Security Radar

Quick Start Guide



V1.0.0

Foreword

General

This manual introduces the structure, installation, and network configurations of the security radar (hereinafter referred to as "the radar").

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.
 NOTE	Provides additional information as the emphasis and supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.0	First release.	January 2021

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 regions. For detailed information, see 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, please refer to our 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 occurred when using the device.
- If there is any uncertainty or controversy, please refer to our final explanation.

Important Safeguards and Warnings

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

Environmental Requirements

- Choose hard ground like concrete ground is optimal as detection area ground. 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 detection area that hinder the normal operation.
- Make sure that there is no electromagnetic interference like air conditioner exterior units and transformers around where the radar is installed or in the detection area.
- Transport, use and store the radar within permitted temperature and humidity level.
- Do not put the radar in humid, dusty, extremely hot or cold, and intense electromagnetic radiation places.
- Pack the radar with its original or the same quality package before transporting.
- Do not press hard, violently vibrate, and soak the radar when transporting, storing, and installing.

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 must 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 must 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 radar performance will be greatly impacted.
- 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 radar surface 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 more than one power supply methods to provide power for the radar at the same time; otherwise, the device might be damaged.

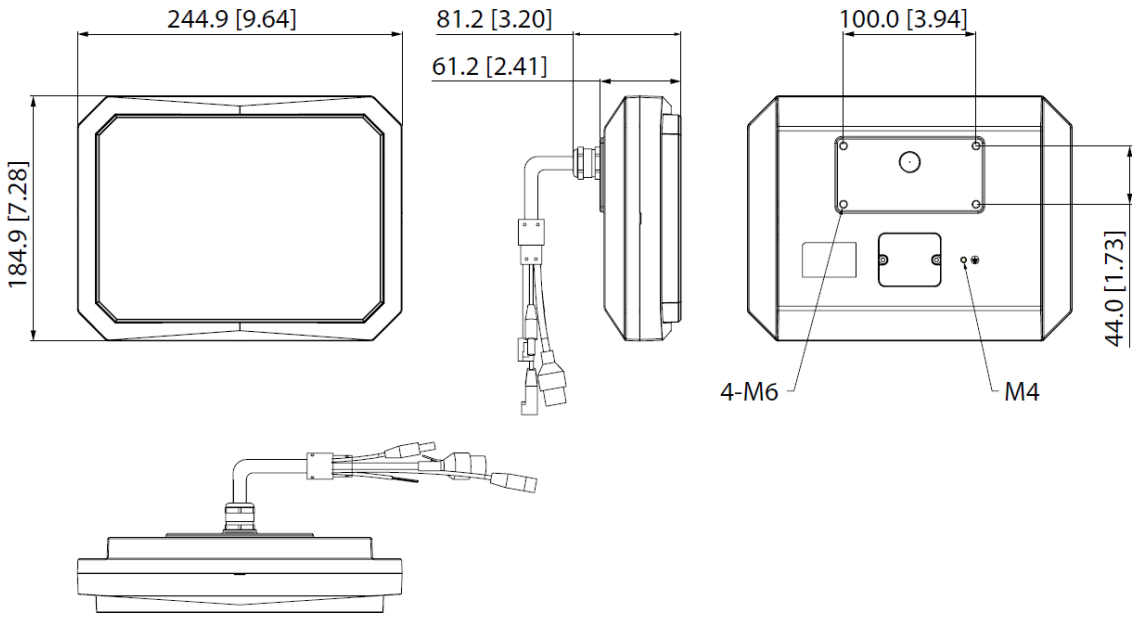
Table of Contents

Foreword ..... **I**
Important Safeguards and Warnings ..... **II**
1 Product Overview **1**
1.1 Dimensions 1
1.2 Structure 1
1.3 Detection Range 2
1.4 Cable Connection 3
2 Installation **5**
2.1 Environmental Requirements 5
2.2 Installation 5
2.2.1 Packing List 5
2.2.2 Installation Methods 6
2.2.3 Procedures 6
3 Network Configuration **9**
3.1 Initialization 9
3.2 Login 9
3.3 Changing IP Address 10
Appendix 1 Cybersecurity Recommendations **11**

1 Product Overview

1.1 Dimensions

Figure 1-1 Dimensions (mm [inch])



1.2 Structure

Figure 1-2 Structure

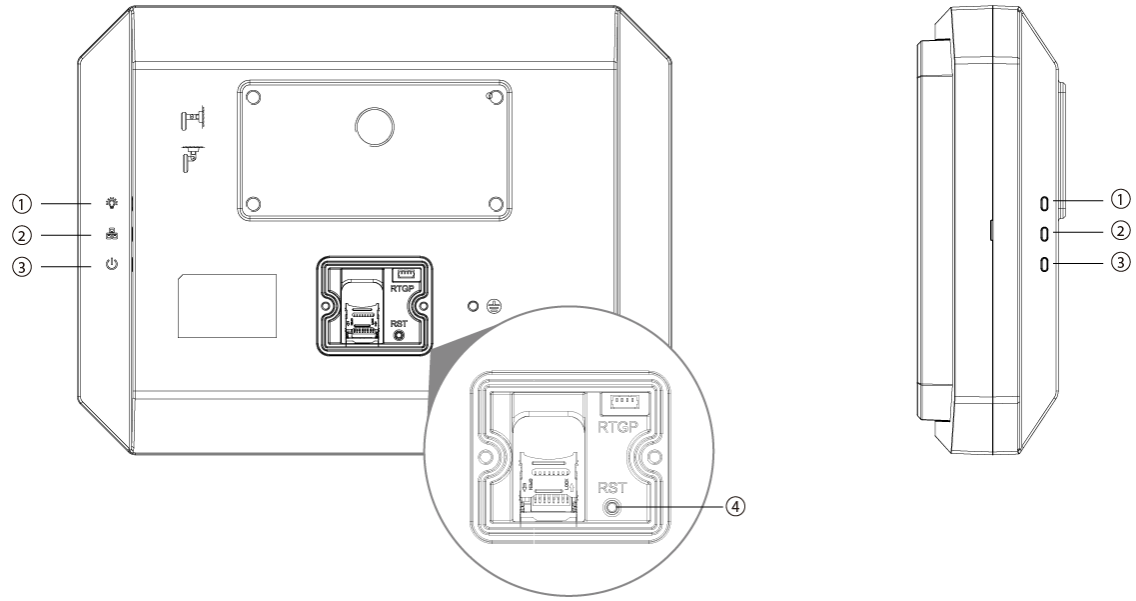


Table 1-1 Radar back descriptions

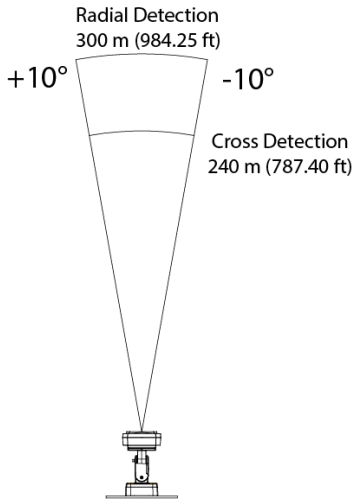
No.	Name	Description
1	Status indicator	● Solid green: Running normally. ● Flashes green: Radar is upgrading.
2	Network indicator	● Solid yellow: Network connected. ● Off: No network.
3	Power indicator	● Solid green: Running normally. ● Flashes green: Radar is being reset or upgraded.
4	Reset button	Press and hold for over 15 s, and then the radar will be restored to the factory settings.

1.3 Detection Range

Detection Angle

The horizontal detection angle of the radar is 20°. Because the radar is using microwave for detection, the detection distance is the longest on the central line, and gradually shortens to the margin of the detection range.

Figure 1-3 Detection distance



Blind Zone for Short Distance

The height of central point of the equivalent reflection interface of detected objects such as humans and vehicles is above 1 m.

Figure 1-4 Max. blind zone distance

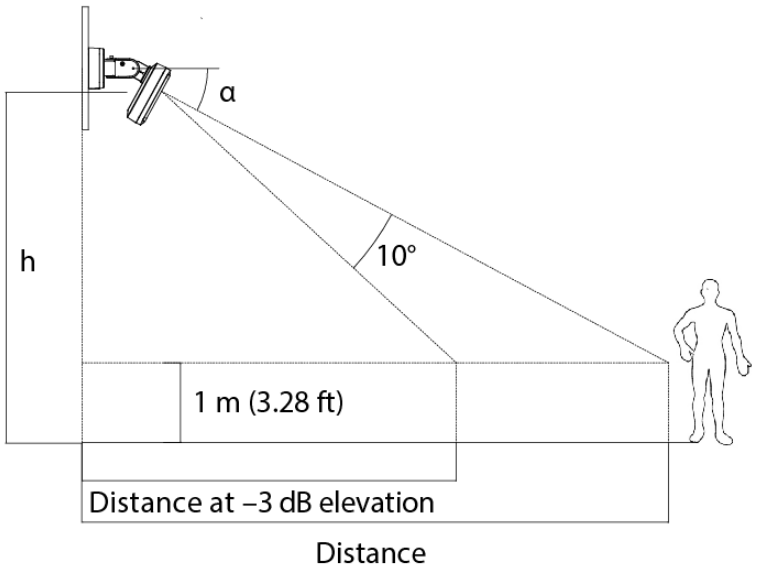


Table 1-2 Blind zone description

Installation Height (h)	Pitch Angle (α)	Blind Zone	Max. Detection Range (for Cross Detection)	Max. Detection Range (for Radial Detection)
3 m (9.84 ft)	1°	12 m (39.37 ft)	240 m (787.40 ft)	300 m (984.25 ft)
4 m (13.12 ft)	2°	16 m (52.49 ft)	240 m (787.40 ft)	300 m (984.25 ft)
5 m (16.40 ft)	3°	24 m (78.74 ft)	240 m (787.40 ft)	300 m (984.25 ft)

1.4 Cable Connection

⚠

Connect the cables according to the labels on the radar; otherwise the device might be damaged.

Figure 1-5 Cable connection

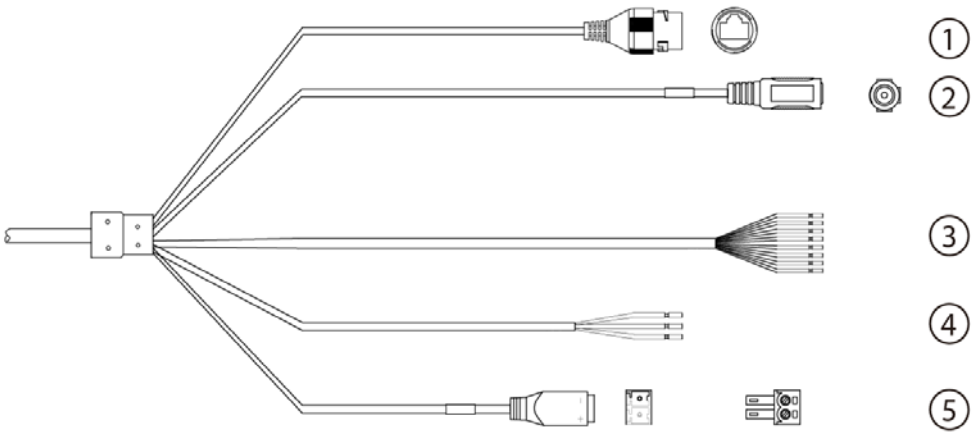


Table 1-3 External connection descriptions

No.	Port Name	Function
1	Network cable (female)	Connect to a standard Ethernet cable. Support PoE power supply. Comply with IEEE 802.3at standard when using PoE power supply.
2	Power input	12 V DC power input.
3	Alarm	● White: Alarm input ground. ● Blue: Alarm input. ● Brown: Alarm output 1. ● Pink: Alarm output 2. ● Green: Alarm output ground 1. ● Red: Alarm output 3. ● Purple: Alarm output 4. ● Light green: Alarm output 5. ● Black: Alarm output ground 2.
4	RS–485	● Yellow: RS–485_A. ● Orange: RS–485_B. ● Grey: GND. Reserved for future use.
5	Power input	24V AC power input.

2 Installation

2.1 Environmental Requirements

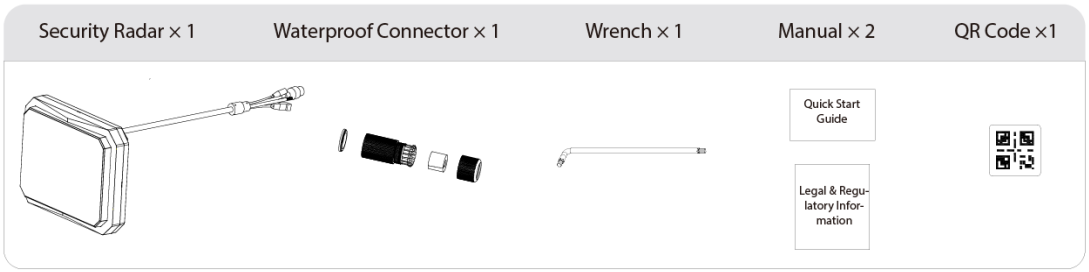
- The installation site has enough space to install the radar and other accessories.
- The wall and pole for installation can carry eight times the weight of the radar and other accessories.
- For wall mount, the wall shall be thick enough to install expansion bolts.
- No large areas of metals or glass 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.

2.2 Installation

2.2.1 Packing List

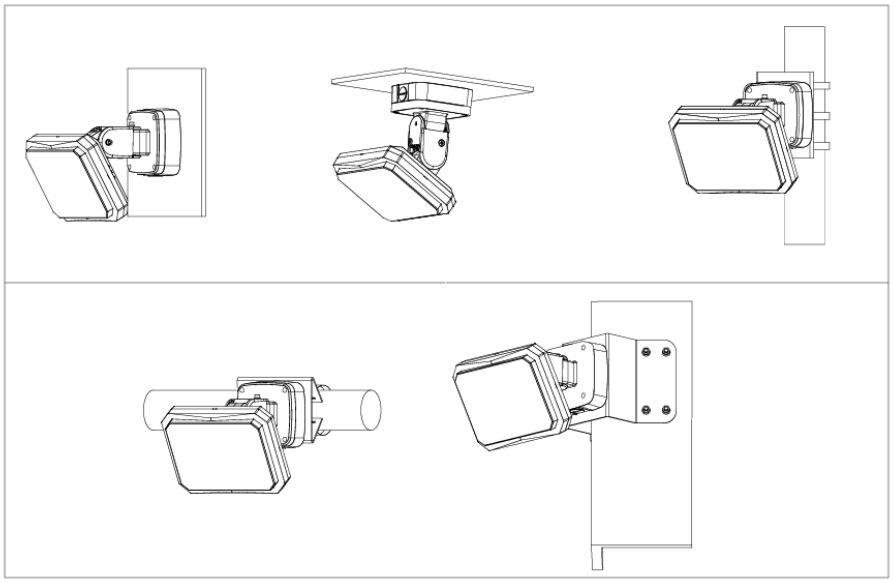
You need to prepare the following tools and cables before installation: Power cord, lightning protector, distribution box, air switch, PoE switch (optional), electric screwdriver, network cable, ladder, insulating gloves, and other things as needed.

Figure 2-1 Packing list



2.2.2 Installation Methods

Figure 2-2 Installation methods



2.2.3 Procedures

Figure 2-3 Install bracket

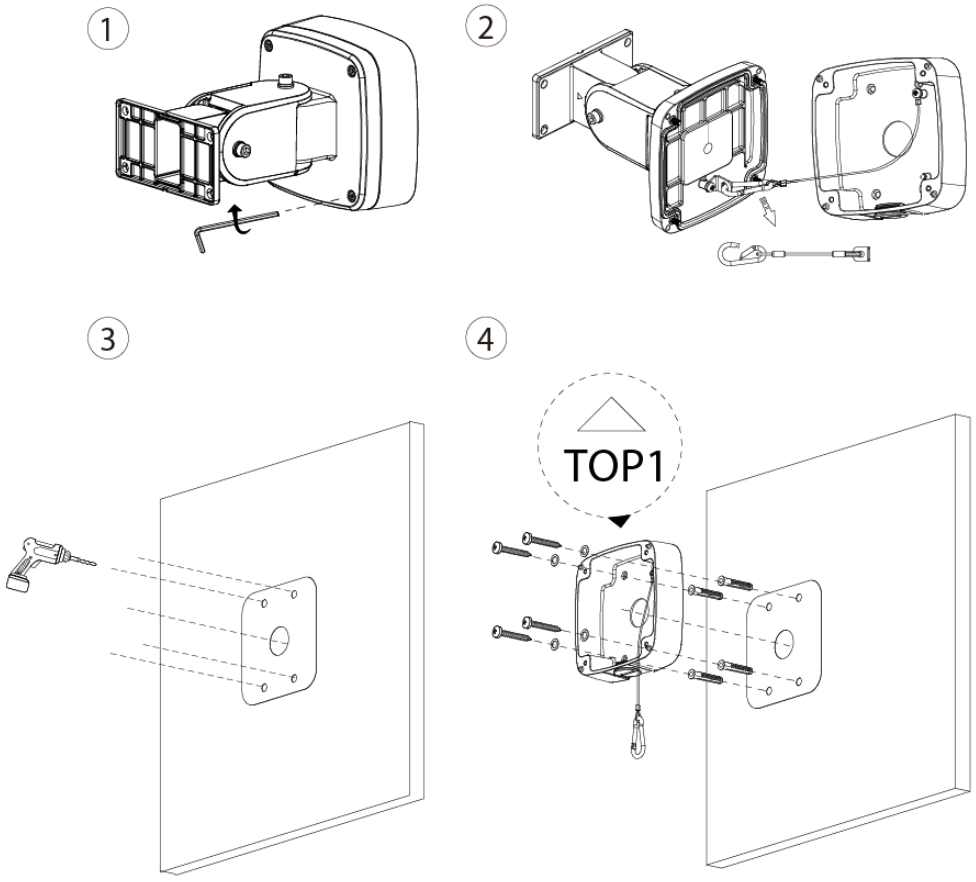


Figure 2-4 Attach radar

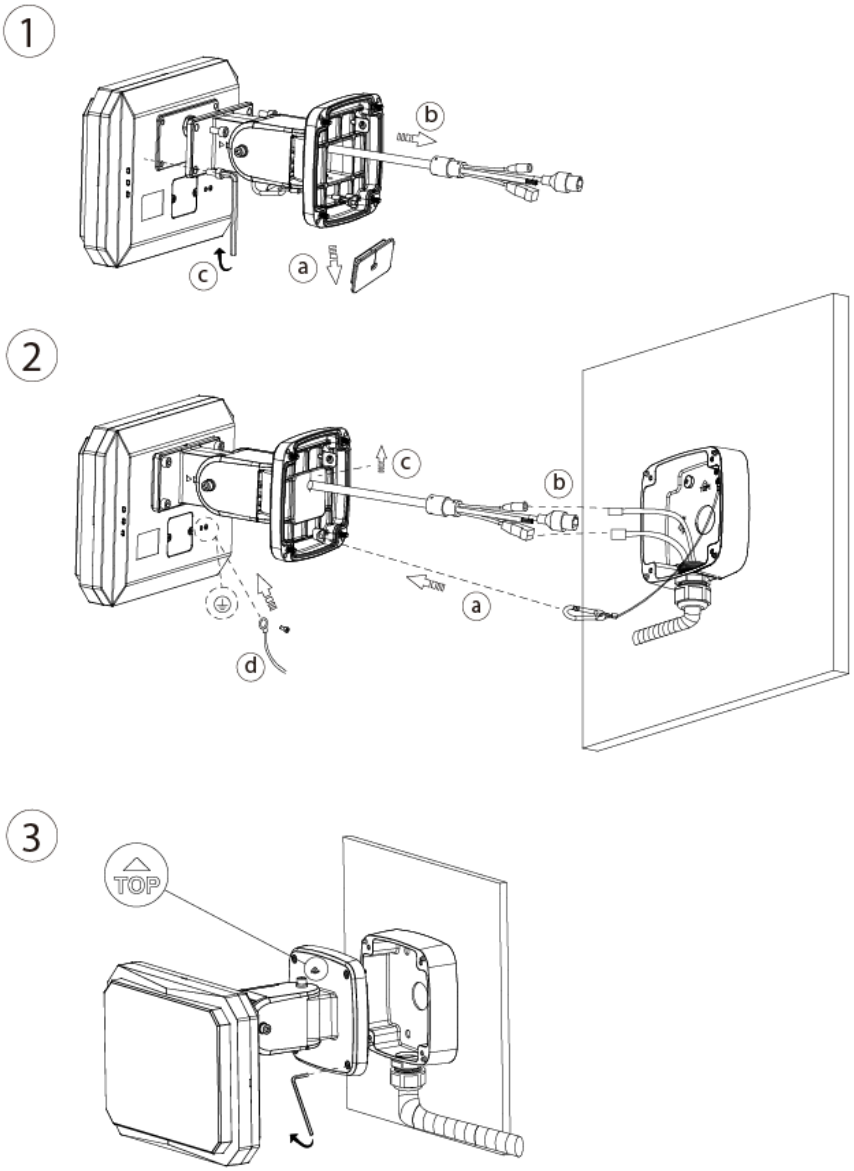
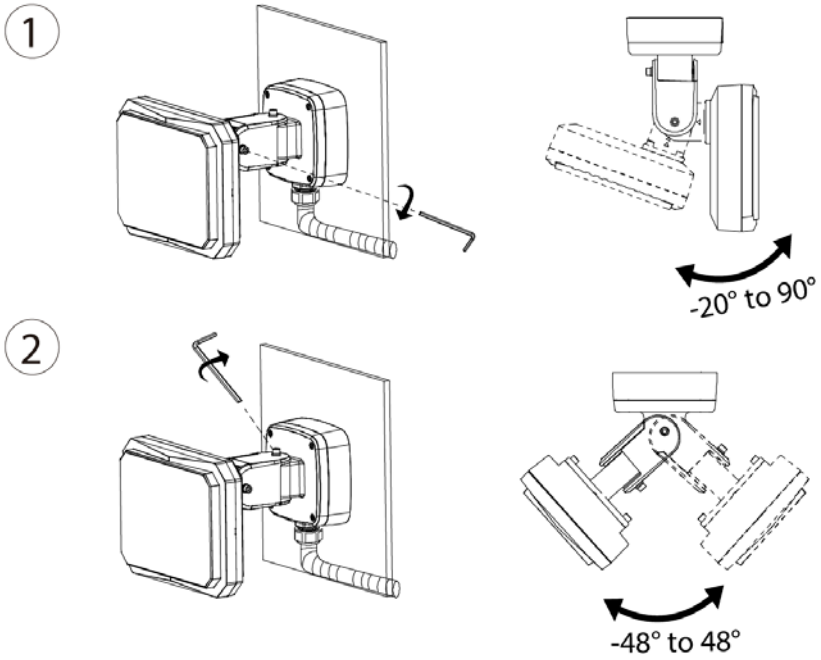


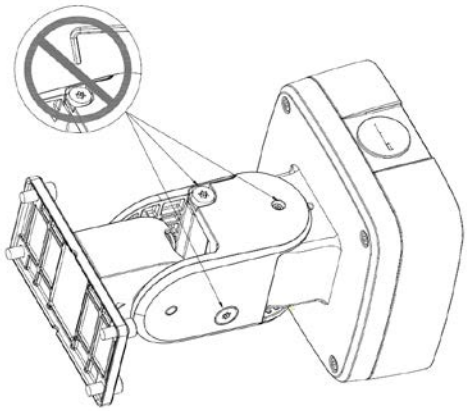
Figure 2-5 Adjusting radar angle



⚠

Do not loosen the three screws as shown below.

Figure 2-6 Do not loosen the three screws



3 Network Configuration

- 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.

3.1 Initialization

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

Step 1 Go to the IP address of the radar.

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

Step 3 Configure the time zone, and click **Next**.

Step 4 Set the password according to the prompt, and click **Next**.

We recommend setting an email address for future resetting password.

Step 5 Select **P2P** in the P2P interface as needed, and click **Next**.

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

3.2 Login

You need to download and install the plug-in for the first time logging in to the web interface.

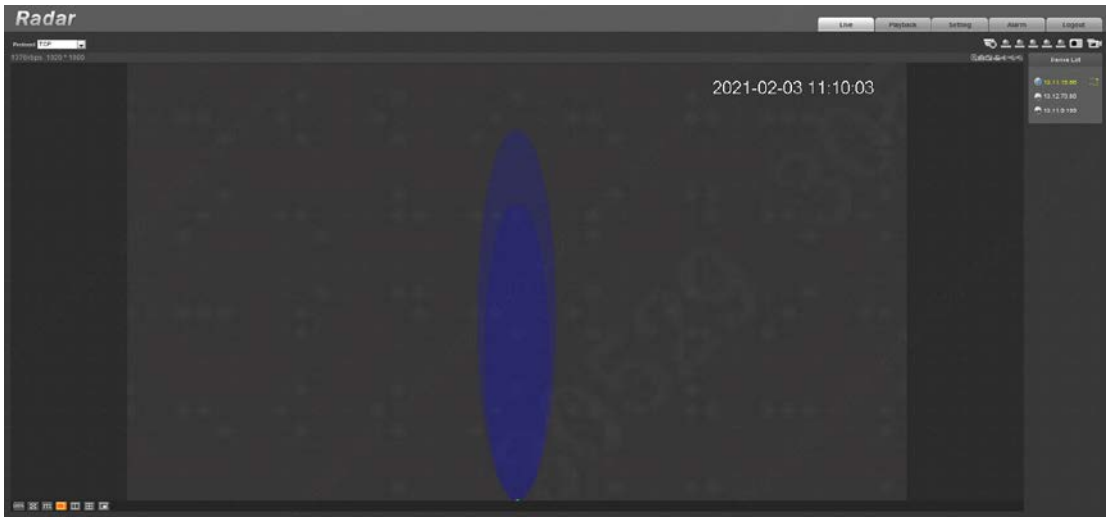
Step 1 On radar web interface, enter username and password, and then click **Login**.

- If you enter the wrong password for continuously 5 times, the account will be locked for 5 minutes.
- 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**.

Figure 3-1 Live



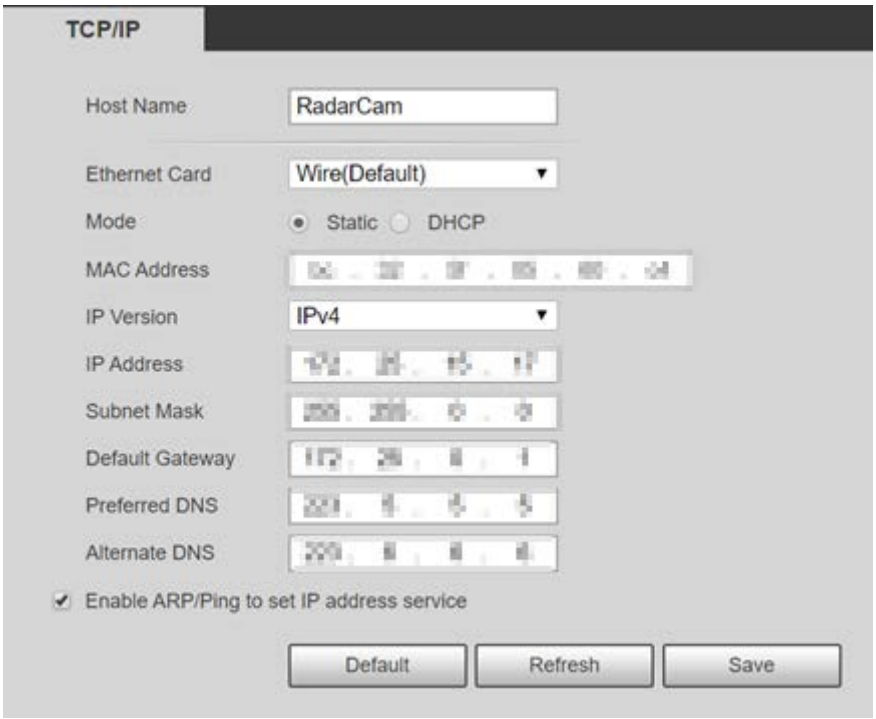
3.3 Changing IP Address

Configure IP address appropriately according to the actual network segment, 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 3-2 TCP/IP



Appendix 1 Cybersecurity Recommendations

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

Mandatory actions to be taken for basic device network security:

1. **Use Strong Passwords**

   Please refer to the following suggestions to set passwords:

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

2. **Update Firmware and Client Software in Time**

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

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

1. **Physical Protection**

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

2. **Change Passwords Regularly**

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

3. **Set and Update Passwords Reset Information Timely**

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

4. **Enable Account Lock**

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

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

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

6. **Enable HTTPS**

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

7. **MAC Address Binding**

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

8. **Assign Accounts and Privileges Reasonably**

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

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

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

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

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

10. **Audio and Video Encrypted Transmission**

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

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

11. **Secure Auditing**

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

12. **Network Log**

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

13. **Construct a Safe Network Environment**

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

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

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