

EAS AM Antenna (110 V)

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
V1.0.1	Add new functions such as alarm mode threshold, false alarm monitoring and parameter monitoring.	November 2022
V1.0.0	First release.	July 2022

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
Overview	1
Product Functions.....	1
Product Features	1
2 Product Structure	2
Product Appearance	2
1.1 Port Description.....	4
1.2	
3 Installation	7
2.1 Out-of-box Checking	7
2.2 Installation Requirements.....	8
Tools	8
3.1 Installation Procedure (Preinstall)	9
3.2 Installation Procedure (Add Installation).....	11
3.3 Installing Advertising Board.....	12
3.4 Alarm linkage with CCTV	14
3.5	
3.6	
4 Device Debugging	16
Sensitivity Adjustment.....	16
4.1 System Parameter Configuration	17
4.2	
4.2.1 Home Page	17
4.2.2 Main Menu	18
4.2.3 Alarm Tone	19
4.2.4 Alarm Volume.....	20
4.2.5 Alarm Mode/ Threshold.....	20
4.2.6 False Alarm Monitoring	21
4.2.7 Parameter Monitoring.....	22
4.2.8 TX Switch/RX Switch	22
4.2.9 TX Mode	22
4.2.10 Phase synchronism/Phase Adjustment.....	23
4.2.11 Tag Too Close.....	23
4.2.12 Jammer Reminder.....	24
4.2.13 System Settings.....	24
5 FAQ	26
Cybersecurity Recommendations	27

Appendix 1

1 Product Information

Overview

- 1.1 2 Series EAS AM Antenna is an anti-theft device that can effectively identify the anti-theft AM tags.. The Device can effectively prevent the theft of goods, cut business operating costs, and improve customer shopping experience. The Device has a simple and elegant appearance with powerful performances and complete functions, which is an important part of the retail loss prevention system.

Product Functions

- 1.2
- 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.
 - Optional accessories: Optional advertising boards are used for customer publicity

1.3

Product Features

- Long detection distance: The maximum detection distance of single-antenna labels is 90 cm to 100 cm, and the maximum detection distance of tags is 100 cm to 120 cm.
- Stable hardware performance: The high-performance transmitting signal 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.
- Power saving and environmental protection: The Device is harmless to the human body.

2 Product Structure

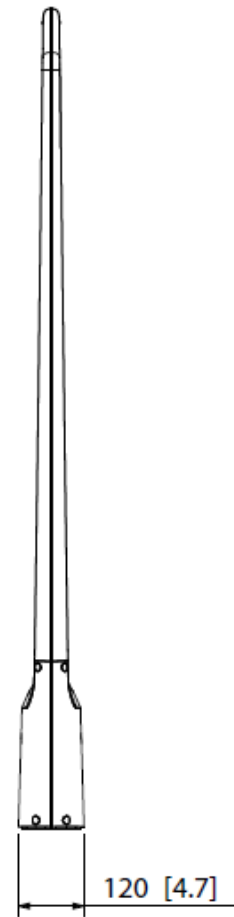
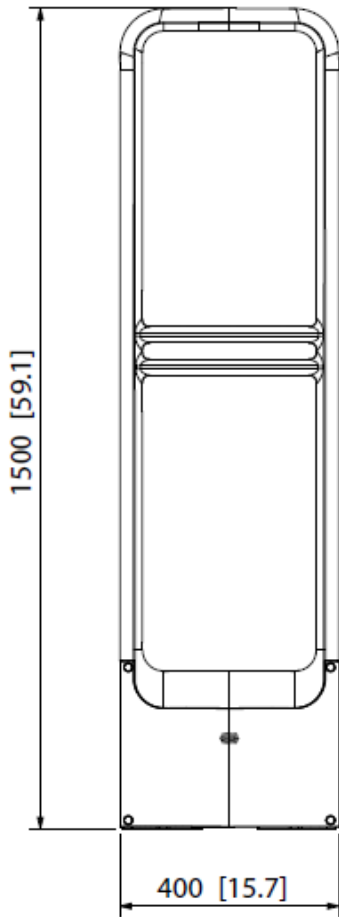
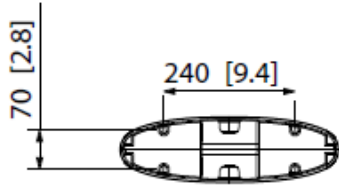
Product Appearance

2.1

Product appearance



Dimensions (Unit: mm [inch])



Port Description

2.2

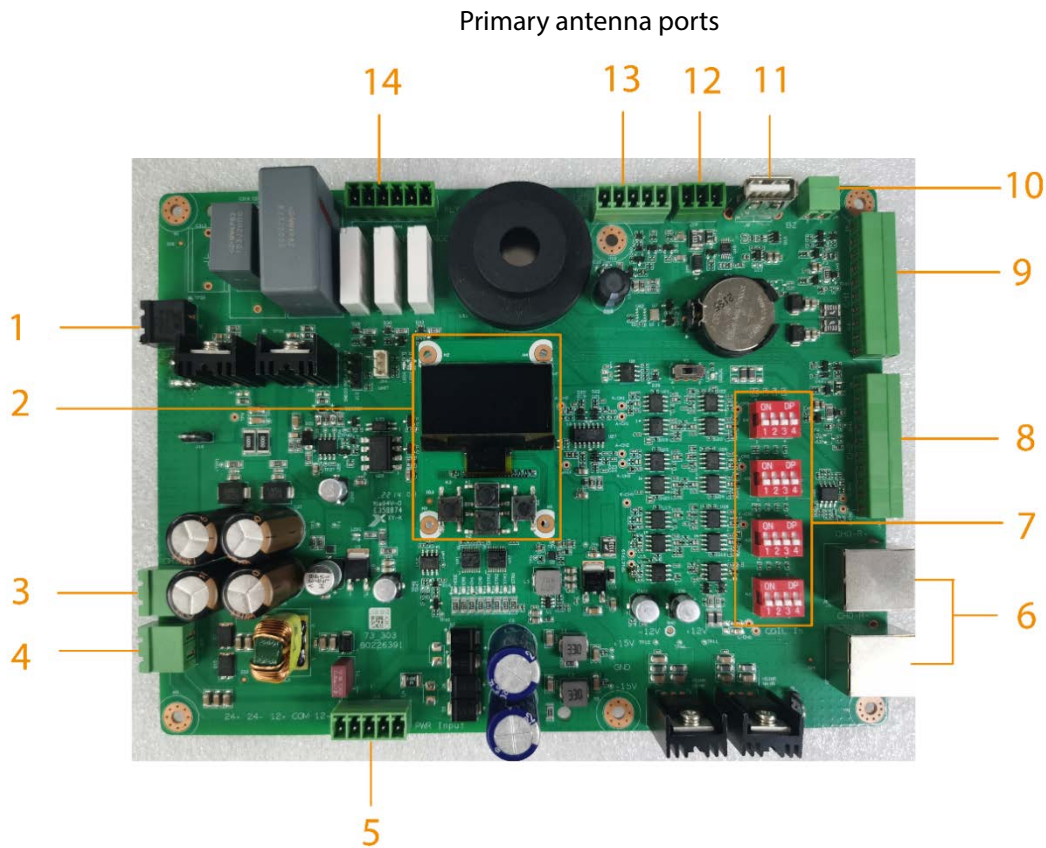




Table 2-1 Primary antenna ports description

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	Sensitivity adjustment button	Sensitivity adjustment button is used to adjust the antenna detection sensitivity.
8	Replica antenna CH3 communication cable port	Replica antenna CH3 communication cable port.
9	Replica antenna CH2 communication cable port	Replica antenna CH2 communication cable port.
10	Standby buzzer port	Connects standby buzzer.
11	USB debugging port	Debugs firmware upgrade.

No.	Parameter	Function
12	LED light board port	LED light board port.
13	Standby communication port	Standby communication port.
14	CCTV linkage port	CCTV linkage port, 3-channel alarm relay output.

Replica antenna ports

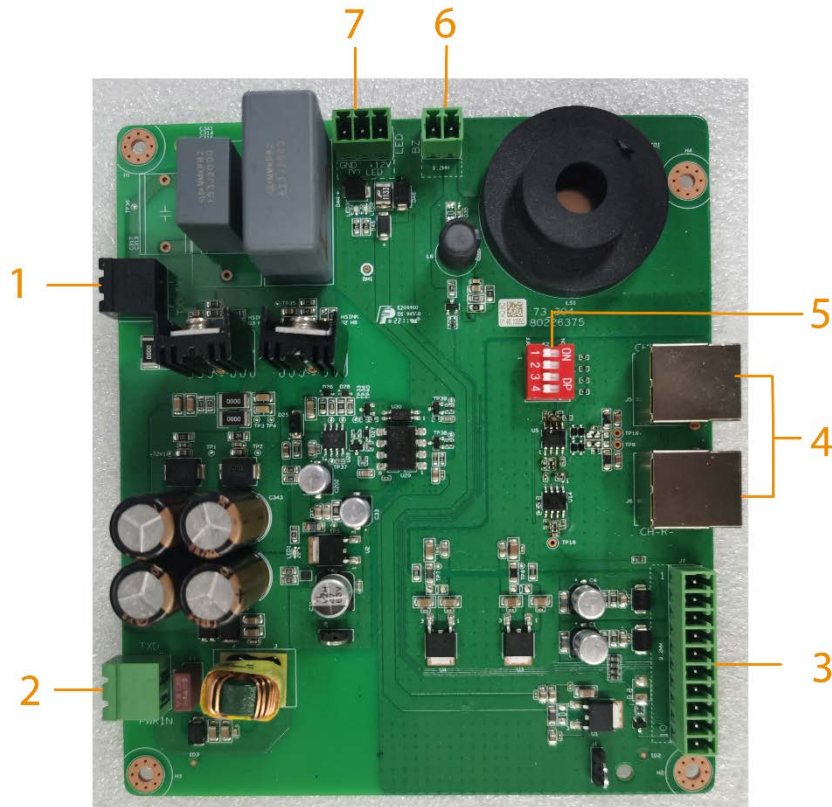




Table 2-2 Replica antenna ports description

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	Sensitivity adjustment button	Adjusts the antenna detection sensitivity.  For details, see "4.1 Sensitivity Adjustment".
6	Standby buzzer port	Connects standby buzzer.
7	LED light board port	LED light board port.

Power filter board ports

Figure 2-5

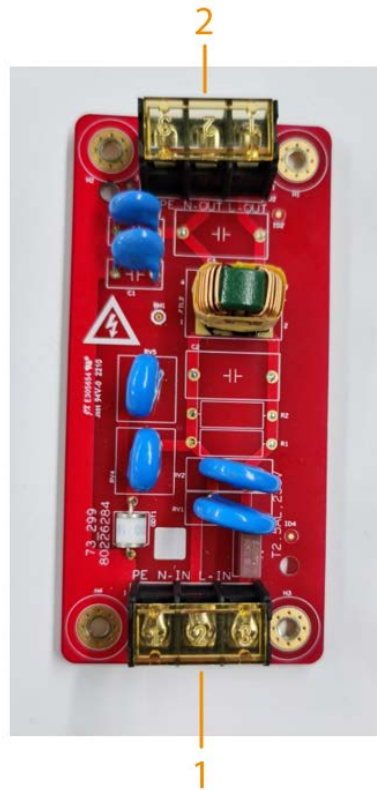


Table 2-3 Power filter board ports description

No.	Parameter	Function
1	AC power cable inlet	External power input (110 VAC). ⚠ Incorrect voltage input or cable connection may cause device damage.
2	Ac power outlet	The external power is output after filtering.


3 Installation

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

3.1

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.

Primary antenna packing list (left) and replica antenna packing list (right)

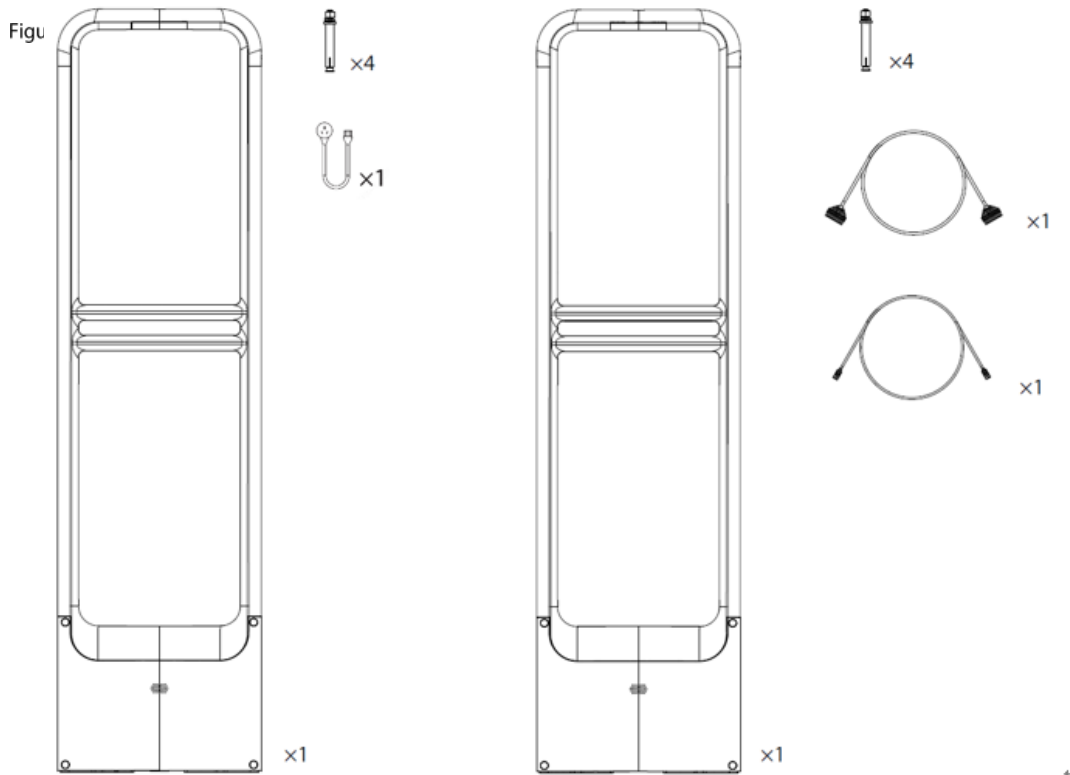


Table 3-2 Primary antenna packing list

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

Table 3-3 Replica antenna packing list

Name	Quantity
Replica antenna	1

Name	Quantity
M10×100 expansion screw	4
10PIN communication cable between primary antenna and replica antenna	1
2PIN replica antenna power cable	1

Installation Requirements

3.2

- 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.












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	

Name	Image	Name	Image
Fine sand		Stainless scuff plate	
Electric drill		—	—

Installation Procedure (Preinstall)

3.4

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. One ϕ 25 cable tube 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

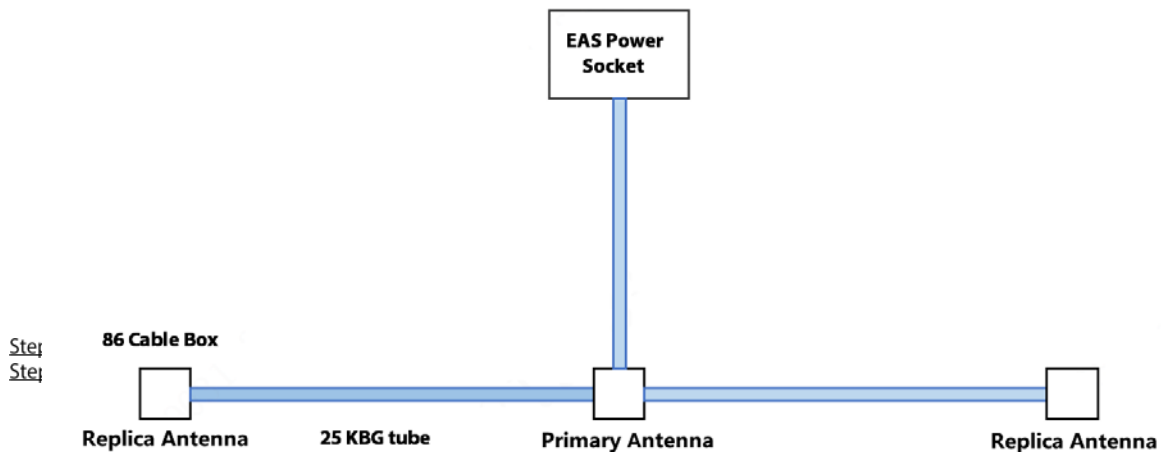
Confirm the position of the EAS power socket, and then reserve a ϕ 25 cable tube or another cable of the same size between the 86 cable box from the primary antenna for routing EAS antenna between the primary antenna and replica antenna.

Step 3

If the 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 camera in advance.

Figure 3-2

Description of the cable and tube reservation



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

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.

Primary antenna and replica antenna terminals (left)/Replica antenna power cable (right)

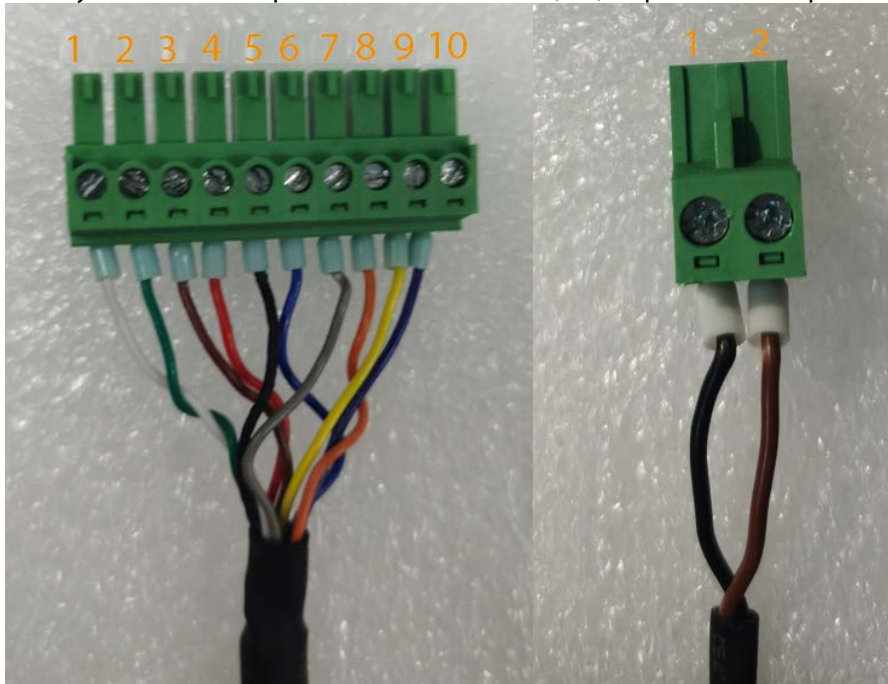
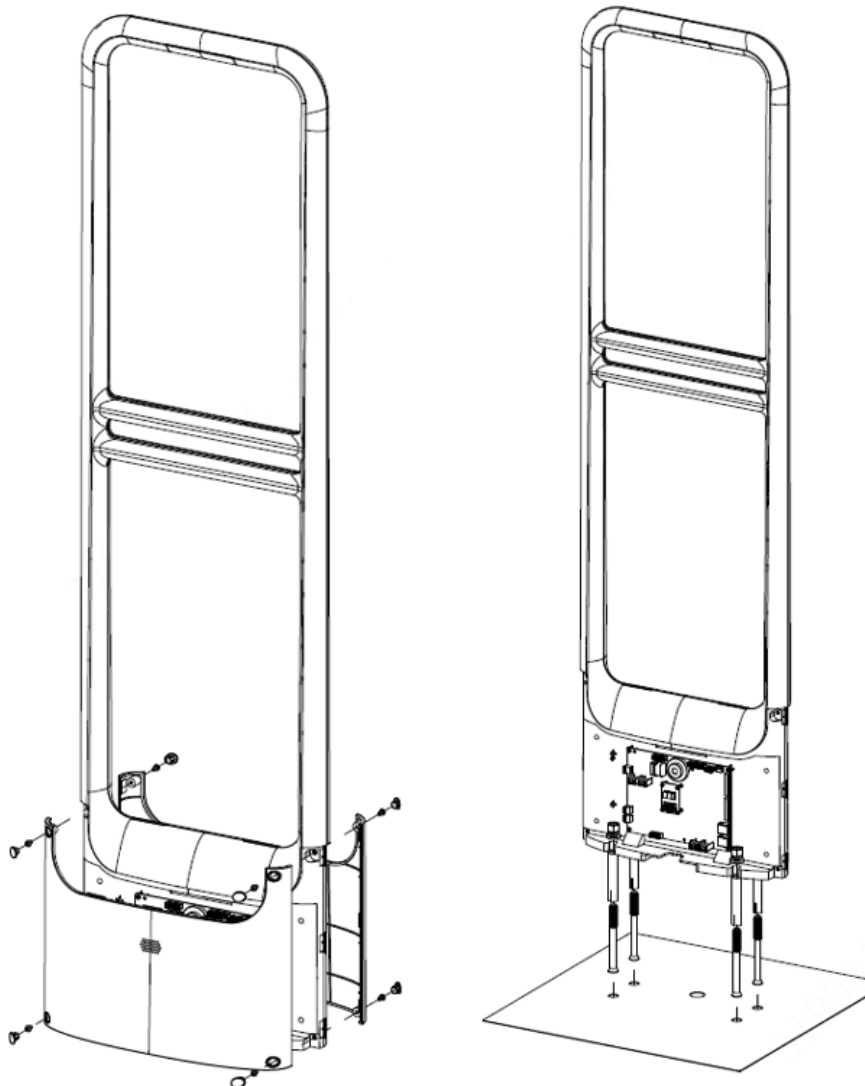


Figure 3-3

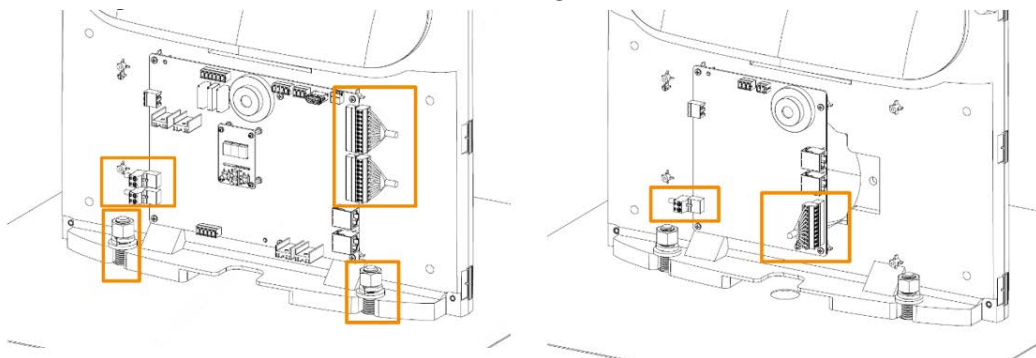
Remove the cover plate, align the antenna with the pre-embedded screws, tighten the screws, and then insert the cable terminal in the specified position.

Step 6

Installation diagram (1)



Installation diagram (2)



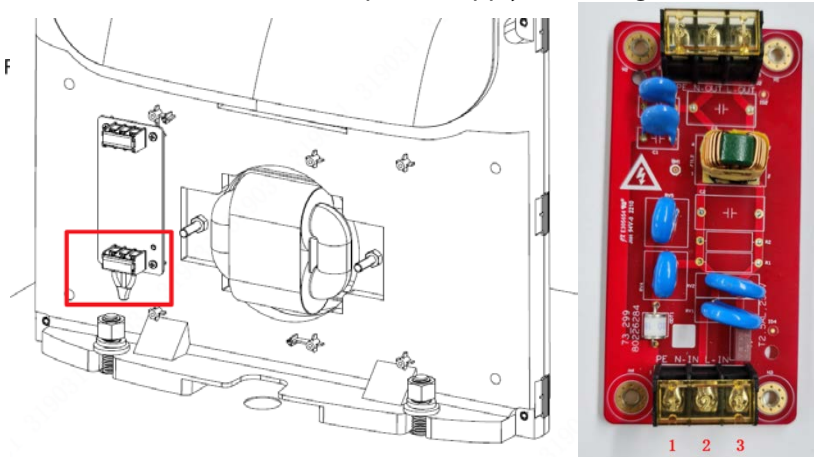
See Figure 3-6, No.1 port connects to the grounding wire (PE), NO.2 port for neutral wire (N) and NO.3 port for live wire (L).



Step 7

Input voltage of the Device is 110 VAC 50/60 Hz. 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.

External power supply cable diagram



3.5

Installation Procedure

Step 1



Step 2

This section is suitable for installing EAS device without pre-embedding cables and tubes for EAS. After determining the installation location, use a marker to draw lines, and then punch holes and cut grooves. Clean up the site.

Installation (1)

Step 3



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

Installation (2)



Install stainless scuff plate to fix the device.

Installation (3)



Step 4

3.6 Installing Advertising Board

In order to meet the needs of customers for publicity and display, the Device reserves sockets for fixing advertising boards. Customers can install according to actual needs.



Advertising board is optional.

Advertising board

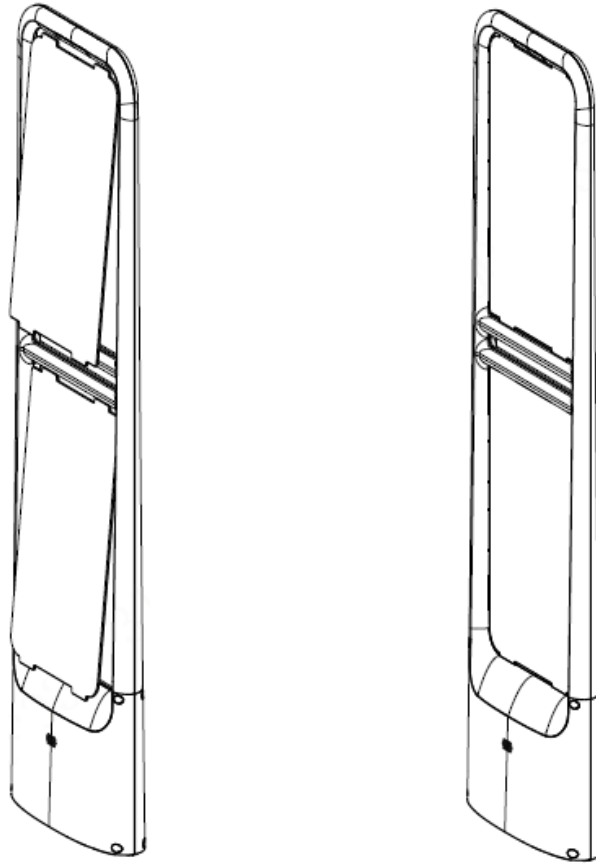
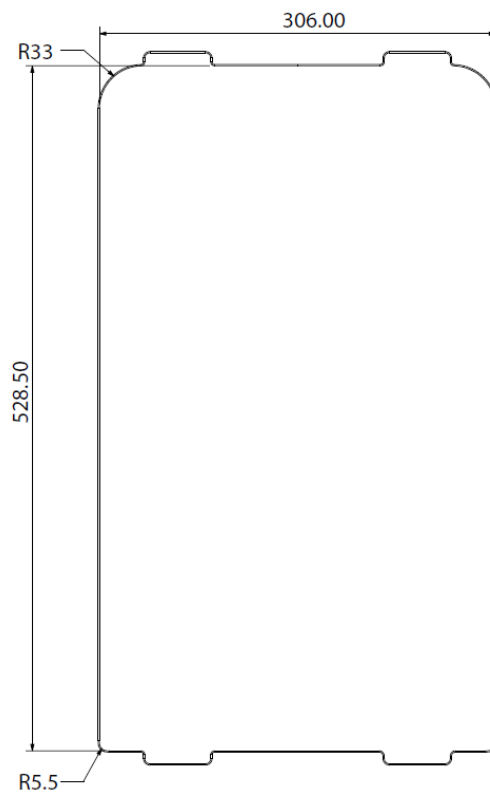


Figure 3-11

Advertising board dimensions (mm)



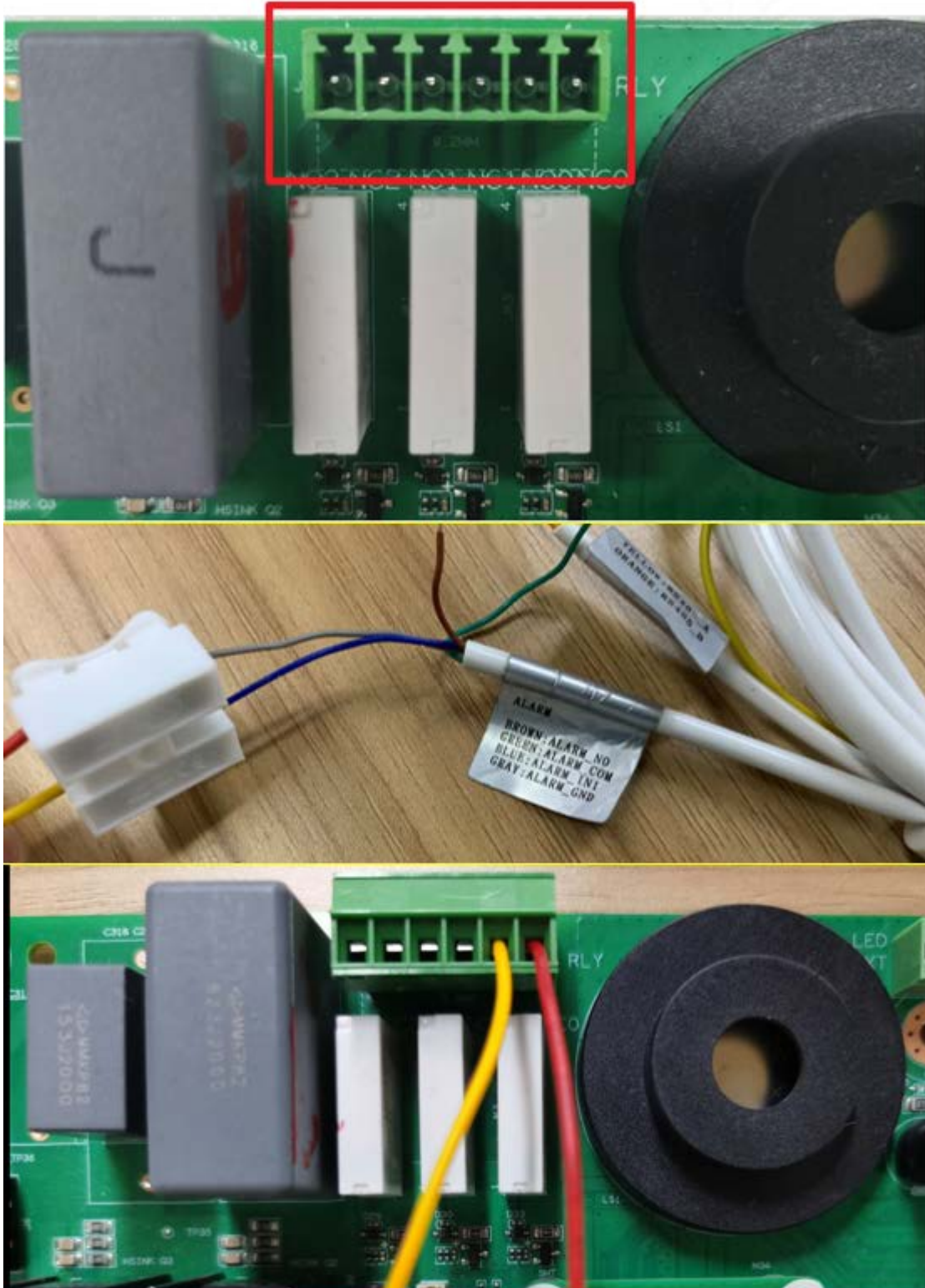
Alarm Linkage with CCTV

Cable Connection

There are 3 linkage alarm switches on the EAS main board, from left to right: NO2, COM2; NO1, COM1; NO0, COM0. Take channel 0 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.

3.7

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.

IPC Configuration

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
 - Snapshot: 1 2

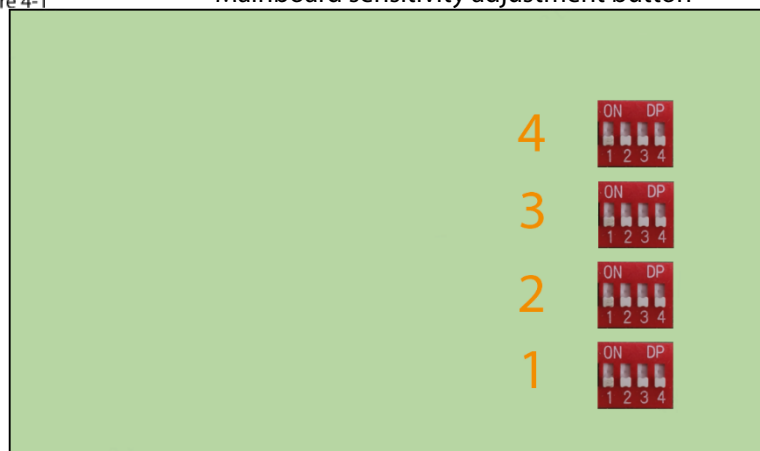
4 Device Debugging

Sensitivity Adjustment

4.1

- During the actual installation and use, the device detection effect is affected by the complex electromagnetic environment on site, and it is also difficult to accurately locate and close the interference sources. In order to deal with this situation, this Device designs a DIP system sensitivity adjustment switch, so that the device can be used normally under different interference intensity. For details on the switch, see“2.2 Port Description”.
- DIP switch No.1 and DIP switch No.2: Responsible for the sensitivity adjustment of CH1 channel (signal transceiver channel integrated on the mainboard). When switch 1 is pushed up separately, the Device has the highest sensitivity and the longest detection distance, suitable for low-noise environments. When switch 2 to switch 4 are pushed up successively, the sensitivity gradually decreases, and the detection distance gradually becomes shorter.
- DIP switch No.5 and DIP switch No.4: Responsible for the sensitivity adjustment of CH2 channel (if CH2 is not connected, it cannot be adjusted). When switch 1 is pushed up separately, the Device has the highest sensitivity and the longest detection distance, suitable for low-noise environments. When switch 2 to switch 4 are pushed up successively, the sensitivity gradually decreases, and the detection distance gradually becomes shorter.
- DIP switch No.6 and DIP switch No.3: Responsible for the sensitivity adjustment of CH3 channel (if CH3 is not connected, it cannot be adjusted). When switch 1 is pushed up separately, the Device has the highest sensitivity and the longest detection distance, suitable for low-noise environments. When switch 2 to switch 4 are pushed up successively, the sensitivity gradually decreases, and the detection distance gradually becomes shorter.

Figure 4-1 Mainboard sensitivity adjustment button



Replica board sensitivity adjustment button (CH2 on the left, CH3 on the right)

Figure 4-

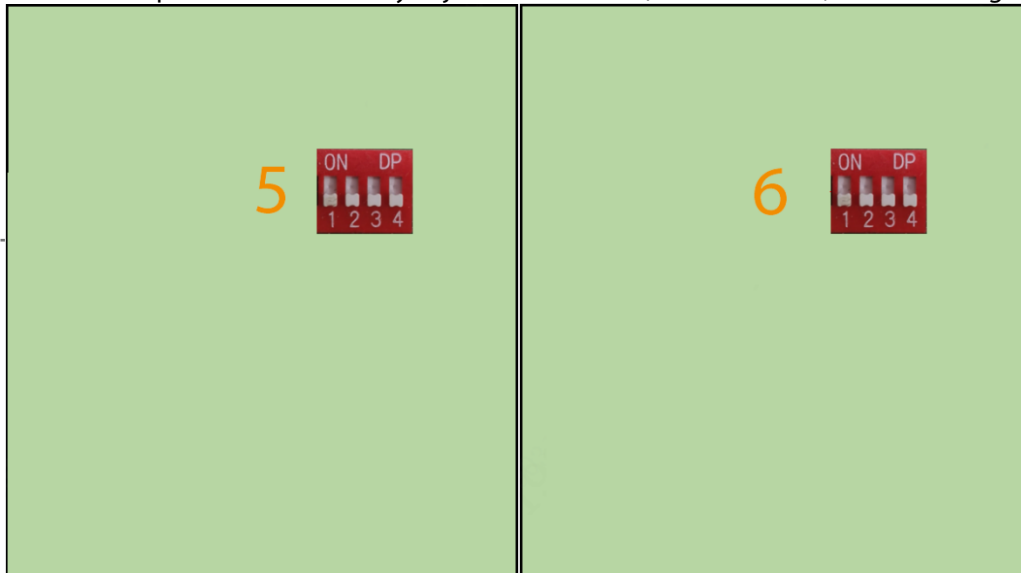


Table 4-1 Description of sensitivity adjustment button

Image	Description
	The highest sensitivity, the worst anti-interference ability, and the longest detection distance in low-interference scenarios.
	High sensitivity, poor anti-interference ability, and long detection distance in low-interference scenarios.
	Low sensitivity, strong anti-interference ability, and long detection distance in the interference scenarios.
	The lowest sensitivity, the strongest anti-interference ability, and the longest detection distance in the interference scenarios.
	Factory setting of DIP switch.



4.2

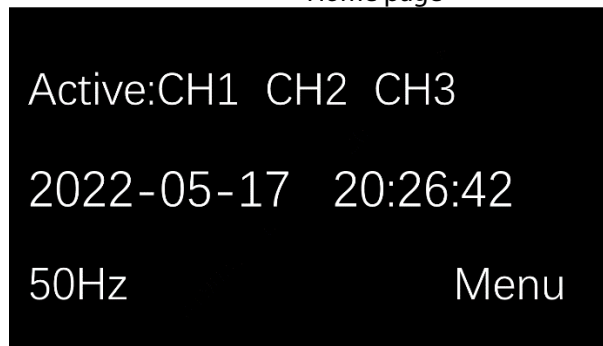
On: ; Off: .

System Parameter Configuration

4.2.1 Home Page





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

Press to go to the home page.



4.2.2 Main Menu

The main menu includes all parameters configuration entries.

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



The interference reminder function is temporarily unavailable.

1.Alarm Tone

2.Alarm Volume

3.Alarm Mode

4.Alarm Threshold

5.False Alarm Monitor

6.Param Monitor

7.Tx Switch

8.Rx Switch

9.Tx Mode

10.Phase Synchronism

11.Phase Adjust

12.Tag Too Close

13.Interfere Remind

14.System Settings

4.2.3 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

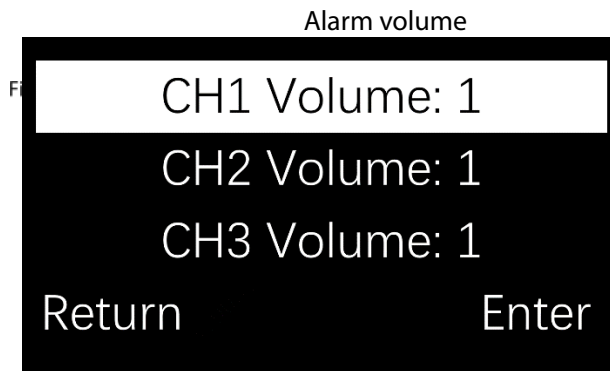
the main menu.



4.2.4 Alarm Volume





The system alarm volume is adjustable in 5 levels.

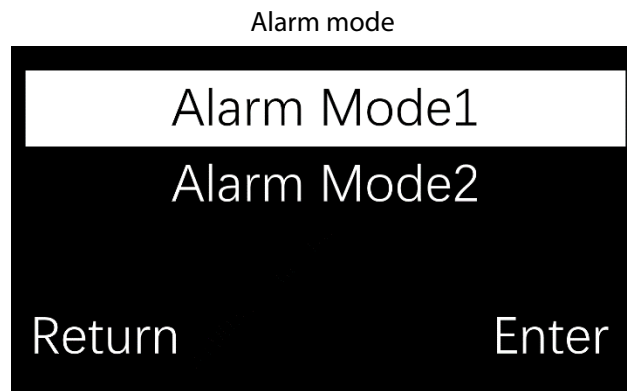
Press  or  to move the cursor to select the channel. After pressing  to confirm the channel, you can press   to adjust the volume. Press  to confirm the volume. Press  to return to the main menu.










4.2.5 Alarm Mode/ Threshold

The system includes 2 alarm modes for different interference environments. The alarm threshold is connected to the alarm mode, and the threshold parameters switch with the alarm mode.

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



- Alarm mode 1 (default): In this mode, the default parameters can be adjusted according to the actual interference conditions. The adjustment range is from 0 to 5 levels. The lower the threshold, the more sensitive the antenna is and the longer the detection distance is. However, false alarms may occur. We recommend you set the threshold to level 2 or higher.

Press  or  to move the cursor to select the channel. After pressing  to confirm the channel, you can press  or  to adjust the alarm threshold. Press  to confirm the threshold or press  to return to the main menu.

Alarm mode 1

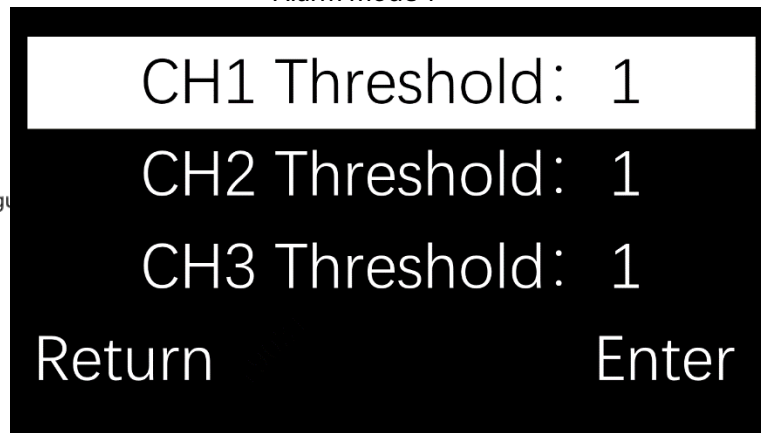












Figure 4-9

- Alarm mode 2 (customized): In this mode, all alarm threshold parameters can be customized and adjustable.

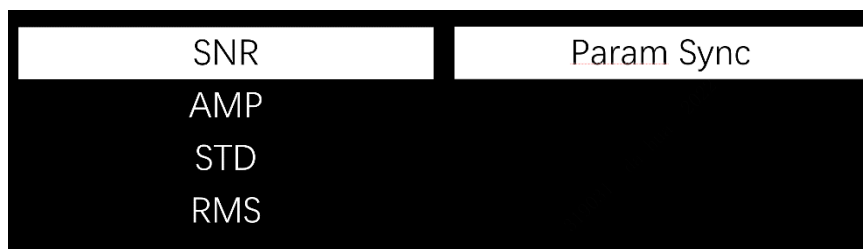
Parameter	Adjustment range	Step size / Long key step
3-channel threshold parameters (SNR (Signal/Noise ratio))	0~50	5
AMP (Amplitude)	0~300	10
STD (Standard Deviation)	0~1500	10
RMS (Root Mean Square)	0~1500	10



You can synchronize all parameters of the selected channel to the other two channels through the parameter synchronization function.


Press  and  to select the parameter for synchronization. And press  to confirm the parameter synchronization to other channels (it is recommended to configure under the development guidance). Press  and  to move the cursor to select the parameter. After pressing  to confirm the channel, you can press  and  to adjust the parameters. Press  to confirm the parameters. Press  to return to the main menu.

Alarm mode 2



4.2.6 False Alarm Monitoring

Displays the number of 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. The falsers alarms displayed, the more alarm thresholds (alarm mode 1) need to be increased to reduce false alarms.

Press  to return to the main menu.

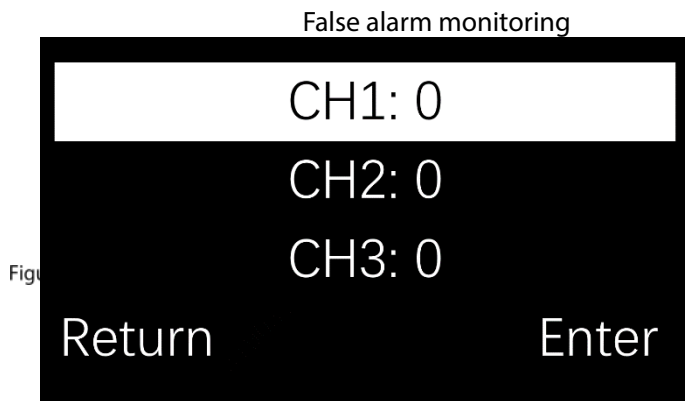


Figure 4-10

4.2.7 Parameter Monitoring

The parameter monitoring displays the SNR (Signal/Noise ratio) bar graph and the 3-channel threshold parameters in real time. Press and to select the channel. If the channel is not connected or the receiving is closed, it will display that the channel is closed. The louder the noise, the greater the environmental interference. If the noise is too loud, the installation location needs to be changed. Press to return to the main menu.

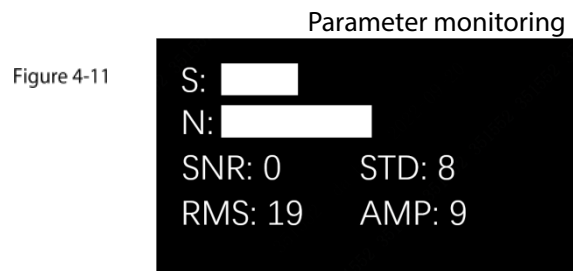


Figure 4-11

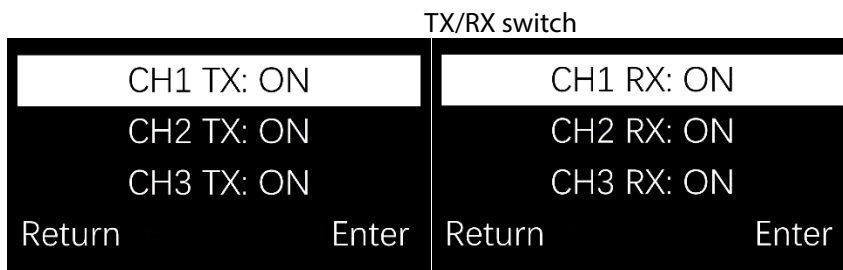
4.2.8 TX Switch/RX Switch

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.







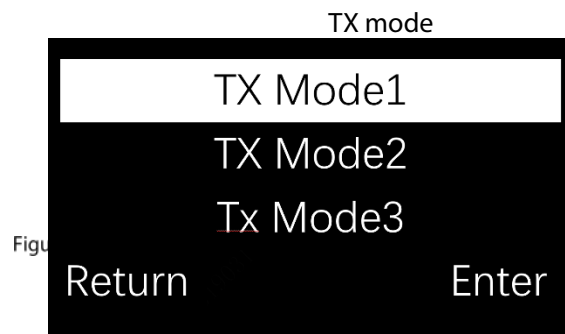
Turning off the transmitter or receiver may cause the alarm function failure.



4.2.9 TX Mode

In this mode, you can set transmission timing and cycle control of the transmitter. TX mode 1 is the default TX mode, TX modes 2 and 3 are fast TX modes (used during test).

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



4.2.10 Phase synchronism/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. In about 1-5 seconds, if other devices exist and there is a timing difference between the devices, the device will prompt **Completed!**, if not, it will prompt that **No sync required**, and the process is completed.










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. The change range is 0 to 120.

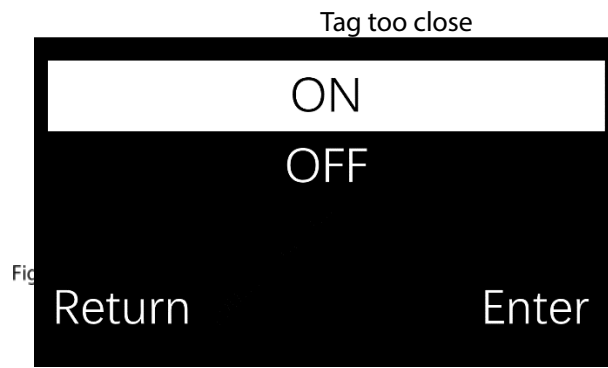
Figure 4-14 Phase synchronism/Phase Adjustment



4.2.11 Tag Too Close

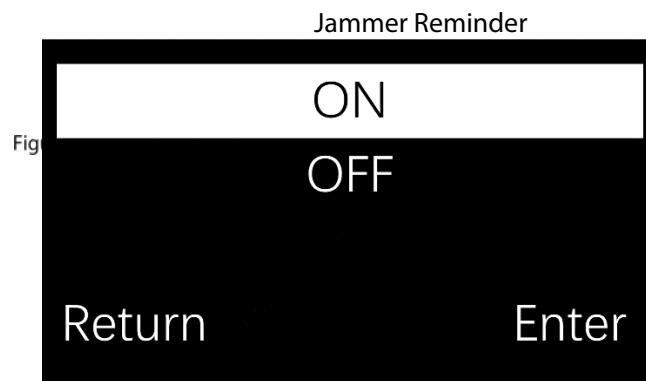
When this function is enabled, when a tag/label stays in the antenna detection area for a long time (≥ 2 minutes), the device uses the flashing light instead of the alarm tone to remind. After entering the flash light mode, and no continuous alarm is detected for more than 3 seconds, it will restore 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.







4.2.12 Jammer Reminder

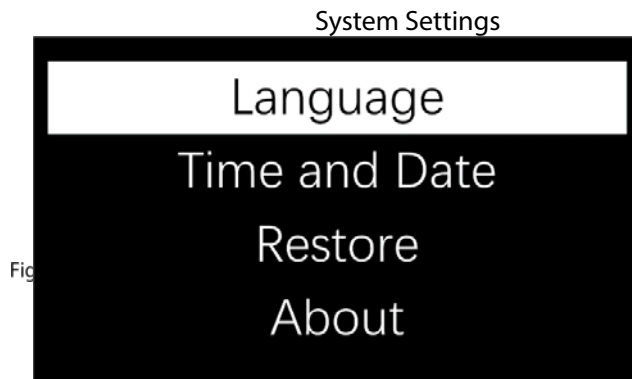
When it is detected out any jammers nearby, the jammer reminder will be triggered.



4.2.13 System Settings

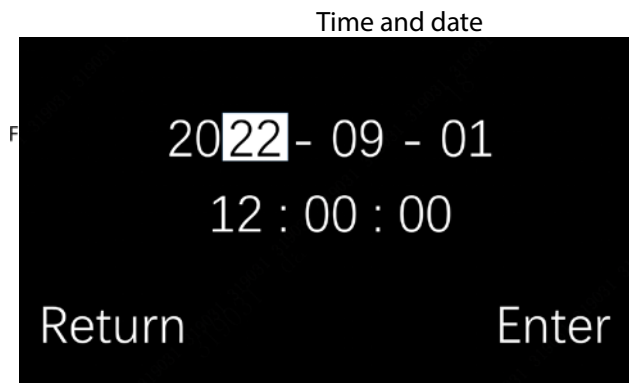
System setting includes **Language**, **Time and Date**, **Restore** and **About**.

Press  or  to select the corresponding parameters. Press  to confirm the setting. Press  to return to the main menu.



(1) Time and date

Set time and date. Press and to set time and date. Press to confirm and press to return to the **System setting** interface.



(2) Restore

Restore to the factory settings. Press to confirm and press to return to the **System setting** interface.

Figure 4-19



(3) About

You can view the **Software version**, **Release time** and **Device ID**.



5 FAQ

- 1. False alarms occur at fixed times every morning and evening.**
 - Reason: Shopping malls and stores open in the morning, and then shut down and out of power at night, causing instantaneous voltage load imbalance and power supply interferences, resulting in false alarms.
 - Solution: This problem cannot be solved completely. Please turn on other electrical devices first in the store every day when opening the store, and then turn on the power of the EAS device last.
- 2. 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 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 label on the device near the EAS antenna, an alarm will be generated.
 - Solution: We recommend you turn off the power of the EAS device during closing time.
- 3. 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.
- 4. 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
- 5. 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. For details, see "4.2.10 Phase synchronism/Phase Adjust".
 - Shorten the distance between the primary antenna and replica antenna, and then reduce the antenna sensitivity. For details, see "4.1 Sensitivity Adjustment".
 - Use a larger label.

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:

Appendix 1 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.