

# Access Controller

## User's Manual

**V1.0.1**

# Cybersecurity Recommendations

## **Mandatory actions to be taken towards cybersecurity**

### **1. Change Passwords and Use Strong Passwords:**

The number one reason systems get “hacked” is due to having weak or default passwords. It is recommended to change default passwords immediately and choose a strong password whenever possible. A strong password should be made up of at least 8 characters and a combination of special characters, numbers, and upper and lower case letters.

### **2. Update Firmware**

As is standard procedure in the tech-industry, we recommend keeping NVR, DVR, and IP camera firmware up-to-date to ensure the system is current with the latest security patches and fixes.

## **“Nice to have” recommendations to improve your network security**

### **1. Change Passwords Regularly**

Regularly change the credentials to your devices to help ensure that only authorized users are able to access the system.

### **2. Change Default HTTP and TCP Ports:**

- Change default HTTP and TCP ports for systems. These are the two ports used to communicate and to view video feeds remotely.
- These ports can be changed to any set of numbers between 1025-65535. Avoiding the default ports reduces the risk of outsiders being able to guess which ports you are using.

### **3. Enable HTTPS/SSL:**

Set up an SSL Certificate to enable HTTPS. This will encrypt all communication between your devices and recorder.

### **4. Enable IP Filter:**

Enabling your IP filter will prevent everyone, except those with specified IP addresses, from accessing the system.

### **5. Change ONVIF Password:**

On older IP Camera firmware, the ONVIF password does not change when you change the system’s credentials. You will need to either update the camera’s firmware to the latest revision or manually change the ONVIF password.

### **6. Forward Only Ports You Need:**

- Only forward the HTTP and TCP ports that you need to use. Do not forward a huge range of numbers to the device. Do not DMZ the device's IP address.
- You do not need to forward any ports for individual cameras if they are all connected to a recorder on site; just the NVR is needed.

#### **7. Disable Auto-Login on SmartPSS:**

Those using SmartPSS to view their system and on a computer that is used by multiple people should disable auto-login. This adds a layer of security to prevent users without the appropriate credentials from accessing the system.

#### **8. Use a Different Username and Password for SmartPSS:**

In the event that your social media, bank, email, etc. account is compromised, you would not want someone collecting those passwords and trying them out on your video surveillance system. Using a different username and password for your security system will make it more difficult for someone to guess their way into your system.

#### **9. Limit Features of Guest Accounts:**

If your system is set up for multiple users, ensure that each user only has rights to features and functions they need to use to perform their job.

#### **10. UPnP:**

- UPnP will automatically try to forward ports in your router or modem. Normally this would be a good thing. However, if your system automatically forwards the ports and you leave the credentials defaulted, you may end up with unwanted visitors.
- If you manually forwarded the HTTP and TCP ports in your router/modem, this feature should be turned off regardless. Disabling UPnP is recommended when the function is not used in real applications.

#### **11. SNMP:**

Disable SNMP if you are not using it. If you are using SNMP, you should do so only temporarily, for tracing and testing purposes only.

#### **12. Multicast:**

Multicast is used to share video streams between two recorders. Currently there are no known issues involving Multicast, but if you are not using this feature, deactivation can enhance your network security.

#### **13. Check the Log:**

If you suspect that someone has gained unauthorized access to your system, you can check the system log. The system log will show you which IP addresses were used to login to your system and what was accessed.

#### **14. Physically Lock Down the Device:**

Ideally, you want to prevent any unauthorized physical access to your system. The best way to achieve this is to install the recorder in a lockbox, locking server rack, or in a room that is behind a lock and key.

**15. Connect IP Cameras to the PoE Ports on the Back of an NVR:**

Cameras connected to the PoE ports on the back of an NVR are isolated from the outside world and cannot be accessed directly.

**16. Isolate NVR and IP Camera Network**






The network your NVR and IP camera resides on should not be the same network as your public computer network. This will prevent any visitors or unwanted guests from getting access to the same network the security system needs in order to function properly.

## General

This document elaborates structure, installation and wiring instruction of 8-door one-way access controller.

## Safety Instructions

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

Signal Words	Meaning
 <b>DANGER</b>	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
 <b>WARNING</b>	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
 <b>CAUTION</b>	Indicates a potential risk which, if not avoided, could result in property damage, data loss, lower performance, or unpredictable result.
 <b>TIPS</b>	Provides methods to help you solve a problem or save you time.
 <b>NOTE</b>	Provides additional information as the emphasis and supplement to the text.

## Privacy Protection Notice

As the device user or data controller, you might collect personal data of others' such as face, fingerprints, car plate number, Email address, phone number, GPS and so on. You need to be in compliance with the local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures include but not limited to: providing clear and visible identification to inform data subject the existence of surveillance area and providing related contact.

## About the Manual

- The Manual is for reference only. If there is inconsistency between the Manual and the actual product, the actual product shall prevail.
- We are not liable for any loss caused by the operations that do not comply with the Manual.
- The Manual would be updated according to the latest laws and regulations of related regions. For detailed information, see the paper User's Manual, CD-ROM, QR code or our official website. If there is inconsistency between paper User's Manual and the electronic version, the electronic version shall prevail.
- All the designs and software are subject to change without prior written notice. The product

updates might cause some differences between the actual product and the Manual. Please contact the customer service for the latest program and supplementary documentation.

- There still might be deviation in technical data, functions and operations description, or errors in print. If there is any doubt or dispute, please refer to our final explanation.
- Upgrade the reader software or try other mainstream reader software if the Guide (in PDF format) cannot be opened.
- All trademarks, registered trademarks and the company names in the Manual are the properties of their respective owners.
- Please visit our website, contact the supplier or customer service if there is any problem occurred when using the device.
- If there is any uncertainty or controversy, please refer to our final explanation.

# Important Safeguards and Warnings

The following description is the correct application method of the device. Please read the manual carefully before use, in order to prevent danger and property loss. Strictly conform to the manual during application and keep it properly after reading.



## WARNING

- Please make sure to use batteries according to requirements; otherwise, it may result in fire, explosion or burning risks of batteries!
- To replace batteries, only the same type of batteries can be used!
- The product shall use electric cables (power cables) recommended by this area, which shall be used within its rated specification!
- Please use power supply that meets SELV (safety extra low voltage) requirements, and supply power with rated voltage that conforms to Limited Power Source in IEC60950-1. For specific power supply requirements, please refer to device labels.
- Products with category I structure shall be connected to grid power output socket, which is equipped with protective grounding.
- Power plug or appliance coupler is a disconnecting device. During normal use, please keep an angle that facilitates operation.



## CAUTION

- Please change default password timely after device deployment, in order to avoid embezzlement.
- Please don't place and install the device in an area exposed to direct sunlight or near heat generating device.
- Please don't install the device in a humid, dusty or fuliginous area.
- Please keep its horizontal installation, or install it at stable places, and prevent it from falling.
- Please don't drip or splash liquids onto the device; don't put on the device anything filled with liquids, in order to prevent liquids from flowing into the device.
- Please install the device at well-ventilated places; don't block its ventilation opening.
- Use the device only within rated input and output range.
- Please don't dismantle the device arbitrarily.
- Please transport, use and store the device within allowed humidity and temperature range.

## Special Statement

- This document is for reference only. Please refer to the actual product for more details.
- The user's manual and program will be updated in a real-time way according to the product, which won't be further notified.
- The user shall undertake any losses resulting from violation of guidance in the document.
- The document may include technically inaccurate contents, inconsistencies with product functions and operations, or misprint. Final explanations of the company shall prevail.



# Table of Contents

<b>Foreword</b> .....	<b>I</b>
<b>Important Safeguards and Warnings</b> .....	<b>III</b>
<b>1 Overview</b> .....	<b>1</b>
<b>2 Appearance and Dimension</b> .....	<b>2</b>
<b>3 Device Installation</b> .....	<b>3</b>
<b>4 Wiring and System Network</b> .....	<b>4</b>
4.1 Wiring Diagram.....	4
4.2 System Network .....	5
<b>5 Technical Parameters</b> .....	<b>6</b>

As a control device, 8-door one-way access controller complements and improves video surveillance and visual intercom products. With neat fashionable appearance and powerful function, it is designed for high-end commercial buildings, prisons, banks, governments and enterprises.

The controller boasts rich functions as follows:

- Industrial professional design with lock and hinge rotation structure. Be able to bear max. 80kg under good vandal-proof design.
- Integrate alarm, access control, video surveillance, fire alarm and control module input.
- Support 8 sets of card readers (which may set to 8-door one-way reader, with RS485 or Wiegand input).
- Support 8 groups of exit buttons, 8 groups of door sensors and 1 group of local vandal-proof alarm.
- Support 4 groups of external alarm input (with anti-cut function).
- Support 8 groups of door lock control output.
- Support 4 groups of external alarm triggering output.
- Support audio module output (which needs external speaker).
- Support external GSM module.
- Support 2 groups of RS485 port, extendible to connect lift control module, alarm or home control module.
- FLASH storage capacity is 16M (extendible to 32M). It supports max. 100,000 card holders and 150,000 records.
- Support vandal-proof alarm, illegal intrusion alarm, door timeout alarm, duress card alarm and duress code setup. It also supports black-white list and patrol card setup.
- Support valid time interval, password and validity setting of cards. Set the times of use of guest card.
- Support 128 groups of schedules, 128 groups of periods and 128 groups of holiday schedules.
- Support permanent data storage in case of outage, built-in RTC and online upgrade.

# 2 Appearance and Dimension

Its appearance and dimension are shown in Figure 2-1. Dimension unit is mm.

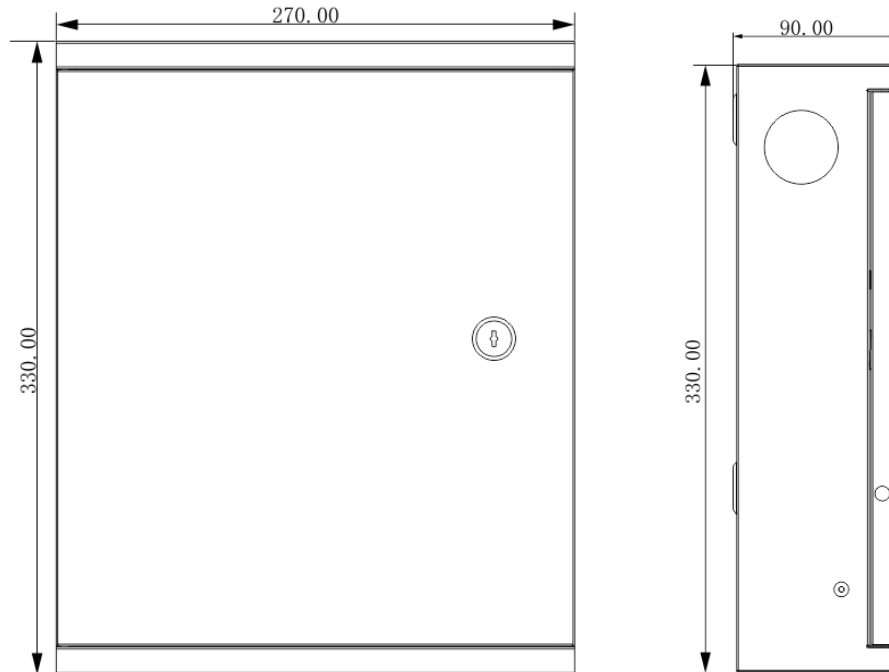


Figure 2-1

# 3 Device Installation

Device installation diagram is shown in Figure 3-1.

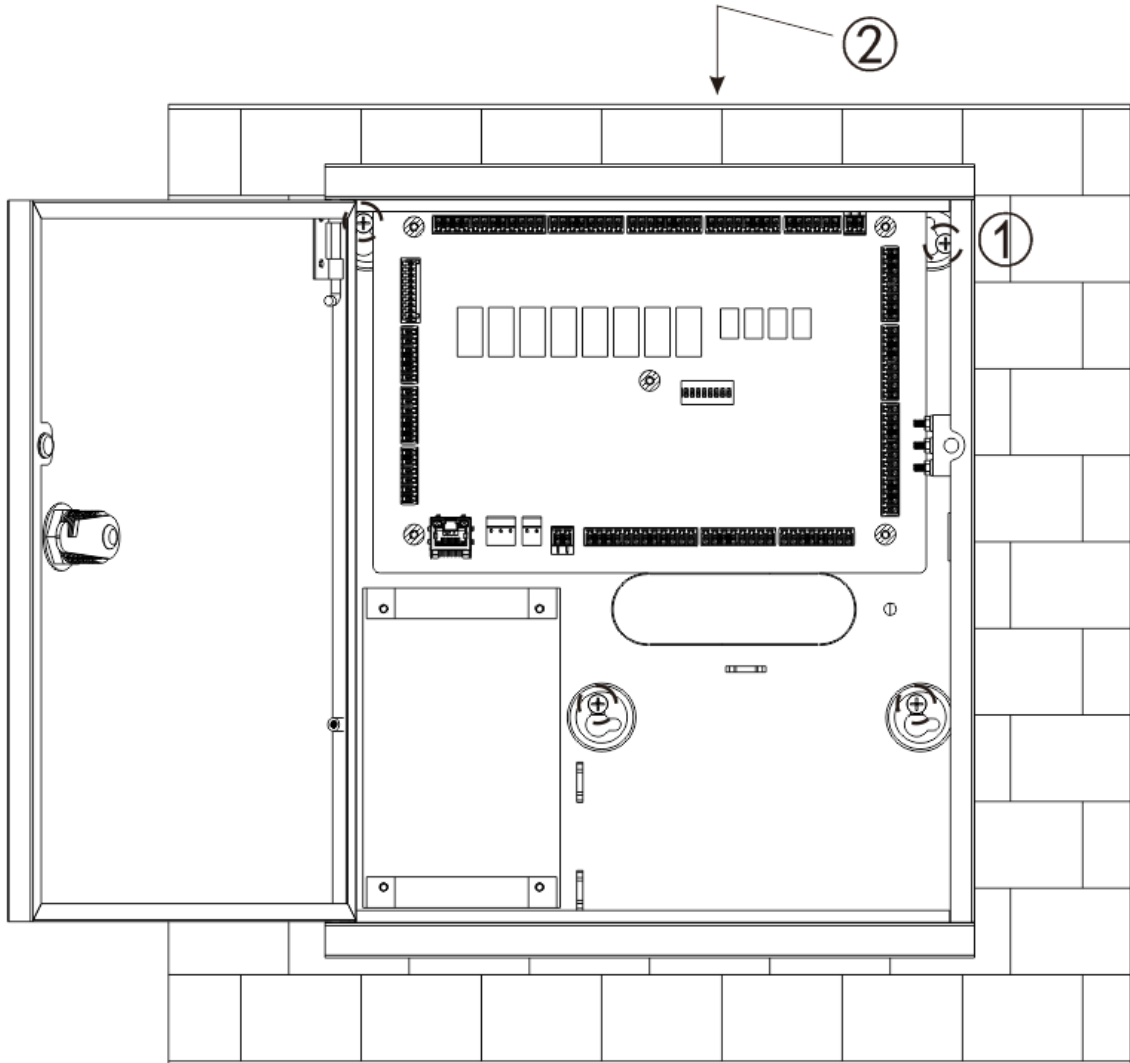


Figure 3-1

 Note

Please ensure that device mounting surface is able to bear 3 times as many as the total weight of the device, bracket and accessories.

Installation steps:

- Step 1 Measure every hole distance and position according to holes at rear shell of the device; drill holes in the wall according to the measured positions, and embed expansion nuts.
- Step 2 Fix screws into the wall via expansion nuts, and hang the whole device onto the screws.

# 4 Wiring and System Network

## 4.1 Wiring Diagram

Device wiring diagram is shown in Figure 4-1.

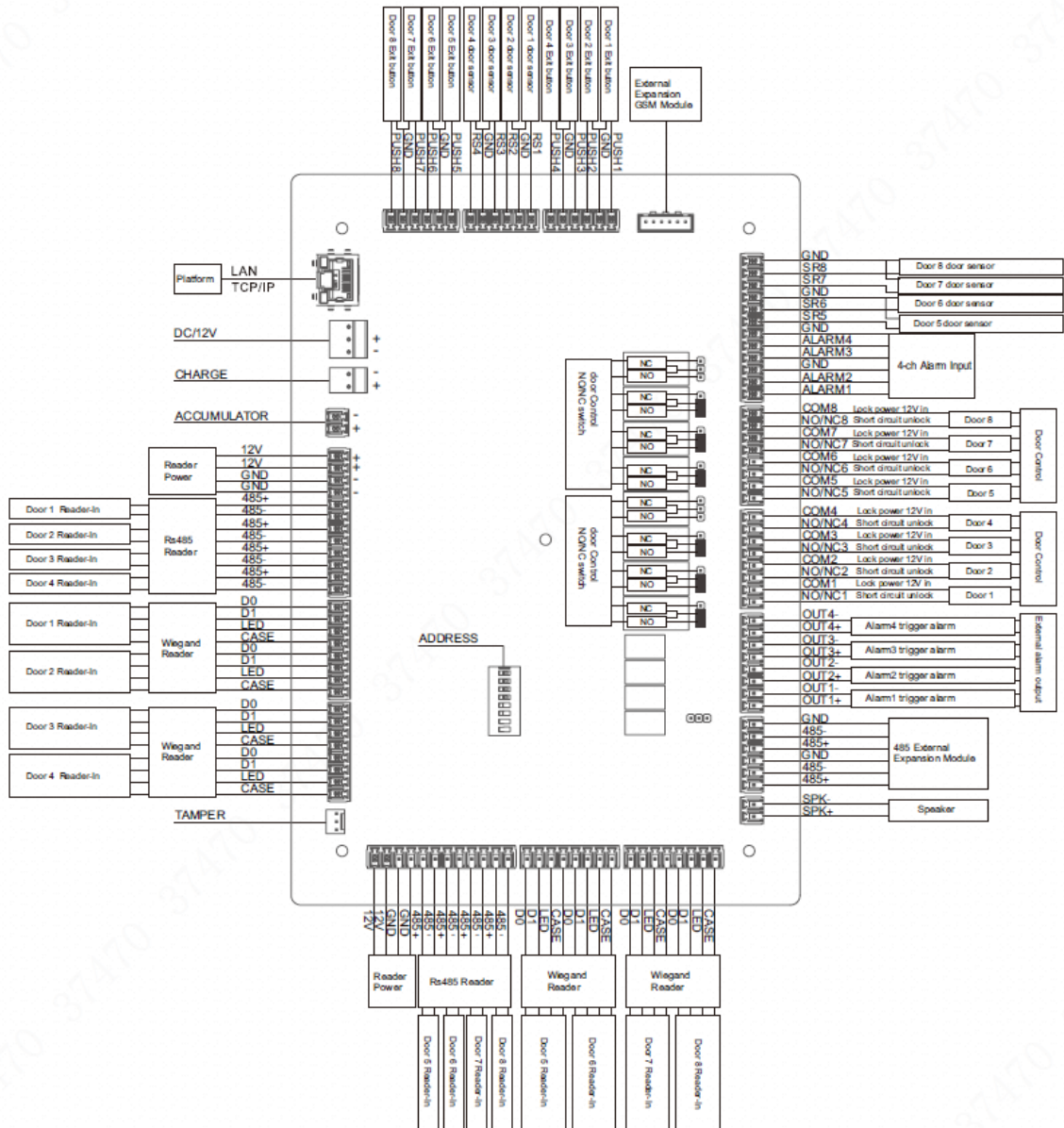


Figure 4-1

# 4.2 System Network

8-door one-way access controller, lock, reader and others connect a system, as shown in Figure 4-2.

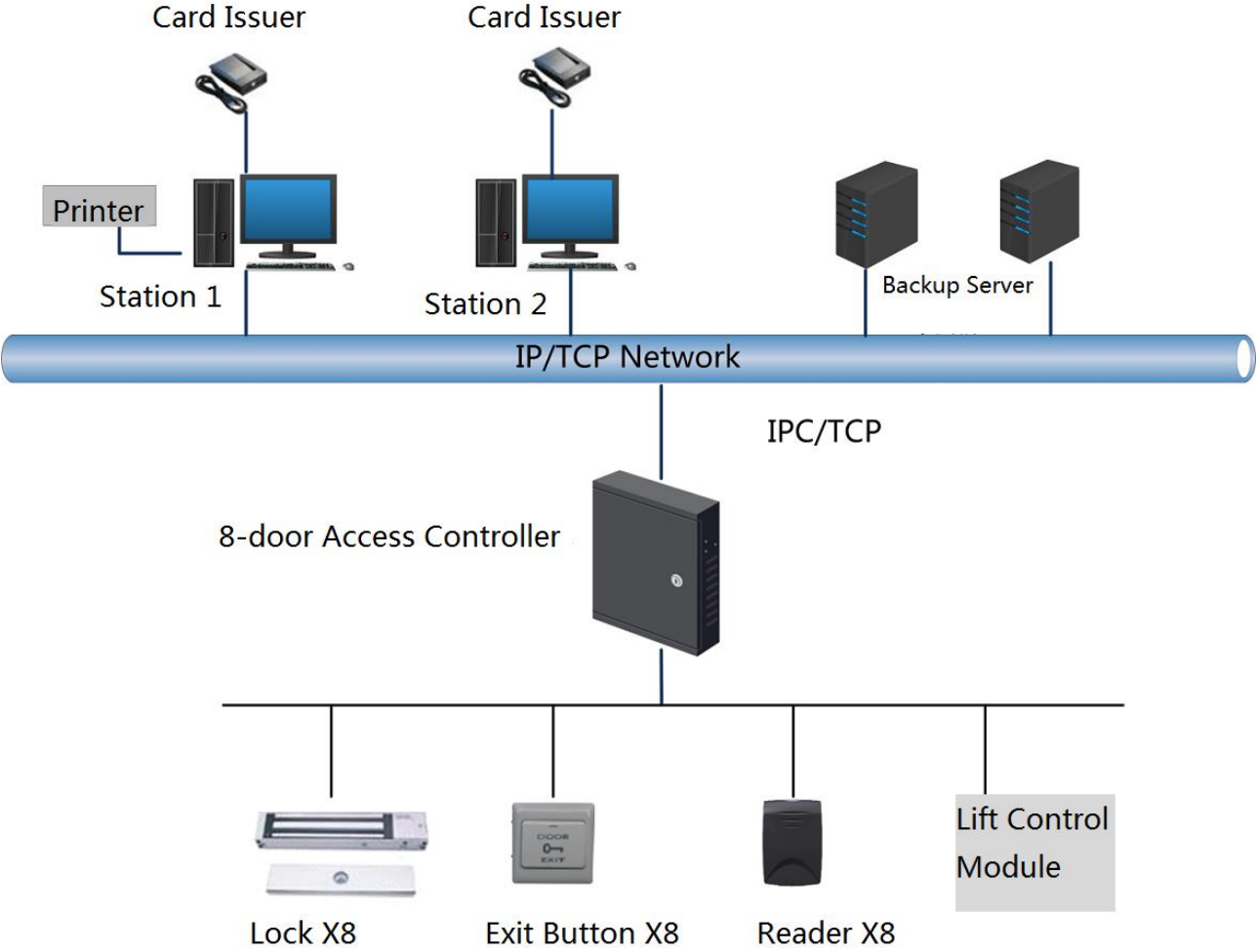


Figure 4-2

# 5

## Technical Parameters

Parameter	Specification
Processor	32-bit ARM processor
Storage Capacity	16M
Max. User	100000
Max. Record	150000
Communication Port of Reader	Wiegand, RS485
Communication Port of Platform	TCP/IP
Input Reader Quantity	8 groups
Working Power	Rated power AC 85V –AC 264V
Schedule	128
Period	128
Holiday	128
Unlock Mode	Card, card + password, password, card or password, card + fingerprint, fingerprint + password, fingerprint or card or password, by period.
Cross-Segment Network	Support
8-door Interlocking	Support
8-door One-way Card Swiping	Support
Real-time Surveillance	Support
Fire Alarm Linkage	Support
Vandal-Proof Alarm	Support
Illegal Intrusion Alarm	Support
Door Timeout Alarm	Support
Duress Card and Duress Code Setting	Support
DST and RTC	Support
Online Upgrade	Support