HIKVISION

Panic Alarm Master Station

User Manual

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 Master 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.

Symbol Conventions

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

Symbol	Description
ℹ 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 Instructions

- Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.
- In the use of the product, you must be in strict compliance with the electrical safety regulations of the nation and region. Please refer to technical specifications for detailed information.
- Input voltage should meet both the SELV (Safety Extra Low Voltage) and the Limited Power Source with 12 VDC according to the IEC60950-1 standard. Please refer to technical specifications for detailed information.
- Do not connect several devices to one power adapter as adapter overload may cause over-heating or a fire hazard.
- Please make sure that the plug is firmly connected to the power socket.
- If smoke, odor or noise rise from the device, turn off the power at once and unplug the power cable, and then please contact the service center.

Preventive and Cautionary Tips

Before connecting and operating your device, please be advised of the following tips:

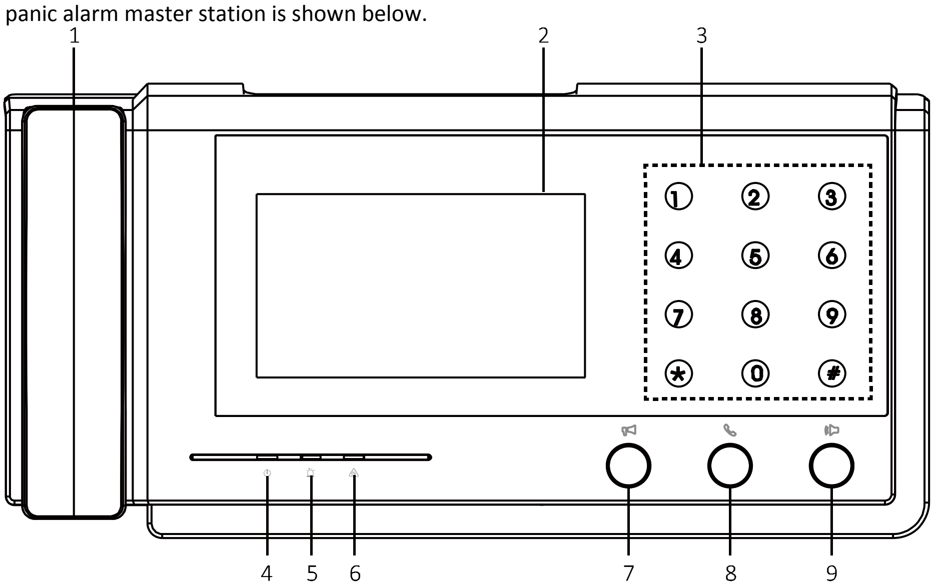
- Ensure unit is installed in a well-ventilated, dust-free environment.
- Unit is designed for indoor use only.
- Keep all liquids away from the device.
- Ensure environmental conditions meet factory specifications.
- Ensure unit is properly secured to a rack or shelf. Major shocks or jolts to the unit as a result of dropping it may cause damage to the sensitive electronics within the unit.
- Use the device in conjunction with an UPS if possible.
- Power down the unit before connecting and disconnecting accessories and peripherals.
- A factory recommended HDD should be used for this device.
- Improper use or replacement of the battery may result in hazard of explosion. Replace with the same or equivalent type only. Dispose of used batteries according to the instructions provided by the battery manufacturer.

目　录

Chapter 1 Appearance

Front Panel

The front panel of panic alarm master station is shown below.



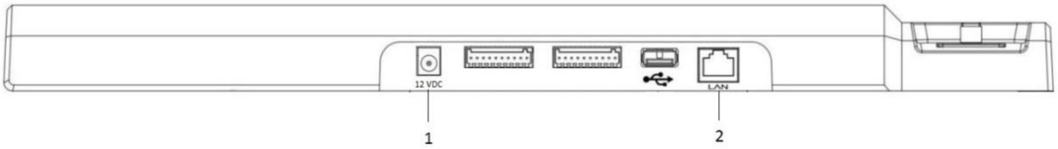
Front Panel

Component Description

No.	Name	Description
1	Handset	For panic /consulting call
2	Screen	7 inch color TFT LCD
3	Keypad	Dialing keypad, call the device by entering device ID
4	Power Indicator	Solid blue when the master station is powered on
5	Alarm Indicator	Flashing blue when alarm is triggered or the master station is answering panic call.
6	Exception Indicator	Flashing red when exception occurs.
7	Broadcast button	Starting/Ending broadcast
8	Call/Ring-off Button	Calling alarm device or ringing-off
9	Hands-free/Answer Button	Entering hands-free mode or answering panic/consulting call

Rear Panel

The rear panel of master station is shown below.



Rear Panel

Rear Panel Component Description

No.	Component	Description
1	Power Interface	Connect to 12 VDC power supply
2	Network Interface	Connect wired network

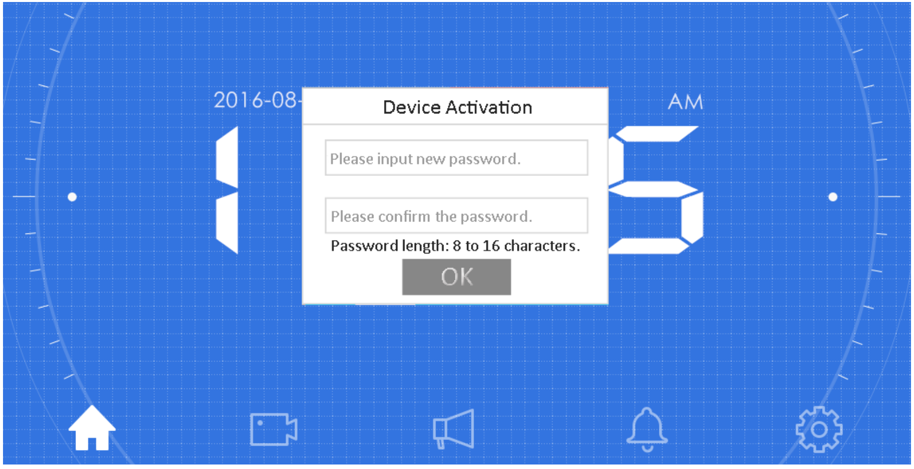
Chapter 2 Activation

You are required to activate the control panel first before you can use the control panel.
Local activation, activation via SADP, and activation via client software are supported.

2.1 Activating Locally

You can activate the device when you access the device for the first time.

Step 1 Power the master station on to enter the activation page.



Device Activation

Please input new password.

Please confirm the password.

Password length: 8 to 16 characters.

Step 2 Create a password and input the password in the password field, and confirm the 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.*

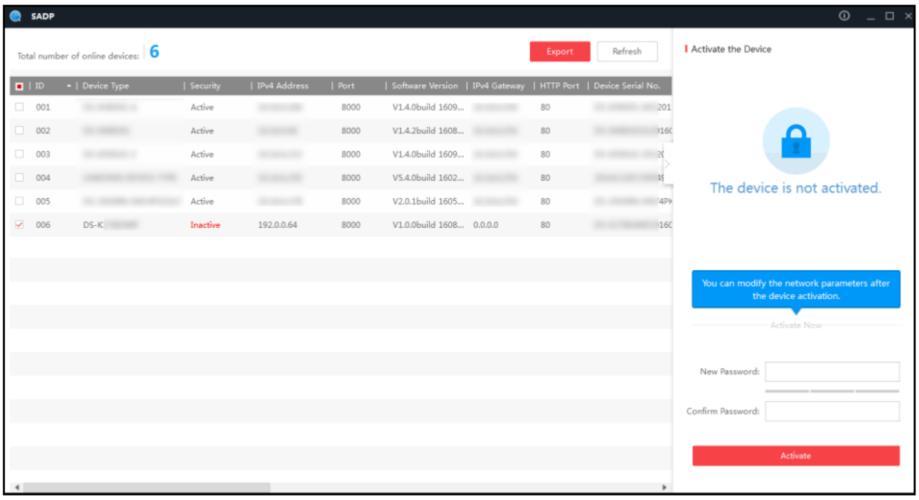
2.2 Activating via SADP Software

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.



SADP

Total number of online devices: 6

☐	ID	Device Type	Security	IPv4 Address	Port	Software Version	IPv4 Gateway	HTTP Port	Device Serial No.
☐	001	[redacted]	Active	[redacted]	8000	V1.4.0build 1609...	[redacted]	80	[redacted]
☐	002	[redacted]	Active	[redacted]	8000	V1.4.2build 1608...	[redacted]	80	[redacted]
☐	003	[redacted]	Active	[redacted]	8000	V1.4.0build 1609...	[redacted]	80	[redacted]
☐	004	[redacted]	Active	[redacted]	8000	V5.4.0build 1602...	[redacted]	80	[redacted]
☐	005	[redacted]	Active	[redacted]	8000	V2.0.1build 1605...	[redacted]	80	[redacted]
☑	006	DS-K[redacted]	Inactive	192.0.0.64	8000	V1.0.0build 1608...	0.0.0.0	80	[redacted]

Activate the Device

The device is not activated.

You can modify the network parameters after the device activation.

Activate Now

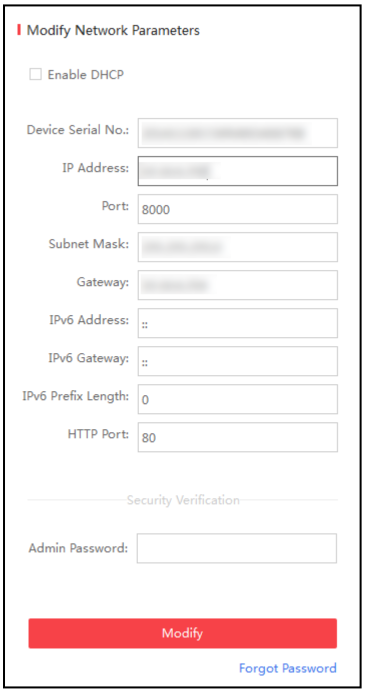
New Password:

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 **Activate** to activate the device.
5. Check the activated device. You can change the device IP address to the same network segment 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.: [redacted]

IP Address: [redacted]

Port: 8000

Subnet Mask: [redacted]

Gateway: [redacted]

IPv6 Address: ::

IPv6 Gateway: ::

IPv6 Prefix Length: 0

HTTP Port: 80

Security Verification

Admin Password:

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

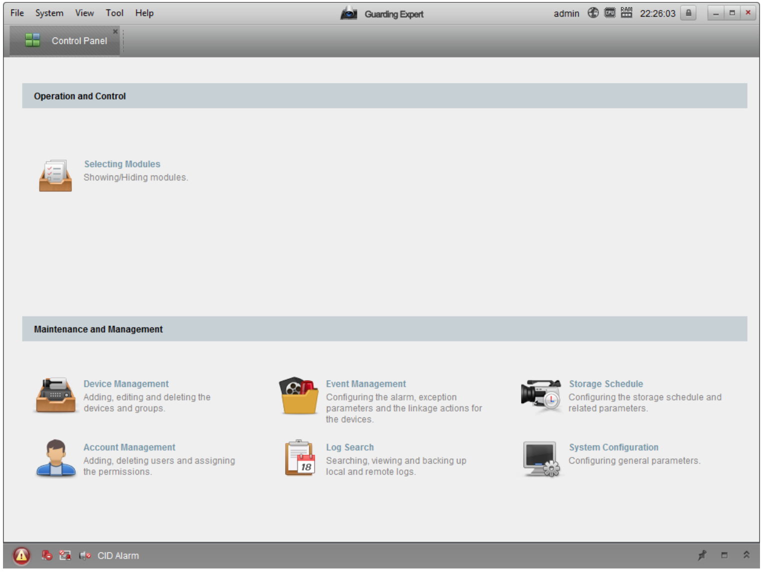
2.3 Activating via Client Software

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

Selecting Modules
Showing/Hiding modules.

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.

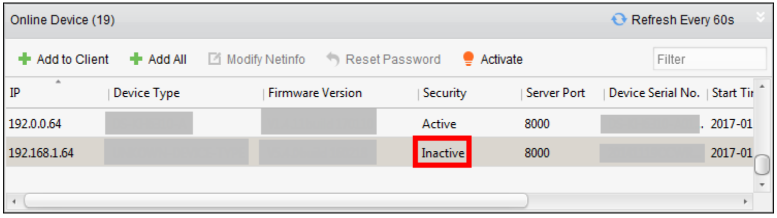
Storage Schedule
Configuring the storage schedule and related parameters.

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.

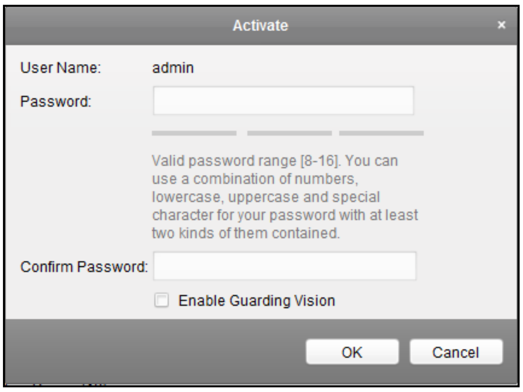
2. Click the **Device Management** to enter the Device Management interface.
3. Check the device status from the device list, and select an inactive device.



IP	Device Type	Firmware Version	Security	Server Port	Device Serial No.	Start Tir
192.0.0.64	[redacted]	[redacted]	Active	8000	[redacted]	2017-01
192.168.1.64	[redacted]	[redacted]	Inactive	8000	[redacted]	2017-01

4. Click the **Activate** button to pop up the Activation interface.
5. In the pop-up window, create a 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.*



User Name: admin

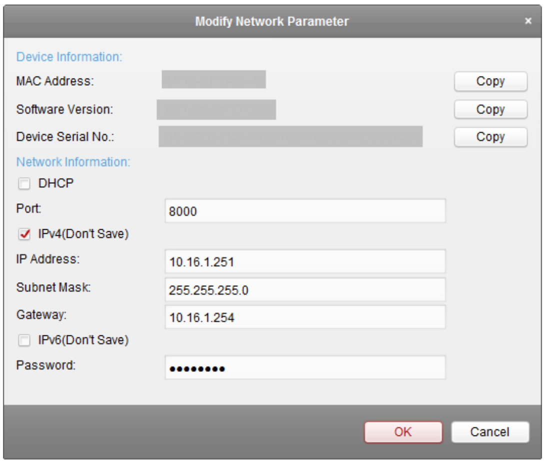
Password:

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:

□ Enable Guarding Vision

6. Click **OK** button to activate
7. Click the **Modify Netinfor** button to pop up the Network Parameter Modification interface.



Modify Network Parameter

Device Information:

MAC Address: [redacted]

Software Version: [redacted]

Device Serial No.: [redacted]

Network Information:

□ DHCP

Port: 8000

☑ IPv4(Don't Save)

IP Address: 10.16.1.251

Subnet Mask: 255.255.255.0

Gateway: 10.16.1.254

□ IPv6(Don't Save)

Password: ••••••••

8. Change the device IP address to the same network segment with your computer by either modifying the IP address manually. Input the password and click the **OK** button to save the settings.

Chapter 3 Local Configuration

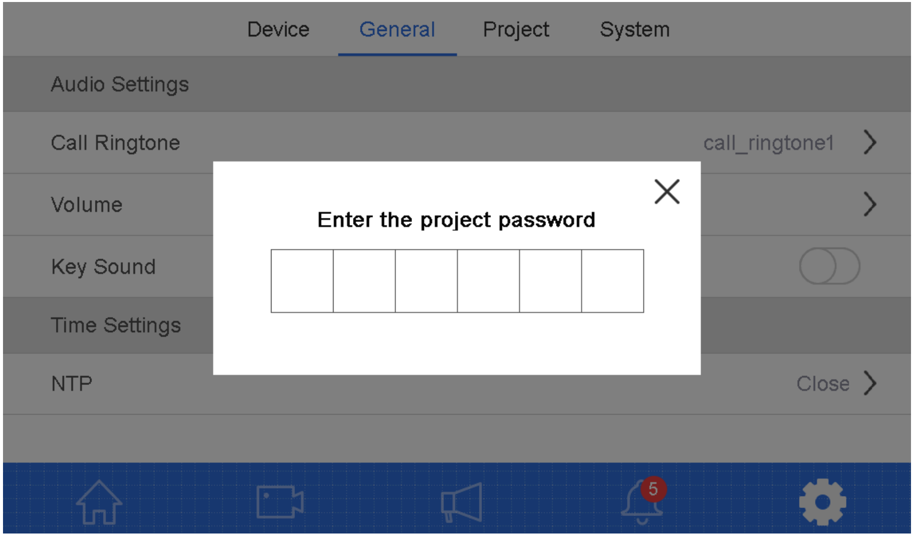
You are required to activate the control panel first before you can use the control panel. Refer to Chapter 3 Activation for details.

3.1 Network Settings

You are required to edit the network parameters after the device being activated.

Step 1 Press ⚙ on the main page, and press **Project**.

Step 2 Enter the project password.



Device General Project System

Audio Settings

Call Ringtone call_ringtone1

Volume

Key Sound

Time Settings

NTP Close

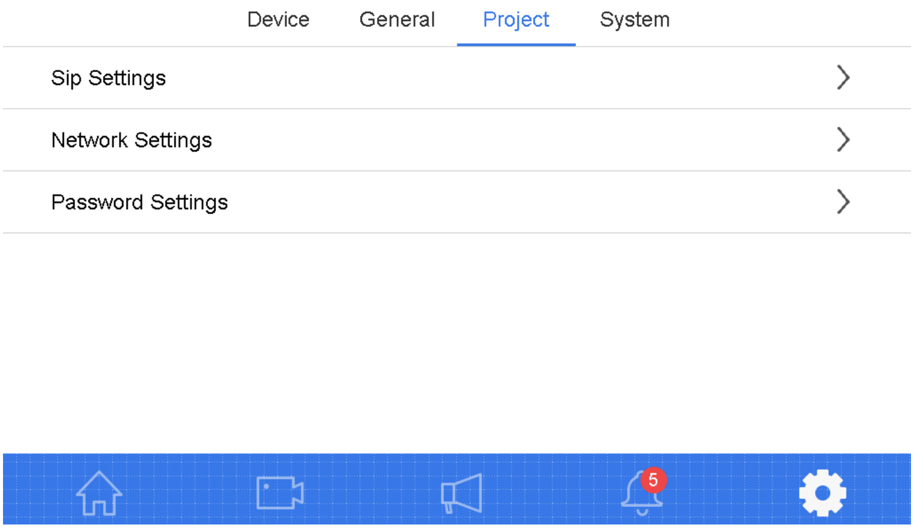
Enter the project password

NOTE

- You need to enter the project password for configuring for some of the local configurations. The default project password is 888999.
- You can change the project password on **Project**-**Password** Settings.

DANGER

The default password is only for the first login. You are required to change your password immediately after login.



Device General Project System

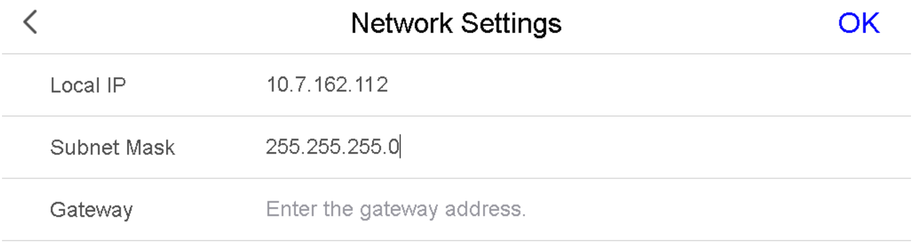
Sip Settings

Network Settings

Password Settings

Step 3 Press **Network Settings**, and edit the device IP address, gateway, and mask on the page.

Step 4 Press OK to conform the settings.



Local IP 10.7.162.112

Subnet Mask 255.255.255.0

Gateway Enter the gateway address.

NOTE

The default IP address for the master station is 192.0.0.64.

3.2 SIP and Master Station ID Settings

Configure the SIP server to achieve normal communication between device and master station or between master stations. Set the master station ID, and you can call the master station by entering the set ID.

Steps:

Step 1 Press ⚙ on the main page, and press **Project**.

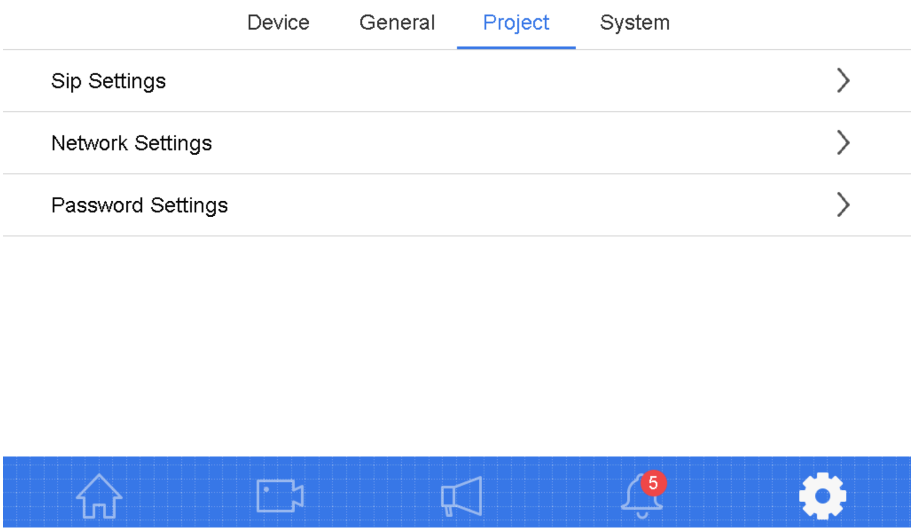
Step 2 Enter the project password.

NOTE

- You need to enter the project password for configuring for some of the local configurations. The default project password is 888999.
- You can change the project password on **Project**-**Password** Settings.

DANGER

The default password is only for the first login. You are required to change your password immediately after login.



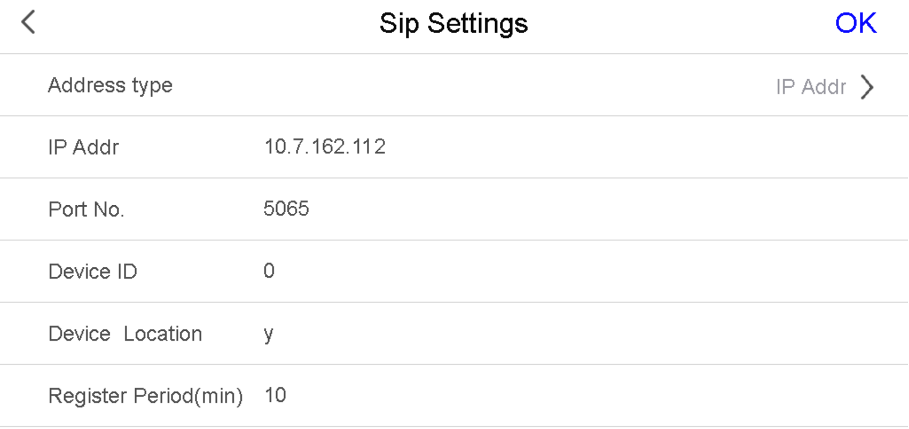
Step 3 Press **SIP Settings** to enter the configuration page.

Step 4 Edit the SIP parameters, such as SIP server IP address, port No., master station ID, location, and registration period.

NOTE

- SIP server IP address: the master station can be used as SIP server. The IP address of a SIP server can be the IP address of master station.
- Default SIP server port No.: 5065

- Registration Period: Time interval of device registering to the SIP server continuously.



Sip Settings

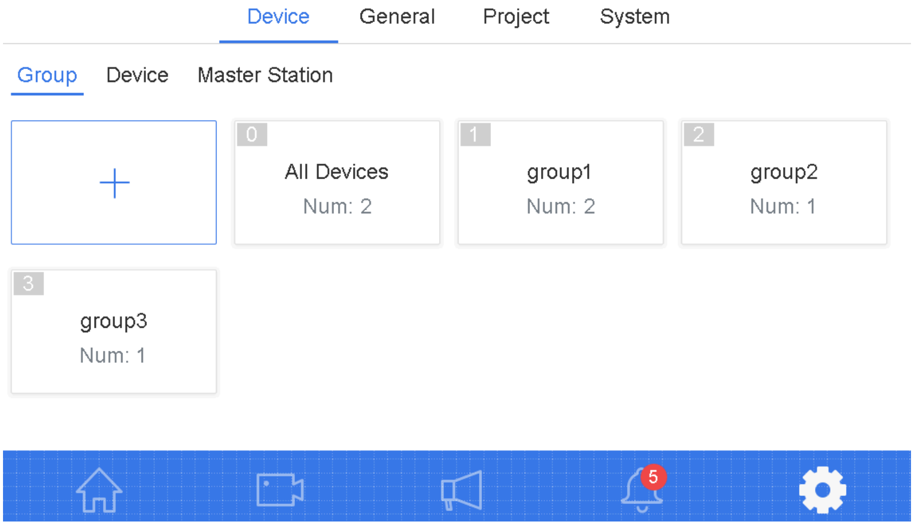
Address type	IP Addr
IP Addr	10.7.162.112
Port No.	5065
Device ID	0
Device Location	y
Register Period(min)	10

3.3 Device Management

You can add security control device and master station to a master station.

I. Security Control Device Management

Press **Device Management**–**Device** to view the devices connected to the master station.
Press **Group** to enter the device group management page. You can classify the connected device by grouping and manage the added groups.
You can add security control device to the master station via client software.
Add the IP address of the master station to the security control device on the **Remote Configuration** interface. The master station displays the related security control device on the **Device** page.



II. Master station management

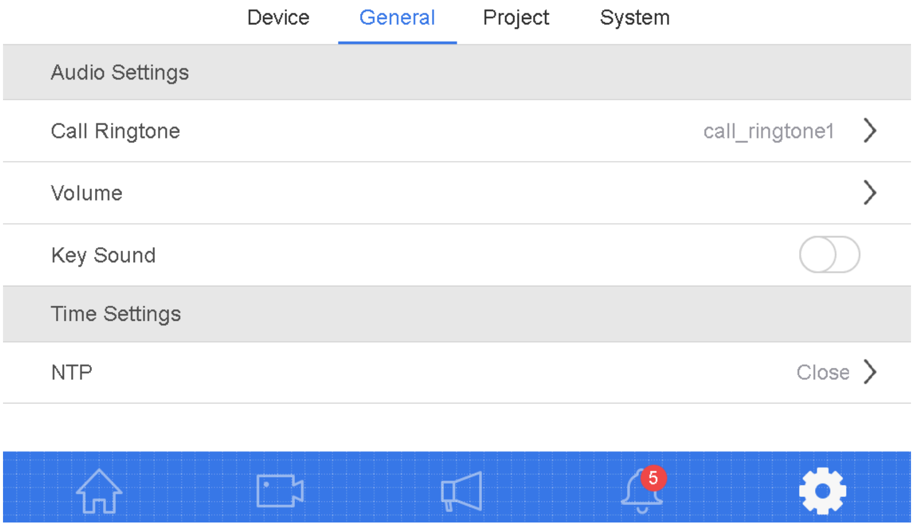
Press **Device Management**–**Master Station** to view other connected master stations.
Press **Group** to enter the device group management page. You can classify the connected master stations by grouping and manage the added groups.

You can add a master station to another master station via client software.
Add the IP address of the master station to another on the **Remote Configuration** interface. The master station displays the related master station on the **Device** page.

3.4 Audio Settings

You can set the call ringtone, volume, and key tone on the audio settings page.

Step 1 Press General to enter general settings page.



Device | General | Project | System

Audio Settings

Call Ringtone call_ringtone1 >

Volume >

Key Sound ○

Time Settings

NTP Close >

Step 2 Press and select the Call Ringtone

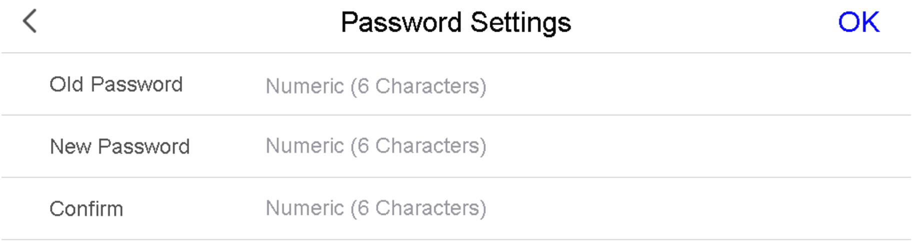
Step 3 Press Volume to set the volume of microphone and loudspeaker.

Step 4 Swipe the block ● to enable/disable the master station key tone.

3.5 Password Settings

The project password is for project management such as network configuration, station ID settings and location information. You can set the project password for the master station

Step 1 Press Project-Password Settings to enter the interface.



< Password Settings OK

Old Password Numeric (6 Characters)

New Password Numeric (6 Characters)

Confirm Numeric (6 Characters)

Step 2 Enter the old password and new password.

Step 3 Confirm the new password and press OK.

NOTE

The default project password is 888999.

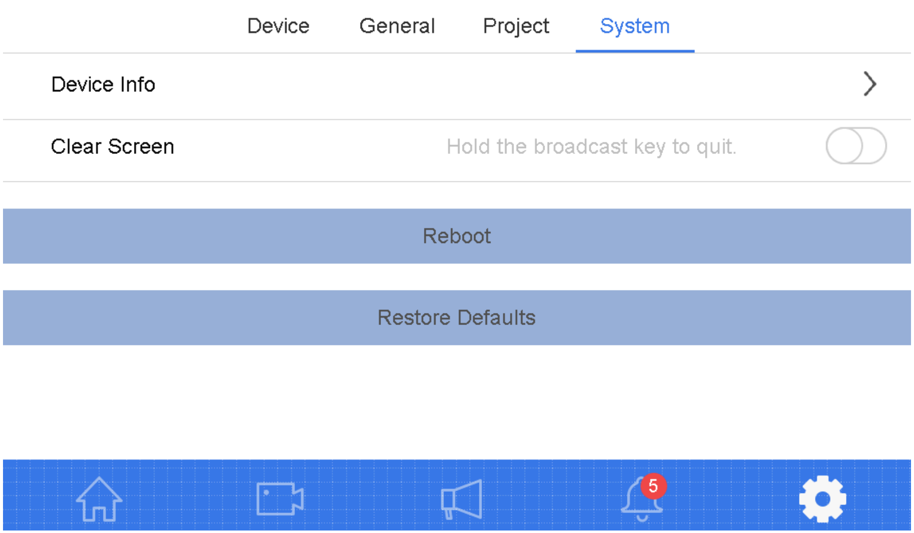
DANGER

The default password is only for the first login. You are required to change your password immediately after login.

3.6 System Maintenance

You can enter the screen clearing mode, view the station information, reboot the device, and restore default parameters.

Step 1 Press System to enter the system maintenance page.



Step 2 Swipe the ● block to enter screen clearing mode.
Hold the Broadcast button to exit the mode.

NOTE

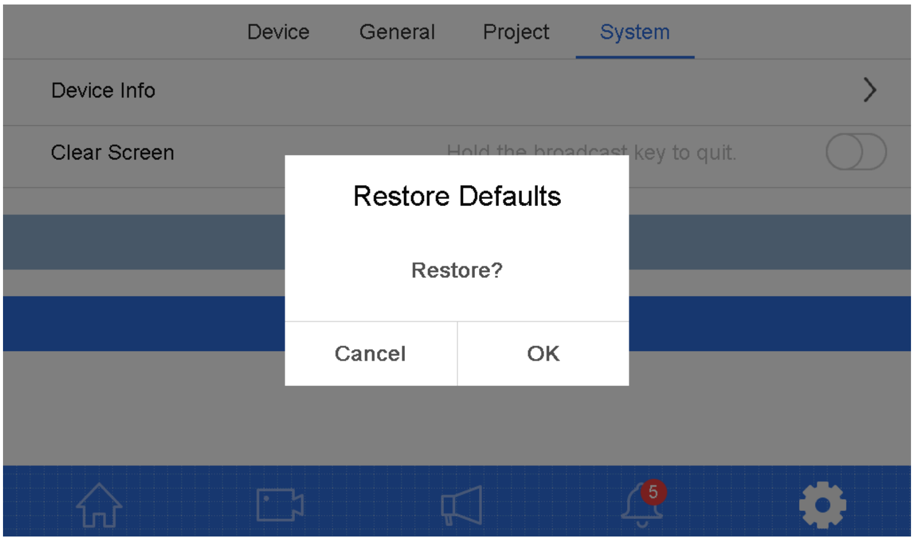
The device will exit the screen clearing mode automatically 10 minutes after entering the mode.

Step 3 Press **Device Restart** to Reboot the device.

3.7 Restore Defaut Settings

Steps:

Step 1 Press System-Default Settings to enter the **Restore Default Settings** page.
Step 2 Press **Restore Default Parameters** to get the pop-up window.
Step 3 Press **OK** to start.



Restore Defaults

Restore?

Cancel OK

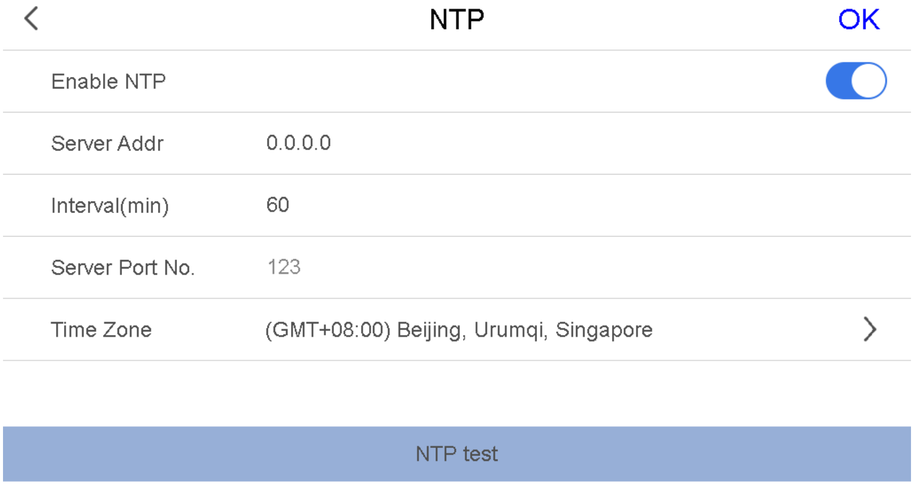
NOTE

- Network parameters and user information cannot be restored through this operation.
- You need to reboot the device after restoring.

3.8 NTP

Steps:

Step 1 Press **General**-**Time Settings**-**NTP** to enter the NTP Interface.



Enable NTP

Server Addr 0.0.0.0

Interval(min) 60

Server Port No. 123

Time Zone (GMT+08:00) Beijing, Urumqi, Singapore

Step 2 Swipe the block to enable/disable NTP function.

Step 3 Enter NTP parameters such as server IP address, Port No., and time zone.

NOTE

The default port No. is 123.

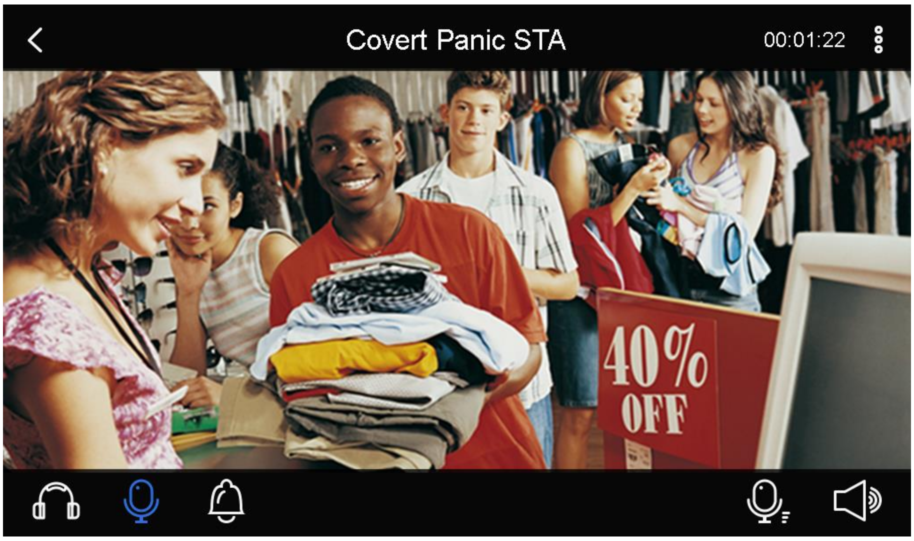
Chapter 4 Local Operation

Calling Security Control Device

Enter the ID of security control device or master station on the calling page of master station. Press 🎙 to call a device.

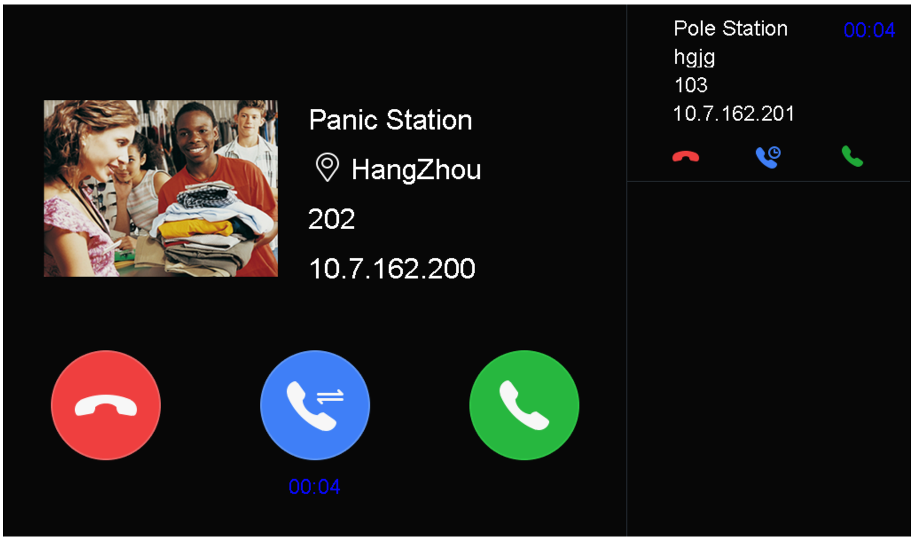
NOTE

The Max. length of ID is 6 characters.



Receiving Panic Help or Consultation

Master station can handle the calls of up to 4 devices at the same time.


Pole Station 00:04
hgjg
103
10.7.162.201

Panic Station
HangZhou
202
10.7.162.200

00:04

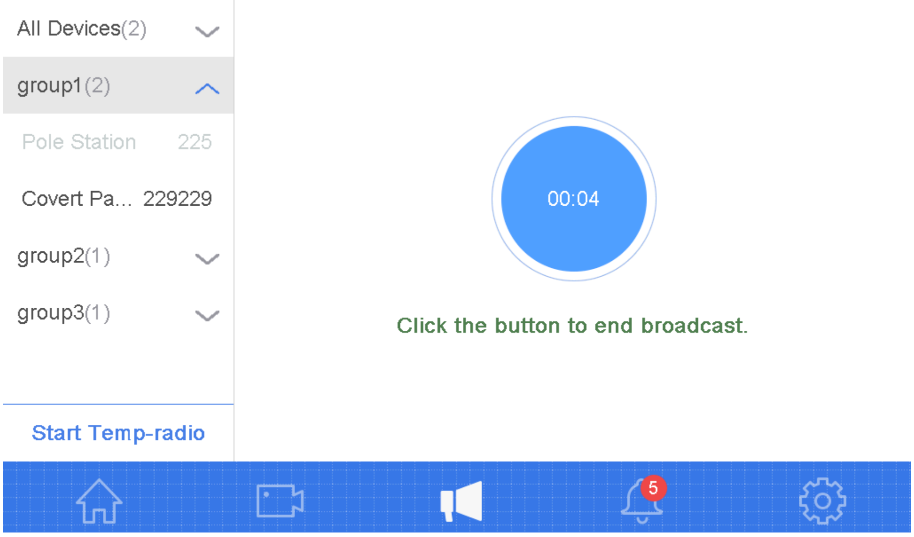
Press 📞 to answer the call.

Press 📞 to hang up the call.

Press 📞 to forward the call.

Broadcast

Press 📢 on the home page of the master station to enter the broadcast page.
Select a group, and press the broadcast button on the right side to do broadcast for all devices in this group.
Press **Start Temp-radio** to start broadcast to the selected devices.

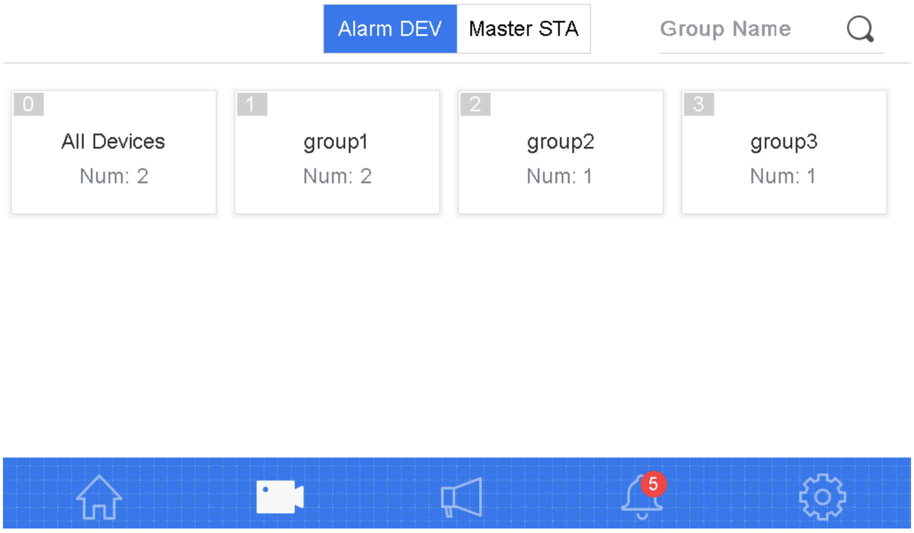


Click the button to end broadcast.

Monitoring Security Control Device

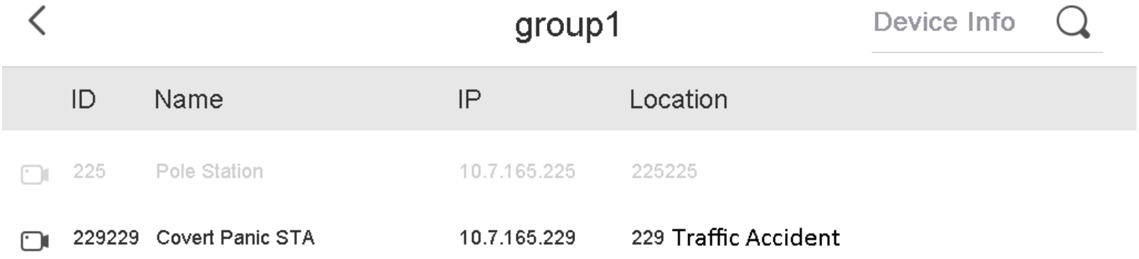
You can view alarm video on the connected security control device.

Step 1 Press 📹 on the home page to enter the group page.



0	All Devices	Num: 2
1	group1	Num: 2
2	group2	Num: 1
3	group3	Num: 1

Step 2 Select a group, and enter the device list in the group.



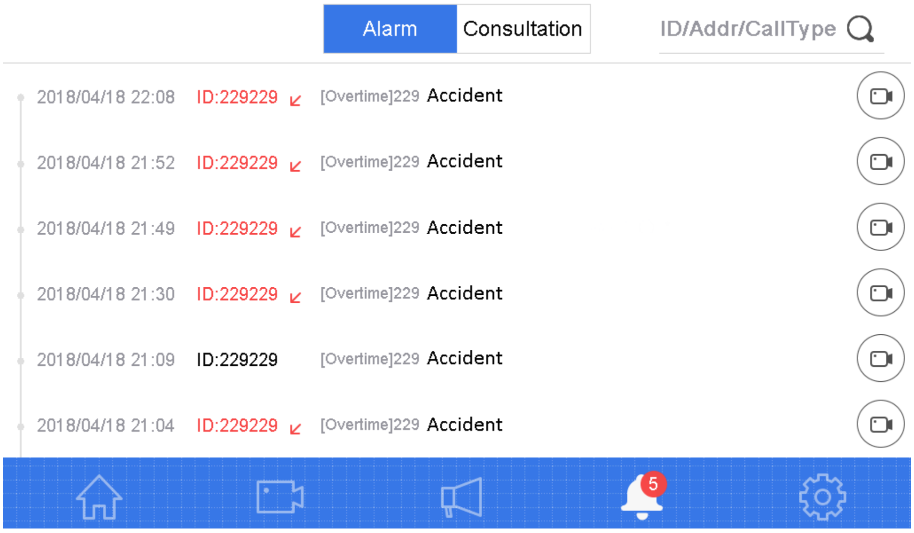
ID	Name	IP	Location
225	Pole Station	10.7.165.225	225225
229229	Covert Panic STA	10.7.165.229	229 Traffic Accident

Step 3 Select a device to enter the video monitoring page.

Record Query

You can search for alarm record and consultation records.

Press 🔔 to enter the records query page.



2018/04/18 22:08	ID:229229 ↙	[Overtime]229 Accident
2018/04/18 21:52	ID:229229 ↙	[Overtime]229 Accident
2018/04/18 21:49	ID:229229 ↙	[Overtime]229 Accident
2018/04/18 21:30	ID:229229 ↙	[Overtime]229 Accident
2018/04/18 21:09	ID:229229	[Overtime]229 Accident
2018/04/18 21:04	ID:229229 ↙	[Overtime]229 Accident

Chapter 5 Remote Configuration

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: 192.0.0.64
- Port No.: 8000
- Admin User Name: admin

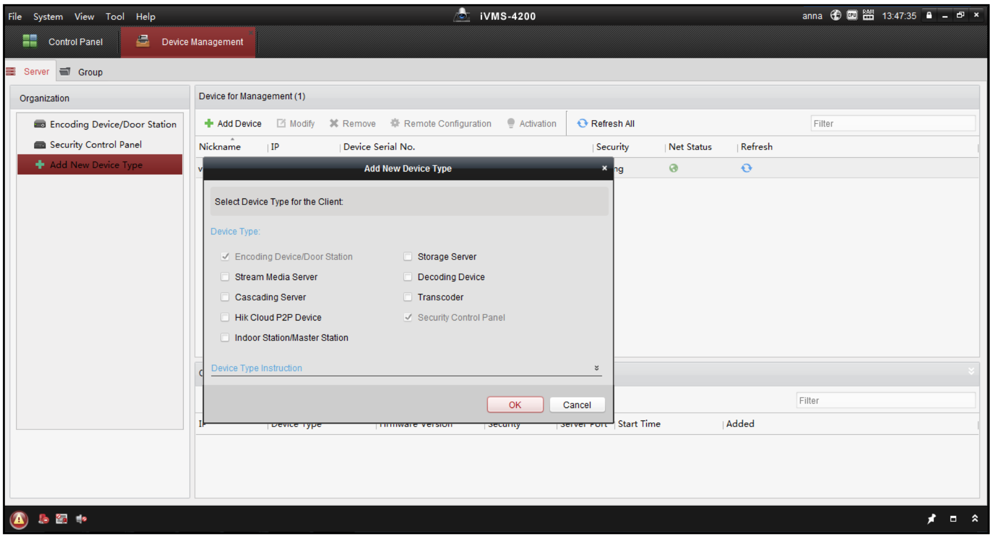
5.1 Device Management

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.

5.1.1 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.

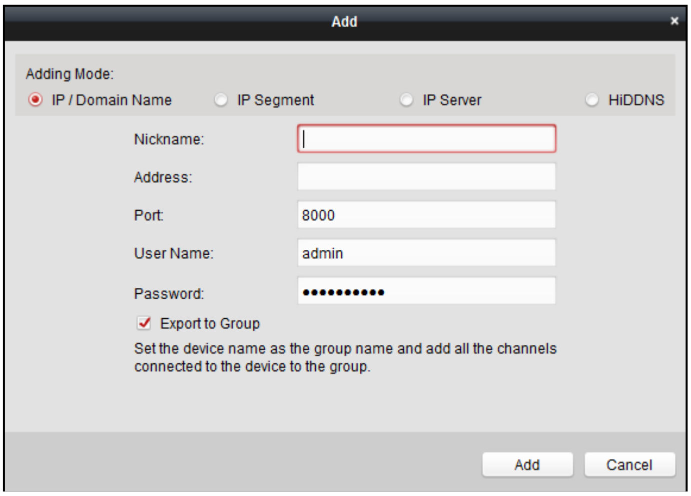


Select Device Type for the Client:

Device Type:

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

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.

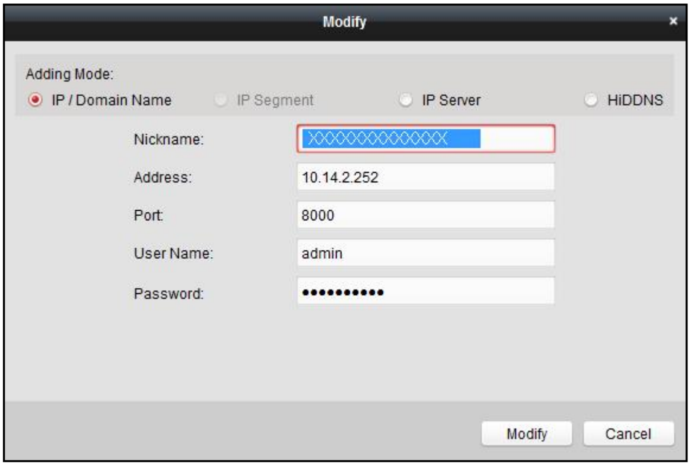
5.1.2 Edit a Device

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: ••••••••••

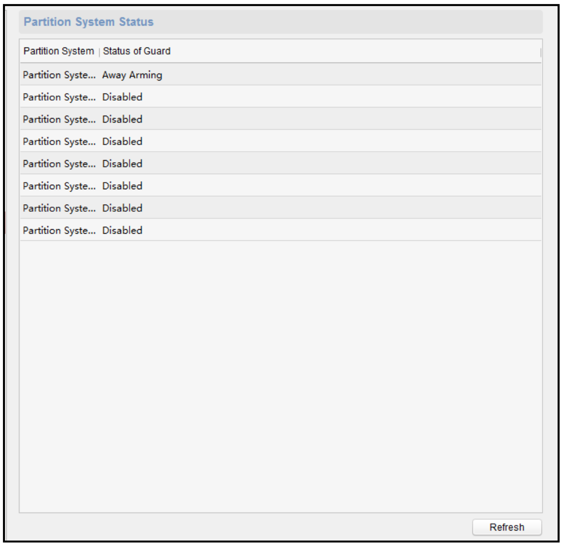
3. Enter the required nick name, address, and port number and then enter the admin username and password.
4. Click **Modify** to save the changes.

5.1.3 Delete a Device

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

5.1.4 Status

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



Partition System Status

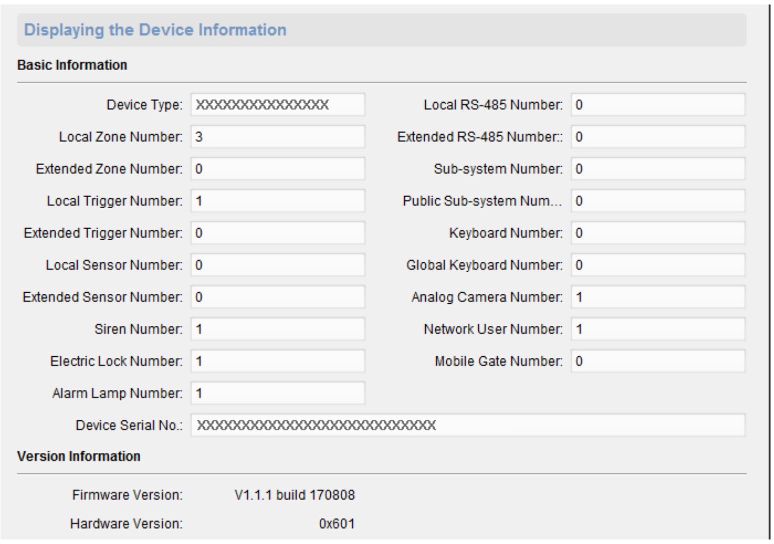
Partition System	Status of Guard
Partition Syste...	Away Arming
Partition Syste...	Disabled
Partition Syste...	Disabled
Partition Syste...	Disabled
Partition Syste...	Disabled
Partition Syste...	Disabled
Partition Syste...	Disabled
Partition Syste...	Disabled

5.2 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:	XXXXXXXXXXXXXXXX	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.:	XXXXXXXXXXXXXXXXXXXXXXXXXXXX		

Version Information

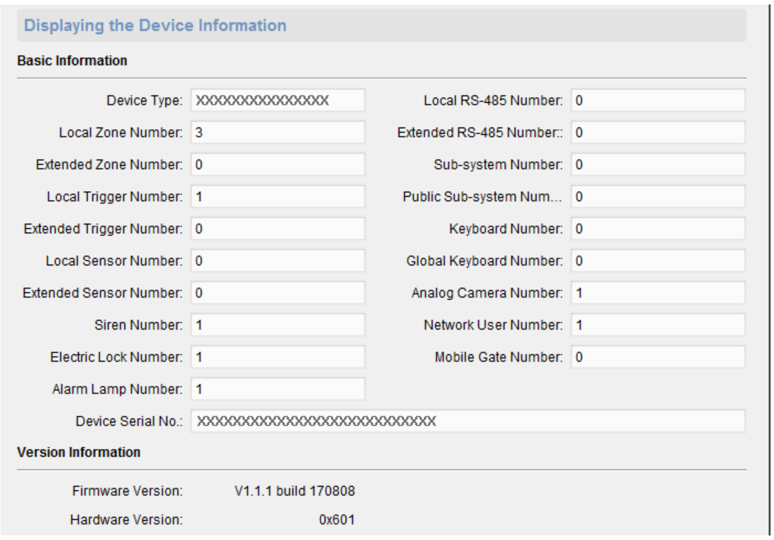
Firmware Version: V1.1.1 build 170808

Hardware Version: 0x601

5.2.1 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:	XXXXXXXXXXXXXXX	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.:	XXXXXXXXXXXXXXXXXXXXXXXXXXX		

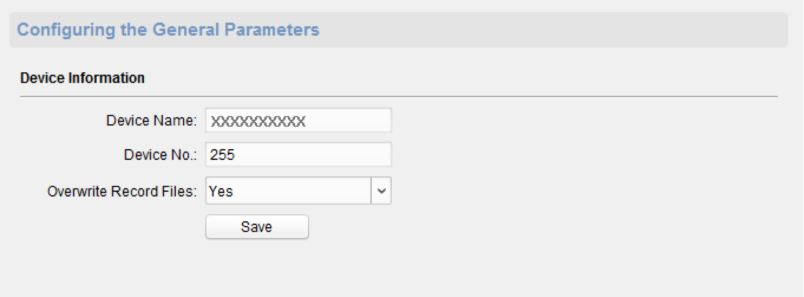
Version Information

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: XXXXXXXXXX

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.

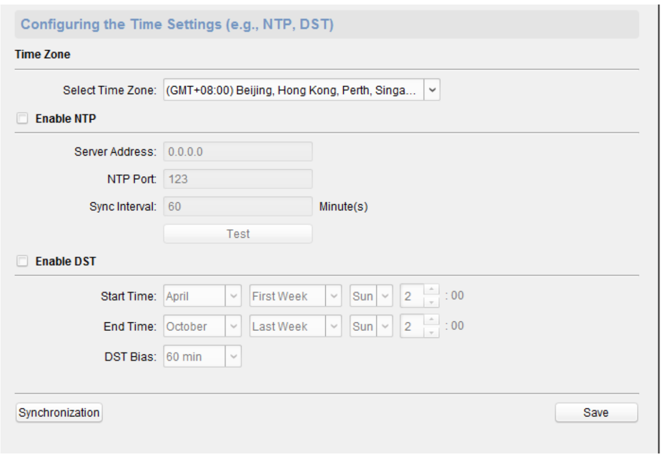
Timing Settings

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

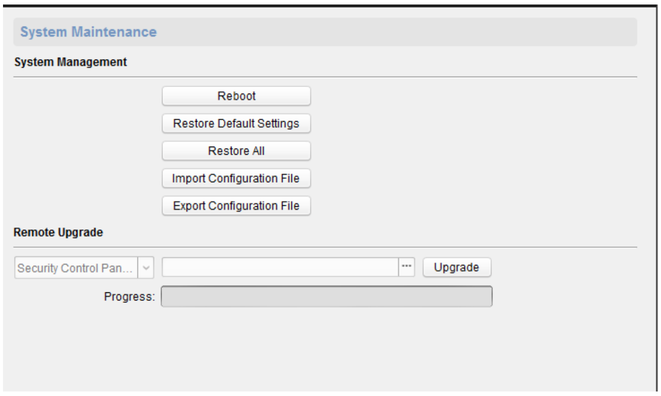
End Time: October Last Week Sun 2 : 00

DST Bias: 60 min

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

System Maintenance

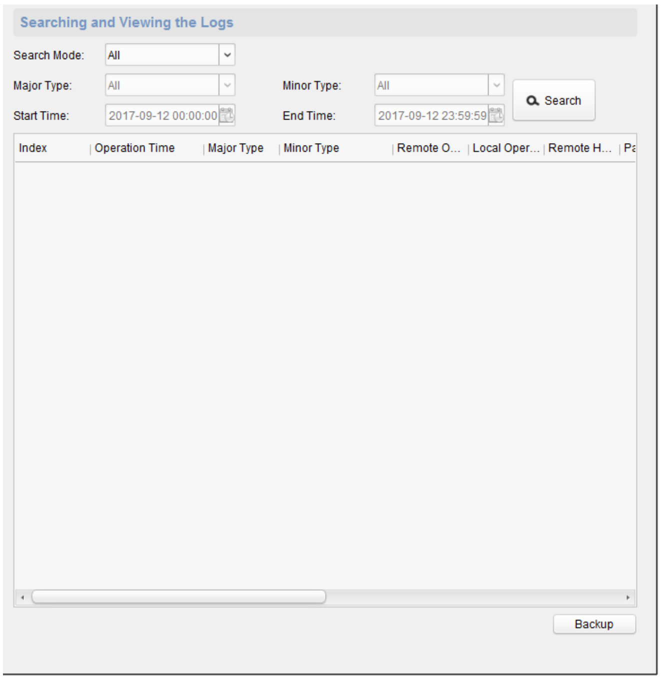
The device supports system maintenance remotely. Click **Remote Configuration > System > System Maintenance** to enter the interface.



- **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.



Searching and Viewing the Logs

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

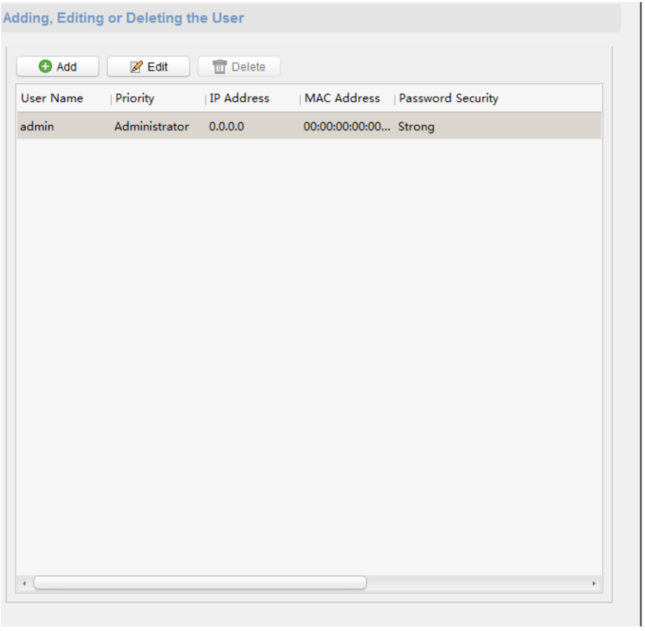
Purpose:

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

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

Steps:

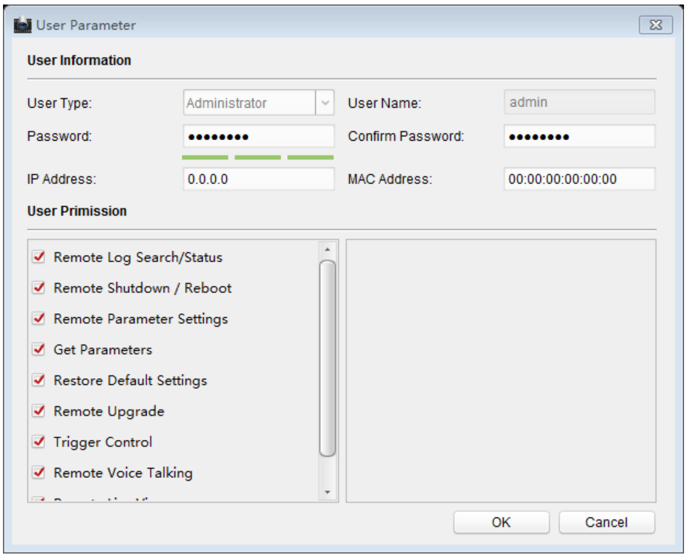
1. Click **Remote Configuration > System > User** to enter the user configuration interface.



Adding, Editing or Deleting the User

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 Parameter

User Information

User Type: Administrator | User Name: admin

Password: •••••••• | Confirm Password: ••••••••

IP Address: 0.0.0.0 | MAC Address: 00:00:00:00:00:00

User Primission

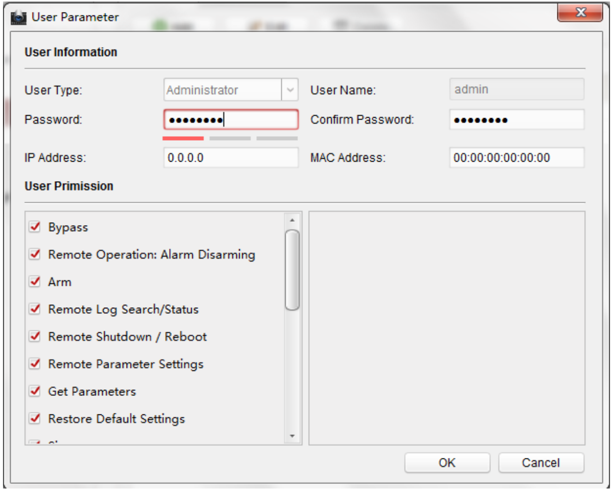
- ☑ Remote Log Search/Status
- ☑ Remote Shutdown / Reboot
- ☑ Remote Parameter Settings
- ☑ Get Parameters
- ☑ Restore Default Settings
- ☑ Remote Upgrade
- ☑ Trigger Control
- ☑ Remote Voice Talking

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 Parameter

User Information

User Type: Administrator | User Name: admin

Password: •••••••• | Confirm Password: ••••••••

IP Address: 0.0.0.0 | MAC Address: 00:00:00:00:00:00

User Primission

- ☑ 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.

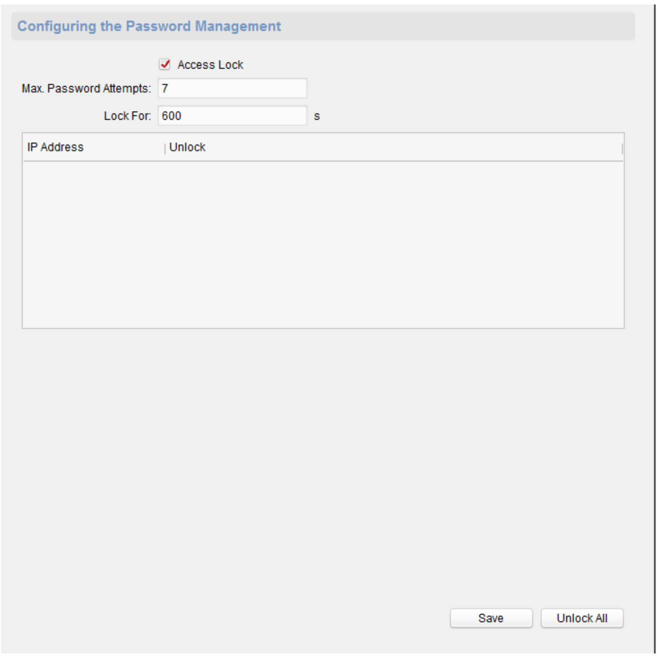
■ **Delete a User**

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

5.2.2 Network Settings

Purpose:

You can edit the general network parameters in this section.

General Network Parameters Settings

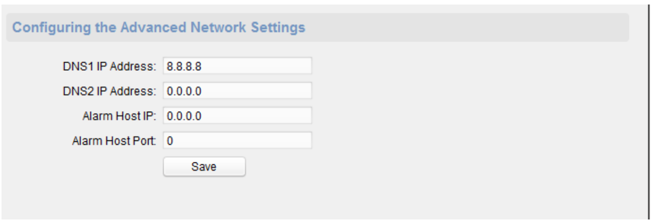
Steps:

1. Click **Remote Configuration > Network > General** to enter the general network configuration interface.
2. Configure the network parameters.
3. Click **Save** to save the above 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

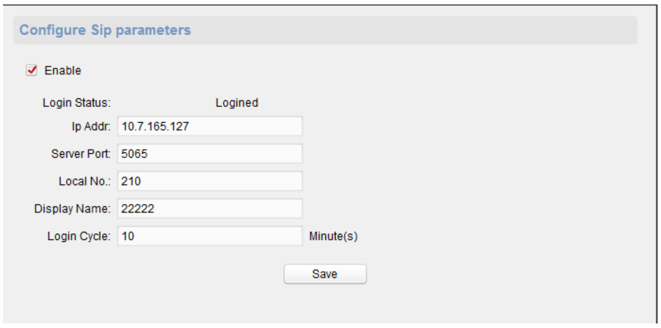
Alarm Host Port: 0

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.

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.

5.2.3 Image Settings

Video& Audio Settings

Select the audio encoding type, click OK to save the settings.

Appendix A **Installation Matters and Attention**

To decrease the impact made by echo, the distance between the master station and panic alarm station is recommended to be no less than 10m.

Appendix B **Wiring Standard**

Table B-1 Wiring Standard

Cable	Standard
Master Station Power Cable	RVV 2*1.0
Master Station Network Cable	Cat5e

0100001080420

UD09930B

See Far, Go Further