



Radar Terminal Controller

User Manual



V1.1.1

Foreword

General

This manual introduces the appearance and installation of floor bracket for face recognition access controller.

Safety Instructions

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

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

Revision History

Version	Revision Content	Release Time
V1.1.1	Modify some function descriptions.	August 2026
V1.1.0	• Update the steps of radar configuration. • Update the parameter configuration method for expert mode. • Add the expert mode parameter description.	October 2025
V1.0.0	First release.	May 2025

Privacy Protection Notice

As the device user, you might collect the personal data of individuals such as their names, email addresses, face images, audio and fingerprints. You shall be fully responsible for any activities associated with processing personal data. You commit to comply with your local privacy protection laws and regulations to protect the legitimate rights and interests of individuals, and shall implement measures which are required by applicable law, including but not limited to, providing clear and comprehensive information to individuals before processing their personal data, obtaining consent from individuals when necessary, informing individuals of the existence of the surveillance area, and providing required contact information.

Intelligent Product Usage Statement

Intelligent products utilize AI technology to effectively enhance security. The intelligent recognition and alarm functions of the product might be affected by factors such as environmental lighting, camera angles, object obstructions, and network delays, potentially leading to false alarms, missed alerts, or response delays. This intelligent product is solely intended to be used as a security assistance tool. The results from performing identification are for reference only and do not constitute absolute guarantee of personal or property safety. Users need to combine these products with necessary physical security measures to enhance overall protection. Except as otherwise provided by laws or in the event of intentional or gross negligence on the part of the company, the company shall not be liable for any losses caused by the aforementioned factors not attributable to the company.

About the Manual

- This manual is provided for general reference only. Discrepancies might exist between the product and this manual, including but not limited to printed, electronic, or any other editions.
- The manual will be updated according to the latest laws and regulations of related jurisdictions. Specifications and documentation are subject to change without prior notice. For the latest versions, as well as legal notices, consult the printed manual, the product webpage, our official website, or scan the QR code to access the electronic edition.
- The manual will be updated as necessary to reflect product changes and applicable legal requirements. These updates will not diminish your statutory rights, nor will they remove or weaken the safety information or essential instructions provided at the time of purchase.
- Although we make every effort to ensure accuracy, errors or deviations in descriptions of functions, operations, or technical data might occur. If there is any uncertainty or controversy, we reserve the right of final explanation.
- All trademarks, registered trademarks and company names referenced in this manual are the property of their respective owners.

Table of Contents

Foreword.....	I
1 Start Using Device.....	1
1.1 Network Connection.....	1
1.2 Device Initialization.....	1
1.3 Login.....	2
1.4 Resetting Password.....	3
2 Live View.....	6
2.1 Encoding Mode Bar.....	6
2.2 Video Information and Tool.....	7
2.3 Window Adjustment Bar.....	7
2.4 Function Tab Bar.....	8
2.5 Live View Function Bar.....	8
2.6 Device List.....	9
2.7 PTZ Operation.....	10
3 Playback.....	11
3.1 Playing back Video.....	11
3.1.1 Play Control Bar.....	12
3.1.2 Record Type.....	12
3.1.3 Assistant.....	12
3.1.4 Playback File.....	13
3.1.5 Playback Clipping.....	14
3.1.6 Progress Bar Time Format.....	14
3.2 Playing back Picture.....	14
3.2.1 Play Control Bar.....	15
3.2.2 Snapshot Type.....	15
3.2.3 Playback File.....	16
4 Setting.....	19
4.1 Radar Settings.....	19
4.1.1 Setting Video Parameters.....	19
4.1.2 PTZ Camera.....	27
4.1.3 Radar.....	29
4.1.4 Linkage Wizard.....	30
4.1.5 Setting Region.....	36
4.1.6 Managing Protection Zone.....	42
4.1.7 Setting IVS.....	43
4.2 Network.....	49
4.2.1 TCP/IP.....	49

4.2.2	Port.....	51
4.2.3	PPPoE.....	53
4.2.4	DDNS.....	54
4.2.5	SMTP (Email).....	55
4.2.6	UPnP.....	57
4.2.7	SNMP.....	58
4.2.8	Bonjour.....	61
4.2.9	Multicast.....	61
4.2.10	Auto Register.....	62
4.2.11	802.1x.....	62
4.2.12	QoS.....	63
4.2.13	Assess Platform.....	64
4.3	Event.....	66
4.3.1	Setting Alarm.....	66
4.3.2	Setting Abnormality.....	67
4.4	Storage.....	69
4.4.1	Schedule.....	69
4.4.2	Destination.....	74
4.4.3	Record Control.....	78
4.5	System.....	79
4.5.1	General Settings.....	79
4.5.2	Account.....	80
4.5.3	Safety.....	87
4.5.4	Default.....	94
4.5.5	Import/Export.....	95
4.5.6	Setting Auto Maintain.....	95
4.5.7	Upgrade.....	95
4.6	Information.....	96
4.6.1	Version.....	96
4.6.2	Querying Log.....	96
4.6.3	Online User.....	97
4.6.4	Legal Information.....	98
5	Alarm.....	99
Appendix 1 Parameter Description.....		101
Appendix 2 Important Safeguards and Warnings.....		105
Appendix 3 Security Commitment and Recommendation.....		108

1 Start Using Device

1.1 Network Connection

Before initialization, all radars are assigned a unified IP address (the default is 192.168.1.108).

To ensure smooth network access to the radar, it is necessary to plan the available IP network segments based on the actual network environment.

Figure 1-1 General radar network (1)

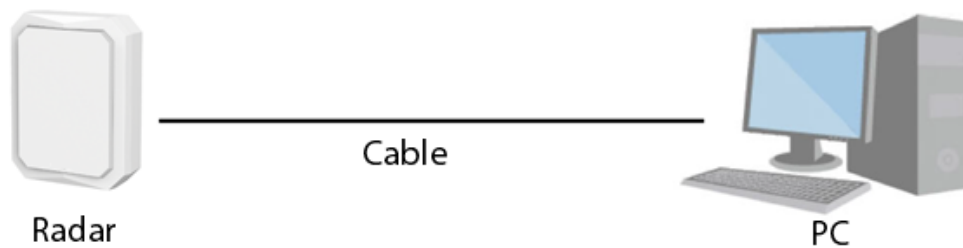
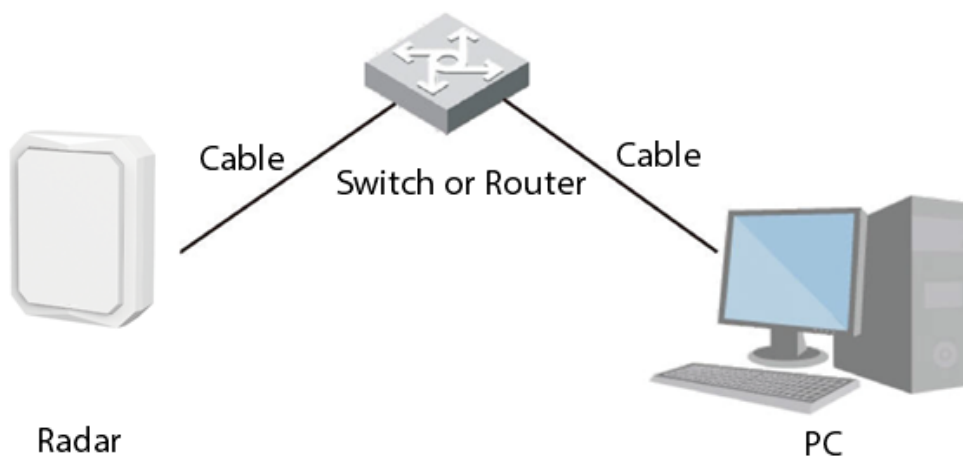


Figure 1-2 General radar network (2)



1.2 Device Initialization

Device initialization is required for the first use.

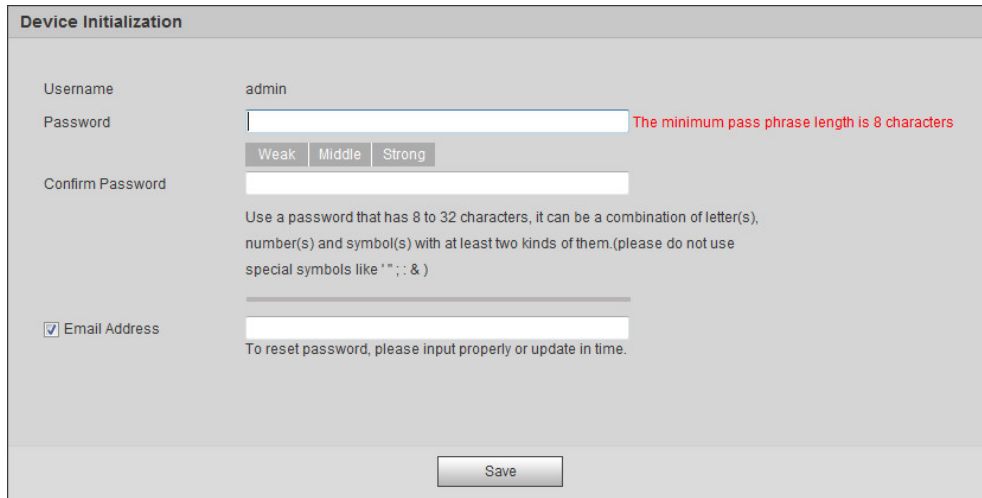
Procedure

- Step 1** Open IE browser, enter the IP address of the device in the address bar, and then press Enter key.
- Step 2** Set the password for admin account.



- 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 ' " ; : &).
- The confirmed password and the new password must be same.
- Set a high security level password according to the password security notice.

Figure 1-3 Device initialization



Device Initialization

Username: admin

Password: The minimum pass phrase length is 8 characters

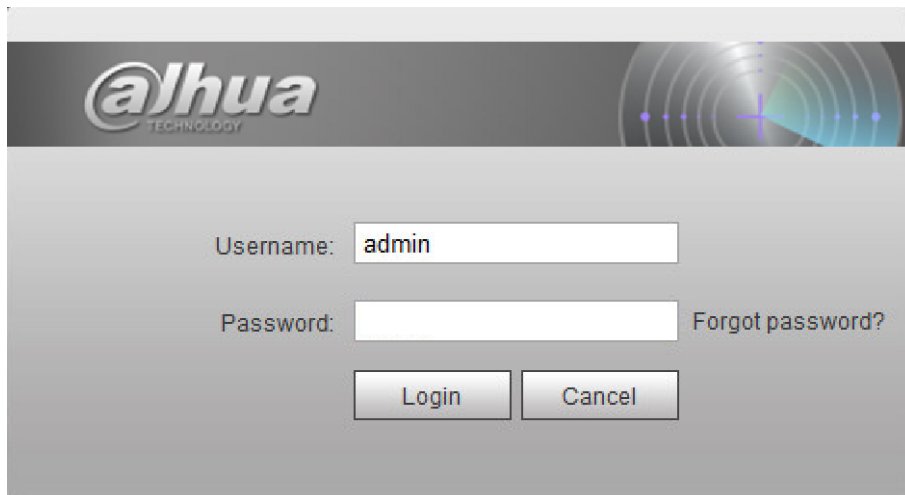
Confirm Password:

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

☒ Email Address

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

Figure 1-4 Log in



dahua TECHNOLOGY

Username:

Password: [Forgot password?](#)

Step 3 Set a mobile phone number for password recovery and click **OK**.



The reserved mobile phone number is used to reset the device password. To ensure the device functions properly, please fill in the reserved mobile phone number whenever possible.

Step 4 Click **Save** in **End-user license agreement** page and then click **Next**.

Step 5 Click **Save** to enter the login page.

1.3 Login

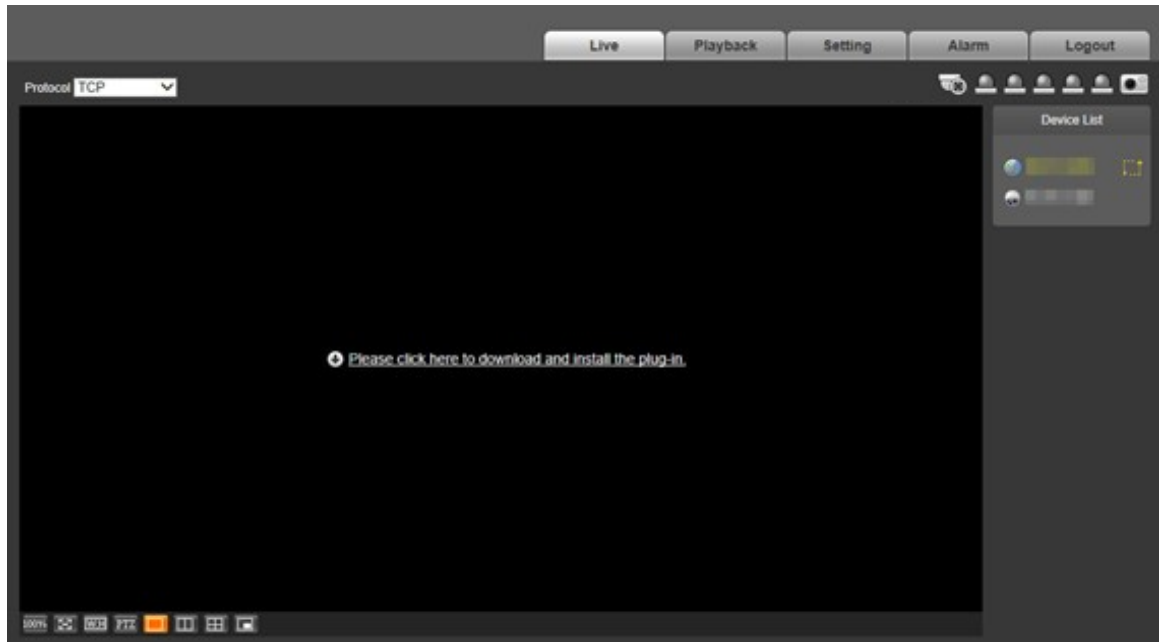
You need to download and install the plug-in for first-time login.

Procedure

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

Step 2 The **Live** page is displayed.

Figure 1-5 Install the plug-in



If you enter the wrong password for 5 times in a row, 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**. Download and install the plug-in according to the on-screen instructions.

Step 3 After the plug-in is installed, the login page is displayed automatically. Enter username and password, and then click **Login**.

Related Operations

- Live: Click **Live** to view the real-time monitoring image.
- Playback: Click **Playback** to play back or download recorded video or image files.
- Setting: Click **Setting** to configure the basic and intelligent functions of the camera.
- Alarm: Click **Alarm** to subscribe and view alarm information.
- Logout: Click **Logout** to go to login page.
- The system will sleep automatically after idling for a period of time.

1.4 Resetting Password

You can reset the admin password through the reserved email address when you forget it.

Procedure

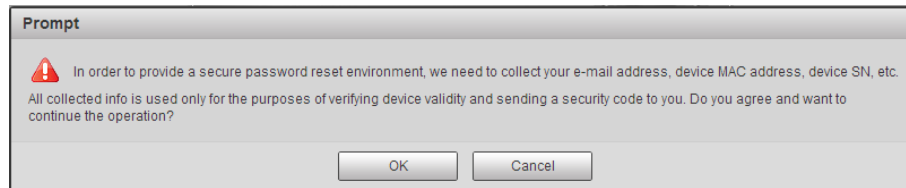
Step 1 Open IE browser, enter the IP address of the controller in the address bar, and then press **Enter**.

The login page is displayed.

Step 2 Click **Forgot password?**

The **Prompt** page is displayed.

Figure 1-6 Prompt

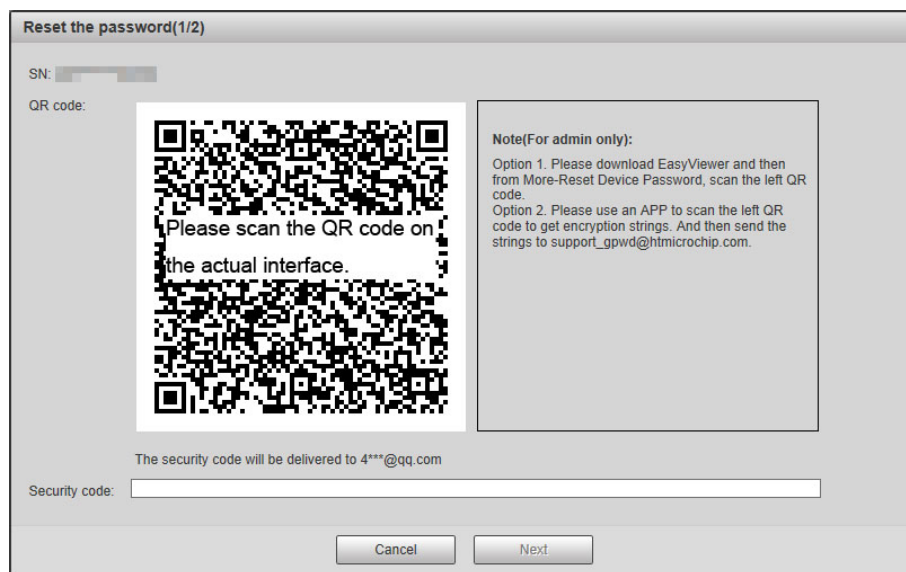


Step 3 Click **OK** and the QR code scanning page is displayed.



After clicking **OK**, your information such as email address, MAC address, and device SN might be collected for authentication.

Figure 1-7 QR code

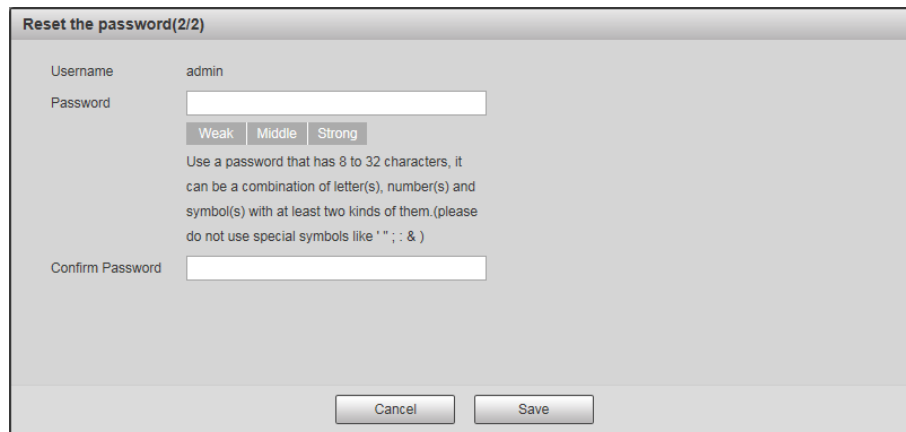


Step 4 Read notes and scan the QR code. Enter security code acquired from the reserved email and then click **Next** and the password resetting page is displayed.



Reset the password within 24 hours after you get the security code; otherwise it will be invalid. If the security code is not used twice continuously, for the third time, the system will prompt that you fail to acquire the security code. For normal use of the device, you need to restore the device to default and then acquire the security code again, or acquire the security code after 24 hours.

Figure 1-8 Reset the password

A screenshot of a web-based password reset dialog box titled "Reset the password(2/2)". The dialog has a light gray background. It contains a "Username" field with the text "admin". Below it is a "Password" field, which is currently empty. To the right of the password field are three buttons labeled "Weak", "Middle", and "Strong". Below these buttons is a text prompt: "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 ' " ; : &)". Below the prompt is a "Confirm Password" field, also empty. At the bottom right of the dialog are two buttons: "Cancel" and "Save".

Step 5 Set the new admin password and then confirm it.



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 characters (excluding ' " ; : &). Follow the password strength prompt to set a password with high security.

Step 6 Click **Save**.

The login page is displayed.

2 Live View

You can do the operations such as watching live video, taking snapshots and records, and setting up video stream.

Figure 2-1 Live view

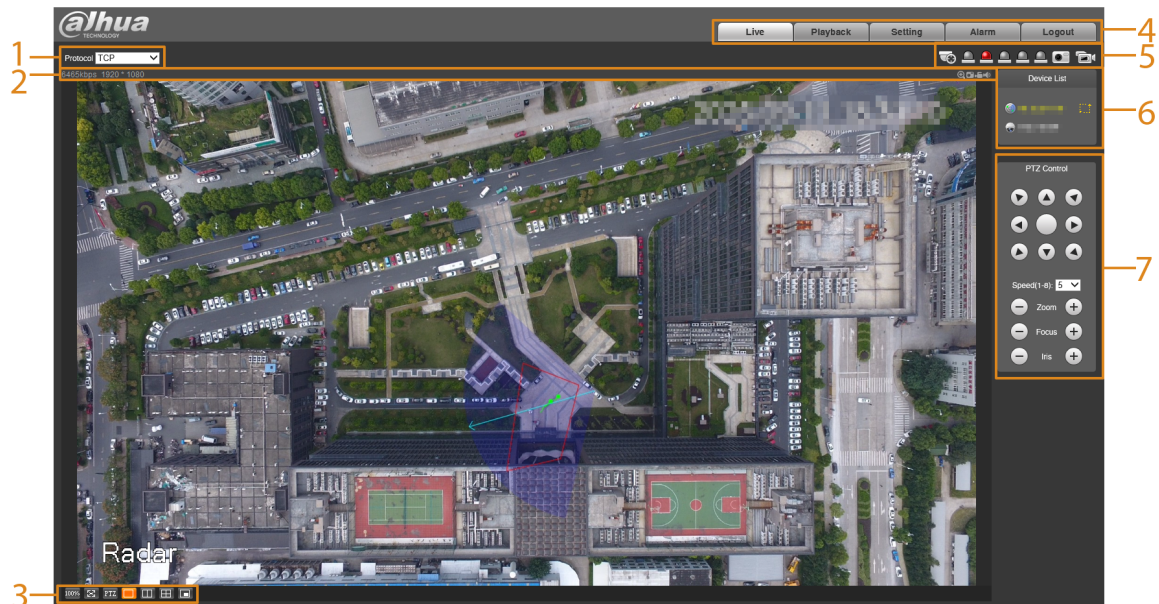


Table 2-1 Description of function bar

No.	Function	Description
1	Encoding mode bar.	For details, see "2.1 Encoding Mode Bar".
2	Video information and tool.	For details, see "2.2 Video Information and Tool".
3	Window adjustment bar.	For details, see "2.3 Window Adjustment Bar".
4	Function tab bar.	For details, see "2.4 Function Tab Bar".
5	Live view function bar.	For details, see "2.5 Live View Function Bar".
6	Device list.	For details, see "2.6 Device List".
7	PTZ operation.	For details, see "2.7 PTZ Operation".

2.1 Encoding Mode Bar

Figure 2-2 Encoding mode



You can select the network transmission protocol as needed, and the options are **TCP** , **UDP** and **Multicast**.



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

2.2 Video Information and Tool

Figure 2-3 Video tool



Table 2-2 Video tool description

No.	Parameter	Description
1	Bitrate	Show the current bitrate.
2	Resolution	Show the current resolution.
3	Local magnification	- Click the icon to zoom in on any part of the video when it is in its original state. When the video is not in its original state, you can drag the zoomed-in area within a certain range and right-click to revert it to its original state. - Click the icon to zoom in or out of the video image by rolling the mouse wheel.
4	Snapshot	Click the icon to take a screenshot of the video.
5	Record	Click the icon to record the video.
6	Audio	Click the icon to enable or disable audio output.

2.3 Window Adjustment Bar

Figure 2-4 Adjust video window



Table 2-3 Adjust video window description

No.	Parameter	Description
1	Original size	Click this icon to display the actual size of the video stream.
2	Full screen	Click this icon to display in full screen. You can also double-click the screen or press the Esc key to exit full screen.
3	PTZ	Click this icon to open the preview page and display the PTZ configuration items.

No.	Parameter	Description
4	Single picture mode	Click this icon and the video preview screen will display the radar preview screen by default.
5	2-Picture mode	Click this icon to display 2 video frames in the preview screen.
6	4-Picture mode	Click this icon to display 4 video frames in the preview screen.
7	Picture-in-Picture	Click this icon to show the video preview in picture-in-picture mode.

2.4 Function Tab Bar

Click the tab to enter corresponding page.

Figure 2-5 Function tabs



2.5 Live View Function Bar

Figure 2-6 Function option

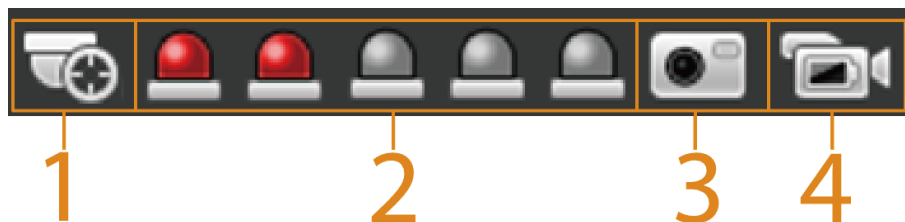


Table 2-4 Function option description

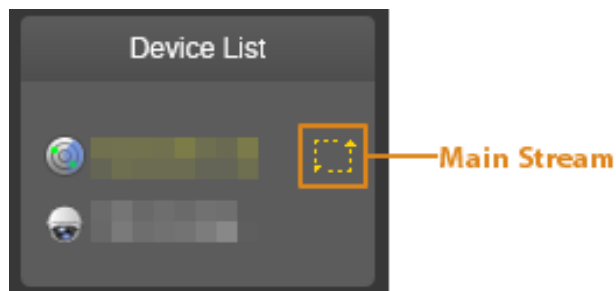
No.	Parameter	Description
1	Manual positioning	Click this icon and then use the mouse to click anywhere on the radar map screen, and all connected dome cameras will quickly locate the area.  - You need to log in to the speed dome camera web page in advance and complete the linkage between the radar and the speed dome camera. - Manual positioning is only supported in 2-picture, 4-picture, or picture-in-picture mode. - If there is no other operation after clicking this icon, the speed dome will return to the default action after 30 seconds.
2	Alarm output	Click this icon to activate the alarm. When the alarm is triggered/ canceled, the light will change to red/gray.

No.	Parameter	Description	
3	Screenshot	Click this icon to take a screenshot of the video.	 Only capture and record images for the radar channel.
4	Video	Click this icon to record the video.	

2.6 Device List

Displays the radar IP address and the IP address of the linked dome camera.

Figure 2-7 Device list



Click  to display **Stream selection**.

Figure 2-8 Stream selection

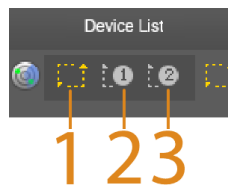


Table 2-5 Device list description

No.	Parameter	Description
1	Main stream	Connect with the protocol selected by the streaming media, and preview or close the video under the main stream configuration. It is generally used for storage and preview.
2	Sub stream1	Connect with the selected streaming protocol and preview or disable the video in the configuration of sub stream 1. When the network bandwidth is insufficient, it is used to replace the main stream for network preview.
3	Sub stream2	Connect with the selected streaming protocol and preview or disable the video in the sub stream 2 configuration. When the network bandwidth is insufficient, it is used to replace the main stream for network preview.

2.7 PTZ Operation

Control the linked dome camera through the PTZ control page.



- The PTZ control page is only for the linkage function. You can skip if it is not needed.
- The PTZ control page is only for the selected dome camera channel.

Figure 2-9 PTZ control page

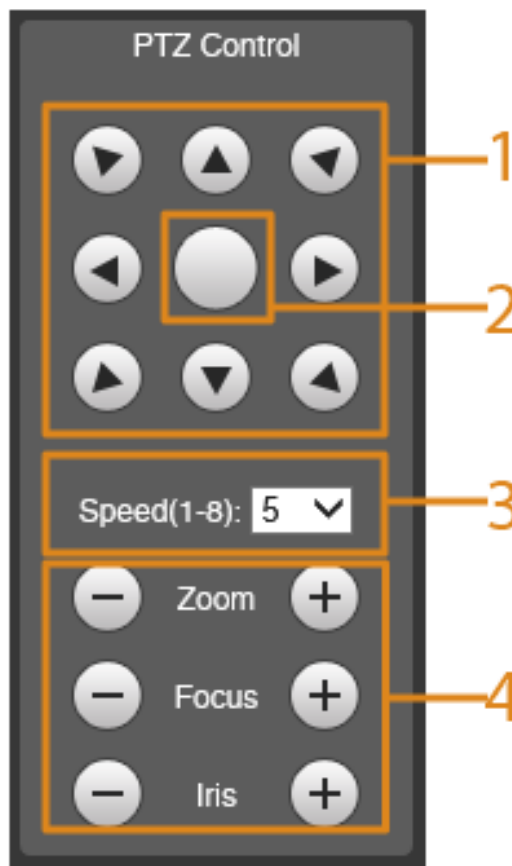


Table 2-6 PTZ control page description

No.	Parameter	Description
1	Direction icon	Supports 8 directions: up, down, left, right, upper left, upper right, lower left, and lower right.
2	Quick positioning	Quick positioning function. Use the mouse to draw a frame on the preview screen, and the PTZ will rotate and zoom to quickly locate the scene.
3	Step length	Refers to the speed at which the gimbal direction changes. The larger the step size you set, the faster the speed you will get.
4	Zoom, focus, aperture	Click  to increase the corresponding parameter value. Click  to decrease it.

3 Playback

You can play back snapshots and videos saved in SD card.



- Snapshot and video playback configurations are only for radar on this web.
- Before playback, you need to configure parameters such as record and snapshot schedule, storage method, and record mode.

Click **Playback** tab. The **Playback** page is displayed.

3.1 Playing back Video

Select **File Type** as **.dav**. On the home page, select playback-file type, and then select **.dav**.

Figure 3-1 Playback video

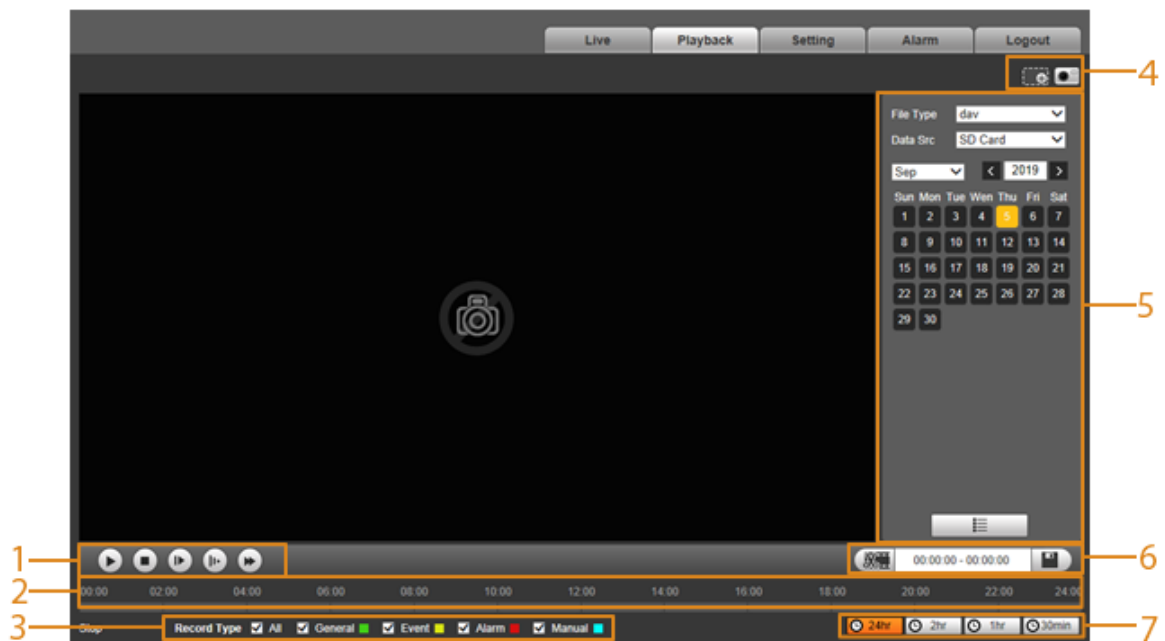


Table 3-1 Playback page description

No.	Function
1	Play control bar
2	Progress bar
3	Record type
4	Assistant
5	Playback video
6	Video clip
7	Time format of progress bar

3.1.1 Play Control Bar

Figure 3-2 Play control bar

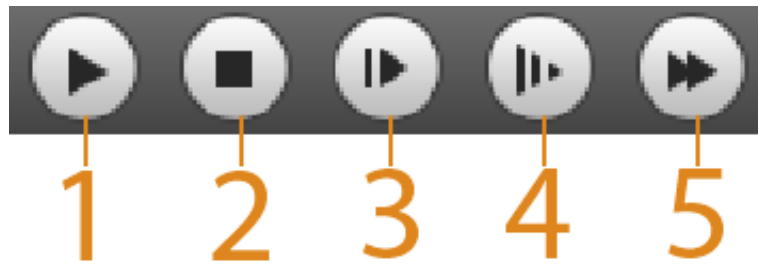


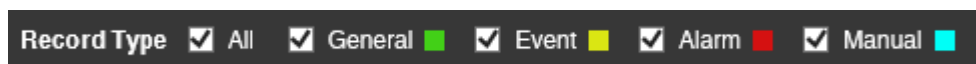
Table 3-2 Play control bar description

No.	Function
1	Click the icon to play back recorded videos.
2	Click the icon to stop playing back recorded videos.
3	Click the icon to play the next frame.
4	Click the icon to slow down the playback.
5	Click the icon to speed up the playback.

3.1.2 Record Type

Select the record video type.

Figure 3-3 Record type



3.1.3 Assistant

Figure 3-4 Assistant

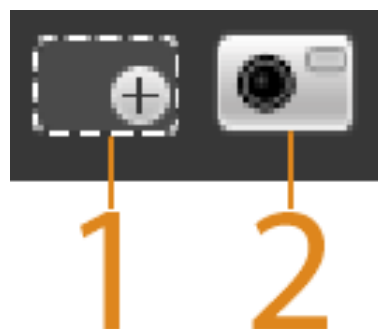


Table 3-3 Assistant description

No.	Icon	Description
1		Zoom in or out video images of the selected area through two operations.
2		Click the icon to capture one picture of the current video, and it will be saved to the configured storage path.

3.1.4 Playback File

Dates with a blue background in the calendar indicate that there are video or screenshot files for the current date.

Figure 3-5 Playback file

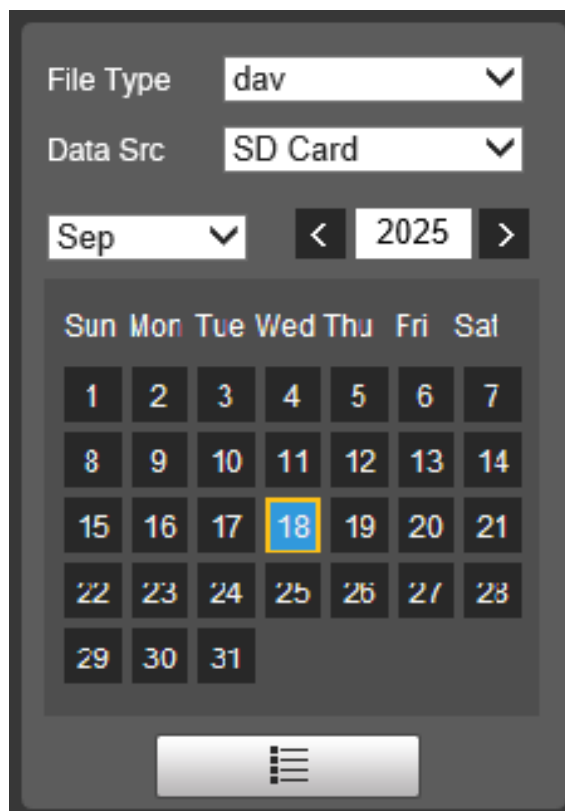


Table 3-4 Playback file description

Parameter/Icon	Description
File Type	Select dav which indicates video playback.
Data Src	Default is the SD card.
	The file list. After clicking, the video files of the selected date will be displayed in the list.

3.1.5 Playback Clipping

Procedure

- Step 1** Click the start time on the timeline. This time must be within the recording file progress bar area.

Figure 3-6 Playback clipping



- Step 2** Move the mouse over the  and **select a start time** appears in the lower right corner.
- Step 3** Click  and set the start time on playback trimming completely.
- Step 4** Click the end time on the timeline. This time must be within the recording file progress bar area.
- Step 5** Move the mouse over the  and **select a end time** appears in the lower right corner.
- Step 6** Click  and set the end time on playback trimming completely.
- Step 7** Click **OK**.

The playback stops and the clipped file is saved in the configured storage path. For the configuration of storage path, see "4.4.2.1 Path".

3.1.6 Progress Bar Time Format

Figure 3-7 Progres bar time Format



Table 3-5 Progress bar time format description

Icon	Description
	The whole progress stands for 24 hours.
	The whole progress stands for 2 hours.
	The whole progress stands for 1 hour.
	The whole progress stands for 30 minutes.

3.2 Playing back Picture

Select **File Type** as **.jpg**.

Figure 3-8 Playback picture

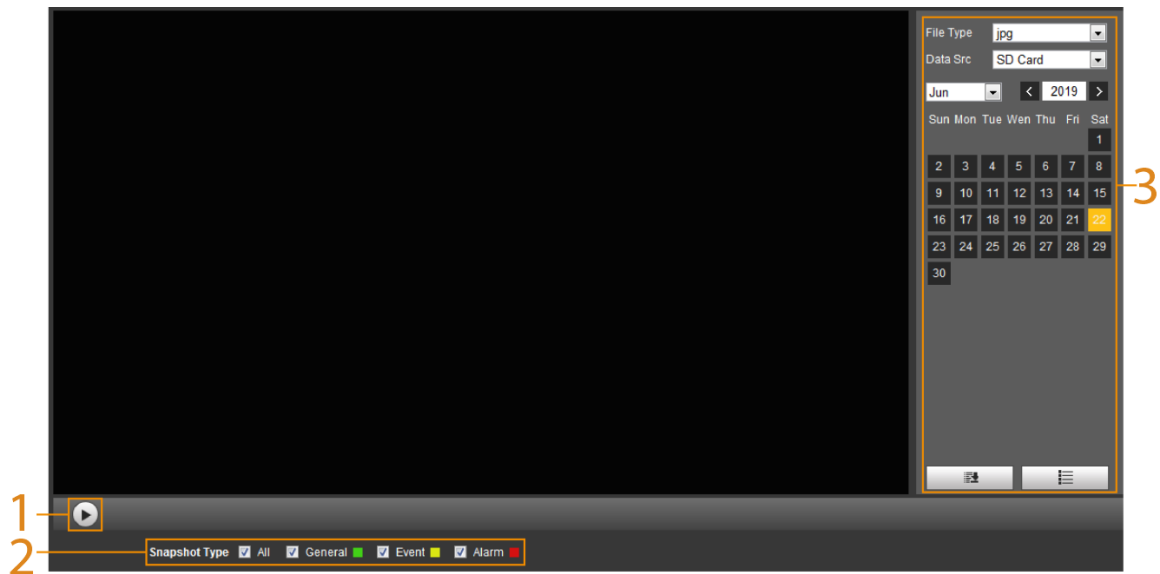
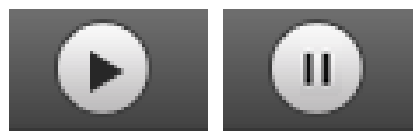


Table 3-6 Playback page description

No.	Function
1	Play control bar
2	Snapshot type
3	Playback file

3.2.1 Play Control Bar

Figure 3-9 Play control bar



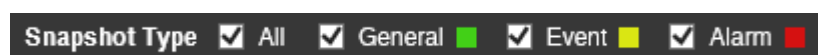
The default status icon is . The image indicates not playing or paused.

- Click the play button to switch to normal playback mode. At this time, the icon appears as .
- Click the pause button to switch to the pause playback state.

3.2.2 Snapshot Type

Select the snapshot type.

Figure 3-10 Snapshot type



3.2.3 Playback File

Figure 3-11 Playback file (1)

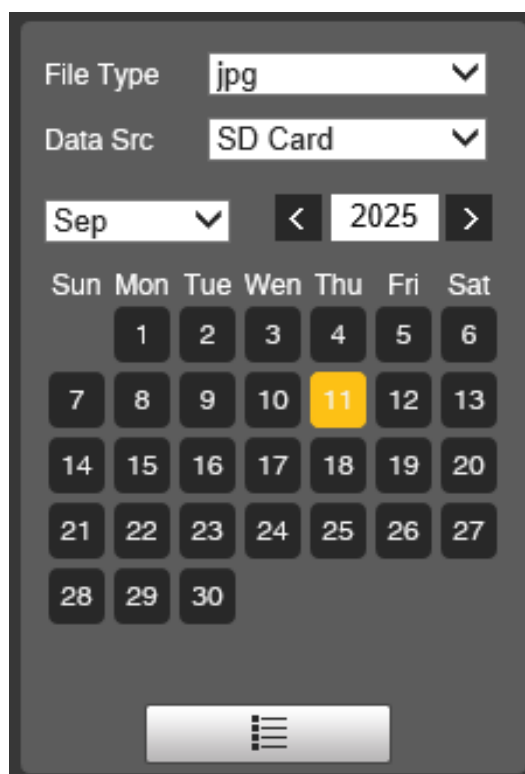


Table 3-7 Playback file description (1)

Parameter Icon	Description
File Type	Select jpg : indicates picture playback.
Data Src	Default is the SD card.
	The file list. After clicking, the picture files of the selected date will be displayed in the list.

Figure 3-12 Playback file (2)



1. Click  and the screenshot files of the selected date will be displayed in the list.
2. Double-click the file in the list to play the screenshot.

Table 3-8 Playback file description (2)

Icon	Description
	Search all screenshot files within the specified time frame and date that you entered.

Icon	Description
	Download the screenshot file to your computer.
	Please return to the calendar page and select the time again.

4 Setting

This chapter introduces how to configure and view the radar information, including settings about radar, network, event, storage, and system.

4.1 Radar Settings



Move the mouse on  to view the parameter meanings.

4.1.1 Setting Video Parameters

Set the radar's video stream, image stream, video overlay, and storage path.

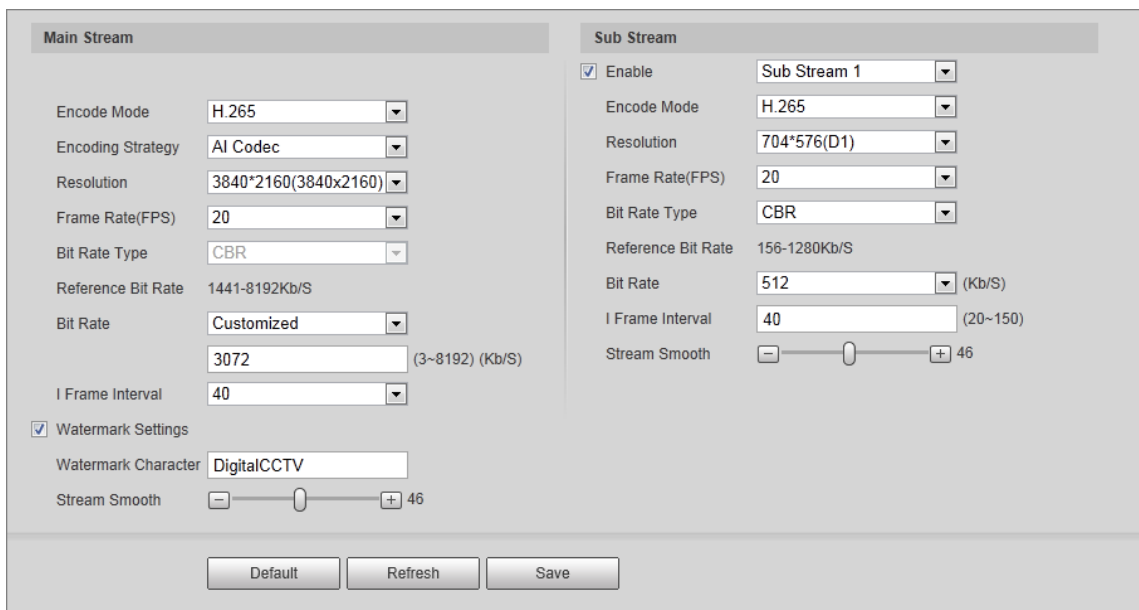
4.1.1.1 Video

Configure video stream parameters.

Procedure

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

Figure 4-1 Video



The screenshot displays the Video Settings interface, divided into two main sections: Main Stream and Sub Stream.

Main Stream Settings:

- Encode Mode: H.265
- Encoding Strategy: AI Codec
- Resolution: 3840*2160(3840x2160)
- Frame Rate(FPS): 20
- Bit Rate Type: CBR
- Reference Bit Rate: 1441-8192Kb/S
- Bit Rate: Customized (3072 Kb/S)
- I Frame Interval: 40
- Watermark Settings:
 - Watermark Character: DigitalCCTV
 - Stream Smooth: 46

Sub Stream Settings:

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

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

Step 2 Configure video parameters.

Table 4-1 Description of video parameters

Parameter	Description
Enable	Select the Enable check box to enable sub stream. It is enabled by default.  - You can enable multiple sub streams simultaneously. - Intelligent event and sub stream 2 are closed automatically when enables image correction.
Encode Mode	Select encode mode. H.264 : Main profile encode mode. Compared with H.264B, it requires smaller bandwidth. H.264H : High profile encode mode. Compared with H.264, it requires smaller bandwidth. H.264B : Baseline profile encode mode. It requires smaller bandwidth. H.265 : Main profile encode mode. Compared with H.264, it requires smaller bandwidth. MJPEG : Under this mode, the image requires high bit rate value to ensure clarity, you are recommended to set the Bit Rate value to the biggest value in the Reference Bit Rate.
Encoding Strategy	Select the encoding strategy as needed. - General: Disable smart codec. - Smart Codec: Enable smart codec to improve video compressibility and save storage space. It is applicable to static scenes. - AI Code: When the bandwidth and storage space are restricted, the camera will select the encoding strategy with lower bit rate to save storage space. It is applicable to dynamic scenes. After AI codec is enabled, Bit Rate Type is CBR, and it cannot be changed. Comparing with general mode, AI codec has lower bite rate. This function is only available on cameras with AI functions.  This function is only available on cameras with AI functions.  After smart codec and AI codec are enabled, the camera would stop supporting the third stream, ROI, and smart event detection. Pages might vary on different models.
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.

Parameter	Description
Video Clip	This function is available only for sub stream 2 of some selected models. • Main stream 1. Select the resolution as needed, and click  next to Resolution. 2. Clip the image on the Area page, and then click Save. View the clipped video on Live page. • Sub stream 2 1. Select Video Clip, and click . 2. View the clipped video on Live page (only the live page of sub stream 2 displays the clipped area).
Frame Rate (FPS)	The number of frames 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. • 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.  The Bit Rate Type can only be set as CBR when Encode Mode is set as MJPEG.
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. You can also customize the value.

Parameter	Description
I Frame Interval	This parameter can be configured only when Encoding Strategy is set as General or AI Codec. The number of P frames between two I frames. The smaller the value, the higher the image quality, and the range changes as Frame Rate(FPS) changes. We recommend you set I Frame Interval twice as big as Frame Rate(FPS). When selecting AI Codec in Encoding Strategy, you can only select the value same as or twice as big as Frame Rate(FPS).
SVC	Scaled video coding, able to encode a high quality video bit stream that contains one or more subset bit streams. When sending stream, to improve fluency, the system will quit some data of related lays according to the network status. 1: The default value, which means that there is no layered coding. 2, 3 and 4: The lay number that the video stream is packed.
Watermark Settings	You can verify the watermark to check if the video has been tampered. 1. Select the check box to enable watermark function. 2. The default character is DigitalCCTV.
Watermark Character	
Stream Smooth	Click ,  or drag  to set the value of Stream Smooth. The higher the value is, the less smooth the stream, but the higher the image definition; the lower the value is, the smoother the stream, but the lower the image definition.  The value of Stream Smooth is 100 by default.

Step 3 Click **Save**.

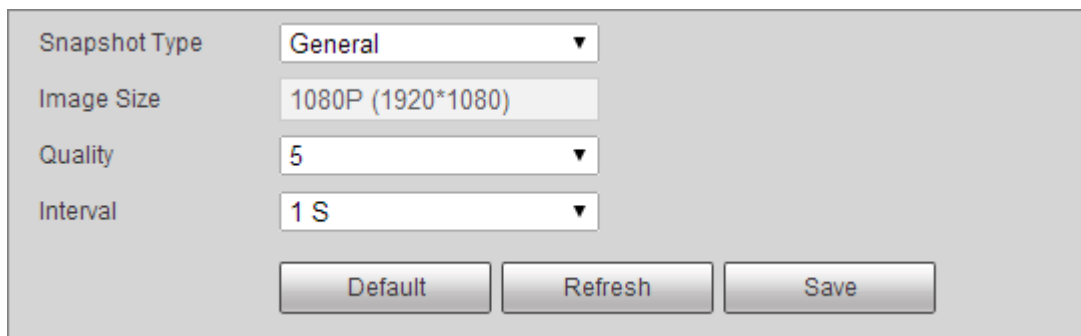
4.1.1.2 Snapshot

Configure snapshot parameters.

Procedure

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

Figure 4-2 Snapshot



Step 2 Configure snapshot parameters.

Table 4-2 Description of snapshot parameter

Parameter	Description
Snapshot Type	You can select General or Event . • General : The system takes snapshot as scheduled. • Event : The system takes snapshot when the video detection, audio detection, event, or alarm is triggered.
Image Size	The same resolution with main stream.
Quality	Configure the snapshot quality. There are six levels of image quality, and the sixth is the best.
Interval	Configure the snapshot frequency.

Step 3 Click **Save**.

4.1.1.3 Overlay

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

Procedure

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

Step 2 Configure video overlay information as needed.

Figure 4-3 Overlay-channel title

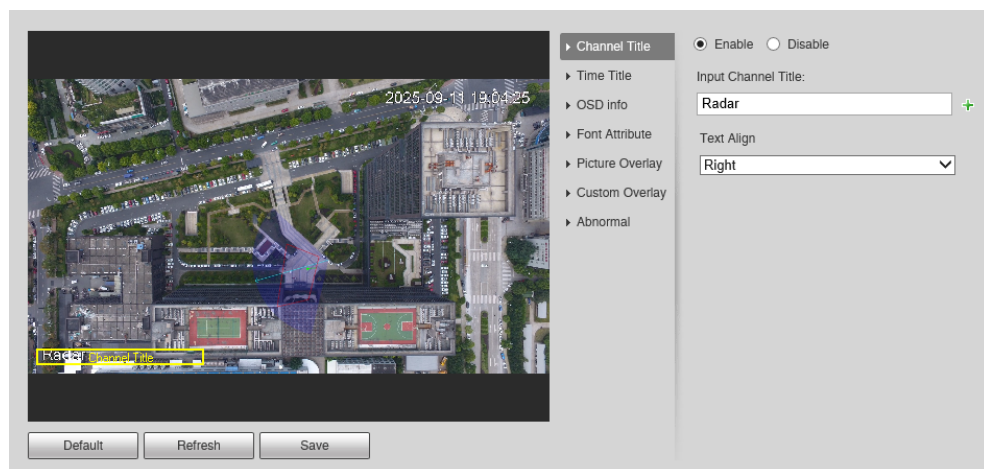


Figure 4-4 Overlay-time title

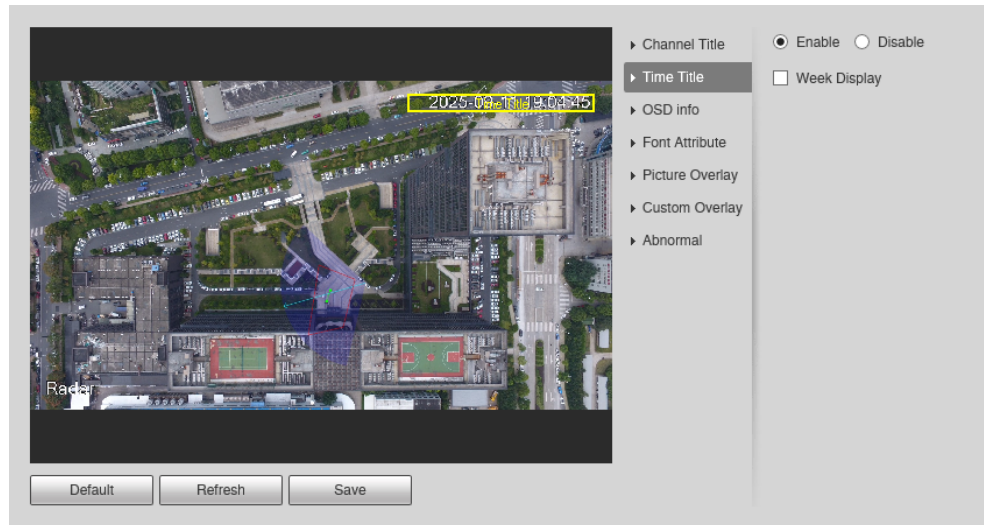


Figure 4-5 Overlay-OSD info

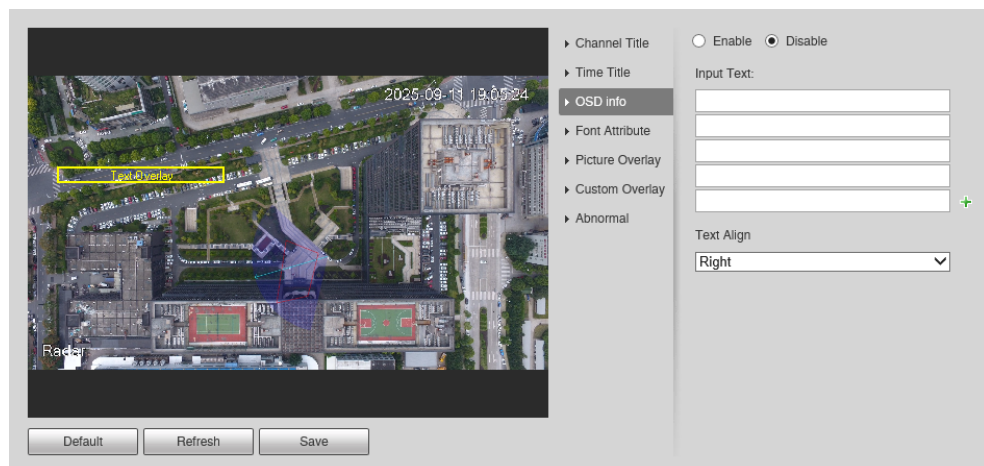


Figure 4-6 Overlay-font attribute

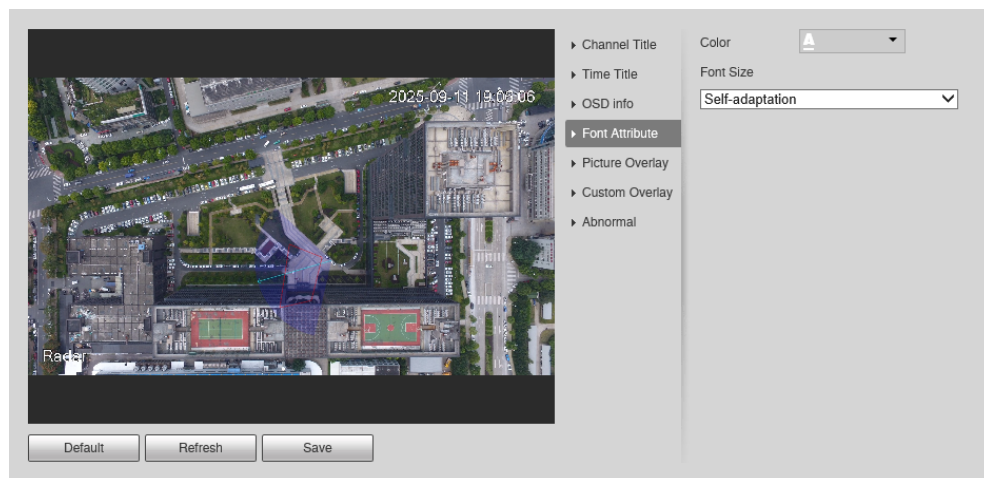


Figure 4-7 Overlay-picture overlay

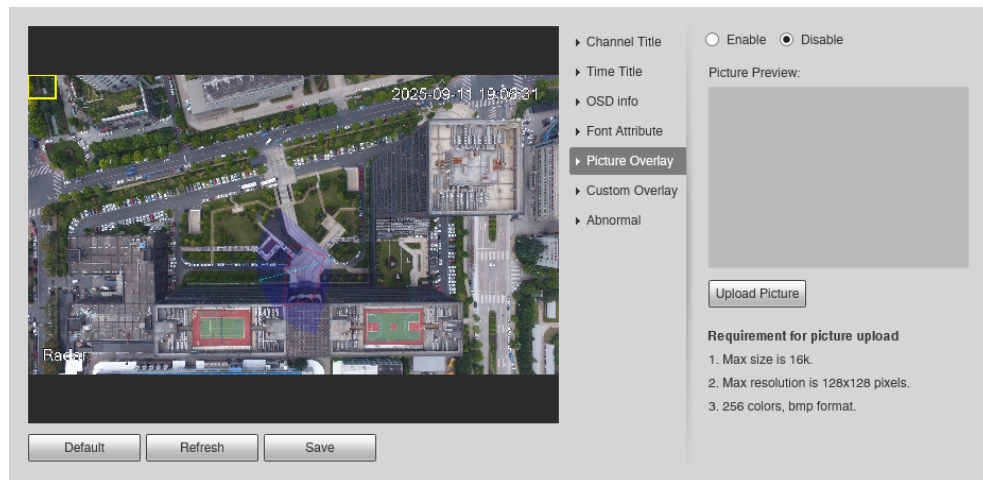


Figure 4-8 Overlay-custom overlay

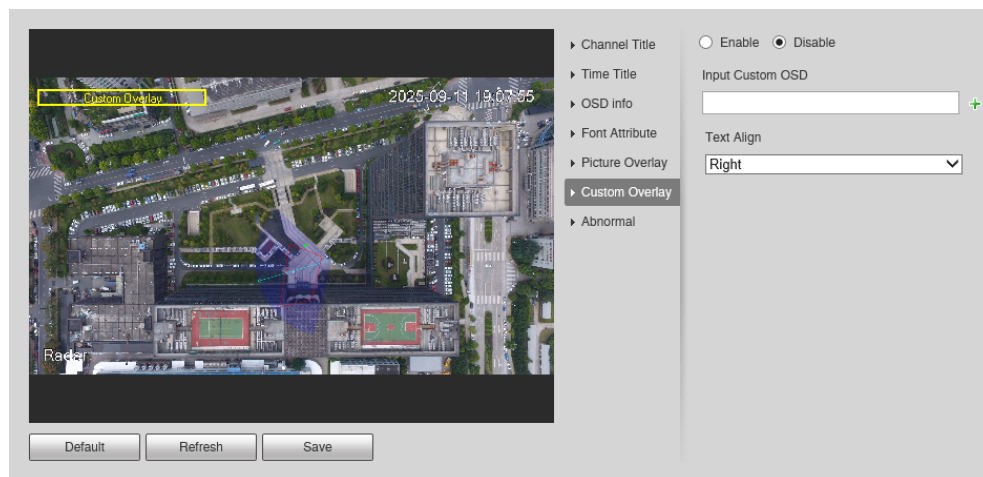


Figure 4-9 Overlay-abnormal

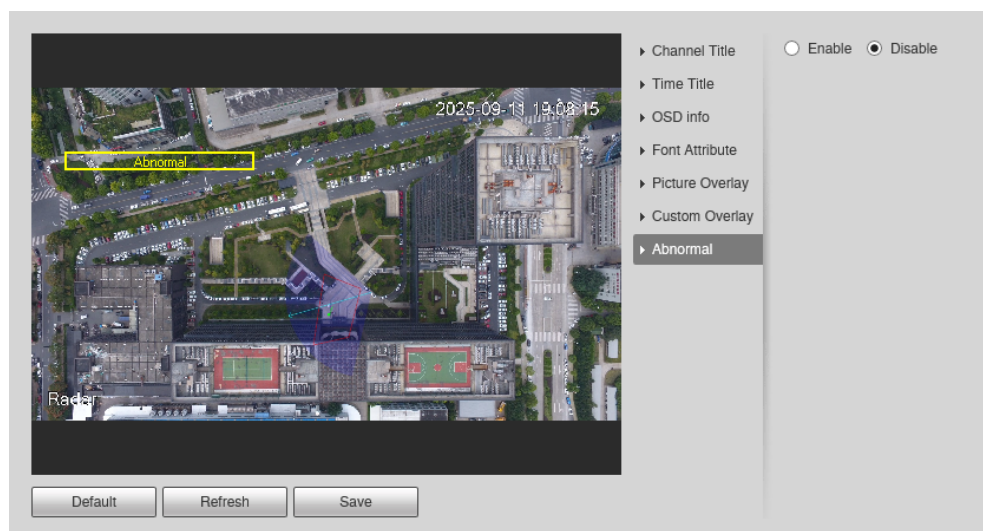


Table 4-3 Description of overlay

Parameter	Description
Channel title	Enable this function when you need to display channel title in the video image. Drag the Channel Title frame to adjust its position. You can align it to the left or right.
Time title	Enable this function when you need to display time in the video image. Drag the frame of the Time Title to adjust its position.
OSD info	Enable this function if you want to display the information of preset, PTZ coordinates, zoom, tour and location on the video image. Drag the OSD Info frame to adjust its position. You can align it to the left or right.
Font attribute	Enable this function if you need to adjust the font size in the video image. Set the font for the channel title, time title, and OSD information. You can adjust the font color, size, and determine whether to outline the font.
Picture overlay	Enable this function if you need to display picture information on the video image. Click on Upload Image to overlay the local image onto the video preview window. You can adjust the position of the overlay image by dragging the yellow frame.  Geolocation and Picture Overlay cannot be enabled at the same time.
Custom overlay	Enable this function when you need to display custom overlay in the video image. Drag the Custom Overlay frame to adjust its position. You can align it to the left or right.
Abnormal overlay	Enable this function if you need to display abnormal information in the video image. Drag the frame of the Abnormal Overlay to adjust its position.

Step 3 Click **Save**.

4.1.1.4 Path

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

Procedure

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

Figure 4-10 Path

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

Step 2 Click **Browse** to select the storage path for functions.

Table 4-4 Description of path

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

Step 3 Click **Save**.

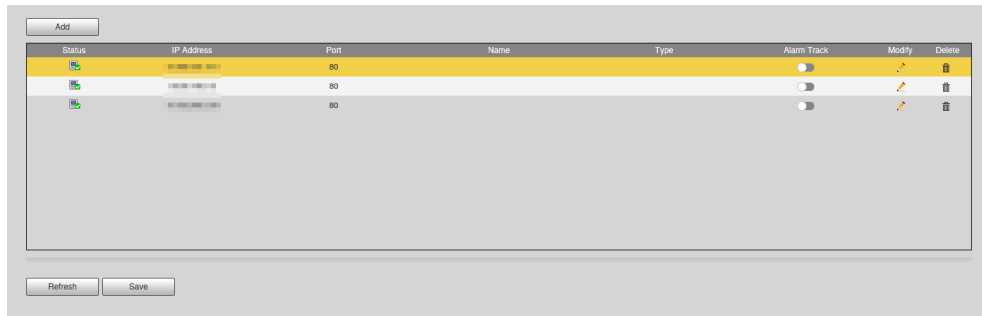
4.1.2 PTZ Camera

You can add or delete PTZ cameras, set camera name and type, and enable or disable alarm track.

Procedure

Step 1 Select **Setting** > **Radar Settings** > **PTZ Camera**.

Figure 4-11 PTZ camera



Step 2 Click **Add**. Enter IP address, port, username, and password of the PTZ camera.



- Port is set to 80 by default. Keep the port consistent with the HTTP port of the PTZ camera.
- If the HTTP port of the linked PTZ camera changes, update this field accordingly to maintain consistency.

Figure 4-12 Add the PTZ camera (1)

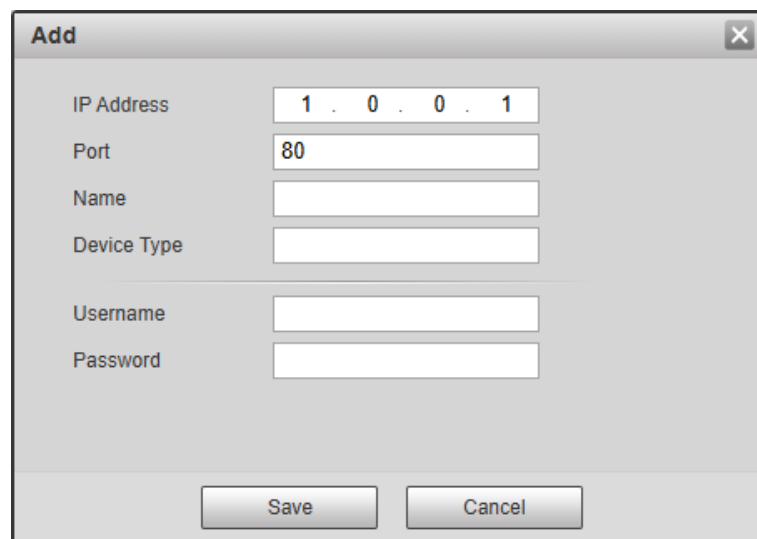
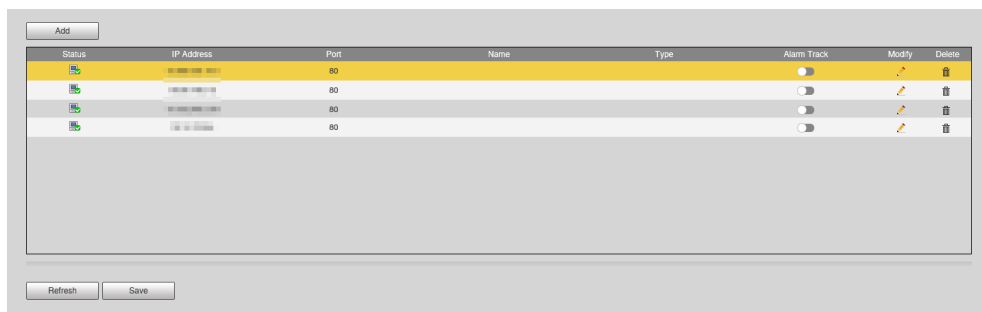


Figure 4-13 Add the PTZ camera (2)



Step 3 Click **Save**.



Click  to enable radar-PTZ linkage.

4.1.3 Radar

On the **Radar** page, you can add radar, delete radar, set radar name and more.

Procedure

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

Figure 4-14 Radar (1)



Step 2 Click **Add**, and enter the required information in the pop-up window.

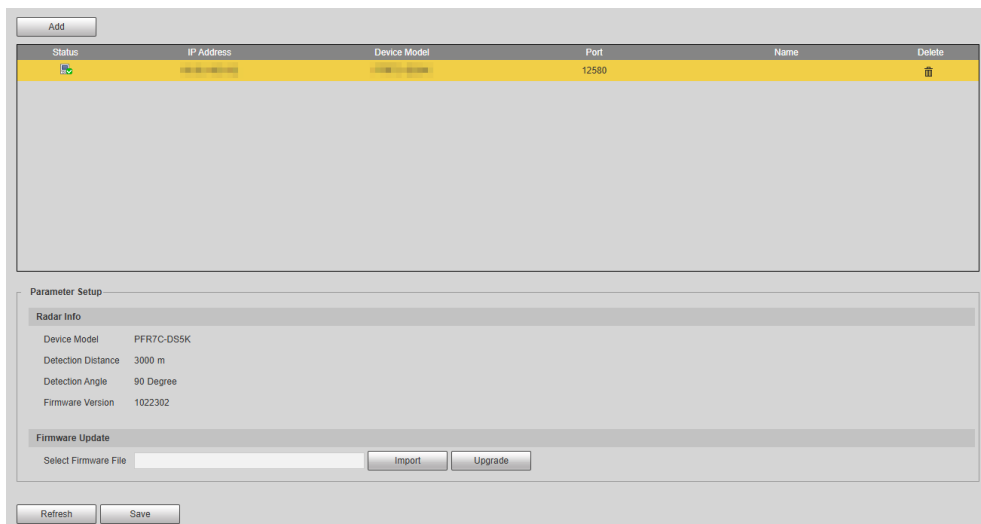


- When adding a radar, fill in the required information according to the radar model.
- If the HTTP port of the linked PTZ camera changes, update this field accordingly to maintain consistency.
- Make sure the radar and the control box are on the same LAN. Up to 4 radars can be added.

Step 3 Click **Save**.

The system displays radar information if the radars are successfully connected.

Figure 4-15 Radar (2)



4.1.4 Linkage Wizard

The linkage wizard page allows for operations such as map import, radar positioning, and radar calibration.

Background Information



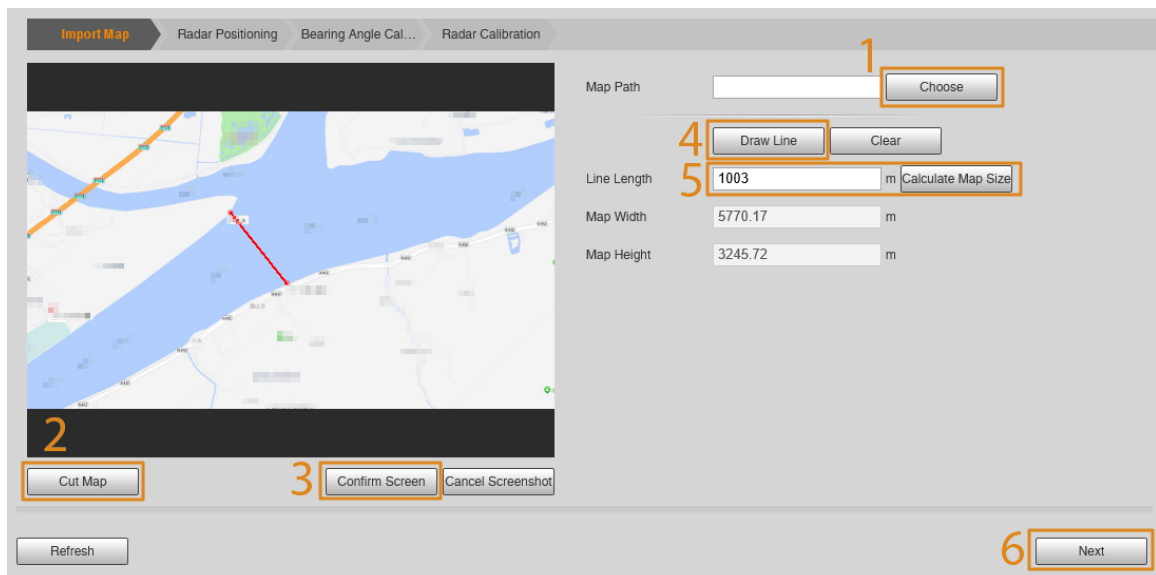
Two people are required to configure the radar calibration function. Person A moves in the detection area as a target, and Person B completes the configuration operation on the computer.

Procedure

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

Step 2 Click **Choose** to import map.

Figure 4-16 Import a map



1. Click **Choose** to import a map.



Support .png, .jpg, and .bmp format.

2. Crop the map according to the detection range of the radar. Drag the box to select the range, and then click **Cut Map**.
3. Click **Confirm Screen** to set the map to have the range you want.
4. Click **Confirm Screenshot** to confirm the cropping in the pop-up page.



Click **Cancel Screenshot** to cancel the cropping.

5. Calculate the map size.
 - a. Measure a distance of the actual detection area.
 - b. On the web client, click **Draw Line** to draw the measured distance on the image.
 - c. Click and hold the left mouse icon to start drawing, and then release the icon to complete drawing.



- Double-click the map to enter full screen display to draw the line more accurately.
- Click **Clear** to clear the line.

6. Enter the actual measured length of the line you drew in the **Line Length** input box and then click **Calculate Map Size**.



The system will automatically calculate the map width and height.

7. Click **Next**.

Step 3

Position the radar.

1. Choose a radar from the **Radar List**.
2. Drag the end points of the yellow sector on the map to adjust the radar orientation.



- The Angle means the angle value between the radar and the true north direction. It can be further accurately adjusted by setting the angle value.
- When the dotted line points horizontally to the right, it is 0°. The degrees increase clockwise.
- Clicking +/- or entering a number to modify the radar north angle in **Angle**.
- Double-click the map to enter full screen to position the radar more accurately. Press [Esc] to exit full screen mode.

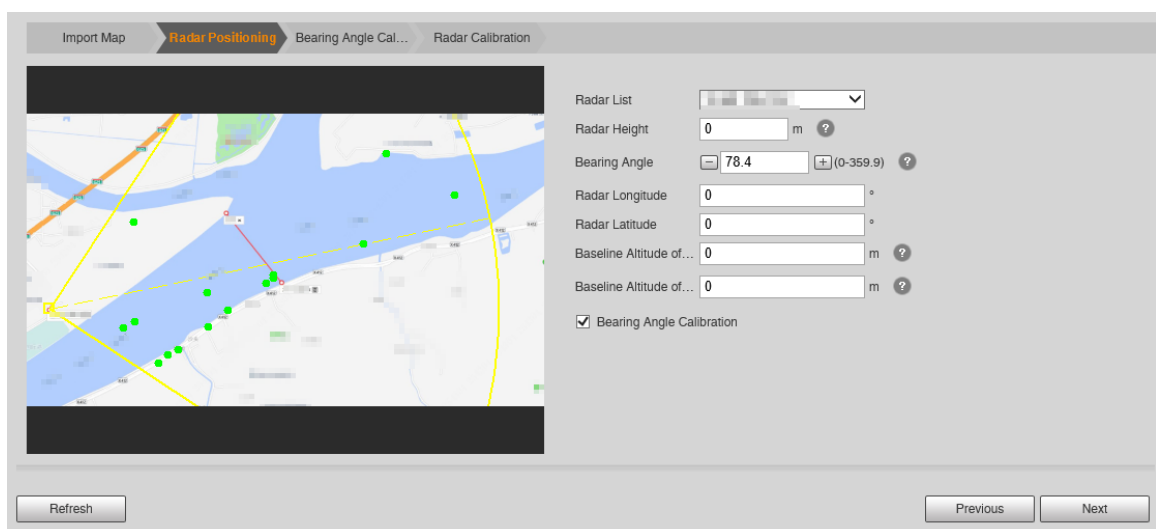
3. Enter the mounting height of the radar on the pole in **Radar Height**.
4. Clicking +/- or entering a number to modify the radar north angle in **Bearing Angle**.
5. Enter the longitude, latitude, reference altitude of the detected surface, and reference altitude of the radar installation surface.
6. (Optional) Choose **Bearing Angle Calibration**.



When selecting **Bearing Angle Calibration**, it is necessary to configure the association with the PTZ camera within the **Bearing Angle Calibration** page.

7. Click **Next**.

Figure 4-17 Radar positioning



Step 4 Bearing angle calibration.

1. Select a PTZ camera from **PTZ Camera List** that needs to be paired with the radar and calibrated, and then enter the username and password used to log in to the webpage of the camera.



Select the radar/PTZ camera that needs to be configured from **Radar List /PTZ Camera List**.

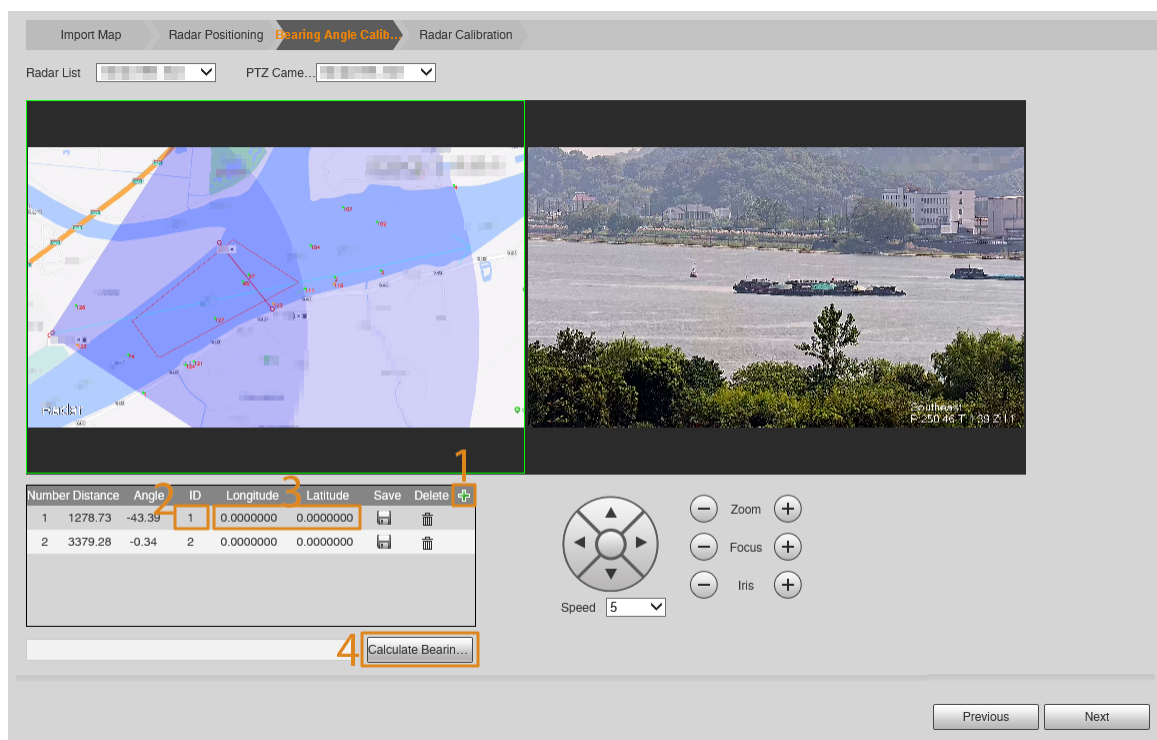
2. Adjust the direction of the PTZ camera through the PTZ control page on the right side of the page.
3. Double click the map to go full screen and click  to add calibration point.
4. Double click the value in the list to edit the point ID and the longitude/latitude values.



- The longitude/latitude values are the values of the target location.
- The system allows the addition of multiple points for calculating the north angle. The more point values you add, the more accurate the calculation results will be.

5. Click **Calculate Bearing Angle** and the system generates the north angle value automatically.

Figure 4-18 Bearing angle calibration



6. Click **Next**.

Step 5

Calibrate the radar.



- Radar calibration is only for Radar-PTZ linkage. You can skip this setting as needed.
- Click **Import** to import multiple calibration point data. Please contact technical support to obtain importing data the tool.
- During the calibration, please fill in the calibration level of P/T value according to the actual situation of the PTZ camera. Move the mouse on  to view the meaning of calibration compensation of P/T value.

1. (Optional) Enter the username and password used to log in to the webpage of the PTZ camera.



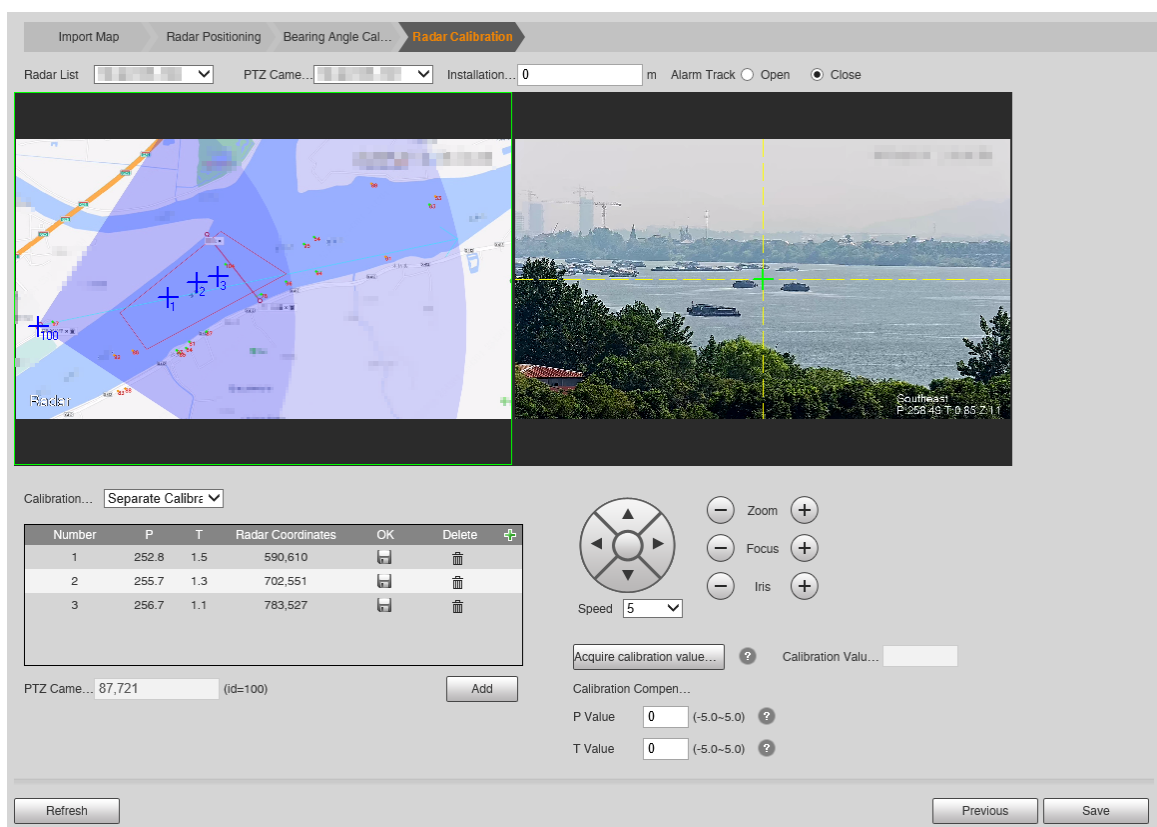
If you are logged in to the PTZ Camera page, the login window will not pop up.

2. Select the radar that needs to be connected to the radar terminal control box from **Radar List**. Select a PTZ camera from **PTZ Camera List** that needs to be paired with the radar and calibrated.



When multiple radars and PTZ cameras need to be configured for linkage control, please switch the IP addresses in the radar and PTZ camera lists and repeat the following calibration operations.

Figure 4-19 Radar calibration (1)

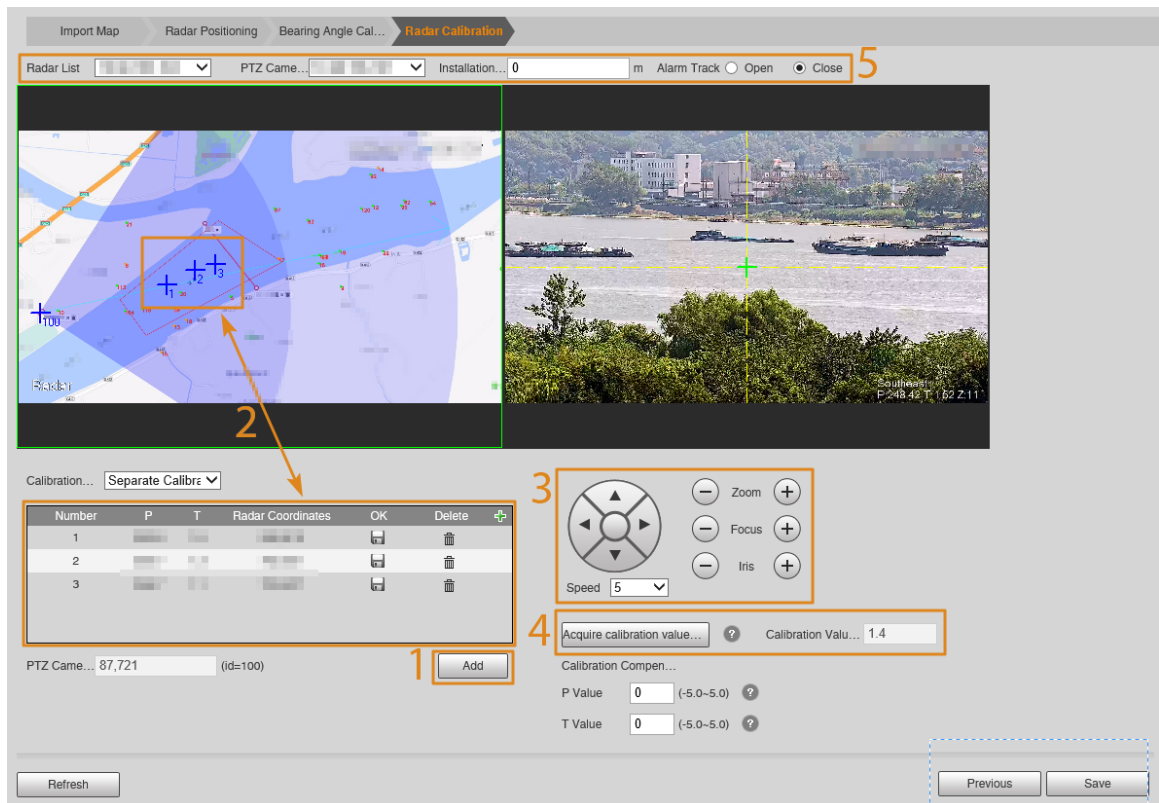


3. Select **Integrated/Separate/GPS** from **Calibration Mode** to carry out various calibration operations.



- Please ensure smooth real-time communication. During the calibration, person A walks in the detection area while person B configures the calibration on PC.
- For accurate calibration, please use professional measuring equipment to obtain latitude, longitude, and altitude information.
- Separate: Applicable for scenarios where the radar and PTZ camera are installed separately, and the target object is within the effective observation range of the radar and PTZ camera.

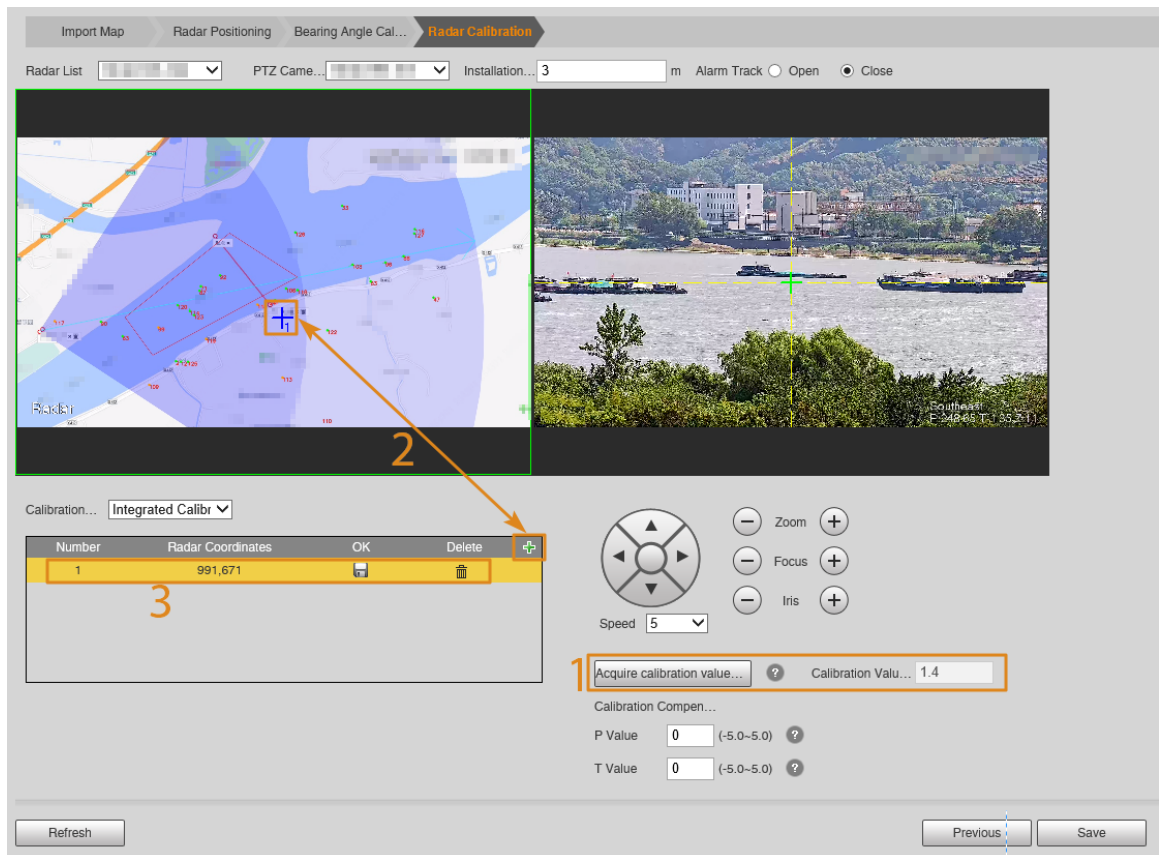
Figure 4-20 Separate calibration



When selecting targets and its center points on the map, ensure the accuracy of the values to avoid affecting the radar and PTZ camera linkage effect.

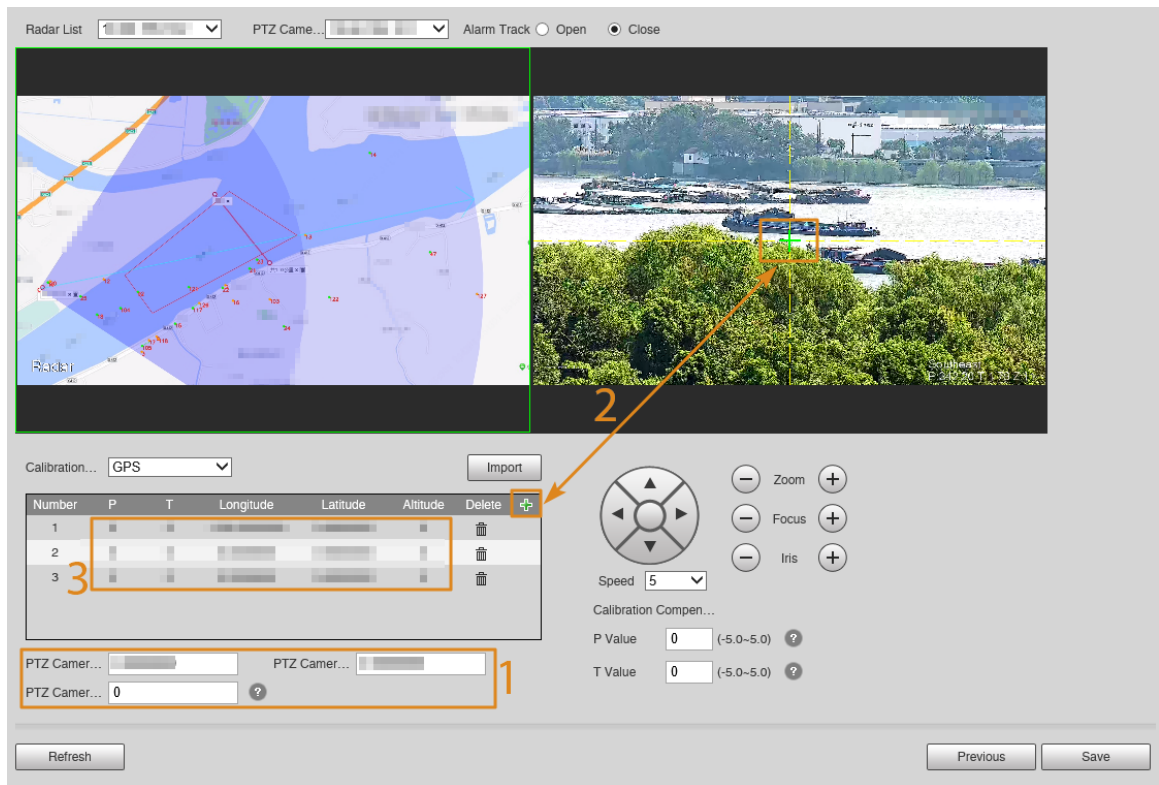
- Select the method as **Separate Calibration**.
 - Select the PTZ camera that needs to be calibrated in **PTZ Camera List**. Click  to obtain the coordinate values of the PTZ camera.
 - Select a target in the map screen as a calibration point, and fill in the coordinate automatically.
 - Adjusting and zooming the PTZ camera to place the target in the center of the picture. Click **Acquire calibration value of PTZ camera** to save the calibration point information.
 - Repeat the above steps to add other calibration points. Please select at least three points that not on the same line in the map. Selecting more points can increase the accuracy of the calibration.
 - Move the PTZ camera coordinates to the actual installation location in the map to confirm it.
- Integrated: When the PTZ camera and radar are installed in same position, please select **Integrated Calibration**. You only need add one calibration point.

Figure 4-21 Integrated calibration



- Select the calibration method as **Integrated Calibration**.
 - Select a target point at a certain distance (recommended 10 m away) that is at the same height as the PTZ camera lens. Adjust the PTZ camera to move the center of the crosshairs at the same height with the target point and click **Acquire calibration value of PTZ camera**.
 - Double click the map to go full screen and click  to add calibration point.
 - Inform person A to move to create a green motion track. After the green track is generated, person A stops. The green track disappears and turns into an orange static track point.
 - Move  and stationary track points overlap. Double-click the screen to exit.
 - Move the center of the PTZ camera screen to the position of person A, ensuring that the entire screen is centered and that its height occupies half of the screen. Click  and the yellow cross mark will turn blue.
- GPS: Before choosing **GPS**, enter the radar altitude, longitude/latitude values in **Linkage Wizard** > **GPS** correctly in order to calculate the north angle of the radar device, and complete the north angle calibration.

Figure 4-22 GPS



- Select the calibration method as **GPS**.
- Enter the latitude, longitude and altitude of the PTZ camera location.
- Click  to add calibration point.
- Inform person A to move in the detection range. Use the PTZ camera to find the target and align the center of the PTZ camera with it. Finally, record the longitude/latitude, altitude, and P/T value of the PTZ camera of person A.
- Record the P value, T value, longitude, latitude and altitude of the PTZ camera as a set of data in a list.
- According to the above way, maintain multiple sets of calibration point data. The selected calibration points should be evenly distributed in the monitoring area.

- Select **Open/Close** from **Alarm Track** to enable linkage tracking.

Step 6 Click **Save**.

4.1.5 Setting Region

You can add, delete, draw areas, set area types, set arming and disarming time periods, and filter areas in the area management page.

4.1.5.1 Region

Procedure

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

Step 2 Click  to add the region. Click **Enable** on the left side of the list to start zone management function.

Step 3 Edit the region name.

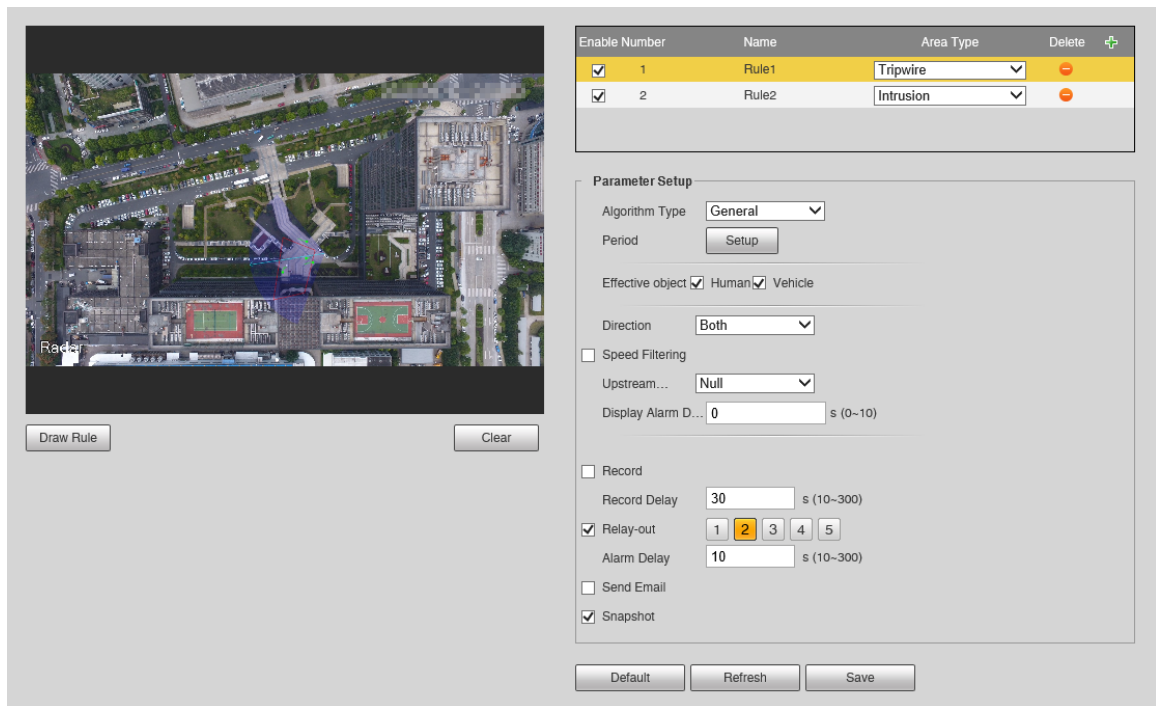
Double click to edit the corresponding area name.

Step 4 Set the region type.

Click to select the area type.

- Tripwire: When the target crosses the tripwire in the set direction, the system executes the alarm linkage action.

Figure 4-23 Region-tripwire



- Intrusion: When the target enters, leaves or appears in the detection area, the system executes the alarm linkage action.

Figure 4-24 Region-intrusion

Enable	Number	Name	Area Type	Delete
☒	1	Rule1	Tripwire	
☒	2	Rule2	Intrusion	

Parameter Setup

Algorithm Type: Human or Vehicle

Period: Setup

Effective object: ☒ Human ☒ Vehicle

Alarm Type: Alarm

☐ Speed Filtering

Display Alarm D...: 0 s (0~10)

☒ Record

Record Delay: 30 s (10~300)

☒ Relay-out: 1 2 3 4 5

Alarm Delay: 10 s (10~300)

☐ Send Email

☒ Snapshot

Default Refresh Save

Step 5 Click **Draw Rule** to draw the detection area in the map.

Draw the area in map. Click to start drawing and click right mouse to end drawing. The begin and end points will automatically connect to create a closed shape.

Step 6 Configure parameters.

Table 4-5 Region parameter description

Parameter	Description
Algorithm Type	Different products support different types of algorithms. Please refer to the actual page for details. Select the target type that the algorithm detects and reports. - General: All identified targets are uploaded to the backend platform. - Human or Vehicle Mode: Forcibly convert non-human/vehicle type targets into vehicle types and upload them to the backend. When the PTZ camera intelligence is activated, the human and vehicle perimeter algorithm is also enabled. - Boat Mode: Converts non-ship targets into ship types and uploads them to the backend. When the PTZ camera intelligence is activated, the ship detection algorithm is enabled for intelligent linkage.
Period	Set the alarm time period, and the alarm event will be triggered only within the set time range. Click Setup to pop up the Period page.

Parameter	Description
Effective object	Select the type of monitoring target for the alarm. You can choose to set alarms for human, vehicle, or boat.
Direction	When setting cross fence detection and tripwire, select A->B , B->A , or A<->B .
Alarm Type	- Set the alarm type for area intrusion, and you can choose Alarm, Pre-warning or Shield. - Priority: Shield > Alarm > Pre-warning.  The rules for area intrusion alarms are described below. Alarm: Low priority. When a target enters the alarm zone, the PTZ camera will track it. When targets are both in alarm zone and warning zone, only the target in the alarm zone will be tracked. Pre-warning: The lowest priority. When the target enters the warning zone, the PTZ camera will track it. When warning zone and alarm zone overlap, the alarm zone takes precedence. Shield: The highest priority. If a shielded area overlaps with another area, the shielded area takes precedence. Targets in shielded area are not tracked, and their trajectories are not displayed. If a scene contains areas prone to false alarms, such as trees, that are outside the control range, it is recommended to block these areas by drawing a shielded area to reduce the impact of false alarms.
Speed Filtering	The default setting is off. When enable this function, no alarm will be generated when the moving target is outside the speed range.
Upstream Direction	Set the upstream direction of information. The options available are empty, A->B , and B->A .
Display Alarm Delay Time	Set the display delay time of the alarm information. When the alarm display delay value is set to X seconds, it means that the target will not be displayed and no alarm information will be generated within X seconds. The target path will be generated only when the target duration exceeds X seconds.
Record	After selecting, when a local alarm occurs, the system will automatically record the alarm. At the same time, you need to set the alarm recording time period in Storage > Schedule.  When linkage tracking is enabled, the radar takes control of the PTZ camera, disabling its own recording rules. When linkage tracking is disabled, the radar no longer controls PTZ camera, and the PTZ camera recording rules are restored.
Record Delay	This indicates that when the alarm stops, the alarm recording will be extended for a certain period before it ceases. The time value range from 10 s–300 s.

Parameter	Description
Relay-out	After selecting, the alarm linkage output port is activated, and the corresponding alarm output device can be linked when a radar alarm occurs.  There are five alarm outputs in total. The 50 m/120 m radar model supports high-voltage equipment control. The No.5 is a high-voltage alarm. The 240 m/300 m/450 m radar model does not support high-voltage alarms.
Alarm Delay	The time unit is the second, with a value range of 10 to 300.
Send Email	When an alarm occurs, an email will be sent to notify the user. The user can set their own email address.
Snapshot	 Before taking a snapshot, please set the alarm screenshot time period. When an alarm occurs, the system automatically takes an online alarm snapshot. The hour must be within the medium settings alarm snapshot time period.

Step 7 Click **Save**.

4.1.5.2 Compensation Area

Set the radar compensation region and rules for the PTZ camera monitoring range.

Procedure

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

Step 2 Select whether to show the compensation area on the screen or not.

Step 3 Select a PTZ camera from the **PTZ Camera List** to add the compensation area.

Step 4 Set the **Frame of P Value Sliding Window** of the video image.



Frame of P Value Sliding Window : When this parameter is set to X, the system saves the P-value data within X frames to estimate the changing trend of the P-value.

Step 5 Click  to add an area. After adding, modify the area name according to actual needs.

Step 6 Click **Draw Rule** and draw the area that needs to be compensated in screen.

Step 7 Click  to enable the area. Configure the compensation parameters for this area.

Figure 4-25 Compensation area

Compensation Area ☐ Display ☒ Hide

PTZ Camera List

Frames of P Value... (0~100)

Enable	Number	Name	Area Type	Delete
☒	1	Area1	Compensation Area	

Parameter Setup

P Value Compens... (-20~20)

T Value Compens... (-20~20)

Speed Limit for P... km/h (0~150)

Frames for P Valu... (0~100)

P Value Incremen... (-20~20)

P Value Decreme... (-20~20)

Frames for P Valu... (0~100)

Table 4-6 Compensation area parameter description

Parameter	Description
P Value Compensation	Set the compensation degree when the PTZ camera rotates in the P direction or T direction. The larger the value, the more obvious the rotation angle.
T Value Compensation	
Speed Limit for P Value Compensation	When the speed of the detected target exceeds the set P-value speed compensation limit value and the accumulated picture frame number exceeds the P value speed anti-shake frame number value, the target needs to be compensated.
Frames for P Value Stabilization	
P Value Incremental Compensation	Make sure the target is in the center of the picture when tracking target. The P-value is compensated in the increasing/decreasing direction.
P Value Decremental Compensation	
Frames for P Value Direction Stabilization	To suppress the camera jitter after compensation, you need to set the anti-shake frame number. Anti-shake compensation starts at the set frame X.

Step 8 Click **Save**.

4.1.6 Managing Protection Zone

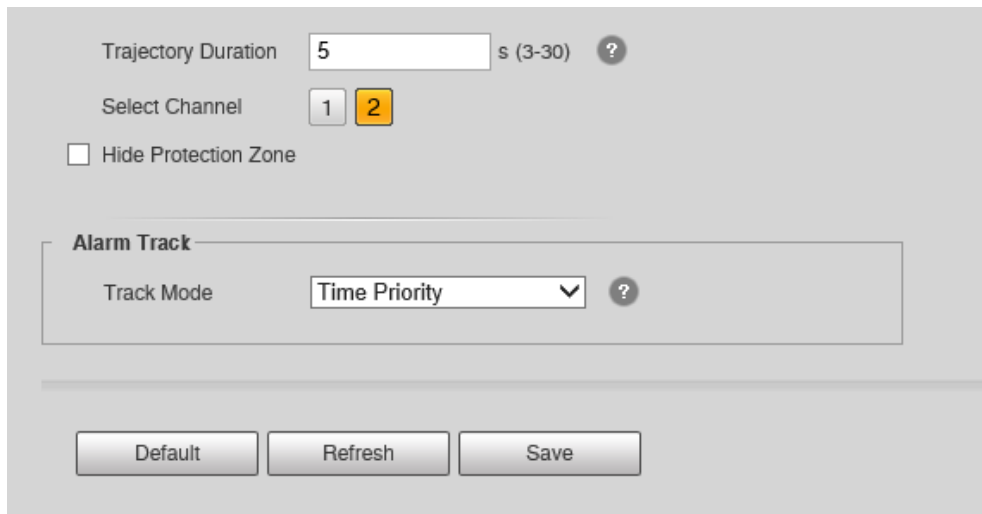
4.1.6.1 Protection Zone Management

Configure track duration, channel selection, hidden defense zone, linkage tracking and other parameters in the defense zone management page.

Procedure

Step 1 Select **Setting > Radar Settings > Protection Zone Management > Protection Zone Management**.

Figure 4-26 Protection zone management



Step 2 (Optional) Select the channel need to be configured.

Step 3 Configure parameters.

Table 4-7 Protection zone management parameter

Parameter	Description
Trajectory Duration	Time length of tack display.
Hide Protection Zone	Enable to hide the defense zone.
Track Mode	Set the radar working mode. ● Time Priority : Track the target which appears earliest. ● Distance Priority : Track the target which is closet to radar earliest. ● Time Prioritized Patrolling : The earliest target point within the tracking area. ● Distance Prioritized Patrolling : The target closest to the radar within the tracking area.
Track Time	Max tracking time of each target.

Step 4 Click **Save**.

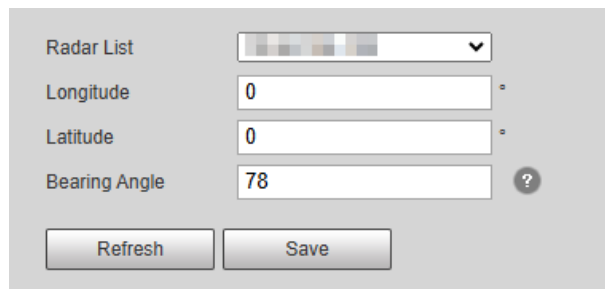
4.1.6.2 Location

Select the radar IP to be connected in the location information page to obtain the radar position information.

Procedure

Step 1 Select **Setting** > **Radar Settings** > **Protection Zone Management** > **Location**.

Figure 4-27 Location



The screenshot shows a web interface for configuring radar location. It includes a 'Radar List' dropdown menu, three input fields for 'Longitude' (containing '0'), 'Latitude' (containing '0'), and 'Bearing Angle' (containing '78'). There are also 'Refresh' and 'Save' buttons at the bottom.

Step 2 Select one radar IP in the **Radar List**.

Step 3 Fill in the radar latitude and longitude information. Users can obtain longitude and latitude information in the following two ways.

- Click **Refresh**. The system will automatically retrieve the longitude and latitude data from the radar device.
- Inputs the latitude and longitude data manually.

Step 4 Click **Save**.

4.1.7 Setting IVS

4.1.7.1 IVS Setup

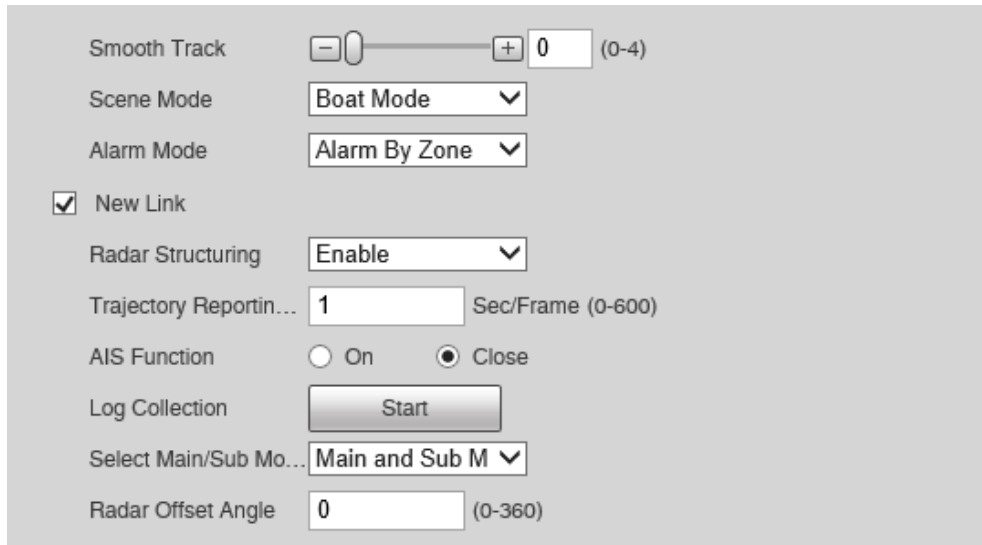
The IVS Setup page allows for the configuration of environmental modes, tracked target presentation, and radar structuring.

Procedure

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

Step 2 Configure parameters.

Figure 4-28 IVS setup



The screenshot shows the IVS setup interface with the following parameters:

- Smooth Track: A slider with minus and plus buttons, currently set to 0 (range 0-4).
- Scene Mode: A dropdown menu set to "Boat Mode".
- Alarm Mode: A dropdown menu set to "Alarm By Zone".
- New Link: A checked checkbox.
- Radar Structuring: A dropdown menu set to "Enable".
- Trajectory Reportin...: A text input field set to 1, with "Sec/Frame (0-600)" as a label.
- AIS Function: Two radio buttons, "On" and "Close", with "Close" selected.
- Log Collection: A button labeled "Start".
- Select Main/Sub Mo...: A dropdown menu set to "Main and Sub M".
- Radar Offset Angle: A text input field set to 0, with "(0-360)" as a label.

Table 4-8 IVS setup parameter description

Parameter	Description
Smooth Track	Click   to adjust the degree of radar track smoothing. The larger the value you set, the smoother the track you will get.
Scene Mode	 Different type of device supports different scene mode type. Please refer to the actual page for details. Select the scene mode type according to the radar usage environment. After turning on the structured function, target information (such as distance, speed, angle, type, TrackID) will be displayed on screen. Different scene modes correspond to different expert mode parameters. For details, please refer to "Appendix 1 Parameter Description".
Alarm Mode	Select the alarm mode according to the actual scenario. You can choose to alarm by target or by zone.
New Link	The linkage mode for adapting the new kind PTZ camera is enabled by enabling this function. Select and enable this function.
Radar Structuring	Enable this function, the preview screen shows the distance, angle, speed and type of the target that the PTZ camera is tracking.
Trajectory Reporting Interval	Set the reporting frequency of radar tracks.
AIS Function	Click to enable the AIS (Automatic Identification System) function.  To obtain AIS data, you need to connect the AIS device to the control box first.
Log Collection	Click Start to collect radar working logs.

Parameter	Description
Select Main/Sub Mode	Set the radar working mode. ● Main Mode : Send the PTZ camera possession data only. ● Sub Mode : Receive the PTZ camera possession data only. ● Main and Sub Mode : Control the PTZ camera and receive the control data at the time.
Radar Offset Angle	The target is tracked when the target offset angle with the radar in the relative coordinate system exceeds the set value. For example, if the radar offset angle is 30°, and the actual position of the target detected by the radar is 100 m away and the offset angle is 10°, the actual reported information is 100 m away and the offset angle is 40°.

Step 3 Configure the link intelligent parameters.

Figure 4-29 Link intelligent

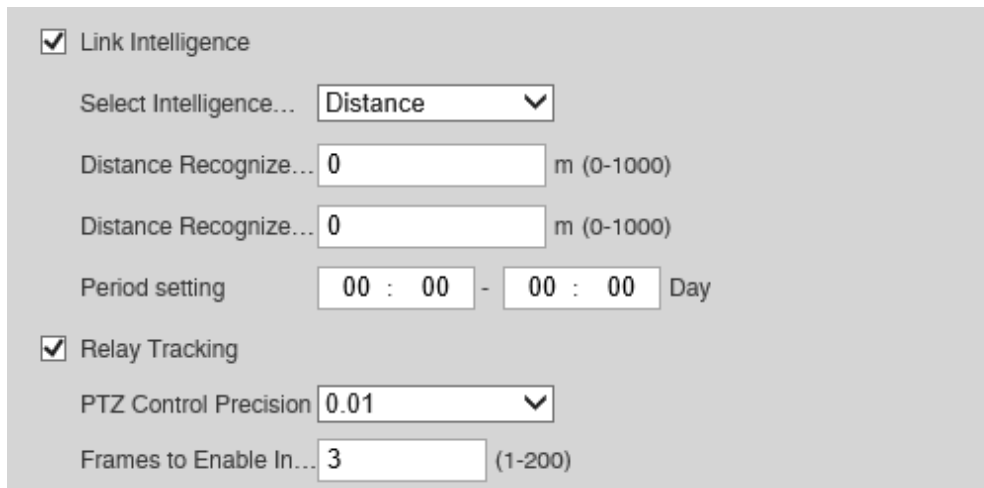


Table 4-9 Link intelligent parameter

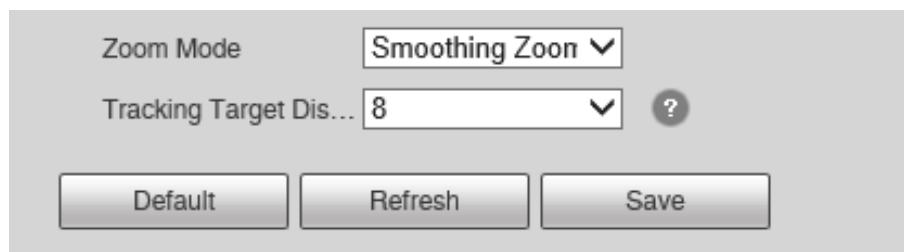
Parameter	Description
Link Intelligent	Enable this function.
Select Intelligence Mode	Select the smart mode type according to actual situation.
Relay Tracking	 The relay tracking function needs to be configured only when the smart mode is on or Time Range. Enable this function. After enabling this function, the radar will track the target until the radar sends a stop message or changes the tracking target.

Parameter	Description
Period Setting	 The time period needs to be configured when the smart mode is Time Range or Distance. Set the time period for the PTZ camera and radar linkage function to be enabled.
Distance Recognized in the Day	 If you need to configure the day distance and night distance if the smart mode is Distance. Set the day/night distance.
Distance Recognized at Night	
PTZ Control Precision	Select the PTZ control precision based on the actual situation.
Frames to Enable Intelligence Linkage	Start intelligence linkage from frame X of the video. For example, setting the parameter value to 8, which means that intelligent tracking starts from the 8th frame of the video.

Step 4 Select the radar zoom mode. You can choose **Smoothing Zoom Mode** or **Fixed Zoom Mode**.

- **Smoothing Zoom Mode** : The size of the target in the PTZ camera screen is used as the judgment standard. The larger the value is set, the larger the target will be in the PTZ camera screen. When the target size exceeds the set value, the zoom will be changed.

Figure 4-30 Smoothing zoom mode



- **Fixed Zoom Mode** : Click  to add zoom data information to the list. When the identified target information reaches the threshold, the magnification is changed.
 - ◇ According to the actual situation, set the **Min Distance** , **Max Distance**, **Zoom1**, **Speed Threshold**, and **Zoom2**.
 - ◇ When set the values for multiple sets of **Min Distance** and **Max Distance**, it is essential to ensure that these limits are continuous, with no gaps in the distance range covered by the various data sets. Please refer to **Min Distance**, **Max Distance**, and coverage range rules in the figure below for guidance on setting these limits.

Figure 4-31 Fixed zoom mode and visual

Zoom Mode	Fixed Zoom Moc						
Visual	Number	Min Distance (m)	Max Distance (m)	Zoom1	Speed Threshold (km/h)	Zoom2	Delete
	1	0	1000	10	20	15	
	2	1000	2000	10	20	15	

- ◇ When the speed threshold is 0, only zoom 1 is effective. When the speed threshold is greater than 0, zoom 1 is used when the target speed is greater than the speed threshold, and zoom 2 is used when the target speed is less than the speed threshold.

Step 5 Configure other smart parameters.

Figure 4-32 Other smart parameter

Track Initiation Time	0	s (0-5)
Min Frames to Esti...	4	Frame (3-10)
Weight of Position E...	500	(0-1000)
Weight of Speed Es...	500	(0-1000)
Frames of Sliding W...	4	(4-10)
Current Weight of S...	500	(0-1000)
Time for Track Disa...	5	s (0-60)

Table 4-10 Other smart parameter

Parameter	Description
Track Initiation Time	To prevent the radar from falsely detecting targets that flash by, the radar is set to monitor targets that have existed within the recognition range for X seconds. For example, when the configuration value is 3, the target survival time is longer than 3 seconds, and the target will not be output if the target appears and disappears in less than 3 seconds.
Min Frames to Estimate Speed	Gives target estimated velocity based on X frames of radar input data.
Weight of Position Estimation	Set the proportion of predicted value when the radar calculates target position data.  The target position data acquired by the radar is obtained by weighted calculation of the radar observation value and the set prediction value.

Parameter	Description
Weight of Speed Estimation	Set the weight of the predicted value when the radar calculates the target speed.  The target speed obtained by the radar is obtained by weighted calculation of the radar observation value and the set prediction value.
Frames of Sliding Window	Set the number of frames of the radar sliding window and estimate the target speed according to the set number of frames.
Current Weight of Speed	Sets the current weight of the target speed.
Time for Track Disappearance	When the radar does not report a target in the disappeared state and there is no valid observation data for this target, the time when the target status is set to the disappeared state.

Step 6 Configure algorithm details for different speed targets.

Figure 4-33 Algorithm configuration

Number	Min Speed(km/h)	Max Speed(km/h)	Min Angle	Smoothing Level(0-4)	Smoothing Method	Prediction Time (s)	Delete	
1	0	20	15	1	Moving Avera	2		
2	20	40	15	1	Weighted Mov	2		
3	40	60	15	1	Holt's Expone	2		

Table 4-11 Algorithm configuration parameter

Parameter	Description
Min Speed	The min and max speed need to be kept continuous to ensure that the complete speed range is covered.
Max Speed	
Min Angle	Tracking is enabled when the angle to the normal exceeds the displayed angle.
Smoothing Level	Set the smoothing level. The higher the smoothing level is, the greater the weighting factor is for the current speed estimate and the historical speed estimate.
Smoothing Method	According to the actual situation, select the algorithm used to calculate the target value.
Prediction Time	Select the data generated after the set prediction time for smoothing calculation.

Step 7 Click **Save**.

4.1.7.2 Expert Mode

Set **Expert Mode** parameters of radar. In order to avoid overlapping detection areas of multiple radars, it is necessary to modify the **Radar Frequency Modulation Mode** to different values.

Background Information



- Some models do not support the expert mode.
- Different type of device supports different expert mode parameters. Please refer to the actual interface for details.
- For detailed expert mode parameters and meanings, please refer to "Appendix 1 Parameter Description".

Procedure

- Step 1 Select **Setting** > **Radar Settings** > **IVS Setup** > **Expert Mode**.
- Step 2 Click **Get** to get the default value of the parameter.
- Step 3 Modify expert mode value according to actual needs.
- Step 4 (Optional) (Optional) After modifying the current value, click **Setup** to save the configuration.

4.2 Network

4.2.1 TCP/IP

You can configure IP address, DNS (Domain Name System) server of the radar to make sure that it can be mutually connected to other devices in the networking.

Background Information

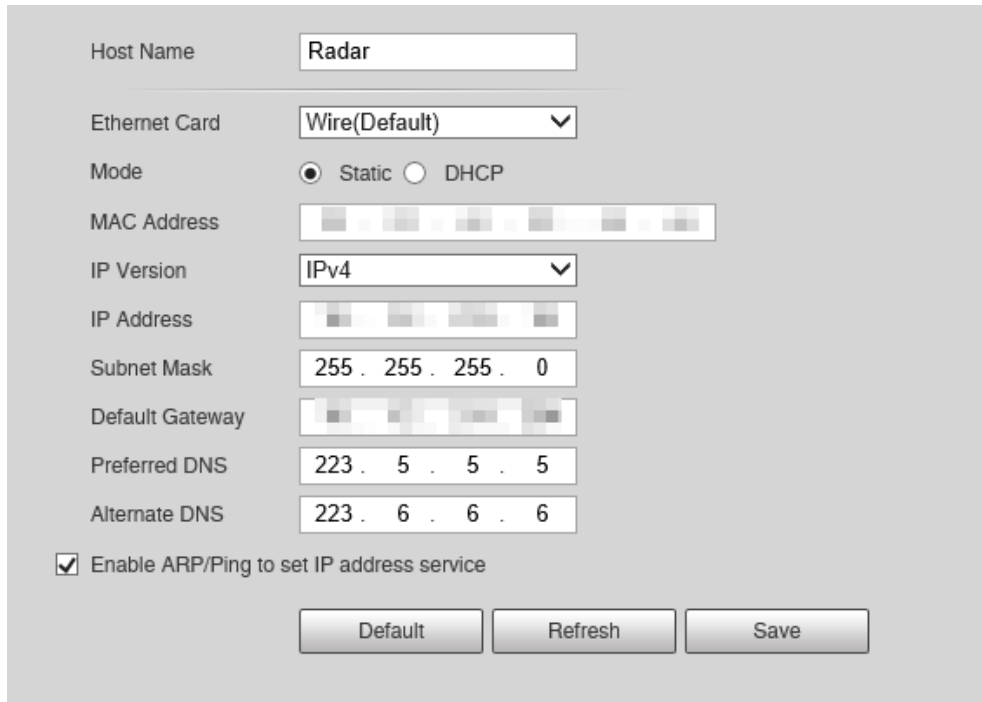


- Confirm the radar has connected to network correctly before setting network parameters.
- Allocate IP address of the same network segment if there is no router in the network.
- Set corresponding gateway and subnet mask if there is a router in the network.

Procedure

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

Figure 4-34 TCP/IP



Step 2 Configure parameters.

Table 4-12 TCP/IP parameter descriptions

Parameter	Description
Host Name	Enter host name, 15 characters at most.
Ethernet Card	Select the Ethernet card that needs to be configured. The default one is Wire.  You can change the default Ethernet card if there is more than one card. Restart radar to activate the new settings once you modify the default settings.
Mode	● DHCP : The system acquires IP address automatically. You cannot set the IP address, subnet mask and default gateway. ● Static : You need to configure IP address, subnet mask and default gateway manually.
MAC Address	Display the MAC address of radar.
IP Version	Select IP version from IPv4 and IPv6 and both versions can be accessed.
IP Address	Enter the IP address, subnet mask, and default gateway as needed when selecting Static mode.  ● IPv6 has no subnet mask. ● The default gateway must be in the same network segment with the IP address.

Parameter	Description
Subnet Mask	Enter the IP address, subnet mask, and default gateway as needed when selecting Static mode.  • IPV6 has no subnet mask. • The default gateway must be in the same network segment with the IP address.
Default Gateway	Enter the IP address, subnet mask, and default gateway as needed when selecting Static mode.  • IPV6 has no subnet mask. • The default gateway must be in the same network segment with the IP address.
Preferred DNS	IP address of the preferred DNS.
Alternate DNS	IP address of the Alternate DNS.
Enable ARP/Ping to set IP address service.	Select the check box, get the device MAC address, and then you can modify and configure the device IP address with ARP/ping command. It is enabled by default. During restarting, you will have no more than 2 minutes to configure the device IP address by a ping packet with defined length, the server will be turned off in 2 minutes, or it will be turned off immediately after the IP address is successfully configured. If the service is not enabled, the IP address cannot be configured with ping packet.

Step 3 Click **Save**.

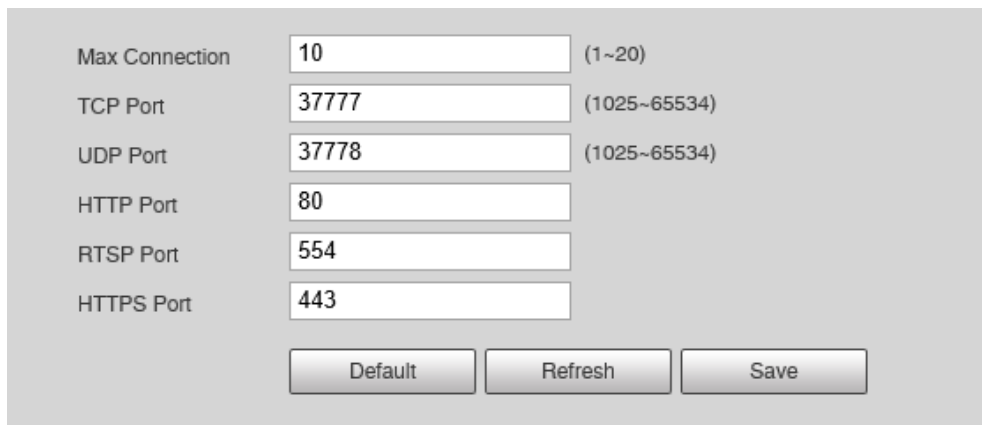
4.2.2 Port

This section introduces configurations of the maximum number of users that can connect to the radar simultaneously and value of each port.

Procedure

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

Figure 4-35 Port



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

Default Refresh Save

Step 2 Configure port parameters.

- The configuration of **Max Connection** takes effect immediately and others after the radar is restarted.
- 0–1024, 1900, 3800, 5000, 5050, 9999, 37776, 37780–37880, 39999, 42323 are occupied for specific uses.
- It is not recommended to use the default value of other ports during port configuration.

Table 4-13 Port parameter description

Parameter	Description
Max Connection	The maximum number of users that can log in to the web page simultaneously of the same radar. The value ranges from 1 to 20 and 10 is set by default.
TCP Port	Transmission control protocol port, the default value is 37777, and it can be modified as needed.
UDP Port	User datagram protocol port, the default value is 37778, and it can be modified as needed.
HTTP Port	Hypertext transfer protocol port, the default value is 80, and it can be modified as needed.

Parameter	Description
RTSP Port	- Real time streaming protocol port, leave it if the value is 554 by default. If you play live view with QuickTime, VLC or Blackberry smart phone, the following URL format is available. - When the URL format requiring RTSP, you need to specify channel number and bit stream type in the URL, and also username and password if needed. - When playing live view with Blackberry smart phone, you need to turn off the audio, and then set the codec mode to H.264B and resolution to CIF. URL format example: <pre>rtsp://username:password@ip:port/cam/realmonitor?channel=1&subtype=0</pre> Among that: - Username: Your username, such as admin. - Password: Your password, such as admin. - IP: Your device IP, such as 192.168.1.122. - Port: Leave it if the value is 554 by default. - Channel: Channel number, which starts from 1. For example, if you are using channel 2, then the channel=2. - Subtype: Bit stream type; 0 means main stream (subtype=0) and 1 means sub stream (subtype=1). So, if you require the sub stream of channel 2 from a certain device, then the URL should be: <pre>rtsp://admin:admin@192.168.1.22:554/cam/realmonitor?channel=2&subtype=1</pre> If user name and password are not needed, then the URL can be: <pre>rtsp://ip:port/cam/realmonitor?channel=1&subtype=0</pre>
HTTPs Port	HTTPs communication port, the default value is 443, and it can be modified as needed.

Step 3 Click **Save**.

4.2.3 PPPoE

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

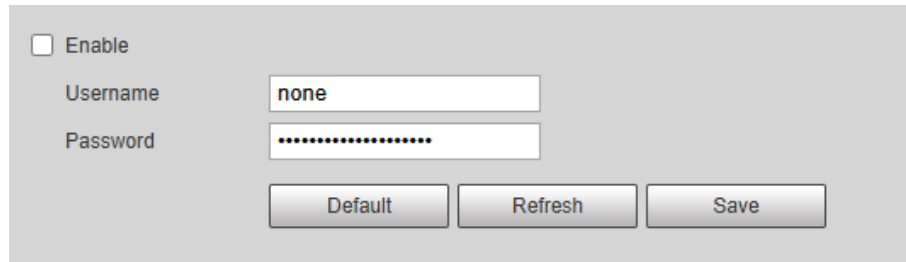
Prerequisites

- The camera has connected to the network.
- You have gotten the account and password from Internet Service Provider.

Procedure

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

Figure 4-36 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 page.

Step 3 Click **Save**.

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

4.2.4 DDNS

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

Prerequisites

Check the type of DNS server supported by the camera.

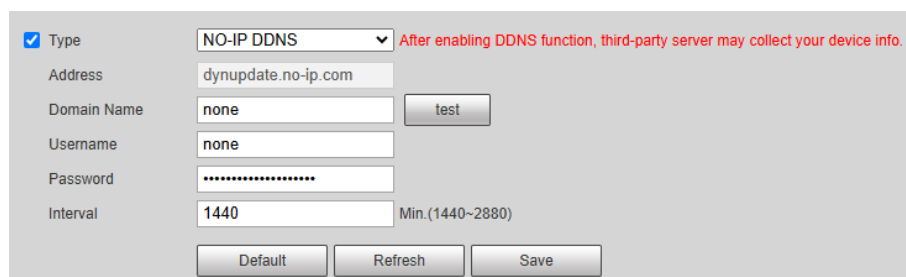
Procedure

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



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

Figure 4-37 DDNS



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

Table 4-14 Description of DDNS parameters

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

Results

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

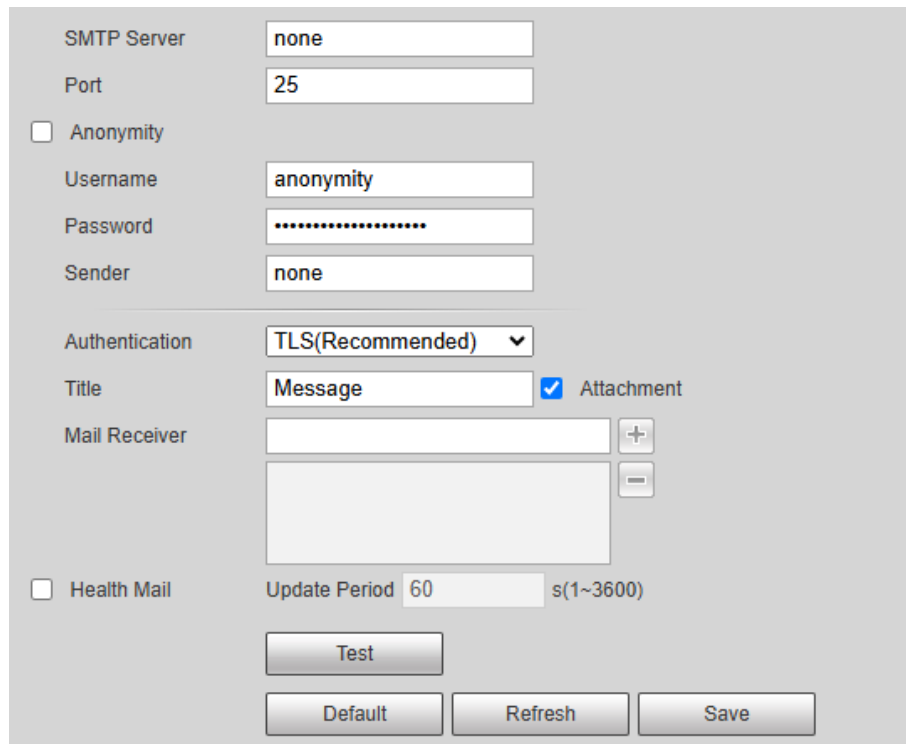
4.2.5 SMTP (Email)

Configure email parameter and enable email linkage. The system sends email to the server of the receiver through SMTP server when alarm or abnormality is triggered. The receiver can receive the email after logging in to the server.

Procedure

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

Figure 4-38 SMTP (Email)



Step 2 Configure parameters.

Table 4-15 SMTP (Email) parameter descriptions

Parameter	Description	
SMTP Server	IP address of SMTP server that sends emails.	 For the detailed configuration, see "Major mailbox configuration".
Port	Port number of the SMTP server that sends emails. The default value is 25.	
Username	Sender's email username.	
Password	Sender's email password.	
Anonymity	By enabling this function, the sender's information is not displayed in the email. You can auto log in anonymously, and do not need to enter the username, password and the sender information.	
Sender	Sender's email address.	
Authentication	Select Authentication from None, SSL and TLS. TLS is set by default.  For the detailed configuration, see "Major mailbox configuration".	
Title	Enter no more than 60 characters in Chinese, English, and Arabic numerals.	
Attachment	Select the check box to support attachment in the email.	
Mail Receiver	Receiver's email address. Support 3 addresses at most.	

Parameter	Description
Health Mail	The system sends test mails to check if the connection is successfully configured. Select Health Mail , configure the Update Period , and then the system sends test mails as the defined period.
Test	Test the email sending and receiving function. If the configuration is correct, you will receive test mail. Save email configuration before running the test.

For the configuration of major mailboxes.

Table 4-16 Major mailbox configuration

Mailbox	SMTP Server	Authentication	Port	Description
QQ	smtp.qq.com	SSL	465	- The authentication type cannot be None. - You need to enable SMTP service in your mailbox. - The authentication code is required as password; either the QQ password or email password is not applicable.  Authentication code, the code you receive when enabling SMTP service.
		TLS	587	
163	smtp.163.com	SSL	465/994	- You need to enable SMTP service in your mailbox. - The authentication code is required as password; 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	You need to enable SMTP service in your mailbox.
		none	25	
126	smtp.126.com	none	25	You need to enable SMTP service in your mailbox.

Step 3 Click **Save**.

4.2.6 UPnP

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

Prerequisites

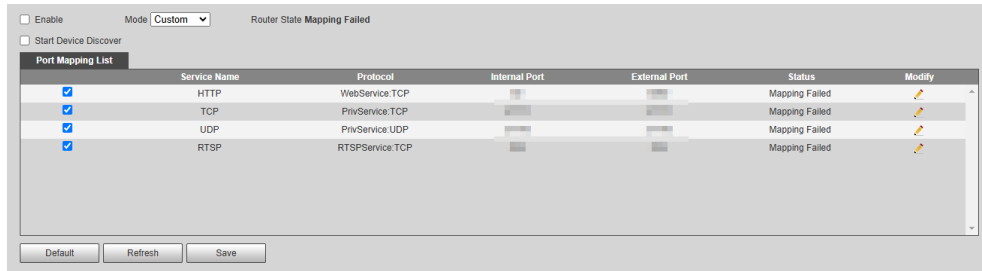
- Make sure the UPnP service is installed in the system.

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

Procedure

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

Figure 4-39 UPnP



Service Name	Protocol	Internal Port	External Port	Status	Modify
HTTP	WebService.TCP			Mapping Failed	
TCP	PrivService.TCP			Mapping Failed	
UDP	PrivService.UDP			Mapping Failed	
RTSP	RTSPService.TCP			Mapping Failed	

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

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

Step 3 Click **Save**.

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

4.2.7 SNMP

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

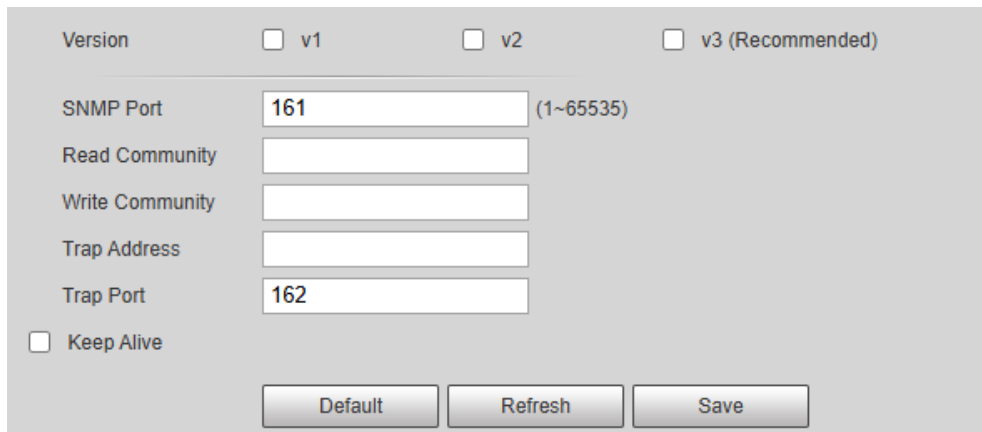
Prerequisites

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

Procedure

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

Figure 4-40 SNMP (1)



Version ☐ v1 ☐ v2 ☐ v3 (Recommended)

SNMP Port (1~65535)

Read Community

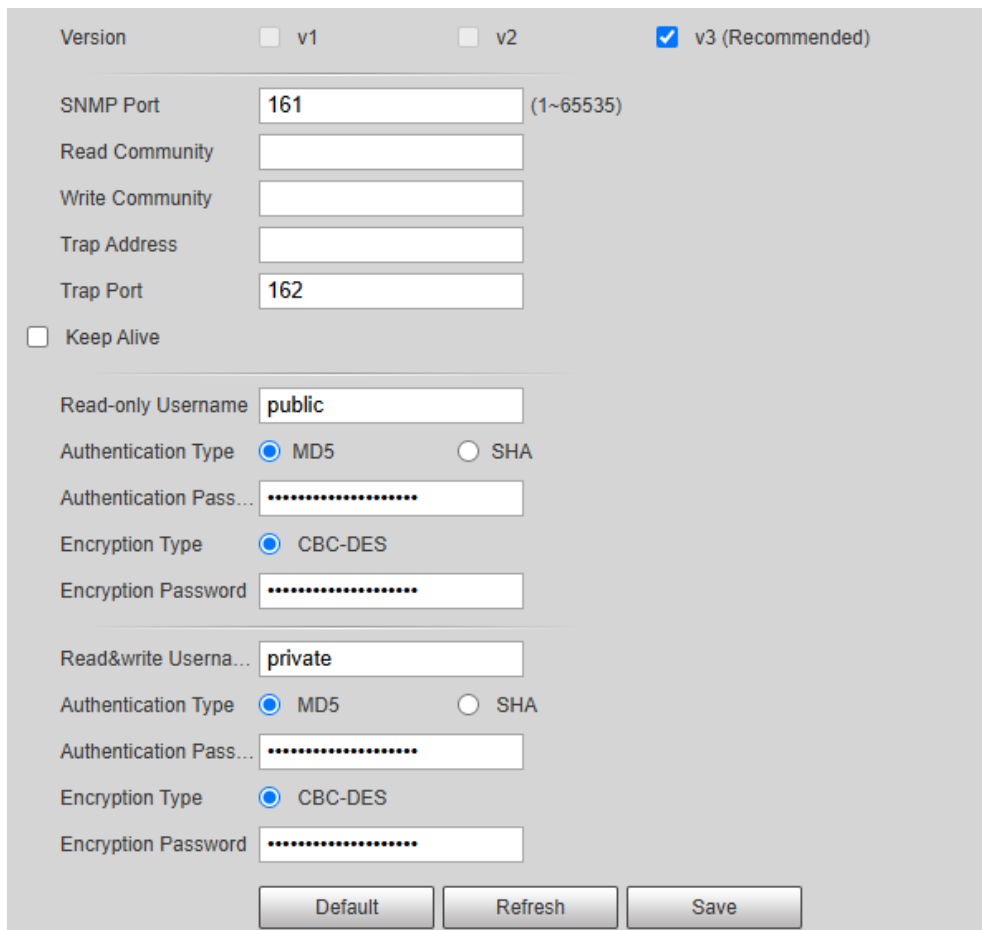
Write Community

Trap Address

Trap Port

☐ Keep Alive

Figure 4-41 SNMP (2)



Version ☐ v1 ☐ v2 ☒ v3 (Recommended)

SNMP Port (1~65535)

Read Community

Write Community

Trap Address

Trap Port

☐ Keep Alive

Read-only Username

Authentication Type ☒ MD5 ☐ SHA

Authentication Pass...

Encryption Type ☒ CBC-DES

Encryption Password

Read&write Userna...

Authentication Type ☒ MD5 ☐ SHA

Authentication Pass...

Encryption Type ☒ CBC-DES

Encryption Password

Step 2 Select SNMP version to enable SNMP.

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



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

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

Table 4-17 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**.

Results

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

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



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

4.2.8 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.

Background Information

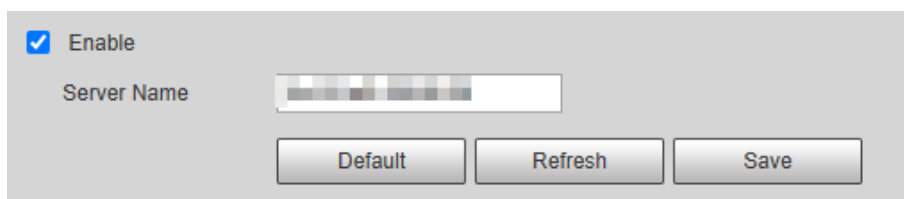


Bonjour is enabled by default.

Procedure

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

Figure 4-42 Bonjour



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

Step 3 Click **Save**.

Results

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

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

4.2.9 Multicast

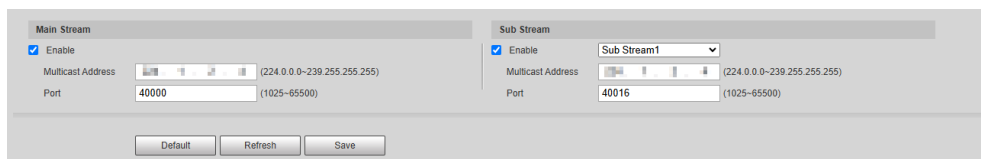
When multiple users are previewing the device video image simultaneously through network, it might fail due to limited bandwidth. You can solve this problem by setting up a multicast IP (224.0.1.0–238.255.255.255) for the camera and adopt the multicast protocol.

Procedure

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

Step 2 Select the multicast type, including **RTS** or **TS**.

Figure 4-43 Multicast



Step 3 Select the **Enable** check box, and enter IP address and port number.

Table 4-18 Description of multicast parameters

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

Step 4 Click **Save**.

Results

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

4.2.10 Auto Register

The device actively registers with the proxy server specified by the user. The proxy server acts as a relay to facilitate the client software to access the device through the proxy server to achieve preview and monitoring.

Procedure

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

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

Figure 4-44 Auto register

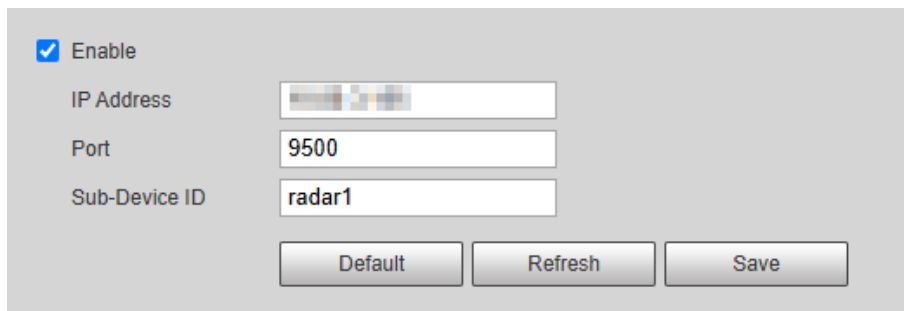


Table 4-19 Description of Auto Register parameters

Parameter	Description
IP Address	IP address or server domain name that needs to be registered.
Port	Port number for automatic registration.
Sub-Device ID	Customize the ID used for this device.

Step 3 Click **Save**.

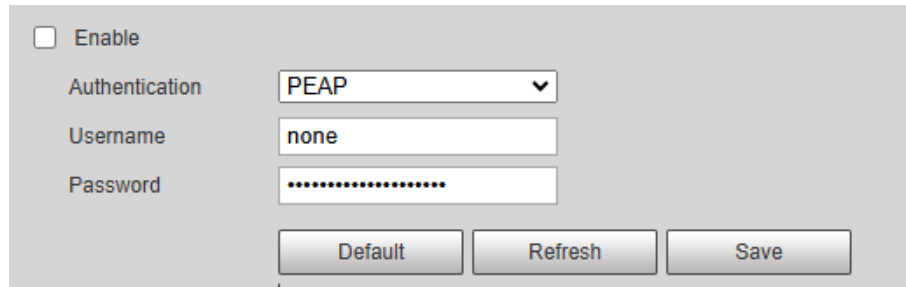
4.2.11 802.1x

Cameras can connect to LAN after passing 802.1x authentication.

Procedure

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

Figure 4-45 802.1x



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

Table 4-20 Description of 802.1x parameters

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

Step 3 Click **Save**.

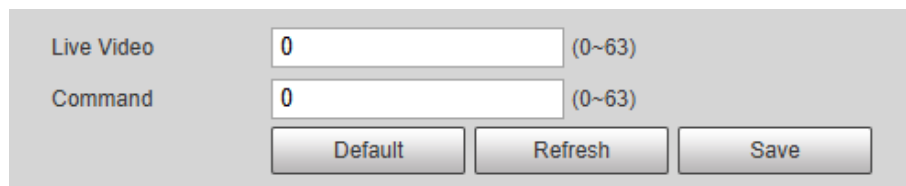
4.2.12 QoS

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.

Procedure

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

Figure 4-46 QoS



Step 2 Configure QoS parameters.

Table 4-21 Description of QoS parameters

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

Step 3 Click **Save**.

4.2.13 Assess Platform

4.2.13.1 RTMP

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

Background Information

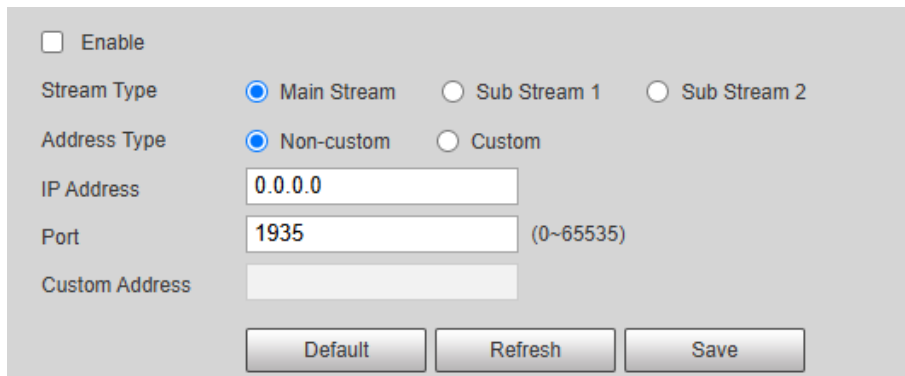


- RTMP can be configured by admin only.
- RTMP supports the H.264, H.264 B and H.264H video formats, and the AAC audio format only.

Procedure

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

Figure 4-47 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 4-22 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. • IP address : Support IPv4 or domain name. • Port : We recommend that you use the default one.

Parameter	Description
Port	When selecting Non-custom , you need to enter server IP address and 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.

Step 4 Click **Save**.

4.2.13.2 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.

Procedure

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

Figure 4-48 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** page.

Step 5 Follow the instructions to finish the settings.

4.2.13.3 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.

Background Information

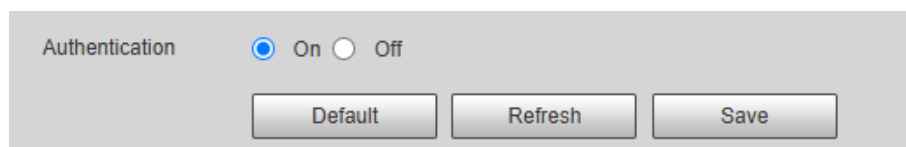


ONVIF is enabled by default.

Procedure

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

Figure 4-49 ONVIF



Step 2 Select **On** in Authentication.

Step 3 Click **Save**.

4.3 Event

4.3.1 Setting Alarm

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

Background Information

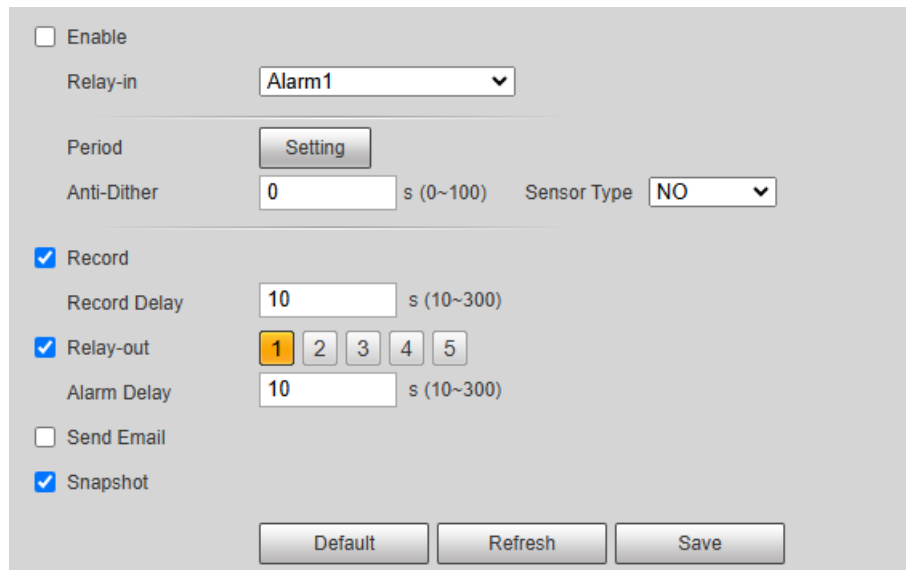


Functions might vary with different models.

Procedure

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

Figure 4-50 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.

Step 5 Click **Save**.

4.3.2 Setting Abnormality

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



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

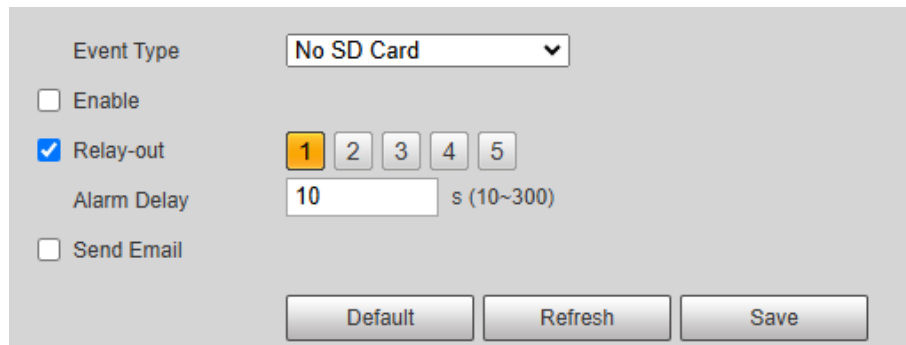
4.3.2.1 Setting SD Card

In case of SD card abnormality, the system performs alarm linkage. The event types include **No SD Card**, **Capacity Warning**, and **SD Card Error**. The introduction is for reference only, and may differ from the actual page.

Procedure

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

Figure 4-51 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.

Step 4 Click **Save**.

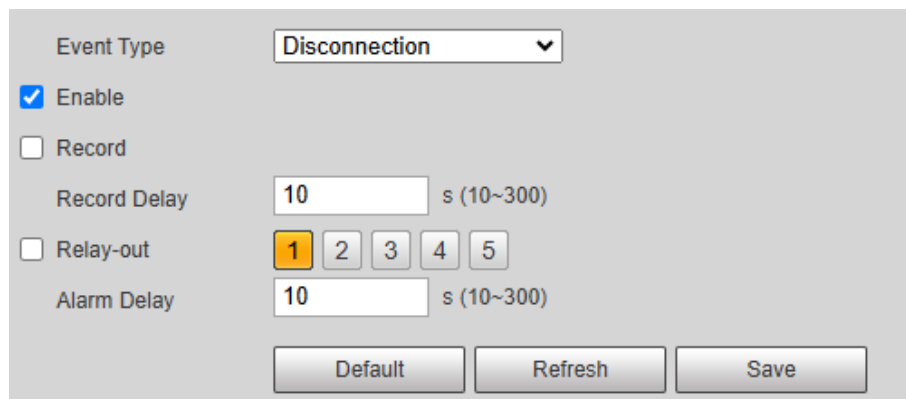
4.3.2.2 Setting Network

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

Procedure

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

Figure 4-52 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.

Step 4 Click **Save**.

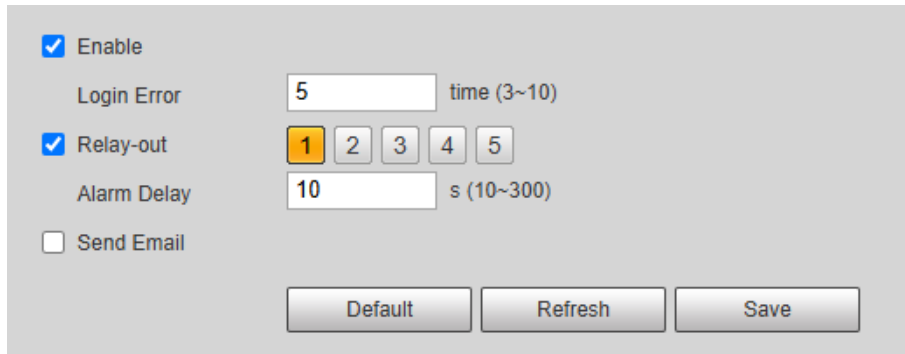
4.3.2.3 Setting Illegal Access

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

Procedure

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

Figure 4-53 Illegal access



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

Step 3 Set Login Error.

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

Step 4 Set alarm linkage actions.

Step 5 Click **Save**.

4.3.2.4 Setting Security Exception

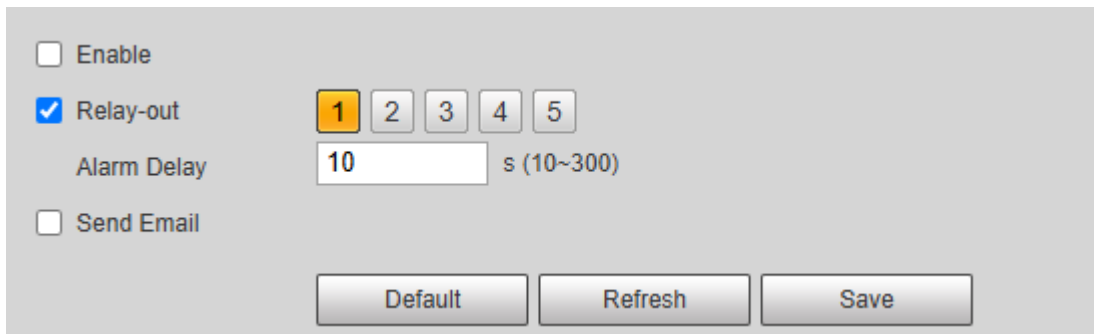
When a hostile attack is detected, the system performs alarm linkage.

Procedure

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

Step 2 Select the Enable check box.

Figure 4-54 Security exception



Step 3 Set alarm linkage actions.

Step 4 Click **Save**.

4.4 Storage

4.4.1 Schedule

4.4.1.1 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.

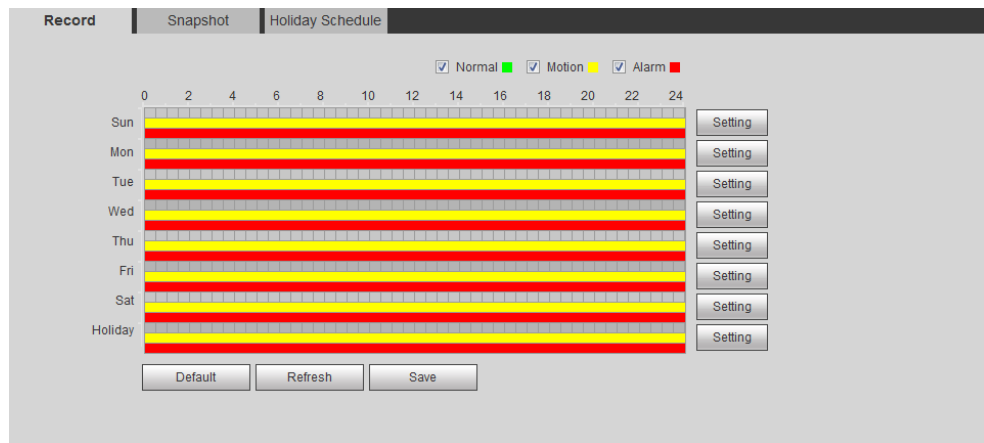
4.4.1.1.1 Setting Record Plan

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

Procedure

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

Figure 4-55 Record



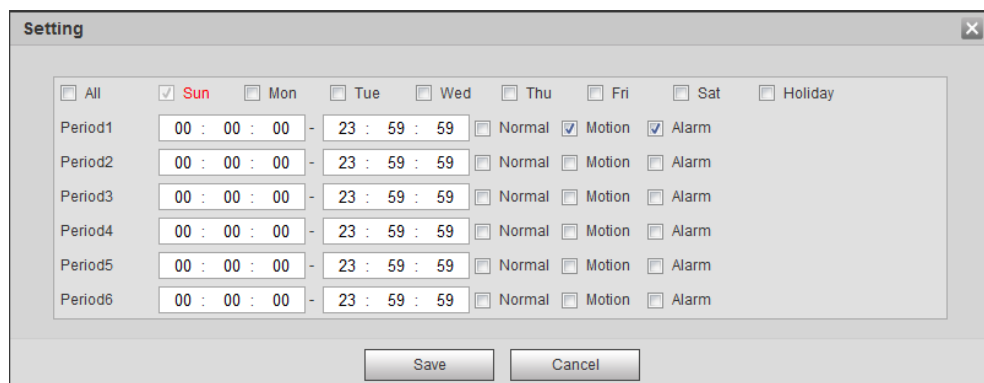
Step 2 Set record plan.

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

- Method one: Select a record type, such as **Normal**, and directly press and drag the left mouse icon 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 4-56 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**.

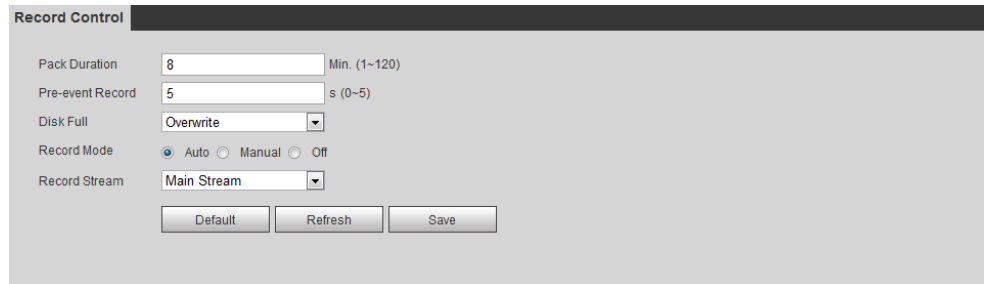
4.4.1.1.2 Setting Record Control

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

Procedure

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

Figure 4-57 Record control



Step 2 Set parameters.

Table 4-23 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.
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**.

4.4.1.1.3 Setting Record Linkage

On the alarm event setting page (such as the motion detection page), 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 4-58 Record linkage

☒ Record

Record Delay

 s (10~300)

4.4.1.2 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.

4.4.1.2.1 Setting Snapshot Plan

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

Procedure

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

Figure 4-59 Snapshot

Record | **Snapshot** | Holiday Schedule

☒ Normal ☒ Motion ☒ Alarm

	0	2	4	6	8	10	12	14	16	18	20	22	24	
Sun	[Timeline with bars]													Setting
Mon	[Timeline with bars]													Setting
Tue	[Timeline with bars]													Setting
Wed	[Timeline with bars]													Setting
Thu	[Timeline with bars]													Setting
Fri	[Timeline with bars]													Setting
Sat	[Timeline with bars]													Setting
Holiday	[Timeline with bars]													Setting

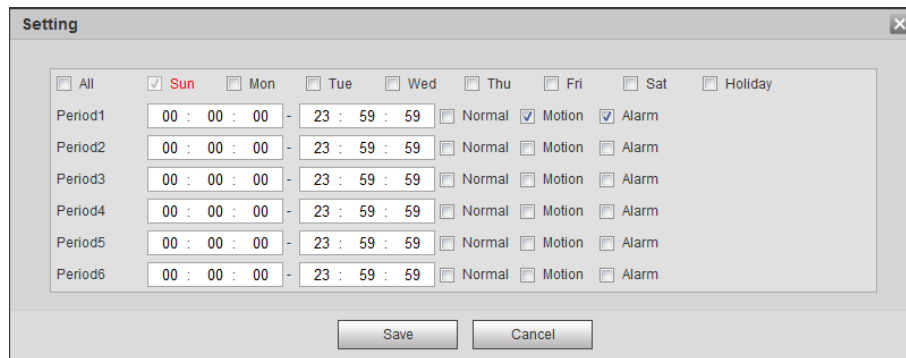
Step 2 Select snapshot type and set time period.

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

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

- Click **Setting** next to a day.

Figure 4-60 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.

Step 3 Click **Save**.

4.4.1.2.2 Setting Snapshot Linkage

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

Figure 4-61 Snapshot linkage



4.4.1.3 Holiday Schedule

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

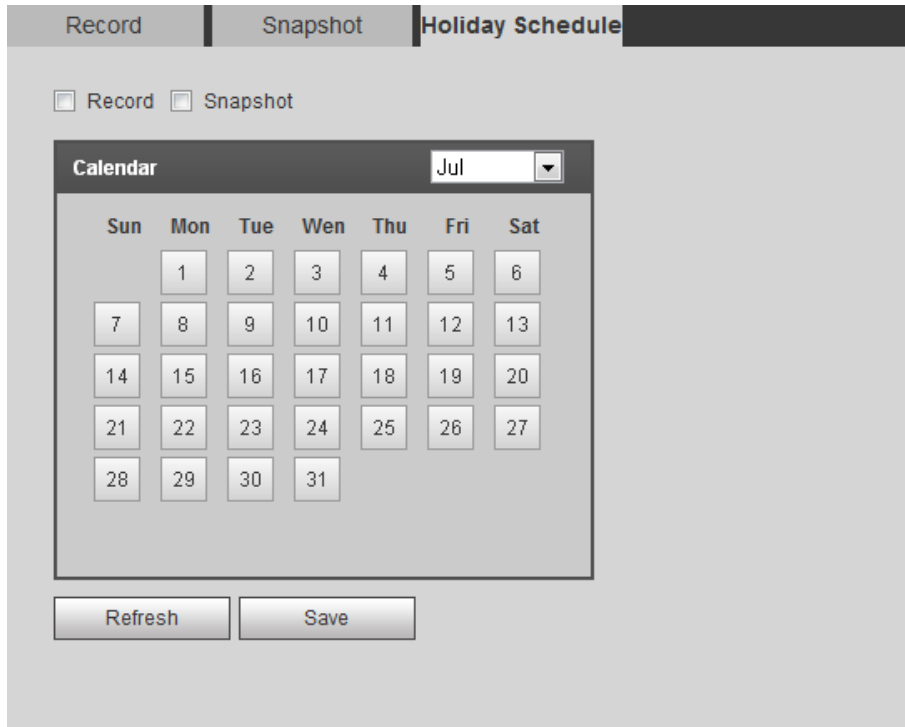
Prerequisites

- Set the record mode to be **Auto** in **Record Control**.
- Configure holiday record and snapshot schedule.

Procedure

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

Figure 4-62 Holiday schedule



Step 2 Select Record or Snapshot.

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

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



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

Step 4 Click **Save**.

4.4.2 Destination

4.4.2.1 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.

Background Information



Local is displayed only on models that support SD card.

Procedure

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

Figure 4-63 Path

Record			Snapshot		
Event Type	Scheduled	Alarm	Event Type	Scheduled	Alarm
Local	☒	☒	Local	☒	☒
FTP	☐	☐	FTP	☐	☐
NAS	☐	☐	NAS	☐	☐

Default Refresh Save

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

Table 4-24 Description of path parameters

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

Step 3 Click **Save**.

Step 4 Configure other path parameters on **Destination** , **FTP** or **NAS** page.

4.4.2.2 Local

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



Functions might vary with different models.

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

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



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

4.4.2.3 FTP

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

Procedure

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

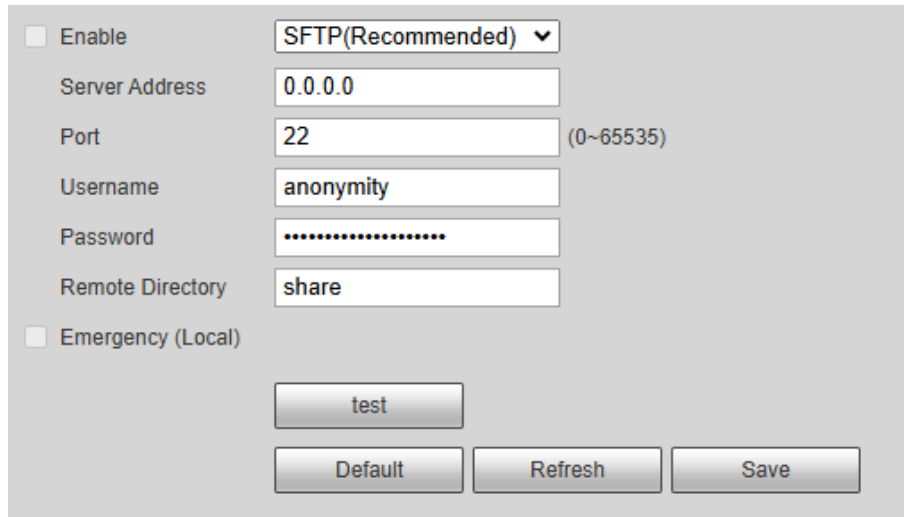
Step 2 Select the Enable check box, and select the FTP type.



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

Step 3 Configure FTP parameters.

Figure 4-64 FTP



The screenshot shows the FTP configuration window. At the top, there is an 'Enable' checkbox and a dropdown menu set to 'SFTP(Recommended)'. Below these are input fields for 'Server Address' (0.0.0.0), 'Port' (22, with a range of 0~65535), 'Username' (anonymity), 'Password' (masked with dots), and 'Remote Directory' (share). There is also an 'Emergency (Local)' checkbox. At the bottom, there are four buttons: 'test', 'Default', 'Refresh', and 'Save'.

Table 4-25 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, and it is shared by default.
Directory Structure	Set the directory structure, which supports three levels at most.
Level 1 Directory	Set the directory name, and you can customize the name.
Level 2 Directory	When you select Custom , enter the custom directory name, which supports numbers, English letters, underlines and dashes.
Level 3 Directory	

Parameter	Description
Customized Picture Name	Click Setting to set picture name. ● Date&Time is required, and it is selected by default. ● Select the other fields of the name, and the corresponding instruction will be displayed on the screen. ● Double-click the symbols under Separator, you can customize the separator. ● Double-click Custom, you can customize the files of the picture name. ● Click the arrow under Ordering, and you can adjust the ordering of the file.  Date&Time and Millisecond is a whole, click the arrow of any one of the two fields, the two moves together. ● The real-time value of Millisecond will be displayed for precise snapshot, and for schedule and normal event, the millisecond displays 0000.
Emergency (Local)	Select Emergency (Local) , and when the FTP server does not work, all the files are saved to the internal SD card.

Step 4 Click **Save**.

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

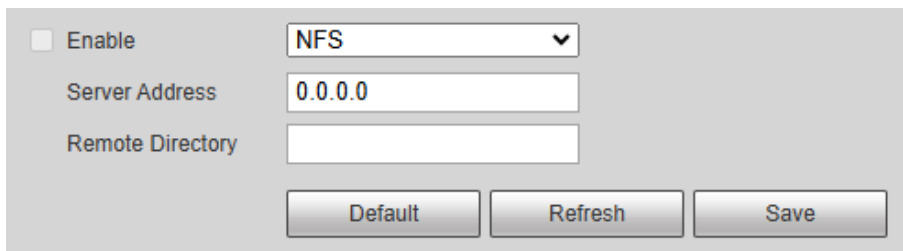
4.4.2.4 NAS

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.

Procedure

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

Figure 4-65 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 to share files through TCP/IP.
- **SMB** (Server Message Block): Provides shared access for clients and the server.

Step 3 Configure NAS parameters.

Table 4-26 Description of NAS parameters

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

Step 4 Click **Save**.

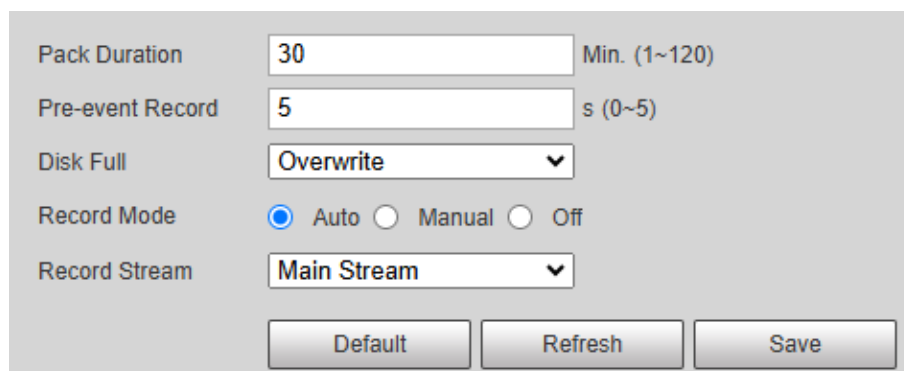
4.4.3 Record Control

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

Procedure

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

Figure 4-66 Record control



Step 2 Set parameters.

Table 4-27 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**.

4.5 System

This chapter introduces system configurations, including general settings, date & time, account, safety, default, import and export configurations, auto maintenance, and upgrade.

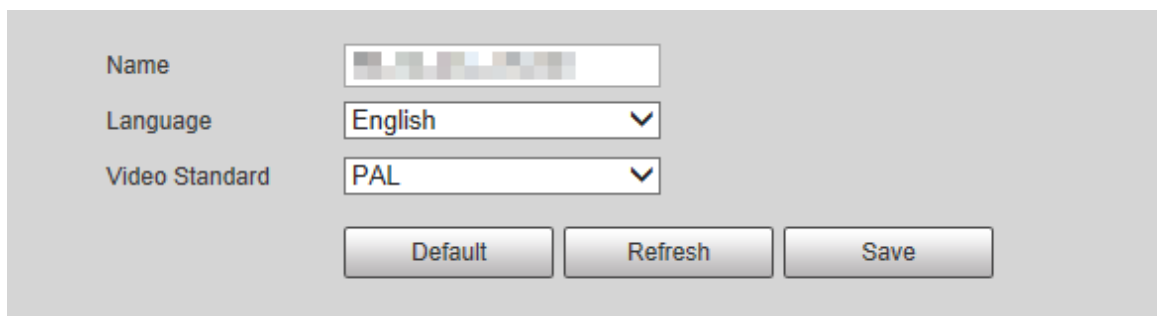
4.5.1 General Settings

You can configure general settings and date & time on **General** page.

4.5.1.1 General

You can configure radar name, system language and video format.

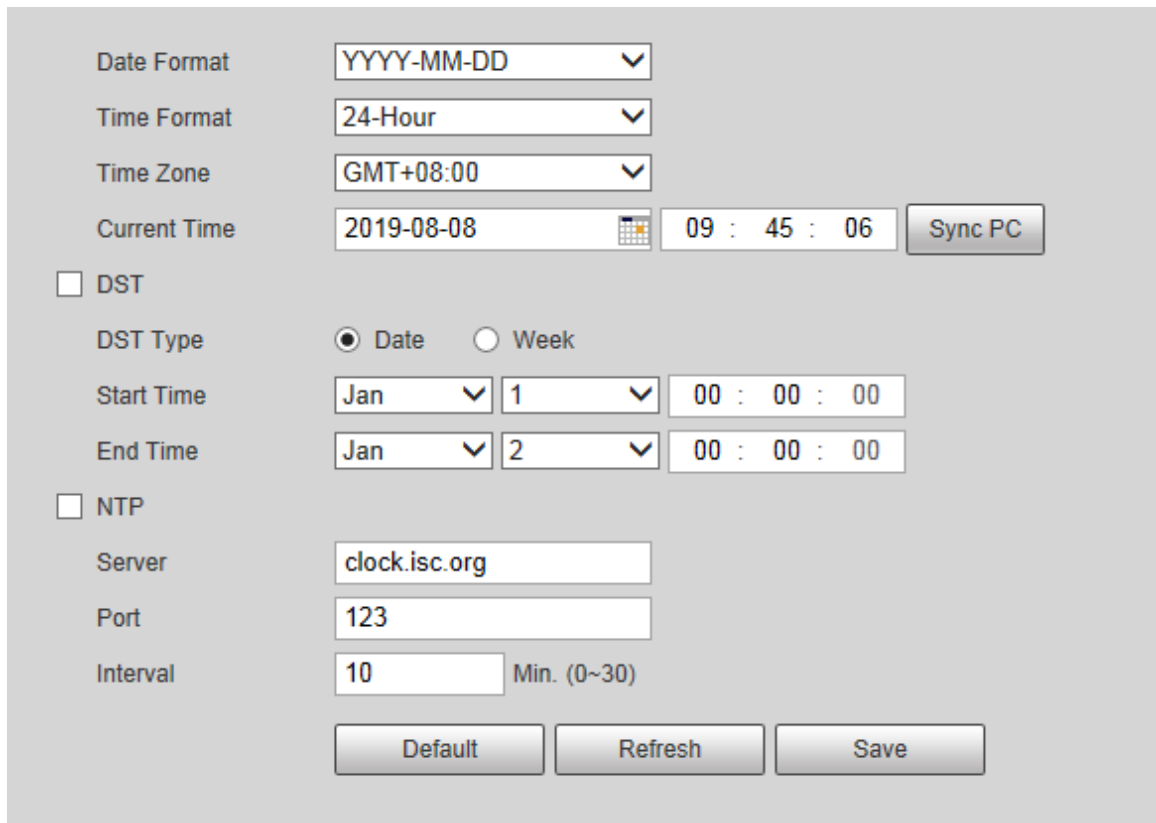
Figure 4-67 General



4.5.1.2 Date & Time

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

Figure 4-68 Date & Time



Date Format:

 Time Format:

 Time Zone:

 Current Time:

☐ DST

 DST Type: ☒ Date ☐ Week

 Start Time:

 End Time:

☐ NTP

 Server:

 Port:

 Interval: Min. (0~30)

4.5.2 Account

4.5.2.1 Account Name

You can add, delete, or modify users and groups. Managing users and groups are only available for administrator users.

- The maximum length of the user or group name is 15 characters. A user name can only consist of numbers, letters, underline, dot and @. A group name can only consist of numbers, letters, and underline.
- 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 ' " ; &). Follow the password security notice to set a high security level password. Make sure that the new password and the confirmed password are the same.
- You can have 18 users and 8 groups at most according to factory settings.
- You can manage users in two methods: Single user or group. Duplicate usernames or group names are not allowed. A user can be in only one group at a time.
- Online users cannot modify their own authority.
- There is one admin by default which has the highest authority.

You are admin user by default. You can add users, delete added users, modify user password, and log in anonymously.

Select **Setting** > **System** > **Account** > **Account** > **Username**. The **Username** page is displayed.

Figure 4-69 Username

☐ Anonymous Login

No.	Username	Group Name	Memo	Restricted Login	Modify	Delete
1	admin	admin	admin's account	/		
2	test2	user				
3	testb	user				
4	test3975	user				
5	admin1	admin				
6	test	test				

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

Add User

Anonymous Login

By selecting **Anonymous Login** check box, you can log in with only entering IP address instead of username and password. Anonymous users only have live view authority. Under **Anonymous Login**, you can log in with other account after clicking **Logout**.

Adding a User

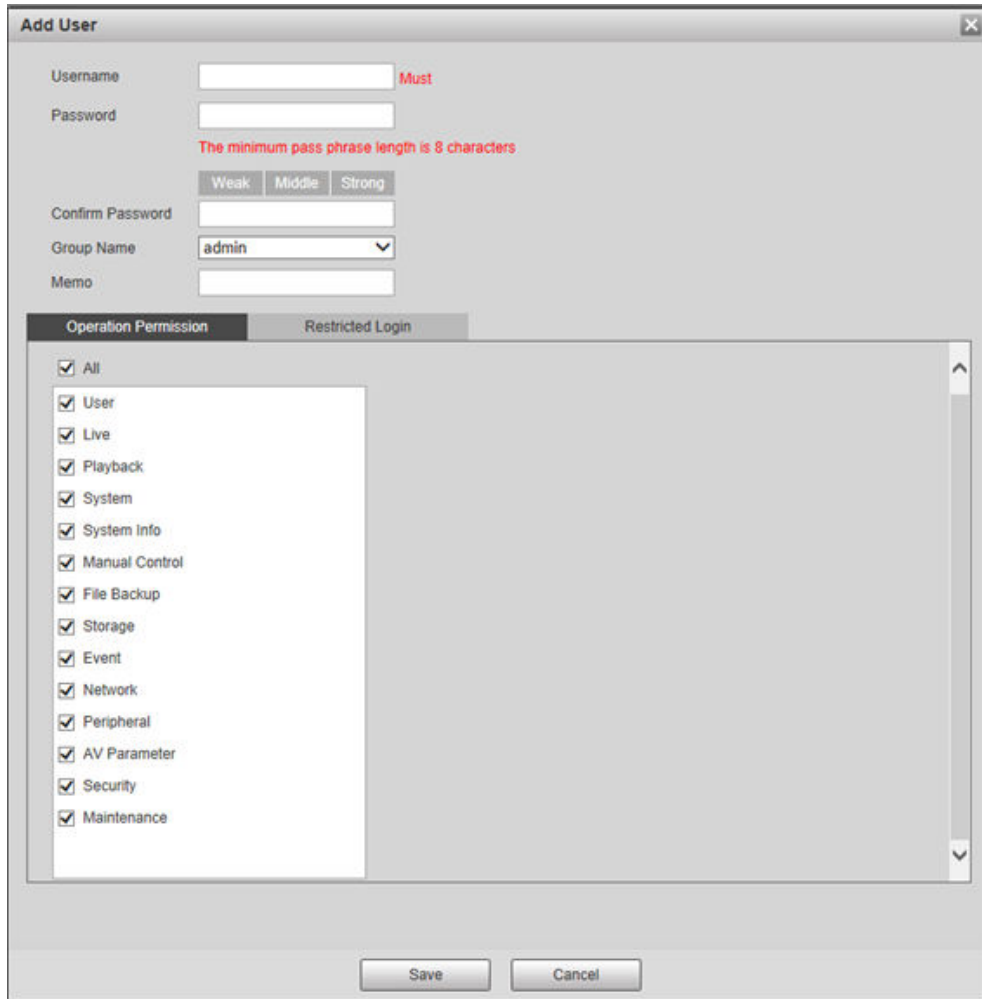
You can add users to the group, and configure user authority.



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

1. Click Add User.

Figure 4-70 Add user

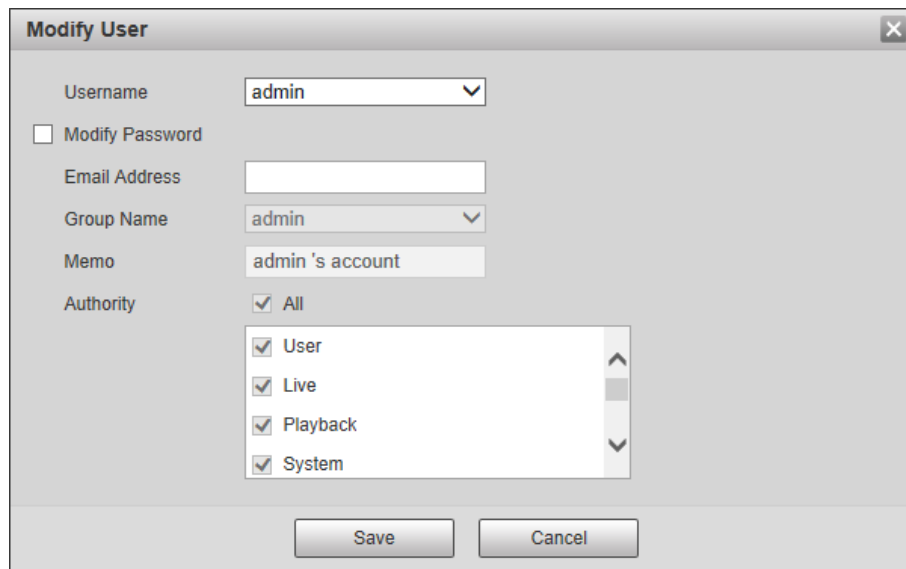


2. Enter username and password, and then select group and operation permission.



- A user can be in only one group at a time, and the group users can own authorities within group authority range.
 - It is recommended to give fewer authorities to normal users than premium users.
3. (Optional) Click **Restricted Login** to set IP address, validity period, and time range of the added user.

Figure 4-71 Modify user

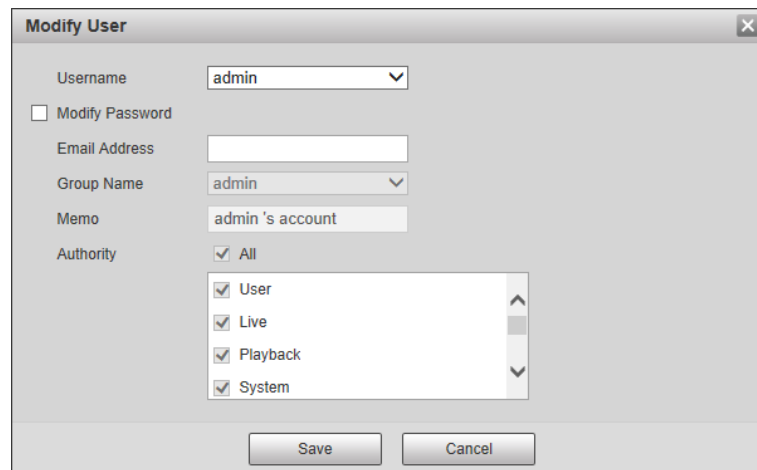


4. Click **Save**.

Modifying a User

1. Click  of the selected user.

Figure 4-72 Modify user



2. Modify user information as needed.
3. Click **Save**.

Modifying the Password

1. Click  of the selected user.
2. Select **Modify Password** check box.
3. Enter the old password, new password, and then confirm the password.
4. Click **Save**.

Deleting a User

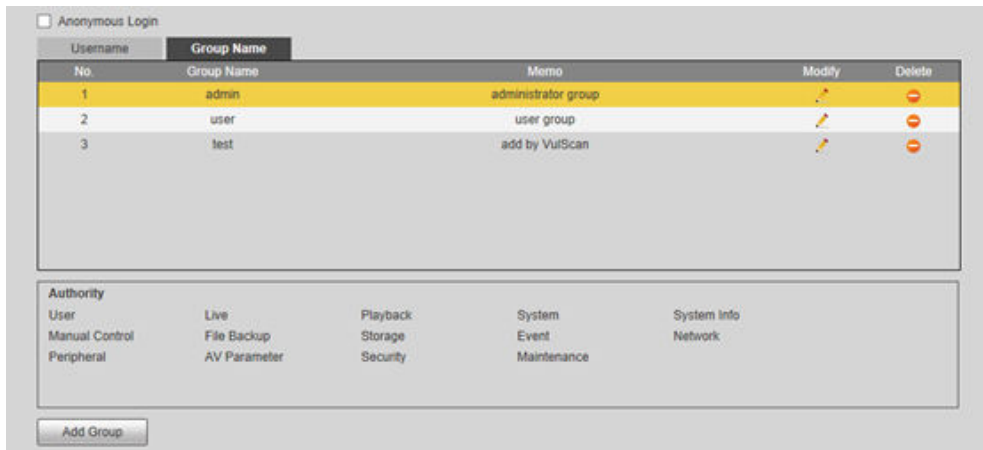
Click  to delete the added user.

Group Name

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

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

Figure 4-73 Group name



No.	Group Name	Memo	Modify	Delete
1	admin	administrator group		
2	user	user group		
3	test	add by VulScan		

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

Add Group

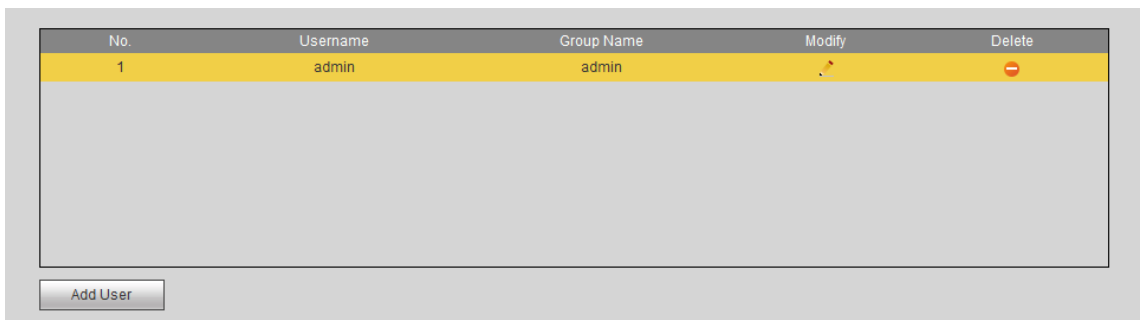
4.5.2.2 ONVIF User

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

Procedure

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

Figure 4-74 ONVIF user

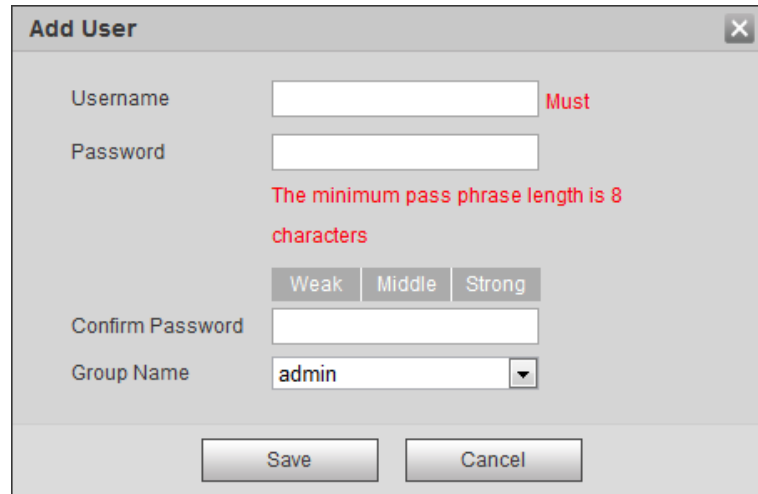


No.	Username	Group Name	Modify	Delete
1	admin	admin		

Add User

Step 2 Click Add User.

Figure 4-75 Add user



Step 3 Configure user parameters.

Table 4-28 Description of user parameters

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

Step 4 Click **Save**.

The newly added user displays in the username list.

Related Operations

Edit user information

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

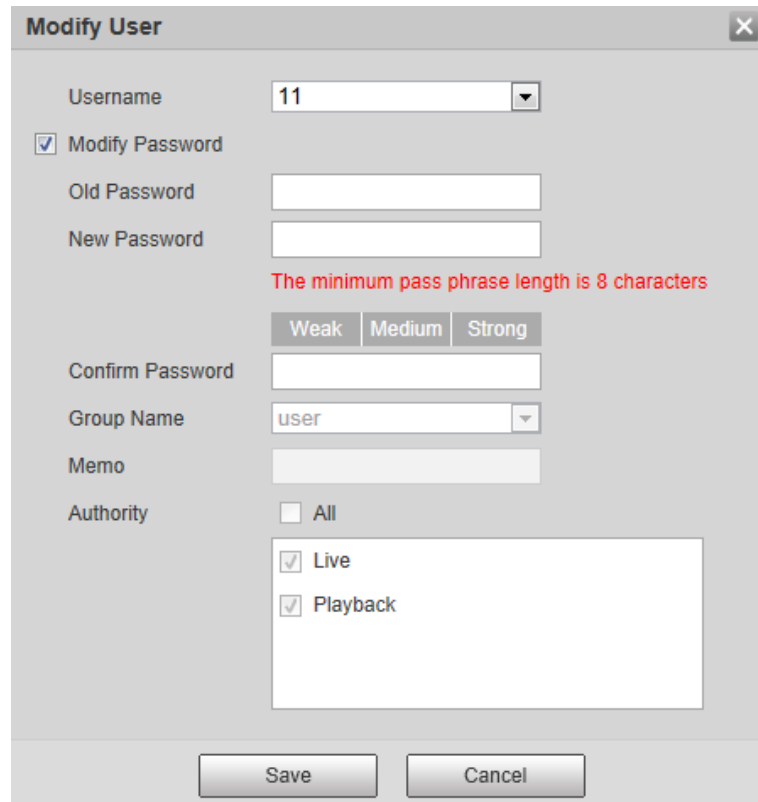


You can only change the password of the admin.

The methods of changing password vary with different accounts.

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

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

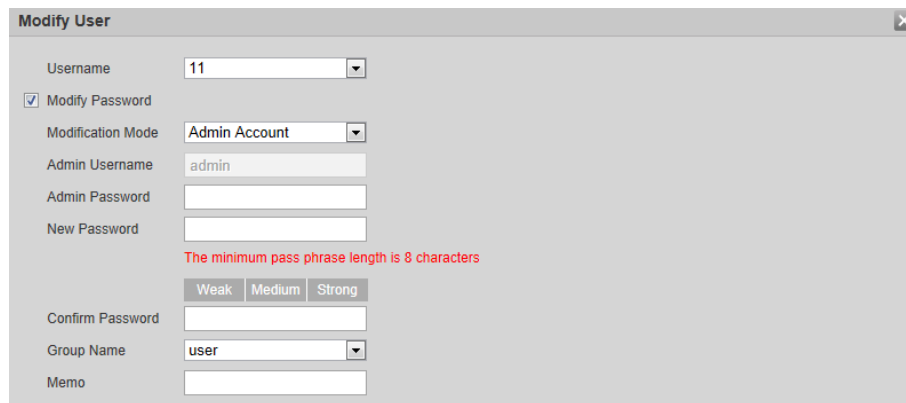


The 'Modify User' dialog box shows the following fields and options:

- Username:** A dropdown menu with '11' selected.
- Modify Password:** A checked checkbox.
- Old Password:** A text input field.
- New Password:** A text input field.
- Confirm Password:** A text input field.
- Group Name:** A dropdown menu with 'user' selected.
- Memo:** A text input field.
- Authority:** A section with a 'All' checkbox and a list of permissions: 'Live' and 'Playback', both of which are checked.
- Buttons:** 'Save' and 'Cancel' buttons at the bottom.
- Warning:** A red text message below the password fields: 'The minimum pass phrase length is 8 characters'.
- Strength Indicators:** Three buttons labeled 'Weak', 'Medium', and 'Strong' are positioned above the 'Confirm Password' field.

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

Figure 4-77 Change password through admin password (login with admin account)



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

- Username:** A dropdown menu with '11' selected.
- Modify Password:** A checked checkbox.
- Modification Mode:** A dropdown menu with 'Admin Account' selected.
- Admin Username:** A text input field with 'admin' entered.
- Admin Password:** A text input field.
- New Password:** A text input field.
- Confirm Password:** A text input field.
- Group Name:** A dropdown menu with 'user' selected.
- Memo:** A text input field.
- Warning:** A red text message below the password fields: 'The minimum pass phrase length is 8 characters'.
- Strength Indicators:** Three buttons labeled 'Weak', 'Medium', and 'Strong' are positioned above the 'Confirm Password' field.

Delete users

Click  to delete the added users.



Admin account cannot be deleted.

View the authorities

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

4.5.3 Safety

4.5.3.1 RTSP Authentication

Set the RTSP authentication mode.

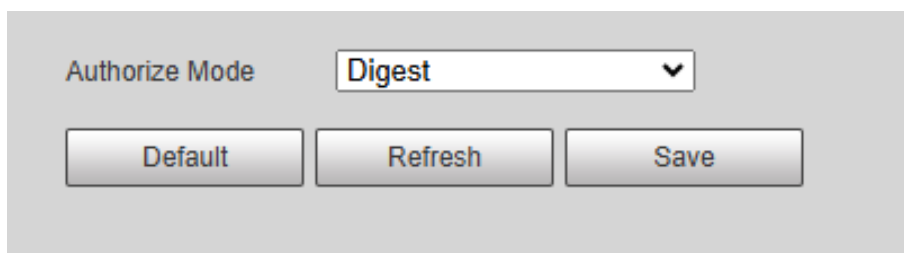
Procedure

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

Step 2 Select authorize Mode.

Supports **Basic** and **Digest** authentication methods. If authentication is not required, select **None**.

Figure 4-78 RTSP Authentication



Step 3 Click **Save**.

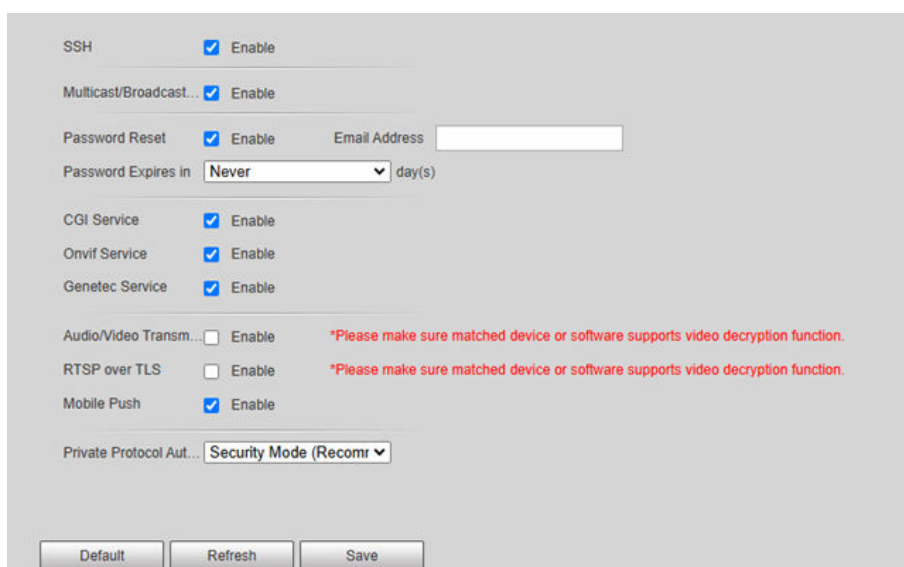
4.5.3.2 System Service

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 page. This is to enhance network and data security.

Procedure

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

Figure 4-79 System service



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

Table 4-29 Description of system service parameters

Function	Description
SSH	You can enable SSH authentication to perform safety management.
Multicast/Broadcast Search	Enable this function, and then when multiple users are previewing the device video image simultaneously through network, they can find your device with multicast/broadcast protocol.
Password Reset	Manage system security with this function.
Password Expires in	When the device uses the password for longer than the setting value, the user will be prompted to change the password.
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.
RTSP over TLS	Enable this function,use TLS tunnel to encrypt RTSP data transmission.
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.
Pravite Protocol Authentication Mode	Set this value, support security mode and compatibility mode.

Step 3 Click **Save**.

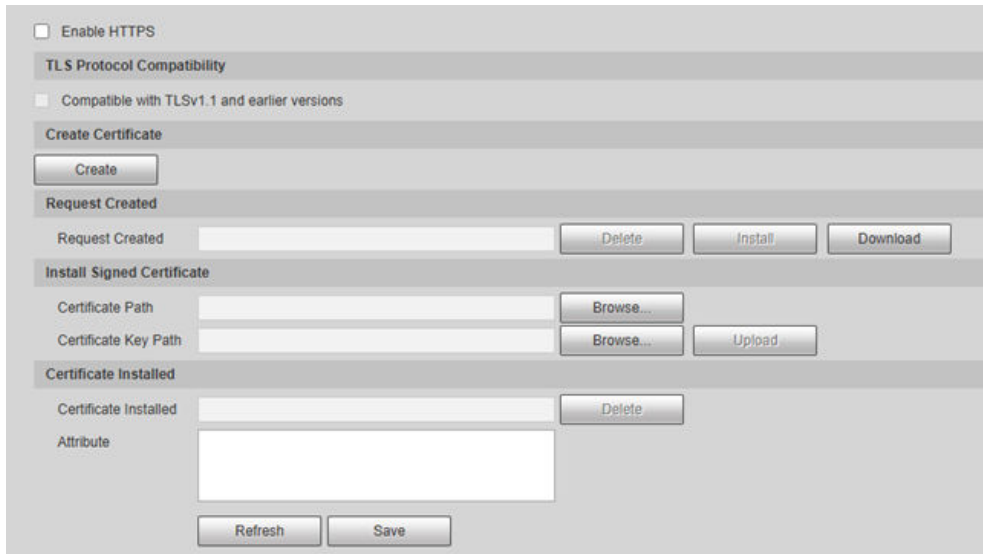
4.5.3.3 HTTPS

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**.

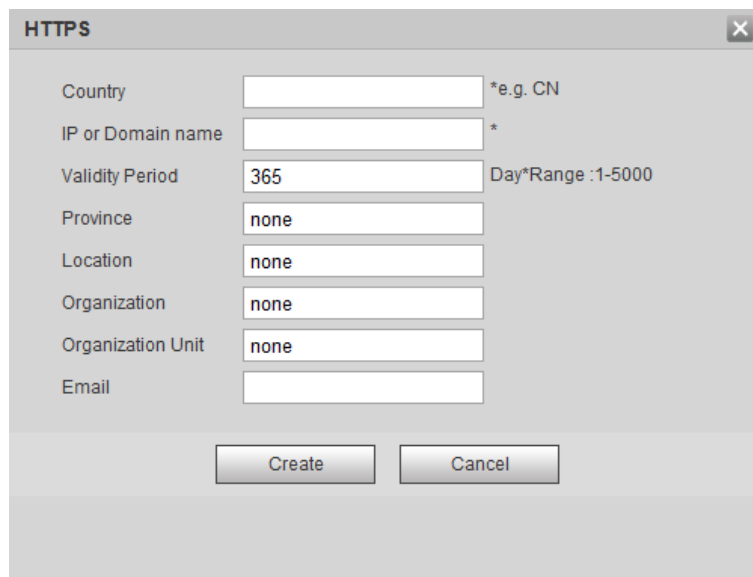
Figure 4-80 HTTPS



Step 2 Create a certificate or upload an authenticated certificate.

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

Figure 4-81 HTTPS dialog box



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

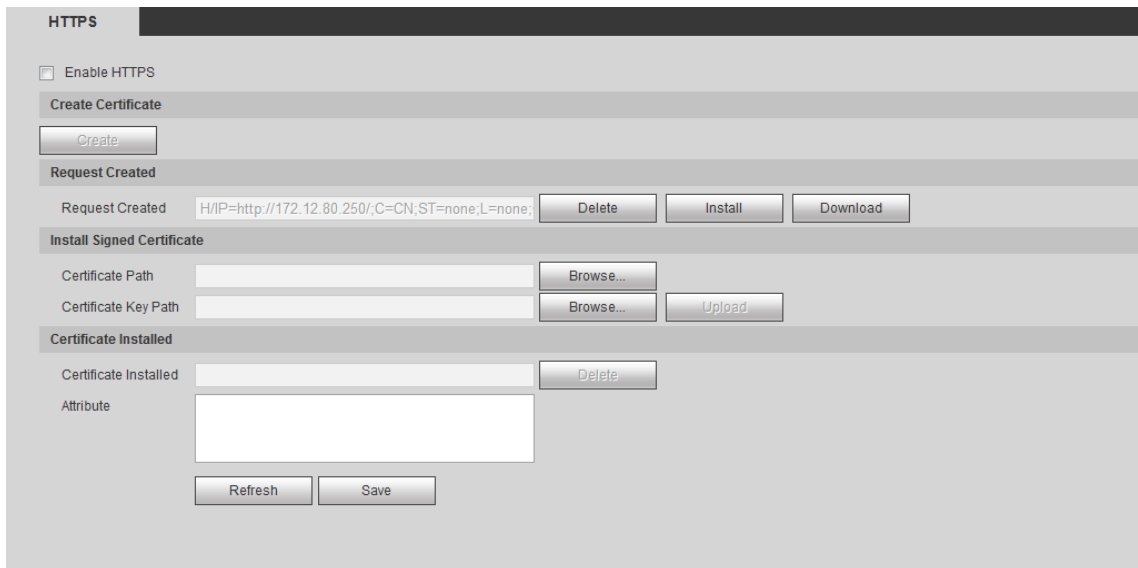
Step 3 Enter the required information and then click **Create**.



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

Step 4 Click **Install**.

Figure 4-82 Certificate installation



The screenshot shows the 'HTTPS' configuration page. It includes a checkbox for 'Enable HTTPS'. Below this is the 'Create Certificate' section with a 'Create' button. The 'Request Created' section shows a text field with the value 'H/IP=http://172.12.80.250;/C=CN,ST=none,L=none;' and buttons for 'Delete', 'Install', and 'Download'. The 'Install Signed Certificate' section has fields for 'Certificate Path' and 'Certificate Key Path', each with a 'Browse...' button, and an 'Upload' button. The 'Certificate Installed' section has a 'Certificate Installed' field with a 'Delete' button and an 'Attribute' field. At the bottom are 'Refresh' and 'Save' buttons.

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

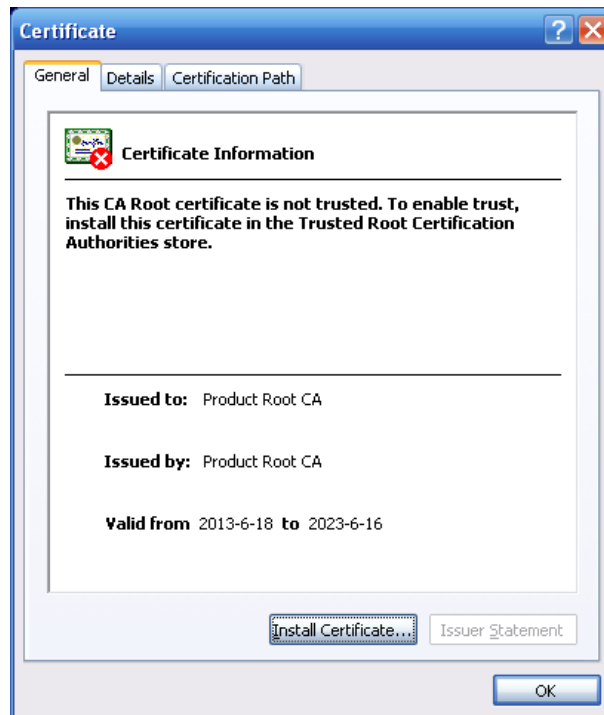
Step 6 Click Download Root Certificate.

Figure 4-83 File download



Step 7 Click **Open**.

Figure 4-84 Certificate information



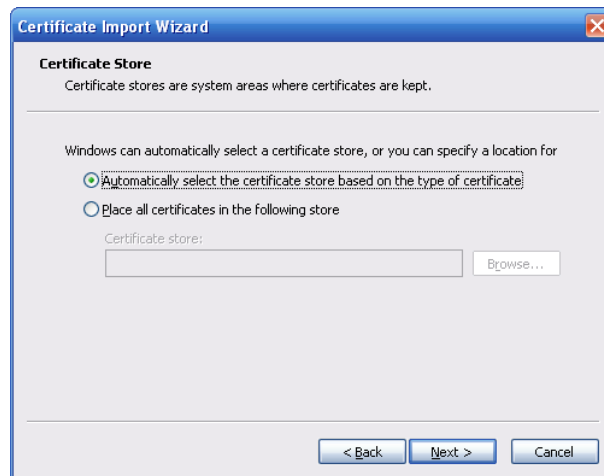
Step 8 Click **Install Certificate**.

Figure 4-85 Certificate import wizard (1)



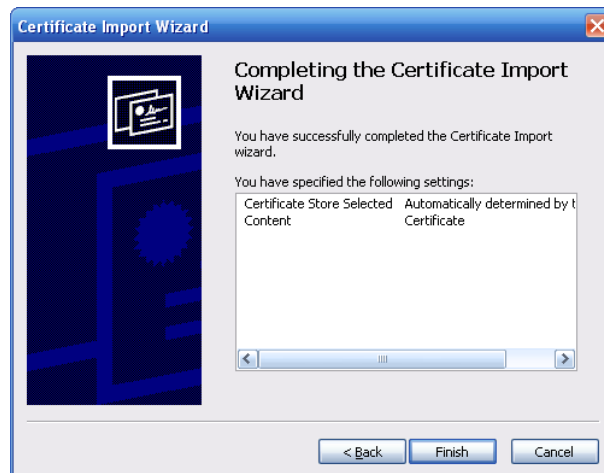
Step 9 Click **Next**.

Figure 4-86 Certificate store



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

Figure 4-87 Certificate import wizard (2)



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

Figure 4-88 Import succeeds



4.5.3.4 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.
 - ◇ **Allowlist:** Only when the IP/MAC of your PC in the allowlist, can you access the camera. Ports are the same.

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



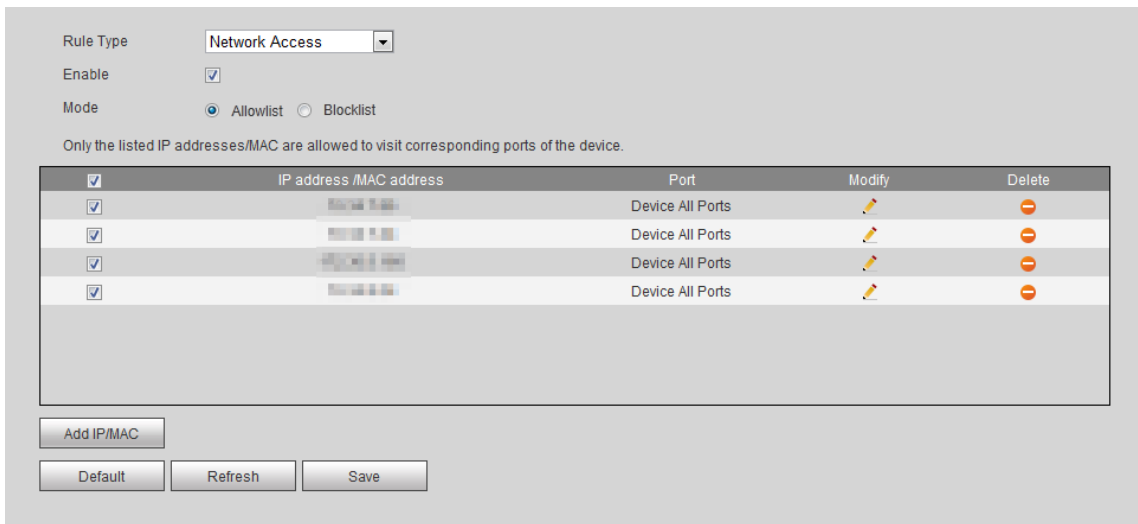
- You cannot set allowlist or blocklist for camera IP or MAC addresses.
- You cannot set allowlist or blocklist for port MAC addresses.
- When the IP addresses of the camera and your PC are in the same LAN, MAC verification takes effect.
- When you access the camera through internet, the camera verifies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

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

Procedure

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

Figure 4-89 Firewall



Rule Type: Network Access

Enable: ☒

Mode: ☒ Allowlist ☐ Blocklist

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

☒	IP address / MAC address	Port	Modify	Delete
☒	192.168.1.1	Device All Ports		
☒	192.168.1.2	Device All Ports		
☒	192.168.1.3	Device All Ports		
☒	192.168.1.4	Device All Ports		

Add IP/MAC

Default Refresh Save

2. Select **Network Access** from **Rule Type** list, and then select the **Enable** check box.
 - Enable **PING prohibited** and **Prevent Semijoin**, and click **Save**. You do not need to configure parameters.
 - Enable **Network Access**, and configure allowlist and blocklist.
 - ◇ Select the mode: **Allowlist** and **Blocklist**.
 - ◇ Click **Add IP/MAC**.

Figure 4-90 Add IP/MAC

The 'Add IP/MAC' dialog box is shown with the following settings:

- Rule Type: IP Address
- IP Version: IPv4
- IP Address: 1
- Device All Ports: ☐
- Device Start Server...: 1
- Device End Server...: 1

Buttons: OK, Cancel

3. Configure parameters.

Table 4-30 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 allowlist or restricted list.
Device All Ports	Set access ports. You can select all ports or the ports in defined areas.
Device Start Server Port	- Device all ports: Set all IP port in allowlist or Blocklist. When selecting BlockList in Mode, and All IP Address in Rule Type, you cannot select the Device All Ports check box. - Device start server port and Device end server port: Set Device start server port and device end server port, and the range is 1–65535.
Device End Server Port	

4. Click **OK**, and the **Firewall** page is displayed.

5. Click **Save**.

4.5.4 Default

Restore the radar to default configurations or factory settings.

Figure 4-91 Default

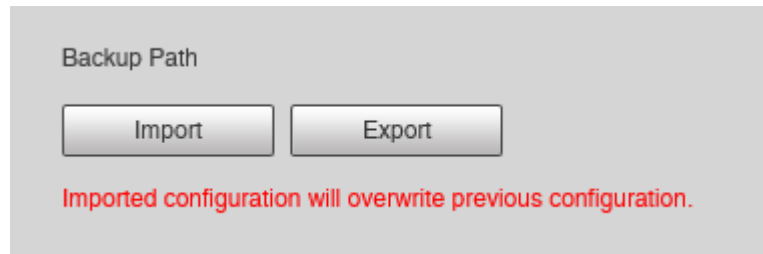
The 'Default' settings page contains the following information:

- Default**: Other configurations will be recovered to default except network IP address, user management and so on.
- Factory Default**: Completely recover device parameters to factory default.

4.5.5 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.

Figure 4-92 Import/Export



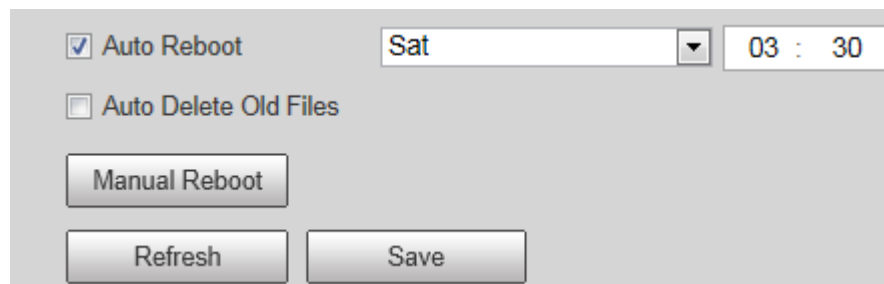
- Click **Export** to export the configuration file (.backup file) to local.
- Click **Import** to import the configuration file into the system.

4.5.6 Setting Auto Maintain

4.5.6.1 Auto Maintain

You can restart the system manually, or set the time of auto restarting and auto deleting old files. The system will execute the corresponding actions at the defined time.

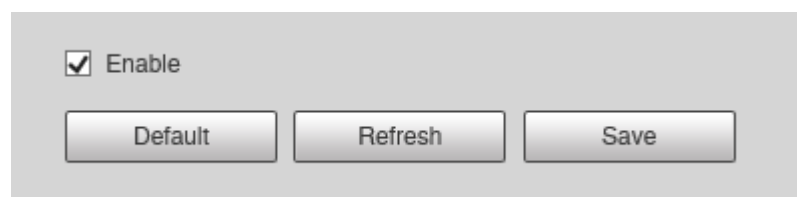
Figure 4-93 Auto maintain



4.5.6.2 Emergency Maintenance

You can enable this function when an emergency occurs in the system.

Figure 4-94 Emergency maintenance



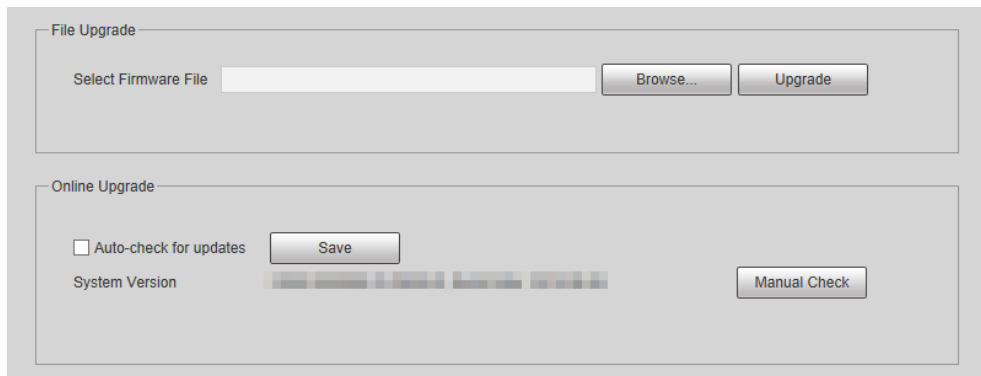
4.5.7 Upgrade

You can upgrade the system to the latest version to improve radar function and stability.



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

Figure 4-95 Upgrade



4.6 Information

4.6.1 Version

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

Select **Setting** > **Information** > **Version** to view the version information.

4.6.2 Querying Log

4.6.2.1 Log

You can view and back up logs.

Procedure

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

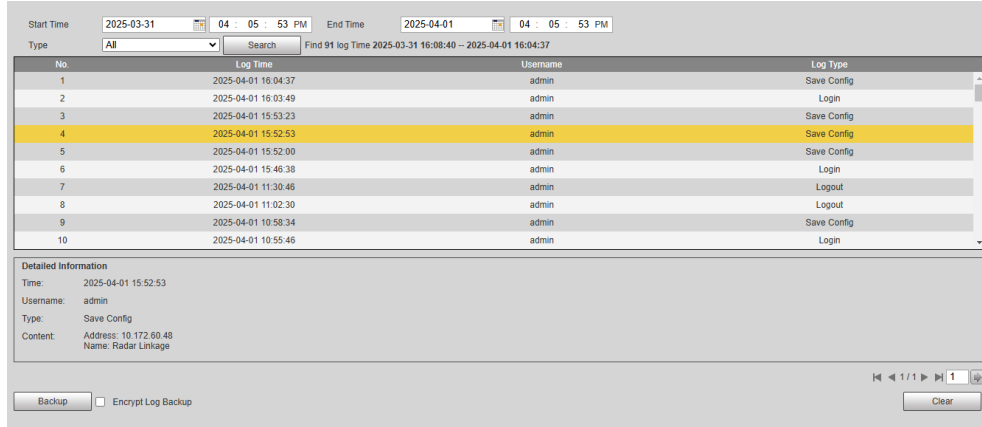
The log type includes All, System, Setting, Data, Event, Record, Account, and Safety.

- **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.
- Click **Clear**, and then you can delete all logs.

Figure 4-96 Log (details)



No.	Log Time	Username	Log Type
1	2025-04-01 16:04:37	admin	Save Config
2	2025-04-01 16:03:49	admin	Login
3	2025-04-01 15:53:23	admin	Save Config
4	2025-04-01 15:52:53	admin	Save Config
5	2025-04-01 15:52:00	admin	Save Config
6	2025-04-01 15:46:38	admin	Login
7	2025-04-01 11:30:46	admin	Logout
8	2025-04-01 11:02:30	admin	Logout
9	2025-04-01 10:58:34	admin	Save Config
10	2025-04-01 10:55:46	admin	Login

Detailed Information
Time: 2025-04-01 15:52:53
Username: admin
Type: Save Config
Content: Address: 10.172.60.48
Name: Radar Linkage

Backup ☐ Encrypt Log Backup Clear

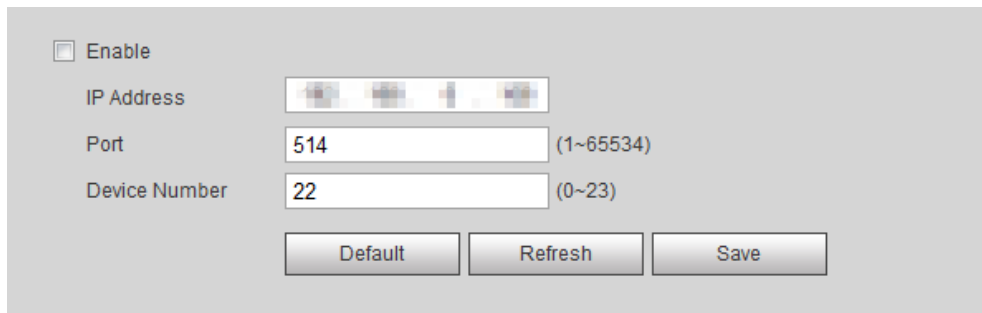
4.6.2.2 Remote Log

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

Procedure

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

Figure 4-97 Remote log



☐ Enable

IP Address

Port (1~65534)

Device Number (0~23)

Default Refresh Save

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

Step 3 Set address, port and device number.

Step 4 Click **Save**.

4.6.3 Online User

View all the current users logging in to web.

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

Figure 4-98 Online user

No.	Username	User Local Group	IP Address	User Login Time
1	admin	admin	10.33.123.55	2025-09-11 19:04:12
2	admin	admin	10.33.7.46	2025-09-11 19:08:43

Refresh

4.6.4 Legal Information

You can view device information such as software license agreement, privacy policy, and open source software notice.

Select **Setting** > **Information** > **Version** to view the version information.

5 Alarm

You can subscribe alarm messages and view the triggered alarm event information on the right column of **Alarm** page. Alarm prompt and alarm tone can also be selected as a reminder.

Click **Alarm** tab, and then the **Alarm** page is displayed.

Figure 5-1 Alarm

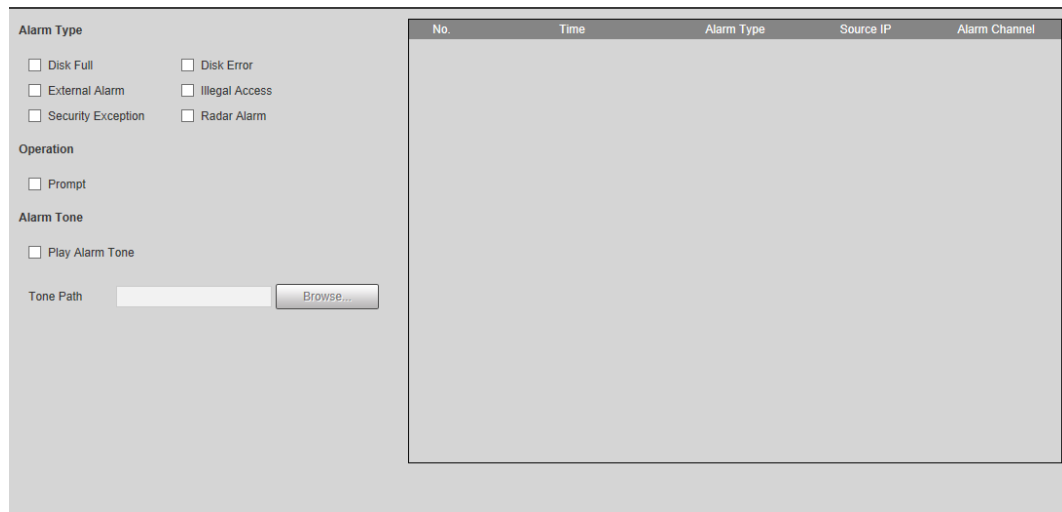


Table 5-1 Alarm parameter descriptions

Parameter	Name	Description
Alarm Type	Disk Full	Select to record the alarm when disk is full.
	Disk Error	Select to record the alarm when disk malfunctions.
	External Alarm	Select to record the alarm when radar receives external alarm.
	Illegal Access	Select to record the alarm when unauthorized access occurs.
	Security Exception	Select to record the alarm when security exception occurs.
	Radar Alarm	Select to record the alarm when an alarm is triggered in the configured detection region.
Operation	Prompt	When an alarm is triggered, if you are not in Alarm page,  icon will be displayed on Alarm tab, and the alarm will be recorded automatically.  icon disappears when you click Alarm tab.  If you are in Alarm page, when the alarm is triggered,  icon will not be displayed, but the alarm will be recorded.
Alarm Tone	Play Alarm Tone	Select the function and choose audio file. When alarm occurs, system automatically generates alarm audio.

Parameter	Name	Description
	Tone Path	Select Browse... to choose alarm audio file.

Appendix 1 Parameter Description



Different device models support different expert parameters. Please refer to the actual page for details.

Radar chip transmit power

Radar transmit power level. The larger the gear value you set, the longer the detection distance you will get.

Radar chip signal receiving gain

Under the same environmental condition, the higher the gain value you set, the longer the transmission distance you will get.

Radar transmitting beam angle

Beam angle: The angle created by the extension line of the radar's central axis to the point where the energy intensity is reduced to half.

You need to set the angles in four directions: **Radar transmitting beam angle 0**, **Radar transmitting beam angle 1**, **Radar transmitting beam angle 2**, **Radar transmitting beam angle 3**.

Stationary object filtering

This function means radar can filter out static targets. If the value is 0, the function is disabled. If the value is 1, dynamic point detection is normal and output no any static point.

Constant false alarm rate

Due to the widespread existence of noise in the external environment, it may have a negative impact on the results of radar target detection. This situation is called radar false alarm. When the intensity of external interference changes, the radar automatically adjusts its constant false alarm rate to ensure the accuracy of the radar monitoring results. The larger the value you set, the stronger shield against false ability alarm events.

Sensitivity

The sensitivity of identifying targets that cross the radar monitoring area. The smaller the sensitivity value you set, the stronger the cross-travel detection capability you will get, which may increase the risk of false alarms.

Maximum/Minimum detecting distance

Set the maximum/minimum detection distance value of the radar.

Maximum/Minimum detecting angle

Set the value (maximum/minimum angle $\times 10$) of radar detection. Unit: $^{\circ}$.

Target point (X/Y) coordinate (maximum/minimum) threshold

The target point coordinate threshold is used to determine whether the location of the radar echo signal is within a reasonable range. Echo signals that exceed the threshold range will be judged as noise. Set the value of the detection range. The larger the value you set, the larger coverage you will get.

Detecting target type

To distinguish the type of radar monitoring target according to the type of the set value.

Interference trajectory removal

When the radar detects that the target moves in a straight line, the angle of motion changes little, and the speed is fast, it will determine that the target trajectory is not real and remove it.

Target response sensitivity

The radar responsiveness to target detection. The larger value you set, the longer target display delay you will get. The smaller value you set, the faster response you will get. But you will get a higher risk of false alarms.

Track direction

The target trajectory is shown in radar monitoring screen. The trajectory in screen may appear angle varying, distance offsetting or reversed. The function is used to reduce the track fluctuation level of radar so that the overall monitoring track remains stable.

Detecting scenario

Different detection scenarios depend on the detection scenarios that the radar set.

Clustering/Correlation Threshold

The radar ability to identify targets can be adjusted by setting the clustering/correlation threshold value. The larger the value you set, the fewer noise points appear in radar detection image. The lower probability of identifying a point as a target point in the picture. However, real targets may be missed.

Maximum/Minimum output speed

Set the maximum/minimum limit of the target speed range that the radar supports detection. The maximum output speed is the upper limit of the target detection speed that radar can support, and the minimum output speed is the lower limit of the target detection speed that radar can support.

Displacement output threshold

The distance value is used to determine whether the target has moved. When the identified target object displacement exceeds the threshold, the radar triggers the displacement output signal. Unit: cm.

Radial displacement output threshold

Radial displacement output threshold is used to determine whether the target has moved. When the identified target object displacement exceeds the threshold, the radar triggers the displacement output signal.

Maximum/Minimum radar radial velocity

Maximum/Minimum radar radial velocity is used to determine whether the target has moved. When the identified target object radial velocity (absolute value) exceeds the threshold, the radar triggers the displacement output signal. Unit: m/s.

Maximum/Minimum tangential detection speed

Maximum/Minimum tangential detection speed is used to determine whether the target has moved. When the identified target object tangential detection speed (absolute value) exceeds the threshold, the radar triggers the displacement output signal. Unit: m/s.

Maximum output tangential speed

Sets the upper limit of target tangential detection velocity (absolute value) that the radar can support. Unit: m/s.

Track merging threshold

The maximum distance between points in a track when merging them.

Detecting threshold

Set the target power of recognition. When the detecting target power exceeds the threshold, the radar starts tracking the target.

Maximum/Minimum detecting speed

The detection speed used to determine whether the target has moved. When the identified target object detection speed (absolute value) exceeds the threshold, the radar triggers the displacement output signal. Unit: m/s.

Appendix 2 Important Safeguards and Warnings

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

Transportation Requirements



- Transport the Device under allowed humidity and temperature conditions.
- Do not place heavy stress on the Device, violently vibrate or immerse it in liquid during transportation.
- Pack the Device with packaging provided by its manufacturer or packaging of the same quality before transporting it.

Storage Requirements



- Store the Device under allowed humidity and temperature conditions.
- Avoid heavy stress, violent vibration, and immersion during storage.
- Do not place the Device in a humid, dusty, extremely hot or cold site that has strong electromagnetic radiation or unstable illumination.
- Do not place the Device in a place exposed to sunlight or near heat sources.

Installation Requirements



- Do not install the Device in humid, dusty or smoky places.
- Do not install the Device in a location that exposes it to sunlight or heat sources.
- Strictly comply with the local electrical safety code and standards.
- Make sure that the power supply is correct before use.
- Install the Device in a well-ventilated place, and do not block its ventilation.
- An emergency disconnect device must be installed during installation and wiring at a readily accessible location for emergency power cut-off.
- Protect the power cord and wires from being walked on or squeezed particularly at plugs, power sockets, and the point where they exit from the Device.
- Use the accessories suggested by the manufacturer. Installation and maintenance must be performed by qualified professionals.



Do not connect the Device to two or more kinds of power supplies, to avoid damage to the Device.



- Ground within the detection area must be hard ground. Concrete ground is the best to have. As for ground covered in vegetation, the height of the vegetation should be below 20 cm.
- Make sure there are no objects in the monitoring area blocking the device such as vegetation, buildings, and vehicles.
- Make sure the rack grounding terminal is reliably grounded during installation.

Operation Requirements



-  The Device or remote control of select models contains button batteries. Do not swallow the batteries due to the risk of chemical burns.

Possible result: The swallowed button battery can cause serious internal burns and death within 2 hours.

Preventive measures (including but not limited to):
 - ◇ Keep new and used batteries out of reach of children.
 - ◇ If the battery compartment is not securely closed, stop using the product immediately and keep out of reach of children.
 - ◇ Seek immediate medical attention if a battery is believed to be swallowed or inserted inside any part of the body.
- Battery Pack Precautions

Preventive measures (including but not limited to):
 - ◇ Do not transport, store or use the batteries in high altitudes with low pressure and environments with extremely high and low temperatures.
 - ◇ Do not dispose the batteries in fire or a hot oven, or mechanically crush or cut the batteries to avoid an explosion.
 - ◇ Do not leave the batteries in environments with extremely high temperatures to avoid explosions and leakage of flammable liquid or gas.
 - ◇ Do not subject the batteries to extremely low air pressure to avoid explosions and the leakage of flammable liquid or gas.



- Use the Device under allowed humidity and temperature conditions.
- Prevent liquid from dripping or splashing on the Device. Do not put any objects filled with liquid on top of the Device.
- Do not dismantle the Device, it can only be repaired by qualified professionals. Non-professionals dismantling the Device can result in it leaking water.
- Place the Device in a location that children cannot easily access.
- Do not spray paint, stick stickers, put colors, objects or dirt on the surface of the Device to avoid degrading the performance of the Device.
- This is a class 1 laser device. You can only insert modules that meet the requirements of class 1 lasers.

Maintenance Requirements



- Use accessories suggested by the manufacturer, and maintained by professionals.

- Battery Pack Precautions

Preventive measures (including but not limited to):

- ◇ Do not transport, store or use the batteries in high altitudes with low pressure and environments with extremely high and low temperatures.
- ◇ Do not dispose the batteries in fire or a hot oven, or mechanically crush or cut the batteries to avoid an explosion.
- ◇ Do not leave the batteries in environments with extremely high temperatures to avoid explosions and leakage of flammable liquid or gas.
- ◇ Do not subject the batteries to extremely low air pressure to avoid explosions and the leakage of flammable liquid or gas.

Appendix 3 Security Commitment and Recommendation

Zhejiang Dahua Vision Technology Co., Ltd. (hereinafter referred to as "Dahua") attaches great importance to cybersecurity and privacy protection, and continues to invest special funds to comprehensively improve the security awareness and capabilities of Dahua employees and provide adequate security for products. Dahua has established a professional security team to provide full life cycle security empowerment and control for product design, development, testing, production, delivery and maintenance. While adhering to the principle of minimizing data collection, minimizing services, prohibiting backdoor implantation, and removing unnecessary and insecure services (such as Telnet), Dahua products continue to introduce innovative security technologies, and strive to improve the product security assurance capabilities, providing global users with security alarm and 24/7 security incident response services to better protect users' security rights and interests. At the same time, Dahua encourages users, partners, suppliers, government agencies, industry organizations and independent researchers to report any potential risks or vulnerabilities discovered on Dahua devices to Dahua PSIRT, for specific reporting methods, please refer to the cyber security section of Dahua official website.

Product security requires not only the continuous attention and efforts of manufacturers in R&D, production, and delivery, but also the active participation of users that can help improve the environment and methods of product usage, so as to better ensure the security of products after they are put into use. For this reason, we recommend that users safely use the device, including but not limited to:

Account Management

1. Use complex passwords

Please refer to the following suggestions to set passwords:

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

2. Change passwords periodically

It is recommended to periodically change the device password to reduce the risk of being guessed or cracked.

3. Allocate accounts and permissions appropriately

Appropriately add users based on service and management requirements and assign minimum permission sets to users.

4. Enable account lockout function

The account lockout function is enabled by default. You are advised to keep it enabled to protect account security. After multiple failed password attempts, the corresponding account and source IP address will be locked.

5. Set and update password reset information in a timely manner

Dahua device supports password reset function. To reduce the risk of this function being used by threat actors, if there is any change in the information, please modify it in time. When setting security questions, it is recommended not to use easily guessed answers.

Service Configuration

1. Enable HTTPS

It is recommended that you enable HTTPS to access Web services through secure channels.

2. Encrypted transmission of audio and video

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

3. Turn off non-essential services and use safe mode

If not needed, it is recommended to turn off some services such as SSH, SNMP, SMTP, UPnP, AP hotspot etc., to reduce the attack surfaces.

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

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

4. Change HTTP and other default service ports

It is recommended that you change the default port of HTTP and other services to any port between 1024 and 65535 to reduce the risk of being guessed by threat actors.

Network Configuration

1. Enable Allowlist

It is recommended that you turn on the allowlist function, and only allow IP in the allowlist to access the device. Therefore, please be sure to add your computer IP address and supporting device IP address to the allowlist.

2. MAC address binding

It is recommended that you bind the IP address of the gateway to the MAC address on the device to reduce the risk of ARP spoofing.

3. Build a secure network environment

In order to better ensure the security of devices and reduce potential cyber risks, the following are recommended:

- Disable the port mapping function of the router to avoid direct access to the intranet devices from external network;
- According to the actual network needs, partition the network: if there is no communication demand between the two subnets, it is recommended to use VLAN, gateway and other methods to partition the network to achieve network isolation;
- Establish 802.1x access authentication system to reduce the risk of illegal terminal access to the private network.

Security Auditing

1. Check online users

It is recommended to check online users regularly to identify illegal users.

2. Check device log

By viewing logs, you can learn about the IP addresses that attempt to log in to the device and key operations of the logged users.

3. **Configure network log**

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

Software Security

1. **Update firmware in time**

According to the industry standard operating specifications, the firmware of devices needs to be updated to the latest version in time in order to ensure that the device has the latest functions and security. If the device is connected to the public network, it is recommended to enable the online upgrade automatic detection function, so as to obtain the firmware update information released by the manufacturer in a timely manner.

2. **Update client software in time**

We recommend you to download and use the latest client software.

Physical Protection

It is recommended that you carry out physical protection for devices (especially storage devices), such as placing the device in a dedicated machine room and cabinet, and having access control and key management in place to prevent unauthorized personnel from damaging hardware and other peripheral equipment (e.g. USB flash disk, serial port).

