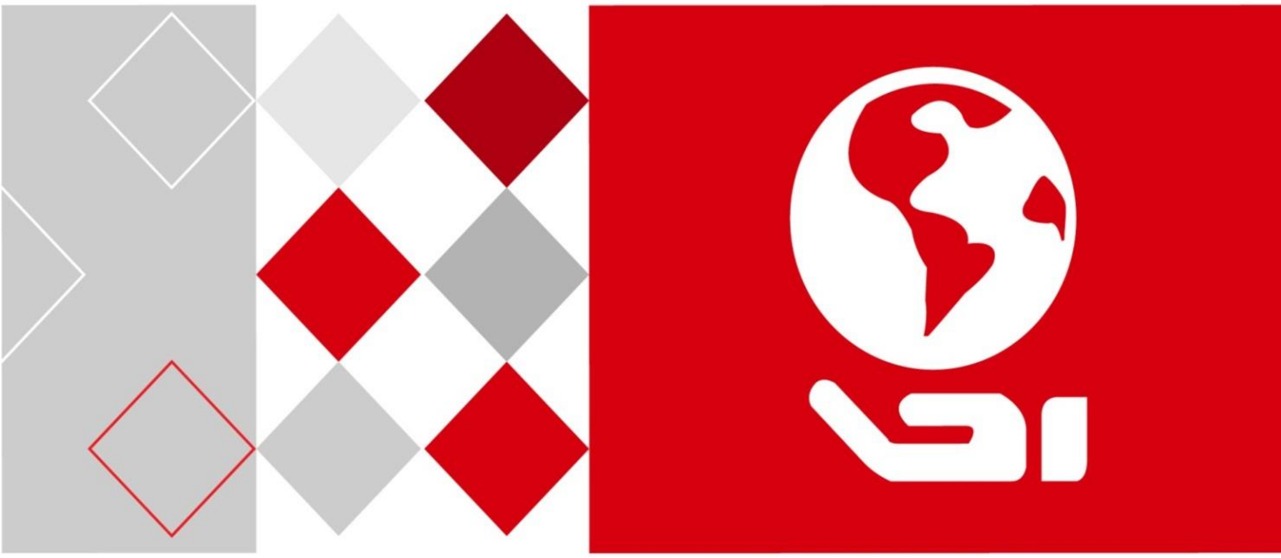
HIKVISION



Estación de alarma de pánico

Manual de usuario

User Manual

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 panic alarm station.

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

Please use this user manual under the guidance of professionals.

Trademarks Acknowledgement

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

Legal Disclaimer

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

REGARDING TO THE PRODUCT WITH INTERNET ACCESS, THE USE OF PRODUCT SHALL BE WHOLLY AT YOUR OWN RISKS. HIKVISION SHALL NOT TAKE ANY RESPONSIBILITES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER ATTACK, HACKER ATTACK, VIRUS INSPECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.

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

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

Regulatory Information

FCC Information

Please take attention that changes or modification not expressly approved by the party responsible for compliance could void the user’s authority to operate the equipment.

FCC Compliance: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

—Reorient or relocate the receiving antenna.
—Increase the separation between the equipment and receiver.
—Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
—Consult the dealer or an experienced radio/TV technician for help

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 2014/30/EU, LVD Directive 2014/35/EU, 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.

Applicable Models

This manual is applicable to the models listed in the following table.

Product	Model
Panic Alarm Station	DS-PEA1-21
Box Panic Alarm Station	DS-PEA2-21
Pole Panic Alarm Station	DS-PEA3M-21 DS-PEA3M-21H

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
NOTE	Provides additional information to emphasize or supplement important points of the main text.
⚠ WARNING	Indicates a potentially hazardous situation, which if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
⚠ DANGER	Indicates a hazard with a high level of risk, which if not avoided, will result in death or serious injury.

Safety Instruction

⚠ **WARNING**

- The device should be used in compliance with local laws and electrical safety regulations. Refer to the appropriate documentation for detailed information.
- The input voltage should conform to IEC60950-1 standard: SELV (Safety Extra Low Voltage) and the Limited Power Source (100～120/200～240 VAC). Refer to the appropriate documentation for detailed information.
- DO NOT connect multiple devices to one power adapter, to avoid over-heating or fire hazards caused by overload.
- Make sure the plug is properly connected to the power socket.
- If smoke, odor, or noise arises from the device, immediately turn off the power, unplug the power cable, and contact the service center.

⚠ **WARNING**

- Do not drop the device or subject it to physical shock.
- Wipe the device gently with a clean cloth and a small quantity of ethanol, if necessary.
- Do not aim the lens at the sun or any other bright light.

- When any laser equipment is in use, make sure that the device lens is not exposed to the laser beam, or it may burn out.
  - Do not expose the device to high electromagnetic radiation or extremely hot, cold, dusty, or damp environments, the appropriate temperature is -40℃ to 60℃.
- Place the device in a dry and well-ventilated environment.
- Keep non-waterproof devices away from liquids.
- Keep the device in original or similar packaging while transporting it.
- A few device components (e.g., electrolytic capacitor) require regular replacement. The average lifespan varies, so periodic checking is recommended. Contact your dealer for details.
- Improper use or replacement of the battery may result in explosion hazard. Replace with the same or equivalent type only. Dispose of used batteries in conformance with the instructions provided by the battery manufacturer.
- Never attempt to disassemble the device.

Table of Content

Chapter 1 Overview

1.1 Description

DS-PEA series of active panic alarm station supports multiple networks. It provides live view, two-way audio, and customized audio input. It supports linkage with the surrounding cameras and external lamp, sound box, etc. It helps to realize alarm aid in emergency.

1.2 Key Features

- Network adaptive and video and audio adaptive
- Audio and video file storage
- H.264/H.265, G.711U, G726
- Video collection and all-day monitoring with 2MP HD IR camera
- Built-in omnidirectional microphone to realize two-way audio
- Multiple network protocols including TCP/IP, SNMP, RTSP and SADP
- Supports Hik-SIP, Ehome, and Ezviz
- Waterproof, anti-electromagnetic interference, tamper-proof, explosion-proof, and anti-lightning (Panic Alarm Station doesn’t support waterproof)

Chapter 2 Structure Description

2.1 Mainboard Description

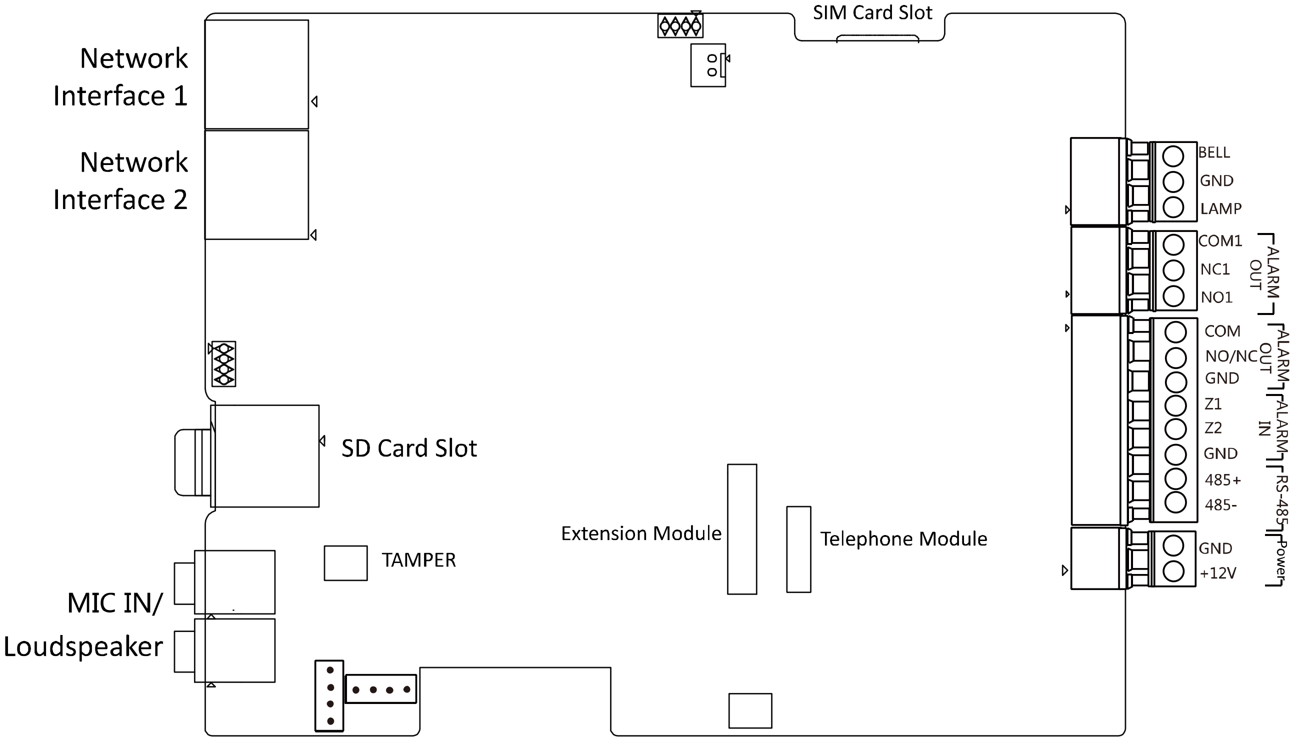


Figure 2-1 Mainboard of panic alarm station

2.2 Appearance Description

2.2.1 Panic Alarm Station

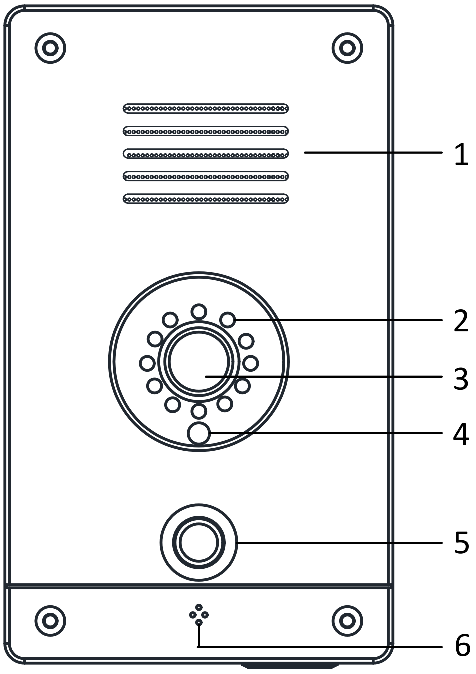


Figure 2-2 One-touch Panic Alarm Station

Table 2-1 Panel Description

No.	Description
1	Loudspeaker
2	IR Light
3	Camera
4	Light Sensor
5	Panic Alarm Button
6	Microphone

2.2.2 Box Panic Alarm Station

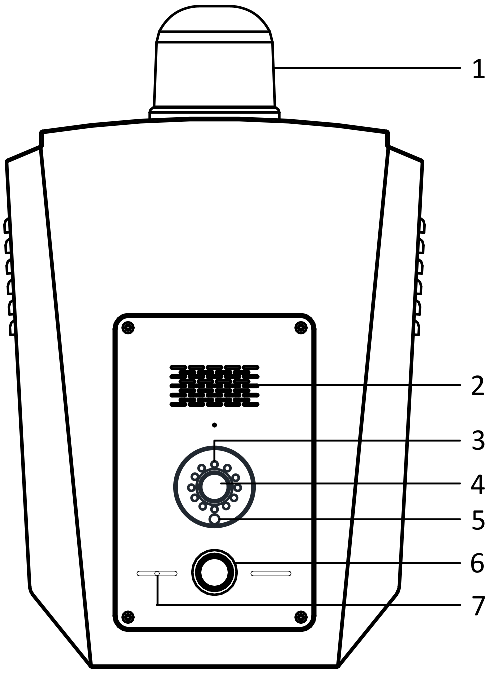


Figure 2-3 Case Panic Alarm Station

Table 2-2 Panel Description

No.	Description
1	Audible Alarm Lamp
2	Loudspeaker
3	IR Light
4	Camera
5	Light Sensor
6	Panic Alarm Button
7	Microphone

2.2.3 Pole Panic Alarm Station

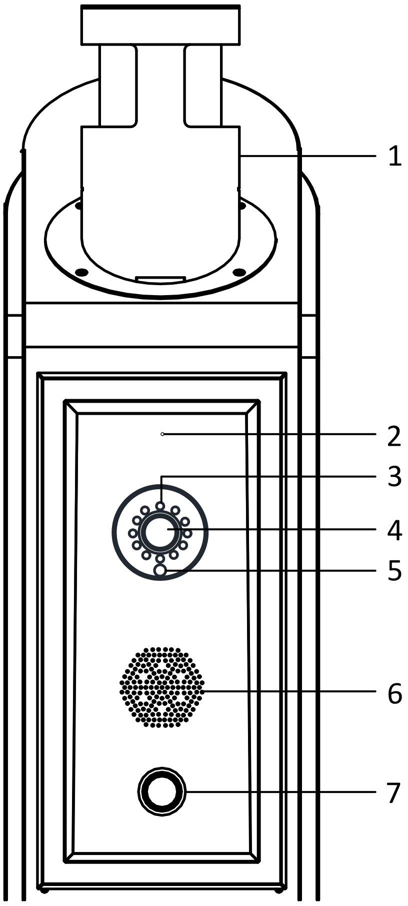


Figure 2-4 Pole Panic Alarm Station

Table 2-3 Panel Description

No.	Description
1	Audible Alarm Lamp
2	Microphone
3	IR Light
4	Camera
5	Light Sensor
6	Loudspeaker
7	Panic Alarm Button

2.3 Installation and Connections

⚠

- The product is suitable for mounting on concrete or other non-combustible surface only.
- For PLUGGABLE EQUIPMENT, the socket-outlet shall be installed near the equipment and should be easily accessible.
- For PERMANENTLY CONNECTED EQUIPMENT, a readily accessible disconnect device (2.5A) shall be incorporated external to the equipment.

2.3.1 Power Supply Wiring

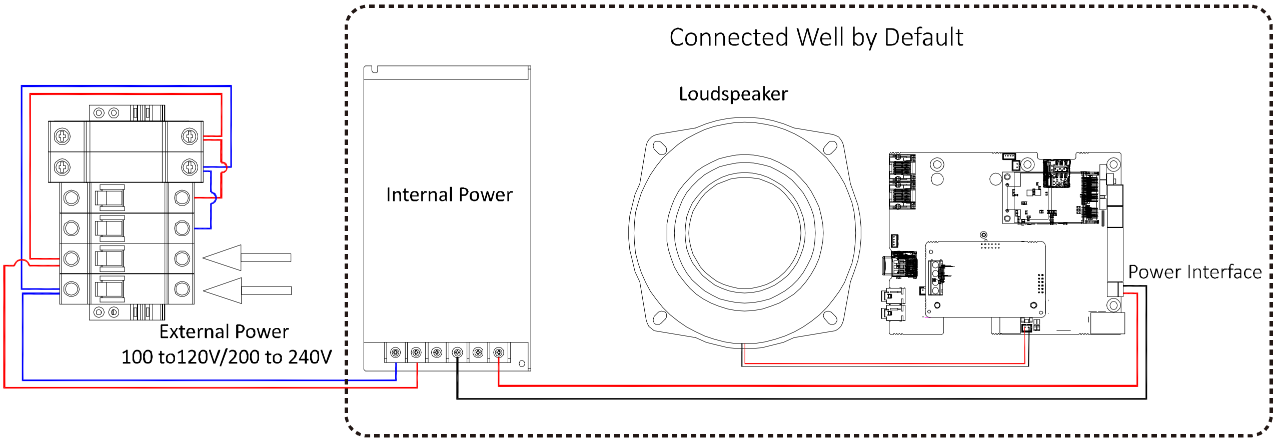


Figure 2-5 Power Supply Wiring

2.3.2 Network Wiring

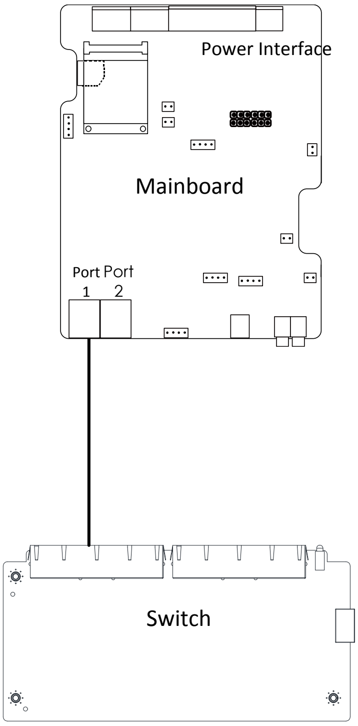


Figure 2-6 Network Wiring

2.3.3 Audible and Visual Alarm Wiring

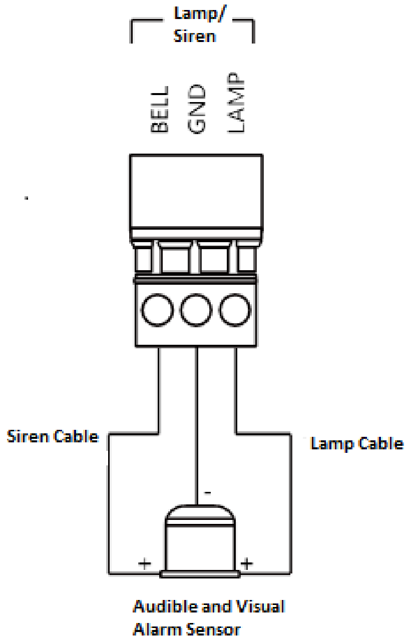


Figure 2-7 Audible and Visual Alarm Wiring

2.3.4 Alarm Input Wiring (Normally Open)

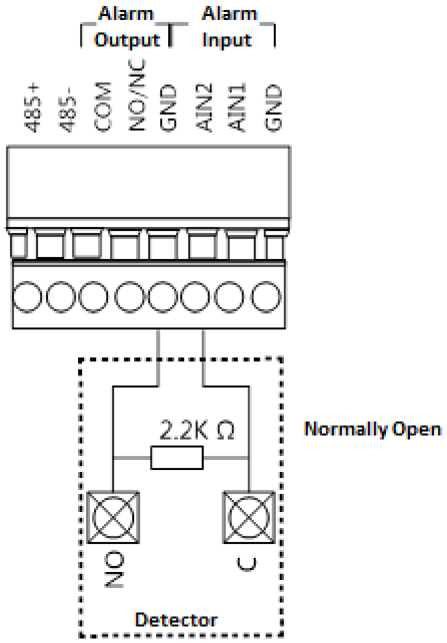


Figure 2-8 Alarm Input Wiring (Normally Open)

2.3.5 Pole Panic Alarm Station Installation

Pole Panic Alarm Station (without Speed Dome Bracket)Dimension

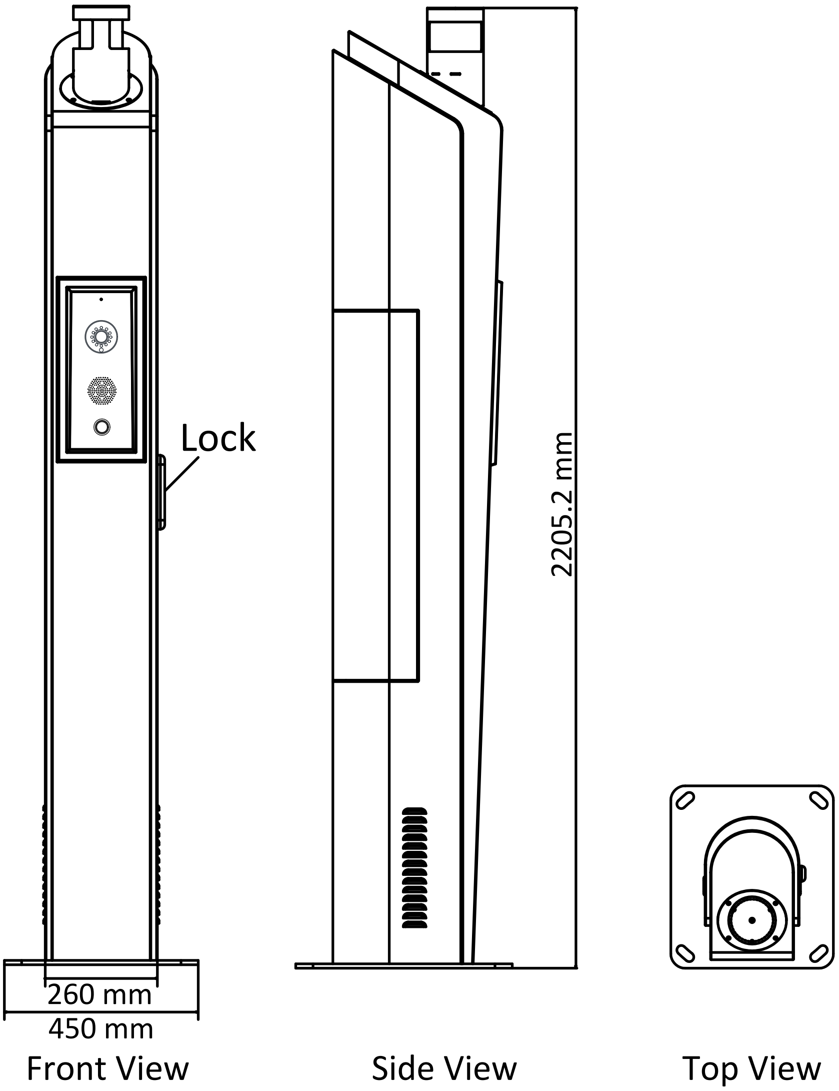


Figure 2-9 Pole Panic Alarm Station (without Speed Dome Bracket)Dimension

Pole Panic Alarm Station (with Speed Dome Bracket)Dimension

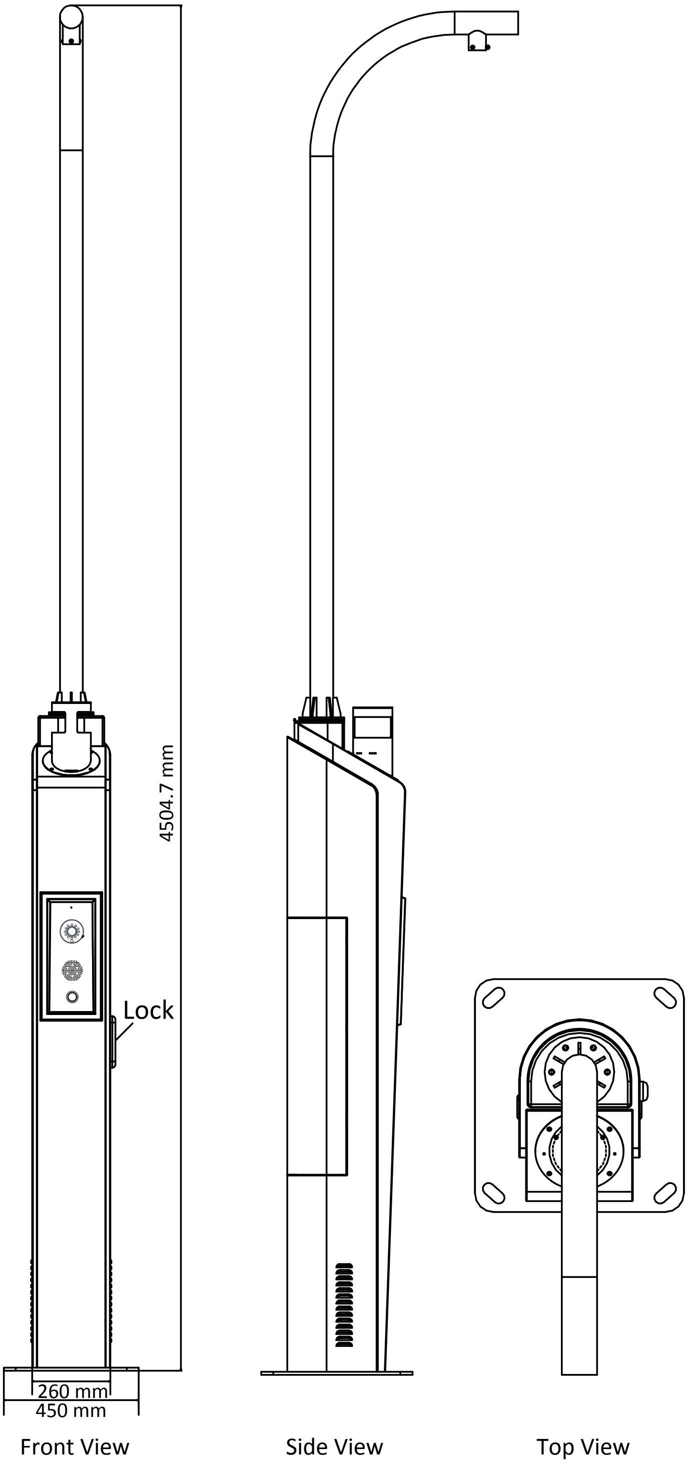


Figure 2-10 Pole Panic Alarm Station (with Speed Dome Bracket)Dimension

Pole Panic Alarm Station Grounding Cage Dimension(without Speed Dome Bracket)

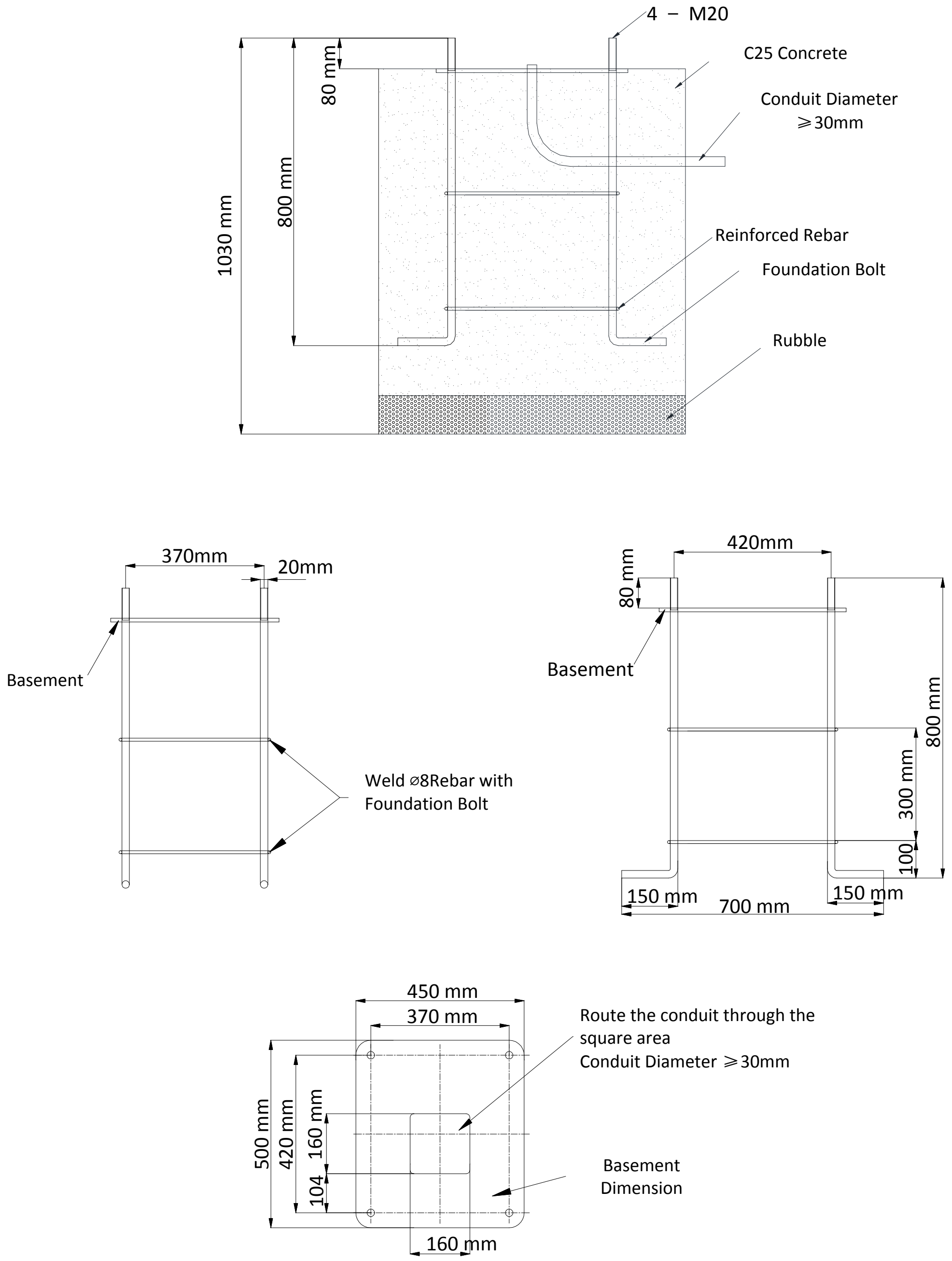


Figure 2-12 Pole Panic Alarm Station Grounding Cage Dimension(without Speed Dome Bracket)

Pole Panic Alarm Station Grounding Cage Dimension(with Speed Dome Bracket)

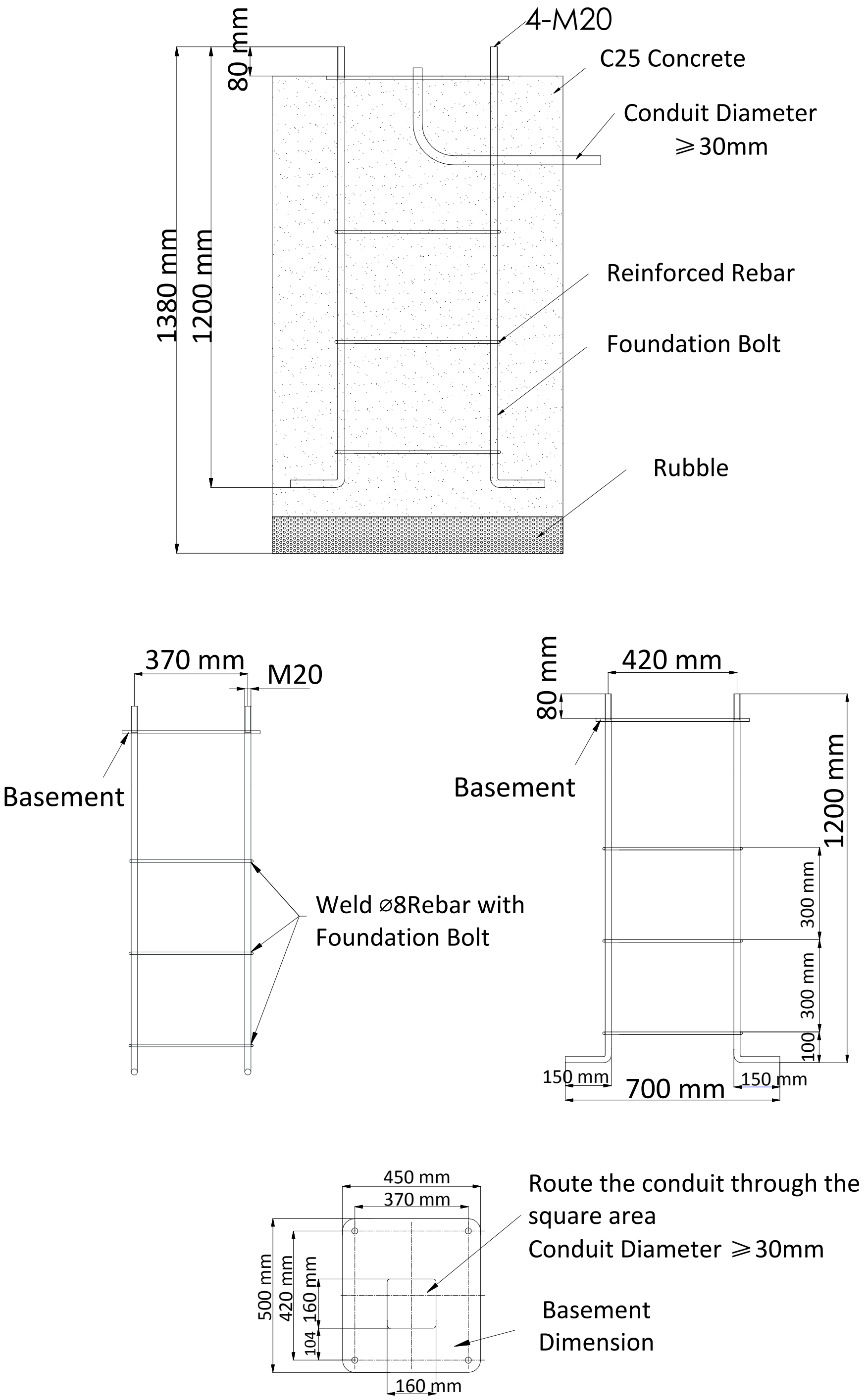


Figure 2-13 Pole Panic Alarm Station Grounding Cage Dimension(with Speed Dome Bracket)

Chapter 3 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.

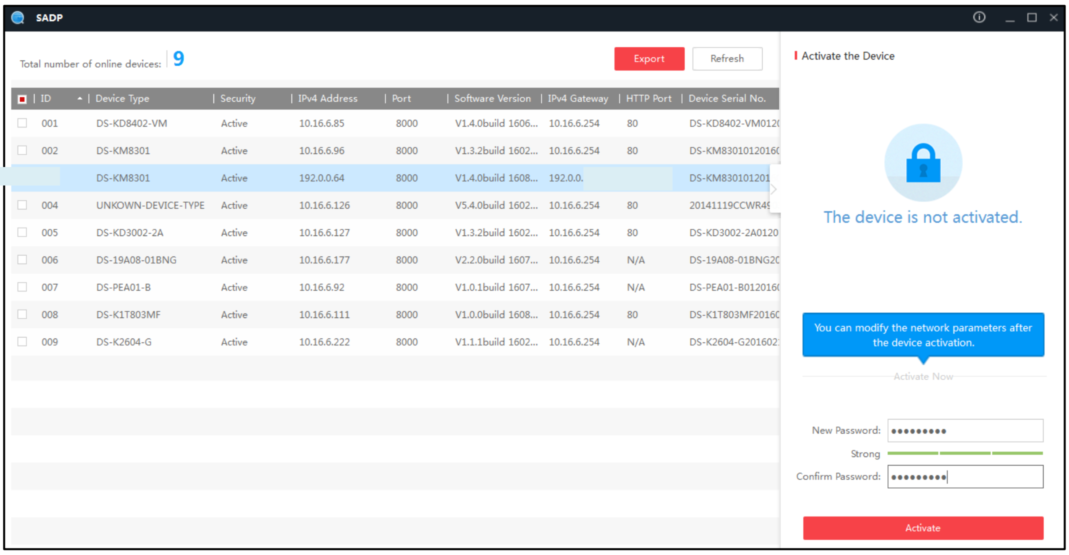
◆ Activation via SADP Software

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.



Total number of online devices: 9

☐	ID	Device Type	Security	IPv4 Address	Port	Software Version	IPv4 Gateway	HTTP Port	Device Serial No.
☐	001	DS-KD8402-VM	Active	10.16.6.85	8000	V1.4.0build 1606...	10.16.6.254	80	DS-KD8402-VM012(
☐	002	DS-KM8301	Active	10.16.6.96	8000	V1.3.2build 1602...	10.16.6.254	80	DS-KM8301012016(
		DS-KM8301	Active	192.0.0.64	8000	V1.4.0build 1608...	192.0.0.		DS-KM830101201
☐	004	UNKOWN-DEVICE-TYPE	Active	10.16.6.126	8000	V5.4.0build 1602...	10.16.6.254	80	20141119CCWR4
☐	005	DS-KD3002-2A	Active	10.16.6.127	8000	V1.3.2build 1602...	10.16.6.254	80	DS-KD3002-2A0120
☐	006	DS-19A08-01BNG	Active	10.16.6.177	8000	V2.2.0build 1607...	10.16.6.254	N/A	DS-19A08-01BNG2(
☐	007	DS-PEA01-B	Active	10.16.6.92	8000	V1.0.1build 1607...	10.16.6.254	N/A	DS-PEA01-B012016(
☐	008	DS-K1T803MF	Active	10.16.6.111	8000	V1.0.0build 1608...	10.16.6.254	80	DS-K1T803MF2016(
☐	009	DS-K2604-G	Active	10.16.6.222	8000	V1.1.1build 1602...	10.16.6.254	N/A	DS-K2604-G201602

Activate the Device

The device is not activated.

You can modify the network parameters after the device activation.

New Password: ●●●●●●●●●

Strong

Confirm Password: ●●●●●●●●●

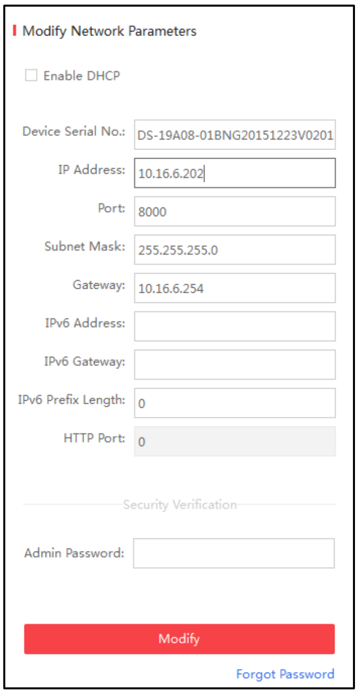
3. Create a password and input the password in the password field, and confirm the password.

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

4. Click **OK** to save the password.

   You can check whether the activation is completed on the popup window. If activation failed, please make sure that the password meets the requirement and then try again.

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



Modify Network Parameters

□ Enable DHCP

Device Serial No.: DS-19A08-01BNG20151223V0201

IP Address: 10.16.6.202

Port: 8000

Subnet Mask: 255.255.255.0

Gateway: 10.16.6.254

IPv6 Address:

IPv6 Gateway:

IPv6 Prefix Length: 0

HTTP Port: 0

Security Verification

Admin Password:

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

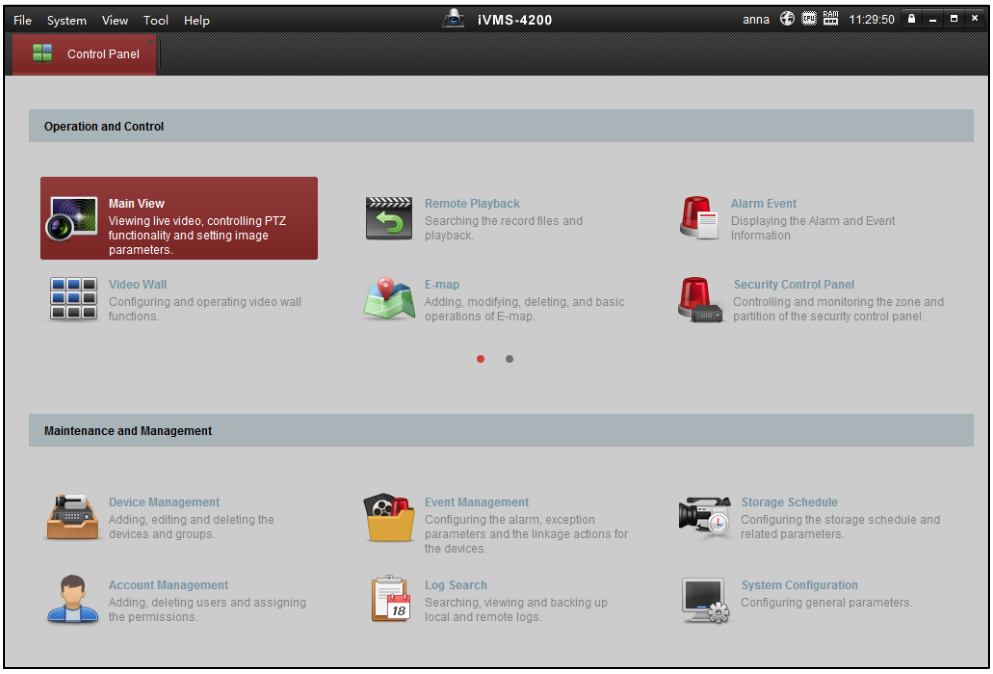
◆ Activation via Client Software

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

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

Steps:

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



Operation and Control

Main View
Viewing live video, controlling PTZ functionality and setting image parameters.

Remote Playback
Searching the record files and playback.

Alarm Event
Displaying the Alarm and Event Information

Video Wall
Configuring and operating video wall functions.

E-map
Adding, modifying, deleting, and basic operations of E-map.

Security Control Panel
Controlling and monitoring the zone and partition of the security control panel.

Maintenance and Management

Device Management
Adding, editing and deleting the devices and groups.

Event Management
Configuring the alarm, exception parameters and the linkage actions for the devices.

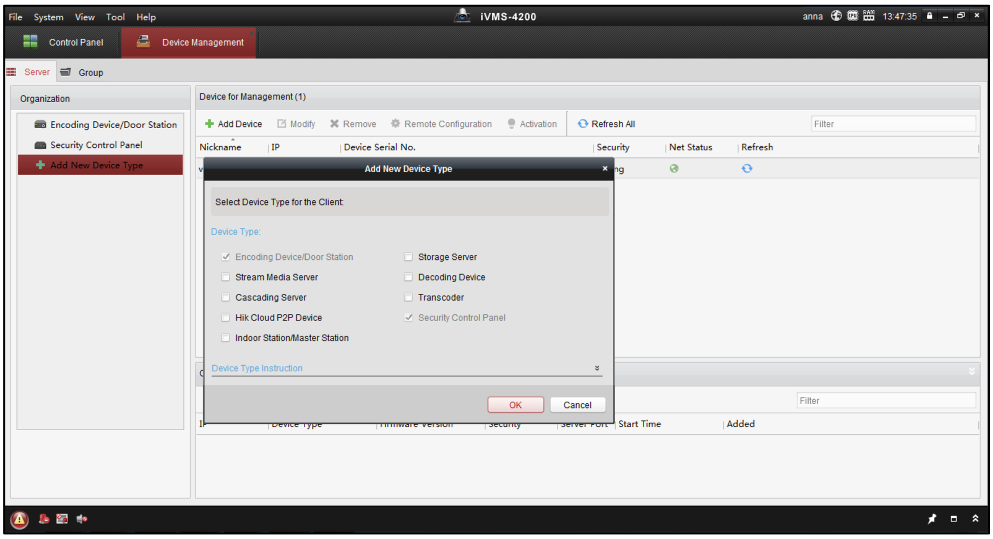
Storage Schedule
Configuring the storage schedule and related parameters.

Account Management
Adding, deleting users and assigning the permissions.

Log Search
Searching, viewing and backing up local and remote logs.

System Configuration
Configuring general parameters.

2. Click the **Device Management** icon to enter the Device Management interface, as shown in the figure below.
3. Click **Add Device Type** to enter the adding device type page.
4. Select **Security Control Panel**.



Add New Device Type

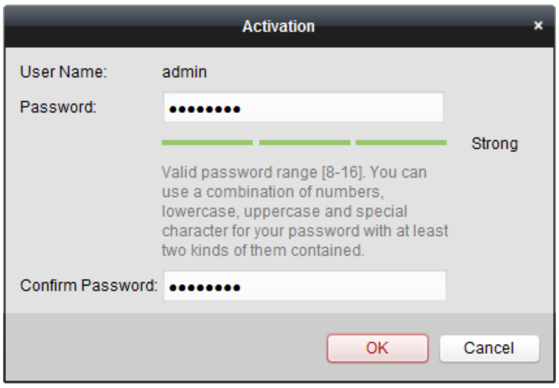
Select Device Type for the Client:

Device Type:

☑ Encoding Device/Door Station	□ Storage Server
□ Stream Media Server	□ Decoding Device
□ Cascading Server	□ Transcoder
□ Hik Cloud P2P Device	☑ Security Control Panel
□ Indoor Station/Master Station	

Device Type Instruction

5. Click **Security Control Panel** in the **Organization** list.
6. Check the device status from the device list, and select an inactive device.
7. Click the **Activate** button to pop up the Activation interface.
8. Create a password and input the password in the password field, and confirm the password.



Activation

User Name: admin

Password: ●●●●●●●●

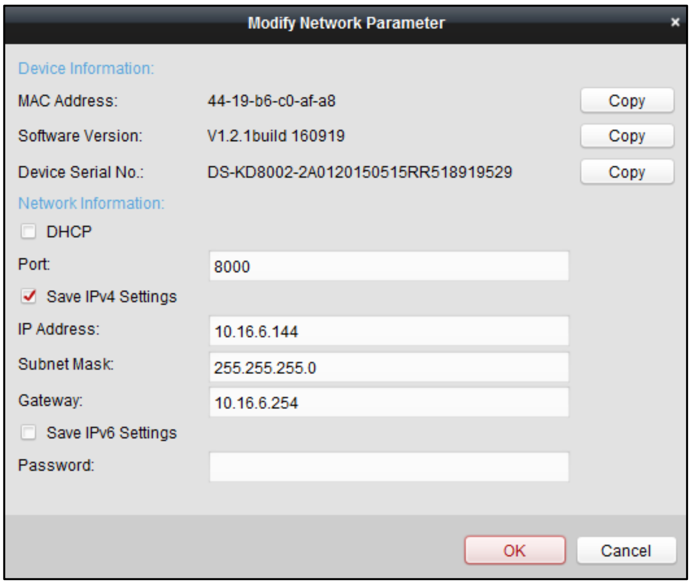
Strong

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 Password: ●●●●●●●●

<u>**STRONG PASSWORD RECOMMENDED**</u>– *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.*

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



Device Information:

MAC Address: 44-19-b6-c0-af-a8 Copy

Software Version: V1.2.1build 160919 Copy

Device Serial No.: DS-KD8002-2A0120150515RR518919529 Copy

Network Information:

□ DHCP

Port: 8000

☑ Save IPv4 Settings

IP Address: 10.16.6.144

Subnet Mask: 255.255.255.0

Gateway: 10.16.6.254

□ Save IPv6 Settings

Password:

11. 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.
12. Input the password to activate your IP address modification.

Chapter 4 Device Remote Operation

For properly running the system, set a login password to activate the panic alarm station before the first use.
You can activate the device via SADP or client software.
The factory settings are show as follows.

IP address: 192.0.0.65

Port No.: 8000

Admin User NameP: admin

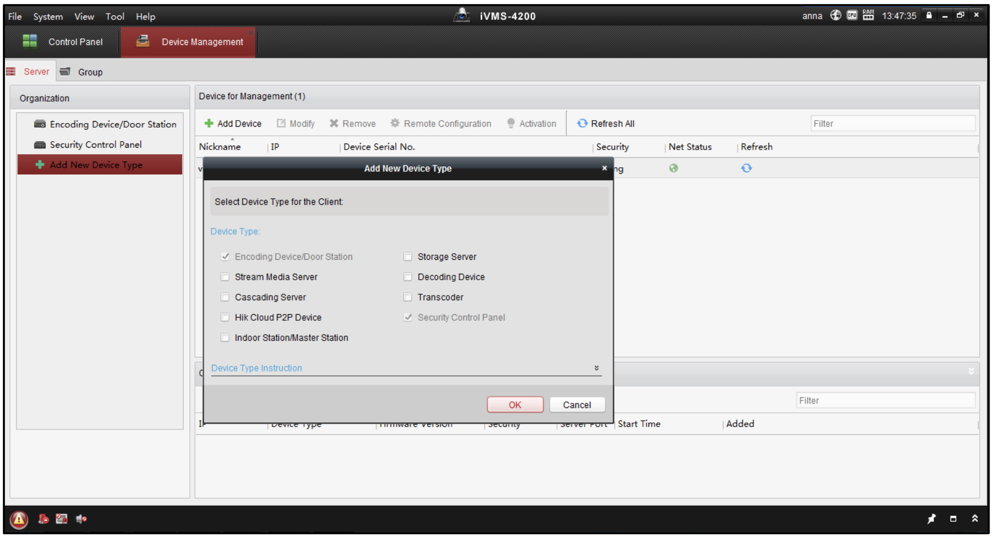
4.1 Device Management

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 device.

4.1.1 Add a Device

Steps:

1. Click the icon on the control panel to enter the Device Management interface and click the **Server** tab.
2. Click **Add New Device Type** on the Organization list and select **Security Control Panel**.
3. Click **OK** to save the settings, and the added security control panel type is displayed on the Organization list.



Add New Device Type

Select Device Type for the Client:

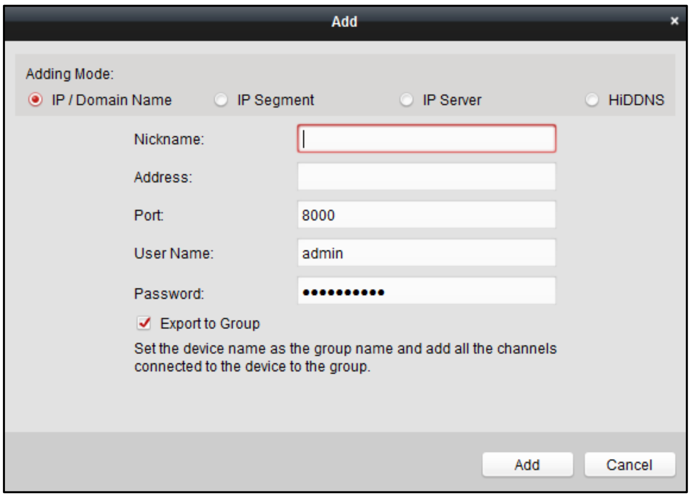
Device Type:

☑ Encoding Device/Door Station
☐ Storage Server
☐ Stream Media Server
☐ Decoding Device
☐ Cascading Server
☐ Transcoder
☐ Hik Cloud P2P Device
☑ Security Control Panel
☐ Indoor Station/Master Station

Device Type Instruction

OK Cancel

4. Click **Security Control Panel** and click **Add Device** to add the device to the management list of the software.
5. You can add the active online devices in the same local subnet with the client software, or select the adding mode by IP/Domain Name, by IP segment, by IP Server, or by HiDDNS, and configure the corresponding settings for the device. Take **IP/Domain Name** as an example.



Adding Mode:
● IP / Domain Name ○ IP Segment ○ IP Server ○ HiDDNS

Nickname:
Address:
Port: 8000
User Name: admin
Password: ••••••••••
☑ Export to Group
Set the device name as the group name and add all the channels connected to the device to the group.

6. 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.
7. 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.
8. Click **Add** to add the device.

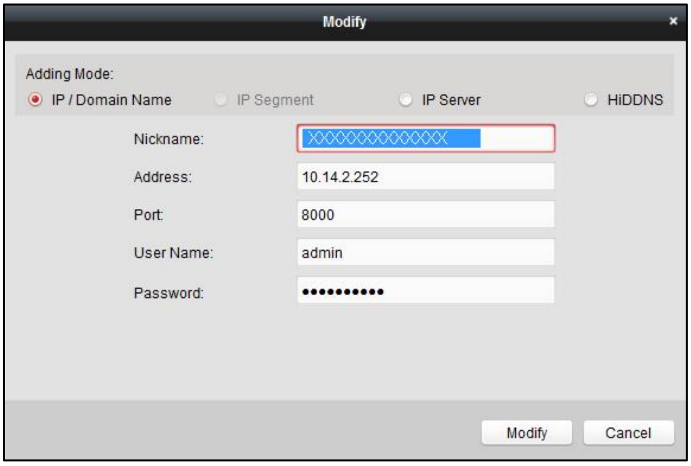
4.1.2 Edit a Device

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.



Adding Mode:
● IP / Domain Name ○ IP Segment ○ IP Server ○ HiDDNS

Nickname: XXXXXXXXXXXXX
Address: 10.14.2.252
Port: 8000
User Name: admin
Password: ••••••••••

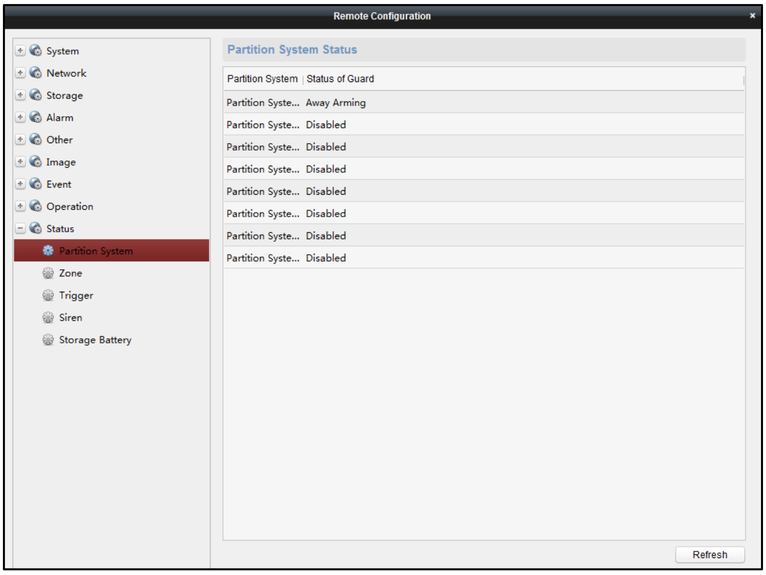
3. Enter the required nick name, address, and port number and then enter the admin username and password.
4. Click **Modify** to save the changes.

4.1.3 Delete a Device

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

4.1.4 Status

Click **Remote Configuration > Status** to view status of the partition, zone, trigger, siren ,and storage battery.



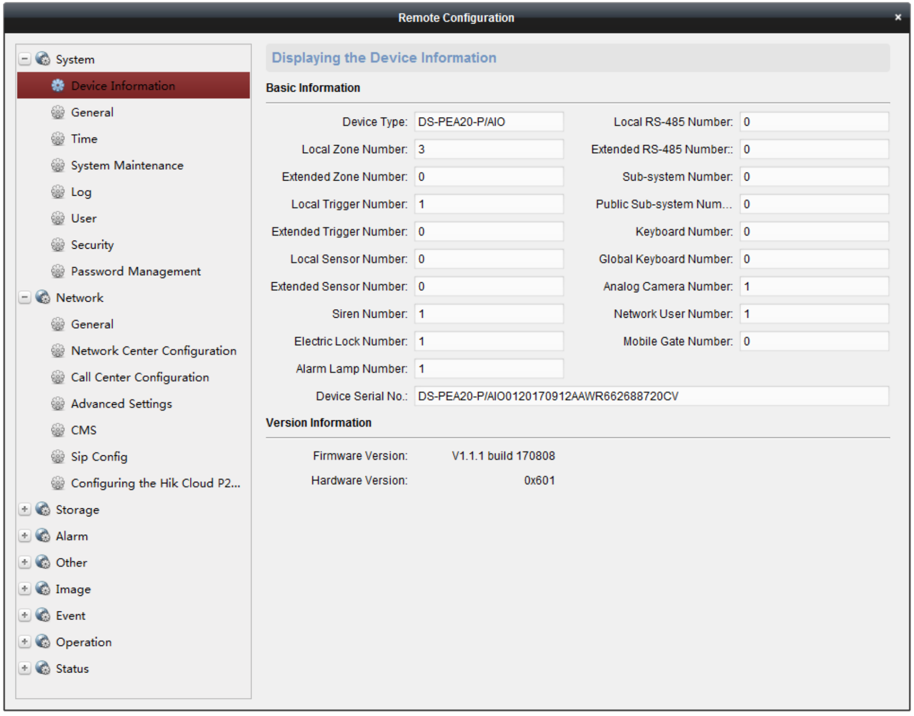
Partition System Status

Partition System	Status of Guard
Partition Syste...	Away Arming
Partition Syste...	Disabled
Partition Syste...	Disabled
Partition Syste...	Disabled
Partition Syste...	Disabled
Partition Syste...	Disabled
Partition Syste...	Disabled
Partition Syste...	Disabled

4.2 Remote Configurations

Purpose:

In this section, you are able to configure device parameters remotely.
Click the **Remote Configuration** button to enter the interface.



Displaying the Device Information

Basic Information

Device Type:	DS-PEA20-P/AIO	Local RS-485 Number:	0
Local Zone Number:	3	Extended RS-485 Number::	0
Extended Zone Number:	0	Sub-system Number:	0
Local Trigger Number:	1	Public Sub-system Num...	0
Extended Trigger Number:	0	Keyboard Number:	0
Local Sensor Number:	0	Global Keyboard Number:	0
Extended Sensor Number:	0	Analog Camera Number:	1
Siren Number:	1	Network User Number:	1
Electric Lock Number:	1	Mobile Gate Number:	0
Alarm Lamp Number:	1		
Device Serial No.:	DS-PEA20-P/AIO0120170912AAWR662688720CV		

Version Information

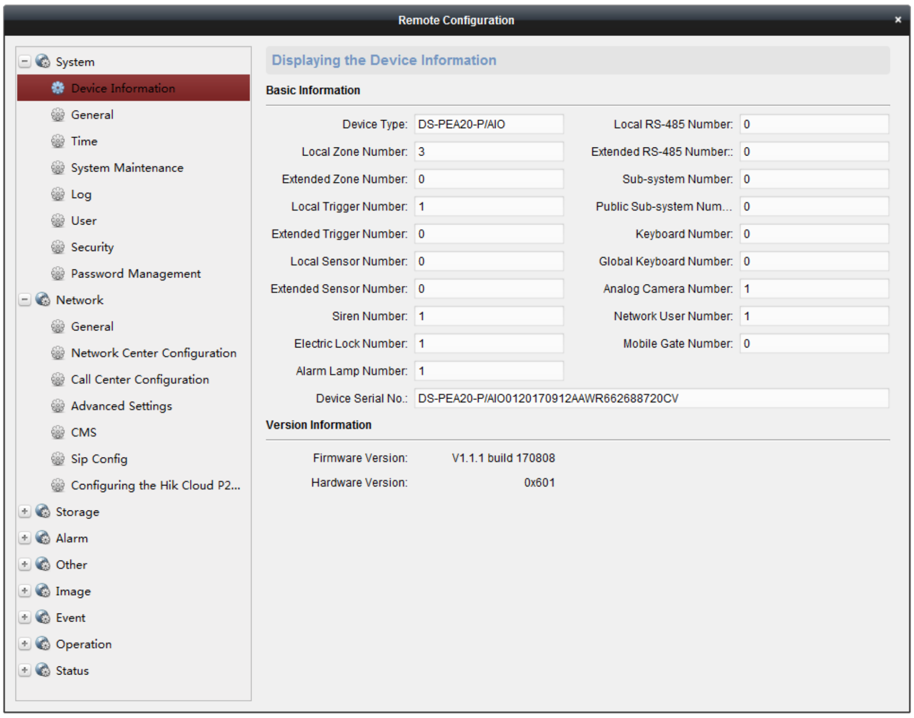
Firmware Version: V1.1.1 build 170808

Hardware Version: 0x601

4.2.1 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.



Displaying the Device Information

Basic Information

Device Type:	DS-PEA20-P/AIO	Local RS-485 Number:	0
Local Zone Number:	3	Extended RS-485 Number::	0
Extended Zone Number:	0	Sub-system Number:	0
Local Trigger Number:	1	Public Sub-system Num...	0
Extended Trigger Number:	0	Keyboard Number:	0
Local Sensor Number:	0	Global Keyboard Number:	0
Extended Sensor Number:	0	Analog Camera Number:	1
Siren Number:	1	Network User Number:	1
Electric Lock Number:	1	Mobile Gate Number:	0
Alarm Lamp Number:	1		
Device Serial No.:	DS-PEA20-P/AIO0120170912AAWR662688720CV		

Version Information

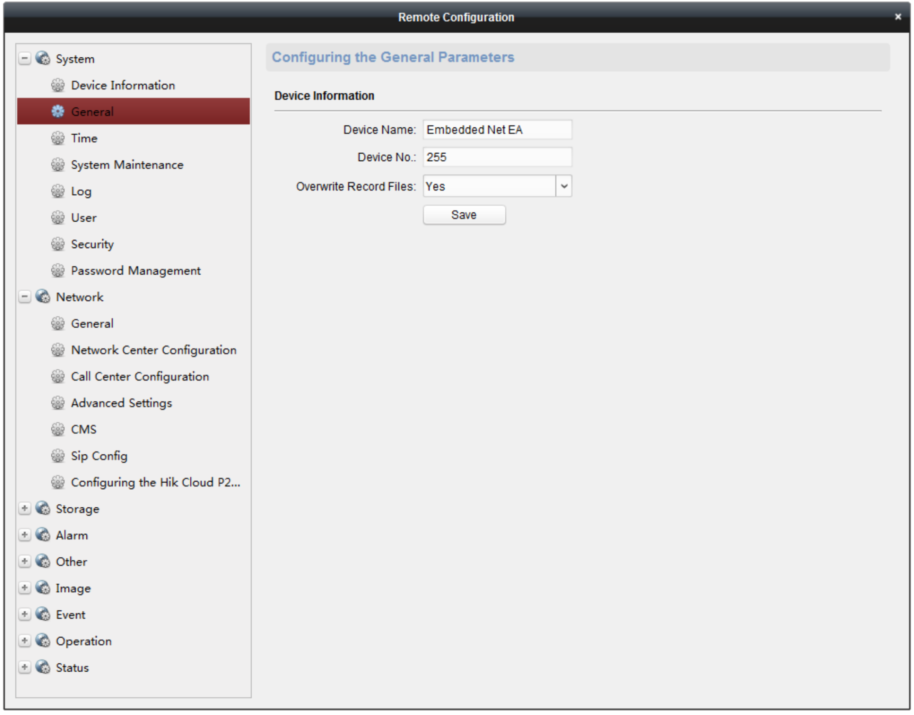
Firmware Version: V1.1.1 build 170808

Hardware Version: 0x601

General Settings

Steps:

1. Click **Remote Configuration > System > General** to enter the general parameters configuration interface.



Configuring the General Parameters

Device Information

Device Name: Embedded Net EA

Device No.: 255

Overwrite Record Files: Yes

2. Input the device name and device number.
3. Click the drop down menu to select whether to overwrite the record files.
4. Click **Save** to save the settings.

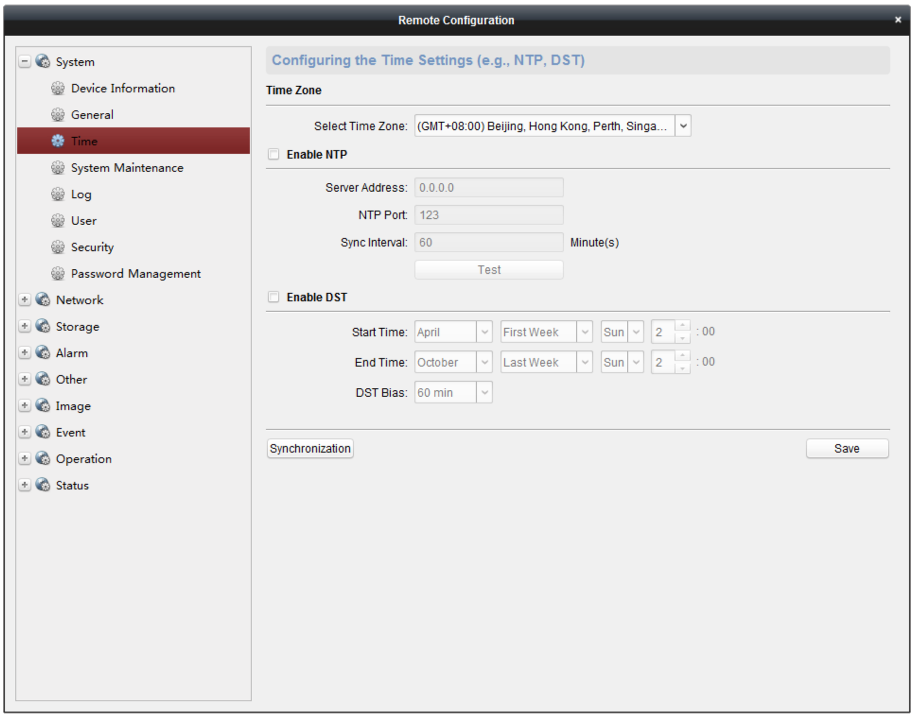
Timing Settings

Purpose:

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

Steps:

1. Click **Remote Configuration > System > Time** to enter the time configuration interface.



Configuring the Time Settings (e.g., NTP, DST)

Time Zone

Select Time Zone: (GMT+08:00) Beijing, Hong Kong, Perth, Singa...

□ Enable NTP

Server Address: 0.0.0.0

NTP Port: 123

Sync Interval: 60 Minute(s)

□ Enable DST

Start Time: April First Week Sun 2 : 00

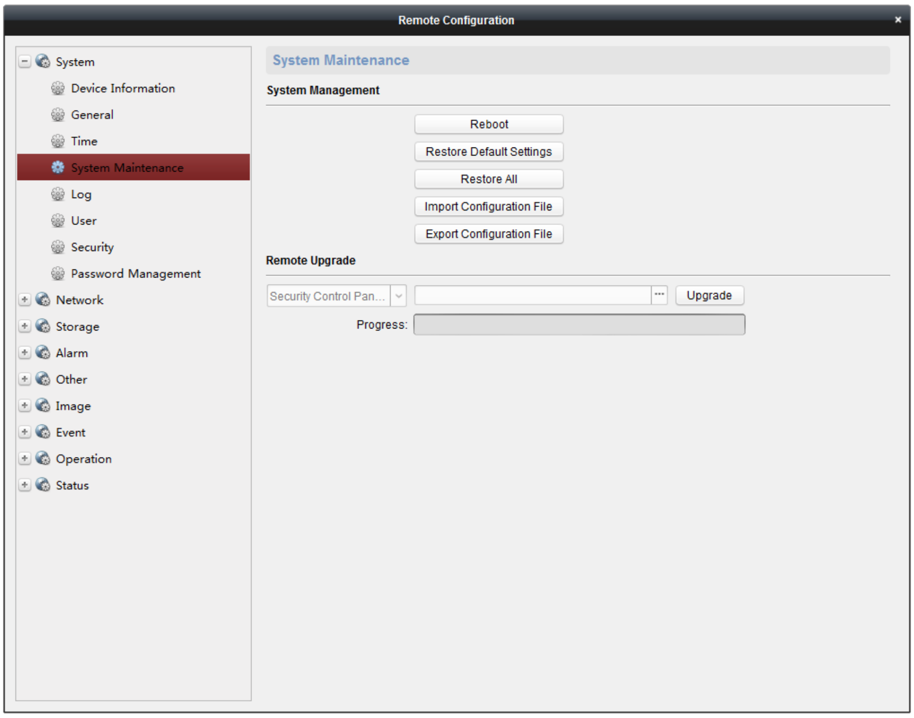
End Time: October Last Week Sun 2 : 00

DST Bias: 60 min

2. Click **Synchronization** to do timing.

System Maintenance

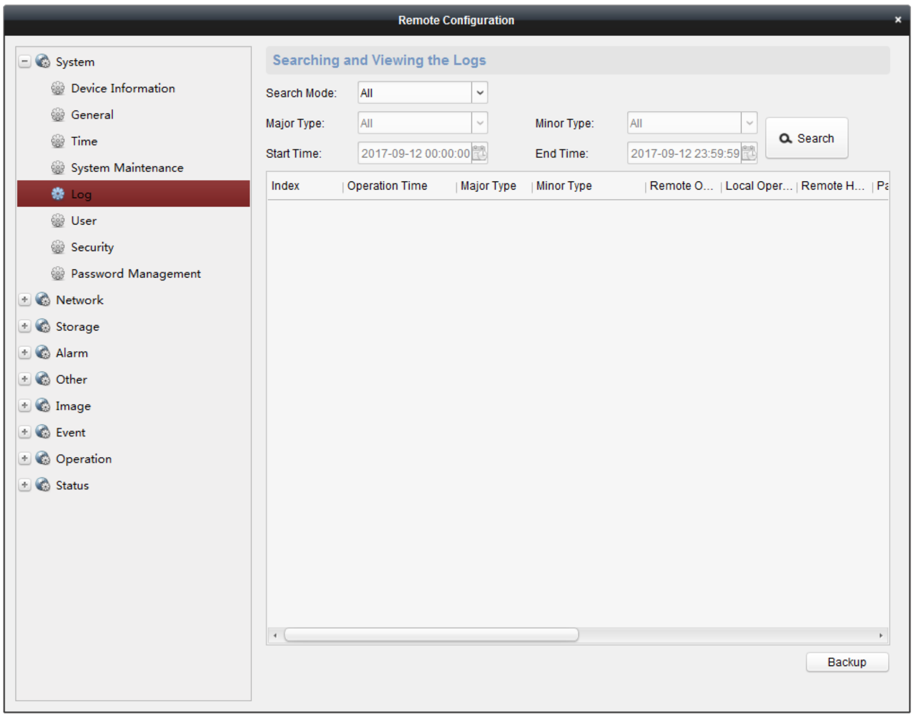
The device supports system maintenance remotely. Click **Remote Configuration > System > System Maintenance** to enter the interface.



- **Restart the System**
  Click **Reboot** to restart the device.
- **Restore Default Settings**
  Click **Restore Default Settings** to restore the default settings.
  NOTE
  Except the IP address and user parameters, all other parameters of the device will be restored to factory default settings.
- **Restore All the Parameters to Default**
  Click **Restore All** to restore all the parameters to factory default settings.
  NOTE
  After restoring the parameters to default, the device needs to be restarted.
- **Import Configuration File**
  The device supports importing the configuration file. Click **Import Configuration File** to import the file.
- **Export Configuration File**
  The device supports exporting the configuration file. Click **Export Configuration File** to export the file.
- **Import/Export IPC Configuration File**
  The device supports importing/exporting the IPC configuration file. Click **Import/Export IPC Configuration File** to import/export the file.
- **Remote Upgrade**
  The device also supports remote upgrading. You can select the upgrade file including security control panel upgrading file and alarm keypad upgrading file. Click ⋯ to select the local upgrading file and click **Upgrade** to upgrade the device. The upgrading progress is shown below.
  You need to enter the keypad address for keypad remote upgrade.
  NOTE
  After upgrading, the device needs to be restarted.

Log Searching

Click **Remote Configuration > System > Log** to search and view the logs. Set the search mode, major type, minor type, start time and end time, and then click **Search** to search the log.



Search Mode: All

Major Type: All

Minor Type: All

Start Time: 2017-09-12 00:00:00

End Time: 2017-09-12 23:59:59

Index	Operation Time	Major Type	Minor Type	Remote O...	Local Oper...	Remote H...	Pa

User Settings

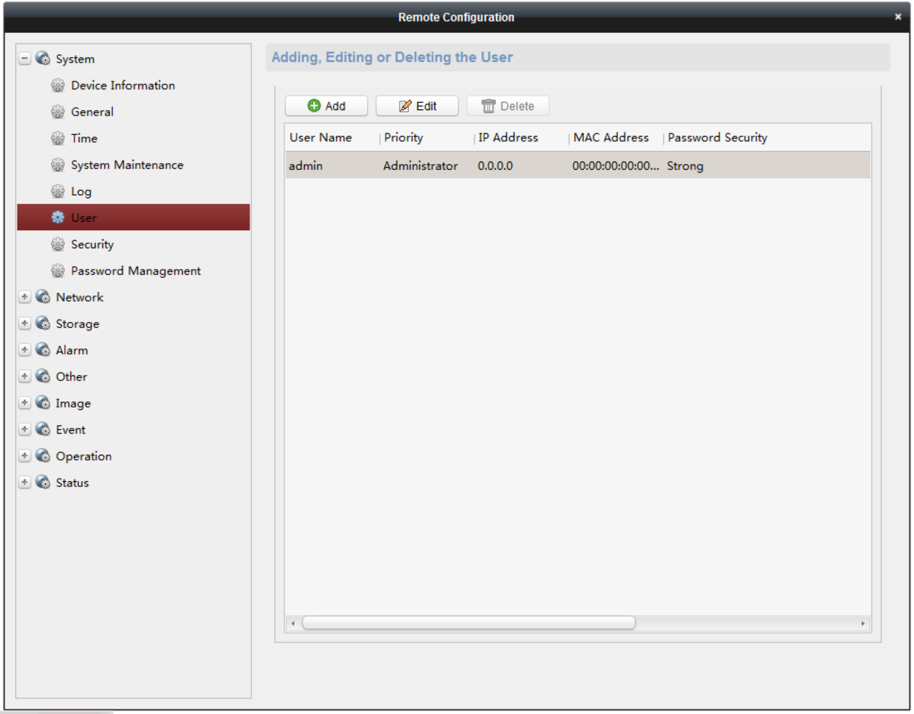
Purpose:

You can add, edit, or delete the user in this section.

- **Add an admin User (Only one admin user can be added)**

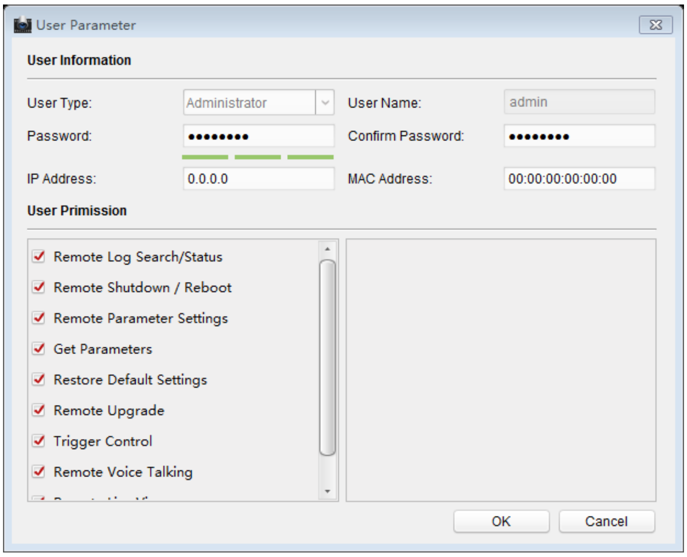
Steps:

1. Click **Remote Configuration > System > User** to enter the user configuration interface.



User Name	Priority	IP Address	MAC Address	Password Security
admin	Administrator	0.0.0.0	00:00:00:00:00...	Strong

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



User Type: Administrator
User Name: admin
Password: ••••••••
Confirm Password: ••••••••
IP Address: 0.0.0.0
MAC Address: 00:00:00:00:00:00

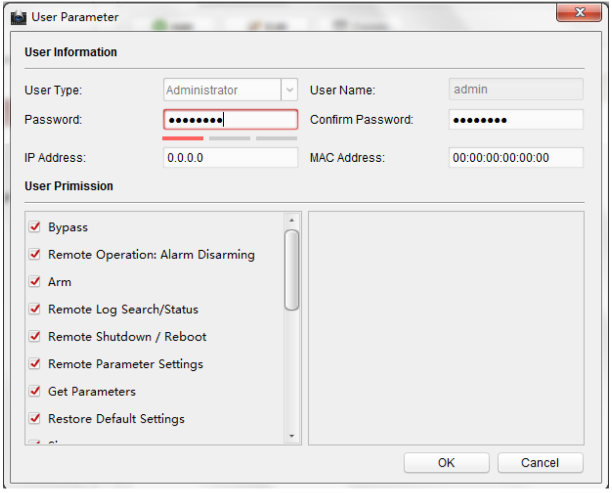
☑ Remote Log Search/Status
☑ Remote Shutdown / Reboot
☑ Remote Parameter Settings
☑ Get Parameters
☑ Restore Default Settings
☑ Remote Upgrade
☑ Trigger Control
☑ Remote Voice Talking

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 Edit to enter the interface of editing the selected user.



User Type: Administrator
User Name: admin
Password: ••••••••
Confirm Password: ••••••••
IP Address: 0.0.0.0
MAC Address: 00:00:00:00:00:00

☑ Bypass
☑ Remote Operation: Alarm Disarming
☑ Arm
☑ Remote Log Search/Status
☑ Remote Shutdown / Reboot
☑ Remote Parameter Settings
☑ Get Parameters
☑ Restore Default Settings

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.

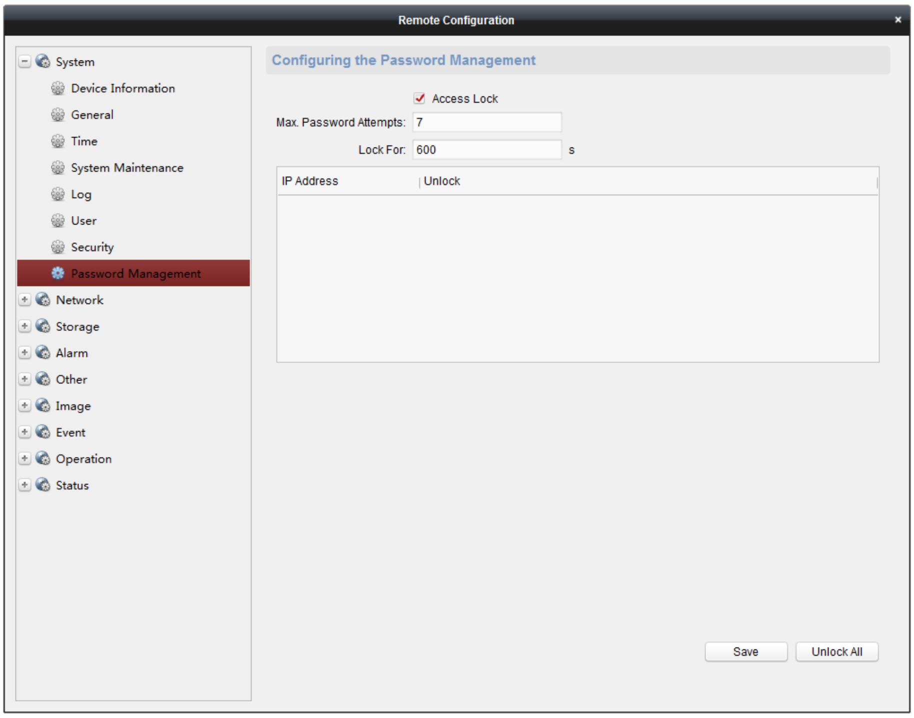
■ **Delete a User**

Steps:

1. Select a user needs to be deleted.
2. Click Delete to delete the user.

Password Management

Click **Remote Configuration > System > Password Management** to set the maximum password attempts and lock duration.



Configuring the Password Management

☑ Access Lock

Max. Password Attempts: 7

Lock For: 600 s

IP Address	Unlock

4.2.2 Network Settings

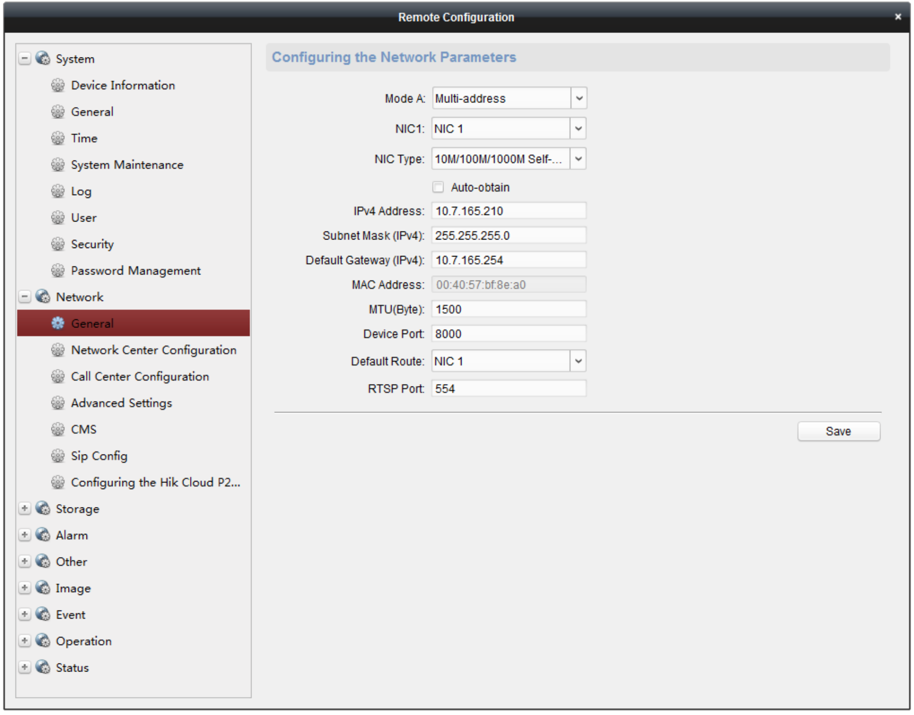
Purpose:

You can edit the general network parameters in this section.

General Network Parameters Settings

Steps:

1. Click **Remote Configuration > Network > General** to enter the general network configuration interface.



Configuring the Network Parameters

Mode A: Multi-address

NIC1: NIC 1

NIC Type: 10M/100M/1000M Self-...

□ Auto-obtain

IPv4 Address: 10.7.165.210

Subnet Mask (IPv4): 255.255.255.0

Default Gateway (IPv4): 10.7.165.254

MAC Address: 00:40:57:bf:8e:a0

MTU(Byte): 1500

Device Port: 8000

Default Route: NIC 1

RTSP Port: 554

2. Configure the NIC setting.
3. Click **Save** to save the above settings.

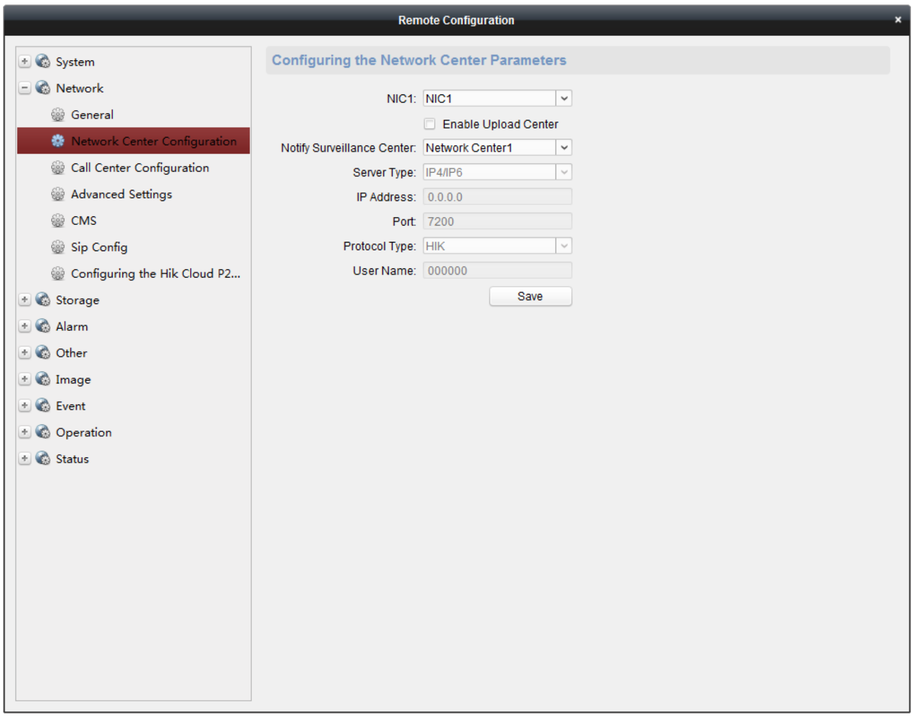
Network Center Settings

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. Click **Remote Configuration > Network > Network Center Configuration** to enter the network center configuration interface.



Configuring the Network Center Parameters

NIC1: NIC1

□ Enable Upload Center

Notify Surveillance Center: Network Center1

Server Type: IP4/IP6

IP Address: 0.0.0.0

Port: 7200

Protocol Type: HIK

User Name: 000000

2. Click and select a network center. Two centers are selectable.
3. Click Enable Upload Center.
4. Click the dropdown menu to select a sever type. Two sever types are available: IP4/IP6 and domain.
5. Enter the IP address which is used to communicate with the network alarm receiving center.
6. Enter the port NO. for communicating with the alarm receiving center.
7. Click the dropdown menu to select the protocol type.
8. Enter the username which is applying for displaying in the alarm receiving center.

NOTE

The length of the username should be 6 characters.

Only numeric (0~9), and letter (A~F&a~f) are valid for this username.

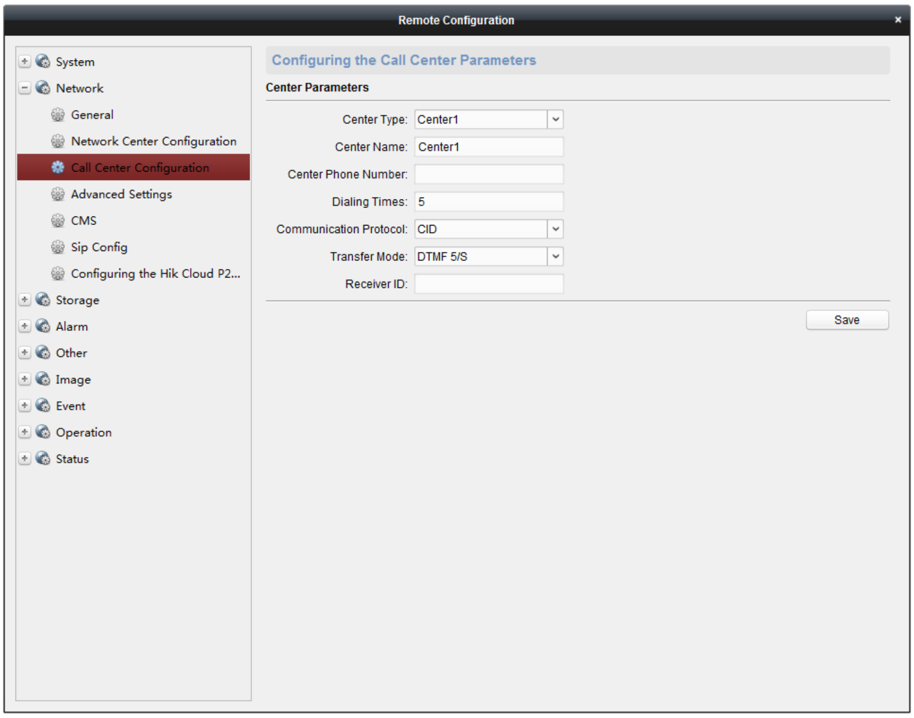
Call Center Settings

Purpose:

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

Steps:

1. Click **Remote Configuration > Network > Call Center Configuration** to enter the call center configuration interface.



Configuring the Call Center Parameters

Center Parameters

Center Type:	Center1
Center Name:	Center1
Center Phone Number:	
Dialing Times:	5
Communication Protocol:	CID
Transfer Mode:	DTMF 5/S
Receiver ID:	

2. Select a center type (only center 1 is available).
3. Enter the center name and phone number.

NOTE

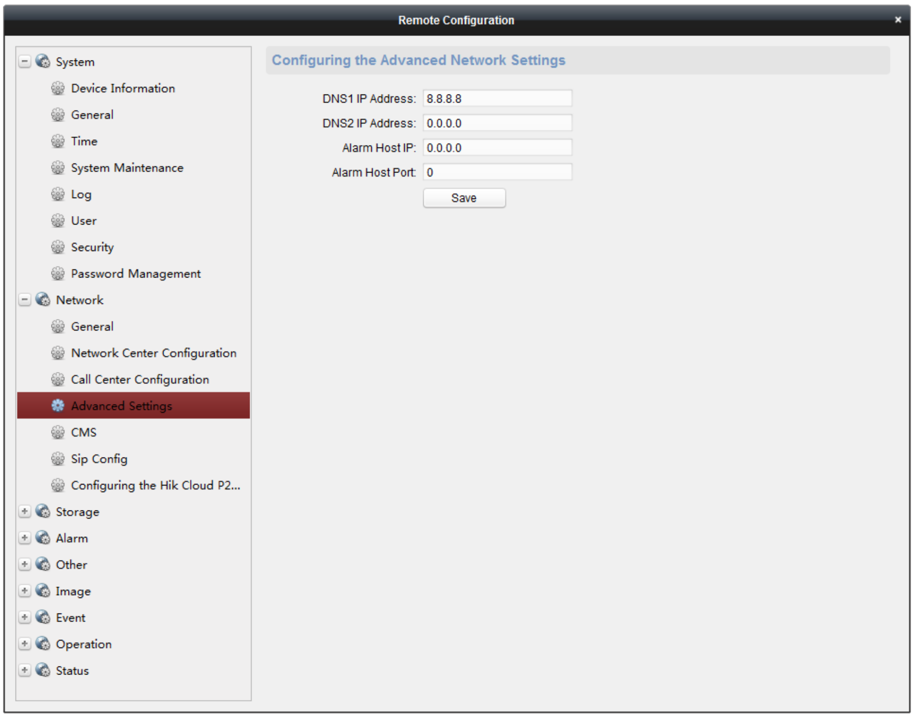
- The maximum length of center name is 32 characters.
- The phone number should be 31 characters and the input mode is
- {NO.}{Dwell Time}{EXT NO.}. For example, in the number of 000088075998FFF8180, the letter F (which means 2 seconds) represents the dwell time, if the number of the letter F is N, the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

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

Advanced Network Parameters Settings

Steps:

1. Click **Remote Configuration** > **Network** > **Advanced Settings** to enter the advanced network configuration interface.



Configuring the Advanced Network Settings

DNS1 IP Address: 8.8.8.8

DNS2 IP Address: 0.0.0.0

Alarm Host IP: 0.0.0.0

Alarm Host Port: 0

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

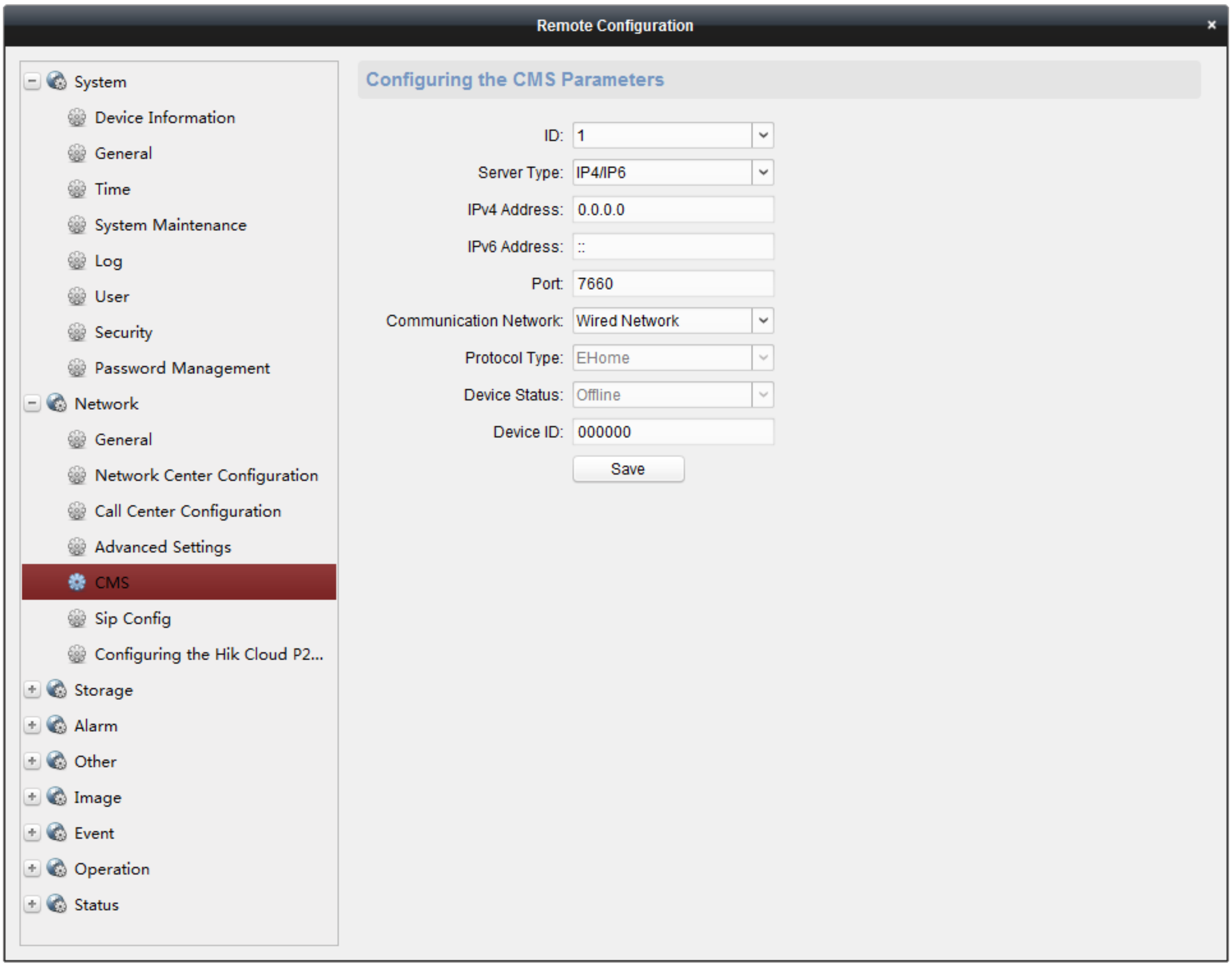
CMS Settings

Purpose:

CMS is used to configure EHome protocol parameters for the device.

Steps:

1. Click **Remote Configuration > Network > CMS** to enter the CMS configuration interface.



Configuring the CMS Parameters

ID: 1

Server Type: IP4/IP6

IPv4 Address: 0.0.0.0

IPv6 Address: ::

Port: 7660

Communication Network: Wired Network

Protocol Type: EHome

Device Status: Offline

Device ID: 000000

2. Click the dropdown menu to select a sever type. Two sever types are available: IP4/IP6 and domain.
3. Enter the IP address which is used to communicate with the service.
4. Enter the port NO. for communicating with the service. The default port NO. for EHome protocol is *7660* and for privacy protocol is *10001*.
5. Click the dropdown menu to select the communication network. Four types are available: Auto, Wired Network Priority, Wired Network and Wireless Network.
6. Enter the device ID where the CID report comes from.

NOTE

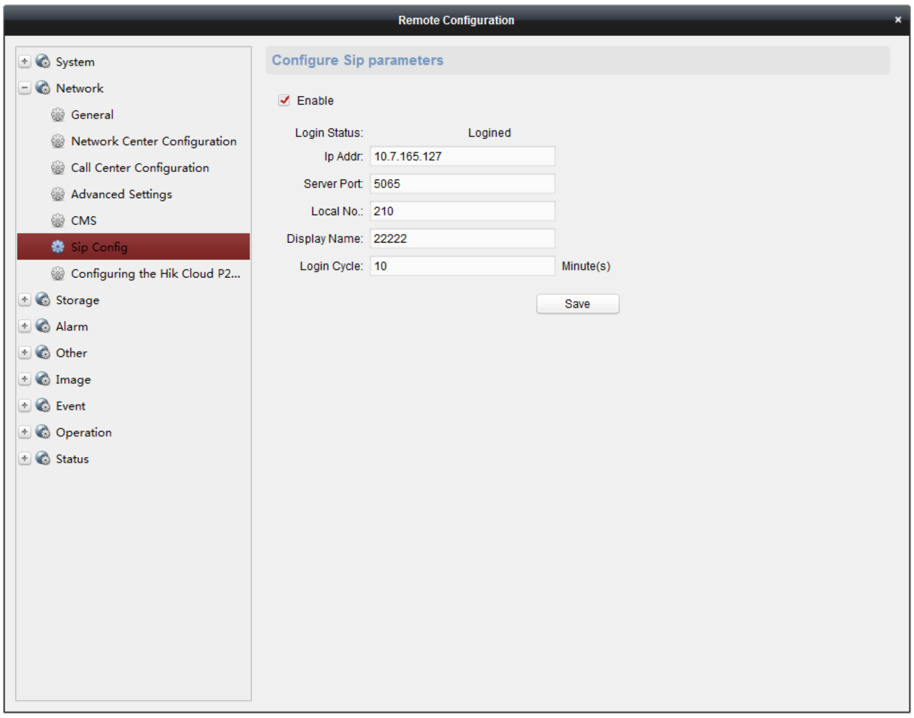
- The length of the device ID should be 6 characters.
- Only numeric (0~9), and letter (A ~ F & a ~ f) are valid for this device ID.

7. Click **Save** to save the settings.

Sip Settings

Steps:

1. Click **Remote Configuration > Network >Sip Config** to enter the Sip configuration interface.



Configure Sip parameters

☑ Enable

Login Status: Logined

Ip Addr: 10.7.165.127

Server Port: 5065

Local No.: 210

Display Name: 22222

Login Cycle: 10 Minute(s)

2. Check **Enable** box to enbale the Sip server.
3. Enter the Sip server parameters including IP address, port No., local No., display name, login cycle.

NOTE

- The server port No. ranges from 1024 to 65535.
- The device ID ranges from 0 to 999999.
- The characters of local No. should be 1 to 64.
- The login cycle ranges from 1 to 30 (min)

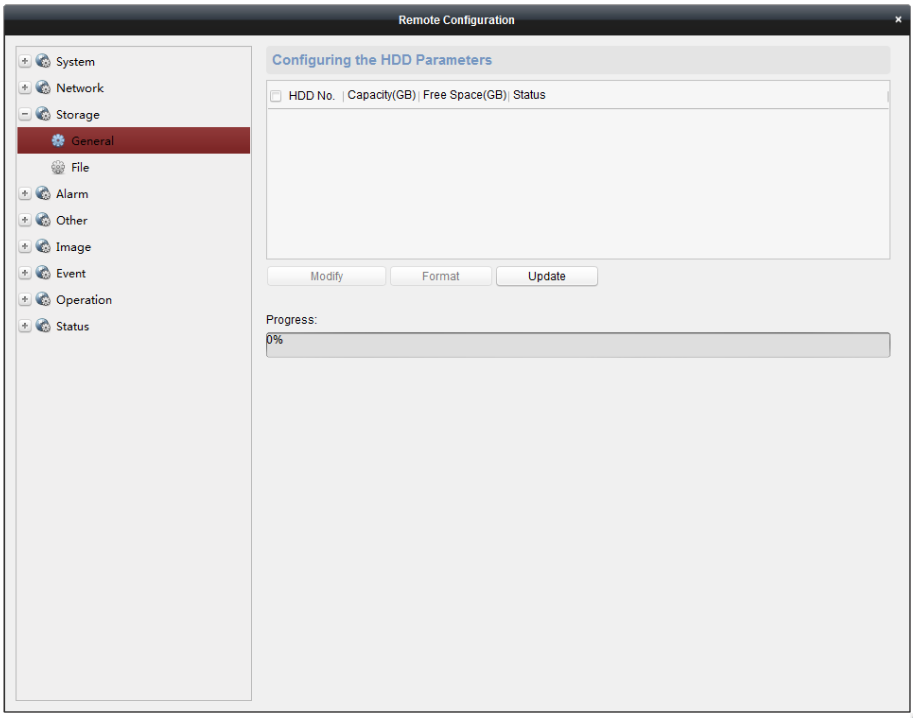
4. Click **Save** to save the settings.

4.2.3 Storage

HDD Information `

Steps:

1. Click **Remote Configuration > Storage > General** to enter the HDD Settings interface. You can view the capacity, free space, status, type and property of the disk.



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

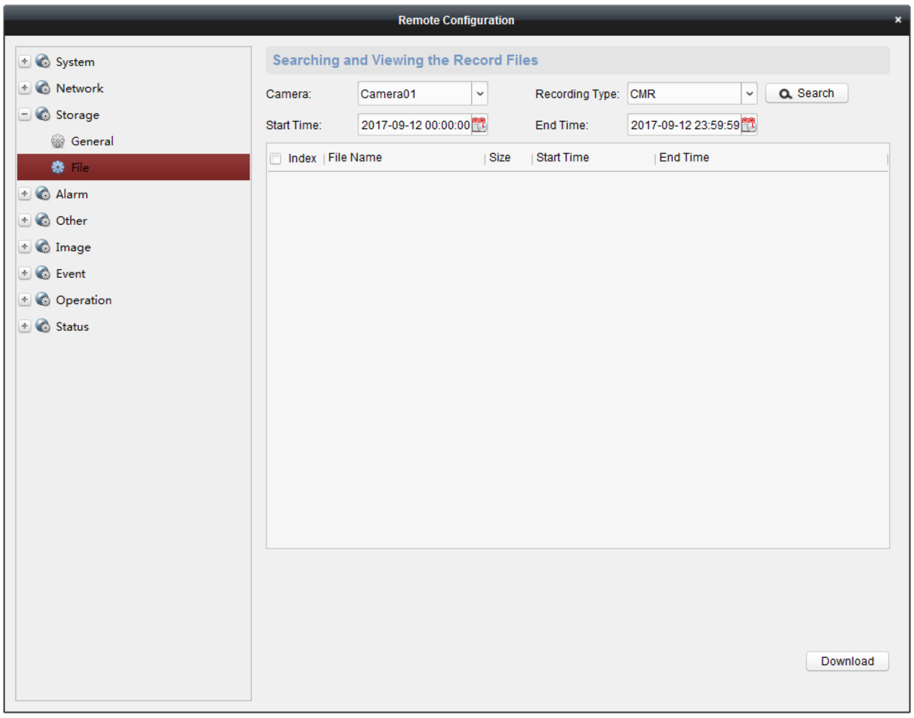
NOTE

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

File Query

Steps:

1. Click **Remote Configuration > Storage > File** to enter the file query interface.



Camera: Camera01

Recording Type: CMR

Start Time: 2017-09-12 00:00:00

End Time: 2017-09-12 23:59:59

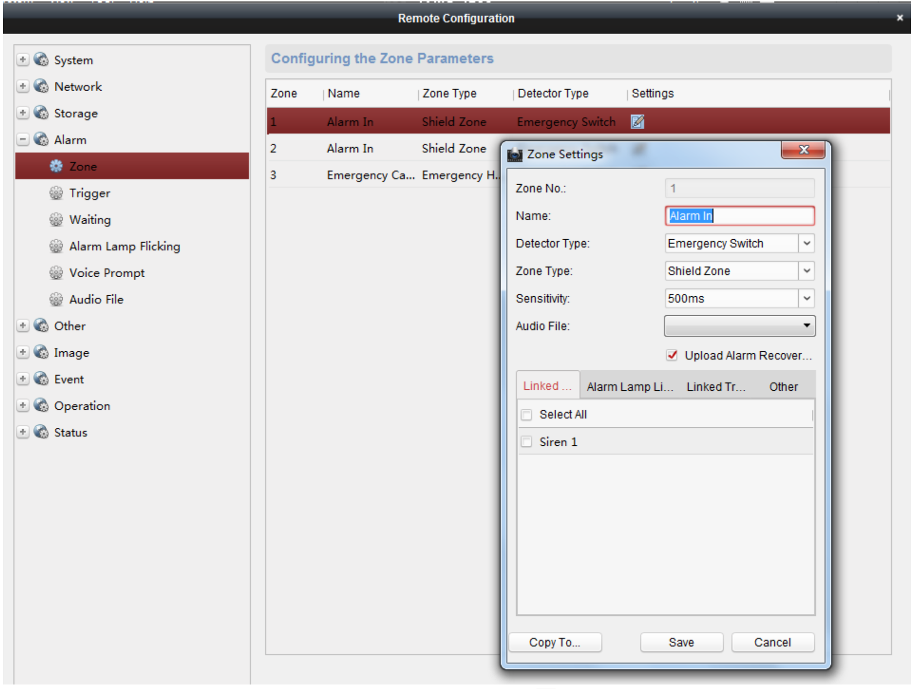
2. Enter the search criteria including camera name, property, start time and end time.
3. Click **Search** to get the file list.

4.2.4 Alarm Settings

Zone Settings

Steps:

1. Click **Remote Configuration > Alarm > Zone** to enter the Zone configuration interface.



Zone	Name	Zone Type	Detector Type	Settings
1	Alarm In	Shield Zone	Emergency Switch	
2	Alarm In	Shield Zone		
3	Emergency Ca...	Emergency H...		

Zone No.: 1

Name: Alarm In

Detector Type: Emergency Switch

Zone Type: Shield Zone

Sensitivity: 500ms

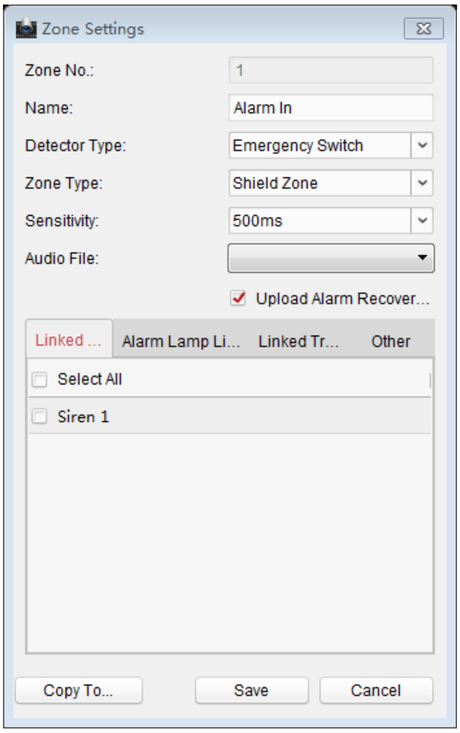
Audio File:

☑ Upload Alarm Recover...

□ Select All

□ Siren 1

2. In the Alarm Input list, select an alarm input channel and click the icon to enter the zone setting interface.



Zone No.: 1

Name: Alarm In

Detector Type: Emergency Switch

Zone Type: Shield Zone

Sensitivity: 500ms

Audio File:

☑ Upload Alarm Recover...

□ Select All

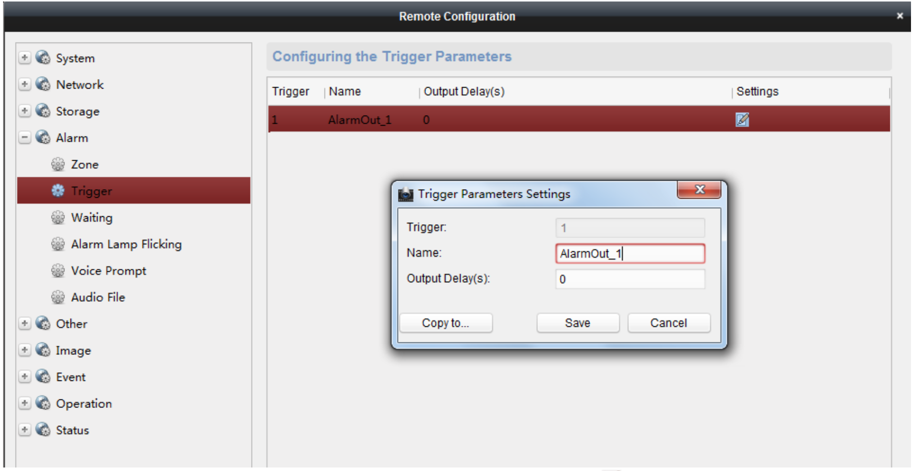
□ Siren 1

3. Edit the general information of the Zone, including name, detector type, zone type, sensitivity and so on.
   Detector Type: Select the type of the detector.
   Zone Type: Select the type of Zone in the partition.
   Sensitivity: Select the response time of the Zone.
4. Select the linked siren and linked trigger.
5. Click **Copy to** to copy all these settings to other Zones.
6. Click **Save** to save the settings.

Trigger Settings

Steps:

1. Click **Remote Configuration > Alarm > Trigger** to enter the trigger configuration interface.



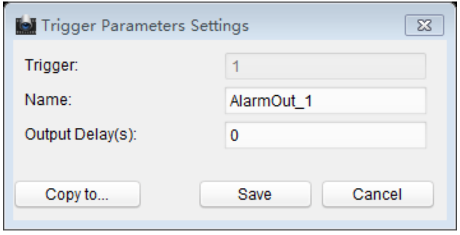
Trigger	Name	Output Delay(s)	Settings
1	AlarmOut_1	0	

Trigger: 1

Name: AlarmOut_1

Output Delay(s): 0

2. In the Alarm Output list, select the alarm output channel and click the icon ✎ to enter trigger parameters setting interface.



Trigger: 1

Name: AlarmOut_1

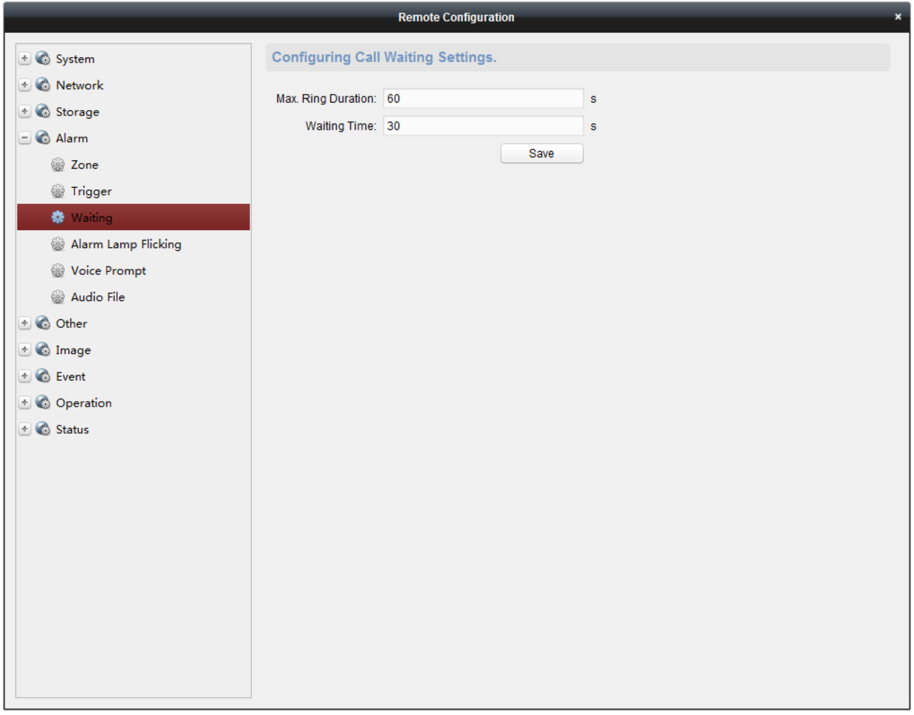
Output Delay(s): 0

3. Edit the general information of the trigger, including name, output delay and so on.
   Output Delay (0~5999s): Configure the alarm output time after the alarm being triggered.
4. Click **Copy to** to copy all these settings to other Zones.
5. Click **Save** to save the settings.

Calling Waiting Settings

Steps:

1. Click **Remote Configuration > Alarm > Waiting** to enter the trigger configuration interface.



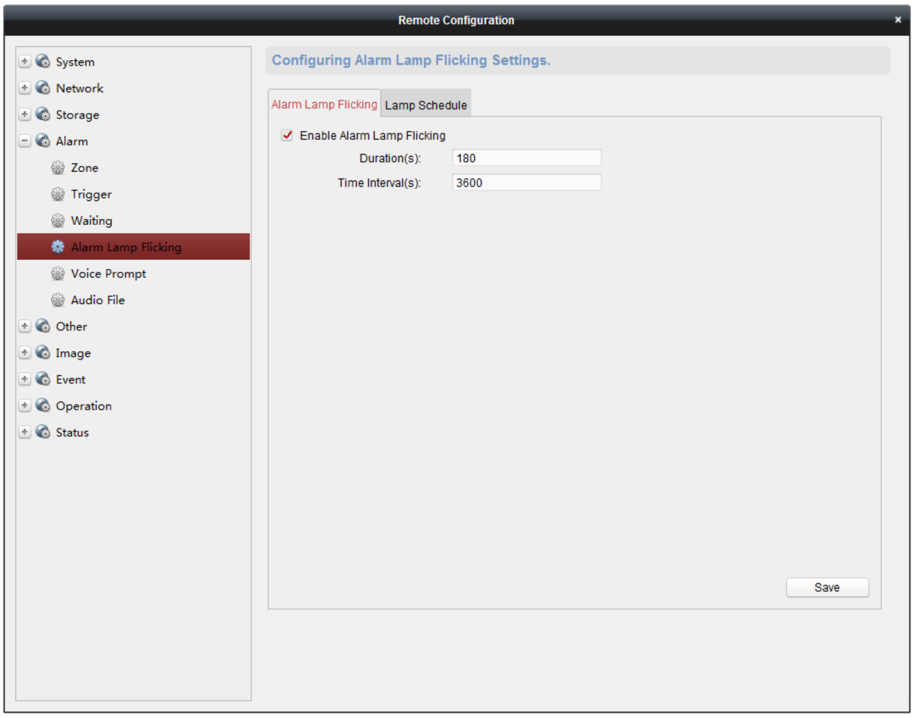
Max. Ring Duration: 60 s
Waiting Time: 30 s

2. Enter the Max. ring duration (40s to 80s)for reporting alarm to the center.
3. Enter the waiting time (10s to 60s) for the center to answer the call.
4. Click **Save** to save the settings.

Alarm Lamp Settings

Steps:

1. Click **Remote Configuration > Alarm > Alarm Lamp Flicking** to enter the trigger configuration interface.



Configuring Alarm Lamp Flicking Settings.

☑ Enable Alarm Lamp Flicking

Duration(s): 180

Time Interval(s): 3600

2. Check **Enable Alarm Lamp Flicking** box.
3. Enter the alarm lamp flashing duration (s).
4. Enter the time interval for each flashing(s).
5. Click **Save** to save the settings.

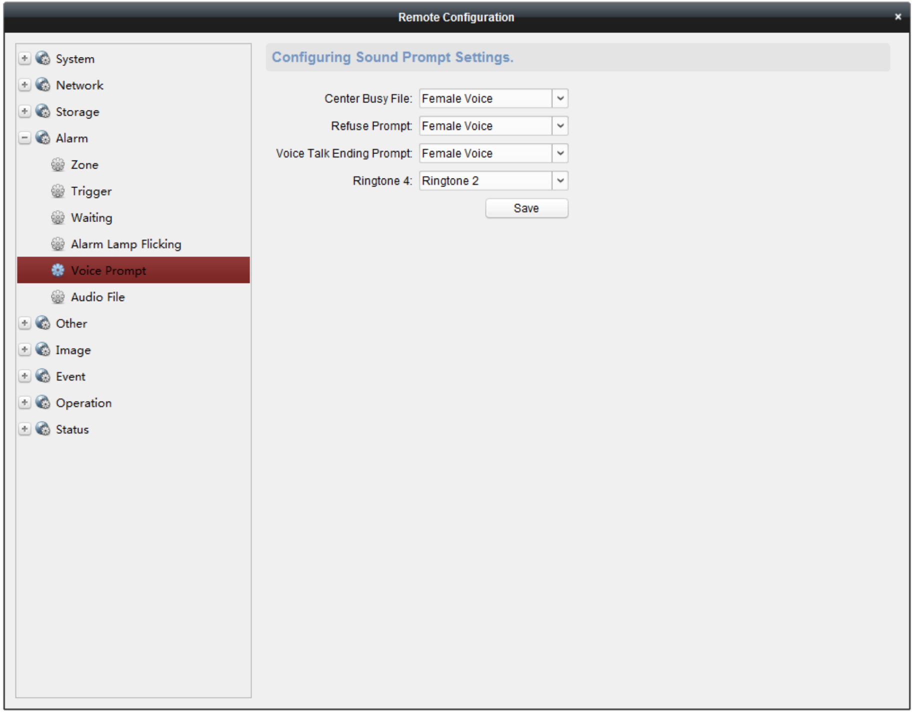
NOTE

If the duration is 180s and the time interval is 3600s, the alarm lamp flashes 3 minutes each hour.

Voice Prompt Settings

Steps:

1. Click **Remote Configuration > Alarm > Voice Prompt**to enter the trigger configuration interface.



Configuring Sound Prompt Settings.

Center Busy File: Female Voice

Refuse Prompt: Female Voice

Voice Talk Ending Prompt: Female Voice

Ringtone 4: Ringtone 2

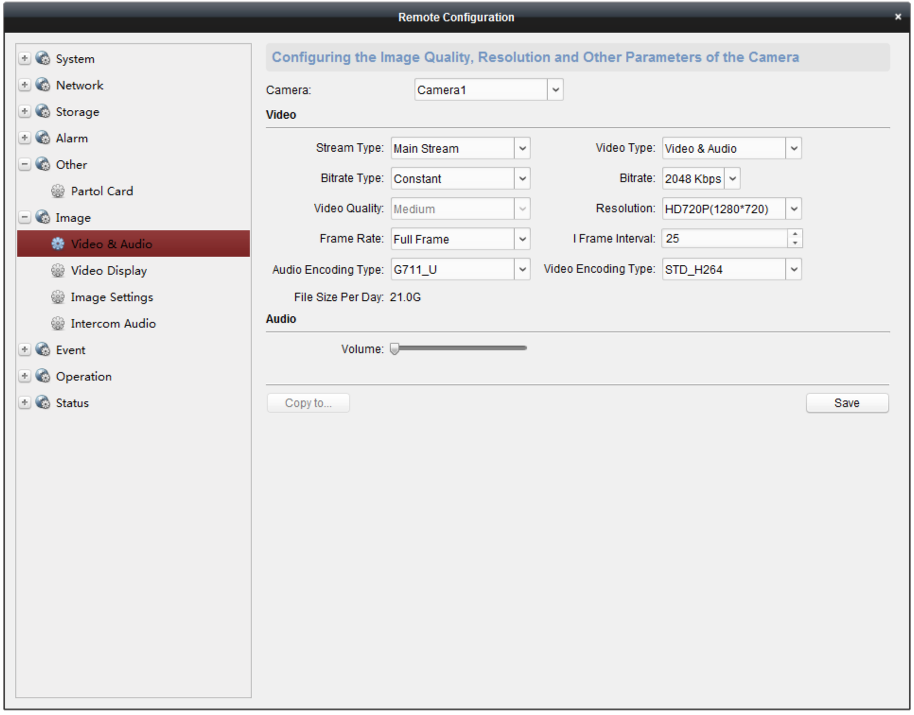
2. Check **Enable Alarm Lamp Flicking** box.
3. Select **Female/Male** voice for center busy file, refuse, and voice talking prompt.
4. Select the ring tone.
5. Slick **Save** to save the settings.

4.2.5 Image Settings

Video& Audio Settings

Steps:

1. Click **Remote Configuration > Image > Video & Audio** to enter the video/audio configuration interface.



Configuring the Image Quality, Resolution and Other Parameters of the Camera

Camera: Camera1

Video

Stream Type: Main Stream

Video Type: Video & Audio

Bitrate Type: Constant

Bitrate: 2048 Kbps

Video Quality: Medium

Resolution: HD720P(1280*720)

Frame Rate: Full Frame

I Frame Interval: 25

Audio Encoding Type: G711_U

Video Encoding Type: STD_H264

File Size Per Day: 21.0G

Audio

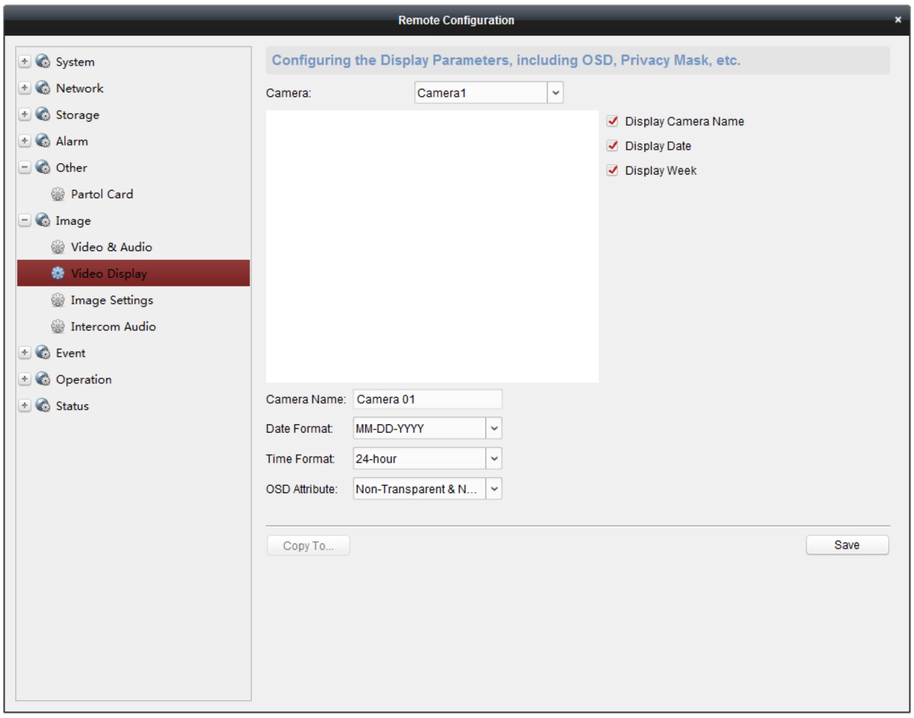
Volume:

2. Select a camera needs to be configured.
3. Edit the general video parameters.
   Scream 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 **Save** to save the settings.

OSD Settings

Steps:

1. Click **Remote Configuration > Image > Video Display** to enter the OSD Settings interface.



Configuring the Display Parameters, including OSD, Privacy Mask, etc.

Camera: Camera1

☑ Display Camera Name

☑ Display Date

☑ Display Week

Camera Name: Camera 01

Date Format: MM-DD-YYYY

Time Format: 24-hour

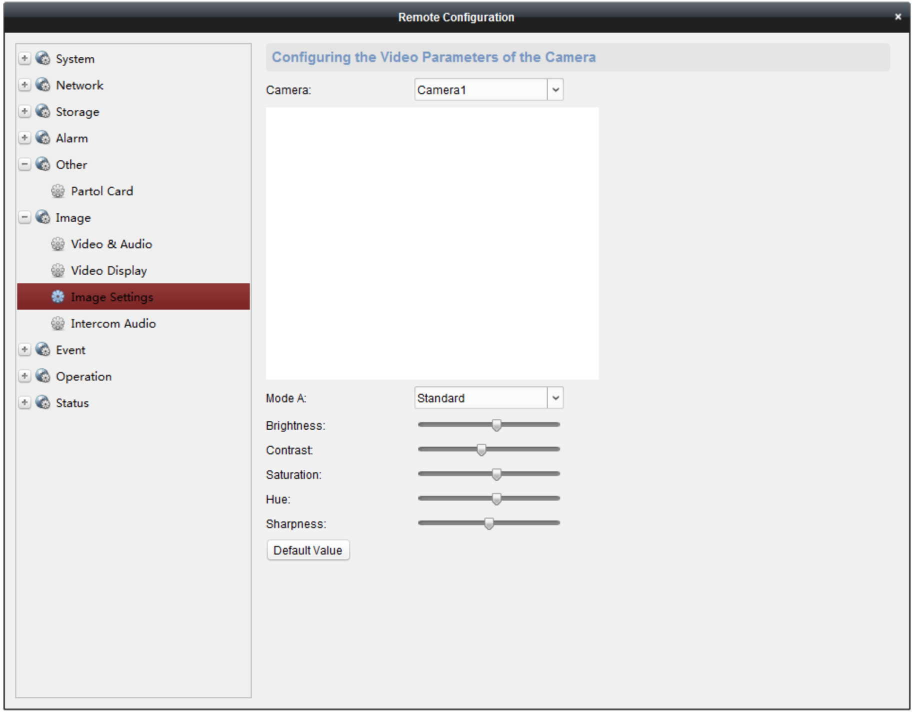
OSD Attribute: Non-Transparent & N...

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 Text in the live view window to adjust the text overlay position.
8. Click **Save** to save the settings.

Image Settings

Steps:

1. Click **Remote Configuration > Image > Image Settings** to enter the image settings interface.



Configuring the Video Parameters of the Camera

Camera: Camera1

Mode A: Standard

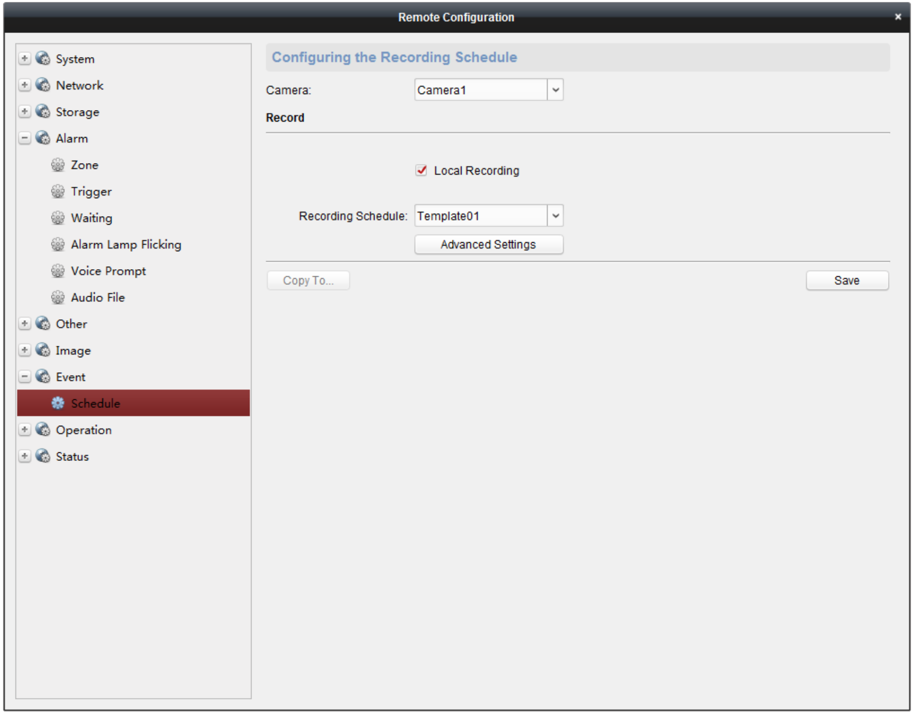
2. Drag the to adjust the brightness, contrast, saturation of the image.

3. You can also click **Default Value** to restore the default values.

4.2.6 Event Settings

Schedule Settings

Click **Remote Configuration > Events > Schedule** to enter the record schedule configuration interface.



Configuring the Recording Schedule

Camera: Camera1

Record

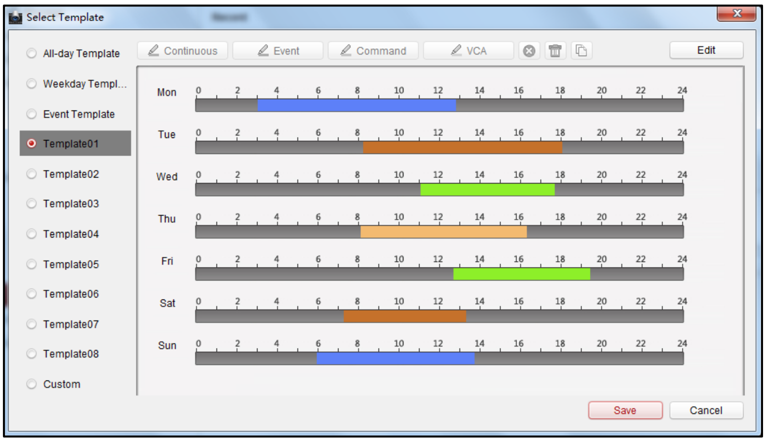
☑ Local Recording

Recording Schedule: Template01

- **Record Schedule Settings**

Steps:

1. Select the camera needs to be configured.
2. Check the checkbox of **Local Recording** to enable the device local recording. You can also check ANR checkbox to enable the device continuing recording even if the network is off.
3. Select from the drop-down list to set the recording type including Main Stream and Sub Stream.
4. Click the Template01 ⌄ icon to set the record schedule.



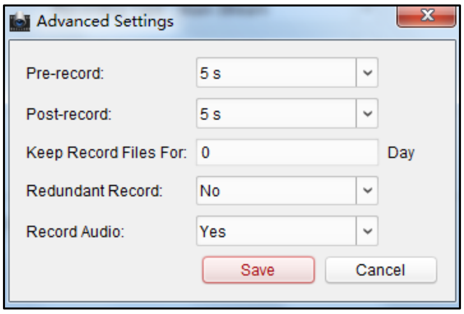
5. Click **Edit** to enter the Templates Management interface. Select the template to be set and you can edit the template name.
6. Set the time schedule for the selected template.

   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.

7. 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.
8. Click **Save** to save the template, or click cancel to exit the interface.
9. Click **Advanced Settings** button to set the pre-record time, post record time, video expired time, redundant record and audio recording.



Pre-record: 5 s
Post-record: 5 s
Keep Record Files For: 0 Day
Redundant Record: No
Record Audio: Yes

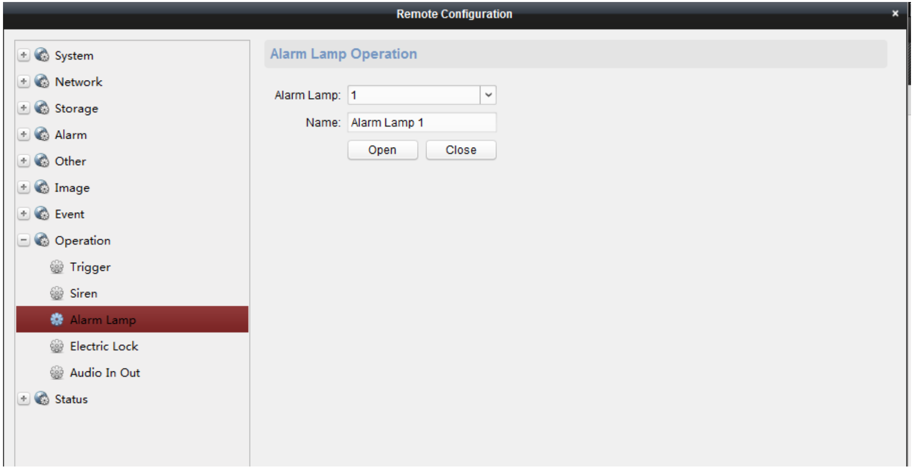
10. Click **Copy to** to copy all these settings to other Zones.
11. Click **Save** to save the settings.

- **Capture Schedule Settings**

1. Check the checkbox of **Capture Settings** to enable the device local capturing.
2. Click the Template01 ⌄ icon to set the capture schedule. For details, refer to *Steps 5, 6, 7 in Record Schedule Settings.*
3. Click **Copy to** to copy all these settings to other Zones.
4. Click **Save** to save the settings.

4.2.7 Operation

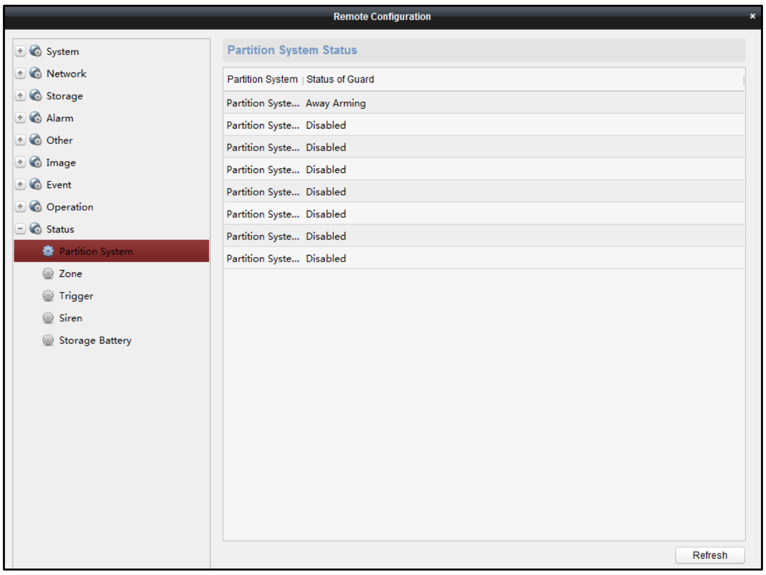
You can configure the trigger, siren, alarm lamp, electric lock, and audio in/out in this section.
Click **Remote Configuration > Operation** to enter the interface.
Trigger: you can select to turn on/off the selected trigger.
Siren: you can enable/disable the specified siren.
Alarm Lamp: You can enable/disable the alarm lamp.
Electric Lock: You can enable/disable the electric lock.
Audio In/Out: You can adjust the input volume and output volume.



Alarm Lamp: 1
Name: Alarm Lamp 1

4.2.8 Status

Click **Remote Configuration > Status** to view status of the partition, zone, trigger, siren ,and storage battery.



Partition System Status

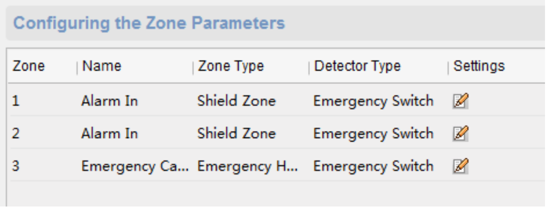
Partition System	Status of Guard
Partition Syste...	Away Arming
Partition Syste...	Disabled
Partition Syste...	Disabled
Partition Syste...	Disabled
Partition Syste...	Disabled
Partition Syste...	Disabled
Partition Syste...	Disabled
Partition Syste...	Disabled

4.3 Zone Settings

4.3.1 Zone Settings

Steps:

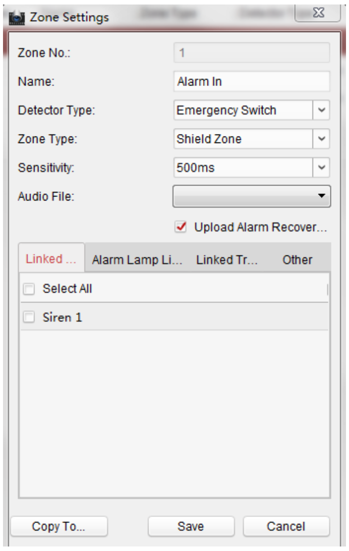
1. Click **Device Management > Security Control Panel > Remote Configuration > Alarm > Zone** to enter the Zone configuration interface.
2. In the Alarm Input list, select an alarm input channel and click the icon ✎ to enter the zone settings interface.



Configuring the Zone Parameters

Zone	Name	Zone Type	Detector Type	Settings
1	Alarm In	Shield Zone	Emergency Switch	✎
2	Alarm In	Shield Zone	Emergency Switch	✎
3	Emergency Ca...	Emergency H...	Emergency Switch	✎

3. Edit the general information of the zone, including name, detector type, zone type, sensitivity, audio file etc.
Detector Type: Select the type of the detector.
Zone Type: Select the type of zone in the partition.
Sensitivity: Select the response time of the zone.



Zone No.: 1

Name: Alarm In

Detector Type: Emergency Switch

Zone Type: Shield Zone

Sensitivity: 500ms

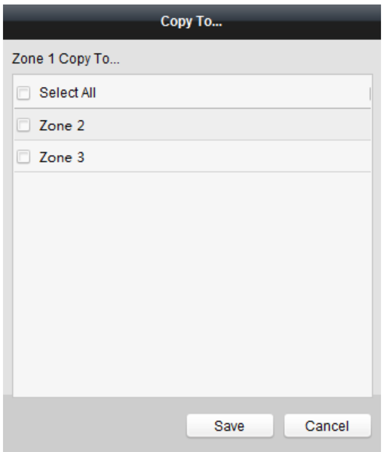
Audio File:

☑ Upload Alarm Recover...

□ Select All

□ Siren 1

4. Select the linked siren, alarm lamp, linked trigger and others.
5. Click **Copy to** to copy all these settings to other zones.



6. Click **Save** to save the settings.

NOTE

Four zone types in the Zone Parameters: Instant Zone, Fire Alarm Arming Zone, 24 Hour Non-voiced Zone and Shield Zone.

Instant Zone Alarm is sent out without any delay once the detector is triggered.

Fire Alarm Arming Zone When the 24-hour armed zone is triggered by fire alarm, sirens will send out resonant and special sound.

24 Hour Non-voiced Zone When the 24-hour armed zone is triggered, it will send alarm reports to the surveillance center without any audible warning. The 24 hour silence alarm zone is not affected by manual or scheduled arming/disarming.

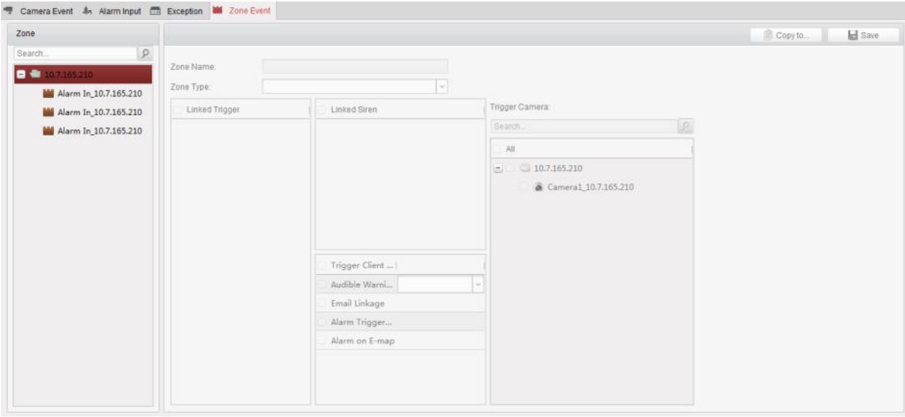
Shield Zone The alarm will not be triggered.

Panic alarm station has three zones among which two are ordinary zones and one is emergency zone.

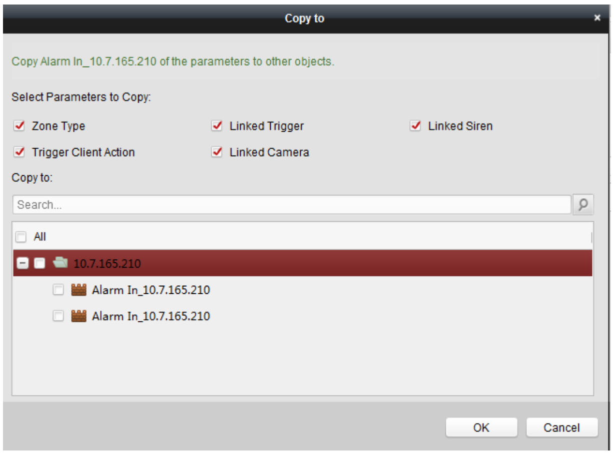
4.3.2 Zone Event Settings

Steps:

1. Click **Control Panel > Event Management > Zone Event** to enter the Zone Event configuration interface.



2. Select the corresponding zone on the left and then tick necessary items.
3. (Optional) Click **Copy to** to tick the necessary items.



Copy to

Copy Alarm In_10.7.165.210 of the parameters to other objects.

Select Parameters to Copy:

☑ Zone Type ☑ Linked Trigger ☑ Linked Siren

☑ Trigger Client Action ☑ Linked Camera

Copy to:

Search...

□ All

□ 10.7.165.210

- □ Alarm In_10.7.165.210
- □ Alarm In_10.7.165.210

OK Cancel

4. Click **Save** to save the settings.

NOTE

The Alarm In is emergent by default.

4.3.3 Alarm Pop-up Window Settings

Purpose

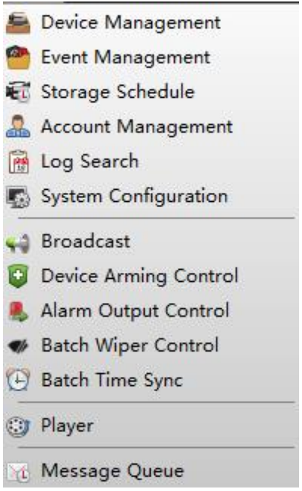
When the devices are armed, the alarm intercom will pop up once the detectors are triggered.

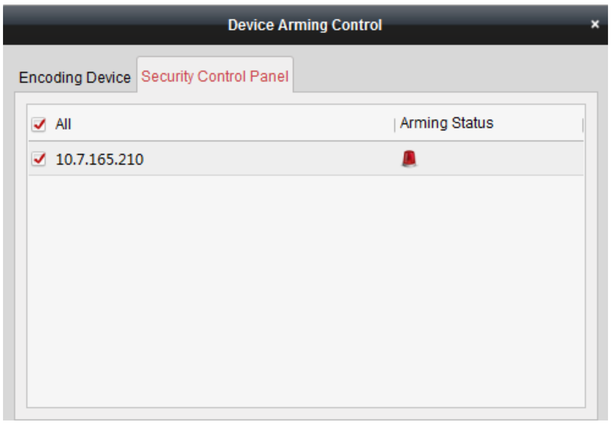
Enable Pop-up Window Function

When the devices are arming, enable the pop-up window by following the steps bellow.

Steps:

1. Click **Tool > Device Arming Control** to enter the device arming control interface.





Device Arming Control

Encoding Device | Security Control Panel

	Arming Status
☑ All	
☑ 10.7.165.210	

2. Click the alarm device to make it in the state of arming.

Pop-up Window Operation

When the window pops up, you can

click to answer the alarm calling or service consulting;

click to reject the alarm calling or service consulting;

click to hold on the calling or consulting;

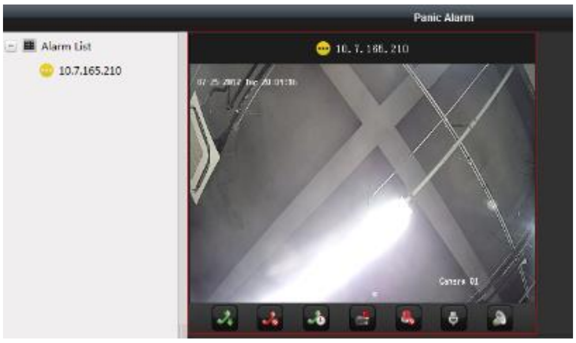
click to turn on electric lock of alarm bar;

click to turn on alarm lamp (applicable to panic alarm station with camera);

click 🎤 to set volume of audio in and click 🔊 to set the volume of audio out;

click 📷 to capture picture;

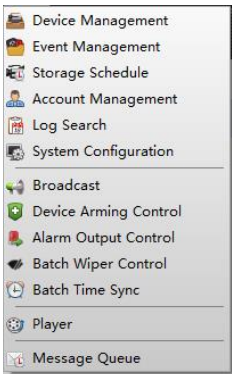
click 🔴 to start videoing and click ⏹ to stop videoing.



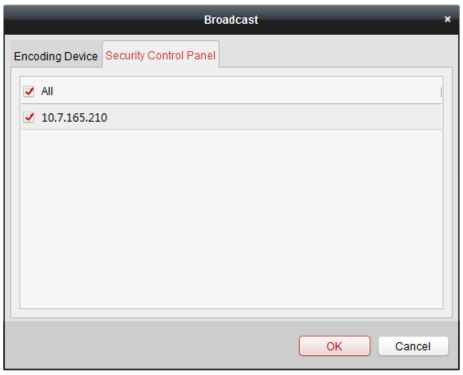
4.4 Broadcast Settings

Steps:

1. Click **Tool > Broadcast** to enter the broadcast management interface.



Device Management
Event Management
Storage Schedule
Account Management
Log Search
System Configuration
Broadcast
Device Arming Control
Alarm Output Control
Batch Wiper Control
Batch Time Sync
Player
Message Queue



Broadcast

Encoding Device | Security Control Panel

☑ All

☑ 10.7.165.210

OK | Cancel

2. Click the corresponding item.
3. (Optional) Unclick the corresponding item if you want to cancel the broadcast.
4. Click **Save** to save the setting.

NOTE

After the broadcast setting, the client can broadcast to multiple devices.

UD09784B

See Far, Go Further

Grupo Instaladores

✉ ventas@rosarioseguridad.com.ar	rosarioseguridadok	https://www.facebook.com/groups/591852618012744/
☎ +54 9 341 6708000	Rosario Seguridad	+54 9 341 6591429
☎ +54 9 341 6799822	Rosario Seguridad	☎ +54 9 341 4577532

Avenida Presidente Perón 3998 - Rosario - Santa Fe - Argentina