Panic Alarm Box

User Manual

Legal Information

© Hangzhou Hikvision Digital Technology Co., Ltd. All rights reserved.
This Manual is the property of Hangzhou Hikvision Digital Technology Co., Ltd. or its affiliates (hereinafter referred to as Hikvision), and it cannot be reproduced, changed, translated, or distributed, partially or wholly, by any means, without the prior written permission of Hikvision. Unless otherwise expressly stated herein, Hikvision does not make any warranties, guarantees or representations, express or implied, regarding to the Manual, any information contained herein.

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 Acknowledgement
- 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.

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

Safety Instruction

WARNING

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

WARNING

- Do not drop the device or subject it to physical shock.
- Wipe the device gently with a clean cloth and a small quantity of ethanol, if necessary.
- Do not aim the lens at the sun or any other bright light.
- When any laser equipment is in use, make sure that the device lens is not exposed to the laser beam, or it may burn out.
- Do not expose the device to high electromagnetic radiation or extremely hot, cold, dusty, or damp environments, the appropriate temperature is -40℃ to 60℃.
- Place the device in a dry and well-ventilated environment.
- Keep non-waterproof devices away from liquids.
- Keep the device in original or similar packaging while transporting it.

- A few device components (e.g., electrolytic capacitor) require regular replacement. The average lifespan varies, so periodic checking is recommended. Contact your dealer for details.
- Improper use or replacement of the battery may result in explosion hazard. Replace with the same or equivalent type only. Dispose of used batteries in conformance with the instructions provided by the battery manufacturer.
- Never attempt to disassemble the device.

Contents

Chapter 1 Overview

Description

DS-PEA series alarm box is a new quick emergency assistance device. It supports two-way audio from the main station to the front-end alarm box, and supports 200W IR supplementary lighting cameras, quick emergency alarm function, and provides faster and more effective quick alarm services. It is mainly used in indoor scenarios such as schools, hospitals, subways, scenic spots, and prisons.

Key Features

- Uses an embedded Linux operating system with an embedded SOC processor, ensuring stable and reliable system operation
- Supports two-way audio with the main station
- H.264, H.265 video encoding
- G711U, AAC, OPUS, PCM, ADPCM audio standards
- Built-in high-sensitivity microphone
- Supports listening and broadcasting functions
- Multiple network protocols including TCP/IP and RTSP
- Supports ISUP, Ezviz Cloud Protocol, HIK_SIP protocols
- Built-in full-band high-quality speaker and microphone, with anti-distortion technology, providing loud and clear sound.
- Protection level: IP54
- Vandal resistance level: IK08
- Supports quick dialing
- Some models support POE power supply and camera

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.

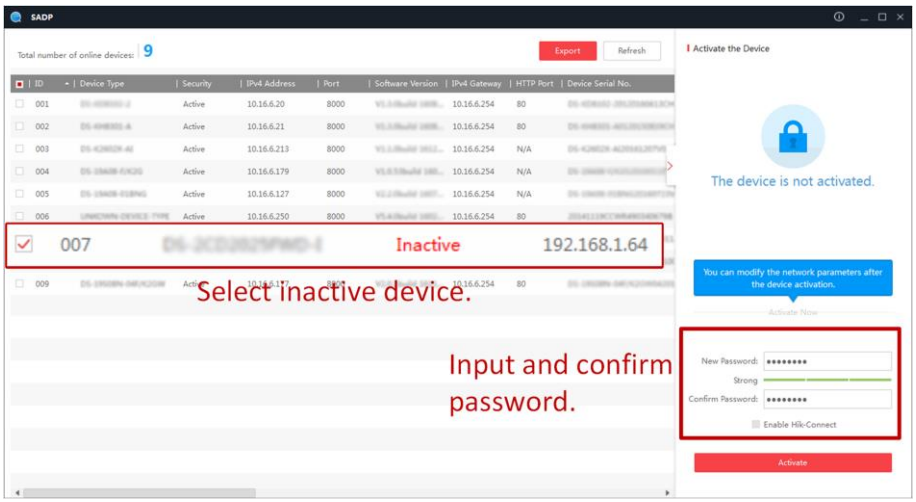


Figure 2-1 Activate via SADP

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.

2.3 Activate via WEB

Use web browser to activate the device. Use SADP software or PC client to search the online device to get the IP address of the device, and activate the device on the web page.

Before You Start

Make sure your device and your PC connect to the same LAN.

Steps

1. Open a web browser and input the IP address of the device.

   Note

   If you connect the device with the PC directly, you need to change the IP address of your PC to the same subnet as the device. The default IP address of the device is 192.0.0.65.

2. Create and confirm the admin 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.

3. Click **OK** to complete activation.
4. Edit IP address of the device.
   1) Enter IP address modification page.
   2) Change IP address.
   3) Save the settings.

Chapter 3 Operation via Web Browser

3.1 Login

You can configure device parameters through the web interface, including events, device management, and device status.

Before You Start

- Make sure that the device is activated.

Note

We recommend using IE11, Firefox 54 or later, or Google Chrome. If there are issues with the functions, we suggest using Google Chrome or upgrading the browser version.

Steps

1. Enter http://device IP address and press **Enter** to access the login interface in the browser address bar.

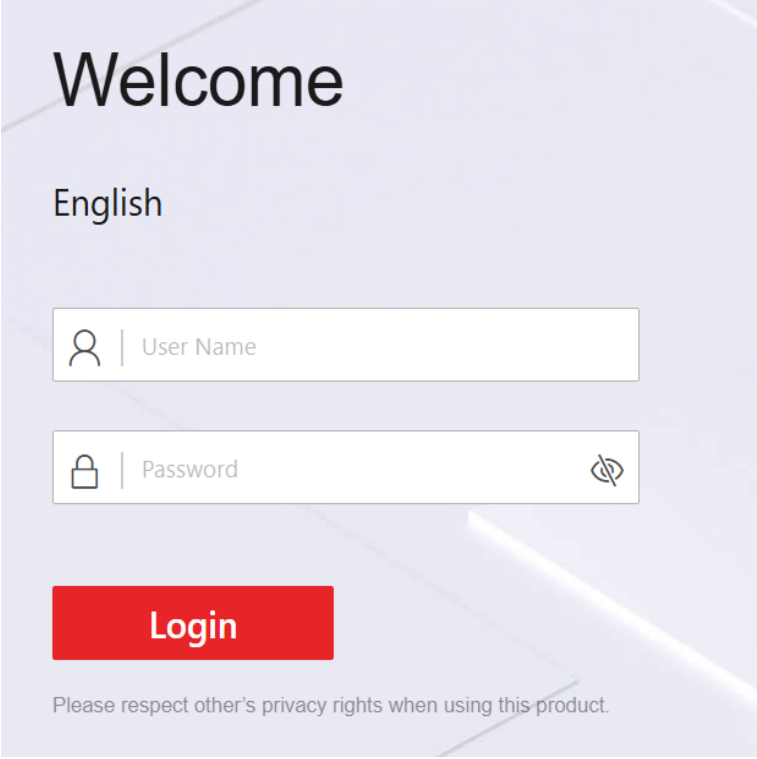


Figure 3-1 Login

2. Enter the username and password, and click **Login**. You will enter the main menu interface.

3.2 Overview

Click **Live View**, you can view related data statistics and status overview of the device.

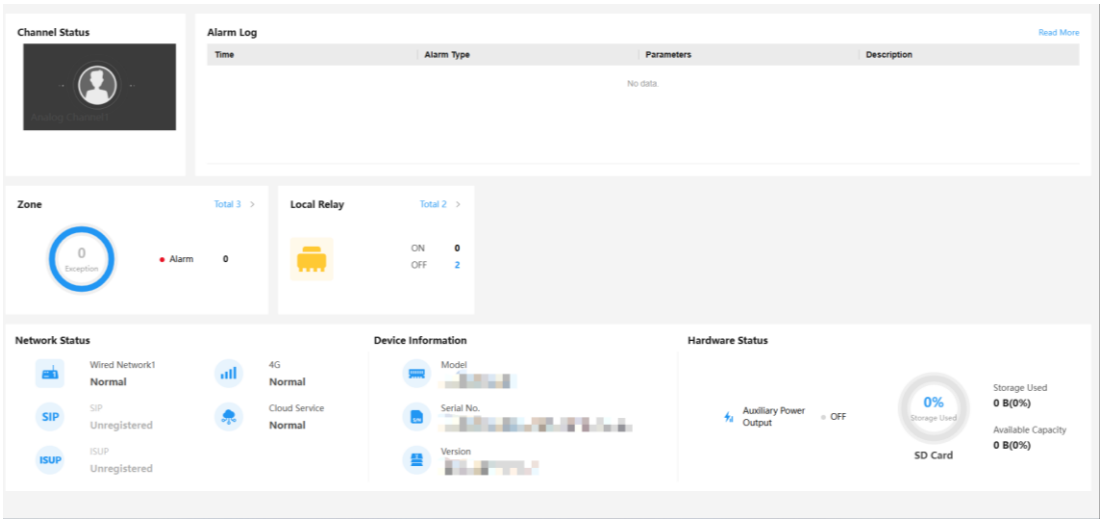


Figure 3-2 Live View

Channel Status

You can view the preview image of the device.

Alarm Log

You can view alarm time, type, parameters, and description.
Click **View More** to enter the log viewing interface for more search and viewing.

Zone

You can view the number of zones in alarm and abnormal states.
Click **Total** in the upper right corner to enter the zone management interface.

Local Relay

You can view the number of relays that are on and off.
Click **Total** in the upper right corner to enter the relay management interface.

Network Status

You can view the connection and registration status of wired, SIP, cloud services, and ISUP.
Click the network name or icon to enter the corresponding network configuration interface.

Device Information

You can view the device model, serial number, and version.
Click any area in the device information region to enter the basic information configuration interface.

Hardware Status

You can view the status of auxiliary power output and SD card usage and remaining capacity.

Click the **Auxiliary Power Output** area to enter the auxiliary power output port configuration interface. Click the SD card icon to enter the SD card management interface.

3.3 Image Search

Steps

1. Enter the device address in the browser, log in, and click **Image Search** to enter the interface.

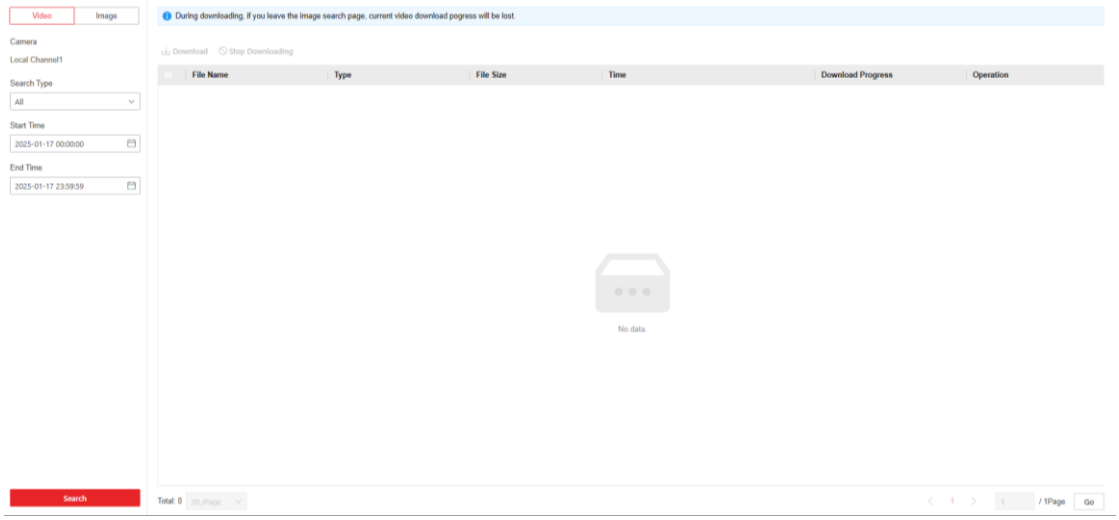


Figure 3-3 Live View

2. Select **Search Type** of video or images to search for.
3. Select **Search Type**.
4. Select **Start Time** and **End Time**.
5. Click **Search**.

The results are displayed in the list on the right side of the interface.

Optional: Click **Download** to download the log content.

3.4 Configuration

3.4.1 Device Information

Enter the device address, log in, and click **Configuration** → **System** → **System Configuration** → **Basic Information** to enter the interface.

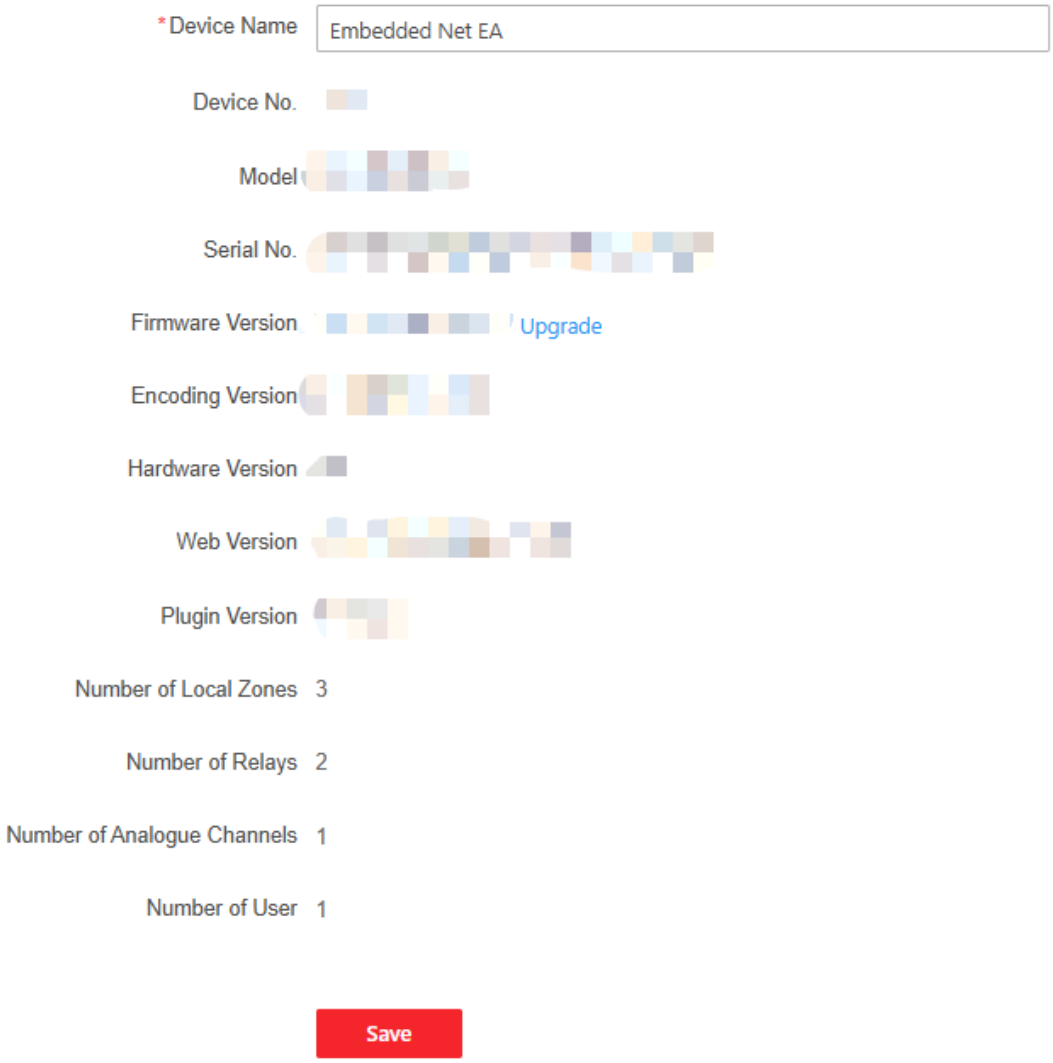


Figure 3-4 Device Information

You can change the device name and click **Save**.
You can view the device language, model, serial No., and version No..
Click **Upgrade** to upgrade the main program.

3.4.2 Device Time

Steps

1. Enter the device address, log in, and click **Configuration** → **System** → **System Configuration** → **Time Configuration** to enter the configuration interface.
2. Select the time zone.
3. Select the time synchronization method.
   – Choose **NTP Time Sync**, and the system will automatically synchronize the server time. Enter the server address, NTP port, and synchronization interval.

– Choose **Manual Time Sync** and manually set the time or click **Sync with Computer**.

4. Click **Save**.

3.4.3 Online User

You can view online users.

Enter the device address, log in, and click **Configuration** → **System** → Online User to enter the interface.

You can view online user information, including username, user type, IP address, and user operation time.

Click **Refresh** to refresh the page.

3.4.4 Network Settings

Set Basic Network Parameters

Set the device's TCP/IP information.

Enter the device address, log in, and click **Configuration → Network → Network Settings → TCP/IP** to enter the configuration page.

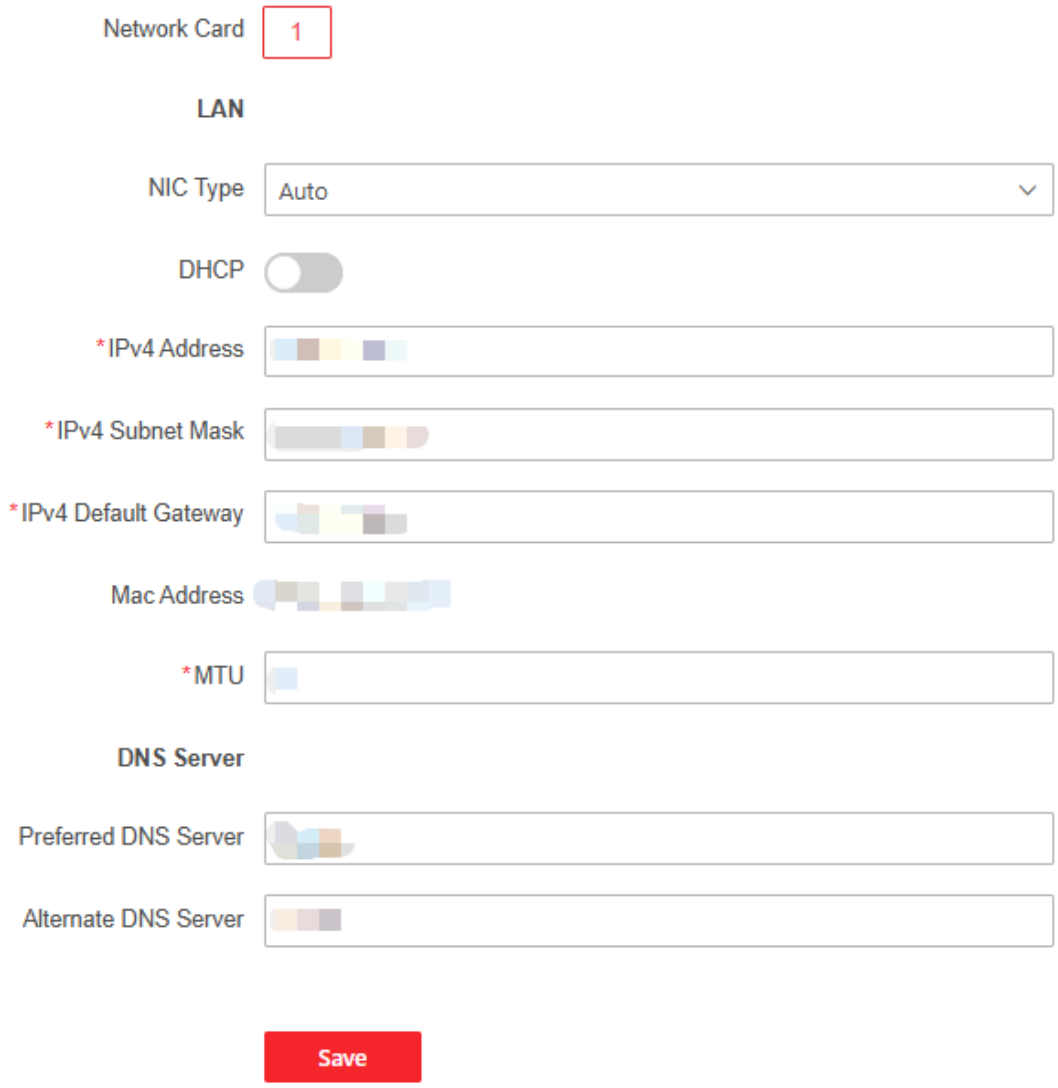


Figure 3-5 Basic Network Parameters Configuration

Click **Save** to save parameters.

Network Card

Default is Network Card 1.

NIC Type

Select the network card type from the drop-down menu. Default is **Auto**.

DHCP

If NOT enabled, you need configure the IPv4 address, IPv4 subnet mask, IPv4 default gateway, primary DNS server, and secondary DNS server manually

If enabled, the system automatically assigns the IPv4 address, IPv4 subnet mask, IPv4 default gateway, primary DNS server, and secondary DNS server.

MTU

Set the MTU value. MTU refers to the maximum transmission unit, representing the maximum size of data packets (in bytes) that a class of communication protocols can transmit at a certain layer. Set this value according to your needs.

Set Ports

You can set the necessary ports when accessing the device via the network.

Set SIP Parameters

SIP servers allow terminals in different network segments to communicate. If not registered, terminals can only communicate within the same network segment. After successfully registering with the SIP server, terminals can dial each other using SIP IDs.

Steps

1. Enter the device address, log in, and click **Configuration → Network → Device Access → SIP** to enter the configuration interface.

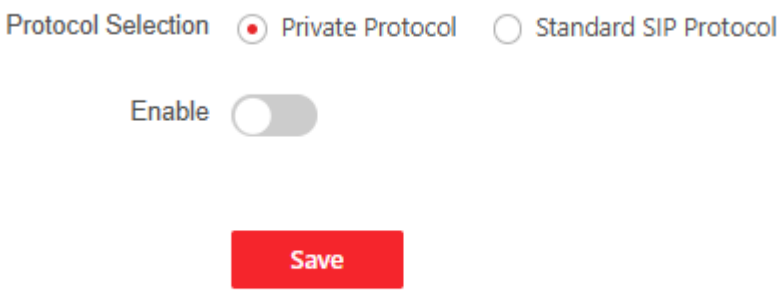


Figure 3-6 SIP Configuration

2. Select **Private Protocol** or **Standard SIP Protocol** based on the SIP service you need to communicate with.
3. Click **Enable**.
4. Click **Save**.

Set HIK-Connect Parameters

Steps

1. Enter the device address, log in, and click **Configuration → Network → Device Access → HIK-Connect** to enter the configuration interface.

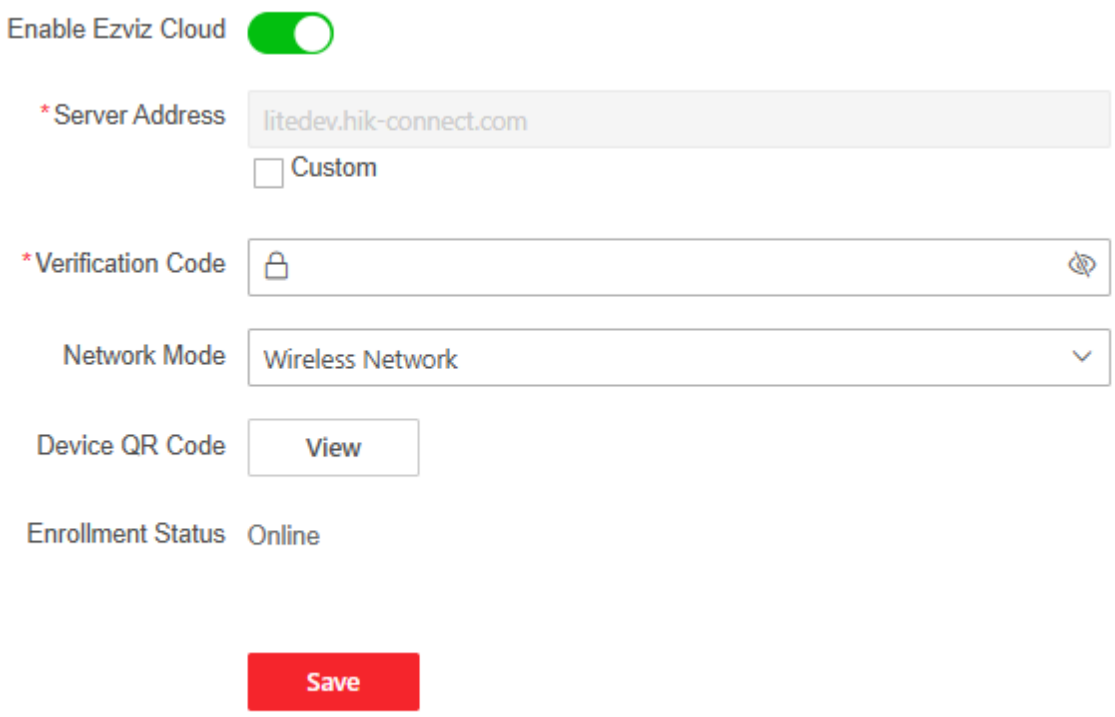


Figure 3-7 HIK-Connect Configuration

2. Enable Ezviz Cloud function.
3. Select **Network Mode**.
4. Click **Save**.

Set ISUP Parameters

Steps

1. Enter the device address, log in, and click **Configuration → Network → Device Access →ISUP** to enter the configuration interface.

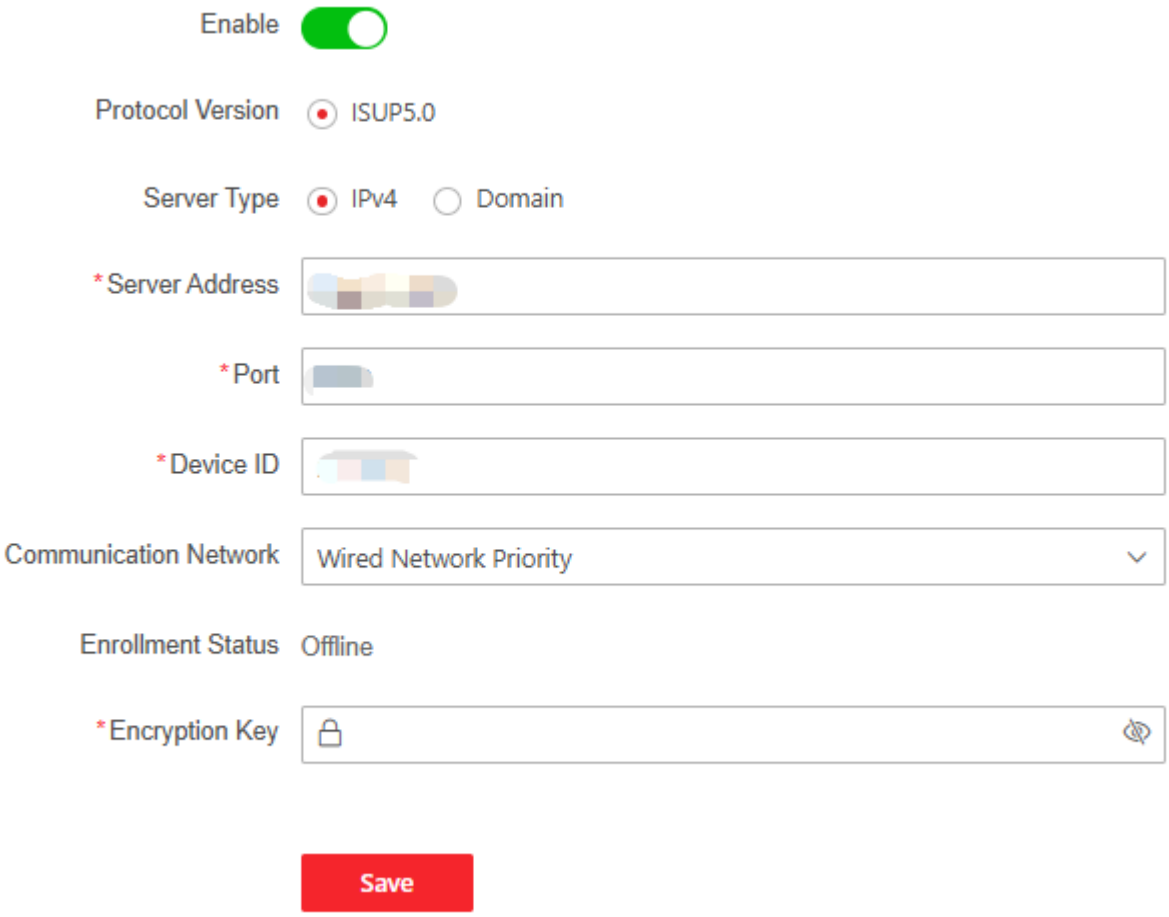


Figure 3-8 ISUP Configuration

2. Enable ISUP function.
3. View the ISUP protocol version and set the server address, port, and device ID.

Note

The default ISUP platform port is 7660.

4. Select **Communication Network** priority.

Auto

Network connection priority is wired network and wireless network.

Wired Network Priority

The system prefers the wired network. If no wired network is detected, it will choose the wireless network.

3G/GPRS

The system only uses 3G/GPRS as the network.

Wired Network Card 1

The system only uses wired network card 1 as the network.

5. Enter the encryption key.
6. Click **Save**.

Set Network Center Parameters

You can set the parameters for uploading alarms to the alarm center. When an alarm is triggered, the alarm message will be uploaded to the configured alarm center.

Steps

1. Enter the device address, log in, and click **Configuration → Network → Alarm Communication →Network Center** to enter the configuration interface.

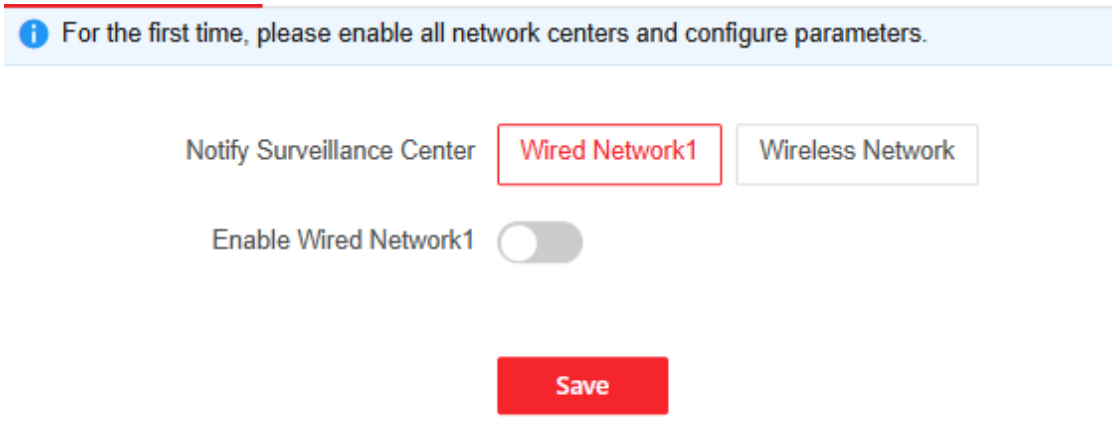


Figure 3-9 Network Center Interface

2. Select surveillance center as **Wired Network 1** or **Wireless Network** based on your needs.
3. Check **Enable Wired Network 1.**

Server Type

The type of central server address, which can be either **IPv4** or **Domain Name**.

IP Address/ Domain Name

Enter the server IP address or domain name based on the configured server type.

Port No.

Central port number.

Protocol Type

Default is **HIK protocol**.

User Name

Supports digits and letters. For **HIK protocol**, the length can be **6~9 characters**; for **NAL2300 protocol**, the length can be **6 characters**.

4. Click **Save**.

3.4.5 Audio/Video Configuration

Set Video Parameters

You can set the image quality and resolution of the device's camera.

Steps

1. Enter the device address in the browser, log in, and click **Configuration** → **Video/Audio** → **Video** to enter the configuration interface.

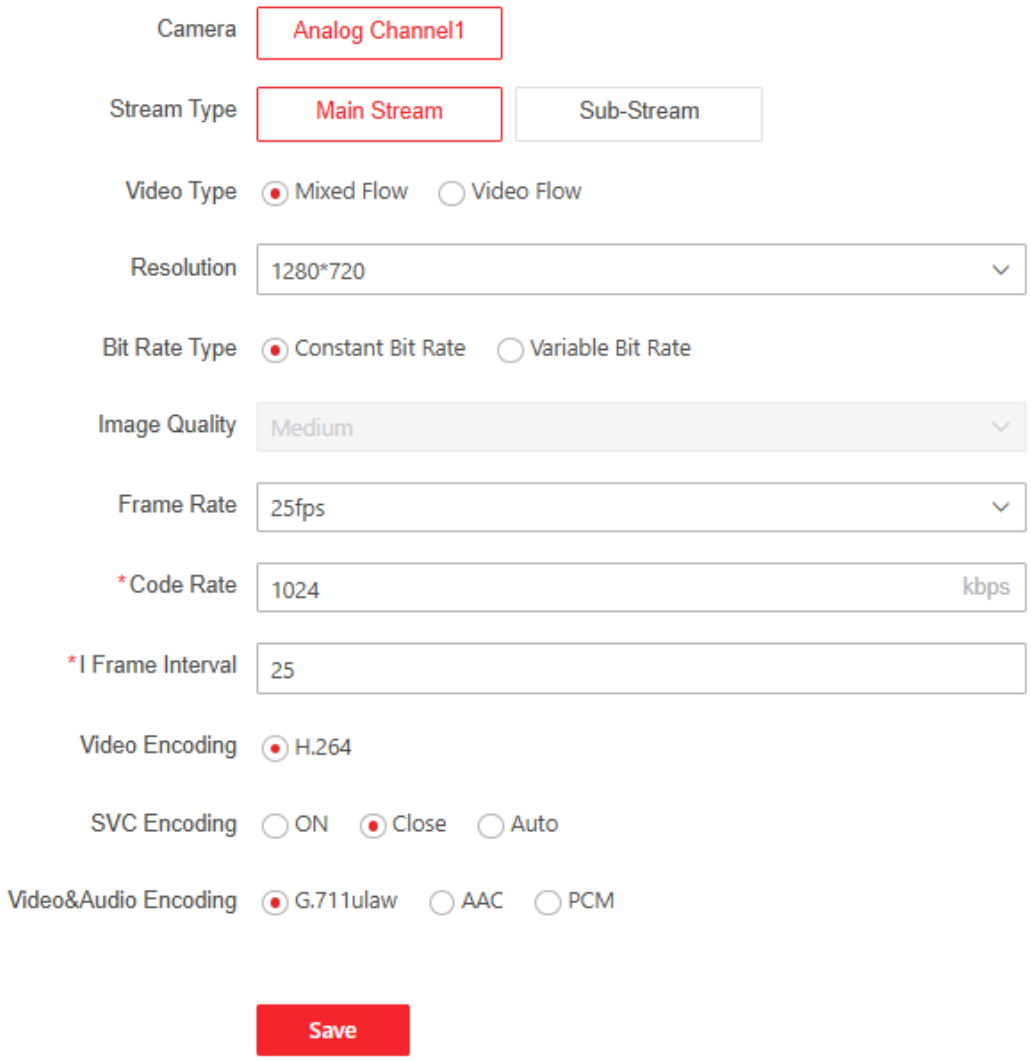


Figure 3-10 Video Configuration Interface

Note

Video intercom devices and non-video intercom devices support different rates and encoding types.

2. Select the channel, configure the stream type, video type, resolution, bitrate type, image quality, frame rate, code rate, I-frame interval, video encoding, SVC encoding, and Video/Audio encoding.
3. Click **Save**.

Set Audio Parameters

You can configure the device's volume.

Steps

1. Enter the device address in the browser, log in, and click **Configuration** → **Video/Audio** → **Audio** to enter the configuration interface.

Figure 3-11 Audio Configuration Interface

2. Configure the audio encoding, audio input, and audio output parameters.
3. Click **Save**.

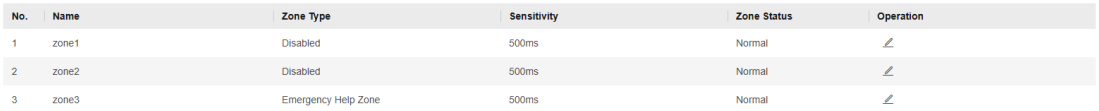
3.4.6 Device Management

Set Zone

Set zone to connect detectors achieving arming.

Steps

1. Enter the device address in the browser, log in, and click **Configuration** → **Device** → **Zone** to enter the configuration interface.



No.	Name	Zone Type	Sensitivity	Zone Status	Operation
1	zone1	Disabled	500ms	Normal	
2	zone2	Disabled	500ms	Normal	
3	zone3	Emergency Help Zone	500ms	Normal	

Figure 3-12 Zones Management

You can view all zone information in the list.

2. Select the zone to configure, click , and a zone parameter settings window will pop up.
3. Modify the zone parameters, including name, detector type, zone type, and audio file.

Zone Type Explanation

Instant Zone

The system enters alarm status immediately after arming. When the zone is triggered, an alarm is immediately generated. This type of zone can be used with various detectors such as infrared detectors and can be installed in places like supermarkets.

Emergency Zone

24-hour alarm. This type of zone is commonly used for emergency buttons, smoke detectors, and glass break detectors.

Fire Zone

24-hour alarm, with fixed system sound (voice, siren) when the zone is triggered.
This type of zone is commonly used for smoke and heat detectors, installed in areas prone to fires.

24-Hour Silent Zone

24-hour alarm, with no system sound (voice, siren) when the zone is triggered.
This type of zone is commonly used for emergency buttons (e.g., banks, jewelry counters for silent alarms) and cannot be bypassed.

Disabled Zone

The zone triggers, but zone tamper does not trigger an alarm. Commonly used to shield faulty detectors.

Consultation Zone

It is used for business inquiries.

4. Optional: Enable the **Report Alarm Recovery** function. If this is enabled, the system will upload a report to the center when the alarm is recovered.

5. Set associated relays, channels, and recordings. When the zone is triggered, the associated relays and channels will also be triggered.
6. Click **Save**.
7. Optional: Click **Copy** to copy the configuration to other zones.

Set Relay

When events occur and need to be associated with relay outputs, configure the relays.

Steps

1. Enter the device address in the browser, log in, and click **Configuration** → **Device** → **Relay** to enter the configuration interface.

Figure 3-13 Relays Management

You can view all relay information in the list.
2. Select the relay to configure, click , and a relay parameter configuration interface will pop up.
3. Modify the relay parameters, including **Name** and **Output Delay(s)**.
4. Optional: Enable Continuous Output or set the input/output delay time.

Note

The relay starts outputting after the configured time. The output delay can be set to 1-600 seconds.

5. Optional: Enable Relay Off When Call Answered. If this is enabled, the relay will turn off when the call is answered; if not enabled, the relay will turn off after the call ends.
6. Click **OK**.
7. Optional: Select the relay in the list and click **ON/OFF** to manually enable or disable the relay.

Set Auxiliary Power Control

The device supports auxiliary power supply and can control the auxiliary power output switch.

Steps

1. Enter the device address in the browser, log in, and click **Configuration** → **Device** → **Auxiliary Power Control** to enter the configuration interface.
2. Enable the auxiliary power output port 1 switch. After enabling, the device can be powered by auxiliary power.

Set Button Backlight

You can set the button backlight on/off method.

Steps

1. Enter the device address in the browser, log in, and click **Configuration** → **Device** → **Button Backlight** to enter the configuration interface.
2. Enable the required configuration items.

Close All The Time

When enabled, the button backlight will not turn on.

Close When Free

When the device is free, the button backlight will not turn on.

Stay On During Two-Way Audio

When the device is in Two-Way Audio, the button backlight will remain on.

Stay On During Calling

When the device is in call, the button backlight will remain on.
3. Click **Save**.

3.4.7 Storage Parameter Settings

SD Card Management

You can view SD card capacity information and format the SD card.

Steps

1. Insert the SD card into the device.
2. Enter the device address in the browser, log in, and click **Configuration** → **Storage** → **Storage Management** to enter the configuration interface.
3. Check the current status and capacity of the SD card.
4. Optional: Click **Format** to format the current SD card. After formatting, all content on the SD card will be cleared.
5. Configure storage parameters, including storage mode, video quota percentage, and audio quota percentage. Click **Save**.

Recording Schedule Settings

You can set the automatic recording time schedule for the device.

Steps

1. Enter the device address in the browser, log in, and click **Configuration** → **Storage** →**Schedule Settings** → **Record Schedule** to enter the configuration interface.
2. Enable the recording schedule function.
3. Click **Save**.

3.4.8 Audio Quality Diagnosis

You can configure audio rules and diagnostic methods.

Steps

1. Enter the device address in the browser, log in, and click **Configuration** → **Event** → **Exception Detection** → **Audio Quality Diagnosis** to enter the configuration interface.

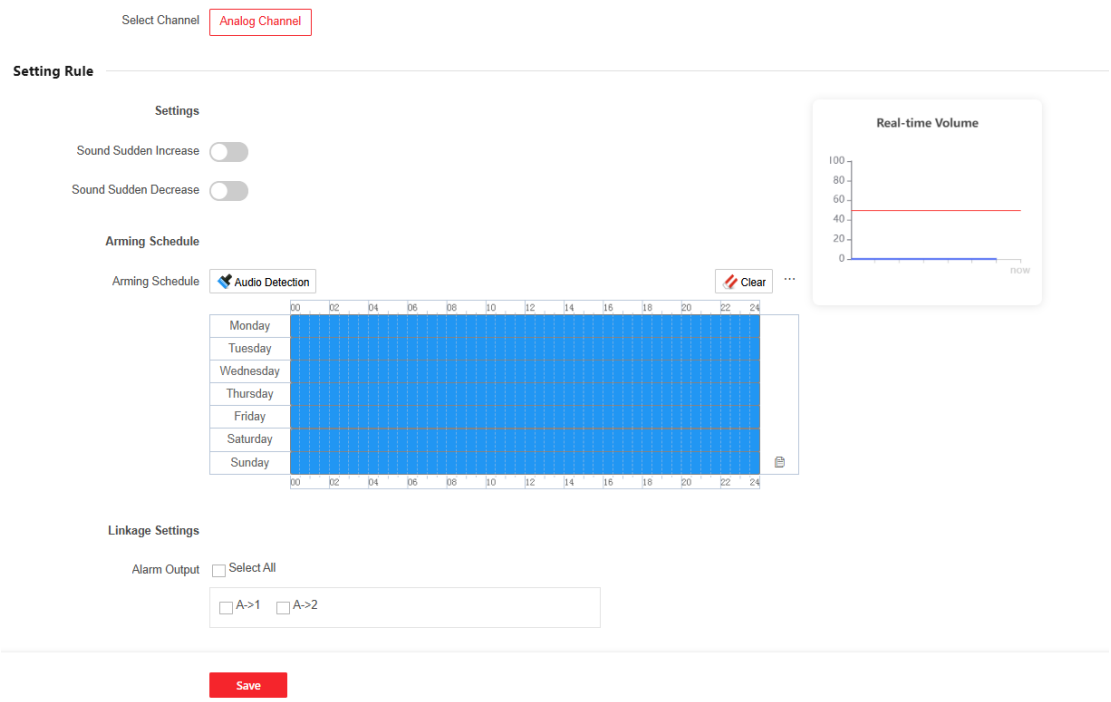


Figure 3-14 Audio Quality Diagnosis Interface

2. Set the parameters.

Select Channel

Default is the **Analog Channel**.

Sound Sudden Increase

If enabled, configure the sensitivity and threshold for the sudden increase in sound intensity. The higher the sensitivity, the easier it triggers; the higher the threshold, the stronger the sound needs to be to trigger.

Sound Sudden Decrease

If enabled, configure the sensitivity for the sudden decrease in sound intensity. The higher the sensitivity, the easier it triggers.

Arming Schedule

Select the arming time brush and draw the time segments on the timeline. During the drawn time segments, audio quality diagnosis will be performed. When the sound intensity exceeds the threshold, an alarm will be triggered.

Alarm Output

Select the alarm output method. When the sound intensity exceeds the threshold, an alarm will be triggered and linked.

3. Click **Save**.

3.4.9 Alarm Parameter Settings

You can set tampering alarms. When enabled, the device will trigger an alarm when it is forcibly removed.

Steps

1. Enter the device address in the browser, log in, and click **Configuration** → **Alarm Setting** → **Alarm Parameter** → **Tampering Alarm** to enter the configuration interface.
2. Enable **Tampering Alarm** based on your needs.
3. Click **Save**.

3.4.10 Intercom Settings

Calling Settings

You can set the parameters for initiating and receiving calls.

Steps

1. Enter the device address in the browser, log in, and click **Configuration** → **Intercom** → **Calling Settings** to enter the configuration interface.
2. Set the call-related parameters.
3. Set the parameters for receiving calls.

Voice Prompt Settings

You can set the device's various prompt sounds and the silent plan for the prompts.

Steps

1. Enter the device address in the browser, log in, and click **Configuration** → **Intercom** → **Voice Prompt** to enter the configuration interface.

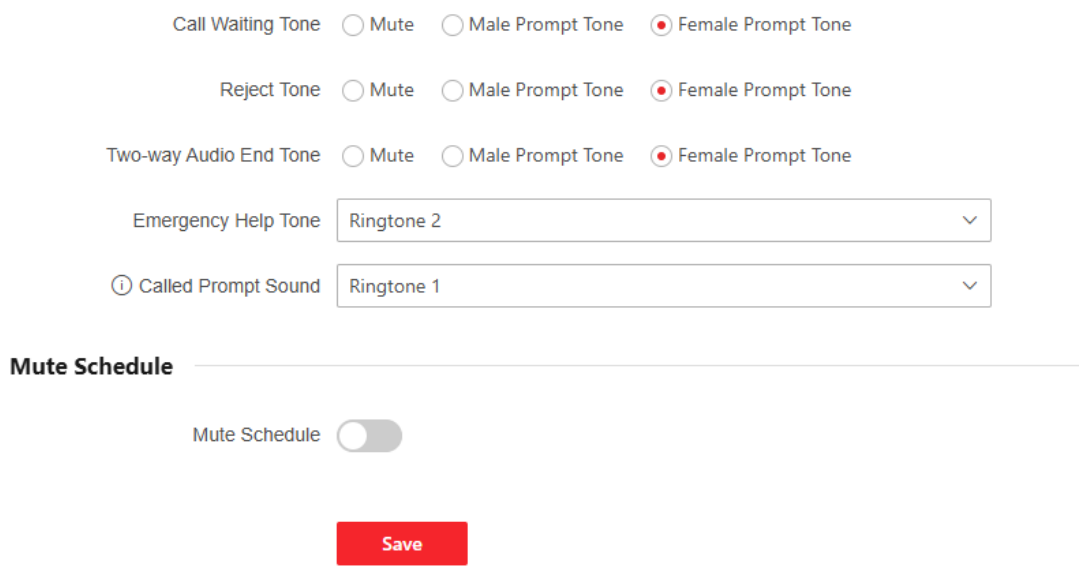


Figure 3-14 Voice Prompt Settings Interface

2. Set the prompt tones.
3. Set the mute schedule. The device is mute during the set time periods.。 enable the **Mute Schedule**.
4. Click **Save**.

Key Settings

You can set the call content for the device's keys.

Steps

1. Enter the device address in the browser, log in, and click **Configuration** → **Intercom** → **Key Settings** to enter the configuration interface.

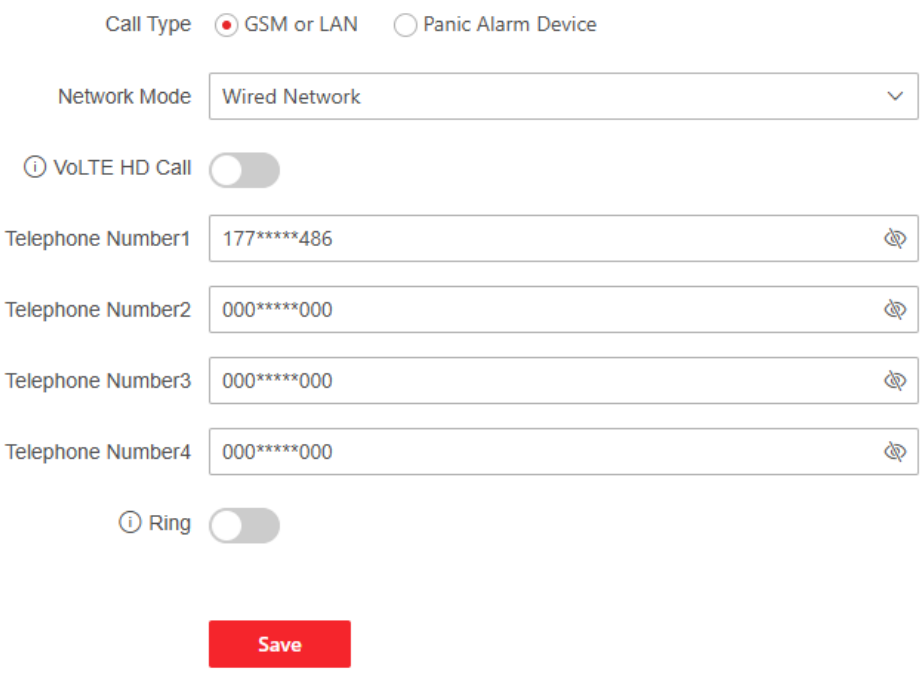


Figure 3-15 Voice Prompt Settings Interface

2. Set the Call Type.

GSM or LAN

When the user presses the button, the device will call the configured phone number.

Panic Alarm Device

Enter the IP address of the device to call. When the user presses the button, the device will call the configured management personnel based on the IP address.

Note

The private SIP service must be enabled and the configured IP must be in the same local network as the device to complete the call.

3. Set **Network Mode.**
4. Click **Save**.

3.4.11 Allowed Numbers Settings

You can set allowed numbers.

Steps

1. Enter the device address in the browser, log in, and click **Configuration** → **Intercom** → **Allowed Numbers List** to enter the configuration interface.

2. Enable list. When enabled, only numbers within the list are allowed to call in.
3. Click **Save**.

3.4.12 Custom Settings

You can set the audio for voice prompts and ringtones.

3.5 Maintenance

You can set the maintenance and security items.

3.6 Change Administrator Password

You can change the login password (device activation password) for the administrator.

Steps

1. Click the icon in the upper right corner **admin** → **Change Password** to enter the configuration page.
2. Enter the old password, create a new password, and confirm the password.

Note

- To better protect your privacy and enhance product security, we strongly recommend setting a more complex password: the password length must be between 8-16 characters, and should consist of at least two of the following types: numbers, uppercase and lowercase letters, special characters.
- You are responsible for reasonably configuring all passwords and other related product security settings.

3. Click **Save**.

3.7 Log Out/Sign Out

Click **admin** → **Sign Out** → **OK** to return to the login interface.

Chapter 4 Operation via Client Software

The device supports configuration through the client software. Scan the QR code below to view the relevant operation manual.

Client User Manual

- **Figure 4-1 Client Software User Manual QR Code**

UD41616B