BLAUPUNKT

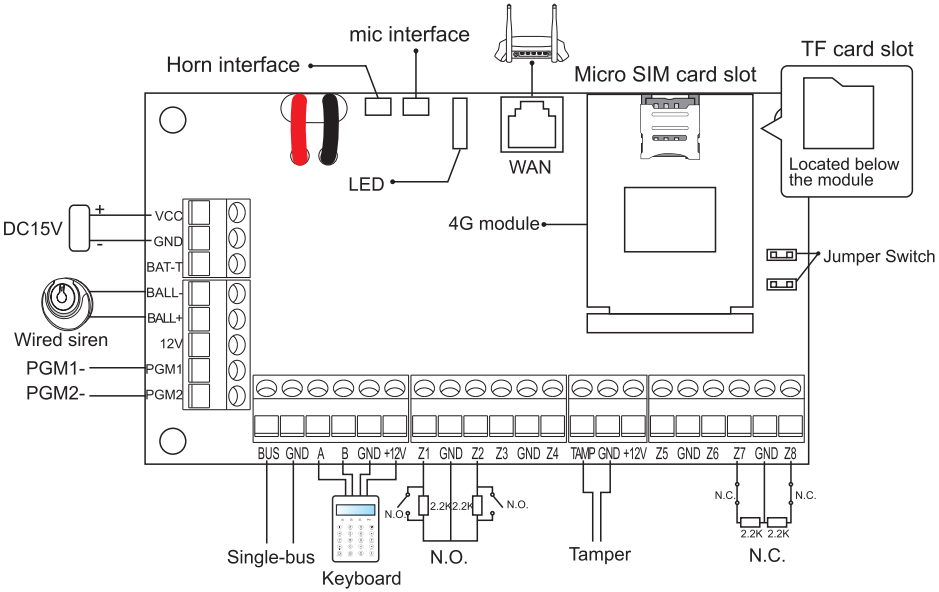
User Manual

ANTI-THEFT ALARM CONTROLLER
BP-AP128NGW-I



Enjoy it.

Wiring Diagram



*Jumper switch: Plug in to enable single bus, disconnect to not enable, please plug it in properly.

The power supply is a switching power supply of DC15V/2.5A.

▲ Use a sealed lead-acid battery of 12VDC, 7Ah, and replace it every 3-5 years.

▲ When not using the siren, a 2.2K resistor can be jumpered to clear the siren fault.

▲ It supports the connection of an siren with a maximum power of 6W (12V/500mA), and the motherboard will be damaged if the rated power is exceeded.

▲ It supports the connection of a PGM with a maximum power of 4.5W (15V/300mA).

▲ The total power demand for the power supply of the keyboard, auxiliary power supply, siren, etc. does not exceed the maximum power of the input power supply.

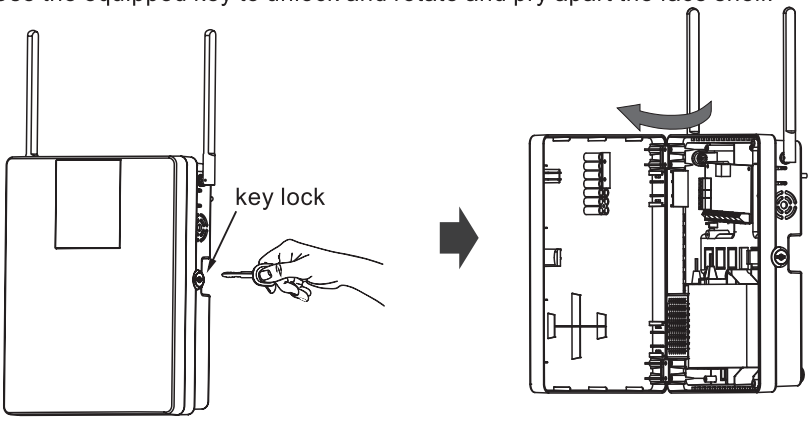
▲ When using wired / single-bus defense zones, it is necessary to set the defense zone properties in the defense zone attribute settings.

Attention: If you need to use a SIM card, please first insert the SIM card into the host card slot before powering on.

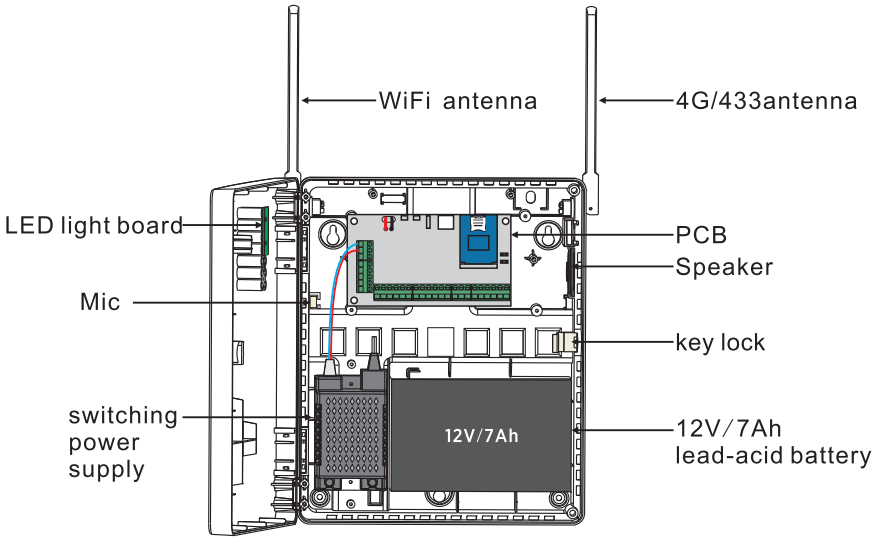
Structural schematic diagram

1.Open the case cover.

Use the equipped key to unlock and rotate and pry apart the face shell.



2. Structural diagram



Content

Foreword ····· 1
Features ····· 2
Technical specifications ····· 3
Keyboard Description ····· 4
Common keyboard operations ····· 7
Card insertion and light display ····· 7
Arm/disarm alarm panel ····· 9
Alarm procedure ····· 10
I. System setting ····· 11
1. Set sys password ····· 11
1.1 Set admin pwd ····· 11
1.2 Set main user code ····· 12
1.3 Set user code ····· 12
2. Set system network ····· 12
2.1 Set DHCP ····· 13
2.2 Set IP ····· 13
2.3 Set gateway ····· 14
2.4 Set subnet mask ····· 14
2.5 Set DNS ····· 14
3. Set CMS ····· 15
3.1 CMS platform ····· 16
3.1.1 Set server IP ····· 16
3.1.2 Set server port ····· 16
3.1.3 Set user ····· 16
3.2 SIA platform ····· 16
4. Set voice phone ····· 16
5. Set SYS options ····· 17
5.1 Sys setting ····· 17
5.1.1 AC off delay ····· 18
5.1.2 Sensor loss check ····· 18
5.1.3 Door sensor check ····· 19
5.1.4 Sensor tamper ····· 19
5.1.5 System low voltage report ····· 20
5.1.6 System tamper check ····· 20
5.1.7 Wired siren type ····· 21
5.2 Alarm setting ····· 21
5.2.1 Entry delay ····· 21

5.2.2 Exit delay · · · · · 22
5.2.3 Bell time · · · · · 22
5.2.4 Force arm · · · · · 23
5.2.5 Arm/disarm rpt · · · · · 23
5.2.6 Voice prompt · · · · · 23
5.2.7 Alarm times limit · · · · · 24
5.2.8 Emergency tone · · · · · 24
6. Set wireless · · · · · 25
6.1 Set remote · · · · · 25
6.1.1 Remote enroll · · · · · 26
6.1.2 Remote code · · · · · 26
6.1.3 Delete remote · · · · · 27
6.2 Set WL detector · · · · · 27
6.2.1 Enroll detector · · · · · 28
6.2.2 Detector code · · · · · 28
6.2.3 Delete detector · · · · · 29
6.3 Set WL siren · · · · · 29
6.3.1 Enroll siren · · · · · 29
6.3.2 Sorem cpde · · · · · 30
6.3.3 Delete siren · · · · · 31
6.4 Set smart device · · · · · 31
6.4.1 Enroll smart device · · · · · 31
6.4.2 smart device code · · · · · 32
6.4.3 Delete smart device · · · · · 32
7. Set system zone · · · · · 33
7.1 Set zone type · · · · · 33
7.2 Set zone siren · · · · · 34
7.3 Set key zone · · · · · 34
7.4 Set zone SMS · · · · · 35
7.5 Set Doorbell tone · · · · · 35
7.6 Set arm prompt · · · · · 36
8. Set system area · · · · · 36
8.1 Device area · · · · · 37
8.2 Password area · · · · · 37
8.3 Keypad area · · · · · 38
8.4 Remote area · · · · · 38
9. Set 4G · · · · · 39
9.1 4G enable · · · · · 39

9.2 4G APN setting · · · 39
9.3 4G user name and password · · · 40
II. WEB setting · · · 41
1. Device startup · · · 41
2. Accessing the host · · · 41
3. Camera addition · · · 42
4. Regional settings · · · 42
5. Addition of accessories · · · 43
6. Scenario management · · · 44
7. Deployment and Deployment Settings · · · 45
8. Video control · · · 45
9. Network Settings · · · 45
10. Platform Connection · · · 46
III. App use · · · 47
1. Download and installation · · · 47
2. Account registration · · · 47
3. Add panel · · · 48
4. WiFi connection · · · 49
5. Add cameras · · · 50
System maintenance · · · 51
Product function limitation · · · 52

Foreword

Thank you for choosing the BLAUPUNKT intelligent security system. This product is designed for reliable alarm and monitoring applications.

The BP-AP128NGW-I is an intelligent network alarm control panel integrating anti-theft, fire prevention, gas leakage prevention and video monitoring functions. It supports wired and wireless alarm devices and can be operated remotely through the Internet, mobile applications and central monitoring stations (CMS).

For dependable operation, the BP-AP128NGW-I uses bus-zone coding and dynamic radio-code technology to reduce interference and false alarms. Alarm transmission supports SIA-2013 over GPRS and the widely used Contact ID protocol. The system is suitable for residential areas, villas, shops, offices and other commercial sites.

Please read this manual carefully before installing or operating the equipment.

Warning:

A.Do not disassemble or modify, otherwise it may cause danger and cause damage to the machine.

B.Do not put other objects into the machine. Metal objects, water and flammable objects are all prone to short circuit or fire.

C.To avoid injury, do not drop the machine or subject it to strong impact.

D.Do not install the machine near a magnetic field, it may cause unstable operation.

E.Keep dry and clean. Do not set it in a place with oily smoke or steam, high temperature or a lot of dust.

F.Avoid high temperatures. Please do not install the unit near a heater or other high-temperature equipment, such as near a spotlight; also do not place it in a place that is easily exposed to direct sunlight, otherwise it may cause color fading. When cleaning, please wipe with a soft cloth. To remove dirt, you need to use detergent solution. Wipe after wringing out.

G.Never use chemicals such as gasoline or paint thinner, otherwise it may cause damage or paint peeling.

Features

▲ It can be divided into 8 independent partitions, with a built-in 64-path wireless defense zone, 8-path wired defense zone, 32-path single-bus defense zone, 16-path keyboard extended defense zone, and a total of 120 defense zones supported.

▲ Definition of defense zone numbers: 1~8 - Wired defense zone, 9~24 - Wired keyboard defense zone, 25~56 - Single-bus defense zone, 57~120 - Wireless defense zone, 121~128 - Remote controller, 129~132 - Wireless siren, 150 ~ 165 - User password; 171 - Telephone for arming and disarming; 175 - Web ; 176 - Platform; 177 - Scenario timed arming and disarming; 200~263 - smart device.

▲ The host has 1 web page administrator account, 1 system administrator password, 1 main user password, and 16 ordinary user passwords.

▲ Support 8 remote controllers, 4 two-way wireless sirens, and 8 keyboards.

▲ Support 4 video channels, and the TF card can store video by being inserted.

▲ Support alarm linkage: The detector can link video recording when the alarm is triggered through binding the camera.

▲ Support 2 network alarm receiving platforms.

▲ Support mobile APP remote control and alarm push.

▲ Support 2.4G frequency band WiFi connection.

▲ The network priority is "Ethernet > WiFi > 4G", that is, Ethernet is used first, WiFi connection is enabled after Ethernet is disconnected, and 4G network is enabled when WiFi is not available.

▲ Support different user passwords for regional management.

▲ The storage of alarm information can reach up to 1,000 pieces.

▲ Support adding timed scenarios, trigger scenarios, and manual scenarios.

Technical specifications

Operating system: embedded Linux

User interface: browser, CMS client, mobile client

Audio format: Supports G711 bidirectional voice

Video format: H.264/H.265

Network interface: 10M/100M adaptive network interface

Modulation method: FSK

Wireless operating frequency: 433/868MHz (optional)

Wireless transmission distance: 100-150m in open areas

Communication protocols for alarm reception center: Ademco Contact ID, SIA-2013, and Meian Private Protocol

Alarm dialing mode: Internet alarm, SMS alarm

Channel support: 4 channels

Equipment quantity: Supports 64 wireless detectors, 8 wired detectors, 32 single bus detectors, 8 remote controls, 8 wired keyboards, 1 wired siren, 4 wireless sirens, and 2 PGM outputs,64 smart devices

4G module : Optional

SIM card type: Micro SIM

Network support: Ethernet, WiFi, 4G

WiFi frequency band: 2.4G

WiFi protocol: 802.11 b/g/n

WiFi communication distance: based on WiFi coverage range

TF card: Supports up to 128G standard TF cards

Power input: DC 15V/2.5A

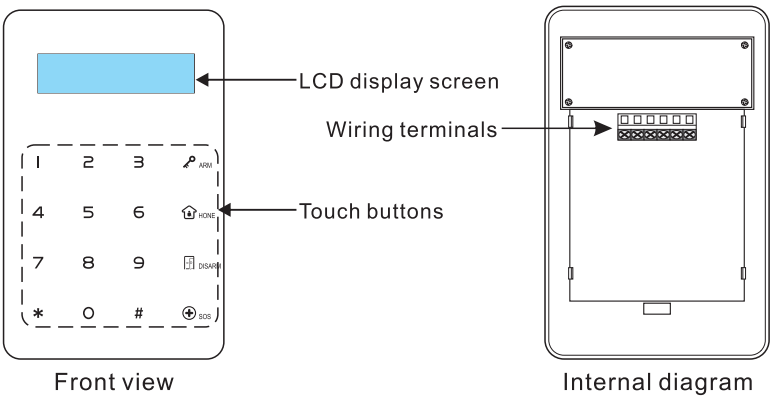
Built in rechargeable battery: 12V7Ah lead-acid battery

Backup power supply duration: approximately 35 hours (when only one keyboard is connected)

Size:L290 * W240 * H86mm (excluding the antenna)

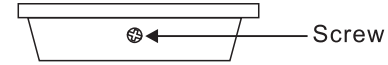
Working environment: temperature -10℃~50℃; Humidity<90% RH

Keyboard Description



1) Wiring

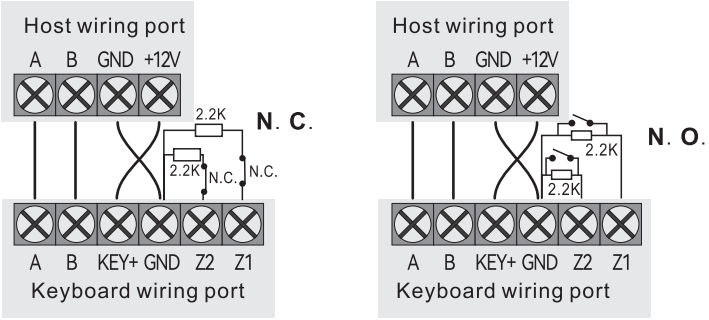
Before connecting the keyboard wires, please unscrew the bottom screw first, and separate the bottom shell from the face cover.



The bottom of the keyboard

2) Wiring

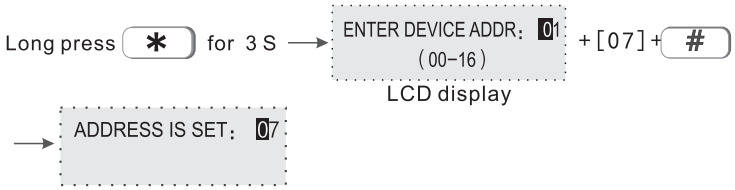
Please follow the wiring diagram below for wiring.



When the keyboard address is 1, Z1 and Z2 respectively correspond to the defense zones as the 9th defense zone and the 10th defense zone. If multiple wired keyboards are connected, the defense zone numbers will be arranged backward according to the serial number of the keyboard address.

3) Keyboard address settings

After connecting the new keyboard, the keyboard shows that the address has not been set. Please disarm and long press " * " in standby mode for three seconds to enter the keyboard address setting. Up to 8 keyboards can be added. For example, add the keyboard to address 07.



The keyboard emits two beeps, indicating that the keyboard address has been successfully set and the keyboard automatically returns to the standby interface.

Please connect the keyboard when the host is powered off. You can connect 8 keyboards. Connect the keyboard and power on the host before scanning and adding it. If the keyboard is added without power off, it will not be scanned by the host and will not work. Different keyboards require different addresses to be set, and after setting, they need to be powered off and restarted to take effect; When the keyboard is first connected and turned on, the display screen will indicate the type of fault, such as battery not connected, network disconnected, etc.

4) Key Description

Icons	Meaning	Explanation
ARM	Deployment/ Return key	Deploy defense in zones; Return to previous menu/exit menu
HONE	Left/Up key	Set up defensive positions in the partition; Select upwards; Long press for 3 S to increase volume
DISARM	Disarm/ Down arrow	Dismantle the zone defense; Select downwards; Long press for 3 seconds to decrease volume
SOS	SOS/ Confirm key	In the standby state, press and hold for 3 S for emergency alarm; after entering the engineering settings, it serves as the confirmation key.

Icons	Meaning	Switchable character
1	No.1	1/“，”/“.”
2	No.2	2abcABC
3	No.3	3defDEF
4	No.4	4ghiGHI
5	No.5	5jklJKL
6	No.6	6mnoMNO
7	No.7	7pqrsPQRS
8	No.8	8tuvTUV
9	No.9	9wsyzWSYZ
0	No.0	"0", " - " and the space bar
*	Settings key	—
#	Confirm key	Enter Options

* When entering text editing, continuous pressing of the number keys can switch characters.

Common keyboard operations

The default password for the system administrator is 012345, and the main user password is 1234.

To improve system security, please change the password in a timely manner and keep it properly.

Enter engineering settings: 012345 * 0#

Restore factory settings: 012345 * 9#

Display system version: * 1#

View host IP address: 1234 * 1 #

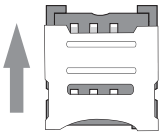
Keyboard key tone adjustment: In standby mode, long press HONE / DISARM , and the keyboard will make a "beep" sound to increase/decrease the volume by one.

Forgot password: Within 1 minute of system startup, enter 000000 * 0 # on the keyboard to log in and fix the user's forgotten password.

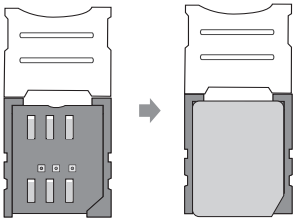
Card insertion and light display

3.1 Mobile Card Insertion

The type of SIM card inserted is Micro SIM card. Placement steps：



A. Push the SIM card holder down until it becomes loose.



B. Push the SIM card holder upwards and insert the SIM card chip downwards;



C. Close the phone holder and gently push it upwards

3.2 TF card insertion

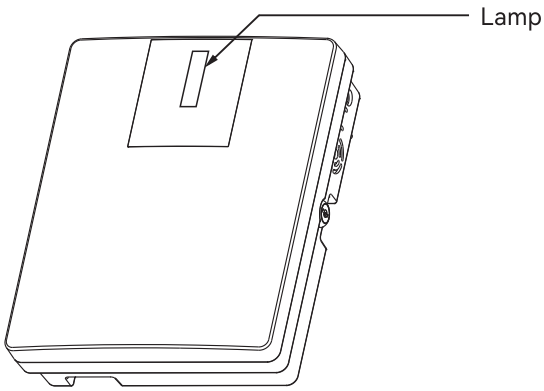
TF cards are used for video storage and can support up to 128G standard TF cards.

TF card insertion: Insert the notch inward.

Remove: Align the TF card and push it inward before releasing it, and the TF card will automatically pop out.



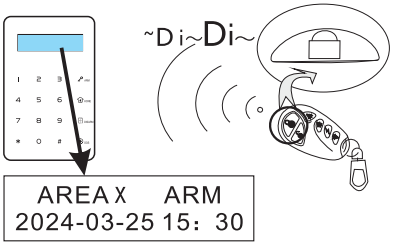
3.3 Lamp display



Icon	Meaning	Color	Light indication
	Arm/disarm	Red	Disarm- off, Arm - always on, Stay - flash
	Alarm	Red	Alarm flashing
	Platform	Green	Online - Always on; Offline - off; Fault - off;
GSM	GSM	Yellow	Normal - always on; Fault - Off

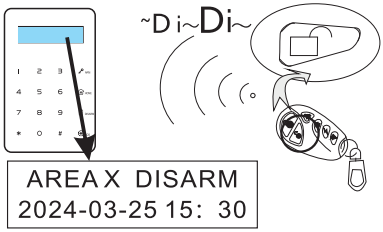
Arm/disarm alarm panel

☆Arm



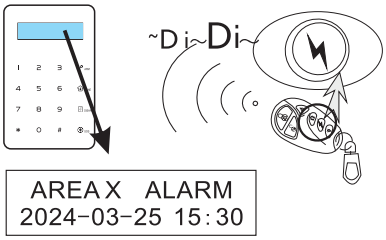
Corresponding user password + ARM or press disarm button remote control.

☆Disarm



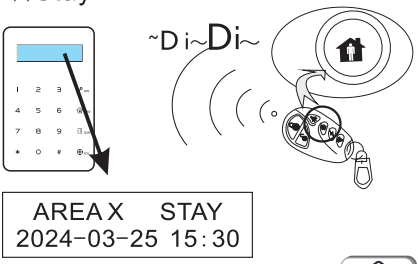
Corresponding user password + DISARM or by pressing the disarm button of the corresponding remote control.

☆Panic alarm



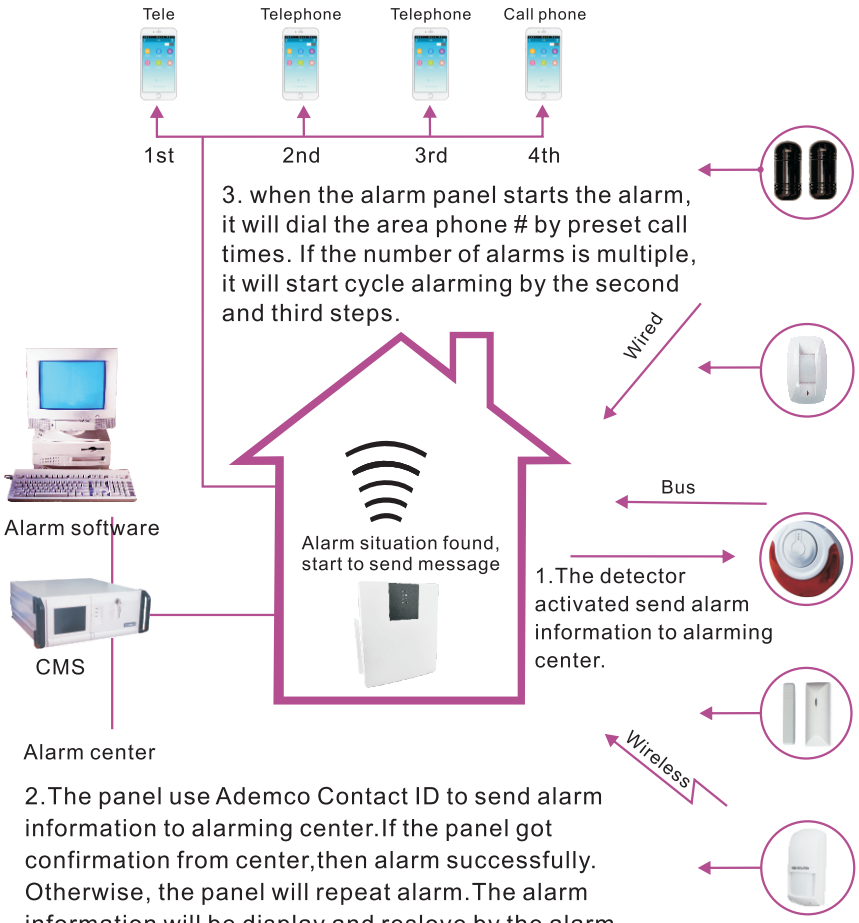
Press and hold for SOS or press the “emergency” button on the remote control for emergency help.

☆Stay

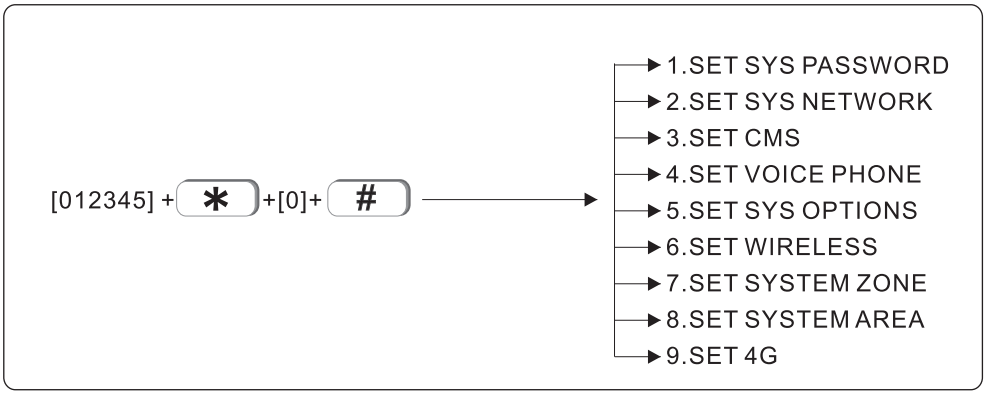


Corresponding user password + or press the home security button of the corresponding remote control.

Alarm procedure

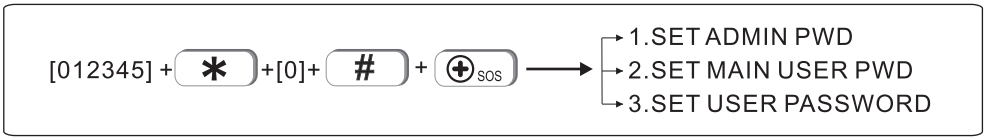


I. System setting

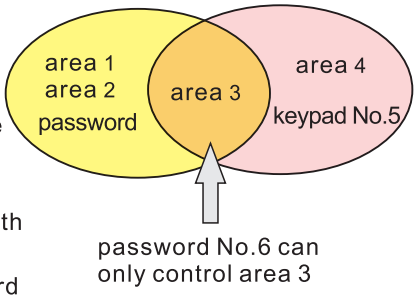


Note: only in disarm status, user can do system setting.

1.Set sys password

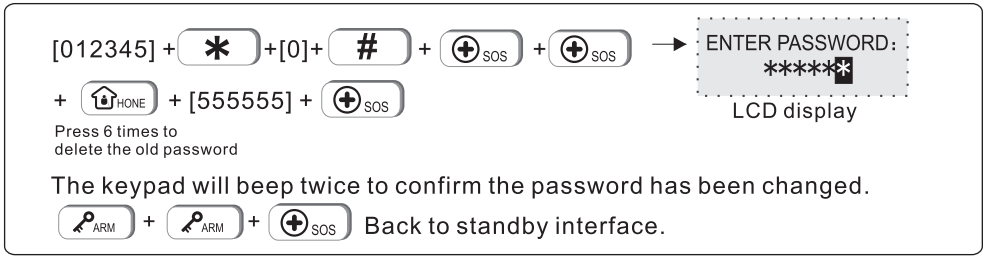


The host has one system administrator password, one main user password, and 16 user passwords. Passwords can control one or more partitions, and the permissions of passwords are determined by the permissions of the password itself and the permissions of the controlled keyboard. For example, managing passwords with permissions for partitions 1, 2, and 3 can only manage partitions 3 when operated on a keyboard that only manages partitions 3 and 4. (As shown in the right figure)



1.1 Set admin password

Admin password has the highest authority. E.g, set admin password as 555555.



Tips: if forget admin password or web login password, please follow: Power off the central panel, and power on again, within 60s, enter 000000 as password to operate and set new password.

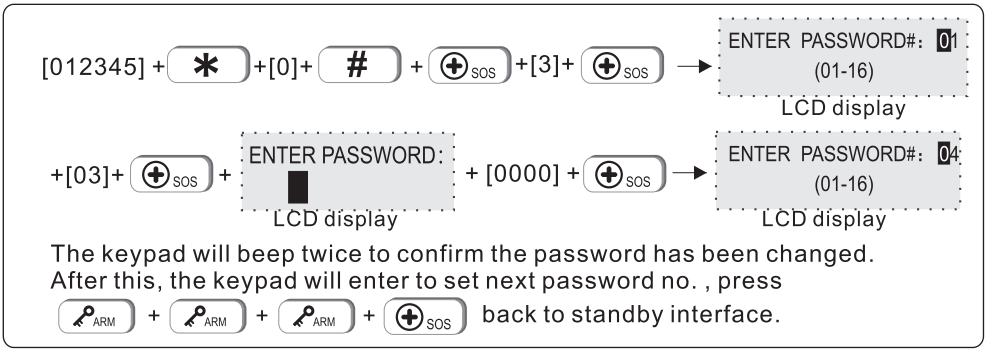
1.2 Set main user password

Please refer to user setting I

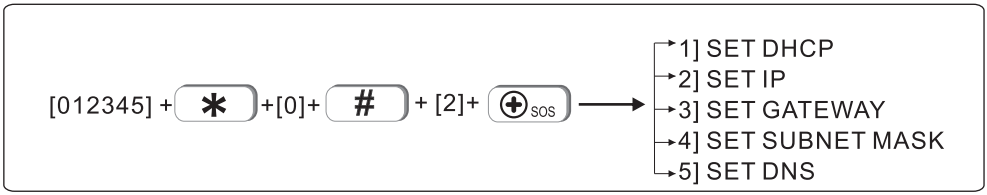
1.3 Set user password

The user password is 4 digits and 16 user passwords must not be the same.

E.g Set user password no. 03 as 0000



2.Set system network



2.1 Set DHCP (Default disable)

User can choose to enable or disable DHCP function.Eg. Enable DHCP function

[012345] + * +[0]+ # + [2]+ SOS + SOS → DHCP: 1>DISABLE 2>ENABLE (LCD display)

+ [2] + SOS

The keypad will beep twice to confirm it has been changed,the keypad will return to previous setting. Press ARM + ARM + SOS back to standby interface.

2.2 Set IP

Factory default IP: 192.168.1.200

Tips: If DHCP is enabled, then it is not able to set IP here.

Users set network parameters based on the actual network environment during use. When setting the IP, if there are not enough three digits, please add "0" before it, such as "192.168.1.81". When entering on the keyboard, "192168001081" should be entered. The network IP of this host is set to 192.168.1.106 by default at the factory. After setting the IP address, it must be powered off and restarted to take effect.

[012345] + * +[0]+ # + [2]+ SOS +[2]+ SOS

→ ENTER IP: 000. 000. 000. 000 (LCD display) + [192168002081] + SOS

The keypad will beep twice to confirm it has been changed, the keypad will return to previous setting.Press ARM + ARM + SOS back to standby interface.

2.3 Set gateway

E.g. Set gateway as 192.168.2.1

[012345] + * +[0]+ # + [2]+ SOS +[3]+ SOS → ENTER GATEWAY: 000. 000. 000. 000

LCD display

+ [192168002001] + SOS

The keypad will beep twice to confirm it has been changed, the keypad will return to previous setting.Press ARM + ARM + SOS back to standby interface.

2.4 Set subnet mask

E.g. Set subnet mask as 255.255.255.0

[012345] + * +[0]+ # + [2]+ SOS +[4]+ SOS

→ ENTER SUBNET MASK: 000. 000. 000. 000 + [255255255000] + SOS

LCD display

The keypad will beep twice to confirm it has been changed, the keypad will return to previous setting.Press ARM + ARM + SOS back to standby interface.

2.5 Set DNS

E.g. Set DNS as 202.96.128.85

[012345] + * +[0]+ # + [2]+ SOS +[5]+ SOS → ENTER DNS SERVER: 000. 000. 000. 000

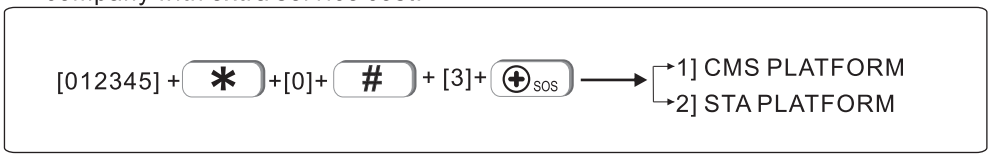
LCD display

+ [202096128085] + SOS

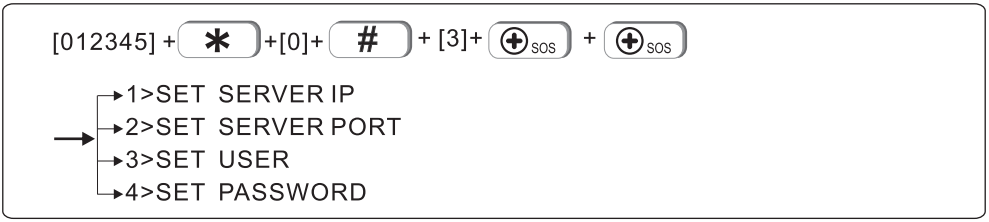
The keypad will beep twice to confirm it has been changed, the keypad will return to previous setting.Press ARM + ARM + SOS back to standby interface.

3. Set CMS

CMS means central monitoring service, which is usually provided by security company with extra service cost.

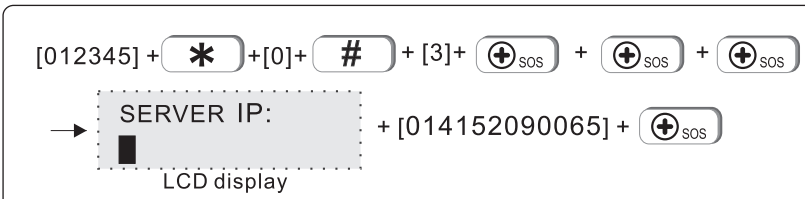


3.1 CMS platform



3.1.1 Set server IP

Set CMS IP as 014.152.090.065



The keypad will beep twice to confirm it has been set, the keypad will return to previous setting.Press ARM + ARM + ARM + SOS back to standby interface.

3.1.2 Set server port

Factory default port: 7974

E.g. Set server port as 6598

[012345] + ✱ +[0]+ # + [3]+ SOS + SOS +[2]+ SOS

→ SERVER PORT: 07974 （00001--65535） + [06598] + SOS

LCD display

The keypad will beep twice to confirm it has been set, the keypad will return to previous setting.Press ARM + ARM + ARM + SOS back to standby interface.

3.2.3 Set user

CMS register ID and password are provided by the CMS operator.

User can search the CMS register ID and password as below:

[012345] + ✱ +[0]+ # + [3]+ SOS + SOS +[3]+ SOS

LCD will show the CMS register ID and password.

Press ARM + ARM + ARM + SOS back to standby interface.

The query CMS password is the same as the registration ID.

3.2 SIA platform

For the setting of SIA platform, please refer to the setting method of CMS .

4.Set voice phone

[012345] + ✱ +[0]+ # + [4] + SOS →

- 1]VOICE PHONE 1
- 2]VOICE PHONE 2
- 3]VOICE PHONE 3
- 4]VOICE PHONE 4

The phone number dialed by the host during the alarm can be set to 4 voice phone numbers, with a maximum of 18 digits for each voice phone number.
E.g.Set the voice phone no. 2 as 88776655.

[012345] + * +[0]+ # + [4] + SOS + [2]+ SOS

→ VOICE PHONE NO.:*DEL
LCD display
+ [88776655] + SOS

The keypad will beep twice to confirm it has been set, the keypad will return to previous setting.Press ARM + ARM + SOS back to standby interface.

5. Set sys options

[012345] + * +[0]+ # + [5] + SOS →
1] SYS SETTING
2] ALARM SETTING

5.1 Sys setting

[012345] + * +[0]+ # + [5] + SOS + SOS

→ 1> AC OFF DELAY
2> SENSOR LOSS CHECK
3> DOOR SENSOR CHECK
4> SENSOR TAMPER
5> SYS LV RPT
6> SYS TAMPER CHECK
7> WIRED SIREN TYPE

5.1.1 AC off delay

Factory default: 15min

It means the time when AC off, the device will delay 15min to report to CMS about AC off.E.g. Set AC off report delay time as 5min

[012345] + * +[0]+ # + [5] + SOS + SOS + SOS

→ AC OFF PRT DELAY: 005
(000--999)M
LCD display
+ [005] + SOS

The keypad will beep twice to confirm it has been set, the keypad will return to previous setting.Press ARM + ARM + ARM + SOS back to standby interface.

5.1.2 Sensor loss check: default value is 10 hour

Example: set detector loss check time is every 4 hours

[012345] + * +[0]+ # + [5] + SOS + SOS + [2] + SOS

→ SENSOR LOSS CHECK: 10
(00--99) H 0 DISABLE
LCD display
+ [04] + SOS

The keypad will beep twice to confirm it has been set, the keypad will return to previous setting.Press ARM + ARM + ARM + SOS back to standby interface.

Note: wireless detector send status report is every 3 hours, if the panel do not receive the report or alarming information, the detector will be regarded as loss. Recommended sensor loss check time is every 4 hours or above.

5.1.3 Door sensor check

When the door sensor is open, the panel will display zone trouble(default value is disable), example: set door sensor check to be enable.

[012345] + * +[0]+ # + [5] + SOS + SOS + [3] + SOS

→ DOOR SENSOR CHECK:1
1>DISABLE 2>ENABLE
LCD display

+ [2] + SOS

The keypad will beep twice to confirm it has been set, the keypad will return to previous setting.Press ARM + ARM + ARM + SOS back to standby interface.

5.1.4 Sensor tamper

After activating the detection, trigger the detector disassembly switch, and the host will alarm (default is disabled), for example: enabling detection.

[012345] + * +[0]+ # + [5] + SOS + SOS + [4] + SOS

→ SENSOR TAMPER: 1
1>DISABLE 2>ENABLE
LCD display

+ [2] + SOS

The keypad will beep twice to confirm it has been set, the keypad will return to previous setting.Press ARM + ARM + ARM + SOS back to standby interface.

5.1.5 System Low Voltage Report

Whether to send a report when the host battery is low voltage, enabled by default, for example: turn off the report.

[012345] + * +[0]+ # + [5] + SOS + SOS + [5] + SOS

SYS LV RPT: 2
1>DISABLE 2>ENABLE
LCD display

+ [1] + SOS

The keypad will beep twice to confirm it has been set, the keypad will return to previous setting.Press ARM + ARM + ARM + SOS back to standby interface.

5.1.6 System tamper check

After activating the detection, trigger the detector disassembly switch, and the host will alarm (default is disabled), for example: enable detection.

[012345] + * +[0]+ # + [5] + SOS + SOS + [6] + SOS

SYS TAMPER CHECK: 1
1>DISABLE 2>ENABLE
LCD display

+ [2] + SOS

The keypad will beep twice to confirm it has been set, the keypad will return to previous setting.Press ARM + ARM + ARM + SOS back to standby interface.

5.1.7 Wired siren type

Select based on the type of alarm signal connected.

For example: select a single bus.

[012345] + ✱ +[0]+ # + [5] + SOS + SOS + [7] + SOS

→ WIRED SIREN TYPE: 2
0>SBUS 1>ACT 2>PAS
LCD display

+ [0] + SOS

The keypad will beep twice to confirm it has been set, the keypad will return to previous setting.Press ARM + ARM + ARM + SOS back to standby interface.

5.2 Alarm setting

[012345] + ✱ +[0]+ # + [5] + SOS + [2] + SOS

→ 1> ENTER DELAY
2> EXIT DELAY
3> BELL TIME
4> FORCE ARM
5> ARM/DISARM RPT
6> VOICE PROMPT
7> ALARM TIMES LIMIT
8> EMERGENCY TONE

5.2.1 Enter delay

When alarm happens from delay zone, the device will delay to alarm for 10s in factory default.E.g. Set enter delay time as 20s.

[012345] + ✱ +[0]+ # + [5] + SOS + [2] + SOS + SOS

→ ENTER DELAY :010
(001--255)S
LCD display

+ [020] + SOS

The keypad will beep twice to confirm it has been set, the keypad will return to previous setting.Press ARM + ARM + ARM + SOS back to standby interface.

5.2.2 Exit delay

Factory default time: 10s

It means, when user arms the system, it can not be valid at once, but only after 30s ,the system will enter into arm status. The delay time can leave the user enough time to leave the house without triggering the system.E.g. Set exit delay time as 20s

[012345] + * +[0]+ # + [5] + SOS + [2] + SOS + [2] + SOS

→ EXIT DELAY:010 (001--255)S + [020] + SOS

LCD display

The keypad will beep twice to confirm it has been set, the keypad will return to previous setting.Press ARM + ARM + ARM + SOS back to standby interface.

5.2.3 Bell time

The alarm to ring after the host alarms，default 5 minutes.

E.g. Set bell time as 10min

[012345] + * +[0]+ # + [5] + SOS + [2] + SOS + [3] + SOS

→ BELL TIME: 05 (00--30)M + [10] + SOS

LCD display

The keypad will beep twice to confirm it has been set, the keypad will return to previous setting.Press ARM + ARM + ARM + SOS back to standby interface.

5.2.4 Force arm

Factory default: enable

When there is zone fault, user will be not able to arm the device. But if set force arm, it is OK to arm, at the same time, the zone in fault will be bypassed with SMS or CMS report. E.g. Enable force arm

[012345] + * +[0]+ # + [5] + SOS + [2] + SOS + [4] + SOS



+ [2] + SOS

LCD display

The keypad will beep twice to confirm it has been set, the keypad will return to previous setting.Press ARM + ARM + ARM + SOS back to standby interface.

5.2.5 ARM/DISARM RPT

Set whether to upload the arm/disarm report to the center (default is enabled).

E. g. Set to disable uploading arm/disarm information to the center.

[012345] + * +[0]+ # + [5] + SOS + [2] + SOS + [5] + SOS



+ [1] + SOS

LCD display

The keypad will beep twice to confirm it has been set, the keypad will return to previous setting.Press ARM + ARM + ARM + SOS back to standby interface.

5.2.6 Voice prompt

The host arm and disarm, alarm and other voice prompts

For example: set to open local voice prompts

[012345] + ✱ +[0]+ # + [5] + SOS + [2] + SOS + [6] + SOS

→ ARM/DISARM TONE: 1
1>DISABLE 2>ENABLE
LCD display

+ [2] + SOS

Tthe keyboard beeps twice, indicating that the local voice prompt is successfully turned on. After setting, the keyboard will automatically return to the previous interface. Press ARM + ARM + ARM + SOS back to standby interface.

5.2.7 Alarm times limit

After the zone alarm, whether the number of times of triggering the zone alarm again is 3 times. If the limit of alarm times is selected, the host will not alarm again after 3 times of alarm (default is unlimited)

For example, set the number of alarms to limit.

[012345] + ✱ +[0]+ # + [5] + SOS + [2] + SOS + [7] + SOS

→ ALARM LIMIT: 1
1>DISABLE 2>ENABLE
LCD display

+ [2] + SOS

The keypad will beep twice to confirm it has been set, the keypad will return to previous setting.Press ARM + ARM + ARM + SOS back to standby interface.

5.2.8 Emergency tone

Factory default: mute.

E.g. Set emergency alarm tone as ring.

[012345] + * +[0]+ # + [5] + SOS + [2] + SOS + [8] + SOS

→ EMERGENCY TONE: 1
1>MUTE 2>SOUND
LCD display
+ [2] + SOS

The keypad will beep twice to confirm it has been set, the keypad will return to previous setting.Press ARM + ARM + ARM + SOS back to standby interface.

6. Set wireless

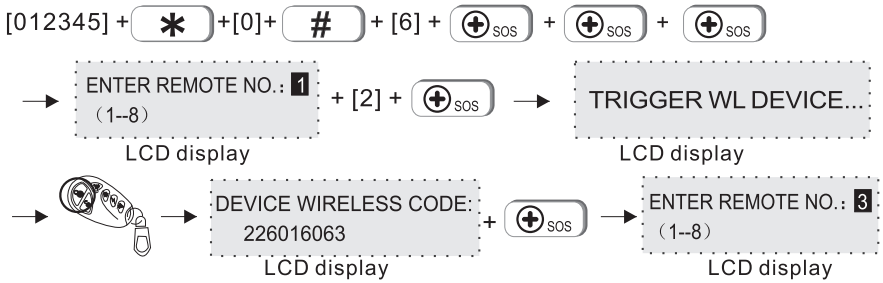
[012345] + * +[0]+ # + [6] + SOS →
- 1] SET REMOTE
- 2] SET WL DETECTOR
- 3] SET WL SIREN
- 4] SET SMART DEVICE
- 5] SET RFID

6.1 Set remote

[012345] + * +[0]+ # + [6] + SOS + SOS →
- 1)REMOTE ENROLL
- 2)REMOTE CODE
- 3)DELETE REMOTE

6.1.1 Remote enroll

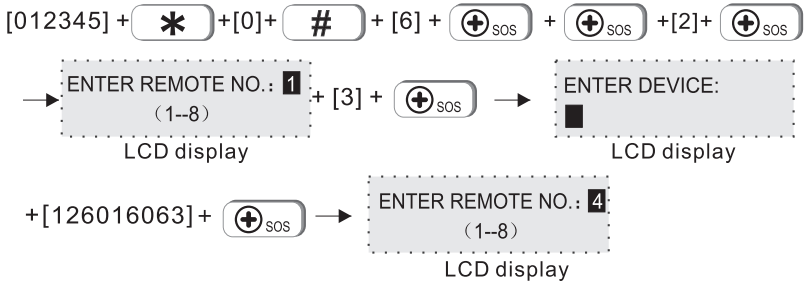
Example: enroll remote to the #2 remote in alarm panel



The keypad will beep twice to confirm it has been set, the keypad will return to previous setting.Press ARM + ARM + ARM + SOS back to standby interface.

6.1.2 Remote code

Example: manually enter the address code of remote 126016063 to be #3 remote in alarm panel

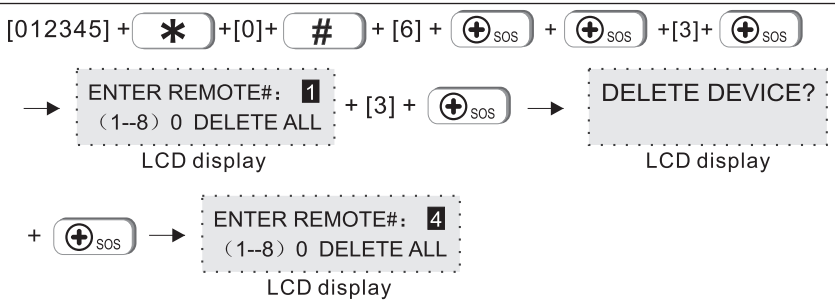


The keyboard beeps twice, indicating success. After the addition is completed, the keyboard will automatically enter the next remote adding.

Press ARM + ARM + ARM + ARM + SOS back to standby interface.

6.1.3 Delete remote

Example: delete #3 remote

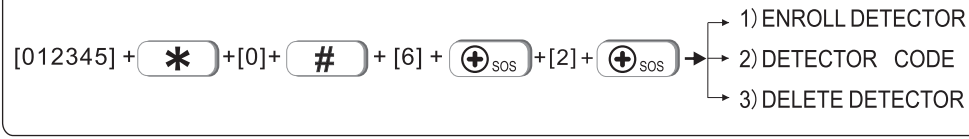


The keyboard beeps twice to indicate success. After the deleting is completed, Keyboard automatically goes to next remote delete.

Press ARM + ARM + ARM + ARM + SOS back to standby interface.

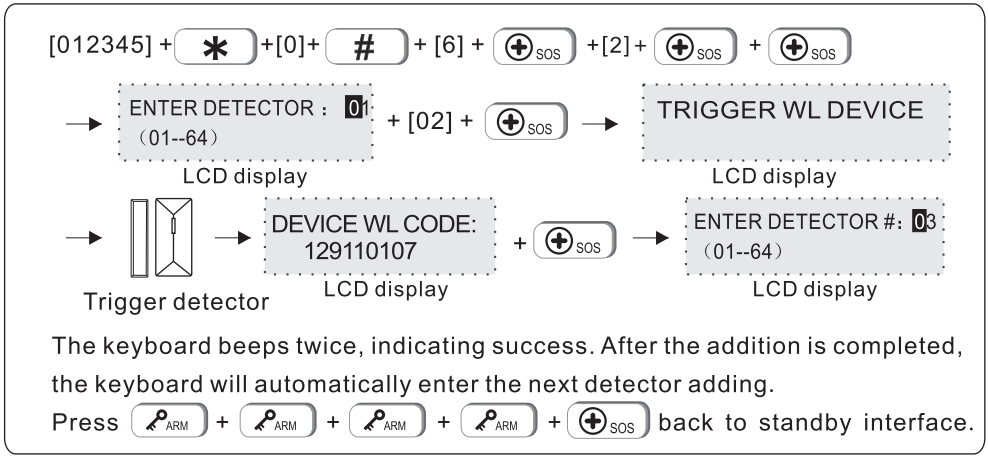
Note: enter 0 to delete all remotes

6.2 Set WL detector



6.2.1 Enroll detector

Example: enroll detector to #2 detector in the alarm panel.

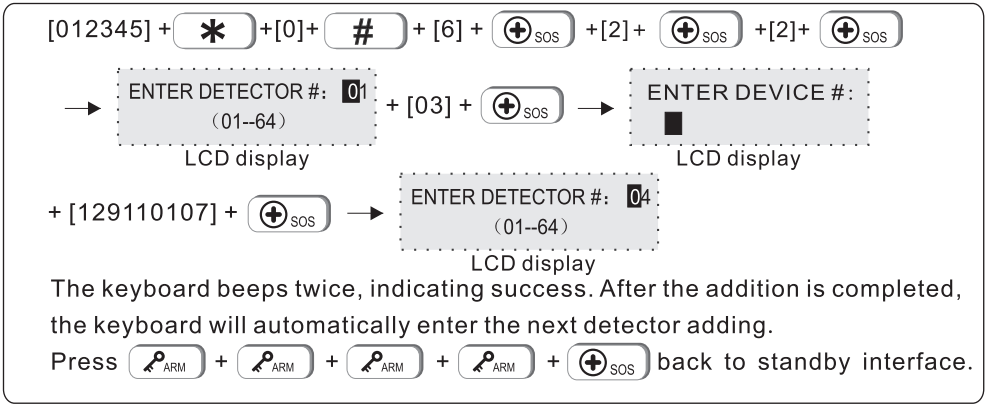


The keyboard beeps twice, indicating success. After the addition is completed, the keyboard will automatically enter the next detector adding.

Press ARM + ARM + ARM + ARM + SOS back to standby interface.

6.2.2 Detector code

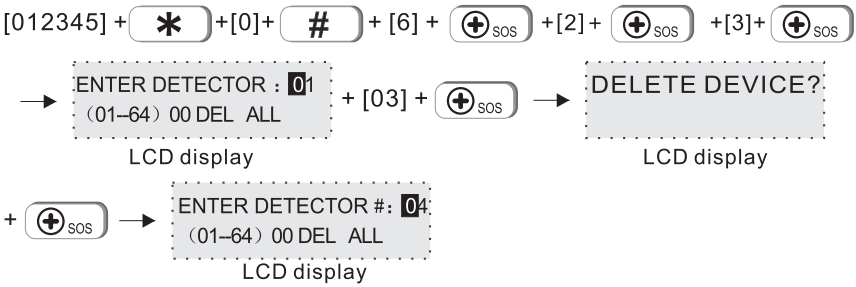
Example: manually enter the address code of detector 129110107 to be #3 detector in alarm panel.



The keyboard beeps twice, indicating success. After the addition is completed, the keyboard will automatically enter the next detector adding.

Press ARM + ARM + ARM + ARM + SOS back to standby interface.

6.2.3 Delete detector



The keyboard beeps twice, indicating success. After the deleting is completed, the keyboard will automatically enter the next detector deleting.

Press ARM + ARM + ARM + ARM + SOS back to standby interface.

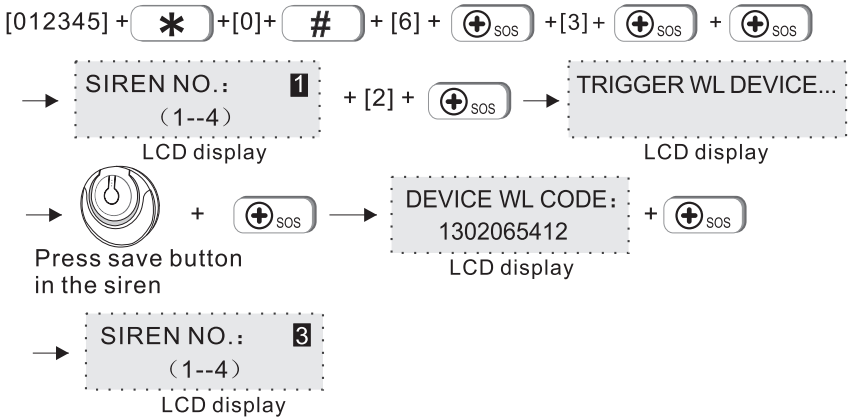
6.3 Set WL siren



Note: When the wired siren is not connected, it will display fault. If you don't want to connect wired siren , pls connect a 2.2k resistor to the wired siren port.

6.3.1 Enroll siren

Example: enroll siren to #2 siren in the alarm panel

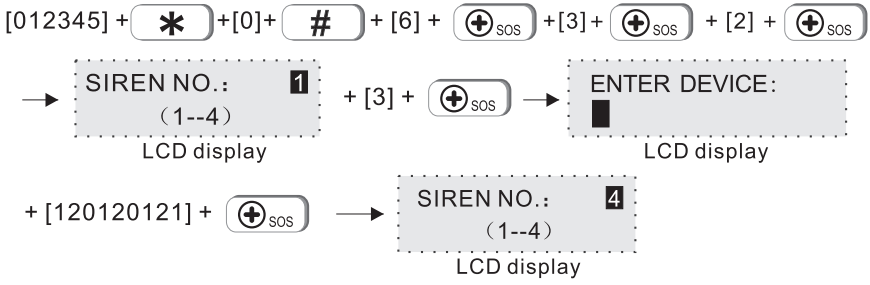


The keyboard beeps twice, indicating success. After the addition is completed, the keyboard will automatically enter the next siren adding.

Press ARM + ARM + ARM + ARM + SOS back to standby interface.

6.3.2 Siren code

For example, add the number 120120121 to #3 siren.

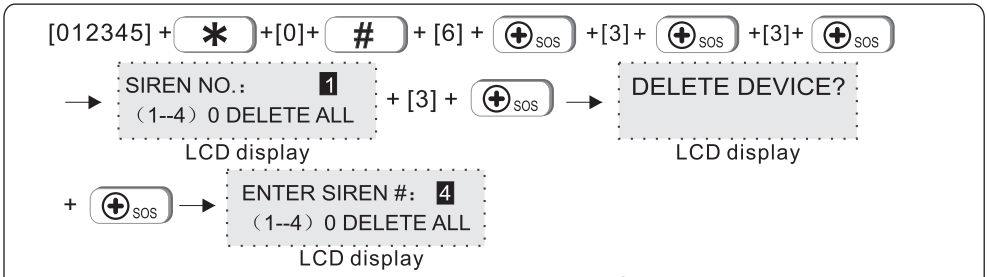


The keyboard beeps twice, indicating success. After the addition is completed, the keyboard will automatically enter the next siren adding.

Press ARM + ARM + ARM + ARM + SOS back to standby interface.

6.3.3 Delete siren

Example: delete #3 siren



The keyboard beeps twice, indicating success. After the deleting is completed, the keyboard will automatically enter the next siren deleting.

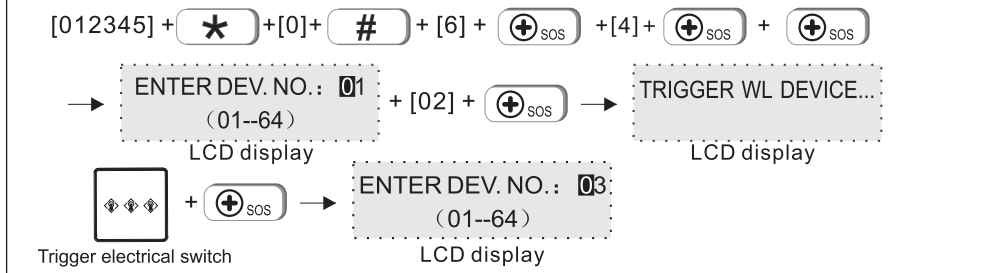
Press ARM + ARM + ARM + ARM + SOS back to standby interface.

6.4 Set smart device



6.4.1 Enroll smart device

Example: auto the wireless switch to the # 2 switch in host.

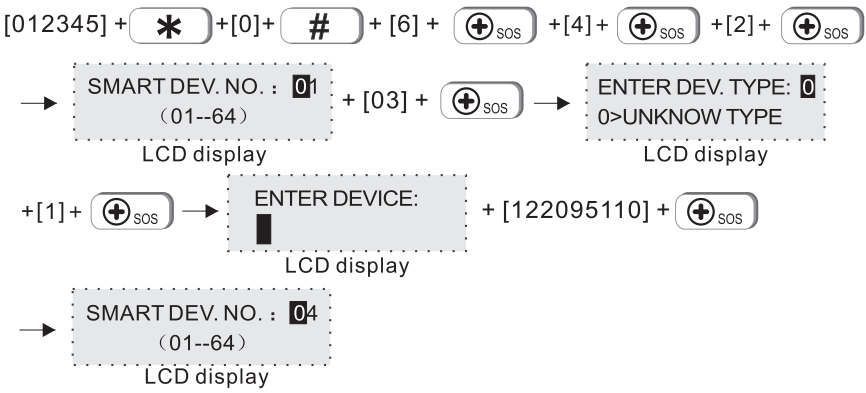


The keyboard beeps twice, indicating success. After the addition is completed, the keyboard will automatically enter the next switch adding.

Press ARM + ARM + ARM + ARM + SOS back to standby interface.

6.4.2 Smart device code

Example:add a wireless switch code of 122095110 to No. 3 in alarm panel.

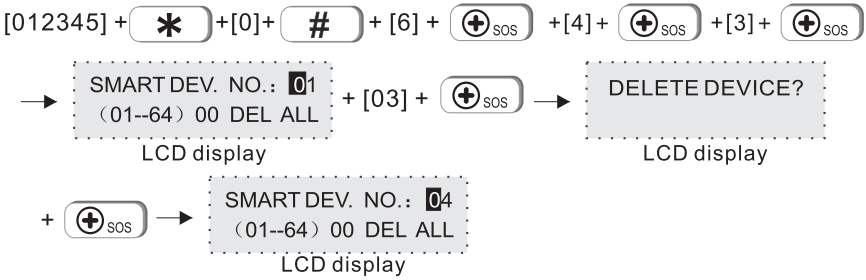


The keyboard beeps twice, indicating success. After the addition is completed, the keyboard will automatically enter the next switch adding.

Press ARM + ARM + ARM + ARM + SOS back to standby interface.

6.4.3 Delete smart device

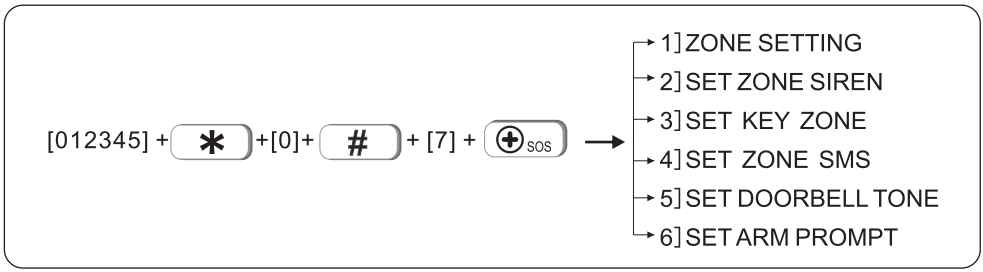
Example: delete the #3 switch.



The keyboard beeps twice, indicating success. After the deleting is completed, the keyboard will automatically enter the next switch deleting.

Press ARM + ARM + ARM + ARM + SOS back to standby interface.

7. Set system zone



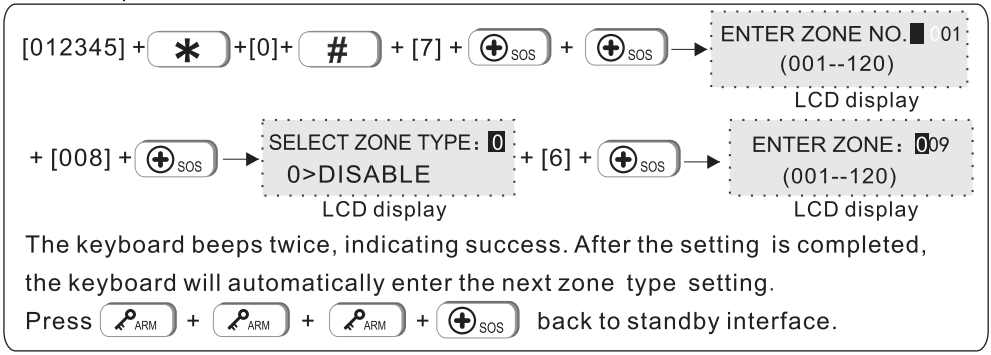
7.1 Set zone type

The options of zone types as below

0>DISABLE	1>DELAY ZONE	2>PERIMETER ZONE
3>INTERIOR ZONE	4>EMERGENCY ZONE	5>24 HOUR ZONE
6>FIRE ZONE	7>WATER ZONE	

1. The zone type refers to the alarm type displayed by the host after the detector set in the zone alarms. When the zone type is 0, the zone disable. Triggering the zone in any state will not cause the host to alarm.
2. The alarm will only be triggered when the internal zone is in the armed state.
3. When the delay and perimeter zone is in the state of home arm, it will alarm when triggered.
4. In any state of emergency, 24-hour, or fire protection zone, it will alarm when triggered.

Example: Set Zone 8 to be fire zone.



7.2 Set zone siren

Example: set zone 108 siren type to be pulse



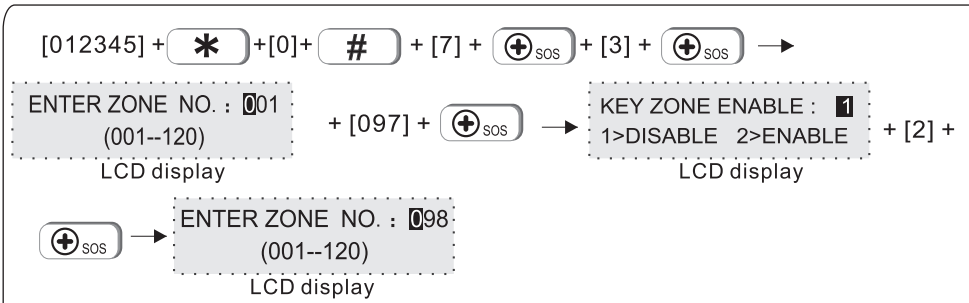
The keyboard beeps twice, indicating success. After the setting is completed, the keyboard will automatically enter the next siren type setting.

Press ARM + ARM + ARM + SOS back to standby interface.

7.3 Set key zone

Only 97 ~ 104 zones can be set with key zone, when the zone is set as key zone, trigger the zone host disarmed, zone recovery host deployment, mainly used for access control system.

For example, set the 97th zone to be the key zone.

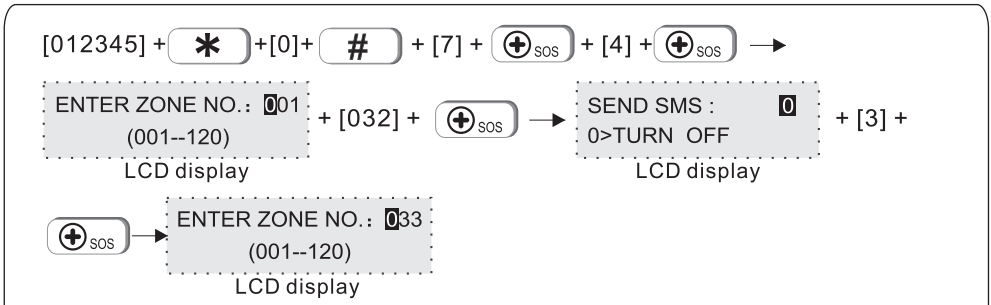


The keyboard beeps twice, indicating that the keyboard zone is successfully set. Then the keyboard will automatically enter the next key zone setting.

Press ARM + ARM + ARM + SOS back to standby interface.

7.4 Set zone SMS

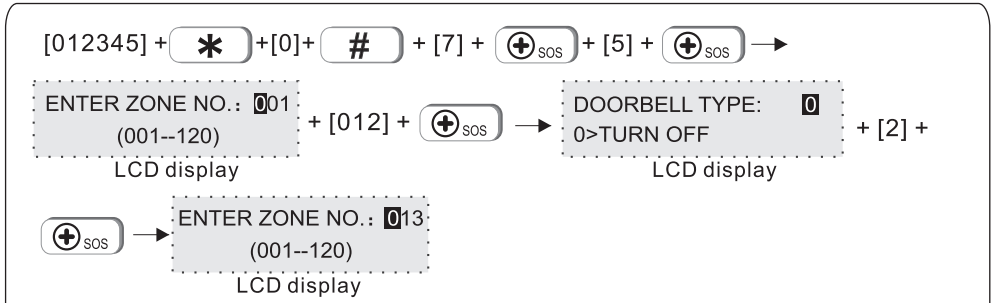
When a zone is triggered, the host sends a text message to the user. Optional SMS types are: 0>TURN OFF 1> ALARM 2>Faults 3>Alarms and Faults
For example, set the 32 zone SMS type to alarm and fault.



The keyboard beeps twice, indicating that the keyboard zone is successfully set.
Then the keyboard will automatically enter the next zone SMS setting.
Press ARM + ARM + ARM + SOS back to standby interface.

7.5 Set doorbell tone

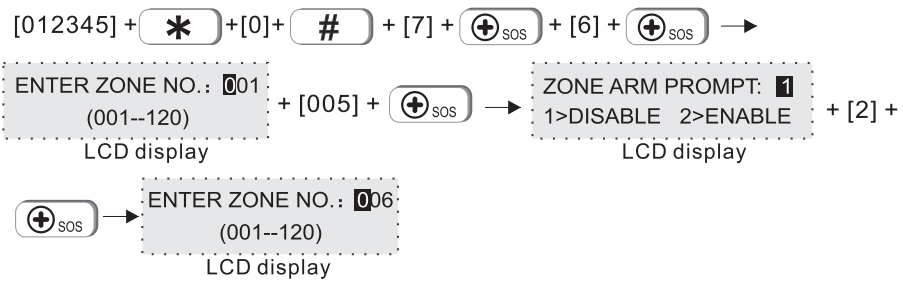
Optional door ring type has 0>TURN OFF, 1>DISARM BELL, 2>ORDINARY BELL.
For example, set the #12 zone doorbell tone to ordinary bell.



The keyboard beeps twice, indicating success. After the setting is completed, the keyboard will automatically enter the next doorbell tone setting.
Press ARM + ARM + ARM + SOS back to standby interface.

7.6 Set arm prompt: Default is disable

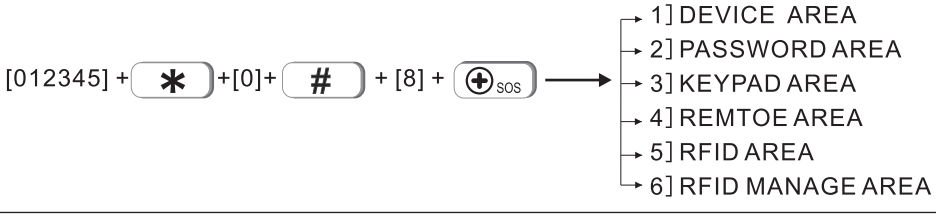
For example, enable Zone 5 deployment alerts.



The keyboard beeps twice, indicating success. After the setting is completed, the keyboard will automatically enter the next arm prompt setting.

Press ARM + ARM + ARM + SOS back to standby interface.

8. Set system area



The host supports 8 partitions, and devices can be assigned to any partition.

Passwords, keyboards, remote controls can be set to manage one or more partitions. When passwords, remote controls, keyboards manage multiple partitions, all actions work simultaneously on all partitions they manage.

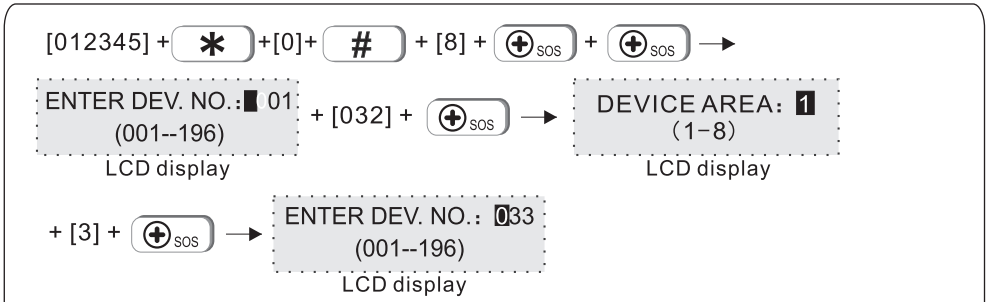
Partition 1 is the primary partition, and all system events are reported to partition 1, and only partition 1 is in the disarmed state when entering the system settings.

Note: This machine does not support RFID function.

8.1 Device area (Default belongs to partition 1)

Devices may be assigned to 1 - 8 partitions.

E.g., setting the device 32 to a 3 partition.



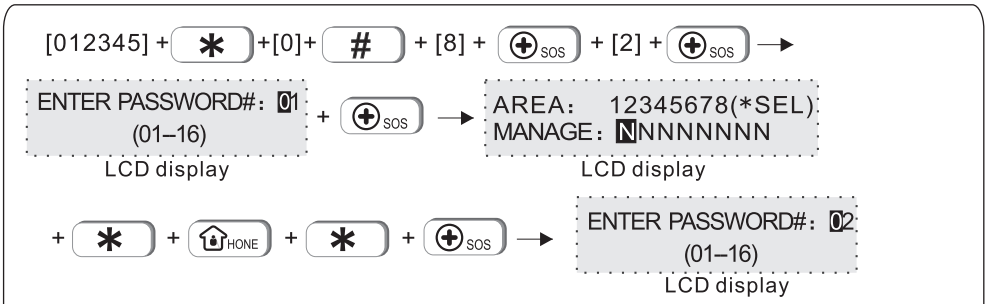
The keyboard beeps twice, indicating success. After the setting is completed, the keyboard will automatically enter the next setting.

Press ARM + ARM + ARM + SOS back to standby interface.

8.2 Password area (Disable by default)

1 user password can control 1 ~ 8 partitions.

E.g., set user password 1 to control 1 partition and 3 partition.



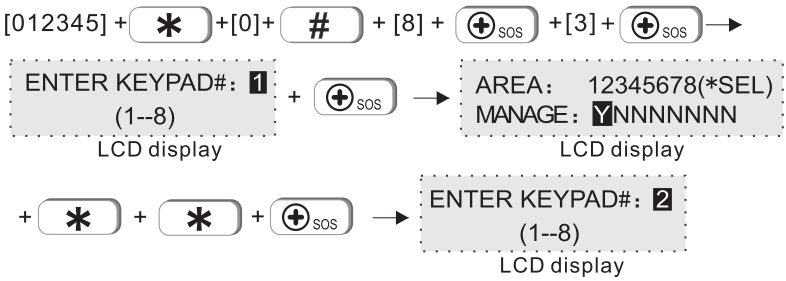
The keyboard beeps twice, indicating success. After the setting is completed, the keyboard will automatically enter the next setting.

Press ARM + ARM + ARM + SOS back to standby interface.

Note: Y--enable N--disable, Press " * " to switch.

8.3 Keypad area (default value is area 1)

The keyboard can only display information about the partition to which it belongs. E. g. , by setting keyboard 1 to control the partition 2.

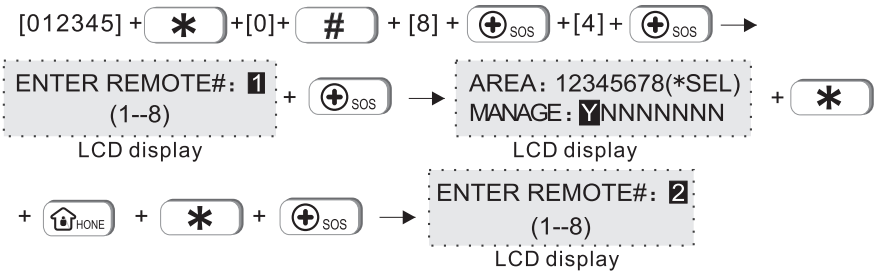


The keyboard beeps twice, indicating success. After the setting is completed, the keyboard will automatically enter the next setting.

Press ARM + ARM + ARM + SOS back to standby interface.

8.4 Remote area (Default management remote control 1 partition)

E.g., setting remote #1 to control partition 3.



The keyboard beeps twice, indicating success. After the setting is completed, the keyboard will automatically enter the next setting.

Press ARM + ARM + ARM + SOS back to standby interface.

9. Set 4G

[012345] + ✱ +[0]+ # + [9] + SOS →
- 1] 4G ENABLE
- 2] 4G APN SETTING
- 3] 4G USER NAME
- 4] 4G PASSWORD

9. 1 4G enable (default enabled)

After inserting the available 4G card, whether to enable 4G function after disconnecting the network cable. For example, disable 4G.

[012345] + ✱ +[0]+ # + [9] + SOS + SOS →

4G ENABLE: 2
1>DISABLE 2>ENABLE

+ [1] + SOS

LCD display

The keyboard beeps twice, indicating success.after the setting is completed, the keyboard will automatically enter the next setting.

Press ARM + ARM + SOS back to standby interface.

9. 2 4G APN setting (default enabled)

Please obtain APN setting information from your carrier. Press the numeric keys 2 ~ 9 repeatedly to switch between upper and lower case letters.

[012345] + ✱ +[0]+ # + [9] + SOS + [2] + SOS →

4G APN SETTING:
CMNET

+ [1] + SOS

LCD display

The keyboard beeps twice, indicating success.after the setting is completed, the keyboard will automatically enter the next setting.

Press ARM + ARM + SOS back to standby interface.

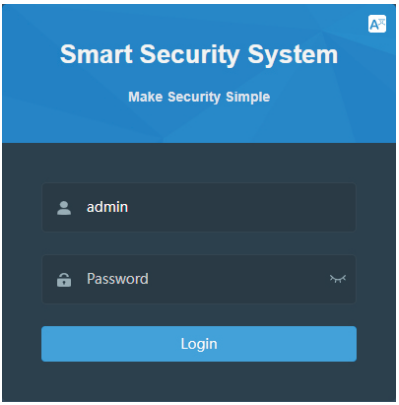
9.3 4G username and password

Please obtain your 4G username and password from your carrier, and press the number keys 2 - 9 repeatedly to switch between upper and lower case letters.Refer to 4G APN settings.

II.Web setting

1. Device startup

Connect the host to the power supply and plug in the network cable. The computer used for webpage login is on the same router as the host.



2. Accessing the host

The default IP address of the host is 192.168.1.106. If the IP address is assigned by the router, users can obtain it through the following two methods:

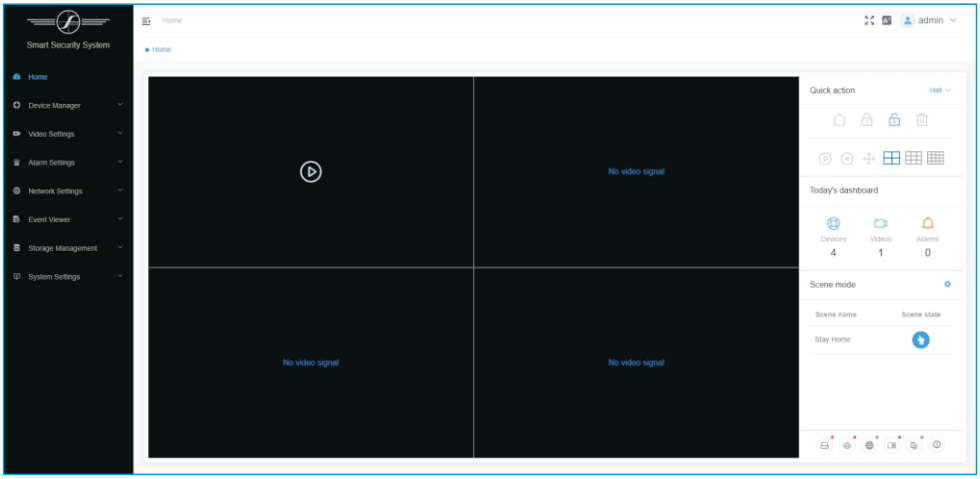
a. Press the keyboard * 2# to query.

b. Log in to the mobile app for query (see the following instructions for app usage).

After obtaining the IP address, enter the IP address in the browser address bar to access the device.

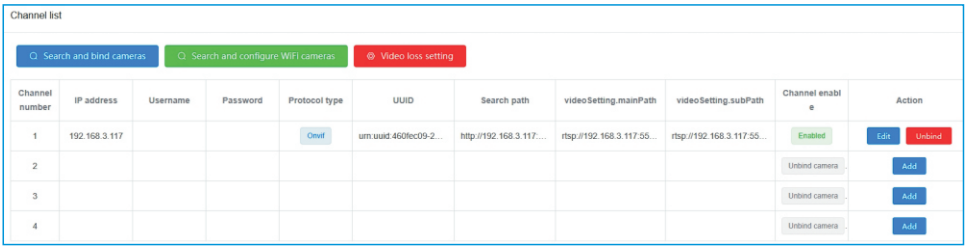
Default username: admin, password is blank (language can be modified in the upper right corner).

After logging in, enter the interface shown in the figure below.



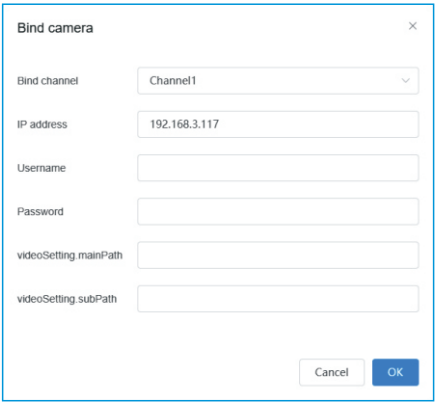
3. Camera addition

When adding a camera, please keep the host and camera on the same LAN, and you can add 4 network cameras or WiFi cameras. Click on "Video Settings - Video Channel" to enter the video search interface on the right.



Search and bind cameras: Use the ONVIF protocol to search for network cameras. Connect the camera and the host to the same LAN (same router), modify the camera IP to the legal address under the router, click "Search and Bind Camera" - click "Bind" in the column of the camera to be added, and fill in the camera information in the pop-up window.

The default user name for the camera is "admin" and there is no user password. If adding cameras from other manufacturers, the actual account password will be filled in. Click on "Edit" in the enabled channel list and close the "Channel Enable" column to deactivate the camera. After setting up, click "Save" and the interface prompts that the operation was successful.



Search and configure WiFi cameras: This feature is only applicable to Meian WiFi cameras. To close the WiFi connection, please first go to "Network Settings - Basic Settings - Wireless STA", close the "Enable" button, and save. During WiFi search, the host acts as a hotspot to configure WiFi for the camera and modify the camera IP address.

Add operation: The WiFi camera and the host are in the same local area network. Click "Search and Configure WiFi Cameras", and in the WiFi camera column found, click "Configure" to disconnect the WiFi camera network cable. After configuration is completed, the channel list displays the bound cameras.

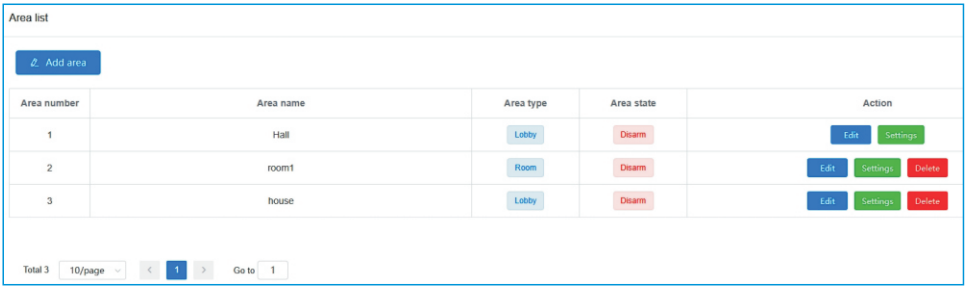
4. Regional settings

Users can set multiple zones and assign devices to their respective zones, making it

easy to locate the alarm device location when an alarm is triggered. They can also set zone deployment and removal to achieve synchronous management of multiple devices within the same zone.

Add/Remove Area: Click on "Device Manager Partition Management Add Area", enter the area name in the pop-up window, select the area type, and click "OK". Region 1 is the default region and cannot be deleted. Other regions can be deleted by clicking the "Delete" button.

Regional Settings: Click on the "Settings" button in the regional table to set whether to send SMS or make phone calls when deploying or disarming. To use this function, please first enter the "Alarm Settings - Alarm Center - Phone Settings" section to set the phone number and number of calls.



5. Addition of accessories

PGM description: Click "Device Manager - Device Management", and Switch 0/Switch 1 in the device list is PGM 1/PGM 2 in the wiring terminal. After connecting to the device, click "Switch Control" to turn it on or off.

Click on "Device Manager - Device Management" to select two methods: "Automatic device search" and "Manual device addition".

5.1 Automatic search device: Add by comparing the code with the host. Place the wireless device within a 3-meter range of the host, click on "Auto Search for Devices", and trigger the device. After successful reception, the webpage displays the device type and ID.

Binding channel: refers to the channel that the device needs to associate with. After deployment and insertion of an available TF card, the binding channel will automatically record when the detector triggers an alarm.

Save and take effect after setting.



5.2 Manual device addition: FSK 433MHz devices and single bus can be added.

a. Select "FSK" for the wireless device access method, manually enter the device ID, which is the nine digit address code on the sticker on the back of the device, to add.

b. Select "Single Bus SBUS" for single bus defense zone. Please select the defense zone code based on the actual single bus dialing.

A red “*” is required.

After setting up, click “Save” to take effect.

6. Scenario management

It is divided into timed scenes, triggered scenes, and manual scenes, and can add up to 200 scenes* This product does not support relay access. In the scenario, Switch 0/Switch 1 is PGM 1/PGM 2.

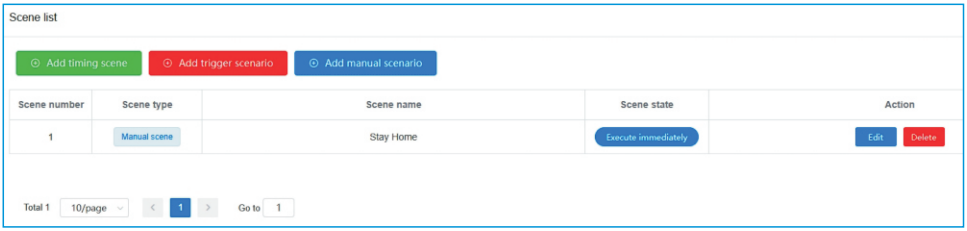
Timed scenario: a. Timed deployment and removal - The selected area automatically executes deployment and removal at the set time.

b. Timed PGM switch - PGM is turned on or off at the time set in the repetition cycle.

Trigger scenario: divided into device triggering and event triggering linkage. After triggering the device or event, the linkage PGM open/close action is executed after the delay time ends.

Manual scene: Manually activate the scene, and execute the deployment/removal/PGM switch after the scene delay time.

After setting up, click 'Save' to take effect.



7. Deployment and Deployment Settings

Go to the "Home" page, click on the "Quick Operations" pop-up window " ⌄ ", select an area, and then deploy/disarm. The screen will have a corresponding pop-up prompt, and the host will voice prompt "Zone X is deployed/disarmed/left behind". Clear the alarm without voice prompt.



8. Video control

8.1 Preview

Click on the shortcut icon on the right side of the homepage to proceed:

Preview all channels Stop previewing

Or click on " ▷ " in a single video channel to preview the current video.

The pan tilt control function requires camera support.

8.2 Video recording and playback

This device only records alarm videos.

Video recording: Video recording needs to be done with the TF card inserted and the detector bound to the channel. When the detector triggers an alarm, the channel will automatically record the video.

Playback: Click on "Storage Management - Video Playback", select the channel and date, and click " ▷ " to play back.

9. Network Settings

Click on "Network Settings" to configure network parameters. Attention: The wireless Ap setting and wireless STA setting cannot be turned on simultaneously.

Ethernet: This machine automatically obtains IP addresses by default. If you need to change the IP address, please turn off automatic acquisition first.

Wireless Ap: This setting is used when the host is connected to a WiFi camera as a hotspot. Non professionals are not allowed to modify it.

Wireless STA: When the host connects to the router, enter the WiFi name and password and click "Save". The encryption method defaults to "auto". After disconnecting the network cable, the host starts connecting to WiFi.

Mobile network: Please consult your phone number operator for access methods, dialing codes, etc. After enabling mobile networks, when both wired and WiFi networks are disconnected, the host starts using 4G networks.

10. Platform Connection

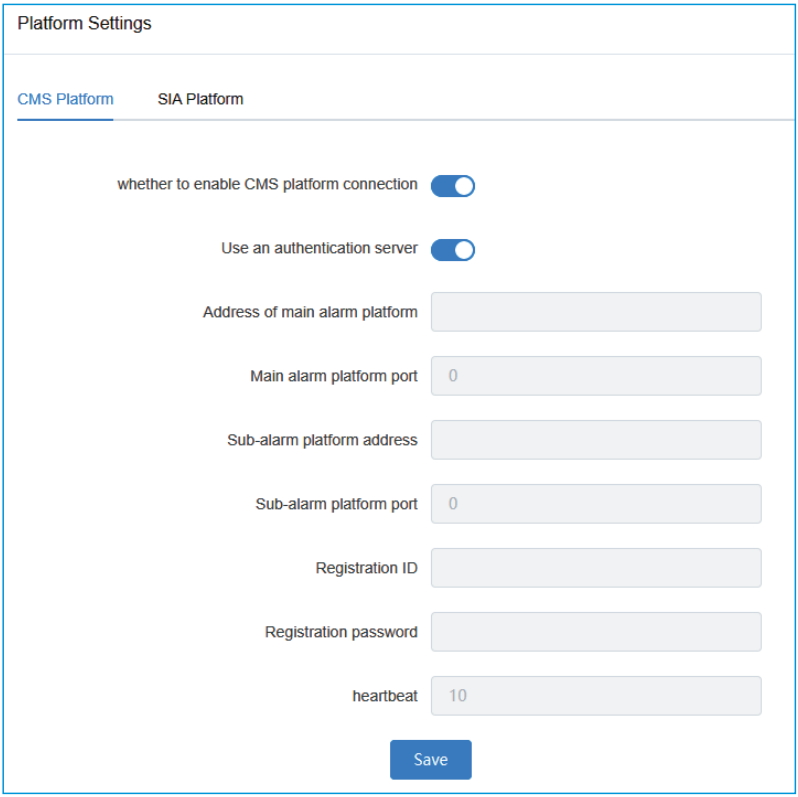
Enter the host webpage 'Network Settings Platform Settings CMS Platform', and automatic authentication will be enabled by default. If manually filled in, Please refer to the following filling:

Main alarm platform address: Fill in according to the actual situation. If you need assistance, please consult the product seller.

Main alarm platform port: 7809.

ID: Go to "System Settings" - "Version Information" to view the device ID (pay attention to capitalization).

After filling it in, click "Save".



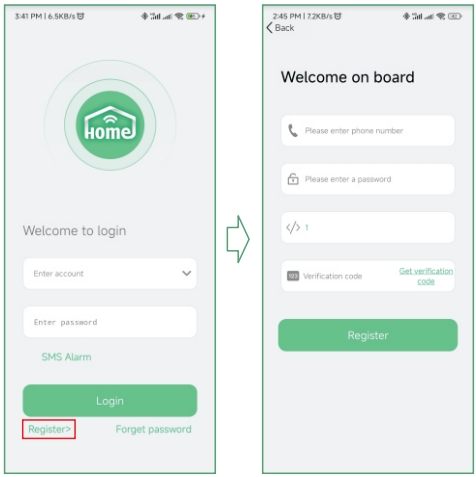
III. App use

1. Download and installation

Please scan QR code below to download iOS & Android app, or search “Smartsecurity” in iOS&Googleplay store.

2. Account registration

Click to enter the APP login interface, new users please click "register", according to the prompt to complete the registration.



3. Add panel

After logging in the account, as shown in Fig 3.1, select " + "--at the upper right " ⛶ " to scan the QR code sticker on the device body or the QR code on the webpage to add the device.

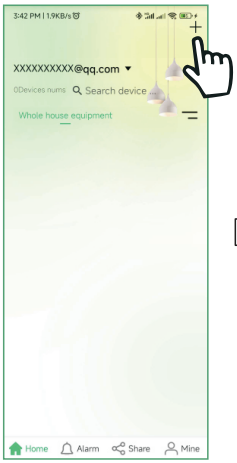


Fig 3.1

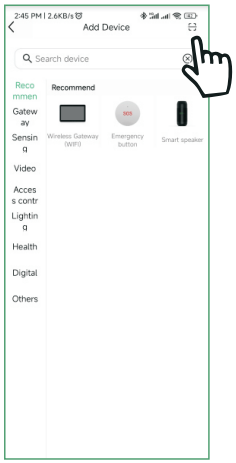


Fig 3.2

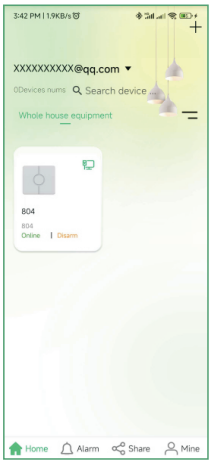


Fig 3.3

Account registration

Click to enter the APP login interface, new users please click "register", according to the prompt to complete theregistration.

4. WiFi connection

Please complete the following operations within 10 minutes after the host is powered on:

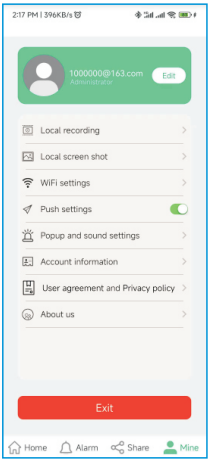
a. Enter the APP and click "WiFi Settings" _"Sonic Configuration WiFi.

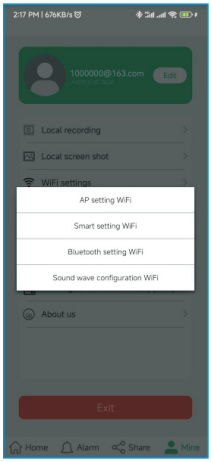
b. Select the WiFi to be configured and enter the WiFi password, click "OK".

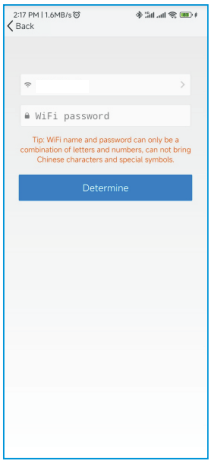
c. Turn up the volume of the phone and bring the phone close to the host.

d. The host voice prompts "WiFi configuration is successful" and returns to the area interface.

After a while, the host goes online.If the host is not online, please check whether the configured WiFi is available and whether thepassword is correct.







5. Add cameras

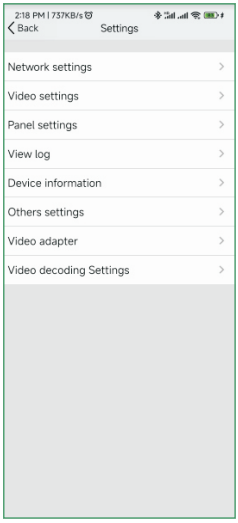
Search for all online cameras on the same local area network as the host.

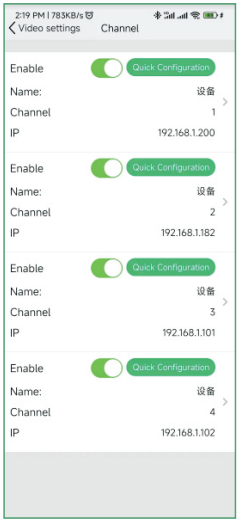
A. Enter the app and click on the online host-settings button at the top right " ⚙ ".

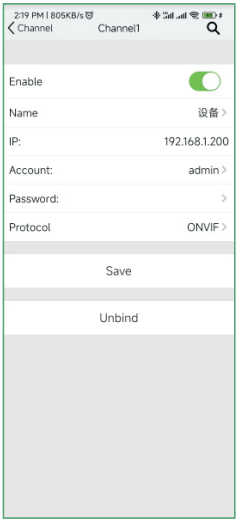
B. Click "Video Settings"-"Video Channel"in turn.

C. Click on the video channel you want to add " > "-Search for Devices " 🔍 ".

D. Select the IP address of the camera to be added, and click "Save"to enter the channel settings.







System maintenance

PERIODIC TESTING

The design idea of safety system is to let you maintain as little as possible. However, in order to ensure the reliability of the system, we still need to carry out "walking test" at least once in three months. If there is any problem, please consult the technician immediately.

CLEAN THE MAIN HOST

After using for a period of time, the host may be stained with oil or dust. Please clean with soft cotton cloth or sponge and wipe dry.

Note: please do not use any friction agent or organic solvent, such as kerosene, acetone, strong glue, etc. to wipe the case, so as not to damage the external appearance of the body.

Product function limitation

Although the alarm device you purchased is highly safe, it is still not 100% safe. No matter how advanced the alarm system is, there will be false alarm or failure. The reasons may be as follows:

Lack of maintenance: if the system is used for a long time, but maintenance and testing are not carried out immediately, the sensitivity of the detector may be reduced and false alarm or missing alarm may occur; the siren may also lose its function and cannot sound.

Power failure: if the AC power supply is cut off for a long time, and the backup battery is insufficient, the system will not continue to work normally, so that the protection area can not alarm accordingly even if there is an alarm.

Limitations of smoke detector: sometimes, because the alarm occurs on different floors of the house or is too far away from the detector, the smoke detector fails to receive a strong enough smoke signal,which will cause missed alarm.

The system fails to receive the alarm information: if the intruder uses the unprotected skylight and some unexpected entrances to enter, or the intruder has the relevant professional knowledge and knows how to find the method to make the alarm equipment fail, the alarm equipment will not report the alarm immediately.

In order to ensure the normal operation of the detector and the whole alarm system, it is recommended that users often carry out periodical testing. Even if the alarm system is installed for protection, users should also be cautious about the safety of their lives and property. We will continue to devote ourselves to the development of new security products. Please keep in touch with us so as to obtain our latest technical products and relevant information. Your support is the driving force of our work! If our series of products are updated, we will publish them on our website. Please visit our website to get the latest information.

For Inquiries, Please contact:

Security Shop doo
Vladimira Nazora 1, 11070 Novi Beograd
Tel: +381 11 318 68 68, www.securityshop.rs

BLAUPUNKT and the BLAUPUNKT logo are trademarks of TALISMAN BRANDS (Luxembourg) S.A.R.L.and are used under license from Talisman Brands, Inc.
BLAUPUNKT licensees are solely responsible for the BLAUPUNKT branded products manufactured, distributed and sold under license.
www.blaupunkt.com