPrio by default. <ul style="list-style-type: none"> ZoomPrio : The Device can automatically adjust laser light brightness according to the zoom times. Manual : Manually set laser light brightness and angle value.
Laser Intensity	Set the intensity of the laser light. The value ranges from 0 to 100.
Laser Angle	Set the angle value from 0 to 100.

Step 3 Click **Save**.

5.1.1.1.9 Defog

Background Information



The defog function cannot be configured if backlight function is enabled. There will be a prompt on the page.

Image quality drops if the Device is installed in foggy or hazy environment. You can enable defog to improve image quality.

Procedure

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

Figure 5-15 Defog settings—manual

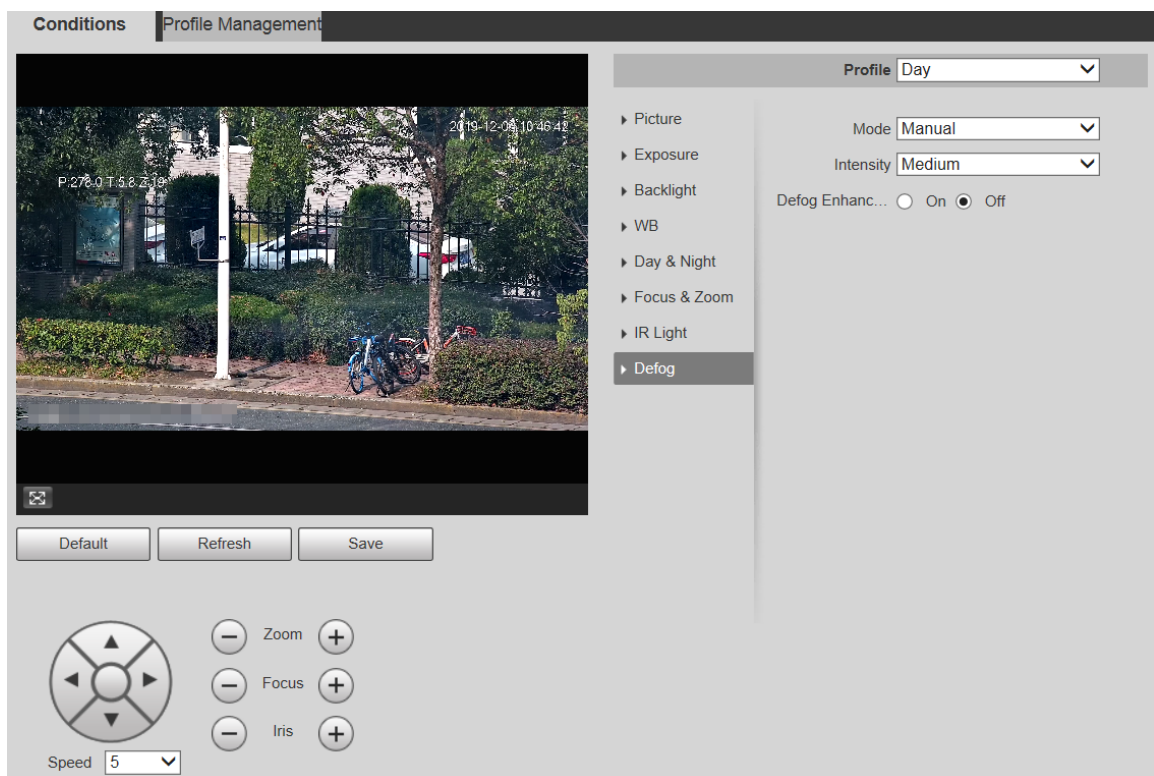
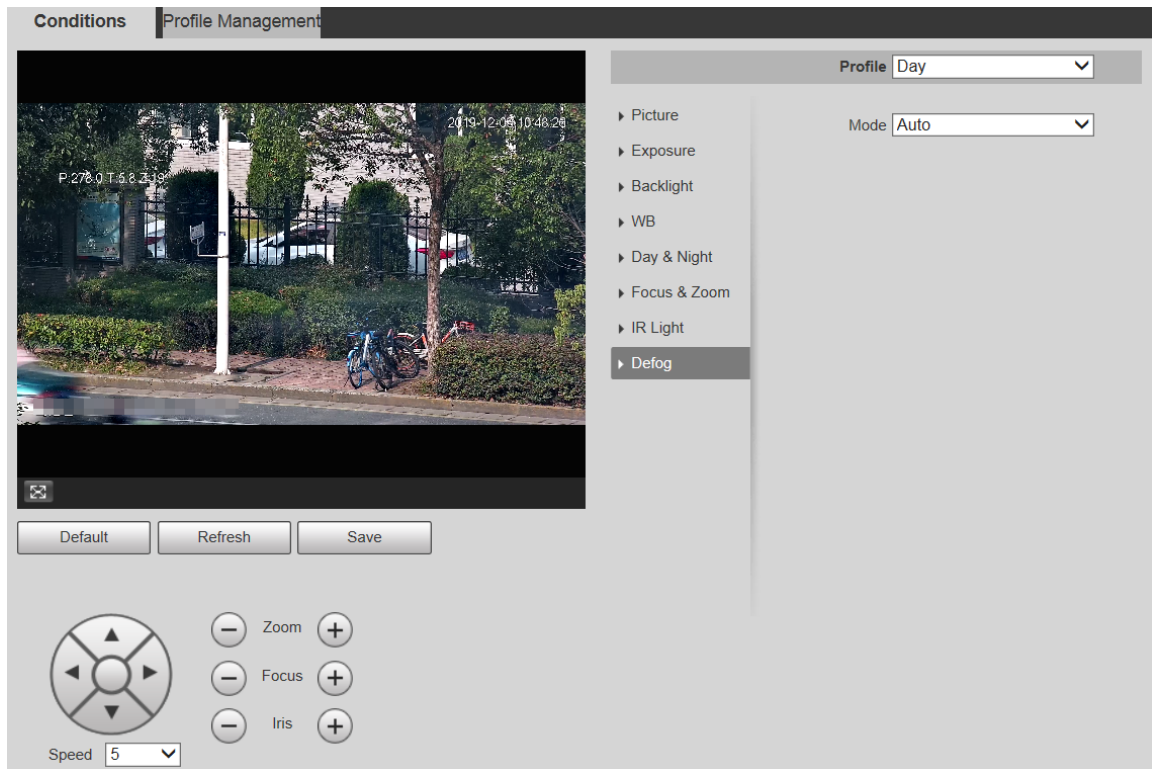


Figure 5-16 Defog settings—auto



Step 2 Configure defog parameter.

Table 5-9 Description of defog parameter

Parameter	Description
Mode	<p>Select the defog mode of the Device. You can select Auto , Manual, or Off. It is Off by default.</p> <p>For the Device that supports optical defog, in Auto mode, optical defog and electronic defog switch automatically according to the algorithm. And in Off mode, electronic defog is enabled by default.</p>
Intensity	<p>Set the defog intensity of the Device. You can select from Low , Medium, or High.</p>
Defog Enhancement	<p>In Manual mode, if you enable this function, both optical defog and electronic defog are enabled. (You need to enable Auto mode for Day & Night to use the function.)</p> <p>Only the Device that supports optical defog has this parameter.</p>

Step 3 Click **Save**.

5.1.1.2 Profile Management

Procedure

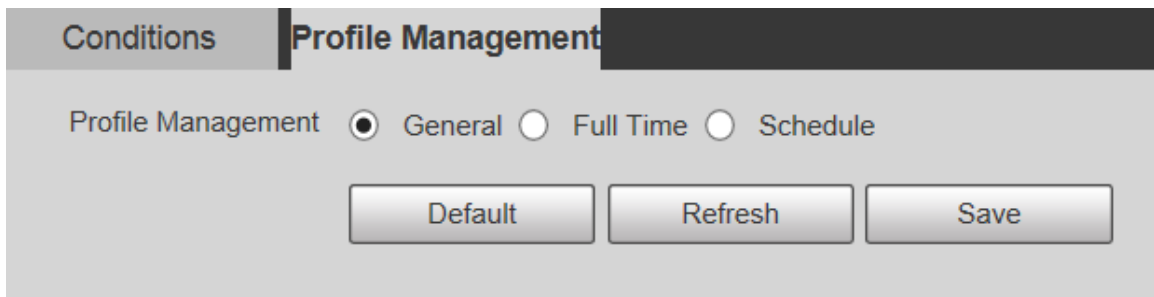
Step 1 Select **Setting** > **Camera** > **Conditions** > **Profile Management**.

Step 2 Select the profile management mode.

There are three options: **General** , **Full Time** and **Schedule**.

- If you select **General**, monitoring is based on the general configuration of the Device.

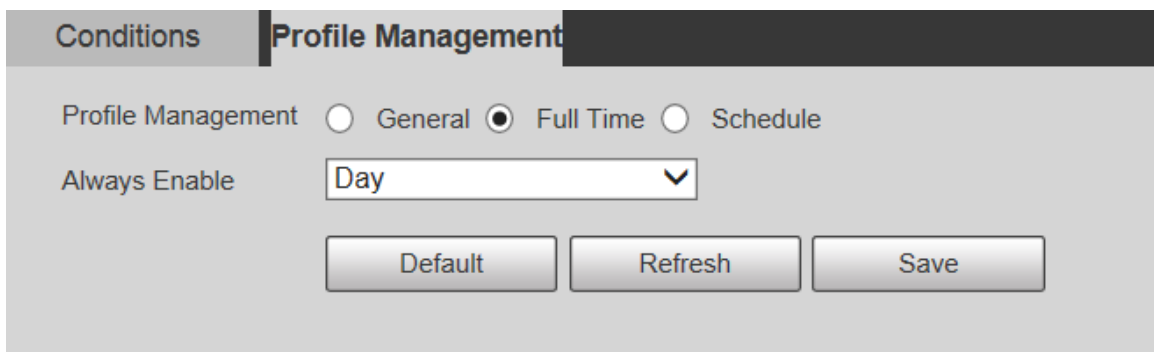
Figure 5-17 Profile management—general



The screenshot shows the 'Profile Management' tab selected. Under 'Profile Management', the 'General' radio button is selected. Below the radio buttons are three buttons: 'Default', 'Refresh', and 'Save'.

- If you select **Full Time** , **Day** and **Night** are selectable, and the corresponding camera property profile is day or night.

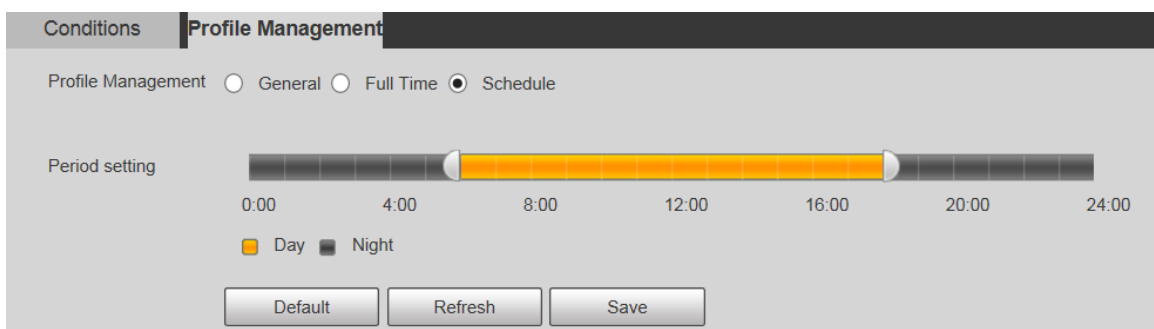
Figure 5-18 Profile management—full time



The screenshot shows the 'Profile Management' tab selected. Under 'Profile Management', the 'Full Time' radio button is selected. Below the radio buttons, there is a dropdown menu labeled 'Always Enable' with 'Day' selected. At the bottom are three buttons: 'Default', 'Refresh', and 'Save'.

- If you select **Schedule**, you can select one period for day configuration and another period for night configuration. For example, you can set the day-time configuration from 6:00 to 18:00, and set the night-time configuration from 18:00 to 6:00 on the next day.

Figure 5-19 Profile management—schedule



The screenshot shows the 'Profile Management' tab selected. Under 'Profile Management', the 'Schedule' radio button is selected. Below the radio buttons, there is a 'Period setting' section with a timeline from 0:00 to 24:00. The timeline is divided into 'Day' (orange) and 'Night' (grey) periods. The 'Day' period is set from 6:00 to 18:00, and the 'Night' period is set from 18:00 to 6:00. At the bottom are three buttons: 'Default', 'Refresh', and 'Save'.

Step 3 Click **Save**.

5.1.2 Video

You can set the video stream, snapshot stream, video overlay, ROI, and storage path of the Device.

5.1.2.1 Video Stream

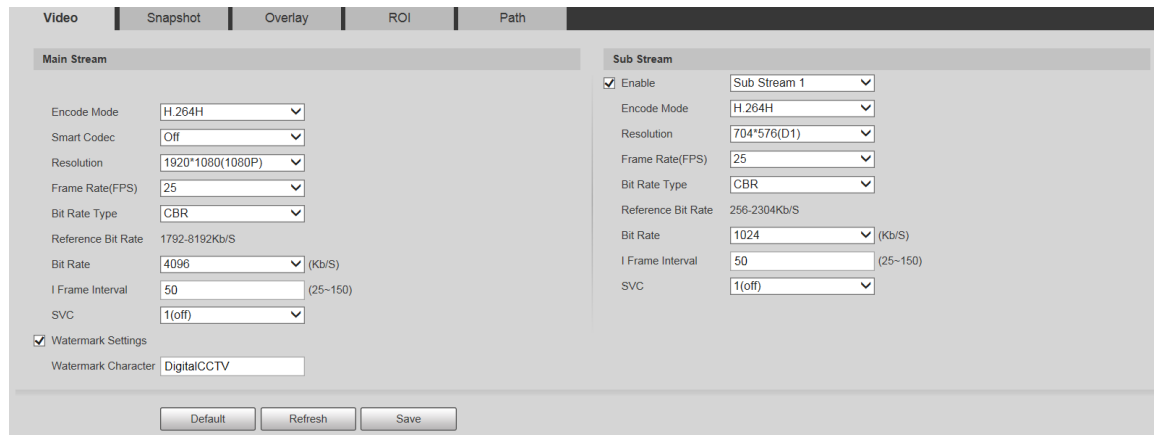
Background Information

This section describes how to set the video stream for the monitoring screen.

Procedure

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

Figure 5-20 Video stream settings





- The stream configuration pages might vary depending on devices, and the actual page shall prevail.
- The default bit rate of different devices might vary, and the actual product shall prevail.

Step 2 Configure video stream parameter.

Table 5-10 Description of video stream parameters

Parameter	Description
Enable	You can select the checkbox to enable sub stream. The sub stream is enabled by default.
Encode Mode	You can select H.264 , H.264H , H.264B , H.265 , MJPEG , MPEG4 , or SVAC .
Smart Codec	<p>Enable Smart Codec to improve video compressibility and save storage space.</p> <p>After Smart Codec is enabled, the Device does not support the third stream, ROI, smart event, and other functions.</p>
Resolution	Multiple resolution types are available for you to choose, and each type corresponds to a unique recommended stream value.
Frame Rate (FPS)	PAL: 1–25 frames/s or 1–50 frames/s. The frame rate changes with the resolution.
Bit Rate Type	<p>There are two options: CBR (constant bit rate) and VBR (variable bit rate).</p> <ul style="list-style-type: none"> • Image quality can be set only in VBR mode, and cannot be set in CBR mode. • In MJPEG encode mode, CBR is the only option for Bit Rate Type.

Parameter	Description
Reference Bit Rate	The recommended bit rate range is based on the resolution and frame rate.
Bit Rate	It is the upper limit of stream in VBR. In CBR, the value is fixed.
I Frame Interval	The number of P frames between two I frames. The range varies with the frame rate, and the maximum value is 150. It is recommended to set the interval twice the frame rate.
SVC	Layered encoding can be done for FPS. SVC is a scalable encoding method on time domain. It is 1 by default, which means no layered coding. You can set 2, 3 or 4 layered encoding.
Watermark Settings	You can verify the watermark to check if the video has been tampered.
Watermark Character	<p>You can verify the watermark to check if the video has been tampered. Select Watermark Settings checkbox to enable Watermark Character. The watermark character is DigitalCCTV by default, and you can modify it.</p> <p></p> <p>Watermark character consists of up to 128 characters from letters, standard symbols, spaces, and special characters.</p>

Step 3 Click **Save**.

5.1.2.2 Snapshot

Background Information

This section describes how to set streams for snapshots.

Procedure

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

Figure 5-21 Snapshot stream settings

Video	Snapshot	Overlay	ROI	Path
Snapshot Type	General			
Image Size	1080P (1920*1080)			
Quality	5			
Interval	1S			
<div> <input type="button" value="Default"/> <input type="button" value="Refresh"/> <input type="button" value="Save"/> </div>				

Step 2 Configure snapshot stream parameter.

Table 5-11 Description of snapshot stream parameters

Parameter	Description
Snapshot Type	<p>You can select General or Event.</p> <ul style="list-style-type: none"> General refers to capturing images within the time range set in the schedule. For details, see "5.6.1 Schedule". Event means capturing images when motion detection, video tampering, or local alarms are triggered. For how to enable snapshots for motion detection, video tampering, or local alarms, see "5.5 Event Management".
Image Size	It is the same as the resolution of the selected snapshot main stream, and cannot be modified on this page.
Quality	You can set the snapshot quality from 1 to 6 levels. Level 1 is the lowest level, and level 6 is the highest level.
Interval	Set the snapshot frequency. You can select from 1 s through 7 s or Customized .

Step 3 Click **Save**.

5.1.2.3 Overlay

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

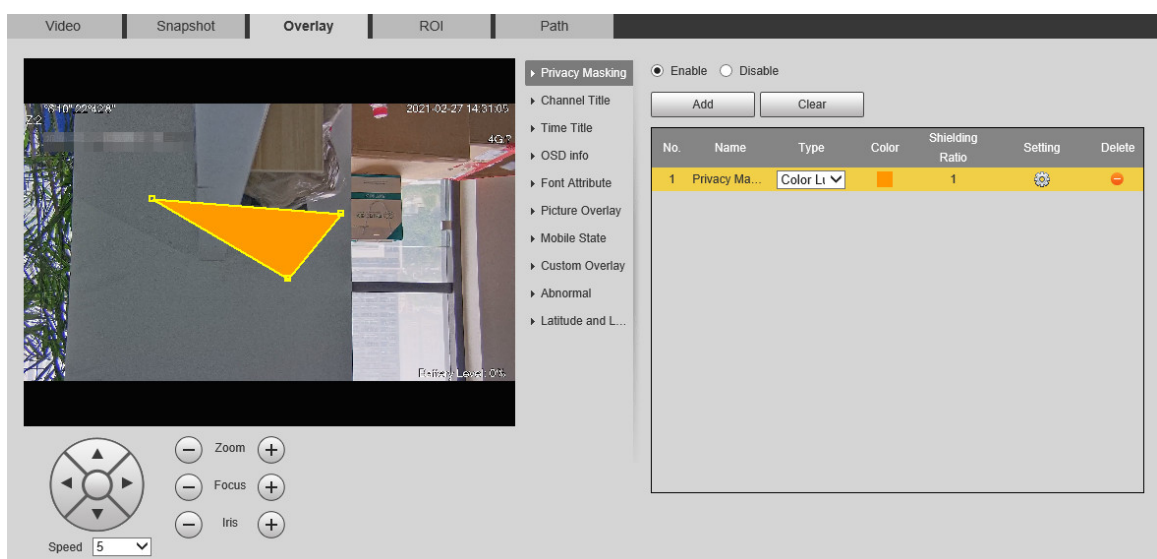
5.1.2.3.1 Privacy Masking

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

Procedure

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

Figure 5-22 Privacy masking



Step 2 Select **Enable**.

Step 3 Click **Add**, select the masking type and color, set the shielding ratio, and then draw blocks on the image.



You can select the masking type 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.
- When selecting **Mosaic**, you can draw rectangles as blocks with mosaic. You can draw 4 blocks at most.
- When selecting both **Color Lump** and **Mosaic**, you can draw 8 blocks at most.

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 block name to edit it.

- Delete the block.

- ◇ Click  to delete blocks one by one.
- ◇ Click **Clear** to delete all blocks.

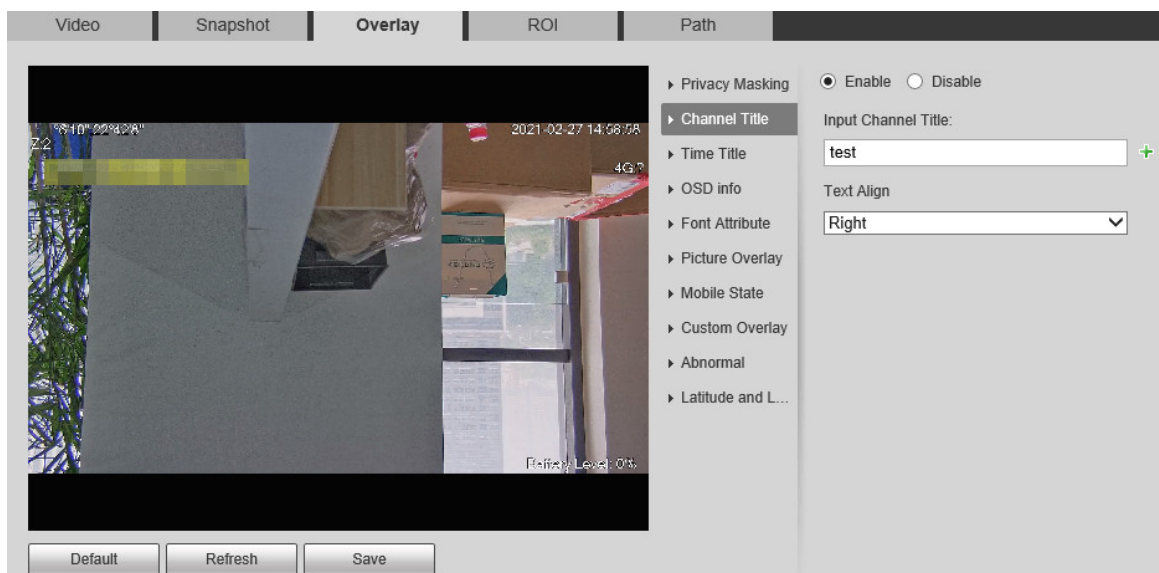
5.1.2.3.2 Channel Title

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

Procedure


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

Figure 5-23 Channel title



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



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**.

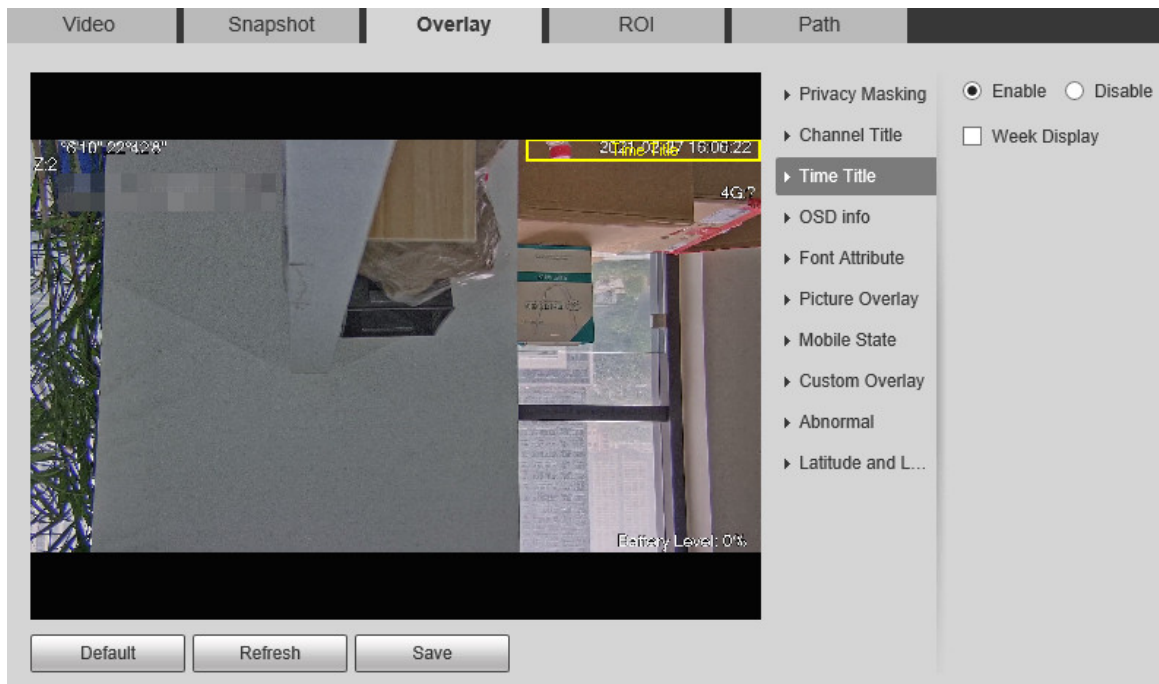
5.1.2.3.3 Time Title

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

Procedure

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

Figure 5-24 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**.

5.1.2.3.4 OSD Info

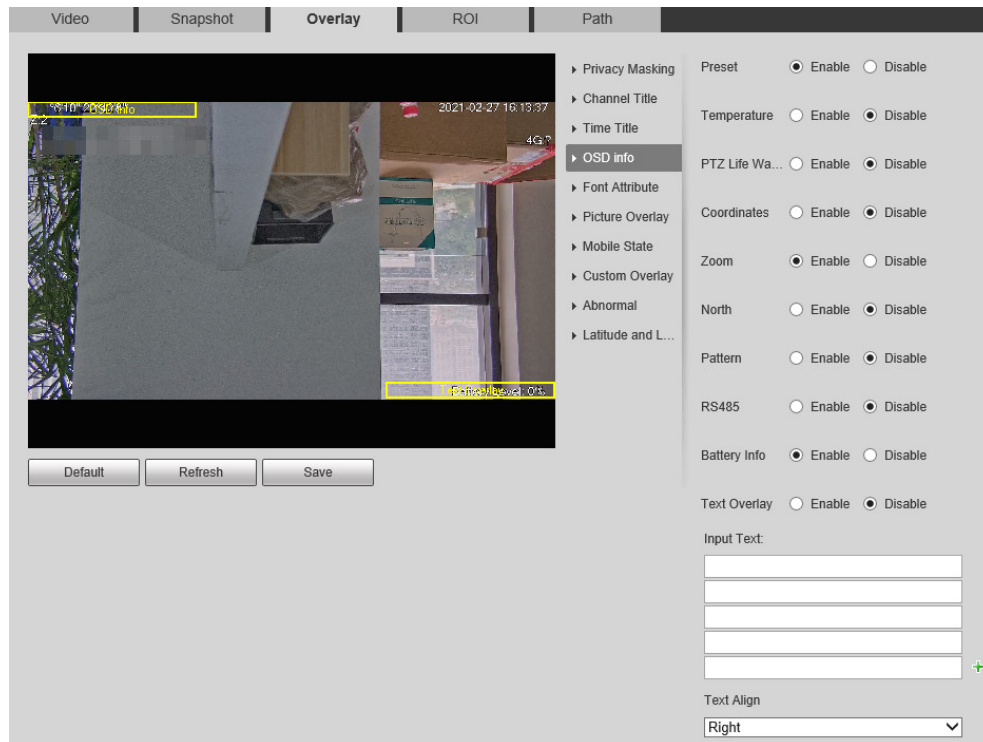
Background Information

You can enable this function if you want to display preset title, temperature, PTZ life warning, coordinates, zoom, north direction, pattern, RS-485, battery information, and other information on the video image.

Procedure

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

Figure 5-25 OSD info



Step 2 Configure OSD information.

Table 5-12 Description of OSD information

Parameter	Description
Preset	Select Enable , and the preset name is displayed on the image when the camera turns to the preset, and it will disappear 3 s later. For some devices, you can set the duration of the preset title displaying on the screen. You can select from Disable , 5s , 15s , Display Permanently , and Custom .
Temperature	Select Enable , and the internal temperature of the current device is displayed.
PTZ Life Warning	When the PTZ lifespan is close to the threshold, a warning will be displayed on the video image. This OSD info is enabled by default.
Coordinates	Select Enable , and the PTZ coordinates information is displayed on the image.
Zoom	Select Enable , and the zoom information is displayed on the image. For example, P 29.4 T 12.0 Z 12 means 12x zoom rate.
North	Select Enable , and the north direction is displayed on the image.
Pattern	Select Enable , and the pattern information is displayed on the image.
RS485	Select Enable , and the RS-485 communication information is displayed on the image.
Battery Info	Select Enable , and the battery level is displayed on the image.
Text Overlay	Select Enable and enter text, and the text is displayed on the image.

Parameter	Description
Input Text	
Text Align	Set the alignment mode of the displayed information on the image.

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

Step 4 Click **Save**.

5.1.2.3.5 Font Attribute

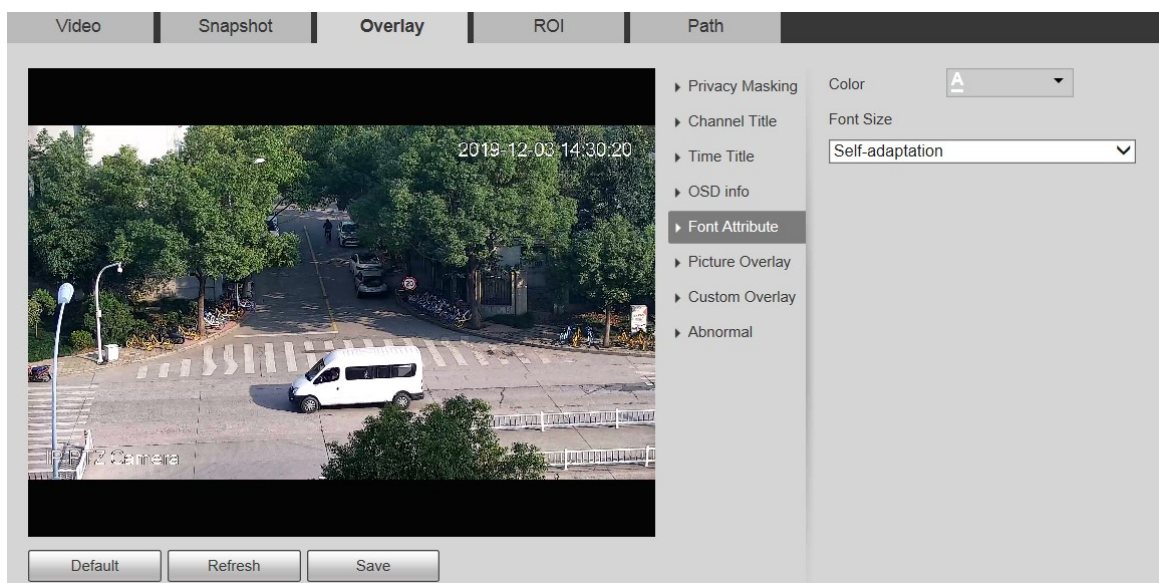
Background Information

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

Procedure

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

Figure 5-26 Font attribute



Step 2 Select the font color and size.

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

Step 3 Click **Save**.

5.1.2.3.6 Picture Overlay

Background Information

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

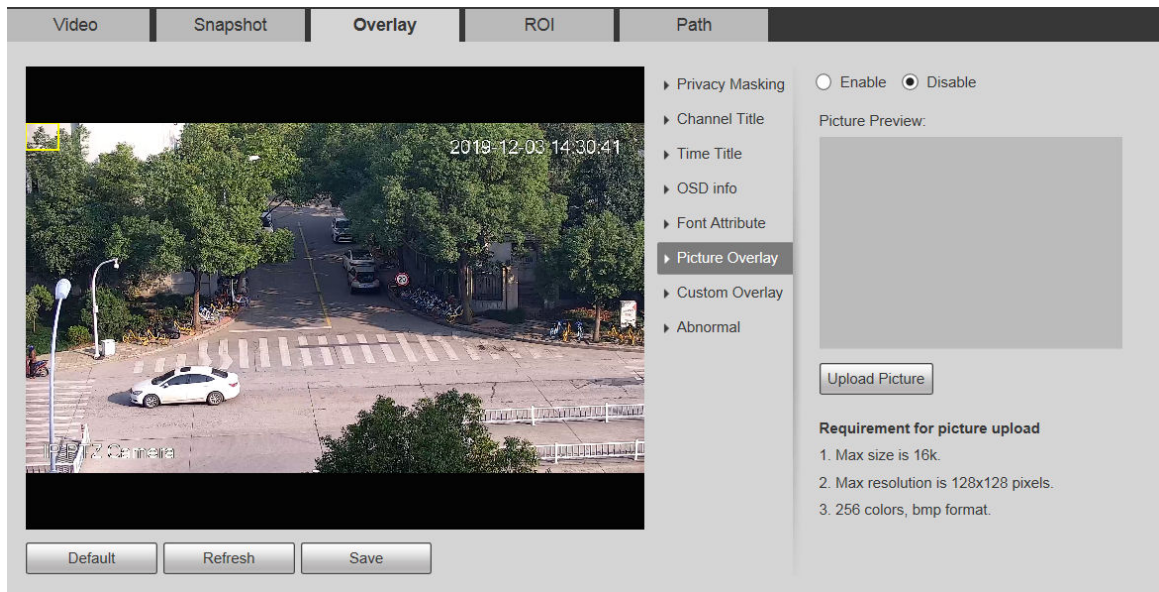


Text overlay and picture overlay cannot be enabled at the same time.

Procedure

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

Figure 5-27 Picture overlay



Step 2 Select the **Enable** checkbox, click **Upload Picture**, and then select the image to be overlaid.

The image is displayed on the video image.

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

Step 4 Click **Save**.

5.1.2.3.7 Mobile State

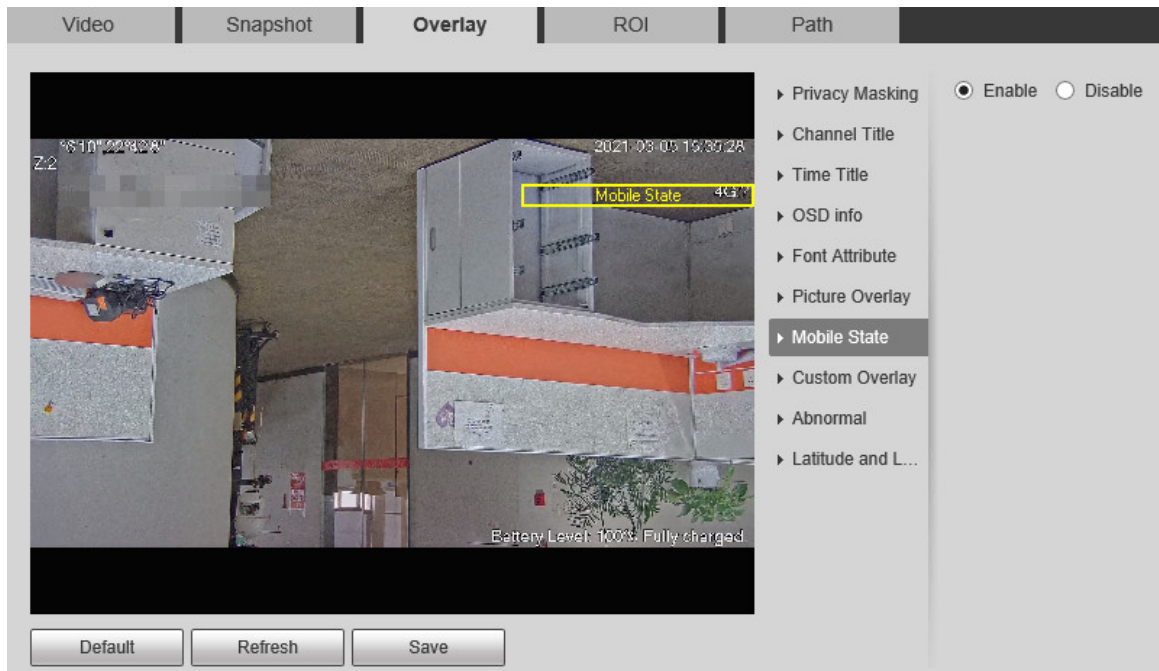
Background Information

You can enable this function if you want to display mobile state on the image.

Procedure

Step 1 Select **Setting > Camera > Video > Overlay > Mobile State**.

Figure 5-28 Mobile state



Step 2 Select the **Enable** checkbox.

Step 3 Drag the mobile state box to the position that you want on the image.

Step 4 Click **Save**.

The mobile state information is displayed on the image.

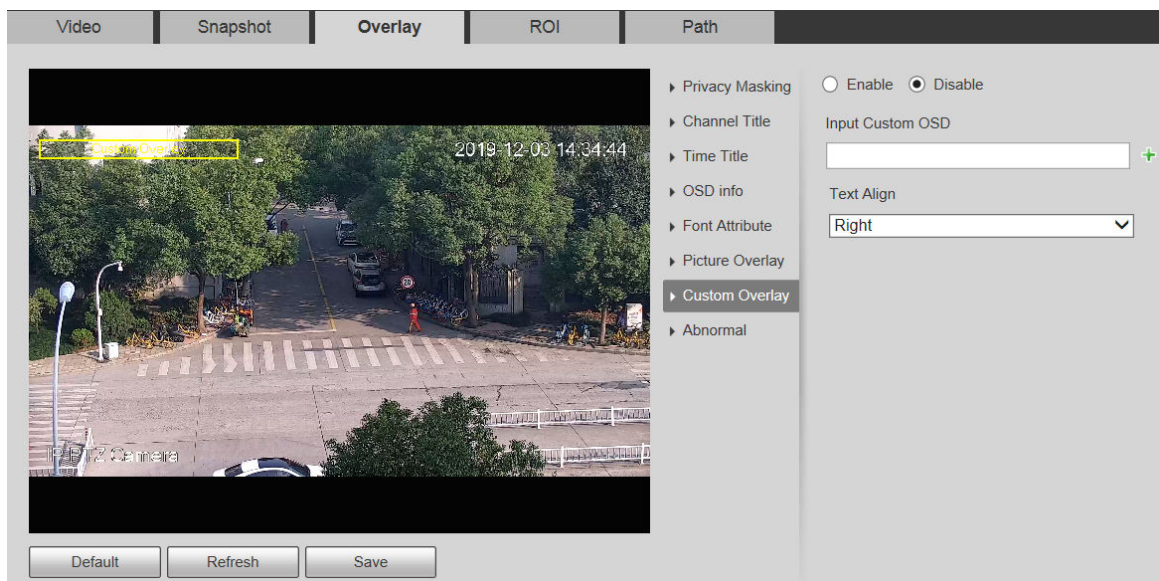
5.1.2.3.8 Custom Overlay

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

Procedure


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

Figure 5-29 Custom overlay



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



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

Step 3 Drag the custom overlay box to the position that you want on the image.

Step 4 Click **Save**.

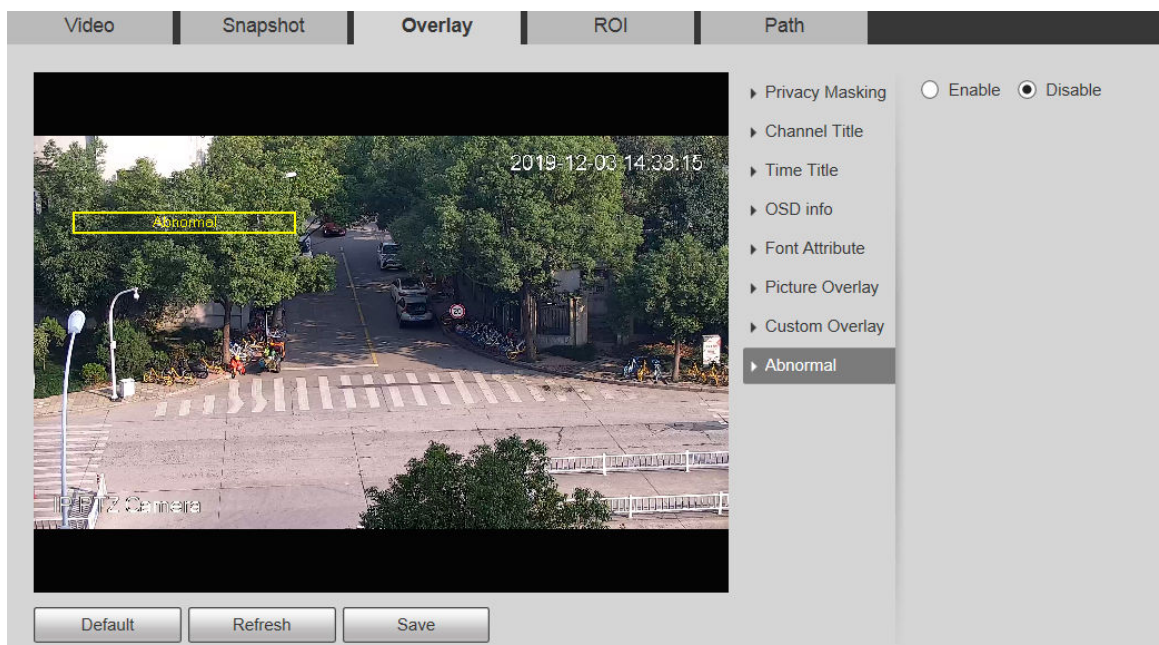
5.1.2.3.9 Abnormal

You can enable this function if you want to display exception information on the image.

Procedure

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

Figure 5-30 Abnormal



Step 2 Select the **Enable** checkbox.

Step 3 Drag the box to the position that you want on the image.

Step 4 Click **Save**.

The exception information is displayed on the image.

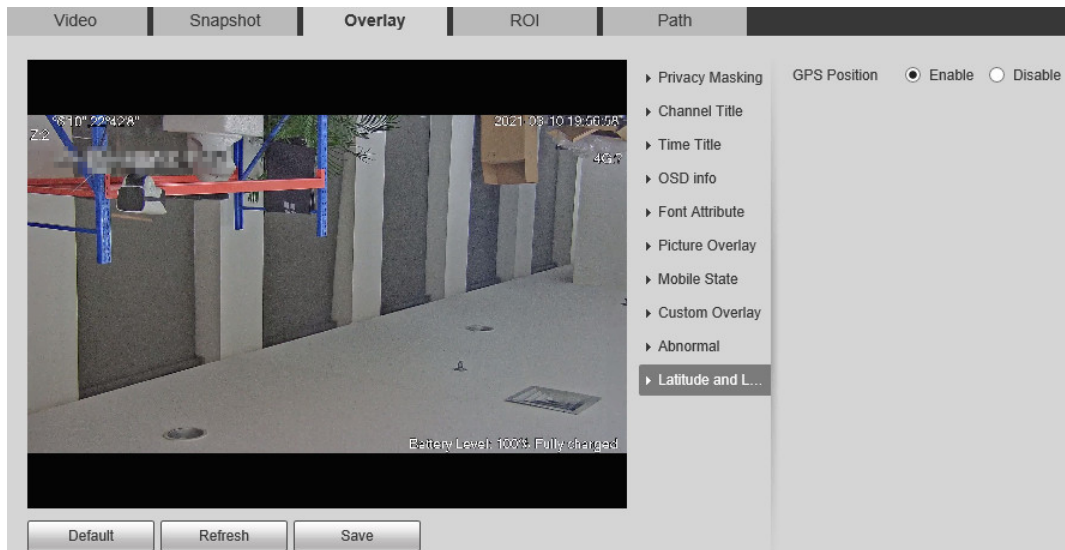
5.1.2.3.10 Latitude and Longitude

You can enable this function if you need to display latitude and longitude on the video image.

Procedure

Step 1 Select **Setting** > **Camera** > **Video** > **Overlay** > **Latitude and Longitude**.

Figure 5-31 Latitude and longitude



- Step 2 Select the **Enable** checkbox.
- Step 3 Drag the box to the position that you want on the image.
- Step 4 Click **Save**.

5.1.2.4 ROI

Background Information

You can set a key monitoring region as a ROI (region of interest), and configure the image quality of this region.

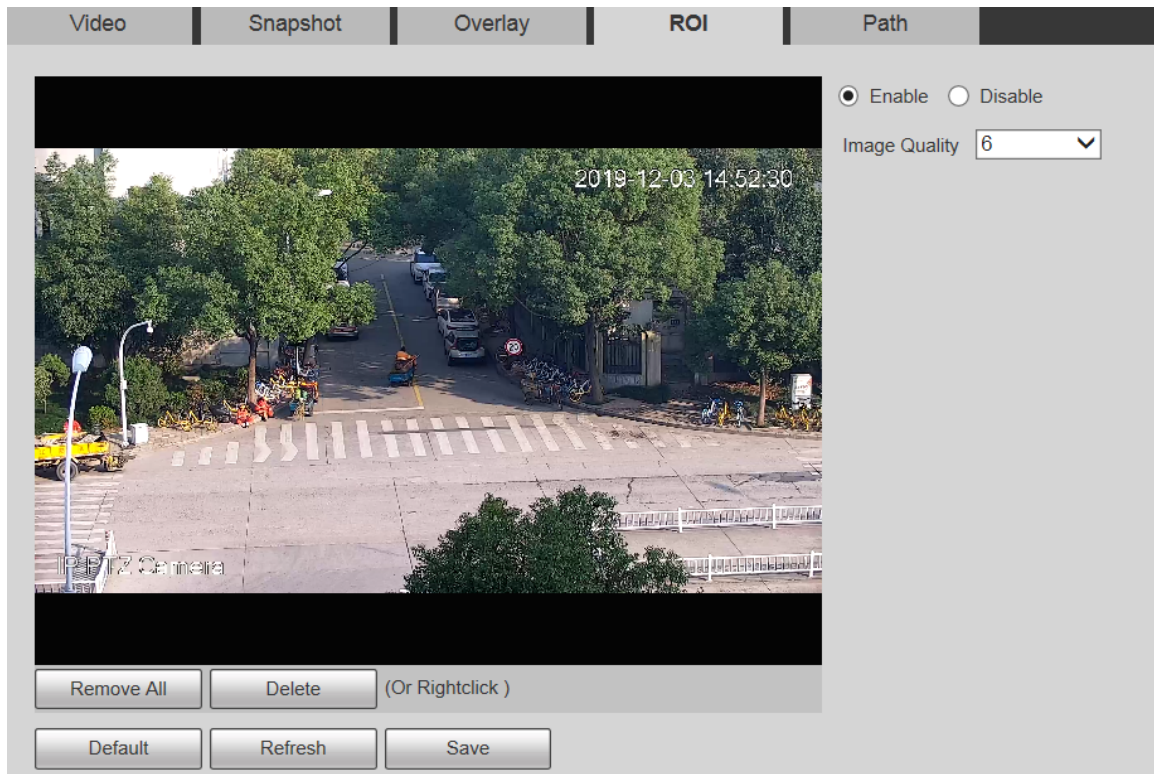


ROI is available on select models.

Procedure

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

Figure 5-32 ROI settings



Step 2 Select **Enable** to enable this function.

Step 3 Press and hold the left mouse button to draw boxes on the monitoring screen. You can draw up to 4 boxes.



- Click **Delete** or right click to delete the drawn boxes.
- Click **Remove All** to clear all boxes.

Step 4 Set the image quality of the ROI.

Step 5 Click **Save**.

5.1.2.5 Path

Background Information

The storage path is associated with the snapshot and recording on the **Live** page. You can set the path of **Live Snapshot** and **Live Record** respectively.

The storage path is associated with the snapshot, downloaded and clipped files on the **Playback** page. You can set the path of **Playback Snapshot**, **Playback Download**, and **Video Clips** respectively.

Procedure

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

Figure 5-33 Path settings

Video	Snapshot	Overlay	ROI	Path
Live Snapshot	C:\Users\...\WebDownload\LiveSnapshot			Browse...
Live Record	C:\Users\...\WebDownload\LiveRecord			Browse...
Playback Snapshot	C:\Users\...\WebDownload\PlaybackSnapshot			Browse...
Playback Download	C:\Users\...\WebDownload\PlaybackRecord			Browse...
Video Clips	C:\Users\...\WebDownload\VideoClips			Browse...
<div>Default</div> <div>Save</div>				

Step 2 Set each storage path.

- Default storage path for snapshots: C:\Users\admin\WebDownload\LiveSnapshot.
- Default storage path for recording: C:\Users\admin\WebDownload\LiveRecord.
- Default storage path for playback snapshot: C:\Users\admin\WebDownload\PlaybackSnapshot.
- Default storage path for playback download: C:\Users\admin\WebDownload\PlaybackRecord.
- Default storage path for video clips: C:\Users\admin\WebDownload\VideoClips.

Step 3 Click **Save**.

5.1.3 Audio

You can configure audio parameters and alarm audio.



The function is available on select models.

5.1.3.1 Configuring Audio Parameters

Background Information

You can set the audio input type, volume and more. After you enable main stream or sub stream, the network stream contains both audio and video; otherwise it is only video stream.

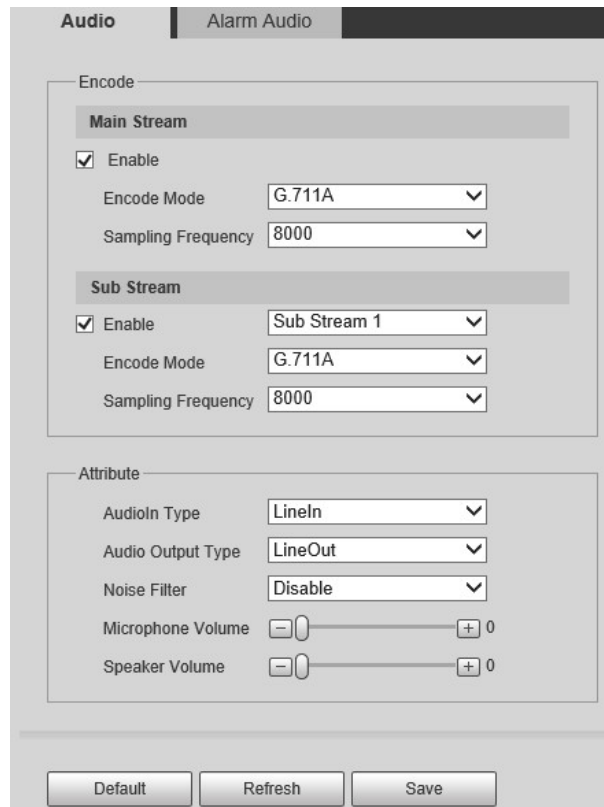


Before enabling sub stream audio, go to **Setting** > **Camera** > **Video** > **Video** to enable video in sub stream.

Procedure

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



Figure 5-34 Audio



Step 2 Enable audio in main stream or sub stream.

Step 3 Configure audio parameters.

Table 5-13 Description of audio parameter

Parameter	Description
Enable	<p>Enable audio in main stream or sub stream.</p> <p> Audio can be enabled only when video has been enabled.</p>
Encode Mode	The audio encoding mode selected here applies to both audio streams and voice talks. We recommend you to keep the default value.
Sampling Frequency	The number of audio signals sampled per second. The higher the sampling frequency, the more samples obtained per unit time, and the more accurate the restored audio signals.
AudioIn Type	<p>Set the audio input type.</p> <ul style="list-style-type: none"> ● LineIn: The Camera collects audio signals through an external audio device. ● Mic: The Camera collects audio signals through the built-in microphone. ● Bluetooth: The Camera collects audio signals through a Bluetooth device. <p> Bluetooth is available on select models.</p>

Parameter	Description
Audio Output Type	<p>Set the audio output type.</p> <ul style="list-style-type: none"> ● LineOut: The Camera outputs audio signals through an external audio device. ● Speaker: The Camera outputs audio signals through the built-in speaker. ● Bluetooth: The Camera outputs audio signals through a Bluetooth device. <p> Bluetooth is available on select models.</p>
Noise Filter	After the function is enabled, noise in the environment will be filtered.
NR (Noise Reduction) Level	<p>Adjust the noise reduction level.</p> <p> This parameter takes effect when noise filter is enabled.</p>
Microphone Volume	Adjust the microphone volume.
Speaker Volume	Adjust the speaker volume.

Step 4 Click **Save**.

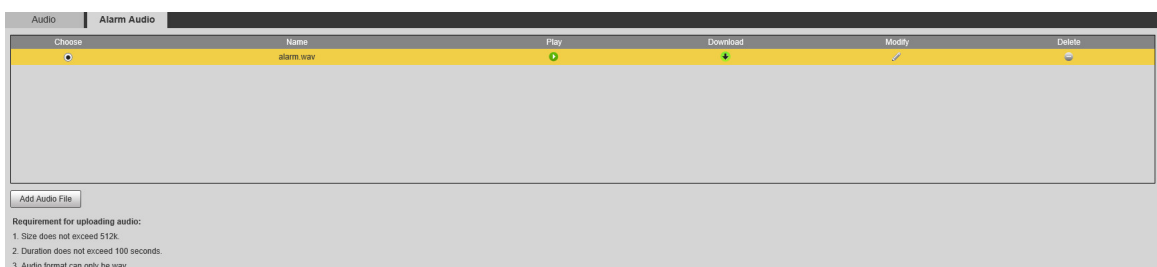
5.1.3.2 Configuring Alarm Audio

You can set the alarm audio to be played when an alarm is triggered. For some devices, you can record or upload alarm audios.

Procedure

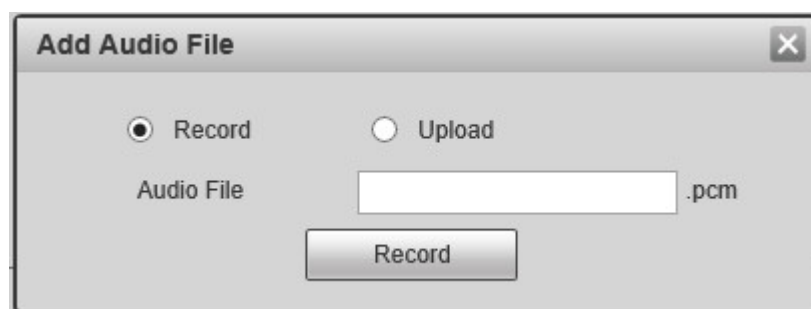
Step 1 Select **Setting** > **Camera** > **Audio** > **Alarm Audio**.

Figure 5-35 Alarm audio




Step 2 Click **Add Audio File**.



Figure 5-36 Add audio file



Step 3 Configure the audio file.



- Select **Record** , enter the audio file name, and then click **Record**.
Click **Stop** to complete recording.
- Select **Upload** , click  , select the audio file to be uploaded, and then click **Upload**.



- The format of recorded audio is .pcm. Audio recording is only supported by some devices.
- Audio file in the format of .wav can be uploaded.
- You can edit and delete recorded or uploaded audio.
 - ◇ Click to  edit audio file.
 - ◇ Click  to delete audio file.

Step 4 Select the audio file that you need.

Related Operations

- Play audio: Click  to play the alarm audio.
- Download audio: Click  to download the alarm audio to local storage. The audio is saved to the default download path of the browser.

5.2 Network Settings

5.2.1 TCP/IP

You can configure the IP address and DNS server of the Device to connect it to other devices in the network.

Prerequisites

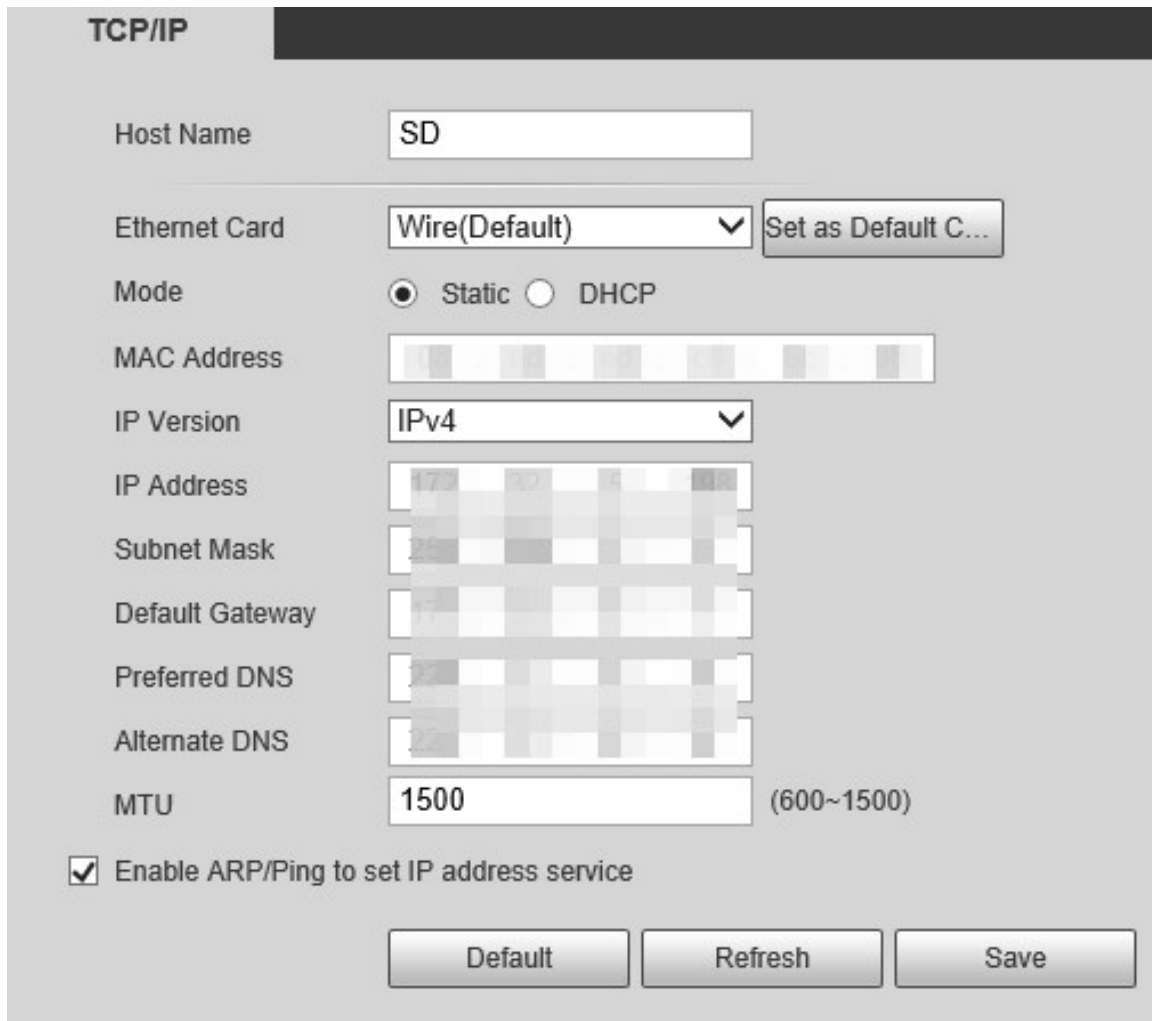
Before configuring network parameters, make sure that the Device is connected to the network properly.

- If there is no router in the network, assign an IP address in the same network segment.
- If there is a router in the network, set the corresponding gateway and subnet mask.

Procedure


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




Figure 5-37 TCP/IP settings



Step 2 Set TCP/IP parameters.

Table 5-14 Description of TCP/IP parameter

Parameter	Description
Host Name	Set the name of the current device. The host name can be English or Chinese within 63 bytes.
Ethernet Card	Select the Ethernet card to be configured. Wire is selected by default.  If the Device is configured with multiple Ethernet cards, the default Ethernet card can be changed. If you reset the default Ethernet card, restart the Device.
Set as Default Card	Click to set the current Ethernet card as the default card.

Parameter	Description
Mode	<p>Static and DHCP modes are available.</p> <ul style="list-style-type: none"> If DHCP is selected, the IP address is obtained automatically. In this case, the IP address, subnet mask, and gateway cannot be set. If Static is selected, you need to set the IP address, subnet mask, and gateway manually.
MAC Address	Display the MAC address of the Device.
IP Version	You can select IPv4 or IPv6 . Both versions are supported and can be accessed.
IP Address	Enter correct digits to change the IP address.
Subnet Mask	<p>Set the subnet mask according to actual conditions. The subnet prefix is a number in the range of 1 to 255. The subnet prefix identifies a specific network link, and usually contains a hierarchical structure.</p> <p> The Device checks the validity of all IPv6 addresses. The IP address and the default gateway must be in the same network segment. Make sure that a certain part of the subnet prefix in the IP address and default gateway are the same.</p>
Default Gateway	<p>Configure as needed. The default gateway must be in the same network segment as the IP address.</p> <p> For IPv6 version, in the IP Address, Default Gateway, Preferred DNS, and Alternate DNS fields, enter 128 bits, and these fields cannot be blank.</p>
Preferred DNS	IP address of the DNS server.
Alternate DNS	Alternate IP address of the DNS server.
MTU	<p>You can set the MTU value to ensure good data transmission according to the network. The value is 1500 by default. Modifying MTU value causes Ethernet card restarting and network disconnection.</p> <p> Here are some suggested value for your reference.</p> <ul style="list-style-type: none"> 1500: It is the maximum and default value of Ethernet packet, typical setting of the network connection without PPPOE or VPN, and is the default setting of some routers, network adapters, and switches. 1492: The optimal value for PPPOE. 1468: The optimal value for DHCP. 1450: The optimal value for VPN.

Parameter	Description
Enable ARP/Ping to set IP address service	<p>Select the checkbox, and then you can modify and set the device IP address through ARP/Ping command if the MAC address is known.</p> <ul style="list-style-type: none"> The function 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 the function is not enabled, the IP address cannot be configured with ping packet.

Step 3 Click **Save**.

Related Operations

An Example of Configuring IP Address with ARP/Ping:

- To obtain a usable IP address, make sure that the Device and your PC are in the same LAN.
- Get the MAC address from the Device label.
- Open command editor on the PC and enter the following command.

Table 5-15 Command list

System	Command
Windows syntax	<pre>arp -s <IP Address> <MAC> ping -l 480 -t < IP Address > Example: arp -s 192.168.1.125 11-40-8c-18-10-11 ping -l 480 -t 192.168.0.125</pre>
UNIX/Linux/Mac syntax	<pre>arp -s <IP Address> <MAC> ping -s 480 < IP Address > Example: arp -s 192.168.1.125 11-40-8c-18-10-11 ping -s 480 192.168.0.125</pre>
Win7 syntax	<pre>netsh i i show in netsh -c "i" add neighbors ldx <IP Address> <MAC> ping -l 480 -t < IP Address > Example: netsh i i show in netsh -c "i" add neighbors 12 192.168.1.125 11-40-8c-18-10-11 ping -l 480 -t 192.168.1.125</pre>

- Power off the Device and then restart it, or restart the Device over the network.
- Check the PC command line. If there is information such as "Reply from 192.168.1.125...", it means the configuration succeeds. In this case, you can close the command editor.
- Enter `http://<IP address>` in the browser address bar to log in.

5.2.2 Port

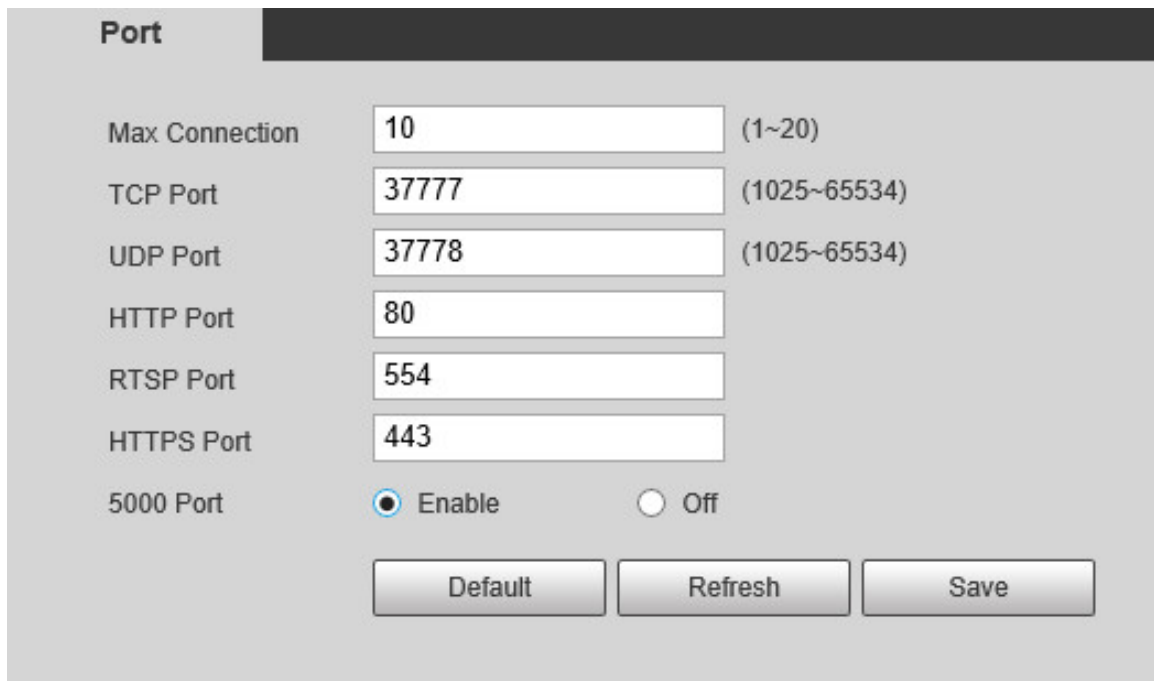
Background Information

You can configure the maximum port numbers and values on this page.

Procedure

Step 1 Select **Setting** > **Network** > **Port**.

Figure 5-38 Port page





Step 2 Configure each port value of the Device.



- Except **Max Connection**, modifications of other parameters will take effect after restart.
- 0–1024, 1900, 3800, 5000, 5050, 9999, 37776, 37780–37880, 39999, and 42323 are occupied for specific uses.
- It is not recommended to use the default values of other ports during port configuration.

Table 5-16 Description of port parameters

Parameter	Description
Max Connection	The maximum number of users that can log in to the webpage of the Device simultaneously. The value ranges from 1 to 10, and it is 10 by default.
TCP Port	TCP service port. The value is 37777 by default. You can set this parameter as needed.
UDP Port	User Datagram Protocol port. The value is 37778 by default. You can set this parameter as needed.
HTTP Port	HTTP communication port. The value is 80 by default. You can set this parameter as needed.

Parameter	Description
RTSP Port	<p>Real Time Streaming Protocol port. Keep the default value 554 if it is displayed. If you play live view through Apple's QuickTime or VLC, the following format is available. This function is also supported by Blackberry mobile phone.</p> <p>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.</p> <p>When playing live view with Blackberry mobile phone, you need to disable the audio, and then set the stream encoding mode to H.264B and resolution to CIF.</p> <p>URL format example:</p> <pre>rtsp://username:password@ip:port/cam/realmonitor?channel=1&subtype=0</pre> <ul style="list-style-type: none"> ● Username: Your username. For example, admin. ● Password: Your password. For example, admin. ● IP: Your device IP. For example, 192.168.1.122. ● Port: Leave it if the value is 554 by default. ● Channel: Channel number starting from 1. For example, if it is channel 2, then enter channel=2. ● Subtype: stream type. The main stream is 0 (subtype=0); the sub stream is 1 (subtype=1). <p>For example, if you require the sub stream of channel 2 from a certain device, then the URL shall be:</p> <pre>rtsp://admin:admin@192.168.1.123:554/cam/realmonitor?channel=2&subtype=1</pre> <p>If certification is not required, you do not need to specify the username and password. Use the following format:</p> <pre>rtsp://ip:port/cam/realmonitor?channel=1&subtype=0</pre>
RTMP	<p>A network protocol for real-time data communication. The value is 1935 by default. You can enter the value as needed.</p> <p> Enable RTMP to push audio and video data to the third-party server. Make sure that the address is trusted; otherwise it might cause data leakage.</p>
HTTPS Port	<p>HTTPS communication port. The value is 443 by default. You can set this parameter as needed.</p>
5000 Port	<p>The port is disabled by default. If you need to connect the Camera to intelligent transportation box through 5000 port, enable this port.</p> <p> There might be network risk if the port is enabled. Be cautious.</p>

Step 3 Click **Save**.

5.2.3 PPPoE

Background Information

You can enable PPPoE (Point-to-Point Protocol over Ethernet) to establish network connection. In this case, the Device obtains a dynamic IP address. To use this function, you need to obtain the PPPoE username and password from the Internet Service Provider (ISP).

Procedure

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

Figure 5-39 PPPoE page (1)

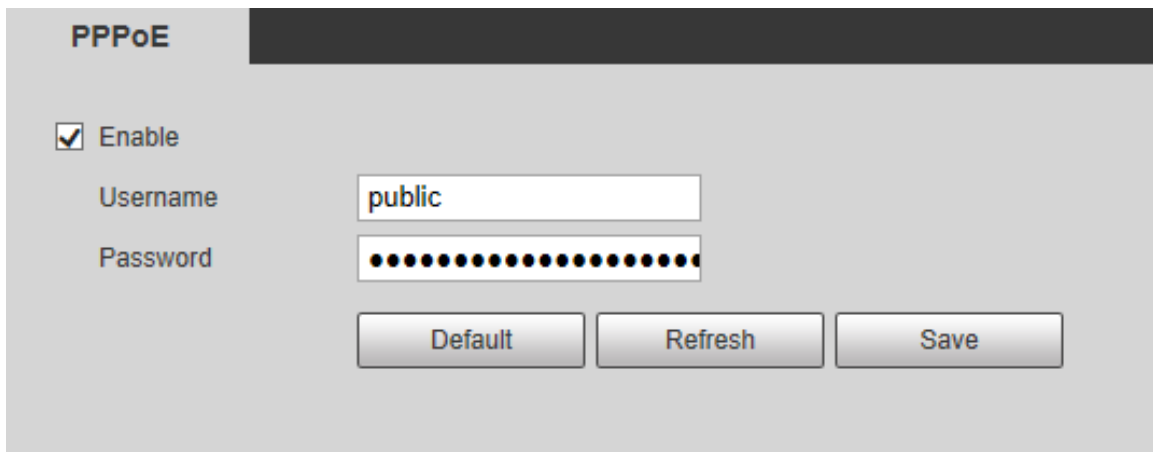


Step 2 Select **Enable**, and then enter PPPoE username and password.

Step 3 Click **Save**.

Save Succeeded! is displayed, and the obtained IP address of public network is displayed in real time. You can access the Device through the IP address.

Figure 5-40 PPPoE page (2)



5.2.4 DDNS

Background Information

Properly configure DDNS, and then the domain name on the DNS server matches your IP address and refresh the matching relation in real time. You can always access your device with the same domain name no matter how much your device IP address changes. Before making any changes, check whether your device supports the DNS server.

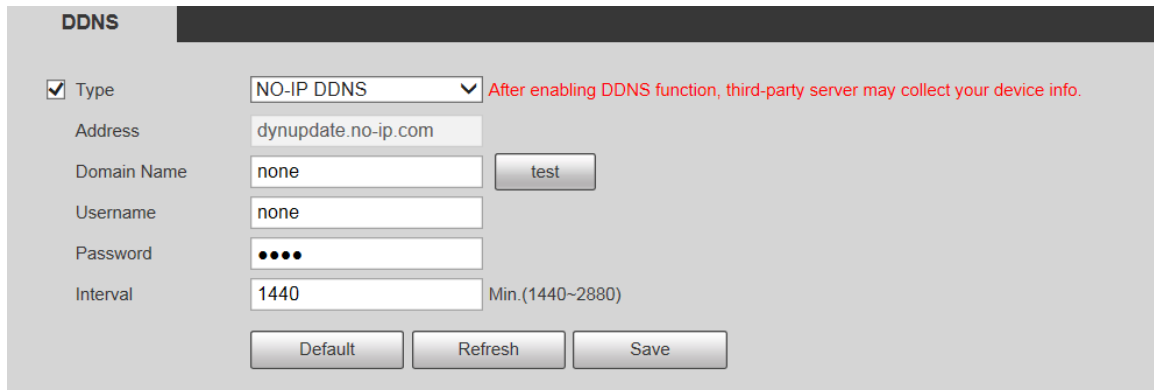


- The third party servers might collect your device information if DDNS is enabled.
- Register and log in to the DDNS website, and then you can view the information of all the connected cameras in your account.

Procedure

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

Figure 5-41 DDNS



Step 2 Select **Type**, and then configure DDNS parameter.

Table 5-17 Description of DDNS parameter

Parameter	Description
Type	The name and website of the DDNS service provider. Here is the matching relationship. <ul style="list-style-type: none"> • CN99 DDNS Server address: www.3322.org • NO-IP DDNS Server address: dynupdate.no-ip.com • Dyndns DDNS Server address: members.dyndns.org
Server Address	
Domain Name	
Username	
Password	Enter the username and password obtained from DDNS service provider. You need to register an account (including username and password) on the website of DDNS service provider.
Interval	The update cycle of the connection between your device and the server, and the time is 10 minutes by default.

Step 3 Click **Save**.

Open the browser, enter the domain name in the address bar, and then press the Enter key. The login page is displayed.

5.2.5 SMTP (Email)

After this function is enabled, the device data will be sent to the given server. There is data leakage risk. Think twice before enabling the function.

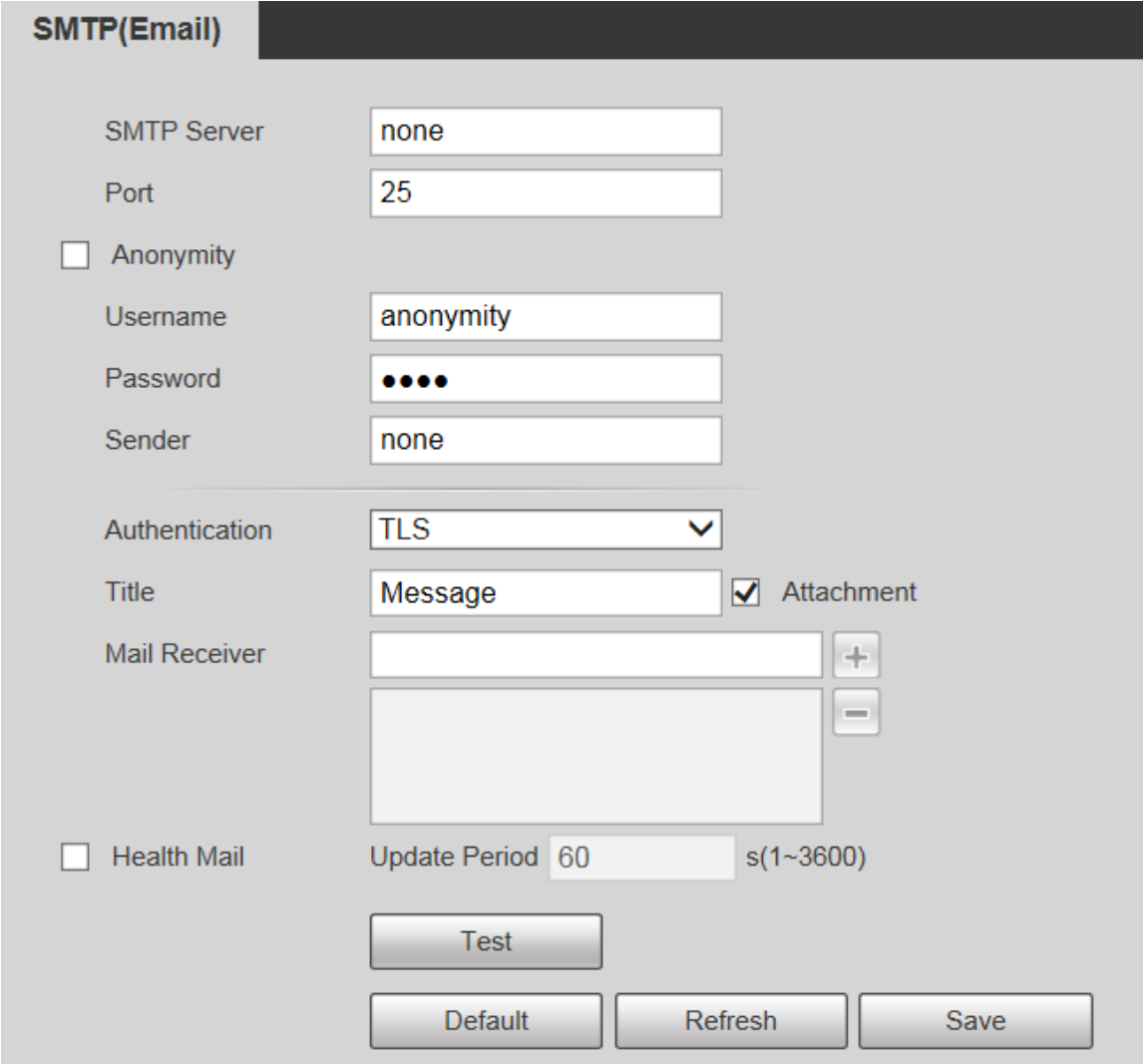
Background Information

After you configure **SMTP (Email)**, when alarms, video detection and abnormal events are triggered, an email will be sent to the recipient server through SMTP server. The recipient can log in to the incoming mail server to receive emails.

Procedure

Step 1 Select **Setting** > **Network** > **SMTP (Email)**.

Figure 5-42 SMTP (Email)



SMTP(Email)

SMTP Server: none

Port: 25

☐ Anonymity

Username: anonymity

Password: ••••

Sender: none

Authentication: TLS

Title: Message ☒ Attachment

Mail Receiver: + -

☐ Health Mail

Update Period: 60 s(1~3600)

Test

Default Refresh Save

Step 2 Configure SMTP (Email) parameter.

Table 5-18 Description of SMTP (Email) parameter





Parameter	Description	
SMTP Server	IP address of the outgoing mail server complying with SMTP protocol.	 For the detailed configuration, see Table 5-19 .
Port	Port number of the outgoing mail server complying with SMTP protocol. It is 25 by default.	
Username	Username of sender mailbox.	
Password	Password of sender mailbox.	
Anonymity	For servers supporting anonymous email, you can log in anonymously without entering username, password, and sender information.	
Sender	Email address of the sender.	
Authentication	Select authentication type from None , SSL and TLS . TLS is selected by default.  <ul style="list-style-type: none">For the detailed configuration, see Table 5-19 .There might be risks if you select the authentication type other than TLS. TLS is recommended.	
Title	You can enter no more than 63 characters in Chinese, English, and Arabic numerals.	
Mail Receiver	Email address of the receiver. Support 3 addresses at most.	
Attachment	Select the checkbox to support attachment in the email.	
Health Mail	The system sends test mail to check if the connection is successfully configured. Select the Health Mail checkbox and configure the Update Period , and then the system sends test mails according to the defined period.	
Test	Test whether the email function is normal. If the configuration is correct, the email address of the receiver will receive the test email. Save the email configuration before running rest.	

Table 5-19 Description of common email configuration

Type	SMTP Server	Authentication	Port	Description
QQ	smtp.qq.com	SSL	465	<ul style="list-style-type: none">● The authentication type cannot be None.● You need to enable SMTP service in your mailbox.● The authentication code is required; either the QQ password or email password is not applicable.  <div>Authentication code is the code you receive when enabling SMTP service.</div>
		TLS	587	
163	smtp.163.com	SSL	465/994	<ul style="list-style-type: none">● You need to enable SMTP service in your mailbox.● The authentication code is required; the email password is not applicable.  <div>Authentication code is the code you receive when enabling SMTP service.</div>
		TLS	25	
		—		
Sina	smtp.sina.com	SSL	465	You need to enable SMTP service in your mailbox.
		—	25	
126	smtp.126.com	—	25	You need to enable SMTP service in your mailbox.

Step 3 Click **Save**.

5.2.6 UPnP



After UPnP is enabled, Intranet service and port of the Device will be mapped to Extranet. Think twice before enabling it.

UPnP (Universal Plug and Play) allows you to establish the mapping relationship between Intranet and Extranet. Extranet users can access Intranet device by visiting Extranet IP address. Intranet port is device port and Extranet port is router port. Users can access the Device by accessing Extranet port. When you are not using routers for UPnP, disable UPnP to avoid affecting other functions.

Once UPnP is enabled, the Device supports UPnP protocol. In Windows XP or Windows Vista, after UPnP is enabled, the Device can be automatically searched by Windows network.

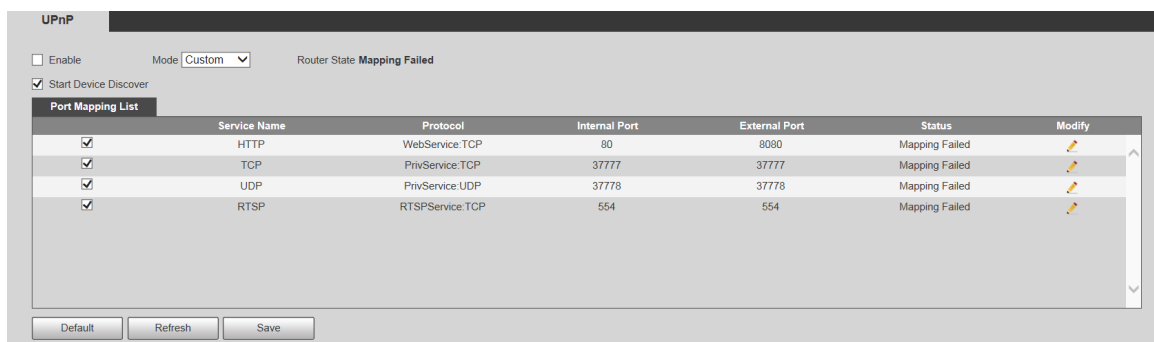
Adding UPnP Network Service in Windows System

1. Open **Control Panel** , and then select **Add or Remove Programs**.
2. Click **Add/Remove Windows Components**.
3. Select **Network Service** from the **Windows Components Wizard** and click **Details** button.
4. Select **Internet Gateway Device Discovery and Control Client** , and **UPnP User page** , and then click **OK** to start installation.

Configuring UPnP

1. Select **Setting** > **Network** > **UPnP**.

Figure 5-43 UPnP



	Service Name	Protocol	Internal Port	External Port	Status	Modify
<input checked="" type="checkbox"/>	HTTP	WebService.TCP	80	8080	Mapping Failed	
<input checked="" type="checkbox"/>	TCP	PrivService.TCP	37777	37777	Mapping Failed	
<input checked="" type="checkbox"/>	UDP	PrivService.UDP	37778	37778	Mapping Failed	
<input checked="" type="checkbox"/>	RTSP	RTSPService.TCP	554	554	Mapping Failed	

2. Select **Enable**.
3. Select a mode from the drop-down list.
There are 2 mapping modes: **Custom** and **Default**.
 - In **Custom** mode, users can modify the external port.
 - Select **Default**, and then the system finishes mapping with unoccupied port automatically. In this case, you do not need to modify mapping relation.
4. Select **Start Device Discover**.
5. Click **Save**.

5.2.7 Bonjour

Introduction

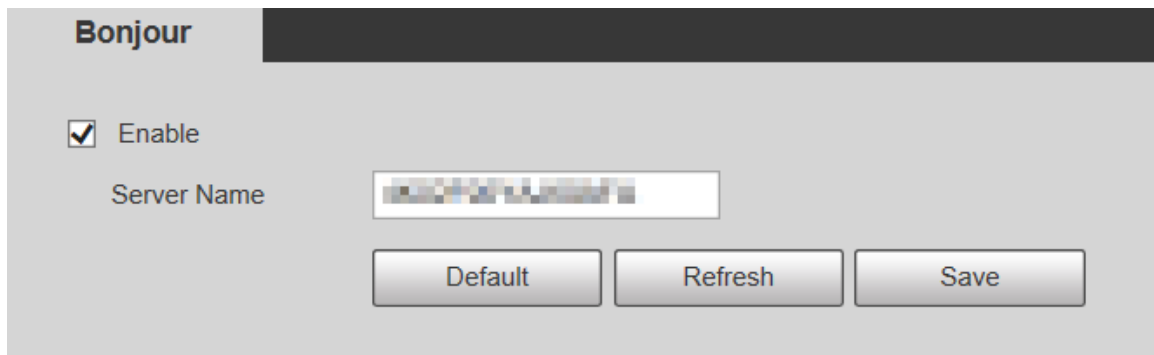
Bonjour is also called zero-configuration networking, which can automatically discover computers, devices and services on IP networks. Bonjour is a protocol of industry standard which allows devices to search and find each other. IP address or DNS server is not required during the process.

Enable this function, and the network camera will be automatically detected by the OS and client with Bonjour function. When the network camera is automatically detected by Bonjour, server name you have set will be displayed.

Configuring Bonjour

1. Select **Setting** > **Network** > **Bonjour**.

Figure 5-44 Bonjour page



2. Select **Enable**, and then set **Server Name**.
3. Click **Save**.

Visiting Webpage with Safari Browser

In the OS and clients that support Bonjour, perform the following steps to visit the webpage of the Device with Safari browser.

1. Click **Show all bookmarks** in Safari.
2. The OS or client automatically detects the network cameras with Bonjour enabled in the LAN.
3. Click to visit the corresponding webpage.

5.2.8 SNMP

After setting SNMP (Simple Network Management Protocol) and connect to the Device through certain software (such as MIB Builder and MG-SOFT MIB Browser), you can manage and monitor devices with the software.

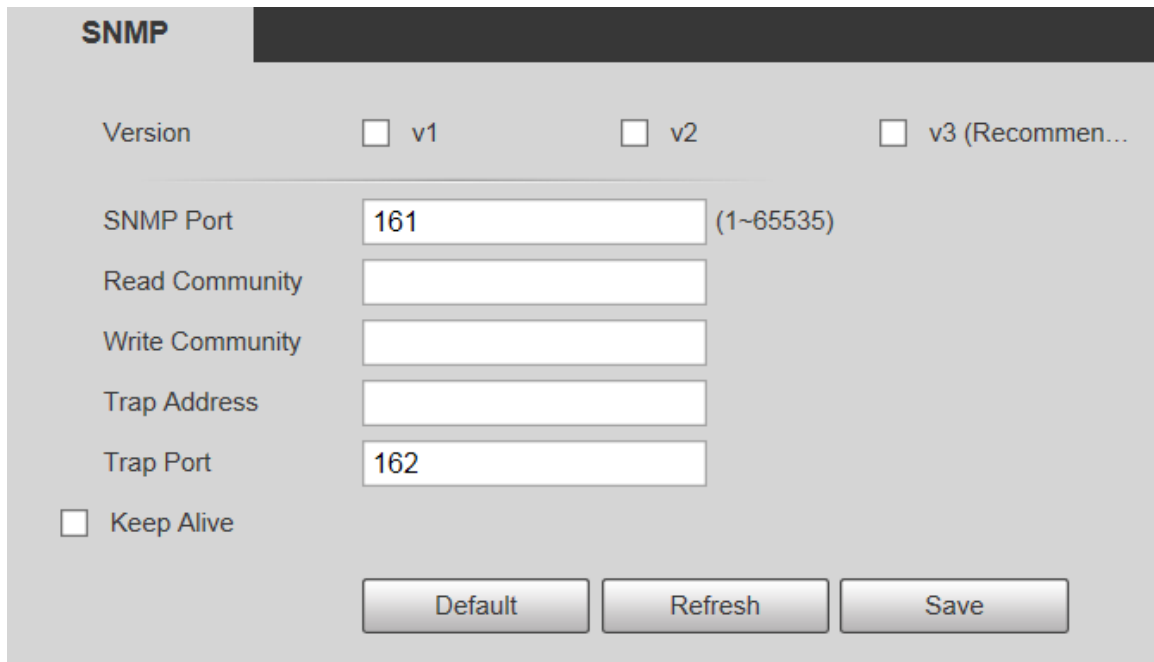
Prerequisites

- Install SNMP monitoring and management tool, such as MIB Builder and MG-SOFT MIB Browser.
- Obtain MIB files corresponding to the current version from the technical personnel.

Procedure

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

Figure 5-45 SNMP (1)

The image shows a web-based configuration interface for SNMP. It has a title bar "SNMP" in a dark grey box. Below the title bar, there are three radio buttons for "Version": "v1", "v2", and "v3 (Recommen...". The "v1" option is selected. Below the version options, there are five text input fields: "SNMP Port" (containing "161"), "Read Community" (empty), "Write Community" (empty), "Trap Address" (empty), and "Trap Port" (containing "162"). To the right of the "SNMP Port" field is a range indicator "(1~65535)". Below the input fields, there is a checkbox labeled "Keep Alive" which is currently unchecked. At the bottom of the form, there are three buttons: "Default", "Refresh", and "Save".

SNMP

Version ☐ v1 ☐ v2 ☐ v3 (Recommen...

SNMP Port (1~65535)

Read Community

Write Community

Trap Address

Trap Port

☐ Keep Alive

Figure 5-46 SNMP (2)

SNMP

Version

☐ v1
☐ v2
☒ v3 (Recommen...

SNMP Port

161

(1~65535)

Read Community

Write Community

Trap Address

Trap Port

162

☐ Keep Alive

Read-only Username

public

Authentication Type

☒ MD5
☐ SHA

Authentication Pass...

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...

private

Authentication Type

☒ MD5
☐ SHA

Authentication Pass...

The minimum pass phrase length is 8 characters

Encryption Type

☒ CBC-DES

Encryption Password

The minimum pass phrase length is 8 characters

Default


Refresh




Save

Step 2 Select a version to enable SNMP.

In the **Trap Address** field, enter the IP address of the PC that has MG-SOFT MIB Browser installed, leaving other parameters to the default values.

Table 5-20 SNMP parameter description

Parameter	Description
Version	<p>Select the check box of the version you need, and the system can process information of the corresponding version.</p> <ul style="list-style-type: none"> 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 need to set the username, password, and authentication type to visit your device from the server. <p> V1 and V2 might cause data leakage, and V3 is recommended.</p>

Parameter	Description
SNMP Port	The listening port of the software agent in the Device.
Read Community/ Write Community	<p>The read and write community strings that the software agent supports.</p> <p> The name can only consist of number, letter, underline (_), and strikethrough (-).</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.
Keep Alive	Select the Keep Alive checkbox, and the system can send data package to ensure network connection without interruption.
Read-only Username	<p>The name is public by default.</p> <p> The username can only consist of number, letter, and underline.</p>
Read&write Username	<p>The name is private by default.</p> <p> The username can only consist of number, letter, and underline.</p>
Authentication Type	You can select from MD5 and SHA , and it is MD5 by default.
Authentication Password	It shall be no less than 8 digits.
Encryption Type	It is CBC-DES by default.
Encryption Password	It shall be no less than 8 digits.

Step 3 Click **Save**.

Step 4 View device information.

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. Expand 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 operating system (OS) and disable SNMP Trap service. The MG-SOFT MIB Browser will display prompt when an alarm is triggered.

5.2.9 Multicast

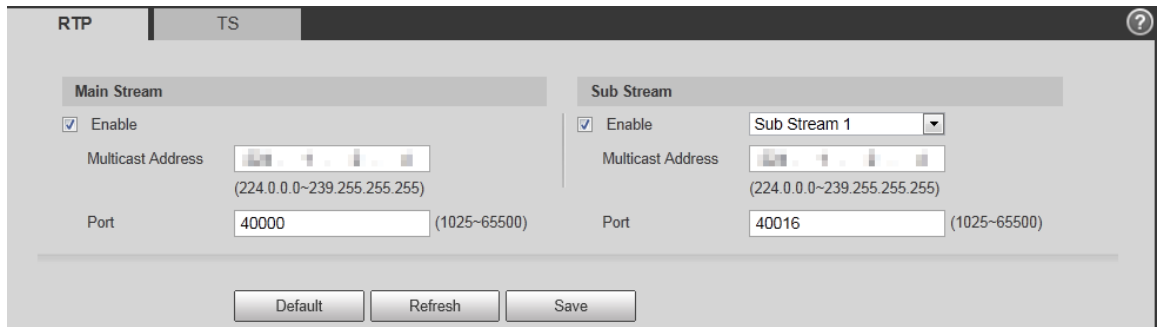
You can access the Device by network to see live view. If the access times exceed its upper limit, preview might fail. You can set multicast IP to access by multicast protocol to solve the problem. The Device supports two multicast protocols: **RTP** and **TS**. RTP is enabled by default when main stream and sub stream are used. TS is disabled by default.

5.2.9.1 RTP

Procedure

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

Figure 5-47 RTP page



Step 2 Enable main stream or sub stream.

Step 3 Enter multicast address and port number.

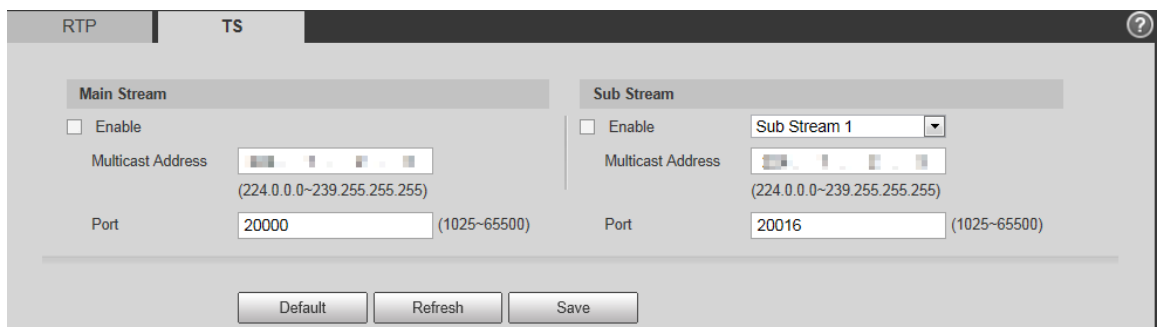
Step 4 Click **Save**.

5.2.9.2 TS

Procedure

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

Figure 5-48 TS page



Step 2 Enable main stream or sub stream.

Step 3 Enter multicast address and port number.

Step 4 Click **Save**.

5.2.10 Auto Register

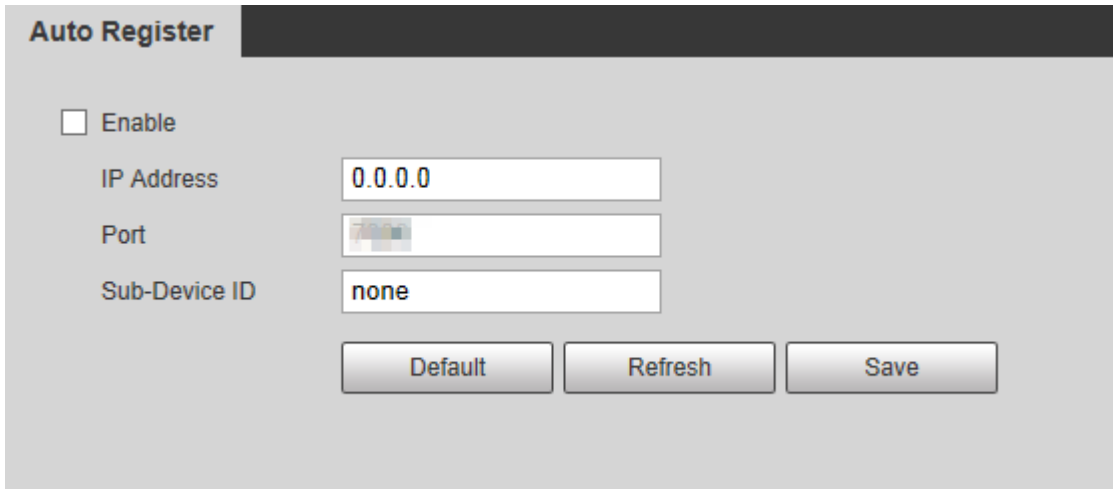
Background Information

After you enable this function, when the Device is connected to 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 Device.

Procedure

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

Figure 5-49 Auto register



Step 2 Select the **Enable** checkbox to enable **Auto Register**.

Step 3 Enter **IP Address** , **Port** and **Sub-Device ID**.

Table 5-21 Description of auto register parameters

Parameter	Description
IP Address	The IP address of server that needs to be registered to.
Port	The port for auto-registration.
Sub-Device ID	Sub device ID assigned by server.

Step 4 Click **Save**.

5.2.11 Wi-Fi

Devices with Wi-Fi function can access network through Wi-Fi.



- Wi-Fi and WPS are available on select models.
- All devices with WPS button support WPS function.

5.2.11.1 Wi-Fi Settings

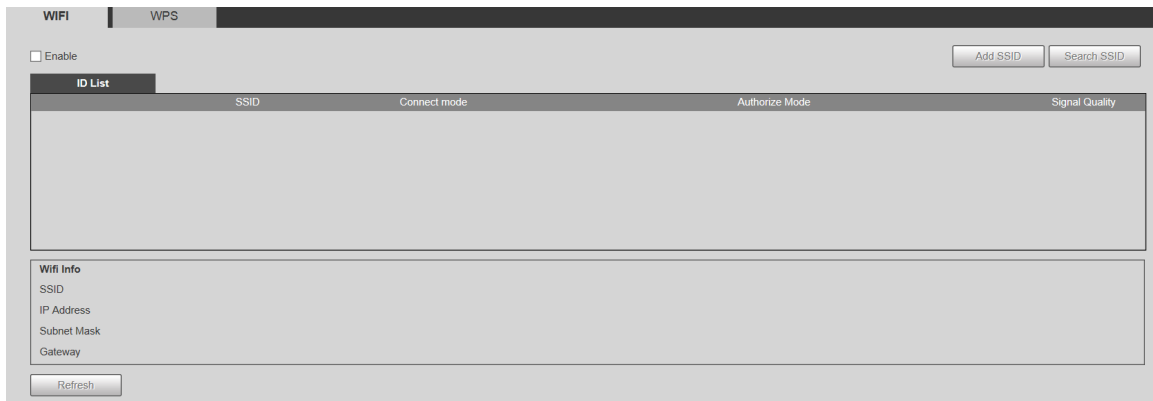
Background Information

The name, status and IP information of current hotspot are displayed in the Wi-Fi information bar. Click **Refresh** after reconnection to make sure that the operating status is displayed in real time. Connecting Wi-Fi hotspot takes some time depending on network signal strength.

Procedure

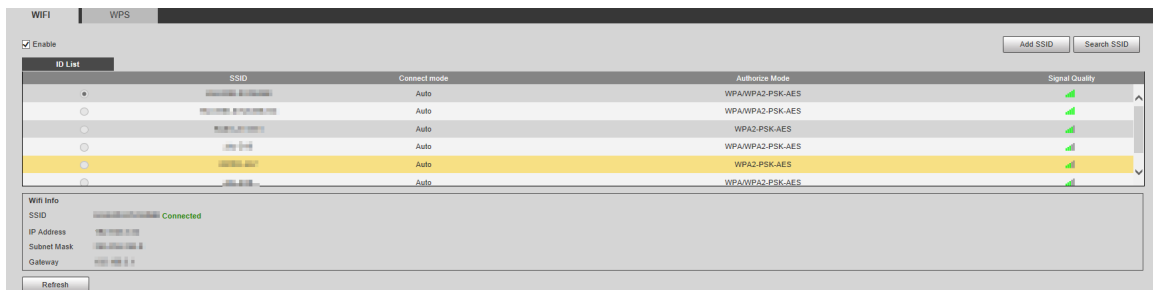
Step 1 Select the **Enable** checkbox.

Figure 5-50 Wi-Fi settings (1)



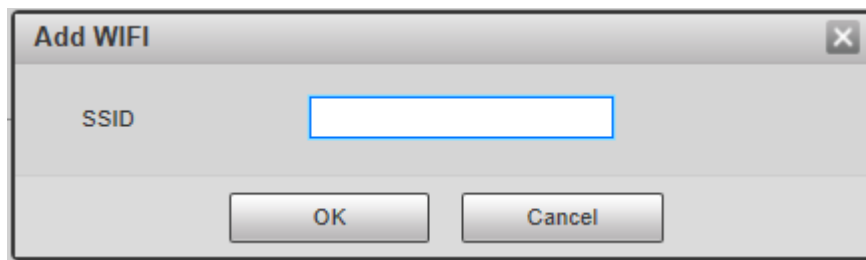
Step 2 Click **Search SSID**, and Wi-Fi hotspots in the environment of current network camera are displayed.

Figure 5-51 Wi-Fi settings (2)



Step 3 To manually add Wi-Fi, click **Add SSID**.

Figure 5-52 Add Wi-Fi



Step 4 Enter a network name in the dialog box.



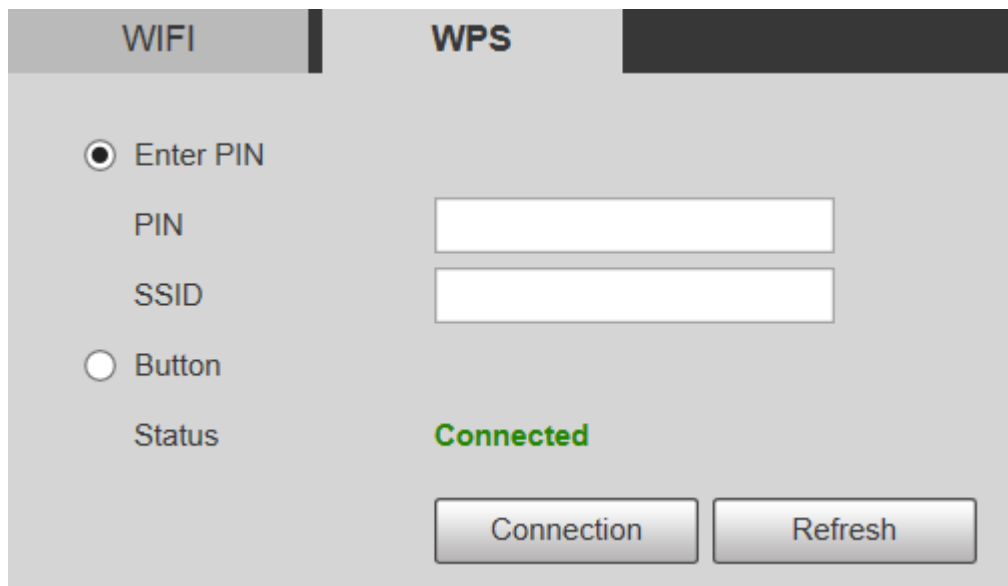
It is recommended to set a secure encryption method for the Device to connect routers.

Step 5 Double-click one hotspot to display the **Signal Quality** and the **Authentication Manner**.

- If the password is required, enter the password. When entering the password, its index number shall be consistent with that on the router.
- Click **Connection** if password is not required.

5.2.11.2 WPS Settings

Figure 5-53 WPS settings



PIN and SSID can be obtained from the router. Enter PIN and SSID, and then click **Refresh** to display operating status in real time.

5.2.11.3 AP Settings

Background Information

You can use the Camera as wireless AP (Access Point), and other devices such as mobile phones can connect to the Camera by searching for the network name. You can then log in to the Camera through the browser on your device. At most 5 accounts can log in to the Camera at the same time. AP and Wi-Fi cannot be both enabled at the same time, and AP is disabled by default.

Procedure

- Step 1** Select **Setting** > **Network** > **WIFI** > **AP**.
- Step 2** Select **Enable**, and then set AP information.

Figure 5-54 AP settings



Table 5-22 AP parameter description

Parameter	Description
SSID	The default name is "device serial number_SD".
Frequency Band	Both 2.4G and 5G are available.

Parameter	Description
Verification Type	It is WPA2 PSK by default, and cannot be changed.
Connection Password	Set the connection password which is required when other devices connect to the Camera. It is 12345678 by default.
Host IP	Displays the IP address of AP.

Step 3 Click **Save**.

Results

1. Open your device such as mobile phone, search for the network name of the AP in the wireless signal list, and then connect to the network.

After it is successfully connected, the IP address and MAC address of the device is displayed on the **AP** page.

2. Open a browser on your device, enter the host IP on the **AP** page or IP address on the **TCP/IP** page, and then you can go to the login page of the Camera.
3. Enter the username and password, and then log in to the Camera.



Live view is available on select devices.

5.2.12 802.1x

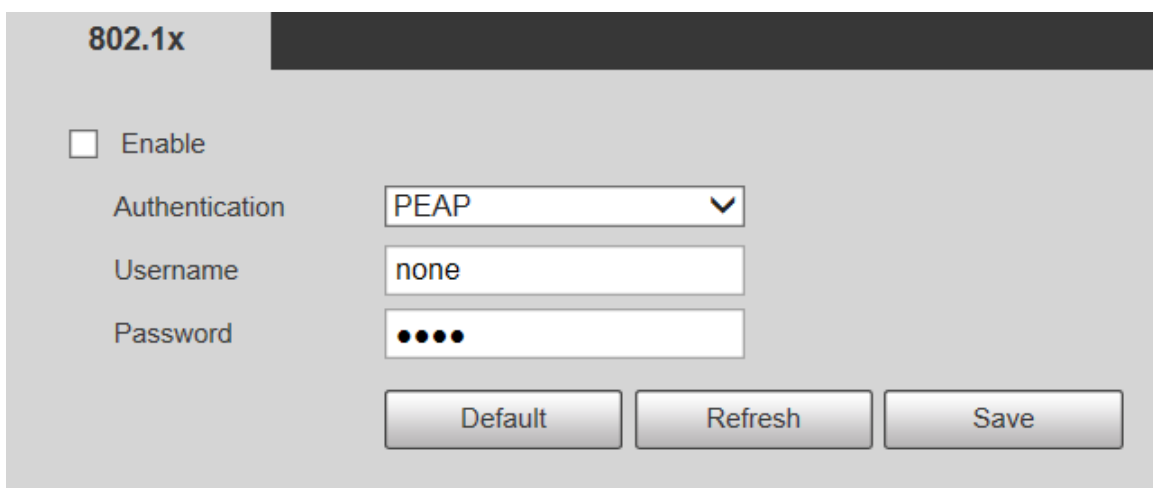
Background Information

802.1x is a port-based network access control protocol. It allows users to manually select authentication mode to control device access to LAN, and meet authentication, billing, safety and management requirements of the network.

Procedure

Step 1 Select **Setting** > **Network** > **802.1x**.

Figure 5-55 802.1x ipage



Step 2 Select the **Enable** checkbox to enable **802.1x**.

Step 3 Select an authentication mode, and then enter username and password.

Table 5-23 Description of 802.1x setting parameter

Parameter	Description
Authentication	PEAP (protected EAP protocol).
Username	The username that was authenticated on the server.
Password	Corresponding password.

Step 4 Click **Save**.

5.2.13 QoS

Background Information

QoS (Quality of Service) is a network security mechanism, and is also a technology to solve network delay, congestion, and other problems.

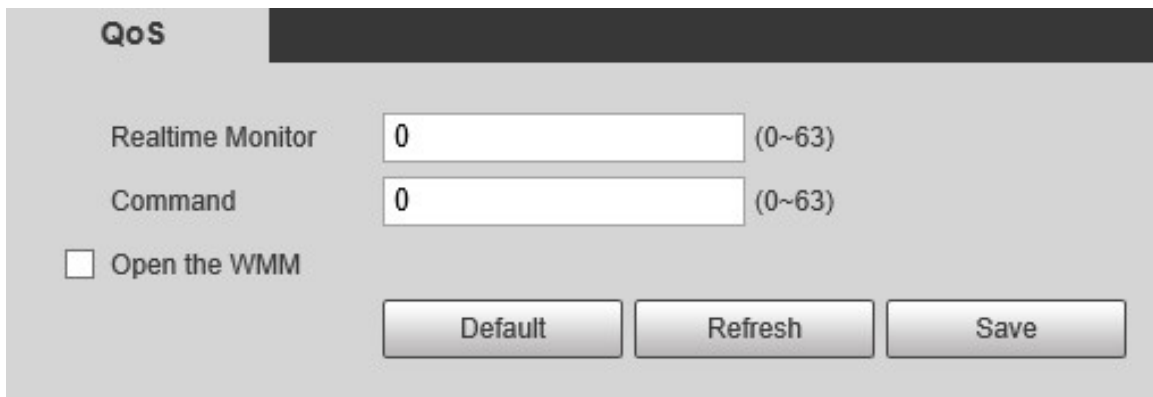
For network business, QoS includes transmission bandwidth, time delay in transmission, and packet loss of data. In network, QoS can be improved by ensuring transmission bandwidth, and reducing time delay in transmission, packet loss rate, and delay jitter.

For DSCP (Differentiated Services Code Point), there are 64 priority degrees (0–63) of data packets. 0 represents the lowest priority, and 63 the highest priority. Based on the priority, the packets are classified into different groups. Each group occupies different bandwidth and has different discard percentage when there is congestion so as to improve service quality.

Procedure

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

Figure 5-56 QoS page



Step 2 Configure QoS setting parameters.

Table 5-24 Description of QoS setting parameter

Parameter	Description
Realtime Monitor	Data packet of network video monitoring. The value ranges from 0 to 63.
Command	Data packet of device configuration and query. The value ranges from 0 to 63.
Open the WMM	Select the checkbox to enable wireless QoS.

Step 3 Click **Save**.

5.2.14 4G/5G

After installing SIM card, you can connect the Device to 4G/5G network through dialing or mobile setting.

- Dialing setting: Connect the Device to 4G/5G network in specified period.
- Mobile setting: Receive alarm linkage messages on your mobile phone. When receiving alarm messages, you can activate the Device to connect to 4G/5G network through SMS or phone calls.



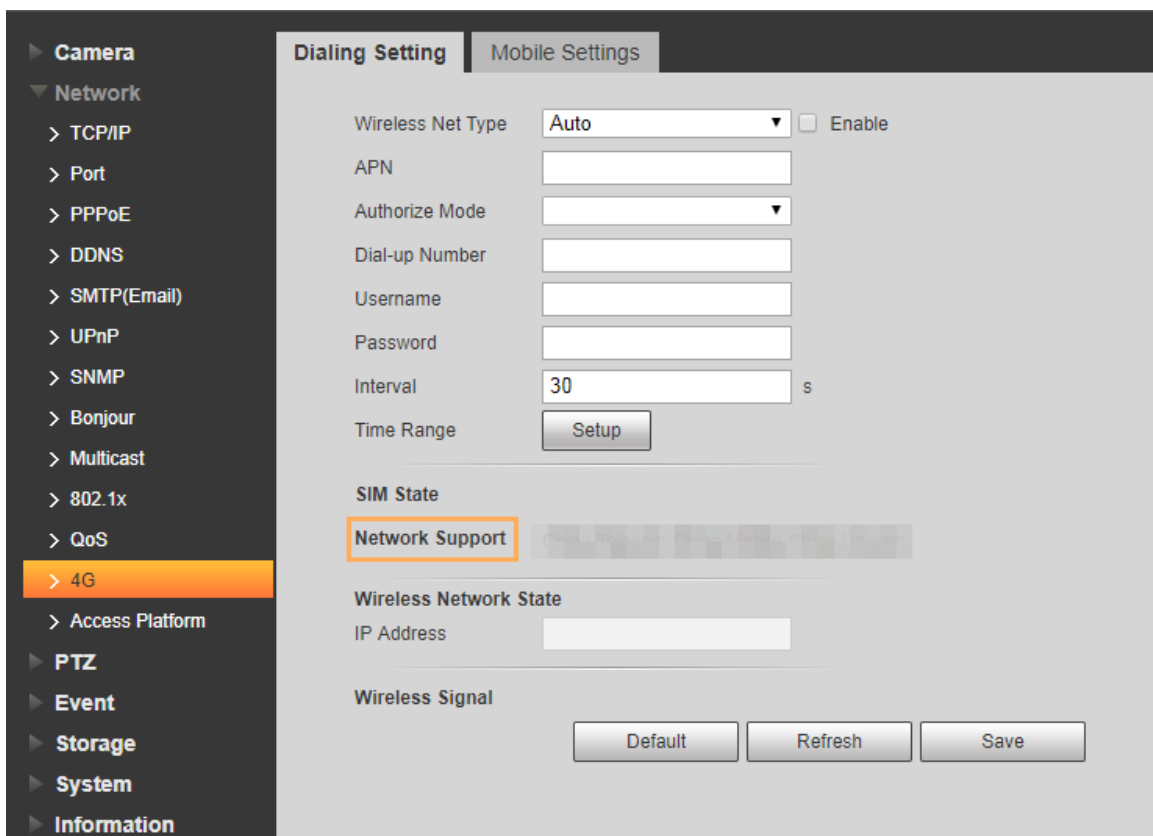
- The function is available on devices with 4G/5G module. This section uses 4G as an example.
- Dual 4G is supported by select models, but only one 4G network adapter can be enabled simultaneously.

5.2.14.1 Dialing Setting

Background Information

Log in to webpage, select **Setting** > **Network** > **4G** > **Dialing Setting**.

Figure 5-57 Dialing setting page




Some devices only support certain mobile carriers, and only the supported carriers are displayed in **Network Support**.

Procedure

Step 1 Select the **Enable** checkbox.

Step 2 Enter **APN** , **Authorize Mode**, **Dial-up Number**, **Username**, and **Password** according to the SIM card inserted.



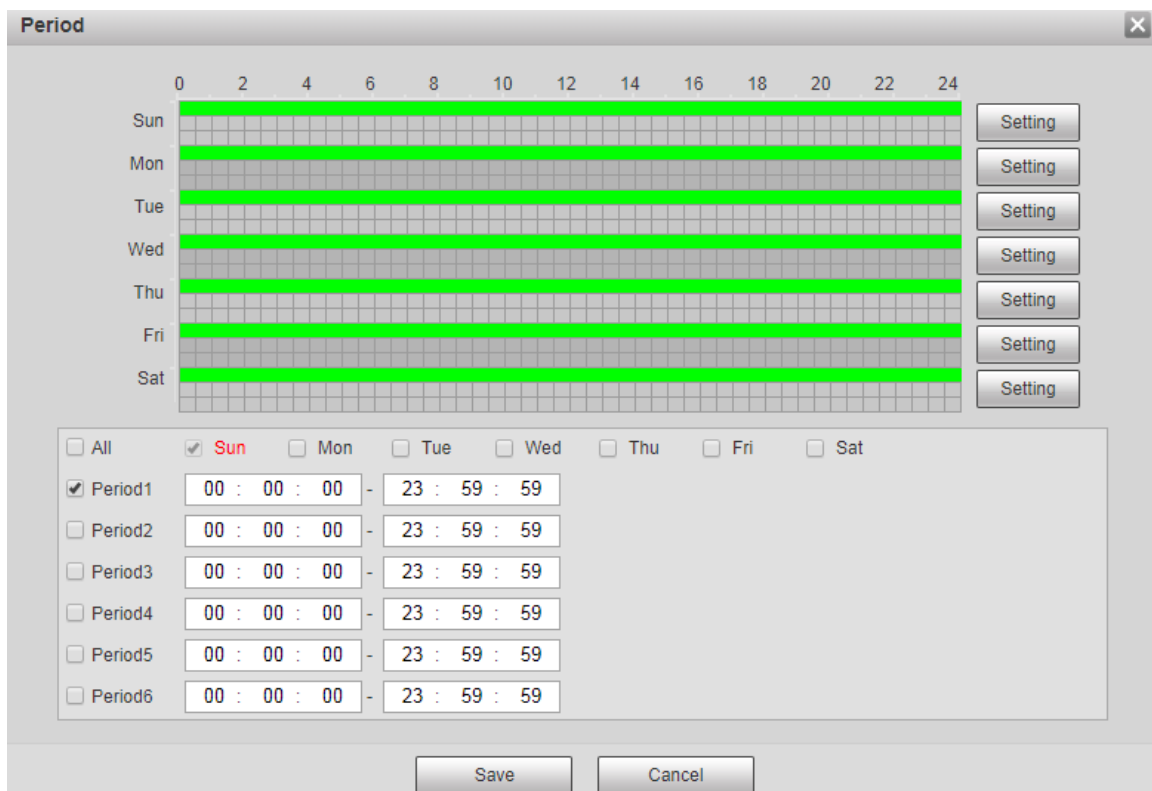
These parameters might vary by countries. Contact local carrier or customer service for details.

Step 3 Set the period to use 4G.



- If the current time is in the period you set, 4G network connection will be enabled. The IP address of the SIM card will be displayed in IP Address. And you can access the device through 4G after finishing the rest steps.
- If the current time is not in the period you set, 4G network connection will not be enabled. Only the corresponding **Wireless Signal** is displayed on the page. And you cannot access the device through 4G.

Figure 5-58 Period setting



Step 4 Set the interval to enable 4G through message or phone call if you want to use 4G outside the period set in **Step 3**.



The value range is 0–7200 s and it is 30 s by default. If the interval is 30 s, after activating 4G, you can use it for 30 s. After 30 s, you need to activate 4G again. If you set the interval to 0 s, you can use 4G without disconnection and you do not need to activate it again. For the method to activate 4G through message or phone call, see "5.2.14.2 Mobile Setting".

Step 5 Click **Save**.

5.2.14.2 Mobile Setting

Background Information

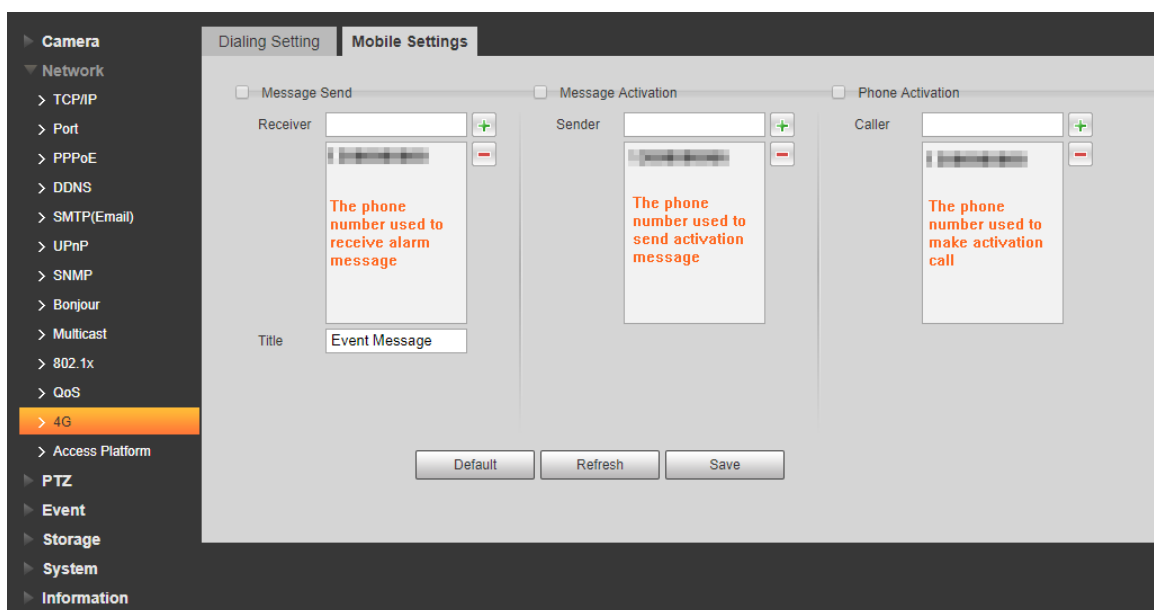
Log in to webpage, select **Setting** > **Network** > **4G** > **Mobile Settings**.

You can add the phone number to receive alarms. You also can add phone number used to activate 4G through message or phone call if you want to use 4G outside the period set in "5.2.14.1 Dialing Setting".



Make sure that you add international calling codes before the phone number to avoid unnecessary charges caused by phone calls or messages to other countries or regions.

Figure 5-59 Mobile setting page




- **Message Send** : When alarms are triggered, the phone number added will receive message.
- **Message Activation** : You can enable 4G through message outside the period you set to use 4G. You need to send "ON" or "OFF" to phone number of the SIM card in the Device. "ON" indicates enabling, and "OFF" indicates disabling.
- **Phone Activation** : You can enable 4G through phone calls outside the period you set to use 4G. You need to call the phone number of the SIM card in the Device. If the call gets through, it means 4G has been enabled.



- Make sure that your SIM card supports making phone calls and sending messages, and it can be used normally.
- Make sure that you use activation function outside the time range you set; otherwise it does not work.

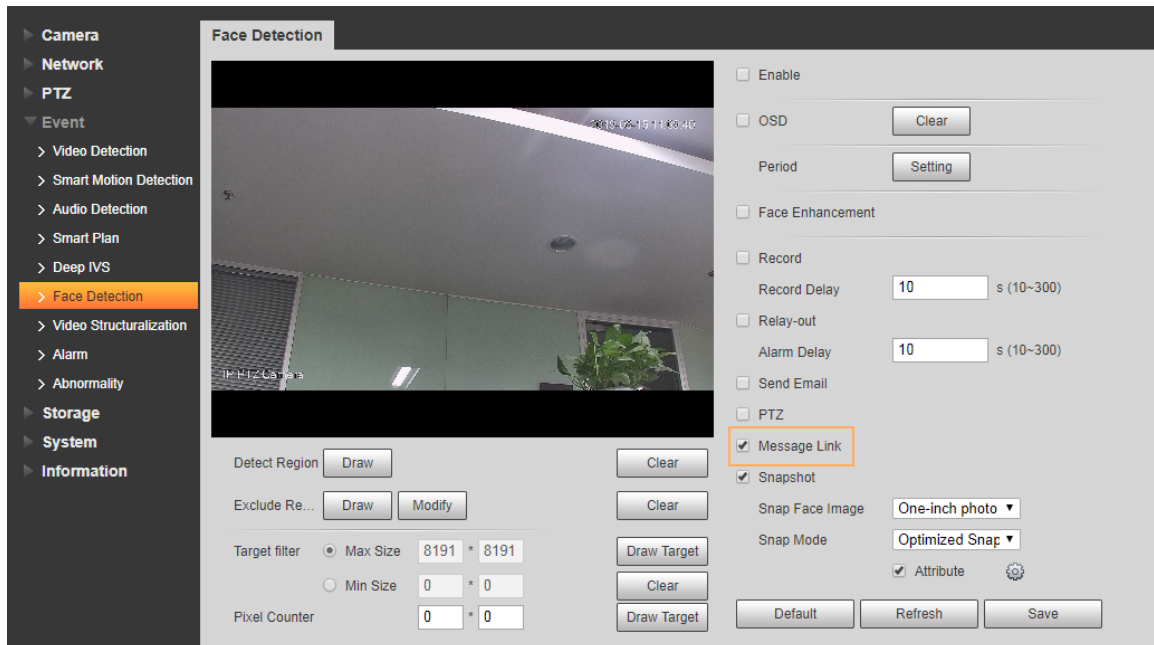
Procedure

- Step 1** Select the checkbox of the service you need to enable. You can select one or more services.
- Step 2** Enter the phone number and click  to add it.
- Step 3** Click **Save**.

Step 4 Select the **Message Link** checkbox on the page of the event for which you want to receive message.

Take Face Detection for example. Click **Setting** > **Event** > **Face Detection**, and then select the **Message Link** checkbox.

Figure 5-60 Message link



Step 5 Click **Save** on the page of the corresponding event. You will receive message if the alarm is triggered.

5.2.15 Access Platform

5.2.15.1 P2P

Background Information

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 your mobile client.

Procedure

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

Figure 5-61 P2P page



- P2P is enabled by default. You can manage the devices remotely.
- When P2P is enabled and the device is connected to network, the status is displayed as **Online**. We might collect the information including IP address, MAC address, device name, and serial number. The information collected is for remote access only. If you do not agree with this, you can clear the **Enable** checkbox.

- Step 2 Log in to mobile phone client, and then tap **Device Management**.
- Step 3 Tap **Add +** at the upper-right corner.
- Step 4 Scan the QR code on the P2P page.
- Step 5 Follow the onscreen instructions to finish settings.

5.2.15.2 ONVIF

Background Information

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 the service.

Procedure

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

Figure 5-62 ONVIF page



Step 2 Select **On** for **Authentication**.

Step 3 Click **Save**.

5.2.15.3 RTMP

Background Information

You can connect the third party platforms (such as YouTube) to play live video through RTMP protocol.

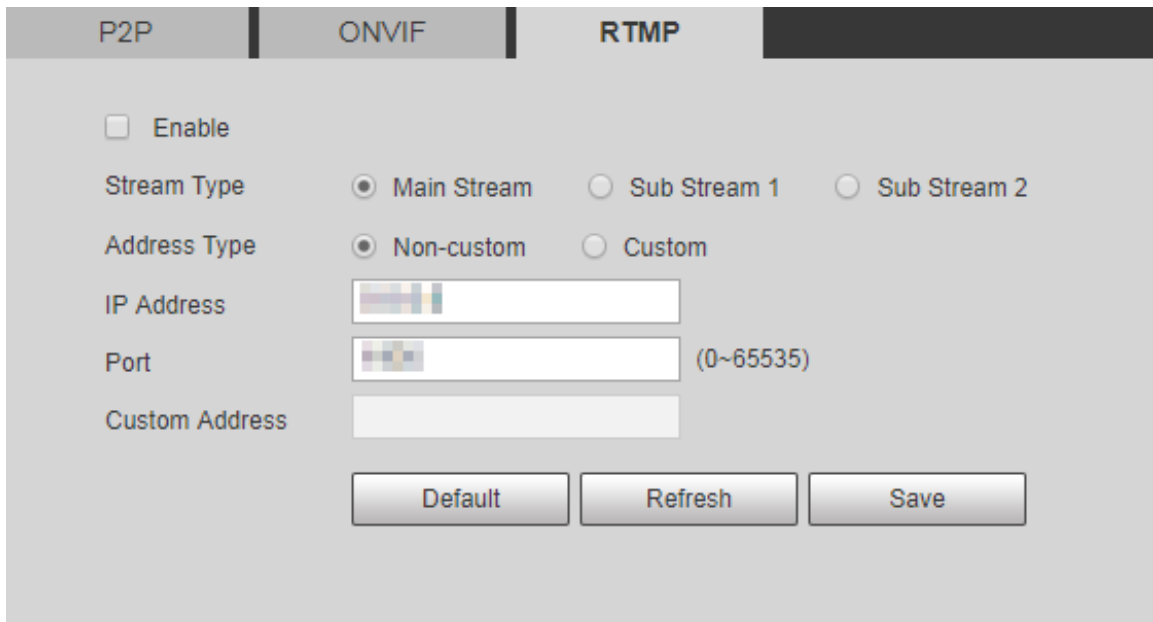


- Only admin user can configure RTMP.
- RTMP only supports H.264, H.264B and H.264H video formats, and Advanced Audio Coding (AAC) audio format.

Procedure

Step 1 Select **Setting** > **Network** > **Access Platform** > **RTMP**.

Figure 5-63 RTMP page



Step 2 Select the **Enable** checkbox to enable RTMP.



When enabling RTMP, make sure that the address can be trusted.

Step 3 Set RTMP parameters.

Table 5-25 Description of RTMP parameter configuration

Parameter	Description
Stream Type	Select live video stream type. Make sure that the video format of the stream is H.264, H.264B or H.264H, and the audio format is AAC.
Address Type	There are two options: Non-custom and Custom . <ul style="list-style-type: none"> ● Non-custom : You need to fill in the IP address or domain name. ● Custom : You need to fill in the address allocated by the server.
IP Address	If you have selected Non-custom , IP address and port need to be filled in. <ul style="list-style-type: none"> ● IP Address: IPv4 or domain name is supported. ● Port: It is recommended to use the default value.
Port	
Custom Address	If you have selected Custom , the address allocated by the server needs to be filled in.

Step 4 Click **Save**.

5.3 Bluetooth Settings

Background Information

You can connect the Camera to Bluetooth devices such as Bluetooth headset for voice broadcast of alarms and voice intercom with the platform.



The function is available on select models.

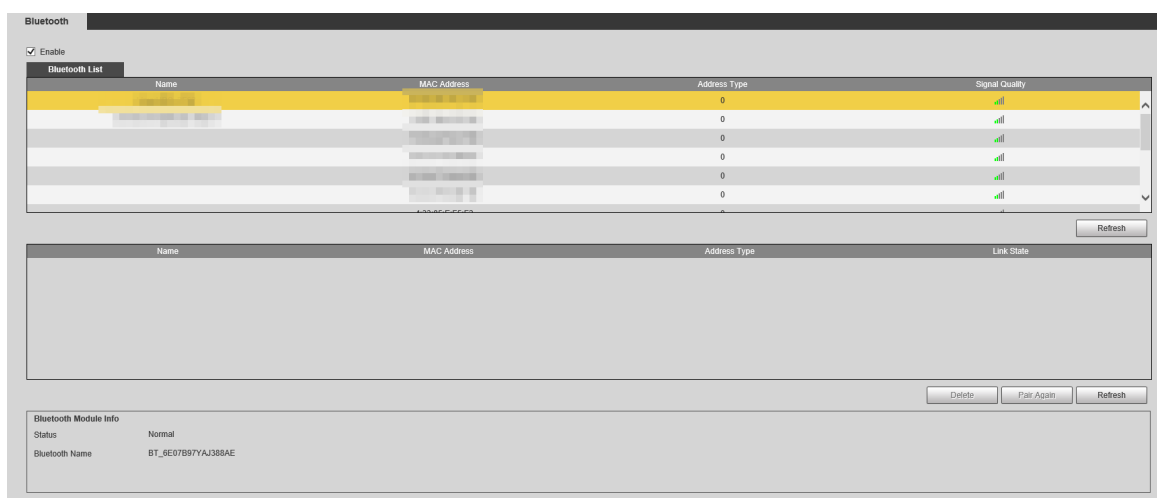
Procedure

Step 1 Select **Setting** > **Connection Settings** > **Bluetooth**.

Step 2 Select **Enable**.

The searched Bluetooth devices are displayed in the **Bluetooth List**. Click **Refresh** at the lower-right corner of the list to search for **Bluetooth** devices again.

Figure 5-64 Bluetooth list

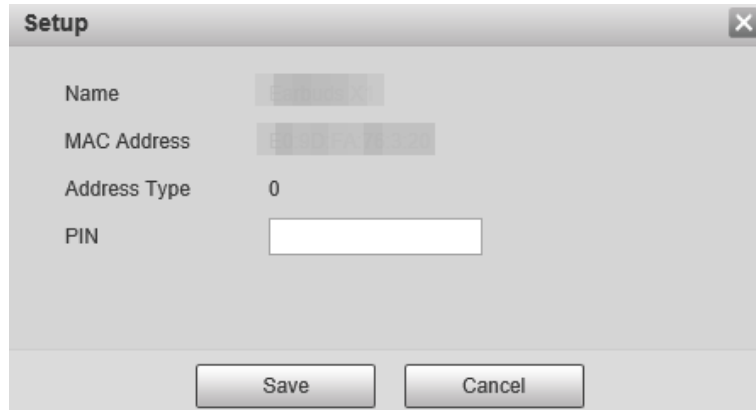


Step 3 Double-click the name of Bluetooth device, and then set PIN on the **Setup** page.



For the PIN of the Bluetooth device, see the corresponding user's manual.

Figure 5-65 Connect to Bluetooth device

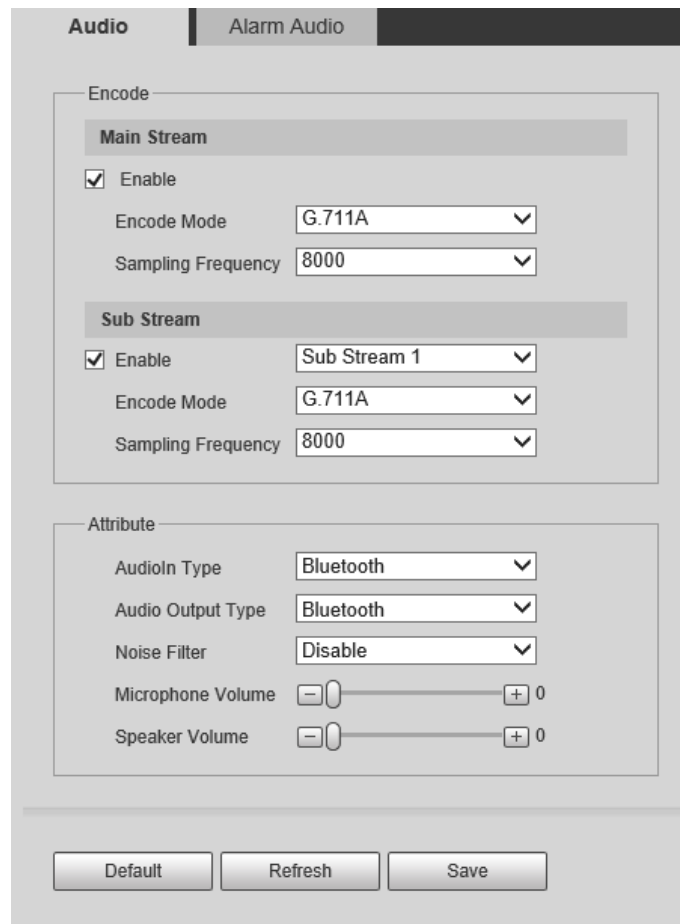


Step 4 Click **Save**.

The connected Bluetooth device is displayed in the list below.

Step 5 Select **Setting** > **Camera** > **Audio** > **Audio**, and then set audio input and audio output types to **Bluetooth**.

Figure 5-66 Set audio



Related Operations

- Click **Refresh** at the lower-right corner of the list to get information of paired Bluetooth devices again.
- Click **Pair Again** to quickly connect to Bluetooth devices paired before.
- Click **Delete** to delete the Bluetooth device.

5.4 PTZ Settings

5.4.1 Protocol



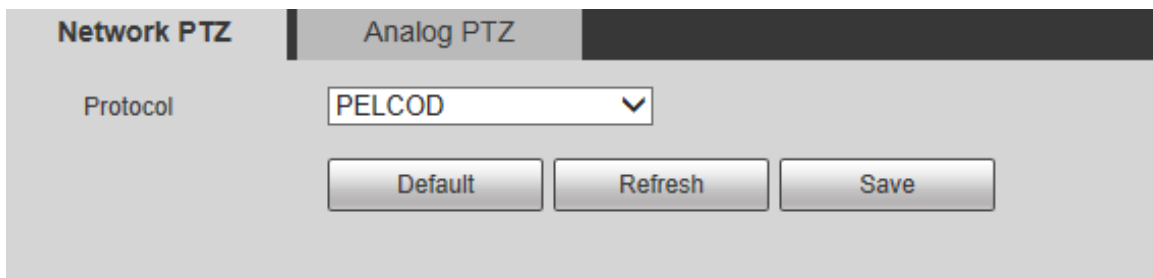
Network PTZ setting and analog PTZ setting are available on select models.

5.4.1.1 Network PTZ Settings

Procedure

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

Figure 5-67 Network PTZ setting



Step 2 Select a protocol.

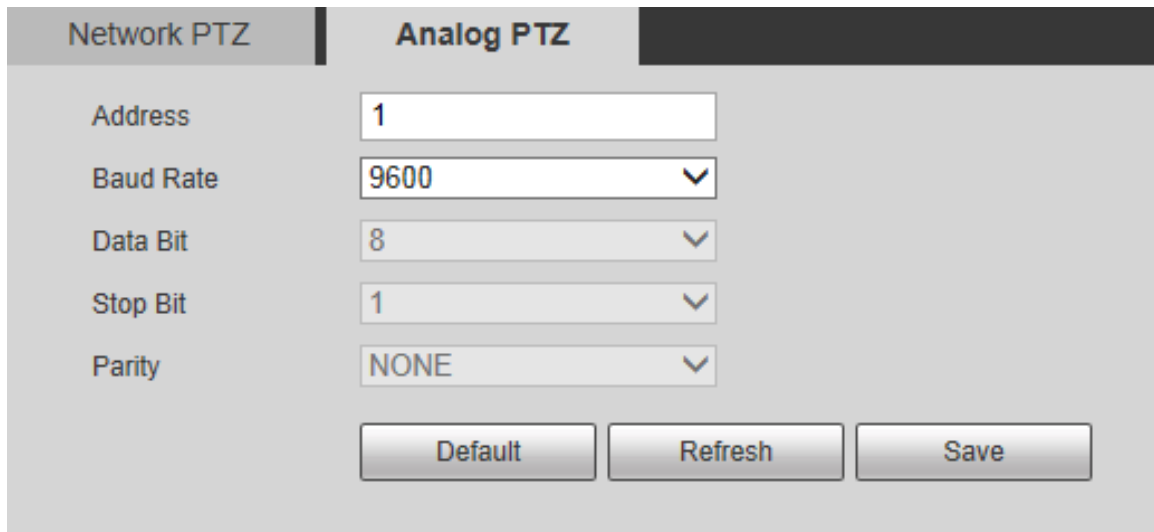
Step 3 Click **Save**.

5.4.1.2 Analog PTZ Settings

Procedure


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

Figure 5-68 Analog PTZ setting



Step 2 Configure analog PTZ parameter.

Table 5-26 Description of analog PTZ parameter

Parameter	Description
Address	Enter the address of the Device.  Make sure that the address is the same as the device address; otherwise you cannot control the device.
Baud Rate	Select the baud rate of the Device.
Data Bit	It is 8 by default.
Stop Bit	It is 1 by default.
Parity	It is NONE by default.

Step 3 Click **Save**.

5.4.2 Function

5.4.2.1 Preset

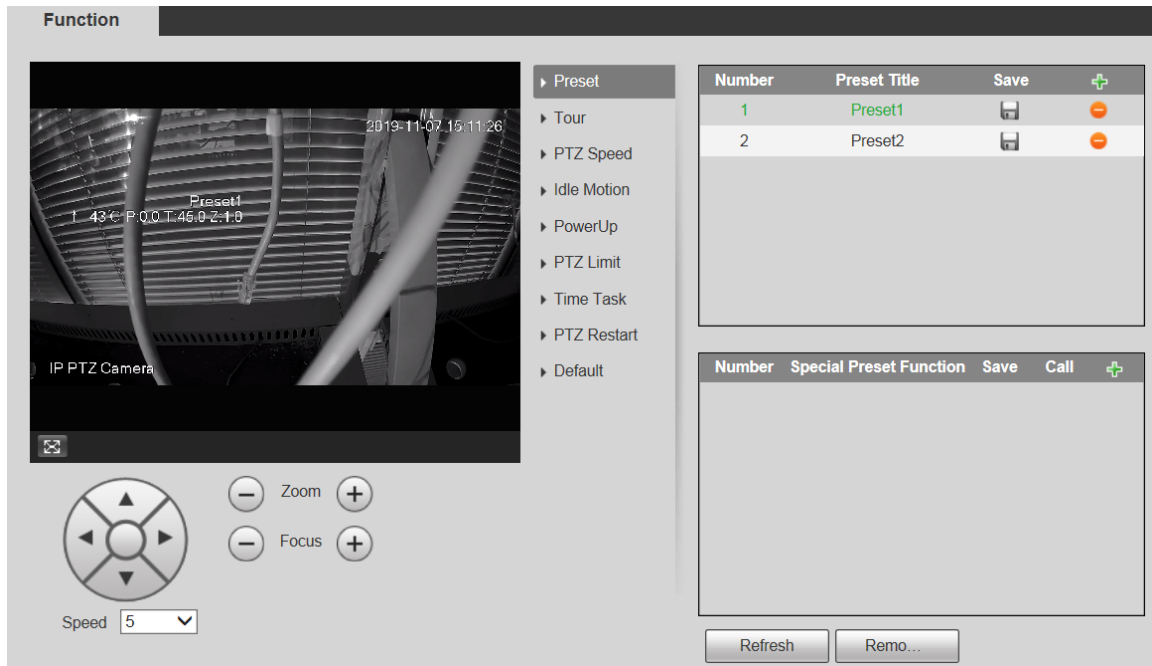
Background Information

Select **Setting** > **PTZ** > **Function** > **Preset**. The **Preset** page is displayed.



If you click **Remove All**, all presets and special presets will be cleared.

Figure 5-69 Preset



5.4.2.1.1 Preset Settings

Background Information

Preset means a certain position to which the Device rotates. Users can adjust the PTZ and camera to the location quickly through calling presets.

Procedure





- Step 1** On the lower left corner of the **Preset** page, click the direction buttons, , and  to adjust the PTZ direction, speed, zoom, and focus of the Device.
- Step 2** Click  to add a preset.
- The current position is set to a preset and is displayed in the list.

Figure 5-70 Add presets

Number	Preset Title	Save	+
1	Preset1		
2	Preset2		

- Step 3** Click  to save the preset.

Step 4 Perform operations on presets.


- Double-click the preset title to edit the title displayed on the monitoring screen.
- Click  to delete the preset.

5.4.2.1.2 Special Preset Settings

Background Information

Special presets serve as the shortcut for some special functions switch or calling, and they no longer represent the location of the PTZ camera.

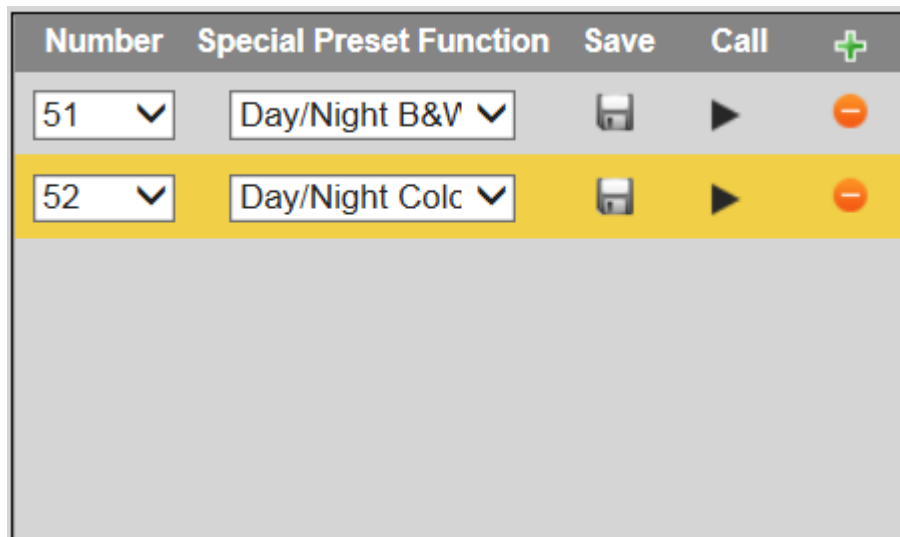
Procedure


Step 1 Click  to add a special preset. The added special preset will be displayed in the list.



The number of special presets starts from 51 by default, and 100 is the largest number.

Figure 5-71 Special presets



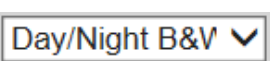


Step 2 Click  to save the added special preset.

Step 3 Perform operations on special presets.



If the PTZ is restored to default settings, all preset configurations will be cleared, but the called function will remain.

Related Operations

- Click  to modify the special preset function.
- Click  to delete the special preset.
- Click  to quickly call the function configured for the special preset.

5.4.2.2 Tour

Background Information

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



You need to set several presets in advance.

Procedure

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

Figure 5-72 Tour settings



Step 2 Select the **Tour Mode** from **Original Path** and **Shortest Path**. **Original Path** is selected by default.

- **Original Path** : Tour in the order of adding presets.
- **Shortest Path** : Starting from the preset with largest horizontal zoom value and vertical zoom value, pass all presets in the tour to ensure the shortest path. The Device reaches the corresponding preset and ensure the minimum number of rotation.

Step 3 Click **Add** at the bottom of the list on the upper right corner of the page to add a tour path.

Step 4 Click **Add** at the bottom of the list on the lower right corner of the page to add several presets.

Step 5 Perform tour operations.

- Double-click tour name to edit the name of the corresponding tour.
- Double-click duration to set the time that the Device stays at the corresponding preset.

- Double-click speed to modify the tour speed. The default value is 7, and the value range is 1–10. The larger the value, the faster the speed.

Step 6 Click **Start** to start the tour.



The ongoing tour stops if any operation is made to the PTZ.

5.4.2.3 Scan

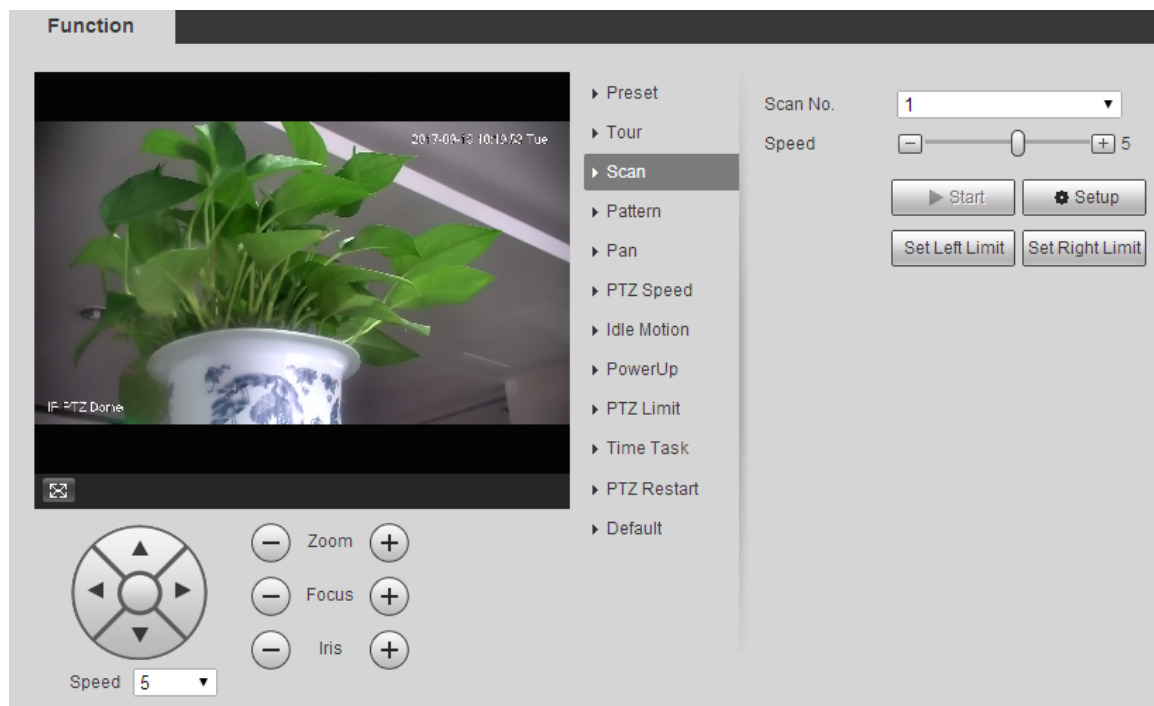
Background Information

Scan means the Device moves horizontally at a certain speed between the defined left and right limits.

Procedure

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

Figure 5-73 Scan settings



Step 2 Select the **Scan No.**.

Step 3 Drag the slider to adjust the scan speed.

Step 4 Click **Setup** to adjust the Device to an ideal position.

Step 5 Click **Set Left Limit** and **Set Right Limit** to set the left and right boundaries of the Device.

Step 6 Click **Start**, and then the Device starts scanning.

Step 7 Click **Stop**, and then the scanning stops.

5.4.2.4 Pattern

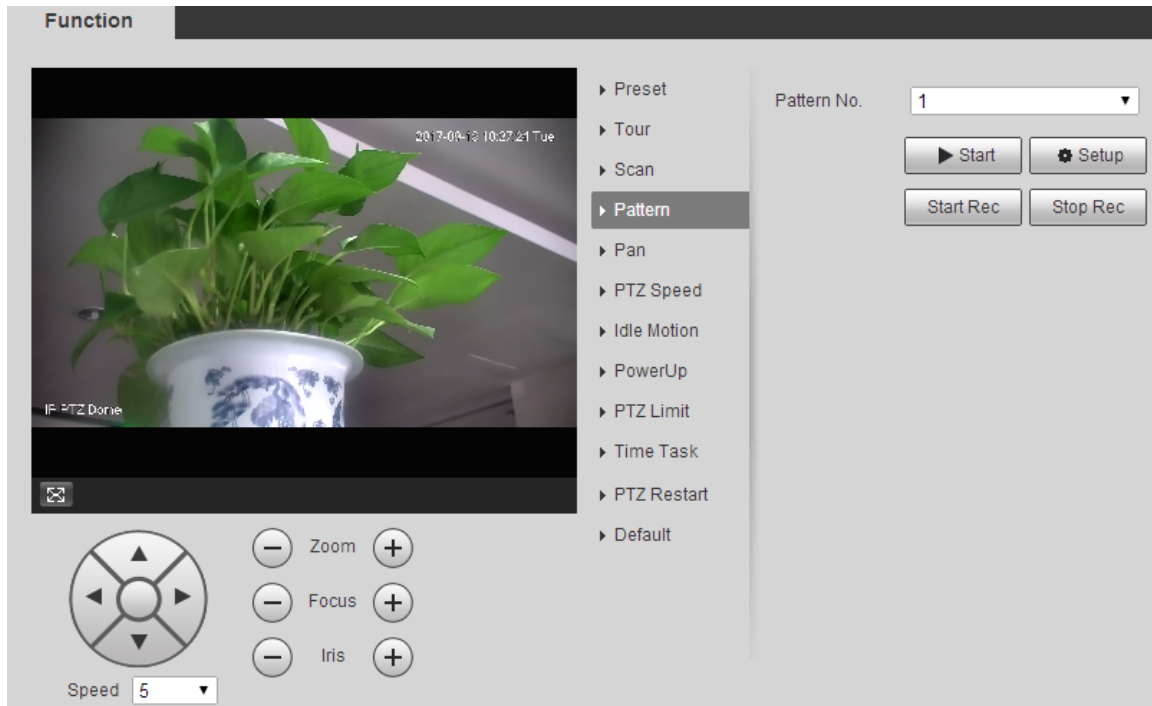
Background Information

Pattern means a record of a series of operations that users make to the Device. 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.

Procedure

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

Figure 5-74 Pattern settings



Step 2 Select the **Pattern No.**.

Step 3 Click **Setup** and **Start Rec**, and then operate the PTZ.

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

Step 5 Click **Start**, and then the Device starts patterning.

Step 6 Click **Stop**, and then the patterning stops.

5.4.2.5 Pan

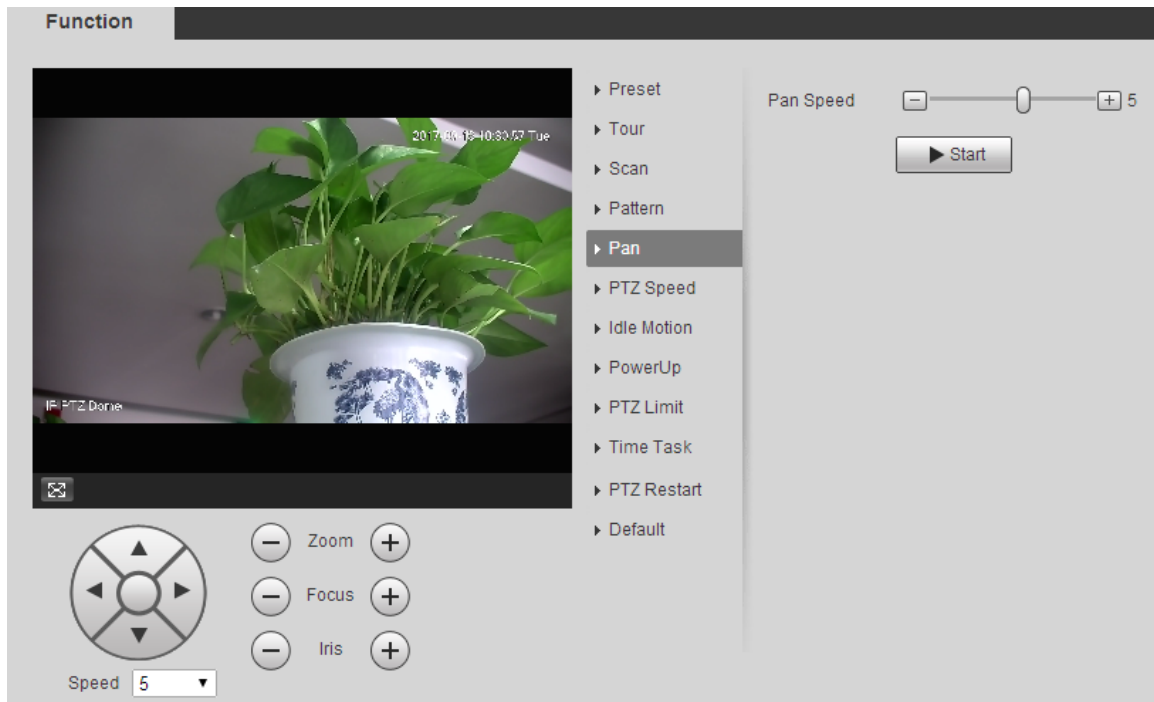
Background Information

Pan refers to the continuous 360° rotation of the Device at a certain speed.

Procedure

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

Figure 5-75 Pan settings



Step 2 Drag the slider to set the **Pan Speed**.

Step 3 Click **Start**, and the Device starts to rotate horizontally at this speed.

5.4.2.6 PTZ Speed

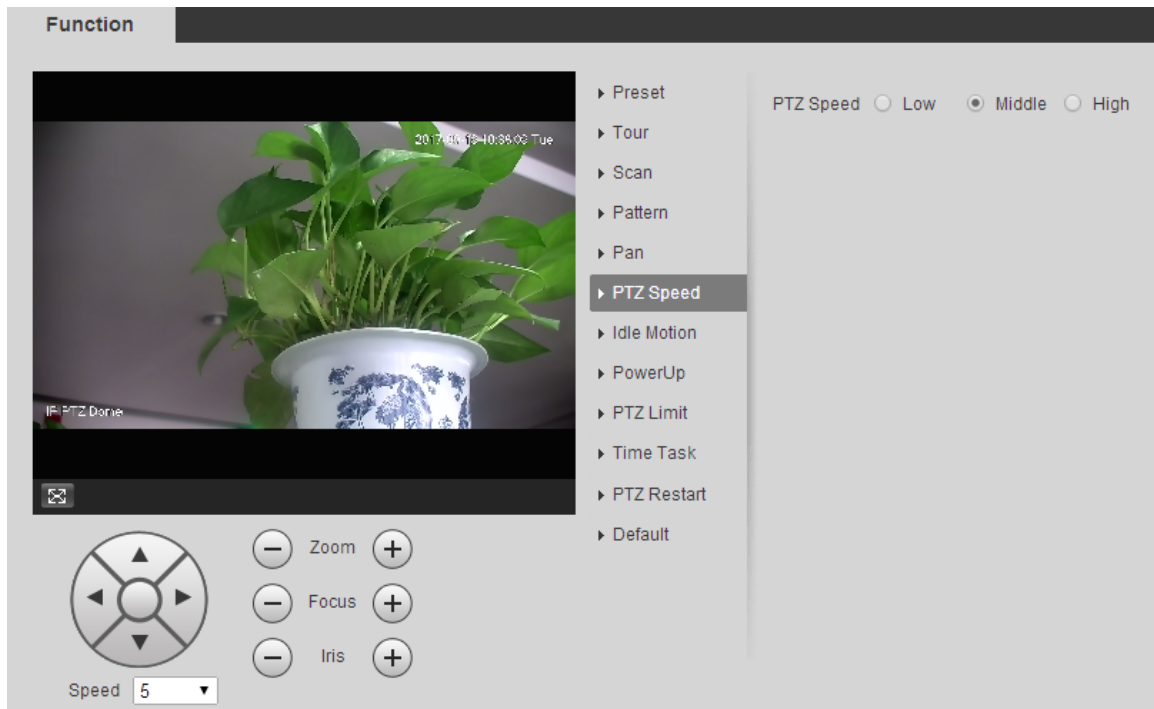
Background Information

You can adjust the manual control speed of the PTZ by setting PTZ speed. This speed does not apply to tour, pattern, or auto tracking.

Procedure

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

Figure 5-76 PTZ speed settings



Step 2 Select **Low** , **Middle** or **High**.

5.4.2.7 Idle Motion

Background Information

Idle motion refers to a set motion when the Device does not receive any valid command within a certain period.

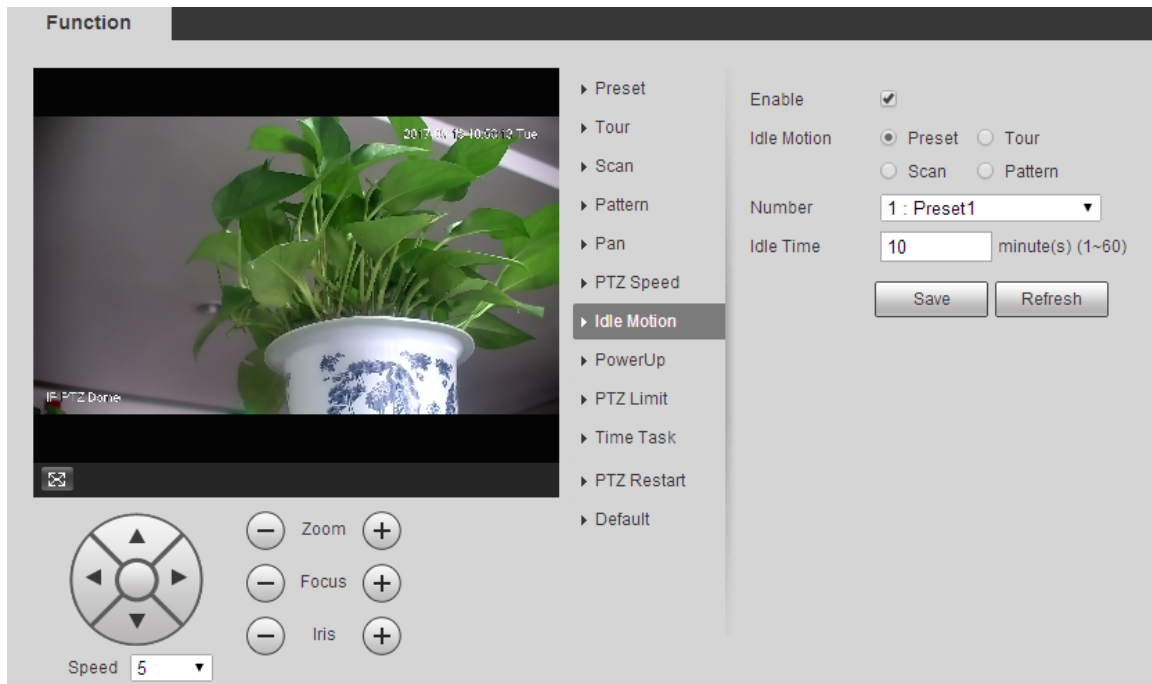


Set **Preset** , **Tour**, **Scan** or **Pattern** in advance.

Procedure

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

Figure 5-77 Idle motion settings



- Step 2** Select the **Enable** checkbox to enable the idle motion.
- Step 3** Select idle motion from **Preset** , **Tour** , **Scan** and **Pattern**.
- Step 4** Select the action number of the selected motion.
- Step 5** Set **Idle Time** for the selected motion.
- Step 6** Click **Save**.

5.4.2.8 PowerUp

Background Information

PowerUp means the automatic operation of the Device after it is powered on.

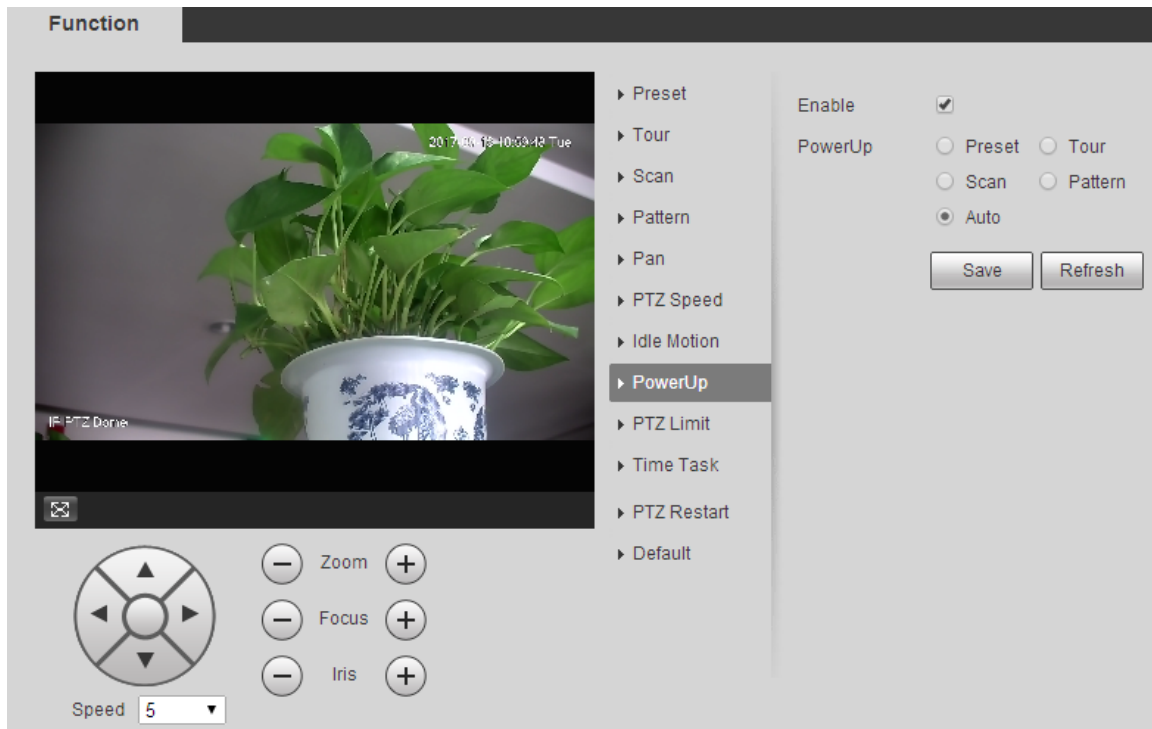


Set **Preset** , **Tour** , **Scan** or **Pattern** in advance.

Procedure

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

Figure 5-78 PowerUp settings



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

Step 3 Select power up motion from **Preset**, **Tour**, **Scan**, **Pattern** or **Auto**.



Select **Auto** and the last motion before you shut down the Device last time will be performed.

Step 4 Select the action number of the selected motion.

Step 5 Click **Save**.

5.4.2.9 PTZ Limit

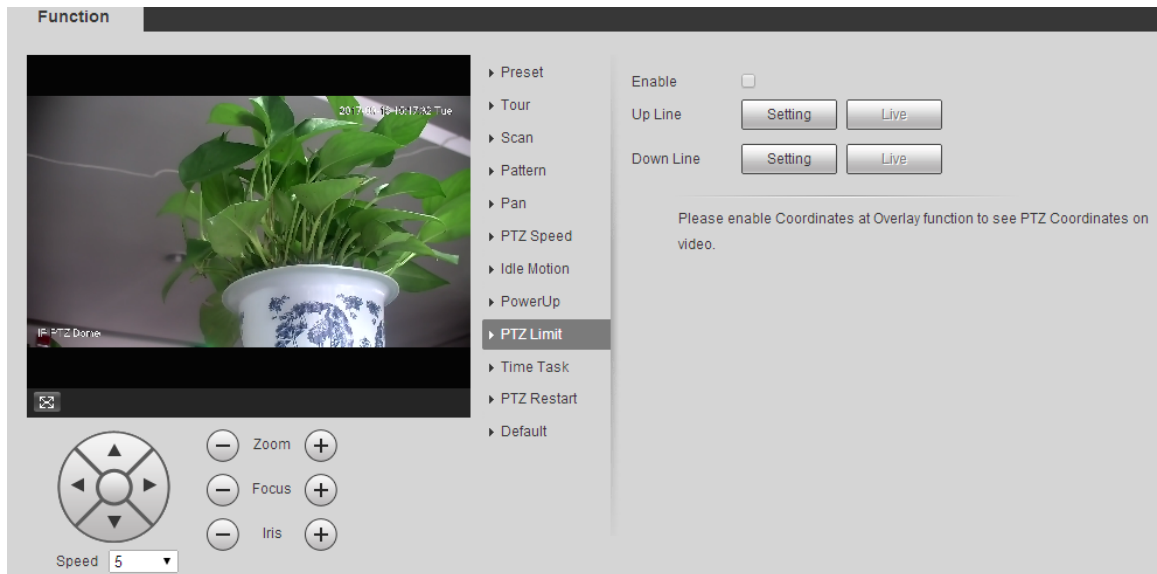
Background Information

After you set the PTZ limit, the Device can only move in the defined area.

Procedure

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

Figure 5-79 PTZ limit settings



- Step 2** Adjust the PTZ direction, and then click **Setting** to set the **Up Line**.
- Step 3** Adjust the PTZ direction, and then click **Setting** to set the **Down Line**.
- Step 4** Click **Live** to preview the already-set up line and down line.
- Step 5** Select the **Enable** checkbox to enable the PTZ limit function.

5.4.2.10 Time Task

Background Information

After you set time task, the Device performs the selected motions during the defined period.

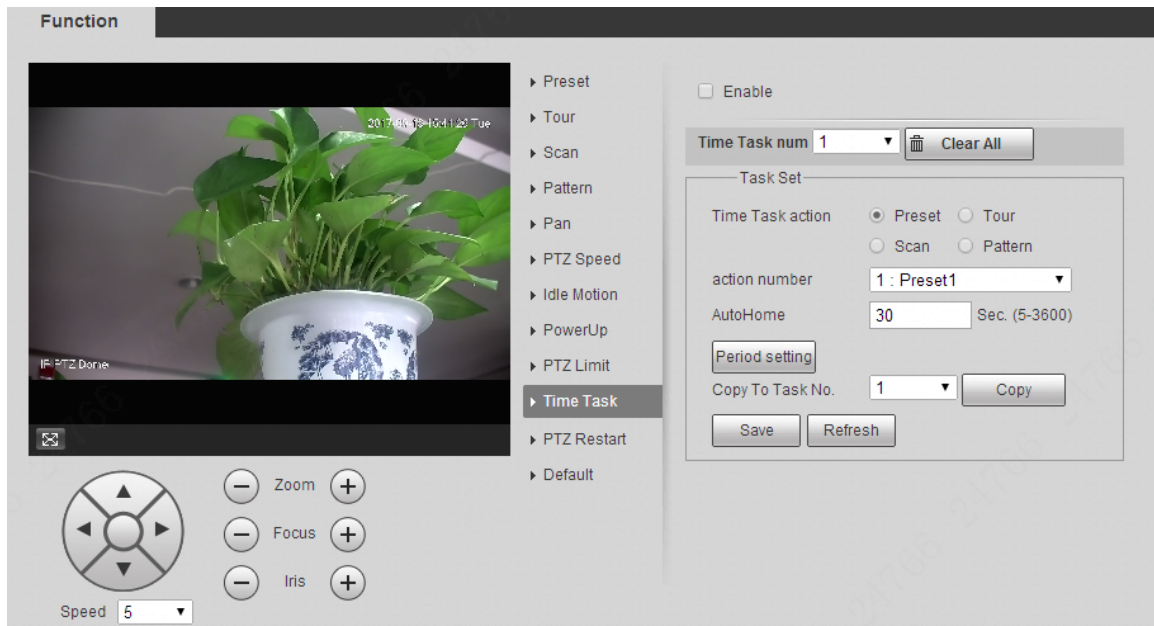


Set **Preset**, **Tour**, **Scan** or **Pattern** in advance.

Procedure

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

Figure 5-80 Time task settings



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

Step 3 Set the time task number.



Click **Clear All** to delete all set time tasks.

Step 4 Select **Time Task** action such as **Preset**, **Tour**, **Scan** or **Pattern**.

Step 5 Select the action number of the selected motion.

Step 6 Set the time for **AutoHome**.



AutoHome refers to the time needed to automatically recover the time task in case of manually calling the PTZ to stop the time task.

Step 7 Click **Period setting** to set the period to perform time tasks.

Step 8 Select the task number to copy settings to the selected task, and then click **Copy**.

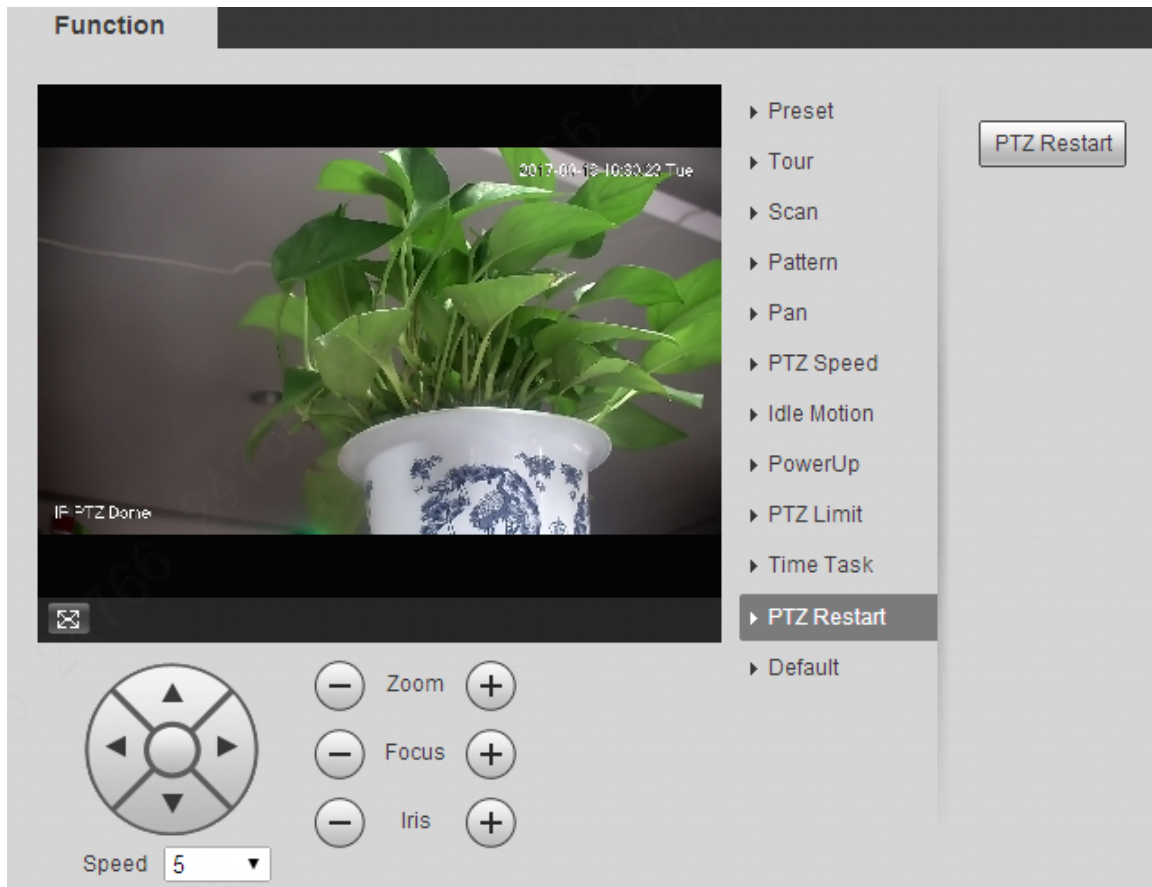
Step 9 Click **Save**.

5.4.2.11 PTZ Restart

Procedure

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

Figure 5-81 PTZ restart



- Step 2** Click **PTZ Restart**.
The PTZ is restarted.

5.4.2.12 Default

Background Information

With the function, you can restore the PTZ to factory defaults.



This function will restore the Device to defaults. Think twice before performing the operation.

Procedure

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

Figure 5-82 Default setting



Step 2 Click **Default**.

The PTZ will be restored to factory defaults.

5.5 Event Management

5.5.1 Video Detection

Video detection includes three event types: **Motion Detection**, **Video Tamper** and **Scene Changing**.

5.5.1.1 Motion Detection

When the moving object appears and moves fast enough to reach the preset sensitivity value, alarms will be triggered.

Procedure

Step 1 Select **Setting** > **Event** > **Video Detection** > **Motion Detection**.

Figure 5-83 Motion detection settings

Motion Detection
Video Tamper
Scene Changing

☒ Enable

Period

Anti-Dither
 s (0~100)

Area

☒ Enable Manual Con...

☒ Record

Record Delay
 s (10~300)

☒ Relay-out

Alarm Delay
 s (10~300)

☐ Send Email

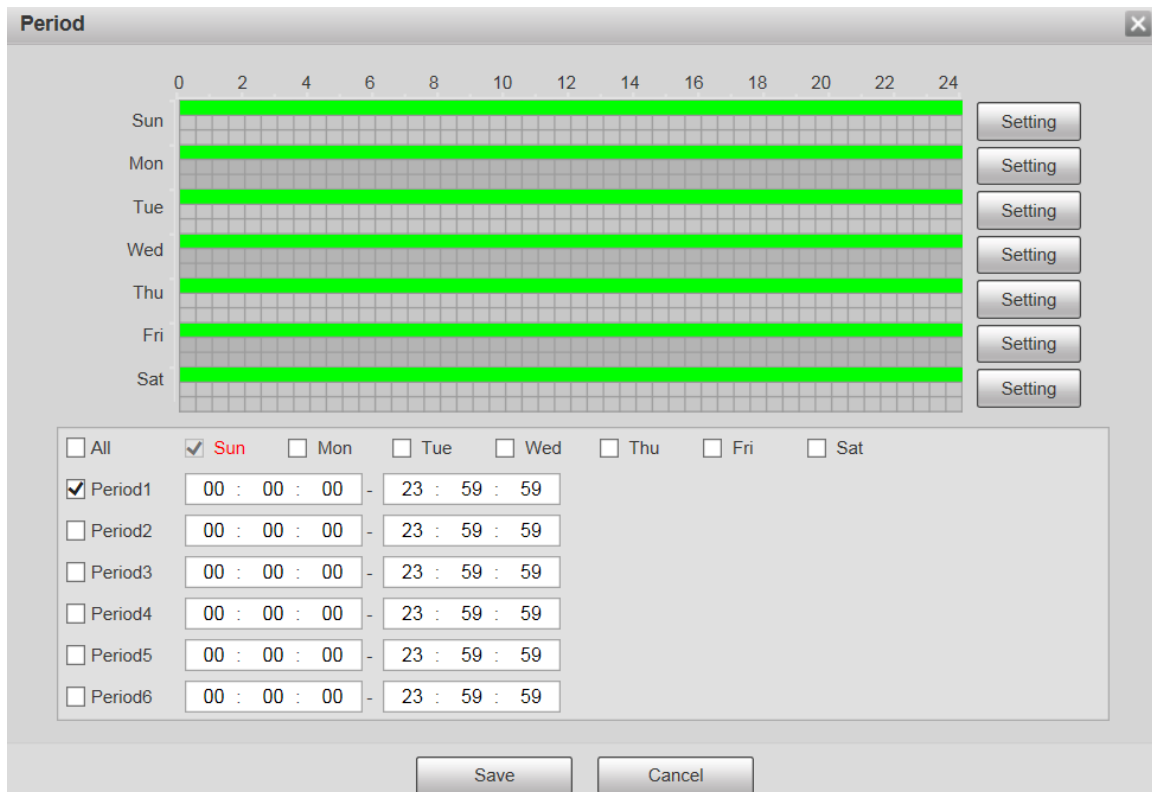
☐ PTZ

☒ Snapshot

Step 2 Select the **Enable** checkbox, and then configure motion detection parameters.

- Set arming and disarming period.
 1. Click **Setting**, and then set the arming period on the page.

Figure 5-84 Arming period settings



2. Set the alarm period to enable alarm events in the period you set.

- ◇ There are 6 time periods for each day. Select the check box for the time period to enable it.
- ◇ Select the day of week (**Sunday** is selected by default; If **All** is selected, the setting is applied to the whole week. You can also select the check box next to the day to set it separately).

3. After completing the settings, click **Save**.

You will return to the **Motion Detection** page.

- Set the area.

Click **Setting**, and the **Area** page is displayed. Refer to Table 5-27 and Table 5-28 for parameters description. Each color represents a certain region, and you can set different motion detection regions for each area. The detection region can be irregular and discontinuous.

Figure 5-85 Area setting

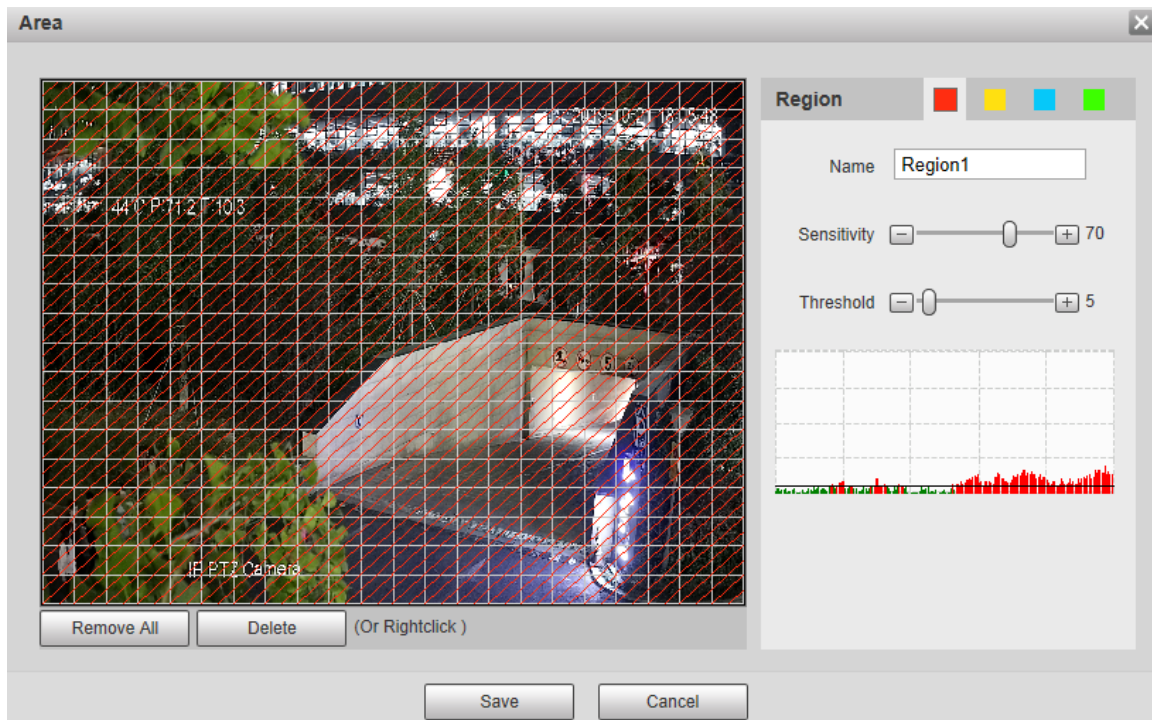


Table 5-27 Description of area setting parameter

Parameter	Description
Name	The default names are Region1, Region2, Region3 and Region4, and the names can be customized.
Sensitivity	Sensitivity to brightness change. The higher the sensitivity is, the easier the motion detection event will occur. You can set different sensitivities for each region, with values ranging from 0 to 100, and 30 to 70 is recommended.
Threshold	Detect the relation between the object and the region. The smaller the threshold is, the easier the motion detection will occur. Set different thresholds for each region, with values ranging from 0 to 100, and 1 to 10 is recommended.
Waveform graph	The red line indicates that motion detection is triggered, and the green line indicates that it is not triggered.
Remove All	Remove all detection regions.
Delete	Delete the detection region of the selected color block.

- Other parameters

Table 5-28 Description of video detection parameter

Parameter	Description
Anti-Dither	The system records only one motion detection event within the defined period. The value range is 0–100 s.

Parameter	Description
Enable Manual Control Trigger	After you enable the function, the motion detection events that occur when you control the PTZ manually will be excluded. In this way, you can reduce the false alarm rate of such events.
Record	After you enable the function, when an alarm is triggered, the system will start recording automatically. Before using the function, you need to set the recording period of the alarm in Storage > Schedule , and select Auto for Record Mode on the Record Control page.
Record Delay	When the alarm is over, the alarm recording will continue for an extended period of time. The time unit is second, and the value range is 10–300.
Relay-out	Select the checkbox, and you can enable the alarm linkage output port, and link corresponding relay-out devices after an alarm is triggered.
Alarm Delay	When the alarm is over, the alarm will continue for an extended period of time. The time unit is second, and the value range is 10–300.
Send Email	After you select the checkbox, when an alarm is triggered, the system sends email to the specified email address. You can configure the email address in "5.2.5 SMTP (Email)."
PTZ	Select PTZ , and then configure the linkage action. When an alarm is triggered, the system links PTZ to rotate to the preset. The Activation options include None , Preset , Tour and Pattern .
Snapshot	Select the Snapshot check box, and then the system takes snapshot automatically when an alarm is triggered. You need to set the alarm snapshot period as described in "5.6.1.2 Snapshot".

Step 3 Click **Save**.

5.5.1.2 Video Tamper

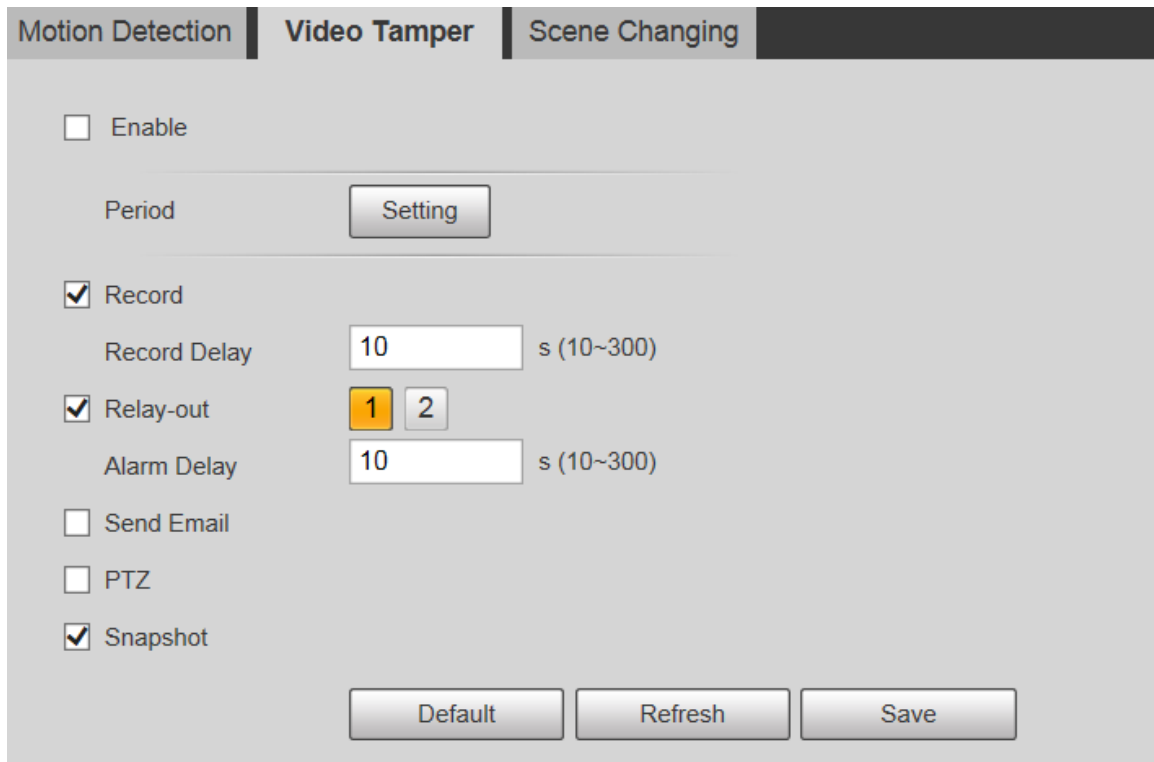
Background Information

Alarms will be triggered if there is video tampering.

Procedure

Step 1 Select **Setting > Event > Video Detection > Video Tamper**.

Figure 5-86 Video tamper settings



Step 2 Select the **Enable** checkbox, and then configure video tamper parameters.



For parameters configuration, see "5.5.1.1 Motion Detection".

Step 3 Click **Save**.

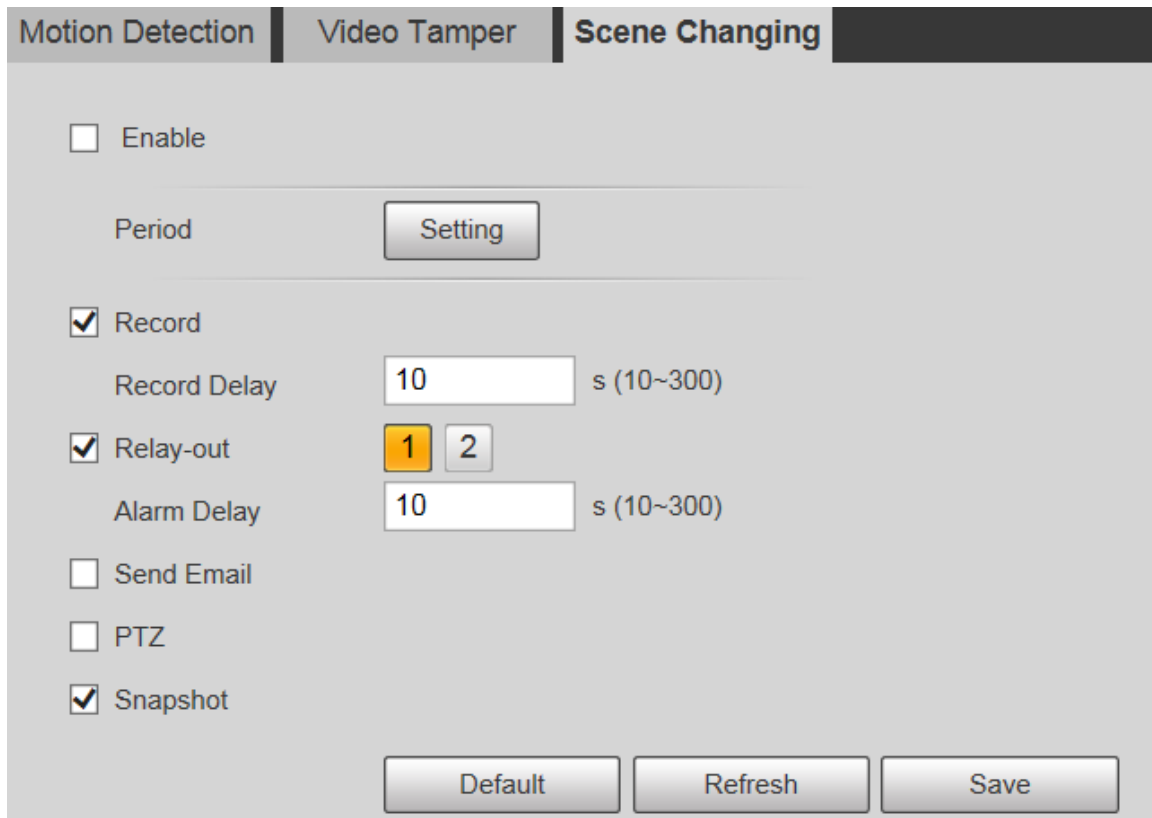
5.5.1.3 Scene Changing

Alarms will be triggered if there is scene changing.

Procedure

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

Figure 5-87 Scene changing settings



Step 2 Select the **Enable** checkbox, and then configure scene changing parameters.



For parameters configuration, see "5.5.1.1 Motion Detection".

Step 3 Click **Save**.

5.5.2 Smart Motion Detection

After you set smart motion detection, when the human, non-motor vehicles and motor vehicles appear and move fast enough to reach the preset sensitivity value, the alarm linkage actions will be performed. The function can help you to avoid the alarms triggered by natural environment change.



- The function depends on the result of motion detection, and all other parameters (except sensitivity) of motion detection function are used, including arming period, area settings, and linkage configurations. If no motion detection is triggered, smart motion detection will not be triggered.
- If motion detection is not enabled, when smart motion detection is enabled, motion detection will also be enabled. If both functions are enabled, when motion detection is disabled, smart motion detection will also be disabled.
- When smart motion detection is triggered and recording is linked, back-end devices can filter recording with human or vehicles through smart search function. For details, see the corresponding user's manual.

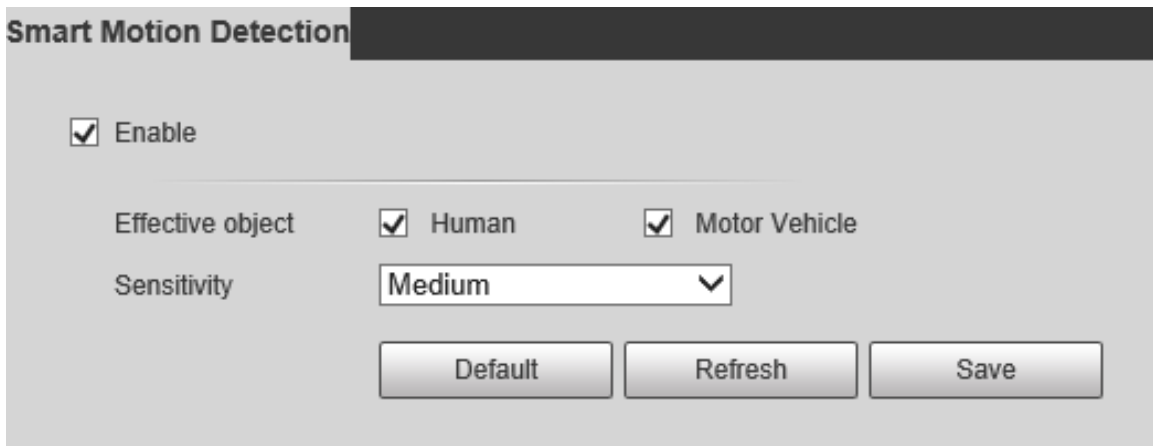
Prerequisites

- Select **Setting** > **Event** > **Video Detection** > **Motion Detection**, and then enable the motion detection function.
- Set the arming period and detection area. The sensitivity of each region is larger than 0, and the threshold is not equal to 100.

Procedure

1. Select **Setting** > **Event** > **Smart Motion Detection**.

Figure 5-88 Smart motion detection



2. Select the **Enable** checkbox to enable **Smart Motion Detection**.
3. Select the effective object and sensitivity.
 - **Effective object** : Select **Human** or **Motor Vehicle**. When **Human** is selected, both people and non-motor vehicles will be detected.
 - **Sensitivity** : Select **High**, **Medium**, or **Low**. The higher the sensitivity, the easier the alarm is triggered.
4. Click **Save**.

5.5.3 Audio Detection

Procedure

- Step 1 Select **Setting** > **Event** > **Audio Detection** > **Audio Detection**.

Figure 5-89 Audio detection settings

Audio Detection

☐ Input Abnormal

☐ Intensity Change

Sensitivity

-

+

50

Threshold

-

+

50

Period

Setting

Anti-Dither

5

s (0~100)

☒ Record

Record Delay

10

s (10~300)

☒ Relay-out

1

2

Alarm Delay

10

s (10~300)

☐ Send Email

☐ PTZ

☒ Snapshot

Default

Refresh

Save

Step 2 Configure audio detection parameter.

Table 5-29 Description of audio detection parameter

Parameter	Description
Input Abnormal	Select Input Abnormal , and then an alarm is triggered when there is abnormal audio input.
Intensity Change	Select Intensity Change , and then an alarm is triggered when the change in sound intensity exceeds the defined threshold.
Sensitivity	The value ranges from 1 to 100. The smaller this value is, the larger the input sound volume changes are needed for it to be judged as an audio anomaly. You need to adjust it according to the actual condition.

Parameter	Description
Threshold	The value ranges from 1 to 100. Configure the ambient sound intensity you need to filter. The louder the ambient noise is, the larger this value shall be. You need to adjust it according to the actual condition.



For other parameters, see "5.5.1.1 Motion Detection".

Step 3 Click **Save**.

5.5.4 Smart Plan

Background Information

Smart plans include IVS, face recognition, heat map, people counting, video metadata, construction monitoring and so on. Only after smart plans have been enabled, can the corresponding smart function come into effect.

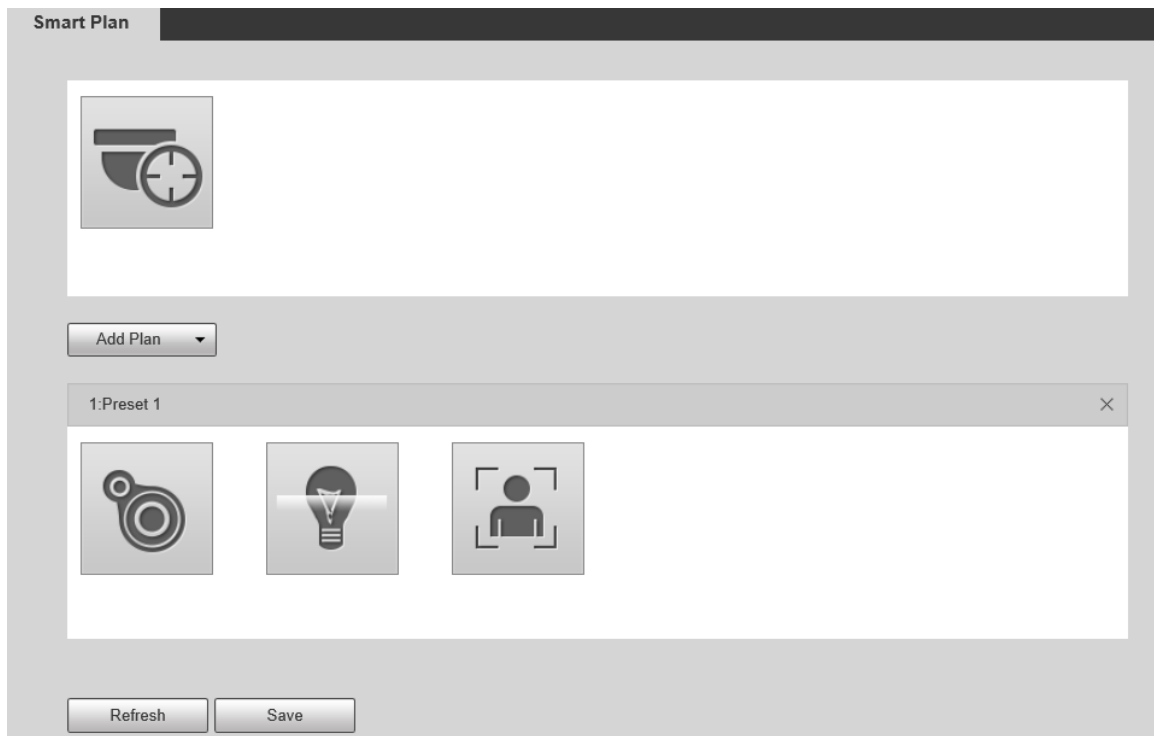


Before configuring the smart plan, you need to set presets in advance. For setting methods, see "5.4.2.1 Preset".

Procedure

Step 1 Select **Setting** > **Event** > **Smart Plan**.

Figure 5-90 Smart plan (1)



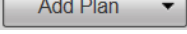
Step 2 (Optional) Click  to enable **Auto Tracking**.

When enabling auto tracking, you do not need to configure smart plans, and the Device performs auto tracking based on internal mechanism. If auto tracking and alarm track of

the smart plan (such as IVS) are both enabled, the Device perform tracking in the order of triggering time.



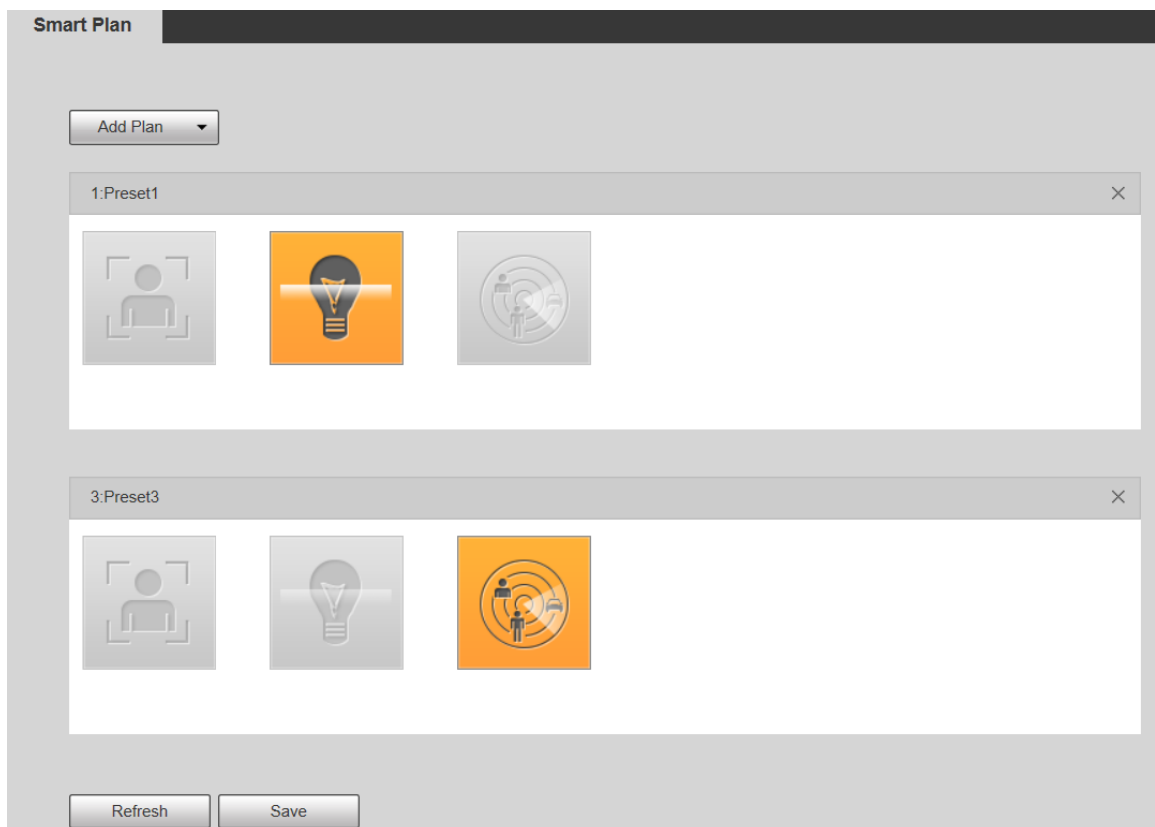
It is recommended to disable auto tracking when alarm track is enabled to avoid disordered tracking.

Step 3 Click  to select the presets to be configured.

Step 4 Select smart plans.

The selected function will be highlighted. Click it again to cancel the selection.

Figure 5-91 Smart plan (2)



Step 5 Click **Save**.

5.5.5 IVS

Basic Requirements for the Scene

- The target size shall not exceed 10% of the image.
- The pixel of the target shall be no less than 10×10; the pixel of abandoned object shall be no less than 15 × 15 (CIF image); the width and height of the target shall be no more than 1/3 of the image. It is recommended that the height of the target is 10% of the image.
- The brightness difference between the target and the background is no less than 10 gray values.
- The target shall be present in the image for no less than 2 consecutive seconds, and the moving distance shall be larger than its width and no less than 15 pixels (CIF image).
- Try to reduce the complexity of monitoring scenes. It is not recommended to enable IVS in scenes with dense targets and frequent light changes.

- Try to avoid the following scenes: scenes with reflective surfaces such as glass, bright ground or water; scenes that disturbed by tree branches, shadows or winged insects; scenes that against light or under direct light exposure.

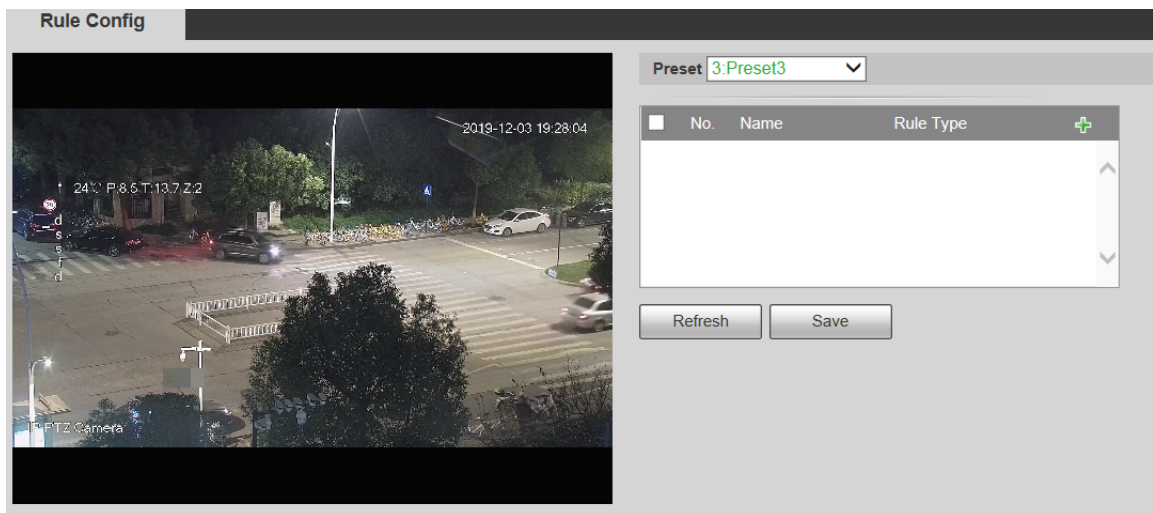


Before using the function, you need to set presets in advance. For setting methods, see "5.3.2.1 Preset."


Rule Config

- Select **Setting** > **Event** > **IVS** > **Rule Config**.

Figure 5-92 Add smart rules



- Select the presets to be configured with smart rules.

- Click  to add smart rules.



Double-click rule type to modify the type of rules.

- Click **Save**.

5.5.5.1 Tripwire

Background Information

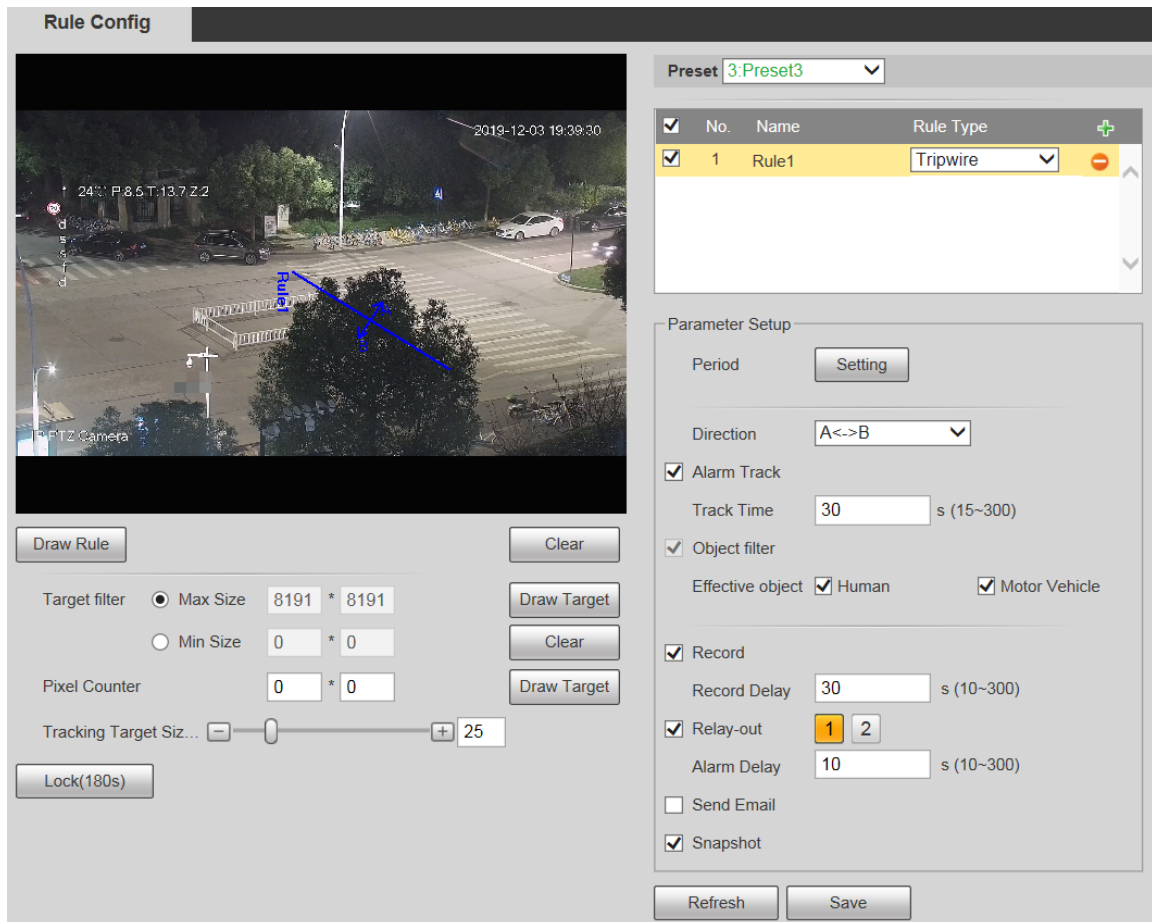
Alarms are triggered when the target crosses the warning line in the defined direction. It requires certain stay time and moving space for the target to be confirmed, so you need to leave some space at both sides of the warning line during configuration and do not draw it near obstacles.

Applicable scenes: Scenes with sparse targets and no occlusion between targets, such as perimeter protection of unattended areas.

Procedure

- Step 1** Select **Tripwire** from the **Rule Type** list.

Figure 5-93 Tripwire rule settings



Rule Config

Preset: 3:Preset3

No.	Name	Rule Type
1	Rule1	Tripwire

Parameter Setup

Period: Setting

Direction: A<->B

☒ Alarm Track
Track Time: 30 s (15~300)

☒ Object filter
Effective object: ☒ Human ☒ Motor Vehicle

☒ Record
Record Delay: 30 s (10~300)

☒ Relay-out: 1 2
Alarm Delay: 10 s (10~300)

☐ Send Email

☒ Snapshot

Refresh Save


Step 2 Click **Draw Rule**, and you can draw rules on the monitoring screen.



Click **Clear** to the right of **Draw Rule** to clear all drawn rules.

Table 5-30 Description of rule drawing parameter

Parameter	Description
Max Size	Set the size range of detection targets to be filtered, and select the maximum or minimum size. <ul style="list-style-type: none"> Max Size: Set the maximum size of targets to be filtered. When the target is larger than this size, the system will ignore it. The unit is pixel. Min Size: Set the minimum size of targets to be filtered. When the target is smaller than this size, the system will ignore it. The unit is pixel.
Min Size	
Pixel Counter	Help to accurately draw the target area. Enter the length and width of the target area in Pixel Counter , and click Draw Target to generate the target area in the monitoring screen. The unit is pixel.

Parameter	Description
Lock/Unlock	<p>Enter the rule configuration page, and the locking function will be automatically enabled, and the locking time is 180 s. During this period, the device cannot track the target. Click Unlock to release the control.</p>  <p>The locking function only takes effect in the rule configuration page. After switching to the Live page, the Device can track the target normally.</p>

Step 3 Configure tripwire parameter.

Table 5-31 Description of tripwire parameter

Parameter	Description
Period	<p>Set the alarming period to enable alarm events in the defined period.</p> <ol style="list-style-type: none"> 1. Click Setting, and then the Period page is displayed. 2. Enter the time value or press and hold the left mouse button, and drag directly on the setting page. There are six periods for each day. Select the checkbox next to the period for it to take effect. 3. Select the day of week (Sunday is selected by default; If All is selected, the setting is applied to the whole week. You can also select the checkbox next to the day to set it separately). 4. After completing the setting, click Save to go back to the rule configuration page.
Direction	Configure the tripwire direction. You can select A->B , B->A or A<->B .
Alarm Track	Select the checkbox, and there will be alarm tracking when a smart rule is triggered.
Track Time	Set the alarm tracking time.
Record	Select the checkbox, and when an alarm is triggered, the system will start recording automatically. Before using the function, you need to set the recording period of the alarm in Storage > Schedule , and select Auto for Record Mode on the Record Control page.
Record Delay	When the alarm is over, the recording will continue for an extended period of time. The value range is 10–300 s.
Relay-out	Select the checkbox, and you can enable the alarm linkage output port, and link corresponding relay-out devices when an alarm is triggered.
Alarm Delay	When the alarm is over, the alarm will continue for an extended period of time. The value range is 10–300 s.
Send Email	Select the Send Email checkbox, and when an alarm is triggered, the system sends an email to the specified mailbox. You can configure the mailbox in Setting > Network > SMTP (Email) .
Snapshot	Select the checkbox, and the system will automatically take snapshots in case of alarms. You need to set snapshot period in Storage > Schedule .

Step 4 Click **Save**.

Step 3 Configure intrusion parameter.

Table 5-32 Description of intrusion parameter

Parameter	Description
Action	Configure intrusion action, and you can select Appear or Cross .
Direction	Select the crossing direction from Enters , Exits , and Enter & Exit .



For other parameters, see "5.5.5.1 Tripwire".

Step 4 Click **Save**.

5.5.5.3 Abandoned Object

Background Information

An alarm will be triggered when the selected target in the monitoring scene stays in the screen for more than the defined time.

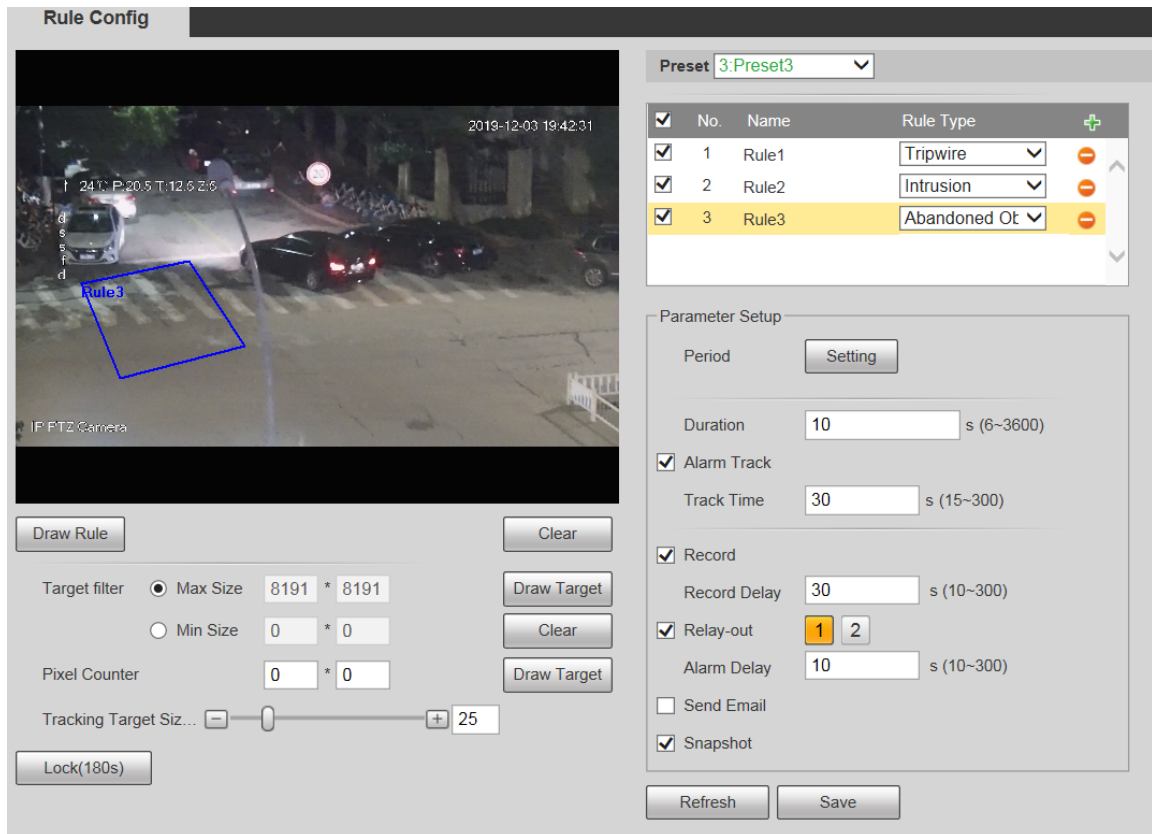
Pedestrians or vehicles that stay for too long would be regarded as abandoned objects. To filter out such alarms, you can use **Target filter**. In addition, the duration can be properly extended to avoid false alarm due to a short stay of people.

Applicable scenes: Scenes with sparse targets, no obvious and frequent light changes. For scenes with intensive targets or too many obstacles, missed alarms would increase; for scenes in which too many people stay, false alarms would increase. Select detection areas with simple texture, because this function is not applicable to scenes with complex texture.

Procedure

Step 1 Select **Abandoned Object** from the **Rule Type** list.

Figure 5-95 Abandoned object settings



Step 2 Click **Draw Rule**, and you can draw rules on the monitoring screen.

For parameter description, see "5.5.5.1 Tripwire".



Click **Clear** to the right of **Draw Rule**, and you can clear all drawn rules.

Step 3 Configure abandoned object parameter.

Duration: For abandoned object, the duration is the shortest time to trigger an alarm after an object is abandoned.



For other parameters, see "5.5.5.1 Tripwire".

Step 4 Click **Save**.

5.5.5.4 Missing Object

Background Information

An alarm will be triggered when the selected target in the scene is taken away for the time longer than the set duration.

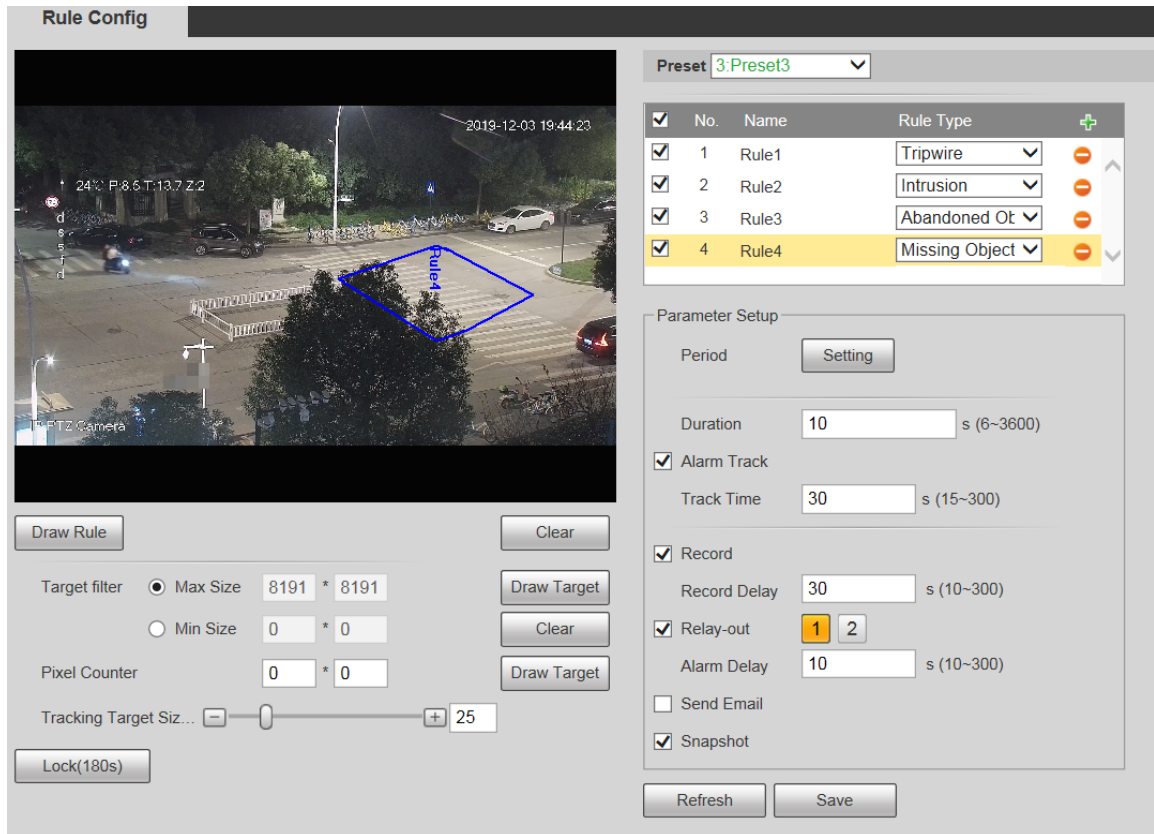
The system analyzes static areas from the foreground, and determines whether it is missing object or abandoned object from the similarity of its foreground and background. When the time exceeds the set period, an alarm is triggered.

Applicable scenes: Scenes with sparse targets, no obvious and frequent light changes. For scenes with intensive targets or too many obstacles, the missed alarm would increase; for scenes in which too many people stay, the false alarm would increase. Keep the detection area texture as possible simple as possible, because this function is not applicable to scenes with complex texture.

Procedure

Step 1 Select **Missing Object** from the **Rule Type** list.

Figure 5-96 Missing object setting



The screenshot shows the 'Rule Config' window. On the left is a live video feed of a street scene with a blue polygon rule drawn on it. Below the video are controls for 'Draw Rule', 'Clear', 'Target filter' (Max Size 8191 * 8191, Min Size 0 * 0), 'Pixel Counter' (0 * 0), 'Tracking Target Siz...' (slider at 25), and 'Lock(180s)'. On the right is the 'Parameter Setup' panel. It includes a 'Preset' dropdown set to '3.Preset3', a table of rules, and various configuration options.

No.	Name	Rule Type
1	Rule1	Tripwire
2	Rule2	Intrusion
3	Rule3	Abandoned Ot
4	Rule4	Missing Object

Parameter Setup

Period:

Duration: s (6~3600)

☒ Alarm Track

Track Time: s (15~300)

☒ Record

Record Delay: s (10~300)

☒ Relay-out:

Alarm Delay: s (10~300)

☐ Send Email

☒ Snapshot

Step 2 Click **Draw Rule**, and you can draw rules on the monitoring screen.

For parameter description, see "5.5.5.1 Tripwire".



Click **Clear** to the right of **Draw Rule** to clear all drawn rules.

Step 3 Configure missing object parameter.

Duration: Configure the shortest time from the object disappearing to the alarm being triggered.



For other parameters, see "5.5.5.1 Tripwire".

Step 4 Click **Save**.

5.5.6 Construction Monitoring

The Device can be used for construction monitoring which include helmet detection, workwear detection, lone working detection and absence detection.

Prerequisites

Select **Setting** > **Event** > **Smart Plan** to enable **Construction Monitoring**.

Procedure

Step 1 Select **Setting** > **Event** > **Construction Monitoring**.

Step 2 Select **Global** or a preset from the **Preset** list.

- If global plan is selected, detection area and rule are set by default, and the detection area cannot be changed.
- If a preset is selected, you need to set detection area and rule manually. The following section uses selecting Preset 1 as an example.

Figure 5-97 Global plan

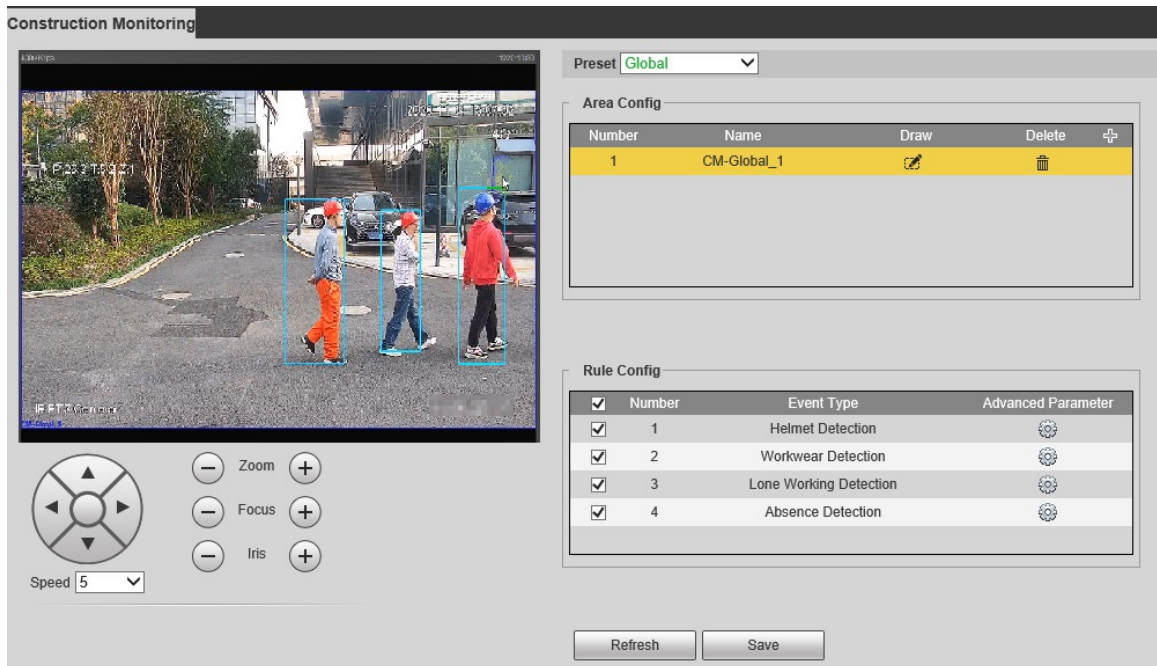
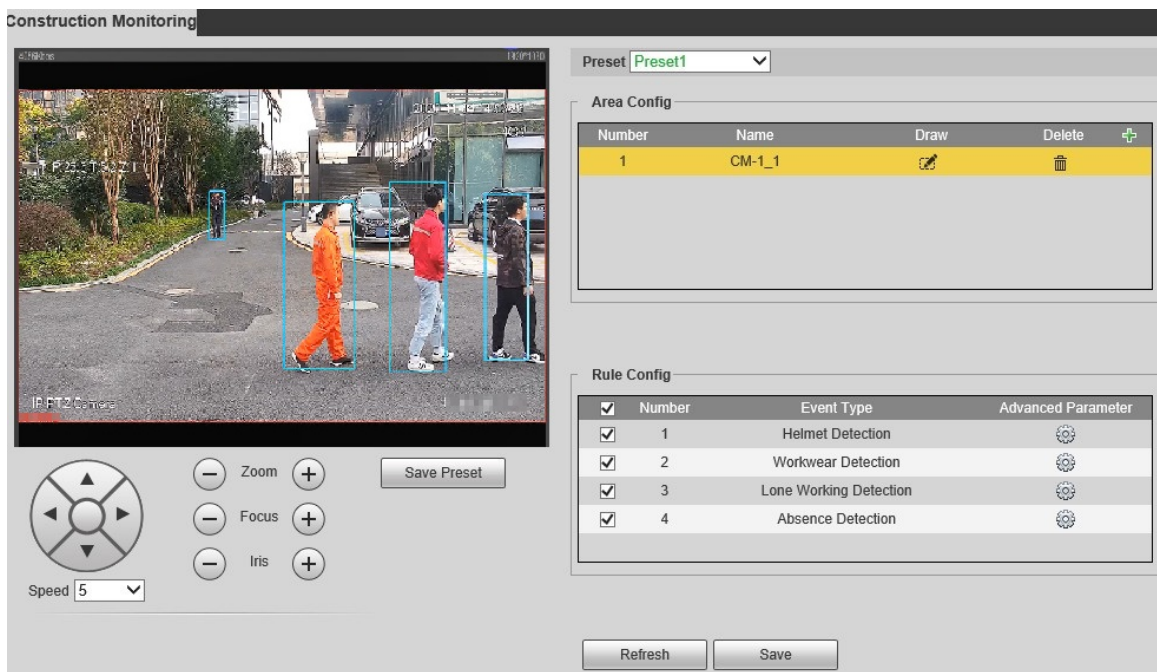




Figure 5-98 Plan by preset



Step 3 Click  at the upper-right corner of the **Area Config** section.



Double click the rule name to modify it.

Step 4 Click  to draw rule box on the video image, and then right-click to complete drawing.



- After drawing is complete, drag the corners of the drawn area to adjust the detection area.
- If you select preset plan, 8 detection areas can be drawn at most.

Step 5 Select the checkbox before the event type to enable the corresponding detection rule.

Table 5-33 Rule description

Rule	Description
Helmet Detection	When the Device detects person not wearing helmet or not wearing helmet in the specified color, alarm linkage actions will be performed.
Workwear Detection	When the Device detects person not wearing workwear in accordance with the rule, alarm linkage actions will be performed. The rule for workwear is long-sleeved tops and trousers in the same color. If short-sleeved shirts, shorts or different colors are detected, it means the rule is not followed.
Lone Working Detection	When the Device detects a single person working in the detection area, alarm linkage actions will be performed.
Absence Detection	When the Device detects nobody working in the detection area, alarm linkage actions will be performed.


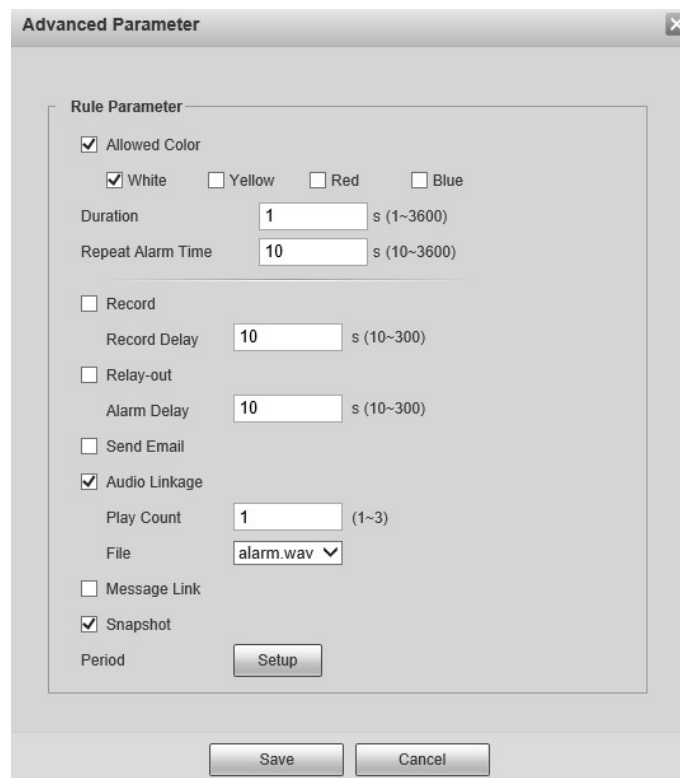
Step 6 Click  next to the detection rule, configure parameters on the **Advanced Parameter** page, and then click **Save**.

Figure 5-99 Helmet detection



Advanced Parameter

Rule Parameter

☒ Allowed Color

☒ White ☐ Yellow ☐ Red ☐ Blue

Duration s (1~3600)

Repeat Alarm Time s (10~3600)

☐ Record

Record Delay s (10~300)

☐ Relay-out

Alarm Delay s (10~300)

☐ Send Email

☒ Audio Linkage

Play Count (1~3)

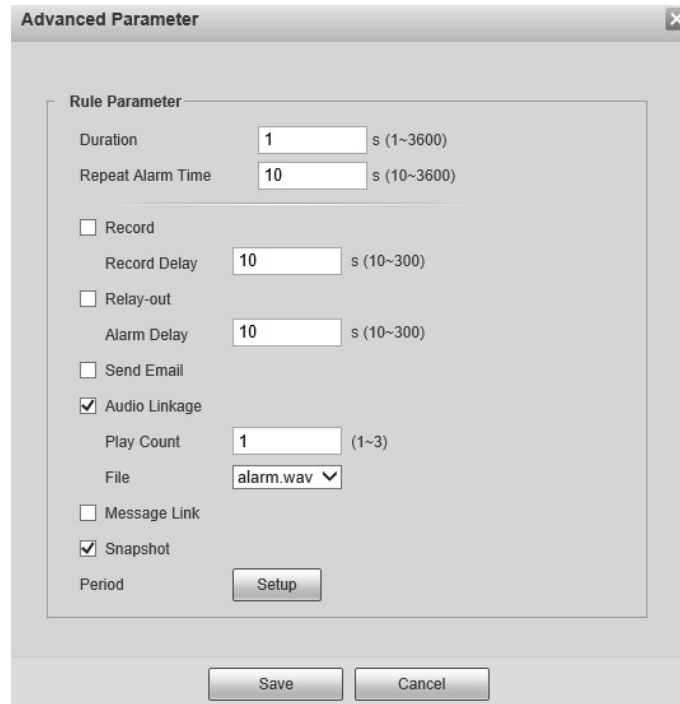
File

☐ Message Link

☒ Snapshot

Period

Figure 5-100 Workwear detection

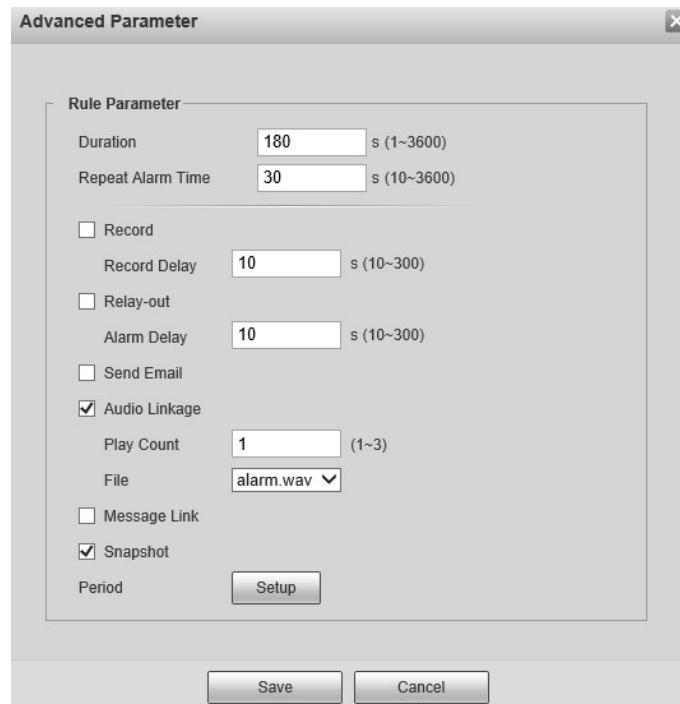


The 'Advanced Parameter' dialog box for Workwear detection contains the following settings:

- Rule Parameter**
 - Duration: 1 s (1~3600)
 - Repeat Alarm Time: 10 s (10~3600)
 - ☐ Record
 - Record Delay: 10 s (10~300)
 - ☐ Relay-out
 - Alarm Delay: 10 s (10~300)
 - ☐ Send Email
 - ☒ Audio Linkage
 - Play Count: 1 (1~3)
 - File: alarm.wav
 - ☐ Message Link
 - ☒ Snapshot
 - Period: Setup

Buttons: Save, Cancel

Figure 5-101 Lone working detection

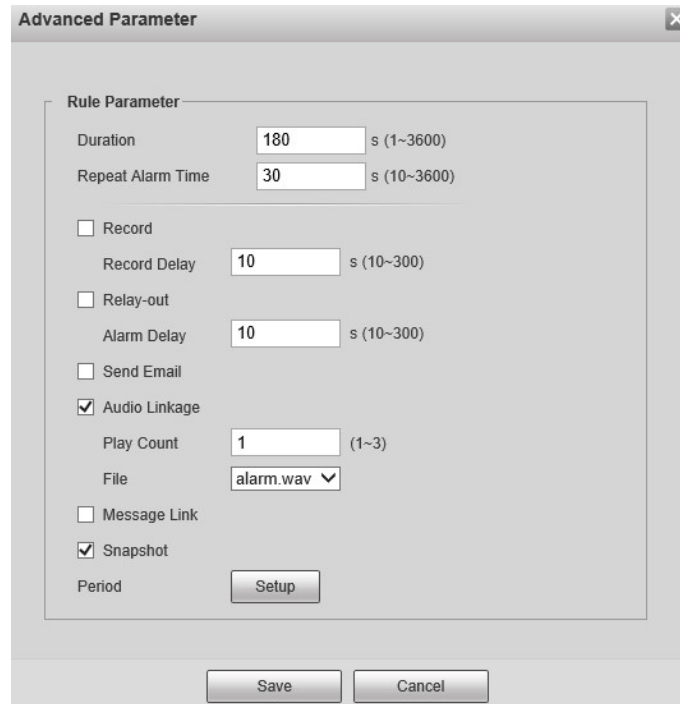


The 'Advanced Parameter' dialog box for Lone working detection contains the following settings:

- Rule Parameter**
 - Duration: 180 s (1~3600)
 - Repeat Alarm Time: 30 s (10~3600)
 - ☐ Record
 - Record Delay: 10 s (10~300)
 - ☐ Relay-out
 - Alarm Delay: 10 s (10~300)
 - ☐ Send Email
 - ☒ Audio Linkage
 - Play Count: 1 (1~3)
 - File: alarm.wav
 - ☐ Message Link
 - ☒ Snapshot
 - Period: Setup

Buttons: Save, Cancel

Figure 5-102 Absence detection



Advanced Parameter

Rule Parameter

Duration: 180 s (1~3600)

Repeat Alarm Time: 30 s (10~3600)

☐ Record

Record Delay: 10 s (10~300)

☐ Relay-out

Alarm Delay: 10 s (10~300)

☐ Send Email

☒ Audio Linkage

Play Count: 1 (1~3)

File: alarm.wav

☐ Message Link

☒ Snapshot

Period: Setup

Save Cancel

Table 5-34 Parameter description

Parameter	Description
Allowed Color	When configuring helmet detection, you can set allowed colors. When the helmet detected is not in the selected colors, alarms will be triggered.
Duration	When events not following the rule are detected and the duration exceeds the defined value, alarms will be triggered. For example, when the duration of helmet detection is 5 seconds, if the Device detects a person not wearing helmet or the helmet color is not allowed for more than 5 seconds, an alarm will be triggered.
Repeat Alarm Time	After an alarm is triggered, when the event lasts for the time reaching repeated alarm time, an alarm will be triggered again.
Record	After you enable the function, when an alarm is triggered, the system will start recording automatically. Before using the function, you need to set the recording period of the alarm in Storage > Schedule , and select Auto for Record Mode on the Record Control page.
Record Delay	When an alarm is over, the alarm recording will continue for an extended period of time.
Relay-out	Select the checkbox, and you can enable the alarm linkage output port, and link corresponding relay-out devices after an alarm is triggered.
Alarm Delay	When an alarm is over, the alarm will continue for an extended period of time.
Send Email	After you select the checkbox, when an alarm is triggered, the system sends email to the specified email address. You can configure the email address in "5.2.5 SMTP (Email)".

Parameter	Description
Audio Linkage	Select the checkbox to play alarm audio when alarms are triggered. You can set the play count and select the audio file. For how to set the audio file, see "5.1.3.2 Configuring Alarm Audio".
Message Link	Select the checkbox to receive message when alarms are triggered.
Snapshot	Select the checkbox, and the system will automatically take snapshots in case of alarms. You need to set snapshot period in Storage > Schedule .
Period	Set the alarm period to enable alarm events in the defined period. <ol style="list-style-type: none"> 1. Click Setup, and the Period page is displayed. 2. Enter the time value or press and hold the left mouse button, and drag directly on the setting page. There are six periods for each day. Select the checkbox next to the period for it to take effect. 3. Select the day of week (Sunday is selected by default; If All is selected, the setting is applied to the whole week. You can also select the checkbox next to the day to set it separately). 4. After completing the setting, click Save to go back to the rule configuration page.

Step 7 Click **Save** on the **Construction Monitoring** page.



If you want to see the alarm information on the **Alarm** tab, you need to subscribe the corresponding alarm type. For details, see "6 Alarm".

Results

Click the **AI Live** tab to view construction monitoring results. For details, see "3.2 AI Live Settings".

5.5.7 Face Recognition

The function can detect faces and compare them with those in the configured face database.



- Select **Setting > Event > Smart Plan** to enable face recognition.
- This function is available on select models.

5.5.7.1 Face Detection

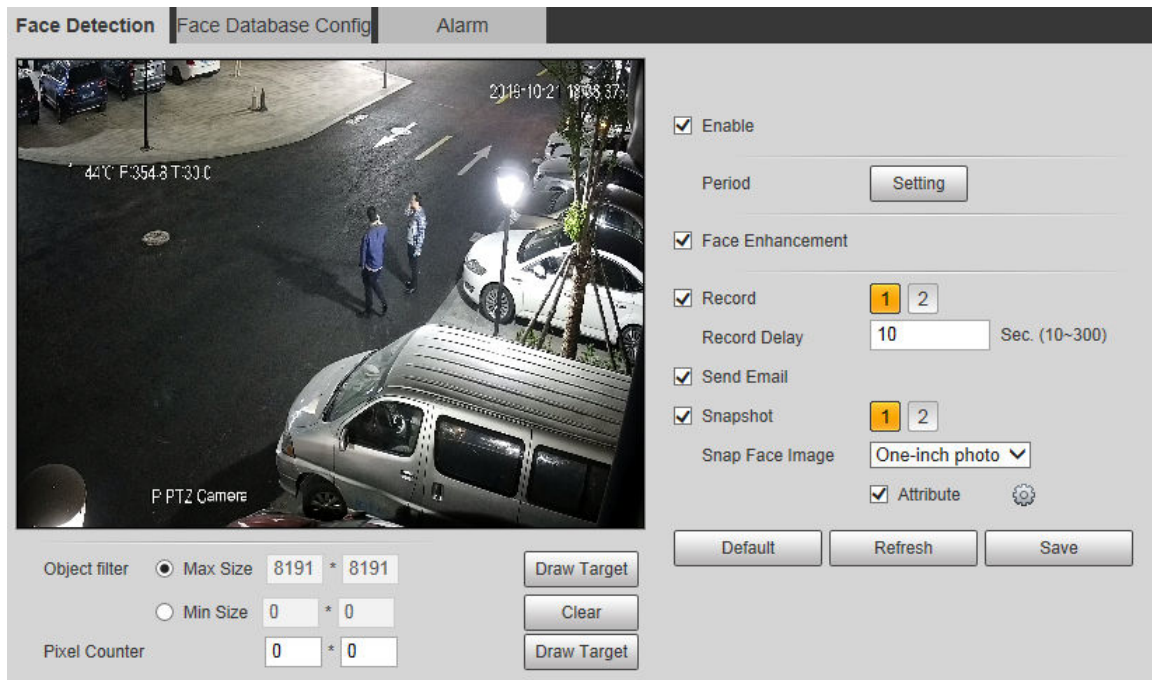
Background Information

When human face is detected in the monitoring screen, an alarm is triggered and the linked action is performed.

Procedure

Step 1 Select **Setting > Event > Face Recognition > Face Detection**.


Figure 5-103 Face detection page





Step 2 Select **Enable** to enable the face detection function.

Step 3 Configure face detection parameters.

Table 5-35 Description of face detection parameter

Parameter	Description
Period	Alarm event will be triggered only within the defined period. For details, see "5.5.1.1 Motion Detection".
Face Enhancement	Select Face Enhancement to preferably guarantee clear faces with low stream.
Record	<p>Select Record, and the system records video when alarms are triggered.</p> <p> To enable video recording, you need to make sure that:</p> <ul style="list-style-type: none"> The motion detection recording is enabled. For details, see "5.6.1.1 Record". The auto recording is enabled. For details, see "5.6.4 Record Control".
Record Delay	The video recording will not stop until the record delay time you set has passed.
Send Email	Select Send Email , and when alarms are triggered, the system sends email to the specified mailbox. For the email settings, see "5.2.5 SMTP (Email)".

Parameter	Description
Snapshot	<p>Select Snapshot, and the system takes snapshot when alarms are triggered.</p>  <ul style="list-style-type: none"> • Enable the motion detection snapshot first. For details, see "5.6.1.1 Record". • For searching and setting snapshot storage path, see "5.1.2.5 Path".
Snap Face Image	Set the snapshot scope, including Face and One-inch photo .
Attribute	Select the Attribute checkbox, click  , and then you can set the human attributes during face detection.

Step 4 Click **Save**.

5.5.7.2 Face Database Config

After you successfully configure the face database, the detected faces can be compared with the information in the face database. Configuring a face database includes creating a face database, adding face images, and face modeling.

5.5.7.2.1 Adding Face Database

Create a face database, and then register face images to add face images to the newly created face database.

Procedure

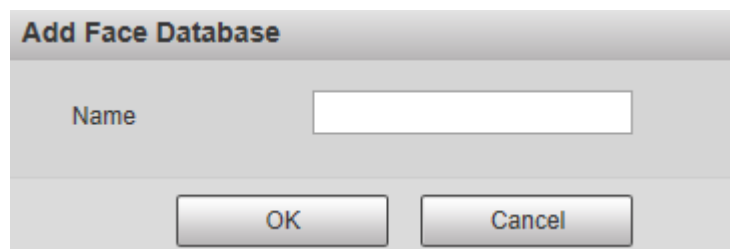
Step 1 Select **Setting** > **Event** > **Face Recognition** > **Face Database Config**.

Figure 5-104 Face database config



Step 2 Click **Add Face Database**.

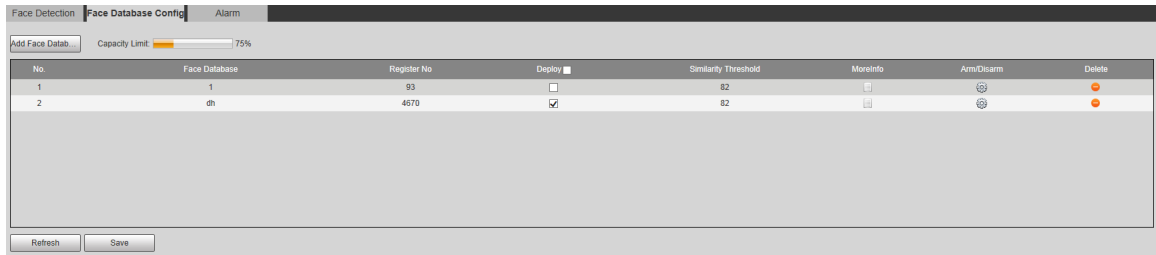
Figure 5-105 Add face database



Step 3 Set face database name.

Step 4 Click **OK** to complete the addition.

Figure 5-106 Add face database completed



Step 5 Configure face database configuration parameters.

Table 5-36 Description of face database config parameter

Parameter	Description
Deploy	Select Deploy and the face database takes effect.
Similarity Threshold	The comparison is successful only when the similarity between the detected face and the face feature in face database reaches the set similarity threshold. After this, the comparison result is displayed on the Live page.
More Info	Click More Info to manage face database. You can set search conditions, register people, and modify people information.
Arm/Disarm	Alarm event will be triggered only within the defined time period. For details, see "5.5.1.1 Motion Detection".
Delete	Delete the selected face database.

5.5.7.2.2 Adding Face Images (Manual Addition)

Add a single face image. Use this method when registering a small number of face images.

Procedure

Step 1 Select **Setting** > **Event** > **Face Recognition** > **Face Database Config**.


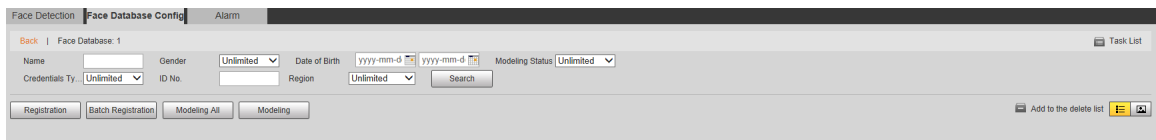
Step 2 Click  **More Info** for the face database to be configured.

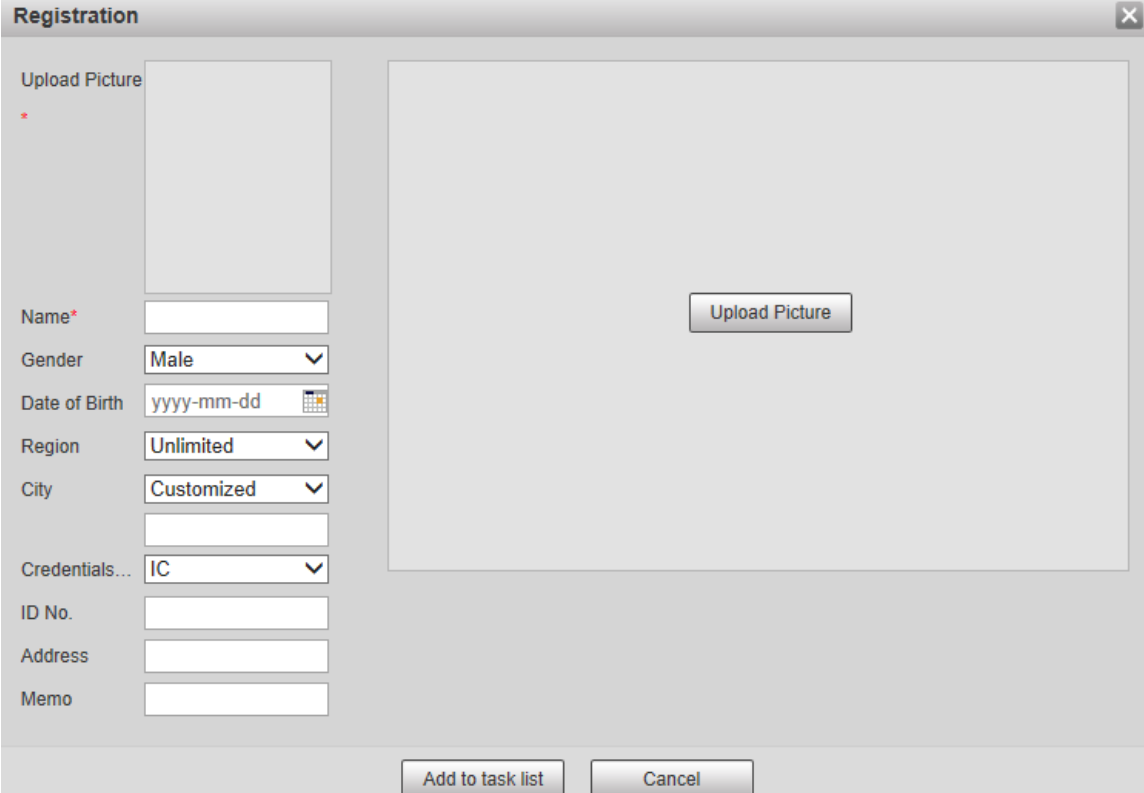
Figure 5-107 More info



Set filtering conditions, and then click **Search**. The search result is displayed.

Step 3 Click **Registration**.

Figure 5-108 Registration page

A screenshot of a web-based registration form titled "Registration". The form is divided into two main sections. On the left, there is a vertical list of input fields: "Upload Picture" (with a red asterisk), "Name*" (text box), "Gender" (dropdown menu with "Male" selected), "Date of Birth" (text box with "yyyy-mm-dd" placeholder and a calendar icon), "Region" (dropdown menu with "Unlimited" selected), "City" (dropdown menu with "Customized" selected), "Credentials..." (dropdown menu with "IC" selected), "ID No." (text box), "Address" (text box), and "Memo" (text box). On the right, there is a large rectangular area for image upload, containing a single "Upload Picture" button. At the bottom of the form, there are two buttons: "Add to task list" and "Cancel".

Step 4 Click **Upload Picture**, and then import the face pictures to be uploaded.



You can manually select a face area. After uploading the picture, select a face area and click **OK**. If there are multiple faces in an image, select the target face and click **OK** to save the face image.

Figure 5-109 Addition completed



The Registration window contains the following fields and controls:

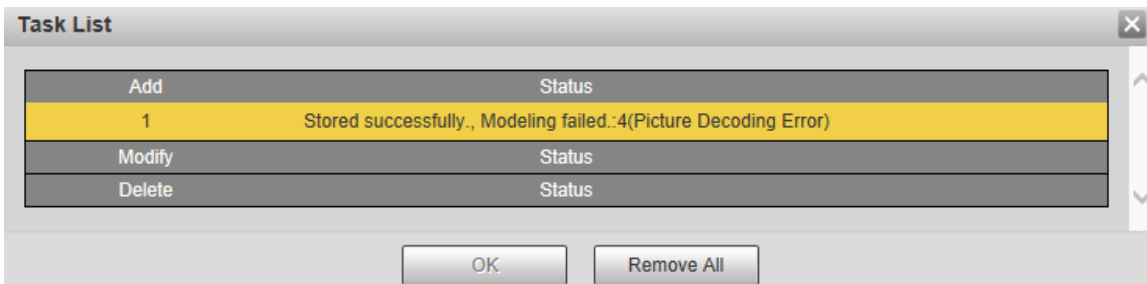
- Upload Picture:** A small thumbnail of the face image and a larger preview window with 'OK' and 'Cancel' buttons.
- Name:** A text input field.
- Gender:** A dropdown menu set to 'Male'.
- Date of Birth:** A date picker set to 'yyyy-mm-dd'.
- Region:** A dropdown menu set to 'Unlimited'.
- City:** A dropdown menu set to 'Customized'.
- Credentials:** A dropdown menu set to 'IC'.
- ID No.:** A text input field.
- Address:** A text input field.
- Memo:** A text input field.
- Buttons:** 'Add to task list' and 'Cancel' at the bottom.

Step 5 Fill in face image information.

Step 6 Click **Add to task list**.

Step 7 Click  **Task List 1**.

Figure 5-110 Task list addition completed



The Task List window displays a table with the following data:

Add	Status
1	Stored successfully., Modeling failed.:4(Picture Decoding Error)
Modify	Status
Delete	Status

Buttons: OK, Remove All



Click **Remove All** to remove all the tasks.

5.5.7.2.3 Adding Face Images (Batch Registration)

Background Information

You can import multiple face images in batches. Use this method when registering a large number of face images.

Before importing images in batches, name the face images in the format of "Name#SGender#BDate of Birth#NRegion#TCredentials Type#MID No. jpg" (for example, "John#S1#B1990-01-01#NCN#T1#M330501199001016222").



Name is required and the rest are optional.

Table 5-37 Naming rules for batch import

Naming Rules	Description
Name	Enter the corresponding name.
Gender	Enter a number. 1: Male; 2: Female.
Date of Birth	Enter numbers in the format of yyyy-mm-dd. For example, 2017-11-23.
Region	Enter the region name.
Credentials Type	Enter a number. 1: ID card; 2: passport.
ID No.	Enter ID No.

Procedure


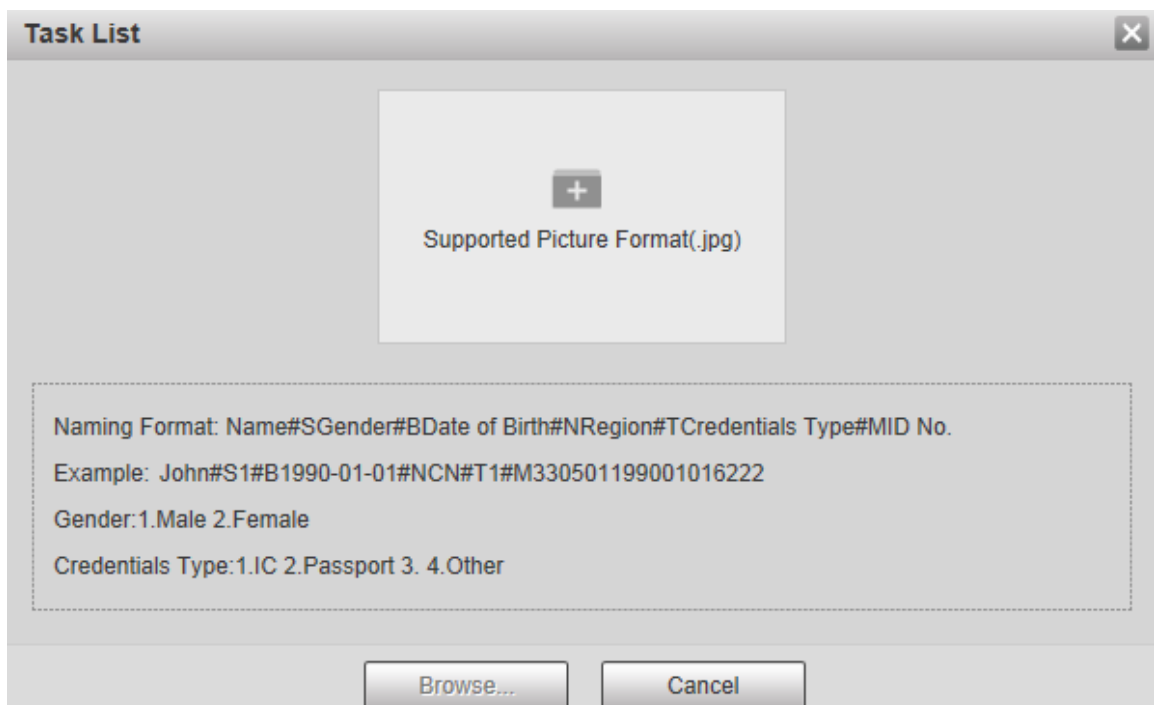
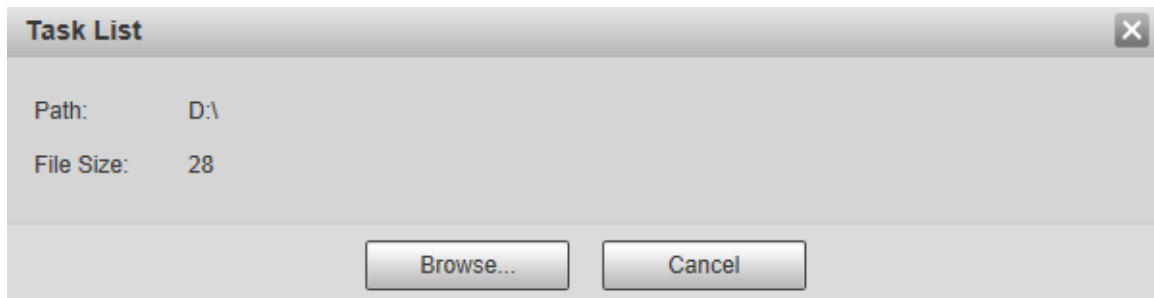
- Step 1** Select **Setting > Event > Face Recognition > Face Database Config**.
The **Face Database Config** page is displayed.
- Step 2** Click  **More Info** for the face database to be configured.
The **Face Database** page is displayed.
- Step 3** Click **Batch Registration**.

Figure 5-111 Batch registration



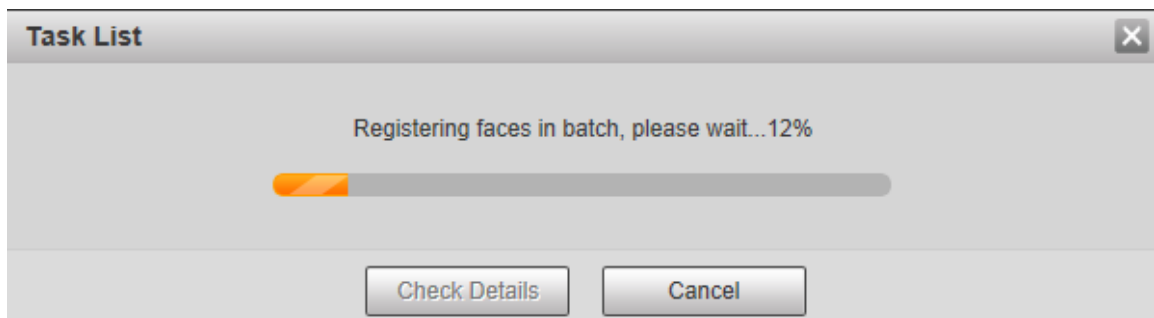
- Step 4** Click  to select the file path.

Figure 5-112 Batch registration



Step 5 Click **Browse**.

Figure 5-113 Registering



Step 6 After the registration is completed, click **Next** to view the registration result.

5.5.7.2.4 Managing Face Images

You can add face images to face database; manage and maintain face images to ensure correct information.

Modifying Face Information



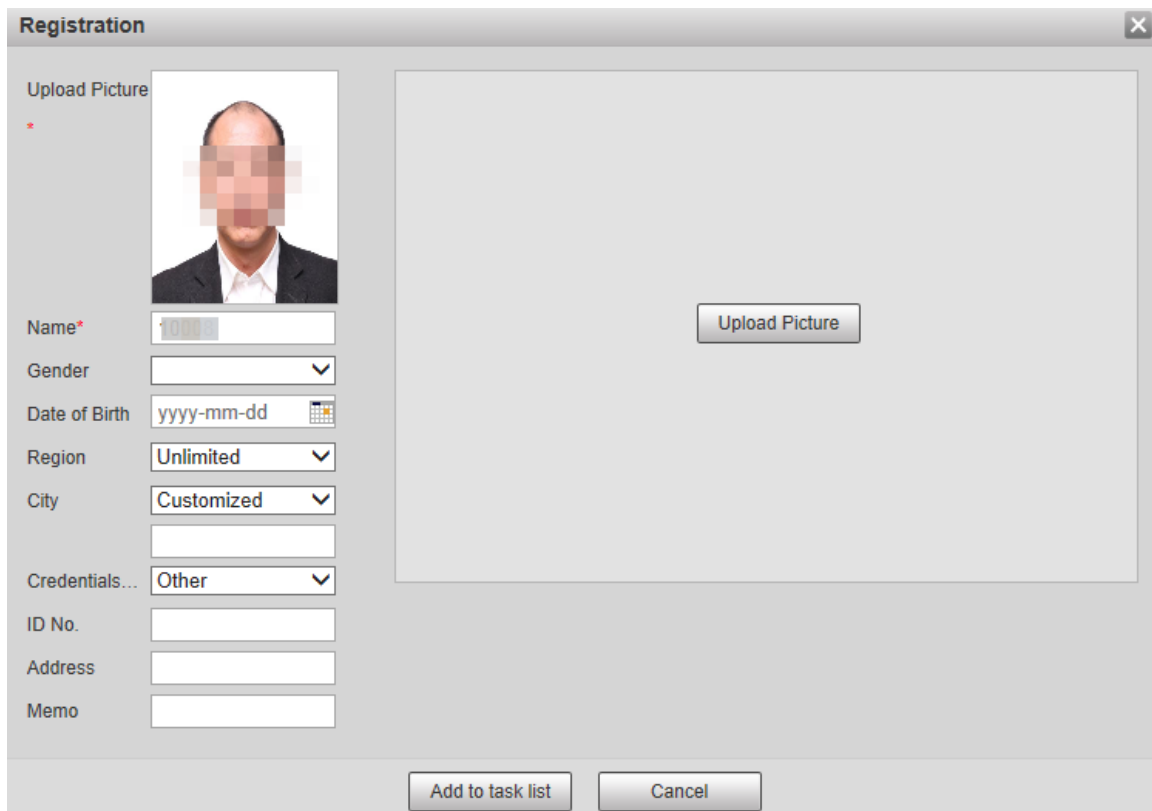
On the **Face Database Config** page, move the mouse pointer to the face image or person information line, and then click  or . After modifying the face image information, click **Add to task list**.





Figure 5-114 Registration page



The screenshot shows a 'Registration' window with a close button (X) in the top right corner. On the left, there is a vertical list of fields: 'Upload Picture' (with a red asterisk), 'Name*' (text input), 'Gender' (dropdown), 'Date of Birth' (calendar icon), 'Region' (dropdown), 'City' (dropdown), 'Credentials...' (dropdown), 'ID No.' (text input), 'Address' (text input), and 'Memo' (text input). To the right of these fields is a large rectangular area for a face image, with an 'Upload Picture' button centered within it. At the bottom of the window are two buttons: 'Add to task list' and 'Cancel'.

Deleting Face Images

Enter face database, and then delete the created face image.

- Single deletion: Move the mouse pointer to the face image or people information line, and then click  or  to delete the face image.
- Batch deletion: Move the mouse pointer to the face image or people information line, and then click ☐ at the upper right corner of the face images, or click ☐ on person information line. After selecting multiple items, click **Add to the delete list**, click , and then click **OK** to delete the selected face images.
- Delete all: When viewing face images in a list, click ☐ on people information line (or select **All** when viewing face images in images), click **Add to the delete list**, click , and then click **OK** to delete all face images.

5.5.7.2.5 Face Modeling

Background Information

You can extract and import the relevant information of face images into the database through face modeling, and create a face feature mode for smart detection such as face comparison.



- The more face images you choose, the longer the modeling time is.
- During the modeling process, some smart detection functions (such as face comparison) are temporarily unavailable and can be resumed after the modeling is complete.

Procedure

Step 1 Select **Setting** > **Event** > **Face Recognition** > **Face Database Config**.


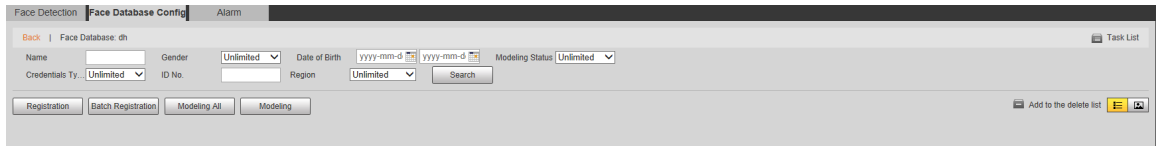
Step 2 Click  **More Info** for the face database to be configured.

Figure 5-115 Face database page



Step 3 Select the face images for modeling



Click  to view the face image in a list. Click  to view the face image as a thumbnail.

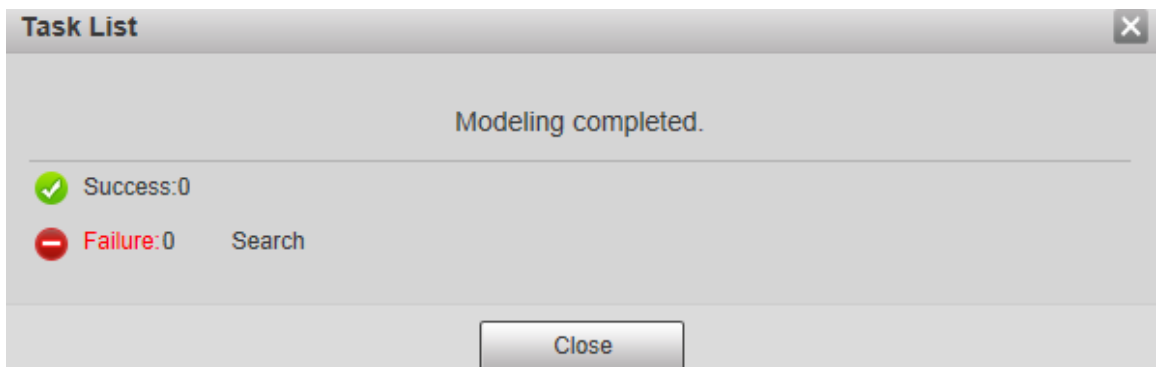
- Modeling All

Click **Modeling All**, and all face images in the face database will be modeled.

- Selective Modeling

If there are many face images in the face database, set filtering conditions and then click **Search** to select face images for modeling.

Figure 5-116 Modeling completed



5.5.7.3 Alarm Linkage

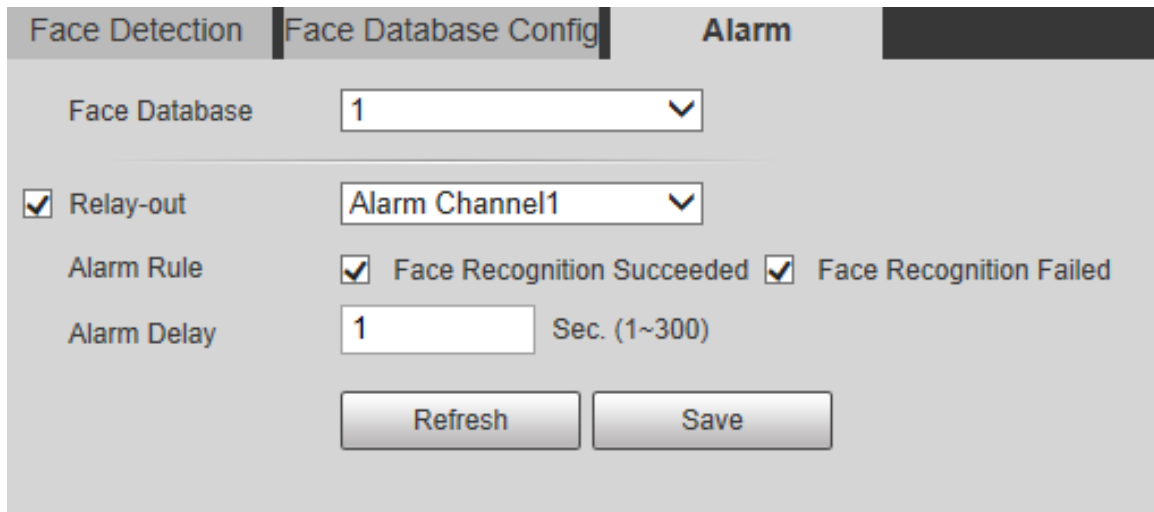
Background Information

Set the alarm linkage mode for face comparison.

Procedure

Step 1 Select **Setting** > **Event** > **Face Recognition** > **Alarm**.

Figure 5-117 Alarm linkage



Step 2 Configure alarm linkage parameter.

Table 5-38 Description of alarm linkage parameter

Parameter	Description
Face Database	Select the face database to be configured with alarm linkage.
Alarm Rule	Select the alarm rule as needed.
Relay-out	Select the Relay-out checkbox, and when an alarm is triggered, the system interacts with the linked alarm devices.
Alarm Delay	The alarm will continue for an extended period of time. The value range is 1–300 s.

Step 3 Click **Save**.

5.5.8 People Counting

You can use this function to count the number of people in the area and generate reports.



- Before using this function, you need to enable **People Counting** in **Smart Plan**.
- The people counting data will be overwritten if the disk is full. Back up the data in time as needed.
- This function is available on select models.

5.5.8.1 People Counting Settings

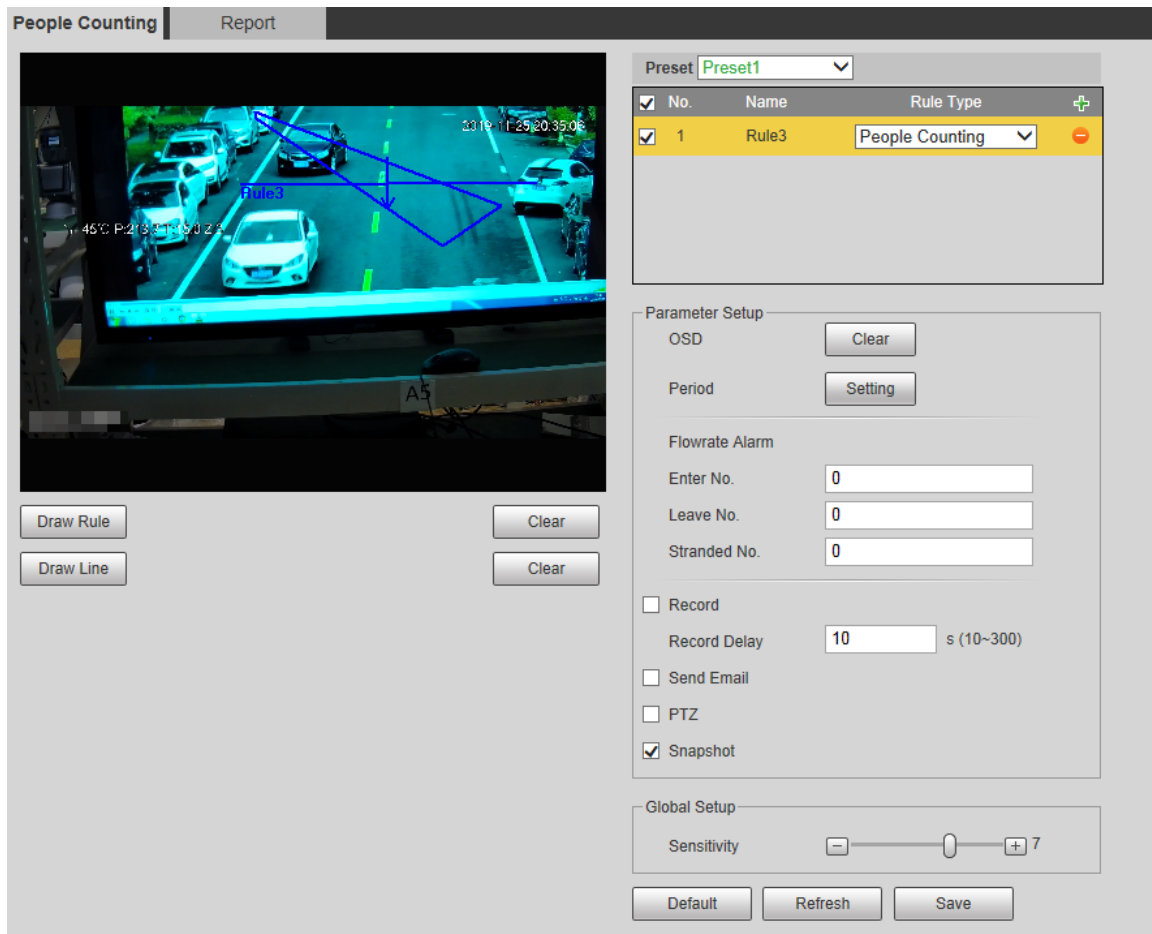
Background Information

With the function, the system can count the number of people appearing in the monitoring screen within a certain period.

Procedure

Step 1 Select **Setting** > **Event** > **People Counting** > **People Counting**.

Figure 5-118 People counting settings



Step 2 Select the presets to be configured.

Step 3 Click **Draw Rule**, and you can draw rules on the monitoring screen. For parameter description, see "5.5.5.1 Tripwire".



Click **Clear** to the right of **Draw Rule**, and you can clear all drawn rules.

Step 4 Configure people counting parameter.

Table 5-39 Description of people counting parameter

Parameter	Description
OSD	Display the number of people displayed in the area in real time. Click Clear , and the current number will be zero.
Enter No.	Set the Enter No. , and when the number of people entering reaches the set value, an alarm will be triggered.
Leave No.	Set the Leave No. , and when the number of people leaving reaches the set value, an alarm will be triggered.
Stranded No.	Set the Stranded No. , and when the number of people staying reaches the set value, an alarm will be triggered.



For other parameters, see "5.5.5.1 Tripwire".

Step 5 Click **Save**.

5.5.8.2 Report

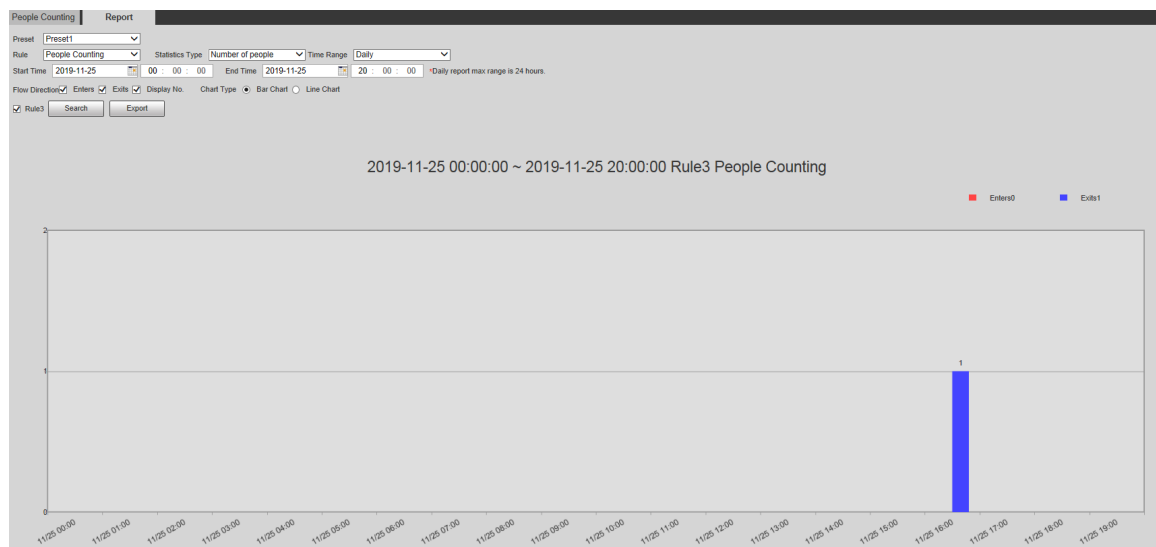
Background Information

You can view the statistics results of people in the scene during the selected period.

Procedure

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

Figure 5-119 People counting report



Step 2 Select a preset.

Step 3 Select the **Rule**, **Statistics Type**, and **Time Range**.

Step 4 Select the start time and end time for searching reports.

Step 5 Select **Flow Direction** and **Chart Type**.

Step 6 Click **Search** to generate reports, and then click **Export** to export the report to local storage.

5.5.9 Heat Map



- Before enabling **Heat Map**, you need to set presets in **PTZ** section, and select the function in the **Smart Plan**.
- The data will be overwritten if the disk is full. Back up the data in time.
- This function is available on select models.

5.5.9.1 Heat Map Settings

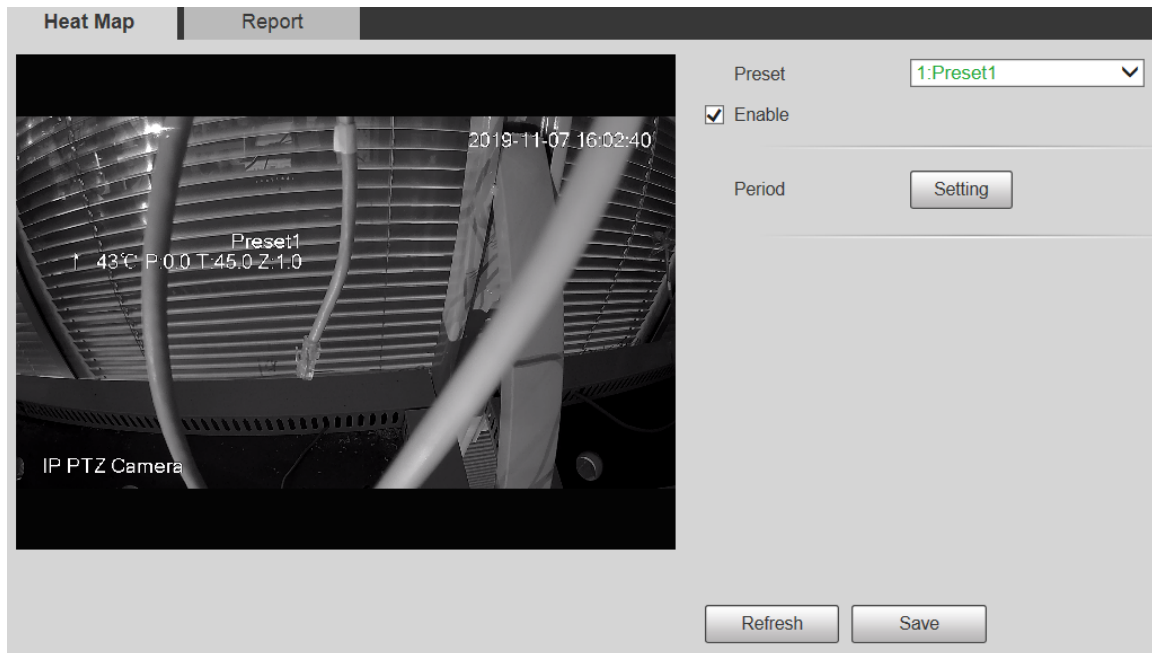
Background Information

The function can be used to detect the activity level of moving objects in the scene during a certain period.

Procedure

Step 1 Select **Setting** > **Event** > **Heat Map** > **Heat Map**.

Figure 5-120 Heat map



- Step 2 Select the presets to be configured.
- Step 3 Select the **Enable** checkbox to enable heat map function.
- Step 4 Click **Setting** to set the arming period. For details, see "5.5.1.1 Motion Detection".
- Step 5 Click **Save**.

5.5.9.2 Report

Background Information

You can view the heat map report for the scene in the selected period.

Procedure

- Step 1 Select **Setting > Event > Heat Map > Report**.
- Step 2 Set the start time and end time to search for the heat map report.
- Step 3 Select a preset.
- Step 4 Click **Search**, and the search results will be displayed on the page.

Figure 5-121 Report



5.5.10 Video Metadata

With the function, the system can count the number of motor vehicles, non-motor vehicles and people in the monitoring screen, identify the features of the vehicles and people in the scene, and take snapshots.



- Before using video metadata, you need to enable the function in the **Smart Plan**.
- This function is available on select models.

5.5.10.1 Scene Setting

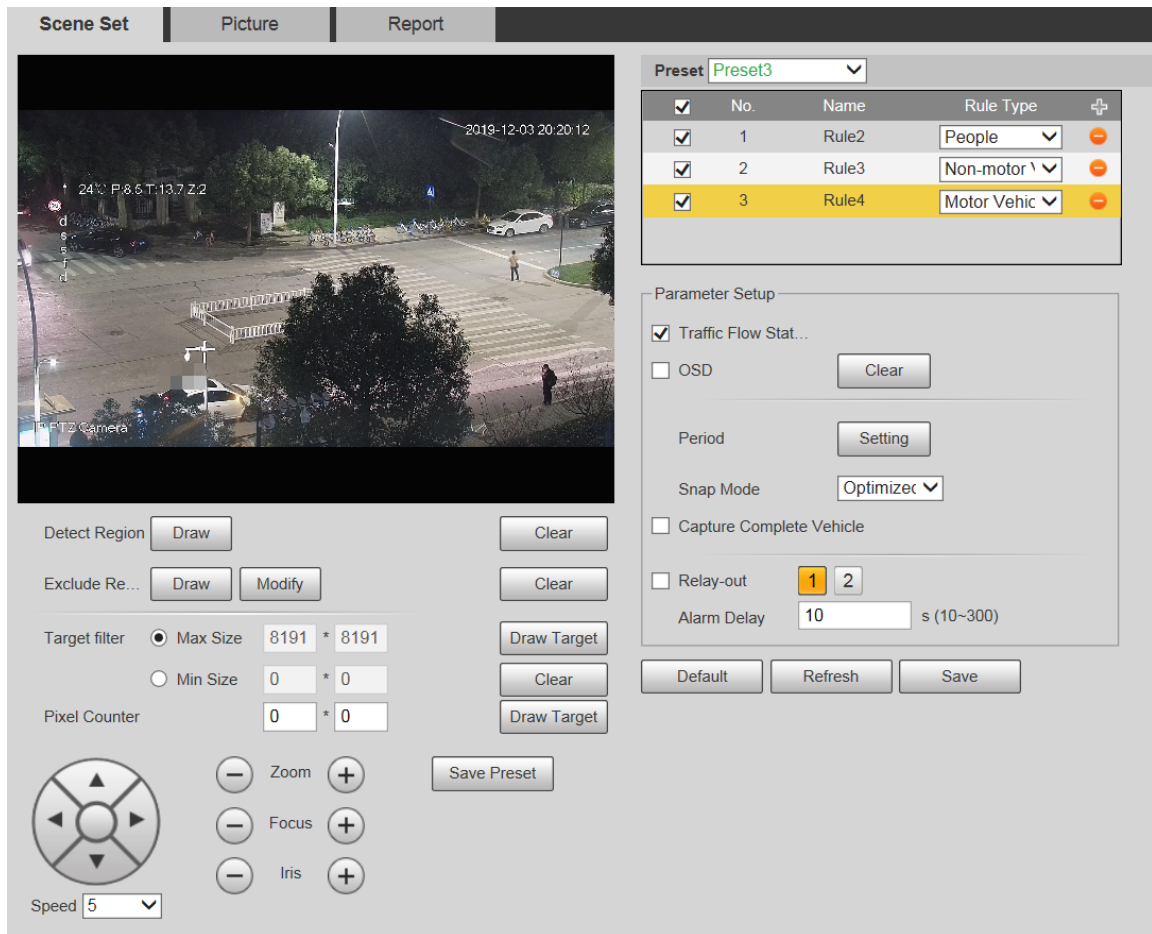
Background Information

Set the parameters of snapshot, analysis and alarm in the scene.

Procedure

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


Figure 5-122 Scene setting



Step 2 Click the **Preset** list to select the preset to configure video metadata.

Step 3 Click  to add a rule type.

Step 4 Modify the parameters.

- Double-click the name to modify the rule name.
- Select the rule type from **People**, **Non-motor Vehicle** and **Motor Vehicle**.
- Click the corresponding  to delete detection items.

Step 5 Configure scene setting parameters.

Table 5-40 Description of scene setting parameter

Parameter	Description
People Flow Statistics	After selection, traffic flow statistics will be displayed on the screen.
Non-motor Vehicle Flow Statistics	
Traffic Flow Statistics	
OSD	Select the checkbox to enable the OSD overlay. The statistics will be displayed on the Live page in the form of OSD information.
Clear	Click it to clear the statistics of motor vehicles, non-motor vehicles and people.



For other parameters, see "5.5.5.1 Tripwire".

Step 6 Click **Save**.

5.5.10.2 Picture Overlay

Background Information

Set the overlay information on the snapshot.

Procedure

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

Step 2 Select **Picture Overlay Type** from **People**, **Non-motor Vehicle** and **Motor Vehicle**.

Figure 5-123 Picture overlay–motor vehicle

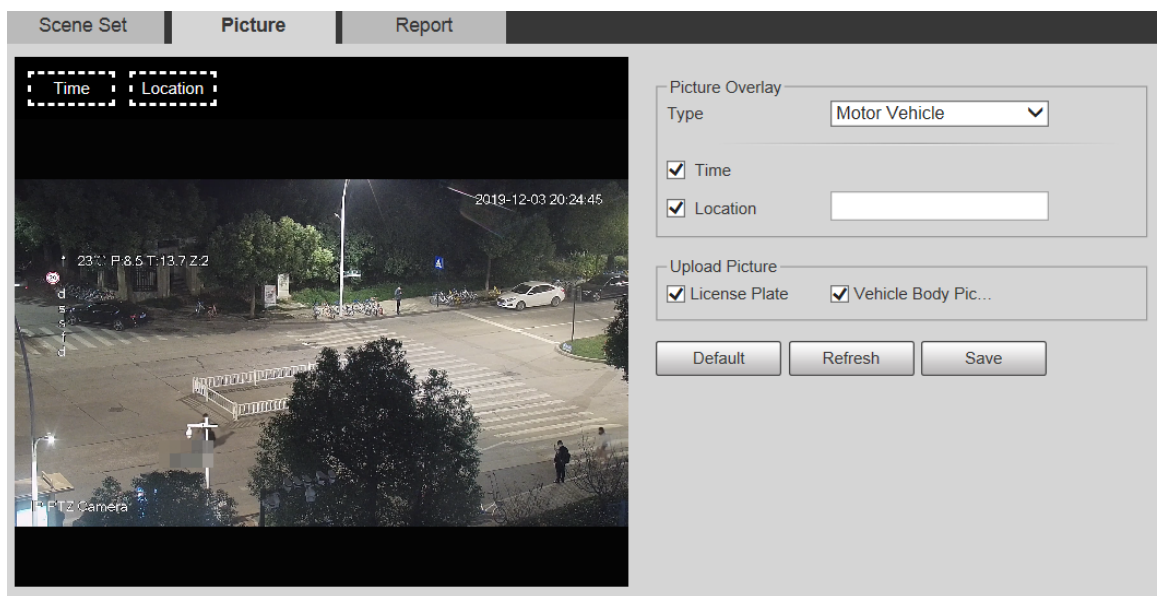


Figure 5-124 Picture overlay–non-motor vehicle

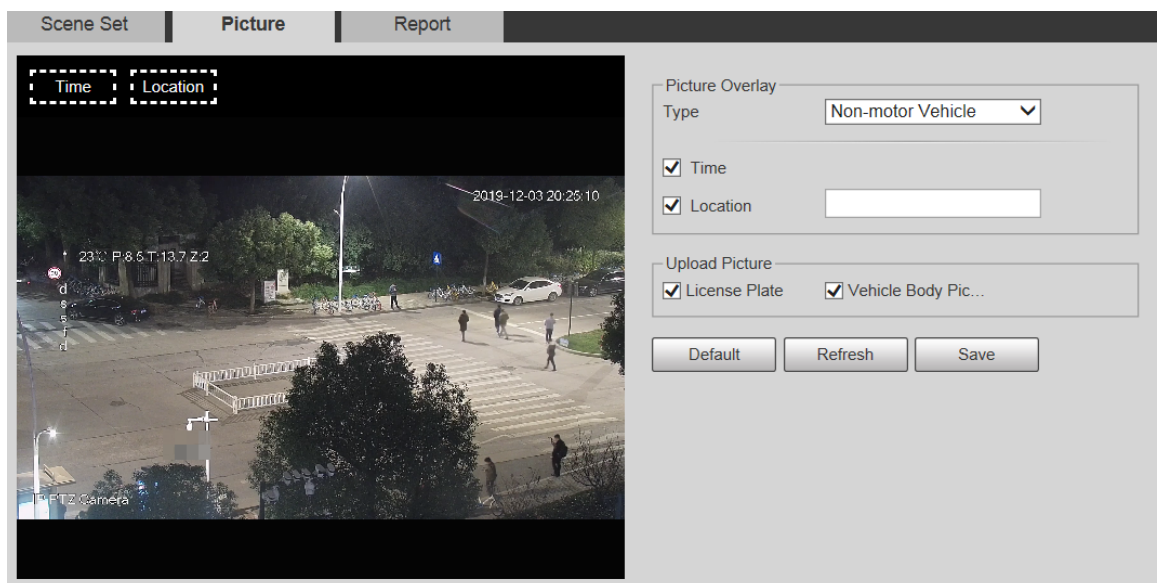
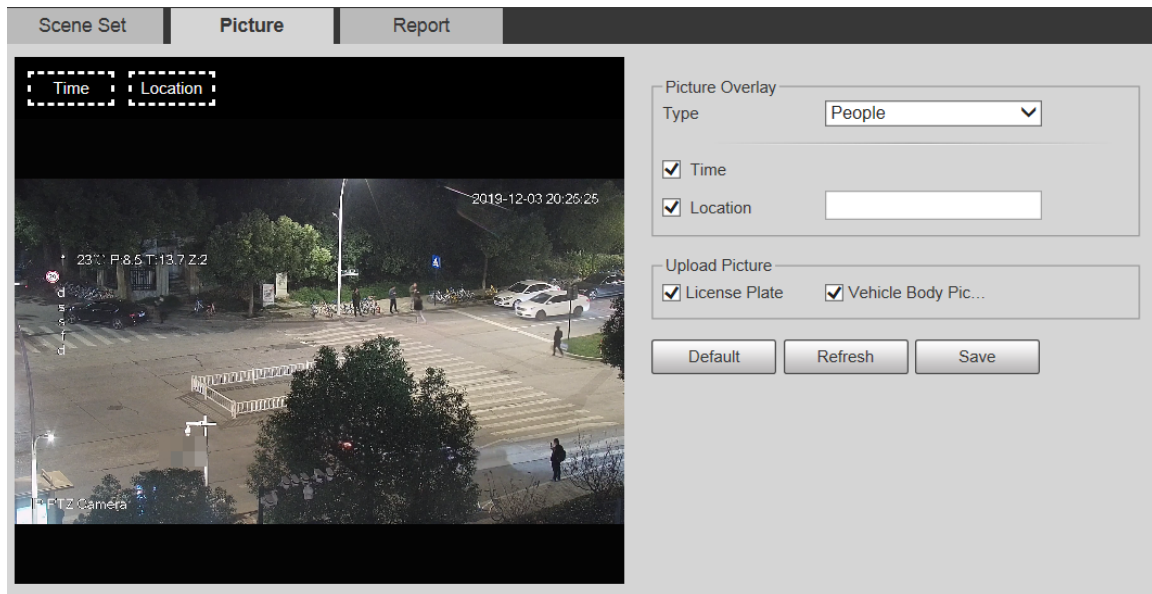


Figure 5-125 Picture overlay–people



Step 3 Select overlay information.



If you select **Location**, you need to manually enter the location of the Device.

Step 4 Click **Save**.

5.5.10.3 Report

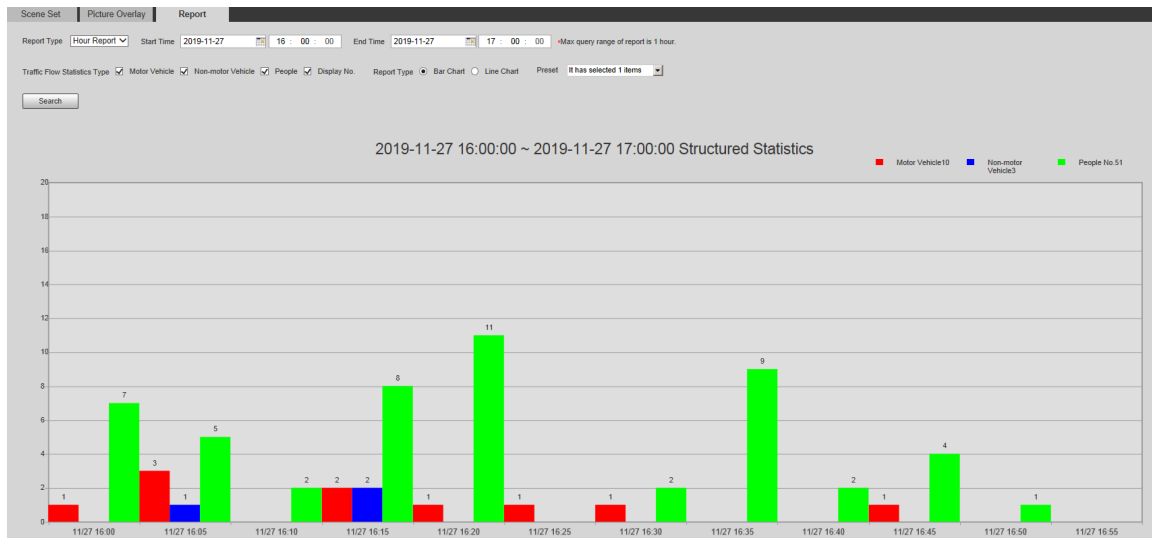
Background Information

You can view the number of vehicles, non-vehicles and people in the scene during the selected period.

Procedure

- Step 1** Select **Setting > Event > Video Metadata > Report**.
- Step 2** Select the **Report Type**.
- Step 3** Select the start time and end time for searching reports.
- Step 4** Select **Traffic Flow Statistics Type**.
- Step 5** Click **Search** to generate reports.

Figure 5-126 Video metadata report



5.5.11 Alarm

Procedure

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

Figure 5-127 Alarm

Alarm

☐ Enable

Relay-in

Alarm1

Period

Setting

Anti-Dither

0

 s (0~100)
 Sensor Type

NO

☒ Record

Record Delay

10

 s (10~300)

☒ Relay-out

1

2

Alarm Delay

10

 s (10~300)

☐ Send Email

☐ PTZ

☒ Snapshot

Default

Refresh

Save

Step 2 Configure alarm setting parameters.

Table 5-41 Description of alarm setting parameter

Parameter	Description
Enable	Select the Enable checkbox, and then the alarm linkage is enabled.
Relay-in	Select alarm input, and 7 alarm inputs are available.
Sensor Type	There are two types: NO (normally open) and NC (normally closed). Switch from NO to NC , and alarm event will be enabled. Switch from NC to NO , and alarm event will be disabled.



For other parameters, see "5.5.1.1 Motion Detection".

Step 3 Click **Save**.

5.5.12 Abnormality

Abnormality includes 7 alarm events: **No SD Card**, **Capacity Warning**, **SD Card Error**, **Disconnection**, **IP Conflict**, **Illegal Access**, and **Security Exception**.

5.5.12.1 SD Card

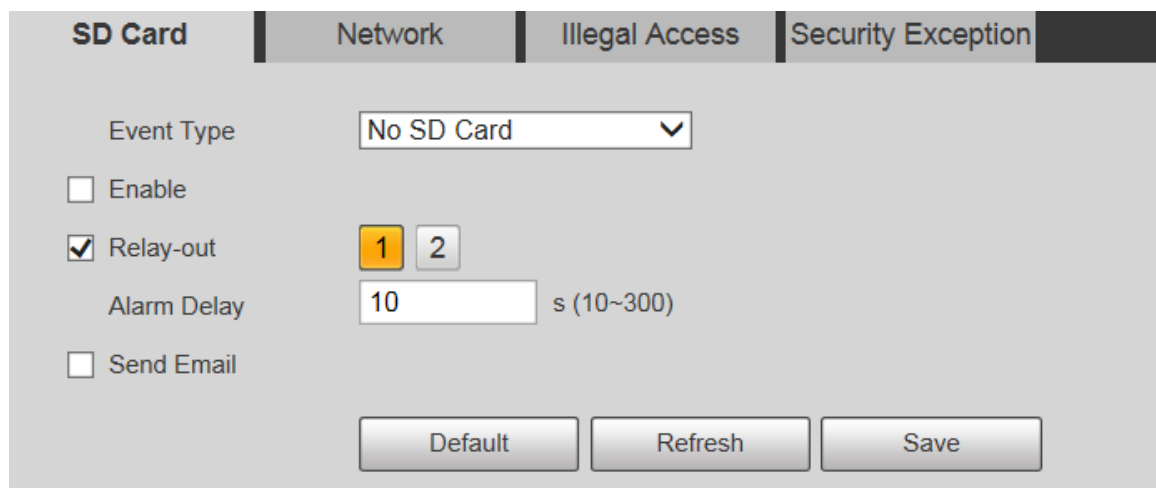
Background Information

In case of an SD card exception, an alarm will be triggered.

Procedure

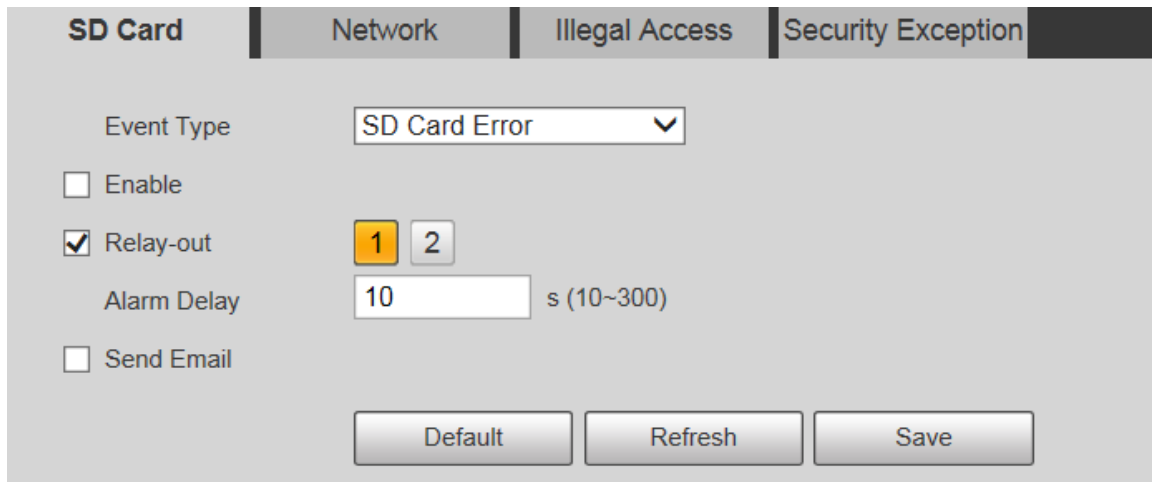
Step 1 Select **Setting** > **Event** > **Abnormality** > **SD Card**.

Figure 5-128 No SD card



The screenshot shows the 'SD Card' configuration page. At the top, there are four tabs: 'SD Card', 'Network', 'Illegal Access', and 'Security Exception'. The 'SD Card' tab is selected. Below the tabs, the 'Event Type' is set to 'No SD Card'. There are four checkboxes: 'Enable' (unchecked), 'Relay-out' (checked), 'Alarm Delay' (set to 10 s), and 'Send Email' (unchecked). At the bottom, there are three buttons: 'Default', 'Refresh', and 'Save'.

Figure 5-129 SD card error



SD Card | Network | Illegal Access | Security Exception

Event Type: SD Card Error

☐ Enable

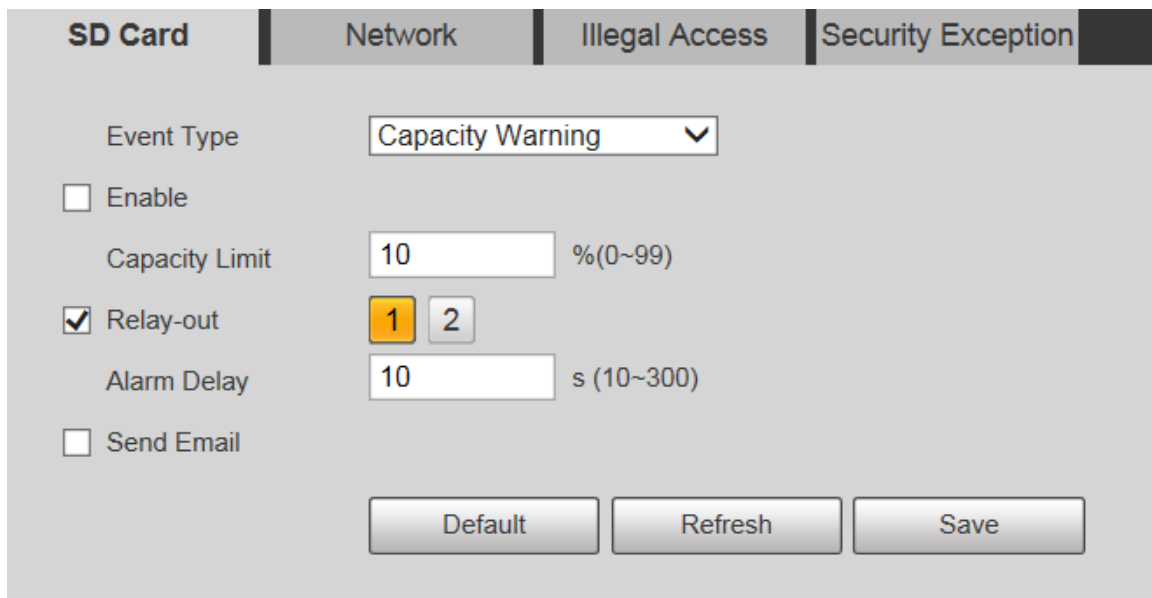
☒ Relay-out

Alarm Delay: 10 s (10~300)

☐ Send Email

Default Refresh Save

Figure 5-130 Capacity warning



SD Card | Network | Illegal Access | Security Exception

Event Type: Capacity Warning

☐ Enable

Capacity Limit: 10 % (0~99)

☒ Relay-out

Alarm Delay: 10 s (10~300)

☐ Send Email

Default Refresh Save

Step 2 Configure SD card exception parameters.

Table 5-42 Description of SD card exception parameter

Parameter	Description
Enable	Select the checkbox to enable this function.
Capacity Limit	Configure the free space percentage, and if the free space in the SD card is less than the defined percentage, an alarm is triggered.



For other parameters, see "5.5.1.1 Motion Detection".

Step 3 Click **Save**.

5.5.12.2 Network Exception

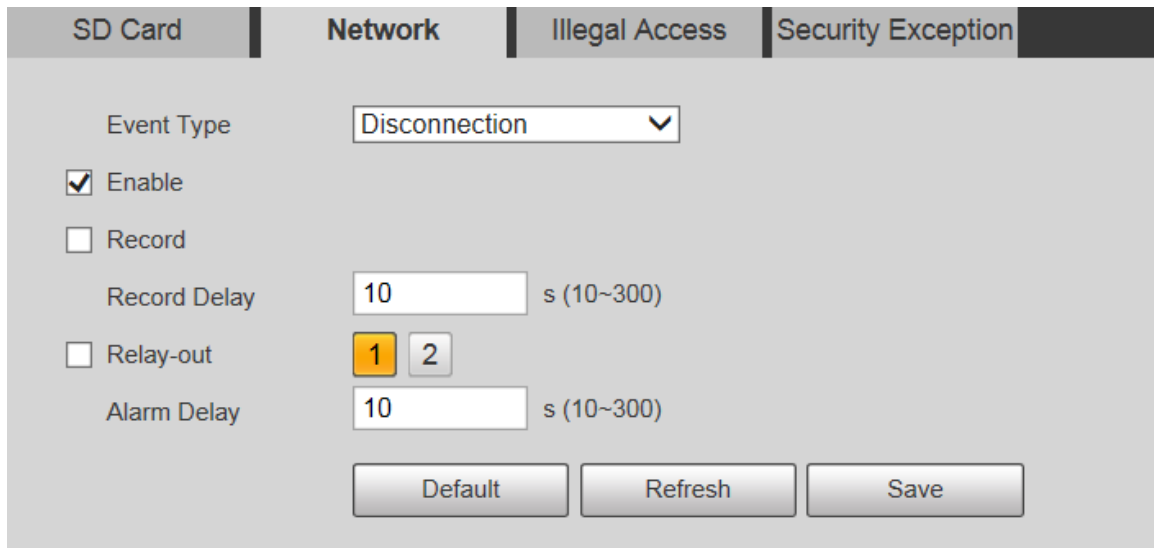
Background Information

In case of a network exception, an alarm will be triggered.

Procedure

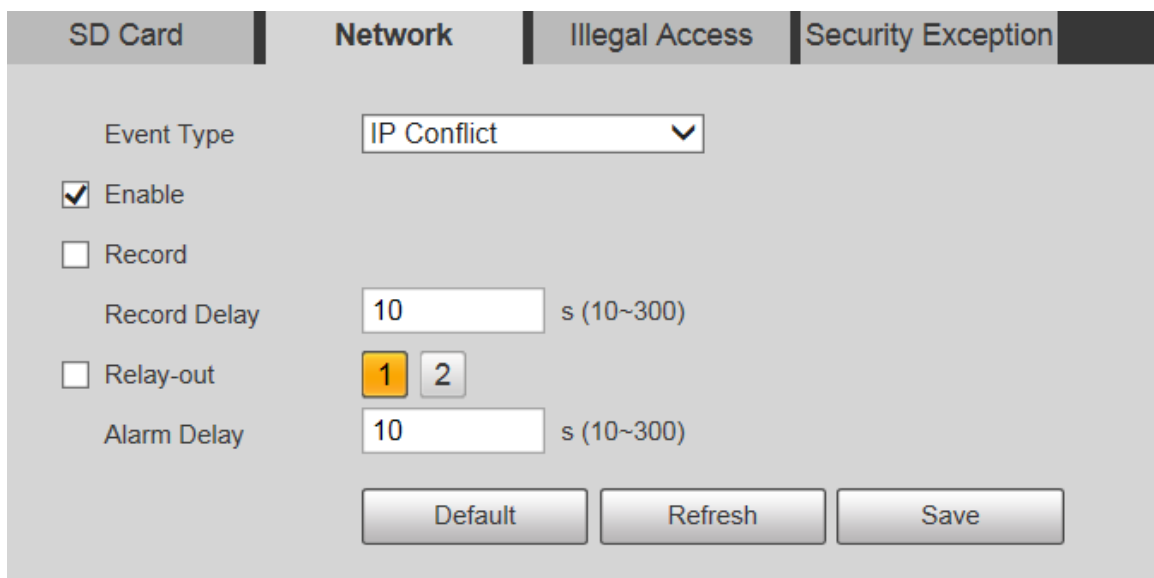
Step 1 Select **Setting** > **Event** > **Abnormality** > **Network**.

Figure 5-131 Disconnection



The screenshot shows the 'Network' tab selected in the top navigation bar. The 'Event Type' dropdown is set to 'Disconnection'. The 'Enable' checkbox is checked. The 'Record' checkbox is unchecked. The 'Record Delay' is set to 10 seconds. The 'Relay-out' checkbox is unchecked. The 'Alarm Delay' is set to 10 seconds. At the bottom, there are buttons for 'Default', 'Refresh', and 'Save'.

Figure 5-132 IP conflict



The screenshot shows the 'Network' tab selected in the top navigation bar. The 'Event Type' dropdown is set to 'IP Conflict'. The 'Enable' checkbox is checked. The 'Record' checkbox is unchecked. The 'Record Delay' is set to 10 seconds. The 'Relay-out' checkbox is unchecked. The 'Alarm Delay' is set to 10 seconds. At the bottom, there are buttons for 'Default', 'Refresh', and 'Save'.

Step 2 Configure network exception parameters.

Table 5-43 Description of network exception parameter

Parameter	Description
Enable	Select the checkbox to enable this function.



For other parameters, see "5.5.1.1 Motion Detection".

Step 3 Click **Save**.

5.5.12.3 Illegal Access

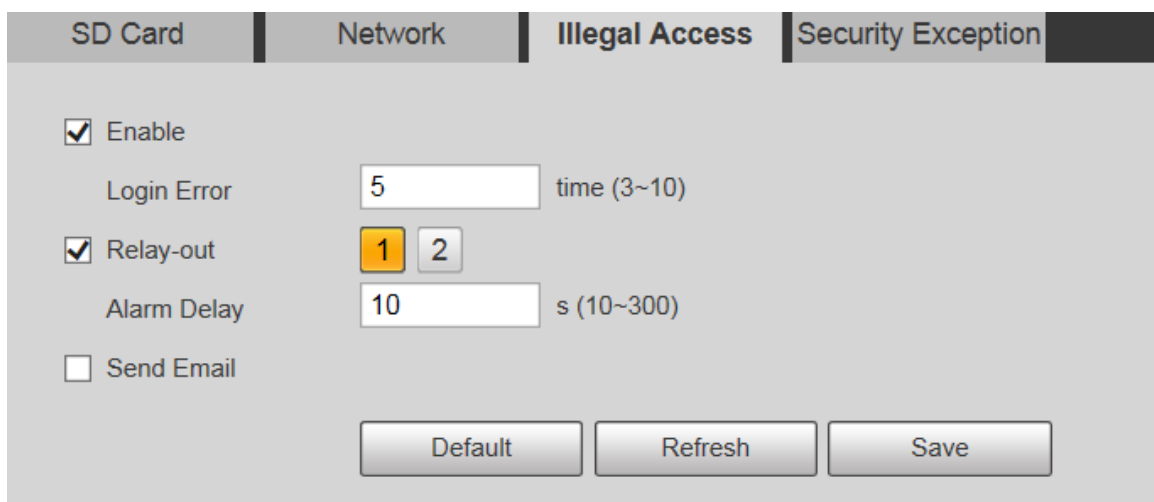
Background Information

Illegal access alarm is triggered when the login password has been wrongly entered for more than the times you set.

Procedure

Step 1 Select **Setting** > **Event** > **Abnormality** > **Illegal Access**.

Figure 5-133 Illegal access



Step 2 Configure illegal access parameters.

Table 5-44 Description of illegal access parameter

Parameter	Description
Enable	Select the checkbox to set the illegal access alarm.
Login Error	After entering a wrong password for the set times, the alarm for illegal access will be triggered, and the account will be locked.



For other parameters, see "5.5.1.1 Motion Detection".

Step 3 Click **Save**.

5.5.12.4 Security Exception

When an event affecting the Device safety occurs, an alarm for safety exception will be triggered.

Procedure

Step 1 Select **Setting** > **Event** > **Abnormality** > **Security Exception**.

Figure 5-134 Security exception



- Step 2** Configure security exception parameter.
For details, see "5.5.1.1 Motion Detection".
- Step 3** Click **Save**.

5.5.12.5 Battery Exception

Background Information

When overtemperature of the battery is detected, alarm linkage actions are performed.

Procedure

- Step 1** Select **Setting** > **Event** > **Abnormality** > **Battery Exception**.

Figure 5-135 Battery exception



- Step 2** Select the **Enable** checkbox to enable battery exception detection.
- Step 3** Set alarm linkage actions.
- Step 4** Click **Save**.

5.6 Storage

5.6.1 Schedule

Before setting the schedule, make sure that the **Record Mode** is **Auto** in **Record Control**.



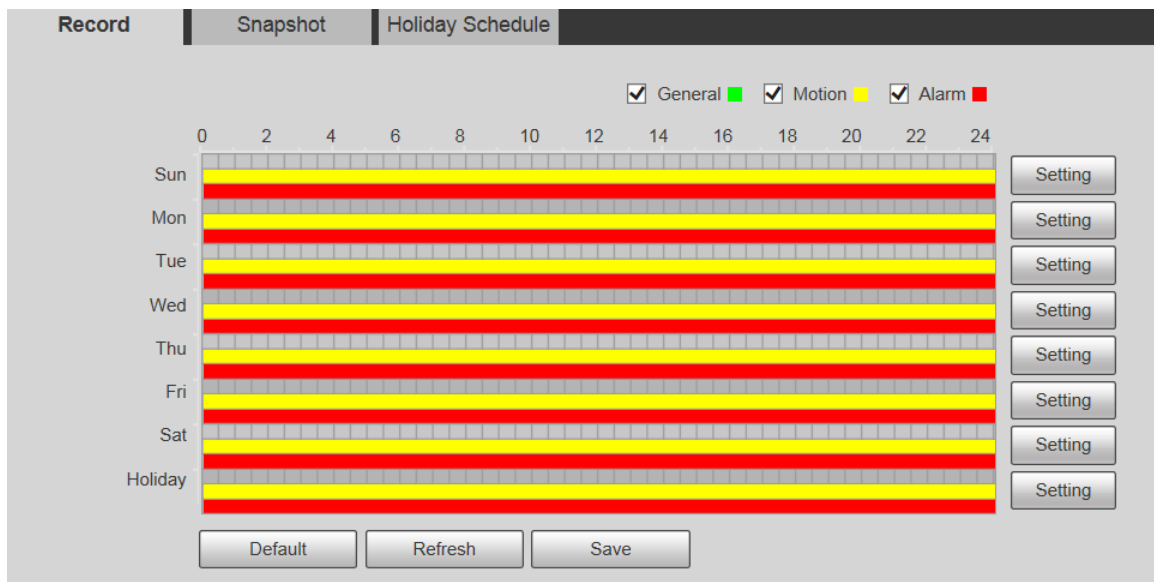
If the **Record Mode** is **Off**, the Device will not record or take snapshots according to the schedule.

5.6.1.1 Record

Procedure

Step 1 Select **Setting** > **Storage** > **Schedule** > **Record**.

Figure 5-136 Record



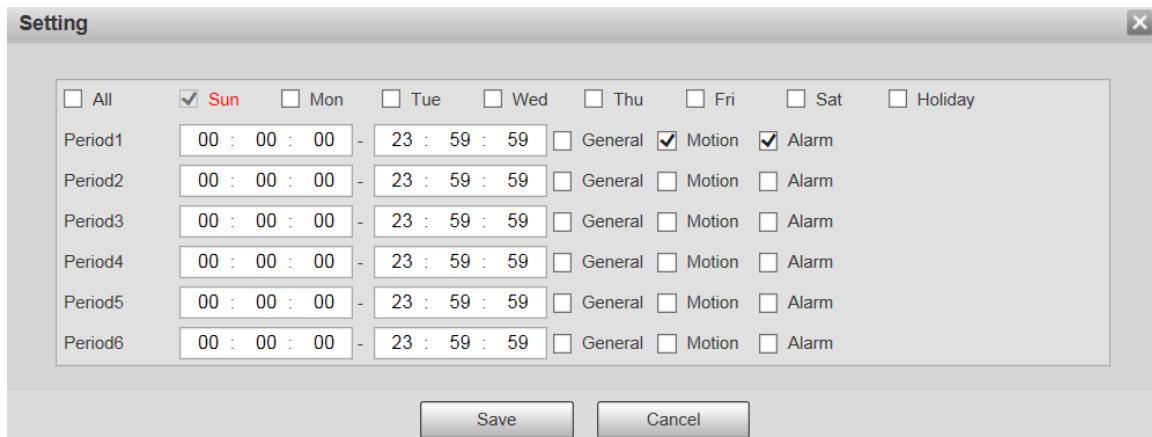
Step 2 Select the day for recording from Monday to Sunday, and then click **Setting** on the right.

- Set the recording period. You can set up to six periods for one day.
- You can select 3 types of recording: **General**, **Motion** and **Alarm**.



To set the time period, you can also press and hold the left mouse button and drag directly on the **Record** page.

Figure 5-137 Record schedule setting



Step 3 Click **Save** to return to the **Record** page.

At this time, the colored chart visually displays the defined period.




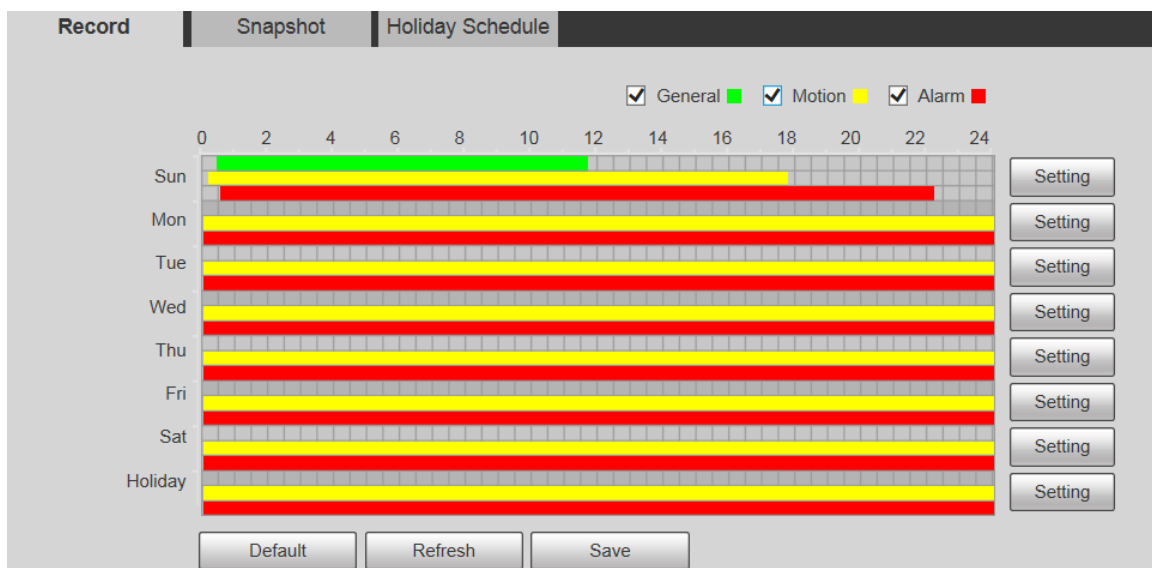
-  : Represents general recording.
-  : Represents motion detection recording.
-  : Represents alarm recording.

Figure 5-138 Recording schedule setting completed



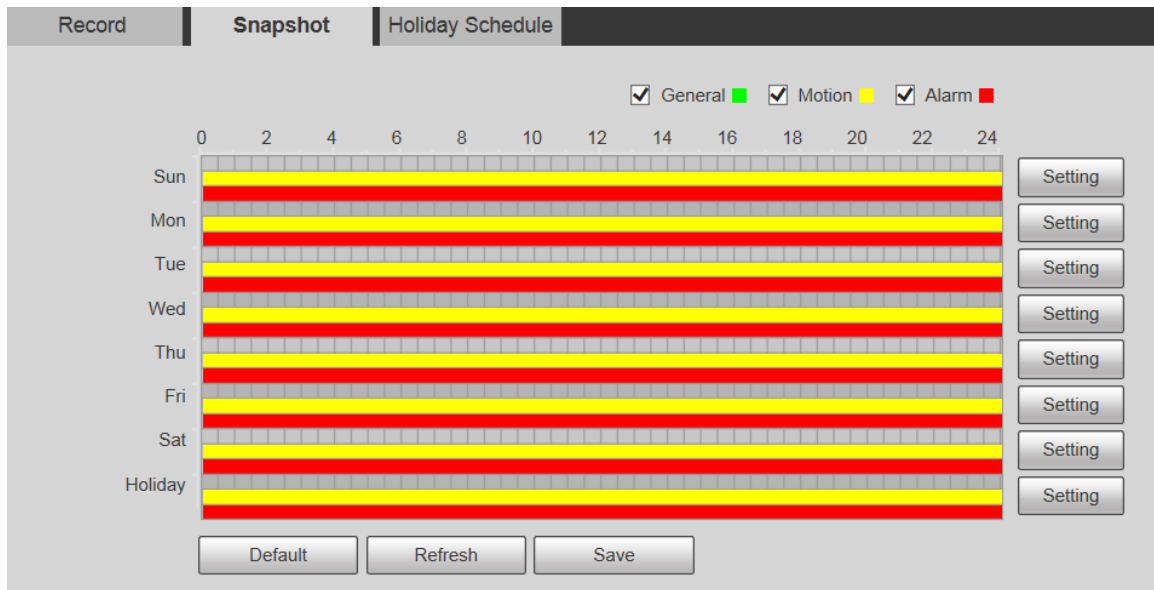
Step 4 On the **Record** page, click **Save**, and the **Save Succeeded!** prompt will be displayed, which means the recording schedule has been set.

5.6.1.2 Snapshot

Procedure

Step 1 Select **Setting** > **Storage** > **Schedule** > **Snapshot**.

Figure 5-139 Snapshot



Step 2 Set snapshot schedule.

For details, refer to "5.6.1.1 Record".

Step 3 Click **Save**, and the **Save Succeeded!** prompt will be displayed, which means the snapshot schedule has been set.

5.6.1.3 Holiday Schedule

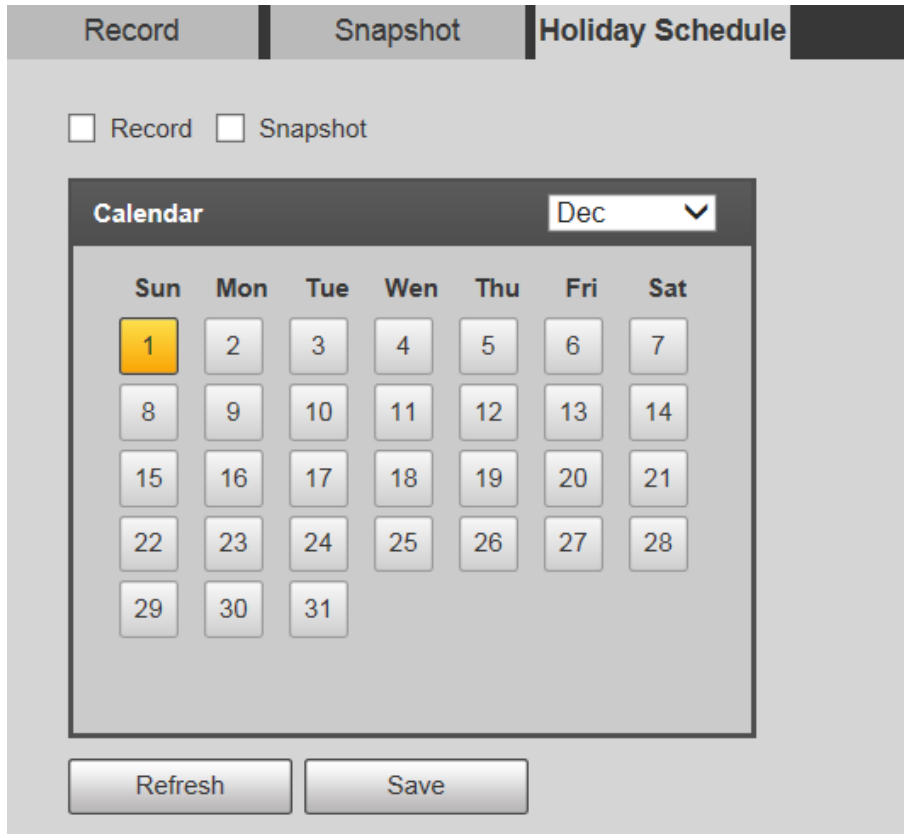
Background Information

You can set specific dates as holidays.

Procedure

Step 1 Select **Setting** > **Storage** > **Schedule** > **Holiday Schedule**.

Figure 5-140 Holiday schedule



Record Snapshot **Holiday Schedule**

☐ Record ☐ Snapshot

Calendar Dec ▼

Sun	Mon	Tue	Wen	Thu	Fri	Sat
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

Refresh Save

Step 2 Select a date.

The selected date will be a holiday and displayed in yellow.

Step 3 Select **Record** or **Snapshot**, and then click **Save**.

The **Save Succeeded!** prompt will be displayed.

Step 4 On the **Record** or **Snapshot** page, click **Setting** to the right of **Holiday**.



The setting method is the same as that of Monday to Sunday.

Step 5 Set the period of one day for the **Holiday**, and the recording or snapshot will be taken according to the holiday time period.

5.6.2 Snapshot by Location

Background Information

The system can take snapshots when the Device rotates to certain presets.

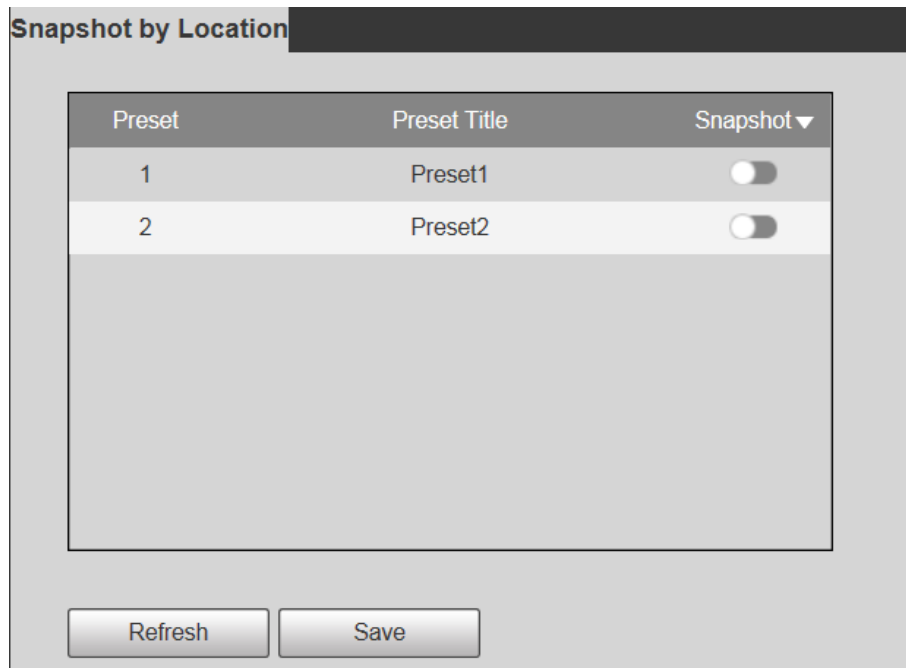


You need to set presets in advance.



Procedure

Step 1 Select **Setting** > **Storage** > **Snapshot by Location**.

Figure 5-141 Snapshot by location



Step 2 Select presets.

- Enable snapshot by location.
 - ◇ Click  to enable the function for the corresponding preset.
 - ◇ Click **Snapshot ▼**, and then select **All Enabled** to enable the function for all presets.
- Disable snapshot by location.
 - ◇ Click  to disable the function for the corresponding preset.
 - ◇ Click **Snapshot ▼**, and then select **All Disabled** to disable the function for all presets.

Step 3 Click **Save**.

5.6.3 Destination

5.6.3.1 Path

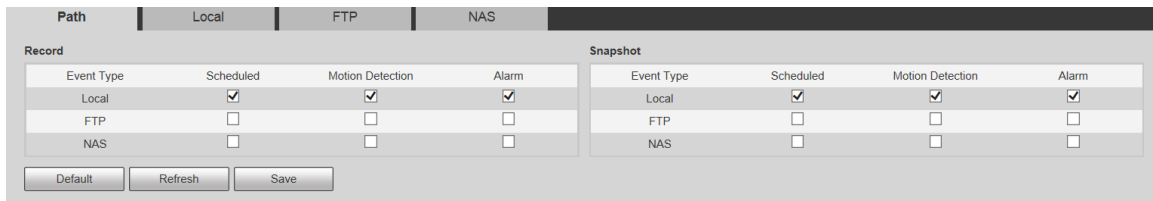
Background Information

Configure the storage path of recordings and snapshots of the Device, and select local SD card, FTP and NAS for storage. Store recordings and snapshots according to the event type, respectively corresponding to **General**, **Motion** and **Alarm** in the schedule, and then select the corresponding type of recordings or snapshots for storage.

Procedure

Step 1 Select **Setting** > **Storage** > **Destination** > **Path**.

Figure 5-142 Path settings



Record				Snapshot			
Event Type	Scheduled	Motion Detection	Alarm	Event Type	Scheduled	Motion Detection	Alarm
Local	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Local	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
FTP	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	FTP	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
NAS	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	NAS	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Default Refresh Save

Step 2 Select the corresponding event type and storage method.

Table 5-45 Description of path parameter

Parameter	Description
Event Type	Select Scheduled , Motion Detection or Alarm .
Local	Save recordings or snapshots to the SD card.
FTP	Save recordings or snapshots to the FTP server.
NAS	Save recordings or snapshots to the NAS server.

Step 3 Click **Save**.

5.6.3.2 FTP

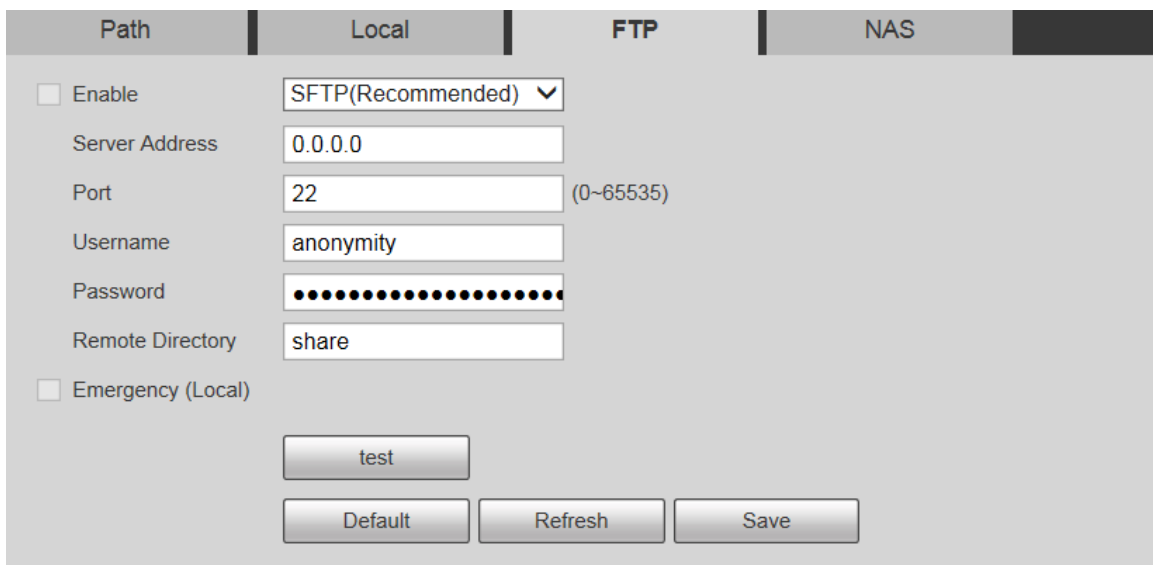
Background Information

FTP function can be enabled only when it is selected as a destination path. When the network is disconnected or does not work, you can save recordings and snapshots to the SD card by using **Emergency (Local)** function.

Procedure

Step 1 Select **Setting** > **Storage** > **Destination** > **FTP**.

Figure 5-143 FTP settings



Path Local **FTP** NAS

☐ Enable SFTP(Recommended) ▼

Server Address 0.0.0.0

Port 22 (0~65535)

Username anonymity

Password ●●●●●●●●●●●●●●●●

Remote Directory share

☐ Emergency (Local)

test

Default Refresh Save

Step 2 Select the **Enable** checkbox to enable FTP function.



- There might be risks if the FTP function is enabled. Think twice before enabling the function.

- **SFTP** is recommended to ensure network security.

Step 3 Configure FTP parameters.

Table 5-46 FTP parameter description

Parameter	Description
Server Address	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.
Remote Directory	The destination path on the FTP server.
Emergency (Local)	If you enable the function, in case of FTP storage exception, the recordings and snapshots will be stored on the local SD card.

Step 4 Click **test** to verify the username and password, and test whether FTP is connected to the Device.

Step 5 Click **Save**.

5.6.3.3 Local

Background Information

SD card information is displayed in the local storage list. You can set it as read only or read & write. You can also hot swap or refresh it.



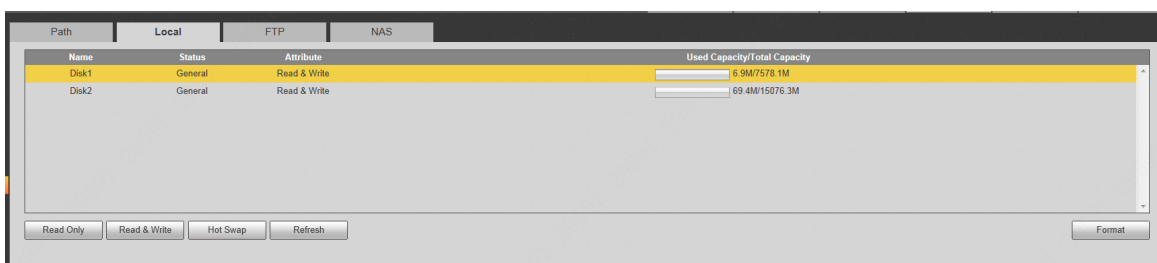
Dual SD cards are supported by some devices. For such devices, the SD card first inserted is called Local Disk 1, and the SD card inserted later is called Local Disk 2.

- If no recordings in both cards, the recording will be saved to Local Disk 1, and then saved to Local Disk 2 when Disk 1 is full.
- If there are recordings in both cards, the recording will be saved to the card with the latest recordings, and then saved to the other card when this card is full.

Procedure

Step 1 Select **Setting > Storage > Destination > Local**.

Figure 5-144 Local storage



Step 2 Select the SD card to be set, and then perform the following operations as needed.

- Click **Read Only** to set the SD card to be read only.
- Click **Read & Write** to set the SD card to be read and write.
- Click **Hot Swap** to remove or insert the SD card when the Camera is running.
- Click **Format** to format the SD card.



After formatting the SD card, all data on it will be cleared. Be cautious.

5.6.3.4 NAS

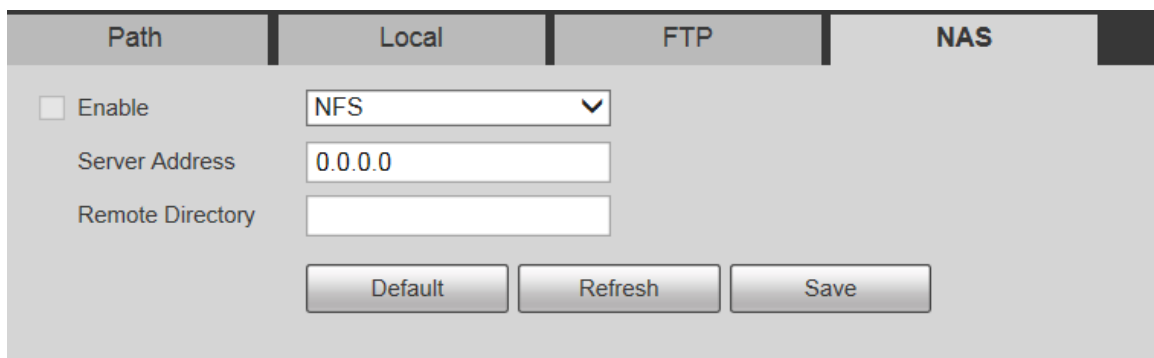
Background Information

This function can be enabled only when NAS is selected as a destination path. Select NAS to store files on the NAS server.

Procedure


Step 1 Select **Setting** > **Storage** > **Destination** > **NAS**.

Figure 5-145 NAS settings



Step 2 Configure NAS setting parameters.

Table 5-47 NAS parameter description

Parameter	Description
Enable	Select the checkbox to enable NAS function. Select NFS or SMB function.  There might be risks if NFS or SMB is enabled. Think twice before enabling the function.
Server Address	The IP address of the NAS server.
Remote Directory	The destination path on the NAS server.

Step 3 Click **Save**.

5.6.4 Record Control

Procedure

Step 1 Select **Setting** > **Storage** > **Record Control**.

Figure 5-146 Record control

Record Control

Pack Duration

30

Min. (1~120)

Pre-event Record

5

s (0~5)

Disk Full

Overwrite

▼

Record Mode

☒ Auto
☐ Manual
☐ Off

Record Stream

Main Stream

▼



Default

Refresh

Save

Step 2 Configure record control parameters.

Table 5-48 Record control parameter description

Parameter	Description
Pack Duration	Set the pack duration of each recording file. It is 30 minutes by default.
Pre-event Record	<p>Set the pre-recording time. For example, if you enter 5, when an alarm is triggered, the system reads the recording of the first 5 seconds in memory, and then records it into a file.</p> <p> If alarm recording or motion detection recording occurs, if there is no recording before, the video data within N seconds before the recording is started will also be recorded into the video file.</p>
Disk Full	<p>You can select Stop or Overwrite.</p> <ul style="list-style-type: none"> Stop: The system stops recording when the disk is full. Overwrite: The system overwrites the oldest files and keeps recording when the disk is full. <p> The data will be overwritten if the disk is full. Back up the file in time as needed.</p>
Record Mode	You can select Auto , Manual or Off . Select Manual mode to start recording immediately, and select Auto mode to record within the schedule.
Record Stream	Select Main Stream or Sub Stream .

Step 3 Click **Save**.

5.7 System Management

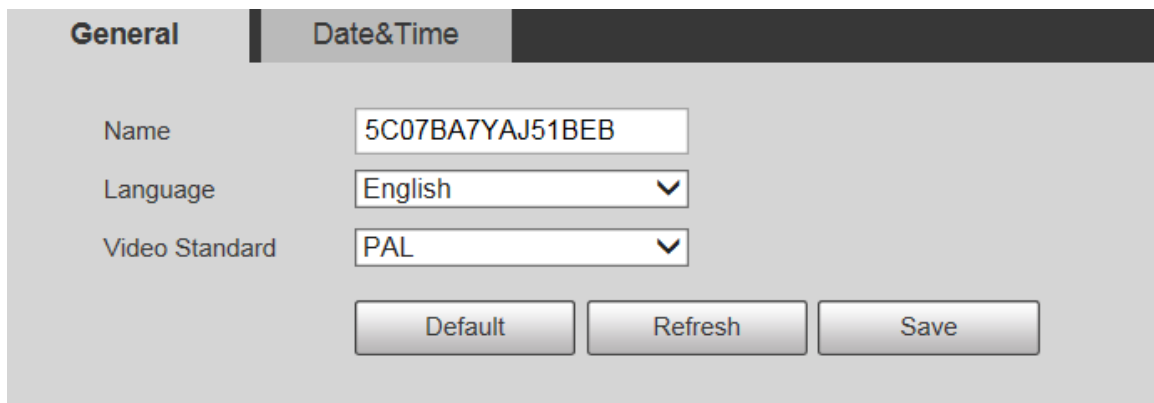
5.7.1 Device Settings

5.7.1.1 General

Procedure


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

Figure 5-147 General settings



Step 2 Configure general setting parameters.

Table 5-49 Description of general setting parameter

Parameter	Description
Name	Set the device name.  Different devices have different names.
Language	Select the language to be displayed.
Video Standard	Select video standard from PAL and NTSC .

Step 3 Click **Save**.

5.7.1.2 Date & Time


Procedure

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

Step 2 Configure date & time parameters.

Table 5-50 Description of date & time parameter

Parameter	Description
Date Format	Select the date format. Three formats are available: YYYY-MM-DD , MM-DD-YYYY and DD-MM-YYYY .

Parameter	Description
Time Format	Select the time format. Two formats are available: 24-Hour and 12-Hour .
Time Zone	Set the local time zone.
Current Time	The current time of the Device.
DST	Set the Start Time and End Time of DST in the Date format or Week format.
NTP	Select the NTP checkbox to enable the network time sync function.
Server	Set the address of the time server.  Set the network timing function of NTP server, and the Device time will be synchronized with the server time.
Port	Set the port number of the time server.
Interval	Set the synchronization interval of the Device and the time server.

Step 3 Click **Save**.

5.7.1.3 Screen Off Settings

Background Information



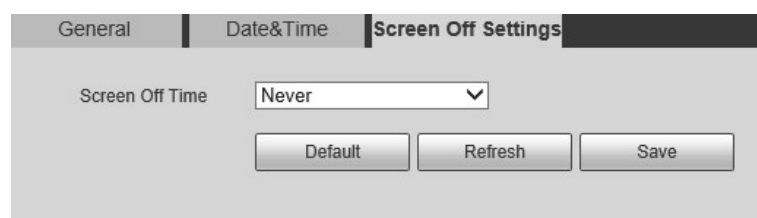
The function is available on select models.

You can set the screen-off time of the device display.

Procedure

Step 1 Select **Setting** > **System** > **General** > **Screen Off Settings**.

Figure 5-148 Screen off settings



Step 2 Set screen-off time.

- **Never** : The screen is never turned off.
- **Custom** : Customize the screen-off time.

Step 3 Click **Save**.

5.7.1.4 Sleep Mode

You can configure the sleep mode and time period of the Device.

Background Information

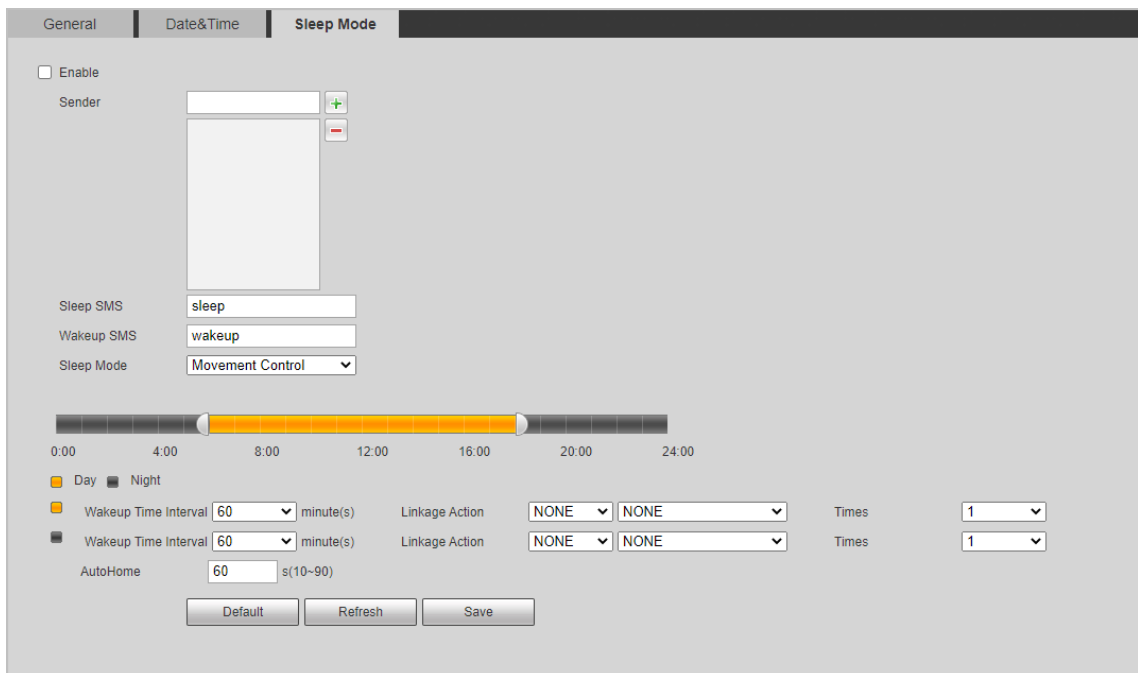


This function is available on select devices.

Procedure

- Step 1** Select **Setting > System > General > Sleep Mode**.
- Step 2** Select **Enable** to enable sleep mode function.
- Step 3** Select sleep mode type, and then configure parameters.
It supports **Movement Control**, **Interval** and **SMS** mode.
- Movement Control
 1. Select **Movement Control** as sleep mode.

Figure 5-149 Movement Control



The screenshot shows the 'Sleep Mode' configuration page. The 'Enable' checkbox is checked. The 'Sender' field is empty. The 'Sleep SMS' field contains 'sleep' and the 'Wakeup SMS' field contains 'wakeup'. The 'Sleep Mode' dropdown is set to 'Movement Control'. A timeline slider shows the day and night periods. The 'Day' period is from 6:00 to 18:00, and the 'Night' period is from 18:00 to 6:00. The 'Wakeup Time Interval' is set to 60 minutes for both day and night. The 'Linkage Action' is set to 'NONE' for both. The 'Times' dropdown is set to 1. The 'AutoHome' field is set to 60 seconds. Buttons for 'Default', 'Refresh', and 'Save' are at the bottom.

2. Drag the slider to set the day and night time periods.

You can set different sleep mode configurations for day and night. For example, you can set the day configuration as 6:00 to 18:00, and set the night configuration as 18:00 to 6:00 the next day.

3. Configure **Wakeup Time Interval** and **Linkage Action** according to actual needs.

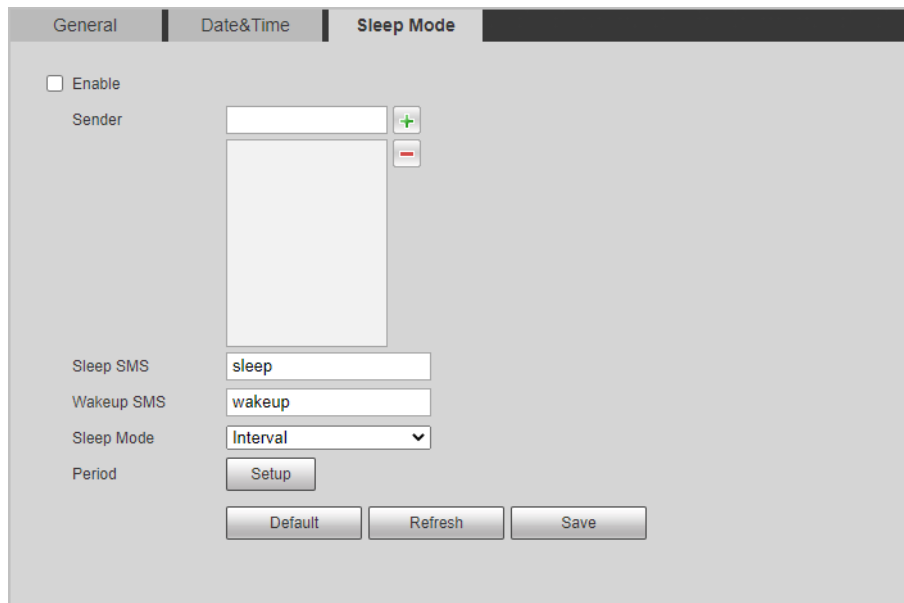
Table 5-51 Description of Movement Control Parameters

Parameter	Description
Wakeup Time Interval	The duration after the device enters sleep mode is not related to the motion time after waking up. The Wakeup Time Interval ranges from 30 to 120 minutes, with a default of 60 minutes.
Linkage Action	The actions performed after the device wakes up. You can select from None or Tour .
Times	The number of actions performed after the device wakes up. The value ranges from 1 to 5 and the default value is 1.

Parameter	Description
AutoHome	During the tour, the PTZ is manually controlled to rotate. After the autohome time, the PTZ will automatically restores to the original tour group. The value of AutoHome ranges from 10 to 90 seconds, and the default value is 60 seconds.

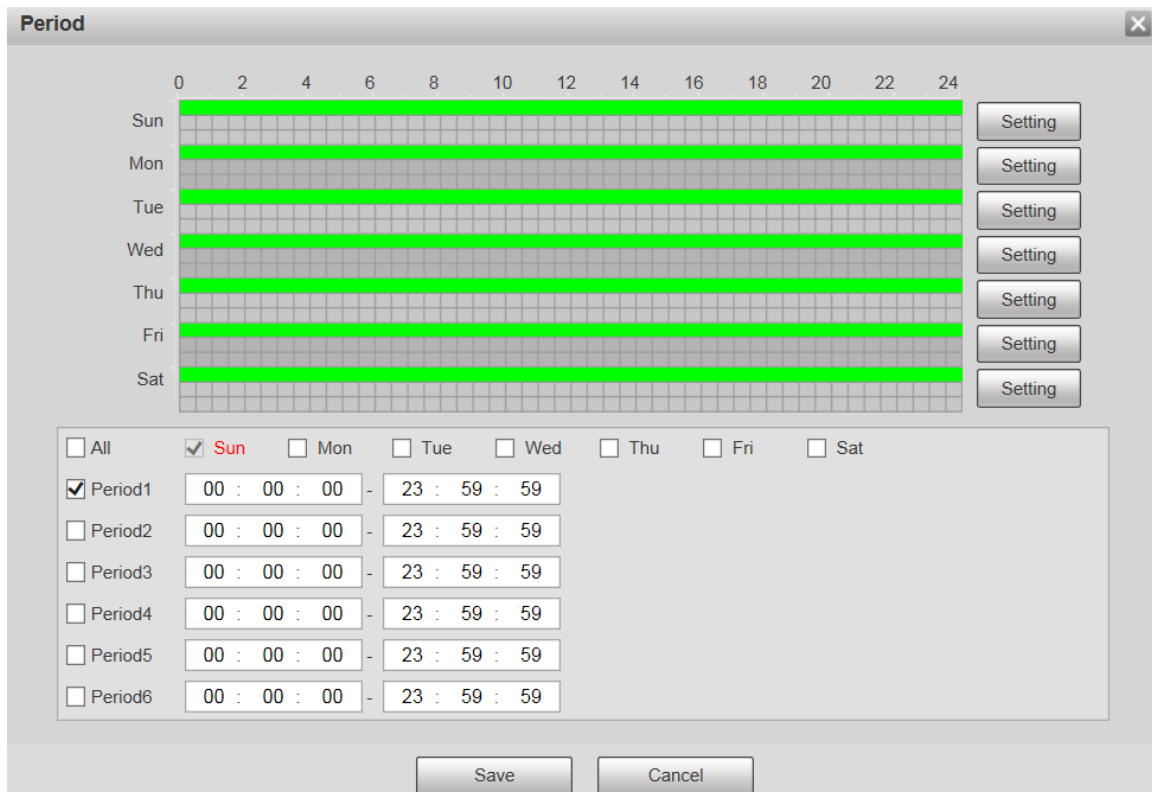
- Interval: Select interval as sleep mode, and then click **Setup** to configure the time period for the sleep function to take effect.

Figure 5-150 Interval



1. Click **Setting**, and then set the arming period on the page.

Figure 5-151 Arming period settings




2. Set the alarm period to enable alarm events in the period you set.

- There are 6 time periods for each day. Select the checkbox for the time period to enable it.
- Select the day of week (**Sunday** is selected by default; If **All** is selected, the setting is applied to the whole week. You can also select the checkbox next to the day to set it separately).


3. After completing the settings, click **Save**.

You will return to the **Motion Detection** page.

- SMS: Click  to add the mobile phone number to the allow list, and then set the contents of sleep SMS and wakeup SMS.

Send a message to the SIM card on the device using the telephone number in the allow list, and then set the message content as **Sleep SMS** or **Wakeup SMS**. The device enters **Sleep State** or **Waking Up State**.



Select an added telephone number, and then click  to delete this number.

Step 4 Click **Save**.

5.7.2 Account Settings

5.7.2.1 Account

User management is only available for admin users.

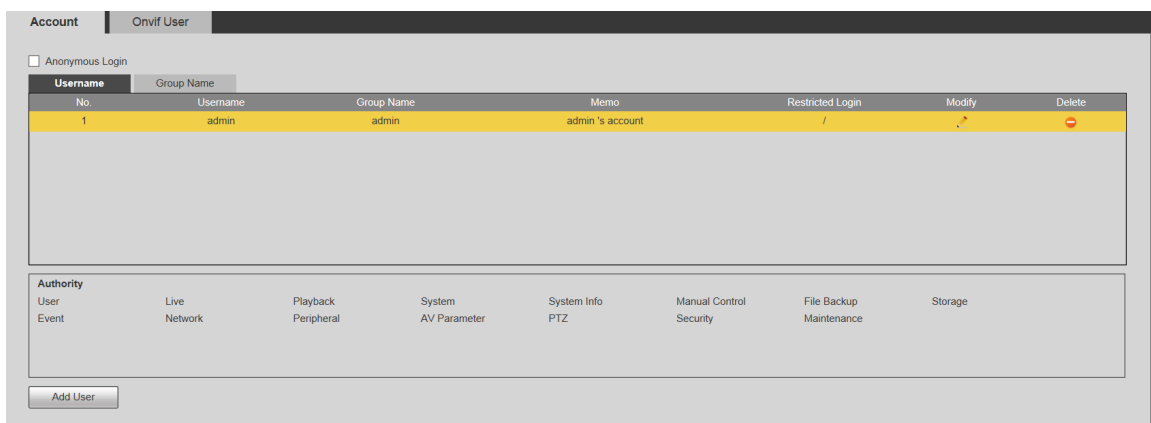
- For **Username** and **Group Name**, the maximum length is 15 characters. Username can only consist of numbers, letters, underlines, dots and @; group name can only consist of numbers, letters and underlines.
- The password should consist of 8 to 32 non-blank characters and contain at least two types of characters among upper case, lower case, number, and special characters (excluding ' ' ; &). The confirming password shall be the same as the new password. Set a high security password according to the prompt of password strength.
- The number of users and groups is 19 and 8 respectively by default.
- User management adopts a two-level method of group and user. Neither group names nor user names can be duplicated, and a user can only belong to one group.
- Users currently logged in cannot modify their own permissions.
- The user is admin by default. The **admin** account is defined as high privileged user.

5.7.2.1.1 Username

Background Information


Select **Setting** > **System** > **Account** > **Account** > **Username** to enable anonymous login, add users, delete users, modify user passwords or perform other operations.

Figure 5-152 Account page



No permission is available for version information and other buttons except **Relay-out**, **Mark**, and **Wiper Control** on the **Live** page for the time being.

5.7.2.1.2 Deleting Users

Click  corresponding to the user to be deleted, and the user can be deleted.



Users/user groups cannot be recovered after deletion. Think twice before performing the operation.

5.7.2.1.3 Modifying Password

Procedure

- Step 1 Select the **Modify Password** checkbox.
- Step 2 Enter old password and new password, and then confirm password.
- Step 3 Click **Save**.

5.7.2.1.4 Modifying Users

Procedure


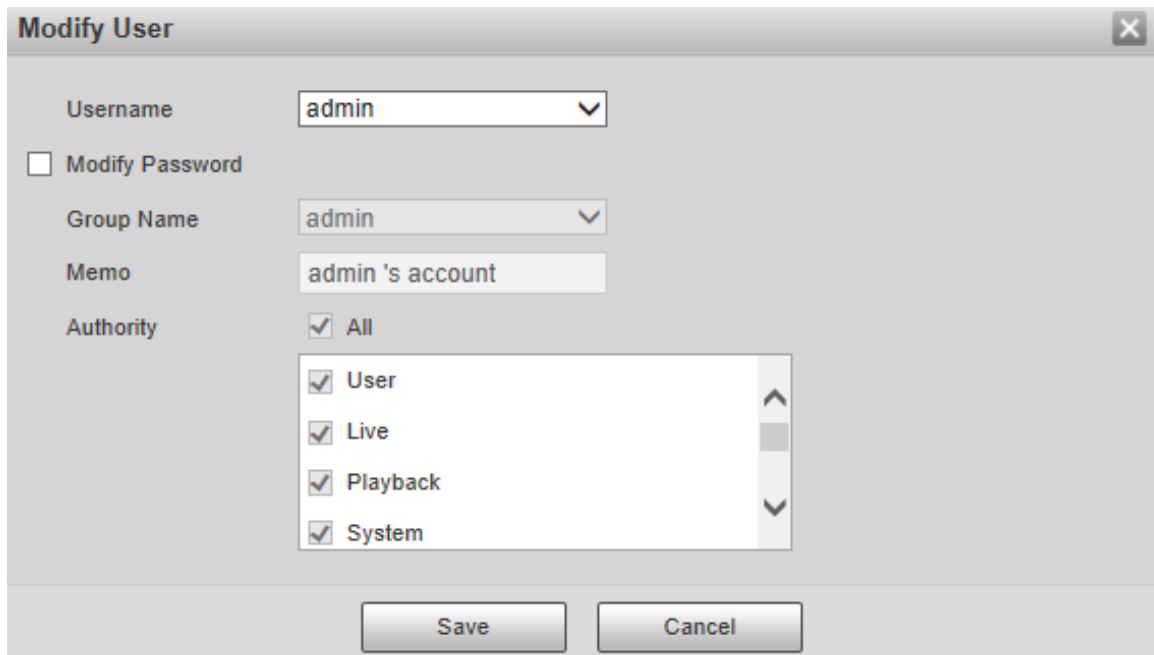
Step 1 Click  corresponding to the user you want to modify.

Figure 5-153 Modify users



The 'Modify User' dialog box contains the following fields and options:

- Username:** A dropdown menu currently showing 'admin'.
- Modify Password:** An unchecked checkbox.
- Group Name:** A dropdown menu currently showing 'admin'.
- Memo:** A text input field containing 'admin 's account'.
- Authority:** A section with a checked 'All' checkbox and a list box containing four items, each with a checked checkbox: 'User', 'Live', 'Playback', and 'System'.
- Buttons:** 'Save' and 'Cancel' buttons at the bottom right.

Step 2 Modify user information.

Step 3 Click **Save**.

5.7.2.1.5 Adding Users

Background Information

Add users in the group and set permissions.

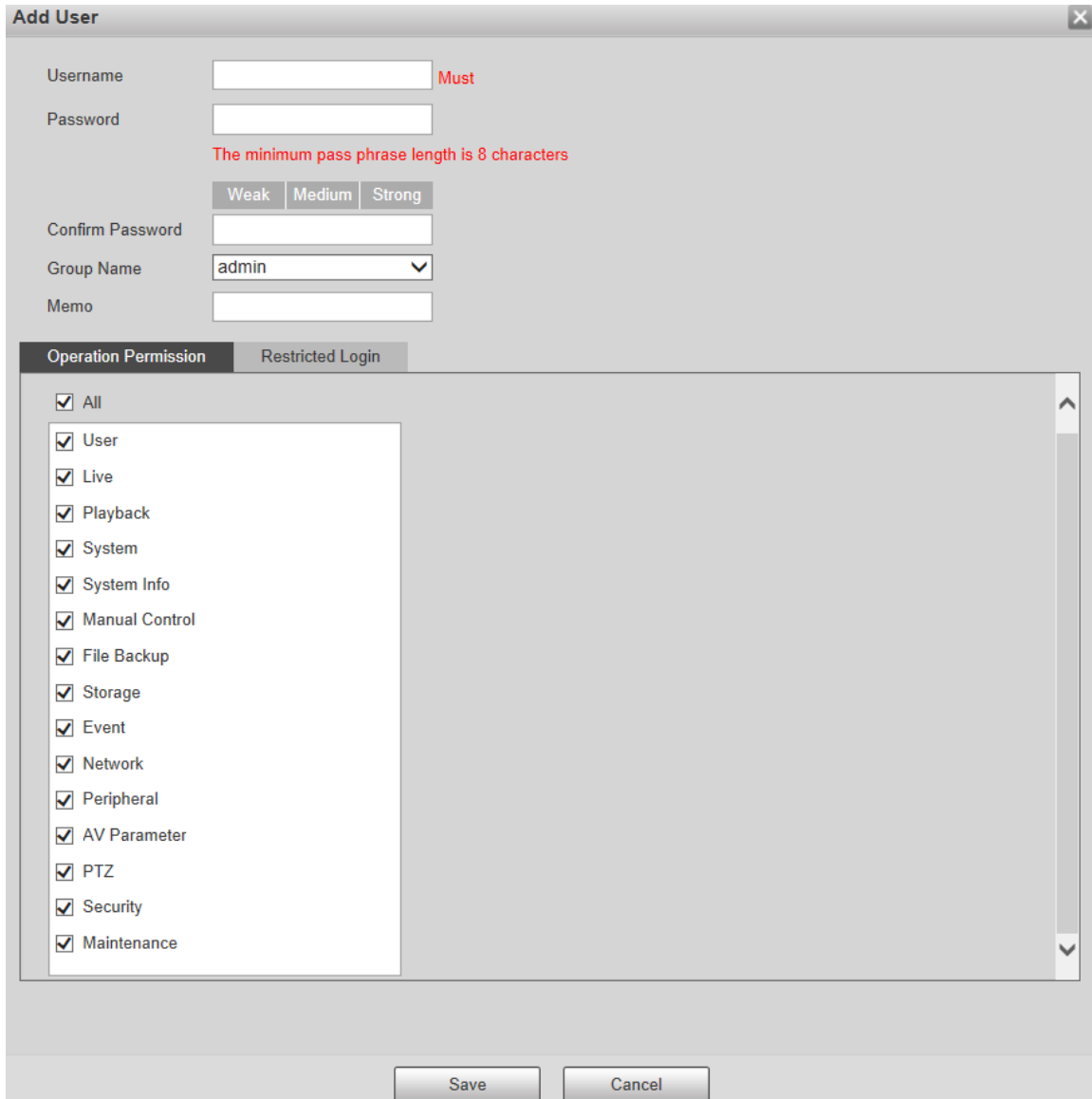


As the default user with the highest authority, admin cannot be deleted.

Procedure

Step 1 Click **Add User**.

Figure 5-154 Add users



Step 2 Enter **Username** and **Password**, confirm password, select **Group Name**, and then add **Memo**.

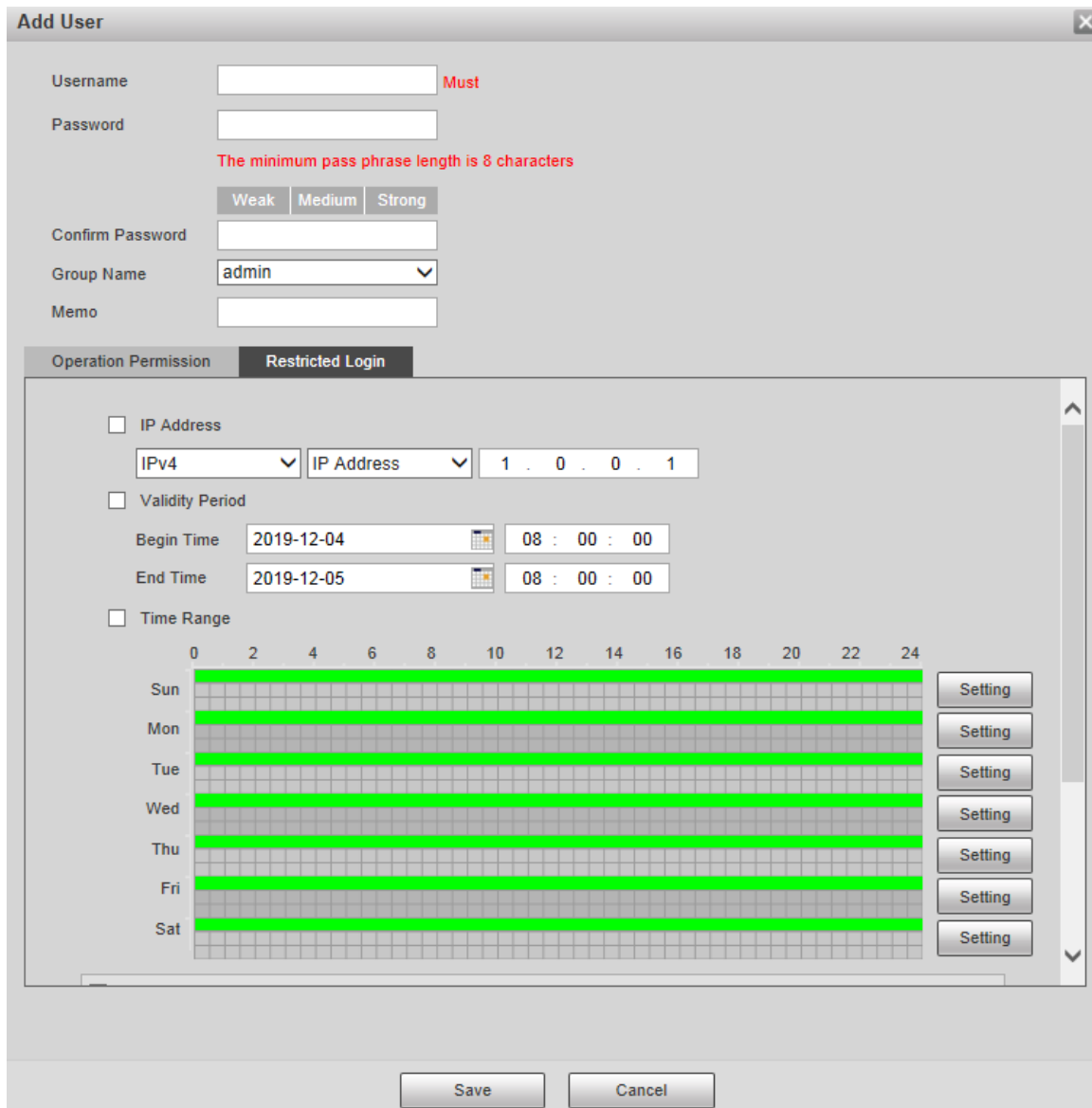
Step 3 Set **Operation Permission** and **Restricted Login**.

- Operation Permission: Click **Operation Permission**, and then select the operation permission of the user as needed.
- Restricted Login: **Click Restricted Login**, and the page shown in "Restricted login" is displayed. You can control login to the Device by setting the **IP Address**, **Validity Period** and **Time Range**.



- Once the group is selected as needed, the user permission can only be a subset of the group, and cannot exceed its permission attributes.
- It is recommended to give less permissions to general users than advanced users.

Figure 5-155 Restricted login



Step 4 Click **Save**.

5.7.2.1.6 Anonymous Login

Select the **Anonymous Login** checkbox, and you can log in to the Device anonymously without username and password after entering IP. Anonymous users only have preview permission in the permission list. In the anonymous login, click **Logout** to log in to the Device by using other usernames.

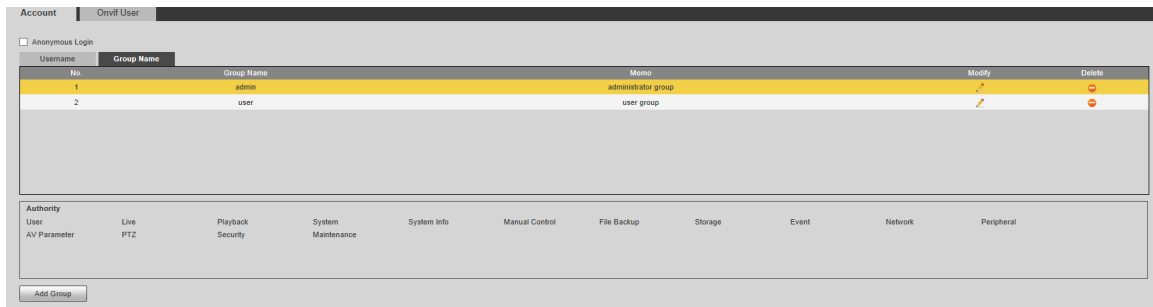


After **Anonymous Login** is enabled, the user can view audio and video data without authentication. Think twice before enabling the function.

5.7.2.1.7 Group Name

Select **Setting** > **System** > **Account** > **Account** > **Group Name** to add groups, delete groups, modify group passwords or perform other operations.

Figure 5-156 User group settings



Configuring User Group

The default authorities of Admin group include 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 5-52 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.
Peripheral	YES	NA	External light, wiper and serial port settings.

Group Authority	Admin	User	Functions
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** authority to modify group authority. The **User** group does not have this authority.
- The functions 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.

Adding Groups

For specific operations, refer to "5.7.2.1.1 Username".

Modifying Groups

For specific operations, refer to "5.7.2.1.1 Username".

Deleting Groups

For specific operations, refer to "5.7.2.1.1 Username".

5.7.2.2 ONVIF User

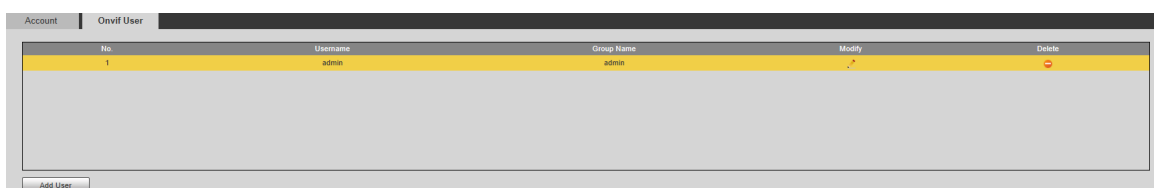
Background Information

On the webpage, you can add ONVIF users, or modify existing users.

Procedure

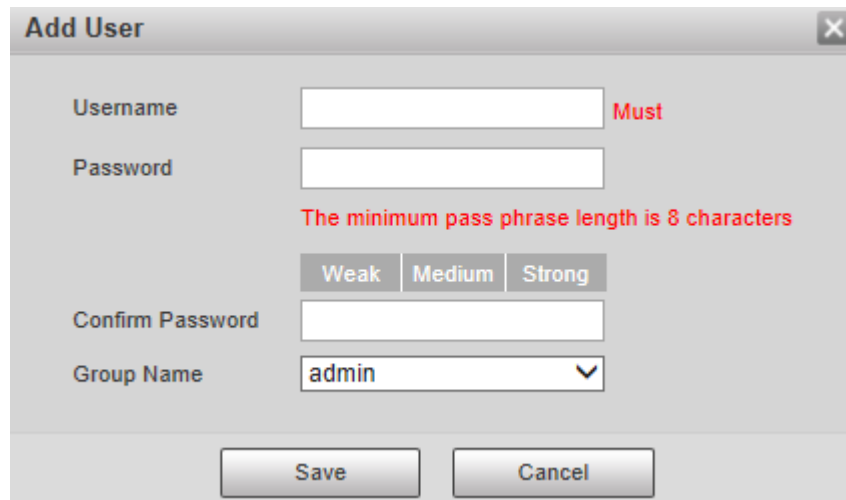
Step 1 Select **Setting** > **System** > **Account** > **Onvif User**.

Figure 5-157 Onvif user



Step 2 Click **Add User**.

Figure 5-158 Add users





The 'Add User' dialog box contains the following fields and controls:

- Username:** A text input field with a red 'Must' label to its right.
- Password:** A text input field.
- Strength Indicator:** Three buttons labeled 'Weak', 'Medium', and 'Strong' are positioned below the password field.
- Confirm Password:** A text input field.
- Group Name:** A dropdown menu currently showing 'admin'.
- Buttons:** 'Save' and 'Cancel' buttons at the bottom.
- Message:** A red text message states 'The minimum pass phrase length is 8 characters'.

Step 3 Set the username and password, confirm password, and then select the group name.

Step 4 Click **Save**.

Related Operations

- Click  to modify user information.
- Click  to delete users.

5.7.3 Safety

5.7.3.1 RTSP Authentication

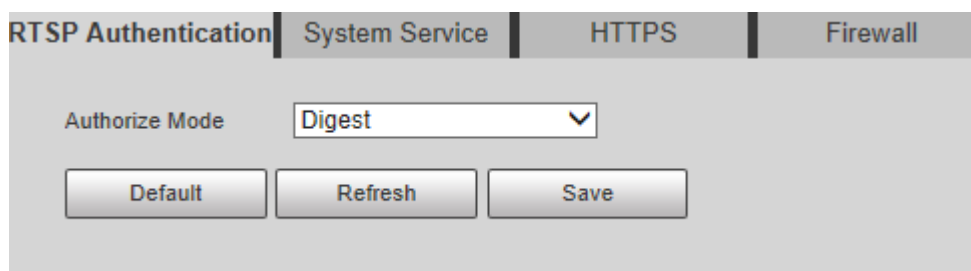
Background Information

Set the authentication method for media stream.

Procedure

Step 1 Select **Setting > System > Safety > RTSP Authentication**.

Figure 5-159 RTSP authentication



The 'RTSP Authentication' configuration page shows the following settings:

- Authorize Mode:** A dropdown menu set to 'Digest'.
- Buttons:** 'Default', 'Refresh', and 'Save' buttons are located at the bottom.

Step 2 Select the **Authorize Mode**.

You can select from **Digest**, **Basic** and **None**. It is **Digest** by default.



- Click **Default**, and **Digest** is selected automatically.
- Select **None**, and "Non-authentication mode may have risk. Are you sure to enable it" prompt will be displayed. Think twice before selecting the mode.
- Select **Basic** mode, and "Basic authentication mode may have risk. Are you sure to enable it?" prompt will be displayed. Think twice before selecting the mode.

5.7.3.2 System Service

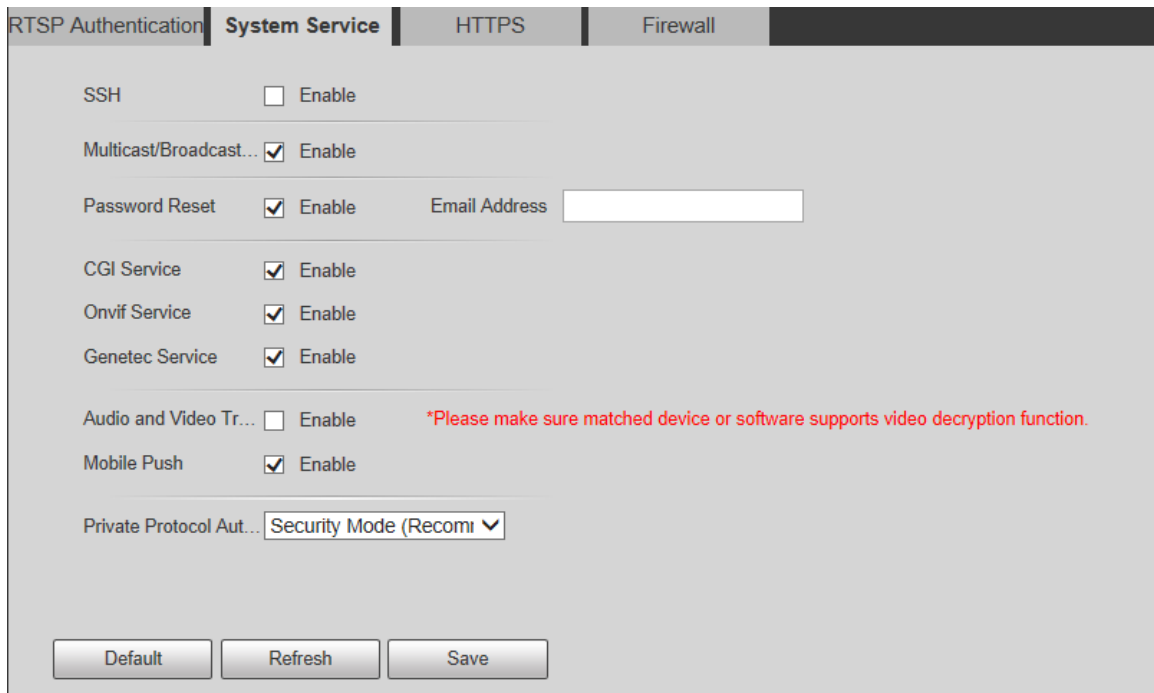
Background Information

You can configure system service to ensure system security.

Procedure



Step 1 Select **Setting** > **System** > **Safety** > **System Service**.






Figure 5-160 System service



Step 2 Configure system service parameters.

Table 5-53 Description of system service parameter

Function	Description
SSH	<p>You can enable SSH authentication to perform safety management. The function is disabled by default.</p> <p> It is recommended to disable SSH. If this function is enabled, there might be security risks.</p>
Multicast/Broadcast Search	<p>Enable this function, and when multiple users are viewing the monitoring screen simultaneously through network, they can find the Device through multicast/broadcast protocol.</p> <p> It is recommended to disable the multicast/broadcast search function. If this function is enabled, there might be security risks.</p>

Function	Description
Password Reset	<p>You can enable Password Reset to perform security management. The function is enabled by default.</p> <p> If the function is disabled, you can only reset the password after restoring the Device to factory defaults through pressing the Reset button on the device.</p>
CGI Service	<p>You can access the Device through this protocol. The function is enabled by default.</p> <p> It is recommended to disable the function. If this function is enabled, there might be security risks.</p>
Onvif Service	<p>You can access the Device through this protocol. The function is enabled by default.</p> <p> It is recommended to disable the function. If this function is enabled, there might be security risks.</p>
Audio and Video Transmission Encryption	<p>Enable this function to encrypt the stream transmitted through the private protocol.</p> <p> <ul style="list-style-type: none"> Make sure that the matched devices or software support video decryption function. It is recommended to enable the function. If the function is disabled, there might be risk of data leakage. </p>
Mobile Push	<p>Push the alarm snapshot triggered by the Device to the mobile phone. The function is enabled by default.</p> <p> It is recommended to disable the function. If this function is enabled, there might be security risks.</p>
Private Protocol Authentication Mode	<p>You can select Security Mode and Compatible Mode. Security mode is recommended. If you select compatibility mode, there might be security risks.</p>

Step 3 Click **Save**.

5.7.3.3 HTTPS

It is recommended to enable HTTPS service. If the service is disabled, there might be risk of data leakage.

Background Information

Create certificate or upload signed certificate, and then you can log in through HTTPS with your PC. HTTPS can ensure data security, and protect user information and device security with reliable and stable technology.

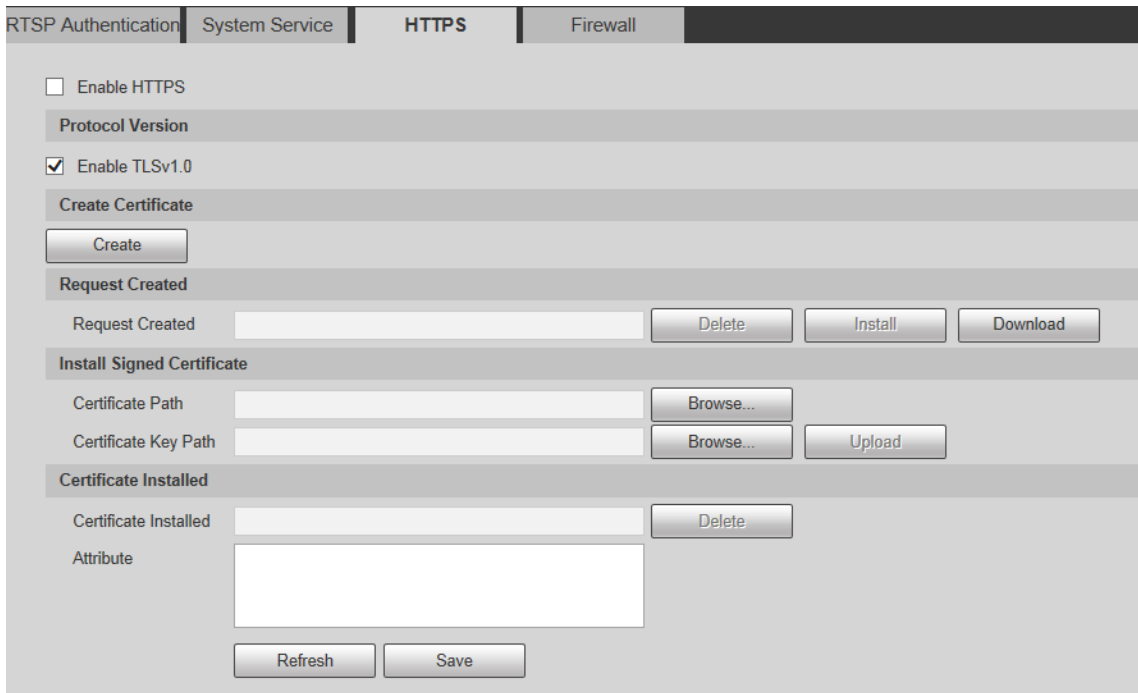
Procedure

Step 1 Create certificate or upload the signed certificate.

- If you select **Create Certificate**, refer to the following steps.

1. Select **Setting > System > Safety > HTTPS**.

Figure 5-161 HTTPS (1)



RTSP Authentication | System Service | **HTTPS** | Firewall

☐ Enable HTTPS

Protocol Version

☒ Enable TLSv1.0

Create Certificate

Create

Request Created

Request Created	Delete	Install	Download

Install Signed Certificate

Certificate Path Browse...

Certificate Key Path Browse... Upload

Certificate Installed

Certificate Installed	Delete
Attribute	

Refresh Save

2. Click **Create**.

Figure 5-162 HTTPS (2)

The screenshot shows a window titled "HTTPS" with a close button (X) in the top right corner. The window contains the following fields and labels:

- Region: *e.g. CN
- IP or Domain name: *
- Validity Period: 365 Day*Range :1-5000
- Province: none
- Location: none
- Organization: none
- Organization Unit: none
- Email:

At the bottom of the window, there are two buttons: "Create" and "Cancel".

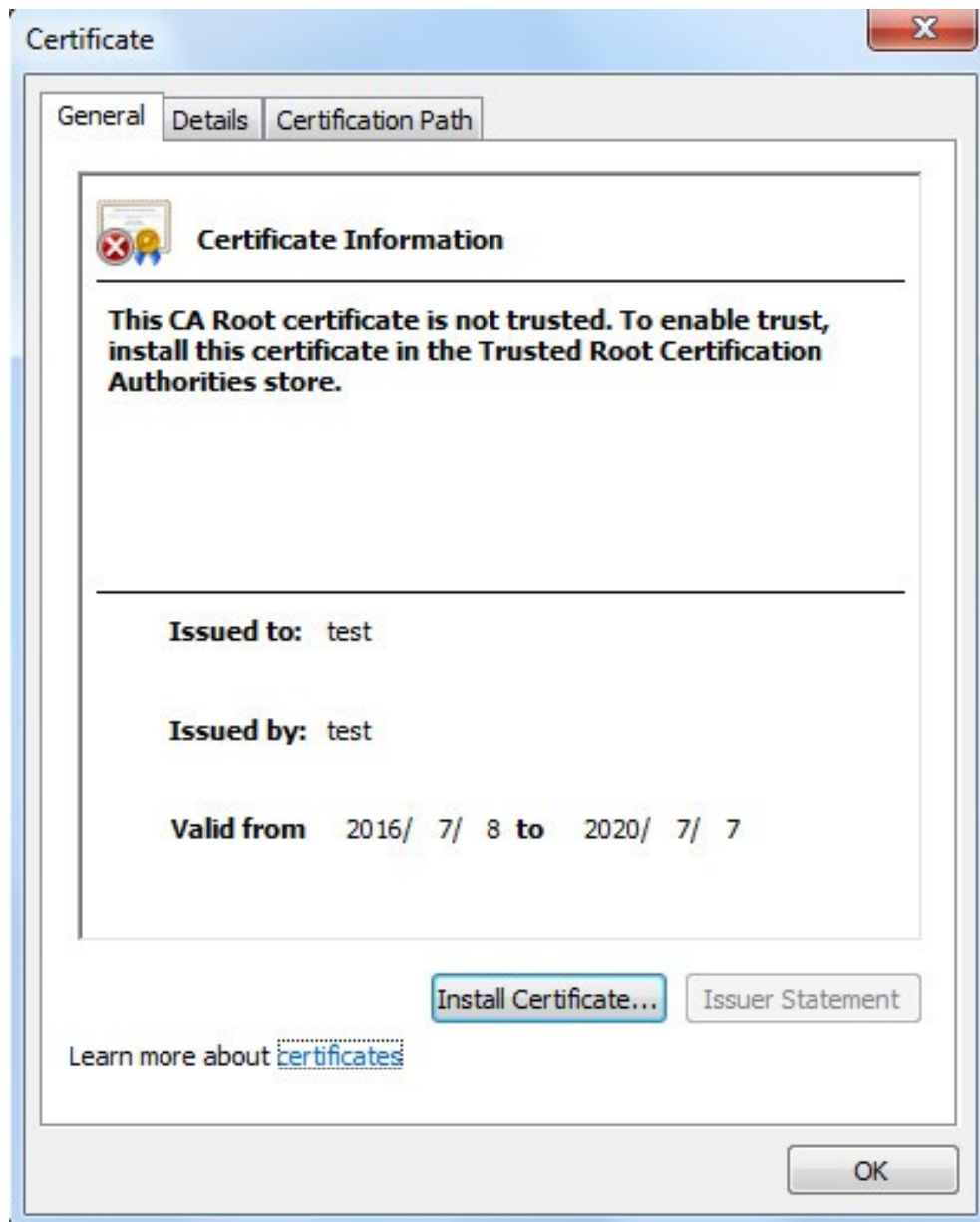
3. Enter the required information, and then click **Create**.



The entered IP or domain name must be the same as the IP or domain name of the Device.

4. Click **Install** to install the certificate on the Device.

Figure 5-165 Certificate information



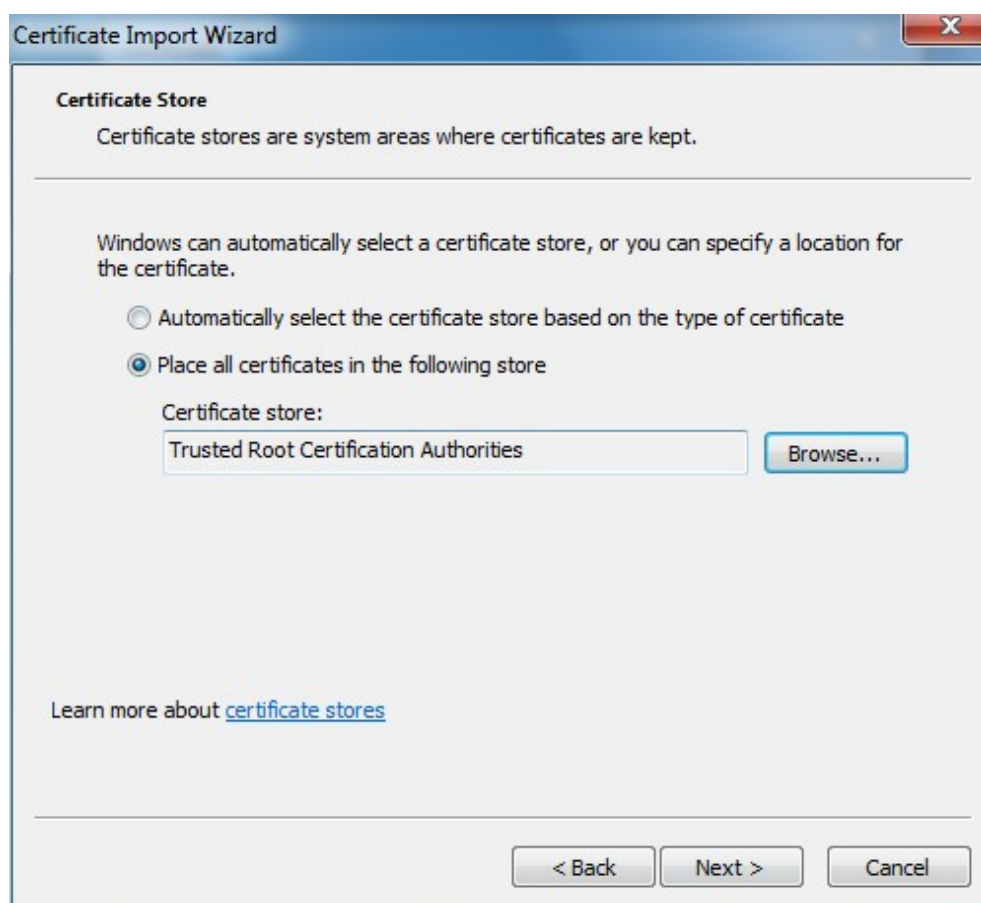
8. Click **Install Certificate**.

Figure 5-166 Certificate import wizard



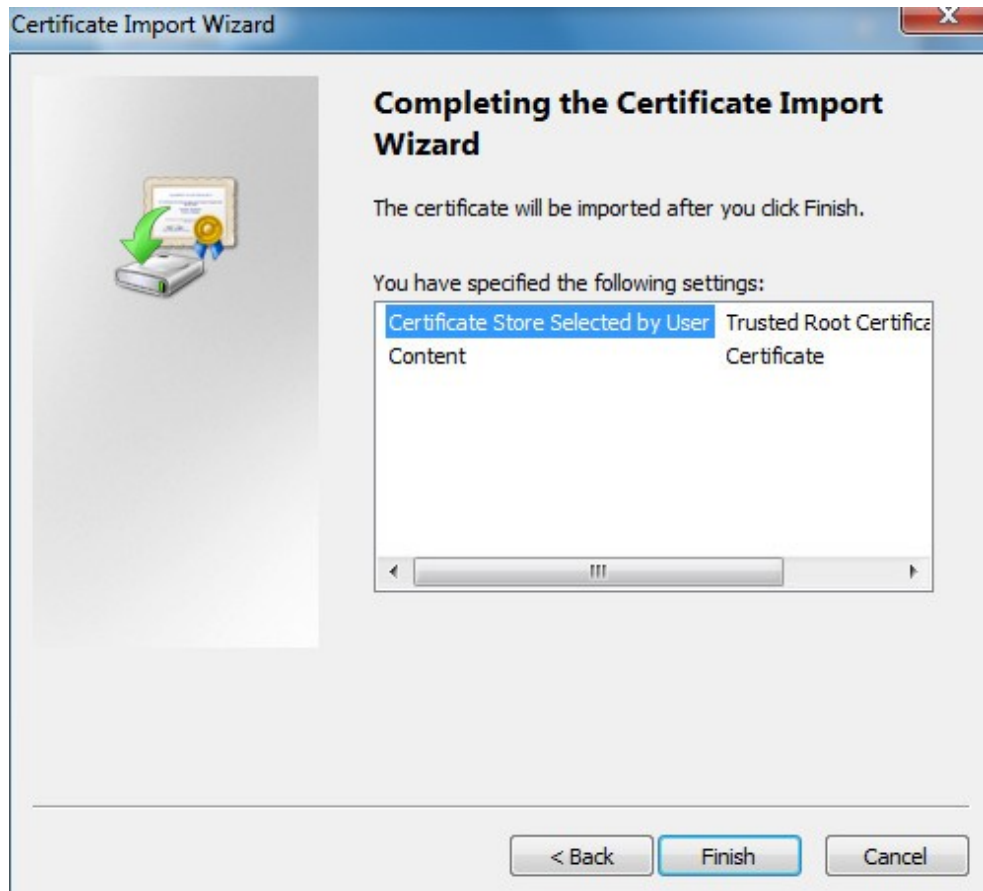
9. Click **Next**, and then select **Trusted Root Certification Authorities**.

Figure 5-167 Certificate storage area



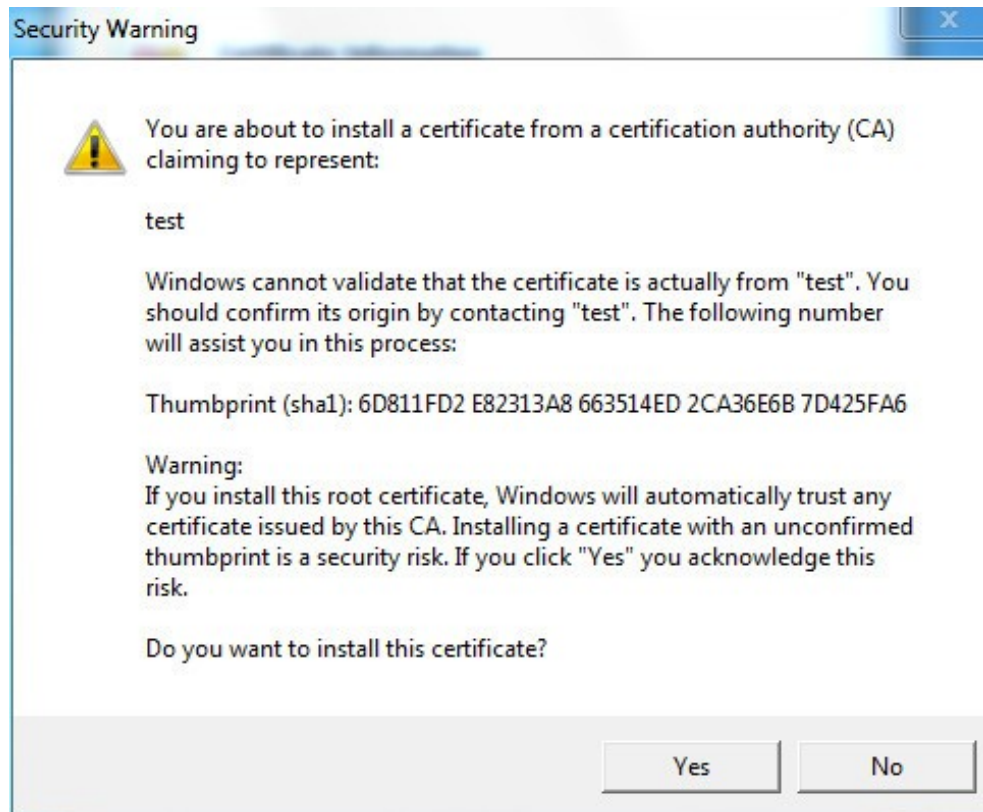
10. Click **Next**.

Figure 5-168 Completing the certificate import wizard



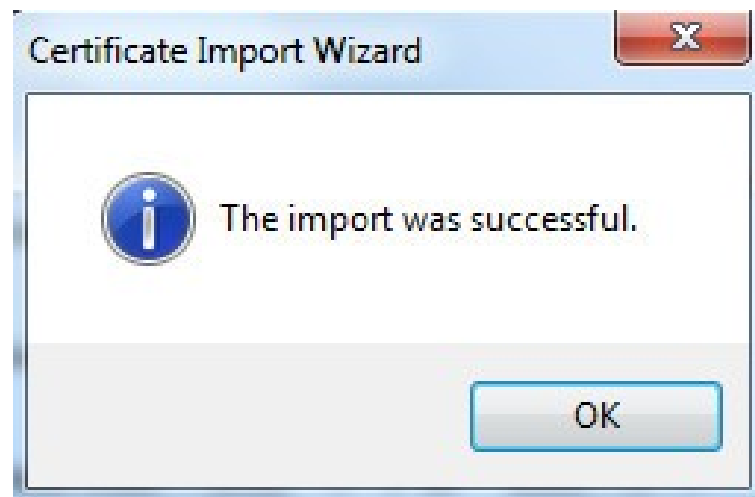
11. Click **Finish**.

Figure 5-169 Security warning



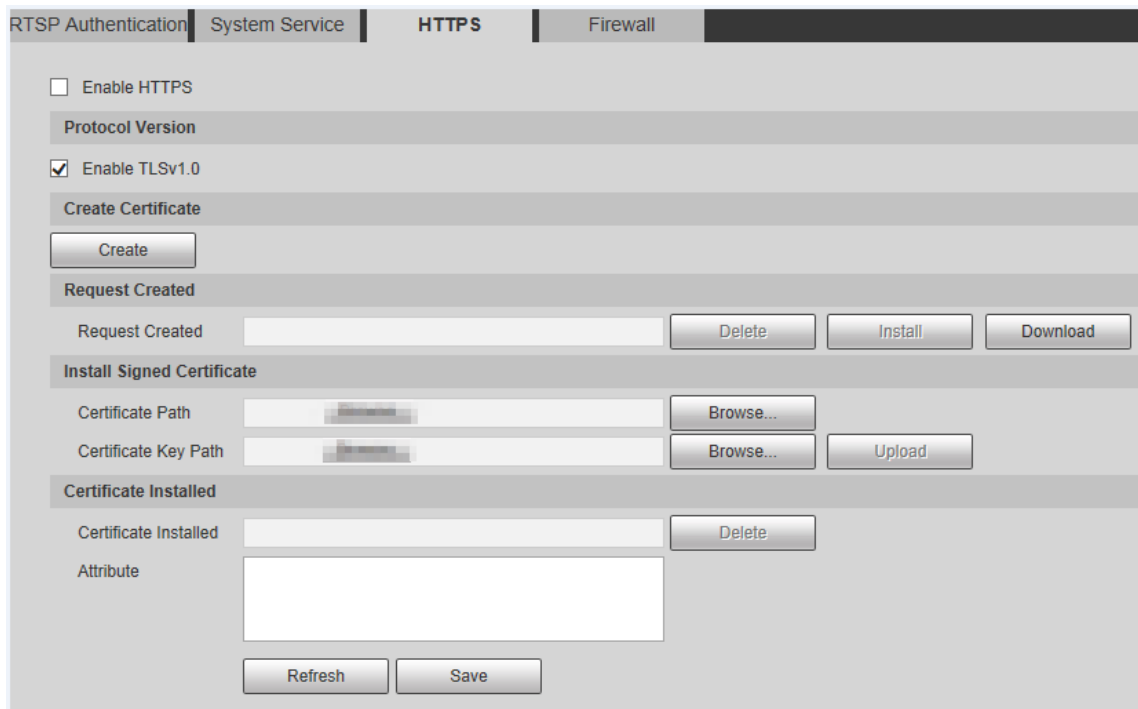
12. Click **Yes**, and then click **OK** to complete the certificate installation.

Figure 5-170 Import success



- If you select **Install Signed Certificate**, refer to the following steps.
 1. Select **Setting > System > Safety > HTTPS**.

Figure 5-171 Install signed certificate

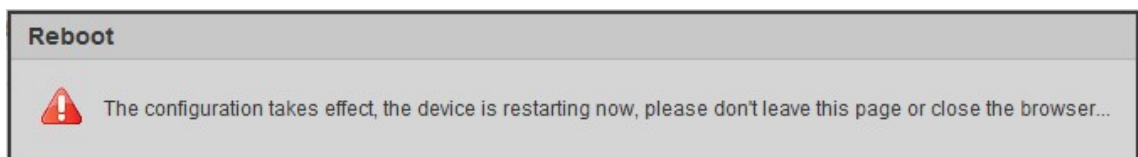


2. Click **Browse** to upload the signed certificate and certificate key, and then click **Upload**.
3. Install the root certificate. For details, see 5 to 12 in [Step 1](#).

[Step 2](#) Select **Enable HTTPS**, and then click **Save**.

The configuration takes effect after reboot.

Figure 5-172 Reboot



Enter `https://xx.xx.xx.xx` in the browser to open the login page. If no certificate is installed, a certificate error prompt will be displayed.



- If HTTPS is enabled, you cannot access the Device through HTTP. The system will switch to HTTPS if you access the Device through HTTP.
- The deletion of created and installed certificates cannot be restored. Think twice before deleting them.

5.7.3.4 Firewall

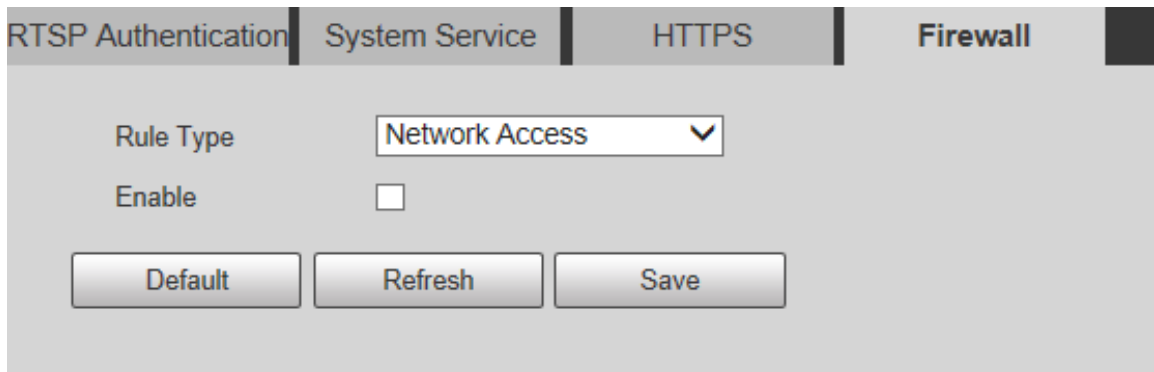
Background Information

Set a firewall for the Device to prevent network attacks after the Device is connected to the network.

Procedure

[Step 1](#) Select **Setting** > **System** > **Safety** > **Firewall**.

Figure 5-173 Firewall



Step 2 Select the type of network attack that the firewall resists. You can select **Network Access**, **PING Prohibited**, or **Prevent Semijoin**.

Step 3 Select **Enable** to enable **Firewall** function.

Step 4 Click **Save**.

5.7.4 Peripheral

Background Information

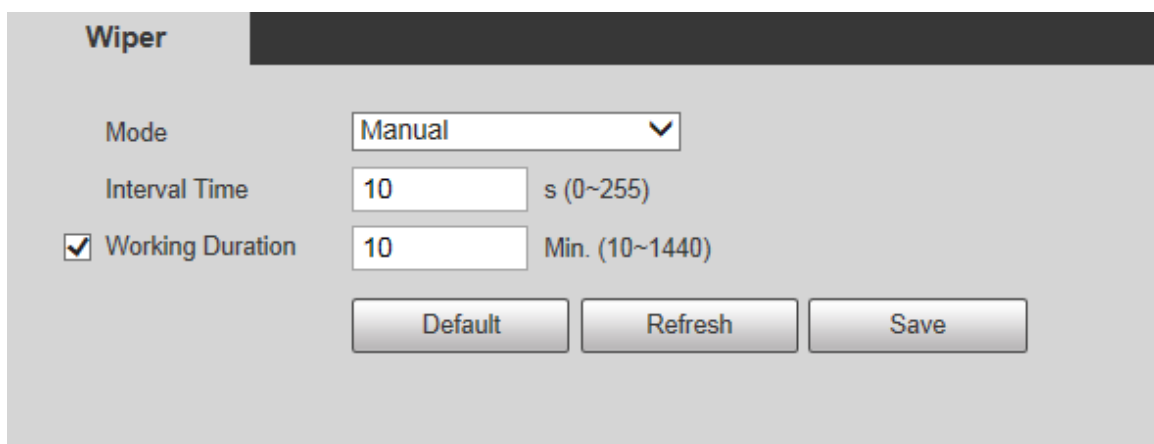


The peripheral functions might vary with different models.

Procedure

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

Figure 5-174 Wiper settings



Step 2 Configure wiper parameters.

Table 5-54 Description of wiper setting parameter

Parameter	Description
Mode	Set the wiper mode. It is Manual by default. In Manual mode, you need to manually start the wiper.
Interval Time	The time between wiper starting to wiper ending.

Parameter	Description
Working Duration	Set the maximum duration of the wiper operating once in Manual mode. The value ranges from 10 minutes to 1440 minutes.

Step 3 Click **Save**.

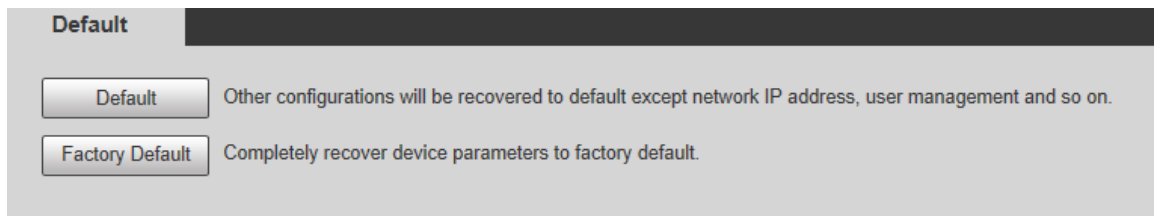
5.7.5 Default



All information except IP address and user management will be restored to defaults. Think twice before performing the operation.

Select **Setting** > **System** > **Default**, and click **Default** to restore the Device.

Figure 5-175 Default page



Select the recovery mode.

- Default: All information except IP address and user management will be restored to defaults.
- Factory Default: The function is equivalent to the Reset button of the Device. All configuration information of the Device can be restored to the factory defaults, and the IP address can also be restored to the original IP address. After clicking **Factory Default**, you need to enter the password of admin user on the page displayed. The Device can be restored to factory defaults only after the system confirms that the password is correct.



- Only admin user can use this function.
- When the Device is restored to factory defaults, all information except the data in the external storage media will be erased. Delete data in external storage media by formatting and other methods.

5.7.6 Import/Export

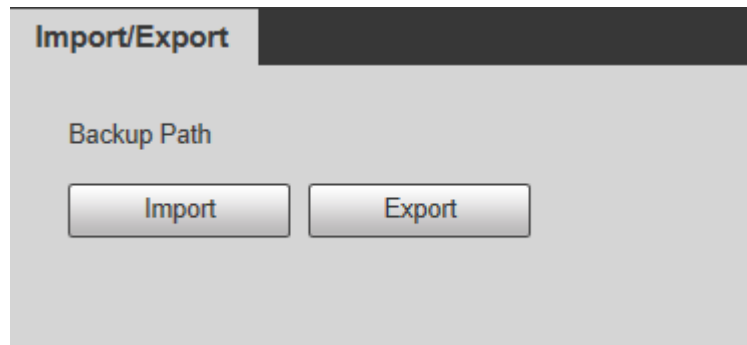
Background Information

When multiple devices share the same configuration methods, they can be quickly configured by importing and exporting configuration files.

Procedure

Step 1 On the webpage of one device, select **Setting** > **System** > **Import/Export**.

Figure 5-176 Import/Export



Step 2 Click **Export** to export the configuration file (.backup file) to the local storage path.

Step 3 Click **Import** on the **Import/Export** page of the Device to be configured to import the configuration file, and the Device will complete the configurations.

5.7.7 System Maintenance

5.7.7.1 Auto Maintain

Background Information

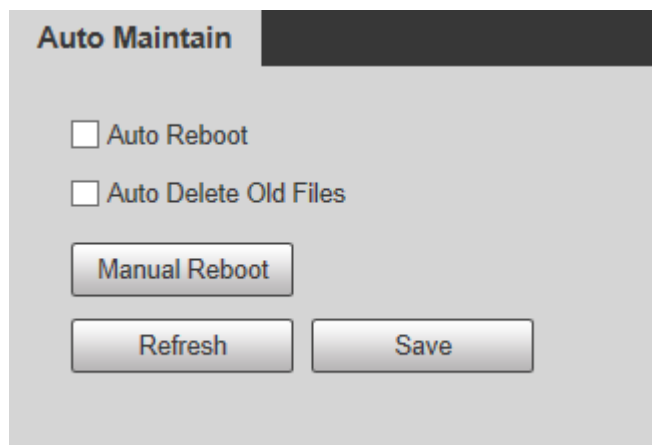
You can select **Auto Reboot** or **Auto Delete Old Files**.

- If you select **Auto Reboot**, the frequency and time need to be set.
- If you select **Auto Delete Old Files**, you need to set the time period for the files to be deleted.

Procedure

Step 1 Select **Setting** > **System** > **Auto Maintain**.


Figure 5-177 Auto maintain



Step 2 Configure parameters of auto maintain.

Table 5-55 Description of auto maintain parameter

Parameter	Description
Auto Reboot	Select the checkbox to set the Device reboot time.

Parameter	Description
Auto Delete Old Files	<p>Select the checkbox to customize the time period for the files to be deleted. The value ranges from 1 day to 31 days.</p> <p> When you enable the function, The deleted files cannot be recovered. Are you sure to enable this function now? prompt will be displayed. Think twice before enabling the function.</p>

Step 3 Click **Save**.

5.7.7.2 Emergency Maintenance

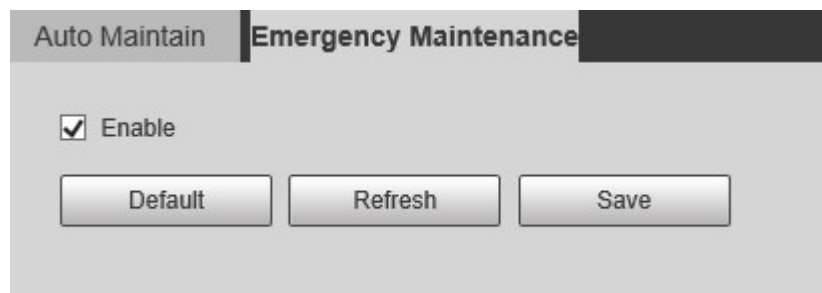
Background Information

By enabling emergency maintenance, you can fix most issues caused by upgrade and configuration.

Procedure

Step 1 Select **Setting** > **System** > **Auto Maintain** > **Emergency Maintenance**.

Figure 5-178 Auto maintain



Step 2 Click **Save**.

5.7.8 Upgrade

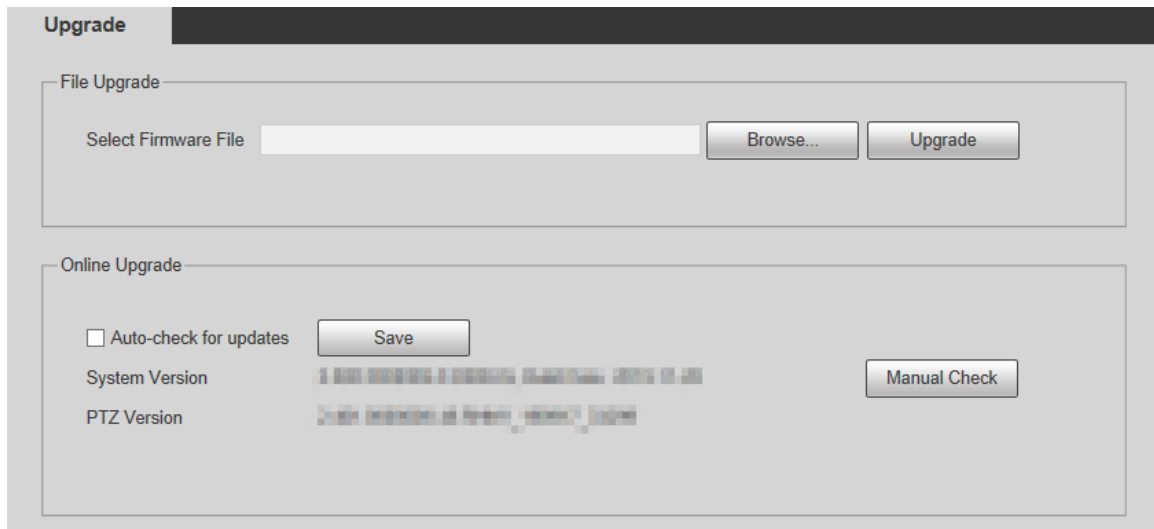
Upgrade the system to improve device function and stability.



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

Select **Setting** > **System** > **Upgrade**.

Figure 5-179 System upgrade



- File Upgrade: Click **Browse** , select the upgrade file, and then click **Upgrade** to upgrade the firmware. The upgrade file is in the format of *.bin.
- Online Upgrade

1. Select the **Auto-check for updates** checkbox.

This will enable the system to check 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 IP address, device name, firmware version, and device serial number to perform auto-check. The collected information is only used to verify the legitimacy of the Device, and push the upgrade notification.

2. Click **Save**.



Click **Manual Check**, and you can check for upgrade manually.

5.8 Information

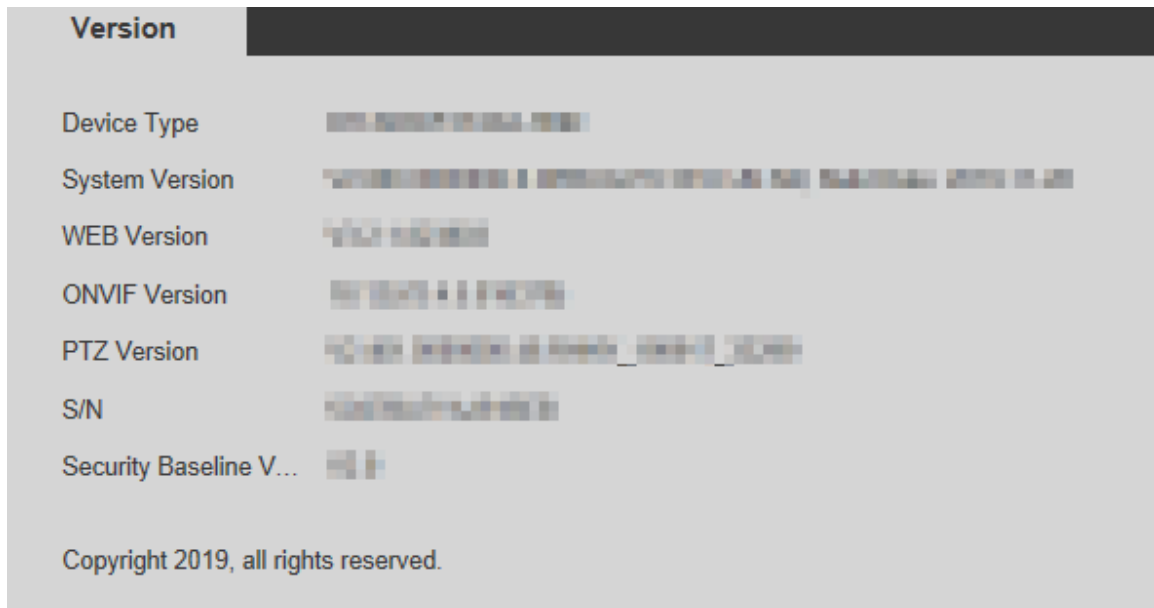
You can view information such as version, online users, log, and life statistics.

5.8.1 Version

You can view information such as system hardware features, software version and release date.

Select **Setting** > **Information** > **Version** > **Version** to view the version information of current web page.

Figure 5-180 Version



5.8.2 Log Information

5.8.2.1 Log

Select **Setting** > **Information** > **Log** > **Log** to view the operation information of the Device and system information.

Figure 5-181 Log

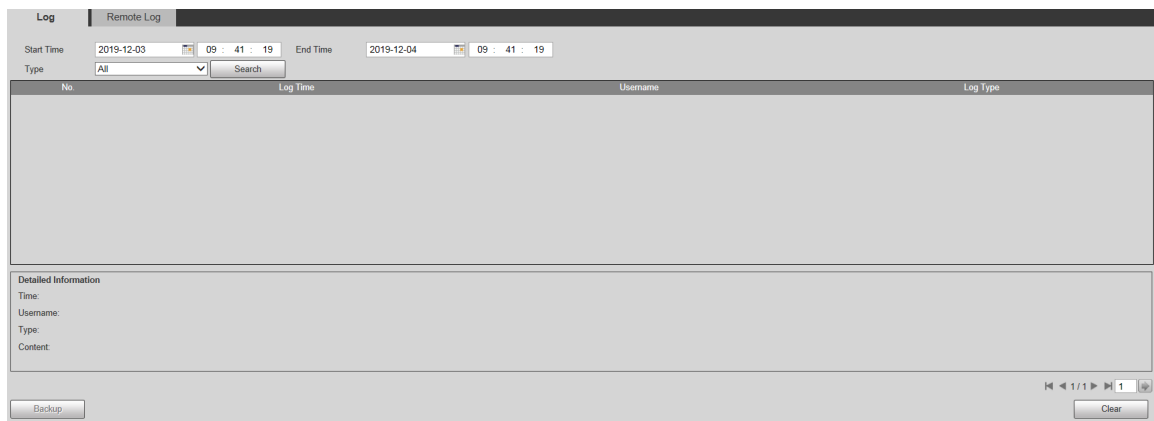



Table 5-56 Log parameter description

Parameter	Description
Start Time	The start time of the log to be searched (January 1, 2000 is the earliest time).
End Time	The end time of the log to be searched (December 31, 2037 is the latest time).
Type	The log type includes All, System, Setting, Data, Event, Record, Account, Clear Log, and Safety.

Parameter	Description
Search	Set the start time and end time of the log to be searched, select the log type, and then click Search . The searched log number and time period will be displayed.
Detailed Information	Click a log to display the details.
Clear	Clear all logs of the Device, and classified clearing is not supported.
Backup	 <p>Back up the searched system logs to the PC currently used by the user. The data will be overwritten if the disk is full. Back up the data in time as needed.</p>

Here are the meanings of different log types.

- **System** : Includes program launch, force exit, exit, program reboot, device shutdown/restart, system reboot, and system upgrade.
- **Setting** : Includes saving configurations, and deleting configuration files.
- **Data** : Includes disk type configurations, data erasing, hot swap, FTP state, and recording mode.
- **Event** (records events such as video detection, smart plan, alarm, and abnormality): Includes starting events, and ending events.
- **Record** : Includes file access, file access error, and file search.
- **Account** (records modification of user management, login, and logout): Includes login, logout, adding user, deleting user, modifying user, adding group, deleting group, and modifying group.
- **Safety** : Includes security-related information.
- **Clear Log** : Clearing logs.

5.8.2.2 Remote Log

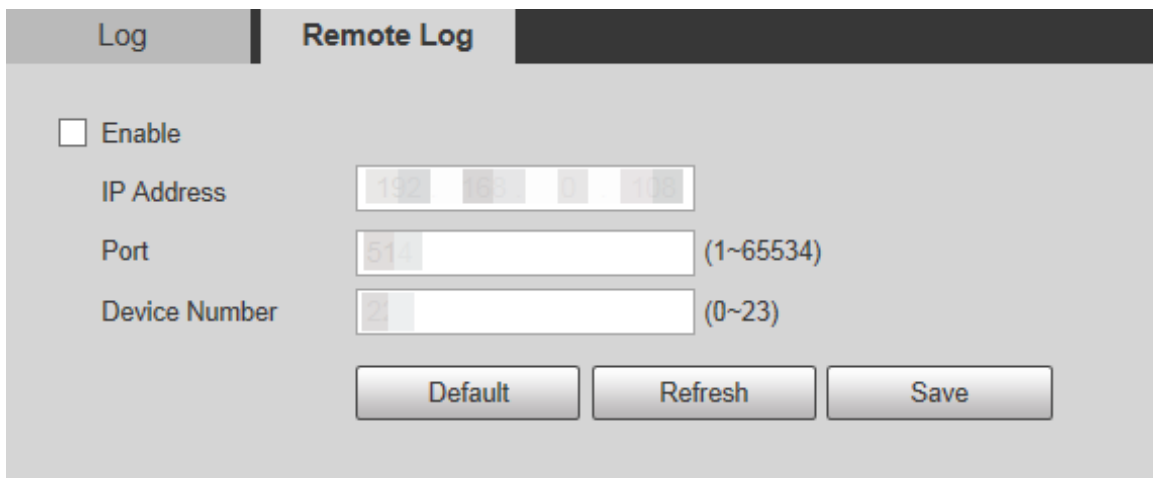
Background Information

Upload the Device operations to the log server.

Procedure

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

Figure 5-182 Remote log



Step 2 Select **Enable** to enable remote log function.

Step 3 Set the **IP Address**, **Port** and **Device Number** of the log server.



Click **Default** to restore the Device to the default settings.

5.8.3 Online User

Select **Setting** > **Information** > **Online User** to view online users.

Figure 5-183 Online users

Online User				
No.	Username	User Local Group	IP Address	User Login Time
1	admin	admin	192.168.1.100	2021-02-23 11:53:22

Refresh

5.8.4 Life Statistics

Select **Setting** > **Information** > **Life Statistics** to view the life statistics of the Device.



The function is available on select models.

Figure 5-184 Online users

Life Statistics	
Total Working Time	62 day(s) 1 hour(s) 0 minute(s)
Upgrade Times	20 time
Last Upgrade Date	2021-02-23 11:53:22

5.8.5 Battery Status

Select **Setting** > **Information** > **Battery Status** to view battery usage of the Device.



The function is available on select models.

Figure 5-185 Online users

Battery Status	
Capacity Limit	100 %
Voltage	8.303 V
Charging or Not	No
<input type="button" value="Refresh"/>	

5.8.6 Legal Information

Select **Setting** > **Information** > **Legal Info** to view legal information of the Device. Click **Software License Agreement**, **Privacy Policy** and **Open Source Software Notice** to respectively view the corresponding content.



The function is available on select models.

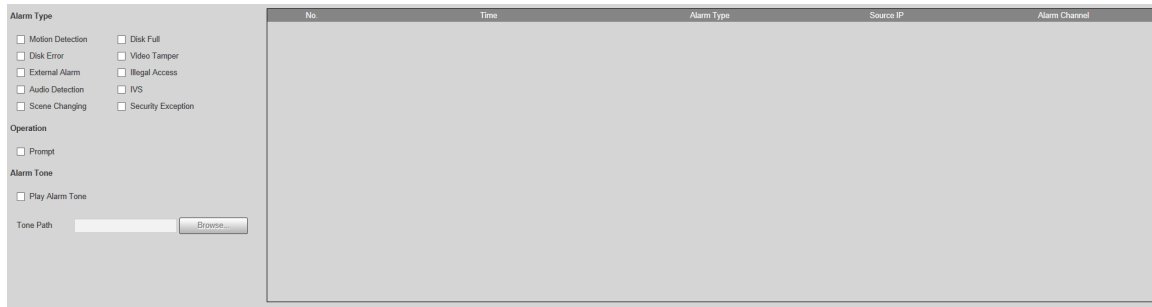
Figure 5-186 Legal information

Software License Agreement	Privacy Policy	Open Source Software Notice
<div>SOFTWARE LICENSE AGREEMENT</div> <div>Last modified: Jun 15, 2020</div>		

6 Alarm

You can select alarm types on the page. When the selected alarms are triggered, detailed alarm information will be displayed on the right side of the page. You can also select **Prompt** or **Play Alarm Tone**. When an alarm occurs, the alarm prompt or tone will be triggered.



Figure 6-1 Alarm setting page



The screenshot shows the 'Alarm Type' configuration interface. On the left, there are three sections: 'Alarm Type' with checkboxes for Motion Detection, Disk Full, Disk Error, Video Tamper, External Alarm, Illegal Access, Audio Detection, IVS, Scene Changing, and Security Exception; 'Operation' with a checkbox for Prompt; and 'Alarm Tone' with a checkbox for Play Alarm Tone and a 'Tone Path' field with a 'Browse...' button. The right section is a large table with columns: No., Time, Alarm Type, Source IP, and Alarm Channel.

Table 6-1 Description of alarm setting parameter

Category	Parameter	Description
Alarm Type	Motion Detection	Record alarm information in case of motion detection.
	Disk Full	Record alarm information in case of full disk.
	Disk Error	Record alarm information in case of disk error.
	Video Tamper	Record alarm information in case of video tampering.
	External Alarm	Record alarm information in case of an external alarm.
	Illegal Access	Record alarm information in case of illegal access.
	Audio Detection	Record alarm information in case of audio detection.
	IVS	Record alarm information in case of smart events.
	Scene Changing	Record alarm information in case of scene changing.
	Security Exception	Record alarm information in case of security exception.

Category	Parameter	Description
Operation	Prompt	<p>Select the Prompt checkbox. When you are not on the Alarm page, and the selected alarm event is triggered, the Relay-out button on the main menu will change to , and the alarm information will be automatically recorded. After you click the Alarm menu bar, the button disappears.</p> <p></p> <p>If you are on the Alarm page, there will be no image prompt when the selected alarm event is triggered, but the corresponding alarm information will be recorded in the alarm list on the right.</p>
	Play Alarm Tone	Select the checkbox, and then select the tone file path. When the selected alarm event is triggered, the selected tone file will be played to prompt you that an alarm event is triggered.
Alarm Tone	Tone Path	Customize the storage path for alarm tones.

7 Logout

Click **Logout** to log out, and the login page is displayed. Enter the username and password to log in again.

Figure 7-1 Login page



Appendix 1 Security Recommendation

Account Management

1. Use complex 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: 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 repeating characters, such as 111, aaa, etc.

2. Change passwords periodically

It is recommended to periodically change the device password to reduce the risk of being guessed or cracked.

3. Allocate accounts and permissions appropriately

Appropriately add users based on service and management requirements and assign minimum permission sets to users.

4. Enable account logout function

The account logout function is enabled by default. You are advised to keep it enabled to protect account security. After multiple failed password attempts, the corresponding account and source IP address will be locked.

5. Set and update password reset information in a timely manner

The device supports password reset function. To reduce the risk of this function being used by threat actors, if there is any change in the information, please modify it in time. When setting security questions, it is recommended not to use easily guessed answers.

Service Configuration

1. Enable HTTPS

It is recommended that you enable HTTPS to access web services through secure channels.

2. Encrypted transmission of audio and video

If your audio and video data contents are very important or sensitive, it is recommended to use encrypted transmission function in order to reduce the risk of your audio and video data being eavesdropped during transmission.

3. Turn off non-essential services and use safe mode

If not needed, it is recommended to turn off some services such as SSH, SNMP, SMTP, UPnP, AP hotspot etc., to reduce the attack surfaces.

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

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

4. Change HTTP and other default service ports

It is recommended that you change the default port of HTTP and other services to any port between 1024 and 65535 to reduce the risk of being guessed by threat actors.

Network Configuration

1. **Enable Allowlist**

It is recommended that you turn on the allowlist function, and only allow IP in the allowlist to access the device. Therefore, please be sure to add your computer IP address and supporting device IP address to the allowlist.

2. **MAC address binding**

It is recommended that you bind the IP address of the gateway to the MAC address on the device to reduce the risk of ARP spoofing.

3. **Build a secure network environment**

In order to better ensure the security of devices and reduce potential cyber risks, the following are recommended:

- Disable the port mapping function of the router to avoid direct access to the intranet devices from external network;
- According to the actual network needs, partition the network: if there is no communication demand between the two subnets, it is recommended to use VLAN, gateway and other methods to partition the network to achieve network isolation;
- Establish 802.1x access authentication system to reduce the risk of illegal terminal access to the private network.

Security Auditing

1. **Check online users**

It is recommended to check online users regularly to identify illegal users.

2. **Check device log**

By viewing logs, you can learn about the IP addresses that attempt to log in to the device and key operations of the logged users.

3. **Configure network log**

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

Software Security

1. **Update firmware in time**

According to the industry standard operating specifications, the firmware of devices needs to be updated to the latest version in time in order to ensure that the device has the latest functions and security. If the device is connected to the public network, it is recommended to enable the online upgrade automatic detection function, so as to obtain the firmware update information released by the manufacturer in a timely manner.

2. **Update client software in time**

It is recommended to download and use the latest client software.

Physical Protection

It is recommended that you carry out physical protection for devices (especially storage devices), such as placing the device in a dedicated machine room and cabinet, and having access control

and key management in place to prevent unauthorized personnel from damaging hardware and other peripheral equipment (e.g. USB flash disk, serial port).

Appendix 2 Security Commitment and Recommendation

Dahua Vision Technology Co., Ltd. (hereinafter referred to as "Dahua") attaches great importance to cybersecurity and privacy protection, and continues to invest special funds to comprehensively improve the security awareness and capabilities of Dahua employees and provide adequate security for products. Dahua has established a professional security team to provide full life cycle security empowerment and control for product design, development, testing, production, delivery and maintenance. While adhering to the principle of minimizing data collection, minimizing services, prohibiting backdoor implantation, and removing unnecessary and insecure services (such as Telnet), Dahua products continue to introduce innovative security technologies, and strive to improve the product security assurance capabilities, providing global users with security alarm and 24/7 security incident response services to better protect users' security rights and interests. At the same time, Dahua encourages users, partners, suppliers, government agencies, industry organizations and independent researchers to report any potential risks or vulnerabilities discovered on Dahua devices to Dahua PSIRT, for specific reporting methods, please refer to the cyber security section of Dahua official website.

Product security requires not only the continuous attention and efforts of manufacturers in R&D, production, and delivery, but also the active participation of users that can help improve the environment and methods of product usage, so as to better ensure the security of products after they are put into use. For this reason, we recommend that users safely use the device, including but not limited to:

Account Management

1. Use complex 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: 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 repeating characters, such as 111, aaa, etc.

2. Change passwords periodically

It is recommended to periodically change the device password to reduce the risk of being guessed or cracked.

3. Allocate accounts and permissions appropriately

Appropriately add users based on service and management requirements and assign minimum permission sets to users.

4. Enable account lockout function

The account lockout function is enabled by default. You are advised to keep it enabled to protect account security. After multiple failed password attempts, the corresponding account and source IP address will be locked.

5. Set and update password reset information in a timely manner

Dahua device supports password reset function. To reduce the risk of this function being used by threat actors, if there is any change in the information, please modify it in time. When setting security questions, it is recommended not to use easily guessed answers.

Service Configuration

1. Enable HTTPS

It is recommended that you enable HTTPS to access Web services through secure channels.

2. Encrypted transmission of audio and video

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

3. Turn off non-essential services and use safe mode

If not needed, it is recommended to turn off some services such as SSH, SNMP, SMTP, UPnP, AP hotspot etc., to reduce the attack surfaces.

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

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

4. Change HTTP and other default service ports

It is recommended that you change the default port of HTTP and other services to any port between 1024 and 65535 to reduce the risk of being guessed by threat actors.

Network Configuration

1. Enable Allowlist

It is recommended that you turn on the allowlist function, and only allow IP in the allowlist to access the device. Therefore, please be sure to add your computer IP address and supporting device IP address to the allowlist.

2. MAC address binding

It is recommended that you bind the IP address of the gateway to the MAC address on the device to reduce the risk of ARP spoofing.

3. Build a secure network environment

In order to better ensure the security of devices and reduce potential cyber risks, the following are recommended:

- Disable the port mapping function of the router to avoid direct access to the intranet devices from external network;
- According to the actual network needs, partition the network: if there is no communication demand between the two subnets, it is recommended to use VLAN, gateway and other methods to partition the network to achieve network isolation;
- Establish 802.1x access authentication system to reduce the risk of illegal terminal access to the private network.

Security Auditing

1. Check online users

It is recommended to check online users regularly to identify illegal users.

2. Check device log

By viewing logs, you can learn about the IP addresses that attempt to log in to the device and key operations of the logged users.

3. **Configure network log**

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

Software Security

1. **Update firmware in time**

According to the industry standard operating specifications, the firmware of devices needs to be updated to the latest version in time in order to ensure that the device has the latest functions and security. If the device is connected to the public network, it is recommended to enable the online upgrade automatic detection function, so as to obtain the firmware update information released by the manufacturer in a timely manner.

2. **Update client software in time**

We recommend you to download and use the latest client software.

Physical Protection

It is recommended that you carry out physical protection for devices (especially storage devices), such as placing the device in a dedicated machine room and cabinet, and having access control and key management in place to prevent unauthorized personnel from damaging hardware and other peripheral equipment (e.g. USB flash disk, serial port).

ENABLING A SMARTER SOCIETY AND BETTER LIVING

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.

Address: No. 1399, Binxing Road, Binjiang District, Hangzhou, P. R. China | Website: www.dahuasecurity.com | Postcode: 310053

Email: dhoverseas@dhvisiontech.com | Tel: +86-571-87688888 28933188