Security Radar (B240)

Quick Start Guide

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD. V1.0.1

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
V1.0.1	Updated the manual.	March 2023
V1.0.0	First release.	January 2021

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, and comply with the guidelines when using it.

Environment Requirements

- Ground within the detection area must be hard ground. Concrete ground is the best to have. As for ground covered in vegetation, the height of the vegetation should be below 20 cm.
- Make sure there are no objects in the monitoring area blocking the device such as vegetation, buildings, and vehicles.
- Make sure the device is installed in an area that does not expose it to electronic interference from devices such as air conditioner units and transformers.
- Transport, use and store the device under allowed humidity and temperature conditions.
- Do not put the device in humid, dusty, extremely hot or cold places with intense electromagnetic radiation.
- Pack the device with packaging provided by its manufacturer or packaging of the same quality before transporting it.
- Do not place heavy stress on the device, violently vibrate or immerse it in liquid during transportation.

Power Requirements

- Strictly comply with the local electrical safety code and standards.
- Make sure that the power supply is correct before operating the device.
- The power supply must conform to the requirements of ES1 in IEC 62368-1 standard and be no higher than PS2. Please note that the power supply requirements are subject to the device label.
- An emergency disconnect device must be installed during installation and wiring at a readily accessible location for emergency power cut-off.
- Protect the power cord and wires from being walked on or squeezed particularly at plugs, power sockets, and the point where they exit from the device.

Maintenance Requirements

- Do not spray paint, stick stickers, put colors, objects or dirt on the surface of the device to avoid degrading the performance of the device.
- Do not dismantle to device, it can only be repaired by qualified professionals. Non-professionals dismantling the device can result in it leaking water.
- Clean the device body with a soft dry cloth. If there are any stubborn stains, clean them away with a soft cloth dipped in a neutral detergent, and then wipe the surface dry. Do not use volatile solvents such as ethyl alcohol, benzene, diluent, or abrasive detergents on the device to avoid damaging the coating and degrading the performance of the device.
- Use the accessories suggested by the manufacturer. Installation and maintenance must be performed by qualified professionals.
- Do not connect the device to two or more kinds of power supplies, to avoid safety risks and

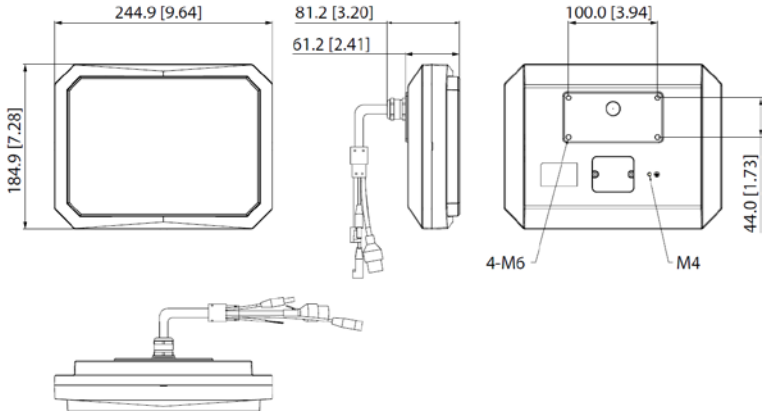
damage to the device.

Table of Contents

1 Overview

1.1 Dimensions

Figure 1-1 Dimensions (mm [inch])



1.2 Structure

Figure 1-2 Structure

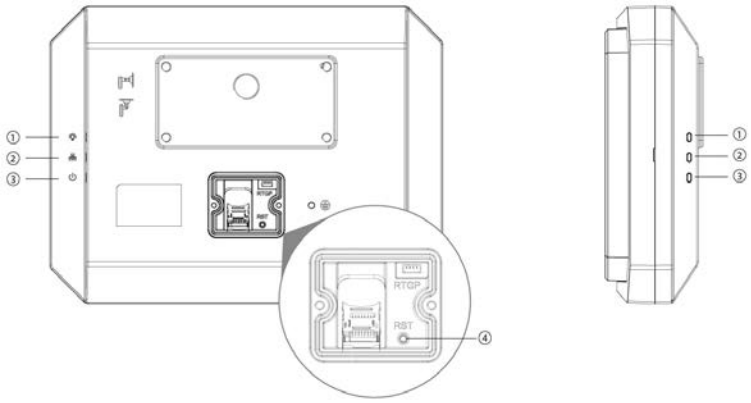


Table 1-1 Descriptions of radar back

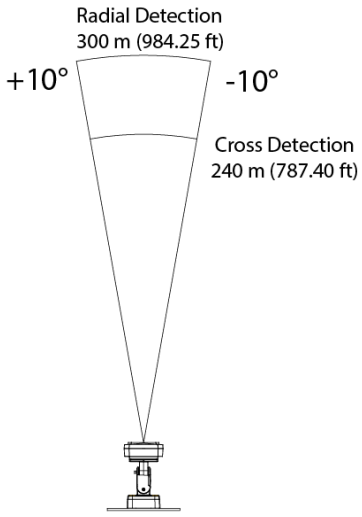
No.	Name	Description
1	Wall mount indicator	Indicate a wall mount radar. A mounting bracket is needed.
2	Ceiling mount indicator	Indicate a ceiling mount radar. A mounting bracket is needed.
3	Status indicator	• Solid green: Radar is running normally. • Flashes red: Alarm events happened in radar's detection region.
4	Network indicator	• Solid yellow: Network is connected. • Off: Network is not connected.
5	Power indicator	• Solid green: Radar is running normally. • Solid green: Radar is upgrading.

1.3 Detection Range

Detection Angle

The horizontal detection angle of the radar is 20°. Due to its microwave feature, 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

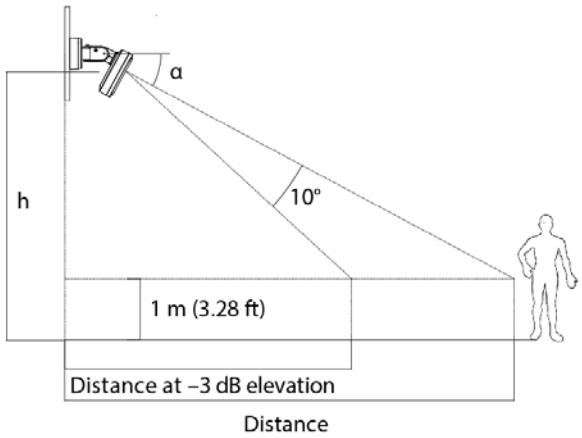


Table 1-2 Blind zone description

Radar Installation Height	Pitch Angle α	Blind Zone	Max. Detection Range (for Cross Detection)	Max. Detection Range (for Radial Detection)
3.0 m (9.84 ft)	1°	12.0 m (39.37 ft)	240 m (787.40 ft)	300 m (984.25 ft)
4.0 m (13.12 ft)	2°	16.0 m (52.49 ft)	240 m (787.40 ft)	300 m (984.25 ft)
5.0 m (16.40 ft)	3°	24.0 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

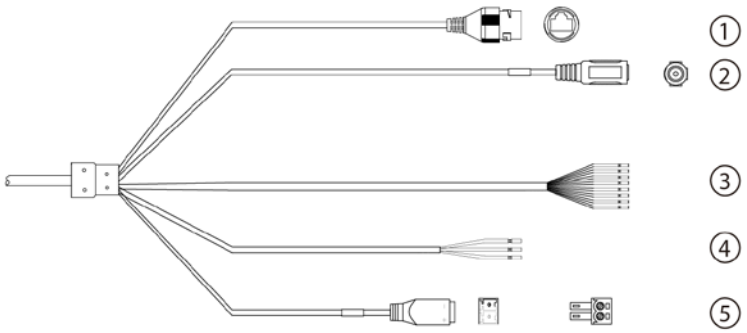


Table 1-3 External connection description

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 VDC 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	24 VAC power input.

2 Installation

2.1 Environmental Requirements

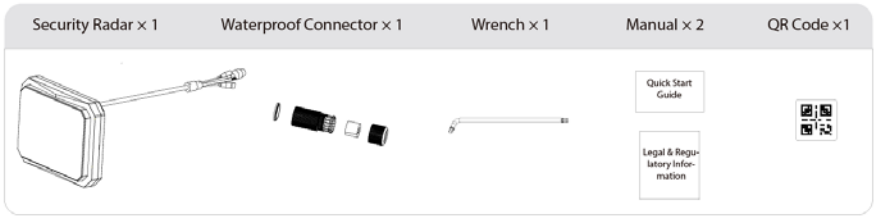
- The installation site has enough space to install the radar and other accessories.
- The wall and pole for installation can carry eight times the weight of the radar and other accessories.
- For wall mount, the wall shall be thick enough to install expansion bolts.
- No large areas of metals or glass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

2.2.1 Packing List

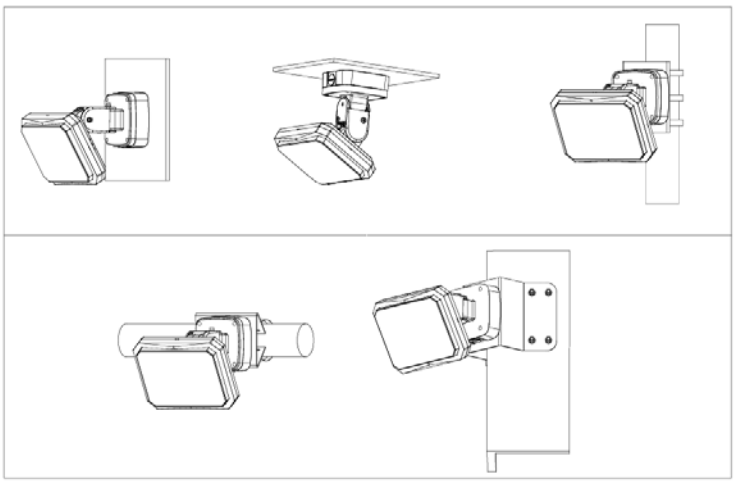
You need to prepare the following tools and cables before installation: Power cord, lightning protector, distribution box, air switch, PoE switch (optional), electric screwdriver, network cable, ladder, insulating gloves, and other things as needed.

Figure 2-1 Packing list



2.2.2 Installation Methods

Figure 2-2 Installation methods



2.2.3 Installation Procedures

Figure 2-3 Install bracket

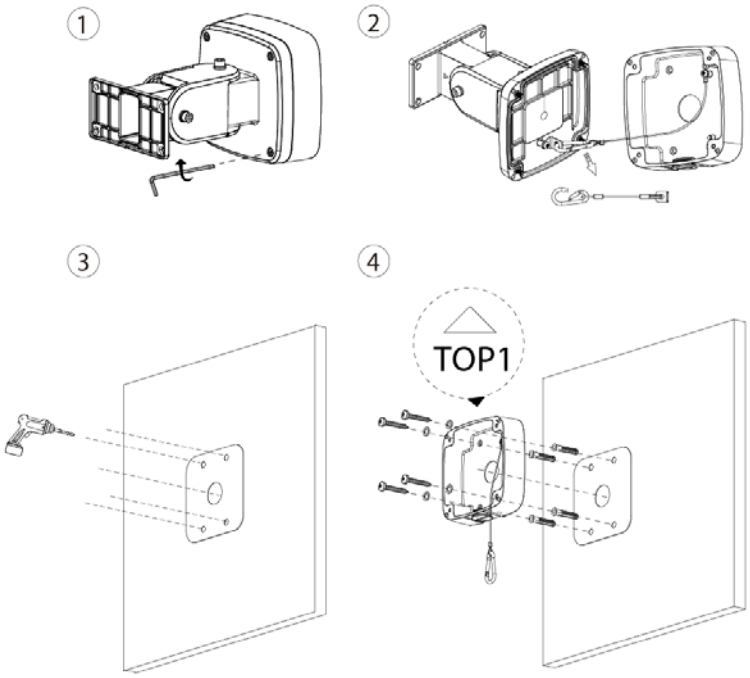


Figure 2-4 Attach radar

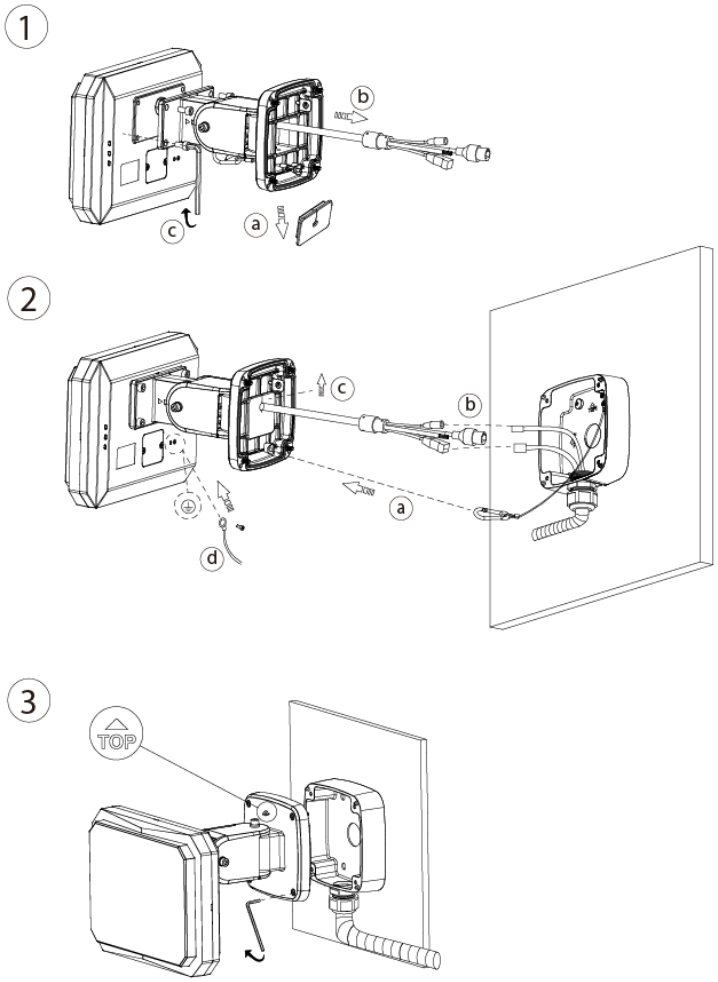


Figure 2-5 Adjusting radar angle

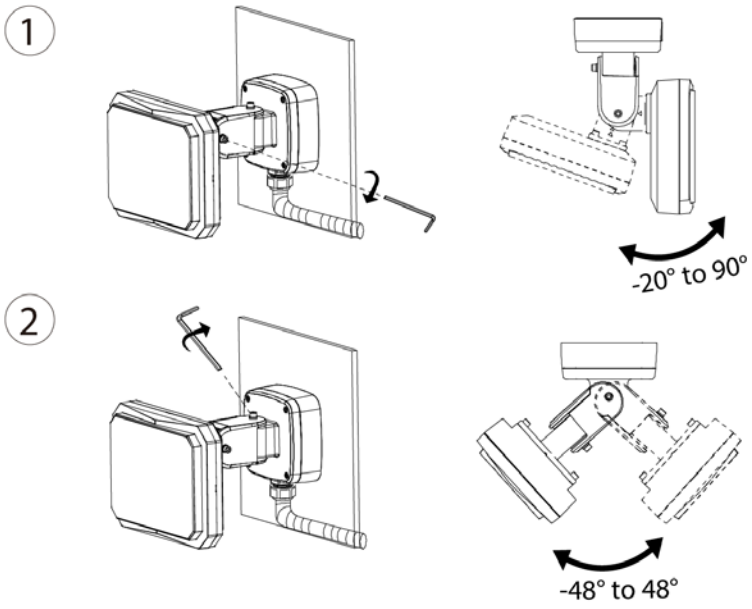
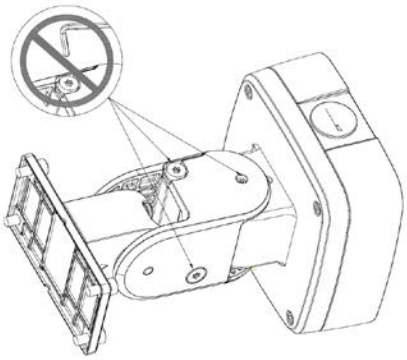


Figure 2-6 Do not loosen the three screws



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.

Procedure

Step 1 Go to the IP address of the radar.

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

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

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

We recommend setting an email address for future resetting password.

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

Procedure

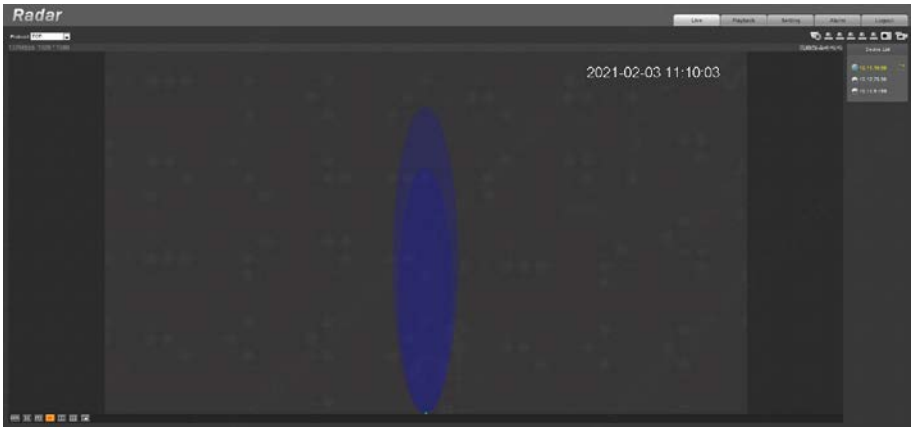
Step 1 On radar web page, enter username and password, and then click **Login**.

- 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

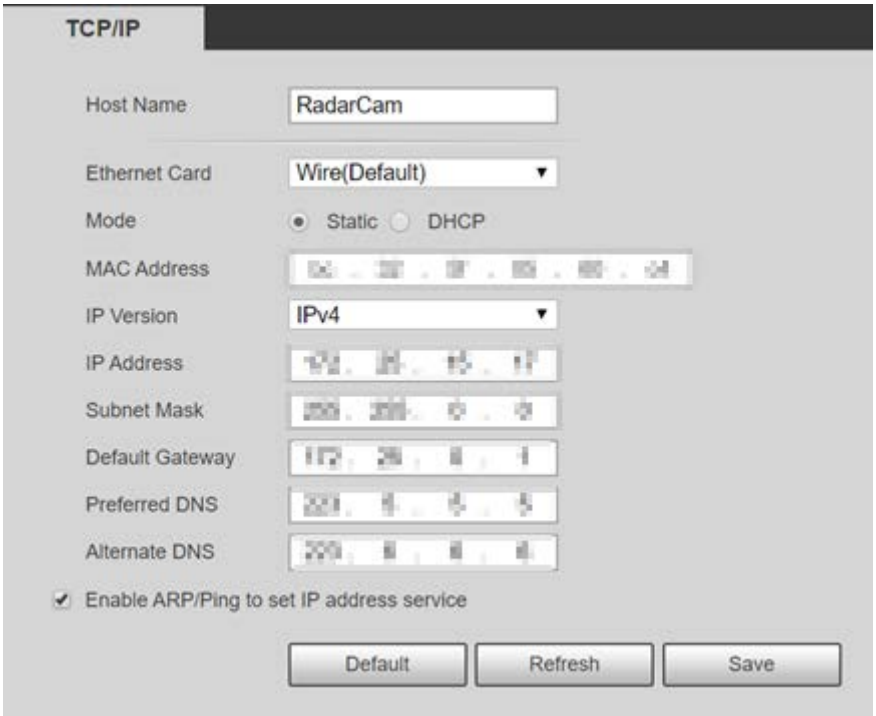
Configure IP address appropriately according to the actual network segment, and make sure that the radar can access the network.

Procedure

Step 1 Log in to the web interface of the radar and select **Setting** > **Setting** > **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 from Dahua 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