Encoding Box

User's Manual

V1.0.2

Foreword

General

This manual introduces the functions and operations of the encoding box device (hereinafter referred to as "the Device").

Safety Instructions

The following signal words might appear in the manual.

Signal Words	Meaning
⚠ DANGER	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
⚠ WARNING	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
⚠ CAUTION	Indicates a potential risk which, if not avoided, could result in property damage, data loss, reductions in performance, or unpredictable results.
TIPS	Provides methods to help you solve a problem or save time.
NOTE	Provides additional information as a supplement to the text.

Revision History

Revision Content	Release Time	Revision Content
V1.0.2	Update local siganl operations.	June 2023
V1.0.1	Update a port parameter.	July 2022
V1.0.0	First release.	August 2021

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, fingerprints, and car plate number. You need to be in compliance with your local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures which include but are not limited: Providing clear and visible identification to inform people of the existence of the surveillance area and provide required contact information.

About the Manual

- The manual is for reference only. Slight differences might be found between the manual and the product.
- We are not liable for losses incurred due to operating the product in ways that are not in compliance with the manual.
- The manual will be updated according to the latest laws and regulations of related jurisdictions. For detailed information, see the paper user's manual, use our CD-ROM, scan the QR code or visit

our official website. The manual is for reference only. Slight differences might be found between the electronic version and the paper version.

- All designs and software are subject to change without prior written notice. Product updates might result in some differences appearing between the actual product and the manual. Please contact customer service for the latest program and supplementary documentation.
- There might be errors in the print or deviations in the description of the functions, operations and technical data. If there is any doubt or dispute, we reserve the right of final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and company names in the manual are properties of their respective owners.
- Please visit our website, contact the supplier or customer service if any problems occur while using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Important Safeguards and Warnings

This section introduces content covering the proper handling of the Device, hazard prevention, and prevention of property damage. Read carefully before using the Device, comply with the guidelines when using it, and keep the manual safe for future reference.

Operation Requirements

⚠

- Make sure that the power supply of the device works properly before use.
- Do not pull out the power cable of the device while it is powered on.
- Only use the device within the rated power range.
- Transport, use and store the device under allowed humidity and temperature conditions.
- Prevent liquids from splashing or dripping on the device. Make sure that there are no objects filled with liquid on top of the device to avoid liquids flowing into it.
- Do not disassemble the device.
- Operating temperature: -10 °C to +45 °C.

Installation Requirements

⚠ WARNING

- Connect the device to the adapter before power on.
- Strictly abide by local electrical safety standards, and make sure that the voltage in the area is steady and conforms to the power requirements of the device.
- Do not connect the device to more than one power supply. Otherwise, the device might become damaged.

⚠

- Observe all safety procedures and wear required protective equipment provided for your use while working at heights.
- Do not expose the device to direct sunlight or heat sources.
- Do not install the device in humid, dusty or smoky places.
- Install the device in a well-ventilated place, and do not block the ventilator of the device.
- Use the power adapter or case power supply provided by the device manufacturer.
- The power supply must conform to the requirements of ES1 in IEC 62368-1 standard and be no higher than PS2. Note that the power supply requirements are subject to the device label.
- Connect class I electrical appliances to a power socket with protective earthing.
- There should be enough gap between the device and the surrounding area to ensure heat dissipation.
- The rated current and power of the device are 2 A and 24 W respectively.

Maintenance Requirements

Power off the device before maintenance.

Table of Contents

1 Product Overview

1.1 Product Profile

This encoding box is a network audio and video encoding device designed for online video surveillance system. It features powerful data processing capability and stable network function. It is easy to extend, maintain, and convenient to access. This design facilitates installation, deployment, unified control and system management of the entire online video surveillance system, while substantially reducing overall system cost.
With embedded operating system, the Device guarantees that the online video surveillance system works in a safe, stable, reliable and efficient way.

1.2 Features

Table 1-1 Features

Unit	Function	Description
Encoding	Encoding performance	Collects audio and video signals through the HDMI and DP ports, and then encodes (H.264/H.265) the signal sources which are transmitted through network. You can preview images of signal source on the web.
Network	Attribute configuration	IP, gateway, subnet mask and other network parameter configuration can be controlled remotely with network.
	NTP	Synchronize system time with the NTP server.
Alarm	Buzzer alarm	Provides buzzer alarm in case of network offline, IP address conflict and MAC address conflict.
Serial port	General serial port	Device debugging console.
User management	Account management	● Add, delete, and modify users or user groups. ● Modify user password.
	Authority management	Configure different authorities for different users.
	Security management	The account will be locked for 30 minutes after 5 consecutive failed login attempts.
Others	Version information	Displays important hardware port information and software version information.
	Search log	Important events are recorded in the log. You can search for the log according to category.
	Time synchronization	System time can be configured manually, or synchronized directly.

Unit	Function	Description
	Auto maintenance	Provides automatic maintenance of the Device at a fixed time.
	DNS	Domain name service.
	Program upgrade	Network upgrade.
	Development support	Provide software development kit (SDK) of the encoder, demonstration software and development description.

📖

- For specific installation requirements of the Device, refer to engineering construction specifications and national standards.
- The cable quality and length affect the video quality. The video might blur, have noise or black edge. Sometimes the video quality might vary when the same video is output with different cables.

2 Unpacking and Cable Connection

2.1 Unpacking and Checking

When you receive the Device, check whether there is any visible damage. The protective materials used for the package of the Device can resist most of accidental collisions during transportation. Keep the label at the bottom of the box well. You might need to present the serial number on the label when we provide after-sales service.

2.2 Device Structure

2.2.1 Front Panel

Figure 2-1 Front panel

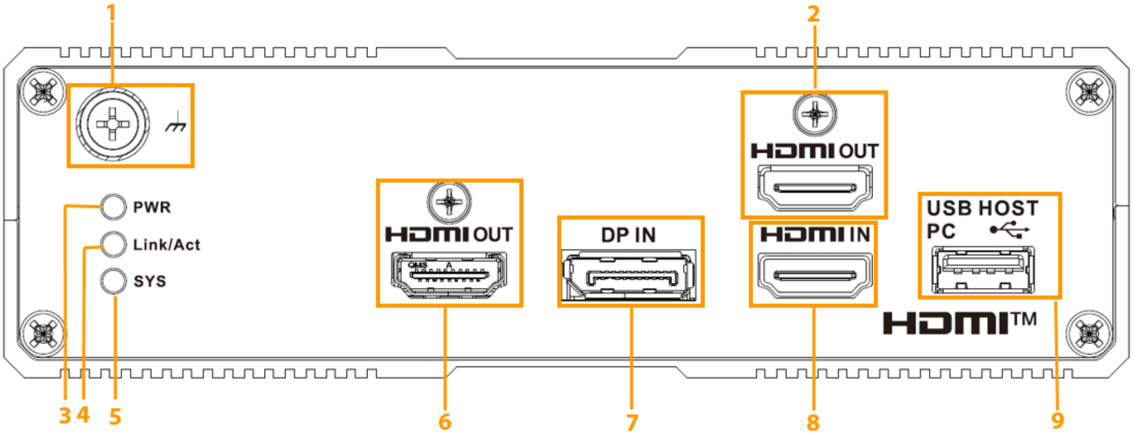


Table 2-1 Description for front panel

No.	Description	No.	Description	No.	Description
1	Ground screw.	2	HDMI video loop output.	3	Power indicator. The light is solid red when the power is on.
4	Reserved indicator.	5	Operation indicator. It is on when application program is operating.	6	HDMI signal output.
7	DP signal input.	8	HDMI video input port.	9	Reserved port.

2.2.2 Rear Panel

Figure 2-2 Rear panel

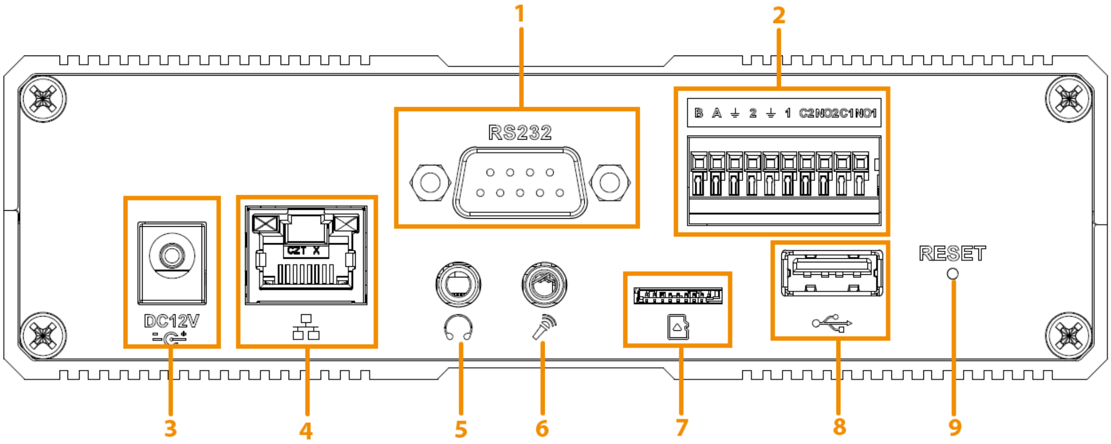


Table 2-2 Description for rear panel

No.	Description	No.	Description	No.	Description
1	RS-232 debugging serial port.	2	RS-485 port, alarm input and alarm output.	3	Power input port.
4	RJ-45 network port.	5	3.5 mm microphone port (Reserved).	6	3.5 mm earphone port (Reserved).
7	SD (TF) card slot (Reserved).	8	USB2.0 ports (Reserved).	9	Reset button. Press and hold it for 5 seconds, and the system will restore to factory settings.

2.3 Installation

2.3.1 Installation and Connection

Figure 2-3 Connection of front panel

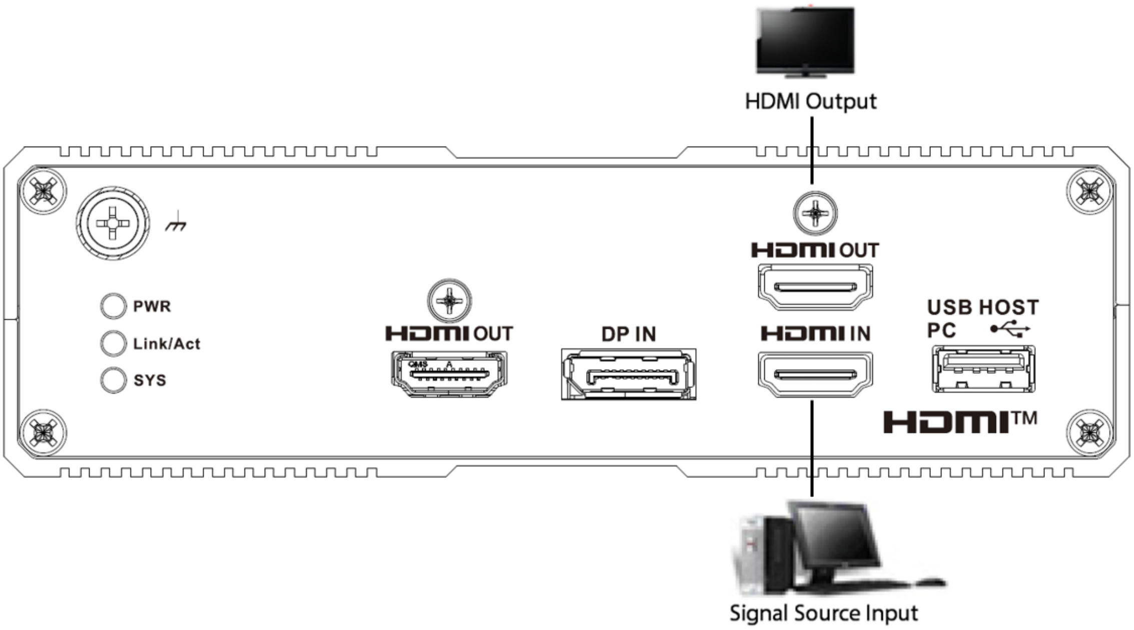
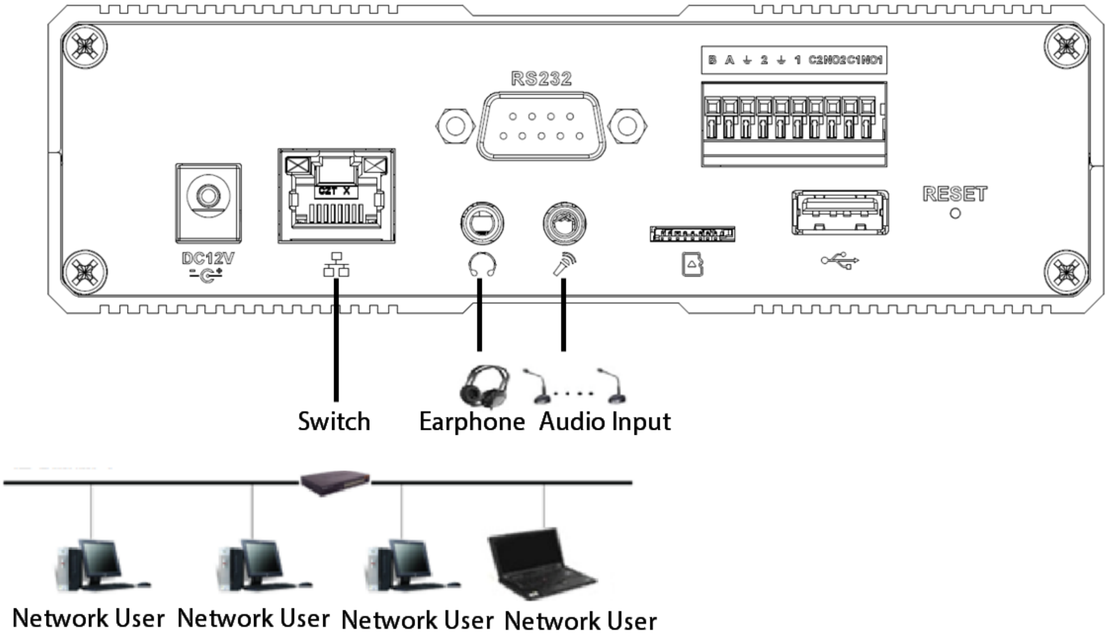


Figure 2-4 Connection of rear panel



2.3.2 Audio and Video Input Connection

Use HDMI IN to input audio and video signals.

2.3.3 Video Output Device Selection and Connection

The Device has 1-channel HDMI input port, 1-channel HDMI loop output port and 1-channel HDMI output port. The loop output port displays signal of the same source, and the HDMI output port is used in local GUI.

2.3.4 Audio Output Device Selection and Connection

The audio output signal can directly connect to low-impedance earphone, active speaker, and can drive other sound output devices through amplifier. Output howling easily occurs when external speaker and pickup cannot be separated spatially. You can take measures as follows:

- Adopt pickup with better directing property.
- Reduce volume of the speaker, until it is lower than threshold value of producing howling.
- Use more sound-absorbing materials in decoration to reduce voice echo and improve acoustics environment.
- Adjust the layout of pickup and speaker, to reduce howling risk.

📖

The Device does not support local operations, please go to the webpage for configurations after the installation.

3 Web Operations

3.1 Network Connection

Procedure

Step 1 Connect the Device and computer to the network.

Step 2 Configure the device IP address, subnet mask, and gateway respectively.

Step 3 Ping ***.***.***.*** (IP of the Device) to check if the network is available.

Step 4 Open Internet Explorer, select **Tools** > **Internet Options** > **Security** > **Custom Level**. Select **Enable** or **Prompt** for all ActiveX controls and plug-ins.

We recommend IE8 or a later version.

3.2 Login

Procedure

Step 1 Enter IP address of the Device in the address bar of the browser.

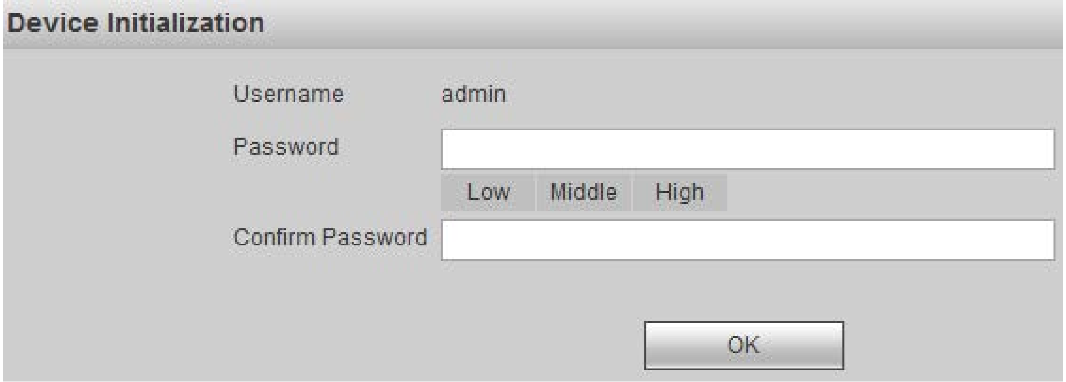
Step 2 Read the **Software License** and **Privacy Policy** and then select **I have read and agree to the terms of the Software License Agreement and Privacy Policy**, and then click **Next**.

Step 3 Initialize the device.

1) Set a strong admin user password according to the password strength prompt.

The password must consist of 8–32 non-blank characters and contain at least two types of the following characteristics: Uppercase, lowercase, number, and special character (excluding ' " ; : &). **Password** and **Confirm Password** must be the same.

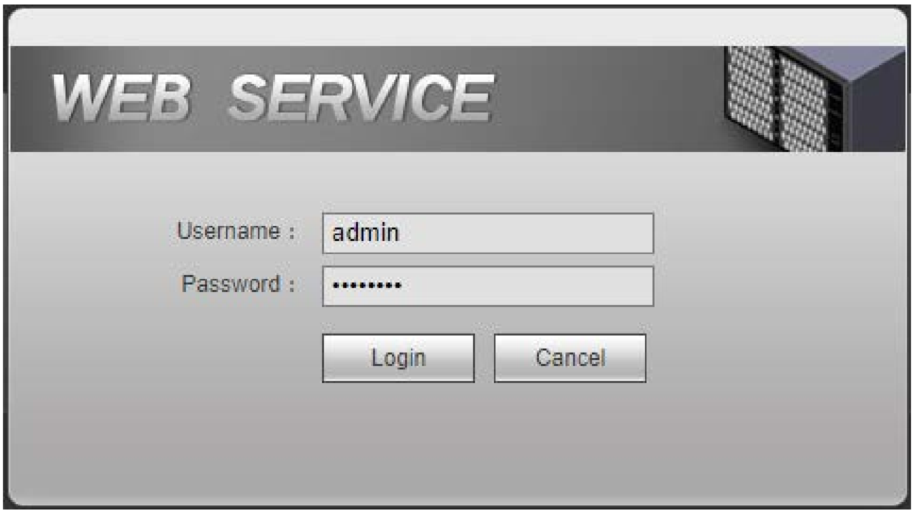
Figure 3-1 Device initialization


Username admin

2) Click **OK**.

Step 4 Enter username and password, and then click **Login**.

Figure 3-2 Login



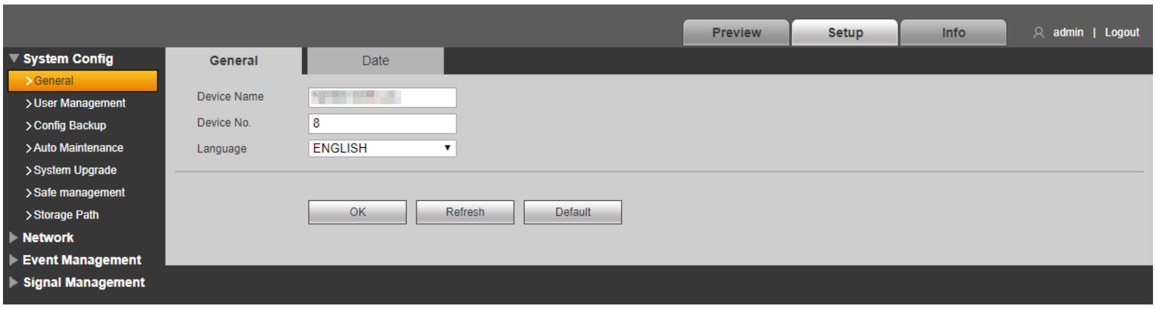
Username : admin

Password : ••••••••

Step 5 Install or load the plug-in as prompted by the system.

Click **Logout** to log out the system.

Figure 3-3 Operation page



Device Name

Device No. 8

Language ENGLISH

3.3 Preview

Click **Preview** to view the real-time monitoring image.

Figure 3-4 Preview page

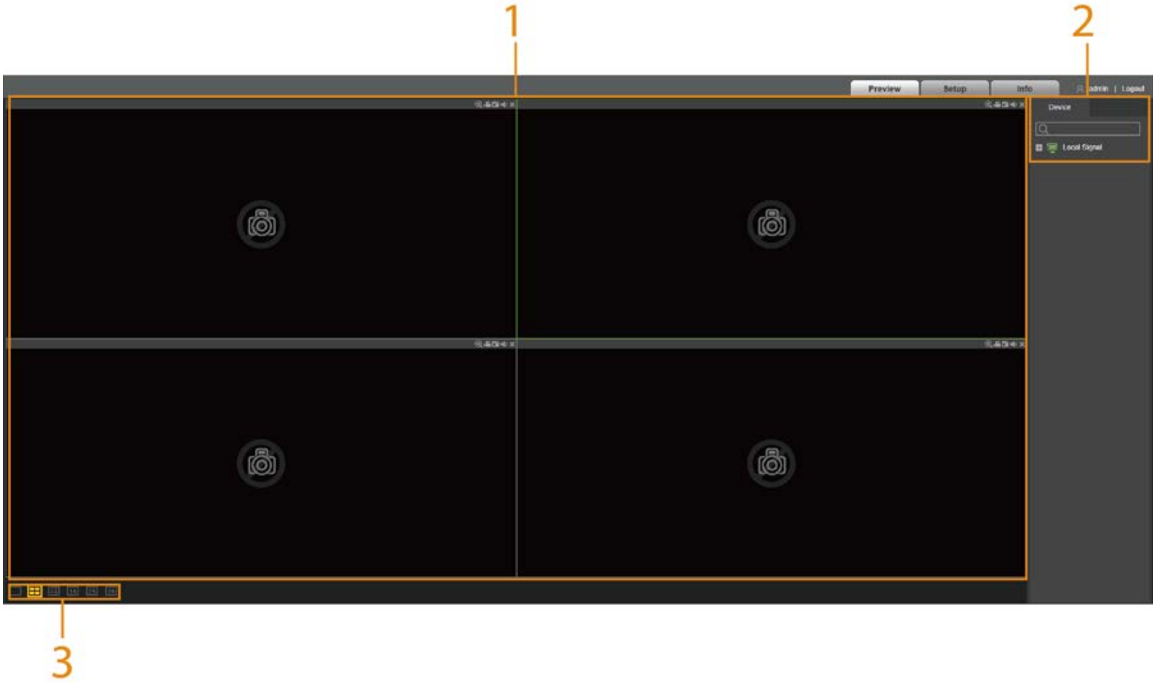


Table 3-1 Function description of preview page

No.	Name	Description
1	Window	Preview video in the window. For details, see "3.3.1 Window Function".
2	Device tree	Select local signals that you want to preview.
3	Window split	You can select single split, 4-split, 9-split, 16-split, 25-split and 36-split.

3.3.1 Window Function

There are functions at the upper-right corner of the window.

Figure 3-5 Window function

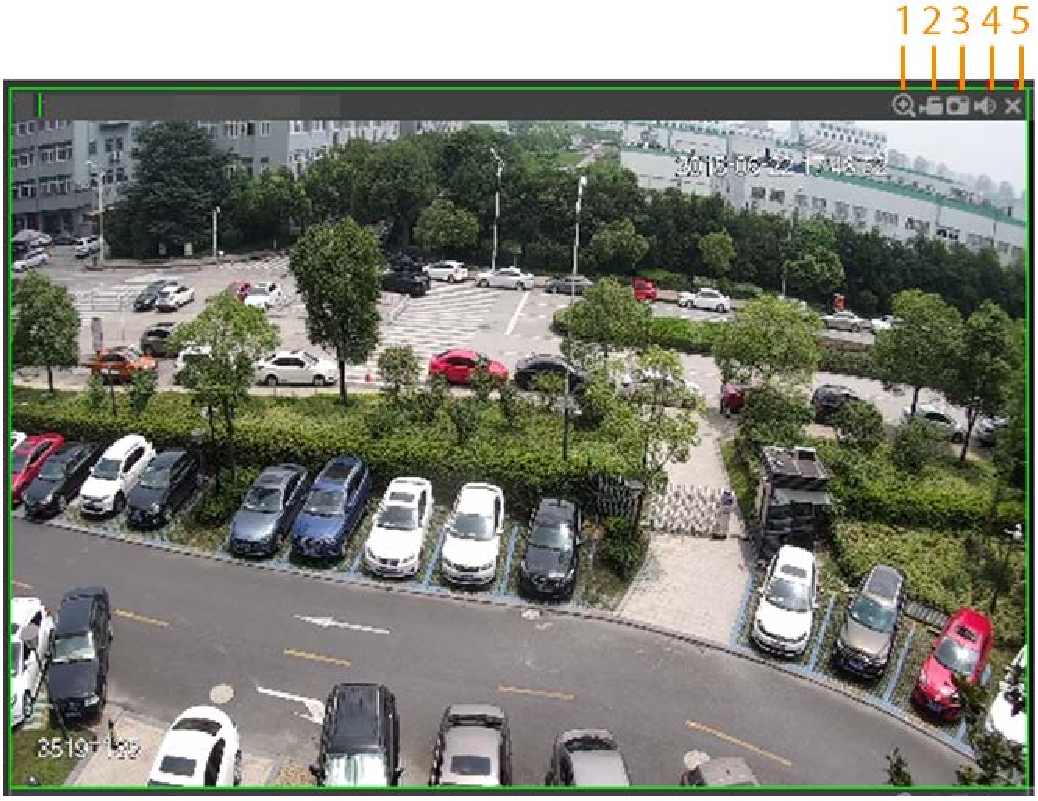


Table 3-2 Function description

No.	Name	Description
1	Local zoom	● Mouse operation ◇ When the video is in the original status, click the icon, press and hold on the left mouse button to select any area. The selected area will be zoomed in. ◇ When the video is zoomed into, press and hold on the left mouse button to drag the video image. ◇ Press the right mouse button to restore to the original status. ● Wheel button operation Click the icon to zoom in and zoom out of the video image with the wheel button.
2	Local record	Click the icon to record the video. The recorded video file is saved in the recorded video path as configured in "3.4.1.7 Configuring Storage Path".
3	Snapshot	Click the icon to take a snapshot. The image is saved in the snapshot path as configured in "3.4.1.7 Configuring Storage Path".
4	Sound control	Click the icon to enable sound of the video. Click again to mute.
5	Close	Close this window.

3.3.2 Signal Source Configuration

After adding a signal source, you can view local signal source information, and configure signal source preview.

3.3.2.1 Device Tree

You can view all local signals on the device tree. For details, see "3.4.4 Local Signal".

3.3.2.2 Image Preview

You can add signals to the preview window, so you can preview the video in the preview window.

Procedure

Step 1 Select a preview window.

Step 2 Select a local signal source from the device tree, and click the signal source to preview images in the corresponding window.

3.4 Setup

You can configure system information, network information abnormal events and local signal.

3.4.1 System Configuration

You can complete general settings, user management, backup configuration, auto maintenance, system update and storage path configuration.

3.4.1.1 Configuring General Information

You can configure basic information of the Device, such as device information and system date.

3.4.1.1.1 General Information Configuration

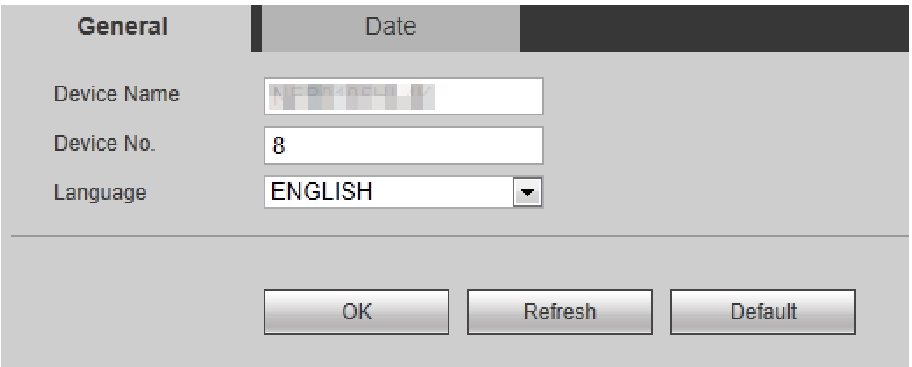
You can configure the Device name, number and more.

Procedure

Step 1 Select **Setup** > **System Config** > **General** > **General**.

Step 2 Configure the parameters.

Figure 3-6 General



Device Name [redacted]

Device No. 8

Language ENGLISH

Table 3-3 General information parameters

Parameter	Description
Device Name	Set the device name and number to differentiate it from other devices.
Device No.	
Language	System language is determined by program package.

Step 3 Click **OK**.

3.4.1.1.2 Date Configuration

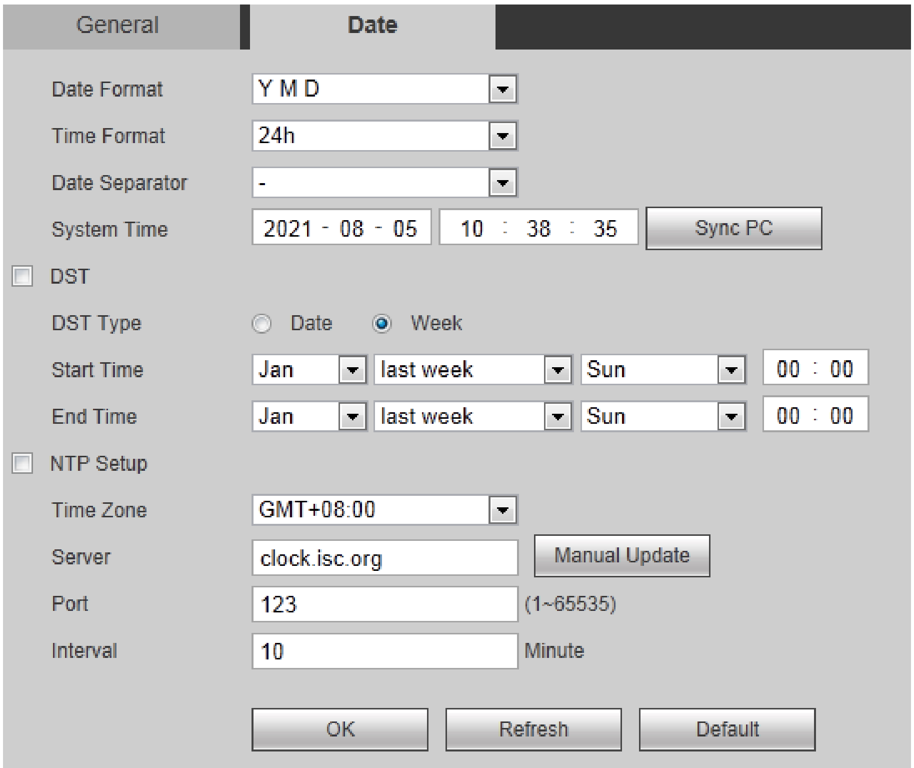
You can configure the system date, and choose to enable NTP (Network Time Protocol) or not. After enabling NTP function, the Device can automatically synchronize time with the NTP server.

Procedure

Step 1 Select **Setup** > **System Config** > **General** > **Date**.

Step 2 Configure parameters.

Figure 3-7 Date configuration



Date Format: Y M D

Time Format: 24h

Date Separator: -

System Time: 2021 - 08 - 05 10 : 38 : 35

□ DST

DST Type: ○ Date ● Week

Start Time: Jan, last week, Sun, 00 : 00

End Time: Jan, last week, Sun, 00 : 00

□ NTP Setup

Time Zone: GMT+08:00

Server: clock.isc.org

Port: 123 (1~65535)

Interval: 10 Minute

Table 3-4 Date parameters

Parameters	Description
Date Format	Select date display format, time format and date separator you want to display.
Time Format	
Date Separator	
System Time	● Configure system time manually. ● Click **Sync PC** to synchronize the system time with the current computer time.
DST	Select the checkbox to enable DST.

Parameters	**Description**
DST Type	Select DST type from **Date** or **Week**.
Start Time/End Time	● When **DST Type** is **Date**, enter year, month, day, start time and end time. ● When **DST Type** is **Week**, select month, week, day, start time and end time from the drop-down list.
NTP Setup	Select the checkbox to enable NTP sync function, and the device time will be synchronized with the server time.
Time Zone	Select the time zone where the NTP server is located.
Server	Enter server address or domain name.
Port	Enter the port number of NTP server.
Interval	Set the interval to update NTP server.

Step 3 Click **OK**.

3.4.1.2 Managing User Information

User management uses two-level management mode: user and user group. You can manage their basic information if you have user management authority.

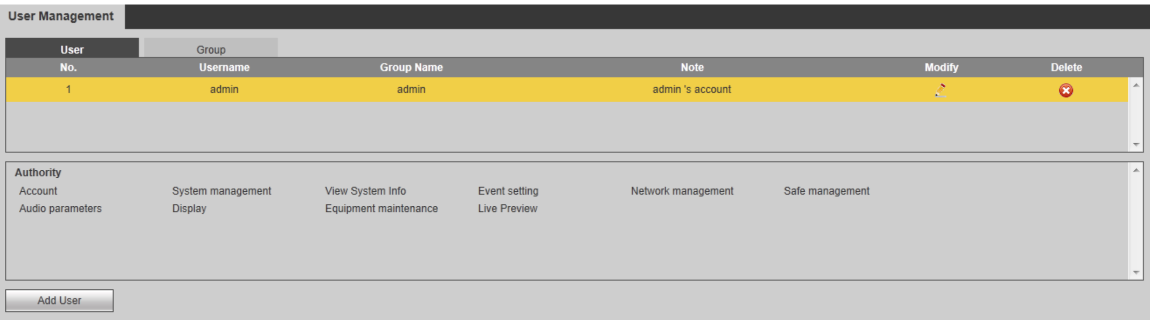
- User name and group name can be up to 6 characters, and can only consist of letters, number, and underlines.
- The password must consist of 8–32 non-blank characters and contain at least two types of the following characters: Uppercase, lowercase, numbers, and special characters (excluding ' " ; : &). The user with user management authority can change his/her own password, and also modify the password of other users.
- According to factory defaults, you can add up to 64 users and 20 user groups.
- Group name and user name must be unique. One user can only belong to one group.
- Current user cannot modify his/her own authority.
- During initialization, there is 1 default user–admin. Admin is defined as a high-authority user when leaving factory.

3.4.1.2.1 User

You can manage user information, add, modify and delete users, and modify user password.

Select **Setup** > **System Config** > **User Management** > **User**.

Figure 3-8 User



User Management

User | Group

No.	Username	Group Name	Note	Modify	Delete
1	admin	admin	admin 's account	✎	⊗

Authority

Account System management View System Info Event setting Network management Safe management
Audio parameters Display Equipment maintenance Live Preview

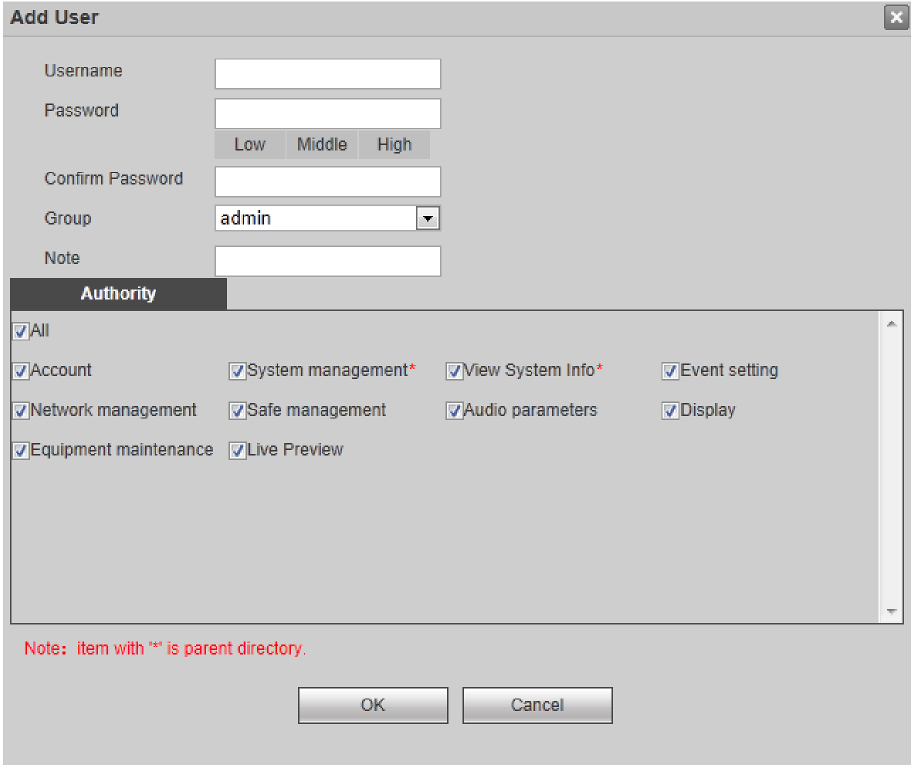
Add User

Adding Users

Add one user to the group, and configure user authority control. Admin cannot be deleted because it has the highest authority.

1. Click **Add User**.
2. Enter **Username**, **Password** and **Confirm Password**. Select **Group** and fill in **Note**.

Figure 3-9 Add User



Add User

Username

Password

Low Middle High

Confirm Password

Group admin

Note

Authority

☑All

☑Account ☑System management* ☑View System Info* ☑Event setting

☑Network management ☑Safe management ☑Audio parameters ☑Display

☑Equipment maintenance ☑Live Preview

Note: item with "*" is parent directory.

- When selecting a group for a user, authority of the users can only be a subset of the group, and should be no higher than the group authority.
- To conveniently manage the users, we suggest that general user authorities should be lower than high-level user authorities.

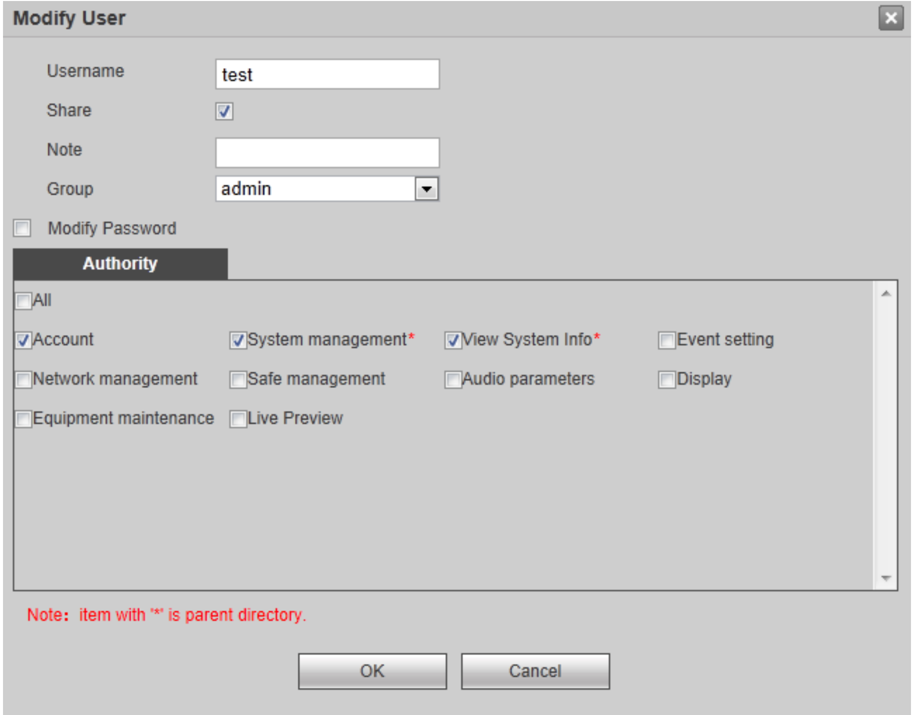
3. In **Authority** list, select operating authorities for the user.
   - Select the check box to enable the authority.
   - Select **All** to select all authorities.
4. Click **OK**.

Modifying Users

1. Click ✎ corresponding to the user you want to modify.
2. Modify user information.

Default user can only modify password, rather than other information.

Figure 3-10 Modify User



Modify User

Username: test

Share: ☑

Note:

Group: admin

□ Modify Password

Authority

□ All

☑ Account	☑ System management*	☑ View System Info*	□ Event setting
□ Network management	□ Safe management	□ Audio parameters	□ Display
□ Equipment maintenance	□ Live Preview		

Note: item with '*' is parent directory.

3. Click **OK**.

Modifying Password

1. On the **Modify User** interface, select **Modify Password**.
2. Enter old password, new password and then confirm.
3. Click **OK**.

Delete User

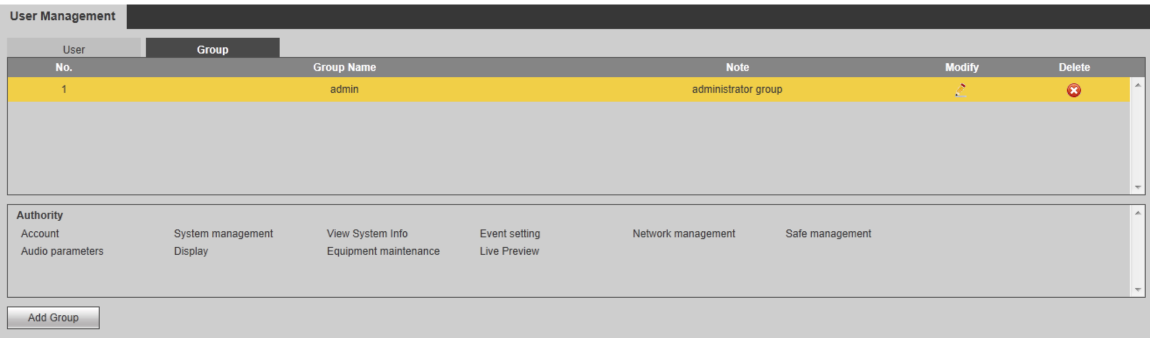
Click ⊗ corresponding to the user you want to delete.

3.4.1.2.2 Group

Different users might have different authorities to access the Device. You can divide the users with the same authority into one group.

Select **Setup** > **System Config** > **User Management** > **Group**, and then you can manage group information, add and delete groups, and modify group password. For details, see "3.4.1.2.1 User".

Figure 3-11 Group



No.	Group Name	Note	Modify	Delete
1	admin	administrator group	✎	⊗

Authority

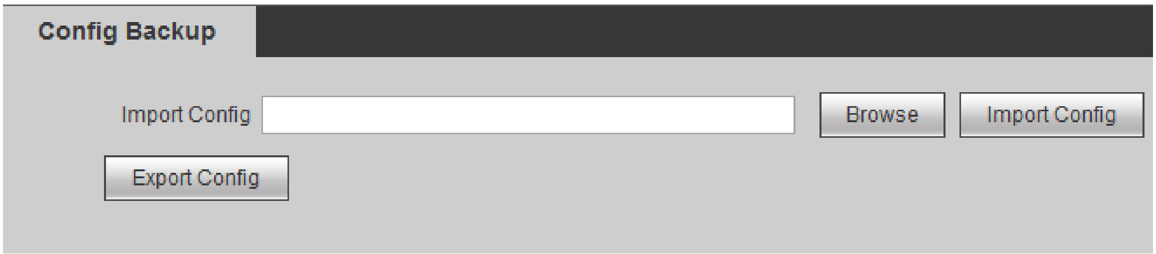
Account	System management	View System Info	Event setting	Network management	Safe management
Audio parameters	Display	Equipment maintenance	Live Preview		

3.4.1.3 Configuring Backup

The configuration file of the Device can be exported to flash drive for backup. When there are issues with Device, you can import configuration file to restore configuration quickly.

Select **Setup** > **System Config** > **Backup**.

Figure 3-12 Configure backup



- Click **Browse**, select configuration file (.backup), and then click **Import Config** to import the configuration file.
- Click **Export Config**, and then select storage path to export configuration file for backup.

3.4.1.4 Configuring Auto Maintenance

You can restart the Device, enable SSH, auto restart the Device and restore to factory default configurations.

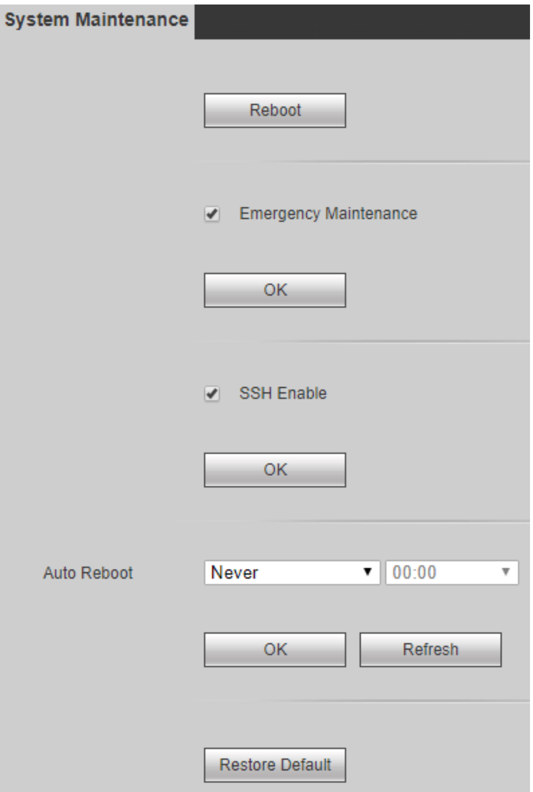
Select **Setup** > **System Config** > **Auto Maintenance**.

- When you select manual reboot, click **Reboot**, and the system will reboot at once.
- When emergencies occur, selelct **Emergency Maintenance**to enable emergency maintenance.
- SSH is used to open background debugging port. Select **SSH Enable**, and click **OK** to enable remote debugging function.
- When you select auto reboot, configure the time you want the Device to restart automatically, and then click **OK**.

⚠

Click **Restore Default**. The system will be restored to the factory default configurations, and your current configurations will be lost.

Figure 3-13 System maintenance



☑ Emergency Maintenance

☑ SSH Enable

Auto Reboot: Never, 00:00

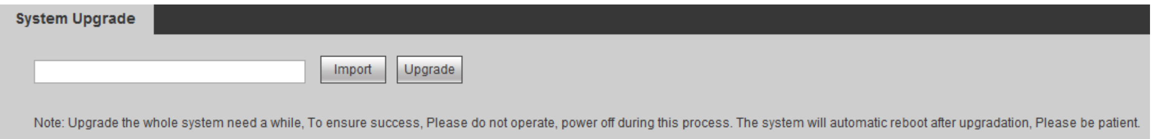
3.4.1.5 Upgrading System

Store upgrade file in the computer that is associated with the Device. You can import upgrade file to upgrade the system.

Procedure

Step 1 Select **Setup** > **System Config** > **System Upgrade**.

Figure 3-14 System upgrade



Note: Upgrade the whole system need a while, To ensure success, Please do not operate, power off during this process. The system will automatic reboot after upgradation, Please be patient.

Step 2 Click **Import**, and select the upgrade file that you want to import.

Step 3 Click **Upgrade**. There is a progress bar during upgrade.

After upgrade file is uploaded according to system prompt, the Device will reboot. Keep the power supply on until the system is automatically restarted.

3.4.1.6 Configuring Safe Management

You can configure firewall, system service, HTTPS, security exception linkage, and bind the static ARP.

3.4.1.6.1 Configuring Firewall

Set a firewall for the Device to prevent network attacks after the Device is connected to the network.

Procedure

Step 1 Select **Setup** > **System Config** > **Safe Management** > **Firewall**.

Step 2 Select the type of network attack that the firewall resists.

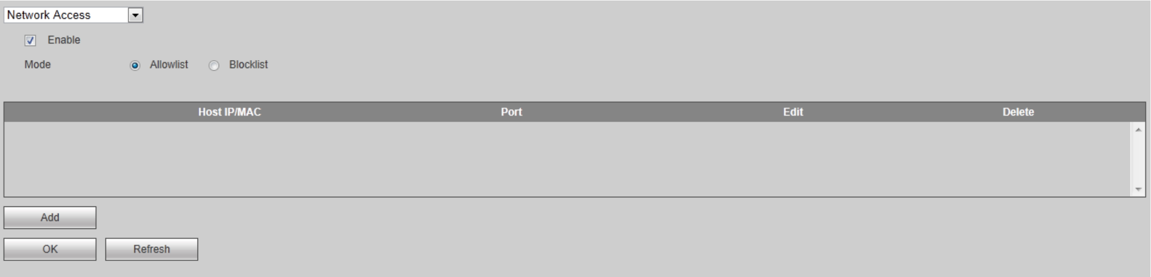
You can select **Network Access**, **Forbid Ping**, or **Semi join**. This section uses **Network Access** as an example.

Step 3 Select the **Enable** checkbox.

Step 4 Select a mode from the drop-down list.

- **Allowlist**: Only the listed IP /MAC addresses are allowed to visit corresponding ports of the Device.
- **Blocklist**: The listed IP /MAC addresses are prohibited from visiting the corresponding ports of the Device.

Figure 3-15 Firewall



Network Access

☑ Enable

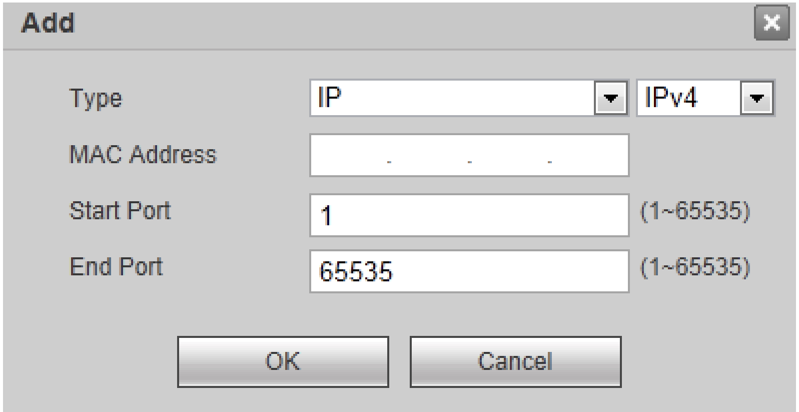
Mode ● Allowlist ○ Blocklist

Host IP/MAC	Port	Edit	Delete

Step 5 Add IP/MAC into your Allowlist/Blocklist.

1) Select **Allowlist** or **Blocklist**.
2) Click **Add IP/MAC**.
3) Configure parameters.

Figure 3-16 Add IP/MAC



Add

Type: IP, IPv4

MAC Address: - - -

Start Port: 1 (1~65535)

End Port: 65535 (1~65535)

4) Click **OK**.

Step 6 Click **OK**.

3.4.1.6.2 Configuring System Service

Configure system service to ensure system security.

Procedure

Step 1 Select **Setup** > **System Config** > **Safe Management** > **System Service**.

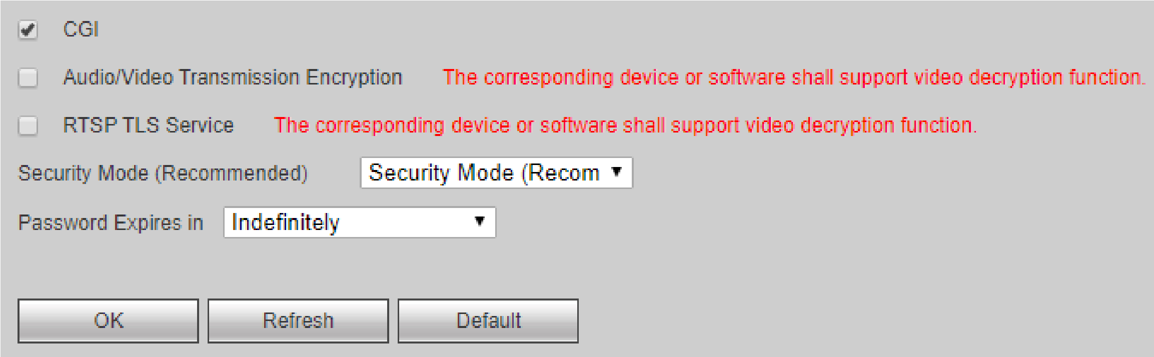
Step 2 Select **CGI**.

The Device can access the web system through this protocol. The function is enabled by default.

Step 3 Select mode.

Security mode is recommended. If you select compatibility mode, there might be security risks.

Figure 3-17 System service



☑ CGI

□ Audio/Video Transmission Encryption The corresponding device or software shall support video decryption function.

□ RTSP TLS Service The corresponding device or software shall support video decryption function.

Security Mode (Recommended) Security Mode (Recom ▼

Password Expires in Indefinitely ▼

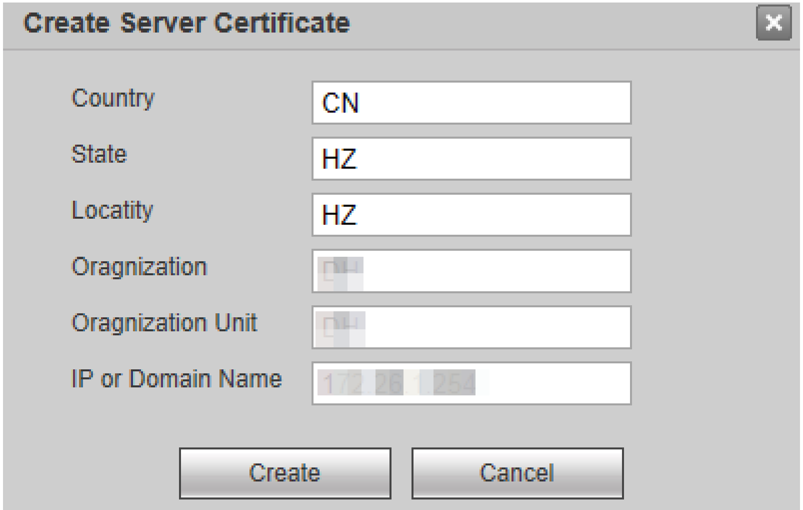
3.4.1.6.3 Configuring HTTPS

Through creating server certificate or downloading root certificate on the HTTPS page, the computer can login by HTTPS, to ensure the security of communication data, and guard the user information and device security with stable technology.

Background Information

- For first time use of this function or after changing IP address of the Device, you need to click **Create Server Certificate** to create a server certificate.

Figure 3-18 Create server certificate



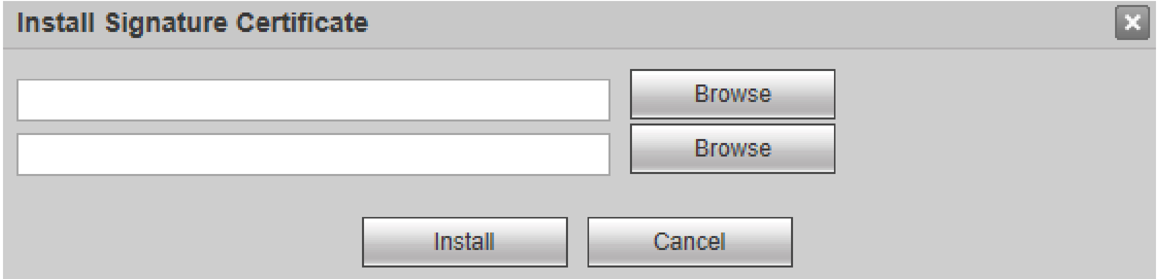
Create Server Certificate

Country	CN
State	HZ
Locatity	HZ
Oragnization	[redacted]
Oragnization Unit	[redacted]
IP or Domain Name	[redacted]

- For first time use of HTTPS after changing a computer, you need to click **Download Root Certificate** to download root certificate.

- If you have a certificate on your computer, click **Install Signature Certificate** and then upload your certificates.

Figure 3-19 Upload certificates



- HTTPS enable status will take effect after reboot.

Procedure

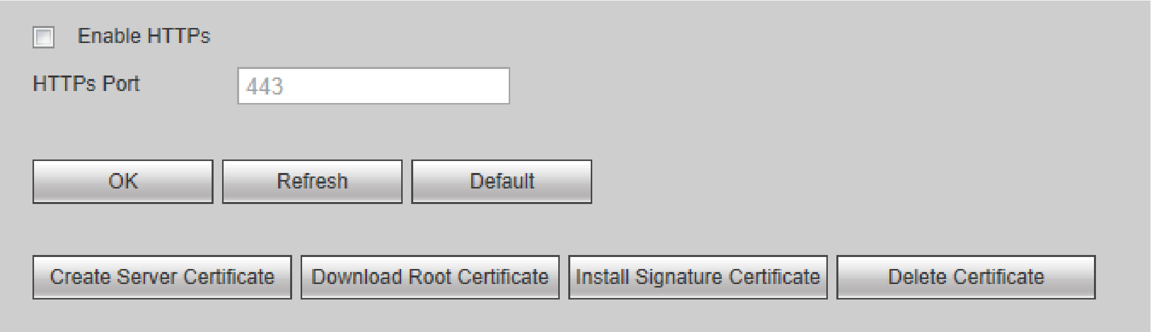
Step 1 Select **Setup** > **System Config** > **Safe Management** > **HTTPS**.

Step 2 Enable **HTTPs**

Step 3 Enter the HTTPs port.

Step 4 Click **OK**.

Figure 3-20 Configure HTTPS



□ Enable HTTPs

HTTPs Port 443

OK
Refresh
Default
Create Server Certificate
Download Root Certificate
Install Signature Certificate
Delete Certificate

- If HTTPS is enabled, you cannot access the Device through HTTP. The system will switch to HTTPS if you access the Device through HTTP.
- The deletion of created and installed certificates cannot be restored. Please be careful.

3.4.1.6.4 Configuring Security Exception Linkage

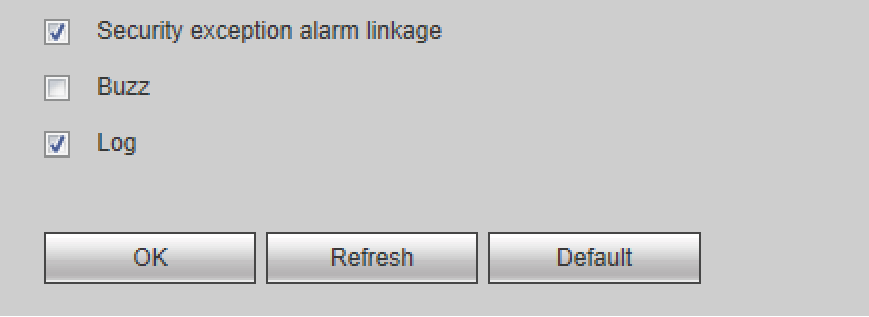
Set alarm linkage actions when an abnormal event occurs.

Procedure

Step 1 Select **Setup** > **System Config** > **Safe Management** > **Security Exception Linkage**.

Step 2 Configure the parameters.

Figure 3-21 Security exception linkage



☑ Security exception alarm linkage

□ Buzz

☑ Log

Table 3-5 Security exception linkage parameters

Parameter	Description
Security exception alarm linkage	Select the checkbox to enable this function.
Buzz	The system activates a buzzer alarm when an alarm event occurs.
Log	Select the **Log** checkbox and the alarm information will be recorded on the computer.

Step 3 Click **OK**.

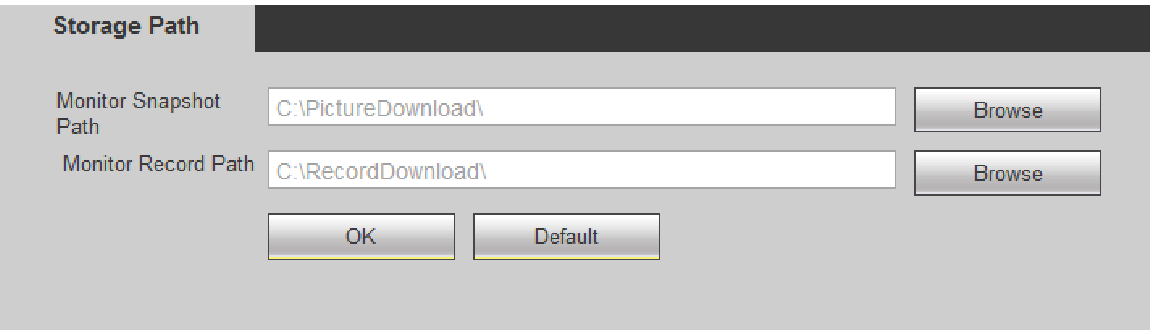
3.4.1.7 Configuring Storage Path

Select the storage path for snapshots and records.

Procedure

Step 1 Select **Setup** > **System Config** > **Storage Path**.

Figure 3-22 Storage path



Storage Path

Monitor Snapshot Path: C:\PictureDownload\

Monitor Record Path: C:\RecordDownload\

Step 2 Click **Browse** to select the storage path for snapshots and records.

Step 3 Click **OK**.

Click **Default** to restore to default path. The default storage path of images and records is C:\PictureDownload and C:\RecordDownload respectively.

3.4.2 Network

3.4.2.1 Configuring TCP/IP

You can configure the device IP address, DNS server information and other information according to network plan.

Prerequisites

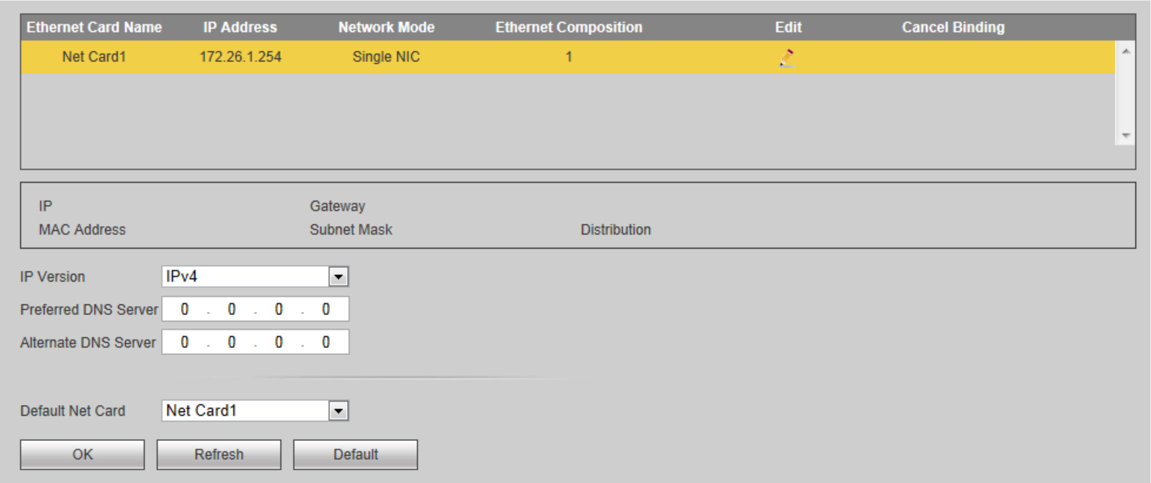
- Before configuring network parameters, make sure that the Device is connected to the network properly.
- If there is no routing device in the network, distribute IP address on the same network segment.
- If there is routing device in the network, you only need to configure gateway and subnet mask.

Procedure

Step 1 Select **Setup** > **Network** > **TCP/IP**.

Step 2 Configure TCP/IP parameters.

Figure 3-23 TCP/IP



Ethernet Card Name	IP Address	Network Mode	Ethernet Composition	Edit	Cancel Binding
Net Card1	172.26.1.254	Single NIC	1	✎	

IP

Gateway

MAC Address

Subnet Mask

Distribution

IP Version: IPv4

Preferred DNS Server: 0 . 0 . 0 . 0

Alternate DNS Server: 0 . 0 . 0 . 0

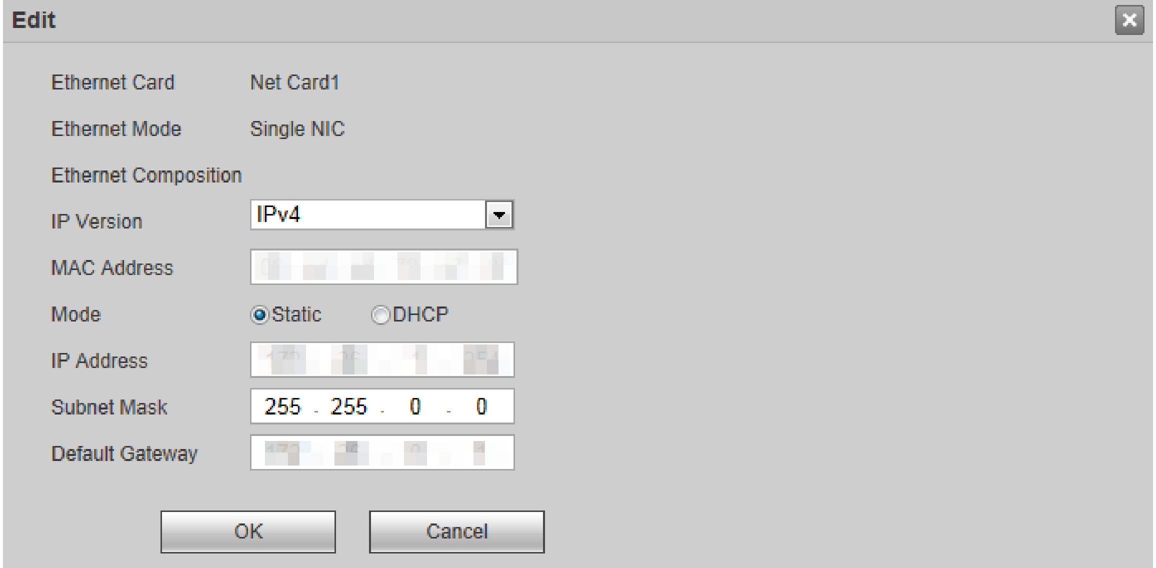
Default Net Card: Net Card1

Table 3-6 TCP/IP parameters description

Parameters	**Description**
IP Version	Select IP version. It is IPv4 by default.
Preferred DNS Server	Enter the configured IP address of DNS server.
Alternate DNS Server	Enter the configured IP address of alternate DNS server.
Default Net Card	Select the default network card.

Step 3 Click ✎ to edit Ethernet card information.

Figure 3-24 Edit



Edit

Ethernet Card: Net Card1

Ethernet Mode: Single NIC

Ethernet Composition

IP Version: IPv4

MAC Address: [redacted]

Mode: ● Static ○ DHCP

IP Address: [redacted]

Subnet Mask: 255 . 255 . 0 . 0

Default Gateway: [redacted]

Table 3-7 Ethernet card parameters description

Parameters	Description
Ethernet Mode	The default mode is Single NIC.
IP Version	It is IPv4 by default.
MAC Address	Displays the MAC address of the Device.
Mode	● Static Manually enter the IP address, subnet mask and gateway. ● DHCP Select the **DHCP** box, the system will automatically get the device IP address. When the **DHCP** function is enabled, the IP address, gateway, and subnet mask cannot be set manually. ◇ If DHCP is effective, the device information will be displayed in the **IP Address** box and **Default Gateway** box. If DHCP is not effective, they all display 0. ◇ To view manually set IP when DHCP is not effective, you should disable DHCP first, and then the Device will display IP information that is not obtained through DHCP. If DHCP is effective, disable DHCP, and static IP information will restore default settings. You need to configure IP again.
IP Address	Enter IP address, and then configure its **Subnet Mask** and **Default Gateway**. IP address and default gateway must be on the same network segment.
Subnet Mask	
Default Gateway	

Step 4 Click **OK** to complete the editing.

Step 5 Click **OK** to complete the configuration.

3.4.2.2 Configuring Port

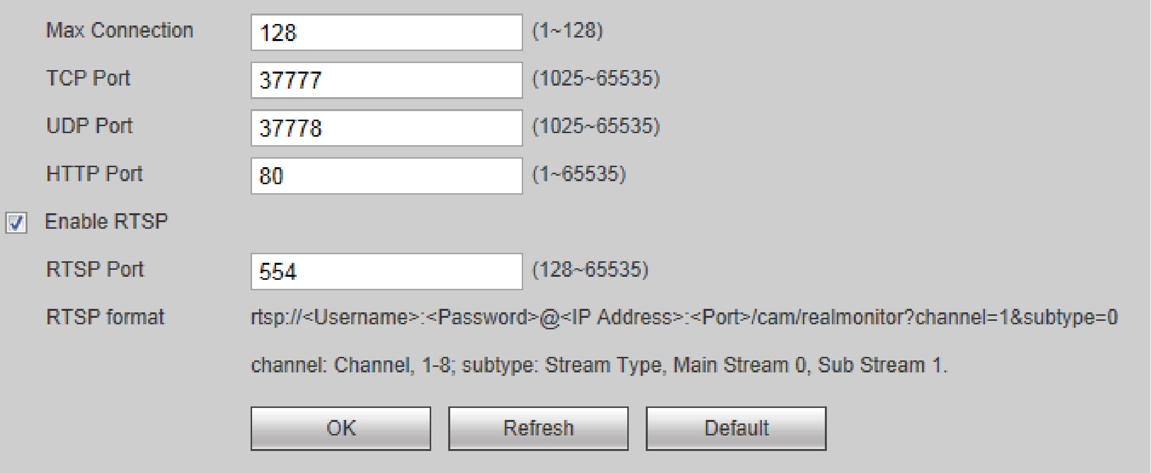
Set maximum connection and port to access the Device through client (including web client and computer client).

Procedure

Step 1 Select **Setup** > **Network** > **Port**.

Step 2 Configure maximum connection and port.

Figure 3-25 Port



Max Connection	128	(1~128)
TCP Port	37777	(1025~65535)
UDP Port	37778	(1025~65535)
HTTP Port	80	(1~65535)
☑ Enable RTSP		
RTSP Port	554	(128~65535)
RTSP format	rtsp://<Username>:<Password>@<IP Address>:<Port>/cam/realmonitor?channel=1&subtype=0 channel: Channel, 1-8; subtype: Stream Type, Main Stream 0, Sub Stream 1.	

Table 3-8 Port parameters description

Parameter	Description
Max Connection	The maximum clients allowed accessing the Device at the same time, such as web, platform, and mobile phone. It is 128 by default.
TCP Port	TCP service port. It is 37777 by default.
UDP Port	User Datagram Protocol port. It is 37778 by default.
HTTP Port	Hyper Text Transfer Protocol port. It is 80 by default. You can enter the value according to your actual situation, and in this case, add the modified value after the address when logging in to the Device on the browser.

Parameter	Description
RTSP Port	Select **Enable RTSP**. ● Real Time Streaming Protocol port. Keep the default value 554 if it is displayed. If you play live view through Apple's QuickTime or VLC, the following format is available. ● When the URL format requiring RTSP, you need to specify channel number and bit stream type in the URL, and also username and password if needed. **URL format instruction:rtsp://<Username>:<Password>@<IP Address>:<Port>/cam/realmonitor?channel=1&subtype=0** ● Username. For example, admin. ● Password. For example, admin. ● IP Address: Device IP. ● Port: It is 554 by default. Keep it as default. ● Channel: Channel number, starting from 1. For example, if it is channel 2, then enter channel=2. ● Subtype: Stream type. The main stream is 0 (subtype=0); the sub stream is 1 (subtype=1). For example, if you acquire the sub stream of channel 2 from a certain device, then the URL can be: rtsp://admin:admin@192.168.4.84:554/cam/realmonitor?channel=2&subtype=1 If certification is not required, you do not need to specify the username and password. Use the following format: rtsp://ip:port/cam/realmonitor?channel=1&subtype=0

Step 3 Click **OK**.

Except **Max Connection**, modifications of other parameters will take effect after restart.

3.4.2.3 Synchronizing IP

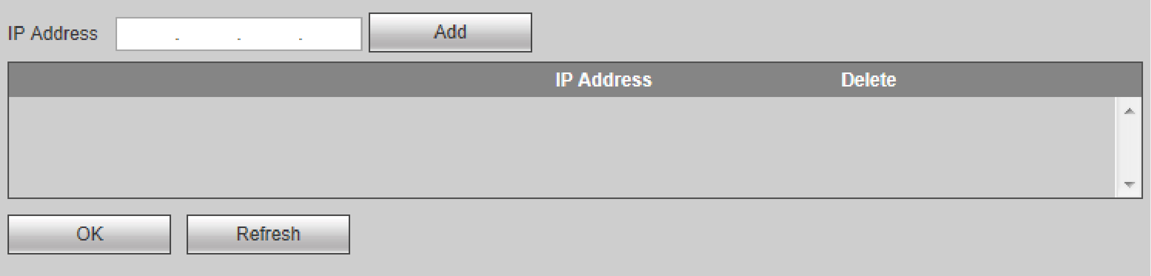
You can add computer IP to synchronize system time, and ensure that the system time is correct.

Procedure

Step 1 Select **Setup** > **NetworkSync IP**.

Step 2 Enter IP address, and then click **Add**.

Figure 3-26 Sync IP



Step 3 Click **OK**.

3.4.3 Settings Abnormal Event

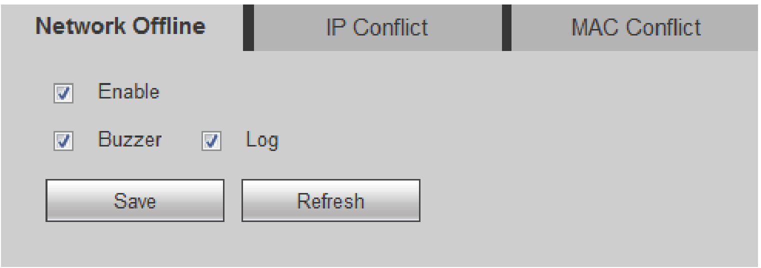
Configure alarm linkage actions when an abnormal event occurs.

Procedure

Step 1 Select **Setup** > **Event Management** > **Abnormal**.

Step 2 Configure the parameters.

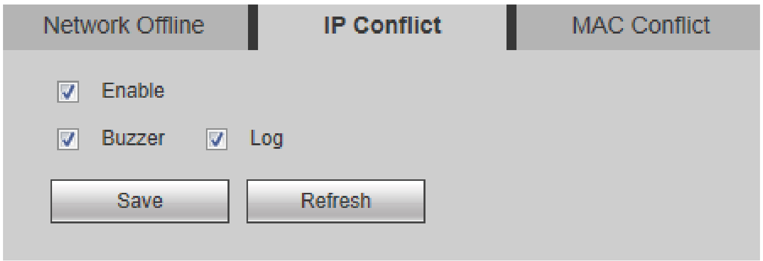
Figure 3-27 Network offline



☑ Enable

☑ Buzzer ☑ Log

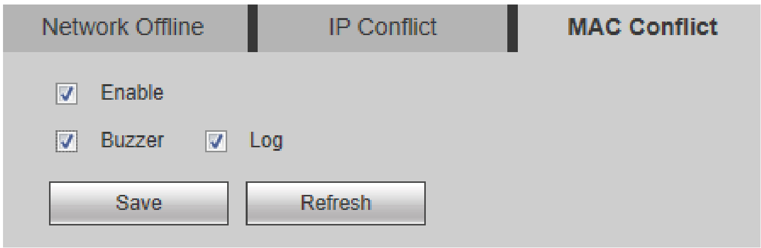
Figure 3-28 IP conflict



☑ Enable

☑ Buzzer ☑ Log

Figure 3-29 MAC conflict



☑ Enable

☑ Buzzer ☑ Log

Table 3-9 Abnormal event setting parameter description

Parameter	Description
Enable	Select **Enable** to enable this abnormal alarm function.
Buzzer	The system activates a buzzer alarm when there is corresponding alarm event.
Log	Select **Log** to enable the Device to record a local alarm log when an alarm event occurs.

Step 3 Click **Save**.

3.4.4 Local Signal

You can configure local signal, including input title, input channel setup and encode setup.

3.4.4.1 Configuring Input Title

You can configure input title and control ID of each channel on the board card. Control ID can correspond to the binding source (such as keyboard), so the binding source can be displayed on the TV wall.

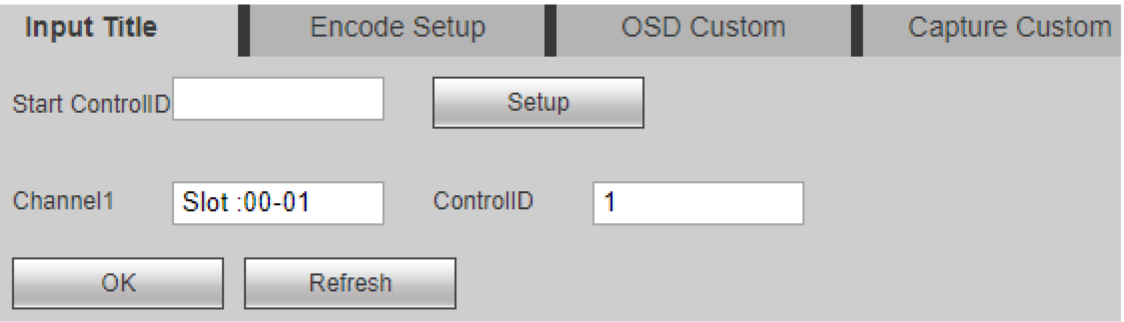
Procedure

Step 1 Select **Setup** > **Signal Management** > **Local Signal** > **Input Title**.

Step 2 Configure **Start ControlID** and **Channel1** name and **ControlID**

Enter **Start ControlID** and click **Setup**. Then, control ID of each channel will be numbered starting from **Start ControlID**.

Figure 3-30 Input title



Input Title | Encode Setup | OSD Custom | Capture Custom

Start ControlID: (empty) — Setup

Channel1: Slot :00-01 — ControlID: 1

OK — Refresh

Step 3 Click **OK**.

3.4.4.2 Configuring Encode Parameters

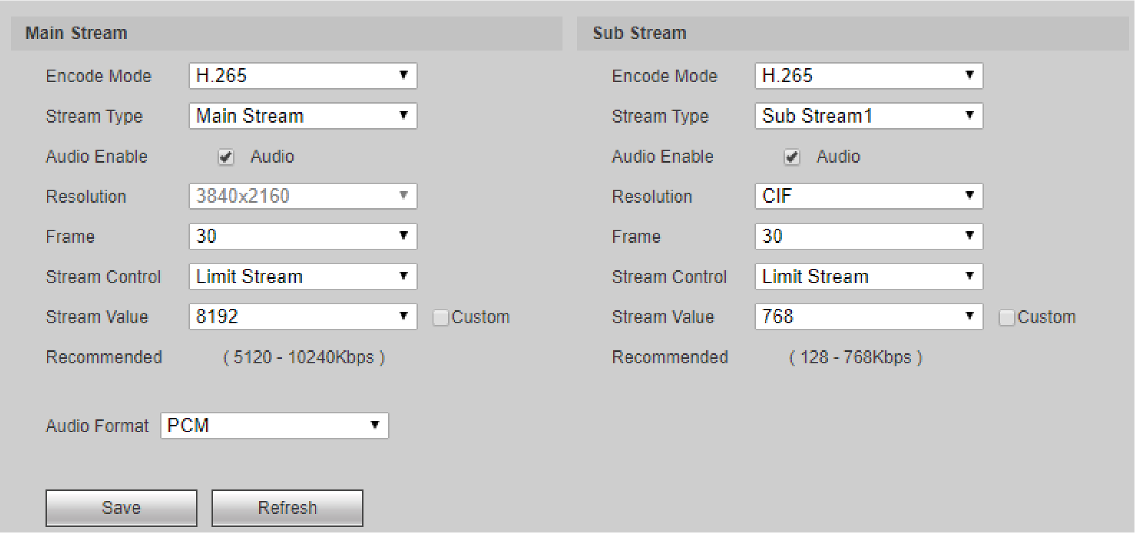
You can configure encode parameters of local audio and video signals, including encode mode, stream type and resolution and so on.

Procedure

Step 1 Select **Setup** > **Signal Management** > **Local Signal** > **Encode Setup**.

Step 2 Configure the parameters.

Figure 3-31 Encode setup



	Main Stream	Sub Stream
Encode Mode	H.265	H.265
Stream Type	Main Stream	Sub Stream1
Audio Enable	☑ Audio	☑ Audio
Resolution	3840x2160	CIF
Frame	30	30
Stream Control	Limit Stream	Limit Stream
Stream Value	8192 □ Custom	768 □ Custom
Recommended	(5120 - 10240Kbps)	(128 - 768Kbps)

Audio Format: PCM

Save — Refresh

Table 3-10 Parameter description

Parameter	Description
Encode Mode	You can select H.264 or H.265.

Parameter	Description
Stream Type	Main stream includes general stream and dynamic stream. Sub stream supports sub stream 1 and sub stream 2. Select different encoding streams for recording events.
Audio Enable	Determine to encode audio or not during recording.
Resolution	Support adaptive main stream resolution.
Frame	PAL: 1 fps – 25 fps, 1 fps – 50 fps or 1 fps – 60 fps.
Stream Control	It includes limit stream and VBR. Picture quality can be configured under VBR mode only, and cannot be set under limit stream mode.
Stream Value	Under VBR mode, this stream value is the upper limit of stream. Under limit stream mode, this value is a fixed value. Select **Custom**, and you can manually enter stream value.
Recommended	The Device recommends the optimal stream range according to the resolution and frame rate settings.
Audio Format	It is PCM by default. 📖 Audio encoding mode here will affect audio stream.

Step 3 Click **Save**.

3.4.4.3 Configuring Custom OSD

You can custom OSD effect of the local signal to display the time and channel title on the video wall.

Background Information

📖

Only NEB0105HI-4K supports this function.

Procedure

Step 1 Select **Setup** > **Signal Management** > **Local Signal** > **OSD Custom**.

Step 2 Select a slot and a channel.

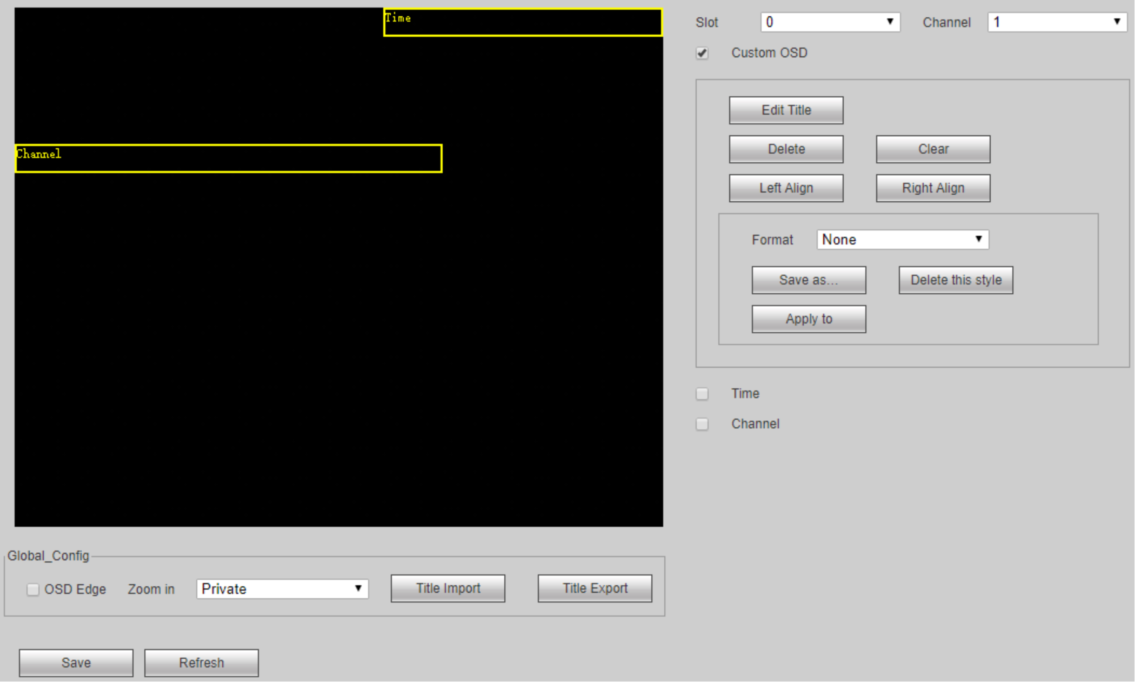
Step 3 Select **Custom OSD**, and then edit the OSD.

- Click **Edit Title**, and then enter the title content to be displayed. Up to six titles can be displayed at the same time.
- In the preview box, select and hold the title to drag it to the desired position.
- In the preview box, select the title and click **Delete** to delete the title.
- Click **Clear** to clear all titles except the time title and channel title.
- In the preview box, select a title and click **Left Align** or **Right Align** to align all titles to the left or right according to the selected title. Except for the time title and channel title.
- Click **Save as**, and then enter the **Style Name** to save the current display as a format.
- Select a format from the **Format** drop-down list to apply this format. Click **Delete this style** to delete the selected format.

Only custom formats can be deleted.

- Click **Apply to** to apply the current format to other slots.

Figure 3-32 OSD custom



Step 4 Select **Time**, and then the time title will be displayed on the vide wall. You can select and hold the time title to drag it to the desired position.

Step 5 Select **Channel**, and the channel title will be displayed on the vide wall. You can select and hold the channel title to drag it to the desired position.

Step 6 Configure the **Global Config**.

Figure 3-33 Global configuration

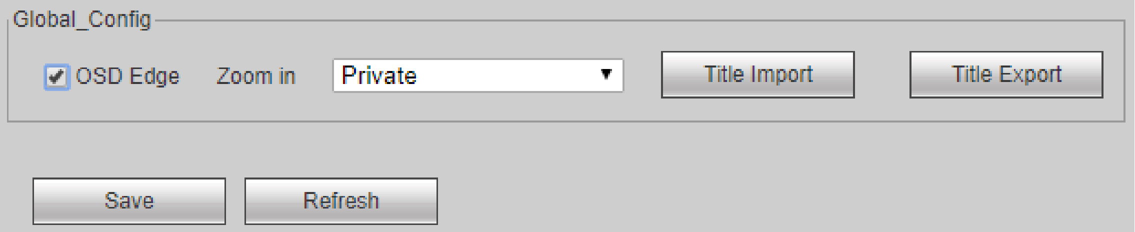


Table 3-11 Global configuration description

Parameter	Description
OSD Edge	Select **OSD Edge**, and there is a black edge around the font.
Zoom in	**Private** and **Standard** are available. It is Private by default. Standard mode zooms in more than that of private mode.
Title Import	Import a configuration table to configure OSD in batches.
Title Export	Export a configuration table, and then enter all channel titles.

Step 7 Click **Save** to save configurations.

3.4.4.4 Configuring Capture Custom

The captured image can be cut according to configured size, and displayed on the output screen according to the configured coordinate.

Procedure

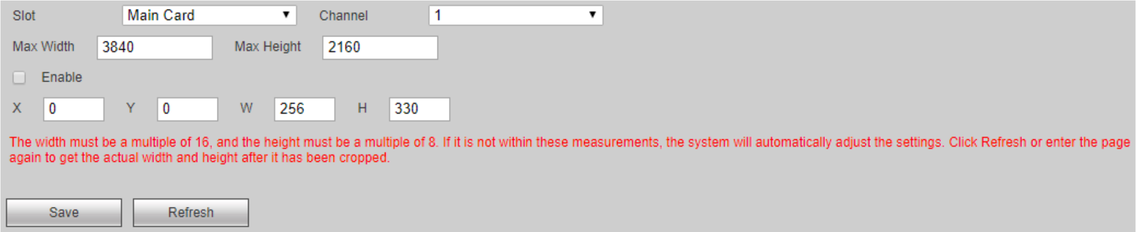
Step 1 Select **Setup** > **Signal Management** > **Local Signal** > **Capture Custom**.

Step 2 Select the slot and channel.

Step 3 Enter the maximum width and height.

For example, the resolution of the captured video is 1080p, and the cut video is 500×900. The maximum width and height are 1920 and 1080 respectively. During encoding, the system automatically stretches the 500×900 video to encode at 1080p resolution.

Figure 3-34 Capture Custom



Slot: Main Card   Channel: 1

Max Width: 3840   Max Height: 2160

□ Enable

X: 0   Y: 0   W: 256   H: 330

The width must be a multiple of 16, and the height must be a multiple of 8. If it is not within these measurements, the system will automatically adjust the settings. Click Refresh or enter the page again to get the actual width and height after it has been cropped.

Step 4 Select **Enable**.

Step 5 Configure the coordinate, width and height.

X/Y refers to the starting pixel coordinate, and W/H refers to the width and height of the image. The unit is pixel.

Step 6 Click **Save**.

3.5 Information

You can view the device information, including system status, system log, online user and version information.

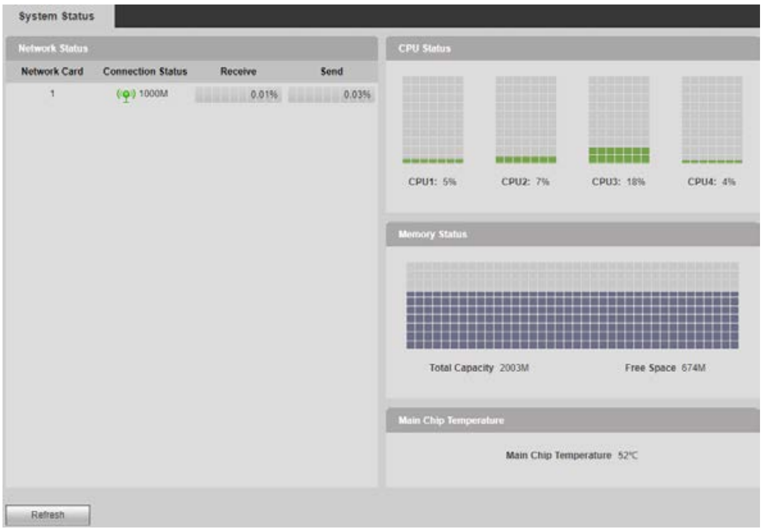
3.5.1 System Status

You can view the network status, CPU status and memory status of the Device.

Select **Info** > **Device Info** > **System Status**.

- Network status: Displays connection status, data receiving and sending of network card.
- CPU status: Displays CPU status of all inserted board cards.
- Memory status: Displays memory status.
- Main chip temperature: Displays main chip temperature.

Figure 3-35 System status



Network Card	Connection Status	Receive	Send
1	1000M	0.01%	0.03%

CPU1: 5% CPU2: 7% CPU3: 18% CPU4: 4%

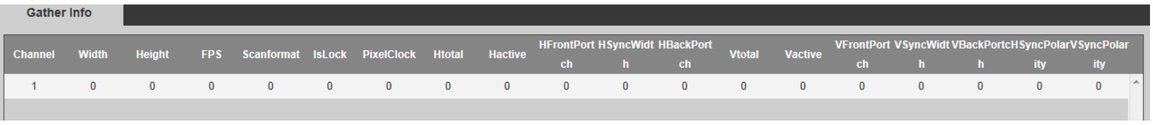
Total Capacity 2003M Free Space 674M

Main Chip Temperature 52℃

3.5.2 Gather Information

The Device collects the information from the computer graphics card to judge whether the video signal parameter is correct.

Figure 3-36 Gather information



Channel	Width	Height	FPS	Scanformat	IsLock	PixelClock	Htotal	Hactive	HFrontPortch	HSyncWidth	HBackPortch	Vtotal	Vactive	VFrontPortch	VSyncWidth	VBackPortch	HSyncPolarity	VSyncPolarity
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

3.5.3 Device Information

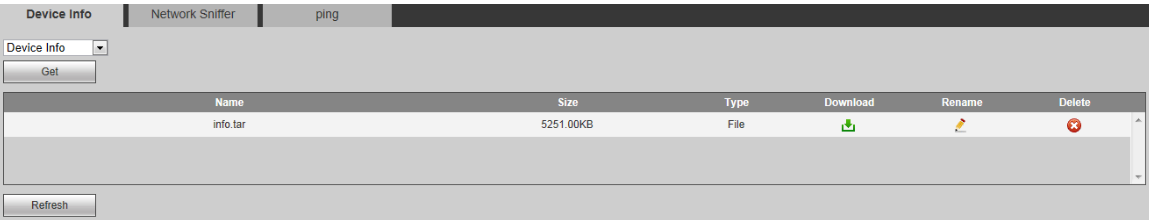
3.5.3.1 Getting Device Information

You can view information file of the Device.

Procedure

Step 1 Select **Info** > **Device Info** > **Device Info**, and then click the **Device Info** tab.

Figure 3-37 Get device information.



Name	Size	Type	Download	Rename	Delete
info.tar	5251.00KB	File	⤓	✎	⊗

Step 2 Select **Device Info**, and click **Get**.

- Click ⤓ to download information file of the Device.
- Click ✎ to rename the information file.
- Click ⊗ to delete the information file. If you delete it by mistake, you can get it again.

3.5.3.2 Network Sniffer

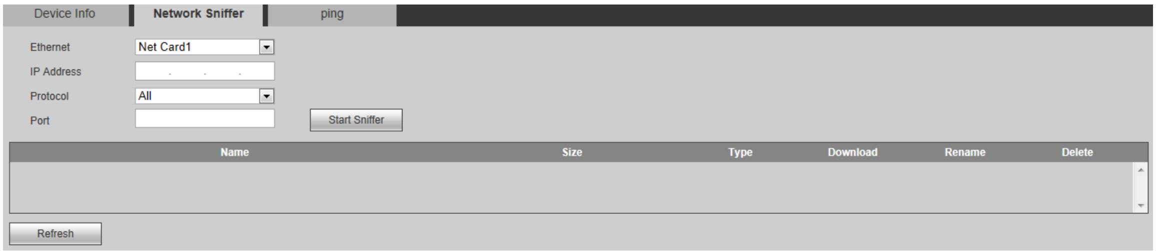
Network sniffer is to intercept, resend, edit and transfer the data received and sent through network, so you can inspect the network security. In case of network error, you can carry out sniffer operation on this page, download the sniffer file to local device, and provide it to technicians to analyze network status.

Procedure

Step 1 Select **Info** > **Device Info** > **Device Info**, and then click **Network Sniffer** tab.

Step 2 Set parameters.

Figure 3-38 Data packet



Ethernet: Net Card1
IP Address: . . .
Protocol: All
Port:

Name	Size	Type	Download	Rename	Delete

Table 3-12 Network sniffer parameter description

Parameter	Description
Ethernet	Select the net card that is bound.
IP Address	Configure network IP address.
Protocol	Select network protocol, including All, TCP and UDP.
Port	Configure network port.

Step 3 Click **Start Sniffer**.

Step 4 After a while, click **Stop Sniffer**.

The obtained data packet is displayed in the list.

Related Operations

- Click ⬇ to download this sniffer file.
- Click ✎ to rename this sniffer file.
- Click ⊗ to delete this sniffer file.

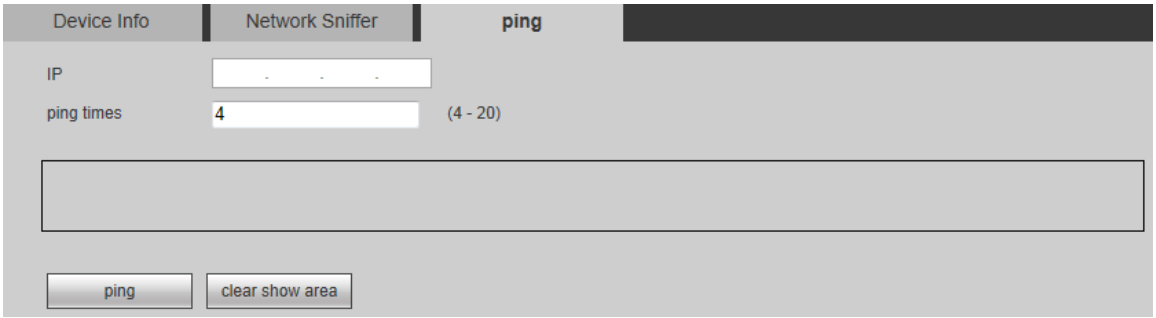
3.5.3.3 Ping

With ping command, you can check whether the Device is connected normally.

Procedure

Step 1 Select **Info** > **Device Info** > **Device Info**, and then click **ping** tab.

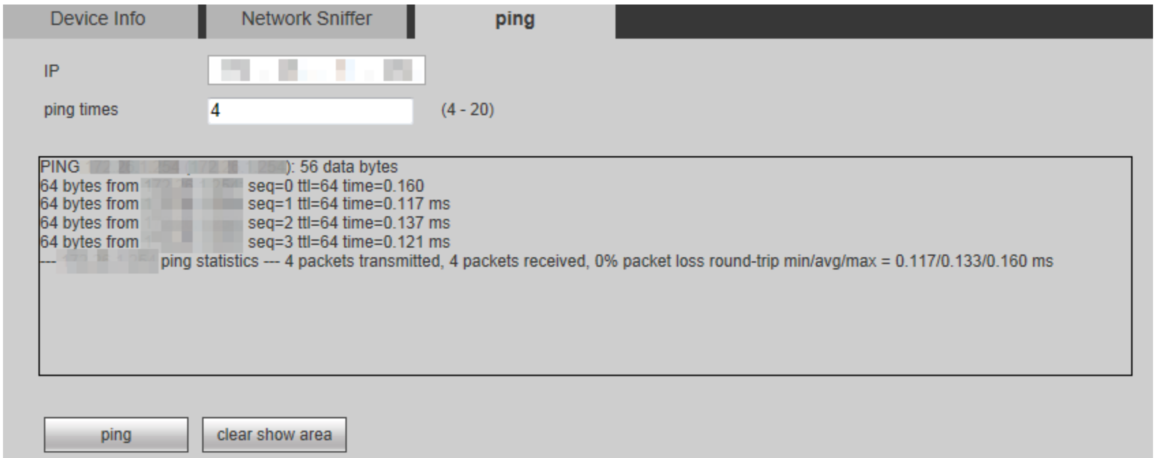
Figure 3-39 ping



Step 2 Enter the IP address and ping times, and click **ping**.

After several seconds, ping information is displayed.

Figure 3-40 Information display



```
PING [redacted]): 56 data bytes
64 bytes from [redacted] seq=0 ttl=64 time=0.160
64 bytes from [redacted] seq=1 ttl=64 time=0.117 ms
64 bytes from [redacted] seq=2 ttl=64 time=0.137 ms
64 bytes from [redacted] seq=3 ttl=64 time=0.121 ms
--- [redacted] ping statistics --- 4 packets transmitted, 4 packets received, 0% packet loss round-trip min/avg/max = 0.117/0.133/0.160 ms
```

When ping function is enabled, you can only open one web. Otherwise, ping information might not be displayed completely.

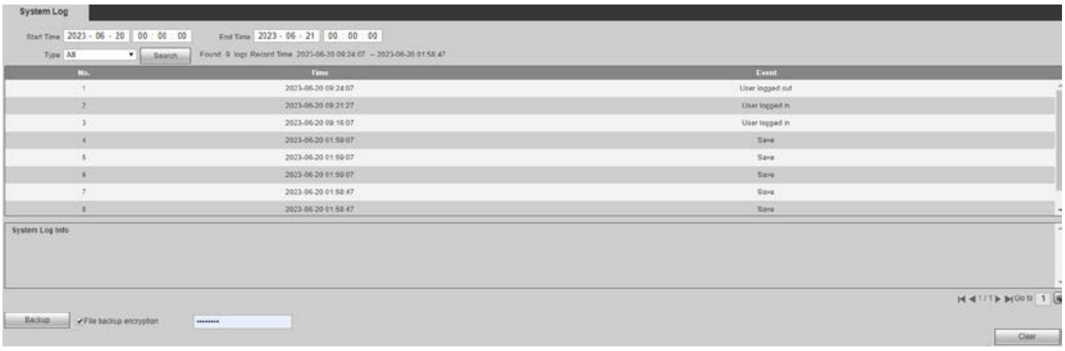
3.5.4 System Log

You can search for and view system log information about the Device according to time and log type, and backup the log to local computer.

Procedure

Step 1 Select **Info** > **Device Info** > **System Log**.

Figure 3-41 System log



Start Time 2023 - 06 - 20 00 : 00 : 00 End Time 2023 - 06 - 21 00 : 00 : 00

Type All

Found 9 logs Record Time 2023-06-20 09:24:07 -- 2023-06-20 01:58:47

No.	Time	Event
1	2023-06-20 09:24:07	User logged out
2	2023-06-20 09:21:27	User logged in
3	2023-06-20 09:16:07	User logged in
4	2023-06-20 01:59:07	Save
5	2023-06-20 01:59:07	Save
6	2023-06-20 01:59:07	Save
7	2023-06-20 01:58:47	Save
8	2023-06-20 01:58:47	Save

1/1 Go to 1

☑ File backup encryption ••••••••

Step 2 Configure **Start Time**, **End Time** and **Type**, and then click **Search**.

- Click the log to show details.
- Click **Clear** to clear all log information on the device. Log information cannot be cleared according to types.

Step 3 (Optional) Click **Backup** to back up the searched system log information to the computer under use.

Related Operations

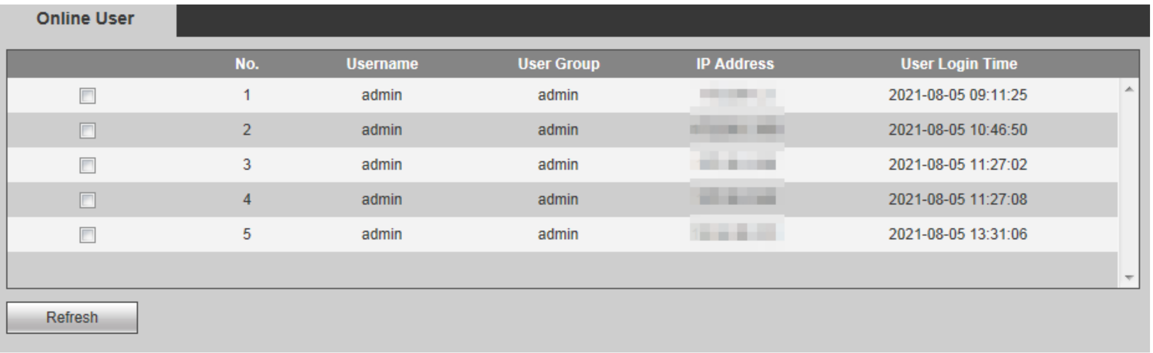
Select **File backup encryption** to encrypt the searched system log.

3.5.5 Online User

You can view usernames, groups, IP addresses and other basic information.

Select **Info** > **Device Info** > **Online User**.

Figure 3-42 Online user



Online User

	No.	Username	User Group	IP Address	User Login Time
☐	1	admin	admin	[redacted]	2021-08-05 09:11:25
☐	2	admin	admin	[redacted]	2021-08-05 10:46:50
☐	3	admin	admin	[redacted]	2021-08-05 11:27:02
☐	4	admin	admin	[redacted]	2021-08-05 11:27:08
☐	5	admin	admin	[redacted]	2021-08-05 13:31:06

3.5.6 About

Select **Info** > **Device Info** > **About**, and then you can view SN, device type and system version information.

3.5.7 Legal Information

Select **Info** > **Device Info** > **Legal Info**, and then you can view software license, privacy policy and open source software notice.

Appendix 1 Cybersecurity Recommendations

Cybersecurity is more than just a buzzword: it's something that pertains to every device that is connected to the internet. IP video surveillance is not immune to cyber risks, but taking basic steps toward protecting and strengthening networks and networked appliances will make them less susceptible to attacks. Below are some tips and recommendations on how to create a more secured security system.

Mandatory actions to be taken for basic equipment network security:

1. **Use Strong Passwords**

   Please refer to the following suggestions to set passwords:

   - The length should not be less than 8 characters;
   - Include at least two types of characters; character types include upper and lower case letters, numbers and symbols;
   - Do not contain the account name or the account name in reverse order;
   - Do not use continuous characters, such as 123, abc, etc.;
   - Do not use overlapped characters, such as 111, aaa, etc.;

2. **Update Firmware and Client Software in Time**

   - According to the standard procedure in Tech-industry, we recommend to keep your equipment (such as NVR, DVR, IP camera, etc.) firmware up-to-date to ensure the system is equipped with the latest security patches and fixes. When the equipment is connected to the public network, it is recommended to enable the "auto-check for updates" function to obtain timely information of firmware updates released by the manufacturer.
   - We suggest that you download and use the latest version of client software.

"Nice to have" recommendations to improve your equipment network security:

1. **Physical Protection**

   We suggest that you perform physical protection to equipment, especially storage devices. For example, place the equipment in a special computer room and cabinet, and implement well-done access control permission and key management to prevent unauthorized personnel from carrying out physical contacts such as damaging hardware, unauthorized connection of removable equipment (such as USB flash disk, serial port), etc.

2. **Change Passwords Regularly**

   We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.

3. **Set and Update Passwords Reset Information Timely**

   The equipment supports password reset function. Please set up related information for password reset in time, including the end user's mailbox and password protection questions. If the information changes, please modify it in time. When setting password protection questions, it is suggested not to use those that can be easily guessed.

4. **Enable Account Lock**

   The account lock feature is enabled by default, and we recommend you to keep it on to guarantee the account security. If an attacker attempts to log in with the wrong password several times, the corresponding account and the source IP address will be locked.

5. **Change Default HTTP and Other Service Ports**

   We suggest you to change default HTTP and other service ports into any set of numbers between 1024~65535, reducing the risk of outsiders being able to guess which ports you are using.

6. **Enable HTTPS**

   We suggest you to enable HTTPS, so that you visit Web service through a secure communication channel.

7. **MAC Address Binding**

   We recommend you to bind the IP and MAC address of the gateway to the equipment, thus reducing the risk of ARP spoofing.

8. **Assign Accounts and Privileges Reasonably**

   According to business and management requirements, reasonably add users and assign a minimum set of permissions to them.

9. **Disable Unnecessary Services and Choose Secure Modes**

   If not needed, it is recommended to turn off some services such as SNMP, SMTP, UPnP, etc., to reduce risks.

   If necessary, it is highly recommended that you use safe modes, including but not limited to the following services:

   - SNMP: Choose SNMP v3, and set up strong encryption passwords and authentication passwords.
   - SMTP: Choose TLS to access mailbox server.
   - FTP: Choose SFTP, and set up strong passwords.
   - AP hotspot: Choose WPA2-PSK encryption mode, and set up strong passwords.

10. **Audio and Video Encrypted Transmission**

    If your audio and video data contents are very important or sensitive, we recommend that you use encrypted transmission function, to reduce the risk of audio and video data being stolen during transmission.

    Reminder: encrypted transmission will cause some loss in transmission efficiency.

11. **Secure Auditing**

    - Check online users: we suggest that you check online users regularly to see if the device is logged in without authorization.
    - Check equipment log: By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.

12. **Network Log**

    Due to the limited storage capacity of the equipment, the stored log is limited. If you need to save the log for a long time, it is recommended that you enable the network log function to ensure that the critical logs are synchronized to the network log server for tracing.

13. **Construct a Safe Network Environment**

    In order to better ensure the safety of equipment and reduce potential cyber risks, we recommend:

    - Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.
    - The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.
    - Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.
    - Enable IP/MAC address filtering function to limit the range of hosts allowed to access the device.