



Smoke Sensing Network Camera

Operation Manual







Foreword

General

This manual introduces the functions, configuration, general operation, and system maintenance of AI-Fire Smoke Sensing Network camera.

Safety Instructions

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

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

Revision History

Version	Revision Content	Release Date
V1.0.1	Modify alarm setting.	February 2022
V1.0.0	First release.	December 2021

Privacy Protection Notice

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

About the Manual

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

contact customer service for the latest program and supplementary documentation.

- There might be errors in the print or deviations in the description of the functions, operations and technical data. If there is any doubt or dispute, we reserve the right of final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and company names in the manual are properties of their respective owners.
- Please visit our website, contact the supplier or customer service if any problems occur while using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Important Safeguards and Warnings

Electrical Safety

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

Environment

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

Operation and Daily Maintenance

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

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

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

 **WARNING**

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

Table of Contents

Foreword	I
Important Safeguards and Warnings.....	III
1 Overview.....	1
1.1 Introduction	1
1.2 Network Connection.....	1
1.3 Function.....	1
1.3.1 Basic Function	1
1.3.2 Intelligent Function.....	2
2 Configuration Flow.....	4
3 Device Initialization	5
4 Basic Configuration.....	8
4.1 Login	8
4.2 Live.....	9
4.2.1 Live Interface	9
4.2.2 Encode bar.....	10
4.2.3 Live View Function Bar.....	10
4.2.4 Window Adjustment Bar.....	12
4.2.4.1 Adjustment.....	12
4.3 Playback.....	13
4.3.1 Playback Interface.....	13
4.3.2 Playing back Video or Picture.....	15
4.3.3 Clipping Video.....	18
4.3.4 Downloading Video or Picture.....	19
4.3.4.1 Downloading A Single File.....	19
4.3.4.2 Downloading Files in Batches.....	19
4.4 Camera	20
4.4.1 Conditions.....	20
4.4.1.1 Conditions	20
4.4.1.1.1 Interface Layout.....	20
4.4.1.1.2 Picture.....	21
4.4.1.1.3 Exposure.....	22
4.4.1.1.4 Backlight.....	24
4.4.1.1.5 WB.....	24
4.4.1.1.6 Day & Night.....	25
4.4.1.1.7 Illuminator.....	26

4.4.1.1.8 Defog.....	27
4.4.1.1.9 LDC.....	28
4.4.1.2 Profile Management.....	28
4.4.2 Setting Video Parameters.....	29
4.4.2.1 Video.....	30
4.4.2.2 Snapshot.....	32
4.4.2.3 Overlay.....	32
4.4.2.3.1 Configuring Privacy Masking.....	33
4.4.2.3.2 Configuring Channel Title.....	34
4.4.2.3.3 Configuring Time Title.....	35
4.4.2.3.4 Configure Text Overlay.....	35
4.4.2.3.5 Configure Font Attribute.....	36
4.4.2.3.6 Configure Picture Overlay.....	36
4.4.2.3.7 Configure Custom Overlay.....	37
4.4.2.3.8 Configure Smoke Alarm.....	38
4.4.2.4 ROI.....	38
4.4.2.5 Path.....	39
4.4.3 Audio.....	40
4.4.3.1 Configuring Audio Parameter.....	40
4.4.3.2 Configuring Alarm Audio.....	42
4.5 Network.....	43
4.5.1 TCP/IP.....	43
4.5.2 Port.....	45
4.5.3 PPPoE.....	47
4.5.4 DDNS.....	48
4.5.5 SMTP (Email).....	49
4.5.6 UPnP.....	52
4.5.7 SNMP.....	53
4.5.8 Bonjour.....	56
4.5.9 Multicast.....	56
4.5.10 802.1x.....	57
4.5.11 QoS.....	58
4.5.12 Access Platform.....	58
4.5.12.1 P2P.....	58
4.5.12.2 ONVIF.....	59
4.5.12.3 RTMP.....	60
4.6 Storage.....	61

4.6.1 Setting Storage Plan	61
4.6.2 Setting Schedule	61
4.6.3 Setting Destination.....	62
4.6.3.1 Path.....	62
4.6.3.2 Local.....	63
4.6.3.3 FTP.....	64
4.6.3.4 NAS.....	66
4.7 System.....	67
4.7.1 General.....	67
4.7.2 Date & Time.....	68
4.7.3 Account.....	69
4.7.3.1 Adding a User.....	69
4.7.3.2 Adding User Group	74
4.7.3.3 ONVIF User	75
4.7.4 Safety.....	78
4.7.4.1 System Service	78
4.7.4.2 HTTPS.....	79
4.7.4.3 Firewall.....	83
5 Event.....	86
5.1 Setting Alarm Linkage.....	86
5.1.1 Alarm Linkage	86
5.1.1.1 Setting Period.....	87
5.1.1.2 Record Linkage	87
5.1.1.2.1 Setting Record Plan.....	88
5.1.1.2.2 Setting Record Control.....	89
5.1.1.2.3 Setting Record Linkage.....	89
5.1.1.3 Snapshot Linkage.....	90
5.1.1.3.1 Setting Snapshot Plan.....	90
5.1.1.3.2 Setting Snapshot Linkage	91
5.1.1.4 Relay-out Linkage.....	91
5.1.1.5 Email Linkage.....	91
5.1.1.6 Audio Linkage.....	92
5.1.2 Subscribing Alarm.....	92
5.1.2.1 About Alarm Types.....	92
5.1.2.2 Subscribing Alarm Information.....	93
5.2 Setting Video Detection.....	93
5.2.1 Setting Motion Detection.....	94

5.2.2 Setting Video Tampering.....	96
5.2.3 Setting Scene Changing.....	97
5.3 Setting Smart Motion Detection.....	98
5.4 Setting Audio Detection.....	99
5.5 Setting Smart Plan.....	101
5.6 Setting Flame Detection.....	101
5.7 Setting Smoke Alarm.....	103
5.8 Setting Abnormality.....	104
5.8.1 Setting SD Card.....	104
5.8.2 Setting Network.....	105
5.8.3 Setting Illegal Access.....	105
5.8.4 Setting Voltage Detection.....	106
5.8.5 Setting Security Exception.....	107
5.8.6 Setting Disarming.....	108
6 Maintenance.....	109
6.1 Requirements.....	109
6.2 Auto Maintain.....	109
6.3 Resetting Password.....	110
6.4 Backup and Default.....	112
6.4.1 Import/Export.....	112
6.4.2 Default.....	113
6.5 Upgrade.....	113
6.6 Information.....	114
6.6.1 Version.....	114
6.6.2 Log.....	114
6.6.3 Remote Log.....	116
6.6.4 Online User.....	116
Appendix 1 Cybersecurity Recommendations.....	118

1 Overview

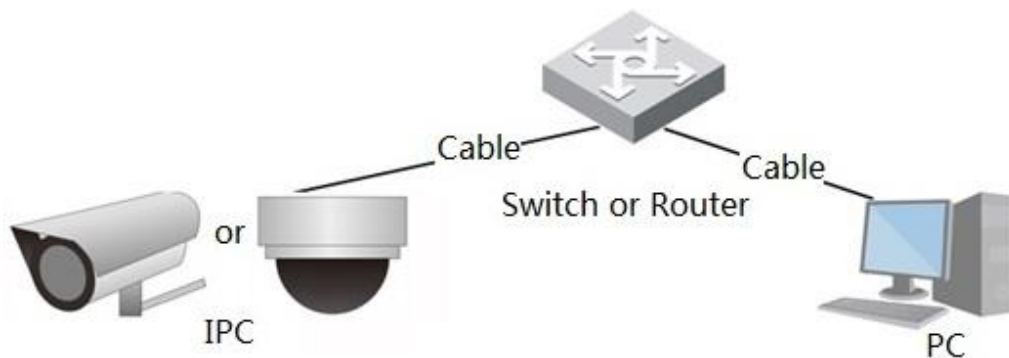
1.1 Introduction

AI-fire smoke sensing network camera (DHI-HY-SAV849HAP-E/DHI-HY-SAV849HAE-E) has the characteristics of high sensitivity and stability. Based on the mounting bracket, it can be easily installed on the ceiling. With built-in high-decibel buzzer, it will send out a visual and audible alarm signal in time to remind users to take effective measures immediately when the smoke and flame appear. The network connection and basic functions of the device are similar to other Dahua's IPCs.

1.2 Network Connection

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

Figure 1-1 General IPC network



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

1.3 Function

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

1.3.1 Basic Function

Real-time Monitoring

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

- Configure coding parameters, and adjust live view image.

Record

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

Account

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

1.3.2 Intelligent Function

Alarm

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

Video Detection

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

Smart Motion Detection

- Avoid the alarms triggered by the environment changes.
- When an alarm is triggered, the system performs linkages such as recording, alarm output, sending email, and snapshot.

Audio Detection

- Audio input abnormal detection and intensity change detection.
- When an alarm is triggered, the system performs linkages such as recording, alarm output, sending email, and snapshot.

Flame Detection

- Flame detection.
- When an alarm is triggered, the system performs linkages such as recording, alarm output, sending email, and snapshot.

Smoke Alarm Setting

- Set sensitivity of smoke alarm.
- When an alarm is triggered, the system performs linkages such as recording, alarm output, sending email, sending email, and snapshot.

Abnormality

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

2 Configuration Flow

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

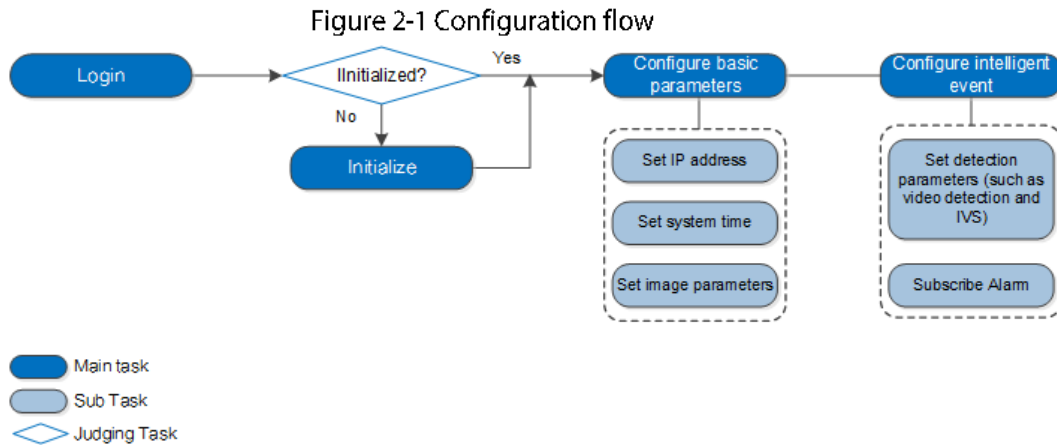


Table 2-1 Description of flow

Configuration	Description	Reference	
Login	Open IE browser and enter IP address to log in to the web interface, The camera IP address is 192.168.1.108 by default.	"4.1 Login"	
Initialization	Initialize the camera when you use it for the first time.	"3 Device Initialization"	
Basic parameters	IP address	Modify IP address according to network planning for the first use or during network adjustment.	"4.5.1 TCP/IP"
	Date & time	Set date and time to ensure the recording time is correct.	"4.7.2 Date & Time"
	Image parameters	Adjust image parameters according to the actual situation to ensure the image quality.	"4.4.1 Conditions"
Intelligent Event	Detection rules	Configure the necessary detection rules, such as video detection and IVS.	"5 Event"
	Subscribe alarm	Subscribe alarm event. When the subscribed alarm is triggered, the system will record the alarm on the alarm tab.	"5.1.2 Subscribing Alarm"

3 Device Initialization

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



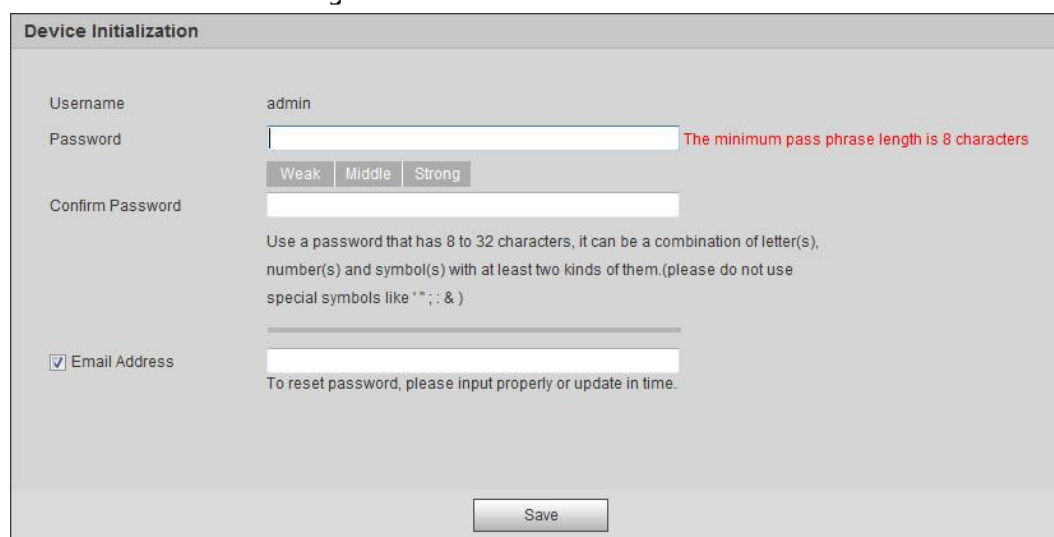
- To ensure the device safety, keep the password properly after initialization and change the password regularly.
- When initializing device, keep the PC IP and device IP in the same network.

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



The IP is 192.168.1.108 by default.

Figure 3-1 Device initialization



The screenshot shows the 'Device Initialization' web page. It contains the following elements:

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

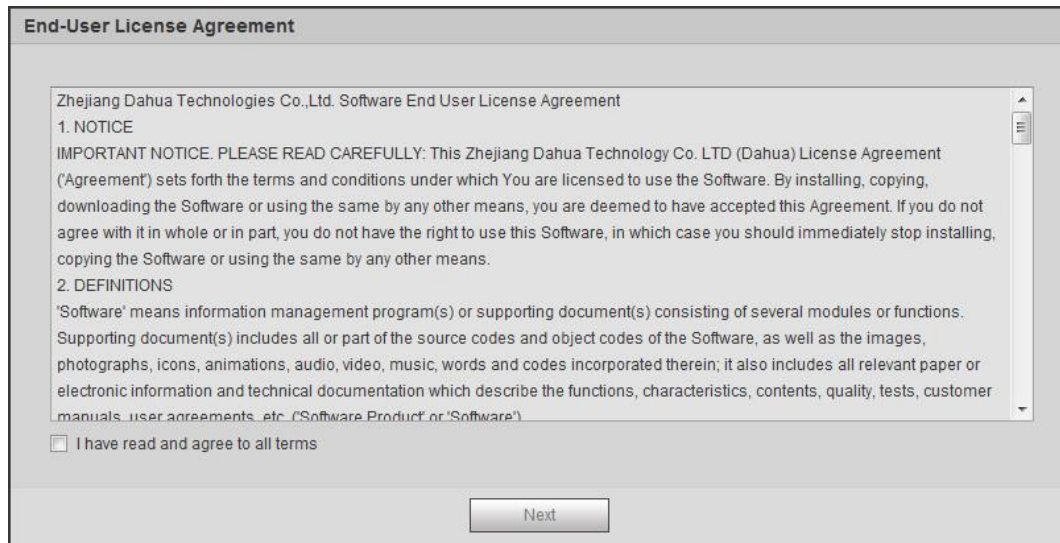
Step 2 Set the password for admin account.

Table 3-1 Description of password configuration

Parameter	Description
Username	The default username is admin.
Password	The password must consist of 8 to 32 non-blank characters and contain at least two types of characters among upper case, lower case, number, and special character (excluding ' ' ; : &). Set a high security level password according to the password security notice.
Confirm password	
email	Enter an email address for password reset, and it is selected by default. When you need to reset the password of the admin account, a security code for password resetting will be sent to the reserved email address.

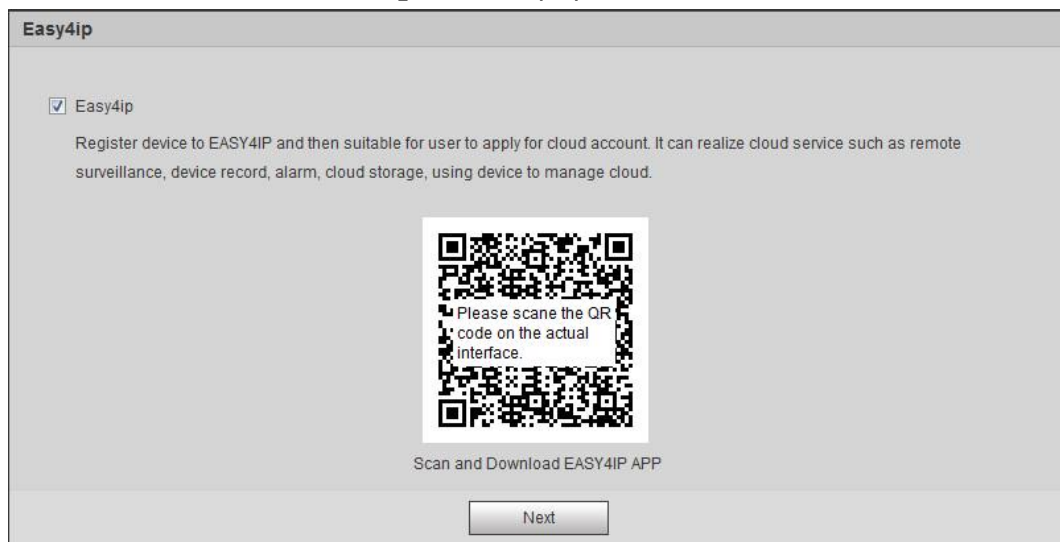
Step 3 Click **Save**.

Figure 3-2 End-user license agreement



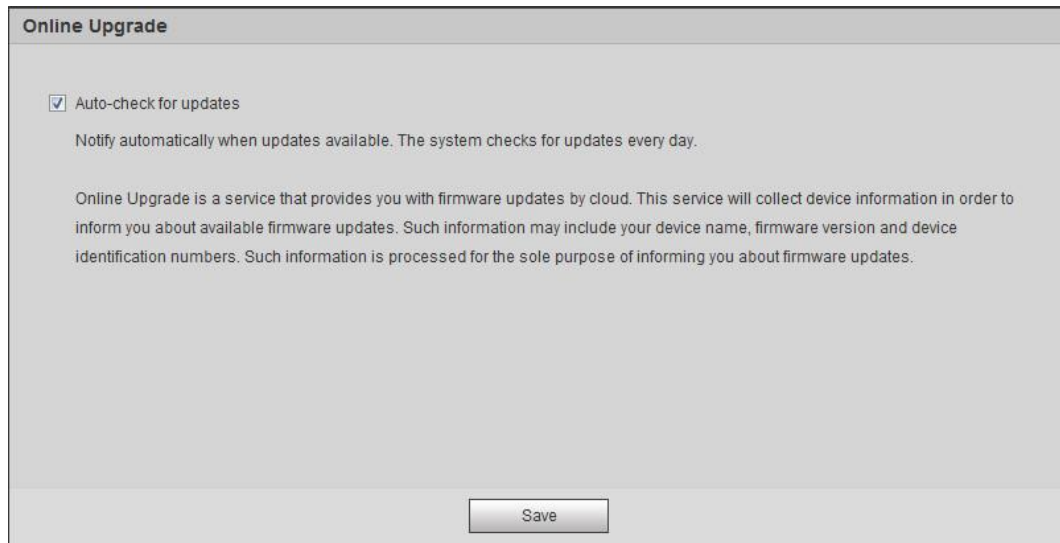
Step 4 Select the **I have read and agree to all terms** check box, and then click **Next**.

Figure 3-3 Easy4ip



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

Figure 3-4 Online upgrade



Online Upgrade

Auto-check for updates
Notify automatically when updates available. The system checks for updates every day.

Online Upgrade is a service that provides you with firmware updates by cloud. This service will collect device information in order to inform you about available firmware updates. Such information may include your device name, firmware version and device identification numbers. Such information is processed for the sole purpose of informing you about firmware updates.

Save

- Step 6** Select the upgrading method as needed.
If you select **Auto-check for updates**, the system checks new version once a day automatically. There will be system notice on **Upgrade** interface and **Version** interface if any new version is available.



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

- Step 7** Click **Save**.
Device initialization is completed.

4 Basic Configuration

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

4.1 Login

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



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

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

Figure 4-1 Login



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



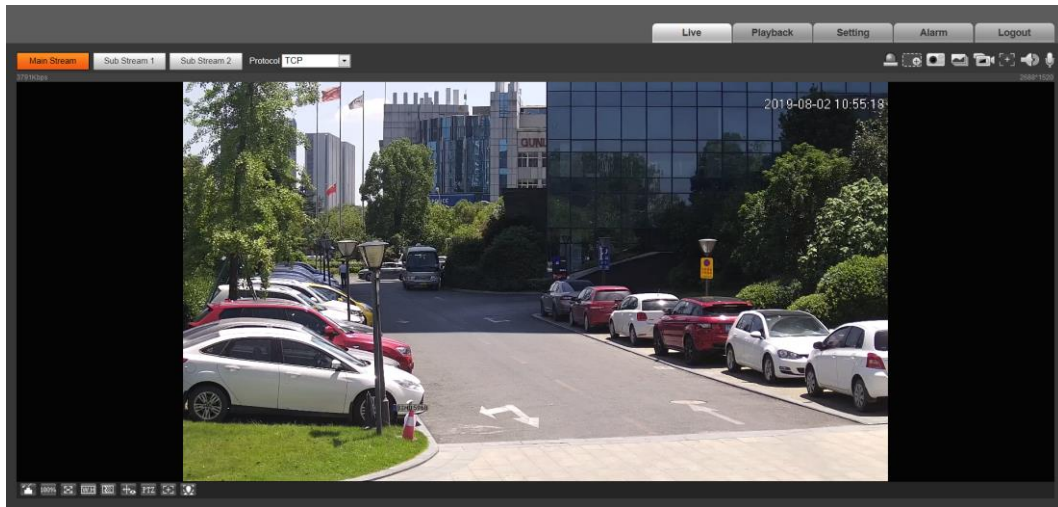
Click **Forget password?**, and you can reset the password through the email address that is set during the initialization. For details, see "6.3 Resetting Password".

Step 3 Click **Login**.

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

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

Figure 4-2 Live



4.2 Live

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

4.2.1 Live Interface

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

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



The functions and interfaces of different models might vary, and the actual product shall prevail.

Figure 4-3 Live

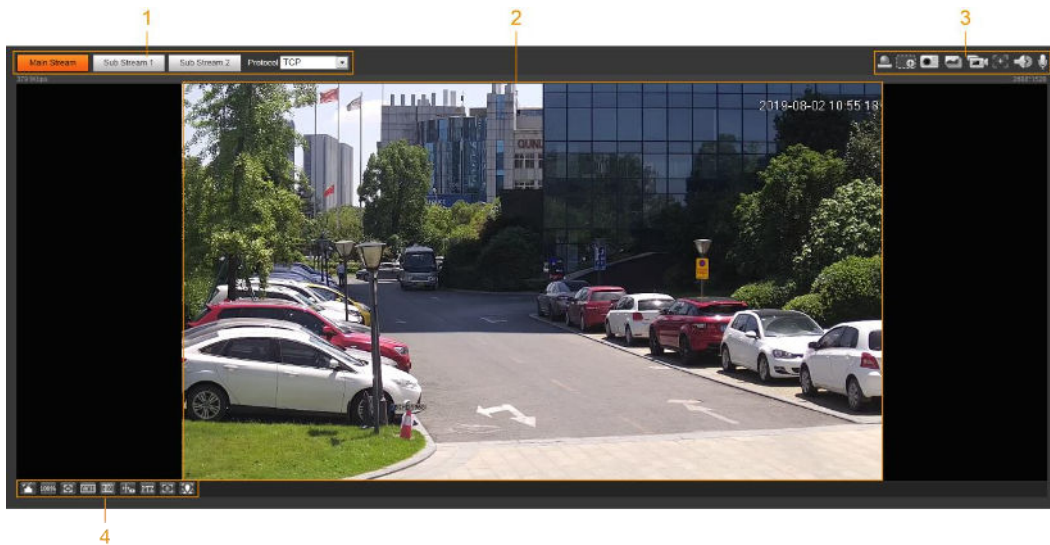


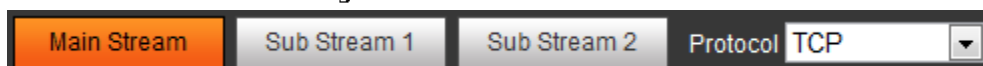
Table 4-1 Description of function bar

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

4.2.2 Encode bar

For encode bar, see Figure 4-4.

Figure 4-4 Encode bar



- **Main Stream:** It has large bit stream value and image with high resolution, but also requires large bandwidth. This option can be used for storage and monitoring. For details, see "4.4.2.1 Video".
- **Sub Stream:** It has small bit stream value and smooth image, and requires less bandwidth. This option is normally used to replace main stream when bandwidth is not enough. For details, see "4.4.2.1 Video".
- **Protocol:** You can select the network transmission protocol as needed, and the options are **TCP**, **UDP** and **Multicast**.















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

4.2.3 Live View Function Bar

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

Table 4-2 Description of live view function bar












Icon	Function	Description
	Remote Sound Elimination	Mute the sound remotely.
	Relay-out 1	Displays alarm output state. Click the icon to force to enable or disable alarm output. Alarm output state description: <ul style="list-style-type: none"> • Red: Alarm output enabled. • Grey: Alarm output disabled.
	Relay-out 2	
	Alarm	Displays alarm sound state. Click the icon to enable or disable the alarm sound forcibly.
	Digital Zoom	You can zoom in or out video image through two operations. <ul style="list-style-type: none"> • Click the icon, and then select an area in the video image to zoom in; right-click on the image to resume the original size. In zoom in state, drag the image to check other area. • Click the icon, and then scroll the mouse wheel in the video image to zoom in or out.
	Snapshot	Click the icon to capture one picture of the current image, and it will be saved to the configured storage path.  About viewing or configuring storage path, see "4.4.2.5 Path".
	Triple Snapshot	Click the icon to capture three pictures of the current image, and they will be saved to the configured storage path.  About viewing or configuring storage path, see "4.4.2.5 Path".
	Record	Click the icon to record video, and it will be saved to the configured storage path.  About viewing or configuring storage path, see "4.4.2.5 Path".
	Audio	Click the icon to enable or disable audio output.
	Talk	Click the icon to enable or disable the audio take.



4.2.4 Window Adjustment Bar

4.2.4.1 Adjustment

This section introduces the adjustment of image.

Table 4-3 Description of adjustment bar

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

Icon	Function	Description
	Fluency	<p>Click the icon to select the fluency from Realtime, Fluency and Normal.</p> <ul style="list-style-type: none"> • Realtime: Guarantees the real time of the image. When the bandwidth is not enough, the image might not be smooth. • Fluency: Guarantees the fluency of the image. There might be delay between live view image and real-time image. • Normal: It is between Realtime and Fluency.
	Rule Info	<p>Click the icon, and then select Enable to display smart rules and detection box; select Disable to stop the display. It is enabled by default.</p>

4.3 Playback

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



- Before playing back video, configure record time range, record storage method, record schedule and record control. For details, see "5.1.1.2.1 Setting Record Plan".
- Before playing back picture, configure snapshot time range, snapshot storage method, snapshot plan. For details, see "5.1.1.3.1 Setting Snapshot Plan".
- When using Dahua smart card, make sure that the card has been authenticated before using.

4.3.1 Playback Interface

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

Figure 4-5 Video playback

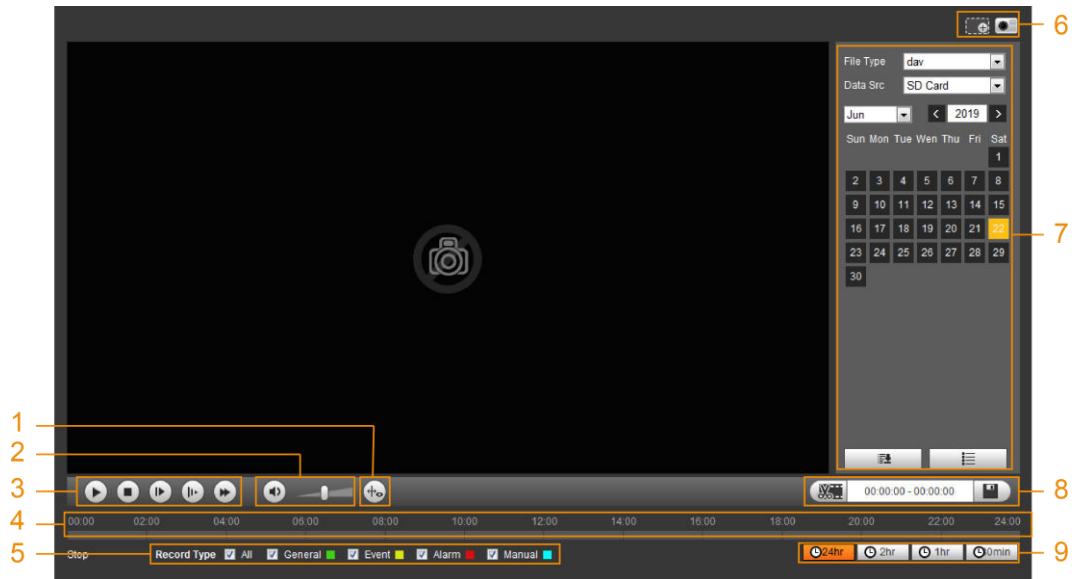


Figure 4-6 Picture playback

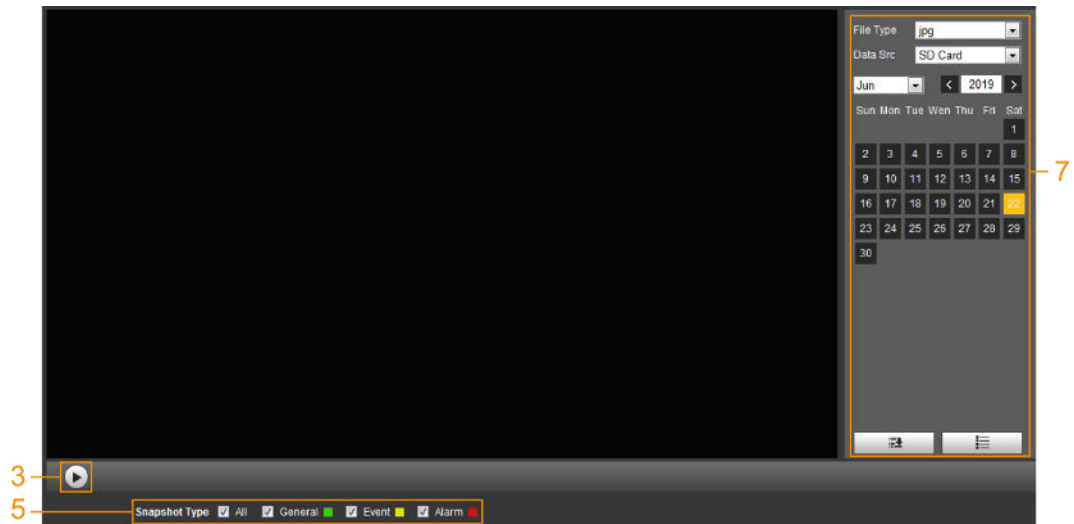






Table 4-4 Playback interface description

No.	Function	Description
1	Rules Info	<p>Click , intelligent rules and object detection box are displayed. It is enabled by default.</p> <p></p> <p>Rules Info is valid only when you enabled the rule during recording.</p>
2	Sound	<p>Controls the sound during playback.</p> <ul style="list-style-type: none"> : Mute mode. : Vocal state. You can adjust the sound.

No.	Function	Description
3	Play control bar	<p>Controls playback.</p> <ul style="list-style-type: none"> : Click the icon to play back recorded videos. : Click the icon to stop playing back recorded videos. : Click the icon to play the next frame. : Click the icon to slow down the playback. : Click the icon to speed up the playback.
4	Progress bar	<p>Displays the record type and the corresponding period.</p> <ul style="list-style-type: none"> Click any point in the colored area, and the system will play back the recorded video from the selected moment. Each record type has its own color, and you can see their relations in Record Type bar.
5	Record/Snapshot Type	<p>Select the record type or snapshot type.</p> <ul style="list-style-type: none"> Record type includes General, Event, Alarm, Manual. Snapshot type includes General, Event, Alarm.
6	Assistant	<ul style="list-style-type: none"> : You can zoom in or out video image of the selected area through two operations. : Click the icon to capture one picture of the current video, and it will be saved to the configured storage path.
7	Playback video	You can select the file type, data source, and record date.
8	Video clip	Clip a certain recorded video and save it. For details, see "4.3.3 Clipping Video".
9	Time format of progress bar	<p>Includes 4 time formats: , , , . Take as an example, the whole progress stands for 24 hours.</p>

4.3.2 Playing back Video or Picture

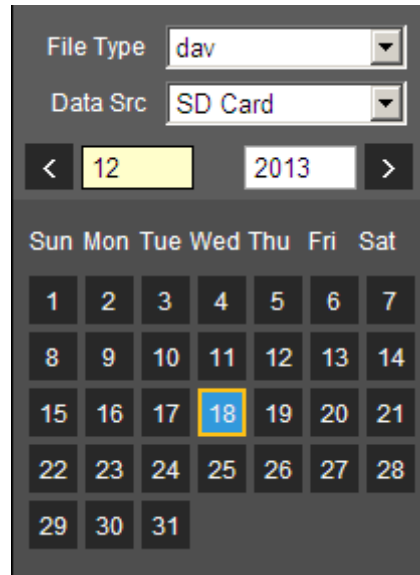
This section introduces the operation of video playback and picture playback. This section takes

video playback as an example.

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

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

Figure 4-7 File type selection



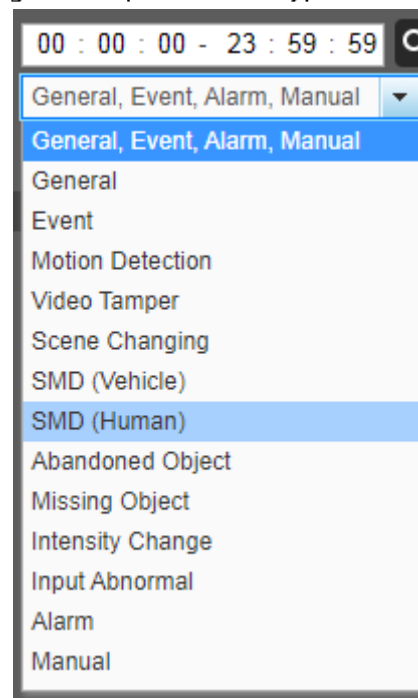
Step 2 Select the record type in **Record Type**.

Figure 4-8 Record type selection



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

Figure 4-9 Specific event types



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



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

Step 4 Play video.


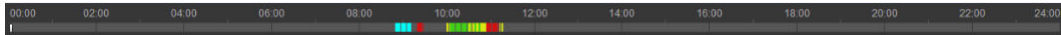
- Click  in the control bar.
The system plays the recorded video of the selected date (in the order of time).
- The system plays the recorded video of the selected date (in the order of time).
- Click any point in the colored area on the progress bar.
The playback starts from that moment.

Figure 4-10 Progress bar





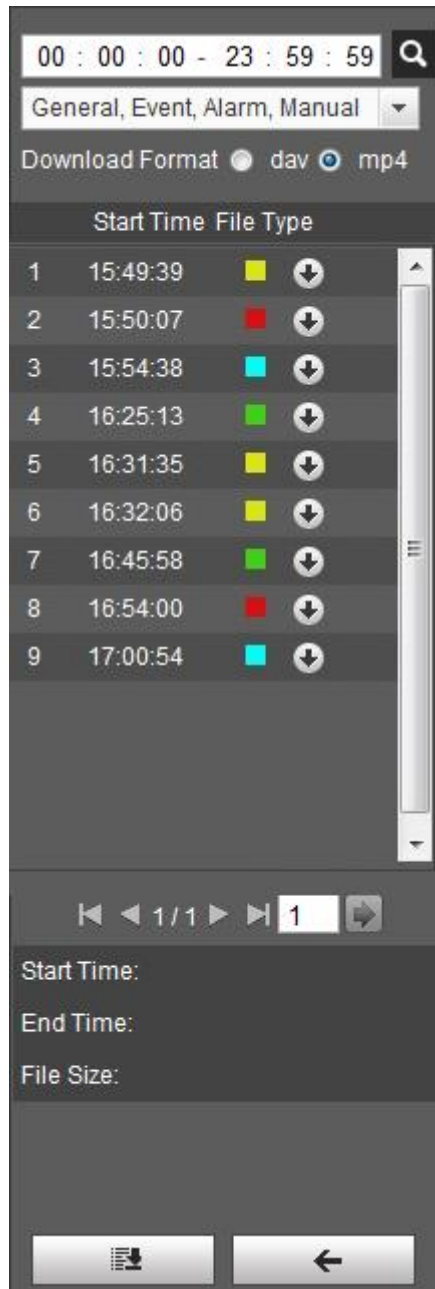
- Click , the video files of the selected date would be listed. Enter the start time and end time, and then click  to search all files between the start time and end time. Double-click the file in the list, and the system plays the video and displays file size, starting time, and ending time.

Figure 4-11 Playback file list



4.3.3 Clipping Video



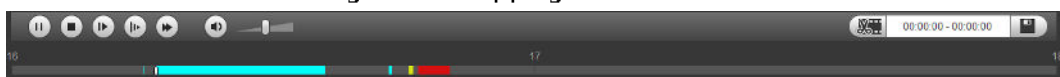


- Step 1** Click , the video files of the selected date are listed.
- Step 2** Select **dav** or **mp4** in **Download Format**.
- Step 3** Click on the progress bar to select the start time of the target video, and then click . See Figure 4-12.

Figure 4-12 Clipping video



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

- Step 5** Click  to download the video.
The system will prompt that it cannot play back and download at the same time.
- Step 6** Click **OK**.
The playback stops and the clipped file is saved in the configured storage path. For the configuration of storage path, see "4.4.2.5 Path".



4.3.4 Downloading Video or Picture

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



- Playback and downloading at the same time is not supported.
- Operations might vary with different browsers, and the actual product shall prevail.
- For details of viewing or setting storage path, see "4.4.2.5 Path".

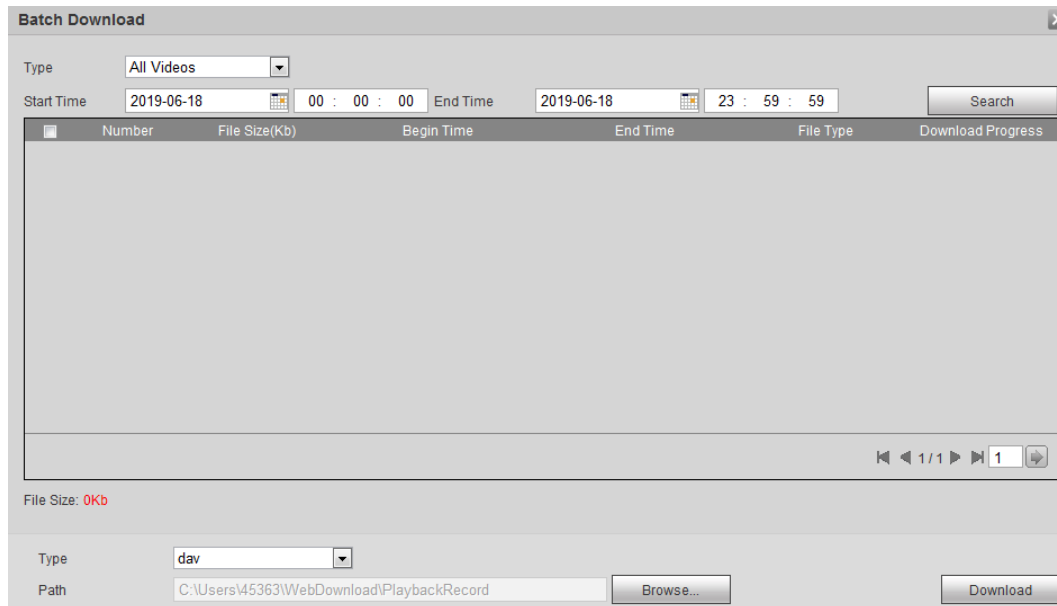
4.3.4.1 Downloading A Single File

- Step 1** Select **dav** from the **Record Type** drop-down list and **SD card** from the **Data Src** drop-down list.
Select **jpg** from **Record Type** drop-down list when playing back pictures, and you do not need to select data source.
- Step 2** Click , the video files of the selected date are listed. See Figure 4-11.
- Step 3** Select **dav** or **mp4** in **Download Format**. Click  next to the file to be downloaded.
The system starts to download the file to the configured path. When downloading pictures, you do not need to select the download format.

4.3.4.2 Downloading Files in Batches

- Step 1** Click  on the playback interface.

Figure 4-13 Batch download



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

4.4 Camera

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



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

4.4.1 Conditions

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

4.4.1.1 Conditions

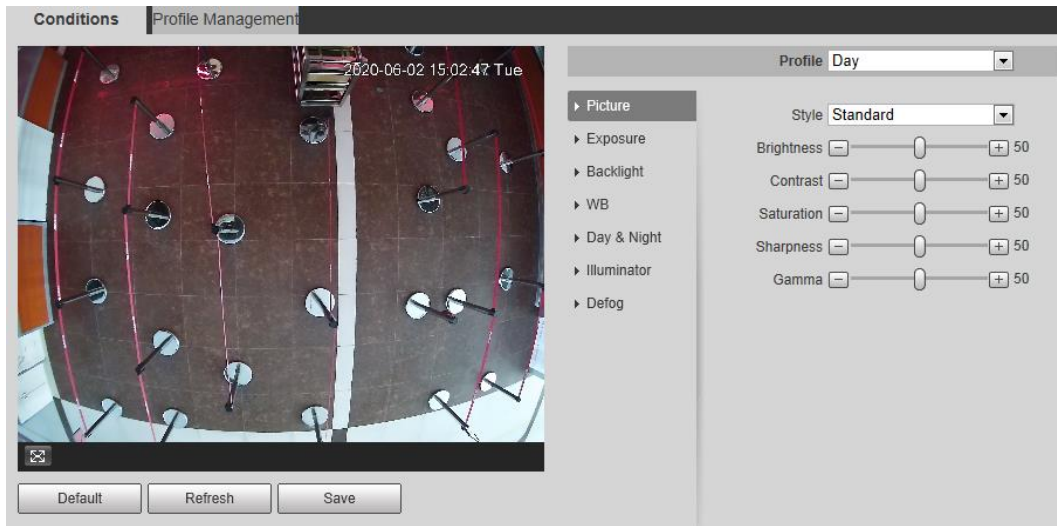
Configure camera parameters according to the actual situation, including picture, exposure, backlight and white balance.

4.4.1.1.1 Interface Layout

Configure camera parameters to improve the scene clarity, and ensure that surveillance goes properly. See Figure 4-14.

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

Figure 4-14 Camera conditions

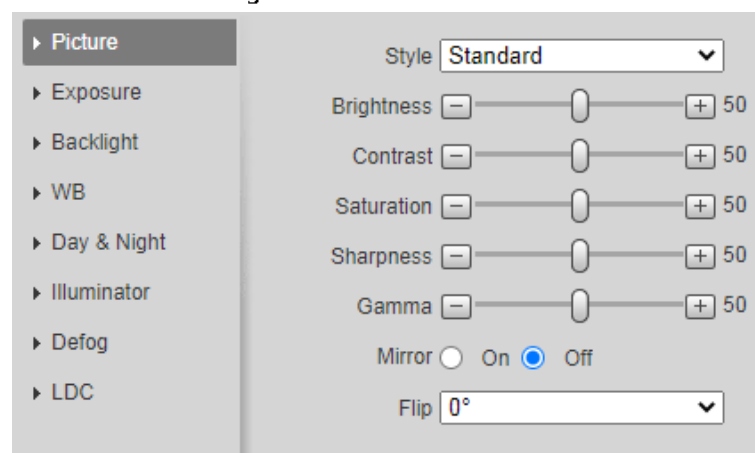


4.4.1.1.2 Picture

You can configure picture parameters as needed.

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


Figure 4-15 Picture



Step 2 Configure picture parameters.

Table 4-5 Description of picture parameters

Parameter	Description
Style	Select the picture style from soft, standard and vivid. <ul style="list-style-type: none"> • Soft: Default image style, displays the actual color of the image. • Standard: The hue of the image is weaker than the actual one, and contrast is smaller. • Vivid: The image is more vivid than the actual one.
Brightness	Changes the value to adjust the picture brightness. The higher the value is, the brighter the picture will be, and the smaller the darker. The picture might be hazy if the value is configured too big.

Parameter	Description
Contrast	Changes the contrast of the picture. The higher the value is, the more the contrast will be between bright and dark areas, and the smaller the less. If the value is set too big, the dark area would be too dark and bright area easier to get overexposed. The picture might be hazy if the value is set too small.
Saturation	Makes the color deeper or lighter. The higher the value is, the deeper the color will be, and the lower the lighter. Saturation value does not change image brightness.
Sharpness	Changes the sharpness of picture edges. The higher the value is, the clearer the picture edges will be, and if the value is set too big, picture noises are more likely to appear.
Gamma	Changes the picture brightness and improves the picture dynamic range in a non-linear way. The higher the value is, the brighter the picture will be, and the smaller the darker.
Mirror	Select On , and the picture would display with left and right side reversed.
Flip	Changes the display direction of the picture, see the options below. <ul style="list-style-type: none"> • 0°: Normal display. • 90°: The picture rotates 90° clockwise. • 180°: The picture rotates 90° counterclockwise. • 270°: The picture flips upside down.  <p>For some models, please set the resolution to be 1080p or lower when using 90° and 180°. For details, see "4.4.2.1 Video".</p>

Step 3 Click **Save**.

4.4.1.1.3 Exposure

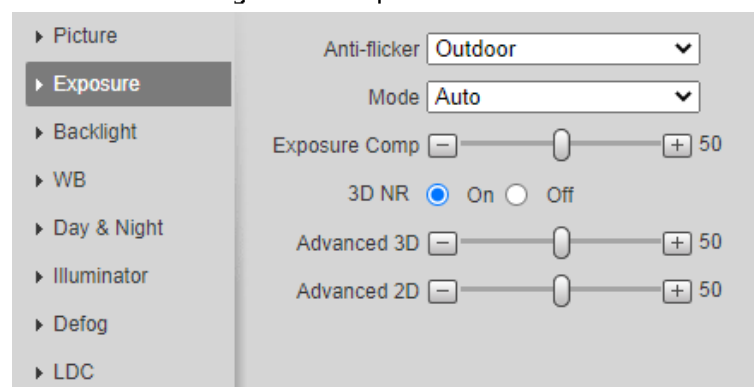
Configure iris and shutter to improve image clarity.



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


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

Figure 4-16 Exposure



Step 2 Configure exposure parameters.

Table 4-6 Description of exposure parameters

Parameter	Description
Anti-flicker	<p>You can select from 50 Hz, 60 Hz and Outdoor.</p> <ul style="list-style-type: none"> • 50 Hz: When the electric supply is 50 Hz, the system adjusts the exposure according to ambient light automatically to ensure that there is no stripe appears. • 60 Hz: When the electric supply is 60 Hz, the system adjusts the exposure according to ambient light automatically to ensure that there is no stripe appears. • Outdoor: You can select any exposure mode as needed.
Mode	<p>Device exposure modes.</p> <ul style="list-style-type: none"> • Auto: Adjusts the image brightness according to the actual condition automatically. • Gain Priority: When the exposure range is normal, the system prefers the configured gain range when auto adjusting according to the ambient lighting condition. If the image brightness is not enough and the gain has reached upper or lower limit, the system adjusts shutter value automatically to ensure the image at ideal brightness. You can configure gain range to adjust gain level when using gain priority mode. • Shutter priority: When the exposure range is normal, the system prefers the configured shutter range when auto adjusting according to the ambient lighting condition. If the image brightness is not enough and the shutter value has reached upper or lower limit, the system adjusts gain value automatically to ensure the image at ideal brightness. • Iris priority: The iris value is set to a fixed value, and the device adjusts shutter value then. If the image brightness is not enough and the shutter value has reached upper or lower limit, the system adjusts gain value automatically to ensure the image at ideal brightness. • Manual: Configure gain and shutter value manually to adjust image brightness. <p> When the Anti-flicker is set to Outdoor, you can select Gain priority or Shutter priority in the Mode list.</p>
Exposure Comp	Sets the value, and it ranges from 0 to 50. The higher the value is, the brighter the image will be.
3D NR	Works with multi-frame (no less than 2 frames) images and reduces noise by using the frame information between previous and latter frames.
Advanced 3D	This configuration is available only when the 3D DNR is enabled.
Advanced 2D	The higher the DNR level is, the better the result will be.

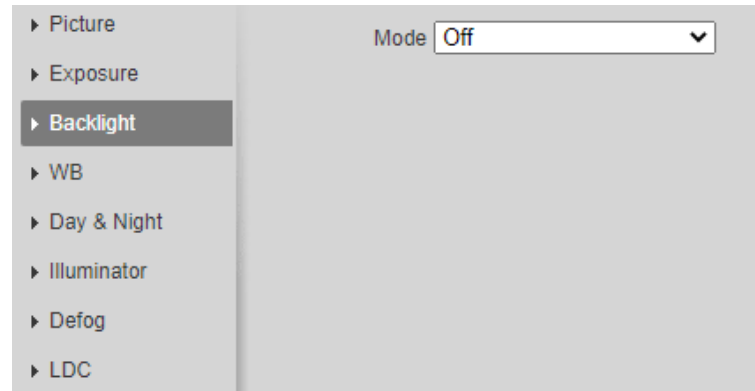
Step 3 Click **Save**.

4.4.1.1.4 Backlight

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


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

Figure 4-17 Backlight



Step 2 Configure backlight parameters.

Table 4-7 Description of backlight parameters

Backlight mode	Description
BLC	<p>Enable BLC, the camera can get clearer image of the dark areas on the target when shooting against light. You can select Default mode or Customized mode.</p> <ul style="list-style-type: none"> When in Default mode, the system adjusts exposure according to ambient lighting condition automatically to ensure the clarity of the darkest area. When in Customized mode, the system auto adjusts exposure only to the set area according to ambient lighting condition to ensure the image of the set area at ideal brightness.
HLC	<p>Enable HLC when extreme strong light is in the environment (such as toll station or parking lot), the camera will dim strong light, and reduce the size of Halo zone to lower the brightness of the whole image, so that the camera can capture human face or car plate detail clearly. The higher the value is, the more obvious the HLC effect will be.</p>
SSA	<p>Enable SSA, the system automatically adjusts the image brightness according to the environment to make the objects in the image clearer.</p>
WDR	<p>The system dims bright areas and compensates dark areas to ensure the clarity of all the area. The higher the value is, the brighter the dark will be, but the more the noise will be.</p> <p> There might be a few seconds of video loss when the device is switching to WDR mode from other mode.</p>

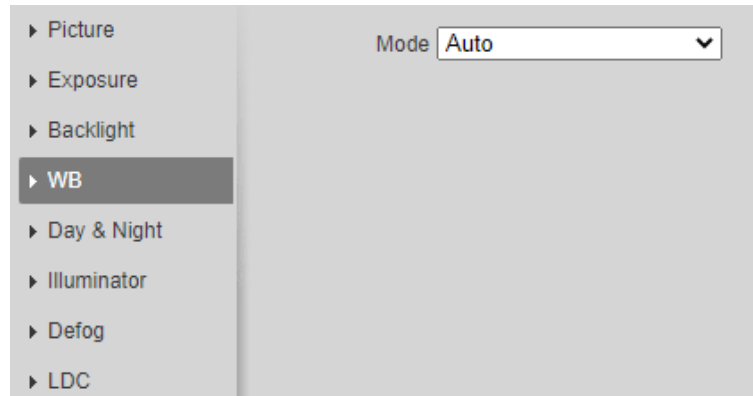
Step 3 Click **Save**.

4.4.1.1.5 WB

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

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

Figure 4-18 WB



Step 2 Configure WB parameters.

Table 4-8 Description of WB parameters

WB mode	Description
Auto	The system compensates WB according to color temperature to ensure color precision.
Natural	The system auto compensates WB to environments without artificial light to ensure color precision.
Street Lamp	The system compensates WB to outdoor night scene to ensure color precision.
Outdoor	The system auto compensates WB to most outdoor environments with natural or artificial light to ensure color precision.
Manual	Configure red and blue gain manually; the system auto compensates WB according to color temperature.
Regional Custom	The system compensates WB only to the set area according to color temperature to ensure color precision.

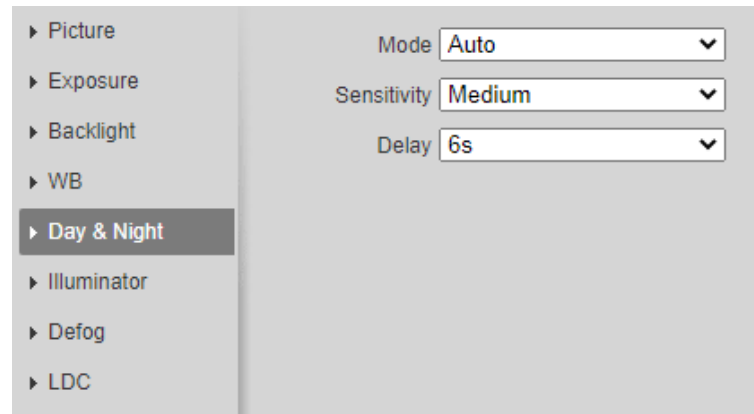
Step 3 Click **Save**.

4.4.1.1.6 Day & Night

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


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

Figure 4-19 Day and night



Step 2 Configure day and night parameters.

Table 4-9 Description of day and night parameters

Parameter	Description
Mode	<p>You can select device display mode from Color, Auto, and B/W.</p>  <p>Day & Night configuration is independent from profile management configuration.</p> <ul style="list-style-type: none"> • Color: The system displays color image. • Auto: The system switches between color and black-and-white display according to the actual condition. • B/W: The system displays black-and-white image.
Sensitivity	<p>This configuration is available only when you set Auto in Mode.</p> <p>You can configure camera sensitivity when switching between color and black-and-white mode.</p>
Delay	<p>This configuration is available only when you set Auto in Mode.</p> <p>You can configure the delay when camera switching between color and black-and-white mode. The lower the value is, the faster the camera switches between color and black-and-white mode.</p>

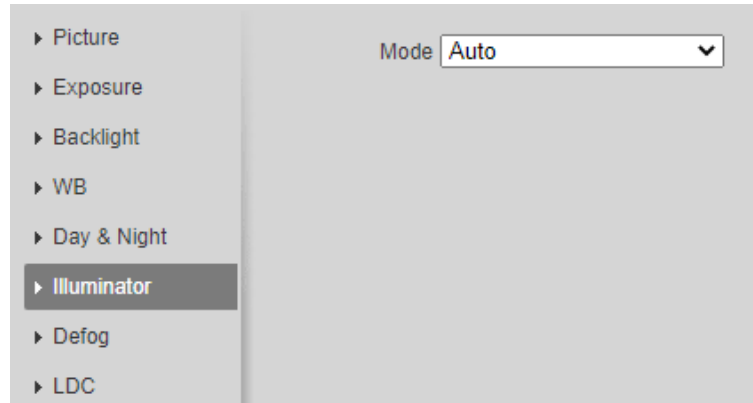
Step 3 Click **Save**.

4.4.1.1.7 Illuminator

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

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

Figure 4-20 Illuminator



Step 2 Configure illuminator parameters.

Table 4-10 Description of illuminator parameters

Illuminator		Description
Mode	Manual	Adjust the brightness of illuminator manually, and then the system will supply illuminator to the image accordingly.
	Auto	The system adjusts the illuminator intensity according to the ambient lighting condition.
	Off	Illuminator is off.

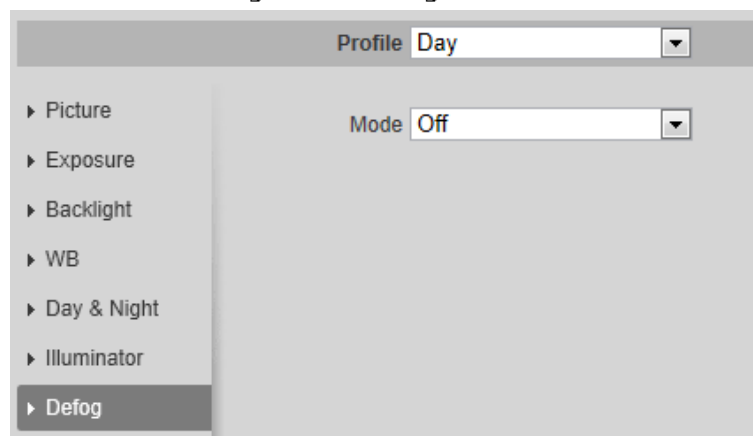
Step 3 Click **Save**.

4.4.1.1.8 Defog

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

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

Figure 4-21 Defog



Step 2 Configure defog parameters.

Table 4-11 Description of defog parameters

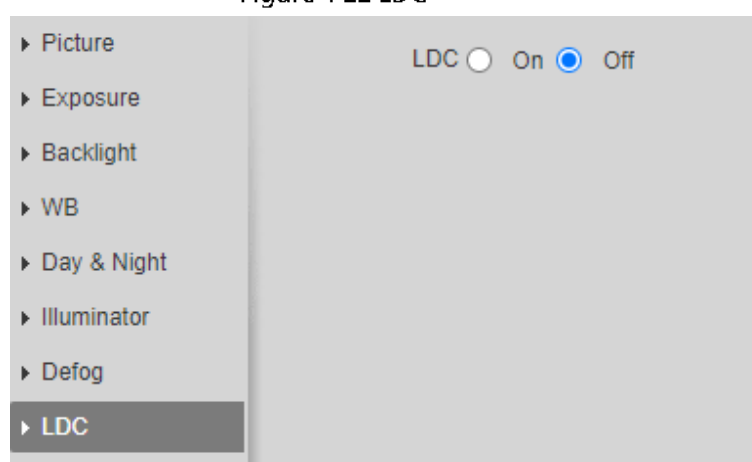
Defog	Description
Manual	Configure function intensity and atmospheric light mode manually, and then the system adjusts image clarity accordingly. Atmospheric light mode can be adjusted automatically or manually.
Auto	The system adjusts image clarity according to the actual condition.
Off	Defog function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

Step 3 Click **Save**.

4.4.1.1.9 LDC

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

Figure 4-22 LDC



Step 2 Enable the LDC function.

4.4.1.2 Profile Management

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

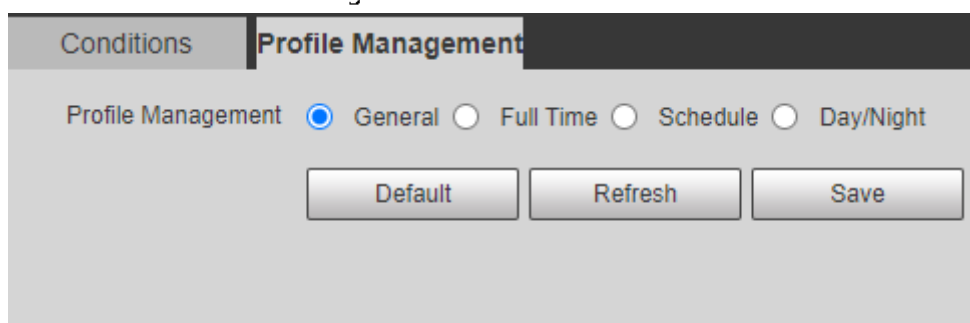
Step 1 Select **Setting > Camera > Conditions > Profile Management**.

The **Profile Management** interface is displayed.

Step 2 Manage profile.

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

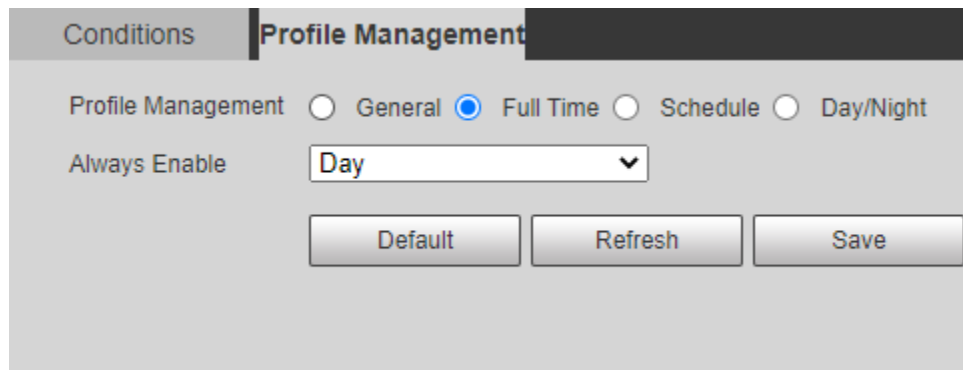
Figure 4-23 General



- When **Profile Management** is set as **Full Time**, you can select **Day** or **Night** in the

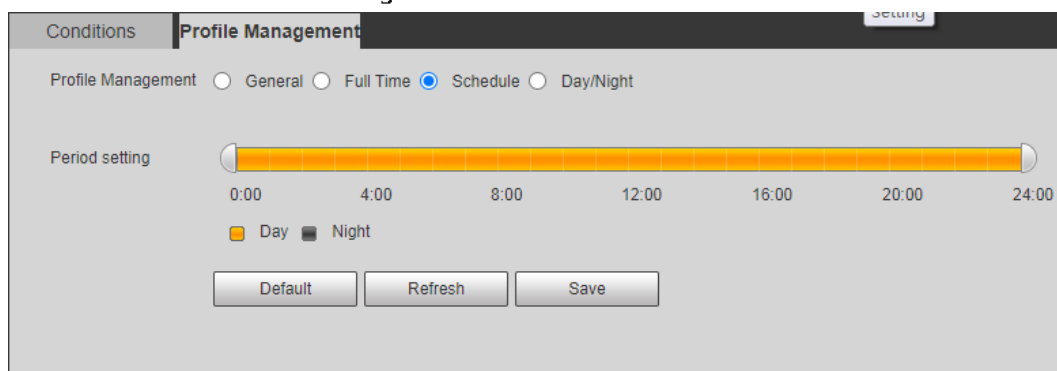
Always Enable list, the surveillance system works under **Always Enable** configuration.

Figure 4-24 Full time



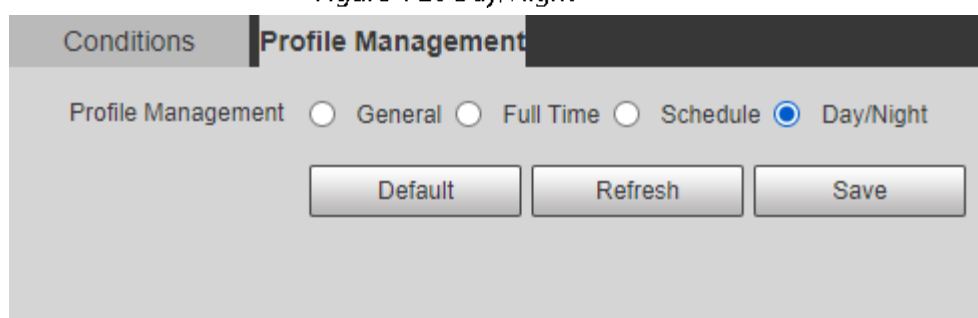
- When **Profile Management** is set as **Schedule**, you can drag the slide block to set certain time as **Day** or **Night**. For example, set 8:00–18:00 as day, and 0:00–8:00 and 18:00–24:00 as night.

Figure 4-25 Schedule



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

Figure 4-26 Day/Night



Step 3 Click **Save**.

4.4.2 Setting Video Parameters

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



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

4.4.2.1 Video

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

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



Figure 4-27 Video

The screenshot shows the 'Video' configuration page with two tabs: 'Main Stream' and 'Sub Stream'. The 'Main Stream' section includes settings for Encode Mode (H.265), Encoding Strategy (General), Resolution (1920*1080(1080P)), Frame Rate(FPS) (30), Bit Rate Type (CBR), Reference Bit Rate (768-6400Kb/S), Bit Rate (1792 (Kb/S)), I Frame Interval (60 (30-150)), and Watermark Settings (checked, DigitalCCTV). The 'Sub Stream' section includes settings for Enable (checked), Sub Stream 1 (dropdown), Encode Mode (H.265), Resolution (704*480(D1)), Frame Rate(FPS) (30), Bit Rate Type (CBR), Reference Bit Rate (211-1280Kb/S), Bit Rate (256 (Kb/S)), and I Frame Interval (60 (30-150)). At the bottom, there are buttons for 'Default', 'Refresh', and 'Save'.

Step 2 Configure video parameters.

Table 4-12 Description of video parameters

Parameter	Description
Enable	Select the Enable check box to enable sub stream, it is enabled by default. You can enable multiple sub streams simultaneously.
Encode Mode	Select encode mode. <ul style="list-style-type: none"> • H.264: Main profile encode mode. Compared with H.264B, it requires smaller bandwidth. • H.264H: High profile encode mode. Compared with H.264, it requires smaller bandwidth. • H.264B: Baseline profile encode mode. It requires smaller bandwidth. • H.265: Main profile encode mode. Compared with H.264, it requires smaller bandwidth.

Parameter	Description
Encoding Strategy	<p>Select the encoding strategy as needed.</p> <ul style="list-style-type: none"> • General: Disable smart codec. • Smart Codec: Enable smart codec to improve video compressibility and save storage space. It is applicable to static scenes. • AI Code: When the bandwidth and storage space are restricted, the camera will select the encoding strategy with lower bit rate to save storage space. It is applicable to dynamic scenes. <p>After AI codec is enabled, Bit Rate Type is CBR, and it cannot be changed. Comparing with general mode, AI codec has lower bite rate. This function is only available on cameras with AI functions.</p> <p> After smart codec and AI codec are enabled, the camera would stop supporting the third stream, ROI, and smart event detection, and the actual interface shall prevail.</p>
Resolution	The resolution of the video. The higher the value is, the clearer the image will be, but the bigger the bandwidth will be required.
Frame Rate (FPS)	The number of frame in one second of video. The higher the value is, the clearer and smoother the video will be.
Bit Rate Type	<p>The bit rate control type during video data transmission. You can select bit rate type from:</p> <ul style="list-style-type: none"> • CBR (Constant Bit Rate): The bit rate changes a little and keeps close to the defined bit rate value. • VBR (Variable Bit Rate): The bit rate changes as monitoring scene changes. <p> The Bit Rate Type can be only be set as CBR when Encode Mode is set as MJPEG.</p>
Reference Bit Rate	The most suitable bit rate value range recommended to user according to the defined resolution and frame rate.
Bit Rate	<p>This parameter can be configured only when the Bit Rate Type is set as CBR.</p> <p>Select bit rate value in the list according to actual condition. You can also customize the value.</p>
I Frame Interval	<p>This parameter can be configured only when Encoding Strategy is set as General or AI Codec.</p> <p>The number of P frames between two I frames. The smaller the value, the higher the image quality, and the range changes as Frame Rate(FPS) changes. It is recommended to set I Frame Interval twice as big as Frame Rate(FPS).</p> <p>When selecting AI Codec in Encoding Strategy, you can only select the value same as or twice as big as Frame Rate(FPS).</p>
Watermark Settings	You can verify the watermark to check if the video has been tampered.

Parameter	Description
Watermark Character	1. Select the check box to enable watermark function. 2. The default character is DigitalCCTV.

Step 3 Click **Save**.

4.4.2.2 Snapshot

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

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

Figure 4-28 Snapshot

Step 2 Configure snapshot parameters.

Table 4-13 Description of snapshot parameter

Parameter	Description
Snapshot Type	You can select General and Event . <ul style="list-style-type: none"> • General: The system takes snapshot as scheduled. For details, see "4.6.2 Setting Schedule". • Event: The system takes snapshot when the video detection, audio detection, event, or alarm is triggered. This function requires the corresponding snapshot being enabled.
Image Size	The same resolution with main stream.
Quality	Configures the snapshot quality. There are six levels of Image quality, and the sixth is the best.
Interval	Configures the snapshot frequency. Select Customized , and then you can configure snapshot frequency manually.

Step 3 Click **Save**.

4.4.2.3 Overlay

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

4.4.2.3.1 Configuring Privacy Masking

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

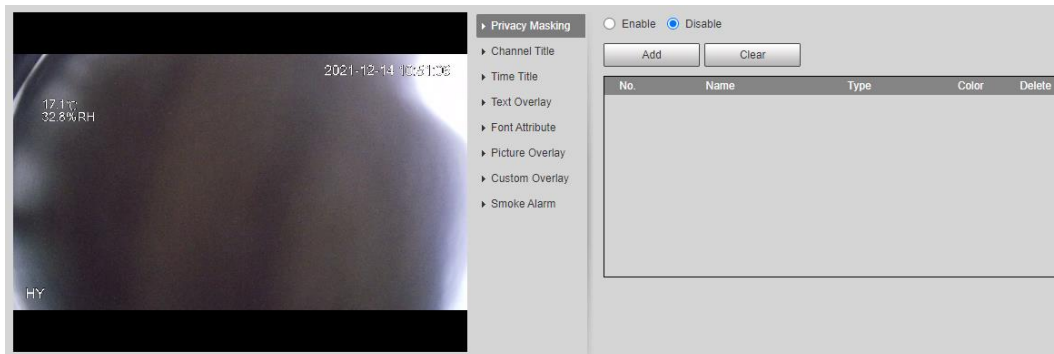


Functions might vary with different models, and the actual interface shall be prevail.

Privacy Masking (1)

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

Figure 4-29 Privacy masking (1)



Step 2 Configure privacy masking.

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



- You can drag 4 rectangles at most.
 - Click **Remove All** to delete all the area boxes; select one box, and then click **Delete** or right-click to delete it.
2. Adjust the size of the rectangle to protect the privacy.
 3. Click **Save**.

Privacy Masking (2)

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

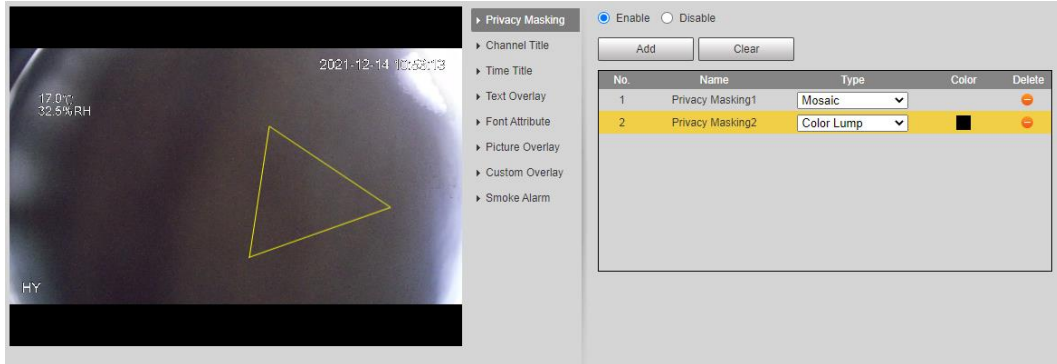
- When selecting **Color Lump** only, you can draw triangles and convex quadrilaterals as blocks. You can drag 8 blocks at most, and the color is black.
- When selecting **Mosaic**, you can draw rectangles as blocks with mosaic. You can draw 4 blocks at most.
- **Color Lump + Mosaic** (≤ 4): You can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

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

Step 2 Select **Enable**.

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

Figure 4-30 Privacy masking (2)



Related Operations

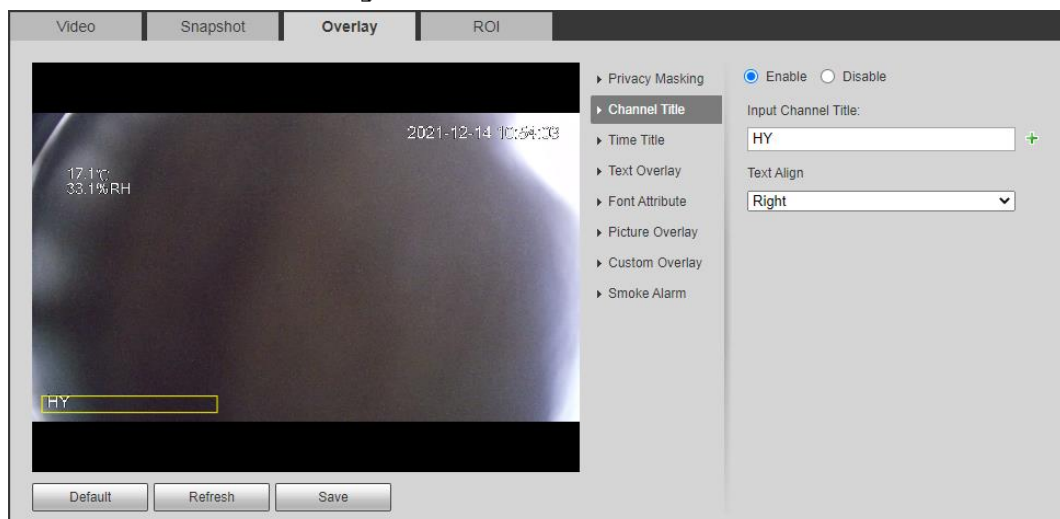
- View and edit the block
 - Select the privacy masking rule to be edited in the list, then the rule is highlighted, and the block frame is displayed in the image. You can edit the selected block as needed, including moving the position, and adjusting the size.
- Edit the block name
 - Double-click the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

4.4.2.3.2 Configuring Channel Title

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

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

Figure 4-31 Channel title



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



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

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

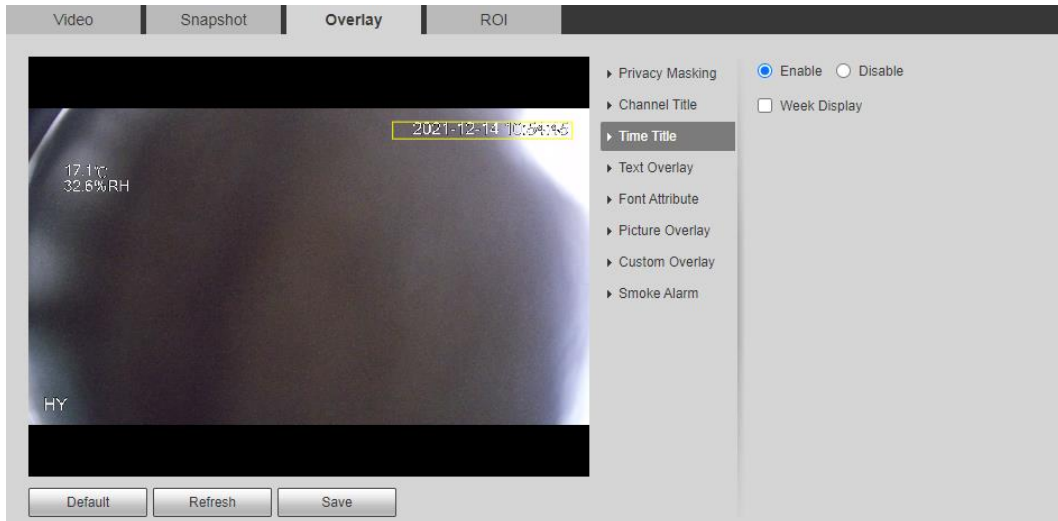
Step 4 Click **Save**.

4.4.2.3.3 Configuring Time Title

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

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

Figure 4-32 Time title



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

Step 3 Select the **Week Display** check box.

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

Step 5 Click **Save**.

4.4.2.3.4 Configure Text Overlay

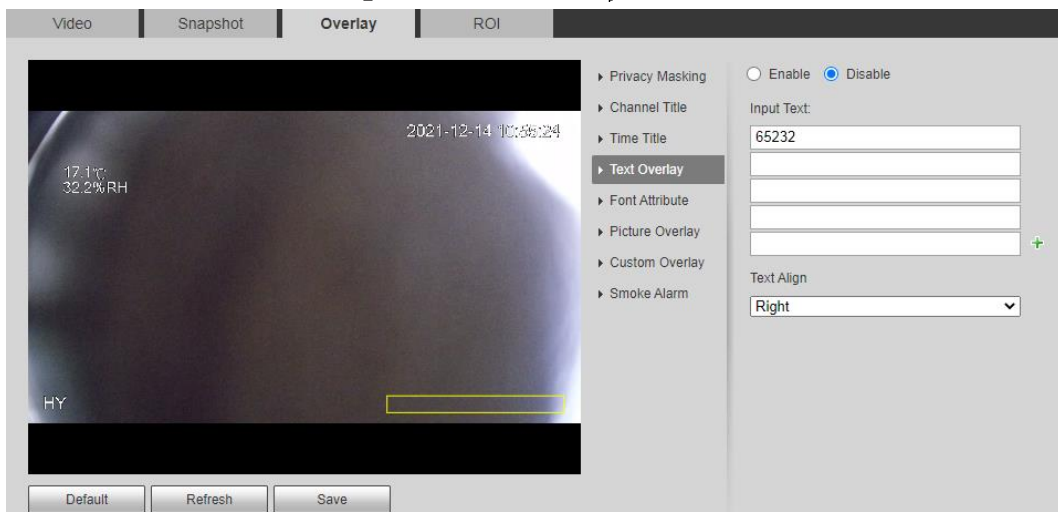
You can enable this function if you need to display text in the video image.



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

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

Figure 4-33 Text overlay



Step 2 Select the **Enable** check box, enter the text you need, and then select alignment. The text

is displayed in the video image.



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

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

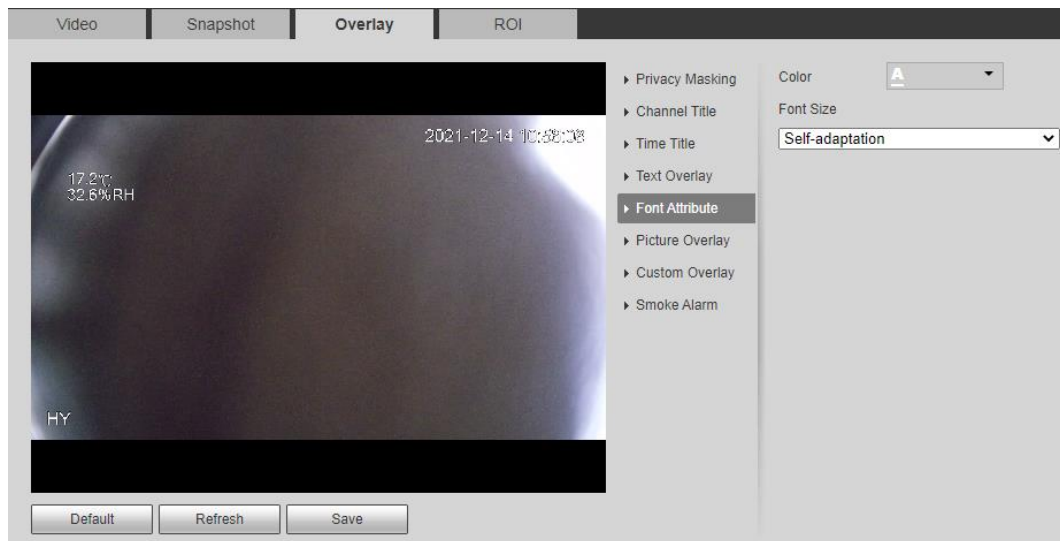
Step 4 Click **Save**.

4.4.2.3.5 Configure Font Attribute

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

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

Figure 4-34 Font attribute



Step 2 Select the font color and size.
Click **More Color** to customize the font color.

Step 3 Click **Save**.

4.4.2.3.6 Configure Picture Overlay

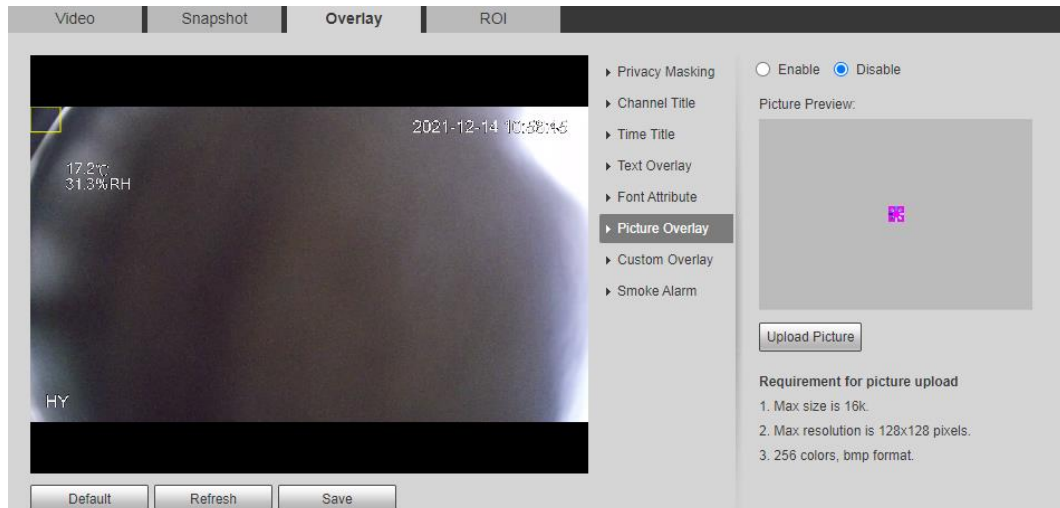
You can enable this function if you need to display picture information on the video image.



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

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

Figure 4-35 Picture overlay



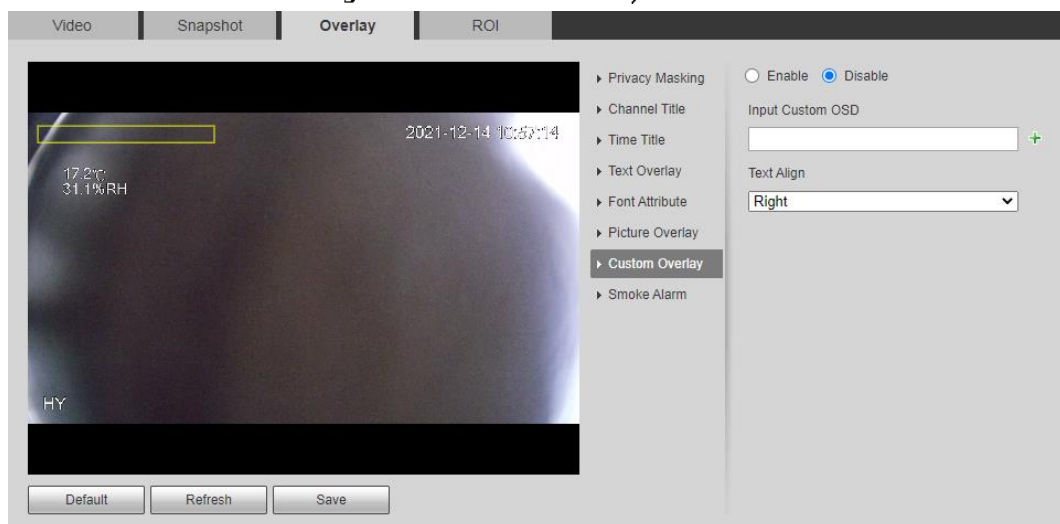
- Step 2** Select the **Enable** check box, click **Upload Picture**, and then select the picture to be overlaid.
The picture is displayed on the video image.
- Step 3** Move the overlaid picture to the position that you want in the image.
- Step 4** Click **Save**.

4.4.2.3.7 Configure Custom Overlay

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

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

Figure 4-36 Custom overlay



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



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

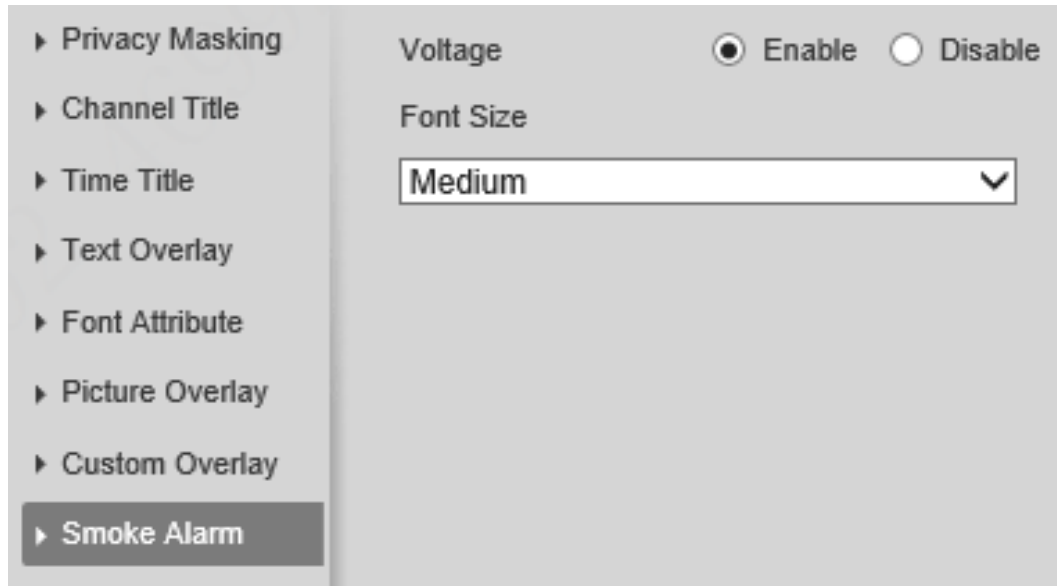
- Step 3** Move the custom box to the position that you want in the image.
- Step 4** Click **Save**.

4.4.2.3.8 Configure Smoke Alarm

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

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

Figure 4-37 Smoke Alarm



Step 2 Configure the smoke alarm overlay parameters, and then select the font size.

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

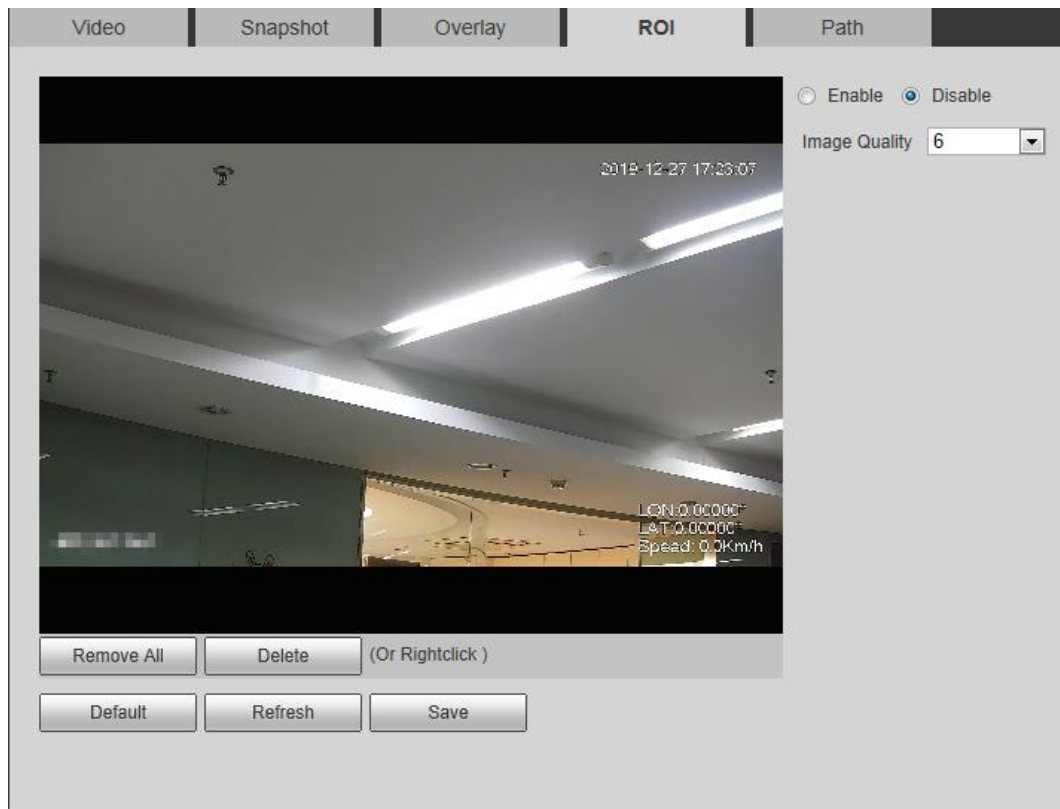
Step 4 Click **Save**.

4.4.2.4 ROI

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

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

Figure 4-38 ROI



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



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

Step 3 Click **Save**.

4.4.2.5 Path

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

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

Figure 4-39 Path



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

Table 4-14 Description of path

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



Admin in the path refers to the account being used.

Step 3 Click **Save**.

4.4.3 Audio

You can configure audio parameters and alarm audio.

4.4.3.1 Configuring Audio Parameter

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

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

Figure 4-40 Audio

The screenshot shows the 'Audio' configuration page with the 'Alarm Audio' tab selected. It is divided into three main sections: 'Encode', 'Attribute', and a bottom control bar.

- Encode Section:**
 - Main Stream:**
 - Enable
 - Encode Mode: G.711A
 - Sampling Frequency: 8000
 - Sub Stream:**
 - Enable
 - Sub Stream 1
 - Encode Mode: G.711A
 - Sampling Frequency: 8000
- Attribute Section:**
 - AudiIn Type: Mic
 - Noise Filter: Enable
 - Microphone Volume: Slider set to 50
 - Speaker Volume: Slider set to 100
- Bottom Control Bar:** Default, Refresh, Save buttons.

- Step 2** Select the **Enable** check box in **Main Stream** or **Sub Stream**.
For the camera with multiple channels, select the channel number.



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

- Step 3** Configure audio parameters.

Table 4-15 Description of audio parameters

Parameter	Description
Encode Mode	You can select audio Encode Mode from G.711A , G.711Mu , AAC , G.726 , PCM and G.723 . The configured audio encode mode applies to both audio and intercom. The default value is recommended.

Parameter	Description
Sampling Frequency	Sampling number per second. The higher the sampling frequency is, the more the sample in a second will be, and the more accurate the restored signal will be. You can select audio Sampling Frequency from 8K, 16K, 32K .
Audioin Type	You can select audioin type from: <ul style="list-style-type: none"> • Linein: Requires external audio device. • Mic: Not require external audio device.
Noise Filter	Enable this function, and the system auto filters ambient noise.
Microphone Volume	Adjusts microphone volume.
Speaker Volume	Adjusts speaker volume.

Step 4 Click **Save**.

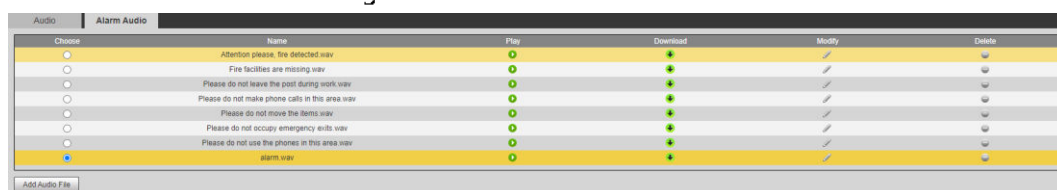
4.4.3.2 Configuring Alarm Audio

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

- Click to play the selected audio.
- Click to download the audio to local storage.

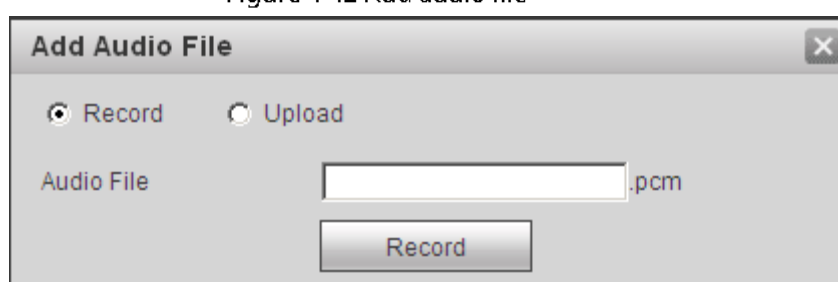
Step 1 Select **Setting > Camera > Audio > Alarm Audio**.

Figure 4-41 Alarm audio



Step 2 Click **Add Audio File**.

Figure 4-42 Add audio file



Step 3 Configure the audio file.

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



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

Step 4 Select the file that you need.

4.5 Network

This section introduces network configuration.

4.5.1 TCP/IP

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

Prerequisites

The camera has connected to the network.

Procedure

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

Figure 4-43 TCP/IP

The screenshot displays the TCP/IP configuration window. At the top, the title is 'TCP/IP'. Below it, there are several configuration fields:


- Host Name:** A text input field containing 'IPC'.
- Ethernet Card:** A dropdown menu showing 'Wire(DEFAULT)' with a 'Set as Default' button to its right.
- Mode:** Two radio buttons, 'Static' (selected) and 'DHCP'.
- MAC Address:** A field with six small input boxes for hexadecimal digits.
- IP Version:** A dropdown menu showing 'IPv4'.
- IP Address:** A field with four small input boxes for octets.
- Subnet mask:** A field with four small input boxes for octets.
- Default Gateway:** A field with four small input boxes for octets.
- Preferred DNS Server:** A field with four small input boxes for octets.
- Alternate DNS Server:** A field with four small input boxes for octets.

 At the bottom, there is a checked checkbox labeled 'Enable ARP/Ping to set IP address service' and three buttons: 'Default', 'Refresh', and 'Save'.

Step 2 Configure TCP/IP parameters.

Table 4-16 Description of TCP/IP parameters

Parameter	Description
Host Name	Enter the host name, and the maximum length is 15 characters.
Ethernet Card	Select the Ethernet card that need to be configured, and the default one is Wire .

Parameter	Description
Mode	<p>The mode that the camera gets IP:</p> <ul style="list-style-type: none"> Static Configure IP Address, Subnet Mask, and Default Gateway manually, and then click Save, the login interface with the configured IP address is displayed. DHCP When there is DHCP server in the network, select DHCP, and the camera acquires IP address automatically.
MAC Address	Displays host MAC address.
IP Version	Select IPv4 or IPv6 .
IP Address	<p>When you select Static in Mode, enter the IP address and subnet mask that you need.</p> <p></p> <ul style="list-style-type: none"> IPv6 does not have subnet mask. The default gateway must be in the same network segment with the IP address.
Subnet Mask	
Default Gateway	
Preferred DNS	IP address of the preferred DNS
Alternate DNS	IP address of the alternate DNS

Parameter	Description
Enable ARP/Ping to set IP address service	<p>Select the check box, get the camera MAC address, and then you can modify and configure the device IP address with ARP/ping command. This is enabled by default. During reboot, you will have no more than 2 minutes to configure the device IP address by a ping packet with certain length, the server will be turned off in 2 minutes, or it will be turned off immediately after the IP address is successfully configured. If this is not enabled, the IP address cannot be configured with ping packet.</p> <p>A demonstration of configuring IP address with ARP/Ping.</p> <ol style="list-style-type: none"> 1. Keep the camera that needs to be configured and the PC within the same local network, and then get a usable IP address. 2. Get the MAC address of the camera from device label. 3. Open command editor on the PC and enter the following command. <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <p>Windows syntax[↵]</p> <pre>arp -s <IP Address> <MAC> ↵ ping -l 480 -t <IP Address> ↵</pre> </div> <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <p>Windows example[↵]</p> <pre>arp -s 192.168.0.125 11-40-8c-18-10-11 ↵ ping -l 480 -t 192.168.0.125 ↵</pre> </div> <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <p>UNIX/Linux/Mac syntax[↵]</p> <pre>arp -s <IP Address> <MAC> ↵ ping -s 480 <IP Address> ↵</pre> </div> <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <p>UNIX/Linux/Mac example[↵]</p> <pre>arp -s 192.168.0.125 11-40-8c-18-10-11 ↵ ping -s 480 192.168.0.125 ↵</pre> </div> <ol style="list-style-type: none"> 4. Restart the camera. 5. Check the PC command line, if information such as Reply from 192.168.0.125... 6. Enter http://(IP address) in the browser address bar to log in.

Step 3 Click **Save**.

4.5.2 Port

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

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

Figure 4-44 Port

Port

Max Connection	<input type="text" value="10"/>	(1~20)
TCP Port	<input type="text" value="37777"/>	(1025~65534)
UDP Port	<input type="text" value="37778"/>	(1025~65534)
HTTP Port	<input type="text" value="80"/>	
RTSP Port	<input type="text" value="554"/>	
RTMP Port	<input type="text" value="1935"/>	(1025~65534)
HTTPS Port	<input type="text" value="443"/>	

Step 2 Configure port parameters.



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

Table 4-17 Description of port parameters

Parameter	Description
Max Connection	The max number of users (web client, platform client or mobile phone client) that can connect to the device simultaneously. The value is 10 by default.
TCP Port	Transmission control protocol port. The value is 37777 by default.
UDP Port	User datagram protocol port. The value is 37778 by default.
HTTP Port	Hyper text transfer protocol port. The value is 80 by default.

Parameter	Description
RTSP Port	<ul style="list-style-type: none"> Real time streaming protocol port, and the value is 554 by default. If you play live view with QuickTime, VLC or Blackberry smart phone, the following URL format is available. When the URL format requiring RTSP, you need to specify channel number and bit stream type in the URL, and also user name and password if needed. When playing live view with Blackberry smart phone, you need to turn off the audio, and then set the codec mode to H.264B and resolution to CIF. <p>URL format example: <code>rtsp://username:password@ip:port/cam/realmonitor?channel=1&subtype=0</code> Among that:</p> <ul style="list-style-type: none"> Username: The user name, such as admin. Password: The password, such as admin. IP: The device IP, such as 192.168.1.112. Port: Leave it if the value is 554 by default. Channel: The channel number, which starts from 1. For example, if you are using channel 2, then the channel=2. Subtype: The bit stream type; 0 means main stream (Subtype=0) and 1 means sub stream (Subtype=1). <p>Example: If you require the sub stream of channel 2 from a certain device, then the URL should be: <code>rtsp://admin:admin@10.12.4.84:554/cam/realmonitor?channel=21&=1</code> If user name and password are not needed, then the URL can be: <code>rtsp://ip:port/cam/realmonitor?channel=11&=0</code></p>
RTMP Port	Real Time Messaging Protocol. The port that RTMP provides service. It is 1935 by default.
HTTPS Port	HTTPS communication port. It is 443 by default.

Step 3 Click **Save**.



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

4.5.3 PPPoE

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

Prerequisites

- The camera has connected to the network.

- You have gotten the account and password from Internet Service Provider.

Procedure

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

Figure 4-45 PPPoE



Step 2 Select the **Enable** check box, and then enter user name and password.



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

Step 3 Click **Save**.

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

4.5.4 DDNS

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

Prerequisites

Check the type of DNS server supported by the camera.

Procedure

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



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

Figure 4-46 DDNS (1)

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

Table 4-18 Description of DDNS parameters

Parameter	Description
Type	The name and web address of the DDNS service provider, see the matching relationship below: <ul style="list-style-type: none"> • CN99 DDNS web address: www.3322.org • NO-IP DDNS web address: dynupdate.no-ip.com • Dyndns DDNS web address: members.dyndns.org
Web Address	
Domain Name	The domain name you registered on the DDNS website.
Test	Only when selecting NO-IP DDNS type, you can click test to check whether the domain name registration is successful.
Username	Enter the username and password that you got from the DDNS server provider. You need to register an account (includes username and password) on the DDNS server provider's website.
Password	
Interval	The update cycle of the connection between the device and the server, and the time is 10 minutes by default.

Step 3 Click **Save**.

Result

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

4.5.5 SMTP (Email)

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

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

Figure 4-47 SMTP (Email)

Step 2 Configure SMTP (Email) parameters.




Table 4-19 Description of SMTP (Email) parameters



Parameter	Description
SMTP Server	SMTP server address
Port	The port number of the SMTP server.
Username	The account of SMTP server.
Password	The password of SMTP server.
Anonymity	Select the check box, and the sender's information is not displayed in the email.
Sender	Sender's email address.
Authentication	Select Authentication from None , SSL and TLS . For details, see Table 4-20.
Title	Enter maximum 63 characters in Chinese, English, and Arabic numerals. Click to select title type, including Name , Device ID , and Event Type , and you can set maximum 2 titles.
Attachment	Select the check box to support attachment in the email.
Mail Receiver	Receiver's email address. Supports 3 addresses at most.

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

For the configuration of major mailboxes, see Table 4-20.

Table 4-20 Description of major mailbox configuration

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

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

Step 3 Click **Save**.

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

4.5.6 UPnP

UPnP (Universal Plug and Play), a protocol that establishes mapping relation between local area and wide area networks. This function enables you to visit local area device through wide area IP address.

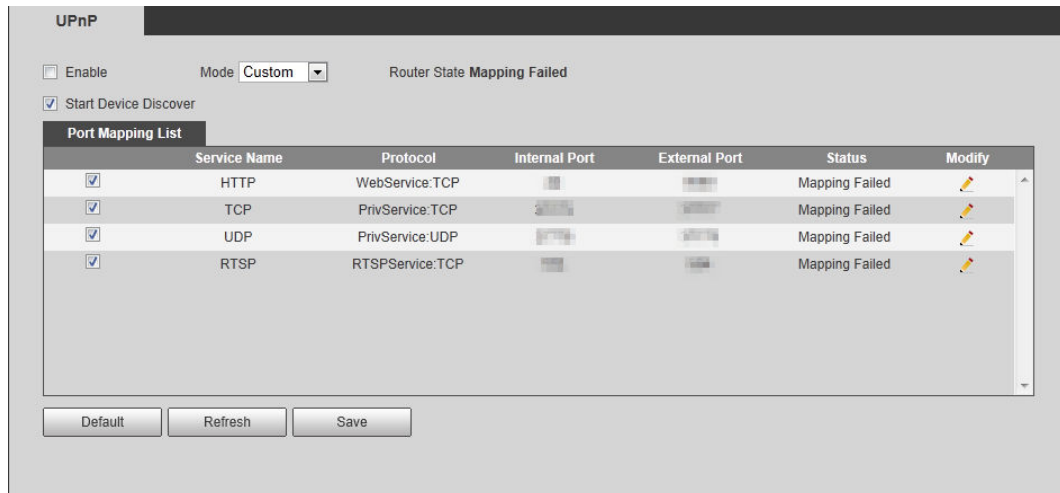
Prerequisites

- Make sure the UPnP service is installed in the system.
- Log in the router, and configure WAN IP address to set up internet connection.
- Enable UPnP in the router.
- Connect your device to the LAN port of the router.
- Select **Setting > Network > TCP/IP**, in **IP Address**, enter the local area IP address of the router or select **DHCP** and acquires IP address automatically.

Procedure

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

Figure 4-48 UPnP



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

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

Step 3 Click **Save**.

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

4.5.7 SNMP

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


Prerequisites

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

Procedure

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

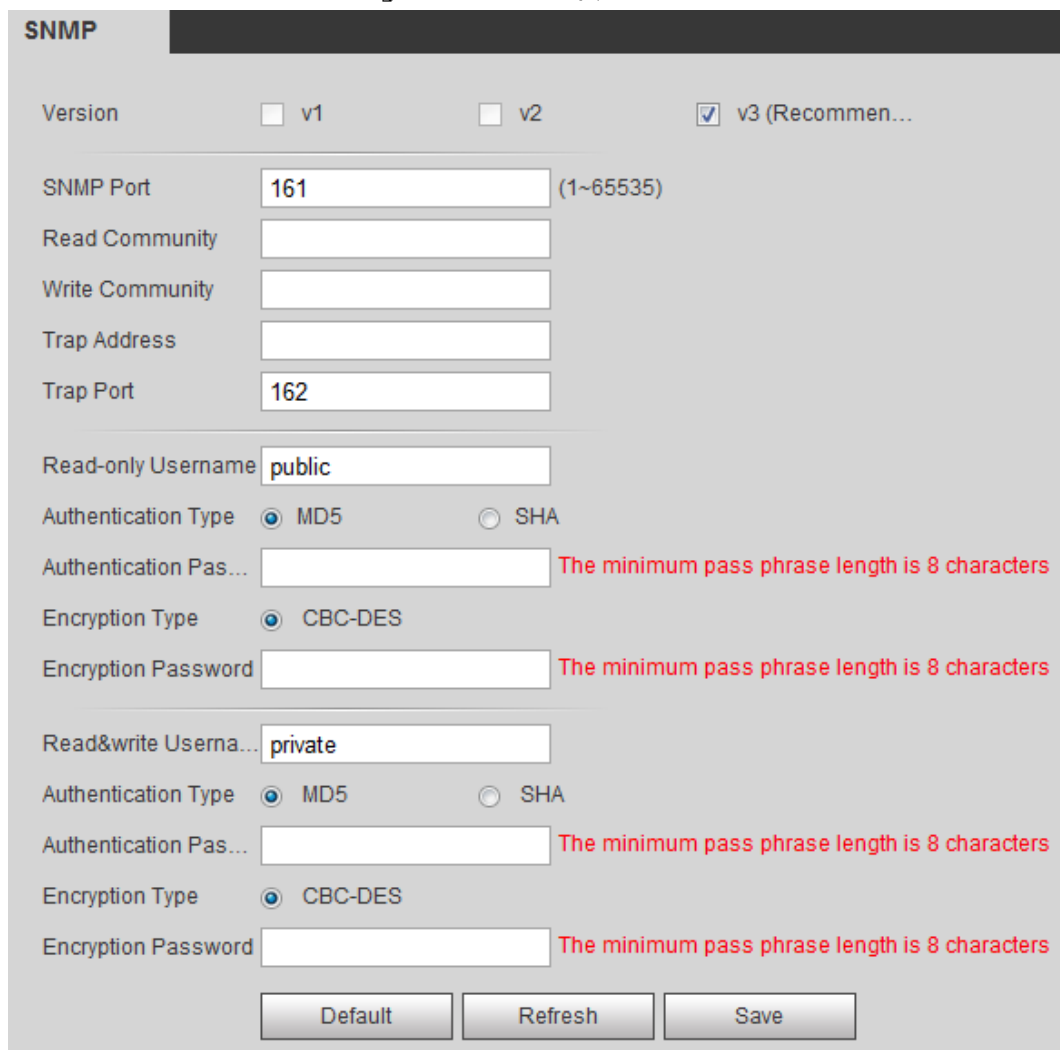
Figure 4-49 SNMP (1)



SNMP configuration interface showing the following fields and options:

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

Figure 4-50 SNMP (2)



SNMP configuration interface showing the following fields and options:

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

Step 2 Select SNMP version to enable SNMP.

- Select **V1**, and the system can only process information of V1 version.
- Select **V2**, and the system can only process information of V2 version.
- Select **V3**, and then **V1** and **V2** become unavailable. You can configure user name,




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



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

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

Table 4-21 Description of SNMP parameters

Parameter	Description
SNMP Port	The listening port of the software agent in the device.
Read Community, Write Community	The read and write community string that the software agent supports.  You can enter number, letter, underline and dash to form the name.
Trap Address	The target address of the Trap information sent by the software agent in the device.
Trap Port	The target port of the Trap information sent by the software agent in the device.
Read-only Username	Set the read-only username accessing device, and it is public by default.  You can enter number, letter, and underline to form the name.
Read/Write Username	Set the read/write username access device, and it is public by default.  You can enter number, letter, and underline to form the name.
Authentication Type	You can select from MD5 and SHA . The default type is MD5 .
Authentication Password	It should be no less than 8 digits.
Encryption Type	The default is CBC-DES.
Encryption Password	It should be no less than 8 digits.

Step 3 Click **Save**.

Result

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

1. Run MIB Builder and MG-SOFT MIB Browser.
2. Compile the two MIB files with MIB Builder.
3. Load the generated modules with MG-SOFT MIB Browser.
4. Enter the IP address of the device you need to manage in the MG-SOFT MIB Browser, and then select version to search.
5. Unfold all the tree lists displayed in the MG-SOFT MIB Browser, and then you can view the

configuration information, video channel amount, audio channel amount, and software version.



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

4.5.8 Bonjour

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

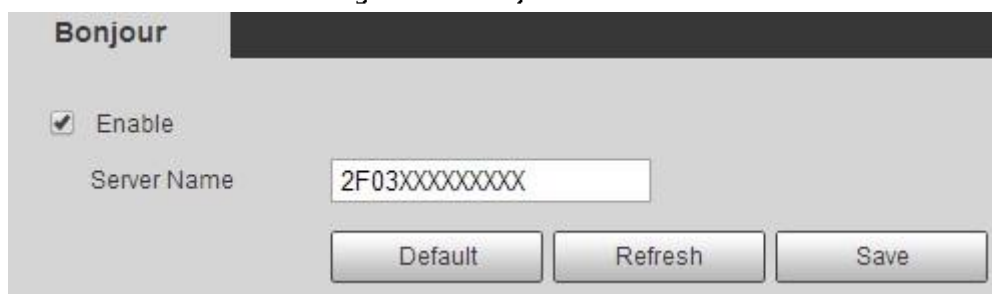


Bonjour is enabled by default.

Procedure

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

Figure 4-51 Bonjour



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

Step 3 Click **Save**.

Result

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

1. Click **Show All Bookmarks** in Safari.
2. Enable **Bonjour**. The OS or client automatically detects the network cameras with Bonjour enabled in the LAN.
3. Click the camera to visit the corresponding web interface.

4.5.9 Multicast

When multiple users are previewing the device video image simultaneously through network, it might fail due to limited bandwidth. You can solve this problem by setting up a multicast IP (224.0.1.0–238.255.255.255) for the camera and adopt the multicast protocol.

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

Figure 4-52 Multicast

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

Table 4-22 Description of multicast parameters

Parameter	Description
Multicast Address	The multicast IP address of Main Stream/Sub Stream is 224.1.2.4 by default, and the range is 224.0.0.0–239.255.255.255.
Port	The multicast port of corresponding stream: Main Stream: 40000; Sub Stream1: 40016; Sub Stream2: 40032, and all the range is 1025–65500.

Step 3 Click **Save**.

Result

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

4.5.10 802.1x

Cameras can connect to LAN after passing 802.1x authentication.

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

Figure 4-53 802.1x

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

Table 4-23 Description of 802.1x parameters

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


Step 3 Click **Save**.

4.5.11 QoS

You can solve problems such as network delay and congestion with this function. It helps to assure bandwidth, reduce transmission delay, packet loss rate, and delay jitter to improve experience. 0–63 means 64 degrees of priority; 0 for the lowest and 63 the highest.

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

Figure 4-54 QoS



Step 2 Configure QoS parameters.

Table 4-24 Description of QoS parameters

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

Step 3 Click **Save**.

4.5.12 Access Platform

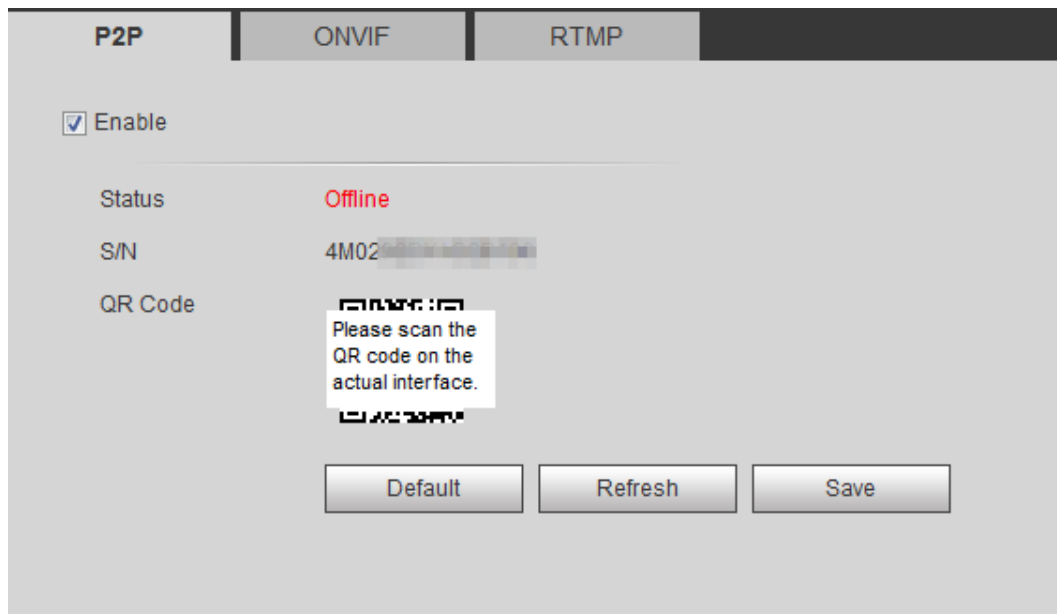
4.5.12.1 P2P

P2P is a private network traversal technology which enables users to manage devices easily without requiring DDNS, port mapping or transit server.

Scan the QR code with your smart phone, and then you can add and manage more devices on the mobile phone client.

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

Figure 4-55 P2P



- When P2P is enabled, remote management on device is supported.
- When P2P is enabled and the device accesses to the network, the status shows online. The information of the IP address, MAC address, device name, and device SN will be collected. The collected information is for remote access only. You can cancel **Enable** selection to reject the collection.

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

Step 3 Tap the + at the upper right corner.

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

Step 5 Follow the instructions to finish the settings.

4.5.12.2 ONVIF

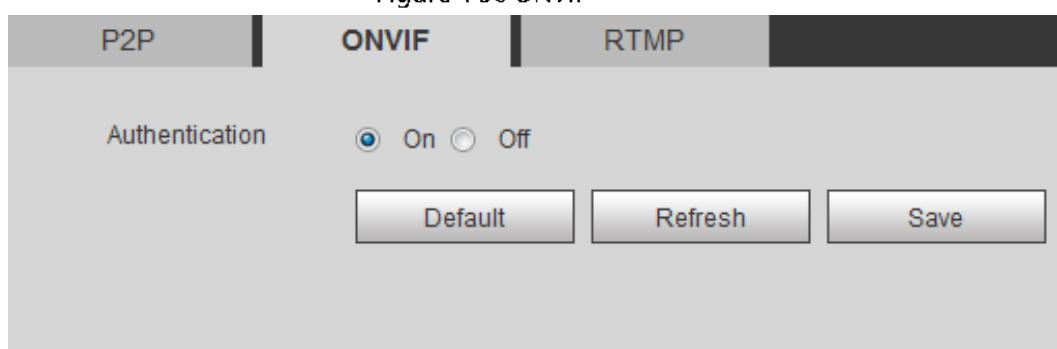
The ONVIF authentication is **On** by default, which allows the network video products (including video recording device and other recording devices) from other manufacturers to connect to your device.



ONVIF is enabled by default.

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

Figure 4-56 ONVIF



Step 2 Select **On** in **Authentication**.

Step 3 Click **Save**.

4.5.12.3 RTMP

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



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

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

Figure 4-57 ONVIF

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



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

Step 3 Configure RTMP parameters. .

Table 4-25 Description of RTMP parameters

Parameter	Description
Stream Type	The stream for live view. Make sure that the video format is the H.264, H.264 B and H.264H, and the audio format is AAC.
Address Type	Includes Non-custom and Custom . <ul style="list-style-type: none"> • Non-custom: Enter the server IP and domain name. • Custom: Enter the path allocated by the server.
IP Address	When selecting Non-custom , you need to enter server IP address and port. <ul style="list-style-type: none"> • IP address: Support IPv4 or domain name. • Port: We recommend that you use the default one.
Port	
Custom Address	When selecting Custom , you need to enter the path allocated by the server.

Step 4 Click **Save**.

4.6 Storage

This section introduces how to manage saved resources (such as recorded video) and storage space. The storage management helps to make best use of storage space.

4.6.1 Setting Storage Plan

- Setting record plan and record control to achieve all-time recording, recording in specific period or alarm linked recording. For details, see "5.1.1.2.1 Setting Record Plan" and "5.1.1.2.2 Setting Record Control".
- Set the snapshot schedule as needed. For details, see "5.1.1.3.1 Setting Snapshot Plan".

4.6.2 Setting Schedule

You can configure record schedule, snapshot schedule and holiday schedule. Set certain days as holiday, and when the **Record** or **Snapshot** is selected in the holiday schedule, the system takes snapshot or records video as holiday schedule defined.

Prerequisites

- Set the record mode to be **Auto** in **Record Control**. For details, see "5.1.1.2.1 Setting Record Plan".
- Configure holiday record and snapshot schedule. For details, see "5.1.1.2.1 Setting Record Plan" and "5.1.1.3.1 Setting Snapshot Plan".

Procedure

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

Figure 4-58 Holiday schedule

Step 2 Select **Record** or **Snapshot**.

Step 3 Select the days you need to set as holiday.

Those days with yellow color indicates that they were set as holidays.



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

Step 4 Click **Save**.

4.6.3 Setting Destination

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

4.6.3.1 Path

You can select different storage paths for the recorded videos and snapshots according to event type. You can select from SD card, FTP and NAS.



Local is displayed only on models that support SD card.

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

Figure 4-59 Path

The screenshot shows a configuration interface with three tabs: Local, FTP, and NAS. The NAS tab is selected. Below the tabs are two tables: 'Record' and 'Snapshot'. Each table has columns for Event Type, Scheduled, Motion Detection, and Alarm. In the Record table, FTP has all three checkboxes checked. In the Snapshot table, FTP also has all three checkboxes checked. Below the tables are three buttons: Default, Refresh, and Save.

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

Table 4-26 Description of path parameters

Parameter	Description
Event Type	Select from Scheduled , Motion Detection and Alarm .
Local	Save in the internal SD card.
FTP	Save in the FTP server.
NAS	Save in the NAS (network attached storage).

Step 3 Click **Save**.

Step 4 Configure other path parameters on **Destination**, **FTP** or **NAS** interface. For details, see "4.6.3 Setting Destination", "4.6.3.3 FTP" or "4.6.3.4 NAS".

4.6.3.2 Local

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



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

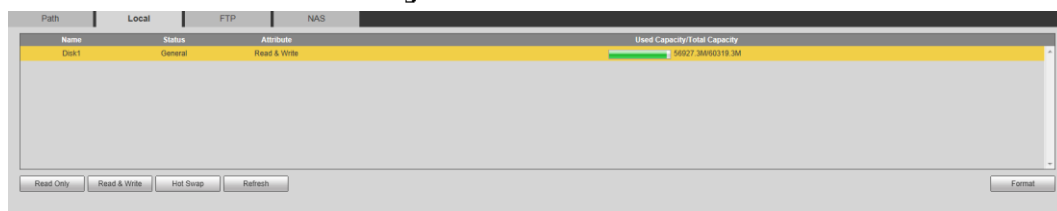
Select **Setting > Storage > Destination > Local**.

- Click **Read Only**, and then the SD card is set to read only.
- Click **Read & Write**, and then the SD card is set to read & write.
- Click **Hot Swap**, and then you can pull out the SD card.
- Click **Refresh**, and then you can format the SD card.
- Click **Format**, and you can format the SD card.



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

Figure 4-60 Local



4.6.3.3 FTP

FTP can be enabled only when it was selected as a destination path. When the network does not work, you can save all the files to the internal SD card for emergency.

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

Step 2 Select the **Enable** check box, and select the FTP type.



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

Step 3 Configure FTP parameters.

Figure 4-61 FTP

Figure 4-62 Picture name settings


No.	Picture Name Content	Separator	Ordering
<input checked="" type="checkbox"/>	1	Date&Time	↔ ↑ ↓
<input checked="" type="checkbox"/>	2	Millisecond	↔ ↑ ↓
<input checked="" type="checkbox"/>	3	Name	↑ ↓
<input checked="" type="checkbox"/>	4	IP Address	↑ ↓
<input type="checkbox"/>	5	Channel NO.	↑ ↓
<input type="checkbox"/>	6	Snapshot Type	↑ ↓
<input type="checkbox"/>	7	Custom	↑ ↓

Date&TimeMillisecond_Name_IP Address_

Separator can only be a dash, underline or space.

Table 4-27 Description of FTP parameters

Parameter	Description
Server Address	The IP address of the FTP server.
Port	The port number of the FTP server.

Parameter	Description
Username	The user name to log in to the FTP server.
Password	The password to log in to the FTP server.
Remote Directory	The destination path in the FTP server, and it is shared by default.
Directory Structure	Set the directory structure, which supports three levels at most.
Level 1 Directory	Set the directory name, and you can customized the name. When you select Custom , enter the custom directory name, which supports numbers, English letters, underlines and dashes.
Level 2 Directory	
Level 3 Directory	
Customized Picture Name	Click Setting to set picture name. <ul style="list-style-type: none"> • Date&Time is required, and it is selected by default. • Select the other fields of the name, and the corresponding instruction will be displayed on the screen. • Double-click the symbols under Separator, you can customize the separator. • Double-click Custom, you can customize the files of the picture name. • Click the arrow under Ordering, and you can adjust the ordering of the file.  <p>Date&Time and Millisecond is a whole, click the arrow of any one of the two fields, the two moves together.</p> <ul style="list-style-type: none"> • The real-time value of Millisecond will be displayed for precise snapshot, and for schedule and normal event, the millisecond displays 0000.
Emergency (Local)	Select Emergency (Local) , and when the FTP server does not work, all the files are saved to the internal SD card.

Step 4 Click **Save**.

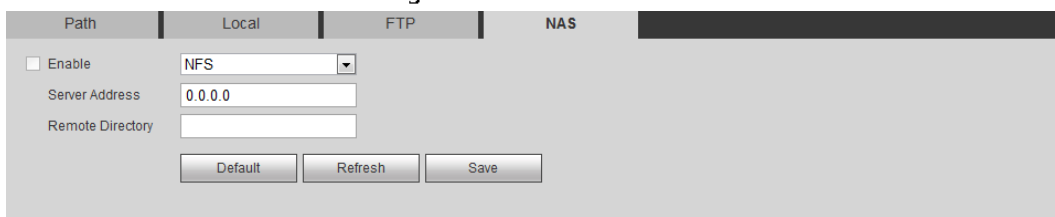
Step 5 Click **test** to test whether FTP function works normally.

4.6.3.4 NAS

This function can be enabled only when NAS was selected as a destination path. Enable this function, and you can save all the files in the NAS.

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

Figure 4-63 NAS



The screenshot shows a configuration window for NAS. At the top, there are four tabs: Path, Local, FTP, and NAS. The 'Path' tab is active. Below the tabs, there is a section for 'Enable' with a checked checkbox. To the right of the checkbox is a dropdown menu currently showing 'NFS'. Below this are three input fields: 'Server Address' with the value '0.0.0.0', and 'Remote Directory' which is empty. At the bottom of the configuration area, there are three buttons: 'Default', 'Refresh', and 'Save'.

Step 2 Select the **Enable** check box to enable NAS function, and select NAS protocol type.

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

Step 3 Configure NAS parameters.

Table 4-28 Description of NAS parameters

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

Step 4 Click **Save**.

4.7 System

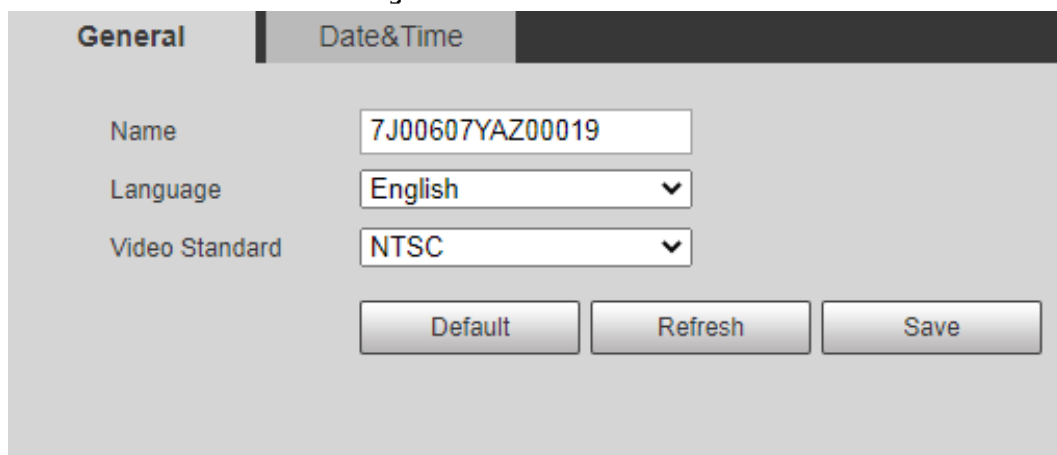
This section introduces system configurations, including general, date & time, account, safety, PTZ settings, default, import/export, remote, auto maintain and upgrade.

4.7.1 General

You can configure device name, language and video standard.


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

Figure 4-64 General



Step 2 Configure general parameters.

Table 4-29 Description of general parameters

Parameter	Description
Name	The name of the device.  Each device has its own name.
Language	Select system language.

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

Step 3 Click **Save**.

4.7.2 Date & Time

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

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

Figure 4-65 Date and time

Step 2 Configure date and time parameters.

Table 4-30 Description of date and time parameters

Parameter	Description
Date Format	Configure the date format.
Time Format	Configure the time format. You can select from 12-Hour or 24-Hour .
Time Zone	Configure the time zone that the camera is at.
Current Time	Configure system time. Click Sync PC , and the system time changes to the PC time.
DST	Enable DST as needed. Select the check box, and configure start time and end time of DST with Date or Week .
NTP	Select the check box, and then NTP (network time protocol) is enabled, the system then syncs time with the internet server in real time. You can also enter the IP address, time zone, port, and interval of a PC which installed NTP server to use NTP.
NTP Server.	
Time Zone	
Port	
Interval	

Step 3 Click **Save**.

4.7.3 Account

Manage all the users. You can add, delete, or modify users. Users include admin, added users and ONVIF users.

Managing users and groups are only available for administrator users.

- The max length of the user or group name is 31 characters which consisted of number, letters, underline, dash, dot and @.
- The password must consist of 8 to 32 non-blank characters and contain at least two types of characters among upper case, lower case, number, and special character (excluding ' " ; &).
- You can have 18 users and 8 groups at most.
- You can manage users through single user or group, and duplicate user names or group names are not allowed. A user can be in only one group at a time, and the group users can own authorities within group authority range.
- Online users cannot modify their own authority.
- There is one admin by default which has highest authority.
- Select **Anonymous Login**, and then log in with only IP address instead of user name and password. Anonymous users only have preview authorities. During anonymous login, click **Logout**, and then you can log in with other username.

4.7.3.1 Adding a User

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

Step 1 Select **Setting > System > Account > Account > Username**.

Figure 4-66 Username

The screenshot shows the 'Account' management interface. At the top, there are tabs for 'Account' and 'Onvif User'. Below the tabs, there is a checkbox for 'Anonymous Login'. The main area contains a table with columns: No., Username, Group Name, Memo, Restricted Login, Modify, and Delete. Below the table is an 'Authority' grid with rows for User, Manual Control, and Peripheral, and columns for Live, File Backup, AV Parameter, Playback, Storage, PTZ, System, Event, Security, System Info, Network, and Maintenance. At the bottom, there is an 'Add User' button.

No.	Username	Group Name	Memo	Restricted Login	Modify	Delete
1	admin	admin	admin's account	/	[Edit]	[Delete]
2	admin1	admin		[Search]	[Edit]	[Delete]

Authority	Live	Playback	System	System Info
User	Live	Playback	System	System Info
Manual Control	File Backup	Storage	Event	Network
Peripheral	AV Parameter	PTZ	Security	Maintenance

Add User

Step 2 Click **Add User**.

Figure 4-67 Add user (operation permission)

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
- Security
- Maintenance

Figure 4-68 Add user (restricted login)

Step 3 Configure user parameters.

Table 4-31 Description of user parameters (1)

Parameter	Description
Username	User's unique identification. You cannot use existed user name.
Password	Enter password and confirm it again.
Confirm Password	The password must consist of 8 to 32 non-blank characters and contain at least two types of characters among upper case, lower case, number, and special character (excluding ' " ; : &).
Group Name	The group that users belong to. Each group has different authorities.
Memo	Describe the user.
Operation Permission	Select authorities as needed.  You are recommended giving fewer authorities to normal users than advance users.


Parameter	Description
Restricted Login	<p>Set the PC address that allows the defined user to log in to the camera and the validity period and time range. You can log in to web with the defined IP in the defined time range of validity period.</p> <ul style="list-style-type: none"> • IP address: You can log in to web through the PC with the set IP. • Validity period: You can log in to web in the set validity period. • Time range: You can log in to web in the set time range. <p>Set as following:</p> <ol style="list-style-type: none"> 1. Select IP Address: Select IP type and set IP address. <ul style="list-style-type: none"> ◇ IP Address: Enter the IP address of the host to be added. ◇ IP segment: Enter the start address and end address of the host to be added. 2. Select Validity Period: Set the begin time and end time. 3. Select Time Range: Set the time range that allow user to log in. For details, see "5.1.1.1 Setting Period".

Step 4 Click **Save**.

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

Related Operations

- Edit user information

Click  to modify password, group, memo, operation authorities, and login authorities.



You can only change the password of the admin.

The methods of changing password vary with different accounts.

- ◇ Login with the admin account, you can change password through **Old Password** and **Admin Account**.
- ◇ Login with non-admin account (an added account with with the permission of user management), you can change password through **Old Password**.
- ◇ **Old Password**: Change the password through entering the old password to be changed, and then the new password.

Figure 4-69 Change password through old password (Login with non-admin account)

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

- Username:** A dropdown menu with '11' selected.
- Modify Password:** A checked checkbox.
- Old Password:** An empty text input field.
- New Password:** An empty text input field.
- Strength:** A red text warning: "The minimum pass phrase length is 8 characters". Below it are three buttons: 'Weak', 'Medium', and 'Strong'.
- Confirm Password:** An empty text input field.
- Group Name:** A dropdown menu with 'user' selected.
- Memo:** An empty text input field.
- Authority:** A checkbox for 'All' (unchecked) and a list box containing 'Live' and 'Playback', both of which are checked.
- Buttons:** 'Save' and 'Cancel' buttons at the bottom.

- ◇ **Admin Account:** Change the password through entering the admin password, and then the new password for the non-admin account to be changed.

Figure 4-70 Change password through admin password (login with admin account)

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


- Username:** A dropdown menu with '11' selected.
- Modify Password:** A checked checkbox.
- Modification Mode:** A dropdown menu with 'Admin Account' selected.
- Admin Username:** A text input field containing 'admin'.
- Admin Password:** An empty text input field.
- New Password:** An empty text input field.
- Strength:** A red text warning: "The minimum pass phrase length is 8 characters". Below it are three buttons: 'Weak', 'Medium', and 'Strong'.
- Confirm Password:** An empty text input field.
- Group Name:** A dropdown menu with 'user' selected.
- Memo:** An empty text input field.

- **Delete users**
Click  to delete the added users.



Admin account cannot be deleted.

- View the authorities

If the current account has with the permission of user management, click  to view the login authorities of other accounts. If not, you can only view the login authorities of the current account.

4.7.3.2 Adding User Group

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

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

Figure 4-71 Group name

The screenshot displays the 'Group Name' configuration page. At the top, there are tabs for 'Account' and 'Onvif User'. Below the tabs, there is a checkbox for 'Anonymous Login'. The main content area features a table with the following data:

No.	Group Name	Memo	Modify	Delete
1	admin	administrator group		
2	user	user group		

Below the table, there is an 'Authority' section with a grid of permissions:

User	Live	Playback	System	System Info
Manual Control	File Backup	Storage	Event	Network
Peripheral	AV Parameter	PTZ	Security	Maintenance

At the bottom left of the page, there is an 'Add Group' button.

Step 2 Click **Add Group**.

Figure 4-72 Add group

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

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

The newly added group displays in the group name list.



- After adding group, click to modify group memo or authorities; click to delete the added group, admin group and user group cannot be deleted.
- Click in the row of admin group or user group to modify group memo.

4.7.3.3 ONVIF User

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

Procedure

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

Figure 4-73 ONVIF user

No.	Username	Group Name	Modify	Delete
1	admin	admin		

Step 2 Click **Add User**.

Figure 4-74 Add user

Step 3 Configure user parameters.

Table 4-32 Description of user parameters (2)

Parameter	Description
Username	User's unique identification. You cannot use existed user name.
Password	Enter password and confirm it again.
Confirm Password	The password must consist of 8 to 32 non-blank characters and contain at least two types of characters among upper case, lower case, number, and special character (excluding ' " ; : &).
Group Name	The group that users belong to. Each group has different authorities.

Step 4 Click **Save**.

The newly added user displays in the user name list.

Related Operations

- Edit user information

Click to modify password, group, memo, operation authorities, and login authorities.



You can only change the password of the admin.

The methods of changing password vary with different account.

- ◇ Login with admin account, you can change password through **Old Password** and **Admin Account**.
The password of admin account can be changed through **Old Password** only.
- ◇ Login with non-admin account (an added account with the permission of user management), you can change password through **Old Password**.
- ◇ **Old Password**: Change the password through entering the old password to be changed, and then the new password.

Figure 4-75 Change password through old password (login with non-admin account)

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

- Username:** A dropdown menu with '11' selected.
- Modify Password:** A checked checkbox.
- Old Password:** An empty text input field.
- New Password:** An empty text input field.
- Strength:** A red text warning: 'The minimum pass phrase length is 8 characters'. Below it are three buttons: 'Weak', 'Medium', and 'Strong'.
- Confirm Password:** An empty text input field.
- Group Name:** A dropdown menu with 'user' selected.
- Memo:** An empty text input field.
- Authority:** A checkbox for 'All' (unchecked) and a list box containing 'Live' and 'Playback', both with checked checkboxes.
- Buttons:** 'Save' and 'Cancel' buttons at the bottom.

- ◇ **Admin Account:** Change the password through entering the admin password, and then the new password for the non-admin account to be changed.

Figure 4-76 Change password through admin password (login with admin account)

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

- Username:** A dropdown menu with '11' selected.
- Modify Password:** A checked checkbox.
- Modification Mode:** A dropdown menu with 'Admin Account' selected.
- Admin Username:** A text input field with 'admin' entered.
- Admin Password:** An empty text input field.
- New Password:** An empty text input field.
- Strength:** A red text warning: 'The minimum pass phrase length is 8 characters'. Below it are three buttons: 'Weak', 'Medium', and 'Strong'.
- Confirm Password:** An empty text input field.
- Group Name:** A dropdown menu with 'user' selected.
- Memo:** An empty text input field.

- Delete users
Click  to delete the added users.



Admin account cannot be deleted.

- View the authorities
 - If the current account has the permission of user management, click to view the login authorities of other accounts. If not, you can only view the login authorities of the current account.

4.7.4 Safety

You can configure system service, HTTPS, and Firewall.

4.7.4.1 System Service

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


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

Figure 4-77 System service

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

Table 4-33 Description of system service parameters

Function	Description
SSH	You can enable SSH authentication to perform safety management.
Multicast/Broadcast Search	Enable this function, and then when multiple users are previewing the device video image simultaneously through network, they can find your device with multicast/broadcast protocol.
Password Reset	Manage system security with this function.

Function	Description
CGI Service	Enable this function, and then other devices can access through this service.
Onvif Service	Enable this function, and then other devices can access through this service.
Genetec Service	Enable this function, and then other devices can access through this service.
Audio and Video Transmission Encryption	Enable to encrypt audio/video transmission.  Make sure that the other devices and software that working together with the camera support video decryption.
Mobile Push	Enable this function, and then the system would send the snapshot that was taken when alarm is triggered to your phone, this is enabled by default.

Step 3 Click **Save**.

4.7.4.2 HTTPS

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

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

Figure 4-78 HTTPS (1)

Step 2 Create a certificate or upload an authenticated certificate.

- For creating a certificate, click **Create**.

Figure 4-79 HTTPS dialog box

- For uploading the authenticated certificate, click **Browse** to select the certificate and certificate key, click **Upload** to upload them, and then skip to [Step 5](#).

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



The entered **IP or Domain name** must be the same as the IP or domain name of the device.

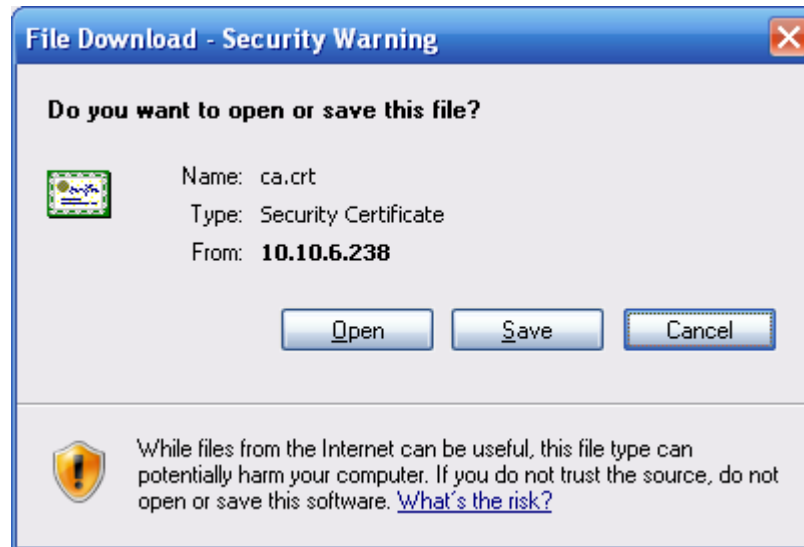
Step 4 Click **Install**.

Figure 4-80 Certificate installation

Step 5 Click **Download** to download root certificate.

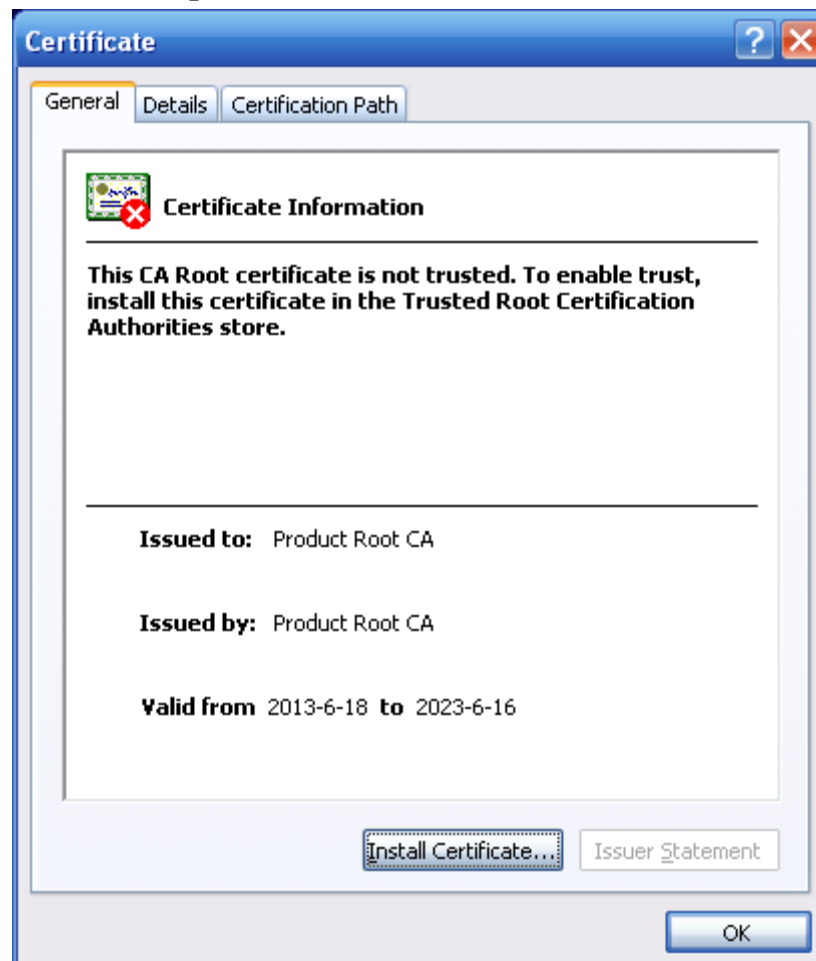
Step 6 Click **Download Root Certificate**.

Figure 4-81 File download



Step 7 Click **Open**.

Figure 4-82 Certificate information



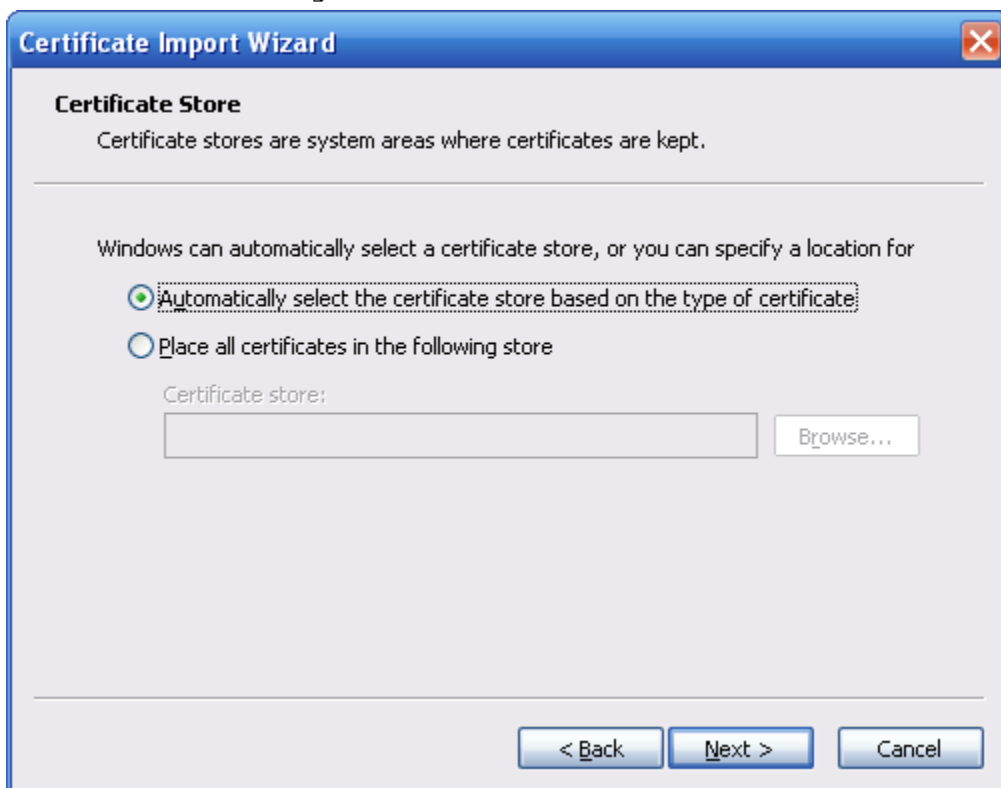
Step 8 Click **Install Certificate**.

Figure 4-83 Certificate import wizard (1)



Step 9 Click **Next**.

Figure 4-84 Certificate Store



Step 10 Select the storage location and click **Next**.

Figure 4-85 Certificate import wizard (2)



Step 11 Click **Finish** and a dialog box showing **The import was successful** pops up.

Figure 4-86 Import succeeds



4.7.4.3 Firewall

Configure **Network Access**, **PING prohibited** and **Prevent Semijoin** to enhance network and data security.

- **Network Access:** Set trusted list and restricted list to limit access.
 - ◇ **Allowlist:** Only when the IP/MAC of your PC in the allowlist, can you access the camera. Ports are the same.
 - ◇ **Blocklist:** When the IP/MAC of your PC is in the blocklist, you cannot access the camera. Ports are the same.
- **PING prohibited:** Enable **PING prohibited** function, and the camera will not respond to the ping request.
- **Prevent Semijoin:** Enable **Prevent Semijoin** function, and the camera can provide service normally under Semijoin attack.



- You cannot set allowlist or blocklist for camera IP or MAC addresses.
- You cannot set allowlist or blocklist for port MAC addresses.
- When the IP addresses of the camera and your PC are in the same LAN, MAC verification takes effect.
- When you access the camera through internet, the camera verifies the MAC address according to the router MAC.

This section takes **Network Access** as an example.

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

Figure 4-87 Firewall

System Service | HTTPS | **Firewall**

Rule Type: Network Access

Enable:

Mode: Allowlist Blocklist

Only the listed IP addresses/MAC are allowed to visit corresponding ports of the device.

<input checked="" type="checkbox"/>	IP address /MAC address	Port	Modify	Delete
<input checked="" type="checkbox"/>	Device All Ports	Device All Ports		
<input checked="" type="checkbox"/>	Device All Ports	Device All Ports		
<input checked="" type="checkbox"/>	Device All Ports	Device All Ports		
<input checked="" type="checkbox"/>	Device All Ports	Device All Ports		

Add IP/MAC

Default Refresh Save

Step 2 Select **Network Access** from **Rule Type** list, and then select the **Enable** check box.

- Enable **PING prohibited** and **Prevent Semijoin**, and click **Save**. You do not need to configure parameters.
- Enable **Network Access**, and configure allowlist and blocklist.
 - ◇ Select the mode: **Allowlist** and **Blocklist**.
 - ◇ Click **Add IP/MAC**.

Figure 4-88 Add IP/MAC

Step 3 Configure parameters.

Table 4-34 Description of adding IP/MAC parameters

Parameter	Description
Rule Type	Select IP address, IP segment, MAC address or all IP addresses. <ul style="list-style-type: none"> • IP address: Select IP version and enter the IP address of the host to be added. • IP segment: Select IP version and enter the start address and end address of the segment to be added. • MAC address: Enter MAC address of the host to be added. • All IP addresses: Set all IP addresses in allowlist or restricted list.
Device All Ports	Set access ports. You can select all ports or the ports in defined areas. <ul style="list-style-type: none"> • Device all ports: Set all IP port in allowlist or Blocklist. When selecting BlockList in Mode, and All IP Address in Rule Type, you cannot select the Device All Ports check box. • Device start server port and Device end server port: Set Device start server port and device end server port, and the range is 1–65535.
Device Start Server Port	
Device End Server Port	

Step 4 Click **OK**, and the **Firewall** interface is displayed.

Step 5 Click **Save**.

5 Event

This chapter introduces intelligent event settings, including video detection, audio detection, smart plan, and abnormality.

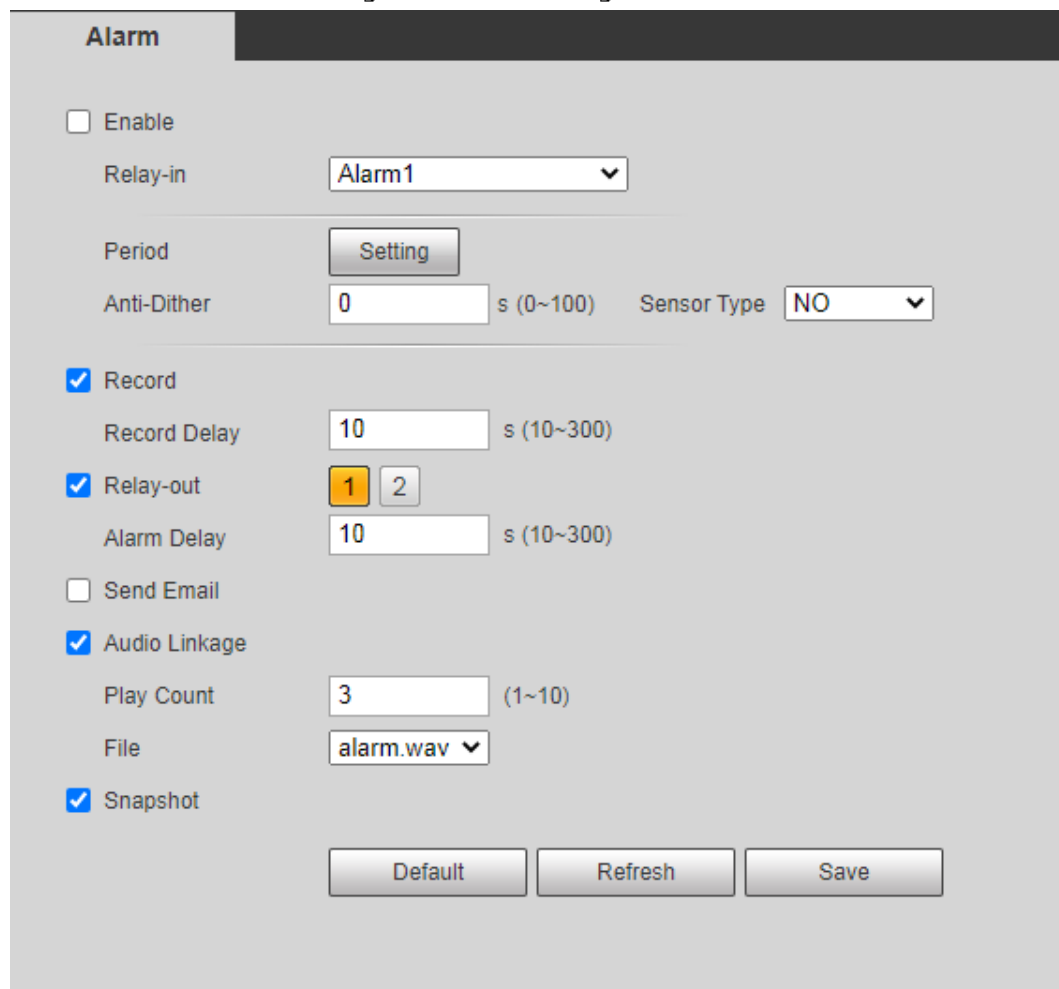
5.1 Setting Alarm Linkage

5.1.1 Alarm Linkage

When an alarm is triggered at the alarm-in port, the system performs alarm linkage. Interfaces might vary with different events, and the actual interface shall prevail.

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

Figure 5-1 Alarm linkage



Step 2 Select the **Enable** check box to enable the alarm linkage function.

Step 3 Select a relay-in port and a sensor type.

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

Step 4 Set arming periods and alarm linkage action. For details, see "5.1.1 Alarm Linkage".

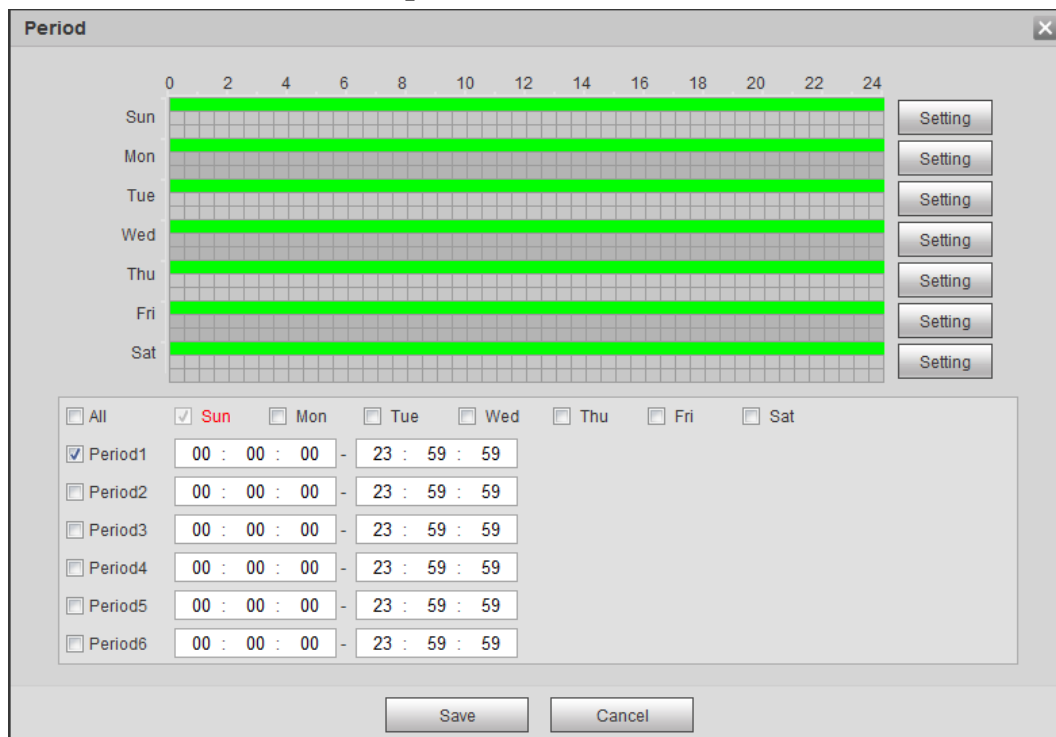
Step 5 Click **Save**.

5.1.1.1 Setting Period

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

Step 1 Click **Setting** next to **Period**.

Figure 5-2 Period



Step 2 Set arming periods. Alarms will be triggered in the time period in green on the timeline.

- Method one: Directly press and drag the left mouse button on the timeline.
- Method two: Enter an actual time period.
 1. Click **Setting** next to a day.
 2. Select a time period to be enabled.
 3. Enter start time and end time of a time period.



- ◇ Select **All** or check boxes of some days to set the time period of multiple days at one time.
- ◇ You can set 6 time periods per day.

Step 3 Click **Save**.

5.1.1.2 Record Linkage

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

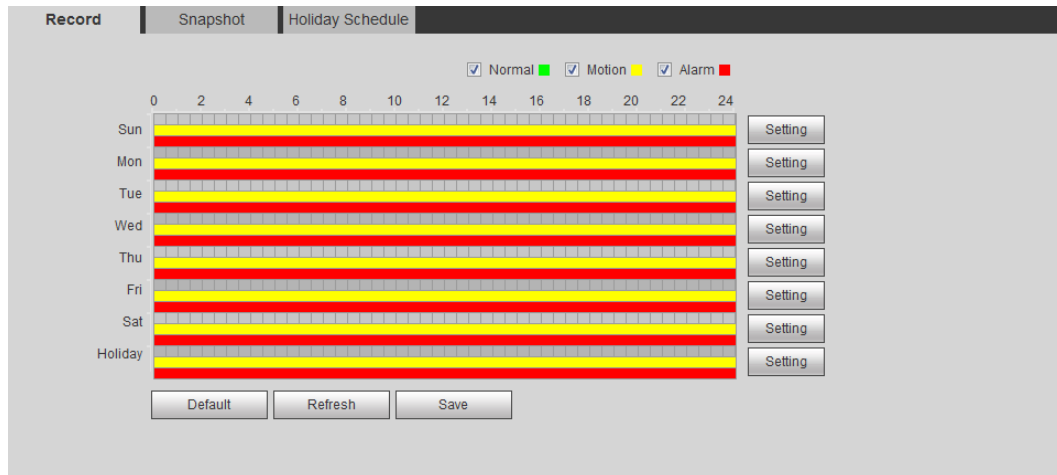
To use the record linkage function, set record plan for motion detection alarm and enable auto recording in record control.

5.1.1.2.1 Setting Record Plan

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

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

Figure 5-3 Record

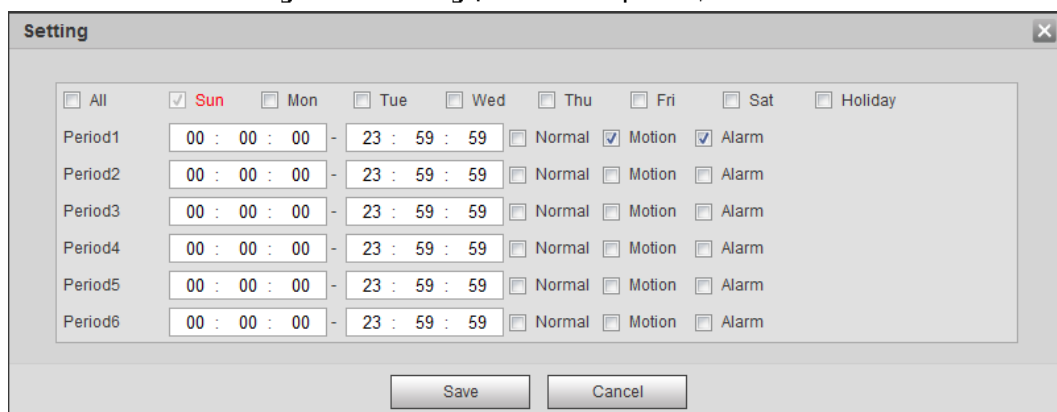


Step 2 Set record plan.

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

- Method one: Select a record type, such as **Normal**, and directly press and drag the left mouse button to set the time period for normal record on the timeline.
- Method two: Enter an actual time period.
 1. Click **Setting** next to a day.

Figure 5-4 Setting (record time period)



2. Select a day, and the alarm type next to a period, and then set the period.



- ◇ Select **All** or check boxes of some days to set the time period of multiple days at one time.
- ◇ You can set 6 time periods per day.

Step 3 Click **Save**.

5.1.1.2.2 Setting Record Control

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



Make sure that the SD card is authenticated before recording if you use Dahua smart card. For details, see "4.4.2.5 Path".

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

Figure 5-5 Record control

Step 2 Set parameters.

Table 5-1 Description of record control parameters

Parameter	Description
Pack Duration	The time for packing each video file.
Pre-event Record	The time to record the video in advance of a triggered alarm event. For example, if the pre-event record is set to be 5 s, the system saves the recorded video of 5 s before the alarm is triggered. When an alarm or motion detection links recording, and the recording is not enabled, the system saves the video data within the pre-event record time to the video file.
Disk Full	Recording strategy when the disk is full. <ul style="list-style-type: none"> • Stop: Stop recording when the disk is full. • Overwrite: Cyclically overwrite the earliest video when the disk is full.
Record Mode	When you select Manual , the system starts recording; when you select Auto , the system starts recording in the configured time period of record plan.
Record Stream	Select record stream, including Main Stream and Sub Stream .

Step 3 Click **Save**.

5.1.1.2.3 Setting Record Linkage

On the alarm event setting interface (such as the motion detection interface), select **Record** and set **Record Delay** to set alarm linkage and record delay.

After **Record Delay** is configured, alarm recording continues for an extended period after the alarm ends.

Figure 5-6 Record linkage

Record
 Record Delay s (10~300)

5.1.1.3 Snapshot Linkage

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

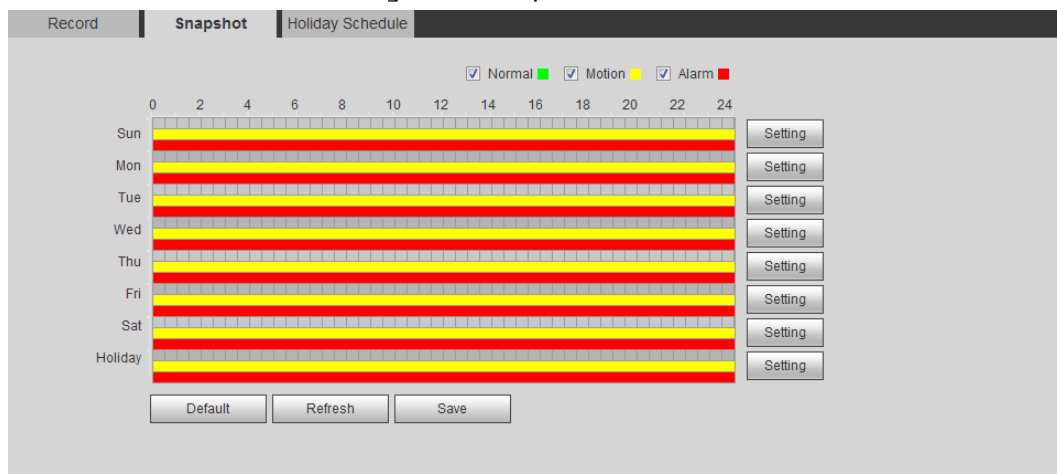
After **Motion** is enabled in **Snapshot**, the system takes snapshots when an alarm is triggered. For querying and setting snapshot storage location, see "4.4.2.5 Path".

5.1.1.3.1 Setting Snapshot Plan

According to the configured snapshot plan, the system enables or disables snapshot at corresponding time.

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

Figure 5-7 Snapshot

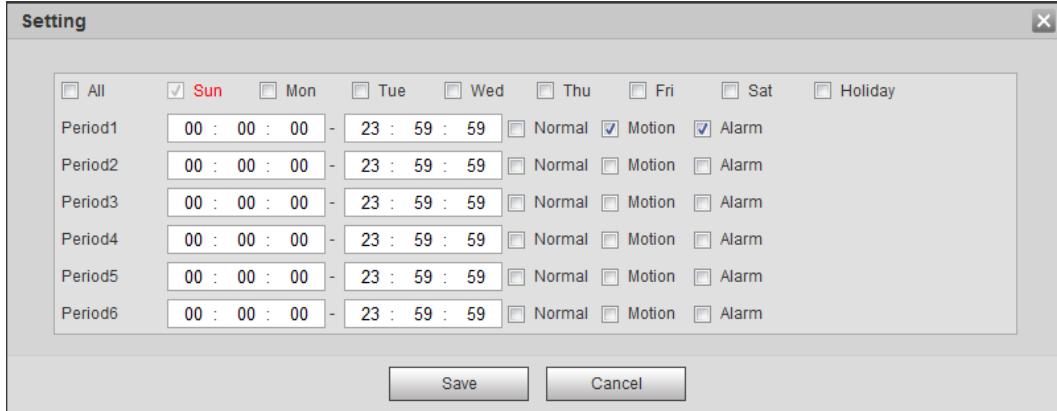


Step 2 Select snapshot type and set time period.

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

- Method one: Select snapshot type, such as **Normal**, and directly press and drag the left mouse button to set time period for normal snapshot on the timeline.
- Method two: Enter an actual time period.
 1. Click **Setting** next to a day.

Figure 5-8 Setting (snapshot time period)



2. Select a day, and the alarm type next to a period. Then set the period.



- ◇ Select **All** or check boxes of some days to set the time period of multiple days at one time.
- ◇ You can set 6 time periods per day.

3. You can set 6 time periods per day.
The **Snapshot** interface is displayed.

Step 3 Click **Save**.

5.1.1.3.2 Setting Snapshot Linkage

On the alarm event setting interface (such as the motion detection interface), select **Snapshot** and set alarm linkage snapshot.

Figure 5-9 Snapshot linkage



5.1.1.4 Relay-out Linkage

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

On the alarm event setting interface (such as the motion detection interface), select **Alarm** and set **Alarm Delay**.

When alarm delay is configured, alarm continues for an extended period after the alarm ends.

Figure 5-10 Relay-out linkage



5.1.1.5 Email Linkage

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

Email linkage takes effect only when SMTP is configured. For details, see "4.5.5 SMTP (Email)".

Figure 5-11 Email linkage



5.1.1.6 Audio Linkage

The system broadcasts alarm audio file when an alarm event occurs. Select **Setting > Camera > Audio > Alarm Audio** to set alarm audio file.

Figure 5-12 Audio linkage



5.1.2 Subscribing Alarm

5.1.2.1 About Alarm Types

For alarm types and preparations of alarm events, see Table 5-2.

Table 5-2 Description of alarm types

Alarm Type	Description	Preparation
Motion Detection	The alarm is triggered when moving object is detected.	Motion detection is enabled. For details, see "5.2.1 Setting Motion Detection".
Disk Full	The alarm is triggered when the free space of SD card is less than the configured value.	The SD card no space function is enabled. For details, see "5.8.1 Setting SD Card".
Disk Error	The alarm is triggered when there is failure or malfunction in the SD card.	SD card failure detection is enabled. For details, see "5.8.1 Setting SD Card".
Video Tampering	The alarm is triggered when the camera lens is covered or there is defocus in video images.	Video tampering is enabled. For details, see "5.2.2 Setting Video Tampering".
External Alarm	The alarm is triggered when there is external alarm input.	The device has alarm input port and external alarm function is enabled. For details, see #d1383e6a1026.
Illegal Access	The alarm is triggered when the number of consecutive login password error is up to the allowable number.	Illegal access detection is enabled. For details, see "5.8.3 Setting Illegal Access".
Audio Detection	The alarm is triggered when there is audio connection problem.	Abnormal audio detection is enabled. For details, see "5.4 Setting Audio Detection".
IVS	The alarm is triggered when intelligent rule is triggered.	Enable IVS, crowd map, face detection or people counting, and other intelligent functions.

Alarm Type	Description	Preparation
Scene Changing	The alarm is triggered when the device monitoring scene changes.	Scene changing detection is enabled. For details, see "5.2.3 Setting Scene Changing".
Voltage Detection	The alarm is triggered when the device detects abnormal voltage input.	Voltage detection is enabled. For details, see "5.8.4 Setting Voltage Detection".
Security Exception	The alarm is triggered when the device detects malicious attack.	Voltage detection is enabled. For details, see "5.8.5 Setting Security Exception".
Smoke Detector Alarm	The alarm is triggered when the device detects smoke.	Smoke detection is enabled. For details, see "5.7 Setting Smoke Alarm".

5.1.2.2 Subscribing Alarm Information

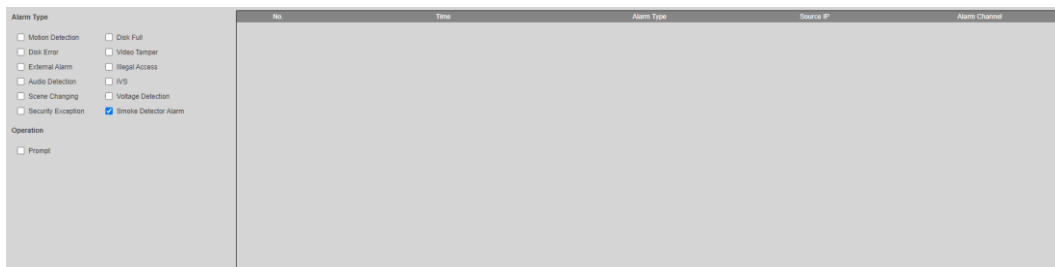
You can subscribe alarm event. When a subscribed alarm event is triggered, the system records detailed alarm information at the right side of the interface.




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

Step 1 Click the **Alarm** tab.

Figure 5-13 Alarm (subscription)



Step 2 Select **Alarm Type** according to the actual need.

- Select **Prompt**. The system prompts and records alarm information according to actual conditions.
 - ◇ When the subscribed alarm event is triggered and the **Alarm** interface is not displayed, the  is displayed on the **Alarm** tab and the alarm information is recorded automatically. Click the **Alarm** tab, and this icon disappears.
 - ◇ When the subscribed alarm event is triggered and the **Alarm** interface is displayed, the corresponding alarm information is displayed in the alarm list at the right side of the **Alarm** interface.
- Select **Play Alarm Tone**, and select the tone path.
The system would play the selected audio file when the selected alarm is triggered.

5.2 Setting Video Detection

Check whether there are considerable changes on the video by analyzing video images. In case of

any considerable change on the video (such as moving object, fuzzy image), the system performs an alarm linkage.

5.2.1 Setting Motion Detection

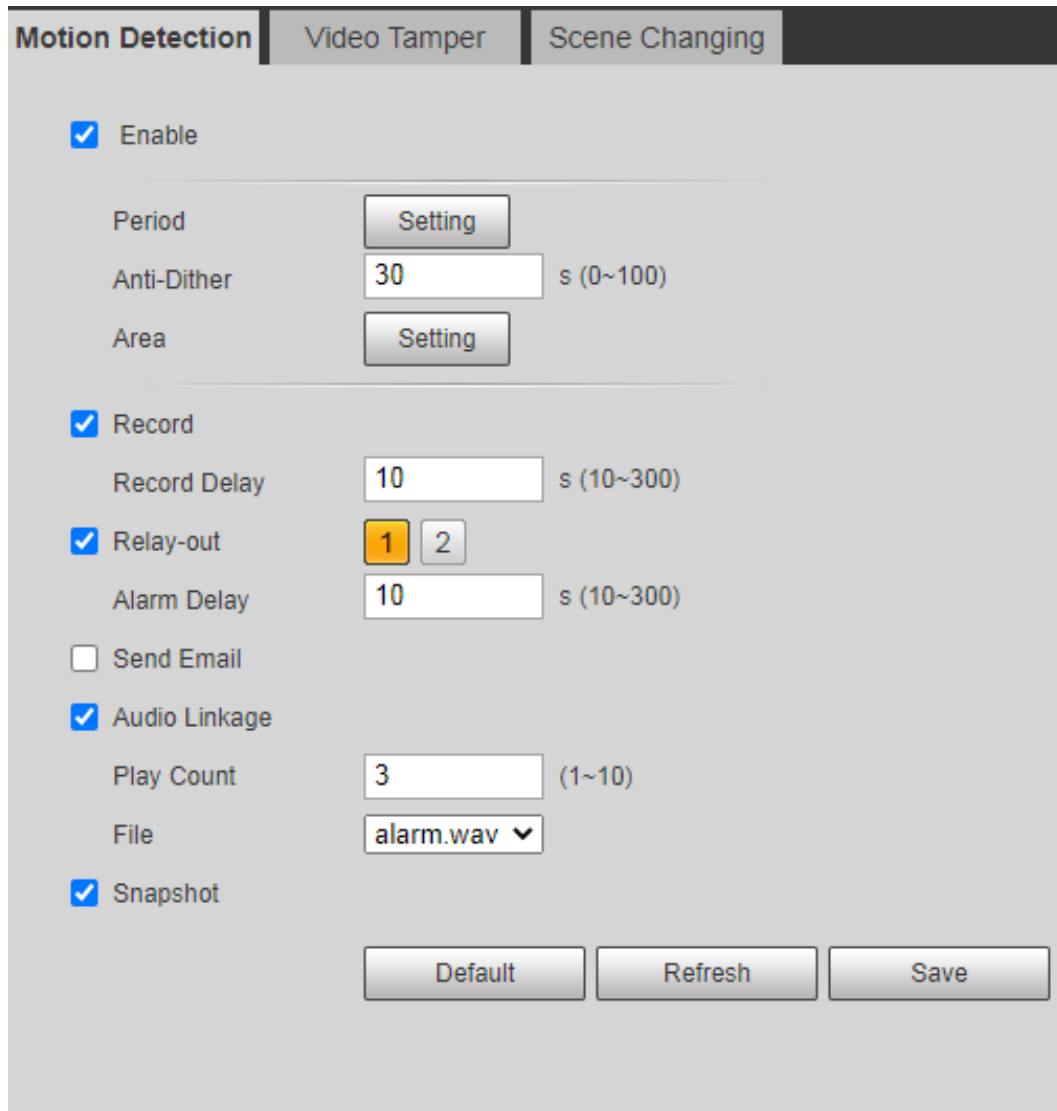
The system performs an alarm linkage when the moving object appears on the image and its moving speed reaches the preset sensitivity.



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

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

Figure 5-14 Motion detection



Motion Detection | Video Tamper | Scene Changing

Enable

Period

Anti-Dither s (0~100)

Area

Record

Record Delay s (10~300)

Relay-out

Alarm Delay s (10~300)

Send Email

Audio Linkage

Play Count (1~10)

File ▼

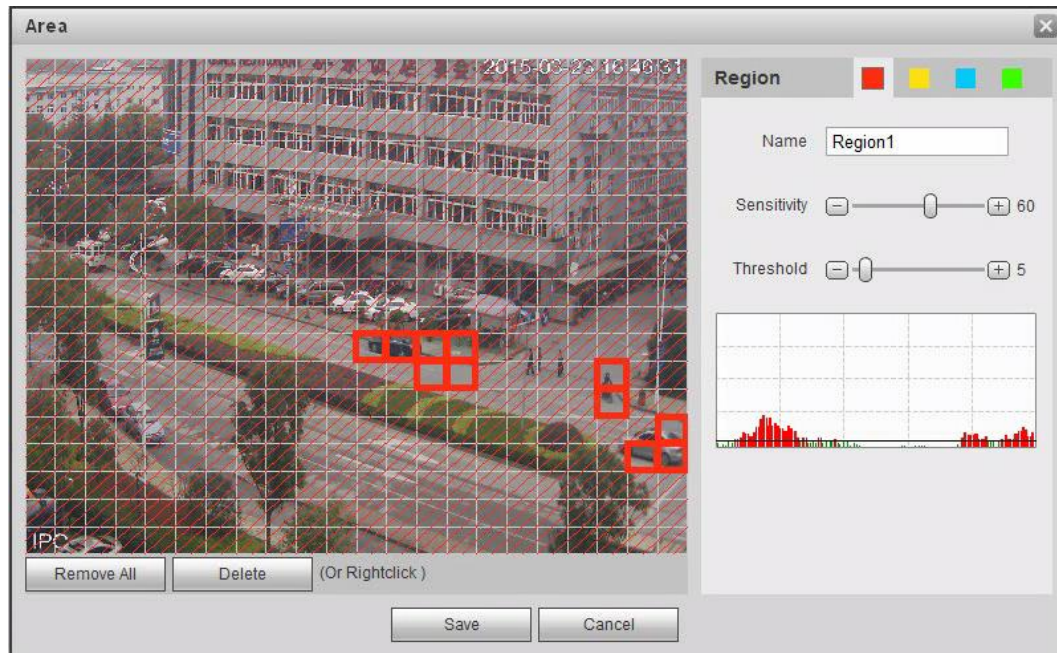
Snapshot

Step 2 Select the **Enable** check box to enable motion detection function.


Step 3 Set the area for motion detection.

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

Figure 5-15 Area



2) Select a color and set the region name. Select an effective area for Motion Detection in the image and set **Sensitivity** and **Threshold**.

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

3) Click **Save**.

Step 4 Set arming periods and alarm linkage action. For details, see "5.1.1 Alarm Linkage".
Anti-dither: After the **Anti-dither** time is set, the system only records one motion detection event in the period.

Step 5 Click **Save**.

5.2.2 Setting Video Tampering

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

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

Step 2 Select the event type.

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

function is available on some select models.

Figure 5-16 Video tampering

Table 5-3 Description of video temper parameter

Parameter	Description
Temper Area	When the percentage of the tampered image and the duration exceed the configured values, an alarm will be triggered. The tamper area is 30% and the duration is 5 s by default.
Duration	
Anti-Dither	Only record one alarm event during the anti-dither period.

Step 3 Set arming periods and alarm linkage action. For details, see "5.1.1 Alarm Linkage".

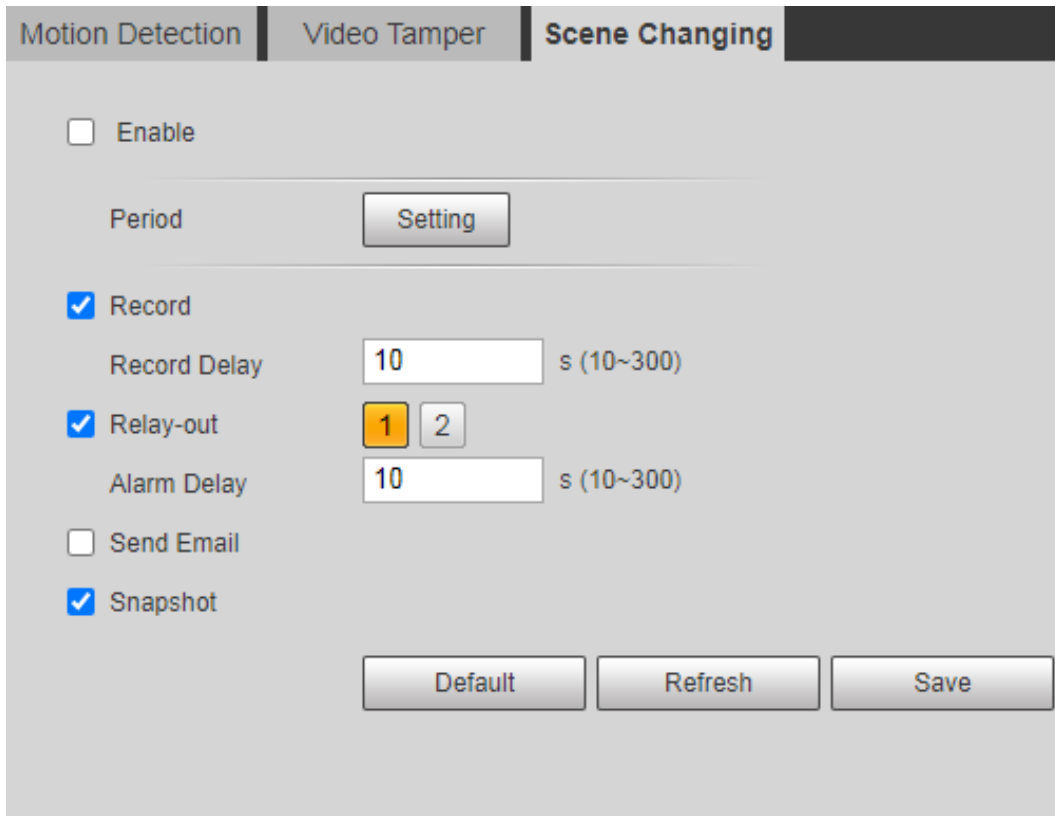
Step 4 Click **Save**.

5.2.3 Setting Scene Changing

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

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

Figure 5-17 Scene changing



Step 2 Set arming periods and alarm linkage action. For details, see "5.1.1 Alarm Linkage".

Step 3 Click **Save**.

5.3 Setting Smart Motion Detection

The system performs alarm linkage when human, non-motorized vehicle, or motor vehicle appear on the image and its moving speed reaches the preset sensitivity. Enabling smart motion detection can avoid the alarms triggered by the environment changes, and the function is enabled by default.

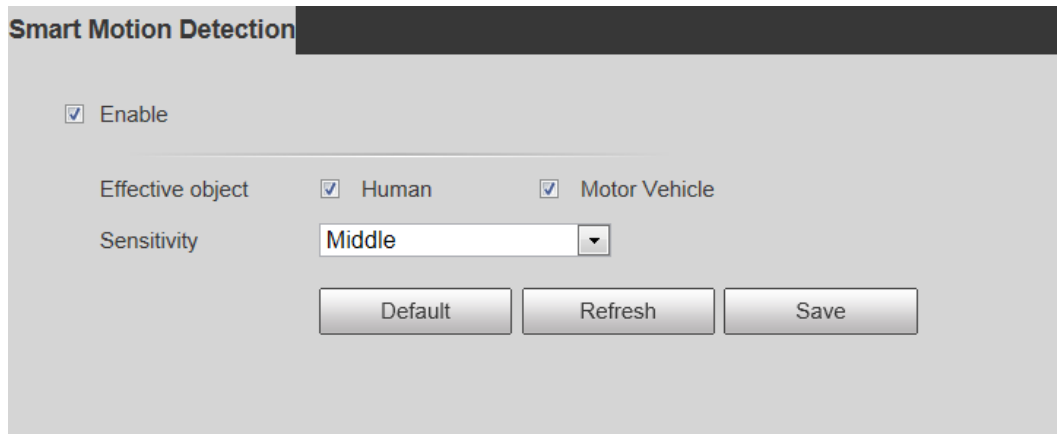
Prerequisites

- Select **Setting > Event > Video Detection > Motion Detection** to enable the motion detection function.
- You have set **Period** and **Area** in **Motion Detection**, and make sure that the sensitivity value is larger than 0, and the threshold value is smaller than 100.

Procedure

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

Figure 5-18 Smart motion detection



- Step 2** Select the **Enable** check box to enable the smart motion detection function.
- Step 3** Set effective object and sensitivity.
- Effective object: Includes **Human** and **Motor vehicle**. When you select **Human**, the camera will detect human and non-motorized vehicle.
 - Sensitivity: Includes **Low**, **Middle**, and **High**. The higher the sensitivity is, the easier the alarm will be triggered.
- Step 4** Click **OK**.

5.4 Setting Audio Detection

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

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

Figure 5-19 Audio detection

Audio Detection

Enable Input Abnormal

Enable Intensity Change

Sensitivity 50

Threshold 50

Working Period

Anti-Dither Second (0~100)

Record

Record Delay Second (10~300)

Relay-out

Alarm Delay Second (10~300)

Send Email

Snapshot

Step 2 Set parameters.

- Input abnormal: Select the **Enable Input Abnormal** check box, and the alarm is triggered when the system detects abnormal sound input.
- Intensity change: Select the **Enable Intensity Change** check box and then set **Sensitivity** and **Threshold**. The alarm is triggered when the system detects that the sound intensity exceeds the set threshold.
 - ◇ It is easier to trigger the alarm with higher sensitivity or smaller threshold. Set a high

threshold for noisy environment.

- ◇ The red line in the waveform indicates audio detection is triggered, and the green one indicates no audio detection. Adjust sensitivity and threshold according to the waveform.

Step 3 Set arming periods and alarm linkage action.

Step 4 Click **Save**.


5.5 Setting Smart Plan

Smart plan includes fire facilities, fire exits, flame detection and personal management. The intelligent function can be enabled only after the corresponding smart plan is enabled.

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


The **Smart Plan** interface is displayed. For smart plan icon, see Table 5-4.

Table 5-4 Description of smart plan icon

Icon	Description
	Flame Detection

Step 2 Enable smart functions as need.

Different cameras support different ways to enable smart functions. Select corresponding ways to enable these functions according to the actual interface.

- Select an icon to enable the corresponding smart plan.
Click an icon to enable it, and the selected smart function is highlighted. Click it again to cancel the selection.
If the icon  on the interface, click it to enable the smart function switch.
- Enable smart plan through **Add Plan**.
 1. Select a preset point from the **Add Plan** the interface.
The smart plan for the point is displayed.
 2. Click the corresponding icon to enable a smart function.
The selected smart function is highlighted. Click it again to cancel the selection.

Step 3 Click **Save**.

5.6 Setting Flame Detection

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


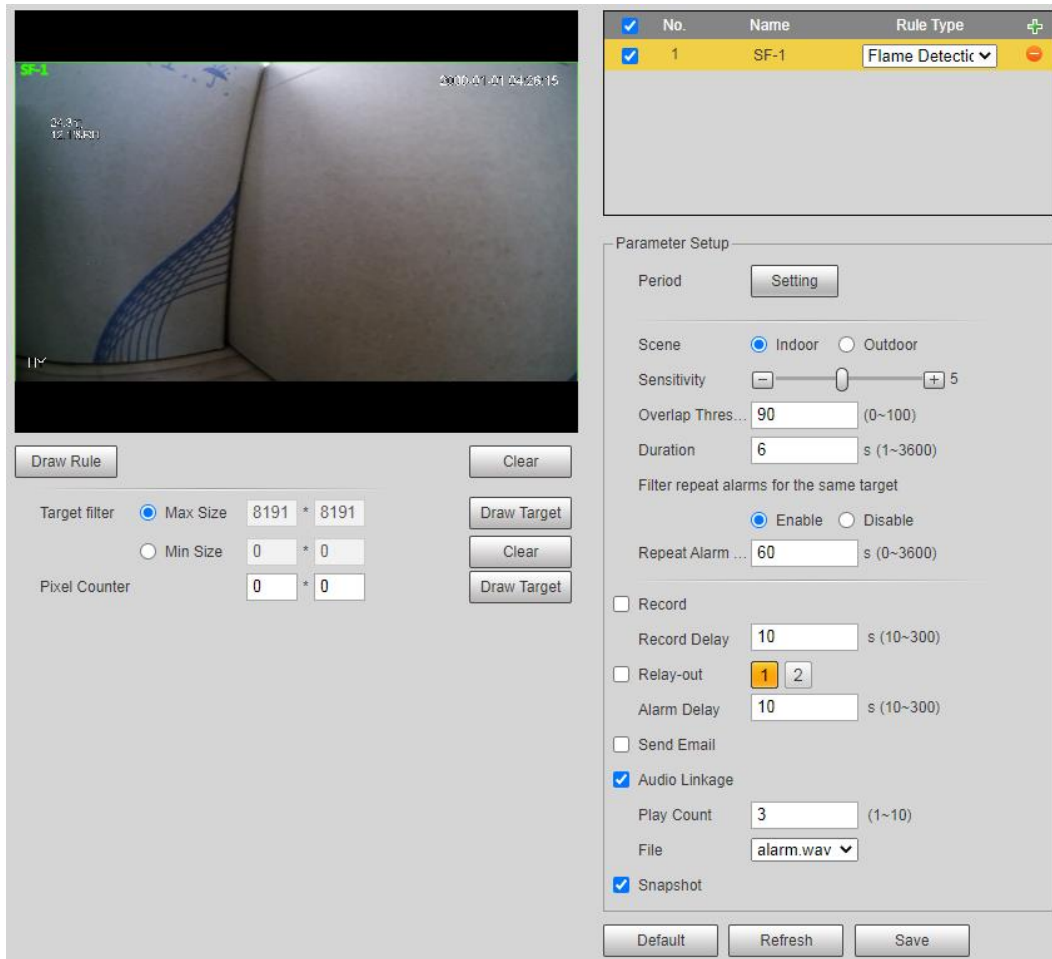
Step 2 Click  to add the flame detection function.

Figure 5-20 Flame Detection




Step 3 Double-click the name to modify the rule name.

Step 4 Select **Max Size** or **Min Size**, click **Draw Target** at the right side of **Target filter**, and then draw the target in the image.

Step 5 Set parameters.

Table 5-5 Description of flame detection parameters

Parameter	Description
Scene	Set scene as Indoor or Outdoor .
Sensitivity	Set the alarm-triggered sensitivity. The higher the sensitivity is, the easier the alarm will be triggered.
Overlap Threshold	Filter the stationary objects. The higher the threshold is, the less obvious the false alarm reduction will be and the easier the alarm will be triggered.
Duration	When the duration of flame in the detection area exceeds the configured value, the system performs an alarm linkage.
Filter repeat alarms	Enable this function, and the system automatically filters repeat alarms.
Repeat Alarm Time	After the alarm is triggered, if the status lasts for the configured time in Repeat Alarm Time , the alarm will be triggered again.  0 indicates that the function is disabled.

Parameter	Description
Record delay	After Record Delay is configured, alarm recording continues for an extended period after the alarm ends.
Relay-out	Select the Relay-out checkbox, and when alarm is triggered, the system interacts with the linked alarm devices.
Alarm delay	The Alarm linkage keeps running for the configured time after alarm is ended.
Send email	Click to enable email linkage function. When an alarm is triggered, the system will automatically send an email to users.
Audio linkage	Click to enable audio linkage function. The system broadcasts alarm audio file when an alarm event occurs.
Snapshot	Click to capture one picture of the current image, and it will be saved to the configured storage path.

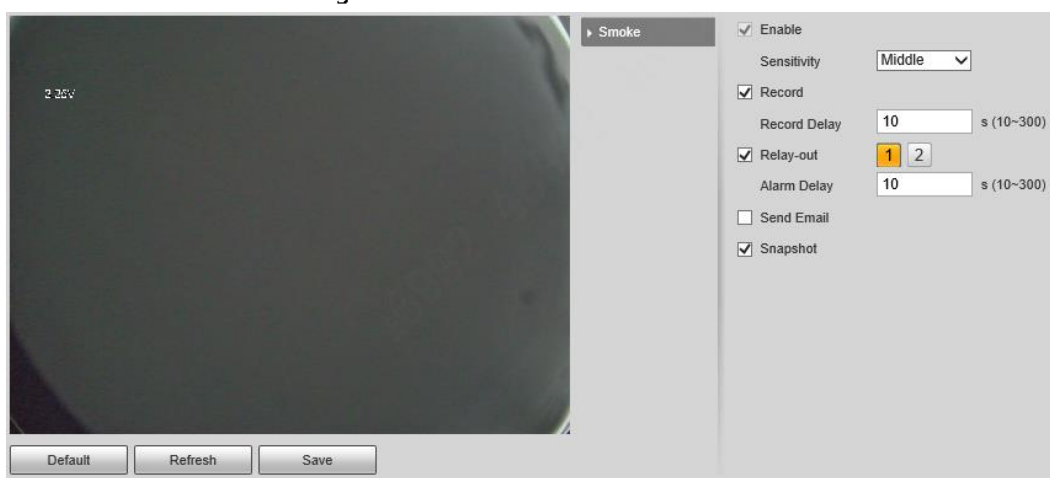
Step 6 Set arming periods and alarm linkage actions. For details, see "5.1.1 Alarm Linkage"

Step 7 Click **Save**.

5.7 Setting Smoke Alarm

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

Figure 5-21 Flame Detection



Step 2 Set parameters.

Table 5-6 Description of smoke alarm setting parameters

Parameter	Description
Sensitivity	Set the alarm-triggered sensitivity. The higher the sensitivity is, the easier the alarm will be triggered.
Record Delay	After Record Delay is configured, alarm recording continues for an extended period after the alarm ends.
Relay-out	Select the Relay-out checkbox, and when alarm is triggered, the system interacts with the linked alarm devices.
Alarm Delay	The Alarm linkage keeps running for the configured time after alarm is ended.

Parameter	Description
Send Email	Click to enable email linkage function. When an alarm is triggered, the system will automatically send an email to users.
Snapshot	Click to capture one picture of the current image, and it will be saved to the configured storage path.

Step 3 Click **Save**.

5.8 Setting Abnormality

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



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

5.8.1 Setting SD Card

In case of SD card abnormality, the system performs alarm linkage. The event types include **No SD Card**, **Capacity Warning**, and **SD Card Error**. Functions might vary with different models, and the actual interface shall prevail.

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

Figure 5-22 SD card

Step 2 Select the event type from the **Event Type** drop-down list, and then select the **Enable** check box to enable the SD card detection function.

When setting **Capacity Warning** as **Event Type**, set **Capacity Limit**. When the remaining space of SD card is less than this value, the alarm is triggered.

Step 3 Set alarm linkage actions. For details, see "5.1.1 Alarm Linkage".

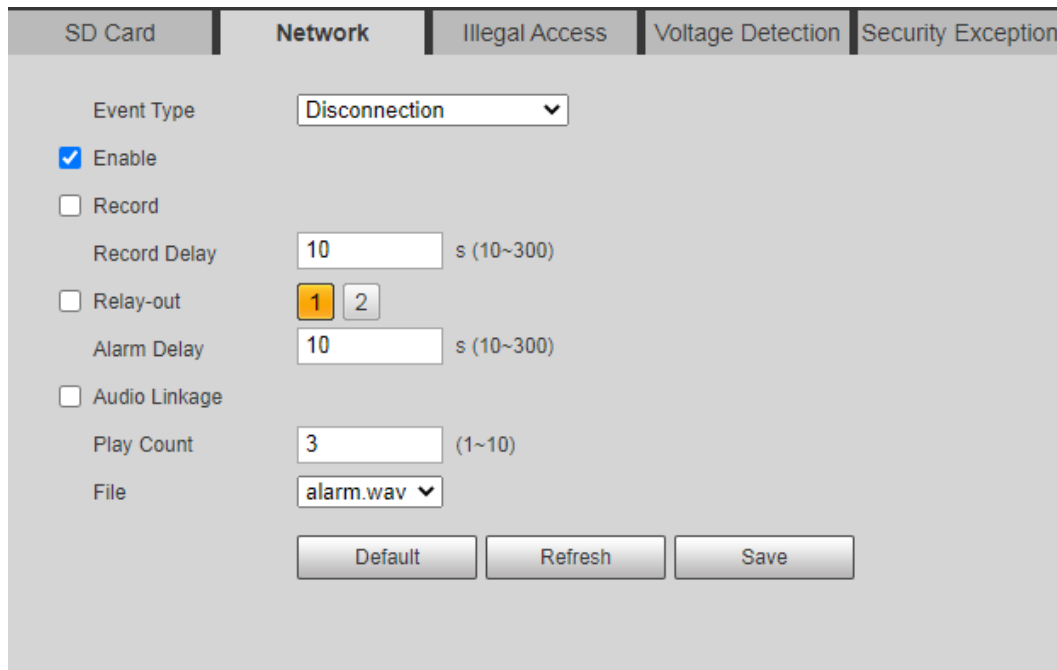
Step 4 Click **Save**.

5.8.2 Setting Network

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

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

Figure 5-23 Network



SD Card	Network	Illegal Access	Voltage Detection	Security Exception
Event Type: Disconnection				
<input checked="" type="checkbox"/> Enable				
<input type="checkbox"/> Record				
Record Delay: 10 s (10~300)				
Relay-out: 1 2				
Alarm Delay: 10 s (10~300)				
<input type="checkbox"/> Audio Linkage				
Play Count: 3 (1~10)				
File: alarm.wav				
Default Refresh Save				

Step 2 Select the event type from the **Event Type** drop-down list, and then select the **Enable** check box to enable the network detection function.

Step 3 Set alarm linkage actions. For details, see "5.1.1 Alarm Linkage".

Step 4 Click **Save**.

5.8.3 Setting Illegal Access

When you enter a wrong login password more than the set times, the system performs alarm linkage.

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

Figure 5-24 Illegal access



- Step 2** Select the **Enable** check box to enable the illegal access detection function.
- Step 3** Set **Login Error**.
If you consecutively enter a wrong password more than the set value, the account will be locked.
- Step 4** Set alarm linkage actions. For details, see "5.1.1 Alarm Linkage".
- Step 5** Click **Save**.

5.8.4 Setting Voltage Detection

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

- Step 1** Select **Setting > Event > Abnormality > Voltage Detection**.

Figure 5-25 Voltage detection

- Step 2** Select the **Enable** check box to enable the voltage detection function.
Select **Overlay**, and the alarm icon is displayed by overlapping when the alarm is triggered.
 indicates undervoltage and  indicates overvoltage.
- Step 3** Set alarm linkage actions. For details, see "5.1.1 Alarm Linkage".
- Step 4** Click **Save**.

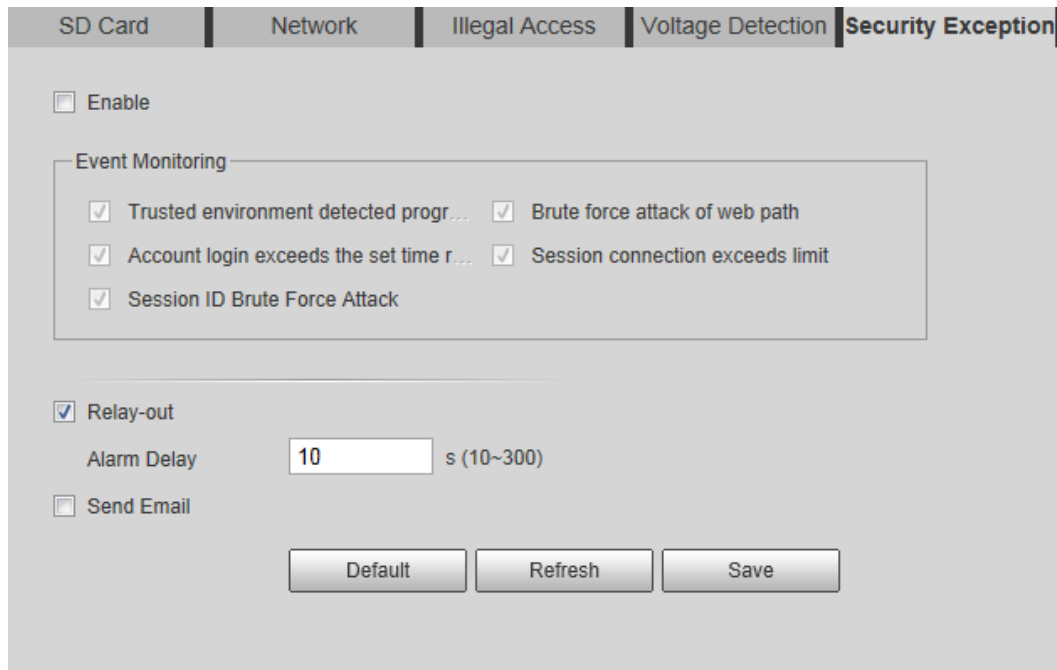
5.8.5 Setting Security Exception

When a hostile attack is detected, the system performs alarm linkage.

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

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

Figure 5-26 Security exception



Step 3 Select the event to be monitored as needed.

Table 5-7 Security exception description

Parameter	Description
Trusted environment detected program	Monitors the programs that run in trusted environment to detect whether there are program running without trusted signature. Select it to prevent the program with trojan and virus.
Account login exceeds the set time range	The account tries to login during the period that does not allow user to log in. Configure Restricted Login in Setting > System > Account > Account > Username , including the IP address, validity period, and time range.
Session ID Brute Force Attack	When sessionid false reaches the configured threshold in the defined period, an alarm will be triggered. Select it to monitor attacks in real time, so that attacks can be prevented timely.
Brute force attack of web path	Generates the web serve directory and send a request through enumeration. When URL false reaches the configured threshold in the defined period, an alarm will be triggered. Select it to monitor attacks in real time, so that attacks can be prevented timely.

Parameter	Description
Session connection exceeds limit	The number of users (web, platform or mobile phone client) exceeds the max number of users that can connect to the device simultaneously. Configure the Max Connection in Setting > Network > Port .

Step 4 Set alarm linkage actions. For details, see "5.1.1 Alarm Linkage".

Step 5 Click **Save**.

5.8.6 Setting Disarming

You can disable the linkage actions through the app on your smart phone, and then the system will not perform any linkage action, but alarm records will still be generated.

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

Figure 5-27 Disarming

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

Step 3 (Optional) Select the **Enable** check box next to **Disarm by Period** to enable the Disarm by Period function, and then you can disarm by period. For setting disarm period, see "5.1.1.1 Setting Period".



This function is only valid when **Disarming** is disabled.

Step 4 Select alarm linkage actions as needed.

Step 5 Click **Save**.

6 Maintenance

6.1 Requirements

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

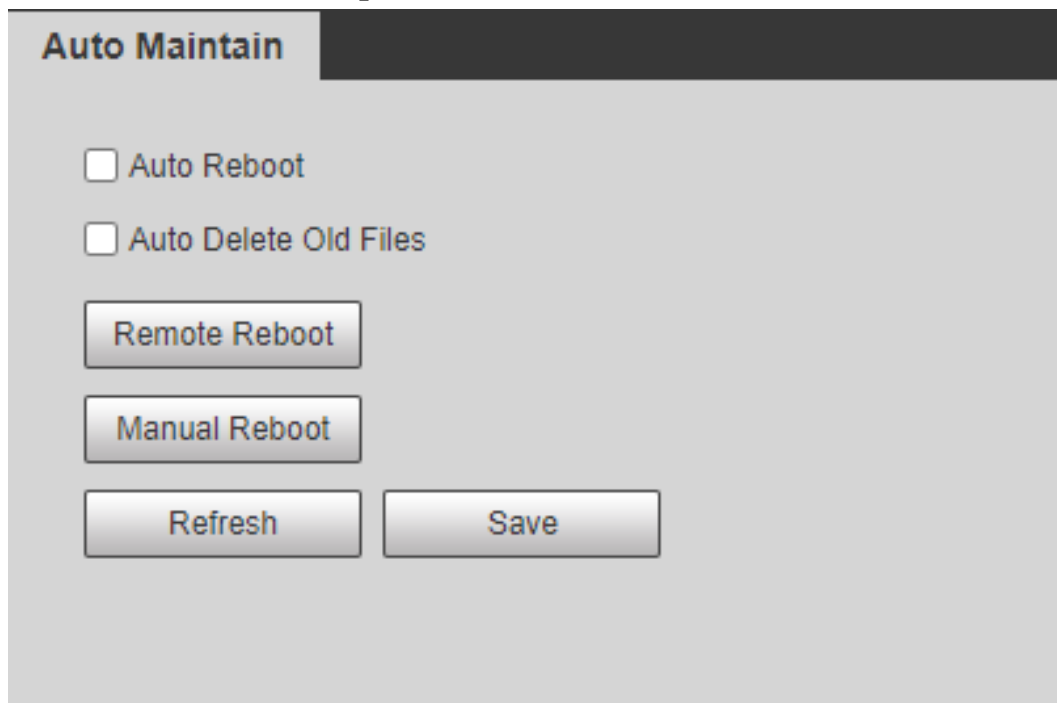
- Check surveillance images regularly.
- Clear regularly user and user group information that are not frequently used.
- Modify the password every three months. For details, see "4.7.3 Account".
- View system logs and analyze them, and process the abnormality in time.
- Back up the system configuration regularly.
- Restart the device and delete the old files regularly.
- Upgrade firmware in time.

6.2 Auto Maintain

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

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

Figure 6-1 Auto maintain



Step 2 Configure auto maintain parameters.

- Select the **Auto Reboot** check box, and set the reboot time, the system automatically restarts as the set time every week.
- Select the **Auto Delete Old Files** check box, and set the time, the system automatically deletes old files as the set time. The time range is 1 to 31 days.



When you enable and confirm the **Auto Delete Old Files** function, The **The deleted files cannot be restored, are you sure?** notice is displayed. Operate it carefully.

- Click **Manual Reboot**, and then click **OK** on the displayed interface, the camera will restart.

Step 3 Click **OK**.

6.3 Resetting Password

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

Prerequisites

You have enabled password reset service. For details, see "4.7.4.1 System Service".

Procedure

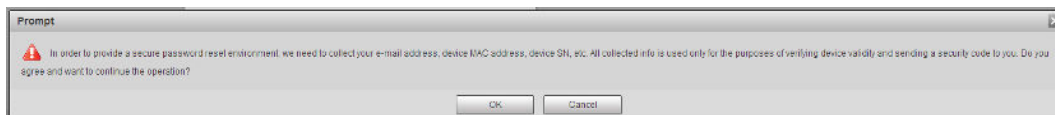
Step 1 Open IE browser, enter the IP address of the device in the address bar and press Enter.

Figure 6-2 Login



Step 2 Click **Forgot password?**

Figure 6-3 Prompt

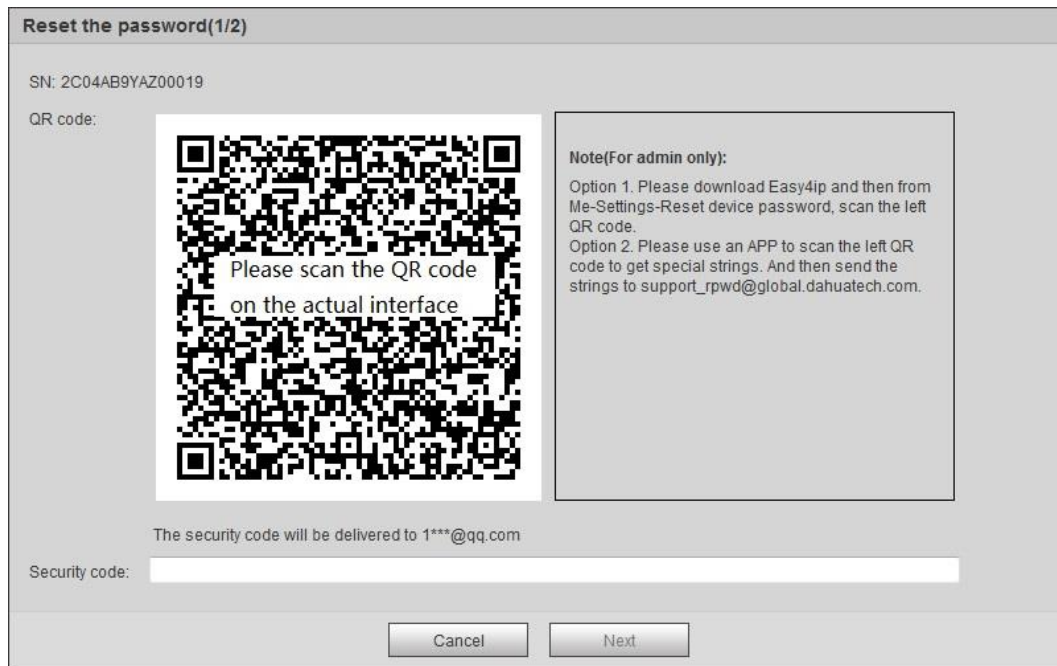


Step 3 Click **OK**.



Clicking **OK** means that you are informed that some of your personal data might be collected to help reset the password, such as phone number, MAC address, and device serial number. Read the prompt carefully to decide whether to authorize the collection activity.

Figure 6-4 Reset the password (1)



Step 4 Reset the password.

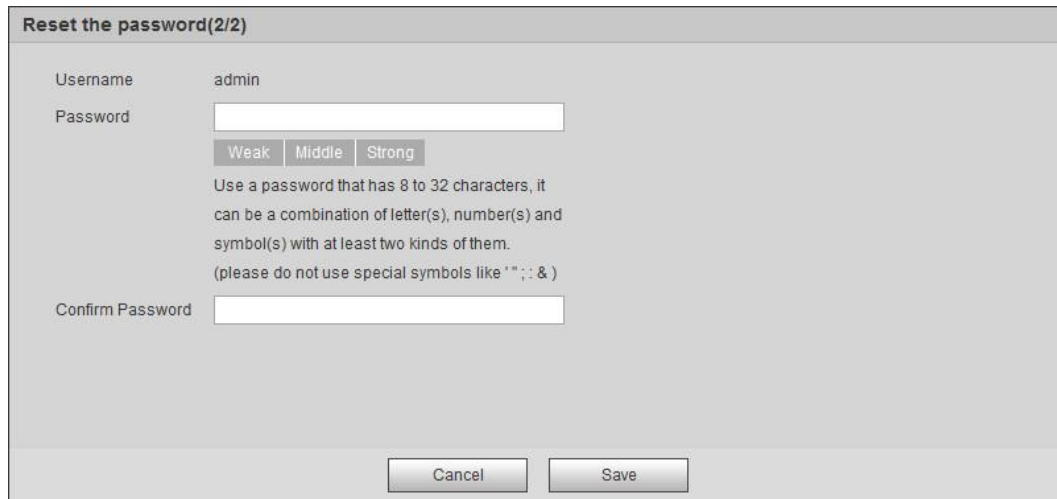
Step 5 Scan the QR code, and there will be a security code sent to the email address you entered. Enter the security code as instructed.



- Please use the security code within 24 hours after you receive it. Otherwise, it will become invalid.
- If you fail to use the security code for two times continuously, there will be fail notice when you try to get a security code for the third time. You have to reset the device to get a security code or wait 24 hours to get it again.

Step 6 Click **Next**.

Figure 6-5 Reset the password (2)



Step 7 Reset and confirm the password.

The password must consist of 8 to 32 non-blank characters and contain at least two types of characters among upper case, lower case, number, and special character (excluding ' " ; ; &).

Step 8 Click **Save**.

The login interface is displayed.

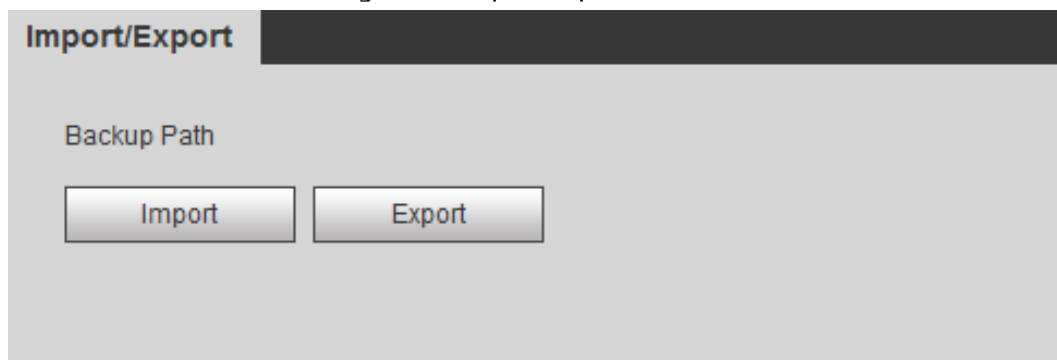
6.4 Backup and Default

6.4.1 Import/Export

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

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

Figure 6-6 Import/Export



Step 2 Click **Import** or **Export**.

- Import: Select local configuration file, and click **Open** to import the local system configuration file to the system.
- Export: Select the storage path, and click **Save** to export the system configuration file to local storage.

Step 3 Click **Save** to finish configuration.

6.4.2 Default

Restore the device to default configuration or factory settings.

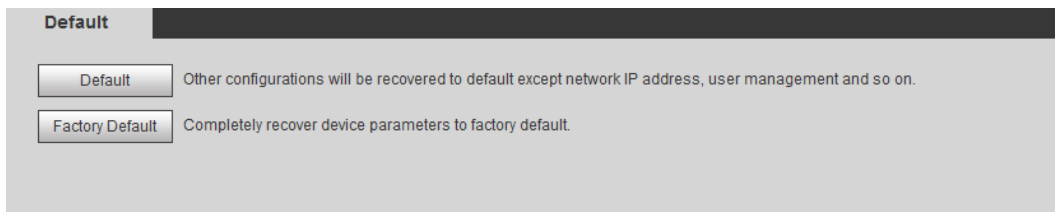


This function will restore the device to default configuration or factory setting.

Select **Setting > System > Default**.

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

Figure 6-7 Default



6.5 Upgrade

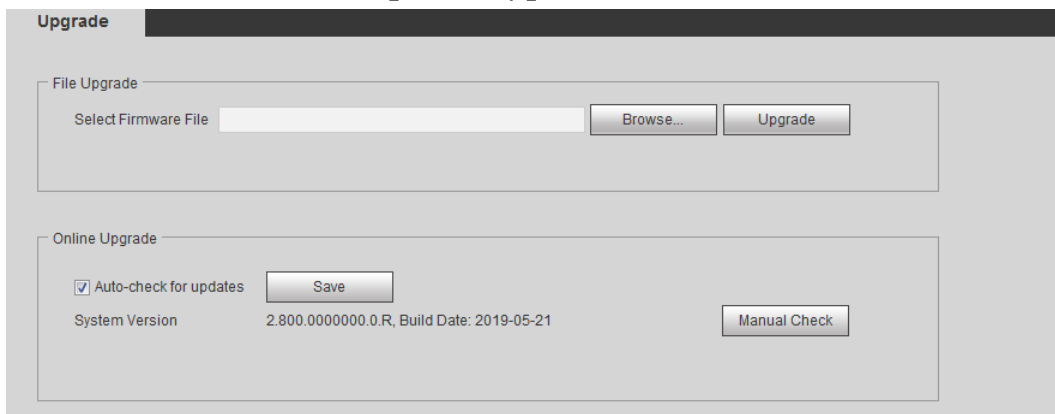
Upgrading to the latest system can perfect camera functions and improve stability.



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

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

Figure 6-8 Upgrade



Step 2 Select upgrading method according to the actual needs.

- File Upgrade
 1. Click **Browse**, and then upload upgrade file.
 2. The upgrade file should be a .bin file.
 3. Click **Upgrade**.
The upgrade starts.
- Online Upgrade
 1. Select the **Auto-check for updates** check box.

The system checks for upgrade once a day automatically, and there will be system notice if any upgrade is available.



We need to collect the data such as device name, firmware version, and device serial number to proceed auto-check. The collected information is only used for verifying the legality of cameras and upgrade notice.

2. If there is any upgrade available, click **Upgrade**, and then the system starts upgrading.



Click **Manual Check** to check for upgrade manually.

6.6 Information

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

6.6.1 Version

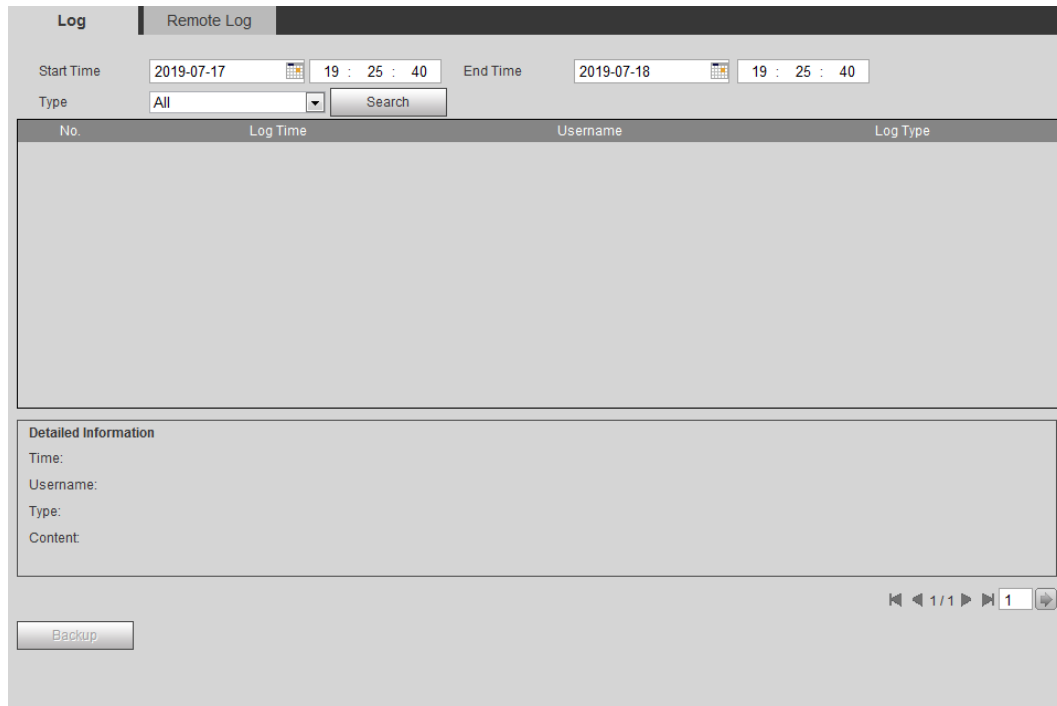
You can view device information such as hardware, system version, and web version.
Select **Setting > Information > Version** to view the version information.

6.6.2 Log

You can view and back up logs.

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

Figure 6-9 Log



- Step 2** Configure **Start Time** and **End Time**, and then select the log type.
 The start time should be later than January 1st, 2000, and the end time should be earlier than December 31, 2037.
 The log type includes All, System, Setting, Data, Event, Record, Account, and Safety.
- **System:** Includes program start, abnormal close, close, program reboot, device closedown, device reboot, system reboot, and system upgrade.
 - **Setting:** Includes saving configuration and deleting configuration file.
 - **Data:** Includes configuring disk type, clearing data, hot swap, FTP state, and record mode.
 - **Event** (records events such as video detection, smart plan, alarm and abnormality): includes event start and event end.
 - **Record:** Includes file access, file access error, and file search.
 - **Account:** Includes login, logout, adding user, deleting user, modifying user, adding group, deleting group, and modifying group.
 - **Safety:** Includes password resetting and IP filter.
- Step 3** Click **Search**.
- Click a certain log, and then you can view the detailed information in **Detailed Information** area.
 - Click **Backup**, and then you can back up all found logs to local PC.

Figure 6-10 Log (details)

The screenshot shows the 'Log' interface with the 'Remote Log' tab selected. At the top, there are filters for 'Start Time' (2019-07-17 19:25:40) and 'End Time' (2019-07-18 19:25:40). Below these is a 'Type' dropdown set to 'All' and a 'Search' button. A status bar indicates 'Find 72 log Time 2019-07-17 19:55:03 -- 2019-07-18 19:01:11'.

No.	Log Time	Username	Log Type
1	2019-07-18 19:01:11	admin	Set Time
2	2019-07-18 19:01:11	admin	Set Time
3	2019-07-18 18:58:51	admin	Set Time
4	2019-07-18 18:56:30	admin	Login
5	2019-07-18 18:17:41	admin	Logout
6	2019-07-18 18:01:11	admin	Set Time
7	2019-07-18 18:01:11	admin	Set Time
8	2019-07-18 17:58:51	admin	Set Time
9	2019-07-18 17:31:36	admin	Set Time
10	2019-07-18 17:31:36	admin	Set Time

Below the table is a 'Detailed Information' section with fields for Time, Username, Type, and Content. At the bottom right, there are navigation arrows and a page indicator '1 / 1'. A 'Backup' button is located at the bottom left.

6.6.3 Remote Log

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

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

Figure 6-11 Remote Log

The screenshot shows the 'Remote Log' configuration interface. It features a 'Log' tab and a 'Remote Log' sub-tab. The main configuration area includes:

- An 'Enable' checkbox, which is currently unchecked.
- An 'IP Address' field with a dropdown menu.
- A 'Port' field containing the value '514' and a range indicator '(1~65534)'.
- A 'Device Number' field containing the value '22' and a range indicator '(0~23)'.
- Three buttons at the bottom: 'Default', 'Refresh', and 'Save'.

Step 2 Select the **Enable** check box to enable remote log function.

Step 3 Set address, port and device number.

Step 4 Click **Save**.

6.6.4 Online User

View all the current users logging in to web.

Select **Setting > Information > Online User**.

Figure 6-12 Online user

No.	Username	User Local Group	IP Address	User Login Time
1	admin	admin	192.168.1.1	2020-01-14 15:02:04

Refresh

Appendix 1 Cybersecurity Recommendations

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

Mandatory actions to be taken for basic equipment network security:

1. Use Strong Passwords

Please refer to the following suggestions to set passwords:

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

2. Update Firmware and Client Software in Time

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

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

1. Physical Protection

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

2. Change Passwords Regularly

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

3. Set and Update Passwords Reset Information Timely

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

4. Enable Account Lock

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

5. **Change Default HTTP and Other Service Ports**

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

6. **Enable HTTPS**

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

7. **MAC Address Binding**

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

8. **Assign Accounts and Privileges Reasonably**

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

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

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

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

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

10. **Audio and Video Encrypted Transmission**

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

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

11. **Secure Auditing**

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

12. **Network Log**

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

13. **Construct a Safe Network Environment**

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

- Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.
- The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.

- Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.
- Enable IP/MAC address filtering function to limit the range of hosts allowed to access the device.

ENABLING A SAFER SOCIETY AND SMARTER LIVING

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.

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

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