

Security Radar

User's Manual



Foreword

General

This manual introduces the installation, functions and operations of the security radar (hereinafter referred to as "the radar"). Read carefully before using the device, and keep the manual safe for future reference.

Safety Instructions

The following signal words might appear in the manual.

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

Revision History

Version	Revision Content	Release Time
V1.0.0	First release.	August 2024

Privacy Protection Notice

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

About the Manual

- The manual is for reference only. Slight differences might be found between the manual and the product.
- We are not liable for losses incurred due to operating the product in ways that are not in

compliance with the manual.

- The manual will be updated according to the latest laws and regulations of related jurisdictions. For detailed information, see the paper user's manual, use our CD-ROM, scan the QR code or visit our official website. The manual is for reference only. Slight differences might be found between the electronic version and the paper version.
- All designs and software are subject to change without prior written notice. Product updates might result in some differences appearing between the actual product and the manual. Please contact customer service for the latest program and supplementary documentation.
- There might be errors in the print or deviations in the description of the functions, operations and technical data. If there is any doubt or dispute, we reserve the right of final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and company names in the manual are properties of their respective owners.
- Please visit our website, contact the supplier or customer service if any problems occur while using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Important Safeguards and Warnings

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

Operation Requirements



- Make sure that the power supply of the device works properly before use.
- Do not pull out the power cable of the device while it is powered on.
- Only use the device within the rated power range.
- Transport, use and store the device under allowed humidity and temperature conditions.
- Prevent liquids from splashing or dripping on the device. Make sure that there are no objects filled with liquid on top of the device to avoid liquids flowing into it.
- Do not disassemble the device.
- Checklist content.

Installation Requirements



WARNING

- Connect the device to the adapter before power on.
- Strictly abide by local electrical safety standards, and make sure that the voltage in the area is steady and conforms to the power requirements of the device.
- Do not connect the device to more than one power supply. Otherwise, the device might become damaged.



- Observe all safety procedures and wear required protective equipment provided for your use while working at heights.
- Do not expose the device to direct sunlight or heat sources.
- Do not install the device in humid, dusty or smoky places.
- Install the device in a well-ventilated place, and do not block the ventilator of the device.
- Use the power adapter or case power supply provided by the device manufacturer.
- The power supply must conform to the requirements of ES1 in IEC 62368-1 standard and be no higher than PS2. Note that the power supply requirements are subject to the device label.
- Connect class I electrical appliances to a power socket with protective earthing.
- Checklist content.

Maintenance Requirements

Checklist content.

Table of Contents

Foreword	I
Important Safeguards and Warnings	III
1 Installation	5
1.1 Environmental Requirements	5
1.2 Installing Radar	5
2 Logging in to the Web Client	6
2.1 Login	6
2.2 Resetting Password	6
3 Live View	9
4 Playback	10
5 Configuring Radar	11
5.1 Configuring Region Management	11
5.2 Configuring IVS Setup	12
5.3 Configuring Device Attitude	14
5.4 Configuring Linkage	14
5.4.1 Auto Calibration	14
5.4.2 Manual Calibration	15
6 Setting	17
6.1 Network	17
6.2 System	22
6.2.1 General	22
6.2.2 Account	24
6.2.3 Manager	28
6.2.4 Upgrade	29
6.3 Alarm	30

1 Installation

1.1 Environmental Requirements

- The installation site has enough space to install the radar and other accessories.
- The wall and pole for installation can carry eight times the weight of the radar and other accessories.
- For wall mount, the wall shall be thick enough to install expansion bolts.
- No large areas of metals or glass objects are within the radar detection range; otherwise mirrored alarm sites might occur. If the metal or glass object cannot be removed, do not let it face the front side of radar during installation. Because electromagnetic wave of the radar cannot penetrate objects such as buildings, rocks, and glasses, a blind zone will be formed behind these objects.
- No weed and swaying branch exists within the radar detection range, and trim regularly if any.
- No interference devices with strong electromagnetic or periodically rotating objects are near the radar or within its detection range, such as external units of air conditioners and wind-driven generators.
- Install the radar securely and stably to ensure detection precision and avoid misinformation.

1.2 Installing Radar

You need to prepare the following tools and cables before installation: Power cord, lightning protector, distribution box, air switch, PoE switch (optional), electric screwdriver, network cable, ladder, insulating gloves, and other things as needed.

2 Logging in to the Web Client

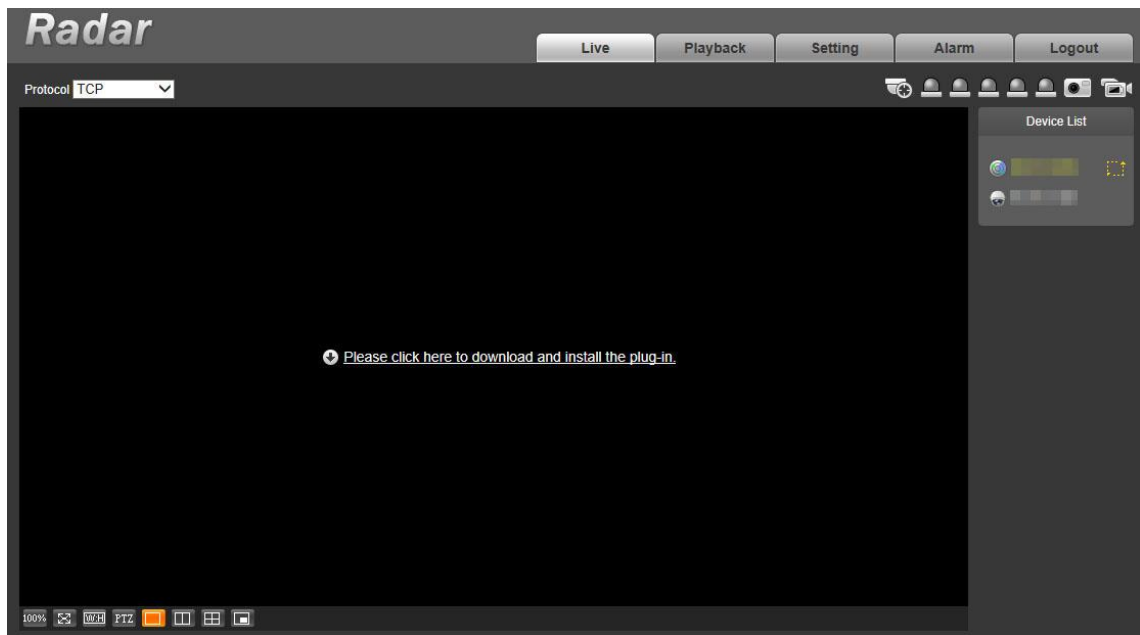
2.1 Login

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

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

The **Live** interface is displayed. See Figure 2-1.

Figure 2-1 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**.

Step 2 Download and install the plug-in according to the on-screen instructions.

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

2.2 Resetting Password

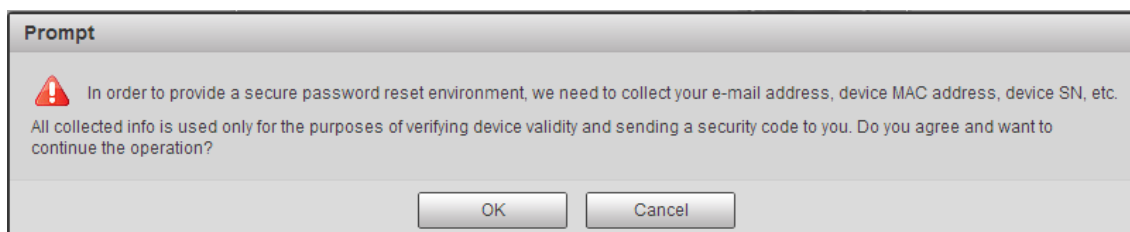
You can reset the admin password through the reserved email address when you forget it.

Step 1 Open IE browser, enter the IP address of the controller in the address bar, and then press Enter. The login interface is displayed.

Step 2 Click Forgot password?

The **Prompt** interface is displayed. See Figure 2-2.

Figure 2-2 Prompt



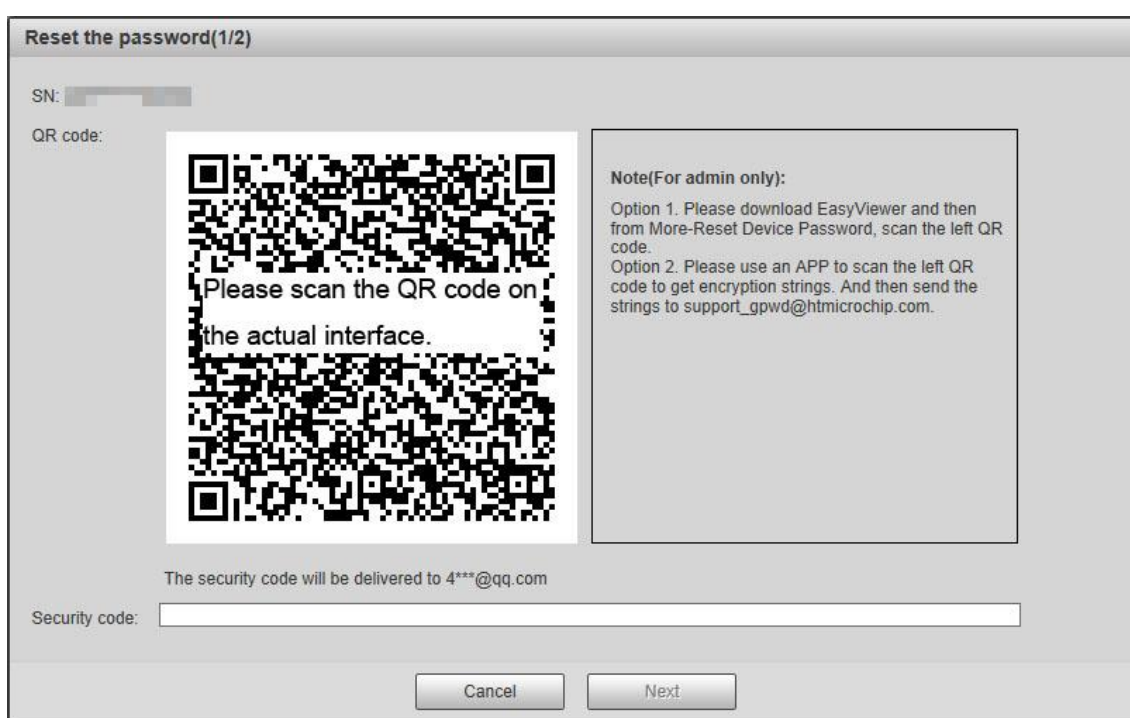
Step 3 Click **OK**.

The QR code scanning interface is displayed. See Figure 2-3.



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

Figure 2-3 QR code



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

The password resetting interface is displayed. See Figure 2-4.



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 2-4 Reset the password

Reset the password(2/2)

Username admin

Password

Weak Middle Strong

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

Confirm Password

Cancel Save

Step 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 interface is displayed.

3 Live View

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

Figure 3-1 Live view

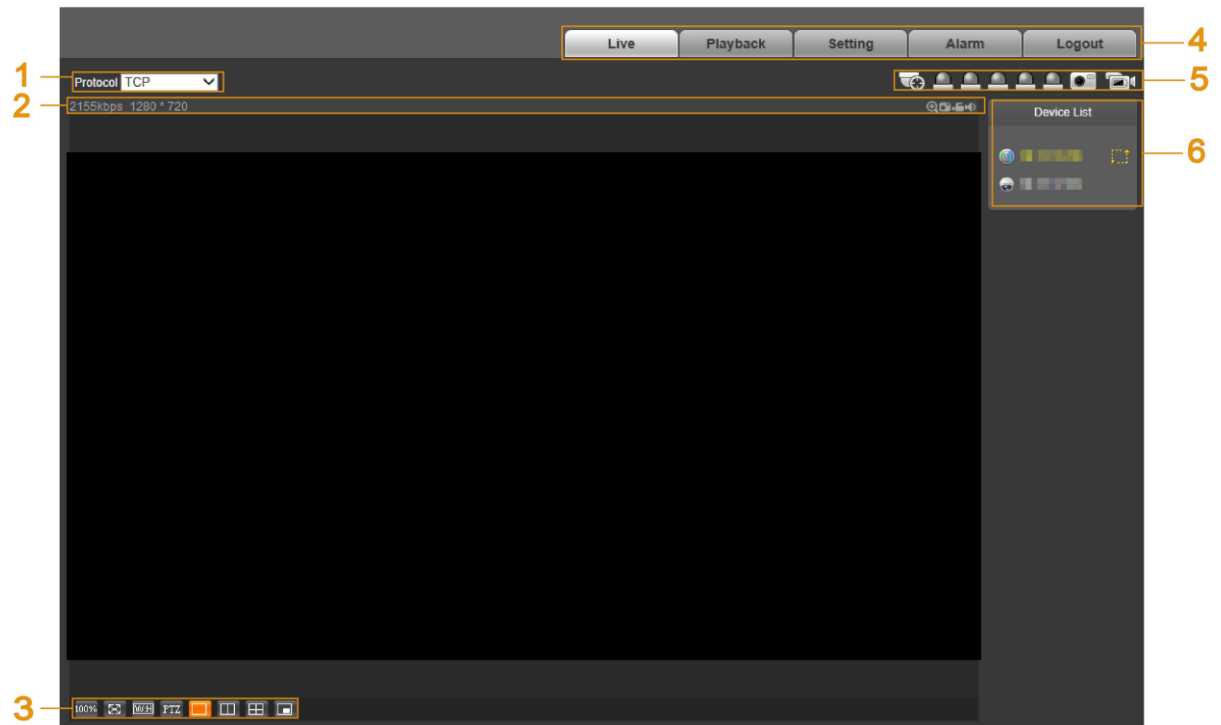


Table 3-1 Live view parameter descriptions

No.	Description	No.	Name
1	Set encoding mode.	2	Video tool.
3	Adjust video window.	4	Function tabs.
5	Function options.	6	Device list.

4 Playback

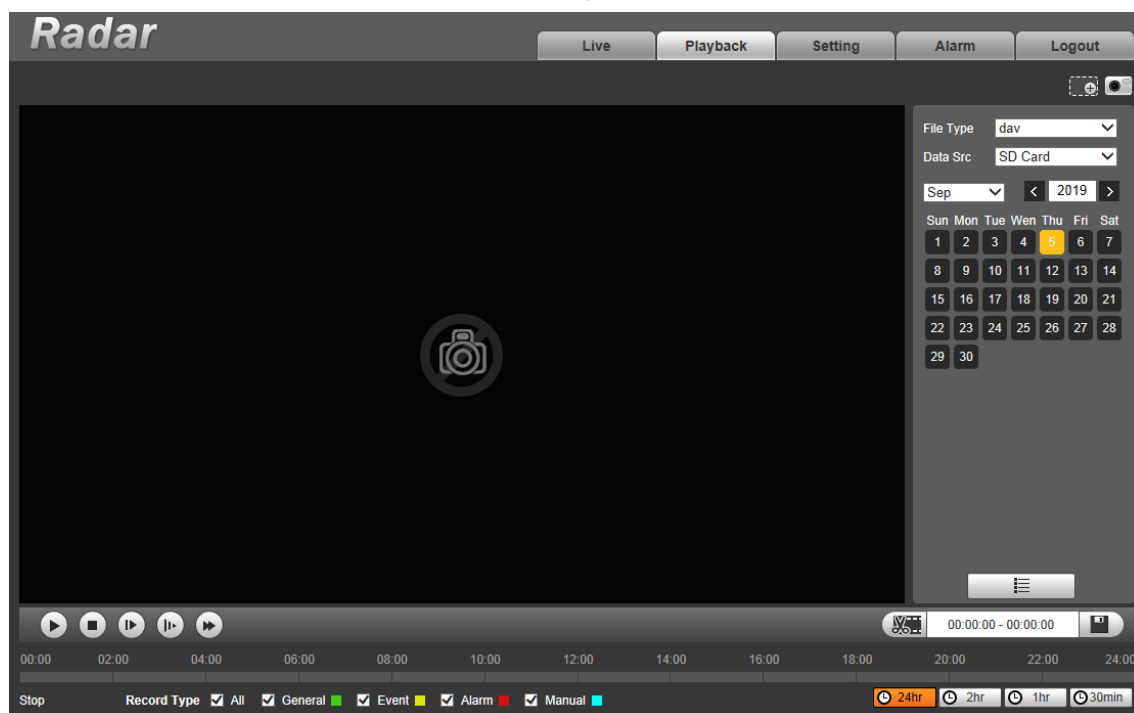
You can play back snapshots and videos saved in SD card.



- 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** interface is displayed. See Figure 4-1.

Figure 4-1 Playback



5 Configuring Radar



- The figures shown in this chapter are for reference only, and the actual interface shall prevail. See the web user's manual of the radar for detailed function instructions.
- Make sure that the IP addresses of your PC and the radar are in the same network segment. The default IP address of the radar is 192.168.1.108.
- You need to have relevant knowledge of radar product and its basic operations.

5.1 Configuring Region Management

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

Procedures

Step 1 Select Setting > Radar Settings > Region.

Figure 5-1 Region management

Enable	Number	Name	Area Type	Delete
☒	1	rule1	Intrusion	
☐	2	rule2	Intrusion	
☐	3	rule3	Intrusion	
☐	4	rule4	Intrusion	

Parameter Setup

Period:

Region Filter: ☐ Human ☐ Vehicle

Alarm Type:

☐ Speed Filtering

☒ Record
Record Delay: s (10-300)

☒ Relay-out
Alarm Delay: s (10-300)

☐ Send Email

☒ Audio Linkage
Play Count: (1-3)
File:

☒ White Light
Mode:
Flicker Frequency:
Duration: s (5-30)

☒ Snapshot

Step 2 Click , and then enter rule name at **Name** column, and then select an alarm type at **Area Type** column.

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

Step 4 For description of rules, see Table 5-1. After drawing, you can adjust the area by dragging the box angles. Click **Clear** to delete all drawn rules.

Table 5-1 Description of region management parameters (1)

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

Step 5 To configure arming/disarming period and alarm linkage.

Table 5-2 Description of region management parameters (2)

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

Step 6 Click **Save**.

5.2 Configuring IVS Setup

You can configure radar structuring, fusion, OSD and map location.



OSD function and text overlay function cannot be enabled at the same time.

Step 1 Select Setting > Radar Settings > IVS Setup.

Figure 5-2 IVS setup

IVS Setup

Radar Structuring: Off

Fusion: Off

ivs.DetectSensitivity: Human [Slider] Vehicle 0

OSD

☒ Enable

Map Location: [Grid of 8 locations: Location1, Location2, Location3, Location4, Location5, Location6, Location7, Location8]

Default Refresh Save

Step 2 Configure parameters.

Table 5-3 IVS setup parameter description

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

Step 3 Click **Save**.

5.3 Configuring Device Attitude

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

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

Procedures

Step 1 Select Setting > Radar Settings > Device Attitude.

Figure 5-3 Device attitude

DeviceAttitude

☒ Enable

Pitch Angle -1.61363685131073 °

Roll Angle 1.390569090843201 °

Yaw Angle 0 °

Pitch angle: The included angle between carrier and horizontal plane. Pitch angle is positive during moving upwards, and negative when moving downwards.

Roll angle: The included angle between carrier and horizontal plane. Roll angle is positive during clockwise rotation, and negative during anticlockwise rotation.

Yaw angle: The included angle between carrier and X-axis. Yaw angle is positive when turning right, and negative when turning left. X-axis represents the forward direction.

Default Refresh Save

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

Step 3 Click **Save**.

5.4 Configuring Linkage

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

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

5.4.1 Auto Calibration

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

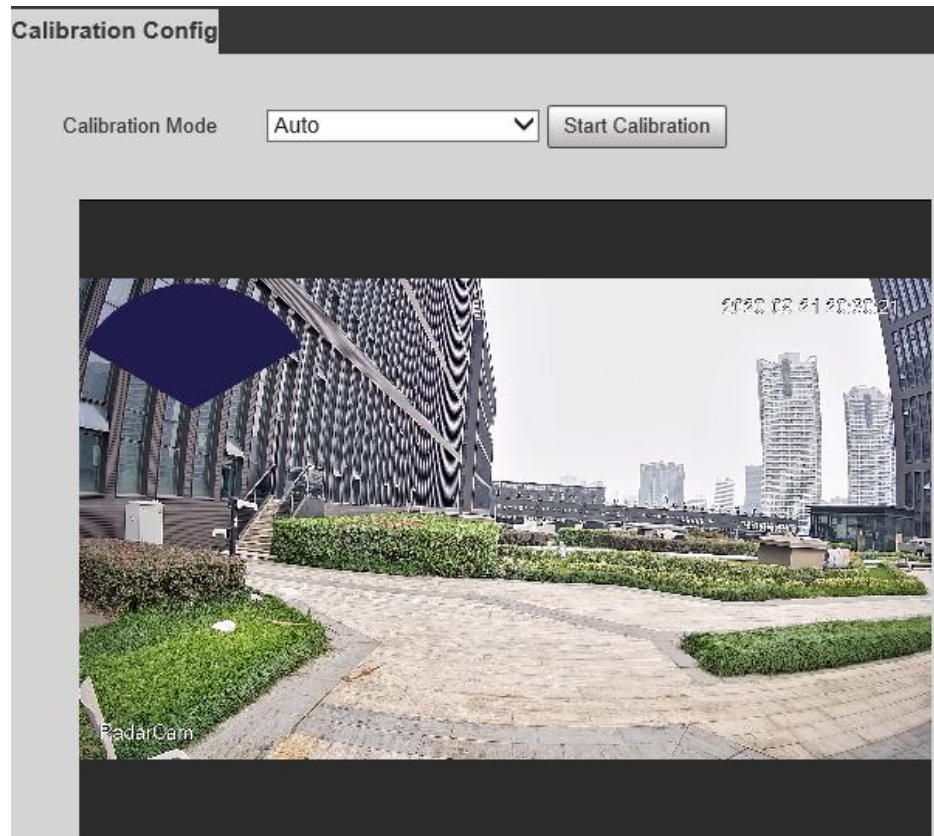
Step 2 In the pull-down list, select **Auto**. See Figure 5-4.

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



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

Figure 5-4 Auto calibration



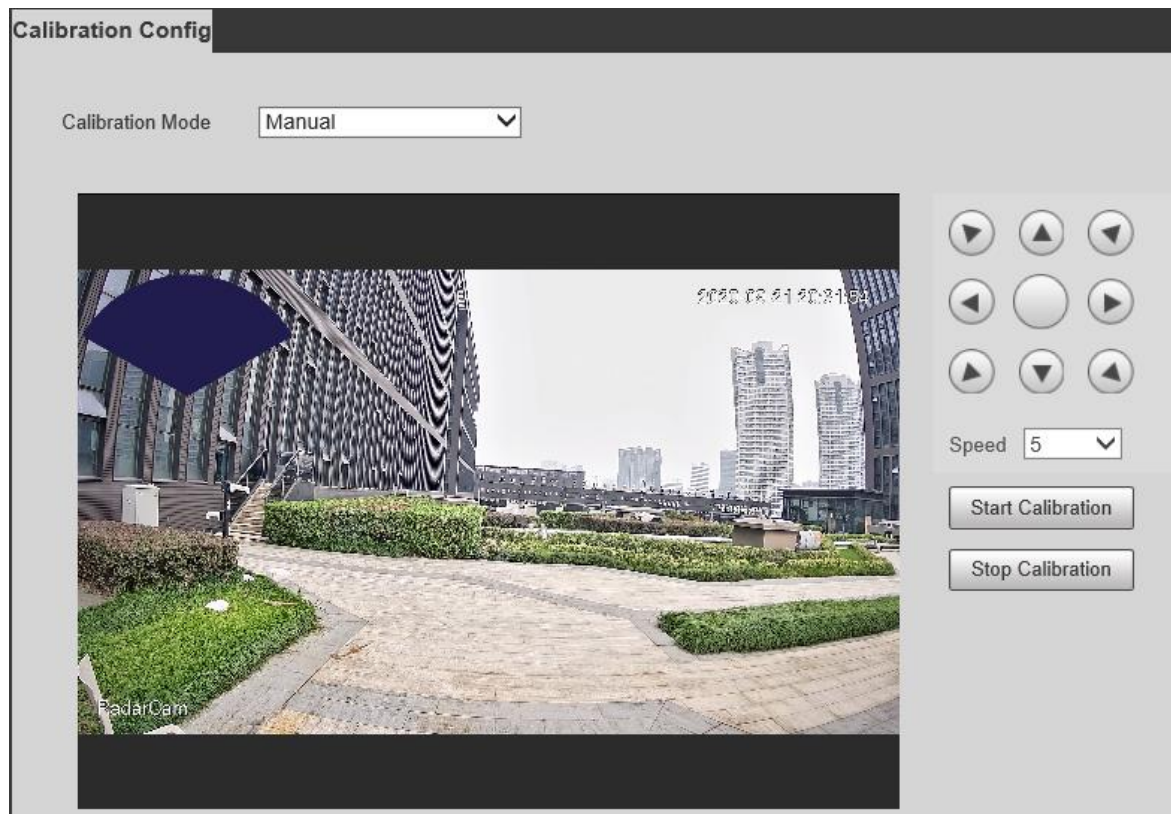
5.4.2 Manual Calibration

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



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

Figure 5-5 Manual calibration



Step 4 Click Stop Calibration.

6 Setting

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

6.1 Network

6.1.1 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.



- 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.

Step 1 Select Setting > Network > TCP/IP.

The **TCP/IP** interface is displayed. See Figure 6-1.

Figure 6-1 TCP/IP

Step 2 Configure parameters. See Table 6-1.

Table 6-1 TCP/IP parameter descriptions

Parameter	Description
Host Name	Enter host name, 15 characters at most.

Parameter	Description
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.
Subnet Mask	
Default Gateway	
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**.

6.1.2 Port

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

Step 1 Select Setting > Network > Port.

The **Port** interface is displayed. See Figure 6-2.

Figure 6-2 Port

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. See Table 6-2.



- 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 6-2 Port parameter description

Parameter	Description
Max Connection	The maximum number of users that can log in to the web interface 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: rtsp://username:password@ip:port/cam/realmonitor?channel=1&subtype=0 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: rtsp://admin:admin@10.12.4.84:554/cam/realmonitor?channel=2&subtype=1 If user name and password are not needed, then the URL can be: rtsp://ip:port/cam/realmonitor?channel=1&subtype=0
HTTPs Port	HTTPs communication port, the default value is 443, and it can be modified as needed.

Step 3 Click **Save**.

6.1.3 SMTP (Email)

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

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

The **SMTP (Email)** interface is displayed. See Figure 6-3.

Figure 6-3 SMTP (Email)

Step 2 Configure parameters. See Table 6-3.

Table 6-3 SMTP (Email) parameter descriptions

Parameter	Description	
SMTP Server	IP address of SMTP server that sends emails.	 For the detailed configuration, see Table 6-4.
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 Table 6-4.	
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.	
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, see Table 6-4.

Table 6-4 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**.

6.2 System

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

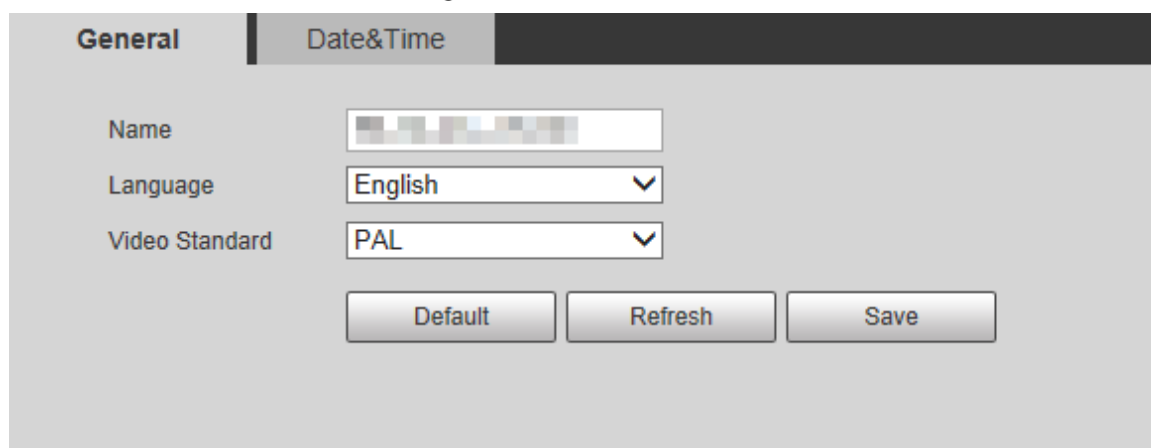
6.2.1 General

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

6.2.1.1 General

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

Figure 6-4 General

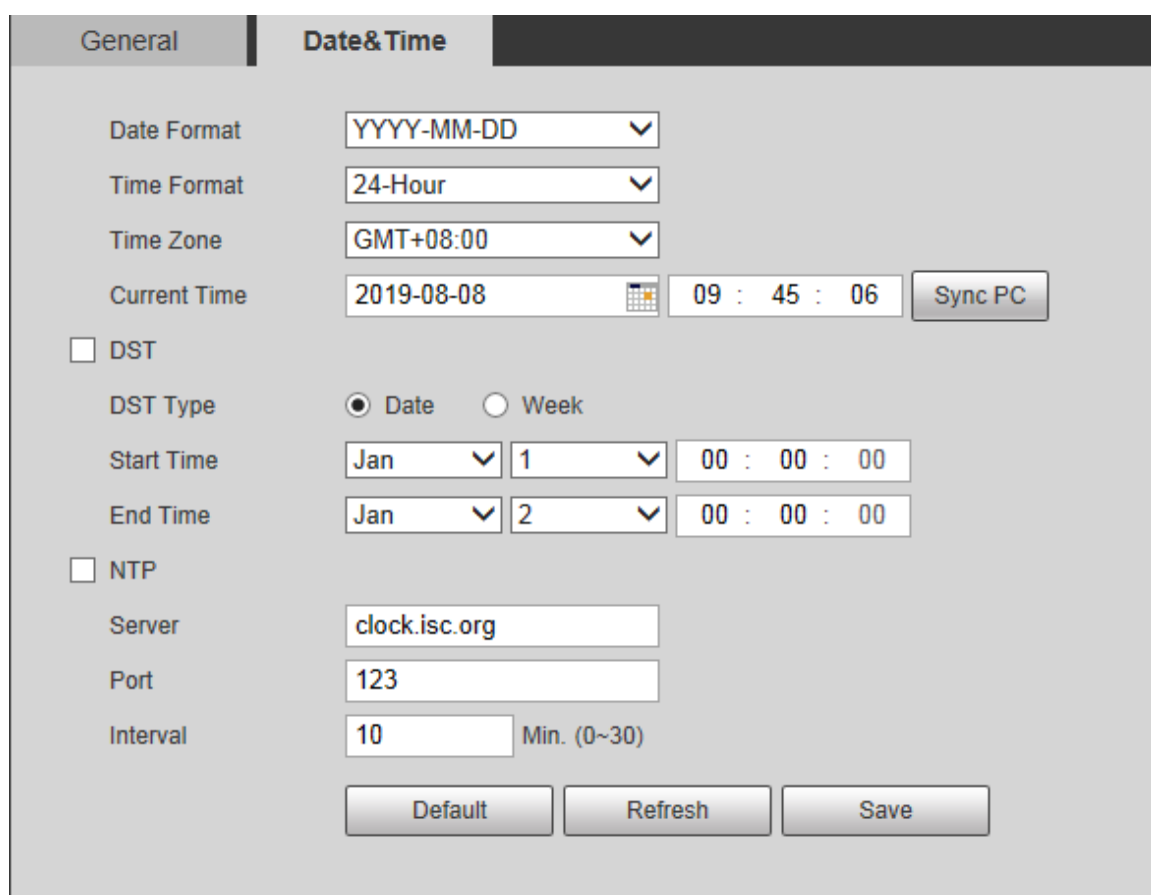


The 'General' configuration window shows the 'Date&Time' tab. It includes fields for 'Name' (a blurred text box), 'Language' (set to 'English'), and 'Video Standard' (set to 'PAL'). At the bottom are three buttons: 'Default', 'Refresh', and 'Save'.

6.2.1.2 Date & Time

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

Figure 6-5 Date & Time



The 'Date & Time' configuration window shows the 'Date&Time' tab. It includes the following settings:

- Date Format:** YYYY-MM-DD
- Time Format:** 24-Hour
- Time Zone:** GMT+08:00
- Current Time:** 2019-08-08, 09 : 45 : 06, with a 'Sync PC' button.
- DST:** ☐ DST
 - DST Type:** ☒ Date ☐ Week
 - Start Time:** Jan, 1, 00 : 00 : 00
 - End Time:** Jan, 2, 00 : 00 : 00
- NTP:** ☐ NTP
 - Server:** clock.isc.org
 - Port:** 123
 - Interval:** 10 Min. (0~30)

At the bottom are three buttons: 'Default', 'Refresh', and 'Save'.

6.2.2 Account

6.2.2.1 User

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

Figure 6-1 Username

Account | Onvif User

☐ 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.

Step 1 Click Add User.

The **Add User** interface is displayed. See Figure 6-2.

Figure 6-2 Add user

Step 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.

Step 3 (Optional) Click **Restricted Login** to set IP address, validity period, and time range of the added user. See Figure 6-3.

Figure 6-3 Restricted login

The screenshot shows the 'Add User' dialog box with the 'Restricted Login' tab selected. The 'Operation Permission' tab is also visible. The 'Restricted Login' section contains the following fields and options:

- ☐ IP Address: IPv4 (selected), IP Address (dropdown), 1 . 0 . 0 . 1
- ☐ Validity Period: Begin Time (2019-08-22, 08 : 00 : 00), End Time (2019-08-23, 08 : 00 : 00)
- ☐ Time Range: A grid showing days of the week (Sun to Sat) and hours (0 to 24). The grid is currently empty, and each row has a 'Setting' button.

At the bottom of the dialog are 'Save' and 'Cancel' buttons.

Step 4 Click **Save**.

Modifying a User

Step 1 Click  of the selected user.

The **Modify User** interface is displayed. See Figure 6-4.

Figure 6-4 Modify user

Modify User

Username: admin

☐ Modify Password

Email Address:

Group Name: admin

Memo: admin 's account

Authority: ☒ All

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

Save Cancel

Step 2 Modify user information as needed.

Step 3 Click **Save**.

Modifying the Password

Step 1 Click  of the selected user.

The **Modify User** interface is displayed.

Step 2 Select **Modify Password** check box.

Step 3 Enter the old password, new password, and then confirm the password.

Step 4 Click **Save**.

Deleting a User

Click  to delete the added user.

6.2.2.2 Group

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

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

The **Group Name** interface is displayed. See Figure 6-5.

Figure 6-5 Group name

The screenshot shows the 'Account' management interface with the 'Onvif User' tab selected. There is an 'Anonymous Login' checkbox. Below it is a table with columns: No., Group Name, Memo, Modify, and Delete. The table contains three rows: 'admin' (administrator group), 'user' (user group), and 'test' (add by VulScan). Below the table is a grid of system functions categorized under 'Authority'. At the bottom is an 'Add Group' button.

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	

Adding a Group

Modifying a Group

Deleting a Group

6.2.3 Manager

6.2.3.1 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.

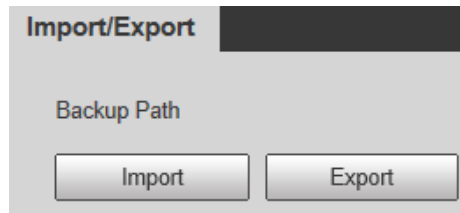
Figure 6-6 Auto Maintain

The screenshot shows the 'Auto Maintain' configuration interface. It has two checkboxes: 'Auto Reboot' (checked) and 'Auto Delete Old Files' (unchecked). The 'Auto Reboot' checkbox is followed by a dropdown menu showing 'Sat' and a time field showing '03 : 30'. Below these are three buttons: 'Manual Reboot', 'Refresh', and 'Save'.

6.2.3.2 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 6-7 Import/Export

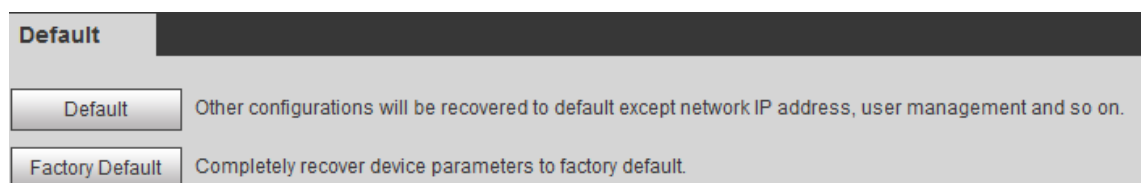


- Click **Export** to export the configuration file (.backup file) to local.
- Click **Import** to import the configuration file into the system.

6.2.3.3 Default

Restore the radar to default configurations or factory settings.

Figure 6-8 Default



- Click **Default**, and then all the configurations except IP address and account management will be restored to default.
- Click **Factory Default**, and all the configurations will be restored to factory settings.

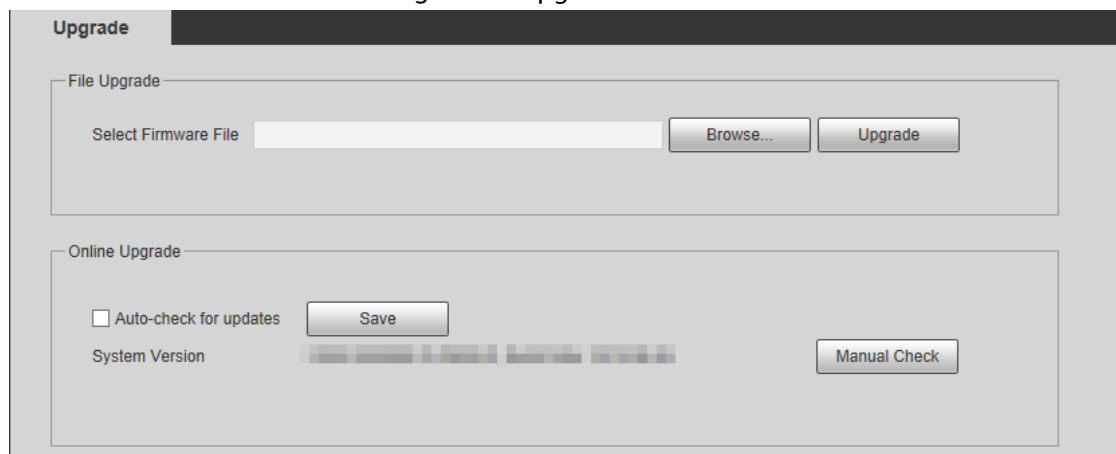
6.2.4 Upgrade

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 6-9 Upgrade



6.3 Alarm

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

Click **Alarm** tab, and then the **Alarm** interface is displayed. See Figure 6-10. For more parameter descriptions, see Table 6-5.

Figure 6-10 Alarm

The screenshot shows the 'Alarm' interface. On the left, there are configuration sections: 'Alarm Type' with checkboxes for Disk Full, Disk Error, External Alarm, Illegal Access, Security Exception, and Radar Alarm; 'Operation' with a checkbox for Prompt; 'Alarm Tone' with a checkbox for Play Alarm Tone; and a 'Tone Path' field with a 'Browse...' button. On the right, there is a large table with columns: No., Time, Alarm Type, Source IP, and Alarm Channel. The table is currently empty.

Table 6-5 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 interface,  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 interface, 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.
	Tone Path	Select Browse... to choose alarm audio file.

