Network Audio/Video Encoder

User Manual

UD.6L0202D2056A01

User Manual

About this Manual

This Manual is applicable to Network Audio/Video Encoder.

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 in the company website (http://overseas.hikvision.com/en/). Please use this user manual under the guidance of professionals.

Trademarks Acknowledgement

HIKVISION and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions. Other trademarks and logos mentioned below are the properties of their respective owners.

Legal Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, IS PROVIDED "AS IS", WITH ALL FAULTS AND ERRORS, AND HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT OF THIRD PARTY. IN NO EVENT WILL HIKVISION, ITS DIRECTORS, OFFICERS, EMPLOYEES, OR AGENTS 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 OR DOCUMENTATION, IN CONNECTION WITH THE USE OF THIS PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

REGARDING TO THE PRODUCT WITH INTERNET ACCESS, THE USE OF PRODUCT SHALL BE WHOLLY AT YOUR OWN RISKS. HIKVISION SHALL NOT TAKE ANY RESPONSIBILITES 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.

SURVEILLANCE LAWS VARY BY JURISDICTION. PLEASE CHECK ALL RELEVANT LAWS IN YOUR JURISDICTION BEFORE USING THIS PRODUCT IN ORDER TO ENSURE THAT YOUR USE CONFORMS THE APPLICABLE LAW. HIKVISION SHALL NOT BE LIABLE IN THE EVENT THAT THIS PRODUCT IS USED WITH ILLEGITIMATE PURPOSES.

IN THE EVENT OF ANY CONFLICTS BETWEEN THIS MANUAL AND THE APPLICABLE LAW, THE LATER PREVAILS.

Regulatory Information

FCC Information

FCC compliance: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

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 2004/108/EC, 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.

Safety Instruction

These instructions are intended to ensure that user can use the product correctly to avoid danger or property loss.

The precaution measure is divided into “Warnings” and “Cautions”

Warnings: Serious injury or death may occur if any of the warnings are neglected.

Cautions: Injury or equipment damage may occur if any of the cautions are neglected.

	
Warnings Follow these safeguards to prevent serious injury or death.	**Cautions** Follow these precautions to prevent potential injury or material damage.

 **Warnings**

- Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.
- In the use of the product, you must be in strict compliance with the electrical safety regulations of the nation and region. Please refer to technical specifications for detailed information.
- Input voltage should meet both the SELV (Safety Extra Low Voltage) and the Limited Power Source with 100~240 VAC, 48VDC or 12 VDC according to the IEC60950-1 standard. Please refer to technical specifications for detailed information.
- Do not connect several devices to one power adapter as adapter overload may cause over-heating or a fire hazard.
- Please make sure that the plug is firmly connected to the power socket.
- If smoke, odor or noise rise from the device, turn off the power at once and unplug the power cable, and then please contact the service center.

Preventive and Cautionary Tips

Before connecting and operating your device, please be advised of the following tips:

- Ensure unit is installed in a well-ventilated, dust-free environment.
- Unit is designed for indoor use only.
- Keep all liquids away from the device.
- Ensure environmental conditions meet factory specifications.
- Ensure unit is properly secured to a rack or shelf. Major shocks or jolts to the unit as a result of dropping it may cause damage to the sensitive electronics within the unit.
- Use the device in conjunction with an UPS if possible.
- Power down the unit before connecting and disconnecting accessories and peripherals.
- A factory recommended HDD should be used for this device.
- Improper use or replacement of the battery may result in hazard of explosion. Replace with the same or equivalent type only. Dispose of used batteries according to the instructions provided by the battery manufacturer.

TABLE OF CONTENTS

Chapter 1 Introduction

1.1 Description

Developed on the basis of the latest encoding technology, DS-6700 Series Audio/Video Encoder Server allows the analog signal to be digitized and then stored in hard disk or transmitted via network, capable of encoding at up to WD1(PAL: 960×576, NTSC: 960×480) or 4CIF resolution. Adopting the latest embedded processor, DS-6700 Series Audio/Video Encoder provides more powerful capabilities in audio/video encoding; data storage via SATA or network disk; various network protocols are supported; and code downloaded in FLASH ensures high stability and reliability of system performance.

1.2 Models

According to the different resolution, connection to HDD and channel numbers, the DS-6700 Series Encoder Server can be classified into the following models:

- DS-6701HFI, DS-6704HFI, DS-6708HFI, DS-6716HFI
- DS-6701HWI, DS-6704HWI, DS-6708HWI, DS-6716HWI
- DS-6701HFI-SATA, DS-6704HFI-SATA, DS-6708HFI-SATA, DS-6716HFI-SATA
- DS-6701HWI-SATA, DS-6704HWI-SATA, DS-6708HWI-SATA, DS-6716HWI-SATA

Description:

- **DS-6700HFI Series:** 1/4/8/16 video inputs; support up to 4CIF resolution; 1 microSD card can be connected to DS-6701/6704HFI for local recording.
- **DS-6700HFI-SATA Series:** 1/4/8/16 video inputs; support up to 4CIF resolution; 1 SATA HDD can be connected with up to 4TB capacity for local recording.
- **DS-6700HWI Series:** 1/4/8/16 video inputs; support up to WD1 resolution, with 4CIF, 2CIF, CIF and QCIF selectable; 1 microSD card can be connected to DS-6701/6704HWI for local recording.
- **DS-6700HWI-SATA Series:** 1/4/8/16 video inputs; support up to WD1 resolution, with 4CIF, 2CIF, CIF and QCIF selectable; 1 SATA HDD can be connected with up to 4TB capacity for local recording.

1.3 Features

Encoding

- Support H.264/MPEG4/MPEG2/MJPEG encoding standards.
- Support encoding video at up to 4CIF resolution for DS-6700HFI (-SATA) models and up to WD1 resolution for DS-6700HWI (-SATA) models.
- Dual stream encoding.
- Either compound streams encoding or video stream encoding selectable; audio and video synchronization during compound streams encoding.

Network

- One 10M/100Mbps adaptive Ethernet interface (PoE) for DS-6701/6704HFI/HWI models.
- One 10M/100M/1000Mbps adaptive Ethernet interface for DS-6708/6716HFI/HWI and DS-6701/6704/6708/6716HFI/HWI-SATA models.
- Accessible by multiple web browsers: IE, FireFox, Chrome and Safari.
- Remote web browser access by HTTPS ensures high security.
- Netfilter builds internet firewalls based on packet filtering.
- QoS protocol enhances the data transmission performance.
- Support SNMPv1/v2c/v3 simple network management protocol.
- mDNS-based Apple's Bonjour protocol enables automatic discovery of devices.
- Support email notifications, FTP upload and alarms upload by SOCKS v4/v5 proxy server.
- Zero configuration networking (Zeroconfig) enables the device to automatically obtain the IPv4 link-local IP addresses (range: 169.254.1.0~169.254.254.255).
- Auto/Manual port mapping by UPnP™.
- Support PSIA, ONVIF, CGI, GENETEC and IEEE802.1X protocols.
- Support SADP software to automatically search and discover the online devices in local network area.
- Automatically get IP address by DHCP protocol.
- RTSP/RTP standard stream media protocol allows user to live view by unicast.
- Multicast address for live view of multiple cameras through network.
- Two-way audio and single-directional broadcasting.
- Transmission via RS-232 and RS-485 transparent channel.
  Note: DS-6701HFI/HWI model provides no RS-232 interface.
- Access to Internet by PPPoE method, and support Peanut Hull, DynDNS, HiDDNS, etc.
- Set time by NTP.
- Connectable with network HDD in NAS, IP SAN mode.
- Send email by SMTP protocol, and support attachment of captured JPEG image and SSL encryption.
- Remote JPEG image capturing with user-defined image resolution and quality.

PTZ Control

- **Support Multiple PTZ Protocols**

  Different channels can be configured with protocol type, RS-485 address, baud rate, data bit, stop bit, even & odd parity, stream control method, etc.; and remote configuration of presets, patrols and patterns.
- **Digital Zooming (with Speed Dome)**

  When connected with Hikvision speed dome, digital zooming can be realized by clicking on the image through client software.
- **PTZ linkage**

  Relay input alarm can be responded with PTZ linkage actions, e.g., callup of predefined presets or patrols.

Alarm

- **Relay Alarm Input**

  Either NO mode or NC mode can be set.

  Four different alarm arming periods are configurable.

  Capabilities of triggering corresponding alarm handling methods, relay alarm output, buzzer alarm, upload to control center, PTZ linkage, presets/patrols/patterns callup, etc.
- **Relay Alarm Output**

  Relay alarm output can be connected with alarm devices for alarm handling within arming period.

Exceptions

- **Exception Alarm Handling**

  Exception alarms include network disconnect alarm, IP address conflict alarm, illegal access alarm, etc.; multiple alarm handling methods are supported, relay alarm output, buzzer alarm, upload to center, etc.

- **Exception Reboot**

  Software watchdog capability: for inspecting important threads and system resources of device; in case of exceptions detected, the device will be automatically rebooted.

  Firmware watchdog: for inspecting the firmware of device; in case of exceptions in system task scheduling, the device will be automatically rebooted.

Logs

The system logs can be classified into the operation logs, alarm logs, exception logs and information logs. User may search and view all recorded system logs by date or type, as well as export the logs to the text format over network.

Note: Hard disk/network disk/microSD card must be connected before log operation.

Chapter 2 Panels and Connections

2.1 Front Panel

DS-6701HWI/HFI:

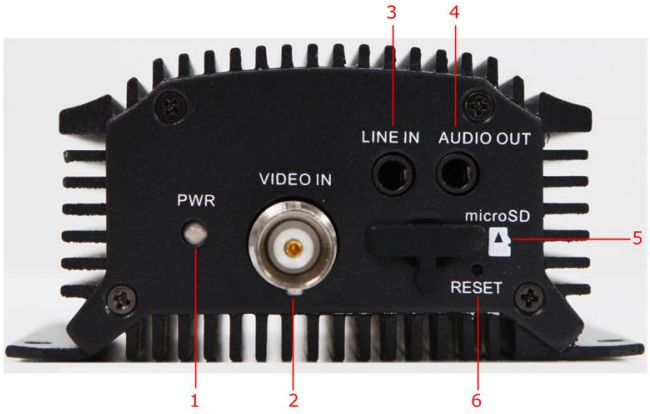


Figure 2. 1 Front Panel of DS-6701HWI/HFI

Table 2. 1 Front Panel of DS-6701HWI/HFI

	Item	Description
1	POWER LED Indicator	Light in red when the device is powered on; light in orange when the SD card is inserted.
2	VIDEO IN	BNC connector for video input.
3	LINE IN	3.5mm interface for two-way audio input or audio input; connect to audio input device or active pick-up, microphone, etc.
4	AUDIO OUT	3.5mm interface; connect to audio output device, e.g., loudspeaker, etc.
5	microSD	microSD interface for data storage.
6	Reset	Restore the factory default settings by holding the *RESET* button for more than 15 seconds after power is turned on.

DS-6704HWI/HFI:

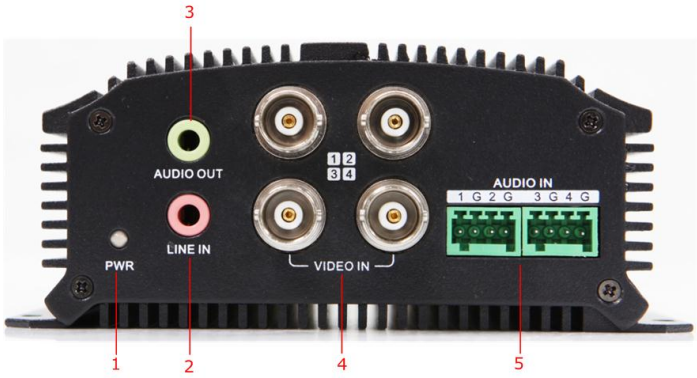


Figure 2. 2 Front Panel of DS-6704HWI/HFI

Table 2. 2 Front Panel of DS-6704HWI/HFI

	Item	Description
1	POWER LED Indicator	Light in red when the device is powered on; light in orange when the SD card is inserted.
2	LINE IN	3.5mm two-way audio input interface; connect to active pick-up, microphone, etc.
3	AUDIO OUT	3.5mm interface; connect to audio output device, e.g., loudspeaker, etc.
4	VIDEO IN	BNC interface for video input.
5	AUDIO IN	Line input interface for audio input.

DS-6708/6716 and DS-6701/6704/6708/6716-SATA:

Figure 2. 3 Front Panel of DS-6708 and DS-6701/6704/6708-SATA

Figure 2. 4 Front Panel of DS-6716 and DS-6716-SATA

Table 2. 3 Front Panel of DS-6708/6716 and DS-6701/6704/6708/6716-SATA

	Indicator	Description
1	POWER	Lights in red when the device is powered on.
2	STATUS	Lights in red when data is being read from or written to HDD. Valid for DS-6708HWI/HFI-SATA model only.
3	Tx/Rx	1. Does not light when the network is not connected; 2. Blinks in green when the data is transmitting / receiving; 3. Blinks at higher frequency when the data for transmitting / receiving is larger.

2.2 Rear Panel

DS-6701HWI/HFI:

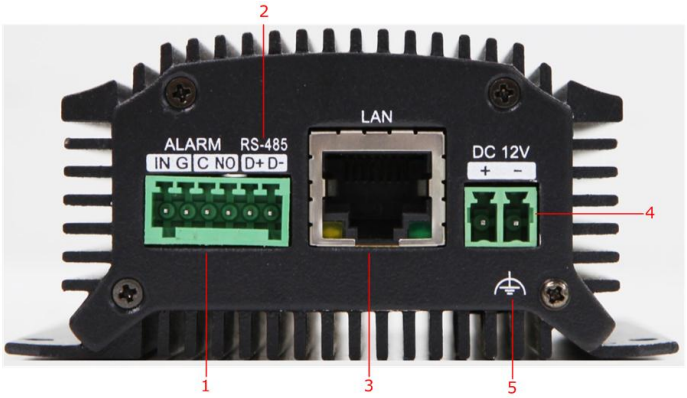


Figure 2. 5 Rear Panel of DS-6701HWI/HFI

Table 2. 4 Rear Panel of DS-6701HWI/HFI

	Item	Description
1	ALARM IN /OUT	Relay alarm input/output. ***Note:*** The alarm output terminal provides no JP2 pin.
2	RS-485	RS-485 serial interface; connect to pan/tilt unit, speed dome, etc.
3	LAN	10M/100Mbps adaptive Ethernet interface (PoE). The right LED indicator lights in green when the network cable is connected, and the left LED indicator blinks in orange when data is transmitting / receiving.
4	DC12V	12V DC power supply.
5	GND	Grounding

DS-6704HWI/HFI:

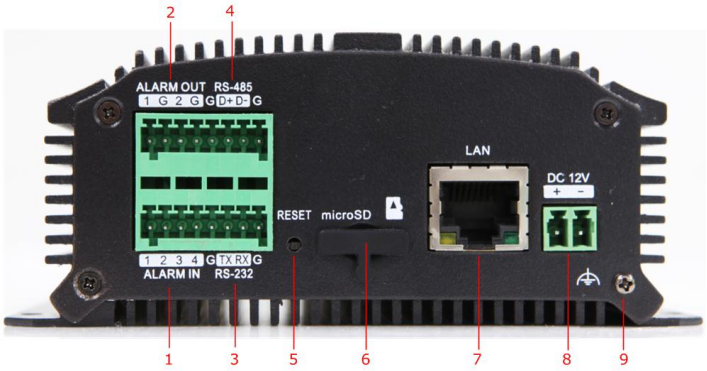


Figure 2. 6 Rear Panel of DS-6704HWI/HFI

Figure 2. 7 Rear Panel of DS-6704HWI/HFI

	Item	Description
1	ALARM IN	Relay alarm input.
2	ALARM OUT	Relay alarm output.
3	RS-232	Serial interface for configuration of device's parameters or used as transparent channel.
4	RS-485	RS-485 serial interface; connect to pan/tilt unit, speed dome, etc.
5	RESET	Restore the factory default settings by holding the *RESET* button for more than 15 seconds after the device is turned on.
6	microSD	microSD interface for data storage.
7	LAN	10M/100Mbps adaptive Ethernet interface (PoE). The right LED indicator lights in green when the network cable is connected, and the left LED indicator blinks in orange when data is transmitting / receiving.
8	DC12V	12V DC power supply.
9	GND	Grounding

Note: The DS-6701HWI/HFI and DS-6704HWI/HFI models provide no beeper.

DS-6708HWI/HFI (-SATA):

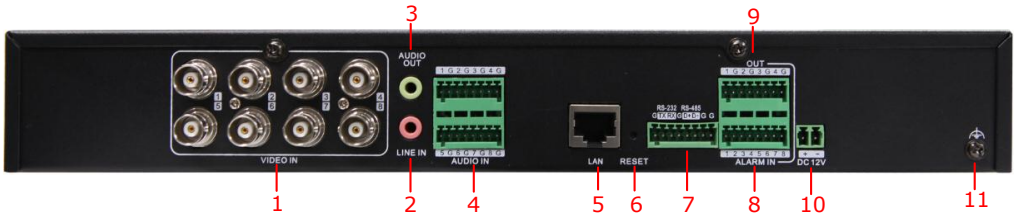


Figure 2. 8 Rear Panel of DS-6708HWI/HFI(-SATA)

Note: DS-6701/6704 HWI-SATA and DS-6701/6704 HFI-SATA models provide 1/4 video input and 1/4 audio input interfaces on the rear panel.

Table 2. 5 Rear Panel of DS-6708HWI/HFI (-SATA)

	Item	Description
1	VIDEO IN	BNC connectors for video input.
2	LINE IN	3.5mm two-way audio input interface; connect to active pick-up, microphone, etc.
3	AUDIO OUT	3.5mm audio output interface; connect to audio output device, e.g., loudspeaker, etc.
4	AUDIO IN	Line input interface for audio input.
5	LAN	10M/100/1000Mbps adaptive Ethernet interface.
6	RESET	Restore the factory default settings by holding the *RESET* button for more than 15 seconds after the device is turned on.
7	RS-232, RS-485	RS-232 serial interface for configuration of device's parameters or used as transparent channel; RS-485 serial interface for connection to pan/tilt unit, speed dome, etc.
8	ALARM IN	Relay alarm input.
9	ALARM OUT	Relay alarm output.
10	DC12V	12V DC power supply.
11	GND	Grounding

DS-6716HWI / HFI (-SATA):

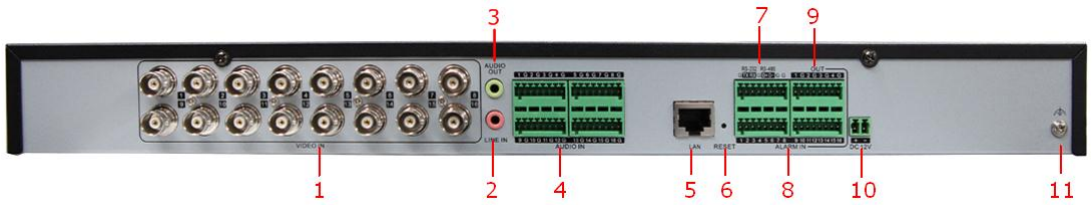


Figure 2. 9 Rear Panel of DS-6716HWI/HFI (-SATA)

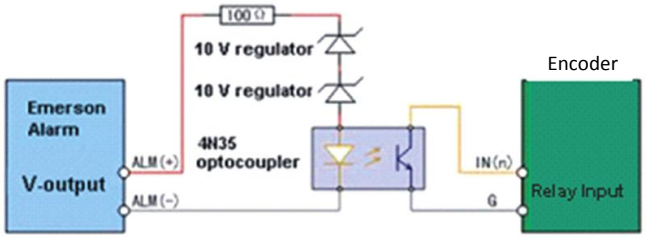
Table 2. 6 Rear Panel of DS-6716HWI/HFI (-SATA)

	Item	Description
1	VIDEO IN	BNC connectors for video input.
2	LINE IN	3.5mm two-way audio interface; connect to active pick-up, microphone, etc.
3	AUDIO OUT	3.5mm audio output interface; connect to audio output device, e.g., loudspeaker, etc.
4	AUDIO IN	Line input interface for audio input.
5	LAN	10M/100/1000Mbps adaptive Ethernet interface.
6	RESET	Restore the factory default settings by holding the *RESET* button for more than 15 seconds after power is turned on.
7	RS-232, RS-485	RS-232 serial interface for configuration of device's parameters or used as transparent channel; RS-485 serial interface for connection to pan/tilt unit, speed dome, etc.
8	ALARM IN	Relay alarm input.
9	ALARM OUT	Relay alarm output.
10	DC12V	12V DC power supply.
11	GND	Grounding

2.3 Alarm Connections

2.3.1 Alarm Input Connections

DS-6700 supports the open/close relay input as the alarm input mode. For the alarm input signal not in open/close relay signal mode, please follow the connections shown as below:
Alarm input connections for Emerson Alarm:



Note: The relay input port of the Encoder should be set to NC mode.

Figure 2. 10 Alarm Input Connections for Emerson Alarm

Alarm input connections for Normal Alarm:

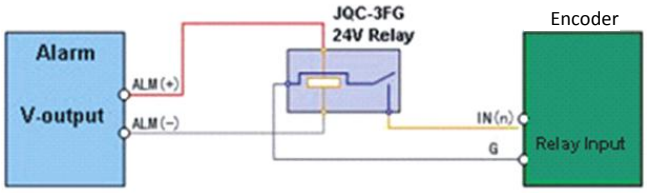


Figure 2. 11 Alarm Input Connections for Normal Alarm

2.3.2 Alarm Output Connections

DS-6700 supports the open/close relay input as the alarm output mode. The alarm input can be selected to *NO* or *NC*. Different alarm output connection methods are applied to the AC or DC load. Please refer to the following diagram:
Alarm output connections diagram:

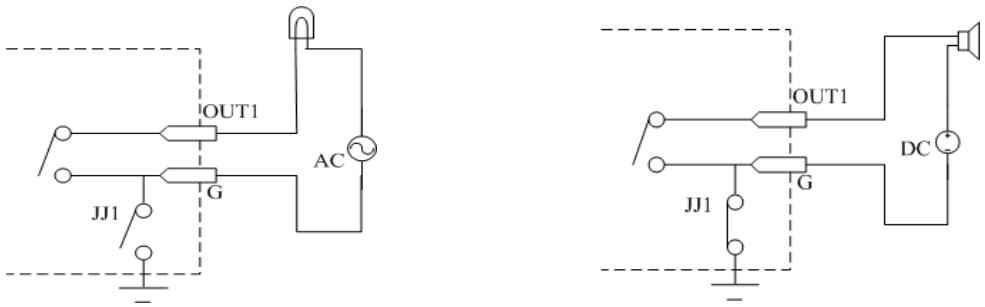


Figure 2. 12 Alarm Output Connections

Note: The DS-6701HWI/HFI has no JJ1 relay.

Please note the different connections of JJ1 shown above.

For DC load, JJ1can be safely used both in *NC* and *NO* methods, and it is recommended to use within the limit of 12V/1A. For external AC input, JJ1 must be open. The motherboard provides two jumpers, each corresponding to one alarm output. And both of two jumpers are factory set to be connected.

Chapter 3 Activation and Initial Network Configuration for the Encoder

You are required to activate the encoder first by setting a strong password for it before you can use the device. Activation via Web Browser, Activation via SADP, and Activation via Client Software are all supported.

3.1 Setting the Admin Password via Web Browser

Steps:

1. Power on the encoder, and connect the encoder to the network.
2. Input the IP address into the address bar of the web browser, and press Enter to enter the activation interface.

Note: The default IP address of the network encoder is 192.0.0.64. You are recommended to change the default IP address after your access.

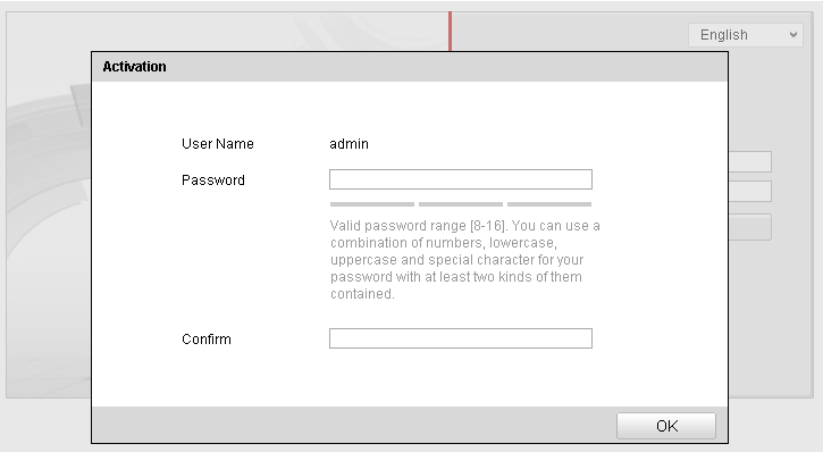


Figure 3. 1 Activation Interface

3. Create a password and input the password into the password field.

STRONG PASSWORD RECOMMENDED– We highly recommend that you create a strong password of your own choosing (using 8-16 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend that you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

4. Confirm the password.
5. Click **OK** to save the password and enter the live view interface.

3.2 Setting Admin Password and Modifying Network Parameters via Client Software

The client software is versatile video management software for multiple kinds of devices.

Get the client software from the supplied disk or the official website, and install the software according to the prompts. Follow the steps to activate the camera.

Steps:

1. Run the client software and the control panel of the software pops up, as shown in the figure below.

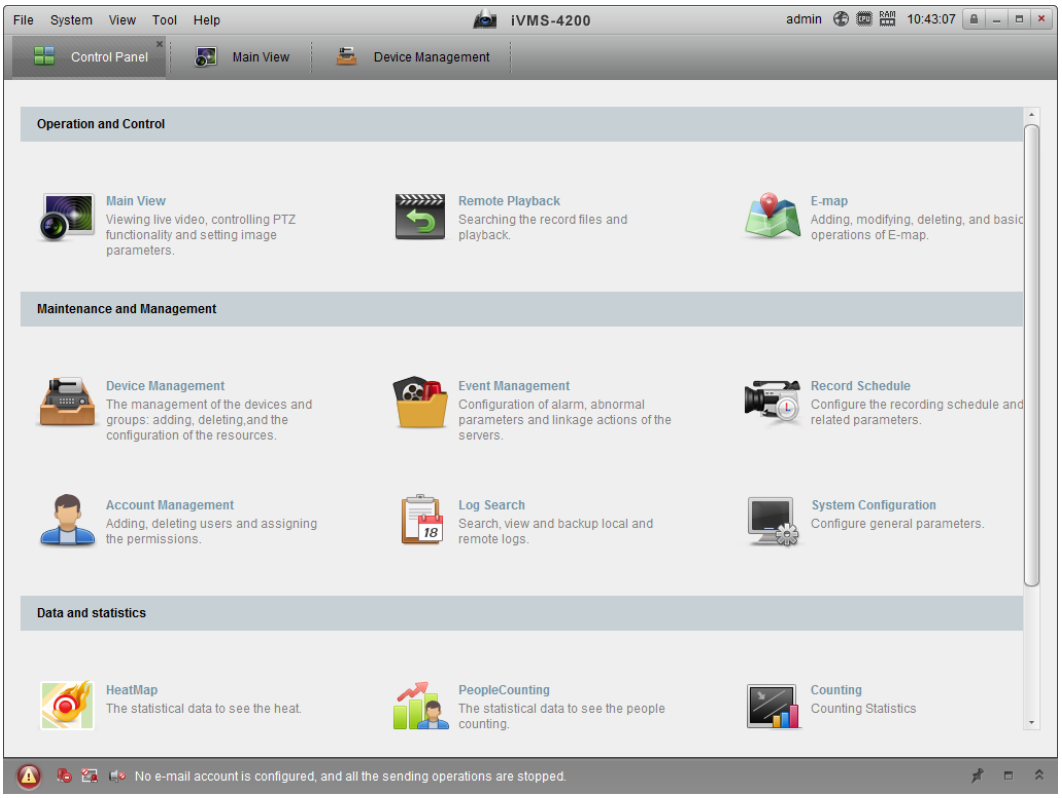


Figure 3. 2 Control Panel

2. Click the **Device Management** icon to enter the Device Management interface, as shown in the figure below.

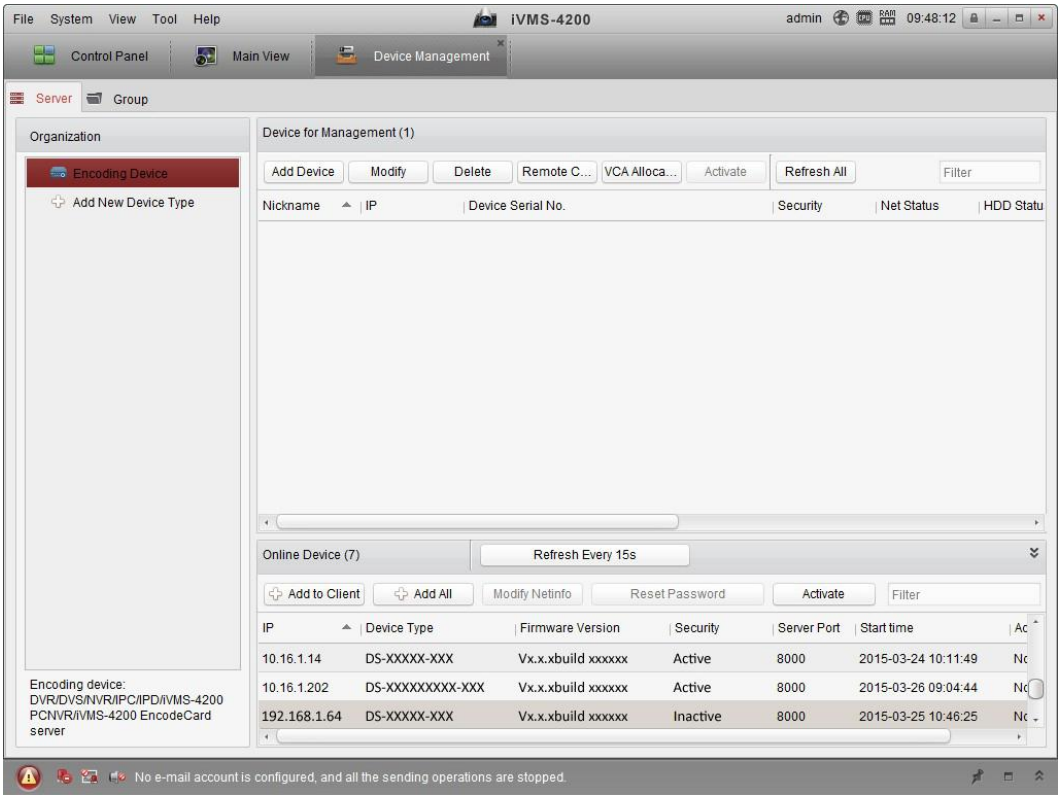


Figure 3. 3 Control Panel

3. Check the device status from the device list, and select an inactive device.
4. Click the **Activate** button to pop up the Activation interface.
5. Create a password and input the password in the password field, and confirm the password.

STRONG PASSWORD RECOMMENDED– We highly recommend that you create a strong password of your own choosing (using 8-16 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend that you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

Figure 3. 4 Activation Interface (Client Software)

6. Click **OK** button to start activation.
7. Click the **Modify Netinfo** button to pop up the Network Parameter Modification interface, as shown in the figure below.

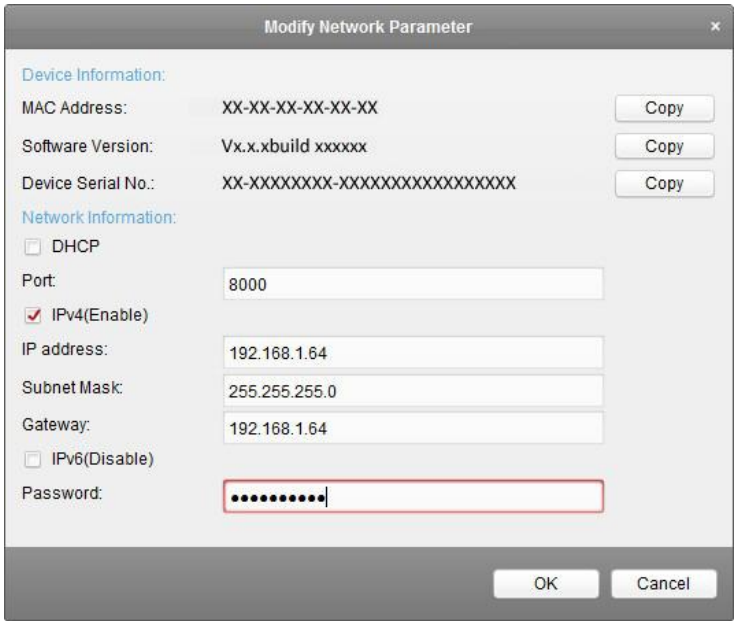


Figure 3. 5 Modifying the Network Parameters

8. Change the device IP address to the same subnet with your computer by either modifying the IP address manually or checking the checkbox of Enable DHCP.
9. Input the password to activate your IP address modification.

Chapter 4 Access to DS-6700 by WEB Browser

The DS-6700 can also be accessed by WEB Browser for configuration and operation. The supported WEB browsers include: Internet Explorer 6/7/8/9, Firefox 3.5 and above, Chrome 8 and above, Safari 5.0.2 and above, Windows XP SP1 and above (32-bit).

Before you start:

- Before access, you need to configure the network settings of device according to *Chapter 3*.
- Connect the device to the LAN, and prepare a PC connected to the same LAN with the device.
- The factory default IP address of the device is *192.0.0.64*.

4.1 Installing Web Components

Steps:

1. Open WEB browser, input the IP address of DS-6700 (e.g., http://192.0.0.64) and then press the **Enter** key on PC. The system will display the login interface.

Note: When the HTTPS feature is enabled, the system will use the HTTPS login mode (e.g., https://192.0.0.64) by default when you input the IP address. You can also input http://IP address/index.asp (e.g., http://192.0.0.64/index.asp) if you want to use HTTP mode to log into the device.

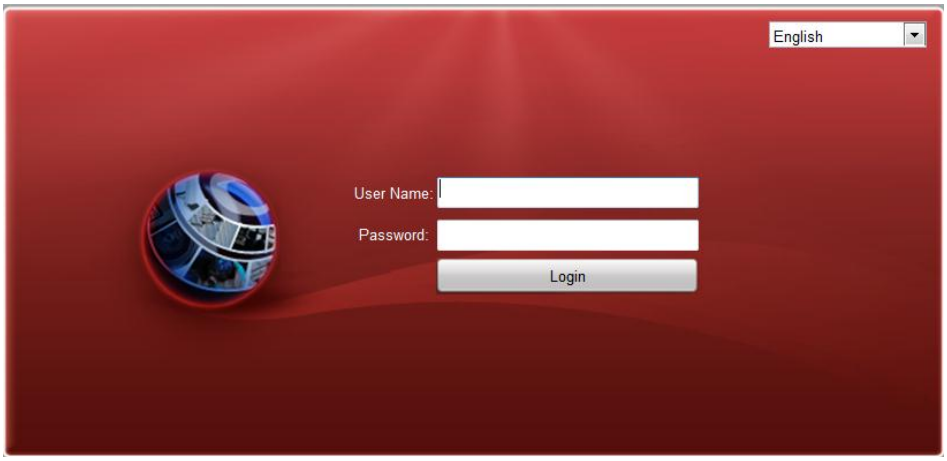


Figure 4. 1 Login Page

Input the user name and the password to log into the system.

Note: In the Login dialog box, if you have entered the wrong password for 7 times for the admin user or 5 times for the normal user, the current user account will be locked for 60 seconds.

2. On the main page of DS-6700, you need to download and install the plug-in.

(1) Click on the live view panel by following the hints on the screen.

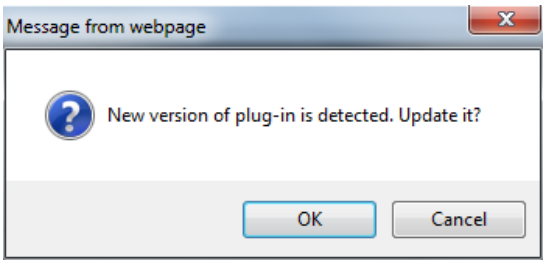


Figure 4. 2 Download and Install Plug-in

(2) Click **Run** or **Save** on the pop-up warning message box.

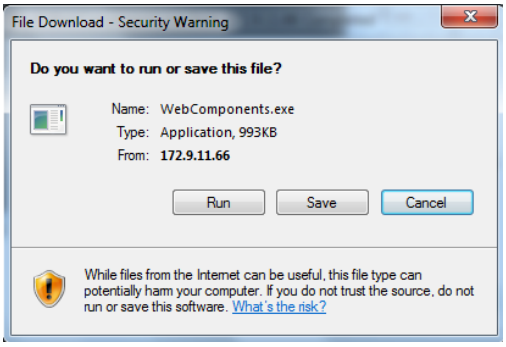


Figure 4. 3 Run Web Components

(3) Click **Next** on the pop-up Setup dialog box.

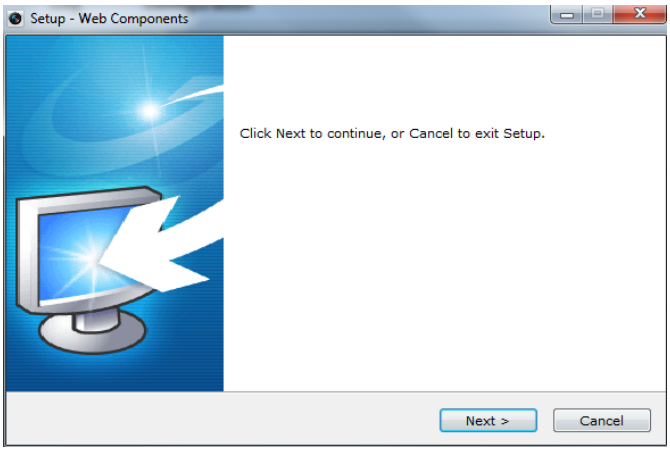


Figure 4. 4 Click Next

(4) When the installation completes, click **Finish** to finish the installation of Web Components.

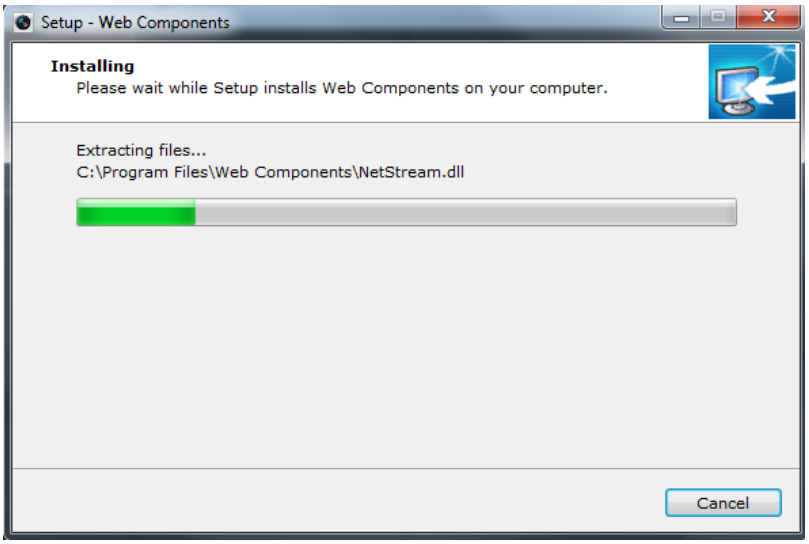


Figure 4. 5 Install the Web Components

4.2 Main Page

After successful login, you will enter the main page automatically.

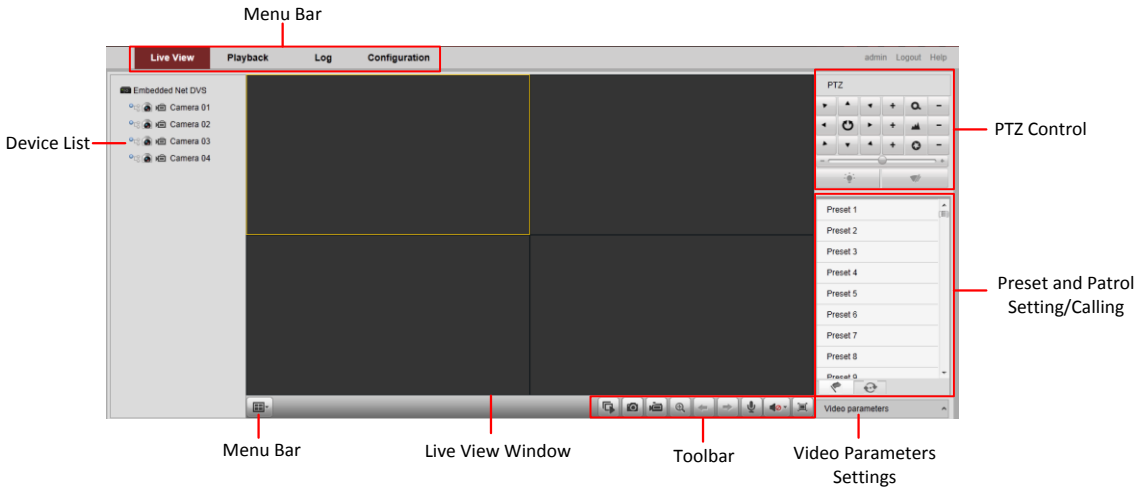


Figure 4. 6 Main Page

Description of the live view page:

Menu Bar: Enter the Live View, Playback, Log and Configuration page respectively.

Device List: Display the connected encoder and its channels.

Window-division: 1/4-division display mode.

Live Video Window: Display the live video of the current camera.

Toolbar: Realize functions in live view mode, e.g., live view, capture, recording, audio on/off, two-way audio, etc.

PTZ Control: Realize PTZ control of the camera (supports PTZ function), and the lighter and wiper control.

Preset Setting/Calling: Set and call the preset for the camera (supports PTZ function).

Video Parameters Settings: Configure the brightness, contrast, hue and saturation of the live video.

Chapter 5 Live View

Live view shows you the video image getting from the connected camera in real time. After successful login, the system will enter the live view page automatically.

5.1 Starting Live View

Steps:

1. In the live view window, select a playing window by clicking the mouse.
2. Double click a camera from the device list to start the live view.

Figure 5. 1 Start Live View

3. You can click the  button on the toolbar to start the live view of all cameras on the device list.

Refer to the following table for the description of buttons on the live view window:

Table 5. 1 Description of Toolbar

Icon	Description
	Select the window-division mode
	Start/Stop live view
	Capture pictures in live view mode
	Manually start/stop recording
	Enable e-PTZ
	Previous page

	Next page
	Audio on/off
	Start/Stop two-way audio
	Switch to full-screen live view mode.

Note: Before using two-way audio function or recording with audio, please select the **Stream Type** to **Video & Audio** on *Section Configuring Video Settings.*

5.1.1 Main/Sub Stream Live View

You can select the main stream or sub stream for live view by clicking the corresponding icon as shown below:

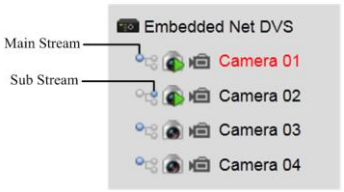


Figure 5. 2 Main Stream/Sub Stream for Live View

The main stream gets higher video quality while the sub stream requires lower bandwidth.

5.1.2 Full-screen Mode

You can click the button on the toolbar or double click on the live video to switch to the full-screen view mode. To switch back to the normal mode, click the or double click on the live video again.
Please refer to the following section for more information:

1. Capturing pictures on *Section Capturing the Picture.* .
2. Configuring recording on *Record/Capture Settings*.
3. Setting the image quality of live view on *Section Local Configuration.*
4. Setting the saving path for the recorded video files and captured pictures on *Section Local Configuration.*
5. Setting the OSD text on live video on *Section Configuring OSD Settings.*

5.2 Capturing the Picture

In live view mode, click the button on the toolbar to capture the live pictures.

When the picture is captured, the following pop-up message box will appear at the lower right corner.

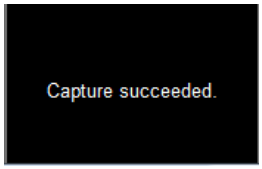


Figure 5. 3 Picture Capture Succeeded

***Notes*:**

- The saving path for the captured pictures can be set at the **Configuration > Local Configuration** page.
- The image is saved as a JPEG file on your computer.

5.3 Operating PTZ Control

Before you start:

1. Make sure the encoder is connected with the camera/dome which supports PTZ function. Connect the *R*+ and *R*− terminals of the pan/tilt unit or speed dome to RS-485 D+ and RS-485 D- terminals of the DS-6700 respectively.
2. The baud rate, PTZ control and address configured in the **RS-485 Settings** interface (**Remote Configuration > Serial Port Settings > 485 Serial Port**), as shown in Figure 6.3, must be the same with the parameters of the connected pan/tilt unit or speed dome.

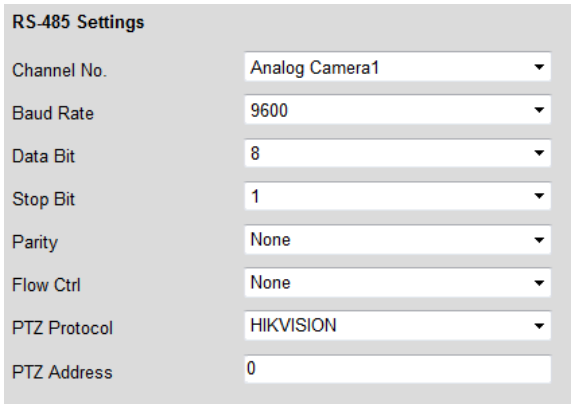


Figure 5. 4 RS-485 Settings

5.3.3 Operating PTZ Movement

In live view mode, you can use the PTZ control buttons to realize pan/tilt/zoom control of the camera lens.

There are 8 directional buttons (up, down, left, right, upper left, upper right, bottom left, bottom right) on the display window when the mouse is located in the relative positions.

Click on the directional buttons to control the pan/tilt movement.

Figure 5. 5 PTZ Control Panel

Click the zoom/iris/focus buttons to realize lens control.

Refer to the following table for description of PTZ control buttons:

Table 5. 2 Description of PTZ Control Buttons

Button	Description
	Zoom in/out
	Focus near/far
	Iris open/close
	Light
	Wiper
	Adjust speed of pan/tilt movement

5.3.4 Setting / Calling a Preset

Setting a Preset:

1. In live view mode, click the  from the PTZ control area to enter the preset settings interface.
2. Select a preset number from the preset list.

Figure 5. 6 Set a Preset

3. Use the PTZ control buttons to move the lens in the desired position. You can use any of the following commands:
   - Pan the camera to the right or left.
   - Tilt the camera up or down.
   - Zoom in or out.
   - Refocus the lens.
4. Click the  icon to finish the setting of current preset.

***Note*:** Up to 256 presets are configurable depending on the PTZ protocol applied.

Calling a Preset:

This feature enables the camera to point to a specified preset scene when an event takes place.

For the pre-defined preset, you can call it at any time to the desired preset scene.

In live view mode, select a predefined preset from the list and click the  icon to call a preset.

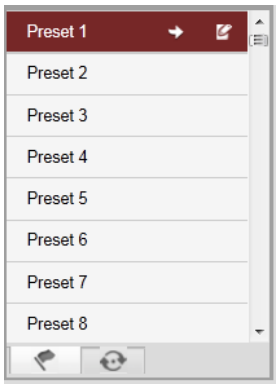


Figure 5. 7 Call a Preset

Linking to Alarm:

The preset can also be used to link to the alarm input when there is alarm event occurring.

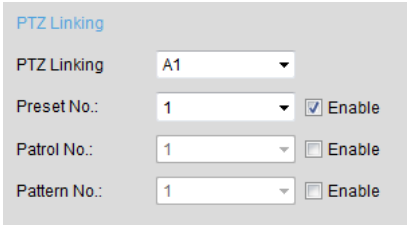


Figure 5. 8 PTZ Linking

Please refer to *Chapter Configuring and Handling Alarms* for the PTZ Linking settings (Remote Configuration>Alarm Settings>Alarm Input>Linkage Method).

5.3.5 Setting / Calling a Patrol

Setting a Patrol:

1. In live view mode, click the  from the PTZ control area to enter the patrol settings interface.
2. Select a patrol number from the patrol list for setting.

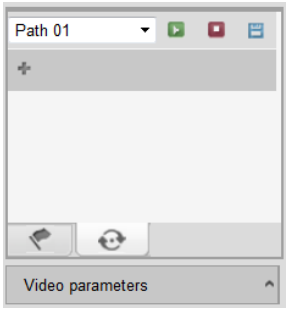


Figure 5. 9 Patrol Setting

3. Click the  button to enter the Add Patrol Path interface.

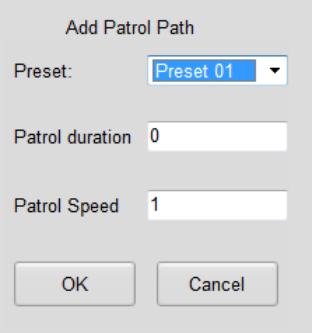


Figure 5. 10 Add Patrol Path

4. Configure patrol parameters, including the preset No., duration of staying for one preset and speed of patrol.

   Preset: determines the order at which the PTZ will follow while cycling through the patrol.

   Patrol Duration: refers to the time span to stay at the corresponding key point. The duration can be set to 0-30 sec.

   Patrol Speed: defines the speed at which the PTZ will move from one key point to the next. The speed can be set to 1-40.

5. Click **OK** to save the path to the current patrol.

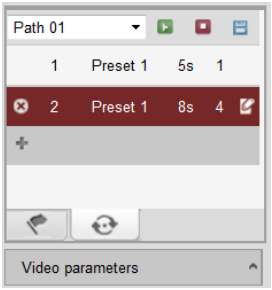


Figure 5. 11 Added Patrol Path

6. Repeat the above step3-5 to add more patrol paths.

   You can also click  to edit the existing patrol path, or click  to delete it.

7. Click  to save the patrol settings.

   Repeat the above steps to configure other patrols.

   ***Note*:** Up to 16 patrols can be configured.

Calling a Patrol:

The PTZ camera will move according to the predefined patrol path when you call a patrol.

In live view mode, select a predefined patrol from the list and click the  icon to start calling a patrol, and click  to stop the calling.

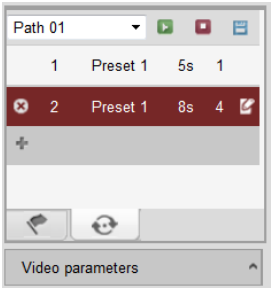


Figure 5. 12 Call a Patrol

5.4 Configuring Video Parameters

Purpose:

You can configure the video parameters, including the brightness, contrast, saturation and hue.

Steps:

1. In the live view interface, click the Video parameters button on the bottom right corner to spread the Video Parameters Setting interface:

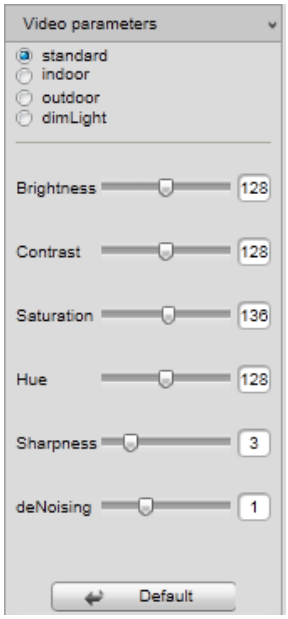


Figure 5. 13 Video Parameters Settings

2. Select the mode according to different light conditions. Four modes are selectable:
   - **Standard**: in general lighting conditions (default).
   - **Indoor:** the image is relatively smoother.
   - **Outdoor:** the image is relatively clearer and sharper. The degree of contrast and saturation is high.
   - **Dim Light:** the image is smoother than the other three modes.
3. Move the slider to set the brightness, contrast, saturation and hue to 0~255. The default value is 128 for the brightness, contrast and hue is 128 and 136 for the saturation.
4. Move the slider to set the sharpness to 0~15 and the denoising level to 0~3. The default value is 3 for the sharpness and 1 for the denoising level.

   ***Note*:** You can click the Default button to restore the default settings.

Chapter 6 Device Configuration

6.1 Local Configuration

Click **Configuration > Local Configuration** to enter the Local Configuration interface.

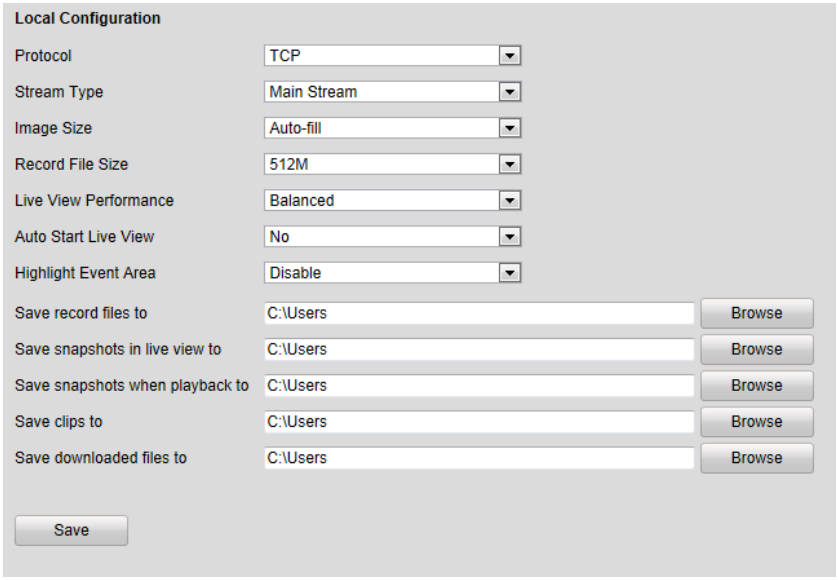


Figure 6. 1 Local Configuration

Configure the following settings:

Protocol Type: Set the protocol type of stream transmission to TCP or UDP.

- **UDP:** provides more real-time audio and video streams.
- **TCP:** ensures complete deliver of streaming data and better video quality, yet its real-time effect is not so good.

Stream Type: Select the stream type to main stream or sub stream used for live view by Web browser. Please refer to *Section Configuring Video Settings* for the parameters settings of the main stream and sub stream respectively.

Image Size: Select the window-division view mode to 4:3, 16:9 or Auto-fill.

Record File Size: Select the size of packed video files during manual recording to 256M, 512M or 1G.

Live View Performance: Set the live viewing performance to Least Delay, Balanced (delay and fluency) or Best Fluency.

Auto Start Live View: Enable or disable the auto-start of live view once you open the Web browser.

Highlight Event Area: Enable or disable the Highlight Event Area. When this feature is enabled, the motion detection triggered frame for the moving targets in the motion detection area will be highlighted in green color. Please refer to *Chapter 8.4.1 Configuring Motion Detection*.

Save record files to: Set the saving path for the manually recorded video files.

Save snapshots in live view to: Set the saving path for the manually captured pictures in live view mode.

Save snapshots when playback to: Set the saving path for the captured pictures in playback mode.

Save clips to: Set the saving path for the clipped video files in playback mode.

Save downloaded files to: Set the saving path for the downloaded video files or pictures.

***Note*:** You can click the **Browse** button to change the directory for saving the video files and pictures.

6.2 Device Parameters

6.2.1 Configuring Time Settings

Steps:

1. Click **Remote Configuration > Device Parameters > Time Settings** to enter the Time Settings interface:

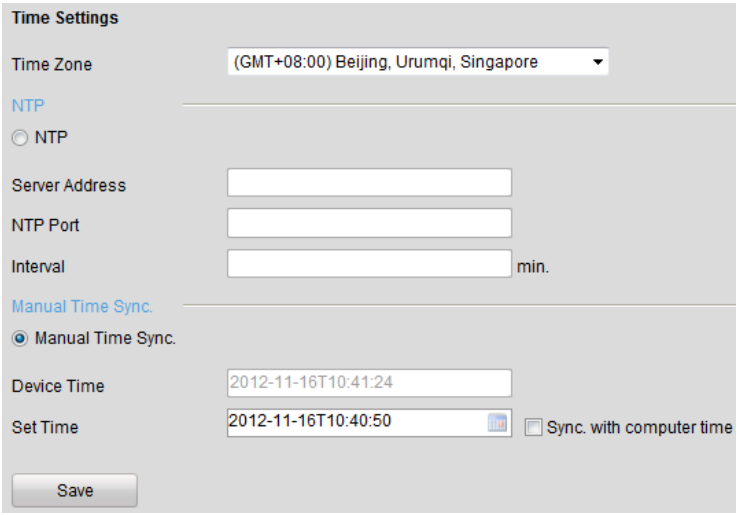


Figure 6. 2 Time Settings

2. Select the Time Zone.

Select the Time Zone that is closest to the device's location from the drop-down menu.

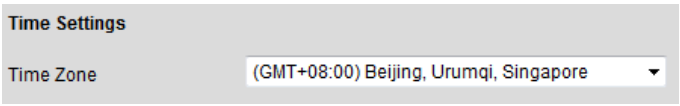


Figure 6. 3 Time Zone Settings

3. Configure the time synchronization by NTP server or by manually.

- **Configuring Time Sync by NTP Server**

A Network Time Protocol (NTP) Server can be configured on your device to ensure the accuracy of system date/time.

If the device is connected to a Dynamic Host Configuration Protocol (DHCP) network that has time server properties configured, the camera will synchronize automatically with the time server.

Enable the **NTP** function by checking the checkbox, and configure the following settings:

NTP Server: IP address of NTP server.

NTP Port: Port of NTP server.

Interval: The time interval between the two synchronizing actions with NTP server. It can be set from 1 to 10080

minutes.

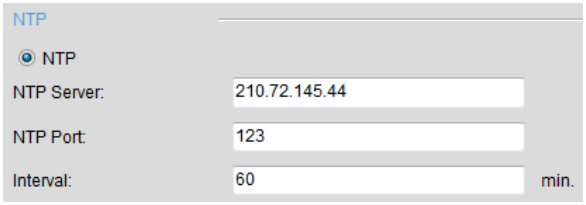


Figure 6. 4 Time Sync by NTP Server

***Note*:** If the device is connected to a public network, you should use a NTP server that has a time synchronization function, such as the server at the National Time Center (IP Address: 210.72.145.44). If the device is set up in a more customized network, NTP software can be used to establish a NTP server used for time synchronization.

- Configuring Time Synchronization by Manually

Enable the **Manual Time Sync** function and then click the icon to set the system time from the pop-up calendar. You can click the icon to quickly select the time.

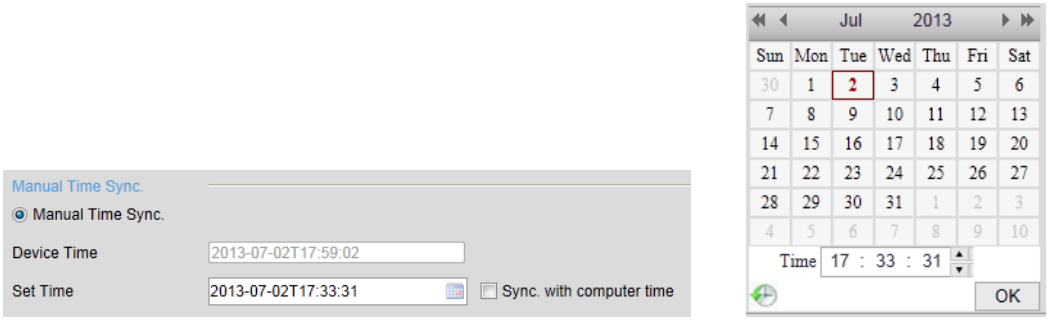


Figure 6. 5 Time Sync by Manually

You can also check the checkbox of **Sync. with computer time** to synchronize the time with the local PC.

- Click the **DST** tab page to enable the DST function and set the date of the DST period.

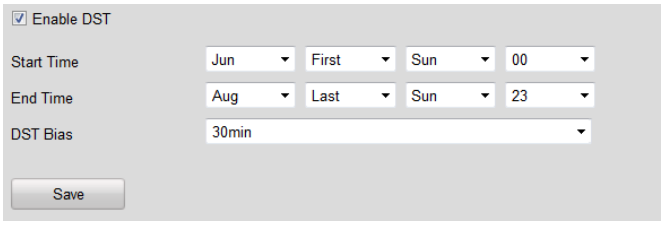


Figure 6. 6 DST Settings

4. Click the **Save** button to save the settings.

6.2.2 Configuring Packet Time of Recording

The recorded file is packed in 1G by default. You can also customize the packet time in the advanced settings page.

Steps:

1. Click **Remote Configuration> Device Parameters> Advanced** to enter the advanced settings interface.

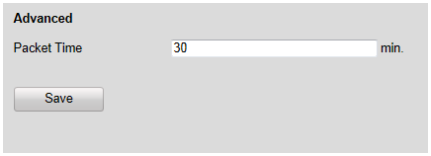


Figure 6. 7 Packet Time of Recording

2. Set the packet time of the recorded file.

   ***Note*:** The packet time can be set to 1~300 minutes.

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

6.3 Network Settings

6.3.1 Configuring TCP/IP Settings

Network settings must be properly configured before you operate device over network.

Steps:

1. Click **Remote Configuration** > **Network Settings** > **TCP/IP** to enter the TCP/IP Settings interface:

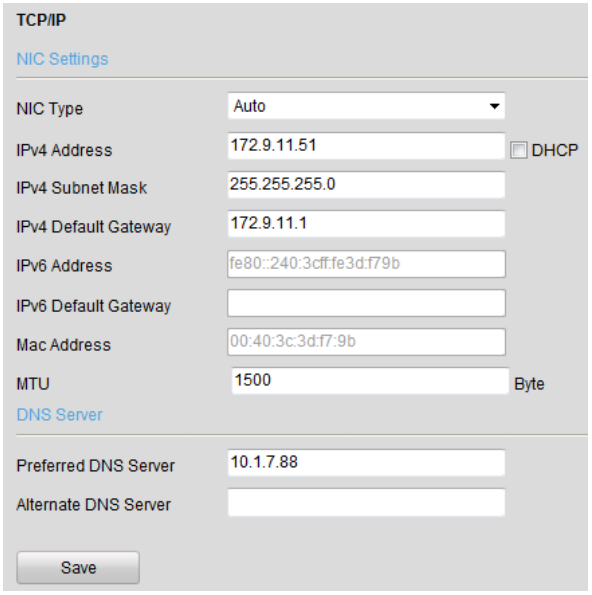


Figure 6. 8 TCP/IP Settings

2. Configure the NIC settings, including the NIC Type, IPv4 Address, IPv4 Subnet Mask, IPv4 Default Gateway, and MTU settings.

   ***Note*:** The valid value range of MTU is 500 ~ 1500.

3. If the DHCP server is available, you can click the checkbox of DHCP to automatically obtain an IP address and other network settings from that server.

4. If the DNS server settings are required for some applications (e.g., sending email), you should properly configure the Preferred DNS Server and Alternate DNS Sever here.

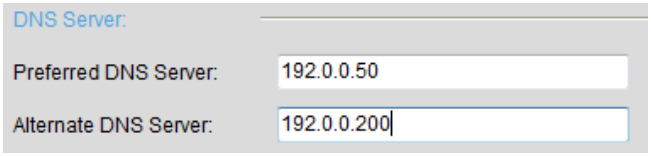


Figure 6. 9 DNS Server Settings

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

6.3.2 Configuring Port Settings

Purpose:

You can set the port No. of the encoder, e.g., HTTP port, RTSP port and HTTPS port.

Steps:

1. Click **Remote Configuration** > **Network Settings** > **Port** to enter the Port Settings interface:

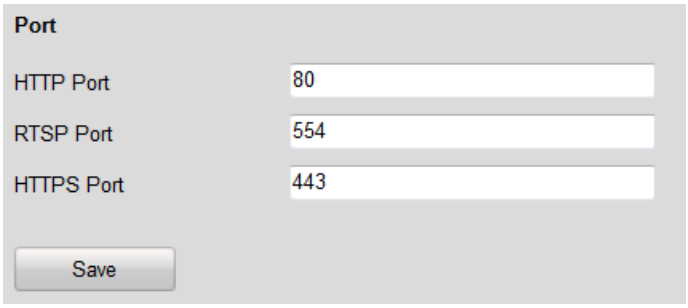


Figure 6. 10 Port Settings

2. Set the HTTP port, RTSP port and HTTPS port of the camera.

   HTTP Port: The default port number is 80.

   RTSP Port: The default port number is 554.

   HTTPS Port: The default port number is 443.

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

***Note*:** It will ask you to reboot the device to activate the settings.

6.3.3 Configuring DDNS Settings

If your device is set to use PPPoE as its default network connection, you may set Dynamic DNS (DDNS) to be used for network access.

Prior registration with your DDNS Provider is required before configuring the system to use DDNS.

Steps:

1. Click the **Remote Configuration** > **Network Settings** > **DDNS Settings** to enter the DDNS Settings interface:

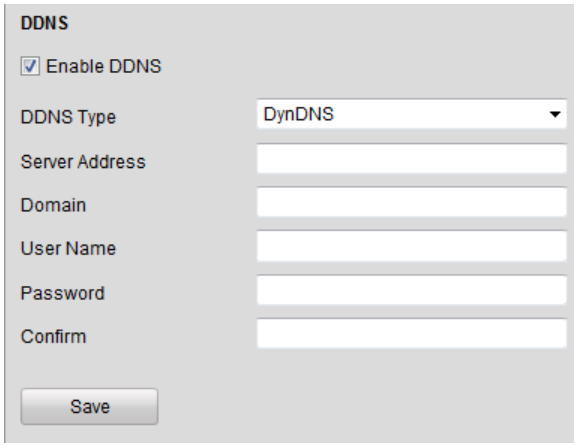


Figure 6. 11 DDNS Settings

2. Check the **Enable DDNS** checkbox to enable this feature.
3. Select **DDNS Type**. Four different DDNS types are selectable: IPServer, DynDNS, PeanutHull and HiDDNS.

- **DynDNS:**

(1) Enter **Server Address** for DynDNS (e.g., members.dyndns.org).

(2) In the **Device Domain Name** text field, enter the domain obtained from the DynDNS website.

(3) Enter the **User Name** and **Password** registered in the DynDNS website.

(4) Click **Save** to save the settings.

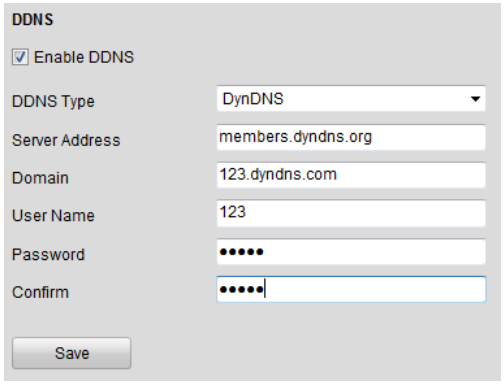


Figure 6. 12 DynDNS Settings

- **IPServer:**

(1) Enter Server Address for IPServer.

(2) Click **Save** to save the settings.

Note: For the IP Server, You have to apply a static IP, subnet mask, gateway and primary DNS from the ISP. The **Server IP** should be entered with the static IP address of the PC that runs IPServer software.

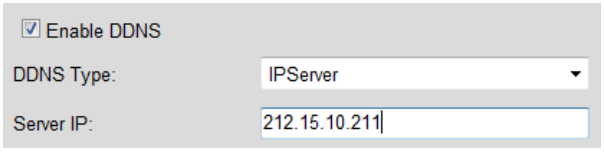


Figure 6. 13 IPServer Settings

- **PeanutHull:**

  (1) Enter User Name and Password obtained from the PeanutHull website.

  (2) Click **Save** to save the settings.

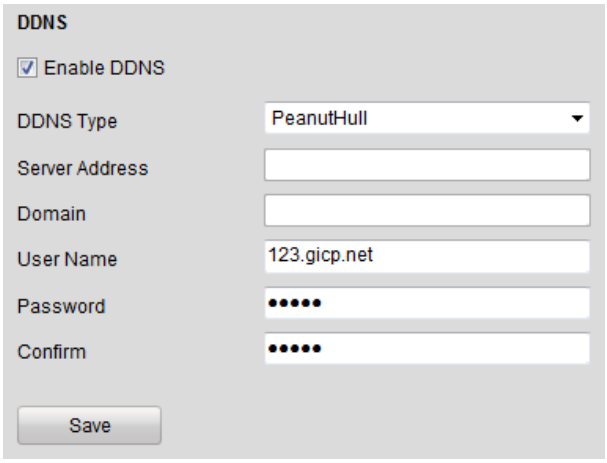


Figure 6. 14 PeanutHull Settings

- **HiDDNS:**

  (1) Enter the **Server Address** of the HiDDNS server: www.hik-online.com.

  (2) Enter the **Domain** name of the device. You can register the alias of the device domain name in the HiDDNS server first and then enter the alias to the domain name in the encoder; you can also enter the domain name directly on the encoder to create a new one.

  Note: If a new alias of the device domain name is defined in the encoder, it will replace the old one registered on the server.

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

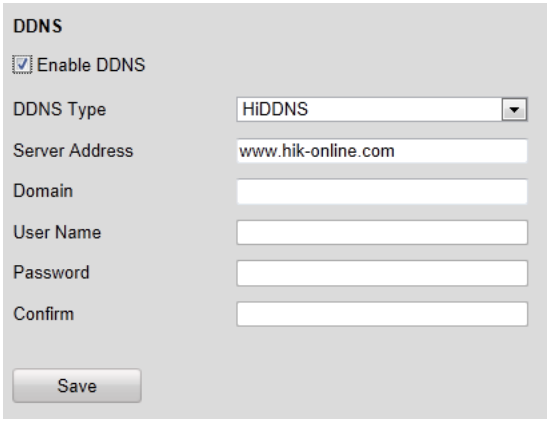


Figure 6. 15 HiDDNS Settings

6.3.4 Configuring PPPoE Settings

Your device also allows access by Point-to-Point Protocol over Ethernet (PPPoE).

Steps:

1. Click the **Remote Configuration** > **Network Settings** > **PPPoE Settings** to enter the PPPoE settings interface:

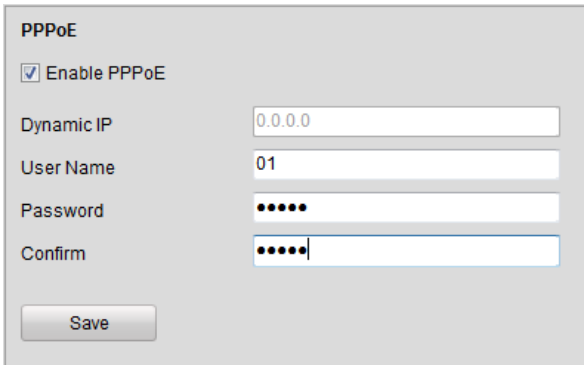


Figure 6. 16 PPPoE Settings

2. Check the **PPPoE** checkbox to enable this feature.
3. Enter **User Name**, **Password**, and **Confirm Password** for PPPoE access.

Note: The User Name and Password should be assigned by your ISP.

4. Click the **Save** button to save and exit.

6.3.5 Configuring Email Settings

Purpose:

The device can be configured to send an Email notification to all designated receivers if an alarm event is detected, e.g., motion detection event, video loss, tamper-proof, etc.

Before you start

1. Before configuring the Email settings, the device must be connected to a local area network (LAN) that maintains an SMTP mail server. The network must also be connected to either an intranet or the Internet depending on the location of the e-mail accounts to which you want to send notification.
2. Please configure the DNS Server settings under **Remote Settings>Network Settings>TCP/IP** before using the Email function.

Steps:

1. Enter the Basic Network Settings (**Remote Configuration > Network Settings > TCP/IP)** to set the IPv4 Address, IPv4 Subnet Mask, IPv4 Default Gateway and the Preferred DNS Server.
2. Click the **Remote Configuration > Network Settings > Email** to enter the Email settings interface:

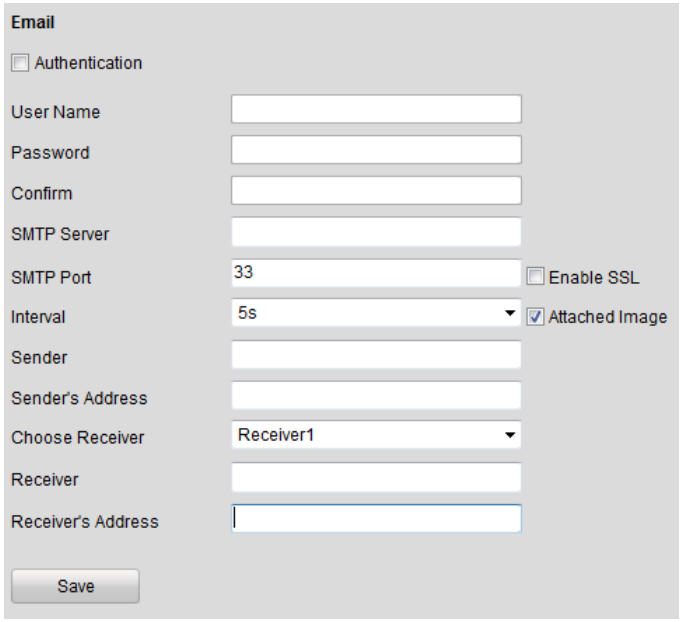


Figure 6. 17 Email Settings (1)

3. Configure the following Email settings:

Authentication (optional): If your mail server requires authentication, check this checkbox to use authentication to log in to this server and enter the login User Name and Password.

SMTP Server: The SMTP Server IP address or host name (e.g., smtp.263xmail.com).

SMTP Port: The SMTP port. The default TCP/IP port used for SMTP is 25.

- **Enable SSL**: Click the checkbox to enable SSL if required by the SMTP server. When the SSL is enabled, the default TCP/IP port used for SMTP is 465.

Interval: The interval refers to the time between two actions of sending attached pictures.

- **Attached Image**: Check the checkbox of **Attached Image** if you want to send email with attached alarm images.

Sender: The name of sender.

Sender's Address: The Email address of sender.

Choose Receiver: Select the receiver to which the Email is sent. Up to 3 receivers can be configured.

Receiver: The name of user to be notified.

Receiver's Address: The Email address of user to be notified.

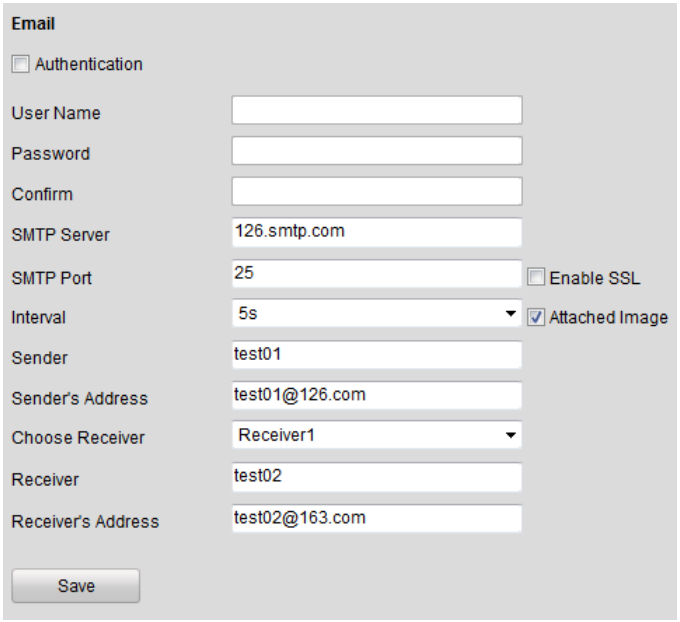


Figure 6. 18 Email Settings (2)

4. Click **Save** to save the Email settings.

Please refer to the following sections for more information:

Configure alarm linking methods with **Send Email** on *Section Configuring Motion Detection*, *Section Configuring External Alarm Input*, *Section Configuring Video Loss Alarm*, *Section Configuring Tamper-proof Alarm* and *Section Handling Exception.*

6.3.6 Adding Network Disk

For DS-6700HWI/HFI models, you must configure the network disk before operating the recording, playback or log searching. For other models with SATA disks connected, the configuration of network disk is selectable.

Before you start:

1. The network storage device is available within the network and is properly connected.
2. The network storage device is configured with NAS or IP SAN mode (please refer to the User Manual of IP SAN/NAS).

Steps:

1. Click **Remote Configuration > Network Settings >NetHDD** to enter the NetHDD settings interface.

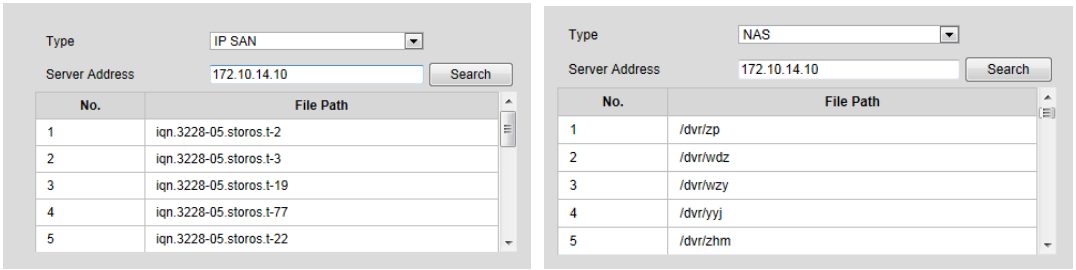


Figure 6. 19 Search Network Disk

2. You can search the available NAS/IP SAN disks in the designated storage sever by entering its IP address.
   1) Select the type to NAS or IP SAN, as shown in Figure 7.19.

2) Enter the IP address of the designated storage server.

3) Click **Search** and the available NAS or IP SAN disks in this storage server will be listed below.

3. Select and double click on the searched NAS or IP SAN disk from the list to add it, as shown in Figure 7.20. You can also manually add the NAS or IP SAN by entering the IP address of the server and file path in the text filed.

   NAS Mode: Enter the IP address of the storage device, and the default file path is */dvr/share*, in which the *share* name is user-defined during creating the DVR of the network storage.

   IP SAN mode: Enter the IP address of the storage device, and the default file path is *iqn.2004-05.storos.t-service ID*, in which the *service ID* is user-defined during creating the iSCSI volume of the network storage.

4. Click the **Save** button to add the configured network disk.

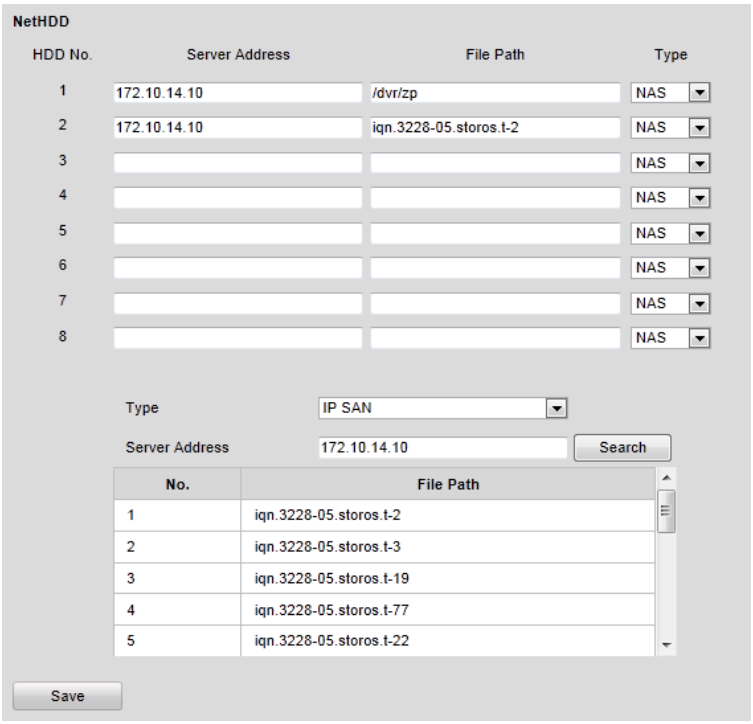


Figure 6. 20 Network Disk Settings

5. Initialize the added network disk.

   1) Click **Remote Configuration > HDD Management** to enter the HDD settings menu, on which you can view the capacity, free space, status, type and property of the added network disk.

   2) If the status of the network disk is **Uninitialized**, select the disk from the list by checking the checkbox and click the **Init** button to start initializing the disk.

   3) When the initialization is complete, the status of disk will become **Normal.**

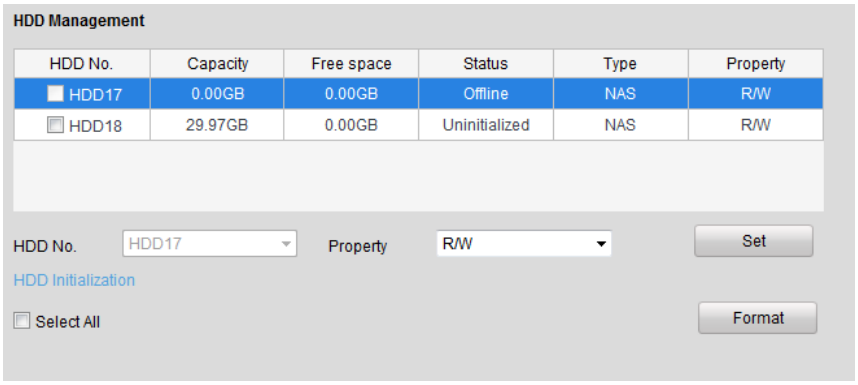


Figure 6. 21 Initial Disk

4) Set the property of the added network disk.

Select the HDD No., and select the property from the drop-down menu to R/W, Read-only or Redundancy.

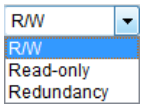


Figure 6. 22 Set HDD Property

Notes:

- Please refer to the User Manual of IP SAN/NAS for the creation of File Path in the network management.
- Up to 8 NAS disks or IP SAN disks can be connected to the DS-6700.

6.3.7 Configuring SNMP Settings

Simple Network Management Protocol (SNMP) is an Internet-standard protocol for managing devices on IP networks. You can use SNMP to get camera status, parameters and alarm related information.

Before you start:

Before setting the SNMP, please download the SNMP software and manage to receive the device information via SNMP port. By setting the Trap Address, the device can send the alarm event and exception messages to the surveillance center.

Note: The SNMP version you select should be the same as that of the SNMP software.

Steps:

1. Click **Remote Configuration > Network Settings >SNMP** to enter the SNMP settings interface.
2. Check the checkbox to enable SNMP v1 or SNMP v2c, and configure the read SNMP community (default: public), write SNMP community (default: private), tap address (default: empty) and trap port (default: 162). You can also enable both SNMP v1 and SNMP v2c.

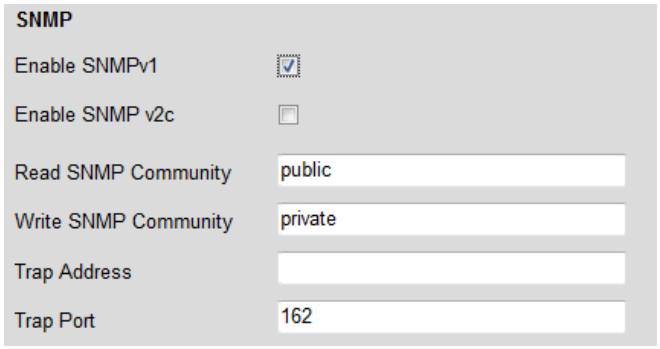


Figure 6. 23 SNMP Settings (1)

3. When the SNMPv3 is enabled, you can configure the read username (default: public).

   ***Note*:** By default settings, the SNMPv1, SNMP v2c and SNMPv3 are disabled.

4. Select the security level to "no auth, no priv", "auth, no priv", "no auth, priv" or "auth, priv".

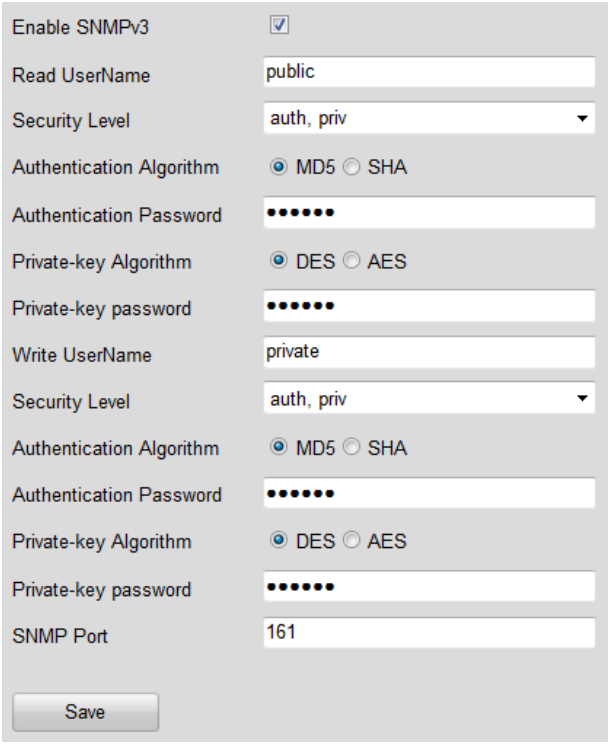


Figure 6. 24 SNMP Settings (2)

5. (1) When the security level is set to "**auth, priv"**, you can configure the Authentication Algorithm and Private-key Algorithm parameters.

   (2) When the security level is set to "**no auth, no priv**", you cannot configure the Authentication Algorithm and Private-key Algorithm parameters.

6. Set the SNMP port (default: 161).
7. Click **Save** to save the above settings.

7.3.8 Configuring QoS Settings

Purpose:

QoS (Quality of Service) can help solve the network delay and network congestion by configuring the priority of data sending. The use of a QoS-aware network can prioritize traffic and thus allow critical flows to be served before flows with lesser priority.

The encoder can mark the data packets for video/audio, event/alarm and management network traffics with different DSCP values which identify different priority levels of data sending.

Steps:

1. Click **Remote Configuration > Network Settings > QoS** to enter the QoS settings interface:

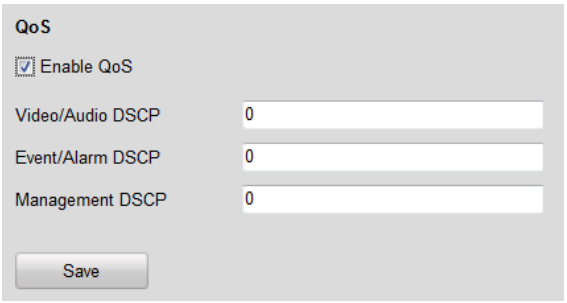


Figure 6. 25 QoS Settings

2. Check the checkbox to enable the QoS function.
3. Enter the DSCP (Differentiated Services Codepoint) value for the video/audio, event/alarm and management traffic. This value is used to mark the traffic's IP header. The DSCP value defines the priority level for the specified type of traffic, for example, how much bandwidth to reserve for it.

   The valid value range of the DSCP is 0-63. The higher DSCP value indicates higher priority level.
4. Click **Save** to save the settings.

Note: It will ask you to reboot the device to activate the settings.

7.3.9 Configuring FTP Settings

Purpose:

The captured pictures can be uploaded to FTP server.

Steps:

1. Click **Remote Configuration > Network Settings > FTP** to enter the FTP Settings interface:

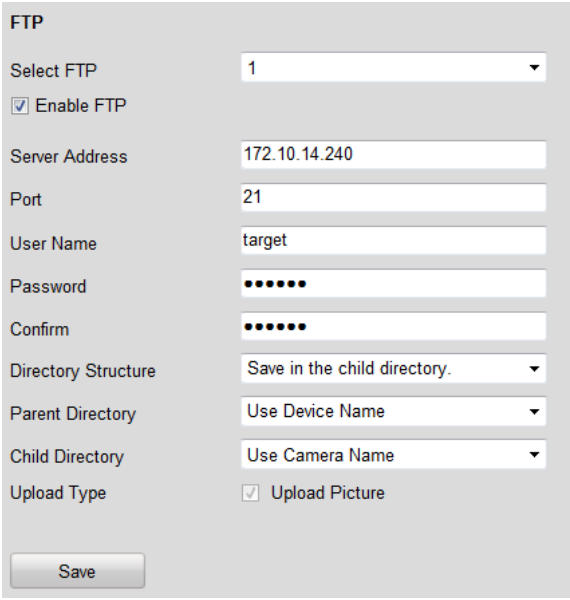


Figure 6. 26 FTP Settings

2. Check the checkbox of **Enable FTP**.
3. Configure the FTP settings, including server address, port, user name, password, directory and upload type.

   Directory: In the **Directory Structure** field, you can select the root directory, parent directory and child directory. When the parent directory is selected, you have the option to use the Device Name, Device Number or Device IP for the name of the directory; and when the Child Directory is selected, you can use the Camera Name or Camera No. as the name of the directory.

   Upload type: To enable uploading the captured picture to the FTP server.
4. Click **Save** to save the settings.

   Note: If you want to upload the captured pictures to FTP server, you have to enable the event-triggered snapshot on **Snapshot** page. For detailed information, please refer to *Section 8.3*.

7.3.10 Configuring SOCKS Settings

Purpose:

SOCKet Secure (SOCKS) is an Internet protocol that routes network packets between a client and server through a proxy server. This feature is useful if the encoder is located on a local network behind a firewall, and Email notifications, FTP uploads, alarms, and such need to be sent to a destination outside the local network (such as the Internet). The SOCKS4 and SOCKS5 are supported, of which the SOCKS5 additionally provides authentication so only authorized users may access a server.

Steps:

1. Click **Remote Configuration > Network Settings > SOCKS** to enter the SOCKS Settings interface:

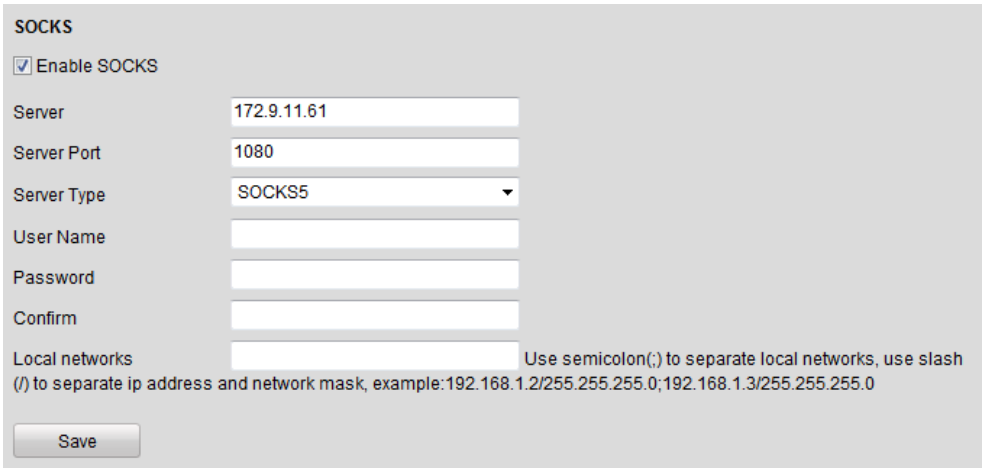


Figure 6. 27 SOCKS Settings

2. Configure the following settings:

   Server: Enter the address of the SOCKS server.

   Server Port: Enter the port of the SOCKS server (default: 1080).

   Server Type: Select the server type to SOCKS4 or SOCKS5. When you select SOCKS5, you can enable the user authentication on the server and then enter the login user name and password here.

   Local networks: Define the local network segment which does not need to use SOCKS proxy server. You can enter multiple network addresses and use the semicolon (;) to separate them, e.g., 10.0.0.0/255.0.0.0; 172.16.0.0/255.240.0.0.

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

7.3.11 Configuring UPnP™ Settings

Purpose:

UPnP™ can permit the device seamlessly discover the presence of other network devices on the network and establish functional network services for data sharing, communications, etc. If you want to use the UPnP™ function to enable the fast connection of the device to the WAN via a router, you should configure the UPnP™ parameters of the device.

Before you start:

If you want to enable the UPnP™ function of the device, you must enable the UPnP™ function of the router to which your device is connected. When the network working mode of the device is set as multi-address, the Default Route of the device should be in the same network segment as that of the LAN IP address of the router.

Steps:

1. Click **Remote Configuration > Network Settings > NAT** to enter the NAT settings interface.
2. Check the checkbox to enable the UPnP™ function.
3. Select the Port Mapping Mode to Auto or Manual.

   When you select **Auto**, the mapping ports can be automatically assigned by the router.

   When you select **Manual**, you should continue Step4 to edit the mapping ports.

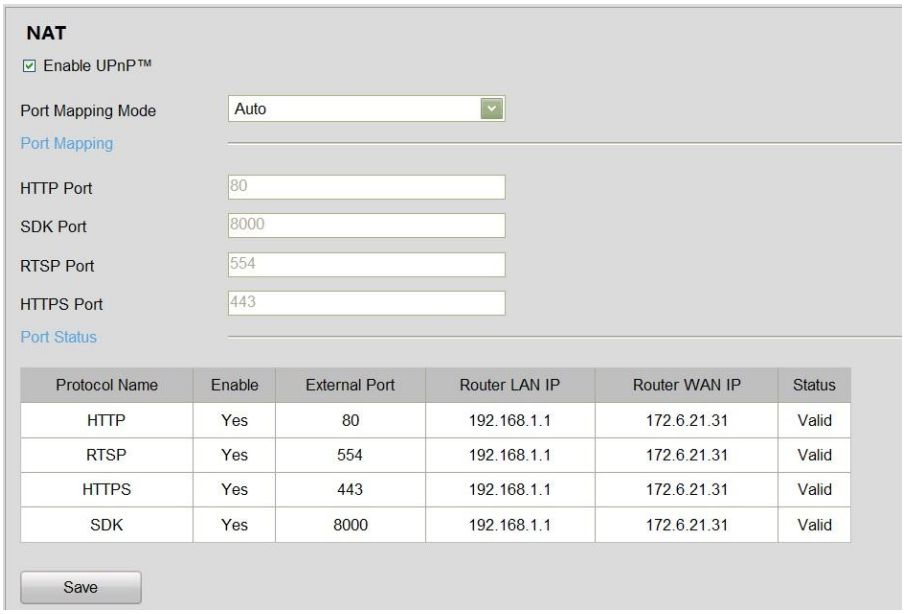


Figure 6. 28 UPnP™ Settings-Auto

4. Configure the HTTP Port (for access by WEB browser), SDK Port Mapping (for access by client software), RTSP Port and HTTPS Port respectively.

   Notes:

   1) You can use the default port No., or change it according to actual requirements.
   2) The Ports indicate the port No. for mapping in the router.

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

   After port mapping is successful, you can view the status of the port mapping on the Port Status area.

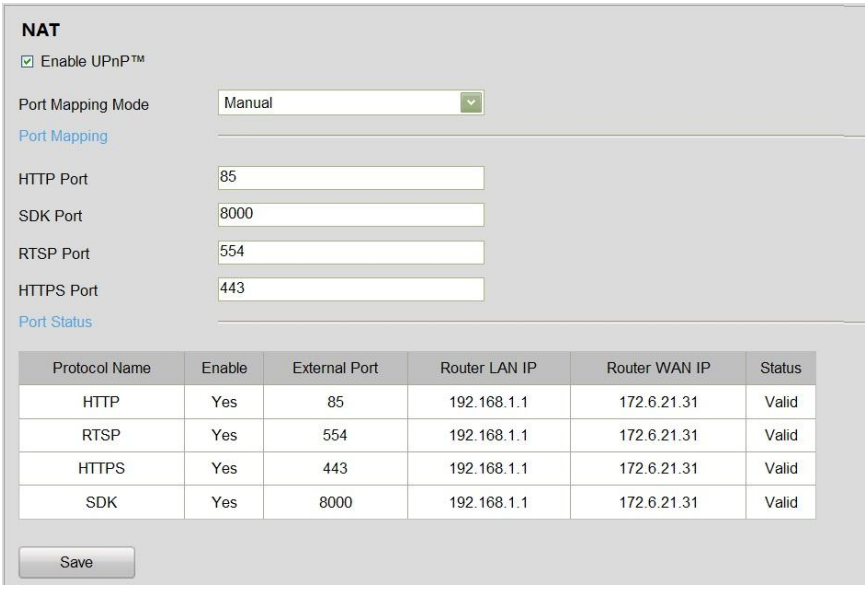


Figure 6. 29 UPnP™ Settings-Manual

7.3.12 Configuring HTTPS Settings

Purpose:

HTTPS (Hyper Text Transfer Protocol Secure) ensures the data transferred is encrypted using Secure Socket Layer (SSL) or Transport Layer Security (TLS). HTTPS provides authentication of the web site and associated web server that one is communicating with and create a secure channel over an insecure network.

HTTPS URLs begin with "https://" and use port 443 by default.

Steps:

1. Click **Remote Configuration > Network Settings > HTTPS** to enter the HTTPS settings interface.
2. Create the self-signed certificate or authorized certificate.

Figure 6. 30 HTTPS Settings

Task1: Create the self-signed certificate

(1) Click the **Create** button to create the following dialog box.

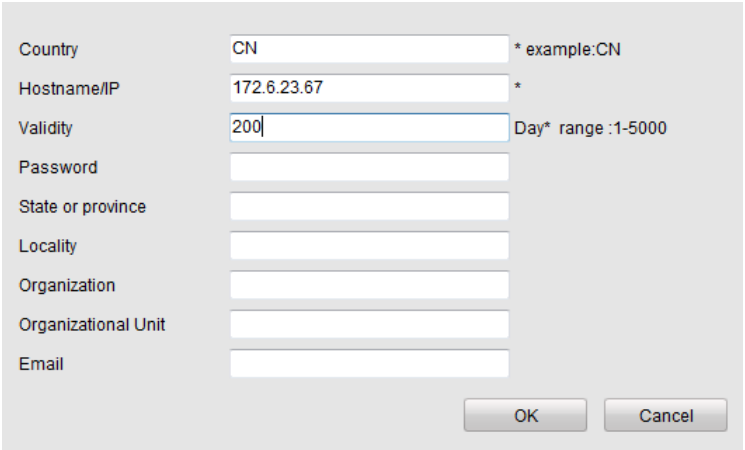


Figure 6. 31 Create Self-signed Certificate

(2) Enter the country, host name/IP, validity and other information.

(3) Click **OK** to save the settings.

Task2: Create the authorized certificate

(1) Click the **Create** button to create the certificate request.

(2) Download the certificate request and submit it to the trusted certificate authority for signature.

(3) After receiving the signed valid certificate, import the certificate to the device.

3. When you have successfully created and installed the certificate, check the checkbox to enable the HTTPS function.

Note:

After the HTTPS feature is enabled, the system will use the HTTPS login mode by default when you input the IP address (e.g., https://192.0.0.64). You can also input http://IP address/index.asp (e.g., http://192.0.0.64/index.asp) if you want to use HTTP mode to log into the device.

7.3.13 Configuring Bonjour Settings

Purpose:

Bonjour is enabled by default, and the video encoder can be automatically detected by operating systems and clients that support this protocol.

Before you start:

Make sure you have installed the Bonjour plug-in on your PC before enabling the Bonjour function.

Steps:

1. Click **Remote Configuration > Network Settings > Bonjour** to enter the Bonjour settings interface.

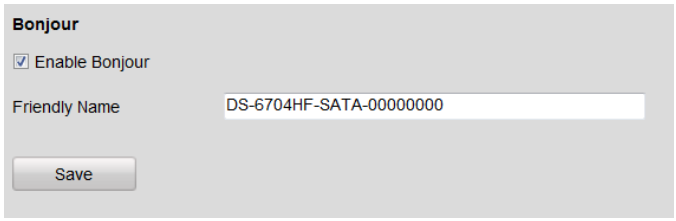


Figure 6. 32 Bonjour Settings

2. Check the checkbox to enable the Bonjour function.
3. Edit the name of device. The name is shown when the device is detected by the system.
   Note: Only the letters, numbers and "-" can be contained in the name.
4. Click **Save** to save the settings.

7.3.14 Configuring IP Address Filter

Purpose:

You can allow or forbid access by specified IP addresses to the encoder by enabling IP Address Filter**.**

Up to 256 IP address can be added to the list (allowed/forbidden) by Web Browser.

Steps:

1. Click **Remote Configuration > Network Settings > IP Address Filter** to enter the IP address filter settings interface.

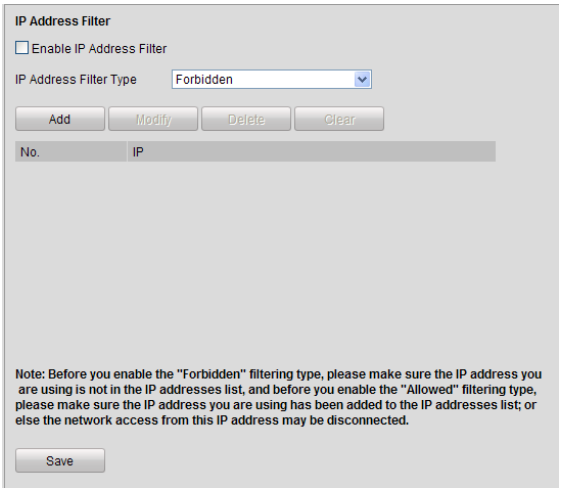


Figure 6. 33 IP Address Filter Settings

2. Check the checkbox of **Enable IP Address Filter**.
3. Select the filter type of IP address to **Allowed** or **Forbidden**.
4. Click the **Add** button to add the IP address to be allowed or forbidden.

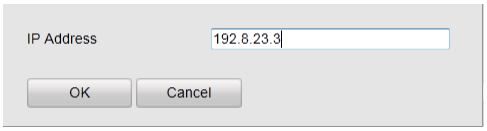


Figure 6. 34 Add IP Address

5. Click the **Add** button to add the IP address to be allowed or forbidden.

   Note: Up to 256 IP address can be added to the list (allowed/forbidden) by Web Browser.
6. Click **Save** to save the settings.

7.3.15 Configuring Multicast Address

Purpose:

The multicast address can be configured to realize live view for more than the maximum number of cameras through network.

A multicast address spans the Class-D IP range of 224.0.0.0 to 239.255.255.255. It is recommended to use the IP address ranging from 239.252.0.0 to 239.255.255.255.

Steps:

1. Click **Remote Configuration** > **Network Settings** > **Advanced** to enter the multicast address settings interface.

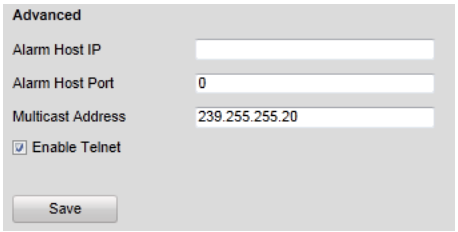


Figure 6. 35 Multicast Address Settings

2. Enter the multicast address in the text filed.

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

Note: The device will reboot automatically to activate the multicast address settings.

7.3.16 Configuring Remote Alarm Host

Purpose:

With a remote alarm host configured, the device will send the alarm event or exception message to the host when an alarm is triggered. The remote alarm host must have the CMS (Client Management System) software installed.

Steps:

1. Click **Remote Configuration > Network Settings > Advanced** to enter the alarm host settings interface.

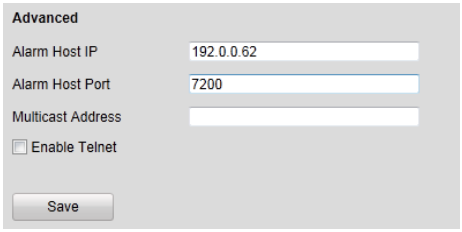


Figure 6. 36 Multicast Address Settings

2. Enter **Alarm Host IP** and **Alarm Host Port** in the text fields.

   The **Alarm Host IP** refers to the IP address of the remote PC on which the CMS (Client Management System) software (e.g., iVMS-4200) is installed, and the **Alarm Host Port** must be the same as the alarm monitoring port configured in the software (default port is 7200).

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

7.3.17 Configuring IEEE 802.1X

Purpose:

The IEEE 802.1X standard is supported by the network cameras, and when the feature is enabled, the camera data is secured and user authentication is needed when connecting the camera to the network protected by the IEEE 802.1X.

Before you start:

The authentication server must be configured. Please apply and register a user name and password for 802.1X in the server.

Steps:

1. Enter the 802.1X Settings interface:

   Configuration > Advanced Configuration > Network > 802.1X

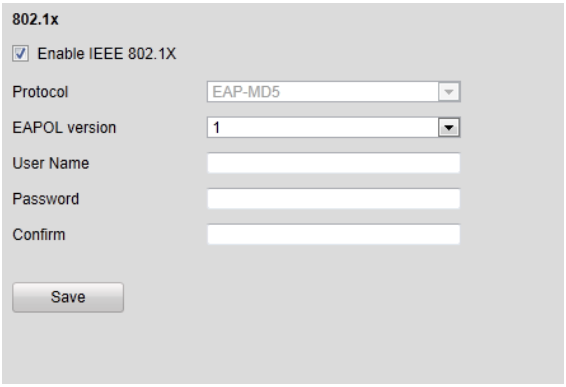


Figure 6. 37 IEEE 802.1X Settings

2. Check the **Enable IEEE 802.1X** checkbox to enable the feature.
3. Configure the 802.1X settings, including EAPOL version, user name and password.

   Note: The EAPOL version must be identical with that of the router or the switch.
4. Enter the user name and password to access the server.
5. Click **Save** to finish the settings.

Chapter 7 Camera Settings

7.1 Configuring OSD Settings

7.1.1 Configuring Display Settings

Purpose:

You can customize the camera name and time on the screen.

Steps:

1. Click the **Remote Configuration >Camera Settings > Display Settings** to enter the Display Settings interface:

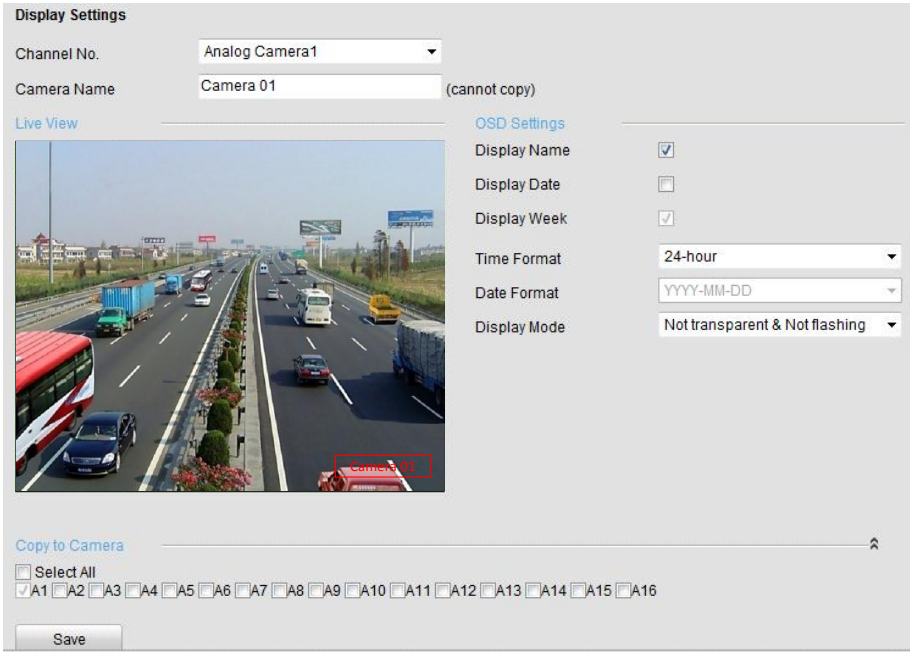


Figure 7. 1 Display Settings

2. Select the camera from the drop-down list.
3. Edit the camera name in the text field of Camera Name.

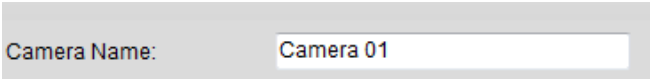


Figure 7. 2 Edit Camera Name

4. Select the display of camera name, date or week by checking the checkboxes if required.
5. Set the time format, date format and OSD display mode by selecting option from the drop-down list.
6. On the preview image, you can adjust the OSD location on the screen by moving the text frame.

Figure 7. 3 Adjust OSD Location

7. If you want to copy the display settings of the current camera to other cameras, spread the **Copy to Camera** panel and select the camera(s) to copy, or click **Select All** to select all cameras.

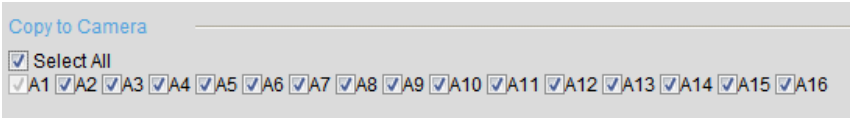


Figure 7. 4 Copy to Camera

8. Click **Save** to validate the above settings.

7.1.2 Configuring Text Overlay

Steps:

1. Click the **Remote Configuration >Camera Settings > Text Overlay Settings** to enter the Text Overlay Settings interface.
2. Select the camera from the drop-down list.
3. Edit the user-defined text content.
   Click the checkbox in the text box below and then input the characters. Up to 8 character strings can be edited.
4. Click **Save**, and the edited text is shown on the image.
5. On the preview image, you can adjust the Text location on the screen by moving the text frame.

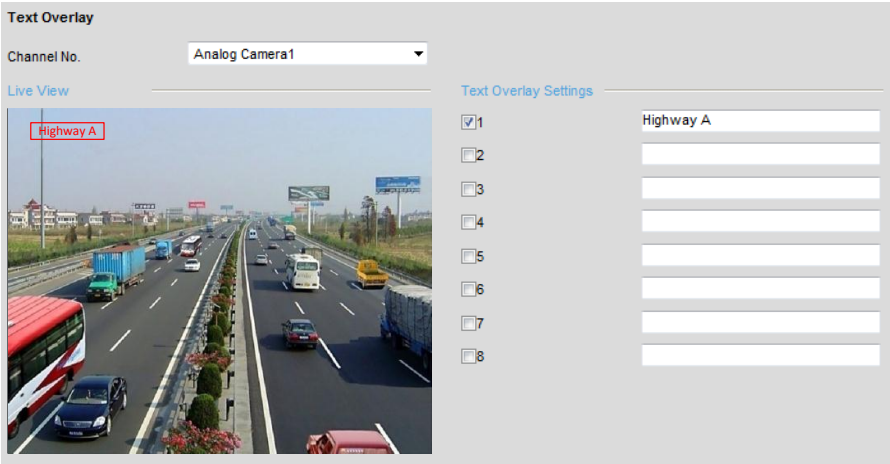


Figure 7. 5 Text Overlay Settings

6. If you want to copy the text overlay settings of the current camera to other cameras, spread the **Copy to Camera** panel and select the camera(s) to copy, or click **Select All** to select all cameras.

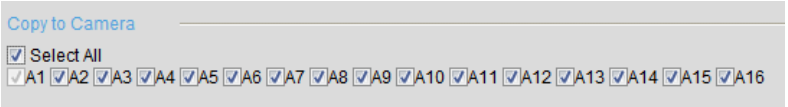


Figure 7. 6 Text Overlay Settings

7. Click **Save** to activate the above settings.

7.2 Configuring Video Settings

Steps:

1. Click **Remote Configuration** > **Camera Settings** >**Video Settings** to enter the Video Settings interface.

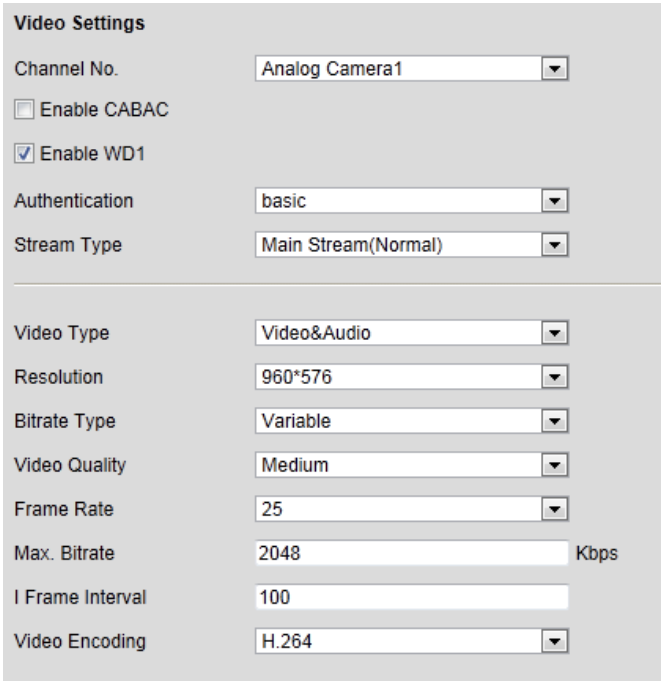


Figure 7. 7 Video Settings

2. Select the camera from the drop-down list to configure.
3. Enable the **CABAC** if required and configure the settings.
   When the CABAC is enabled, the recorded file will occupy less disk space or bandwidth without reducing the image quality, however, the higher decoding resource will be required.
4. For DS-6700HWI and DS-6700HWI-SATA series, you can enable WD1 on demand by checking the checkbox.
5. Enable the RTSP authentication by selecting the **Authentication** to basic, or disable it.
6. Select the **Stream Type** of the camera to Main Stream (Normal), Main Stream (Event) or Sub Stream.
   The main stream is usually for recording and live viewing with good bandwidth, and the sub stream can be used for live viewing when the bandwidth is low. Refer to the *Chapter Local Configuration* on changing the main stream to sub stream for live viewing.
7. You can customize the following parameters for the selected Main Stream or Sub Stream:
   Video Type: Select the video type to video stream, or video & audio composite stream. The audio signal will be recorded only when the **Video Type** is **Video & Audio**.
   Resolution: Select the resolution of the video input. For DS-6700HWI and DS-6700HWI-SATA series, the resolution of 960*576 is selectable when the WD1 is enabled.
   Bitrate Type: Select the bitrate type to constant or variable.
   Video Quality: When bitrate type is selected to **Variable**, 6 levels of video quality can be configured.
   Frame Rate: Set the frame rate to 1~30 fps.
   The frame rate used to describe the frequency at which a video stream is updated is measured in frames per

second (fps). A higher frame rate is advantageous when there is movement in the video stream, as it maintains image quality throughout.

Max. Bitrate: Set the Max. bitrate to 32~8192 Kbps.

I Frame Interval: Set the I frame interval to 1~ 400 (frames). The higher value results in lower video quality.

Video Encoding: Select the video encoding standard to H.264, MPEG2, MPEG4 or MJPEG.

Note: When the MJPEG video encoding standard is selected, the frame rate can be set to 1~15fps and the max. bitrate is not configurable.

8. If you want to copy the display settings of the current camera to other cameras, spread the **Copy to Camera** panel and select the camera(s) to copy, or click **Select All** to select all cameras.

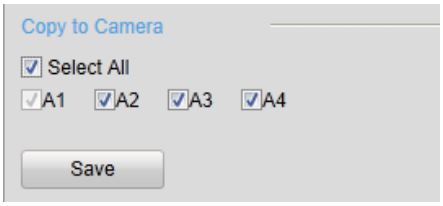


Figure 7. 8 Copy to Camera

9. Click **Save** to save the above settings.

7.3 Configuring Snapshot Settings

Purpose:

You can configure the scheduled snapshot and event-triggered snapshot. The captured picture can be stored in the HDD, SD card (if supported) or the netHDD. You can also upload the event-triggered snapshots to a FTP server.

Steps:

1. Click **Remote Configuration > Camera Settings > Snapshot** to enter the Snapshot settings interface:

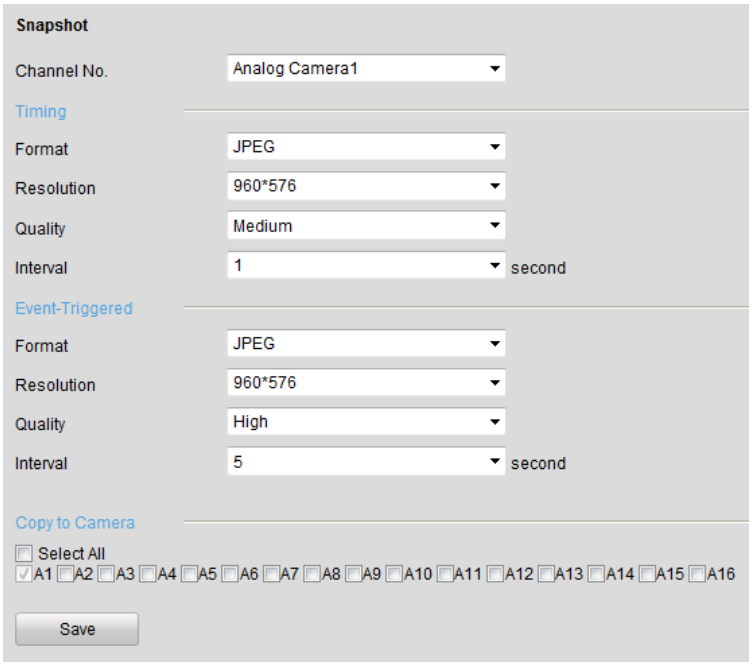
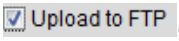


Figure 7. 9 Snapshot Settings

2. Select the channel No. from which the pictures to be captured.
3. Configure the timing snapshot and the event-triggered snapshot parameters, including the format, resolution, quality and the interval between two snapshots.
4. Select the channel (s) you want to copy the same settings if needed.
5. Click **Save** to save the settings.

Notes:

1. The timing snapshots are stored in HDD, SD card (if supported) or netHDD. The event-triggered snapshots can be uploaded to FTP.
2. You should check the 

checkbox in Motion Detection Settings or Alarm Input interface. Please refer to *Step 3* in *Section Configuring* ***Motion Detection*** *or Step 4* in *Section Configuring* ***External Alarm Input***.
3. Please refer to *Section 7.3.9* ***Configuring FTP Settings*** for more details to configure FTP parameters.

7.4 Configuring and Handling Alarms

Purpose:

This section explains how to configure the network camera to respond to alarm events, including Motion Detection, External Alarm Input, Video Loss, Tamper-proof and Exception. And the alarm events can trigger the alarm actions, such as Notify Surveillance Center, Send Email and Trigger Alarm Output.

7.4.3 Configuring Motion Detection

Motion detection is a feature which can alert the personnel and record the video for the motion occurred in the surveillance scene.

Steps:

1. **Set the Motion Detection Area**

   Steps:

   (1) Click **Remote Configuration> Camera Settings> Motion Detection** to enter the motion detection settings interface.

   (2) Select the camera to configure the motion detection.

   (3) Check the checkbox of **Enable Motion Detection**.

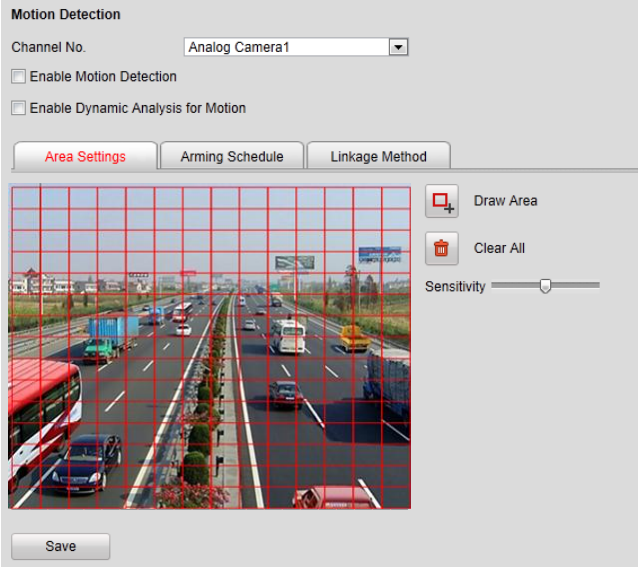
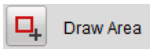


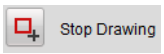
Figure 7. 10 Motion Detection Settings

(4) You can check the checkbox of **Enable Dynamic Analysis for Motion**. When this feature is enabled, the motion detection triggered frame (green) for the moving targets in the motion detection area will be displayed on the live video.

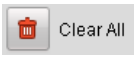
(5) Click the 

button. Draw motion detection area by clicking and dragging the mouse in the live video image.

Note: By default, the full screen motion detection is configured.

(6) Click the 

button to finish drawing.

You can click the 

button to clear all areas.

(7) Move the slide bar 

to set the sensitivity of the camera.

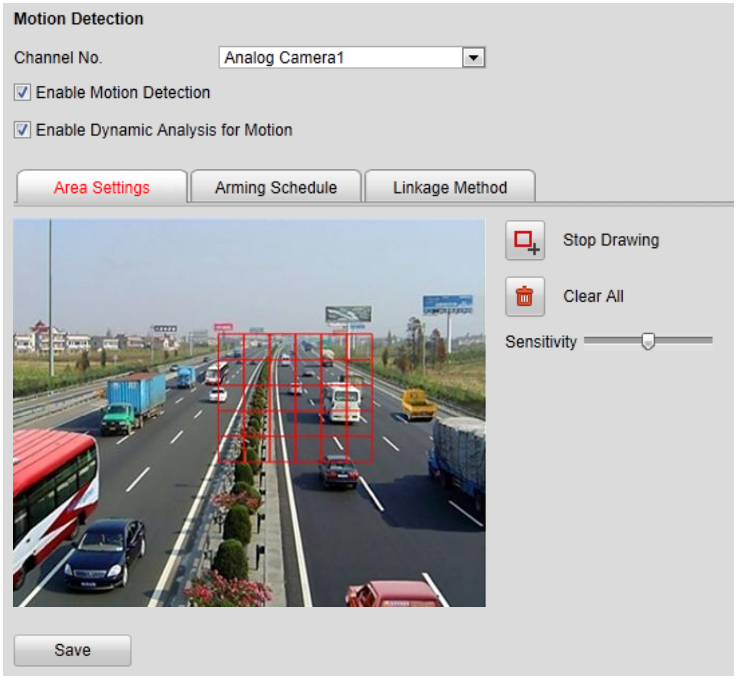


Figure 7. 11 Motion Detection-Area Settings

(8) Click **Save** button to save the settings.

2. **Set the Arming Schedule for Motion Detection**

Steps:

(1) Click the **Arming Time** tab.

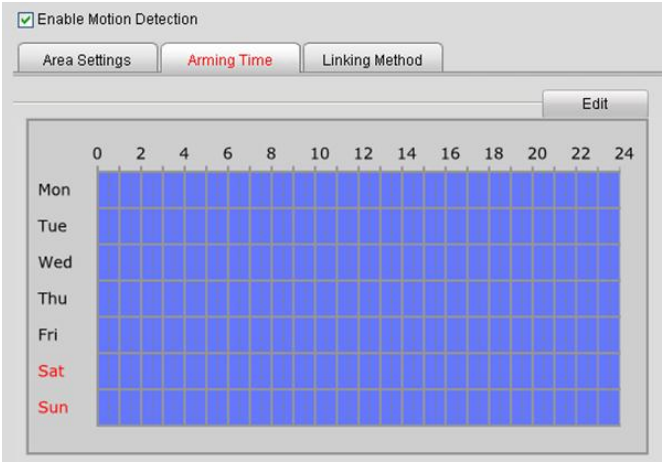


Figure 7. 12 Motion Detection-Arming Time Settings

(2) Click the **Edit** button to edit the arming schedule.

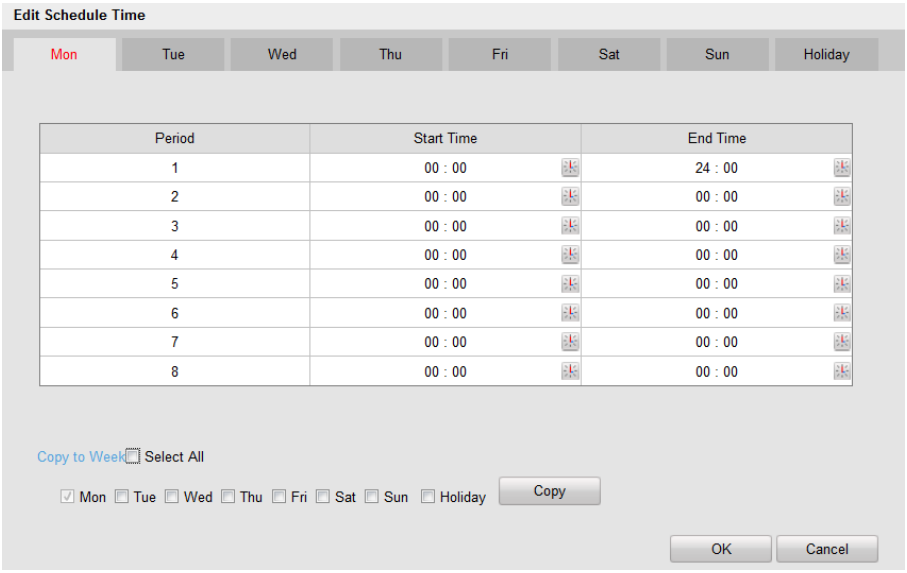


Figure 7. 13 Motion Detection-Edit Arming Schedule

Notes:

1. The time of each segment can't be overlapped. Up to 8 segments can be configured for each day.
2. The **Holiday** option is available in the Schedule dropdown list when you have enabled holiday schedule in **Holiday settings**.

(3) Choose the day you want to set the arming schedule.

(4) Click the button to set the time period for the arming schedule.

(5) After you set the arming schedule, you can copy the schedule to other days.(Optional)

(6) Click **OK** button to save the settings.

3. **Set the Alarm Actions Taken for Motion Detection**

Purpose:

You can specify the alarm type when an event is triggered.

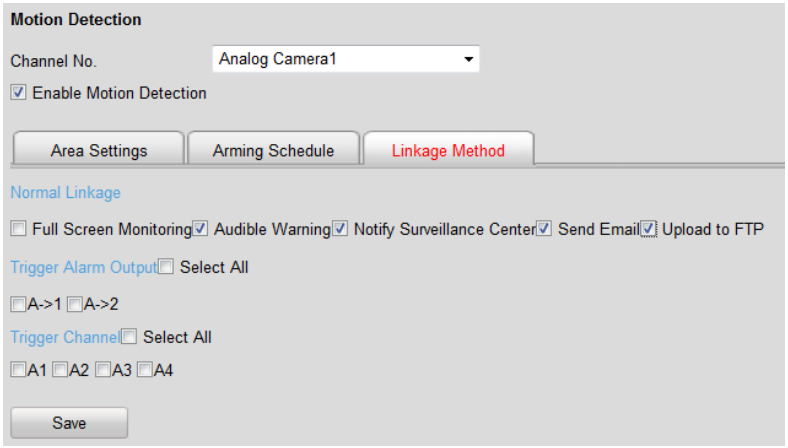


Figure 7. 14 Motion Detection-Linking Method

Steps:

(1) Click the **Linkage Method** tab to enter the setting interface.

(2) Select the alarming linkage method(s) including Audible Warning, Notify Surveillance Center, Send Email and Upload to FTP.

- **Audible Warning**

Trigger an audible beep when an alarm is detected.

Note: The DS-6701/6704HWI and DS-6701/6704HFI models provide no audio beep.

- **Notify Surveillance Center**

Send an exception or alarm signal to remote alarm host when an event occurs. The alarm host refers to the PC installed with Remote Client.

- **Send Email**

Send an email with alarm information to a user or users when an event occurs.

Note: To send the Email when an event occurs, you need to go to the network setting interface to set the related parameters. Refer to *SectionConfiguring Email Settings*.

- **Upload to FTP**

Capture the image when an alarm is triggered and upload the picture to a FTP server.

(3) Select the channel you want to trigger an external alarm output when a motion detection event occurs.

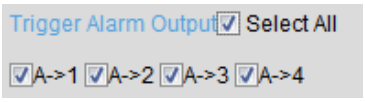


Figure 7. 15 Motion Detection-Trigger Alarm Output

Note: To trigger an external alarm output when an event occurs, you need to go to the Alarm Output Settings interface to set the related parameters.

1) Click **Remote Configuration**> **Alarm Settings**> **Alarm Output** to enter the Alarm Output Settings interface.

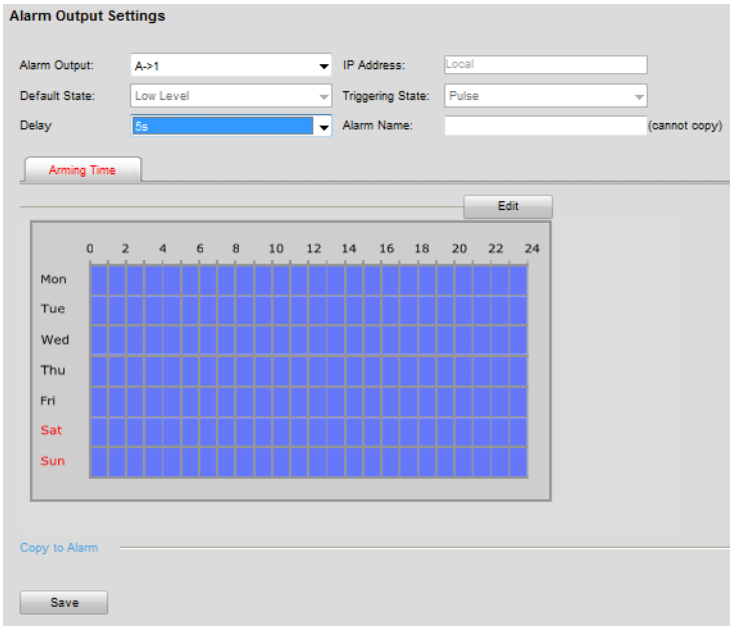


Figure 7. 16 Motion Detection-Alarm Output Settings

2) Select one alarm output channel in the **Alarm Output** drop-down list.

3) The D**elay** time can be set to **5sec**, **10sec**, **30sec**, **1min**, **2min**, **5min, 10min** or **Manual**. The **Delay** refers to the time duration that the alarm output remains in effect after alarm occurs.

Note: If you choose **Manual**, you need to manually disable the alarm output.

4) Click **Edit** to enter the **Edit Schedule Time** interface. The time schedule configuration is the same as the Setting of the Arming Schedule for Motion Detection. Refer to *Step 2* ***Set the Arming Schedule for Motion Detection*** in *Section Configuring Motion Detection.*

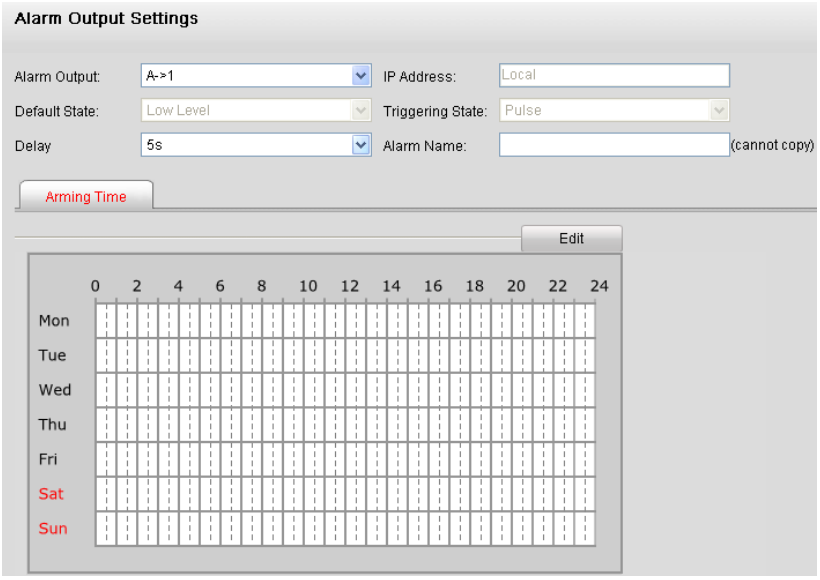


Figure 7. 17 Motion Detection-Alarm Output Settings

5) Return to the Alarm Output Settings interface and click **Save** to save the settings.

(4) Select the channel you want to trigger recording when a motion detection event occurs.

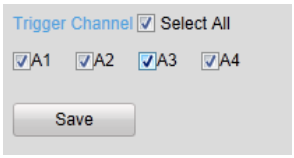


Figure 7. 18 Motion Detection-Alarm Linked Recording

(5) Click **Save** to save the settings of linking method motion detection.

7.4.4 Configuring External Alarm Input

Steps:

1. Click **Remote Configuration> Alarm Settings> Alarm Input** to enter the Alarm Settings interface.
2. Choose the alarm input number and the Alarm Type. The alarm type can be NO (Normally Open) and NC (Normally Closed).

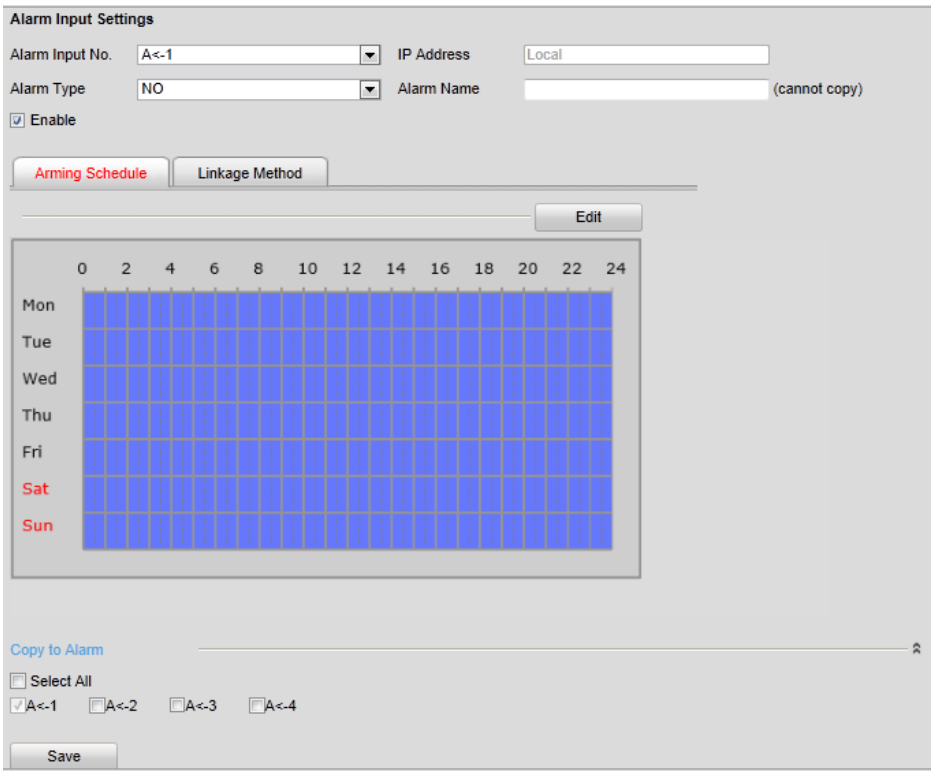


Figure 7. 19 Alarm Input Settings-Arming Time

3. Check the checkbox of **Enable** to enable the alarm input.
4. Set the arming schedule for the alarm input. Refer to *Step 2* ***Set the Arming Schedule for Motion Detection*** in *Section Configuring Motion Detection*.
5. Click the **Linkage Metho**d tab to set the actions taken for the alarm input. Refer to *Step 3* ***Set the Alarm Actions Taken for Motion Detection*** in *Section Configuring Motion Detection*.

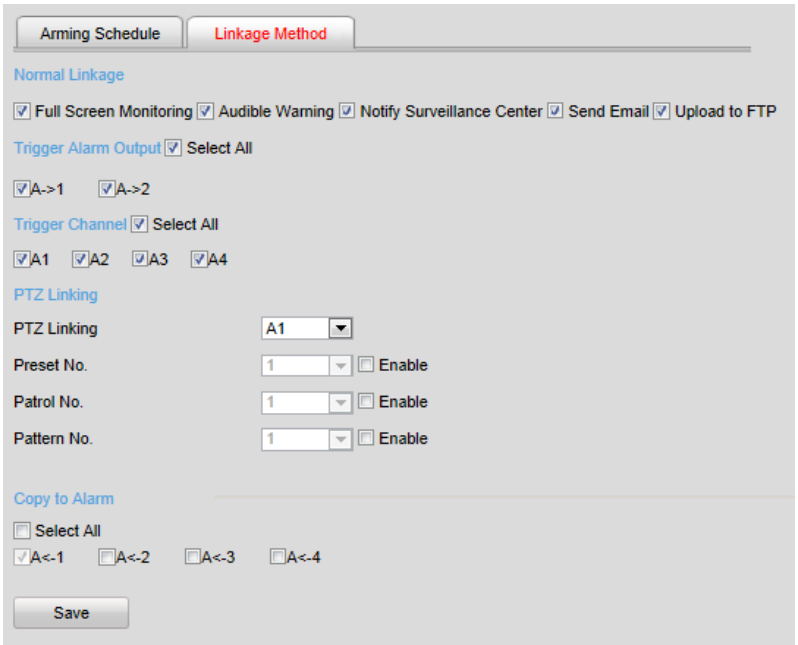


Figure 7. 20 Alarm Input Settings-Linking Method

6. You can also choose the PTZ linking for the alarm input if your camera is installed with a pan/tilt unit.
   (1) Choose the PTZ Linking channel.
   (2) Check the relative checkbox to enable Preset Calling, Patrol Calling or Pattern Calling.
7. You can copy your settings to other alarm inputs.
8. Click **Save** to save the settings.

7.4.5 Configuring Video Loss Alarm

Steps:

1. Click **Remote Configuration> Camera Settings> Video Loss** to enter the video loss alarm setting interface.

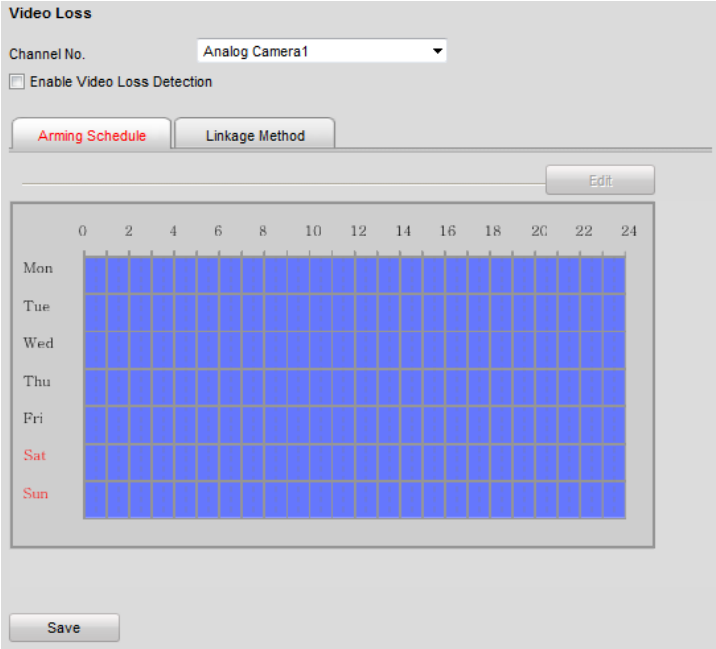


Figure 7. 21 Video Loss Alarm Settings

2. Select the camera to configure the video loss alarm.
3. Check the checkbox of **Enable Video Loss**.
4. Click **Edit** to edit the arming schedule for video loss detection. The arming schedule configuration is the same as the Setting of the Arming Schedule for Motion Detection. Please refer to *Step 2* **Set the Arming Schedule for Motion Detection** in *Section Configuring Motion Detection*.
5. Click the **Linkage Method** tab to set the actions taken for the video loss alarm. Please refer to *Step 3* **Set the Alarm Actions Taken for Motion Detection** in *Section Configuring Motion Detection*.

7.4.6 Configuring Tamper-proof Alarm

Purpose:

If you enable this function, an alarm will be triggered when the image of camera is tampered with.

Steps:

1. Click **Remote Configuration> Camera Settings> Tamper-proof** to enter the Tamper-proof Settings

interface.

2. Select the camera to configure the tamper-proof detection alarm.

Figure 7. 22 Tamper-proof Alarm Settings

3. Click checkbox of **Enable Tamper-proof**.

4. Set the tamper-Proof area. Please refer to *Step 1 Set the Motion Detection Area* in *Chapter 8.3.1*.

5. Click **Edit** to edit the arming schedule for tamper-proof. The arming schedule configuration is the same as the Setting of the Arming Schedule for Motion Detection. Please refer to *Step 2 Set the Arming Schedule for Motion Detection* in *Section Configuring Motion Detection.*

6. Click the **Linkage Method** tab to set the actions taken for the tamper-proof alarm. Please refer to *Step 3* **Set the Alarm Actions Taken for Motion Detection** in *Section Configuring Motion Detection*.

7.4.7 Handling Exception

The exception type can be HDD full, HDD error, network disconnected, IP address conflict, illegal access, video standard mismatch, video signal exception, record/capture exception and video resolution mismatch.

Note: When the selected resolution under **Remote Configuration > Camera Settings >Video Settings** and the actual video input resolution are mismatched, the exception alarm will occur. Please refer to *Section Configuring Video Settings.*

Steps:

1. Click **Remote Configuration> Exception** to enter the Exception Settings interface.

2. Check the checkbox to set the actions taken for the Exception alarm. Please refer to *Step 3* ***Set the Alarm Actions Taken for Motion Detection*** in *Section Configuring Motion Detection*.

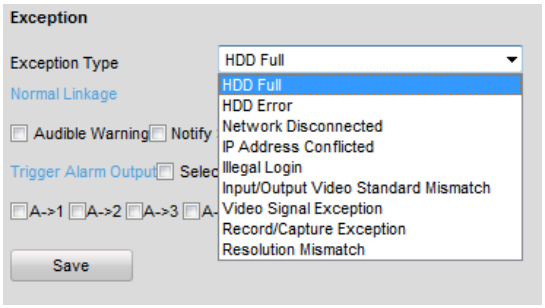


Figure 7. 23 Handling Exceptions

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

7.5 Configuring Privacy Mask

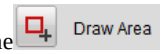
Purpose:

Privacy Mask enables you to cover certain areas on the video of the channel to prevent your privacy from live viewing and recording.

Steps:

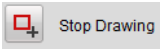
1. Click **Configuration>Remote Configuration>Camera Settings>Privacy Mask** to enter the privacy mask settings interface.
2. Select the camera to configure privacy mask.
3. Check the checkbox of **Enable Privacy Mask** to enable this function.

Figure 7. 24 Privacy Mask Settings

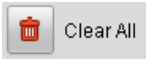
4. Click the 

button.
5. Draw the mask area by clicking and dragging the mouse in the live video image.

Note: Up to 4 privacy mask areas can be configured.

6. When finishing the area setting, click the 

button to finish drawing.

   You can click the 

button to clear all of the areas you set without saving it.

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

8.6 Configuring RS-232/485 Settings

7.5.1 RS-232 Settings

Note: The DS-6701HWI-HFI models provide no RS-232 serial port.

Purpose:

The RS-232 serial port can be used for the configuration by the serial port management tools.

Steps:

1. Click **Remote Configuration> Serial Port Settings> 232 Serial Port** to enter RS-232 port setting interface:

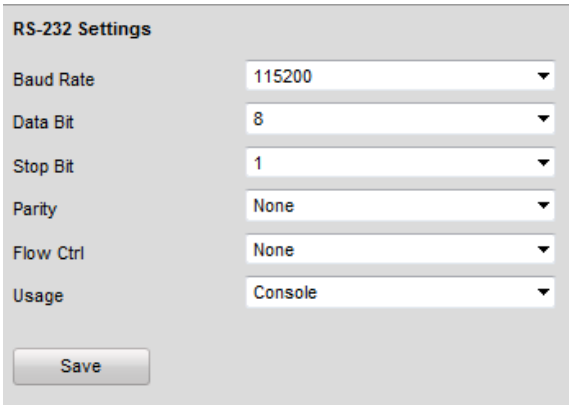


Figure 7. 25 RS-232 Port Settings

Note: If you want to connect the encoder by the RS-232 port, the parameters of the RS-232 should be exactly the same with the parameters you configured here.

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

7.5.2 RS-485 Settings

Purpose:

The RS-485 serial port is used to control the PTZ of the camera. The configuring of the PTZ parameters should be done before you control the PTZ unit.

Steps:

1. Click **Remote Configuration> Serial Port Settings> 485 Serial Port** to enter RS-485 port setting interface:

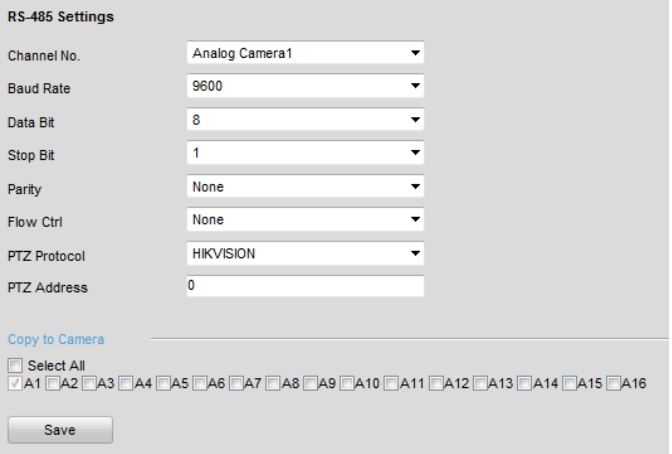


Figure 7. 26 RS-485 Port Settings

2. Set the RS-485 parameters.

   By default, the Baud Rate is set as 9600, the Data Bit as 8, the Stop Bit as 1 and the Parity and Flow Control as None.

   Note: The Baud Rate, Address and PTZ Protocol parameters should be exactly the same as the parameters of the connected PTZ camera.

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

Chapter 8 Record/Capture Settings

Before you start

Make sure the Encoder is connected with HDD (for DS-6700HWI/HFI-SATA) or network disk, and the HDD or network disk has been initialized for the first time to use.

Two record/capture types can be configured: Manual and Scheduled. The following section introduces the configuration of scheduled record/capture.

8.1 Configuring Holiday Settings

Purpose:

You may want to have different plan for recording on holiday. Follow the steps to configure the record schedule on holiday.

Steps:

1. Click **Remote Configuration> Camera Settings> Holiday Settings** to enter holiday settings interface.

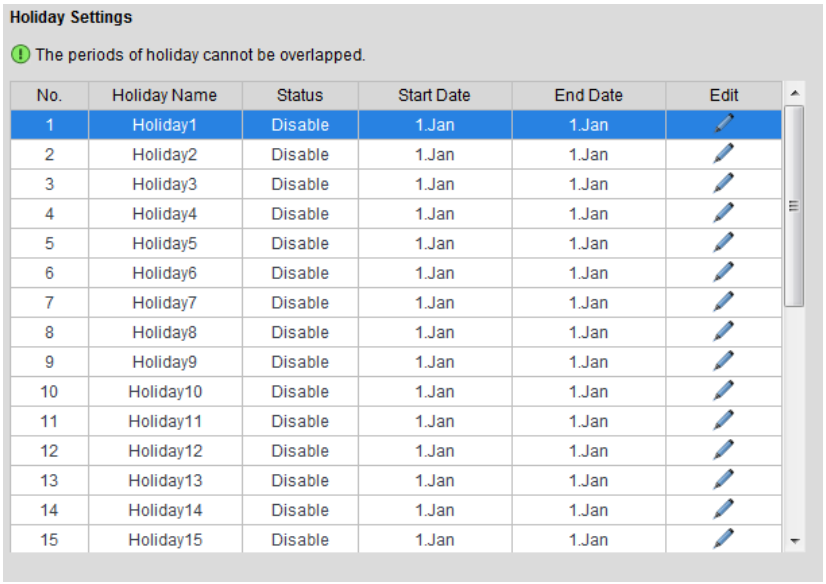


Figure 8. 1 Holiday Settings

2. Select an item from the list and click to edit the holiday.
   (1) Edit the holiday name.
   (2) Check the checkbox to enable holiday.
   (3) Select the holiday type from the dropdown list to by month, by week or by date.
   (4) Set the start and end date.
   (5) Click **OK** to save the settings and back to the Holiday Settings interface.

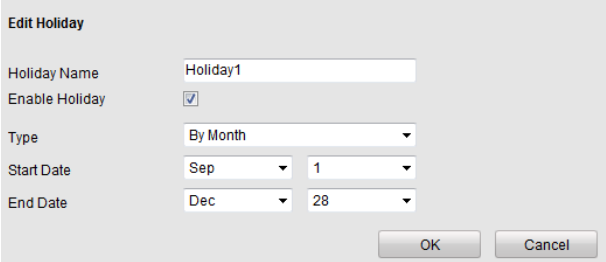


Figure 8. 2 Edit Holiday

3. You can check the finished holiday settings on the list.
4. Repeat the same steps to edit other holidays. Up to 32 holidays can be configured.

No.	Holiday Name	Status	Start Date	End Date	Edit
1	Holiday1	Enable	1.Sep	28.Dec	
2	Holiday2	Disable	1.Jan	1.Jan	
3	Holiday3	Disable	1.Jan	1.Jan	

Figure 9.1 List of Holidays

Note: The **Holiday** option is available in the Schedule dropdown list when you have enabled holiday schedule in **Holiday settings**.

8.2 Configuring Scheduled Record/Capture

Steps:

1. Click **Remote Configuration> Camera Settings> Schedule Settings** to enter record schedule settings interface.
2. Select the camera to configure the record / capture schedule.
3. Click the **Record** or **Capture** tab.
4. Check the checkbox of **Enable Record Schedule** or **Enable Capture Schedule** to enable the record/capture schedule.

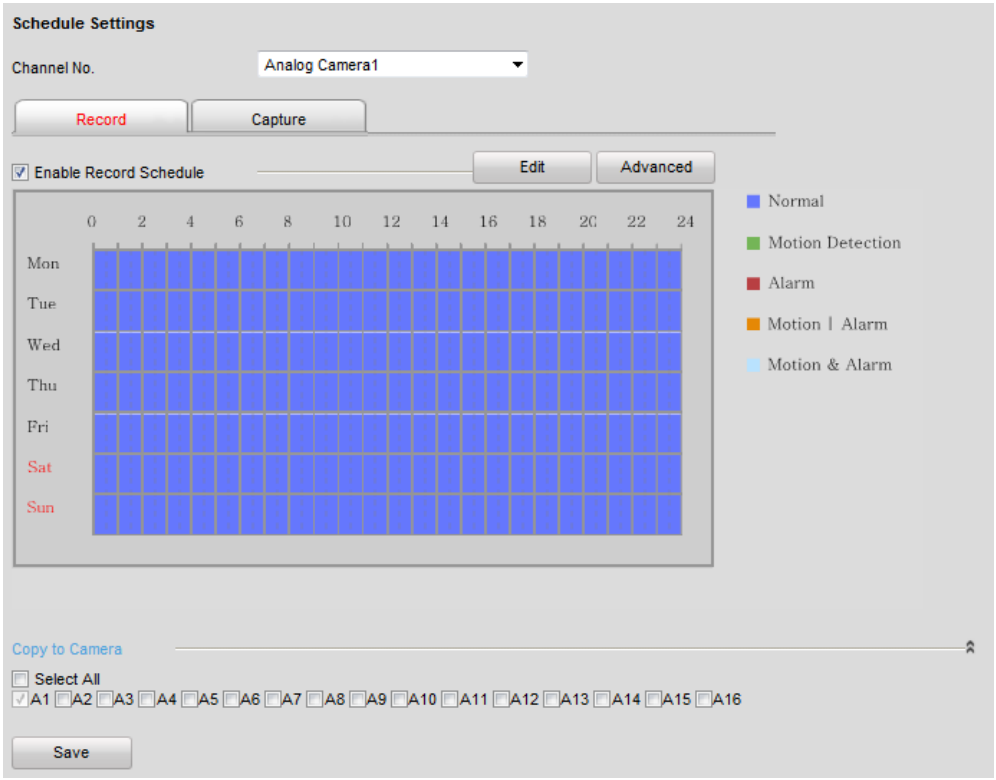


Figure 8. 3 Schedule Settings Interface

5. Click **Edit** to enter the Edit Schedule interface.
6. Choose the day in a week to configure scheduled record/capture.

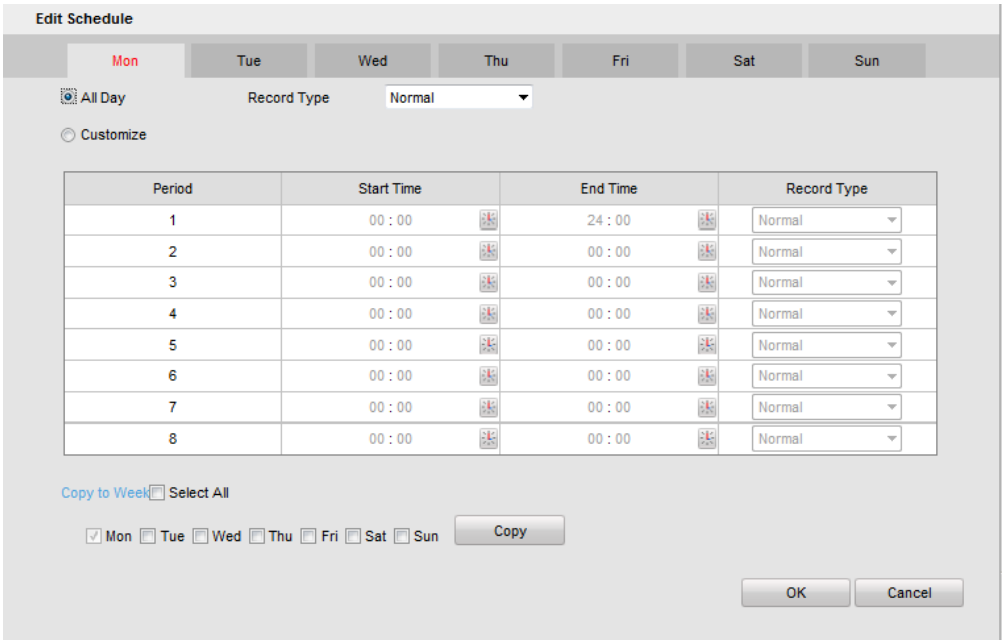


Figure 8. 4 Edit Schedule

1) Configure All Day or Customized period record/capture:

- If you want to configure the all-day record/capture, please check the **All Day** checkbox.
- If you want to record/capture in different time sections, check the **Customize** checkbox. Set the **Start**

Time and **End Time** of each period.

Note: The time of each period can't be overlapped. Up to 8 periods can be configured.

2) Select a **Record Type** or **Capture Type**. The record/capture type can be Normal, Motion, Alarm, Motion & Alarm, and Motion | Alarm.

- **Normal**

  If you select **Normal**, the video will be recorded / captured automatically according to the time of the schedule.

- **Record/Capture Triggered by Motion Detection**

  If you select **Motion**, the video will be recorded / captured when the motion is detected.

  Besides configuring the record/capture schedule, you have to set the motion detection area and check the checkbox of **Trigger Channel** on the **Linkage Method** of **Motion Detection** settings interface. Refer to the *Step 1* ***Set the Motion Detection Area*** in the *Section Configuring Motion Detection*.

- **Record/Capture Triggered by Alarm**

  If you select **Alarm**, the video will be recorded / captured when the alarm is triggered.

  Besides configuring the record / capture schedule, you have to set the **Alarm Type** and check the checkbox of **Trigger Channel** on the **Linkage Method** of **Alarm Input Settings** interface.

- **Record/Capture Triggered by Motion & Alarm**

  If you select **Motion & Alarm**, the video will be recorded / captured when the motion and alarm are triggered at the same time.

  Besides configuring the record/capture schedule, you have to configure the settings on the **Motion Detection** and **Alarm Input Settings** interfaces.

- **Record/Capture Triggered by Motion | Alarm**

  If you select **Motion | Alarm**, the video will be recorded/captured when the alarm is triggered or the motion is detected.

  Besides configuring the record/capture schedule, you have to configure the settings on the **Motion Detection** and **Alarm Input Settings** interfaces.

3) Check the checkbox of **Select All** and click **Copy** to copy settings of this day to the whole week. You can also check any of the checkboxes before the date and click **Copy**.

4) Click **OK** to save the settings and exit the **Edit Schedule** interface.

7. Click **Advanced** to configure advanced record parameters**.**

- **Pre-record:** The Pre-Record time can be configured as No Pre-Record, 5 s, 10 s, 15 s, 20 s, 25 s or 30 s.
- **Post-record:** The Post Record time can be configured as 5 s, 10 s, 30 s, 1 min, 2 min, 5 min or 10 min.
- **Redundant Record:** Enabling redundant record means you save the record files in the redundant HDD. You can enable or disable the redundant record by setting it to Yes or No.

  Notes:

  - The redundant record is used when you want to save the record files in the redundant HDD. You must configure the redundant HDD in HDD settings.
  - The **Redundant Record** option is only available when the HDD mode is *Group*.
- **Overwrite:** Select to overwrite the earlier recorded files or not when the HDD is full. If the Overwrite mode is enabled, the earlier recorded files will be overwritten when the HDD is full; otherwise, the recording will stop and trigger alarm when the HDD is full.
- **Record Audio:** Enable or disable the audio record.
- **Stream Type:** Select the Main Stream and Sub Stream for analog camera recording.
- **Expired Time:** The expired time is the longest time for a record file to be kept in the HDD, if the deadline

is reached, the file will be deleted. You can set the expired time to 0, and then the file will not be deleted. The actual keeping time for the file should be determined by the capacity of the HDD.

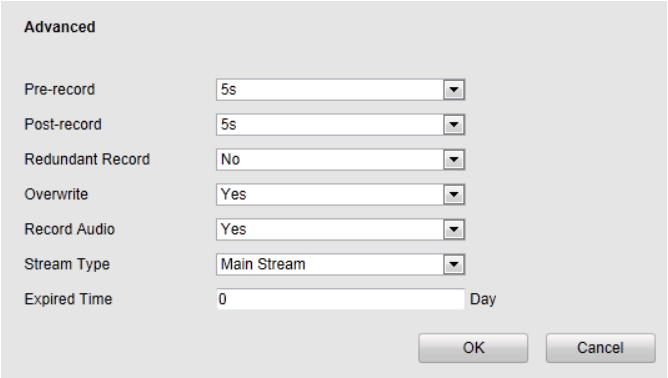


Figure 8. 5 Edit Schedule

8. If you want to copy the display settings of the current camera to other cameras, spread the **Copy to Camera** panel and select the camera(s) to copy, or click **Select All** to select all cameras.

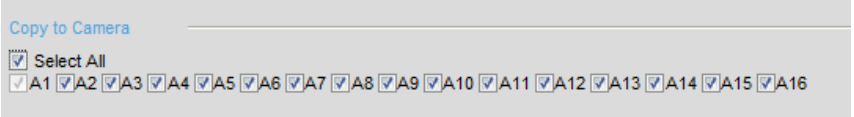


Figure 8. 6 Copy to Camera

9. Click **Save** to validate the above settings.

Chapter 9 Playback

Purpose:

The recorded video files can be remotely played back through the WEB browser.

Steps:

1. Click **Playback** on the menu bar to enter playback interface:

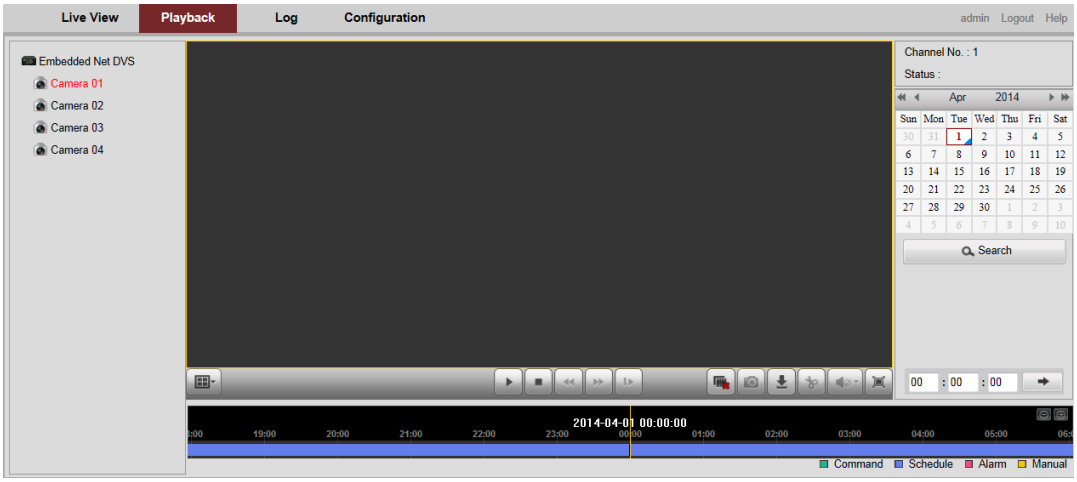


Figure 9. 1 Playback Page

2. Click the camera from the device list for playback.
3. Select the date from the calendar and click **Search**.

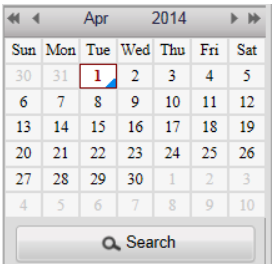


Figure 9. 2 Select Date for Search

4. Click the **Play** button to play the video file searched on the current date.

Figure 9. 3 Playback Page

5. Use the buttons on the toolbar to operate in playback mode.

Figure 9. 4 Playback Toolbar

Table 9. 1 Description of Toolbar

Button	Operation	Button	Operation
	Select window-division mode		Play/Pause
	Stop playing		Slow forward
	Fast forward		Play by single frame
	Stop all channels from playing		Capture pictures in playback mode
	Download video files		Start/Stop clipping video files
	Audio on/off		Switch to full-screen live view mode.

6. You can also drag the progress bar with the mouse to locate the exact playback point. You can also input the time and click button to locate the playback point.

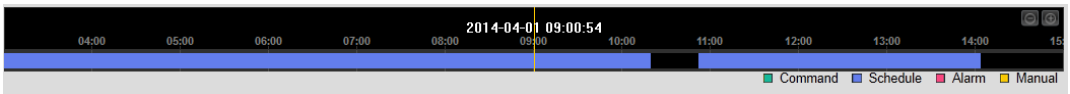


Figure 9. 5 Progress Bar

The color of the video on the progress bar stands for the different video types.

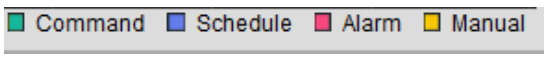


Figure 9. 6 Progress Bar

Chapter 10 Managing User Accounts

Click **Remote Configuration**>**Remote Configuration**>**User Management** to enter the User Information interface:

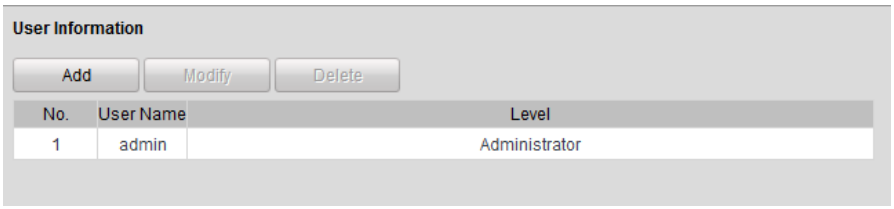


Figure 10. 1 User Information Interface

The **admin** user is allowed to create normal users. And up to 31 users can be created. .

10.2 Adding a User

Steps:

1. Click **Add** to enter the Add user interface.
2. Edit the **User Name**.
3. Select the **Level** to **Operator** or **User**.
4. Set the **Password**, and confirm the same password.

STRONG PASSWORD RECOMMENDED– We highly recommend that 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. We recommend that you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

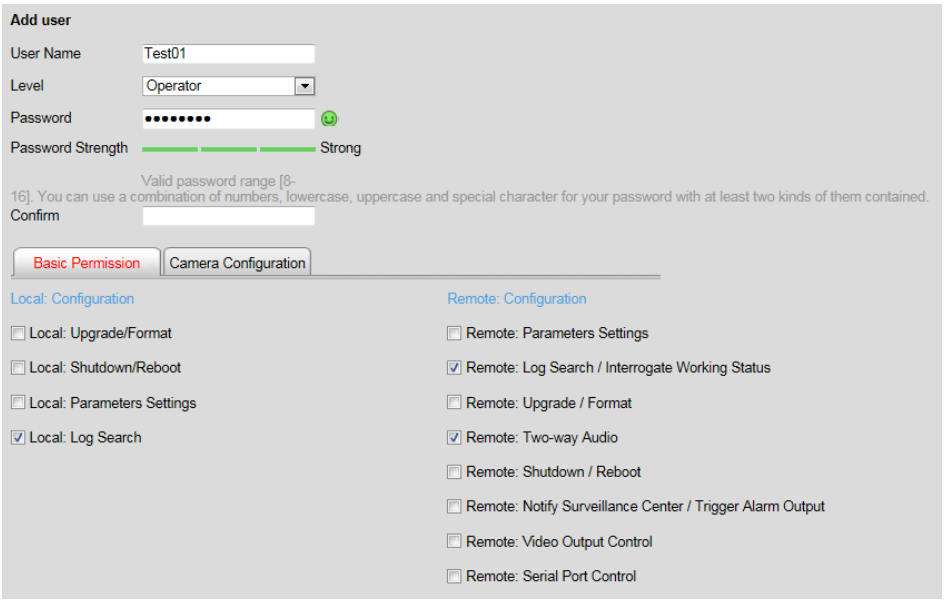
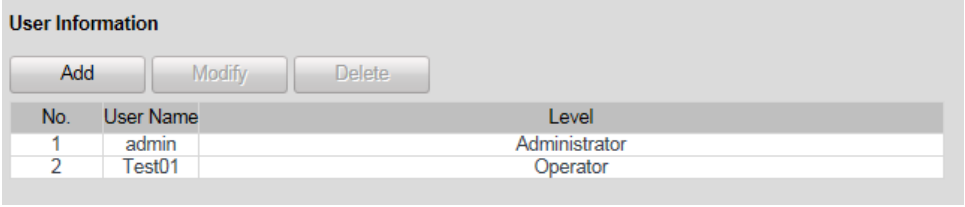


Figure 10. 2 Add a User

Different user level is given with different permissions:

- **Operator:** The *Operator* user level has permission of Local Log Search in Local Configuration, Remote Log Search and Two-way Audio in Remote Configuration and all operating permission in Camera Configuration.
- **User:** The Guest user has permission of Local Log Search in Local Configuration, Remote Log Search in Remote Configuration and only has the local/remote playback in the Camera Configuration.

5. Configure the user permissions for the created user account, including the Basic Permission and Camera Operation.
6. Click **OK** to finish the user addition.



10.3 Modifying a User

Steps:

1. Select a user account from the list on the User Information interface to be modified.

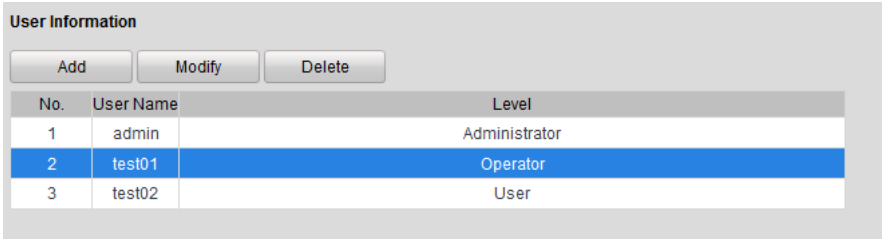


Figure 10. 3 Select a User

2. Click **Modify** to enter the modification interface.

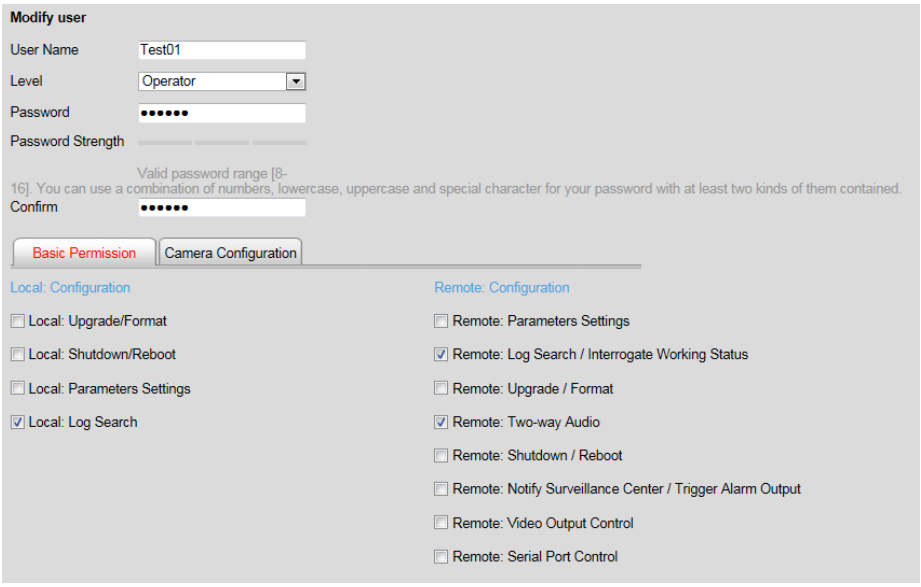


Figure 10. 4 Modify a User

3. Modify the **User Name**, **Password** and then select **User type**. You are highly recommended to use the strong password.
4. Configure the user permission for the user, including the Basic Permission and Camera Operation.
5. Click **OK** to finish the user modification.

Note: You need the admin password to modify the admin user.

10.4 Deleting a User

Steps:

1. Select a user account from the list on the User Information interface to be deleted.
2. Click **Delete,** and the information box will pop up:

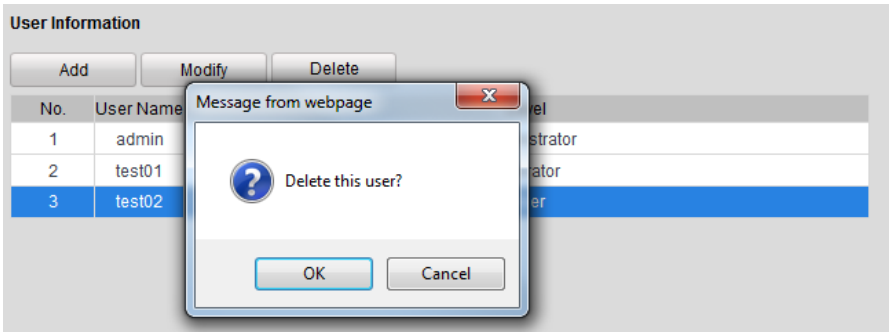


Figure 10. 5 Delete a User

3. Click **OK** to delete the selected user account.

Chapter 11 Log Search and Maintenance

11.1 Log Search

Purpose

The operation, alarm, exception and information of the device can be stored in log files, which can be viewed and exported at any time.

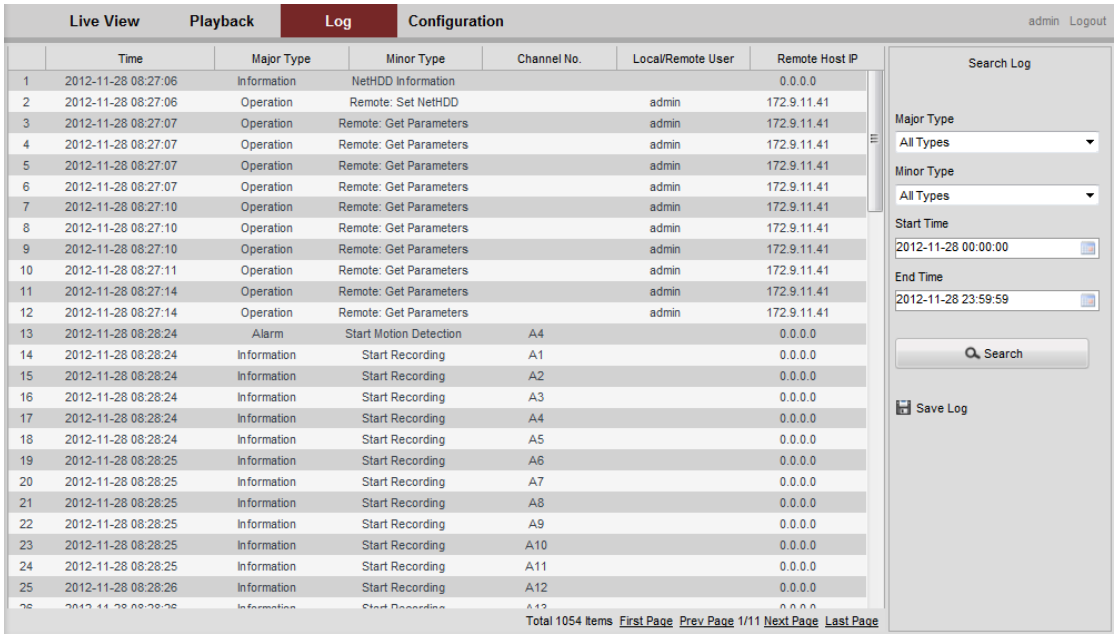
Before you start

The Log function can be realized only when the Encoder is connected with HDD (for DS-6700HWI/HFI-SATA) or network disk. And make sure the HDD or network disk has been initialized for the first time to use. Please refer to *Section Adding Network Disk* for details.

Steps:

1. Click **Log** on the menu bar to enter the Log interface.
2. Set the log search conditions to refine your search, including the Major Type, Minor Type, Start Time and End Time.
3. Click the **Search** button to start searching log files.
4. The matched log files will be displayed on the list shown below.

   ***Note*:** Up to 100 log files can be displayed each time.



	Time	Major Type	Minor Type	Channel No.	Local/Remote User	Remote Host IP
1	2012-11-28 08:27:06	Information	NetHDD Information			0.0.0.0
2	2012-11-28 08:27:06	Operation	Remote: Set NetHDD		admin	172.9.11.41
3	2012-11-28 08:27:07	Operation	Remote: Get Parameters		admin	172.9.11.41
4	2012-11-28 08:27:07	Operation	Remote: Get Parameters		admin	172.9.11.41
5	2012-11-28 08:27:07	Operation	Remote: Get Parameters		admin	172.9.11.41
6	2012-11-28 08:27:07	Operation	Remote: Get Parameters		admin	172.9.11.41
7	2012-11-28 08:27:10	Operation	Remote: Get Parameters		admin	172.9.11.41
8	2012-11-28 08:27:10	Operation	Remote: Get Parameters		admin	172.9.11.41
9	2012-11-28 08:27:10	Operation	Remote: Get Parameters		admin	172.9.11.41
10	2012-11-28 08:27:11	Operation	Remote: Get Parameters		admin	172.9.11.41
11	2012-11-28 08:27:14	Operation	Remote: Get Parameters		admin	172.9.11.41
12	2012-11-28 08:27:14	Operation	Remote: Get Parameters		admin	172.9.11.41
13	2012-11-28 08:28:24	Alarm	Start Motion Detection	A4		0.0.0.0
14	2012-11-28 08:28:24	Information	Start Recording	A1		0.0.0.0
15	2012-11-28 08:28:24	Information	Start Recording	A2		0.0.0.0
16	2012-11-28 08:28:24	Information	Start Recording	A3		0.0.0.0
17	2012-11-28 08:28:24	Information	Start Recording	A4		0.0.0.0
18	2012-11-28 08:28:24	Information	Start Recording	A5		0.0.0.0
19	2012-11-28 08:28:25	Information	Start Recording	A6		0.0.0.0
20	2012-11-28 08:28:25	Information	Start Recording	A7		0.0.0.0
21	2012-11-28 08:28:25	Information	Start Recording	A8		0.0.0.0
22	2012-11-28 08:28:25	Information	Start Recording	A9		0.0.0.0
23	2012-11-28 08:28:25	Information	Start Recording	A10		0.0.0.0
24	2012-11-28 08:28:25	Information	Start Recording	A11		0.0.0.0
25	2012-11-28 08:28:26	Information	Start Recording	A12		0.0.0.0

Figure 11. 1 Log Search Interface

5. You can click the Save Log button to save the searched log files to local directory.

11.2 Viewing Device Information

Click **Remote Configuration** > **Device Parameters** > **Device Information** to enter the Device Information interface of the encoder:

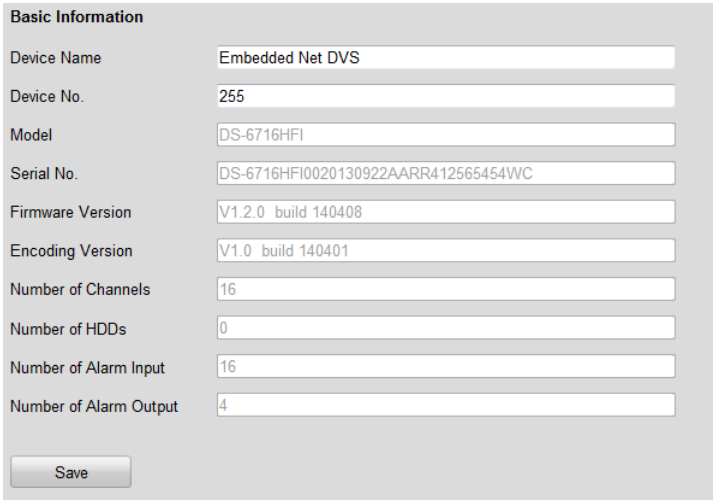


Figure 11. 2 1 Device Information

You can edit the Device Name and Device No., and view the device information, including Model, Serial No., Firmware/Encode Version, Number of Channels, Number of HDDs, and Number of Alarm Input / Output.

11.3 Maintenance

Click **Remote Configuration** >**Maintenance** to enter the Maintenance interface of the encoder:

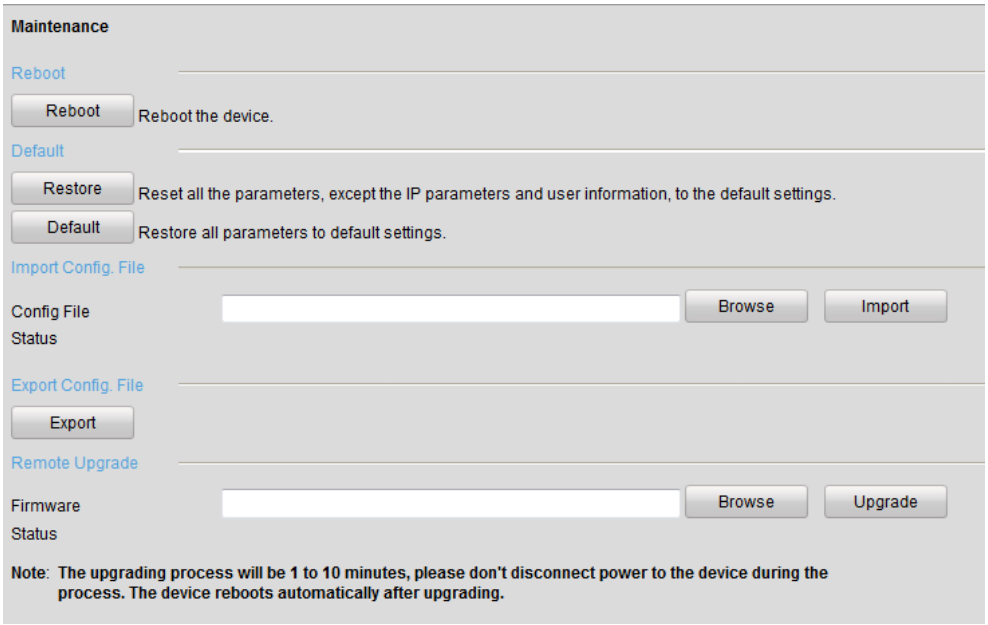


Figure 11. 3 Maintenance Page

11.3.1 Restarting the Device

On the **Maintenance> Reboot** interface, click **Reboot** to enter the following message box:

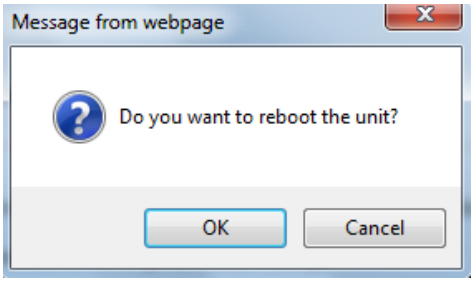


Figure 11. 4 Reboot the Device

Click **OK** to reboot the device or **Cancel** to cancel the operation.

11.3.2 Restoring Default Settings

On the **Maintenance> Default** interface, click **Restore or Default** to restore device parameters to the factory settings.

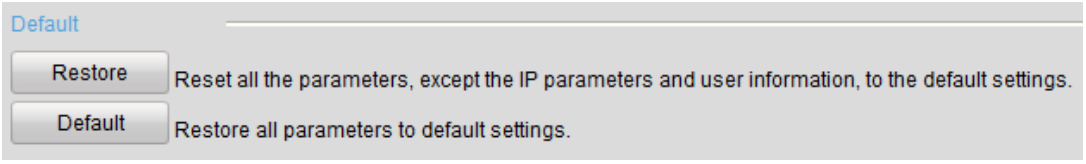


Figure 11. 5 Restore Default Settings

- By selecting the **Restore** button, the device restores the default settings for the parameters except the IP address, subnet mask, gateway and port.
- By selecting the **Default** button, the device restores the default settings for all parameters.

On the pop-up message box, click **OK** to restore and reboot the device to validate the settings.

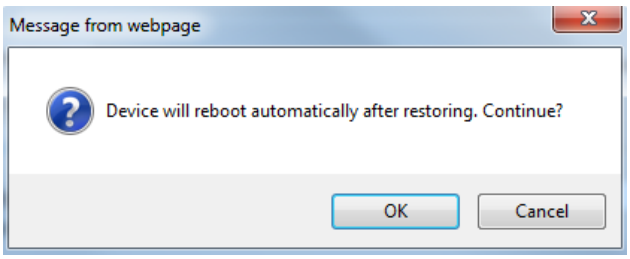


Figure 11. 6 Pop-up Message Box

11.3.3 Importing/Exporting Configuration Files

The configuration files of the device can be exported to local device for backup; and the configuration files of one device can be imported to multiple device devices if they are to be configured with the same parameters.

- On the **Maintenance> Import Config File** interface, click **Browse** to select the file from the selected

backup device and then click the **Import** button to import a configuration file.

Note: After having finished the import of configuration files, the device will reboot automatically.

- On the **Maintenance> Export Config File** interface, click the **Export** button to export configuration files to the selected local backup device.

Figure 11. 7 Import/Export Config Files

11.3.4 Upgrading the System

On the **Maintenance> Remote Upgrade** interface, click **Browse** to select the local update file and then click **Upgrade** to start remote upgrade.

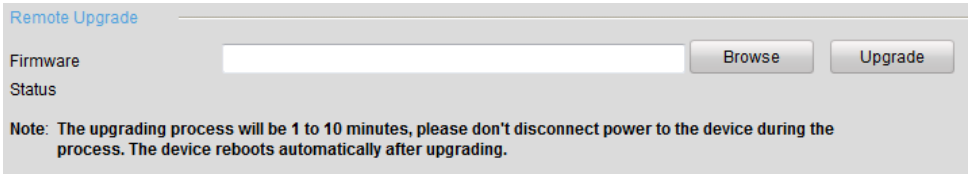


Figure 11. 8 Remote Upgrade

Chapter 12 FAQ

- **Why cannot ping the Encoder?**

  Please refer to Chapter 3 to configure the device's IP being in the same segment as your PC, and check the cable and switch.

- **Why the transparent channel has been set, but the encoder still cannot receive data?**

  1. Check if RS-232 has been set as transparent channel first.
  2. Check the connection of encoder.

- **Why cannot add encoder with software?**

  1. Check the encoder IP.
  2. Make sure the cable is connected.
  3. User name and password of encoder are correct.

- **Why cannot control the connected PTZ camera or speed dome through the encoder?**

  1. Check the RS-485 connection of the device with the PTZ camera or dome.
  2. Check whether the PTZ address, protocol and baud rate of the device are set to be the same with the connected camera or speed dome.

- **Why cannot view the video image through IE browser?**

  1. Check the network connection.
  2. Check the user name and password of encoder are entered correctly.
  3. Check the port of encoder is entered correctly.