

Supermarket anti-theft product

User's Manual













V1.0.0

Foreword

This manual introduces the introduction and operations of supermarket anti-theft product. Read carefully before using the product, and keep the manual safe for future reference.

Safety Instructions

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

Signal Words	Descriptions
 DANGER	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
 WARNING	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
 CAUTION	Indicates a potential risk which, if not avoided, could result in property damage, data loss, lower performance, or unpredictable result.
 ESD PROTECTION	Indicates electrostatic sensitive equipment.
 WARNING ELECTRIC SHOCK	Indicates high voltage danger.
 LASER RADIATION	Indicates strong laser radiation.
 FAN WARNING	Indicates dangerous moving parts, please stay away from moving fan blades.
 WARNING MECHANICAL INJURY	Indicates that equipment parts will cause mechanical wounding to people.
 TIPS	Provides methods to help you solve a problem or save you time.
 NOTE	Provides additional information as the emphasis and supplement to the text.

Revision History

Version	Revision Content	Release date
V1.0.0	First release.	Nov 2024

Privacy Protection Notice

As the product user or data controller, you might collect the personal data of others such as their face, audio, fingerprints, and license plate number. You need to be in compliance with your local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures which include but are not limited: Providing clear and visible identification to inform people of the existence of the surveillance area and provide required contact information.

About the Manual

- The manual is for reference only. Slight differences might be found between the manual and the product.
- We are not liable for losses incurred due to operating the product in ways that are not in compliance with the manual.
- The manual will be updated according to the latest laws and regulations of related jurisdictions. For detailed information, see the paper user's manual, use our CD-ROM, scan the QR code or visit our official website. The manual is for reference only. Slight differences might be found between the electronic version and the paper version.
- All designs and software are subject to change without prior written notice. Product updates might result in some differences appearing between the actual product and the manual. Please contact customer service for the latest program and supplementary documentation.
- There might be errors in the print or deviations in the description of the functions, operations and technical data. If there is any doubt or dispute, we reserve the right of final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and company names in the manual are properties of their respective owners.
- Please visit our website, contact the supplier or customer service if any problems occur while using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Important Safeguards and Warnings

This section introduces content covering the proper handling of the detector, hazard prevention, and prevention of property damage. Read carefully before using the detector, and comply with the guidelines when using it.

Transportation Requirements



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

Storage Requirements



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

Installation Requirements



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

Operation Requirements



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

Maintenance Requirements



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

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

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



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

Table of Contents

Foreword	I
Important Safeguards and Warnings	III
1 Overview	6
1.1 Introduction	6
2 Installation	7
2.1 Checking List	7
2.2 Matters Needing Attention	7
Appendix 1 Cybersecurity Recommendations	8

1 Overview

1.1 Introduction


Supermarket anti-theft products, combined with their own advantages and characteristics, can play an alarm role in the process of product theft, not limited to lighting and sound, preventing product theft and playing an important role in preventing losses for various retailers. Supermarket anti-theft products are suitable for various scenarios, such as supermarkets, shopping malls, clothing stores, etc.

2 Installation

2.1 Checking List

After you receive the product 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 2-1 Checklist

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

2.2 Matters Needing Attention

- Keep away from static large metal items.
- Keep away from the EM interference source and the EM radiation source.
- The Device must be strictly grounded.
To ensure personal and Device safety, enhance Device anti-interference capability and improve detection distance, the Device needs to be reliably grounded in accordance with regulations.
- Keep the electric and electronic wirings separate.
- Electric and electronic are prone to mutual influence and cause safety problems, so the two wirings need to be separate.



The following can be the EM interference source and the EM radiation source that affects the product: 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 ballas.

Appendix 1 Cybersecurity Recommendations

Mandatory actions to be taken for basic device network security:

1. Use Strong Passwords

Please refer to the following suggestions to set passwords:

- The length should not be less than 8 characters.
- Include at least two types of characters; character types include upper and lower case letters, numbers and symbols.
- Do not contain the account name or the account name in reverse order.
- Do not use continuous characters, such as 123, abc, etc.
- Do not use overlapped characters, such as 111, aaa, etc.

2. Update Firmware and Client Software in Time

- According to the standard procedure in Tech-industry, we recommend to keep your device (such as NVR, DVR, IP camera, etc.) firmware up-to-date to ensure the system is equipped with the latest security patches and fixes. When the device is connected to the public network, it is recommended to enable the “auto-check for updates” function to obtain timely information of firmware updates released by the manufacturer.
- We suggest that you download and use the latest version of client software.

"Nice to have" recommendations to improve your device network security:

1. Physical Protection

We suggest that you perform physical protection to device, especially storage devices. For example, place the device in a special computer room and cabinet, and implement well-done access control permission and key management to prevent unauthorized personnel from carrying out physical contacts such as damaging hardware, unauthorized connection of removable device (such as USB flash disk, serial port), etc.

2. Change Passwords Regularly

We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.

3. Set and Update Passwords Reset Information Timely

The device supports password reset function. Please set up related information for password reset in time, including the end user's mailbox and password protection questions. If the information changes, please modify it in time. When setting password protection questions, it is suggested not to use those that can be easily guessed.

4. Enable Account Lock

The account lock feature is enabled by default, and we recommend you to keep it on to guarantee the account security. If an attacker attempts to log in with the wrong password several times, the corresponding account and the source IP address will be locked.

5. Change Default HTTP and Other Service Ports

We suggest you to change default HTTP and other service ports into any set of numbers between 1024–65535, reducing the risk of outsiders being able to guess which ports you are using.

6. Enable HTTPS

We suggest you to enable HTTPS, so that you visit Web service through a secure communication channel.

7. MAC Address Binding

We recommend you to bind the IP and MAC address of the gateway to the device, thus reducing the risk of ARP spoofing.

8. Assign Accounts and Privileges Reasonably

According to business and management requirements, reasonably add users and assign a minimum set of permissions to them.

9. Disable Unnecessary Services and Choose Secure Modes

If not needed, it is recommended to turn off some services such as SNMP, SMTP, UPnP, etc., to reduce risks.

If necessary, it is highly recommended that you use safe modes, including but not limited to the following services:

- SNMP: Choose SNMP v3, and set up strong encryption passwords and authentication passwords.
- SMTP: Choose TLS to access mailbox server.
- FTP: Choose SFTP, and set up strong passwords.
- AP hotspot: Choose WPA2-PSK encryption mode, and set up strong passwords.

10. Audio and Video Encrypted Transmission

If your audio and video data contents are very important or sensitive, we recommend that you use encrypted transmission function, to reduce the risk of audio and video data being stolen during transmission.

Reminder: encrypted transmission will cause some loss in transmission efficiency.

11. Secure Auditing

- Check online users: we suggest that you check online users regularly to see if the device is logged in without authorization.
- Check device log: By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.

12. Network Log

Due to the limited storage capacity of the device, the stored log is limited. If you need to save the log for a long time, it is recommended that you enable the network log function to ensure that the critical logs are synchronized to the network log server for tracing.

13. Construct a Safe Network Environment

In order to better ensure the safety of device and reduce potential cyber risks, we recommend:

- Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.
- The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.
- Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.
- Enable IP/MAC address filtering function to limit the range of hosts allowed to access the device.