



Panic Alarm Station with Covert Camera

User Manual

User Manual

COPYRIGHT ©2018 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 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 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.

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 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 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 DS-PEA series panic alarm station.

Product	Model
Panic Alarm Station	DS-PEA1-N1, DS-PEA1-N2

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 (24 VAC/12 VDC). 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°C to 60°C.

- 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
1.1 Description.....	1
1.2 Key Features	1
Chapter 2 Appearance	2
2.1 Panic Alarm Station without Help Buttonn	2
2.2 Panic Alarm Station with Help Button.....	3
Chapter 3 Installation and Wiring	4
3.1 Typical Application	4
3.2 Wiring Description	5
3.2.1 Network Wiring.....	6
3.2.2 Alarm Output Wiring	6
3.2.3 Alarm Input Wiring (Normally Open)	7
3.2.4 Power Supply Wiring.....	8
3.3 Installation	9
3.3.1 Installation Description	9
Chapter 4 Device Remote Operation	10
4.1 Activation via SADP Tool	10
4.2 Remote Operation via Client Software	11
4.2.1 Activation via Client Software	11
4.2.2 Add a Device	13
4.2.3 Zone Settings	14
4.2.4 Zone Event Settings.....	16
4.2.5 Alarm Pop-up Window Settings	17
4.3 Broadcast Settings	18
Chapter 5 Remote Operation via iVMS-4200	19
5.1 System Information Settings	19
5.1.1 General Settings.....	19
5.1.2 Timing Settings.....	20
5.1.3 System Maintenance.....	21
5.1.4 Log Searching	22
5.1.5 User Settings	23
5.1.6 Password Management	25
5.2 Network Settings	25
5.2.1 General Network Parameters Settings	25
5.2.2 Network Center Settings.....	26
5.2.3 Call Center Settings	27
5.2.4 Advanced Network Parameters Settings.....	28
5.2.5 CMS Settings	29
5.2.6 Sip Settings.....	30
5.3 Storage Settings	31
5.3.1 HDD Information	31
5.3.2 File Query.....	32
5.4 Alarm Settings.....	33
5.4.1 Zone Settings	33
5.4.2 Trigger Settings	35
5.4.3 Calling Waiting Settings.....	35
5.4.4 Alarm Lamp Settings	36
5.4.5 Voice Prompt Settings.....	37
5.5 Image Settings	37
5.5.1 Video& Audio Settings	37
5.5.2 OSD Settings.....	38
5.5.3 Image Settings.....	39
5.6 Event Settings	40
5.6.1 Schedule Settings.....	40
5.7 Camera Parameter Settings	42
5.7.1 Video Parameter Settings	42
5.7.2 WDR Settings	43
5.8 Audio Detection	43

Chapter 1 Overview

1.1 Description

This series of panic alarm station with covert camera supports two-way audio communication. It is equipped with a 2MP built-in covert camera. The device with help button or without help button can be selected. It implements cascading communication via network cable wiring.

1.2 Key Features

- Network, video and audio adaptive
- Voice intercom, alarm video storage, video download and playback
- Two RJ45 network interfaces, supports cascading communication
- Video compression: H.264
- Audio compression: G.711 and G726
- Audio detection
- Built-in 2MP 1080P IR HD wide angle camera; supports capture, record, and live view
- Built-in high sensitivity microphone
- Full-band speakers and pickups supports anti-breaking sound technology
- Multiple network protocols: TCP/IP, SNMP, RTSP and SADP
- Anti-electromagnetic interference, tamper-proof, explosion-proof, and anti-lightning

Chapter 2 Appearance

There are two types of the panic alarm stations: Panic alarm station without Help button and panic alarm station with Help button.

2.1 Panic Alarm Station without Help Button

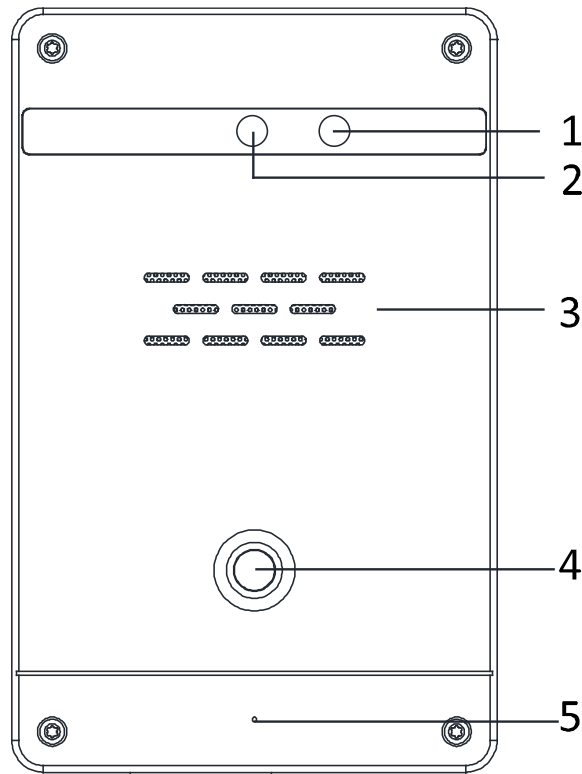


Figure 2-1 Panic Alarm Station without Help Button

Table 2-1 Components Description

No.	Description	No.	Description
1	IR Light	4	Panic Button
2	Covert Camera	5	Microphone
3	Loudspeaker		

2.2 Panic Alarm Station with Help Button

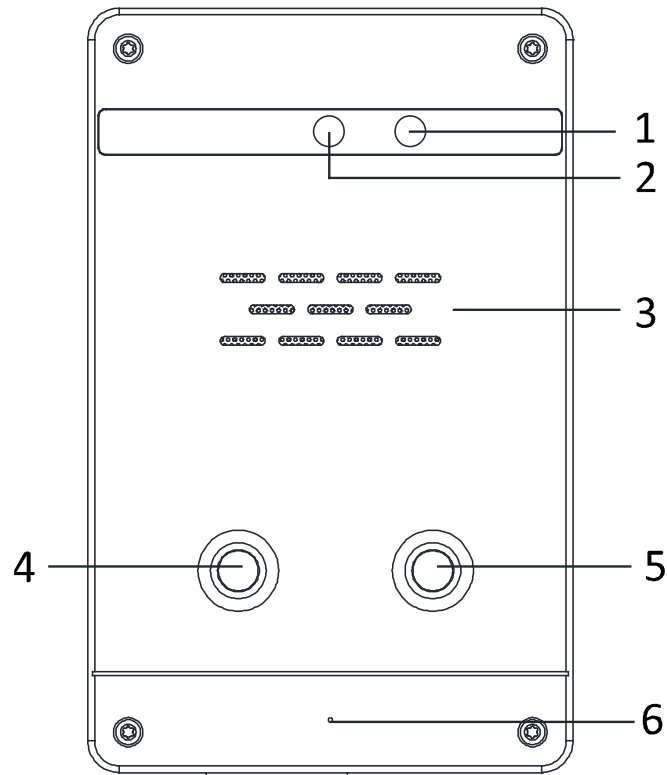


Figure 2-2 Panic Alarm Station with Help Button

Table 2-2 Components Description

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

Chapter 3 Installation and Wiring

3.1 Typical Application

The series of panic alarm station supports cascading communication via network cable wiring. The typical application of the system is shown in the following picture.

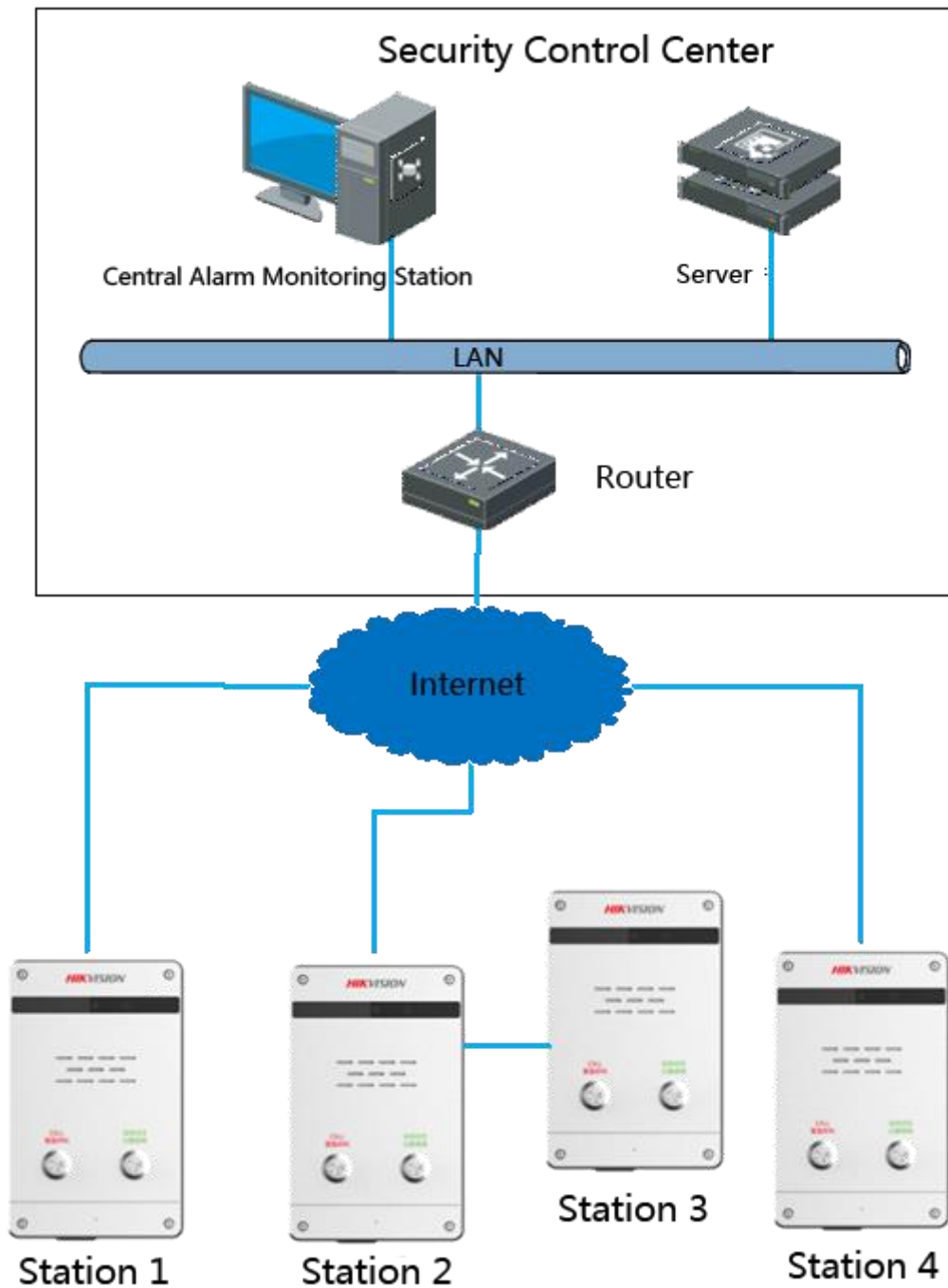


Figure 3-1 Typical Application

3.2 Wiring Description

Take the panic alarm station with help button as an example, the main board description is shown in Figure 3-2.

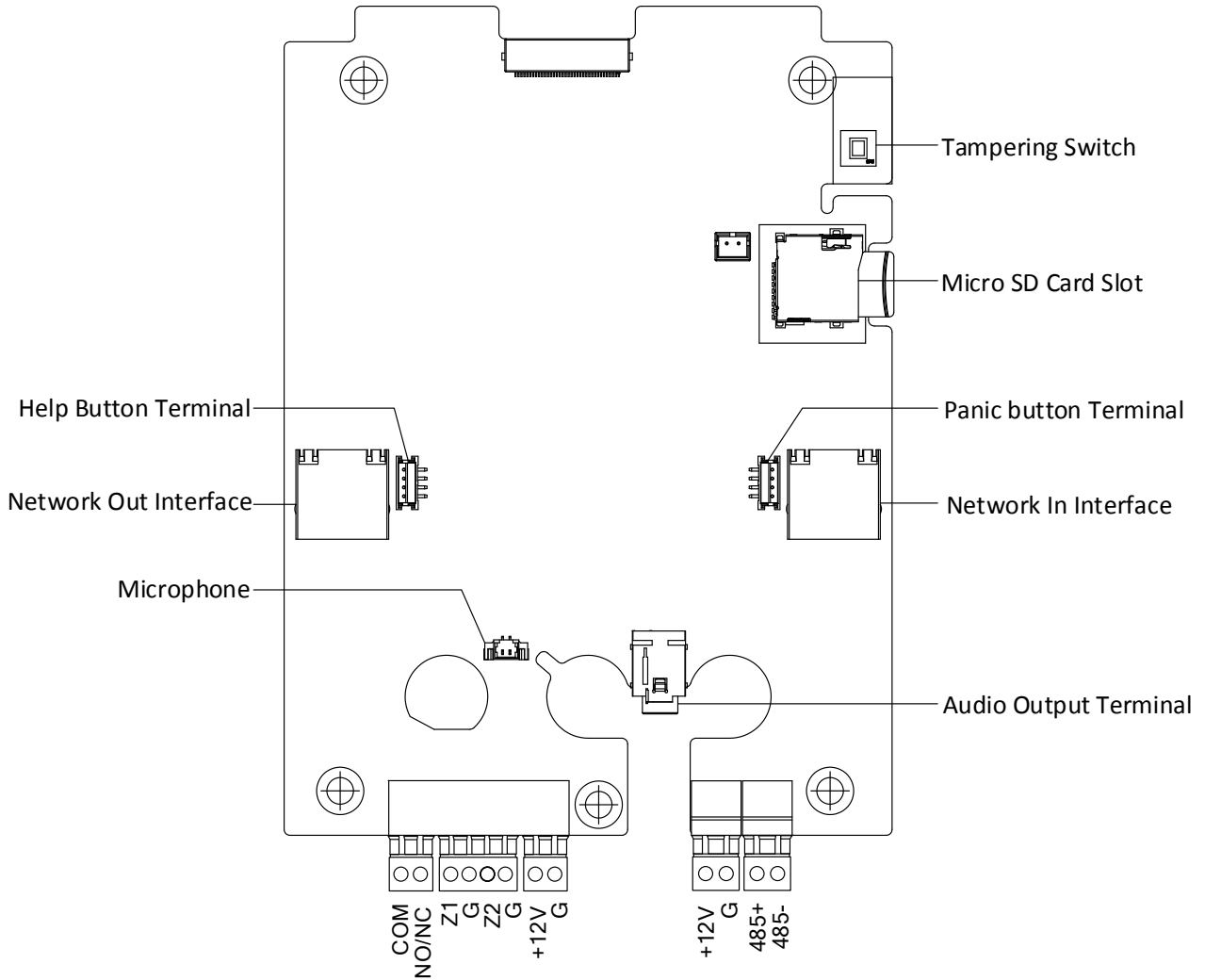


Figure 3-2 Mainboard of Alarm Station

3.2.1 Network Wiring

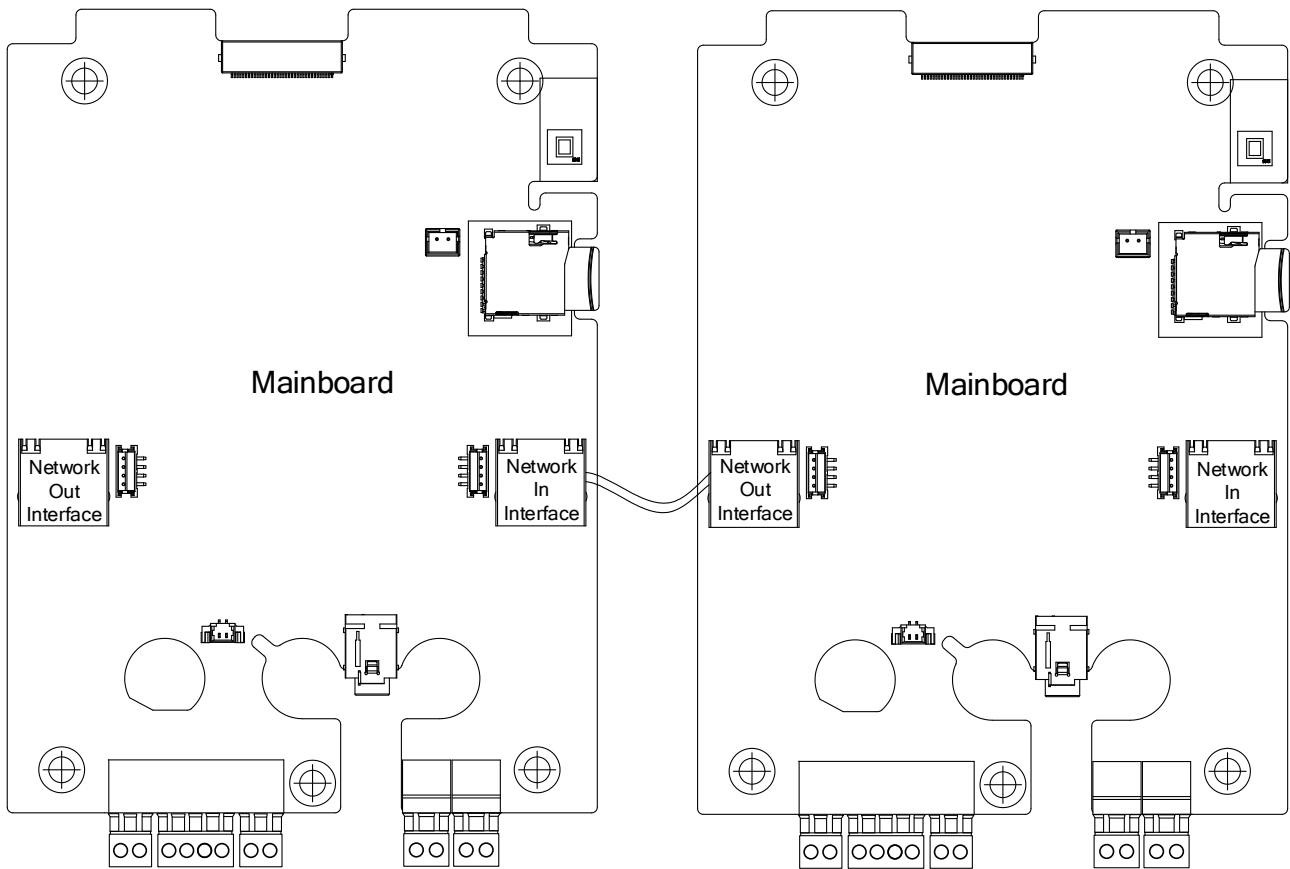
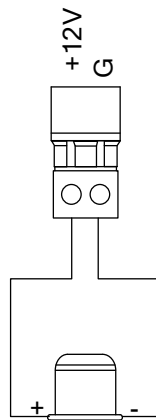


Figure 3-3 Network Wiring

3.2.2 Alarm Output Wiring



Alarm Sensor

Figure 3-4 Alarm Output Wiring

3.2.3 Alarm Input Wiring (Normally Open)

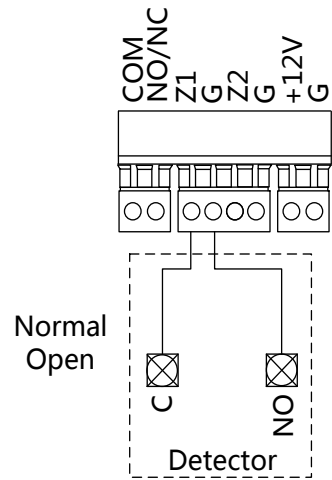


Figure 3-5 Alarm Input Wiring (NO)

3.2.4 Power Supply Wiring

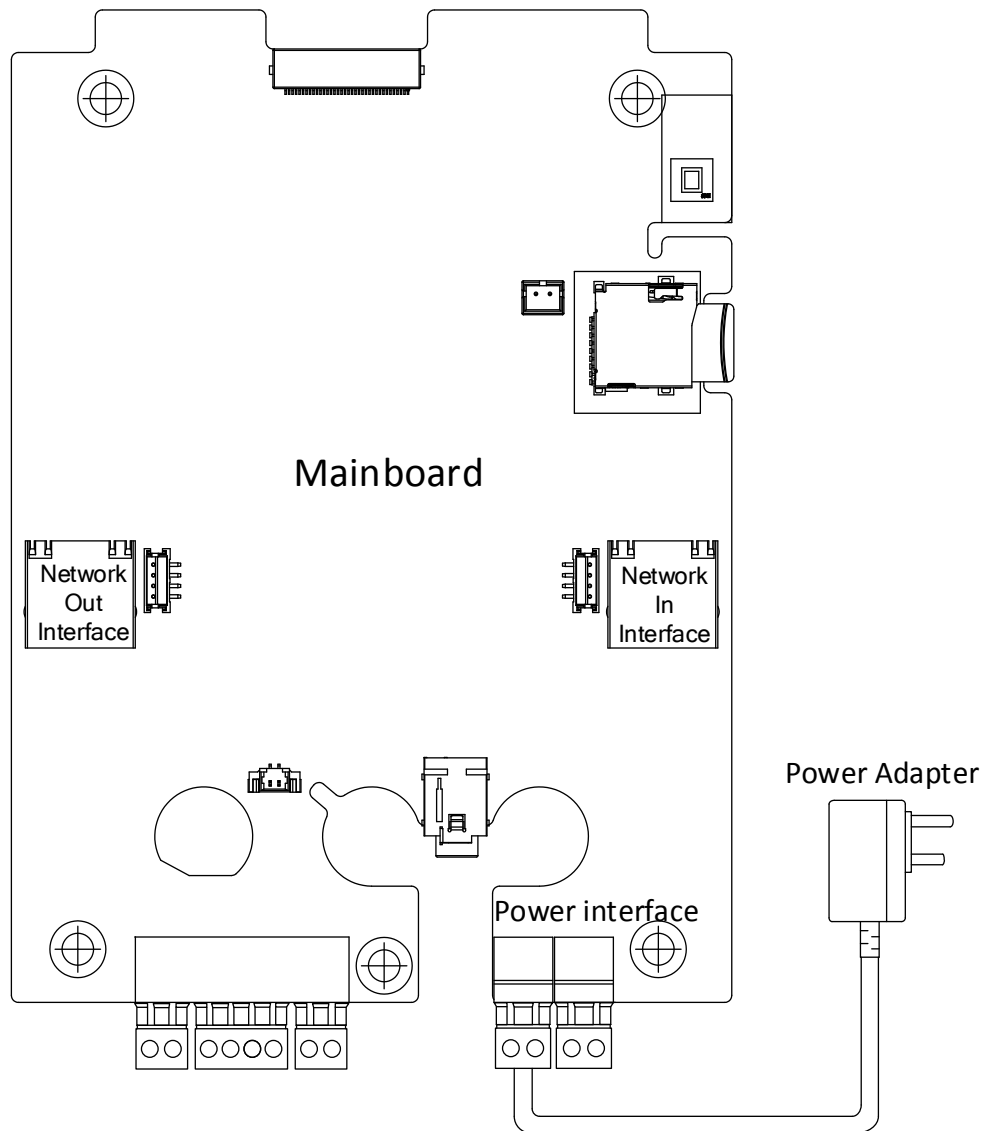


Figure 3-6 Power Supply Wiring

NOTE

The standard of power supply should be 12 VDC/2A.

3.3 Installation

3.3.1 Installation Description

 **NOTE**

- Please check whether there are all relevant accessories in the package before installation. The installation of the alarm station requires 86 gang box. (Gang box is optional.)
- Make sure the power supply is appropriated (12VDC).
- Make sure the device is powered off before installation..

Step 1 Drill a hole in the wall, and fix the gang box in the wall. The size of the hole should be 76 mm (width) × 76 mm (length) × 50 mm (depth).

Step 2 Fix the rear panel of the alarm station to the gang box with two screws (supplied).

Step 3 Route the cables and complete the wiring. Refer to 3.1 for wiring details.

Step 4 Secure the panic alarm station to the rear panel with four screws (supplied).

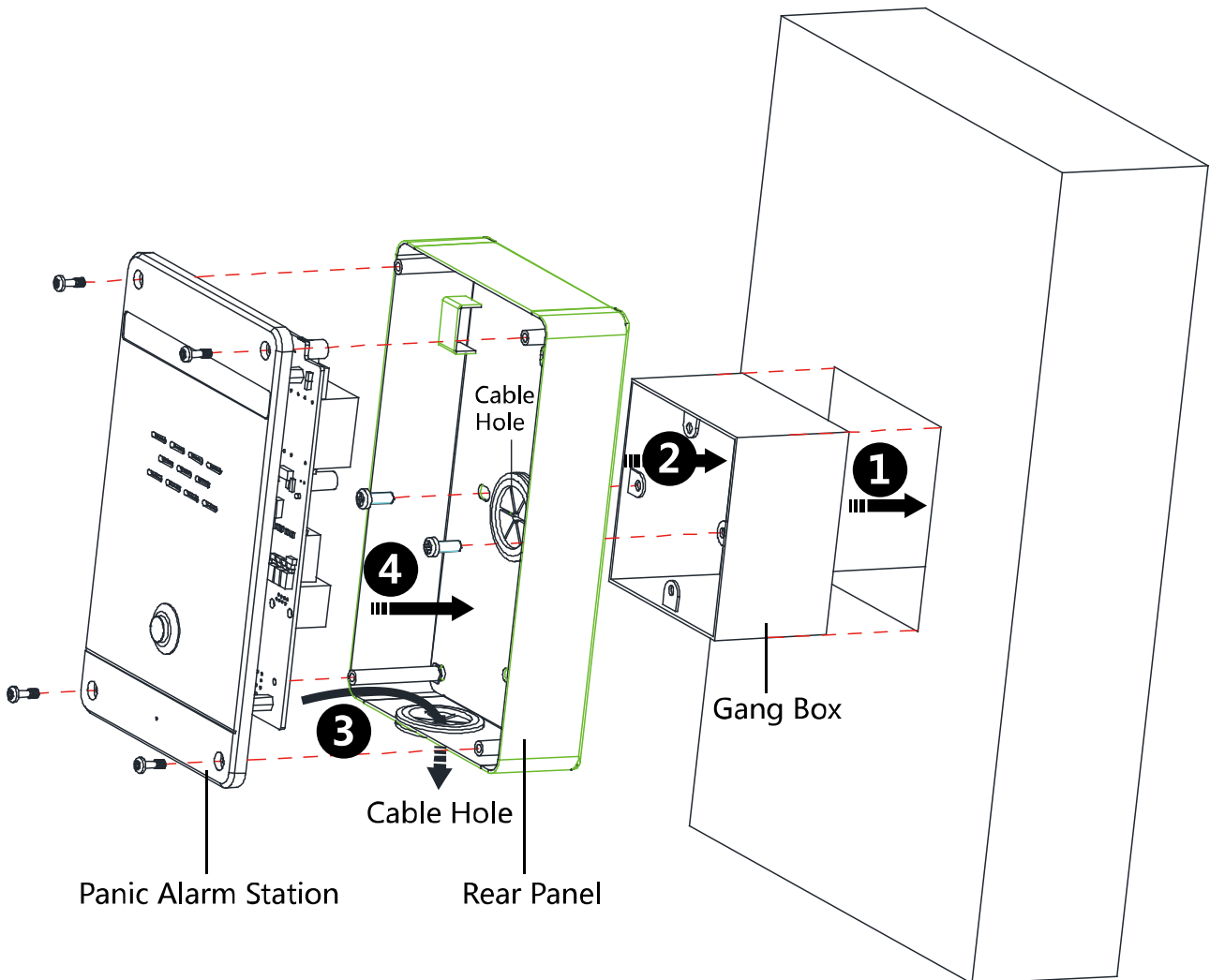


Figure 3-7 Installation

Chapter 4 Device Remote Operation

Purpose:

For the first time use of the device, you are required to activate the device and set the activation password. You can activate the device with SADP Tool, or with iVMS-4200 client software.

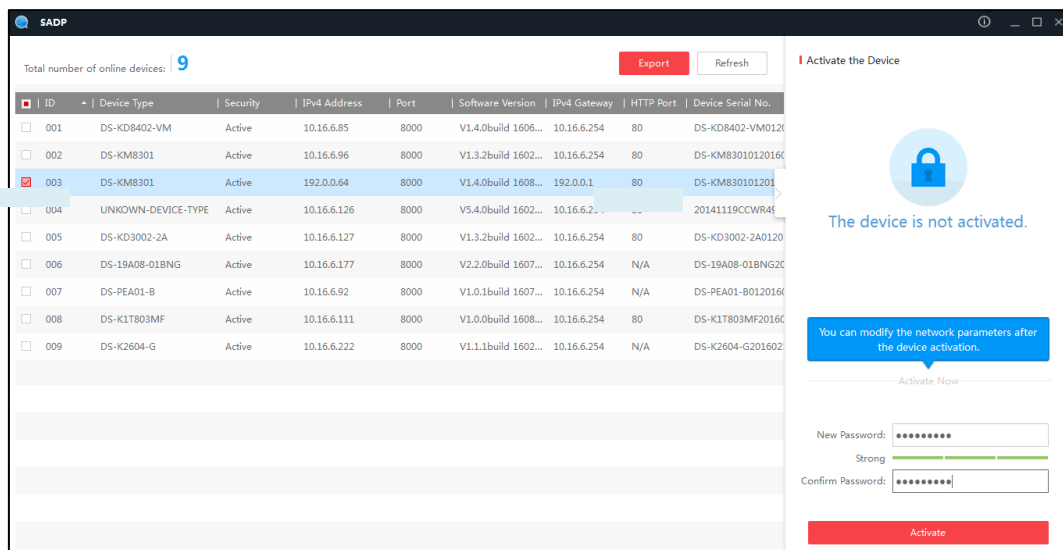
The default values of alarm station are as follows.

- The default IP address: 192.0.0.65.
- The default port No.: 8000.
- The default username (administrator): admin.

4.1 Activation via SADP Tool

Step 1 Run the SADP software to search the online devices.

Step 2 Check the device status from the device list, and select an inactive device.



Step 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.

Step 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.

Step 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.

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

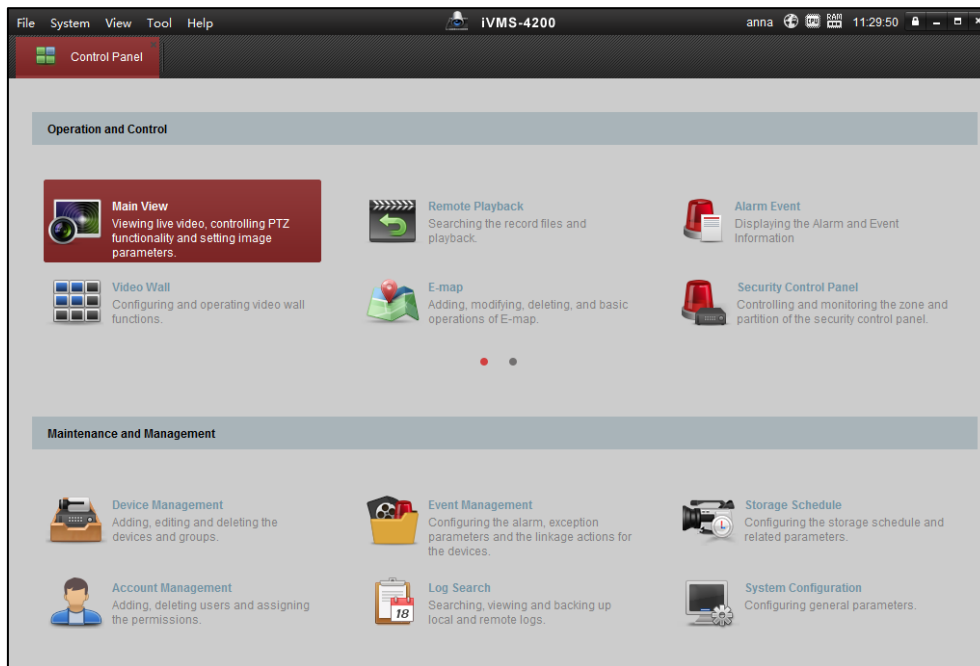
4.2 Remote Operation via Client Software

4.2.1 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.

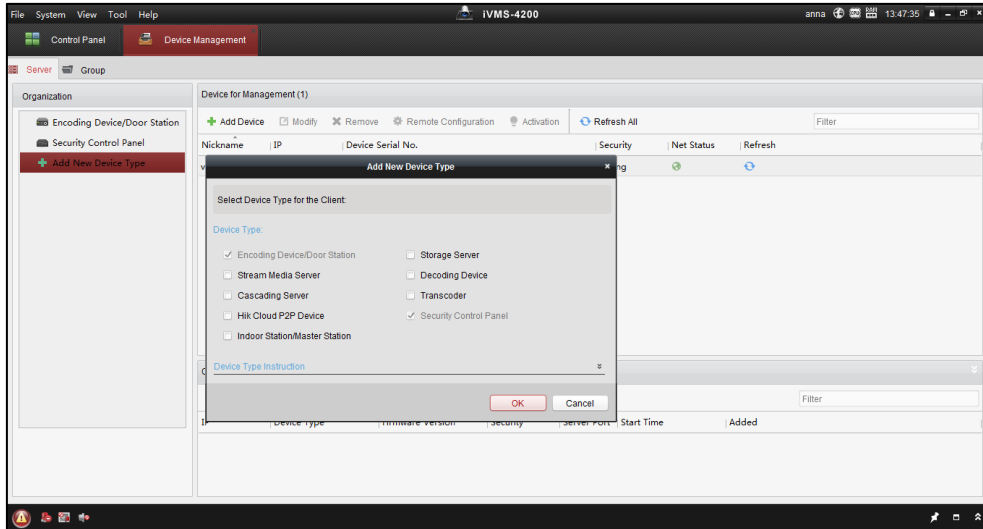
Step 1 Run the client software and the control panel of the software pops up, as shown in the figure below.



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

Step 3 Click **Add Device Type** to enter the adding device type page.

Step 4 Select **Security Control Panel**.

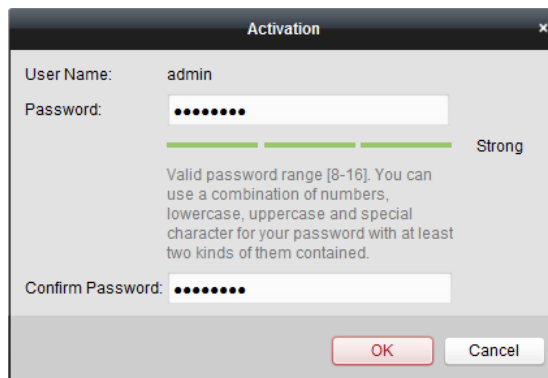


Step 5 Click Security **Control Panel** in the **Organization** list.

Step 6 Check the device status from the device list, and select an inactive device.

Step 7 Click the **Activate** button to pop up the Activation interface.

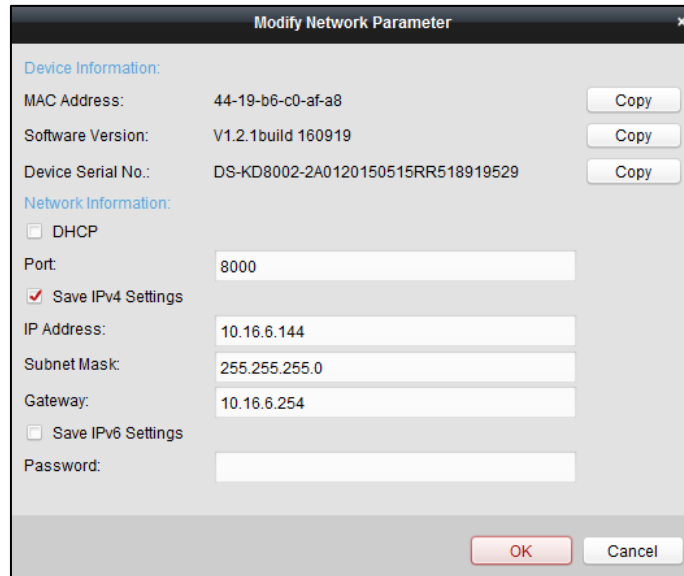
Step 8 Create a password and input the password in the password field, and confirm the password.



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.

Step 9 Click OK button to start activation.


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



Step 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.

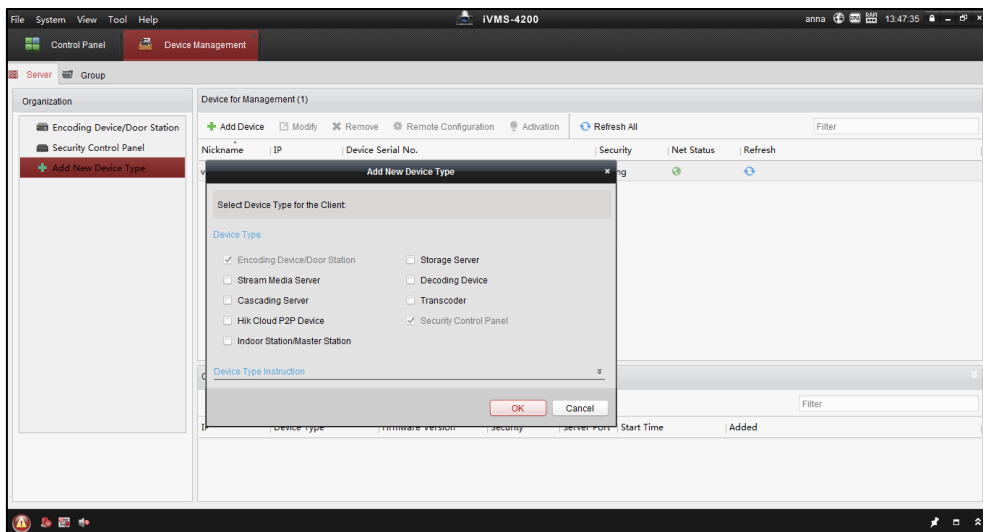
Step 12 Input the password to activate your IP address modification.

4.2.2 Add a Device

Step 1 Click the  icon on the control panel to enter the Device Management interface and click the **Server** tab.

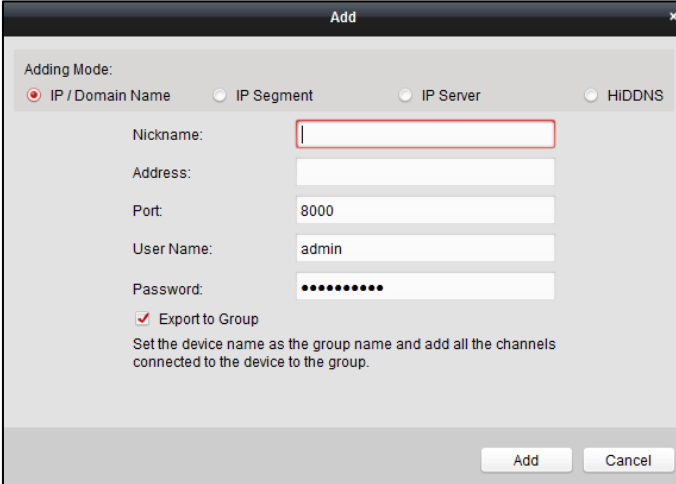
Step 2 Click **Add New Device Type** on the Organization list and select **Security Control Panel**.

Step 3 Click **OK** to save the settings, and the added security control panel type is displayed on the Organization list.



Step 4 Click Security Control Panel and click Add Device to add the device to the management list of the software.

Step 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.



Step 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.

Step 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.

Step 8 Click **Add** to add the device.

4.2.3 Zone Settings

Step 1 Click **Device Management > Security Control Panel > Remote Configuration > Alarm > Zone** to enter the Zone configuration interface.

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

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	
4	Consulting	Consult Zone	Emergency Switch	

Step 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 Settings

Zone No.: 1

Name: Alarm In

Detector Type: Emergency Switch

Zone Type: Shield Zone

Sensitivity: 500ms

Audio File:

Upload Alarm Recover...

Linked Trigger Other

Select All

Trigger 1

Copy To... Save Cancel

Step 4 Select the linked trigger and others.

Step 5 Click **Copy to** to copy all these settings to other zones.

Copy To...

Zone 1 Copy To...

Select All

Zone 2

Zone 3

Save Cancel

Step 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.

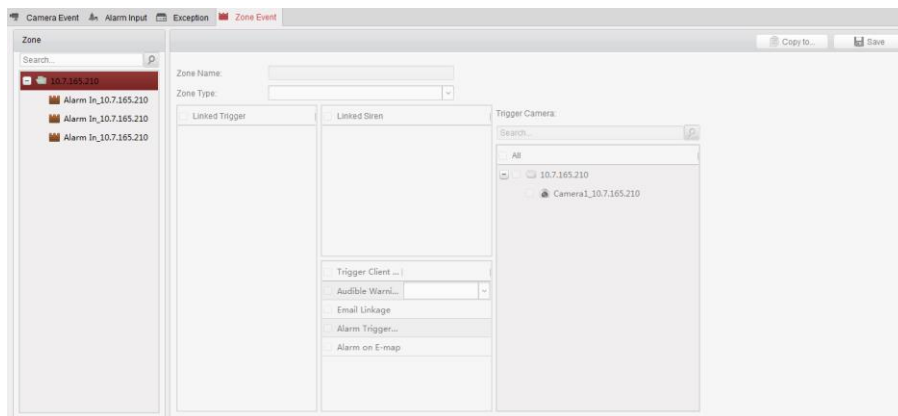
Instant Zone	Alarm is sent out without any delay once the detector is triggered.
Fire Alarm Arming Zone	When the 24-hour armed zone is triggered by fire alarm, sirens will send out resonant and special sound.
24 Hour Non-voiced Zone	When the 24-hour armed zone is triggered, it will send alarm reports 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.

4.2.4 Zone Event Settings

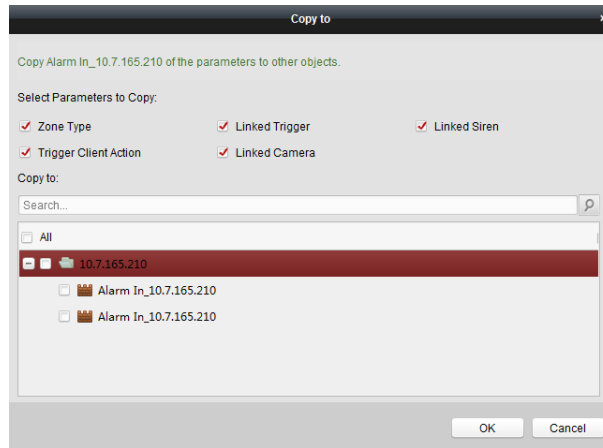
Steps:

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



Step 2 Select the corresponding zone on the left and then tick necessary items.

Step 3 (Optional) Click **Copy to** to tick the necessary items.



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

 **NOTE**

The Alarm In is emergent by default.

4.2.5 Alarm Pop-up Window Settings

Purpose :

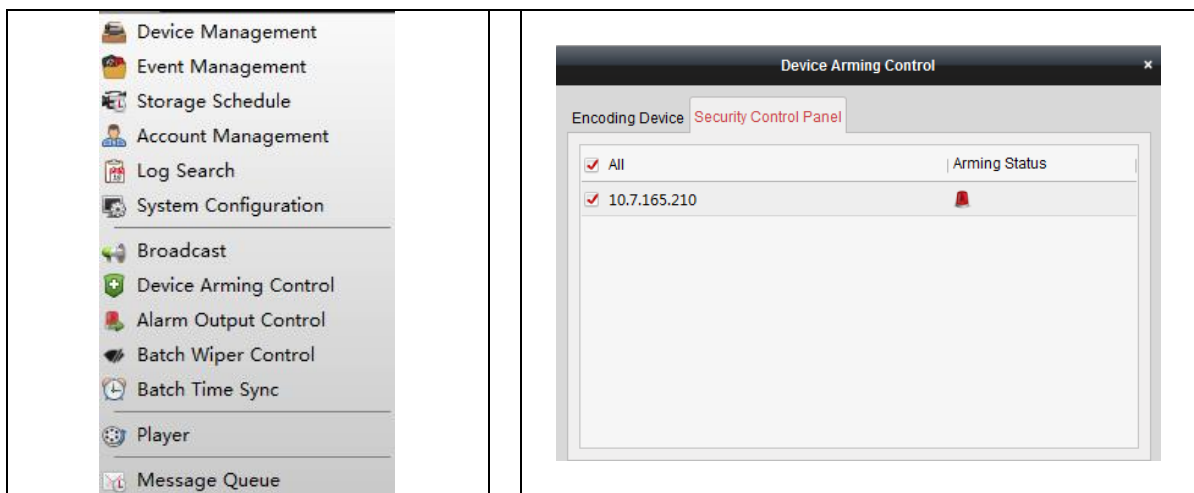
When the devices are armed, the alarm intercom will pop up once the detectors are triggered.

Enable Pop-up Window Function

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

Steps:









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

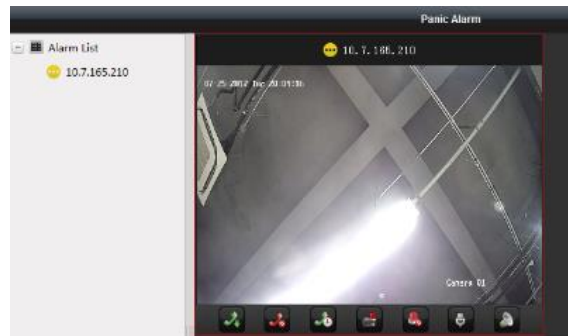


Step 2 Click the alarm device to make it in the state of arming.

Pop-up Window Operation

When the window pops up, you can

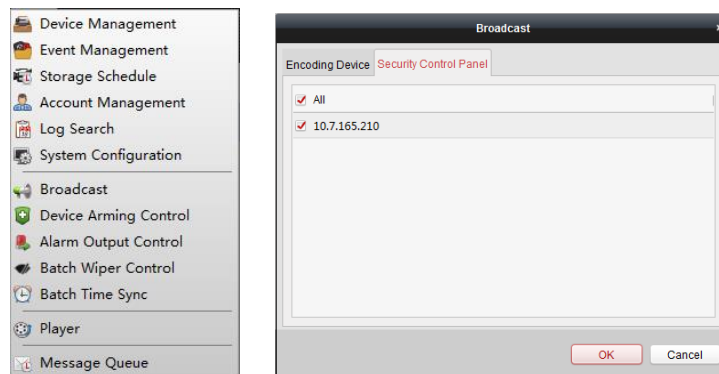
- click  to answer the alarm calling or service consulting;
- click  to reject the alarm calling or service consulting;
- click  to hold on the calling or consulting;
- click  to set volume of audio in and click  to set the volume of audio out;
- click  to capture picture;
- click  to start videoing and click  to stop videoing.



4.3 Broadcast Settings

Steps:

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



Step 2 Click the corresponding item.

Step 3 (Optional) Unclick the corresponding item if you want to cancel the broadcast.

Step 4 Click Save to save the setting.

NOTE

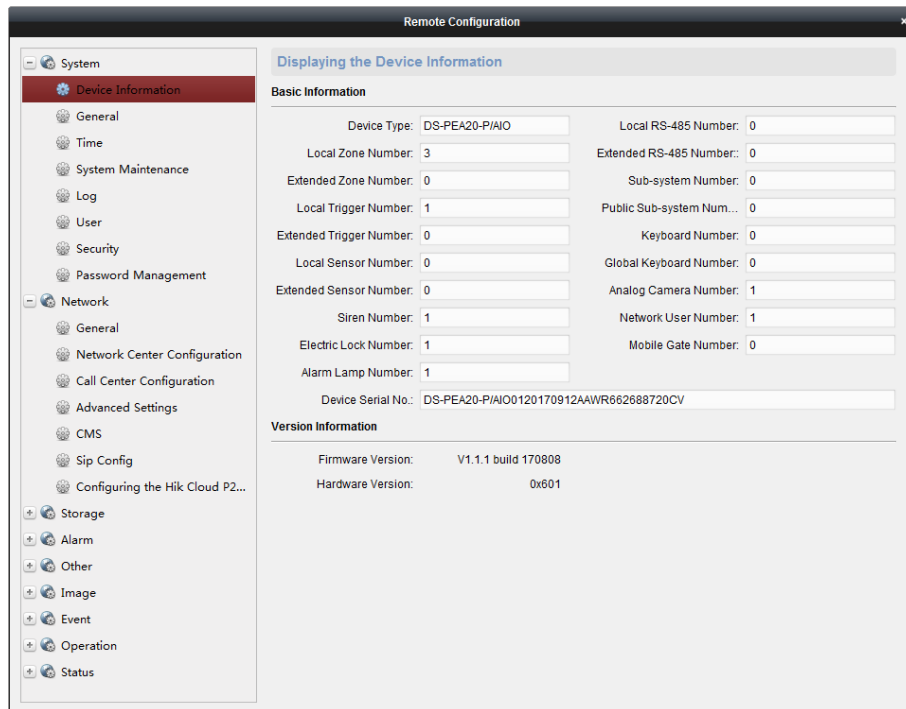
After the broadcast setting, the client can broadcast to multiple devices.

Chapter 5 Remote Operation via iVMS-4200

5.1 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.



5.1.1 General Settings

Steps:

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

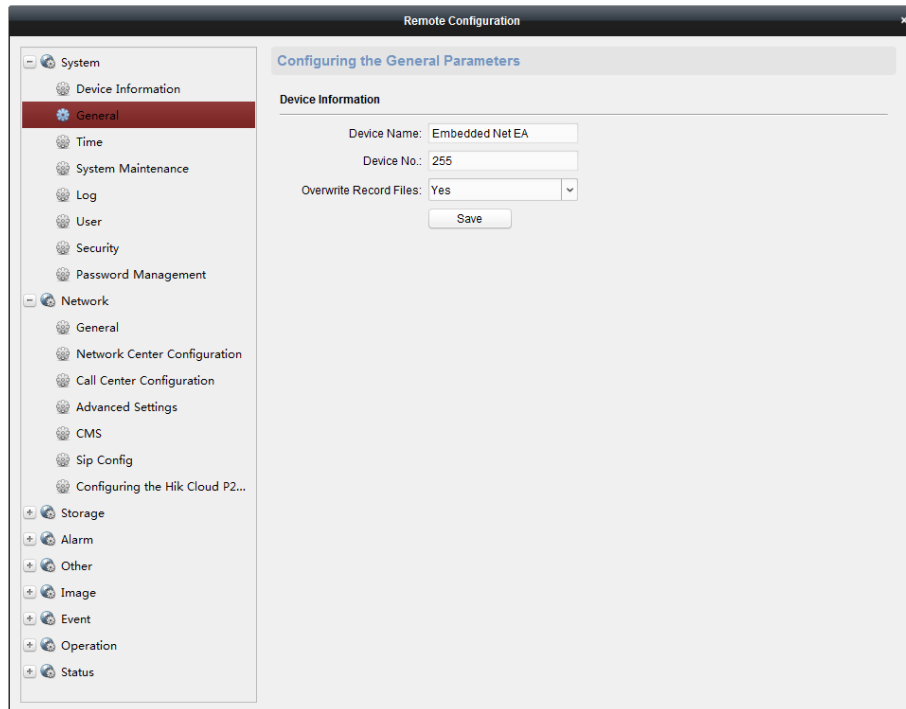


Figure 5-1 Device information

Step 2 Input the device name and device number.

Step 3 Click the drop down menu to select whether to overwrite the record files.

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

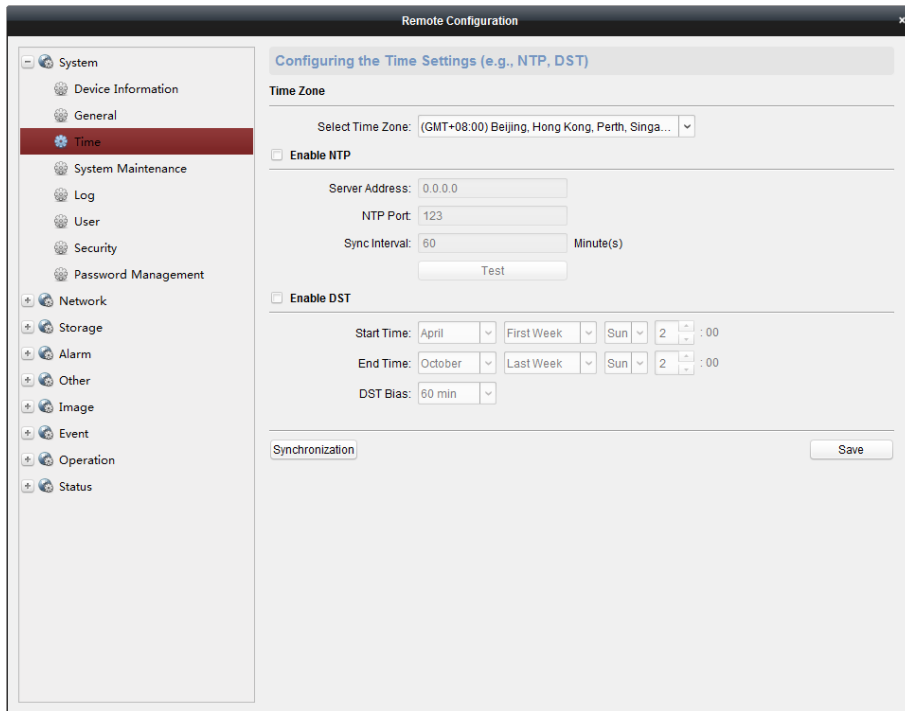
5.1.2 Timing Settings

Purpose:

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

Steps:

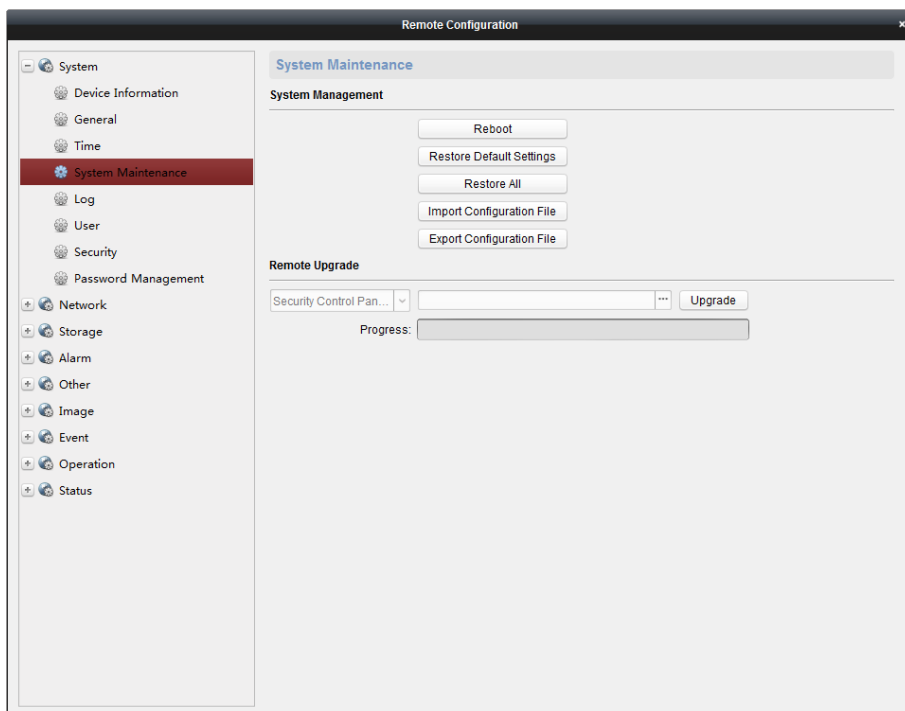
Step 1 Click Remote **Configuration > System > Time** to enter the time configuration interface.



Step 2 Click Synchronization to do timing.

5.1.3 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.

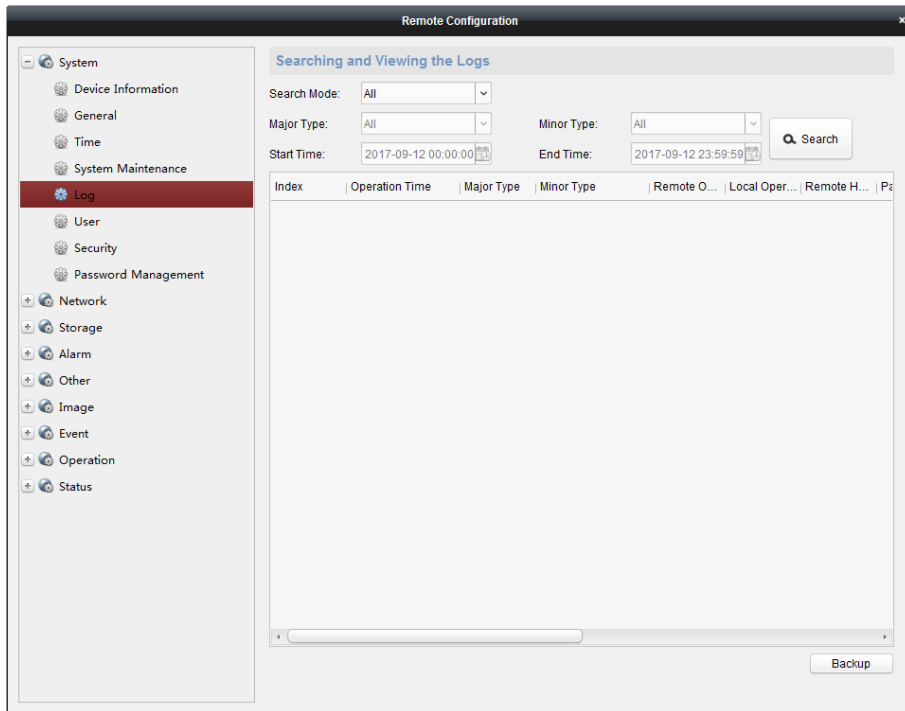


NOTE

After upgrading, the device needs to be restarted.

5.1.4 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.



5.1.5 User Settings

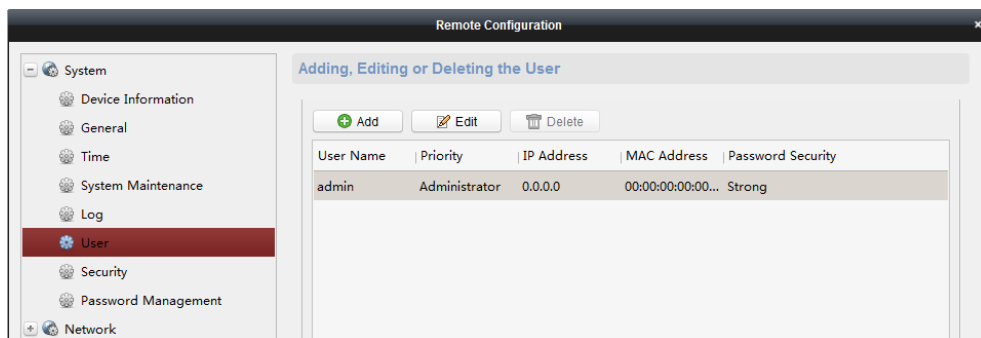
Purpose:


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

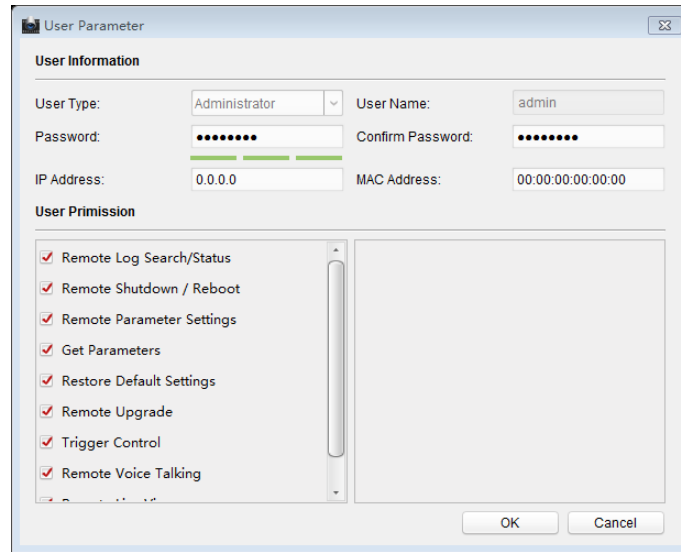
- Add an admin User (Only one admin user can be added)

Steps:

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



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




Step 3 Enter the corresponding user information including the user type, user name, password, IP address, and MAC address.

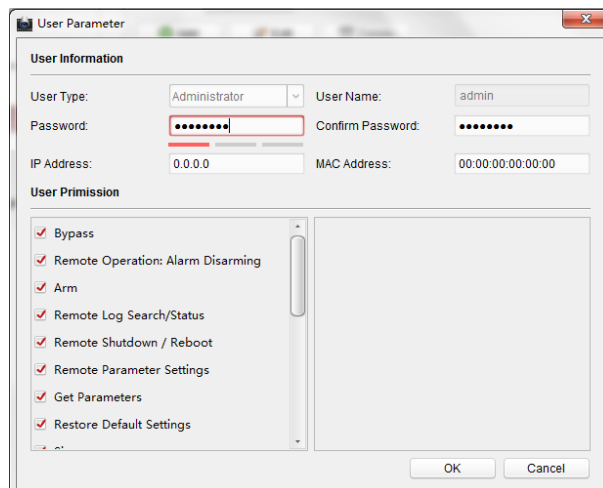
Step 4 Select the permission of the user.

Step 5 Click OK to finish the settings.

Edit a User

Steps:

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



Step 2 Edit the corresponding user information including the user type, user name, password, IP address, and MAC address.


Step 3 Edit the permission of the user.

Step 4 Click **OK** to finish the settings.

Delete a User

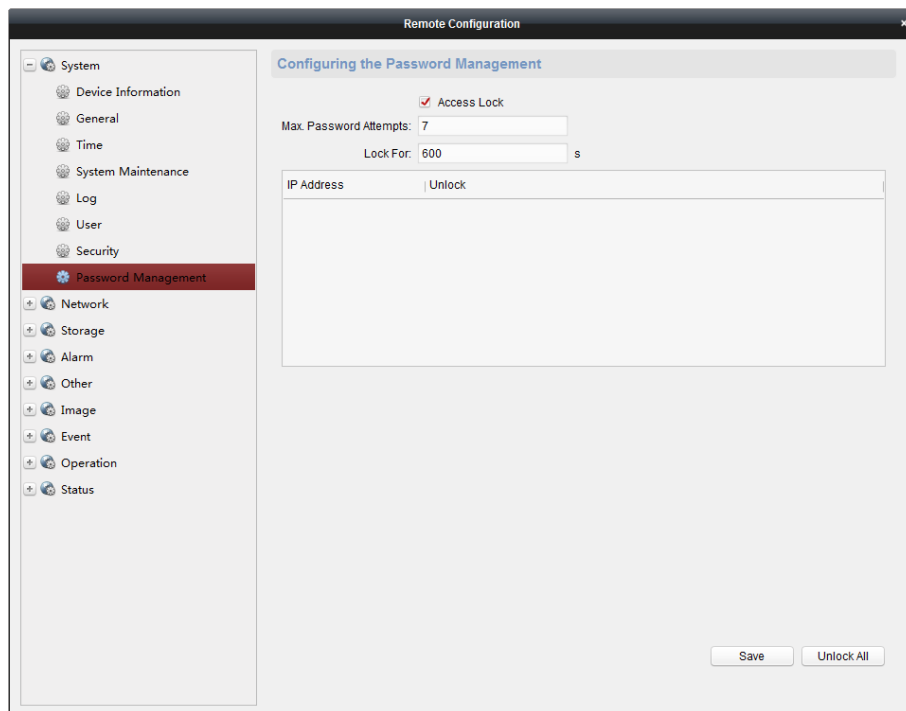
Steps:

Step 1 Select a user needs to be deleted.

Step 2 Click  to delete the user.

5.1.6 Password Management

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



5.2 Network Settings

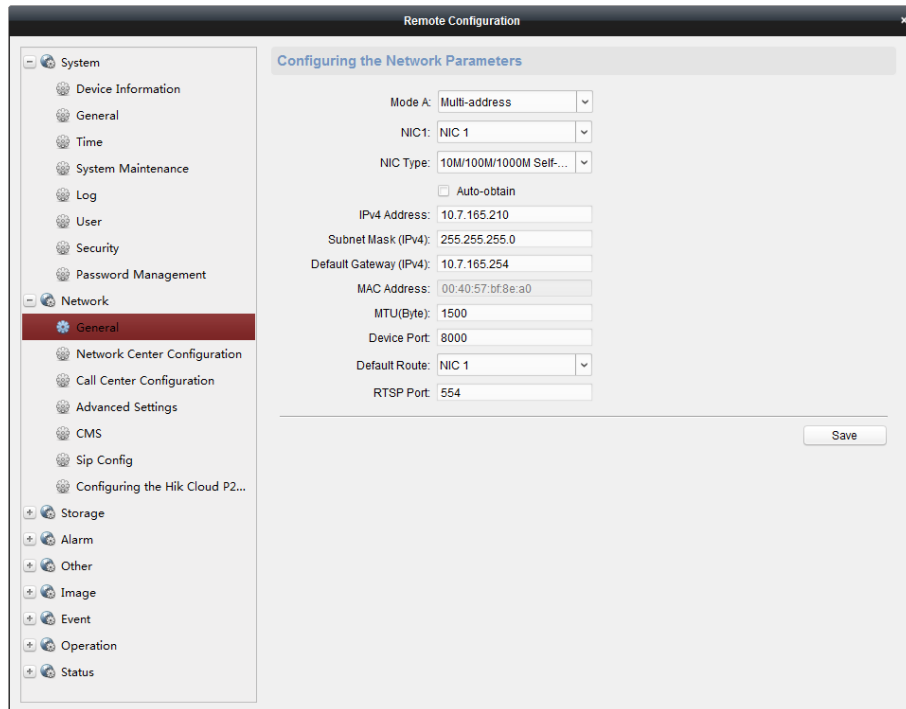
Purpose:

You can edit the general network parameters in this section.

5.2.1 General Network Parameters Settings

Steps:

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



Step 2 Configure the NIC setting.

Step 3 Click **Save** to save the above settings.

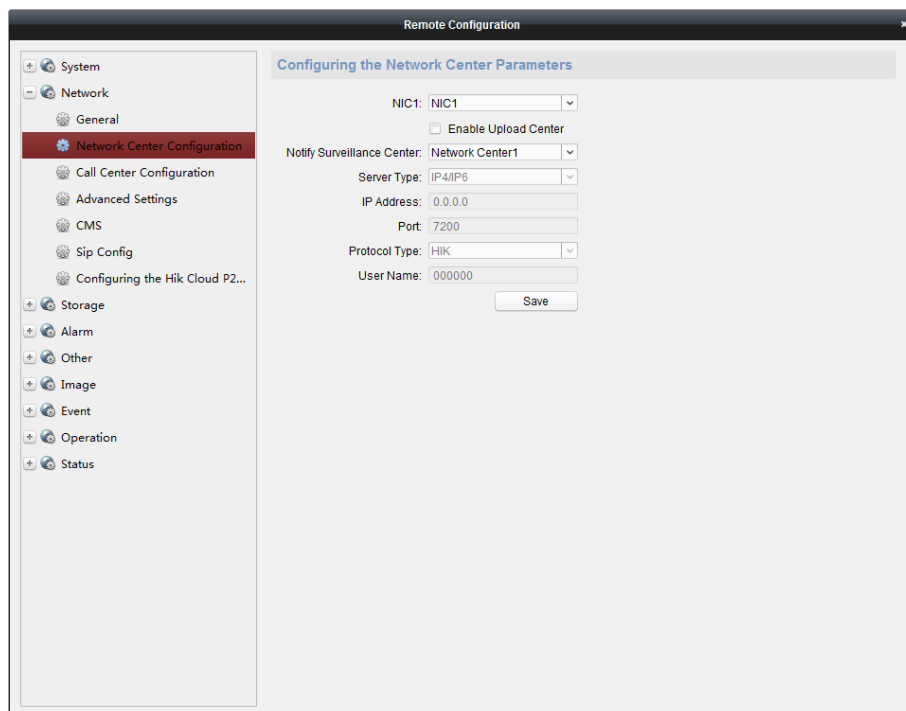
5.2.2 Network Center Settings

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:

Step 1 Click **Remote Configuration > Network > Network Center Configuration** to enter the network center configuration interface.



Step 2 Click and select a network center. Two centers are selectable.

Step 3 Click Enable Upload Center.

Step 4 Click the dropdown menu to select a sever type. Two sever types are available: IP4/IP6 and domain.

Step 5 Enter the IP address which is used to communicate with the network alarm receiving center.

Step 6 Enter the port NO. for communicating with the alarm receiving center.

Step 7 Click the dropdown menu to select the protocol type.

Step 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.

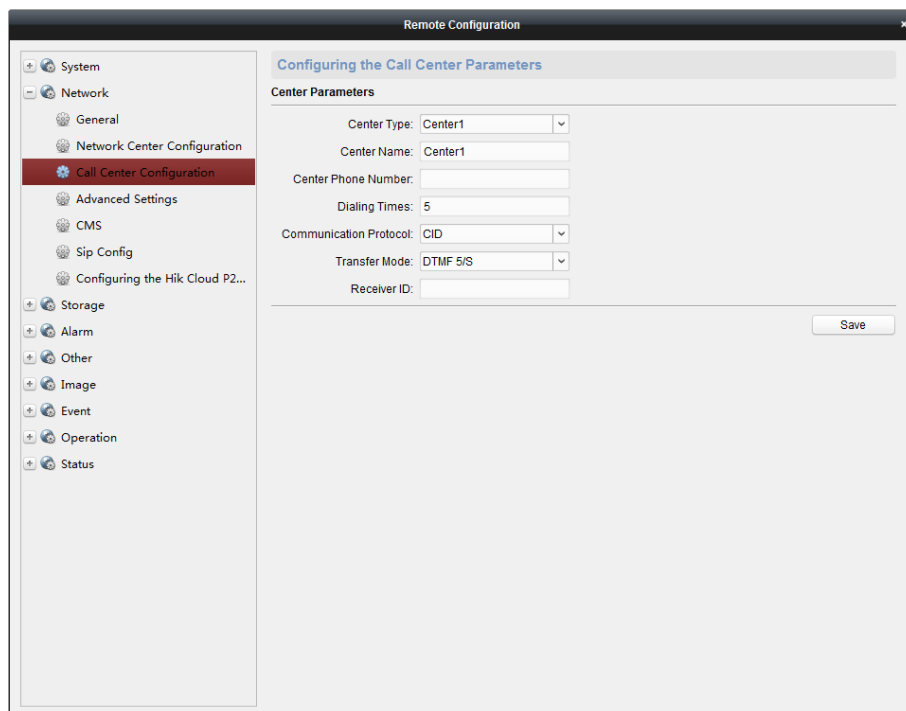
5.2.3 Call Center Settings

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:

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



Step 2 Select a center type (only center 1 is available).

Step 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.

Step 4 Enter the dialing times (1~15). The dialing times represents the times that the control panel trying to communicate the alarm receiving center.

Step 5 Select the communication protocol.

Step 6 Select the transmission mode: DTMF5/S and DTMF10/S.

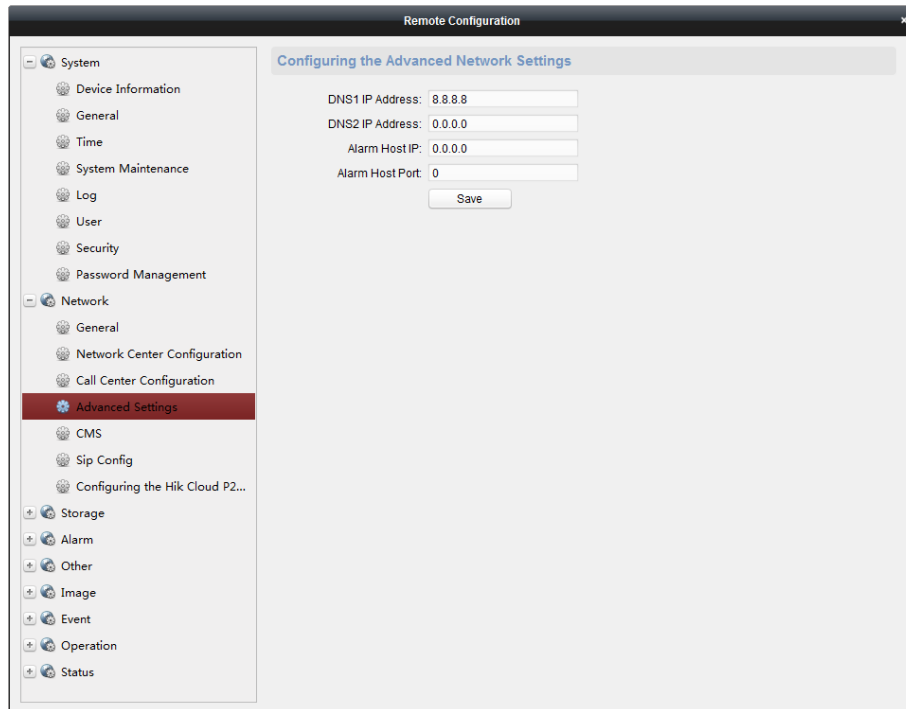
Step 7 Enter the receiver ID which is the authentication account while doing the communication with the alarm receiving center.

Step 8 Click Save to save the settings.

5.2.4 Advanced Network Parameters Settings

Steps:

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



Step 2 Enter the corresponding DNS sever address.

Step 3 Enter the IP address and port NO. of the control panel.

Step 4 Click Save to save the settings.

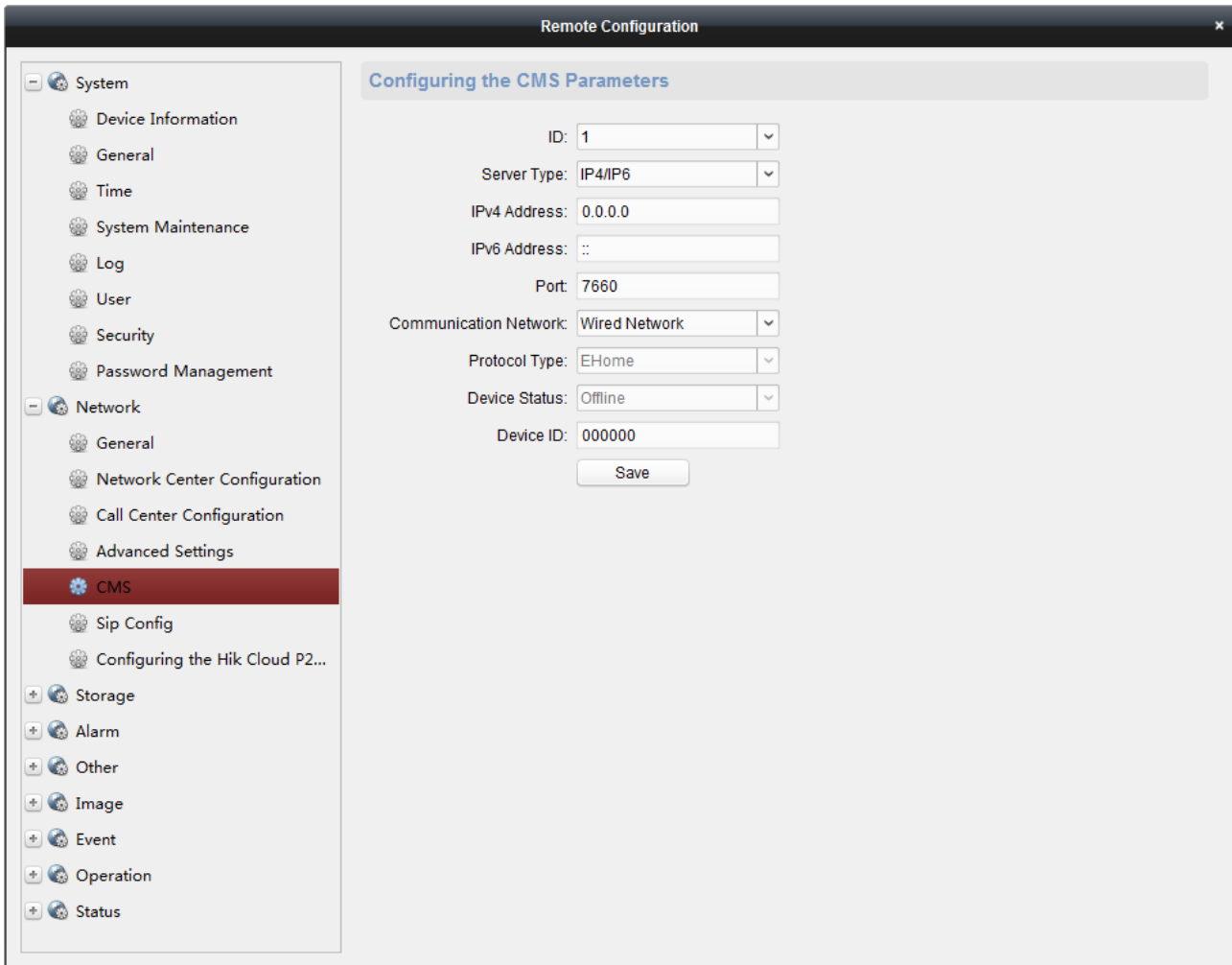
5.2.5 CMS Settings

Purpose:

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

Steps:

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



Step 2 Click the dropdown menu to select a sever type. Two sever types are available: IP4/IP6 and domain.

Step 3 Enter the IP address which is used to communicate with the service.

Step 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.

Step 5 Click the dropdown menu to select the communication network. Four types are available: Auto, Wired Network Priority, Wired Network and Wireless Network.

Step 6 Enter the device ID where the CID report comes from.

 **NOTE**

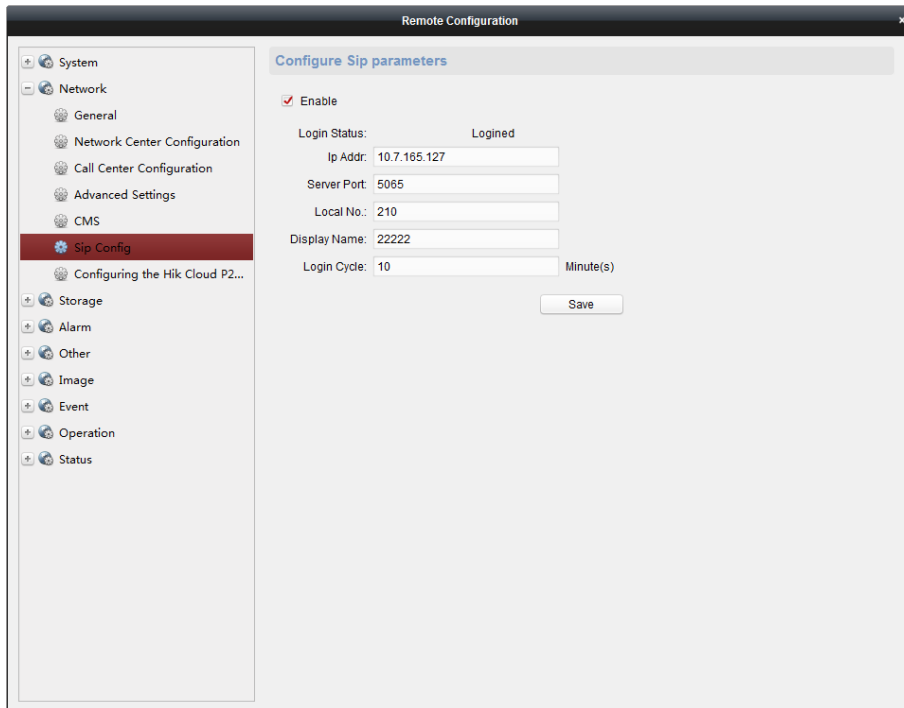
- The length of the device ID should be 6 characters.
- Only numeric (0~9), and letter (A ~ F & a ~ f) are valid for this device ID.

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

5.2.6 Sip Settings

Steps:

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



Step 2 Check **Enable** box to enable the Sip server.

Step 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)

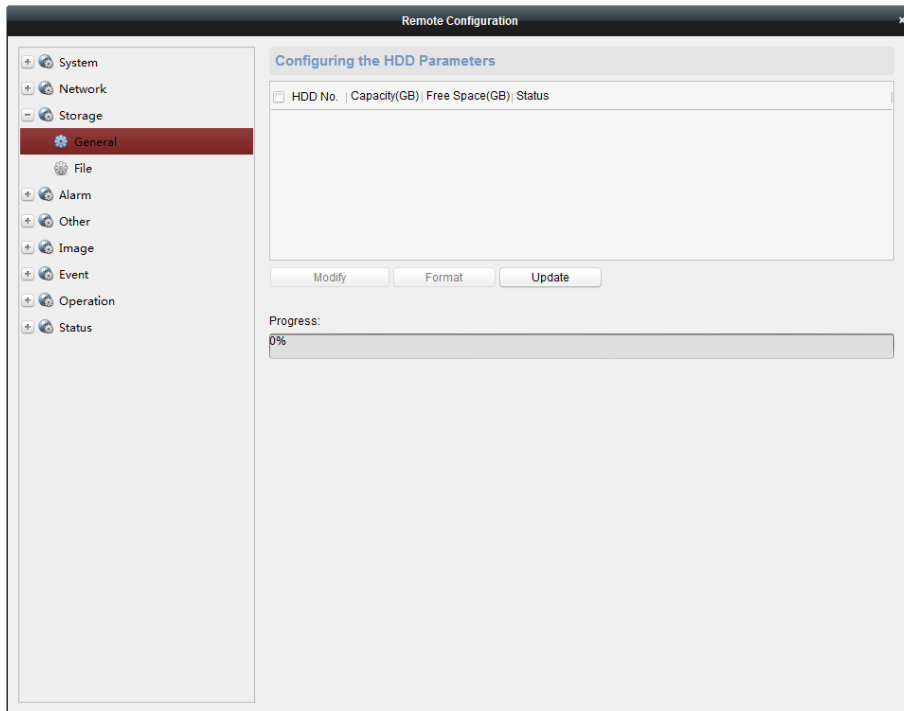
Step 4 Click **Save** to save the settings.

5.3 Storage Settings

5.3.1 HDD Information`

Steps:

Step 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.



Step 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.

Step 3 Click Save to save the settings.

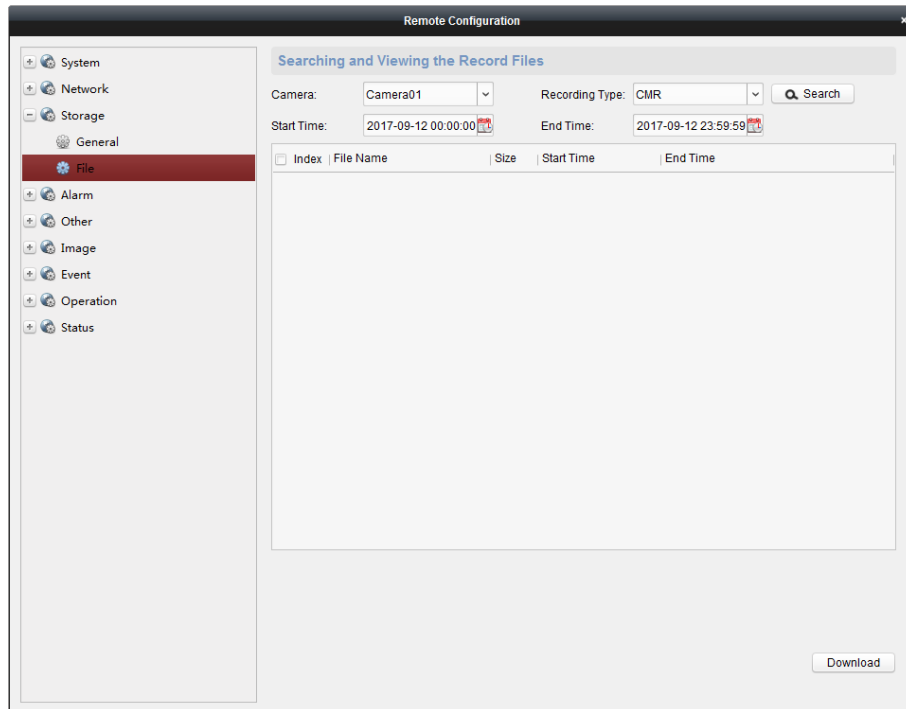
 **NOTE**

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

5.3.2 File Query

Steps:

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



Step 2 Enter the search criteria including camera name, property, start time and end time.

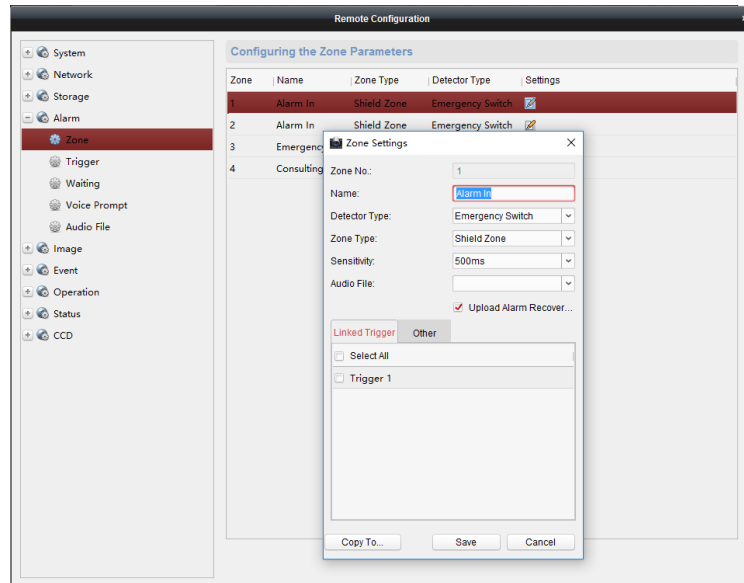
Step 3 Click **Search** to get the file list.


5.4 Alarm Settings

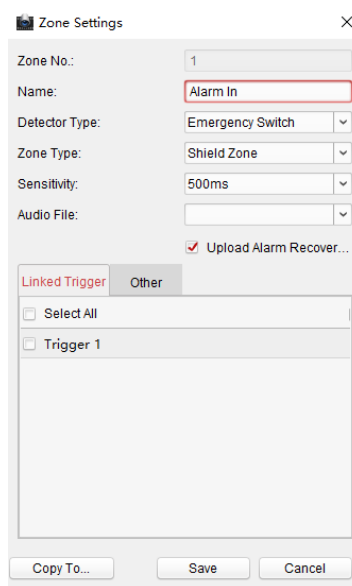
5.4.1 Zone Settings

Steps:

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



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



Step 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.

Step 4 Select the linked trigger and others.

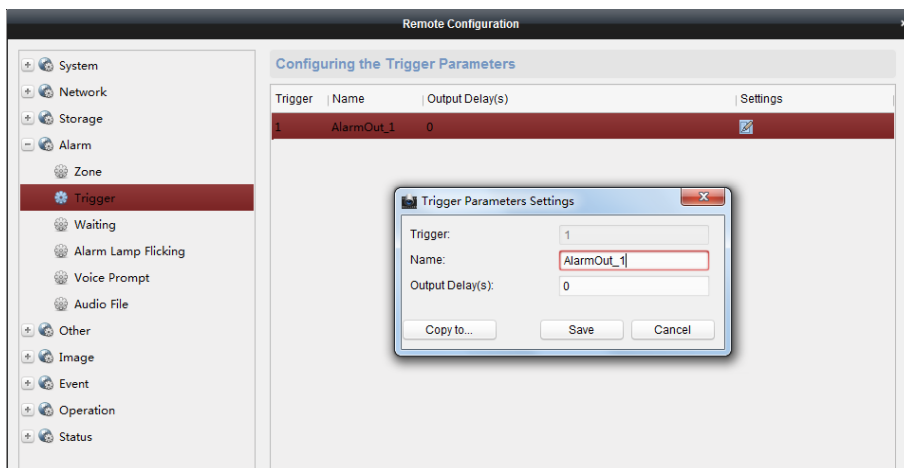
Step 5 Click **Copy to** to copy all these settings to other Zones.


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

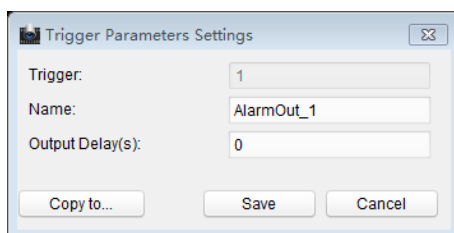
5.4.2 Trigger Settings

Steps:

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



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



Step 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.

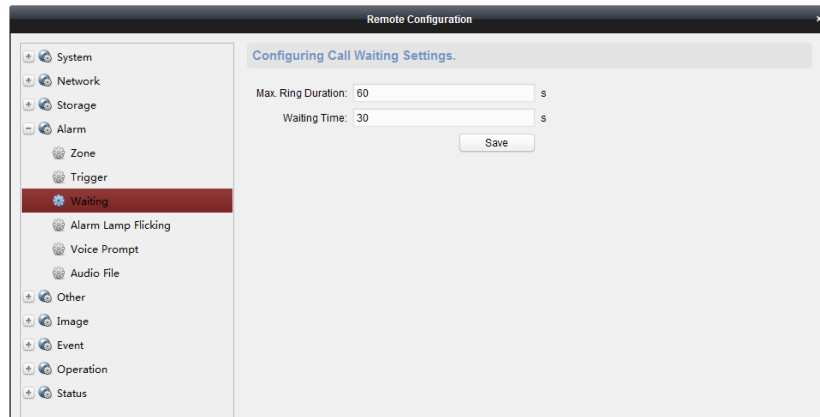
Step 4 Click **Copy to** to copy all these settings to other Zones.

Step 5 Click **Save** to save the settings.

5.4.3 Calling Waiting Settings

Steps:

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



Step 2 Enter the Max. ring duration (40s to 80s)for reporting alarm to the center.

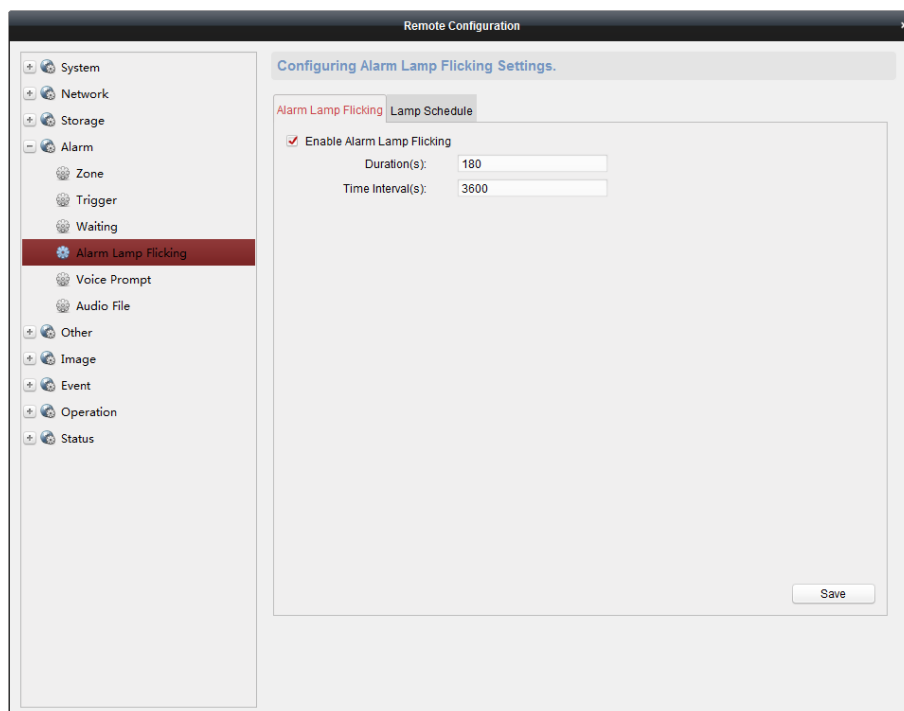
Step 3 Enter the waiting time (10s to 60s) for the center to answer the call.

Step 4 Click Save to save the settings.

5.4.4 Alarm Lamp Settings

Steps:

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



Step 2 Check Enable Alarm Lamp Flicking box.

Step 3 Enter the alarm lamp flashing duration (s).

Step 4 Enter the time interval for each flashing(s).

Step 5 Click Save to save the settings.

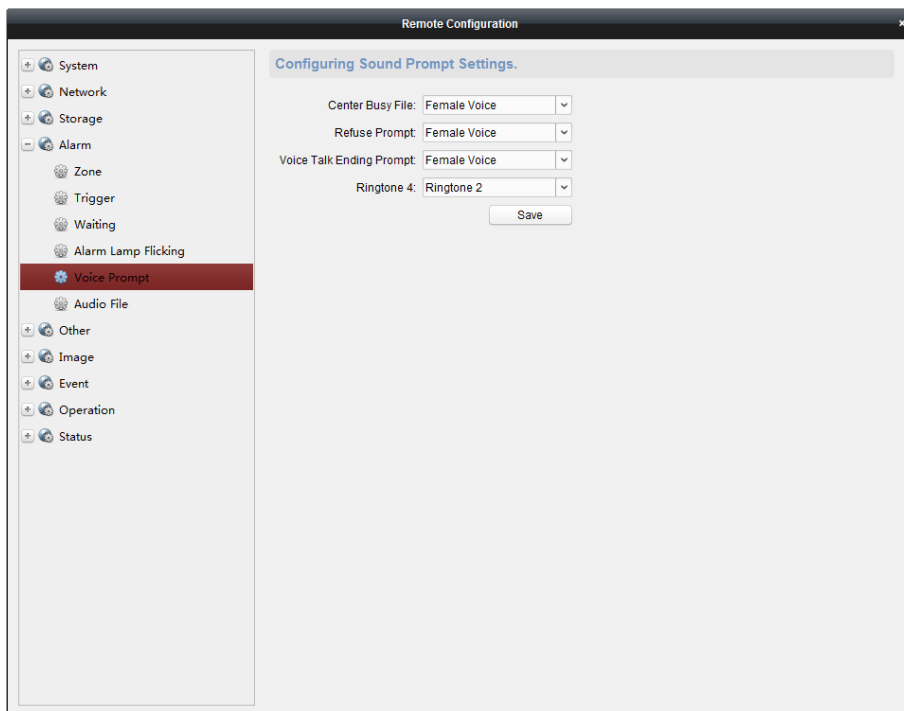
 **NOTE**

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

5.4.5 Voice Prompt Settings

Steps:

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



Step 2 Check Enable Alarm Lamp Flicking box.

Step 3 Select Female/Male voice for center busy file, refuse, and voice talking prompt.

Step 4 Select the ring tone.

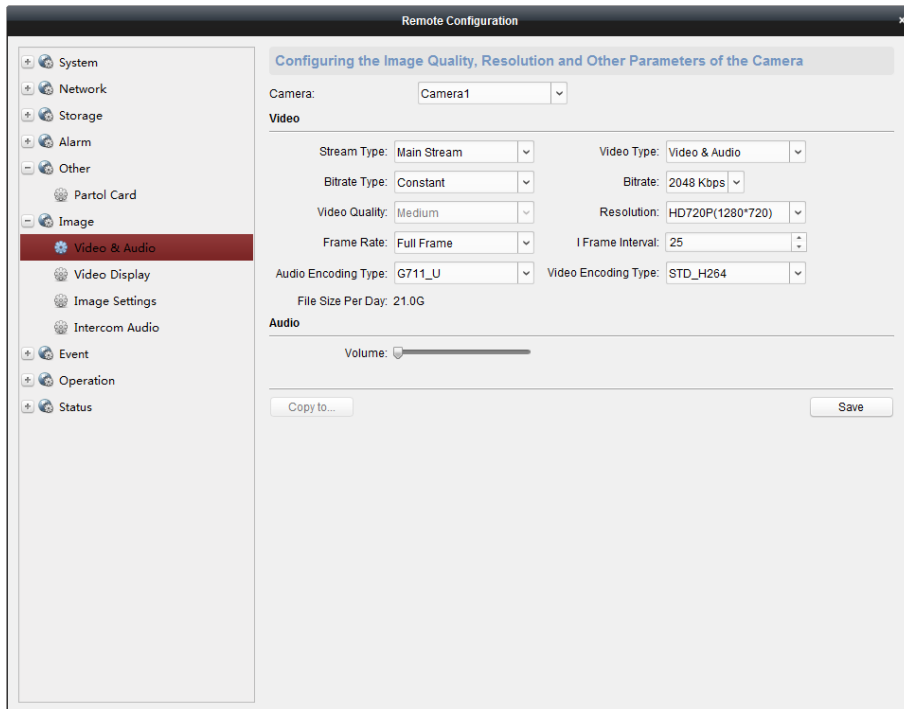
Step 5 Slick Save to save the settings.

5.5 Image Settings

5.5.1 Video& Audio Settings

Steps:

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



Step 2 Select a camera needs to be configured.

Step 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.

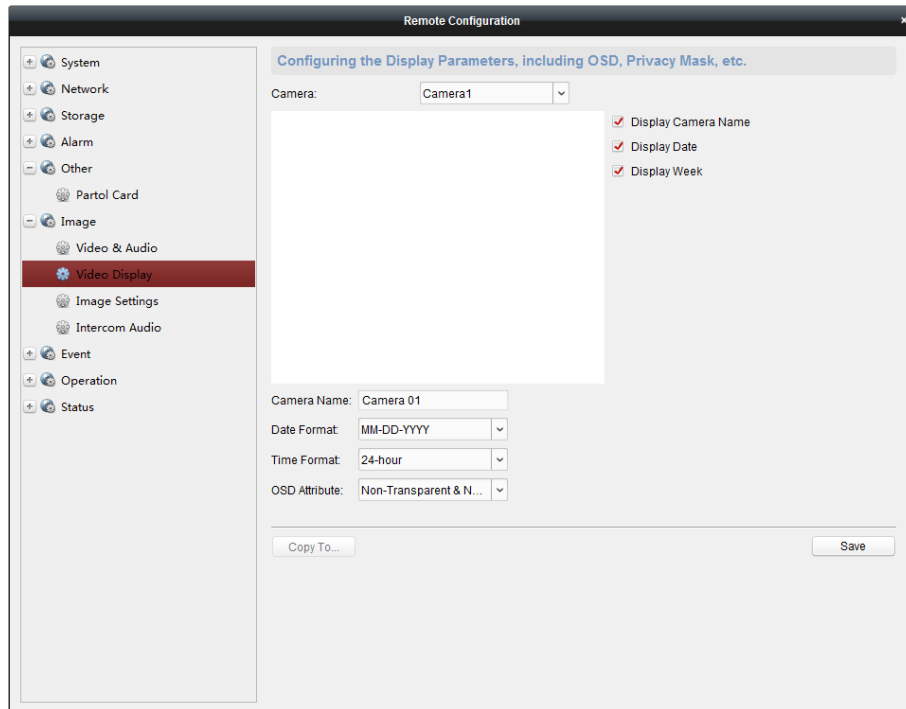
Step 4 Click Copy to to copy all these settings to other Zones.

Step 5 Click Save to save the settings.

5.5.2 OSD Settings

Steps:

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




Step 2 Check the corresponding checkbox to select the display of camera name, date or week if required.

Step 3 Edit the camera name in the text field of Camera Name.

Step 4 Select from the drop-down list to set the time format, date format and display mode.

Step 5 Check the checkbox in front of textbox to enable the on-screen display.

Step 6 Input the characters in the textbox.

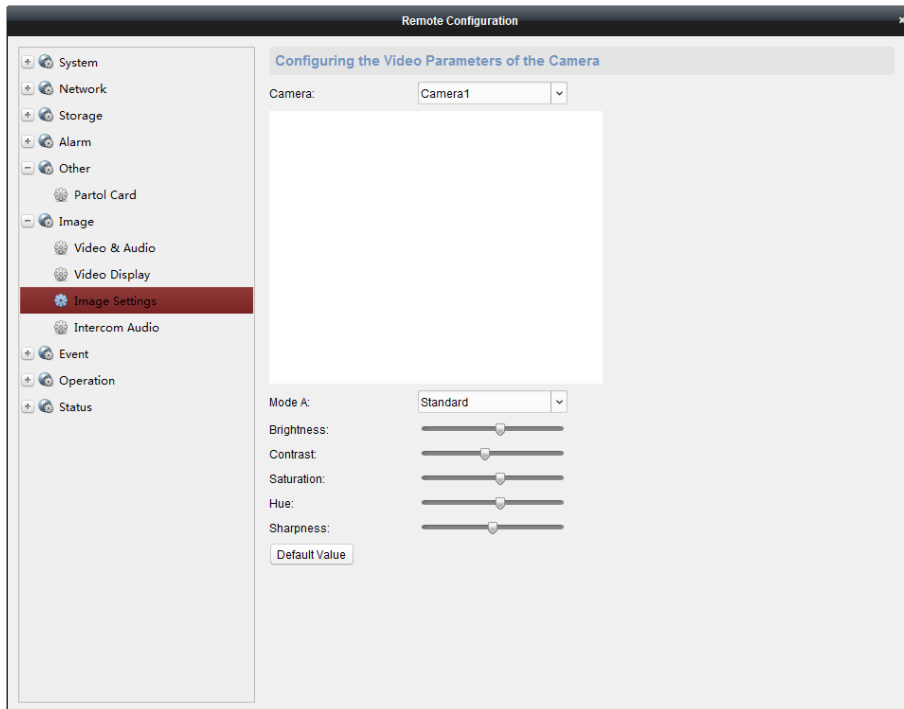
Step 7 Use the mouse to click and drag the red text frame  in the live view window to adjust the text overlay position.

Step 8 Click Save to save the settings.

5.5.3 Image Settings

Steps:

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



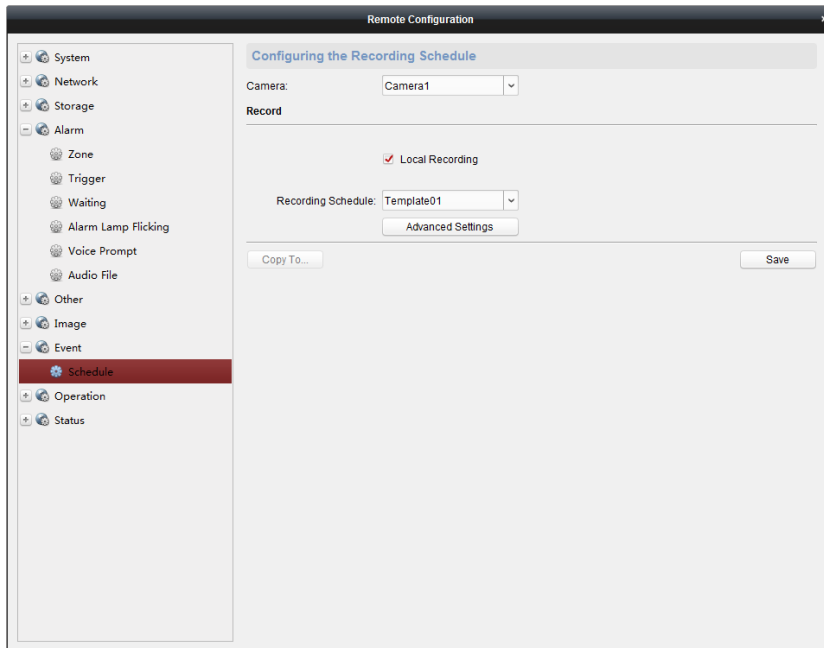
Step 2 Drag the  to adjust the brightness, contrast, saturation of the image.

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

5.6 Event Settings

5.6.1 Schedule Settings

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



● Record Schedule Settings

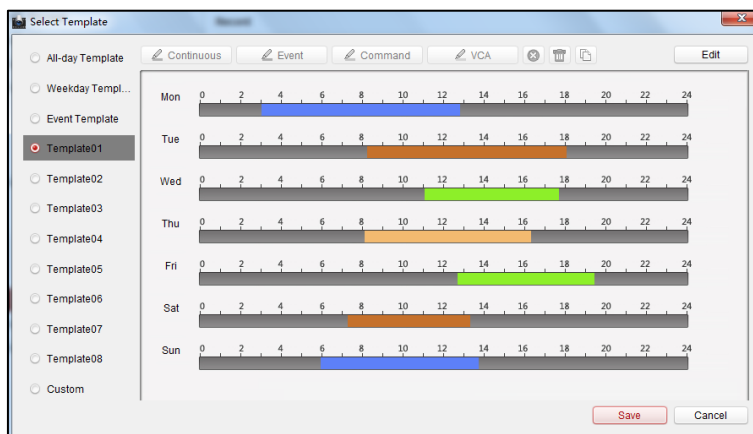
Steps:

Step 1 Select the camera needs to be configured.

Step 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.


Step 3 Select from the drop-down list to set the recording type including Main Stream and Sub Stream.


Step 4 Click the icon to set the record schedule.




Step 5 Click Edit to enter the Templates Management interface. Select the template to be set and you can edit the template name.


Step 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.

Step 7 Optionally, you can select the schedule time bar,

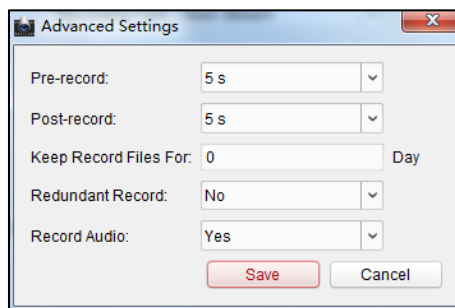
And then click the icon  to delete the selected time bar,

Or click the icon  to delete all the time bars,

Or click the icon  to copy the time bar settings to the other dates.

Step 8 Click **Save** to save the template, or click cancel to exit the interface.

Step 9 Click **Advanced Settings** button to set the pre-record time, post record time, video expired time, redundant record and audio recording.




Step 10 Click **Copy to** to copy all these settings to other Zones.

Step 11 Click **Save** to save the settings.

- Capture Schedule Settings

Step 1 Check the checkbox of Capture Settings to enable the device local capturing.

Step 2 Click the  icon to set the capture schedule. For details, refer to Steps 5, 6, 7 in Record Schedule Settings.

Step 3 Click Copy to to copy all these settings to other Zones.

Step 4 Click Save to save the settings.

5.7 Camera Parameter Settings

5.7.1 Video Parameter Settings

Steps:

Step 1 Click **Remote Configuration > Camera Parameter > Video Parameter** to enter the interface.

Step 2 Select the monitoring point.

Step 3 Click **Save** to save the settings.

5.7.2 WDR Settings

Steps:

Step 1 Click **Remote Configuration > Camera Parameter > WDR** to enter the interface.

Step 2 Select the monitoring point and then choose whether to open.


Step 3 Set the WDR level.

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

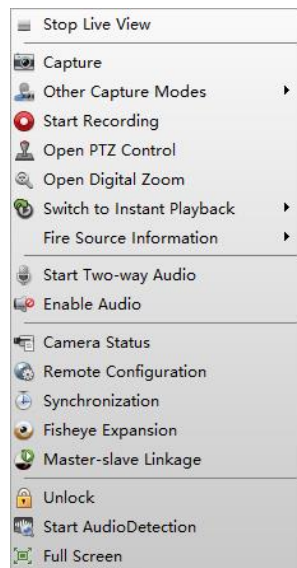
5.8 Audio Detection

Audio detection is used to whether the voice function of the alarm station is complete and whether the network is stable.

Steps:

Step 1 Click the  icon on the control panel to enter the live viewing.

Step 2 Right click and click **Start AudioDetection**.



Step 3 Use the microphone to detect the audio function.

Step 4 Click **Stop Audio Detection**.



See Far, Go Further