



Visual Radar

Quick Start Guide



Foreword

General




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

Model

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

Safety Instructions

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

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

Revision History

Version	Revision content	Release Time
V1.0.1	Modified models.	October 2020
V1.0.0	First release.	August 2020

About the Manual

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

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

Important Safeguards and Warnings

The following contents are about the proper ways of using the Radar, preventing dangers and property damage when it is in use. Read the manual carefully before using the Radar, strictly abide by the manual and properly keep it for future reference.

Environmental Requirements

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

Electrical Safety

- All installation and operation should conform to your local electrical safety codes.
- Make sure that the power supply is correct before operating the Radar.
- The power source shall conform to the requirement of the Safety Extra Low Voltage (SELV) standard, and supply power with rated voltage which conforms to Limited power Source requirement according to IEC60950-1. Please note that the power supply requirement is subject to the device label.
- A readily accessible disconnect device shall be installed for emergency power off.
- Prevent the power cable from being trampled or pressed, especially wires around the holes where the plug, power socket, and the junction are threaded through.

Operation and Daily Maintenance

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



- Use accessories suggested by the manufacturer, and install and maintain the Radar by professional personnel.
- Do not use two or more than two kinds of power supply modes to provide power for the Radar at the same time; otherwise, the device might be damaged.

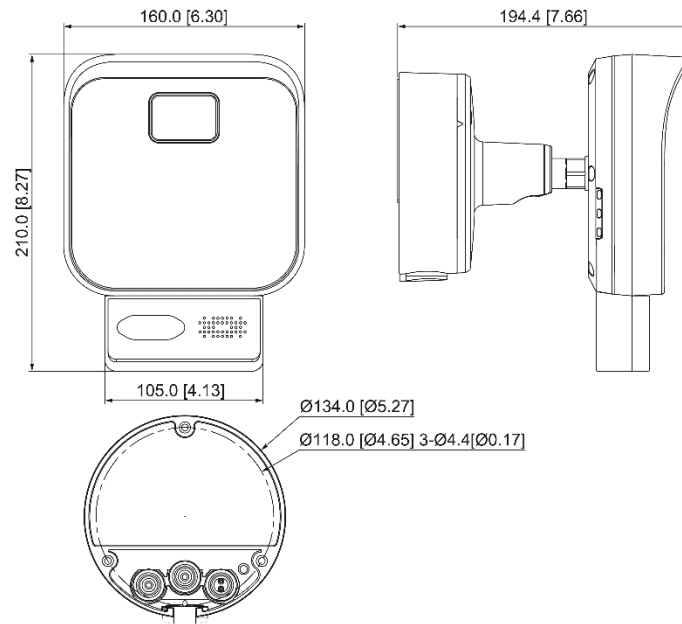
Table of Contents

Foreword.....	I
Important Safeguards and Warnings.....	III
1 Introduction.....	1
1.1 Dimensions.....	1
1.2 Appearance.....	1
1.2.1 Indicator Light.....	1
1.2.2 Reset Button and Memory Card.....	2
1.3 Ports.....	3
1.4 Alarm Settings.....	4
2 Installation.....	5
2.1 Installation Preparations	5
2.1.1 Environmental Requirements	5
2.1.2 Installation Tools and Cables	5
2.2 Detection Range.....	5
2.3 Unpacking the Box.....	7
2.4 Installation	8
2.4.1 Installing Methods.....	8
2.4.2 Installation Procedures	8
2.5 Verification after the Installation	13
3 Network Configuration	14
3.1 Device Initialization	14
3.2 Logging in to the Web Client.....	17
3.3 Changing IP Address.....	18
4 Quick Operation	20
4.1 Configuring Calibration	20
4.1.1 Auto Calibration	20
4.1.2 Manual Calibration	20
4.2 Adjusting Radar Direction	21
Appendix 1 FAQ.....	23
Appendix 2 Cybersecurity Recommendations.....	24

1 Introduction

1.1 Dimensions

Figure 1-1 Radar dimensions (mm [inch])



1.2 Appearance

1.2.1 Indicator Light

Figure 1-2 Indicator light

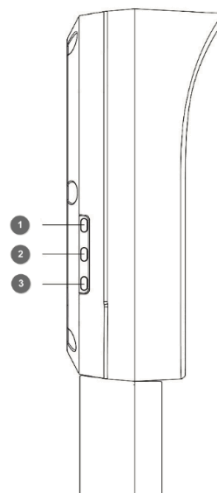


Table 1-1 Indicator light description

No.	Name	Description
1	Status indicator light	<ul style="list-style-type: none"> • Solid green: Radar is running normally. • Flashing red: Alarm events occur in the detection range of Radar.
2	Power indicator light	<ul style="list-style-type: none"> • Solid green: Radar is running normally. • Flashing green: Radar is upgrading.
3	Network indicator light	<ul style="list-style-type: none"> • Solid yellow: Network is connected. • Off: Network is not connected.

1.2.2 Reset Button and Memory Card

Open the rear cover of the Radar with a screwdriver. The reset button and memory card slot are displayed.

Figure 1-3 Reset button and memory card

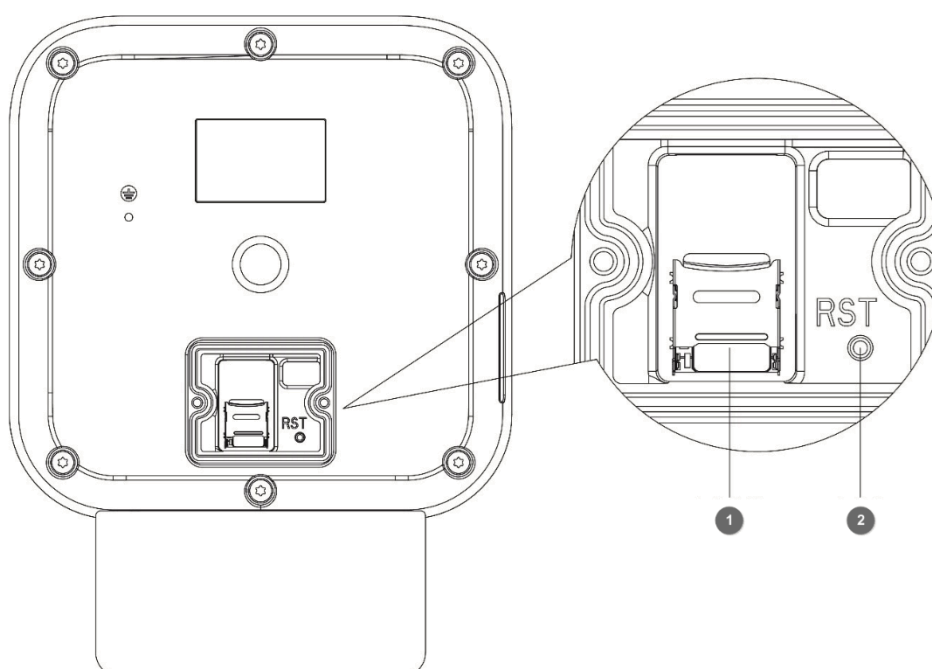


Table 1-2 Reset button and memory card

No.	Name	No.	Name
1	Memory card slot	2	Reset button

1.2.2.1 Using the Reset Button

You can use the reset button to restore the Radar to factory default settings.

When the Radar is running normally, open the rear cover of the Radar. Then press and hold the reset button for over 15 s, and the Radar will be restored.

1.2.2.2 Installing Memory Card

You can insert a memory card to store recordings and images. Face the memory card with metal contacts downwards, and insert the card into the card slot.



The memory card cannot be removed when the Radar is reading or writing data; otherwise files might be lost and the memory card might be damaged.

1.3 Ports

Figure 1-4 Ports

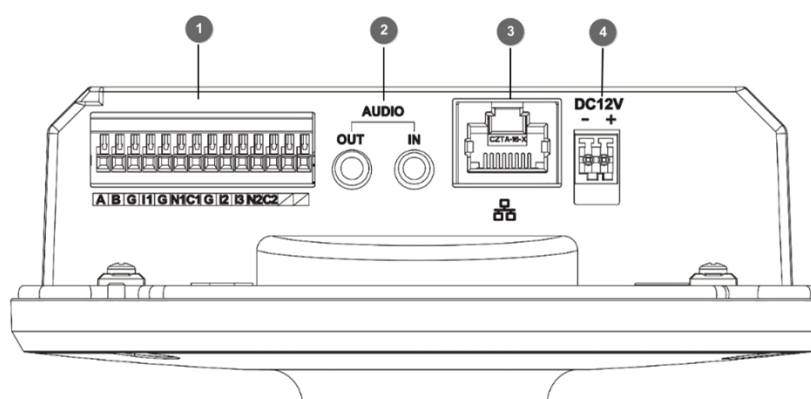



Table 1-3 Port description

No.	Name	Description
1	A	Connects to RS-485_A, controls external devices.
	B	Connects to RS-485_B, controls external devices.
	G	Ground connection end of alarm input port I1, I2, I3.
	I1	External alarm input port. The default level is high. If the level is low, alarm will be triggered.
	I2	
	I3	
	N1	<ul style="list-style-type: none"> N1/N2: Alarm output port 1. C1/C2: Alarm output port 2.  <p>You can only connect N1 to C1 and N2 to C2. Short circuit will occur between N and C ports when alarm is triggered; otherwise, N and C ports connection will keep open-circuited.</p>
	N2	
	C1	
	C2	
2	Audio output	Outputs audio signal to external devices such as speaker.
	Audio input	Inputs audio signal. Receives analog audio signal from devices such as pickup.

No.	Name	Description
3	Network	Connects to standard Ethernet cable. Supports PoE power supply.
4	Power input	12V DC power input.

1.4 Alarm Settings

This function is available on select models.

Step 1 Connect to alarm input device.

By following the instructions below, the device can collect different statuses of the alarm input port.

- Device collects logic "1" when input signal is connecting to +3V to +5V or idling.
- Device collects logic "0" when input signal being connected to the ground.

Figure 1-5 Alarm input

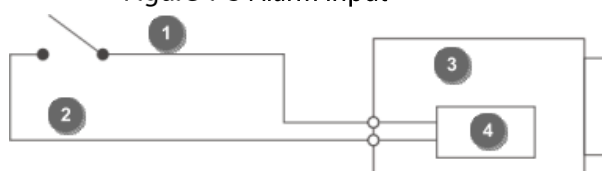


Table 1-4 Alarm input

No.	Name	No.	Name
1	Alarm input	2	Ground wire
3	Network camera	4	Collecting

Step 2 Connect to alarm output device.

The alarm output is relay switch output, which can only connect to NO alarm devices.

The N port and the C port with the same number constitute a switch for alarm output. See Figure 1-6. The switch is open normally and closes when there is alarm output.

Figure 1-6 Alarm output

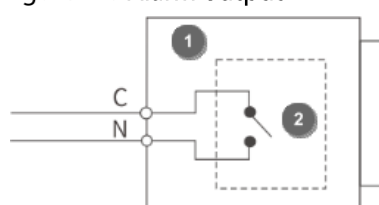


Table 1-5 Alarm output

No.	Name	No.	Name
1	Network camera	2	Alarm output

Step 3 Log in to the web client, and configure the alarm input and output in **Setting > Event > Alarm**.

- Alarm input on the web client is corresponding to the alarm input end of I/O port. Please set the input mode to "NO" (default) if the alarm input signal is logic "0" and to "NC" if the alarm input signal is logic "1".
- The alarm output on the web client is corresponding to the alarm output end of I/O port.

2 Installation

2.1 Installation Preparations

2.1.1 Environmental Requirements

- The installation site has enough space to install the Radar and its mounting components.
- The wall and pole for installation can sustain eight times the weight of the Radar and its mounting components.
- 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 the Radar during installation. Because radar electromagnetic wave cannot penetrate objects such as buildings, rocks, and glasses, a blind zone might 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 installation location or within its detection range, such as outdoor air conditioners and wind-driven generators.
- Make sure that the Radar is installed securely and stably. Swaying will reduce its detection precision, or cause misinformation which influences the normal usage of radar.

2.1.2 Installation Tools and Cables

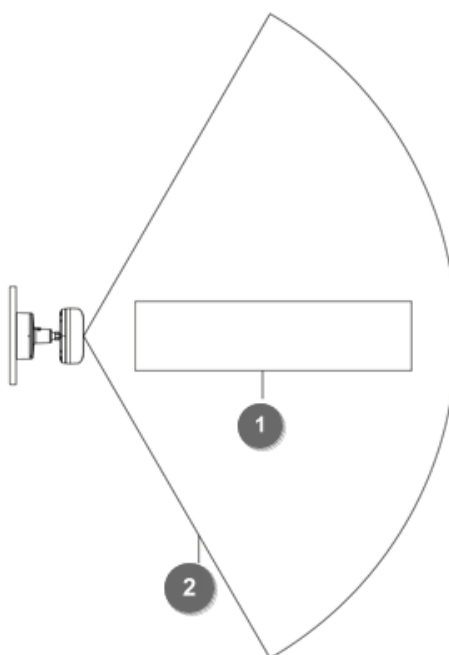
Except for the accessories provided, you need to prepare the following tools and cables before installation: Power cord, lightning protector, distribution box, air switch, PoE switch (optional), electric screwdriver, network cable, ladder, insulating gloves, and other things as needed.

2.2 Detection Range

Horizontal Direction

Make sure that the front side of the Radar faces the central part of the detection area.

Figure 2-1 Horizontal direction



In Figure 2-1, number 1 represents detection area and number 2 represents horizontal detection angle.

Detection Range

Due to the microwave feature, the detection distance of margins is shorter than the central detection distance. See Figure 2-1.

Blind Zone for Short Distance

The height of central point of the equivalent reflection interface of detected objects such as human and vehicle is above 1 m. Radar's maximum distance of blind zone is shown in Figure 2-2. For other maximum blind zone distance with typical parameters, see Table 2-2.

Figure 2-2 Max blind zone distance

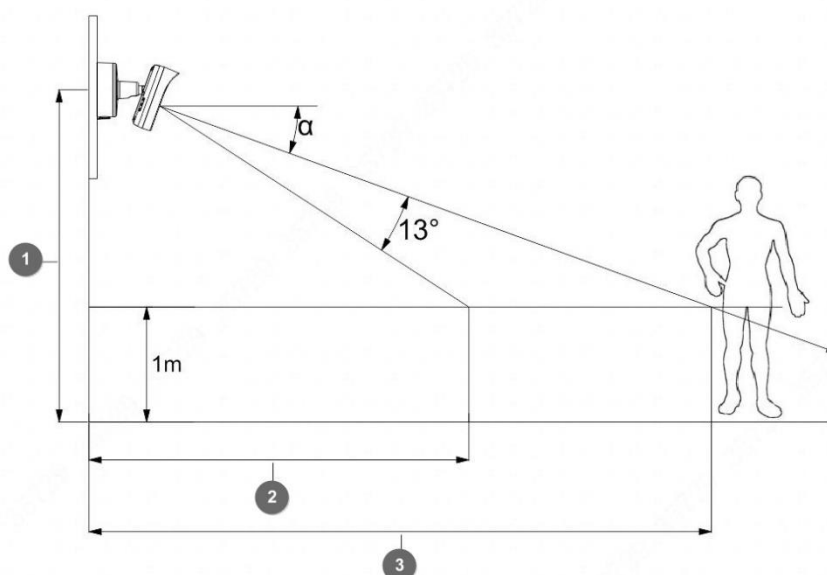


Table 2-1 Max blind zone distance

No.	Name	No.	Name
1	Installation height	2	Blind zone
3	Max. detection range	—	—

Table 2-2 Max blind zone parameters (60 m radar)

Installation height (h)	Pitch Angle (α)	Blind Zone	Max Detection Range
2.0 m (6.56 ft)	0–3°	3.0 m (9.87 ft)	60.0 m (196.85 ft)
3.0 m (9.84 ft)	0–3°	5.0 m (16.40 ft)	60.0 m (196.85 ft)
4.0 m (13.12 ft)	0–3°	8.5 m (27.89 ft)	60.0 m (196.85 ft)

2.3 Unpacking the Box

After unpacking the box, check if there is obvious damage to the appearance of the Radar, and make sure that the components are complete against the packing list.

Table 2-3 Packing list

Item	Quantity
Visual radar	1
Waterproof silicon plug	3
Wrench	1
Cable puller	1
Screw pack	3 screws in one pack
Quick start guide	1
Positioning map	1
QR code label	1

2.4 Installation

2.4.1 Installing Methods

Figure 2-3 Wall mount

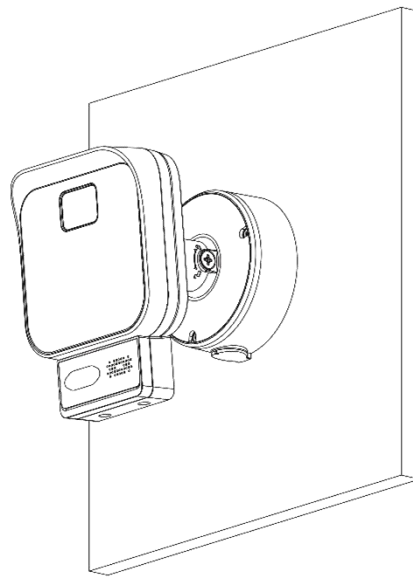
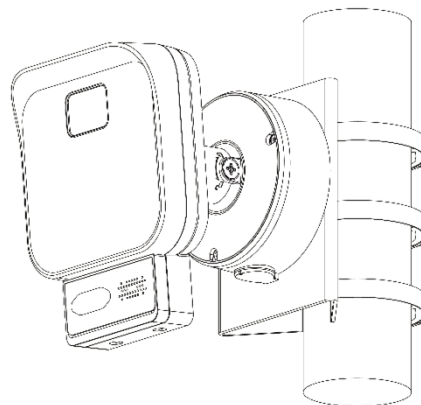


Figure 2-4 Pole mount

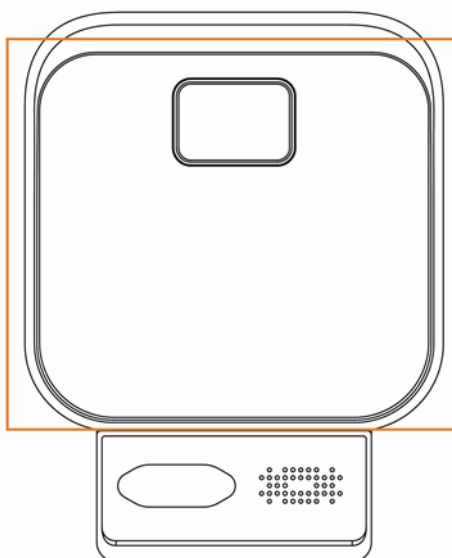


2.4.2 Installation Procedures



The Radar panel is easy to be scratched, please install carefully.
Remove the film after installation.

Figure 2-5 Radar panel



This section takes wall mounting as an example.

Figure 2-6 Unscrew the screws

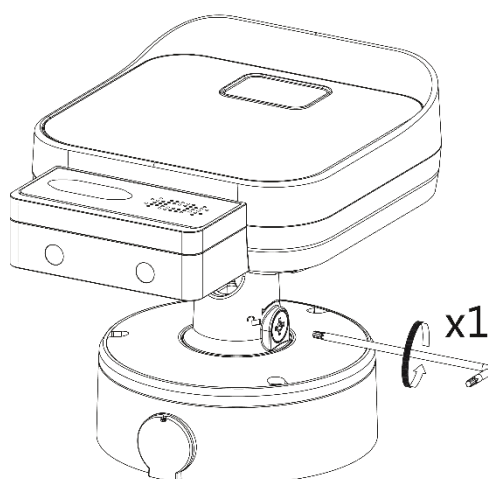


Figure 2-7 Unscrew and remove the junction box

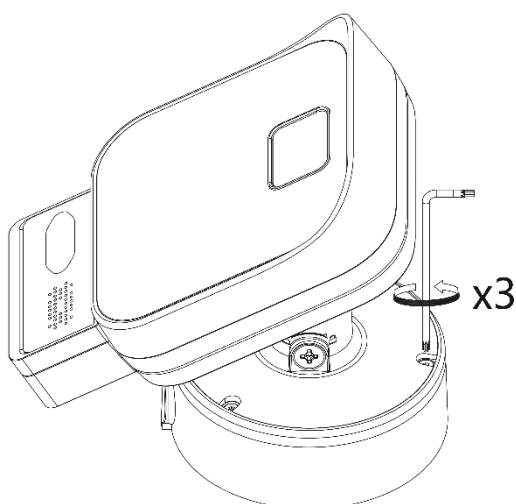
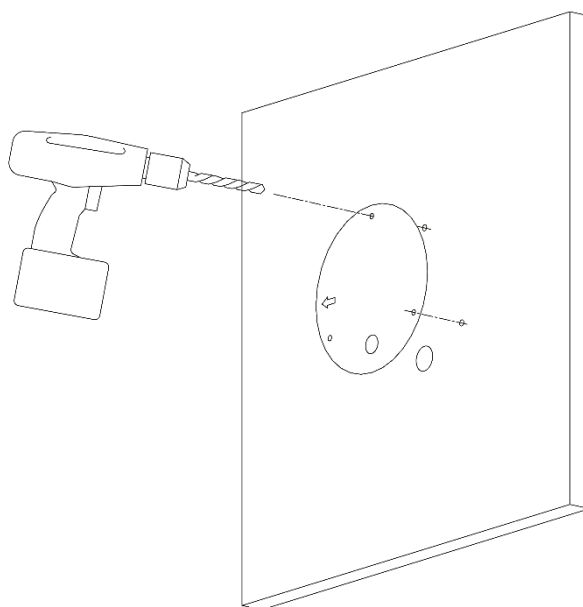


Figure 2-8 Stick the positioning map and drill three screw holes



The arrow direction in the positioning map always points to the left.

Figure 2-9 Install wall anchor and pull the cables out of the cable holes

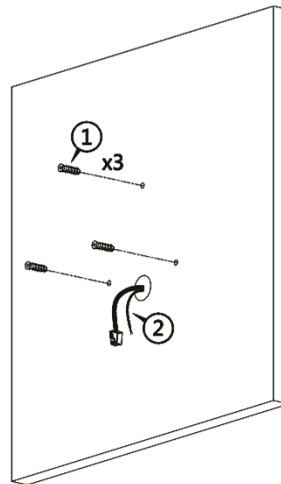


Figure 2-10 Thread the waterproof silicon plugs through the cables

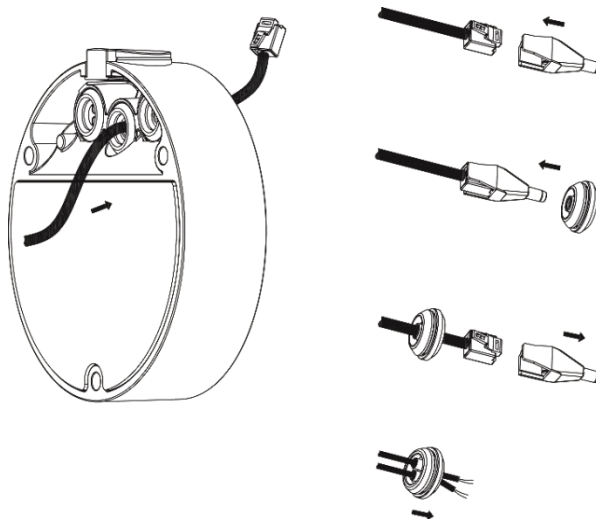


Figure 2-11 Install the junction box

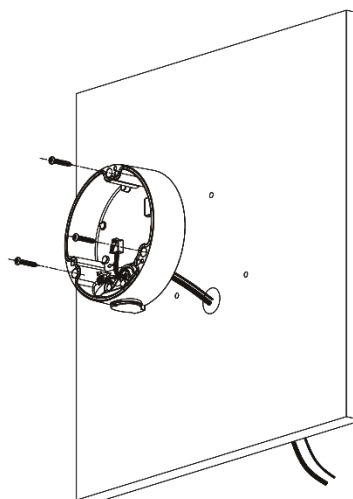
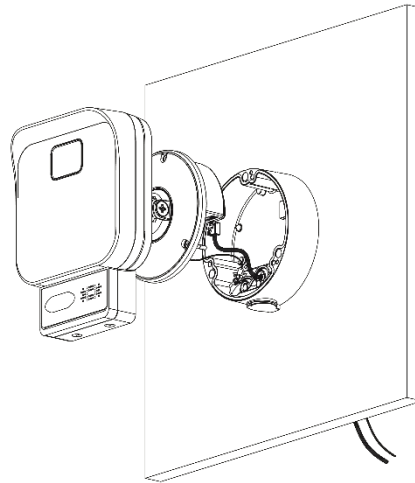


Figure 2-12 Install the cables



While installing the device, use safety rope to avoid dropping.

Figure 2-13 Mount the screws

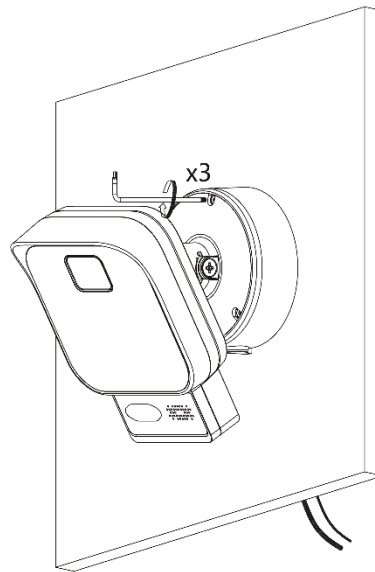
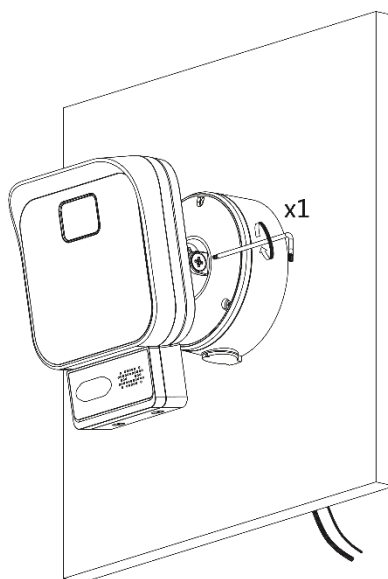


Figure 2-14 Adjust the detection angle and tighten the screws



When adjusting the detection angle of the Radar, you can check the angle by enabling the device attitude on the web client. It is suggested that the angle of the device should be -3° , and the equipment should face the middle of the area to be monitored. See "4.2 Adjusting Radar Direction" for details.

2.5 Verification after the Installation

After the installation and all the wires are connected, verify if the Radar can work normally. Follow the standards below:

- Power indicator light is on solid green after the Radar is powered.
- Status indicator light is on solid green after the Radar starts.
- Network indicator light is on solid yellow after network is connected.

3 Network Configuration

Prerequisites

- 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.

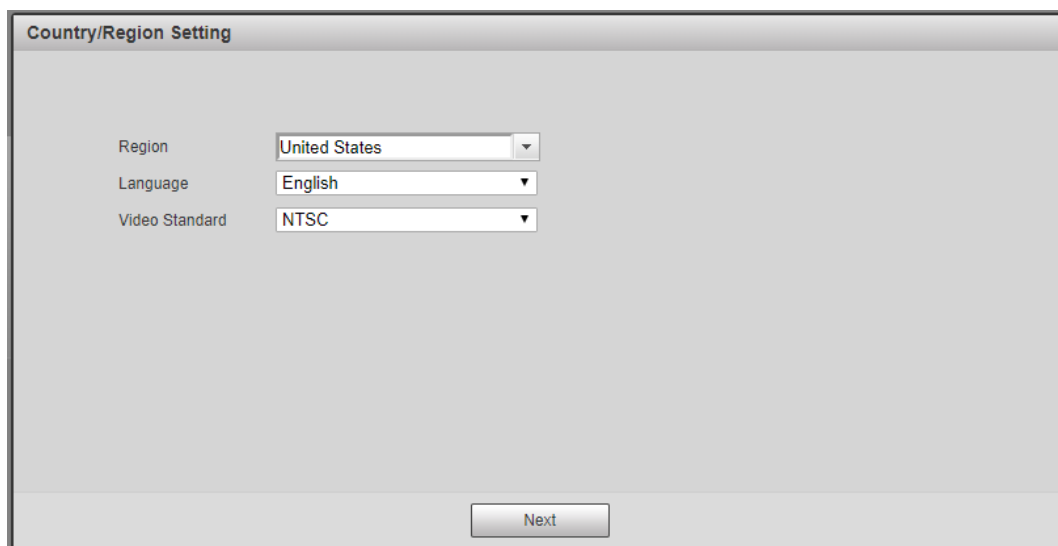
3.1 Device Initialization

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

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

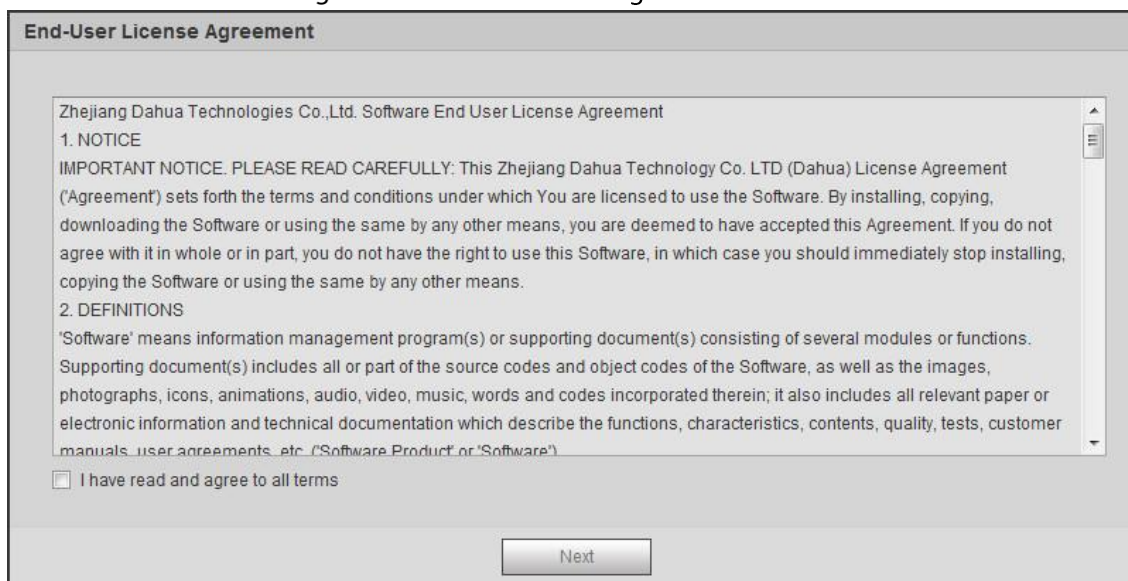
Step 2 Select your region, language and video standard, and click **Next**.

Figure 3-1 Country/Region setting

A screenshot of a web-based configuration window titled "Country/Region Setting". The window has a light gray background. On the left side, there are three labels: "Region", "Language", and "Video Standard". To the right of each label is a dropdown menu. The "Region" dropdown is set to "United States", the "Language" dropdown is set to "English", and the "Video Standard" dropdown is set to "NTSC". At the bottom center of the window, there is a button labeled "Next".

Step 3 Select I have read and agree to all terms, and then click **Next**.

Figure 3-2 End-user license agreement



End-User License Agreement

Zhejiang Dahua Technologies Co.,Ltd. Software End User License Agreement

1. NOTICE

IMPORTANT NOTICE. PLEASE READ CAREFULLY: This Zhejiang Dahua Technology Co. LTD (Dahua) License Agreement ('Agreement') sets forth the terms and conditions under which You are licensed to use the Software. By installing, copying, downloading the Software or using the same by any other means, you are deemed to have accepted this Agreement. If you do not agree with it in whole or in part, you do not have the right to use this Software, in which case you should immediately stop installing, copying the Software or using the same by any other means.

2. DEFINITIONS

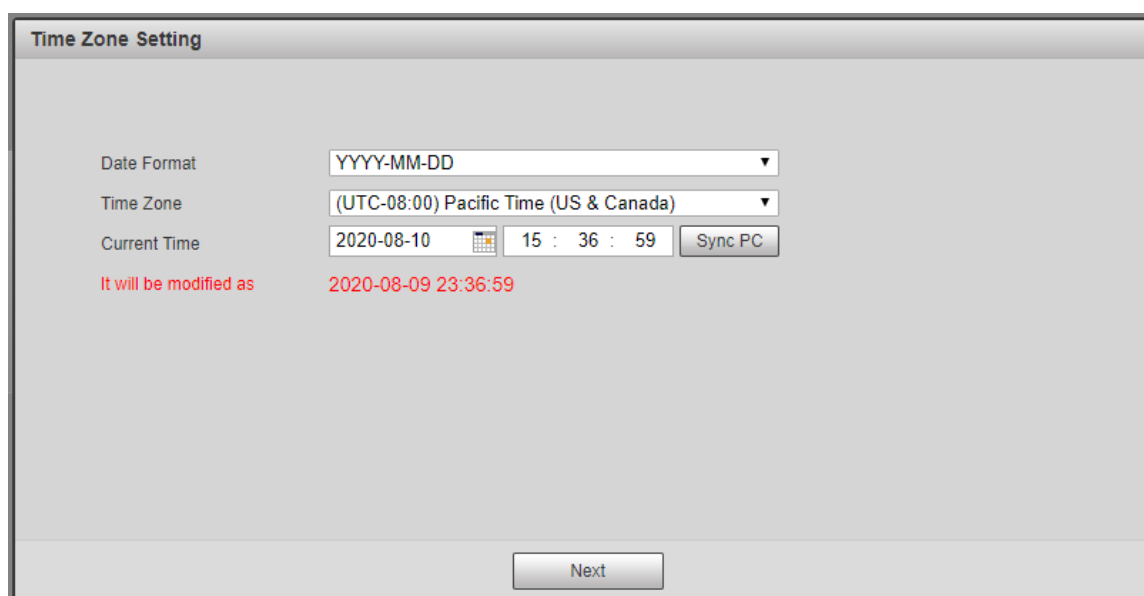
'Software' means information management program(s) or supporting document(s) consisting of several modules or functions. Supporting document(s) includes all or part of the source codes and object codes of the Software, as well as the images, photographs, icons, animations, audio, video, music, words and codes incorporated therein; it also includes all relevant paper or electronic information and technical documentation which describe the functions, characteristics, contents, quality, tests, customer manuals, user agreements, etc. ('Software Product' or 'Software').

☐ I have read and agree to all terms

Next

Step 4 Configure the time zone, and click **Next**.

Figure 3-3 Time zone setting



Time Zone Setting

Date Format: YYYY-MM-DD

Time Zone: (UTC-08:00) Pacific Time (US & Canada)

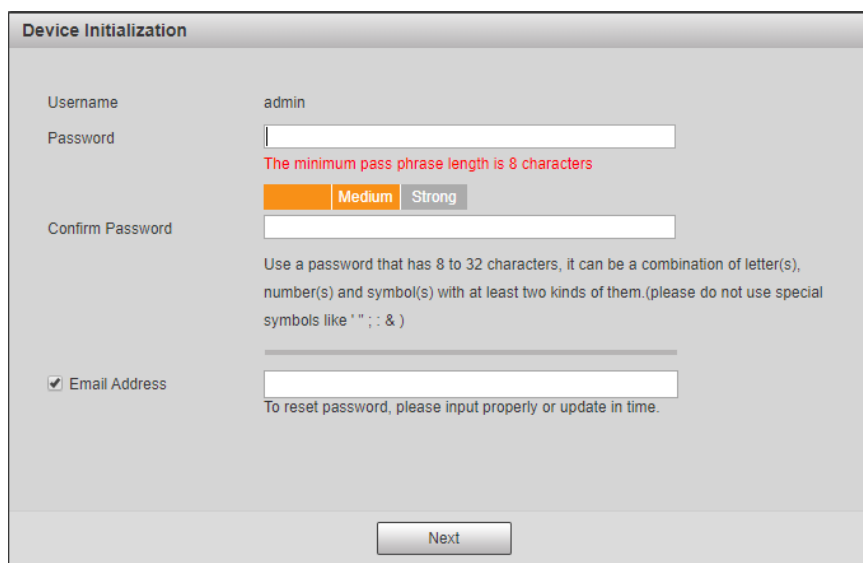
Current Time: 2020-08-10 15 : 36 : 59 Sync PC

It will be modified as 2020-08-09 23:36:59

Next

Step 5 Set the password according to the prompt, and click **Next**.

Figure 3-4 Set admin password



Device Initialization

Username: admin

Password:

The minimum pass phrase length is 8 characters

Medium Strong

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.

Next



The email address is for password reset. We recommend entering the email address to guarantee normal use of the Radar.

Step 6 Select **P2P** in the P2P interface as needed, and click **Next**.

Figure 3-5 P2P



P2P

☒ P2P

To assist you in remotely managing your device, the P2P will be enabled. After enabling P2P and connecting to Internet, we need to collect IP address, MAC address, device name, device SN, etc. All collected info is used only for the purpose of remote access. If you don't agree to enable P2P function, please deselect the check box.

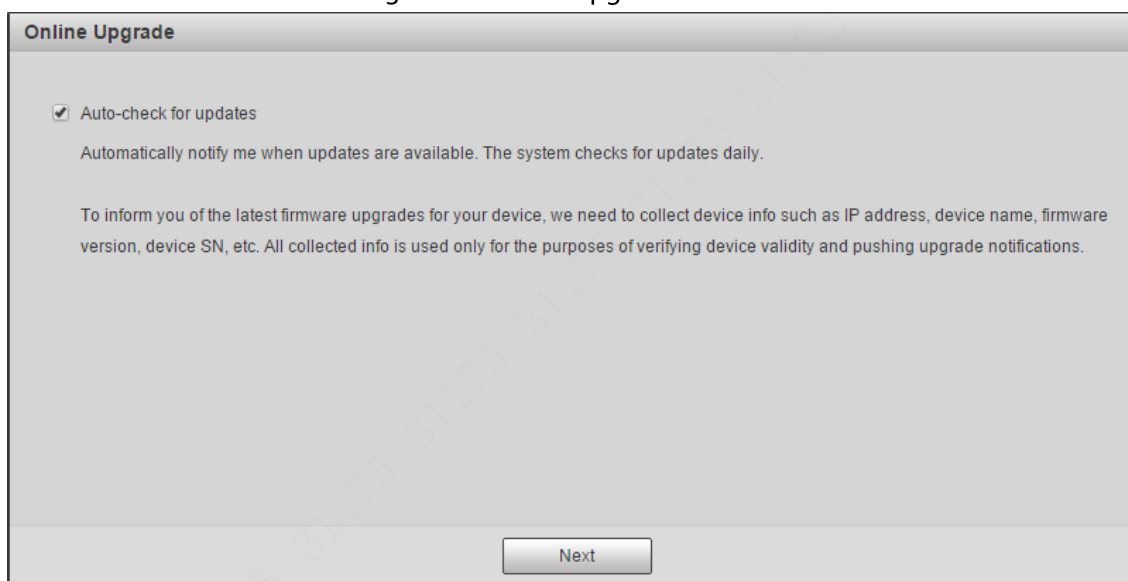
Please scan the QR code on the actual interface

Scan and Download APP

Next

Step 7 Select **Auto-check for updates** as needed, and then click **Save** to complete initialization.

Figure 3-6 Online upgrade

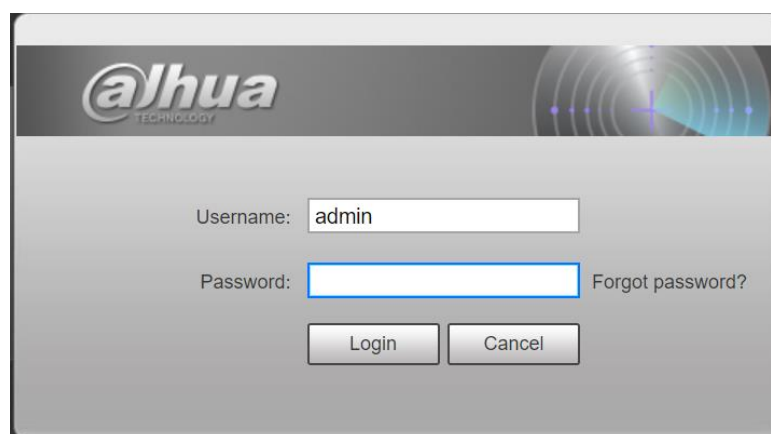


3.2 Logging in to the Web Client

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

Step 1 On the web interface, enter username and password, and then click **Login**.

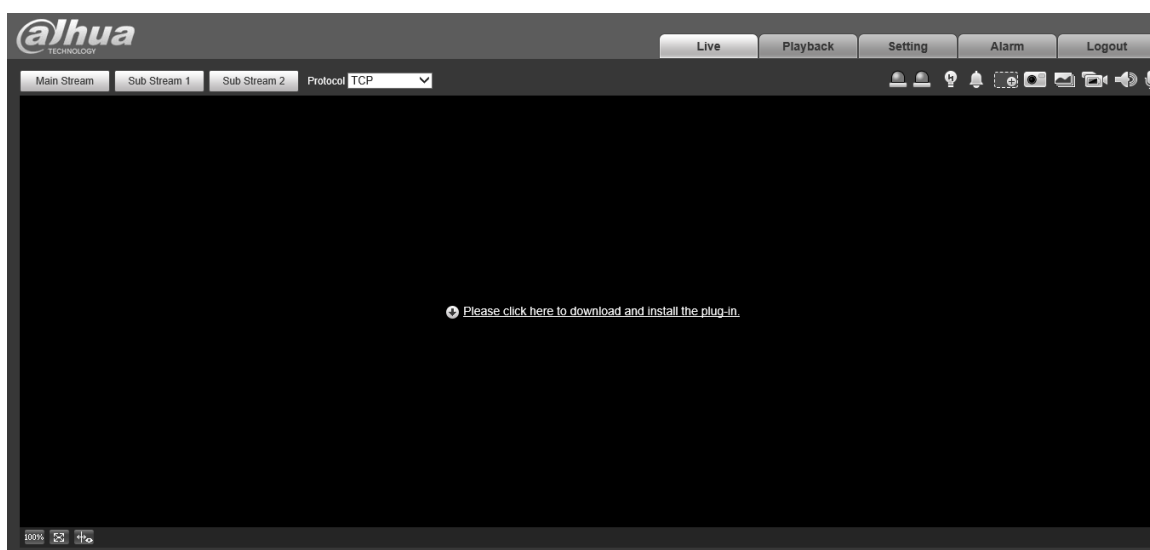
Figure 3-7 Login interface




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

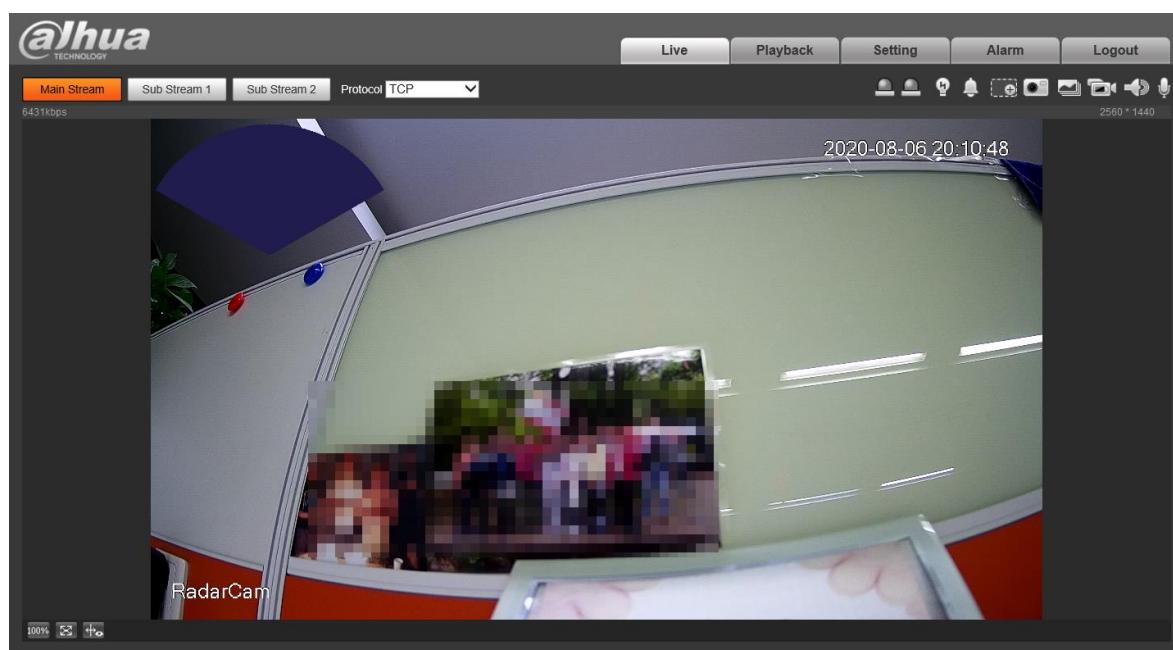
Step 2 Download and install the plug-in according to the on-screen instructions.

Figure 3-8 Install the plug-in



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

Figure 3-9 Live view



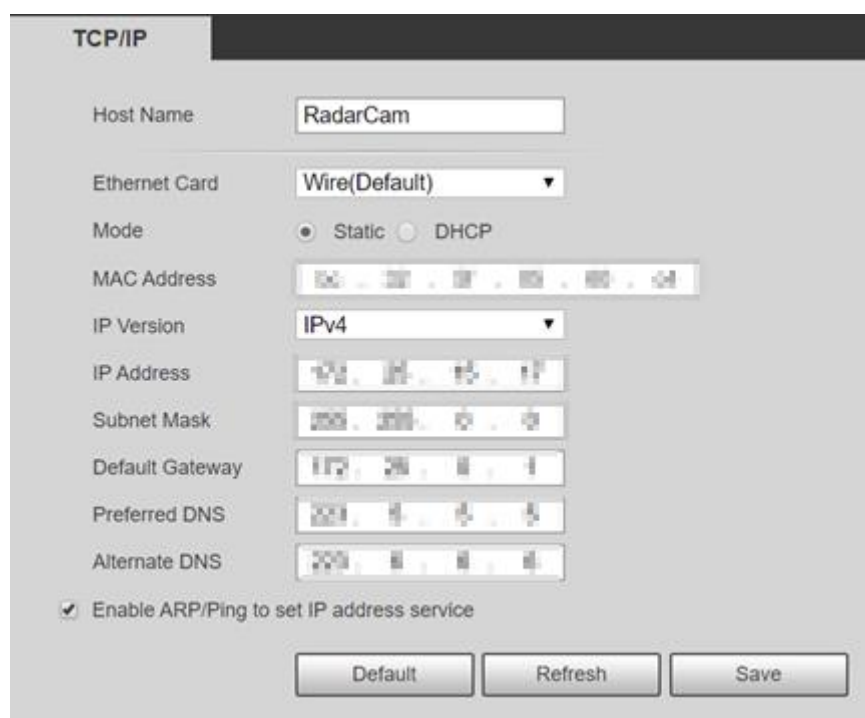
3.3 Changing IP Address

Configure IP address appropriately according to the actual network usage, and make sure that the Radar can access the network.

Step 1 Log in to the web interface of the Radar and select **Setting > Network > TCP/IP**.

Step 2 Change IP address and configure other parameters as needed, and then click **Save**.

Figure 3-10 TCP/IP

The image shows a web-based configuration interface for TCP/IP settings. It has a title bar "TCP/IP" and a list of configuration fields. The "Host Name" is "RadarCam". The "Ethernet Card" is "Wire(Default)". The "Mode" is "Static". The "MAC Address" is "00:00:00:00:00:00". The "IP Version" is "IPv4". The "IP Address" is "192.168.1.1". The "Subnet Mask" is "255.255.0.0". The "Default Gateway" is "192.168.1.1". The "Preferred DNS" is "209.14.1.1". The "Alternate DNS" is "209.14.1.1". There is a checkbox "Enable ARP/Ping to set IP address service" which is checked. At the bottom are three buttons: "Default", "Refresh", and "Save".

TCP/IP

Host Name: RadarCam

Ethernet Card: Wire(Default)

Mode: ☒ Static ☐ DHCP

MAC Address: 00 . 00 . 00 . 00 . 00 . 00

IP Version: IPv4

IP Address: 192 . 168 . 1 . 1

Subnet Mask: 255 . 255 . 0 . 0

Default Gateway: 192 . 168 . 1 . 1

Preferred DNS: 209 . 14 . 1 . 1

Alternate DNS: 209 . 14 . 1 . 1

☒ Enable ARP/Ping to set IP address service

Default Refresh Save

4 Quick Operation

4.1 Configuring Calibration

To raise the detecting accuracy, we recommend configuring calibration of a moving person or object within the Radar detection range.

4.1.1 Auto Calibration

To configure the auto calibration:

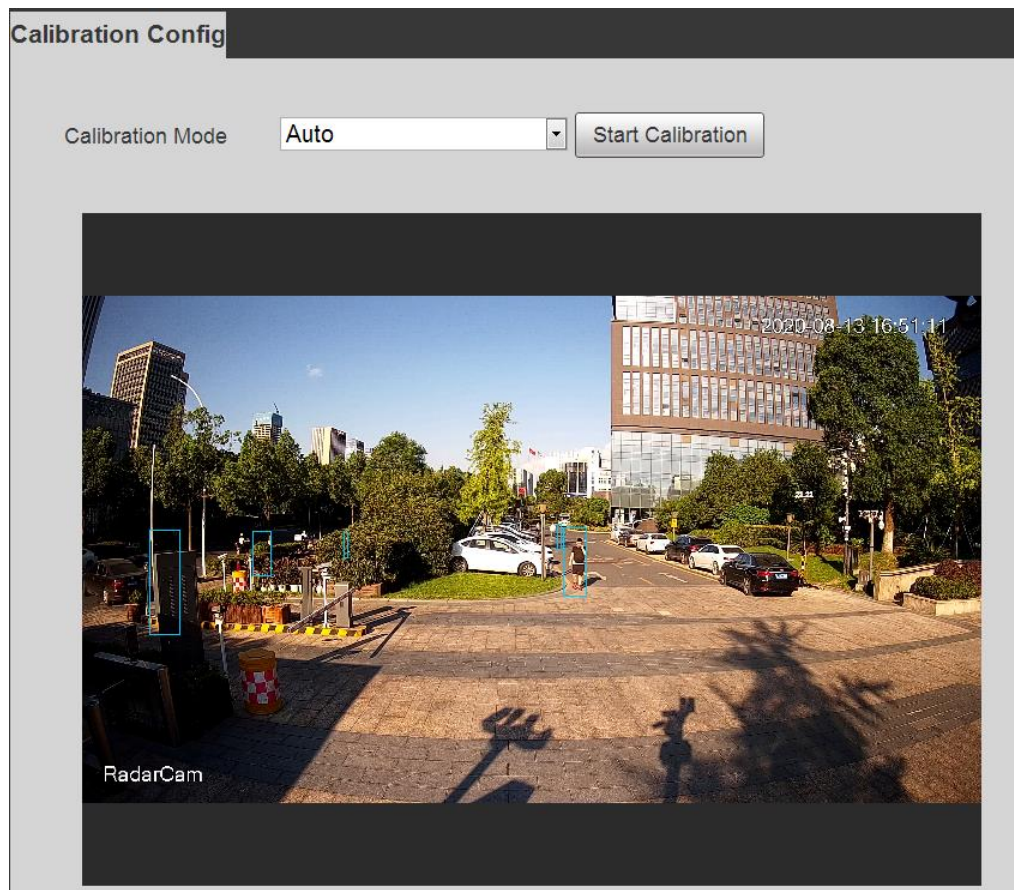
Step 1 Enable device attitude in **Setting > Radar Settings > Device Attitude**.

Step 2 Select **Setting > Radar Settings > Linkage**.

Step 3 In the calibration mode drop-down list, select **Auto**.

Step 4 In the live view interface, confirm whether the target position corresponds to the bounding box. You can configure the calibration manually if the auto effect is unsatisfactory.

Figure 4-1 Auto calibration



4.1.2 Manual Calibration

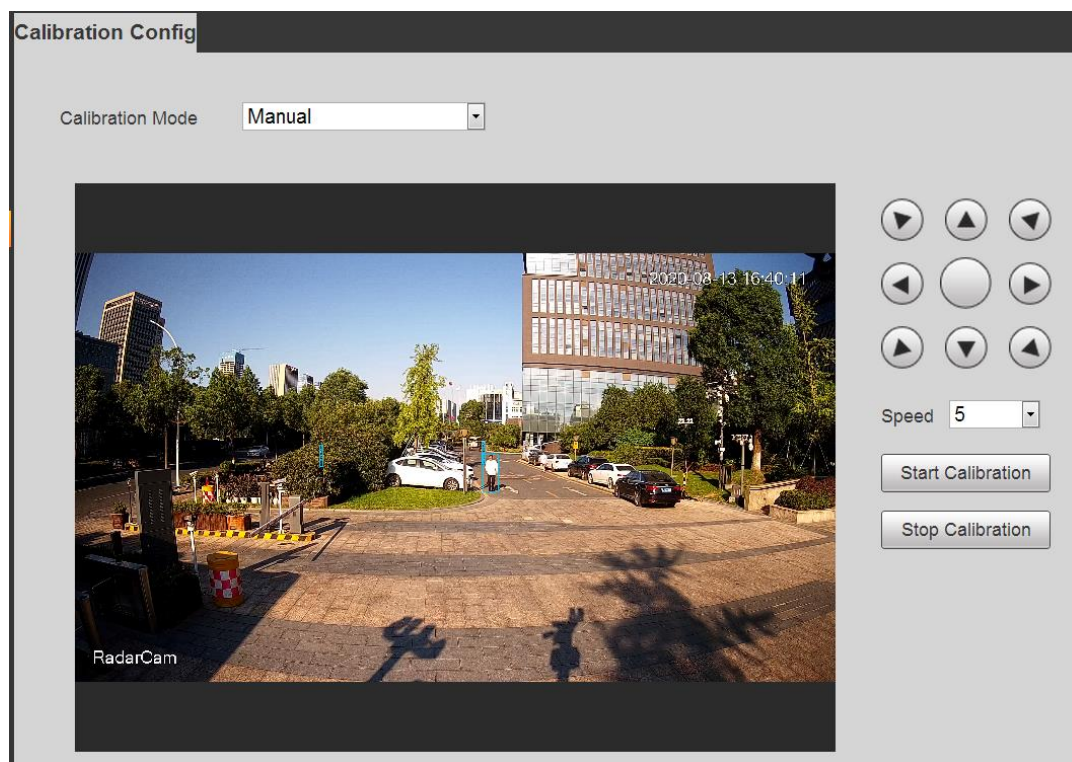
To configure the manual calibration:

Step 1 In the calibration mode drop-down list, select **Manual**.

Step 2 Click Start Calibration.

Adjust the position of the bounding box through the directional buttons and speed on the right side of the live view, so that the position of the box is basically synchronized with the position of the moving person or car.

Figure 4-2 Manual calibration



Step 3 Click **Stop Calibration** to save the settings.

4.2 Adjusting Radar Direction

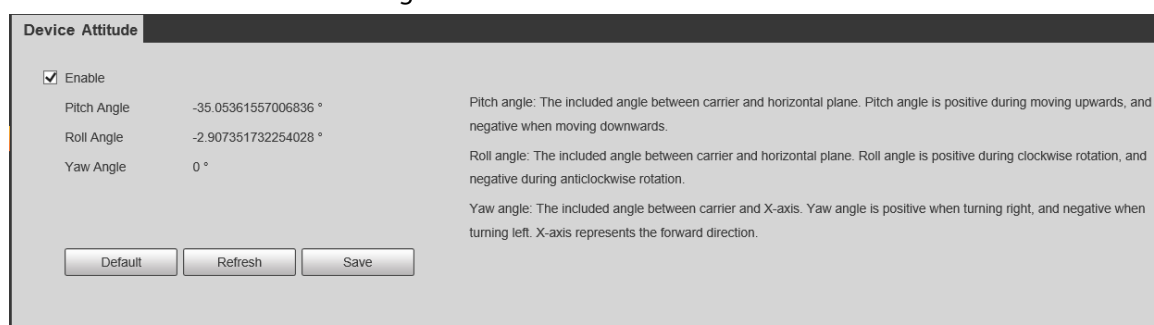
Device Attitude is enabled by default. When the direction of the Radar needs to be adjusted after the installation, you can enable the device attitude function to check whether the equipment is installed properly.

To enable the device attitude:

Step 1 In the web client of the Radar, select **Setting > Radar Settings > Device Attitude**.

Step 2 Select **Enable**.

Figure 4-3 Device Attitude



Step 3 Adjust the direction of the Radar. The recommended pitch angle is -3° and the roll angle is 0° .

Step 4 Click **Save**.

Appendix 1 FAQ

Problem	Solution
No response after the Radar is powered on.	<ul style="list-style-type: none"> When the Radar is powered on, the power indicator light will glow. If not, check whether the power cord is firmly connected. Check whether the polarity of the power cord is correct, the supply current and voltage conform to the Radar label, and PoE (802.3at) power supply is normal.
Power supply is normal but the Radar cannot detect objects.	<ul style="list-style-type: none"> Make sure that radar's installation direction is correct. See "2.2 Detection Range" and "2.4 Installation". Check whether the network port is connected.
No object is found in the detection area but there are detection signals.	<ul style="list-style-type: none"> Check if the Radar installation direction faces the detection region, and there is no intense electromagnetic equipment in the detection region to interfere the Radar. The pole with the Radar installed on is not swaying. No weed or swaying branch in the detection region. If any, prune them regularly or draw a shield area around them.
Does a target behind a solid object can be detected by the Radar?	Electromagnetic wave of the Radar cannot penetrate objects such as cement, rocks, glasses, and metals. If any, a blind zone will be formed behind these objects.
Is radar's detection range a sector?	No. The detection distance in front of the Radar is farther than the sector shows, but for the margin area, it is shorter than the sector shows.
Targets close to the Radar cannot be detected.	Due to limitations of installation height and horizontal detection angles of the Radar, a blind zone will be formed close to the Radar. The vertical detection angle of the Radar is $\pm\alpha$ (Generally, if signal strength is -3 dB, α is 10°). For detailed maximum blind zone distance, see Figure 2-2.
How does the Radar perform in severe weather?	<ul style="list-style-type: none"> Electromagnetic wave of the Radar can detect the target in blurry visual conditions such as heavy fog. In foggy or rainy days, radar's detection range might decrease slightly for the reason that electromagnetic wave might be damaged more or less. However, there is certain redundancy for the Radar performance when it leaves the factory, so it can conform to the standard requirements even though it is influenced by adverse factors. A false alarm might occur in areas with hail or heavy snow.

Appendix 2 Cybersecurity Recommendations

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

Mandatory actions to be taken for basic device network security:

1. Use Strong Passwords

Please refer to the following suggestions to set passwords:

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

2. Update Firmware and Client Software in Time

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

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

1. Physical Protection

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

2. Change Passwords Regularly

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

3. Set and Update Passwords Reset Information Timely

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

4. Enable Account Lock

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

5. Change Default HTTP and Other Service Ports

We suggest you to change default HTTP and other service ports into any set of numbers

between 1024~65535, reducing the risk of outsiders being able to guess which ports you are using.

6. Enable HTTPS

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

7. MAC Address Binding

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

8. Assign Accounts and Privileges Reasonably

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

9. Disable Unnecessary Services and Choose Secure Modes

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

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

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

10. Audio and Video Encrypted Transmission

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

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

11. Secure Auditing

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

12. Network Log

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

13. Construct a Safe Network Environment

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

- Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.
- The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.
- Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.

- Enable IP/MAC address filtering function to limit the range of hosts allowed to access the device.

More information

Please visit Dahua official website security emergency response center for security announcements and the latest security recommendations

ENABLING A SAFER SOCIETY AND SMARTER LIVING

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.

Address: No. 1399, Binxing Road, Binjiang District, Hangzhou, P. R. China | Website: www.dahuasecurity.com | Postcode: 310053

Email: dhoverseas@dhvisiontech.com | Tel: +86-571-87688888 28933188