HIKVISION

Panic Alarm Station

User Manual

Legal Information

About this Manual

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 of this Manual at the Hikvision website (https://www.hikvision.com/).

Please use this Manual with the guidance and assistance of professionals trained in supporting the Product.

Trademarks

HIKVISION and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions.

Other trademarks and logos mentioned are the properties of their respective owners.

Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS MANUAL AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED "AS IS" AND "WITH ALL FAULTS AND ERRORS". HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION 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, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.

YOU ACKNOWLEDGE THAT THE NATURE OF THE INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INFECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.

YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ILLEGAL HUNTING ANIMALS, INVASION OF PRIVACY OR ANY OTHER PURPOSE WHICH IS ILLEGAL OR DETRIMENTAL TO THE PUBLIC INTEREST. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.

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-PEA102S DS-PEA102R DS-PEA102Y

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 -25℃ to 55℃.
- 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.

Serial Port Accessing

While accessing with serial port, enter 'debug' and then the system will print a string. Enter the string in the URL of http://psh.hikvision.com.cn:8080/sso/home/page to get the terminal control command. Insert the command to access to the device serial port.

Table of Content

Chapter 1 Overview

1.1 Description

DS-PEA102 series of panic alarm station supports two-way audio communication, and panic alarm, which realize alarm aid in emergency.

The product is applied in school, hospital, metro, scenic area, prison, etc.

1.2 Key Features

- Network adaptive and video and audio adaptive
- Built-in omnidirectional microphone
- Supports two-way audio communication and configuration
- Supports listening and broadcast
- Multiple network protocols including TCP/IP and RTSP
- Supports Standard SIP, ISUP, and HIK-Connect
- Protection level: IP54
- Anti-Explosion level: IK08
- Supports external siren and strobe light

Chapter 2 Activation

In order to protect personal security and privacy and improve the network security level, you should activate the device the first time you connect the device to a network.

2.1 Activate via SADP

SADP is a tool to detect, activate and modify the IP address of the device over the LAN.

Before You Start

- Get the SADP software from the supplied disk or the official website ***http://www.hikvision.com/en/***, and install the SADP according to the prompts.
- The device and the PC that runs the SADP tool should be within the same subnet.

The following steps show how to activate a device and modify its IP address. For batch activation and IP addresses modification, refer to *User Manual of SADP* for details.

Steps

1. Run the SADP software and search the online devices.

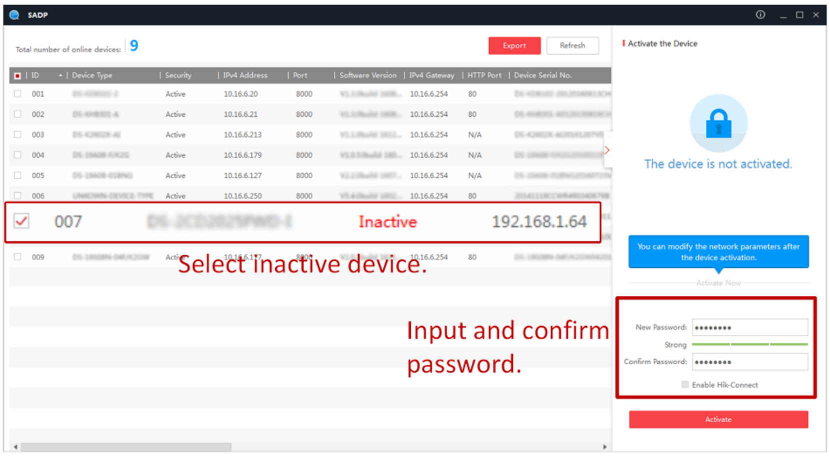
2. Find and select your device in online device list.

3. Input new password (admin password) and confirm the password.

Caution

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 start activation.



Total number of online devices: 9

☐	ID	Device Type	Security	IPv4 Address	Port	Software Version	IPv4 Gateway	HTTP Port	Device Serial No.
☐	001	[illegible]	Active	10.16.6.20	8000	[illegible]	10.16.6.254	80	[illegible]
☐	002	[illegible]	Active	10.16.6.21	8000	[illegible]	10.16.6.254	80	[illegible]
☐	003	[illegible]	Active	10.16.6.213	8000	[illegible]	10.16.6.254	N/A	[illegible]
☐	004	[illegible]	Active	10.16.6.179	8000	[illegible]	10.16.6.254	N/A	[illegible]
☐	005	[illegible]	Active	10.16.6.127	8000	[illegible]	10.16.6.254	N/A	[illegible]
☐	006	[illegible]	Active	10.16.6.250	8000	[illegible]	10.16.6.254	80	[illegible]
☑	007	[illegible]	Inactive	192.168.1.64					
☐	009	[illegible]	Active	10.16.6.177	8000	[illegible]	10.16.6.254	80	[illegible]

Select inactive device.

Activate the Device

The device is not activated.

You can modify the network parameters after the device activation.

Activate Now

New Password: ••••••••

Strong

Confirm Password: ••••••••

☐ Enable Hik-Connect

Activate

Input and confirm password.

Figure 2-1 Activate via SADP

Status of the device becomes **Active** after successful activation.

5. Modify IP address of the device.

    1) Select the device.
    2) Change the device IP address to the same subnet as your computer by either modifying the IP address manually or checking **Enable DHCP**.
    3) Input the admin password and click **Modify** to activate your IP address modification.

2.2 Activate Device via Client Software

Before You Start

- Get the iVMS-4200 client software from the supplied disk or the official website ***http://www.hikvision.com/en/***. Install the software by following the prompts.
- The device and the PC that runs the software should be in the same subnet.

Steps

1. Run the client software.

2. Enter **Device Management** → **Device** in the **Maintenance and Management** list.

3. Click **Online Device**.

4. Check the device status from the online device list, and select an inactive device.

5. Click **Activate**.

6. Create and confirm the admin password of the device.

⚠ **Caution**

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.

7. Click **OK** to start activation.

Device status will change to **Active** after successful activation.

8. Edit IP address of the device.

    1) Select a device and click 🌐 on the online device list.
    2) Change the device IP address to the same subnet with your computer.
    3) Enter the admin password of the device and click **OK** to complete modification.

9. Optional: Check the device on the online device list and click **Add** to add the device to the device list.

Chapter 3 Remote Settings

In the client software, go to **Device Management**, click and select the device in the device list, and click ⚙ to enter the **Remote Configuration** page.

Note

- The device should be activated the first time it is used to log in and use properly. See ***Activation*** to activate the device.
- You need to add the device to the client software before configure it. See ***Add Device via Client Software***.
- Get the client software from the technical support, and install the software according to the prompts.

3.1 Device Management

3.1.1 Add Device to the Client Software

Before You Start

Activate the device and ensure that the device is on the same subnet as the PC.

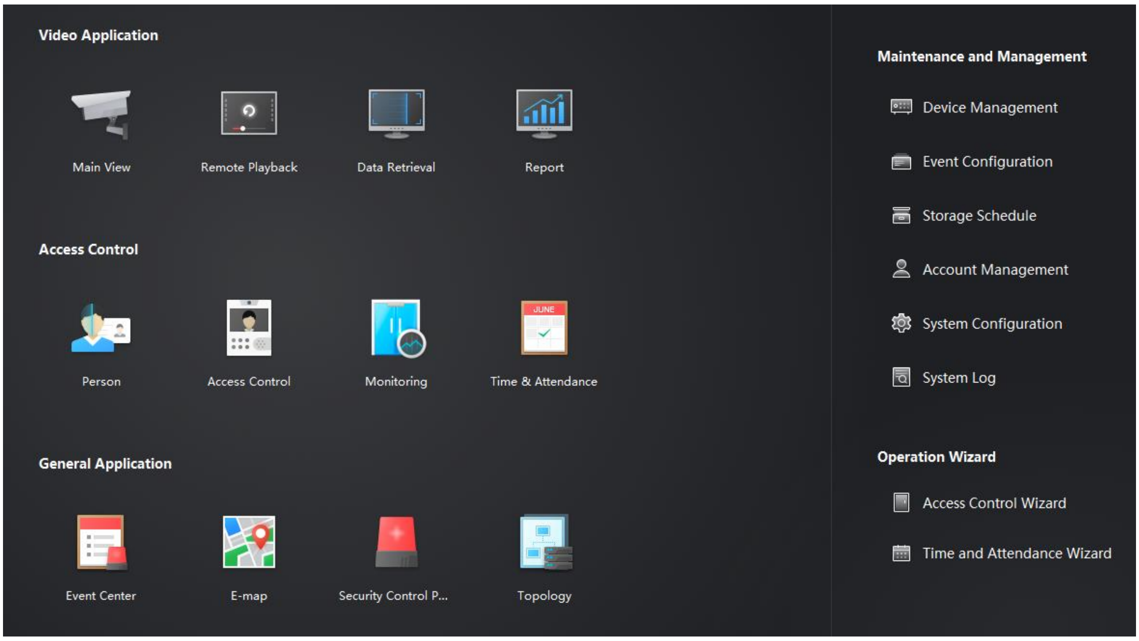


Figure 3-1 Client Software Main Page

In the client software, go to **Device Management** → **Device** on the **Maintenance and Management** list. You can add devices to client software by several methods on the device management page. The following describes how to add devices through IP/Domain Name. For more information, see *iVMS-4200 Client Software User Manual*.

Steps

1. On the **Device** page, click **Add**.

2. Select **IP/Domain** as the adding mode, edit the device information, including **Name**, **Address**, **Port**, **User Name**, and **Password**.

3. Click **Add** to add the device.

3.1.2 Edit Network Parameters

Edit the device network parameters so that the device IP address is in the same subnet as the computer IP address.

You can edit the network parameters through the SADP software, or the client software. The SADP software is taken as an example for explanation.

Steps

1. Run the SADP software, check the activated device, and edit the **IP Address**, **Subnet Mask**, Gateway and other parameters in the **Modify Network Parameters** list on the right.

Note

If check **Enable DHCP**, the device can automatically obtain network parameters.

2. Enter the activation password, click **Modify**, and the prompt ***Modify parameters is successful*** indicate that the settings take effect.

3.2 Network Configuration

3.2.1 Set General Network Parameters

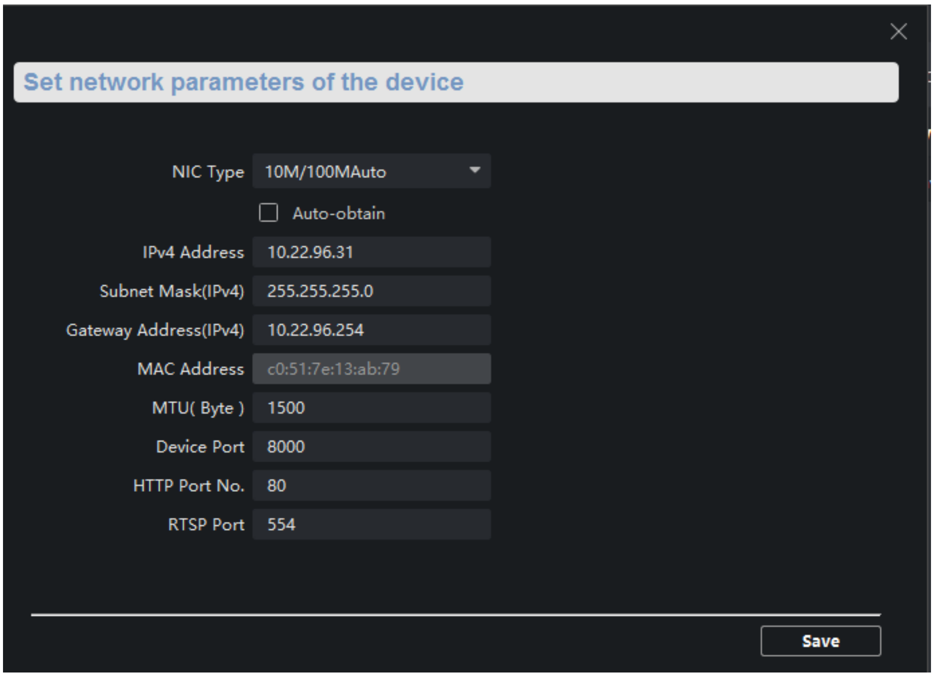
Configure network mode, IP address, NIC and NIC type, subnet mask, gateway, MAC address, MTU settings, and port No. for device.

Before You Start

Make sure the cable of the device is connected.

Steps

1. Click ⚙ to enter the **Remote Configuration** page, go to **Network** → **General**.



Set network parameters of the device

NIC Type: 10M/100MAuto

□ Auto-obtain

IPv4 Address: 10.22.96.31

Subnet Mask(IPv4): 255.255.255.0

Gateway Address(IPv4): 10.22.96.254

MAC Address: c0:51:7e:13:ab:79

MTU(Byte): 1500

Device Port: 8000

HTTP Port No.: 80

RTSP Port: 554

Figure 3-2 Network Basic Settings Page

2. Select the NIC type.

3. Set the network address.

   − Automatically obtain the network address

   Check **Auto-obtain**, the device automatically obtains the network address (**IPv4 Address**, **Subnet Mask (IPv4)**, **Default Gateway (IPv4)**) through DHCP.

   − Manually set the network address

   According to the actual network environment, manually set the network address **IPv4 Address**, **Subnet Mask (IPv4)**, **Gateway Address (IPv4)**.

4. Set the MTU(Byte), Device Port, HTTP port, and RTSP port for the device.

MTU(Byte)

Maximum transmission unit, which refers to the maximum packet size passed by TCP/UDP protocol network transmission. The default is 1500.

Device Port

The default device port number is 8000.

HTTP port

The default port number is 80, and it can be changed to any port No. which is not occupied.

RTSP port

The default port number is 554 and it can be changed to any port No. ranges from 1 to 65535.

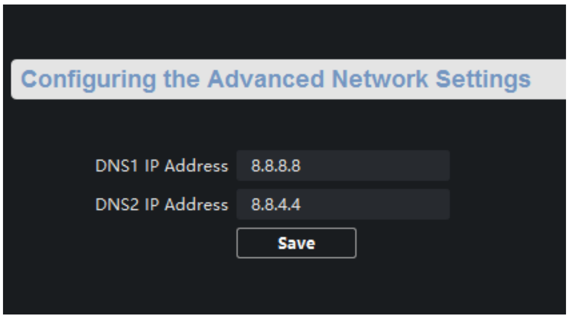
5. Click **Save** to save the settings.

3.2.2 Set DNS

When the device accesses the network through the domain name, you need to configure the correct and available DNS server IP address.

The device supports 2 DNS address.

Click ⚙ to enter the **Remote Configuration** page, go to **Network** → **DNS**, set the DNS server IP address and click **Save** to save the settings.



Configuring the Advanced Network Settings

DNS1 IP Address: 8.8.8.8

DNS2 IP Address: 8.8.4.4

Figure 3-3 DNS Setting Page

Note

When DHCP is enabled, the DNS cannot be set.

3.2.3 Set NAT

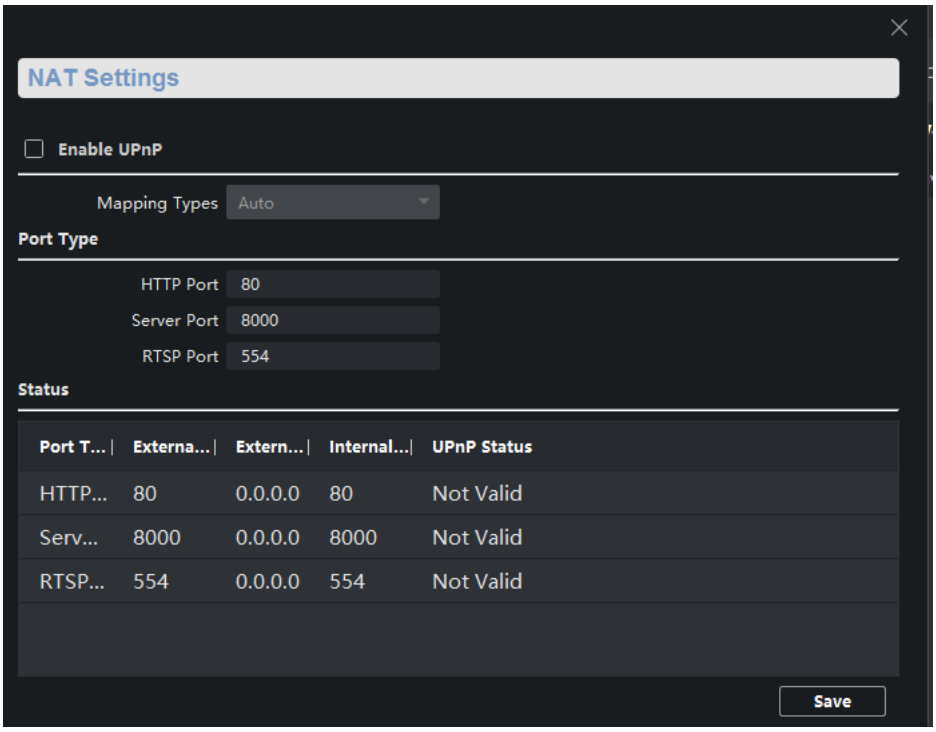
Enable the UPnP function, and you don't need to configure the port mapping for each port, and the device is connected to the Wide Area Network via the router.

Steps

Note

Universal Plug and Play (UPnP™) is a networking architecture that provides compatibility among networking equipment, software and other hardware devices. The UPnP protocol allows devices to connect seamlessly and to simplify the implementation of networks in the home and corporate environments.

1. Click ⚙ to enter the **Remote Configuration** page, go to **Network** → **NAT.**



□ Enable UPnP

Mapping Types: Auto

Port Type

HTTP Port: 80

Server Port: 8000

RTSP Port: 554

Status

Port T...	Externa...	Extern...	Internal...	UPnP Status
HTTP...	80	0.0.0.0	80	Not Valid
Serv...	8000	0.0.0.0	8000	Not Valid
RTSP...	554	0.0.0.0	554	Not Valid

Figure 3-4 NAT Setting Page

2. Check **Enable UPnP**, and set **Mapping Types** as **Manual** or **Auto**.

   – Set Mapping Types as Auto

   The Ports are read-only, and the external ports are set by the router automatically.

   – Set Mapping Types as Manual

   You can edit the external port on your demand. And then you should enable UPnP function on the router.

Caution

Please do not arbitrarily edit the default port number. If there is a port conflict and you need to edit the port number, please modify the port number as follows.

HTTP Port

By default, the value of the HTTP port No. is 80.

Server Port

By default, the value of the Server port No. is 8000. If the value is changed, you need to enter the server port number on the login page when you log in the device by client software.

RTSP Port

Real-time transport protocol port, please make sure that the port you modified is available. By default, the value of the RTSP port No. is 554.

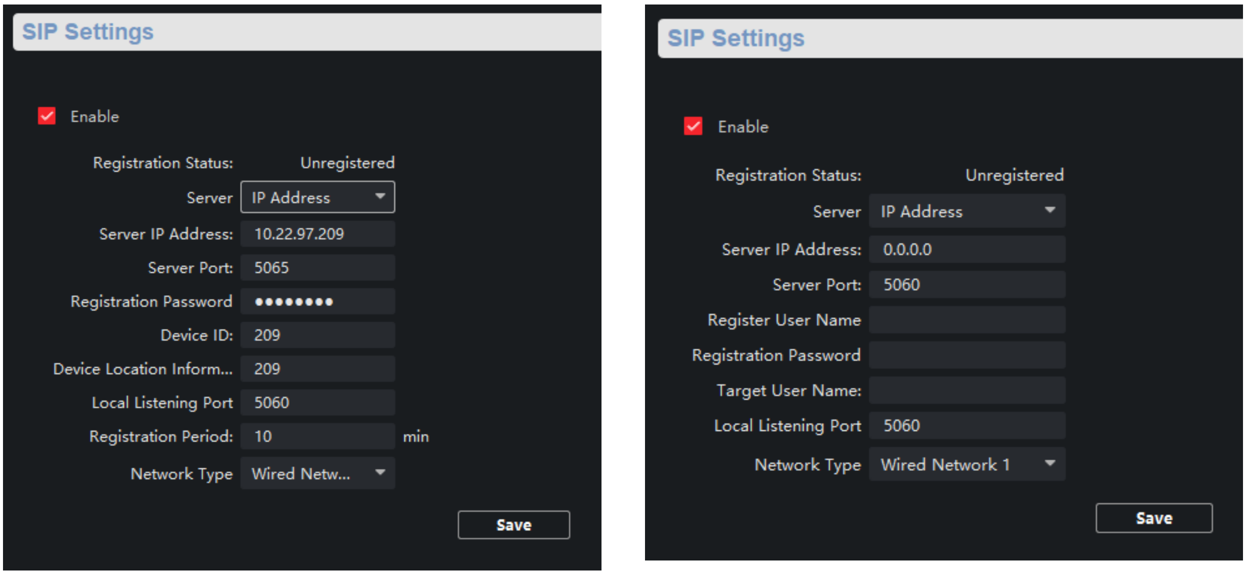
3. Click **Save** to save the settings.

3.2.4 Set SIP

After the SIP server address is set, the device actively registers to the SIP server, and devices under the same SIP server address can communicate with each other.

Steps

1. Click ⚙ to enter the **Remote Configuration** page, go to **Network** → **SIP Settings**.



SIP Settings

☑ Enable

Registration Status: Unregistered

Server: IP Address

Server IP Address: 10.22.97.209

Server Port: 5065

Registration Password: ••••••••

Device ID: 209

Device Location Inform...: 209

Local Listening Port: 5060

Registration Period: 10 min

Network Type: Wired Netw...

Save

SIP Settings

☑ Enable

Registration Status: Unregistered

Server: IP Address

Server IP Address: 0.0.0.0

Server Port: 5060

Register User Name:

Registration Password:

Target User Name:

Local Listening Port: 5060

Network Type: Wired Network 1

Save

Figure 3-5 SIP Settings Page (Private Protocol & SIP Protocol)

2. Check **Enable** box to enbale the Sip server.

3. Enter the Sip server parameters.

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)

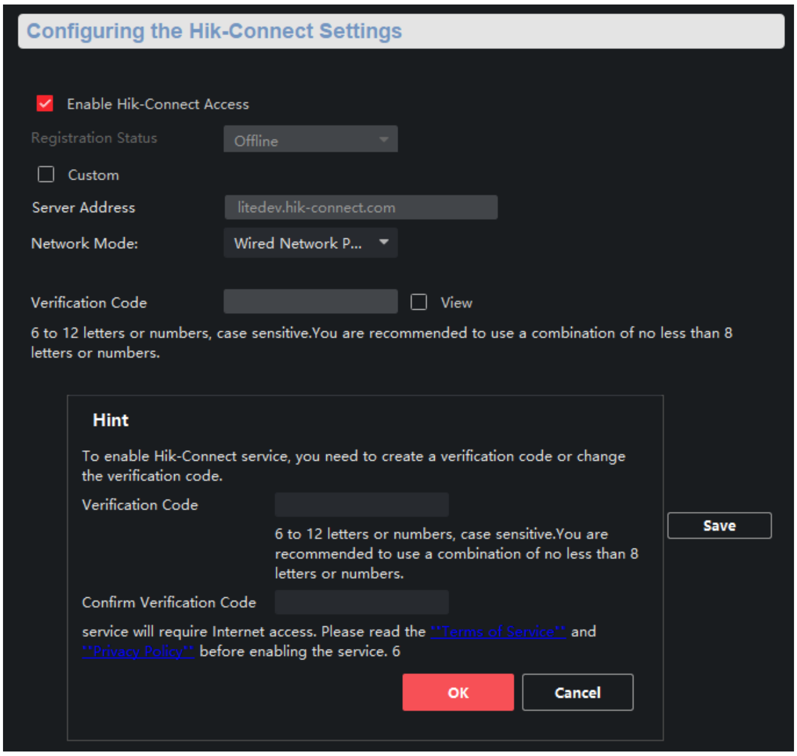
4. Click **Save**.

3.2.5 Set Hik-Connect

Enable Hik-Connect service and you can add the device to Hik-Connect.

Steps

1. Click ⚙ to enter the **Remote Configuration** page, go to **Network** → **Configuring the Hik-Connect Settings.**



Configuring the Hik-Connect Settings

☑ Enable Hik-Connect Access

Registration Status: Offline

□ Custom

Server Address: litedev.hik-connect.com

Network Mode: Wired Network P...

Verification Code □ View

6 to 12 letters or numbers, case sensitive.You are recommended to use a combination of no less than 8 letters or numbers.

Hint

To enable Hik-Connect service, you need to create a verification code or change the verification code.

Verification Code

6 to 12 letters or numbers, case sensitive.You are recommended to use a combination of no less than 8 letters or numbers.

Confirm Verification Code

service will require Internet access. Please read the **Terms of Service** and **Privacy Policy** before enabling the service. 6

Figure 3-6 Hik-Connect Service Setting Page

2. Check **Enable Hik-Connect Access** and enter the verification code to enable Hik-Connect service.
3. Optional: If you want to edit **Server Address**, check **Custom** and enter the server address.

Note

The default server address is ***litedev.hik-connect.com***.

4. Select **Network Mode**.
5. Enter a verification code and click **Generate QR code**.

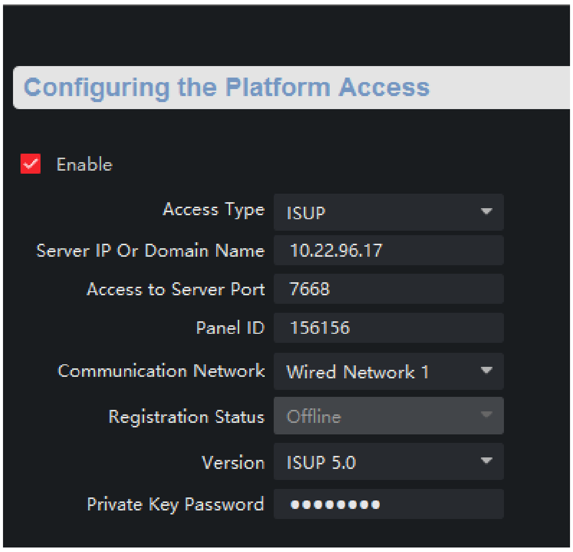
   There will be a QR code displaying on the page.
6. Click **Save**.
7. Scan the QR code via Hik-Connect and the device will be added to Hik-Connect.

3.2.6 Access the Platform

Platform access provides you an option to manage the devices via platform.

Steps

1. Click ⚙ to enter the **Remote Configuration** page, go to **Network** → **Platform Access**.



Configuring the Platform Access

☑ Enable

Access Type: ISUP

Server IP Or Domain Name: 10.22.96.17

Access to Server Port: 7668

Panel ID: 156156

Communication Network: Wired Network 1

Registration Status: Offline

Version: ISUP 5.0

Private Key Password: ••••••••

Figure 3-7 Platform Access Configuration

2. Check **Enable Platform Access** to enable the Platform Access function.

3. Set the platform access parameters.

Access Type

Select the platform to be accessed.

Server IP or Domain Name

Enter the IP address or domain name of the platform.

Access to Server Port

Enter the port number of the platform.

Panel ID

Panel ID is the unique identification of the device.

Communication Network

Select the network mode for communication with platform.

Registration Status

Display the status which the device registers to the platform.

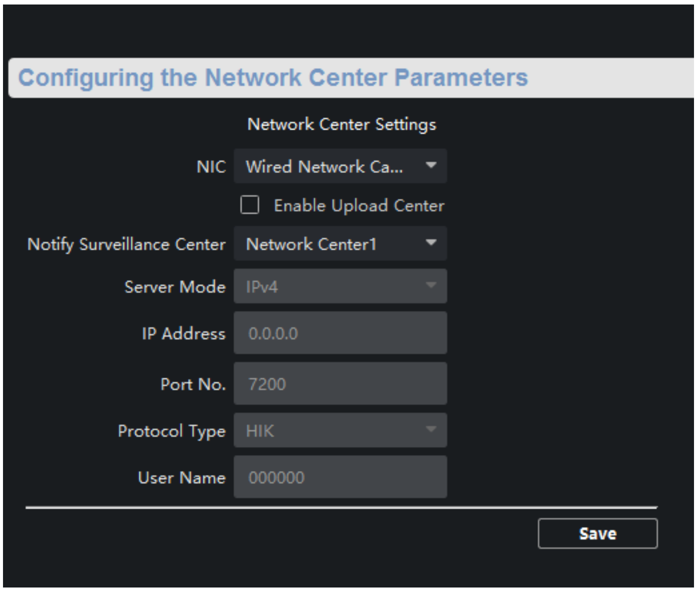
4. Click **Save**, and you can access to the device via platform.

3.2.7 Set Alarm Center

Configure the alarm center. When an alarm is triggered, the alarm information can be uploaded to the configured alarm center.

Steps

1. Click ⚙ to enter the **Remote Configuration** page, go to **Network** → **Network Center Settings**.



Configuring the Network Center Parameters

Network Center Settings

NIC: Wired Network Ca...

☐ Enable Upload Center

Notify Surveillance Center: Network Center1

Server Mode: IPv4

IP Address: 0.0.0.0

Port No.: 7200

Protocol Type: HIK

User Name: 000000

Figure 3-8 Network Center Settings

2. Select a NIC.

Note

The device supports two wired networks and one wireless network. Each network supports uploading alarm information to one alarm center.

3. Check **Enable Upload Center** to enable the alarm center, and set the upload center parameters.

Notify Surveillance Center

Each NIC supports only one upload center, and the default is **Net Center 1**.

Server Mode

The address type of the upload center server. You can set **Server Type** as **IP4/IP6** or **Domain Name**.

IP Address/Server Domain Name

Enter the server IP address or server domain name according to the server type you set.

Port No.

The port number of the upload center. The HIK protocol defaults to 7200.

Protocol Type

The default is **HIK**.

User Name

Supports numbers and letters. The HIK protocol can be set to a length ranging from 6 to 9 digits.

Note

If you set the protocol type as **HIK**, you do not need to edit the user name.

4. Click **Save**.

3.3 Alarm Settings

3.3.1 Set Zone

The device supports four alarm input zones and two default zones (emergency call help and consulting). You need to configure zone parameters.

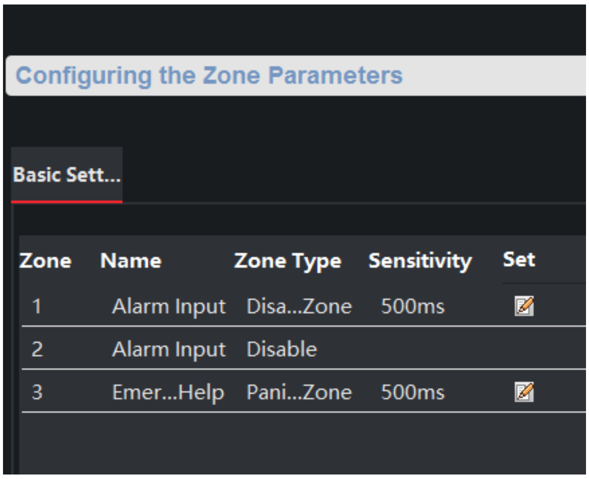
Steps

Note

The default zone has a default zone type, default audio file, and the default zone will automatically upload an alarm recovery report. These three parameters (**Zone Type**, **Audio File** and **Upload Alarm Recovery Report**) do not need to be set.

1. In the client software, go to **Device Management**, select the device in the device list, and click ⚙ to enter the **Remote Configuration** page.

2. Go to **Input Settings** → **Zone**.

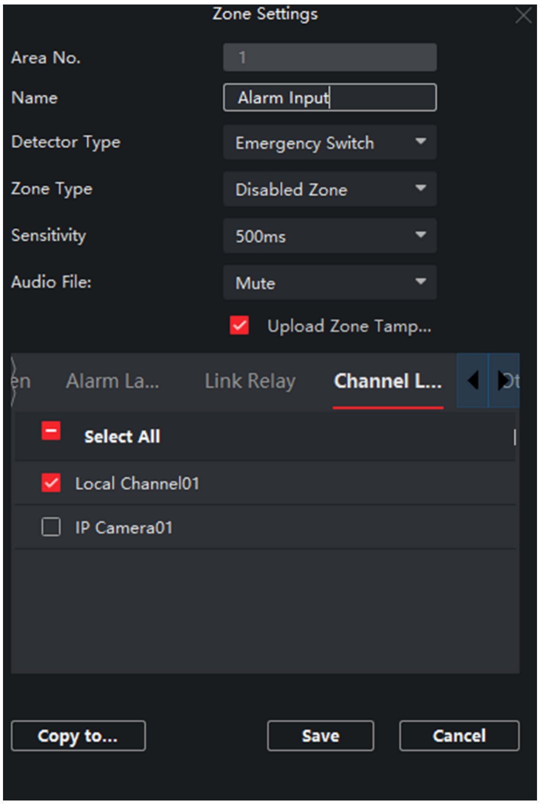


Configuring the Zone Parameters

Zone	Name	Zone Type	Sensitivity	Set
1	Alarm Input	Disa...Zone	500ms	✎
2	Alarm Input	Disable		
3	Emer...Help	Pani...Zone	500ms	✎

Figure 3-9 Zone

3. Select an zone, click ✎.



Zone Settings

Area No. 1

Name Alarm Input

Detector Type Emergency Switch

Zone Type Disabled Zone

Sensitivity 500ms

Audio File: Mute

☑ Upload Zone Tamp...

☐ Select All

☑ Local Channel01

☐ IP Camera01

Figure 3-10 Set Zone

4. Set zone parameters.

Name

Zone name.

Detector Type

The detector type of the zone.

Zone Type

Four zone type can be set for Non-default zones: Instant Zone, Fire Zone, 24-hour Non-voiced Zone, Shield Zone.

Instant Zone

In the armed state, as long as the detector connected to the zone is triggered, an alarm is generated immediately without delay.

Fire Zone

The fire zone must be set to a 24-hour alarm zone. When the fire zone is triggered, start the external siren/sounder.

24-hour Non-voiced Zone

The detector working in 24-hour non-voiced zone is in an alert state for 24 hours, and will not be affected by the disarming operation. Once triggered, the information is immediately uploaded to the center with no alarm sound.

Shield Zone

No events will trigger an alarm.

Sensitivity

The default value is 500 ms.

Audio File

Select an audio file for zone.

Upload Alarm Recovery Report

If check **Upload Alarm Recovery Report**, the report will be uploaded to the center when the alarm is restored.

5. Select the zone linkage.

Linked Trigger

After the zone is triggered, the selected alarm output is on.

Channel

After the zone is triggered, the selected video channel is linked.

6. Optional: Click **Copy to...**, copy the zone parameter configuration to other zones.

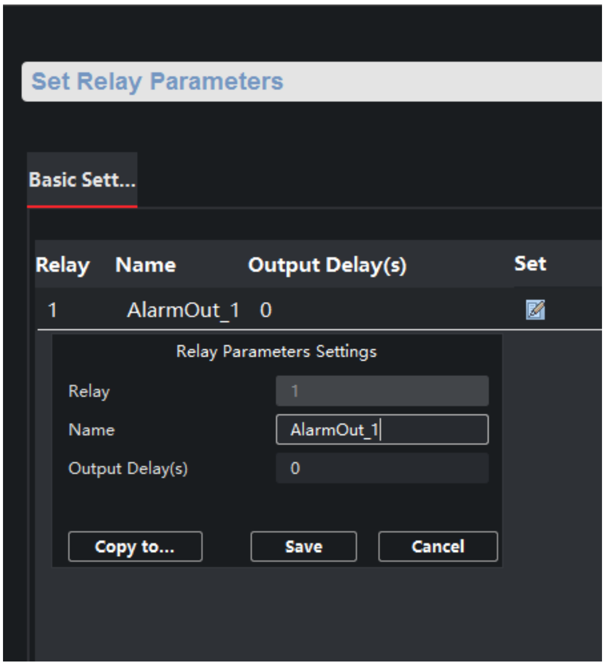
7. Click **Save**.

3.3.2 Set Relay

Configure the relay parameters, include the relay name and the output delays.

Steps

1. Click ⚙ to enter the **Remote Configuration** page, go to **Output Settings** → **Relay**.
2. Select a relay and click ✎, set the relay parameters.



Set Relay Parameters

Basic Sett...

Relay	Name	Output Delay(s)	Set
1	AlarmOut_1	0	✎

Relay Parameters Settings

Relay: 1

Name: AlarmOut_1

Output Delay(s): 0

Figure 3-11 Relay Configuration Page

Name

The relay name.

Output Delay(s)

The output delay time, can be set from 0 to 2000s. After the zone event is triggered, the relay will turn off the relay output after the output delay time is ended.

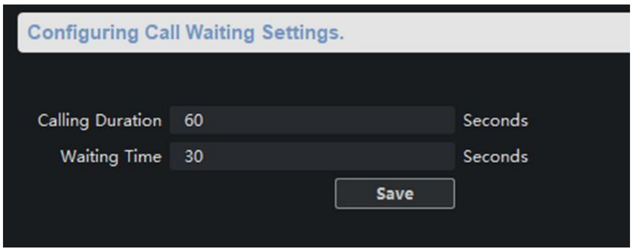
3. Click **Save**.
4. Optional: Click **Copy to...**, you can copy the relay settings to other relays.

3.3.3 Set Call Waiting

Configure the call waiting parameters, include the maximum ring duration and waiting time.

Steps

1. Click ⚙ to enter the **Remote Configuration** page, go to **Output Settings** → **Waiting**.



Configuring Call Waiting Settings.

Calling Duration 60 Seconds

Waiting Time 30 Seconds

Figure 3-12 Call Waiting Settings Page

2. Set the call waiting parameters.

Calling Duration

The playback time of the calling tone when calling, can be set from 40 s to 80 s.

Waiting Time

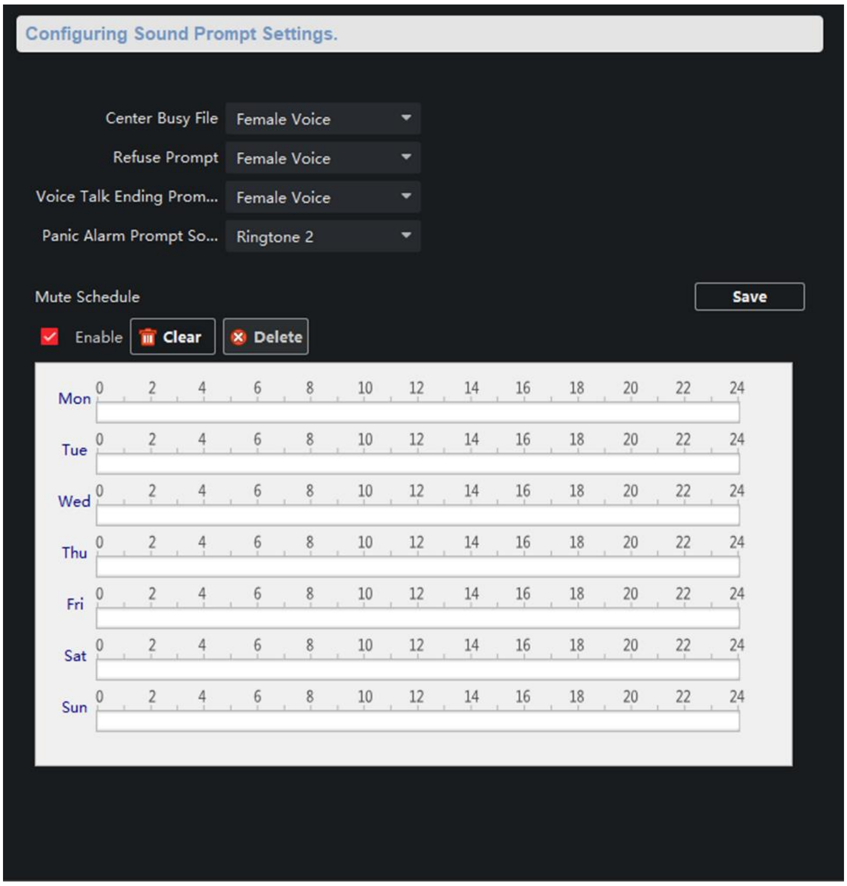
The extended playback time of the prompt tone based on the maximum ring time when calling the center station and pressing the call waiting button, can b set from 10 seconds to 60 s.

3. Click **Save**.

3.3.4 Set Voice Prompt

Steps

1. Click ⚙ to enter the **Remote Configuration** page, go to **Output Settings** → **Voice Prompt**.



Configuring Sound Prompt Settings.

Center Busy File: Female Voice

Refuse Prompt: Female Voice

Voice Talk Ending Prom...: Female Voice

Panic Alarm Prompt So...: Ringtone 2

Mute Schedule

☑ Enable

Figure 3-13 Voice Prompt Configuration Page

2. Set the **Center Busy File**, **Refuse Prompt**, **Voice Talk Ending Prompt**, and **Panic Alarm Prompt Sound**.

3. Optional: Configure the mute program.

1) Check **Enable** to enable the mute program.
2) Click and drag the mouse on the time bar to draw the scheduled time period.
3) 3Optional: Edit the time period.

- Modify the time period

  Click and select the added time period, drag to modify the time period position; click and select the added time period, then moves the cursor to both ends of the time period, when the cursor becomes a double arrow, you can drag the mouse left and right to modify the time period.

- Delete one time period

  Click and select the time period, and click **Delete** to delete the selected time period.

- Delete all time periods

  Click **Clear** to delete all time periods.
  The device will be muted during the configured time period.

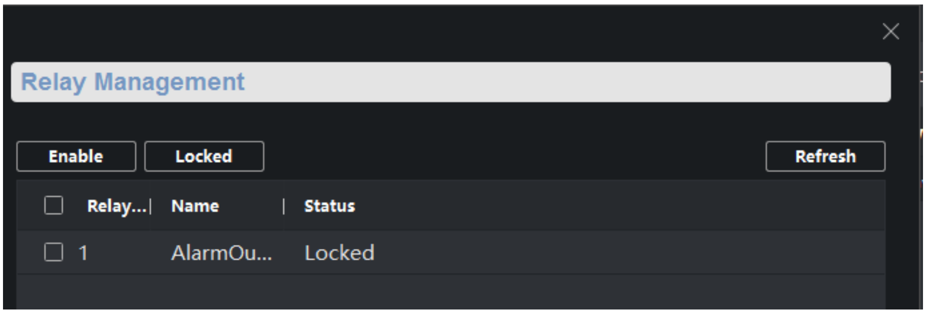
4. Click **Save**.

3.4 Alarm Management

3.4.1 Manage Relay

Open or close the relay via client software.

Click ⚙ to enter the **Remote Configuration** page, go to **Alarm Management** → **Relay**



□	Relay...	Name	Status
□	1	AlarmOu...	Locked

Figure 3-14 Relay

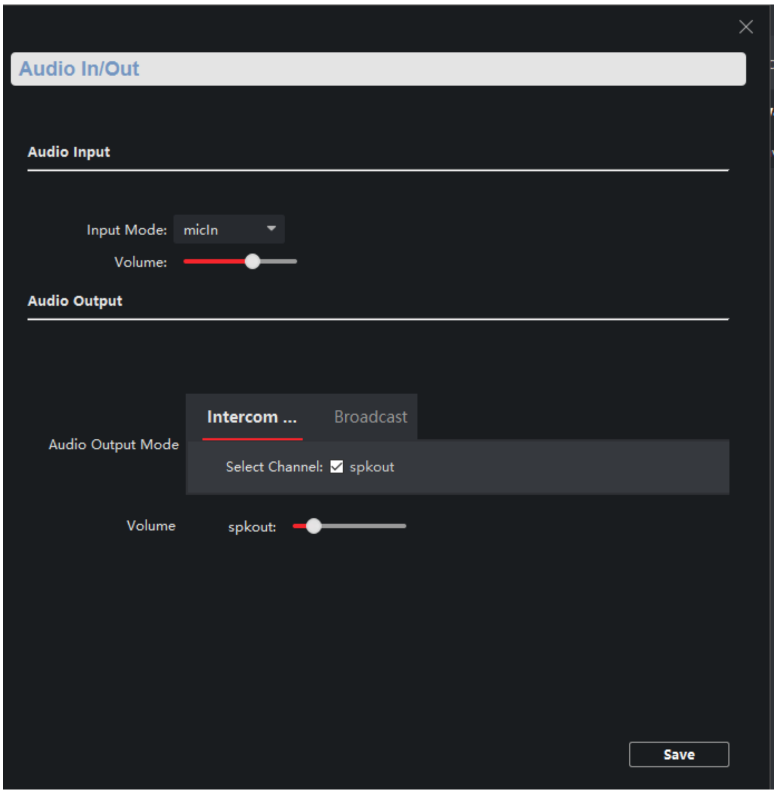
Check the relays that need to be turned on/off. Click **Enable/Locked** to change the relay switch status. Click **Refresh**, you can refresh the relay switch status.

3.4.2 Manage Audio Input/Output

Configure the audio input/audio output mode and the volume of the corresponding mode.

Steps

1. Click ⚙ to enter the **Remote Configuration** page, go to **Alarm Management** → **Audio In/Out**.



Audio In/Out

Audio Input

Input Mode: micIn

Volume:

Audio Output

Audio Output Mode: Intercom ... | Broadcast

Select Channel: ☑ spkout

Volume: spkout:

Figure 3-15 Audio Input/Output

2. Set the audio input/output mode and volume.

Note

spkOut is the device's own audio input/output.

3. Click **Save**.

3.4.3 Manage Audio File

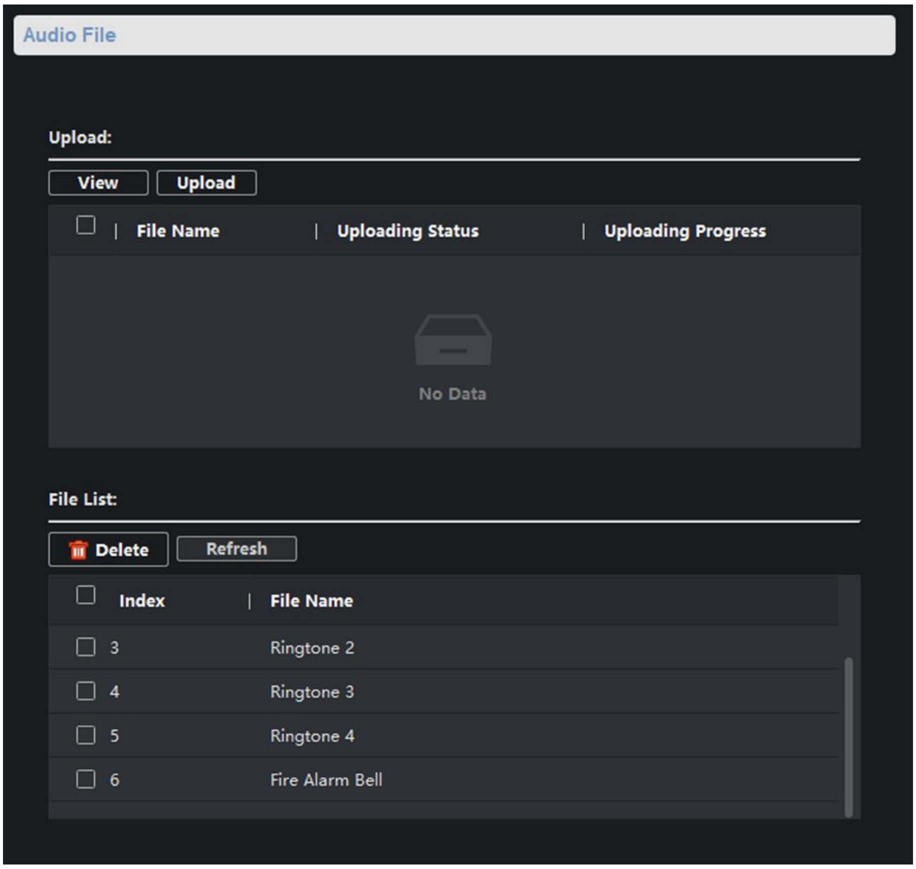
Upload the custom audio files to SD card, and delete the audio file in the SD card.

Before You Start

Insert the SD card into the device.

Steps

1. Click ⚙ to enter the Remote Configuration page, go to **Alarm Management** → **Audio File**.



□ Index	File Name
□ 3	Ringtone 2
□ 4	Ringtone 3
□ 5	Ringtone 4
□ 6	Fire Alarm Bell

Figure 3-16 Audio File Management

2. Upload the custom audio files.
   1) Click **View** to select the audio file (can be selected in batch).
   2) Check the audio file in the Upload File list and click **Upload**.

Note

- Supported Audio file format: .mp3 and .wav (8 kHz, 16 bit, and single track). The file name can't contain spaces at the beginning and end. The length of the file name should be not more than 31, and the file name cannot contain symbols: ?\/*”<>|.
- Each audio file size up to 2MB, and up to 16 audio files are uploaded.
- An audio file will be overwritten if uploading an audio file with the same name.

3. Optional: Delete the audio files in the SD card.
   1) In the **File List**, click **Refresh** to display the audio files.
   2) Check the audio file needs to be deleted, click **Delete**.

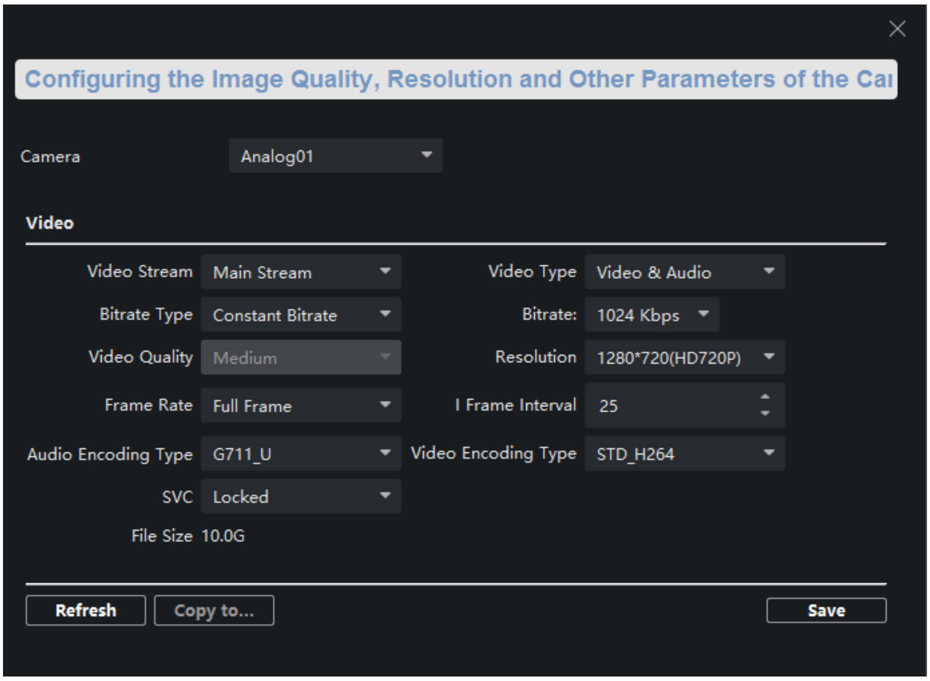
The function using the deleted audio files will restore the default audio file configuration.

3.5 Video & Audio Settings

3.5.1 Video & Audio Settings

Configure the image quality, resolution and other parameters of the camera.

Click to enter the **Remote Configuration** page, click **Image** → **Video & Audio**.



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

Camera: Analog01

Video

Video Stream	Main Stream	Video Type	Video & Audio
Bitrate Type	Constant Bitrate	Bitrate:	1024 Kbps
Video Quality	Medium	Resolution	1280*720(HD720P)
Frame Rate	Full Frame	I Frame Interval	25
Audio Encoding Type	G711_U	Video Encoding Type	STD_H264
SVC	Locked		
File Size	10.0G		

Figure 3-17 Video & Audio

Select a camera, and set the video and audio parameters. Click **Save** to save the settings.

Note

- You can click **Copy to...** to copy the parameters to other camera.
- After editing the video and audio parameters, the device won't reboot.
- Please combine the actual demand and storage capacity to configure the video and audio parameters.

Stream Type

The stream type of camera can be set as **Main Stream** or **Sub Stream**. By default, it is **Main Stream**. The main stream is used for HD storage and preview; the sub stream is used for SD storage and preview when the network bandwidth is insufficient.

Video Type

The video type can be set as **Video** or **Video & Audio**. By default, it is **Video & Audio**, where video contains sound and images. If you don't need sound, choose **Video Stream**.

Bitrate Type

The bitrate type can be set as **Constant** or **Variable**. By default, it is **Constant**, where you should select a constant value from the **Bitrate** drop-down box. You are supposed to select the maximum bitrate when the bitrate type is set as **Variable**.

Video Quality

You are able to choose different level of the video quality. The video quality is not optional by default when the bitrate type is **Constant**.

Resolution

According to the requirements for video clarity, the higher the resolution, the higher the bandwidth requirement for the network.

Frame Rate

Video frames per second. According to the actual bandwidth setting, the higher the video frame rate, the higher the required bandwidth and the higher the required storage space.

I Frame Interval

The number of frames between the two key frames before and after. The larger the I frame interval is, the smaller the code stream fluctuation is, but the image quality is relatively poor. Otherwise, the code stream fluctuation is larger and the image quality is higher. It is recommended to use the default value.

Audio Encoding Type

When the stream type is the **Main Stream**, the audio encoding type can be set as **G711_U**, **AAC or PCM**. And the audio encoding type of the sub stream is the same as the audio encoding type set in the main stream.

Video Encoding Type

By default, it is **STD_H264**.

SVC

It is a scalable video coding technology. The SVC function can be used for framed video recording to reduce storage space. The framed video file still supports normal decoding. When the SVC function is selected to be **On**, both the storage device and the decoding device must be required to support the function. When the SVC function is selected as **Auto**, the device will adapt to the current network environment and decide whether to send framed video to ensure that the image can be previewed normally.

File Size

According to the video and audio parameters, the video file size of the whole day will be automatically calculated.

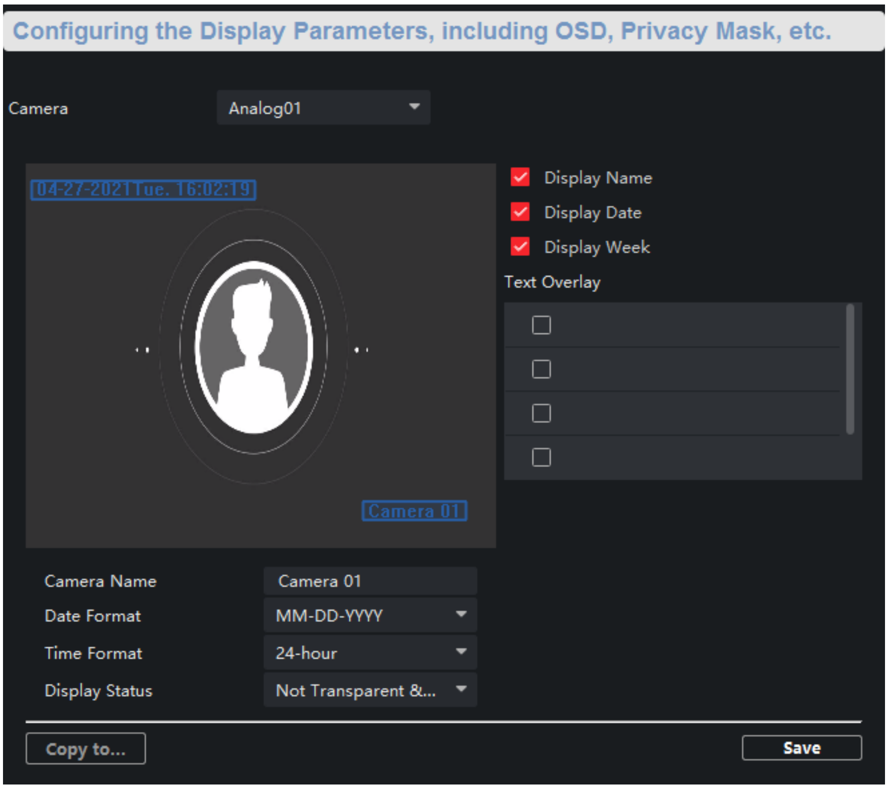
Note

- After the video and audio parameters are changed, the device won't reboot.
- Please combine the actual demand and storage capacity to configure the video and audio parameters.

3.5.2 Set Display

Edit the display information of the camera.

Click ⚙ to enter the **Remote Configuration** page, go to **Image** → **View Scale**.



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

Camera: Analog01

☑ Display Name
☑ Display Date
☑ Display Week

Text Overlay

□
□
□
□

Camera Name: Camera 01
Date Format: MM-DD-YYYY
Time Format: 24-hour
Display Status: Not Transparent &...

Figure 3-18 View Scale

Select a camera from the drop-down box to configure the display parameters of the camera, including display position, display format and optional display content, you are able to add custom display information.

Editing the display position

Drag the blue box on the live view page to change the position of the display information, click **Save**, and then the position of the display information will be updated.

Editing the display format

Date Format

Select the display format of the date in the **Date Format Drop-Down** box.

Time Format

Select Time Format as 24-hour or 12-hour.

OSD Format

There are four freely combined display status to choose from depending on whether the display information is transparent or flashing. For example, when the display status is **Transparent & Blinking**, the displayed information will be displayed with a certain transparency and will flash. .

Editing the display content

You are able to select the display content optionally, edit the camera name, and add the custom display content.

- Selecting the display content

According to your requirement, check **Display Name**, **Display Date**, **Display Week** to display the selected display content. Click **Save** to save the settings.

- Editing the camera name

Editing the camera name in the Camera Name text box and click **Save**.

- Adding custom display content

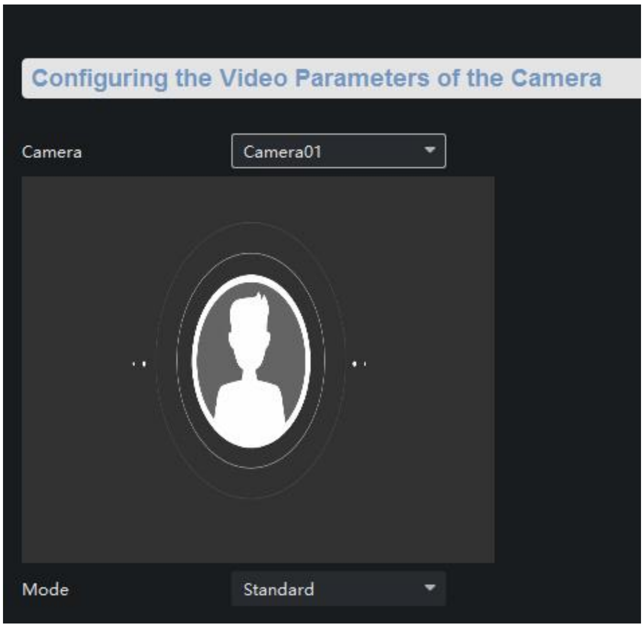
Click the right area of the check box in the **Text Overlay** List and enter display content in the text box. Check the text and click **Save** to display the custom information.

Note

You can drag the content to modify the location, or remove the check to cancel the display.

3.5.3 Set Image Parameters

For the device with camera, you can set the image parameters for camera.
Click ⚙ to enter the **Remote Configuration** page, go to **Image** → **Picture Settings**.



Configuring the Video Parameters of the Camera

Camera: Camera01

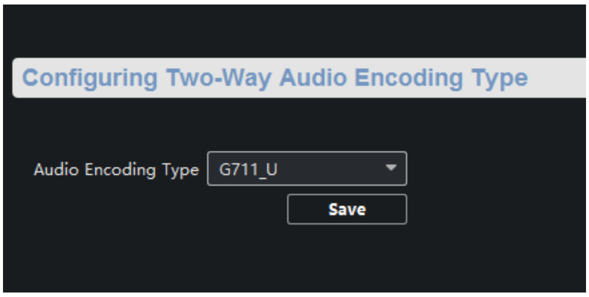
Mode: Standard

Figure 3-19 Picture Settings Page

Select a camera to configure the mode.

3.5.4 Set Intercom Audio

Click ⚙ to enter the **Remote Configuration** page, go to **Image** → **Intercom Audio**.



Configuring Two-Way Audio Encoding Type

Audio Encoding Type: G711_U

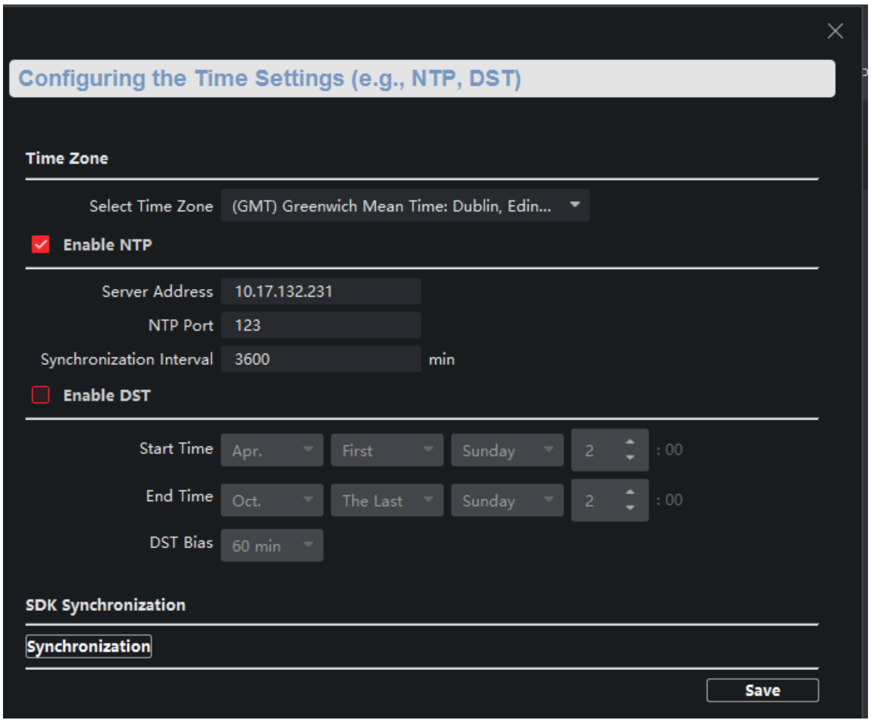
Figure 3-20 Intercom Audio

Select the **Audio Encoding Type** as **G711_U**, **PCM**, **ADPCM**, **AAC**, or **OPUS** from the drop-down box. And click **Save** to save the settings.

3.6 System Settings

3.6.1 Set Time

Click ⚙ to enter the **Remote Configuration** page, go to **Device Information** → **Time**.



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

Time Zone

Select Time Zone: (GMT) Greenwich Mean Time: Dublin, Edin...

☑ Enable NTP

Server Address: 10.17.132.231

NTP Port: 123

Synchronization Interval: 3600 min

☐ Enable DST

Start Time: Apr. First Sunday 2 : 00

End Time: Oct. The Last Sunday 2 : 00

DST Bias: 60 min

SDK Synchronization

Figure 3-21 Time

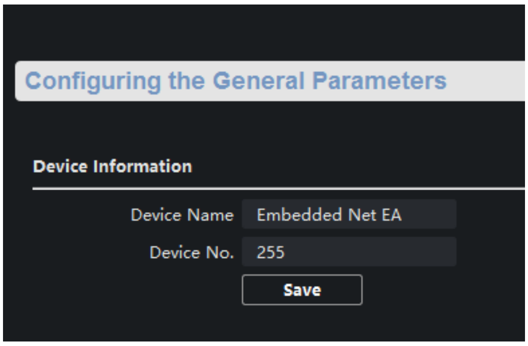
You can set the time zone, NTP, DST on the Time page.

You can also click Synchronization to implement SDK synchronization.

3.6.2 Set System Parameters

Set the device name, device No. and configure the video files.

Click ⚙ to enter the **Remote Configuration** page, go to **System** → **General Parameters**.



Configuring the General Parameters

Device Information

Device Name: Embedded Net EA

Device No.: 255

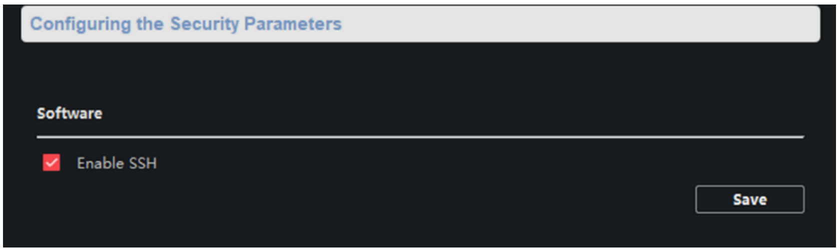
Figure 3-22 General Parameters

Set the device name and device No.. Click **Save** to save the settings.

3.6.3 Set Security

Enable/disable SSH service, which is used to provide security configuration for remote debugging.

Click ⚙ to enter the **Remote Configuration** page, go to **System** → **Security**.



Configuring the Security Parameters

Software

☑ Enable SSH

Figure 3-23 Secuirty

Check **Enable SSH** to enable SSH service, and click **Save**.

Note

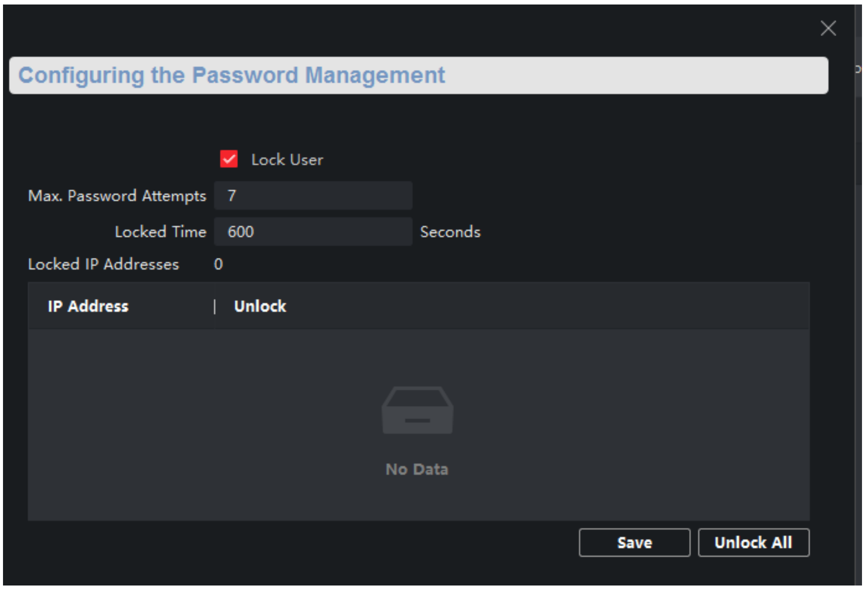
By default, the SSH service is not enabled. The default setting will be restored after the restart.

3.6.4 Set Password

Set the maximum password attempts, the lock duration of the locked user. And you can unlock the user remotely.

Steps

1. Click ⚙ to enter the **Remote Configuration** page, go to **System** → **Password Management**.



Configuring the Password Management

☑ Lock User

Max. Password Attempts: 7

Locked Time: 600 Seconds

Locked IP Addresses: 0

IP Address	Unlock

No Data

Figure 3-24 Password Management

IP Address

The IP address of the terminal in which the locked user logs.

Unlock

The user's access lock status on the corresponding IP address.

2. Enable the access lock function and set the lock parameters.

   1) Check **Access Lock** to enable the access lock function.
   2) Set the user lock parameters, including maximum password attempts and lock duration.

Max. Password Attempts

The maximum times that the user attempts to enter the password. By default, it is 7, the available value is 3 to 10.

Lock Time

The lock duration of the locked user. By default, it is 600 s, the available value is 10 to 3600 s.

   3) Click **Save**.

3. Optional: Click **Unlock All** to unlock all user.

3.6.5 Set User

Steps

Note

The device only has the admin user and only supports modifying the admin user password.

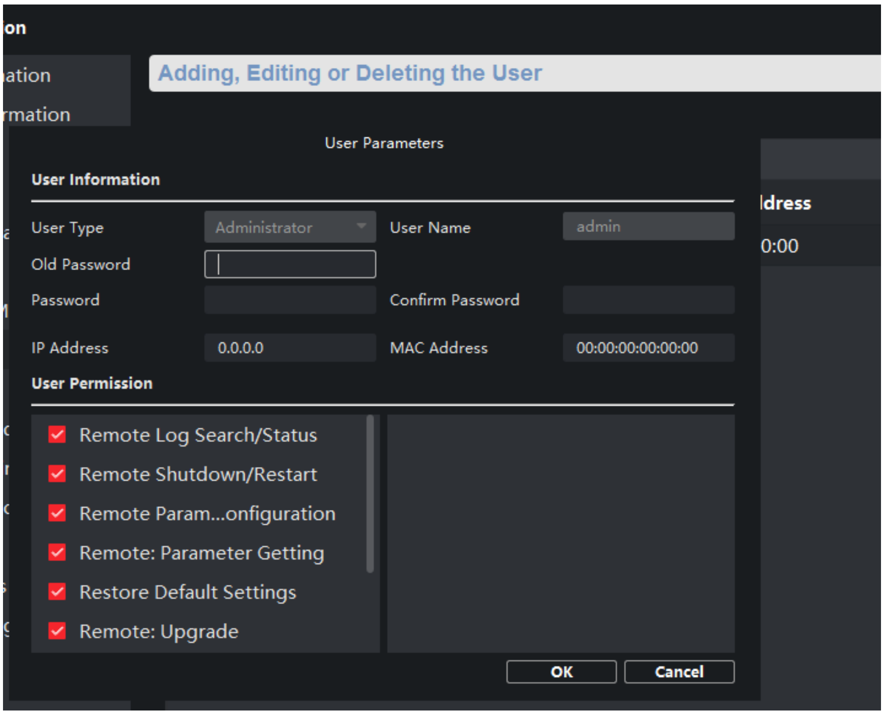
1. Click ⚙ to enter the **Remote Configuration** page, go to **System** → **User**.

2. Edit the admin user password.

   1) Select the admin user and click **Edit**.

2) Enter the new password and confirm it.

3) Click **Save**.



Adding, Editing or Deleting the User

User Parameters

User Information

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

User Permission

- ☑ Remote Log Search/Status
- ☑ Remote Shutdown/Restart
- ☑ Remote Param...onfiguration
- ☑ Remote: Parameter Getting
- ☑ Restore Default Settings
- ☑ Remote: Upgrade

OK Cancel

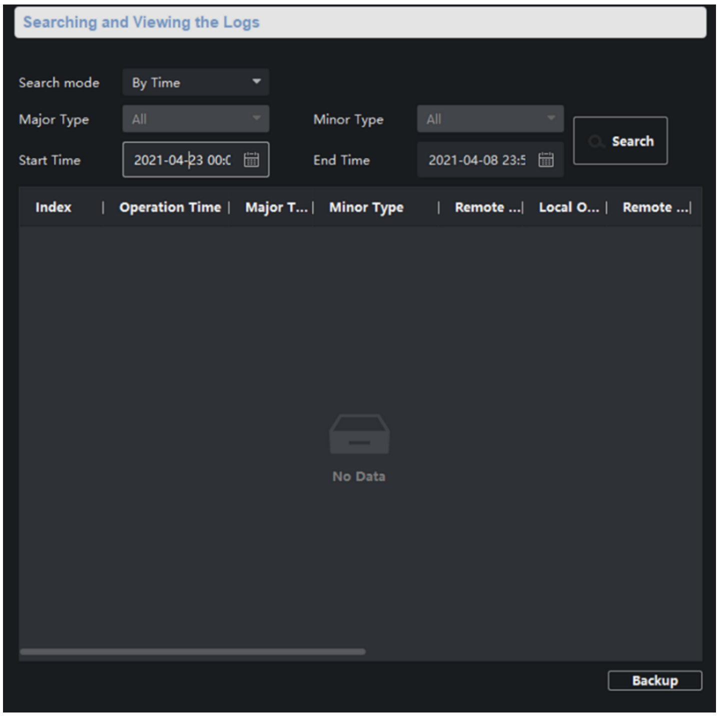
Figure 3-25 User

3.6.6 Search for Log

Search and view the alarm logs, exception logs, operation logs and event logs.

Click ⚙ to enter the **Remote Configuration** page, go to **System** → **Log Query**.

You can set the search criteria and click **Search**, and the search result is in the list.



Searching and Viewing the Logs

Search mode: By Time

Major Type: All

Minor Type: All

Start Time: 2021-04-23 00:(

End Time: 2021-04-08 23:5

Index	Operation Time	Major T...	Minor Type	Remote ...	Local O...	Remote ...

No Data

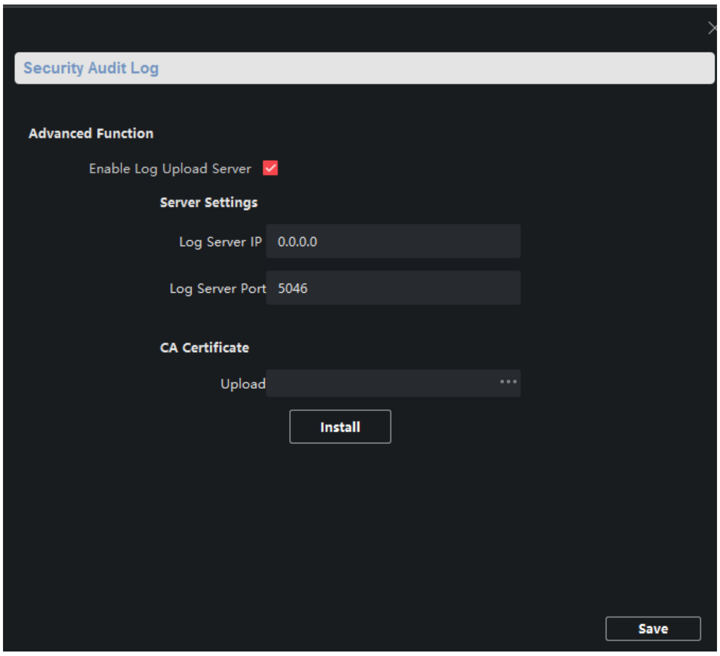
Figure 3-26 Log Query

Note

You can click **Backup** and download the search result.

3.6.7 Security Audit Log

Click ⚙ to enter the **Remote Configuration** page, go to **System** → **Security Audit Log**.



Security Audit Log

Advanced Function

Enable Log Upload Server ☑

Server Settings

Log Server IP: 0.0.0.0

Log Server Port: 5046

CA Certificate

Upload: ...

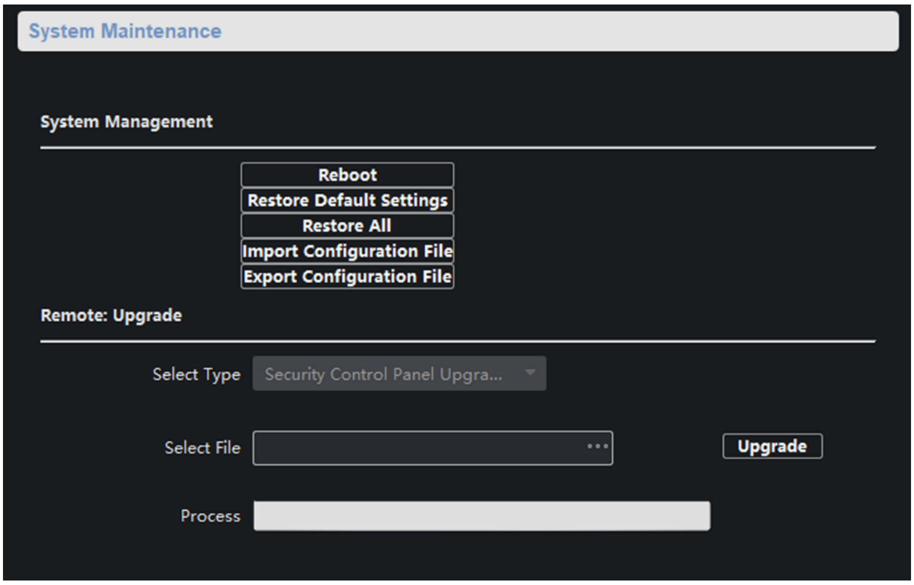
Figure 3-27 Security Audit Log

1. Check **Enable Log Upload Server**.
2. Set log server IP and server port.
3. Click **…** to upload the CA certificate.
4. Click **Save**.

3.6.8 Maintain the System

System management and remote upgrade.

Click ⚙ to enter the **Remote Configuration** page, go to **System** → **System Maintenance**.



Select Type: Security Control Panel Upgra...

Figure 3-28 System Maintenance

System Management

You can reboot the device, restore default settings, restore all settings, and import/export configuration file.

Reboot

Restart the device.

Restore Default Settings

Restore the default settings, that is, except the IP address and user information, all other parameters of the device will be restored to factory default settings.

Restore All

Restore all the parameters to factory default settings, and the device needs to be reactivated after restoring the parameters to default.

Import Configuration File

Import the configuration file from the client software to the device.

Note

- The configuration file contains the parameter information of the device.
- It is required to enter the password created when exporting when import a file.

Export Configuration File

Export the configuration file from the device to the client software.

Note

- The configuration file contains the parameter information of the device.
- It is required to set a password for the exported file. The password is used for importing verification.

Remote Upgrade

Upgrade the device remotely via the client software.

Click and select the upgrading file. And click **Upgrade** to upgrade the device.

Note

An invalid upgrade occurs when using a mismatched upgrade file, and then the device program is still the program before the upgrade.

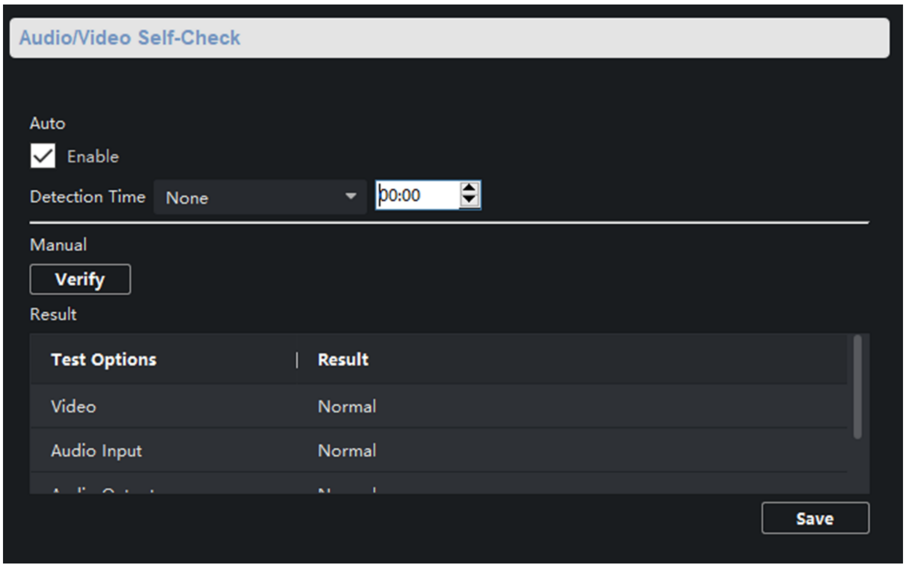
Caution

Do not power off the device during the upgrade process.

3.6.9 View Device Information

Automatically or manually check the video and audio status.

Click to enter the **Remote Configuration** page, go to **System** → **Video/Audio Self-Check**.



Audio/Video Self-Check

Auto

☑ Enable

Detection Time: None 00:00

Manual

Result

Test Options	Result
Video	Normal
Audio Input	Normal

Figure 3-39 Video and Audio Check Page

Auto check

Check the video and audio status automatically.
Check **Enable**, set the detection time and click **Save**.

Note

The detection time can be selected as none, everyday or one day of the week.

None

Auto check function is not enabled.

Everyday

Check every day according to the set time.

One day of the week

The device performs a check at the set time on this day of the week.

Manual check

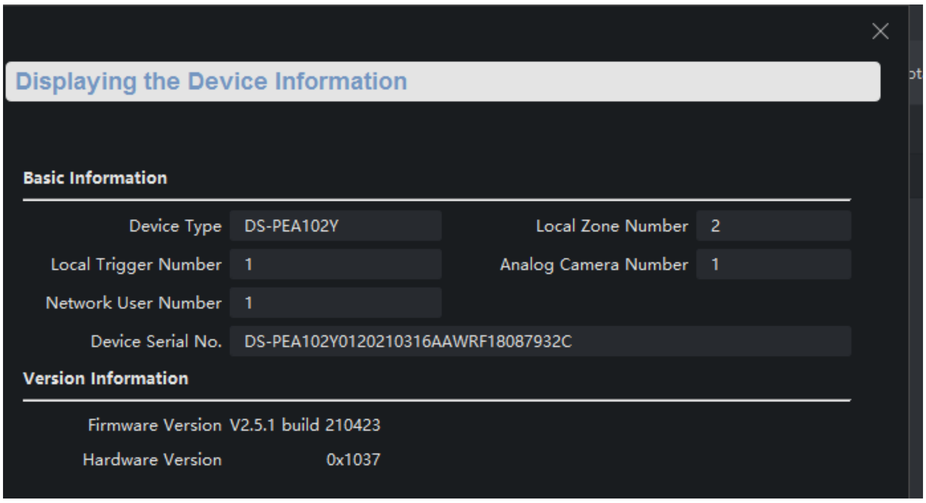
Click **Verity** to start the check and the check results are displayed in the list.

Table 3-1 Description of Check Results

Check results	Description
Normal	Video/audio input/audio output signal is normal.
Exception	Video/audio input/audio output signal is loss.
Unknown	Audio input is exception and cannot detect audio output status.

3.6.10 View Device Information

Click ⚙ to enter the **Remote Configuration** page, go to **Device Information**→ **Device Information**.



Displaying the Device Information

Basic Information

Device Type: DS-PEA102Y
Local Zone Number: 2
Local Trigger Number: 1
Analog Camera Number: 1
Network User Number: 1
Device Serial No.: DS-PEA102Y0120210316AAWRF18087932C

Version Information

Firmware Version: V2.5.1 build 210423
Hardware Version: 0x1037

Figure 3-29 Device Information

3.7 Check Status

3.7.1 Check Zone Status

Click ⚙ to enter the **Remote Configuration** page, go to **Status** → **Zone**, you can view the status of zone alarm.

3.7.2 Check Relay Status

Click ⚙ to enter the **Remote Configuration** page, go to **Status** → **Relay**, you can view the relay status.

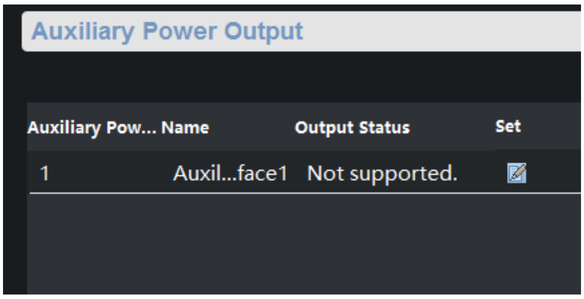
3.8 Other Settings

3.8.1 Set Auxiliary Output

Enable the auxiliary power output to use the 12 V auxiliary power.

Steps

1. Click ⚙ to enter the **Remote Configuration** page, go to **Other** → **Auxiliary Power Output**.



Auxiliary Power Output

Auxiliary Pow...	Name	Output Status	Set
1	Auxil...face1	Not supported.	✎

Figure 3-30 Auxiliary Power Output Configuration

2. Click ✎, and select the **Aux Power Output** as **Not Support** or **12V**

   Not Support

   Disable the auxiliary power output.

   12V

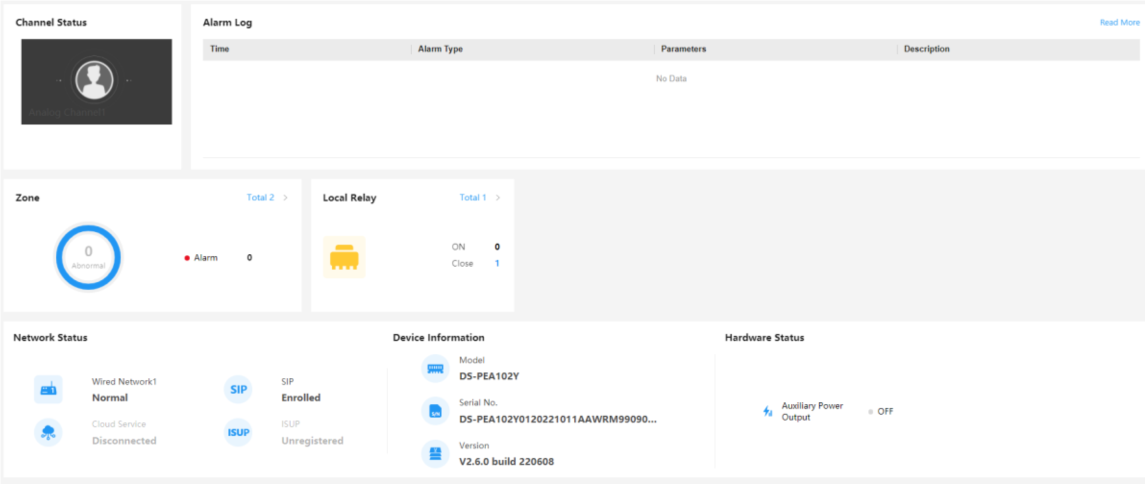
   Enable the auxiliary power output.

3. Click **Save**.

Chapter 4 Web Client Settings

4.1 Live View

You can see channel status, alarm log, zone, local relay, network status, device information, hardware status, etc. on live view page.



Channel Status

Alarm Log

Read More

Time	Alarm Type	Parameters	Description

No Data

Zone — Total 2

0 Abnormal

Alarm 0

Local Relay — Total 1

ON 0

Close 1

Network Status

Wired Network1: Normal

SIP: Enrolled

Cloud Service: Disconnected

ISUP: Unregistered

Device Information

Model: DS-PEA102Y

Serial No.: DS-PEA102Y0120221011AAWRM99090...

Version: V2.6.0 build 220608

Hardware Status

Auxiliary Power Output: OFF

Figure 4-1 Live View Page

4.2 Configuration

4.2.1 System

System Settings – Basic Information

Click **System** → **System Settings** → **Basic Information**.
You can change device name in this page. And you can see device No., Model, Serial NO., version, etc.

System Settings – Time Settings

Click **System** → **System Settings** → **Time Settings**.
Select **Time Zone**.

NTP

Configure **Server Address**, **NTP Port** and **Interval**. The device will periodically synchronize time from the FTP server according to the interval.

Manual Time Sync.

Click **Sync. with computer time**, the computer time will be synced to the device.

Enable **DST**. Configure **Start Time**, **End Time** and **DST Bias.**
Click **Save**.

System Settings – About

Click **System** → **System Settings** → **Time Settings**.
Click **View Licenses** to view open source software licenses.

User Management

Click **System** → **User Management**.
You can see all online users.

4.2.2 Network

Network Settings

Steps

1. Click **Network** → **Network Settings** → **TCP/IP**.
2. Enter **IPv4 Address**, **IPv4 Subnet Mask**, etc., or enable DHCP to get address automatically.
3. Click **Save**.

Network Service

Steps

1. Click **Network** → **Network Service**.
2. Configure port parameters.

Note

- Please do not change the default port parameters at will. When there is a port conflict and you need to change the port number, please change the following information accordingly.

HTTP(S)

- HTTP

The default HTTP port is 80. To change the port, you need to add the changed port number after the address when you log in using the browser. For example, if the HTTP port number changes to 81, you need to enter http://192.168.1.64:81 (The front part of ":" is the current IP address of the device).

- HTTPS

The default HTTPS port is 443. The range is 1 to 65535.

- HTTP Listening

Select **Server Type** as **IP** or **Domain Name**. Enter IP or domain name, URL and port.

RTSP

The default RTSP port is 554. It is the real time transport protocol port. Please ensure that the port you changed is available.

Sever Port

The default server port is 8000. When using the client to log in, if the server port is changed, you need to enter the port number in the login page.

3. Go to **NAT** page, enable UPnP to open the device port.
4. Select **Port Mapping Mode** as **Auto** or **Manual**.

Auto

You do not need to set port mapping on the router. You can open the port only by enabling UPnP.

Manual

When you select Manual and enable UPnP, you need to enter the external port number and enable UPnP on the router to open the port. You do not need to change the port of the device itself.

5. Click **Save**.

Device Access - SIP

After setting the SIP server, the device will be enrolled to the SIP server automatically. The devices under the same SIP server address can communicate with each other.

Click **Network** → **Device Access** → **SIP**.

Private Protocol

Steps

1. Enable SIP.

Enrollment Status

Display the device enrollment status. If the device has been enrolled to the SIP server, it displays **Enrolled**. Otherwise it displays **Not Enrolled**.

2. Select IPv4 or Domain.
3. Set parameters.

Device ID

The device ID can only be set as a number and no more than 6 digits. It is a unique identification of the device, which facilitates the interaction between the panic alarm center station and front-end device.

Device Location

You can enter the device location information with a maximum of 32 characters.

User Information

You can enter **IP**, **Server Port**, **Enrollment Password**, etc.

Local Port

The default local port is 5060.

Enrollment Period

The time interval between devices registering with the SIP server.

4. Click **Save**.

Standard SIP Protocol

Steps

1. Enable SIP.

   Enrollment Status

   Display the device enrollment status. If the device has been enrolled to the SIP server, it displays **Enrolled**. Otherwise it displays **Not Enrolled**.

2. Select IPv4 or Domain.
3. Set parameters.

   User Information

   You can enter **IP**, **Server Port**, **User Name**, **Enrollment Password**, etc.

   Local Port

   The default local port is 5060.

4. Click **Save**.

Device Access – Hik-Connect

Ezviz is a micro video service platform. After enrolling devices to Ezviz platform, you can access the devices through Ezviz.

Steps

1. Click **Network** → **Device Access** → **Hik-Connect**.
2. Enable Ezviz Cloud.

Note

- When it is enabled for the first time, you need to set the verification code.

3. Set **Server Address**. You can select default or custom.
   When **Custom** is checked, you need to set the server address manually. You can contact the technical support to get the address.
4. Set **Network Mode**. The default mode is wired network.
5. Enter the set verification code. The code is a 6-sigit random code used for QR code encryption. It can be set to 6~12 characters and supports English letters (case sensitive) and numbers. It is recommended to combine more than 8 digits of numbers and letters.
6. Click **View** to see the Hik-Connect QR code.
7. Click **Save**.

Device Access - ISUP

ISUP platform refers to Intelligent Security Uplink Protocol.

Steps

1. Click **Network** → **Device Access** → **ISUP**.
2. Enable ISUP.
3. Select **Protocol Version** as **Ehome2.0** or **ISUP5.0**.
4. Select **Server Type** as **IPv4** or **Domain**.
5. Set parameters.

   Port

   The default port number is 7660. The range is 2000 to 65535.

Device ID

The device ID number can only be set as a number and no more than 6 digits. The ID is the unique identification of the device, which facilitates the interaction between the panic alarm center station and front-end device.

6. Click **Save**.

Alarm Communication

Steps

1. Click **Network** → **Alarm Communication**.
2. Enable Wired Network and set parameters.

Notify Surveillance Center

Each network card only supports one upload center, which is Wired Network1 by default.

Server Type

Address type of central server. You can select as **IPv4** or **Domain**.

IP/Domain

Enter the IP address or domain name of the server according to the set server type.

Port

The central port number. The HIK protocol is 7200 by default. The NAL2300 protocol should be set as 4001.

Protocol

The default protocol is HIK Protocol.

User Name

It supports numbers and letters. The HIK protocol can set the length range to 6~9 digits. The NAL2300 protocol can set the length range to 6 digits.

3. Click **Save**.

4.2.3 Video/Audio

Configure the video and audio parameters of the channels.

Video

Click **Video/Audio** → **Video** to set video parameters, which will take effect after saving.

Stream Type

You can select **Main Stream** or **Sub-Stream** to see the live view. The default type is main stream.
Main stream is used for high-definition storage and preview.
Sub-stream is used for standard definition storage and preview when the network bandwidth is insufficient.

Video Type

You can select **Mixed Flow** or **Video Flow**. The default is mixed flow, that is, the video contains sound and pictures. If you do not need sound, you can select video flow.

Resolution

Select according to the requirements of video definition. The higher the resolution, the higher the network bandwidth required.

Bit Rate Type

You can select **Constant Bit Rate** or **Variable Bit Rate**. The default is constant bit rate. If constant bit rate is selected, you need to select a fixed rate value; if variable bit rate is selected, you need to select a limit value of the rate.

Image Quality

You can select different levels of image quality according to your requirements. The higher the quality, the higher the network bandwidth required. When the bit rate is constant bit rate, the image quality can not be selected by default.

Frame Rate

Display the number of frames per second of the video. According to the bandwidth settings, the higher the frame rate, the higher network bandwidth required, and the higher the storage space required.

I Frame Interval

The number of frames between the two key frames. The larger the I frame interval is, the smaller the code stream fluctuation is, but the image quality is relatively poor. On the contrary, the larger the code stream fluctuation is, the higher the image quality is. It is recommended to use the default value.

Video Encoding

The default video encoding type is H.264.

SVC Encoding

It is an expandable video encoding technology. The SVC function can be used to extract frames for video recording to reduce storage space. The video files after frame extraction still support normal decoding. When the SVC function is enabled, the storage device and the decoding device should all support this function. When the SVC function is selected as automatic, the device will adapt to the current network environment and decide whether to send frames to ensure that the image can be previewed normally.

Video&Audio Encoding

The video and audio encoding type supported by the current device. When the stream type is the main stream, the types are G.711ulaw, AAC, PCM; The sub-tream is consistent with the main stream.

Audio

Steps

1. Click **Video/Audio** → **Audio**.
2. Set parameters.

Audio Encoding

The current device supports G.711ulaw, AAC, OPUS, PCM and ADPCM.

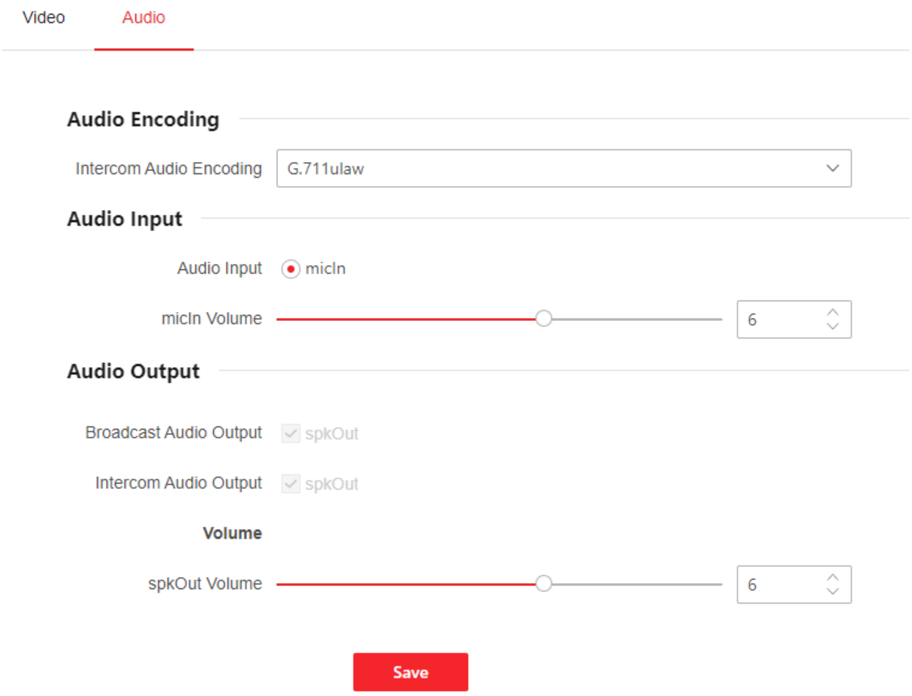
Audio Input

The input type is micIn by default. You can set the volume.

Audio Output

The output type is spkOut. You can set the volume.

3. Click **Save**.



Audio Encoding

Intercom Audio Encoding: G.711ulaw

Audio Input

Audio Input: ● micIn

micIn Volume: 6

Audio Output

Broadcast Audio Output: ☑ spkOut

Intercom Audio Output: ☑ spkOut

Volume

spkOut Volume: 6

Figure 4-2 Audio Parameters

4.2.4 Image

Steps

1. Click **Image** → **OSD Settings**.
2. Set parameters.

Change Display Position

Drag the red box on the preview interface to change the position of the displayed information. After saving, the displayed information will be updated to a new position.

Change Display Format

- Date Format

You can select the date display format in the date format drop-down box.

- Time Format

You can select **24-hour** or **12-hour** format in the time format drop-down box.

- Display Mode

According to whether the display information is transparent or flashing, there are four freely combined display mode for selection. For example, if the display mode is transparent and flashing, the information will be displayed with a certain transparency and will flash.

- OSD Size

You can select the font size in the OSD size drop-down box.

- Alignment

You can select **Align Left**, **Custom**, **Align Right** or **International Mode** in the alignment drop-down box.

Change Display Content

You can select the display content on the image, including the channel name, date and week, or change the channel name and add customized display content.

- Display Content

Select whether to display the name, date or week according to your need. After selecting, the corresponding information will be displayed on the image.

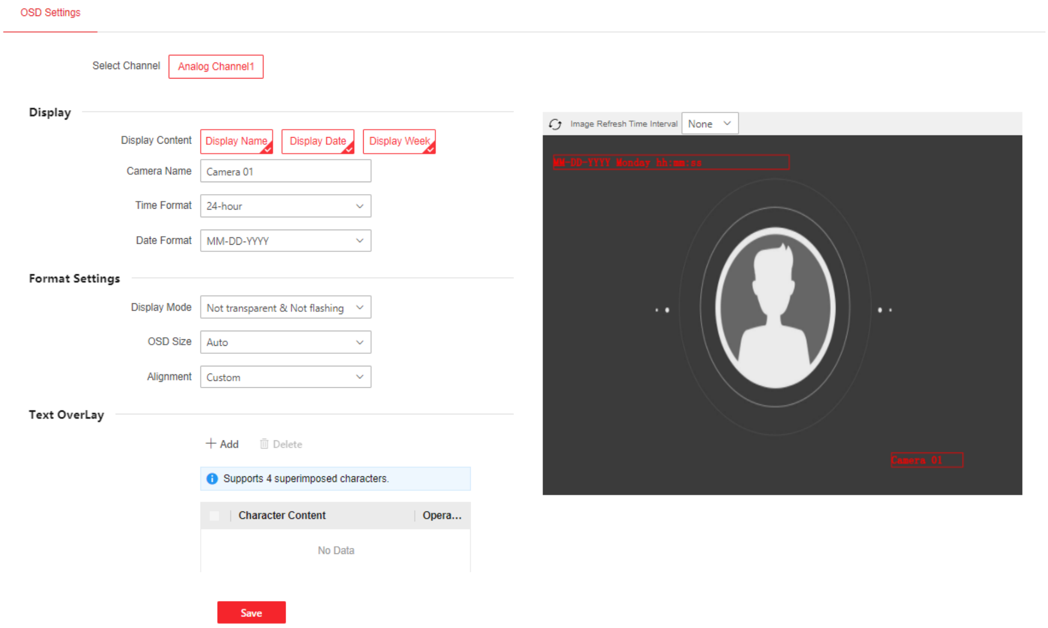
- Channel Name

You can change the channel name in the channel name text box.

- Custom

In the Text Overlay interface below, click **+Add**, and the text input box will appear. Enter content, and the customized content will be displayed in the image.

3. Change the image refresh time interval above the screen.



OSD Settings

Select Channel: Analog Channel1

Display

Display Content: Display Name, Display Date, Display Week

Camera Name: Camera 01

Time Format: 24-hour

Date Format: MM-DD-YYYY

Format Settings

Display Mode: Not transparent & Not flashing

OSD Size: Auto

Alignment: Custom

Text OverLay

Supports 4 superimposed characters.

Character Content	Opera...
No Data	

Figure 4-3 OSD Settings

4.2.5 Device

Zone Settings

Steps

1. Click **Device** → **Zone**.
2. Click ✎ to enter the **Zone Settings** page.
3. Set parameters.

Detector Type

Type of zone detector.

Zone Type

- Instant

Under the arming status, as long as the detector connected to the zone is triggered, the alarm controller will immediately generate an alarm without delay.

- Fire

The fire zone is a 24-hour alarm zone. When the fire zone is triggered, the external sounder will give a fire alarm sound.

- 24H Silent Zone

Detectors working in this zone are on alert for 24 hours, and will not be affected by arming and disarming operations. Once triggered, they will immediately transmit information to the command center, but there is no alarm sound.

- Disabled

No event will trigger an alarm.

Audio File

Select the zone audio file. Mute can be selected.

Upload Restored Alarm

After enabling, when the alarm is recovered, the report will be uploaded to the center.

4. Check the **Link Relay**, **Linked Channel**, etc.
5. (Optional) Click **Copy to**, copy the zone parameters to other zones.
6. Click **Save**.

Relay Settings

Steps

1. Click **Device** → **Relay**.
2. Click ✎ to set relay parameters.

Output Delay

After the zone event is triggered, the relay will close the relay output after the output delay. The setting range is 0 to 2000 seconds.

3. Click **Save**.
4. Check the relay, click **ON** or **OFF** to open or close the relay.

Auxiliary Power Output

Steps

1. Click **Device** → **Auxiliary Power Output**.
2. Enable **Switch of Auxiliary Power Output**.
3. Click **Save**.

4.2.6 Two-way Audio Settings

Calling Settings

Steps

1. Click **Two-way Audio Settings** → **Calling Settings**.

2. Configure parameters.

Call Timeout

Refers to the playing time of the call prompt tone. The range is 40 to 60 seconds.

Call Extension Time

When you press the call wait during calling the panic alarm center station, the extension time of the prompt tone based on the maximum ringing time is call extension time. The range is 10 to 60 seconds.

3. Click **Save**.

Voice Prompt

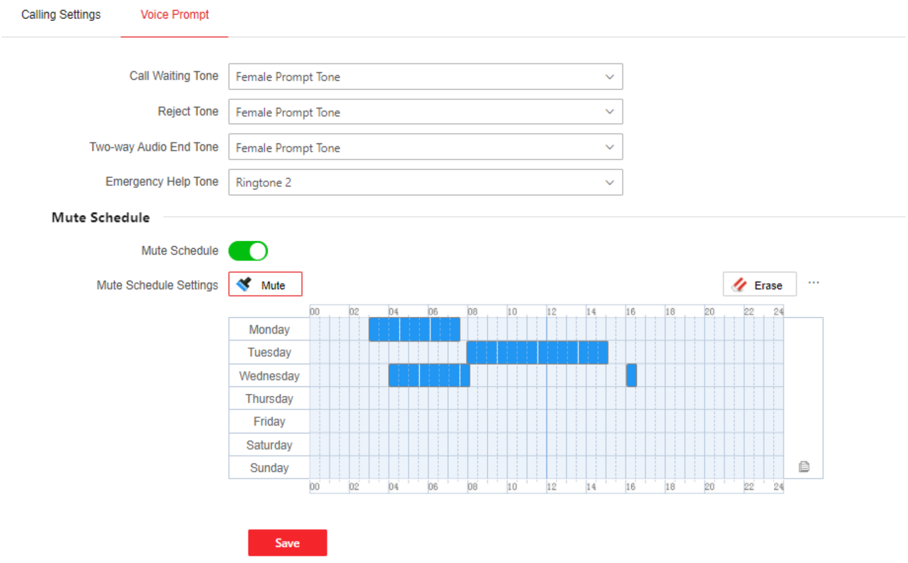
Steps

1. Click **Two-way Audio Settings** → **Voice Prompt**.

2. Configure **Call Waiting Tone**, **Reject Tone**, **Two-way Audio End Tone**, **Emergency Help Tone**.

3. Enable **Mute Schedule**.

4. Click Mute, move the mouse over the time bar, and long press and drag the left mouse button to draw the time period.



Calling Settings | Voice Prompt

Call Waiting Tone: Female Prompt Tone

Reject Tone: Female Prompt Tone

Two-way Audio End Tone: Female Prompt Tone

Emergency Help Tone: Ringtone 2

Mute Schedule

Mute Schedule: ●

Mute Schedule Settings

Figure 4-4 Mute Schedule Settings

5. Edit the time period.

Edit Time Period Length and Start/End Time

Click the drawn time period to adjust the start/end time in the pop-up window.

Delete Time Period

Click **Erase**, long press and drag the mouse on the drawn time period to erase.

Delete All Time Period

Click **…** → **Clear All**, you can delete all drawn time period.

Copy Time Period

Move the mouse to the time bar, click 🗐 in the right of the day, and select time period to copy to that day. Click **OK** to save.

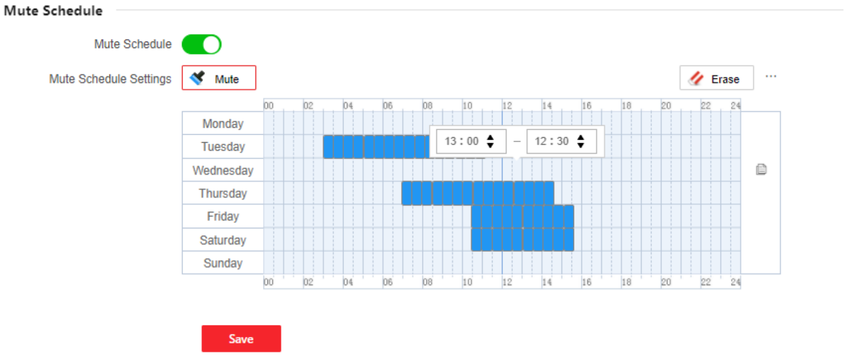


Figure 4-5 Edit Mute Schedule

6. Click **Save**.

4.2.7 Custom

Remote upload audio files to SD card with storage space.

Steps

1. Click **Custom**.

2. Click **Import**, select the file address in the pop-up window and import.

Note

- Audio file is .wav or .mp3 format, the file name can be composed of English characters, numbers and Chinese characters, and does not contain spaces at the beginning and end. The length of the file name (including the suffix of 4 bytes) is up to 31 English characters (9 Chinese characters). The symbols that cannot be included in the file name are:\/* “ ” <>|.
- The maximum size of each audio file is 2MB.
- Uploading audio files with the same name will overwrite the audio files before.

3. Check audio files to be deleted, Click **Delete**, all the checked files will be deleted.

Note

- Multiple files can be deleted for batch deletion.
- After deleting the audio file in SD card, and use the function of the file, the name will recover

to the default audio file.

4.3 Maintenance and Security

4.3.1 Maintenance

Reboot

Click **Maintenance and Security** → **Maintenance** → **Reboot** to restart the device manually.

Upgrade

Steps

Click **Maintenance and Security** → **Maintenance** → **Upgrade**. Click 🗀, select the upgrade file. Click **Upgrade**.

Note

- When upgrading an unmatched upgrade file, the upgrade fails and remains the same as before.
- During the upgrade process, do not power off the device.

Backup and Reset

Click **Maintenance and Security** → **Maintenance** → **Backup and Reset**.

Export

Click **Export** to export configuration file, which includes device parameters.

Restore to Default Settings

Click **Restore**, device parameters except for IP address will restore to default settings.

Restore to Factory Settings

Click **Default**, all device parameters will restore to default settings, and you need to activate the device when you use it again.

Import Parameters

Select file and click **Import**, the configuration file will be imported to device.

Log

Click **Maintenance and Security** → **Maintenance** → **Log**, set **Major Type**, **Minor Type** and **Select Time**, click Search, the query results will be shown.

Security Audit Log

Click **Maintenance and Security** → **Maintenance** → **Security Audit Log**, enable **Log Upload Server**. Configure **Log Server IP** and **Log Server Port**, and import **CA Certificate**.

Audio&Video Self-Test

Click **Maintenance and Security** → **Maintenance** → **Audio&Video Self-Test**, set manual test or auto test.

Auto Test

Audio and video self-test will be automatically performed according to the set detection time.

Restore to Default Settings

Click **Test**, the results will be shown in the result table.

Test Result	Note
Normal	Video/audio input /audio output signal is normal.
Exception	Video/audio input /audio output signal is lost.
Unknown	Audio input fails. It is unable to detect audio output status.

4.3.2 Security

IP Address Filter

Steps

1. Click **Maintenance and Security** → **Security** → **IP Address Filter**.
2. Enable filter, click **+Add** to add IP address to the list.
3. Click ✎ to change IP address. Click 🗑 to delete address.
4. Click **Save**.

Block List

The IP address in this list will be blocked. Other IP address can communicate normally.

Allow List

Only the IP address in this list can communicate normally. Other IP address will be blocked.

Note

- You can only enable one kind of list.

Security Service

Click **Maintenance and Security** → **Security** → **Security Service**.

Enable **SSH**, and click **Save**.

Note

- SSH is used for remote debugging. For your safety, it is recommended to disable SSH when it is not needed.

Locking User

Steps

1. Click **Maintenance and Security** → **Security** → **Locking User**.

2. Enable **Locking**, set parameters.

   Max. Failure Attempts

   The default setting is 7 times, and the setting range is 3 to 10.

   Locking Duration

   The default setting is 600 seconds, and the setting range is 10 to 3600.

3. Click **Save**.

Note

- If you enter the wrong password more than the set number of times, the IP address of the login terminal of the locked user will be displayed in the list.

4. (Optional) The user can be unlocked through the following operations.

Click 🔓 to unlock the locked user in the list.

Click 🔓 **Unlock All** to unlock all locked users.

Chapter 5 Communication Matrix and Device Command

Scan the QR code to get the communication matrix and device command

See Far, Go Further