



# Non-Visible Panic Alarm Station

Configuration Guide

## Legal Information

©2021 Hangzhou Hikvision Digital Technology Co., Ltd. All rights reserved.

### 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 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 INSPECTION, 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 ANY PROHIBITED END-USES, INCLUDING THE DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR

## Non-Visible Panic Alarm Station Configuration Guide




---

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.

## Symbol Conventions

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

Symbol	Description
 <b>Danger</b>	Indicates a hazardous situation which, if not avoided, will or could result in death or serious injury.
 <b>Caution</b>	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
 <b>Note</b>	Provides additional information to emphasize or supplement important points of the main text.

## 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, 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](http://www.recyclethis.info)

# Contents

<b>Chapter 1 Overview</b> .....	<b>1</b>
<b>Chapter 2 Activation</b> .....	<b>2</b>
<b>2.1 Activate via SADP</b> .....	<b>2</b>
<b>2.2 Activate Device via Client Software</b> .....	<b>3</b>
<b>Chapter 3 Remote Settings</b> .....	<b>5</b>
<b>3.1 Device Management</b> .....	<b>5</b>
<b>3.1.1 Add Device to the Client Software</b> .....	<b>5</b>
<b>3.1.2 Edit Network Parameters</b> .....	<b>6</b>
<b>3.2 Network Configuration</b> .....	<b>6</b>
<b>3.2.1 Basic Settings</b> .....	<b>6</b>
<b>3.2.2 Set DNS</b> .....	<b>8</b>
<b>3.2.3 Set NAT</b> .....	<b>8</b>
<b>3.2.4 Set Alarm Center</b> .....	<b>10</b>
<b>3.2.5 Set SIP</b> .....	<b>11</b>
<b>3.2.6 Set Hik-Connect</b> .....	<b>13</b>
<b>3.2.7 Access the Platform</b> .....	<b>14</b>
<b>3.2.8 Set Intercom Parameters</b> .....	<b>15</b>
<b>3.2.9 Set Integrate Protocol Parameters</b> .....	<b>16</b>
<b>3.3 Alarm Settings</b> .....	<b>17</b>
<b>3.3.1 Set Zone</b> .....	<b>17</b>
<b>3.3.2 Set Relay</b> .....	<b>19</b>
<b>3.3.3 Set Call Waiting</b> .....	<b>20</b>
<b>3.3.4 Set Voice Prompt</b> .....	<b>21</b>
<b>3.4 Alarm Management</b> .....	<b>23</b>
<b>3.4.1 Manage Relay</b> .....	<b>23</b>
<b>3.4.2 Manage Audio Input/Output</b> .....	<b>23</b>
<b>3.4.3 Manage Siren</b> .....	<b>24</b>
<b>3.4.4 Manage Audio File</b> .....	<b>25</b>
<b>3.5 Event Settings</b> .....	<b>26</b>

## Non-Visible Panic Alarm Station Configuration Guide

---

<b>3.5.1 Set Audio Exception Detection</b> .....	26
<b>3.6 Video &amp; Audio Settings</b> .....	28
<b>3.6.1 Video &amp; Audio Settings</b> .....	28
<b>3.6.2 Set Display</b> .....	30
<b>3.6.3 Set Image Parameters</b> .....	31
<b>3.6.4 Set Intercom Audio</b> .....	31
<b>3.7 System Settings</b> .....	32
<b>3.7.1 Set Time</b> .....	32
<b>3.7.2 Set System Parameters</b> .....	33
<b>3.7.3 Set Security</b> .....	33
<b>3.7.4 Set Password</b> .....	34
<b>3.7.5 Set User</b> .....	35
<b>3.7.6 Search for Log</b> .....	35
<b>3.7.7 Maintain the System</b> .....	36
<b>3.7.8 Check Video &amp; Audio Status</b> .....	38
<b>3.7.9 Security Audit Log</b> .....	39
<b>3.8 Check Status</b> .....	40
<b>3.8.1 Check Zone Status</b> .....	40
<b>3.8.2 Check Relay Status</b> .....	40
<b>3.8.3 Check Siren Status</b> .....	40

## Chapter 1 Overview

### Description

DS-PEA101 series of active panic alarm station has 1-channel alarm input and 1-channel alarm output. It supports center call, two-way video intercom, real-time monitoring, first time alarm help and audio anomaly detection. It can provide faster and more effective services for the society, effectively deter criminals, reassure the public, and stabilize the society.

The device is mainly used in hospitals, scenic spots, communities and prisons etc.



## 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.

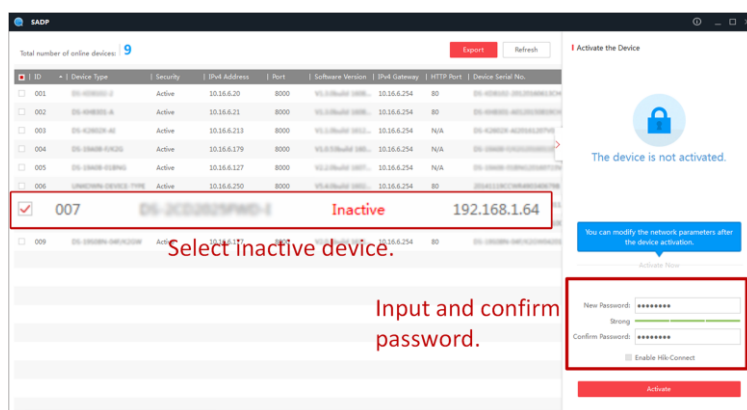


Figure 2-1 SADP Page

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.
- Get the Guarding Vision client software from the supplied disk. 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. Optional: Click , select the **Cloud P2P Region**, and login the Cloud P2P account.

---

### Note


- For the first use, you need to register a cloud P2P account.
  - After logging in, you can store your device on the cloud.
- 

3. Enter **Device Management** → **Device** in the **Maintenance and Management** list.
  4. Click **Online Device**.
  5. Check the device status from the online device list, and select an inactive device.
  6. Click **Activate**.
  7. 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.

---


8. Click **OK** to start activation.  
Device status will change to **Active** after successful activation.
  9. Edit IP address of the device.
    - 1) Select a device and click  on the online device list.
-

## Non-Visible Panic Alarm Station Configuration Guide

---

- 2) Change the device IP address to the same subnet with your computer and set port number as 80.
- 3) Enter the admin password of the device and click **OK** to complete modification.
10. 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 go to **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 to the 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.

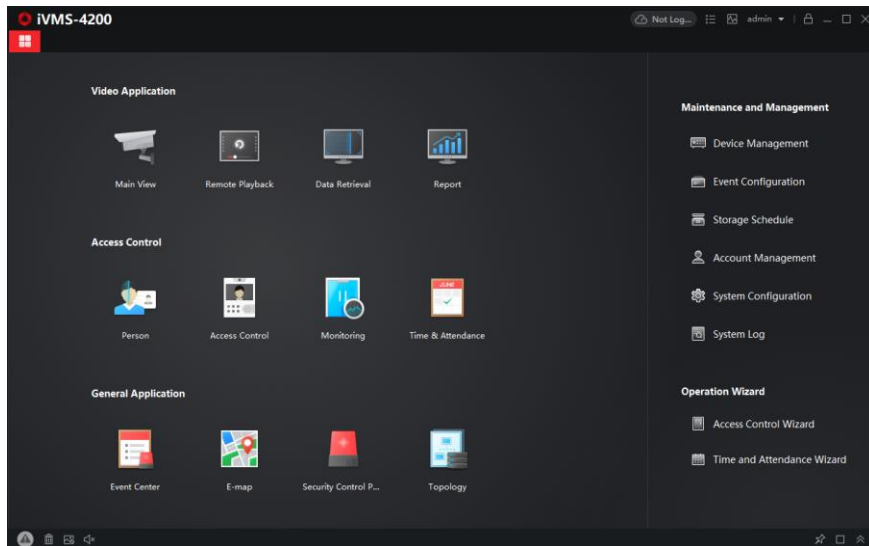


Figure 3-1 Client Software Main Page

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**.

---

#### **Note**

The port No. is 8000.

---

3. Check **Import to Group**.
4. 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, the client software, or the device. 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 Basic Settings

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.

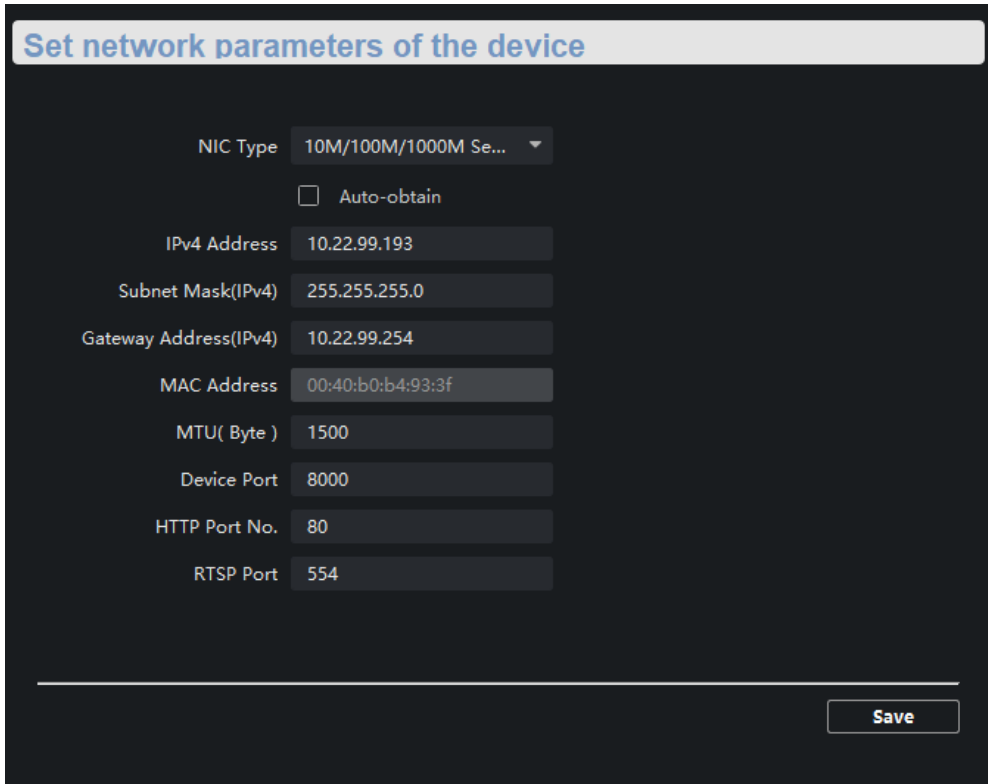
### Steps

#### Note

The network mode is multiple networks mode, you can set the basic network parameters for NIC 1 and NIC 2.

---

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



Set network parameters of the device	
NIC Type	10M/100M/1000M Se... ▾
<input type="checkbox"/>	Auto-obtain
IPv4 Address	10.22.99.193
Subnet Mask(IPv4)	255.255.255.0
Gateway Address(IPv4)	10.22.99.254
MAC Address	00:40:b0:b4:93:3f
MTU( Byte )	1500
Device Port	8000
HTTP Port No.	80
RTSP Port	554
<input type="button" value="Save"/>	

Figure 3-2 Network Basic Settings Page

2. Select the NIC and 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)**, **Gateway Address (IPv4)**) through DHCP.

#### Note

NIC 1 and NIC 2 are independent of 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**, **RTSP port** for the device.

#### **MTU(Byte)**

---

## Non-Visible Panic Alarm Station Configuration Guide

---

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 1024 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.

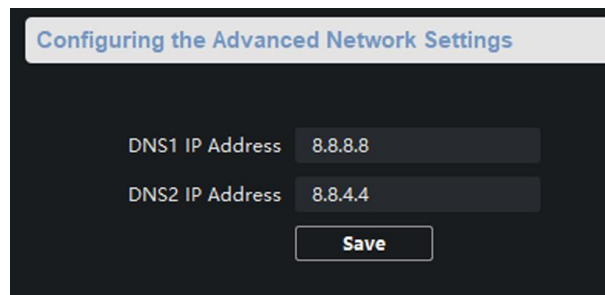


Figure 3-3 DNS Setting Page

---

### 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

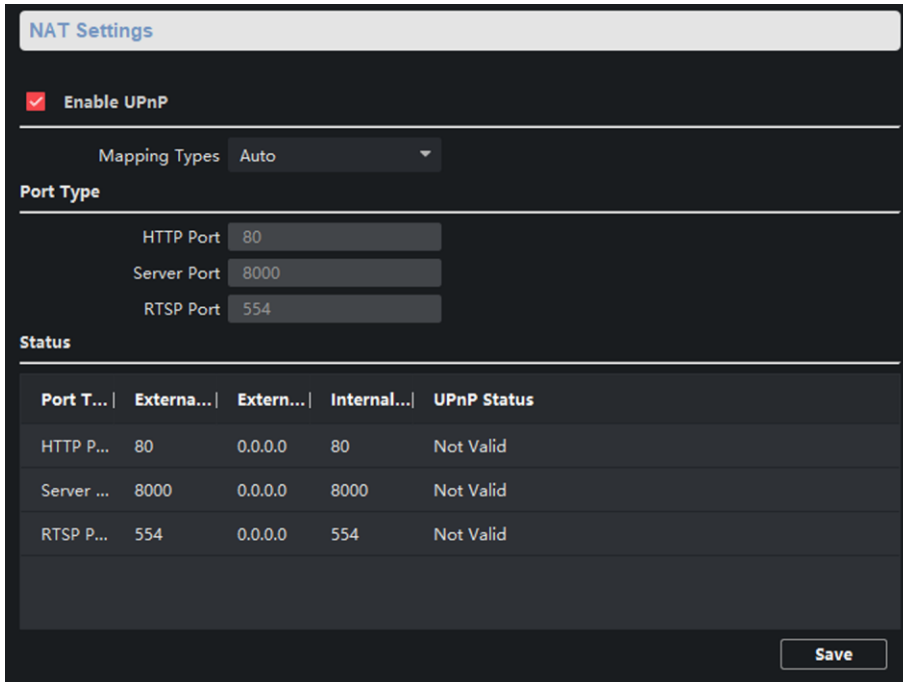
---

#### 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**.



Port T...	Externa...	Extern...	Internal...	UPnP Status
HTTP P...	80	0.0.0.0	80	Not Valid
Server ...	8000	0.0.0.0	8000	Not Valid
RTSP P...	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. If the value is changed, you need to add

---



## Non-Visible Panic Alarm Station Configuration Guide

---

the modified port number to the address when you log in using the browser. For example, when the HTTP port number is changed to 81, you need to enter ***http://192.168.1.64:81*** when you log in using a browser.

### 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.


---

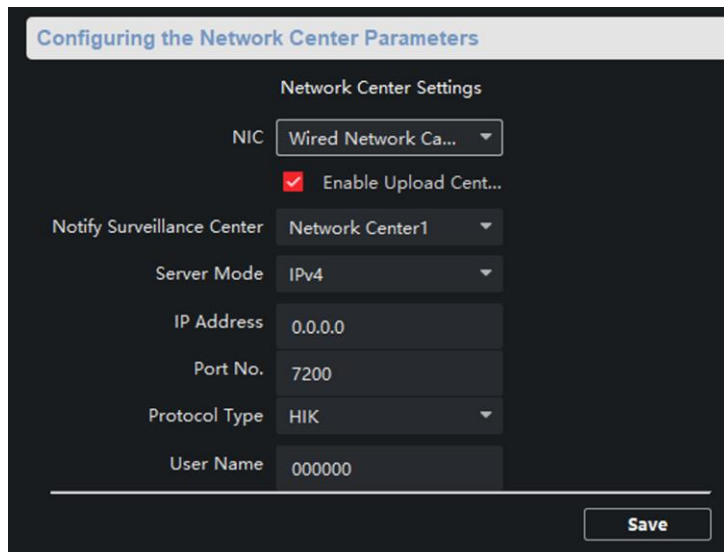
3. Click **Save** to save the settings.

## 3.2.4 Set 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**.



Network Center Settings	
NIC	Wired Network Ca... ▼
	<input checked="" type="checkbox"/> Enable Upload Cent...
Notify Surveillance Center	Network Center1 ▼
Server Mode	IPv4 ▼
IP Address	0.0.0.0
Port No.	7200
Protocol Type	HIK ▼
User Name	000000

Save

Figure 3-5 Alarm Center Configuration

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.



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

---

4. Click **Save**.

### 3.2.5 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



You can also configure the SIP server parameters locally.

---

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

---



The SIP parameters need to be configured will vary as the selected intercom protocol type. For intercom protocol settings, please see **Set Intercom Parameters**.

---

**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

Figure 3-6 SIP Setting Page (Private Protocol)

**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 3-7 SIP Setting Page (SIP Protocol)

### Registration Status

Display the status of the device registers to the SIP server.

2. Select the **Server** as **IP Address** or **Domain Name**.
3. According to the selected address type, enter the IP address or domain name of the SIP server.
4. Set the **Server Port** and the **Local Listening Port**.

### Server Port

The SIP server port. By default, the server port of SIP protocol is 5060, and the server port of private SIP protocol is 5065. The available port number should be between 1024 and 65535.

### Local Listening Port

The local port of the device SIP function. By default, it is 5060, the available server port number should be between 1024 and 65535.

5. Configure the SIP parameters according to the selected intercom protocol.
  - If configuring the SIP parameters based on Private Protocol, please set the **Device ID**, **Device Local Information**, **Local Listening Port**, **Register Period (min)** and **Network Type**.
  - If configuring the SIP parameters based on SIP Protocol, please enter the **Register User Name**, **Registration Password** and **Target User Name**.

### Device ID

Device ID is the unique identification of the device, facilitating the communication between the devices.

### Device Local Information

You can enter the position information of the device for easy management.

### Register Period (min)

The interval that the device continuously registers to the SIP server, the register period ranges from 1 to 30 (min).

### Network Type

Select the **Network Type** as **Wired Network 1**, **Wired Network 2** or **Wireless Network**.

---

#### Note

When you select a wired network, the wired network is used regardless of whether the wired network is normal; when you select a wireless network, only the wireless network is used.

---

### Register User Name

The user name which the device registers to the SIP server.

### Registration Password

The password which the device registers to the SIP server.

### Target User Name

The user name of the user which the device calls.

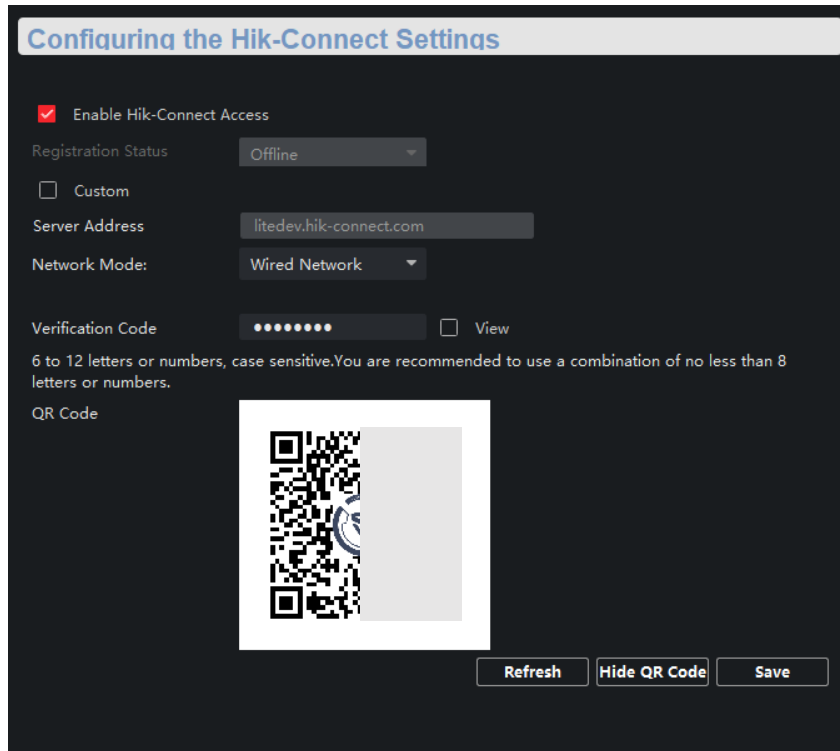
6. Click **Save**.

## 3.2.6 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

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.

QR Code

Refresh Hide QR Code Save

**Figure 3-11 Hik-Connect Service Setting Page**

2. Check **Enable Hik-Connect Access** 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*.

---

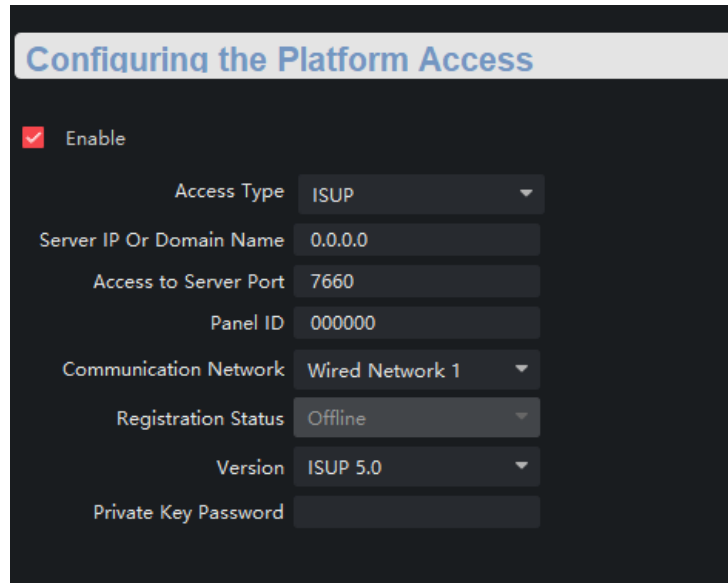
4. Select **Network Mode**.
5. Enter a verification code and click **Generate QR code**.  
There will be a QR code displaying on the page.
6. Click **Save**.
7. Scan the QR code via Hik-Connect and the device will be added to Hik-Connect.

### 3.2.7 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**.



**Figure 3-12 Platform Access Configuration**

2. Check **Enable** 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. The device ID length ranges from 6 to 9.

### **Communication Network**

Select the network mode for communication with platform.

### **Registration Status**

Display the status which the device registers to the platform.

### **Private Key Password**

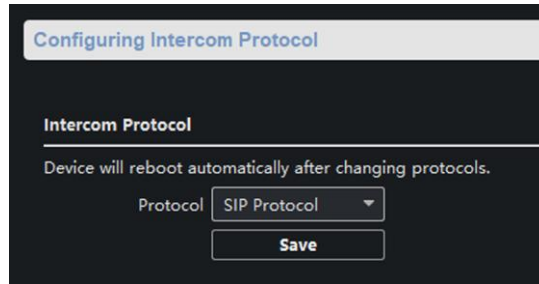
Enter the private key password.

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

## **3.2.8 Set Intercom Parameters**

### **Steps**

1. Click  to enter the **Remote Configuration** page, go to **Network** → **Intercom Protocol**.



**Figure 3-13 Intercom Parameters Configuration**


2. Select the **Protocol** as **SIP Protocol** or **Private Protocol**.
3. Click **Save**.

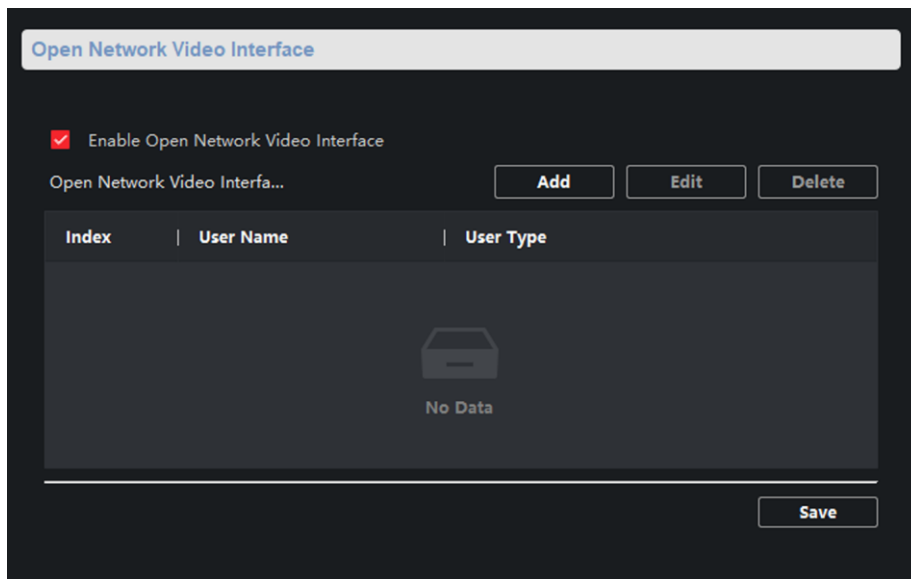
The device will reboot automatically after switching the protocol successfully.

### 3.2.9 Set Integrate Protocol Parameters

If you need to access to the device through ONVIF protocol, you can configure the ONVIF user to enhance the network security.

#### Steps

1. Click  to enter the **Remote Configuration** page, go to **Network** → **Open Network Video Interface**.



**Figure 3-14 Open Network Video Interface**

2. Check **Enable Open Network Video Interface**.
3. Click **Add** to configure the user.
4. Edit the users.

**Delete** Delete the selected user(s).

**Edit** Edit the selected user(s).

5. 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

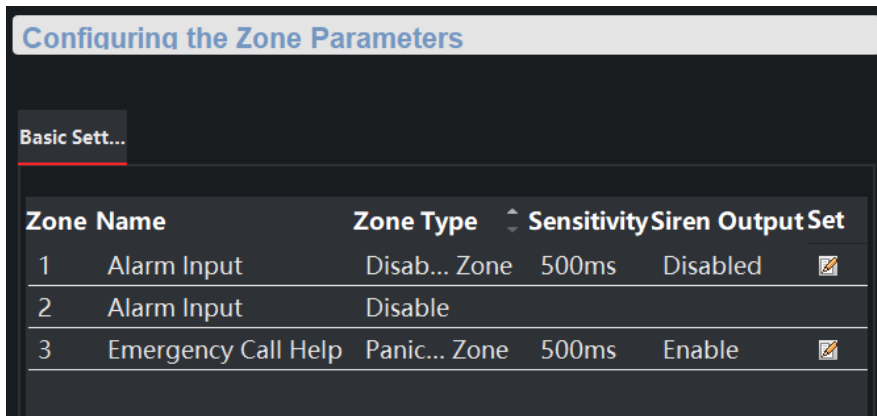
---



#### 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.
2. Click  to enter the **Remote Configuration** page, go to **Input Settings**→ **Zone**.

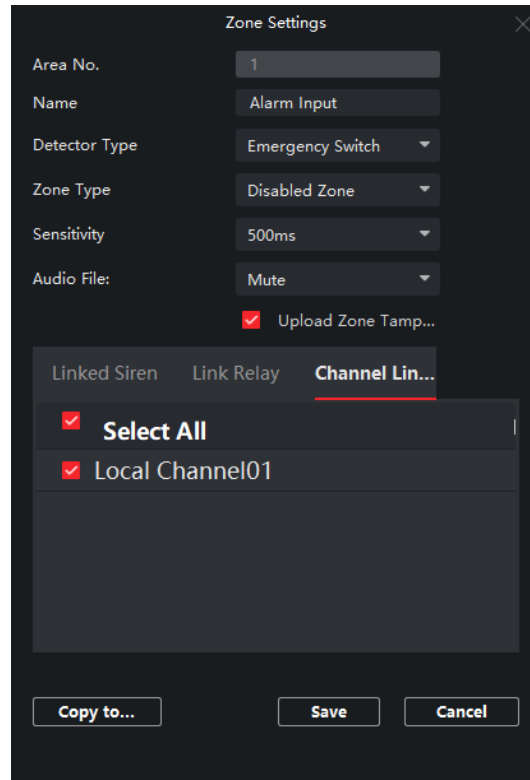


	Zone Name	Zone Type	Sensitivity	Siren Output Set
1	Alarm Input	Disab... Zone	500ms	Disabled 
2	Alarm Input	Disable		
3	Emergency Call Help	Panic... Zone	500ms	Enable 

**Figure 3-16 Zone Configuration Page**

3. Select an zone, click .





**Figure 3-17 Set Zone Parameters**

#### 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.

### 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 Siren** After the zone is triggered, the selected siren sounds.

**Linked Relay** After the zone is triggered, the selected trigger outputs.



#### Note

The relay output can set the output delay time, that is, when the zone is triggered, the trigger outputs a signal, and the trigger will turn off the output after the output delay time ends. Please refer to the user manual for the output delay time setting.

**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.

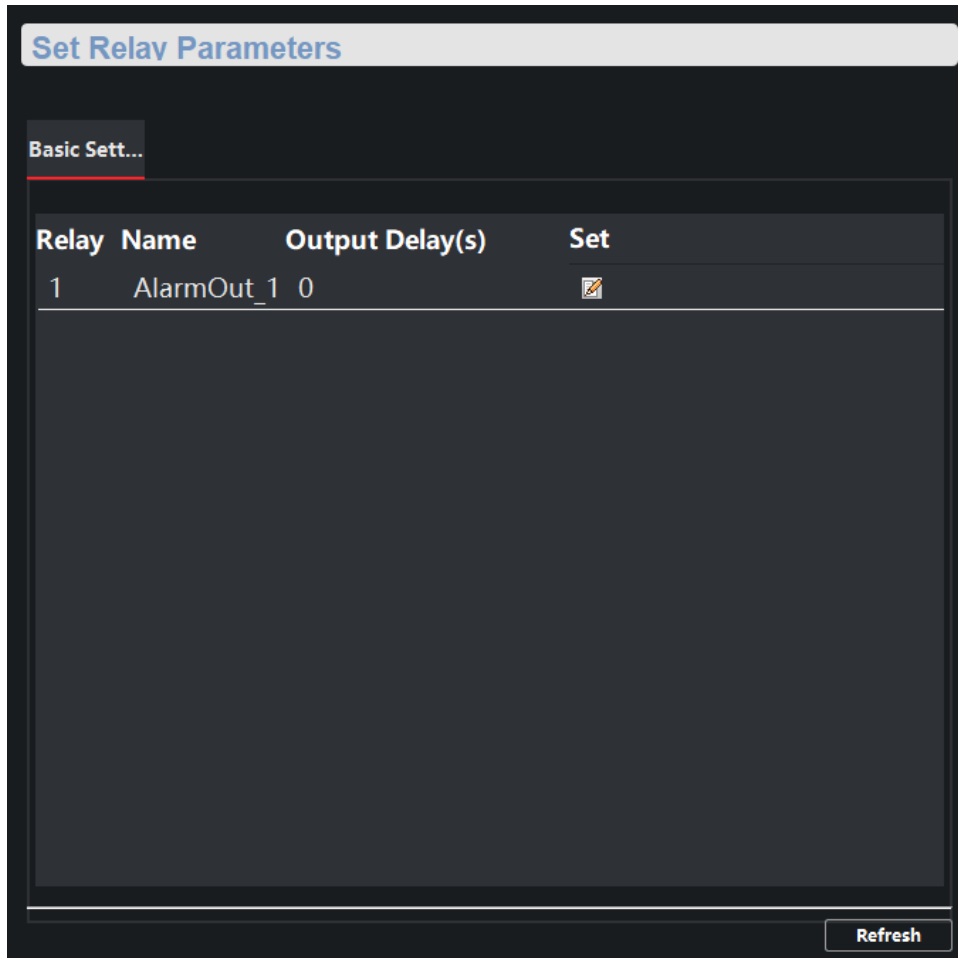


Figure 3-18 Relay Configuration Page

### 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**.

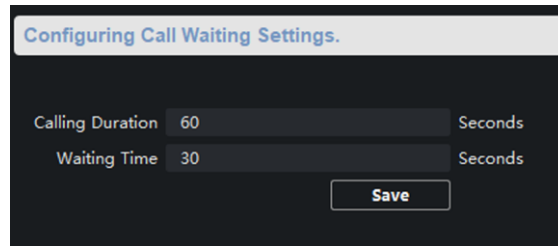
4. Optional: Click **Copy to...**, you can copy the relay settings to other relays.

### 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**.



**Figure 3-19 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**

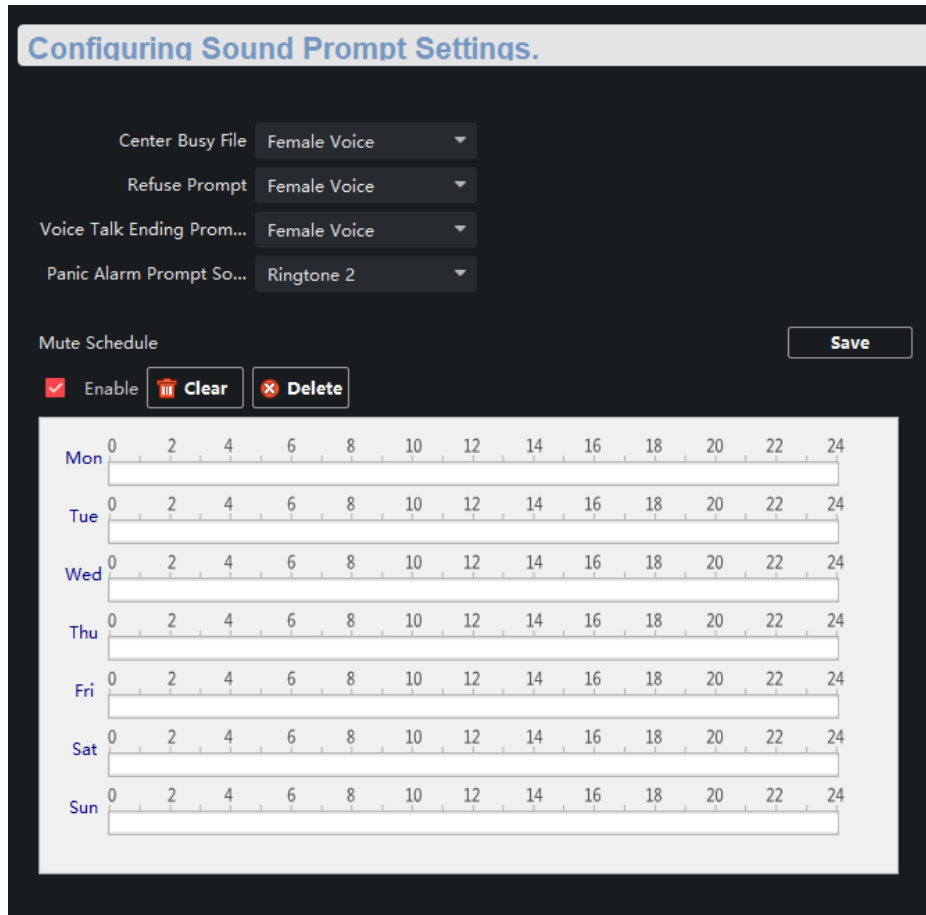
The extended playback time of the prompt tone based on the maximum ring time when calling the master station and pressing the call waiting button, can be set from 10 seconds to 60 s.

3. Click **Save**.

## **3.3.4 Set Voice Prompt**

### **Steps**

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



**Figure 3-20 Voice Prompt Configuration Page**

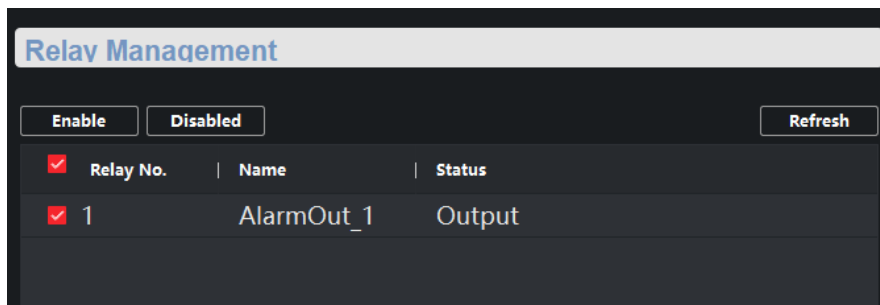
2. Set the **Center Busy File**, **Refuse Prompt**, **Voice Talk Ending Prompt** and **Panic Alarm Prompt Sound**.
  3. Optional: Configure the mute program.
    - 1) Check **Enable** to enable the mute program.
    - 2) Click and drag the mouse on the time bar to draw the scheduled time period.
    - 3) Optional: 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**




**Figure 3-21 Relay Management Page**

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**.

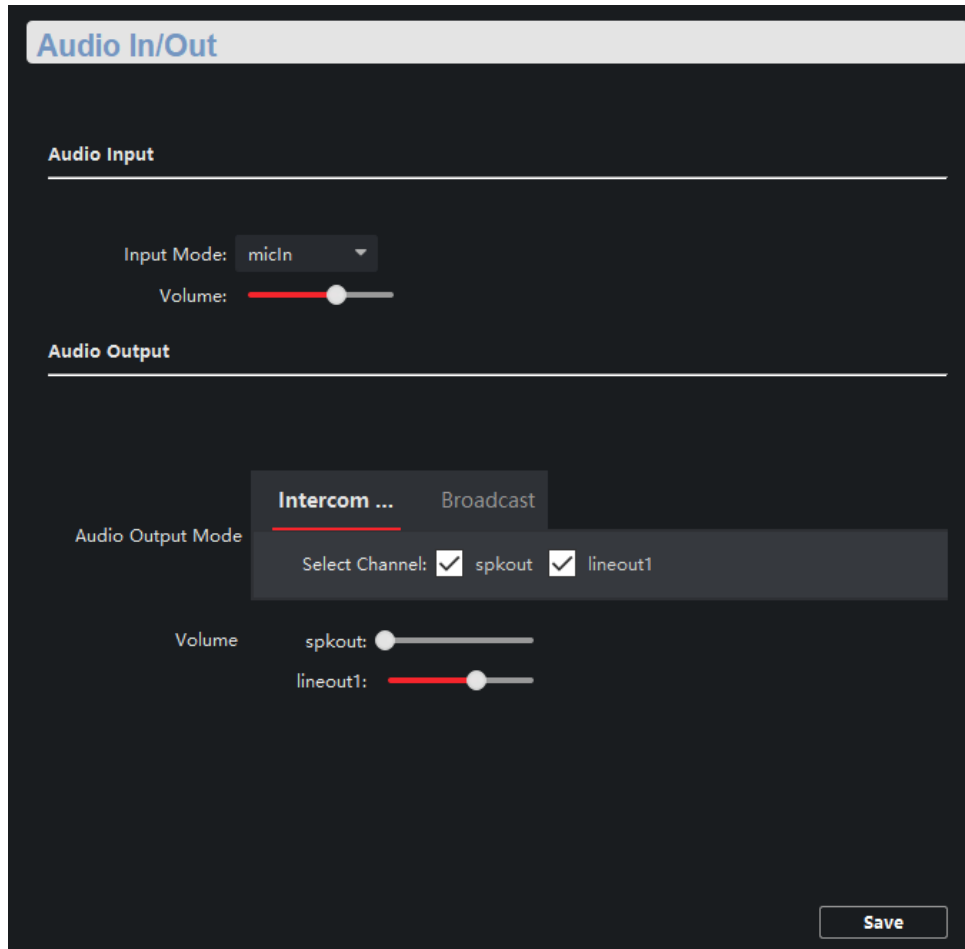


Figure 3-22 Alarm Input/Output Configuration Page

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

---

### Note

- **micIn/ spkOut** is the device's own audio input/output. **lineOut1** is a 3.5mm hole interface, which can connect to the external microphones and speakers. The device defaults to **micIn** and **spkOut**.
  - In the audio output mode, the volume of **spkOut** and **lineOut1** can be set independently.
  - The volume range is 0-10, and the default volume is 6.
- 

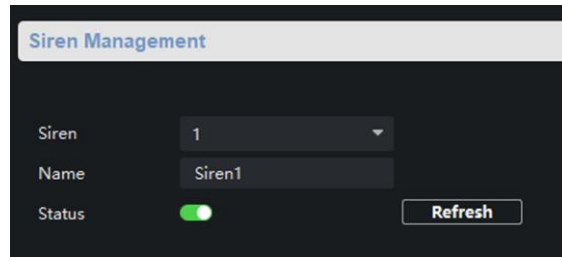
3. Click **Save**.

### 3.4.3 Manage Siren

Open/Close the siren via the client software.

#### Steps

1. Click  to enter the **Remote Configuration** page, go to **Alarm Management** → **Siren**.



**Figure 3-23 Siren Management Page**

2. Select a siren and enable **Status** to open the siren, or disable **Status** to close the siren.
3. Optional: Click **Refresh** to refresh the siren status.

### 3.4.4 Manage Audio File

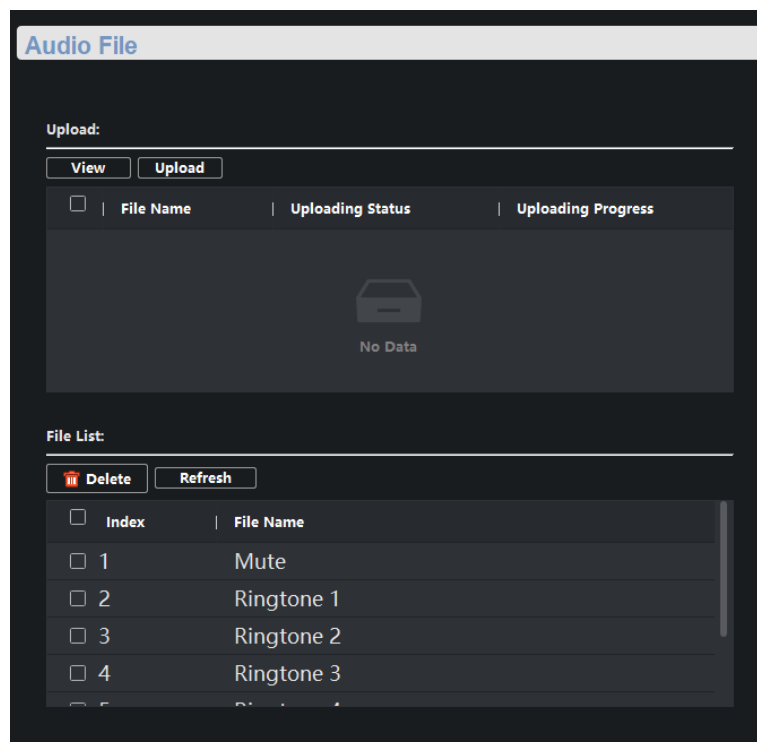
Upload the custom audio files to SD card, and delete the audio file in the SD card.

#### 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**.



**Figure 3-25 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 (16 kHz, 16 bit mono). 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 can not 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.

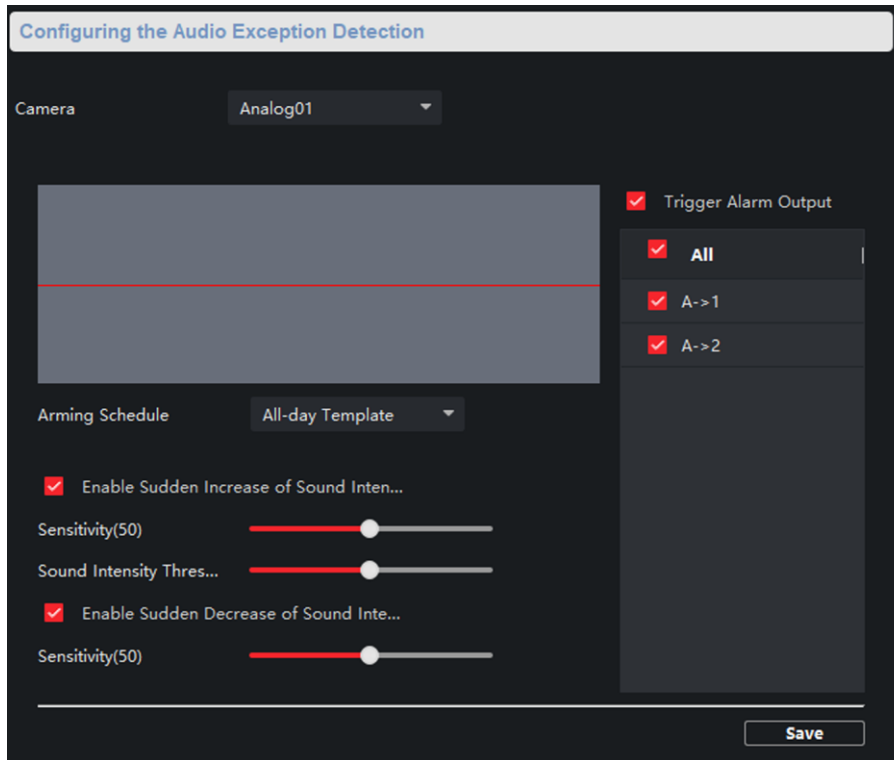
## 3.5 Event Settings

### 3.5.1 Set Audio Exception Detection

Audio exception detection means that when the sound in the environment is detected as sudden increase of sound intensity or sharp decrease of sound intensity, an alarm output will be triggered.

#### Steps

1. Click  to enter the **Remote Configuration** page, go to **Event** → **Audio Exception Detection**



**Figure 3-31 Audio Exception Detection Configuration Page**

2. According to actual needs, select and check **Enable Sudden Increase of Sound Intensity**, **Enable Sudden Decrease of Sound Intensity**. And set the parameters.

---

**Note**

**Sensitivity(50)** and **Sound Intensity Thresholds(50)** can be set from 1 to 100 and default to 50.

---

3. Click the drop-down box of **Arming Schedule** and set the arming schedule for audio exception detection.

---

**Note**

There are three schedules.

- The schedule template (not editable) that comes with the system, such as all-day template, weekday template and event template.
  - Editable schedule template01 to template08. For detailed edit method, see **Set System Schedule**.
  - Custom schedule. For detailed edit method, see **Set Custom Schedule**.
- 

4. Check **Trigger Alarm Output**, select and check the alarm output signal that is linked when the audio exception is detected.
5. Click **Save**.

**Result**

During the configured arming schedule, the audio anomaly event is detected according to the

---

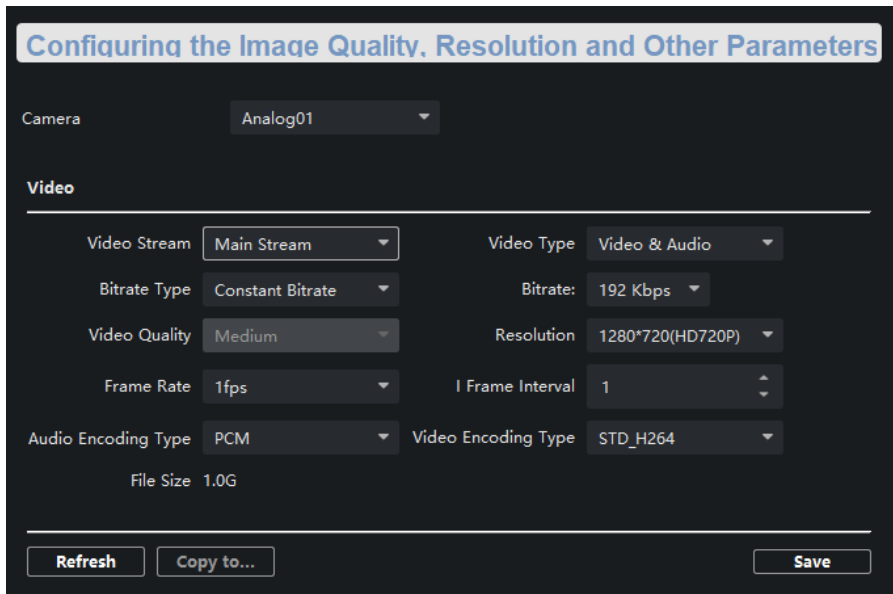
enabled detection items, and the selected alarm output signal is linked when the audio exception is detected.

### 3.6 Video & Audio Settings

#### 3.6.1 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**.



**Figure 3-32 Video & Audio Configuration Page**

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.
- 

#### **Video Stream**

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

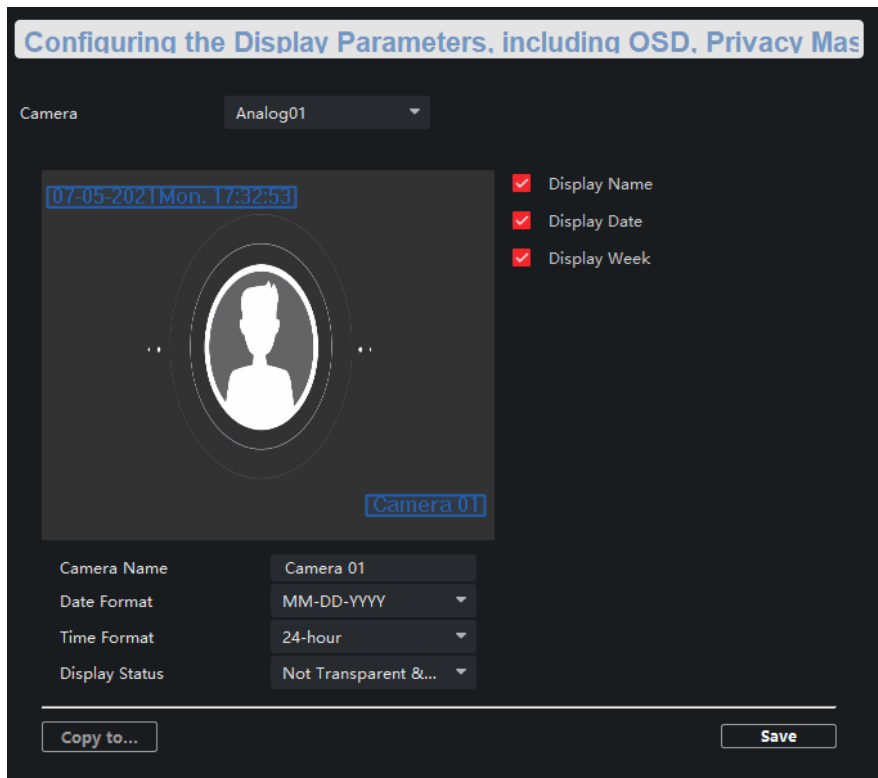
- After the video and audio parameters are changed, the device won't reboot.

- Please combine the actual demand and storage capacity to configure the video and audio parameters.
- 

### 3.6.2 Set Display

Edit the display information of the camera.

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



**Figure 3-33 View Scale Configuration Page**

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**.

### 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.

---

### 3.6.3 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**.

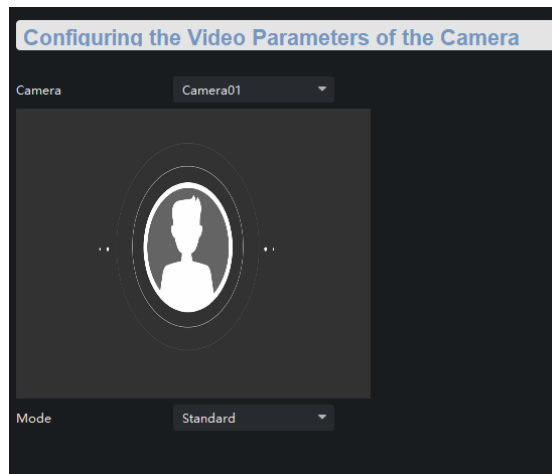


Figure 3-34 Picture Settings Page

### 3.6.4 Set Intercom Audio

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

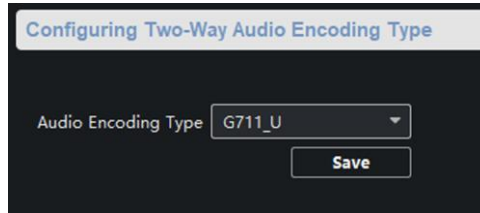


Figure 3-35 Intercom Audio Configuration Page

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.

---

### Note

EZVIZ intercom only supports G711\_U and AAC.

---

## 3.7 System Settings

### 3.7.1 Set Time

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

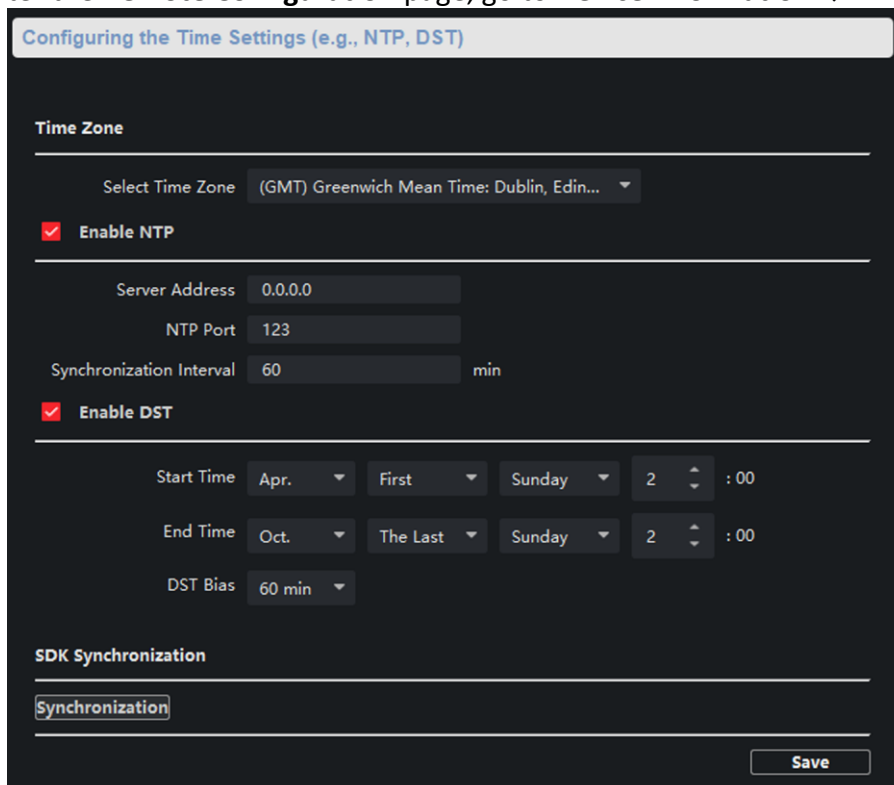

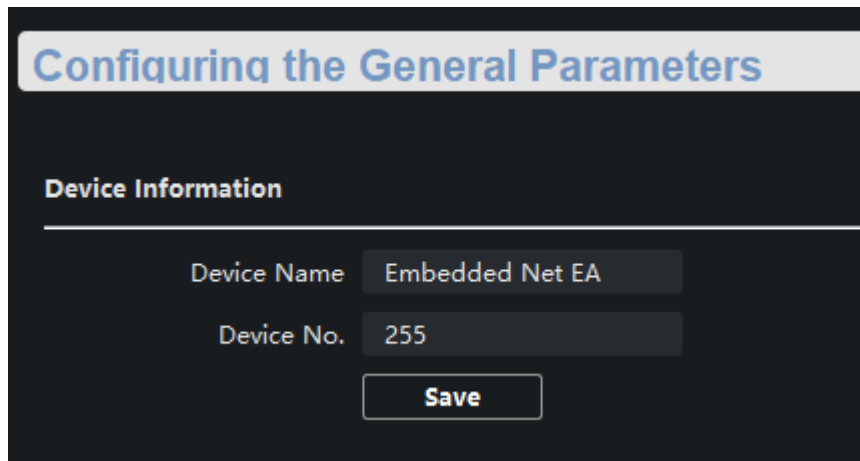


Figure 3-36 Time Setting Page

You can set the time zone, NTP, DST on the Time page.  
You can also click Synchronization to implement SDK synchronization.

### 3.7.2 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**.

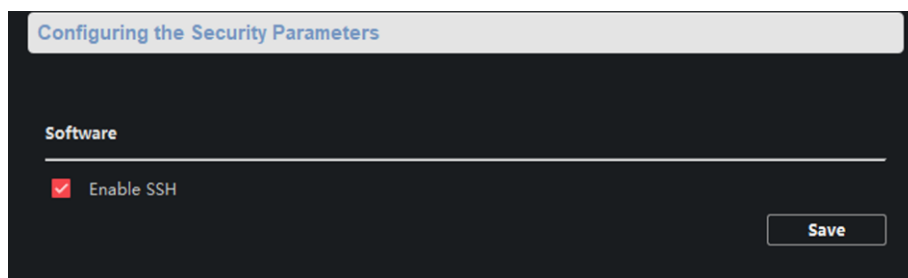


**Figure 3-37 System Parameters Setting Page**

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

### 3.7.3 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**.



**Figure 3-38 Security Parameters Configuration Page**

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.


---



### 3.7.4 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**.

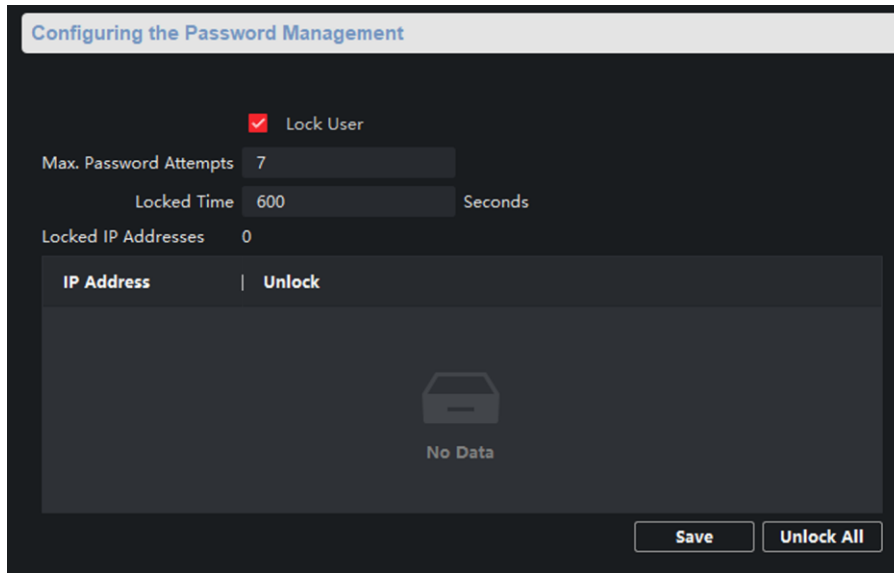


Figure 3-39 Password Management Page

#### 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. The available value is 10 to 3600 s.

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


### 3.7.5 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**.

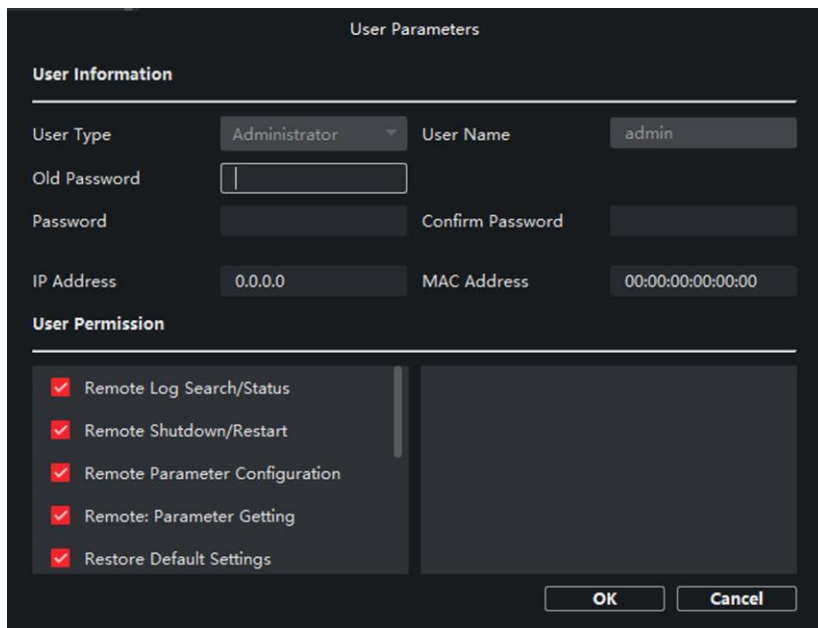


Figure 3-40 Edit Admin User

### 3.7.6 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 Type and Ti...  
Major Type: All    Minor Type: All    Search  
Start Time: 2021-07-06 00:00    End Time: 2021-07-06 23:59

Index	Operation Time	Major T...	Minor Type	Remote ...	Local O...	Remote ..
1	2021-07-...	Oper...	Remote L...	admin		10.2...
2	2021-07-...	Oper...	Remote L...	admin		10.2...
3	2021-07-...	Oper...	Remote L...	admin		10.2...
4	2021-07-...	Oper...	Remote L...	admin		10.2...
5	2021-07-...	Oper...	Remote L...	admin		10.2...
6	2021-07-...	Oper...	Remote L...	admin		10.2...
7	2021-07-...	Oper...	Remote L...	admin		10.2...
8	2021-07-...	Oper...	Remote L...	admin		10.2...
9	2021-07-...	Oper...	Remote L...	admin		10.2...
10	2021-07-...	Oper...	Remote L...	admin		10.2...
11	2021-07-...	Oper...	Remote L...	admin		10.2...
12	2021-07-...	Oper...	Remote L...	admin		10.2...

Backup

Figure 3-41 Search and View the Log

---


### Note

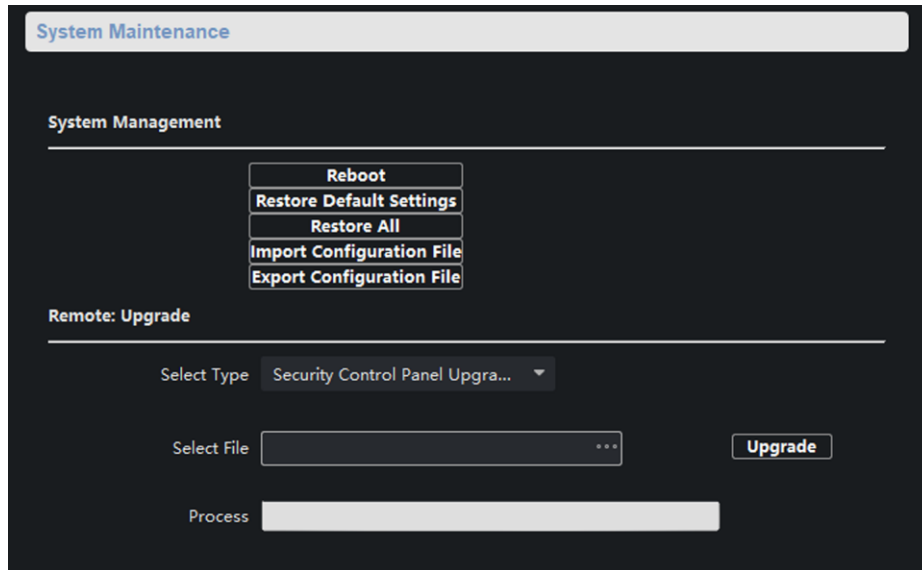
You can click **Backup** and download the search result.

---

### 3.7.7 Maintain the System

System management and remote upgrade.

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



**Figure 3-42 System Maintenance Page**

### 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, 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.

---

#### 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.

---

### 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.

---

### 3.7.8 Check Video & Audio Status

Automatically or Manually check the video and audio status.

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

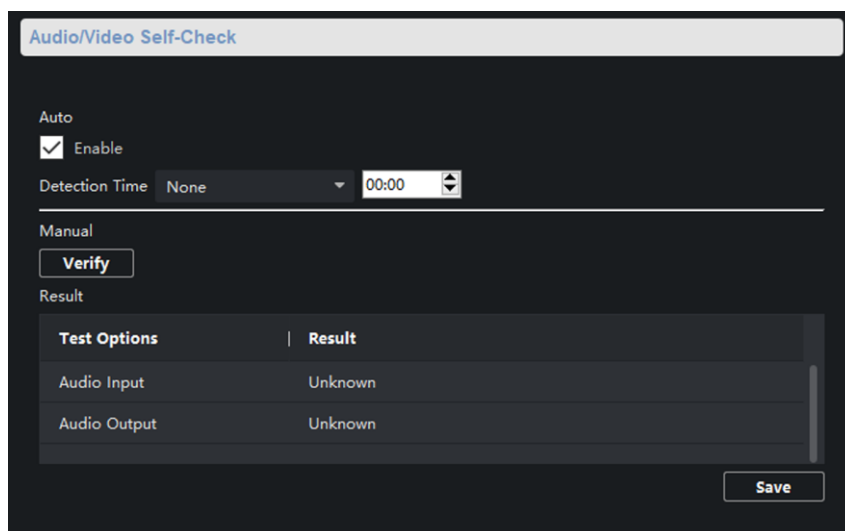


Figure 3-43 Video/Audio Self-Check

#### 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.

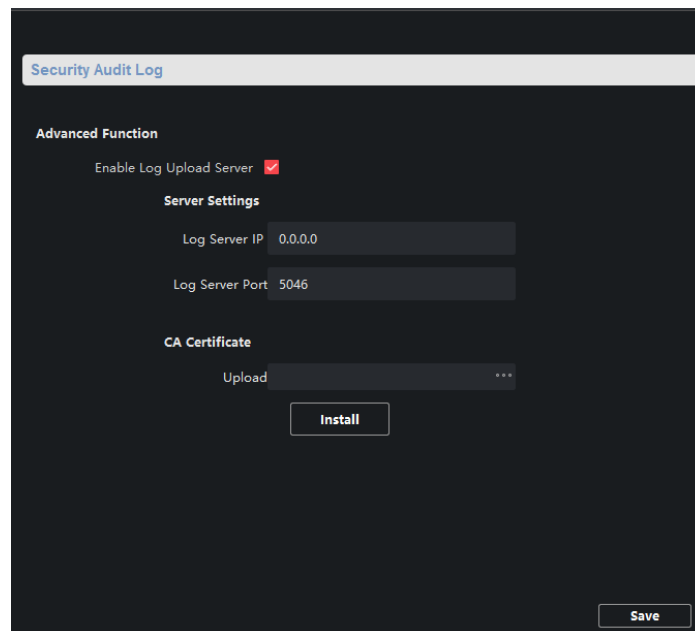
**Table 3-1 Description of Check Results**

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

## 3.7.9 Security Audit Log

### Steps

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




**Figure 3-44 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**.

### 3.8 Check Status


#### 3.8.1 Check Zone Status

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

#### 3.8.2 Check Relay Status

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

#### 3.8.3 Check Siren Status

Click  to enter the **Remote Configuration** page, go to **Status** → **Siren**, you can view the siren status.

### 3.9 Communication Matrix and Device Command



Scan the QR code to get the communication matrix.



Scan the QR code to get the device command.





See Far, Go Further