

Wide-body EAS AM Antenna

User's Manual








Foreword

General

This manual introduces the installation, functions and operations of the EAS AM 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 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.	May 2023

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 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



- Keep the detector away from dampness, dust or soot.
- Store the detector under the allowed humidity and temperature conditions.

Installation Requirements



- Do not place or install the detector in a place exposed to sunlight or near the heat source.
- Keep the detector installed horizontally on a stable place to prevent it from falling.
- Install the detector in a well-ventilated place, and do not block the ventilation of the detector.

Operation Requirements



- Do not drop or splash liquid onto the detector, and make sure that there is no object filled with liquid on the detector to prevent liquid from flowing into the detector.
- Operate the detector within the rated range of power input and output.
- Do not disassemble the detector.
- Use the detector under the allowed humidity and temperature conditions.

Maintenance Requirements



- Use the battery of specified manufacturer. When replacing battery, make sure that the same type is used. Improper battery use might result in fire, explosion, or inflammation.
- Use the recommended power cables in the region and conform to the rated power specification.
- Use the power adapter provided with the detector; otherwise, it might result in people

injury and device damage.



- **Use power supply that meets ES1 but does not exceed PS2 limits defined in IEC 62368-1. For specific power supply requirements, refer to device labels.**
- **Connect the detector (I-type structure) to the power socket with protective earthing.**
- **The appliance coupler is a disconnection device. Keep the angle for easy operation.**

Table of Contents

Foreword	I
Important Safeguards and Warnings	III
1 Product Information	1
1.1 Overview	1
1.2 Product Functions	1
1.3 Product Features	1
2 Product Structure	3
2.1 Product Appearance	3
2.2 Port Description	5
3 Installation	8
3.1 Out-of-box Checking	8
3.2 Installation Requirements	9
3.3 Tools	9
3.4 Installation Procedure (Preinstall)	10
3.5 Installation Procedure	12
3.6 Alarm linkage with CCTV	14
4 Device Debugging	17
4.1 System Parameter Configuration	17
4.1.1 Home Page	17
4.1.2 Main Menu	17
4.1.3 Alarm Tone	18
4.1.4 Alarm Volume	19
4.1.5 Alarm Mode	19
4.1.6 Alarm Threshold	19
4.1.7 Signal Gain	20
4.1.8 False Alarm Monitoring	20
4.1.9 Parameter Monitoring	20
4.1.10 TX Switch/RX Switch	21
4.1.11 Phase Sync/Phase Adjustment	21
4.1.12 Tag Too Close	22
4.1.13 Jammer Reminder	22
4.1.14 System Settings	22
5 Configuration on the Webpage	27
5.1 Initial Settings	27
5.2 Login	27
5.3 System Settings	27
5.4 Environment Monitoring	29
5.4.1 Parameter Monitoring	29
5.4.2 False Alarm Monitoring	30
5.5 Phase Synchronism	30
5.6 Eco Mode	31
5.7 Network Settings	31
5.8 System Log	31
5.9 User Management	32

5.10 System Status32

6 FAQ 33

Appendix 1 Cybersecurity Recommendations34

1 Product Information

1.1 Overview

Wide-body Network EAS AM Antenna is an anti-theft device that can effectively identify the anti-theft AM tags, which has higher detection performance than standard version. The Device can effectively prevent the theft of goods, cut business operating costs, and improve customer's shopping experience. The Device has a simple and elegant appearance with powerful performance and complete functions, which is an important part of the retail loss prevention system. It has network communication function, which enables the antenna connect to the network platform at any time to remotely configure and get equipment operating status.

1.2 Product Functions

- **Anti-theft label detection:** The Device can effectively detect and identify AM anti-theft labels within the coverage range.
- **Sound and light alarm:** When the label is detected, the Device will give off alarms and flashing lights. The Device supports a variety of adjustable alarm tone effects with adjustable volume.
- **Phase synchronism:** The Device supports one-click automatic synchronization of surrounding phases, which can effectively avoid interference from the other AM EAS devices around.
- **CCTV linkage:** The standard CCTV module can output the alarm signal to the monitoring camera, and then the camera can automatically save the video at the alarm time for future use.
- **On-board configuration system:** The mainboard has built-in on-board buttons and screens, which can directly configure related parameters on the device without connecting to a computer.
- **Supports auto-adjustment of sensitivity,** suitable for various environments.
- **Supports WEB login on LAN and device parameter configuration.**
- **Network communication function,** which enables the antenna connect to the network platform at any time to remote configure and get equipment operating status.

1.3 Product Features

- **Long detection distance:** The maximum detection distance of double-antenna labels is 1.8 m to 2 m, and the maximum detection distance of tags is 2 m to 2.4 m (depending on the environment).
- **Stable hardware performance:** The high-performance signal transmission driver cooperates with the multistage amplifier, which has stable operation with no temperature drift. It can be used for a long time without performance degradation.

- **Strong anti-interference ability:** The Device has a variety of sensitivity adjustment methods that can effectively resist the interference of environmental noise on the device.
- **Strong signal processing capability:** The unique received signal filtering algorithm ensures accurate identification of label signals with low false alarm rate.
- **Integrated transceiver design:** The primary and replica antenna are both integrated transceivers, and can be used flexibly. The detection effects of the primary and replica antenna are the same.
- **Wide application:** Compatible with most AM labels and tags.
- **Supports remote real-time configuration and device operating records acquiring.**
- **Power saving and environmental protection:** The Device is harmless to the human body. Support setting energy saving mode during non-business hours, in line with ROHS standards.

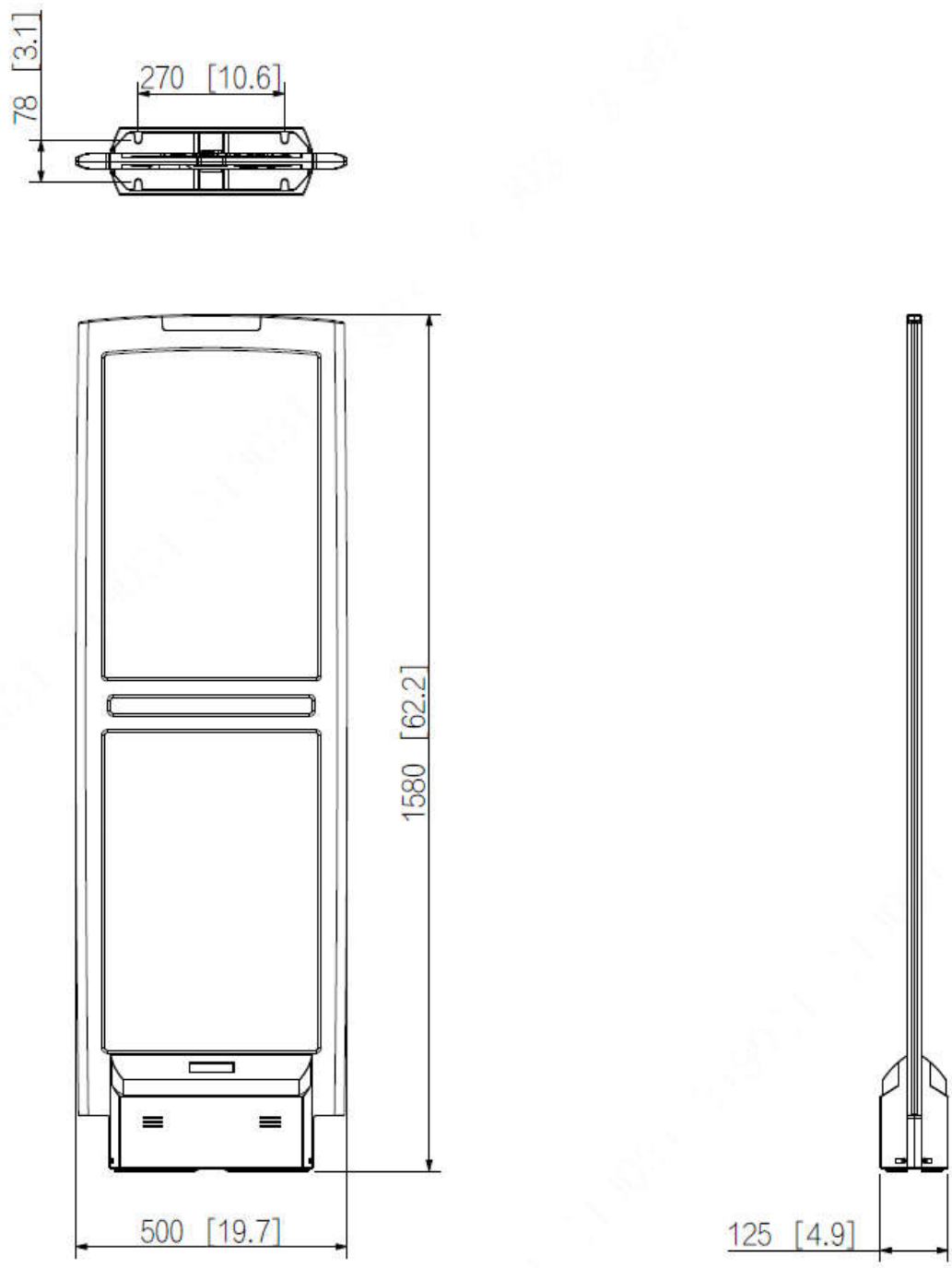
2 Product Structure

2.1 Product Appearance

Figure 2-1 Product appearance



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



2.2 Port Description

Figure 2-3 Primary antenna ports

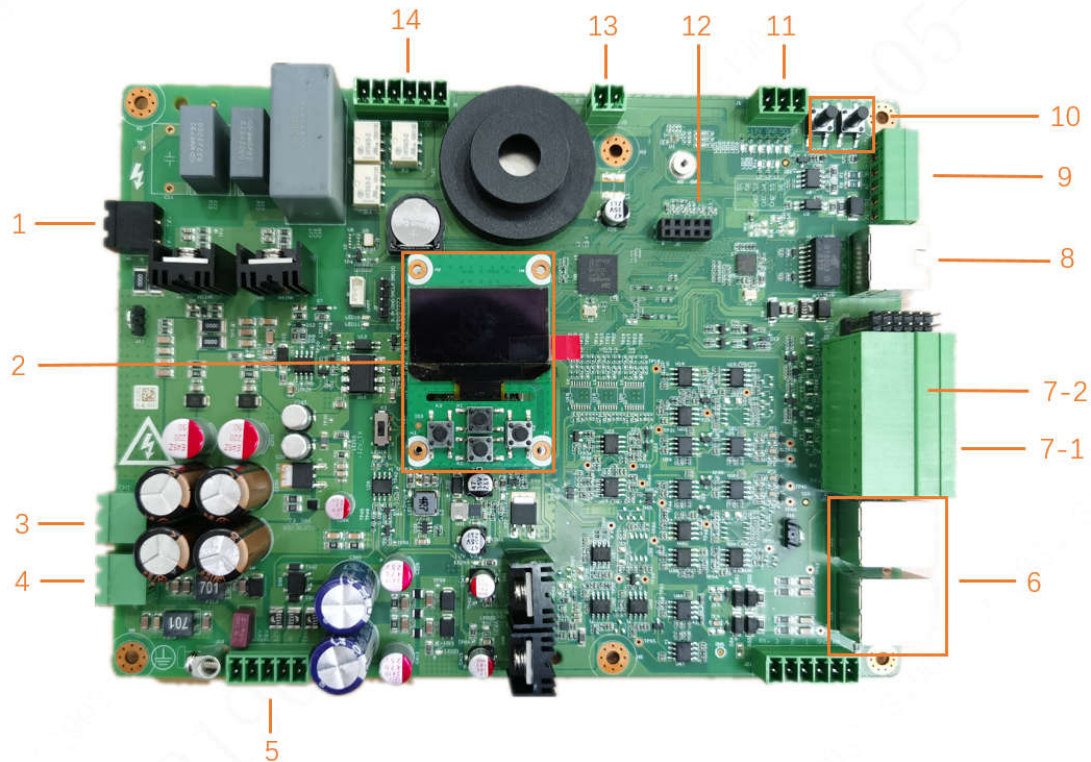







Table 2-1 Primary antenna ports description

No.	Parameter	Function
1	Transmitting antenna port	EAS active detection signal transmitting coil port.
2	Screen buttons for system parameter configuration	Screen buttons for system parameter configuration. For example,  ,  ,  ,  .
3	Replica antenna CH2 power port	Replica antenna CH2 power output (24 VAC).
4	Replica antenna CH3 power port	Replica antenna CH3 power output (24 VAC).
5	Primary antenna power port	Inputs 24 VAC or 12 VAC power to the primary antenna.  Incorrect voltage input or cable connection may cause device damage.
6	Receiving antenna port	EAS signal receiving coil port.
7-1	Replica antenna CH2 communication cable port	Replica antenna CH2 communication cable port (bottom interface).
7-2	Replica antenna CH3 communication cable port	Replica antenna CH3 communication cable port (top interface)
8	Network communication port	Network communication
9	Standby communication interface	Standby communication interface

No.	Parameter	Function
10	Reset button	The WIFI configuration reset button is on the left, and the system reset button is on the right.
11	LED light board port	LED light board port
12	WIFI module port	Optional WIFI module port
13	Buzzer port	A port for connecting to the standby buzzer.
14	CCTV linkage port	CCTV linkage port, 3-channel alarm relay output.

Figure 2-4 Replica antenna ports

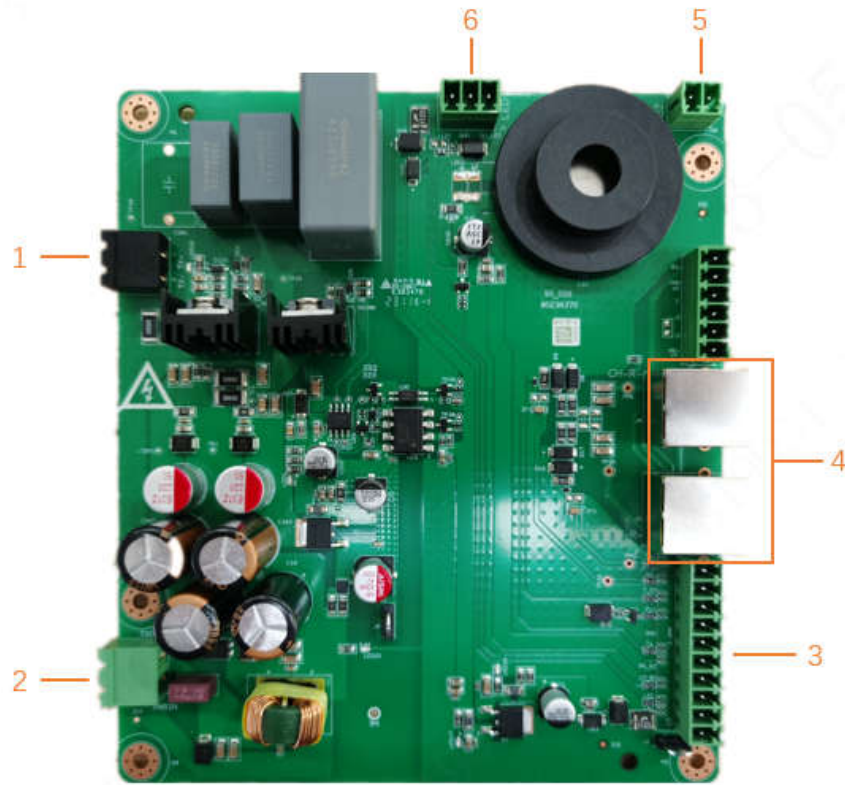


Table 2-2 Replica antenna ports description



No.	Parameter	Function
1	Transmitting antenna port	EAS active detection signal transmitting coil port.
2	Replica antenna power port	Replica antenna power input (24 VAC).  Incorrect voltage input or cable connection may cause device damage.
3	Replica antenna communication cable port	Replica antenna communication cable port.
4	Receiving antenna port	EAS signal receiving coil port.
5	Standby buzzer port	Connects standby buzzer.
6	LED light board port	LED light board port.

Figure 2-5 Power filter board ports



Table 2-3 Power filter board ports description

No.	Parameter	Function
1	AC power cable inlet	<p>External power input (220 VAC)</p> <p></p> <p>The input voltage of the antenna is 220 VAC 50/60Hz. Incorrect voltage input or cable connection may cause device damage.</p>
2	Ac power outlet	The external power is output after filtering.

3 Installation

3.1 Out-of-box Checking

After you received 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


Sequence	Item		Content
1	Overall packing	Appearance	No obvious damage.
		Packing	Not distorted or broken.
		Component	No missing.
2	Host	Appearance	No obvious damage.
		Device 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 3-2 Primary antenna packing list (left) and replica antenna packing list (right)

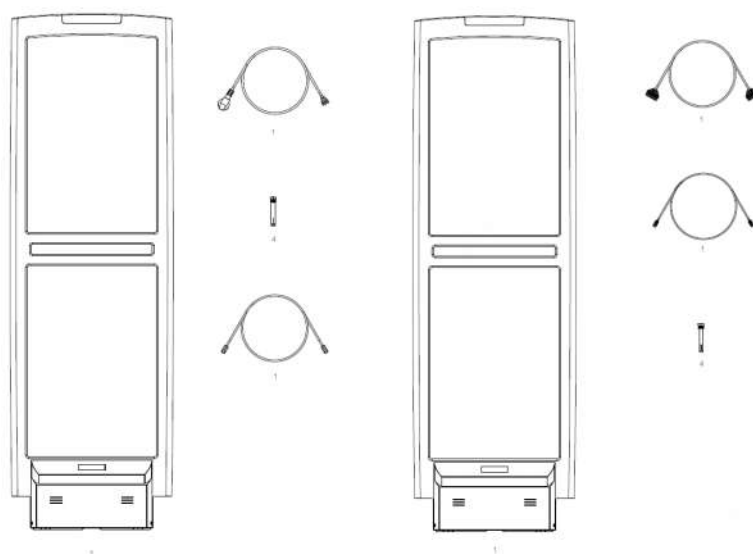


Table 3-2 Primary antenna packing list

Name	Quantity
Primary antenna	1
M10×100 expansion screw	4
Power cord	1
Network cable	1

Table 3-3 Replica antenna packing list

Name	Quantity
Replica antenna	1
M10×100 expansion screw	4
10PIN communication cable between primary antenna and replica antenna	1
2PIN replica antenna power cable	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 EM interference source and the EM radiation source.
Since the bilateral sending and receiving technology are 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.
- If there is any EAS label deactivator around the antenna, the phase sync is required to avoid false alarms.




The following can be the EM interference source and the EM radiation source that affect 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 3-4 Tools

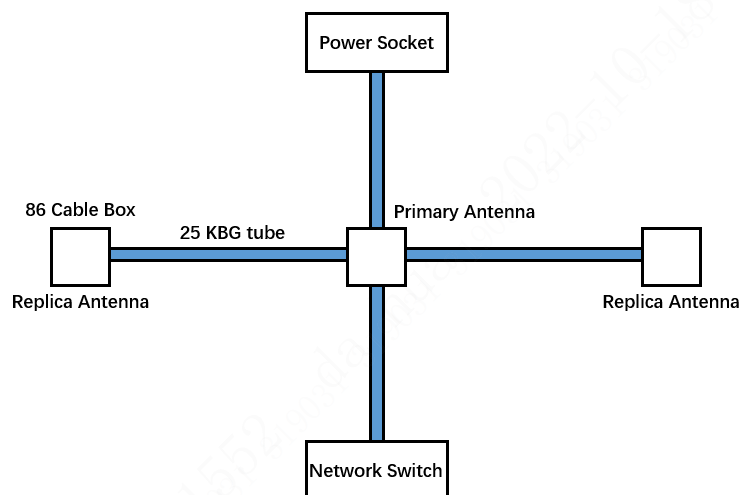
Name	Image	Name	Image
Crosshead screwdriver, slotted screwdriver		M10 × 100 expansion screws × 4 (standard accessories)	
Marker		Open-end wrench	
Cutting machine		Hammer	
Fine sand		Stainless scuff plate	

Name	Image	Name	Image
Electric drill		—	—

3.4 Installation Procedure (Preinstall)

- Step 1** 86mm square cable boxes are reserved for each EAS antenna base. The distance between the cable boxes is adjusted according to the layout plan. Two ϕ 25 cable tubes or other cables of the same size are reserved between each cable box for routing EAS antenna between the primary antenna and replica antenna.
- 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 routing EAS antenna between the primary antenna and replica antenna.
- Step 3** If the network or CCTV linkage function is required, an additional ϕ 25 cable tube or another cable of the same size needs to be embedded between the host and the network switch or camera in advance.

Figure 3-3 Description of the cable and tube reservation



- Step 4** Embed expansion screws in advance according to the holes of the antenna base.
- Step 5** Remove the terminal of the connecting cable, and then thread the connecting cable and power cable into the cable tube. When threading, you need to remove the terminal, and then cut the cable length according to the actual situation.
- Install the primary antenna and replica antenna terminals in the sequence of 1 white, 2 green, 3 brown, 4 red, 5 black, 6 blue, 7 gray, 8 orange, 9 yellow, and 10 purple, and then install the replica antenna power cable terminals in the sequence of 1 black and 2 brown.



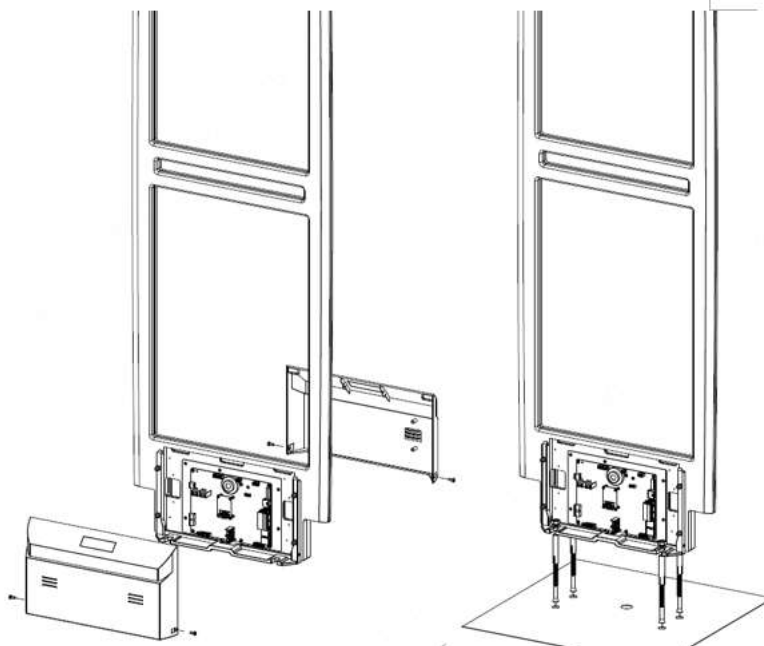
The cable sequence of the terminals on both sides must be in one-to-one correspondence, otherwise the Device may be damaged and short circuit may occur.

Figure 3-4 Primary antenna and replica antenna terminals (left)/Replica antenna power cable (right)

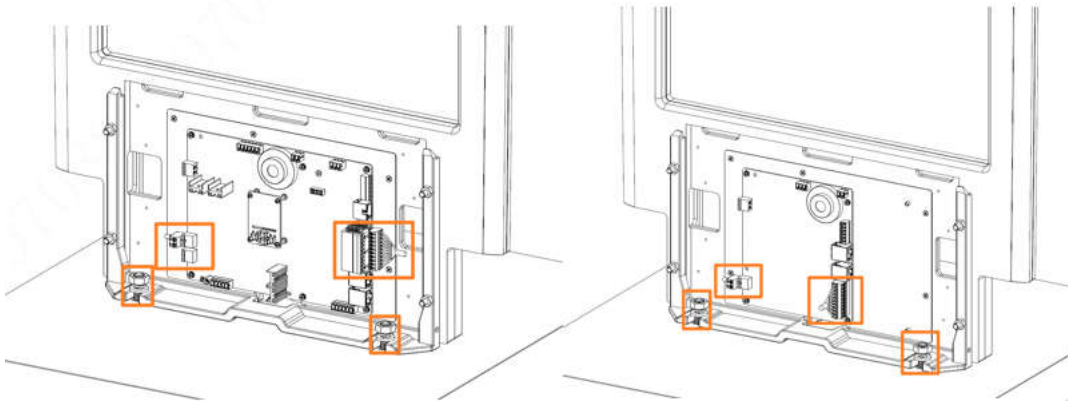


Step 6 Remove the cover plate, align the antenna with the pre-embedded screws, tighten the screws, and then insert the cable terminal in the specified position.

Figure 3-5 Installation diagram (1)



**Figure 3-6 Installation diagram
(2)**

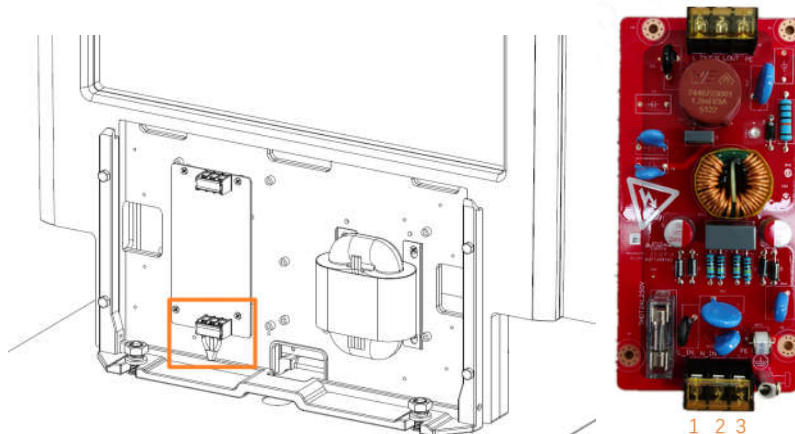


Step 7 See Figure 3-6, Connect to the power cable according to the following wiring order: 1. live wire (L), 2. neutral wire (N) and 3. protecting earthing cable(PE).



Input voltage of the Device is 220 VAC 50/60Hz. Please confirm whether the Device is suitable for local voltage and ask a professional electrician to operate during the installation. Incorrect voltage input or cable connection may cause device damage.

Figure 3-7 External power supply cable diagram



3.5 Installation Procedure

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

Figure 3-8 Installation (1)



Step 2 Cover the cutting groove with fine sand to fill the gap and protect the cable.

Figure 3-9 Installation (2)



Step 3 Install stainless scuff plate to fix the device.

Figure 3-10 Installation (3)

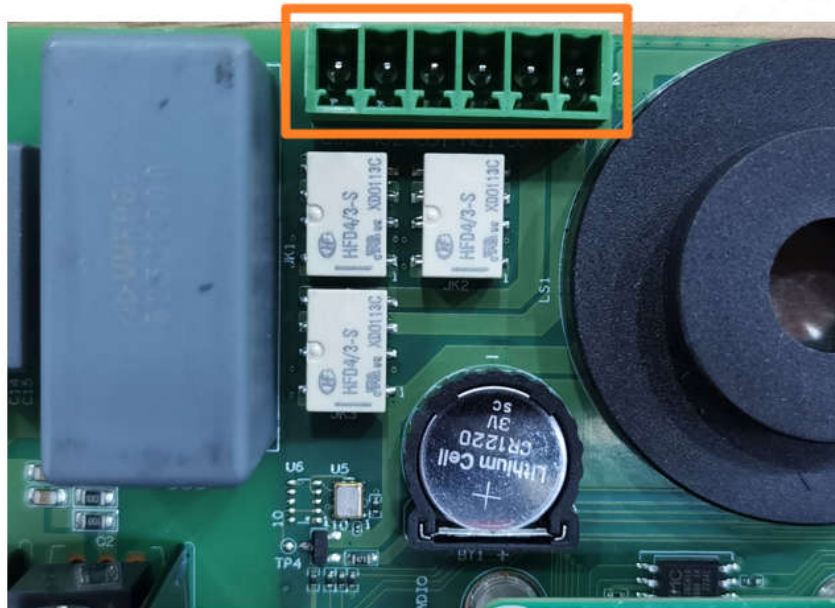


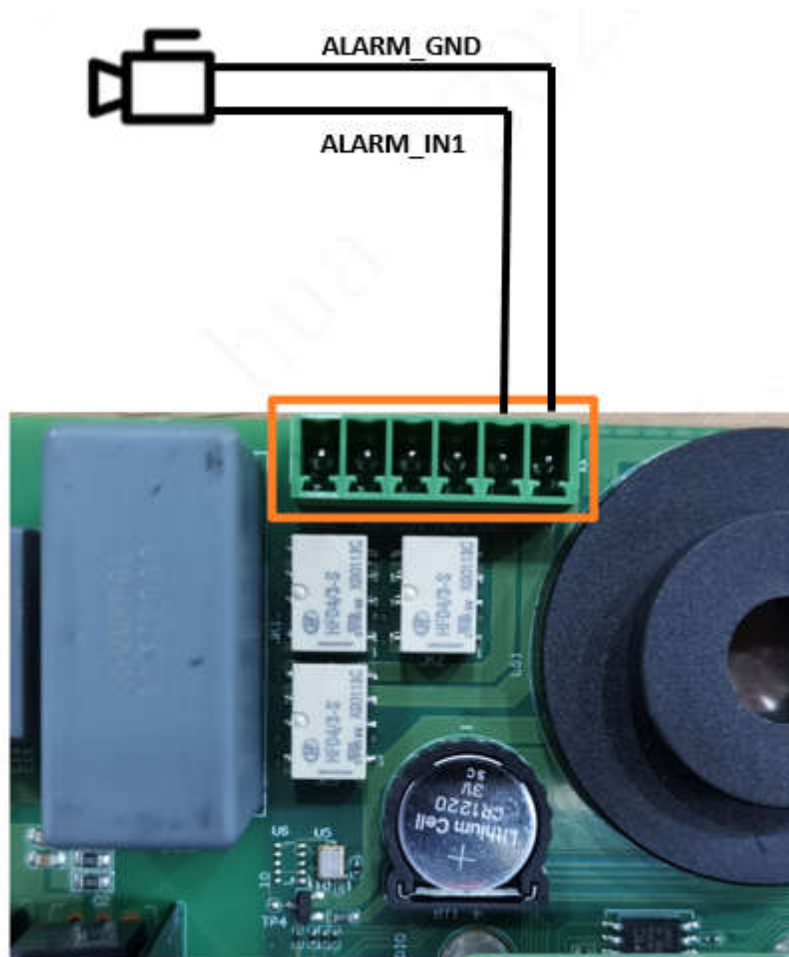
3.6 Alarm linkage with CCTV

Cable Connection

There are 3 linkage alarm switches on the EAS main board, from left to right: COM2,NO2;; COM1,NO1;; COM0,NO0, Take channel 1 as an example: connect NO0 and COM0 to the two alarm input ports of ALARM IN1 and ALARM GND in the ALARM port of the camera respectively.

Figure 3-11 Alarm linkage cable connection





IPC Configuration

Log in to the web page of the IPC device and then select Setting > Event Management > Alarm Setting > Alarm Linkage.

The sensor type needs to be NO. On this page, you can enable alarm linkage, configure whether to record, capture pictures, linkage alarm tone and more.

Figure 3-12 IPC Configuration

The image shows a web-based configuration interface for an IPC (Intrusion Prevention Control) system. On the left is a dark sidebar with a menu of categories: Camera, Network, Peripheral, Smart Thermal, Event, Video Detection, Audio Detection, Temperature Alarm, Alarm (highlighted in orange), Blackbody abnormal ..., Abnormality, Temperature, Storage, System, and Information. The main area is titled 'Alarm' and contains various settings. At the top, there is an 'Enable' checkbox. Below it is a 'Relay-in' dropdown menu set to 'Alarm1'. A 'Period' button is next to it. The 'Anti-Dither' field is set to '0' with a unit of 's (0~100)'. The 'Sensor Type' dropdown is set to 'NO'. The 'Record' checkbox is checked, with a 'Record Delay' of '10' s (10~300). The 'Relay-out' checkbox is also checked, with an 'Alarm Delay' of '3' s (2~300). Below these are checkboxes for 'Send Email', 'PTZ', and 'Audio Linkage'. The 'Play Count' is set to '5' (1~15), and the 'File' dropdown is set to 'alarm1.pcr'. The 'White Light' checkbox is unchecked. Its 'Mode' dropdown is set to 'Flicker', 'Flicker Frequency' is 'Medium', and 'Duration' is '10' s (5~30). There is a 'Period' button for the White Light section. The 'Snapshot' checkbox is unchecked, with a 'Period' button and a '1' '2' selector. At the bottom are 'Default', 'Refresh', and 'Save' buttons.

Alarm

☐ Enable

Relay-in: Alarm1

Period: Setting

Anti-Dither: 0 s (0~100) Sensor Type: NO

☒ Record

Record Delay: 10 s (10~300)

☒ Relay-out

Alarm Delay: 3 s (2~300)

☐ Send Email

☐ PTZ

☐ Audio Linkage

Play Count: 5 (1~15)

File: alarm1.pcr

☐ White Light

Mode: Flicker

Flicker Frequency: Medium

Duration: 10 s (5~30)

Period: Setting

☐ Snapshot

1 2

Default Refresh Save

4 Device Debugging

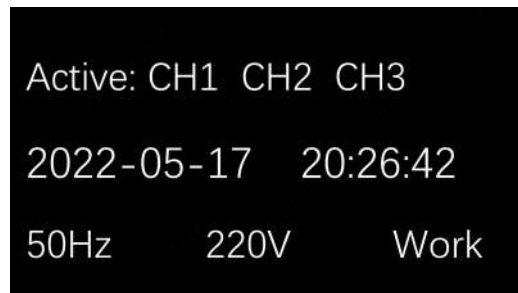
4.1 System Parameter Configuration

4.1.1 Home Page

The home page includes the current active channel, the system time and the current mains voltage and frequency.

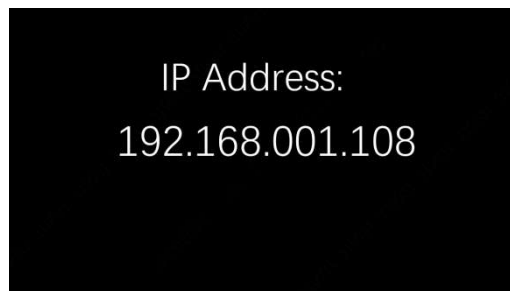
Press  and  simultaneously for 3 seconds to enter the main menu.

Figure 4-1 Home page



Press  to view the local IP address. Press  to return to the home page.

Figure 4-2 Local IP address



4.1.2 Main Menu

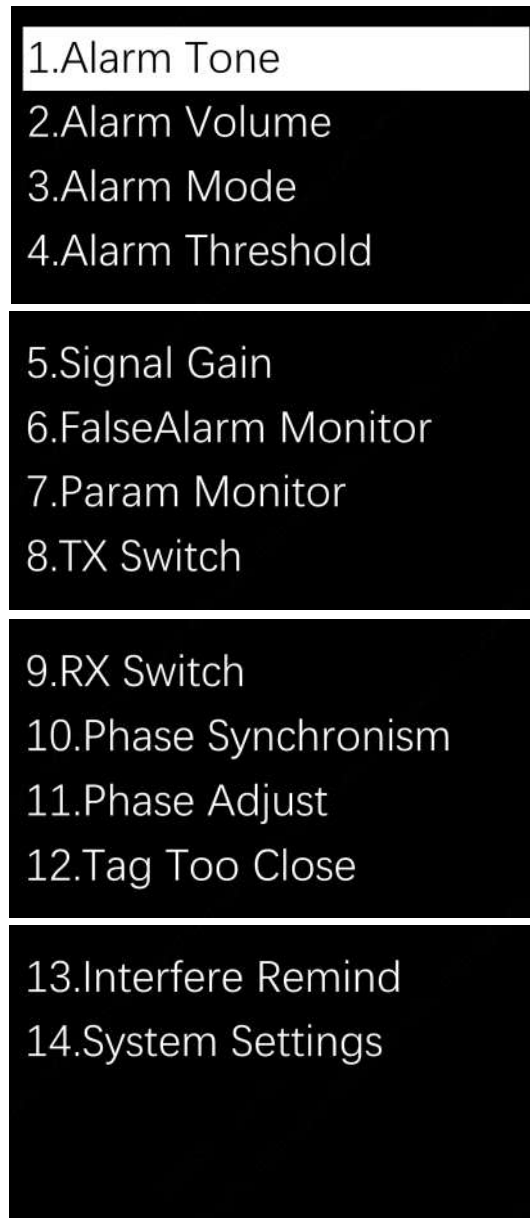
The main menu includes all parameters configuration entries.

Press  or  to move the cursor. Press  to enter the sub-menu. Press  to return to the home page.



The interference reminder function is temporarily unavailable.

Figure 4-3 Main Menu

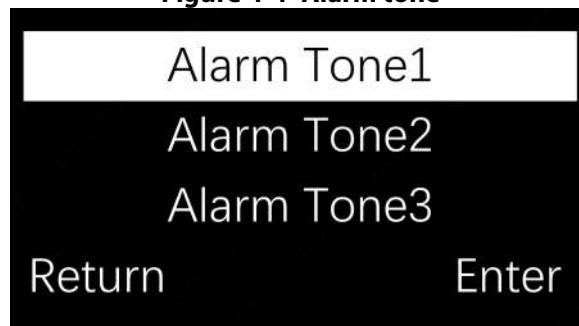


4.1.3 Alarm Tone

The system has 3 built-in alarm tones.

Press  or  to move the cursor. Press  to confirm the alarm tone. Press  to return to the main menu.

Figure 4-4 Alarm tone



4.1.4 Alarm Volume

The system alarm volume is adjustable in 5 levels.





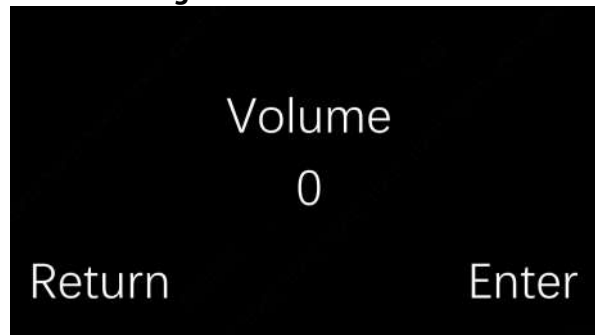
Press   to adjust the volume. Press  to confirm the volume. Press  to return to the main menu.

Figure 4-5 Alarm volume



4.1.5 Alarm Mode

The system includes 2 alarm modes to be used in different interference environments. Alarm mode 1 automatically adjusts parameters in real time according to the field environment to avoid false alarms. Alarm mode 2 collects environmental parameters for a period of time to avoid false alarms (this process takes about 15s).





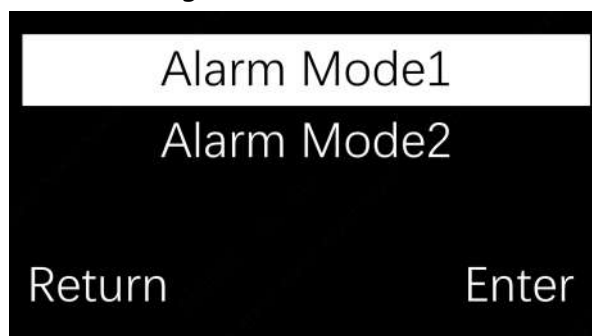
Press  or  to move the cursor to select the alarm mode. Press  to confirm the alarm mode. Press  to return to the main menu.

Figure 4-6 Alarm mode



4.1.6 Alarm Threshold

By setting the alarm threshold of each channel, the antenna detection distance can be effectively adjusted and false alarms can be reduced. The adjustment range of Signal/Noise ratio (SNR) is 0-50, and the adjustment range of Root Mean Square (RMS) is 0-1500. The lower the value of the two parameters, the farther the detection distance but the higher the risk of false alarms. The above parameters can be adjusted according to the data of parameter monitoring (For details, see 4.1.9.). The adjustment range of the Number of Alarm reviews (NUM) is 0-10, which is used to improve the accuracy of label recognition. The lower the value, the easier it is to trigger the alarms, but the higher the risk of false alarms, which can be appropriately adjusted according to the false alarm monitoring data (see 4.1.8). The Param Sync function can copy the parameters of one channel to other channels.

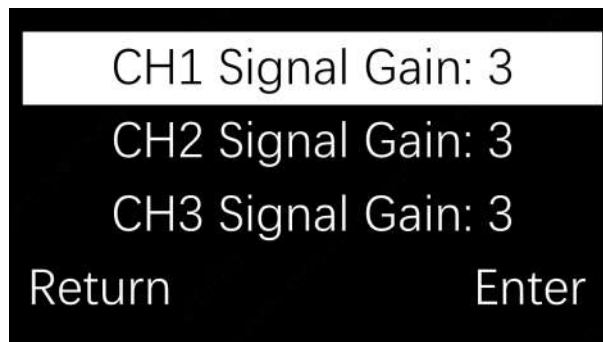
Figure 4-7 Alarm threshold



4.1.7 Signal Gain

It is not recommended to change the default value of this parameter without the professional personnel.

Figure 4-8 Signal gain



4.1.8 False Alarm Monitoring

False alarm monitoring displays the number of suspected false alarms of 3 channels since entering the function interface in real time, which is used for on-site troubleshooting of false alarms and test acceptance after device installation. If the number of false alarms increases significantly within a short period of time, increase the value of alarm review number (NUM) of the corresponding channel (see 4.1.6) to reduce false alarms.

Press  to return to the main menu.

Figure 4-9 False alarm monitoring

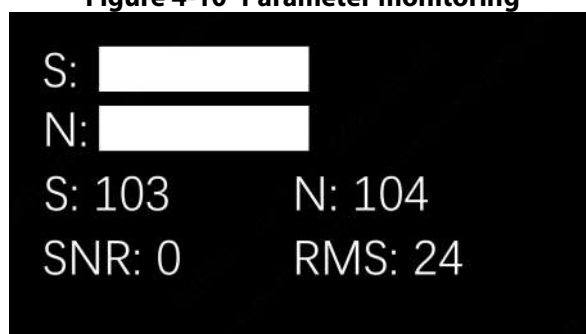


4.1.9 Parameter Monitoring

The parameter monitoring displays the SNR (Signal/Noise ratio) bar graph, SNR and RMS parameters in real time. Press  and  to select the channel. If the channel is not connected or the receiving is closed. You can set the threshold by observing the parameter change of the EAS label/tag when it passes through the antenna (see 4.1.6).








Press  to return to the main menu.

Figure 4-10 Parameter monitoring



4.1.10 TX Switch/RX Switch

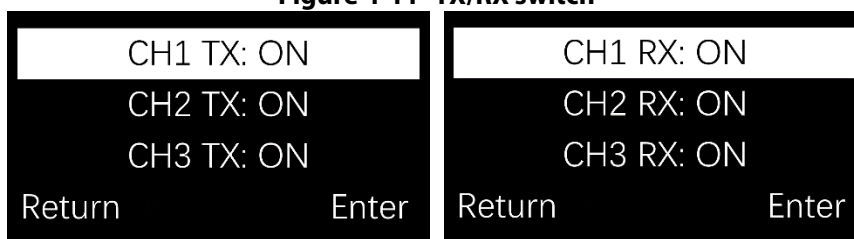
The TX/RX antenna can be switched on and off in the menu, and the transmitter/receiver of the specified channel can be temporarily turned off during the configuration process.

Press  and  to move the cursor to select the channel. After pressing  to confirm the channel, you can press  and  to select the switch. Press  to confirm the switch. Press  to return to the main menu.



Turning off the transmitter or receiver will cause the alarm function failure.

Figure 4-11 TX/RX switch



4.1.11 Phase Sync/Phase Adjustment

Phase synchronism can synchronize the transmission timing between the device and other brands of EAS systems to avoid false alarms due to timing inconsistencies. You can select Rising Edge or Falling Edge synchronization in the menu. After startup, the device enters the automatic Phase synchronism state. In this state, the system cannot detect tags/labels and will last for 5-20 seconds.









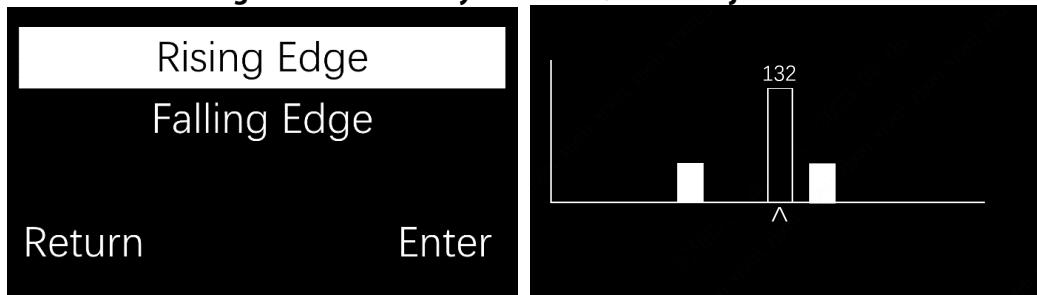
Press  and  to select synchronization method. Press  to confirm, and then the system will automatically synchronize with the same type of nearby signals. Press  to return to the main menu. If auto Phase synchronism is unsuccessful, press  and  in Phase Adjustment interface to manually change the current phase. And press  to enter the Saving interface, and press  to confirm.

Figure 4-12 Phase synchronism/Phase Adjustment



4.1.12 Tag Too Close

When this function is enabled, if a tag/label stays in the antenna detection area for a long time (≥ 2 minutes), the device will use the flashing light instead of the alarm tone to remind. After entering the flash light mode, and no continuous alarm is detected for more than 3 seconds, it will restore to the normal alarm state. Tag too close alarms can be reported to the platform.

Press and to select on and off.

Press to confirm. Press to return to the main menu.

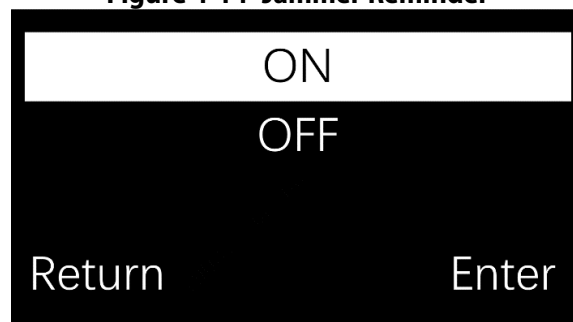
Figure 4-13 Tag too close



4.1.13 Jammer Reminder

When it is detected out any jammers nearby, the jammer reminder will be triggered. (This function is not available now.)

Figure 4-14 Jammer Reminder



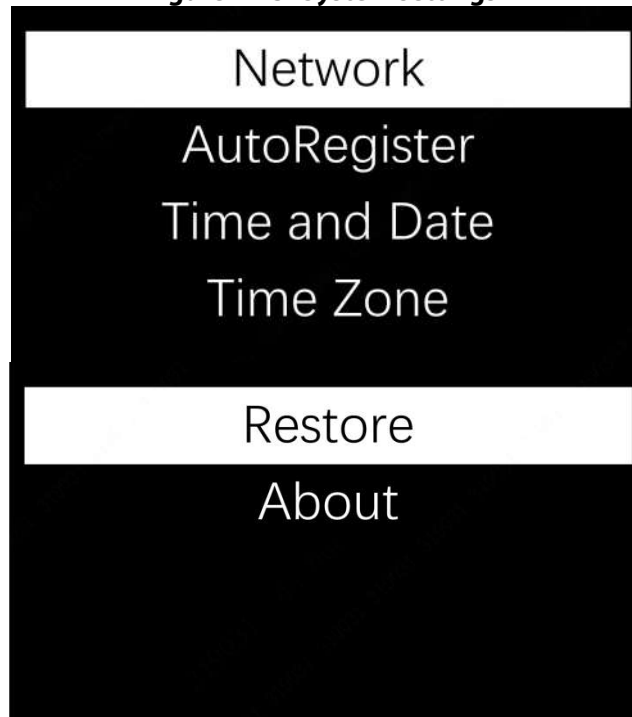
4.1.14 System Settings

System setting includes Network Parameters, Auto Registration, Time and Date, Time Zone, Restore and About.

Press or to select the corresponding parameters.

Press to confirm the setting. Press to return to the main menu.

Figure 4-15 System settings



(1) Network Parameters

The network parameters include the local IP address, Subnet mask, Gateway and DNS address. The above parameters are represented by four bytes. The adjustable range of each byte separated by a dot is: 0~255.



You can only connect to the network after initializing the device on the webpage.





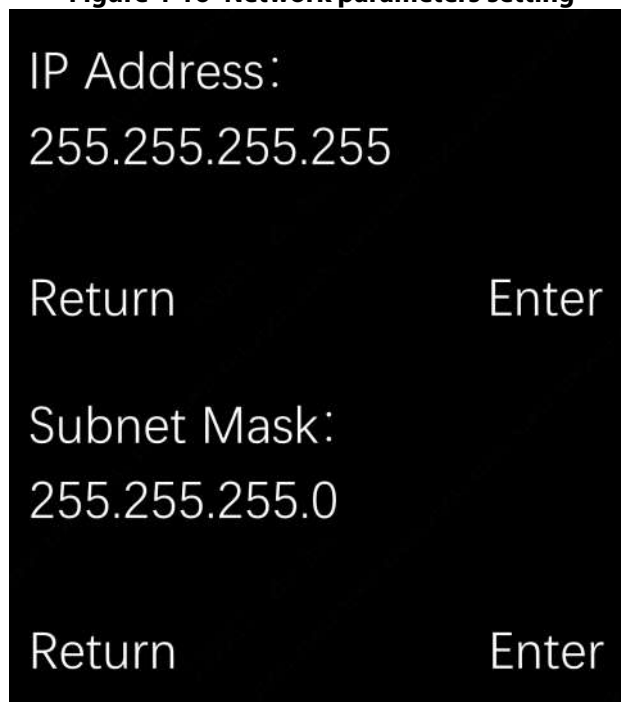
Press  and  to set the parameters. After all settings are completed, press  to confirm the restart, otherwise the setting is invalid, and press  to return to the System setting interface.

Figure 4-16 Network parameters setting





(2) **Auto registration**

Auto registration can connect the antenna to the network platform. After the connection is successful, the operation of the antenna can be remotely checked on the platform.






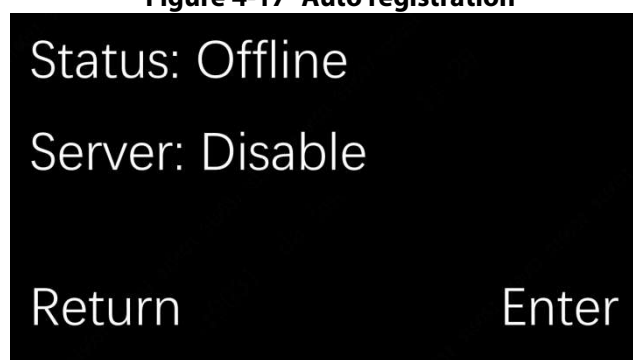
Press  and  to disable/enable this function, and press  to confirm. After enabling this function, you can choose to add the server IP address or preset address. After all settings are completed, press  to confirm and save, and it will take effect immediately after saving, Press  to return to the System setting interface.

Figure 4-17 Auto registration





(3) Time and Date





Time and Date function is used for setting the device date and time. Press  and  to set time and date. And press  to confirm and press  to return to the System setting interface.

Figure 4-18 Time and date



(4) Time zone

Time zone function is used for adjusting the local time based on the Greenwich Mean Time (GMT) and the local time zone. A total of 36 options are available.

Press  and  to set the time zone. And Press  to confirm and press  to return to the System setting interface.

Figure 4-19 Time zone



(5) Restore

5 Configuration on the Webpage

5.1 Initial Settings

When using the Device for the first time, or after restoring factory defaults, initialize the device, and set the basic information.



- Keep the password of admin user safe and change it regularly to ensure device security.
- Make sure that IP of the device is in same network with PC.
- The device can connect to the network or platform after initialization.

Step 1 Open the browser, enter IP address, and then press the Enter key. The default IP addresses is 192.168.1.108.

Step 2 Set the time zone, date and time, and then click Next.

Step 3 Input password of admin and click Complete.

5.2 Login

Log in to the webpage for system configuration and operation Before login, it needs to meet the following requirements.

- Log in to the webpage after initialization.
- Make sure that IP of the device is in same network with PC.

Step 1 Open the browser, enter IP address, and then press the Enter key.

Step 2 Input the user name and password.



- The user name is admin by default.
- If need to change the password, select User Management to change. For details, see 5.9 User Management.

5.3 System Settings

Configure the system operation parameters, including TX switching, RX switching, alarm mode, alarm threshold, time and date and more.

Step 1 Select System Settings on the webpage.


Step 2 Configure parameters.

Figure 5-1 System settings

The screenshot displays the 'System Settings' page. On the left, a vertical menu lists various system functions, with 'System Settings' highlighted. The main content area is divided into several sections, each with a title and a set of controls. The 'TX Switch' and 'RX Switch' sections each have three checkboxes for CH1, CH2, and CH3, all of which are checked. The 'Tag Too Close' and 'Interfere Reminder' sections each have two radio buttons for ON and OFF, with 'OFF' selected in both. The 'Alarm Tone' section has three radio buttons for Alarm Tone1, Alarm Tone2, and Alarm Tone3, with Alarm Tone1 selected. The 'Alarm Volume' section has a numeric input field set to '1' and a range of '(0~5)'. The 'Alarm Threshold' section includes a dropdown menu for 'CH1' and three input fields for 'SNR' (set to '10'), 'RMS' (set to '0'), and 'NUM' (set to '3'), each with a range. The 'Signal Gain' section has three input fields for 'CH1', 'CH2', and 'CH3', all set to '0', each with a range of '(0~6)'. The 'Alarm Mode' section has two radio buttons for Alarm Mode1 and Alarm Mode2, with Alarm Mode2 selected. The 'Time Zone' section has a dropdown menu set to 'GMT+08:00'. The 'Time and Date' section has a text input field set to '2007-05-25 21:49:53'. Each section has a 'Save' button, and some have additional buttons like 'Default', 'Reboot', or 'Restore'.

Table 5-1 Parameters description

Parameter	Description
TX Switch	3 channel are enabled by default. Click <input checked="" type="checkbox"/> to close the signal transmitting function of corresponding channel. Alarm of corresponding channel cannot be trigger when the function is closed
RX Switch	3 channel are enabled by default. Click <input checked="" type="checkbox"/> to close the signal receiving function of corresponding channel. Alarm of corresponding channel cannot be trigger when the function is closed
Tag Too Close	The function is closed by default. After enabled, when a tag stays in the antenna area for a long time (≥ 2 minutes), the alarm audio will be turned off, and the alarm light will change to flash mode. If no continued alarm is triggered for more than 3 seconds after entering into flashing mode, it will turn back to normal alarm mode.
Jammer Reminder	Not available currently.
Alarm tone	3 tones available.
Alarm volume	0-5 level volume adjustable, 0 is silent, 5 is the maximum.

Alarm threshold	<p>Select a channel from the drop-down list. The adjustment range of Signal/Noise ratio (SNR) is 0-50, and the adjustment range of Root Mean Square (RMS) is 0-1500. The lower the value of the two parameters, the farther the detection distance but the higher the risk of false alarms. The adjustment range of the Number of Alarm reviews (NUM) is 0-10, which is used to improve the accuracy of label recognition. The lower the value, the easier it is to trigger the alarms, but the higher the risk of false alarms. The above parameters can be adjusted according to the data of parameter monitoring.</p>  <p>For the monitoring values corresponding to each alarm parameter, please refer to "5.4 Environment Monitoring" for details.</p>
Signal gain	It is not recommended to change the default value of this parameter without the professional personnel.
Alarm mode	Alarm mode 1 automatically adjusts parameters in real time according to the field environment to avoid false alarms. Alarm mode 2 collects environmental parameters for a period of time to avoid false alarms (this process takes about 15s).
Time zone& Time and date	The current time zone, time, and date can be modified.

Step 3 Click Save.

5.4 Environment Monitoring

Real-time monitoring and display of equipment signal value, ambient noise, SNR and RMS. Set alarm threshold parameters based on the environmental monitoring value. The rules for parameter setting are as follows: When no EAS label/tag is near the antenna, the curve should be lower than the threshold. When an EAS label/tag is near the antenna, the curve should be higher than the threshold. In this way, labels/tags can be identified effectively and false alarms can be avoided. The environment data can be paused to view in the lower right corner.

5.4.1 Parameter Monitoring

- S represents the signal value.
- N represents the environment noise value.
- SNR represents the signal and noise ratio value. The range is 0~50.
- RMS represents the root mean square, the confidence coefficient of EAS tag signal. The range is 0~1500.

Figure 5-2 Environment monitoring



5.4.2 False Alarm Monitoring

Detect and display the false alarm numbers of each channel. You can check the false alarm numbers in the Environment Monitoring interface when debugging the device. Monitor for a period of time. If the number of the false alarms is big, it means there is interference in the environment or the alarm threshold is not reasonable. You need to perform Phase Sync or modify the value of NUM in System Settings.

5.5 Phase Synchronism

Phase synchronization can synchronize the transmission timing of the device with other EAS system, avoiding false alarms due to timing inconsistencies. For example, when the signal receiving timing of the device is same with the transmission timing of another device in the environment, then false alarms will be triggered. You need to synchronize the phase of the device.

Step 1 Select Phase Synchronism on the webpage.

Step 2 Select the channels that needs to be phase synchronized.

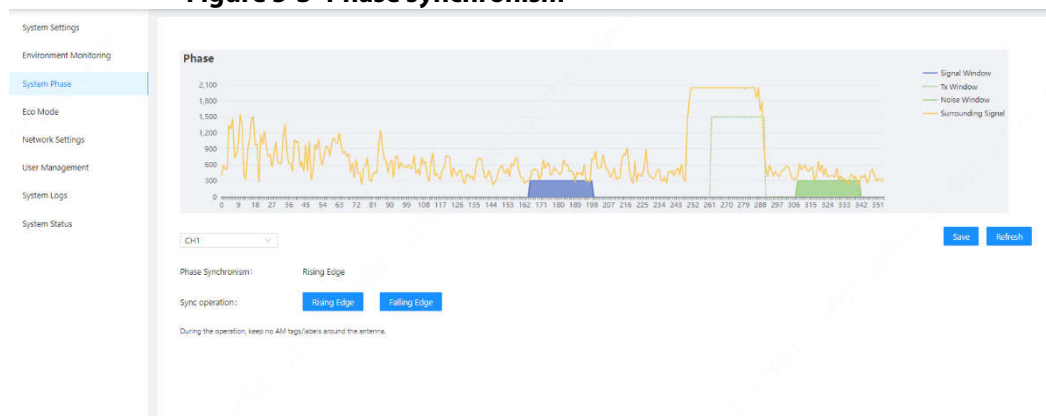
Step 3 Click Rising Edge or Falling Edge. The phase will synchronize automatically.



- **Rising Edge** means the signal transmission timing synchronizes along the rising direction of power common frequency. **Falling Edge** means the signal receiving timing synchronizes along the falling direction of power common frequency.

Step 4 Refresh the page to check whether the TX sync is successful. If the Device is in TX mode 1, the sample window (blue slider) should avoid the area with large fluctuations before transmitting. Drag the slider and click Save.

Figure 5-3 Phase synchronism



5.6 Eco Mode

After the Eco mode is enabled, the device sleeps for a specified period of time and does not have the label detection capability during the period.

Figure 5-4 Eco mode

The screenshot shows the 'Eco Mode' configuration page. On the left is a sidebar menu with options: System Settings, Environment Monitoring, System Phase, Eco Mode (highlighted), Network Settings, User Management, System Logs, and System Status. The main content area has a title 'Eco Mode' with radio buttons for 'ON' and 'OFF' (selected). A note states: 'After the ECO mode is enabled, the detection cannot be performed within the selected period.' Below this are three 'Time Quantum' settings, each with a start and end time picker (00:00:00 to 23:59:59) and a checkbox. At the bottom, there are checkboxes for 'All' and individual days of the week (Mon, Tues, Wed, Thur, Fri, Sat, Sun).

5.7 Network Settings

On this page, you can set the IP address, subnet mask, gateway, and DNS address of the Device and more, select the target server address for active registration, and initiate network detection for the specified address.

Figure 5-5 网络设置

The screenshot shows the 'Network Settings' page. The left sidebar menu is the same as in Figure 5-4, with 'Network Settings' highlighted. The main content area has fields for 'IP Address', 'Net Mask', 'Gateway', and 'DNS Server', each with a dotted input field (e.g., 10 . 35 . 36 . 197). Below these are 'Save' and 'Cancel' buttons. Further down, there is an 'AutoRegister Status' dropdown set to 'Offline', an 'AutoRegister Server' dropdown set to 'Disable', and another 'Save' and 'Cancel' button. At the bottom, there is a 'Diagnostic Type' dropdown set to 'Default', and 'Start', 'End', and 'Clear Data' buttons.

5.8 System Log

It displays Device operation logs. Supports log export and clear. A maximum of 1000 logs can be displayed.

Figure 5-6 System logs

MessageType	SubType	Details	Time and Date
Config	Activating	Axis	2017-05-23 13:0411
Config	Phase	Phase01	2017-05-23 13:0719
Config	Phase	Phase02	2017-05-23 13:0754
Config	Phase	Phase03	2017-05-23 13:0807
Config	Phase	Phase04	2017-05-23 13:0853
Config	Phase	Phase05	2017-05-23 13:0940
Config	Phase	Phase06	2017-05-23 13:0953
Config	Phase	Phase07	2017-05-23 13:0957
Config	Phase	Phase08	2017-05-23 13:0947
Config	Phase	Phase09	2017-05-23 13:0940

5.9 User Management

Change the user's password. Select User Management on the webpage. Input old password and new password, and then click Save.

If forget the old password, you can only reset the password after restoring factory defaults.

5.10 System Status

View the device status, including active channel (main device), software version, phase, power voltage, frequency and more. After the phase adjusted or power frequency changed, click Refresh to view the phase and power frequency at present.

6 FAQ

1. Irregular occasional false alarms.

- Reason 1: The clerk did not place the device with the EAS label outside the detection range, which was too close to the EAS antenna, resulting in a false alarm.
- Solution: Place devices with the EAS tag outside the detection range of the EAS antenna as required.
- Reason 2: There is a similar coil near the EAS antenna to form a loop, generating the tag signal.
- Solution: Check if there are coiled wires or closed rings of metal forming loops near the EAS antenna that generate label signals and cause false alarms.
- Reason 3: There are other electrical equipment connected to the EAS exclusive circuit, and then the power interference leads to false alarms.
- Solution: Check whether any electrical equipment is mistakenly plugged into the EAS exclusive circuit. If there is, please remove it.
- Reason 4: There are other EAS devices suppliers installing and debugging in other nearby stores, and the unsynchronized phase of EAS devices causes false alarms.
- Solution: Please communicate with the store, and ask their EAS equipment supplier to stay in the store to observe after the installation and debugging to ensure that the EAS device has been synchronized without interference with each other.
- Reason 5: The newly added electrical device in the store is near the EAS antenna, and spatial interference leads to false alarms.
- Solution: Before the store needs to add new electrical device near the EAS antenna, please temporarily power on the device to test whether it will cause interference to the EAS antenna. Please contact the technician to confirm whether it can be installed

2. The label detection rate is low, and no alarm is sent through the antenna area.

- Check whether the power cable connection, and the connection between the primary antenna and replica antenna are correct.
- After confirming the connection is correct, set Phase synchronism.
- Reduce the values of threshold and NUM.
- Use a larger label.

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.