Visual Radar WEB

User's Manual

Foreword

General

This manual introduces the functions and operations of the Visual Radar (hereinafter referred to as "the radar").

Model

DH-PFR5QI-E60, DH-PFR5QI-E60-PV.

Safety Instructions

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

Signal Words	Meaning
⚠ WARNING	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
⚠ CAUTION	Indicates a potential risk which, if not avoided, could result in property damage, data loss, lower performance, or unpredictable result.
🔑 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 Time
V1.0.0	First release.	September 2020

About the Manual

- The manual is for reference only. If there is inconsistency between the manual and the actual product, the actual product shall prevail.
- We are not liable for any loss caused by the operations that do not comply with the manual.
- The manual would be updated according to the latest laws and regulations of related jurisdictions. For detailed information, refer to the paper manual, CD-ROM, QR code or our official website. If there is inconsistency between paper manual and the electronic version, the electronic version shall prevail.
- All the designs and software are subject to change without prior written notice. The product updates might cause some differences between the actual product and the manual. Please contact the customer service for the latest program and supplementary documentation.

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

Important Safeguards and Warnings

This chapter introduces the contents covering proper handling of the product, hazard prevention, and prevention of property damage. Read these contents carefully before using the product, comply with them when using, and keep the manual well for future reference.

Environmental Requirement

- As for ground within the monitoring area, hard ground like concrete ground is optimal. As for ground covered by vegetation, vegetation height should be below 20 cm.
- Make sure that there is no vegetation, buildings and vehicles within the monitoring area that hinder the work of the radar.
- Make sure that there is no electromagnetic interference like air conditioner exterior units and transformers around where the radar is installed.
- Transport, use and store the radar within permitted temperature range and humidity level.
- Don't put the radar in humid, dusty, extremely hot or cold, and intense electromagnetic radiation places.
- Pack the radar with packaging provided by its manufacturer or packaging with the same quality before transporting it.
- Don't press hard, violently vibrate, and soak the radar when transporting, storing, and installing it.

Power Source Requirement

- Strictly comply with the local electric safety standards.
- Make sure that the power supply is correct before operating the Illuminator.
- The power source shall conform to the requirement of the Safety Extra Low Voltage (SELV) standard, and supply power with rated voltage which conforms to Limited power Source requirement according to IEC60950-1. Note that the power supply requirement is subject to the device label.
- Install easy-to-use device for power off before installing wiring, which is for emergent power off when necessary.
- Protect the power supply wires from treading and pressing with great force, especially wires around the holes where the plug and outlet are threaded through.

Maintenance

- Don't spray paint, stick stickers, put colors and any other objects or smudges on the surface of the radar; otherwise the performance of the radar will be greatly influenced.
- Don't disassemble the radar, for there are no components inside that can be repaired by users. Disassembling may result in water leaks.
- Clean the surface of the radar with a soft dry cloth. If there are stains, clean the surface with a soft cloth dipped in neutral detergent, and then dry the surface. Don't use detergent with strong abrasiveness and volatile solvents like ethyl alcohol, benzene, and diluent; otherwise the coating on the surface will be damaged and the performance of the radar will

be degraded.

⚠️

- Use accessories suggested by the manufacturer, and install and maintain the radar by professional personnel.
- Don't provide two or more than two kinds of power supply modes; otherwise, the radar may be damaged.

Table of Contents

1 Product Overview

1.1 General

There are mainly two connection methods between the radar and PC. See Figure 1-1 and Figure 1-2. The IP address of the radar is 192.168.1.108 by default. Use IP segment reasonably according to actual network environment so that the radar can connect to network.
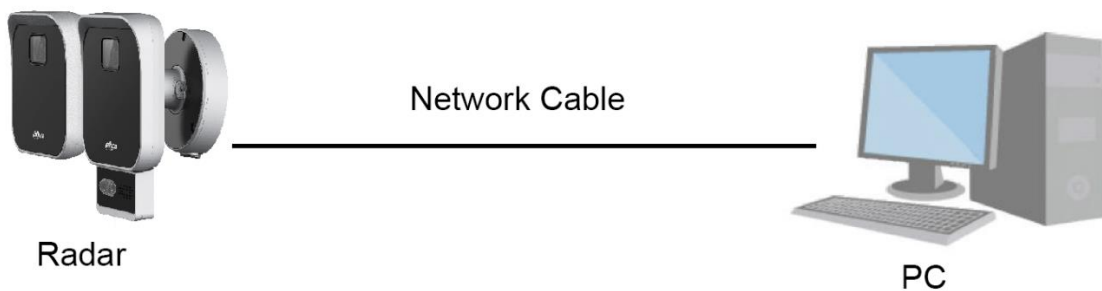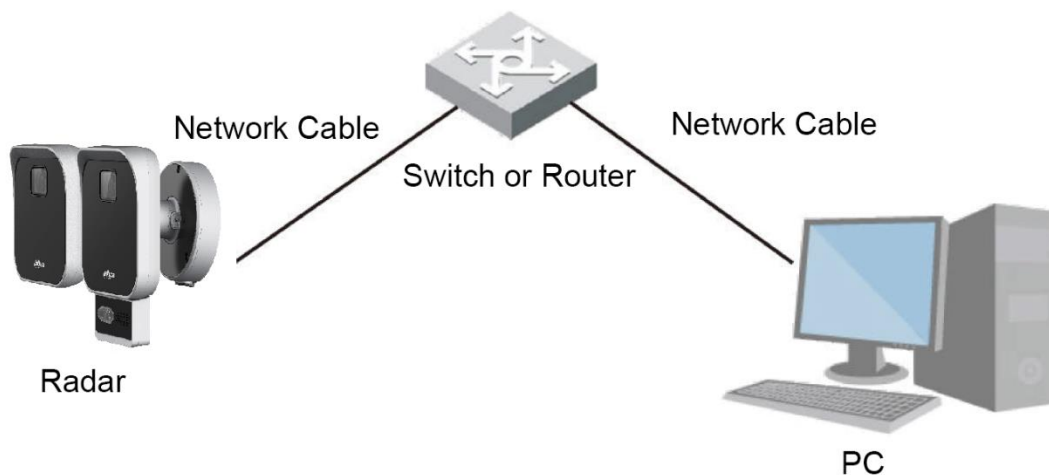
Figure 1-1 Connected by network cable

Figure 1-2 Connected through router or switch

1.2 Functions

1.2.1 Basic Functions

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 abnormalities.
- Snapshot and triple snapshot to capture abnormalities of the monitoring image for

subsequent view and processing.
- Record abnormalities 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, change and delete user group, and manage user authorities according to user group.
- Add, change and delete user, and configure user authorities.
- Change user password.

1.2.2 Intelligent Functions

Alarm

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

Alarm Setting

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

Abnormality

- SD card error, network disconnection, illegal access, and security exception.
- When SD card error or illegal access is detected, the system links alarm output and sending email.
- When network disconnection alarm is triggered, the system links recording and alarm output.

2 Network Configuration

2.1 Device Initialization

The radar needs to be initialized for the first-time use or after restoring to factory defaults.

<u>Step 1</u> Open IE browser, enter the IP address of the radar in the address bar, and then press the Enter key.

Figure 2-1 Device initialization

<u>Step 2</u> Set the password.

The password should consist of 8 to 32 non-blank characters and contain at least two types of characters among upper case, lower case, number, and special characters (excluding ' " ; : &). Make sure that the password and the confirmed password are the same. Follow the password strength prompt to set a password with high security.

<u>Step 3</u> (Optional) Set the email address which is used to reset password.

We recommend you to enter the email address to guarantee normal use of the radar.

<u>Step 4</u> On the End-User License Agreement interface, select **I have read and agree to all terms** check box, and then click **Next**.

Figure 2-2 End-user license agreement
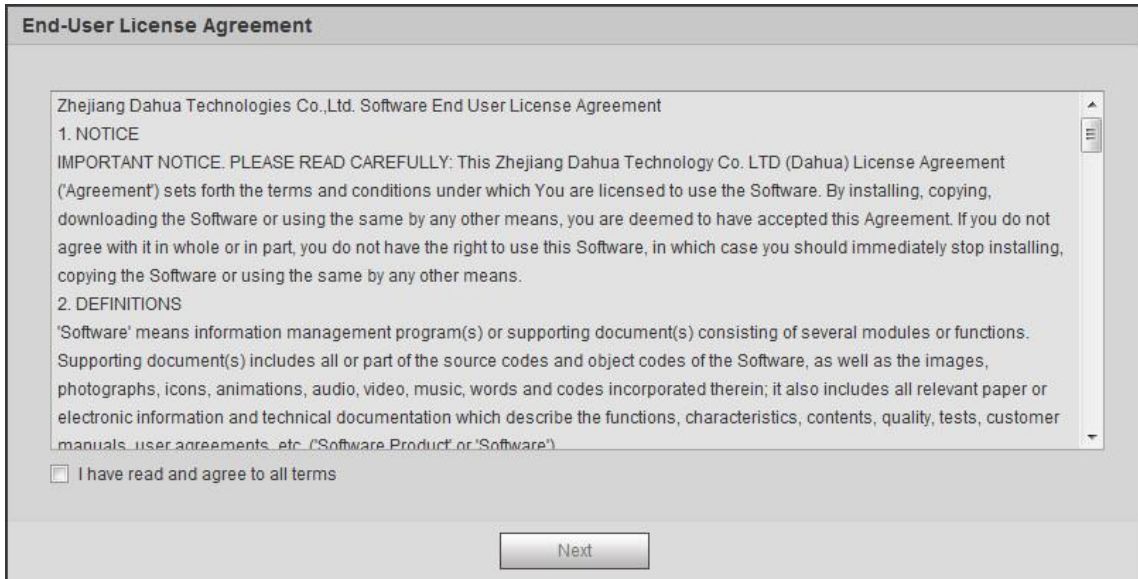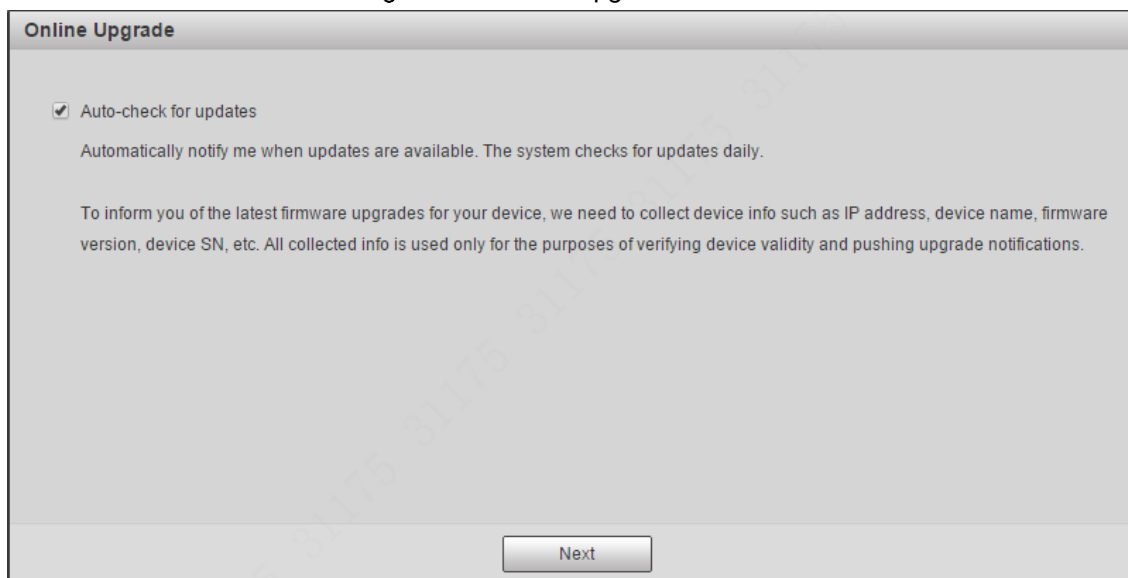
Step 5　On the P2P interface, select **P2P**, and then click **Next**.

Figure 2-3 P2P

Step 6　Select **Auto-check for updates** check box as needed, and then click **Next** to complete initialization.

Figure 2-4 Online Upgrade
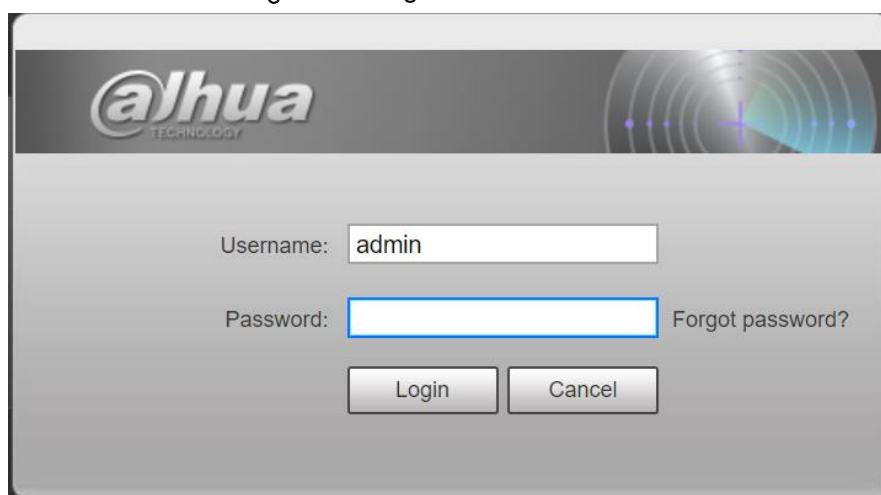
2.2 Logging in to the Web Interface

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

Step 1　Enter username and password, and then click **Login**.

Figure 2-5 Login interface

- The default username is admin, and the password is the one set during initialization.
- If you enter the wrong password for continuously 5 times, the account will be locked for 5 minutes. After the locked time ends, you can log in to the radar again.
- You can set the allowed wrong password times in **Setting > Event > Abnormality > Illegal Access**.

Step 2　After successful login, download and install the plug-in according to the prompt.

Figure 2-6 Installing the plug-in
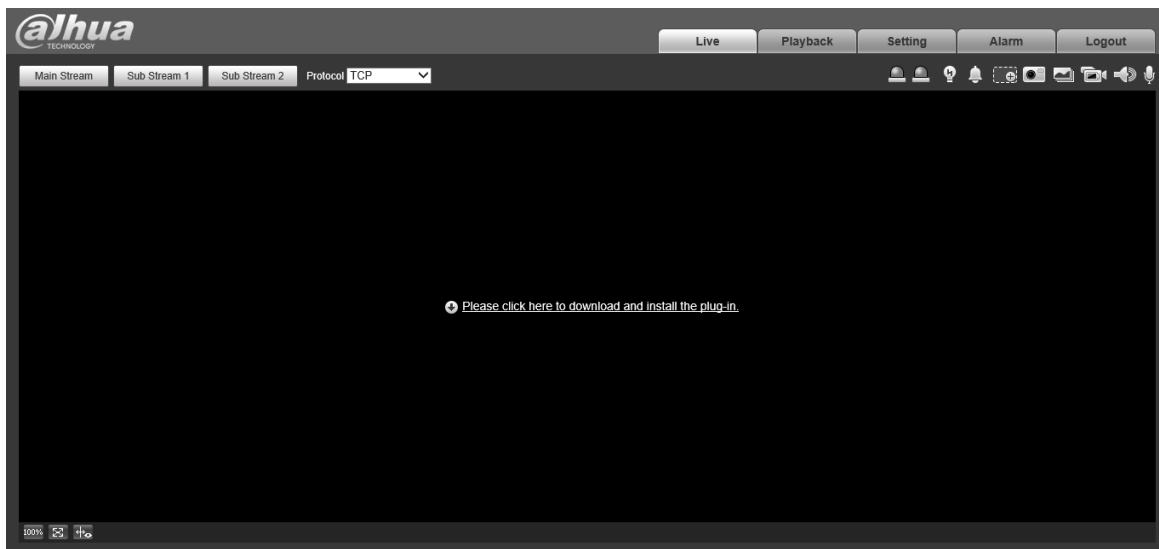
Step 3   After the plug-in is installed, the login interface is displayed automatically. Enter
username and password again, and then click **Login**. The **Live** interface is displayed.

Figure 2-7 Live view
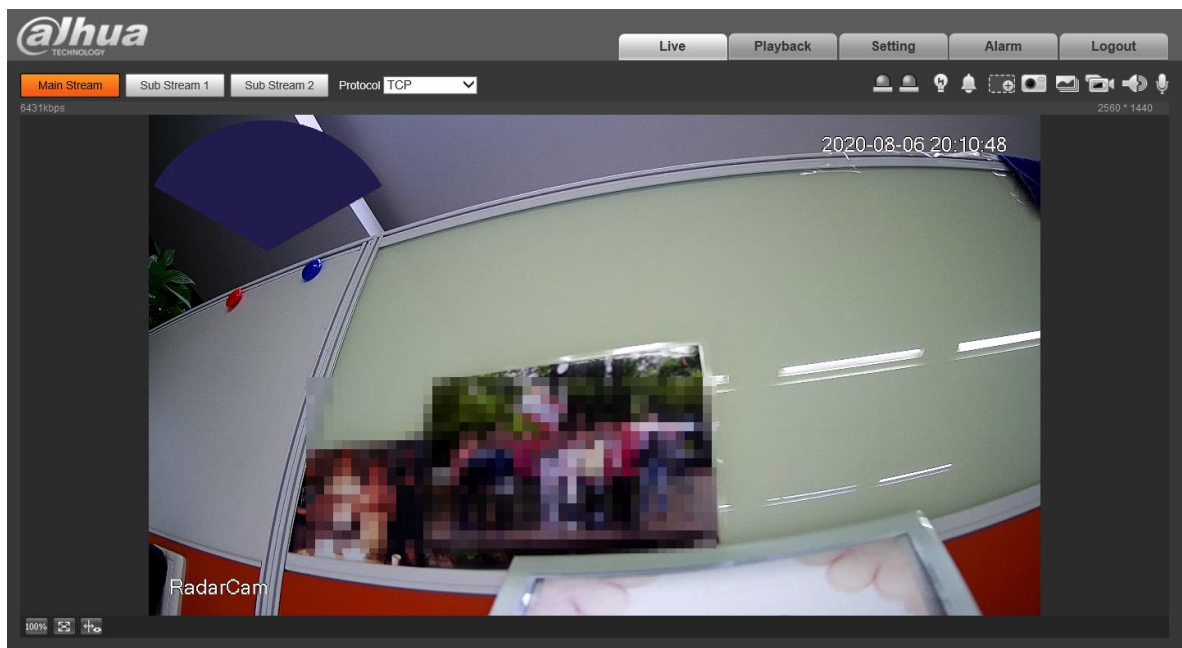
- **Live**: To view the real-time monitoring image.
- **Playback**: Play back or download recorded video or image files. When playing back multi-
channel images or recordings, you can choose channel No. to play back.
- **Setting**: Configure the basic and intelligent functions of the device. For the device with
multiple channels, through selecting channel No., you can set the parameters of different
channels.
- **Alarm**: Subscribe and view alarm information.
- **Logout**: Log out and go to login interface. The system will sleep automatically after idling
for a period of time.
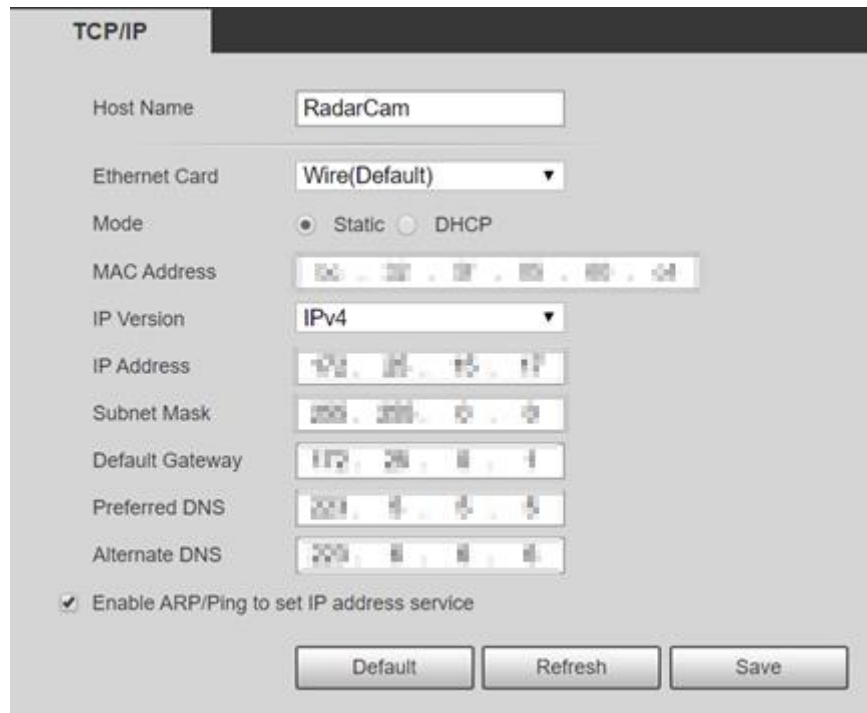
2.3 Changing IP Address

To ensure that the radar can be connected to the network, set an appropriate IP address.

<u>Step 1</u> On the web interface, select **Setting > Network > TCP/IP**.

<u>Step 2</u> Configure IP related parameters, and then click **Save**.

Figure 2-8 TCP/IP

3 Basic Configuration

3.1 Live

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

3.1.1 Live Interface

Figure 3-1 Live interface
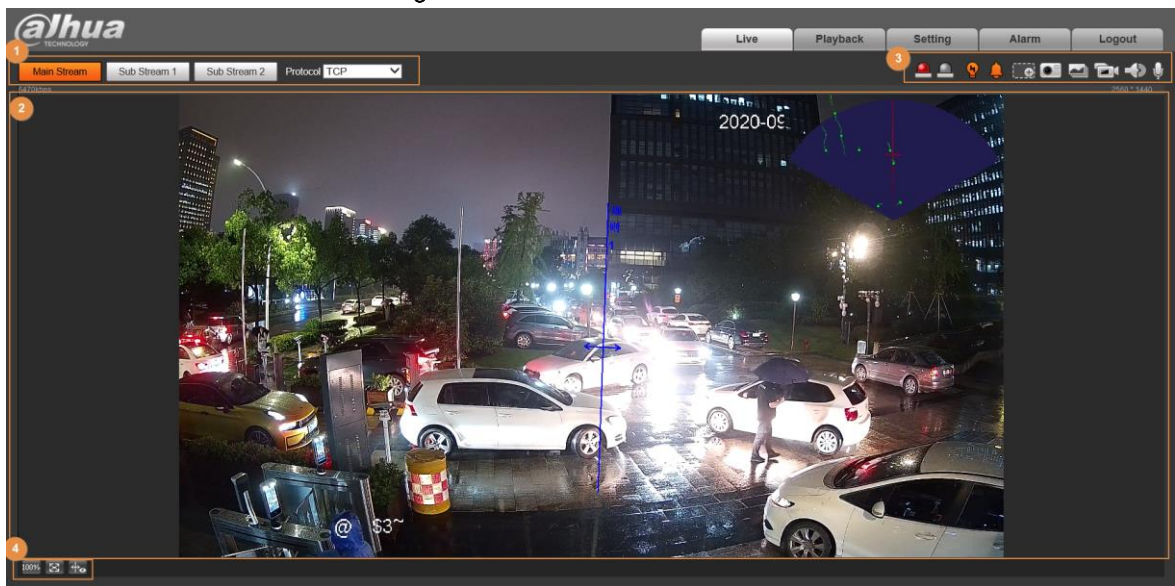
Table 3-1 Live interface description

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

3.1.2 Encode bar

Operations on encode bar:

Figure 3-2 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.
- **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.
- **Protocol**: You can select the network transmission protocol as needed, and the options are

TCP, **UDP** and **Multicast**.

3.1.3 Function Bar

Figure 3-3 Function bar

Table 3-2 Description of function bar

No.	Function	Description
1	Relay-out	Displays alarm output state. Click to enable or disable alarm output. ● Red: Alarm output enabled. ● Grey: Alarm output disabled.
2	Warning Light	: Off. : On. When an alarm rule (alarm, early warning, tripwire) is triggered, the warning light is on. The light turns off when alarm is ended.
3	Alarm Speaker	When an alarm is triggered, the icon turns yellow and the corresponding audio is played. Click the icon to manually play the defined alarm audio. Some models support recording or uploading alarm audio file. For alarm audio settings, see "3.3.3.2 Configuring Alarm Audio" for details.
4	Digital Zoom	Click the icon, and then select an area in the video image to zoom in; right-click on the image to restore the original size. In zoom-in state, drag the image to check other areas.
5	Snapshot	Click to capture one picture of the current image, and it will be saved to the configured storage path. About viewing or changing storage path, see "3.3.2.4 Path".
6	Triple Snapshot	Click the icon to capture three pictures of the current view (1 pic per second), and they will be saved to the configured storage path. About viewing or changing storage path, see "3.3.2.4 Path".
7	Record	Click to record video, and it will be saved to the configured storage path.

No.	Function	Description
		📖 About viewing or changing storage path, see "3.3.2.4 Path".
8	Audio	Click to enable or disable audio output.
9	Talk	Click to enable or disable audio talk.

3.1.4 Window Adjustment Bar

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

Figure 3-4 Adjusting device image

Table 3-3 Description of adjustment bar

No.	Function	Description
1	Original Size	Click to display the original video size.
2	Full Screen	Click to enter full screen mode; double-click or press Esc to exit.
3	Rule Info	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.

3.2 Playback

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

📖

● Before playing back video, ensure that you have inserted the SD card and configured record plan, record storage method, record schedule and record control. For details, see "5.1.1.3.1 Configuring Record Plan" and "5.1.1.3.2 Configuring Record Control".
● Before playing back picture, configure snapshot plan. For details, see "5.1.1.4.1 Configuring Snapshot Plan".

3.2.1 Playback Interface

Click the **Playback** tab, and the **Playback** interface is displayed. The video playback and picture playback interface layout are different, see Figure 3-5 and Figure 3-6. For details, see Table 3-4.

Figure 3-5 Video playback
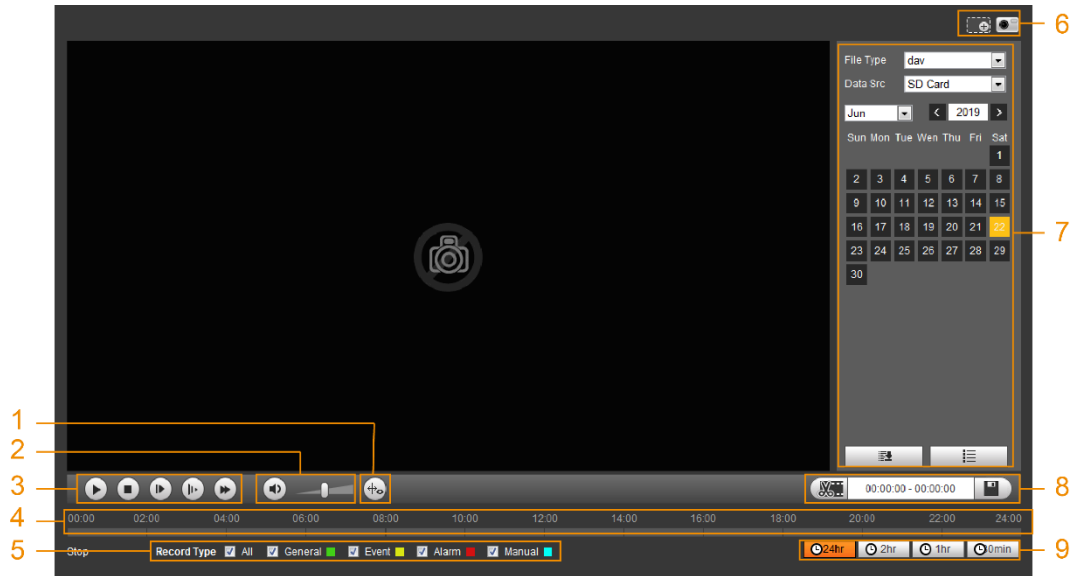
Figure 3-6 Picture playback
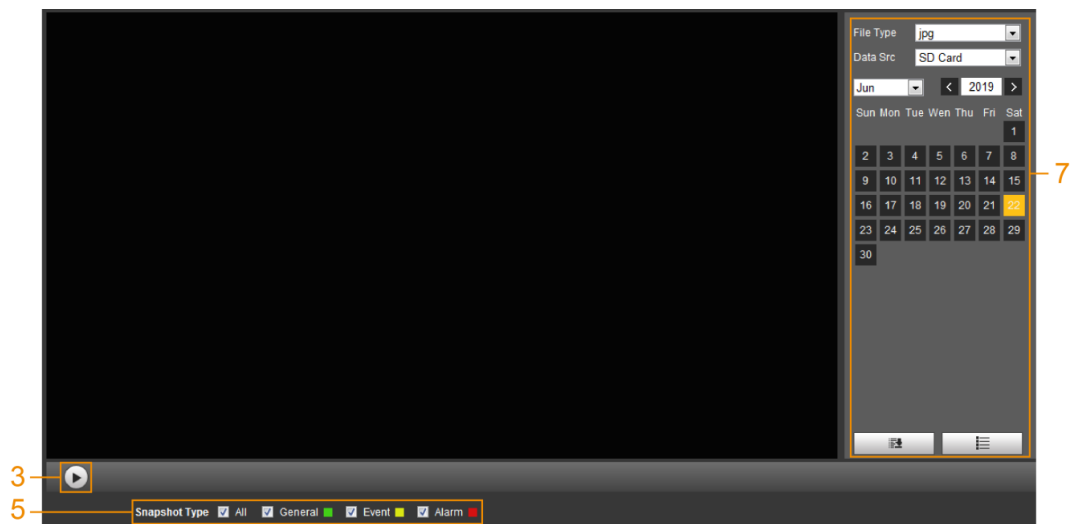
Table 3-4 Playback interface description

No.	Function	Description
1	Rule Info	Click to display the smart rules and object detection box on the live view interface. It is enabled by default. Rules Info is valid only when you enabled the rule during recording.
2	Sound	Controls the sound during playback.

No.	Function	Description
3	Play Control Bar	Controls playback. ![play icon]: Click to play. ![stop icon]: Click to stop playing. ![next frame icon]: Click to play the next frame. ![note icon] You need to pause the playback before using play by frame. ![slow icon]: Click to slow down the playback. ![fast icon]: Click the icon to speed up the playback.
4	Progress Bar	Displays the record type and the corresponding period. ● 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, see relations in **Record Type**.
5	Record/Snapshot Type	Select the record type or snapshot type. ● Record type includes **General**, **Event**, **Alarm**, and **Manual**. ● Snapshot type includes **General**, **Event**, and **Alarm**.
6	Assistant	● ![zoom icon]: Zoom video image of the selected area through two operations. ◇ 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. ◇ Click the icon, and then scroll the mouse wheel in the video image to zoom in or out. ● ![camera icon]: Click the icon to capture one picture of the current video, and it will be saved to the configured storage path. ![note icon] For viewing or changing storage path, see "3.3.2.4 Path".
7	Playback Video	You can select file type, data source and record date and downloaded files.
8	Video Clip	Clip a certain recorded video and save it. For details, see "3.2.3 Clipping Video".
9	Time Format of Progress Bar	Includes 4 time formats: ![24hr], ![2hr], ![1hr], and ![30min].

3.2.2 Playing Back Video or Picture

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

<u>Step 1</u> Select **dav** from the **Record Type** drop-down list when playing back videos.

Select **jpg** from **Record Type** drop-down list when playing back pictures. The data source is **SD card** by default.

Figure 3-7 File type selection

File Type	dav ▼
Data Src	SD Card ▼
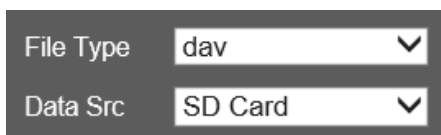
<u>Step 2</u> Select the record type in **Record Type**.

Figure 3-8 Specific event types (video)

Record Type ☑ All ☑ General ▪ ☑ Event ▪ ☑ Alarm ▪ ☑ Manual ▪

<u>Step 3</u> Select the month and year of the video that you want to play.

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

<u>Step 4</u> Play video.

- Click ▶ in the control bar. The system plays the recorded video of the selected date (in chronological order).

- Click any point in the colored area on the progress bar. The playback starts from that moment.

Figure 3-9 Progress bar

| 06:00 | 08:00 | 10:00 | 12:00 | 14:00 |
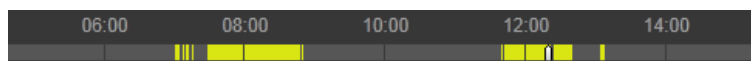
- Click ☰ , the video files of the selected date would be listed. Enter the start time and end time, and then click 🔍 to search all files between the start time and end time. Double-click the file in the list, and the system plays the video and displays file size, starting time, and ending time.

Figure 3-10 Playback file list

3.2.3 Clipping Video

Step 1   Click [≣].

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
[✂].

Figure 3-11 Clipping video
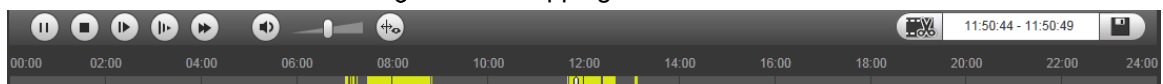
Step 4   Click again on the progress bar to select the end time, and then click [✂].

Step 5   Click [💾] to download the video.

Playback and downloading cannot be performed 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 "3.3.2.4 Path".

3.2.4 Downloading Video or Picture

Download video or picture to a defined path.

📖

● Playing and downloading at the same time is not supported.

● Operations might vary with different browsers, and the actual interface shall prevail.
● For details of viewing or setting storage path, see "3.3.2.4 Path".

To download a file:

Step 1 Select **dav** from the **Record Type** drop-down list when playing back videos.

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.

Step 3 Select **dav** or **mp4** in **Download Format**. Click [⊙] next to the file to be download.

The system starts to download the file to the configured path. When downloading pictures, you do not need to select the download format.

3.3 Camera

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

3.3.1 Configuring Camera Conditions

Configure camera parameters according to the actual situation, including managing configuration files and zoom in/out.

3.3.1.1 Setting Picture Parameters

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

3.3.1.1.1 Interface Layout

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

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 3-12 Camera conditions
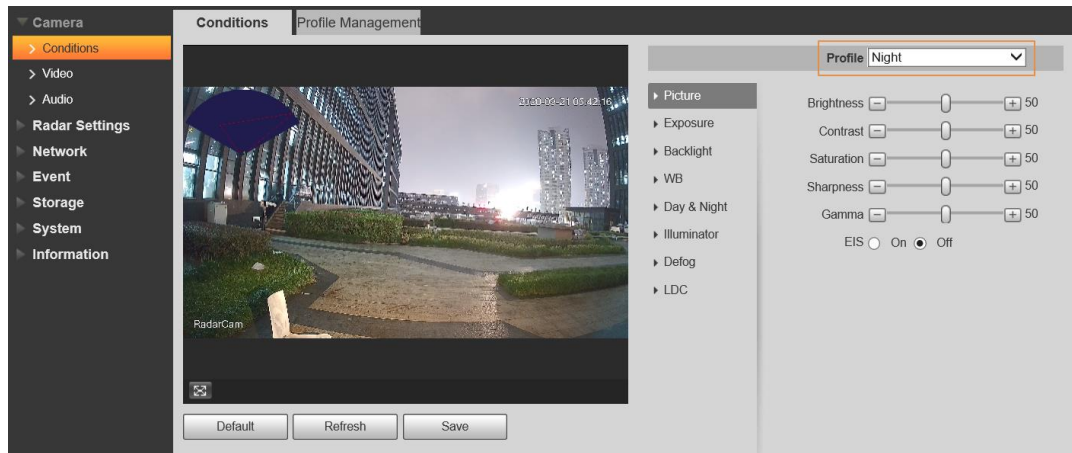
3.3.1.1.2 Picture

You can configure picture parameters as needed.

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

Step 2   Configure parameters. For details, see Table 3-5.

Figure 3-13 Picture

Table 3-5 Description of picture parameters

Parameter	Description
Brightness	The overall brightness of the picture. The higher the value is, the brighter the picture will be. The picture might be hazy if the value is configured too high.
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. Do not make the value too large to prevent image noise.
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.

Parameter	Description
EIS	Corrects the device shaking with difference comparison algorithm and improves the image clarity, effectively solves the picture shaking problem.

<u>Step 3</u> Click **Save**.

3.3.1.1.3 Exposure

Configure iris and shutter to improve image clarity.

<u>Step 1</u> Select **Setting > Camera > Conditions > Conditions > Exposure**.

<u>Step 2</u> Configure exposure parameters. For details, see Table 3-6.

Figure 3-14 Exposure
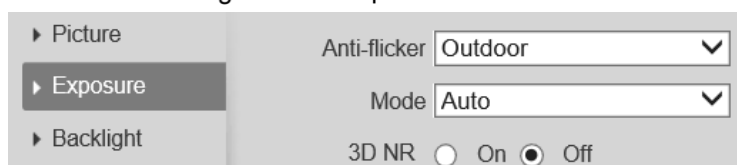
Table 3-6 Description of exposure parameters

Parameter	Description
Anti-flicker	You can select from 50 Hz, 60 Hz and Outdoor. ● **50 Hz**: When the electric supply is 50 Hz, exposure settings can be configured to Manual and Auto. ● **60 Hz**: When the electric supply is 60 Hz, exposure settings can be configured to Manual and Auto. ● **Outdoor**: You can select any exposure mode as needed.
Mode	Device exposure modes. ● **Auto**: Adjusts the image brightness according to the actual condition automatically. ● **Gain Priority**: When the exposure range is normal, the system prefers the configured gain range when auto adjusting according to the ambient lighting condition. If the image brightness is not enough and the gain has reached upper or lower limit, the system adjusts shutter value automatically to ensure the image at ideal brightness. You can configure gain range to adjust gain level when using gain priority mode. ● **Shutter priority**: When the exposure range is normal, the system prefers the configured shutter range when auto adjusting according to the ambient lighting condition. If the image brightness is not enough and the shutter value has reached upper or lower limit, the system adjusts gain value automatically to ensure the image at ideal brightness. ● **Manual**: Configure gain and shutter value manually to adjust image brightness. When the **Anti-flicker** is set to **Outdoor**, you can select **Gain priority** or **Shutter priority** in the **Mode** list.

Parameter	Description
3D NR	Works with multi-frame (no less than 2 frames) images and reduces noise by using the frame information between previous and latter frames. Unabled by default.

Step 3   Click **Save**.

3.3.1.1.4 Backlight

You can select backlight mode from Auto, BLC, WDR, and HLS.
Step 1   Select **Setting > Camera > Conditions > Conditions > Backlight**.
Step 2   Configure backlight parameters. For details, see Table 3-7.
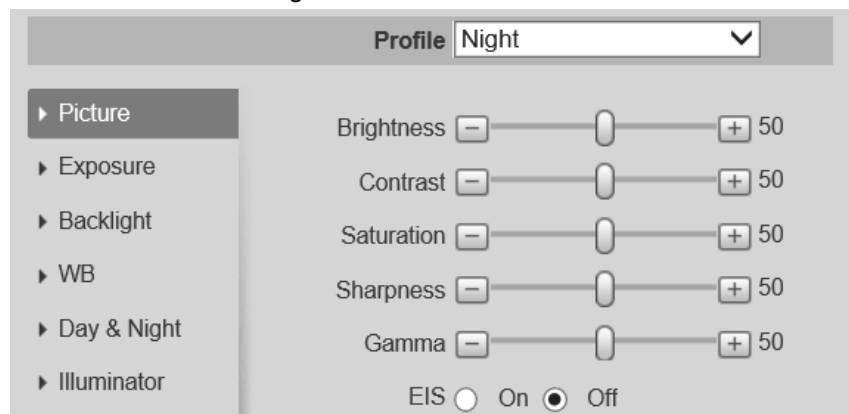
Figure 3-15 Backlight

Table 3-7 Description of backlight parameters

Backlight mode	Description
BLC	Enable BLC, the camera can get clearer image of the dark areas on the target when shooting against light. You can select **Default** or **Customized** mode. ● 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	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 larger the value is, the more obvious the HLC effect will be.
WDR	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. There might be a few seconds of video loss when the device is switching to WDR mode from other mode.

Step 3   Click **Save**.

3.3.1.1.5 WB

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

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

Step 2 Configure WB parameters, for the detailed description, see Table 3-8.

Figure 3-16 WB
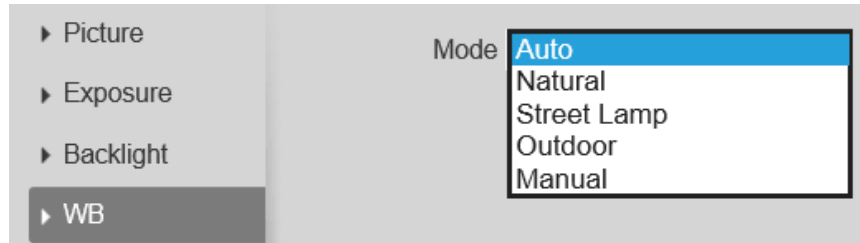
Table 3-8 Description of WB parameters

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.

Step 3 Click **Save**.

3.3.1.1.6 Day and 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**.

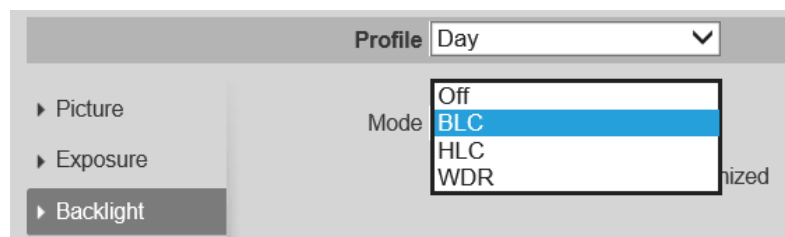Step 2 Configure day and night parameters. For details, see Table 3-9.

Figure 3-17 Day & Night
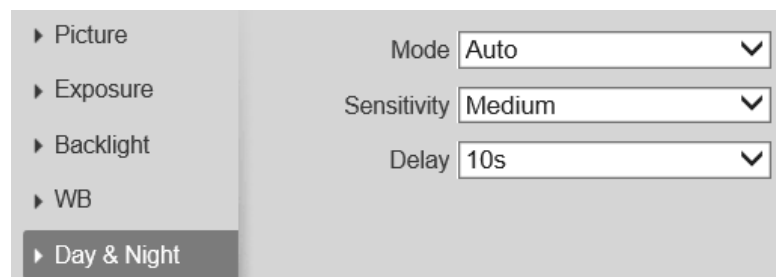
Table 3-9 Description of day and night parameters

Parameter	Description
Mode	You can select device display mode from **Color**, **Auto**, and **B/W**. ● **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. Day & Night configuration is independent from profile management configuration.
Sensitivity	You can configure camera sensitivity when switching between color and black-and-white mode. The higher the sensitivity, the easier the switching will be triggered.
Delay	This configuration is available only when you set **Auto** in **Mode**. You can configure the delay when camera switching between color and black-and-white mode. The lower the value is, the faster the camera switches between color and black-and-white mode.

Step 3 Click **Save**.

3.3.1.1.7 Illuminator

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

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

Step 2 Configure illuminator parameters. For the detailed description, see Table 3-10.

Figure 3-18 Illuminator
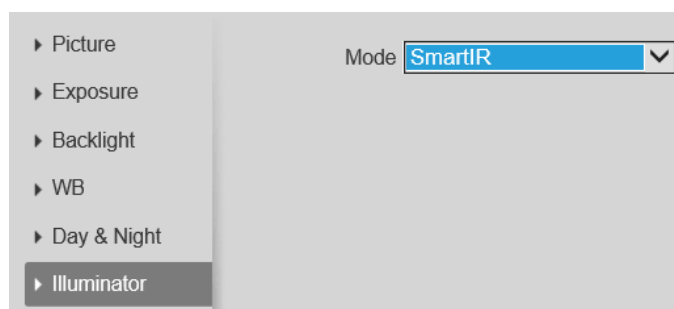
Table 3-10 Description of illuminator parameters

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

Step 3 Click **Save**.

3.3.1.1.8 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**.

Step 2 Configure defog parameters. For the detailed description, see Table 3-11.

Figure 3-19 Defog
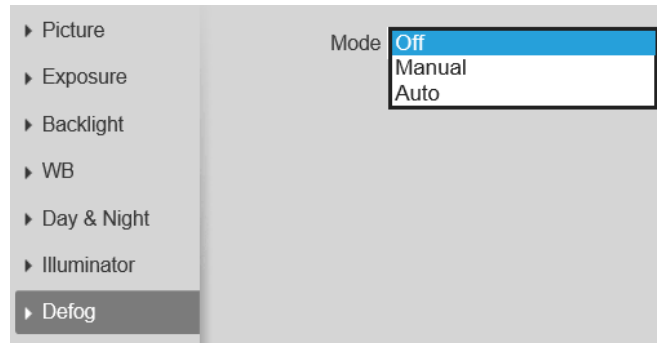
Table 3-11 Description of defog parameters

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**.

3.3.1.1.9 LDC

Correct the image according to actual scene.

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

Figure 3-20 LDC
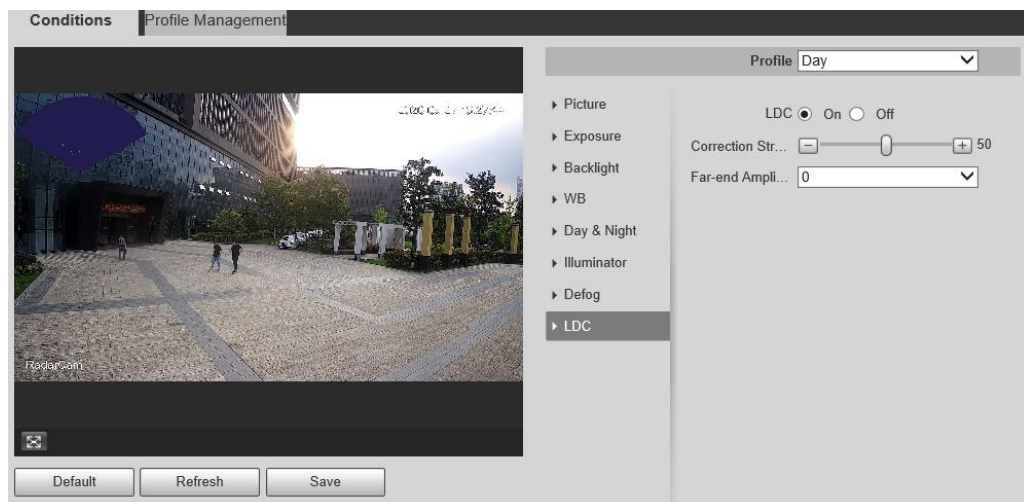
Step 2 Select **On**.

Step 3 Configure parameters. For details, see Table 3-12.

Table 3-12 LDC parameters description

Parameters	Description
Correction Strength	The correction strength of the image. The smaller the value is, the more obvious the image stretch effect is.
Far-end Amplification	The far-end amplication of the image. The bigger the value is, the more obvious the amplification effect is.

Step 4   Click **Save**.

3.3.1.2 Profile Management

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

Prerequisites

You have already configured profile parameters in **Camera > Conditions > Conditions**.

Procedures

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

Step 2   Manage profile.
- When **Profile Management** is set as **General**, the surveillance system works under General configuration.
- 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 3-21 Full time
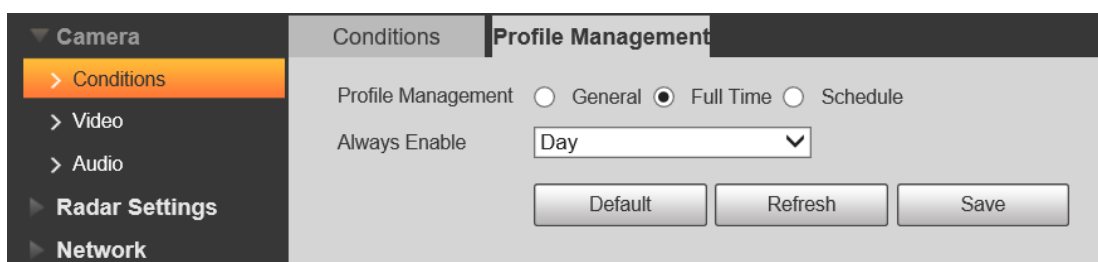
- When Profile Management is set as **Schedule**, you can drag the slide block to set certain time as **Day** or **Night**. For example, set 8:00–18:00 as day, and 0:00–8:00 and 18:00–24:00 as night.

Figure 3-22 Schedule
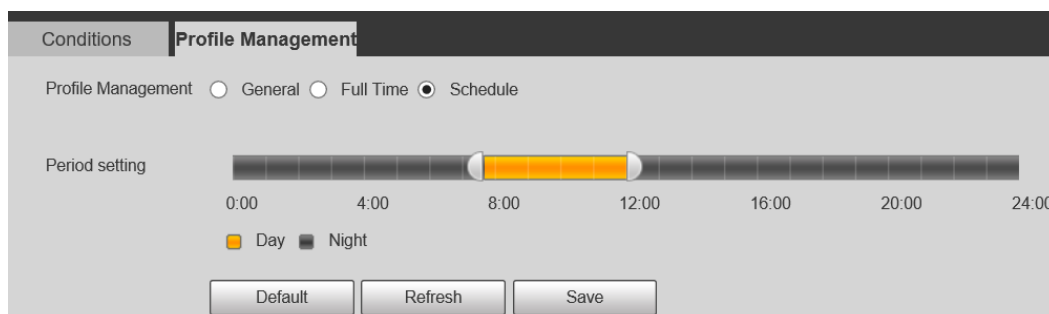
Step 3   Click **Save**.

3.3.2 Configuring Video Parameters

This section introduces video parameters, such as stream, overlay, and path.
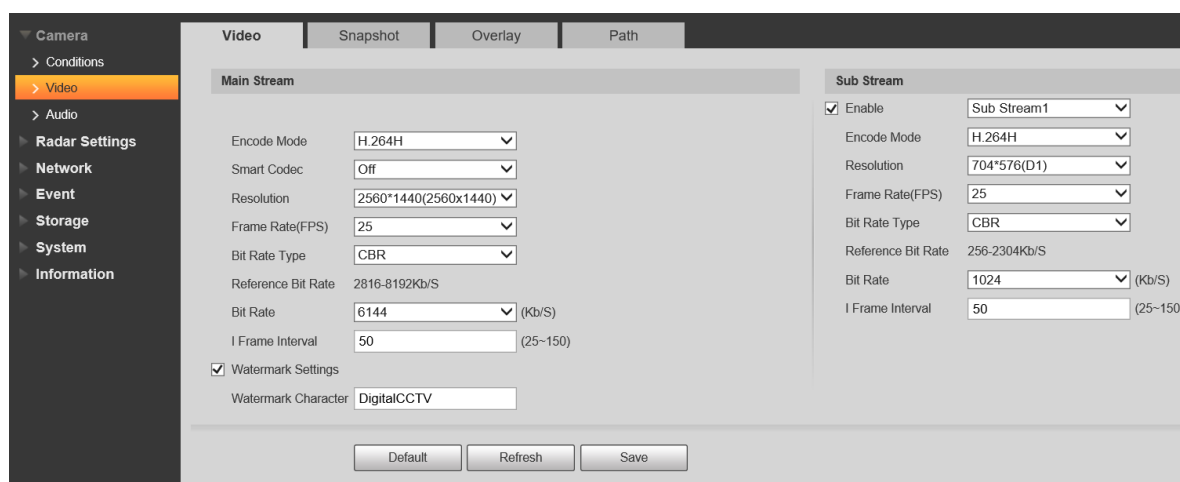
3.3.2.1 Video

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

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

Step 2 Configure video parameters. For details, see Table 3-13.

Figure 3-23 Video

Table 3-13 Description of Video parameter

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. ● H.264: Main profile encode mode. Compared with H.264B, it requires smaller bandwidth. ● H.265: Main profile encode mode. Compared with H.264, it requires smaller bandwidth.
Smart Codec	Enable **Smart Codec** to improve video compressibility and save storage space.
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	The bit rate control type during video data transmission. You can select bit rate type from: ● 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.

Parameter	Description
Quality	This parameter can be configured only when the **Bit Rate Type** is set as **VBR**. The better the quality is, the larger the bandwidth will be requested.
Reference Bit Rate	The most suitable bit rate value range recommended to user according to the defined resolution and frame rate.
Max Bit Rate	This parameter can be configured only when the **Bit Rate Type** is set as **VBR**. You can select the value of the **Max Bit Rate** according to the **Reference Bit Rate** value. The bit rate then changes as monitoring scene changes, but the max bit rate keeps close to the defined value.
Bit Rate	This parameter can be configured only when the **Bit Rate Type** is set as **CBR**. Select bit rate value in the list according to actual condition.
I Frame Interval	The number of P frames between two I frames, and the **I Frame Interval** range changes as **FPS** changes. It is recommended to set **I Frame Interval** twice as big as **FPS**.
Watermark Settings	You can verify the watermark to check if the video has been tampered. Select the check box to enable watermark function. The default character is DigitalCCTV.
Watermark Character	

Step 3 Click **Save**.

3.3.2.2 Snapshot

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

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

Step 2 Configure snapshot parameters. For details, see Table 3-14.

Figure 3-24 Snapshot
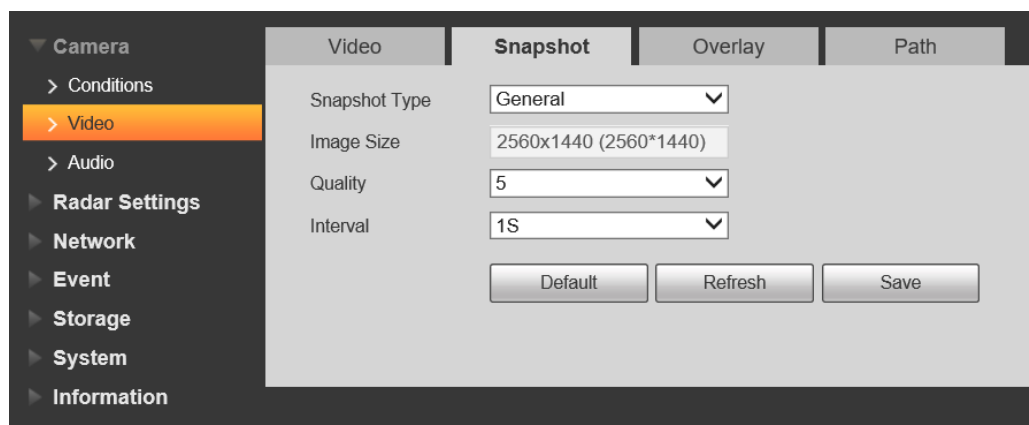
Table 3-14 Description of snapshot parameter

Parameter	Description
Snapshot Type	● **General**: The system takes snapshot as scheduled. See "3.5.2 Configuring Schedule" for details. ● **Event**: The system takes snapshot when the video detection, audio detection, event, or alarm is triggered. This function requires the corresponding event snapshot being enabled.

Parameter	Description
Image Size	The same resolution with main stream.
Quality	Configures the snapshot quality.
Interval	Configure the snapshot frequency. Select **Customized**, and then you can configure snapshot frequency manually.

Step 3 Click **Save**.

3.3.2.3 Overlay

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

3.3.2.3.1 Configuring Privacy Masking

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

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

Step 2 Select **Enable**, and then draw the rectangles to the area that you need to cover.

📖

- Maximum 4 rectangles are supported.
- Click **Remove All** to delete all drawn rectangles. Select a specific rectangle, and click **Delete** or right-click to delete it.

Step 3 Resize the rectangle to protect privacy.

Figure 3-25 Privacy Masking
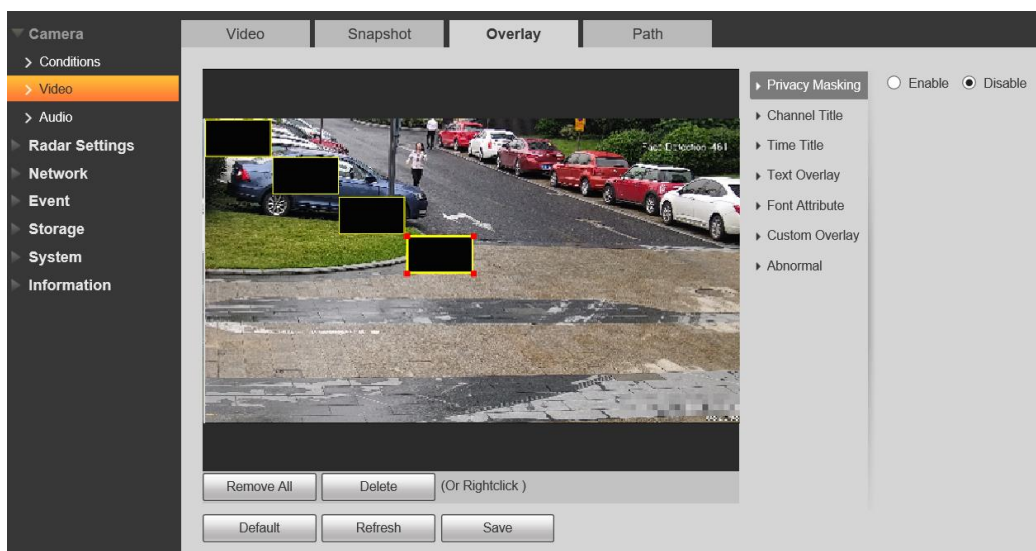
Step 4 Click **Save**.

3.3.2.3.2 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**.

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

⊞

Click + to add channel titles, and you can expand 1 line at most.

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

Figure 3-26 Channel title
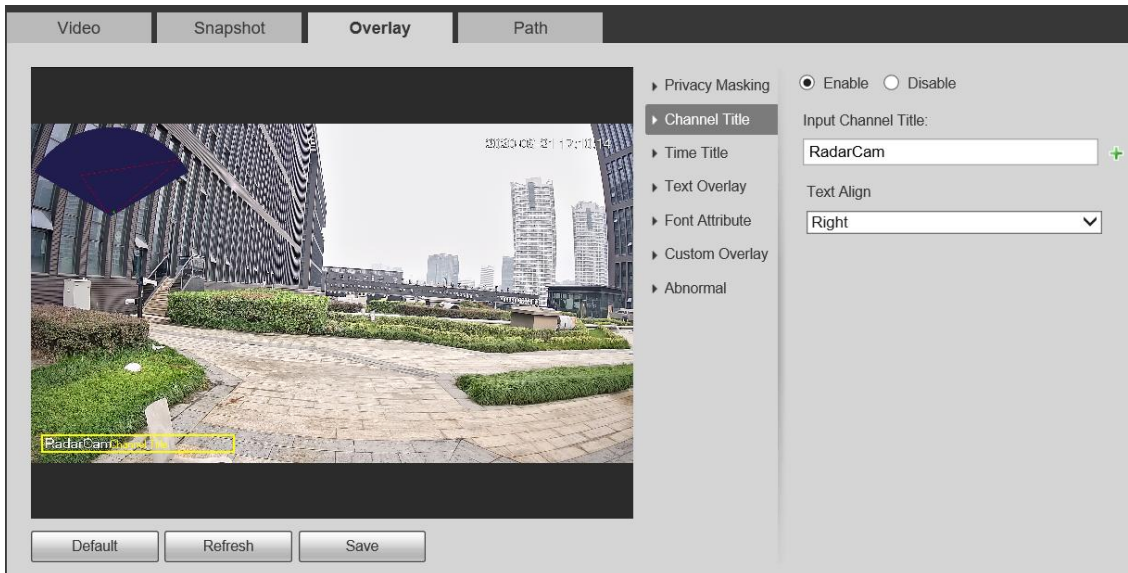
Step 4 Click **Save**.

3.3.2.3.3 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**.

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.

Figure 3-27 Time title
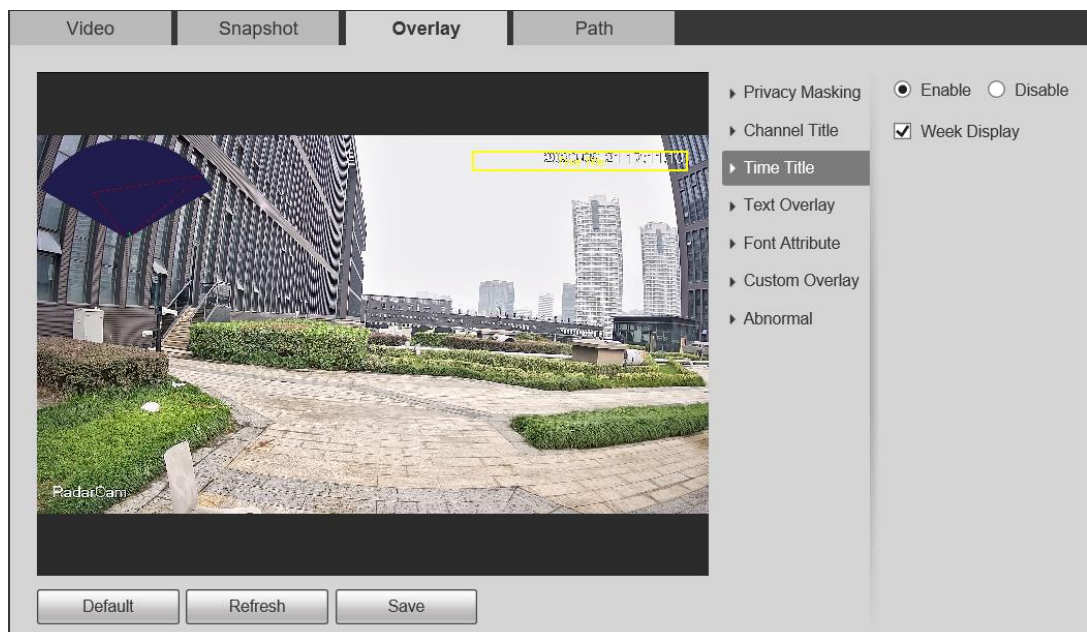
Step 5 Click **Save**.

3.3.2.3.4 Configuring Text Overlay

You can enable this function if you need to display additional information such as geographical location in the video image.

📖

Text overlay and OSD overlay (**Setting > Radar Settings > IVS Setup**) cannot be enabled at the same time.

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

Step 2   Select **Enable**, and enter text and select text align.

📖

Click + to add additional text overlay. Maximum 9 lines are supported.

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

Figure 3-28 Text Overlay
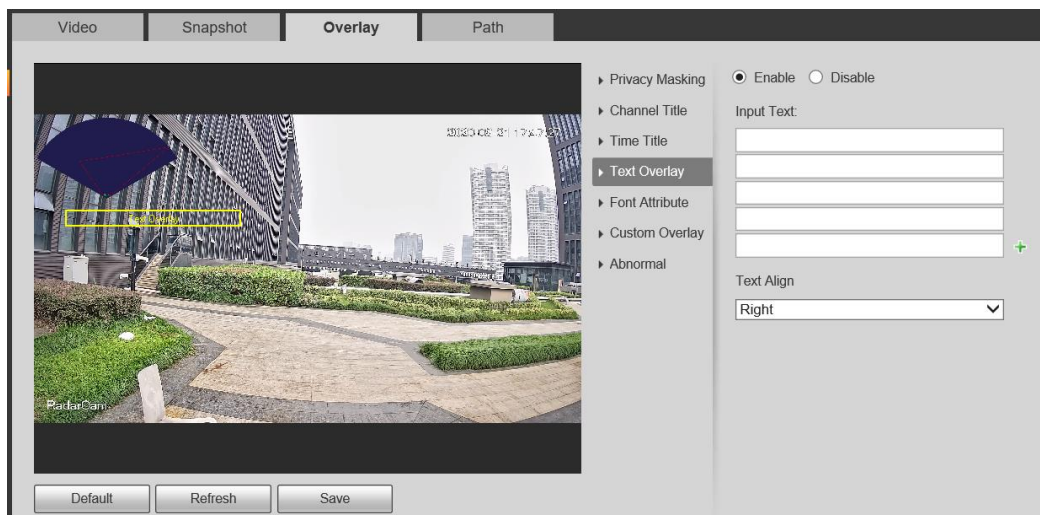
Step 4   Click **Save**.

3.3.2.3.5 Configuring 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**.

Step 2   Select the font color and size.

Figure 3-29 Font attribute
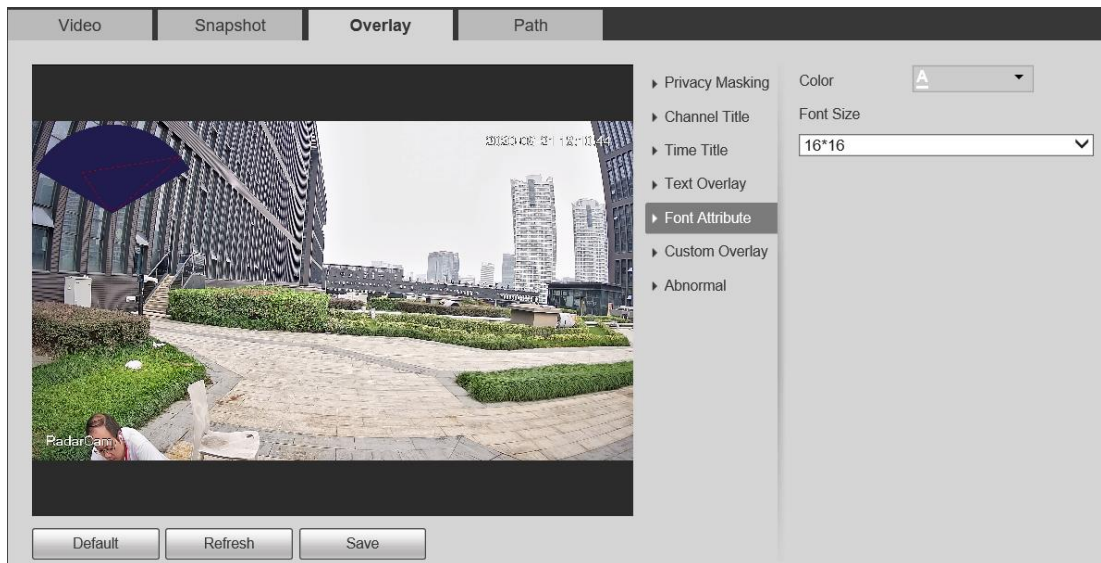
Step 3 Click **Save**.

3.3.2.3.6 Configuring 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**.
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.

Figure 3-30 Custom Overlay
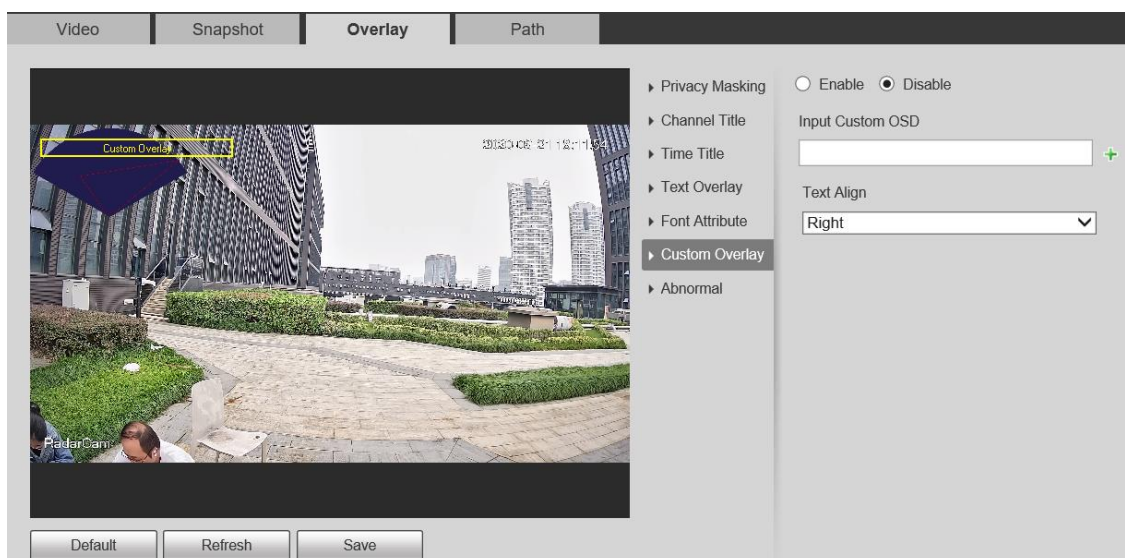
Step 4 Click **Save**.

3.3.2.3.7 Configuring Abnormality Overlay

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

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

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

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

Figure 3-31 Abnormal
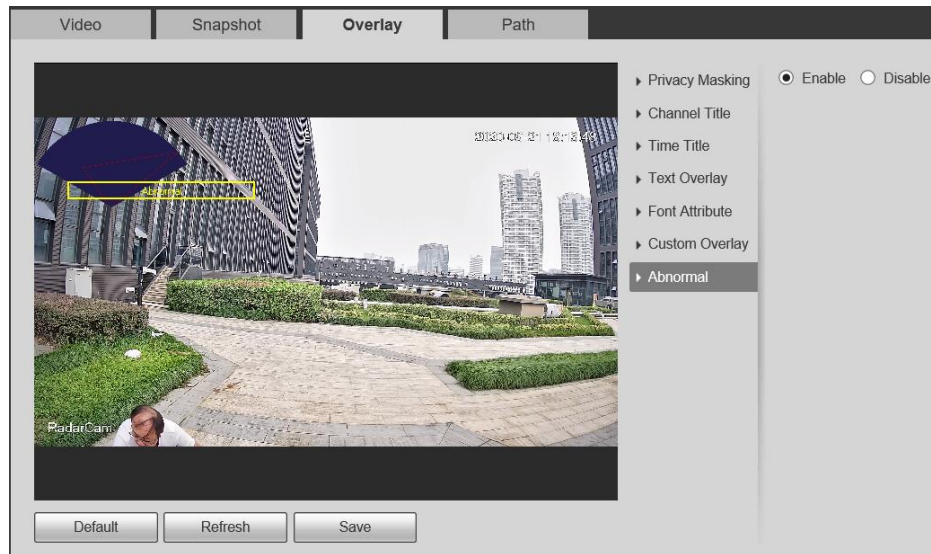
Step 4   Click **Save**.

3.3.2.4 Path

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

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

Step 2   Click **Browse** to select the storage path. For details, see Table 3-15.

Figure 3-32 Path
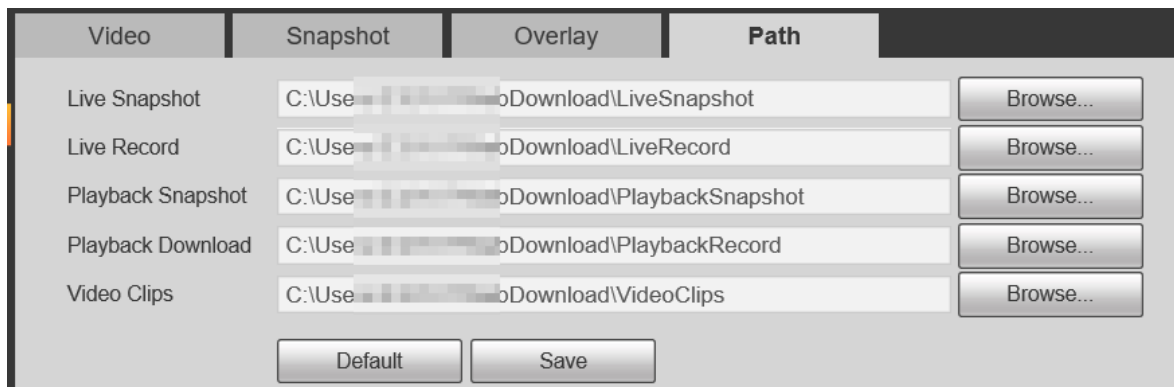
Table 3-15 Path description

Parameter	Description	
Live Snapshot	The snapshot of live interface. The default path is "C:\Users\admin\WebDownload\LiveSnapshot".	"Admin" in the path refers to the account being used.
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 ".	

Step 3   Click **Save**.

3.3.3 Audio

You can configure audio parameters and alarm audio.

3.3.3.1 Configuring Audio Parameter

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

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

Figure 3-33 Audio

Step 2 Select the **Enable** check box in **Main Stream** or **Sub Stream**.

For the camera with multiple channels, select the channel number.

Step 3 Configure audio parameters.

Table 3-16 Description of audio parameters

Parameter	Description
Encode Mode	The configured audio encode mode applies to both audio and intercom. The default value is recommended.
Sampling Frequency	Sampling number per second. The higher the sampling frequency is, the more the sample in a second will be, and the more accurate the restored signal will be.
AudioIn Type	**LineIn** by default.
Audio Output Type	**LineOut** by default.
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**.

3.3.3.2 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 3-34 Alarm audio
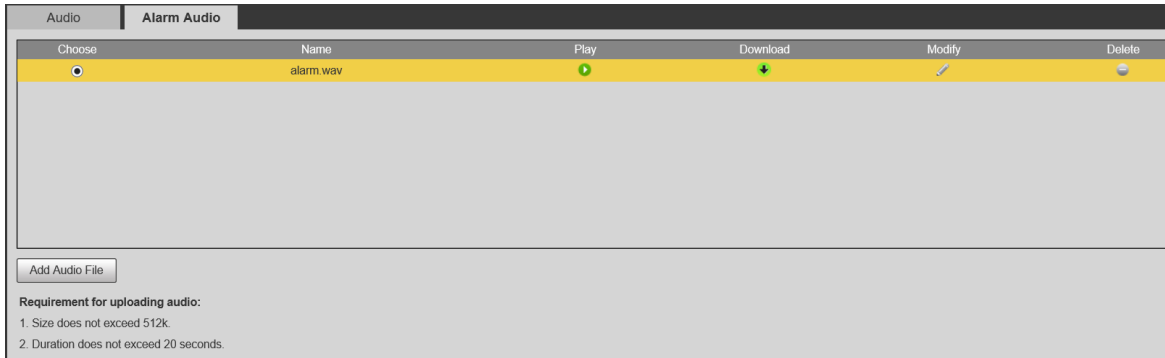
Step 2 Click **Add Audio File**.

Figure 3-35 Add audio file
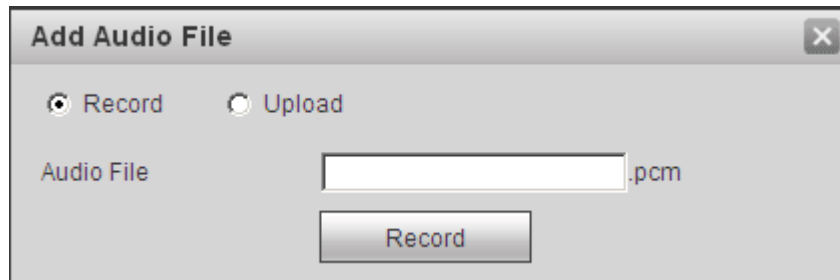
Step 3 Configure the audio file.

    ● 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 recorded audio file with .pcm format only, and you can upload audio files with .wav formats only.

Step 4 Select the file that you need.

3.4 Network

This section introduces network configuration.

3.4.1 TCP/IP

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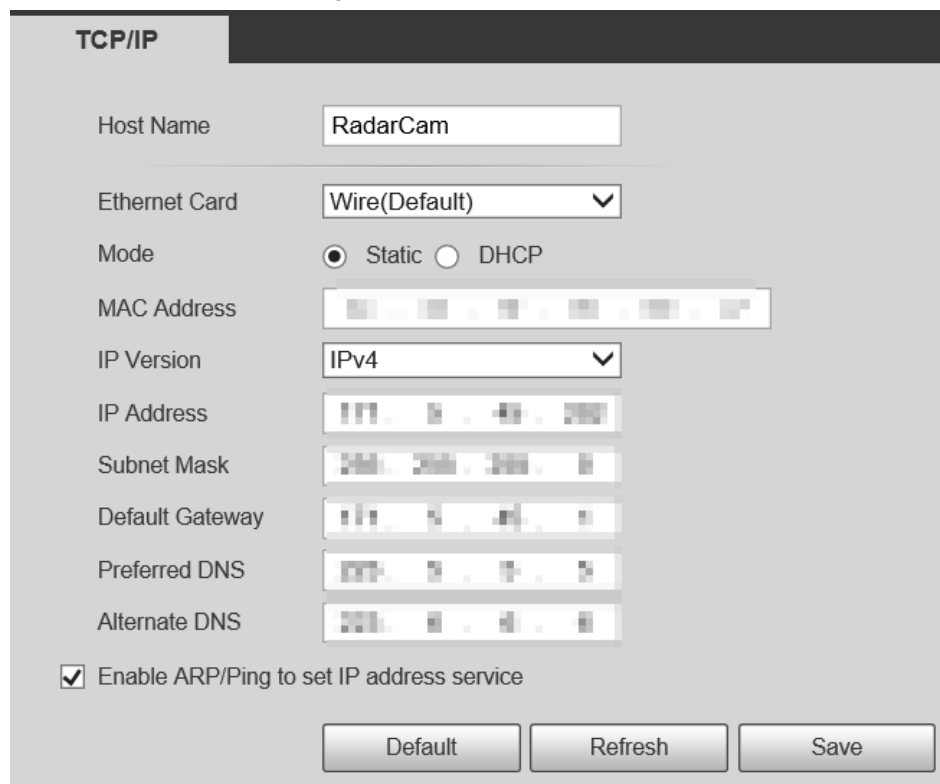
Prerequisites

The camera has connected to the network.

Procedure

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

Figure 3-36 TCP/IP

Step 2   Configure TCP/IP parameters.

Table 3-17 Description of TCP/IP parameters

Parameter	Description
Host Name	The maximum length is 15 characters.
Ethernet Card	Select the Ethernet card that need to be configured.

Parameter	Description
Mode	The mode that the camera gets IP: ● **Static** Configure **IP Address**, **Subnet Mask**, and **Default Gateway** manually, and then click **Save**, the login interface with the configured IP address is displayed. ● **DHCP** When there is DHCP server in the network, select **DHCP**, and the camera acquires IP address automatically.
MAC Address	Displays host MAC address.
IP Version	Select **IPv4** or **IPv6**.
IP Address	When you select **Static** in **Mode**, enter the IP address and subnet mask that you need.
Subnet Mask	
Default Gateway	● IPv6 does not have subnet mask. ● The default gateway must be in the same network segment with the IP address.
Preferred DNS	IP address of the preferred DNS
Alternate DNS	IP address of the alternate DNS

Parameter	Description
Enable ARP/Ping to set IP address service	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. **A demonstration of configuring IP address with ARP/Ping.** 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. Windows syntax↵ arp –s \<IP Address\> \<MAC\> ↵ ping –l 480 –t \<IP Address\> ↵ Windows example↵ arp -s 192.168.0.125 11-40-8c-18-10-11↵ ping -l 480 -t 192.168.0.125↵ UNIX/Linux/Mac syntax↵ arp –s \<IP Address\> \<MAC\> ↵ ping –s 480 \<IP Address\> ↵ UNIX/Linux/Mac example↵ arp -s 192.168.0.125 11-40-8c-18-10-11↵ ping -s 480 192.168.0.125↵ 4. Restart the camera. 5. Check the PC command line, if it outputs information such as **Reply from 192.168.0.125…** which means the setting is completed. 6. Enter http://(IP address) in the browser address bar to log in.

Step 3   Click **Save**.

3.4.2 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 3-37 Port

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 3-18 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	- 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. URL format example: rtsp://username:password@ip:port/cam/realmonitor?channel=1&subtype=0 Among that: - 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). Example: If you require the sub stream of channel 2 from a certain device, then the URL should be: rtsp://admin:admin@10.12.4.84:554/cam/realmonitor?channel=21&=1 If user name and password are not needed, then the URL can be: rtsp://ip:port/cam/realmonitor?channel=11&=0
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.

3.4.3 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 3-38 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.

3.4.4 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 3-39 DDNS (1)

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

Table 3-19 Description of DDNS parameters

Parameter	Description
Type	The name and web address of the DDNS service provider, see the matching relationship below:
Web Address	● CN99 DDNS web address: www.3322.org ● NO-IP DDNS web address: dynupdate.no-ip.com ● Dyndns DDNS web address: members.dyndns.org
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	

Parameter	Description
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.

3.4.5 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 3-40 SMTP (Email)

Step 2   Configure SMTP (Email) parameters.

Table 3-20 Description of SMTP (Email) parameters

Parameter	Description	
SMTP Server	SMTP server address	

Parameter	Description	
Port	The port number of the SMTP server.	
Username	The account of SMTP server.	For details, see Table 4-26.
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 4-26.	
Title	Enter maximum 63 characters in Chinese, English, and Arabic numerals.	
Attachment	Select the check box to support attachment in the email.	
Mail Receiver	Receiver's email address. Supports 3 addresses at most.	
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.	

Table 3-21 Description of major mailbox configuration

Mailbox	SMTP Server	Authentication	Port	Description
163	smtp.163.com	SSL	465/994	● You need to enable SMTP service in your mailbox. ● The authentication code is required; the email password is not applicable. Authentication code: the code you receive when enabling SMTP service.
		TLS	25	
		None	25	
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.

3.4.6 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.
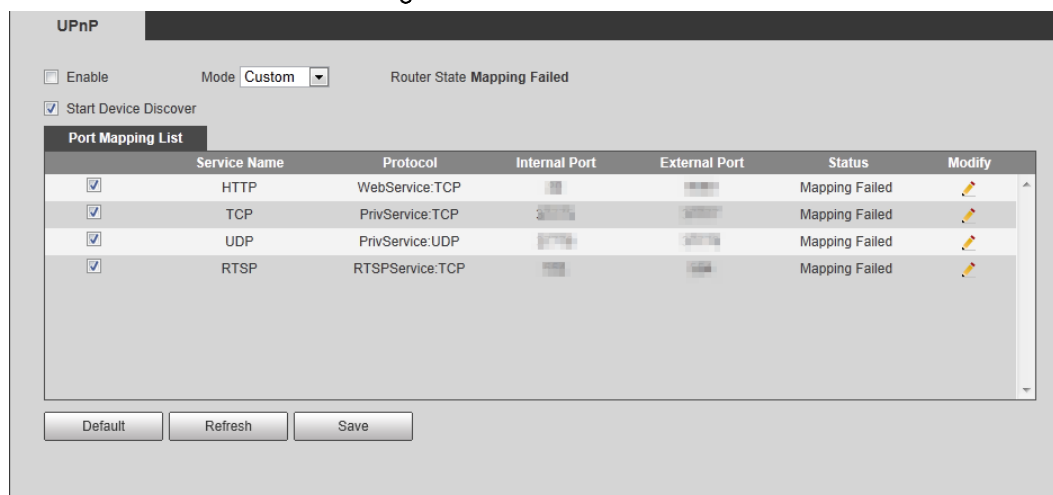
Prerequisites

● Make sure the UPnP service is installed in the system.

● Log in to 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 3-41 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.

3.4.7 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 3-42 SNMP (1)

Figure 3-43 SNMP (2)

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.
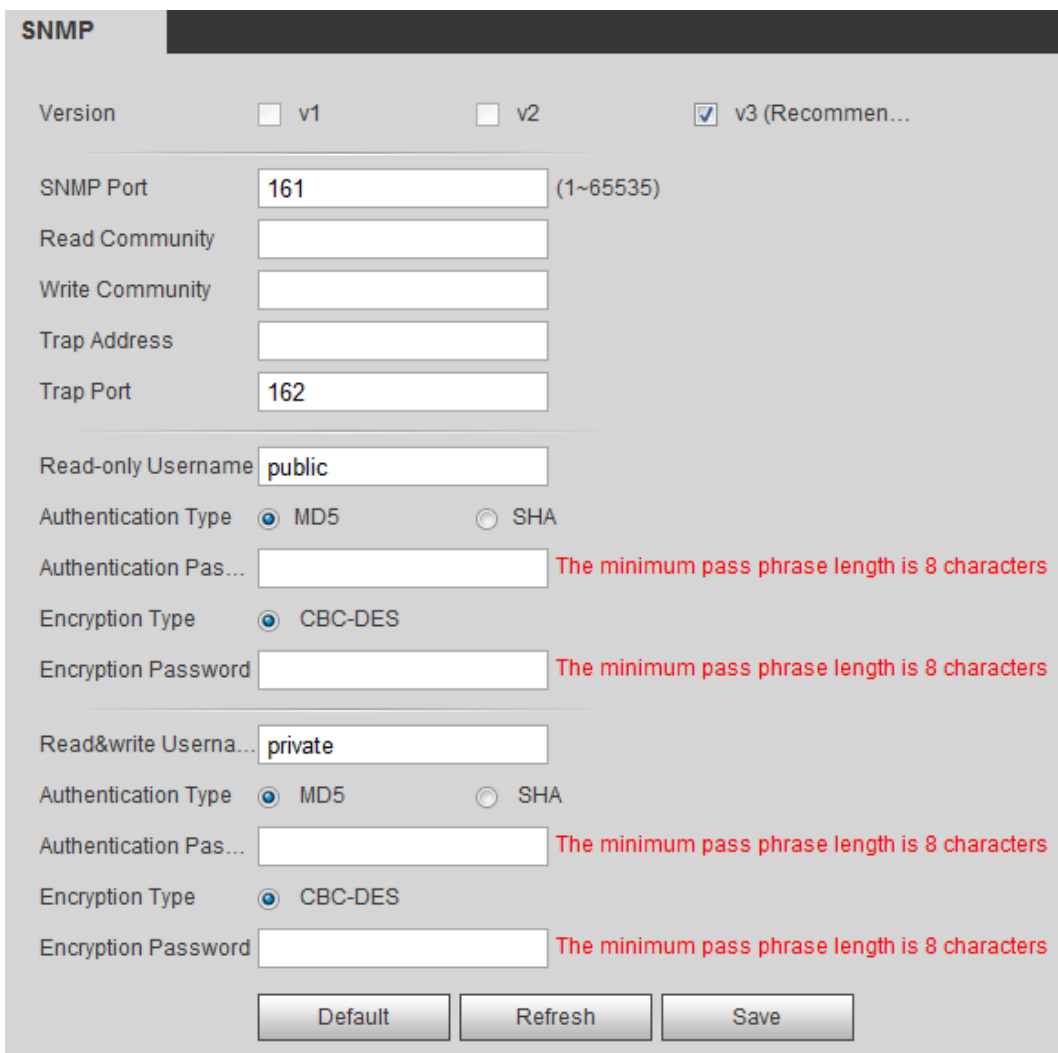- Select **V3**, and then **V1** and **V2** become unavailable. You can configure user name, password and authentication type. It requires corresponding user name, password and authentication type to visit your device from the server.

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

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

Table 3-22 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.

3.4.8 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 3-44 Bonjour
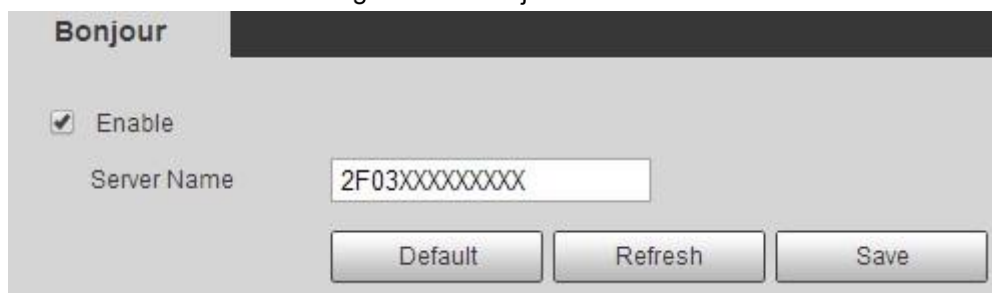
Step 2   Select the **Enable** check box, and then configure server name.

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.

3.4.9 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 3-45 Multicast

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

Table 3-23 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.

3.4.10 Auto Register

The device actively registers with the proxy server designated by the user, and the proxy server serves as a relay function, which facilitates the client software to access the device through the proxy server for live viewing and monitoring.

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

Step 2   Select **Enable**, and configure parameters.

Figure 3-46 Auto register

Table 3-24 Description of auto register

Parameters	Description
IP Address	Server IP address or server domian that needs to be registered.
Port	Port of the server for auto registration.
Sub-Device ID	Custom device ID.

3.4.11 802.1x

Cameras can connect to LAN after passing 802.1x authentication.

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

Figure 3-47 802.1x

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

Table 3-25 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**.

3.4.12 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 3-48 QoS

Step 2   Configure QoS parameters.

Table 3-26 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**.

3.4.13 Access Platform

3.4.13.1 P2P

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

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

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

Figure 3-49 P2P
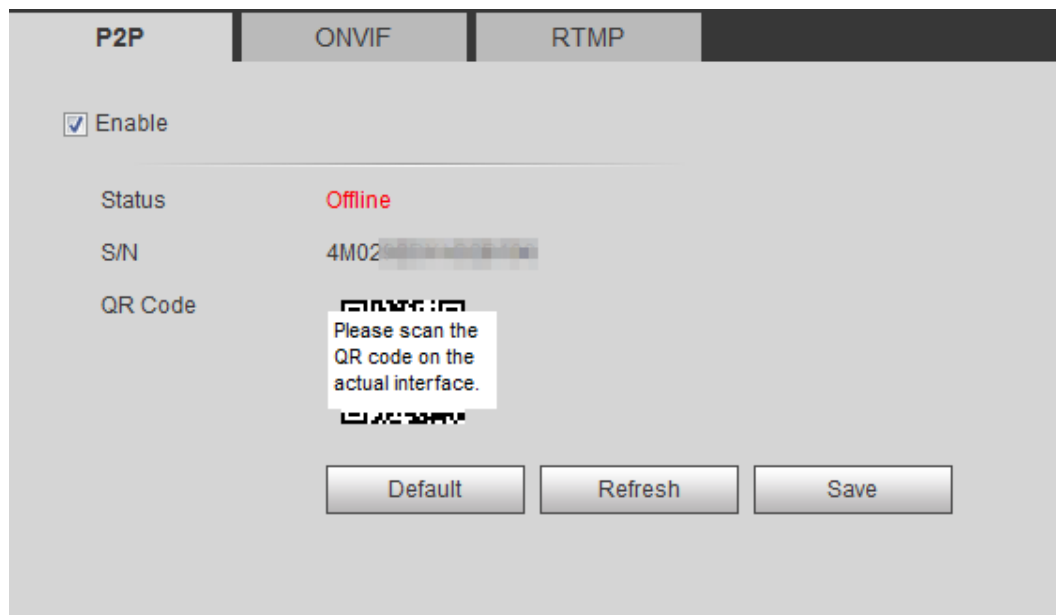
- When P2P is enabled, remote management on device is supported.
- When P2P is enabled and the device accesses to the network, the status shows online. The information of the IP address, MAC address, device name, and device SN will be collected. The collected information is for remote access only. You 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.

3.4.13.2 ONVIF

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

ONVIF is enabled by default.

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

Figure 3-50 ONVIF

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

Step 3 Click **Save**.

3.4.13.3 RTMP

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

📖

● RTMP can be configured by admin only.

● RTMP supports the H.264, H.264 B and H.264H video formats, and the AAC audio format only.

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

Figure 3-51 RTMP

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

⚠

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

Step 3 Configure RTMP parameters. .

Table 3-27 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**. ● **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.
Port	● **IP address**: Support IPv4 or domain name. ● **Port**: We recommend that you use the default one.
Custom Address	When selecting **Custom**, you need to enter the path allocated by the server.

<u>Step 4</u>   Click **Save**.

3.5 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.

3.5.1 Configuring Storage Plan

● Setting record plan and record control to achieve all-time recording, recording in specific period or alarm linked recording. For details, see "5.1.1.3.1 Configuring Record Plan" and "5.1.1.3.2 Configuring Record Control ".

● Set the snapshot schedule as needed. For details, see "5.1.1.4.1 Configuring Snapshot Plan".

3.5.2 Configuring 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

● Configure the record mode to be **Auto** in **Record Control**. For details, see "5.1.1.3.1 Configuring Record Plan".

● Configure holiday record and snapshot schedule. For details, see "5.1.1.3.1 Configuring Record Plan" and "5.1.1.4.1 Configuring Snapshot Plan".

Procedure

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

Figure 3-52 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.

[book icon]

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**.

3.5.3 Configuring Destination

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

3.5.3.1 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 3-53 Path

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

Table 3-28 Description of path parameters

Parameter	Description
Event Type	Select from **Scheduled** and **Alarm**.
Local	Save in the 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 "3.5.3 Setting Destination", "3.5.3.3 FTP" or "3.5.3.4 NAS".

3.5.3.2 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, and reset password for it.

● Normal mode: The new SD cards and the cards whose password are cleared successfully show normal mode. The SD cards of this status do not support authorization operation.

- Unauthorized mode: The SD card authorized by other devices shows unauthorized mode. The SD cards of this status do not support operations of setting read only, read & write, formatting and encryption.

- Encrypted mode: The SD cards encrypted and authorized on this camera show encrypted mode. The camera can record max. 10 pieces of encrypted SD information. When the recorded videos exceed 10 pieces, the earliest ones will be overwritten.

📖

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

- If you enter the wrong password for five times when authorizing, modifying, and clearing password, the camera will be locked for five minutes.

- Make sure that the SD card has been authorized before recording and playback.

- The health status of SD card:
  - ◇ Green: The health status is excellent.
  - ◇ Blue: The health status is good.
  - ◇ Orange: The health status is moderate.
  - ◇ Red: The health status is poor, and you need to replace the SD card.

Step 1   Select **Setting > Storage > Destination > Local**, and then the **Local** interface is displayed. See Figure 3-54.

Step 2   Select the SD card.
- Click **Read Only**, and then the SD card is set to read only.
- Click **Read & Write**, and then the SD card is set to read & write.
- Click **Hot Swap**, and then you can pull out the SD card.
- Click **Refresh**, and then you can format the SD card.
- Click **Format**, and you can format the SD card.

Figure 3-54 Local
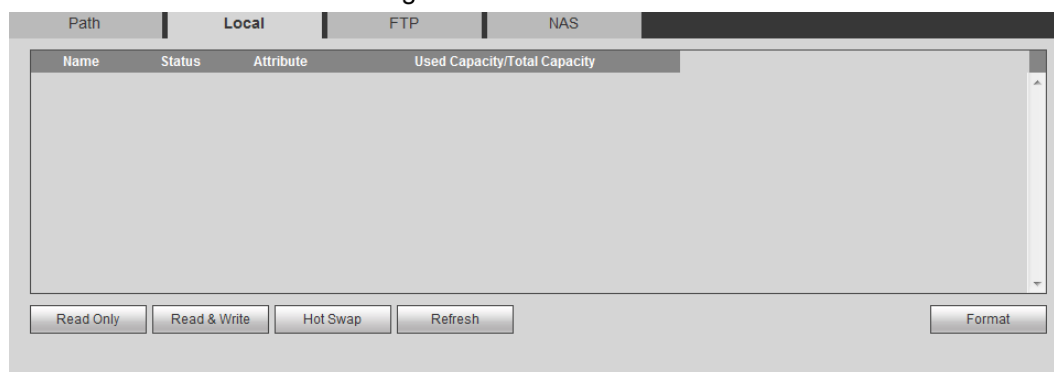
3.5.3.3 FTP

FTP function 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**.

Figure 3-55 FTP

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

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

Step 3   Configure FTP parameters.

Table 3-29 Description of FTP parameters

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

3.5.3.4 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 3-56 NAS

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 3-30 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**.

3.6 System

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

3.6.1 General

You can configure device name, language and video standard.

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

Figure 3-57 General

Step 2　Configure general parameters.

Table 3-31 Description of general parameters

Parameter	Description
Name	The name of the device. 📖 Each device has its own name.
Language	Select system language.
Video Standard	Select video standard from **PAL** and **NTSC**.

Step 3　Click **Save**.

3.6.2 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 3-58 Date and time

Step 2　Configure date and time parameters.

Table 3-32 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 with NTP server to use NTP.
NTP Server.	
Time Zone	
Port	
Interval	

Step 3　Click **Save**.

3.6.3 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 consist 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 permissions within group permission range.

- Online users cannot modify their own permission.

- There is one admin by default which has highest permission.

- Select **Anonymous Login**, and then log in with only IP address instead of user name and password. Anonymous users only have preview permissions. During anonymous login, click **Logout**, and then you can log in with another username.

3.6.3.1 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 3-59 Username
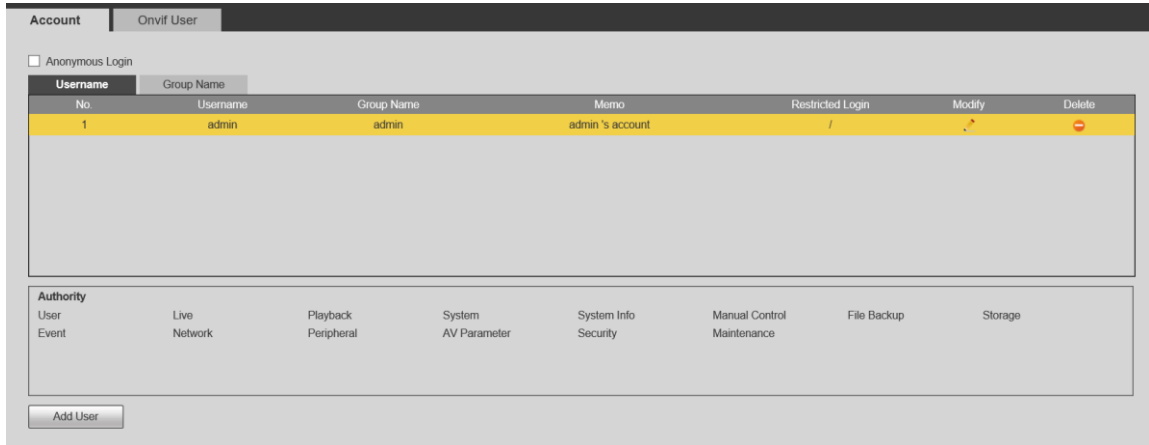
Step 2 Click **Add User**.

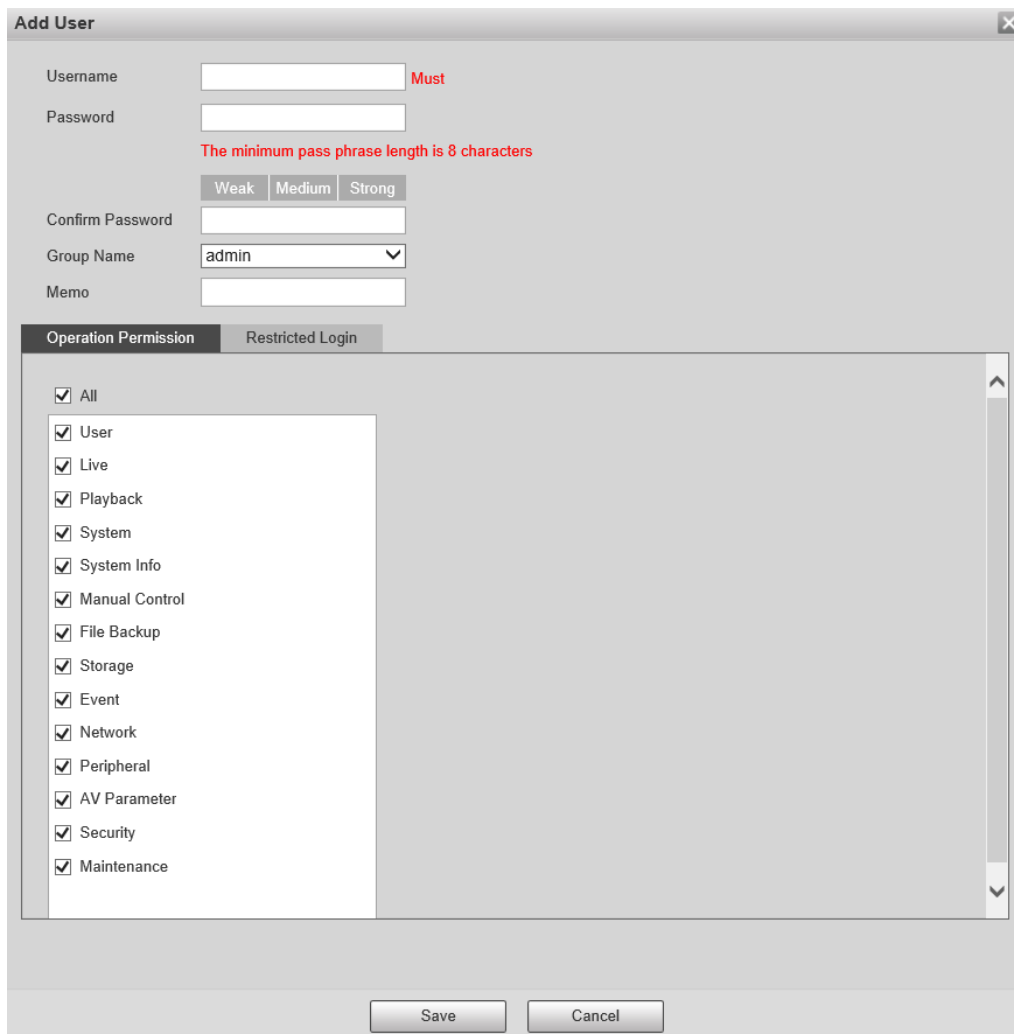Figure 3-60 Add user (operation permission)

Figure 3-61 Add user (restricted login)

Step 3   Configure user parameters.

Table 3-33 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.

Parameter	Description
Operation Permission	Select authorities as needed. 📖 You are recommended giving fewer authorities to normal users than premium users.

Restricted Login	Set the PC address that allows the defined user to log in to the camera and the validity period and time range. You can log in to the web interface with the defined IP in the defined time range of validity period.
	
	● IP address: You can log in to web through the PC with the defined IP.
	● Validity period: You can log in to web in the defined validity period.
	● Time Range: You can log in to web in the defined time range.
	
	Set as follows:
	
	1. Select **IP Address**: Select IP type and defined IP address.
	
	  ◇ 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**: Configure the begin time and end time.
	
	3. Select **Time Range**: Configure the time range that allows user to log in. For details, see "5.1.1.2 Configuring Period".

Step 4　Click **Save**.

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

▭

- After adding user, click ✐ to modify password, group, memo or authorities; click ⊖ to delete the added users. Admin user cannot be deleted.
- Click ✐ in the **admin** row to modify its username and email address.

3.6.3.2 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 3-62 Group name
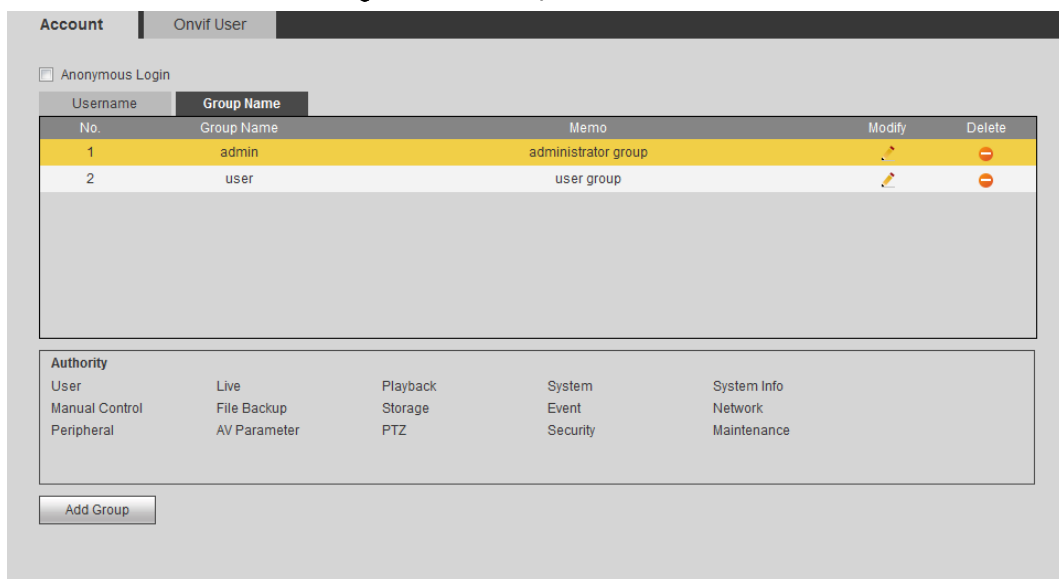
Step 2   Click **Add Group**.

Figure 3-63 Add group
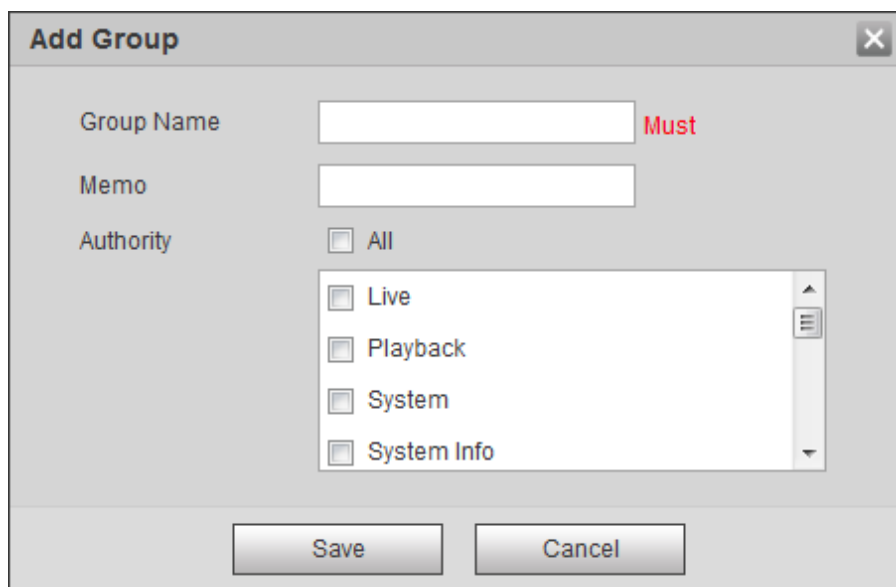
Step 3   Enter the group name and memo, and then select group authorities.

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.

3.6.3.3 ONVIF User

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

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

Figure 3-64 ONVIF user
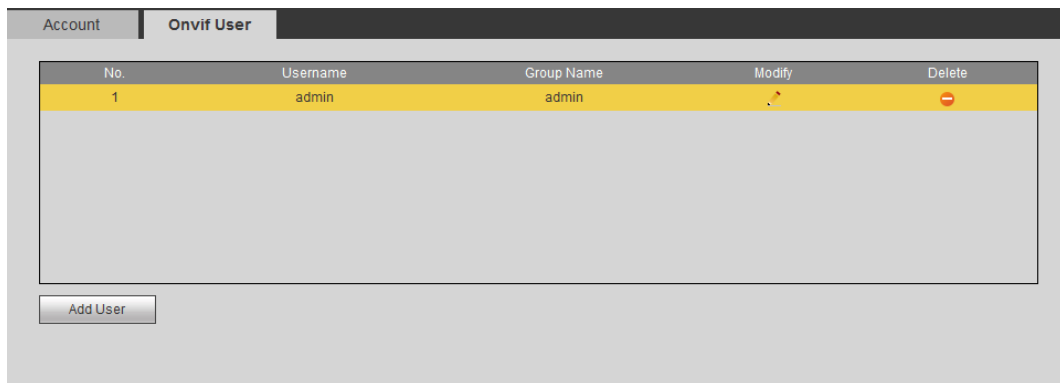
Step 2 Click **Add User**.

Figure 3-65 Add user

Step 3 Configure user parameters.

Table 3-34 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 permissions.

Step 4 Click **Save**.

The newly added user displays in the user name list.

- After adding user, click 🖉 to modify password, group, memo or authorities; click ⊖ to delete the added user. Admin user cannot be deleted.
- Click 🖉 in the **admin** row to modify its username and email address.

3.6.4 Safety

You can configure RTSP, system service, HTTPS, and Firewall to improve safety.

3.6.4.1 RTSP Authentication

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

Figure 3-66 RTSP authentication

RTSP Authentication	System Service	HTTPS	Firewall

Authorize Mode   Digest ▽

Default   Refresh   Save
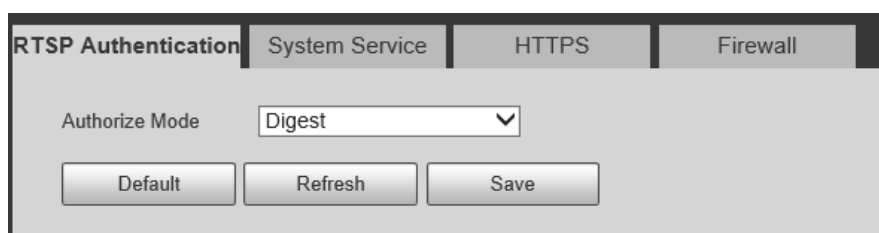
Step 2 Select Authorize Mode from Digest, Basic and None.
Step 3 Click **Save**.

3.6.4.2 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 3-67 System service

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

Table 3-35 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 viewing the device video image simultaneously through network, they can find your device with multicast/broadcast protocol.
Password Reset	Manage system security with this function.
CGI Service	Enable this function, and then other devices can access through this service.
Onvif Service	
Genetec 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.

Function	Description
RTSP over TLS	Enable to encrypt bit rate transmission. 📖 ● Ensure that the supporting device or software supports video decryption. ● The audio and video data with third-party platforms or devices do not support encrypted transmission. To ensure the security of audio and video data, it is recommended to turn off the CGI service and ONVIF service.
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.
Private Protocol Authentication Mode	Security mode and compatible mode.

Step 3   Click **Save**.

3.6.4.3 HTTPS

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

Procedure

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

Figure 3-68 HTTPS (1)

Step 2   Create a certificate or upload an authenticated certificate.

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

Figure 3-69 HTTPS dialog box

● For uploading the authenticated certificate, click **Browse** to select the certificate and certificate key, click **Upload** to upload them, and then skip to Step5.

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

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

Step 4   Click **Install**.

Figure 3-70 Certificate installation
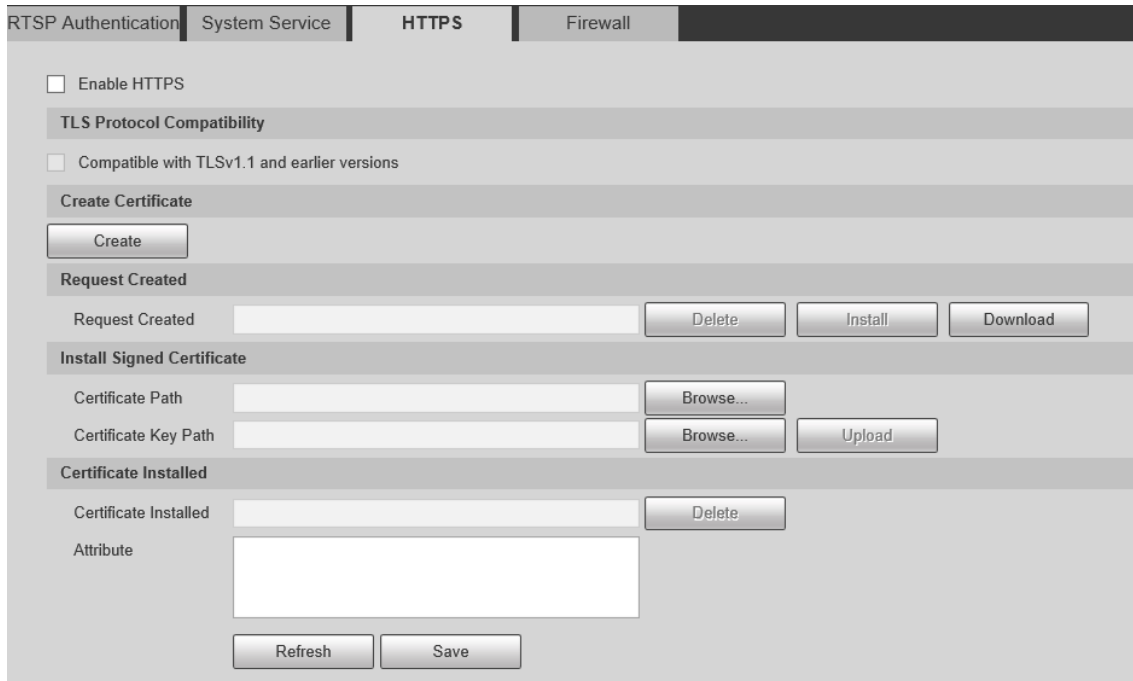
Step 5   Click **Download** to download root certificate.

Step 6   Click **Download Root Certificate**.

Figure 3-71 File download
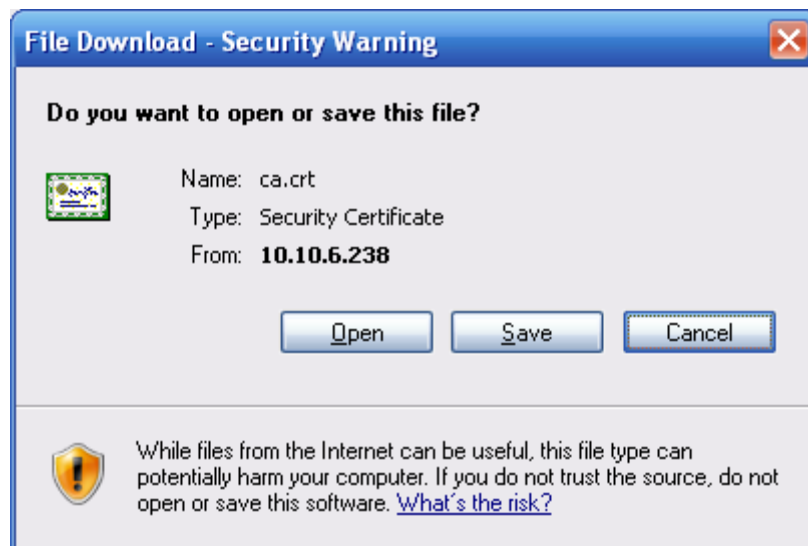
Step 7   Click **Open**.

Figure 3-72 Certificate information
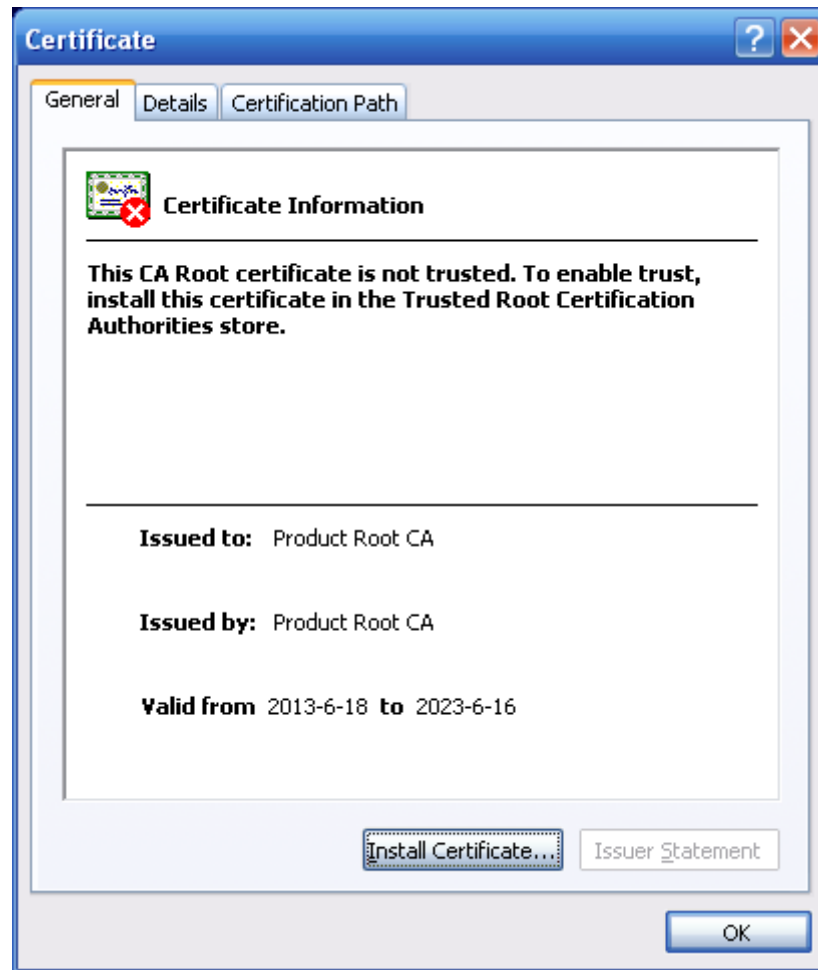
Step 8   Click **Install Certificate**.

Figure 3-73 Certificate import wizard (1)

Step 9   Click **Next**.

Figure 3-74 Certificate Store
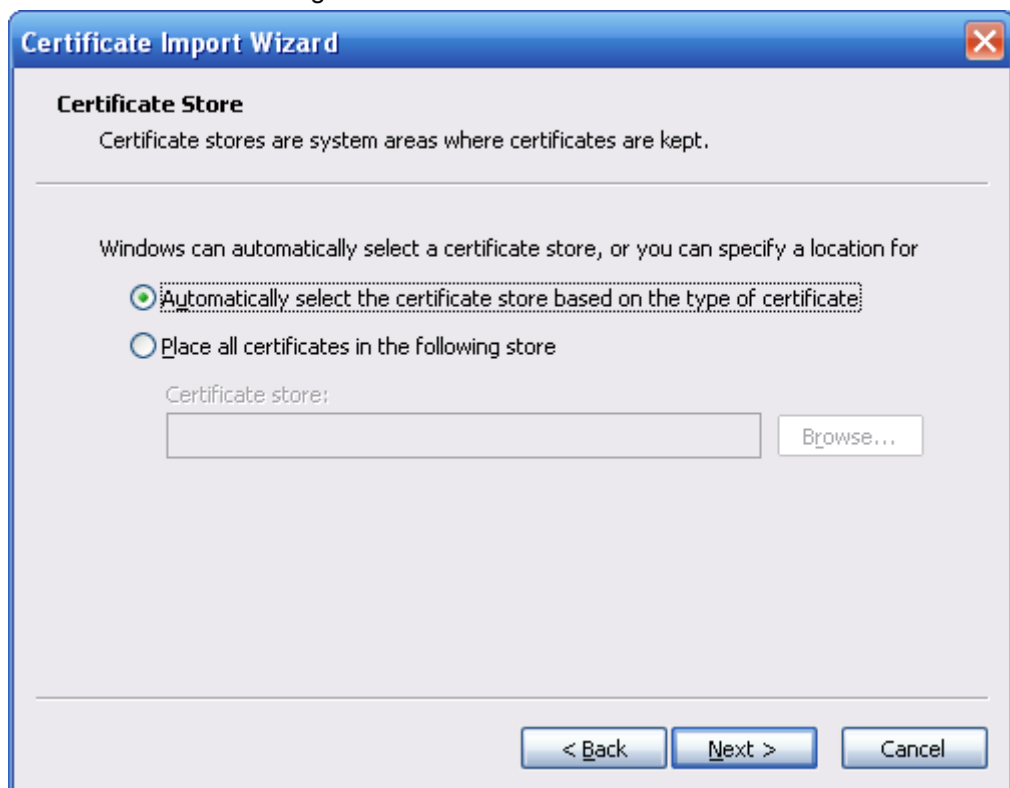
Step 10 Select the storage location and click **Next**.

Figure 3-75 Certificate import wizard (2)
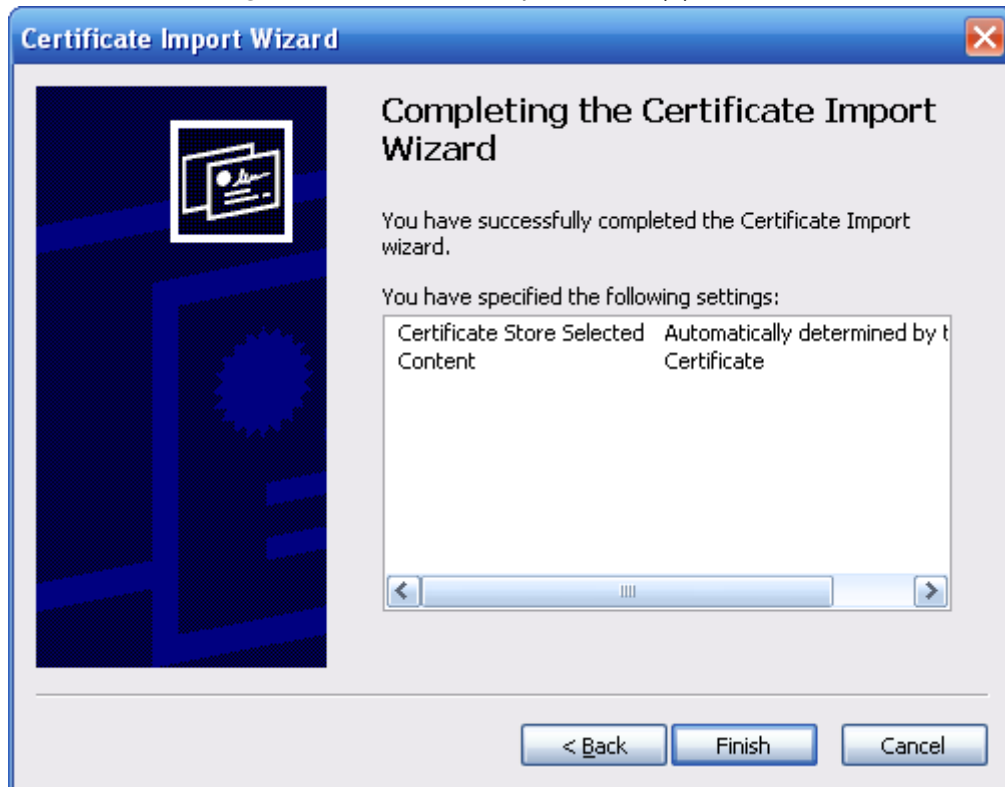
Step 11 Click **Finish** and then click OK in the pop-up box.

Figure 3-76 Import succeeds

3.6.4.4 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.
  ◇ **Trust list**: Only when the IP/MAC of your PC in the trusted list, can you access the camera. Ports are the same.
  ◇ **Banned list**: When the IP/MAC of your PC is in the banned list, 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 trust or banned list for camera IP or MAC addresses.

● You cannot set trust or banned list 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 3-77 Firewall
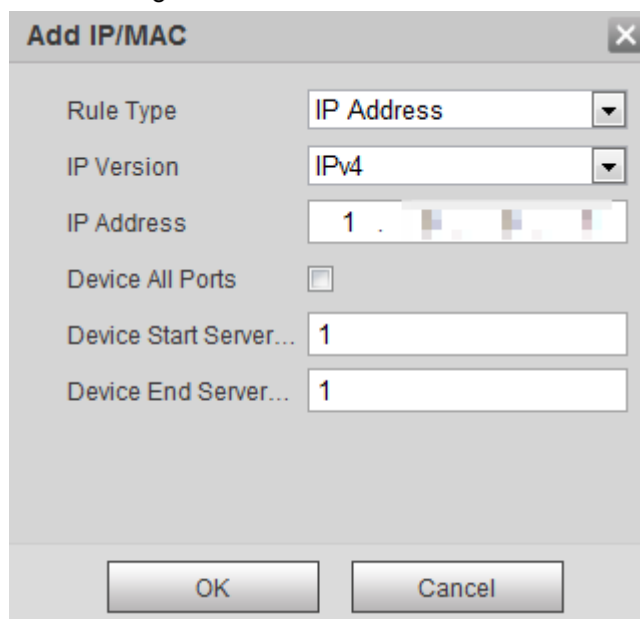
Step 2   Select **Network Access** from **Rule Type** list, and then select the **Enable** check box.

● 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 3-78 Add IP/MAC

Step 3   Configure parameters.

Table 3-36 Description of adding IP/MAC parameters

Parameter	Description
Rule Type	Select IP address, IP segment, MAC address or all IP addresses. ● 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 trusted list or restricted list.
Device All Ports Device Start Server Port Device End Server Port	Set access ports. You can select all ports or the ports in defined areas. ● Device all ports: Set all IP port in trust list or Banned list. When selecting **BannedList** 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.

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

Step 5   Click **Save**.

4 Configuring Radar

Configure radar functions, including region management, IVS setup, device attitude and linkage.

4.1 Configuring Region Management

You can configure functions, including setting alarm rules, area type, arming/disarming period and region filtering.

Procedures

Step 1   Select **Setting > Radar Settings > Region**.

Figure 4-1 Region management
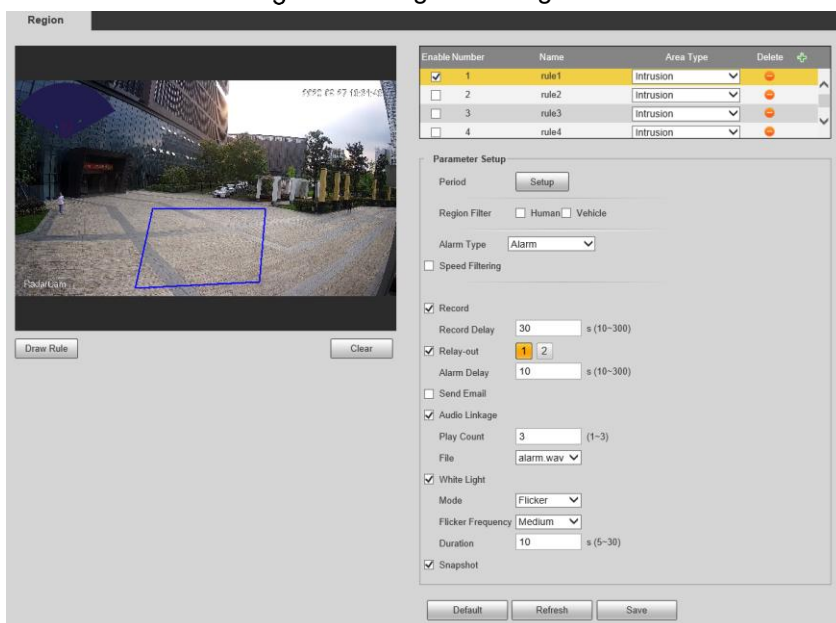
Step 2   Click , and then enter rule name at **Name** column, and then select an alarm type at **Area Type** column.

Step 3   Click **Draw Rule**, and then draw lines in the live image. Right click to finish drawing.

Step 4   For description of rules, see Table 4-1. After drawing, you can adjust the area by dragging the box angles. Click **Clear** to delete all drawn rules.

Table 4-1 Description of region management parameters (1)

Rule	Description
Tripwire	Draw 1 detection line. When a target crosses the line toward the defined direction, the alarm is triggered and the linkage is executed. Applicable scene: areas with sparse targets and nearly no obstacles between them, such as unmanned perimeter protection.

Rule	Description
Intrusion	Draw 1 detection area. When the target enters/exits or presents in the detection area, the alarm is triggered and the linkage is executed. Applicable scene: areas with sparse targets and nearly no obstacles between them, such as unmanned perimeter protection.

Step 5 To configure arming/disarming period and alarm linkage, see "5.1.1 Alarm Linkage".

Table 4-2 Description of region management parameters (2)

Parameter	Description
Region Filter	Select target filtering type, including **Human** and **Vehicle**.
Alarm Type	Select alarm type: **Alarm**, **Pre-warning** and **Shield**.
Target Filter	Select **Target Filter** check box, and then enter the target speed that you want to retain.

Step 6 Click **Save**.

4.2 Configuring IVS Setup

You can configure radar structuring, fusion, OSD and map location.
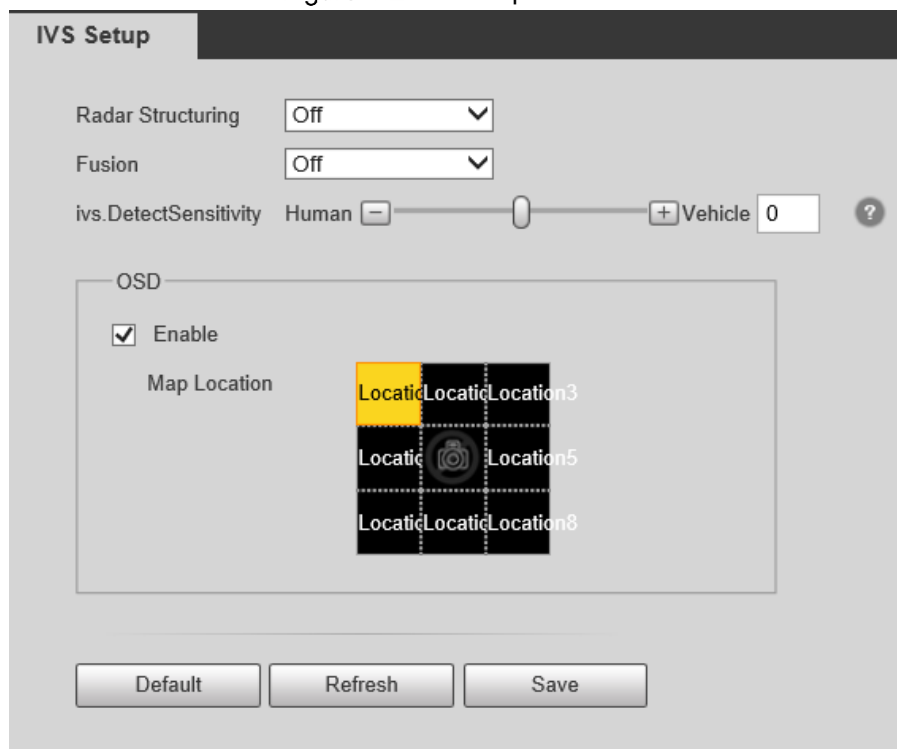
OSD function and text overlay function cannot be enabled at the same time.

Step 1 Select **Setting > Radar Settings > IVS Setup**.

Figure 4-2 IVS setup

Step 2 Configure parameters.

Table 4-3 IVS setup parameter description

Parameter	Description
Radar Structuring	After enabling radar structuring, the live view will display information including target distance, angle, speed, and type. 📖 You need to enable Fusion before enable Radar Structuring.
Fusion	After enabling fusion, the live view will display the historic track of the moving target within the detection range.
Trajectory Duration	The displayed duration of target moving trajectory. The value ranges from 3 to 30 seconds, and the default value is 10 seconds.
Detection Sensitivity	Configure the detection sensitivity of human and vehicle. The value ranges from –5 to 5. The default value is 0. The smaller the value is, the higher the detection accuracy for human is. The bigger the value is, the higher the detection accuracy for vehicle is.
OSD	After being enabled, the live view will display a sector according to the selected map location. The sector is a virtual area that displays the track point within the detection range. The radius of the sector is 60 m, and the angle is 120°.
Map Location	8 options. Corresponds to the live view location.

Step 3 Click **Save**.

4.3 Configuring Device Attitude

Device attitude is enabled by default. After installation, if you need to adjust the device orientation, configure device attitude to see if the device is installed correctly.

The embedded chip monitors the device attitude in real time. Parameters include pitch angle, roll angle and yaw angle (always 0°).

Procedures

Step 1 Select **Setting > Radar Settings > Device Attitude**.

Figure 4-3 Device attitude
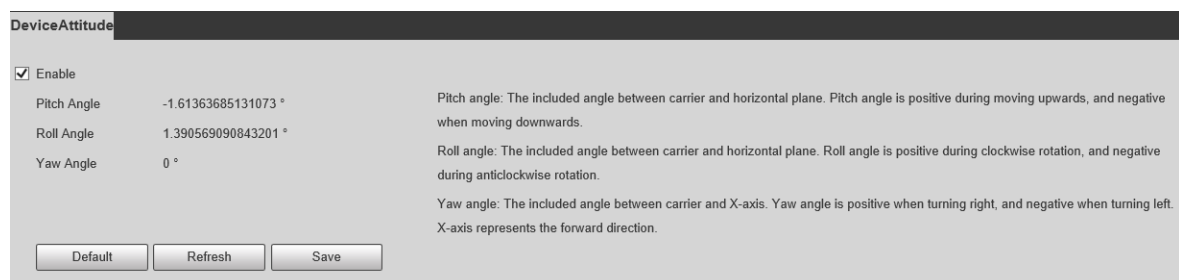
Step 2 When adjusting the radar orientation, it is recommended to set the pitch angle to around –3°, and roll angle 0°.

Step 3 Click **Save**.

4.4 Configuring Linkage

To raise the detection accuracy, it is recommended that you calibrate the radar by taking a moving human or object as reference.

After enabling fusion and calibrating accurately, the trajectory displayed on live view will be more accurate.

4.4.1 Auto Calibration

Step 1   On the web interface, select **Setting > Radar Settings > Linkage**.

Step 2   In the pull-down list, select **Auto**. See Figure 4-4.

Step 3   In the live view, taking a moving human or vehicle as reference to see if the calibration effect is good. If not, you can adjust by manual calibration.

$\square$

- You need to enable device attitude first to configure auto calibration.
- Preferred effect: The target and the box are consistent with each other during calibration.

Figure 4-4 Auto calibration
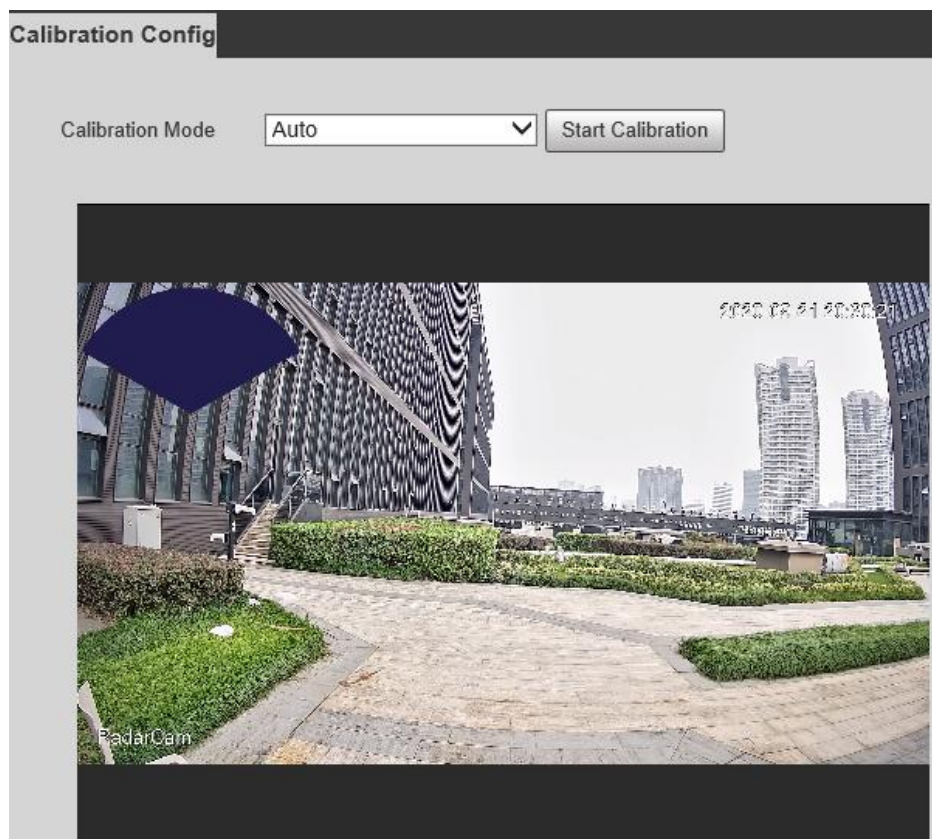
4.4.2 Manual Calibration

Step 1   In the pull-down list, select **Manual**. See Figure 4-5.
Step 2   Taking a moving human or vehicle as reference, click **Start Calibration**.
Step 3   Adjust the calibration box position by manually controlling the directional buttons and speed.

Preferred effect: The target and the box is consistent with each other during calibration.

Figure 4-5 Manual calibration
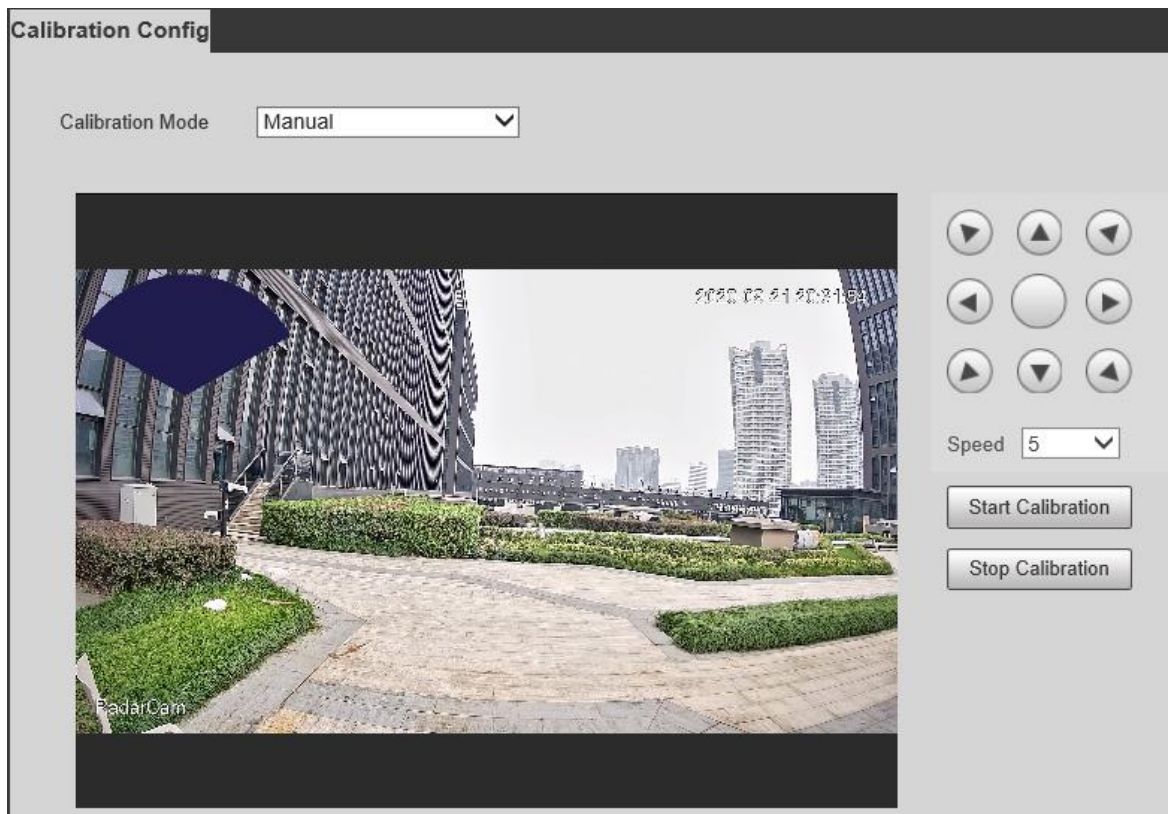
Step 4   Click **Stop Calibration**.

5 Configuring Alarms and Abnormality

5.1 Configuring Alarm Linkage

5.1.1 Alarm Linkage

When configuring alarm events in **Setting > Event > Alarm**, select alarm linkages (such as record, snapshot). When the corresponding alarm is triggered in the configured arming period, the alarm will be triggered.

Figure 5-1 Alarm linkage

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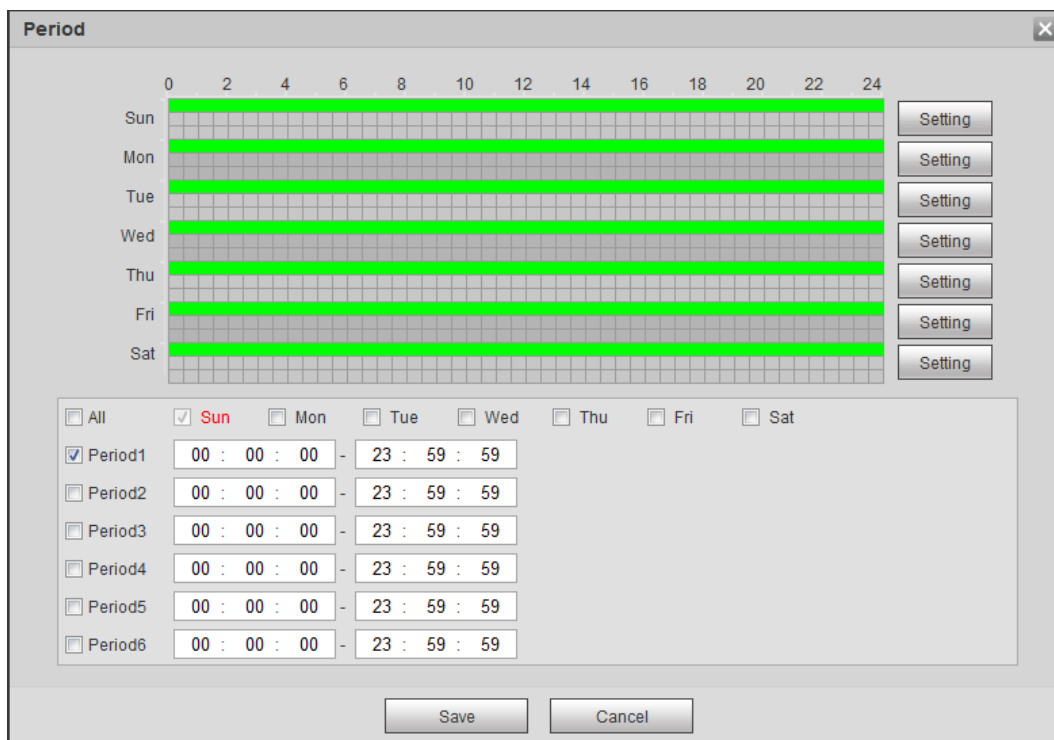
Step 2   Set arming periods. Alarms will be triggered in the time period in green on the timeline.

- Directly press and drag the left mouse button on the timeline.

- 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**.

5.1.1.3 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.

5.1.1.3.1 Configuring Record Plan

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

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

Figure 5-3 Record
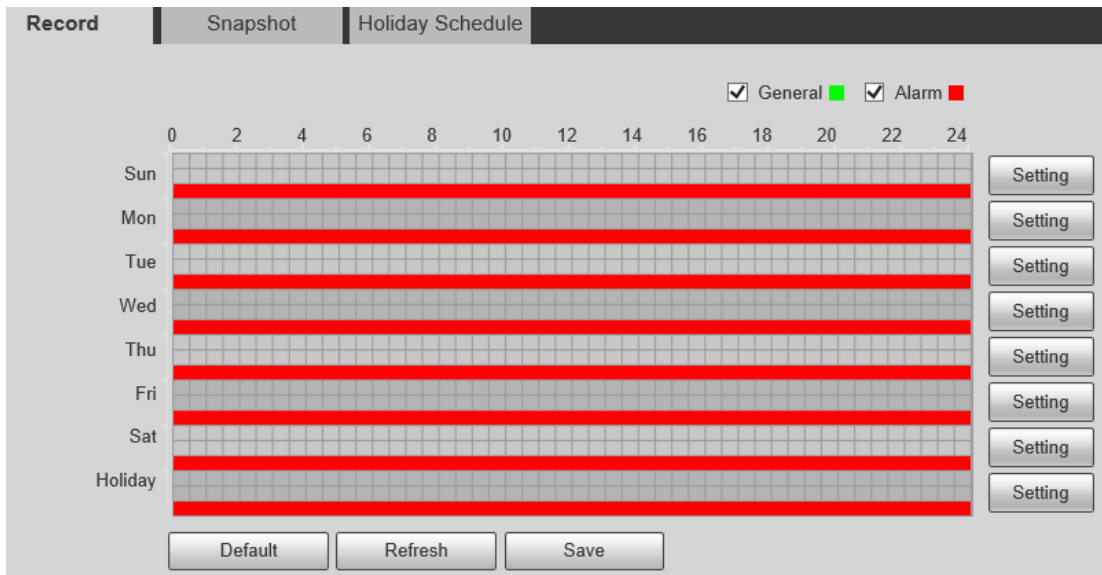
Step 2   Set record plan.

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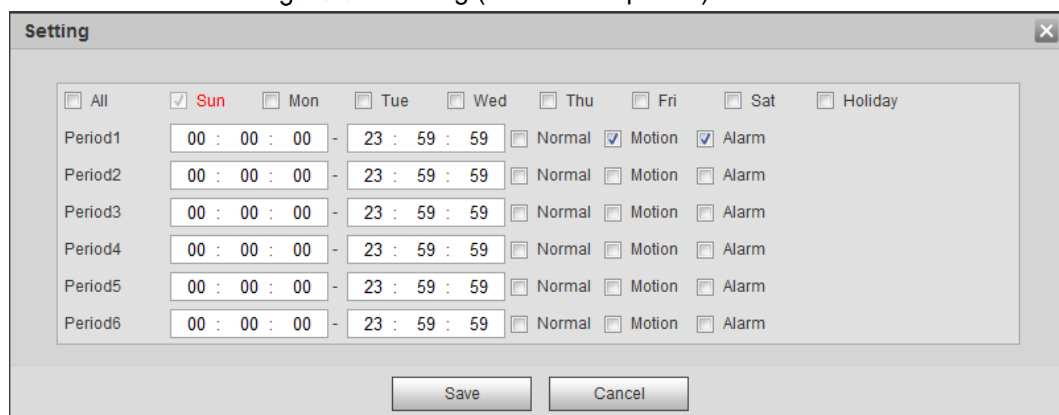
2. Select a day, and the alarm type next to a period, and then set the period.

📖
    ◇ 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**.

5.1.1.3.2 Configuring 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 "3.3.2.4 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. ● **Stop**: Stop recording when the disk is full. ● **Overwrite**: Cyclically overwrite the earliest video when the disk is full.

Parameter	Description
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**.

5.1.1.3.3 Configuring Record Linkage

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

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

Figure 5-6 Record linkage

5.1.1.4 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 "3.3.2.4 Path".

5.1.1.4.1 Configuring 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
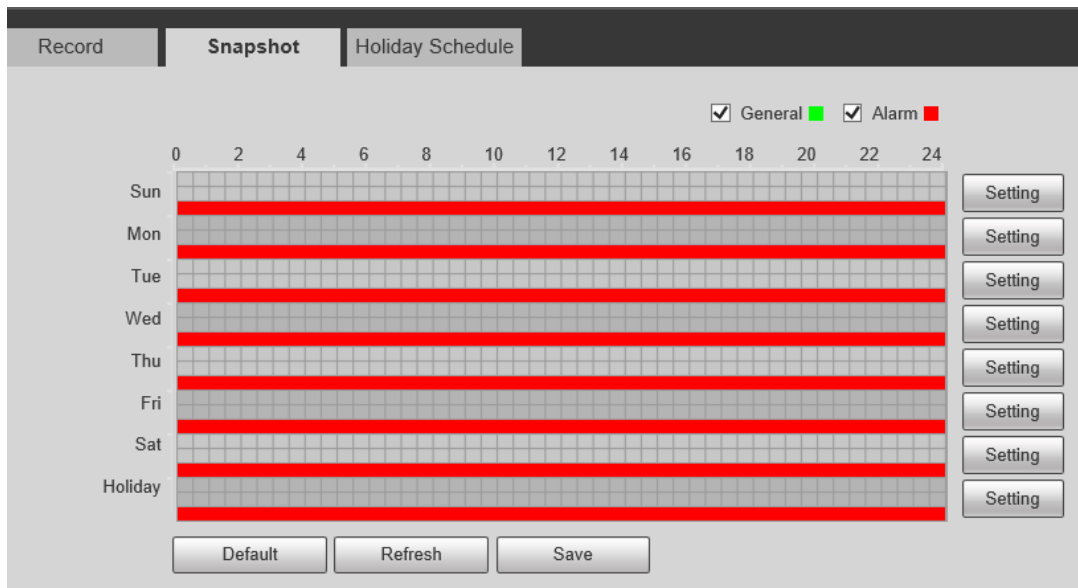
Step 2 Select snapshot type and set time period.

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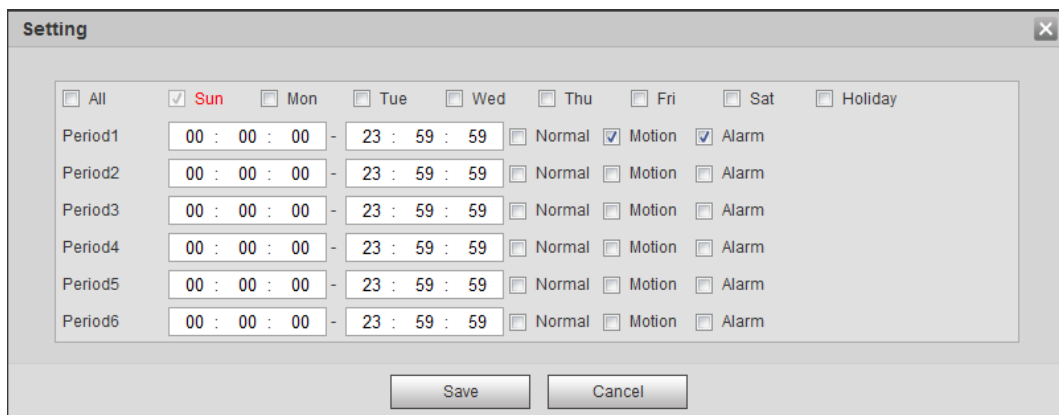
  2. Select a day, and the alarm type next to a period. Then set the period.

◇ 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**.

5.1.1.4.2 Configuring Snapshot Linkage

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

Figure 5-9 Snapshot linkage

☐ Snapshot

5.1.1.5 Relay-out Linkage

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

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

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

Figure 5-10 Relay-out linkage

☑ Relay-out | 1 | 2 |

Alarm Delay | 10 | s (10~300)

5.1.1.6 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 "3.4.5 SMTP (Email)".

Figure 5-11 mail linkage

☐ Send Email

5.1.1.7 White Light Linkage

When an alarm is triggered, the system can automatically enable the white light.

Set **Mode**, **Flicker Frequency**, and **Duration**.

● **Mode**: The display mode of the white light when an alarm is triggered. It includes **Normally on** and **Flicker**. When set flicker as the mode, you need to set the flicker frequency.

- **Duration**: After setting white light duration, the white light is turned off after an extended time of period after an alarm. It is 5 seconds–30 seconds.

5.1.1.8 Audio Linkage

The system broadcasts alarm audio file when an alarm event occurs. Select **Setting > Radar Settings > Region** 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
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 "5.3.1 SD Card Abnormality".
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 "5.3.1 SD Card Abnormality".
External Alarm	The alarm is triggered when there is external alarm input.	The device has alarm input port and external alarm function is enabled.
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 "5.3.3 Configuring Illegal Access.
Audio Detection	The alarm is triggered when there is audio connection problem.	Abnormal audio detection is enabled.
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
Security Exception	The alarm is triggered when the device detects malicious attack.	Voltage detection is enabled. For details, see "5.3.4 Configuring Security Exception".
Radar Alarm	The alarm triggered by radar.	Enable radar alarm function.

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)

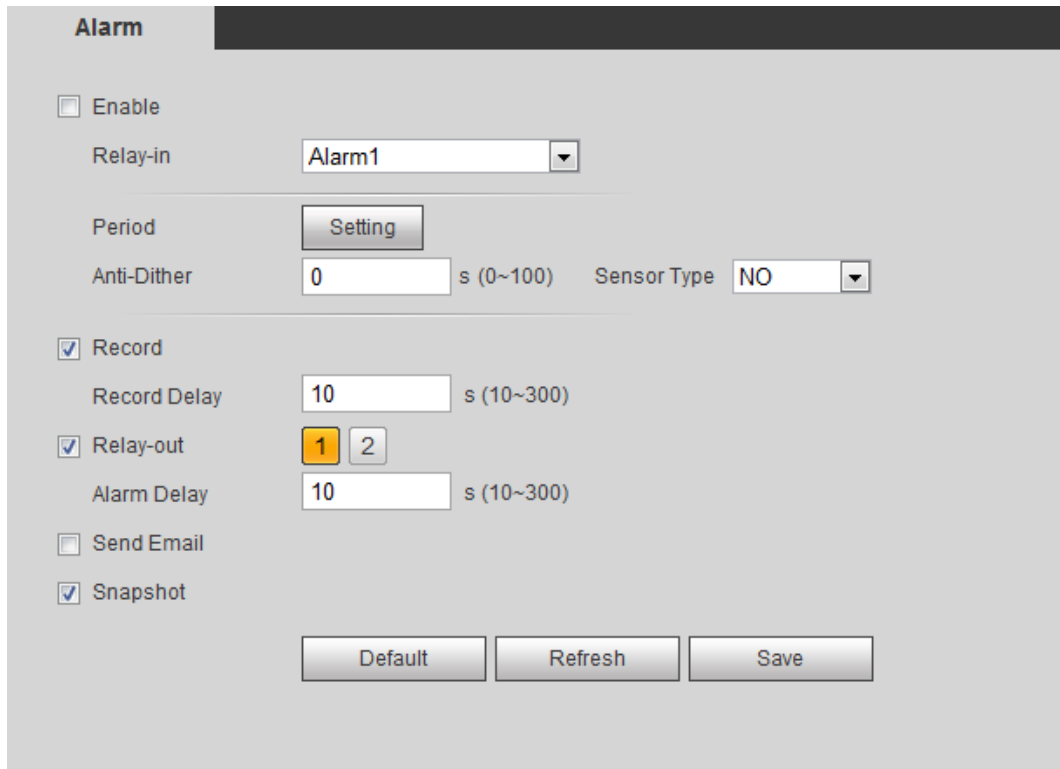Step 2   Select **Alarm Type** according to the actual need.

● 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 on 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 Configuring Relay-in

When an alarm is triggered at the alarm-in port, the system performs alarm linkage.

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

Figure 5-14 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**.

5.3 Configuring Abnormality

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

$\square$

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

5.3.1 SD Card Abnormality

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 > Exception Handling > SD Card**.

Figure 5-15 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".
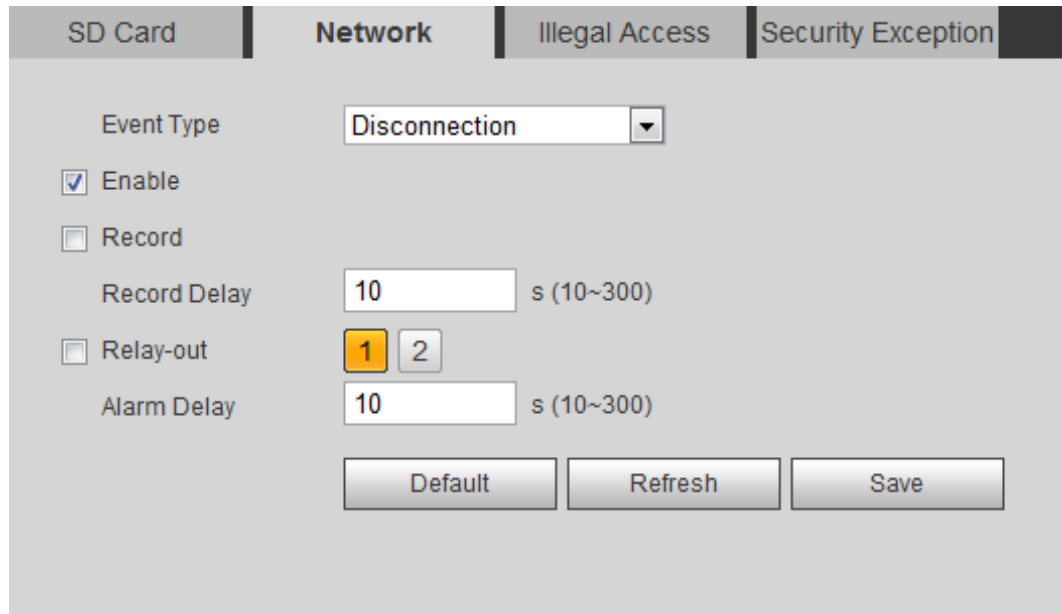
Step 4　Click **Save**.

5.3.2 Network Abnormality

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 5-16 Network

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**.

5.3.3 Configuring Illegal Access

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

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

Figure 5-17 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 defined value, the account will be locked.

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

Step 5   Click **Save**.

5.3.4 Configuring Security Exception

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

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

Figure 5-18 Security exception

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

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

Step 4   Click **Save**.

6 Maintenance

6.1 Requirements

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

● Check surveillance images regularly.

● Clear regularly user and user group information that are not frequently used.

● Change the password every three months.

● View system logs and analyze them, and process the abnormity in time.

● Back up the system configuration regularly.

● Restart the device and delete the old files regularly.

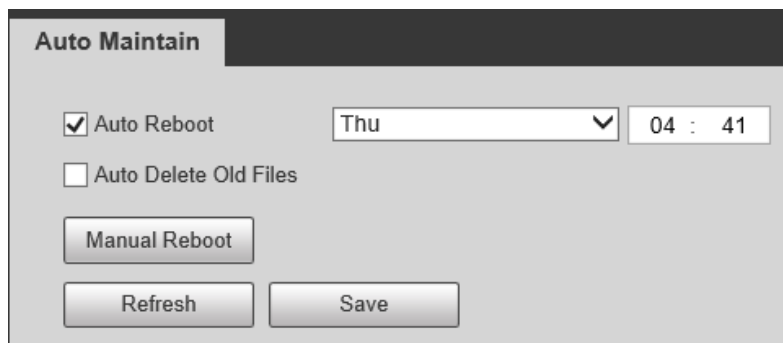● Upgrade firmware in time.

6.2 Auto Maintenance

You can restart the system manually, and set the time of auto reboot and auto deleting old files.

This function is disabled by default.

Step 1   Select **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.

● 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.

Procedure

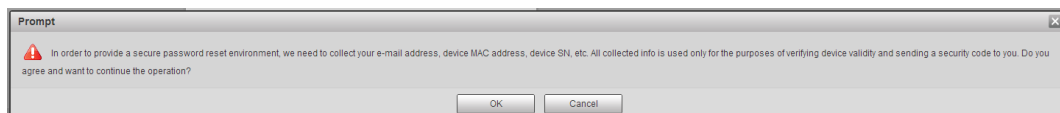Step 1　Open IE browser, enter the IP address of the device in the address bar and press Enter.

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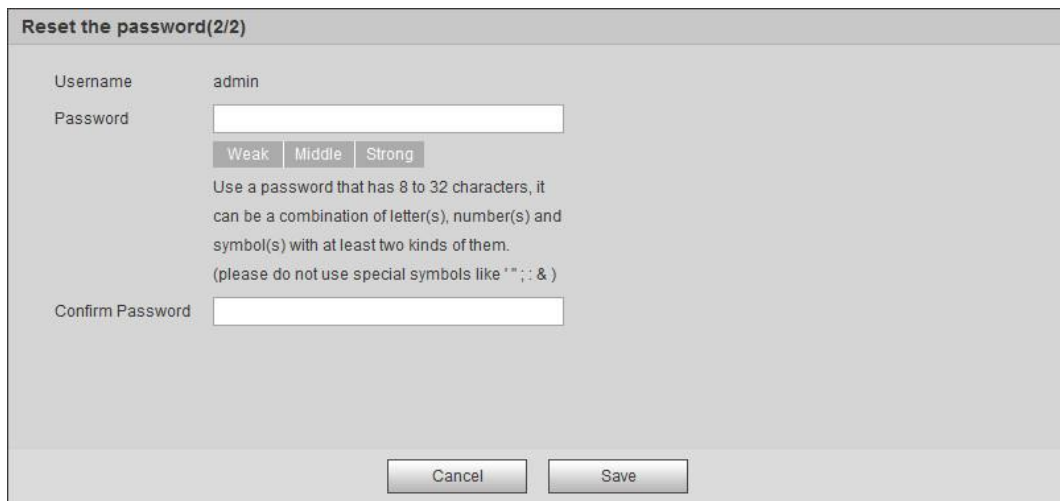
Step 5   Scan the QR code, and there will be a security code sent to the email address you entered. Enter the security code as instructed.

⚠️

● 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)

```
Reset the password(2/2)

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

Confirm Password [                    ]

                        [Cancel]    [Save]
```

Step 7   Reset and confirm the password.

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

Step 8   Click **Save**.

The login interface is displayed.

6.4 Backup and Default
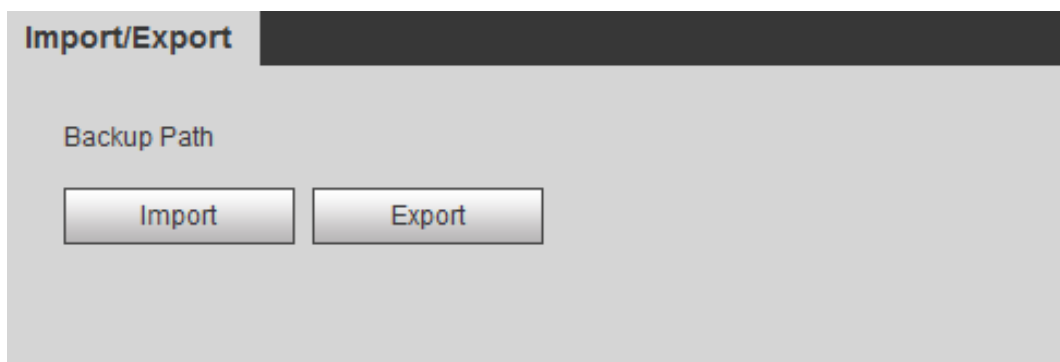
6.4.1 Import/Export

- 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

```
Import/Export

Backup Path

    [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.

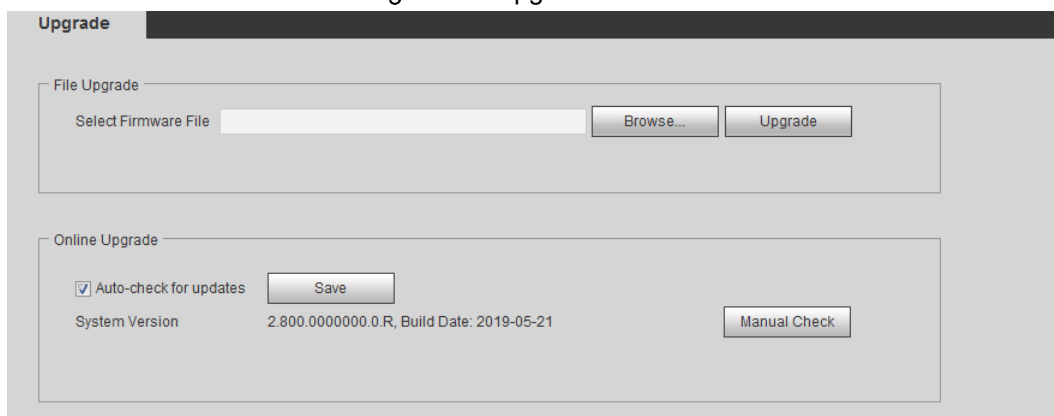Figure 6-7 Default
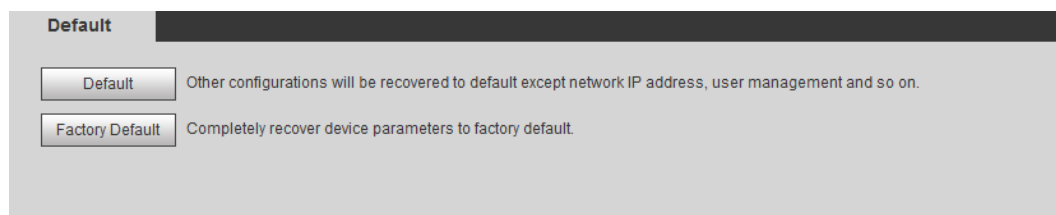
6.5 Upgrade

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

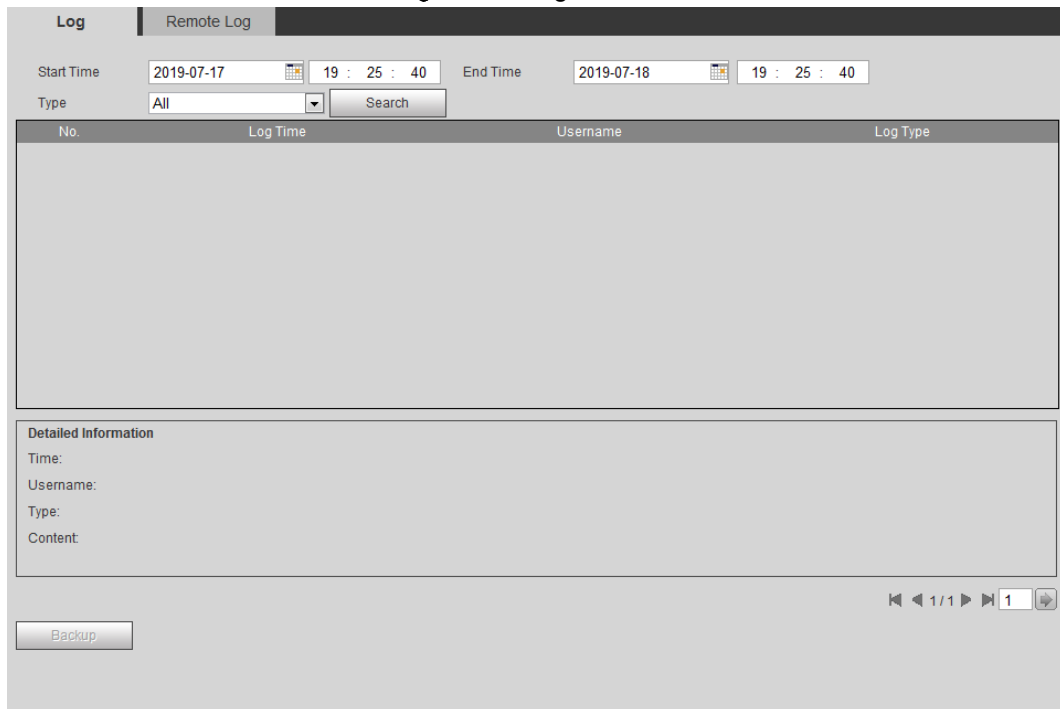You can view device information such as hardware, system version, and web version.

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.
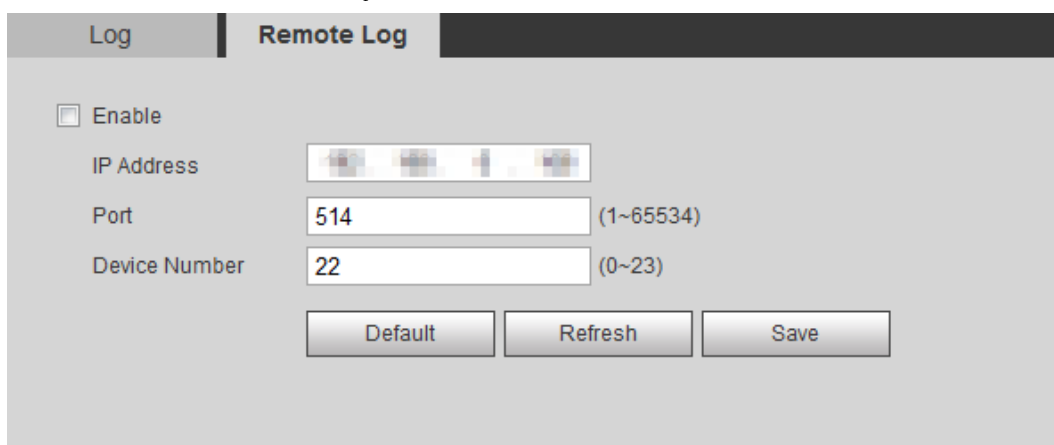
Figure 6-10 Log (details)
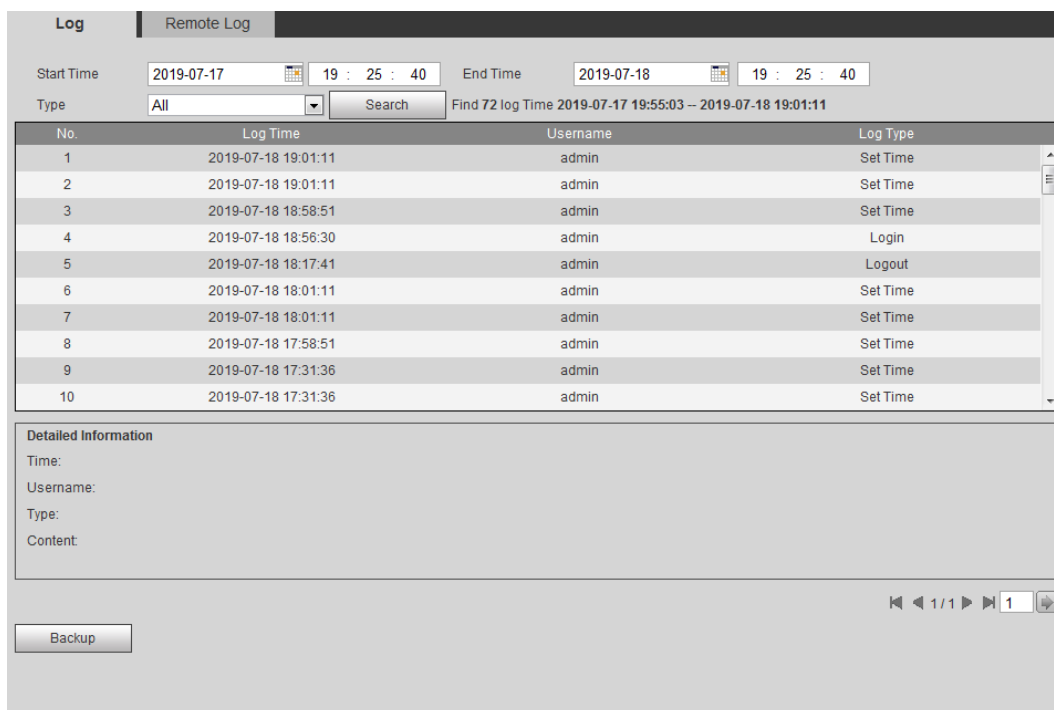
6.6.3 Remote Log

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

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

Figure 6-11 Remote Log

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

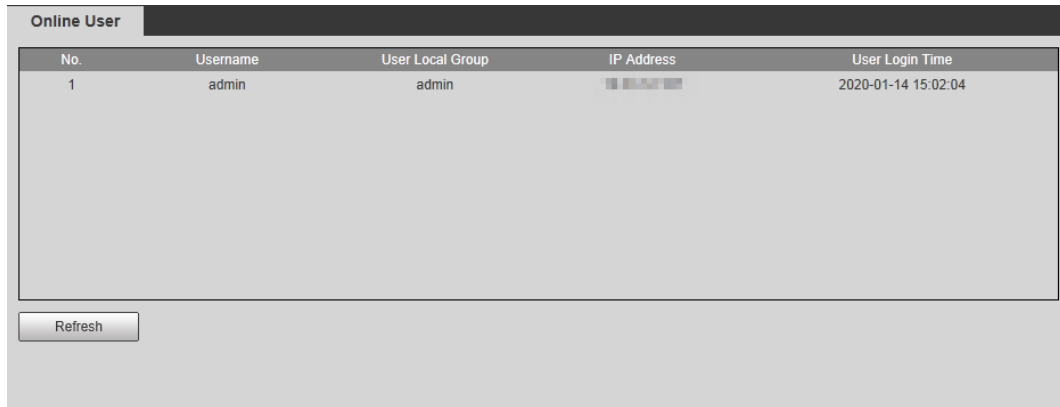Step 3　Set address, port and device number.

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

7 Logout

Click **Logout** tab. The login interface is displayed.

Figure 7-1 Logout interface

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 device 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 device (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 device 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 device network security:

1. **Physical Protection**

   We suggest that you perform physical protection to device, especially storage devices. For example, place the device 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 device (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 device 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 device, 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 device 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 device, 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 device 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