Network Security Control Panel

User Manual

UD.6L0206D1044A02

User Manual

About this Manual

This Manual is applicable to Control Panel

The Manual includes instructions for using and managing the product. Pictures, charts, images and all other information hereinafter are for description and explanation only. The information contained in the Manual is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version in the company website (http://overseas.hikvision.com/en/).

Please use this user manual under the guidance of professionals.

Trademarks Acknowledgement

HIKVISION and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions. Other trademarks and logos mentioned below are the properties of their respective owners.

Legal Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, IS PROVIDED "AS IS", WITH ALL FAULTS AND ERRORS, AND HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT OF THIRD PARTY. IN NO EVENT WILL HIKVISION, ITS DIRECTORS, OFFICERS, EMPLOYEES, OR AGENTS BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA OR DOCUMENTATION, IN CONNECTION WITH THE USE OF THIS PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

REGARDING TO THE PRODUCT WITH INTERNET ACCESS, THE USE OF PRODUCT SHALL BE WHOLLY AT YOUR OWN RISKS. HIKVISION SHALL NOT TAKE ANY RESPONSIBILITES FOR ABNORMAL OPERATION,

PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER ATTACK, HACKER ATTACK, VIRUS INSPECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.

SURVEILLANCE LAWS VARY BY JURISDICTION. PLEASE CHECK ALL RELEVANT LAWS IN YOUR JURISDICTION BEFORE USING THIS PRODUCT IN ORDER TO ENSURE THAT YOUR USE CONFORMS THE APPLICABLE LAW. HIKVISION SHALL NOT BE LIABLE IN THE EVENT THAT THIS PRODUCT IS USED WITH ILLEGITIMATE PURPOSES.

IN THE EVENT OF ANY CONFLICTS BETWEEN THIS MANUAL AND THE APPLICABLE LAW, THE LATER PREVAILS.

0100001050519

Regulatory Information

FCC Information

FCC compliance: This equipment has been tested and found to comply with the limits for 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.

FCC Conditions

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.
2. This device must accept any interference received, including interference that may cause undesired operation.

EU Conformity Statement

This product and - if applicable - the supplied accessories too are marked with "CE" and comply therefore with the applicable harmonized European standards listed under the EMC Directive 2004/108/EC, the RoHS Directive 2011/65/EU.

2012/19/EU (WEEE directive): Products marked with this symbol cannot be disposed of as unsorted municipal waste in the European Union. For proper recycling, return this product to your local supplier upon the purchase of equivalent new equipment, or dispose of it at designated collection points. For more information see: www.recyclethis.info.

2006/66/EC (battery directive): This product contains a battery that cannot be disposed of as unsorted municipal waste in the European Union. See the product documentation for specific battery information. The battery is marked with this symbol, which may include lettering to indicate cadmium (Cd), lead (Pb), or mercury (Hg). For proper recycling, return the battery to your supplier or to a designated collection point. For more information see: www.recyclethis.info.

Industry Canada ICES-003 Compliance

This device meets the CAN ICES-3 (A)/NMB-3(A) standards requirements.

Safety Instruction

These instructions are intended to ensure that the user can use the product correctly to avoid danger or property loss.

The precaution measure is divided into 'Warnings' and 'Cautions':

Warnings: Serious injury or death may be caused if any of these warnings are neglected.

Cautions: Injury or equipment damage may be caused if any of these cautions are neglected.

	
Warnings Follow these safeguards to prevent serious injury or death.	**Cautions** Follow these precautions to prevent potential injury or material damage.

 **Warnings:**

- Please adopt the power adapter which can meet the safety extra low voltage (SELV) standard. The power consumption cannot be less than the required value.
- Do not connect several devices to one power adapter as an adapter overload may cause over-heating and can be a fire hazard.
- When the product is installed on a wall or ceiling, the device should be firmly fixed.
- To reduce the risk of fire or electrical shock, do not expose the indoor used product to rain or moisture.
- This installation should be made by a qualified service person and should conform to all the local codes.
- Please install blackouts equipment into the power supply circuit for convenient supply interruption.
- If the product does not work properly, please contact your dealer or the nearest service center. Never attempt to disassemble the product yourself. (We shall not assume any responsibility for problems caused by unauthorized repair or maintenance.)
- Please do not look directly into the laser light within 6 meters because laser is hazardous to humans.

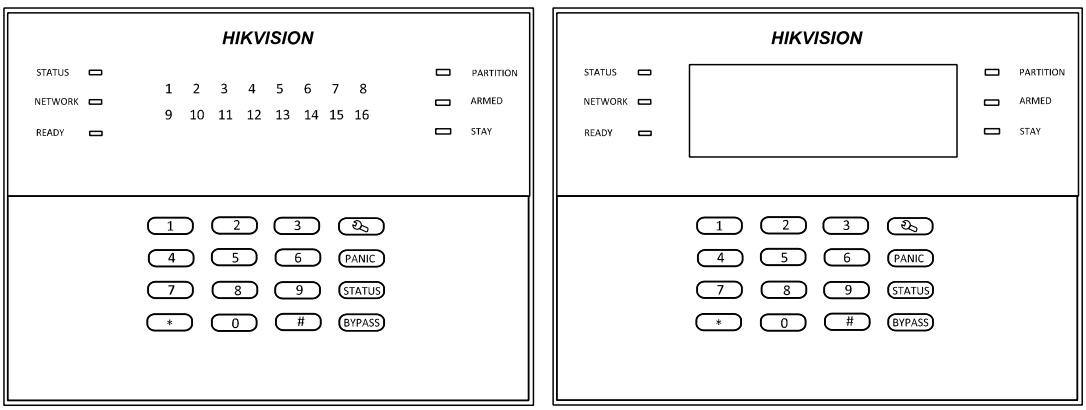
Cautions:

- Make sure the power supply voltage is correct before using the product.
- Do not drop the product or subject it to physical shock. Do not install the product on vibratory surface or places.
- Do not expose it to high electromagnetic radiating environment.
- Do not aim the lens at the strong light such as sun or incandescent lamp. The strong light can cause fatal damage to the product.
- The sensor may be burned out by a laser beam, so when any laser equipment is being used, make sure that the surface of the sensor not be exposed to the laser beam.
- For working temperature, please refer to the specification manual for details.
- To avoid heat accumulation, good ventilation is required for a proper operating environment.
- While shipping, the product should be packed in its original packing.
- Please use the provided glove when open up the product cover. Do not touch the product cover with fingers directly, because the acidic sweat of the fingers may erode the surface coating of the product cover.
- Please use a soft and dry cloth when clean inside and outside surfaces of the product cover. Do not use alkaline detergents.
- Improper use or replacement of the battery may result in hazard of explosion. Please use the manufactur*er recommended battery type.*

Content

Chapter 1 Introduction

1.1 Overview



The DS-19A08-F/Kx(G) is a commercial control panel with 8 partitions supported. The panel uses embedded microcontroller technology for zones monitoring and system status detection. The alarm or status reports can be transmitted to the central alarm monitoring station through programming. An integrated master keypad with the LED/LCD display is designed for implementing a readable programming progress. Multiple alarm types and report transmission methods (telephone network, the Ethernet network and the GPRS wireless network) are supported for the panel. A mobile client is attached for remote control such as pushing notifications of the alarm or status reports and remote arming/ disarming. The control panel is mainly deployed in the security system of shopping malls, stores, residences, apartments, communities and so on.

1.2 Feature

Hardwire Zones and Relay Outputs

8 hardwire zones;

Tamper supervision on the hardwire zones;

1 channel of relay output;

Up to 8 channel extension relay outputs;
Relay outputs can be triggered by alarm events or system events;

Partitioning
8 partitions, which can be controlled independently;
1 common partition (No.1 partition), that can be programmed to be linked with any other two partitions;

Event Log *
Provides a Contact ID report cache that can store up to 250 reports;
Up to 8000 alarm event logs, 2000 operation events logs and 1500 management event logs can be stored with time tag;
Support event logs tracing over the Ethernet System Communication;
GPRS communication and Short Message Service (SMS) (DS-19A08-F/KxG only);
ADEMCO Contact ID communication over the telephone network;
Encrypted NAL2300 communication over the Ethernet and the GPRS wireless network;
HIK-SDK communication over the Ethernet network;

Report Strategy
Support up to 2 independent central stations over the phone lines;
Support up to 2 independent central stations over the Ethernet network;
Support up to 2 independent central stations over the GPRS wireless network;
Support up to 6 independent report channel groups consisted of one main channel and 3 backup channels each, that can transmit reports in parallel;
Each report channel can be configured to transmit reports to the central alarm monitoring station over the telephone, Ethernet or GPRS wireless network;
Report can be pushed to a mobile phone with mobile client;
Report message can be transmitted to the mobile users with a bound phone number (SIM card);
Supports 6 communication channels over the Ethernet network base on the HIK-SDK protocol;

Remote Control
Up to 32 key fobs for radio transmitter operations;

Allows remote control operations with mobile client;
Message control operations, such as arming, disarming, and clearing the alarm, via short messages sent from the bound phone number;

Peripherals Devices
Provides a half-duplex RS-485 device bus, which can interface with keypads and relay modules;
Up to 8 addressable keypads;
1 external audio output for alarm warning devices, such as sirens, bells or horns with 12VDC power supply;

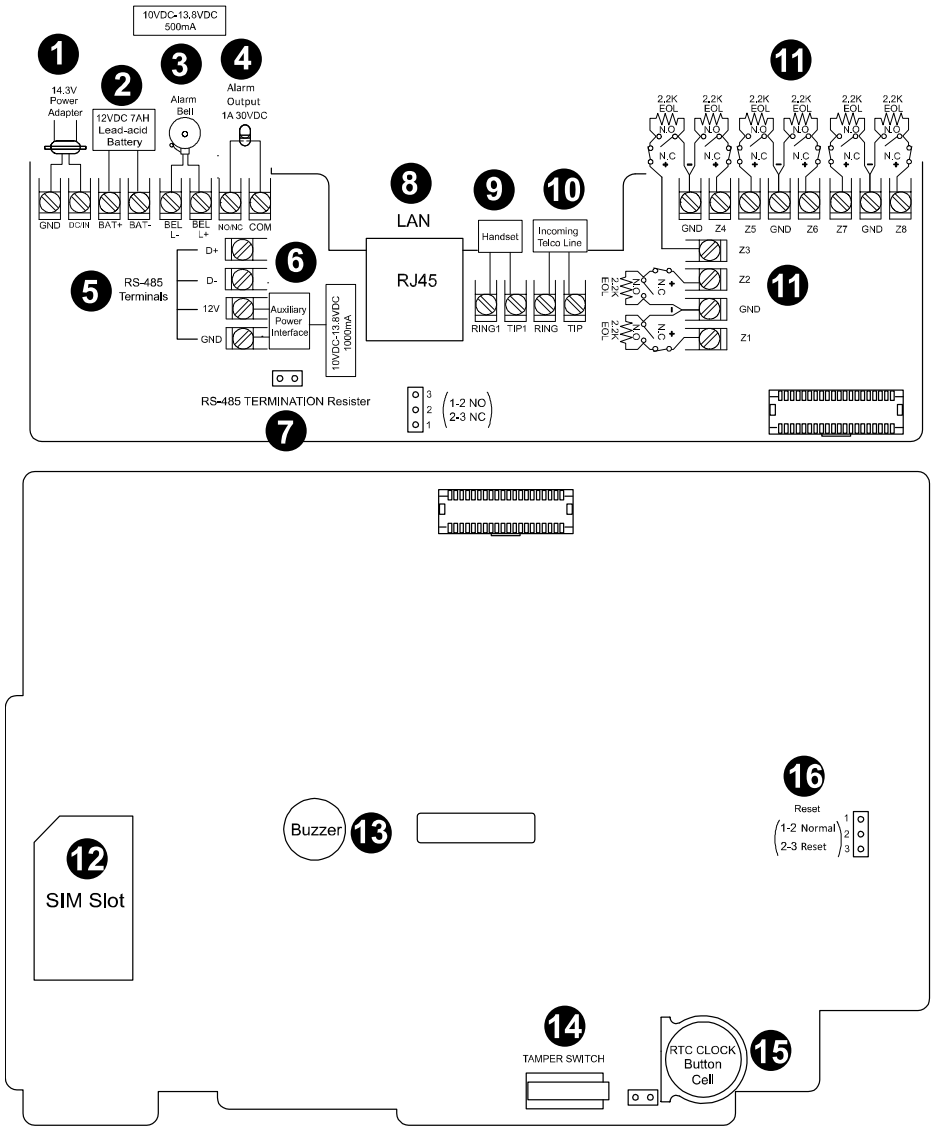
User Management
Users are consisted of an Installer, a Master User, 15 keypad operators and 16 network operators;
Authority level management of users assigned different security codes;

Power Supply Management
14VDC power adapter;
Provides a power supply interface with battery sensing hardware to prevent deep discharging an charge management circuit hardware for the external backup battery;
Automatically switch between A.C. power supply and backup battery power supply;
1 auxiliary power output rated max. 14VDC, 750mA;
Supports manually hardware reset to factory defaults;

Additional Features
Integrated master keypad with the LED/LCD display;
Tamper and movement protection function;
Support scheduling operations, such as arming, disarming, and output activating.

Chapter 2 Installation and Wiring

2.1 Main Board Overview

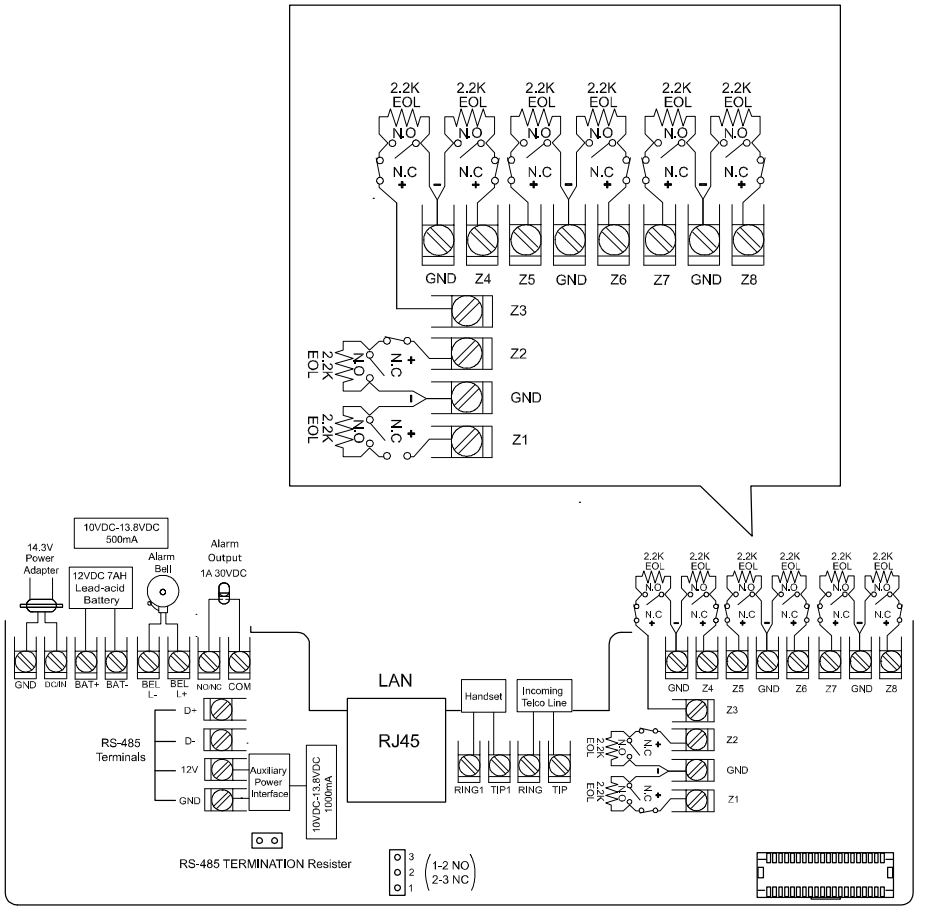


No.	Description	No.	Description
1	Power Adapter	9	Handset Interface
2	Lead-acid Battery	10	Incoming Telco Line Interface
3	Alarm Bell	11	Alarm Input Interface
4	Alarm Output (Alarm Lamp)	12	SIM Card/2G Card Slot
5	RS-485 Terminals	13	Buzzer
6	Auxiliary Power Interface (DC Output）	14	TAMPER Switch
7	RS-485 TERMINATION Resister	15	RTC CLOCK Button Cell
8	LAN Interface	16	Reset Button

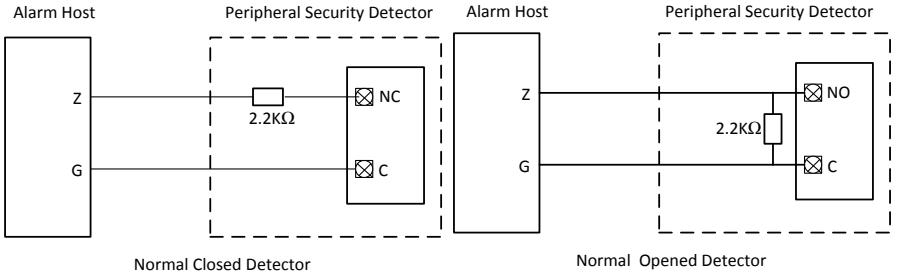
2.2 Device Wiring

2.2.1 Detector Wiring

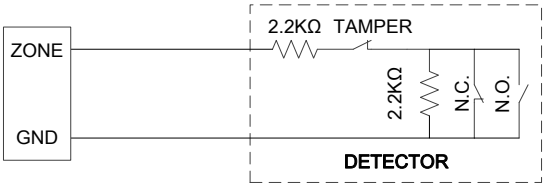
The alarm input interfaces of the control panel are show as follows.



The wiring of sensor is shown as follows.

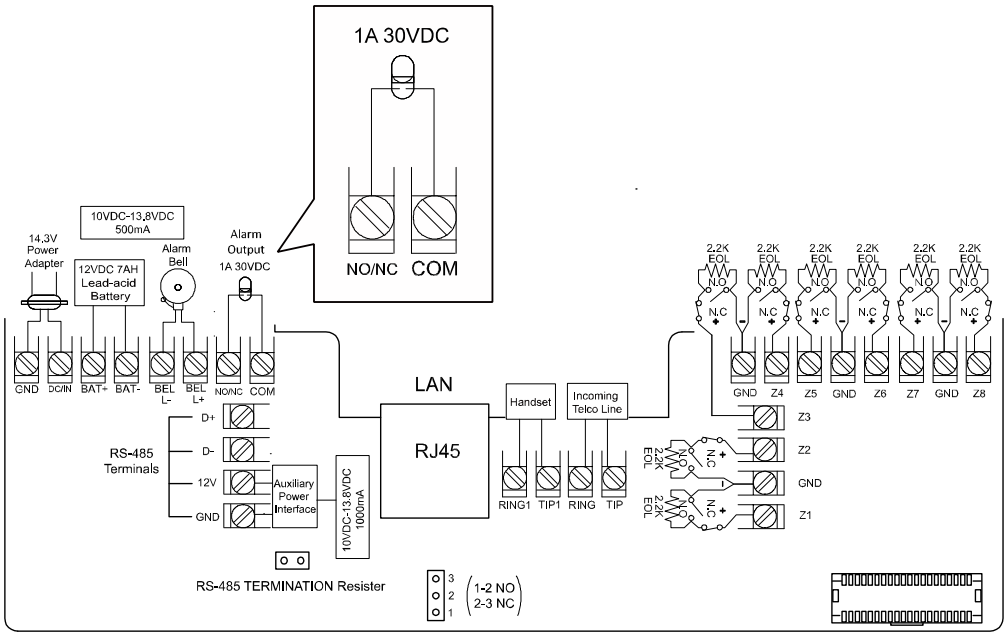


The Tamper-proof wiring is shown below.

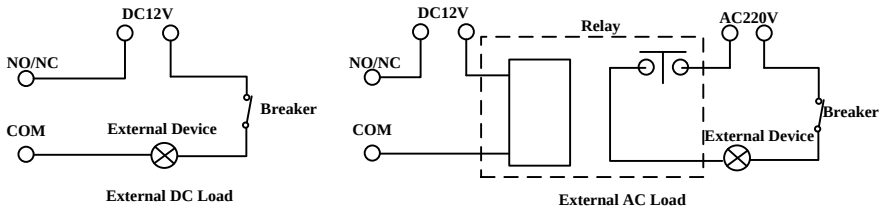


2.2.2 Alarm Output Wiring

The alarm output interfaces of the control panel are show as follows.



The wiring of alarm output is shown as follows:

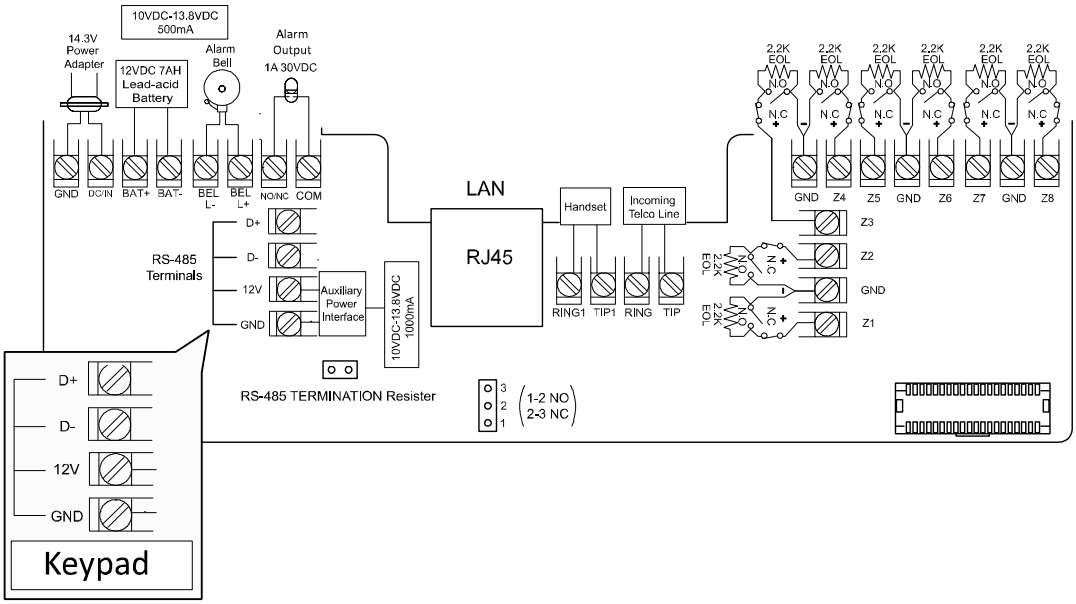


NOTE

The DC current supplied by the control panel is used for external devices. The load current cannot be over 1A.

2.2.3 Keypad Wiring

The keypad wiring is shown as follows.



2.3 System Start-up

For configuring the security control panel, you should restore the system of the control panel after start-up.

2.3.1 Control Panel Start-up

The keypad registration will be completed in 10 seconds after the control panel being power on. The system then will complete the start-up and enter the properly status of working.

2.3.2 Alarm Keypad Start-up

The LED keypad will make continuously prompt tones if the keypad does not receive the registration respond from the control panel in 20 seconds after it being power on. While the registration is succeeded, the working status indicator will turn green.

LED Alarm Keypad **Network** Indicator

Working Status	Indicator Status
Proper Network	Green (Flickering)
Network Exception	Off

LED Alarm Keypad **Status** Indicator

Working Status	Indicator Status
System Works Properly	Off
System Exception	Red (Continuously Light)

LED Alarm Keypad **Partition** Indicator

Working Status	Indicator Status
Single Partition	Off
Multi-partition	Green (Continuously Light)

LED Alarm Keypad **Stay** Indicator

Working Status	Indicator Status
Stay Arming Disabled	Off
Stay Arming Enabled	Orange (Continuously Light)

LED Alarm Keypad **Armed** Indicator

Working Status	Indicator Status
Partition Arming	Red (Continuously Light)
Partition Disarming	Green (Continuously Light)
In Programming	Green (Flickering)
Main Operator Password Editing	Green (Flickering)

Working Status	Indicator Status
Remote Control Connecting	Green (Flickering)
Pacing Mode	Red (Continuously Light)

LED Alarm Keypad **Ready** Indicator

Working Status	Indicator Status
Normal	Green (Continuously Light)
In Project	Red (Flickering)
Main Operator Password Editing	Green (Flickering)
Remote Control Connecting	Red (Flickering)
In Programming	Green (Flickering)

LED Alarm Keypad **Channel** Indicator

Working Status	Indicator Status
Normal	Off
Alarm	Red (Flickering)
Exception	Red (Continuously Light)
Bypass	Green (Continuously Light)

LED Alarm Keypad **Channel** Indicator Status in Project Mode

No.	Description	No.	Description
1	Off-hook	**5**	Send CID Report
2	Dialing	**6**	Receive Confirmation Sound
3	Alarm Connecter	**7**	Control Panel On-hook

No.	Description	No.	Description
	Disconnection		
4	Receive Hands-shake Sound	8	Alarm Connecter On-hook

LED Alarm Keypad **Channel** Indicator Status in Status Mode

No.	Description	No.	Description
1	AC Power Outages	5	Keypad Disconnection
2	Low Battery for Accumulator	6	Network Disconnection
3	Control Panel Tampering Alarm Enabled	7	No SIM Card
4	Telephone Line Disconnection	8	Reserved

2.3.3 Keypad Address

An address is required for each alarm keypad in the system. These addresses cannot be repeated. Once exchanging the alarm keypad, the address of the new keypad must be the same as the replaced one. You should configure the address via DIP switch of the keypad before powering on the system. The address should be in the range of 1~31.

2.3.4 Factory Settings

If powering on the system before zone connection, a 2.2k Ohm resistance is required for bridge connection between each zone.

Password and Report

Installer Password: 012345

Main User Password: 1234
Power Recovery Default Installer Password: No
Arming/Disarming Report: Yes
Control Panel Hijack Report: N/A

CID Report：

Account#1#2: No
Dialing Type: DTMF
Remote control Programming: No

For Detailed CID code, Please refer to CID Report.

Zone:

Zone 1 to 8: Real-time zone
Urgent Soft Zone: Buzzing prompt sound

Test:

Testing Report Interval： N/A

Timing:

Entering Duration: 10 sec
Exiting Duration: 30 sec
Belling Duration: 5 min

Network Parameters:

IP Address: 192.0.0.64
Port No.: 8000

2.3.5 Activating the Control Panel

Purpose:

You are required to activate the control panel first before you can use the control panel.

Activation via SADP, and Activation via client software are supported.

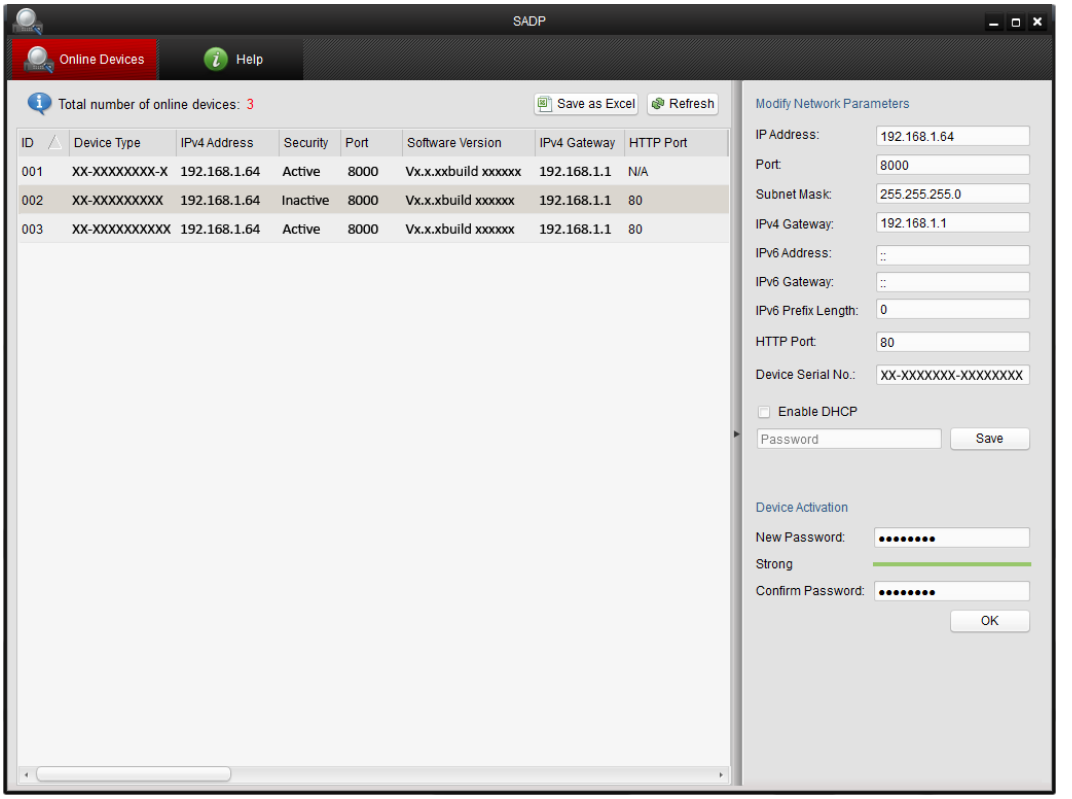
◆ Activation via SADP Software

SADP software is used for detecting the online device, activating the device, and resetting the password.

Get the SADP software from the supplied disk or the official website, and install the SADP according to the prompts. Follow the steps to activate the control panel.

Steps:

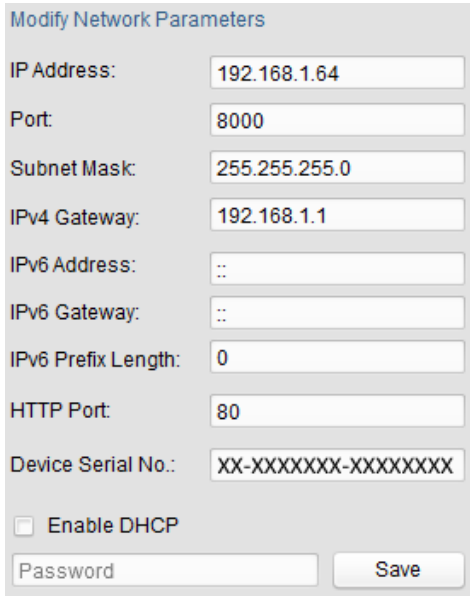
1. Run the SADP software to search the online devices.
2. Check the device status from the device list, and select an inactive device.



3. Create a password and input the password in the password field, and confirm the password.

STRONG PASSWORD RECOMMENDED– *We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.*

4. Click **OK** to save the password.
   You can check whether the activation is completed on the popup window. If activation failed, please make sure that the password meets the requirement and then try again.
5. Change the device IP address to the same subnet with your computer by either modifying the IP address manually or checking the checkbox of Enable DHCP.



6. Input the password and click the **Save** button to activate your IP address modification.

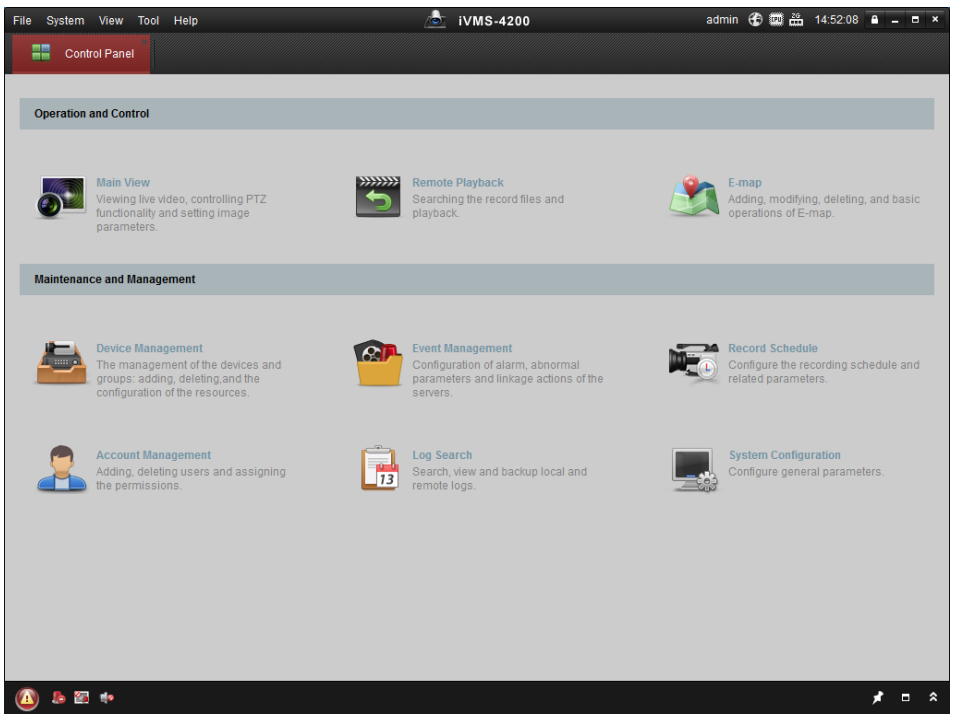
◆ Activation via Client Software

The client software is versatile video management software for multiple kinds of devices.

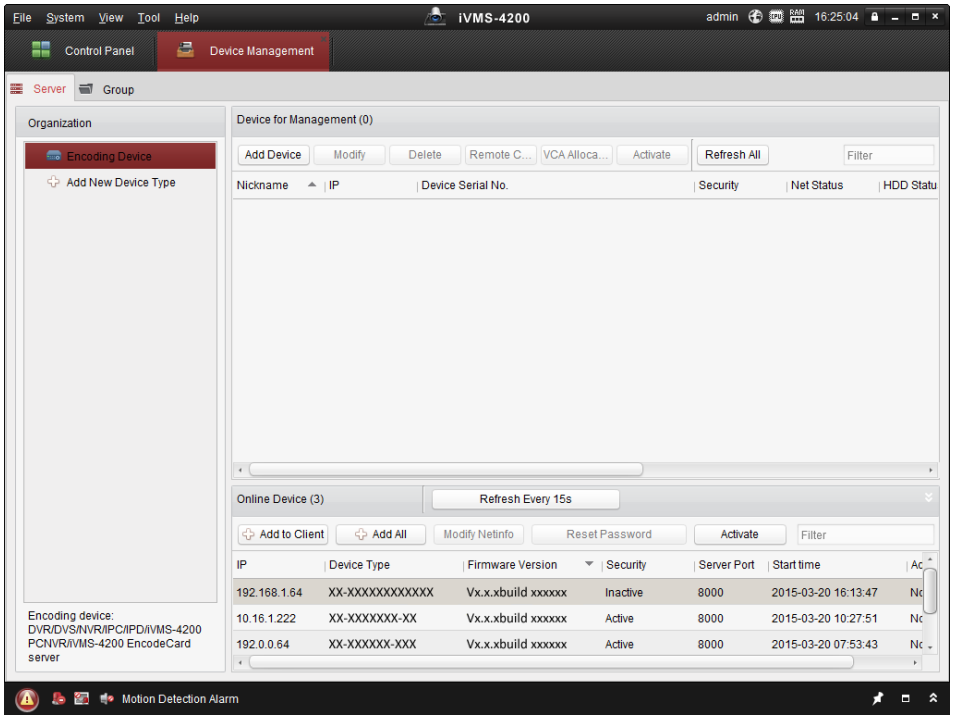
Get the client software from the supplied disk or the official website, and install the software according to the prompts. Follow the steps to activate the control panel.

Steps:

1. Run the client software and the control panel of the software pops up, as shown in the figure below.

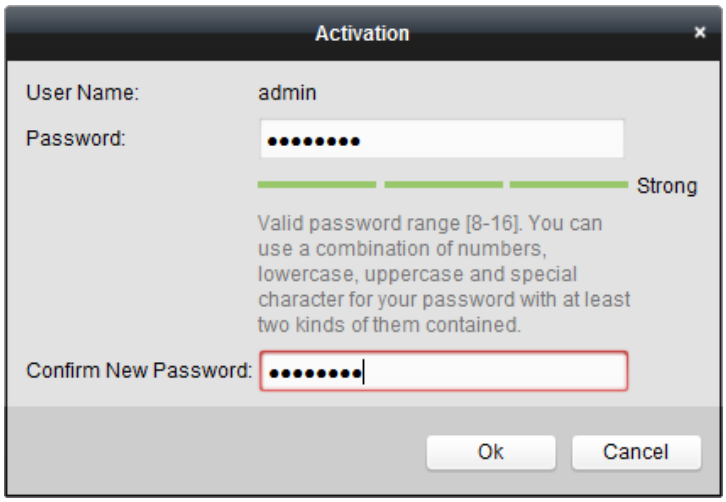


2. Click the **Device Management** icon to enter the Device Management interface, as shown in the figure below.

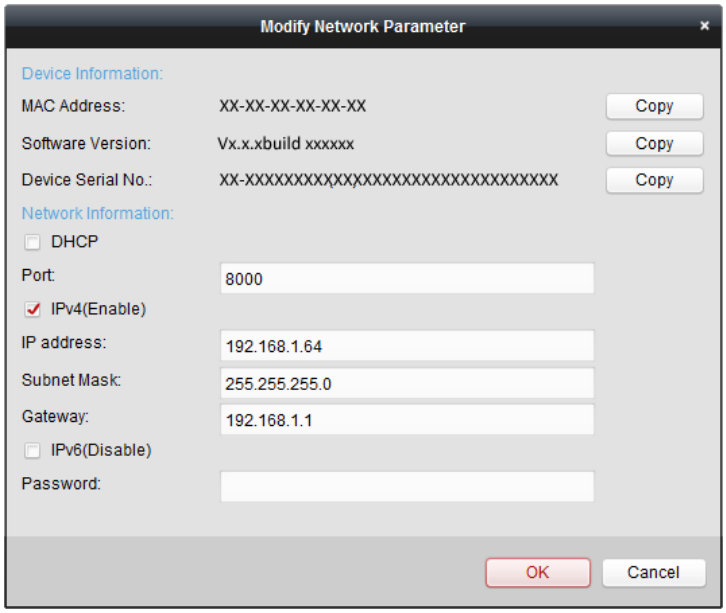


3. Check the device status from the device list, and select an inactive device.
4. Click the **Activate** button to pop up the Activation interface.
5. Create a password and input the password in the password field, and confirm the password.

STRONG PASSWORD RECOMMENDED– *We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.*



6. Click **OK** button to start activation.
7. Click the **Modify Netinfo** button to pop up the Network Parameter Modification interface, as shown in the figure below.



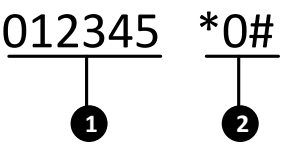
8. Change the device IP address to the same subnet with your computer by either modifying the IP address manually or checking the checkbox of Enable DHCP.

Input the password to activate your IP address modification.

Chapter 3 Keypad Operation (Local Operation）

3.1 Alarm Keypad Configuration

You should access the programming mode (only installer can access the programming mode) before keypad configuration. The command is shown below:



{1} Installer password: 012345

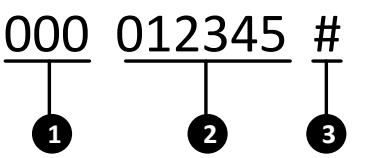
{2} Command Key: *0 #

NOTE

The command for exiting programming mode is *#.

3.1.1 Installer Password Settings

The password of installer is used for accessing programming and initializing mode. The command is shown below.



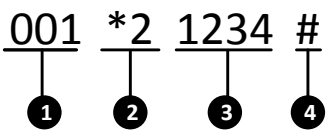
{1} Installer Password Programming Address: 000.

{2} Installer Password: The default password is 012345. The length of the configured password should be 1~ 6 characte.

{3} End the command.

3.1.2 Operator Configuration

The programming command of operator configuration is shown below.



{1} Operator Programming Address: 001～016.

{2} User Permission: 12 permissions. For details, please refer to the following table.

No.	Permission	No.	Permission
1	Arming No Arming Report Unavailable Bypass	**2**	Arming/Disarming No Disarming Report Unavailable Bypass
3	Arming/Disarming No Arming/Disarming Report, Unavailable Bypass	**4**	Arming Arming Report Unavailable Bypass
5	Disarming Disarming Report Unavailable Bypass	**6**	Arming/ Disarming Arming/Disarming Report Unavailable Bypass
7	Arming No Disarming Report	**8**	Disarming No Arming/Disarming Report
9	Arming/Disarming No Arming/Disarming Report Bypass	***0**	Arming Arming Report Bypass
***1**	Disarming	***2**	Arming/Disarming

	Disarming Report Bypass		Arming/Disarming Report Bypass

{3} Specified the username and password, the length of user name should be in the range of 2 to 5 characters.

{4} End the command.

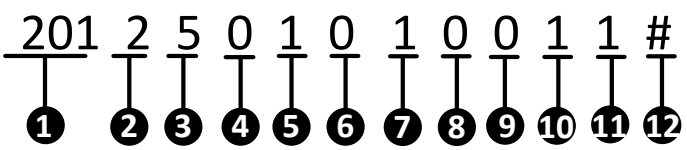
NOTE

The username and password cannot be empty. If the password is configured as 0, the user will be deleted. The password of 00, 000, 0000, or 00000 all signify of deleting the user.

The default password of the main operator is 1234 with the permission of 2. The default permission of other operators is 6.

3.1.3 Zone Parameters Configuration

The parameters of zone include zone response time, zone arming type, linked local alarm output, linked siren output. The detailed command is shown below.



{1} Zone Parameters Programming Address: 201～208/216

NOTE

For 8-zone network security control panel , the zone parameters programming address is 201~208.

For 16-zone network security control panel, the zone parameters programming address is 201~216.

{2} Zone Response Time. The 4 kinds of zone response time is shown as follows.

Command	Command Description	Command	Command Description
0	10 ms	**1**	250 ms
2	500 ms	**3**	750 ms

{3} Zone Arming Type

Command	Command Description	Command	Command Description
0	None	**1**	24-hour voiced zone
2	Delay Zone	**3**	Internal Delay Zone
4	Key Arming/Disarming Zone	**5**	Real-time Zone
6	Fire Zone	**7**	24-hour non-voiced Zone
8	Stay Arming		

{4} Linked Trigger

Command	Command Description	Command	Command Description
0	Non-linked Local Alarm Output	**1**	Linking Local 1 Alarm Output
2	Linking Local 2 Alarm Output	**3**	Linking Local 1/2Alarm Output
4	Linking Local 3 Alarm Output	**5**	Linking Local 1/3 Alarm Output
6	Linking Local 2/3 Alarm Output	**7**	Linking Local 1/2/3 Alarm Output
8	Linking Local 4 Alarm Output	**9**	Linking Local 1/4 Alarm Output
***0**	Linking Local 2/4	***1**	Linking Local

Command	Command Description	Command	Command Description
	Alarm Output		1/2/4Alarm Output
*2	Linking Local 3/4 Alarm Output	*3	Linking Local 1/3/4 Alarm Output
*4	Linking Local 2/3/4 Alarm Output	*5	Linking Local 1/2/3/4 Alarm Output

{5} Liked Alarm Output.

Command	Command Description	Command	Command Description
0	Non-linked Alarm Output	1	Linked Alarm Output

{6} Bypass Group

Command	Command Description	Command	Command Description
0	Unsuport	1	Support

{7} Alarm Recovery Report.

Command	Command Description	Command	Command Description
0	No Alarm Recovery Report	1	Alarm Recovery Report

{8} Zone Loop Type

Command	Command Description
0	Zone Loop without Tampering Prevention Switch
1	NC Type of Loop with Tampering Prevention Zone Loop
2	NO Type of Loop with Tampering Prevention Zone Loop

The fire alarm zone do not support the configuration of zone loop type, and can only be set as 0,or an error value will be returned.

{9} Tampering Prevention Linked Trigger

Command	Command Description	Command	Command Description
0	Non-linked Local Alarm Output	**1**	Linking Local 1 Alarm Output
2	Linking Local 2 Alarm Output	**3**	Linking Local 1/2Alarm Output
4	Linking Local 3 Alarm Output	**5**	Linking Local 1/3 Alarm Output
6	Linking Local 2/3 Alarm Output	**7**	Linking Local 1/2/3 Alarm Output
8	Linking Local 4 Alarm Output	**9**	Linking Local 1/4 Alarm Output
***0**	Linking Local 2/4 Alarm Output	***1**	Linking Local 1/2/4Alarm Output
***2**	Linking Local 3/4 Alarm Output	***3**	Linking Local 1/3/4 Alarm Output
***4**	Linking Local 2/3/4 Alarm Output	***5**	Linking Local 1/2/3/4 Alarm Output

{10} Tampering Prevention Linked Siren Output

Command	Command Description	Command	Command Description
0	No Linked Siren Output	**1**	With Linked Siren Output

{11} No Tampering Prevention Recovery Report

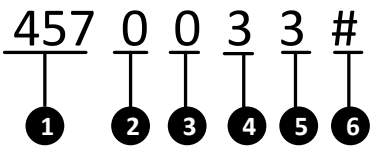
Command	Command	Command	Command

	Description		Description
0	No Tampering Prevention Recovery Report	**1**	With Tampering Prevention Recovery Report

{12} End the command.

3.1.4 Telco Line Communication Control

The communication control command is used for setting the phone connection mode of alarm center 1 and 2. The detailed command is shown below.



{1} The Telco line communication control programming address: 457
{2} Dialing Mode of Telephone Center1
{3} Dialing Mode of Telephone Center2

Command	Command Description	Command	Command Description
0	DTMF- double tone& multi-frequency (5/sec)	**1**	DTMF- double tone& multi-frequency (10/sec)

{4} Dialing Times of Telephone Center1
{5} Dialing Times of Telephone Center2

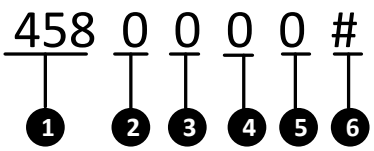
Command	Command Description	Command	Command Description
1	1	**9**	9 Times
2	2 Times	***0**	10 Times
3	3 Times	***1**	11 Times

Command	Command Description	Command	Command Description
4	4 Times	***2**	12 Times
5	5 Times	***3**	13 Times
6	6 Times	***4**	14 Times
7	7 Times	***5**	15 Times
9	8 Times		

{6} End the command.

3.1.5 Dialing Account Configuration

The control panel supports phone dialing to upload alarm information. The dialing account command is shown below.



{1} Dialing Account Programming Address: 458~459

Command	Command Description	Command	Command Description
458	Corresponding Alarm Center 1 Dialing Account	**459**	Corresponding Alarm Center 2 Dialing Account

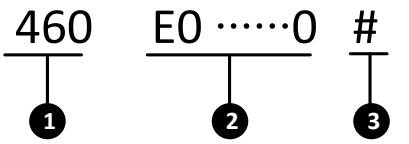
{2}~{5} Account No.. The value range of the account No. is 0~F.

It is recommended that the dilaing account should be the same as the allocated account of the alarm connecter.

{6} End the command.

3.1.6 Alarm Receiver Phone Number Settings

The control panel supports two dialing accounts. The maximum length of dialing number of each account is 31 digits. The command is shown as follows.



{1} Programming Address of Phone Number of Alarm Connecter: 460~463

Address	Command Description	Address	Command Description
460	Alarm Center1 Phone Number Programming Address	**462**	Alarm Center2 Phone Number Programming Address
461		**463**	

A telephone number is separated into two segments. The 460 and 461 group represents the dialing number which is connected with alarm center1. The 462 and 463 group represents the dialing number which is connected with alarm center2.

{2} The dialing number is 16 digits.

- All the telephone number should be end with *4.
- The length of the each center number is 31 digits, and the entering format should be {No.} + {Dwell Time} + {ext.No.}
- The default center number is E0000000000000000000000000000000.

{3} End the command.

Example 1:

If the tele-phone number is 0571-88075998, you can enter 460057188075998*4# with the keypad for completing the configuration.

Example 2：

If the telephone number is 17951-88075998, there are two steps to set the

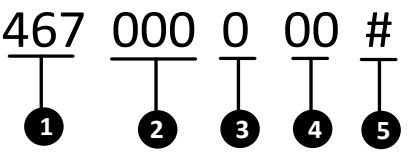
phone number via the keypad.

Steps:

1. Enter 46017951FFF88075998# with the keypad.
2. Enter 461*4# to complete the settings.

3.1.7 Zone Associated Trigger Configuration

The detailed programming command is shown below.



{1} Trigger Configuration Programming Address: 467

{2} Zone No.

{3} Add/Delete Trigger

Command	Command Description	Command	Command Description
0	Delete	**1**	Add

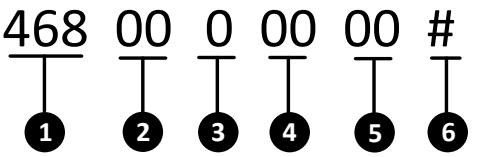
{4} Trigger No.

{5} End the command.

- After successfully operating once, you can continuously do configuration with the command of **{**Project**}** + **{**Trigger No.**}** + **{#}**.
- No more than 9 triggers can be linked.

3.1.8 Trigger Event Linkage Configuration

For trigger event linkage configuration, please refer to the command below.



{1} The programming address of enabling trigger event linkage is 468～469.

Command	Function Description	Command	Function Description
468	Enable Trigger Event Linkage	**469**	Disable Trigger Event Linkage

{2} Trigger No.

{3} Add/ Delete Trigger

Command	Function Description	Command	Function Description
0	Delete Trigger	**1**	Add Trigger

{4} Selecting Device/ System

Command	Function Description	Command	Function Description
00	Device	**01**	System

{5} Event No.

The device event command is shown below.

Command	Command Description	Command	Command Description	Command	Command Description
00	None	**01**	AC Power Down	**02**	Low Battery
03	Telephone Line Disconnection	**04**	Wired Network Exception	**05**	No Network Exception

The system event command is shown below.

Command	Command Description	Command	Command Description	Command	Command Description
01	Entering Delay	**02**	Exiting Delay	**03**	Arming
04	Disarming	**05**	Alarm	**06**	Alarm Clearing
07	Alarm Recovery				

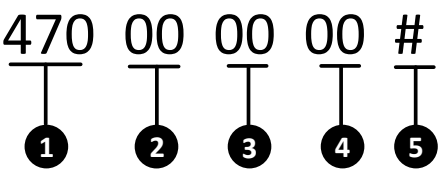
{6} End the command.

NOTE

After successfully operating once, you can continuously do configuration with the command of **{**Project**}** + **{** Trigger No.**}** + **{**System Command.**}** + **{**Event Command**}** + **{#}**.

3.1.9 Trigger Time Settings

For Trigger output time settings, please refer to the command below.



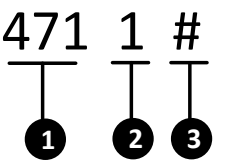
{1} Trigger Time Programming Address: 470
{2} Trigger No.
{3} Duration: In minute
{4} Duration: In second
{5} End the command.

NOTE

The maximum duration of triggering is 99 minutes and 59 seconds. The default duration is 30 seconds.
After operating once, you can continuously configure with the command of {Project} + {Trigger No.} + {Duration} + {#}

3.1.10 Siren Configuration

For siren configuration, please refer to the command below.



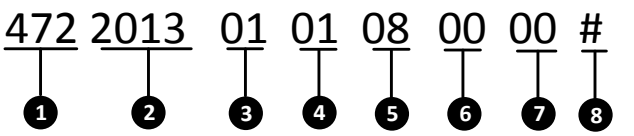
{1} Siren Configuration Programming Address: 471
{2} Enable/Disable Siren Command

Command	Command Description	Command	Command Description
0	Disable	**1**	**Enable**

{3} End the Command.

3.1.11 Control Panel Time Settings

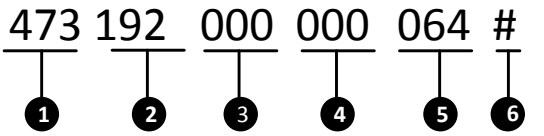
For control panel time settings, please refer to the command below.



{1} Control Panel Time Settings Programming Address: 472
{2} Year
{3} Month
{4} Day
{5} Hour
{6} Minute
{7} Second
{8} End the Command.

3.1.12 Control Panel IP Configuration

For control panel IP configuration, please refer to the command below.



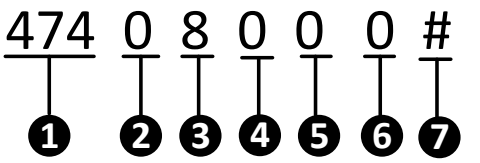
{1} Control Panel IP Configuration Programming Address: 473.
{2} Unit 1
{3} Unit 2
{4} Unit 3
{5} Unit 4.
{6} End the command.

NOTE

The IP address programming includes 12 digits. The 1 to 12 place indicates the IP address of the control panel. Each unit of the IP address includes 3 digits. You should enter 0 if the entered address is less than 3 digits for each unit for complement. For example, you should enter 192 002 028 066 for validating the IP address of 192.2.28.66.

Local Port Number Configuration

The programming command of local port number setting is shown below:



{1} The programming command address of local port number setting is: 474;
{2} Port: Ten Thousands' Digit
{3} Port: Thousands' Digit
{4} Port: Hundreds' Digit
{5} Port: Tens' Digit
{6} Port: Units' Digit

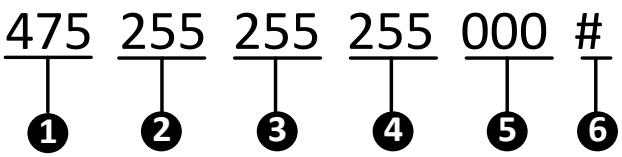
{7} End the command.

NOTE

Corresponding port number must be 5 digits. When the place is not sufficient, fill it up with 0.
For example: When the port number is 6000, the programming command is: 474 06000#.

3.1.13 Subnet Mask Configuration

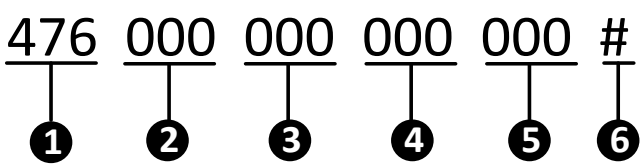
The programming command of control panel subnet mask setting is shown below:



{1} The programming command address of control panel subnet mask setting is: 475;
{2} The First Unit;
{3} The Second Unit;
{4} The Third Unit;
{5} The Fourth Unit;
{6} End the command.

3.1.14 Gateway Configuration

The programming command of gateway settings is shown below:

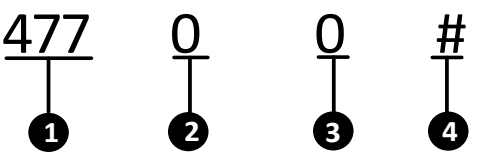


{1} The programming command address of control panel gateway setting is: 476;
{2} The First Unit;

{3} The Second Unit;
{4} The Third Unit;
{5} The Fourth Unit;
{6} End the command.

3.1.15 GPRS Configuration

The programming command of GPRS settings is shown below:



{1} The programming command address of GPRS setting are: 477
{2} Name of APN;

Command	Description	Command	Description
1	CMNET	**2**	UNINET

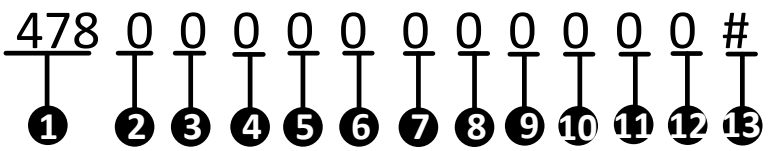
{3} Time of detecting link;

Command	Time	Command	Time
0	10s	**8**	170s
1	30s	**9**	190s
2	50s	***0**	210s
3	70s	***1**	230s
4	90s	***2**	250s
5	110s	***3**	270s
6	130s	***4**	290s
7	150s	***5**	300s

{4} End the command.

3.1.16 SIM Card No. Configuration

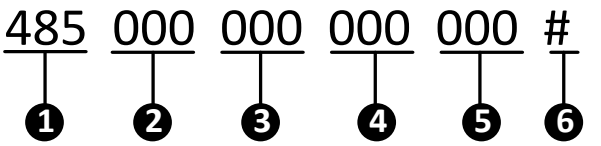
The programming command of SIM Card No. settings is shown below:



{1} The programming command address of SIM card No. settings is 478.
{2}~{12} SIM card No.
{13} End the command.

3.1.17 Uploading Center IP Configuration

The programming command of uploading center IP setting is shown below:



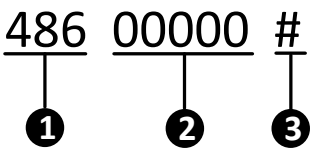
{1} The programming command address of uploading center IP setting are: 485,488,491,494;

Command	Description	Command	Description
485	Programming Address of Network Center 1 IP Settings	**488**	Programming Address of Network Center 2 IP Settings
491	Programming Address of GPRS Center 1 IP Settings	**494**	Programming Address of GPRS Center 2 IP Settings

{2} The First unit;
{3} The Second unit;
{4} The Third unit;
{5} The Fourth unit;
{6} End the command.

3.1.18 Uploading Center Port Configuration

The programming command of uploading center port setting is shown below:



{1} The programming command addresses of uploading center port setting are: 486, 489, 492, 495;

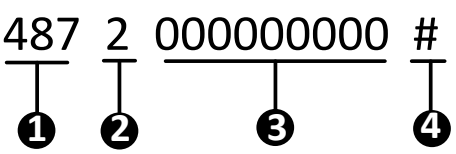
Command	Description	Command	Description
486	Programming Address of Network Center 1 Port Settings	**489**	Programming Address of Network Center 2 Port Settings
492	Programming Address of WIFI Center 1 Port Settings	**495**	Programming Address of WIFI Center 2 Port Settings

{2} Port number;

{3} End the command.

3.1.19 Center Protocol and Account Configuration

The programming command of center protocol and account setting is shown below:



{1} The programming command addresses of center protocol and account settings are: 487, 490, 493, 496;

Command	Description	Command	Description

487	Network Center 1 Protocol and Programming Address of Account Settings	**490**	Network Center 2 Protocol and Programming Address of Account Settings
493	GPRS Center 1 Protocol and Programming Address of Account Settings	**496**	GPRS Center 2 Protocol and Programming Address of Account Settings

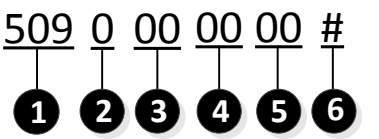
{2} Protocol Type:

Command	Description
1	HIK

{3} Account;

{4} End the command.

3.1.20 Siren Linked Event Configuration



{1} The programming command address of siren linked event configuration is 509(default: null)

{2} Add/Delete Event Configuration

Command	Description	Command	Description
0	Delete Event	**1**	Add Event

{3} Event Type

Command	Description	Command	Description
00	Global Event	**01**	Partition Event

{4} Detailed Event Type

The global event types are shown below.

Command	Description	Command	Description	Command	Description
00	Null	**01**	Control Panel Tampering Alarm	**02**	Global Keypad Emergency Alarm
03	Ac Disconnected	**04**	Low Battery Voltage	**05**	Telco Line Disconnected
06	Wired Network Exception	**07**	Wireless Network Exception	**08**	Keypad /485 Device Disconnected

The partition event types are shown below.

Command	Description	Command	Description
00	Null	**01**	Emergency Alarm
02	Arming	**03**	Disarming

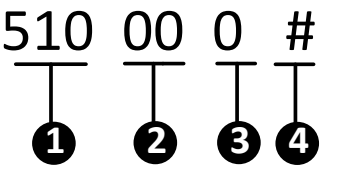
{5} Partition No. (It is not necessary to enter the partition No. when configuring global event)

Command	Description	Command	Description	Command	Description
00	Global Partition	**01**	No.1 Partition	**02**	No.2 Partition
03	No.3 Partition	**04**	No.4 Partition	**05**	No.5 Partition
06	No.6 Partition	**07**	No.7 Partition	**08**	No.8 Partition

{6} End the command.

3.1.21 Emergency Alarm Linkage Configuration

The programming command of emergency alarm linkage settings is shown below:



{1} The programming command address of emergency alarm linkage setting is: 510;

{2} Partition Number, 00 indicate the global keypad, 01~08 indicate partitions No.1~No.8;

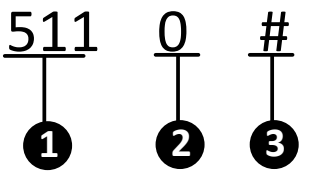
{3} Whether to link the siren or not;

Command	Description	Command	Description
0	Not link the Siren	**1**	Link the Siren

{4} End the command.

3.1.22 Control Panel Tampering Alarm Configuration

The programming command of control panel tampering alarm settings is shown below:



{1} The programming command address of control panel tampering alarm is: 511;

{2} whether to link the siren or not;

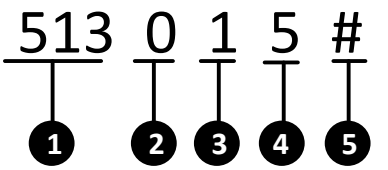
Command	Description	Command	Description
0	Not link the Siren	**1**	Link the Siren

{3} End the command.

3.1.23 Testing Report Configuration

The testing report is used to validate the communication of control panel and

alarm center. The detailed operation is show as follows.



{1} The testing report programming address is 513.

{2} Enable/Disable the Testing Report

Command	Command Description	Command	Command Description
0	Disable	**1**	**Enable**

{3} Timer of the Testing Report.

Command	Command Description	Command	Command Description
0	1/4H	**4**	3H
1	1/2H	**5**	4H
2	1H	**6**	6H
3	2H	**7**	8H
Command	**Command Description**	**Command**	**Command Description**
8	10H	***2**	18H
9	12H	***3**	20H
***0**	14H	***4**	22H
***1**	16H	***5**	24H

{4} Testing Report Sending Interval

Command	Command Description	Command	Command Description	Command	Command Description
1	1H	**4**	12H	**7**	3D
2	2H	**5**	24H	**8**	5D

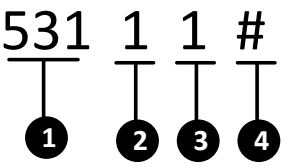
3	4H	**6**	2D	**9**	7D

{5} End the command.

3.1.24 Partition Configuration

Partition Start-up Configuration

The programming command of the partition start-up configuration is shown below.



{1} The programming of partition start-up configuration is: 531～538.

{2} The configuration item of 1 indicates the start-up configuration of the partition.

{3} Enable/Disable the Partition.

Command	Command Description	Command	Command Description
0	Disable	**1**	Enable

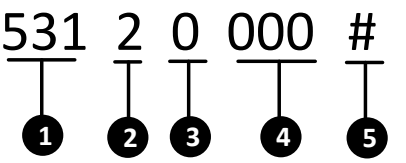
{4} End the command.

NOTE

Only the No.1 partition is enabled as the default settings.

Partition Keypad User Configuration

The programming command of keypad user configuration of the partition is shown as follows.



{1} The programming command address of keypad user configuration is 531～538.

{2} The configuration item of 2 indicates the keypad user configuration.

{3} Add/Delete the user.

Command	Command Description	Command	Command Description
0	Delete	**1**	Add

{4} The user No.

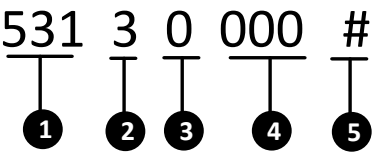
{5} End the command

NOTE

- **Added Separately**: for instance, to add an user with the No. of 160 to the No.8 partition, the command should be 538 2 1 160 #
- **Added/Deleted Continually**: only continuous adding or deleting operation is supported. After adding/deleting a user separately, enter the command [Project]+[User No.]+[#] to continually add/delete users. For instance, to add users with the No. of 2,3,and 5, the command should be 538 2 1 002 # Project # 003 # Project # 005 #.
- **Added/Delete in Batch**: the formate is 531 2 x xxx xxx #.
- **Added with user No. interval**: for instance, to add users with the No. between 100~149 to the No.3 partition, the command should be 533.2.1.100.149 #.

Partition Zone Configuration

The programming command of zone configuration of the partition is shown below.



{1} The programming command addressof zone configuration is 531～538.

{2} The configuration item of 3 indicates zone configuration of the partition.

{3} Add/Delete Zone.

Command	Command Description	Command	Command Description
0	Delete	**1**	Add

{4} Zone No.

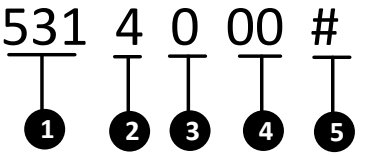
{5} End the command.

NOTE

There are three mode to add/delete zone for the partition, adding/deleting separately, Adding/ Deleting continually and adding/deleting in Batch, for details, refer to the ***Partition Keypad User Configuration.***

Partition Keypad Configuration

The programming command of keypad configuration of the partition is shown as follows.



{1} The programming command address of zone configuration is 531～

538.

{2} The configuration item of 4 indicates keypad configuration.

Add/Delete Keypad**Command**	**Command Description**	**Command**	**Command Description**
0	Delete	**1**	Add

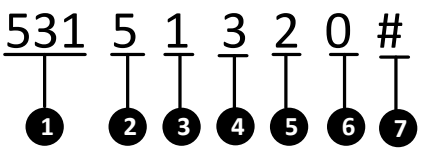
{3} Keypad No.

{4} End the command.

There are three mode to add/delete zone for the partition, adding/deleting separately, Adding/ Deleting continually and adding/deleting in Batch, for details, refer to the ***Partition Keypad User Configuration***.

Partition Time and Control Panel Hijack Report Configuration

To configure the system time and hijack report, please see the command below.



{1} System Time and Hijacking Report Programming Address: 531

{2} Classification Option of System Time and Hijacking Report: 5

{3} Entering Delay

Command	**Command Description**	**Command**	**Command Description**	**Command**	**Command Description**
1	**10sec**	**6**	60sec	***1**	110sec
2	20sec	**7**	70sec	***2**	120sec
3	30sec	**8**	80sec	***3**	130sec
4	40sec	**9**	90sec	***4**	140sec
5	50sec	***0**	100sec	***5**	150sec

{4} Exiting Delay

Command	Command Description	Command	Command Description	Command	Command Description
1	10sec	**6**	60sec	***1**	110sec
2	20sec	**7**	70sec	***2**	120sec
3	**30sec**	**8**	80sec	***3**	130sec
4	40sec	**9**	90sec	***4**	140sec
5	50sec	***0**	100sec	***5**	150sec

{5} Siren Working Duration

Command	Command Description	Command	Command Description	Command	Command Description
1	2min	**2**	**5min**	**3**	10min
4	15min	**5**	30min		

{6} Enable/Disable Control Panel Hijacking Report

Command	Command Description	Command	Command Description
0	**Disable**	**1**	Enable

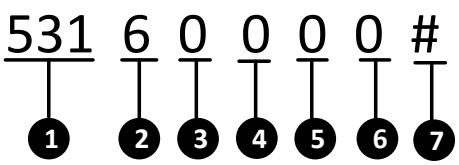
{7} End the command.

NOTE

The 24-hour non-voiced zone does not support linked siren output.

Partition Report and Arming Prompt Sound Configuration

To configure the system report and arming prompt sound, please see the command below.



{1} system report and arming prompt sound programming address: 531
{2} Classification Option of Report and Arming Prompt Sound: 6
{3} Arming/disarming Report Ending Prompt Sound
{4} Manual Testing Report Sending Prompt Sound.
{5} Prompting sound of arming succeeded.
{6} Prompting sound of disarming succeeded

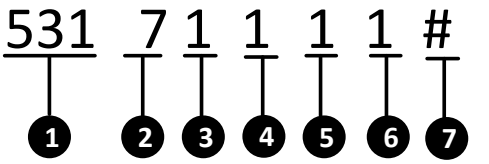
{3}～{6}

Command	Command Description	Command	Command Description
0	**Disable**	**1**	Enable

{7} End the command.

Partition Key User Permission Configuration

To configure the permission of key user, please see the command below.



{1} System key user permission programming address: 531.
{2} System key user classification option: 7
{3} Arming Permission
{4} Disarming Permission
{5} Arming Report Permission
{6} Disarming Report Permission

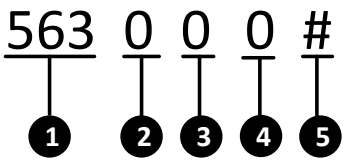
{3}～{6}

Command	Command Description	Command	Command Description
0	**Disable**	**1**	**Enable**

{7} End the command.

3.1.25 Public Partition Settings

The programming commands of public partition settings are as below:



{1} The public partition settings address is 563.
{2} Enable/Disable public partition.

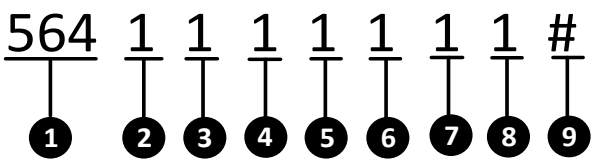
Command	Command Description	Command	Command Description
0	Disable	**1**	**Enable**

{3} Linked System No.1.
{4} Linked System No.2.
{5} End the command.

3.1.26 Fault Detection Configuration

Control Panel System Fault Detection Configuration

To configure control panel system fault detection, please see the command below.



{1} Control panel system fault detection address: 564.
{2} Ac Power Down
{3} Low Battery
{4} Control Panel Tampering Alarm
{5} Phone Line Disconnection
{6} Main keypad Disconnection

{7} Neywork Exception
{8} Wireless Network Exception

Command	Command Description	Command	Command Description
0	Disable	**1**	**Enable**

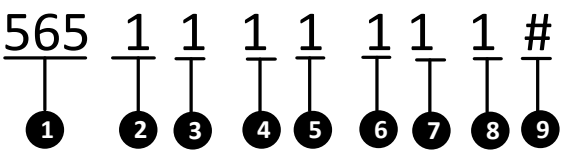
{9} End the command.

NOTE

If the fault detection is disabled, the control panel will not detect or report this sort of fault.

Keypad Fault Display Configuration

To configure the system fault display, please refer to the command below.



{1} Keypad fault display configuration programming address: 565
{2} Ac Power Down
{3} Low Battery
{4} Control Panel Tampering Alarm
{5} Phone Line Disconnection
{6} Main keypad Disconnection
{7} Neywork Exception
{8} GPRS Exception

Command	Command Description	Command	Command Description
0	Disable	**1**	**Enable**

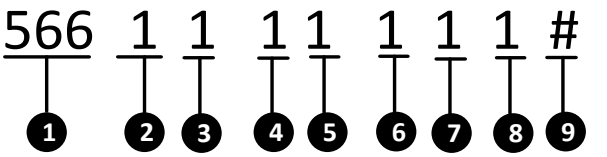
{9} End the command.

NOTE

After successfully operating once, you can continuously do configuration with the command of {Project} + {Partition No.} + {Configuration} + {#}.

Keypad Fault Prompt Sound Configuration

To configure the keypad fault prompt sound, please see the command below.



{1} Keypad fault prompt sound configuration programming address: 566.
{2} Ac Power Down
{3} Low Battery
{4} Control Panel Tampering Alarm
{5} Phone Line Disconnection
{6} Main keypad Disconnection
{7} Network Exception
{8} GPRS Exception

Command	Command Description	Command	Command Description
0	Disable	**1**	**Enable**

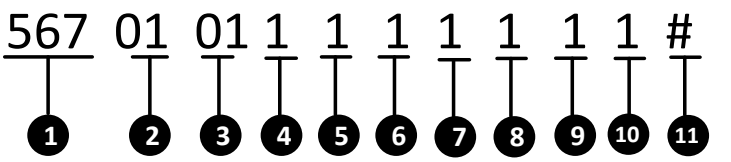
{9} End the command.

NOTE

After successfully operating once, you can continuously do configuration with the command of {Project} + {Partition No.} + {Configuration} + {#}.

Partition Fault Display Configuration

To configure the partition fault display, please see the command below.



{1} Partition fault display configuration programming address: 567.

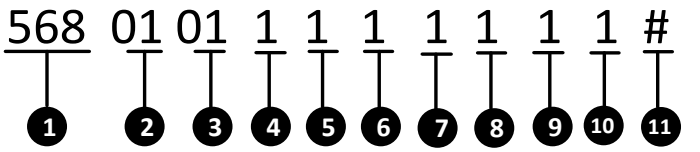
{2} The Tens' Digit of the Partition No.
{3} The Units' Digit of the Partition No.
{4} Ac Power Down
{5} Low Battery
{6} Control Panel Tampering Alarm
{7} Phone Line Disconnection
{8} Main keypad Disconnection
{9} Neywork Exception
{10}GPRS Exception

Command	Command Description	Command	Command Description
0	Disable	**1**	**Enable**

{11}End the command.

Partition Fault Prompt Sound Configuration

To configure the partition fault prompt sound, please see the command below.



{1} Partition fault display configuration programming address: 568.
{2} The Tens' Digit of the Partition No.
{3} The Units' Digit of the Partition No.
{4} Ac Power Down
{5} Low Battery
{6} Control Panel Tampering Alarm
{7} Phone Line Disconnection
{8} Main keypad Disconnection
{9} Network Exception
{10}GPRS Exception

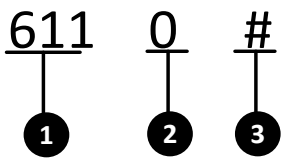
Command	Command Description	Command	Command Description
0	Disable	**1**	Enable

{11}End the command.

3.1.27 Center Group Configuration

Center Group Enabling Configuration

To enable the center group, please see the command below.



{1} Center Group Enabling Programming Address: 611, 615, 619, 623, 627and 631.

Command	Command Description	Command	Command Description
611	Center Group 1 Enabling Programming Address	**615**	Center Group 2 Enabling Programming Address
619	Center Group 3 Enabling Programming Address	**623**	Center Group 4 Enabling Programming Address
627	Center Group 5 Enabling Programming Address	**631**	Center Group 6 Enabling Programming Address

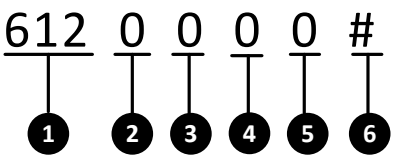
{2} Enable/Disable the Center Group

Command	Command Description	Command	Command Description
0	Disable	**1**	Enable

{3} End the command.

Center Group Uploading Mode Configuration

To configure the center group uploading mode, please see the command below.



{1} Center Group Uploading Mode Programming Address: 612, 616, 620, 624, 628 and 632.

Command	Command Description	Command	Command Description
612	Center Group1 Uploading Mode Programming Address	**616**	Center Group 2 Uploading Mode Programming Address
620	Center Group 3 Uploading Mode Programming Address	**624**	Center Group 4 Uploading Mode Programming Address
628	Center Group 5 Uploading Mode Programming Address	**632**	Center Group 6 Uploading Mode Programming Address

{2} Main Channel
{3} Backup Channel 1
{4} Backup Channel 2
{5} Backup Channel 3

{2}～**{5}**The channel can be selected as follows.

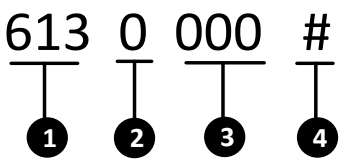
Command	Command Description	Command	Command Description
0	**OFF**	**1**	T1
2	T2	**3**	N1
4	N2	**5**	G1
6	G2		

{6} End the command.

There are 6 channels (T1, T2, N1, N2, G1 and G2) of the network security control panel. Each channel can be only used once during the center group uploading configuration, no matter it is served as the main channel or backup channel,

Center Group Zone Alarm Report Configuration

To configure the center group zone alarm report, please refer to the following command.



{1} Center Group Zone Alarm Report Programming Address: 613, 617, 621, 625, 629 and 633.

Command	Command Description	Command	Command Description
613	Center Group 1 Zone Alarm Report Programming Address	**617**	Center Group 2 Zone Alarm Report Programming Address
621	Center Group 3 Zone Alarm Report	**625**	Center Group 4 Zone Alarm Report

Command	Command Description	Command	Command Description
	Programming Address		Programming Address
629	Center Group 5 Zone Alarm Report Programming Address	**633**	Center Group 6 Zone Alarm Report Programming Address

{2} Delete/Add

{3} Zone No.

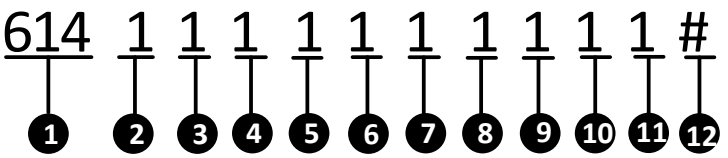
{4} End the command.

NOTE

The operation of adding/ deleting is just for current center group sending/not sending report, and will not impact other center groups.

Center Group Non-zone Alarm Report Configuration

To configure the non-zone alarm report of the center group, please refer to the command below.



{1} Center Group Non-zone Alarm Report Programming Address: 614, 618, 622, 626, 630and 634.

Command	Command Description	Command	Command Description
614	Center Group1 Non-zone Alarm Report Programming Address	**618**	Center Group 2Non-zone Alarm Report Programming Address
622	Center Group3	**626**	Center Group 4

	Non-zone Alarm Report Programming Address		Non-zone Alarm Report Programming Address
630	Center Group 5 Non-zone Alarm Report Programming Address	**634**	Center Group 6 Non-zone Alarm Report Programming Address

{2} Soft Zone Report
{3} System Status Report
{4} Alarm Clearing Report
{5} Testing Report
{6} Arming Report
{7} Disarming Report
{8} Control Panel Hijack Reportage
{9} Alarm Recovery Report
{10}Bypass Report
{11}Bypass Recovery Report

{2}～**{11**}Set the value as 1 to send the report. Set the value as 0 not to send the report.

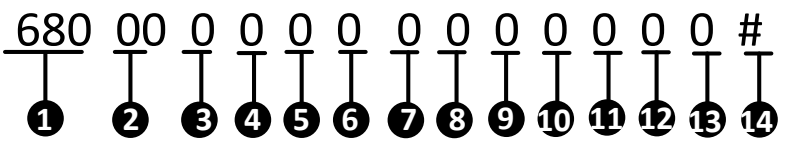
Command	Command Description	Command	Command Description
0	Not Sending	**1**	Sending

{12}End the command.

3.1.28 Whitelist Parameters Configuration

Non-zone Alarm Report Configuration

To configure the non-zone alarm report, please refer to the command below.



{1} Non-zone Alarm Report Configuration Command Address: 680.
{2} White List Number. 01~08 indicate white list No.1~No.8.
{3} Enable/Disable the Non-zone Alarm Report

Command	Command Description	Command	Command Description
0	Disable	**1**	Enable

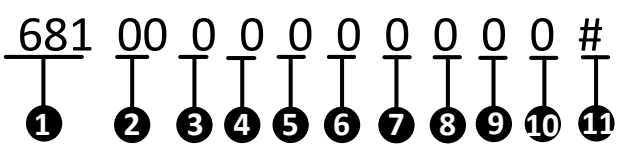
{4} Soft Zone Report
{5} System Status Report
{6} Alarm Clearing Report
{7} Testing Report
{8} Arming Report
{9} Disarming Report
{10}Control Panel Hijack Report
{11}Alarm Recovery Report
{12}Bypass Report
{13}Bypass Recovery Report
{4}~{13} Set the value as 1 to send the report. Set the value as 0 not to send the report.

Command	Command Description	Command	Command Description
0	Not Sending	**1**	Sending

{14}End the command.

Partition Arming Permission Configuration

To configure the permission of partition arming, please refer to the command below.



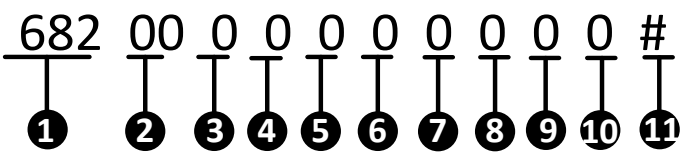
{1} Partition Arming Permission Configuration Command Address: 681
{2} White List Number. 01~08 indicate white list No.1~No.8.
{3} The Arming Permission of Partition 1
{4} The Arming Permission of Partition 2
{5} The Arming Permission of Partition 3
{6} The Arming Permission of Partition 4
{7} The Arming Permission of Partition 5
{8} The Arming Permission of Partition 6
{9} The Arming Permission of Partition 7
{10}The Arming Permission of Partition 8
{3}~{10} Enable/Disable the Permission of Partition Arming

Command	Command Description	Command	Command Description
0	Disable	**1**	Enable

{11}End the command.

Partition Disarming Permission Configuration

To configure the permission of partition disarming, please refer to the command below.



{1} Partition Disarming Permission Configuration Command Address: 682
{2} White List Number. 01~08 indicate white list No.1~No.8.
{3} The Disarming Permission of Partition 1
{4} The Disarming Permission of Partition 2
{5} The Disarming Permission of Partition 3
{6} The Disarming Permission of Partition 4
{7} The Disarming Permission of Partition 5
{8} The Disarming Permission of Partition 6
{9} The Disarming Permission of Partition 7
{10}The Disarming Permission of Partition 8

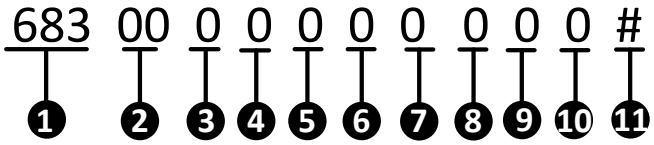
{3}~{10} Enable/Disable the Permission of Partition Disarming

Command	Command Description	Command	Command Description
0	Disable	**1**	Enable

{11}Completing

Partition Alarm Clearing Permission Configuration

To configure the permission of partition alarm clearing, please refer to the command below.



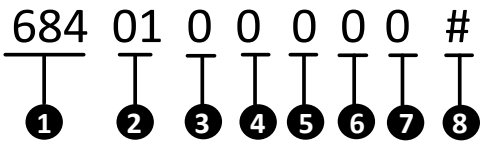
{1} Partition Alarm Clearing Permission Configuration Command Address: 683
{2} White List Number. 01~08 indicate white list No.1~No.8.
{3} The Alarm Clearing Permission of Partition 1
{4} The Alarm Clearing Permission of Partition 2
{5} The Alarm Clearing Permission of Partition 3
{6} The Alarm Clearing Permission of Partition 4
{7} The Alarm Clearing Permission of Partition 5
{8} The Alarm Clearing Permission of Partition 6
{9} The Alarm Clearing Permission of Partition 7
{10}The Alarm Clearing Permission of Partition 8
{3}~{10} Enable/Disable the Permission of Partition Alarm Clearing

Command	Command Description	Command	Command Description
0	Disable	**1**	Enable

{11}End the command.

The Interval Time of Whitelist Configuration

To configure the interval time of white list, please refer to the command below.



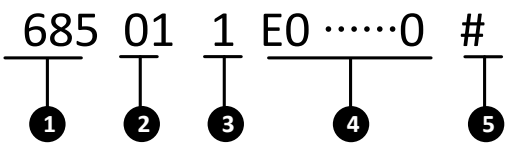
{1} The interval time of White List Configuration Command Address: 684.
{2} White List Number. 01~08 indicate white list No.1~No.8.
{3} Interval Time. The command is shown below.

Command	Description	Command	Description	Command	Description
0	0s	**1**	10s	**2**	30s
3	1min	**4**	5min	**5**	5-10min
6	User Defined				

{4} The user defined interval time: Thousands' Digit
{5} The user defined interval time: Hundreds' Digit
{6} The user defined interval time: Tens' Digit
{7} The user defined interval time: Digit
{4}~{7} Valid only when **{3}** is 6.
{8} End the command.

Handset Number Settings

To configure the handset number, please refer to the command below.



{1} Handset Number Command Address: 685.
{2} White List Number. 01~08 indicate white list No.1~No.8.

{3} Handset No. Segment

Command	Command Description	Command	Command Description
1	The first 16 characters of the 32 characters	**2**	The last 16 characters of the 32 characters

{4} The dialing number is 16 digits.

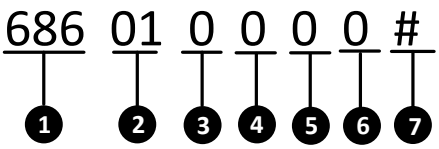
NOTE

- The letter E at the beginning of **{5}** can be set as A, indicating "+".
- The length of the each telephone number is 31 digits, and all the telephone number should be ended with *4.

{5} End the command.

Zone Report Type Configuration

To configure the zone report type, please refer to the command below.



{1} Zone Report Type Configuration Command Address: 686.
{2} White List Number. 01~08 indicate white list No.1~No.8.
{3} Set the value as 1 to send the report. Set the value as 0 not to send the report.

Command	Command Description	Command	Command Description
0	Not Sending	**1**	Sending

{4} Zone No.: Hundreds' Digit
{5} Zone No.: Tens' Digit
{6} Zone No.: Digit

NOTE

- When the Zone No. has no hundreds' digit, **{4}** can be omitted.
  Example: When you want to send report of Zone No.16. The command is 68601116#.
- When the Zone No. has no hundreds' digit and tens' digit, **{4}** and **{5}** can be omitted.
  Example: When you want to send report of Zone No.8. The command is 6860118#.

{7} End the command.

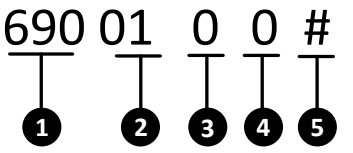
NOTE

After operating once, you can continuously configure with the command of {Project} + {Zone No.} + {#}

3.1.29 Schedule Configuration

Enabling Weekly Schedule

To enable the weekly schedule, please refer to the command below.



{1} Enabling Weekly Schedule Command Address: 690.
{2} Partition Number, 01~08 indicate partitions No.1~No.8.
{3} Enable/Disable Mandatory Arming

Command	Command Description	Command	Command Description
0	Disable	**1**	Enable

{4} It indicates to enable/disable the weekly schedule.

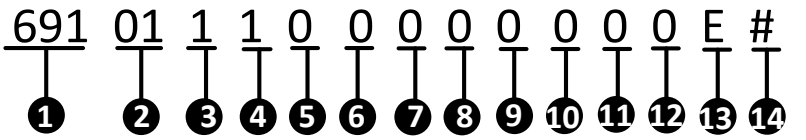
Command	Command Description	Command	Command Description

0	Disable	1	Enable

{5} End the command.

Weekly Schedule Time Parameter Configuration

To configure the time parameters of the weekly schedule, please refer to the command below.



{1} Weekly Schedule Time Parameter Configuration Command Address: 691.

{2} Partition Number. 01~08 indicate partitions No.1~No.8.

{3} Monday to Sunday

Command	Description	Command	Description	Command	Description
1	Monday	**2**	Tuesday	**3**	Wednesday
4	Thursday	**5**	Friday	**6**	Saturday
7	Sunday				

{4} Time bucket composed by **{5}~{12}**. The value range is 1~8.

{5}~{12} It indicates the start time and end time during the time bucket of **{4}**.

Start Time: **{5}{6}:{7}{8}**

End Time: **{9}{10}:{11}{12}**

NOTE

- When you set the start and end time as 00:00 and 00:00, all the settings from the present time bucket to the maximum time bucket will be cleared.
- When you set the start and end time as non-zero, the previous time bucket must be non-zero.
- When you set the start and end time as non-zero, only Arming in **{13}** can be set.

- When you set the start and end time as non-zero, end time must be greater than start time in every time bucket.
- When you set the start and end time as non-zero, the start time must be 5min greater than the end time of the previous time bucket.
- When you set the start and end time as non-zero, if the time bucket is overlapped with the latter ones, or the difference between them is less than 5min, all the settings of the latter ones will be cleared.

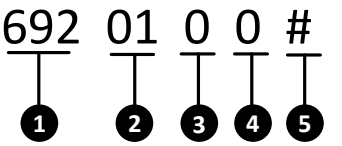
{13}Three types of Arming/Disarming.

Command	Command Description	Command	Command Description	Command	Command Description
A	General Arming/Disarming	**B**	Real-time Arming/Disarming	**C**	Stay Arming/Disarming

{14}End the command.

Copying Weekly Schedule

To copy the settings of the day **(n)** to another day **(l)** of the week in partition **(m)**, please refer to the command below.



{1} Copy Weekly Schedule Command Address: 692.
{2} Partition **(m)** Number. 01~08 indicate partitions No.1~No.8.
{3} It indicates the value range of the day **(n).**

Command	Description	Command	Description	Command	Description
1	Monday	**2**	Tuesday	**3**	Wednesday
4	Thursday	**5**	Friday	**6**	Saturday
7	Sunday				

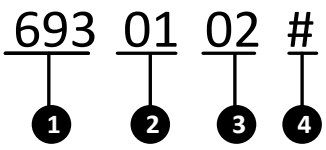
{4} It indicates the value range of the day **(l)**.

Command	Description	Command	Description	Command	Description
1	Monday	**2**	Tuesday	**3**	Wednesday
4	Thursday	**5**	Friday	**6**	Saturday
7	Sunday				

{5} Completing

Copy Weekly Schedule of Partition

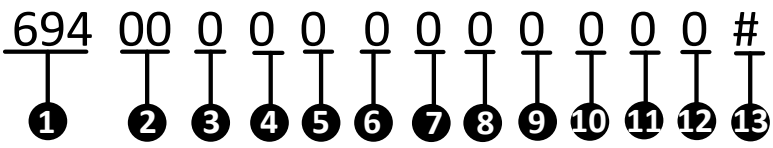
To copy the settings of partition **(m)** to partition **(n)**, please refer to the command below.



{1} Copy Weekly Schedule of Partition Command Address: 693.
{2} Partition **(m)** Number. 01~08 indicate partitions No.1~No.8.
{3} Partition **(n)** Number. 01~08 indicate partitions No.1~No.8.
{4} End the command.

Prior Schedule Date Parameter Configuration

To configure the date parameters of the prior schedule, please refer to the command below.



{1} Prior Schedule Date Parameter Configuration Command Address: 694.
{2} It indicates the prior schedule number. 00~30 indicate prior schedules No.00~No.30.

{3} It indicates to enable/disable the mandatory arming/disarming.

Command	Command Description	Command	Command Description
0	Disable	**1**	Enable

{4} It indicates to enable/disable the prior schedule.

Command	Command Description	Command	Command Description
0	Disable	**1**	Enable

{5}~{12} It indicates the start date and end date.

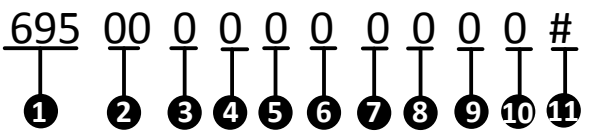
Start Date: **{5}{6}/{7}{8}**. The former is the month (value range 1~12), while the latter is the day (value range 1~30).

End Date: **{9}{10}/{11}{12}**. The former is the month (value range 1~12), while the latter is the day (value range 1~30).

{5} End the command.

Enabling Prior Schedule

To enable the prior schedule, please refer to the command below.



{1} Enabling Prior Schedule Command Address: 695.

{2} It indicates the prior schedule number. 01~30 indicate prior schedule No.1~No.30.

{3} Partition 1

{4} Partition 2

{5} Partition 3

{6} Partition 4

{7} Partition 5

{8} Partition 6

{9} Partition 7

{10}Partition 8

{3}~{10} It indicates to enable/disable prior schedule of Partition

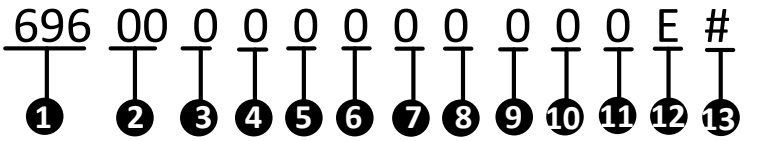
No.1~No.8.

Command	Command Description	Command	Command Description
0	Disable	**1**	Enable

{11}End the command.

Prior Schedule Time Parameter Configuration

To configure the time parameters of the prior schedule, please refer to the command below.



{1} Prior Schedule Time Parameter Configuration Command Address: 696.

{2} It indicates the prior schedule number. 01~30 indicate prior schedule No.1~No.30.

{3} It presents the time bucket composed by **{4}~{11}**. The value range is 1~8.

{4}~{11} It indicates the start time and end time during the time bucket of **{3}**.

Start Time: **{4}{5}:{6}{7}**

End Time: **{8}{9}:{10}{11}**

NOTE

- When you set the start and end time as 00:00 and 00:00, all the settings from the present time bucket to the maximum time bucket will be cleared.
- When you set the start and end time as non-zero, the previous time bucket must be non-zero.
- When you set the start and end time as non-zero, only Arming in **{12}** can be set.
- When you set the start and end time as non-zero, end time must be greater than start time in every time bucket.

- When you set the start and end time as non-zero, the start time must be 5min greater than the end time of the previous time bucket.
- When you set the start and end time as non-zero, if the time bucket is overlapped with the latter ones, or the difference between them is less than 5min, all the settings of the latter ones will be cleared.

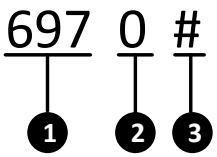
{12}Three types of Arming/Disarming.

Command	Command Description	Command	Command Description	Command	Command Description
A	General Arming/Disarming	**B**	Real-time Arming/Disarming	**C**	Stay Arming/Disarming

{13}End the command.

Enabling Trigger Schedule

To enable the trigger schedule, please refer to the command below.



{1} Enabling Trigger Schedule Command Address: 697.

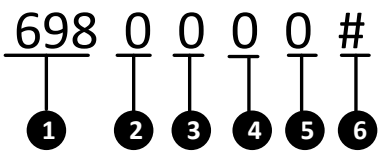
{2} It indicates to enable/disable the trigger schedule.

Command	Command Description	Command	Command Description
0	Enable	**1**	Disable

{3} End the command.

Trigger Schedule Trigger Parameter Configuration

To configure the trigger parameters of the trigger schedule, please refer to the command below.



{1} Trigger Schedule Trigger Parameter Configuration Command Address: 698.

{2} It indicates to delete/add the trigger schedule.

Command	Command Description	Command	Command Description
0	Delete	**1**	Add

{3} Trigger No.: Hundreds' Digit

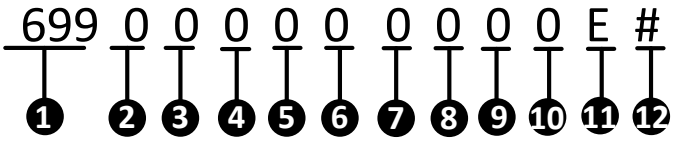
{4} Trigger No.: Tens' Digit

{5} Trigger No.: Digit

{6} End the command.

Trigger Schedule Time Parameter Configuration

To configure the time parameters of the trigger schedule, please refer to the command below.



{1} Trigger Schedule Time Parameter Configuration Command Address: 699.

{2} It presents the time bucket composed by **{3}~{10}**. The value range is 1~8.

{3}~{10} It indicates the start time and end time during the time bucket of **{2}**.

Start Time: **{3}{4}:{5}{6}**

End Time: **{7}{8}:{9}{10}**

- When you set the start and end time as 00:00 and 00:00, all the settings from the present time bucket to the maximum time bucket will be cleared.
- When you set the start and end time as non-zero, the previous time bucket must be non-zero.
- When you set the start and end time as non-zero, only Enable in **{11}** can be set.
- When you set the start and end time as non-zero, end time must be greater than start time in every time bucket.
- When you set the start and end time as non-zero, the start time must be 5min greater than the end time of the previous time bucket.
- When you set the start and end time as non-zero, if the time bucket is overlapped with the latter ones, or the difference between them is less than 5min, all the settings of the latter ones will be cleared.

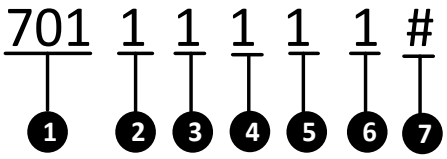
{11}Enable/disable the trigger schedule.

Command	Command Description	Command	Command Description
A	Enable	**B**	Disable

{12}End the command.

3.1.30 Wireless User Permission Configuration

To configure the permission of wireless users, please see the command below.



{1} Wireless User Permission Configuration Command Address: 701~732. 701~732 indicate wireless users No.1~No.32.
{2} Arming
{3} Arming Report
{4} Disarming
{5} Disarming Report

{6} Alarm Clearing

{2}~{6}

Command	Command Description	Command	Command Description
0	Supported	**1**	Unsupported

{7} End the command.

3.2 Keypad Alarm Operation Code

3.2.1 Device Initialization

Control panel can be recovered through the alarm keypad initialization; see the command below.

{Installer Code} + {*} + {8} + {9} + {#}

- The default password for the installer：012345.
- When doing initialization for the device, the No.1 partition is enabled by default and the partition-system mode of the global keypad cannot be switched to the global mode. When a non-No.1 partition is enabled, the global mode of the system will be enabled automatically.

3.2.2 Control panel Arming and Disarm

The operation of control panel arming and disarming is the same. Take the password 1234 as an example, and the command is shown below.

{1} +{2} + {3} +{4} +{#}

After the operation is completed, the arming status of the control panel will be changed (the status of arming will be exchanged into disarming), vice versa.

Operation method: {User password} + {*} + {1} + {7} + {#}.Take the password 1234 as an example, and the command is shown below:

{1} + {2} + {3} + {4} + {*} + {7} + {#}

After the operation is completed, the partition will change the status of

disarming (current status) into arming immediately. The exiting delay of partition is 0.

3.2.3 Stay Arming

Operation Method: {User password} + {*****} + {**4**} + {#}.Take the password 1234 as an example, and the operation is shown as follows:

{1} + {2} + {3} + {4} + {*} + {4} + {#}

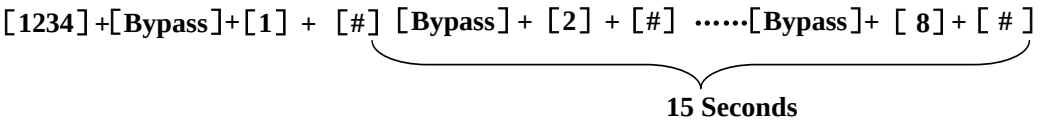
After the operation is completed, the partition will change the status of disarming (current status) into arming immediately. The bypass-supported zone of the partition will do auto-bypass simultaneously.

3.2.4 Zone Bypass/Recovery

After bypassing a zone, all the alarm devices in this zone will be blocked. ; see the command below

{User password} + {bypass} + {Zone Number} + {#}

For continuous bypass/ recovery; see the command below:



Continuous operation of multi-zone bypass/ recovery should be completed within 15 seconds

3.2.5 Group Bypass

After a partition is conducted with group bypass, all the alarm devices in group-bypass supported zone of the partition will be blocked. See the command below.

{User Password} + {*} + {4} + {1} + {#}

3.2.6 Group Bypass Recovery

After recovering the group bypass of a partition, all the alarm devices in group-bypass supported zone of the partition will be revalidated. See the command below.

{User Password} + {*} + {4} + {2} + {#}

3.2.7 Keypad Cancel Alarm

When the alarm is trigged, it can be canceled by keypad. The alarm can be canceled both under the arming and the disarming status.

Alarm Clearing under the Arming Status

Operation Method: {User Password} + {*} + {1} + {#}

Alarm clearing under the disarming Status

Operation Method (1): {*} + {1} + {#}

Operation Method(2): {Users Password} + {*} + {1} + {#}

3.2.8 Alarm Output Operation

For enabling alarm output of the alarm keypad, see the command below.

{Password} + {*} + {8} + {5} + {n} + {#}

For disabling alarm output of the alarm keypad, see the command below.

{Password} + {*} + {8} + {6} + {n} + {#}

The control panel supports 16 channels of alarm outputs, the N valuation should be 1-16.

3.2.9 Emergency Alarm

Press the {PANIC} button on the alarm keypad for 3 seconds or more. The emergency alarm will be triggered after a double-beep sound.

3.2.10 System Status Query

In query mode, there are special meanings (see the table below) for the 8 indicators on alarm keypad. Press the {Status} key for current system information Query.

Serial Number	Meaning	Serial Number	Meaning
1	AC Power Loss	**5**	Keypad Disconnection
2	Low Battery	**6**	Network Disconnection
3	Tampering Alarm Enabling	**7**	GPRS Exception
4	Telephone line Disconnection	8	Expansion Bus Exception

3.2.11 Control Panel and Wireless Device Connection

The steps of connecting wireless device with the control panel are shown as follows.

1. Enter the command of **{password} + {*} + {91} + {wireless device No.} + {#}** with the RF keypad to enter the connection mode.
2. Press any key on the keyboard to complete the connection.

3.2.12 Deleting the Specified Connected Wireless Device

Follow the command below to delete the connected wireless device.

{password} + {*} + {90} + {wireless device No.} + {#}

3.2.13 Deleting all the Connected Wireless Device

Follow the command below to delete all the connected wireless devices.

{password} + {*} + {92} + {#}

3.2.14 Main Operator Password Changing

The user password can be changed by main operator. The operations are divided into following steps:

Steps:

1. **{Master Code} } + {*} + {0} + {#}**
2. **{User Number} + {#}**
3. **{New Password} +{#}**
4. **{New Password}+{#}**

The password will be changed by the above four steps

The User Number must be expressed into three digits, such as 002.

3.2.15 Control Programming Operation

The control panel can be configured via alarm keypad operation; configuration process is generally divided into three steps:

Steps:

1. Enter the programming mode; see the command below:

   {Installer Code} + {*} + {0} + {#}
2. Control panel configuration operation (see section 4.1)
3. Exit programming mode; see the command below:

   {*} + {#}

3.2.16 Entering Partition

See the command below to enter the partition.

{*} + {3} + {n} + {#}

3.2.17 Alarm Center Test

Partition keypad operation is used to test the communication between control panel and the alarm center; see the command below:

{password} + {*} + {6} + {1} + {#}

One operation generates one test report. It is used to test the communication between the control panel and center after installing the system or during the inspection.

3.2.18 Project Mode

Enter the project mode to debug alarm control panel; see the command below:

{password} + {project} + {9} + {0} + {n} + {#}

Long press {Project} / {State} or {*} {#} key to exit the project mode after debugging.

When the evaluation of n is 1 or 2, the handset 1 and 2 are in dialing status.

When the evaluation of n is 3 or 4, the network center1 and 2 are in uploading status.

When the evaluation of n is 5 or 6, the GPRS center is 1 and 2 are in uploading status.

3.2.19 Enabling/Disabling Key Tone

For keypad tone status switch, see the command below:

{*} + {5} + {1} + {#}

3.2.20 LCD Backlight Control

For LCD backlight control; see the command below：

{*} + {5} + {2} + {n} + {n} + {n} + {#}

{n}{n}{n}refers to the light duration in seconds, and 999 means the LCD is always light The default duration is 900 seconds, and the parameters will be restored after reboot.

3.2.21 LCD Backlight off

For Disabling the LCD backlight, see the command below:

{*} +{8} + {#}

3.2.22 Pacing

The pacing function is used for debugging; see the command below:

{password} + {*} + {6} + {0} + {#}

NOTE

- The function of pacing is only available under the status of disarming and non-fault of the zone. The system will do auto-arming in the pacing mode without reporting any CID log. The siren will start warning after the alarm is triggered and stop warning if the alarm is dismissed.
- If the zone is disarmed, it will exit the pacing mode automatically.

3.2.23 SMS Arming/Disarming

The control panel supports SMS arming/disarming, the command is shown below:

- Away arming for the partition

  {#} +{121} +{#} +{Partition No.} + {#}
- Instant arming for the partition

  {#} +{122} +{#} +{Partition No.} + {#}
- Stay arming for the partition

  {#} +{123} +{#} +{Partition No.} + {#}
- Partition disarming

  {#} +{120} +{#} +{Partition No.} + {#}
- Partition alarm clearing

  {#} +{100} +{#} +{Partition No.} + {#}

NOTE

The partition No. is with three digits. for example. If the partition No. is 1. The command of partition alarm clearing is **{#} +{100} +{#} +{001} + {#}**

3.2.24 Control Panel Soft Recovery

For control panel soft recovery; see the command below:

{master code} + {*} + {6} + {8} + {#}

- All unissued CID logs will not be reissued. Newly generated report will be issued after system recovery.
- The timer of the test report will not be cleared, and will remain the value before recovery till the recovery processes being completed.

3.2.25 Current Fault Tone Disabling

To disable the current fault tone; see the command below:

{*} + {5} + {6} + {#}

If there are new faults, the prompt sound will re-Tip.

3.2.26 Test Report Manually Triggering

To trigger test report manually; see the command below:

{password} + {*} + {6} + {1} + {#}

One operation generates one test report. It is used to test the communication between the control panel and center after installing the system or during the inspection.

3.2.27 Keypad Locking and Unlocking

If a user failed to operate for five times, the keypad will be locked for 30 seconds. During the lock duration, the keypad backlight blinks and all of the key operations are invalid. The keypad will be unlocked after 30 seconds.

3.2.28 Exiting the Operation

See the command below to exit the operation.

{*}{#}

3.3 System Status Display Demonstration

The system status display demonstration indicates the keypad display interface of system status without any key pressing.

Powering on Display Demonstration

The display demonstration after powering on is shown below.

HIKVISION

System Status (normal) Display Demonstration

The display demonstration of system status (working properly) is shown below.

Global Keypad

SYS1D	SYS2R	SYS3A	SYS4R
SYS5R	SYS6R	SYS7R	SYS8R

The system status description is shown below.

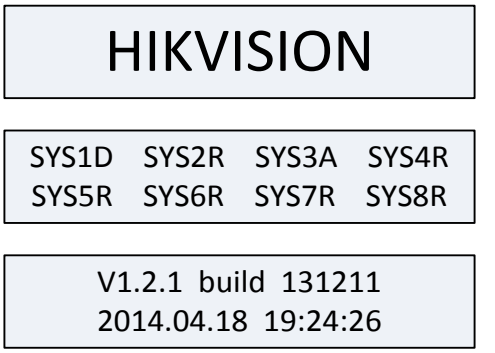
System Status	Description
SYS1D	Partition1 Disarmed
SYS2R	Partition2 Ready
SYS3A	Partition3 Armed
SYS4R	Partition4 Ready
SYS5R	Partition5 Ready
SYS6R	Partition6 Ready
SYS7R	Partition7 Ready
SYS8R	Partition8 Ready

Partition Keypad

HIKVISION
System Fault

Keypad Standby Status Display Demonstration

The standby status display demonstration is shown below.



NOTE

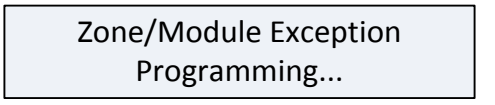
The LCD keypad displays the version of the control panel and the time of operation.

Global Keypad Programming Status Display Demonstration

The programing status includes normal status and abnormal status. The demonstration is shown below.

Normal Status

Abnormal Status



System Status (abnormal) Display Demonstration

Global Keypad

SYS1D	SYS2R	SYS3A	SYS4R
SYS5R	SYS6R	SYS7R	SYS8R

Partition Keypad

The system exception display of the partition keypad includes interfaces of alarm, fault and bypass.

- **Zone Alarm**

Zone Alarm
001 002 003 004 005 006

- **Zone Offline**

Zone Offline
001 002 003 004 005 006

- **Zone Fault**

Zone Fault
001 002 003 004 005 006

- **Zone Bypass**

Zone Bypass
001 002 003 004 005 006

System Pacing Display Demonstration

The system pacing display demonstration is shown below.

Work Test
001 002 003 004 005 006

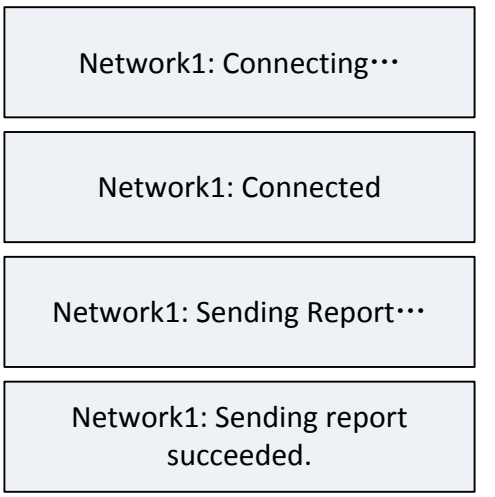
System Fault Display Demonstration

The system fault display demonstration is shown below.

AC Power Off; Low Battery Voltage;

Display Demonstration in Project Mode

The demonstration is shown below.



Chapter 4 Accessing by Client Software

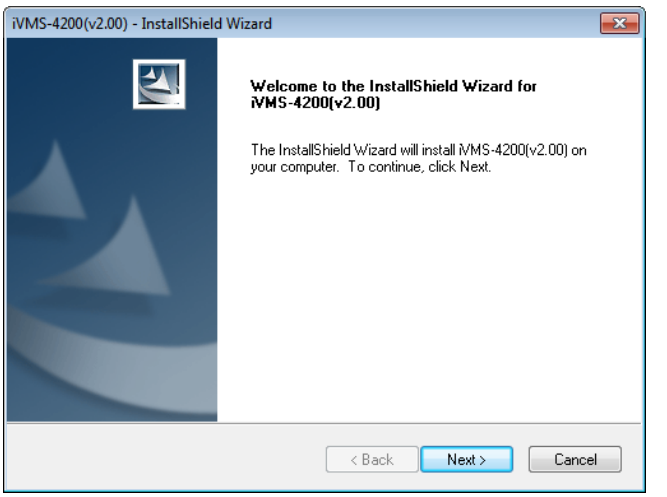
Check the package contents and make sure that the device in the package is in good condition and all the assembly parts are included.

4.1 Installing the iVMS-4200

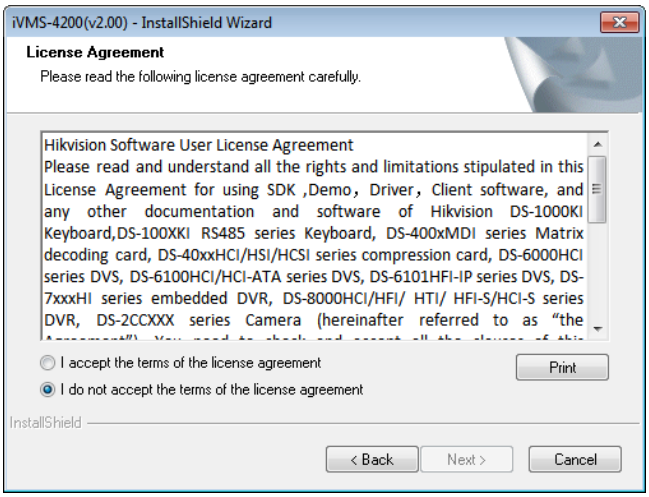
Insert the installation media of iVMS-4200 into the appropriate computer.

Perform the following steps to install the iVMS-4200 client software.

1. Double-click the program file iVMS-4200(v2.00) to enter the welcome panel of the InstallShield Wizard. Click Next to start the InstallShield Wizard.



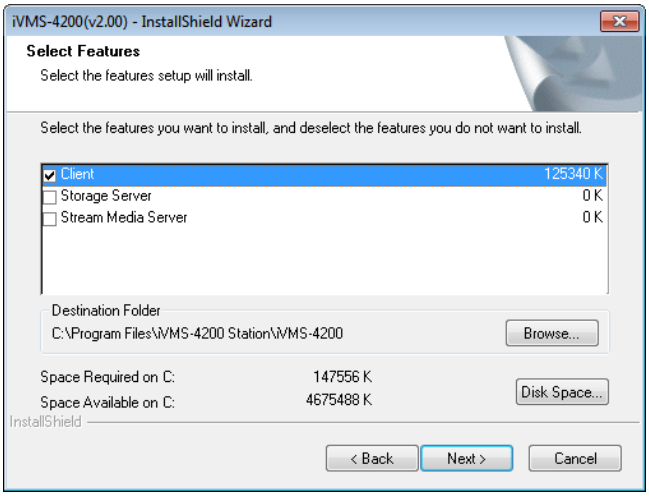
2. Read the License Agreement. Click Print if you want to print the license agreement.



If you accept the terms of the license agreement, click I accept the terms of license agreement. Click Next to continue.

Otherwise click **I do not accept the terms of the license agreement**, and then click **Cancel** to cancel the installation

3. On the next panel , you are prompted to select the function module to install.



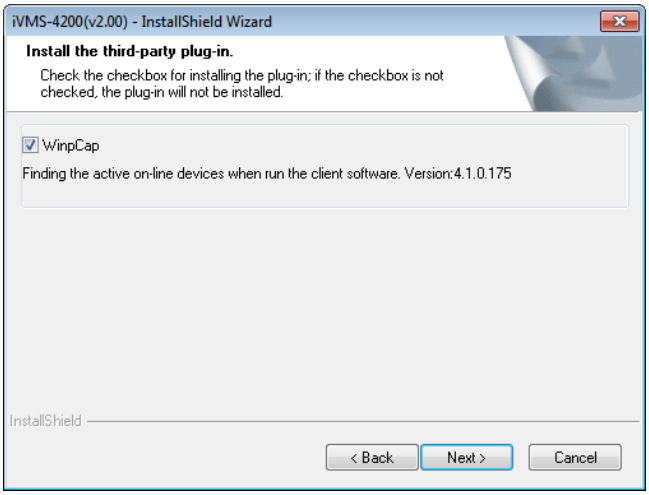
Set installation directory where the client software is to be installed. You can either accept the default directory that is displayed, or click **Browse** and select a different directory.

NOTE

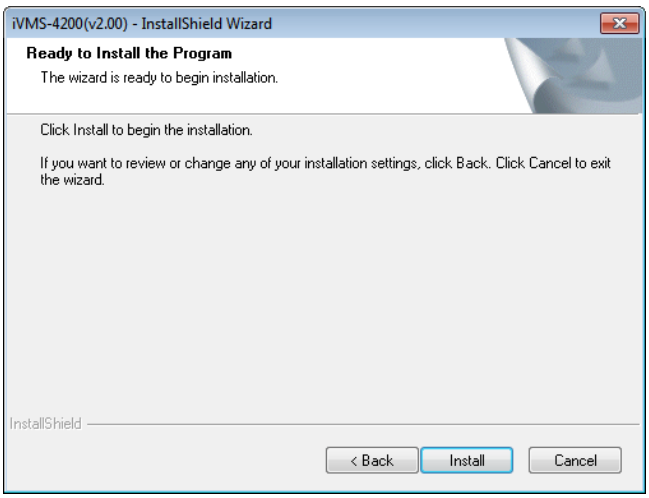
The default directory is *C:\Program Files\iVMS-4200 Station\iVMS-4200*.

Click **Next** to continue.

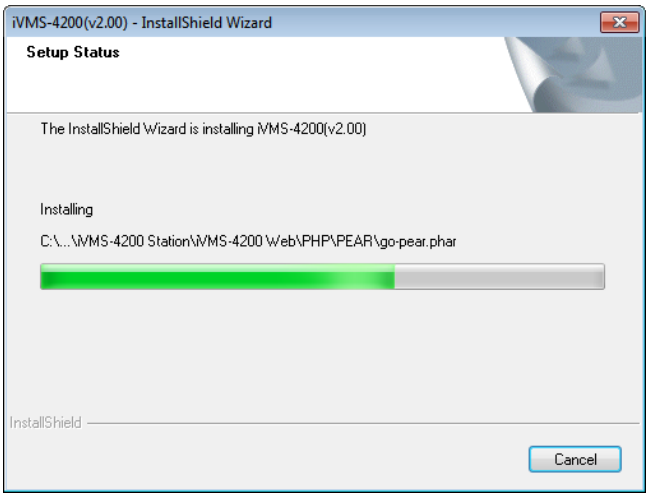
4. Install the WinpCap plug-in according to the prompts to detect the online devices when running the client software.



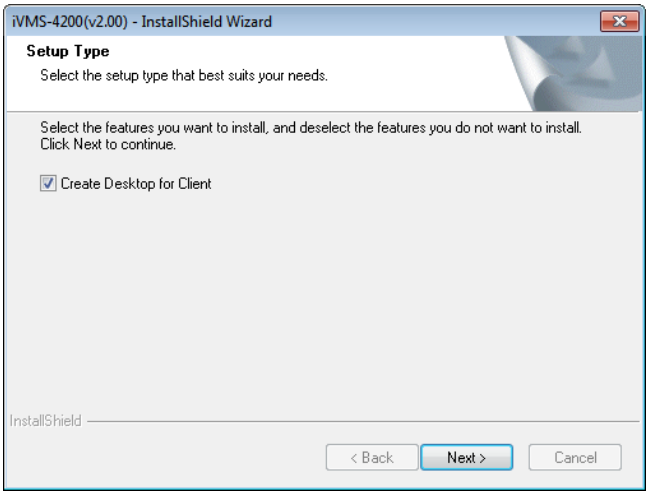
5. Read the pre-install information and click **Install** to begin the installation.



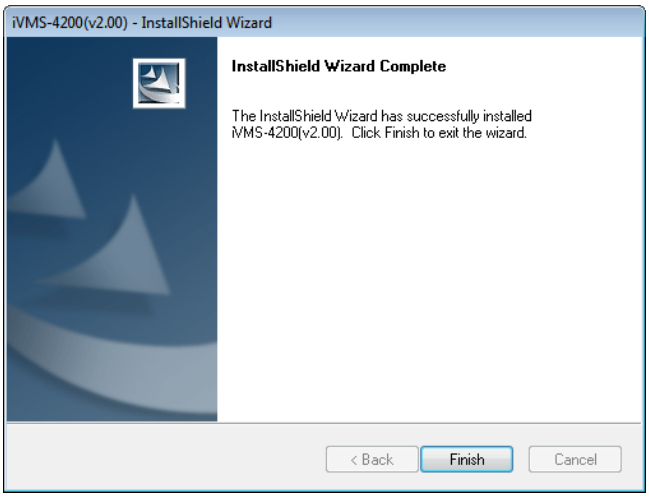
6. A panel indicating progress of the installation is displayed. A percentage completion bar is updated as the installation progresses.



7. Select the setup type according to your need.
   You can check the checkbox of **Create Desktop for Client** to create a shortcut icon on the desktop for the client software.



8. Read the post-install information and click **Finish**.

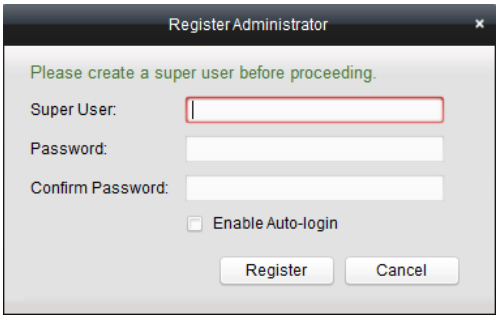


4.2 User Registration and Login

For the first time to use iVMS-4200 software, you need to register a super user for login.

Steps:

1. Input the super user name and password.
2. Confirm the password.
3. Optionally, check the checkbox of **Enable Auto-login** to log in the software automatically.
4. Click **Register**. Then, you can log in the software as the super user.



- A user name cannot contain any of the following characters: / \ : * ? " < > |
- The password cannot be empty and the length of the password should be no less than six characters.

When opening iVMS-4200 after registration, you can log in the software with the registered user name and password.

Steps:

1. Input the user name and password you registered.
2. Optionally, check the checkbox of **Enable Auto-login** to log in the software automatically.
3. Click **Login**.

4.3 Network Security Control Panel Settings

Purpose:

In this section, you are able to configure or view the basic parameters (such as the system information, alarm information, network data, device status and so on) of the video security control panel.

4.3.1 Add/Edit/Delete the Device

Add a Device:

Steps:

1. Click **Add Device** to open the device adding dialog box.
2. Select **IP/Domain** as the adding mode.
3. Input the required information.
   Nickname: Edit a name for the device as you want.
   Address: Input the device's IP address or domain name.
   Port: Input the device port number. The default value is *8000*.
   User Name: Input the device user name.
   Password: Input the device password.
4. Optionally, you can check the checkbox **Export to Group** to create a group by the device name. All channels and alarm inputs of the device will be imported to the corresponding group by default.
5. Click **Add** to add the device.

Edit a Device

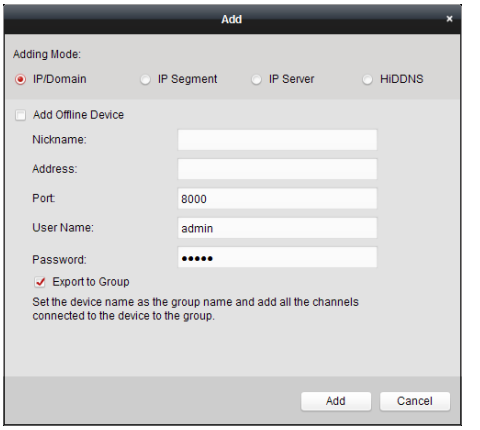
Purpose:

You can edit the device information in this section, including the device name,

address and port number.

Steps:

1. On the **Device Management** interface, click and select a control panel in the device list.
2. Click on the **Modify** button on the upper side of the list to enter the device modify interface.



3. Enter the required nick name, address, and port number and then enter the admin username and password.
4. Click **Modify** to save the changes.

Delete a Device

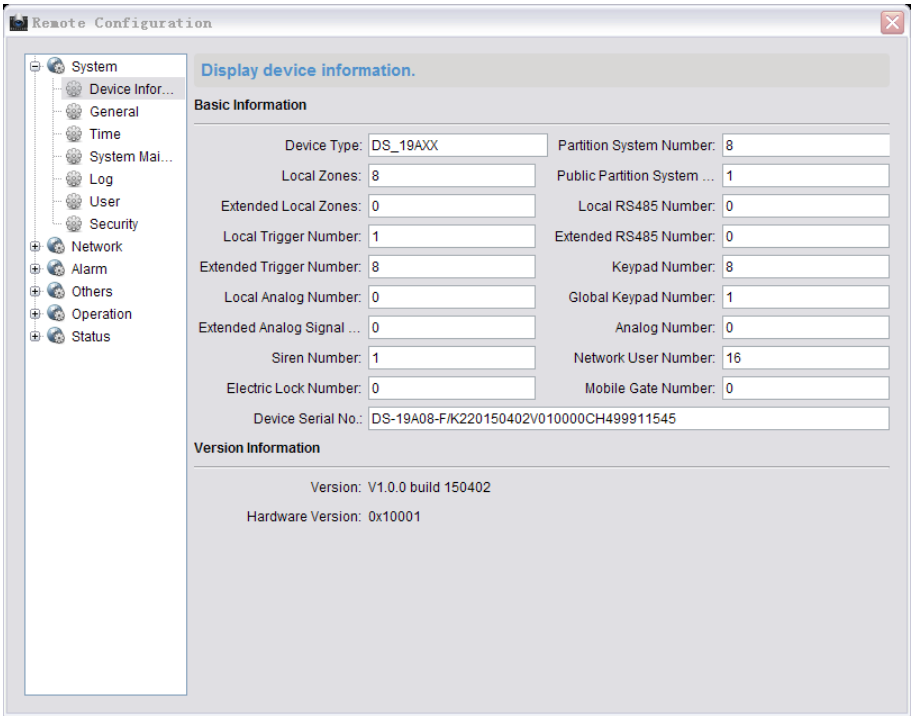
Select device from the list, click **Modify**/**Delete**, and then you can modify/delete the information of the selected device.

4.4 Remote Configuration

Purpose:

In this section, you are able to configure device parameters remotely.

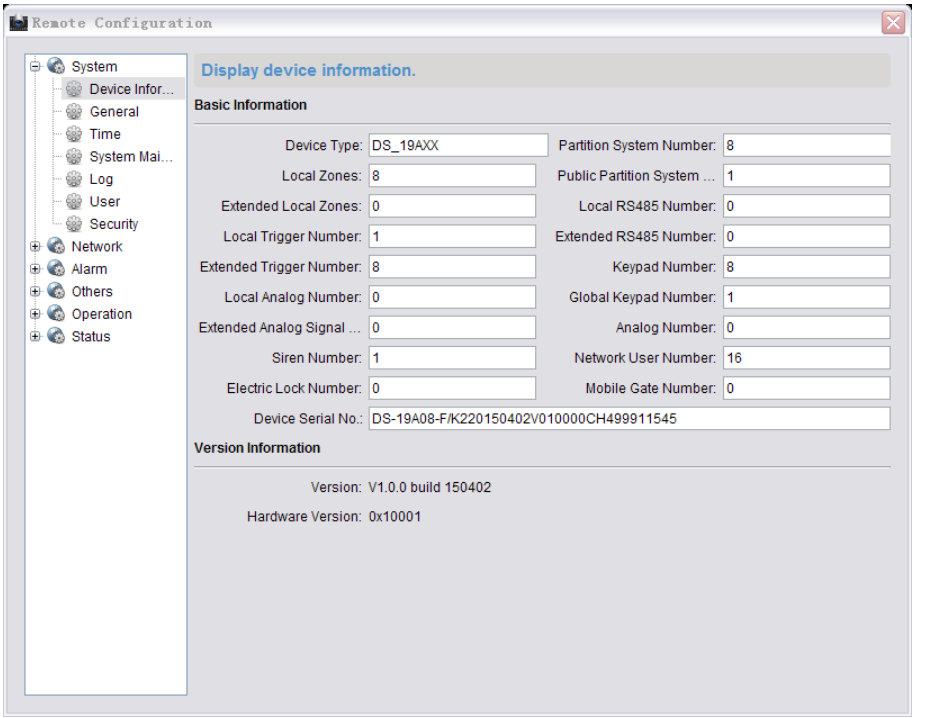
Click the **Remote Configuration** button to enter the interface.



4.4.2 System Information Configuration

Purpose:

In this section, you can configure the system parameters (such as time, log, user, security, system maintenance and so on) for the device.

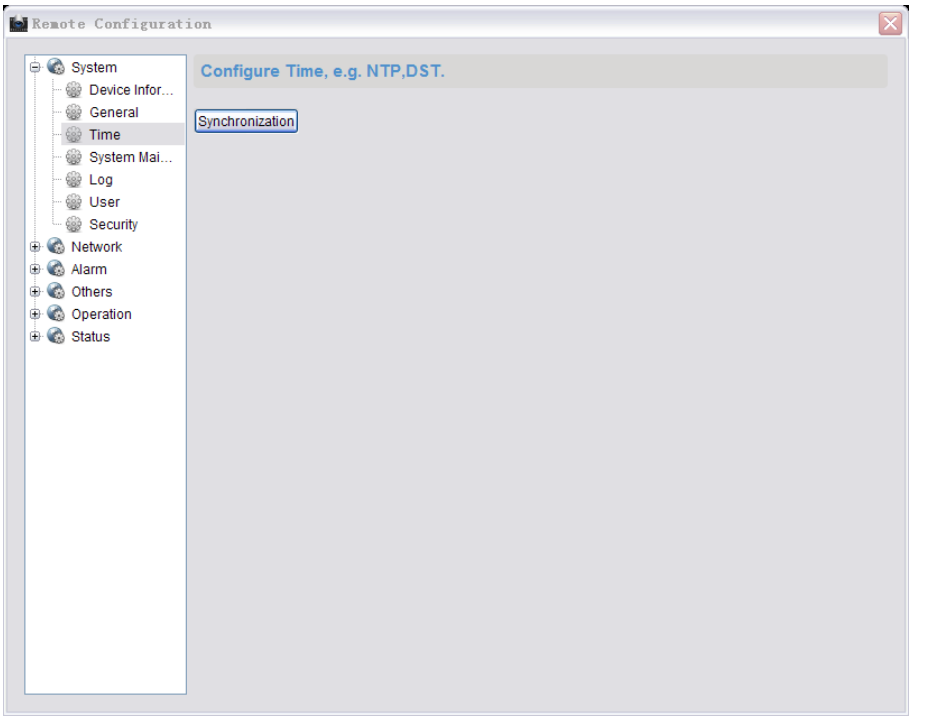


Timing Configuration

Before You Start:

Before you start configuring the security control panel, you need to do timing for the device first.

Enter **Remote Configuration>System->Time** to get the configuration page. Click the **Synchronization** button to complete the settings.



User Configuration

Purpose:

You can add, edit, or delete the network operator and keypad operator in this section.

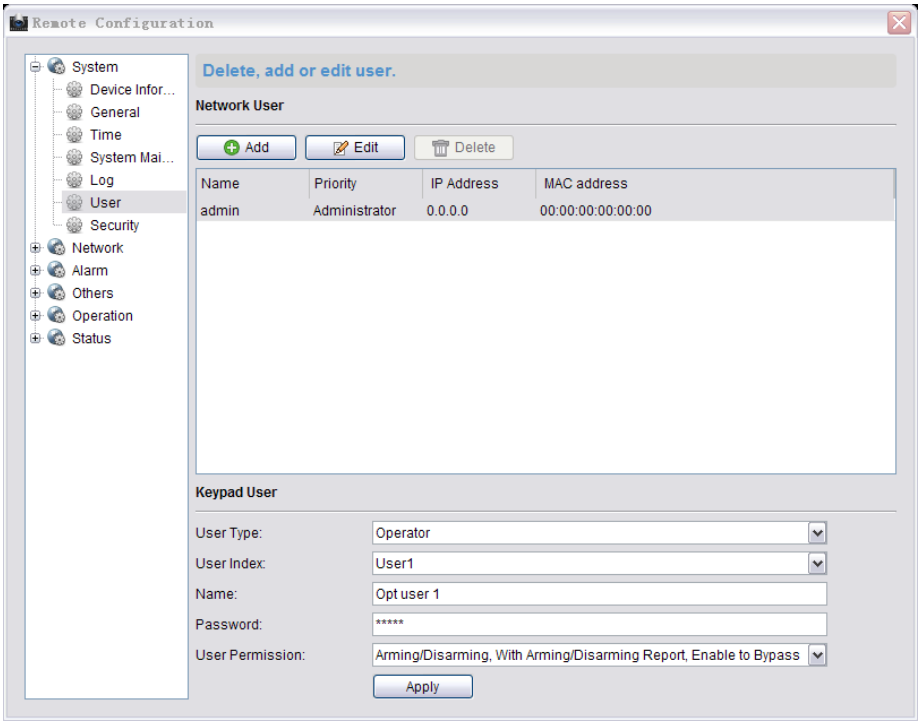
- **Network User**

  Add a Network User

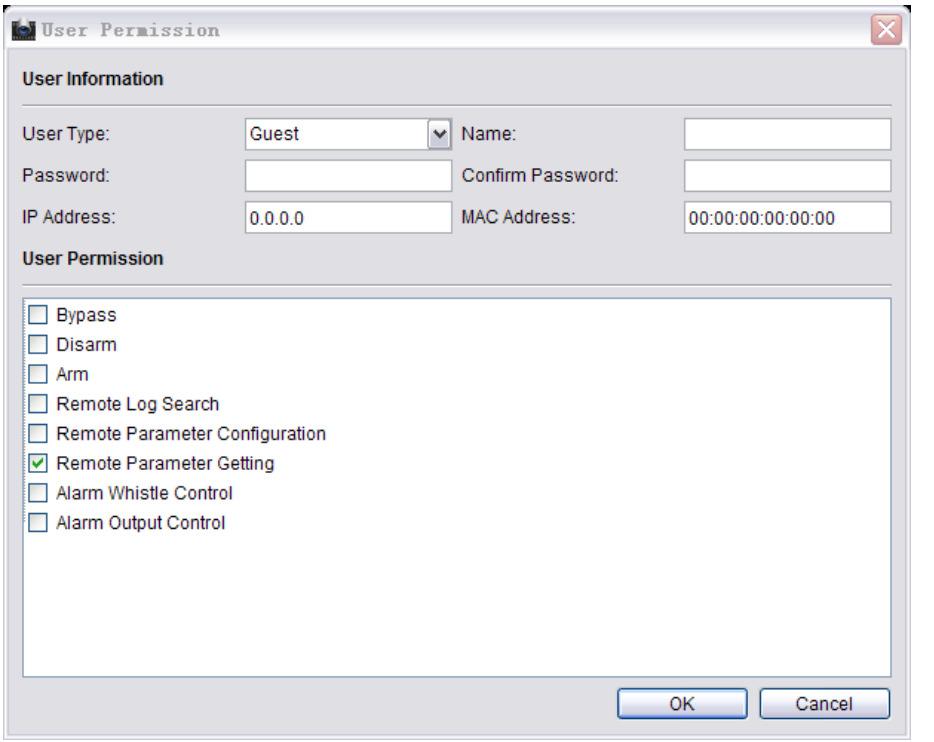
  Steps:

  1. Enter the user configuration interface.

     Remote Configuration->System->User



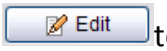
2. Click  to enter the interface of adding a network user.



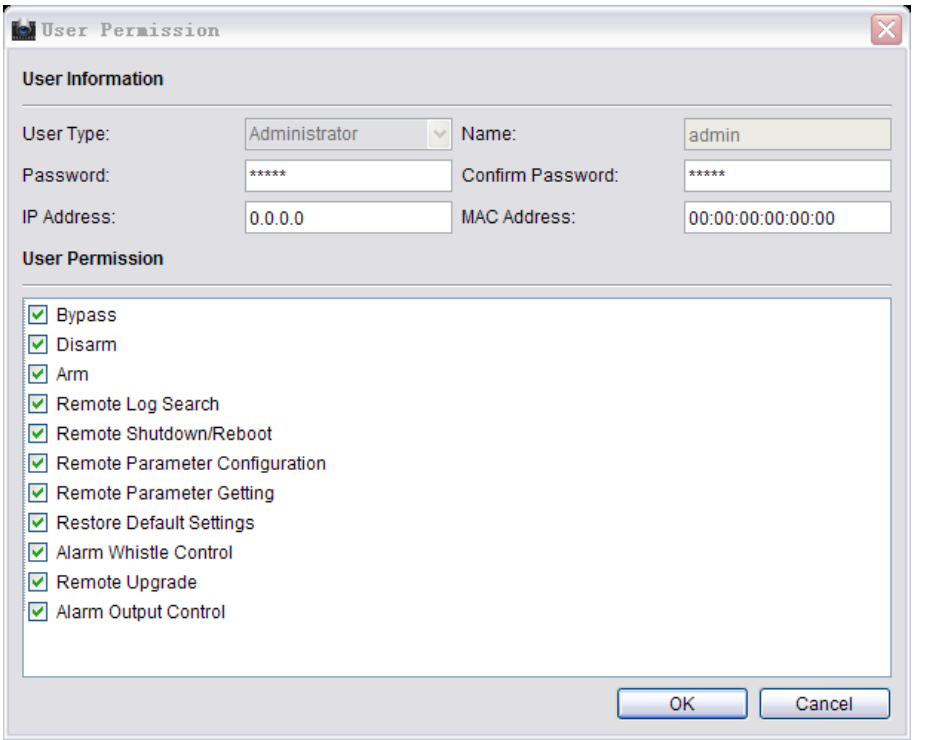
3. Enter the corresponding user information including the user type, user name, password, IP address, and MAC address.
4. Select the permission of the user.
5. Click **OK** to finish the settings.

Edit a User

Steps:

1. Click 

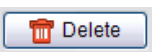
to enter the interface of editing the selected user.



2. Edit the corresponding user information including the user type, user name, password, IP address, and MAC address
3. Edit the permission of the user.
4. Click **OK** to finish the settings.

Delete a user

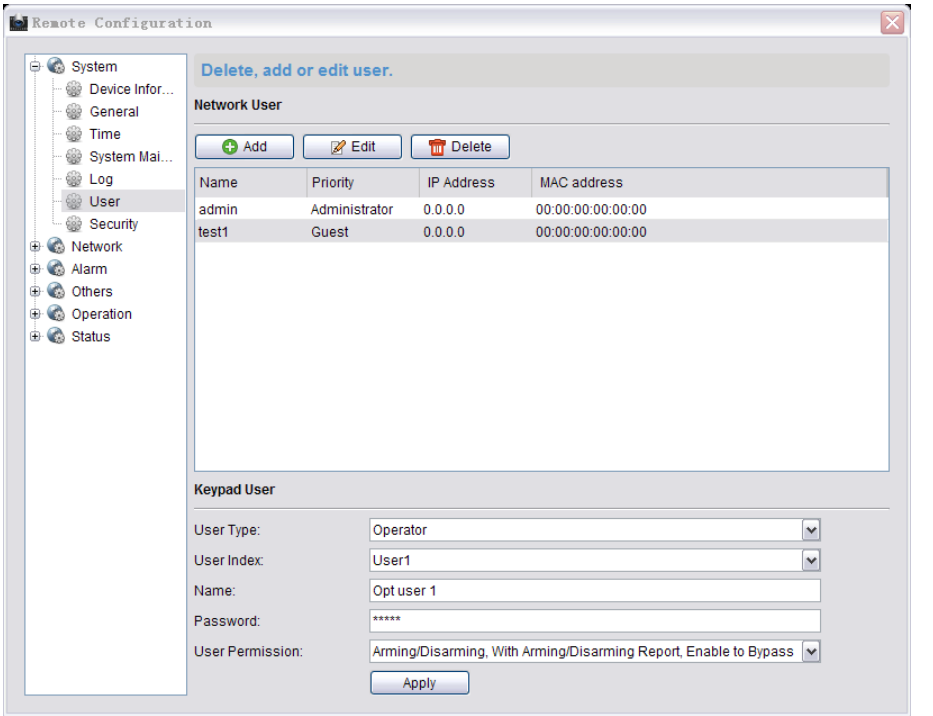
Steps:

1. Select a user needs to be deleted.
2. Click 

to delete the user.

- **Keypad User**

  The control panel supports at most 16 keypad operators.



Steps:

1. Select the user type. Operator and installer can be selected.
2. Select the index number of the keypad user, up to 16 numbers can be selected.
3. Enter the name of the keypad operator.
4. Enter the password of the operator.
5. Click the dropdown menu to select the user permission.
6. Click **Apply** to save the settings.

4.4.3 Network Configuration

Purpose:

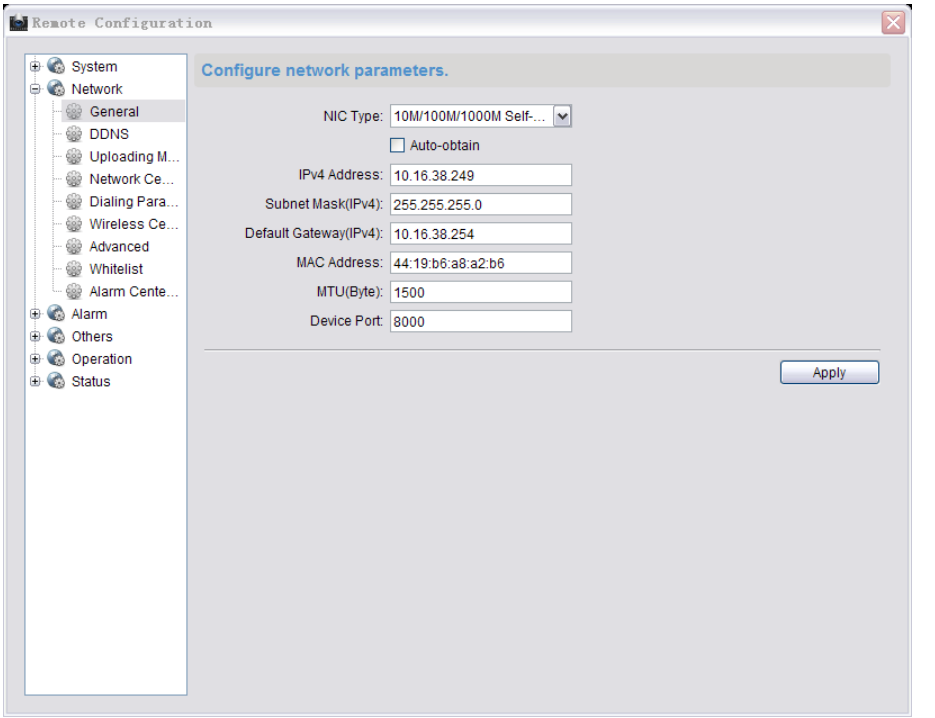
You can edit the general network parameters in this section.

- **General Network Parameters Configuration**

Steps:

1. Enter the general network configuration page.

   Remote Configuration-> Network->General



2. Configure the NIC settings, including the IPv4(IPv6) Address, IPv4(IPv6) Subnet Mask and IPv4(IPv6) Default Gateway.
3. Click **Apply** to save the above settings.

NOTE

- The valid value range of Maximum Transmission Unit (MTU) is 500 ~ 9676. The default value is 1500.
- The Multicast sends a stream to the multicast group address and allows multiple clients to acquire the stream at the same time by requesting a copy from the multicast group address.
  Before utilizing this function, you have to enable the Multicast function of your router and configure the gateway of the control panel.

DDNS Configuration

Purpose:

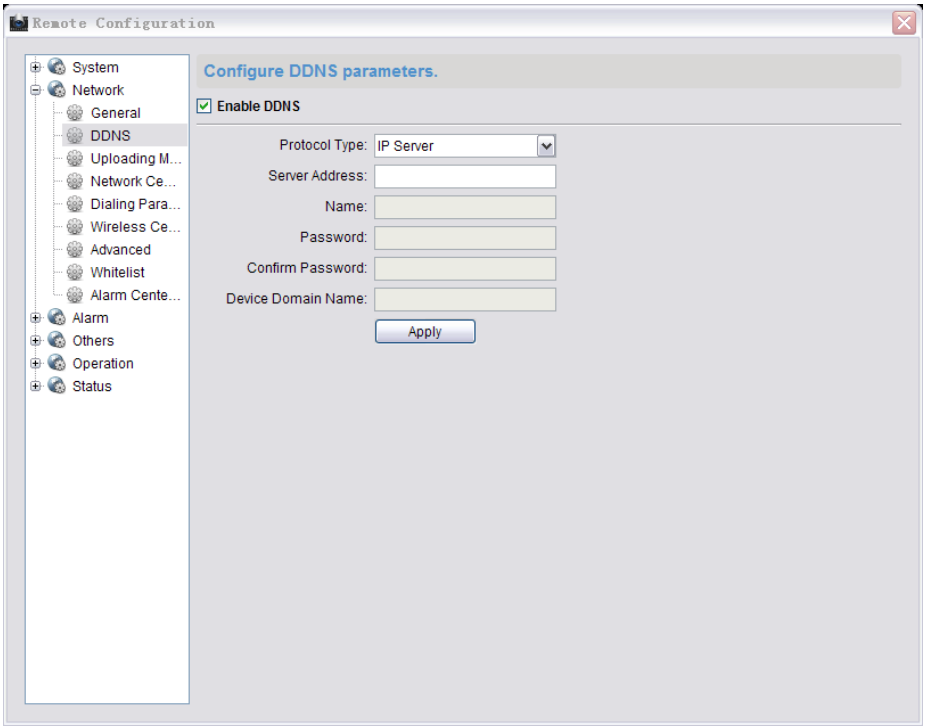
If your control panel is set to use PPPoE as its default network connection, you can use the Dynamic DDNS for network access.

***Before you start*:**

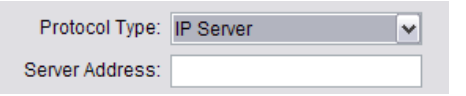
Registration on the DDNS server is required before configuring the DDNS settings of the control panel.

Steps:

1. Enter the DDNS Settings interface:
   Remote Configuration> Network > DDNS



2. Check the **Enable DDNS** checkbox to enable this feature.
3. Select **DDNS Type**.



4. Enter the Server Address of the IP Server.
5. Click **Apply** to save the settings.

NOTE

The **Server Address** should be entered with the static IP address of the computer that runs the IP Server software. For the IP Server, you have to apply a static IP, subnet mask, and gateway and preferred DNS from the ISP.

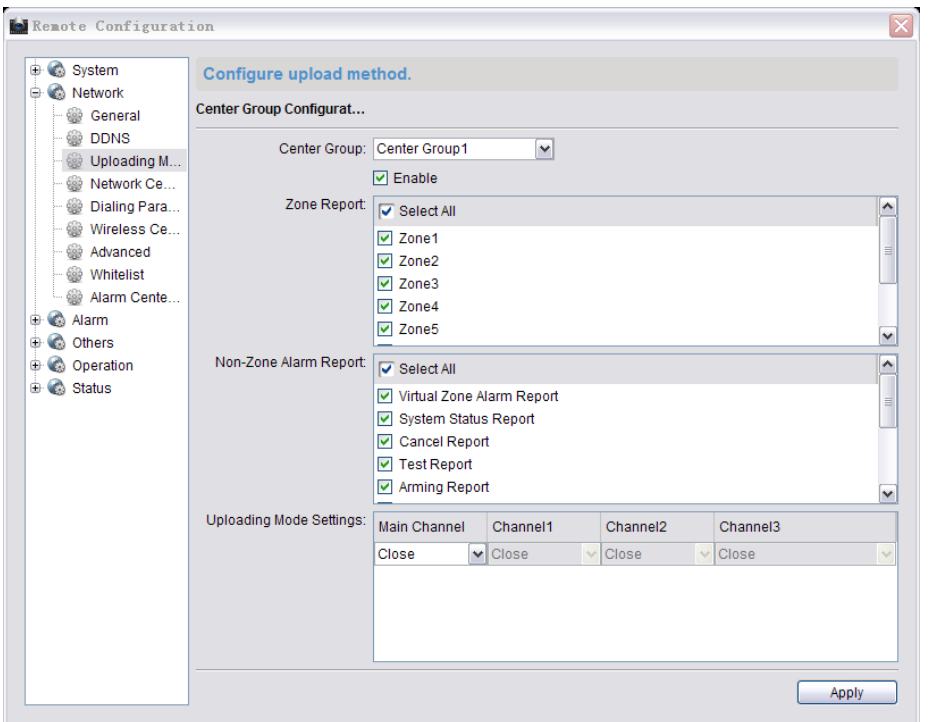
Uploading Mode Configuration

Purpose:

You can select to send Zone report, alarm report and configure the uploading mode of the selected center group in this section.

Steps:

1. Enter the uploading mode configuration page.
   Remote Configuration->Uploading Mode Settings



2. Click the drop down menu to select a center group.
3. Check the **Enable** checkbox to enable the configuration
4. Check the checkbox to select the required Zone for sending the Zone report for the Zones without Zone report.

   NOTE At most 6 center groups can be inter-combined to send the alarm report.
5. Check the checkbox to select the type of non-Zone alarm report.

6. Click each dropdown menu to configure the uploading channel.
7. Click **Apply** to save the settings.

NOTE The alarm channel of each center group should be configured in order.

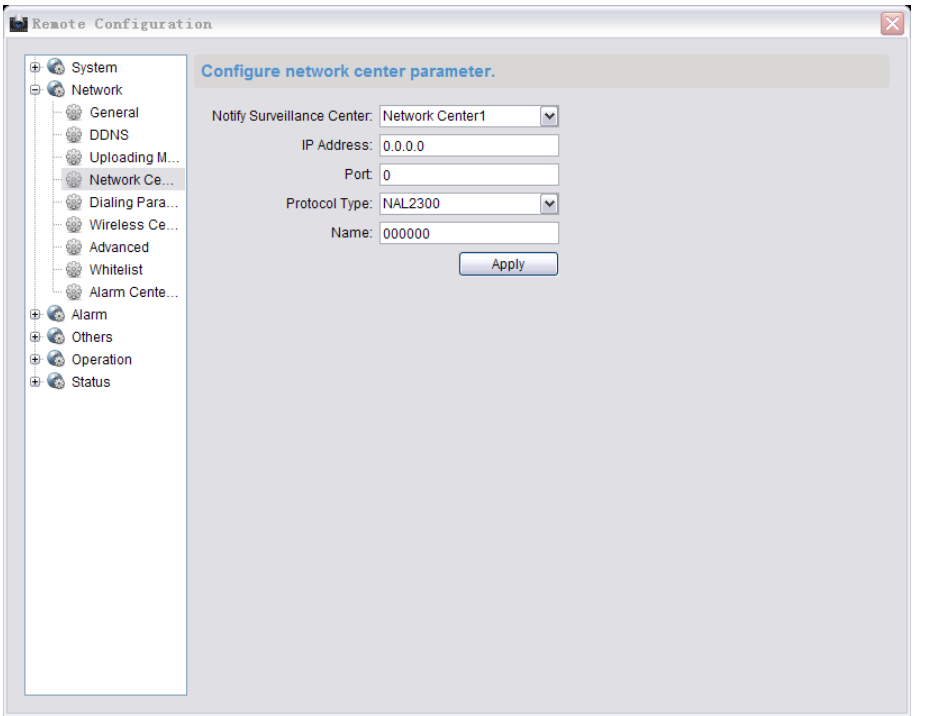
Network Center Configuration

Purpose:

In this section, you can configure the parameters(such as server type, IP address, port No.,and so on)of the network center.

Steps:

1. Enter the network center configuration page.
   Remote Configuration->Network Center



2. Click and select a network center. Two centers are selectable.
3. Click the dropdown menu to select a sever type. Two sever types are available: IP4/IP6 and domain.
4. Enter the IP address that is used to communicate with the network alarm

receiving center.

5. Enter the port No. for communicating with the alarm-receiving center.
6. Click the dropdown menu to select the protocol type.
7. Enter the username that is applying for displaying in the alarm-receiving center.

NOTE

The length of the username should be 6 characters.
Only numeric (0~9), and letter (A~F&a~f) are valid for this username.

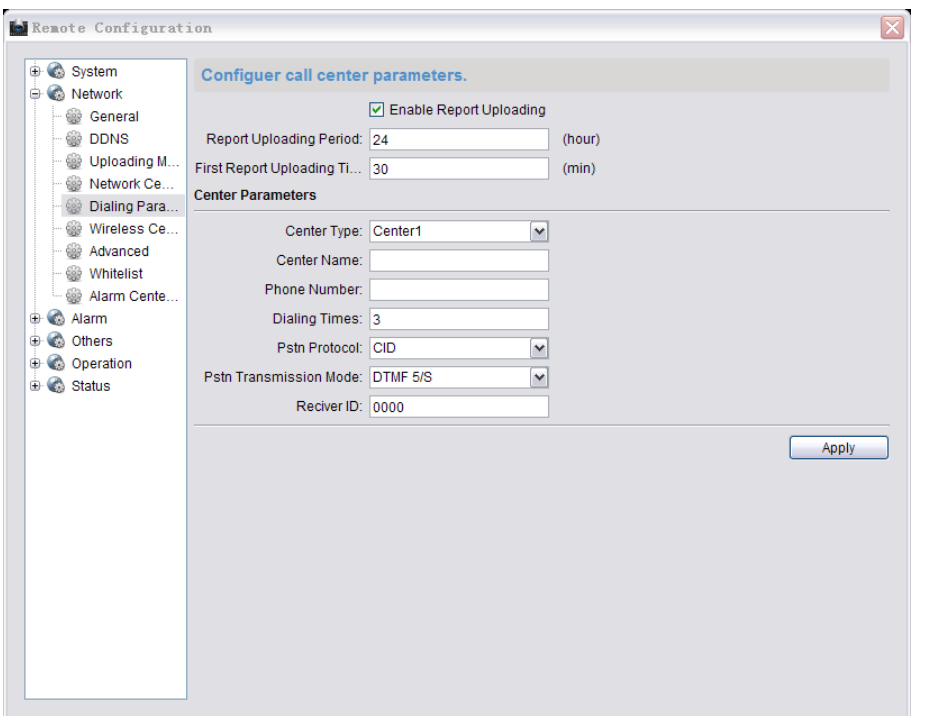
Dialing Center Configuration

Purpose:

You can configure the parameters(such as report uploading time period, center name, phone number and so on) for each dialing center in this section.

Steps:

1. Enter the dialing center configuration page.
   Remote Configuration->Dialing Parameters



2. Check the checkbox to enable report uploading.
3. Enter the report-uploading period (unit: hour). The report-uploading period represents the time interval between uploading the first report and the next report.
4. Enter the first report uploading time interval (unit: minute). The first report uploading time interval represents the time interval between enabling the report uploading function and sending the first report.
5. Select a center type.
6. Enter the center name and phone number.

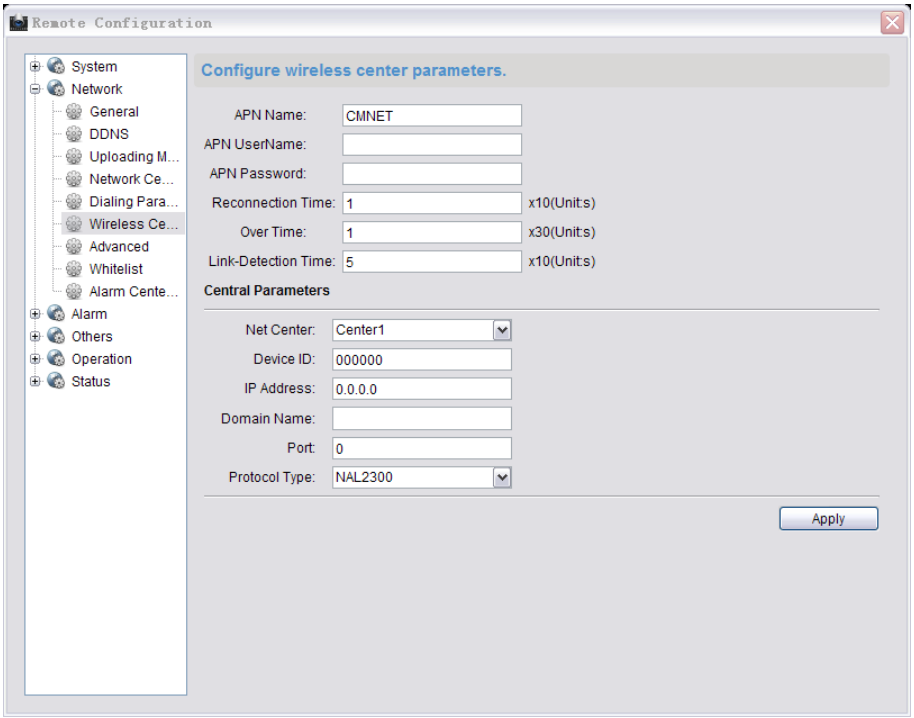
- The maximum length of center name is 32 characters.
- The phone number should be 31 characters and the input mode is
- {No.}{Dwell Time}{EXT No.}. For example, in the number of 000088075998FFF8180, the letter F (which means 2 seconds) represents the dwell time, if the number of the letter F is N, the dwell time is N*F seconds. The number of F is suggested to be more than 3, which means the dwell time should be more than 6 seconds.

7. Enter the dialing times (1~15). The dialing times represents the times that the control panel trying to communicate the alarm receiving center.
8. Select the Pstn protocol.
9. Select the Pstn transmission mode: DTMF5/S and DTMF10/S.
10. Enter the receiver ID which is the authentication account while doing the communication with the alarm receiving center.
11. Click **Apply** to save the settings.

Wireless Center Parameter Settings

Steps:

1. Enter the wireless center parameter settings page.
   Remote Configuration->**Network**->**Wireless Center**



2. Click the dropdown menu to select the net center.
3. Enter the device ID which is applying for displaying in the alarm receiving center.

NOTE

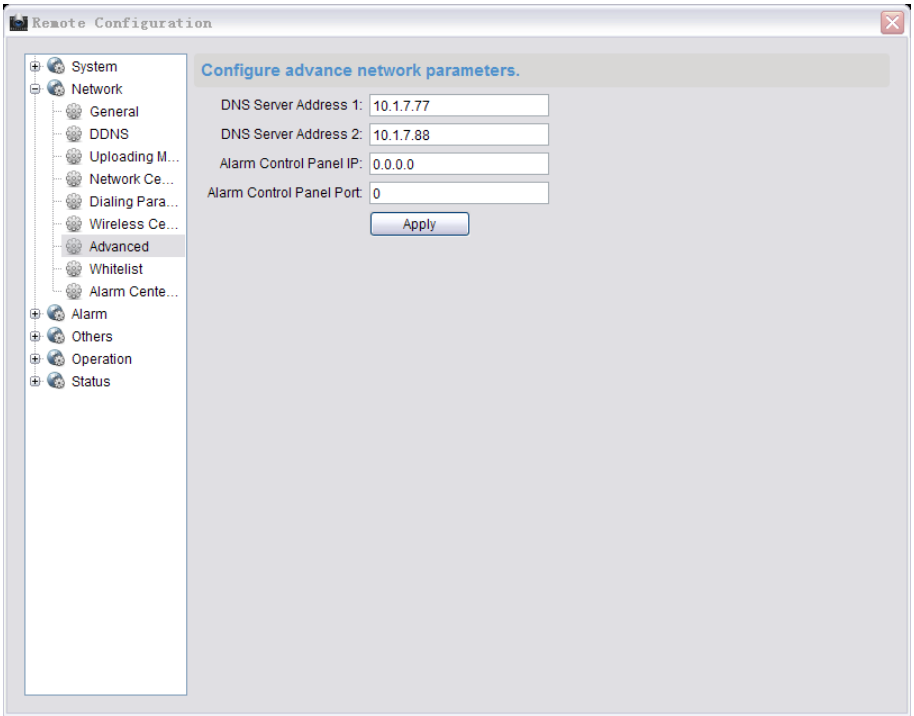
- The length of the username should be 6 characters.
- Only numeric (0~9), and letter (A~F&a~f) are valid for this username.

4. Enter the IP address that is used to communicate with the wireless alarm receiving center.
5. Enter the port No. for communicating with the alarm receiving center.
6. Click the dropdown menu to select the protocol type.
7. Click **Apply** to save the settings.

Advanced Network Parameters Settings

Steps:

1. Enter the advanced network configuration page.
   Remote Configuration->Network->Advanced



2. Enter the corresponding DNS sever address.
3. Enter the IP address and port No. of the control panel.
4. Click **Apply** to save the settings.

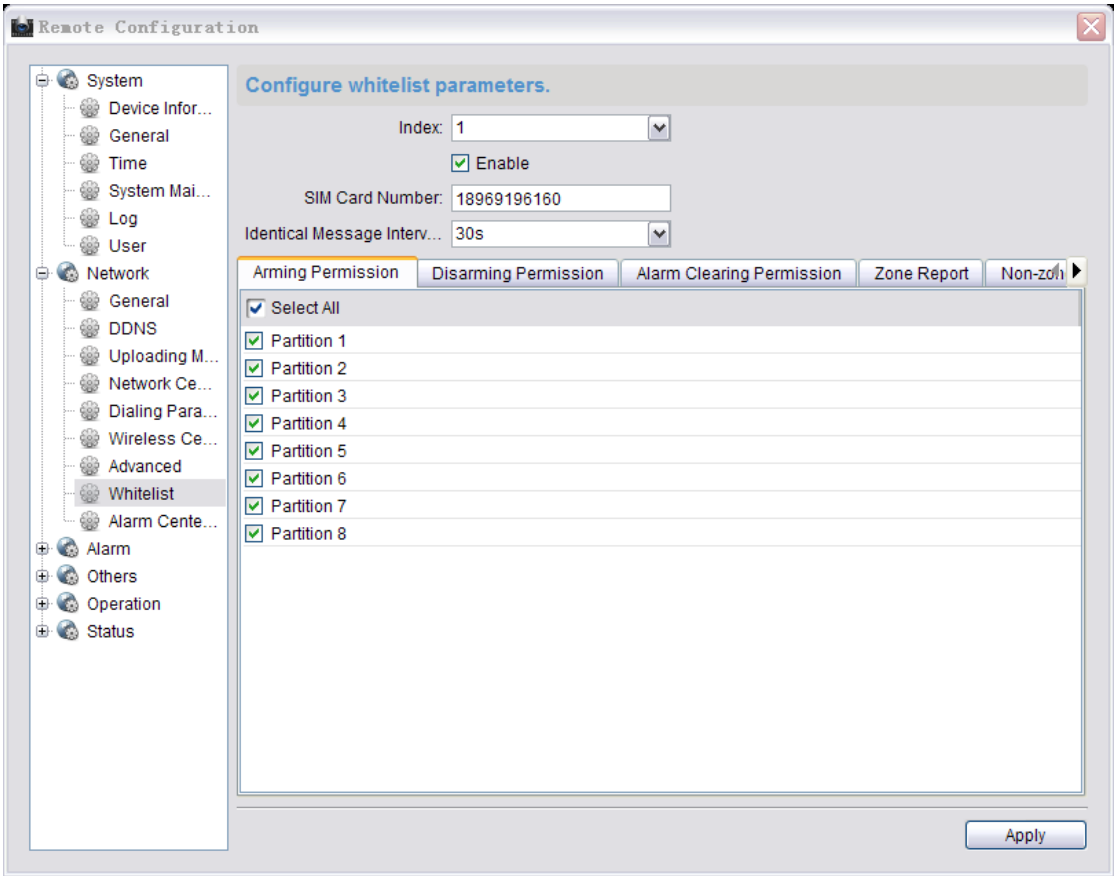
Whitelist Configuration

Purpose:

The whitelist is the list of phone numbers which are authorized to interact with the control panel.

Steps:

1. Enter the whitelist configuration interface.
   Remote Configuration->**Network**->**Configure Whitelist**



2. Select the index of the whitelist.
3. Check the **Enable** checkbox to enable the configuration.
4. Enter the phone number of the whitelist into the SIM Card Number text box.
5. Select the identical message time interval that represents the interval of sending message triggered by the same event.
6. Select the permission of the whitelist on the permission panel.
7. Click **Apply** to save the settings.

4.4.4 Alarm Configuration

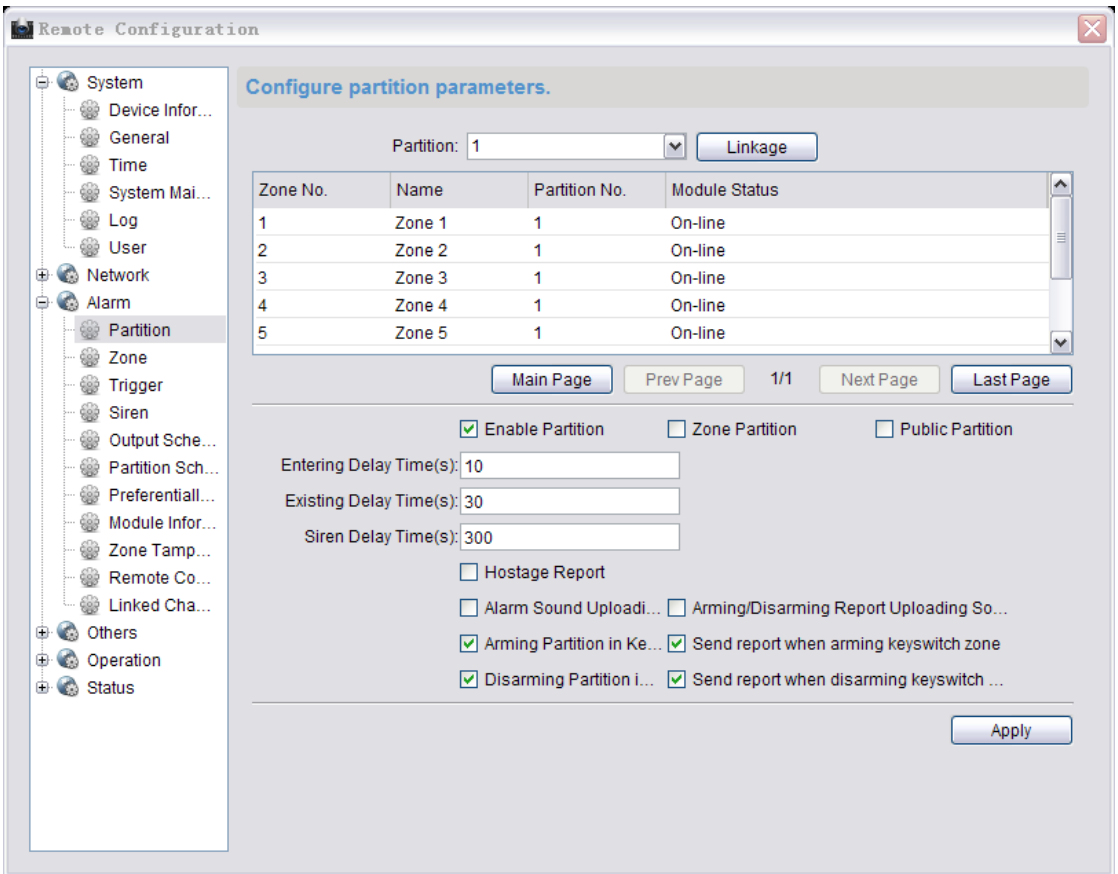
Partition Configuration

Purpose:

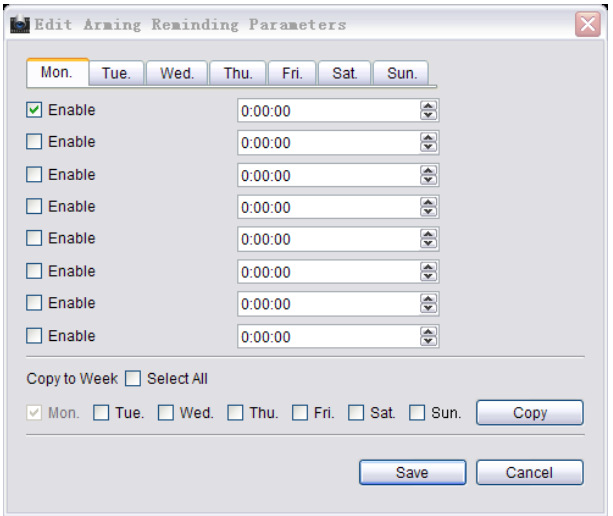
You can configure the detailed alarm parameters of the zone in the partition in this section.

Steps:

1. Enter the partition alarm triggering configuration interface.
   Remote Configuration->Alarm->Partition



2. Click the partition dropdown menu to select a partition.
3. Click the **Linkage** button to add required Zone, keypad, or keypad user to the partition.
4. Check the check box of **Enable Partition** or **Public Partition** to enable functions of the partition or set the system as a public system.
5. Enter the **Entering Delay** and **Existing Delay** duration (unit: second).
6. Enter the siren-delay time (unit: second). The siren-delay time represents the duration of siren ringing when the alarm of the partition is triggered.
7. Click **Edit** to edit the arming schedule. Select the alarm type.

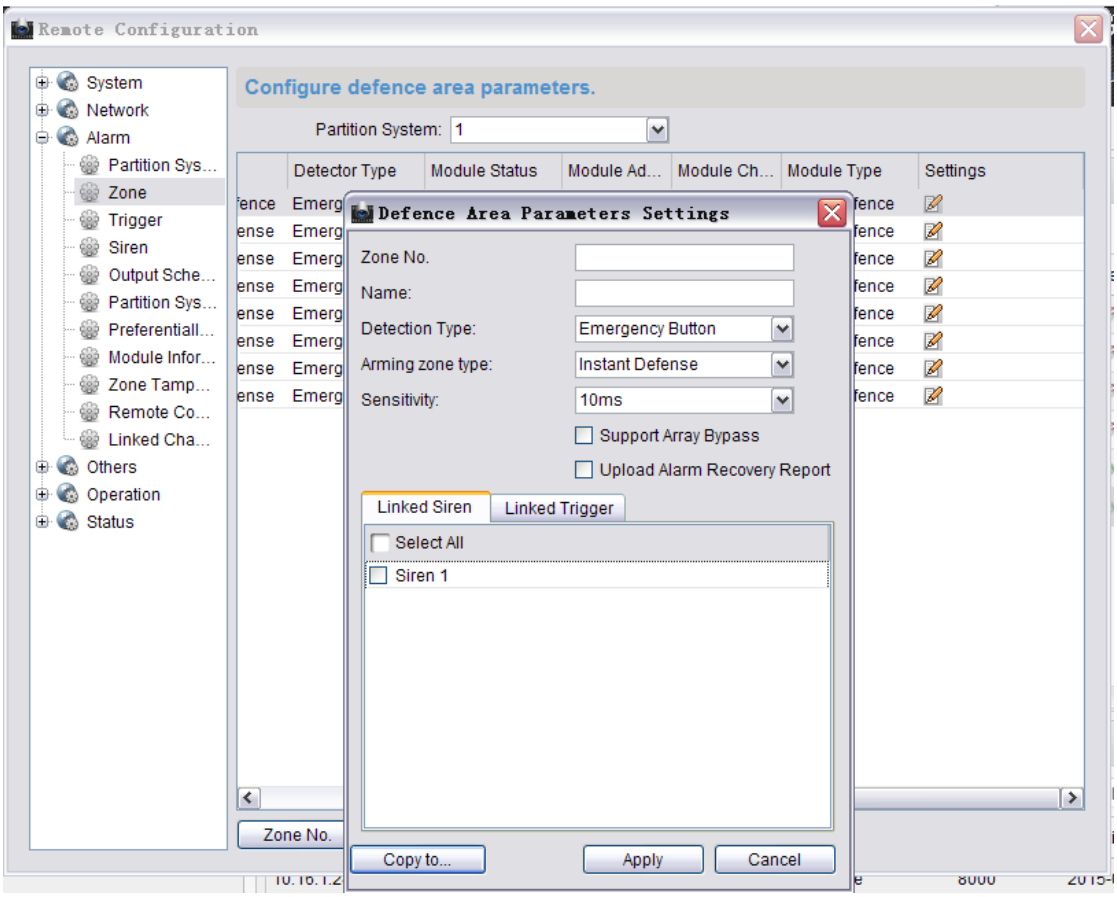


8. Select an alarm type.
   - **Hostage Report**: Enable uploading the hijack report of control panel.
   - **Arming/Disarming Report Uploading Sound**: Enable the prompt sound when uploading the arming/disarming report.
   - **Alarm Sound Uploading Manual Test**: Enable the prompt sound when successfully uploading the manual test report.
   - **Arming Partition in Key switch Zone**: Support the key Zone to arm the current partition
   - **Send Report when Arming Key Switch Zone**: Enable uploading report when the key Zone arms the current partition.
   - **Disarming Partition in Key switch Zone**: Support the key Zone to disarm the current partition
   - **Send Report when Arming Key Switch Zone**: Enable uploading report when the key Zone disarms the current partition.
9. Click **Apply** to save the settings.

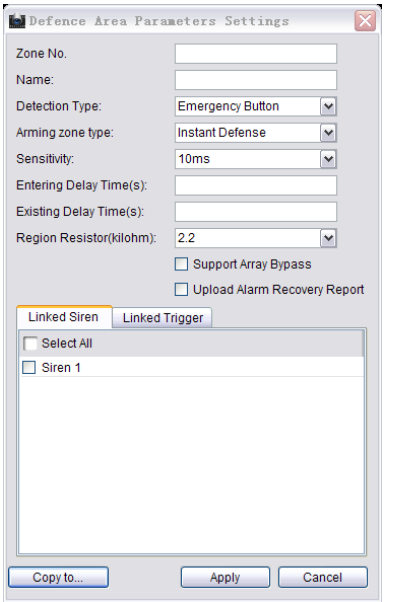
Zone Configuration

Steps:

1. Enter the Zone configuration interface.
   Remote Configuration-> **Alarm**-> **Zone**



2. Click the **Partition** dropdown menu to select a partition.
3. In the Alarm Input list, select an alarm input channel and click the icon to enter Zone configuration page.

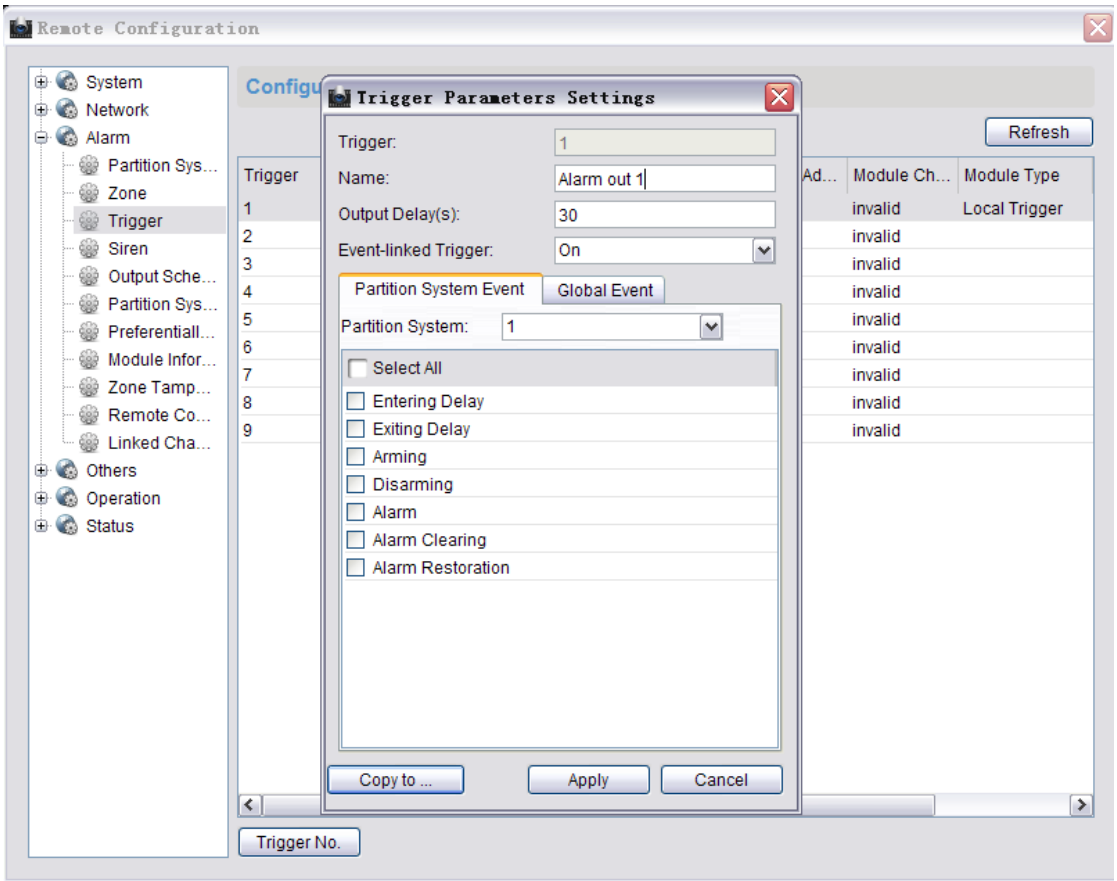


4. Edit the general information of the Zone, including name, probe type, arming Zone type, sensitivity, entering delay, and existing delay and so on.
   Probe Type: Select the type of the detector.
   Arming Zone Type: Select the type of Zone in the partition
   Sensitivity: Select the response time of the Zone.
5. Select the linked siren and linked trigger.
6. Click **Copy to** to copy all these settings to other Zones.
7. Click **Apply** to save the settings.

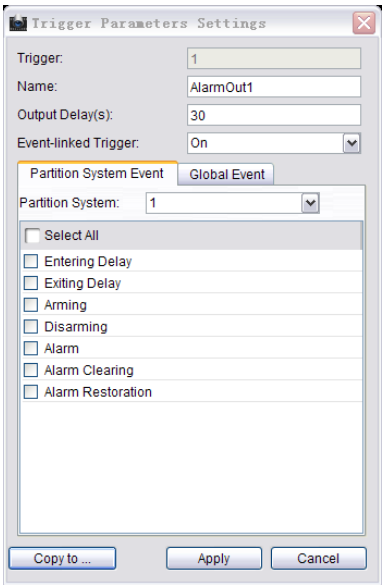
Trigger Configuration

Steps:

1. Enter the Zone configuration interface.
   Remote Configuration-> **Alarm**-> **Trigger**



2. In the Alarm Output list, select an alarm input channel and double click the trigger to enter zone configuration page.

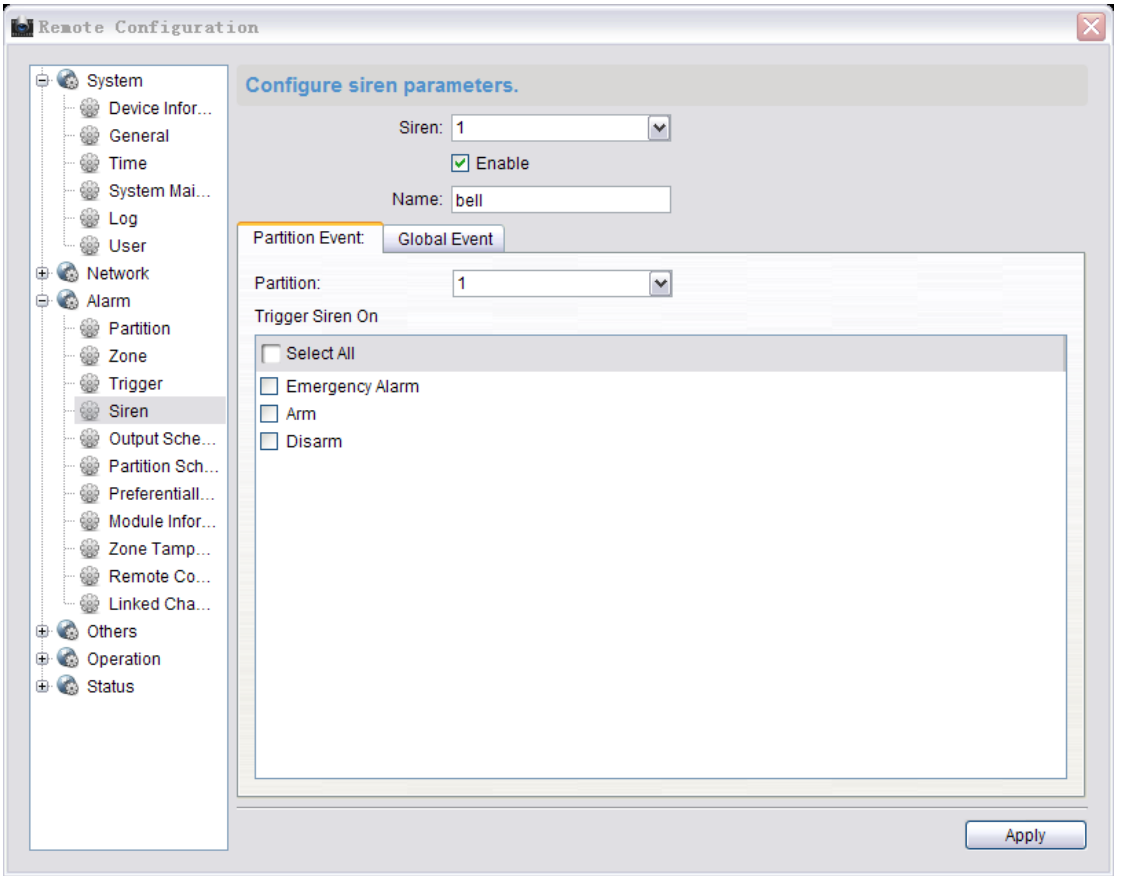


3. Edit the general information of the zone, including name, output delay and so on.
   Output Delay (0~5999s): Configure the alarm output time after the alarm being triggered.
4. Click the dropdown menu to enable/disable the event-linked trigger.
5. Select the detailed operation after the alarm being triggered on the partition event panel.
6. Select the global event of alarm triggering.
7. Click **Copy to** to copy all these settings to other Zones.
8. Click **Apply** to save the settings.

Siren Configuration

Steps:

1. Enter the siren configuration page.
   Remote Configuration->**Alarm**->**Siren**



2. Click the **Siren** dropdown menu to select a siren needs to be configured.
3. Check the **Enable** box to enable the configuration.
4. Edit the siren name.
5. Select the detailed operation after the alarm being triggered on the partition event panel.
6. Select the global event of alarm triggering.
7. Click **Apply** to save the settings.

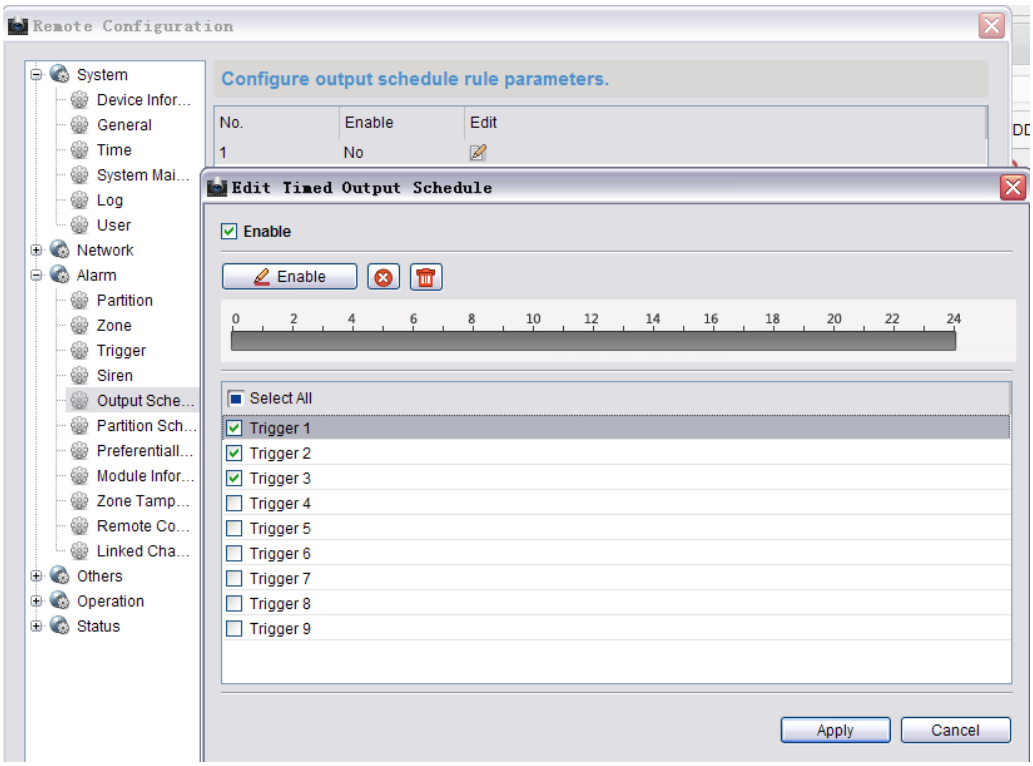
Relay Output Schedule Configuration

Purpose:

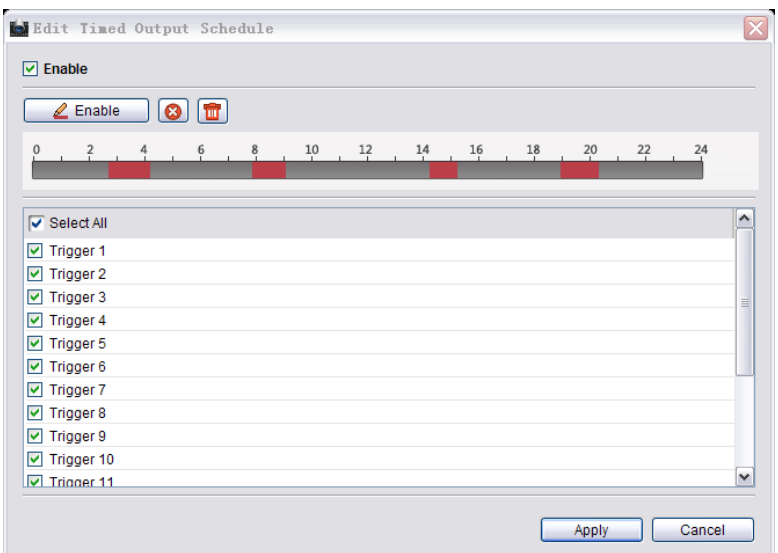
You can set the schedule for turning on/off the relay in this section.

Steps:

1. Enter the relay output schedule configuration interface.
   Remote Configuration->**Alarm**-> **Output Schedule Rule**



2. In the relay list, select an alarm input channel and click the icon to enter the Zone configuration page.

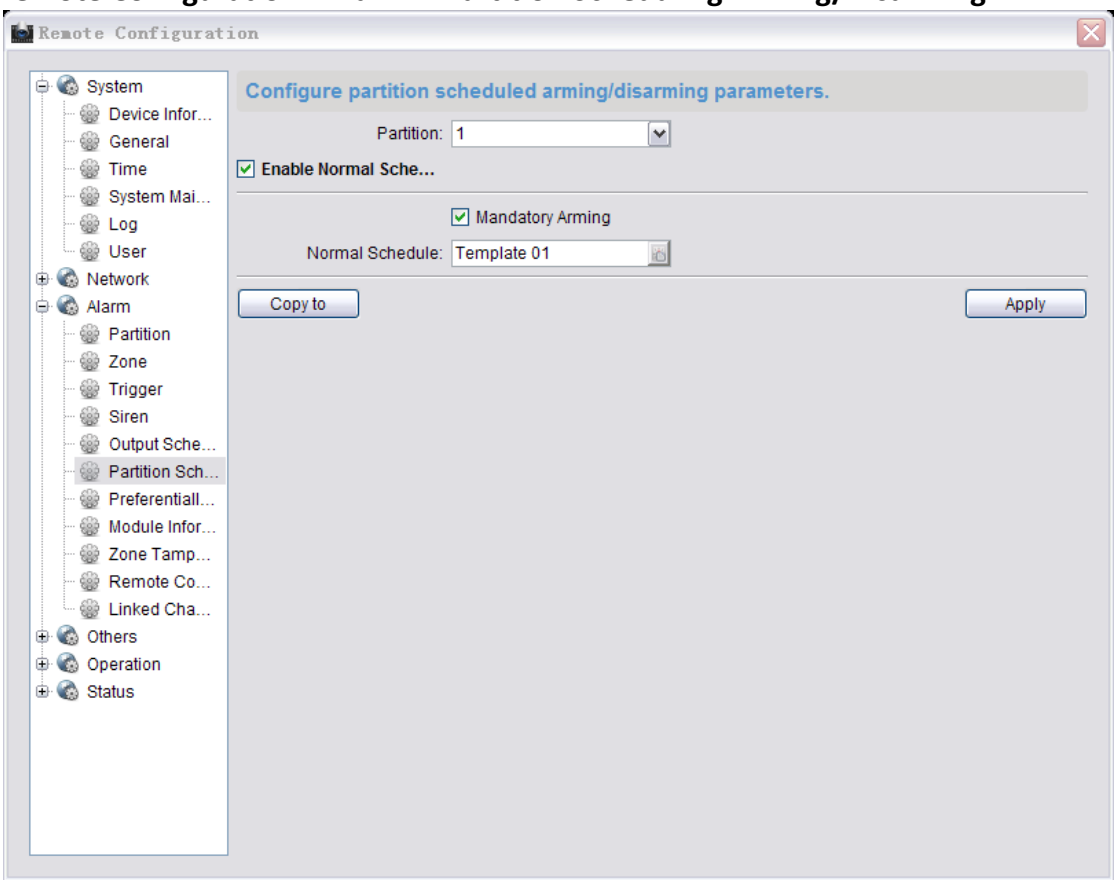


3. Check the **Enable** checkbox to enable the configuration.
4. Click the icon Enable, click and drag the mouse on the time bar (the time bar is divided into 24 segments which represent 24 hours) to draw the required schedule.
   Delete Schedule: click the drawn color bar and click the icon to delete the color bar.
   Clear Schedule: Click the icon to clear the drawn the schedule.
5. Check the **Trigger** checkbox to select the trigger.
6. Click **Apply** to save the settings.

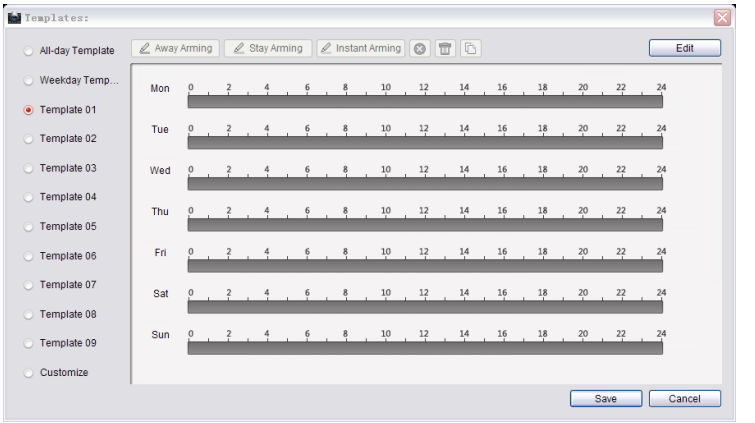
Partition Arming/Disarming Schedule Configuration

Steps:

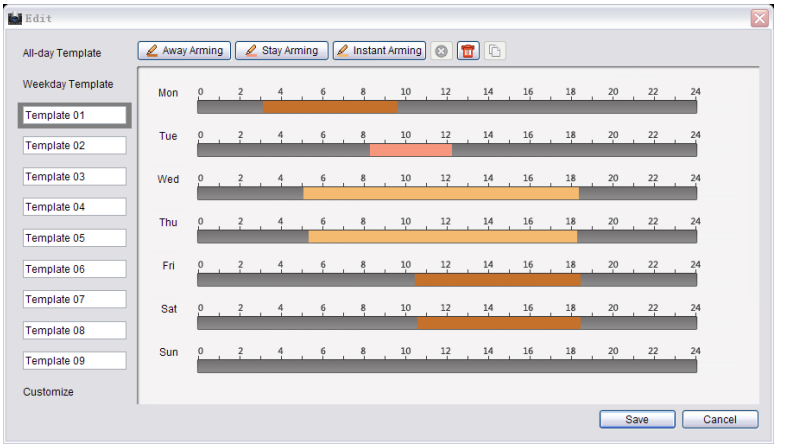
1. Enter the arming/disarming schedule configuration interface.
   Remote Configuration->Alarm ->Partition Scheduling Arming/Disarming



2. Select a partition needs to be configured.
3. Check the **Enable Normal Schedule** checkbox to enable daily schedule for the partition. You can select to enable the mandatory arming function.
4. Click the icon of the **Template** box to enter the schedule configuration interface.



5. Click **Edit** to enable the schedule configuration.
6. Click and select a template.



7. Click the button Away Arming / Stay Arming / Instant Arming to select an arming type.
8. Click and drag the mouse on the time bar to draw the daily schedule.
   Delete Schedule: Click the drawn color bar and click the icon to delete the color bar.
   Clear Schedule: Click the icon to clear the drawn the schedule.

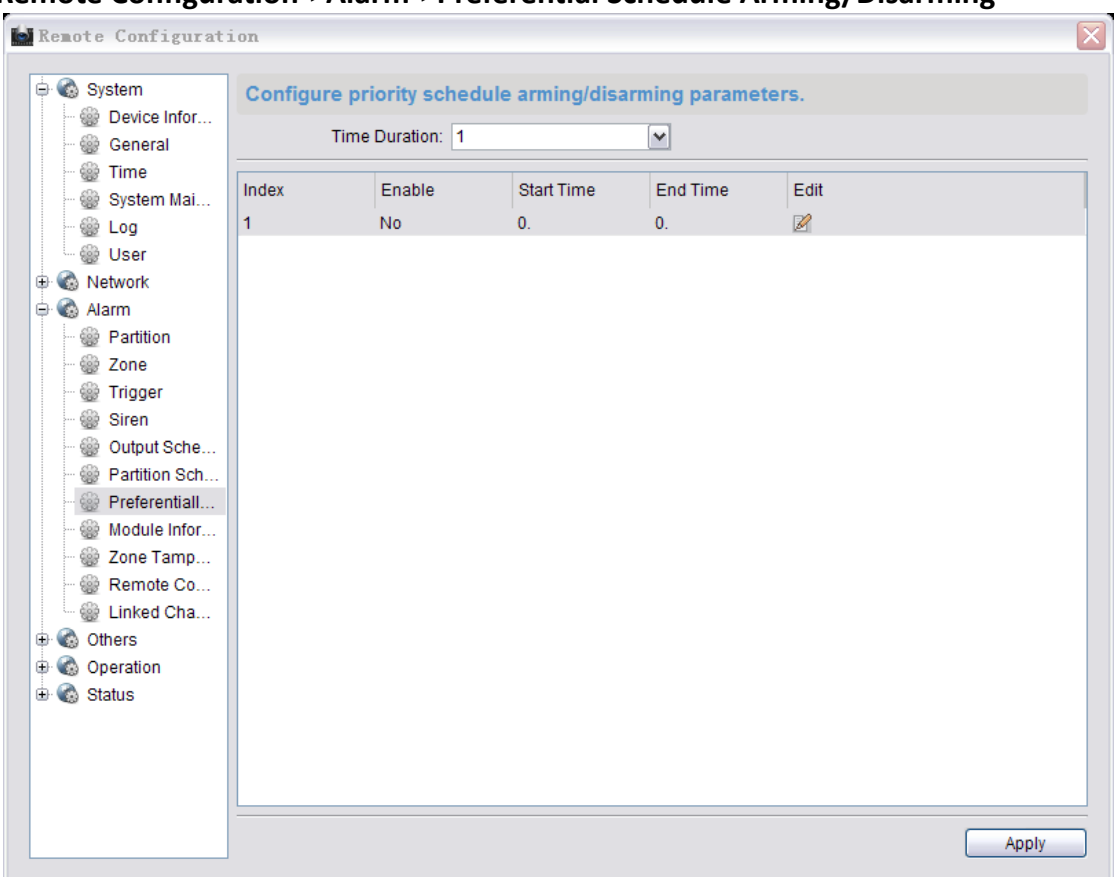
Copy Schedule: Click the drawn color bar and click the icon to copy this arming schedule to other day of the week.

9. Click **Save** to save the settings and click **Cancel** to exit the page.
10. Click **Copy to** to copy all these settings to other Zones.
11. Click **Apply** to save the settings.

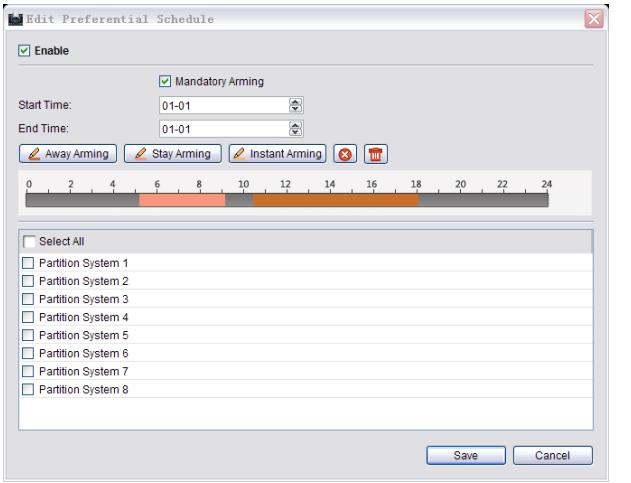
Arming/Disarming Preferential Schedule Configuration

Steps:

1. Enter the arming/disarming preferential schedule configuration interface.
   Remote Configuration->Alarm->Preferential Schedule Arming/Disarming



2. Click the drop down menu to select the time duration.
3. Click the icon to enter the preferential schedule configuration page.



4. Click the button Away Arming / Stay Arming / Instant Arming to select an arming type.
5. Click and drag the mouse on the time bar to draw the daily schedule.
6. Click **Save** to save the settings and click **Cancel** to exit the page.
7. Click **Copy to** to copy all these settings to other Zones.
8. Click **Apply** to save the settings.

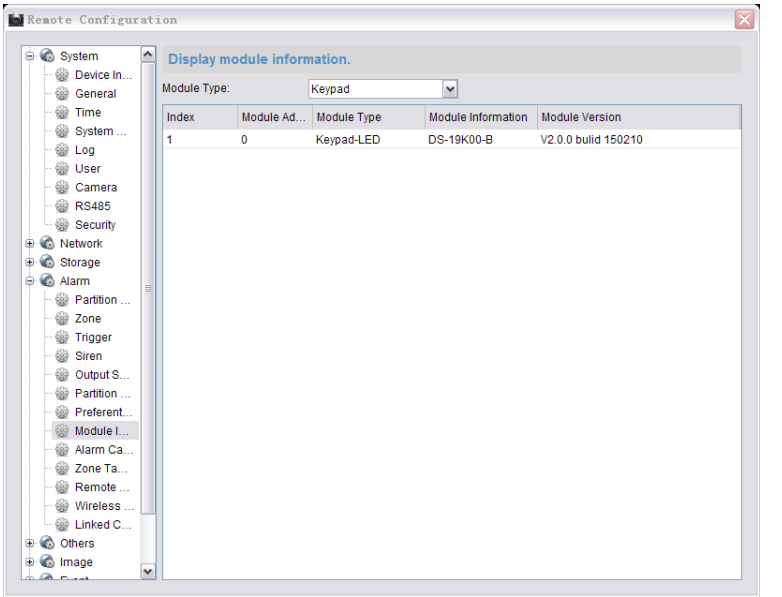
Module Information

Purpose:

You can view the information of external keypad and trigger in this section.

Steps:

1. Enter the module information interface.
   Remote Configuration->Alarm->Module Information

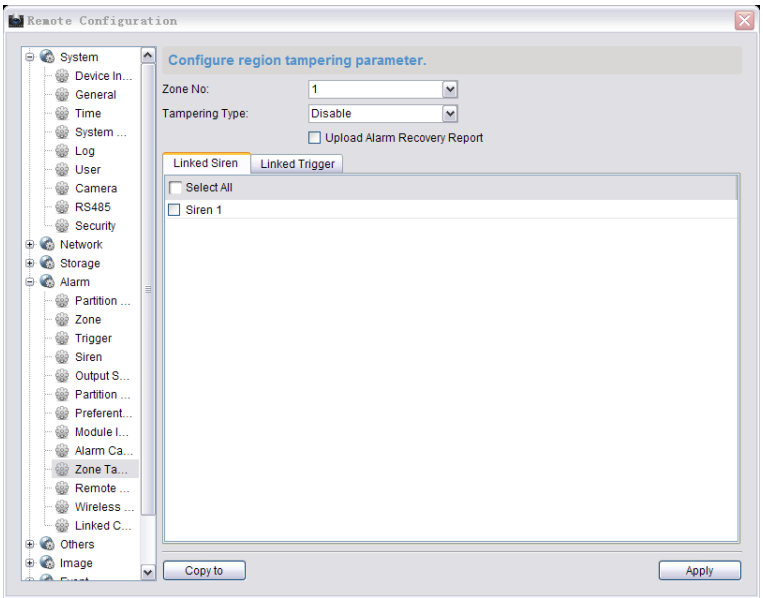


2. Click and select the external device from the module type dropdown menu.
3. View the information about the selected device.

Zone Tampering-proof Configuration

Steps:

1. Enter the Zone tampering configuration interface.
   Remote Configuration->Alarm->Zone Tampering Proof

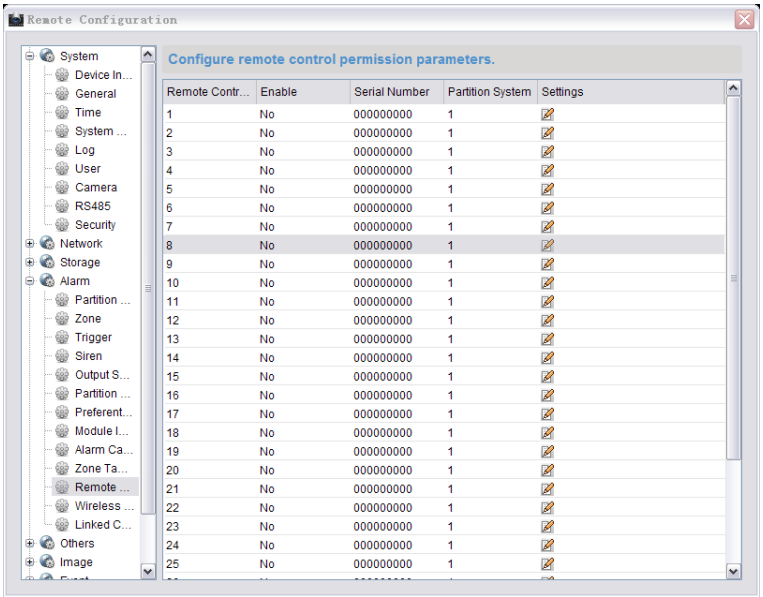


2. Click dropdown menu to select a Zone needs to be configured.
3. Select a tampering type.
4. Check the **Upload Alarm Recovery Report** checkbox to enable the function of uploading alarm recovery report.
5. Select the linked siren on the **Linked Siren** panel.
6. Select the linked trigger on the **Linked Trigger** panel.
7. Click **Copy to** to copy all these settings to other Zones.
8. Click **Apply** to save the settings.

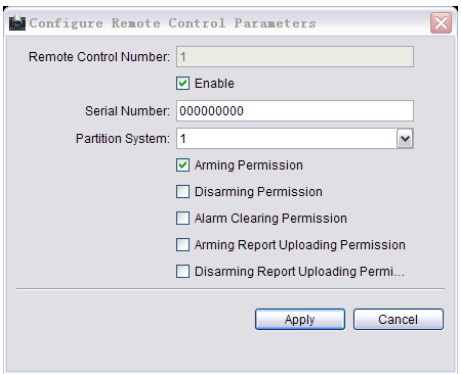
Remote Control Permission Configuration

Steps:

1. Enter the remote control permission configuration interface.
   Remote Configuration->**Alarm**->**Remote Control Permission**



2. Click the icon to enter the remote control permission configuration page.



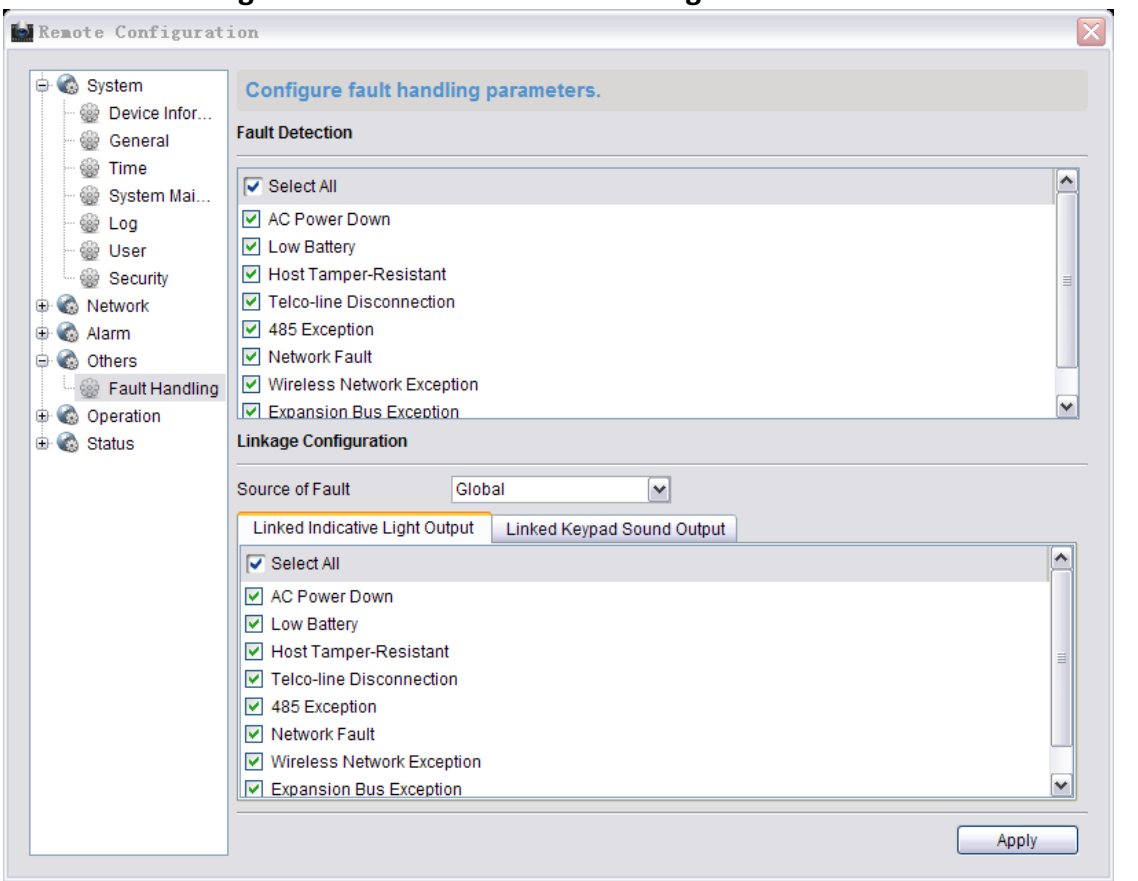
3. Check the **Enable** checkbox to enable the configuration
4. Enter the serial number of the remote control.
5. Select the partition No. needs to be controlled.
6. Check the checkbox and select the permission for the remote control.
7. Click **Apply** to save the settings.

4.5 Fault Handling

In this section , you can select the fault detection type, alarm linked keypad and output mode.

Steps:

1. Enter the fault handling interface.
   Remote Configuration->Others->Fault Handling



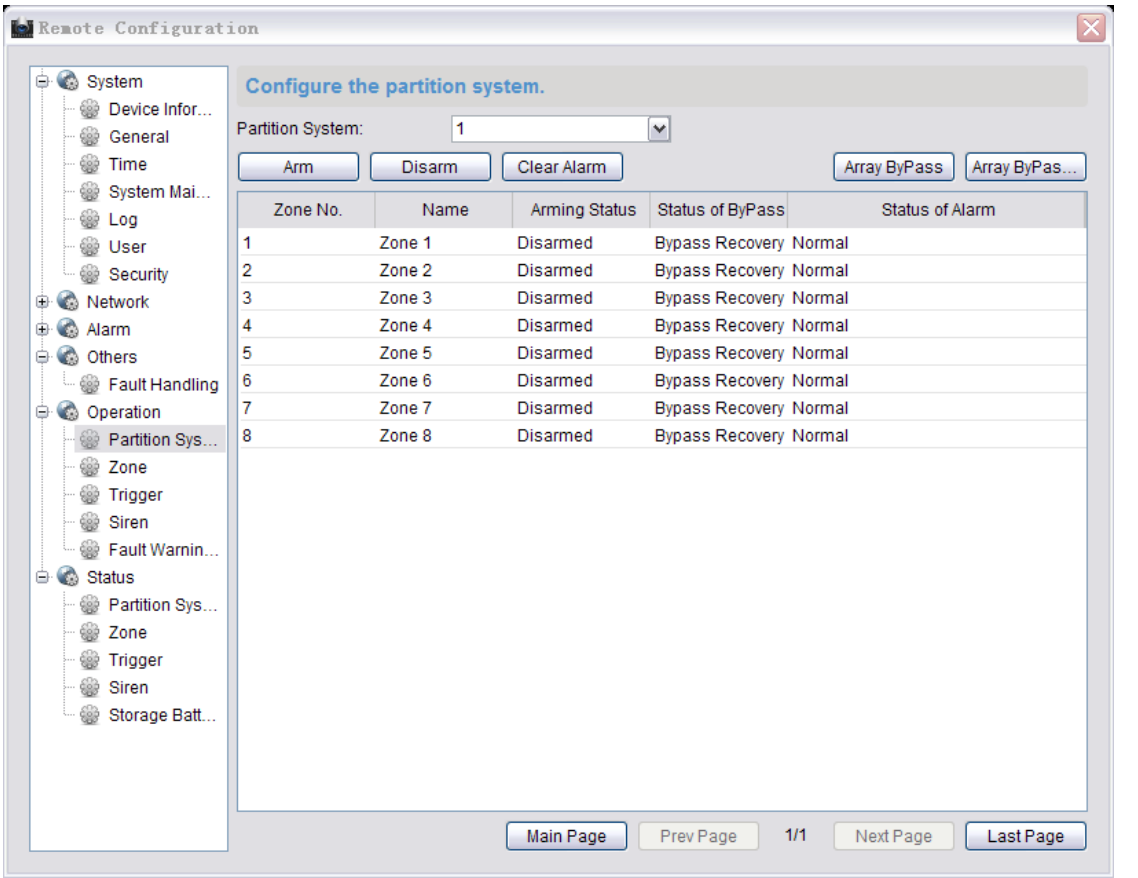
2. Select the fault detection type.
3. Click the **Source of Fault** dropdown menu to select the linked keypad.
4. Select the alarm output mode and corresponded fault detection type. The alarm output mode can be selected as **Linked Indicative Light** and **Linked Keypad Sound**.
5. Click **Apply** to save the settings.

4.6 Operation

You can configure the partition, zone, trigger, siren, and fault warning audio in this section.

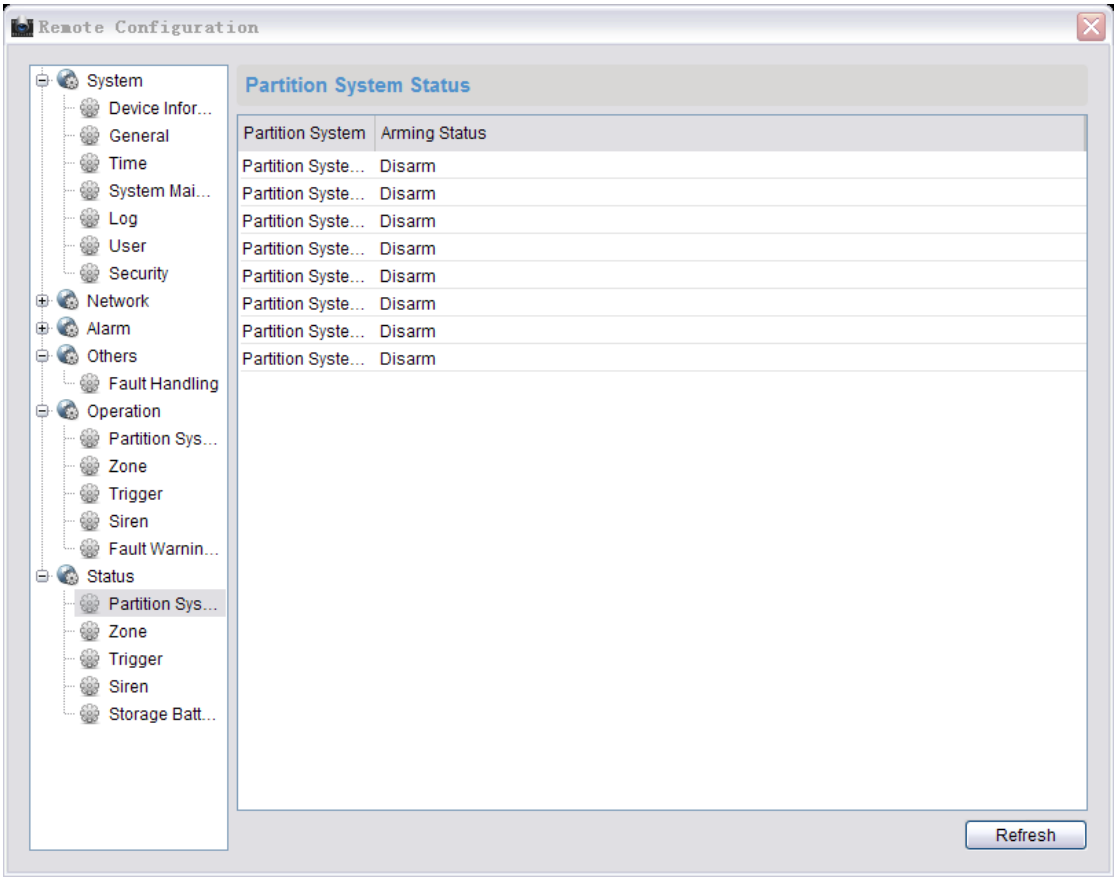
Click **Remote Configuration->Operation** to enter the interface.

Partition: you can arm/disarm the partition, clear alarm, bypass, and recover bypass of the system.
Zone: you can bypass or recover bypass of the selected zone.
Tigger: you can select to turn on/off the selected trigger.
Siren: you can enable/disable the specified siren.
Fault Warning Audio: you can select the faulted keypad and select to disable the warning audio.



4.7 Status

You can view status of the partition, zone, trigger, siren ,and storage battery in this section.


Remote Configuration
System
Device Infor...
General
Time
System Mai...
Log
User
Security
Network
Alarm
Others
Fault Handling
Operation
Partition Sys...
Zone
Trigger
Siren
Fault Warnin...
Status
Partition Sys...
Zone
Trigger
Siren
Storage Batt...
Partition System Status
Partition System
Arming Status
Partition Syste... Disarm
Partition Syste... Disarm
Partition Syste... Disarm
Partition Syste... Disarm
Partition Syste... Disarm
Partition Syste... Disarm
Partition Syste... Disarm
Partition Syste... Disarm
Refresh

Chapter 5 Trouble Shooting

Q: What is the function of Project button  of LCD keypad?

A: Project button  has button switch function besides normal instruction button, such as:

When sensor or module is abnormal, press and hold the **Project** button to switch to other interfaces manually. When the sensor/module is abnormal or the keypad, press the **Project** button once and the current display interface will be paused for 20s; press it again to switch to the next LCD screen interface.

Q: How to manually switch to other abnormal interfaces when the LCD keypad displays sensor/module is abnormal?

A:

1. Among the LCD keypad abnormal display interfaces, display interface of the sensor alarm, module abnormal display interface are of first priority; the sensor abnormal interface is of second priority, sensor bypass interface is of third priority.
2. If interfaces of different priority exist at same time, the system automatically displays the interface of first priority.
3. The switch between interfaces of same priority: there are two ways to switch display interface of the sensor alarm to sensor off-line display interface.
    1) System auto-switch: The system will refresh automatically. If the current display interface is accomplished and other interfaces of same priority exist, system will auto switch to other interfaces.
    2) Manually switch: Press the **Project** button continuously until it switches to the interface to display.
4. Switch between interfaces of different priority: from sensor alarm interface to sensor bypass interface:
   Press and hold the **Project** button for multiple times until it switches to the interface to display.

Q: What is the meaning of LCD keypad Arm/Disarm, Operate indicators?

A: LCD system keypad indicator:

1. The meaning of Arm/Disarm indicator (Red and Green) is shown below:

Working Status	Indicator Status	Working Status	Indicator Status
Enter programming	Green, Blink	Parameters Initialization	Green, Blink
System Arming	Red, Normally On	System Disarming	Green, Normally On

2. The meaning of Operate indicator (Green) is shown below:

Working Status	Indicator Status	Working Status	Indicator Status
Enter programming	Green, Blink	Parameters Initialization	Green, Blink
System Abnormal	Green, Blink	System Normal	Green, Normally On

Q: What are the steps of LED keypad to program the control panel？

A：

1. In overall keypad programming mode, the program command is: {installer password} + {*} + {0} + {#};
2. To view the configuring operation for alarm control panel, please refer to alarm keypad configuring code;
   For example: program user password 2#, the password has arm/disarm function, does not send arming report, does not allow bypass, password is 5678, and the program code is shown as follow:

Command Code	Arming Type	Password	End
{0}{0}{2}	**{3}**	**{5}{6}{7}{8}**	**{#}**

3. Set program command
   There are 2 alert sound of correct or 5 alert sound of error and corresponding OSD notices after each program command is over. When 5 alert sound of error is heard and the screen displays **Operation Failed**, there is error in program command setting and the user need to reset correct program command. When 2 alert sound of correct is heard and the screen displays **Operation Succeeded** but the setting parameters are not the

parameters needed, you can operate according to program command once again.

4. Exit program mode, the program command is: {*} + {#}.

Q: What is the meaning of LED keypad Arm/Disarm, Operate, Camera indicators?

A:

LED alarm keypad **Arm/Disarm** indicator:

Working Status	Indicator Status	Working Status	Indicator Status
Armed	Red, Normally On	Enter Programming	Green, Blink
Disarmed	Green, Normally On	Main Operator Change Password	Green, Blink

LED alarm keypad **Operate** indicator:

Working Status	Indicator Status	Working Status	Indicator Status
Normal	Green, Normally On	Keypad Not Logged In	Red, Blink
System Error	Orange, Blink	Enter Programming	Green, Blink
Project	Red, Normally On	Change Password	Green. Blink

LED alarm keypad **Camera** indicator:

Working Status	Indicator Status	Working Status	Indicator Status
Sensor Normal	Off	Sensor Error	Red, Normally On
Sensor Alarm	Red, Blink	Sensor Bypass	Green, Normally On

LED keypad **Camera** indicator under **Project Mode**:

No.	Description	No.	Description
1	Off-hook	**5**	Send CID Report
2	Dial	**6**	Receive Alert Sound
3	Alarm Connecter	**7**	Control Panel Off-hook

	Disconnection		
4	Receive the Hand-shack Sound	**8**	Alarm Connector On-hook

LED keypad **Camera** indicator under **Status Mode**:

No.	Description	No.	Description
1	AC Power off	**5**	Keypad Off-line
2	Battery Low Voltage	**6**	Network Cable Off-line
3	Control Panel Tamper-proof On	**7**	No SIM Card
4	ADSL Cable Off-line	**8**	Reserved

Q: What is the meaning of LED keypad alert sound?

A: The meaning of LED keypad alert sound is as follows:

No.	Keypad Alert Sound	Description
1	1 Sound	Keypad Prompt, Error Operating Prompt
2	2 Sound	Correctly answered, report uploading succeeded
3	5 Sound	Incorrectly answered, report uploading failed in 60s
4	Last for 2s	Error Prompt
5	Intermittent Slow Sound, Continuously	Enter/Exit Delay
6	Intermittent Rapid Sound, Continuously	Enter/Exit Delay, 10s Left
7	Rapid Beep	Sensor Alarm, Keypad not logged in
8	3 Long 2 Short	Keypad Tamper-proof On

Q: How to remove alarm memory?

A: There are two situations of removing alarm memory as shown below:

1) Under disarming mode: Press {*} + {1} + {#} or {Password} + {*} + {1} + {#}.
2) Under arming mode: Press {Password} + {*} + {1} + {#}.

Q: How to input hexadecimal number?

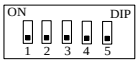
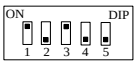
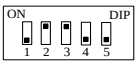
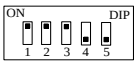
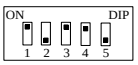
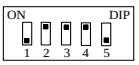
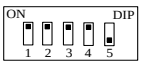
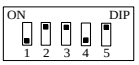
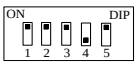
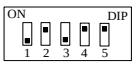
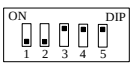
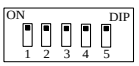
A: Input hexadecimal number with {*} button and number button {0} ~ {5}.

Conversion Table

Hexadecimal Number	Corresponding Key
A	*0
B	*1
C	*2
D	*3
E	*4
F	*5

Q: How to set LED keypad address?

A: Set LED keypad address with the DIP address of keypad.

DIP	Add.	DIP	Add.	DIP	Add.	DIP	Add.
	0		1		2		3
	4		5		6		7
	8		9		10		11
	12		13		14		15
	16		17		18		19
	20		21		22		23
	24		25		26		27
	28		29		30		31

Q: Why is it needed to input E at the end of keypad configured phone number?

A: Control panel can process phone number with 31 characters. Input number with 16 characters in each command address so that 2 addresses are needed for storage phone number. However, the phone numbers are different in every place so the control panel needs a special data bit to check if the phone number is complete. Character E ({*} {4}) is for checking if the phone number is complete.

For example: The first Alarm connecter phone number is 0571-88075998, user can input the following command:

Command Address 460

0	5	7	1	8	8	0	7	5	9	9	8	E			

For example: The first alarm connecter phone number is 17951-88075998**, user can input the following command:**

Command Address 460

1	7	9	5	1	F	F	F	8	8	0	7	5	9	9	8

Command Address 461

E															

For example: The first alarm connecter phone number is 0571-88075998-8888**, user can input the following command:**

Command Address 460

0	5	7	1	8	8	0	7	5	9	9	8	F	F	F	8

Command Address 461

8	8	8	E												

Q: What are notes for setting password?

A: The password for each operator should be different; otherwise the setting will be failed. For example, if the password of operator 1 is set to be 1234 hen password of operator 2 is also 1234, it will prompt to be error. In addition, the password of each operator should be different from the control panel age code of other operators; otherwise the setting will be failed. For example if the password of operator No.3 is 3456 and the password of operator No.4 is set to be3455 or 3457, it will prompt to be error.

Q: What are notes for setting duress code?

A:

1. The description of duress code is as follow:
   Input duress code when the user is under duress, it will work as if the user inputs valid password, but the system will auto-upload the alarm information. For example when a criminal forces the user to disarm the alarm, user can input the control panel age code to disarm the system and upload the alarm information to the center automatically and off the criminal's guard.
2. Please note when setting duress code: duress code is the valid password with its last number±1.
   For example: Valid Password: 1234, Duress Code: 1235 and 1233.
   For example: Valid Password: 1230, Duress Code: 1231 and 1239.

For example: Valid Password: 1239, Duress Code: 1230 and 1238.

3. Please take the following notes while using duress code:
   While using duress code, it is needed to enable duress report firstly, as to program the control panel age report and delay. The programming command to enable **Control Panel Hijack Report** is as follow:

Command Address	**{**4**}{**6**}{**4**}**
Enter Delay	**{**3**}**
Exit Delay	**{**6**}**
Siren Working Duration	**{**2**}**
Control Panel Hijack Report	**{1}**
End	**{#}**

Q: How to solve the problem of two LED keypad address being same?

A: When two LED keypad addresses are the same, the situation of two keypads demanding bus communication at the same time will appear and cause conflict. The only solution is to remove one keypad and reset the other keypad to an unused legal address. Restore the control panel by processing program code ({Main Operator}{*}{6}{8}{#})

Q: Why there is no Disarming Report?

A: To make sure the user has permission of **Disarming Report, please refer to** Operator Configuration.

Q: What to do if the user cannot disarm after arming the system?

A: There are two different situations:

1. The user does not have permission to disarm, please contact the administrator.
2. Take the follow instructions when there is only one user in the system without permission to disarm;
   1) Initialize the hardware, restore the password of operator, main operator password and permission, and then disarm with main operator. The initialization password of operator is: 012345, the initialization password of main operator is: 1234, the permission is: arm/disarm. There is arm/disarm report and bypass is permitted. Please refer to FAQ of hardware initialization for more information about hardware initialization.
   2) The command code to restore factory parameters: {Password of operator}

+ {*} + {8} + {9} + {#}.

This method is not recommended because it will initialize all programming contents.

Q: How to do the hardware initialization?

A: Control panel hardware initialization only initializes operator password: 012345 and main operator password: 1234, main operator permission is arm/disarm. There are arming/disarming report and allows bypass.

Steps:

1) Power off the control panel and open the cover;
2) Short the restore switch of the control panel with shorting nut or connection cables;
3) Power on the control panel and power off it 10s later;
4) Please remove the shorting nut or connection cable on the restore switch;
5) Cover the control panel well;
6) Recharge the control panel;

Q: Why is there no response for keypad operational order but alert sound of error 10s later?

A: It may be caused by follow situations:

1) Poor contact of the connection cable between LED keypad and the control panel, please check if the cable is normal;
2) The LED keypad is considered as off-line in the communication. If there is other keypad operates normal, process program command {Main Operator Password} + {*} + {6} + {8} + {#}to restore it or power off the control panel and reboot.

Q: How does the control panel detect alternating current, storage battery, control panel tamper-proof and ADSL cable?

A: The status of the control panel detection is as follows:

1) The control panel detects AC power supply status once in a while;
2) The control panel detects storage battery status once in a while;
3) The control panel detects tamper-proof status once in a while;
4) The control panel detects ADSL cable status once in a while.

Q: The network is disconnected.

A:

1) Please check if the network status indicator of the board is normal on;
2) If the network status indicator is not normal on, please check if the network cable connection is normal.

Q: What if the client cannot log in the device?

A: Troubleshoot according to the prompt.

Please check if the device IP Address and Port No. are correct. The device default IP Address is: 192.0.0.64, and the Port No. is: 8000.

Please check if the user name and password to log in the control panel are correct. The default user name is: admin, the word is: 12345.

Q: Why the control panel cannot communicate with the alarm center group?

A: The configuration of control panel communicating with the alarm center group is as follows:

1) If the user communicates with the center via LAN: Configure parameters such as monitoring IP, Port No., User Account and Communication Protocols of the remote alarm center in **Remote Configuration**-> **Others**-> **Network Center Configuration**;
2) If the user communicates via dialing: Configure parameters such as phone number, receiver identity account and communication protocols of the remote alarm center in **Remote Configuration**-> **Others**-> **Dialing Parameter Setting**;
3) If the user communicates via WIFI: Configure APN Name and Parameters of remote alarm center in **Remote Configuration**-> **Others**-> **WIFI Parameter Setting**. The parameters include monitoring IP, Port No., User Account and Communication Protocol, etc.;
4) After setting dialing parameters, LAN parameters and WIFI parameters, configure the uploading mode in **Remote Configuration**-> **Uploading Mode Configuration**

Q: How to configure the communication way of control panel and alarm center group?

A:

1. Center uploading mode supports at most 6 center groups, each center group divides in main channel and 3 backup channels;
2. If the center group is enabled. Enable the center group before the use.
3. For example: The control panel needs to upload report to network alarm center 1 and dialing alarm center1 and network alarm center 1 needs to upload report to network alarm center 2 when it fails to upload it. The configurations are as follows:
   1) Enable Group1 and Group2;
   2) In the uploading mode configuration list, select N1 in center group 1 main channel, select N2 in backup channel 1, select T1 in Center group2 main channel.
   3) Click **Apply**.

   If the client is not opened, the user can realize communication with alarm center by programming with keypad. For detailed operations please refer to program command 611~634.

Q: Why cannot it upload report and control after WIFI is enabled?

A: The follow situations may lead to WIWI connection failure:

1) No SIM Card or poor contact;
2) 3G module antenna is not normally connected or with poor signal;
3) WIFI parameter setting is incorrect;
4) SIM Card has no enough tariffs.

Appendix1：Specifications

Model		DS-19A08-F/Kx	DS-19A08-F/KxG
Security control panel Parameters	Alarm Input	8 Zones Alarm Input	
	Alarm Output	Local 1-ch+8-ch expandable, 1A/30VDC	
	Siren Power Supply	DC12V/300mA	
	Telephone Line	1-ch PSTN	
	Keypad	K1: LED Keypad; K2: LCD Keypad	
	Supported Keypads (LCD/LED)	8	
	Tamper-proof Switch	Support Tamper-proof and Movement Prevention Function of Security control panel	
	Timed Arm/Disarm	8 Time Periods Each Day	
	Partition	8 Partitions, 1 Public Partition	
	Sensor Tamper-proof Alarm	Support	
	Message Alarm	N/A	Support
	Message Arm/disarm	N/A	Support
	Supported Remote Controllers	32 (Unobstructed Effective Range of 100m)	
Wireless Network Parameters	Wireless Interface	N/A	1, Support Alarming Report Upload
	Wireless Network Standard		GPRS
	UIM Card Slot		1
	SMA Antenna Interface		1
Network Management	Network Protocol	SADP (Search IP Address Automatically), DHCP (Obtain IP address Automatically) etc.	
External Interface	Network Interface	1 RJ45 10M/100M Self-adaptive	
	Keypad Bus	1, RS485 Half-duplex	
	Port for Storage Battery	1 Port, for Storage Battery Accessing	
Others	Power Supply	DC14.3V/1.7A	
	Consumption (Without HDD and Power Supply for External Device)	2W	3W
	Working Temperature	-10°C~+55°C	
	Working Humidity	10%~90%	
	Mounting	Wall-mounted	
	Dimensions	170×125×29mm	
	Weight	≤ 0.32kg	

Appendix2：CID Report

CID Code	Description	CID Code	Description
1103	Real-time Zone Alarm	3103	Real-time Zone Alarm Recovery
1110	Fire Zone Alarm	3110	Fire Zone Alarm Recovery
1122	24-hour Non-voiced Zone Alarm	3122	24-hour Non-voiced Zone Alarm Recovery
1123	24-hour Voiced Zone Alarm	3123	24-hour Voiced Zone Alarm Recovery
1131	Perimeter Zone Alarm	3131	Perimeter Zone Alarm Recovery
1132	Internal Delay Zone Alarm	3132	Internal Delay Zone Alarm Recovery
1134	Delay Zone Alarm	3134	Delay Zone Alarm Recovery
1137	Tampering Alarm	3137	Tampering Alarm Recovery
1301	AC Power Down	3301	AC Power Down Recovery
1302	Low Battery	3302	Low Battery Recovery
1305	Control Panel Restoring	1121	Control Panel Age
1336	Printer Disconnection	3336	Printer Disconnection Recovery
1354	Phone Line Disconnection	3354	Phone Line Disconnection Recovery
1382	Local Expanded	3382	Local Expanded Zone

CID Code	Description	CID Code	Description
	Zone Fault		Recovery
1401	Disarming	3401	Arming
1406	Alarm Clearing Memory Canceling	1810	Soft Zone Emergency Alarm
1570	Zone Bypass	3570	Zone Bypass Recovery
1574	Group Bypass	3574	Group Bypass Recovery
1601	Manual Testing Report	1602	Regular Testing Report
1627	Programming Entering	1628	Programming Exiting
1910	Keypad Disconnection	3910	Keypad Disconnection Recovery
1911	Keypad Bus Trigger Disconnection	3911	Keypad Bus Trigger Disconnection Recovery
1921	Wireless Network Exception	3921	Wireless Network Recovery
1931	Wired Network Exception	3931	Wired Network Recovery
1930	IP Address Conflict	3930	IP Address Recovery
1931	Network Cable Disconnection	3931	Network Cable Recovery
1940	Motion Detection Enabling	3940	Motion Detection Disabling
1941	Tampering Alarm Enabling	3941	Tampering Alarm Disabling
1942	Video Loss Alarm	3942	Video Loss Alarm

CID Code	Description	CID Code	Description
	Enabling		Disabling
1943	Unmatched Input/ Output Format	3943	Input/ Output Format Recovery
1944	Video Input Exception	3944	Video Input Recovery
1945	HDD Full Alarm	3945	HDD Recovery (For HDD Full)
1946	HDD Fault Alarm	3946	HDD Recovery (For HDD Fault)
3408	Real-time Arming	3441	Stay Arming

Appendix3：LED Keypad Prompt Sound

No.	Keypad Prompt Sound	Description
1	1 Sound	Keypad Prompt, Error Operating Prompt
2	2 Sound	Correctly answered, report uploading succeeded
3	5 Sound	Incorrectly answered, report uploading failed in 60s
4	Last for 2s	Error Prompt
5	Intermittent Slow Sound, Continuously	Enter/Exit Delay
6	Intermittent Rapid Sound, Continuously	Enter/Exit Delay, 10s Left
7	Rapid Beep	Sensor Alarm, Keypad not logged in
8	3 Long 2 Short	Keypad Tamper-proof On

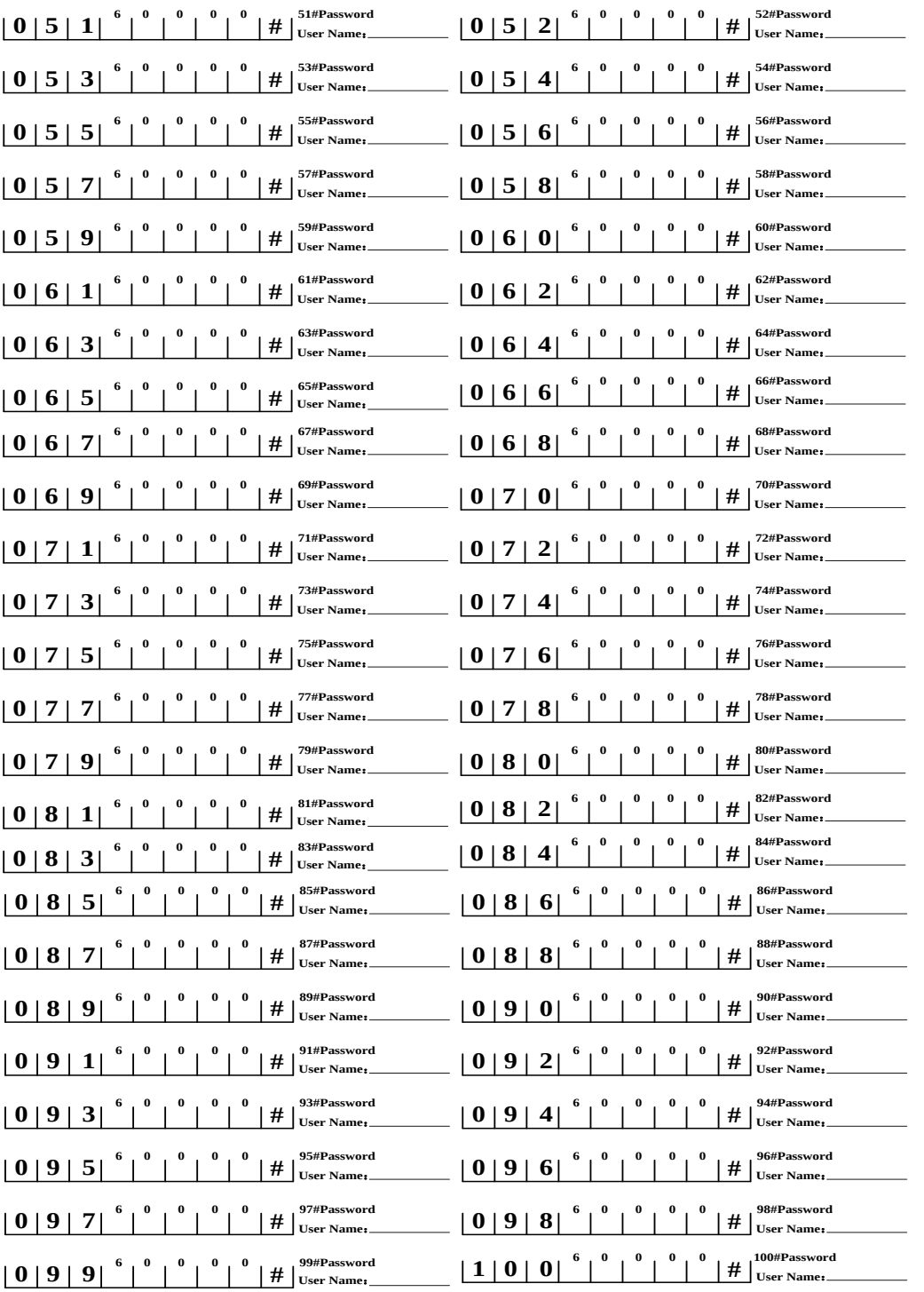
Appendix4：Conversion Table

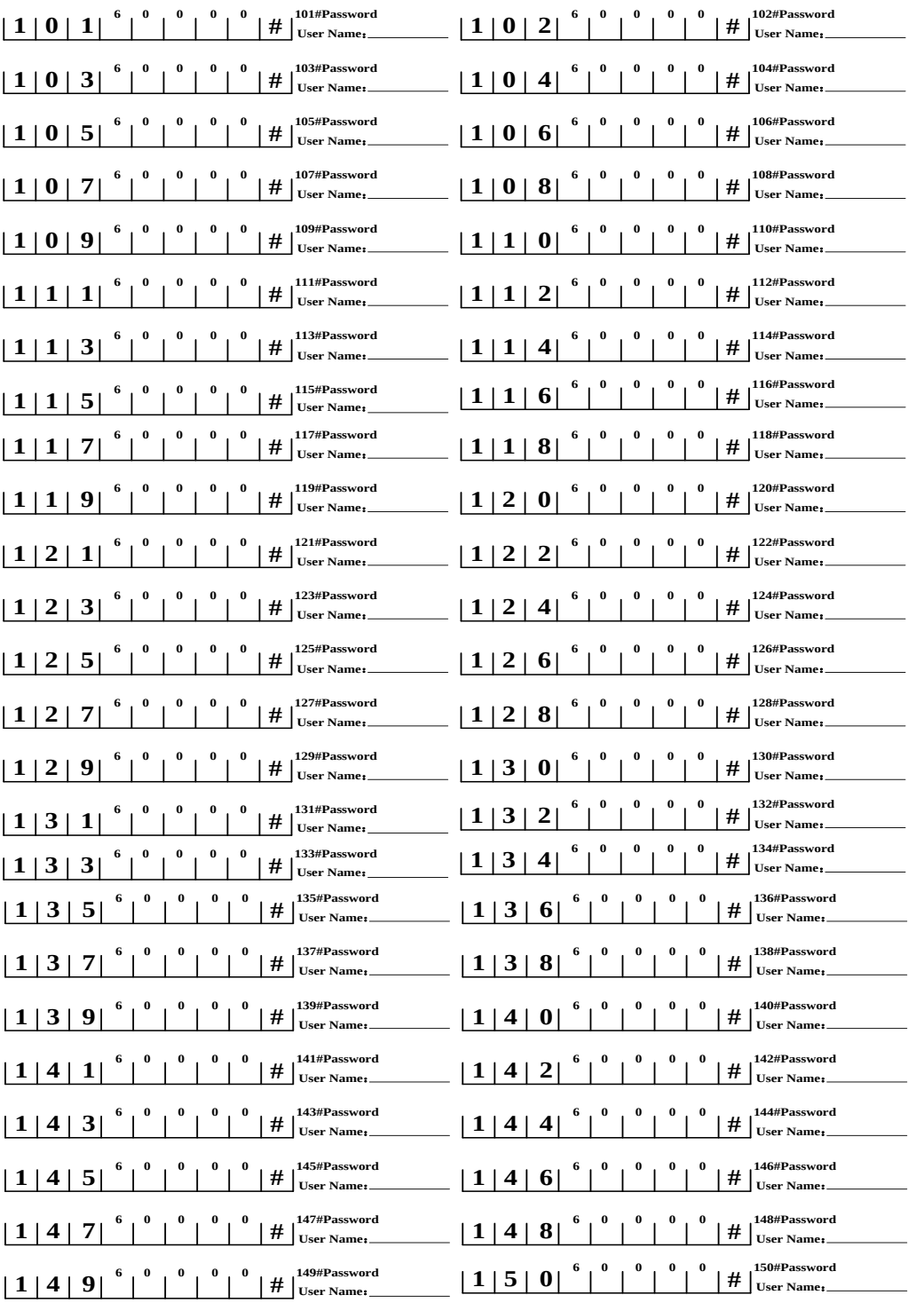
Conversion Table

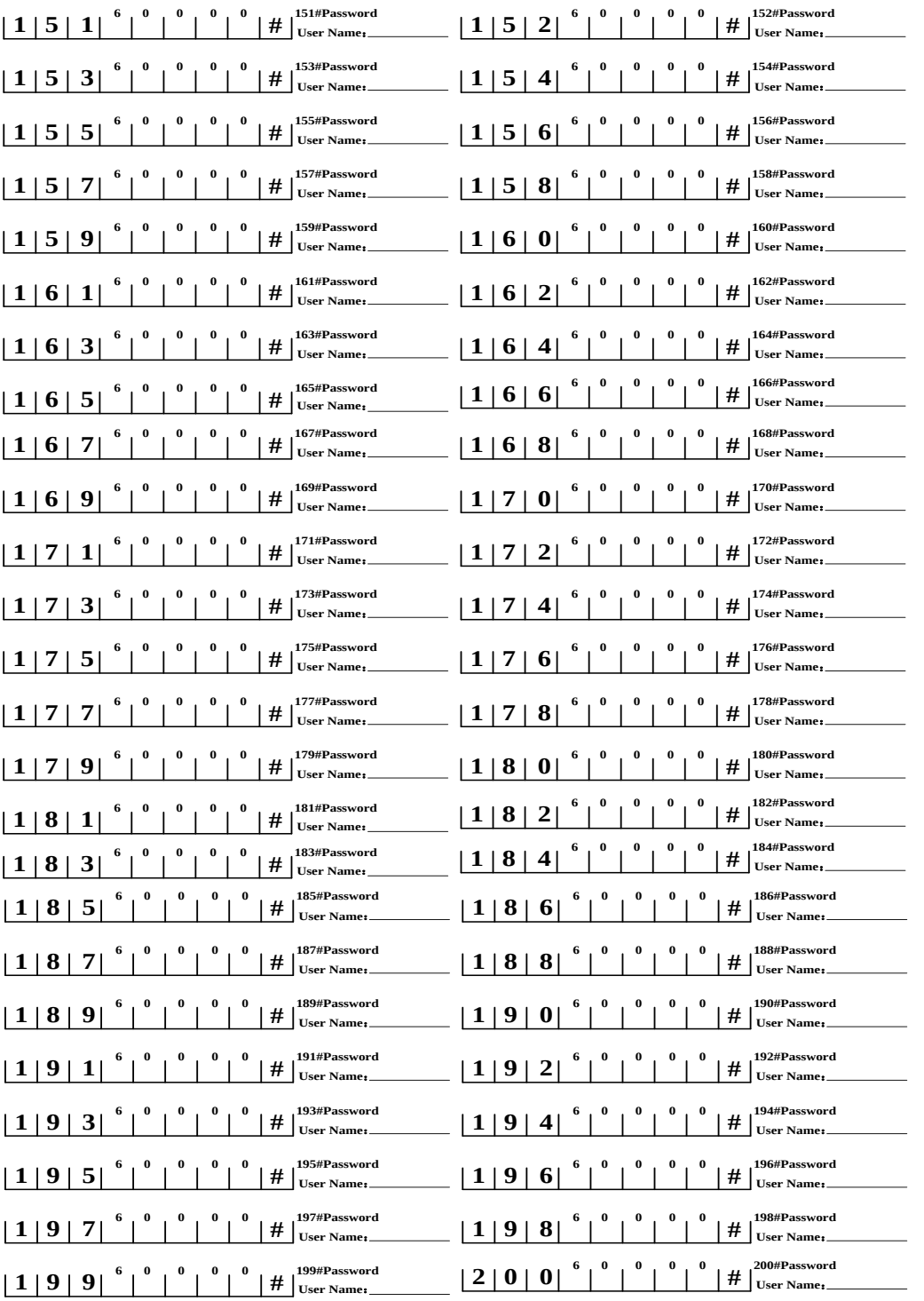
Hexadecimal Number	Corresponding Key
A	*0
B	*1
C	*2
D	*3
E	*4
F	*5

Control Panel Command Table

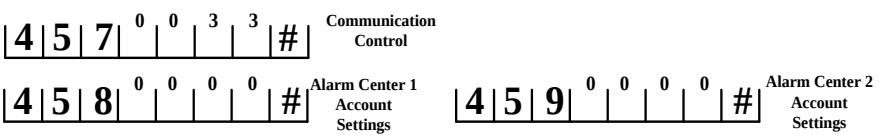
0	0	0	0	1	2	3	4	5	#	Installer Password	
0	0	1	*2	1	2	3	4	#	1#Password User Name:_____	0	0	2	6	0	0	0	0	#	2#Password User Name:_____
0	0	3	6	0	0	0	0	#	3#Password User Name:_____	0	0	4	6	0	0	0	0	#	4#Password User Name:_____
0	0	5	6	0	0	0	0	#	5#Password User Name:_____	0	0	6	6	0	0	0	0	#	6#PasswordPassword User Name:_____
0	0	7	6	0	0	0	0	#	7#Password User Name:_____	0	0	8	6	0	0	0	0	#	8#Password User Name:_____
0	0	9	6	0	0	0	0	#	9#Password User Name:_____	0	1	0	6	0	0	0	0	#	10#Password User Name:_____
0	1	1	6	0	0	0	0	#	11#Password User Name:_____	0	1	2	6	0	0	0	0	#	12#Password User Name:_____
0	1	3	6	0	0	0	0	#	13#Password User Name:_____	0	1	4	6	0	0	0	0	#	14#Password User Name:_____
0	1	5	6	0	0	0	0	#	15#Password User Name:_____	0	1	6	6	0	0	0	0	#	16#PasswordPassword User Name:_____
0	1	7	6	0	0	0	0	#	17#Password User Name:_____	0	1	8	6	0	0	0	0	#	18#Password User Name:_____
0	1	9	6	0	0	0	0	#	19#Password User Name:_____	0	2	0	6	0	0	0	0	#	20#Password User Name:_____
0	2	1	6	0	0	0	0	#	21#Password User Name:_____	0	2	2	6	0	0	0	0	#	22#Password User Name:_____
0	2	3	6	0	0	0	0	#	23#Password User Name:_____	0	2	4	6	0	0	0	0	#	24#Password User Name:_____
0	2	5	6	0	0	0	0	#	25#Password User Name:_____	0	2	6	6	0	0	0	0	#	26#Password User Name:_____
0	2	7	6	0	0	0	0	#	27#Password User Name:_____	0	2	8	6	0	0	0	0	#	28#Password User Name:_____
0	2	9	6	0	0	0	0	#	29#Password User Name:_____	0	3	0	6	0	0	0	0	#	30#Password User Name:_____
0	3	1	6	0	0	0	0	#	31#Password User Name:_____	0	3	2	6	0	0	0	0	#	32#Password User Name:_____
0	3	3	6	0	0	0	0	#	33#Password User Name:_____	0	3	4	6	0	0	0	0	#	34#Password User Name:_____
0	3	5	6	0	0	0	0	#	35#Password User Name:_____	0	3	6	6	0	0	0	0	#	36#Password User Name:_____
0	3	7	6	0	0	0	0	#	37#Password User Name:_____	0	3	8	6	0	0	0	0	#	38#Password User Name:_____
0	3	9	6	0	0	0	0	#	39#Password User Name:_____	0	4	0	6	0	0	0	0	#	40#Password User Name:_____
0	4	1	6	0	0	0	0	#	41#Password User Name:_____	0	4	2	6	0	0	0	0	#	42#Password User Name:_____
0	4	3	6	0	0	0	0	#	43#Password User Name:_____	0	4	4	6	0	0	0	0	#	44#Password User Name:_____
0	4	5	6	0	0	0	0	#	45#Password User Name:_____	0	4	6	6	0	0	0	0	#	46#Password User Name:_____
0	4	7	6	0	0	0	0	#	47#Password User Name:_____	0	4	8	6	0	0	0	0	#	48#Password User Name:_____
0	4	9	6	0	0	0	0	#	49#Password User Name:_____	0	5	0	6	0	0	0	0	#	50#Password User Name:_____

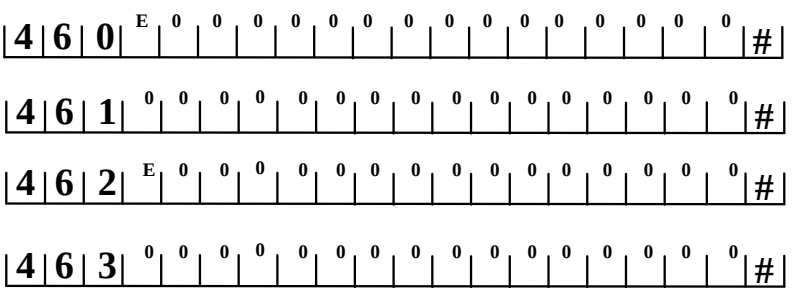

051#Password User Name:
052#Password User Name:
053#Password User Name:
054#Password User Name:
055#Password User Name:
056#Password User Name:
057#Password User Name:
058#Password User Name:
059#Password User Name:
060#Password User Name:
061#Password User Name:
062#Password User Name:
063#Password User Name:
064#Password User Name:
065#Password User Name:
066#Password User Name:
067#Password User Name:
068#Password User Name:
069#Password User Name:
070#Password User Name:
071#Password User Name:
072#Password User Name:
073#Password User Name:
074#Password User Name:
075#Password User Name:
076#Password User Name:
077#Password User Name:
078#Password User Name:
079#Password User Name:
080#Password User Name:
081#Password User Name:
082#Password User Name:
083#Password User Name:
084#Password User Name:
085#Password User Name:
086#Password User Name:
087#Password User Name:
088#Password User Name:
089#Password User Name:
090#Password User Name:
091#Password User Name:
092#Password User Name:
093#Password User Name:
094#Password User Name:
095#Password User Name:
096#Password User Name:
097#Password User Name:
098#Password User Name:
099#Password User Name:
100#Password User Name:

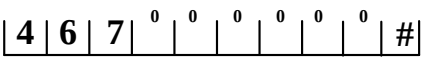

101#Password User Name:
102#Password User Name:
103#Password User Name:
104#Password User Name:
105#Password User Name:
106#Password User Name:
107#Password User Name:
108#Password User Name:
109#Password User Name:
110#Password User Name:
111#Password User Name:
112#Password User Name:
113#Password User Name:
114#Password User Name:
115#Password User Name:
116#Password User Name:
117#Password User Name:
118#Password User Name:
119#Password User Name:
120#Password User Name:
121#Password User Name:
122#Password User Name:
123#Password User Name:
124#Password User Name:
125#Password User Name:
126#Password User Name:
127#Password User Name:
128#Password User Name:
129#Password User Name:
130#Password User Name:
131#Password User Name:
132#Password User Name:
133#Password User Name:
134#Password User Name:
135#Password User Name:
136#Password User Name:
137#Password User Name:
138#Password User Name:
139#Password User Name:
140#Password User Name:
141#Password User Name:
142#Password User Name:
143#Password User Name:
144#Password User Name:
145#Password User Name:
146#Password User Name:
147#Password User Name:
148#Password User Name:
149#Password User Name:
150#Password User Name:


1 5 1 6 0 0 0 0 # 151#Password User Name:
1 5 2 6 0 0 0 0 # 152#Password User Name:
1 5 3 6 0 0 0 0 # 153#Password User Name:
1 5 4 6 0 0 0 0 # 154#Password User Name:
1 5 5 6 0 0 0 0 # 155#Password User Name:
1 5 6 6 0 0 0 0 # 156#Password User Name:
1 5 7 6 0 0 0 0 # 157#Password User Name:
1 5 8 6 0 0 0 0 # 158#Password User Name:
1 5 9 6 0 0 0 0 # 159#Password User Name:
1 6 0 6 0 0 0 0 # 160#Password User Name:
1 6 1 6 0 0 0 0 # 161#Password User Name:
1 6 2 6 0 0 0 0 # 162#Password User Name:
1 6 3 6 0 0 0 0 # 163#Password User Name:
1 6 4 6 0 0 0 0 # 164#Password User Name:
1 6 5 6 0 0 0 0 # 165#Password User Name:
1 6 6 6 0 0 0 0 # 166#Password User Name:
1 6 7 6 0 0 0 0 # 167#Password User Name:
1 6 8 6 0 0 0 0 # 168#Password User Name:
1 6 9 6 0 0 0 0 # 169#Password User Name:
1 7 0 6 0 0 0 0 # 170#Password User Name:
1 7 1 6 0 0 0 0 # 171#Password User Name:
1 7 2 6 0 0 0 0 # 172#Password User Name:
1 7 3 6 0 0 0 0 # 173#Password User Name:
1 7 4 6 0 0 0 0 # 174#Password User Name:
1 7 5 6 0 0 0 0 # 175#Password User Name:
1 7 6 6 0 0 0 0 # 176#Password User Name:
1 7 7 6 0 0 0 0 # 177#Password User Name:
1 7 8 6 0 0 0 0 # 178#Password User Name:
1 7 9 6 0 0 0 0 # 179#Password User Name:
1 8 0 6 0 0 0 0 # 180#Password User Name:
1 8 1 6 0 0 0 0 # 181#Password User Name:
1 8 2 6 0 0 0 0 # 182#Password User Name:
1 8 3 6 0 0 0 0 # 183#Password User Name:
1 8 4 6 0 0 0 0 # 184#Password User Name:
1 8 5 6 0 0 0 0 # 185#Password User Name:
1 8 6 6 0 0 0 0 # 186#Password User Name:
1 8 7 6 0 0 0 0 # 187#Password User Name:
1 8 8 6 0 0 0 0 # 188#Password User Name:
1 8 9 6 0 0 0 0 # 189#Password User Name:
1 9 0 6 0 0 0 0 # 190#Password User Name:
1 9 1 6 0 0 0 0 # 191#Password User Name:
1 9 2 6 0 0 0 0 # 192#Password User Name:
1 9 3 6 0 0 0 0 # 193#Password User Name:
1 9 4 6 0 0 0 0 # 194#Password User Name:
1 9 5 6 0 0 0 0 # 195#Password User Name:
1 9 6 6 0 0 0 0 # 196#Password User Name:
1 9 7 6 0 0 0 0 # 197#Password User Name:
1 9 8 6 0 0 0 0 # 198#Password User Name:
1 9 9 6 0 0 0 0 # 199#Password User Name:
2 0 0 6 0 0 0 0 # 200#Password User Name:

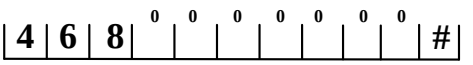

201 2 5 0 1 0 1 # Region1 Parameters Configuration
202 2 5 0 1 0 1 # Region2 Parameters Configuration
203 2 5 0 1 0 1 # Region3 Parameters Configuration
204 2 5 0 1 0 1 # Region4 Parameters Configuration
205 2 5 0 1 0 1 # Region5 Parameters Configuration
206 2 5 0 1 0 1 # Region6 Parameters Configuration
207 2 5 0 1 0 1 # Region7 Parameters Configuration
208 2 5 0 1 0 1 # Region8 Parameters Configuration
209 2 5 0 1 0 1 # Region9 Parameters Configuration
210 2 5 0 1 0 1 # Region10 Parameters Configuration
211 2 5 0 1 0 1 # Region11 Parameters Configuration
212 2 5 0 1 0 1 # Region12 Parameters Configuration
213 2 5 0 1 0 1 # Region13 Parameters Configuration
214 2 5 0 1 0 1 # Region14 Parameters Configuration
215 2 5 0 1 0 1 # Region15 Parameters Configuration
216 2 5 0 1 0 1 # Region16 Parameters Configuration


457 0 0 3 3 # Communication Control
458 0 0 0 0 # Alarm Center 1 Account Settings
459 0 0 0 0 # Alarm Center 2 Account Settings

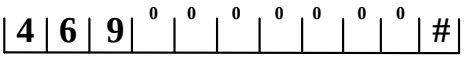

460 E 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 # Alarm Center 1Phone Number Settings
461 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 # Alarm Center 1Phone Number Settings
462 E 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 # Alarm Center 2Phone Number Settings
463 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 # Alarm Center 2Phone Number Settings



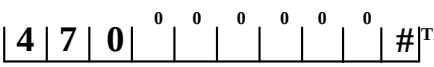
Region Linked Trigger Configuration



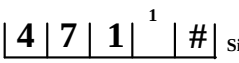
Enable Trigger Event Linkage Configuration



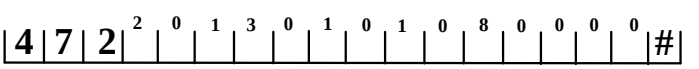
Disable Trigger Event Linkage Configuration



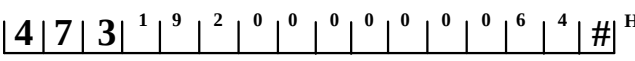
Trigger Time Settings



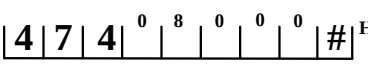
Siren Settings



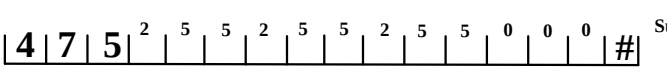
Host Time Settings



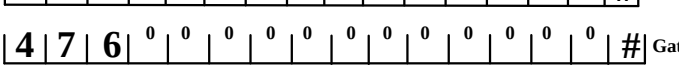
Host IP Address Settings



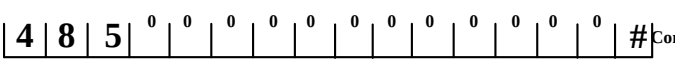
Host Port Number Settings



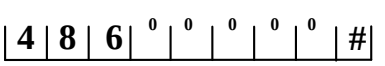
Subnet Mask Settings



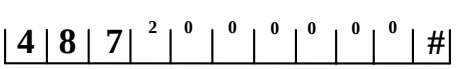
Gateway Settings



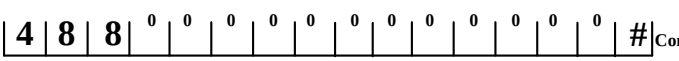
Network Center 1 IP Configuration Programming Address



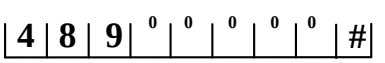
Network Center 1 Port Configuration Programming Address



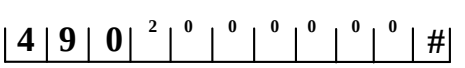
Network Center 1 Protocol and Account Configuration Programming Address



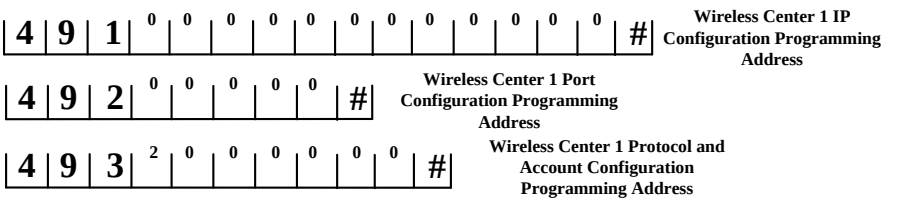
Network Center 2 IP Configuration Programming Address

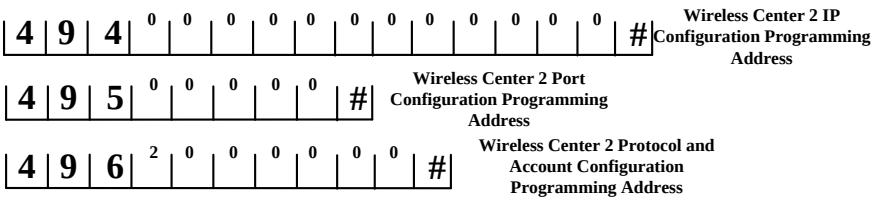


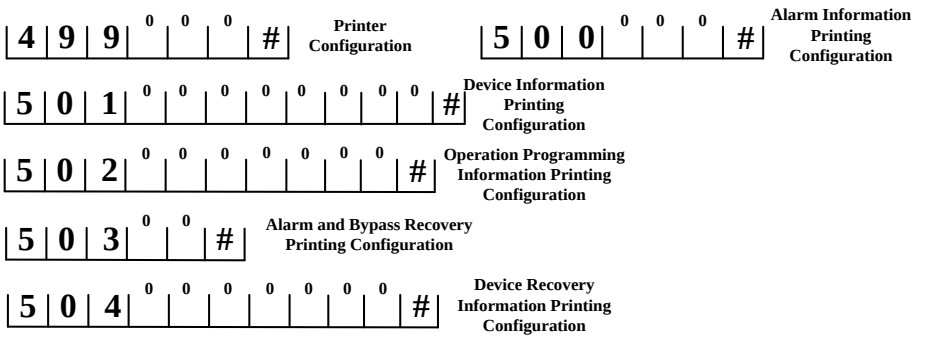
Network Center 2 Port Configuration Programming Address

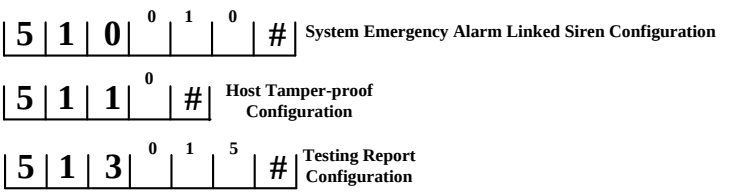


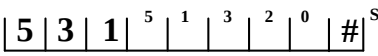
Network Center 2 Protocol and Account Configuration Programming Address


4 9 1 0 0 0 0 0 0 0 0 0 0 0 #
Wireless Center 1 IP Configuration Programming Address
4 9 2 0 0 0 0 0 #
Wireless Center 1 Port Configuration Programming Address
4 9 3 2 0 0 0 0 0 0 #
Wireless Center 1 Protocol and Account Configuration Programming Address

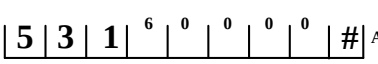

4 9 4 0 0 0 0 0 0 0 0 0 0 0 #
Wireless Center 2 IP Configuration Programming Address
4 9 5 0 0 0 0 0 #
Wireless Center 2 Port Configuration Programming Address
4 9 6 2 0 0 0 0 0 0 #
Wireless Center 2 Protocol and Account Configuration Programming Address


4 9 9 0 0 0 #
Printer Configuration
5 0 0 0 0 0 #
Alarm Information Printing Configuration
5 0 1 0 0 0 0 0 0 0 0 #
Device Information Printing Configuration
5 0 2 0 0 0 0 0 0 0 0 #
Operation Programming Information Printing Configuration
5 0 3 0 0 #
Alarm and Bypass Recovery Printing Configuration
5 0 4 0 0 0 0 0 0 0 0 #
Device Recovery Information Printing Configuration

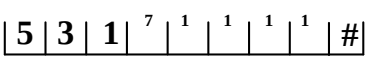

5 1 0 0 1 0 #
System Emergency Alarm Linked Siren Configuration
5 1 1 0 #
Host Tamper-proof Configuration
5 1 3 0 1 5 #
Testing Report Configuration



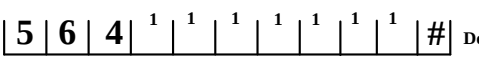
System Time and Hostage Report Configuration



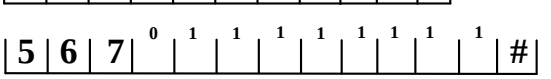
System Report and Arming/Disarming Prompt Configuration



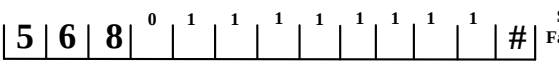
System Key User Permission Configuration



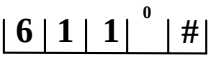
Host System Fault Detection Configuration



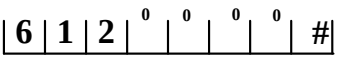
System Fault Display Configuration



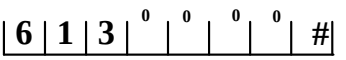
System Keyboard Fault Prompt Sound Configuration



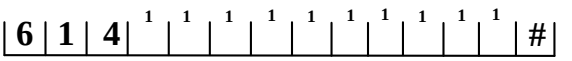
Center Group 1 Enabling Configuration



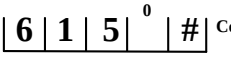
Center Group 1 Uploading Mode Configuration



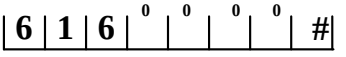
Center Group 1 Region Alarm Report Configuration



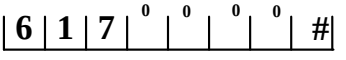
Center Group 1 Non-region Alarm Report Configuration



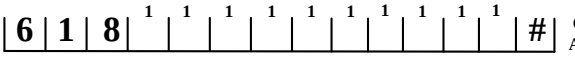
Center Group 2 Enabling Configuration



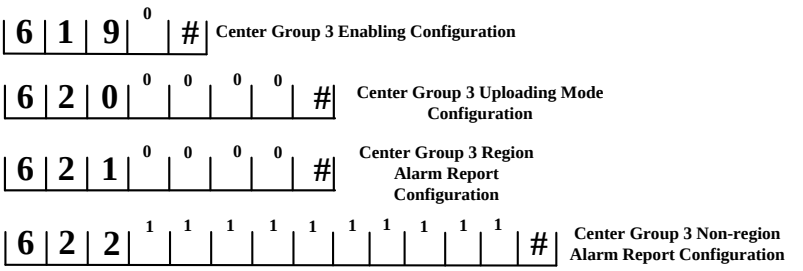
Center Group 2 Uploading Mode Configuration

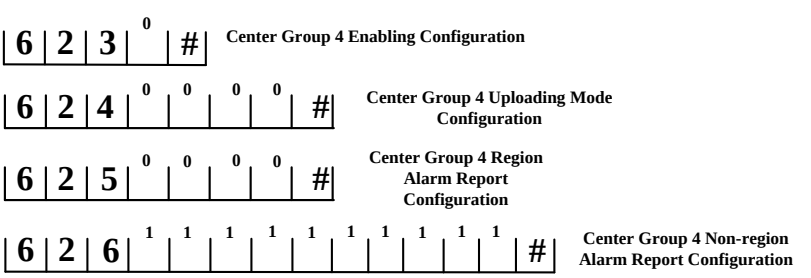


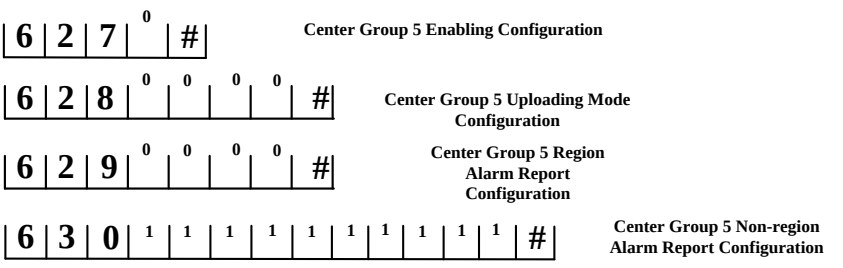
Center Group 2 Region Alarm Report Configuration

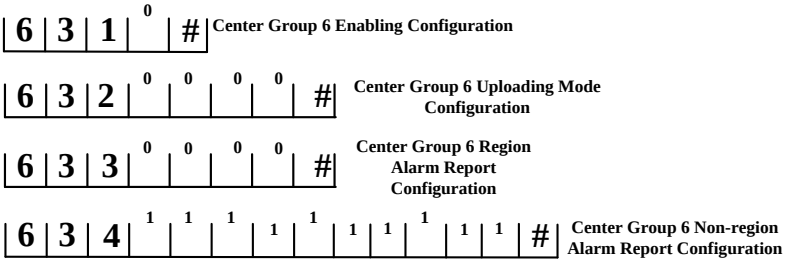


Center Group 2 Non-region Alarm Report Configuration


6 1 9 0 #
Center Group 3 Enabling Configuration
6 2 0 0 0 0 0 #
Center Group 3 Uploading Mode Configuration
6 2 1 0 0 0 0 #
Center Group 3 Region Alarm Report Configuration
6 2 2 1 1 1 1 1 1 1 1 1 1 #
Center Group 3 Non-region Alarm Report Configuration


6 2 3 0 #
Center Group 4 Enabling Configuration
6 2 4 0 0 0 0 #
Center Group 4 Uploading Mode Configuration
6 2 5 0 0 0 0 #
Center Group 4 Region Alarm Report Configuration
6 2 6 1 1 1 1 1 1 1 1 1 1 #
Center Group 4 Non-region Alarm Report Configuration


6 2 7 0 #
Center Group 5 Enabling Configuration
6 2 8 0 0 0 0 #
Center Group 5 Uploading Mode Configuration
6 2 9 0 0 0 0 #
Center Group 5 Region Alarm Report Configuration
6 3 0 1 1 1 1 1 1 1 1 1 1 #
Center Group 5 Non-region Alarm Report Configuration


6 3 1 0 #
Center Group 6 Enabling Configuration
6 3 2 0 0 0 0 #
Center Group 6 Uploading Mode Configuration
6 3 3 0 0 0 0 #
Center Group 6 Region Alarm Report Configuration
6 3 4 1 1 1 1 1 1 1 1 1 1 #
Center Group 6 Non-region Alarm Report Configuration

First Choice for Security Professionals