



HIKVISION

Video Security Control Panel

User Manual

UD.6L0206D1028A01

User Manual

COPYRIGHT ©2015 Hangzhou Hikvision Digital Technology Co., Ltd.

ALL RIGHTS RESERVED.

Any and all information, including, among others, wordings, pictures, graphs are the properties of Hangzhou Hikvision Digital Technology Co., Ltd. or its subsidiaries (hereinafter referred to be “Hikvision”). This user manual (hereinafter referred to be “the Manual”) cannot be reproduced, changed, translated, or distributed, partially or wholly, by any means, without the prior written permission of Hikvision. Unless otherwise stipulated, Hikvision does not make any warranties, guarantees or representations, express or implied, regarding to the Manual.

About this Manual

This Manual is applicable to Video Security 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 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, CONSEQUENTIALS, 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 RESPONSIBILITIES 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.

0200001050505

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 *manufacturer recommended battery type*.

Content

Chapter 1	Introduction	11
1.1	Overview	11
1.2	Feature	11
Chapter 2	Installation and Wiring	13
2.1	Main Board Overview	13
	Main Board Description	15
2.2	Wiring Device	16
2.2.1	Wiring Detector	16
2.2.2	Wiring Alarm Output	17
2.2.3	Wiring Keypad	19
2.2.4	Wiring Video/Audio Input	19
2.2.5	Wiring Video/Audio Output	20
2.3	System Start-up	22
2.3.1	Video Security Control Panel Start-up	22
2.3.2	Alarm Keypad Start-up	22
2.3.3	Keypad Address	24
2.3.4	Factory Settings	25
2.3.5	Activating the Control Panel	27
Chapter 3	Keypad Operation (Local Operation)	32
3.1	Alarm Keypad Settings	32
3.1.1	Installer Password Settings	32
3.1.2	Operator Settings	33
3.1.3	Zone Parameters Settings	34
3.1.4	Zone Linked Trigger Settings	37
3.1.5	Trigger Event Linkage Settings	37
3.1.6	Trigger Time Settings	39
3.1.7	Siren Settings	39
3.1.8	Control Panel Time Settings	40
3.1.9	Control Panel IP Settings	40
3.1.10	Local Port Number Settings	41
3.1.11	Sub-net Mask Settings	41

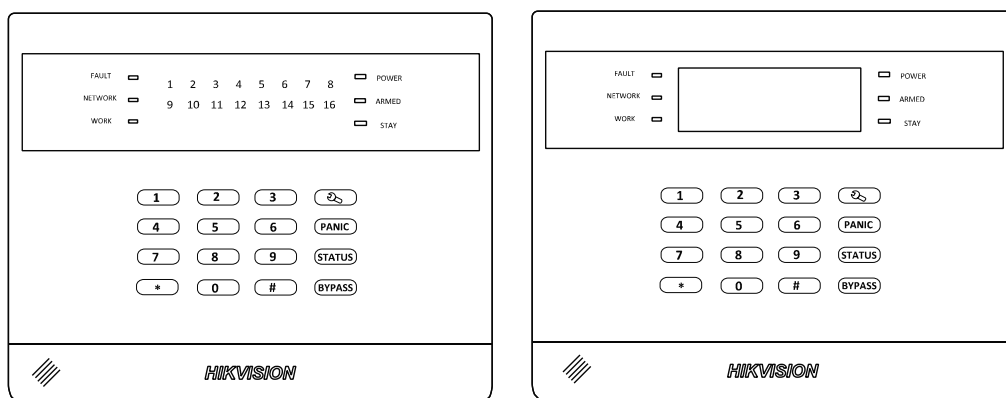
3.1.12	Gateway Settings _____	42
3.1.13	Uploading Center IP Settings _____	42
3.1.14	Uploading Center Port Settings _____	43
3.1.15	Center Protocol and Account Settings _____	43
3.1.16	Printer Parameters Settings _____	44
3.1.17	Alarm Message Settings _____	45
3.1.18	Device Information Settings _____	45
3.1.19	Operation Programming Information Settings _____	46
3.1.20	Restoring Information of Alarm and Bypass Settings _____	46
3.1.21	Device Recovering Information Settings _____	47
3.1.22	Siren Linked Event Settings _____	48
3.1.23	Emergency Alarm Linkage Siren Setting _____	49
3.1.24	Control Panel Tamper-proof Linked Siren Settings _____	49
3.1.25	Testing Report Settings _____	50
3.1.26	Partition Settings _____	51
3.1.27	Control Panel System Fault Detection Settings _____	57
3.1.28	Partition Fault Display Settings _____	57
3.1.29	Partition Fault Prompt Sound Settings _____	58
3.1.30	DHCP Settings _____	58
3.1.31	Delay Zone Time Settings _____	59
3.1.32	Center Group Enabling Settings _____	60
3.1.33	Center Group Uploading Mode Settings _____	60
3.1.34	Center Group Zone Alarm Report Settings _____	61
3.1.35	Center Group Non-zone Alarm Report Settings _____	62
3.1.36	White-list Parameters Settings _____	63
3.1.37	Schedule Settings _____	68
3.1.38	Wireless User Permission Settings _____	76
3.1.39	Video Live View Settings _____	76
3.2	Keypad Alarm Operation Code _____	77
3.2.1	Device Initialization _____	77
3.2.2	Security control panel Arming and Disarm _____	77
3.2.3	Stay Arming _____	78
3.2.4	Zone Bypass/Recovery _____	78
3.2.5	Group Bypass _____	78
3.2.6	Group Bypass Recovery _____	78
3.2.7	Keypad Cancel Alarm _____	79
3.2.8	Alarm Output Operation _____	79

3.2.9	Emergency Alarm	79
3.2.10	System Status Query	79
3.2.11	Main Operator Password Changing	80
3.2.12	Entering Partition System	80
3.2.13	Control Panel Programming Operation	80
3.2.14	Alarm Center Test	81
3.2.15	Project Mode	81
3.2.16	Enabling/Disabling Key Tone	81
3.2.17	Connecting Wireless Device and Control Panel	81
3.2.18	Deleting Connected Wireless Device	81
3.2.19	Deleting All Wireless Devices Connected to the Control Panel	82
3.2.20	Setting the Schedule	82
3.2.21	LCD Backlight Control	82
3.2.22	Disabling LCD Backlight	82
3.2.23	Pacing	82
3.2.24	Control Panel Soft Recovery	83
3.2.25	Current Fault Tone Disabling	83
3.2.26	Test Report Manually Triggering	83
3.2.27	Keypad Locking and Unlocking	83
Chapter 4	Accessing by Client Software	84
4.1	Installing the iVMS-4200	84
4.2	User Registration and Login	88
4.3	Video Security Control Panel Settings	89
	Adding/Editing/Deleting the Device	89
4.4	Remote Settings	90
	System Information Settings	91
	Network Settings	97
	Alarm Settings	107
	Storage	122
	Image Settings	123
	Event Settings	125
	Operation	132
	Status	133
Chapter 5	Trouble Shooting	135
Appendix1:	Specifications	143

Appendix2: CID Report	148
Appendix3: LED Keypad Prompt Sound	150
Appendix4: Conversion Table	150

Chapter 1 Introduction

1.1 Overview



These series of commercial-grade video control panels implement multi-functions of alarm input/output, scheduled arming/disarming, video signal processing and so on.

It is mainly applied to the security systems of shopping mall, stores, residence, apartments, communities, etc. It can be used cooperatively with the video surveillance and access control partition through the software operation.

1.2 Feature

Signal Input/ Output

- 8 zones alarm input;
- 4-ch network / analog camera, support dual-stream;
- 1-ch audio output, 1-ch two-way audio, 1-ch loudspeaker;
- 1-ch VGA output;
- 1-ch local alarm output, 8-ch extension alarm output;

Remote Control

- 32 remote controls;
- SMS alarm data-push and remote arming/disarming function (DS-19S08N-04F/KxGx supports message alarm data-push function);

Report Transmission

- 2 transmission modes: network transmission, 3G/4G transmission (DS-19S08N-4F/KxGx supports GPRS transmission);
- 2 groups of stand-alone Ethernet alarm centers;
- 2 groups of stand-alone 3G/4G alarm centers (DS-19S08N-4F/KxGx supports 3G/4G alarm center);

External Equipment

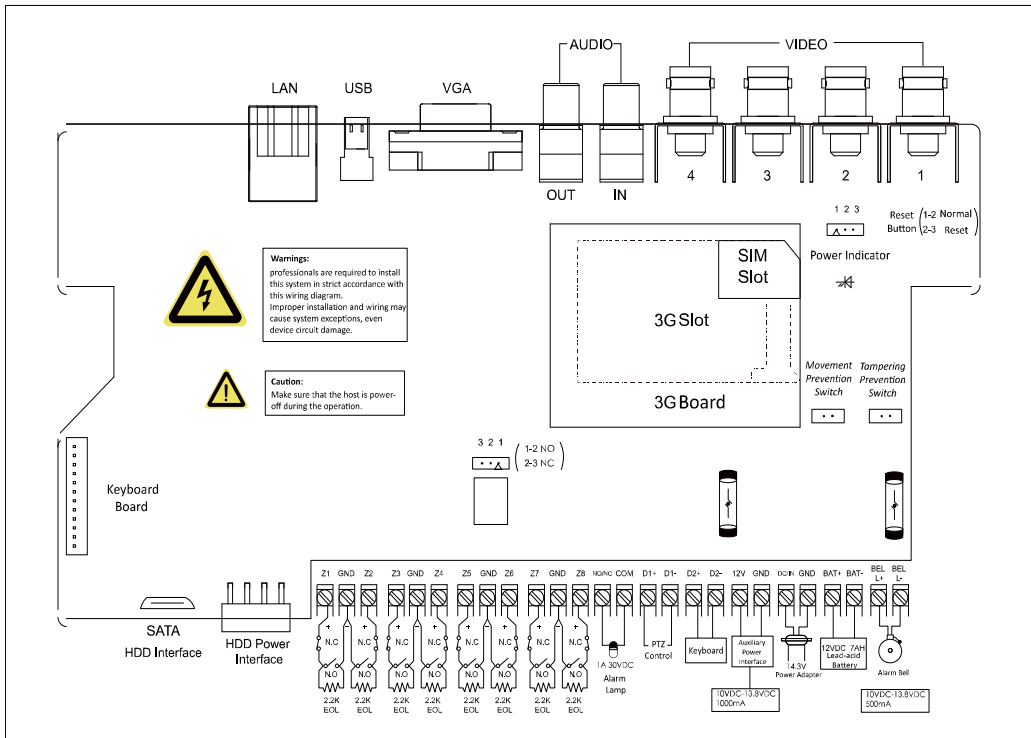
- 8 external alarm keypads are accessible;
- External storage battery for power supply;

Various Applications

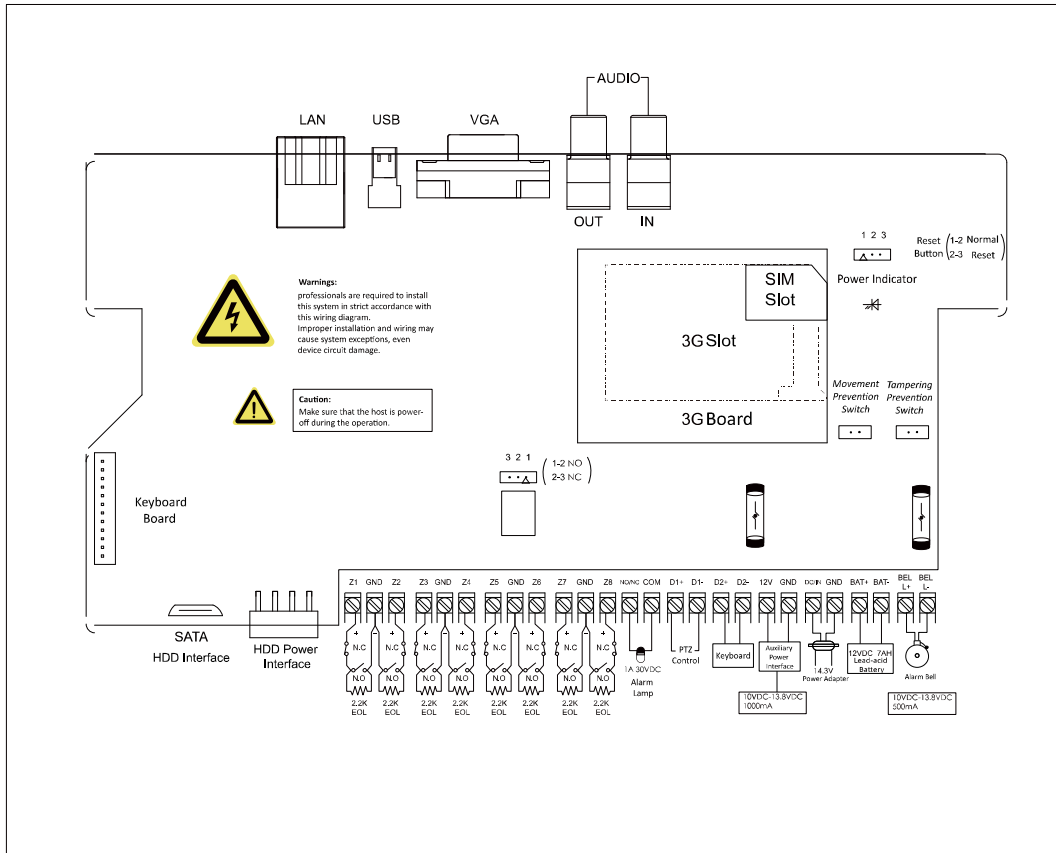
- Equipped with LED/LCD keypad;
- Scheduled arming/disarming function;
- Tamper-proof alarm and movement prevention alarm for the control panel and tamper-proof alarm for the detector;
- Support post-view function, the duration of post-view can be configured;
- Support rechecking of alarm linked live view and capture. Support video motion detection, video loss detection function;
- PTZ control is available;
- 1-ch siren (12VDC) output.

Chapter 2 Installation and Wiring

2.1 Main Board Overview



DS-19S08-04F/Kx (Gx)



DS-19S08N-04F/Kx (Gx)

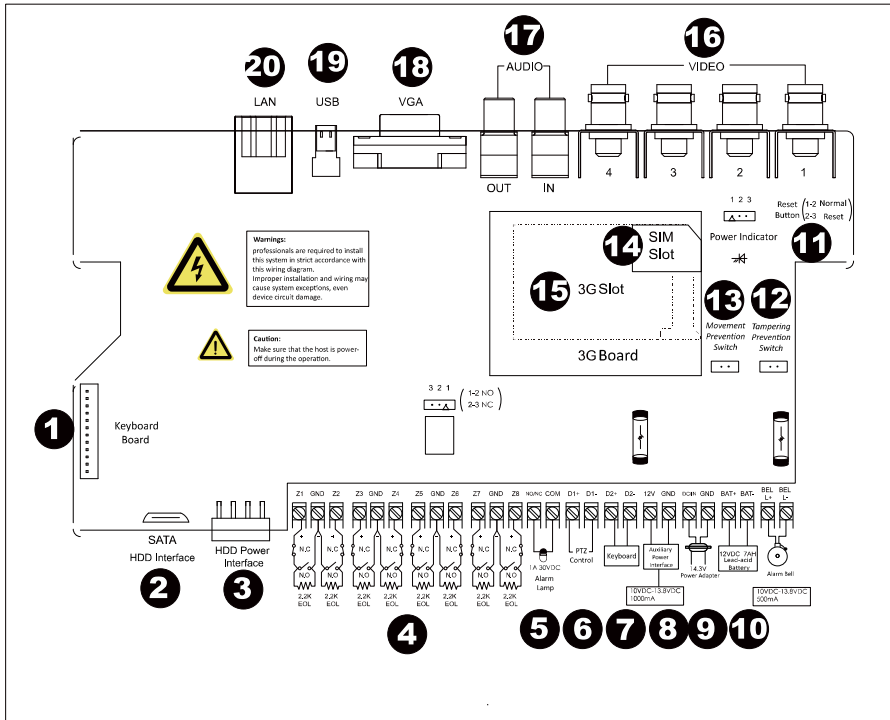
Main Board Description

The main board description is shown as follows.

Take the model of DS-19S08-04F/Kx (Gx) as an example.



This module varies depending on the models of control panel.



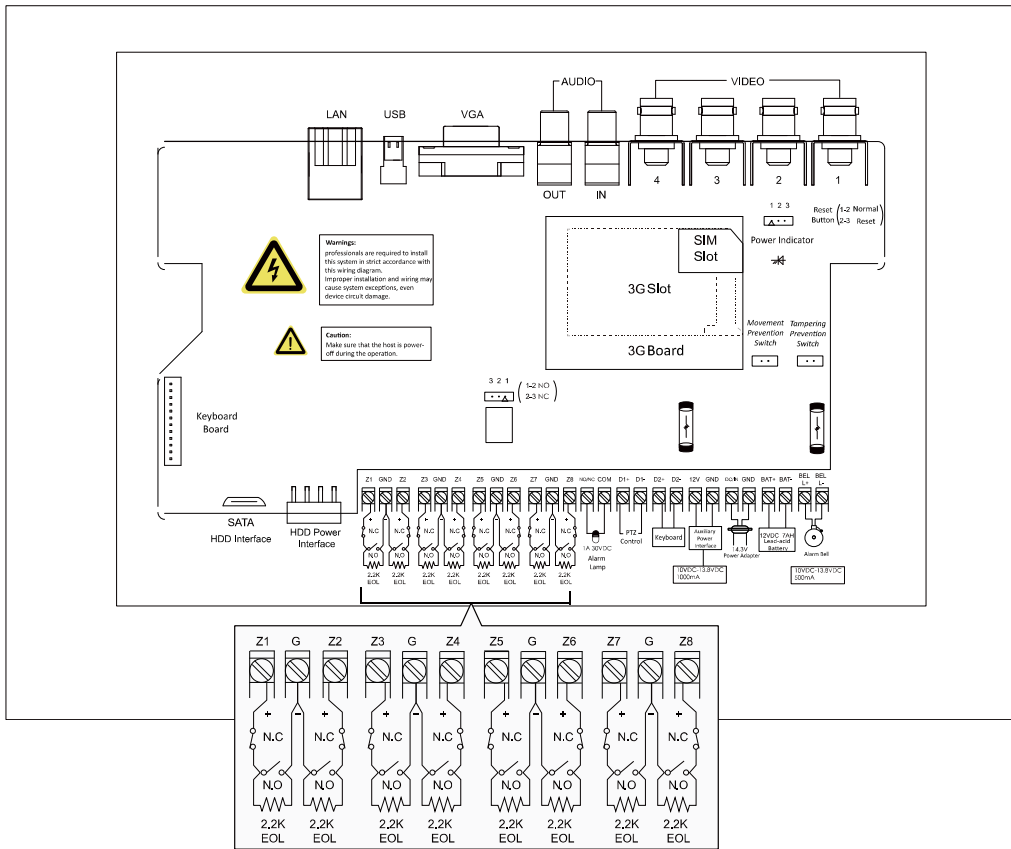
NO.	Description	NO.	Description
1	Keypad Board Interface	11	Reset Button Switch
2	SATA HDD Interface	12	Tampering Prevention
3	HDD Power Interface	13	Movement Prevention Switch
4	Alarm Input Interface	14	SIM Card Slot
5	Alarm Output (Alarm Lamp)	15	3G Card Slot
6	PTZ Control Interface	16	Video Input Interface
7	Keypad Connection Interface	17	Audio Input Interface
8	Auxiliary Power Interface	18	VGA Interface
9	Power Adapter	19	USB Interface
10	Lead-acid Battery	20	LAN Interface

2.2 Wiring Device

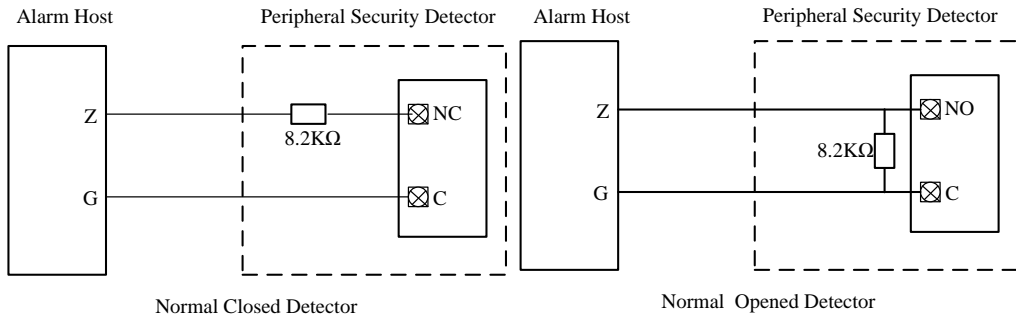
2.2.1 Wiring Detector

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

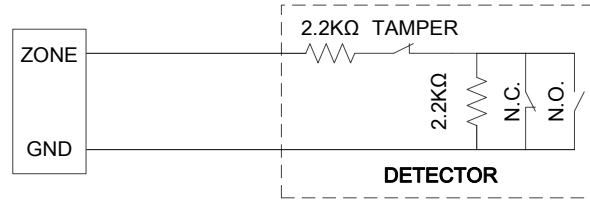
Take the model of DS-19S08-04F/Kx (Gx) as an example.



The wiring of sensor is shown as follows.



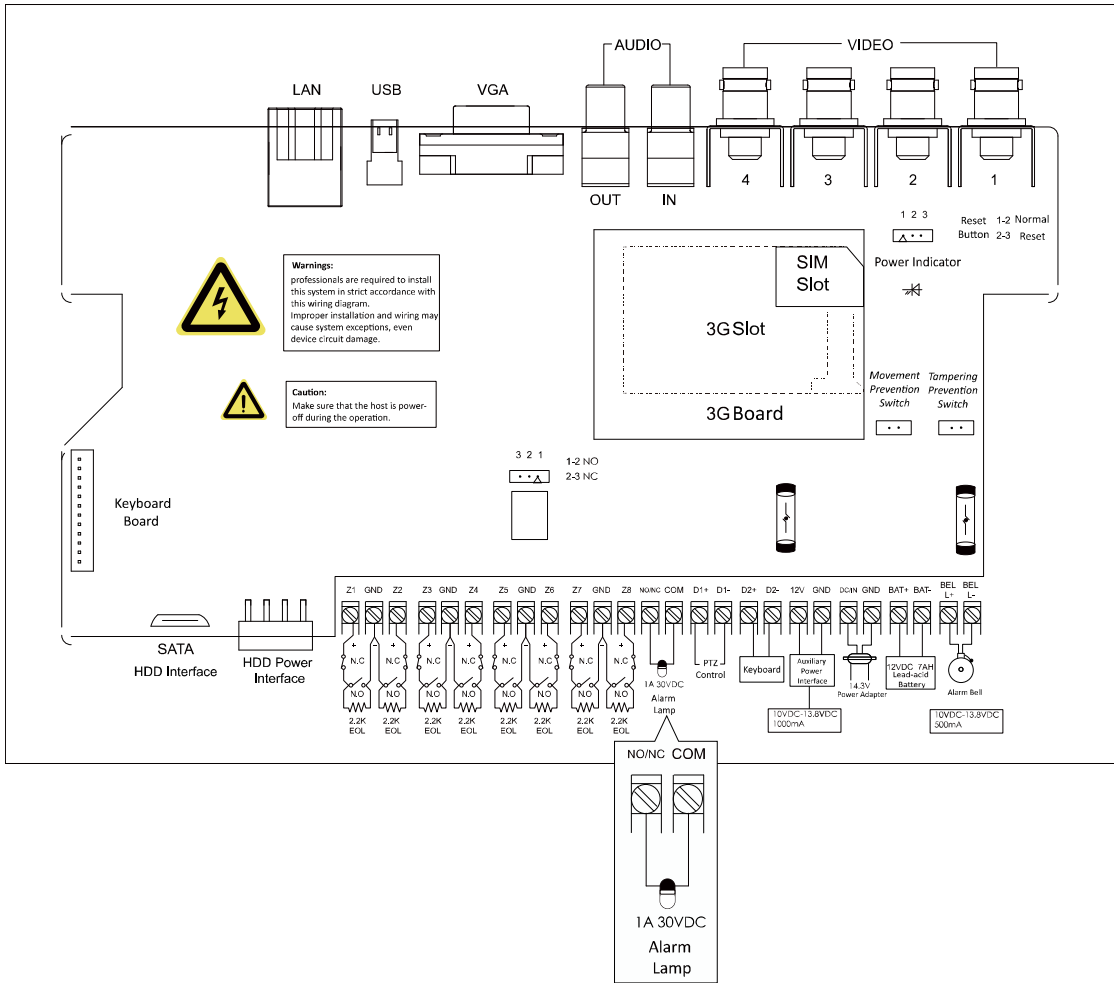
The Tamper-proof wiring is shown below.



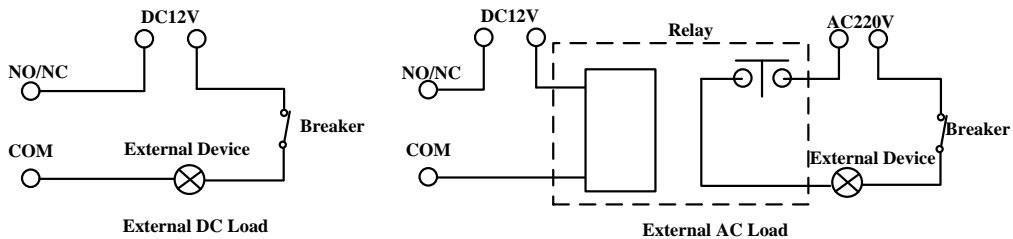
- The resistance of $2.2K\ \Omega$ or $3.3K\ \Omega$ supports tamper-proof and non-tamper-proof wiring.
- The resistance of $4.7K\ \Omega$ only supports tamper-proof wiring.
- The resistance of $5.6K\ \Omega$ or $8.2K\ \Omega$ only supports non-tamper-proof wiring.

2.2.2 Wiring Alarm Output

Take the model of DS-19S08-04F/Kx (Gx) as an example, the alarm output interfaces of the video security control panel are show as follows.



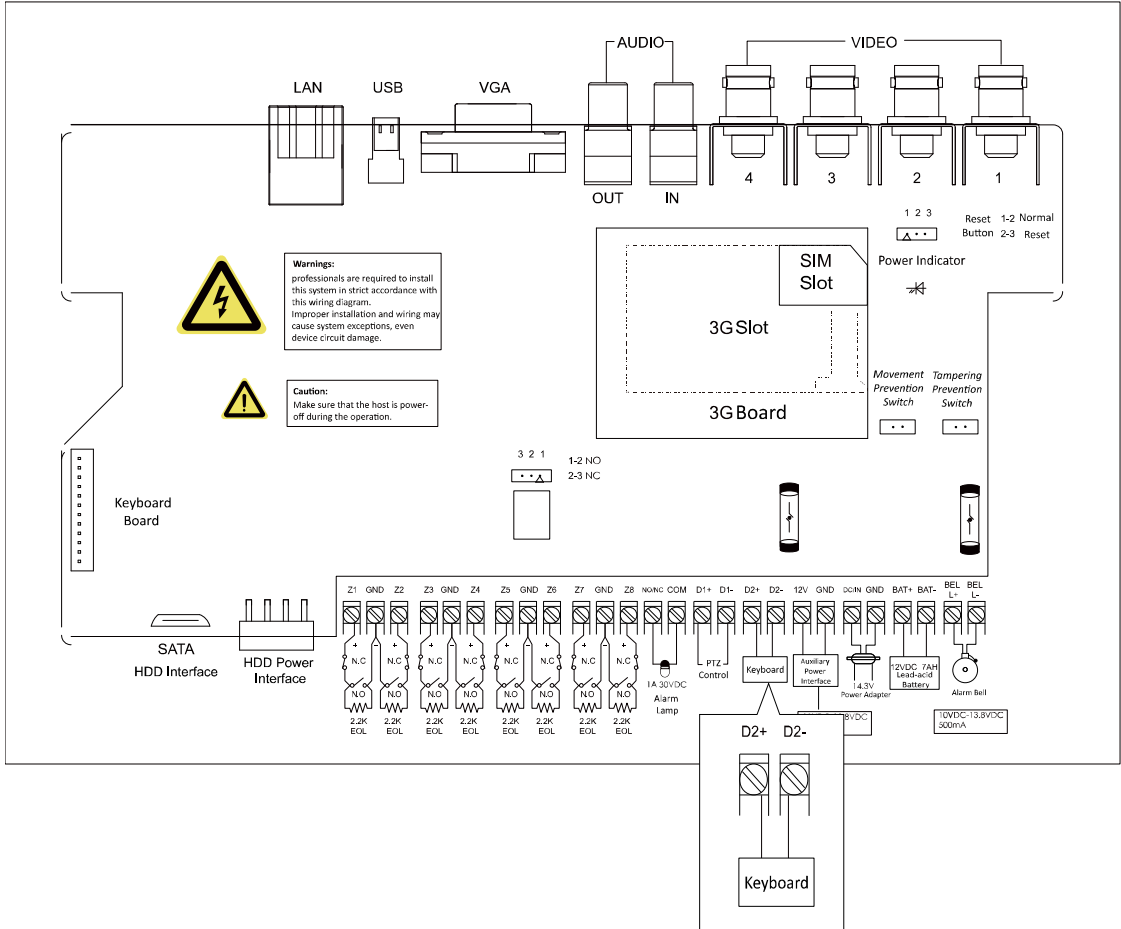
The wiring of alarm output is shown as follows:



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

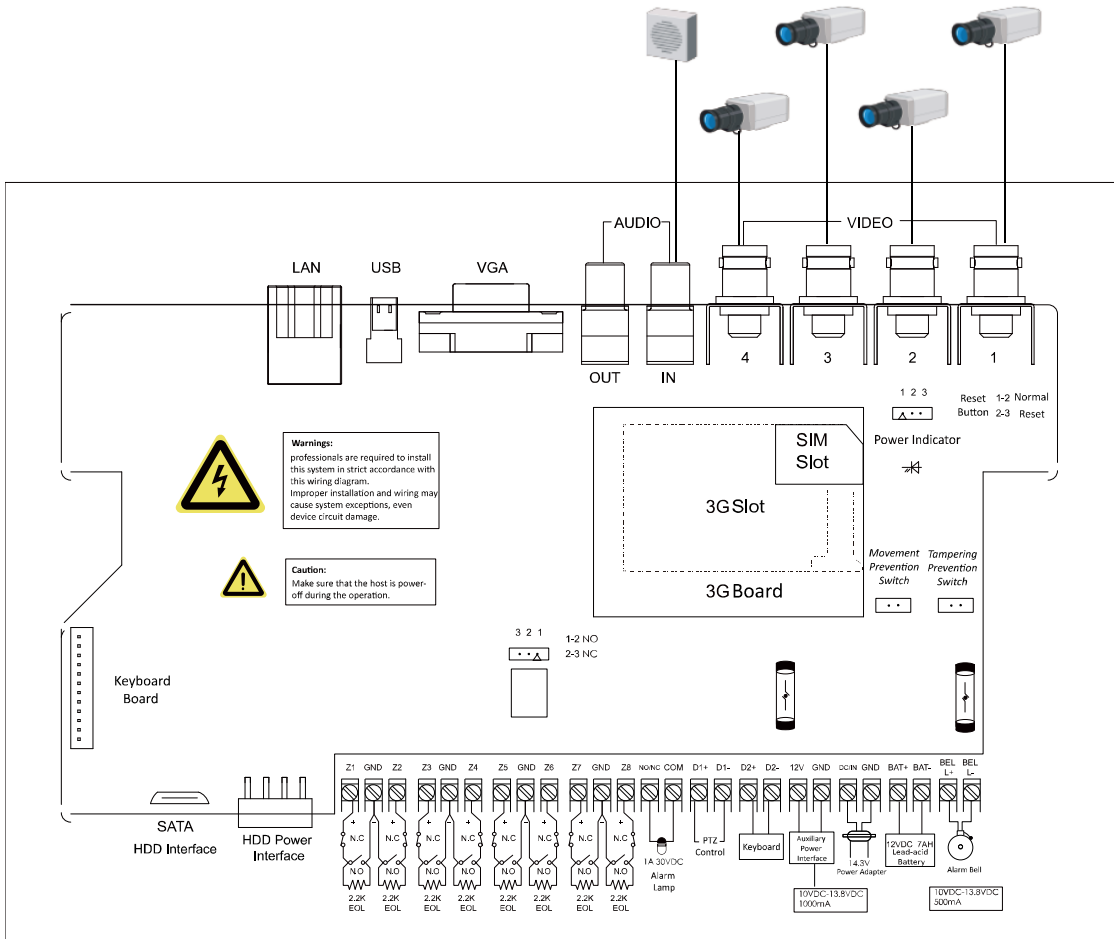
2.2.3 Wiring Keypad

The keypad wiring is shown as follows. Take the model of DS-19S08-04F/Kx (Gx) as an example.



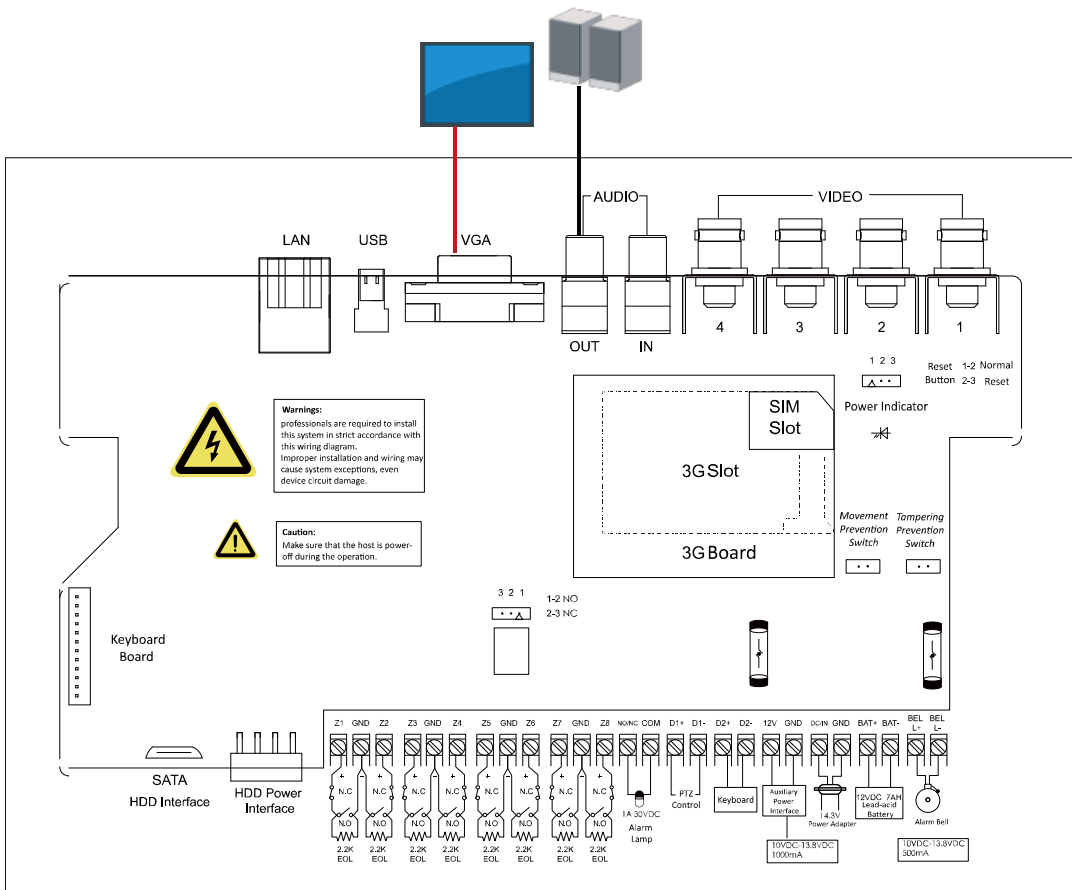
2.2.4 Wiring Video/Audio Input

The video/audio wiring is shown as follows. Take the model of DS-19S08-04F/Kx (Gx) as an example.



2.2.5 Wiring Video/Audio Output

Take the model of DS-19S08-04F/Kx (Gx) as an example



2.3 System Start-up



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

2.3.1 Video Security Control Panel Start-up

The keypad registration will be completed in 10 seconds after the video security control panel is being powered on. The system then will complete the start-up and enter the proper 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 powered on. If the registration is succeeded, the working status indicator will turn green.

LED Alarm Keypad Arming/Disarming Status

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

LED Alarm Keypad Working Status

Working Status	Indicator Status	Working Status	Indicator Status
Normal	Green (Continuously Light)	Unregistered	Red (Flickering)
System Exception	Orange (Flickering)	In Programming	Green (Flickering)
In Project	Red (Continuously Light)	Main Code Password Editing	Green (Flickering)

LED Alarm Keypad Channel Status

Working Status	Indicator Status	Working Status	Indicator Status
Normal	Extinguishing	Exception	Red (Continuously Light)

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

LED Alarm Keypad Channel 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		8	Reservation

LCD Global Keypad Indicator

LCD Global Keypad Arming/Disarming Status

Working Status	Indicator Status	Working Status	Indicator Status
In Programming	Green (Flickering)	Main Operator Password Editing	Green (Flickering)
Parameters Initialization	Green (Flickering)	Re-searching	Green (Flickering)
Re-registration	Green (Flickering)	Arming All Working Partition	Red (Continuously Light)
Disarming All Working Partition	Green (Continuously Light)	No Enabled Partition	Extinguishing

LCD Global Keypad Working Status

Working Status	Indicator Status	Working Status	Indicator Status
In Programming	Green (Flickering)	Main Operator Password Editing	Green (Flickering)
Parameters Initialization	Green (Flickering)	Re-searching	Green (Flickering)
Re-registration	Green (Flickering)	System Fault	Green (Flickering)

Working Status	Indicator Status	Working Status	Indicator Status
System Ready	Green (Continuously Light)		

LCD Partition Keypad Indicator

LCD Partition Keypad Arming/Disarming Status


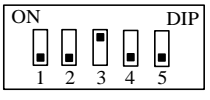
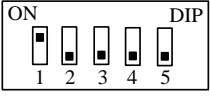
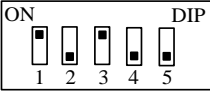
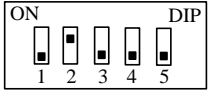
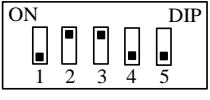
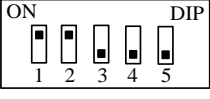
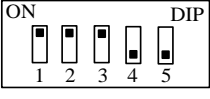
Working Status	Indicator Status	Working Status	Indicator Status
In Programming	Green (Flickering)	Parameters Initialization	Green (Flickering)
Re-searching	Green (Flickering)	Re-registration	Green (Flickering)
Enable Partition Arming	Red (Continuously Light)	Enable Partition Disarming	Green (Continuously Light)
Partition Not Enabled	Extinguishing		

LCD Partition Keypad Working Status

Working Status	Indicator Status	Working Status	Indicator Status
In Programming	Green (Flickering)	Parameters Initialization	Green (Flickering)
Re-searching	Green (Flickering)	Re-registration	Green (Flickering)
System Fault	Green (Flickering)	System Works Properly	Green (Continuously Light)
Keypad Not Enabled	Extinguishing		

2.3.3 Keypad Address

A unique address is required for each alarm keypad in the system. 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 0~7.

DIP	Address	DIP	Address
	0		4
	1		5
	2		6
	3		7



The DIP switch 4 and 5 are for reservation, and should be in the status of OFF.

2.3.4 Factory Settings



If you power 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 Duress Report: N/A

CID Report:

- Account#1#2: No
- DIP Type: DTMF
- Remote Control Programming: No



For Detailed CID code, Please refer to CID Report.

Zone:

Zone 1to8: Real-time zone

Urgent Soft zone: Buzzing prompt sound

Test:

Testing Report Interval: N/A

Timing:

Entering Delay Duration: 10 sec

Exiting Delay 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.

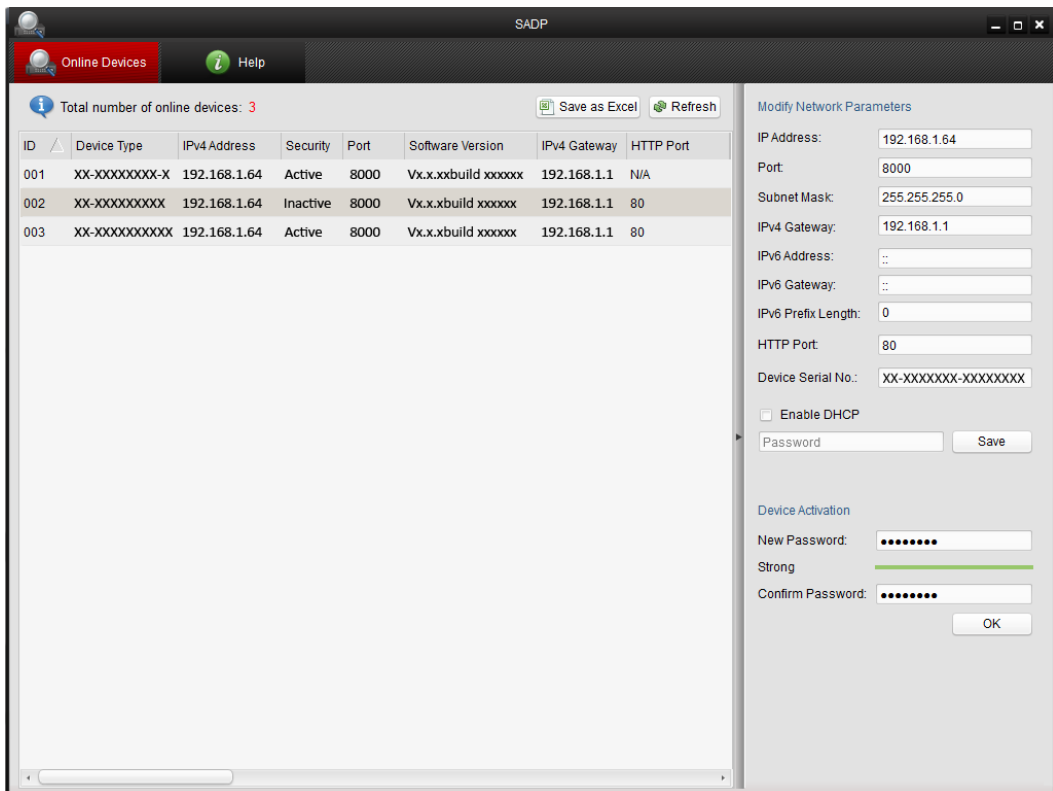
◆ **Activation via SADP Software**

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.

- 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.

- 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.

Modify Network Parameters

IP Address: 192.168.1.64

Port: 8000

Subnet Mask: 255.255.255.0

IPv4 Gateway: 192.168.1.1

IPv6 Address: ::

IPv6 Gateway: ::

IPv6 Prefix Length: 0

HTTP Port: 80

Device Serial No.: XX-XXXXXXX-XXXXXXX

Enable DHCP

Password Save

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

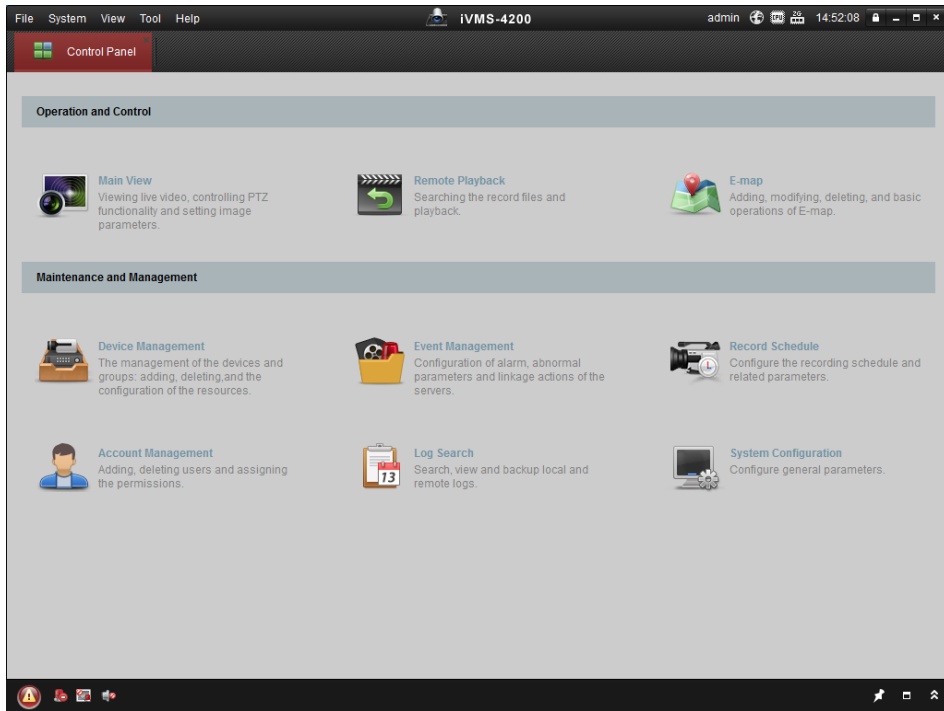
◆ Activation via Client Software

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

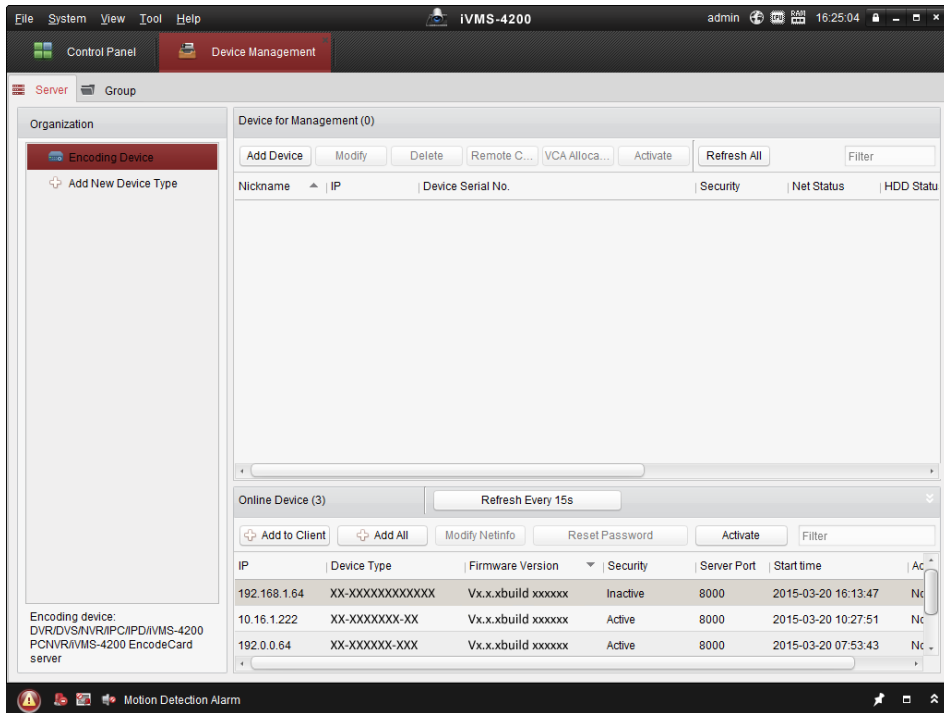
Get the client software from the supplied disk or the official website, and install the software according to the prompts. Follow the steps to activate the control panel.

Steps:

- 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.*

The screenshot shows a dialog box titled "Activation" with a close button (X) in the top right corner. It contains the following fields and text:

- User Name:** admin
- Password:** A text box containing eight black dots. Below it is a green progress bar that is nearly full, with the word "Strong" to its right.
- Instructions:** "Valid password range [8-16]. You can use a combination of numbers, lowercase, uppercase and special character for your password with at least two kinds of them contained."
- Confirm New Password:** A text box containing eight black dots.
- Buttons:** "Ok" and "Cancel" buttons at the bottom right.

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.

Modify Network Parameter

Device Information:

MAC Address: XX-XX-XX-XX-XX-XX

Software Version: Vx.x.xbuild xxxxxx

Device Serial No.: XX-XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Network Information:

DHCP

Port: 8000

IPv4(Enable)

IP address: 192.168.1.64

Subnet Mask: 255.255.255.0

Gateway: 192.168.1.1

IPv6(Disable)

Password:

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.
9. Input the password to activate your IP address modification.

Chapter 3 Keypad Operation (Local Operation)

3.1 Alarm Keypad Settings

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

012345 *0#
 ① ②

{1} Installer Password: 012345

{2} Command Key: *0 #



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.

000 012345 #
 ① ② ③

{1} Installer Password Programming Address: 000.

{2} Installer Password: The default password is 012345. The configured password cannot be NULL, but can be 0.

{3} End the command.

3.1.2 Operator Settings

The operator configuration programming command is shown below.

001 *2 1234 #
 ① ② ③ ④

{1} Operator Programming Address: 001~200.

{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	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 Bypass	8	Disarming No Arming/Disarming Report Bypass
9	Arming/Disarming No Arming/Disarming Report Bypass	*0	Arming Arming Report Bypass
*1	Disarming Disarming Report Bypass	*2	Arming/Disarming Arming/Disarming Report Bypass

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

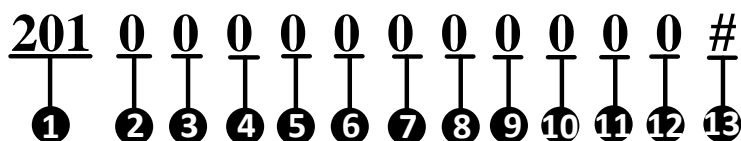
{4} End the command.



The user name 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 are all signified of deleting the user.

3.1.3 Zone Parameters Settings

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



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

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

{2} Zone Response Time. The 4 kinds of zone response time are 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	9	24-hour Auxiliary Zone
*0	24-hour Shock Alarm		

Command	Command Description	Command	Command Description
	Zone		

{4} Linked Trigger

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

{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	Not support	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

Command	Command Description
2	NO Type of Loop with Tampering Prevention Zone Loop



The fire alarm zone does 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	Linked Local 1 Alarm Output
2	Reserved	3	Reserved
4	Reserved	5	Reserved
6	Reserved	7	Reserved
8	Reserved	9	Reserved
*0	Reserved	*1	Reserved
*2	Reserved	*3	Reserved
*4	Reserved	*5	Reserved

{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 Description	Command	Command Description
0	No Tampering Prevention Recovery Report	1	With Tampering Prevention Recovery Report

{12} Selection of the tamper-proof EOL resistance.

Command	Command Description	Command	Command Description
0	2.2KΩ	1	3.3KΩ

Command	Command Description	Command	Command Description
2	4.7KΩ	3	5.6KΩ
4	8.2KΩ		

{13} End the command. .

3.1.4 Zone Linked Trigger Settings

The detailed programming command is shown below.

467 000 0 00 #

1
2
3
4
5

{1} Trigger Settings Programming Address: 467

{2} Zone No.

{3} Adding/Deleting 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.}+{#}.

3.1.5 Trigger Event Linkage Settings

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

468 00 0 00 00 #

1
2
3
4
5
6

{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} Adding /Deleting 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
00	None	03	Reserved
01	AC Power Down	04	Wired Network Exception
02	Low Battery	05	No Network Exception

The system event command is shown below.

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

{6} End the command.



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

3.1.6 Trigger Time Settings

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

470
00
00
00

①
②
③
④
⑤

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



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} + {#}

3.1.7 Siren Settings

For siren configuration, please refer to the command below.

471
1

①
②
③

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

Command	Command Description	Command	Command Description
0	Disable	1	Enable

- {3} End the command.

3.1.8 Control Panel Time Settings

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

472 2013 01 01 08 00 00 #

1
2
3
4
5
6
7
8

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

3.1.9 Control Panel IP Settings

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

473 192 000 000 064 #

1
2
3
4
5
6

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



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

3.1.10 Local Port Number Settings

The programming commands of local port number setting are as below:

<u>4</u>	<u>7</u>	<u>4</u>	<u>0</u>	<u>8</u>	<u>0</u>	<u>0</u>	<u>0</u>	<u>#</u>
1	2	3	4	5	6	7		

- {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: Digit
- {7} End the command.



Corresponding port number must be 5 bytes. 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#.

3.1.11 Sub-net Mask Settings

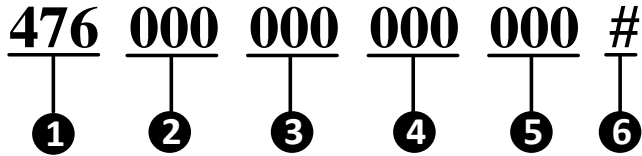
The programming commands of control panel sub-net mask setting are as below:

<u>4</u>	<u>7</u>	<u>5</u>	<u>2</u>	<u>5</u>	<u>2</u>	<u>5</u>	<u>2</u>	<u>5</u>	<u>0</u>	<u>0</u>	<u>0</u>	<u>#</u>
1	2	3	4	5	6							

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

3.1.12 Gateway Settings

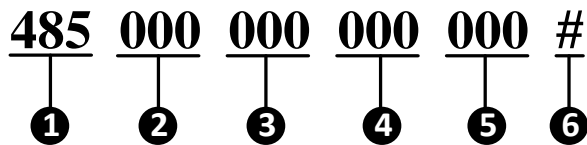
The programming commands of control panel gateway setting are as below:



- {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.

3.1.13 Uploading Center IP Settings

The programming commands of uploading center IP setting are as 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 Setting	488	Programming Address of Network Center 2 IP Setting
491	Programming Address of WIFI Center 1 IP Setting	494	Programming Address of WIFI Center 2 IP Setting

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



This function varies depending on the models of the control panel.

3.1.14 Uploading Center Port Settings

The programming commands of uploading center port setting are as below:

486 00000 #
1 2 3

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

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

{2} Port Number;

{3} End the command.

3.1.15 Center Protocol and Account Settings

The programming commands of center protocol and account setting are as below:

487 2 000000000 #
1 2 3 4

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

Command	Description	Command	Description
487	Network Center 1 Protocol and Programming Address of Account Setting	490	Network Center 2 Protocol and Programming Address of Account Setting

Command	Description	Command	Description
493	GPRS Center 1 Protocol and Programming Address of Account Setting	496	GPRS Center 2 Protocol and Programming Address of Account Setting

{2} Protocol Type:

Command	Description	Command	Description
1	HIK	2	NAL2300

{3} Account (control panel No., 6~9 digits);

{4} End the command.

3.1.16 Printer Parameters Settings

The programming commands of printer parameters setting are as below:

499 0 0 0 #
 ────┬───┬───┬───┬───
 1 2 3 4 5

{1} The programming command address of printer parameter setting is:499;

{2} Enable/disable the printer;

Command	Description	Command	Description
0	Disable the Printer	1	Enable the Printer

{3} Enable/disable the off-line detection of printer;

Command	Description	Command	Description
0	Disable the Off-line Detection of Printer	1	Enable the Off-line Detection of Printer

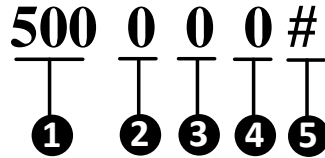
{4} Whether to print the reporting time or not, known as the time of control panel when event/alarm occurs;

Command	Description	Command	Description
0	Not print the reporting time	1	Print the reporting time

{5} End of the command.

3.1.17 Alarm Message Settings

The programming commands of print setting of alarm message are as below:



{1} The programming command address of alarm message printing is: 500.

{2} Enable/disable the sensor alarm;

Command	Description	Command	Description
0	Disable Sensor Alarm	1	Enable Sensor Alarm

{3} Enable/disable emergency alarm;

Command	Description	Command	Description
0	Disable Emergency Alarm	1	Enable Emergency Alarm

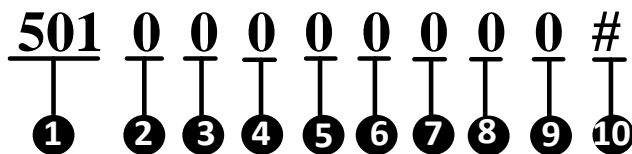
{4} Enable/disable duress alarm;

Command	Description	Command	Description
0	Disable Control Panel Duress Alarm	1	Enable Duress Alarm

{5} End the command.

3.1.18 Device Information Settings

The programming commands of print setting of device information are as below:



{1} The programming command address of device information printing is: 501.

{2} AC Power Off;

{3} The storage battery is under voltage;

{4} Reserved, enter 0;

{5} Test Report;

- {6} Tamper-proof of the Control Panel;
- {7} The 485 device is off-line;
- {8} Network error;
- {9} GPRS exception.

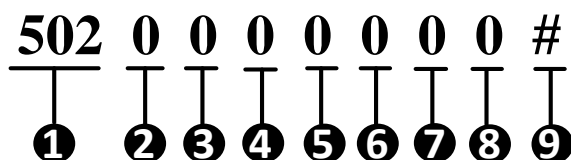
It indicates disabled status when 2) ~9) are set to be 0, and indicates enabled status when 2) ~9) are set to be 1.

Command	Description	Command	Description
0	Disabled	1	Enabled

{10} End of the command.

3.1.19 Operation Programming Information Settings

The programming commands of print setting of operation programming information are as below:



- {1} The programming command address of print setting of operation programming information is: 502;
- {2} Arming;
- {3} Disarming;
- {4} Canceling the alarm;
- {5} Bypass;
- {6} Enter the programming;
- {7} Exit the programming;
- {8} Control Panel Restoring;

It indicates disabled status when 2) ~8) are set to be 0, and indicates enabled status when 2) ~8) are set to be 1.

Command	Description	Command	Description
0	Disabled	1	Enabled

{9} End the command.

3.1.20 Restoring Information of Alarm and Bypass Settings

The programming commands of print setting of restoring information of alarm and bypass are as below:

503 0 0 #
 ────┬───┬───┬───┬───
 │ │ │ │ │
 ① ② ③ ④

{1} The programming command address of print setting of restoring information of alarm and bypass is: 503;

{2} Sensor Alarm Recovering;

Command	Description	Command	Description
0	Disabled	1	Enabled

{3} Bypass Recovering;

Command	Description	Command	Description
0	Disabled	1	Enabled

{4} End the command.

3.1.21 Device Recovering Information Settings

The programming commands of print setting of device recovering information are as below:

504 0 0 0 0 0 0 0 #
 ────┬───┬───┬───┬───┬───┬───┬───┬───
 │ │ │ │ │ │ │ │
 ① ② ③ ④ ⑤ ⑥ ⑦ ⑧ ⑨

{1} The programming command address of print setting of device recovering information is: 504;

{2} AC power on;

{3} The storage battery is not under voltage;

{4} Reserved, enter 0;

{5} The tamper-proof of the control panel is recovered;

{6} The 485 device is on-line;

{7} The network error is recovered;

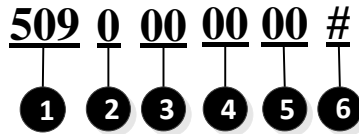
{8} The GPRS exception is recovered.

It indicates disabled status when 2) ~8) are set to be 0, and indicates enabled status when 2) ~8) are set to be 1.

Command	Description	Command	Description
0	Disabled	1	Enabled

{9} End of command.

3.1.22 Siren Linked Event Settings



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

{2} Add/Delete Event Settings

Command	Description	Command	Description
0	Delete Event	1	Add Event

{3} Event Type

Command	Description	Command	Description
00	Global Event	01	Partition System 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 system event types are shown below.

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

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

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

{6} End the command.

3.1.23 Emergency Alarm Linkage Siren Setting

The programming commands of emergency alarm linkage siren setting are as below:

510 00 0 #
 ────┬───┬───┬───
 │ │ │ │
 ① ② ③ ④

- {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.

3.1.24 Control Panel Tamper-proof Linked Siren Settings

The programming commands of control panel tamper-proof disconnecting linkage siren setting are as below:

511 0 #
 ────┬───┬───
 │ │ │
 ① ② ③

{1} The programming command address of control panel tamper-proof disconnecting linkage siren is: 511;

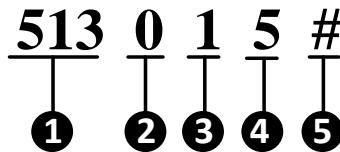
{2} It indicates whether to link the siren or not;

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

{3} End the command.

3.1.25 Testing Report Settings

The testing report is used to validate the communication of control panel and alarm center. The detailed operation is show as follows.



{1} Testing Report Programming Address: 513

{2} Enable/Disable the testing report

Command	Command Description	Command	Command Description
0	Disable	1	Enable

{3} Timer of the testing report. It indicates the time of firstly sending the test report. The initial value is the time of enabling the test 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
8	10H	*2	18H
9	12H	*3	20H

Command	Command Description	Command	Command Description
*0	14H	*4	22H
*1	16H	*5	24H

{4} Testing Report Sending Interval

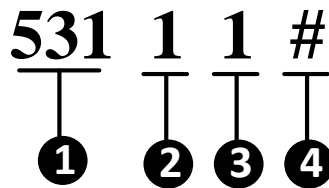
Command	Command Description	Command	Command Description
1	1H	6	2D
2	2H	7	3D
3	4H	8	5D
4	12H	9	7D
5	24H		

{5} End the command

3.1.26 Partition Settings

Partition Start-up Settings

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.



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

Partition Keypad User Settings

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

531 2 0 000 #
1 2 3 4 5

- {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



- **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 Settings

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

531 3 0 000 #
┆ ┆ ┆ ┆ ┆
┆ ┆ ┆ ┆ ┆
1 2 3 4 5

- {1} The programming command address of 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.



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 Settings**.

Partition Keypad Settings

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

531 4 0 00 #
┆ ┆ ┆ ┆ ┆
┆ ┆ ┆ ┆ ┆
1 2 3 4 5

- {1} The programming command address of zone configuration is 531~538.
- {2} The configuration item of 4 indicates keypad configuration.
- {3} Add/Delete Keypad

Command	Command Description	Command	Command Description
0	Delete	1	Add

{4} Keypad No.

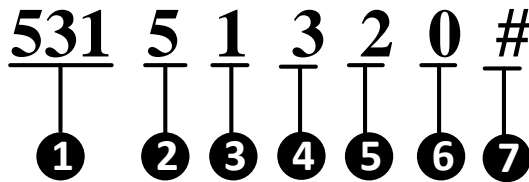
{5} End the command.



There are three mode to add/delete zones for the partition , adding/deleting separately, adding/ deleting continually and adding/deleting in batch, for details, refer to the **Partition Keypad User Settings**.

Partition Time and Control Panel Duress Report Settings

To configure the system time and control panel duress report, please see the command below.



{1} System Time and Control Panel Duress Report Programming Address: 531

{2} Classification Option of System Time and Control Panel Duress 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
---------	---------------------	---------	---------------------	---------	---------------------

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 duress Report

Command	Command Description	Command	Command Description
0	Disable	1	Enable

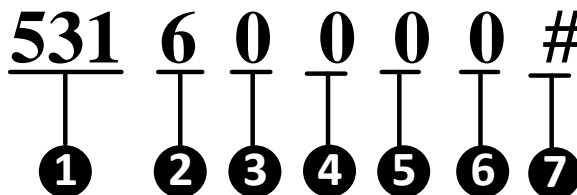
{7} End the command.



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

Partition Report and Arming Prompt Sound Settings

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 Settings

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

531
7
1
1
1
1
#

1
2
3
4
5
6
7

- {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.



The operation permission of all key zones in each partition is configured by this command.

3.1.27 Control Panel System Fault Detection Settings

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

564 1 1 1 1 1 1 1 #
 ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓
① ② ③ ④ ⑤ ⑥ ⑦ ⑧ ⑨

- {1} Control panel system fault detection address: 564.
- {2} Ac Power Down
- {3} Low Battery
- {4} Control Panel Tampering Alarm
- {5} Reserved, enter 0.
- {6} Main keypad Disconnection
- {7} Network Exception
- {8} Wireless Network Exception

Command	Command Description	Command	Command Description
0	Disable	1	Enable

- {9} End the command.



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

3.1.28 Partition Fault Display Settings

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

567 01 01 1 1 1 1 1 1 1 #
 ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓
① ② ③ ④ ⑤ ⑥ ⑦ ⑧ ⑨ ⑩ ⑪

- {1} Partition fault display configuration Programming address: 567.
- {2} The Tens' Digit of the Partition System No.
- {3} The Units' Digit of the Partition System No.
- {4} Ac Power Down

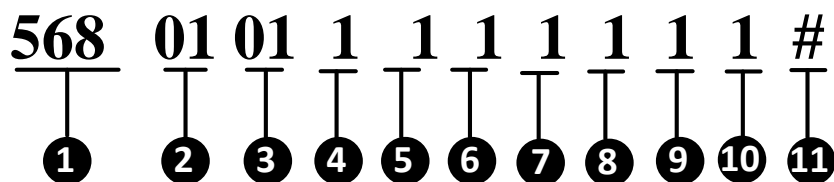
- {5} Low Battery
- {6} control panel Tampering Alarm
- {7} Reserved, enter 0
- {8} Main keypad Disconnection
- {9} Network Exception
- {10} GPRS Exception

Command	Command Description	Command	Command Description
0	Disable	1	Enable

{11} End the command.

3.1.29 Partition Fault Prompt Sound Settings

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

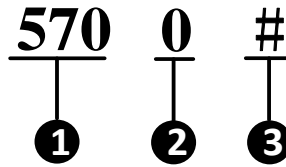


- {1} Partition fault display configuration Programming address: 568.
- {2} The Tens' Digit of the Partition System No.
- {3} The Units' Digit of the Partition System No.
- {4} Ac Power Down
- {5} Low Battery
- {6} Control Panel Tampering Alarm
- {7} Phone Line Disconnection
- {8} Main keypad Disconnection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

Command	Command Description	Command	Command Description
0	Disable	1	Enable

3.1.30 DHCP Settings

To enable the DHCP, please refer to the command below.



{1} The DHCP configuration address is 570

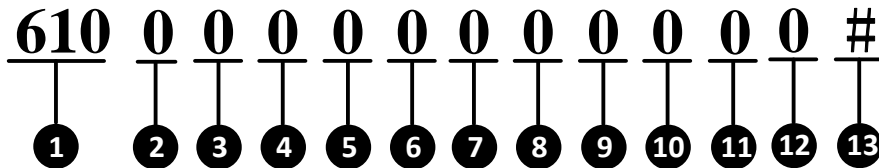
{2} Enable DHCP function?

Command	Description	Command	Description
0	Disable	1	Enable

{3} End the command.

3.1.31 Delay Zone Time Settings

The programming command of configuring zone time is shown below.



{1} The configuration address of delay zone time settings is 610.

{2} The hundreds's digit of the zone No.

{3} The tens' digit of the zone No.

{4} The units' digit of the zone No.

{5} The thousands' digit of the delay exiting time

{6} The hundreds's digit of the delay exiting time

{7} The tens' digit of the delay exiting time

{8} The units' digit of the delay exiting time

{9} The thousands' digit of the delay entering time

{10} The hundreds's digit of the delay entering time

{11} The tens' digit of the delay entering time

{12} The units' digit of the delay entering time

{13} End the command

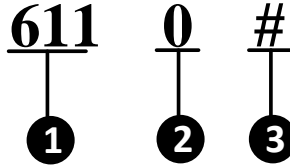


The range of zone No. is 1 to 8/16.

The range of entering/exiting delay time is 1 to 5999s.

3.1.32 Center Group Enabling Settings

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



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

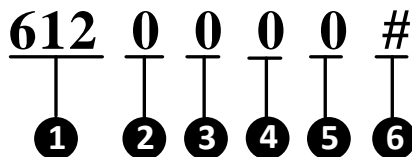
{3} End the command.



This the number of center groups varies depending on the models of the control panel.

3.1.33 Center Group Uploading Mode Settings

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 video 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,

This the number of center groups varies depending on the models of the control panel.

3.1.34 Center Group Zone Alarm Report Settings

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

613 0 000 #
 ↓ ↓ ↓ ↓
① ② ③ ④

{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 Programming address	625	Center group 4 zone alarm report 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.



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

3.1.35 Center Group Non-zone Alarm Report Settings

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

614 1 1 1 1 1 1 1 1 1 1 #
 ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓
① ② ③ ④ ⑤ ⑥ ⑦ ⑧ ⑨ ⑩ ⑪ ⑫

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

Command	Command Description	Command	Command Description
614	Center Group1 Non-zone	618	Center Group 2Non-zone

Command	Command Description	Command	Command Description
	Alarm Report Programming Address		Alarm Report Programming Address
622	Center Group3 Non-zone Alarm Report Programming Address	626	Center Group 4 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 Duress Report
- {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.

3.1.36 White-list Parameters Settings

Non-zone Alarm Report Settings

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

680 00 0 0 0 0 0 0 0 0 0 0 0 #

1
2
3
4
5
6
7
8
9
10
11
12
13
14

- {1} Non-zone Alarm Report Settings Command Address: 680.
- {2} It indicates the white list number. 01~08 indicate white list No.1~No.8.
- {3} It indicates to 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 Duress 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 Settings

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

681 00 0 0 0 0 0 0 0 0 #

↓↓↓↓↓↓↓↓↓↓↓

①②③④⑤⑥⑦⑧⑨⑩⑪

- {1} Partition Arming Permission Settings Command Address: 681
- {2} It indicates the 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} It indicates to enable/disable the permission of Partition Arming.

Command	Command Description	Command	Command Description
0	Disable	1	Enable

{11} End the command.

Partition Disarming Permission Settings

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

682 00 0 0 0 0 0 0 0 0 #
1 2 3 4 5 6 7 8 9 10 11

{1} Partition Disarming Permission Settings Command Address: 682

{2} It indicates the 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} It indicates to enable/disable the permission of Partition Disarming.

Command	Command Description	Command	Command Description
0	Disable	1	Enable

{11} End the command.

Partition Alarm Clearing Permission Settings

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

683 00 0 0 0 0 0 0 0 0 #
1 2 3 4 5 6 7 8 9 10 11

- {1} Partition Alarm Clearing Permission Settings Command Address: 683
- {2} It indicates the 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} It indicates to 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 White-list Settings

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

684 01 0 0 0 0 0 #
1 2 3 4 5 6 7 8

- {1} The interval time of White List Settings Command Address: 684.
- {2} It indicates the white list number. 01~08 indicate white list No.1~No.8.
- {3} It indicates the interval time. The command is shown below.

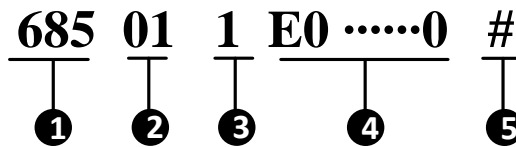
Command	Description	Command	Description
0	0s	4	5min

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

- {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.

Telephone Number Settings

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



- {1} Telephone Number Command Address: 685.
- {2} It indicates the white list number. 01~08 indicate white list No.1~No.8.
- {3} Telephone 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 bytes.



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

- {5} End the command.

Zone Report Type Settings

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

686 01 0 0 0 0 #

- {1} Zone Report Type Settings Command Address: 686.
- {2} It indicates the 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



- 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 6860116#.
- 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.



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

3.1.37 Schedule Settings

Enabling Weekly Schedule

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

690 01 0 0 #
 ┆ ┆ ┆ ┆ ┆
1 2 3 4 5

- {1} Enabling Weekly Schedule Command Address: 690.
- {2} It indicates the partition number. 01~08 indicate partitions No.1~No.8.
- {3}

Command	Command Description	Command	Command Description
0	Not mandatory	1	Mandatory

- {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 Settings

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

691 01 1 1 0 0 0 0 0 0 0 0 E #
 ┆ ┆ ┆ ┆ ┆ ┆ ┆ ┆ ┆ ┆ ┆ ┆ ┆ ┆
1 2 3 4 5 6 7 8 9 10 11 12 13 14

- {1} Weekly Schedule Time Parameter Settings Command Address: 691.
- {2} It indicates the partition number. 01~08 indicate partitions No.1~No.8.
- {3} Day of the Week

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

- {4} It presents the 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}



- 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 later 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
A	General Arming\
B	Instant Arming
C	Stay Arming
D	Disarming

{14} End the command.

Copy 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.

692 01 0 0 #
 ────┬───┬───┬───┬───
 | | | | |
 ① ② ③ ④ ⑤

- {1} Copy Weekly Schedule Command Address: 692.
- {2} It indicates the 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
1	Monday	5	Friday
2	Tuesday	6	Saturday
3	Wednesday	7	Sunday
4	Thursday		

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

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

{5} End the command.

Copy Weekly Schedule of Partition

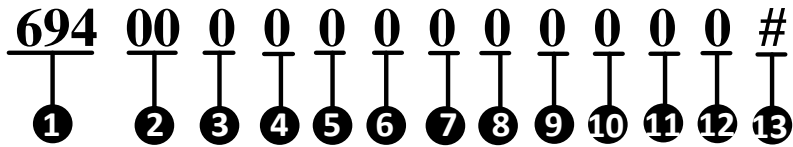
To copy the settings of partition (m) to partition (n), please refer to the command below.

693 01 02 #
 ① ② ③ ④

- {1} Copy Weekly Schedule of Partition Command Address: 693.
- {2} It indicates the partition (m) number. 01~08 indicate partitions No.1~No.8.
- {3} It indicates the partition (n) number. 01~08 indicate partitions No.1~No.8.

Prior Schedule Date Parameter Settings

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



- {1} Prior Schedule Date Parameter Settings 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.

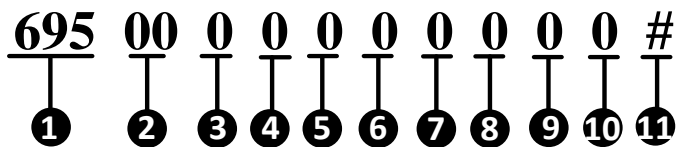
Start Date: {5}{6}/{7}{8}. The former is the month (value range 1~12), while the latter is the day (value range 1~30).

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 Settings

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

696 **00** **0** **0** **0** **0** **0** **0** **0** **0** **0** **E** **#**
 ┆ ┆ ┆ ┆ ┆ ┆ ┆ ┆ ┆ ┆ ┆ ┆ ┆
1 **2** **3** **4** **5** **6** **7** **8** **9** **10** **11** **12** **13**

{1} Prior Schedule Time Parameter Settings 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}



- 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
A	General Arming
B	Instant Arming
C	Stay Arming
D	Disarming
E	None

{13} End the command.

Enabling Trigger Schedule

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

697 0 #
 | | |
1 **2** **3**

{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 Settings

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

698 0 0 0 0 #
 | | | | | |
1 **2** **3** **4** **5** **6**

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

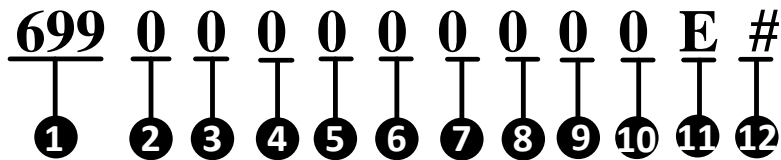
{2} It indicates to delete/add the trigger schedule.

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 Settings

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



- {1} Trigger Schedule Time Parameter Settings 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.

3.1.38 Wireless User Permission Settings

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

701 1 1 1 1 1 #

 ↓ ↓ ↓ ↓ ↓ ↓ ↓
① ② ③ ④ ⑤ ⑥ ⑦

{1} Wireless User Permission Settings 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.



This function varies depending on the models of the control panel.

3.1.39 Video Live View Settings

To enable the video live view, Please refer to the command below.

$\underline{801} \quad \underline{1} \quad \underline{1} \quad \underline{1} \quad \underline{1} \quad \underline{\#}$
 $\downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow$
① ② ③ ④ ⑤ ⑥

{15} Video Live View Settings Programming Address:801

{2}~{5}Set the value as 1 to enable the live view.

Command	Command Description	Command	Command Description
0	Disable	1	Enable

{6} End the command.

3.2 Keypad Alarm Operation Code

3.2.1 Device Initialization

Video security control panel can be recovered through the alarm keypad initialization; see the command below.

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



The default password for the installer: 012345.

3.2.2 Security control panel Arming and Disarm

The operation of security 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

$$\{\text{User password}\} + \{\text{bypass}\} + \{\text{zone Number}\} + \{#\}$$

For continuous bypass/ recovery; see the command below:

$$[1234] + [\text{Bypass}] + [1] + [\#] \underbrace{[\text{Bypass}] + [2] + [\#] \dots [\text{Bypass}] + [8] + [\#]}_{15 \text{ Seconds}}$$


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.

$$\{\text{User Password}\} + \{*\} + \{4\} + \{1\} + \{#\}$$

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 re-validated. See the command below.

$$\{\text{User Password}\} + \{*\} + \{4\} + \{2\} + \{#\}$$

3.2.7 Keypad Cancel Alarm

When the alarm is triggered, it can be canceled by the 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): {User 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 security control panel supports 16 channels of alarm outputs, the N valuation should be 1-16.

3.2.9 Emergency Alarm

Press the {Emergency} 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	Device Disconnection
2	Low Battery	6	Network

Serial Number	Meaning	Serial Number	Meaning
			Disconnection
3	Tampering Alarm Enabling	7	3G Exception
4	Telephone line Disconnection		

3.2.11 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 bytes, such as 002.

3.2.12 Entering Partition System

See the command below to enter the partition system.

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

3.2.13 Control Panel Programming Operation

The security 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. Security control panel configuration operation (see section 3.1)
3. Exit programming mode; see the command below:
{*} + {#}

3.2.14 Alarm Center Test

Partition keypad operation is used to test the communication between security 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 security control panel and center after installing the system or during the inspection.

3.2.15 Project Mode

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

{password} + {engineering} + {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 test dialing center is in dialing status.

3.2.16 Enabling/Disabling Key Tone

For keypad tone status switch, see the command below:

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

3.2.17 Connecting Wireless Device and Control Panel

If the control panel and keypad are both working properly, enter the following code with the keypad to enter the connecting mode.

[Password] + [*] + [91] + [No.] + [#]

Press any key to exit the mode after connecting succeeded.

The range of No. is 01~32, which indicates 32 wireless devices.

3.2.18 Deleting Connected Wireless Device

Enter the following code with the keypad to delete the device associated to the wireless user No..

[Password] + [*] + [90] + [No.] + [#]

3.2.19 Deleting All Wireless Devices Connected to the Control Panel

Enter the following code with the keypad to delete the all devices **connected to the control panel**.

[Password] + [*] + [92] + [#]

3.2.20 Setting the Schedule

Resetting Intraday Schedule

To update the intraday preferential schedule and weekly schedule, refer to the code below.

[Installer Password] + [*] + [8] + [1] + [#]

Clearing Weekly Schedule

[Installer Password] + [*] + [8] + [2] + [#]

Clearing Preferential Schedule

[Installer Password] + [*] + [8] + [3] + [#]

3.2.21 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.

3.2.22 Disabling LCD Backlight

For Disabling the LCD backlight, see the command below:

{*} + {8} + {#}

3.2.23 Pacing

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

{Password} + {*} + {6} + {0} + {#}



- 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.

3.2.24 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 security 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.


Chapter 4 Accessing by Client Software

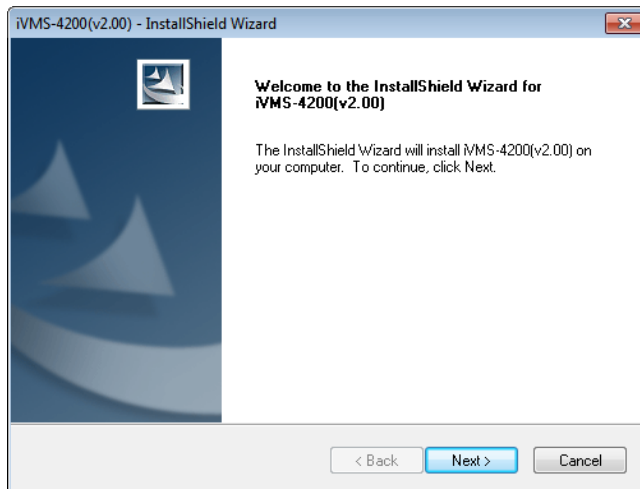
Check the package contents and make sure that the device in the package is in good condition and all the assembly parts are included.

4.1 Installing the iVMS-4200

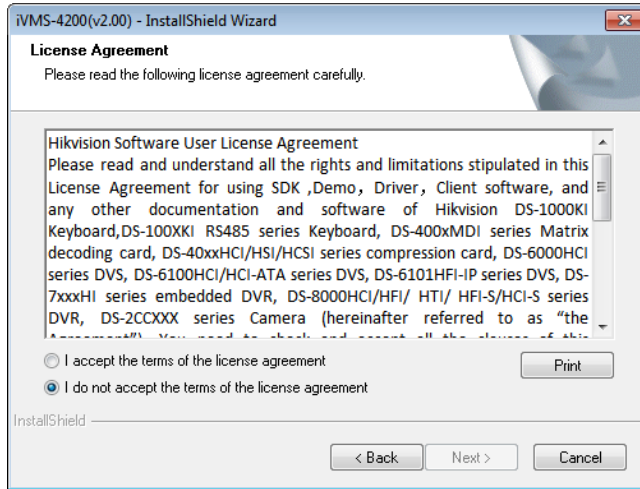
Insert the installation media of iVMS-4200 into the appropriate computer.

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.

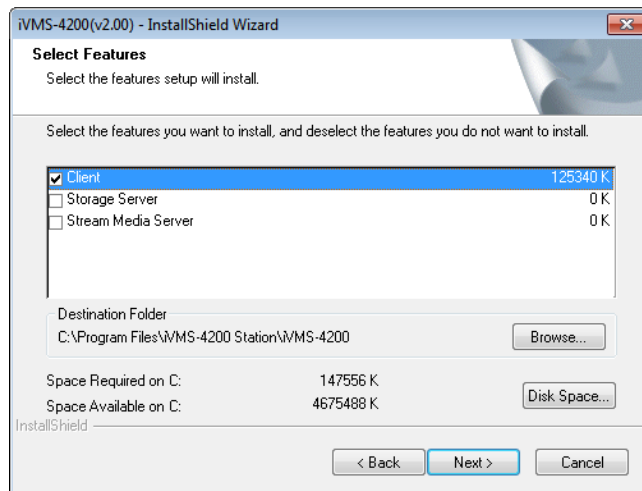


If you accept the terms of the license agreement, click I accept the terms of license agreement.

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.

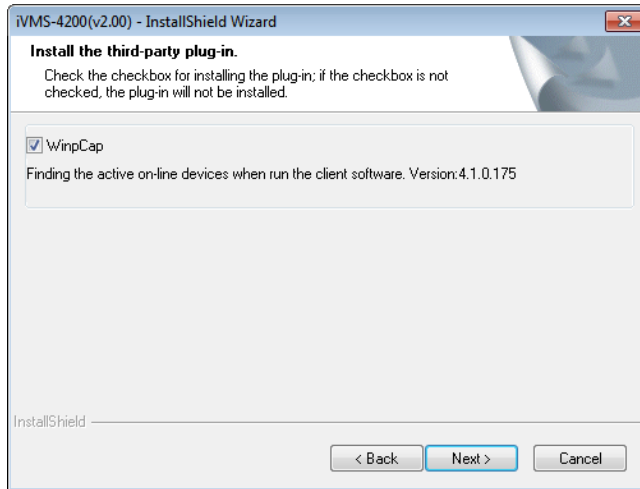


The default directory is *C:\Program Files\iVMS-4200 Station\iVMS-4200*.

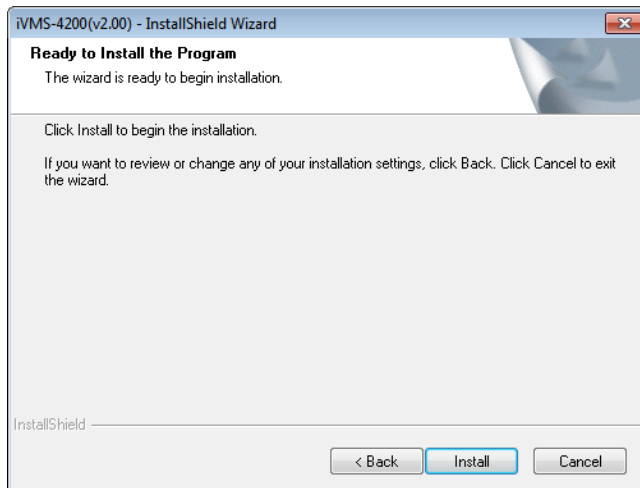
Click **Next** to continue.

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

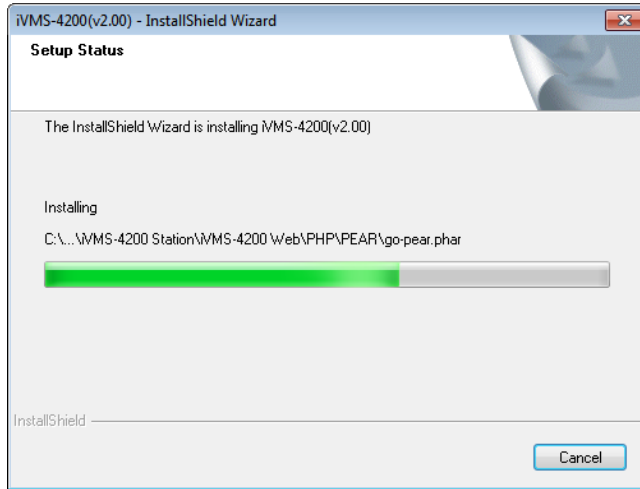
software.



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

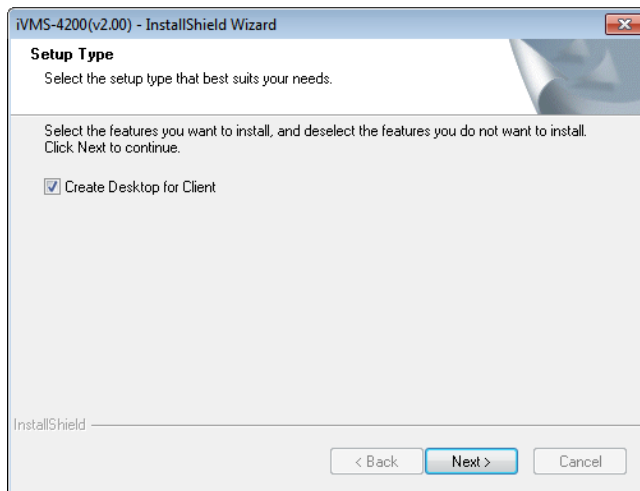


3. A panel indicating progress of the installation is displayed. A percentage completion bar is updated as the installation progresses.

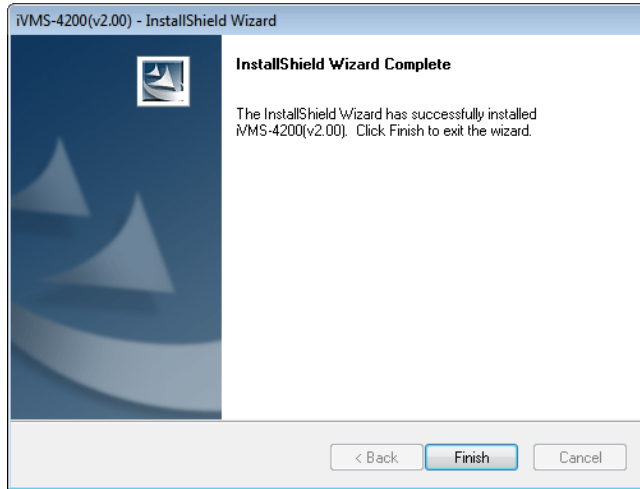


4. Select the setup type according to your need.

You can check the checkbox of **Create Desktop for Client** to create a shortcut icon on the desktop for the client software.



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

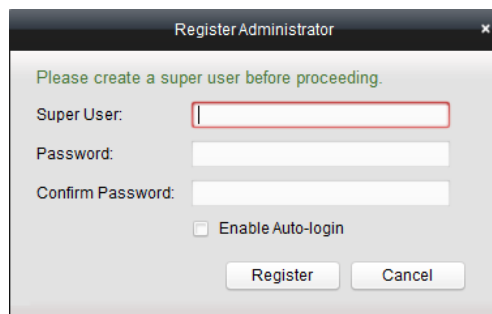


4.2 User Registration and Login

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 Video 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,

Adding/Editing/Deleting 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.

Modify

Adding Mode:

IP/Domain IP Segment IP Server HIDDNS

Nickname: video alarm

Address: 10.16.37.248

Port: 8000

User Name: admin

Password: ••••••

Modify Cancel

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

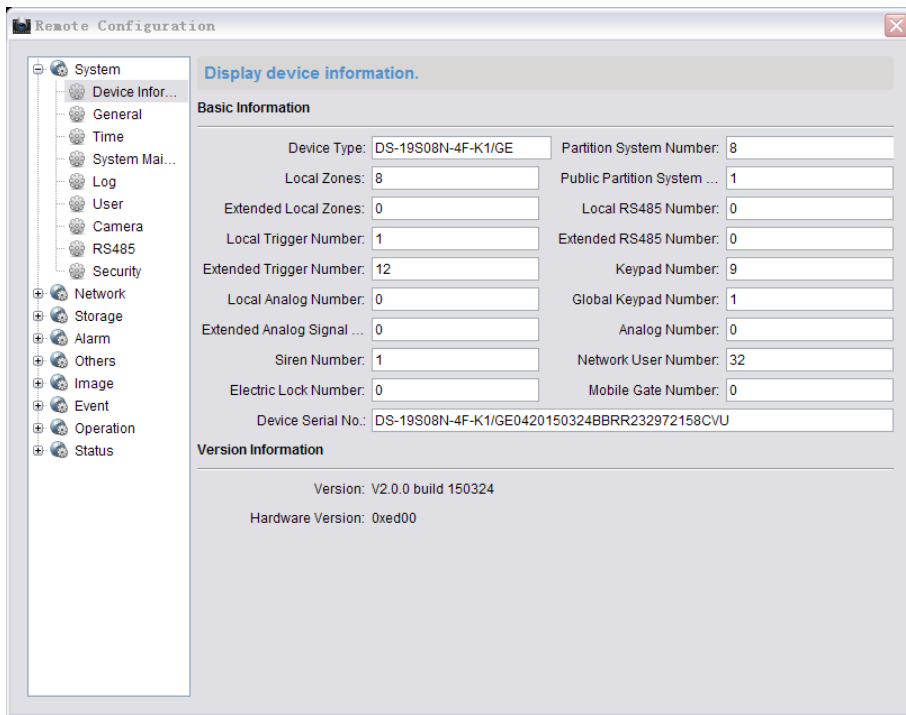
Select device from the list, click **Modify/Delete**, and then you can modify/delete the information of the selected device.

4.4 Remote Settings

Purpose:

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

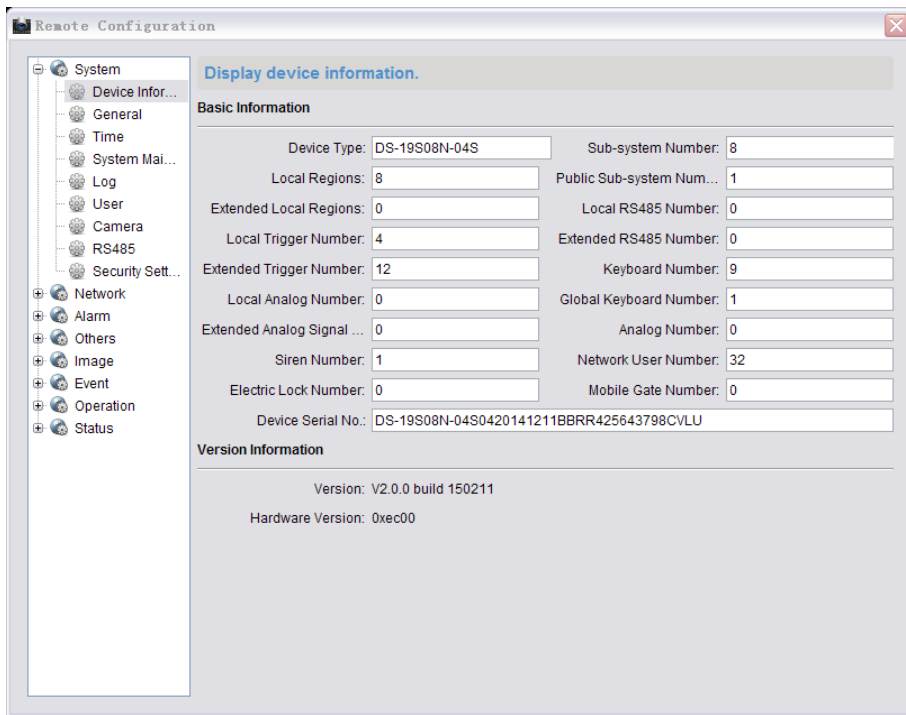
Click the **Remote Settings** button to enter the interface.



System Information Settings

Purpose:

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

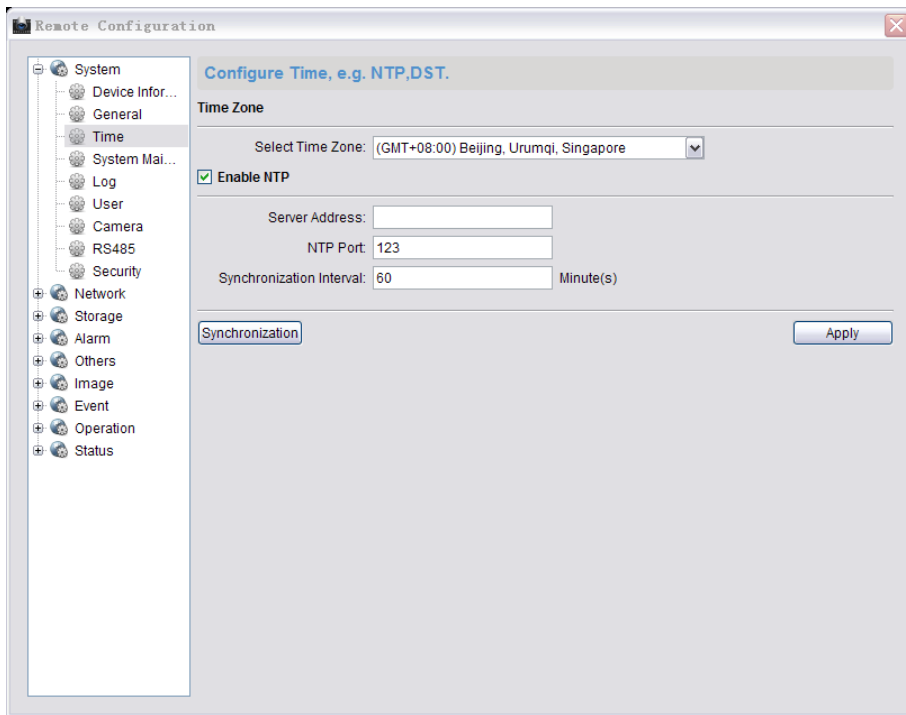


Timing Settings

Before You Start:

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

Enter **Remote Settings>System->Time** to get the configuration page.



User Settings

Purpose:

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

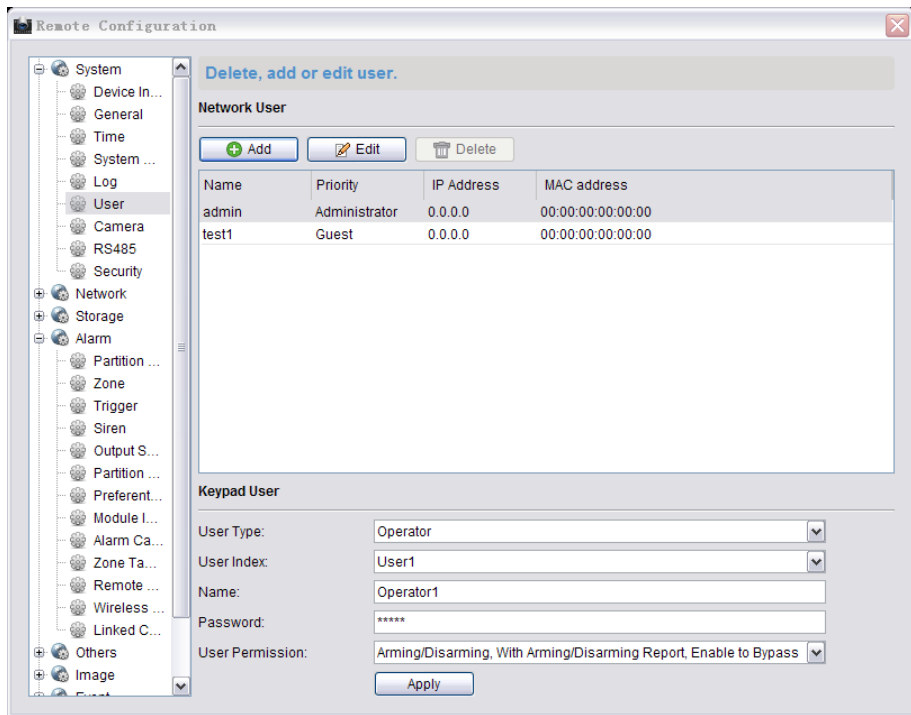
● **Network User**


Add a Network User

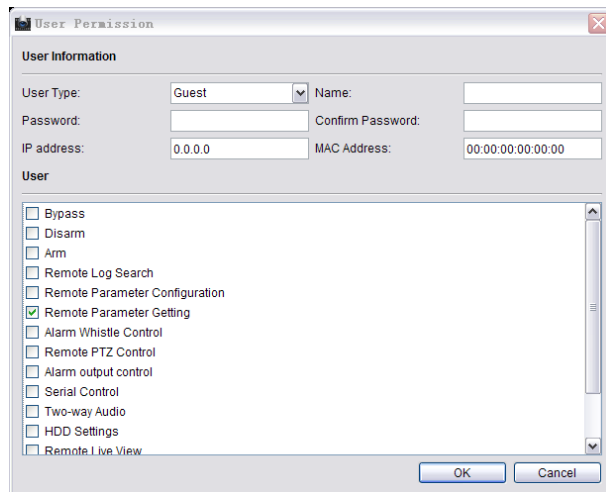
Steps:

1. Enter the user configuration interface.

Remote Settings->System->User



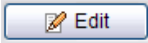
2. Click  to enter the interface of adding a network user.

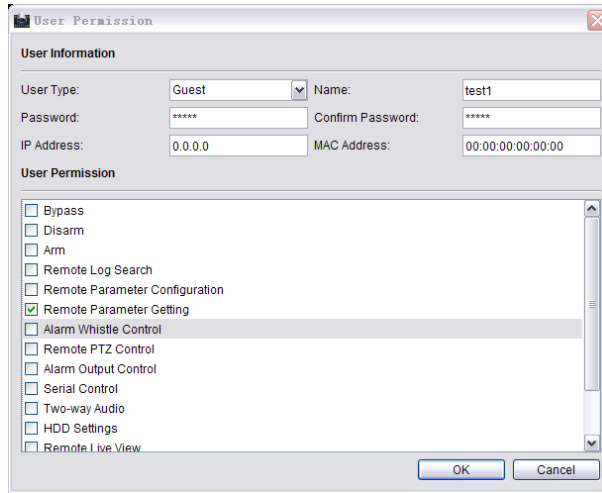


3. Enter the corresponding user information including the user type, user name, password, IP address, and MAC address.
4. Select the permission of the user.
5. Click **OK** to finish the settings.

Edit a User

Steps:

1. Click  to enter the interface of editing the selected user



The image shows a 'User Permission' dialog box with the following fields and options:


- User Information:**
 - User Type: Guest (dropdown)
 - Name: test1
 - Password: *****
 - Confirm Password: *****
 - IP Address: 0.0.0.0
 - MAC Address: 00:00:00:00:00:00
- User Permission:**
 - Bypass
 - Disarm
 - Arm
 - Remote Log Search
 - Remote Parameter Configuration
 - Remote Parameter Getting
 - Alarm Whistle Control
 - Remote PTZ Control
 - Alarm Output Control
 - Serial Control
 - Two-way Audio
 - HDD Settings
 - Remote Live View

Buttons: OK, Cancel

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.

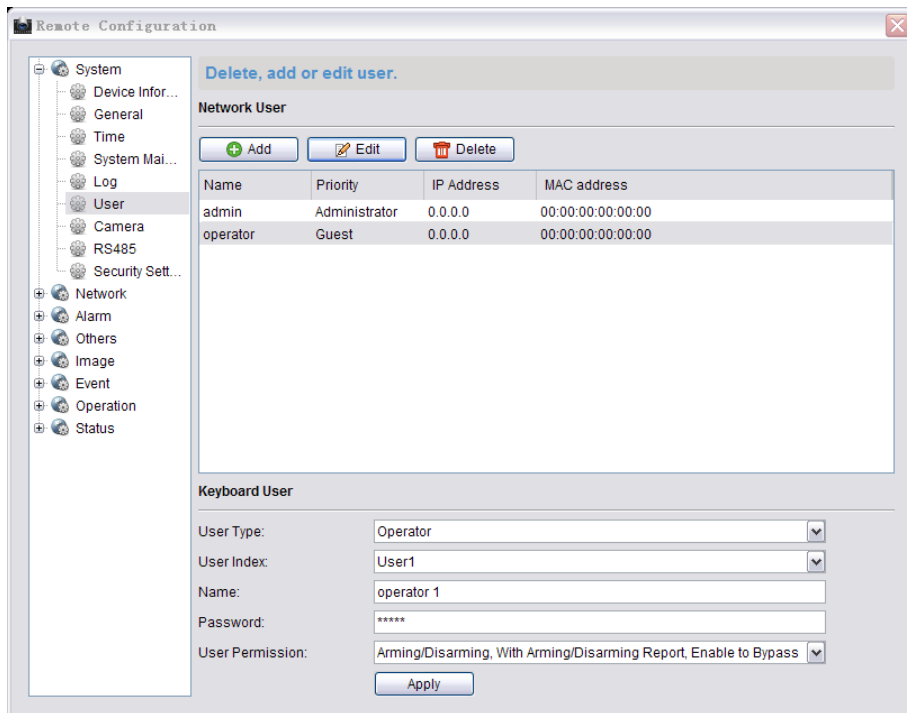
Delete a user

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.

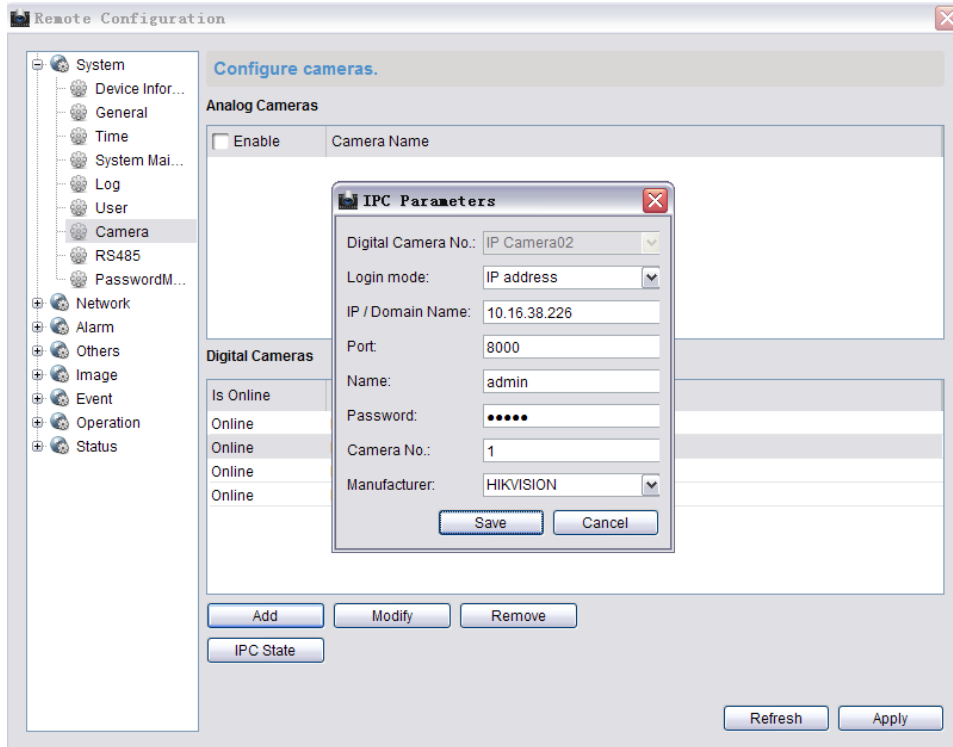
Camera Settings

You can select to enable analog camera or add, edit, remove, and view status of network camera in this section.

Steps:

1. Enter the general camera configuration page.

Remote Settings-> System ->Camera



2. Click **Enable** to enable the analog camera.
3. Click Add to enter the network camera adding interface.
4. Select the login mode, enter information such as IP address or domain name, port No., name, password and so on.
5. Click Save to save the settings.
6. You can also click **Modify** or **Remove** to edit or delete the camera.

Network Settings

Purpose:

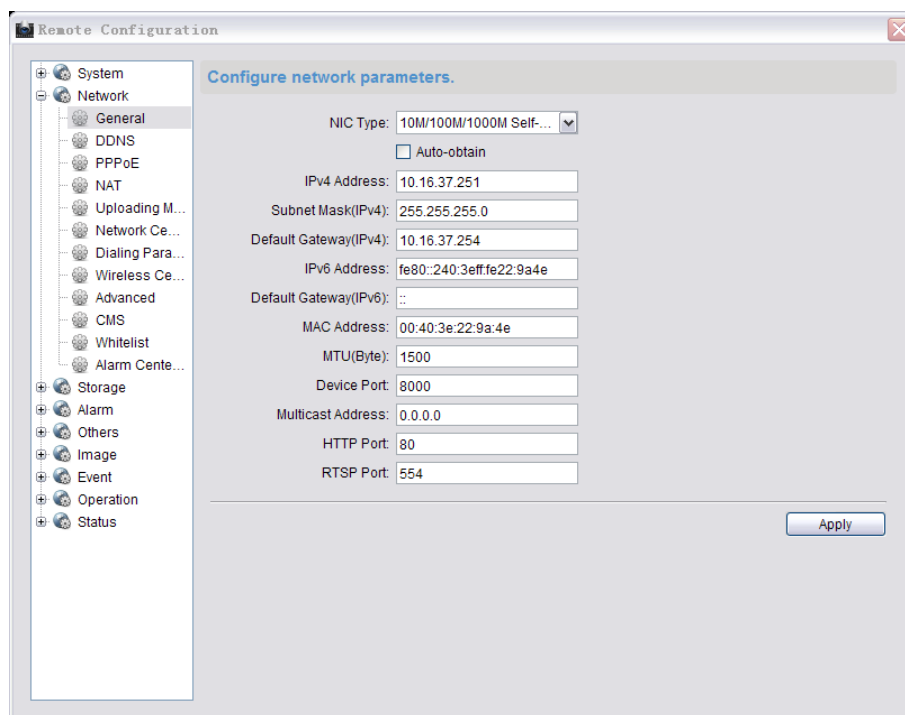
You can edit the general network parameters in this section.

- **General Network Parameters Settings**

Steps:

7. Enter the general network configuration page.

Remote Settings-> Network->General



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



- 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 Settings**

Purpose:

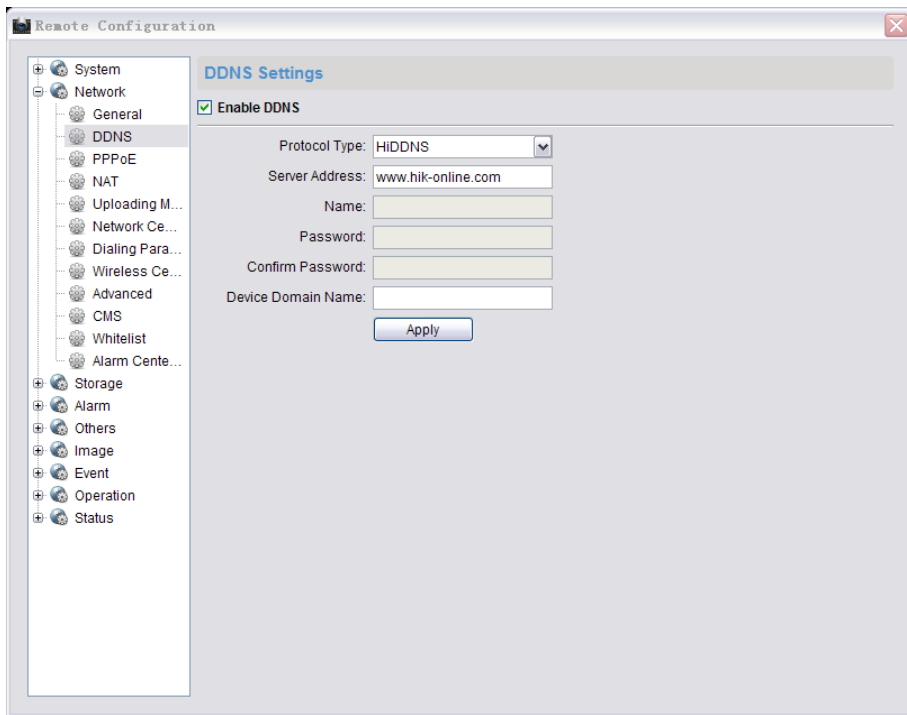
If your control panel is set to use PPPoE as its default network connection, you can use the Dynamic DDNS for network access.

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 Settings> Network > DDNS

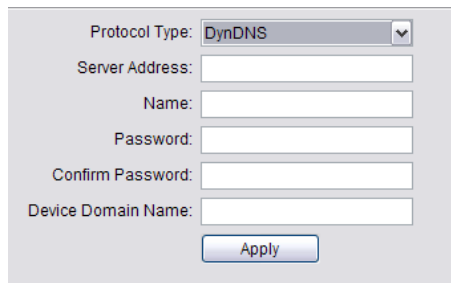


2. Check the **Enable DDNS** checkbox to enable this feature.
3. Select **DDNS Type**. Four DDNS types are selectable: IP Server, HiDDNS, PeanutHull and DynDNS.

● **DynDNS:**

Steps:

- (1) Enter **Server Address** of DynDNS (e.g. members.dyndns.org).
- (2) Enter the **User Name** and **Password** registered on the DynDNS website.
- (3) Enter the domain name obtained from the DynDNS website.
- (4) Click **Apply** to save the settings.



● **IP Server:**

Steps:

- (1) Enter the Server Address of the IP Server.
- (2) Click **Apply** to save the settings.



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.

Protocol Type: ▼
 Server Address:

● **PeanutHull**

Steps:

- (1) Enter the **User Name** and **Password** registered on the NO-IP website.
- (2) Click **Apply** to save the settings.

Uploading Mode Settings

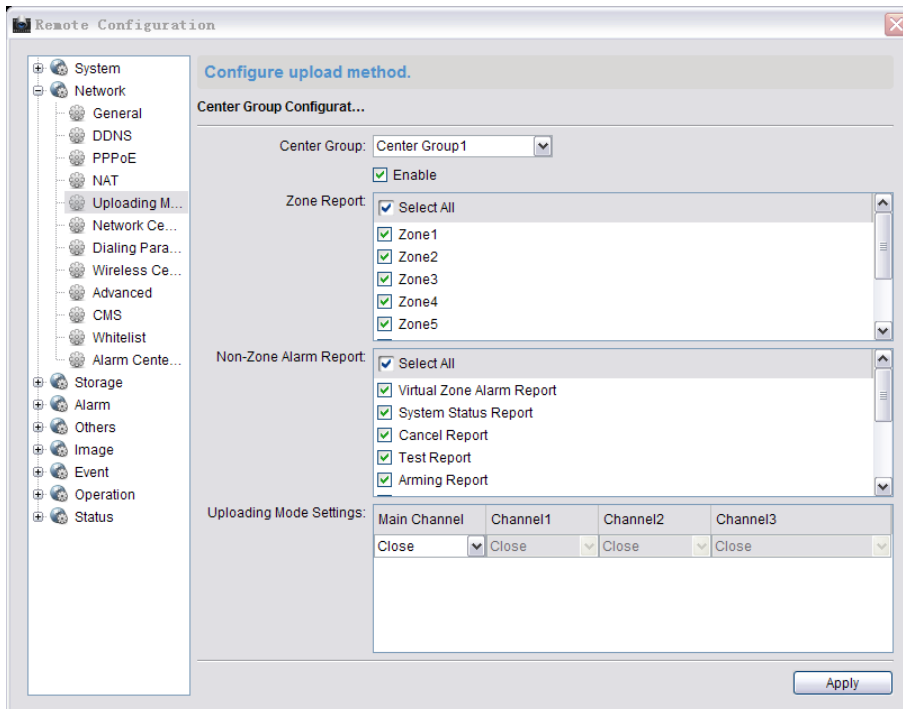
Purpose:

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 Settings->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.



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.



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

Network Center Settings

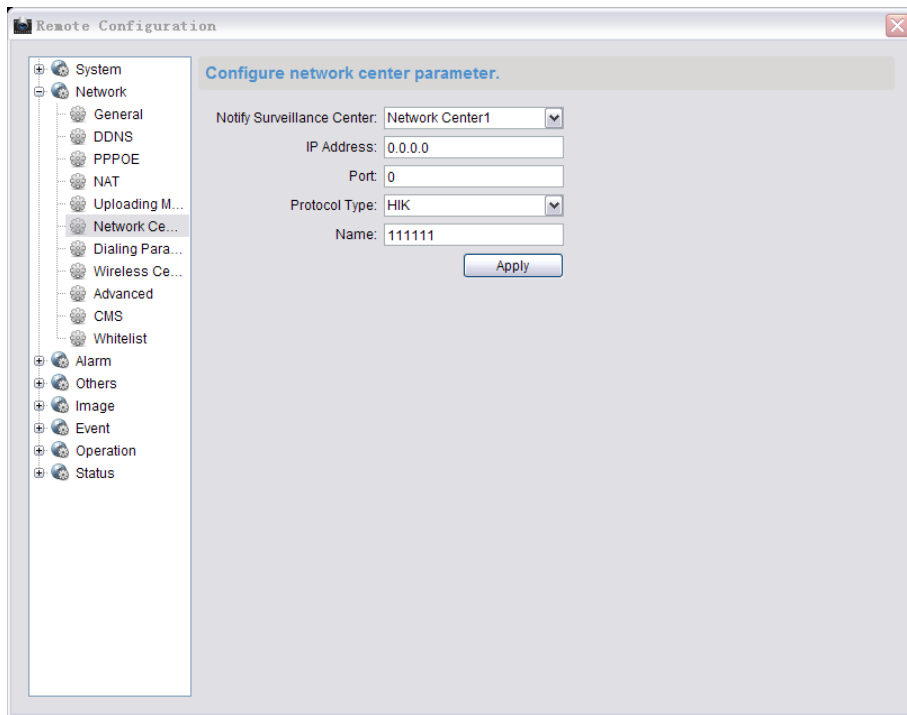
Purpose:

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 Settings->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 which 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 which is applying for displaying in the alarm receiving center.



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 Settings

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 Settings->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.



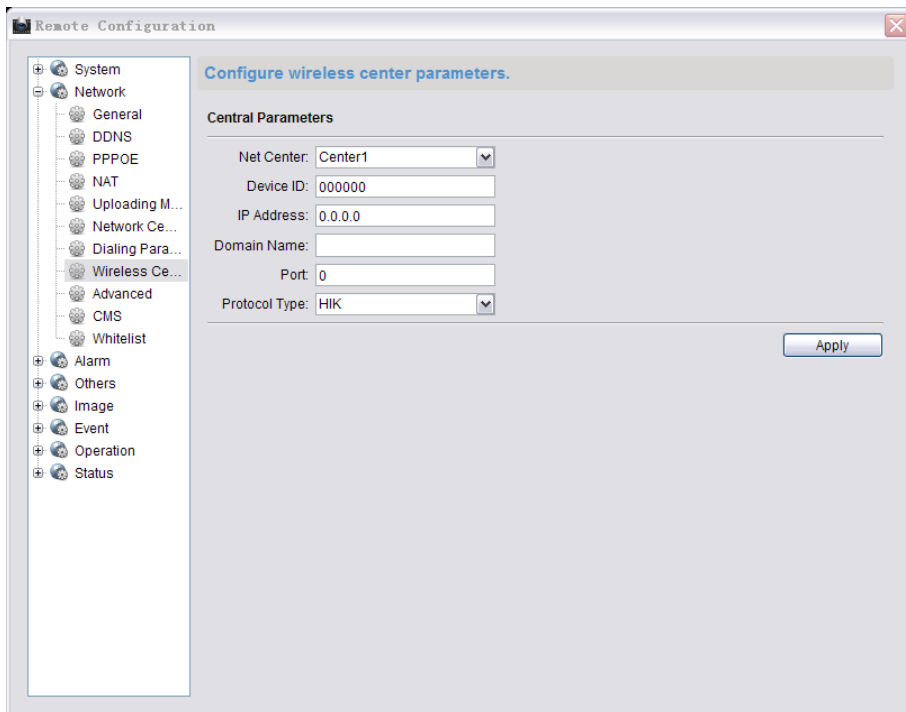
This function varies depending on the models of the control panel.

Wireless Center Parameter Settings

Steps:

1. Enter the wireless center parameter settings page.

Remote Settings->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.



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

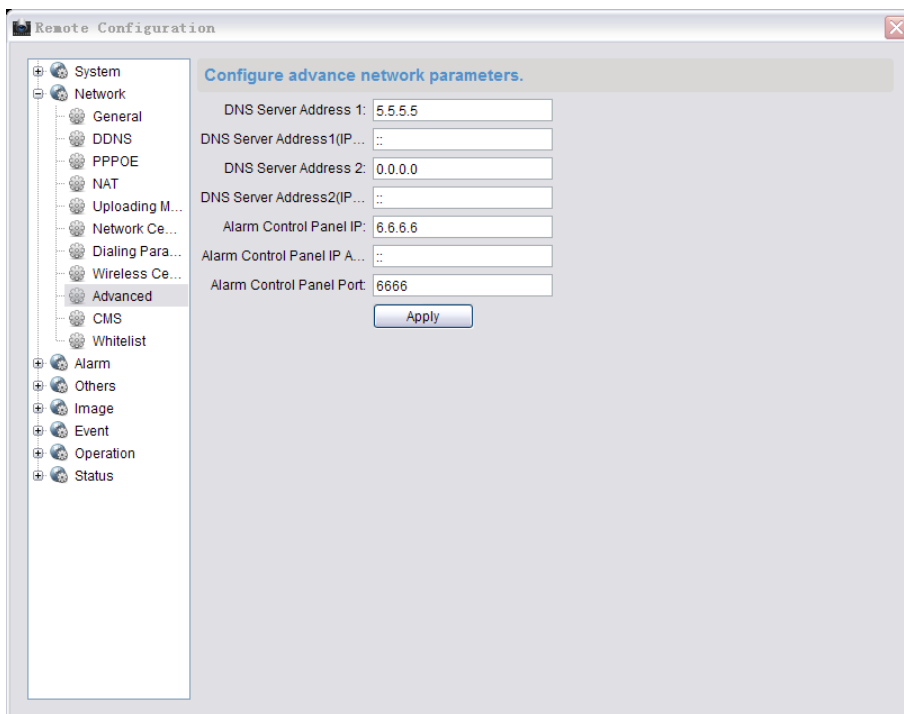
4. Enter the IP address which is used to communicate with the wireless alarm receiving center.
5. Enter the port NO. for communicating with the alarm receiving center.
6. Click the dropdown menu to select the protocol type.
7. Click **Apply** to save the settings.

Advanced Network Parameters Settings

Steps:

1. Enter the advanced network configuration page.

Remote Settings->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.

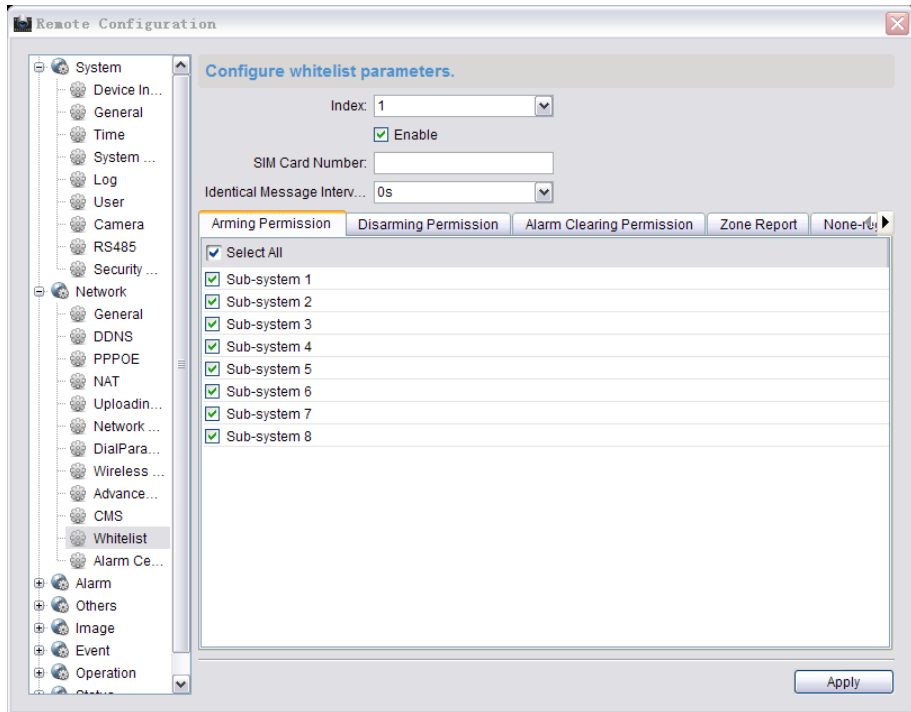
Whitelist Settings

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 Settings->Network-> 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 which 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.



This function varies depending on the models of the control panel.

Alarm Settings

Partition Settings

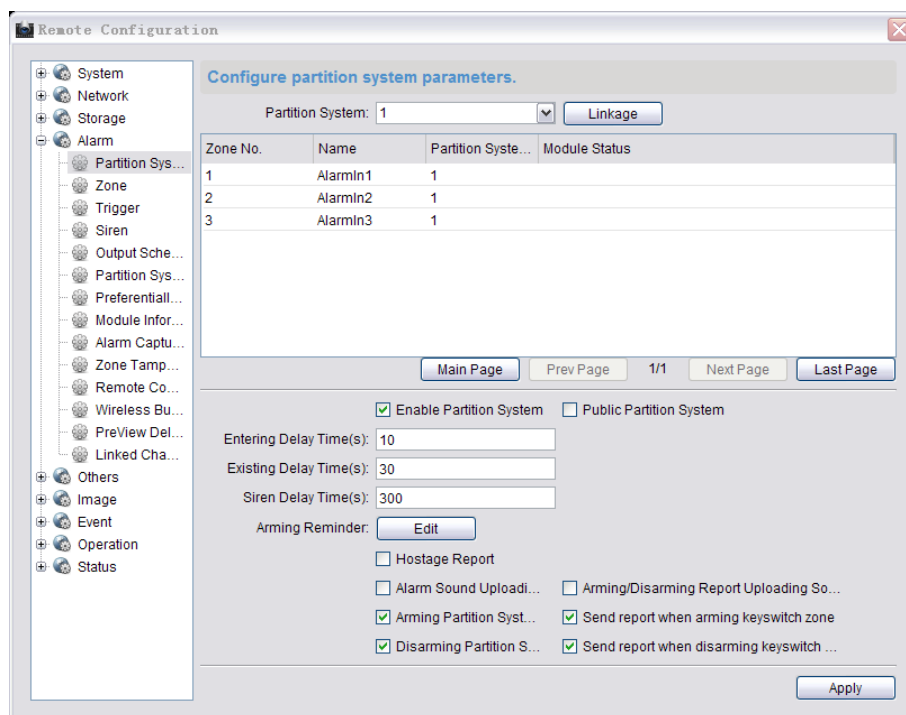
Purpose:

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

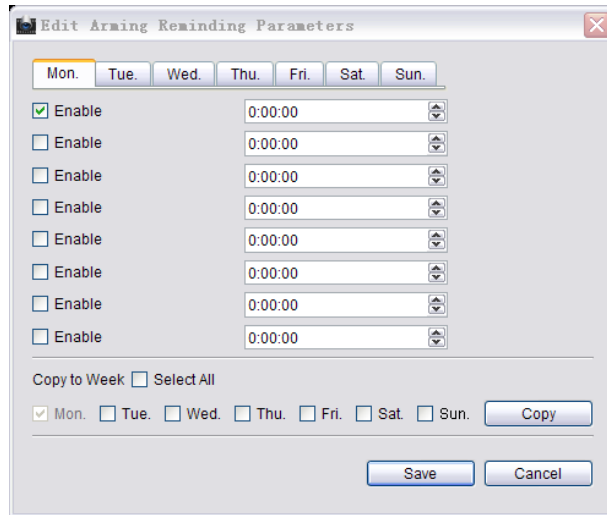
Steps:

1. Enter the partition alarm triggering configuration interface.

Remote Settings->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.

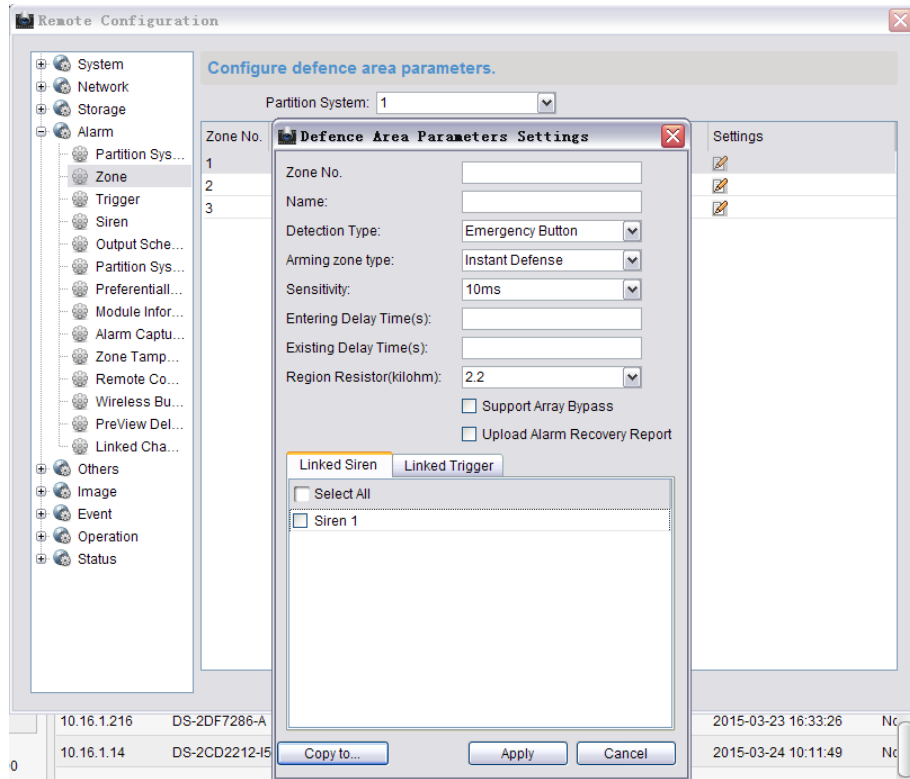



8. Select an alarm type.
 - **Hostage Report:** Enable uploading the duress report.
 - **Arming/Disarming Report Uploading Sound:** Enable the prompt sound when uploading the arming/disarming report.
 - **Alarm Sound Uploading Manual Testing:** Enable the prompt sound when successfully uploading the 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.

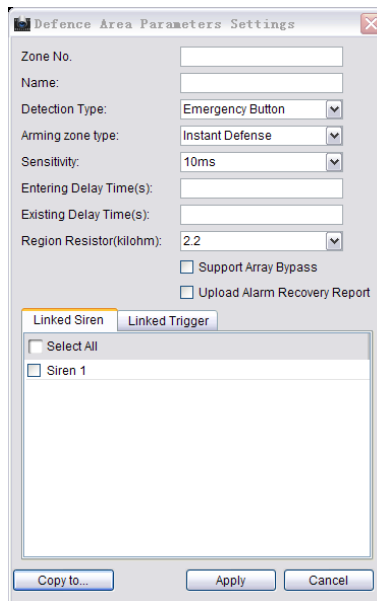
Zone Settings

Steps:

1. Enter the Zone configuration interface.
Remote Settings-> 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.

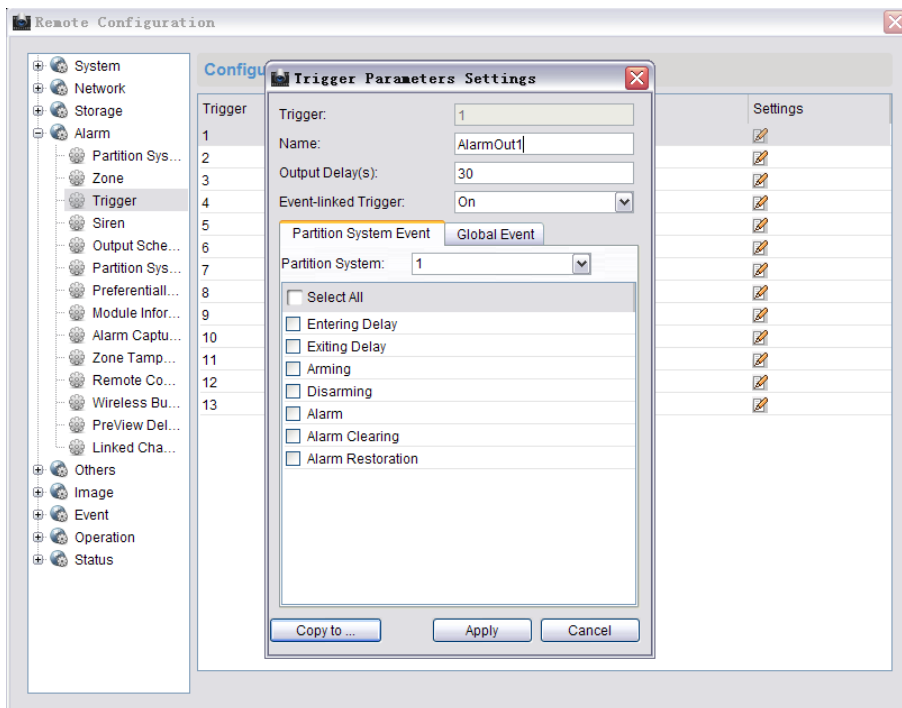



4. Edit the general information of the Zone, including name, probe type, arming Zone type, sensitivity, entering delay, existing delay and so on.
 - Probe Type:** Select the type of the detector.
 - Arming Zone Type:** Select the type of Zone in the partition
 - Sensitivity:** Select the response time 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.

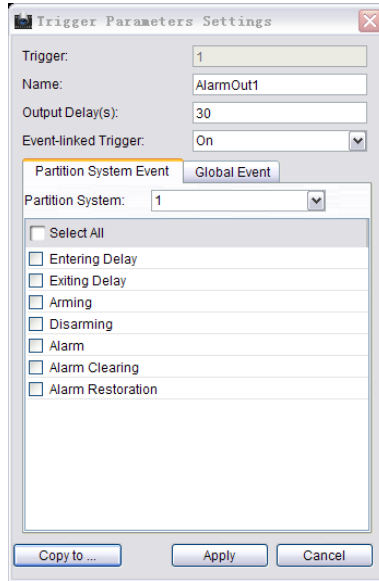
Trigger Settings

Steps:

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



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

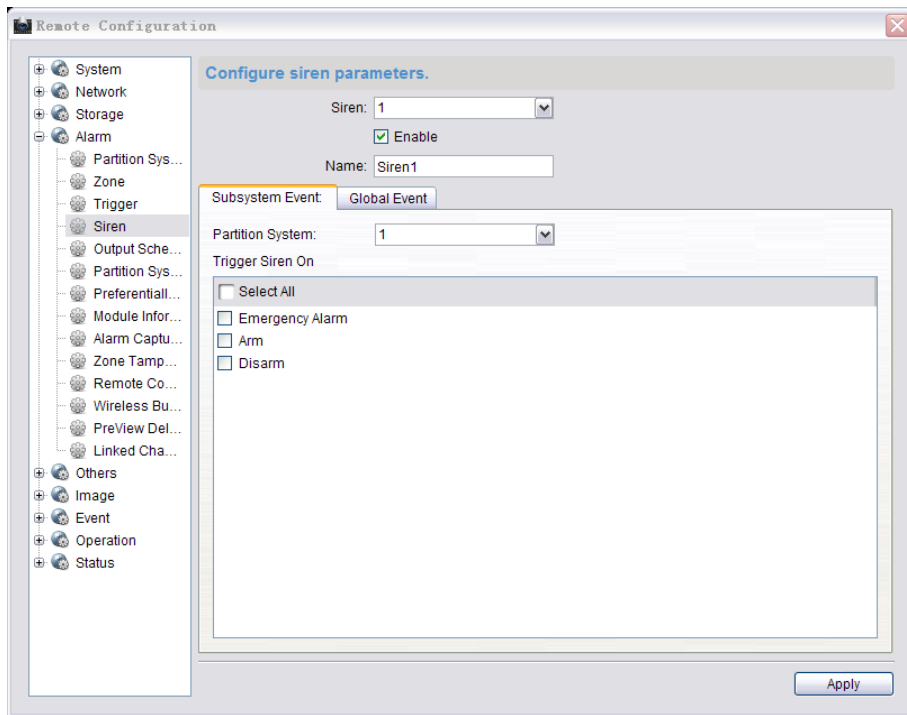


3. Edit the general information of the zone, including name, output delay and so on.
Output Delay (0~5999s): Configure the alarm output time after the alarm being triggered.
4. Click the dropdown menu to enable/disable the event-linked trigger.
5. Select the detailed operation after the alarm being triggered on the sub-system 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 Settings

Steps:

1. Enter the siren configuration page.
Remote Settings->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 sub-system event panel.
6. Select the global event of alarm triggering.
7. Click **Apply** to save the settings.

Trigger Output Schedule Settings

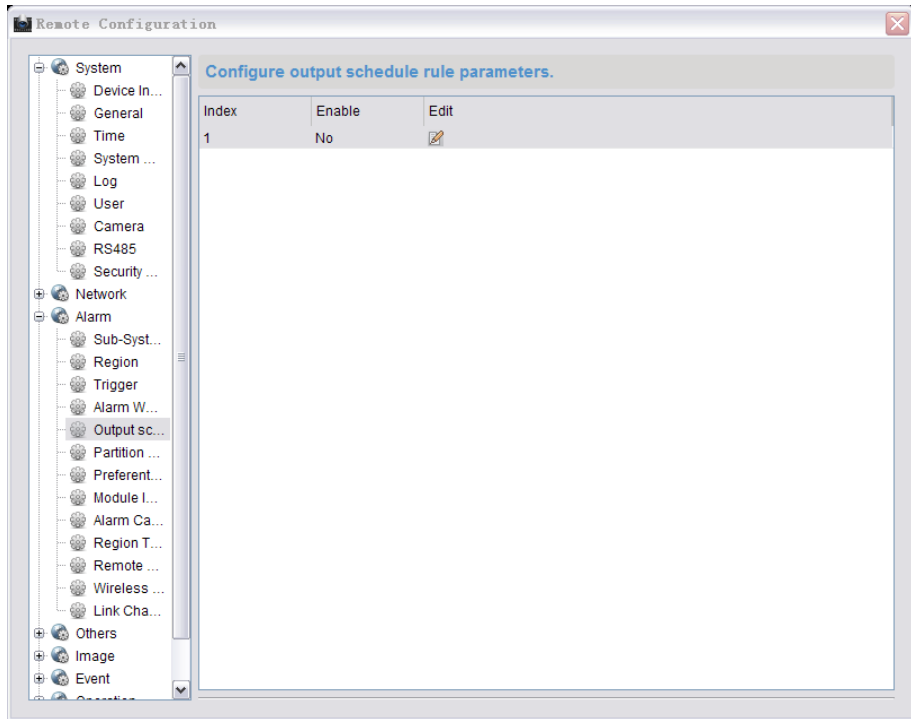
Purpose:

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

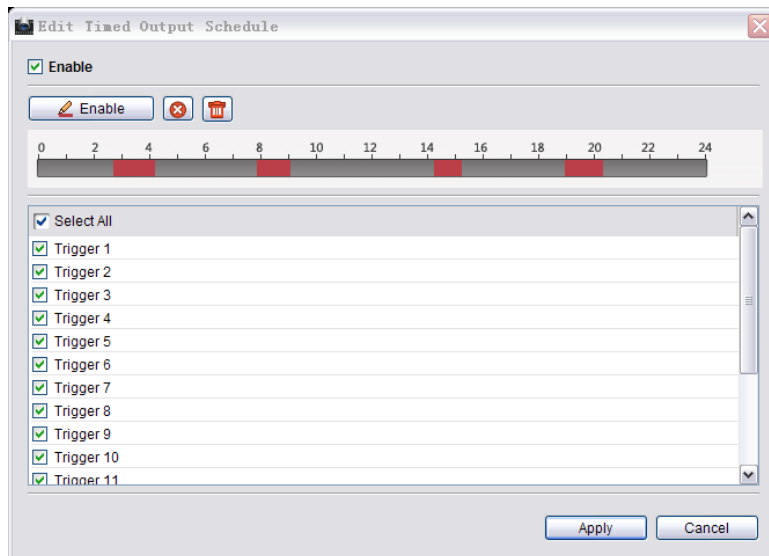
Steps:

1. Enter the relay output schedule configuration interface.

Remote Settings->Alarm-> Output Schedule Rule



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



- Check the **Enable** checkbox to enable the configuration.
- 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.

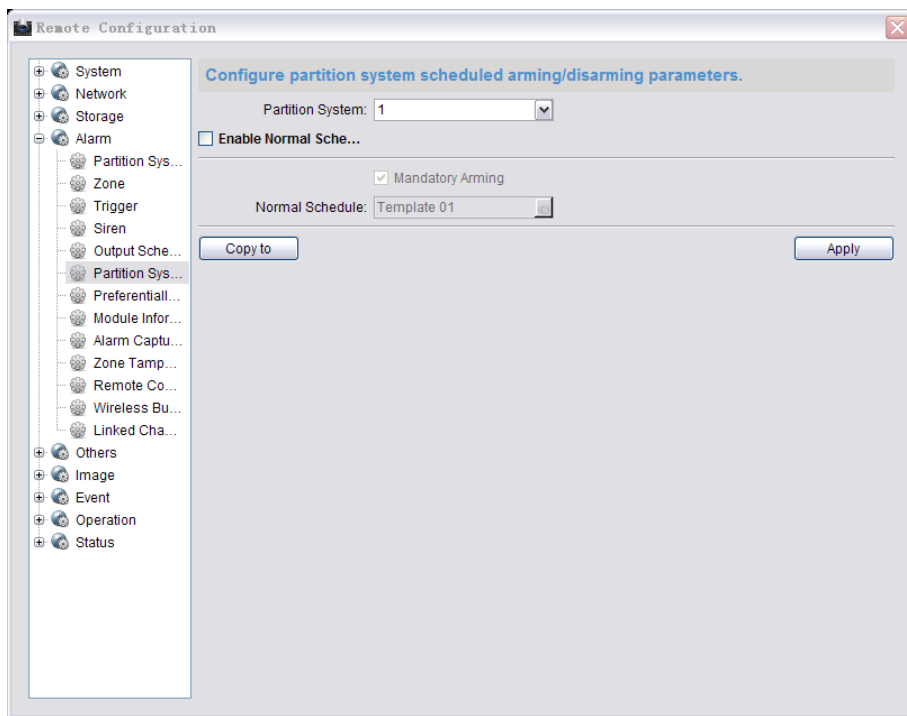
5. Check the **Trigger** checkbox to select the trigger.
6. Click **Apply** to save the settings.


Partition Arming/Disarming Schedule Settings

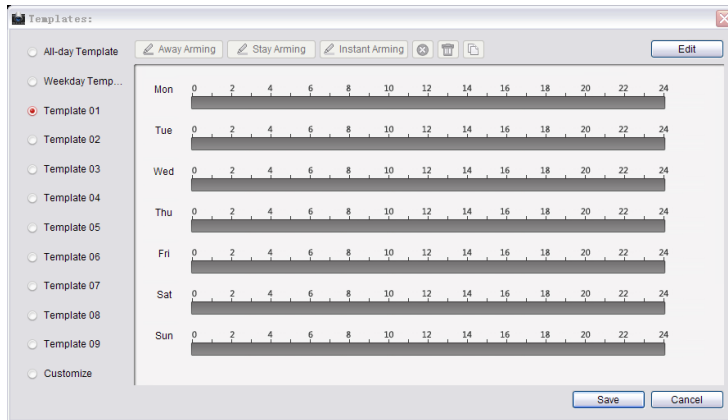
Steps:

1. Enter the arming/disarming schedule configuration interface.

Remote Settings->Alarm ->Partition Scheduling Arming/Disarming


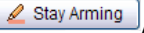
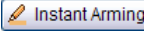



2. Select a partition needs to be configured.
3. Check the **Enable Normal Schedule** checkbox to enable daily schedule for the partition. You can select to enable the mandatory arming function.
4. Click the icon  of the **Template** box to enter the schedule configuration interface.




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



7. Click the button  /  /  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.

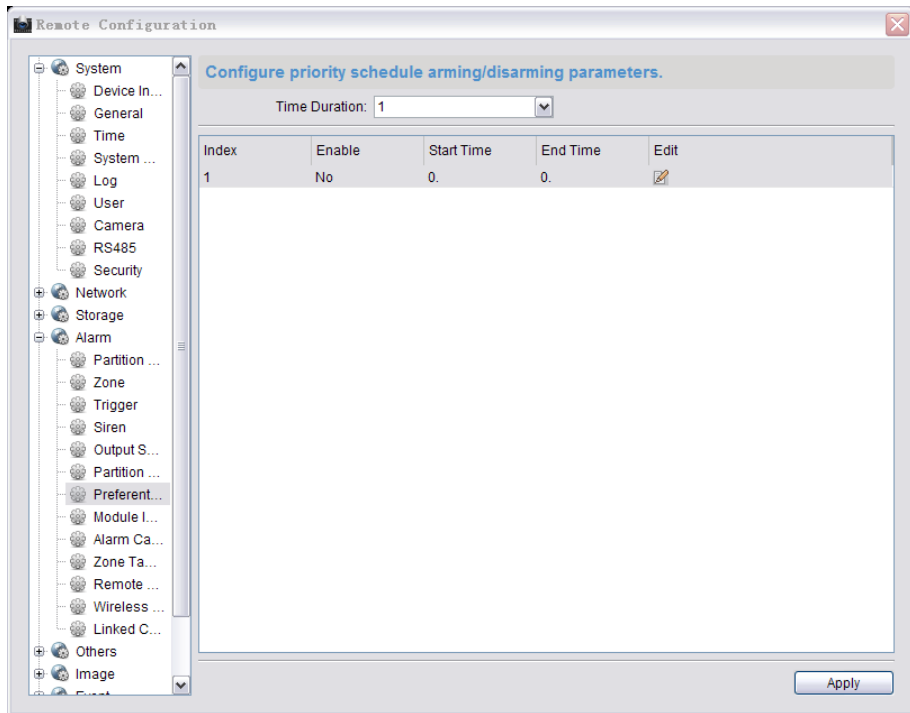
Copy Schedule: Click the drawn color bar and click the icon  to copy this arming schedule to other day of the week.

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 Settings

Steps:

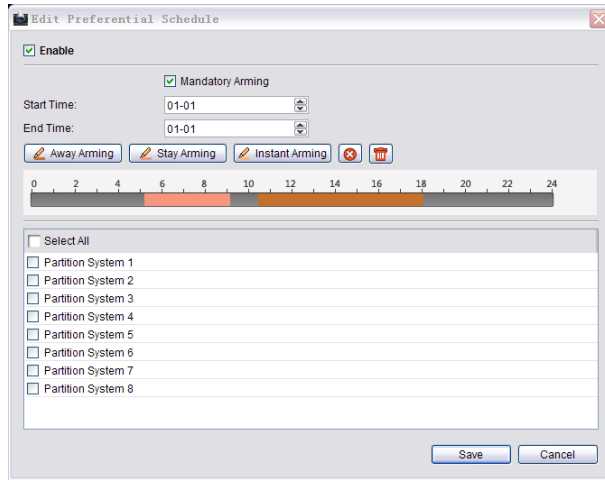
1. Enter the arming/disarming preferential schedule configuration interface.
Remote Settings->Alarm->Preferential Schedule Arming/Disarming

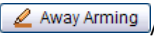
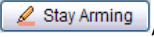
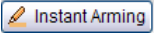


2. Click the drop down menu to select the time duration.
3. Click the icon to enter the preferential schedule configuration page.



The permission level of preferential schedule is higher than the weekly arming/disarming schedule's.



4. Click the button  /  /  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

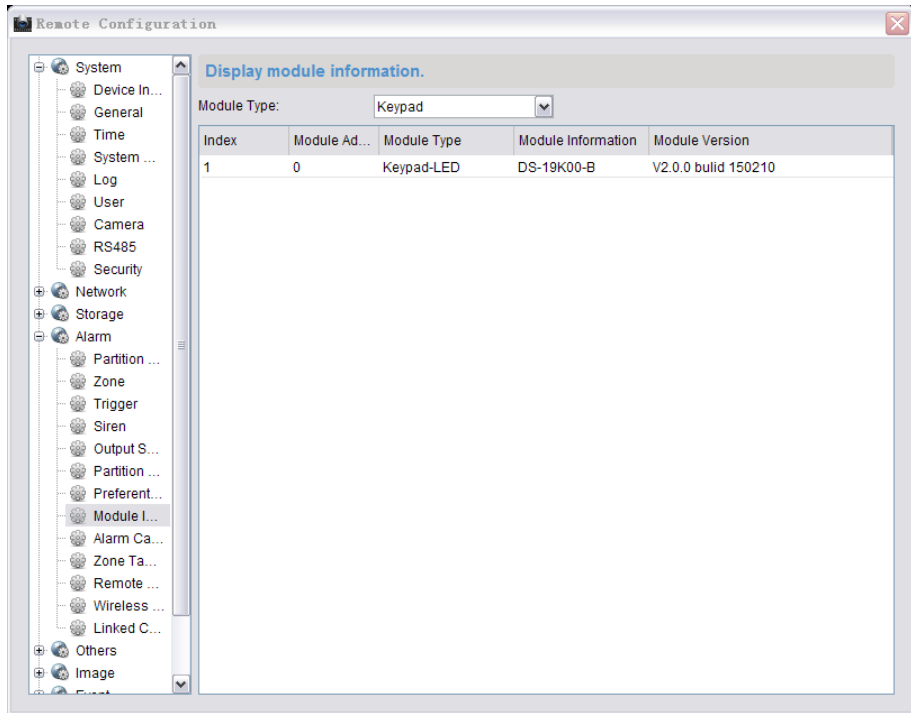
Purpose:

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

Steps:

1. Enter the module information interface.

Remote Settings->Alarm->Module Information

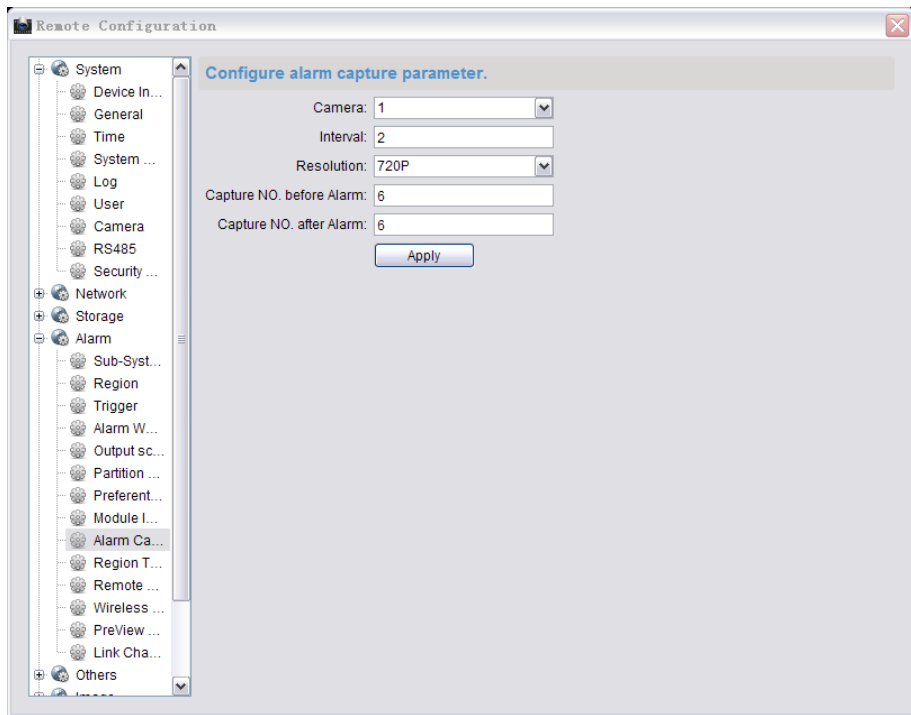


2. Click and select the external device from the module type dropdown menu.
3. View the information about the selected device.

Alarm Capture Settings

Steps:

1. Enter the alarm capture configuration interface.
Remote Settings->Alarm->Alarm Capture Parameters

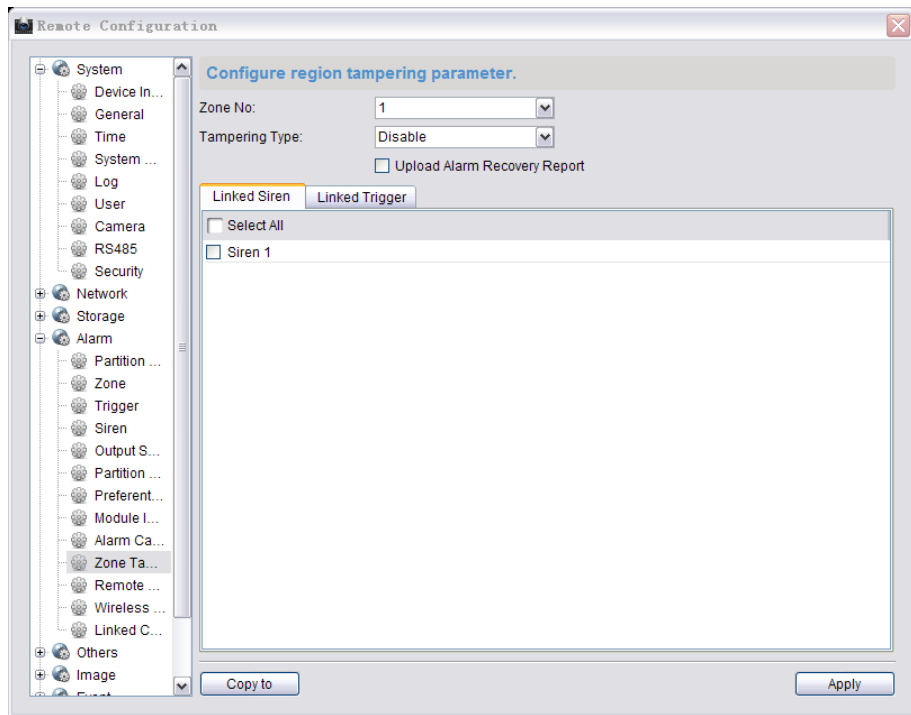


2. Select the camera needs to be configured.
3. Enter the capture interval between the previous picture and the next picture. Default:2s.
4. Select the resolution of the captured picture.
5. Set the number of pictures needs to be captured before/after the alarm being triggered.
6. Click **Apply** to save the settings.

Zone Tampering-proof Settings

Steps:

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

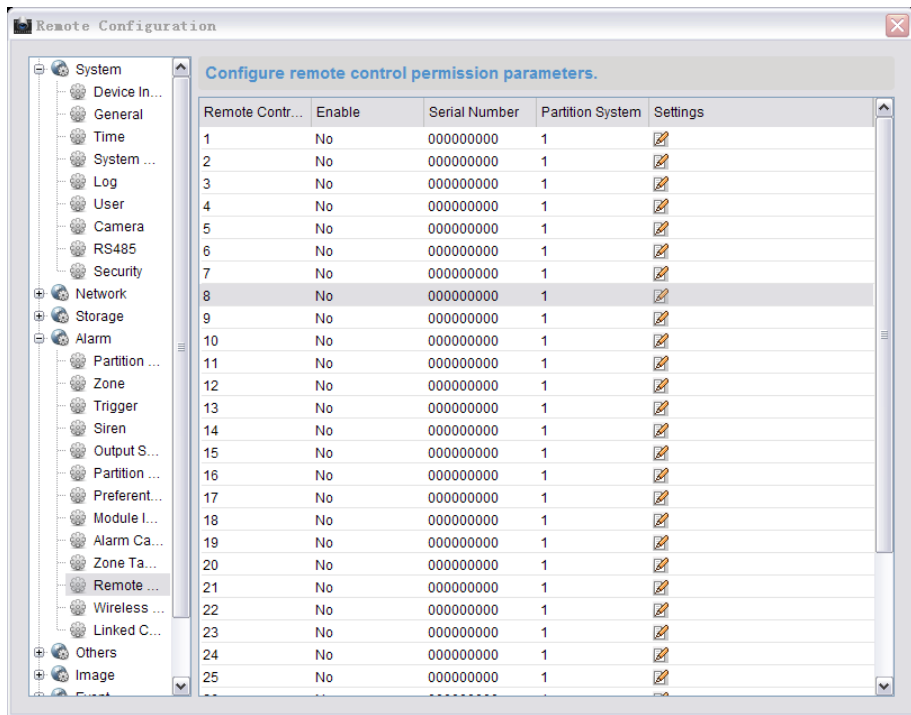



2. Click dropdown menu to select a Zone needs to be configured.
3. Select a tampering type.
4. Check the **Upload Alarm Recovery Report** checkbox to enable the function of uploading alarm recovery report.
5. Select the linked siren on the **Linked Siren** panel.
6. Select the linked trigger on the **Linked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

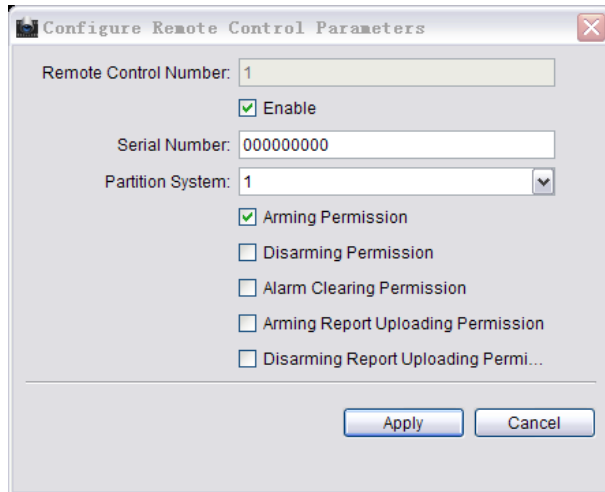
Remote Control Permission Settings

Steps:

1. Enter the remote control permission configuration interface.
Remote Settings->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. The number of 000000000 indicates to delete the remote control.
5. Select the partition NO. to be controlled.
6. Check the checkbox and select the permission for the remote control.
7. Click **Apply** to save the settings.

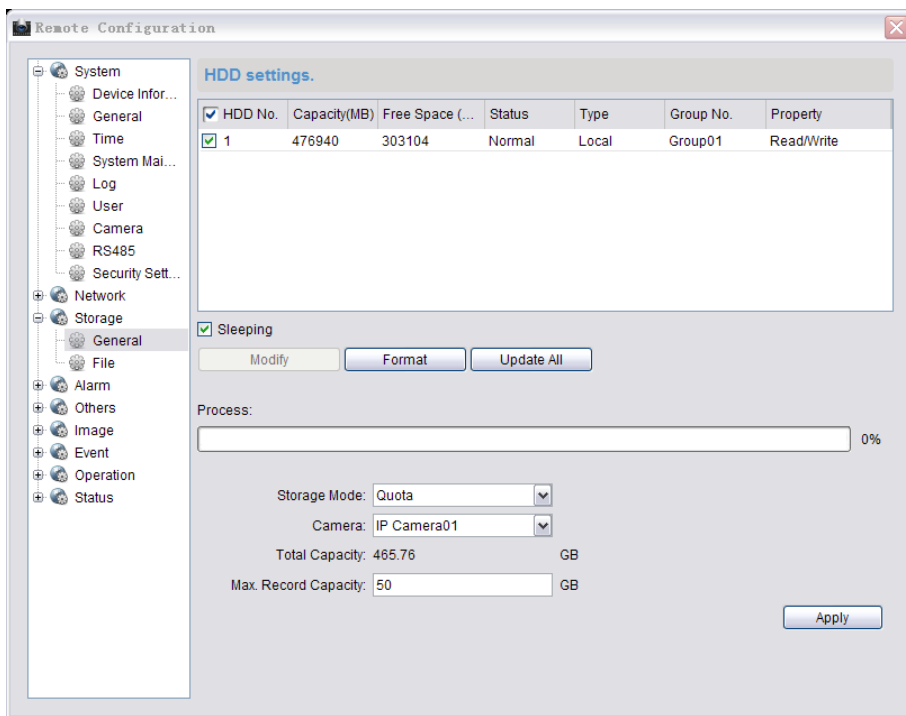
Storage

HDD Information

Steps:

1. Enter the HDD Settings interface in which you can view the capacity, free space, status, type and property of the disk.

Remote Settings > Storage > General,



2. If the status of the HDD is **Uninitialized**, check the corresponding checkbox to select the disk and click to start initializing the disk. When the initialization completed, the status of disk will become **Normal**
3. Click **Apply** to save the settings.



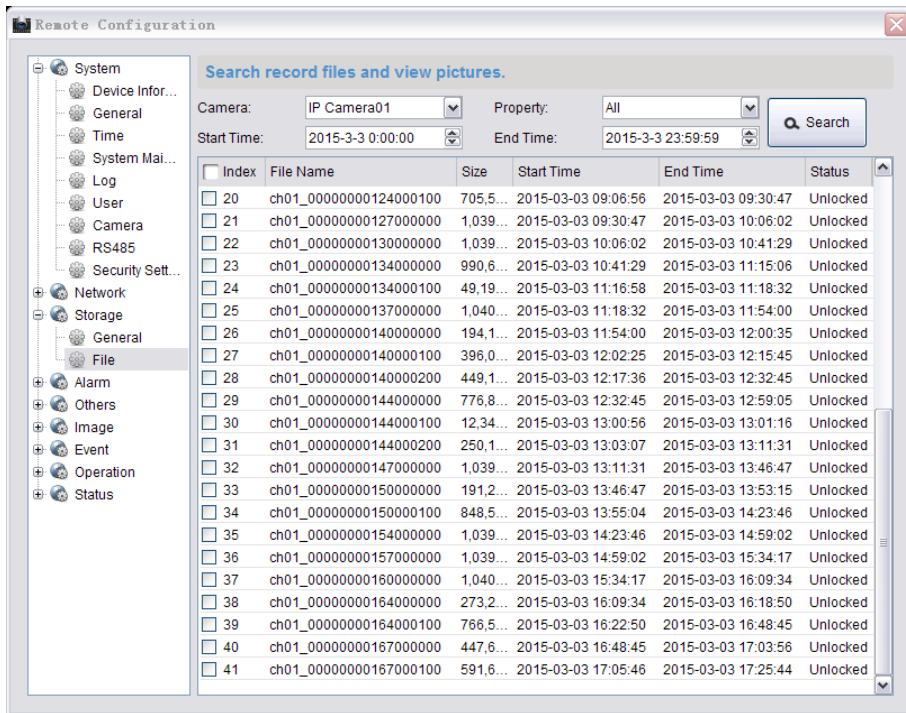
This function is available only if the device is connected with HDD.

File Query

Steps:

1. Enter the file query interface.

Remote Settings->Storage->File



2. Enter the search criteria including camera name, property, start time and end time.
3. Click Search to get the file list.

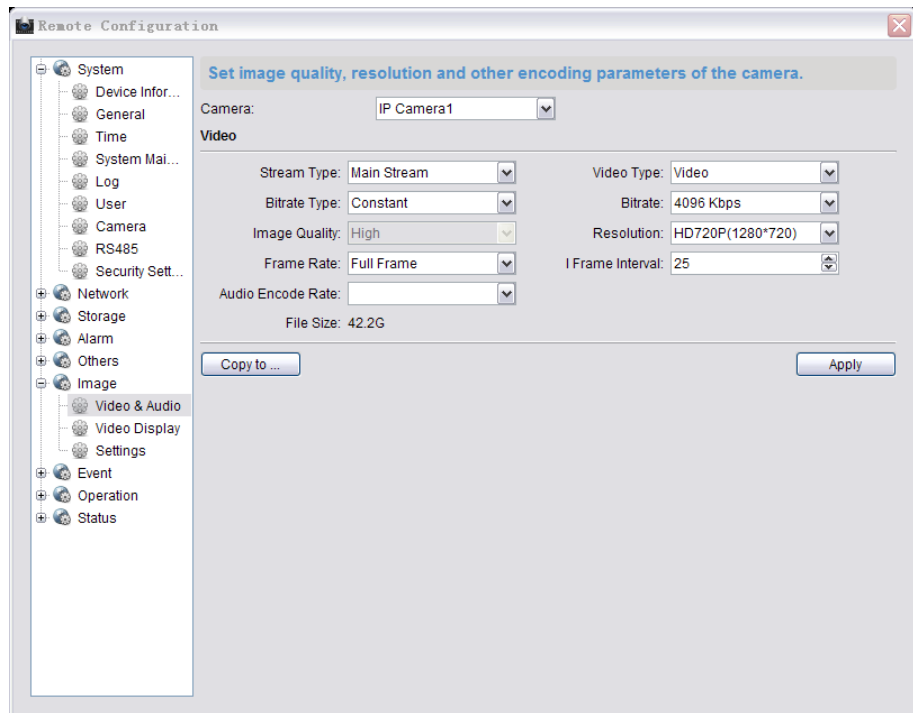
Image Settings

Video & Audio Settings

Steps:

1. Enter the video/audio configuration interface.

Remote Settings->Image->Video & Audio



2. Select a camera needs to be configured.
3. Edit the general video parameters.

Stream Type: The main stream is usually for recording and live viewing with good bandwidth, and the sub-stream can be used for live viewing when the bandwidth is limited.

Video Type: Select the stream type to video stream, or video & audio composite stream.

Bitrate Type: Select the bitrate type to constant or variable.

Resolution: Select the resolution of the video output.

Frame Rate: The frame rate is to describe the frequency at which the video stream is updated and it is measured by frames per second (fps). A higher frame rate is advantageous when there is movement in the video stream, as it maintains image quality throughout.

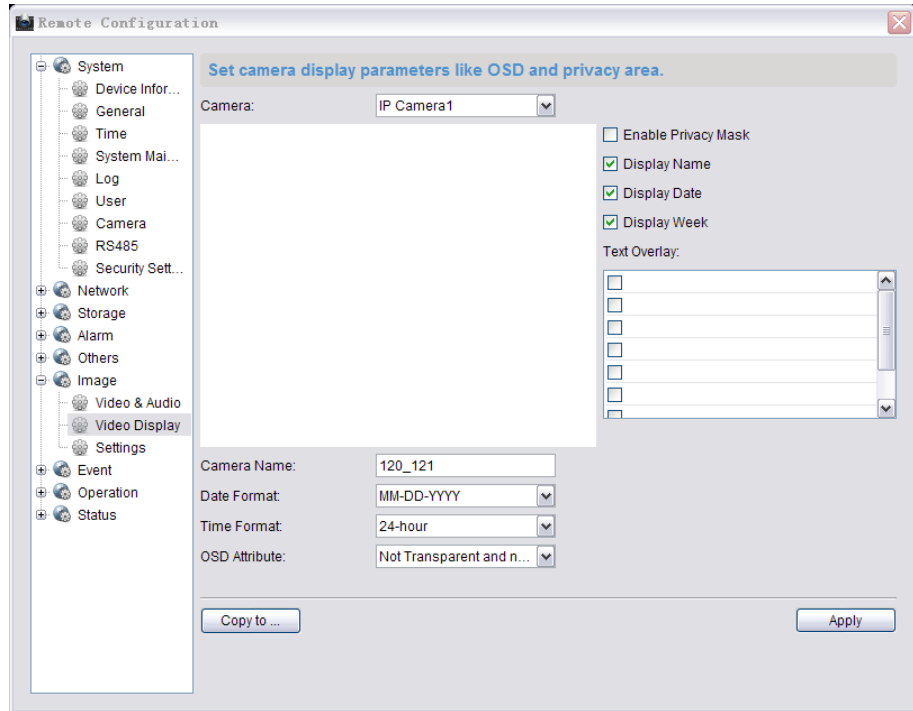
I Frame Interval: Set the I-Frame interval from 1 to 400.


4. Click **Copy to** to copy all these settings to other Zones.
5. Click **Apply** to save the settings.

OSD Settings

Steps:

1. Enter the OSD Settings interface:
Remote Settings > Image > Video Display



2. Check the corresponding checkbox to select the display of camera name, date or week if required
3. Edit the camera name in the text field of **Camera Name**.
4. Select from the drop-down list to set the time format, date format and display mode.
5. Check the checkbox in front of textbox to enable the on-screen display.
6. Input the characters in the textbox.
7. Use the mouse to click and drag the red text frame  in the live view window to adjust the text overlay position.
8. Click **Apply** to save the settings.

Event Settings

Motion Detection Settings

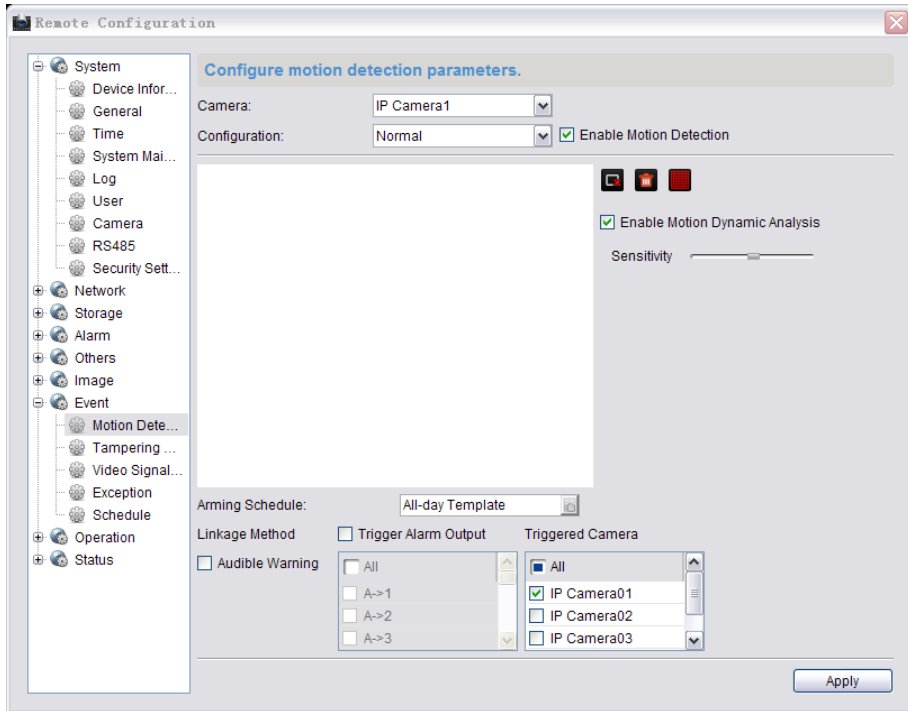
Purpose:


Motion detection is a feature which can trigger alarm actions and actions of recording videos when the motion occurred in the surveillance scene.

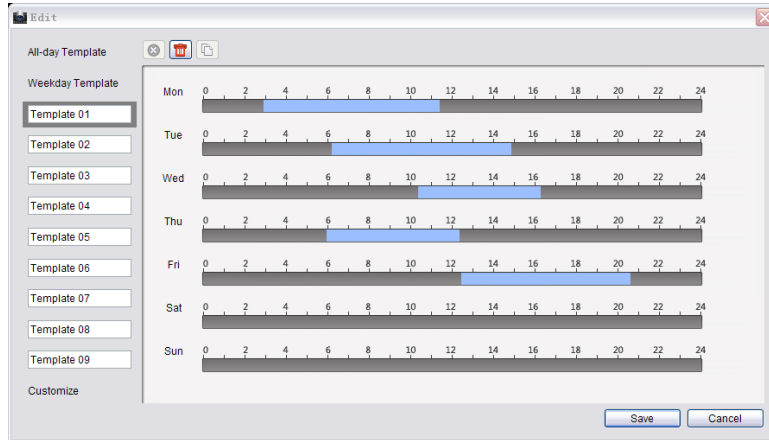
Steps:

1. Enter the motion detection setting interface:

Remote Settings > Event > Motion Detection



2. Select a camera needs to be configured.
3. Check the checkbox of the **Enable Motion Detection** to enable this function.
4. You can check the **Enable Motion Dynamic Analysis** checkbox if you want the detected object get marked with rectangle in the live view.
5. Click the icon . Click and drag the mouse on the live video image to draw a motion detection area.
6. Move the slider of **Sensitivity** to set the sensitivity of the detection.
7. Set the Arming Schedule for Motion Detection.



9. Click **Apply** to save the settings.

Tampering Alarm Settings

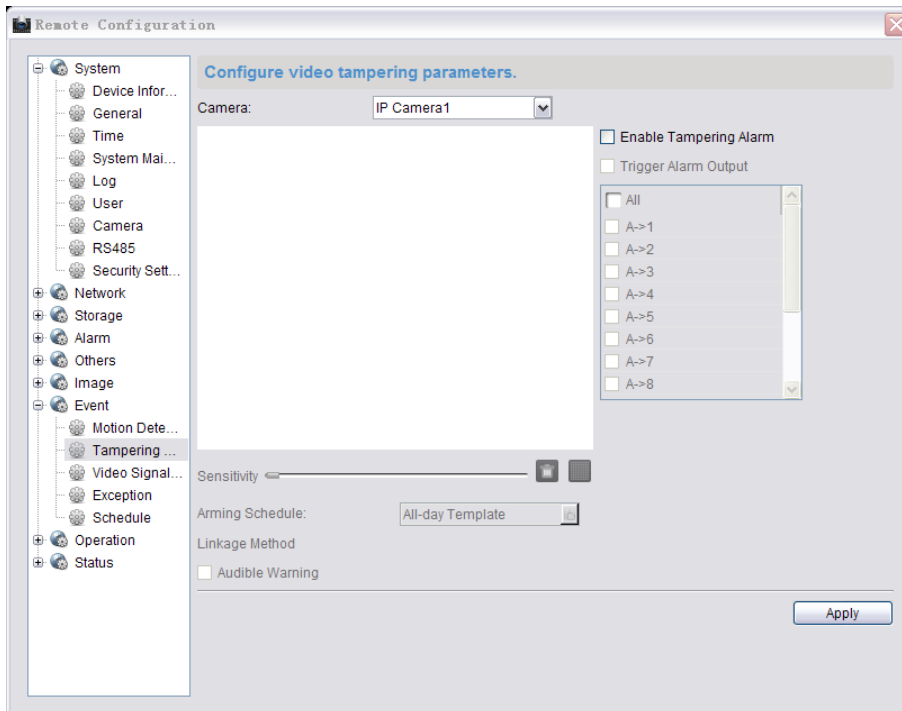
Purpose:

You can configure the camera to trigger the alarm actions when the lens is covered.

Steps:

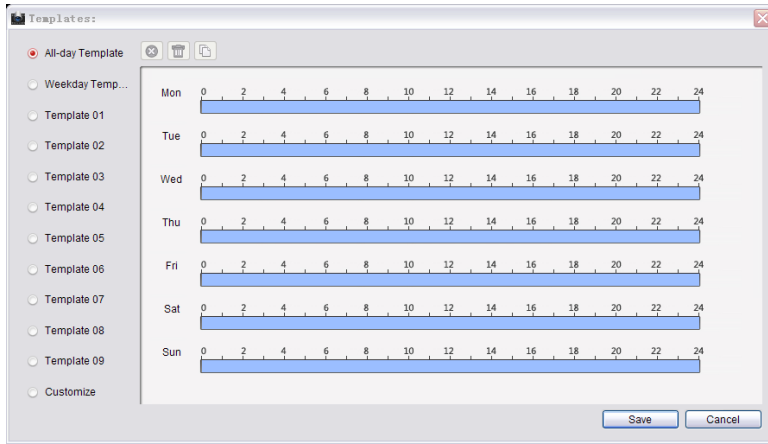
1. Enter the video tampering Settings interface:

Remote Settings > Event > Tampering Alarm



2. Select a camera needs to be configured.

3. Check **Enable Tampering Alarm** checkbox to enable the tampering detection.
4. Set the tampering area. Refer to *Step 5* in **Section 5.2.26.1 Motion Detection Settings**.
5. Set the arming schedule for tampering.

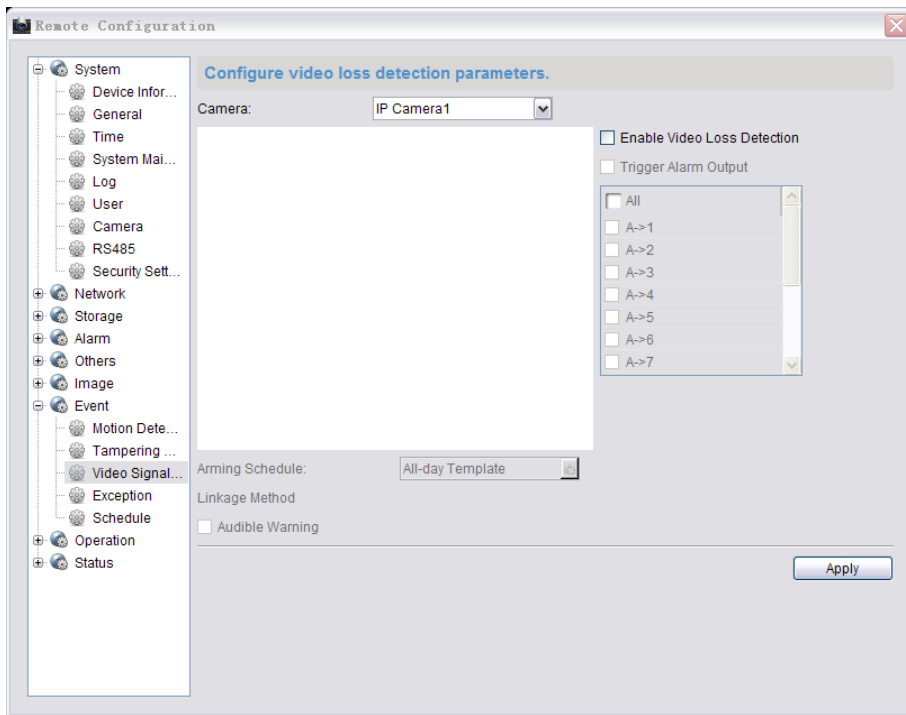


6. Check the **Audible Warning** checkbox to enable audible warning for the detection.
7. Click **Apply** to save the settings.

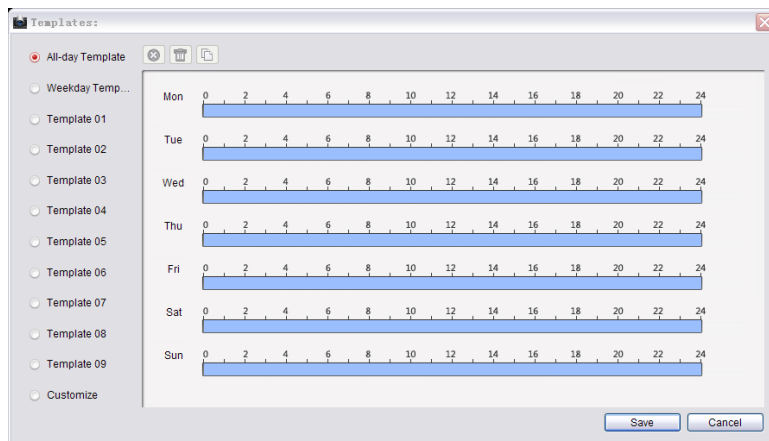
Video Loss Detection Settings

Steps:

1. Enter the Video Loss Setting interface:
Remote Settings > Event > Video Signal Loss



2. Select a camera needs to be configured.
3. Check the **Enable Video Loss Detection** checkbox to enable the video loss detection.
4. Check the check box to link the camera with alarm output.
5. Set the schedule for the video loss detection.



6. Check the **Audible Warning** checkbox to enable audible arming for the detection.
7. Click **Apply** to save the settings.

Exception Detection

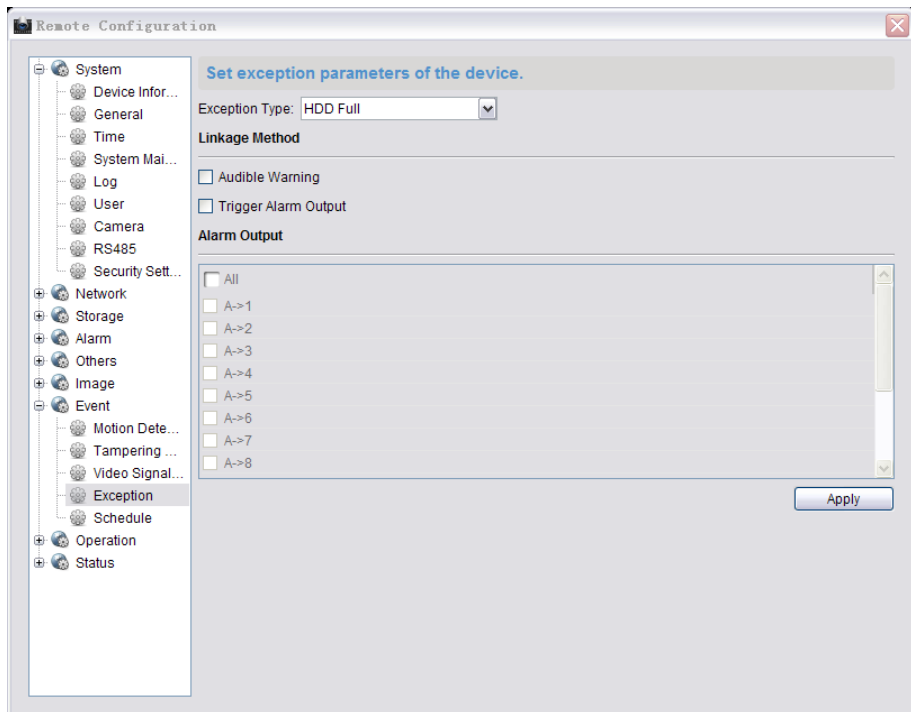
Purpose:

The exception type can be HDD full, HDD error, network disconnected, IP address conflicted, record/capture exception and illegal login to the camera.

Steps:

1. Enter the Exception Settings interface:

Remote Settings > Events > Exception

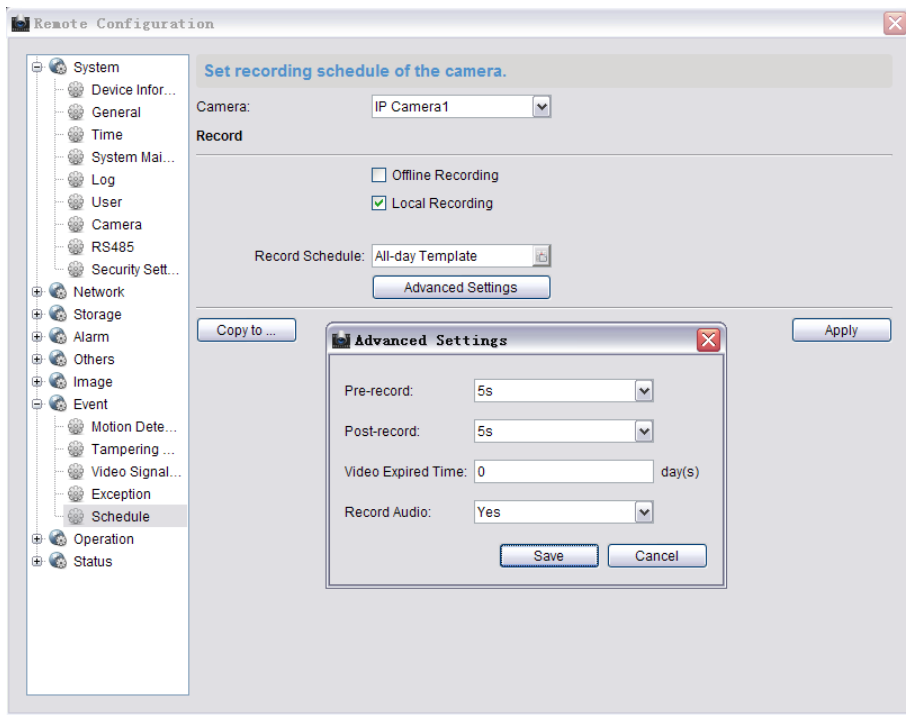



2. Select a camera needs to be configured.
3. Select an exception type.
4. Check the checkbox to set the actions taken for the Exception alarm.
5. Check the check box to link the camera with alarm output.
6. Click **Apply** to save the setting.

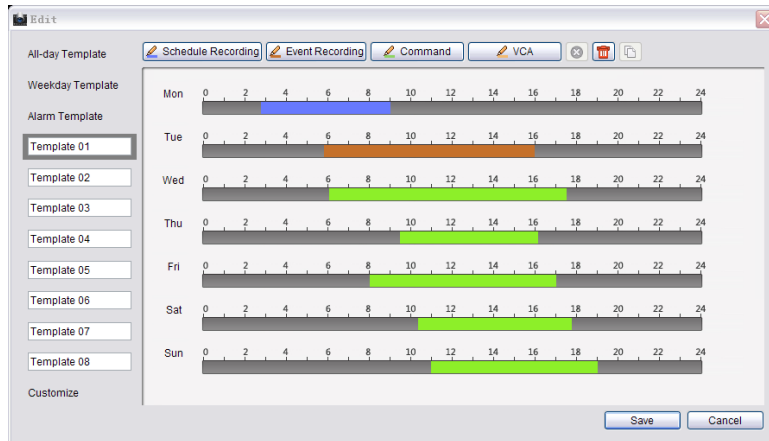
Record Schedule Settings



Steps:


1. Enter the record schedule configuration interface.
2. **Remote Settings > Events > Schedule**






3. Select the camera needs to be configured.
4. Check the checkbox on the **Record** panel to select the record type.
5. Click the  icon to set the record schedule.



6. Click **Edit** to enter the Templates Management interface. Select the template to be set and you can edit the template name.
7. Set the time schedule for the selected template.
 When the cursor turns to , you can edit the schedule time bar.
 When the cursor turns to , you can move the selected time bar you just edited.

When the cursor turns to , you can lengthen or shorten the selected time bar.

8. Optionally, you can select the schedule time bar,
And then click the icon  to delete the selected time bar,
Or click the icon  to delete all the time bars,

Or click the icon  to copy the time bar settings to the other dates.
9. Click **Save** to save the settings and click cancel to exit the interface.
10. Click **Advanced Settings** button to set the pre-record time, post record time, video expired time, and audio recording.
11. Click **Copy to** to copy all these settings to other Zones.

Click Apply to save the settings.

Operation

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

Click **Remote Settings->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.

Configure the partition system.

Partition System: ▼

Zone No.	Name	Arming Status	Status of ByPass	Status of Alarm
1	Zone 1	Disarmed	Bypass Recovery	Normal
2	Zone 2	Disarmed	Bypass Recovery	Normal
3	Zone 3	Disarmed	Bypass Recovery	Normal
4	Zone 4	Disarmed	Bypass Recovery	Normal
5	Zone 5	Disarmed	Bypass Recovery	Normal
6	Zone 6	Disarmed	Bypass Recovery	Normal
7	Zone 7	Disarmed	Bypass Recovery	Normal
8	Zone 8	Disarmed	Bypass Recovery	Normal

1/1

Status

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


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 the 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, sensor alarm display interface, 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 sensor alarm display interface 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 security 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

Working Status	Indicator Status	Working Status	Indicator Status
Project	Red, Normally On	Change Password	Green, Blink

LED alarm keypad **Channel** 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 **Channel** indicator under **Project Mode**:

No.	Description	No.	Description
1	Off-hook	5	Send CID Report
2	Dial	6	Receive Alert Sound
3	Alarm Connector Disconnection	7	control panel Off-hook
4	Receive the Hand-shack Sound	8	Alarm Connector On-hook

LED keypad **Channel** 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 meanings of LED keypad alert sound are as follow:

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

No.	Keypad Alert Sound	Description
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} + {#}.






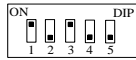

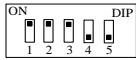
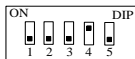
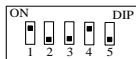

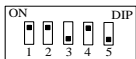
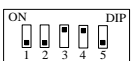
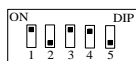

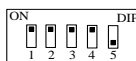




Q: How to input hexadecimal number?






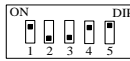

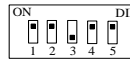




A: Input hexadecimal number with {*} button and number button {0} ~ {5}.

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

DIP	Add.	DIP	Add.	DIP	Add.	DIP	Add.
	20		21		22		23
	24		25		26		27
	28		29		30		31

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 duress 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 duress 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 duress report and delay. The programming command to enable **control panel duress report** is as follow:

Command Address/ Enter Delay/ Exit Delay/ Siren Working Duration/ **control panel duress report**/ End

{4}{6}{4}/ {3}/ {6}/ {2}/ {1}/ {#}

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 ({Operator Password}{*}{6}{8}{#})

Q: Why there is no Disarming Report?

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

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: Video security 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 video security 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 Settings-> Others-> Network Center Settings**;
- 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 Settings-> Others-> Dialing Parameter Setting**;
- 3) If the user communicates via WIFI: Configure APN Name and Parameters of remote alarm center in **Remote Settings-> 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 Settings-> Uploading Mode Settings**

Q: How to configure the communication way of video security 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

The specification of DS-19S08N-04F/Kx (Gx) video security control panel.

Model		DS-19S08N-04F/Kx	DS-19S08N-04F/KxGx
Security Control Panel Parameters	Alarm Input	8-zone Alarm Input	
	Alarm Output	1-ch Local +8-ch expandable, 30VDC/1A	
	Siren Power Supply	12VDC /500mA	
	Keypad	K1: LED Keypad; K2: LCD Keypad	
	Supported External Keypads	8	
	Tamper-proof Switch	Support Tamper-proof and Movement Prevention Function	
	Partition System	8 Partition Systems, 1 Public Partition System	
	Scheduled Arming/Disarming	8 Time Periods Each Day	
	Detector Tamper-proof Alarm	Support	
	Mobile APP	Support iOS, Alarm Push, Remote Arming/Disarming Function	
	Supported Remote Controllers	32 (Unobstructed Effective Range of 100m)	
	SMS Alarm Data-push	N/A	Support
	SMS Arming/disarming Data-push	N/A	Support
Media Parameters	Network Video Input	4-ch HD Network Camera	
	Network Bandwidth	25Mbps	
	VGA Output Resolution	1-ch, Resolution: 1024×768/60Hz, 1280×720/60Hz, 1280×1024/60Hz, 1600×1200/60Hz, 1920×1080p/60Hz	

Model		DS-19S08N-04F/Kx	DS-19S08N-04F/KxGx
	Audio Output	1-ch, RCA Interface (Linear, 1kΩ)	
	Two-way Audio	1-ch, RCA Interface (Linear, 1kΩ)	
	Loudspeaker	1-ch, Build-in	
	Record Resolution	1080P/720P/VGA/4CIF/DCIF/2CIF/CIF/QCIF	
	Synchronous Playback	4-ch	
	Post-view	Delay duration can be configured.	
	Capture for Recheck	10 Captures (5 Captures before/after Alarm)	
	Record Mode	Manual Record, Scheduled Record, Motion Detection Record	
	Playback Mode	Instant Playback, Normal Playback, Event Playback	
	HDD Information	Build-in 500G 2.5"HDD, SATA Interface	
Wireless Network Parameters	Wireless Network Standard	N/A	GLT: 4G TDD-LTE GLF: 4G FDD-LTE GW: 3G WCDMA GE: 3G EVDO
	UIM Card Slot		1
	SMA Antenna Interface		1
Interfaces and Appearance	Network Interface	1 RJ45 10M/100M Self-adaptive	
	RS485	1, RS485 Half-duplex, Support PTZ Control	
	Keypad Bus	1, RS485 Half-duplex	
	USB Interface	1, USB2.0	
	Storage Battery Port	1 Port, for Storage Battery Accessing	
	Power Supply	14.3VDC /2.8A	
	Consumption	6.5W (Without HDD and Power Supply for External Device)	

Model		DS-19S08N-04F/Kx	DS-19S08N-04F/KxGx
	Working Temperature	-10°C~+55°C (14°F~131°F)	
	Working Humidity	10%~90%	
	Mounting	Wall-mounted	
	Dimensions	200×247×35mm	
	Weight	≤0.81Kg	

The specification of DS-19S08-04F/Kx (Gx) video security control panel.

Model		DS-19S08-04F/Kx	DS-19S08-04F/KxGx
Security Control Panel Parameters	Alarm Input	8-zone Alarm Input	
	Alarm Output	1-ch Local+8-ch expandable, 30VDC/1A	
	Siren Power Supply	12VDC /500mA	
	Keypad	K1: LED Keypad; K2: LCD Keypad	
	Supported External Keypad	8	
	Tamper-proof Switch	Support Tamper-proof and Movement Prevention Function	
	Scheduled Arming/Disarming	8 Time Periods Each Day	
	Partition system	8 Partition Systems, 1 Public Partition System	
	Detector Tamper-proof Alarm	Support	
	Supported Remote Controls	32 (Unobstructed Effective Range of 100m)	
	SMS Alarm Data-push	N/A	Support
	SMS Arming/disarming Data-push	N/A	Support
Media Parameters	Video Input	4-ch WD1/960H, PAL/NTSC Self-adaptive	
	Video Input Interface	BNC Interface (1.0 Vp-p, 75Ω)	
	VGA Output Resolution	1-ch, Resolution: 1024×768/60Hz, 1280×720/60Hz, 1280×1024/60Hz, 1600×1200/60Hz,	1-ch, Resolution: 1024×768/60Hz, 1280×720/60Hz, 1280×1024/60Hz, 1600×1200/60Hz, 1920×1080p/60Hz
	Audio Input	1-ch, RCA (Linear, 1kΩ)	
	Audio Output	1-ch, RCA (Linear, 1kΩ)	
	Audio Compression	G.711u	
	Audio Code Rate	8Kbps	
	Two-way Audio	1-ch, RCA Interface (Linear, 1kΩ)	
	Loudspeaker	1-ch Built-in	
	Video Encoding Standard	H.264	
Resolution	WD1/4CIF/CIF/QCIF, Real-time		

Model		DS-19S08-04F/Kx	DS-19S08-04F/KxGx
	Video Frame Rate	PAL: 1/16~25fps NTSC: 1/16~30fps	
	Video Bitrate	32Kbps~16Mbps	
	Stream Type	Video & Audio/Video	
	Dual Stream	Support; Sub-stream: CIF/QCIF	
	Synchronous Playback	4-ch	
	Post View	Delay duration can be configured	
	Capture for Rechecking	20 Captures (10 Captures before/after Alarm)	
	Record Type	Manual Record, Scheduled Record, Motion Detection Record	
	Playback Mode	Instant Playback, Normal Playback, Event Playback	
	HDD Information	500G 2.5"HDD, SATA Interface	
Wireless Network Parameters	Wireless Network Standard	N/A	GLT: 4G TDD-LTE/GLF: 4G FDD-LTE/ GW: 3G WCDMA/GE: 3G EVDO
	UIM Card Slot		1
	SMA Antenna Interface		1
	Network Protocol	NTP, SADP, PPPoE, DHCP	
Interfaces and Appearance	Network Interface	1 RJ45 10M/100M Self-adaptive	
	RS485	1, RS485 Half-duplex, Support PTZ Control	
	Keypad Bus	1, RS485 Half-duplex	
	USB Interface	1, USB2.0	
	Storage Battery Port	1 Port, for Storage Battery Accessing	
	Power Supply	14.3VDC /2.8A	
	Consumption	6.5W (Without HDD and Power Supply for External Device)	
	Working Temperature	-10°C~+55°C (14°F~131°F)	
	Working Humidity	10%~90%	
	Installation Mode	Wall-mounted	
	Dimensions	200×247×35mm	
Weight	≤ 0.81kg		

Appendix2: CID Report

CID Code	Description	CID Code	Description
1103	Instant 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 Duress Alarm
1336	Printer Disconnection	3336	Printer Disconnection Recovery
1354	Phone Line Disconnection	3354	Phone Line Disconnection Recovery
1382	Local Expanded Zone Fault	3382	Local Expanded Zone 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

CID Code	Description	CID Code	Description
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 Enabling	3942	Video Loss Alarm 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
383	Detector Tamper-proof	442	Compulsive Arming/Disarming
443	Auto-switch Trigger	455	Auto-arming failed.
460	Tigger auto-enabling failed.	461	Tigger auto-disabling failed.
462	Auto-disarming failed.		

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

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#PasswordPa ssword 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#PasswordP assword 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: _____

0 5 1 6 0 0 0 0 #	51#Password User Name: _____	0 5 2 6 0 0 0 0 #	52#Password User Name: _____
0 5 3 6 0 0 0 0 #	53#Password User Name: _____	0 5 4 6 0 0 0 0 #	54#Password User Name: _____
0 5 5 6 0 0 0 0 #	55#Password User Name: _____	0 5 6 6 0 0 0 0 #	56#Password User Name: _____
0 5 7 6 0 0 0 0 #	57#Password User Name: _____	0 5 8 6 0 0 0 0 #	58#Password User Name: _____
0 5 9 6 0 0 0 0 #	59#Password User Name: _____	0 6 0 6 0 0 0 0 #	60#Password User Name: _____
0 6 1 6 0 0 0 0 #	61#Password User Name: _____	0 6 2 6 0 0 0 0 #	62#Password User Name: _____
0 6 3 6 0 0 0 0 #	63#Password User Name: _____	0 6 4 6 0 0 0 0 #	64#Password User Name: _____
0 6 5 6 0 0 0 0 #	65#Password User Name: _____	0 6 6 6 0 0 0 0 #	66#Password User Name: _____
0 6 7 6 0 0 0 0 #	67#Password User Name: _____	0 6 8 6 0 0 0 0 #	68#Password User Name: _____
0 6 9 6 0 0 0 0 #	69#Password User Name: _____	0 7 0 6 0 0 0 0 #	70#Password User Name: _____
0 7 1 6 0 0 0 0 #	71#Password User Name: _____	0 7 2 6 0 0 0 0 #	72#Password User Name: _____
0 7 3 6 0 0 0 0 #	73#Password User Name: _____	0 7 4 6 0 0 0 0 #	74#Password User Name: _____
0 7 5 6 0 0 0 0 #	75#Password User Name: _____	0 7 6 6 0 0 0 0 #	76#Password User Name: _____
0 7 7 6 0 0 0 0 #	77#Password User Name: _____	0 7 8 6 0 0 0 0 #	78#Password User Name: _____
0 7 9 6 0 0 0 0 #	79#Password User Name: _____	0 8 0 6 0 0 0 0 #	80#Password User Name: _____
0 8 1 6 0 0 0 0 #	81#Password User Name: _____	0 8 2 6 0 0 0 0 #	82#Password User Name: _____
0 8 3 6 0 0 0 0 #	83#Password User Name: _____	0 8 4 6 0 0 0 0 #	84#Password User Name: _____
0 8 5 6 0 0 0 0 #	85#Password User Name: _____	0 8 6 6 0 0 0 0 #	86#Password User Name: _____
0 8 7 6 0 0 0 0 #	87#Password User Name: _____	0 8 8 6 0 0 0 0 #	88#Password User Name: _____
0 8 9 6 0 0 0 0 #	89#Password User Name: _____	0 9 0 6 0 0 0 0 #	90#Password User Name: _____
0 9 1 6 0 0 0 0 #	91#Password User Name: _____	0 9 2 6 0 0 0 0 #	92#Password User Name: _____
0 9 3 6 0 0 0 0 #	93#Password User Name: _____	0 9 4 6 0 0 0 0 #	94#Password User Name: _____
0 9 5 6 0 0 0 0 #	95#Password User Name: _____	0 9 6 6 0 0 0 0 #	96#Password User Name: _____
0 9 7 6 0 0 0 0 #	97#Password User Name: _____	0 9 8 6 0 0 0 0 #	98#Password User Name: _____
0 9 9 6 0 0 0 0 #	99#Password User Name: _____	1 0 0 6 0 0 0 0 #	100#Password User Name: _____

1 0 1 6 0 0 0 0 #	101#Password User Name: _____	1 0 2 6 0 0 0 0 #	102#Password User Name: _____
1 0 3 6 0 0 0 0 #	103#Password User Name: _____	1 0 4 6 0 0 0 0 #	104#Password User Name: _____
1 0 5 6 0 0 0 0 #	105#Password User Name: _____	1 0 6 6 0 0 0 0 #	106#Password User Name: _____
1 0 7 6 0 0 0 0 #	107#Password User Name: _____	1 0 8 6 0 0 0 0 #	108#Password User Name: _____
1 0 9 6 0 0 0 0 #	109#Password User Name: _____	1 1 0 6 0 0 0 0 #	110#Password User Name: _____
1 1 1 6 0 0 0 0 #	111#Password User Name: _____	1 1 2 6 0 0 0 0 #	112#Password User Name: _____
1 1 3 6 0 0 0 0 #	113#Password User Name: _____	1 1 4 6 0 0 0 0 #	114#Password User Name: _____
1 1 5 6 0 0 0 0 #	115#Password User Name: _____	1 1 6 6 0 0 0 0 #	116#Password User Name: _____
1 1 7 6 0 0 0 0 #	117#Password User Name: _____	1 1 8 6 0 0 0 0 #	118#Password User Name: _____
1 1 9 6 0 0 0 0 #	119#Password User Name: _____	1 2 0 6 0 0 0 0 #	120#Password User Name: _____
1 2 1 6 0 0 0 0 #	121#Password User Name: _____	1 2 2 6 0 0 0 0 #	122#Password User Name: _____
1 2 3 6 0 0 0 0 #	123#Password User Name: _____	1 2 4 6 0 0 0 0 #	124#Password User Name: _____
1 2 5 6 0 0 0 0 #	125#Password User Name: _____	1 2 6 6 0 0 0 0 #	126#Password User Name: _____
1 2 7 6 0 0 0 0 #	127#Password User Name: _____	1 2 8 6 0 0 0 0 #	128#Password User Name: _____
1 2 9 6 0 0 0 0 #	129#Password User Name: _____	1 3 0 6 0 0 0 0 #	130#Password User Name: _____
1 3 1 6 0 0 0 0 #	131#Password User Name: _____	1 3 2 6 0 0 0 0 #	132#Password User Name: _____
1 3 3 6 0 0 0 0 #	133#Password User Name: _____	1 3 4 6 0 0 0 0 #	134#Password User Name: _____
1 3 5 6 0 0 0 0 #	135#Password User Name: _____	1 3 6 6 0 0 0 0 #	136#Password User Name: _____
1 3 7 6 0 0 0 0 #	137#Password User Name: _____	1 3 8 6 0 0 0 0 #	138#Password User Name: _____
1 3 9 6 0 0 0 0 #	139#Password User Name: _____	1 4 0 6 0 0 0 0 #	140#Password User Name: _____
1 4 1 6 0 0 0 0 #	141#Password User Name: _____	1 4 2 6 0 0 0 0 #	142#Password User Name: _____
1 4 3 6 0 0 0 0 #	143#Password User Name: _____	1 4 4 6 0 0 0 0 #	144#Password User Name: _____
1 4 5 6 0 0 0 0 #	145#Password User Name: _____	1 4 6 6 0 0 0 0 #	146#Password User Name: _____
1 4 7 6 0 0 0 0 #	147#Password User Name: _____	1 4 8 6 0 0 0 0 #	148#Password User Name: _____
1 4 9 6 0 0 0 0 #	149#Password User Name: _____	1 5 0 6 0 0 0 0 #	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: _____

2 0 1 2 5 0 1 0 1 #	Region1 Parameters Configuration	2 0 2 2 5 0 1 0 1 #	Region2 Parameters Configuration
2 0 3 2 5 0 1 0 1 #	Region3 Parameters Configuration	2 0 4 2 5 0 1 0 1 #	Region4 Parameters Configuration
2 0 5 2 5 0 1 0 1 #	Region5 Parameters Configuration	2 0 6 2 5 0 1 0 1 #	Region6 Parameters Configuration
2 0 7 2 5 0 1 0 1 #	Region7 Parameters Configuration	2 0 8 2 5 0 1 0 1 #	Region8 Parameters Configuration
2 0 9 2 5 0 1 0 1 #	Region9 Parameters Configuration	2 1 0 2 5 0 1 0 1 #	Region10 Parameters Configuration
2 1 1 2 5 0 1 0 1 #	Region11 Parameters Configuration	2 1 2 2 5 0 1 0 1 #	Region12 Parameters Configuration
2 1 3 2 5 0 1 0 1 #	Region13 Parameters Configuration	2 1 4 2 5 0 1 0 1 #	Region14 Parameters Configuration
2 1 5 2 5 0 1 0 1 #	Region15 Parameters Configuration	2 1 6 2 5 0 1 0 1 #	Region16 Parameters Configuration
<hr/>			
4 5 7 0 0 3 3 #	Communication Control		
4 5 8 0 0 0 0 #	Alarm Center 1 Account Settings	4 5 9 0 0 0 0 #	Alarm Center 2 Account Settings
<hr/>			
4 6 0 E 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 #	Alarm Center 1Phone Number Settings		
4 6 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 #	Alarm Center 1Phone Number Settings		
4 6 2 E 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 #	Alarm Center 2Phone Number Settings		
4 6 3 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 #	Alarm Center 2Phone Number Settings		

4 6 7 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | # | Region Linked Trigger Configuration
4 6 8 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | # | Enable Trigger Event Linkage Configuration
4 6 9 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | # | Disable Trigger Event Linkage Configuration
4 7 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | # | Trigger Time Settings **4 7 1** | 1 | # | Siren Settings

4 7 2 | 2 | 0 | 1 | 3 | 0 | 1 | 0 | 1 | 0 | 8 | 0 | 0 | 0 | 0 | # | Host Time Settings
4 7 3 | 1 | 9 | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 6 | 4 | # | Host IP Address Settings
4 7 4 | 0 | 8 | 0 | 0 | 0 | # | Host Port Number Settings

4 7 5 | 2 | 5 | 5 | 2 | 5 | 5 | 2 | 5 | 5 | 0 | 0 | 0 | # | Subnet Mask Settings
4 7 6 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | # | Gateway Settings

4 8 5 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | # | Network Center 1 IP Configuration Programming Address
4 8 6 | 0 | 0 | 0 | 0 | 0 | # | Network Center 1 Port Configuration Programming Address
4 8 7 | 2 | 0 | 0 | 0 | 0 | 0 | 0 | # | Network Center 1 Protocol and Account Configuration Programming Address

4 8 8 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | # | Network Center 2 IP Configuration Programming Address
4 8 9 | 0 | 0 | 0 | 0 | 0 | # | Network Center 2 Port Configuration Programming Address
4 9 0 | 2 | 0 | 0 | 0 | 0 | 0 | 0 | # | Network Center 2 Protocol and Account Configuration Programming Address

4 9 1 0 0 0 0 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 0 #	Wireless Center 1 Port Configuration Programming Address		
4 9 3 2 0 0 0 0 0 0 0 #	Wireless Center 1 Protocol and Account Configuration Programming Address		
<hr/>			
4 9 4 0 0 0 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 0 #	Wireless Center 2 Port Configuration Programming Address		
4 9 6 2 0 0 0 0 0 0 0 #	Wireless Center 2 Protocol and Account Configuration Programming Address		
<hr/>			
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 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		
<hr/>			
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		
<hr/>			
5 3 1 5 1 3 2 0 #	System Time and Hostage Report Configuration		
5 3 1 6 0 0 0 0 #	System Report and Arming/Disarming Prompt Configuration		
5 3 1 7 1 1 1 1 #	System Key User Permission Configuration		

5	6	4	1	1	1	1	1	1	1	1	1	#	Host System Fault Detection Configuration
5	6	7	0	1	1	1	1	1	1	1	1	#	System Fault Display Configuration
5	6	8	0	1	1	1	1	1	1	1	1	#	System Keyboard Fault Prompt Sound Configuration

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

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

8 0 1 1 1 1 # Video Preview Configuration

First Choice for Security Professionals