6-Series EAS Radio-Frequency Transceiver Antenna

User's Manual

V1.0.0

Foreword

This manual introduces the installation, functions and operations of the 6-Series EAS Radio-Frequency Transceiver Antenna (hereinafter referred to as "the Device"). Read carefully before using the device, and keep the manual safe for future reference.

Safety Instructions

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

Signal Words	Descriptions
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, lower performance, or unpredictable result.
ESD PROTECTION	Indicates electrostatic sensitive equipment.
WARNING ELECTRIC SHOCK	Indicates high voltage danger.
LASER RADIATION	Indicates strong laser radiation.
FAN WARNING	Indicates dangerous moving parts, please stay away from moving fan blades.
WARNING MECHANICAL INJURY	Indicates that equipment parts will cause mechanical wounding to people.
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 date
V1.0.0	First release.	May 2024

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: 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 detector, hazard prevention, and prevention of property damage. Read carefully before using the detector, and comply with the guidelines when using it.

Transportation Requirements

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

Storage Requirements

- Store the detector under the allowed humidity and temperature conditions.

Installation Requirements

- Install the detector in a well-ventilated place, and do not block the ventilation of the detector.
- It is recommended that the Device be installed 2 meters away from large motor-type equipment (such as elevators, high-power switching power supplies) to avoid interference.

Operation Requirements

- Use the detector under the allowed humidity and temperature conditions.

Maintenance Requirements

- Use the recommended power cables in the region and conform to the rated power specification.
- Only use the standard power adapter of the device, otherwise the user will be responsible for personnel injury or device damage.
- The power source shall conform to the requirements of the Safety Extra Low Voltage (SELV) standard, and supply power with rated voltage which conforms to Limited power Source

requirement according to（IEC60065）or（IEC60950-1.) Please note that the power supply requirements are subject to the device label.

- Be strictly grounded and powered independently. It's recommended not to work with other electrical equipment.

⚠

- Prevent liquids from splashing or dripping on the device. Make sure that there are no objects filled with liquid on top of the device to avoid liquids flowing into it.
- Do not press hard, vibrate violently, or soak the device.
- Perform the grounding work well to improve the anti-interference ability of the Device.

Table of Contents

Foreword ..... **I**
Important Safeguards and Warnings ..... **III**
1 Overview **6**
1.1 Introduction 6
1.2 Function 6
1.3 Feature 6
2 Structure **7**
2.1 Appearance 7
2.2 Port 9
3 Installation **11**
3.1 Checking List 11
3.2 Installation Requirements 12
3.3 Tools 13
3.4 Installation Procedures (Preinstall) 13
3.5 Installation Procedures 15
3.6 Alarm linkage with CCTV 16
4 WEB Configuration **17**
4.1 Device Initialization 17
4.2 WEB Interface Login 17
4.3 System Settings 17
4.4 Environment Monitoring 19
4.5 Network Configuration 19
4.6 User Management 20
4.7 System Log 20
4.8 System Status 21
5 FAQ **22**
Appendix 1 Cybersecurity Recommendations **23**

1 Overview

1.1 Introduction

Equipped with superior performance, the 6-Series EAS Radio-Frequency Transceiver Antenna has proven its advantages in detecting various RF labels and tags within its detection range. It has an excellent anti-interference capacity, which plays a significant part in preventing loss for various retailers. There are irreplaceable features such as sturdy and colorfast aluminum alloy material as well as minimalist design, which contributes to less maintenance and easy operation. The antenna is equipped with the network communication function. This function enables the device to connect to the network platform and supports the remote viewing of the device at any time.

1.2 Function

- Detection of RF tags & labels: Effectively detects and identifies the RF tags and labels within coverage.
- Sound and light alarm: When the RF tags or labels are detected, the loud alarm tone will be triggered, and the alarm indicator will turn from off to a red flashing light to remind. Multiple alarm tones and alarm volume levels are selectable.
- Alarm output: This function can be used with a CCTV module to synchronize the alarm signal to the monitoring camera, and the camera will record the alarm videos automatically for future reference.
- Network communication function: Supports web configuration, network platform connection, cloud service, remote configuration and more.

1.3 Feature

- Reading distance: Under the laboratory circumstance, the max distance of the tag is from 0.8 m to 0.9 m (RF Square TagT004W), the max distance of the label is from 0.7 m to 0.8 m (RF Label 4040).
- Stable hardware performance: The high-performance signal transmission driver works perfectly with the multi-level operational signal receiving structure, which has features as stable operation, no temperature drift, and no performance degradation in long-term use.
- Strong anti-interference ability: Equipped with a sensitivity adjustment function, it can effectively reduce the interference of environmental noise on the Device.
- Powerful signal processing capability: A unique receiving signal filtering algorithm ensures accurate identification of tag signals with an extremely low false alarm rate.
- Wide applicability: Compatible with most RF tags and labels.

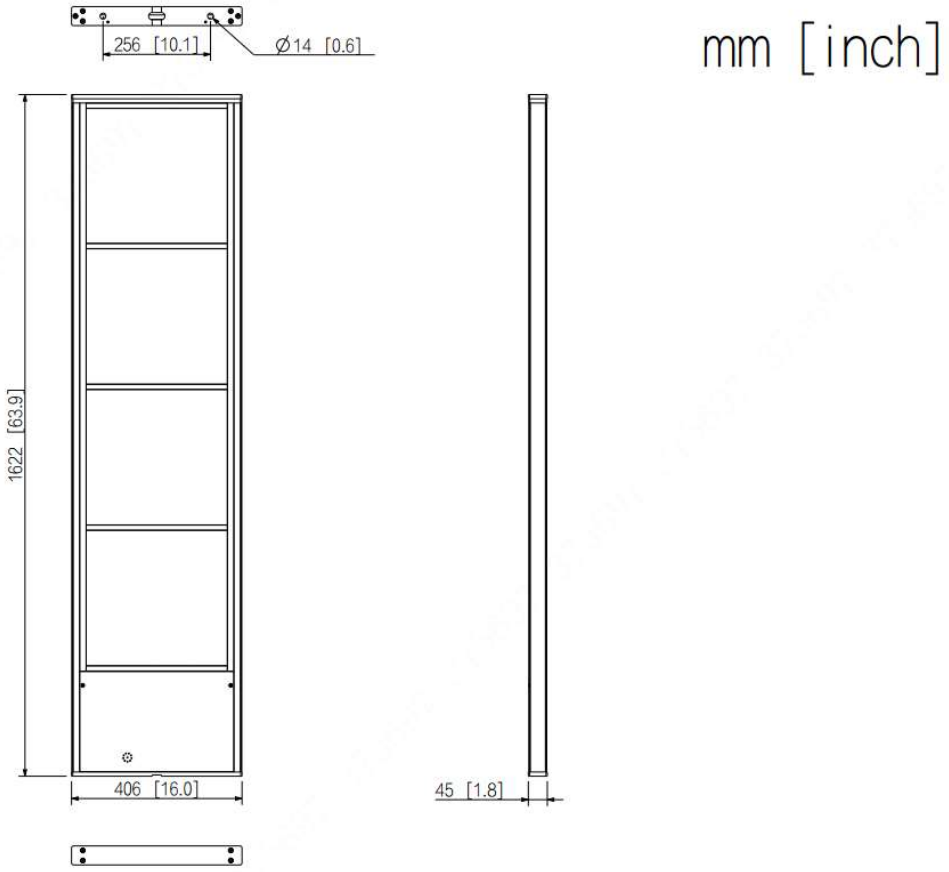
- Strong & Durable: Forged aluminum alloy material is beneficial for its excellent impact resistance. And it has features such as minimalist design, simple installation as well as easy configuration, which is suitable for all types of malls.

2 Structure

2.1 Appearance

Figure 2-1 Appearance

Figure 2-2 Product Dimensions (Unit: mm [inch])



2.2 Port

Figure 2-3 Ports of primary board descriptions

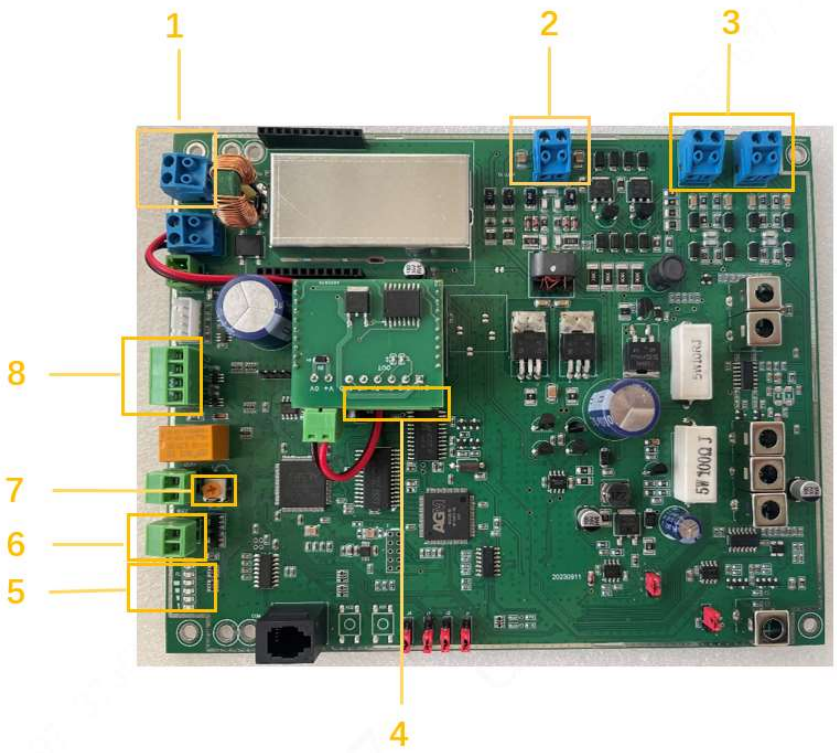


Table 2-1 Ports of primary board descriptions

No.	Name	Function
1	Power port	Primary board 24 VDC power input ⚠ Incorrect voltage input or wrong wiring may cause device damage!
2	TX antenna port	TX coil port for RF detection signals
3	RX antenna port	RX coil port for RF detection signals
4	Primary board communication port	For communicating with the network board
5	Environment status indicator	Used to display environmental interference. When 1-2 green indicators are on, the environment is good. When 3 green indicators are on, there is interference. When 4 green indicators are on, the environment is poor.
6	Buzzer port	For connecting buzzer
7	Buzzer volume adjustment knob	Adjust the volume: clockwise to decreases and counterclockwise to increase.
8	Alarm port	LED light strip port

Figure 2-4 Descriptions of network board ports

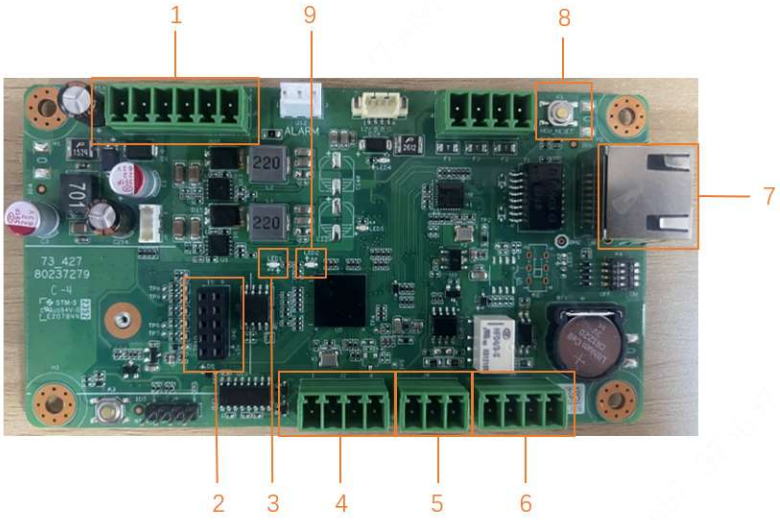


Table 2-2 Descriptions of network board ports

No.	Name	Function
1	Network board communication port	For communicating with the primary board.
2	Wi-Fi module port	Reserved Wi-Fi module port
3	Power indicator of the network board	The solid green indicator means the normal power supply of the network board.
4	RS232 port	For RS232 serial port communication
5	RS485 port	For RS485 serial port communication
6	Alarm output port	For camera linkage
7	RJ45 port	RJ45 network port
8	MCU-RESET button	For restoring to factory settings
9	System operating indicator of the network board	Flashes for 2 s, which indicates the system is normally working.

3 Installation

3.1 Checking List

After you receive the device from the forwarder, please open the box and check with the following sheet. If there is any problem, contact your local retailer or service engineer for help.

Table 3-1 Checklist

No.	Item		Description
1	Overall packing	Appearance	No obvious damage.
		Packaging	Not distorted or broken.
		Accessory	No missing.
2	Host	Appearance	No obvious damage.
		Model	Matches with the purchase order.
		Labels on the Device	Not torn up. Do not tear off or throw away the labels, otherwise the warranty services can be compromised. You need to provide the serial number of the Device when calling after-sales service.

Figure 3-1 Packing List

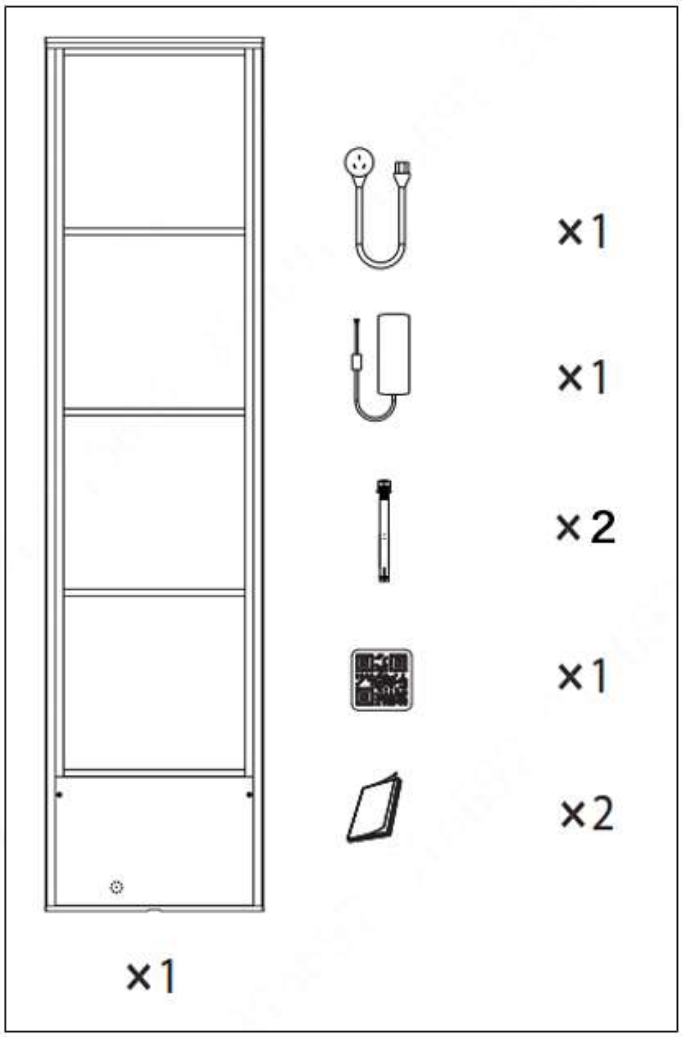


Table 3-2 Packing List

Name	Quantity
EAS Radio-Frequency Antenna	1
Power adapter	1
Power cord	1
M10×100 Expansion screw	2
QSG	1
Regulatory Guide	1
User's Manual QR code	1

3.2 Installation Requirements

- Keep away from static large metal items.
  Install the Device at least 100 cm away from a still or fixed large metal item. Otherwise, the detection distance will be affected.
- The floor where the device is installed must be flat and solid.
  Install the Device on the flat and solid floor, in order to prevent the equipment from shaking caused by vibrations when people step on the floor.
- Keep away from the EM interference source and the EM radiation source.
- Since the bilateral TX and RX technology is used in the antenna, the Device should be installed at least 200 cm away from the EM interference source and the EM radiation source to prevent false alarms.
- The Device must be strictly grounded.
  To ensure personal and Device safety, enhance Device anti-interference capability and improve detection distance, the Device needs to be reliably grounded in accordance with regulations.
- Keep the electric and electronic wirings separate.
- Electric and electronic are prone to mutual influence and cause safety problems, so the two wirings need to be separate.

  The following can be the EM interference source and the EM radiation source that affects the Device: Electric control cabinets, RF devices, computer and peripheral devices, video monitors, high-power motors, high-power transformers, AC wires, thyristor circuits (high-power switching power supply, inverter welding machines), engines, motored machines, and fluorescent lamp with conventional electronic ballast.

3.3 Tools

Table 3-3 Tools

Name	Image	Name	Image
Cross screwdriver and slotted screwdriver		M10×100 Expansion screw * 4 (included)	
Marker		Open-end wrench	
Cutting machine		Hammer	
Fine sand		Scuff plate	
Impact driver		-	-

3.4 Installation Procedures (Preinstall)

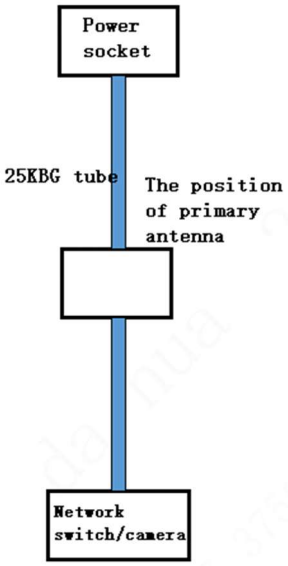
Step 1 86 cable boxes are reserved for each EAS antenna base. The distance between the cable boxes is adjusted according to the layout plan.

Step 2 Confirm the position of the EAS power socket, and then reserve a φ 25 cable tube or another cable of the same size between the 86 cable box from the primary antenna for the wiring between the EAS antenna and power supply.

Step 3 If the CCTV linkage function is required, an additional φ 25 cable tube or another cable of the same size needs to be embedded between the primary antenna and the camera in advance.

Step 4 If the device needs to be connected to an NVR or network platform, the cable tube with the same dimensions as above needs to be embedded between the host box and the switch.

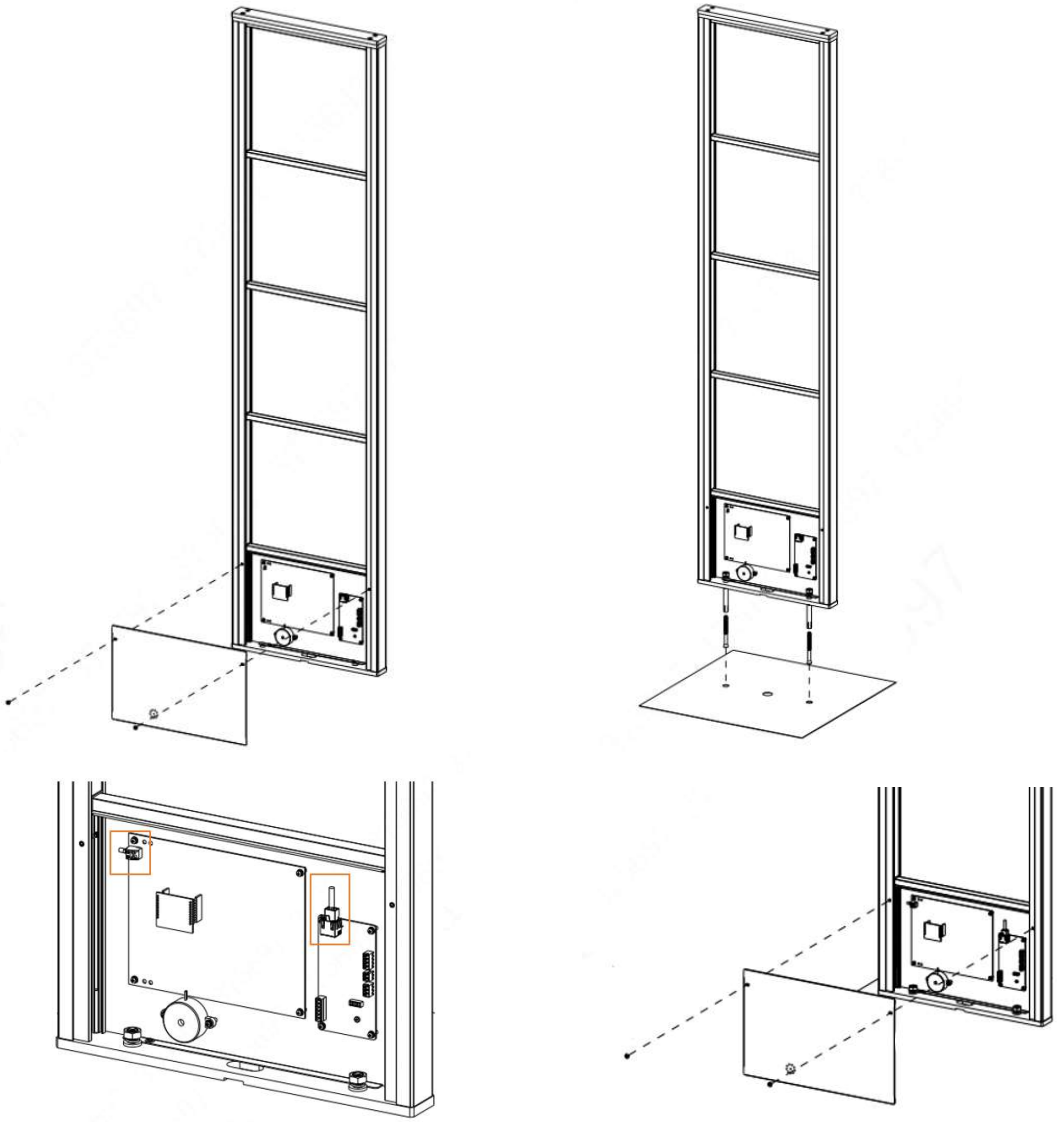
Figure 3-2 Description of the cable and tube reservation



Step 5 Embed expansion screws in advance according to the holes of the antenna base.

Step 6 Remove the cover plate, align the antenna with the pre-embedded screws, tighten the screws, and then insert the terminal blocks in the specified position.

Figure 3-3 Installation diagram

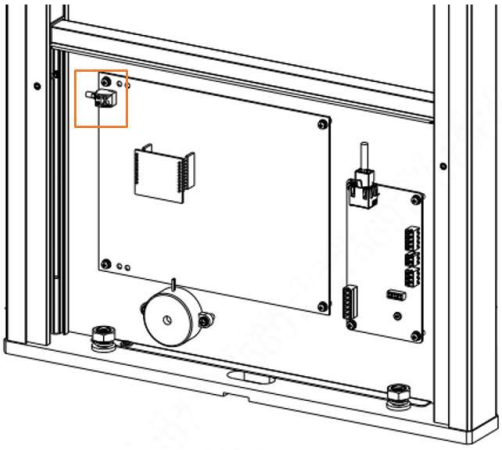


Step 7 Connect the power adapter to the power port of the primary board as shown in the following figure. And all the installation is completed.

⚠

The input voltage of the device is 100–240 VAC, 50/60 Hz. Incorrect voltage input or wrong cable connection may cause device damage.

Figure 3-4 External power cord



3.5 Installation Procedures

Step 1 After determining the installation location, use a marker to draw lines, punch holes, and cut grooves. Then clean up the site.

Figure 3-5 Installation 1

Step 2 Cover the cutting groove with fine sand to fill the gap and protect the cable. And install a stainless scuff plate to fix the device.

Figure 3-6 Installation 2

Step 3 Install a stainless scuff plate to fix the device. The device installation is complete.

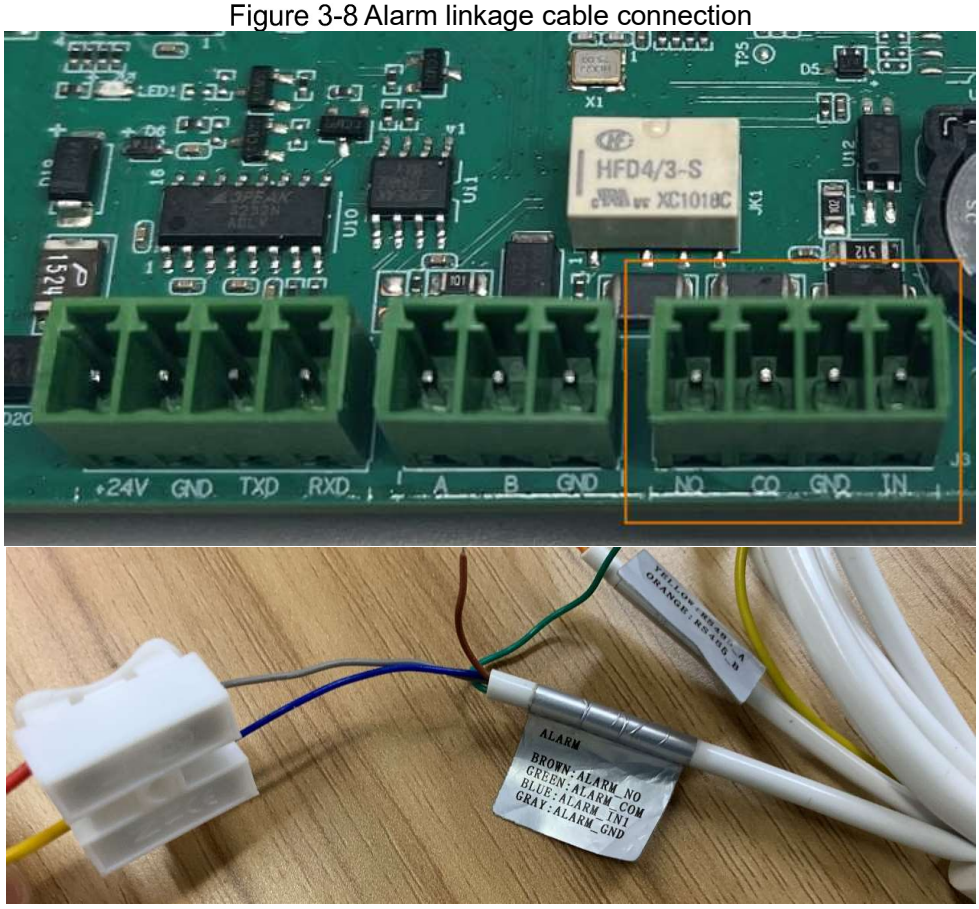
Figure 3-7 Installation 3

3.6 Alarm linkage with CCTV

Cable Connection

There is a 1-channel linkage alarm switch on the RX antenna primary board, from left to right:——NO, COM, GND and IN. Connect NO and COM to the alarm input ports ALARM_IN1 and ALARM_GND respectively in the camera ALARM port.

Figure 3-8 Alarm linkage cable connection



4 WEB Configuration

4.1 Device Initialization

When using the device for the first time or after restoring the factory configuration, device initialization is required (including setting the password of the device admin user, time zone and more).

- To ensure the security of the device, please keep the password of admin properly after the device initialization and change it regularly.
- When initializing the device, make sure the IP address of the PC is in the same network as the IP address of the Device.

Step 1 Open Chrome browser, enter the IP address of the Device in the address bar (the default IP address is 192.168.1.108) and press the **Enter** key.

Step 2 Set the time zone, time and date of the Device and click **Next**.

Step 3 Set the login password of admin, and click **OK**.

4.2 WEB Interface Login

Log in to the Device through the browser. Before logging in to the Device, make sure the following conditions are met.

- Log in to the Device WEB interface after completing the initialization of the Device.
- When logging in to the Device, make sure that the IP address of the PC and the IP address of the Device are in the same network segment.

Step 1 Open a browser, enter the Device IP address in the address bar, and then press the **Enter** key.

Step 2 Enter the user name and password.

- The default user name is admin.
- If you need to change the password, click **User Management** to reset the password.

4.3 System Settings

Configure the system settings, including TX strength, gain, threshold, anti-noise level and more.

Step 1 Select **System Settings** on the home page.

Step 2 Configure some parameters.

Figure 4-1 System Settings

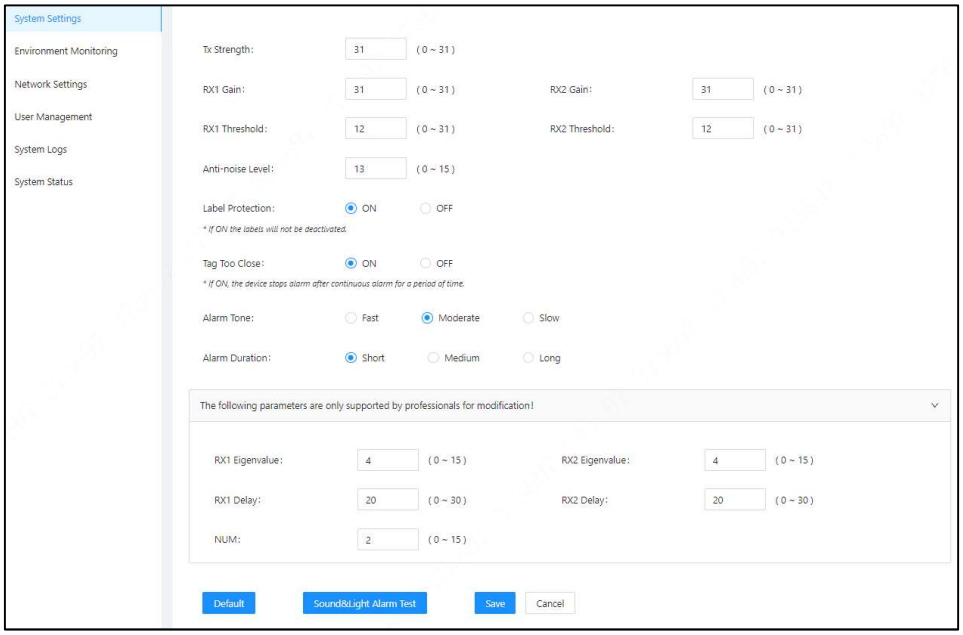


Table 4-1 Descriptions of system settings

Parameters	Descriptions
TX Strength	31 by default, 0-31 level adjustable. The lager the value, the longer the detection distance.
RX1 Gain	31 by default. 0-31 level adjustable. The larger the value, the better the reading effect.
RX2 Gain	31 by default. 0-31 level adjustable. The larger the value, the better the reading effect.
RX1 Threshold	12 by default. 0-31 level adjustable. The lower the value, the better the reading effect. However, when a lot of noise values are close to or exceed the threshold, the gain value should be increased.
RX2 Threshold	12 by default. 0-31 level adjustable. The lower the value, the better the reading effect. However, when a lot of noise values are close to or exceed the threshold, the gain value should be increased.
Anti-noise Level	13 by default. 0-15 level adjustable. The larger the value, the stronger the anti-noise capacity and the lower the detection effect.
Label Protection	On by default. If ON, the labels will not be deactivated. But when the label is too close to the antenna, it is still likely to be deactivated. The effect varies with different manufacturers.
Tag Too Close Alarm	On by default. If ON, the Device stops the alarm after continuous alarm for a while.
Alarm Tone	Quick by default. There are 3 modes for selection.
Alarm Duration	Short by default. There are 3 modes for selection.
RX1 Eigenvalue	4 by default. 0-15 level adjustable. In the case of false alarms, the increase of the value will reduce the false alarms to a certain extent.
RX2 Eigenvalue	4 by default. 0-15 level adjustable. In the case of false alarms, the increase of the value will reduce the false alarms to a certain extent.
RX1 Delay	20 by default. 0-30 level adjustable. In the case of false alarms, the increase of the value will reduce the false alarms to a certain extent.
RX2 Delay	20 by default. 0-30 level adjustable. In the case of false alarms, the increase of the value will reduce the false alarms to a certain extent.
NUM	2 by default. 0-15 level adjustable. When there are false alarms, add the value to reduce the false alarms.
Time Zone	Time zone selection
Time and Date	Time and date setting
Language	7 languages available: English, Portuguese, Spanish, German, French and Japanese, Italiano.

Step 3 Click **save**.

4.4 Environment Monitoring

In the environment monitoring interface, the operating frequency, alarm number, real-time signal and noise waveform changes of the equipment can be viewed.

Figure 4-2 Environment Monitoring

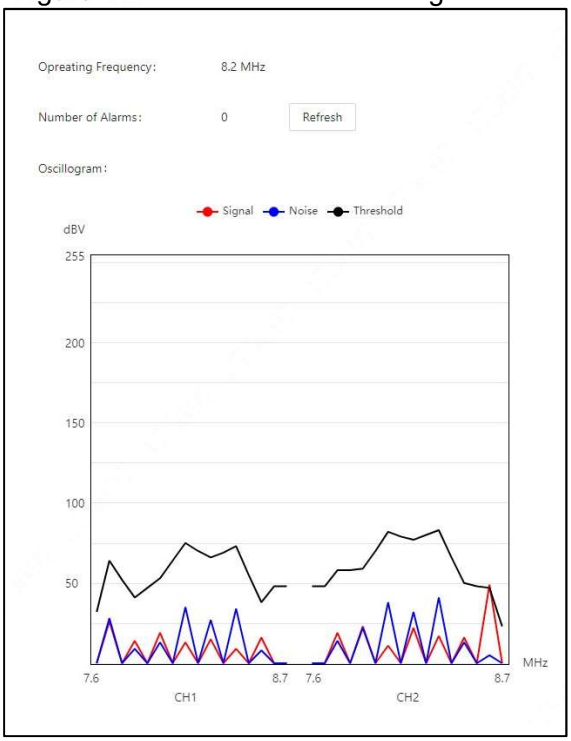


Table 4-2 Descriptions of environment monitoring parameters

Parameters	Descriptions
Operating Frequency	The operating frequency of the Device is 8.2MHz.
Number of Alarms	Refresh to view the latest number of alarms.
Oscillogram	The dynamic change of signal, noise and other parameters of the Device is displayed in real time.

4.5 Network Configuration

Select **Network Configuration** on the home page. Change the Device IP address, set the DNS server address and set the auto registration server address through network configuration.

Figure 4-3 Network Configuration

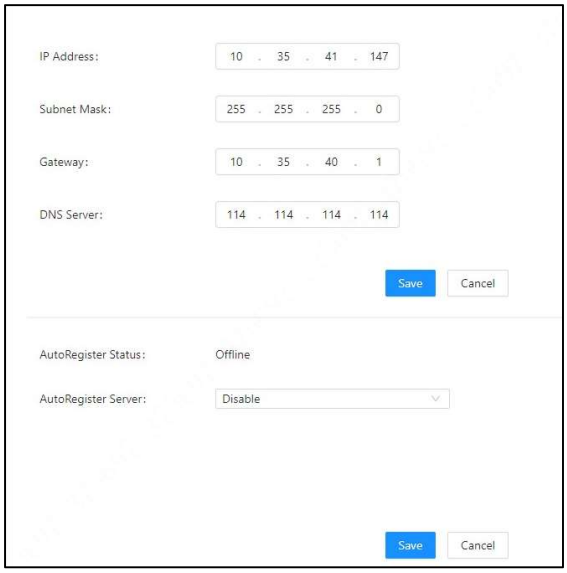


Table 4-3 Descriptions of network configuration parameters

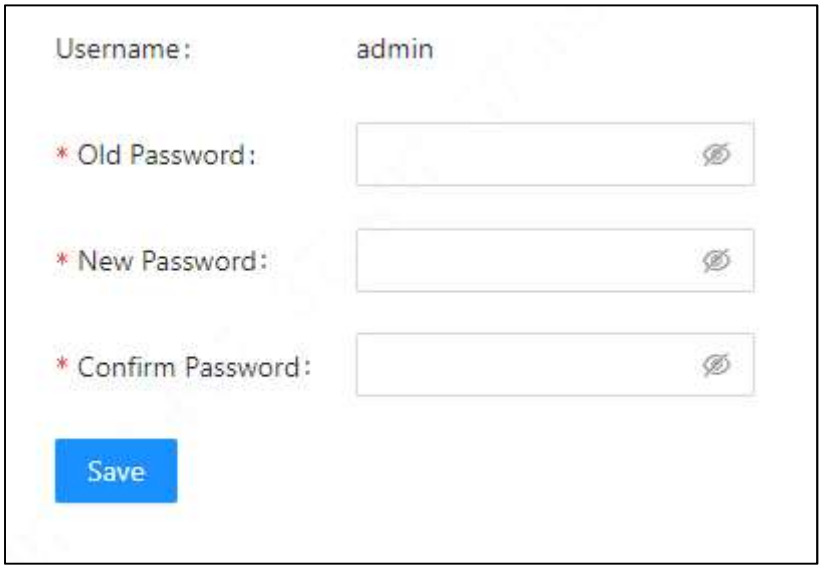
Parameters	Descriptions
IP address	The default IP address is 192.168.1.108, and the IP address can be changed.
Subnet mask	Set subnet mask
Gateway	Set the gateway
DNS server	Set the domain server address
Auto registration status	Auto registration status: Online/Offline
Auto registration server	Set the auto registration server address.
Diagnostic Type	Select the network diagnostic type.
Start	Start the diagnosis.
End	End the diagnosis.
Clear Data	Clear the diagnostic process data.

4.6 User Management

Reset the user password. Select **User Management** in the home page, then enter the old password and the new password, and click **Save**.

If you forget the old password, reset the password after restoring the factory settings on the Device.

Figure 4-4 Password Management



4.7 System Log

On the **System Log** interface, modification records of system configuration, alarm records and other information can be viewed.

Figure 4-5 System Log

4.8 System Status

Select **System status** on the home page to view the Device status which includes software version, web version, serial number and more information.

5 FAQ

1. **After the store is closed every day, an alarm is generated at night when no one is there.**
   - Reason: In order to ensure the normal detection performance of the EAS RF device when the store is open, it is usually debugged according to the business environment. At night, the interference of the ambient power supply at night is reduced, and then the detection performance of the Device is relatively improved. At this time, if there is an EAS RF label on the Device near the EAS RF antenna, an alarm will be generated.
   - Solution: We recommend you turn off the power of the EAS RF device during closing time.
2. **False alarms occur every few days and then disappear after a few days without debugging. The phenomenon reoccurs.**
   - Reason: Shopping malls regularly hold events, and the stage has temporary large electrical equipment, space and power interference, which leads to false alarms.
   - Resolution: Check the newly added electrical equipment during the false alarm period. After the interference source is determined by the elimination method, move the interference source away from the antenna.
3. **Irregular occasional false alarms.**
   - Reason 1: The clerk did not place the Device with the EAS RF label outside the detection range, which was too close to the EAS RF antenna, resulting in a false alarm.
   - Solution: Place devices with the EAS RF tag outside the detection range of the EAS RF antenna as required.
   - Reason 2: There is a similar coil near the EAS RF antenna to form a loop, and then generates the tag signal.
   - Solution: Check if there are coiled wires or closed rings of metal forming loops near the EAS RF antenna that generate label signals and cause false alarms.
   - Reason 3: The newly added electrical device in the store is near the EAS RF antenna, and spatial interference leads to false alarms.
   - Solution: Before adding a new electrical device near the EAS RF antenna, please temporarily power on the Device to test whether it will cause interference to the EAS RF antenna. Please contact the technician to confirm whether it can be installed.
4. **The label detection rate is low, and no alarm is sent through the antenna area.**
   - Check whether the power cable connection is correct.
   - Try to increase TX strength, gain and other parameters of the antenna.
   - Check whether the electric and electronic wiring are separate.
   - Shorten the distance between two devices.
   - Use a larger label.
   - Check whether the noise indicator is all on. If yes, eliminate surrounding noise interference.

Appendix 1 Cybersecurity Recommendations

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.