

Body Thermometer and Metal Detector Security Gate Quick Guide

Contents

1 Packing List	1
2 Note	1
3 Introduction	2
3.1 Appearances and dimensions	2
3.2 Structure	4
4 Device Installation	6
4.1 Installation environment	6
4.2 Preparation	7
4.3 Cable connection	7
4.4 Installation	8
5 Device Startup	14
6 Device Configuration	14
7 FAQ	16

1 Packing List

No.	Name	Qty	Unit
1	Door panel	2	PCS
2	Control unit	1	PCS
3	Crosspiece	1	PCS
4	Hex key	1	PCS
5	Bolts	8	PCS
6	Remote control	1	PCS
7	Power cable	1	PCS
8	Data cable	2	PCS
9	Keys	2	PCS
10	User manual	1	Set

2 Note

- The device contains high voltage. Only trained technicians are allowed to disassemble the device.
- Knocking or smashing the device may cause false alarms.
- Metallic objects (such as keys, mobile phones, coins) must be removed and put aside before people walk through the gate.
- People must walk through the gate one by one. A crowd of people standing around the gate may affect the detection.
- The person behind must wait till the person in front completely passes through the gate without setting off an alarm. If an alarm is set off, the person behind must wait till the alarm stops.
- An alarm sound means metal is detected.

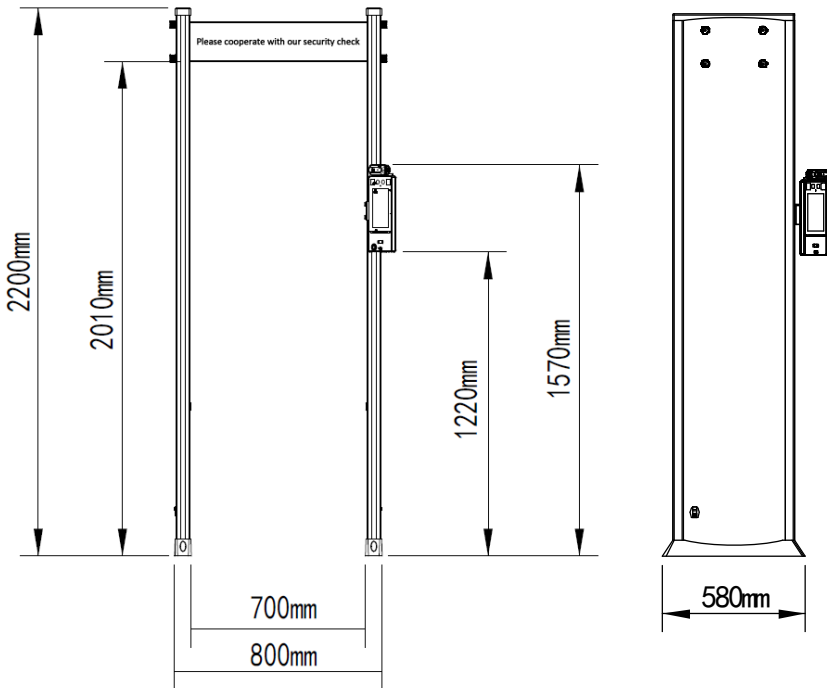
3 Introduction

This security gate can detect metals and measure body temperatures when people walk through. When an abnormal body temperature is detected, an alarm is displayed on the face recognition access control terminal. When metal is detected, the gate sounds an alarm and indicates the detection zone. Alarms can be reported to the access control system to alert security personnel.

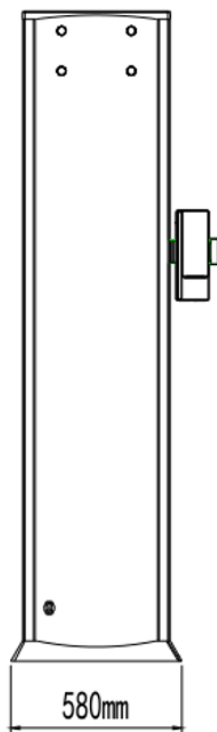
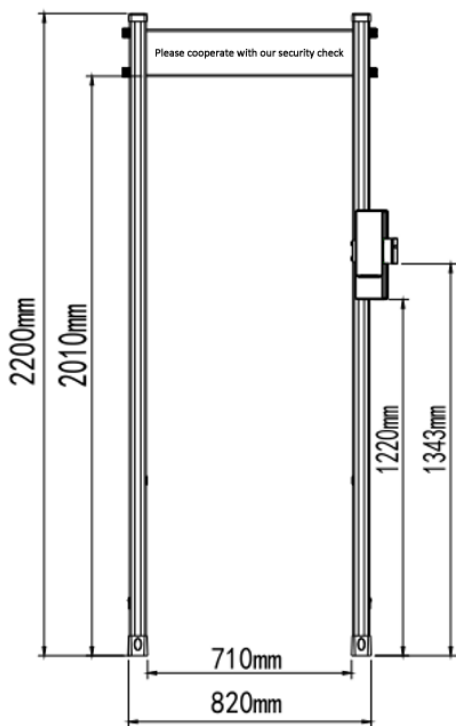
3.1 Appearances and dimensions

The appearances and dimensions vary with device model.

Appearance and dimensions 1

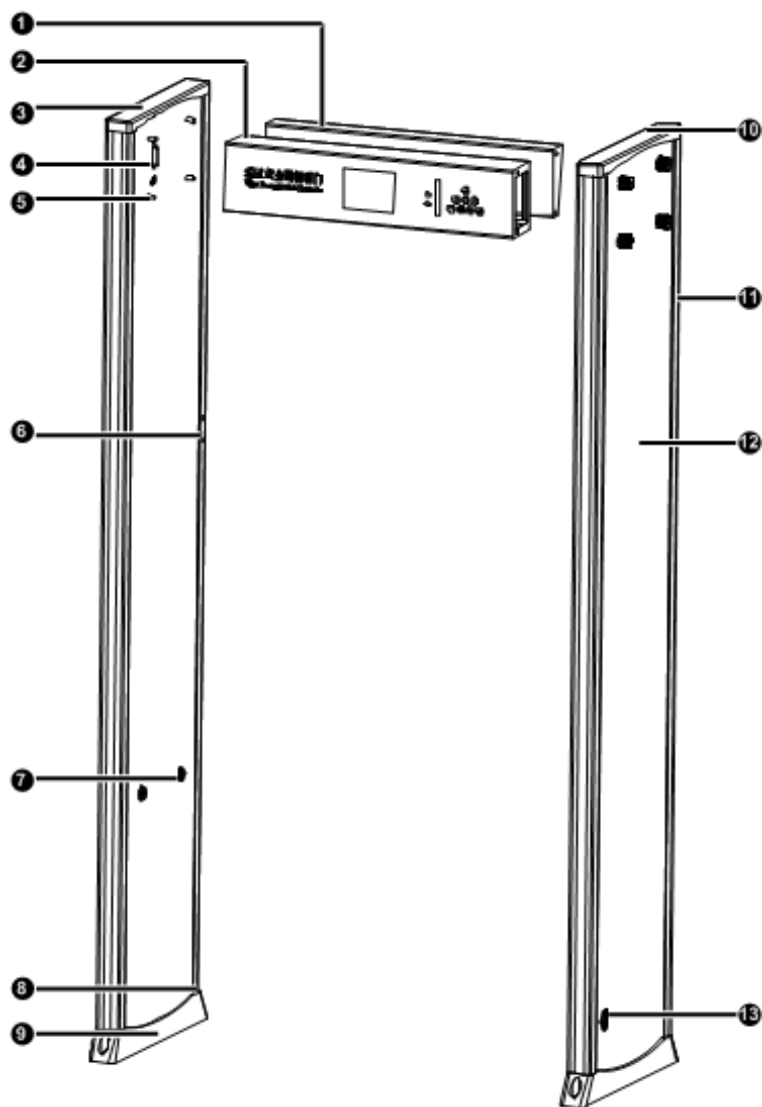


Appearance and dimensions 2



3.2 Structure

1 Parts

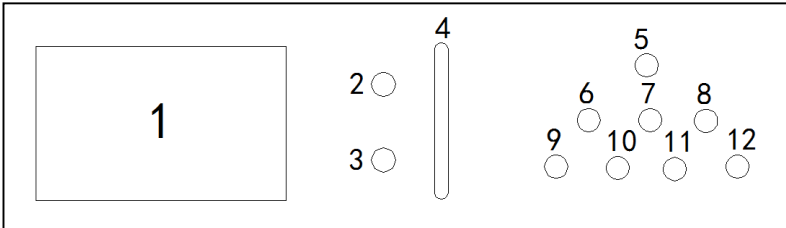






1. Crosspiece	2. Control unit
3. Right panel	4. Wiring terminal
5. Fixing hole	6. Fixing hole/wiring terminal for access control bracket

7. Infrared sensor	8. Network cable inlet
9. Waterproof foot cover	10. Left panel
11. Alarm zone LED	12. Built-in probe
13. 220V power cable interface	

2 Control panel

The control panel is described as follows.



Item	Name	Description
1	LCD display	Displays the number of people walking through and the number of alarms.
2	Standby indicator	Green: Standby Off: Alarm
3	Alarm indicator	Red: Alarm
4	Signal interference indicator	Indicates the current environment interference
5		Access the upper-level menu or increase value when setting password.
6		Adjustment key, increase parameter value.
7		Access the lower-level menu or decrease value when setting password.
8		Adjustment key, decrease parameter value.
9	MENU	Access the menu.
10	ENTER	Save settings and exit the menu, or access an item.
11	EXIT	Exit the menu without saving settings.
12	RESET	Reset button. Pressing and holding the button for 5s will start or shut down the device.

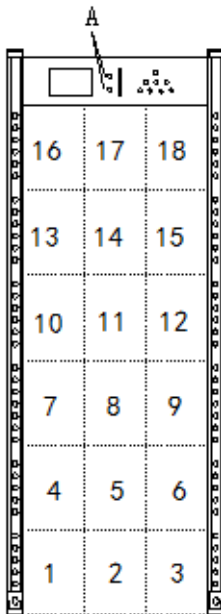


NOTE!

The buttons on the remote control are basically the same as the buttons on the control panel. For more information about using the remote control, see the above descriptions for reference.

3 Detection zones

Both the left and right panels have 6 sets of pinpoint LEDs for 18 detection zones, as shown in the figure below. A detection zone LED is either on or off. When a metallic object is detected, a detection zone LED turns on and the alarm sounds.



4 Device Installation

4.1 Installation environment

The installation environment shall meet the following requirements in order to avoid false alarms.

- The gate is at least 0.5m away from large stationary or fixed metallic objects such as aluminum windows.

- The gate is at least 5m away from large mobile metallic objects such as elevators, cars and rolling gates.
 - The floor or ground must be smooth and firm, and strong wind must be avoided in the environment.
 - The gate is kept away from sources of electromagnetic interference and electromagnetic radiation. A minimum distance of 1m is recommended.
 - For side-by-side installations, ensure a minimum distance of 50cm between the gates.
-



NOTE!

The recommended distance from interference sources is only for reference. Adjust the distance appropriately according to factors such as metal area size and electromagnetic signal strength.

4.2 Preparation

Tools

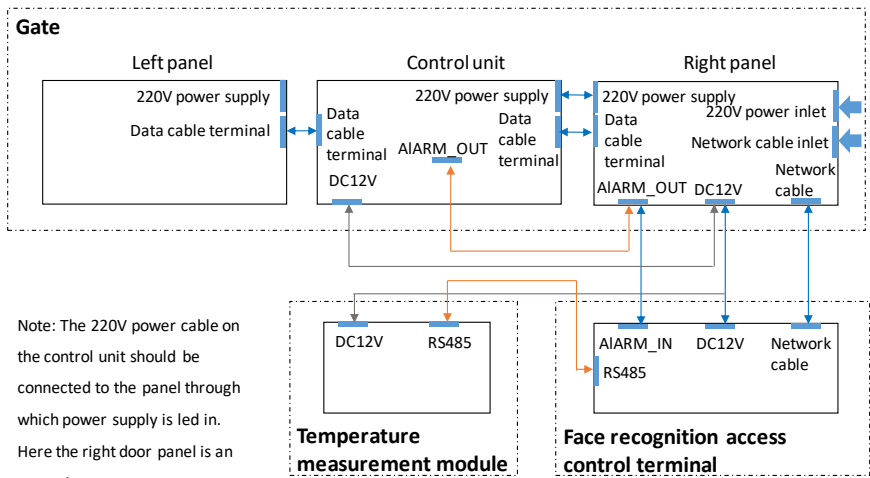
- Cross screwdriver
- Antistatic wrist strap or antistatic gloves
- Hex key

Documentation

Open the Digital Temperature Measurement Module Quick Guide and the Face Recognition Access Control Terminal Quick Guide in the package.

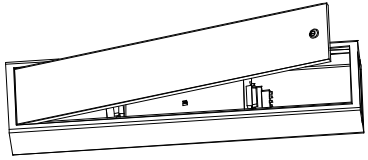
4.3 Cable connection

See the illustration below to connect cables for the gate, temperature measurement module and face recognition access control terminal. See the corresponding quick guides for information about wiring terminals of the temperature measurement module and face recognition access control terminal.

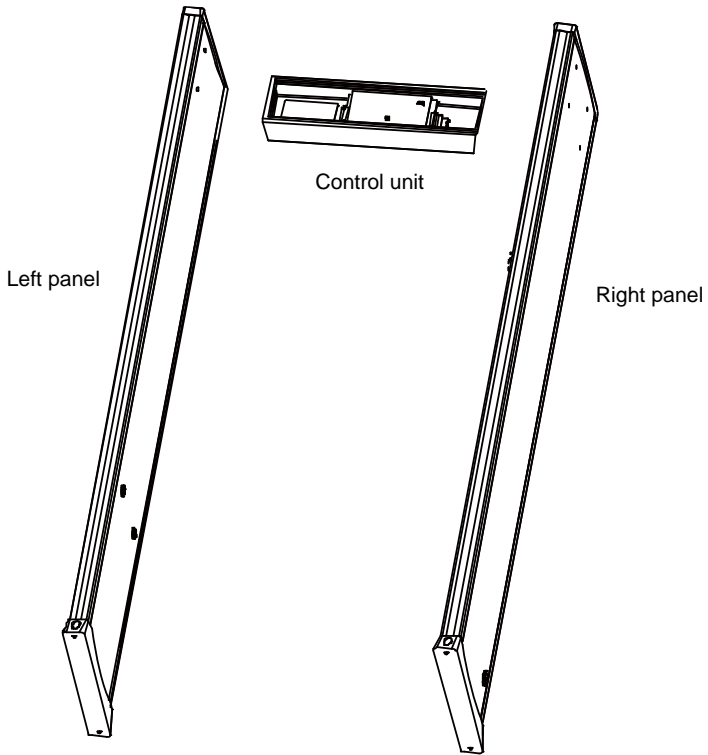


4.4 Installation

1. Unpack the control unit and door panels.
2. Use the shipped key to open the rear cover plate of the control unit.



3. Place the control unit (facing downward), left and right panels as shown in the figure below.



NOTE!

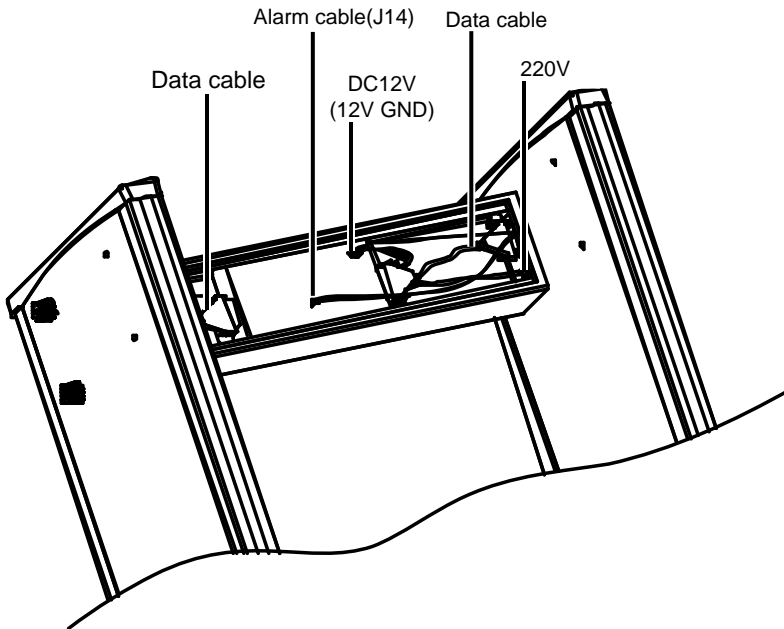
The right panel has installation holes for the temperature measurement module and the face recognition access control terminal.

4. Follow the steps to connect cables for the control unit and door panels:
 - (1) Connect the control unit and both panels with data cables. The data cables are shipped with the device.
 - (2) Connect the control unit and the right panel with the 220V power cable.
 - (3) Connect the DC 12V power cable (12V GND) and the alarm cable (J14) on the right panel to the wiring terminals on the control unit.

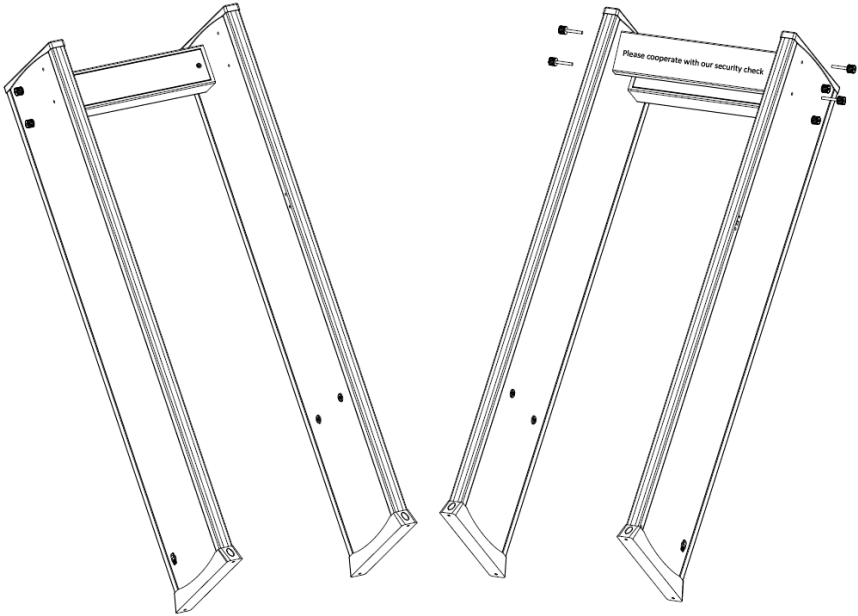


NOTE!

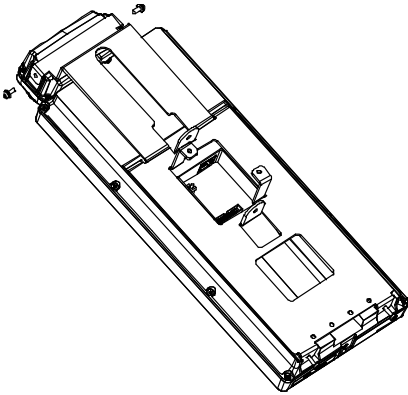
- The power cable on the control unit should be connected to the panel through which power supply is led in. The figure below takes the right panel as an example.
 - Make sure all the cables are securely connected.
-



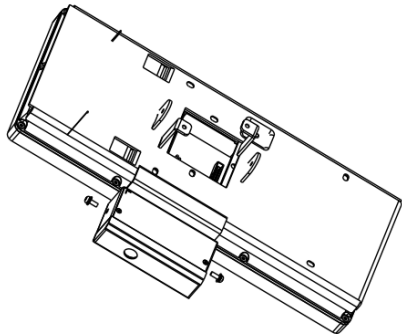
5. Close the rear cover plate on the control unit and use the supplied bolts to secure the control unit and the crosspiece.



6. Lift the gate vertically and move it to the intended position.
7. Fix the temperature measurement module and the face recognition access control terminal to the bracket. Refer to the Digital Temperature Measurement Module Quick Guide and the Face Recognition Access Control Terminal Quick Guide for more information.



Mount option 1



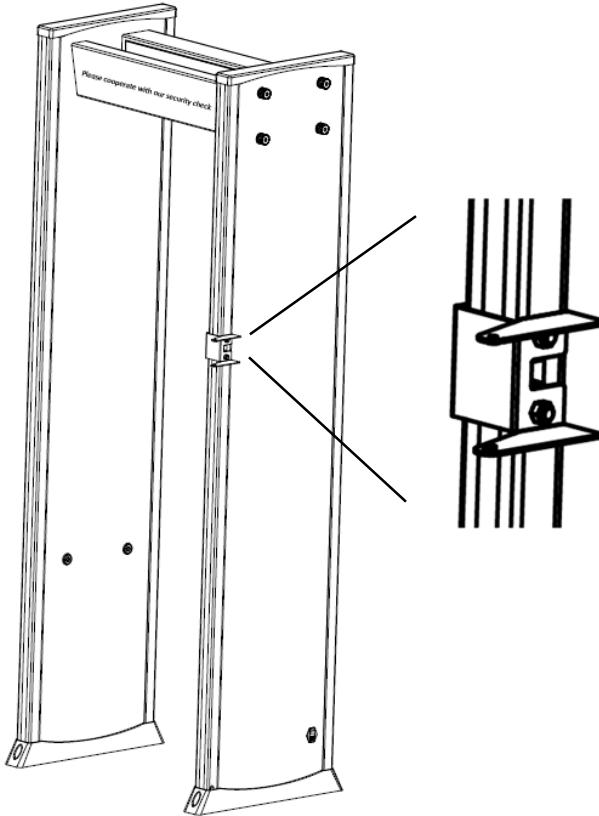
Mount option 2



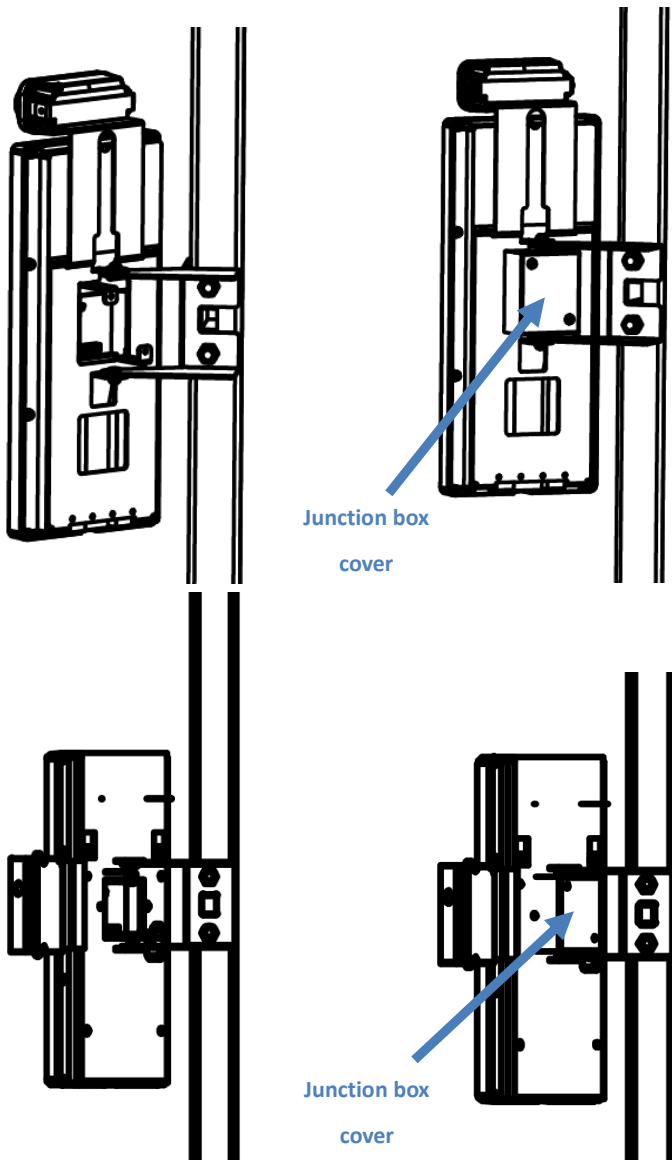
NOTE!

- Use a separately supplied bracket. Do not use the bracket shipped with the face recognition access control terminal.
 - Complete cable connections (RS485 and DC12V) between the temperature measurement module and the face recognition access control terminal first.
-

8. Secure the bracket to the right panel.



9. Secure the temperature measurement module and the face recognition access control terminal to the bracket on the right panel, and then close the junction box.



NOTE!

Before installation, please complete cable connections (DC12V cable, alarm cable and network cable) between the temperature measurement module, face recognition access control terminal and the gate.

10. (Optional) Draw a line 50cm in front of and behind the gate so people can wait behind the line and pass through the gate one by one.

5 Device Startup

After installation is completed, connect one end of the supplied power cable to the 220V power socket on the right panel, and connect the other end of the power cable to the mains. Turn on the power switch on the right panel to power on. The following is displayed on the LCD screen:

```
PASS CNT  000000
ALARMCNT 000000
```



NOTE!

After startup, the device makes a self-test to achieve the best detection performance. The self-test takes about one minute.

Device adjustment

The device achieves the best detection performance when in stable status. The device is stable if these requirements are met:

1. The device is steady (no shaking) after completing the self-test.
2. Walk through the gate without carrying any metallic items, and no alarm is set off.

6 Device Configuration

Use the menu to set zone sensitivity, alarm duration, operating frequency, language, and detector ID.


Press MENU on the control panel or remote control and then input the password to access the menu. Configure the device in accordance with descriptions in the Control panel section.



NOTE!

The default password is 1234. If you forgot your password, you can enter the universal password 8888 to reset a new password.

1.SETTING
1.SENSITIVITY LEVEL 2.ALARM DELAY 3.FREQUENCY SPAN 4.QUICK SETTING 5.SELECT LANGUAGE 6.DETECTOR ID 7.CHANGE PASSWORD 8.RESTORE TO DEFAULT 9.VOLUME

No.	Item	Description
1	SENSITIVITY LEVEL	Set sensitivity for all detection zones. A greater value means higher sensitivity. Range: 0-255. Default: 235. Note The positions of detection zones are described in Detection zones. Sensitivity is set for a group of 3 zones, for example, Zone 1-3, 4-6, etc.
		Press and hold  for 7s to set total sensitivity. A smaller value means higher sensitivity. Range: 5-50. Default: 40.
2	ALARM DELAY	Range: 1-3s. Default: 1.
3	FREQUENCY SPAN	Range: 1-12.
4	QUICK SETTING	Choose a scene for your gate. 10 options are available: NIGHTCLUB/COURT/HARDWARE FACTORY/SCHOOL/HOSPITAL/BARRACKS, EMBASSY/EXHIBITION HALL/AIRPORT, STATION, CUSTOMS/PRECIOUS METALS, ELECTRONICS/PRISON
5	SELECT LANGUAGE	中文 or ENGLISH.
6	DETECTOR ID	This setting is effective when the device is connected to network.
7	CHANGE PASSWORD	Enter the new 4-digit password.

8	RESTORE TO DEFAULT	Restore factory default settings.
9	VOLUME	NONE or HIGH. Default: HIGH.

7 FAQ

Question/Problem	Answer/Solution
How to prevent small metallic objects (e.g., rings, keys) from triggering alarms?	<ol style="list-style-type: none"> 1. Choose a small metallic object such as a key to test the minimum sensitivity that won't trigger an alarm. 2. Set a high sensitivity so that walking through the gate with the key will trigger an alarm. 3. Decrease the sensitivity gradually and test till the key does not trigger any alarms. <p>NOTE If sensitivity in a detection zone is too high, lower sensitivity for that zone.</p>
Counting failed.	<ol style="list-style-type: none"> 1. Check that data cables are well connected in the control unit for the infrared sensors. 2. Check for infrared interference around the gate, for example, infrared surveillance system, infrared remote control (when in used), outdoor sunlight. 3. Replace the infrared sensors if the problem still exists.
Frequent false alarms.	<ol style="list-style-type: none"> 1. Check if there are any large moving or stationary metallic objects around the gate. 2. Check if it is the wind that causes the false alarms. 3. Check if there is any frequency conversion equipment around. 4. Decrease sensitivity for all detection zones. If the problem still exists, change the frequency of the device. 5. Change the installation location if the problem still exists,.

Copyright Statement

©2020 Zhejiang Uniview Technologies Co., Ltd. All rights reserved.

No part of this manual may be copied, reproduced, translated or distributed in any form by any means without prior content in writing from Zhejiang Uniview Technologies Co., Ltd (referred to as Uniview or us hereafter).

The product described in this manual may contain proprietary software owned by Uniview and its possible licensors. Unless permitted by Uniview and its licensors, no one is allowed to copy, distribute, modify, abstract, decompile, disassemble, decrypt, reverse engineer, rent, transfer, or sublicense the software in any form by any means.

Trademark Acknowledgements

 are trademarks or registered trademarks of Uniview.

All other trademarks, products, services and companies in this manual or the product described in this manual are the property of their respective owners.

Export Compliance Statement

Uniview complies with applicable export control laws and regulations worldwide, including that of the People's Republic of China and the United States, and abides by relevant regulations relating to the export, re-export and transfer of hardware, software and technology. Regarding the product described in this manual, Uniview asks you to fully understand and strictly abide by the applicable export laws and regulations worldwide.

Privacy Protection Reminder

Uniview complies with appropriate privacy protection laws and is committed to protecting user privacy. You may want to read our full privacy policy at our website and get to know the ways we process your personal information. Please be aware, using the product described in this manual may involve the collection of personal information such as face, fingerprint, license plate number, email, phone number, GPS. Please abide by your local laws and regulations while using the product.

About This Manual

- This manual is intended for multiple product models, and the photos, illustrations, descriptions, etc, in this manual may be different from the actual appearances, functions, features, etc, of the product.
- This manual is intended for multiple software versions, and the illustrations and descriptions in this manual may be different from the actual GUI and functions of the software.
- Despite our best efforts, technical or typographical errors may exist in this manual. Uniview cannot be held responsible for any such errors and reserves the right to change the manual without prior notice.
- Users are fully responsible for the damages and losses that arise due to improper operation.
- Uniview reserves the right to change any information in this manual without any prior notice or indication. Due to such reasons as product version upgrade or regulatory requirement of relevant regions, this manual will be periodically updated.

Disclaimer of Liability

- To the extent allowed by applicable law, in no event will Uniview be liable for any special, incidental, indirect, consequential damages, nor for any loss of profits, data, and documents.
- The product described in this manual is provided on an "as is" basis. Unless required by applicable law, this manual is only for informational purpose, and all statements, information, and recommendations in this manual are presented without warranty of any kind, expressed or implied, including, but not limited to, merchantability, satisfaction with quality, fitness for a particular purpose, and noninfringement.
- Users must assume total responsibility and all risks for connecting the product to the Internet, including, but not limited to, network attack, hacking, and virus. Uniview strongly recommends that users take all necessary measures to enhance the protection of network, device, data and personal information. Uniview disclaims any liability related thereto but will readily provide necessary security related support.
- To the extent not prohibited by applicable law, in no event will Uniview and its employees, licensors, subsidiary, affiliates be liable for results arising out of using or inability to use the product or service, including, not limited to, loss of profits and any other commercial damages or losses, loss of data, procurement of substitute goods or services; property damage, personal injury, business interruption, loss of business information, or any special, direct, indirect, incidental, consequential, pecuniary, coverage, exemplary, subsidiary losses, however caused and on any theory of liability, whether in contract, strict liability or tort (including negligence or otherwise) in any way out of the use of the product, even if Uniview has been advised of the possibility of such damages (other than as may be required by applicable law in cases involving personal injury, incidental or subsidiary damage).
- To the extent allowed by applicable law, in no event shall Uniview's total liability to you for all damages for the product described in this manual (other than as may be required by applicable law in cases involving personal injury) exceed the amount of money that you have paid for the product.

Network Security

Please take all necessary measures to enhance network security for your device.

The following are necessary measures for the network security of your device:

- **Change default password and set strong password:** You are strongly recommended to change the default password after your first login and set a strong password of at least nine characters including all three elements: digits, letters and special characters.
- **Keep firmware up to date:** It is recommended that your device is always upgraded to the latest version for the latest functions and better security. Visit Uniview's official website or contact your local dealer for the latest firmware.

The following are recommendations for enhancing network security of your device:

- **Change password regularly:** Change your device password on a regular basis and keep the password safe. Make sure only the authorized user can log in to the device.
- **Enable HTTPS/SSL:** Use SSL certificate to encrypt HTTP communications and ensure data security.
- **Enable IP address filtering:** Allow access only from the specified IP addresses.
- **Minimum port mapping:** Configure your router or firewall to open a minimum set of ports to the WAN and keep only the necessary port mappings. Never set the device as the DMZ host or configure a full cone NAT.
- **Disable the automatic login and save password features:** If multiple users have access to your computer, it is recommended that you disable these features to prevent unauthorized access.
- **Choose username and password discretely:** Avoid using the username and password of your social media, bank, email account, etc, as the username and password of your device, in case your social media, bank and email account information is leaked.
- **Restrict user permissions:** If more than one user needs access to your system, make sure each user is granted only the necessary permissions.
- **Disable UPnP:** When UPnP is enabled, the router will automatically map internal ports, and the system will automatically forward port data, which results in the risks of data leakage. Therefore, it is recommended to disable UPnP if HTTP and TCP port mapping have been enabled manually on your router.
- **SNMP:** Disable SNMP if you do not use it. If you do use it, then SNMPv3 is recommended.
- **Multicast:** Multicast is intended to transmit video to multiple devices. If you do not use this function, it is recommended you disable multicast on your network.
- **Check logs:** Check your device logs regularly to detect unauthorized access or abnormal operations.
- **Physical protection:** Keep the device in a locked room or cabinet to prevent unauthorized physical access.
- **Isolate video surveillance network:** Isolating your video surveillance network with other service networks helps prevent unauthorized access to devices in your security system from other service networks.

Learn More

You may also obtain security information under Security Response Center at Uniview's official website.

Safety Warnings

The device must be installed, serviced and maintained by a trained professional with necessary safety knowledge and skills. Before you start using the device, please read through this guide carefully and make sure all applicable requirements are met to avoid danger and loss of property.

Storage, Transportation, and Use

- Store or use the device in a proper environment that meets environmental requirements, including and not limited to, temperature, humidity, dust, corrosive gases, electromagnetic radiation, etc.
- Make sure the device is securely installed or placed on a flat surface to prevent falling.
- Unless otherwise specified, do not stack devices.
- Ensure good ventilation in the operating environment. Do not cover the vents on the device. Allow adequate space for ventilation.
- Protect the device from liquid of any kind.
- Make sure the power supply provides a stable voltage that meets the power requirements of the device. Make sure the power supply's output power exceeds the total maximum power of all the connected devices.
- Verify that the device is properly installed before connecting it to power.
- Do not remove the seal from the device body without consulting Uniview first. Do not attempt to service the product yourself. Contact a trained professional for maintenance.
- Always disconnect the device from power before attempting to move the device.
- Take proper waterproof measures in accordance with requirements before using the device outdoors.

Power Requirements

- Installation and use of the device must be in strict accordance with your local electrical safety regulations.
- Use a UL certified power supply that meets LPS requirements if an adapter is used.
- Use the recommended cordset (power cord) in accordance with the specified ratings.
- Only use the power adapter supplied with your device.
- Use a mains socket outlet with a protective earthing (grounding) connection.
- Ground your device properly if the device is intended to be grounded.

Battery Use Caution

- When battery is used, avoid:
 - High or low extreme temperatures during use, storage and transportation;
 - Extremely low air pressure, or low air pressure at high altitude.
- Use the battery properly. Improper use of the battery such as the following may cause risks of fire, explosion or leakage of flammable liquid or gas.
 - Replace battery with an incorrect type;
 - Dispose of a battery into fire or a hot oven, or mechanically crushing or cutting of a battery;

- Dispose the used battery according to your local regulations or the battery manufacturer's instructions

Regulatory Compliance

FCC Statements

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Compliance Information Statement refer to:

http://en.uniview.com/Support/Download_Center/Product_Installation/Declaration/

Caution: The user is cautioned that changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

NOTE: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense

LVD/EMC Directive



This product complies with the European Low Voltage Directive 2014/35/EU and EMC Directive 2014/30/EU.

WEEE Directive–2012/19/EU



The product this manual refers to is covered by the Waste Electrical & Electronic Equipment (WEEE) Directive and must be disposed of in a responsible manner.

Battery Directive-2013/56/EC



Battery in the product complies with the European Battery Directive 2013/56/EC. For proper recycling, return the battery to your supplier or to a designated collection point.

Better Security, Better World



www.uniview.com



globalsupport@uniview.com