



Panic Alarm Station

Configuration Guide

Legal Information

© 2022 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.

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 DS-PEA series panic alarm station.

Product	Model
Panic Alarm Station	DS-PEA22-F(B)
Box Panic Alarm Station	DS-PEA22-B(B)
Pole Panic Alarm Station	DS-PEA22-P(B), DS-PEA12-P, DS-PEA12-P/ZJ

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.

Panic Alarm Station Configuration Guide

- If smoke, odor, or noise arises from the device, immediately turn off the power, unplug the power cable, and contact the service center.



WARNING

- Do not drop the device or subject it to physical shock.
- Wipe the device gently with a clean cloth and a small quantity of ethanol, if necessary.
- Do not aim the lens at the sun or any other bright light.
- When any laser equipment is in use, make sure that the device lens is not exposed to the laser beam, or it may burn out.
- Do not expose the device to high electromagnetic radiation or extremely hot, cold, dusty, or damp environments, the appropriate temperature is -40 °C to 60 °C.
- Place the device in a dry and well-ventilated environment.
- Keep non-waterproof devices away from liquids.
- Keep the device in original or similar packaging while transporting it.
- A few device components (e.g., electrolytic capacitor) require regular replacement. The average lifespan varies, so periodic checking is recommended. Contact your dealer for details.
- Improper use or replacement of the battery may result in explosion hazard. Replace with the same or equivalent type only. Dispose of used batteries in conformance with the instructions provided by the battery manufacturer.
- Never attempt to disassemble the device.

Contents

Chapter 1 Overview	1
Chapter 2 Activation	2
2.1 Activate via SADP	2
2.2 Activate Device via Client Software	3
Chapter 3 Remote Settings	5
3.1 Device Management	5
3.1.1 Add Device to the Client Software	5
3.1.2 Edit Network Parameters	6
3.2 Network Configuration	6
3.2.1 Basic Settings	6
3.2.2 Set DNS	8
3.2.3 Set NAT	8
3.2.4 Set Alarm Center	10
3.2.5 Set SIP	11
3.2.6 Set Hik-Connect	13
3.2.7 Access the Platform	14
3.2.8 Set Call Center Parameters	15
3.2.9 Set Intercom Parameters	16
3.3 Alarm Settings	17
3.3.1 Set Zone	17
3.3.2 Set Relay	19
3.3.3 Set Call Waiting	20
3.3.4 Set Voice Prompt	21
3.4 Alarm Management	22
3.4.1 Manage Relay	22
3.4.2 Manage Audio Input/Output	22
3.4.3 Manage Siren	23
3.4.4 Manage Alarm Light	24
3.4.5 Manage Audio File	24

3.4.6 Manage Strobe Light Flicking.....	26
3.5 Event Settings	27
3.5.1 Schedule Settings	27
3.5.2 Set Audio Exception Detection	32
3.6 Video & Audio Settings	33
3.6.1 Video & Audio Settings	33
3.6.2 Set Display	35
3.6.3 Set Image Parameters	36
3.6.4 Set Intercom Audio	37
3.7 System Settings	38
3.7.1 Set Time	38
3.7.2 Set System Parameters	38
3.7.3 Set Security	39
3.7.4 Set Password	39
3.7.5 Set User.....	40
3.7.6 Search for Log	41
3.7.7 Maintain the System	42
3.7.8 Check Video & Audio Status	44
3.7.9 View Device Information	45
3.8 Set Camera.....	46
3.8.1 Add Camera	46
3.8.2 Set Video Parameters.....	47
3.8.3 Set WDR.....	47
3.8.4 Set Other Parameters.....	48
3.9 Storage Settings.....	48
3.9.1 Initialize HHD	48
3.9.2 Search for File	49
3.10 Check Status	50
3.10.1 Check Zone Status	50
3.10.2 Check Relay Status	50
3.10.3 Check Siren Status	50

3.10.4 Check Alarm Lamp Status	50
Chapter 4 Web Client Settings	51
4.1 Live View	51
4.2 Configuration	51
4.2.1 System	51
4.2.2 Network	52
4.2.3 Video/Audio	56
4.2.4 Image	57
4.2.5 Device	59
4.2.6 Storage	61
4.2.7 Event	63
4.2.8 Two-way Audio Settings	64
4.2.9 Custom	65
4.3 Maintenance and Security	66
4.3.1 Maintenance	66
4.3.2 Security	67
Communication Matrix and Device Command	69

Chapter 1 Overview

Description

DS-PEA series of active panic alarm station supports multiple networks. It provides live view, two-way audio, and customized audio input. It supports linkage with the surrounding cameras and external lamp, sound box, etc. It helps to realize alarm aid in emergency.

Key Features

- Network adaptive and video and audio adaptive
- Audio and video file storage
- H.264/H.265, G.711U, AAC, OPUS, PCM, ADPCM
- Video collection and all-day monitoring with 2MP HD IR camera
- Built-in omnidirectional microphone to realize two-way audio
- Multiple network protocols including TCP/IP, RTSP and SADP
- Supports Standard SIP, ISUP, and HIK-Connect
- Waterproof, anti-electromagnetic interference, tamper-proof and explosion-proof (Panic Alarm Station doesn't support waterproof)

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.

Panic Alarm Station Configuration Guide

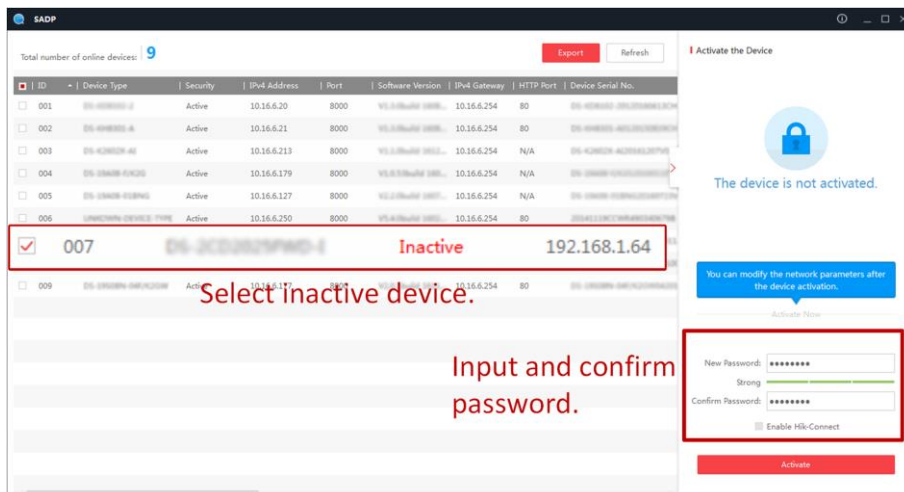


Figure 2-1 Activate via SADP

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.

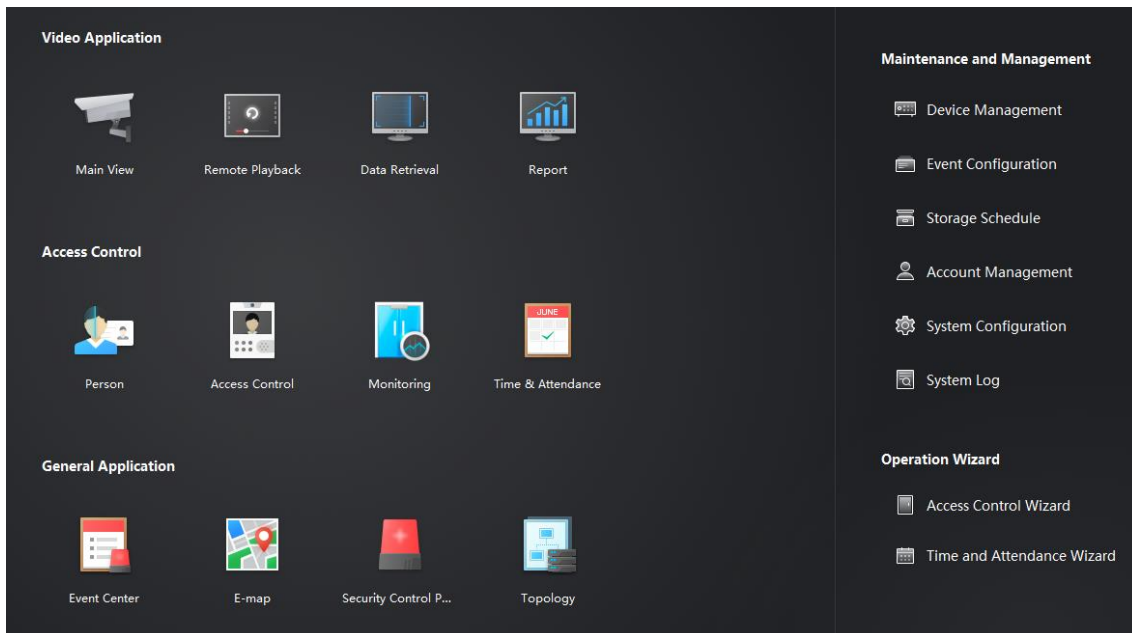


Figure 3-1 Client Software Main Page

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. 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, 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 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

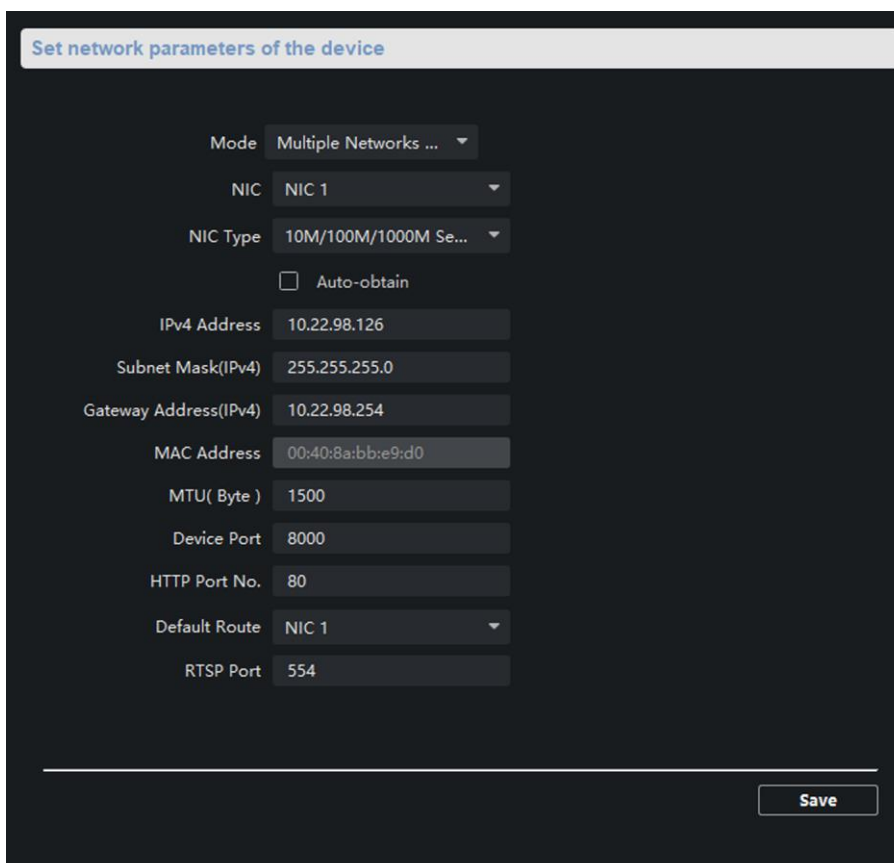
Make sure the cable of the device is connected.

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**.



Mode	Multiple Networks ...
NIC	NIC 1
NIC Type	10M/100M/1000M Se...
	<input type="checkbox"/> Auto-obtain
IPv4 Address	10.22.98.126
Subnet Mask(IPv4)	255.255.255.0
Gateway Address(IPv4)	10.22.98.254
MAC Address	00:40:8a:bb:e9:d0
MTU(Byte)	1500
Device Port	8000
HTTP Port No.	80
Default Route	NIC 1
RTSP Port	554

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**, and **Default NIC** 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 8000, 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.

Default Route


The default Route is NIC 1 and it can be set to NIC 1 or NIC 2.

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.

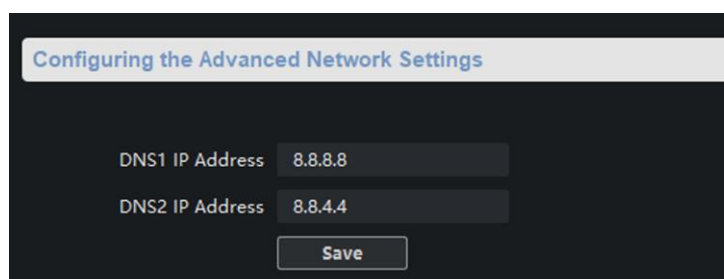


Figure 3-3 DNS Setting Page

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

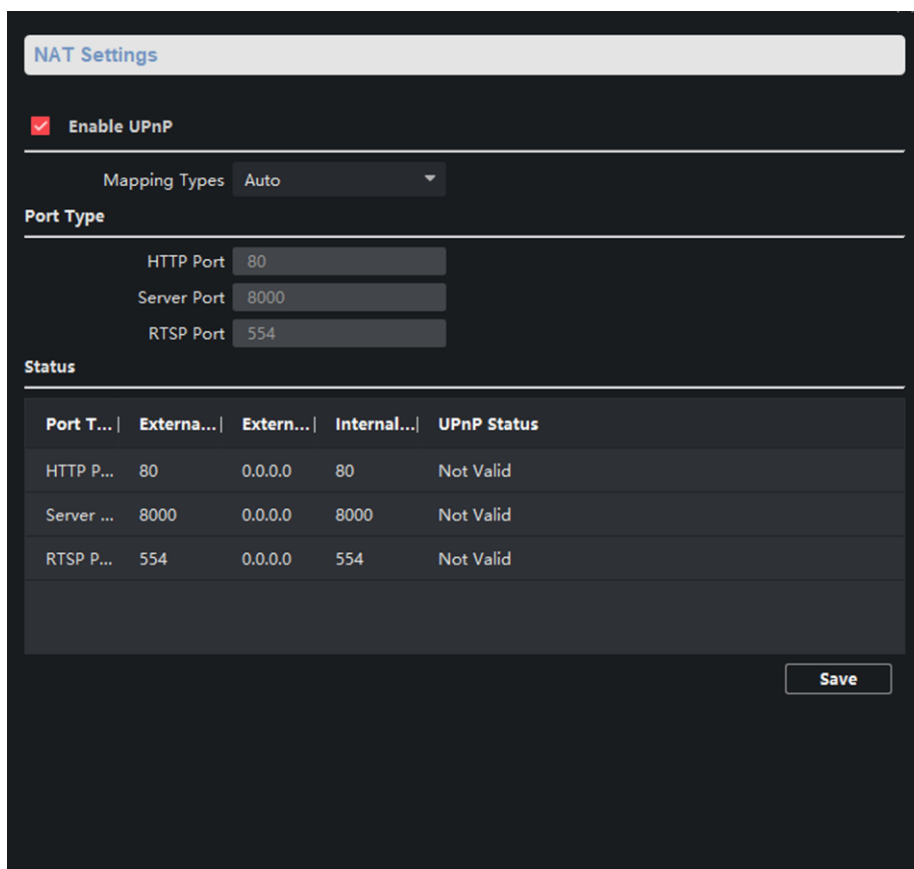
the device is connected to the Wide Area Network via the router.

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.

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.

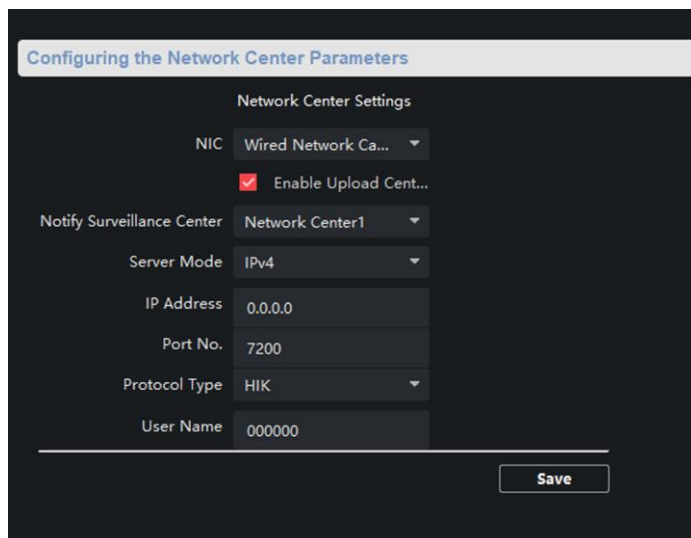
3. Click **Save** to save the settings.

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 Parameters**.



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 Mode** 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**.

3.2.5 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

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

Note

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 private SIP port is 5065 and the standard SIP port is 5060. The available server port number should be between 1024 and 65535.

Local Listening Port

The local port of the device SIP function. By default, the local listening port is 5060. The available 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** or **Wired Network 2**.

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 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

Save OK Cancel

Figure 3-8 Hik-Connect 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.

3.2.7 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 3-9 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.

3.2.8 Set Call Center Parameters

Steps

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

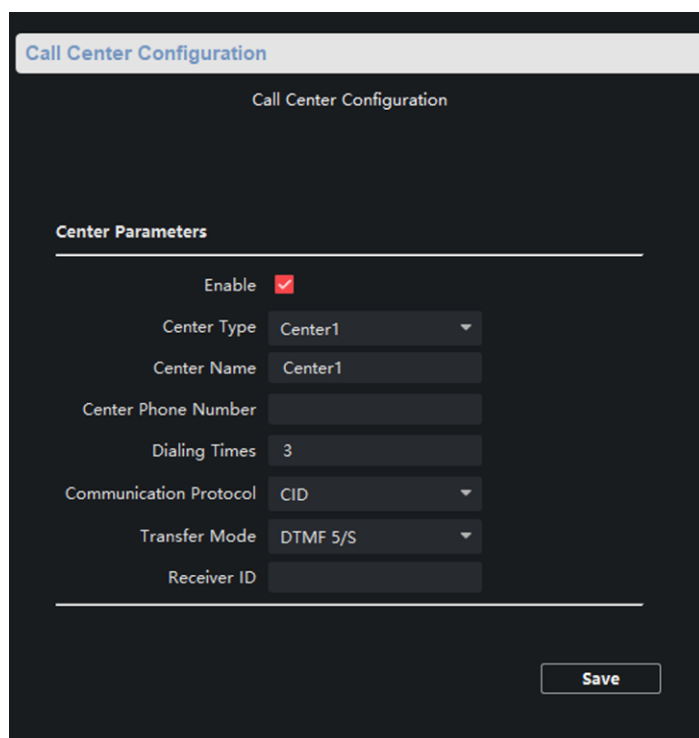


Figure 3-10 Call Center Configuration

2. Check to enable the function
3. Set call center parameters including center type, center name, phone number, dialing times, communication protocol, transfer mode, and receiver ID.
3. Click **Save**.

3.2.9 Set Intercom Parameters

Steps

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

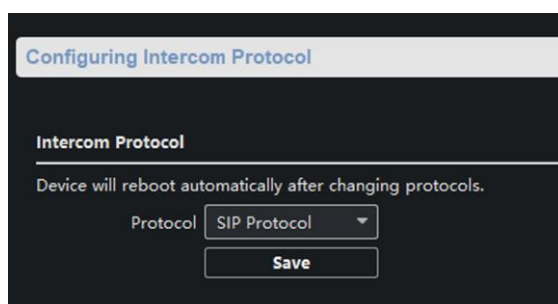


Figure 3-11 Intercom Parameters Configuration

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

The device will reboot automatically after switching the protocol successfully.

3.3 Alarm Settings


3.3.1 Set Zone

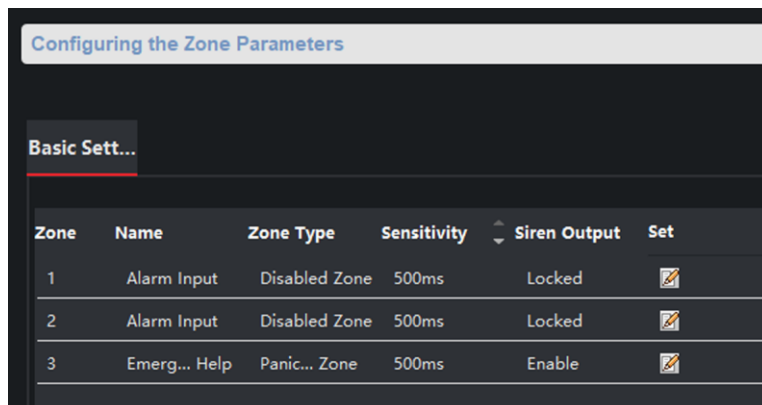
The device supports four alarm input zones and two default zones (emergency call help and consulting). You need to configure zone parameters.

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 **Maintenance and Management** → **Device Management**, select the device in the device list, and click  to enter the **Remote Configuration** page.
2. Go to **Input Settings** → **Zone**.



The screenshot shows a web interface titled "Configuring the Zone Parameters". Under the "Basic Sett..." tab, there is a table with the following data:




Zone	Name	Zone Type	Sensitivity	Siren Output	Set
1	Alarm Input	Disabled Zone	500ms	Locked	
2	Alarm Input	Disabled Zone	500ms	Locked	
3	Emerg... Help	Panic... Zone	500ms	Enable	

Figure 3-12 Zone Configuration Page

3. Select an zone, click .

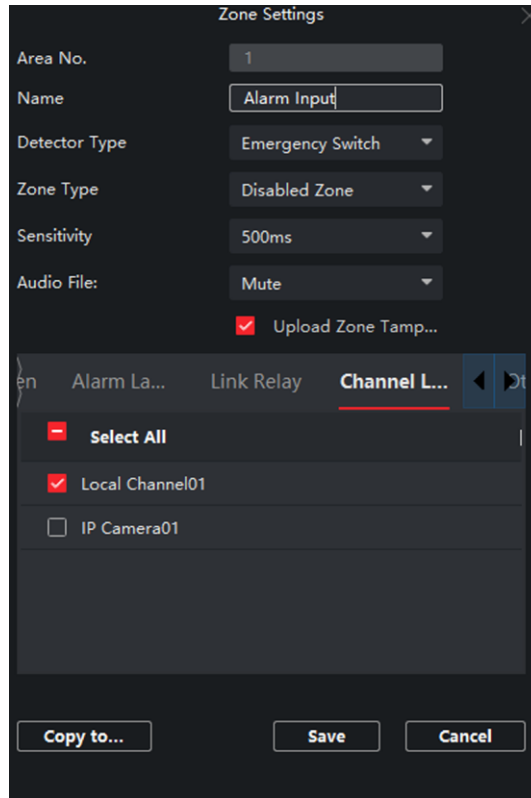


Figure 3-13 Set Zone Parameters

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.

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

Alarm Lamp After the zone is triggered, the selected alarm lamp is on.

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.

Other You can select **Recording Linkage** and **FTP Linkage**.

Recording Linkage

After the zone is triggered, the event video is recorded.

FTP Linkage

After the zone is triggered, the event image is captured.

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.

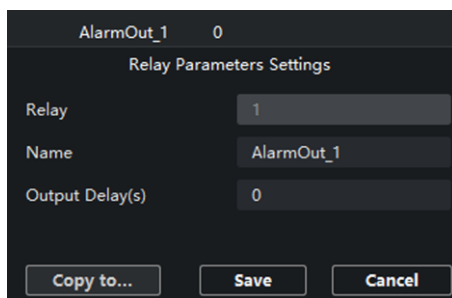


Figure 3-14 Relay Configuration Page

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**.

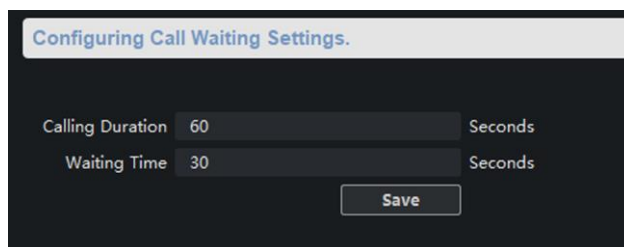


Figure 3-15 Call Waiting Settings Page

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 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**.

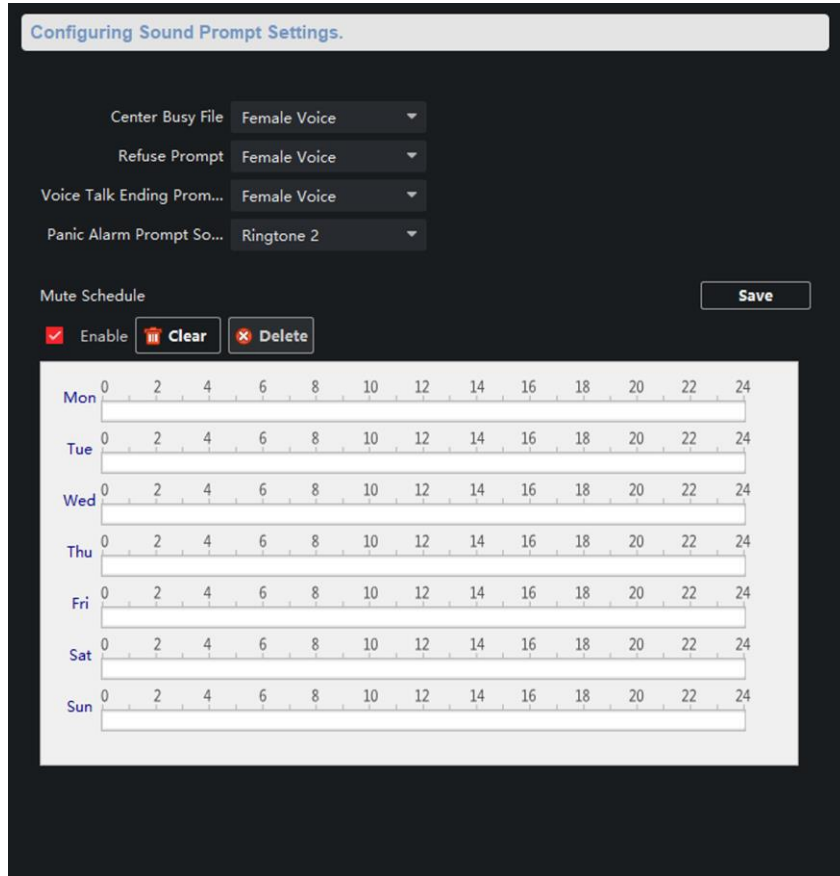


Figure 3-16 Voice Prompt Configuration Page

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**

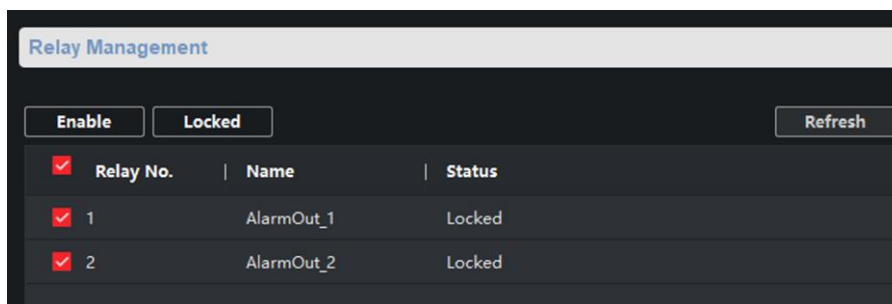



Figure 3-17 Relay Management Page

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**.

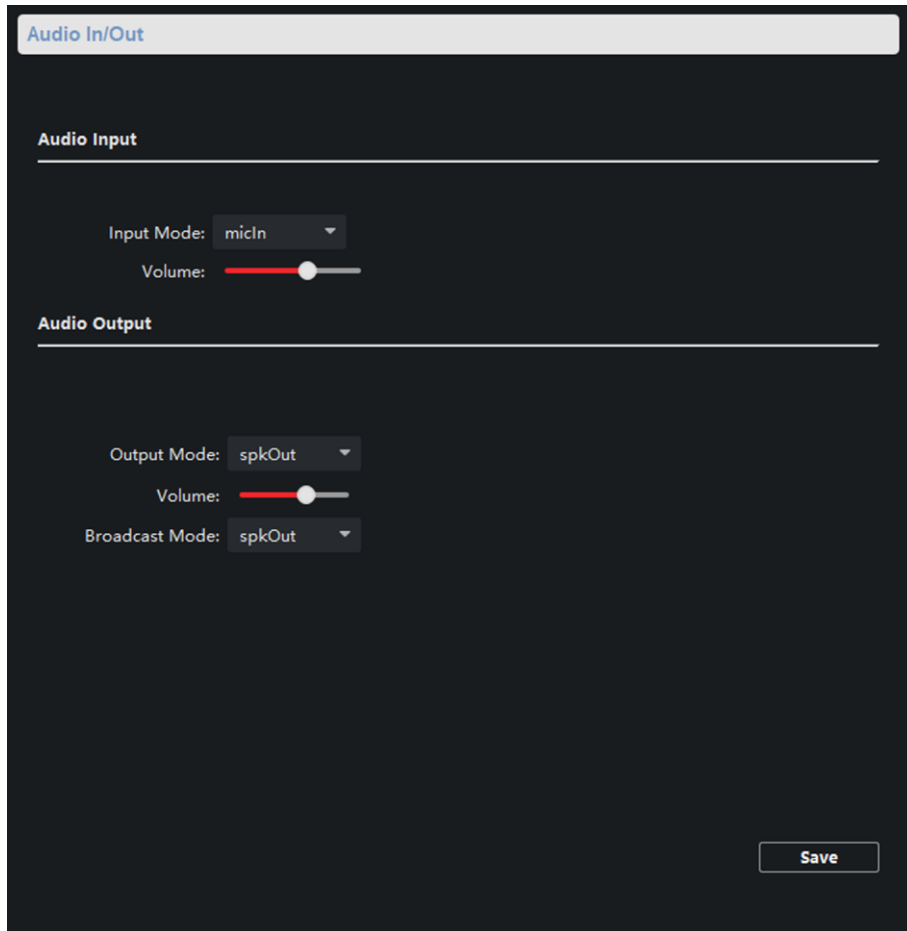


Figure 3-18 Alarm Input/Output Configuration Page

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

Note

- **spkOut** is the device's own audio input/output. **lineOut1** are 3.5mm hole interfaces, which can connect to the external microphones and speakers. The device defaults to **micIn** and **spkOut**.

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**.

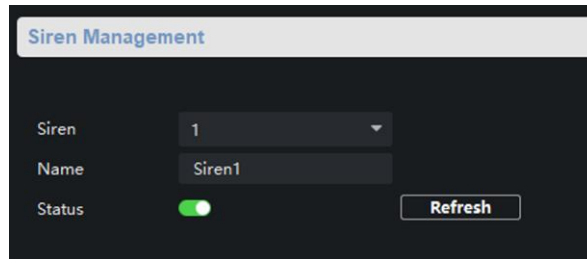



Figure 3-19 Siren Management Page

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 Alarm Light

Open/Close the strobe lamp via the client software.

Steps

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

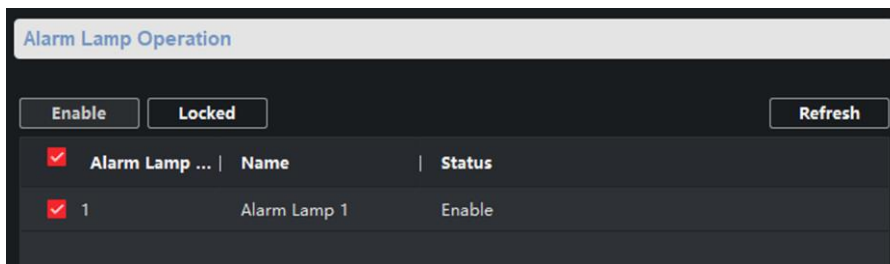


Figure 3-20 Alarm Light Management Page

2. Check the strobe light in the list, and click **Enable/Locked** to open or close the selected strobe light.
3. Optional: Click **Refresh** to refresh the strobe light status.


3.4.5 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**.

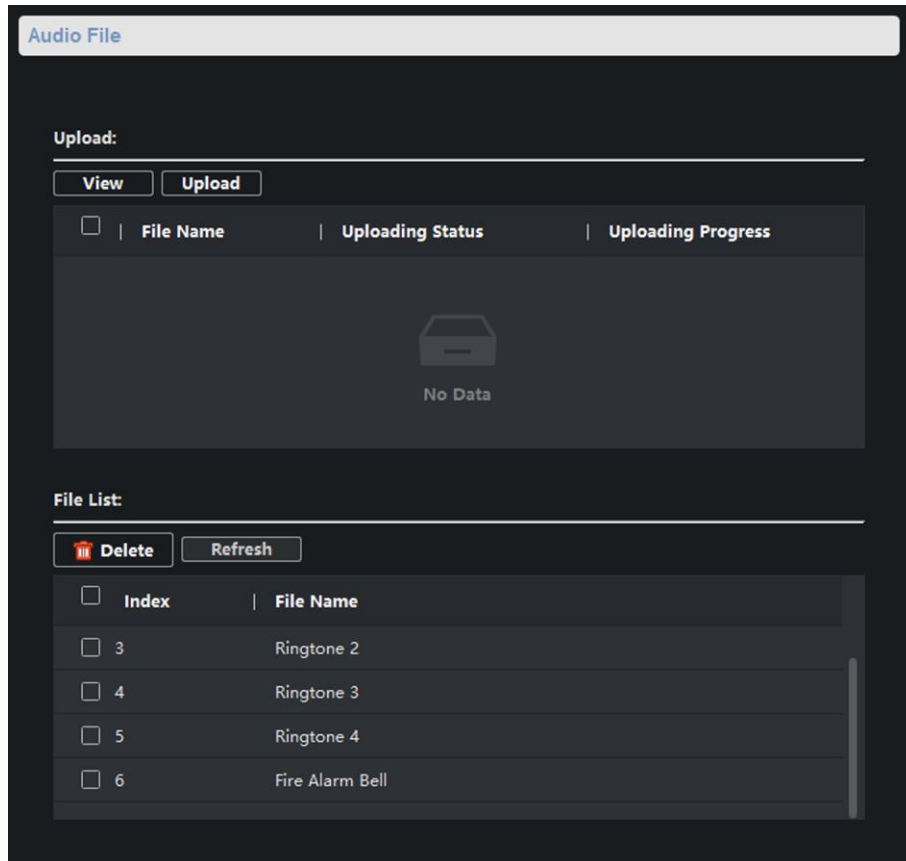


Figure 3-21 Audio File Management

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.

3.4.6 Manage Strobe Light Flicking

Enable the strobe light flicking, and you can configure the strobe light flicking schedule.

Steps

1. Click  to enter the **Remote Configuration** page, go to **Alarm Management** → **Alarm Lamp Flicking**.
2. You can enable the strobe light flicking or configure the schedule.
 - Enable the strobe light flicking
Click **Alarm Lamp Flicking**. Check **Enable Alarm Lamp Flicking** to enable flicking, and set the duration and interval of the strobe light flicking.

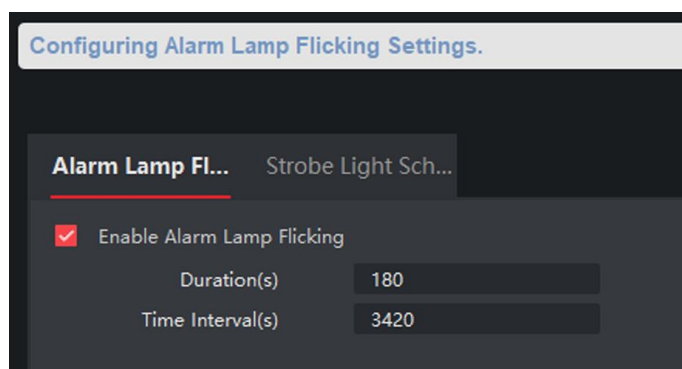


Figure 3-22 Strobe Light Flicking Page

- Enable the strobe light flicking schedule
You can configure the strobe light flicking schedule for the device, and the strobe light will flick in the scheduled time.
Click **Strobe Light Schedule**. Check **Enable Strobe Light by Schedule** to enable schedule, click **Enable Strobe Light** drag the mouse to draw the time period for opening the strobe light.

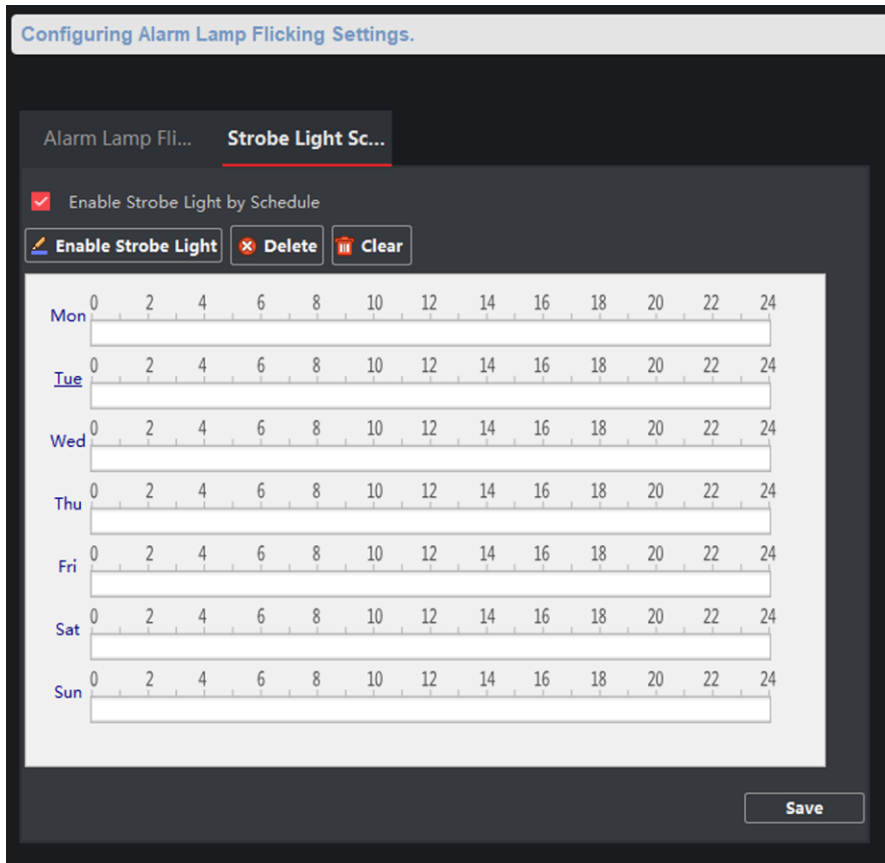


Figure 3-23 Strobe Light Flicking Schedule

Note

You can delete the drawn time period.

- Select a time period, and click **Delete** to delete it.
- Click **Clear** to delete all time period.

3. Click **Save**.

3.5 Event Settings

3.5.1 Schedule Settings

Configure the recording and capture schedule.

Click  to enter the **Remote Configuration** page, go to **Event** → **Schedule**.

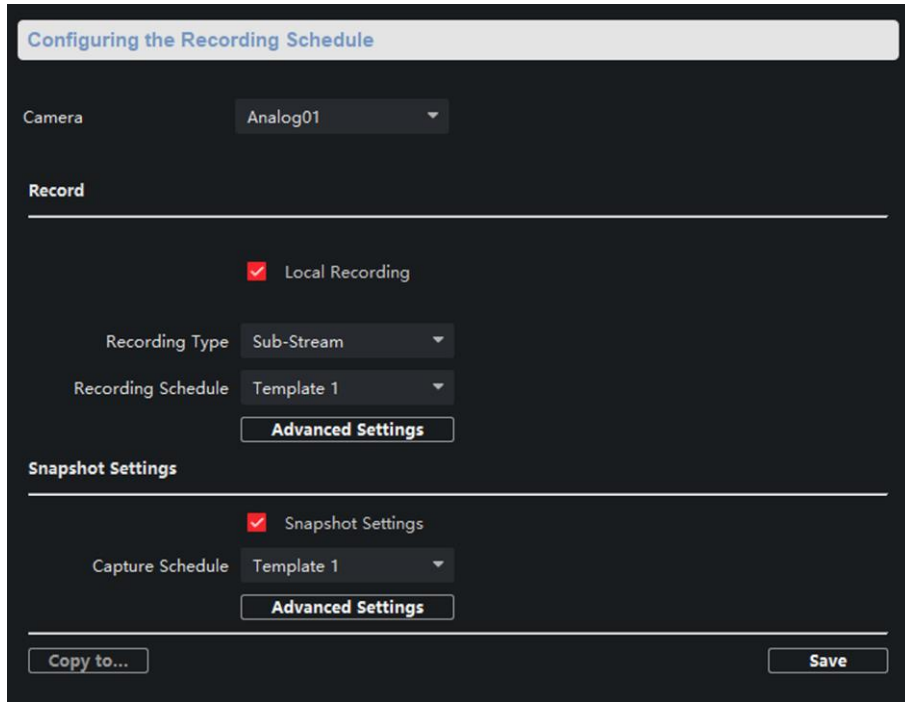


Figure 3-24 Schedule Configuration Page

Select a camera, and configure the record and capture schedule. Click **Save** to save the settings.

Note

The panic alarm station without camera does not support capture schedule configuration.

Record schedule configuration

Local Recording

Check **Local Recording** to enable the recording.

Recording Type

Main Stream and **Sub Stream** is optional.

Recording Schedule

Click the drop-down box of **Recording Schedule**, and configure the recording schedule.

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**.

Advanced Settings

Click **Advanced Settings** and set the pre-recording time, Post-recording time, and record audio as needed.

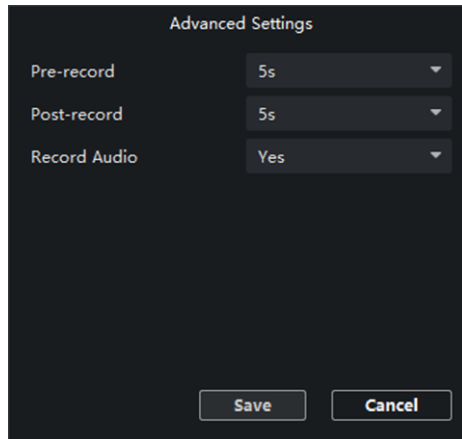


Figure 3-25 Advanced Settings of Record

Pre-record

The pre-recording time can be selected as **5 s** or **not pre-record**.

Post-record

The delay recording time can be selected as **5 s** or **10 s**.

Record Audio

The record audio can be set as **Yes** or **No**. If you select **Yes**, record file will contain audio.

Capture schedule configuration

Capture Settings

Check **Capture Settings** to enable the capture schedule.

Capture Schedule

Click the drop-down box of **Capture Schedule**, and configure the capture schedule. The settings of capture schedule is the same as the settings of recording schedule.

Advanced Settings

Click **Advanced Settings** and configure the capture settings.

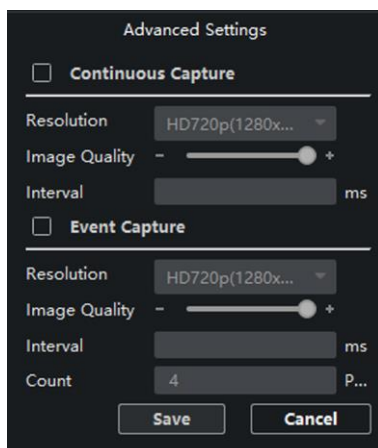


Figure 3-26 Advanced Settings of Capture

- **Continuous capture configuration**

Check **Continuous Capture** to enable the timed capture function, which can capture the image at regular intervals according to the set interval.

Resolution

Select the picture resolution. By default, it is **HD720p(1280×720)**.

Image Quality

Set the image quality. The higher the value, the better the image quality.

Interval

Timed capture based on this time interval.

- **Event capture configuration**

Check **Event Capture** to enable the event capture function, which can capture multiple pictures when an event is triggered.

Resolution

Select the picture resolution. By default, it is **HD720p(1280×720)**.

Image Quality

Set the image quality. The higher the value, the better the image quality.

Interval

The interval between the two event captures.

Count

The total number of the event capture.

Set System Schedule

Steps

1. Select and click the text box of system editable template (**Template01** to **Template08**).
2. Click **Edit** to go to the editing page.

3. Optional: Select the schedule type.

- **Continuous:** Regardless of whether an event is triggered or not, the system records video according to the scheduled recording time period.
- **Event:** The event is recorded during the scheduled recording time period when the event is triggered.
- **Zone:** If an alarm occurs in the zone and the channel linkage of the zone is set, the event is recorded during the scheduled recording time period.

Note

You can refer to **Set Zone** for channel linkage settings.

- **Panic Alarm/ Asking for Help:** The panic alarm /asking for help event is recorded during scheduled recording time period when there is a panic alarm call for help.

Note

If the schedule template does not have the schedule type selection button, you can skip this step.


4. Move the mouse to the time bar. When the cursor changes to a pen, click and drag the mouse within the time bar to draw the schedule time period.

5. Edit the schedule time period.

Modify the time period

Move the mouse to the time period that has been drawn. When the cursor changes to the hand, click the drag time period to modify the time period position; move the mouse to the end of the drawn time period, when the cursor changes to double arrow, you can drag the mouse to modify the time period.


Delete a time period

Select the time period, and click  to delete it.

Delete all time period

Click  to delete all.

Copy the time period

Select the time period and click , you can check the day and copy the current time period to the checked day.

6. Click **Save**.

Set Custom Schedule

Steps

1. Check **Custom** to go to the custom schedule editing page.
2. Draw the schedule time period. For detailed, see **Set System Schedule**.
3. Click **Save**.

3.5.2 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. On the **Remote Configuration** page, go to **Event** → **Audio Exception Detection**

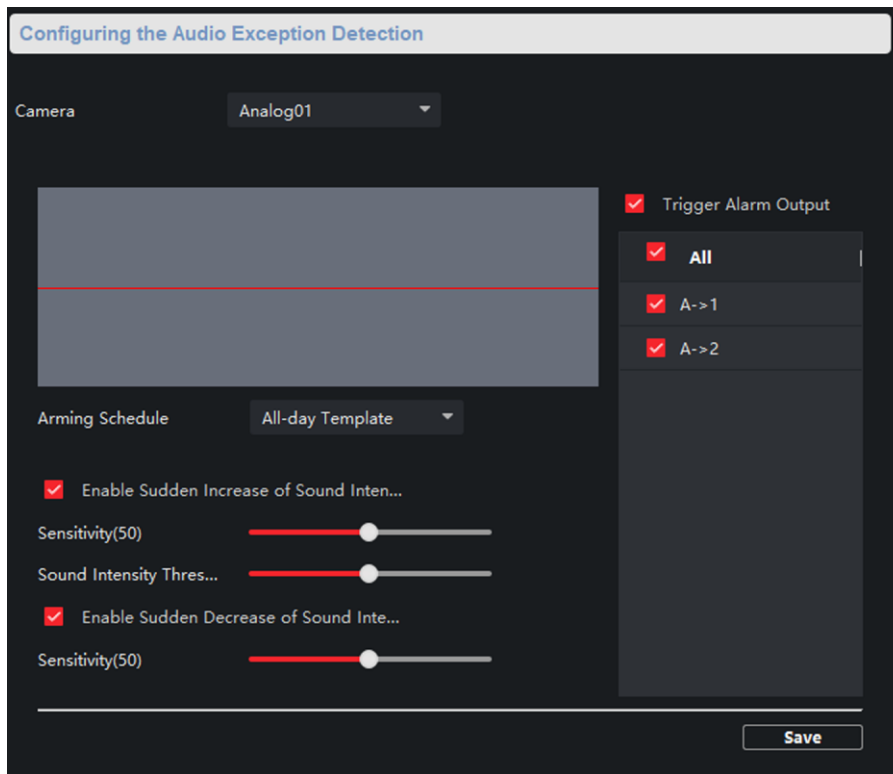


Figure 3-27 Audio Exception Detection Configuration Page

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

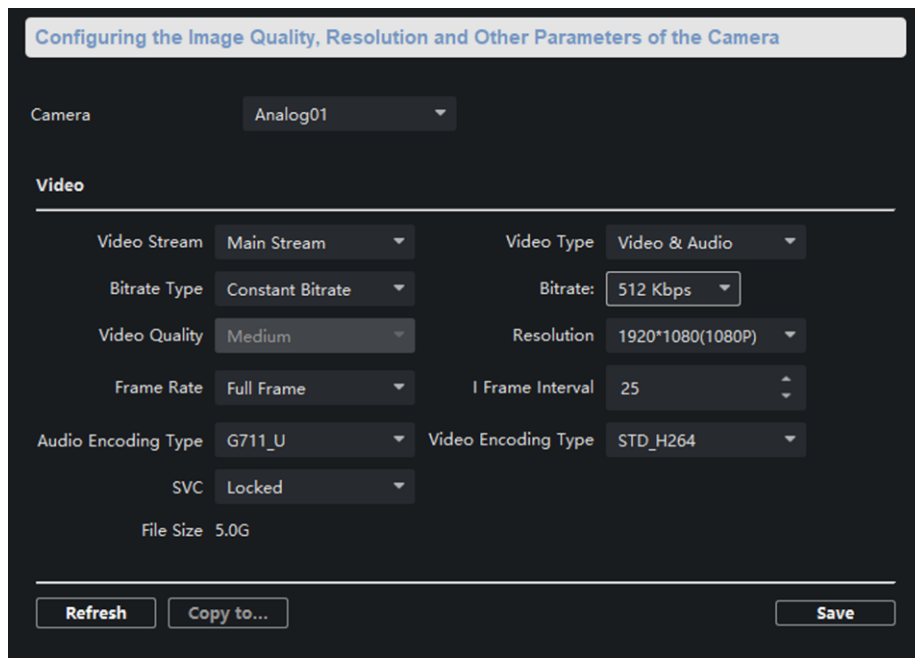
During the configured arming schedule, the audio anomaly event is detected according to the enabled detection items, and the selected alarm output signal is linked when the audio exception is detected.

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**.



The screenshot shows a configuration page titled "Configuring the Image Quality, Resolution and Other Parameters of the Camera". The camera selected is "Analog01". Under the "Video" section, the following settings are visible:

Video Stream	Main Stream	Video Type	Video & Audio
Bitrate Type	Constant Bitrate	Bitrate	512 Kbps
Video Quality	Medium	Resolution	1920*1080(1080P)
Frame Rate	Full Frame	I Frame Interval	25
Audio Encoding Type	G711_U	Video Encoding Type	STD_H264
SVC	Locked		
File Size	5.0G		

At the bottom of the page, there are three buttons: "Refresh", "Copy to...", and "Save".

Figure 3-28 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**.

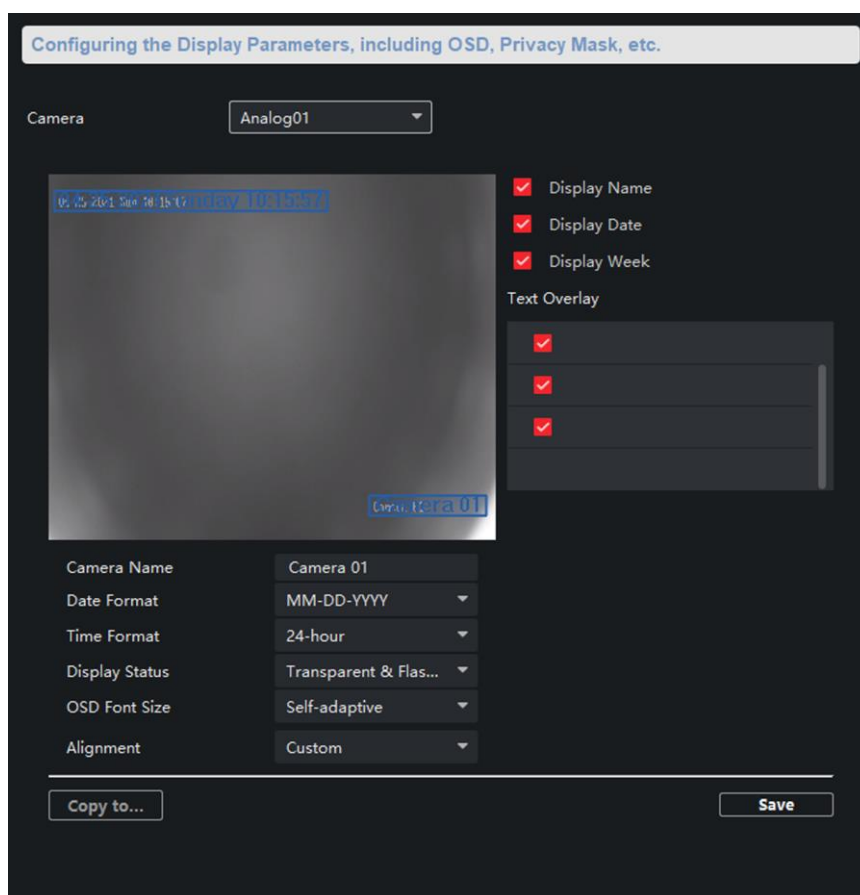


Figure 3-29 View Scale Settings Page

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**.

OSD Format Size

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.

3.6.3 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**.

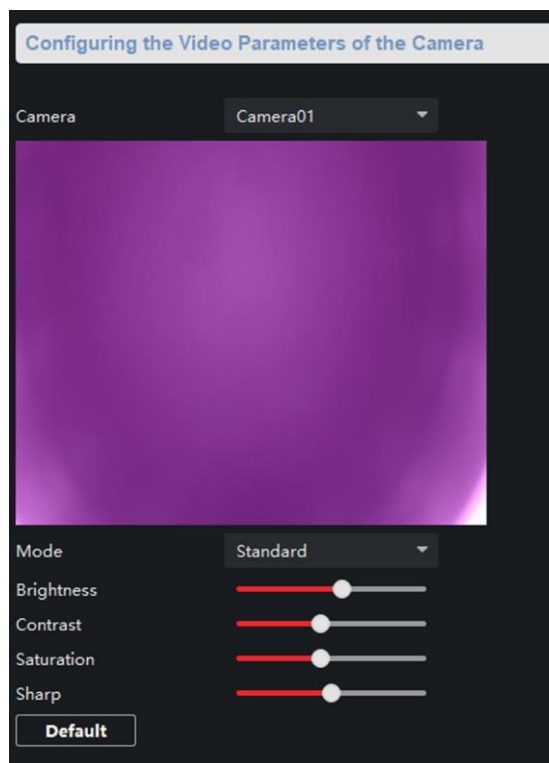


Figure 3-30 Picture Settings Page

Select a camera to configure the video parameters, including brightness, contrast, saturation and sharp.

Note

- By default, the brightness is 6, the contrast is 5, the saturation is 6, and the sharp is 50.

Click **Default**, you can restore all video parameters to default.

3.6.4 Set Intercom Audio

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

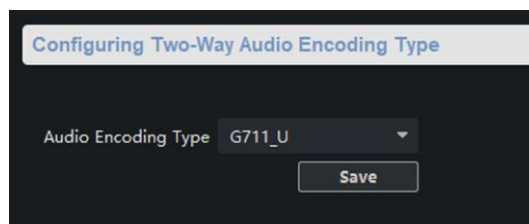


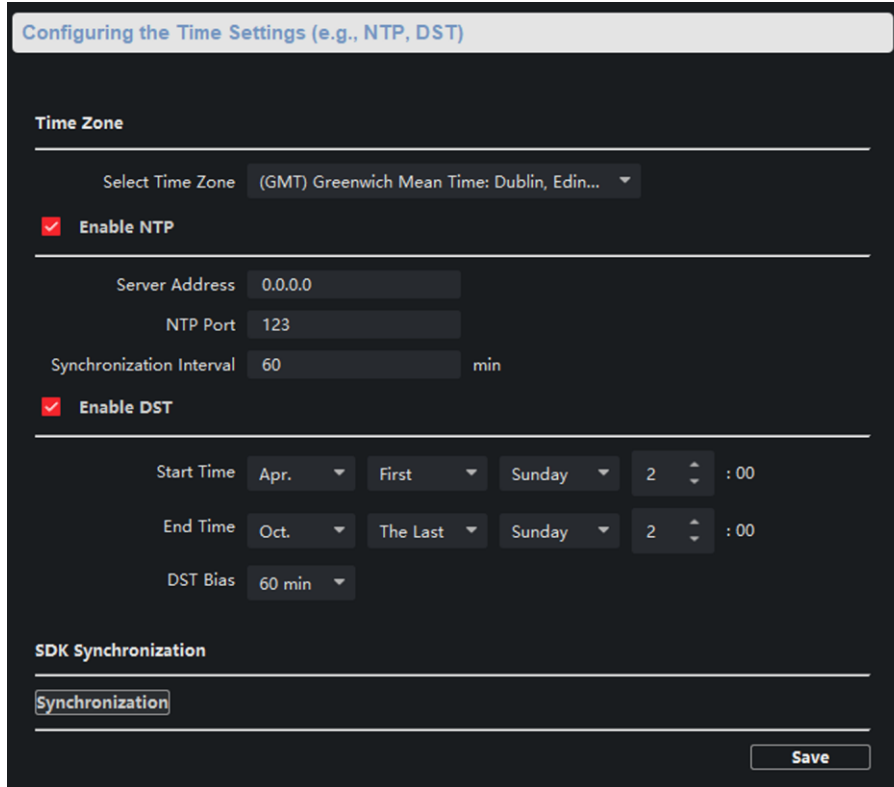
Figure 3-31 Intercom Audio Configuration Page

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.

3.7 System Settings

3.7.1 Set Time

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




The screenshot shows the 'Configuring the Time Settings (e.g., NTP, DST)' page. It features a 'Time Zone' section with a dropdown menu set to '(GMT) Greenwich Mean Time: Dublin, Edin...'. Below this are two checked checkboxes: 'Enable NTP' and 'Enable DST'. The 'Enable NTP' section includes input fields for 'Server Address' (0.0.0.0), 'NTP Port' (123), and 'Synchronization Interval' (60 min). The 'Enable DST' section includes 'Start Time' (Apr., First, Sunday, 2 : 00), 'End Time' (Oct., The Last, Sunday, 2 : 00), and 'DST Bias' (60 min). At the bottom, there is an 'SDK Synchronization' section with a 'Synchronization' checkbox and a 'Save' button.

Figure 3-32 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**.

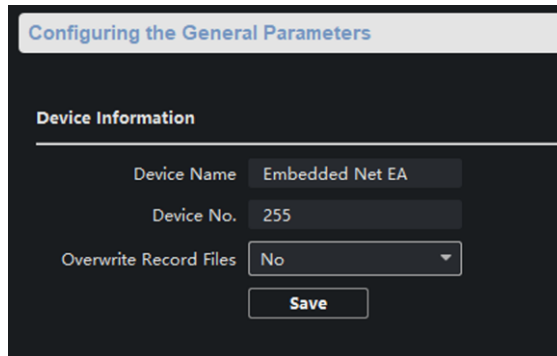



Figure 3-33 System Parameters Setting Page

Set the device name and device No., and select **Yes** or **No** from the **Overwrite Record Files** drop-down box. Click **Save** to save the settings.

Note

Select **Overwrite Record Files** as **Yes**, the new video file will overwrite the earliest video file when the device storage is full.

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**.

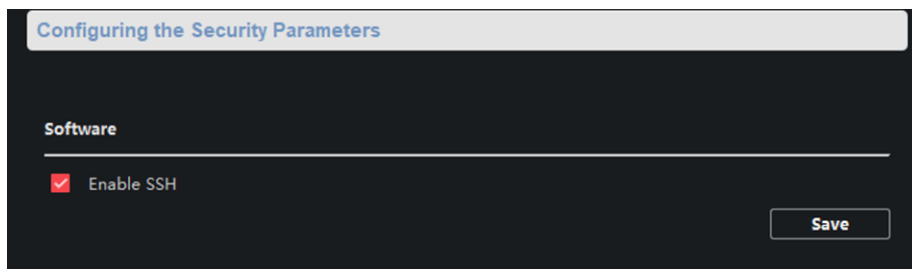


Figure 3-34 Security Parameters Configuration Page

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**.

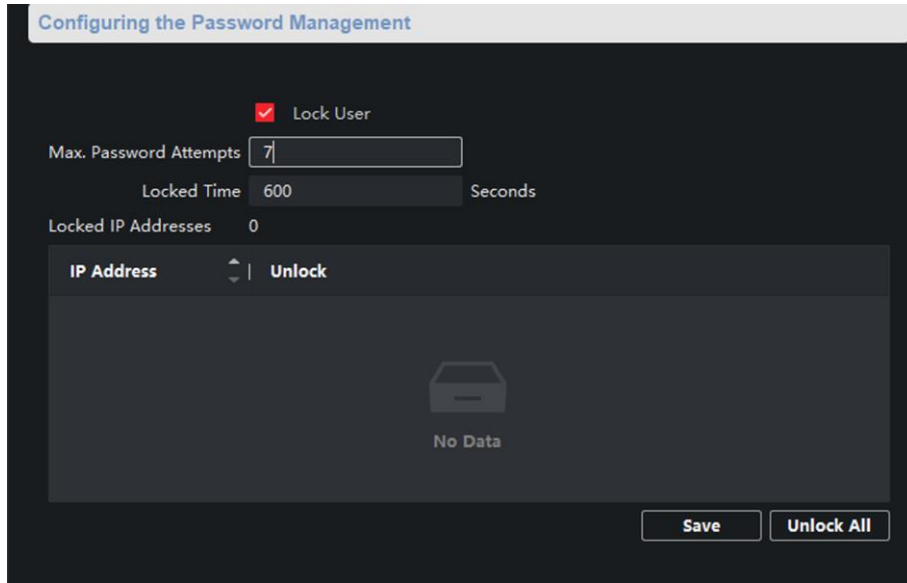


Figure 3-35 Password Management Page

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

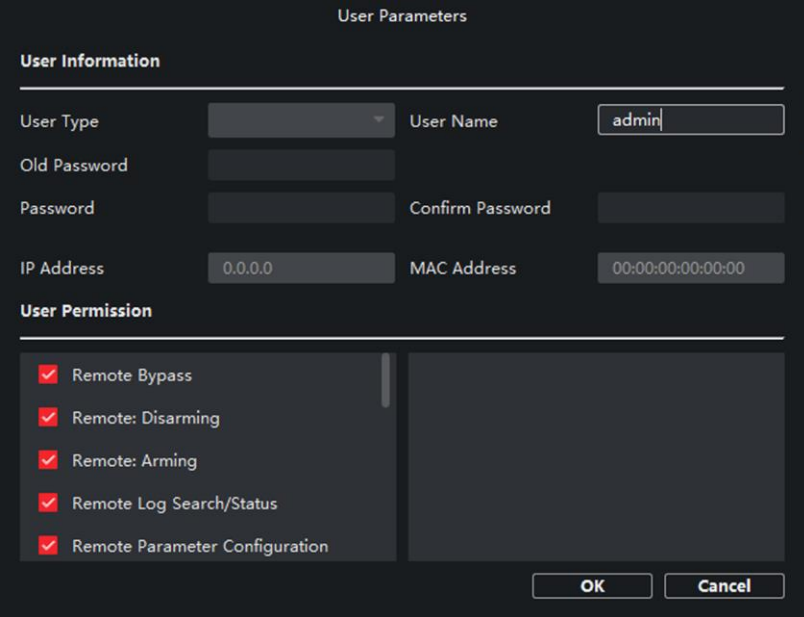


Note

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**.



The screenshot shows a 'User Parameters' configuration window with two main sections: 'User Information' and 'User Permission'. The 'User Information' section includes fields for 'User Type' (a dropdown menu), 'User Name' (containing 'admin'), 'Old Password', 'Password', 'Confirm Password', 'IP Address' (containing '0.0.0.0'), and 'MAC Address' (containing '00:00:00:00:00:00'). The 'User Permission' section features a list of five permissions, each with a checked checkbox: 'Remote Bypass', 'Remote: Disarming', 'Remote: Arming', 'Remote Log Search/Status', and 'Remote Parameter Configuration'. At the bottom right of the window are 'OK' and 'Cancel' buttons.

Figure 3-36 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.

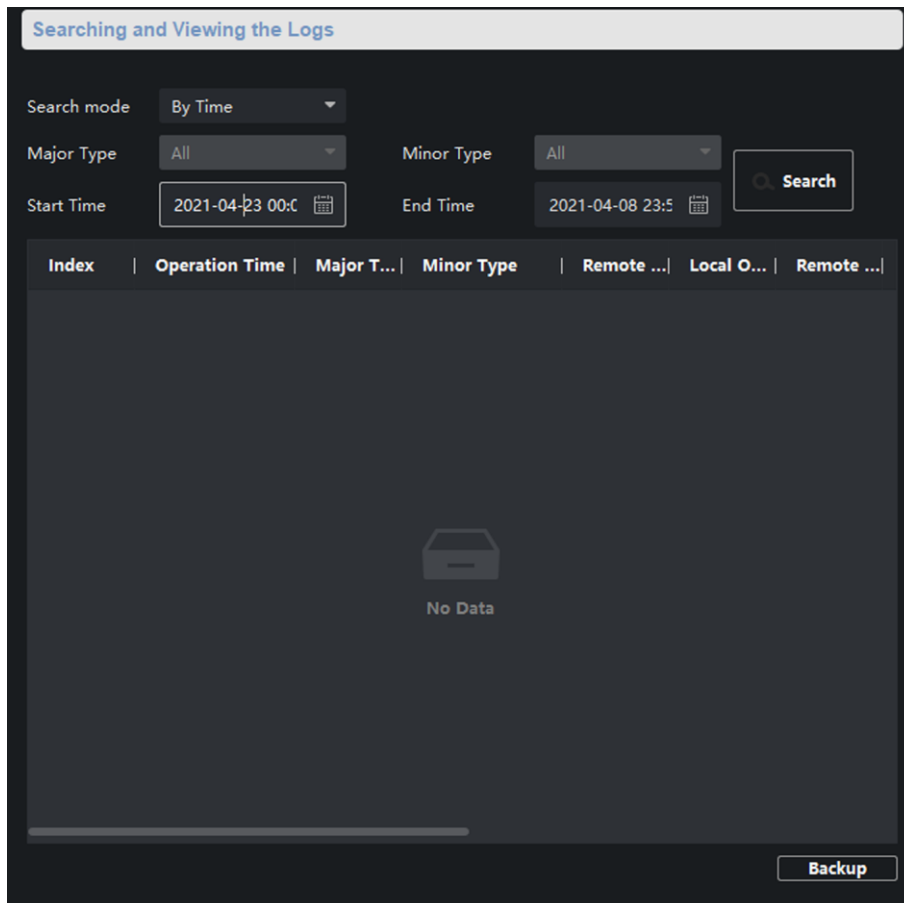


Figure 3-37 Search and View the Log

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**.

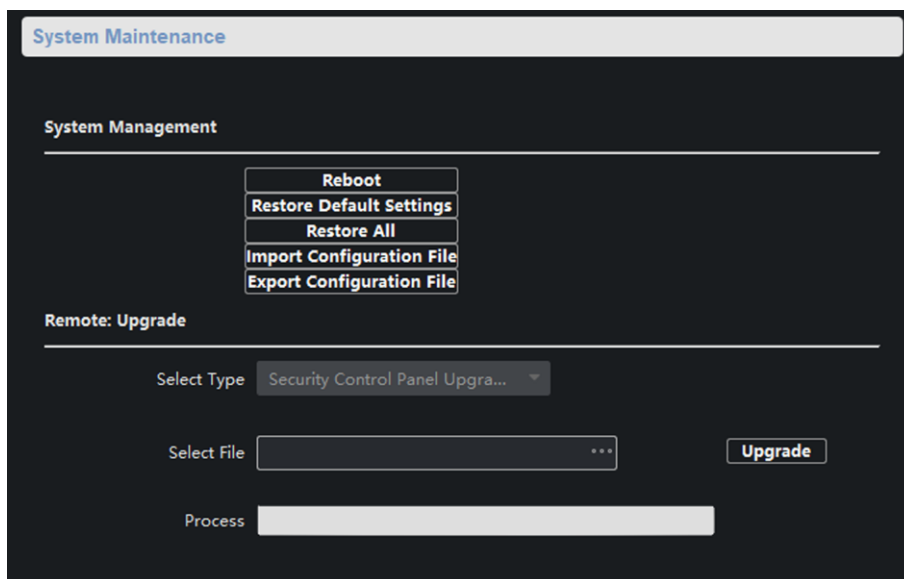


Figure 3-38 System Maintenance Page

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 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.

3.7.8 Check Video & Audio Status

Automatically or manually check the video and audio status.

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

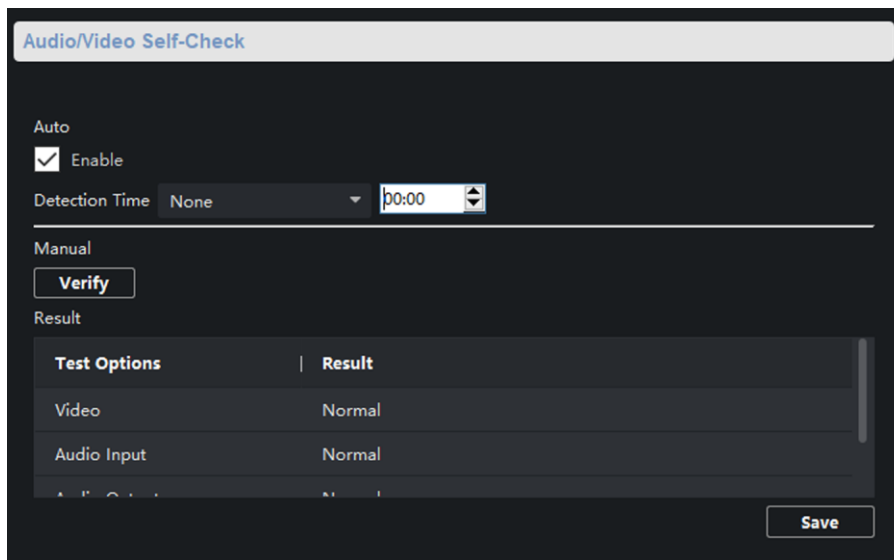


Figure 3-39 Video/Audio Self-Check

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 **Verify** 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 View Device Information

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

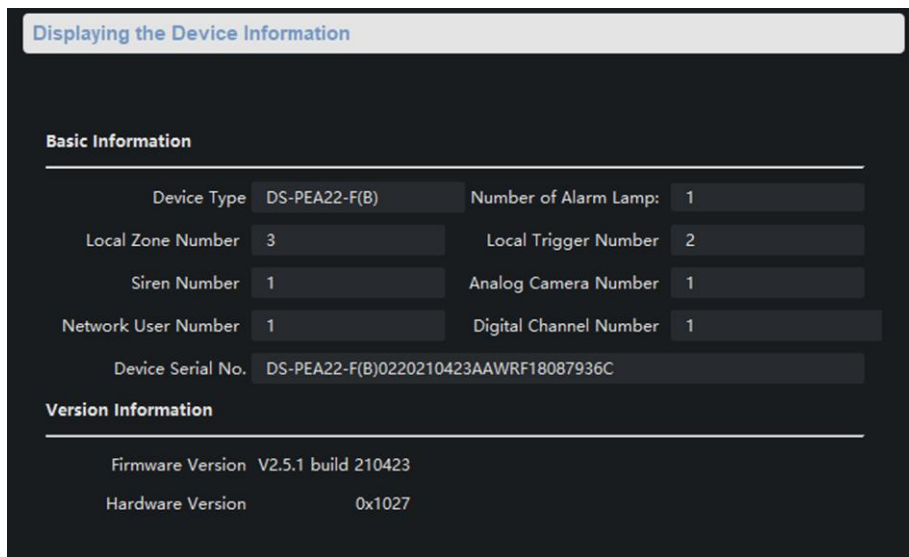


Figure 3-40 Device Information Page

3.8 Set Camera

Configure the camera parameters, including the camera, WDR (Wide Dynamic Range) function, and video standard.

3.8.1 Add Camera

Add, modify and delete an external network camera, and enable the camera.

Steps



Only one network camera can be added to the device.

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

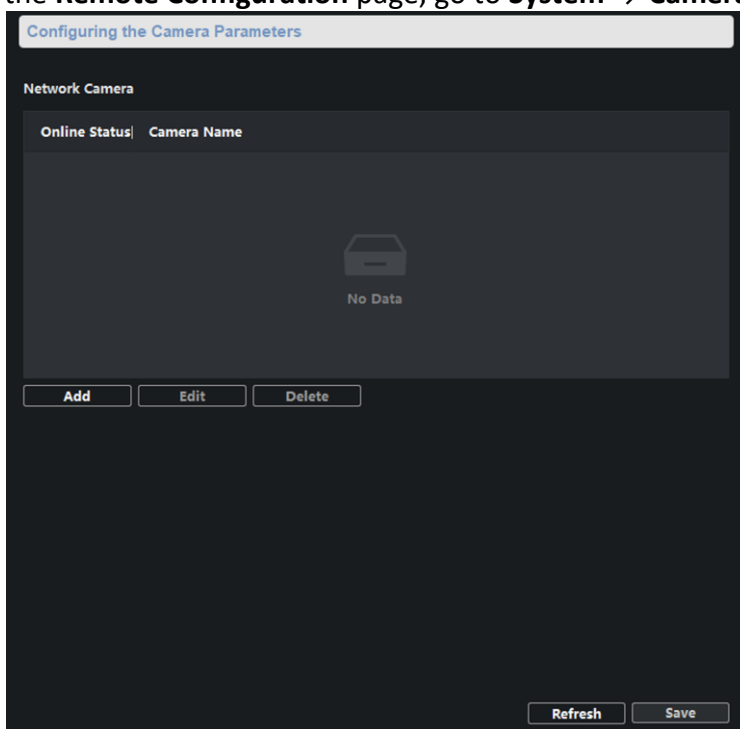


Figure 3-41 Camera

2. Add a camera.
 - 1) Click **Add**, and enter the IP address, port, user name, and password of the camera.
 - 2) Click **Next**, select the camera number.
 - 3) Click **Save**
3. Optional: You can select the camera in the list, and click **Edit** to edit the camera parameters, or click **Delete** to delete the added camera.

4. Click **Save**.
5. Optional: Click **Refresh** to refresh the camera status.

3.8.2 Set Video Parameters

Click  to enter the **Remote Configuration** page, go to **CCD** → **Video Parameters**.

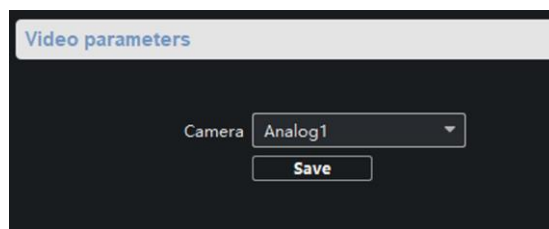


Figure 3-42 Video Configuration Page

Select the camera from the drop-down box. Click **Save**.

3.8.3 Set WDR

When WDR is enabled, the device automatically balances the brightest and darkest parts of the camera picture, improving the dynamic range of the overall picture to see more details of the camera picture.

Steps

1. Click  to enter the **Remote Configuration** page, go to **CCD** → **WDR**.

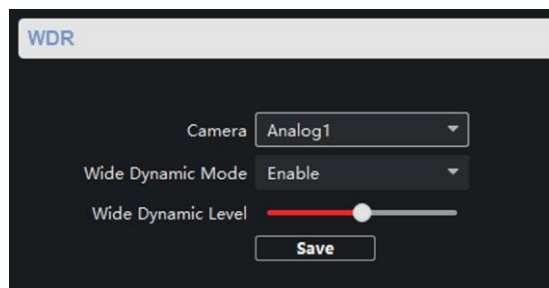


Figure 3-43 WDR function Configuration

2. Select a camera, set **Wide Dynamic Mode** as **Enable**.
3. Set **Wide Dynamic Level**.

Note

The WDR level can change the wide dynamic strength.

4. Click **Save** to enable WDR.

3.8.4 Set Other Parameters

Steps

1. Click  to enter the **Remote Configuration** page, go to **CCD** → **Other**.

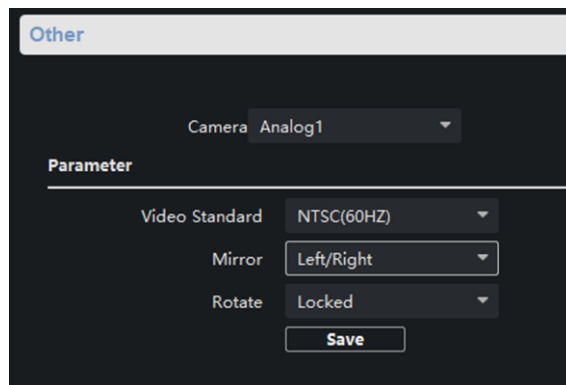


Figure 3-44 Video Standard Configuration Page

2. Select a camera, and set the video standard, mirror and rotate.

Note

When selecting **Video Standard** as **PAL (50HZ)**, the highest frame rate is 25 fps, and when selecting **Video Standard** as **NTSC (60HZ)**, the highest frame rate is 30 fps.

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

Result


The changed video standard parameters take effect after restarting the device.

3.9 Storage Settings

3.9.1 Initialize HHD

In order to store pictures and video files, you must format the MicroSD card first.

Steps

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. Click **Storage** → **General**.

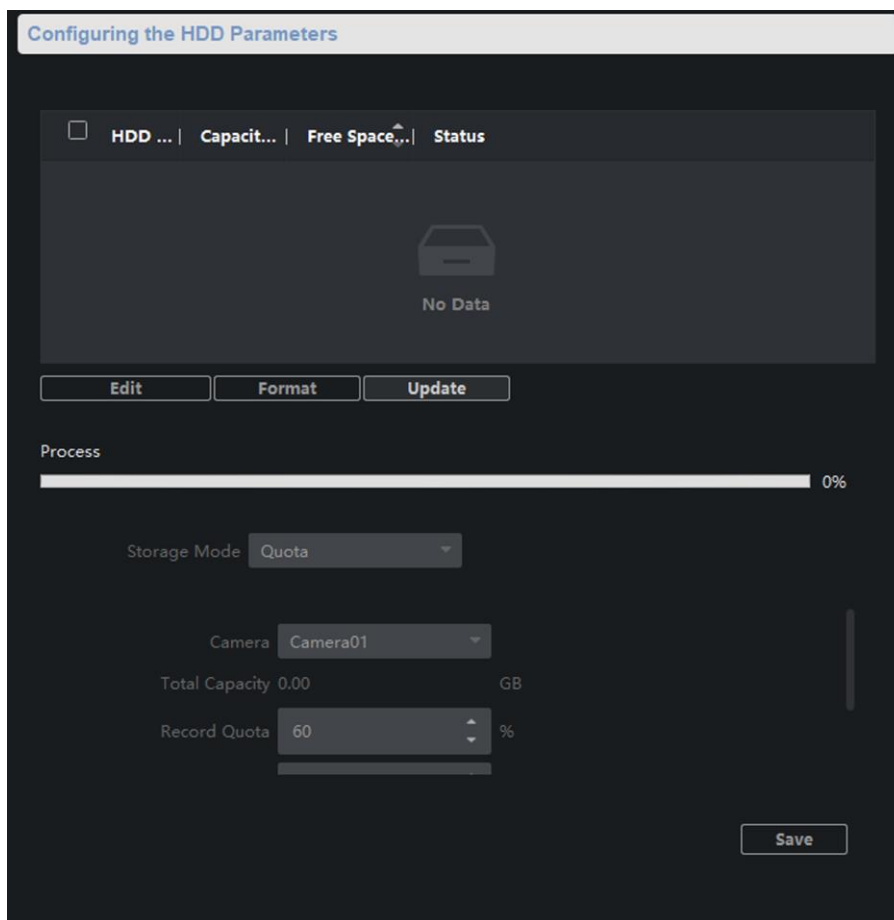


Figure 3-45 HDD Parameters Configuration Page

3. Set the storage quota, and click **Save**.
4. Select and check the MicroSD card, click **Format**.


Note

The progress bar shows the formatted process. When the MicroSD card is formatted, the status of the MicroSD card will display **Active**.

3.9.2 Search for File


Search and download the record file and captured picture.

Steps


1. Click  to enter the **Remote Configuration** page, go to **Storage** → **File**.
2. Select the searched file type as **Record File** or **Picture**.
3. Select the camera, recording type, start time and end time, and click **Search**.
The search results are displayed in the list.
4. Click **Download** to download the result to PC.

3.10 Check Status


3.10.1 Check Zone Status

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


3.10.2 Check Relay Status

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

3.10.3 Check Siren Status

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

3.10.4 Check Alarm Lamp Status

Click  to enter the **Remote Configuration** page, go to **Status** → **Alarm Lamp**, you can view the alarm lamp status.

Chapter 4 Web Client Settings

Enter device IP in the browser, enter user name and password to log in to the website.

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.

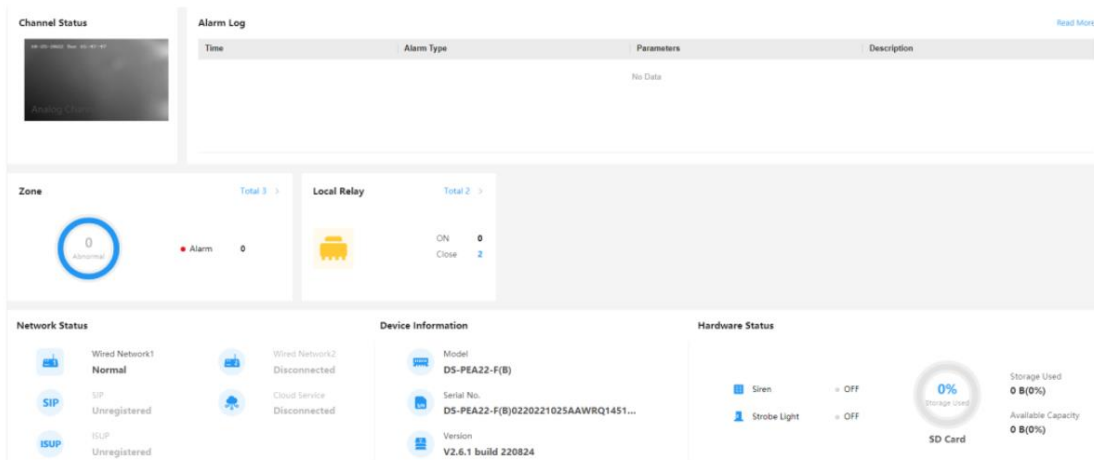


Figure 4-1 Live View Page

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 Information

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-digit 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**.

Device Access – Open Network Video Interface

Steps

1. Click **Network** → **Device Access** → **Open Network Video Interface**.
2. Enable Open Network Video Interface.
3. Click **Add**. Enter user name and password to add the user.
4. Click  to modify the user, and click  to delete the user.
5. Click Save.

Alarm Communication

Network Center

Steps

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

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.

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.

Turning Center

Steps

1. Click **Network** → **Alarm Communication** → **Turning Center**.
2. Enable Alarm Receiver Center and set parameters.

Center Name

It supports numbers and letters.

Center Number

Only 0 to 9 and F can be entered.

Receiver Identification Account

The number can only be 4 digits.

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

Panic Alarm Station Configuration Guide

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-stream 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**.

The screenshot shows the 'Audio' configuration page. At the top, there are two tabs: 'Video' and 'Audio', with 'Audio' being the active tab. Below the tabs, there are three main sections: 'Audio Encoding', 'Audio Input', and 'Audio Output'.
1. **Audio Encoding**: A dropdown menu labeled 'Intercom Audio Encoding' is set to 'G.711ulaw'.
2. **Audio Input**: There are two radio buttons: 'micIn' (selected) and 'lineIn1'. Below them is a slider for 'micIn Volume' with a value of 6.
3. **Audio Output**: There are two groups of checkboxes. The first group is 'Broadcast Audio Output' and the second is 'Intercom Audio Output'. Both groups have 'spkOut' checked, while 'lineOut1' and 'spkOut_lineOut1' are unchecked. Below these is a slider for 'Volume' with a value of 6.
At the bottom center, there is a red 'Save' button.

Figure 4-2 Audio Parameters

4.2.4 Image

Display Settings

Steps

1. Click **Image** → **Display Settings**.
2. Select the channel and set parameters.

Image Adjustment

Drag the slider or enter a number to adjust the brightness, contrast, saturation, and

sharpness of the image.

Backlight Settings

Enable WDR or HLC. Drag the slider or enter a number to adjust the wide dynamic level.

Video Adjustment

Select Mirror. The video can show left/right, up/down or center images. Or you can select to disable this function.

Enable Rotate, the video can rotate.

Select Video Standard as PAL(50HZ) or NTSC(60HZ)

OSD Settings

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.

Panic Alarm Station Configuration Guide

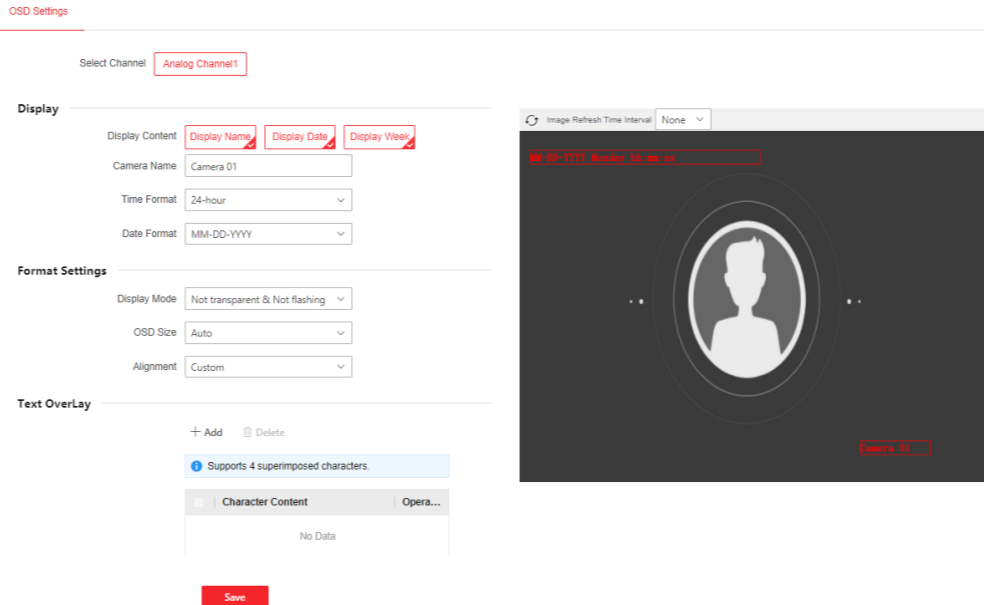



Figure 4-3 OSD Settings

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

Panic Alarm Station Configuration Guide

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**.

Siren Settings

Steps

1. Click **Device** → **Siren**.
2. Enable **Sounder Switch**.
3. Click **Save**.

Strobe Light Settings

Steps

1. Click **Device** → **Strobe Light**.
2. Enable **Strobe Light Switch**.
3. Enable **Scheduled Flashing**, enter lighting duration and light off duration. The strobe light will flash according to the scheduled time.
4. Enable **Flashing Schedule**.
5. Click **Flashing**, move the mouse over the time bar, and long press and drag the left mouse button to draw the time period.

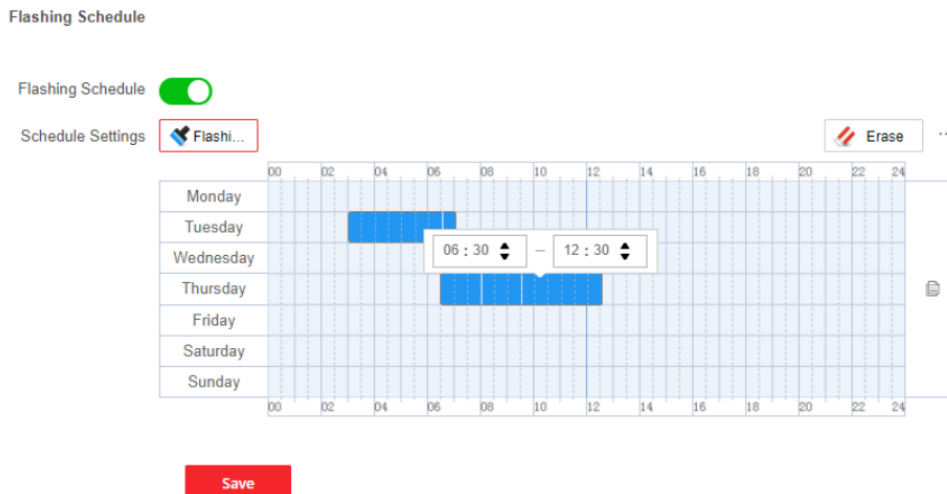


Figure 4-4 Flashing Schedule Settings

6. 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.

7. 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**.

Network Camera Settings

Steps

1. Click **Device** → **Network Camera**.
2. Click **Click to Add**.
3. Enter IP, Port No, user name and password. Click **Save** to add the camera.
4. Click **Delete Camera** to delete.

4.2.6 Storage

Storage Management

Click **Storage** → **Storage Management**.

View SD card status and capacity.

Record Schedule

Steps

1. Click **Storage** → **Schedule Settings** → **Record Schedule**.
2. Enable record schedule.
3. Click **Schedule**, **Event**, **Zone Alarm** or **Panic Alarm**.

Schedule

No matter whether there is an event trigger or not, the system will record according to the scheduled recording time.

Event

During the selected time, when the event is triggered, the event will be recorded.

Zone Alarm

During the selected time, when an alarm occurs in the zone, the event will be recorded.

Panic Alarm

Panic Alarm Station Configuration Guide

During the selected time, when there is an emergency call for help, the call will be recorded.

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

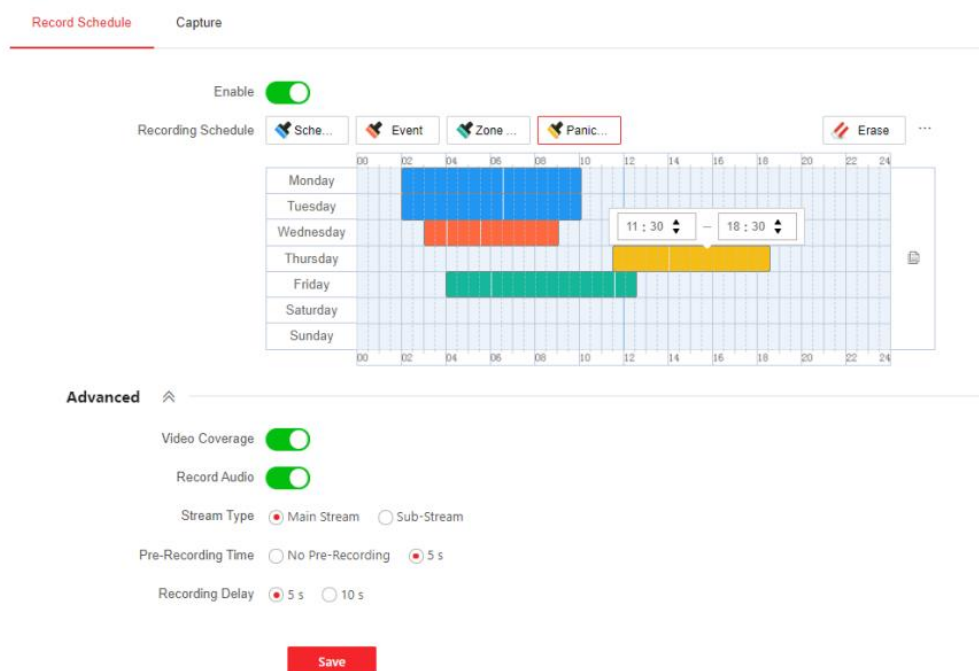


Figure 4-5 Record Schedule Settings

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.

6. Set advanced parameters.

Video Coverage

Enable to support video coverage.

Record Audio

Enable to record audio during recording.

Stream Type

Select Main Stream or Sub-Stream.

Pre-Recording Time

The time before the start time point of the record schedule.

Recording Delay

The time after the end time point of the record schedule.

7. Click **Save**.

Capture

Steps

1. Click **Storage** → **Schedule Settings** → **Capture**.
2. Enable capture schedule.

Note

Please refer to Record Schedule Settings to set the capture schedule.

3. Set capture parameters.

Scheduled Capture

Enable to select Image Quality and set Capture Interval.

Trigger by Event

Enable to select Image Quality and set Capture Interval and Capture Number.

4. Click **Save**.

4.2.7 Event

Steps

1. Click **Event** → **Exception Detection** → **Audio Quality Diagnosis**.

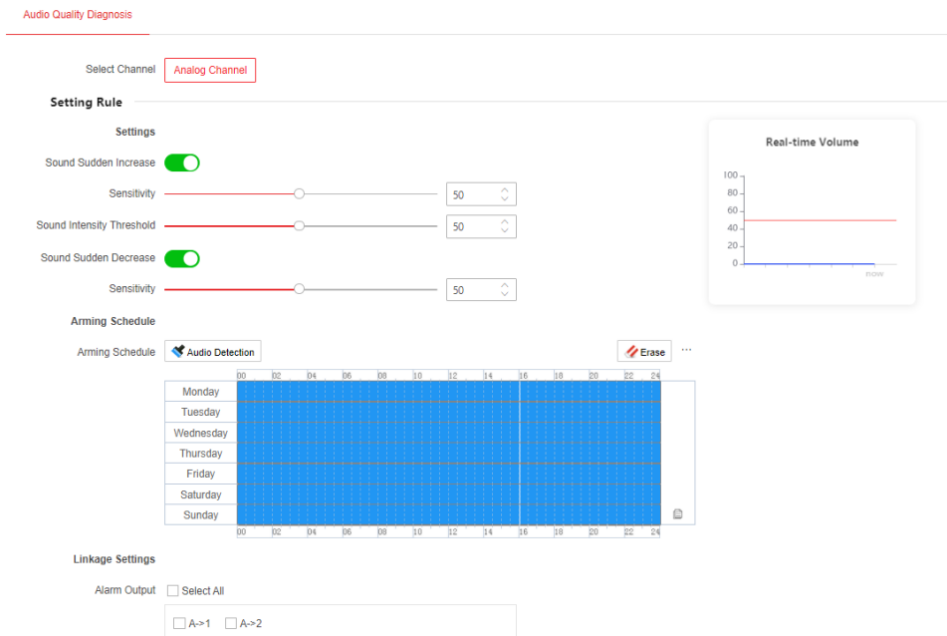


Figure 4-6 Audio Quality Diagnosis

2. Enable **Sound Sudden Increase** and **Sound Sudden Decrease** according to your needs, and set sensitivity and threshold.
3. Click **Audio Detection**, move the mouse over the time bar, and long press and drag the left

mouse button to draw the time period.

4. 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.

5. Select alarm output linkage.

6. Click **Save**.

4.2.8 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.

Panic Alarm Station Configuration Guide

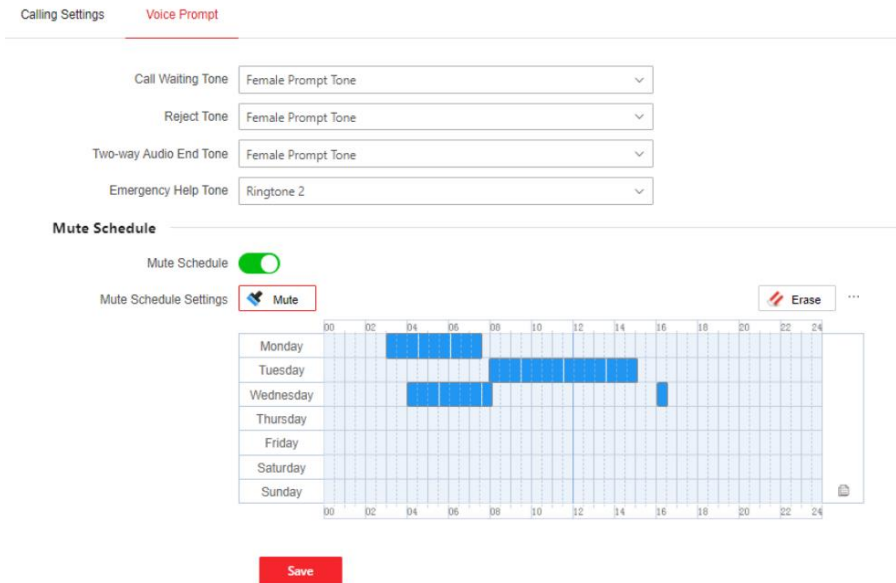


Figure 4-7 Mute Schedule Settings

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.

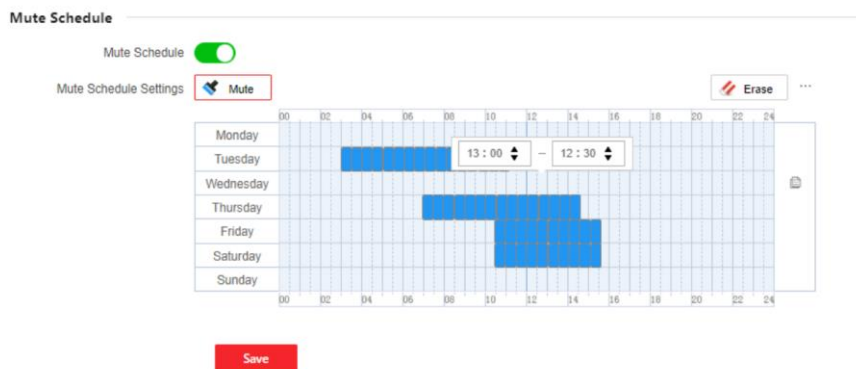


Figure 4-8 Edit Mute Schedule

6. Click **Save**.

4.2.9 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 the browse icon, 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.



You can only enable one kind of list.

Security Service

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

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



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**.
-



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.

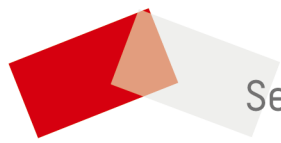
Click  to unlock the locked user in the list.

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

Communication Matrix and Device Command



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



See Far, Go Further