Walk-through Metal Detector

Quick Start Guide

V1.0.1

Foreword

General

This manual introduces the functions and operations of the walk-through metal detector (hereinafter referred to as the "Detector").

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	Update port description and installation procedure. Add the temperature overlay function.	November 2021
V1.0.0	First release.	June 2021

Interface Declaration

This manual mainly introduces the relevant functions when you use the Device. The interfaces used for manufacture, returning to the factory for inspection, and locating fault are not described in this manual. Please contact technical support if you need information about these interfaces.

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, fingerprints, and car 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 chapter describes the contents covering proper handling of the Device, hazard prevention, and prevention of property damage. Read these contents carefully before using the Device, comply with them when using, and keep the manual well for future reference.

Transportation Requirements

⚠

Transport the Device under the allowed humidity and temperature conditions.

Storage Requirements

⚠

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

Installation Requirements

⚠

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

Operation Requirements

⚠

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

Maintenance Requirements

⚠ WARNING

● Use the battery of specified manufacturer; otherwise there might result in explosion. When replacing battery, make sure that the same type is used. Improper battery use might result in fire, explosion, or inflammation.
● Always replace with the same type of batteries.
● Use the recommended power cables in the region and conform to the rated power specification.
● Use the power adapter provided with the Device; 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 Device (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

1 Overview

1.1 Introduction

The device is a high-performance walk-through metal detector. It is light-weighted and has high metal detection sensitivity, strong anti-interference capabilities and stable performance. The device, made of high-strength special materials, is light-weighted and easy to transport and install. The device has a modular design and is manufactured on unified assembly lines, ensuring the good stability. It also delivers a simplicity and user-friendly interface.

The walk-through metal detector is suitable for use in the following scenarios: Security screening of prohibited metal items in law enforcement sites such as public security, the procuratorate, tribunal, labor camp, and detention house. It is also suitable for security checks at the entrances of public spaces, including stadiums, entertainment places, airports, customs, exhibition halls and museums.

1.2 Technical Advantages

- Start-stop Technology
  The IR units support manual start-stop technology for longer service life.
- Adjustable Sensitivity
  The sensitivity of each detection zone can be adjusted as needed to meet different sensitivity requirements of different zones.
- Alarm
  Light and sound alarm for sharp alert. The sound duration and volume can be adjusted as needed.
- Search
  The system supports real-time search.
- Detection Capability
  60 to 100 people detected per min.
- Filtering
  Pre-define metal item weight, volume, size, part; exclude keys, jewelries, belt buckles and more.
- Security Protection
  In line with EMC electromagnetic radiation standards and adopting weak magnetic field technology, the Device is harmless to cardiac pacemaker wearers, pregnant women, floppy disks, film, and videotapes.

2 Structure

2.1 Dimensions

Figure 2-1 Dimensions (unit: mm [inch])
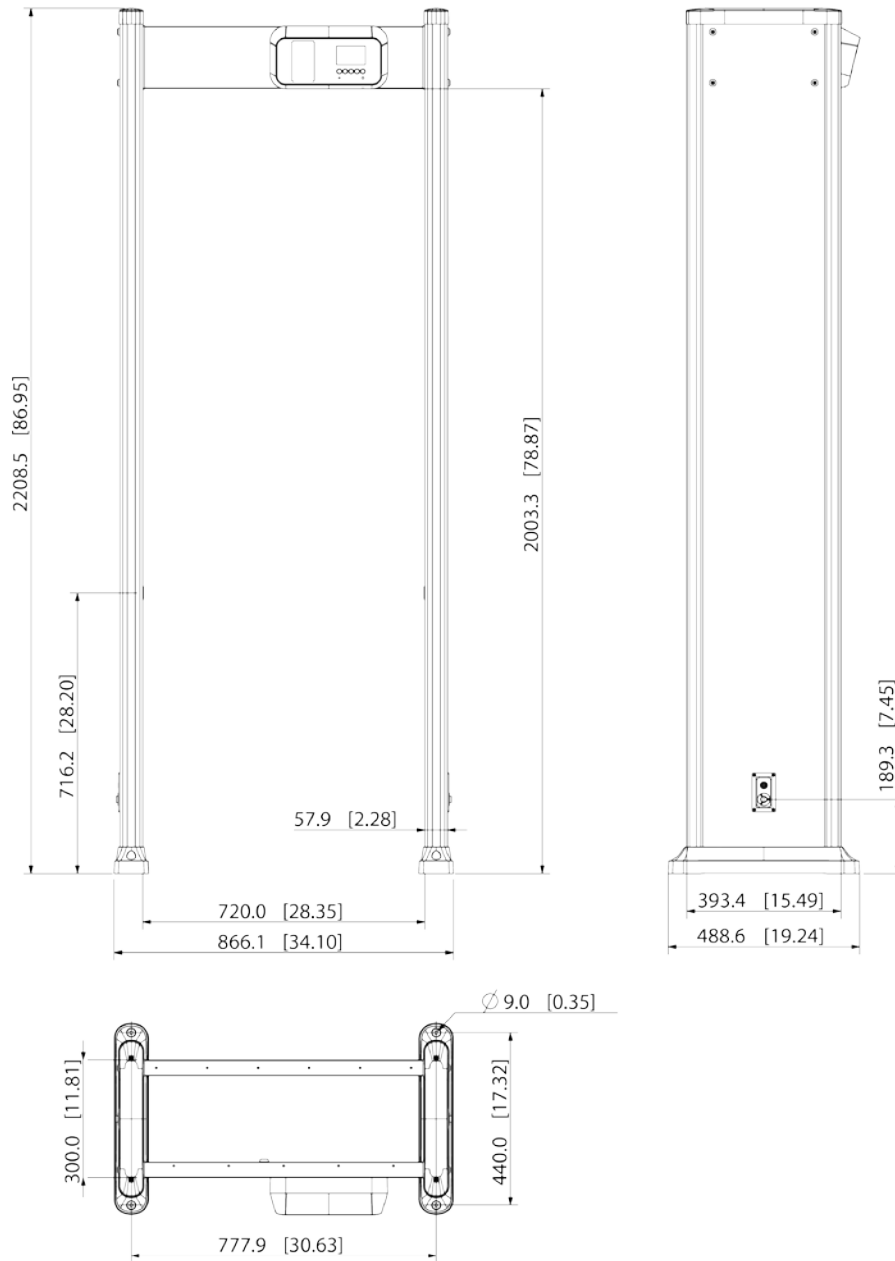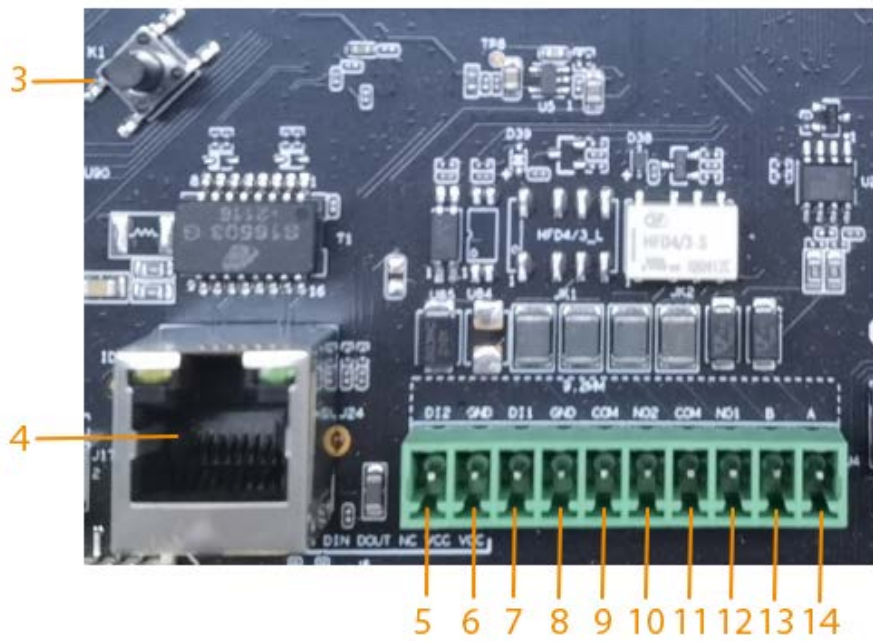
2.2 Port

Figure 2-2 Port (1)

Figure 2-3 Port (2)

Figure 2-4 Port (3)

Table 2-1 Port description

No.	Name	Description
1	Power supply switch	Turns on or off the Device.
2	Power input port	Connects to power cable to get power supply.
3	Reset button	Long press the button for more than 5 s to restore the detector to factory default.
4	Ethernet port	Connects to network with network cable.
5	Alarm in +	Receives the signal of external alarm source.
6	Alarm in–	
7	NC	Reserved port.
8		
9		
10		
11	Alarm out C	Outputs alarm signal to alarm device.
12	Alarm out NO	
13	RS-485 B	Controls external devices, such as PTZ.
14	RS-485 A	📖 ● Connect A and B cables (which both control RS-485) to devices such as PTZ cameras. ● If there are a large number of PTZ decoders, connect A and B cables to 120 Ω resistors.
15	DB25	Signal port for metal detection.
16	Power in	Inputs 12 VDC power. Be sure to supply power as instructed in the manual. ⚠ Device damage might occur if power is not supplied correctly.
17	Power out	Outputs 12 VDC power.

3 Installation

3.1 Checklist

After receiving the product, check against the table below. If there are any problems, contact the after-sales service personnel.

Table 3-1 Checklist

No.	List		Description
1	Overall packaging	Appearance	Obvious damage
		Packaging	Accidental impact
		Accessories	Complete or not
2	Host	Appearance	Obvious damage
		Model	Whether consistent with the order contract

Table 3-2 Packing list

Name	Quantity
Detector panel	2
Host box	1
Beam	2
Power cable (power input)	1
DB25 cable	2
Fixing screws (M6 × 16)	4
Fixing screws (M8 × 80)	8
Remote control	1
Wrench	1

3.2 Environment Requirements

- The ground is flat and sturdy
  The ground should be flat and firmly supporting to prevent vibration. If there is a vibrating metal structure under the ground, there can be unnecessary alarm when people pass through the metal detector.
  Do not install the detector on a metal ground.
- Keep away from fixed metal objects
  Large metal objects that are fixed or immobile should be at least 50 cm away from the detector (detecting large metal objects) because they might make the Device more susceptible to vibration.

The distance in this section is the recommended distance. The actual installation distance depends on the installation site conditions.

- Keep away from moving metal objects
  Large moving metal objects should be kept 0.5 m to 2 m away from the detector to avoid false alarms. Depending on the size of the metal object, the distance between the moving metal object and the detector might vary.
- Keep away from radioactive electronic interference
  The distance between the electronic interference source and the receiving coil should be as large as possible. The recommended minimum distance is 0.5 m to 4 m. However, the actual distance needs to be based on specific circumstances. For example, you can go through a metal detector with a source of interference until the best position is found. Interference can occur from electronic control panels, radios and computers, image displays, high-power motors and transformers, AC wires, transistor control circuits, flash fluorescent tubes, arc welding equipment, and more.
- Keep away from conductive electronic interference
  Connect the power cable to a line that is not connected to other large loads, such as high-power motors, because they can cause a large power or voltage shock in the line.

3.3 Installing Detector

Step 1   Open the packing box and take out the accessories.
Step 2   Open the front beam with the key, and then attach the host box to the front beam with four M6 × 16 screws.

Figure 3-1 Attach host box
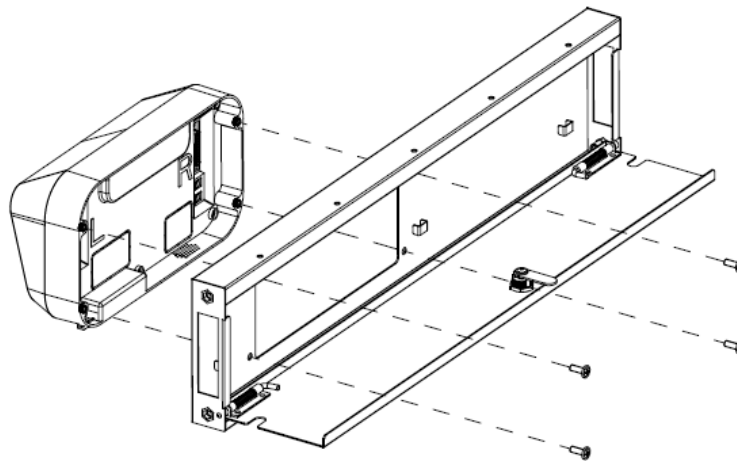
Step 3   Connect two DB25 cables and one power cable to the host box, and then separately run the two DB25 cables through the two holes at the two ends of the beam. Select one end of the beam, and then run the power cable.

Figure 3-2 Connect to host box
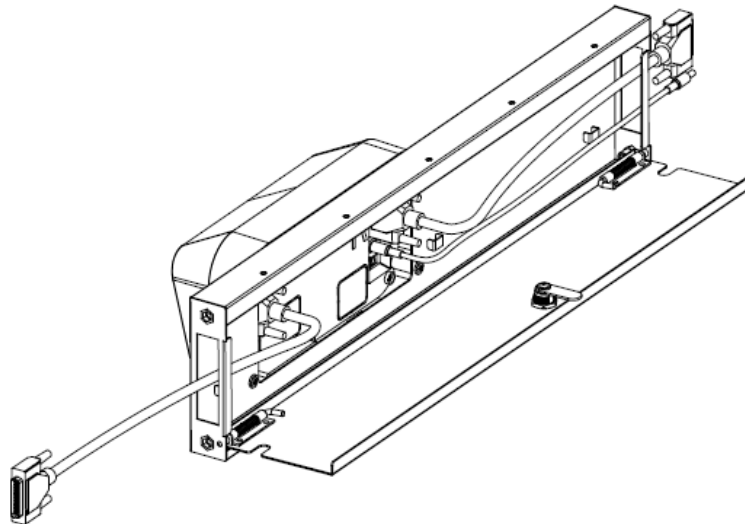
Step 4   Connect one end of the two DB25 cables and power cable to one detector panel, and then attach the front beam and rear beam to the detector panel with four M8 × 8 screws.
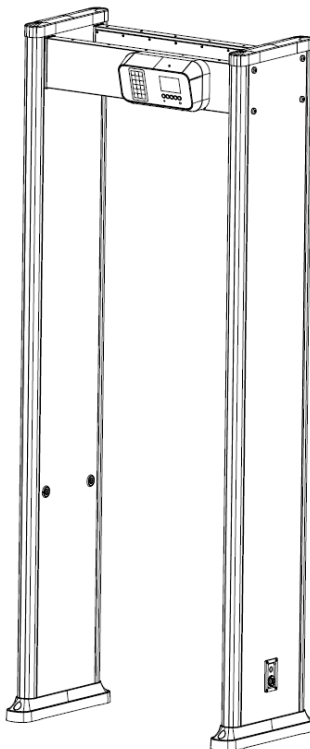
Figure 3-3 Attach beams (1)
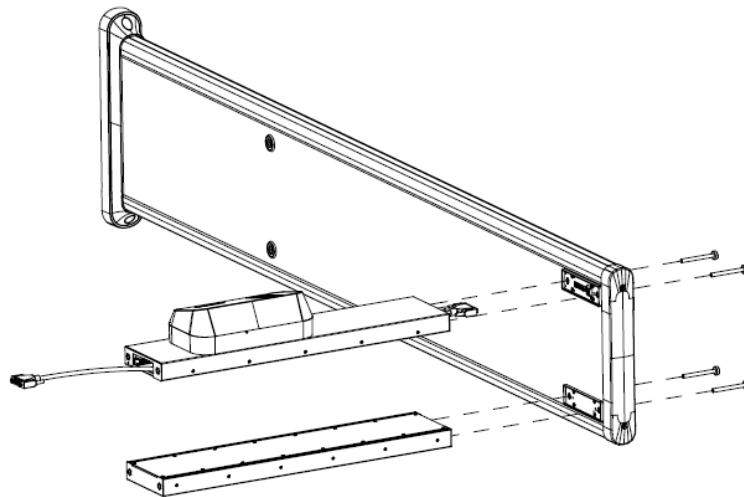
Step 5   Connect the other end of the two DB25 cables and power cable to one detector panel, and then attach the front beam and rear beam to the detector panel with four M8 × 8 screws.

Figure 3-4 Attach beams (2)
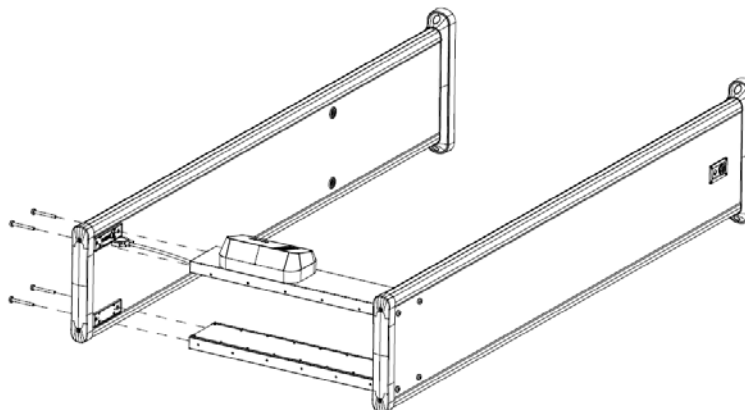
Step 6   Stand the Detector up.

Figure 3-5 Stand the Detector up

Step 7 Connect the power supply to the Detector, and then turn on the power switch to start the Detector.

3.4 Multiple Walk-through Detectors Site Installation

When installing multiple devices, space the devices at least 50 cm, and also space the device and X-ray security screening machine larger than 50 cm. This recommended spacing can make the little metal objects (such as coin) detected. If you install the devices with space smaller than 50 cm, there might be false alarm. If the spacing needs to be shorten because of limited installation site, you need to adjust the frequency, lower the security level and sensitivity according to the actual situation; otherwise, small metal objects might not be detected.

Figure 3-6 Multiple walk-through detectors site installation

d1=50
d2=50
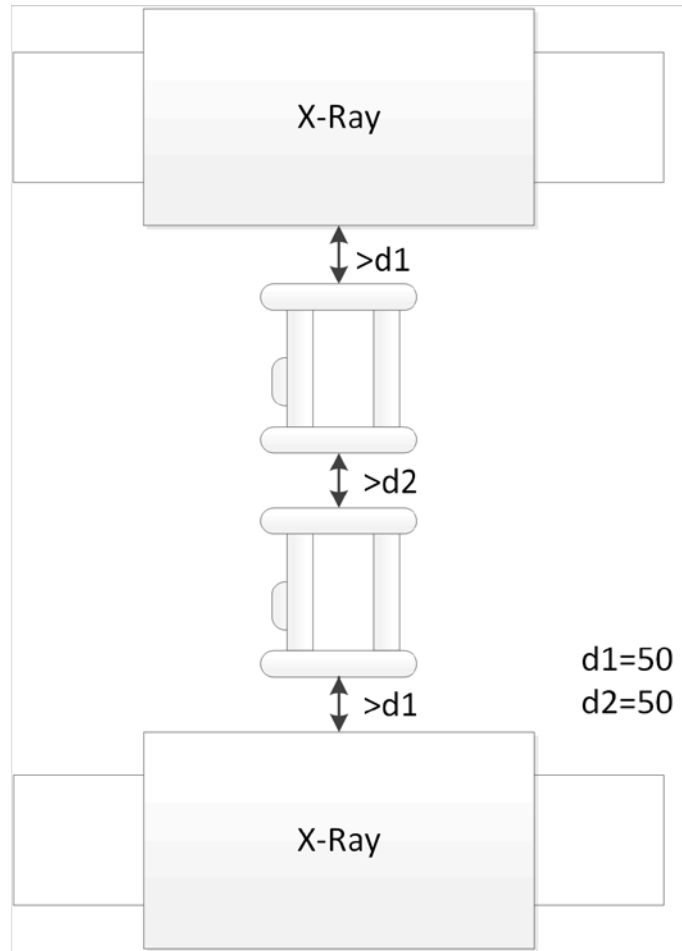
3.5 Stabilizing Detector

To make the Device work normally, stabilize the Device before use by tightening the fixing screws.

Figure 3-7 Tighten the fixing screws

4 Detector Configuration

4.1 Configuration Panel
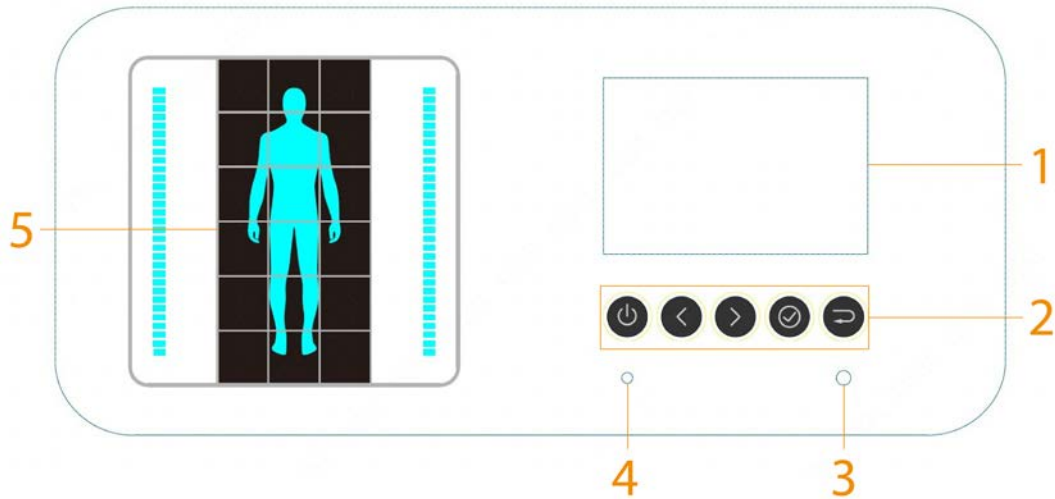
Figure 4-1 Configuration panel

Table 4-1 Configuration panel description

No.	Description
1	Displays number of passes, alarm times, signal strength bar, mode (normal, test, or alarm), current working frequency, volume and time. 📖 ● With increase of the detected metals, the color will grow from green to red. There are 10 degrees: Degree 1-4 is green, degree 5-7 is yellow, and degree 8-10 is red. When the degree is up to 8, an alarm will be triggered. ● Different colors of mode icon indicate different modes: 　◇ Yellow: Test mode. 　◇ Green: Normal mode. 　◇ Red: Alarm.
2	● Power switch. Turn on or off the Device. ● Press and hold the button for 3 s to clear the counting data.
	Select buttons. Press ⊘ or ⊘ to move the cursor.
	● Go to the parameter setting interface. ● Set parameter value. ● Confirm and save settings.
	Returns to the previous menu or exits the menu setting interface.
3	IR sensor.
4	Power indicator light.

No.	Description
5	Displays metal position indication with 18 indicators (red zone). 📖 This function is only available on 18-zone detectors.

4.2 Remote Control

You can set the parameters of the Device remotely through the remote control. Install the batteries before using the remote control.

Figure 4-2 Remote control

Table 4-2 Operation description

| No.	Name	Description
1	Power	Turn on or off the Device.
2	Reset	Press the button, and the number of passes and alarm times will be cleared.
3	Direction	● Press the buttons to switch and select menus. ● When setting a parameter, press left or right button to move the cursor, and then press up or down button to change the number or parameter value.
4	Confirm	● Go to the parameter setting interface. ● Confirm and save the setting.
5	Menu	Press the button to switch menus quickly. If the current parameter is the last one, press this button to switch to the first one.
6	Back	Returns to the previous menu or exits the menu setting interface.
7	Home	Go to the home page.

4.3 Detector Operations

4.3.1 Login

You can log in to the Device with the default password (000000). Change the password the first time you use it.

Procedure

Step 1   Connect the power supply, press the switch button.
          The main interface is displayed.
Step 2   Enter the password.
          Press ◀ or ▶ to move the cursor, and then press ⊘ to set the number.
Step 3   Press ▶ to move the cursor to **OK**, and the press ⊘ to confirm the password.
          If the password is wrong, the error note will be displayed.

Figure 4-3 Password error

Passwords err,PLZ enter again.
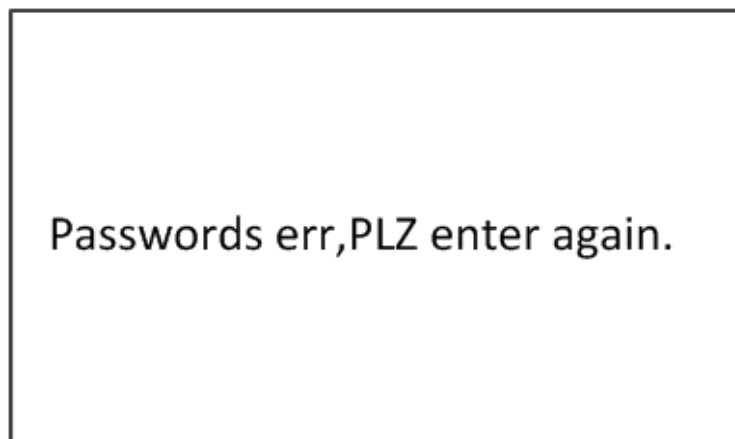
Related Operations

If you forget the password, long press the reset button for more than 5 s to restore the Detector, and then the Detector restarts.

4.3.2 Setting Sensitivity

Sensitivity can be set separately for each zone. It ranges from 0 to 255. The higher the value is, the more sensitive the Device is.
Step 1   Log in to the Detector. For details, see "4.3.1 Login".

Figure 4-4 Sensitivity setting

```
Counter    Date&Time    Audio

Frequency  Sensitivity  Program

System     Password     Restore
```
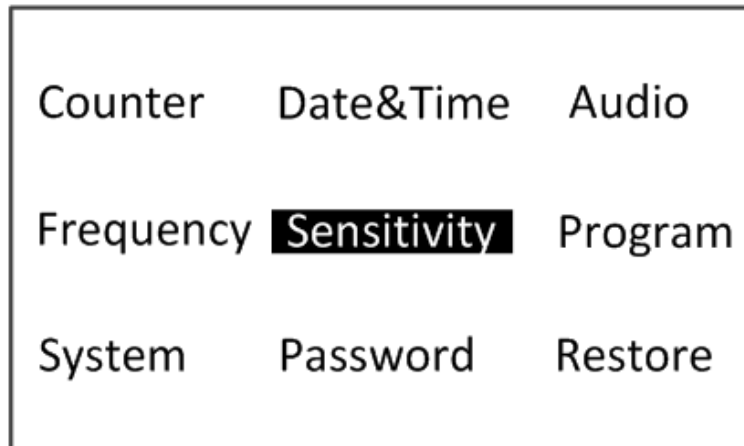
Step 2   Press ◁ or ▷ to move the cursor to **Sensitivity**, and then press ⊘ to go to the sensitivity setting interface.

Figure 4-5 Set sensitivity

```
L6Zo:221   R6Zo:221   Security
L5Zo:221   R5Zo:221   Level:060
L4Zo:221   R4Zo:231
L3Zo:221   R3Zo:231
L2Zo:221   R2Zo:221
L1Zo:221   R1Zo:221
                           OK
```
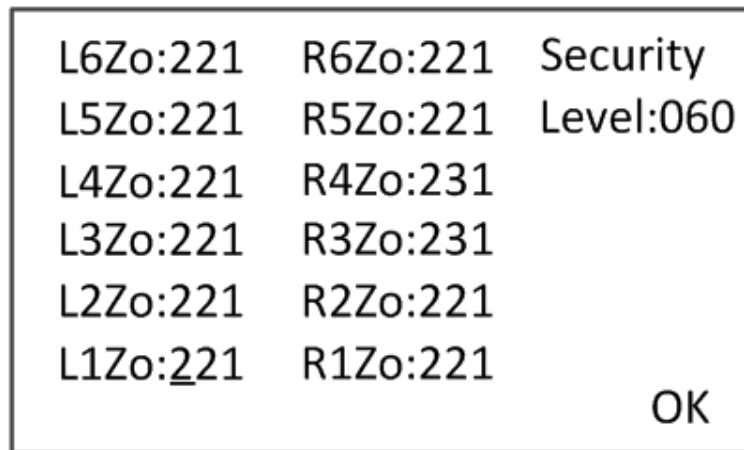
Step 3   Select the zone that needs to be set, and then set sensitivity.

Press ◁ or ▷ to move the cursor to a zone (for example, L1Zo), and then press ⊘ to set the value.

- L1Zo–L6Zo: The detection sensitivity of left detector panel (models with 12 zones and 18 zones) and models with 6 zones.
- R1Zo–R6Zo: The detection sensitivity of right detector panel (models with 12 zones and 18 zones).

Figure 4-6 Setting security level

| 6zones | 12zones | 18zones |
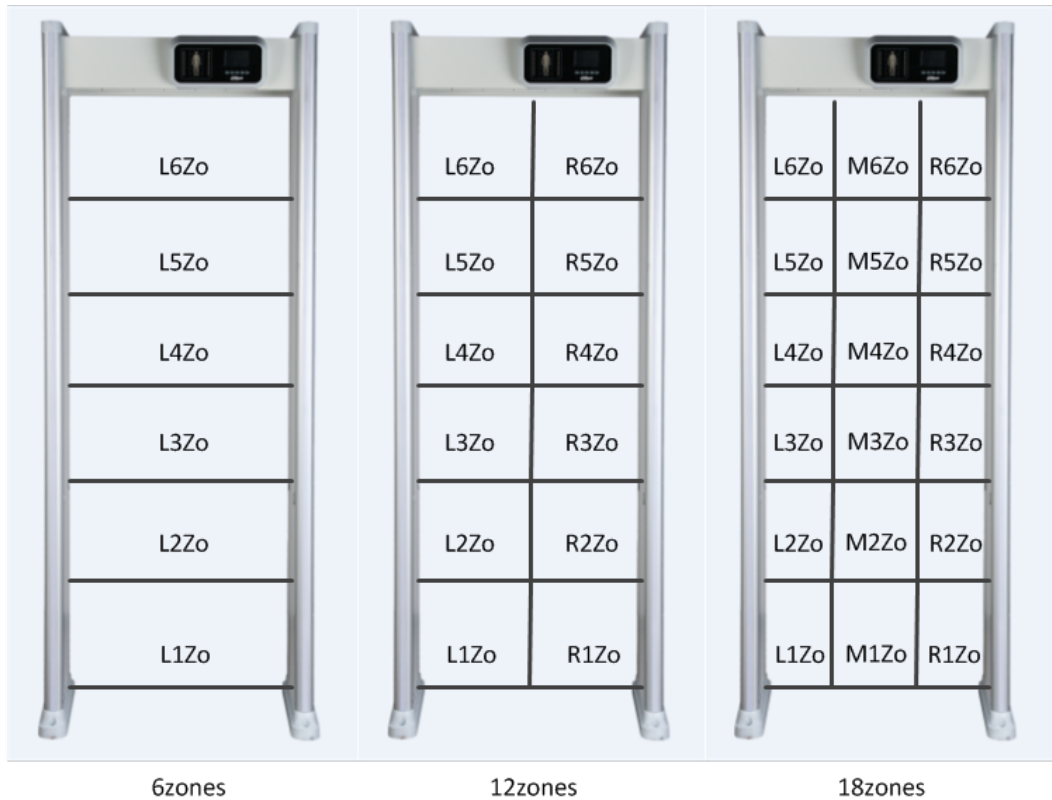
Step 4 Press ⊙ to move the cursor to **OK**, and then press ⊙ to save the setting.

Result

When both the defined threshold of security level and sensitivity are reached, an alarm will be triggered.

When both the defined threshold of security level and sensitivity are reached, an alarm will be triggered. For the details of sensitivity, see #d246e7a1026.

4.3.3 Setting Frequency

Electromagnetic interference from ambient environment varies with different frequencies. The frequency for lower interference makes the Device have higher sensitivity. When multiple devices work simultaneously, set different frequencies for each device to reduce mutual interference.

The Device can search the frequency for lowest interference, and sets it to the working frequency. You can also set the frequency manually. It ranges from 1 to 20.

Step 1 Log in to the Detector. For details, see "4.3.1 Login".

Step 2 Press ⊙ or ⊙ to move the cursor to **Frequency**, and then press ⊙ to go to the frequency setting interface.

Figure 4-7 Frequency setting
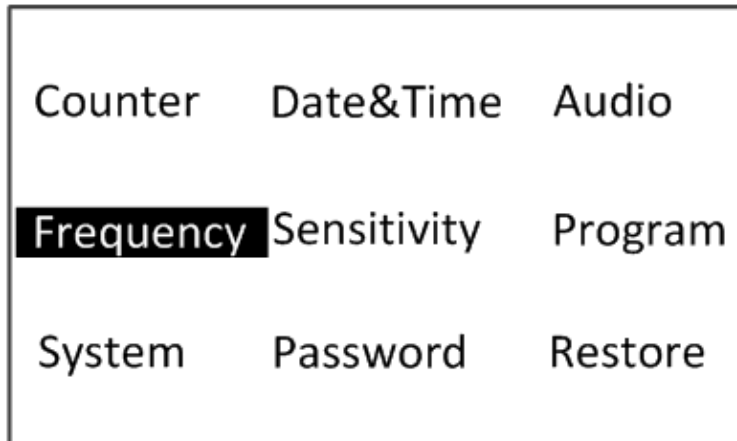
Step 3   Set the frequency.

- Auto search frequency: Press ⬅ or ➡ to move the cursor, and press ⊙ to enable the auto search frequency function. The Device will set the suitable working frequency automatically. If the working frequency still needs to be adjusted, you can set the value manually.

  📖

  ◇ Do not pass or approach to the detector during auto searching.
  ◇ Alarm might be triggered during auto searching. Auto-searching function lasts about 2 minutes

- Set frequency manually: When the auto search frequency function is disabled, press ⬅ or ➡ to move the cursor, and then press ⊙ to set the value manually.

Figure 4-8 Set frequency
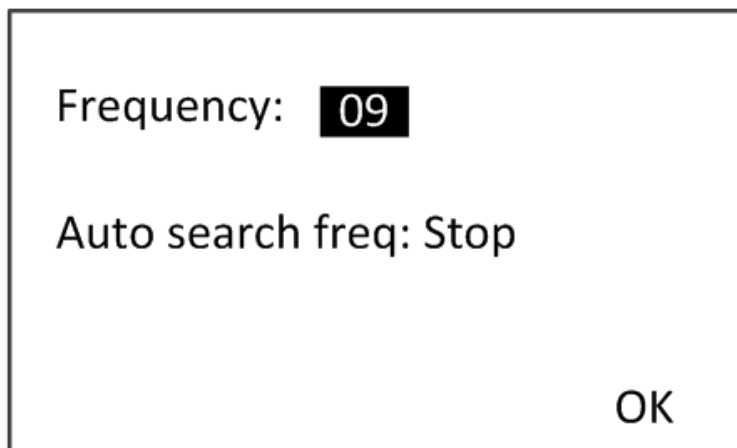
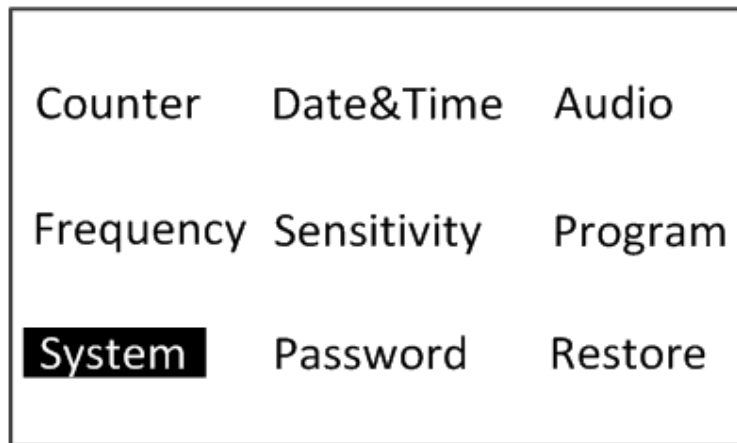Step 4   Press ➡ to move the cursor to **OK**, and then press ⊙ to save the setting.

4.3.4 Setting Temperature Overlay

After you enable the temperature overlay function, body temperature and the number of temperature alarms will be displayed on the screen.

Step 1   Log in to the Detector. For details, see "4.3.1 Login".

Step 2   Press ⬅ or ➡ to move the cursor to **System**, and then press ⊙.

Figure 4-9 System

Step 3   Press ◀ or ▶ to move the cursor to **Alarm**, and then press ⊘.

Figure 4-10 Alarm
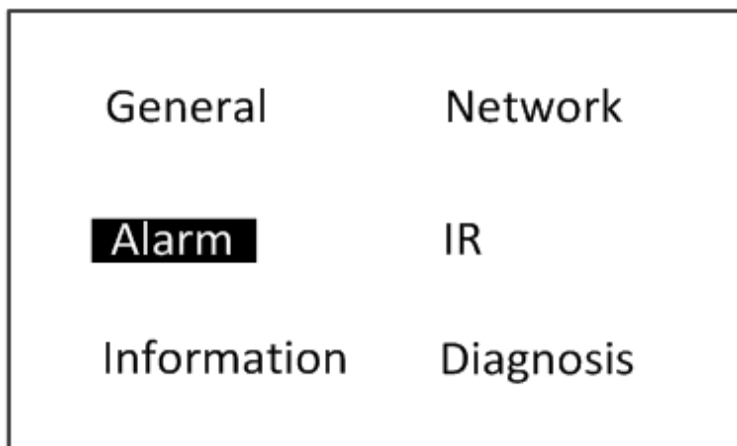
Step 4   Press ◀ or ▶ to move the cursor to **ON**, and then press ⊘ to enable the
          temperature overlay function.

          📖

          Press ▶, **ON** becomes **OFF**, and then press ⊘ to disable the function.

Figure 4-11 Set Temp Overlay
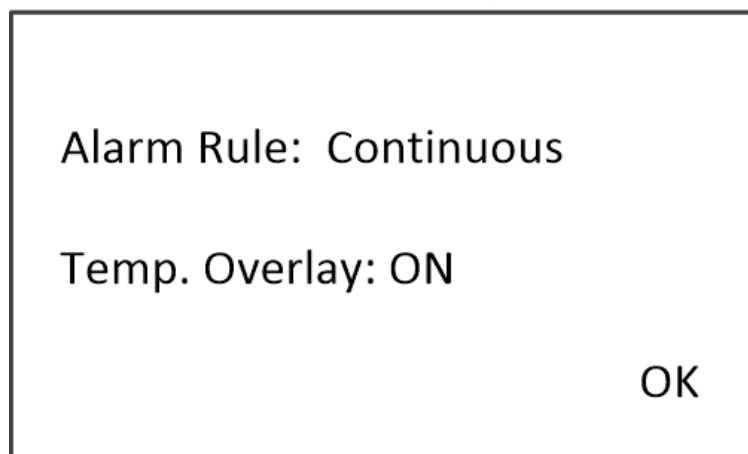
Step 5   Press ◀ or ▶ to move the cursor to **OK**, and then press ⊘. Body temperature and
          the total number of temperature alarms are displayed on the screen.
          When the body temperature is normal, the words on the screen are white and the duration
          is 1 s. When the body temperature is abnormal, the words are red and the duration is 3 s.

Figure 4-12 Temperature Alarm

Face Temp.:37.2℃

Temp. Alarm:101

Appendix 1 Cybersecurity Recommendations

Mandatory actions to be taken for basic equipment 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 equipment (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 equipment 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 equipment network security:

1. **Physical Protection**

   We suggest that you perform physical protection to equipment, especially storage devices. For example, place the equipment 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 equipment (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 equipment, 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 equipment 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 equipment, 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 equipment 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.