

Network Speed Dome & PTZ Camera User's Manual

Web 3.0



Foreword

General

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

Safety Instructions

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

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

Revision History

Version	Revision Content	Release Time
V2.0.2	Added the note to provide international calling codes for 4G models.	June 2020
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

About the Manual

- The manual is for reference only. If there is inconsistency between the manual and the actual product, the actual product shall prevail.

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

Important Safeguards and Warnings

The manual will help you to use the Device properly. Read the manual carefully before using the Device, and keep it well for future reference.

Operation Requirements

- Avoid heavy stress, violent vibration, and water splash during transportation, storage, and installation. Complete package is necessary during the transportation. We assume no responsibility for any damage or problem caused by the incomplete package during the transportation.
- To avoid damage, protect the Device from falling down and heavy vibration. Arrange more than one person to move the Device when necessary.
- Buckle the safety hook before installing the Device if it is included.
- Keep the Device away from devices that generate electromagnetic field like televisions, radio transmitters, electromagnetic devices, electric machine, transformers, and speakers; otherwise image quality will be influenced.
- Keep the Device away from smoke, vapor, heat, and dust.
- Do not install the Device near heating furnace, spotlight, and other heat sources. If it is installed on ceiling, in kitchen or near boiler room, the Device temperature might rise.
- Do not disassemble the Device; otherwise it might cause dangers or device damage. Contact your local retailer or customer service center for internal setup or maintenance requirement.
- Make sure that there is no metal, or inflammable, explosive substance in the Device; otherwise it might cause fire, short-circuit, or other damage. Power off the Device and disconnect the power cord immediately if there is water or liquid falling into the Device. And contact your local retailer or customer service center. Avoid sea water or rain eroding the Device.
- Avoid aiming the lens at intense light source, including sunlight, and incandescent light; otherwise the lens might be damaged.
- Clean the enclosure with soft cloth. To remove the dirt, you can dip the soft cloth in proper detergent, wring the soft cloth out, and then dry the enclosure with soft cloth. Do not use gasoline, paint thinner, or other chemicals to clean the enclosure; otherwise it might result in enclosure transfiguration or paint flake. Read all the manuals included before using chemical cloth. Avoid long time touch between the plastic or rubber material and the enclosure; otherwise it might result in device damage and paint flake.
- It is recommended to use the Device with a lightning-proof device for better lightning-proof effect.

Requirements for Installation and Maintenance Personnel

- Have certificates or experiences related to installation and maintenance of the closed-circuit television (CCTV), and have certificates related to working at height.
- Have basic knowledge and installation skills of CCTV system.
- Have basic knowledge and operation technique for low-voltage wiring and low-voltage electronic circuit connection.
- Have the ability to read and understand the manual.

Requirements for Lifting the Device

- Use secure lifting appliances suitable for the installation place and the product installation mode.
- Make sure that the selected tools reach the installation height and have high safety performance.



- All installation and operations shall conform to local electrical safety regulations.
- The power source shall conform to the requirements of the Safety Extra Low Voltage (SELV) standard, and supply power with rated voltage which conforms to Limited Power Source requirement according to IEC60950-1. Note that the power supply requirement is subject to the device label.
- Use the power adapter recommended by the manufacturer.
- For the Device that supports laser, do not aim the laser directly at eyes. And keep a proper distance from the flammable to avoid fire.
- Do not connect several devices to one power adapter; otherwise it might result in overheat or fire if it exceeds the rated load.
- Make sure that the power is off when you connect the cables, install or uninstall the Device.
- Power off the Device and disconnect the power cord immediately if there is any smoke, disgusting smell, or noise from the Device. And contact your local retailer or customer service center.
- Contact your local retailer or customer service center if the Device is abnormal. Do not disassemble or repair the Device by yourself. We assume no responsibility for any problems caused by unauthorized modifications, disassembly or repair, incorrect installation or use, and overuse of certain components.

Table of Contents

Foreword	I
Important Safeguards and Warnings	III
1 Network Configuration.....	1
1.1 Network Connection.....	1
1.2 Logging in to the Web Interface	1
1.2.1 Device Initialization	1
1.2.2 First-time Login	5
1.2.3 Device Login	6
1.2.4 Resetting Password.....	7
2 Live.....	9
2.1 Encoding Setting	9
2.2 Video Window Adjustment	10
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 Interface	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.....	29
4.1.4 Video Playback File Search and Display Area	30
4.1.5 Video Clipping Area	33
4.1.6 Progress Bar Time Formats.....	33
4.2 Picture Playback	34
4.2.1 Picture Playing Functions	34
4.2.2 Picture Playback File Search and Display Area	35
4.2.3 Snapshot Types	36
5 Setting	37
5.1 Camera.....	37
5.1.1 Conditions Settings.....	37
5.1.2 Video	53
5.1.3 Audio	63
5.2 Network Settings	65
5.2.1 TCP/IP	65
5.2.2 Port	68
5.2.3 PPPoE	70

5.2.4 DDNS.....	70
5.2.5 SMTP (Email).....	72
5.2.6 UPnP.....	74
5.2.7 SNMP.....	75
5.2.8 Bonjour.....	77
5.2.9 Multicast.....	78
5.2.10 Auto Register	79
5.2.11 Wi-Fi.....	80
5.2.12 802.1x	81
5.2.13 QoS.....	82
5.2.14 4G	83
5.2.15 Access Platform	86
5.3 PTZ Settings	89
5.3.1 Protocol.....	89
5.3.2 Function	90
5.4 Event Management.....	101
5.4.1 Video Detection	101
5.4.2 Smart Motion Detection	107
5.4.3 Audio Detection.....	108
5.4.4 Smart Plan	110
5.4.5 IVS	111
5.4.6 Face Recognition.....	117
5.4.7 People Counting	127
5.4.8 Heat Map	128
5.4.9 Video Metadata.....	130
5.4.10 Alarm.....	134
5.4.11 Abnormality	134
5.5 Storage.....	139
5.5.1 Schedule	139
5.5.2 Snapshot by Location	142
5.5.3 Destination	143
5.5.4 Record Control.....	146
5.6 System Management	147
5.6.1 Device Settings.....	147
5.6.2 Account Settings	149
5.6.3 Safety.....	155
5.6.4 Peripheral.....	166
5.6.5 Default.....	167
5.6.6 Import/Export	167
5.6.7 Auto Maintain	168
5.6.8 Upgrade	169
5.7 Information	169
5.7.1 Version.....	169
5.7.2 Log Information.....	170
5.7.3 Online User.....	172
6 Alarm.....	172
7 Logout	174

1 Network Configuration

1.1 Network Connection

To view the web interface on your PC, connect the Device to the PC first. There are mainly two connection modes between the Device and PC. See Figure 1-1 and Figure 1-2.

Figure 1-1 Direct connection by using a network cable

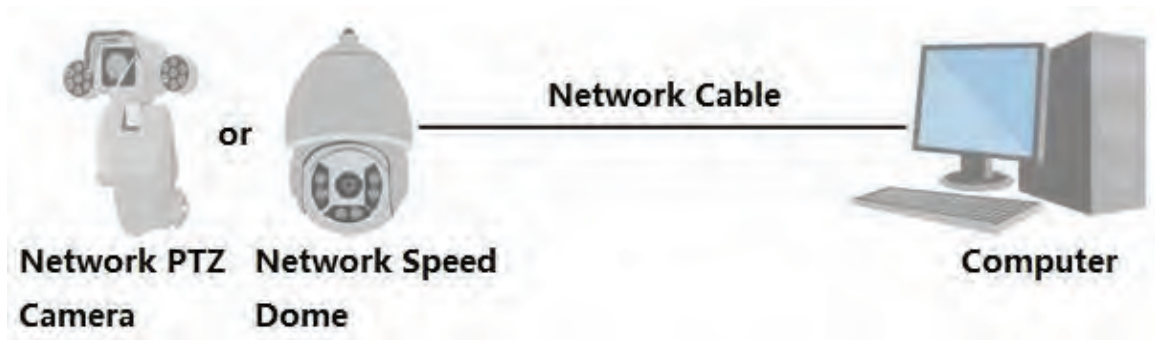
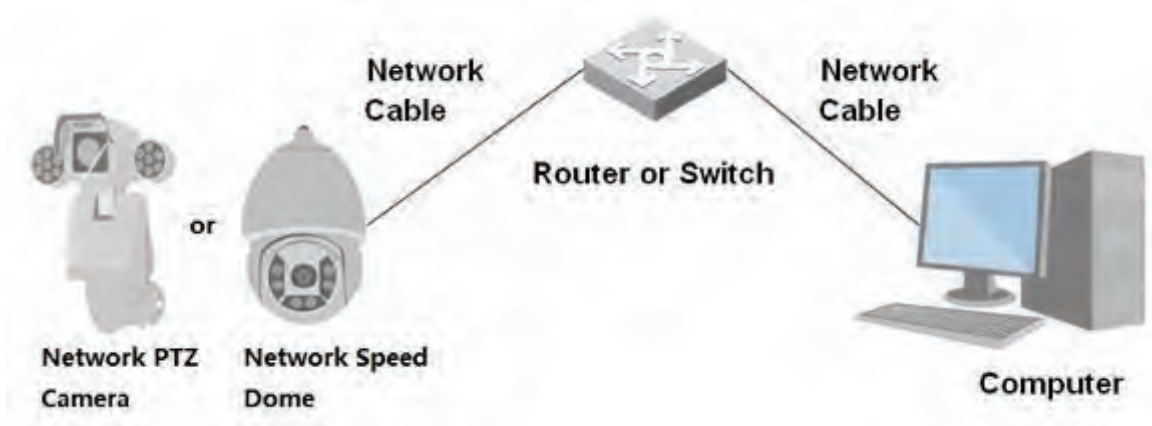


Figure 1-2 Connection over by using a switch or router



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

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 Logging in to the Web Interface

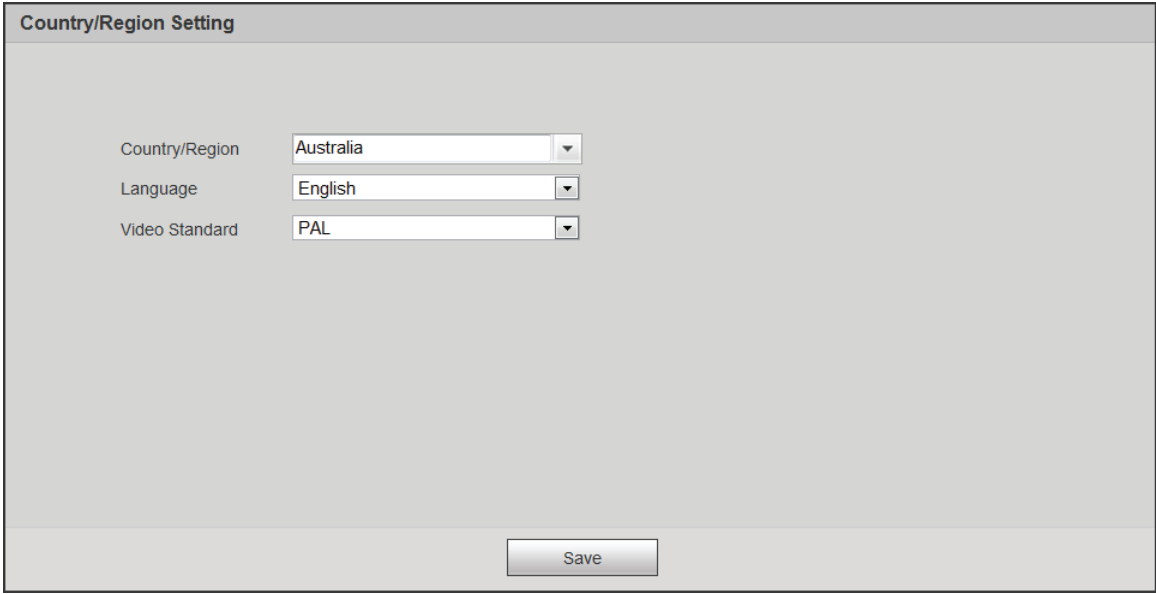
1.2.1 Device Initialization

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

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

The **Country/Region Setting** interface is displayed. Set the **Country/Region**, **Language** and **Video Standard** as needed. See Figure 1-3.

Figure 1-3 Country/region setting interface

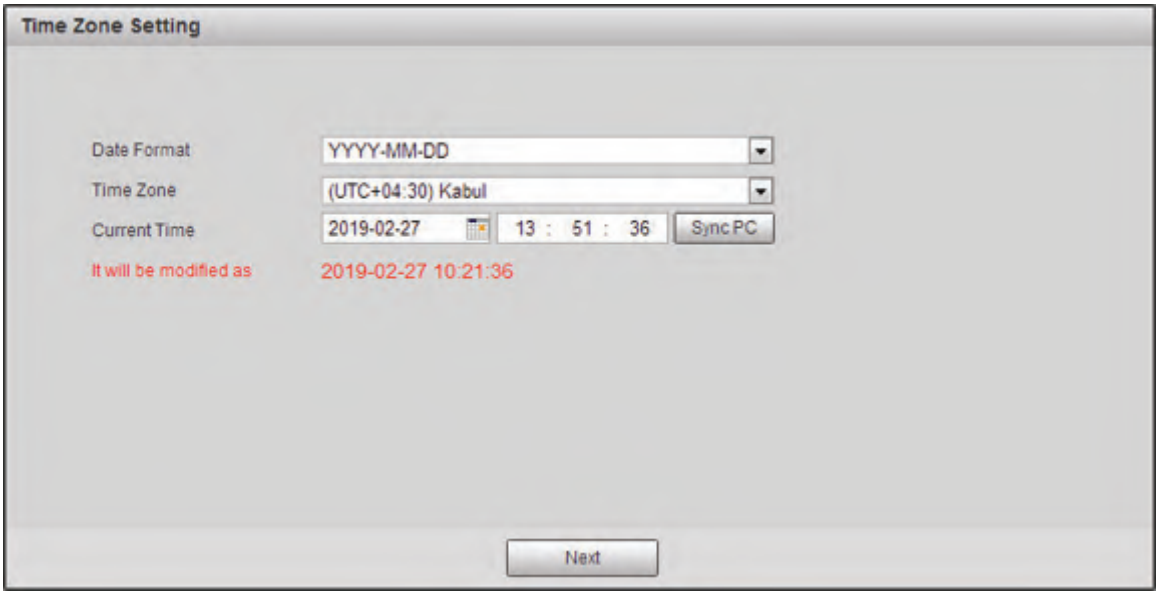
The image shows a software window titled "Country/Region Setting". Inside the window, there are three rows of settings, each with a label and a dropdown menu. The first row is "Country/Region" with "Australia" selected. The second row is "Language" with "English" selected. The third row is "Video Standard" with "PAL" selected. At the bottom center of the window is a "Save" button.

Country/Region	Australia
Language	English
Video Standard	PAL

Save

Step 2 Click **Save**, and the **Time Zone Setting** interface is displayed. Configure time parameters. See Figure 1-4.

Figure 1-4 Time zone setting interface

The image shows a software window titled "Time Zone Setting". It contains several settings: "Date Format" is set to "YYYY-MM-DD"; "Time Zone" is set to "(UTC+04:30) Kabul"; "Current Time" shows the date "2019-02-27" and time "13 : 51 : 36", with a "Sync PC" button next to it. Below these, a red text label says "It will be modified as" followed by the time "2019-02-27 10:21:36". At the bottom center is a "Next" button.

Date Format	YYYY-MM-DD
Time Zone	(UTC+04:30) Kabul
Current Time	2019-02-27 13 : 51 : 36

Sync PC

It will be modified as 2019-02-27 10:21:36

Next

Step 3 Click **Next**.

The **Device Initialization** interface is displayed. For the interface, see Figure 1-5. For the parameter description, see Table 1-1.

Figure 1-5 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: [input field]

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 4 Click **Save**.

The **P2P** interface is displayed. See Figure 1-6.

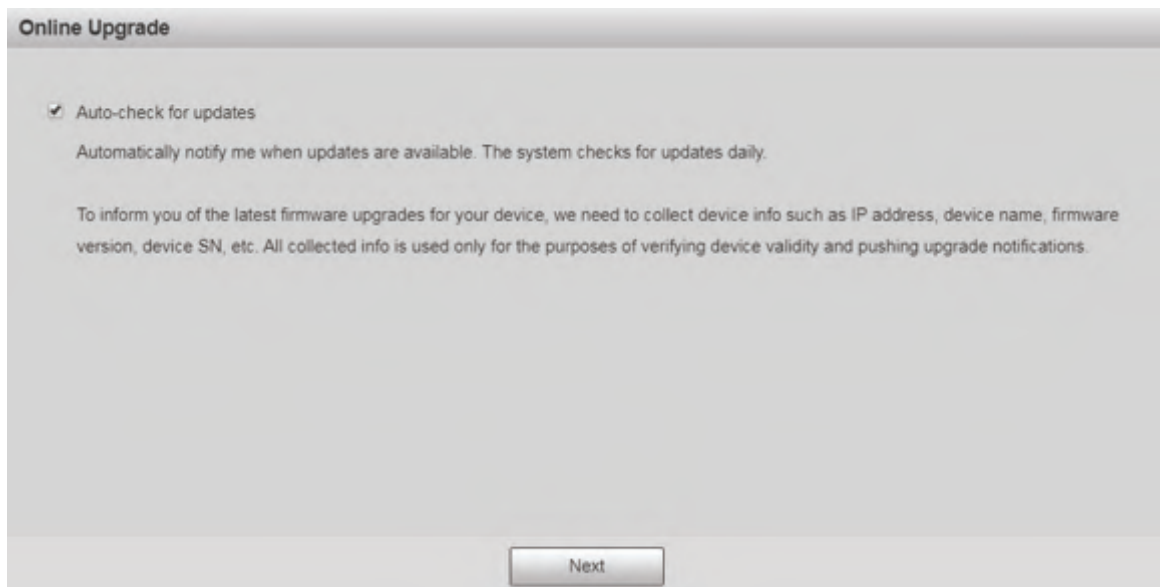
Figure 1-6 P2P interface



Step 5 Scan the QR code on the interface, download the app, and then finish configurations according to the instructions on your mobile device. After that, click **Next**.

The **Online Upgrade** interface is displayed. See Figure 1-7.

Figure 1-7 Online upgrade



Step 6 Select **Auto-check for updates** check box as needed.

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 7 Click **Next**, and the login interface is displayed. See Figure 1-8.

Figure 1-8 Login interface



1.2.2 First-time Login

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

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

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

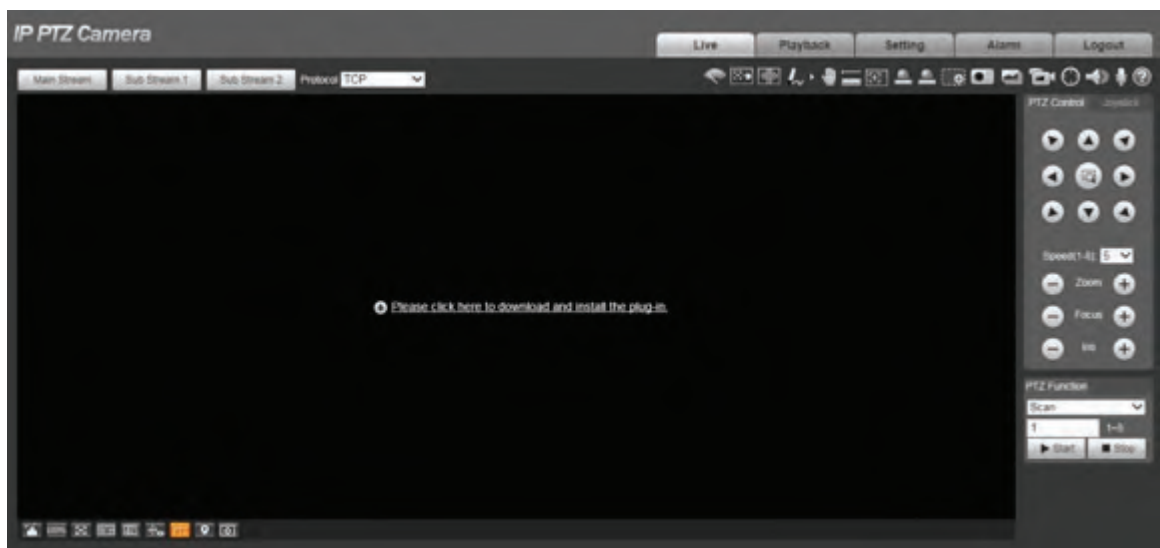
The web interface is displayed.



- 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 web interface again.
- You can set the number of allowed password attempts and locked time in "5.4.11.3 Illegal Access."

Step 3 Download and install the plug-in according to the on-screen instruction after logging in to the web interface. See Figure 1-9.

Figure 1-9 Installing the plug-in



Step 4 After the plug-in is installed, the web interface will be refreshed automatically, and the video is displayed in **Live** interface. See Figure 1-10.

Figure 1-10 Live interface



The **Live** interface shown in the manual is for reference only, and the actual interface shall prevail.

1.2.3 Device Login

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

The **Login** interface is displayed. See Figure 1-11.

Figure 1-11 Device login



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

The web interface is displayed, and the video is displayed in **Live** interface.



- 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 web interface again.
- You can set the number of allowed password attempts and locked time. For details, see "5.4.11.3 Illegal Access."

1.2.4 Resetting Password

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 "5.6.3.2 System Service."

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

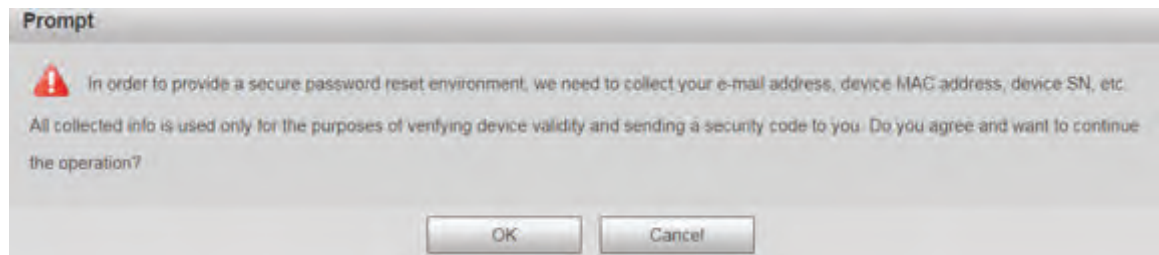
The **Login** interface is displayed. See Figure 1-12.

Figure 1-12 Login



Step 2 Click **Forgot password?**, and the **Prompt** interface is displayed. See Figure 1-13.

Figure 1-13 Prompt



Step 3 Click **OK** to reset the password. The **Reset the password (1/2)** interface is displayed.



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

Figure 1-14 Resetting the password (1)

Reset the password(1/2)

QR code:

Please scan the QR code on the actual interface

Notes(For admin only):
Please use an APP to scan the left QR code to get special strings. And then send the strings to support_gpwd@htrmicrochip.com

The security code will be delivered to [***@****.com]

Security code:

Cancel Next

Step 4 Scan the QR code on the actual interface 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)** interface is displayed. See Figure 1-15.

Figure 1-15 Resetting the password (2)

Reset the password(2/2)

Username: admin

Password:

The minimum pass phrase length is 8 characters

Weak Middle Strong

Use a password that has 8 to 32 characters, it can be a combination of letter(s), number(s) and symbol(s) with at least two kinds of them. (please do not use special symbols like ' ' ; : &)

Confirm Password:

Cancel Save

Step 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** interface is displayed. See Figure 2-1.

Figure 2-1 Live interface



For descriptions of function bars on the **Live** interface, see Table 2-1.

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



Some devices do not support two sub streams.

For the encoding setting area, See Figure 2-2. For the parameter description, see Table 2-2.

Figure 2-2 Encoding setting

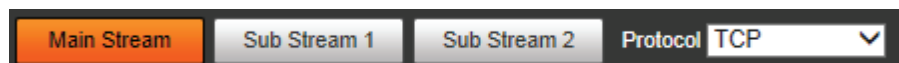


Table 2-2 Encoding setting parameter description

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.
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	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.
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

For the video window adjustment bar, See Figure 2-3. For parameter description, see Table 2-3.

Figure 2-3 Video window adjustment



Table 2-3 Video window adjustment parameter description

No.	Parameter	Description
1	Image Adjustment	Click this button, and the Image Adjustment interface is displayed on the right side of the Live interface. You can adjust parameters such as brightness, contrast, hue, and saturation on the interface.
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 button.
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 interface after the function is enabled. The function is

No.	Parameter	Description
		enabled by default.
7	PTZ	Click this button, and PTZ configurations are displayed on the Live interface after the function is enabled.
8	Face	Click this button, and face pictures 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.
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 interface. You can perform operations such as positioning, calling presets, and setting tours.

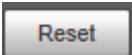
Image Adjustment

For **Image Adjustment** interface, see Figure 2-4. For parameter description, see Table 2-4.

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 interface 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

For the **Panorama** interface, see Figure 2-5.

Figure 2-5 Panorama interface



- You can perform positioning in this window by drawing a box with the left mouse button. The located area is displayed on the **Live** interface 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 **Preset** to call a corresponding preset on the right side of the window. For the interface, see Figure 2-6. For how to set a preset, see "5.3.2.1 Preset."

Figure 2-6 Preset



You can click **Tour** to call a corresponding tour on the right side of the window. For the interface, see Figure 2-7. For how to set a tour, see "5.3.2.2 Tour."

Figure 2-7 Tour



Face

For the **Face** interface, see Figure 2-8. Face recognition result is displayed on the left side, and the captured face picture and attributes are displayed on the right side.

Figure 2-8 Face



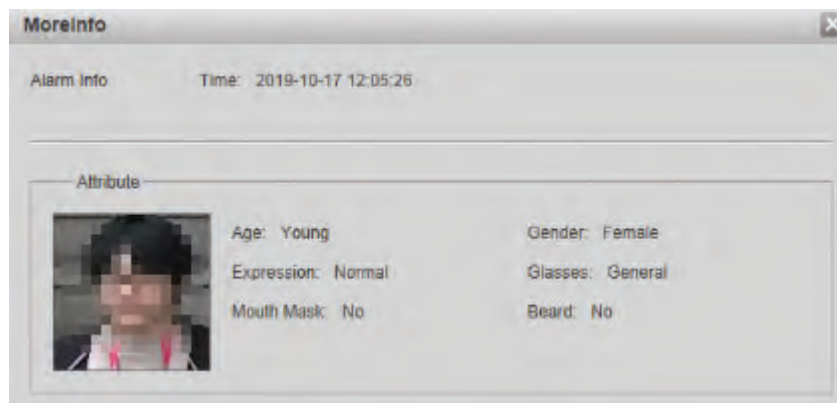
- Face recognition result display area: Displays the captured small face pictures, the corresponding face pictures in the database, and the similarities between them. After you click the picture, the attributes and details are displayed. See Figure 2-9.

Figure 2-9 Face recognition result display



- **Face and attributes display zone:** Displays the captured small face pictures and information such as gender, age, and expression. After you click the picture, the details are displayed. See Figure 2-10.

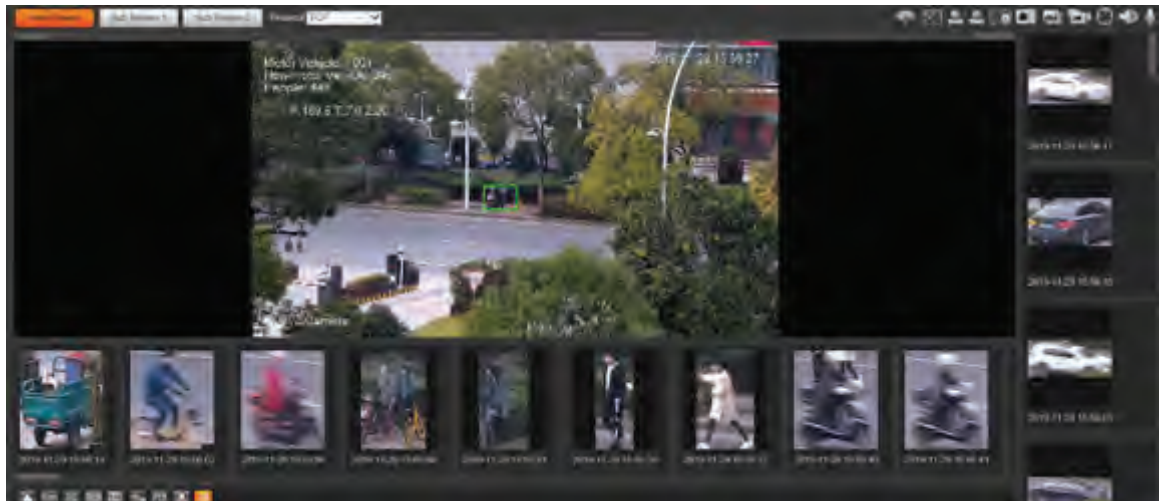
Figure 2-10 Face and attributes display



Video Metadata

For the interface, see Figure 2-11. Motor vehicle information is displayed on the right side, and the information about human and non-motor vehicles is at the bottom of the interface. For more details, see "5.4.9 Video Metadata."

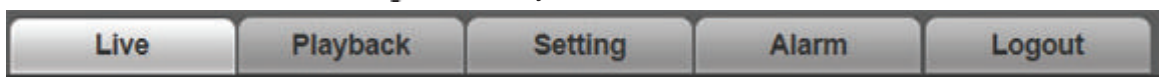
Figure 2-11 Video metadata



2.3 System Menu

To access an interface, click the corresponding tab on the system menu. For the system menu, see Figure 2-12.

Figure 2-12 System menu



2.4 Video Window Functions

For the video window function buttons, See Figure 2-13. For the parameter description, see Table 2-5.

Figure 2-13 Video window function buttons

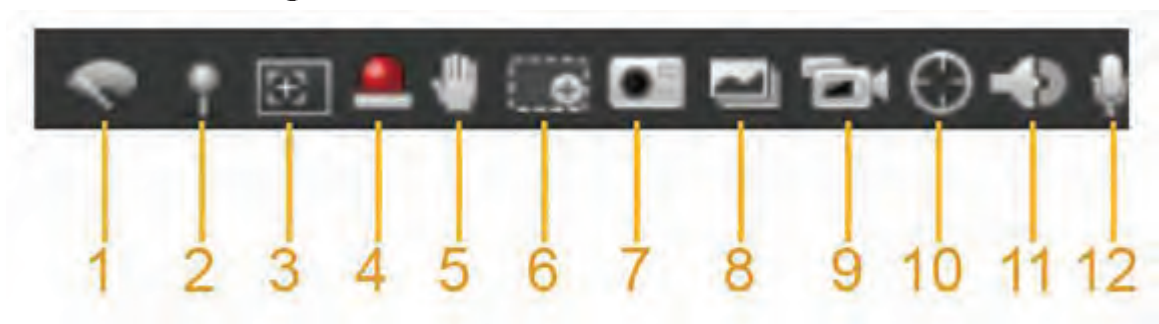


Table 2-5 Video window function button description

No.	Parameter	Description
1	Wiper Control	Click this button to select wiper operation. 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

No.	Parameter	Description
		left to right for one time.
2	Mark	Click this button, right-click on the Live interface, and the function menu is displayed. See Figure 2-14. You can add information on the Live interface, and also manage added comments. ● Add Info: Select Add Info from the pop-up menu, and enter the comment. For the interface, see Figure 2-15. ● Managing comments: Select Info Management from the pop-up menu to display, hide, or delete added comments. For the interface, see Figure 2-16.
3	Regional Focus	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.
4	Relay-out	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.
5	Gesture Control	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.
6	Digital Zoom	● 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	Click the button to capture one picture of the current image, and it will be saved to the live snapshot storage path set in "5.1.2.5 Path."
8	Triple Snapshot	Click the button, and three pictures 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

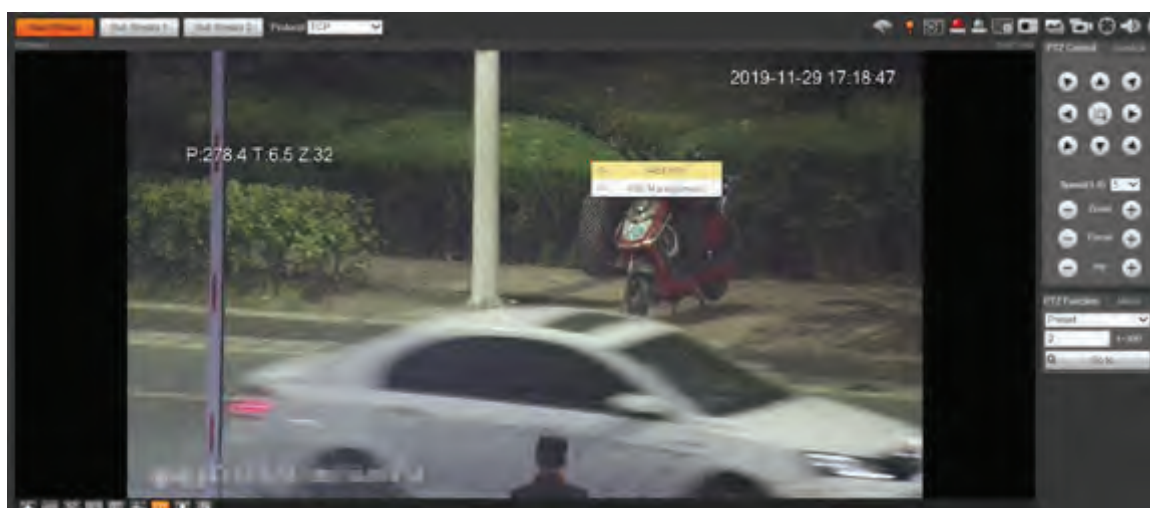
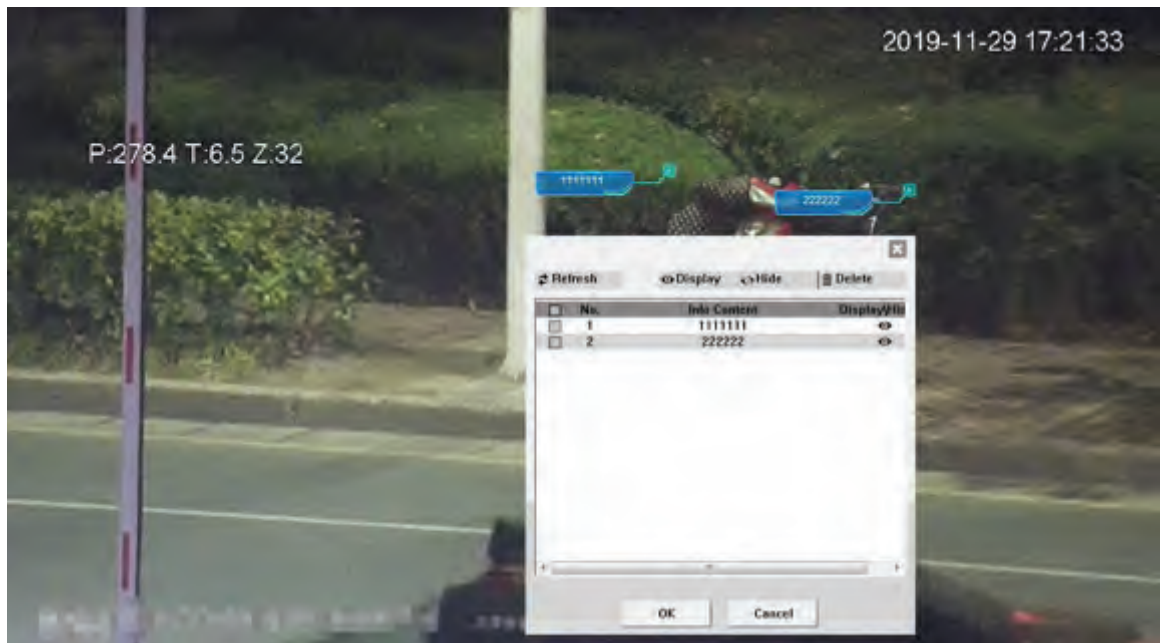


Figure 2-15 Mark—adding comments



Figure 2-16 Mark—managing 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**.

For **PTZ Control** panel, See Figure 2-17. For parameter description, see Table 2-6.

Figure 2-17 PTZ control

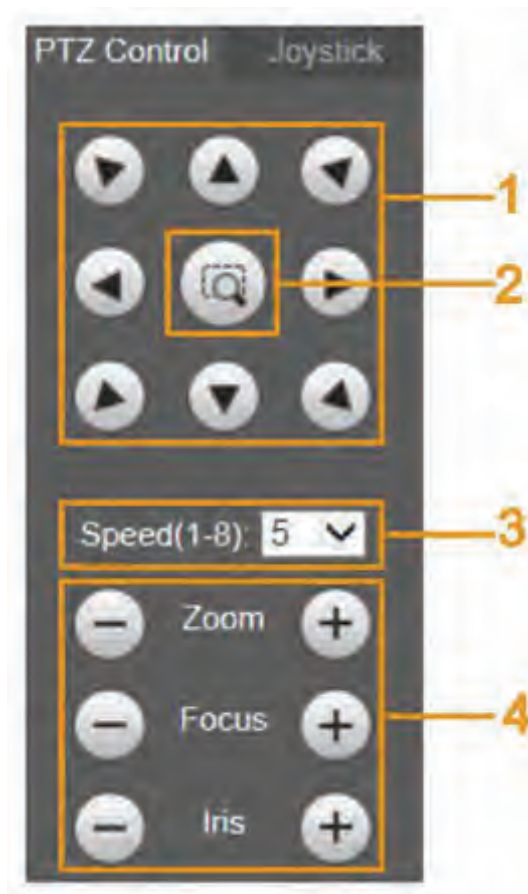


Table 2-6 PTZ control parameter description

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 an 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. For the operation interface, see Figure 2-18. 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 **Start** or **Go to** to start using the function, and then click **Stop** to stop using the function. For the configuration interface, see Figure 2-19. For the supported functions and settings, see Table 2-7.

Figure 2-19 PTZ function



Table 2-7 PTZ functions description

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.
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.

Parameter	Description
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	- 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

For the menu interface, see Figure 2-20. For the parameter description, see Table 2-8.

Figure 2-20 Menu interface

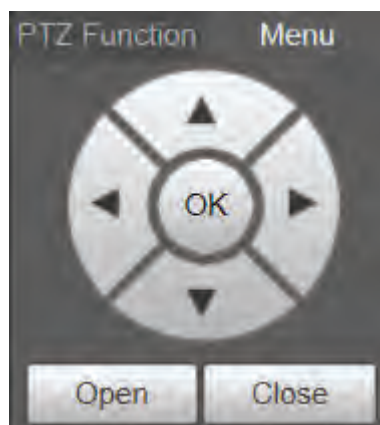
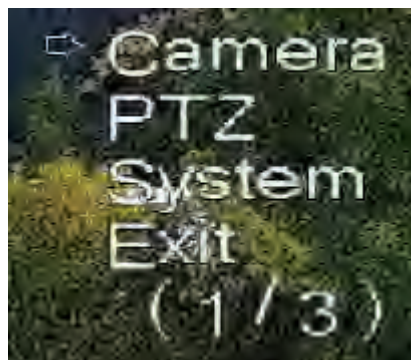


Table 2-8 Menu parameter description

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. See Figure 2-21.

Figure 2-21 OSD menu



You can finish the following settings through the menu:

- Camera settings: See "5.1 Camera."
- PTZ settings: See "5.3 PTZ Settings."
- System management: See "5.6 System Management."



You can change the location of the OSD menu in "5.1.2.3 Overlay."

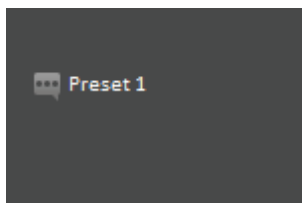
2.6 PTZ Status

On the **Live** interface, the PTZ status is displayed at the lower right corner. See Figure 2-22.



The function is available on select models.

Figure 2-22 PTZ status



When the PTZ lifespan is close to the threshold, the warning will be displayed on the **Live** interface. See Figure 2-23 and Figure 2-24.

Figure 2-23 Warning (1)

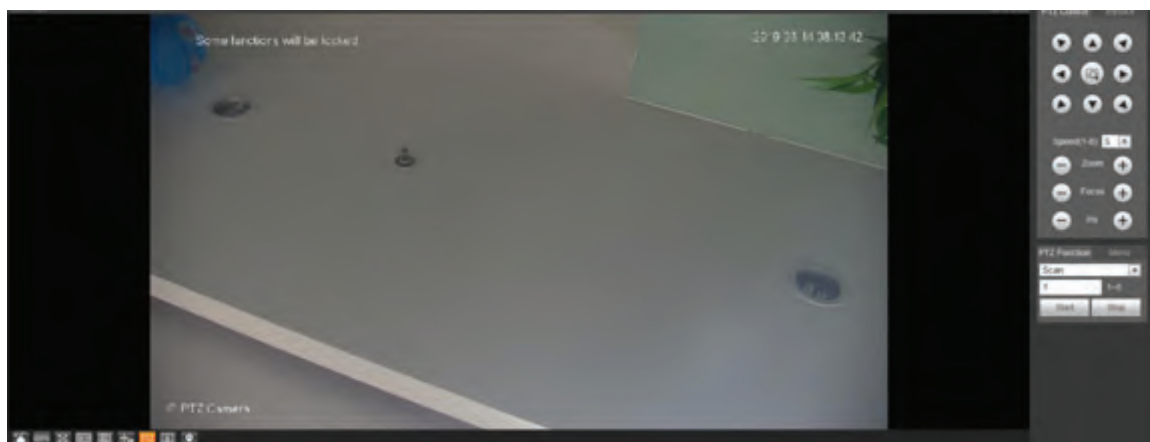
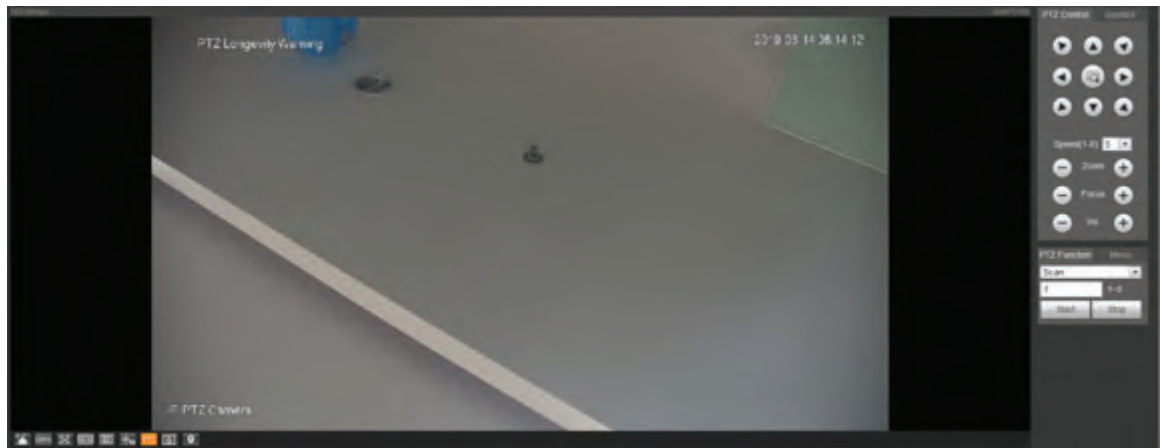


Figure 2-24 Warning (2)



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 Interface

For the **AI Live** interface, see Figure 3-1. For the layout description, see Table 3-1.

Figure 3-1 AI live interface

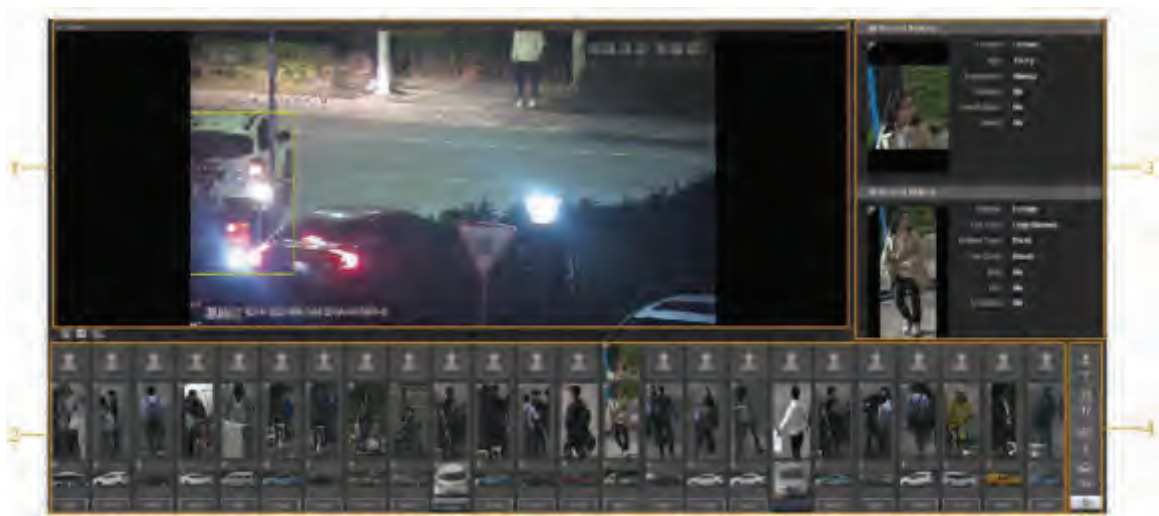


Table 3-1 AI live interface description

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

Display the information of the captured targets in real time. See Figure 3-2.

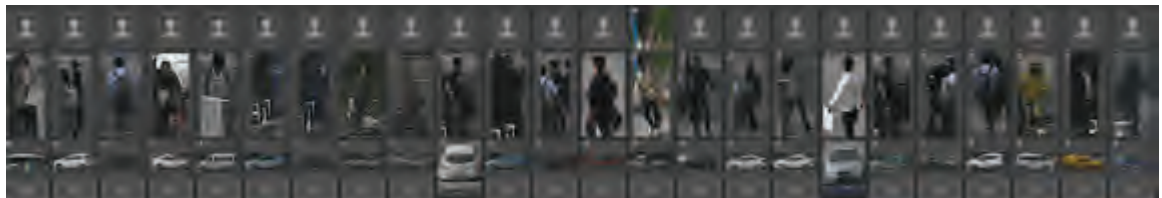
Figure 3-2 Information display of the detected targets



3.1.2 Snapshot Display Area

Display the snapshots of the detected targets. See Figure 3-3. 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

Display the number of the captured target in real time. See Figure 3-4.

Figure 3-4 Statistics area of the detected targets

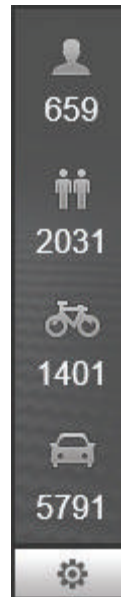


Table 3-2 Statistics area description of the detected targets

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	Available detection items: License plate, vehicle body color, vehicle type, vehicle logo, vehicle series, sunshield, seatbelt, smoking, calling, ornament, and annual inspection mark.  Up to 7 items can be selected at the same time for motor vehicle detection.
	Settings	Click the button to select the detection items.

3.2 AI Live Settings

Preparation

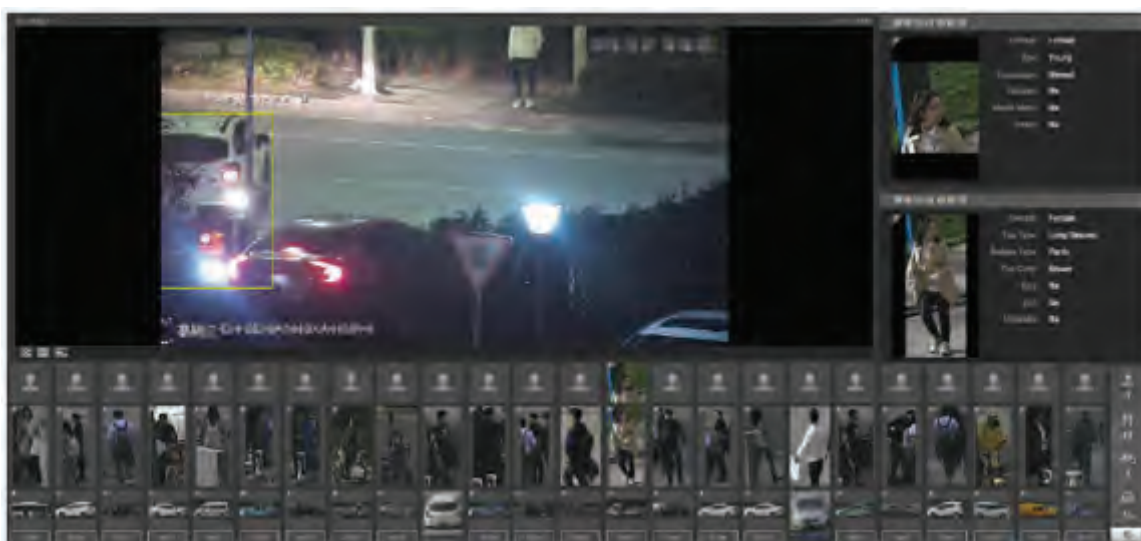
Select **Setting > Event > Smart Plan**, and then enable **Face Detection**, **Face Recognition** or **Video Metadata**. For the method to enable the function, see "5.4.4 Smart Plan.". For the operations, see "5.4.6 Face Recognition" or "5.4.9 Video Metadata."

Procedure

Step 1 Click the **AI Live** tab. The **AI Live** interface is displayed. See Figure 3-5. 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 interface



Step 2 Click  to set the detection items of the targets. See Figure 3-6.

Figure 3-6 Detection items selection interface



Step 3 Click  to complete the configuration

4 Playback

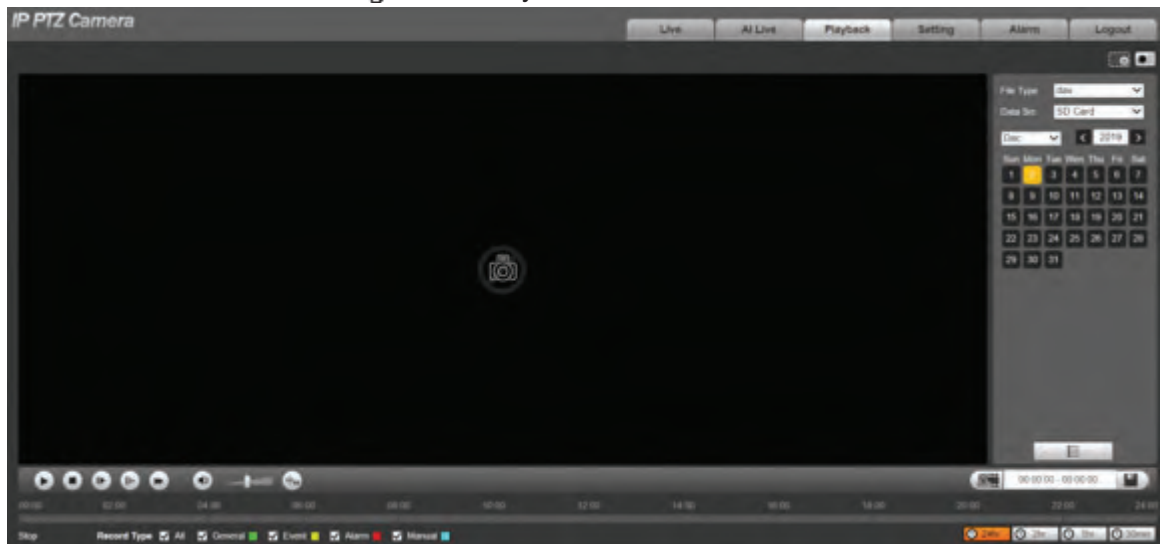
You can watch the saved pictures and videos on the **Playback** interface.



Before using the function, you need to set the period, storage method, and record control of recording and snapshot first. For details, see "5.5 Storage."

Click the **Playback** tab, and the **Playback** interface is displayed. See Figure 4-1.

Figure 4-1 Playback interface



4.1 Video Playback

Select **dav** from the **File Type** list, and the video playback interface is displayed. See Figure 4-2. For parameter description, see Table 4-1.

Figure 4-2 Video playback

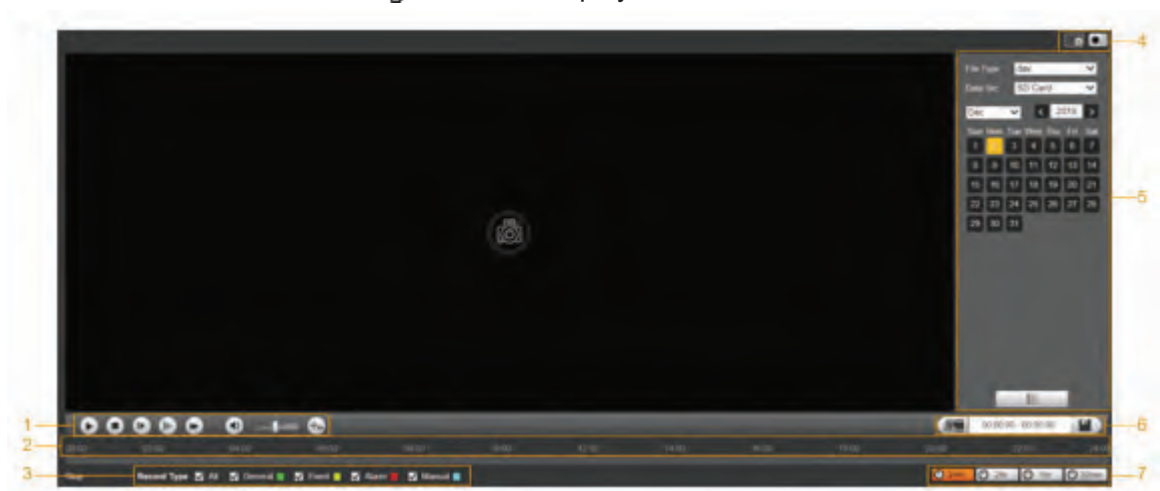


Table 4-1 Video playback parameter description

No.	Description
1	Video playing function bar
2	Progress bar

No.	Description
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

For the video playing function bar, see Figure 4-3. For the parameter description, see Table 4-2.

Figure 4-3 Video playing function bar



Table 4-2 Video play function bar description

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 interface 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. See Figure 4-4.

Figure 4-4 Recording Type



4.1.3 Auxiliary Functions

For the auxiliary functions, see Figure 4-5. For the parameter description, see Table 4-3.

Figure 4-5 Auxiliary functions



Table 4-3 Auxiliary functions parameter description

No.	Parameter	Description
1	Digital Zoom	- 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

There are videos and snapshots on days with blue shading. See Figure 4-6. For the parameter description, see Table 4-4.

Figure 4-6 Playback file (1)

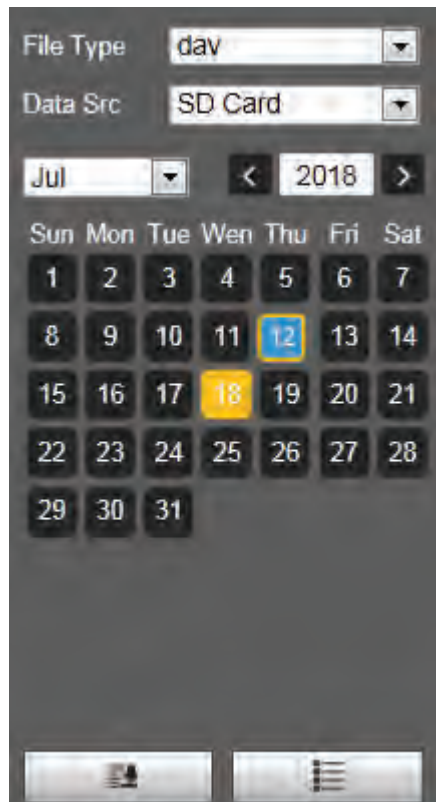
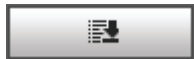


Table 4-4 Playback file parameter description (1)

Parameter	Description
File Type	- To play back a recording, select dav. - To play back a picture, select jpg.
Data Src	The SD Card is used by default.
	Click this button, and recordings or pictures of a certain type on specific dates can be downloaded in batch.  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.

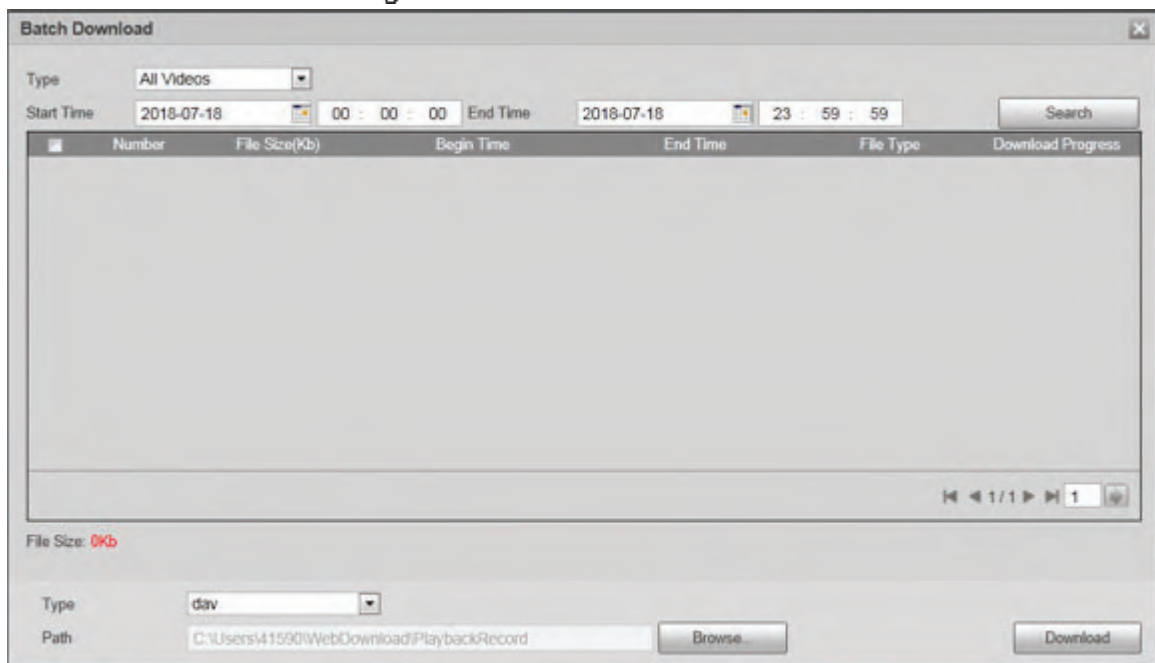
Download in Batches

Step 1 Click



The **Batch Download** interface is displayed. See Figure 4-7.

Figure 4-7 Batch download



Step 2 Configure parameters as needed. For the parameter description, see Table 4-5.

Table 4-5 Batch download parameters description

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/EndTime	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 click **Download**. The video files are downloaded and saved in the saving path.



You can select multiple files to download them.

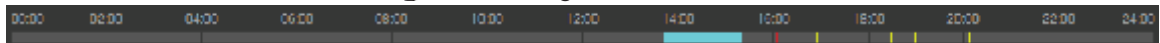
Displaying File List

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. For the progress bar, see Figure 4-8.

Figure 4-8 Progress bar



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

Step 4 For the playback file list, see Figure 4-9. For the parameter description, see Table 4-6. To play back a file in the list, double-click the file.

Figure 4-9 Playback file (2)

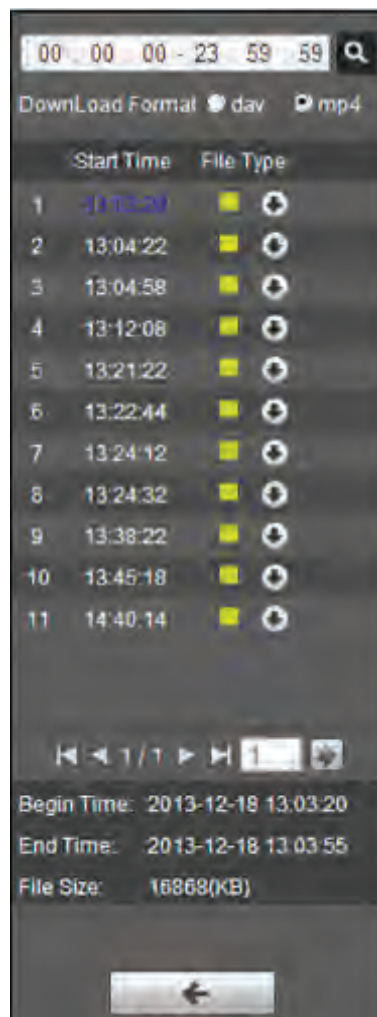


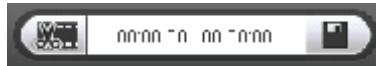
Table 4-6 Playback file parameter description (2)

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 .
	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 interface.

4.1.5 Video Clipping Area

You can clip the videos in this area. See Figure 4-10.

Figure 4-10 Video clipping



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

For the progress bar time format, see Figure 4-11. For the parameter description, see Table 4-7.

Figure 4-11 Progress bar time formats



Table 4-7 Progress bar time format description

Parameter	Description
	Click the button, and then the progress bar displays the recordings in 24-hour mode.
	Click the button, and then the video within the 2-hour period in which this video was recorded is displayed.
	Click the button, and then the video within the 1-hour period in which this video was recorded is displayed.
	Click the button, and then the video within the 30-minute period in which this video was recorded is displayed.

4.2 Picture Playback

Select **jpg** from the **File Type** list. For the picture playback interface, see Figure 4-12. For the parameter description, see Table 4-8.

Figure 4-12 Picture playback

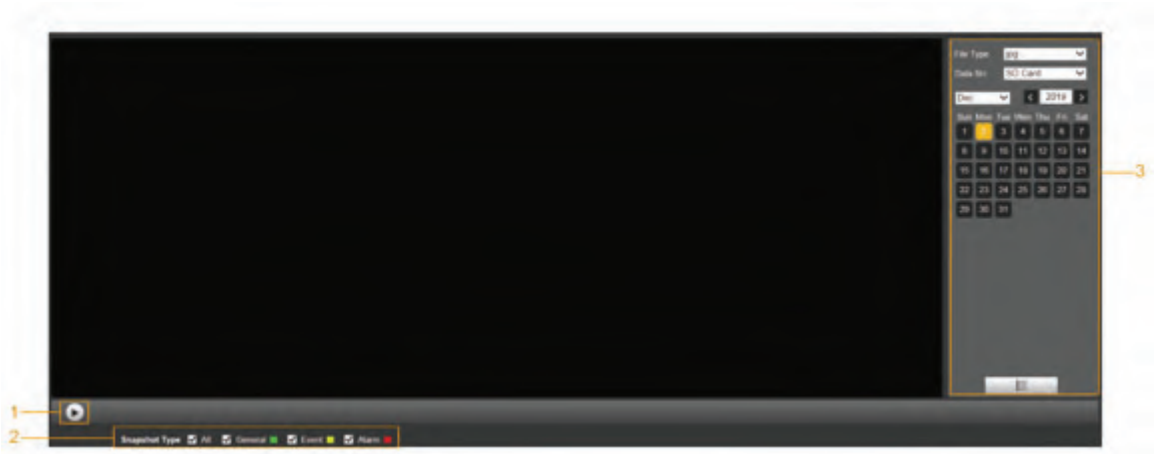


Table 4-8 Picture playback parameter description

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

4.2.1 Picture Playing Functions

For the picture playing buttons, see Figure 4-13.

Figure 4-13 Picture playing buttons



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

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

- To pause the picture play, click .

4.2.2 Picture Playback File Search and Display Area

For the playback file interface, see Figure 4-14 and Figure 4-15. For the description of buttons on the interface, see Table 4-9.

Figure 4-14 Playback file (1)

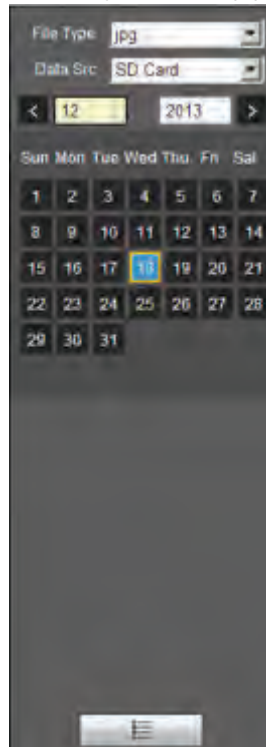


Table 4-9 Button description

Parameter	Description
File Type	Select jpg from the File Type list, and the picture will be played if any.
Data Src	The SD Card is used 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)



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. For the parameter description, see Table 4-10.

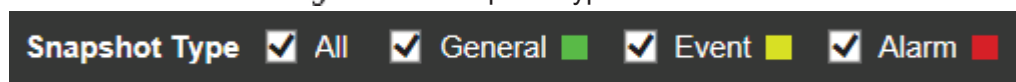
Table 4-10 Playback file parameter description

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 interface.

4.2.3 Snapshot Types

After you select a snapshot type, only the files of the selected type are displayed in the file list. For snapshot types, See Figure 4-16.

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

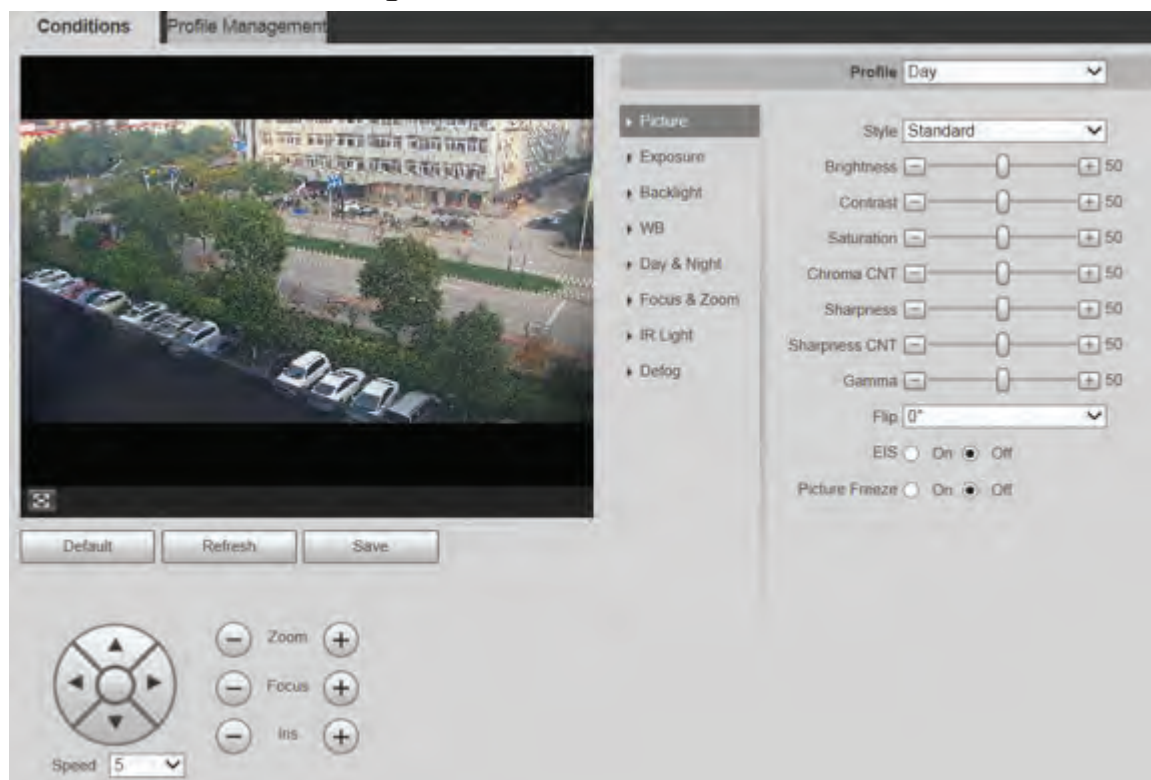
Picture

Set camera attributes and picture parameters to achieve the best display effect.

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

The **Picture** interface is displayed. See Figure 5-1.

Figure 5-1 Picture interface



Step 2 Configure parameters as needed. For parameter description, see Table 5-1.

Table 5-1 Picture setting parameter description

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.
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	The larger the value, the higher suppression on image colors. The value ranges from 0 to 100.  This parameter takes effect only when the Device is in the environment with low luminance.
Sharpness	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.  If the value is too large, there might be image noise. Set the value according to the actual condition.
Sharpness CNT	The larger the value is, the stronger the sharpness CNT will be. The value ranges from 0 to 100.  This parameter takes effect only when the Device is in the environment with low luminance.
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	Monitoring videos can be flipped over. There are two options. ● 0°: The monitoring video is normally displayed. It is 0° by default. ● 180°: The monitoring video is flipped over.
EIS	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.  ● 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**.

Exposure

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

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

The **Exposure** interface is displayed. See Figure 5-2 to Figure 5-6.

Figure 5-2 Exposure—auto mode

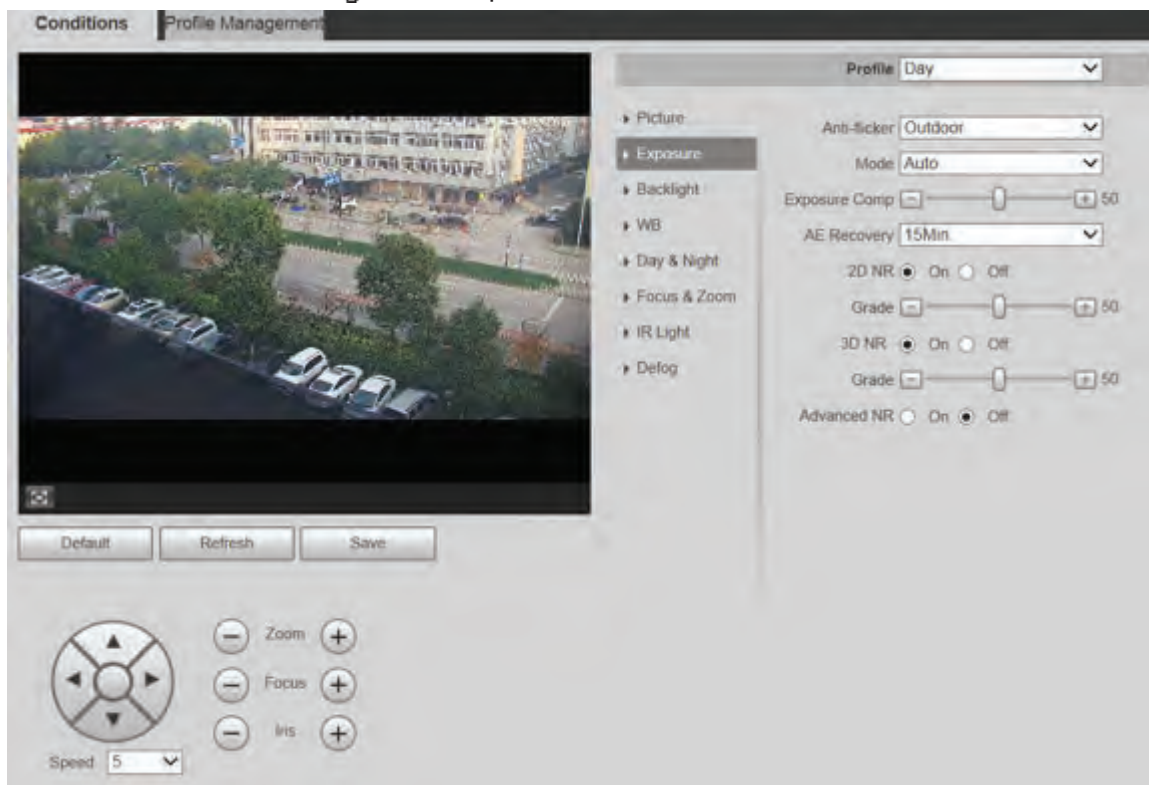


Figure 5-3 Exposure—aperture priority mode

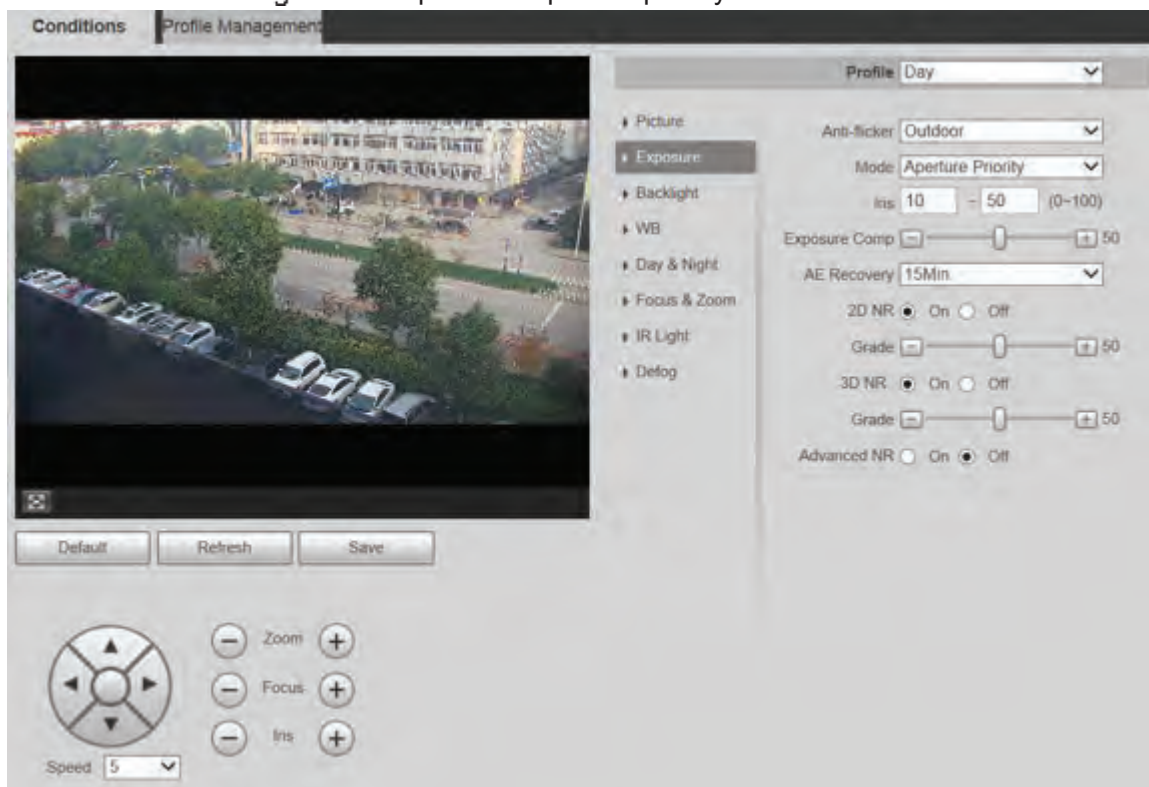


Figure 5-4 Exposure—shutter priority mode

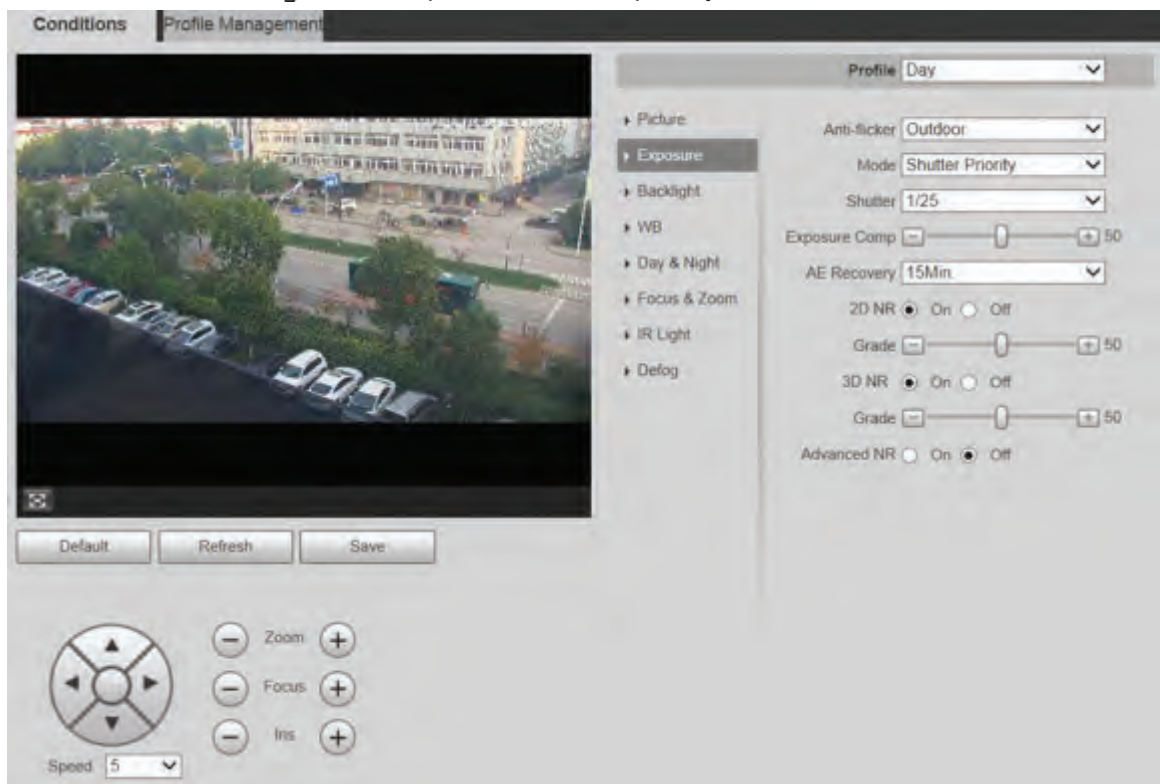


Figure 5-5 Exposure—gain priority mode

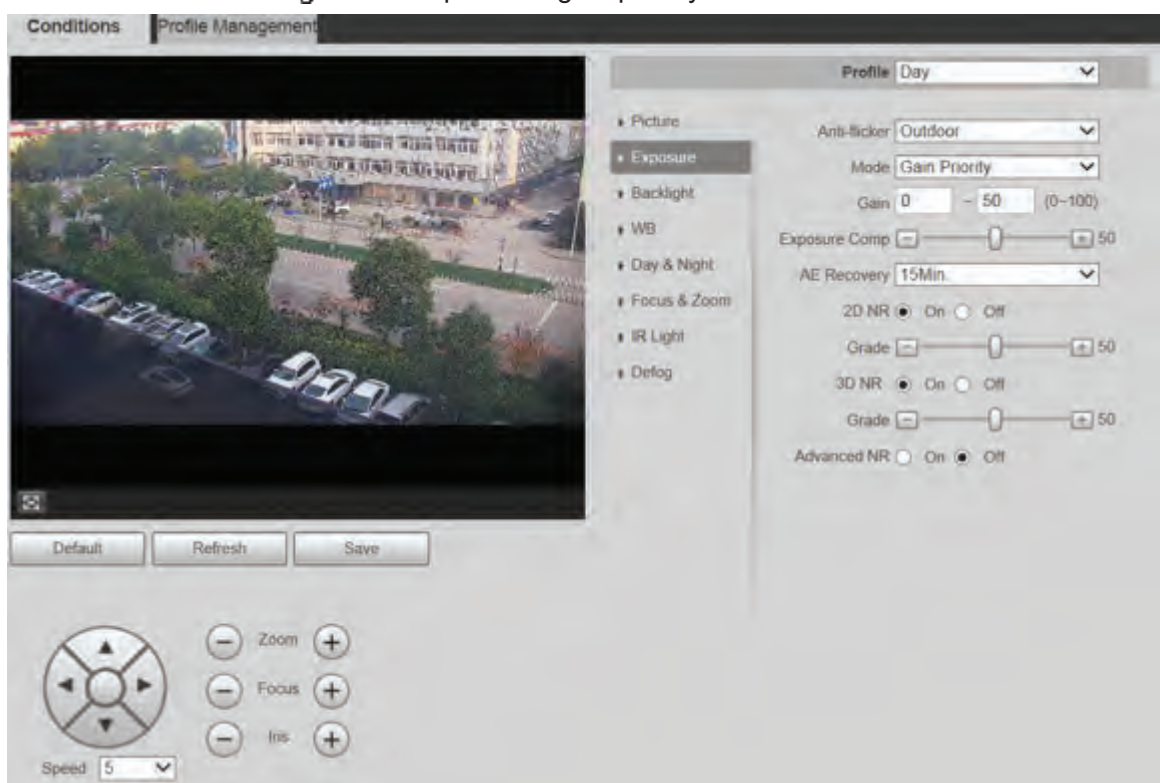
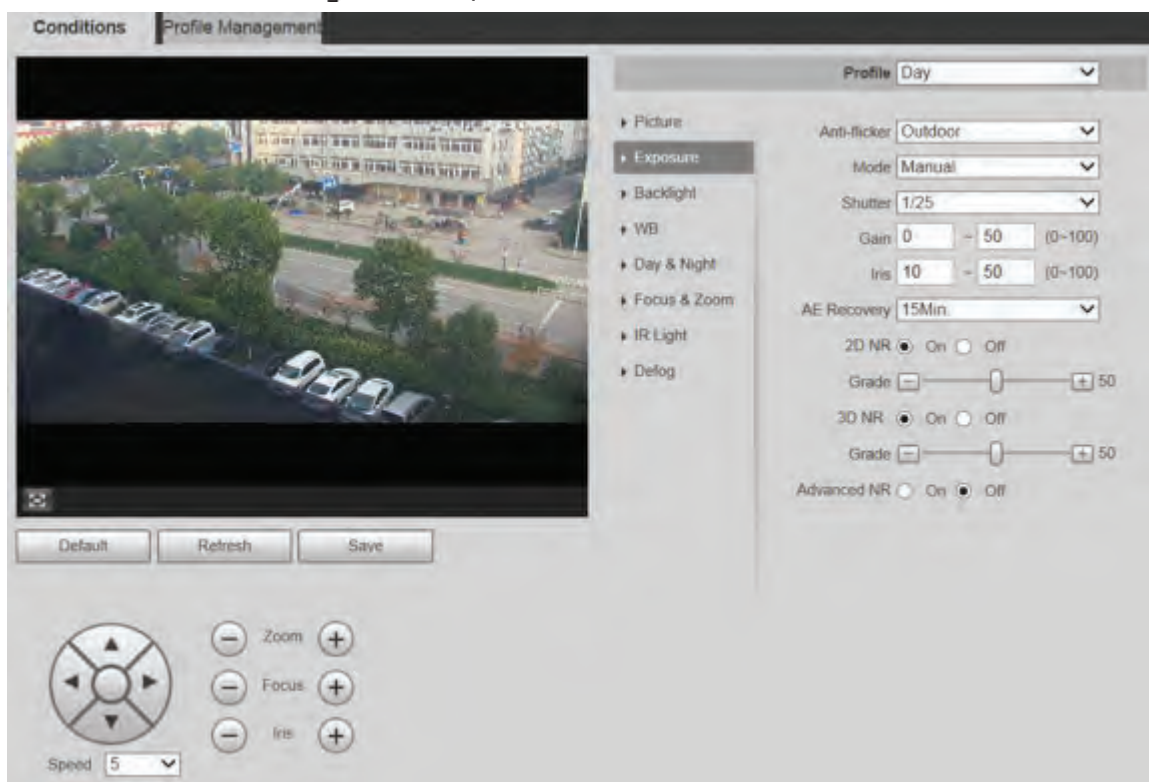


Figure 5-6 Exposure—manual mode



Step 2 Configure parameters as needed. For parameter description, see Table 5-2.

Table 5-2 Exposure setting parameter description

Parameter	Description
Anti-flicker	You can select 50Hz, 60Hz, or Outdoor from the list. ● 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	Set the exposure modes. You can select Auto, Manual, Aperture Priority, Shutter Priority, Gain Priority. The Auto mode is selected by default. ● 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.

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

Step 3 Click **Save**.

Backlight



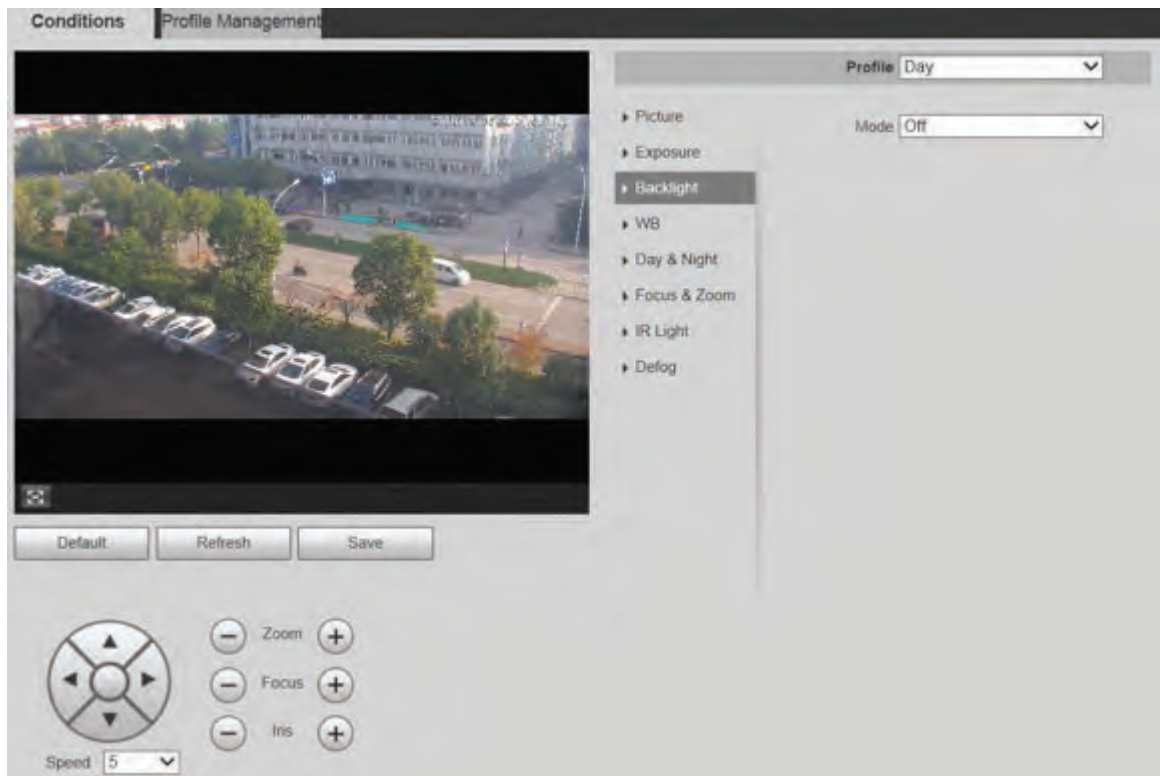
The backlight function cannot be configured if defog function is enabled. There will be a prompt on the interface.

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

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

The **Backlight** interface is displayed. See Figure 5-7.

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

Step 3 Click **Save**.



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

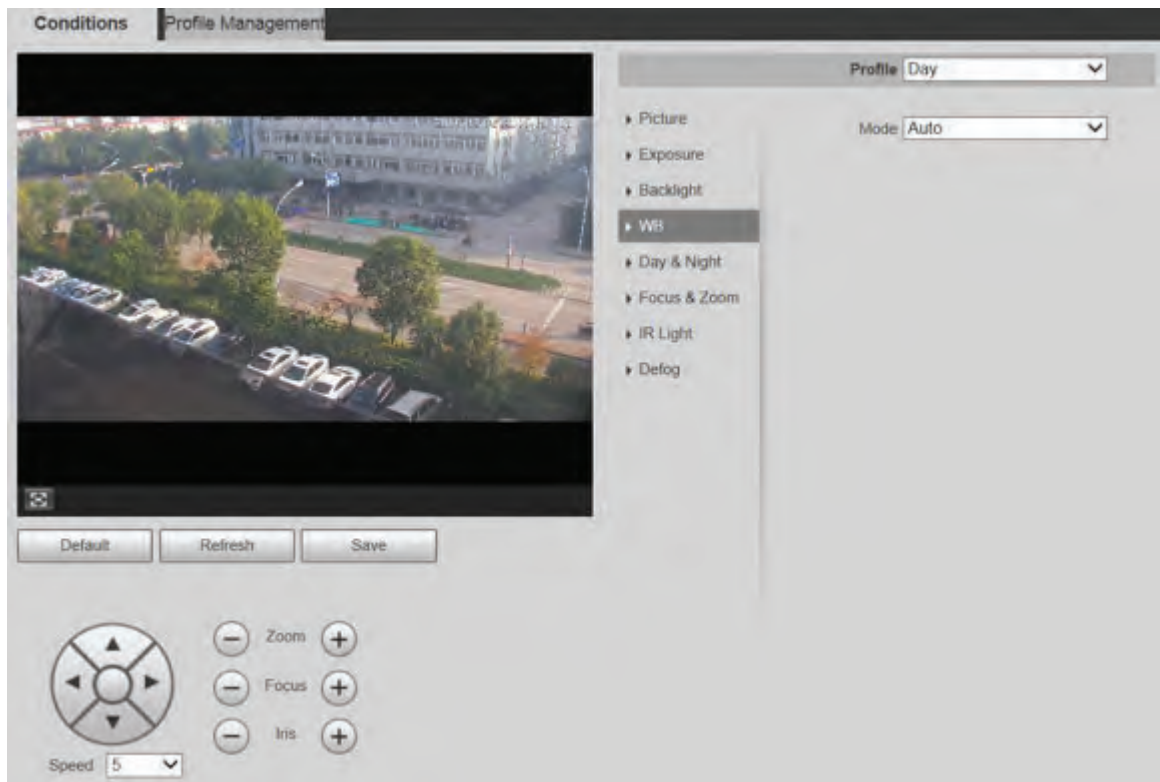
WB

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

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

The **WB** interface is displayed. See Figure 5-8.

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**.

Day & Night



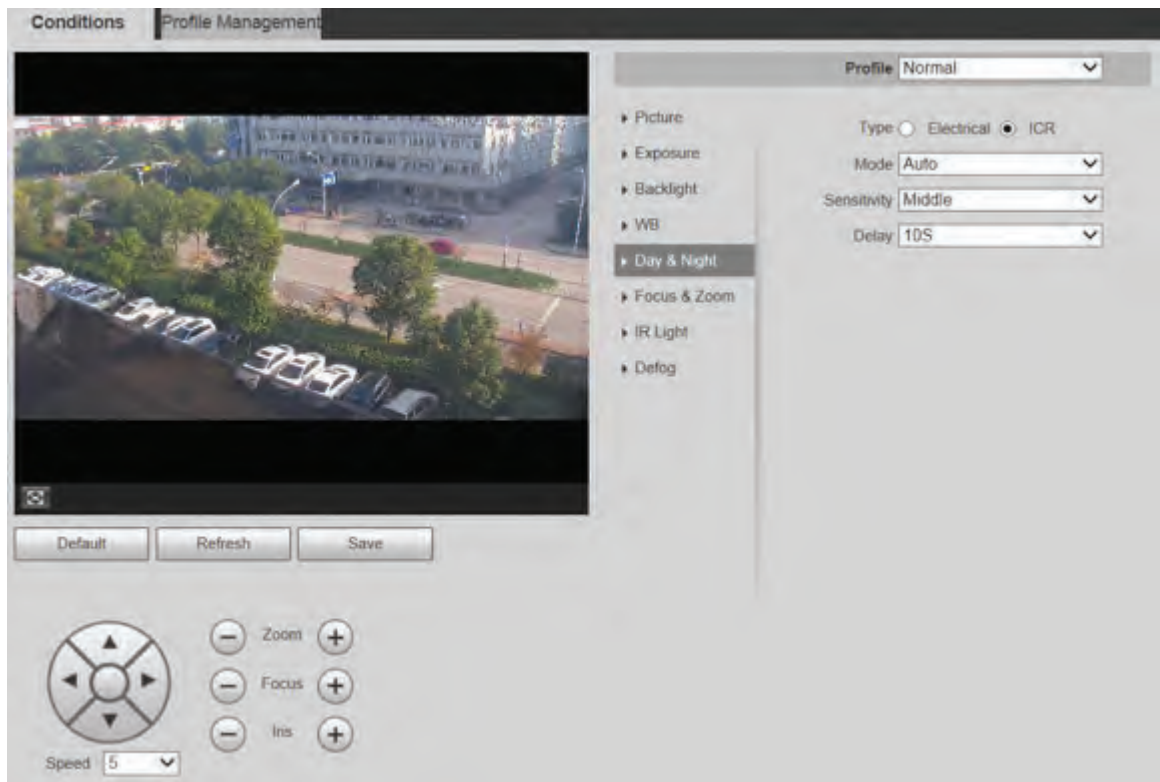
Defog function cannot be configured if **Day & Night** function is enabled. There will be a prompt on the interface.

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

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

The **Day & Night** interface is displayed. See Figure 5-9.

Figure 5-9 Day & night settings



Step 2 Configure parameters as needed. For parameter description, see Table 5-3.

Table 5-3 Day & night parameter description

Parameter	Description
Type	There are two options: Electrical and ICR . ICR is selected by default. - ICR: IR filter is used for day & night switch. - Electrical: Image processing method 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. 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 .  You can set sensitivity only when Day & Night mode is set to Auto.
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**.

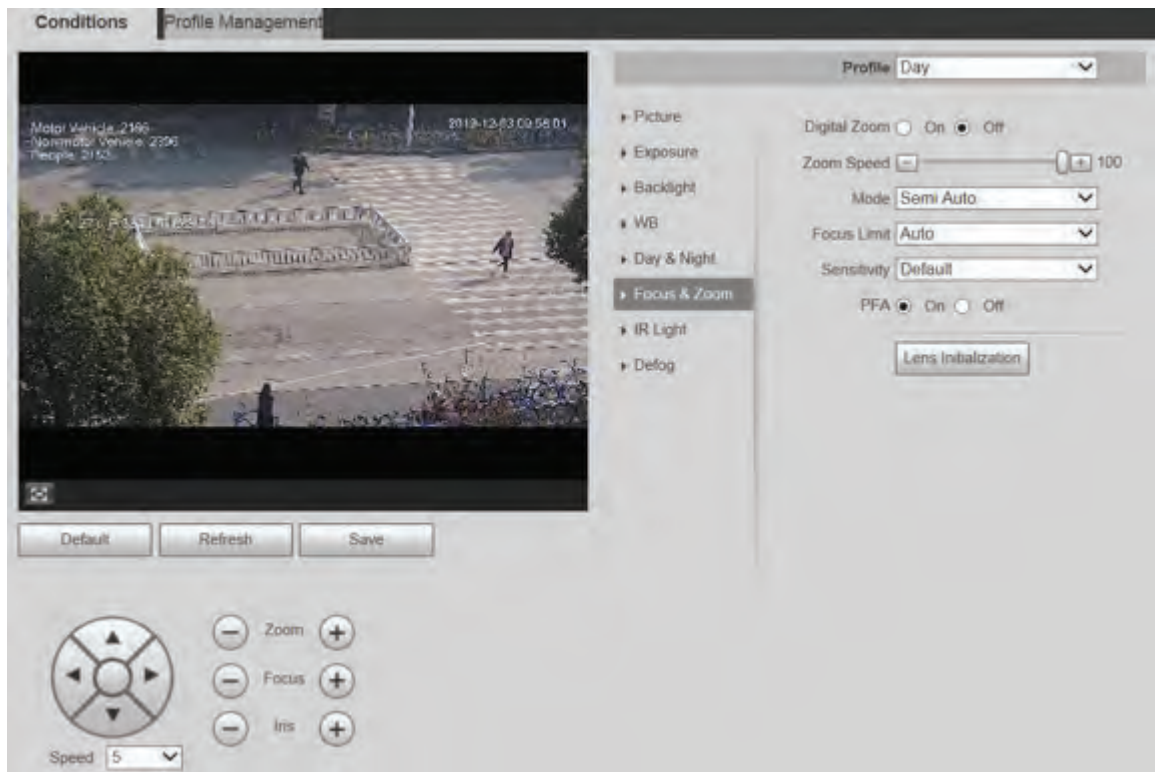
Focus & Zoom

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

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

The **Focus & Zoom** interface is displayed. See Figure 5-10.

Figure 5-10 Focus & zoom settings



Step 2 Configure each parameter as needed. See Table 5-4.

Table 5-4 Focus & zoom parameter description

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.
Mode	Select the focus triggering mode. There are three options: Semi Auto , Auto , and Manual . Semi Auto is selected by default. ● 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	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.
Sensitivity	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.
PFA	If you enable this function, the image is relatively clear during zoom. If you disable this function, the speed is relatively high during zoom.

Parameter	Description
Lens Initialization	Click this button, and the lens will be initialized automatically. The lens will be extended to calibrate the zoom and focus.

Step 3 Click **Save**.

IR Light

Common illuminators are classified into infrared IR lights, white lights, and laser lights. Different device models support different types of illuminators, and have different configuration interfaces. The actual interface shall prevail. This section describes how to configure these light types.

Infrared IR Light/White Light

These are the conditions for using infrared 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, infrared 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 infrared IR light is turned on; in **Color** mode, the white light is turned on.



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

Perform the following steps to set illuminators.

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

The **IR Light** interface is displayed. See Figure 5-11.

Figure 5-11 IR light settings—ZoomPrio

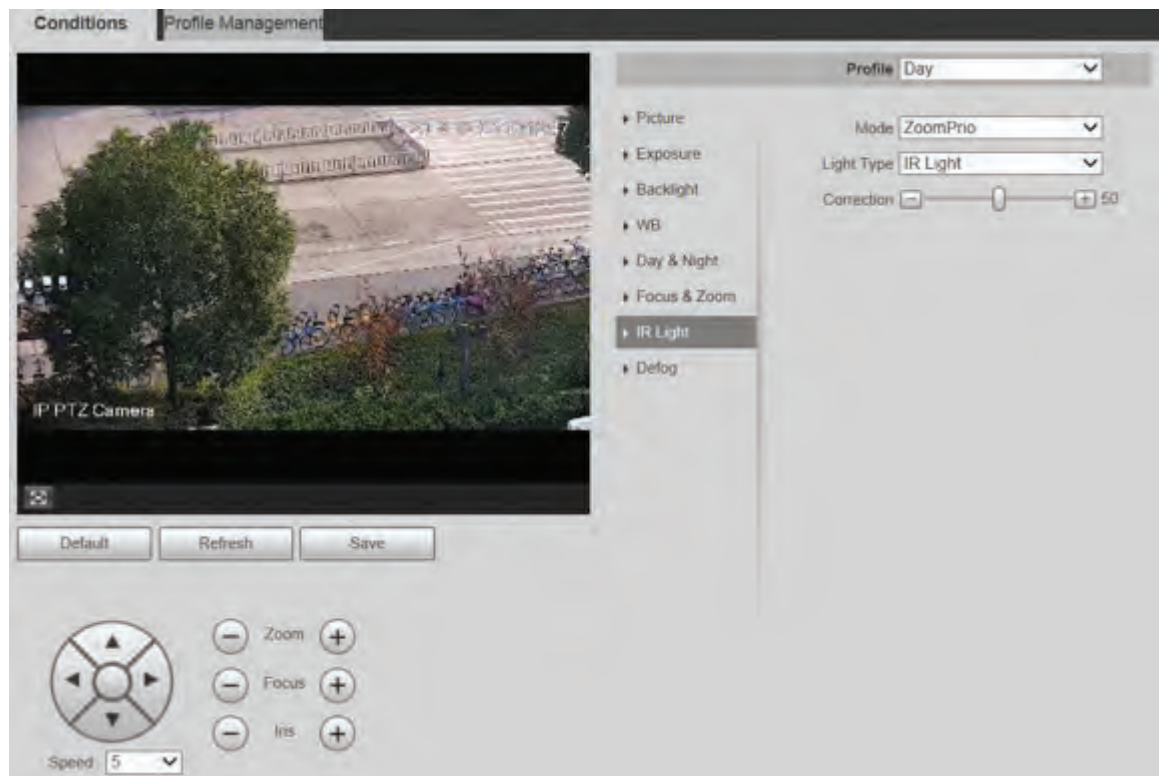


Figure 5-12 IR light settings—SmartIR

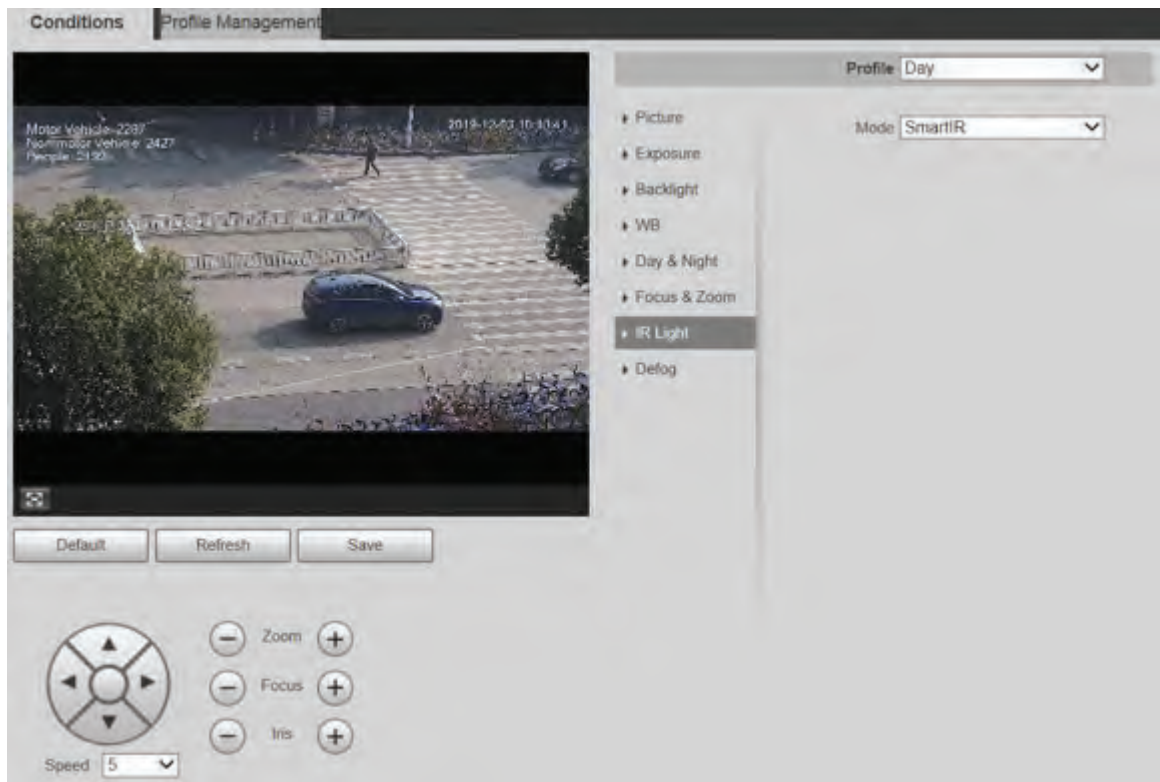


Figure 5-13 IR light settings—manual

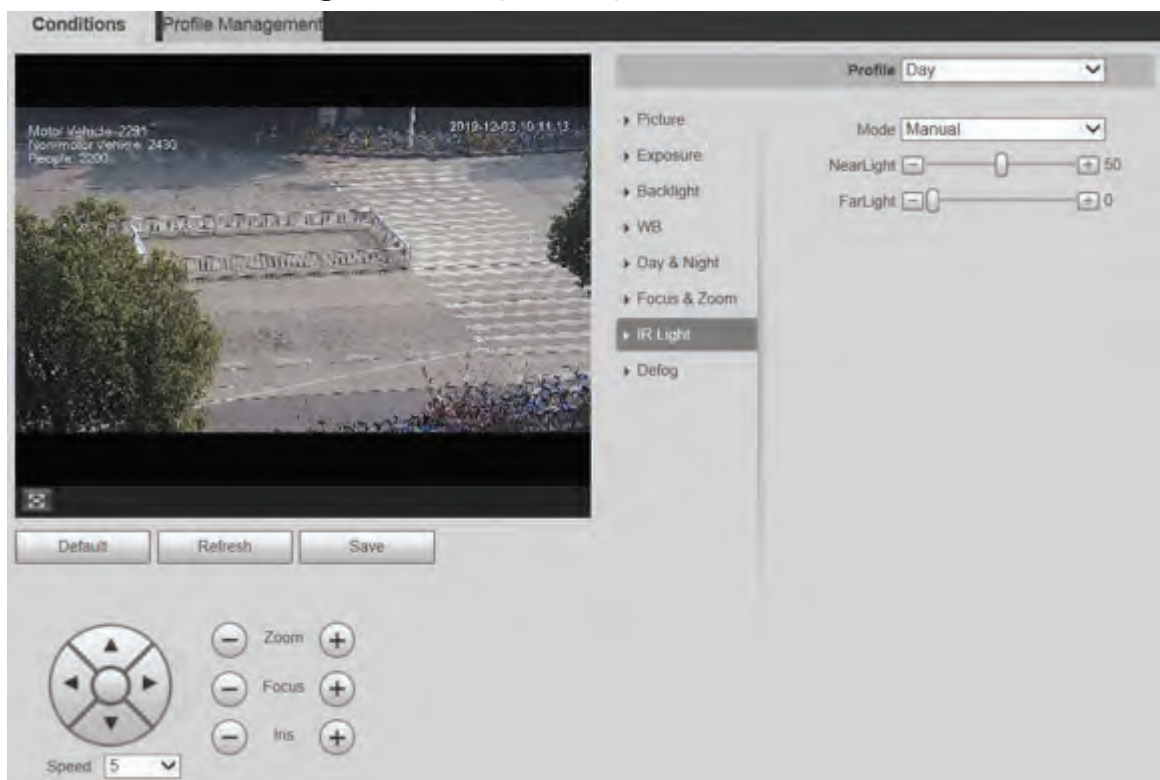


Figure 5-14 IR light setting—timing

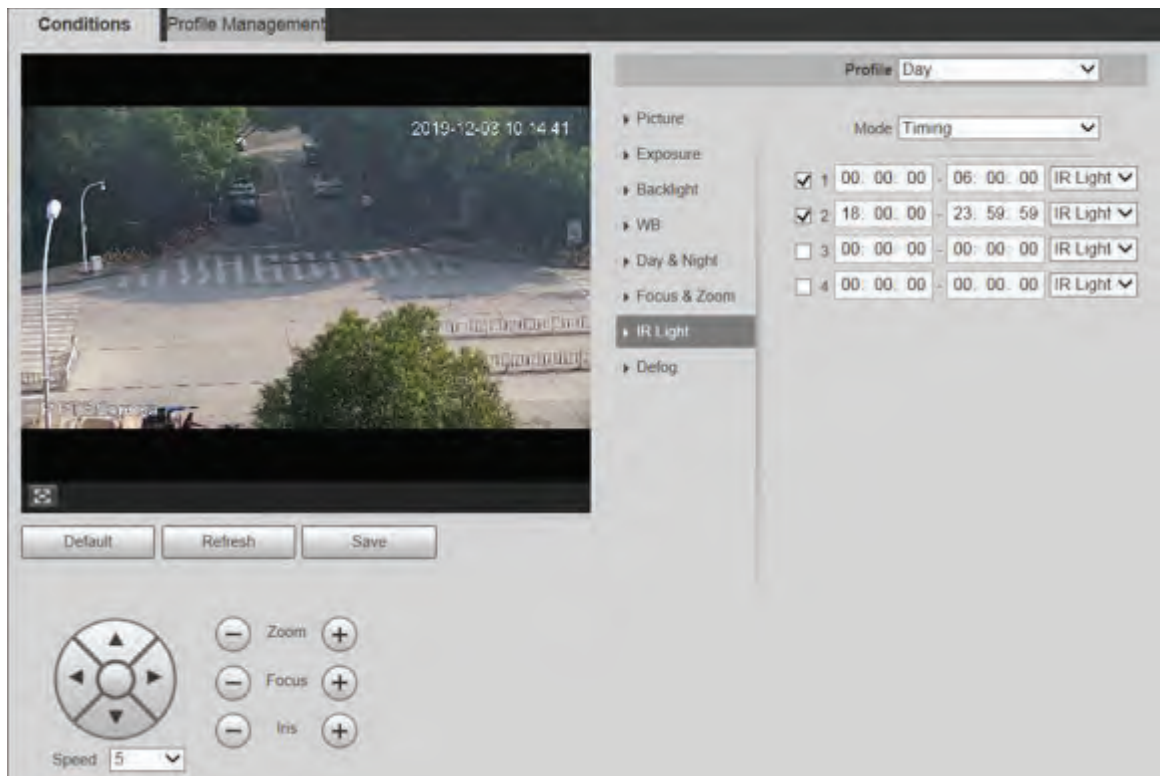
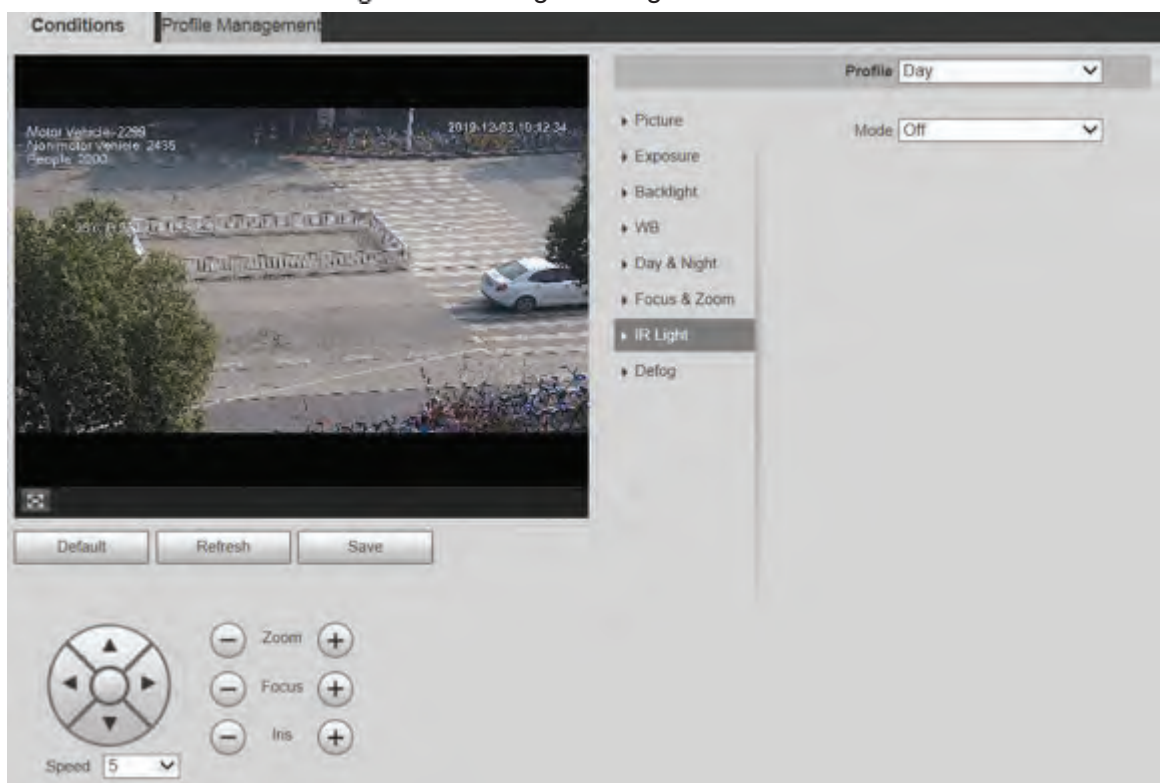


Figure 5-15 IR light setting—off



Step 2 Configure each parameter as needed. For the parameter description, see Table 5-5.

Table 5-5 IR light parameter description

Parameter	Description
Mode	There are 5 options: Manual, SmartIR, ZoomPrio, Timing, and Off. ● ZoomPrio: The system adjusts the IR light brightness automatically according to the zoom times. ● SmartIR: The system controls the IR light intensity according to actual

Parameter	Description
	conditions. ● Manual: Set IR light brightness manually. ● Timing: Enable different light types in different time periods according to actual condition. ● Off: Turn off the IR light.  ● Some models do not support SmartIR, Manual, Timing, or Off. ● In ZoomPrio mode, IR light and white light are supported, and IR light is selected by default. ● In Timing mode, you can set four periods with different light types. ● Only infrared IR light supports the SmartIR mode. ● The IR light is turned off for cameras with low power consumption by default. Turn on the IR light if necessary.
Light Type	You can select IR Light or White Light .
Correction	Compensate for the brightness of the IR light. The value ranges from 0 to 100.
Near Light	Set the brightness of the near light. The value ranges from 0 to 100.
Far Light	Set the brightness of the far light. The value ranges from 0 to 100.

Step 3 Click **Save**.

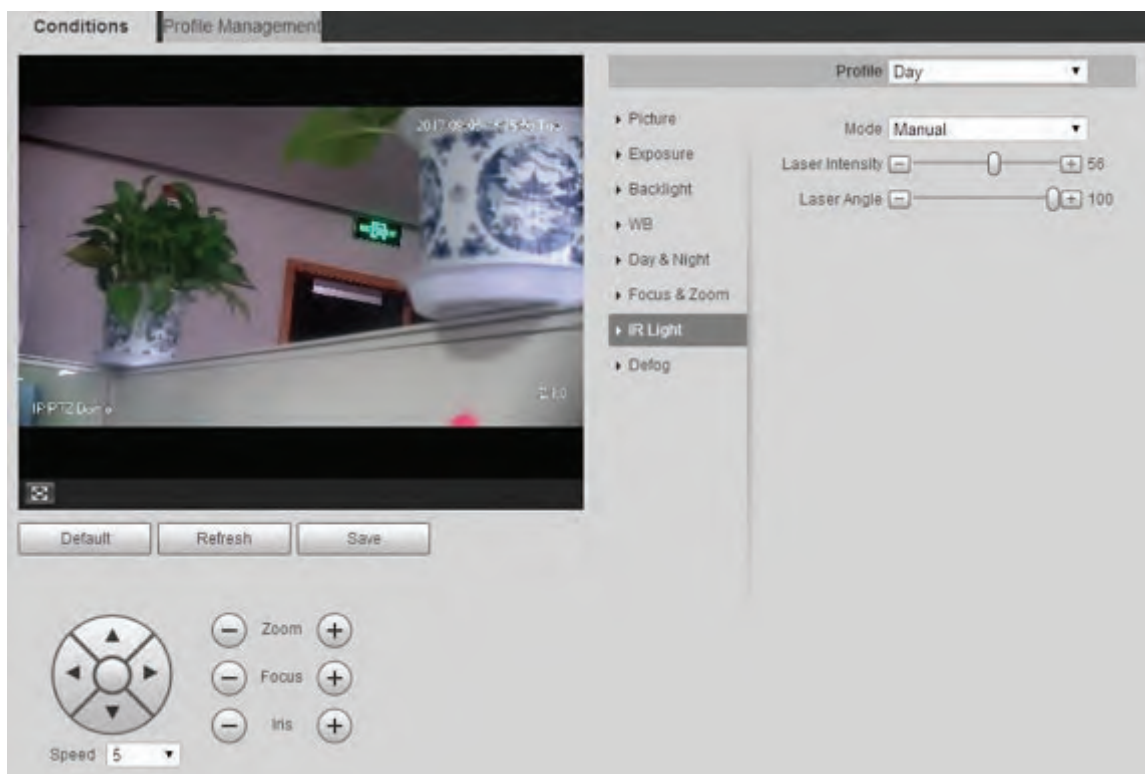
Laser Light

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

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

The **IR Light** interface is displayed. See Figure 5-16.

Figure 5-16 Laser light settings



Step 2 Configure parameter as needed. Refer to Table 4-6 for more details.

Table 5-6 Laser light setting parameter description

Parameter	Description
Mode	Select the laser light mode from ZoomPrio and Manual. It is ZoomPrio by default. ● 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**.

Defog



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

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

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

The **Defog** interface is displayed. See Figure 5-17 and Figure 5-18.

Figure 5-17 Defog settings—manual

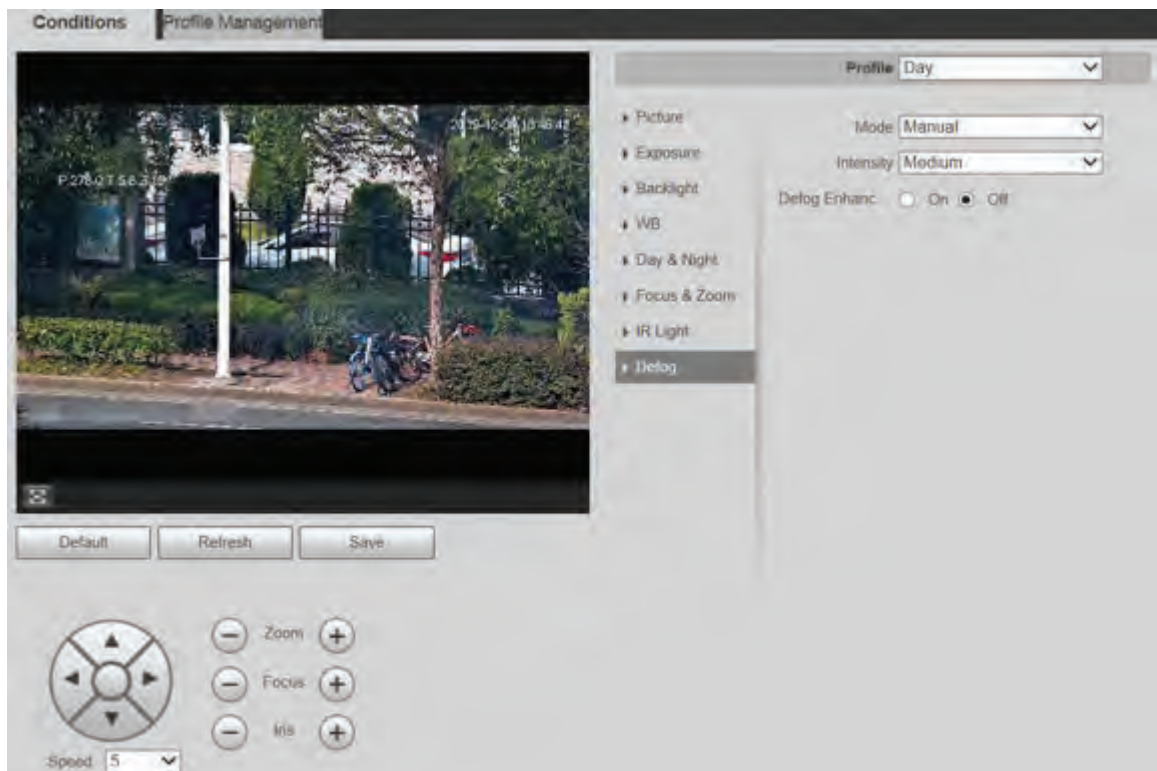
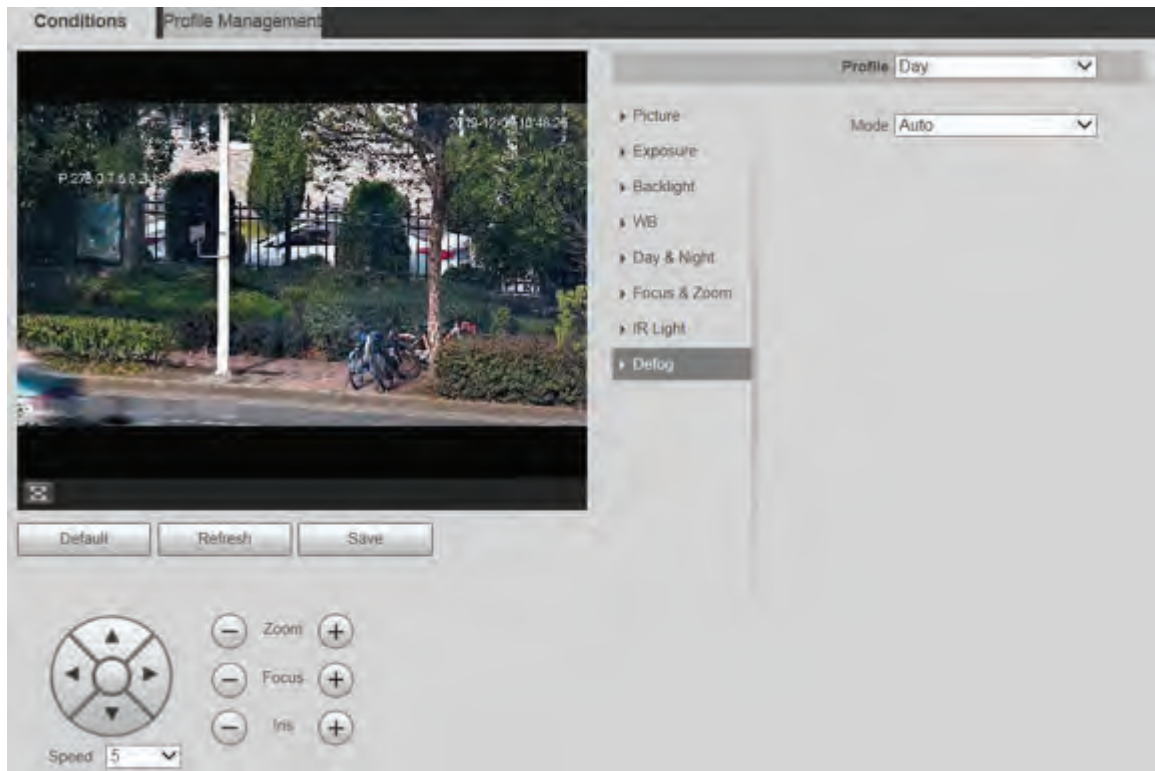


Figure 5-18 Defog settings—auto



Step 2 Configure parameters as needed. For parameter description, see Table 5-7.

Table 5-7 Defog parameter description

Parameter	Description
Mode	Select the defog mode of the Device. You can select Auto, Manual, or Off. It is Off by default.  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.
Intensity	Set the defog intensity of the Device. You can select from Low, Medium, or High.
Defog Enhancement	 Only the Device that supports optical defog has this parameter. 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.)

Step 3 Click **Save**.

5.1.1.2 Profile Management

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

The **Profile Management** interface is displayed.

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. See Figure 5-19.

Figure 5-19 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. See Figure 5-20.

Figure 5-20 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 is a dropdown menu labeled 'Always Enable' with 'Day' selected. Below the dropdown 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 the configuration interface, see Figure 5-21. 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 5-21 Profile management—schedule

The screenshot shows the 'Profile Management' tab selected. Under 'Profile Management', the 'Schedule' radio button is selected. Below the radio buttons is a 'Period setting' section with a timeline from 0:00 to 24:00. A yellow bar indicates the 'Day' period from 6:00 to 18:00. Below the timeline 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

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

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

The **Video** interface is displayed. See Figure 5-22.

Figure 5-22 Video stream settings



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

Step 2 Configure parameters as needed. For parameter description, see Table 5-8.

Table 5-8 Video stream parameter description

Parameter	Description
Enable	You can select the check box 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	Enable Smart Codec to improve video compressibility and save storage space.  After Smart Codec is enabled, the Device does not support the third stream, ROI, smart event, and other functions. The actual interface shall prevail.
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	There are two options: CBR (constant bit rate) and VBR (variable bit rate). - Picture 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.
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.

Parameter	Description
Watermark Settings	You can verify the watermark to check if the video has been tampered.
Watermark Character	You can verify the watermark to check if the video has been tampered. Select Watermark Settings check box to enable Watermark Character. The watermark character is DigitalCCTV by default, and you can modify it.  Watermark character consists of up to 128 characters from letters, standard symbols, spaces, and special characters.

Step 3 Click **Save**.

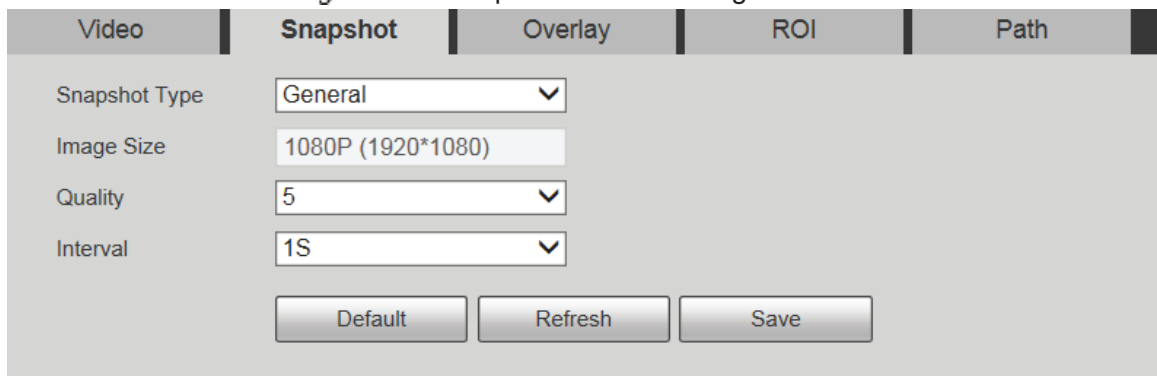
5.1.2.2 Snapshot

This section describes how to set streams for snapshots.

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

The **Snapshot** interface is displayed. See Figure 5-23.

Figure 5-23 Snapshot stream settings



Step 2 Configure parameters as needed. For parameter description, see Table 5-9.

Table 5-9 Snapshot stream parameter description

Parameter	Description
Snapshot Type	You can select General or Event. ● General refers to capturing pictures within the time range set in the schedule. For details, see "5.5.1 Schedule." ● Event means capturing pictures when motion detection, video tampering, or local alarms are triggered. For how to enable snapshots for motion detection, video tampering, or local alarms, see "5.4 Event Management."
Image Size	It is the same as the resolution of the selected snapshot main stream, and cannot be modified on this interface.
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

This section describes how to set the overlay information on the monitoring screen.

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

The **Overlay** interface is displayed.

Step 2 Configure overlay information as needed. For the configuration interfaces, see the following figures. For the parameter description, see Table 5-10.

Figure 5-24 Overlay settings—privacy masking

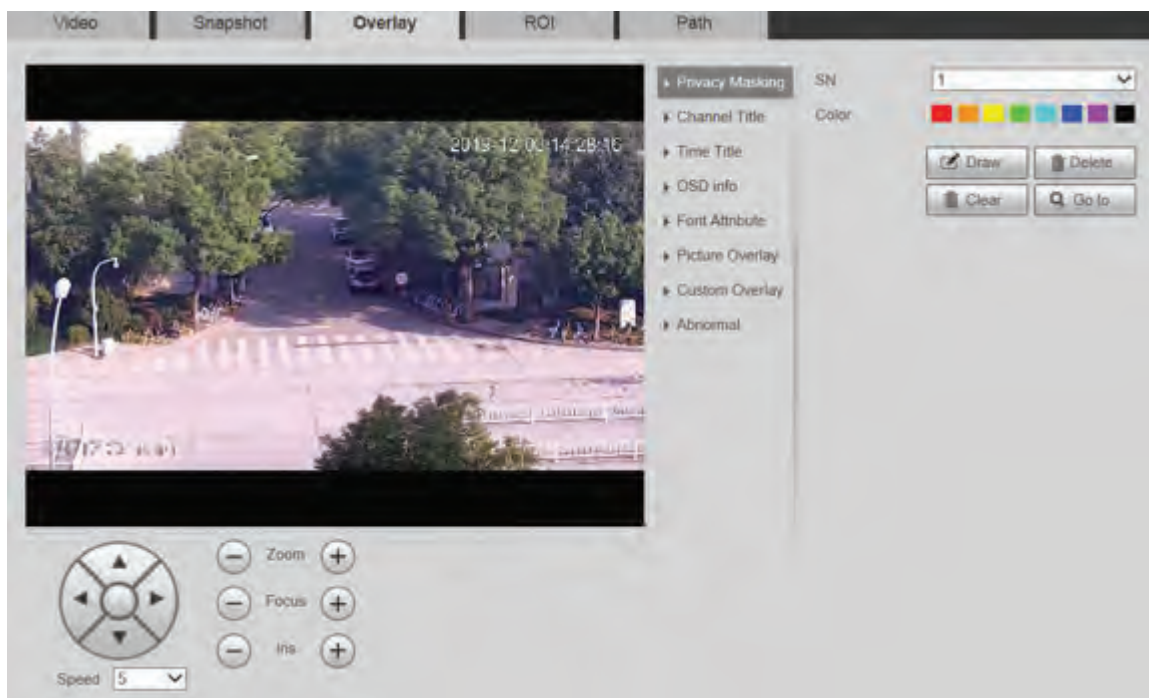


Figure 5-25 Overlay settings—channel title

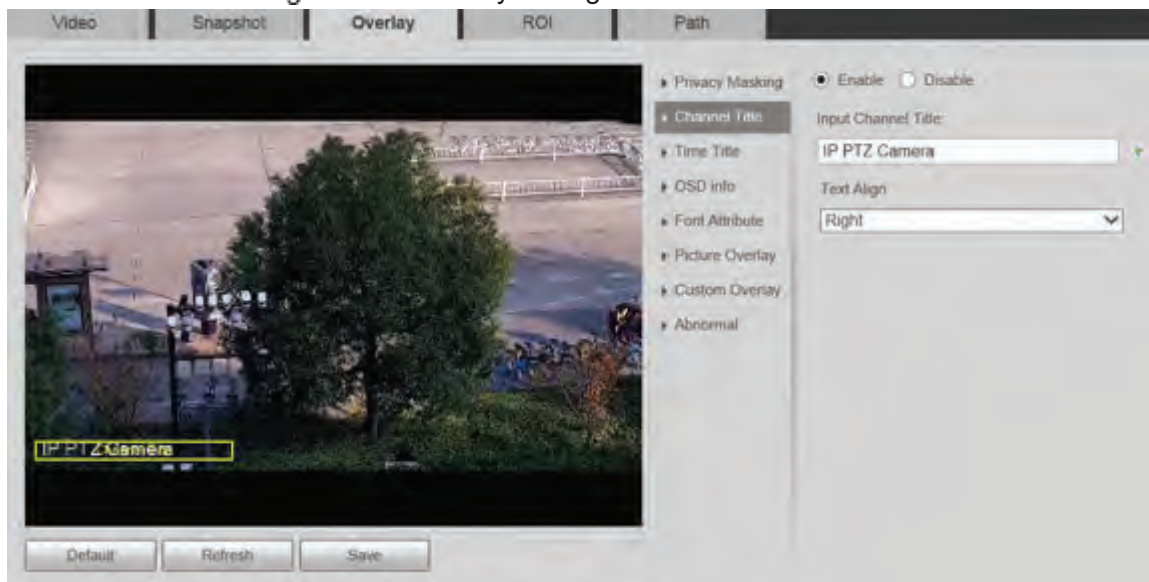


Figure 5-26 Overlay settings—time title

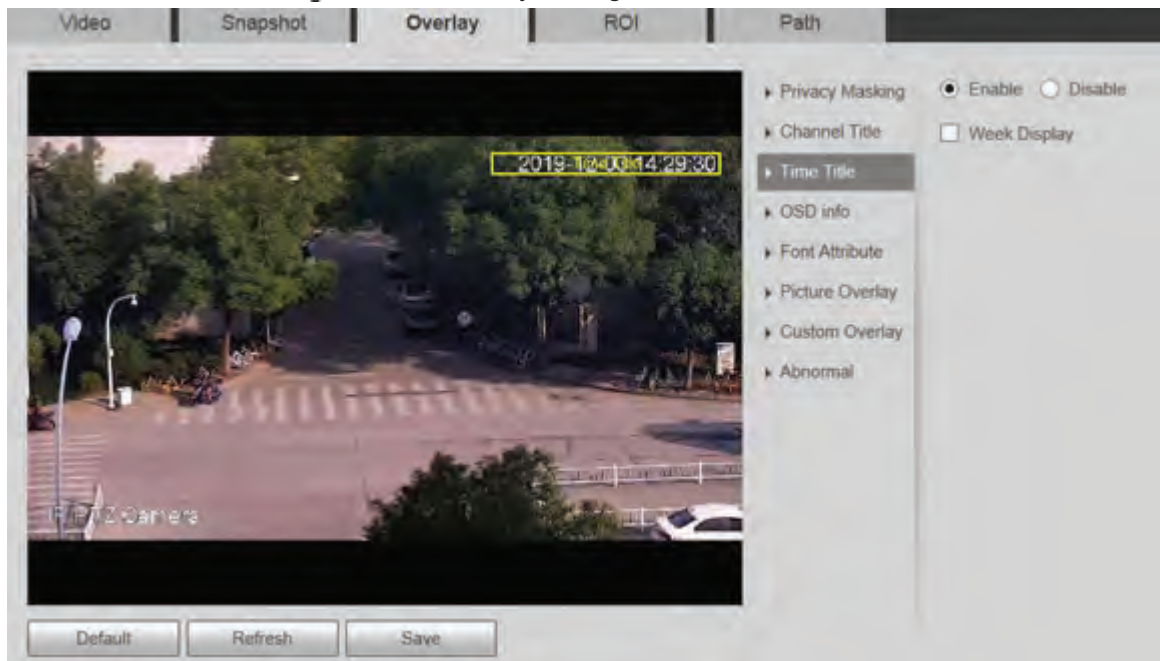


Figure 5-27 Overlay settings—OSD info

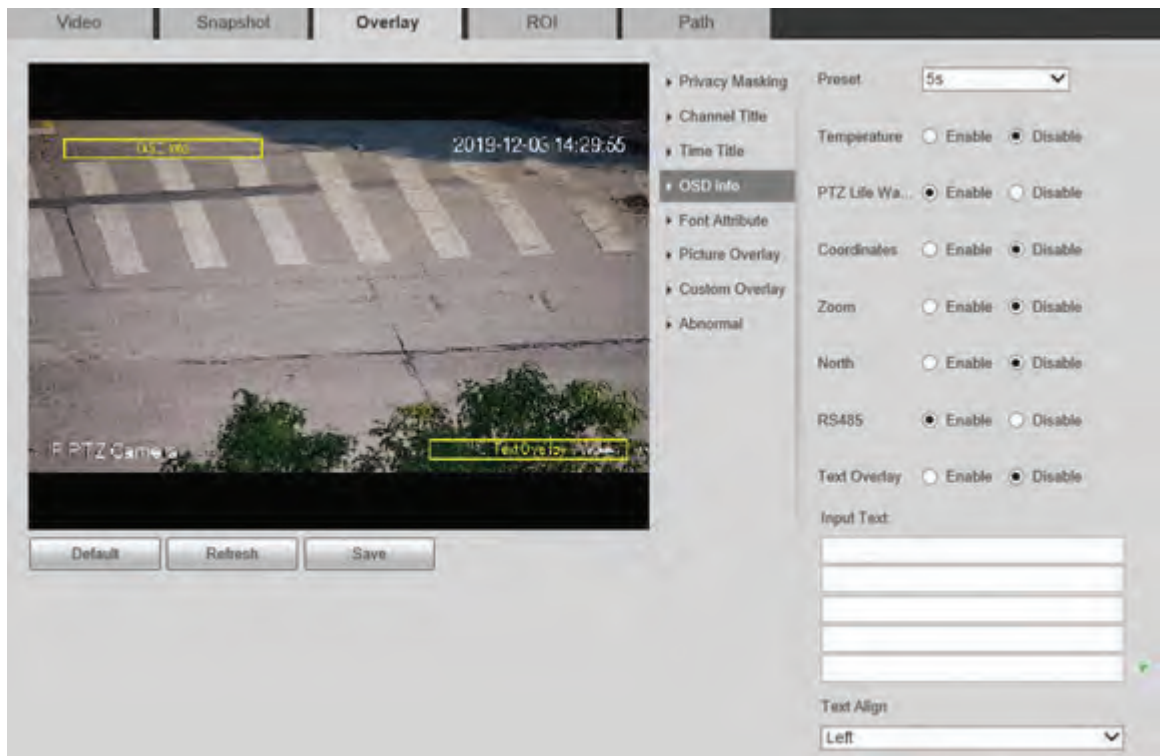


Figure 5-28 Overlay settings—font attribute

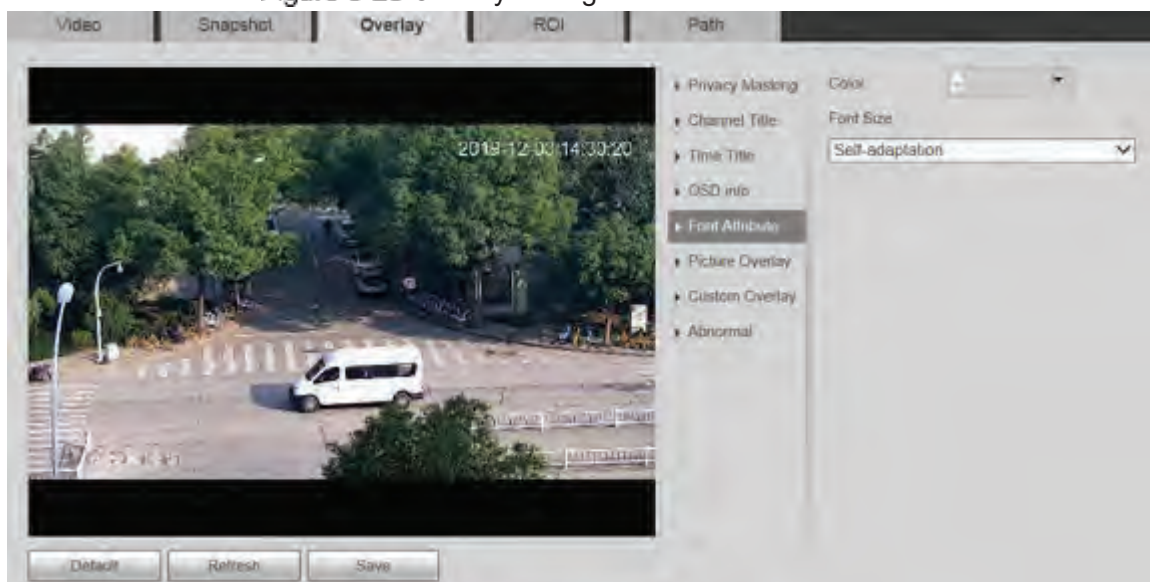


Figure 5-29 Overlay settings—picture overlay

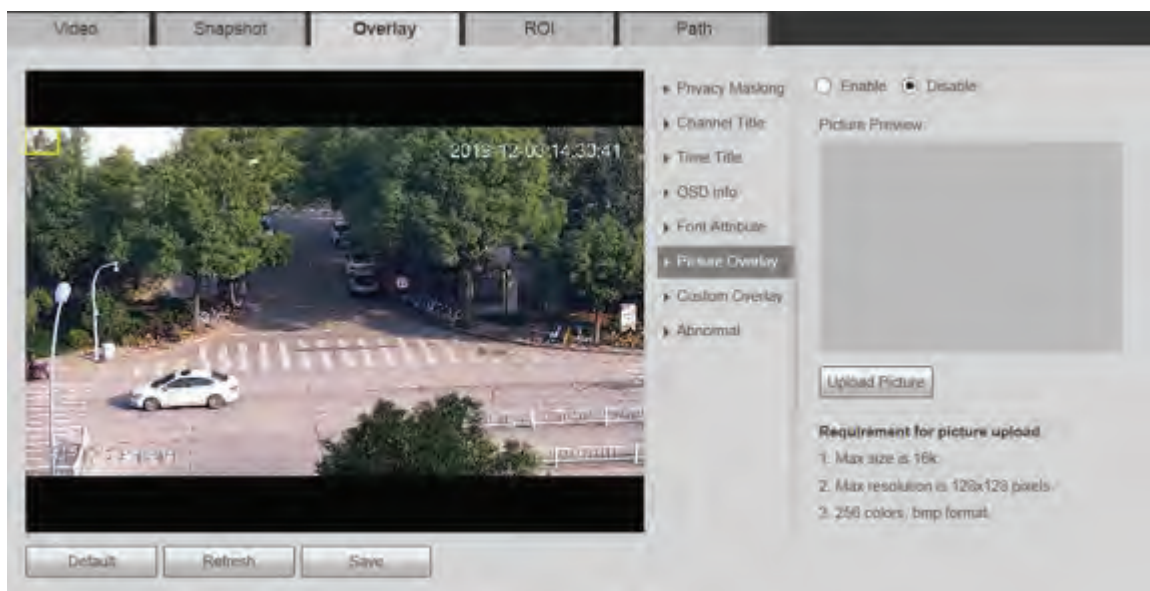


Figure 5-30 Overlay settings—abnormal

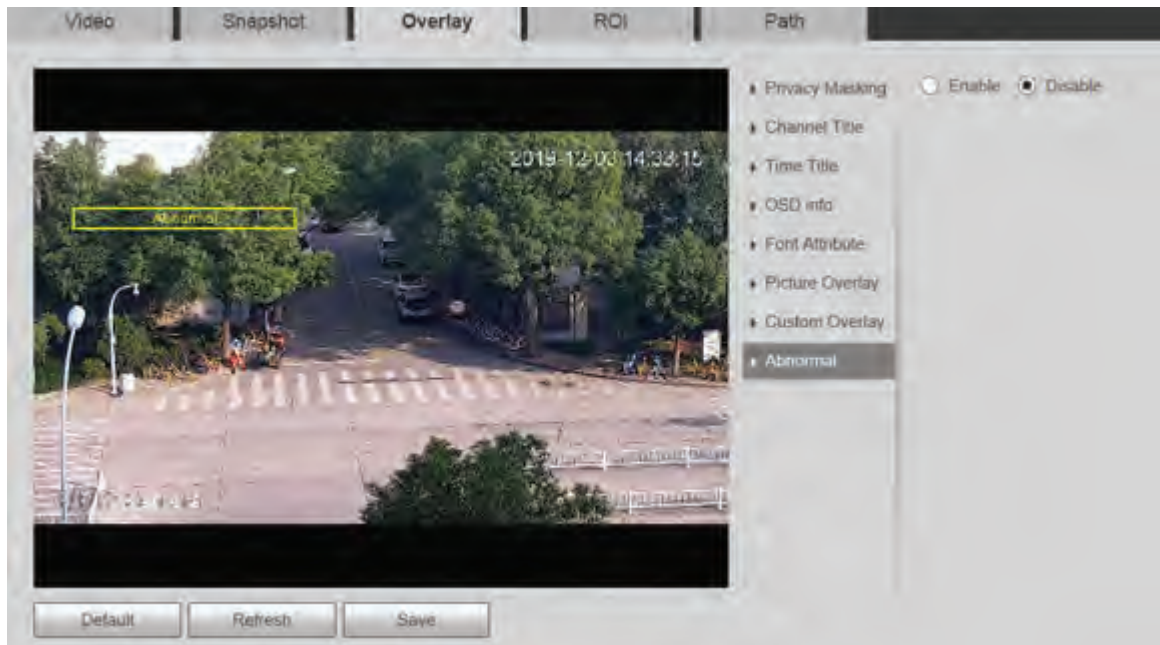


Figure 5-31 Overlay settings—GPS position



Figure 5-32 Overlay settings—custom overlay

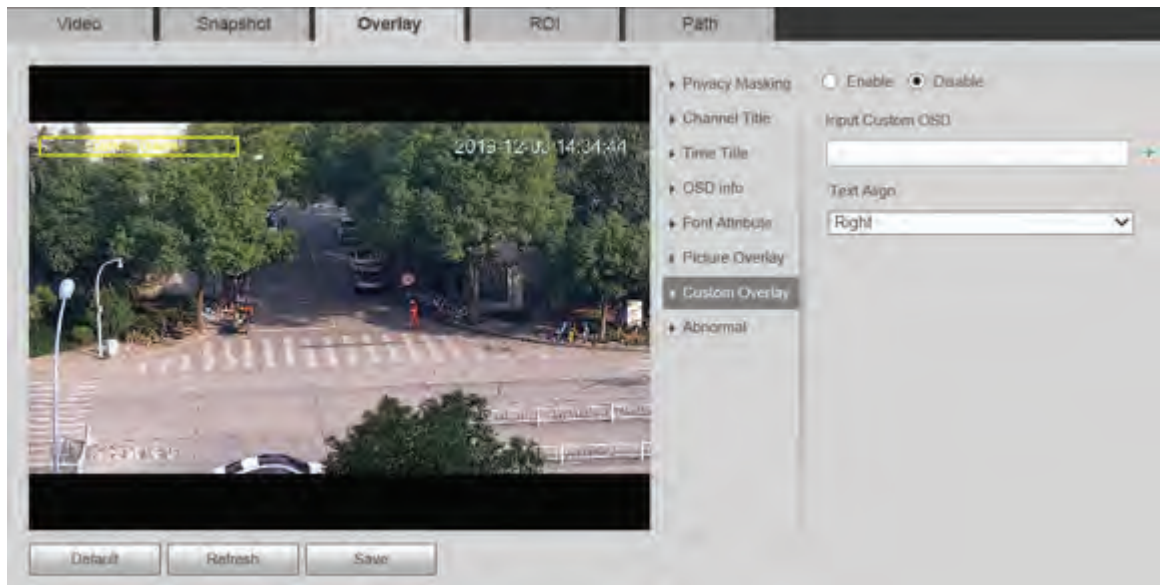


Table 5-10 Overlay setting parameter description

Parameter	Description
Privacy Masking	Privacy masking refers to setting a certain region in the monitoring screen to protect privacy. ● To draw a privacy mask in the live view, click Draw. ● To delete a privacy mask, click Delete. ● To clear all privacy masks, click Clear. You can set the number, type and color of the privacy mask. To view a privacy mask, click Go to.
Channel Title	Set whether to display the channel title on the monitoring screen. You can adjust the channel title location by dragging the box. Click  to add a channel title. You can also select the Text Align of the channel title.
Time Title	Set whether to display time on the monitoring screen, and you can select whether to display the week. You can adjust the time title location by dragging the box.

Parameter	Description
OSD info	If you want to display preset title, temperature, PTZ life warning, coordinates, zoom, north direction, RS485, and other information on the monitoring screen, you can set OSD info. ● Preset: Set the duration of the preset title displaying on the screen. You can select from Disable, 5s, 15s, Display Permanently, and Custom. ● Temperature: Select the Enable check box, select the temperature unit, and then the internal temperature of the Device is displayed. ● PTZ Life Warning: When the PTZ lifespan is close to the threshold, a warning will be displayed on the Live interface. This OSD info is enabled by default. ● Coordinates/Zoom/North/RS485/Text Overlay: Select the Enable check box to display the corresponding OSD info on the screen.  ● You can adjust the OSD info location by dragging the box. ● There are two options for alignment of text overlay: Left and Right.
Font Attribute	Set the font of the channel title, time title, and OSD info, and you can also set the color and size of the font.
Picture Overlay	Set whether to display the overlaid picture on the monitoring screen. Click Upload Picture to overlay local pictures on the monitoring screen. You can adjust the location of an overlaid picture by dragging the yellow box.  Geographic location and picture overlay cannot be both enabled.
Abnormal	Set whether to display abnormality information on the monitoring screen.
Custom Overlay	Add custom OSD information on the monitoring screen. Click  to add one line of custom OSD information. You can also select the Text Align of the channel title.

Step 3 Click **Save**.

5.1.2.4 ROI



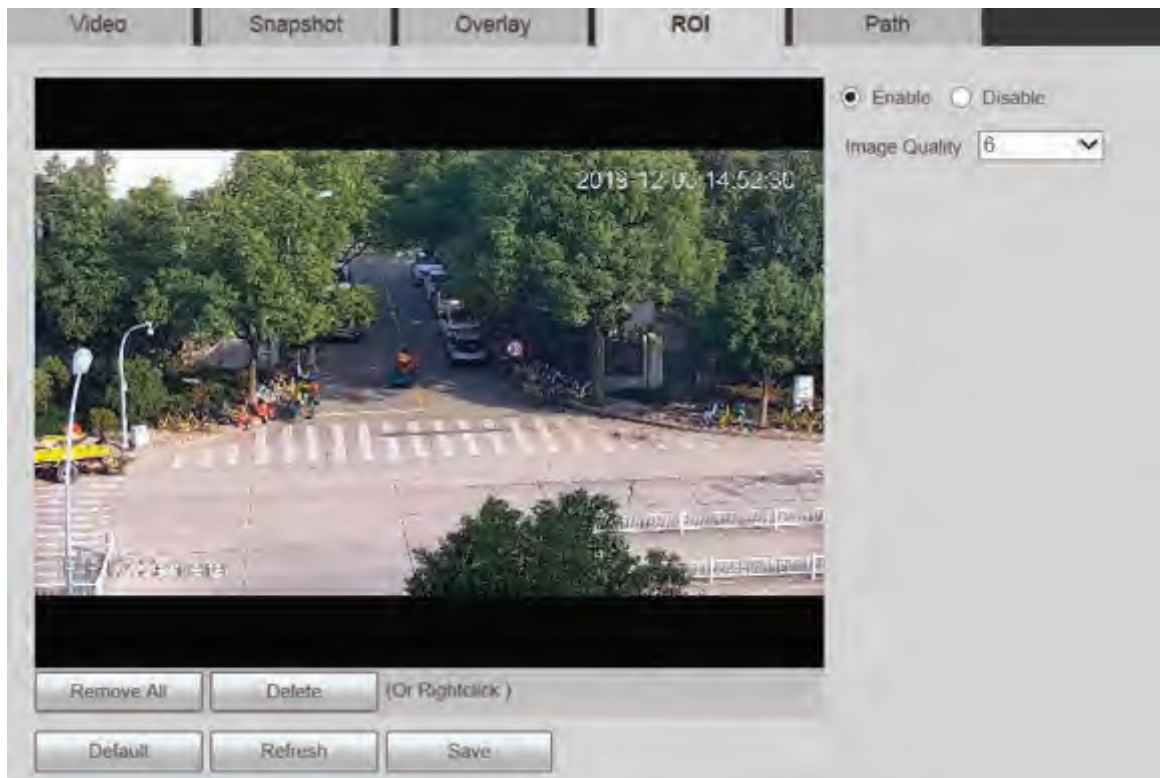
ROI is available on select models.

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

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

The **ROI** interface is displayed. See Figure 5-33.

Figure 5-33 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

The storage path is associated with the snapshot and recording on the **Live** interface. 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** interface. You can set the path of **Playback Snapshot**, **Playback Download**, and **Video Clips** respectively.

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

The **Path** interface is displayed. See Figure 5-34.

Figure 5-34 Path settings

	Video	Snapshot	Overlay	ROI	Path
Live Snapshot		C:\Users\admin\WebDownload\LiveSnapshot			Browse...
Live Record		C:\Users\admin\WebDownload\LiveRecord			Browse...
Playback Snapshot		C:\Users\admin\WebDownload\PlaybackSnapshot			Browse...
Playback Download		C:\Users\admin\WebDownload\PlaybackRecord			Browse...
Video Clips		C:\Users\admin\WebDownload\VideoClips			Browse...

Default Save

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.



admin is the login account.

Step 3 Click **Save**.

5.1.3 Audio



This function is available on select models.

5.1.3.1 Audio

Set audio parameters of the Device.

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

The **Audio** interface is displayed. See Figure 5-35.

Figure 5-35 Audio settings

Audio

Encode

Main Stream

☐ Enable

Encode Mode: G.711A

Sampling Frequency: 8000

Sub Stream

☐ Enable

Sub Stream 1

Encode Mode: G.711A

Sampling Frequency: 8000

Attribute

AudioIn Type: LineIn

Noise Filter: Disable

Microphone Volume: 50

Speaker Volume: 50

Default Refresh Save

Step 2 Configure parameters as needed. For parameter description, see Table 5-11.

Table 5-11 Audio setting parameter description

Parameter	Description
Enable	Enable Main Stream or Sub Stream, and then the network stream contains both audio and video; otherwise, it is only video stream.  Audio can be enabled only when video has been enabled.
Encode Mode	The audio encoding modes include G.711A, G.711Mu, G726, PCM, MPEG2-Layer2, G.722.1, G.729, and AAC. It is G.711A by default.  The audio encoding mode set here applies to both audio streams and voice talks.
Sampling Frequency	The supported sampling frequencies include 8000, 16000, 32000, 48000, and 64000.  The sampling frequency varies depending on the encoding mode. Select an encoding mode as needed.
AudioIn Type	Set the audio input type. You can select LineIn or Mic .
Noise Filter	Set whether to enable noise filter. The function is enabled by default.

Parameter	Description
NR (Noise Reduction) Level	Adjust the noise reduction level from 0 to 100.  This parameter takes effect when noise filter is enabled.
Microphone Volume	Adjust the microphone volume from 0 to 100.
Speaker Volume	Adjust the speaker volume from 0 to 100.

Step 3 Click **Save**.

5.2 Network Settings

5.2.1 TCP/IP

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



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.

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

The **TCP/IP** interface is displayed. See Figure 5-36.

Figure 5-36 TCP/IP settings

Step 2 Set TCP/IP parameters. For details, see Table 5-12.

Table 5-12 TCP/IP parameter description

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.
Mode	Static and DHCP modes are available. - 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	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.

Parameter	Description	
	 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.	
Default Gateway	Configure as needed. The default gateway must be in the same network segment as the IP address.	 For IPv6 version, in the IP Address, Default Gateway, Preferred DNS, and Alternate DNS fields, enter 128 bits, and these fields cannot be blank.
Preferred DNS	IP address of the DNS server.	
Alternate DNS	Alternate IP address of the DNS server.	
MTU	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.  Here are some suggested value for your reference. 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.	
Enable ARP/Ping to set IP address service	Select the check box, and then you can modify and set the device IP address through ARP/Ping command if the MAC address is known. 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**.

An Example of Configuring IP Address with ARP/Ping

Step 1 To obtain a usable IP address, make sure that the Device and your PC are in the same LAN.

Step 2 Get the MAC address from the Device label.

Step 3 Open command editor on the PC and enter the following command. See Table 5-13.

Table 5-13 Command lists

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</pre>

System	Command
	ping -l 480 -t 192.168.0.125
UNIX/Linux/Mac syntax	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
Win7 syntax	netsh i i show in netsh -c "i" add neighbors idx <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

Step 4 Power off the Device and then restart it, or restart the Device over the network.

Step 5 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.

Step 6 Enter *http://<IP address>* in the browser address bar to log in.

5.2.2 Port

Configure the maximum port numbers and values on this interface.

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

The **Port** interface is displayed. See Figure 5-37.

Figure 5-37 Port interface

Port		
Max Connection	10	(1~20)
TCP Port	37777	(1025~65534)
UDP Port	37778	(1025~65534)
HTTP Port	80	
RTSP Port	554	
HTTPS Port	443	
Default Refresh Save		

Step 2 Configure each port value of the Device. For details, see Table 5-14.



- 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 5-14 Port parameter description

Parameter	Description
Max Connection	The maximum number of users that can log in to the web interface 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.
RTSP Port	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. When the URL format requiring RTSP, you need to specify channel number and bit stream type in the URL, and also username and password if needed. When playing live view with Blackberry mobile phone, you need to disable the audio, and then set the stream encoding mode to H.264B and resolution to CIF. URL format example: rtsp://username:password@ip:port/cam/realmonitor?channel=1&subtype=0 ● 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). For example, if you require the sub stream of channel 2 from a certain device, then the URL shall be: rtsp://admin:admin@192.168.1.123:554/cam/realmonitor?channel=2&subtype=1 If certification is not required, you do not need to specify the username and password. Use the following format: rtsp://ip:port/cam/realmonitor?channel=1&subtype=0
RTSP Port	A network protocol for real-time data communication. The value is 1935 by default. You can enter the value as needed.  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.

Parameter	Description
HTTPS Port	HTTPS communication port. The value is 443 by default. You can set this parameter as needed.

Step 3 Click **Save**.

5.2.3 PPPoE

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).

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

The **PPPoE** interface is displayed. See Figure 5-38.

Figure 5-38 PPPoE interface (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. See Figure 5-39. You can access the Device through the IP address.

Figure 5-39 PPPoE interface (2)

5.2.4 DDNS

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.

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

The **DDNS** interface is displayed. See Figure 5-40.

Figure 5-40 DDNS

Step 2 Select **Type**, and then configure the parameters as needed. For details, see Table 5-15.

Table 5-15 DDNS parameter description

Parameter	Description
Type	The name and website of the DDNS service provider. Here is the matching relationship:
Server address	● CN99 DDNS Server address: www.3322.org ● NO-IP DDNS Server address: dynupdate.no-ip.com ● Dyndns DDNS Server address: members.dyndns.org
Domain Name	The domain name you registered on the DDNS website.
Username	Enter the username and password obtained from DDNS service provider.
Password	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 interface 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.

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.

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

The **SMTP (Email)** interface is displayed. See Figure 5-41.

Figure 5-41 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 parameters as needed. For parameter description, see Table 5-16.

Table 5-16 SMTP (Email) parameter description

Parameter	Description	
SMTP Server	IP address of the outgoing mail server complying with SMTP protocol.	For the detailed configuration, see Table 5-17.
Port	Port number of the outgoing mail server complying with SMTP protocol. It is 25 by default.	

Parameter	Description	
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.  - For the detailed configuration, see Table 5-17. - 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 check box 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 check box 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.	

For common email configurations, see Table 5-17.

Table 5-17 Common email configuration description

Type	SMTP Server	Authentication	Port	Description
QQ	smtp.qq.com	SSL	465	- 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.  Authentication code is the code you receive when enabling SMTP service.
		TLS	587	
163	smtp.163.com	SSL	465/994	- You need to enable SMTP service in your mailbox. - The authentication code is required; the email password is not applicable.  Authentication code is the code you receive when enabling SMTP service.
		TLS	25	
		—	25	

Type	SMTP Server	Authentication	Port	Description
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.

Perform the following steps to add UPnP network service in the Windows system.

Step 1 Open **Control Panel**, and select **Add or Remove Programs**.

Step 2 Click **Add/Remove Windows Components**.

Step 3 Select **Network Service** from the **Windows Components Wizard** and click **Details** button.

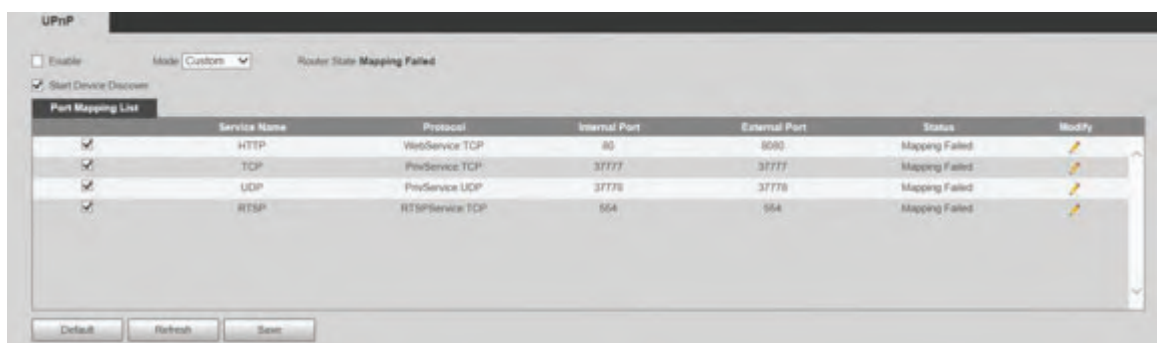
Step 4 Select **Internet Gateway Device Discovery and Control Client**, and **UPnP User Interface**, and then click **OK** to start installation.

Perform the following steps to configure UPnP:

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

The **UPnP** interface is displayed. See Figure 5-42.

Figure 5-42 UPnP



Step 2 Select **Enable**.

Step 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.

Step 4 Select **Start Device Discover** as needed.

Step 5 Click **Save**.

5.2.7 SNMP

SNMP (Simple Network Management Protocol) is a basic network management framework. You need to install certain software to the Device to obtain the configuration information of the Device.

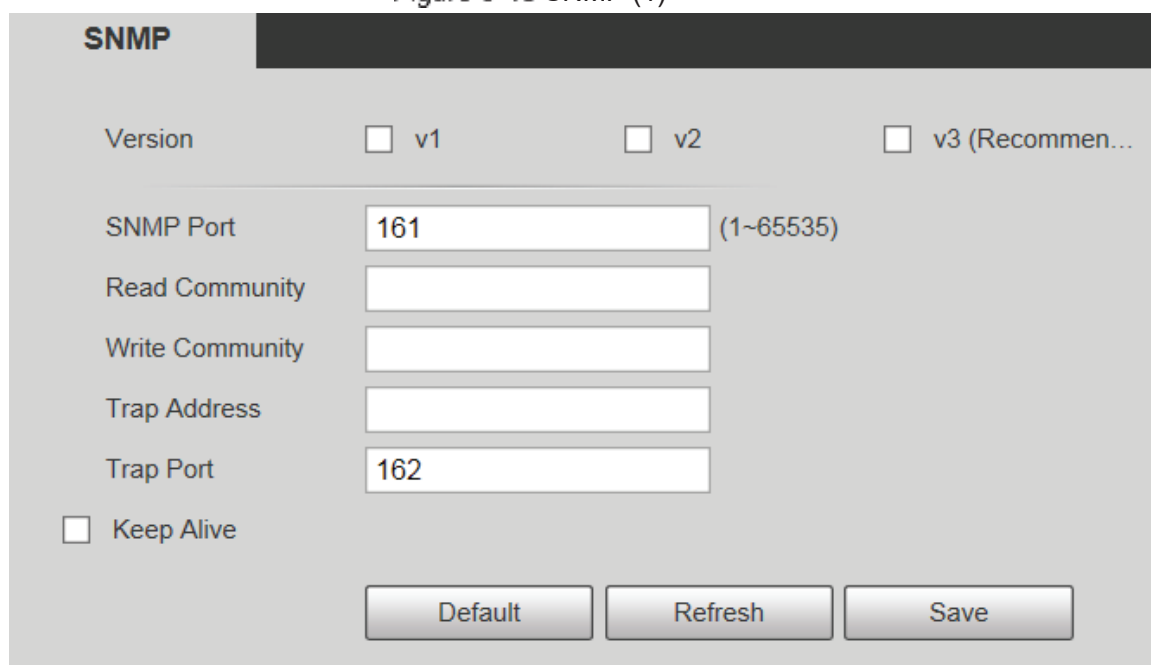
The following requirements must be satisfied if you want to use SNMP function:

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

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

The **SNMP** interface is displayed. See Figure 5-43 and Figure 5-44.

Figure 5-43 SNMP (1)



The screenshot shows the 'SNMP' configuration page. At the top, there's a title bar with 'SNMP' on the left and a dark grey bar on the right. Below the title bar, there are three radio buttons for 'Version': 'v1', 'v2', and 'v3 (Recommen...'. The 'v3' option is selected. Below the version selection, 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, there 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'.

Figure 5-44 SNMP (2)

The image shows a web-based configuration interface for SNMP. At the top, there's a title bar 'SNMP'. Below it, the 'Version' section has three radio buttons: 'v1', 'v2', and 'v3 (Recommended)'. The 'v3' option is selected. Below this, there are input fields for 'SNMP Port' (set to 161), 'Read Community', 'Write Community', 'Trap Address', and 'Trap Port' (set to 162). A 'Keep Alive' checkbox is present and unchecked. The 'Read-only Username' is set to 'public'. Under 'Authentication Type', 'MD5' is selected over 'SHA'. There are two password fields for authentication, both with a red warning: 'The minimum pass phrase length is 8 characters'. Similarly, under 'Encryption Type', 'CBC-DES' is selected over 'SHA', with two password fields also having the same red warning. At the bottom, there are three buttons: 'Default', 'Refresh', and '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 5-18 SNMP parameter description

Parameter	Description
Version	Select the check box of the version you need, and the system can process information of the corresponding version. ● 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.  V1 and V2 might cause data leakage, and V3 is recommended.
SNMP Port	The listening port of the software agent in the Device.

Parameter	Description
Read Community/Write Community	The read and write community strings that the software agent supports.  The name can only consist of number, letter, underline (_), and strikethrough (-).
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 check box, and the system can send data package to ensure network connection without interruption.
Read-only Username	The name is public by default.  The username can only consist of number, letter, and underline.
Read&write Username	The name is private by default.  The username can only consist of number, letter, and underline.
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.

5.2.8 Bonjour

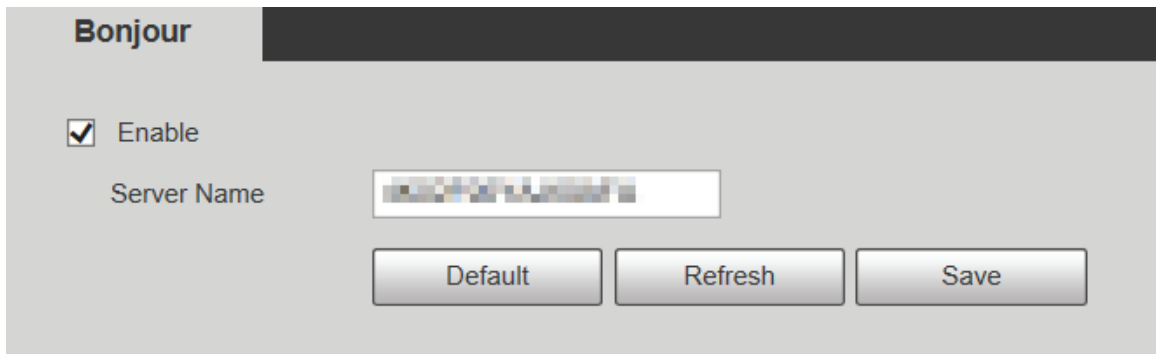
Bonjour is also called zero-configuration networking, which can automatically discover computers, devices and services on IP networks. Bonjour is a protocol of industry standard which allows devices to search and find each other. IP address or DNS server is not required during the process.

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.

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

The **Bonjour** interface is displayed. See Figure 5-45.

Figure 5-45 Bonjour interface



Step 2 Select **Enable**, and then set **Server Name**.

Step 3 Click **Save**.

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

Step 1 Click **Show all bookmarks** in Safari.

Step 2 The OS or client automatically detects the network cameras with Bonjour enabled in the LAN.

Step 3 Click to visit the corresponding web interface.

5.2.9 Multicast

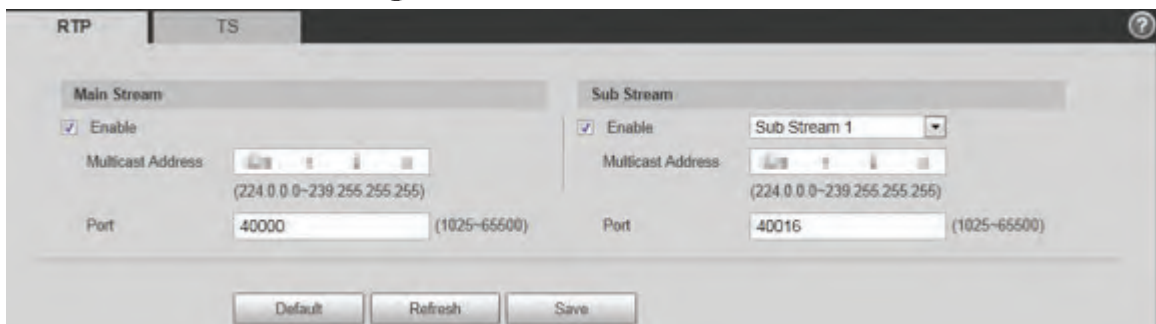
Access the Device by network to see live view. If the access times exceed its upper limit, preview might fail. You can set multicast IP to access by multicast protocol to solve the problem. The Device supports two multicast protocols: **RTP** and **TS**. RTP is enabled by default when main stream and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

5.2.9.1 RTP

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

The **RTP** interface is displayed. See Figure 5-46.

Figure 5-46 RTP interface



Step 2 Enable main stream or sub stream as needed.

Step 3 Enter multicast address and port number.

Step 4 Click **Save**.

5.2.9.2 TS

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

The **TS** interface is displayed. See Figure 5-47.

Figure 5-47 TS interface

The screenshot shows the 'TS' interface with two sections: 'Main Stream' and 'Sub Stream'. Each section has an 'Enable' checkbox, a 'Multicast Address' field with a range '(224.0.0.0-239.255.255.255)', and a 'Port' field with a range '(1025-65500)'. The 'Main Stream' port is set to '20000' and the 'Sub Stream' port is set to '20016'. At the bottom are 'Default', 'Refresh', and 'Save' buttons.

Step 2 Enable main stream or sub stream as needed.

Step 3 Enter multicast address and port number.

Step 4 Click **Save**.

5.2.10 Auto Register

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.

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

The **Auto Register** interface is displayed. See Figure 5-48.

Figure 5-48 Auto register

The screenshot shows the 'Auto Register' interface. It has an 'Enable' checkbox, an 'IP Address' field with '0.0.0.0', a 'Port' field with a blurred value, and a 'Sub-Device ID' field with 'none'. At the bottom are 'Default', 'Refresh', and 'Save' buttons.

Step 2 Select the **Enable** check box to enable **Auto Register**.

Step 3 Enter **IP Address**, **Port** and **Sub-Device ID**. For details, see Table 5-19.

Table 5-19 Auto register parameter description

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.

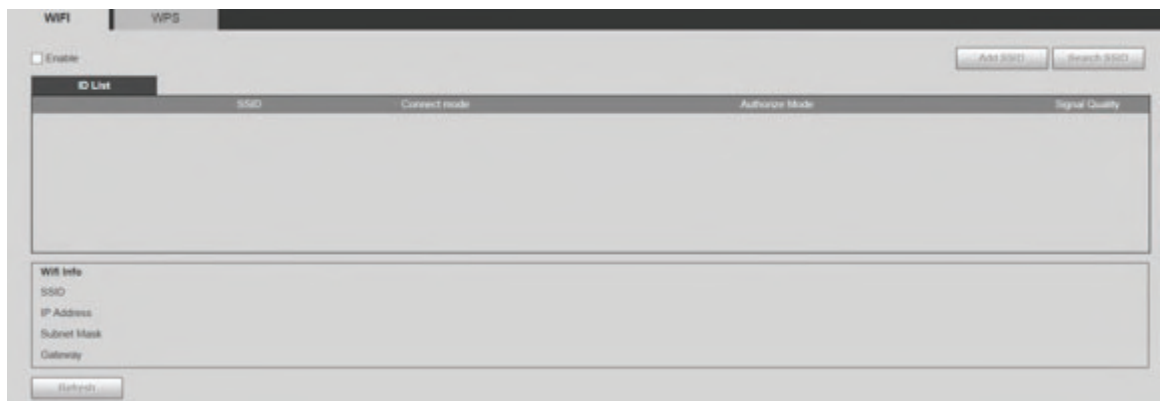


- Wi-Fi and WPS are available on select models.
- All devices with WPS button support WPS function.

5.2.11.1 Wi-Fi

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. For Wi-Fi configuration interface, see Figure 5-49.

Figure 5-49 Wi-Fi interface

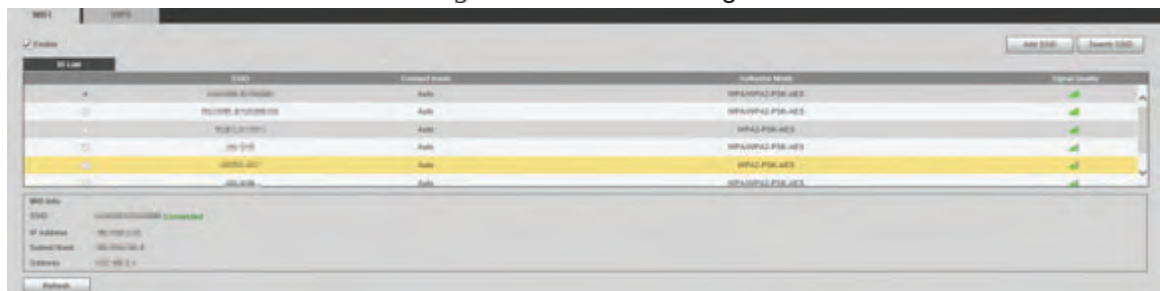


Perform the following steps to configure Wi-Fi.

Step 1 Select the **Enable** check box.

Step 2 Click **Search SSID**, and Wi-Fi hotspots in the environment of current network camera are displayed. See Figure 5-50.

Figure 5-50 Wi-Fi setting



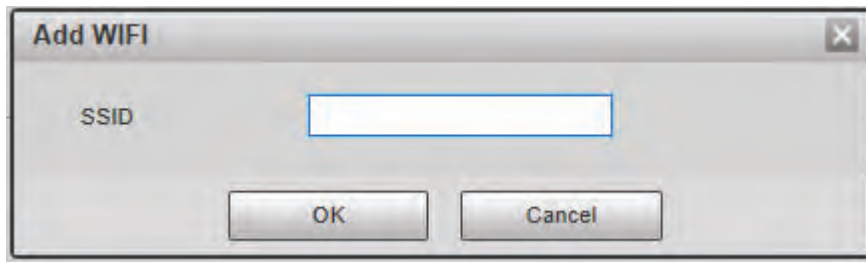
Step 3 To manually add Wi-Fi, click **Add SSID**, and the **Add WiFi** interface is displayed. See Figure 5-51.

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.

Figure 5-51 Adding Wi-Fi

A dialog box titled "Add WIFI" with a close button (X) in the top right corner. It contains a label "SSID" followed by a text input field. At the bottom, there are two buttons: "OK" and "Cancel".

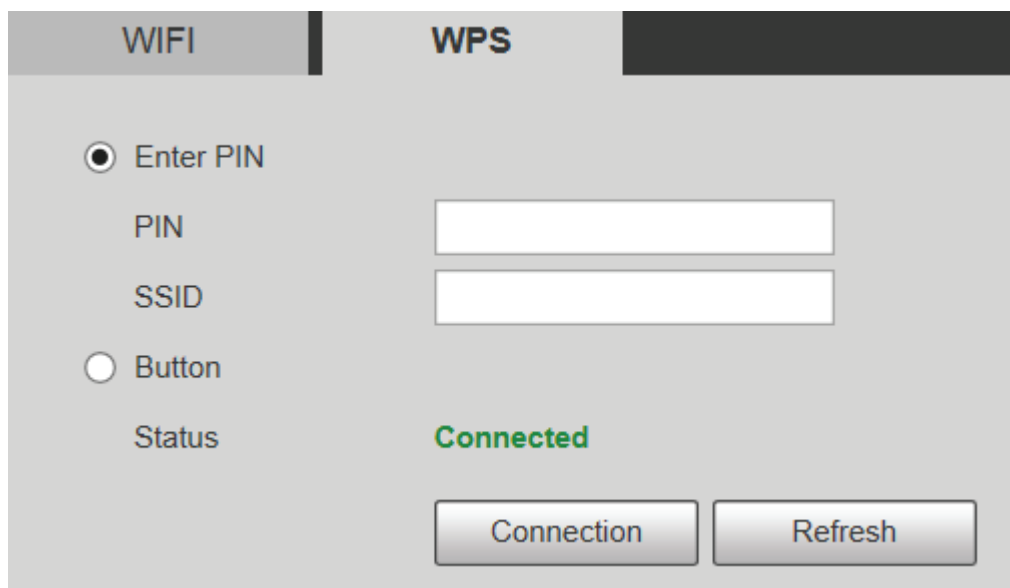
Step 5 Double-click one hotspot to display the **Signal Quality** and the **Authentication Manner**.

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

5.2.11.1.2 WPS

For WPS configuration interface, see Figure 5-52.

Figure 5-52 WPS setting

The WPS configuration interface has two tabs: "WIFI" and "WPS". The "WPS" tab is selected. It contains two radio buttons: "Enter PIN" (selected) and "Button". Below "Enter PIN" are two text input fields labeled "PIN" and "SSID". Below "Button" is a label "Status" with the text "Connected" in green. At the bottom, there are two buttons: "Connection" and "Refresh".

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

5.2.12 802.1x

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.

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

The **802.1x** interface is displayed, see Figure 5-53.

Figure 5-53 802.1x interface

Step 2 Select the **Enable** check box to enable **802.1x**.

Step 3 Select an authentication mode, and enter username and password. For parameter description, see Table 5-20.

Table 5-20 802.1X setting parameter description

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

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.

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

The **QoS** interface is displayed. See Figure 5-54.

Figure 5-54 QoS interface

Step 2 Configure **Realtime Monitor** and **Command**. For parameter description, see Table 5-21.

Table 5-21 QoS setting parameter description

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.

Step 3 Click **Save**.

5.2.14 4G

5.2.14.1 Dialing Setting

Log in to web interface, select **Setting > Network > 4G > Dialing Setting** and the **Dialing Setting** interface is displayed. See Figure 5-55.

Figure 5-55 Dialing setting interface



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

Step 1 Select the **Enable** check box.

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. See Figure 5-56.



- 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 interface. And you cannot access the device through 4G.

Figure 5-56 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 "4.2.12.2 Mobile Setting."

Step 5 Click **Save**.

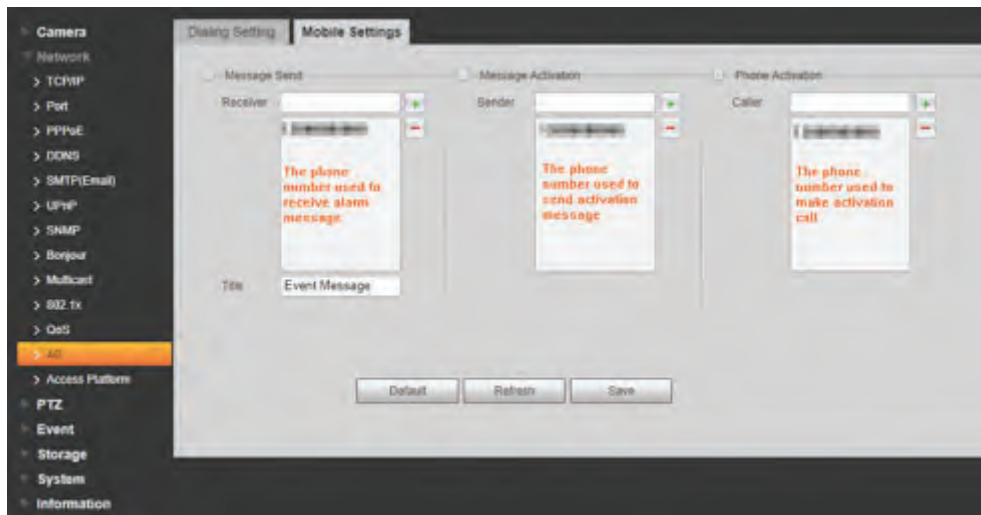
5.2.14.2 Mobile Setting

Log in to web interface, select **Setting > Network > 4G > Mobile Settings**, and the **Mobile Setting** interface is displayed. See Figure 5-55.

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 Step 3 of "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 5-57 Mobile setting interface



- **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.

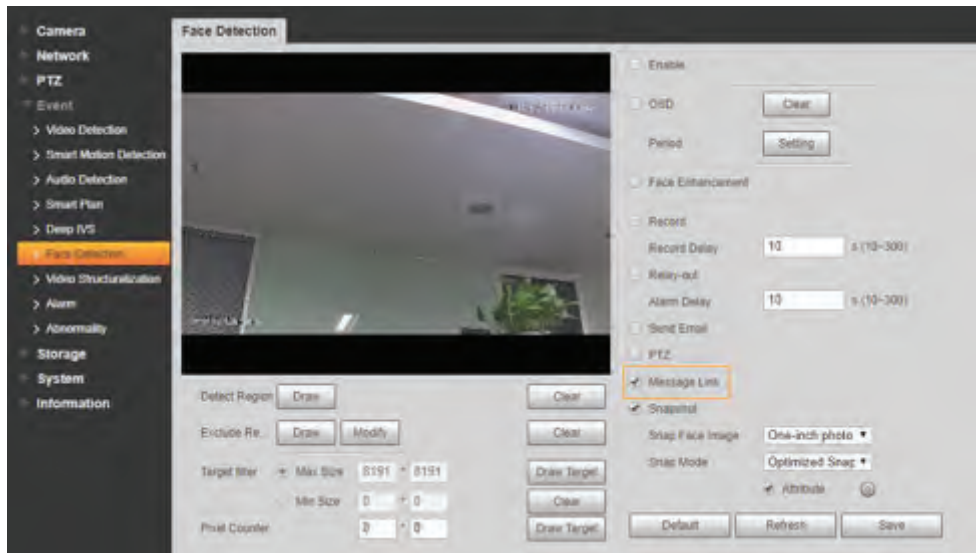
Step 1 Select the check box of the service you need to enable. You can select one or more services.

Step 2 Enter the phone number and click  to add it.

Step 3 Click **Save**.

Step 4 Select the **Message Link** check box on the interface of the event for which you want to receive message.
Take Face Detection for example. Click **Setting > Event > Face Detection** and select the **Message Link** check box.

Figure 5-58 Message link



Step 5 Click **Save** on the interface of the corresponding event. And you will receive message if the alarm is triggered.

5.2.15 Access Platform

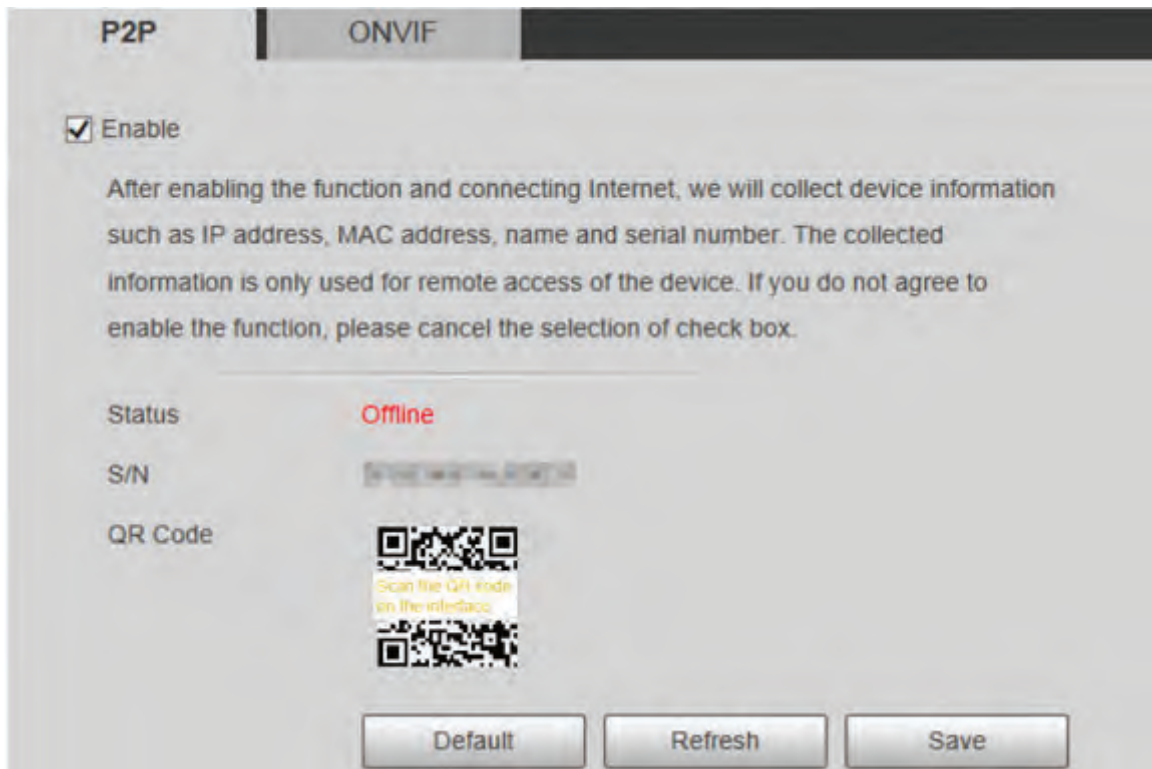
5.2.15.1 P2P

P2P is a private network traversal technology which enables users to manage devices easily without requiring DDNS, port mapping or transit server. Scan the QR code with your smart phone, and then you can add and manage more devices on your mobile client.

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

The **P2P** interface is displayed.

Figure 5-59 P2P interface



- 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** check box.

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

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

Step 4 Scan the QR code on the P2P interface.

Step 5 Follow the instructions to finish settings.

5.2.15.2 ONVIF

The ONVIF authentication is **On** by default, which allows the network video products (including video recording device and other recording devices) from other manufacturers to connect to the Service.

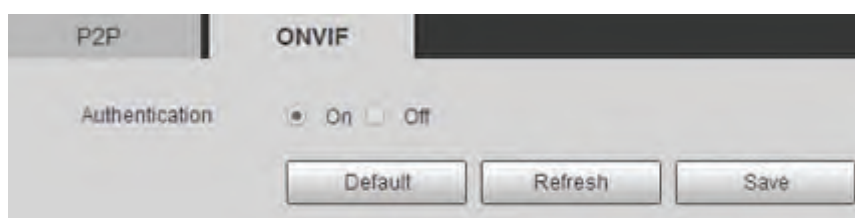


ONVIF is enabled by default.

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

The **ONVIF** interface is displayed. See Figure 5-60.

Figure 5-60 ONVIF interface



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

Step 3 Click **Save**.

5.2.15.3 RTMP

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.

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

The **RTMP** interface is displayed. See Figure 5-61.

Figure 5-61 RTMP interface

The screenshot shows the RTMP configuration page. At the top, there are three tabs: P2P, ONVIF, and RTMP. The RTMP tab is selected. Below the tabs, there is an 'Enable' checkbox. Under 'Stream Type', there are three radio buttons: 'Main Stream' (selected), 'Sub Stream 1', and 'Sub Stream 2'. Under 'Address Type', there are two radio buttons: 'Non-custom' (selected) and 'Custom'. Below these are input fields for 'IP Address', 'Port' (with a range of 0~65535), and 'Custom Address'. At the bottom, there are three buttons: 'Default', 'Refresh', and 'Save'.

Step 2 Select the **Enable** check box, and RTMP will be enabled.



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

Step 3 Set parameters. For details, see Table 4-20.

Table 5-22 RTMP parameter setting description

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 . 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. IP Address: IPv4 or domain name is supported. Port: It is recommended to use the default value.
Port	

Parameter	Description
Custom Address	If you have selected Custom , the address allocated by the server needs to be filled in.

Step 4 Click **Save**.

5.3 PTZ Settings

5.3.1 Protocol



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

5.3.1.1 Network PTZ Settings

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

The **Network PTZ** interface is displayed. See Figure 5-62.

Figure 5-62 Network PTZ setting

Step 2 Select a protocol as needed. You can select **DH-SD1**, **DH-SD3**, **PELCOD**, or **PELCOP**. **DH-SD1** is selected by default.



DH-SD1 protocol supports up to 80 presets, and DH-SD3 protocol supports up to 300 presets.

Step 3 Click **Save**.

5.3.1.2 Analog PTZ Settings

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

The **Analog PTZ** interface is displayed. See Figure 5-63.

Figure 5-63 Analog PTZ setting

The screenshot shows a web interface for configuring PTZ settings. It has two tabs: 'Network PTZ' and 'Analog PTZ'. The 'Analog PTZ' tab is active. Below the tabs are five configuration fields: 'Address' with a text input containing '1', 'Baud Rate' with a dropdown menu showing '9600', 'Data Bit' with a dropdown menu showing '8', 'Stop Bit' with a dropdown menu showing '1', and 'Parity' with a dropdown menu showing 'NONE'. At the bottom of the form are three buttons: 'Default', 'Refresh', and 'Save'.

Step 2 Configure parameters as needed. See Table 5-23.

Table 5-23 Analog PTZ parameter description

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**.

5.3.2 Function

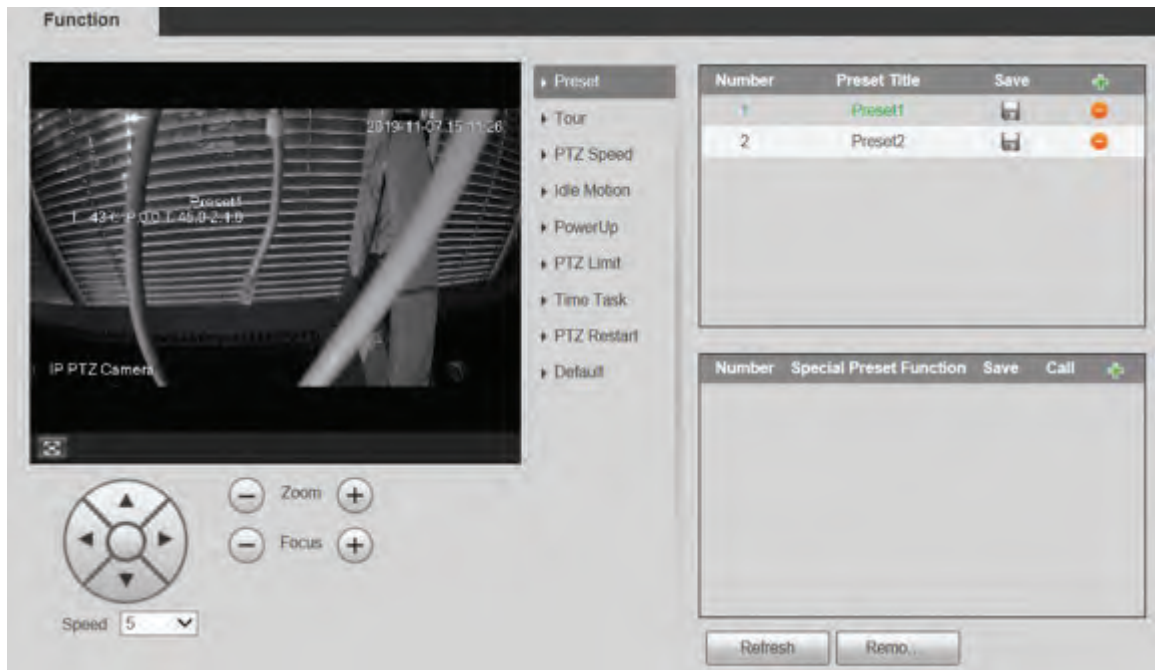
5.3.2.1 Preset

Select **Setting > PTZ > Function > Preset**. The **Preset** interface is displayed. See Figure 5-64.



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

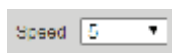
Figure 5-64 Preset settings



Preset

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

Step 1 At the lower left corner of the **Preset** interface, click the direction buttons,



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. See Figure 5-65

Figure 5-65 Adding 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.

Special Preset

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

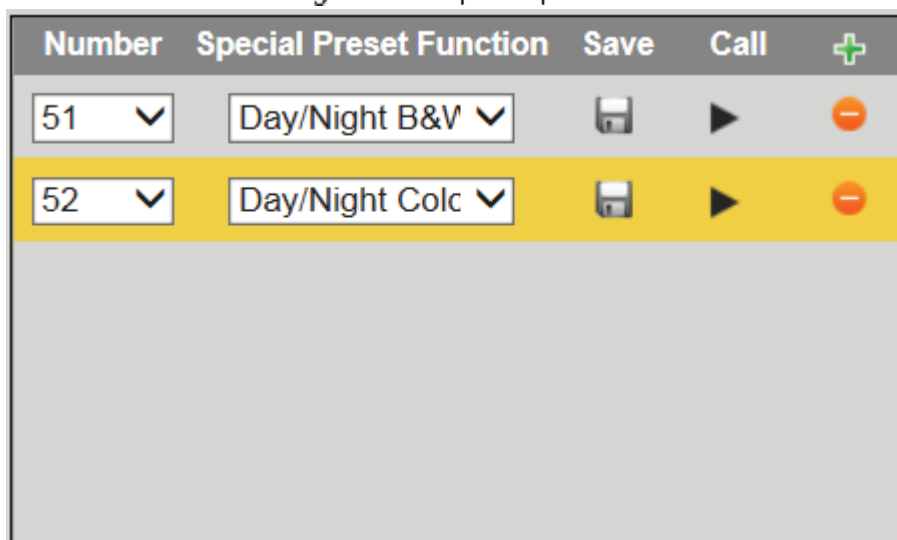
Step 1 Click  to add a special preset. The added special preset will be displayed in the list.

See Figure 4-60.



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

Figure 5-66 Special presets



Step 2 Click  to save the added special preset.

Step 3 Perform operations on special presets.

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



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

5.3.2.2 Tour

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

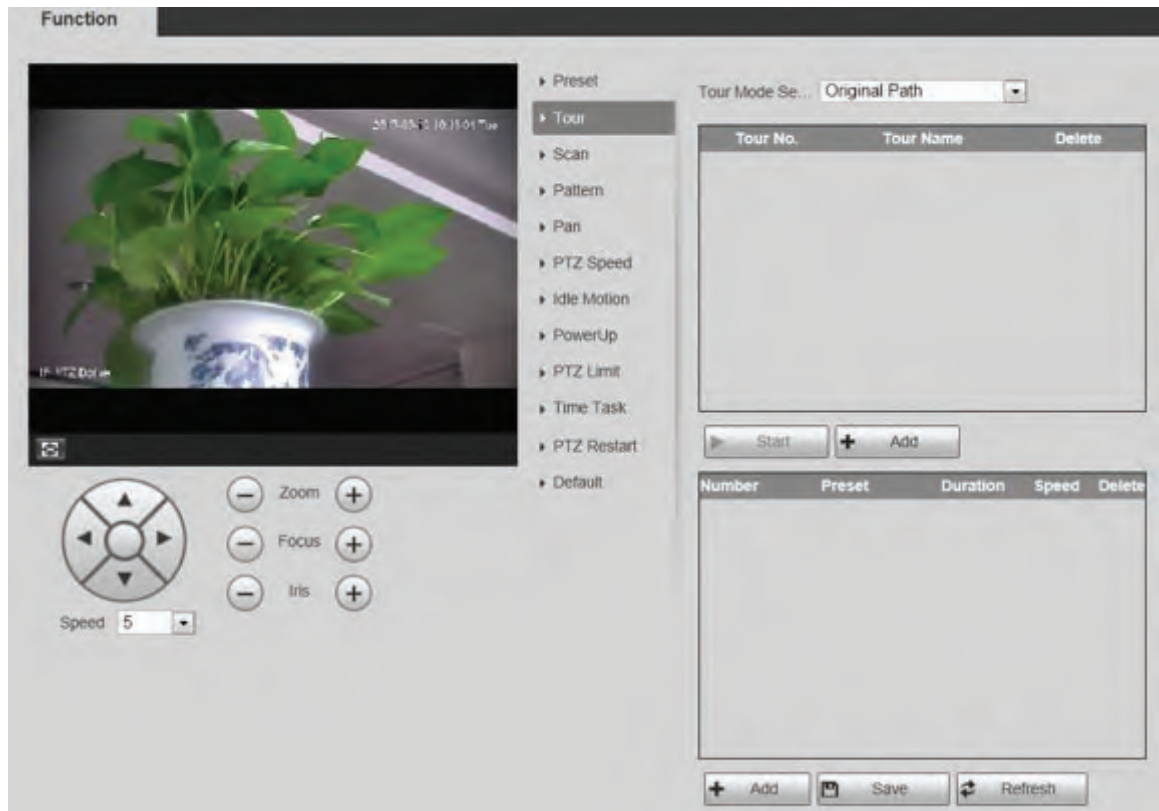


You need to set several presets in advance.

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

The **Tour** interface is displayed. See Figure 5-67.

Figure 5-67 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 at the upper right corner of the interface to add a tour path.

Step 4 Click **Add** at the bottom of the list at the lower right corner of the interface 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.

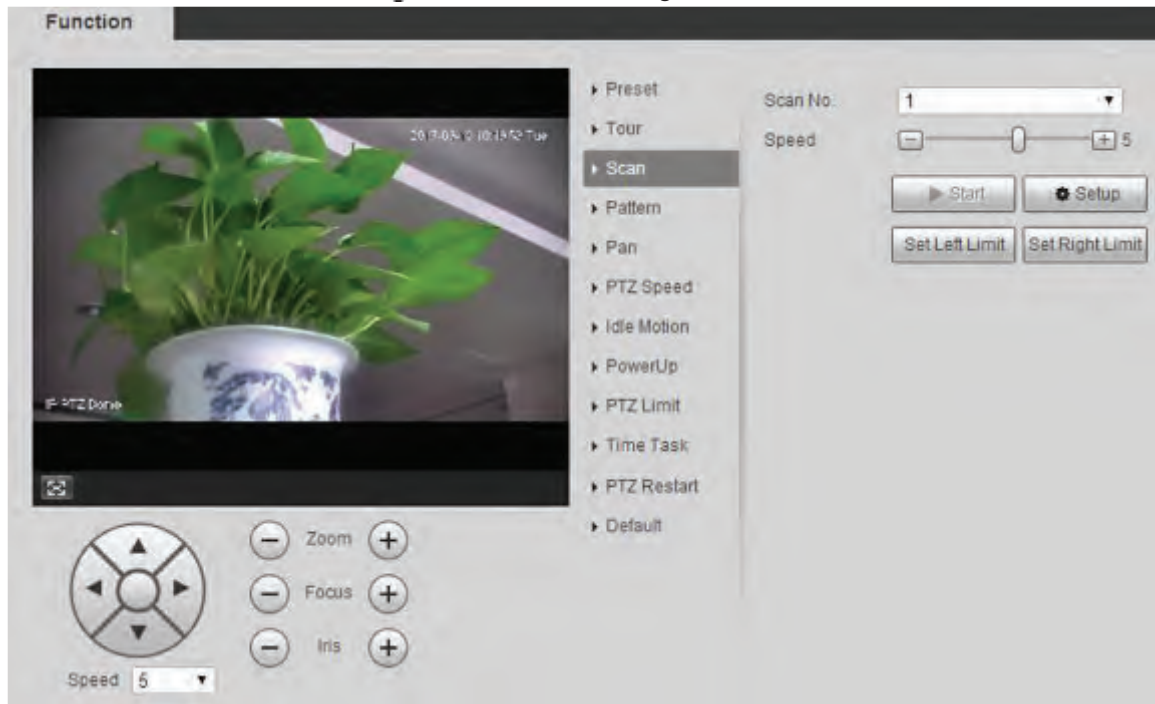
5.3.2.3 Scan

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

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

The **Scan** interface is displayed. See Figure 5-68.

Figure 5-68 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 the Device starts scanning.

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

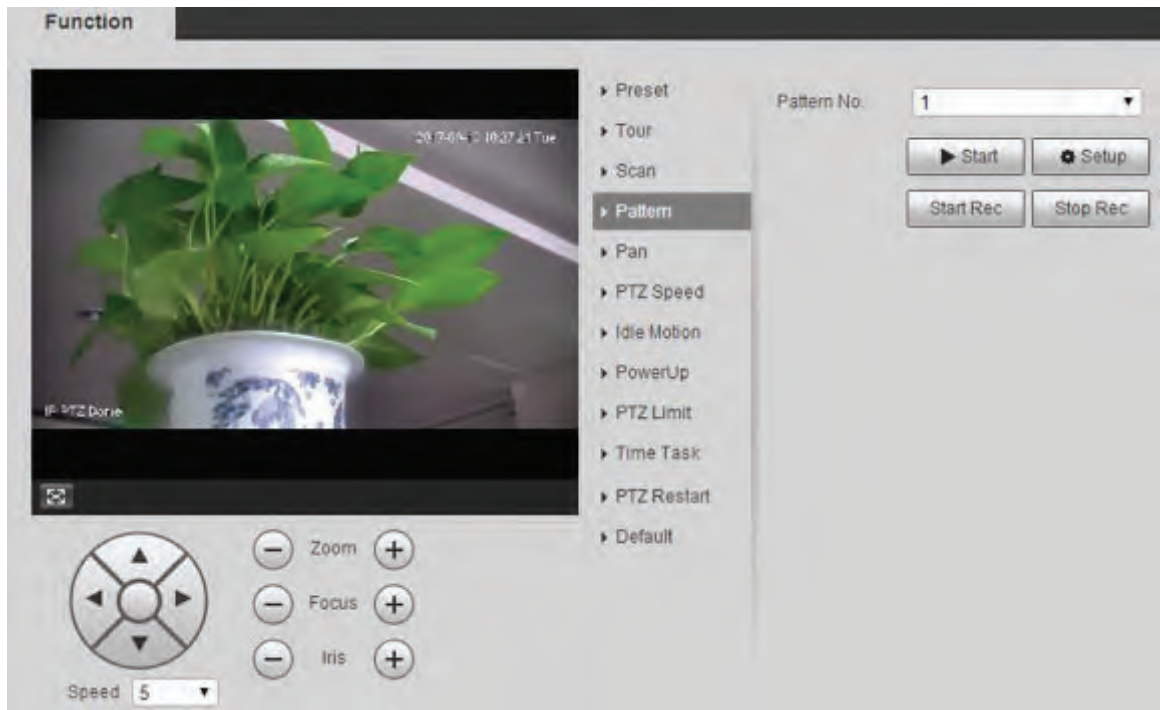
5.3.2.4 Pattern

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.

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

The **Pattern** interface is displayed. See Figure 5-69.

Figure 5-69 Pattern settings



Step 2 Select the **Pattern No.**

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

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

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

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

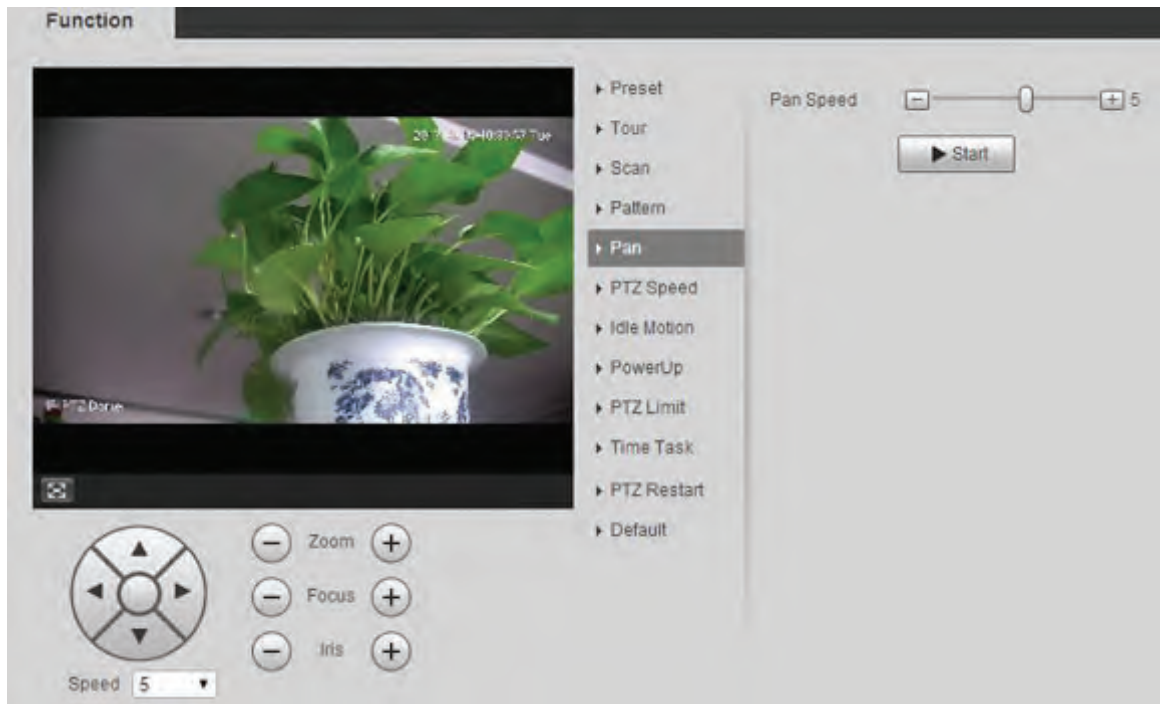
5.3.2.5 Pan

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

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

The **Pan** interface is displayed. See Figure 5-70.

Figure 5-70 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.

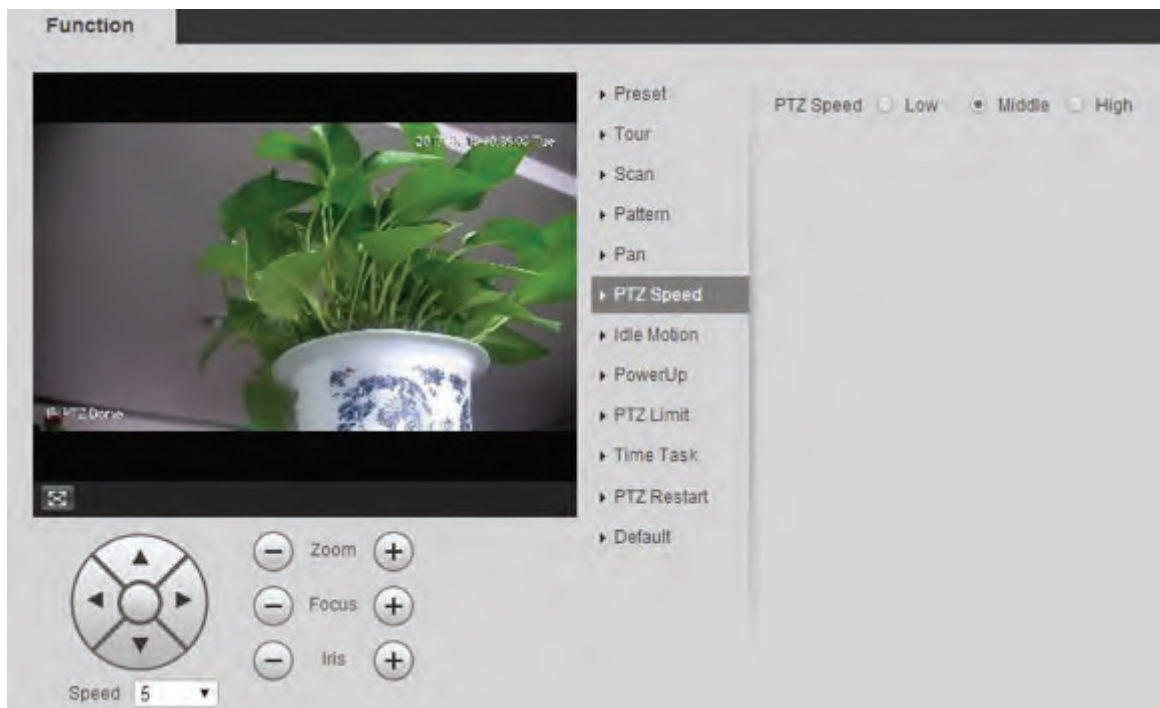
5.3.2.6 PTZ Speed

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.

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

The **PTZ Speed** interface is displayed. See Figure 5-71.

Figure 5-71 PTZ speed settings



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

5.3.2.7 Idle Motion

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

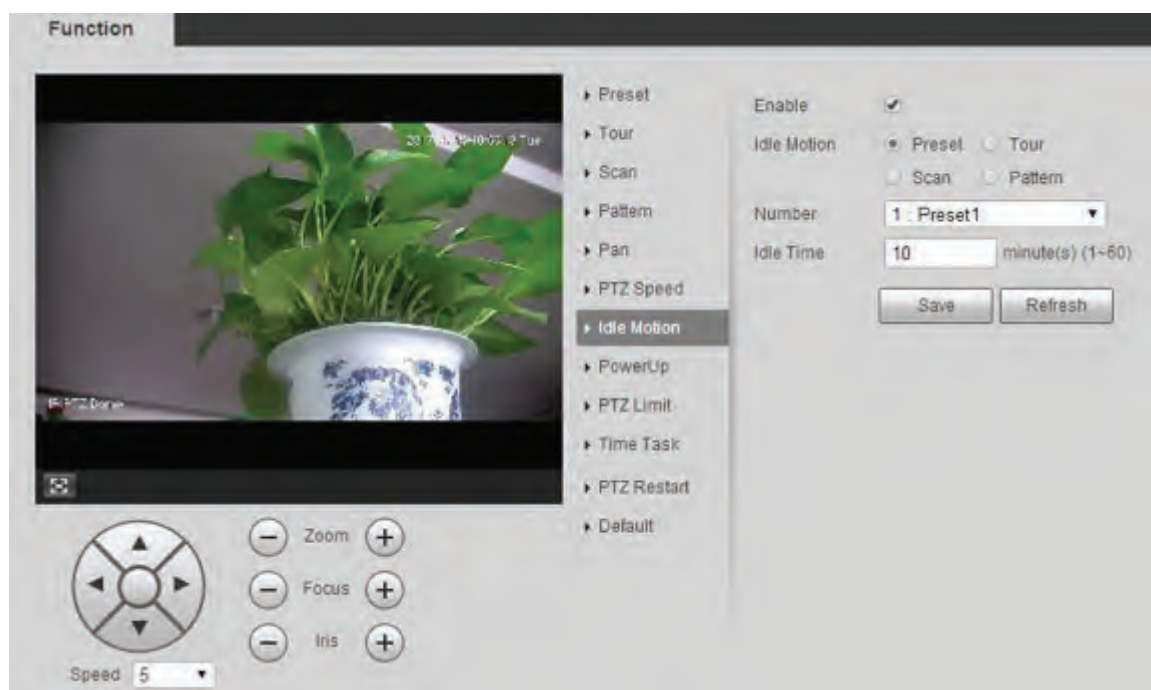


Set **Preset**, **Tour**, **Scan** or **Pattern** in advance.

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

The **Idle Motion** interface is displayed. See Figure 5-72.

Figure 5-72 Idle motion settings



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

5.3.2.8 PowerUp

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

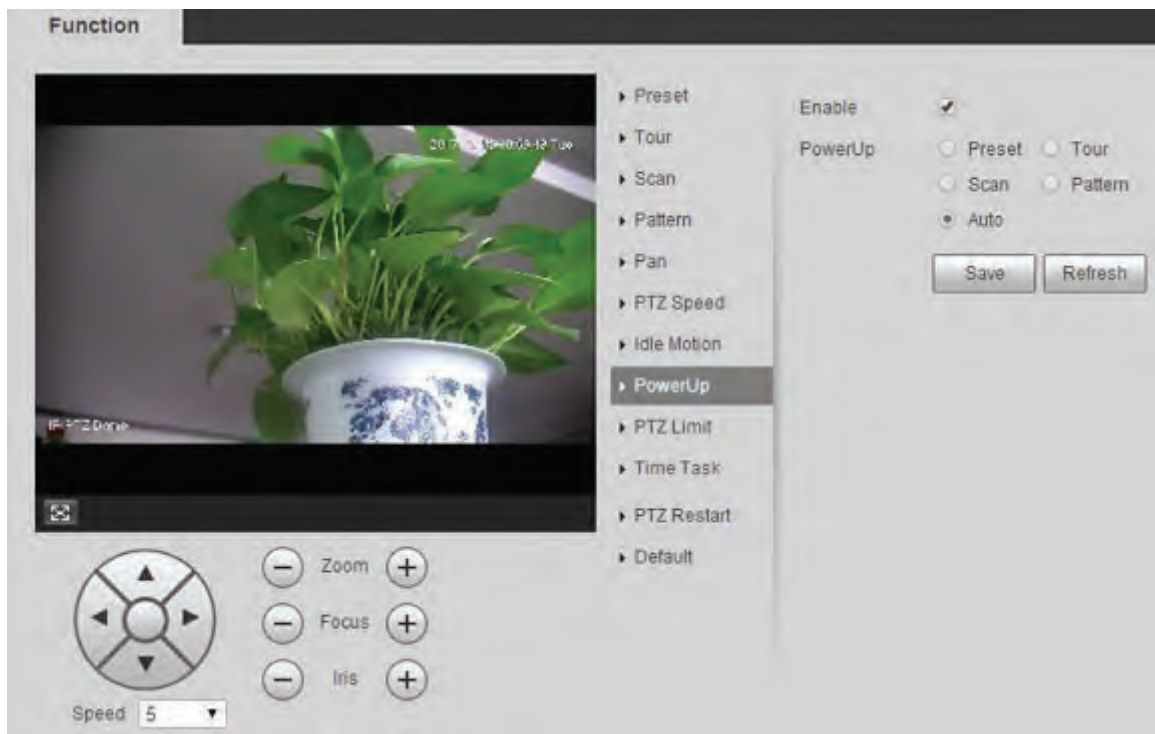


Set **Preset**, **Tour**, **Scan** or **Pattern** in advance.

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

The **PowerUp** interface is displayed. See Figure 5-73.

Figure 5-73 PowerUp settings



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

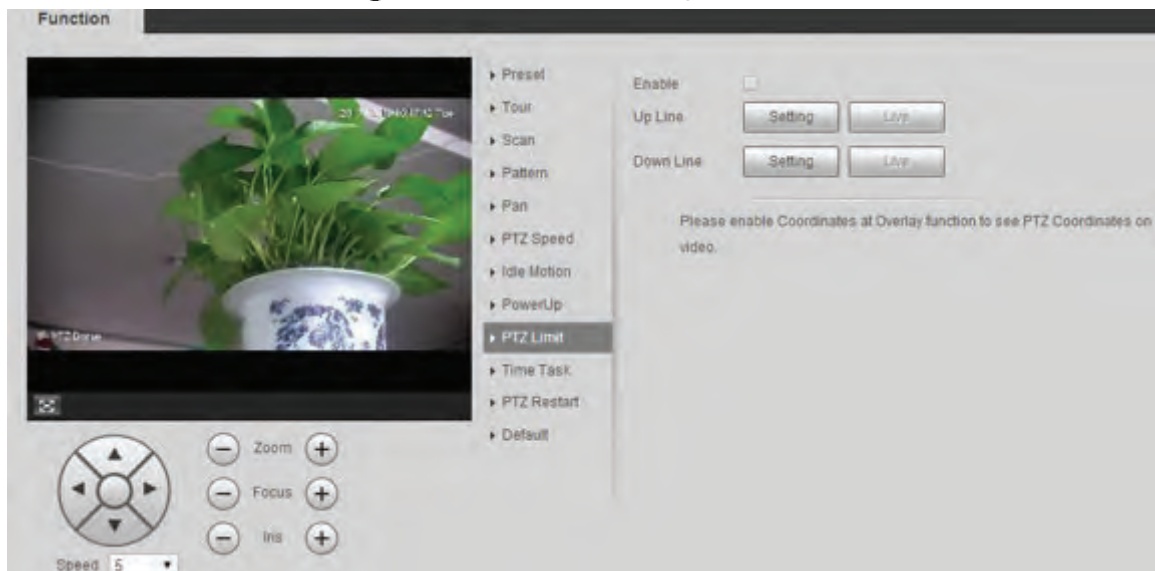
5.3.2.9 PTZ Limit

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

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

The **PTZ Limit** interface is displayed. See Figure 5-74.

Figure 5-74 PTZ limit settings



- Step 2** Adjust the PTZ direction and click **Setting** to set the **Up Line**.
- Step 3** Adjust the PTZ direction and 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** check box to enable the PTZ limit function.

5.3.2.10 Time Task

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

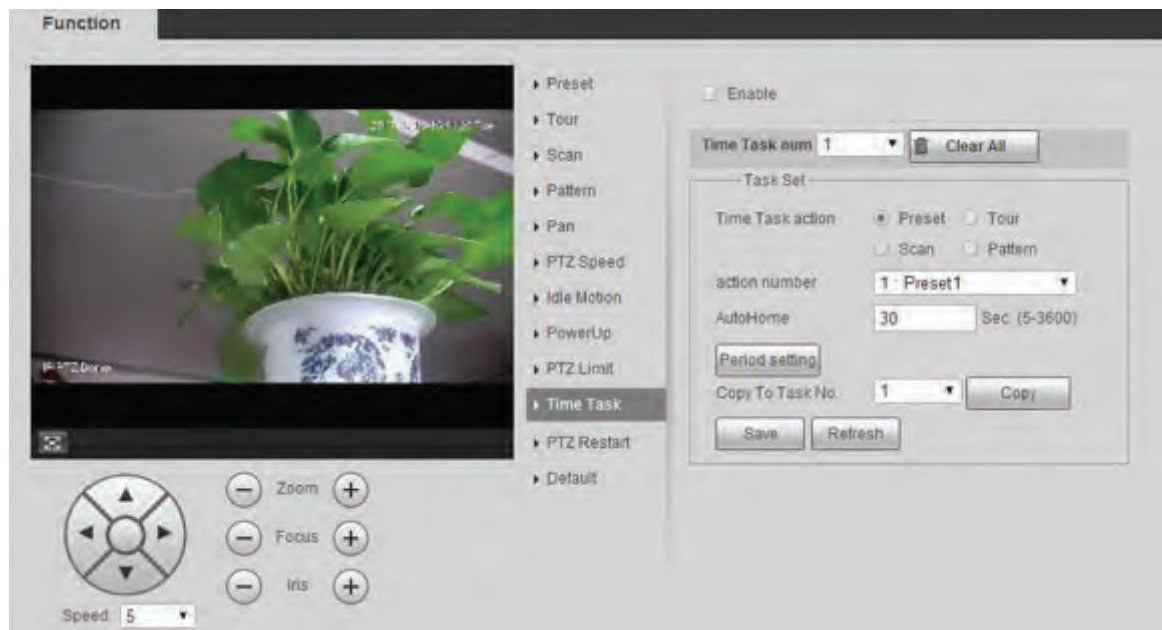


Set **Preset**, **Tour**, **Scan** or **Pattern** in advance.

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

The **Time Task** interface is displayed. See Figure 5-75.

Figure 5-75 Time task settings



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

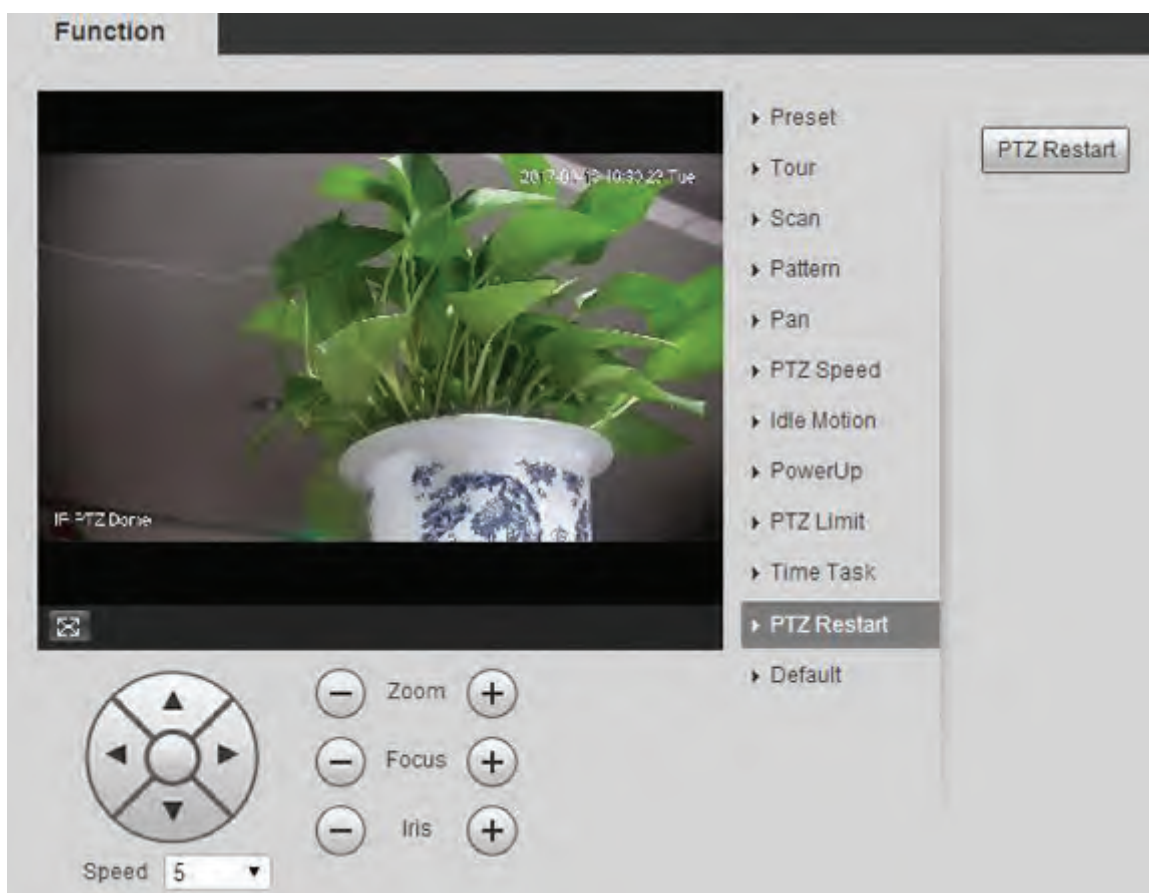
5.3.2.11 PTZ Restart

Restart the PTZ. Follow these steps to complete the configuration.

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

The **PTZ Restart** interface is displayed. See Figure 5-76.

Figure 5-76 PTZ restart



Step 2 Click **PTZ Restart**.

The PTZ is restarted.

5.3.2.12 Default

Restore the PTZ to factory defaults.



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

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

The **Default** interface is displayed. See Figure 5-77.

Figure 5-77 Default setting



Step 2 Click **Default**.

The PTZ will be restored to factory defaults.

5.4 Event Management

5.4.1 Video Detection

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

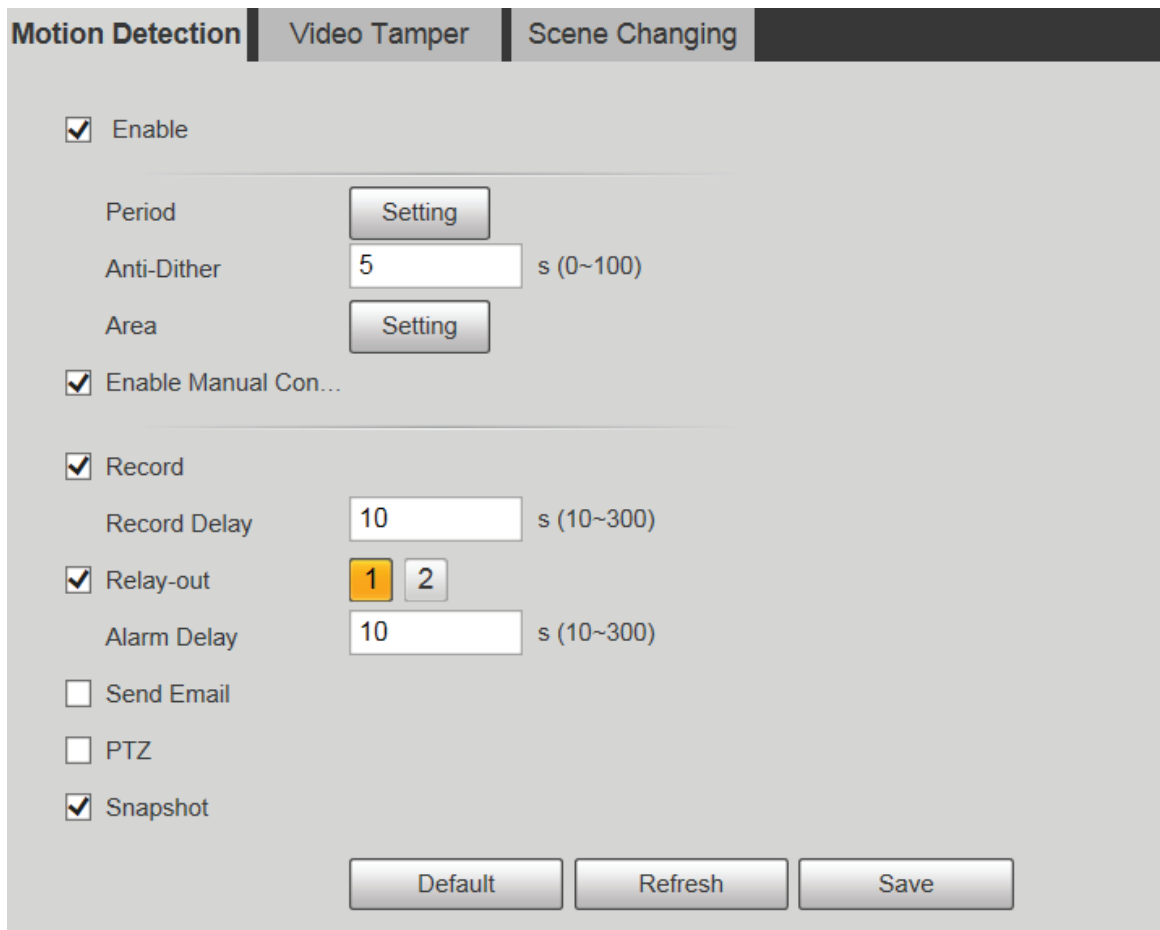
5.4.1.1 Motion Detection

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

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

The **Motion Detection** interface is displayed. See Figure 5-78.

Figure 5-78 Motion detection settings



The image shows a web-based configuration interface for motion detection. At the top, there are three tabs: 'Motion Detection' (selected), 'Video Tamper', and 'Scene Changing'. Below the tabs, the 'Motion Detection' section contains several settings. A 'Period' label is followed by a 'Setting' button. The 'Anti-Dither' setting has a text input field with the value '5' and a unit 's (0~100)'. The 'Area' setting is followed by another 'Setting' button. There are two 'Enable' checkboxes: one for 'Enable' (checked) and one for 'Enable Manual Con...' (checked). Below these, there is a 'Record' checkbox (checked) followed by a 'Record Delay' setting with a text input field containing '10' and a unit 's (10~300)'. The 'Relay-out' checkbox is also checked, followed by a numeric selector with '1' selected and '2' as an alternative. Below this is an 'Alarm Delay' setting with a text input field containing '10' and a unit 's (10~300)'. There are three unchecked checkboxes: 'Send Email', 'PTZ', and 'Snapshot'. At the bottom of the settings area, there are three buttons: 'Default', 'Refresh', and 'Save'.

Motion Detection | Video Tamper | Scene Changing

☒ Enable

Period Setting

Anti-Dither s (0~100)

Area Setting

☒ Enable Manual Con...

☒ Record

Record Delay s (10~300)

☒ Relay-out 1 2

Alarm Delay s (10~300)

☐ Send Email

☐ PTZ

☒ Snapshot

Default Refresh Save

Step 2 Select the **Enable** check box, and then configure parameters as needed.

- Set arming and disarming period.
 - 1) Click **Setting**, and then set the arming and disarming period on the interface. See Figure 5-79.

Figure 5-79 Arming and disarming period settings

The 'Period' settings window displays a 24-hour timeline at the top. Below the timeline, seven rows represent the days of the week (Sun to Sat), each with a green bar indicating the active period and a 'Setting' button. At the bottom, there are checkboxes for 'All' (selected), 'Sun' (checked), 'Mon', 'Tue', 'Wed', 'Thu', 'Fri', and 'Sat'. Below these are six time periods (Period1 to Period6) with start and end time selectors. 'Period1' is selected. At the very bottom are 'Save' and 'Cancel' buttons.

- 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** interface.
- Set the area.
Click **Setting**, and the **Area** interface is displayed. See Figure 5-80. Refer to Table 5-24 and Table 5-25 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 5-80 Area setting

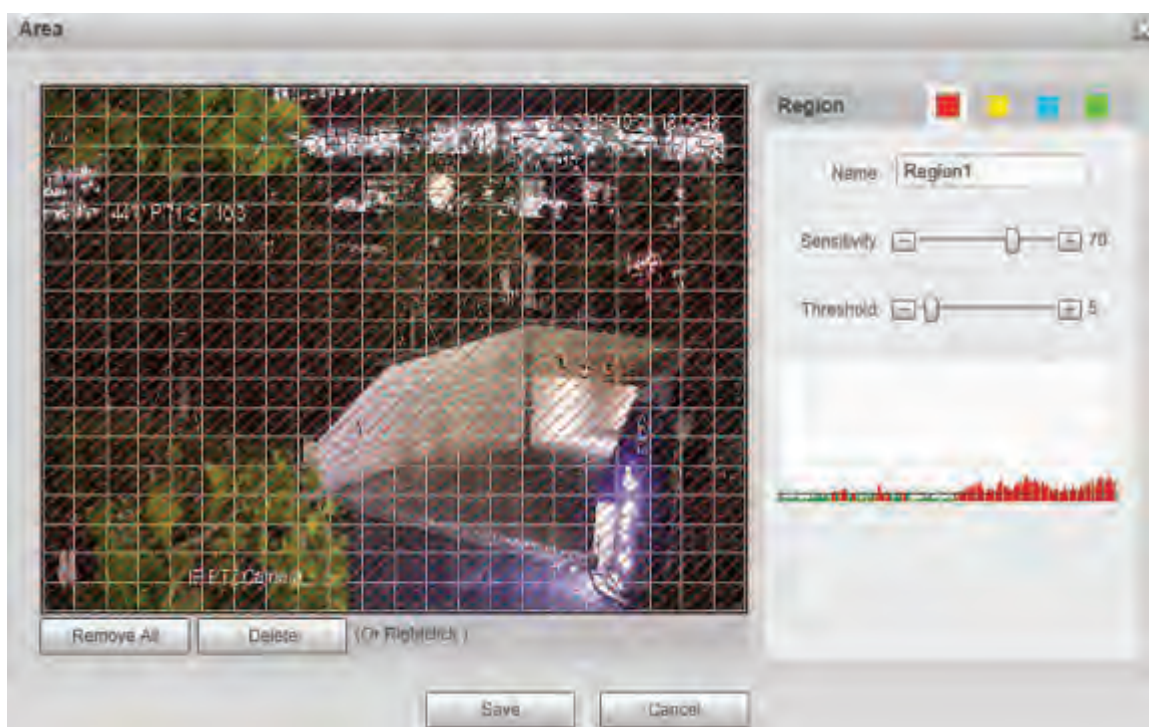


Table 5-24 Area setting parameter description

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 5-25 Video detection parameter description

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

Parameter	Description
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 interface.
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 check box, 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 check box, 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 "5.5.1.2 Snapshot."

Step 3 Click **Save**.

5.4.1.2 Video Tamper

Alarms will be triggered if there is video tampering.

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

The **Video Tamper** interface is displayed. See Figure 5-81.

Figure 5-81 Video tamper settings

Motion Detection | **Video Tamper** | Scene Changing

☐ Enable

Period Setting

☒ Record

Record Delay s (10~300)

☒ Relay-out 1 2

Alarm Delay s (10~300)

☐ Send Email

☐ PTZ

☒ Snapshot

Default Refresh Save

Step 2 Select the **Enable** check box, and then configure parameters as needed.



For parameters configuration, see "5.4.1.1 Motion Detection."

Step 3 Click **Save**.

5.4.1.3 Scene Changing

Alarms will be triggered if there is scene changing.

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

The **Scene Changing** interface is displayed. See Figure 5-82.

Figure 5-82 Scene changing settings

Motion Detection | Video Tamper | **Scene Changing**

☐ Enable

Period Setting

☒ Record

Record Delay s (10~300)

☒ Relay-out 1 2

Alarm Delay s (10~300)

☐ Send Email

☐ PTZ

☒ Snapshot

Default Refresh Save

Step 2 Select the **Enable** check box, and then configure parameters as needed.



For parameters configuration, see "5.4.1.1 Motion Detection."

Step 3 Click **Save**.

5.4.2 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.

Preparation

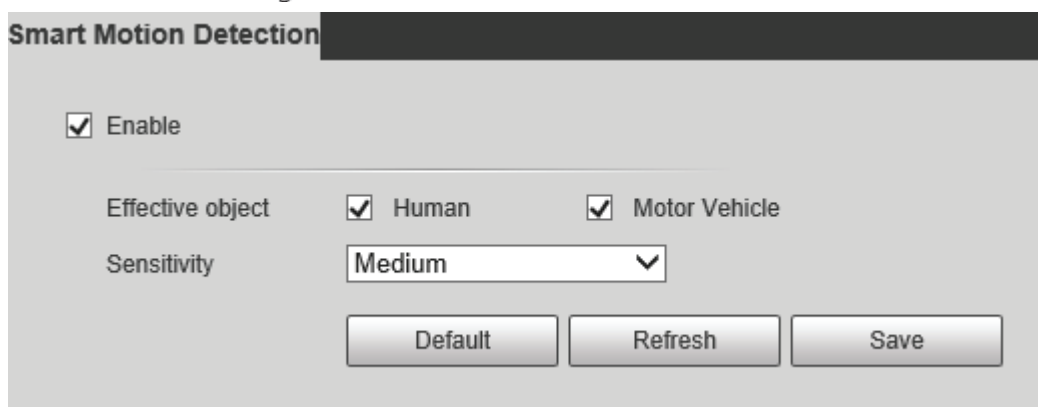
- Select **Setting > Event > Video Detection > Motion Detection**, and then enable the motion detection function.
- Set the arming period and detection area. The sensitivity of each region is larger than 0, and the threshold is not equal to 100.

Procedure

Step 4 Select **Setting > Event > Smart Motion Detection**.

The **Smart Motion Detection** interface is displayed. See Figure 5-83.

Figure 5-83 Smart motion detection



The screenshot shows the 'Smart Motion Detection' configuration window. At the top, the title 'Smart Motion Detection' is visible. Below the title, there is a section with a checked checkbox labeled 'Enable'. Underneath, there are two checkboxes for 'Effective object': 'Human' and 'Motor Vehicle', both of which are checked. Below these, there is a 'Sensitivity' dropdown menu currently set to 'Medium'. At the bottom of the window, there are three buttons: 'Default', 'Refresh', and 'Save'.

Step 5 Select the **Enable** check box, and then the **Smart Motion Detection** is enabled.

Step 6 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.

Step 7 Click **Save**.

5.4.3 Audio Detection

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

The **Audio Detection** interface is displayed. See Figure 5-84.

Figure 5-84 Audio detection settings

Step 2 Configure parameters as needed. For the parameter description, see Table 5-26.

Table 5-26 Audio detection parameter description

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.
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 "5.4.1.1 Motion Detection."

Step 3 Click **Save**.

5.4.4 Smart Plan

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

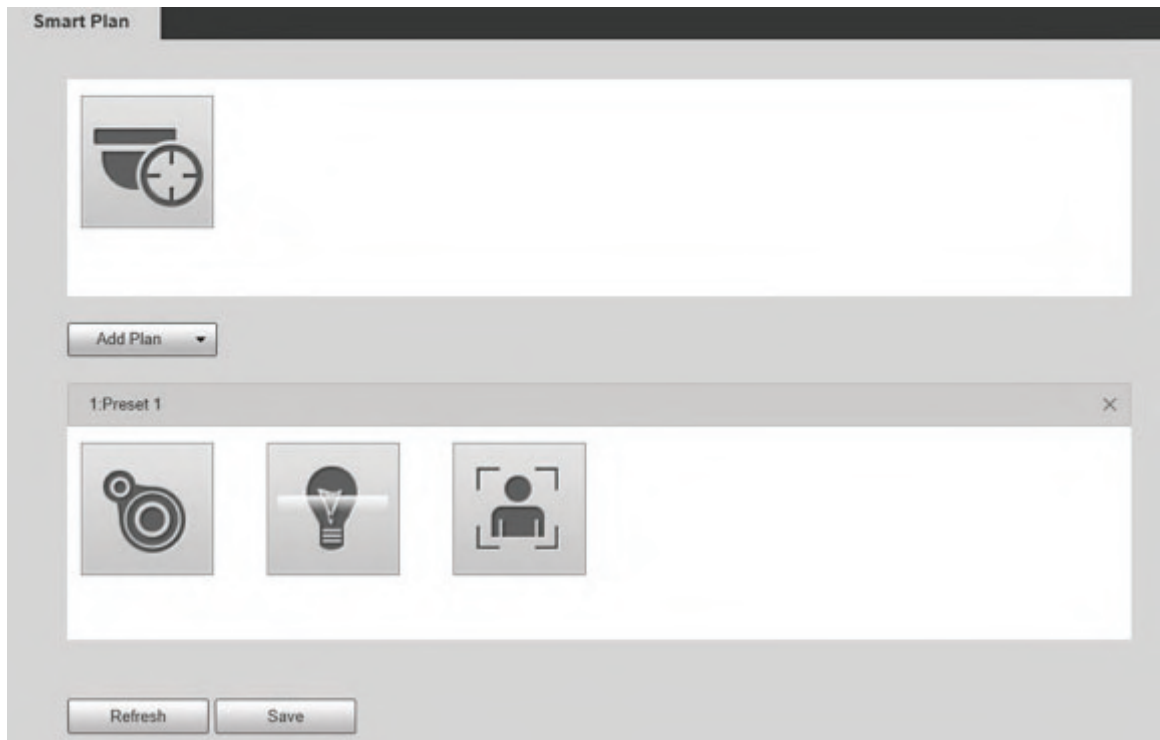


Before configuring the smart plan, you need to set presets in advance. For setting methods, see "5.3.2.1 Preset."

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

The **Smart Plan** interface is displayed.

Figure 5-85 Smart plan (1)

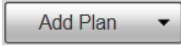


Step 2 (Optional) Click  to enable **Auto Tracking**.

When enabling auto tracking, you do not need to configure smart plans, and the Device perform 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.



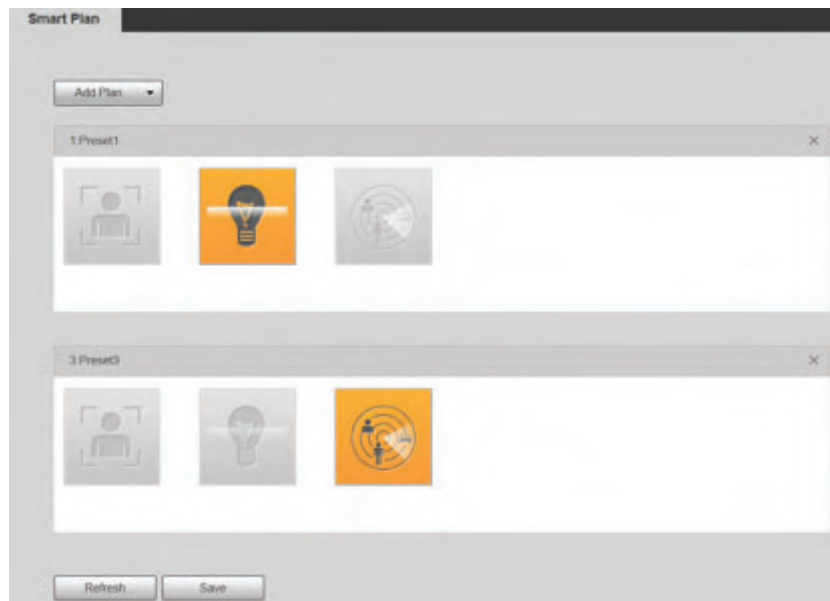
It is recommended to disable auto tracking when alarm track is enabled to avoid disordered tracking.

Step 3 Click  to select the presets to be configured.

Step 4 Select smart plans as needed.

The selected function will be highlighted. See Figure 5-86. Click it again to cancel the selection.

Figure 5-86 Smart plan (2)



Step 5 Click **Save**.

5.4.5 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."

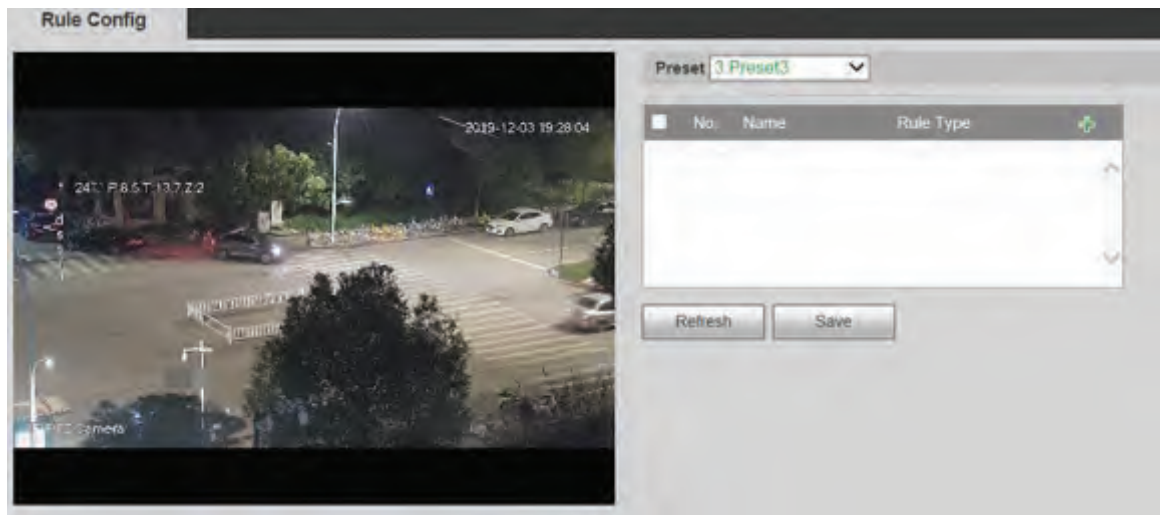
5.4.5.1 Rule Config

Set smart rules. Follow these steps to complete the configuration.

Step 1 Select **Setting > Event > IVS > Rule Config**.

The **Rule Config** interface is displayed. See Figure 5-87.

Figure 5-87 Adding smart rules



Step 2 Select the presets to be configured with smart rules.

Step 3 Click  to add smart rules.



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

Step 4 Click **Save**.

5.4.5.1.1 Tripwire

Alarms are triggered when the target crosses the warning line in the defined direction.

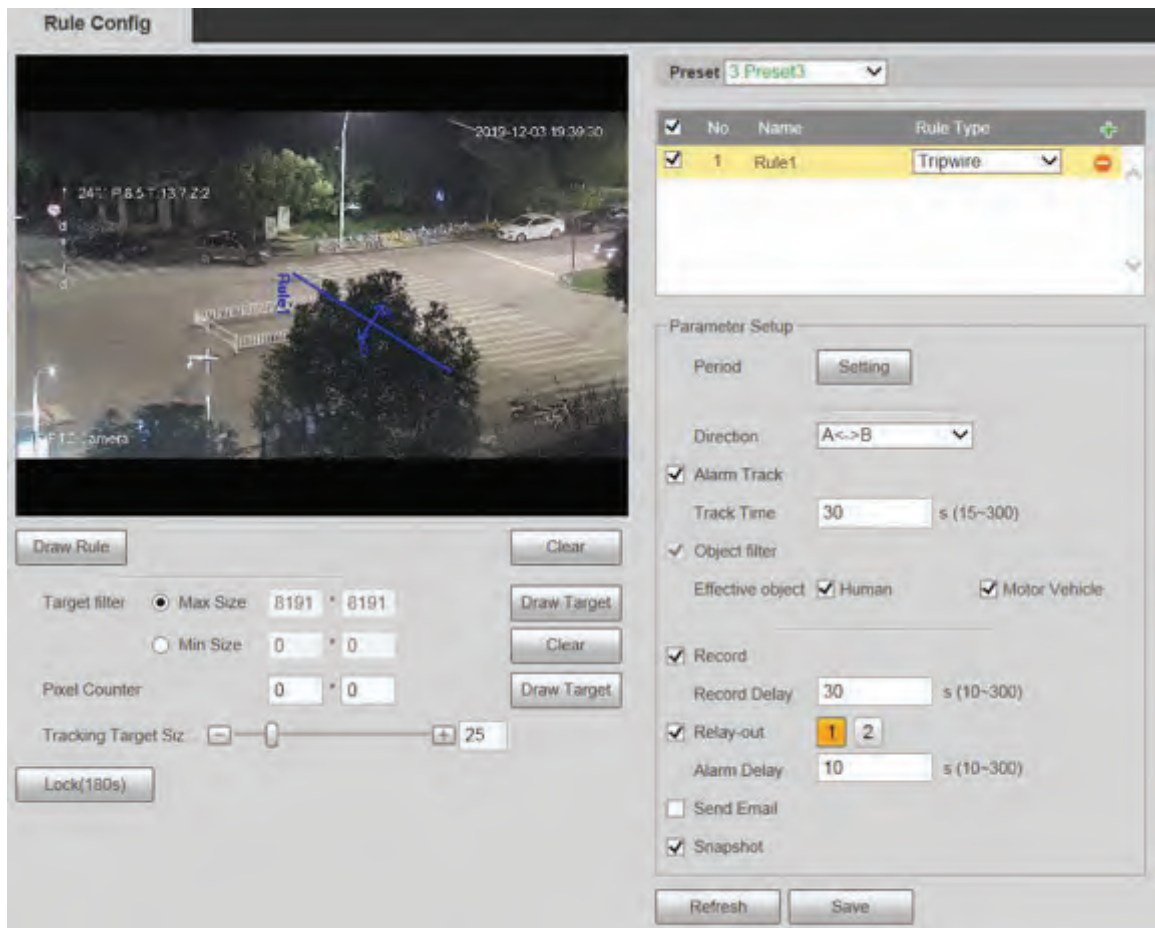
It requires certain stay time and moving space for the target to be confirmed, so you need to leave some space at both sides of the warning line during configuration and do not draw it near obstacles.

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

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

The configuration interface is displayed. See Figure 5-88.

Figure 5-88 Tripwire rule settings



Step 2 Click **Draw Rule**, and you can draw rules on the monitoring screen. For parameter description, see Table 5-27.



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

Table 5-27 Rule drawing parameter description

Parameter	Description
Max Size	Set the size range of detection targets to be filtered, and select the maximum or minimum size.
Min Size	- 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.
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.
Lock/Unlock	Enter the rule configuration interface, 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.  The locking function only takes effect in the rule configuration interface. After switching to the Live interface, the Device can track the target normally.

Step 3 Configure parameters as needed. For the parameter description, see Table 5-28.

Table 5-28 Tripwire parameter description

Parameter	Description
Period	 Set the alarming period to enable alarm events in the period you set. 1. Click Setting, and then the Period interface is displayed. 2. Enter the time value or press and hold the left mouse button, and drag directly on the setting interface. There are six periods for setting each day. Select the check box next to the period, and the set period will be effective. 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 check box next to the day to set it separately). 4. After completing the setting, click Save to return to the rule configuration interface.
Direction	Configure the tripwire direction. You can select A->B , B->A or A<->B .
Alarm Track	Select the check box, and there will be alarm tracking when an smart rule is triggered.
Track Time	Set the alarm tracking time.
Record	Select the check box, 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 in the Record Control interface.
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 check box, 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 check box, 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 check box, and the system will automatically take snapshots in case of alarms. You need to set snapshot period in Storage > Schedule .

Step 4 Click **Save**.

5.4.5.1.2 Intrusion

Intrusion includes crossing areas and in-area functions.

- Crossing area means an alarm will be triggered when a target enters or leaves the area.
- In-area function means an alarm will be triggered when a specified number of targets appear in a set alarming area at a given time. In-area function only counts the number of targets in the detection area, regardless of whether they are the same targets.
- For the reporting time interval of the in-area functions, the system will trigger the first alarm and then detect whether the same event occurs in the interval period. If no same event occurs in this period, the alarm counter will be cleared.

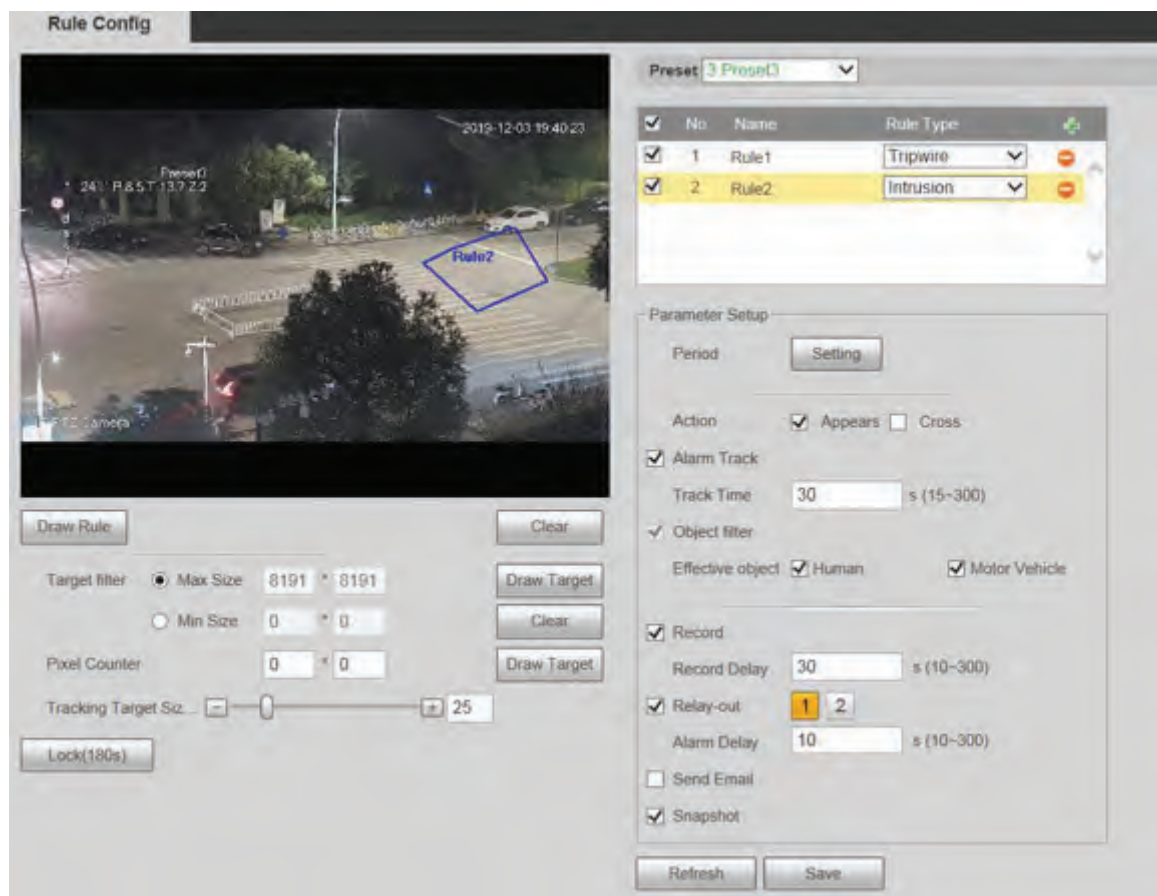
Similar to the warning line, to detect an entry/exit event, a certain movement space should be reserved at the periphery of the area line.

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

Step 1 Select **Intrusion** from the **Rule Type** list.

The configuration interface is displayed. See Figure 5-89.

Figure 5-89 Intrusion settings



Step 2 Click **Draw Rule**, and you can draw rules on the monitoring screen. For parameter description, see Table 5-27.



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

Step 3 Configure parameters as needed. For the parameter description, see Table 5-29.

Table 5-29 Intrusion parameter description

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 "5.4.5.1.1 Tripwire."

Step 4 Click **Save**.

5.4.5.1.3 Abandoned Object

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

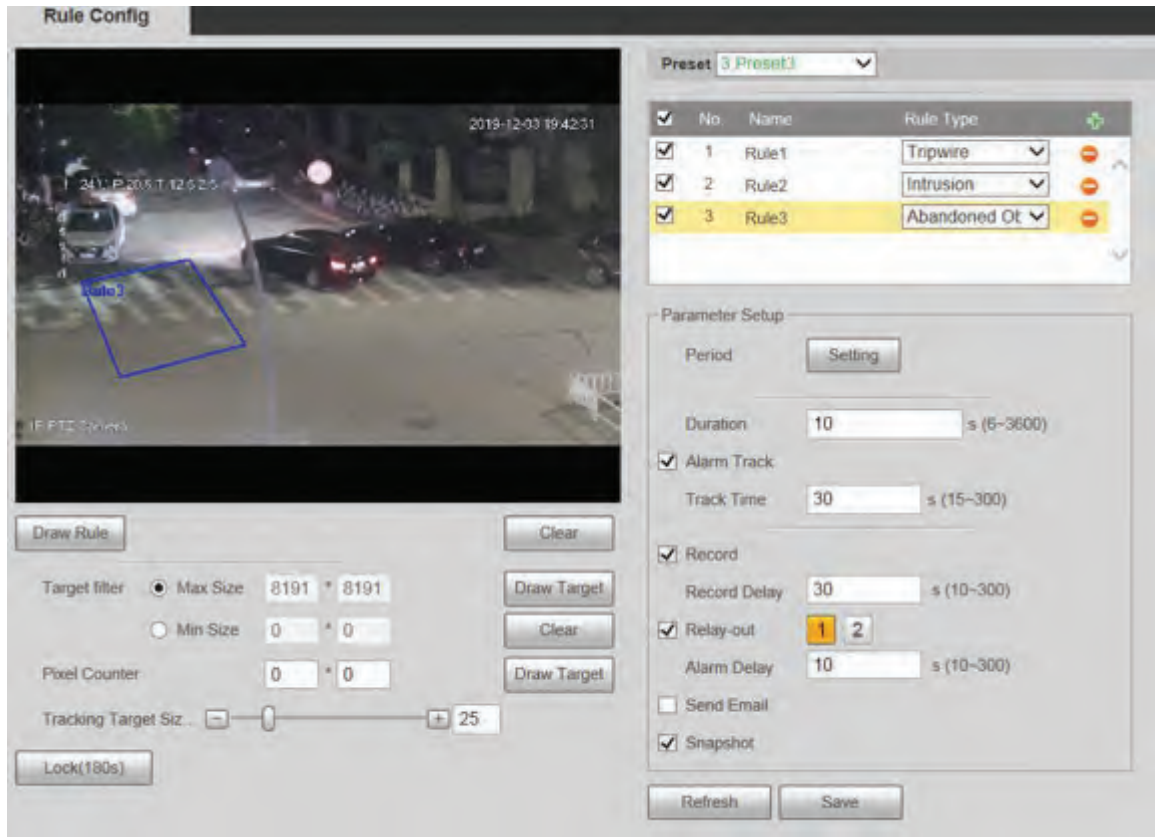
Pedestrians or vehicles that stay for too long would be regarded as abandoned objects. To filter out such alarms, you can use **Target filter**. In addition, the duration can be properly extended to avoid false alarm due to a short stay of people.

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.

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

The configuration interface is displayed. See Figure 5-90.

Figure 5-90 Abandoned object settings



Step 2 Click **Draw Rule**, and you can draw rules on the monitoring screen. For parameter description, see Table 5-27.



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

Step 3 Configure parameters as needed. For the parameter description, see Table 5-30.

Table 5-30 Abandoned object parameter description

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

For other parameters, see "5.4.5.1.1 Tripwire."

Step 4 Click **Save**.

5.4.5.1.4 Missing Object

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

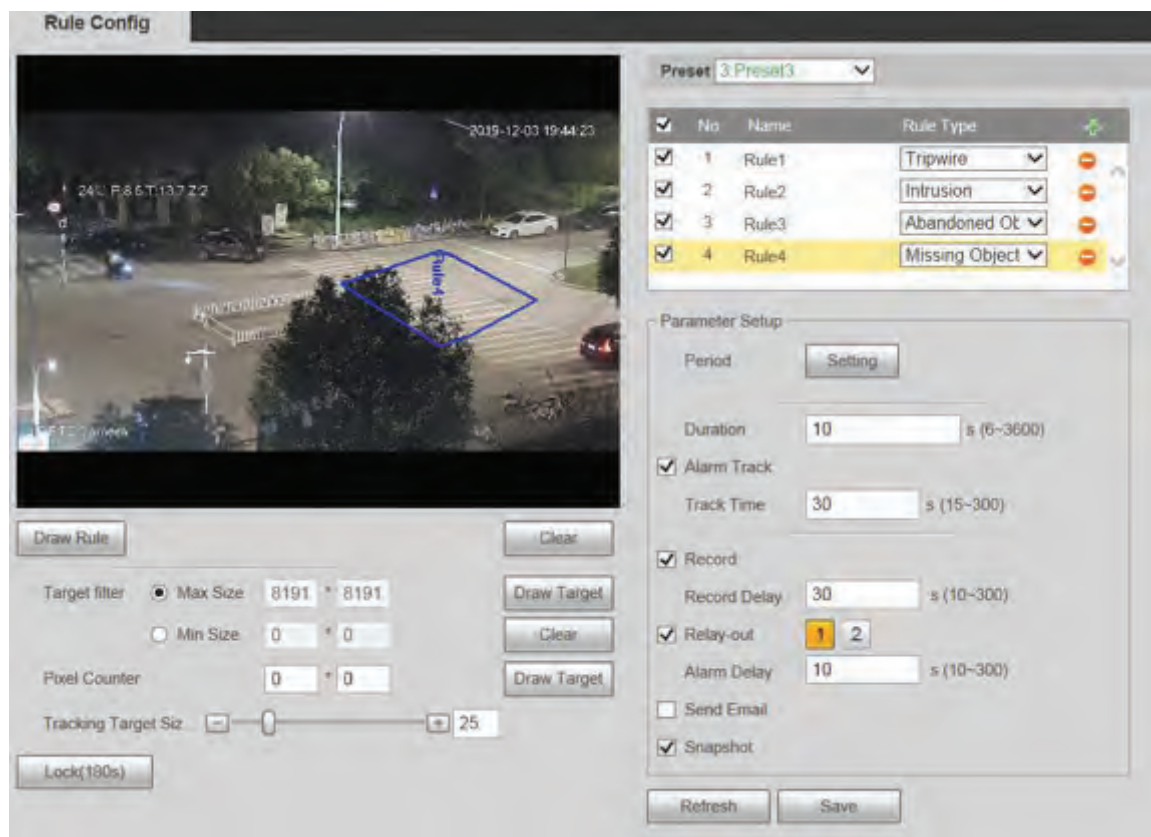
The system analyzes static areas from the foreground, and determines whether it is missing object or abandoned object from the similarity of its foreground and background. When the time exceeds the set period, an alarm is triggered.

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.

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

The configuration interface is displayed. See Figure 5-91.

Figure 5-91 Missing object setting



Step 2 Click **Draw Rule**, and you can draw rules on the monitoring screen. For parameter description, see Table 5-27.



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

Step 3 Configure parameters as needed. For the parameter description, see Table 5-31.

Table 5-31 Missing object parameter description

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

For other parameters, see "5.4.5.1.1 Tripwire."

Step 4 Click **Save**.

5.4.6 Face Recognition



- Select **Setting > Event > Smart Plan**, and then enable face recognition.

- This function is available on select models.

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

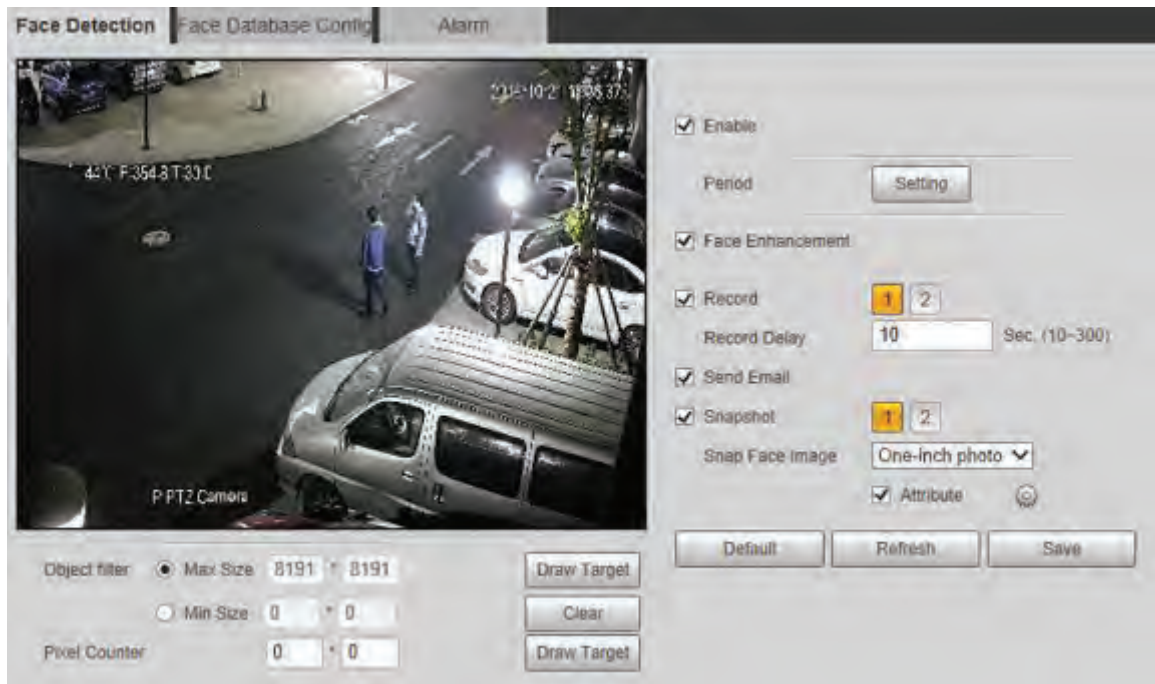
5.4.6.1 Face Detection

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

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

The **Face Detection** interface is displayed. See Figure 5-92.

Figure 5-92 Face detection interface



Step 2 Select **Enable**, and you can enable the face detection function.

Step 3 Configure parameters as needed. For the parameter description, see Table 5-32.

Table 5-32 Face detection parameter description

Parameter	Description
Period	Alarm event will be triggered only within the defined time period. See "5.4.1.1 Motion Detection."
Face Enhancement	Select Face Enhancement to preferably guarantee clear faces with low stream.
Record	Select Record , and the system records video when alarms are triggered.  To enable video recording, you need to make sure that: • The motion detection recording is enabled. For details, see "5.5.1.1 Record." • The auto recording is enabled. For details, see "5.5.4 Record Control."
Record Delay	The video recording will not stop until the record delay time you set has passed.

Parameter	Description
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)."
Snapshot	Select Snapshot , and the system takes snapshot when alarms are triggered.  - Enable the motion detection snapshot first. For details, see "5.5.1.1 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 check box, click  , and then you can set the human attributes during face detection.

Step 4 Click **Save**.

5.4.6.2 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 pictures, and face modeling.

5.4.6.2.1 Adding Face Database

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

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

The **Face Database Config** interface is displayed. See Figure 5-93.

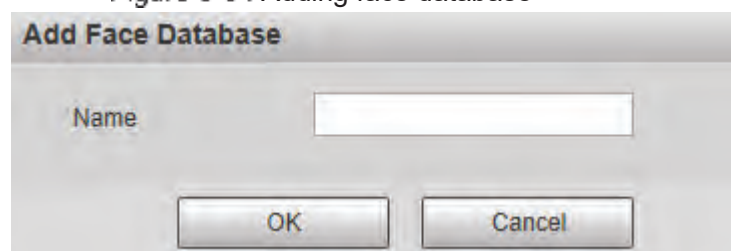
Figure 5-93 Face database config



Step 2 Click **Add Face Database**.

The **Add Face Database** interface is displayed. See Figure 5-94.

Figure 5-94 Adding face database

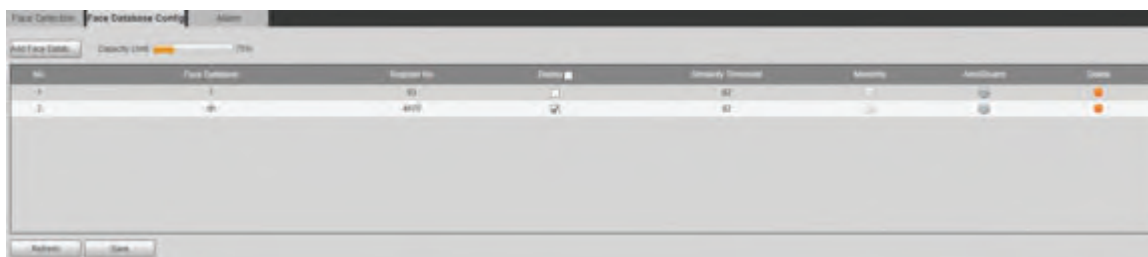


Step 3 Set face database name.

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

The added face database is displayed. See Figure 5-95.

Figure 5-95 Adding face database completed



Step 5 Configure parameters as needed. For the parameter description, see Table 5-33.

Table 5-33 Face database config parameter description

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 interface.
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. See "5.4.1.1 Motion Detection."
Delete	Delete the selected face database.

5.4.6.2.2 Adding Face Pictures

Add face pictures to the created face database. Manual addition and batch import are supported.

Manual Addition

Add a single face picture. Use this method when registering a small number of face pictures.

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

The **Face Database Config** interface is displayed.

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

The interface is displayed. See Figure 5-96.

Figure 5-96 More info

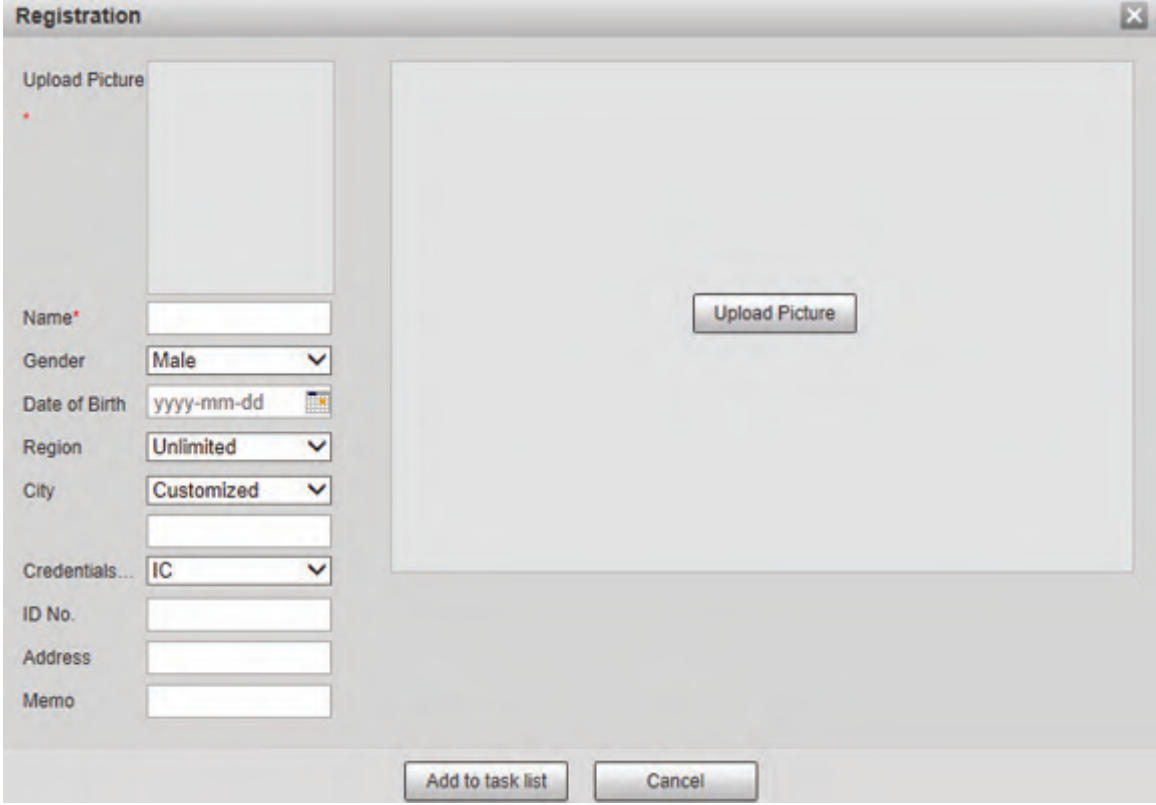


Set filtering conditions as needed, and then click **Search**. The search result is displayed.

Step 3 Click **Registration**.

The **Registration** interface is displayed. See Figure 5-97.

Figure 5-97 Registration interface



The image shows a software window titled "Registration" with a close button in the top right corner. On the left side, there is a vertical list of input fields: "Upload Picture" (with a red asterisk and a small square icon), "Name*" (text input), "Gender" (dropdown menu showing "Male"), "Date of Birth" (text input with "yyyy-mm-dd" placeholder and a calendar icon), "Region" (dropdown menu showing "Unlimited"), "City" (dropdown menu showing "Customized"), "Credentials..." (dropdown menu showing "IC"), "ID No." (text input), "Address" (text input), and "Memo" (text input). On the right side, there is a large rectangular area for image upload, containing a button labeled "Upload Picture". At the bottom of the window, there are two buttons: "Add to task list" and "Cancel".

Step 4 Click **Upload Picture**.

Import the face pictures to be uploaded. The interface is displayed. See Figure 5-98.



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

Figure 5-98 Addition completed



The Registration window displays a form for adding a new task. On the left, there is a vertical list of fields: Name*, Gender (Male), Date of Birth (yyyy-mm-dd), Region (Unlimited), City (Customized), Credentials... (IC), ID No., Address, and Memo. Above these fields is a small thumbnail of a face picture. To the right of the thumbnail is a larger preview window showing the selected face picture. At the bottom of the window are two buttons: 'Add to task list' and 'Cancel'.

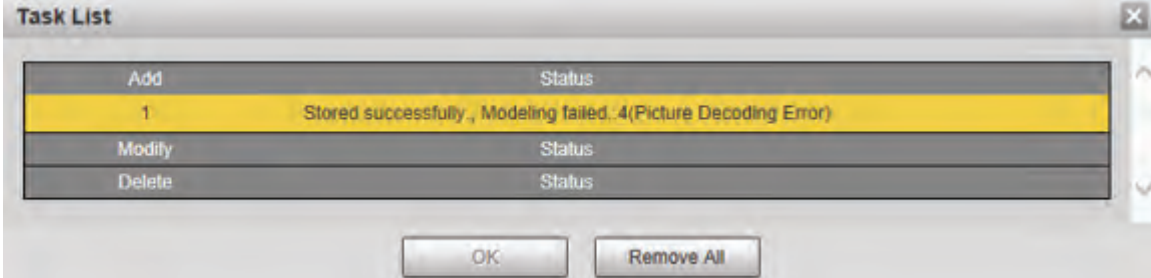
Step 5 Fill in face picture information as needed.

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

Step 7 Click  **Task list 1**.

The **Task List** interface is displayed. See Figure 5-99.

Figure 5-99 Task list addition completed



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

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

At the bottom of the window are two buttons: 'OK' and 'Remove All'.



Click **Remove All**, and you can remove all the tasks.

Batch Registration

Import multiple face pictures in batch. Use this method when registering a large number of face pictures.

Before importing pictures in batches, name the face pictures 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"). For naming rules, see Table 5-34.



Name is required and the rest are optional.

Table 5-34 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.

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

The **Face Database Config** interface is displayed.

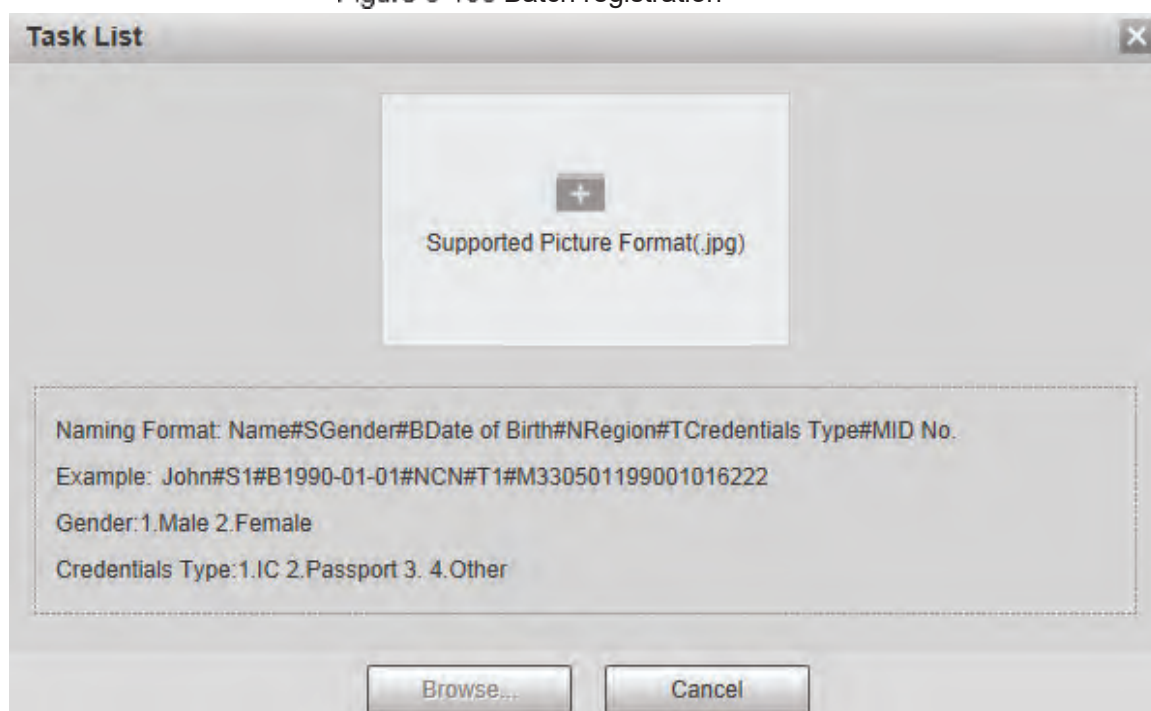
Step 2 Click  **More Info** for the face database to be configured.

The **Face Database** interface is displayed.

Step 3 Click **Batch Registration.**

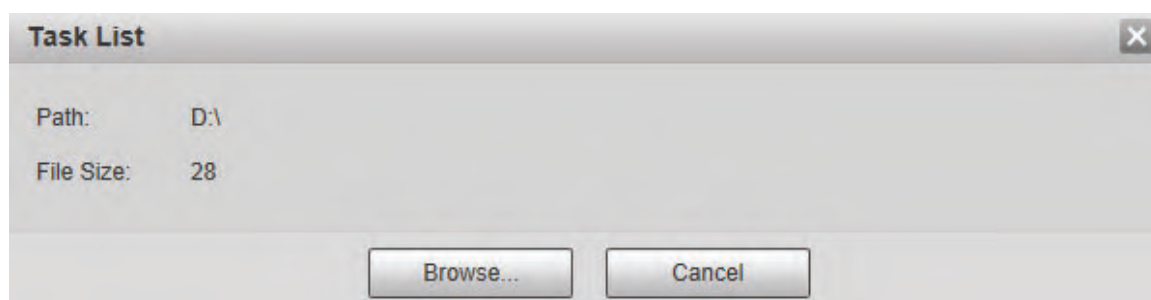
The **Task List** interface is displayed. See Figure 5-100.

Figure 5-100 Batch registration



Step 4 Click  to select the file path.

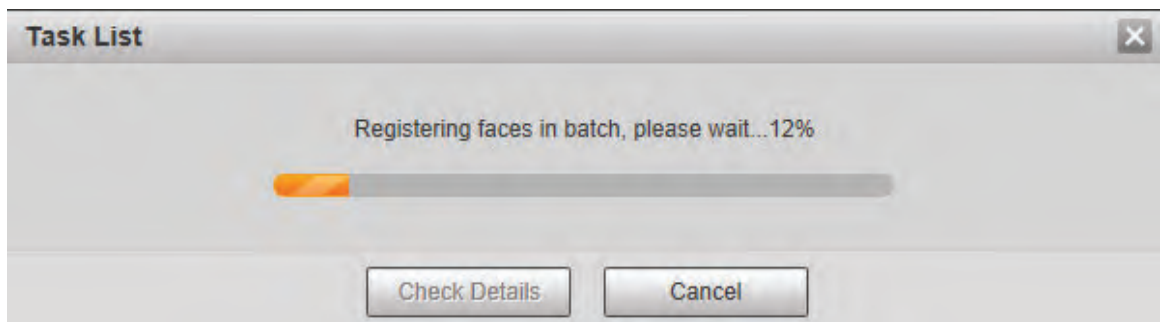
Figure 5-101 Batch registration



Step 5 Click **Browse.**

The registering interface is displayed. See Figure 5-101.

Figure 5-102 Registering



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

5.4.6.2.3 Managing Face Pictures

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

Modifying Face Information

On the **Face Database Config** interface, move the mouse pointer to the face picture or person information line. Click  or , and the **Registration** interface is displayed. See Figure 5-103. After modifying the face picture information as needed, click **Add to task list**.

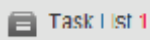
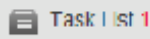
Figure 5-103 Registration interface

A "Registration" dialog box with a close button (X) in the top right corner. On the left side, there is a section titled "Upload Picture" with a small red dot below it, followed by a placeholder image of a man's face. Below the image are several form fields: "Name*" (text input), "Gender" (dropdown menu), "Date of Birth" (text input 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 "Other" selected), "ID No." (text input), "Address" (text input), and "Memo" (text input). On the right side of the dialog is a large empty rectangular area with an "Upload Picture" button centered within it. At the bottom of the dialog are two buttons: "Add to task list" and "Cancel".

Deleting Face Pictures

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

- Single deletion: Move the mouse pointer to the face picture or people information line, and then click  or  to delete the face picture.

- Batch deletion: Move the mouse pointer to the face picture or people information line, and then click  at the upper right corner of the face pictures, 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 pictures.
- Delete all: When viewing face pictures in a list, click  on people information line (or select **All** when viewing face pictures in pictures), click **Add to the delete list**, click , and then click **OK** to delete all face pictures.

5.4.6.2.4 Face Modeling

Extract and import the relevant information of face pictures into the database through face modeling, and create a face feature mode for smart detection such as face comparison.



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

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

The **Face Database Config** interface is displayed.

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

The face database interface is displayed. See Figure 5-104.

Figure 5-104 Face database interface



Step 3 Choose the face pictures for modeling as needed.



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

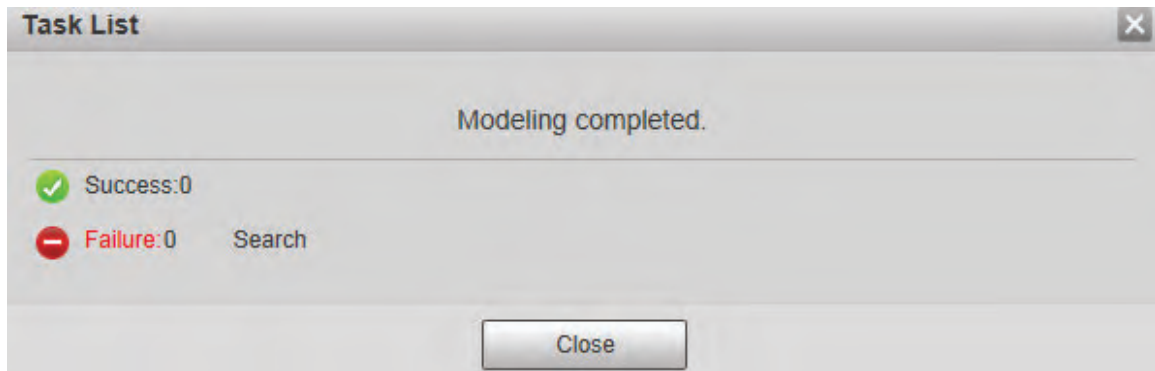
- Modeling All

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

- Selective Modeling

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

Figure 5-105 Modeling completed



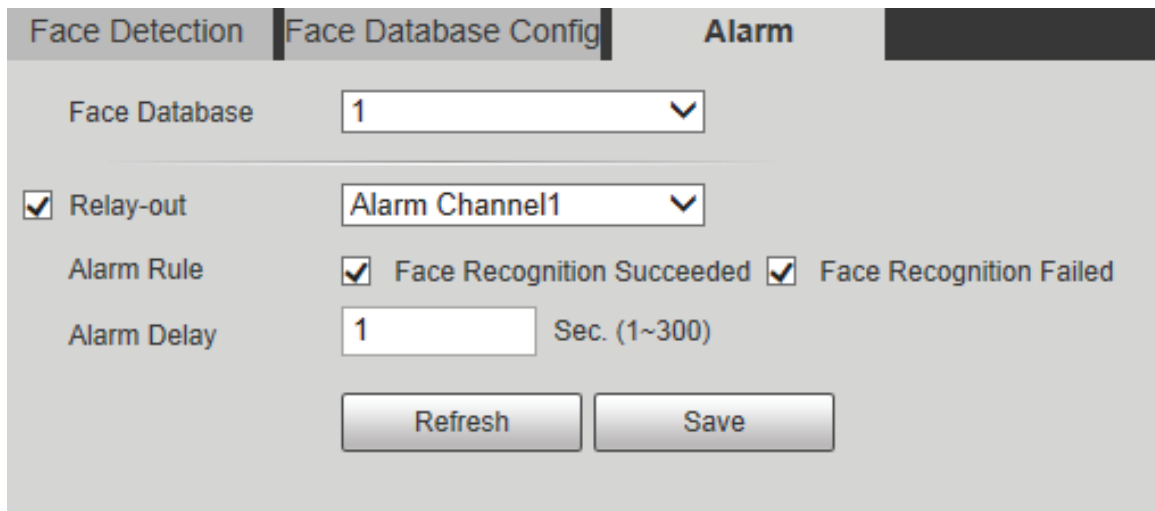
5.4.6.3 Alarm Linkage

Set the alarm linkage mode for face comparison.

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

The **Alarm** interface is displayed. See Figure 5-106.

Figure 5-106 Alarm linkage



Step 2 Configure parameters as needed. For the parameter description, see Table 5-35.

Table 5-35 Alarm linkage parameter description

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 check box, 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**.

5.4.7 People Counting



- 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.

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

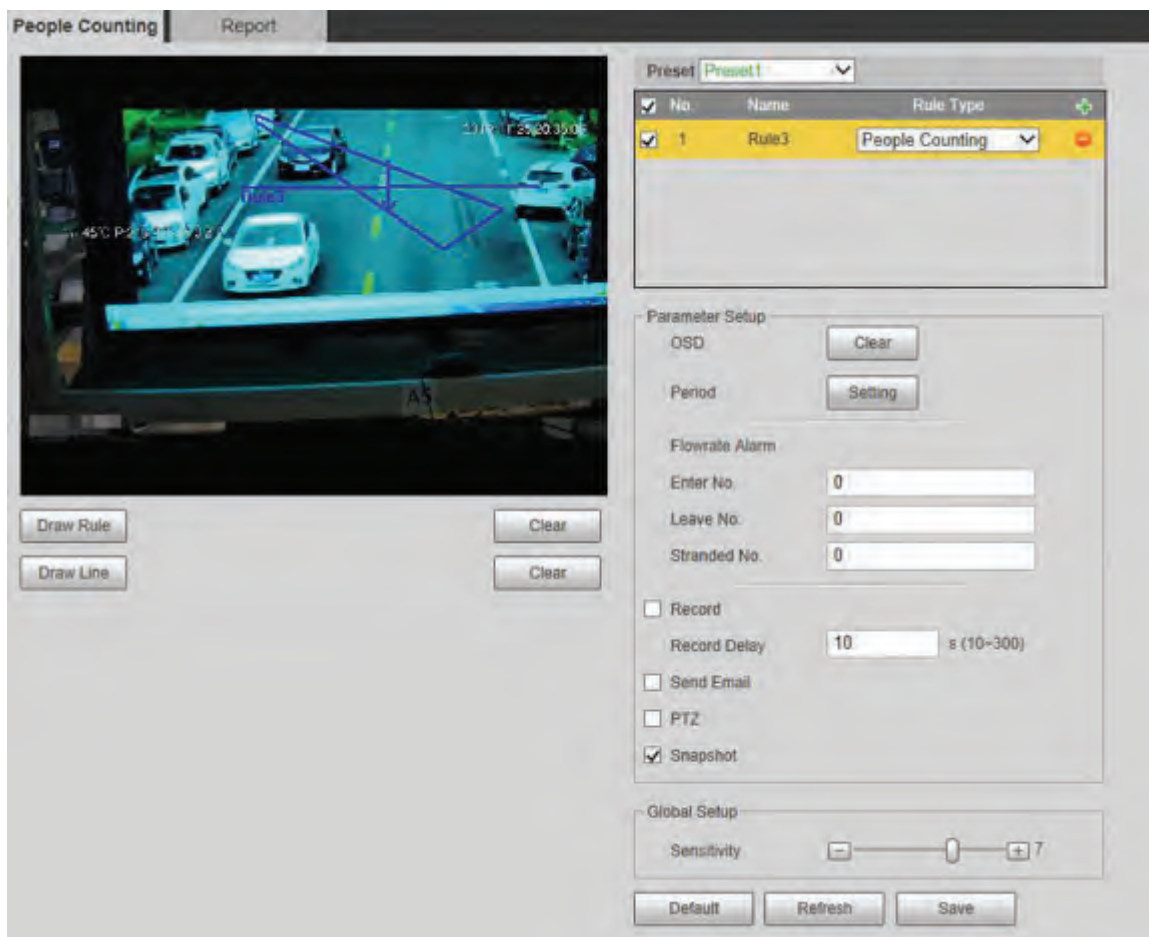
5.4.7.1 People Counting

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

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

The **People Counting** interface is displayed. See Figure 5-107.

Figure 5-107 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 Table 5-27.



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

Step 4 Configure parameters as needed. For the parameter description, see Table 5-36.

Table 5-36 People counting parameter description

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, refer to "5.4.5.1.1 Tripwire."

Step 5 Click **Save**.

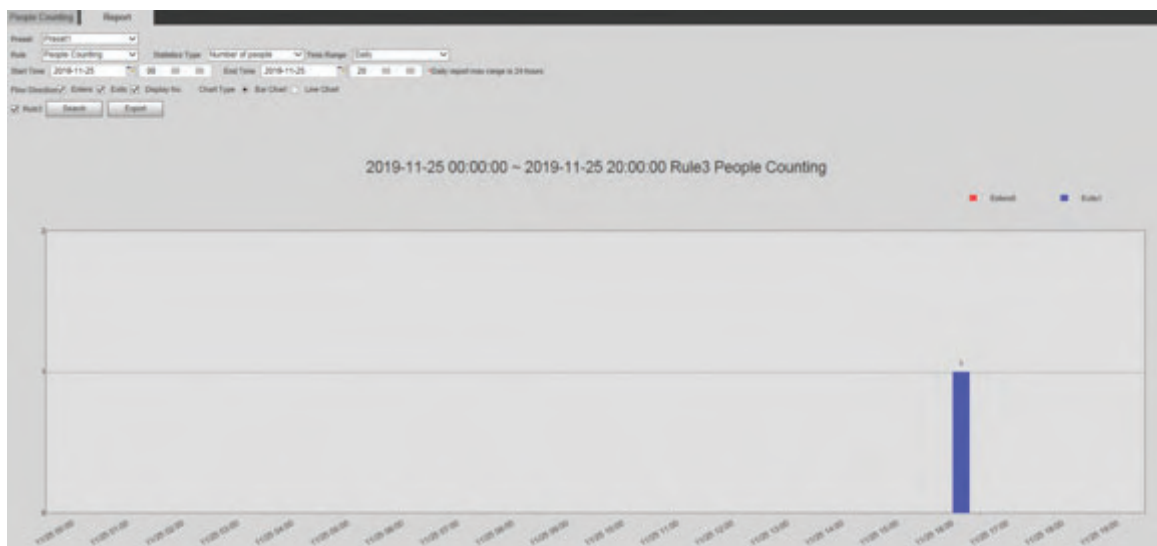
5.4.7.2 Report

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

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

The **Report** interface is displayed. See Figure 5-108.

Figure 5-108 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 click **Export** to export the report to local storage.

5.4.8 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 as needed.

- This function is available on select models.

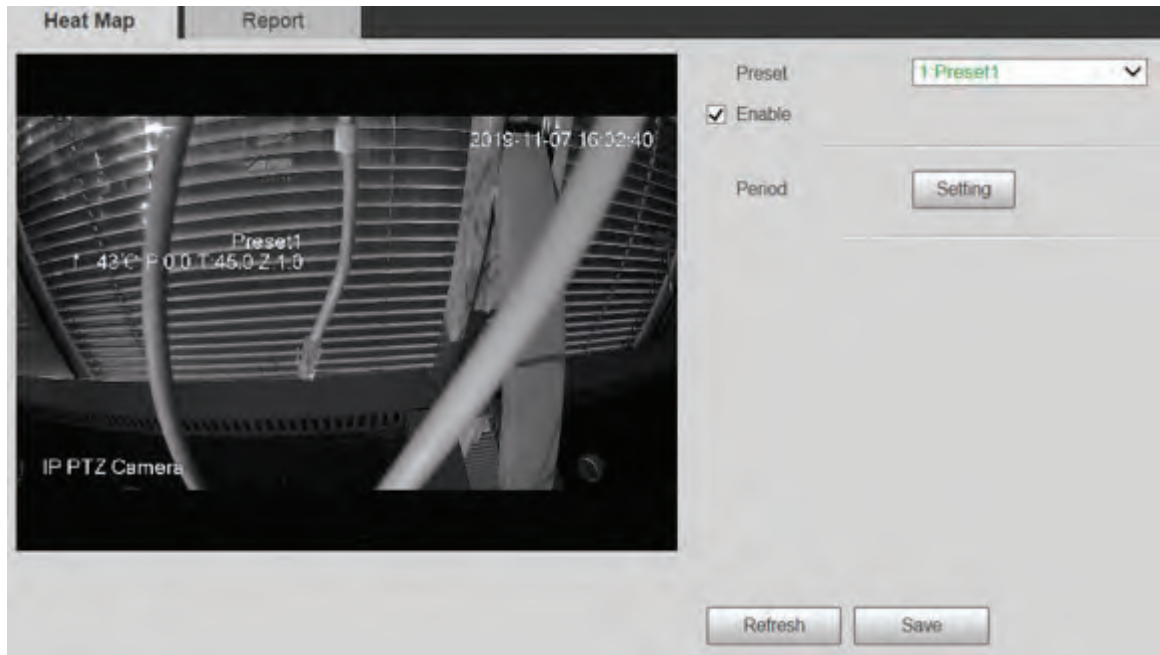
5.4.8.1 Heat Map

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

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

The **Heat Map** interface is displayed. See Figure 5-109.

Figure 5-109 Heat map interface



Step 2 Select the presets to be configured.

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

Step 4 Click **Setting** to set the arming period. For details, see "5.4.1.1 Motion Detection."

Step 5 Click **Save**.

5.4.8.2 Report

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

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

The **Report** interface is displayed.

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 interface. See Figure 5-110.

Figure 5-110 Report



5.4.9 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.

5.4.9.1 Scene Setting

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

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

The **Scene Set** interface is displayed. See Figure 5-111.

Figure 5-111 Video metadata–scene set



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 as needed.

- 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 parameters as needed. For parameter description, see Table 5-37.

Table 5-37 Scene set parameter description

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 check box to enable the OSD overlay. The statistics will be displayed on the Live interface 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 "5.4.5.1.1 Tripwire."

Step 6 Click **Save**.

5.4.9.2 Picture Overlay

Set the overlay information on the snapshot.

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

The **Picture** interface is displayed.

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

See Figure 5-112, Figure 5-113 and Figure 5-114.

Figure 5-112 Picture overlay–motor vehicle

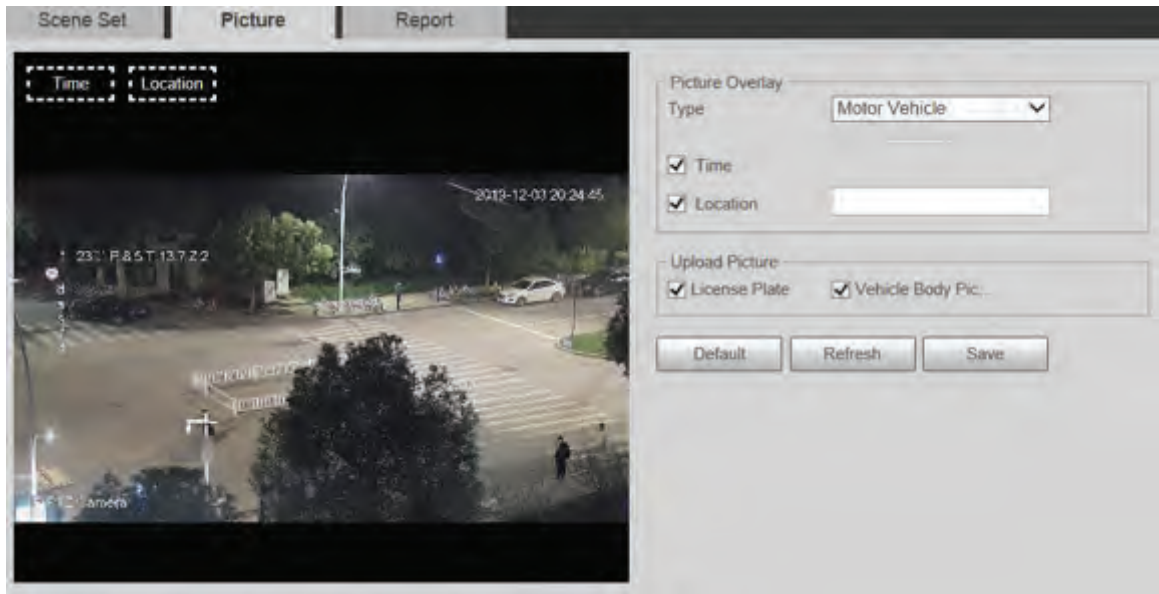


Figure 5-113 Picture overlay–non-motor vehicle

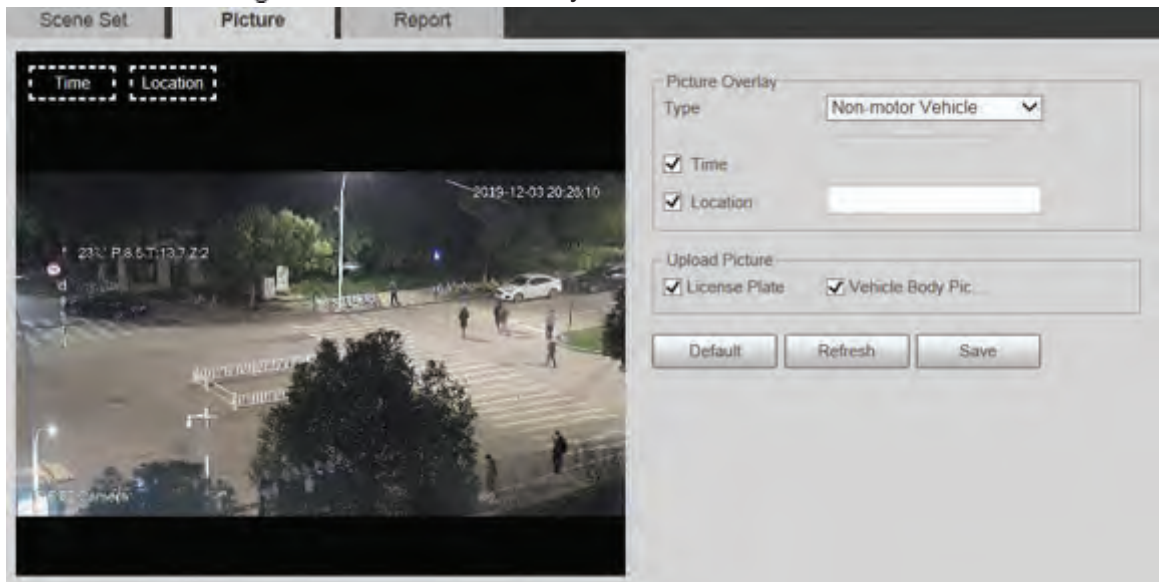
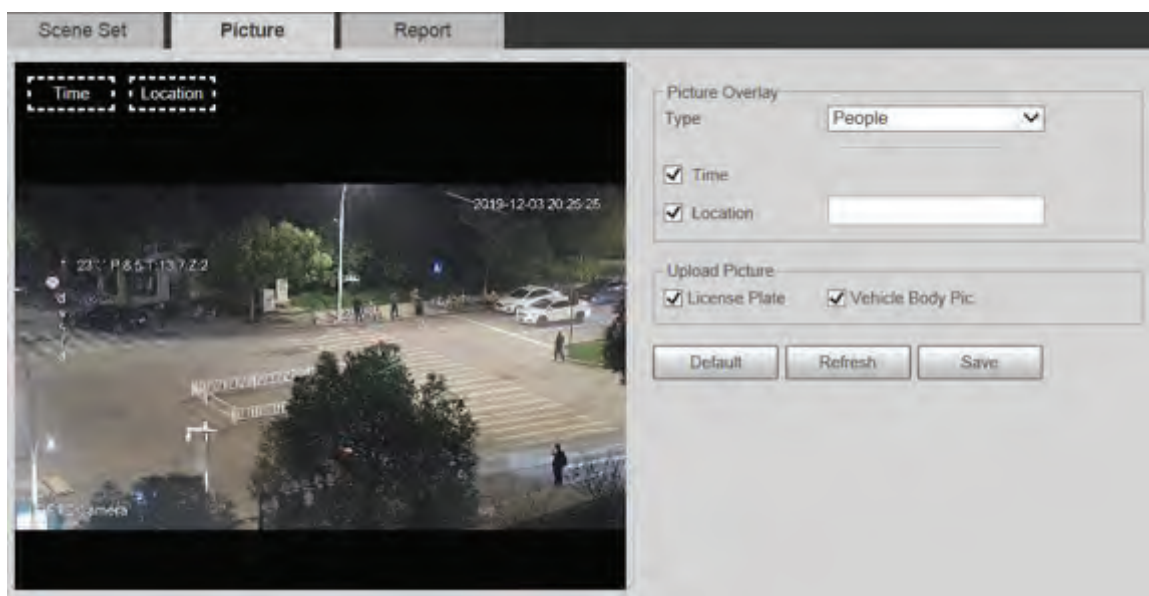


Figure 5-114 Picture overlay–people



Step 3 Select overlay information as needed.



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

Step 4 Click **Save**.

5.4.9.3 Report

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

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

The **Report** interface is displayed.

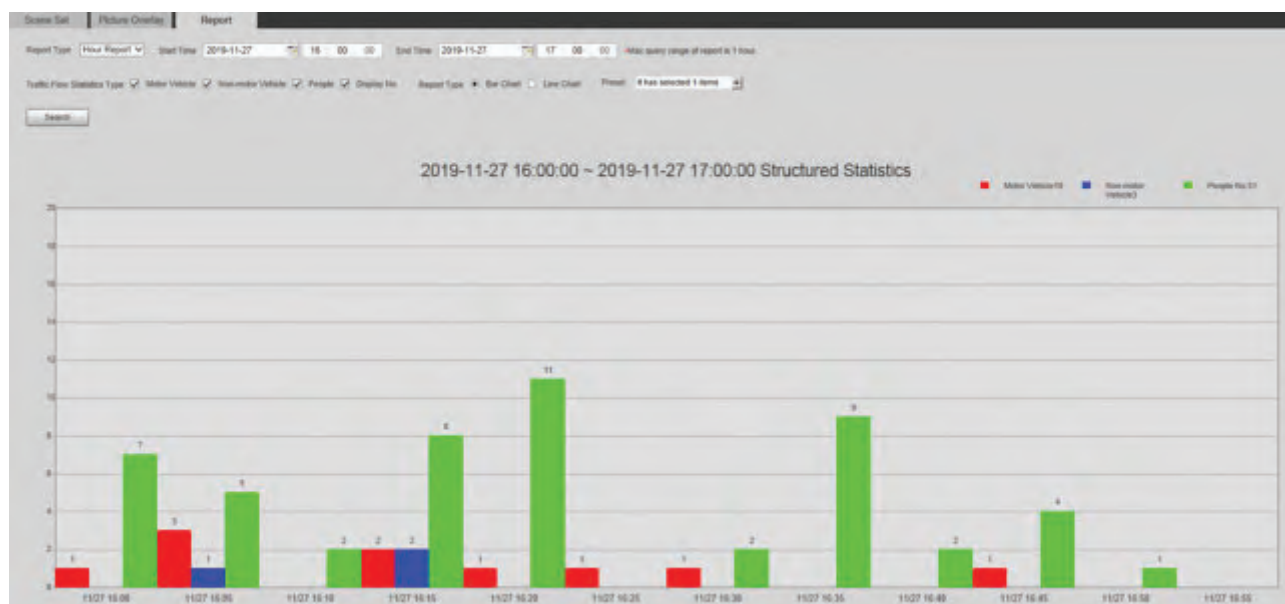
Step 2 Select the **Report Type**.

Step 3 Select the start time and end time for searching reports.

Step 4 Select the Traffic Flow Statistics Type.

Step 5 Click **Search** to generate reports. See Figure 5-115.

Figure 5-115 Video metadata report



5.4.10 Alarm

Step 1 Select **Setting > Event > Alarm**.
The **Alarm** interface is displayed. See Figure 5-116.

Figure 5-116 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

12

Alarm Delay

10

s (10~300)

☐ Send Email

☐ PTZ

☒ Snapshot

Default

Refresh

Save

Step 2 Configure parameters as needed. For parameter description, see Table 5-38.

Table 5-38 Alarm setting parameter description

Parameter	Description
Enable	Select the Enable check box, 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 "5.4.1.1 Motion Detection."

Step 3 Click **Save**.

5.4.11 Abnormality

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

5.4.11.1 SD Card

In case of an SD card exception, an alarm will be triggered. Follow these steps to complete the configuration.

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

The **SD Card** interface is displayed. See Figure 5-117, Figure 5-118, and Figure 5-119.

Figure 5-117 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' dropdown menu is set to 'No SD Card'. There are three checkboxes: 'Enable' (unchecked), 'Relay-out' (checked), and 'Send Email' (unchecked). The 'Relay-out' checkbox is accompanied by two buttons labeled '1' and '2'. Below these, the 'Alarm Delay' is set to '10' seconds, with a range of '(10~300)' indicated. At the bottom, there are three buttons: 'Default', 'Refresh', and 'Save'.

Figure 5-118 SD card error

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' dropdown menu is set to 'SD Card Error'. There are three checkboxes: 'Enable' (unchecked), 'Relay-out' (checked), and 'Send Email' (unchecked). The 'Relay-out' checkbox is accompanied by two buttons labeled '1' and '2'. Below these, the 'Alarm Delay' is set to '10' seconds, with a range of '(10~300)' indicated. At the bottom, there are three buttons: 'Default', 'Refresh', and 'Save'.

Figure 5-119 Capacity warning

The screenshot shows the 'SD Card' configuration tab. The 'Event Type' is set to 'Capacity Warning'. The 'Enable' checkbox is unchecked. The 'Capacity Limit' is set to 10, with a unit of % (0~99). The 'Relay-out' checkbox is checked, and the value is set to 1. The 'Alarm Delay' is set to 10, with a unit of s (10~300). The 'Send Email' checkbox is unchecked. At the bottom, there are three buttons: 'Default', 'Refresh', and 'Save'.

Step 2 Configure parameters as needed. For parameter description, see Table 5-39.

Table 5-39 SD card exception parameter description

Parameter	Description
Enable	Select the check box 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 "5.4.1.1 Motion Detection."

Step 3 Click **Save**.

5.4.11.2 Network Exception

In case of a network exception, an alarm will be triggered. Follow these steps to complete the configuration.

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

The **Network** interface is displayed. See Figure 5-120 and Figure 5-121.

Figure 5-120 Disconnection

The screenshot shows the 'Network' tab selected. The 'Event Type' 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, with '1' and '2' buttons next to it. The 'Alarm Delay' is set to 10 seconds. At the bottom are 'Default', 'Refresh', and 'Save' buttons.

Figure 5-121 IP conflict

The screenshot shows the 'Network' tab selected. The 'Event Type' 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, with '1' and '2' buttons next to it. The 'Alarm Delay' is set to 10 seconds. At the bottom are 'Default', 'Refresh', and 'Save' buttons.

Step 2 Configure parameters as needed. See Table 5-40.

Table 5-40 Network exception parameter description

Parameter	Description
Enable	Select the check box to enable this function.



For other parameters, see "5.4.1.1 Motion Detection."

Step 3 Click **Save**.

5.4.11.3 Illegal Access

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

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

The **Illegal Access** interface is displayed. See Figure 5-122.

Figure 5-122 Illegal access

Step 2 Configure parameters as needed. For parameter description, see Table 5-41.

Table 5-41 Illegal access parameter description

Parameter	Description
Enable	Select the check box 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 "5.4.1.1 Motion Detection."

Step 3 Click **Save**.

5.4.11.4 Security Exception

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

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

The **Security Exception** interface is displayed. See Figure 5-123.

Figure 5-123 Security exception

Step 2 Configure each parameter as needed. For details, refer to "5.4.1.1 Motion Detection."

Step 3 Click **Save**.

5.5 Storage

5.5.1 Schedule

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



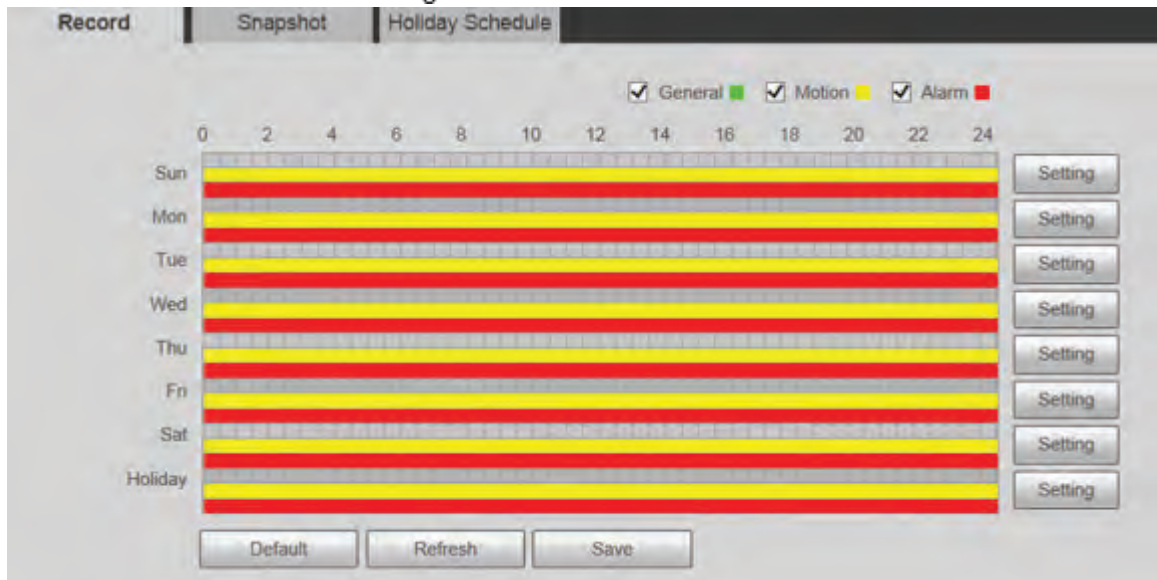
If the **Record Mode** is **Off**, the Device will not record or take snapshots according to the schedule.

5.5.1.1 Record

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

The **Record** interface is displayed. See Figure 5-124.

Figure 5-124 Record



Step 2 Select the day for recording from Monday to Sunday. Click **Setting** on the right, and the **Setting** interface is displayed. See Figure 5-125.

- Set the recording period as needed. 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** interface.

Figure 5-125 Record schedule setting

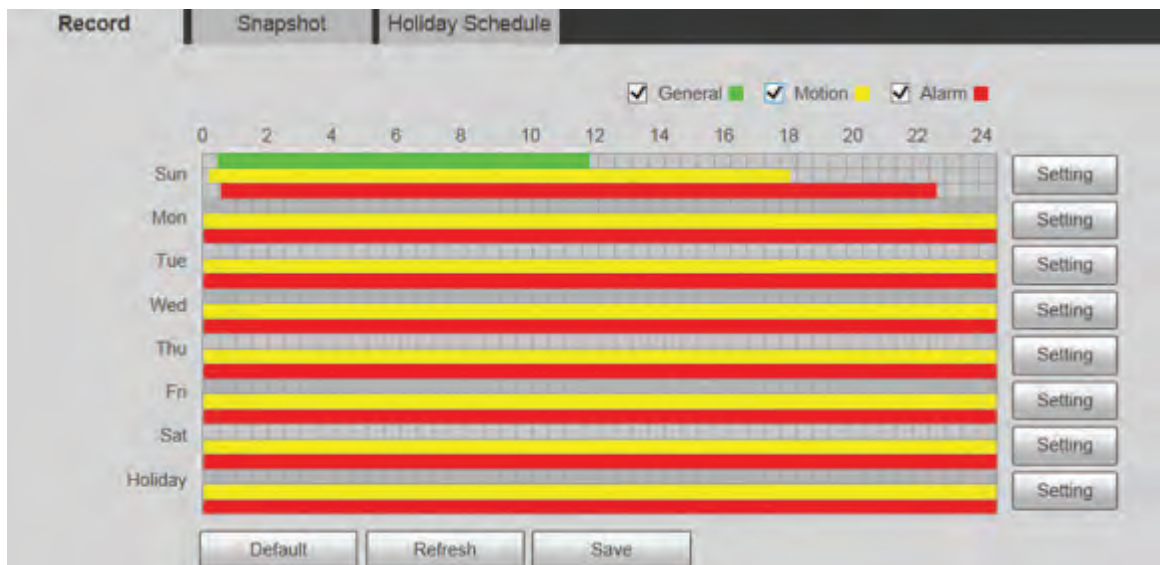
The 'Setting' window displays a configuration interface for recording schedules. At the top, there are checkboxes for days of the week: All, Sun (checked), Mon, Tue, Wed, Thu, Fri, Sat, and Holiday. Below this, there are six rows labeled Period1 through Period6. Each row contains two time selection fields (HH:MM:SS) separated by a hyphen, and three checkboxes: General, Motion, and Alarm. For Period1, the time range is 00:00:00 to 23:59:59, and all three checkboxes are checked. For Period2 through Period6, the time range is 00:00:00 to 23:59:59, and only the 'General' checkbox is checked. At the bottom of the window are 'Save' and 'Cancel' buttons.

Step 3 Click **Save** to return to the **Record** interface. See Figure 5-126.

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

- Green: Represents general recording.
- Yellow: Represents motion detection recording.
- Red: Represents the alarm recording.

Figure 5-126 Recording schedule setting completed



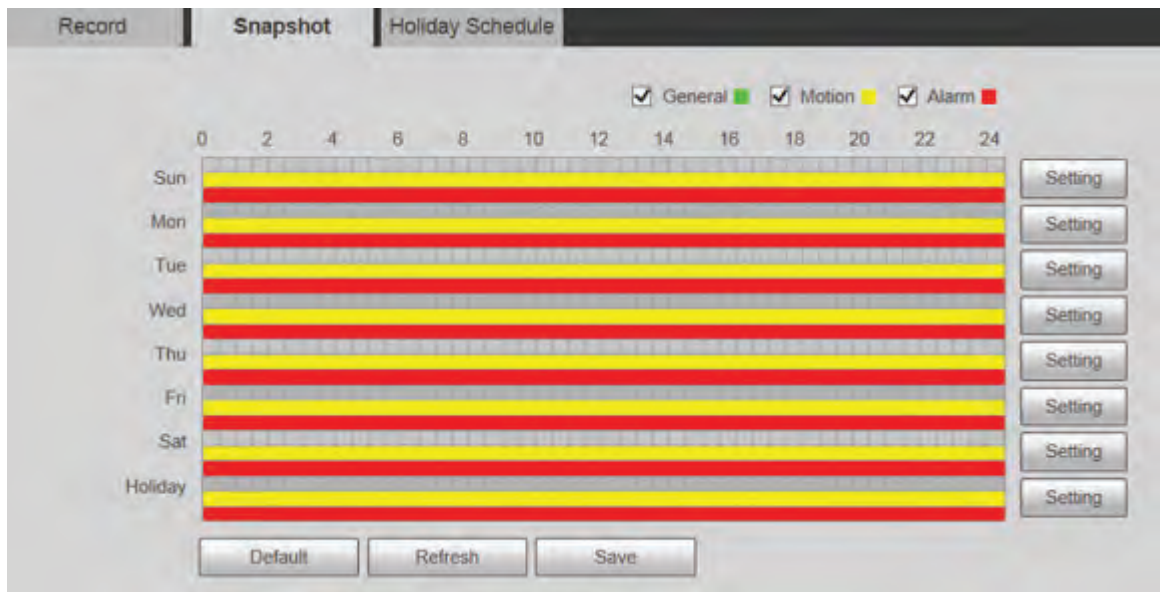
Step 4 On the **Record** interface, click **Save**, and the **Save Succeeded!** prompt will be displayed, which means the recording schedule has been set.

5.5.1.2 Snapshot

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

The **Snapshot** interface is displayed. See Figure 5-127.

Figure 5-127 Snapshot



Step 2 For the snapshot schedule settings, refer to Step 2 and Step 3 in "5.5.1.1 Record."

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

5.5.1.3 Holiday Schedule

You can set specific dates as holidays.

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

The **Holiday Schedule** interface is displayed. See Figure 5-128.

Figure 5-128 Holiday schedule

The screenshot shows a software interface for setting a holiday schedule. It features three tabs at the top: 'Record', 'Snapshot', and 'Holiday Schedule'. Below the tabs are two checkboxes, 'Record' and 'Snapshot', both of which are unchecked. The main area contains a 'Calendar' widget with a dropdown menu set to 'Dec'. The calendar grid shows days of the week (Sun to Sat) and dates (1 to 31). The date '1' is highlighted in yellow. At the bottom of the calendar widget are two buttons: 'Refresh' and '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** interface, click **Setting** to the right of **Holiday**. The setting method is the same as that of Monday to Sunday.

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

5.5.2 Snapshot by Location

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

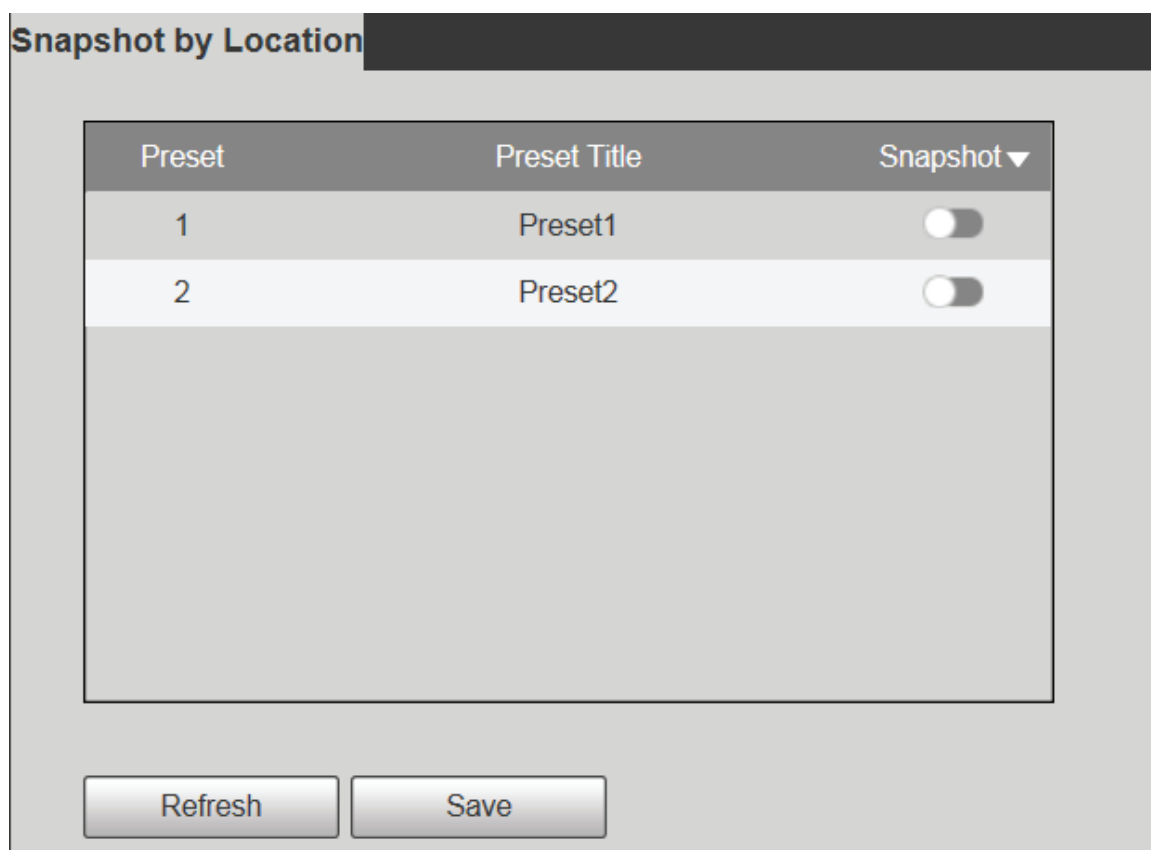


You need to set presets in advance.

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

The **Snapshot by Location** interface is displayed. See Figure 5-129.

Figure 5-129 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**.

5.5.3 Destination

5.5.3.1 Path

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.

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

The **Path** interface is displayed, see Figure 5-130.

Figure 5-130 Path settings

Event Type	Scheduled	Motion Detection	Alarm
Local	☒	☒	☒
FTP	☐	☐	☐
NAS	☐	☐	☐

Event Type	Scheduled	Motion Detection	Alarm
Local	☒	☒	☒
FTP	☐	☐	☐
NAS	☐	☐	☐

Default Refresh Save

Step 2 Select the corresponding event type and storage method as needed. For details, refer to Table 5-42.

Table 5-42 Path parameter description

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**.

5.5.3.2 Local

Display the SD card information. You can set it as read only or read & write; you can also hot swap or refresh it.

Select **Setting > Storage > Destination > Local**, and the **Local** interface is displayed. See Figure 5-131.

Figure 5-131 Local storage

Name	Status	Attribute	Used Capacity/Total Capacity
------	--------	-----------	------------------------------

Read Only Read & Write Hot Swap Refresh Format

- Click **Read Only**, and the SD card is set to read only.
- Click **Read & Write**, and the SD card is set to read & write.
- Click **Hot Swap** to remove the SD card.
- Click **Refresh** to start formatting the SD card.



After the SD card is formatted, the data will be cleared. Think twice before performing the operation.

5.5.3.3 FTP

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.

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

The **FTP** interface is displayed. See Figure 5-132.

Figure 5-132 FTP settings

The screenshot shows the FTP settings interface. At the top, there are four tabs: 'Path', 'Local', 'FTP' (which is selected), and 'NAS'. Below the tabs, the following settings are visible:

- Enable:** An unchecked checkbox.
- Server Address:** A text field containing '0.0.0.0'.
- Port:** A text field containing '22', with a range '(0~65535)' indicated to the right.
- Username:** A text field containing 'anonymity'.
- Password:** A text field with masked characters (dots).
- Remote Directory:** A text field containing 'share'.
- Emergency (Local):** An unchecked checkbox.

At the bottom of the interface, there are three buttons: 'test', 'Default', and 'Save'.

Step 2 Select the **Enable** check box, and the FTP function is enabled.



- 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 parameters as needed. For parameter description, see Table 5-43.

Table 5-43 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**.

5.5.3.4 NAS

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

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

The **NAS** interface is displayed. See Figure 5-133.

Figure 5-133 NAS settings

Step 2 Configure parameters as needed. For parameter description, see Table 5-44.

Table 5-44 NAS parameter description

Parameter	Description
Enable	Select the check box 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**.

5.5.4 Record Control

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

The **Record Control** interface is displayed. See Figure 5-134.

Figure 5-134 Record control

Step 2 Configure parameters as needed. For parameter description, see Table 5-45.

Table 5-45 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	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.  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.
Disk Full	You can select Stop or Overwrite. • 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.  The data will be overwritten if the disk is full. Back up the file in time as needed.
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**.

5.6 System Management

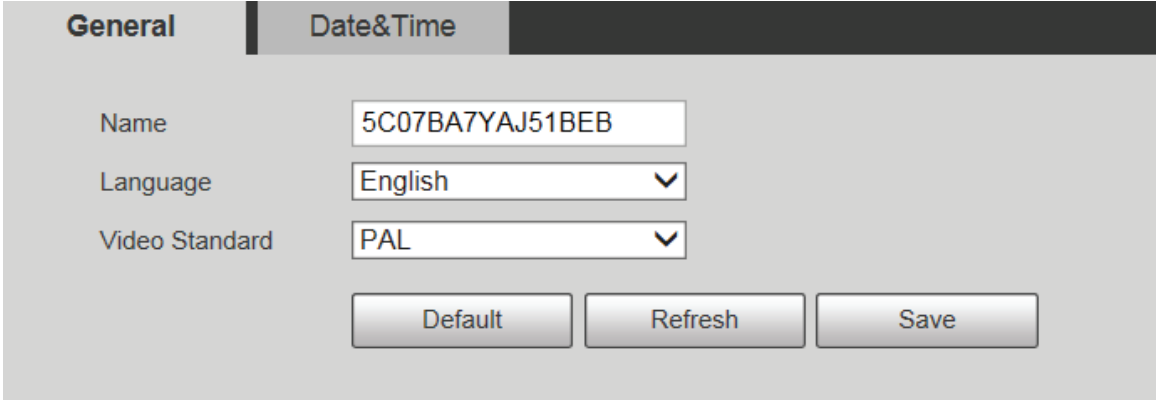
5.6.1 Device Settings

5.6.1.1 General

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

The **General** interface is displayed. See Figure 5-135.

Figure 5-135 General settings



Step 2 Configure parameters as needed. For parameter description, see Table 5-46.

Table 5-46 General setting parameter description

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 .

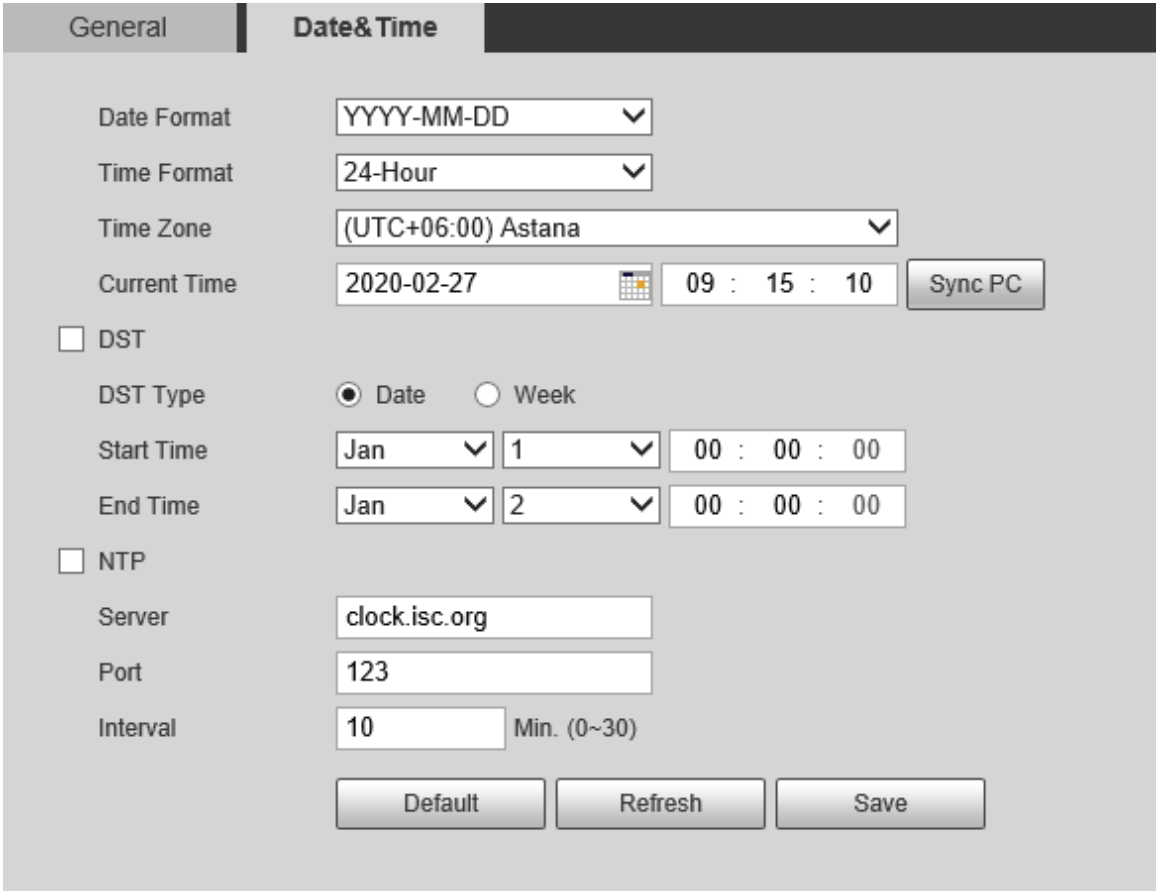
Step 3 Click **Save**.

5.6.1.2 Date & Time

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

The **Date&Time** interface is displayed. See Figure 5-136.

Figure 5-136 Date & time



The screenshot shows the 'Date&Time' configuration page. It includes dropdown menus for Date Format, Time Format, and Time Zone. There are input fields for Current Time, Start Time, and End Time, each with a calendar icon. A 'Sync PC' button is next to the Current Time field. There are checkboxes for DST and NTP. For DST, there are radio buttons for Date and Week, and input fields for Start Time and End Time. For NTP, there are input fields for Server, Port, and Interval. At the bottom, there are buttons for Default, Refresh, and Save.

Step 2 Configure parameters as needed. See Table 5-47.

Table 5-47 Date & time parameter description

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

Parameter	Description
NTP	Select the NTP check box 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**.

5.6.2 Account Settings

5.6.2.1 Account

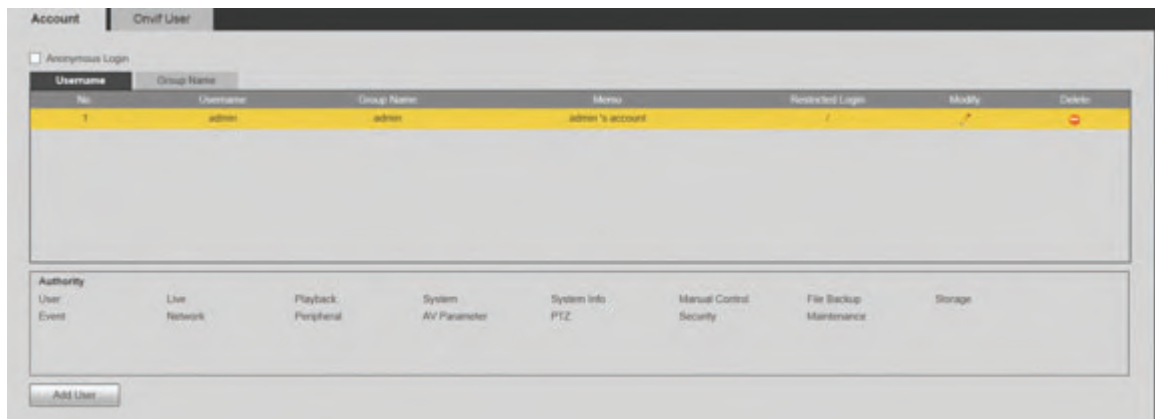
User management is only available for admin users.

- 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.

5.6.2.1.1 Username

Select **Setting > System > Account > Account > Username**, and you can enable anonymous login, add users, delete users, modify user passwords, and perform other operations. For the configuration interface, see Figure 5-137.

Figure 5-137 Account interface





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

Anonymous Login

Select the **Anonymous Login** check box, 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.

Adding Users

Add users in the group and set permissions.



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

Step 1 Click **Add User**.

The **Add User** interface is displayed. See Figure 5-138.

Figure 5-138 Adding users

Add User

Username **Must**

Password

The minimum pass phrase length is 8 characters

Confirm Password

Group Name

Memo

Operation Permission **Restricted Login**

☒ All

☒ User

☒ Live

☒ Playback

☒ System

☒ System Info

☒ Manual Control

☒ File Backup

☒ Storage

☒ Event

☒ Network

☒ Peripheral

☒ AV Parameter

☒ PTZ

☒ Security

☒ Maintenance

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 interface shown in Figure 5-139 is displayed. You can control login to the Device by setting the **IP Address**, **Validity Period** and **Time Range**.

Figure 5-139 Restricted login



- 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.

Step 4 Click **Save**.

Modifying Users

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

The **Modify User** interface is displayed. See Figure 5-140.

Figure 5-140 Modifying users

Modify User

Username: admin

☐ Modify Password

Group Name: admin

Memo: admin's account

Authority: ☒ All

- ☒ User
- ☒ Live
- ☒ Playback
- ☒ System

Save Cancel

Step 2 Modify user information as needed.

Step 3 Click **Save**.

Modifying Password

Step 1 Select the **Modify Password** check box.

Step 2 Enter old password and new password, and confirm password.

Step 3 Click **Save**.

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.

5.6.2.1.2 Group Name

Select **Setting > System > Account > Account > Group Name**, and you can add groups, delete groups, modify group passwords, and perform other operations. For the interface, see Figure 5-141.

Figure 5-141 User group settings

User group settings

No.	Group Name	Group Password	Memo	Authority	Action
1	administrative group			Administrative group	 
2	user group			User group	 

Authority: User, Live, Playback, System, System Info, Manual Control, File Backup, Storage, Event, Network, Peripheral

Add Group

Adding Groups

For specific operations, refer to "5.6.2.1.1 Username."

Modifying Groups

For specific operations, refer to "5.6.2.1.1 Username."

Deleting Groups

For specific operations, refer to "5.6.2.1.1 Username."

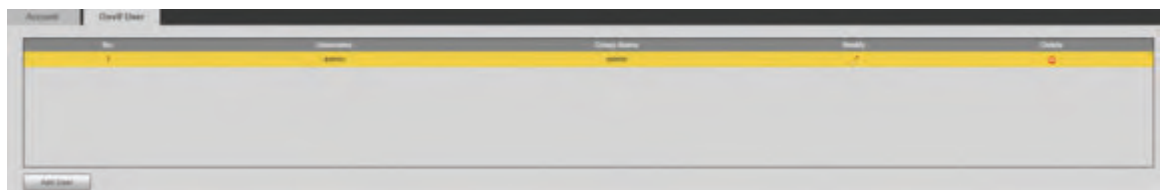
5.6.2.2 Onvif User

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

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

The **Onvif User** interface is displayed. See Figure 5-142.

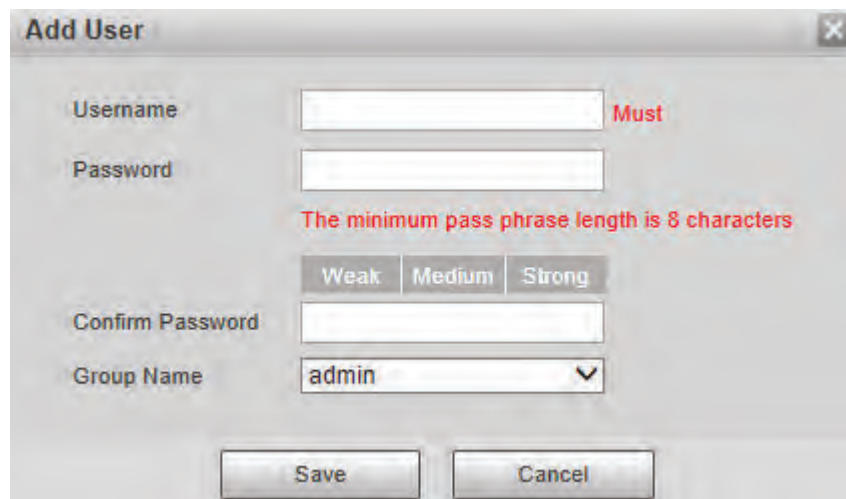
Figure 5-142 Onvif user



Step 2 Click **Add User**.

The **Add User** interface is displayed. See Figure 5-143.

Figure 5-143 Adding users



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

Step 4 Click **Save**.



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

5.6.3 Safety

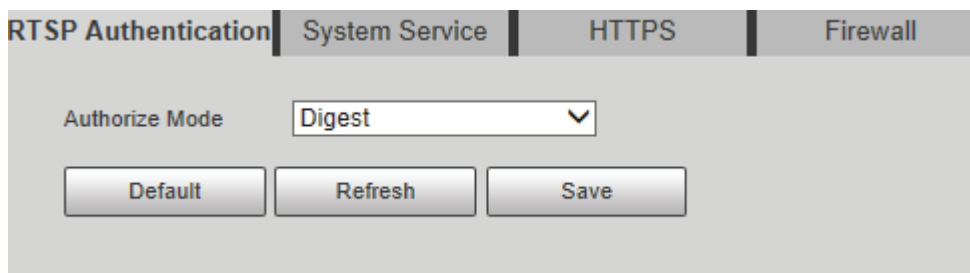
5.6.3.1 RTSP Authentication

Set the authentication method for media stream.

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

The **RTSP Authentication** interface is displayed. See Figure 5-144.

Figure 5-144 RTSP authentication



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.

5.6.3.2 System Service

You can configure system service to ensure system security.

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

The **System Service** interface is displayed. See Figure 5-145.

Figure 5-145 System service

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

SSH ☐ Enable

Multicast/Broadcast Search ☒ Enable

Password Reset ☒ Enable Email Address

CGI Service ☒ Enable

Onvif Service ☒ Enable

Genetec Service ☒ Enable

Audio and Video Transcoding ☐ Enable *Please make sure matched device or software supports video decryption function.

Mobile Push ☒ Enable

Private Protocol Authentication: Security Mode (Recommended) ▼

Default Refresh Save

Step 2 Configure system service parameters. For the detailed description, see Table 5-48.

Table 5-48 System service parameter description

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

Function	Description
	It is recommended to disable the function. If this function is enabled, there might be security risks.
Audio and Video Transmission Encryption	Enable this function to encrypt the stream transmitted through the private protocol.  - 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.
Mobile Push	Push the alarm snapshot triggered by the Device to the mobile phone. The function is enabled by default.  It is recommended to disable the function. If this function is enabled, there might be security risks.
Private Protocol Authentication Mode	You can select Security Mode and Compatible Mode . Security mode is recommended. If you select compatibility mode, there might be security risks.

Step 3 Click **Save**.

5.6.3.3 HTTPS



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

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.

Step 1 Create certificate or upload the signed certificate.

- If you select **Create Certificate**, refer to the following steps.
 - Select **Setting > System > Safety > HTTPS**.
The **HTTPS** interface is displayed. See Figure 5-146.

Figure 5-146 HTTPS (1)

- 2) Click **Create**.

The **HTTPS** dialog box is displayed. See Figure 5-147.

Figure 5-147 HTTPS (2)

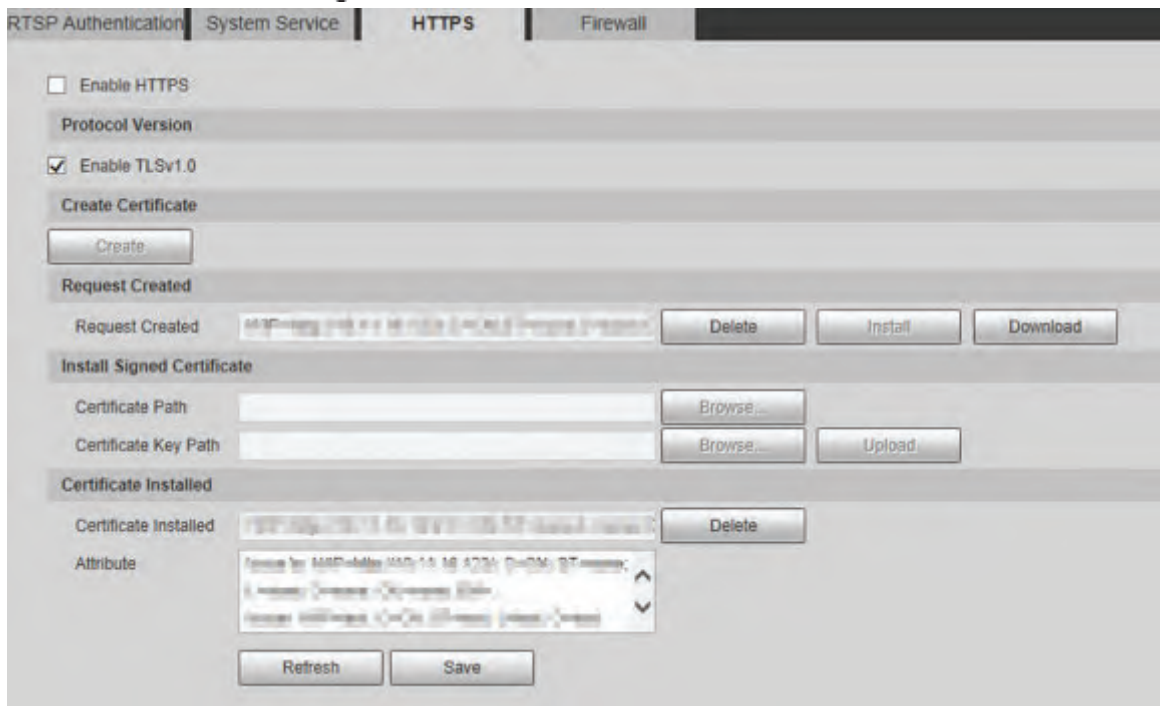
- 3) Enter the required information, and then click **Create**.



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

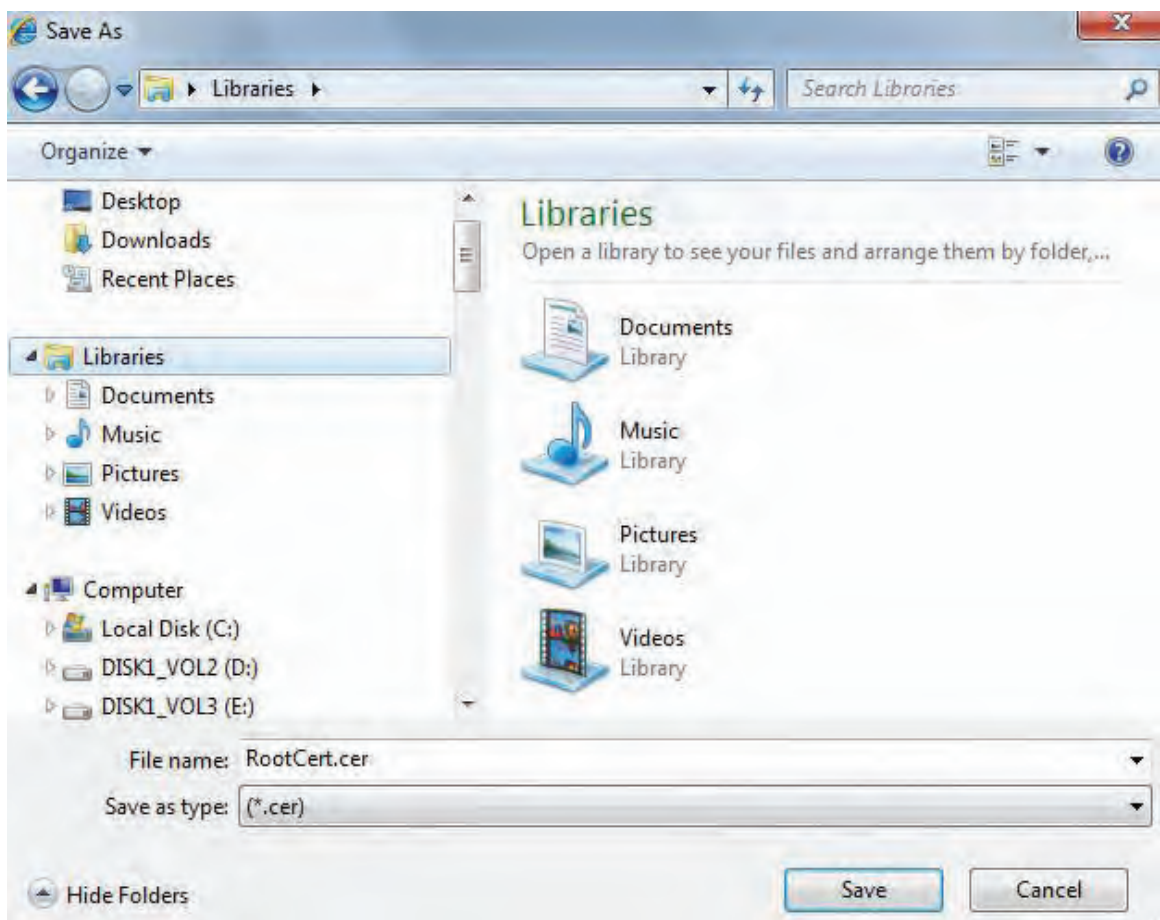
- 4) Click **Install** to install the certificate on the Device. See Figure 5-148.

Figure 5-148 Certificate installation



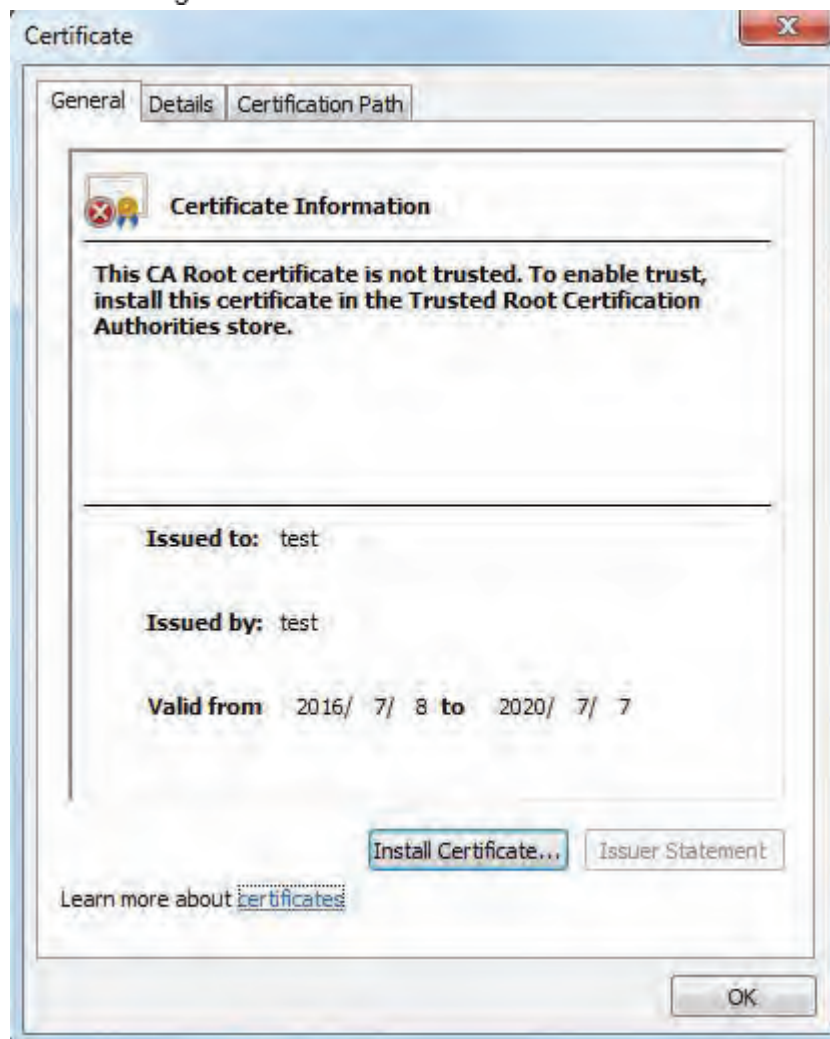
- 5) Click **Download** to download root certificate.
The **Save As** dialog box is displayed. See Figure 5-149.

Figure 5-149 Downloading root certificate



- 6) Select storage path, and then click **Save**.
- 7) Double-click the **RootCert.cer** icon.
The **Certificate** interface is displayed. See Figure 5-150.

Figure 5-150 Certificate information



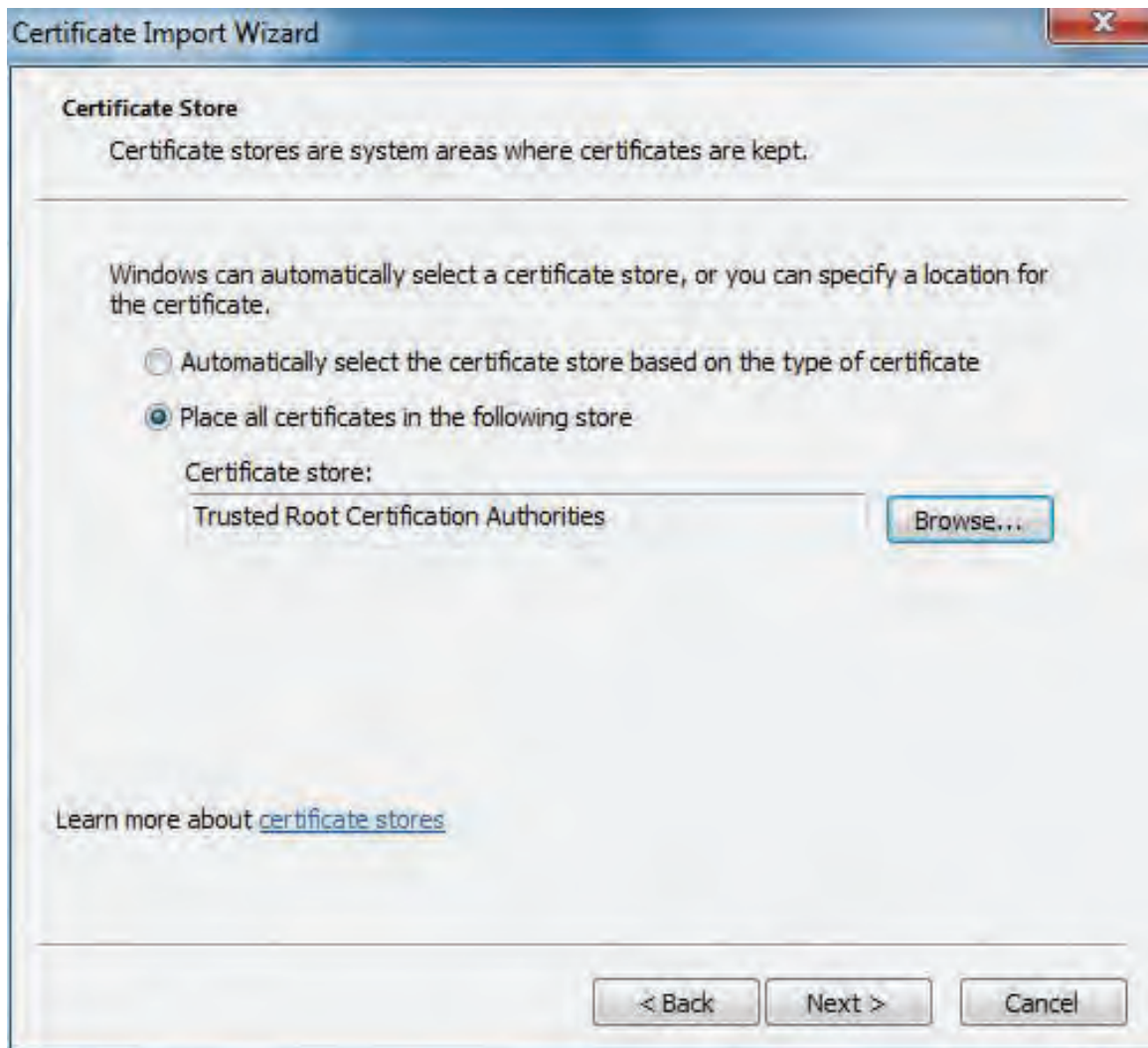
- 8) Click **Install Certificate**.
The **Certificate Import Wizard** interface is displayed. See Figure 5-151.

Figure 5-151 Certificate import wizard



- 9) Click **Next**.
Select **Trusted Root Certification Authorities**. See Figure 5-152.

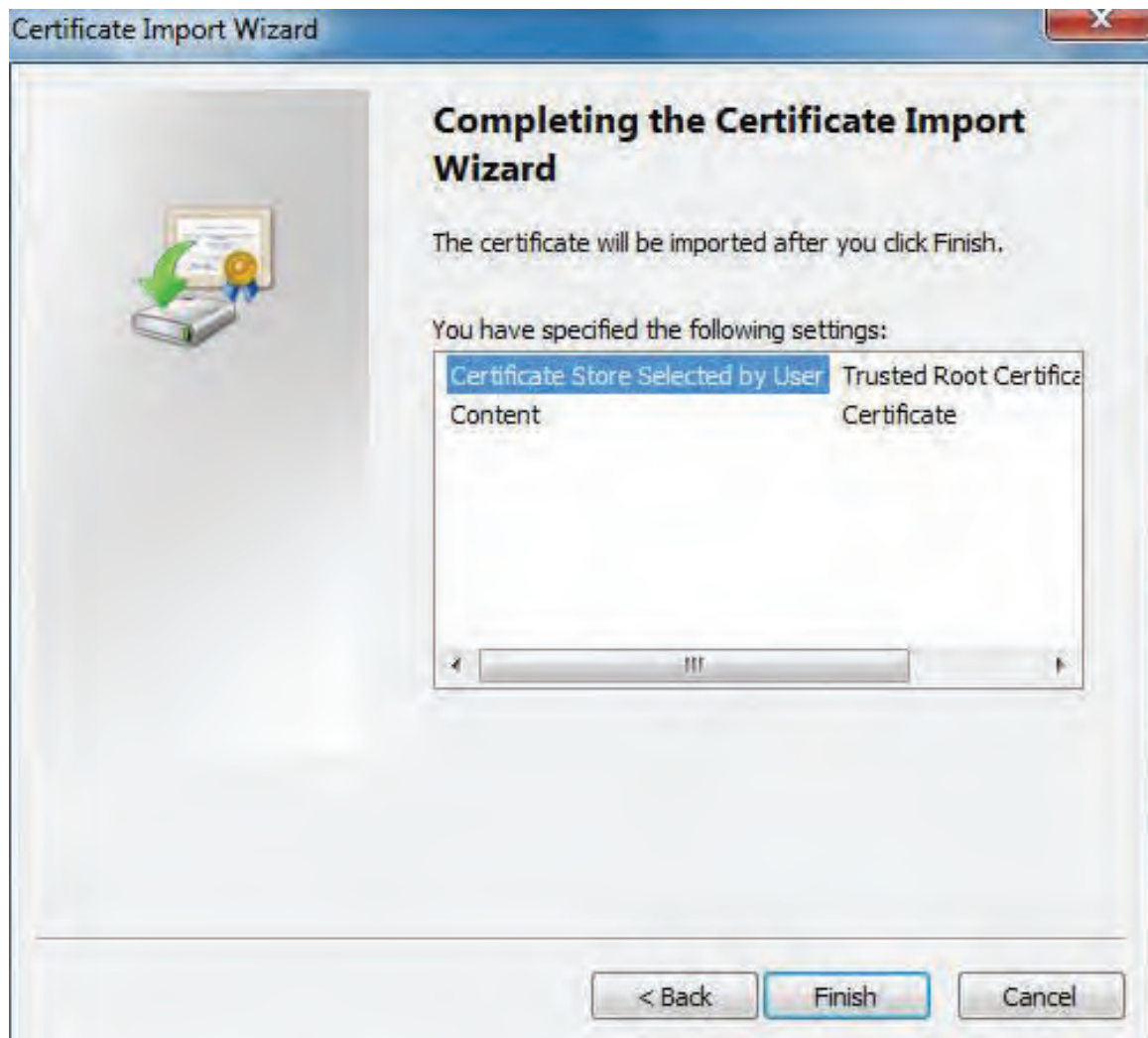
Figure 5-152 Certificate storage area



10) Click **Next**.

The **Completing the Certificate Import Wizard** interface is displayed, see Figure 5-153.

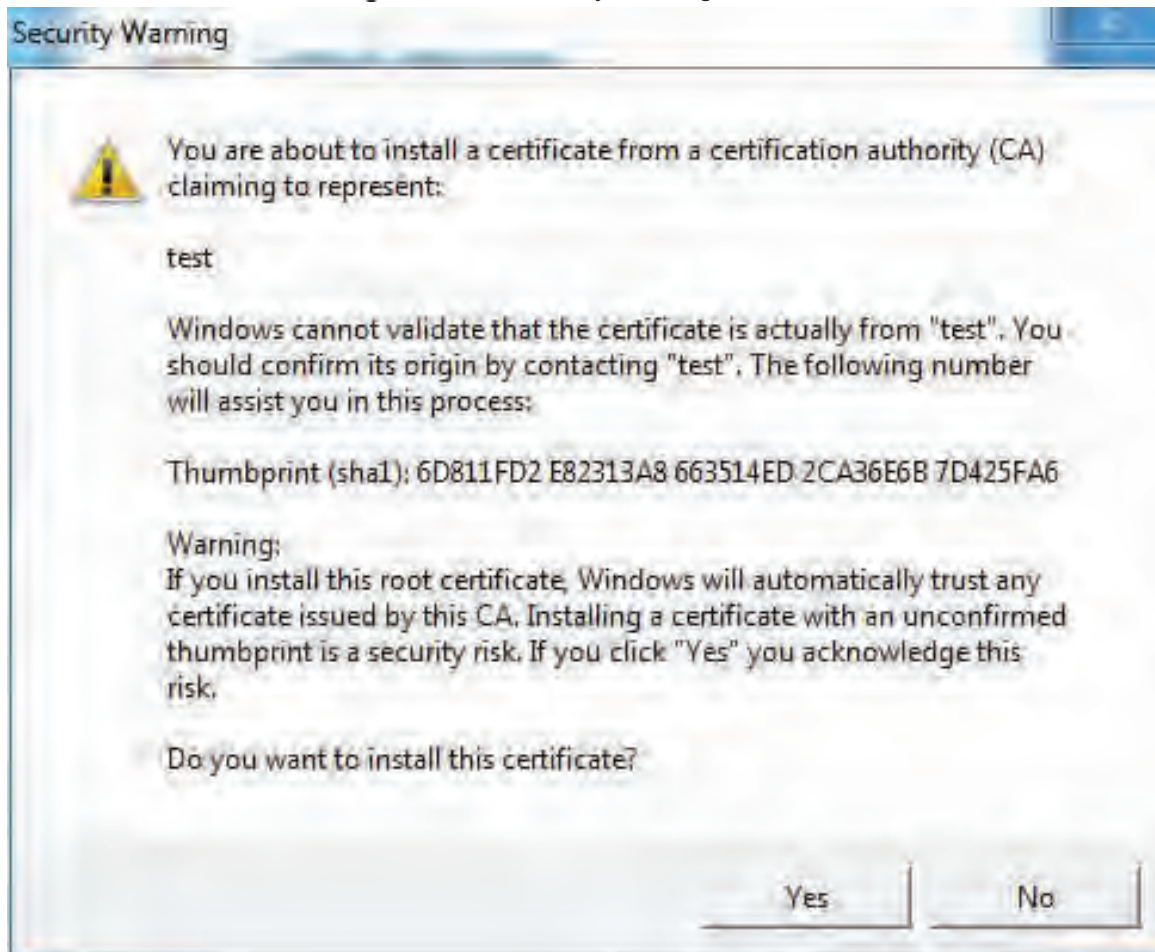
Figure 5-153 Completing the certificate import wizard



11) Click **Finish**.

The **Security Warning** dialog box is displayed. See Figure 5-154.

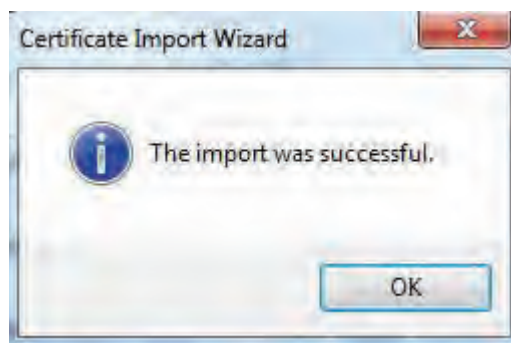
Figure 5-154 Security warning



12) Click **Yes**.

The **import was successful** dialog box is displayed. Click **OK** to complete the certificate installation. See Figure 5-155.

Figure 5-155 Import success



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

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

The **HTTPS** interface is displayed. See Figure 5-156.

Figure 5-156 Install signed certificate

The screenshot shows the 'HTTPS' configuration page. It includes a 'Create Certificate' section with a 'Create' button. Below it is a 'Request Created' table with columns for 'Request Created', 'Delete', 'Install', and 'Download'. The 'Install Signed Certificate' section has fields for 'Certificate Path' and 'Certificate Key Path', each with a 'Browse...' button, and an 'Upload' button. The 'Certificate Installed' section has a table with columns for 'Certificate Installed' and 'Delete', and an 'Attribute' field. At the bottom are 'Refresh' and 'Save' buttons.

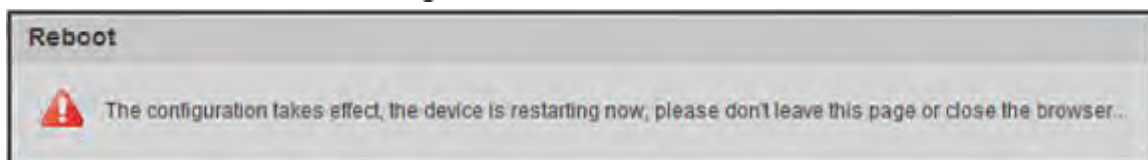
2) Click **Browse** to upload the signed certificate and certificate key, and then click **Upload**.

3) To install the root certificate, refer to Step 5) to 12) in **Create Certificate**.

Step 2 Select **Enable HTTPS** and click **Save**.

The **Reboot** interface is displayed, and the configuration takes effect after reboot. See Figure 5-157.

Figure 5-157 Reboot



Enter <https://xx.xx.xx.xx> in the browser to open the login interface. 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.

5.6.3.4 Firewall

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

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

The **Firewall** interface is displayed. See Figure 5-158.

Figure 5-158 Firewall

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

Step 3 Select **Enable**, and then the **Firewall** is enabled.

Step 4 Click **Save**.

5.6.4 Peripheral



The peripheral functions might vary with different models, and the actual interface shall prevail.

5.6.4.1 Wiper

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

The **Wiper** interface is displayed. See Figure 5-159.

Figure 5-159 Wiper settings

Step 2 Configure parameters as needed. For parameter description, see Table 5-49.

Table 5-49 Wiper setting parameter description

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.
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**.

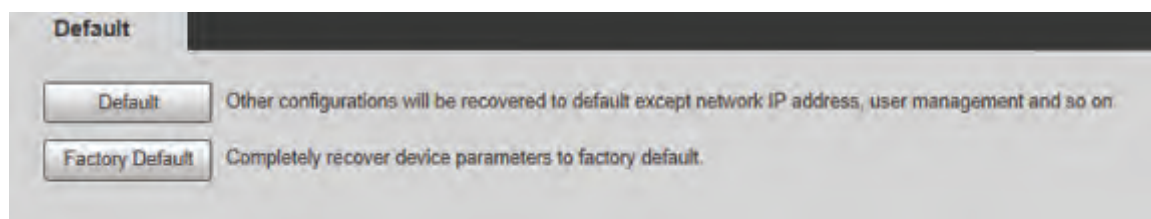
5.6.5 Default



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. The configuration interface is displayed. See Figure 5-160.

Figure 5-160 Default interface



Select the recovery mode as needed.

- **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 interface 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.

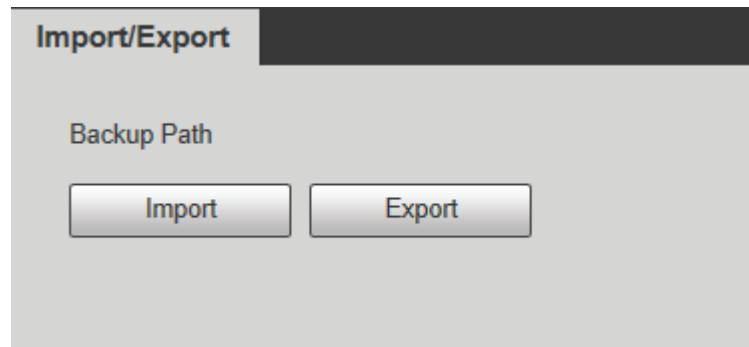
5.6.6 Import/Export

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

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

The **Import/Export** interface is displayed. See Figure 5-161.

Figure 5-161 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** interface of the Device to be configured to import the configuration file, and the Device will complete the configurations.

5.6.7 Auto Maintain

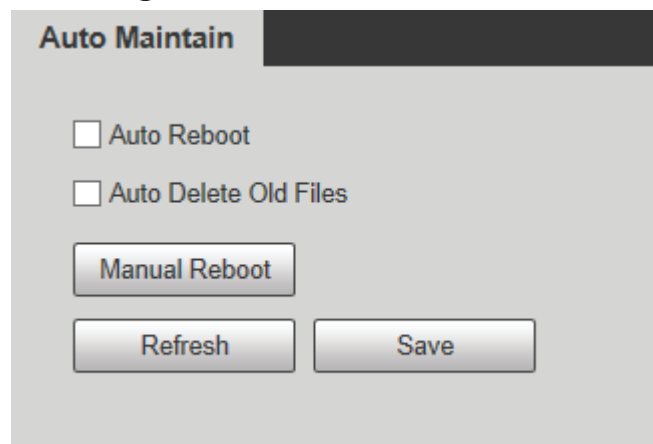
You can select **Auto Reboot** or **Auto Delete Old Files**.

- 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.

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

The **Auto Maintain** interface is displayed. See Figure 5-162.

Figure 5-162 Auto maintain



Step 2 Configure parameters as needed. For parameter description, see Table 5-50.

Table 5-50 Auto maintain parameter description

Parameter	Description
Auto Reboot	Select the check box to set the Device reboot time.
Auto Delete Old Files	Select the check box to customize the time period for the files to be deleted. The value ranges from 1 day to 31 days.  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.

Step 3 Click **Save** and the configuration will take effect.

5.6.8 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**. The configuration interface is displayed. See Figure 5-163.

Figure 5-163 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** check box.

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.

5.7 Information

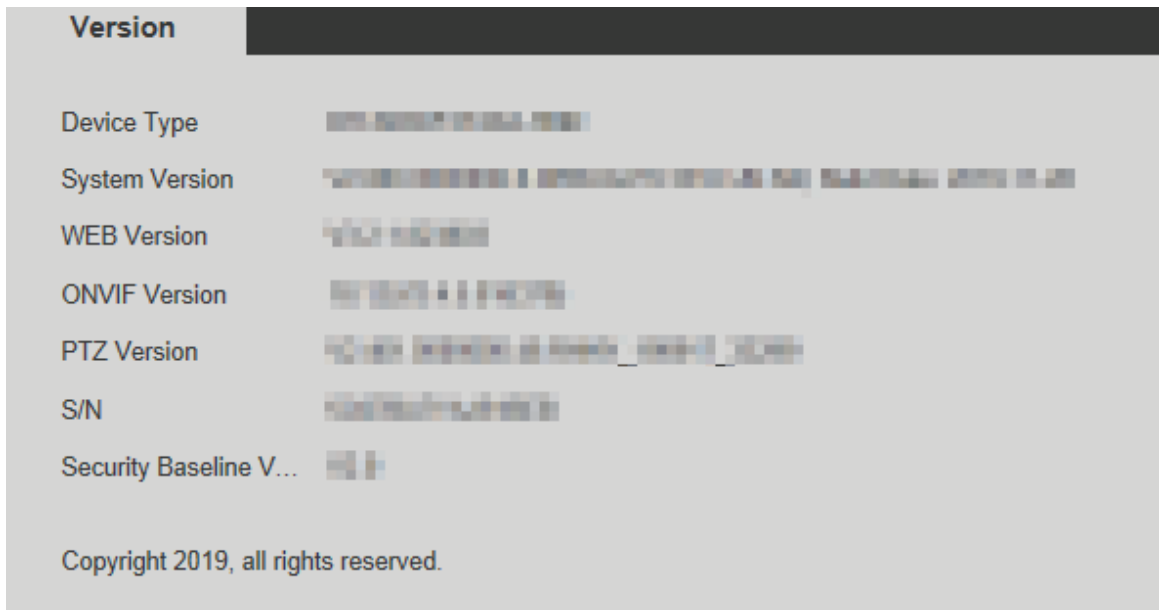
You can view information such as version, online users, log, and life statistics.

5.7.1 Version

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

Select **Setting > Information > Version > Version**, and then you can see the version information of current web interface. See Figure 5-164.

Figure 5-164 Version



5.7.2 Log Information

5.7.2.1 Log

Select **Setting > Information > Log > Log**, and then you can see the operation information of the Device, and some system information. See Figure 5-165. For parameter description, see Table 5-51.

Figure 5-165 Log

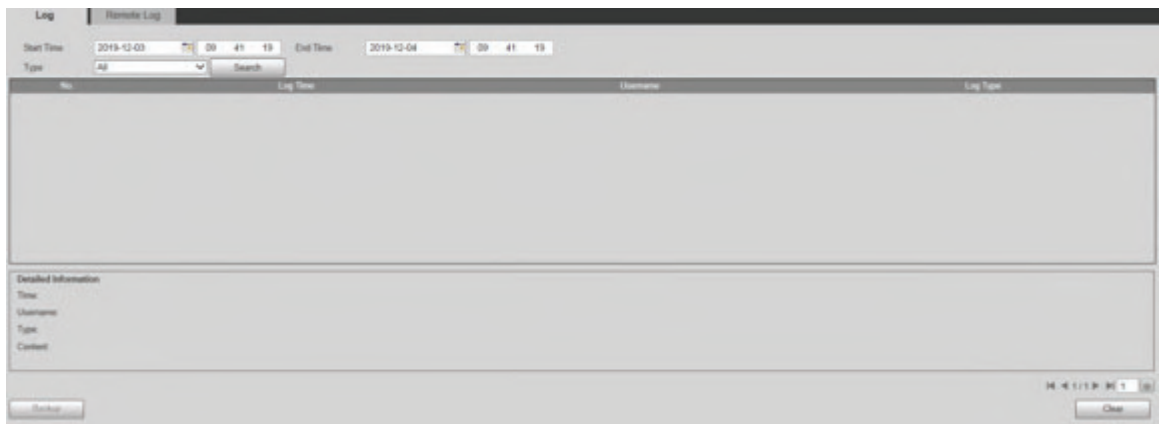


Table 5-51 Log parameter description

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.
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	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.

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.

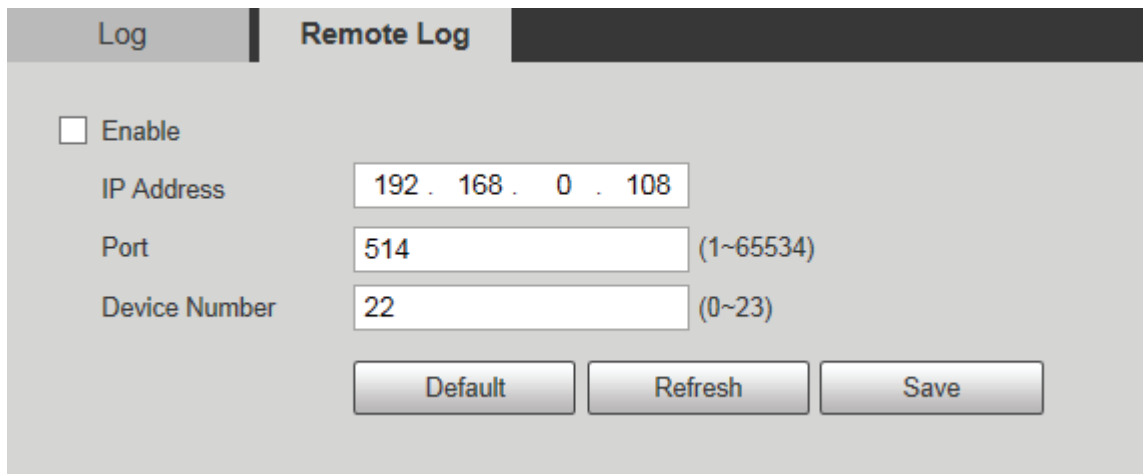
5.7.2.2 Remote Log

Upload the Device operations to the log server.

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

The **Remote Log** interface is displayed. See Figure 5-166.

Figure 5-166 Remote log



The interface shows a 'Remote Log' tab with an 'Enable' checkbox. Below it are input fields for 'IP Address' (192.168.0.108), 'Port' (514), and 'Device Number' (22). The port and device number fields have ranges (1~65534) and (0~23) respectively. At the bottom are 'Default', 'Refresh', and 'Save' buttons.

Step 2 Select **Enable**, and then remote log function is enabled.

Step 3 Set the **IP Address**, **Port** and **Device Number** of the log server.



Click **Default** to restore the Device to the default settings.

5.7.3 Online User

Select **Setting > Information > Online User**, and the **Online User** interface is displayed. See Figure 5-167.

Figure 5-167 Online users



No.	Username	User Local Group	IP Address	Times Login Time
1	admin	admin	192.168.1.100	2015-10-10 10:10:10

6 Alarm

You can select alarm types on the interface. When the selected alarms are triggered, detailed alarm information will be displayed on the right side of the interface. You can also select **Prompt** or **Play Alarm Tone**. When an alarm occurs, the alarm prompt or tone will be triggered. For the **Alarm** setting interface, see Figure 6-1. For parameter description, see Table 6-1.

Figure 6-1 Alarm setting interface



The interface is divided into two main sections. The left section contains 'Alarm Type' with checkboxes for Motion Detection, Disk Full, Disk Error, Motion Tamper, External Alarm, Illegal Access, Audio Detection, PIR, Scene Changing, and Security Exception. Below this are 'Operation' (Prompt), 'Alarm Tone' (Play Alarm Tone), and a 'Tone Path' field. The right section is a large table for displaying alarm events with columns for No., Time, Alarm Type, Triggering IP, and Alarm Channel.

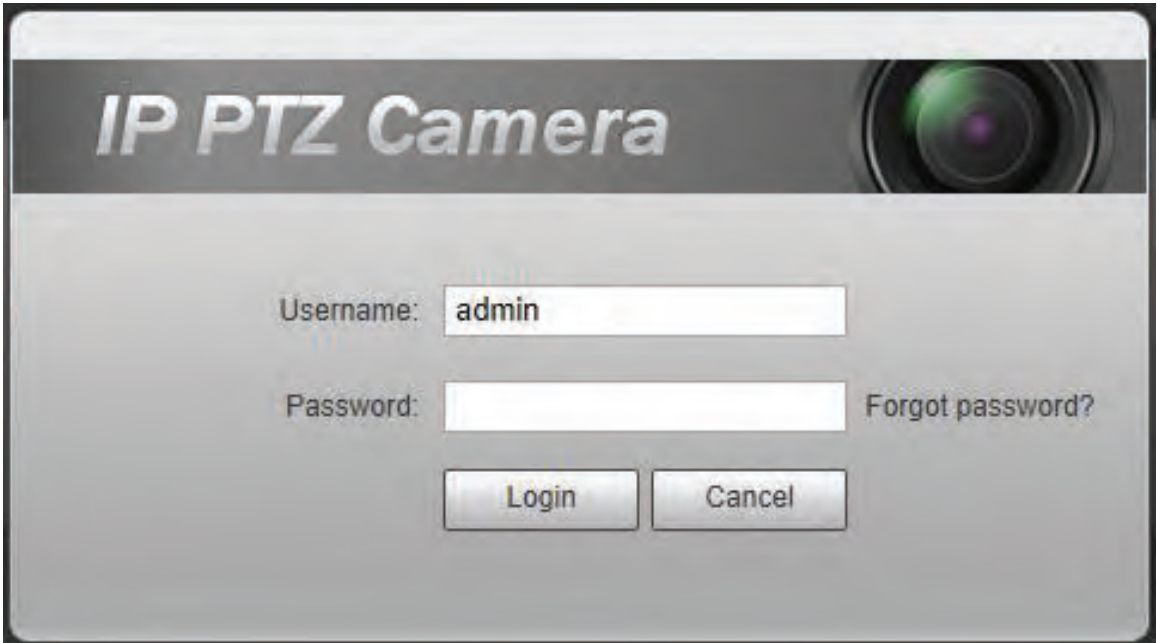
Table 6-1 Alarm setting parameter description

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.
Operation	Prompt	Select the Prompt check box. When you are not on the Alarm interface, 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.  If you are on the Alarm interface, 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.
Alarm Tone	Play Alarm Tone	Select the check box, 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.
	Tone Path	Customize the storage path for alarm tones.

7 Logout

Click **Logout** to log out, and the login interface is displayed. See Figure 7-1. Enter the username and password to log in again.

Figure 7-1 Login interface

The image shows a web-based login interface for an IP PTZ camera. At the top, there is a dark grey header bar with the text "IP PTZ Camera" in a light grey, italicized font on the left, and a small image of a camera lens on the right. Below the header, the background is a light grey gradient. The login form consists of two text input fields: the first is labeled "Username:" and contains the text "admin"; the second is labeled "Password:" and is empty. To the right of the password field is a link that says "Forgot password?". Below the password field are two buttons: "Login" and "Cancel".

IP PTZ Camera

Username:

Password: [Forgot password?](#)

Appendix 1 Cybersecurity Recommendations

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

Mandatory actions to be taken for basic equipment network security:

1. Use Strong Passwords

Please refer to the following suggestions to set passwords:

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

2. Update Firmware and Client Software in Time

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

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

1. Physical Protection

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

2. Change Passwords Regularly

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

3. Set and Update Passwords Reset Information Timely

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

4. Enable Account Lock

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

5. Change Default HTTP and Other Service Ports

We suggest you to change default HTTP and other service ports into any set of numbers between 1024~65535, reducing the risk of outsiders being able to guess which ports you are using.

6. Enable HTTPS

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

7. Enable Whitelist

We suggest you to enable whitelist function to prevent everyone, except those with specified IP addresses, from accessing the system. Therefore, please be sure to add your computer's IP address and the accompanying equipment's IP address to the whitelist.

8. MAC Address Binding

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

9. Assign Accounts and Privileges Reasonably

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

10. Disable Unnecessary Services and Choose Secure Modes

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

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

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

11. Audio and Video Encrypted Transmission

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

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

12. Secure Auditing

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

13. Network Log

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

14. Construct a Safe Network Environment

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

- Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.
- The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is

suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.

- Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.

Legal and Regulatory Information

Legal Considerations

Video surveillance can be regulated by laws that vary from country to country. Check the laws in your local region before using this product for surveillance purposes.

Disclaimer

Every care has been taken in the preparation of this document. Please inform your nearest Dahua office of any inaccuracies or omissions. Dahua Technology shall not be held responsible for any technical or typographical errors and reserves the right to make changes to the product and manuals without prior notice. Dahua Technology makes no warranty of any kind with regard to the material contained within this document, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Dahua Technology shall not be liable or responsible for incidental or consequential damages in connection with the furnishing, performance or use of this material. This product is only to be used for its intended purpose.

Intellectual Property Rights

Dahua Technology retains all intellectual property rights relating to technology embodied in the product described in this document.

Equipment Modifications

This equipment must be installed and used in strict accordance with the instructions given in the user documentation. This equipment contains no user-serviceable components. Unauthorized equipment changes or modifications will invalidate all applicable regulatory certifications and approvals.

Trademark Acknowledgments

 ,  ,  ,  are registered trademarks or trademark applications of Dahua Technology in various jurisdictions. All other company names and products are trademarks or registered trademarks of their respective companies.

Regulatory Information

European Directives Compliance



This product complies with the applicable CE marking directives and standards:

- Low Voltage (LVD) Directive 2014/35/EU.
- Electromagnetic Compatibility (EMC) Directive 2014/30/EU.
- Restrictions of Hazardous Substances (RoHS) Directive 2011/65/EU and its amending Directive (EU) 2015/863.

A copy of the original declaration of conformity may be obtained from Dahua

Technology.

The most up to date copy of the signed EU Declaration of Conformity (DoC) can be downloaded from: www.dahuasecurity.com/support/notice/

CE-Electromagnetic Compatibility (EMC)

This digital equipment is compliant with Class A according to EN 55032.



Warning:

This is a Class A product. In a domestic environment this product may cause radio interference, in which case the user may be required to take adequate measures.

CE-Safety

This product complies with IEC/EN/UL 60950-1 or IEC/EN/UL 62368-1, Safety of Information Technology Equipment.

Declaration of Conformity CE

(Only for the product has RF function)

Hereby, Dahua Technology declares that the radio equipment is compliant with Radio Equipment Directive (RED) 2014/53/EU. The full text of the EU declaration of conformity is available at the following internet address: www.dahuasecurity.com/support/notice/

USA Regulatory Compliance

FCC

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- (1) This device may not cause harmful interference.
- (2) This device must accept any interference received, including interference that may cause undesired operation.

Attention that changes or modification not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

FCC SDOC Statement can be downloaded from:
<https://us.dahuasecurity.com/support/notices/>

RF exposure warning

(Only for the product has RF communication function)

This equipment must be installed and operated in accordance with provided

instructions and the antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter. End-users and installers must be provided with antenna installation instructions and transmitter operating conditions for satisfying RF exposure compliance.

This equipment should be installed and operated with a minimum distance 20cm between the radiator and your body.

Canada Regulatory Compliance

ICES-003

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la Classe A est conforme à la norme NMB-003 du Canada.

This device complies with Industry Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions:

- (1) This device may not cause interference, and
- (2) This device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radioexempts de licence. L'exploitation est autorisée aux deux conditions suivantes:

- (1) l'appareil ne doit pas produire de brouillage, et
- (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

RF exposure warning

(Only for the product has RF communication function)

This equipment should be installed and operated with a minimum distance 20cm between the radiator and your body.

Cet équipement doit être installé et utilisé à une distance minimale de 20 cm entre le radiateur et votre corps.

Under Industry Canada regulations, this radio transmitter may only operate using an antenna of a type and maximum (or lesser) gain approved for the transmitter by Industry Canada. To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that necessary for successful communication.

Conformément à la réglementation d'Industrie Canada, le présent émetteur radio peut fonctionner avec une antenne d'un type et d'un gain maximal (ou inférieur) approuvé pour l'émetteur par Industrie Canada. Dans le but de réduire les risques de brouillage radioélectrique à l'intention des autres utilisateurs, il faut choisir le type d'antenne et son gain de sorte que la puissance isotrope rayonnée équivalente (p.i.r.e.) ne dépasse pas l'intensité nécessaire à l'établissement d'une communication satisfaisante.

Japan Regulatory Compliance

VCCI

These products comply with the requirements of VCCI Class A Information

Technology Equipment.

CAUTION

This is a Class A equipment. Operation of this equipment in a residential environment could cause radio interference. In such a case, the user may be required to take corrective actions.

Batteries

Correct disposal of batteries in this product



This marking on the battery indicates that the batteries in this product should not be disposed of with other household waste at the end of their working life. Where marked, the chemical symbols Hg, Cd or Pb indicate that the battery contains mercury, cadmium or lead above the reference levels in Directive 2006/66/EC and its amending Directive 2013/56/EU. If batteries are not properly disposed of, these substances can cause harm to human health or the environment.

CAUTION

Do not ingest battery. Chemical Burn Hazard.

This product contains a coin cell battery. If the coin cell battery is swallowed, it can cause severe internal burns in just 2 hours and can lead to death.

Keep new and used batteries away from children.

If the battery compartment does not close securely, stop using the product and keep it away from children.

If you think batteries might have been swallowed or placed inside any part of the body, seek immediate medical attention.

CAUTION

Risk of explosion if the battery is replaced by an incorrect type.

Do not throw or immerse into water, heat to more than 100°C (212°F), repair or disassemble, leave in an extremely low air pressure environment or extremely high-temperature environment, crush, puncture, cut or incinerate.

Dispose of the battery as required by local ordinances or regulations.

Safety

The product complies with IEC/EN/UL 60950-1, Information Technology Equipment – Safety – Part 1: General Requirements; or complies with IEC/EN/UL 62368-1, Audio/video, information and communication technology equipment – Part 1: Safety requirements.

If the power supply to the product is from external power adaptor without connecting to AC Mains, and the product is not shipped with power adaptor, customers are required to use the external power adaptor that must fulfill the requirements for Safety Extra Low Voltage (SELV) and Limited Power Source (LPS).

Waste Electrical and Electronic Equipment (WEEE) statements

Disposal and Recycling

When this product has reached the end of its useful life, dispose of it according

to local laws and regulations. For information about your nearest designated collection point, contact your local authority responsible for waste disposal. In accordance with local legislation, penalties may be applicable for incorrect disposal of this waste.



■ This symbol means that the product shall not be disposed of together with household or commercial waste. Directive 2012/19/EU on waste electrical and electronic equipment (WEEE) is applicable in the European Union member states. To prevent potential harm to human health and the environment, the product must be disposed of in an approved and environmentally safe recycling process. For information about your nearest designated collection point, contact your local authority responsible for waste disposal. Businesses should contact the product supplier for information about how to dispose of this product correctly.

Privacy Protection Notice

As the device user or data controller, you might collect personal data of others such as face, fingerprints, car plate number, Email address, phone number, GPS and so on. You need to be in compliance with the local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures, including but not limited to: providing clear and visible identification to inform data subject the existence of surveillance area and providing related contact.

About the Manual

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

Support

Should you require any technical assistance, please contact your Dahua distributor. If your questions cannot be answered immediately, your distributor will forward your queries through the appropriate channels to ensure a rapid

response. If you are connected to the Internet, you can:

- Download user documentation and software updates.
- Search by product, category, or phrase.
- Report problems to Dahua support staff by logging in to your private support area.
- Chat with Dahua support staff.
- Visit Dahua Support at www.dahuasecurity.com/support

Contact Information

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.

Address: No.1199, Bin'an Road, Binjiang District, Hangzhou, P.R. China

Postcode: 310053

Tel: +86-571-87688883

Fax: +86-571-87688815

Email: overseas@dahuatech.com

Website: www.dahuasecurity.com

English

Important Safeguards and Warnings

This Chapter describes the contents covering proper handling of the device, hazard prevention, and prevention of property damage. Read these contents carefully before using the device, comply with them when using, and keep it well for future reference.

Safety Instructions

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

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

Safety Requirement

- Abide by local electrical safety standards to ensure that the voltage is stable and complies with the power supply requirement of the device.
- Transport, use, and store the device under the allowed humidity and temperature conditions. Refer to the corresponding technical specifications of

device for specific working temperature and humidity.

- Do not place the device in a location exposed to dampness, dust, extreme hot or cold, strong electronic radiation, or unstable lighting conditions.
- Do not install the device in a place near the heat source, such as radiator, heater, furnace, or other heat generating device to avoid fire.
- Prevent liquid from flowing into the device to avoid damage to internal components.
- Install the device horizontally or install on the stable place to prevent it from falling.
- Install the device in a well-ventilated place, and do not block the ventilation of the device.
- Do not disassemble the device arbitrarily.
- Avoid heavy stress, violent vibration, and soaking during transportation, storage, and installation. Complete package is necessary during the transportation.
- Use the factory package or the equivalent for transportation.

Battery

Low battery power affects the operation of the RTC, causing it to reset at every power-up. When the battery needs replacing, a log message will appear in the product's server report. For more information about the server report, see the product's setup pages or contact Dahua support.



WARNING

- Risk of explosion if the battery is incorrectly replaced.
- Replace only with an identical battery or a battery which is recommended by Dahua.
- Dispose of used batteries according to local regulations or the battery manufacturer's instructions.

Polski

Ważne środki ostrożności i ostrzeżenia

Niniejszy rozdział opisuje właściwe sposoby korzystania z urządzenia, sposoby zapobiegania zagrożeniom, a także sposoby zapobiegania uszkodzeniu mienia. Przed rozpoczęciem korzystania z urządzenia zapoznaj się dokładnie z tymi informacjami i zachowaj je na przyszłość do celów referencyjnych.

Instrukcje dot. bezpieczeństwa

W podręczniku mogą pojawić się następujące symbole. Ich znaczenie wyjaśnia poniższa tabela.

Symbol	Znaczenie
 ZAGROŻENIE	Oznacza potencjalne zagrożenie wysokiego stopnia, którego nieuniknięcie może skutkować poważnymi urazami lub śmiercią.
 OSTRZEŻENIE	Oznacza potencjalne zagrożenie średniego lub niskiego stopnia, którego nieuniknięcie może skutkować pomniejszymi lub średnimi urazami.
 UWAGA	Oznacza potencjalne zagrożenie, którego nieuniknięcie może skutkować zniszczeniem mienia, utratą danych, spadkiem wydajności lub mieć inne nieprzewidziane skutki.

Symbol	Znaczenie
 WSKAZÓWKI	Oznacza wskazówki pozwalające na rozwiązanie problemu lub oszczędność czasu.
 UWAGA	Oznacza informacje uzupełniające tekst główny.

Wymogi dot. Bezpieczeństwa

- Przestrzegaj lokalnych standardów bezpieczeństwa elektrycznego celem upewnienia się, że źródło napięcia jest stabilne i zgodne z wymogami określonymi dla urządzenia.
- Urządzenie należy transportować, używać i przechowywać w warunkach o dozwolonym poziomie wilgotności i temperatury. Szczegółowe informacje na temat wilgotności i temperatury roboczej znaleźć można w odpowiedniej specyfikacji technicznej urządzenia.
- Nie umieszczaj urządzenia w miejscach narażonych na wilgoć, kurz, ekstremalne temperatury, silne promieniowanie elektroniczne oraz niestabilne warunki oświetleniowe.
- Nie instaluj urządzenia w pobliżu źródeł ciepła, takich jak kaloryfery, grzałki, piece bądź inne urządzenia generujące ciepło, aby zapobiegać wystąpieniu pożaru.
- Zabezpiecz urządzenie przed dostaniem się do jego wnętrza cieczy, ponieważ może to spowodować uszkodzenie komponentów wewnętrznych.
- Zamontuj urządzenie poziomo lub wybierz stabilne miejsce, tak aby wyeliminować ryzyko upadku.
- Zamontuj urządzenie w dobrze wentylowanym miejscu i upewnij się, że jego otwory wentylacyjne nie są zablokowane.
- Nie rozmontowuj urządzenia samodzielnie.
- Chroń urządzenie przed dużymi obciążeniami i naprężeniami, silnymi wibracjami oraz zalaniem zarówno podczas transportu, przechowywania, jak i montażu. Na potrzeby transportu wymagane jest korzystanie z kompletnego opakowania.
- Do transportu używaj oryginalnego opakowania lub innego zapewniającego podobny poziom ochrony.

Akumulator

Niski poziom naładowania akumulatora wpływa na działanie zegara czasu rzeczywistego, powodując jego resetowanie przy każdym włączeniu. Gdy akumulator wymaga wymiany, w raporcie serwerowym dla produktu pojawi się stosowna wiadomość. Aby uzyskać więcej informacji na temat raportu serwerowego, zapoznaj się z instrukcjami konfiguracji urządzenia lub skontaktuj się z personelem pomocy technicznej firmy Dahua.



OSTRZEŻENIE

- W przypadku niewłaściwej wymiany akumulatora występuje zagrożenie wybuchem.
- Akumulator należy zastępować wyłącznie takim samym typem lub innym typem zalecanym przez firmę Dahua.
- Akumulatory należy utylizować zgodnie z lokalnymi regulacjami lub instrukcjami producenta akumulatora.

Dansk

Vigtige sikkerhedsanvisninger og advarsler

Kapitlet beskriver korrekt håndtering af produktet, undgåelse af risici og undgåelse af skader på ejendom. Læs kapitlet omhyggeligt, før du bruger produktet, overhold alle anvisninger og advarsler under brugen, og gem kapitlet til senere brug.

Sikkerhedsanvisninger

Følgende signalord med beskrivelse kan forekomme i vejledningen.

Signalord	Beskrivelse
 FARE	Angiver høj risiko, som, hvis den ikke undgås, kan medføre død eller alvorlig personskade.
 ADVARSEL	Angiver middel eller lav risiko, som, hvis den ikke undgås, kan medføre lettere til moderat personskade.
 FORSIGTIG	Angiver mulig risiko, som hvis den ikke undgås, kan resultere i skade på ejendom, tab af data, reduceret ydelse eller uforudsigelige resultater.
 TIPS	Indeholder forslag, som hjælper dig med at løse et problem eller sparer tid.
 BEMÆRK	Indeholder yderligere oplysninger, som understreger og supplerer teksten.

Sikkerhedskrav

- Følg lokale standarder for elsikkerhed for at sikre, at spændingen er stabil og i overensstemmelse med produktets krav til strømforsyning.
- Transportér, brug og opbevar produktet i henhold til de tilladte klimatiske forhold (temperatur og luftfugtighed). Se produktets tekniske specifikationer for specifik temperatur og luftfugtighed ved drift.
- Placér ikke produktet et sted med fugt, støv, stærk varme eller kulde, stærk elektronisk udstråling eller ustabile lysforhold.
- Installér ikke produktet i nærheden af en varmekilde, såsom en radiator, et varmeapparat, et centralfyr eller andre varmeafgivende enheder, for at undgå ildebrand.
- Undgå, at væske løber ind i produktet og dermed forårsager skade på de indvendige komponenter.
- Installér produktet vandret, eller installér det et stabilt sted for at undgå, at det falder ned.
- Installér produktet et sted med god udluftning, og blokér ikke produktets ventilationsåbninger.
- Adskil ikke produktet.
- Undgå stærkt tryk, kraftige vibrationer og gennemblødning under transport, opbevaring og installation. Produktet skal være fuldt emballeret under transport.
- Brug fabriksemballagen eller tilsvarende til transporten.

Batteri

Lav batterispænding påvirker driften af realtidsuret og får uret til at nulstille, hver gang produktet tændes. Der vises en logbesked i produktets serverrapport, når batteriet skal udskiftes. Se konfigurationssiderne til produktet, eller kontakt Dahuas supportteam for at få flere oplysninger om serverrapporten.



ADVARSEL

- Der er risiko for eksplosion, hvis batteriet udskiftes forkert.
- Udskift kun med et tilsvarende batteri eller et batteri, der anbefales af Dahua.

- Bortskaf brugte batterier i overensstemmelse med lokale bestemmelser eller batteriproducentens anvisninger.

Suomi

Tärkeitä varotoimenpiteitä ja varoituksia

Tässä luvussa kuvataan laitteen asianmukainen käsittely, vaarojen torjunta ja omaisuusvahinkojen estäminen. Lue tämä sisältö huolellisesti ennen laitteen käyttämistä ja noudata näitä ohjeita, kun käytät laitetta. Säilytä ohjeet tulevia tarpeita varten.

Turvallisuusohje

Seuraavat luokitellut huomiosanat kuvatulla merkityksellä saattavat esiintyä oppaassa.

Huomiosanat	Merkitys
 VAARA	Ilmaisee suuren potentiaalisen vaaran, joka johtaa kuolemaan tai vakavaan loukkaantumiseen, jos sitä ei vältetä.
 VAROITUS	Ilmaisee keskisuuren tai pienen potentiaalisen vaaran, joka saattaa johtaa lievään tai kohtalaiseen loukkaantumiseen, jos sitä ei vältetä.
 HUOMIO	Ilmaisee mahdollisen vaarallisen tilanteen, joka saattaa johtaa omaisuusvahinkoon, tietojen menetykseen, suoritustehon heikkenemiseen tai odottamattomiin tuloksiin, jos sitä ei vältetä.
 VINKIT	Tarjoavat apua ongelmien ratkaisemiseen tai säästävät aikaa.
 HUOMAUTUS	Tarjoaa lisätietoa, joka korostaa tai täydentää tekstiä.

Turvallisuusvaatimus

- Noudata paikallisia sähköturvallisuusstandardeja varmistaaksesi, että jännite on vakaa ja vastaa laitteen virtalähteelle asetettuja vaatimuksia.
- Kuljeta, käytä ja säilytä laitetta sallituissa kosteus- ja lämpötilaolosuhteissa. Katso laitteen erityinen käyttölämpötila ja -kosteus laitteen vastaavista teknisistä tiedoista.
- Älä sijoita laitetta paikkaan, jossa se altistuu kosteudelle, pölylle, erittäin kuumalle tai kylmälle lämpötilalle, voimakkaalle sähkösäteilylle tai epävakaille valaistusolosuhteille.
- Älä asenna laitetta lähelle lämmönlähdettä, kuten lämpöpatteria, lämmitintä, uunia tai muuta lämpöä tuottavaa laitetta, tulipalon välttämiseksi.
- Vältä nesteen pääsemistä laitteen sisälle sisäisten komponenttien vahingoittumisen estämiseksi.
- Asenna laite vaakasuoraan tai asenna se vakaaseen paikkaan estääksesi sen kaatumisen.
- Asenna laite hyvin ilmastoituun paikkaan äläkä peitä laitteen tuuletusaukkoja.
- Älä pura laitetta omavaltaisesti.
- Vältä kovaa räsitusta, voimakasta tärinää ja kosteutta kuljetuksen, säilytyksen ja asennuksen aikana. Kuljetus vaatii täydellisen pakkaamisen.
- Käytä tehtaan pakkausta tai vastaavaa kuljetuksen aikana.

Paristo

Alhainen pariston varaustaso vaikuttaa tosiaikakellon (RTC:n) toimintaan nollaten sen jokaisella käynnistyskerralla. Lokiviesti ilmestyy tuotteen palvelinraporttiin, kun paristo on vaihdettava. Lisätietoa palvelinraportista saat tuotteen asetussivuilta tai ottamalla yhteyttä Dahuan tukeen.



VAROITUS

- Räjähdysvaara, jos paristo asetetaan väärin paikalleen.
- Vaihda vain samanlaiseen paristoon tai Dahuan suosittelemaan paristoon.
- Hävitä käytetty paristot ja akut paikallisten määräysten tai valmistajan ohjeiden mukaisesti.

Magyar

Fontos óvintézkedések és figyelmeztetések

A jelen Fejezet leírja az Eszköz megfelelő kezelését, a veszélyek megelőzését és a vagyoni károk megelőzését. Az Eszköz használata előtt olvassa el figyelmesen, a használata során tartsa be, és őrizze meg jól jövőbeni hivatkozás céljára.

Biztonsági utasítások

Az Útmutatóban az alábbi meghatározott jelentéssel bíró kategorizált figyelmeztetések jelenhetnek meg.

Figyelmeztetés	Jelentés
 VESZÉLY	Nagy potenciális veszélyt jelez, amely, ha nem kerüli el, halált vagy súlyos sérülést okoz.
 FIGYELEM	Közepes vagy kis potenciális veszélyt jelez, amely, ha nem kerüli el, enyhe vagy mérsékelt sérülést okozhat.
 VIGYÁZAT	Olyan potenciális kockázatot jelez, amely, ha nem kerüli el, vagyoni kárt, adatvesztést, alacsonyabb teljesítményt vagy kiszámíthatatlan eredményt okozhat.
 TIPPEK	Olyan módszereket biztosít, amelyek segítenek megoldani a problémáját vagy időt takarítanak meg.
MEGJEGYZÉSEK	További információkat biztosít a szöveg kiemelésével és kiegészítésével.

Biztonsági követelmények

- Tartsa be a helyi elektromos biztonsági szabványokat annak biztosítása érdekében, hogy a feszültség stabil és az eszköz áramellátási követelményének megfelelő legyen.
- Az eszközt a megengedett páratartalom és hőmérséklet viszonyok között szállítsa, használja, és tárolja. A konkrét üzemi hőmérsékletet és páratartalmat megtalálja az eszköz műszaki leírásában.
- Ne tegye az eszközt olyan helyre, ahol nedvességnak, pornak, rendkívüli melegnek vagy hidegnek, erős elektronikus sugárzásnak, vagy instabil fényviszonyoknak van kitéve.

- A tűz elkerülése érdekében ne telepítse az eszközt hőforrás, mint például radiátor, hőszugárzó, kemence, vagy más hőtermelő eszköz közelében lévő helyre.
- A belső alkatrészek károsodásának elkerülése érdekében akadályozza meg, hogy folyadék folyjon az eszközbe.
- A leesésének megakadályozása érdekében az eszközt vízszintesen telepítse, vagy stabil helyre telepítse.
- Az eszközt jól szellőző helyre telepítse, és ne blokkolja az eszköz szellőzését.
- Önkényesen ne szerelje szét az eszközt.
- A szállítás, tárolás és telepítés során kerülje a nagy igénybevételt, erős rezgést, és az eláztatást. A szállítás során a teljes csomagolásra szükség van.
- A szállításhoz gyári csomagolást vagy azzal egyenértékűt használjon.

Elem

Az alacsony elem töltöttségi szint hatással van az RTC működésére, minden bekapcsoláskor alaphelyzetbe áll. Amikor az elemet cserélni kell, egy napló üzenet jelenik meg a termék szerver jelentésében. A szerver jelentésről további információkat talál a termék beállítási oldalain, vagy forduljon a Dahua támogatáshoz.



FIGYELEM

- Robbanásveszély, ha az elemet nem megfelelőre cseréli.
- Csak ugyanolyan elemre vagy a Dahua által ajánlott elemre cserélje.
- A használt elemet a helyi előírások vagy az elemgyártó utasításai szerint ártalmatlanítsa.

Б ъ л г а р с к и

Важни предпазни мерки и предупреждения

Тази глава описва инструкциите за правилна експлоатация на устройството, за предотвратяване на опасностите и материалните щети. Прочетете внимателно тези инструкции, преди да използвате устройството, спазвайте ги при използването на устройството, и ги запазете за бъдещи справки.

Инструкции за безопасност

Ръководството съдържа следните определени сигнални думи.

Сигнални думи	Значение
 ОПАСНОСТ	Показва висока потенциална опасност, която, ако не бъде избегната, ще доведе до смърт или сериозно нараняване.
 ПРЕДУПРЕЖДЕНИЕ	Показва средна или ниска потенциална опасност, която, ако не бъде избегната, може да доведе до леки или умерени наранявания.
 ВНИМАНИЕ	Посочва потенциален риск, който, ако не бъде избегнат, може да доведе до материални щети, загуба на данни, по-ниска производителност или непредсказуем резултат.

Сигнални думи	Значение
 СЪВЕТИ	Обозначава начини, които да ви помогнат да разрешите проблем или да спестите време.
 ЗАБЕЛЕЖКА	Предоставя допълнителна информация като акцент и допълнение към основния текст.

Изисквания за безопасност

- Спазвайте местните стандарти за електрическа безопасност, за да осигурите стабилно напрежение, отговарящо на изискването за захранване на устройството.
- Транспортирайте, използвайте и съхранявайте устройството при указаните условия на влажност и температура. Направете справка в съответните технически спецификации на устройството за конкретната работна температура и влажност.
- Не поставяйте устройството на място, изложено на влага, прах, много висока или ниска температура, със силно електронно излъчване или на място с променливо осветление.
- Не поставяйте устройството близо до източник на топлина, като радиатор, нагревател, печ или друго устройство за генериране на топлина, за да избегнете пожар.
- Не допускайте в устройството да попадне течност, за да не се повредят вътрешните компоненти.
- Монтирайте устройството хоризонтално или го поставете на стабилно място, за да не падне.
- Монтирайте устройството на добре проветриво място и не блокирайте вентилацията на устройството.
- Не разглобявайте устройството произволно.
- Избягвайте силно натоварване, вибрации и намокряне по време на транспортиране, съхранение и монтаж. При транспортиране следва да се опакова напълно.
- Използвайте за транспортиране фабричната опаковка или подобна.

Батерия

Ниската мощност на батерията влияе на работата на часовника в реално време (RTC), което води до нулиране при всяко включване. Когато батерията трябва да бъде сменена, в отчета на сървър на продукта ще се покаже съобщение. За повече информация относно отчета на сървър вижте страниците за настройка на продукта или се свържете с екипа на Dahua.



ПРЕДУПРЕЖДЕНИЕ

- Ако батерията е неправилно подменена, има риск от експлозия.
- Сменяйте само със същата или батерия, препоръчана от Dahua.
- Изхвърляйте използваните батерии в съответствие с местните разпоредби или инструкциите на производителя на батерията.

Românesc

Masuri de siguranta si Atentionari

Acest capitol descrie indicatiile de utilizare corecta a Dispozitivului , prevenirea pericolului si prevenirea distrugerii proprietatii.Cititi aceste randuri inaintea folosirii

Instrucțiuni de siguranță

Următoarele semne categorizate pot apărea în Ghid.

Signal Words	Meaning
 PERICOL	Indică un risc potențial ridicat care, dacă nu este evitat, va duce la deces sau vătămări grave.
 AVERTIZARE	Indică un pericol potențial mediu sau scăzut care, dacă nu este evitat, poate duce la răni ușoare sau moderate.
 ATENȚIE	Indică un risc potențial care, dacă nu este evitat, ar putea duce la daune materiale, pierderi de date, performanțe mai scăzute sau rezultate imprevizibile.
 SFATURI	Oferă metode care să vă ajute să rezolvați o problemă sau să economisiți timp.
 NOTA	Oferă informații suplimentare ca accent și supliment la text.

Cerințe de siguranță

- Respectați standardele locale de siguranță electrică pentru a vă asigura că tensiunea este stabilă și respectă cerințele de alimentare ale dispozitivului.
- Transportați, utilizați și depozitați dispozitivul sub condițiile de umiditate și temperatură admise. Consultați specificațiile tehnice corespunzătoare ale dispozitivului pentru temperatură și umiditate specifice de lucru.
- Nu așezați dispozitivul într-o locație expusă la umezeală, praf, extrem de caldă sau rece, de radiații electronice puternice sau de condiții de iluminare instabile.
- Nu instalați dispozitivul într-un loc în apropierea sursei de căldură, cum ar fi radiatorul, încălzitorul, cuptorul sau alt dispozitiv generator de căldură, pentru a evita incendiul.
- Împiedicați curgerea lichidului în dispozitiv pentru a evita deteriorarea componentelor interne.
- Instalați dispozitivul în poziție orizontală sau instalați-l pe un loc stabil pentru a preveni căderea acestuia.
- Instalați aparatul într-un loc bine ventilat și nu blocați ventilația aparatului.
- Nu dezamblați dispozitivul voit.
- Evitați loviturile puternice, vibrațiile violente și umiditatea în timpul transportului, depozitării și instalării. Este necesar un pachet complet în timpul transportului.
- Utilizați pachetul de fabrică sau echivalent în timpul transportului.

Bateriile

Puterea redusă a bateriei afectează funcționarea RTC, determinând resetarea la fiecare pornire. Când bateria are nevoie de înlocuire, în raportul serverului produsului va apărea un mesaj de jurnal. Pentru mai multe informații despre raportul serverului, consultați paginile de configurare ale produsului sau contactați asistența Dahua.



AVERTIZARE

- Risc de explozie dacă bateria este înlocuită incorrect.
- Înlocuiți numai cu o baterie identică sau cu o baterie recomandată de Dahua.
- Aruncați bateriile uzate în conformitate cu reglementările locale sau cu instrucțiunile producătorului bateriei.

Čeština

Důležitá bezpečnostní opatření a varování

Tato kapitola popisuje obsah vztahující se na správnou manipulaci se zařízením, prevenci nebezpečí a prevenci škod na majetku. Pečlivě si tyto informace přečtěte před použitím zařízení, během používání zařízení je dodržujte a uschovejte je pro budoucí použití.

Bezpečnostní pokyny

Tato příručka může obsahovat následující kategorie signálních slov.

Signální slova	Význam
 NEBEZPEČÍ	Označuje možnost závažného nebezpečí, které, pokud by mu nebylo zamezeno, může mít za následek smrt nebo vážné zranění.
 VAROVÁNÍ	Označuje možnost středně nebo málo závažného nebezpečí, které, pokud by mu nebylo zamezeno, může mít za následek lehké nebo nepříliš závažné zranění.
 UPOZORNĚNÍ	Označuje možné riziko, které, pokud by mu nebylo zamezeno, může mít za následek škodu na majetku, ztrátu dat, snížení výkonu nebo neočekávaný výsledek.
 TIPY	Uvádí metody, které vám pomohou vyřešit problém nebo vám ušetří čas.
 POZNÁMKA	Poskytuje dodatečné informace formou důrazu a doplnění textu.

Bezpečnostní požadavek

- Dodržujte místní normy pro elektrickou bezpečnost pro zajištění stabilního napětí a dodržení požadavků na napájení zařízení.
- Zařízení přepravujte, používejte a skladujte při odpovídající teplotě a vlhkosti. Konkrétní pracovní teplotu a vlhkost naleznete v příslušných technických specifikacích zařízení.
- Neumísťujte zařízení tam, kde bude vystaveno vlhkosti, prachu, extrémnímu horku nebo chladu, silnému elektronickému záření nebo nestabilním světelným podmínkám.
- Neinstalujte zařízení v blízkosti zdrojů tepla, jako je radiátor, ohřívač, kotel nebo jiné zařízení generující teplo, aby nedošlo k požáru.
- Zamezte proniknutí kapalin do zařízení, aby nedošlo k poškození jeho vnitřních součástí.
- Zařízení instalujte vodorovně nebo je instalujete na stabilním místě, aby bylo chráněno před pádem.

- Zařízení instalujte na dobře větraném místě a neblokuje odvětrávání zařízení.
- Zařízení svévolně nedemontujte.
- Během přepravy, skladování a instalace zamezte silnému tlaku, prudkým vibracím a namočení. Při přepravě je nezbytné úplné zabalení.
- Při přepravě použijte obal z výroby nebo obdobný obal.

Baterie

Nízké nabití baterie ovlivňuje fungování hodin ve skutečném čase a způsobuje, že se při každém spuštění resetují. V případě, že je třeba baterii vyměnit, se v serverové zprávě produktu zobrazí zpráva protokolu. Další informace o serverové zprávě naleznete na stránkách o nastavení produktu, případně kontaktujte podporu společnosti Dahua.



VAROVÁNÍ

- Nebezpečí výbuchu v případě nesprávné výměny baterie.
- Vyměňte pouze za totožnou baterii nebo baterii doporučenou společností Dahua.
- Použité baterie likvidujte v souladu s místními předpisy nebo pokyny výrobce baterie.

Ε λ λ η ν ι κ ά

Σημαντικές Διασφαλίσεις και Προειδοποιήσεις

Αυτό το Κεφάλαιο περιγράφει το περιεχόμενο που καλύπτει το σωστό χειρισμό της Συσκευής, την πρόληψη των κινδύνων και την πρόληψη της καταστροφής της ιδιοκτησίας. Διαβάστε προσεκτικά τα αναγραφόμενα πριν χρησιμοποιήσετε τη Συσκευή, τηρήστε τα κατά τη χρήση και κρατήστε τα καλά για μελλοντική χρήση.

Οδηγίες Ασφαλείας

Τα ακόλουθα κατηγοριοποιημένα σήματα με λέξεις έχουν καθορισμένη σημασία και ενδέχεται να εμφανίζονται στις Οδηγίες Χρήσης.

Σήματα με λέξεις	Σημασία
 Κ Ι Ν Δ Υ Ν Ο Σ	Δείχνει έναν υψηλό δυνητικό κίνδυνο, ο οποίος, εάν δεν αποφευχθεί, θα έχει ως αποτέλεσμα θάνατο ή σοβαρό τραυματισμό.
 Π Ρ Ο Ε Ι Δ Ο Π Ο Ι Η Σ Η	Υποδεικνύει έναν μεσαίο ή χαμηλό δυνητικό κίνδυνο, ο οποίος, αν δεν αποφευχθεί, θα μπορούσε να προκαλέσει ελαφρύ ή μέτριο τραυματισμό.
 Π Ρ Ο Σ Ο Χ Η	Δείχνει έναν πιθανό κίνδυνο, ο οποίος, εάν δεν αποφευχθεί, θα μπορούσε να προκαλέσει ζημιά στην ιδιοκτησία, απώλεια δεδομένων, χαμηλότερη απόδοση ή απρόβλεπτο αποτέλεσμα.

Σήματα με λέξεις	Σημασία
 Σ Υ Μ Β Ο Υ Λ Ε Σ	Παρέχει μεθόδους που θα σας βοηθήσουν να επιλύσετε ένα πρόβλημα ή να εξοικονομήσετε χρόνο.
 Σ Η Μ Ε Ι Ω Σ Η	Παρέχει πρόσθετες πληροφορίες δίνοντας έμφαση και συμπληρώνοντας το κείμενο.

Απαιτήσεις ασφαλείας

- Τηρήστε τα τοπικά πρότυπα ηλεκτρικής ασφάλειας για να βεβαιωθείτε ότι η τάση είναι σταθερή και συμμορφώνεται με την απαίτηση τροφοδοσίας της συσκευής.
- Μεταφέρετε, χρησιμοποιήστε και αποθηκεύστε τη συσκευή υπό τις επιτρεπόμενες συνθήκες υγρασίας και θερμοκρασίας. Ανατρέξτε στις αντίστοιχες τεχνικές προδιαγραφές της συσκευής για τη συγκεκριμένες συνθήκες λειτουργίας θερμοκρασίας και υγρασίας.
- Μην τοποθετείτε τη συσκευή σε θέση που είναι εκτεθειμένη σε υγρασία, σκόνη, ακραία ζέστη ή κρύο, ισχυρή ηλεκτρονική ακτινοβολία ή ασταθές φωτισμό.
- Μην τοποθετείτε τη συσκευή σε μέρος κοντά στην πηγή θερμότητας, όπως καλοριφέρ, θερμάστρα, κλίβανο ή άλλη συσκευή παραγωγής θερμότητας για να αποφύγετε τη φωτιά.
- Αποφύγετε να ρέει υγρό μέσα στη συσκευή για να αποφύγετε την αποδυνάμωση των εσωτερικών εξαρτημάτων.
- Εγκαταστήστε τη συσκευή οριζόντια ή εγκαταστήστε την στο σταθερό μέρος για να μην πέσει.
- Τοποθετήστε τη συσκευή σε καλά αεριζόμενο μέρος και μην εμποδίζετε τον εξαερισμό της συσκευής.
- Μην αποσυναρμολογείτε αυθαίρετα τη συσκευή.
- Αποφύγετε την υψηλή συμπίεση, το υψηλό βάρος, τη βίαιη δόνηση και τη διαβροχή κατά τη διάρκεια της μεταφοράς, της αποθήκευσης και της εγκατάστασης. Το πλήρες πακέτο είναι απαραίτητο κατά τη μεταφορά.
- Χρησιμοποιήστε το εργοστάσιακό πακέτο ή το αντίστοιχο για μεταφορά.

Μπαταρία

Η χαμηλή ισχύς της μπαταρίας επηρεάζει τη λειτουργία του RTC, προκαλώντας την επαναφορά του σε κάθε επανεκκίνηση. Όταν η μπαταρία χρειάζεται αντικατάσταση, ένα μήνυμα συμβάντος θα εμφανιστεί στην αναφορά συμβάντων του διακομιστή. Για περισσότερες πληροφορίες σχετικά με την αναφορά διακομιστή, ανατρέξτε στις σελίδες εγκατάστασης του προϊόντος ή επικοινωνήστε με την υποστήριξη Dahua.



Π Ρ Ο Ε Ι Δ Ο Π Ο Ι Η Σ Η

- Κίνδυνος έκρηξης σε περίπτωση λανθασμένης αντικατάστασης της μπαταρίας.
- Αντικαταστήστε μόνο με πανομοιότυπη μπαταρία ή μπαταρία που συνιστάται από τη Dahua.
- Απορρίψτε τις χρησιμοποιημένες μπαταρίες σύμφωνα με τους τοπικούς κανονισμούς ή τις οδηγίες του κατασκευαστή της μπαταρίας.

Važne zaštitne mjere i upozorenja

Ovo poglavlje opisuje sadržaj koji obuhvaća pravilno rukovanje uređajem, sprječavanje opasnosti i sprečavanje oštećenja imovine. Pažljivo pročitajte ove sadržaje prije korištenja Uređaja, pridržavajte ih se pri upotrebi i sačuvajte ih za buduću uporabu.

Sigurnosne upute

U vodiču se mogu pojaviti sljedeće kategorizirane signalne riječi s definiranim značenjem.

Signal Words	Meaning
 OPASNOST	Označava veliku potencijalnu opasnost koja će, ako se ne izbjegne, rezultirati smrću ili ozbiljnim ozljedama.
 UPOZORENJE	Označava srednju ili malu potencijalnu opasnost koja, ako se ne izbjegne, može rezultirati malom ili umjerenom ozljedom.
 OPREZ	Ukazuje na potencijalni rizik koji, ako se ne izbjegne, može rezultirati oštećenjem imovine, gubitkom podataka, manjom učinkovitošću ili nepredvidivim rezultatom.
 SAVJETI	Pružava vam metode kojim vam pomaže riješiti problem ili će vam uštedjeti vrijeme.
 BILJEŠKA	Pružava dodatne informacije kao naglasak i dopunu teksta.

Sigurnosni zahtjevi

- Avoid heavy stress, violent vibration, and soaking during during transportation, storage, and installation. Complete package is necessary during the transportation.
- Pridržavajte se lokalnih električnih sigurnosnih standarda kako biste osigurali da je napon stabilan i da udovoljava zahtjevima napajanja uređaja.
- Prijenosite, upotrebljavajte i pohranjujte uređaj pod dopuštenim uvjetima vlage i temperature. Pogledajte odgovarajuće tehničke specifikacije uređaja za određenu radnu temperaturu i vlagu.
- Nemojte postavljati uređaj na mjesto izloženo vlazi, prašini, ekstremno vrućoj ili hladnoj okolini, jakom elektronskom zračenju ili nestabilnim uvjetima osvjetljenja.
- Kako biste izbjegli požar nemojte postavljati uređaj na mjesto u blizini izvora topline, kao što su radijator, grijač, peć ili neki drugi uređaj za stvaranje topline.
- Spriječite da tekućina teče u uređaj kako bi se izbjegla šteta na unutarnjim dijelovima.
- Ugradite uređaj vodoravno ili ga postavite na stabilno mjesto kako biste spriječili padanje.
- Ugradite uređaj na dobro prozračeno mjesto i ne blokirajte ventilaciju uređaja.
- Nemojte rastavljati uređaj samovoljno.
- Izbjegavajte teški stres, nasilne vibracije i natapanje tijekom prijevoza, skladištenja i instalacije. Prilikom prijevoza potrebno je koristiti tvorničko

- zaštitno pakiranje.
- Koristite tvorničko pakiranje ili ekvivalent za transport.

Baterija

Niska baterija utječe na rad RTC, uzrokujući da se resetira pri svakom uključivanju. Kad bateriju treba zamijeniti, pojaviti će se poruka u izvješću poslužitelja (server). Dodatne informacije o izvješću poslužitelja (server) potražite na stranicama priručnika proizvođača ili se obratite Dahua podršci.



UPOZORENJE

- Rizik od eksplozije ako se baterija nepravilno zamijeni.
- Zamijeniti samo sa jednakom baterijom ili sa baterijom koja je preporučena od strane Dahua Technology.
- instructions. Dotrajale baterije treba zbrinuti u skladu sa lokalnim propisima ili u skladu s uputama proizvođača baterije.

Slovenčina

Dôležité bezpečnostné pokyny a varovania

Táto kapitola obsahuje informácie týkajúce sa správnej manipulácie so zariadením, prevencie pred nebezpečenstvom a prevencie poškodenia majetku. Pred používaním zariadenia si pozorne prečítajte tieto informácie, dodržiavajte ich pri používaní a uchovajte ich na budúce použitie.

Bezpečnostné pokyny

V príručke sa môžu nachádzať nasledujúce kategorizované signálne výrazy s definovaným významom.

Signálne výrazy	Význam
 NEBEZPEČENSTVO	Označuje vysoké potenciálne nebezpečenstvo, ktoré spôsobí smrť alebo vážne zranenie, ak sa mu nevyhnete.
 VAROVANIE	Označuje stredné alebo nízke potenciálne nebezpečenstvo, ktoré môže mať za následok mierne alebo stredne ťažké zranenie, ak sa mu nevyhnete.
 POZOR	Označuje potenciálne riziko, ktoré môže viesť k poškodeniu majetku, strate údajov, zníženiu výkonu alebo nepredvídateľnému výsledku, ak sa mu nevyhnete.
 TIPY	Poskytuje metódy, ktoré vám pomôžu vyriešiť problém alebo ušetriť čas.
 POZNÁMKA	Poskytuje ďalšie informácie ako zdôraznenie a doplnenie textu.

Požiadavky na bezpečnosť

- Dodržujte miestne elektrické bezpečnostné normy, aby ste zabezpečili, že napätie je stabilné a zodpovedá požiadavkám na napájanie zariadenia.
- Zariadenie prepravujte, používajte a uchovávajte pri povolených podmienkach

vlhkosti a teploty. Prečítajte si príslušné technické špecifikácie zariadenia pre špecifickú pracovnú teplotu a vlhkosť.

- Zariadenie neumiestňujte na miesto vystavené vlhkosti, prachu, extrémnemu teplu alebo chladu, silnému elektronickému žiareniu alebo nestabilným podmienkam osvetlenia.
- Zariadenie neinštalujte na miesto, ktoré sa nachádza blízko zdroja tepla, ako je napríklad radiátor, ohrievač, pec alebo iné zariadenie na tvorbu tepla. Predídete tak vzniku požiaru.
- Zabráňte vnikaniu kvapaliny do zariadenia, aby nedošlo k poškodeniu vnútorných komponentov.
- Zariadenie nainštalujte horizontálne alebo ho nainštalujte na stabilné miesto, aby ste zabránili pádu.
- Zariadenie nainštalujte na dobre vetranom mieste a neblokujte ventiláciu zariadenia.
- Zariadenie svojvoľne nerozoberajte.
- Počas prepravy, skladovania a inštalácie sa vyhnite silnému namáhaniu, prudkým vibráciám a namáčaniam. Počas prepravy je potrebné prepravovať kompletne balenie.
- Na prepravu použite továrenské balenie alebo jeho ekvivalent.

Batéria

Nízka kapacita batérie ovplyvňuje prevádzku RTC, čo spôsobí jeho vynulovanie pri každom zapnutí. Keď je batériu potrebné vymeniť, v správe servera produktu sa zobrazí hlásenie. Ďalšie informácie o hlásení servera nájdete na stránkach s nastaveniami produktu alebo sa obráťte na podporu spoločnosti Dahua.



VAROVANIE

- Nebezpečenstvo výbuchu, ak je batéria nesprávne vymenená.
- Vymeňte iba za tú istú batériu alebo batériu, ktorú odporúča spoločnosť Dahua.
- Použité batérie zlikvidujte v súlade s miestnymi predpismi alebo pokynmi výrobcu batérie.

Српски

Važne Zaštitne mere i Upozorenja

Ovo poglavlje opisuje sadržaj koji pokriva pravilno rukovanje uređajem, sprečavanje opasnosti i sprečavanje oštećenja imovine. Pažljivo pročitajte ove sadržaje pre korišćenja uređaja, pošaljite ih kada koristite i čuvajte ga za buduću referencu.

Bezbednosna Uputstva

Sledeće kategorije reči sa definisanim značenjem mogu se pojaviti u „Vodiču“.

Oznaka	Značenje
 OPASNOST	Označava visoku potencijalnu opasnost koja će, ako se i ne izbegne, rezultirati smrću ili ozbiljnim povredama.

Oznaka	Značenje
 UPOZORENJE	Označava opasnost srednje ili niske potencijale koja bi, ukoliko se ne izbegne, mogla dovesti do blagih ili umerenih povreda.
 OPREZ	Označava potencijalni rizik koji bi, ukoliko se to ne izbegne, mogao dovesti do oštećenja imovine, gubitka podataka, niže performanse ili nepredvidivog rezultata.
 PREPORUKE	Pruža metode za pomoć u rešavanju problema ili uštede vremena.
 BELEŠKA	Pruža dodatne informacije kao naglasak i dodatak tekstu.

Bezbednosna Uputstva

- Pridržavajte se lokalnih standarda električne sigurnosti kako biste bili sigurni da je napon stabilan i da odgovara zahtevu za napajanje uređaja.
- Prevoz, korišćenje i skladištenje uređaja treba da budu u skladu sa dozvoljenim uslovima vlage i temperaturnim uslovima. Pogledajte odgovarajuće tehničke specifikacije uređaja koji se odnose na specifičnu radnu temperaturu i vlažnost vazduha.
- Nemojte postavljati uređaj na mesto izloženo vlazi, prašini, ekstremnom vrućem ili hladnom vazduhu, jakom elektronskom zračenju ili nestabilnim uslovima osvetljenja.
- Ne postavljajte uređaj na mesto blizu izvora toplote, kao što je radiator, grejač, peć ili drugi uređaj za proizvodnju toplote kako biste izbegli požar.
- Sprečite tečnost da teče u uređaj kako bi se izbeglo oštećenje unutrašnjih komponenti.
- Instalirajte uređaj horizontalno ili postavite na stabilno mesto kako biste sprečili padanje.
- Ugradite uređaj na dobro provetreno mesto i ne blokirajte ventilaciju uređaja.
- Nemojte rastavljati uređaj proizvoljno.
- Izbegavajte jak pritisak, nasilne vibracije i usisavanje tokom transporta, skladištenja i instalacije. Kompletan paket je neophodan tokom transporta.
- Koristite fabričko pakovanje ili ekvivalent u toku transporta.

Baterija

Baterija male snage utiče na rad RTC-a, dovodeći do reseta pri svakom uključivanju. Kada se baterija mora zameniti, logovna poruka će se pojaviti u izveštaju servera proizvođača. Za više informacija o izveštaju servera, pogledajte stranice za podešavanje proizvođača ili kontaktirajte Dahua podršku.



UPOZORENJE

- Opasnost od eksplozije ako se baterija nepravilno zameni.
- Zamenite je samo sa identičnom baterijom ili sa baterijom koju preporučuje Dahua.
- Odložite iskorišćene baterije u skladu sa lokalnim propisima ili uputstvima proizvođača baterije.

Türkçe

Önemli Kurallar ve Uyarılar

Bu Bölüm, Cihazın doğru kullanımını, tehlike önlemeyi ve mal zararının önlenmesini kapsayan içerikleri anlatmaktadır. Cihazı kullanmadan önce bu içerikleri dikkatli şekilde okuyun, kullanırken bunlara uyun ve ileride başvurmak üzere saklayın.

Güvenlik Talimatları

Aşağıda, belirtilen açıklamaya sahip kategorize edilmiş uyarı sözcüklerini Kılavuzda görebilirsiniz.

Uyarı Sözcükleri	Anlamı
 TEHLİKE	Kaçınılmaması durumunda ölüm veya ciddi yaralanmalara neden olacak yüksek potansiyelli bir tehlikeyi belirtir.
 UYARI	Kaçınılmaması durumunda hafif veya orta dereceli yaralanmaya neden olabilecek orta veya düşük potansiyelli bir tehlikeyi belirtir.
 DİKKAT	Kaçınılmaması durumunda mal hasarına, veri kaybına, düşük performansa veya tahmin edilemeyen sonuca neden olabilecek potansiyel bir riski belirtir.
 İPUÇLARI	Bir problemi çözmenize veya zamandan tasarruf etmenize yardımcı olmak için yöntemler sunar.
 NOT	Metne pekiştirme ve ek olarak ilave bilgiler sağlar.

Güvenlik Gereksinimi

- Voltajın istikrarlı olduğundan ve cihazın güç kaynağı gereksinimine uygun olduğundan emin olmak için yerel elektrik güvenliği standartlarına uyun.
- Cihazı izin verilen nem ve sıcaklık şartları altında nakledin, kullanın ve saklayın. Belirli çalışma sıcaklığı ve nem değerleri için cihazın ilgili teknik özelliklerine bakın.
- Cihazı rutubete, toza, aşırı ısıya veya soğuğa, güçlü elektronik radyasyona veya değişken aydınlatma şartlarına maruz kalan bir yere yerleştirmeyin.
- Yangını önlemek için cihazı radyatör, ısıtıcı, fırın veya başka ısı üreten cihazlar gibi ısı kaynağına yakın bir yere monte etmeyin.
- İçerisindeki parçaların hasar görmesini önlemek için cihazın içerisine sıvıların girmesini önleyin.
- Cihazın düşmesini önlemek için yatay olarak veya dayanıklı bir yere monte edin.

- Cihazı iyi havalandırılan bir yere monte edin ve cihazın hava sirkülasyonunu engellemeyin.
- Cihazın parçalarını gelişigüzel sökmeyin.
- Cihazın nakliyesi, saklanması ve montajı esnasında ağır baskılardan, şiddetli sarsıntılardan ve sıvıya batmalardan kaçının. Cihazın nakliyesi esnasında ambalajın tamamı gereklidir.
- Nakliye için fabrikasyon ambalajı ya da eş değerini kullanın.

Pil

Düşük pil gücü, her güç açma esnasında sıfırlanmasına neden olarak RTC'nin çalışmasını etkiler. Pillerin değiştirilmesi gerektiğinde ürünün sunucu raporunda bir günlük iletisi görüntülenir. Sunucu raporu hakkında daha fazla bilgi için ürünün kurulum sayfalarına bakın veya Dahua destek merkeziyle iletişime geçin.



UYARI

- Pil yanlış şekilde takılırsa patlama tehlikesi.
- Sadece aynı türde veya Dahua tarafından önerilen bir pil takın.
- Eski pilleri, yerel yönetmeliklere veya pil üreticisinin talimatlarına göre elden çıkarın.

עברית

חשיבות בעלי ואזהרות זהירות אמצעי

יש רכוש נזקי ומניעת בעיות מניעת, במכשיר נאות טיפול בנושא התכנים את מתאר זה פרק המכשיר הפעלת בעת לאורם לפעול, במכשיר שימוש לפני לב בתשומת אלה תכנים לקרוא עתידי לעיון אותם ולשמור.

בטיחות הנחיות

במדריך להופיע עשויות המוגדרים הפירושים עם הבאות המסווגות הסימון מילות.

משמעות	סימון מילות
לגרום עשויה, תימנע לא שאם, גבוהה בסבירות סכנה מציינת קשה לפציעה או למוות.	 סכנה
עשויה, תימנע לא שאם, נמוכה או בינונית בסבירות סכנה מציינת בינונית או קלה לפציעה לגרום.	 אזהרה
אובדן, לנזק לגרום עשויה, תימנע לא שאם לסכנה סבירות מציינת צפויות לא לתוצאות או הביצועים ברמת הפחתה, מידע.	 זהירות
זמן לך שיחסכו או בעיות לפתור לך שיסייעו שיטות מספקות.	 עצות

סימון מילות	משמעות
הערה 	ולהשלמתו לטקסט להדגשה נוסף מידע מספקת.

בטיחות דרישת

- ותואם יציב שהמתח להבטיח מנת על בחשמל לבטיחות המקומיים התקנים לכל לציית יש המכשיר של החשמל אספקת לדרישות.
- המותרים והלחות הטמפרטורה לתנאי בהתאם יעשו המוצר של ואחסון שימוש, הובלה המוגדרים וללחות לטמפרטורה המכשיר של המקבילים הטכניים למפרטים להתייחס יש עבודה לביצוע.
- קרינה, קיצוניים חום או קור תנאי, אבק, לרטיבות חשוף במקום המכשיר את למקם אין יציבים לא תאורה תנאי או חזקה חשמלית.
- מכשיר או כבשן, תנור, מקרן כגון, חום מקור בקרבת המכשיר את להתקין אין מנת על חום שפולט אחר.
- הפנימיים למרכיביו נזק למנוע מנת על המכשיר על נזל משפיכת להימנע יש יציב במקום או מאוזנת בצורה המכשיר את להתקין יש, לייפו שלא מנת על.
- למכשיר האוויר מעבר את לחסום ולא היטב מאוורר במקום המכשיר את להתקין יש.
- עצמך בכוחות המכשיר את לפרק אין.
- אחסונו, המכשיר הובלת במהלך הרטבתו או חזק טלטול, כבד משקל מהצבת להימנע יש.
- המלאה באריזתו להשתמש שי המכשיר העברת לשם. התקנתו או.
- במקבילה או היצרן ידי על המסופקת באריזה להשתמש יש המכשיר העברת לשם.

סוללה

צורך יש כאשר. שלו הדלקה בכל להתאפס לו ותגרום RTC-ה פעולת על תשפיע חלשה סוללה ח"דו אודות נוסף למידע. המוצר של השרת ח"דו אירועים יומן הודעת תופיע, הסוללה בהחלפת Dahua של התמיכה עם קשר ליצור או המוצר של ההגדרה בדפי לעיין יש, השרת



אזהרה

- לפיצוץ לגרום עלולה הסוללה של נכונה לא החלפה.
- Dahua ידי על שמומלצת כזו או זהה בסוללה ורק אך להחליף יש.
- היצרן של להנחיותיו או המקומיות לתקנות בהתאם משומשות סוללות לסלק יש.

Français

Précautions et avertissements importants

Le contenu de ce chapitre aborde la bonne manipulation de l'appareil, la prévention des risques et la prévention des dommages matériels. Lisez ce contenu soigneusement avant d'utiliser l'appareil, respectez-le lorsque vous l'utilisez, et conservez-le pour vous y référer ultérieurement.

Précautions d'emploi

Les mentions d'avertissement catégorisées suivantes ayant un sens défini sont susceptibles d'apparaître dans le manuel.

Mentions d'avertissement	Signification
 DANGER	Indique un danger à risque élevé qui entraînera la mort ou des blessures graves si les instructions données ne sont pas respectées.
 AVERTISSEMENT	Indique une situation moyennement ou faiblement dangereuse qui entraînera des blessures faibles ou modérées si les instructions données ne sont pas respectées.
 AVERTISSEMENT	Indique une situation potentiellement dangereuse qui pourra entraîner des dommages de la propriété, des pertes de données, une performance moindre ou des résultats imprévisibles, si les instructions données ne sont pas respectées.
 ASTUCES	Fournit des instructions qui vous permettront de résoudre un problème ou de vous faire gagner du temps.
 REMARQUE	Fournit des informations supplémentaires pour mettre en évidence et compléter le texte.

Exigences de sécurité

- Respectez les normes de sécurité électrique locales pour vous assurer que la tension est stable et conforme aux exigences d'alimentation de l'appareil.
- Transportez, utilisez et stockez l'appareil dans les conditions d'humidité et de température autorisées. Consultez les spécifications techniques correspondantes de l'appareil pour connaître la température et l'humidité de fonctionnement spécifiques.
- Ne placez pas l'appareil dans un lieu exposé à l'humidité, à la poussière, à une chaleur ou un froid extrême, à de forts rayonnements électroniques, ou à des conditions d'éclairage instables.
- N'installez pas l'appareil près d'une source de chaleur telle qu'un radiateur, un chauffage, une chaudière, ou tout autre dispositif générant de la chaleur afin d'éviter les risques d'incendie.
- Empêchez aux liquides de couler sur l'appareil afin d'éviter d'endommager les composants internes.
- Installez l'appareil horizontalement ou sur une surface stable afin de l'empêcher de tomber.
- Installez l'appareil dans un lieu bien ventilé et ne bloquez pas la ventilation de l'appareil.
- Ne démontez pas l'appareil de façon arbitraire.
- Au cours du transport, du stockage et de l'installation de l'appareil, évitez de le soumettre à de fortes contraintes, à des vibrations violentes ou à une immersion. L'emballage complet est nécessaire au cours du transport.
- Utilisez l'emballage d'usine ou équivalent pour le transport.

Batterie

Un niveau de batterie faible affecte le fonctionnement du RTC, qui se réinitialisera à chaque redémarrage. Lorsque la batterie doit être remplacée, un message de journal apparaît dans le rapport du serveur du produit. Pour plus d'informations sur le rapport du serveur, consultez les pages de configuration du produit ou contactez l'assistance Dahua.



AVERTISSEMENT

- Risque d'explosion si la batterie est remplacée de façon incorrecte.
- Remplacez la batterie uniquement par une batterie recommandée par Dahua.
- Éliminez les batteries usagées conformément aux réglementations locales ou aux instructions du fabricant de la batterie.

Español(España)

Advertencias y precauciones de seguridad importantes

En este capítulo se describe el contenido que cubre la manipulación correcta del dispositivo, la prevención de riesgos y la prevención de daños materiales. Lea detenidamente este contenido antes de usar el dispositivo, sígalo cuando lo utilice y consérvelo para consultas futuras.

Instrucciones de seguridad

Las siguientes palabras de advertencia con un significado definido podrían aparecer en la guía.

Palabras de advertencia	Significado
 PELIGRO	Indica un riesgo potencial alto que, si no se evita, resultará en muerte o lesiones graves.
 ADVERTENCIA	Indica un riesgo potencial medio o bajo que, si no se evita, podría resultar en lesiones leves o moderadas.
 PRECAUCIÓN	Indica un riesgo potencial que, si no se evita, podría resultar en daños materiales, pérdida de datos, rendimiento menor o resultados impredecibles.
 CONSEJOS	Ofrece métodos para ayudarle a resolver un problema o ahorrar tiempo.
 NOTA	Proporciona información adicional como hincapié y complemento para el texto.

Requisitos de seguridad

- Cumpla las normas locales de seguridad eléctrica para garantizar que la tensión sea estable y cumpla los requisitos de alimentación eléctrica del dispositivo.
- Transporte, utilice y almacene el dispositivo bajo las condiciones de humedad y temperatura permitidas. Consulte las especificaciones técnicas

correspondientes del dispositivo para la temperatura y humedad operativas específicas.

- No coloque el dispositivo en un lugar expuesto a humedad, polvo, calor o frío extremos, radiaciones electrónicas fuertes o condiciones de iluminación inestables.
- No instale el dispositivo en un lugar cerca de fuentes de calor, como radiadores, calentadores, hornos u otros dispositivos generadores de calor, para evitar un incendio.
- No deje que entre líquido en el dispositivo para evitar daños en los componentes internos.
- Instale el dispositivo horizontalmente o instálelo sobre un lugar estable para evitar que caiga.
- Instale el dispositivo en un lugar bien ventilado y no obstruya la ventilación.
- No desmonte de forma arbitraria el dispositivo.
- Evite las presiones excesivas, las vibraciones violentas y mojar el dispositivo durante el transporte, almacenamiento e instalación. Es necesario utilizar el embalaje completo durante el transporte.
- Utilice el embalaje de fábrica o uno equivalente para transportarlo.

Pilas

La baja batería afecta al funcionamiento del RTC, provocando que se restablezca cada vez que recibe alimentación. Cuando sea necesario sustituir las pilas, aparecerá un mensaje de registro en el informe de servidor del producto. Para más información acerca del informe de servidor, consulte las páginas de configuración del producto o póngase en contacto con el departamento de soporte de Dahua.



ADVERTENCIA

- Riesgo de explosión si se sustituyen incorrectamente las pilas.
- Sustitúyalas únicamente por pilas idénticas o pilas recomendadas por Dahua.
- Elimine las pilas gastadas en conformidad con la normativa local o las instrucciones del fabricante de las pilas.

Deutsch

Wichtige Sicherheits- und Warnhinweise

Dieses Kapitel beschreibt die Inhalte zum richtigen Umgang mit dem Gerät, zur Verhütung von Gefahren und zur Vermeidung von Sachschäden. Lesen Sie dieses Kapitel sorgfältig durch, bevor Sie das Gerät verwenden, halten Sie die Anweisungen bei der Verwendung ein und bewahren Sie diese Anleitung zum späteren Nachlesen gut auf.

Sicherheitshinweise

Die folgenden kategorisierten Signalwörter mit definierter Bedeutung können in der Kurzanleitung verwendet werden.

Signalwörter	Bedeutung
 GEFAHR	Weist auf ein hohes Gefahrenpotential hin, das, wenn es nicht vermieden wird, zum Tod oder zu schweren Verletzungen führt.

Signalwörter	Bedeutung
 WARNUNG	Weist auf eine mittlere oder geringe potentielle Gefahr hin, die, wenn sie nicht vermieden wird, zu leichten oder mittelschweren Verletzungen führen kann.
 VORSICHT	Weist auf ein potenzielles Risiko hin, das, wenn es nicht vermieden wird, zu Sachschäden, Datenverlust, geringerer Leistung oder unvorhersehbaren Ergebnis führen kann.
 TIPPS	Stellt Methoden bereit, mit denen Sie ein Problem lösen oder Zeit sparen können.
 HINWEIS	Bietet zusätzliche Informationen als Schwerpunkt und Ergänzung zum Text.

Sicherheitsanforderungen

- Halten Sie sich an die örtlichen elektrischen Sicherheitsnormen, um sicherzustellen, dass die Spannung stabil ist und den Anforderungen an die Stromversorgung des Geräts entspricht.
- Transportieren, verwenden und lagern Sie das Gerät unter den zulässigen Feuchtigkeits- und Temperaturbedingungen. Die entsprechenden technischen Spezifikationen des Geräts für die jeweilige Betriebstemperatur und Luftfeuchtigkeit sind zu beachten.
- Stellen Sie das Gerät nicht an Orten auf, an denen es Feuchtigkeit, Staub, extremer Hitze oder Kälte, starker elektronischer Strahlung oder instabilen Lichtverhältnissen ausgesetzt ist.
- Installieren Sie das Gerät nicht in der Nähe einer Wärmequelle, z. B. einem Heizkörper, Heizlüfter, Ofen oder anderen Wärme erzeugenden Geräten, um Feuer zu vermeiden.
- Verhindern Sie, dass Flüssigkeit in das Gerät fließt, um Schäden an internen Bauteilen zu vermeiden.
- Installieren Sie das Gerät waagerecht oder an einem stabilen Ort, damit es nicht herunterfällt.
- Installieren Sie das Gerät an einem gut belüfteten Ort und blockieren Sie die Belüftung des Geräts nicht.
- Nehmen Sie das Gerät nicht eigenmächtig auseinander.
- Vermeiden Sie starke Belastungen, Vibrationen und eindringende Nässe während des Transports, der Lagerung und der Installation. Das Gerät sollte immer vollständig verpackt transportiert werden.
- Verwenden Sie die ab Werk verwendete Verpackung oder eine gleichwertige Verpackung für den Transport.

Batterie

Eine niedrige Batterieleistung beeinträchtigt den Betrieb der Echtzeituhr, wodurch sie bei jedem Einschalten zurückgesetzt wird. Wenn die Batterie ausgetauscht werden muss, wird eine Protokollmeldung im Serverbericht des Produkts angezeigt. Weitere Informationen zum Serverbericht finden Sie auf den Einrichtungsseiten des Produkts oder wenden Sie sich an den Support von Dahua.



WARNUNG

- Bei nicht ordnungsgemäßigem Austausch der Batterie besteht

Explosionsgefahr.

- Ersetzen Sie die Batterie nur durch eine identische Batterie oder eine Batterie, die von Dahua empfohlen wird.
- Entsorgen Sie leere Batterien entsprechend den örtlichen Vorschriften oder den Anweisungen des Batterieherstellers.

Italiano

Norme di sicurezza e avvertenze importanti

Il presente capitolo descrive le procedure per una corretta manipolazione del dispositivo, per la prevenzione dei rischi e per la prevenzione di danni materiali. Leggere attentamente queste informazioni prima di utilizzare il dispositivo, attenersi alle istruzioni fornite durante l'uso e conservarle come futuro riferimento.

Istruzioni di sicurezza

I seguenti indicatori di pericolo, aventi i significati indicati, possono apparire nella presente guida.

Indicatori di pericolo	Significato
 PERICOLO	Indica una situazione ad alto rischio che, se non viene evitata, può causare il decesso o gravi lesioni.
 AVVERTENZA	Indica una situazione a medio o basso rischio che, se non viene evitata, può causare lesioni di leggera o moderata entità.
 ATTENZIONE	Indica un rischio potenziale che, se non evitato, può causare danni materiali, perdite di dati, riduzione delle prestazioni o altre conseguenze imprevedibili.
 CONSIGLI	Spiegano metodi utili per risolvere un problema o per aiutarvi a risparmiare tempo.
 NOTA	Fornisce informazioni aggiuntive che completano quelle riportate nel testo.

Requisiti di sicurezza

- Attenersi alle leggi locali sulla sicurezza elettrica per garantire una tensione stabile e soddisfare i requisiti di alimentazione del dispositivo.
- Trasportare, utilizzare e conservare il dispositivo alle condizioni di umidità e temperatura consentite. Fare riferimento alle specifiche tecniche del dispositivo per conoscere i valori specifici della temperatura di esercizio e dell'umidità.
- Non posizionare il dispositivo in un ambiente esposto ad una eccessiva umidità, a polvere, a condizioni di caldo e freddo estremi, a forti radiazioni elettroniche o a condizioni di illuminazione non stabile.
- Non installare il dispositivo vicino ad una fonte di calore, quali ad esempio radiatori, apparecchi di riscaldamento, forni o altri dispositivi di generazione del calore, per evitare il rischio di incendio.
- Evitare di versare liquido sul dispositivo per non danneggiare i componenti interni.
- Installare il dispositivo in posizione orizzontale, oppure in una zona stabile, per evitare che possa cadere.

- Installare il dispositivo in un ambiente adeguatamente ventilato e non ostruire la circolazione dell'aria.
- Non smontare il dispositivo in modo casuale.
- Evitare forte sollecitazioni, violente vibrazioni e non bagnare il prodotto durante il trasporto, lo stoccaggio e l'installazione. Trasportare il prodotto utilizzando un imballaggio adeguato.
- Utilizzare l'imballaggio standard previsto o un imballaggio equivalente.

Batteria

L'uso di una batteria scarica può compromettere il funzionamento del dispositivo RTC, che si resetterà ad ogni avvio. Quando è necessario sostituire la batteria, nel report del server del prodotto viene visualizzato un messaggio di log. Per ulteriori informazioni sul report del server, leggere le pagine di configurazione del prodotto, oppure contattare il servizio assistenza di Dahua.



AVVERTENZA

- Se la batteria non viene sostituita correttamente, può generare il rischio di esplosione.
- Sostituire solo con una batteria identica o una batteria raccomandata da Dahua.
- Smaltire le batterie usate in conformità con le normative locali o attenendosi alle istruzioni del produttore della batteria.

Nederlands

Belangrijke voorzorgsmaatregelen en waarschuwingen

Dit hoofdstuk beschrijft de inhoud die de juiste omgang met het apparaat behandelt, het voorkomen van gevaren alsmede het voorkomen van materiële schade. Lees deze inhoud zorgvuldig door voordat u het apparaat gebruikt, houdt u eraan tijdens het gebruik, en bewaar ze goed voor toekomstige referentie.

Veiligheidsinstructies

De volgende gecategoriseerde signaalwoorden met gedefinieerde betekenis staan in de handleiding vermeld.

Signaalwoorden	Betekenis
 GEVAAR	Geeft een hoog potentieel gevaar aan dat, indien niet voorkomen, kan leiden tot overlijden of ernstig.
 WAARSCHUWING	Geeft een gemiddeld of laag potentieel gevaar aan dat, indien niet voorkomen, kan leiden tot licht of matig letsel.
 LET OP	Geeft een potentieel risico aan dat, indien niet voorkomen, kan leiden tot materiële schade, gegevensverlies, lagere prestaties of onvoorspelbaar resultaat.
 TIPS	Biedt methodes om u te helpen een probleem op te lossen of tijd te besparen.
 OPMERKING	Biedt aanvullende informatie als nadruk op en aanvulling van de tekst.

Veiligheidsvereiste

- Houdt u aan plaatselijke veiligheidsstandaarden om ervoor te zorgen dat het voltage stabiel is en voldoet aan de vereiste stroomvoorziening van het apparaat.
- Transporteer, gebruik en bewaar het apparaat onder de toegestane relatieve luchtvochtigheid en temperaturomstandigheden. Zie de overeenkomstige technische specificaties van het apparaat voor specifieke werktemperatuur en relatieve luchtvochtigheid.
- Plaats het apparaat niet op een locatie die blootgesteld is aan vocht, stof, extreme hitte of koude, sterke elektronische straling of onstabiele verlichtingsomstandigheden.
- Installeer het apparaat niet op een plek vlakbij de warmtebron, zoals een radiator, verwarming, fornuis of ander warmte-genererend apparaat om brand te voorkomen.
- Voorkom dat er vloeistof in het apparaat loopt om schade aan interne componenten te vermijden.
- Installeer het apparaat horizontaal of installeer het op een stabiele plek om te voorkomen dat het valt.
- Installeer het apparaat in een goed geventileerde ruimte en blokkeer de ventilatie van het apparaat niet.
- Haal het apparaat niet willekeurig uit elkaar.
- Vermijd zware druk, hevige trilling en nat worden tijdens het transport, de opslag en de installatie. De complete verpakking is noodzakelijk tijdens het transport.
- Gebruik de fabrieksverpakking of gelijkwaardig voor het transport.

Batterij

Lage batterijstroom beïnvloedt de bediening van de RTC, waardoor deze bij iedere stroominschakeling reset. Als de batterij vervangen moet worden, verschijnt een logbericht in het serverrapport van het product. Zie voor meer informatie over het serverrapport de setuupagina's van het product of neem contact op met Dahua Support.



WAARSCHUWING

- Gevaar op ontploffing als de batterij onjuist wordt vervangen.
- Vervang alleen met een identieke batterij die wordt aanbevolen door Dahua.
- Verwerk de gebruikte batterijen volgens de plaatselijke regelgeving of de instructies van de batterijfabrikant.

Portugués

Instruções e advertências importantes

Este capítulo descreve os conteúdos relativos ao manuseamento correto do dispositivo, à prevenção de riscos e à prevenção de danos materiais. Leia estes conteúdos atentamente antes de utilizar o dispositivo, respeite as instruções durante a utilização e guarde-as em boas condições para consulta futura.

Instruções de segurança

As seguintes palavras-sinal categorizadas, com um significado definido, poderão surgir no Guia.

Palavras-sinal	Significado
 PERIGO	Indica um risco potencial elevado que, se não for evitado, resultará em morte ou ferimentos graves.
 AVISO	Indica um risco potencial médio ou baixo que, se não for evitado, poderá resultar em ferimentos ligeiros ou moderados.
 ATENÇÃO	Indica um risco potencial que, se não for evitado, pode resultar em danos materiais, perda de dados, desempenho inferior ou resultados imprevisíveis.
 SUGESTÕES	Disponibiliza métodos para o ajudar a resolver um problema ou a poupar o seu tempo.
 NOTA	Disponibiliza informações adicionais como destaque e complemento ao texto.

Requisitos em termos de segurança

- Respeite as normas locais de segurança elétrica de forma a garantir que a tensão é estável e respeita os requisitos da fonte de alimentação do dispositivo.
- Transporte, utilize e armazene o dispositivo nas condições de humidade e temperatura permitidas. Consulte as respetivas especificações técnicas do dispositivo para conhecer a temperatura e humidade de funcionamento específicas.
- Não coloque o dispositivo num local exposto a humidade, poeira, condições de calor ou frio extremas, radiação eletrónica intensa ou condições de iluminação instáveis.
- Não instale o dispositivo num local próximo de uma fonte de calor, como, por exemplo, um radiador, aquecedor, fornalha ou outro dispositivo de geração de calor de forma a evitar incêndios.
- Não permita o escoamento de líquidos para o dispositivo, evitando, assim, danos nos componentes internos.
- Instale o dispositivo numa posição horizontal ou num local estável, prevenindo possíveis quedas.
- Instale o dispositivo num local bem ventilado e não bloqueie a ventilação do dispositivo.
- Não desmonte o dispositivo de forma arbitrária.
- Evite pressões intensas, vibrações violentas e a imersão do dispositivo durante o transporte, armazenamento e instalação. Para o transporte, é necessária a embalagem completa.
- Utilize a embalagem de fábrica ou equivalente para efetuar o transporte.

Bateria

Uma bateria fraca afeta a operação do RTC, fazendo com que este reinicie sempre que é ligado. Quando a bateria tiver de ser substituída, surgirá uma mensagem de registo no relatório do servidor do produto. Para mais informações sobre o relatório do servidor, consulte as páginas de configuração do produto ou contacte a Dahua para obter assistência.



AVISO

- Risco de explosão se a bateria não for corretamente colocada.
- Substitua apenas por uma bateria idêntica ou por uma bateria recomendada pela Dahua.
- Elimine as baterias usadas de acordo com os regulamentos locais ou com as instruções do fabricante da bateria.