60 GHz Anti-Smashing Radar

User Manual

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD. V1.0.0

Foreword

General

This manual introduces the installation, functions and operations of the 60 GHz anti-smashing 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.	December 2025

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, audio, 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 to: 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 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.

Transportation Requirements

- Pack the device with packaging provided by its manufacturer or packaging of the same quality before transporting it.
- Transport the device under allowed humidity and temperature conditions.

Storage Requirements

Store the device under allowed humidity and temperature conditions.

Installation Requirements

- Do not connect the power adapter to the device while the adapter is powered on.
- Strictly comply with the local electric safety code and standards. Make sure the ambient voltage is stable and meets the power supply requirements of the device.
- Do not connect the device to two or more kinds of power supplies, to avoid damage to the device.
- Use the accessories suggested by the manufacturer. Installation and maintenance must be performed by qualified professionals.
- When using a laser beam device, avoid exposing the surface of the device to laser beam radiation.

- Personnel working at heights must take all necessary measures to ensure personal safety including wearing a helmet and safety belts.
- Do not place the device in a place exposed to sunlight or near heat sources.
- Keep the device away from dampness, dust, and soot.
- Put the device in a well-ventilated place, and do not block its ventilation.
- Use an adapter or cabinet power supply provided by the manufacturer.

- 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.
- Put the device in a well-ventilated place, and do not block its ventilation.

Operation Requirements

- Check whether the power supply is correct before use.
- Do not unplug the power cord on the side of the device while the adapter is powered on.
- Operate the device within the rated range of power input and output.
- Use the device under allowed humidity and temperature conditions.
- Do not drop or splash liquid onto the device, and make sure that there is no object filled with liquid on the device to prevent liquid from flowing into it.
- Do not disassemble the device without professional instruction.
- Do not aim the device at strong light sources (such as lamplight, and sunlight) when focusing it.
- Do not vibrate, squeeze or immerse the device in liquid during transportation, storage or installation.
- We recommend you use the device with a lightning protection device for stronger protection against lightning. For outdoor scenarios, strictly comply with the lightning protection regulations.
- Ground the function grounding portion of the device to improve its reliability. The device is a class I electrical appliance. Make sure that the power supply of the device is connected to a power socket with protective grounding.

Maintenance Requirements

Clean the device with a soft dry cloth or a clean soft cloth dipped in neutral detergent.

Table of Contents

1 Product Information

1.1 Overview

The Radar is specially designed for entrance and exit control in parking facilities, such as basement parking lots. Integrated with main control board of the barrier, it precisely controls the rise and fall of the arm to prevent accidental impacts and provide intelligent anti smash protection. Built on highly integrated Radio Frequency System-on-Chip (RFSoC), the Radar delivers a compact, cost effective solution for 24/7 operation with high detection sensitivity, reliable accuracy, simple commissioning and convenient installation.

This radar operates at a frequency of 60 GHz, utilizing a Linear Frequency-Modulated Continuous Wave (LFMCW) waveform. With an available bandwidth of up to 4 GHz, it achieves a range resolution of 40 mm (1.57″) and a ranging accuracy better than 20 mm (0.79″). The millimeter-wave antenna employs a Multiple-Input Multiple-Output (MIMO) configuration, delivering high angular resolution and precise angle measurement. The signal processing and control unit adopts a dual-core architecture (DSP + ARM). Through hardware-software co-design optimization, the system accurately identifies and distinguishes targets (including pedestrians, and vehicles) within the gate barrier area, thus effectively preventing malfunctions such as barrier arm strikes vehicle, person, and failure to lower the arm.

1.2 Features

- Uses intelligent algorithms to filter interference from various barrier arm types and its wide field of view improves monitoring coverage and detection predictability.
- Uses Digital Beamforming (DBF) with narrow-beam logic to focus detection, effectively mitigating barrier-induced errors.
- Compatible with mainstream barrier types, including advertising, fence, straight-arm and folding-arm barriers.
- Uses MIMO (multiple-input multiple-output) technology to recognize movement directions of targets, ideal for scenes with both vehicles and people entering and leaving.
- Adjustable detection distance and width with no need of reading scene data, and applicable to complicated scenes.
- Applicable to multiple complex onsite environments without background learning.
- Supports updating through RS-485 and mobile app (with Wi-Fi connection), and allows online commissioning and firmware upgrade, providing ease of operation.
- Convenient installation and maintenance: Comparing with loops, you can easily install the Radar by tightening the screws, with no need of road construction.
- Capable of identifying vehicles and people, preventing the barrier arm from hitting the vehicles and people.
- Two LED indicators are designed to better know the working status of the Radar: Red for power, and green for activity.
  - ◇ Solid red: Powered on.
  - ◇ Solid green: Target is detected. When the target leaves, the green indicator turns off.

- Automatically goes to the last working status before it is powered off.
- Adaptable to harsh environments and its detection performance will not be influenced by electromagnetic interference, light, dust, rain, and snow.

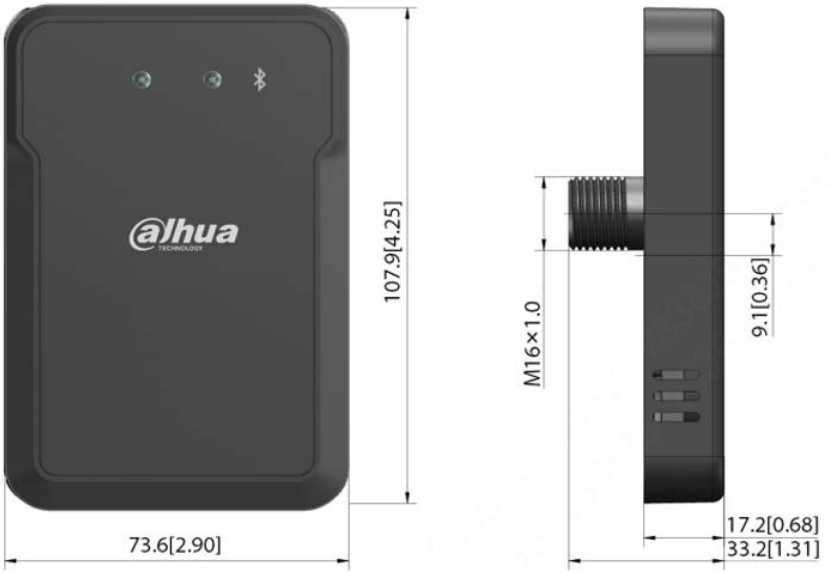
2 Structure

2.1 Appearance

Figure 2-1 Appearance

2.2 Dimensions

Figure 2-2 Dimensions (mm[inch])



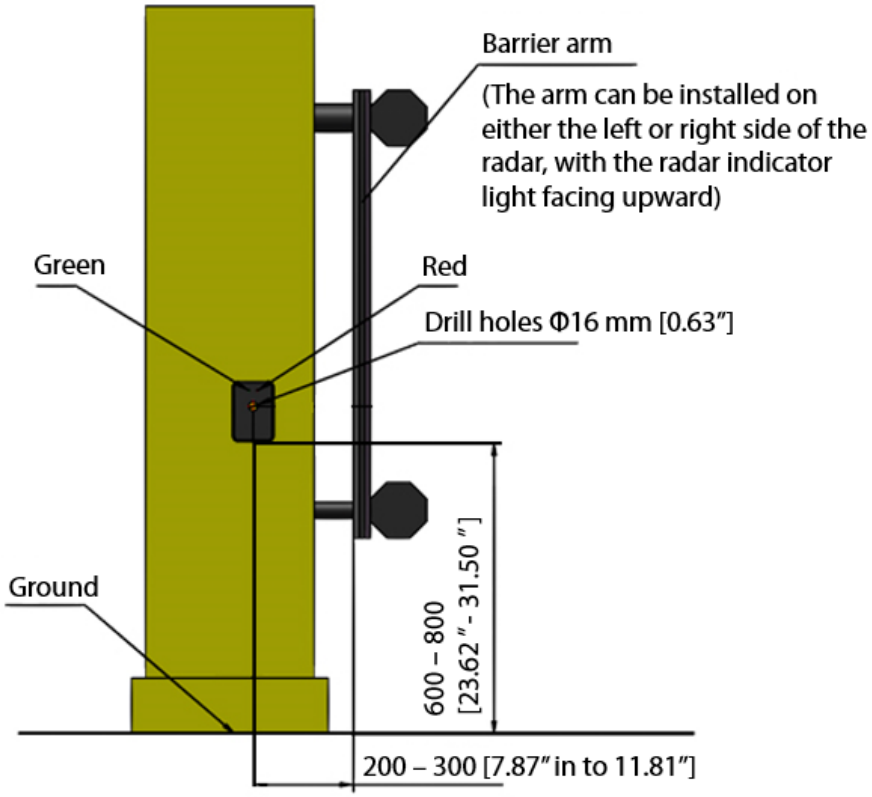
3 Installation

3.1 Installation Location

The radar should be installed on the barrier casing perpendicularly to the direction of the lane.

- The installation hole for the Radar should be located 200 mm - 300 mm (7.87″ - 11.81″) from the inner side of the arm.
- The distance from the lower edge of the Radar to the lane ground (excluding the cement pier):
  - ◇ Passenger vehicles: The lower edge of the Radar should be installed 600 mm - 700 mm (23.62″ - 27.56″) above the ground.
  - ◇ Trucks with a chassis height exceeding 700 mm (27.56″): The lower edge of the Radar should be installed 700 mm - 800 mm (27.56″ - 31.50″) above the ground.

Figure 3-1 Installation position (mm [inch])



Parameter	Description
Red	Power indicator, lighting up when the radar is powered on.
Green	Signal indicator, lighting up only when a target is detected during normal operation.

3.2 Installing the Radar

Step 1 Drill a fixing hole using an electric drill at the selected position of the barrier casing. We recommend you use a drill with a drill bit of 16mm (0.63”).

Holes for installing the Radar onto Dahua barrier casing are preserved by standard. Skip drilling holes when you are using Dahua barriers.

Step 2 Fix the Radar to the turnstile casing through the bottom bolts (with a torque value less than 20 N*m).

Step 3 Insert the radar into the hole position of the casing, cover it with the gasket, and then fix it with M16 nuts.

Step 4 Insert the wire harness end down into the radar, and then lock the metal buckle.

Figure 3-2 Install the Radar (1)

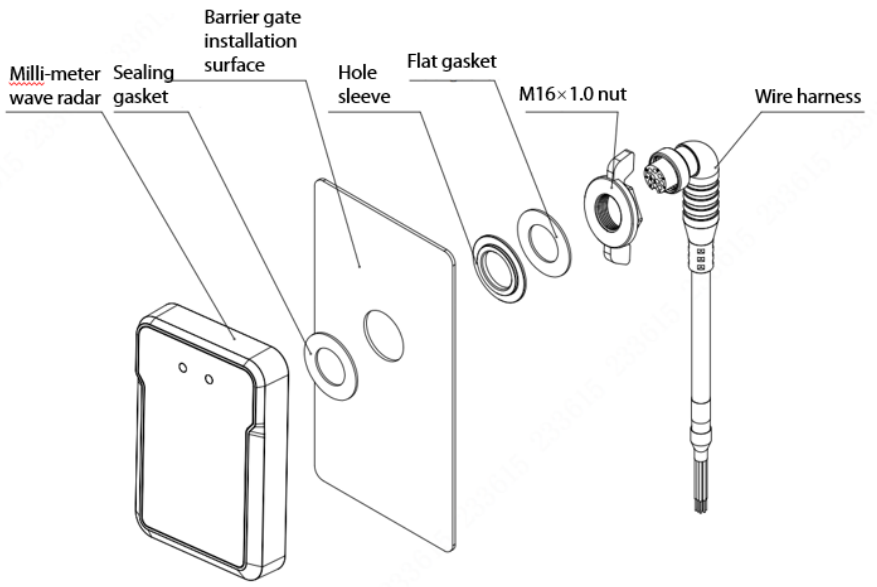


Figure 3-3 Install the Radar (2)

Figure 3-4 Radar installation completed

3.3 Wiring

Figure 3-5 Cable connection

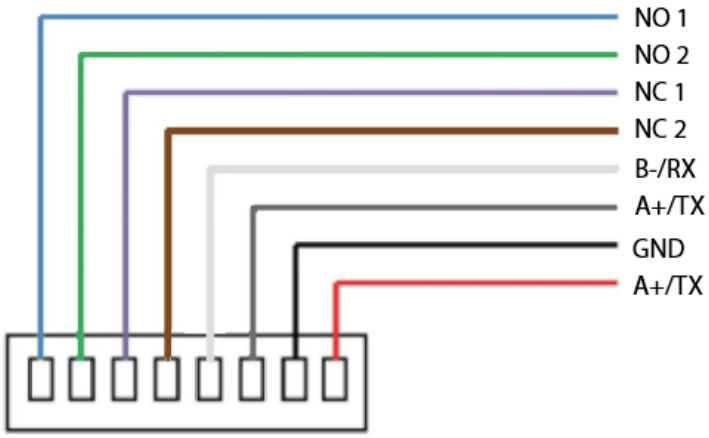


Table 3-1 Cable description

Cable	Color	Description
NO 1	Blue	Relay (normally open) output terminal. Connects to the radar/loop port and GND/common port of the barrier control box. The connection does not distinguish between the positive and negative.
NO 2	Green	
NC 1	Purple	Relay (normally closed) output terminal, reserved.
NC 2	Brown	
B-/RX	White	RS-485 port, retrieves radar running status and logs from the camera without affecting actual running.
A+/TX	Gray	
GND	Black	Power input of the Radar. The connection distinguishes between the positive and negative. We recommend using a 12 V/1 A external adaptor for power supply.

4 App Debugging

Scan the QR code provided in the accessory to download and install the R-Sight app.

Make sure that you have granted the app permissions of your Bluetooth, location, network and storage information.

4.1 Connecting Radar

Step 1 Download the App.

- If you use the Android system, scan the following QR code to download the app.

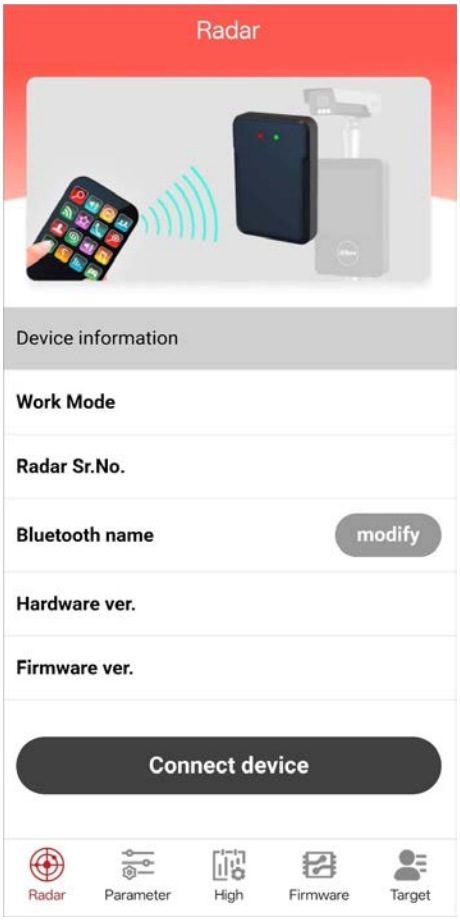
Figure 4-1 Download the app

- If you use the IOS system, search R-Sight app in the app store to download it.

  Whatever you use the Android system or IOS system, you can search the app through the applet of WeChat, and then use it dierectly.

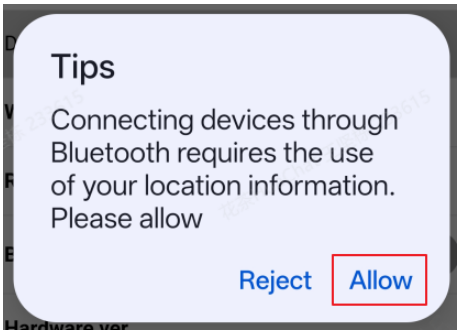
Step 2 Tap the app to go to the Rader screen, and then tap **Connect device**.

Figure 4-2 Radar status



Step 3 (Optional) Upon first connection, it will request location permission. Tap **Allow**.

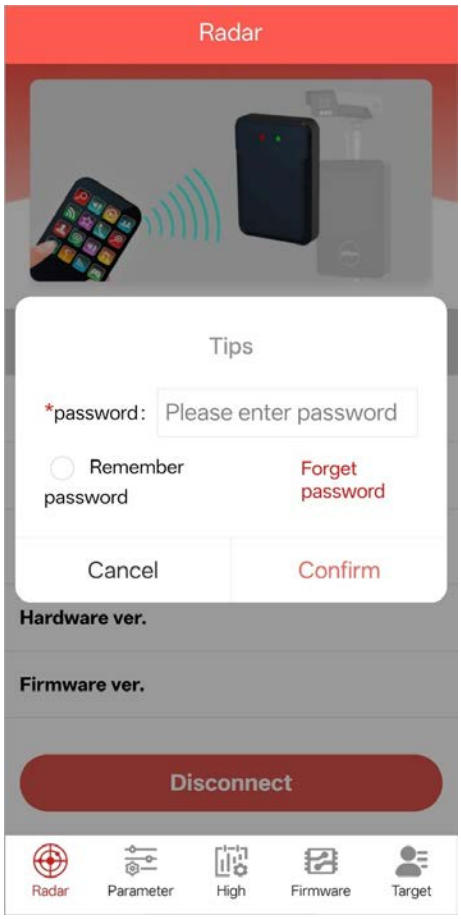
Figure 4-3 Allow location permission



Step 4 In the pop-up Bluetooth list, select the corresponding Bluetooth device, and then enter the default password (88888888).

For your first login, we recommend you modify the radar name and password.

Figure 4-4 Enter the password

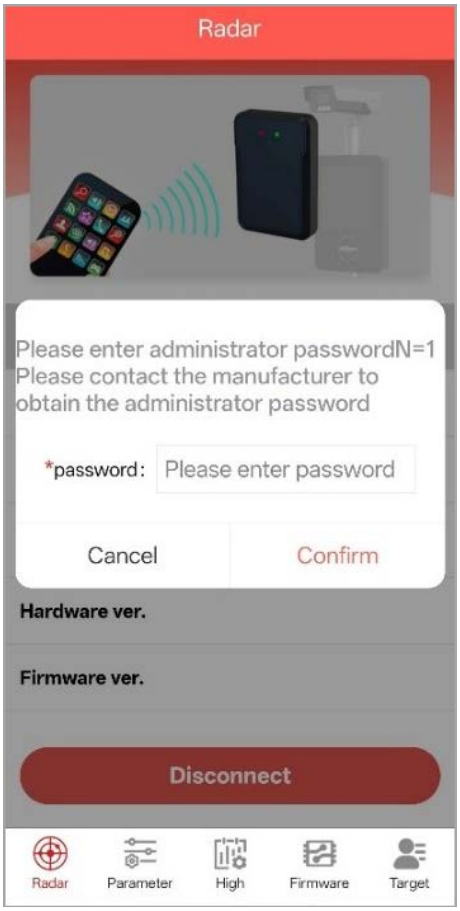


Related Operations

- On the radar status screen, tap **Disconnect** to terminate the connection between the app and the radar.
- If you forget your password, reset the password.
  1) Tap **Forget password**, and then enter the default administrator password (contact the manufacturer to obtain the administrator password).

     After you enter the default administrator password once, it will expire. If you require it again, contact the manufacturer to obtain the latest administrator password.
  2) Tap Confirm.

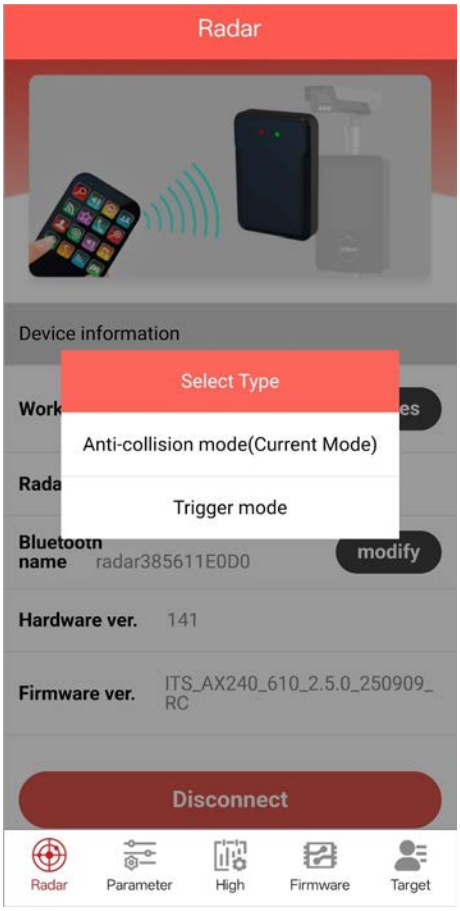
Figure 4-5 Reset password



3) Change the default administrator password immediately after successfully connecting.

Step 5 Tap **Switching modes** to select the radar working mode.

Figure 4-6 Select anti-collision mode



4.2 Configuring Radar Parameters

After the Radar is installed and connected to the app, you need to adjust the corresponding parameters based on the actual site.

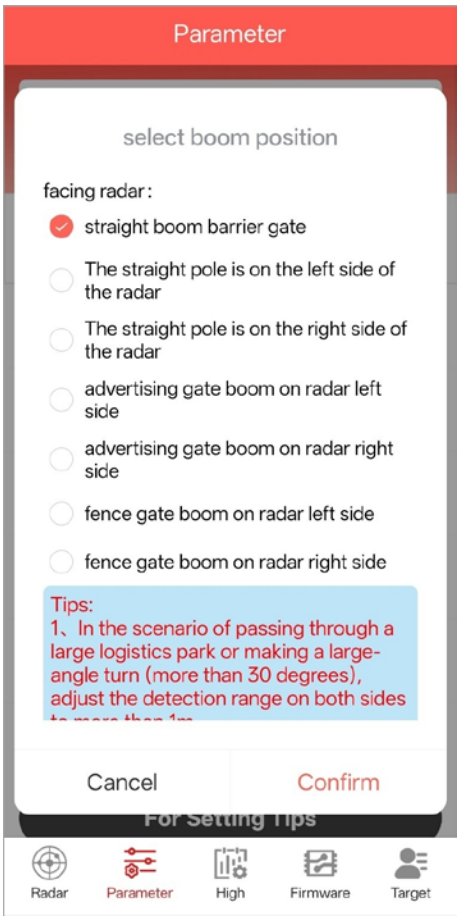
By restoring factory settings, the radar will be reset to its default factory state (anti-collision mode). To switch modes, you must manually select it again.

Prerequisites

Select Anti-collision mode when connecting devices.

Step 1 After the device is successfully connected, select **Parameter > Boom type selection**.

Figure 4-7 Select boom position



Step 2 Adjust parameters as needed.

- Enable: The radar detects only vehicles, not pedestrians, indicating that vehicles can trigger the radar, but pedestrians cannot.

Since the accuracy of human/vehicle distinction cannot achieve 100%, mixed human-vehicle traffic scenarios may result in false triggers when pedestrians pass by. In such cases, radar systems should not serve as the primary anti-crushing safeguard. For reliable protection, we recommend you use a loop detector.

- Disable: Both pedestrians and vehicles can trigger the radar (recommended).

Tap < or > to quickly adjust parameter values.

Figure 4-8 Parameter setting

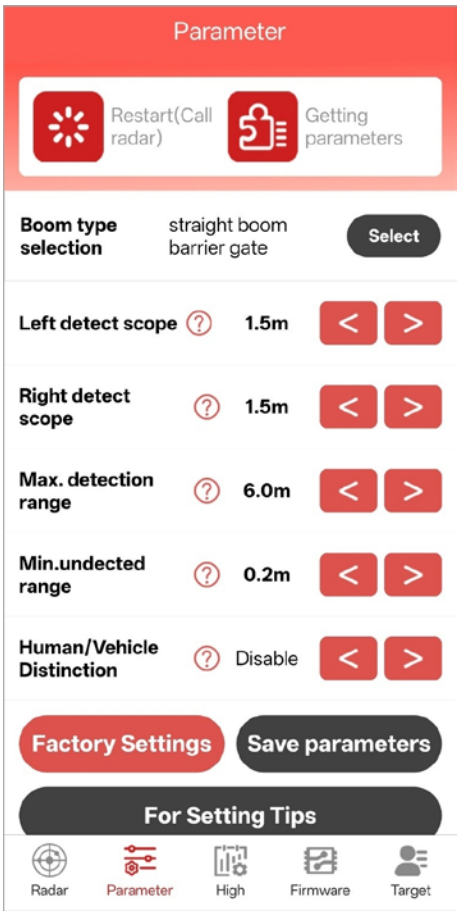


Table 4-1 Parameter setting

Parameter	Description
Boom type	Barrier gate type: Straight boom barrier gate by default. You can set it as needed. For non-standard straight poles such as round poles, folding poles, and telescopic poles, or straight poles with billboards, select **The straight pole is on the left side of the radar** and **The straight pole is on the right side of the radar**.
Left detect scope	The range filtered by the Radar. We recommend you leave it as 1.5 m (4.92 ft). You can adjust it as needed, with a minimum limit of 0.5 m (1.64 ft). When people face the Radar, the left side is the left detect scope and the right side is the right detect scope.
Right detect scope	
Max. detection range	Set based on the actual pole length. The actual pole length minus 0.3 m (0.98 ft) is recommended.
Min. undetected range	No detection is performed within 0.2 m (0.66 ft) (default) of the radar detection range.

Parameter	Description
Human/Vehicle Distinction	By default, it does not distinguish between pedestrian and vehicle modes, but can be set as needed. Since the accuracy of human/vehicle distinction cannot achieve 100%, mixed human-vehicle traffic scenarios may result in false triggers when pedestrians pass by. In such cases, radar systems should not serve as the primary anti-crushing safeguard. For reliable protection, we recommend you use a loop detector.
Radar log	Enabled by default. You can connect the camera to the RJ- 485 port to read logs from the Web end.

Step 3 Tap **Save parameters** to save the parameter settings.

4.3 Background Learning

Before configuring target information display or false alarm operations, configure background learning parameters.

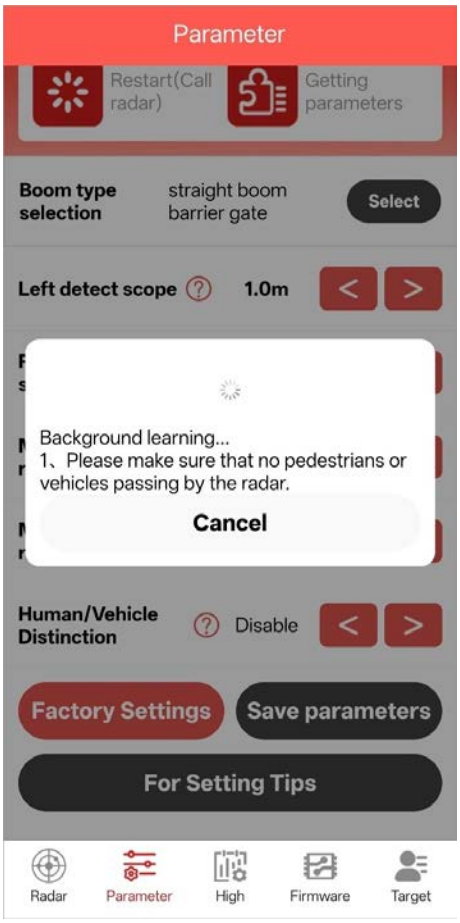
- During the background learning process, ensure that no people or vehicles pass by the radar. If any, restart the radar, and then perform background learning again.
- In boom barrier gate mode, lift the arm for background learning. In fence/advertising arm mode, use the remote control to continuously operate the rise and fall of the arm until it prompts that background learning is successfully configured.

Step 1 After the device is successfully connected, tap **Parameter** > **Select**, and then configure the barrier type as needed.

Step 2 Tap **Background learning**, and then wait for 30–60 seconds until it prompts that background learning is successfully configured. Otherwise, background learning should be performed

again.

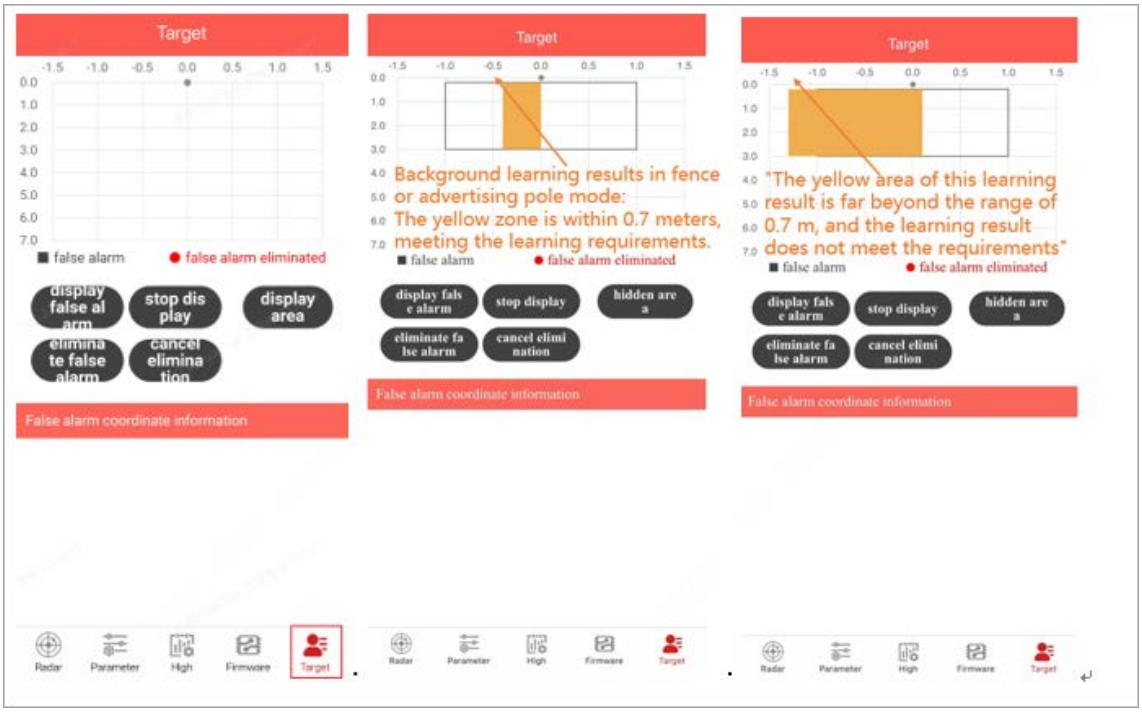
Figure 4-9 Perform background learning



Step 3 On the Target screen, tap **display area** to check background learning results:

- In fence/advertising arm mode, if the yellow zone (arm range) is within 0.7 m (2.30 ft), the learning is considered normal. If the yellow zone extends far beyond 0.7 m (2.30 ft), the arm learning range is too large, and parameters must be adjusted before performing background learning again.
- In straight arm mode, the display area screen should show no yellow zone. If a yellow zone appears, the learning is considered abnormal. Adjust the parameters and perform background learning again, ensuring no targets pass by the radar detection area.

Figure 4-10 Check learning background results



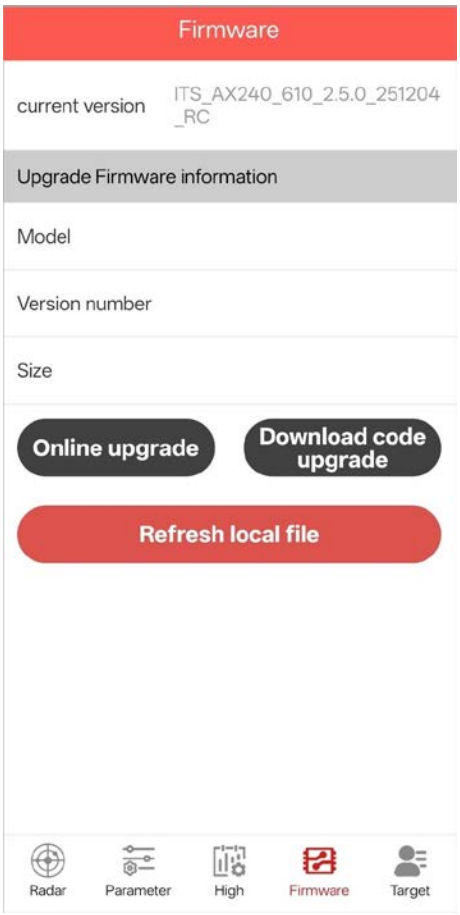
4.4 Updating Firmware

Supports viewing available firmware list on the **Firmware Upgrade** screen.

Step 1 After the device is connected successfully, select **Firmware**.

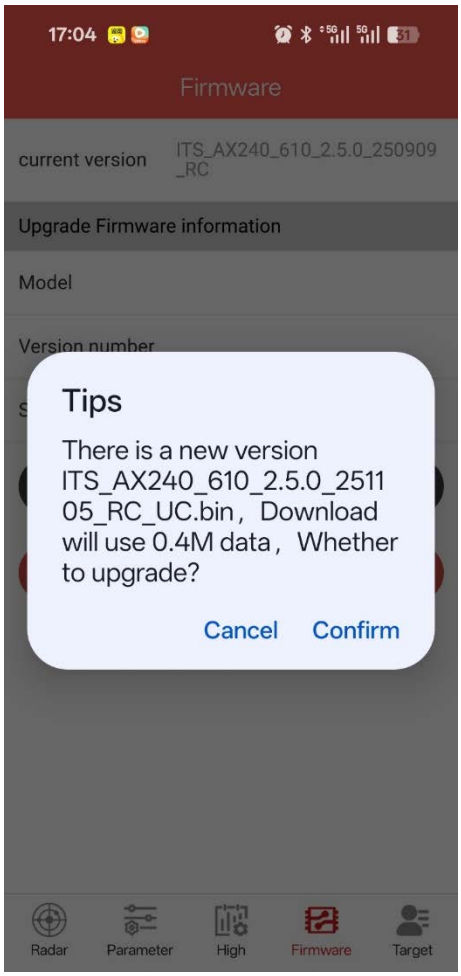
Step 2 Tap **Online upgrade** to download the latest firmware version online.

Figure 4-11 Update firmware (1)



Step 3 Tap **Confirm** to start upgrade.

Figure 4-12 Update firmware (2)



- Do not exit the App or switch to other apps during update. Otherwise the update may fail.
- If update fails, disconnect and restart the Radar to restore the firmware to previous version.

4.5 Displaying Target Information

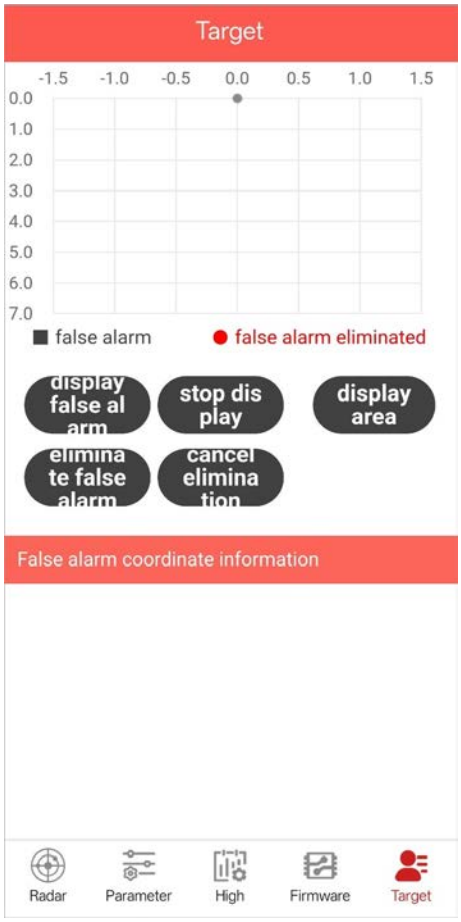
Prerequisites

You should finish the background learning before going to the Target Information screen. For details, see 4.3 Background Learning.

Step 1 After the background learning is completed, select **Target > display false alarm**.

If a false alarm is displayed, do not perform operations except stop display.

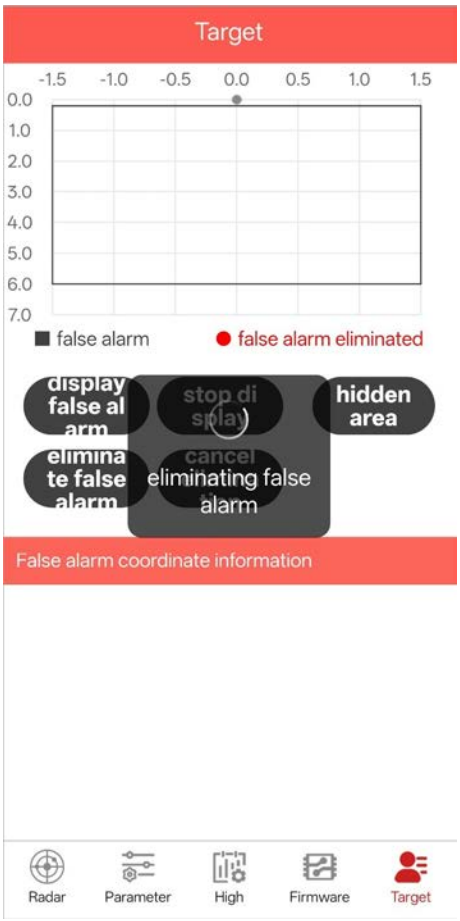
Figure 4-13 Display false alarms



Step 2 (Optional) If a false alarm is displayed on the screen, tap **stop display**, and then tap **eliminate**

the false alarm.

Figure 4-14 Eliminating false alarms

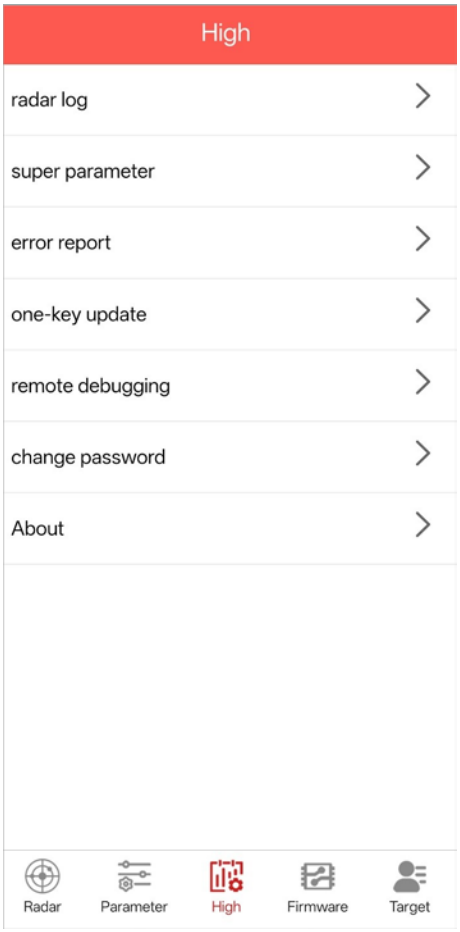


- This function is only available when the Radar detects a false alarm and the barrier arm cannot rise or fall normally.
- Make sure that the barrier arm is arisen before enabling the function. If many false alarms appear, we recommend adjusting background environment or starting the Radar on background learning again.

4.6 Other Functions

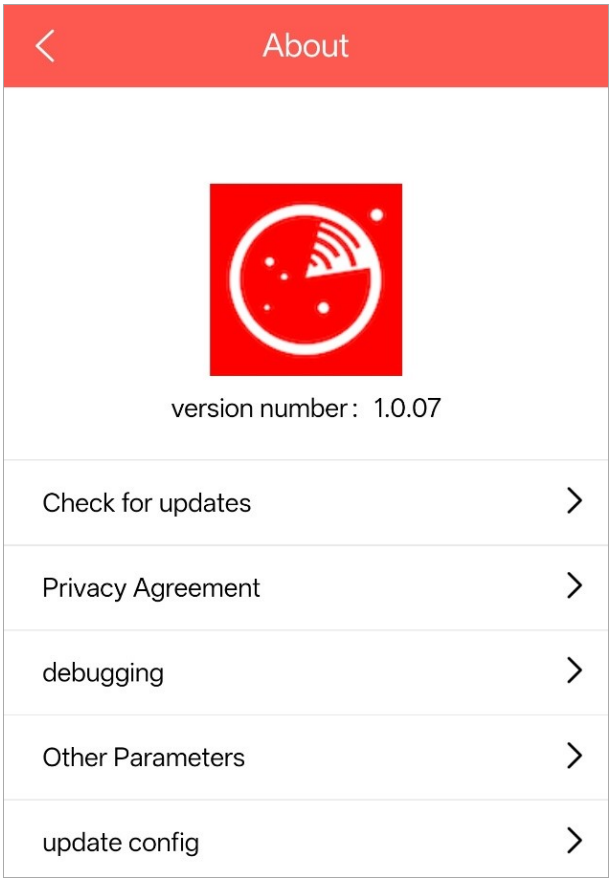
Supports viewing radar log, super parameter, error report, one-key update, remote debugging, change password, and about by tapping **High** at the bottom of the app.

Figure 4-15 View other functions



- Error Report: If the app malfunctions or performs other unexpected actions, tap error report, and then the error log will be uploaded to quickly locate the error.
- About: Includes app version number display, check for updates, privacy agreement, debugging, and other administrator-related functions. You need to enter the administrator password for access to the administrator-related functions.

Figure 4-16 About



5 Precautions

- 12 V/1 A power supply adapter is recommended for stable power supply to prevent radar performance degradation.
- For small passing vehicles, the recommended installation height is 0.6 m (1.97 ft). For large vehicles passing, the recommended installation height is 0.7 m (2.30 ft).
- The Radar antennas are concealed inside of it. When the surface is covered by foreign objects, such as water drops, frost, rain and snow, or dust, the Radar performance can be affected. Clean the Radar in time.
- Make sure no objects, such as metal fences, advertising boards, ANPR cameras or walls, exist within the Radar detection range, to avoid the Radar receiving interference.
- Radar is not recommended for single-lane mixed-in/out scenarios involving fence and advertising arm installations. A separate radar should be mounted on the other side of the arm to assure safe passing for vehicles.
- For situations where vehicles that have a gap wider than 1 m (3.28 ft) on their body, such as semi-trailers and tank cars, we recommend using 2 radars or control the barrier arms through remote control.
- Do not install the Radar on muddy roads, or under extreme weathers, such as cloudbursts and blizzards, to avoid impacting the performance of the Radar.
- Normally, set the detection distance according to the arm length. We recommend you to set it to the distance from the radar surface to the end of the arm minus 0.1 mm - 0.2 m (0.33 ft - 0.66 ft) to prevent the radar from detecting people or objects passing outside the barrier.
- When learning the environment, the fence/advertising arm might shake after lowering. Wait until the arm is completely stable before proceeding with further operations.
- If the radar causes repeated lifting (the arm lowered is detected by the radar and lifts again), relearn the background.
- When strong metal reflectors (such as iron plates) like speed bumps are directly in front of the radar, the radar installation height should be 0.75 m – 0.8 m (2.46 ft - 2.62 ft).
- Make sure to securely fix the barrier at a wobble angle no larger than 5°. In addition, when railings are installed outside the lane, make sure they are securely fixed to avoid the Radar moving or wobbling.
- Do not place metal debris within 1 m (3.28 ft) in front of the radar. Install metal objects such as guardrails and speed bumps as far away as possible from the radar, ensuring the end of the arm is more than 0.5 m (1.64 ft) away from metal objects.
- Do not place objects made of metal within 1 m (3.28 ft) range of the Radar. Make sure to install railings or speed bumps that contain metal far away from the Radar.
- Do not use the Radar in environments with strong magnetism.
- Make sure to insulate the unused bare wires after installation.
- Contact technical support when the Radar is installed in special environments.
- The anti-smashing radar is not suitable for mixed human-vehicle traffic scenarios. Since the accuracy of human/vehicle distinction cannot achieve 100%, mixed human-vehicle traffic scenarios may result in false triggers when pedestrians pass by. In such cases, radar should not be relied upon for anti-crushing protection. Instead, a loop detector is recommended.

Appendix 1 Security Commitment and Recommendation

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

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

1. Account Management

1.1 Use complex passwords

Please refer to the following suggestions to set passwords:

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

1.2 Change passwords periodically

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

1.3 Allocate accounts and permissions appropriately

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

1.4 Enable account lockout function

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

1.5 Set and update password reset information in a timely manner

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

2. Service Configuration

2.1 Enable HTTPS

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

2.2 Encrypted transmission of audio and video

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

2.3 Turn off non-essential services and use safe mode

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

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

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

2.4 Change HTTP and other default service ports

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

3. Network Configuration

3.1 Enable Allow list

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

3.2 MAC address binding

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

3.3 Build a secure network environment

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

Disable the port mapping function of the router to avoid direct access to the intranet devices from external network;

According to the actual network needs, partition the network: if there is no communication demand between the two subnets, it is recommended to use VLAN, gateway and other methods to partition the network to achieve network isolation;

Stablish 802.1x access authentication system to reduce the risk of illegal terminal access to the private network.

4. Security auditing

4.1 Check online users

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

4.2 Check device log

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

4.3 Configure network log

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

5. Software Security

5.1 Update firmware in time

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

5.2 Update client software in time

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

6. Physical protection

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

ENABLING A SMARTER SOCIETY AND BETTER 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