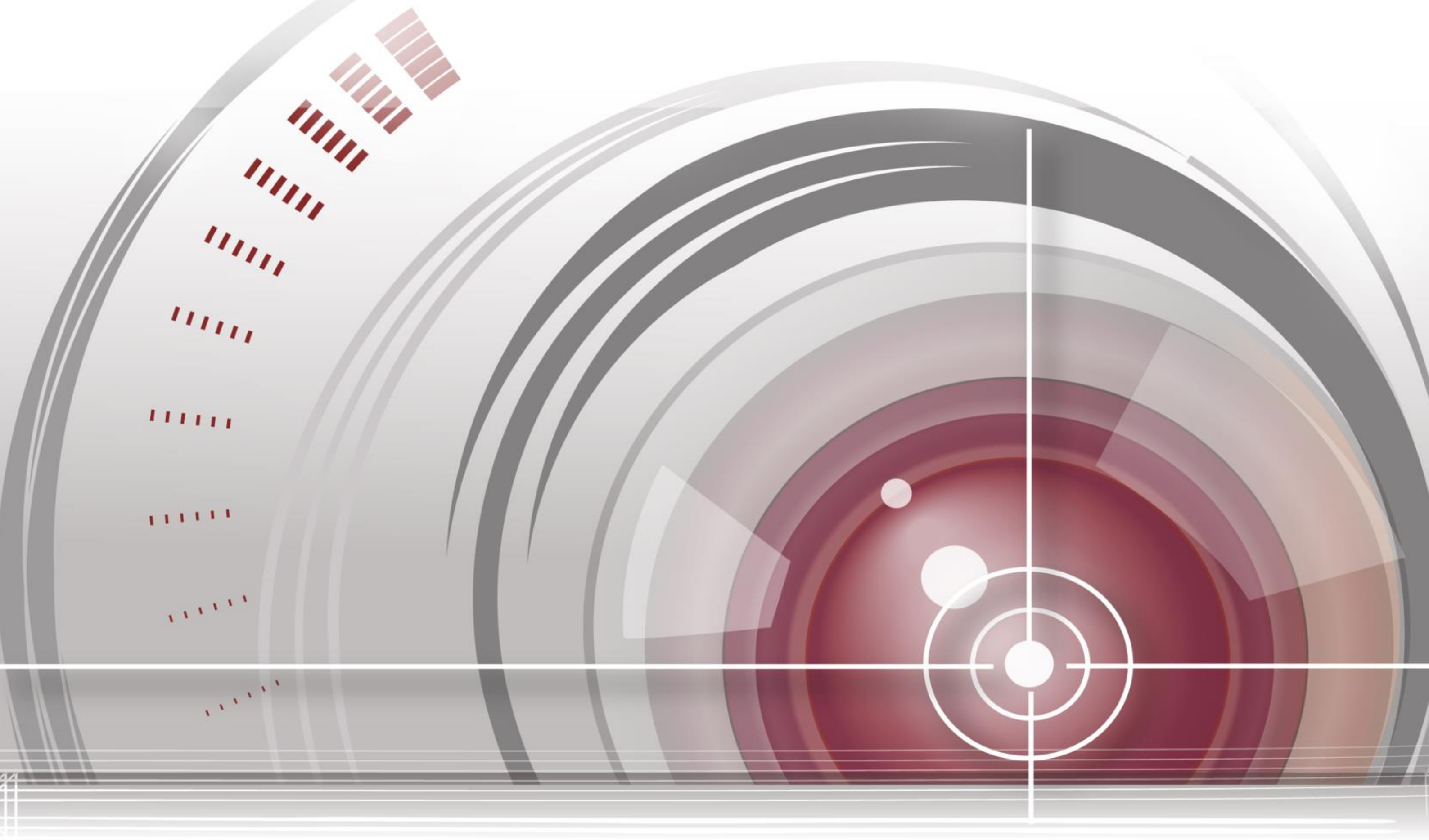
HIKVISION



Network Audio/Video Encoder

User Manual

UD.6L0202D2215A01

User Manual

Any and all information, including, among others, wordings, pictures, graphs are the properties of Hangzhou Hikvision Digital Technology Co., Ltd. or its subsidiaries (hereinafter referred to be "Hikvision"). This user manual (hereinafter referred to be "the Manual") cannot be reproduced, changed, translated, or distributed, partially or wholly, by any means, without the prior written permission of Hikvision. Unless otherwise stipulated, Hikvision does not make any warranties, guarantees or representations, express or implied, regarding to the Manual.

About this Manual

This Manual is applicable to Network HD 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, THIS MANUAL AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED "AS IS" AND "WITH ALL FAULTS AND ERRORS". HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.

YOU ACKNOWLEDGE THAT THE NATURE OF THE INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INFECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.

YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.

IN THE EVENT OF ANY CONFLICTS BETWEEN THIS MANUAL AND THE APPLICABLE LAW, THE LATTER 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-6700HFHI/V Series Audio/Video Encoder Server allows the analog signal to be digitized and then stored in micro SD card/network disk or transmitted via network. The DS-6700HFHI/V provides HDMI and VGA input at up to 1080p resolution

Adopting the latest embedded processor, the DS-6700HFHI/V Series Audio/Video Encoder provides more powerful capabilities in audio/video encoding; various network protocols are supported; and code downloaded in FLASH ensures high stability and reliability of system performance.

1.2 Features

Encoding

- H.264 encoding formats available; independent configuration of encoding formats for main stream and sub stream;
- 1-ch HDMI or VGA video input and 1-ch VGA video loop output provided;
- Encoding at HD resolution of 1080p/720p/UXGA, etc.;
- Dual stream encoding.
- VGA picture position adjustment and target cropping (for HDMI/VGA output).
- Up to 128G Micro SD card available;
- NFS/iSCSI protocol to realize NAS/IPSAN network storage;
- Either compound streams encoding or video stream encoding selectable; audio and video synchronization during compound streams encoding.

Network

- One 10M/100Mbps adaptive Ethernet interface.
- Cross-platform access via multi-browsers such as IE, FireFox, Chrome, Safari, etc.;
- Remote web browser access by HTTPS ensures high security.
- Support SNMP simple network management protocol.
- Auto/Manual port mapping by UPnP™.
- Support ONVIF and ISAP 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-485 transparent channel.
- Access to Internet by PPPoE method, and support Peanut Hull, DynDNS, HiDDNS, etc.
- Easy network access via Hikvision EZVIZ Cloud P2P;
- 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.

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

Network disk/microSD card must be connected before log operation.

Chapter 2 Panels and Connections

2.1 Front Panel

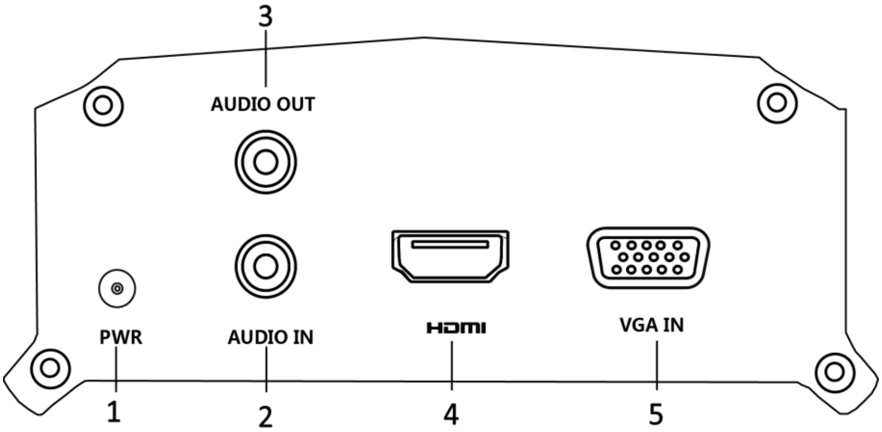


Figure 2. 1 Front Panel

Table 2. 1 Description of Front Panel

No.	Item	Description
1	POWER LED Indicator	Lights in red when the device is powered on; light in orange when the SD card is inserted.
2	AUDIO IN	3.5mm interface for line in and audio input; connect to audio input device or active pick-up, microphone, etc.
3	AUDIO OUT	3.5mm interface; connect to audio output device, e.g., loudspeaker, etc.
4	HDMI	HDMI video input connector.
5	VGA IN	VGA video input connector.

2.2 Rear Panel

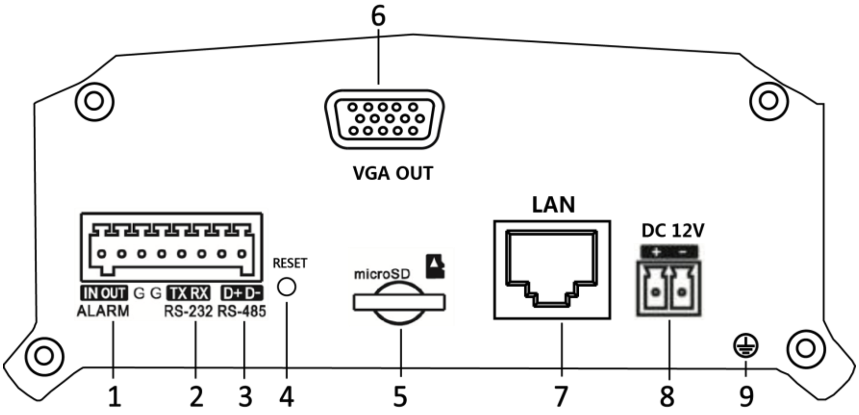


Figure 2. 2 Rear Panel

Table 2. 2 Description of Rear Panel

No.	Item	Description
1	ALARM IN	Relay alarm input.
	ALARM OUT	Relay alarm output.
2	RS-232	Serial interface for configuration of device's parameters or used as transparent channel.
3	RS-485	RS-485 serial interface; connect to pan/tilt unit, speed dome, etc.
4	RESET	Restore the factory default settings by holding the *RESET* button for more than 15 seconds after the device is turned on.
5	microSD	microSD interface for data storage.
6	VGA OUT	VGA video output connector.
7	LAN	10M/100Mbps adaptive Ethernet interface
8	DC12V	12 VDC power supply.
9	GND	Grounding

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.

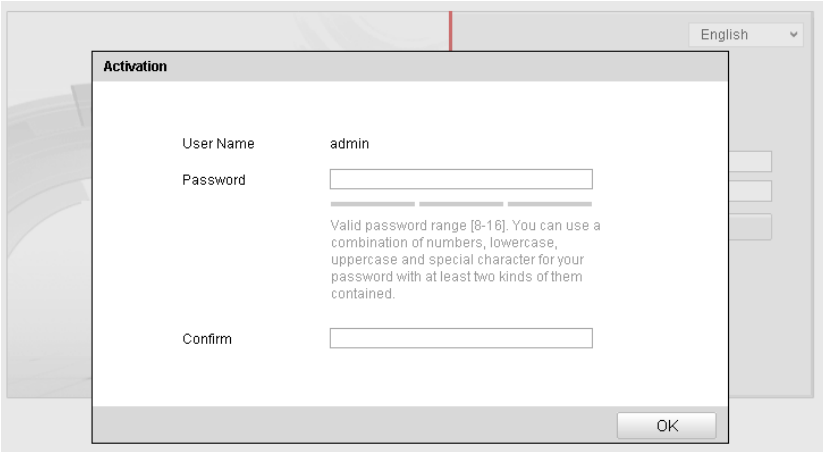
3.1 Setting the Admin Password via Web Browser

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 the **Enter** button 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.



User Name admin

Password

Valid password range [8-16]. You can use a combination of numbers, lowercase, uppercase and special character for your password with at least two kinds of them contained.

Confirm

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.

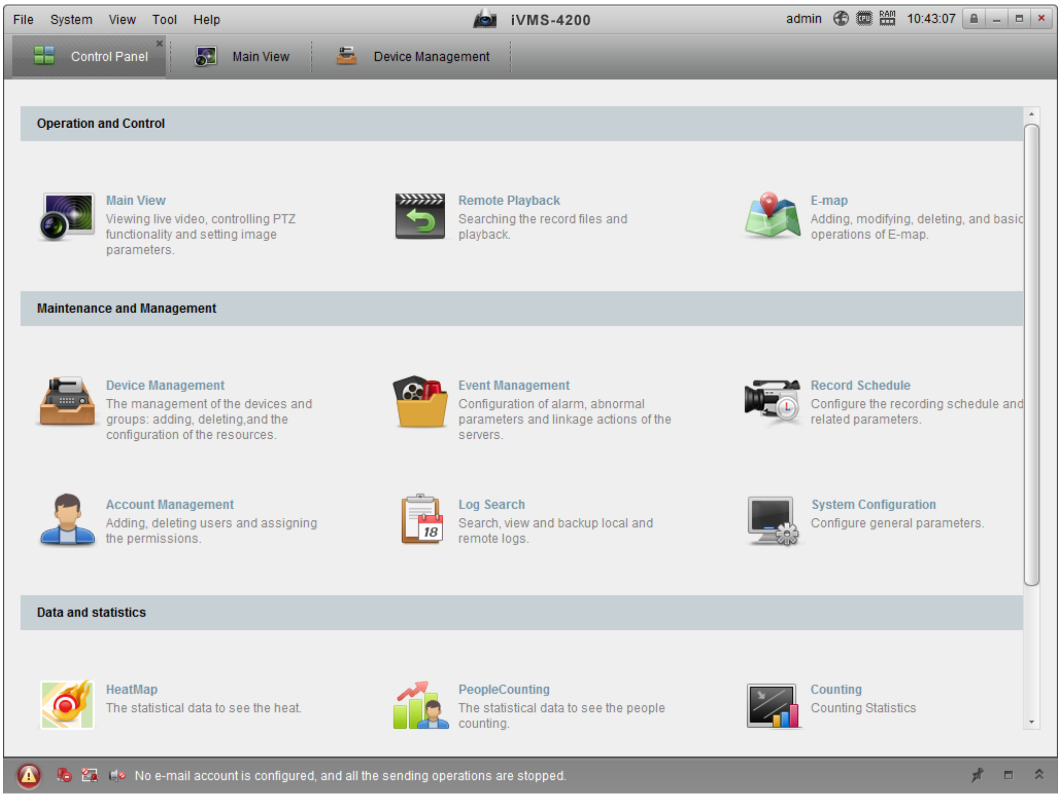
3.2 Setting Admin Password and Modifying Network Parameters via Client Software

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.



Main View
Viewing live video, controlling PTZ functionality and setting image parameters.

Remote Playback
Searching the record files and playback.

E-map
Adding, modifying, deleting, and basic operations of E-map.

Device Management
The management of the devices and groups: adding, deleting,and the configuration of the resources.

Event Management
Configuration of alarm, abnormal parameters and linkage actions of the servers.

Record Schedule
Configure the recording schedule and related parameters.

Account Management
Adding, deleting users and assigning the permissions.

Log Search
Search, view and backup local and remote logs.

System Configuration
Configure general parameters.

HeatMap
The statistical data to see the heat.

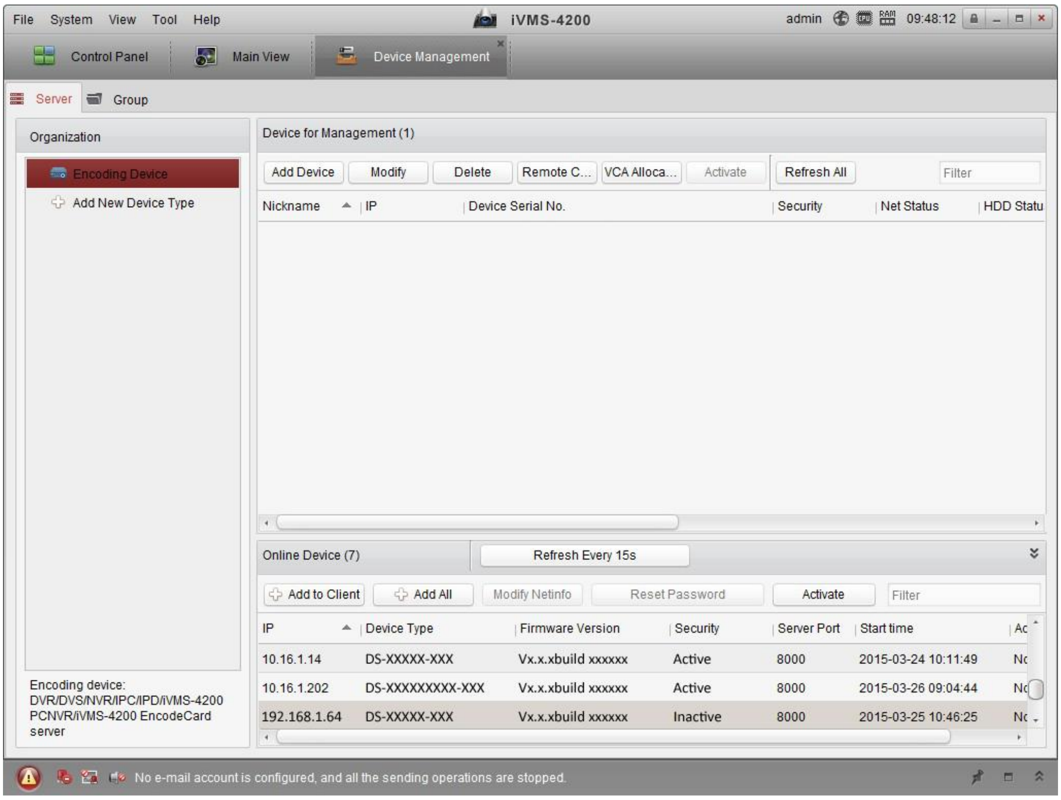
PeopleCounting
The statistical data to see the people counting.

Counting
Counting Statistics

No e-mail account is configured, and all the sending operations are stopped.

Figure 3. 2 Control Panel

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



Encoding device: DVR/DVS/NVR/IPC/IPD/iVMS-4200 PCNVR/iVMS-4200 EncodeCard server

IP	Device Type	Firmware Version	Security	Server Port	Start time	Ac
10.16.1.14	DS-XXXXX-XXX	Vx.x.xbuild xxxxxx	Active	8000	2015-03-24 10:11:49	Nc
10.16.1.202	DS-XXXXXXXXX-XXX	Vx.x.xbuild xxxxxx	Active	8000	2015-03-26 09:04:44	Nc
192.168.1.64	DS-XXXXX-XXX	Vx.x.xbuild xxxxxx	Inactive	8000	2015-03-25 10:46:25	Nc

No e-mail account is configured, and all the sending operations are stopped.

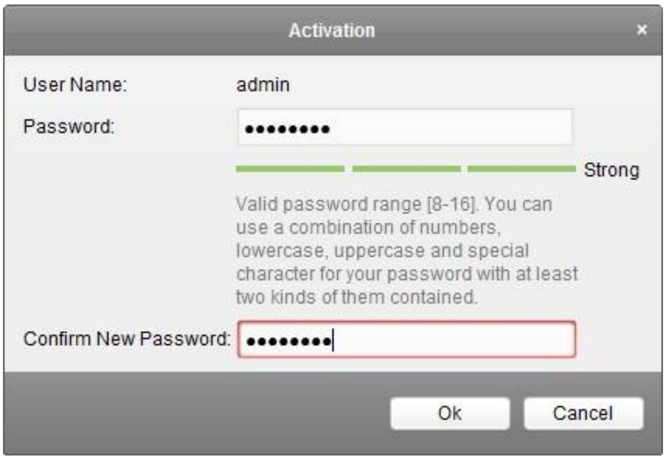
Figure 3. 3 Control Panel

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.



User Name: admin

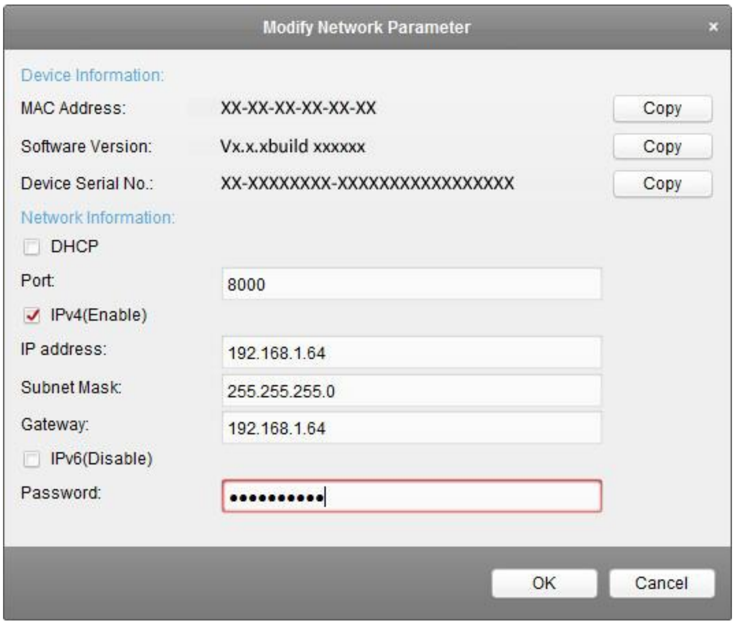
Password: ••••••••• Strong

Valid password range [8-16]. You can use a combination of numbers, lowercase, uppercase and special character for your password with at least two kinds of them contained.

Confirm New Password: ••••••••

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.



Modify Network Parameter

Device Information:

MAC Address: XX-XX-XX-XX-XX-XX

Software Version: Vx.x.xbuild xxxxxx

Device Serial No.: XX-XXXXXXXX-XXXXXXXXXXXXXXXXX

Network Information:

□ DHCP

Port: 8000

☑ IPv4(Enable)

IP address: 192.168.1.64

Subnet Mask: 255.255.255.0

Gateway: 192.168.1.64

□ IPv6(Disable)

Password: ●●●●●●●●●●●

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 Activation and Initial Network Configuration for the Encoder*.
- 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.*

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 after 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.

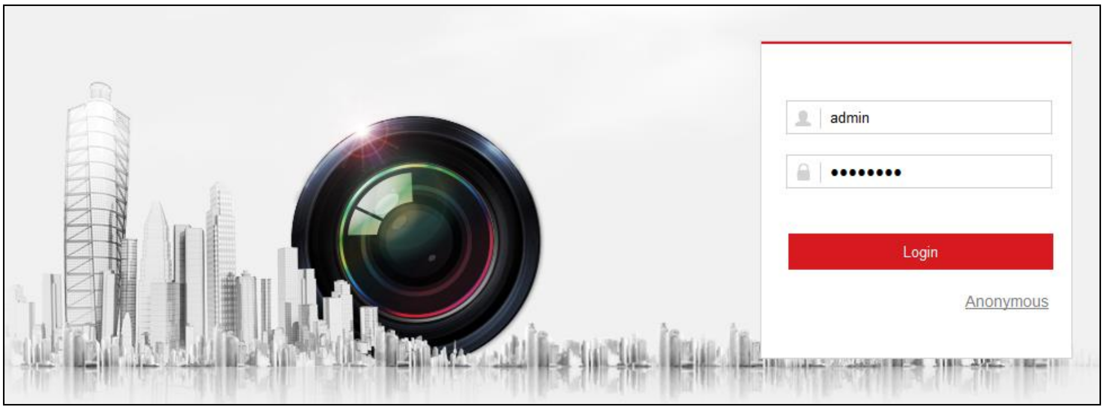


Figure 4. 1 Login Page

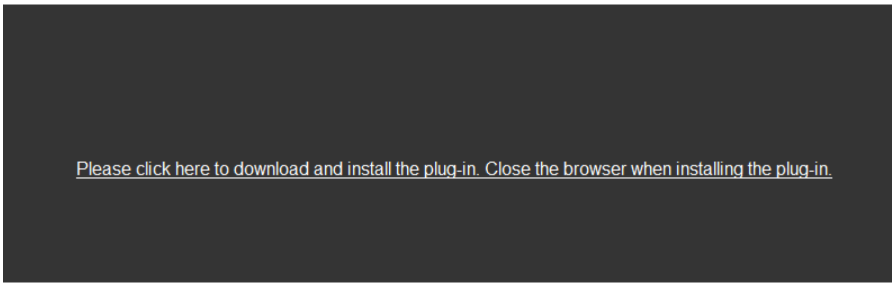
2. Input the user name and the password to log into the system.

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.

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

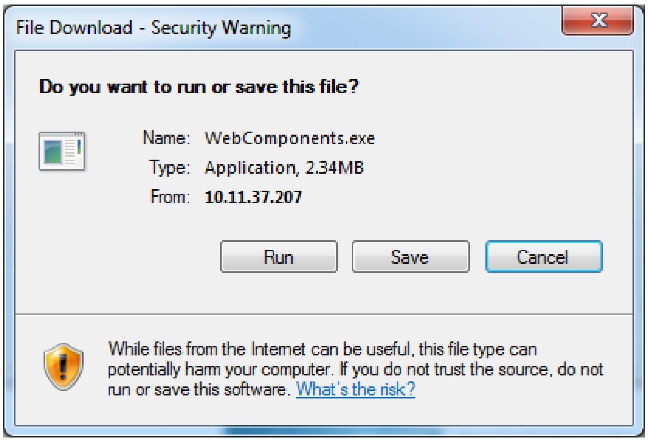
   (1) Click on the live view window by following the hints on the screen.



Please click here to download and install the plug-in. Close the browser when installing the plug-in.

Figure 4. 2 Download and Install Plug-in

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



File Download - Security Warning

Do you want to run or save this file?

Name: WebComponents.exe

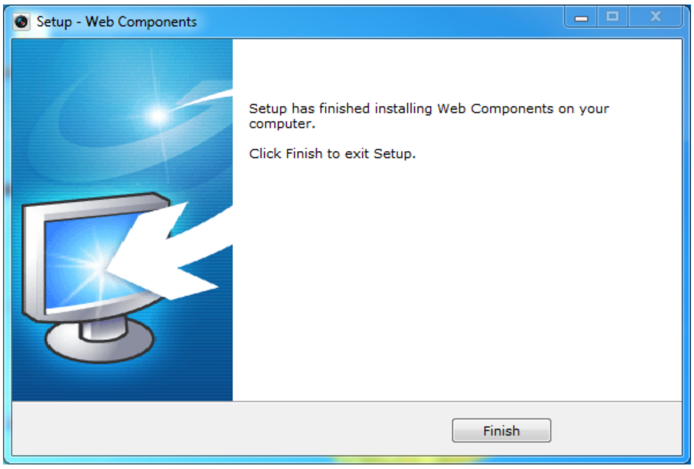
Type: Application, 2.34MB

From: 10.11.37.207

While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not run or save this software. What's the risk?

Figure 4. 3 Run Web Components

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



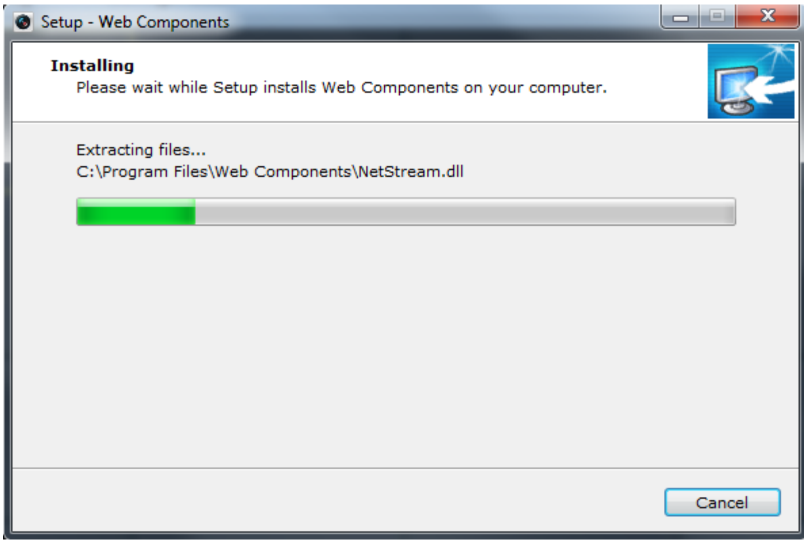
Setup - Web Components

Setup has finished installing Web Components on your computer.

Click Finish to exit Setup.

Figure 4. 4 Click Next

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



Setup - Web Components

Installing

Please wait while Setup installs Web Components on your computer.

Extracting files...

C:\Program Files\Web Components\NetStream.dll

Figure 4. 5 Install the Web Components

4. After having successfully installed the web components, you enter the main page.

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.

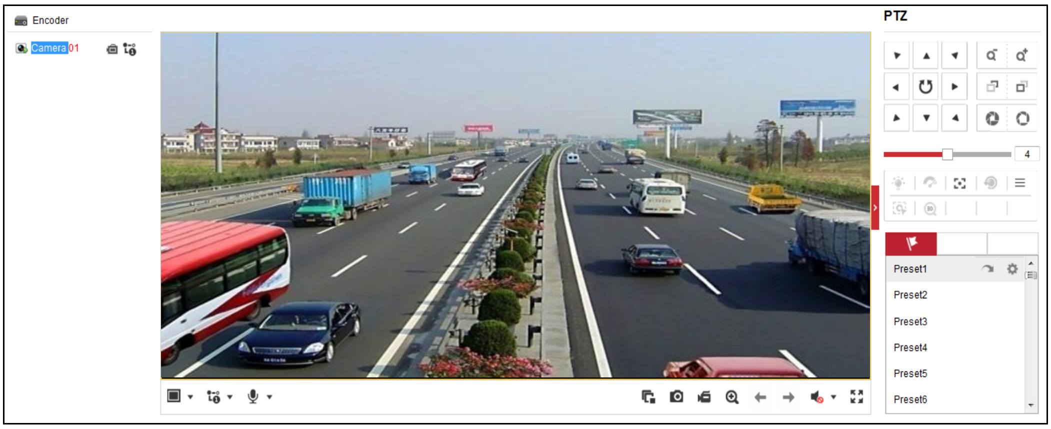


Figure 5. 1 Start Live View

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 all live view
📷	Capture pictures in live view mode
🎥/🎥	Manually start/stop recording
🔍	Enable digital zoom
←	Previous page
→	Next page

🔊▾/🔇▾	Audio on/off
🎙/🎙	Start/Stop two-way audio
① ②	Select the main stream or sub stream for live view
⛶	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:

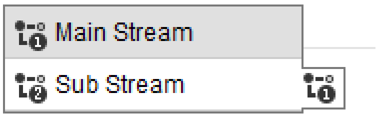


Figure 5. 2 Main Stream/Sub Stream for Live View

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 **Esc** key on PC or double click on the live video again.

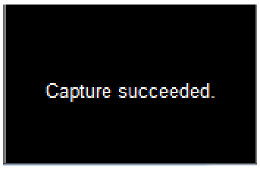
Please refer to the following section for more information:

1. Capturing pictures on *Section 5.2 Capturing the Picture*. .
2. Configuring recording on *Section 8.2 Record* Settings.
3. Setting the image quality of live view on *Section 6.1 Local Configuration.*
4. Setting the saving path for the recorded video files and captured pictures on *Section 6.1 Local Configuration*.
5. Setting the OSD text on live video on *Section 7.2 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.



Capture succeeded.

Figure 5. 3 Picture Capture Succeeded

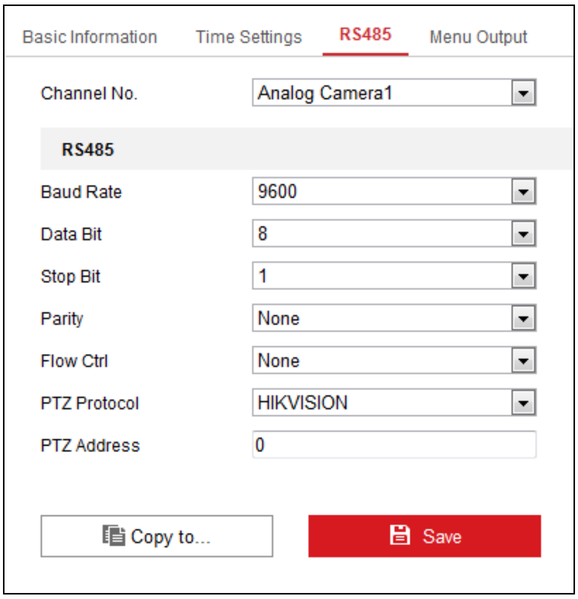
NOTE

- 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 (**Configuration** > **System Settings** > **RS485**), as shown in Figure 5.4, must be the same with the parameters of the connected pan/tilt unit or speed dome.



Channel No. Analog Camera1

RS485

Baud Rate 9600

Data Bit 8

Stop Bit 1

Parity None

Flow Ctrl None

PTZ Protocol HIKVISION

PTZ Address 0

Figure 5. 4 RS-485 Settings

5.3.1 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.

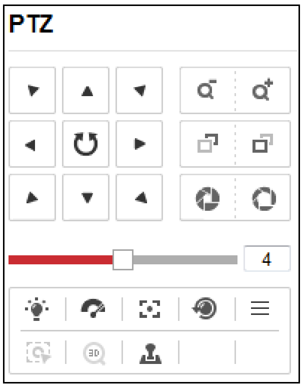


Figure 5. 5 PTZ Control Panel

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

Icon	Description
🔍− 🔍+	Zoom in/out
⧉ ⧉	Focus near/far
● ○	Iris +/-
▬▬▭── 4	PTZ speed adjustment
💡	Light on/off
◓	Wiper on/off
⛶	Auxiliary focus
⟲	Initialize lens
☰	Adjust speed of pan/tilt movements
⛶	Start manual tracking
3D	Start 3D Zoom

5.3.2 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.

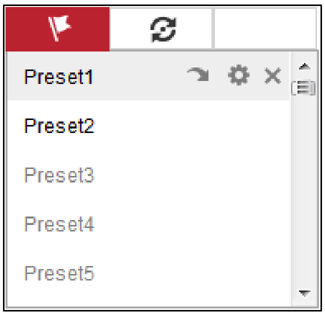


Figure 5. 6 Set a Preset

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.

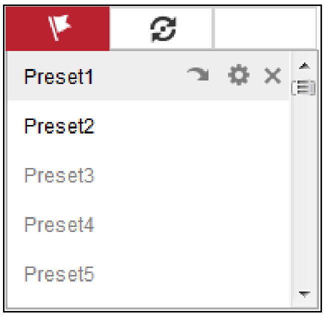
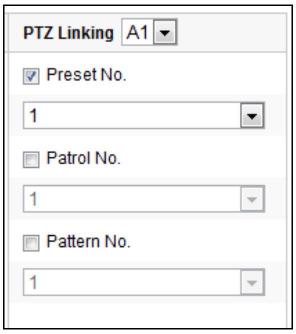


Figure 5. 7 Call a Preset

Linking to Alarm:

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



PTZ Linking A1

☑ Preset No.

1

□ Patrol No.

1

□ Pattern No.

1

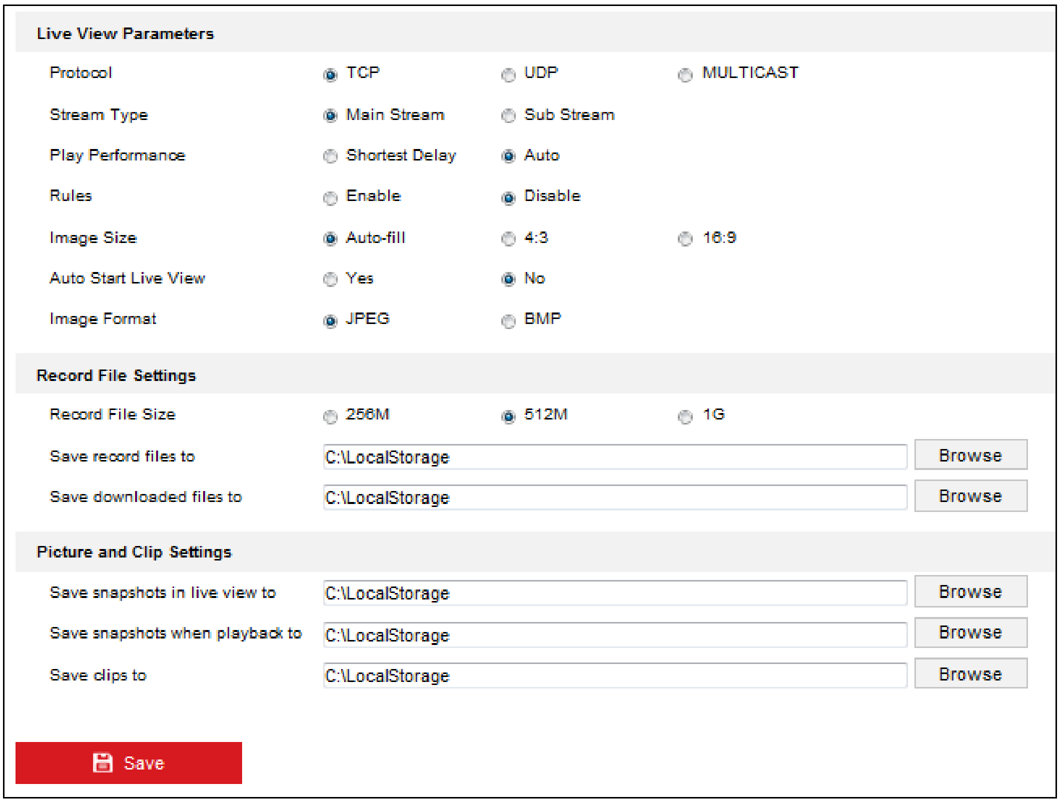
Figure 5. 8 PTZ Linking

Please refer to *Chapter 7.7 Configuring and Handling Alarms* for the PTZ Linking settings (Configuration>Event >Basic Event>Alarm Input>Linkage Method).

Chapter 6 Device Configuration

6.1 Local Configuration

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



Live View Parameters

Protocol	● TCP	○ UDP	○ MULTICAST
Stream Type	● Main Stream	○ Sub Stream	
Play Performance	○ Shortest Delay	● Auto	
Rules	○ Enable	● Disable	
Image Size	● Auto-fill	○ 4:3	○ 16:9
Auto Start Live View	○ Yes	● No	
Image Format	● JPEG	○ BMP	

Record File Settings

Record File Size	○ 256M	● 512M	○ 1G
Save record files to	C:\LocalStorage	Browse	
Save downloaded files to	C:\LocalStorage	Browse	

Picture and Clip Settings

Save snapshots in live view to	C:\LocalStorage	Browse
Save snapshots when playback to	C:\LocalStorage	Browse
Save clips to	C:\LocalStorage	Browse

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.

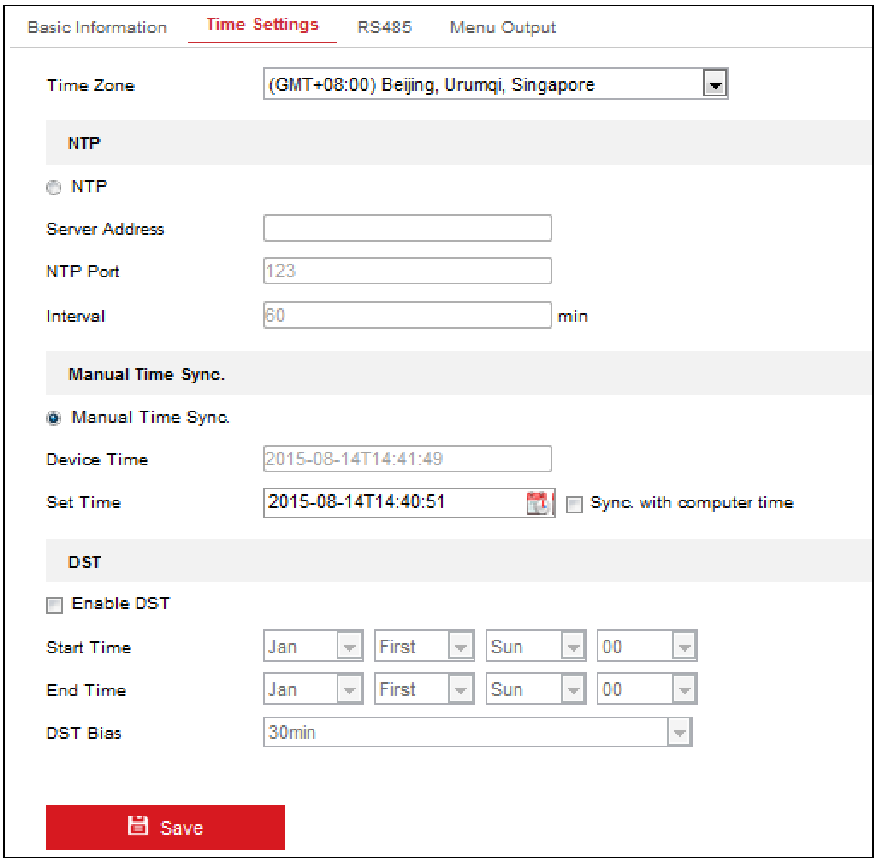
NOTE

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

6.2 System Time Settings

Steps:

1. Click **Configuration** > **System** > **System Settings** > **Time Settings** to enter the Time Settings interface:



Time Zone: (GMT+08:00) Beijing, Urumqi, Singapore

NTP

○ NTP

Server Address:

NTP Port: 123

Interval: 60 min

Manual Time Sync.

● Manual Time Sync.

Device Time: 2015-08-14T14:41:49

Set Time: 2015-08-14T14:40:51 □ Sync. with computer time

DST

□ Enable DST

Start Time: Jan First Sun 00

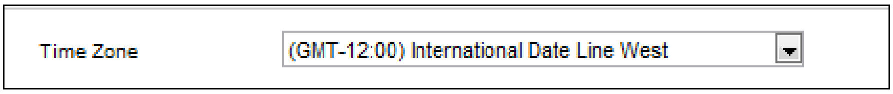
End Time: Jan First Sun 00

DST Bias: 30min

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.



Time Zone (GMT-12:00) International Date Line West

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.

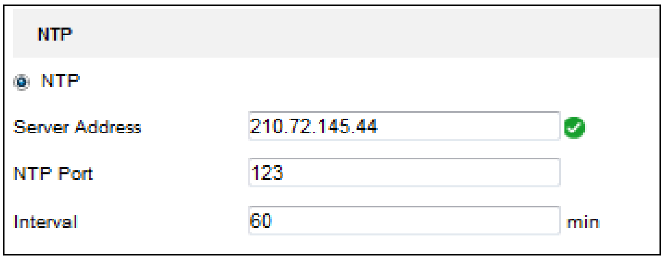
If the device is connected to a Dynamic Host Configuration Protocol (DHCP) network that has time server properties configured, the camera will synchronize automatically with the time server.

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.



NTP

● NTP

Server Address 210.72.145.44 ✓

NTP Port 123

Interval 60 min

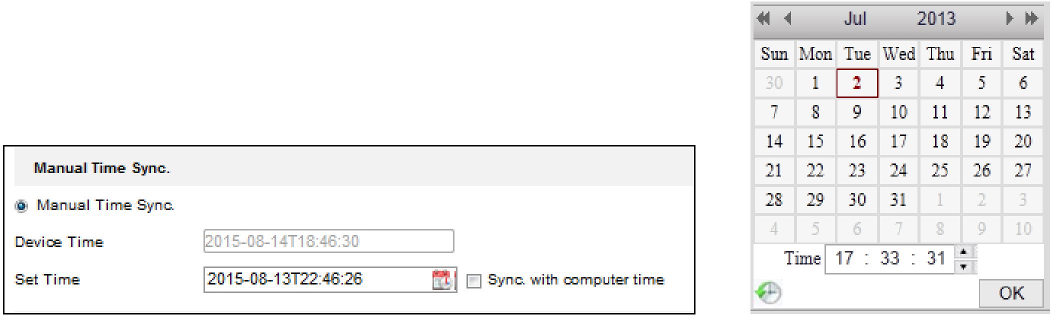
Figure 6. 4 Time Sync by NTP Server

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.



Manual Time Sync.

● Manual Time Sync.

Device Time 2015-08-14T18:46:30

Set Time 2015-08-13T22:46:26 □ Sync. with computer time

Jul 2013

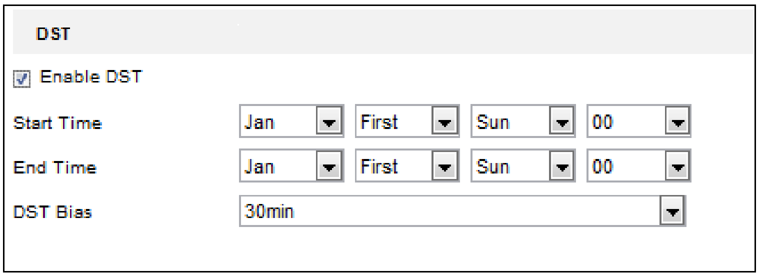
Sun	Mon	Tue	Wed	Thu	Fri	Sat
30	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31	1	2	3
4	5	6	7	8	9	10

Time 17 : 33 : 31

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.



DST

☑ Enable DST

Start Time: Jan, First, Sun, 00

End Time: Jan, First, Sun, 00

DST Bias: 30min

Figure 6. 6 DST Settings

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

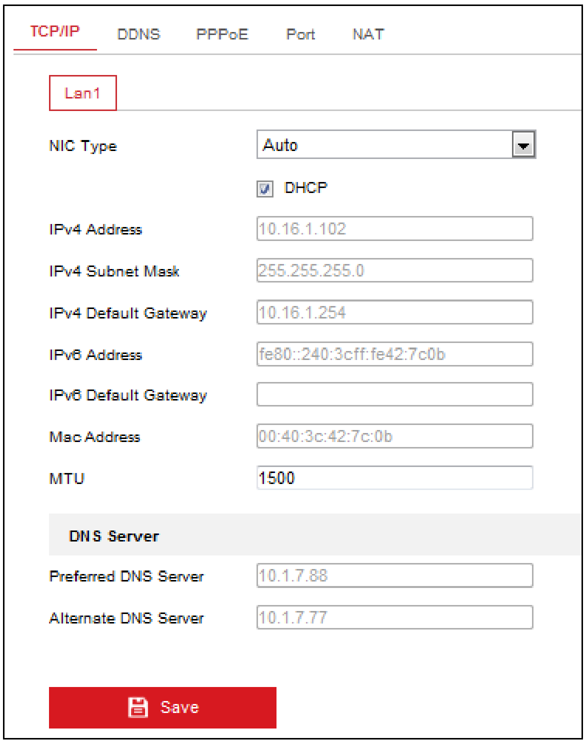
6.3 Network Settings

6.3.1 Configuring TCP/IP Settings

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

Steps:

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



NIC Type: Auto

☑ DHCP

IPv4 Address: 10.16.1.102

IPv4 Subnet Mask: 255.255.255.0

IPv4 Default Gateway: 10.16.1.254

IPv6 Address: fe80::240:3cff:fe42:7c0b

IPv6 Default Gateway:

Mac Address: 00:40:3c:42:7c:0b

MTU: 1500

DNS Server

Preferred DNS Server: 10.1.7.88

Alternate DNS Server: 10.1.7.77

Figure 6. 7 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.
5. Click the **Save** button to save the above settings.

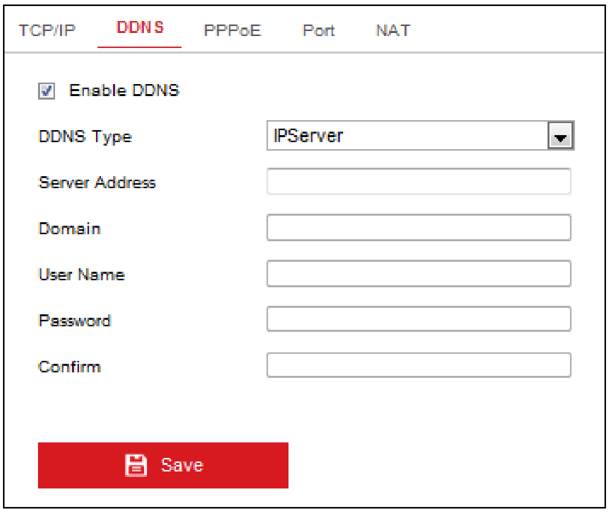
6.3.2 Configuring DDNS Settings

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 **Configuration** > **Network** > **Basic Settings** > **DDNS** to enter the DDNS Settings interface:



☑ Enable DDNS

DDNS Type: IPServer

Server Address:

Domain:

User Name:

Password:

Confirm:

Figure 6. 8 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, HiDDNS and NO-IP.

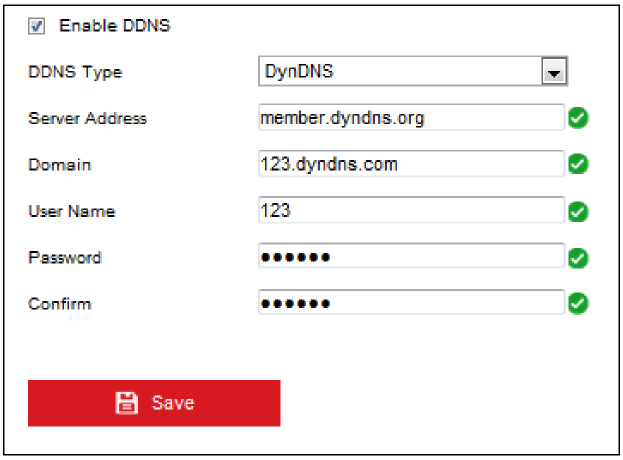
- **DynDNS:**

(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.



☑ Enable DDNS

DDNS Type: DynDNS

Server Address: member.dyndns.org ✓

Domain: 123.dyndns.com ✓

User Name: 123 ✓

Password: •••••• ✓

Confirm: •••••• ✓

Figure 6. 9 DynDNS Settings

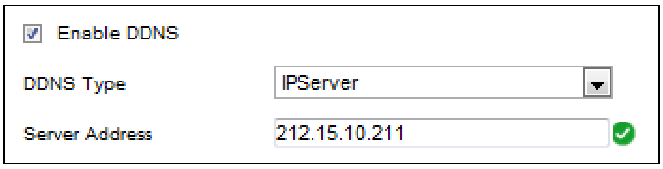
- **IPServer:**

(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.



☑ Enable DDNS

DDNS Type: IPServer

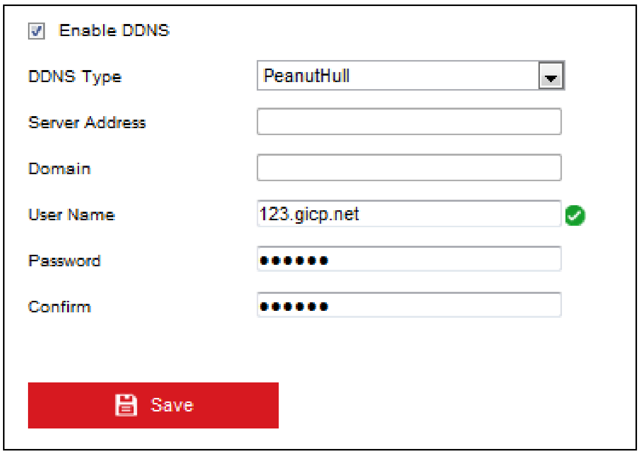
Server Address: 212.15.10.211 ✓

Figure 6. 10 IPServer Settings

- **PeanutHull:**

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

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



☑ Enable DDNS

DDNS Type: PeanutHull

Server Address:

Domain:

User Name: 123.gicp.net ✓

Password: ●●●●●●

Confirm: ●●●●●●

Figure 6. 11 PeanutHull Settings

- **HiDDNS:**

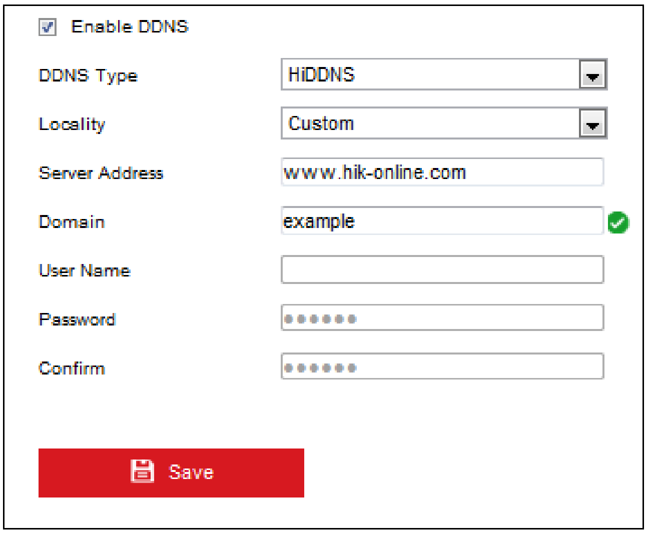
  (1) Enter the **Server Address** of the HiDDNS server: www.hik-online.com.

  (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.



☑ Enable DDNS

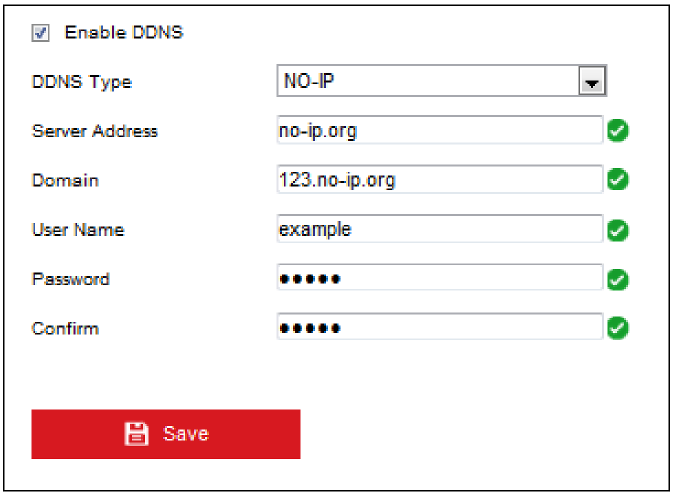
DDNS Type	HiDDNS
Locality	Custom
Server Address	www.hik-online.com
Domain	example ✓
User Name	
Password	••••••
Confirm	••••••

Figure 6. 12 HiDDNS Settings

- **NO-IP:**

  Enter the account information in the corresponding fields. Refer to the DynDNS settings.

  1) Enter **Server Address** for NO-IP.
  2) In the **Device Domain Name** text field, enter the domain obtained from the NO-IP website (www.no-ip.com).
  3) Enter the **User Name** and **Password** registered in the NO-IP website.
  4) Click **Save** to save the settings.



☑ Enable DDNS

DDNS Type	NO-IP
Server Address	no-ip.org ✓
Domain	123.no-ip.org ✓
User Name	example ✓
Password	••••• ✓
Confirm	••••• ✓

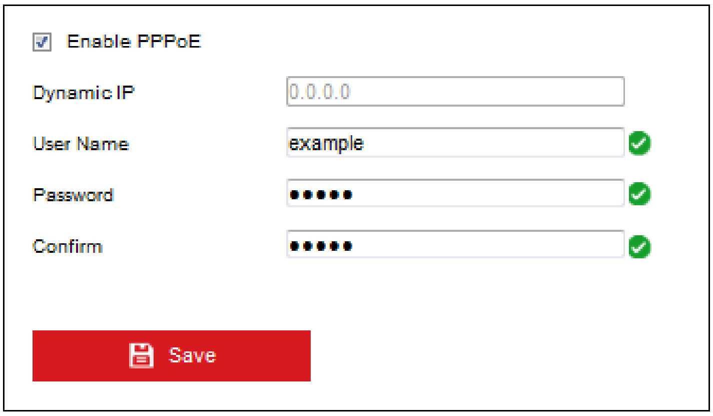
Figure 6. 13 NO-IP Settings Interface

6.3.3 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:



☑ Enable PPPoE

Dynamic IP: 0.0.0.0

User Name: example ✓

Password: ●●●●● ✓

Confirm: ●●●●● ✓

Figure 6. 14 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.

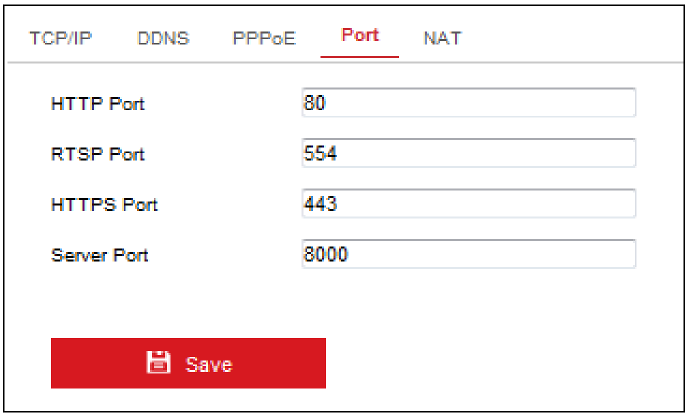
6.3.4 Configuring Port Settings

Purpose:

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

Steps:

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



HTTP Port: 80

RTSP Port: 554

HTTPS Port: 443

Server Port: 8000

Figure 6. 15 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.

6.3.5 Configuring NAT 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:

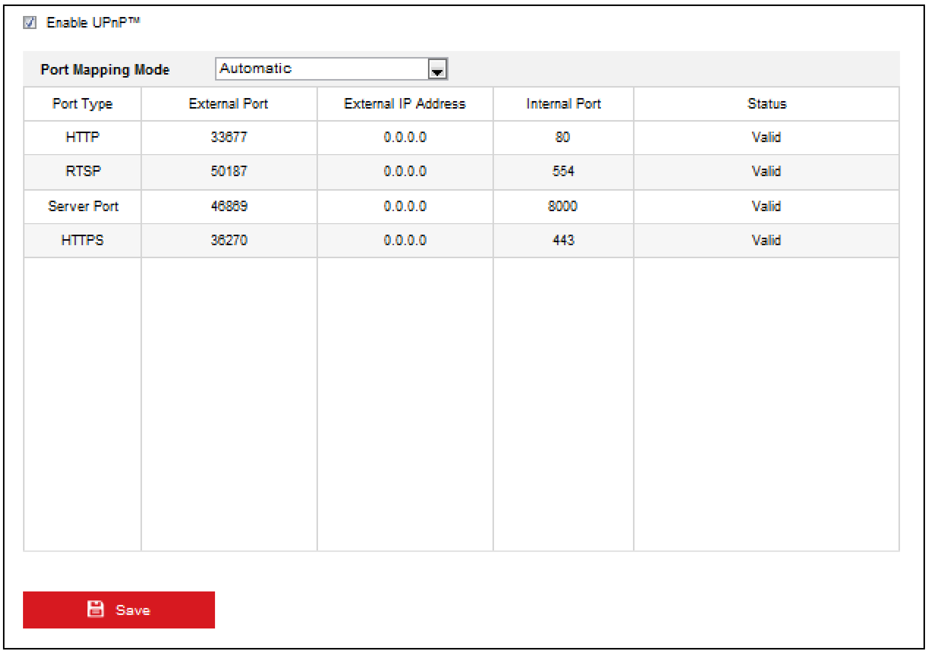
If you want to enable the UPnP™ function of the device, you must enable the UPnP™ function of the router to which your device is connected. When the network working mode of the device is set as multi-address, the Default Route of the device should be in the same network segment as that of the LAN IP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

Steps:

1. Click **Configuration > Network > Basic Settings > NAT** to enter the NAT settings interface.
2. Check the checkbox to enable the UPnP^{TM} 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.



☑ Enable UPnP™

Port Mapping Mode: Automatic

Port Type	External Port	External IP Address	Internal Port	Status
HTTP	33677	0.0.0.0	80	Valid
RTSP	50187	0.0.0.0	554	Valid
Server Port	46869	0.0.0.0	8000	Valid
HTTPS	36270	0.0.0.0	443	Valid

Figure 6. 16 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.

   NOTE

   - You can use the default port No., or change it according to actual requirements.

- 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.

6.3.6 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:

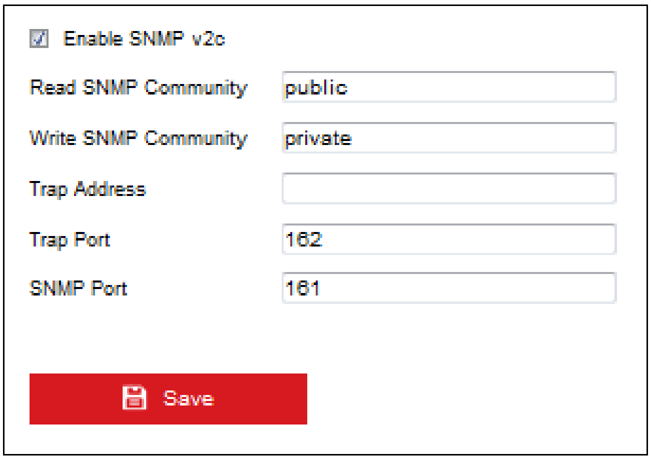
Before setting the SNMP, please download the SNMP software and manage to receive the device information via SNMP port. By setting the Trap Address, the device can send the alarm event and exception messages to the center.

NOTE

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

Steps:

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



☑ Enable SNMP v2c

Read SNMP Community	public
Write SNMP Community	private
Trap Address	
Trap Port	162
SNMP Port	161

Figure 6. 17 SNMP Settings (1)

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

6.3.7 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

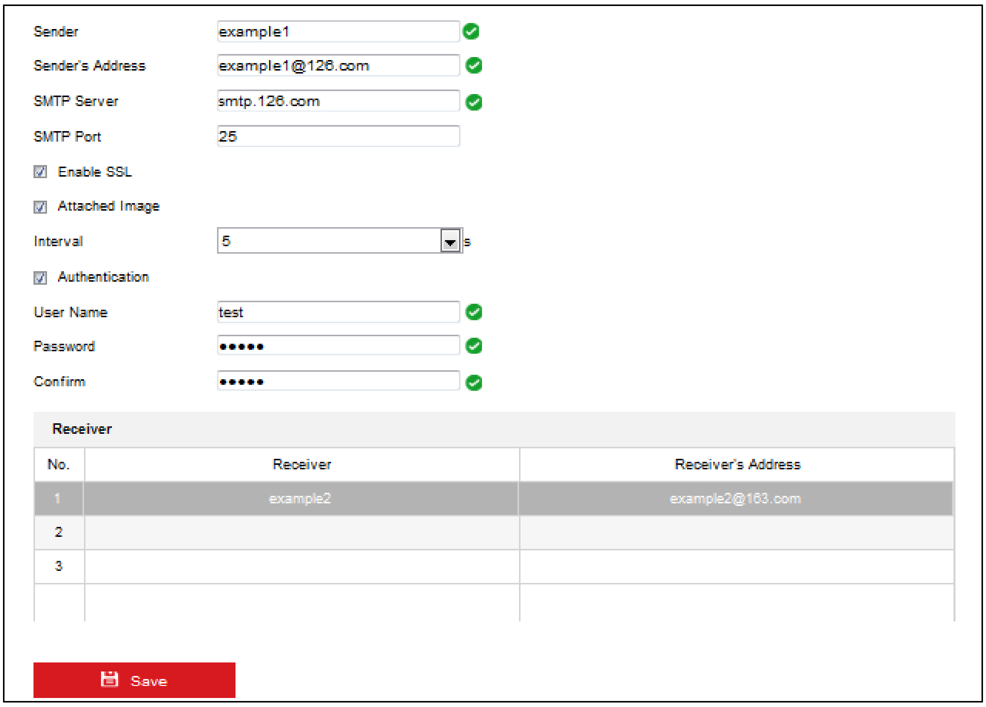
1. Before configuring the Email settings, the device must be connected to a local area network (LAN) that maintains an SMTP mail server. The network must also be connected to either an intranet or the Internet

depending on the location of the e-mail accounts to which you want to send notification.

2. Please configure the DNS Server settings under **Configuration** > **Network** > **Basic Settings** > **TCP/IP** before using the Email function.

Steps:

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



Sender: example1 ✓

Sender's Address: example1@126.com ✓

SMTP Server: smtp.126.com ✓

SMTP Port: 25

☑ Enable SSL

☑ Attached Image

Interval: 5 s

☑ Authentication

User Name: test ✓

Password: ••••• ✓

Confirm: ••••• ✓

Receiver

No.	Receiver	Receiver's Address
1	example2	example2@163.com
2		
3		

Figure 6. 18 Email Settings

3. Configure the following Email settings:

   Sender: The name of sender.

   Sender's Address: The Email address of sender.

   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 (optional): 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.

   Attached Image(optional): Check the checkbox of Attached Image if you want to send email with attached alarm images. Set the interval between two actions of sending attached pictures.

   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.

   Receiver: The name of user to be notified. Up to 3 receivers can be configured.

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

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 Video Tampering* Alarm and *Section Handling Exception.*

6.3.8 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.

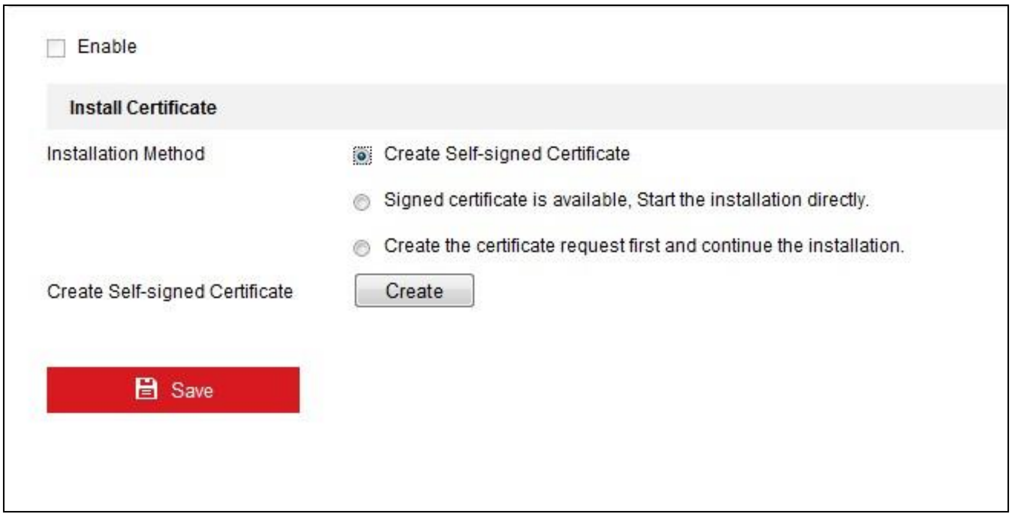
Steps:

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

- Create the self-signed certificate

(1) Select **Create Self-signed Certificate** as the Installation Method.

(2) Click **Create** button to enter the creation interface.



☐ Enable

Install Certificate

Installation Method: ● Create Self-signed Certificate
○ Signed certificate is available, Start the installation directly.
○ Create the certificate request first and continue the installation.

Create Self-signed Certificate: Create

Figure 6. 19 Create Self-signed Certificate

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

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

NOTE

If you already had a certificate installed, the Create Self-signed Certificate is grayed out.

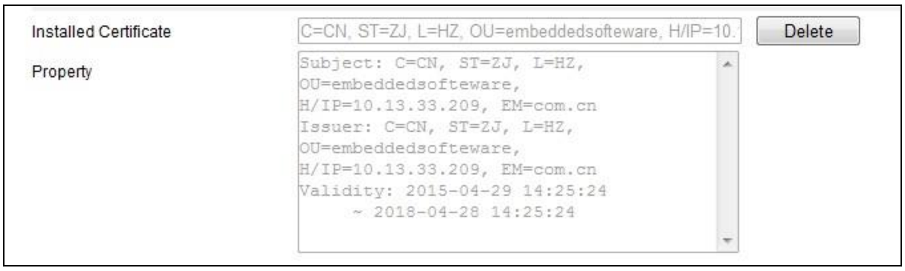
- Create the authorized certificate

(1) Select **Create the certificate request first and continue the installation** as the Installation Method.

(2) Click **Create** button to create the certificate request. Fill in the required information in the popup window.

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

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



Installed Certificate: C=CN, ST=ZJ, L=HZ, OU=embeddedsofteware, H/IP=10.

Property:

```
Subject: C=CN, ST=ZJ, L=HZ,
OU=embeddedsofteware,
H/IP=10.13.33.209, EM=com.cn
Issuer: C=CN, ST=ZJ, L=HZ,
OU=embeddedsofteware,
H/IP=10.13.33.209, EM=com.cn
Validity: 2015-04-29 14:25:24
    ~ 2018-04-28 14:25:24
```

Figure 6. 20 Installed Certificate

3. When you have successfully created and installed the certificate, check the checkbox of **Enable** to enable the HTTPS function.
4. Click the **Save** button to save the settings.

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.

6.3.9 Configuring Active Multicast

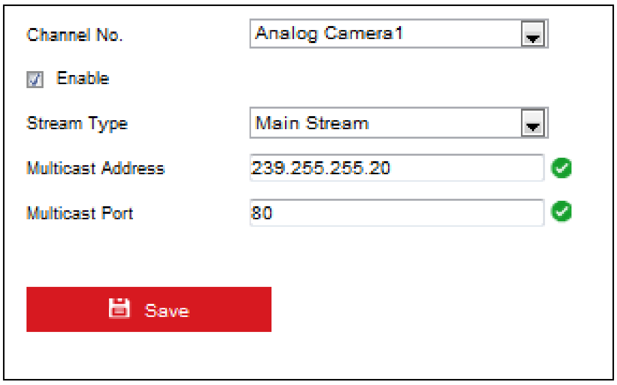
Purpose:

The active multicast address can be configured to realize live view for more than the maximum number of cameras through network, and after successful configuration, the device can actively send the stream to the multicast address.

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 **Configuration > Network > Advanced Settings >Active Multicast** to enter the active multicast address settings interface.



Channel No.: Analog Camera1

☑ Enable

Stream Type: Main Stream

Multicast Address: 239.255.255.20

Multicast Port: 80

Figure 6. 21 Multicast Address Setting

2. Select the camera to configure the multicast.
3. Check the checkbox of **Enable** to enable the feature.
4. Select the stream type to Main Stream or Sub Stream which is sent to the multicast address for live view.

5. Enter the active multicast address in the text filed.
6. Enter the multicast port (rang: 1-65535)
7. Click **Save** to save the settings.

NOTE

Reboot the device to activate the active multicast address settings.

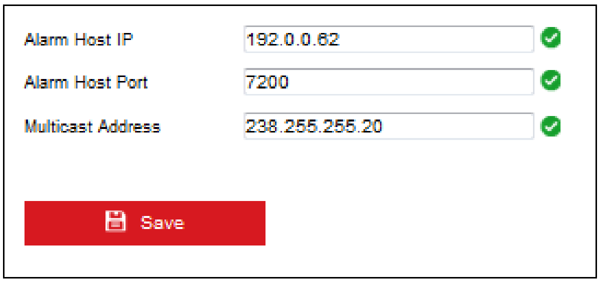
6.3.10 Configuring Remote Alarm Host and Multicast

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 **Configuration > Network > Advanced Settings > Other** to enter the alarm host settings interface.



Alarm Host IP 192.0.0.62 ✓

Alarm Host Port 7200 ✓

Multicast Address 238.255.255.20 ✓

Figure 6. 22 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. Enter the multicast address in the text filed.
4. Click **Save** to save the settings.

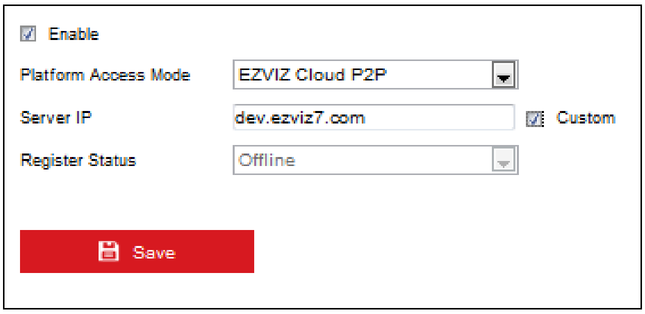
6.3.11 Configuring Platform Access

Purpose:

EZVIZ Cloud P2P provides the mobile phone application and as well the service platform page to access and manage your connected NVR, which enables you to get a convenient remote access to the video security system.

Steps:

1. Click **Configuration > Network > Advanced Settings > Platform Access** to enter platform access settings interface.
2. Check the **Enable** checkbox to activate this feature.
3. Select the EZVIZ Cloud P2P in the Platform Access Mode.
4. If required, select the checkbox of **Custom** and input the **Server Address**.



☑ Enable

Platform Access Mode: EZVIZ Cloud P2P

Server IP: dev.ezviz7.com ☑ Custom

Register Status: Offline

Figure 6. 23 EZVIZ Cloud P2P Settings

After configuration, you can access and manage the device by your mobile phone on which the EZVIZ Cloud P2P application is installed or by the EZVIZ website (www.ezviz7.com).

NOTE

For more operation instructions, please refer to the help file on the EZVIZ official website (www.ezviz7.com).

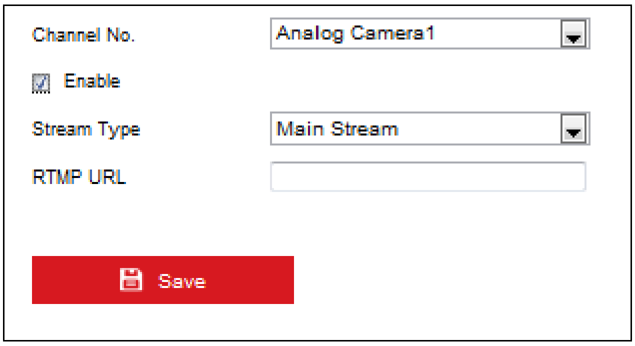
6.3.12 Configuring RTMP

Purpose:

The Real-Time Messaging Protocol (RTMP) was designed for high-performance transmission of audio, video, and data in Adobe Flash.

Steps:

1. Click **Configuration > Network > Advanced Settings >RTMP** to enter the RTMP settings interface.



Channel No.: Analog Camera1

☑ Enable

Stream Type: Main Stream

RTMP URL:

Figure 6. 24 RTMP Settings

2. Select the camera to configure the RTMP.
3. Check the checkbox of **Enable** to enable the feature.
4. Select the stream type to Main Stream or Sub Stream.
5. Enter the RTMP URL in the text field.
6. Click **Save** to save the settings.

Chapter 7 Camera Settings

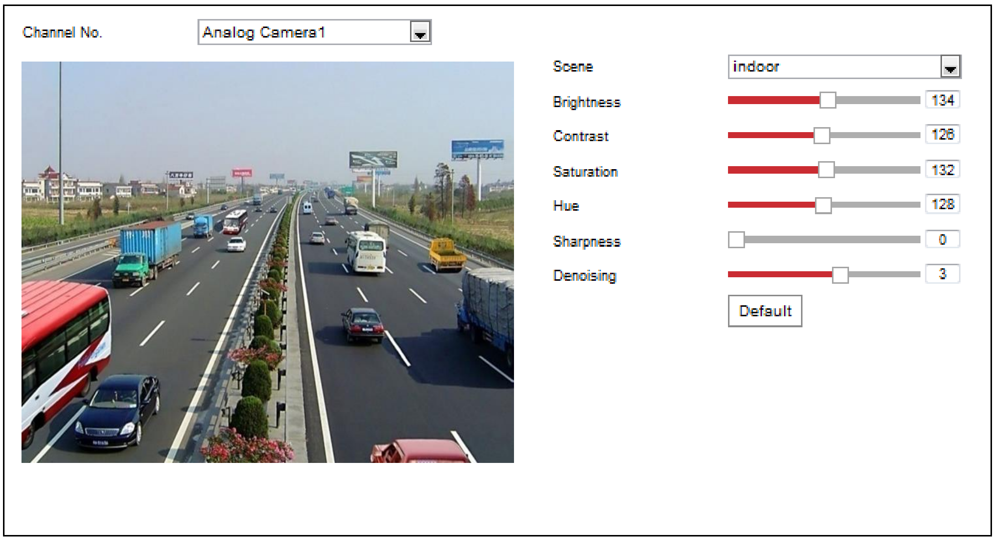
7.1 Configuring Display Parameters

Purpose:

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

Steps:

1. Click the **Configuration > Image> Display Settings** to enter the Display Settings interface:
2. Select the camera to configure the video parameters.
3. 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.



Channel No. Analog Camera1

Scene: indoor

Brightness: 134

Contrast: 126

Saturation: 132

Hue: 128

Sharpness: 0

Denoising: 3

Figure 7. 1 Video Parameters Settings

4. 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.
5. 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.

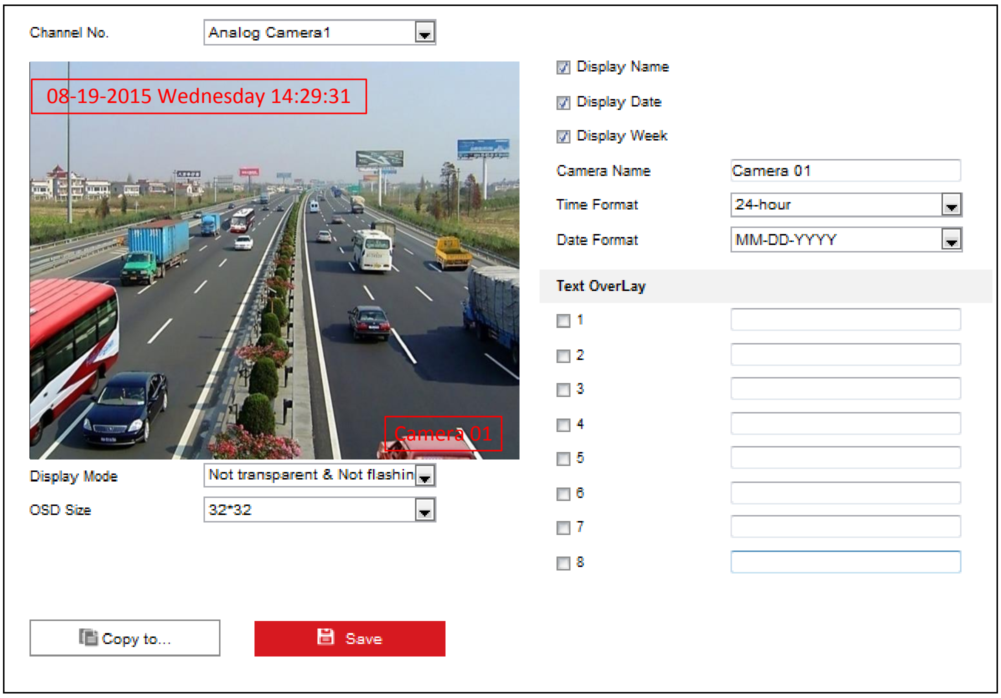
7.2 Configuring OSD Settings

Purpose:

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

Steps:

1. Click the **Configuration > Image>OSD Settings** to enter the OSD Settings interface:



Channel No. Analog Camera1

☑ Display Name

☑ Display Date

☑ Display Week

Camera Name: Camera 01

Time Format: 24-hour

Date Format: MM-DD-YYYY

Text OverLay

□ 1

□ 2

□ 3

□ 4

□ 5

□ 6

□ 7

□ 8

Display Mode: Not transparent & Not flashin

OSD Size: 32*32

Figure 7. 2 Display Settings

2. Select the camera from the drop-down list to configure the OSD settings.
3. Select the display of camera name, date or week by checking the checkboxes if required.
4. Edit the camera name in the text field of Camera Name.
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.

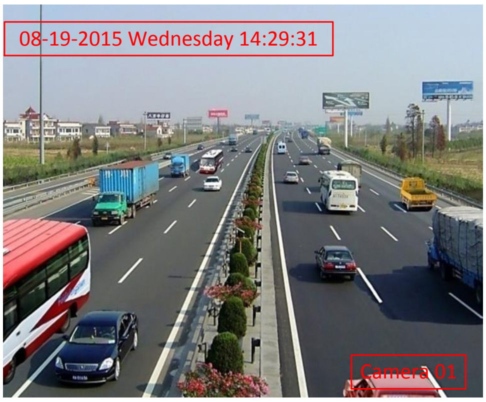
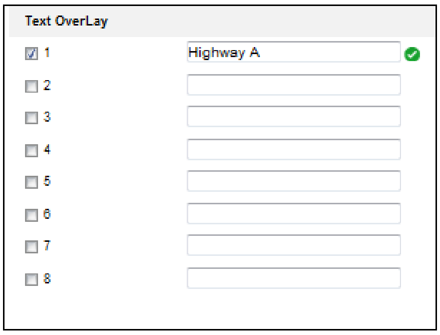


Figure 7. 3 Adjust OSD Location

7. Edit the user-defined text content.

1) Click the checkbox in the text box below and then input the characters. Up to 8 character strings can be edited.



Text OverLay

☑ 1	Highway A ✓
☐ 2	
☐ 3	
☐ 4	
☐ 5	
☐ 6	
☐ 7	
☐ 8	

Figure 7. 4 Configure Text Overlay

2) Click **Save**, and the edited text is shown on the image.

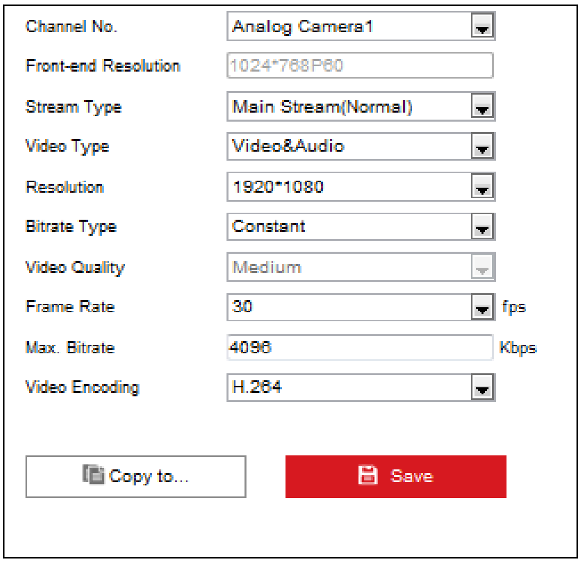
3) On the preview image, you can adjust the Text location on the screen by moving the text frame

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

7.3 Configuring Video Settings

Steps:

1. Click **Configuration > Video/Audio > Video** to enter the Video Settings interface.



Channel No.	Analog Camera1	
Front-end Resolution	1024*768P60	
Stream Type	Main Stream(Normal)	
Video Type	Video&Audio	
Resolution	1920*1080	
Bitrate Type	Constant	
Video Quality	Medium	
Frame Rate	30	fps
Max. Bitrate	4096	Kbps
Video Encoding	H.264	

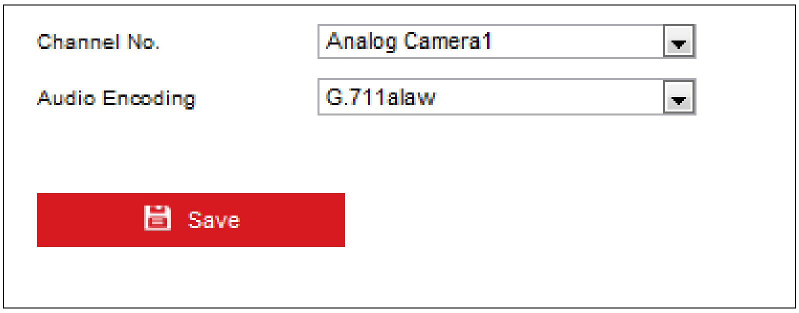
Figure 7. 5 Video Settings

2. Select the camera from the drop-down list to configure. The resolution of the camera will be shown in the field of Front-end Resolution.
3. 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.
4. 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.
   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 from 1fps to full frame.
   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 32Kbps~16Mbps.
   Video Encoding: Select the video encoding standard to H.264.
5. Click **Save** to save the above settings.

7.4 Configuring Audio Settings

Steps:

1. Click **Configuration > Video/Audio > Audio** to enter the Audio Settings interface.



Channel No. Analog Camera1

Audio Encoding G.711alaw

2. Select the camera from the drop-down list to configure.
3. Select the audio encoding format to G.711alaw, G.711μlaw or AAC.
4. Click **Save** to save the above settings.

7.5 Configuring Target Cropping

Purpose:

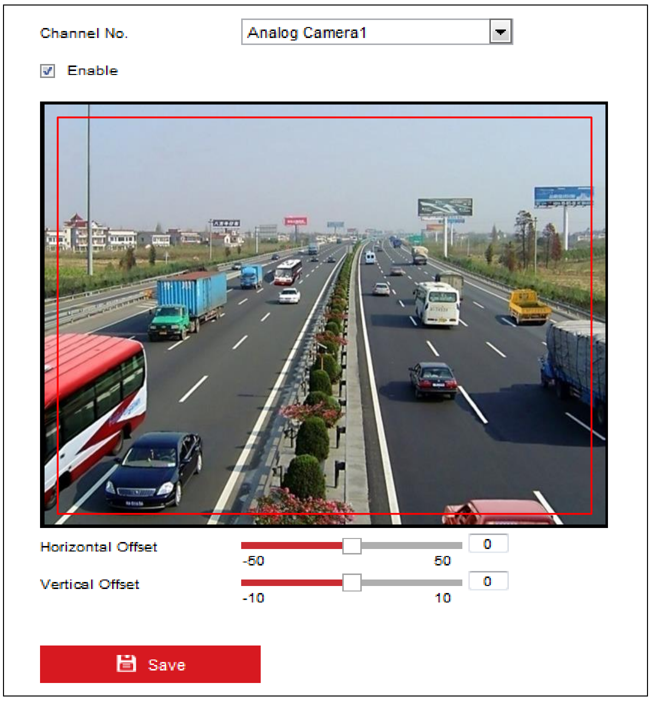
When image of the HDMI/VGA video input is off position or has dark edges, you can use the target cropping function to specify a rectangle on the live video to remain the demanded image area.

NOTE

Target cropping function varies according to different camera models.

Steps:

1. **Configuration > Video/Audio > Target Cropping** to enter the **Target Cropping** settings interface.
2. Check the **Enable** checkbox to enable the function.



Channel No. Analog Camera1

☑ Enable

Horizontal Offset -50 50 0

Vertical Offset -10 10 0

Figure 7. 6 Target Cropping

3. Select the cropping resolution for the video display of target area. A red rectangle is displayed on the live video to mark the target area, and you can click-and-drag the rectangle to locate the target area as desired.
4. Click **Save** to save the settings.

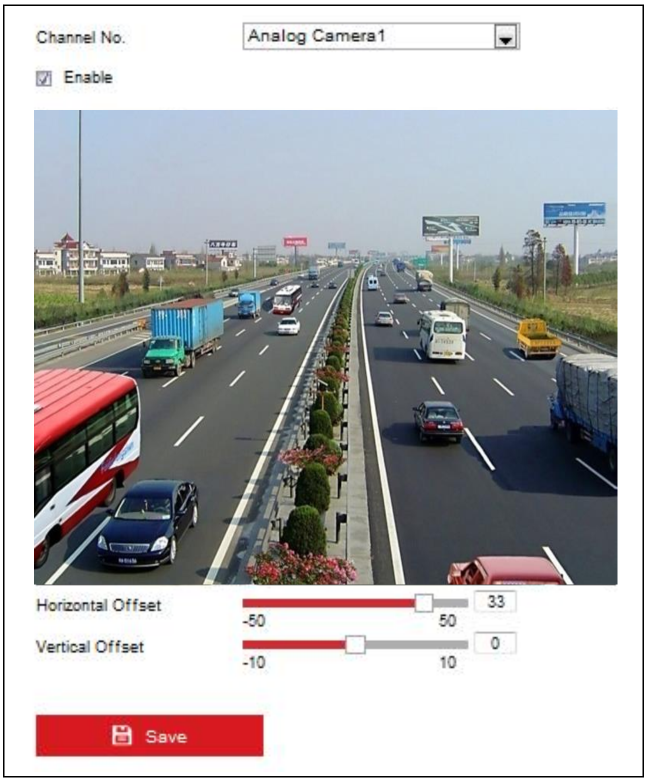
7.6 Adjusting VGA Output Position

Purpose:

You can adjust VGA input video to the desired position by configuring the horizontal and vertical offset values.

Steps:

1. **Configuration > Video/Audio > VGA Position Adjustment** to enter the VGA Position Adjustment settings interface.
2. Check the **Enable** checkbox to enable the function.



Channel No. Analog Camera1

☑ Enable

Horizontal Offset 33 (-50 to 50)

Vertical Offset 0 (-10 to 10)

Figure 7. 7 VGA Position Adjustment

3. Adjust the horizontal position of the VGA input video by moving the slider bar of Horizontal Offset (range: -50 to 50).
4. Adjust the vertical position of the VGA input video by moving the slider bar of Vertical Offset value (range: -10 to 10).
5. Click **Save** to save the settings.

7.7 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 Send Email and Trigger Alarm Output.

7.7.1 Configuring Motion Detection

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

Steps:

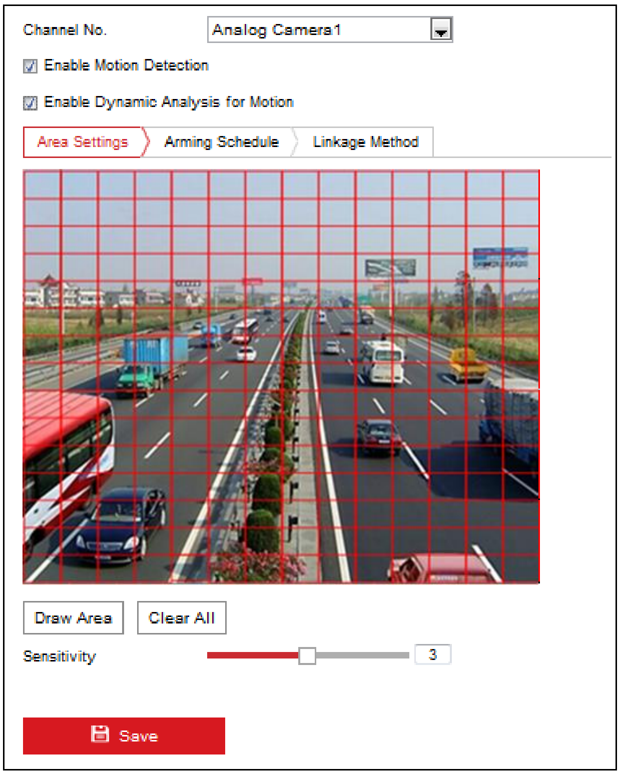
1. **Set the Motion Detection Area**

   Steps:

   (1) Click **Configuration> Event > Basic Event > Motion** to enter the motion detection settings interface.

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

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



Channel No. Analog Camera1

☑ Enable Motion Detection

☑ Enable Dynamic Analysis for Motion

Sensitivity 3

Figure 7. 8 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 **Draw Area** 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 **Stop Drawing** button to finish drawing.

You can click the **Clear All** button to clear all areas.

(7) Move the slide bar of Sensitivity to set the sensitivity of the camera.

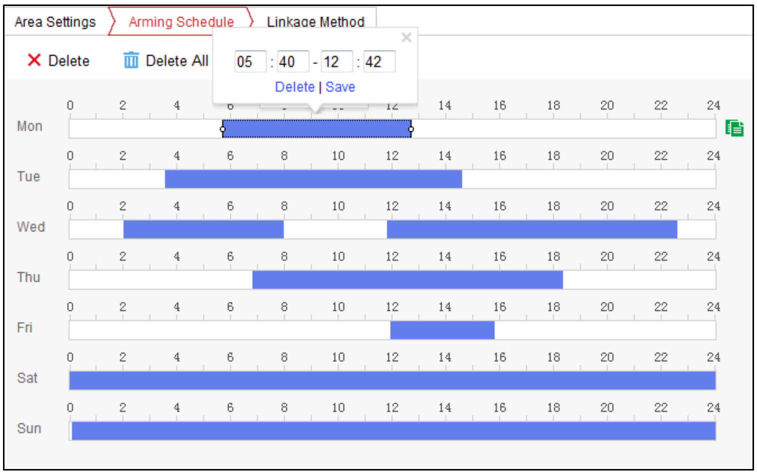
(8) Click **Save** button to save the settings.

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

Steps:

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

(2) Click on the time bar and drag the mouse to select the time period.



05 : 40 - 12 : 42

Figure 7. 9 Motion Detection-Arming Time Settings

NOTE

Click on the selected time period, you can adjust the time period to the desired time by either moving the time bar or input the exact time period.

(3) (Optional) Click Delete to delete the current arming schedule, or click Save to save the settings.

(4) Move the mouse to the end of each day, a copy dialogue box pops up, and you can copy the current settings to other days.

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

NOTE

The time of each period can’t be overlapped. Up to 8 periods can be configured for each day.

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

Purpose:

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

Steps:

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

(2) Select the alarming linkage method(s).

- **Audible Warning**

  Trigger an audible beep when an alarm is detected.

- **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**

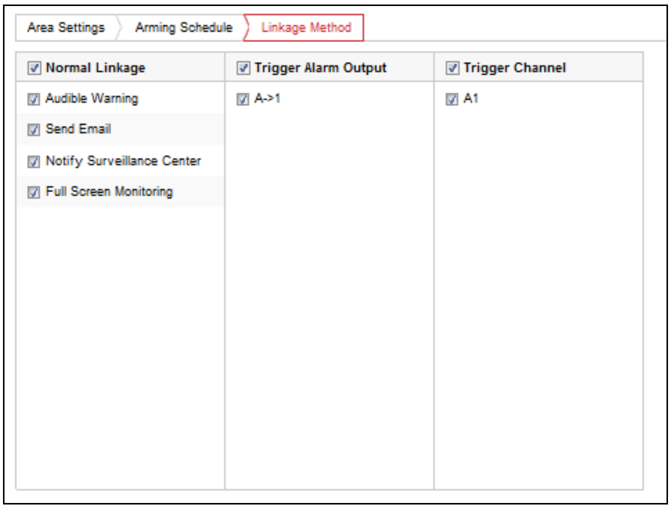
Send an email with alarm information to a user or users when an event occurs.

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 *Section6.3.6 Configuring Email Settings.*

- **Upload to FTP**

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



Area Settings | Arming Schedule | Linkage Method

☑ Normal Linkage	☑ Trigger Alarm Output	☑ Trigger Channel
☑ Audible Warning	☑ A->1	☑ A1
☑ Send Email		
☑ Notify Surveillance Center		
☑ Full Screen Monitoring		

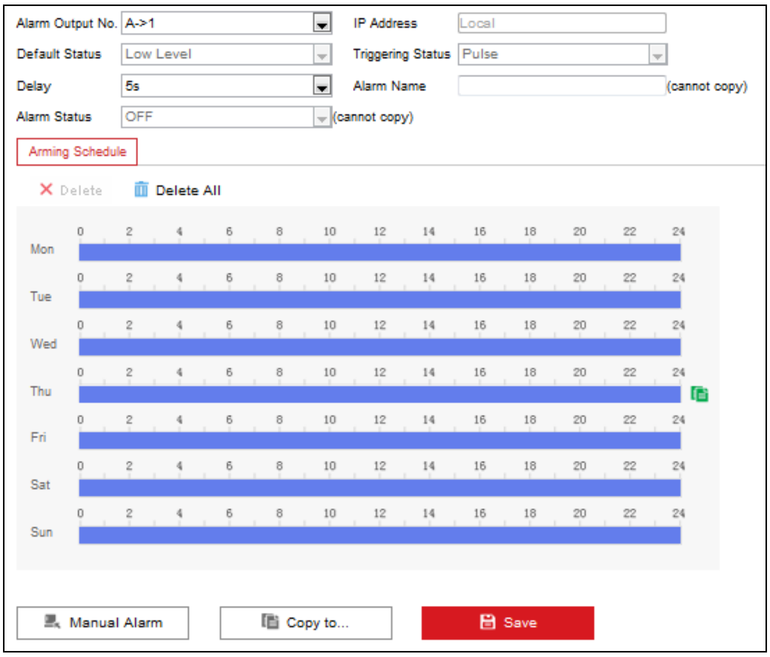
Figure 7. 10 Motion Detection-Linking Method

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

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 **Configuration> Event > Basic Event > Alarm Output** to enter the Alarm Output Settings interface.



Alarm Output No. A->1

IP Address Local

Default Status Low Level

Triggering Status Pulse

Delay 5s

Alarm Name (cannot copy)

Alarm Status OFF (cannot copy)

Figure 7. 11 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 on the time bar and drag the mouse to select the time period. 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.*

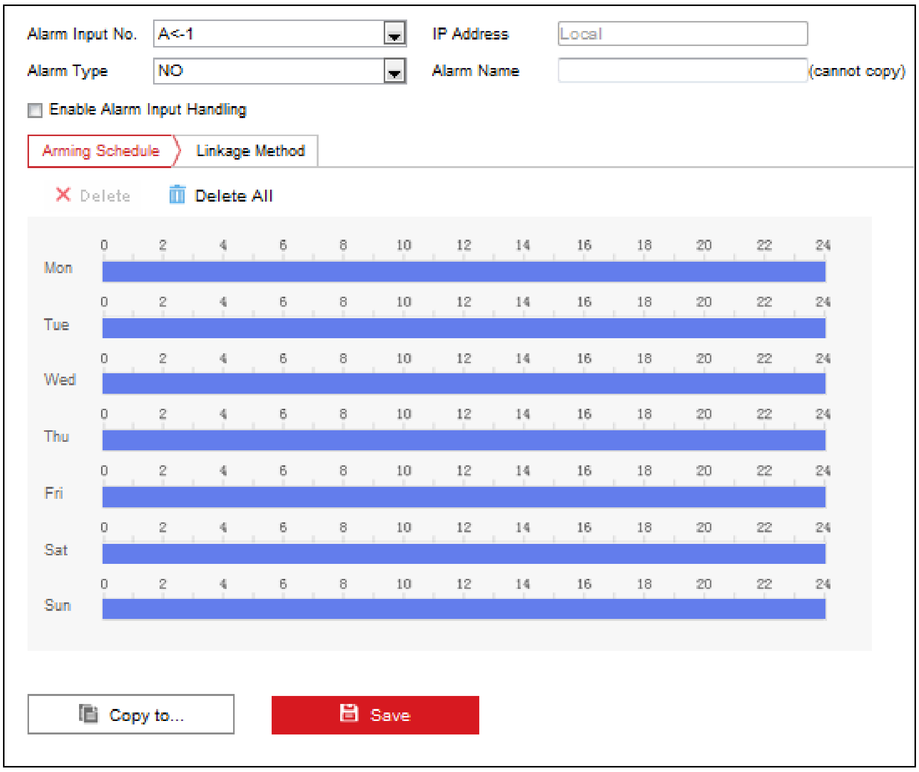
5) Return to the Alarm Output Settings interface and click **Save** to save the settings.

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

7.7.2 Configuring External Alarm Input

Steps:

1. Click **Configuration> Event > Basic Event > 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).



Alarm Input No. A<-1

IP Address Local

Alarm Type NO

Alarm Name (cannot copy)

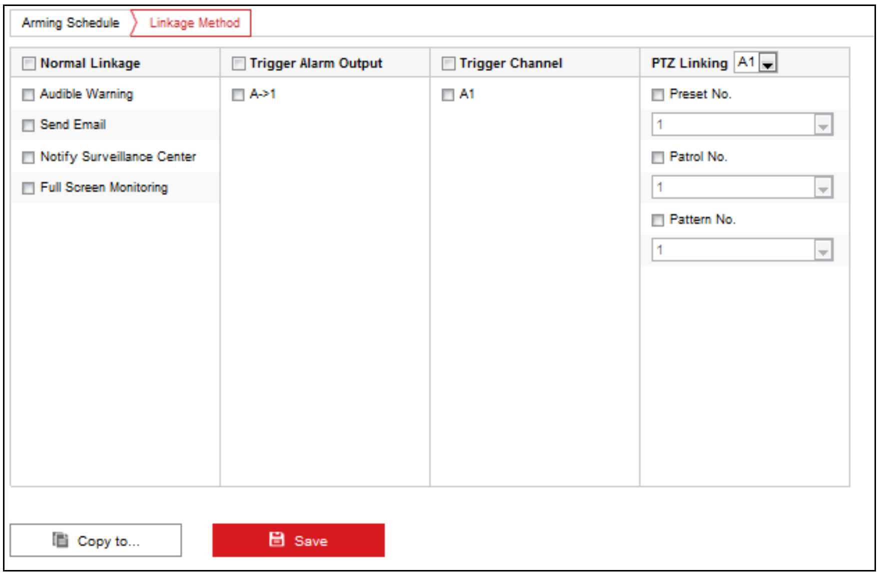
☐ Enable Alarm Input Handling

Figure 7. 12 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*.



☐ Normal Linkage	☐ Trigger Alarm Output	☐ Trigger Channel	PTZ Linking A1
☐ Audible Warning	☐ A->1	☐ A1	☐ Preset No.
☐ Send Email			1
☐ Notify Surveillance Center			☐ Patrol No.
☐ Full Screen Monitoring			1
			☐ Pattern No.
			1

Figure 7. 13 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.

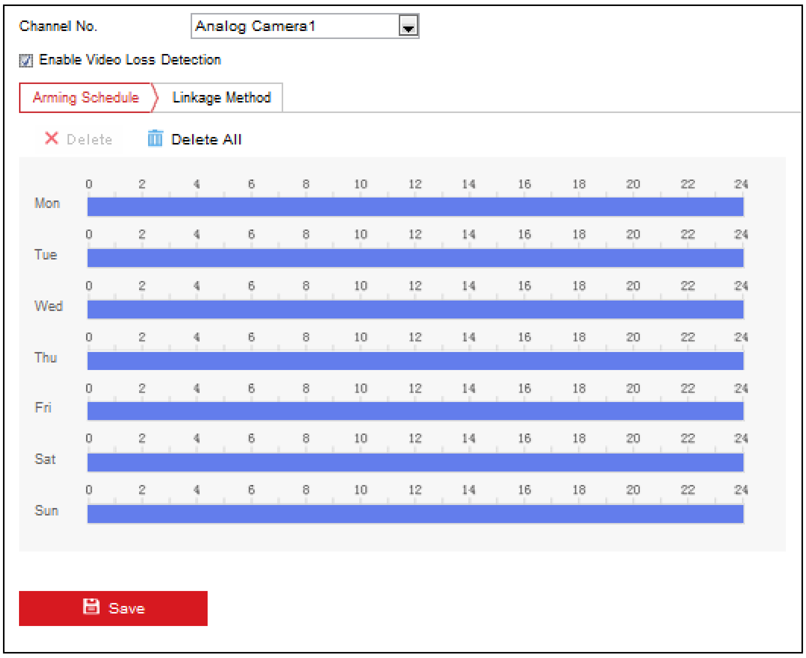
7. You can copy your settings to other alarm inputs.

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

7.7.3 Configuring Video Loss Alarm

Steps:

1. Click **Configuration> Event** > **Basic Event** > **Video Loss** to enter the video loss alarm setting interface.



Channel No. Analog Camera1

☑ Enable Video Loss Detection

Figure 7. 14 Video Loss Alarm Settings

2. Select the camera to configure the video loss alarm.

3. Check the checkbox of **Enable Video Loss**.

4. Configure 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*.

7.7.4 Configuring Video Tampering Alarm

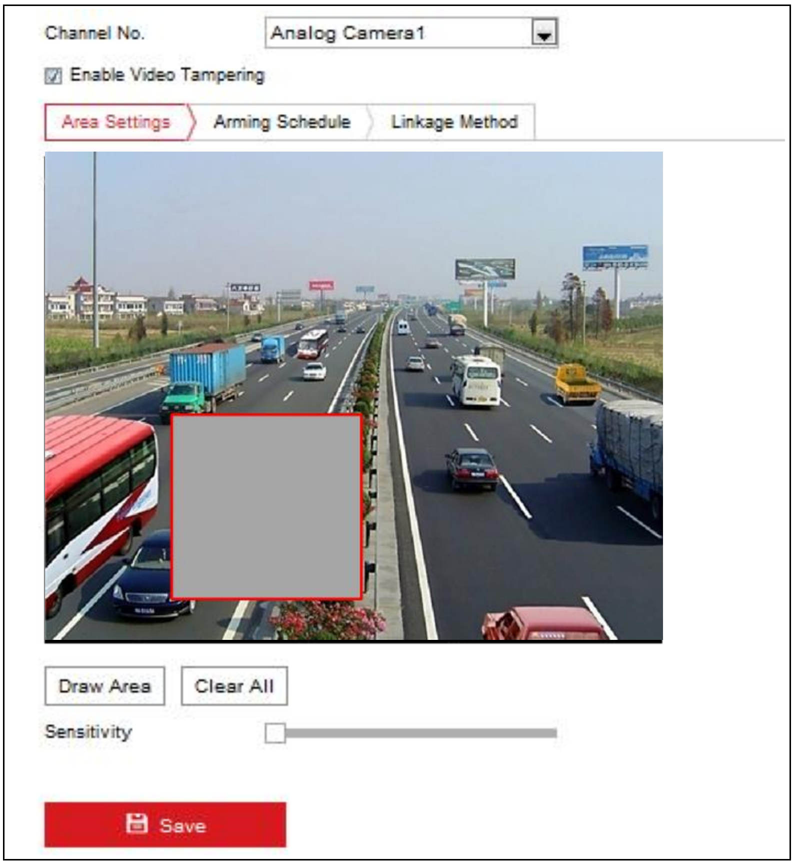
Purpose:

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

Steps:

1. Click **Configuration> Event** > **Basic Event** > **Tamper-proof** to enter the Video Tampering Settings interface.

2. Select the camera to configure the video tampering detection alarm.



Channel No. Analog Camera1

☑ Enable Video Tampering

Figure 7. 15 Video Tampering Alarm Settings

3. Click checkbox of **Enable Video Tampering**.

4. Set the video tampering detection area. Please refer to *Step 1 Set the Motion Detection Area* in *Chapter 8.3.1.*

5. Configure the arming schedule for video tampering 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.*

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.*

7.7.5 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 exception and video resolution mismatch.

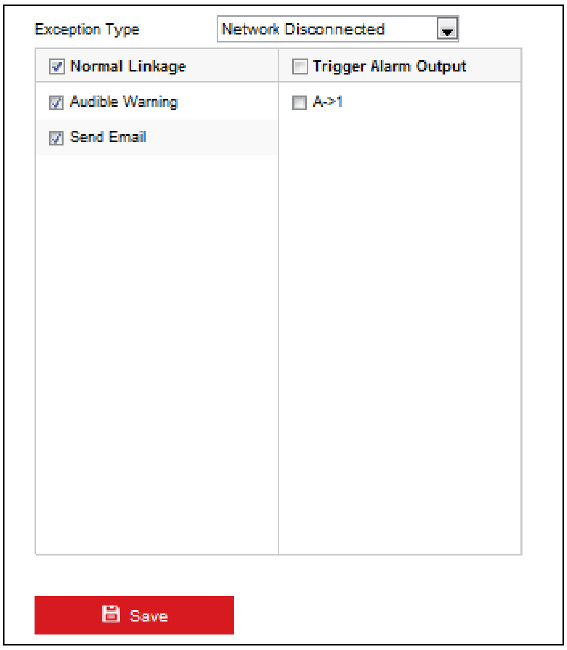
NOTE

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

Steps:

1. Click **Configuration> Event > Basic Event > 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.*



Exception Type: Network Disconnected

☑ Normal Linkage
☑ Audible Warning
☑ Send Email

□ Trigger Alarm Output
□ A->1

Figure 7. 16 Handling Exceptions

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

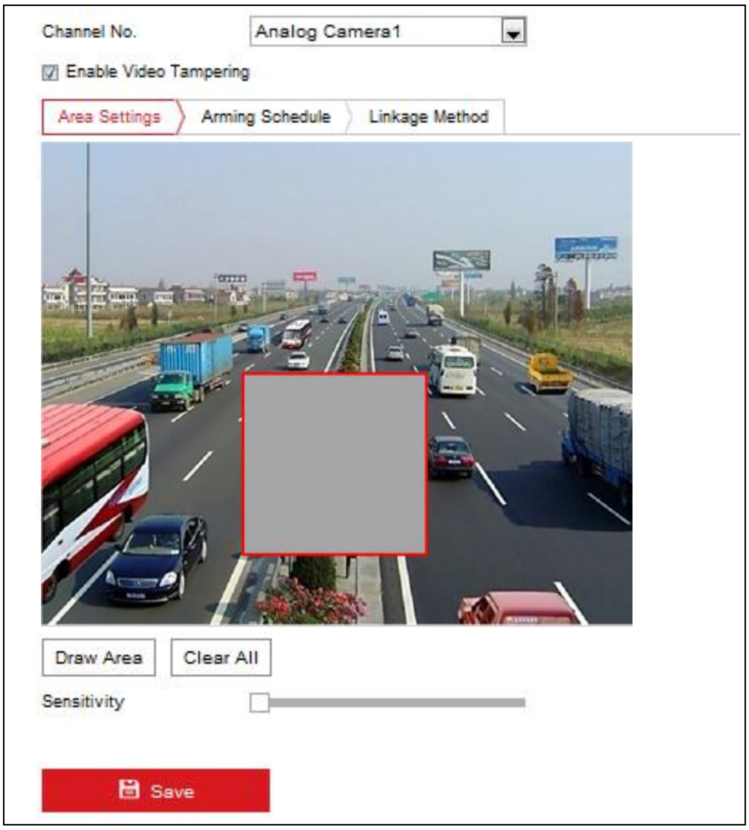
7.8 Configuring Privacy Mask

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** > **Image** > **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.



Channel No. Analog Camera1

☑ Enable Video Tampering

Figure 7. 17 Privacy Mask Settings

4. Click the **Draw Area** 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 **Stop Drawing** button to finish drawing.

   You can click the **Clear All** button to clear all of the areas you set without saving it.

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

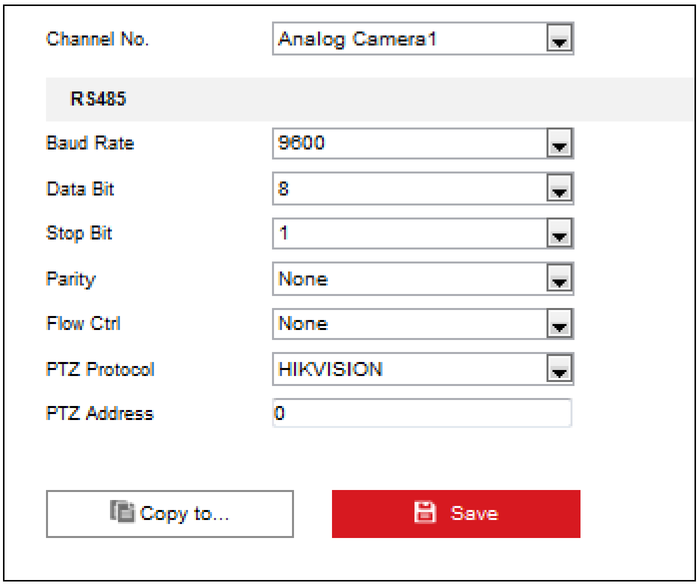
7.9 Configuring RS-485 Settings

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 **Configuration** > **System** > **System Settings**> **RS485** to enter RS-485 port setting interface:



Channel No. Analog Camera1

RS485

Baud Rate 9600

Data Bit 8

Stop Bit 1

Parity None

Flow Ctrl None

PTZ Protocol HIKVISION

PTZ Address 0

Figure 7. 18 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 Storage Configuration

8.1 Adding Network Disk

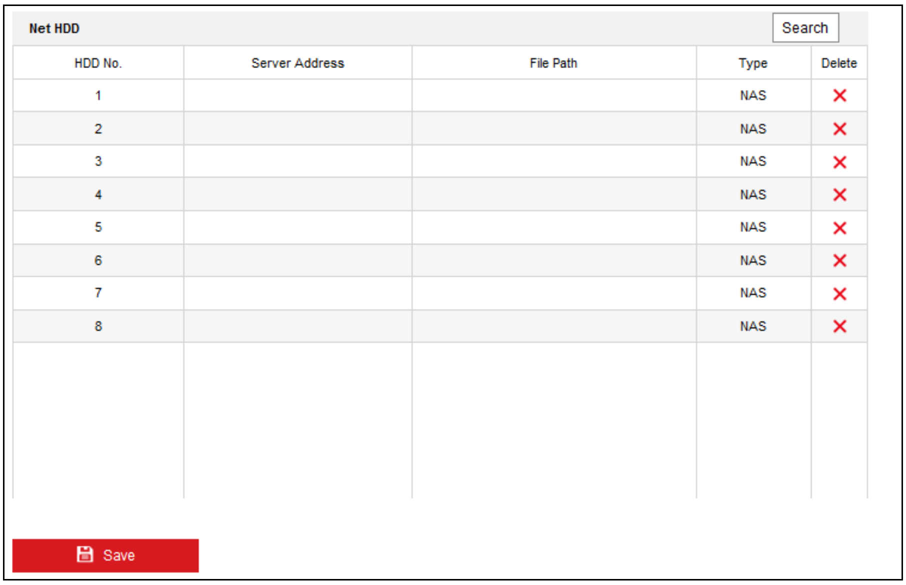
You must configure the network disk before operating the recording, playback or log searching.

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 **Configuration** > **Storage** > **Storage Management** > **Net HDD** to enter the network disk settings interface.



Net HDD

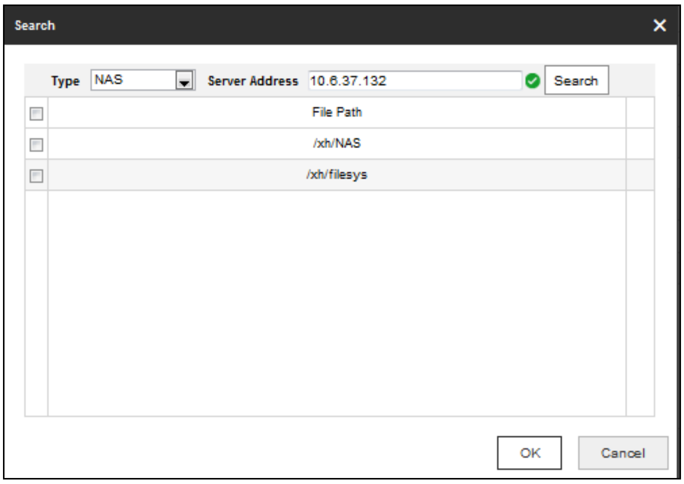
Search

HDD No.	Server Address	File Path	Type	Delete
1			NAS	✕
2			NAS	✕
3			NAS	✕
4			NAS	✕
5			NAS	✕
6			NAS	✕
7			NAS	✕
8			NAS	✕

Save

Figure 8. 1 Net HDD Settings Interface

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.



Search

Type: NAS   Server Address: 10.6.37.132

□	File Path
□	/xh/NAS
□	/xh/filesys

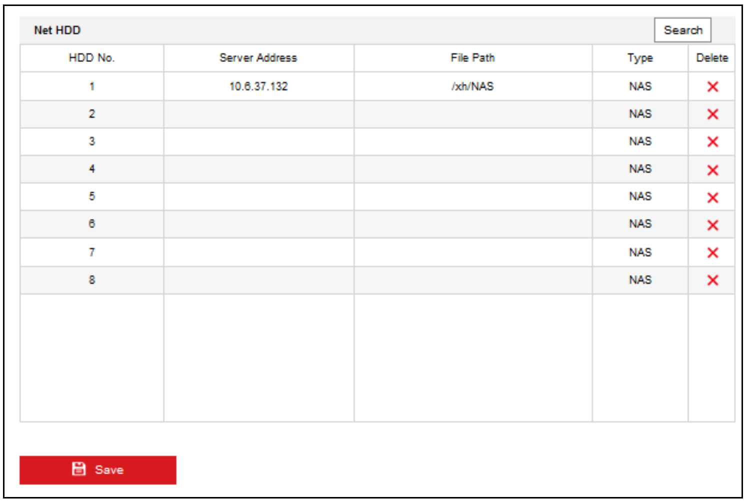
Figure 8. 2 Search Network Disk

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.

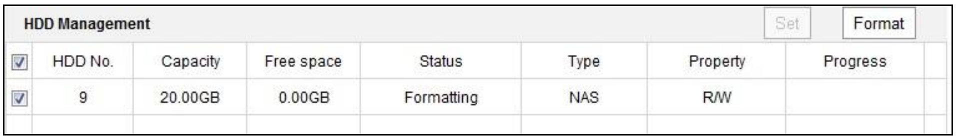


Net HDD

HDD No.	Server Address	File Path	Type	Delete
1	10.6.37.132	/xh/NAS	NAS	✕
2			NAS	✕
3			NAS	✕
4			NAS	✕
5			NAS	✕
6			NAS	✕
7			NAS	✕
8			NAS	✕

Figure 8. 3 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.**



HDD Management

☑	HDD No.	Capacity	Free space	Status	Type	Property	Progress
☑	9	20.00GB	0.00GB	Formatting	NAS	R/W	

Figure 8. 4 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.

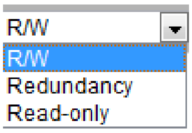


Figure 8. 5 Set HDD Property

NOTE

- 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.

8.2 Record Settings

Before you start

Make sure the Encoder is connected with network disk or micro SD card, and the disk or card has been initialized for the first time to use.

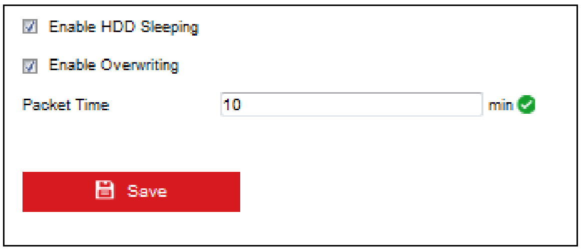
Two recording types can be configured: Manual and Scheduled. The following section introduces the configuration of scheduled record/capture.

8.2.1 Configuring Packet Time of Recording

The recorded file is packed in 512M by default. You can also customize the packet time in the advanced settings page.

Steps:

1. Click **Configuration> Storage > Advanced Settings > Other** to enter the following interface.



☑ Enable HDD Sleeping

☑ Enable Overwriting

Packet Time 10 min

Figure 8. 6 Record File Settings

2. Set the size of the recorded file.
3. Click **Save** to save the settings.

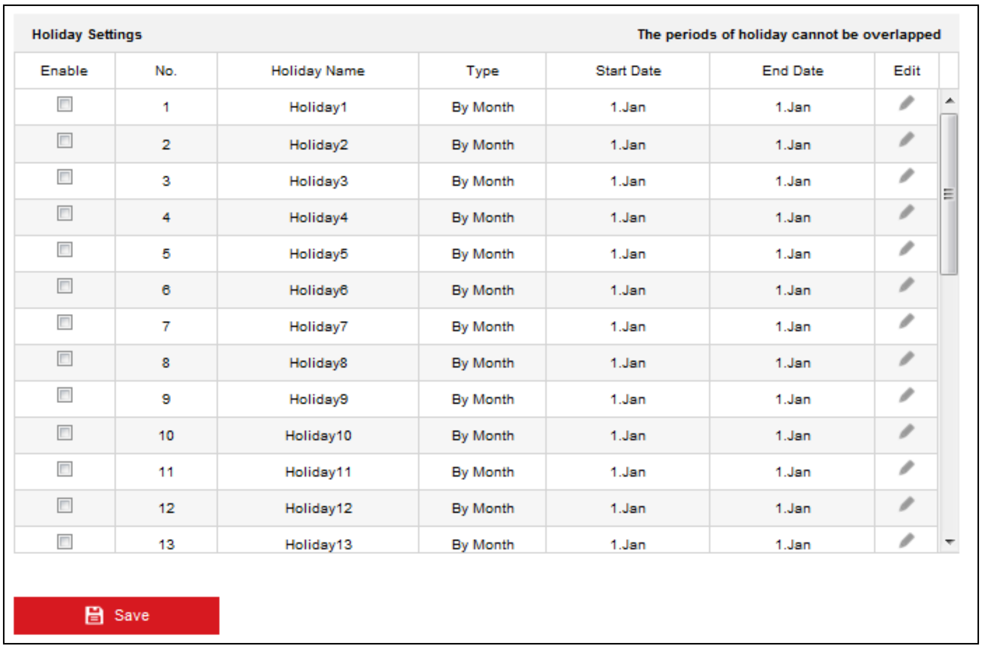
8.2.2 Configuring Holiday Settings

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 **Configuration> Storage > Advanced Settings > Holiday** to enter holiday settings interface.



Holiday Settings

The periods of holiday cannot be overlapped

Enable	No.	Holiday Name	Type	Start Date	End Date	Edit
□	1	Holiday1	By Month	1.Jan	1.Jan	✎
□	2	Holiday2	By Month	1.Jan	1.Jan	✎
□	3	Holiday3	By Month	1.Jan	1.Jan	✎
□	4	Holiday4	By Month	1.Jan	1.Jan	✎
□	5	Holiday5	By Month	1.Jan	1.Jan	✎
□	6	Holiday6	By Month	1.Jan	1.Jan	✎
□	7	Holiday7	By Month	1.Jan	1.Jan	✎
□	8	Holiday8	By Month	1.Jan	1.Jan	✎
□	9	Holiday9	By Month	1.Jan	1.Jan	✎
□	10	Holiday10	By Month	1.Jan	1.Jan	✎
□	11	Holiday11	By Month	1.Jan	1.Jan	✎
□	12	Holiday12	By Month	1.Jan	1.Jan	✎
□	13	Holiday13	By Month	1.Jan	1.Jan	✎

Figure 8. 7 Holiday Settings

2. Select an item from the list and click ✎ to edit the holiday.

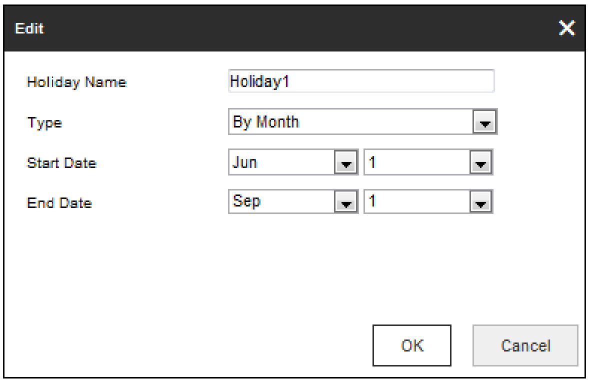
(1) Edit the holiday name.

(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.



Edit

Holiday Name: Holiday1

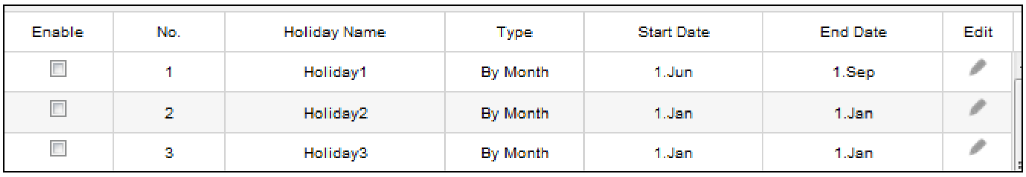
Type: By Month

Start Date: Jun 1

End Date: Sep 1

Figure 8. 8 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.



Enable	No.	Holiday Name	Type	Start Date	End Date	Edit
□	1	Holiday1	By Month	1.Jun	1.Sep	✎
□	2	Holiday2	By Month	1.Jan	1.Jan	✎
□	3	Holiday3	By Month	1.Jan	1.Jan	✎

Figure 8. 9 List of Holidays

NOTE

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

8.2.3 Configuring Scheduled Recording

Configuring Record Scheduled

Steps:

1. Click **Configuration** > **Storage** > **Schedule Settings** > **Record Schedule** to enter record schedule settings interface.
2. Select the camera to configure the record schedule.
3. Check the checkbox of **Enable** to enable the record schedule.
4. Select a Record Type from the drop-down menu. The record type can be Continuous, Motion, Alarm, Motion & Alarm, Motion | Alarm and Smart.
   - **Continuous**

     If you select **Continuous**, the video will be recorded automatically according to the time of the schedule.
   - **Record Triggered by Motion Detection**

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

     Besides configuring the record 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 Triggered by Alarm**

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

     Besides configuring the record 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 Triggered by Motion & Alarm**

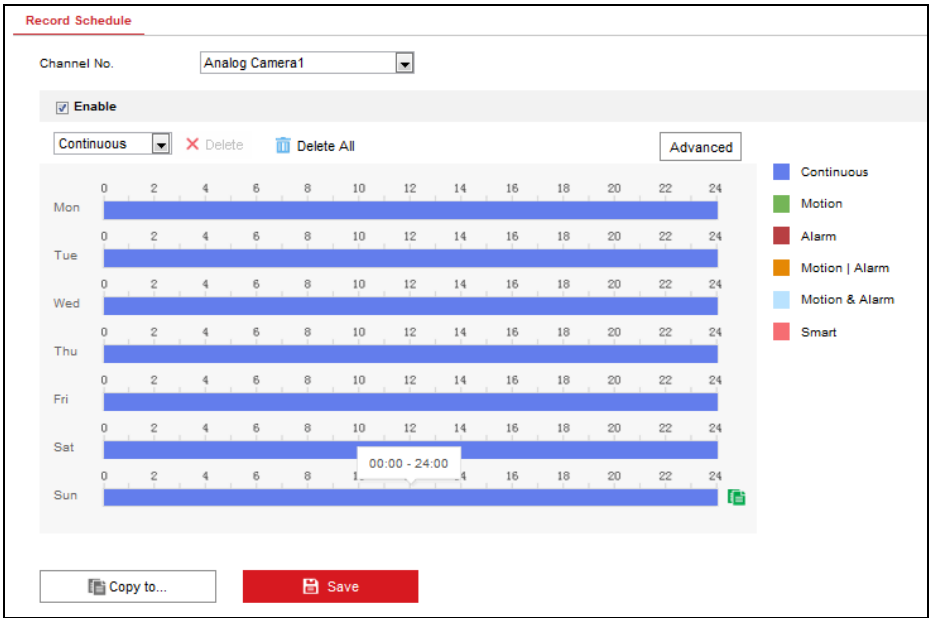
     If you select **Motion & Alarm**, the video will be recorded when the motion and alarm are triggered at the same time.

     Besides configuring the record schedule, you have to configure the settings on the **Motion Detection** and **Alarm Input Settings** interfaces.
   - **Record Triggered by Motion | Alarm**

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

     Besides configuring the record schedule, you have to configure the settings on the **Motion Detection** and **Alarm Input Settings** interfaces.
   - **Record Triggered by Smart**

     If you select **Smart**, the video will be recorded if any of the events is triggered. Besides configuring the recording schedule, you have to configure the event settings.



Record Schedule

Channel No. Analog Camera1

☑ Enable

Continuous | ✕ Delete | Delete All | Advanced

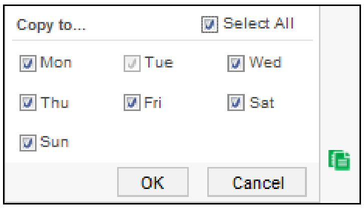
Figure 8. 10 Configure Record Schedule

5. Click and drag the mouse on the timeline of each day to set the period of the selected recording type.

NOTE

The time of each period can’t be overlapped. Up to 8 periods can be configured.

6. After having configured one day, you can move the mouse to end of the timeline and click 📋 to copy the schedule settings of the current day to other days of the week or to all week days.



Copy to... ☑ Select All

☑ Mon ☑ Tue ☑ Wed

☑ Thu ☑ Fri ☑ Sat

☑ Sun

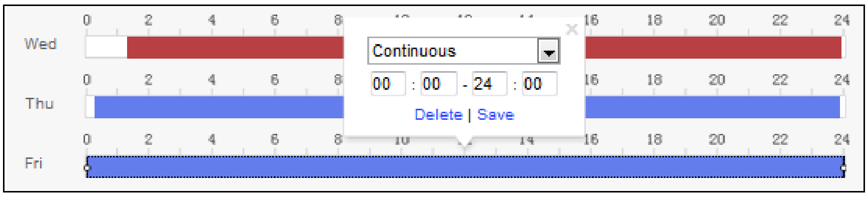
Figure 8. 11 Copy Schedule Settings

Editing/Deleting the Record Schedule

You can edit or delete the configured record schedule on the Record Schedule interface.

Task 1: Editing the Record Schedule

1. For the configured record schedule, you can click the timeline of a day to edit the start time/end time and the recording type.
2. Click **Save** to save the settings.



Continuous

00 : 00 - 24 : 00

Figure 8. 12 Edit the Record Schedule

Task 2: Deleting the Record Schedule

Click a segment on the time line configured with record schedule, and click the **Delete** from the pop-up configuration box or click the ✕ Delete to delete the selected record schedule of a day.

You can also click Delete All to clear the record schedule settings of all days.

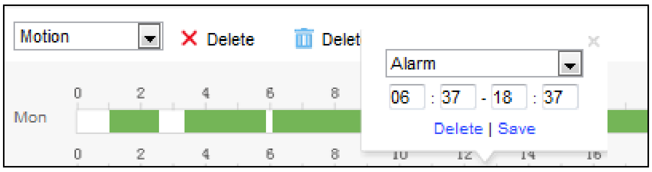
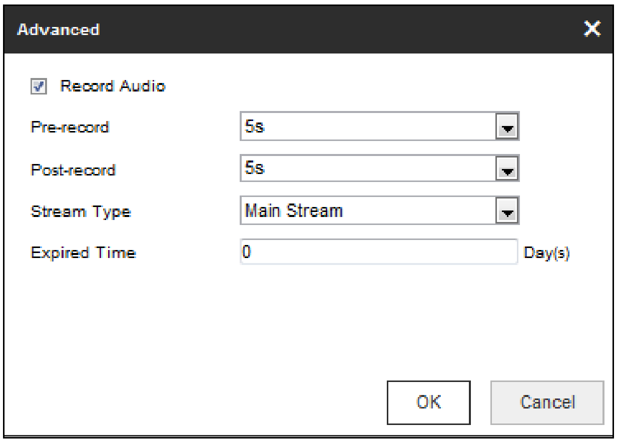


Figure 8. 13 Delete the Record Schedule

Configuring Advanced Record Settings

1. Click **Configuration** > **Storage** > **Schedule Settings** > **Record Schedule** to enter record schedule settings interface.
2. Click **Advanced** to configure the advanced record parameters**.**
   - **Record Audio:** Enable or disable the audio record.
   - **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.
   - **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.



☑ Record Audio

Pre-record 5s

Post-record 5s

Stream Type Main Stream

Expired Time 0 Day(s)

Figure 8. 14 Edit Schedule

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

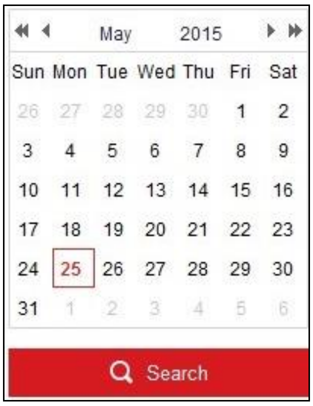
Chapter 9 Playback

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



May 2015

Sun	Mon	Tue	Wed	Thu	Fri	Sat
26	27	28	29	30	1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31	1	2	3	4	5	6

Search

Figure 9. 1 Select a Date for Playback

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

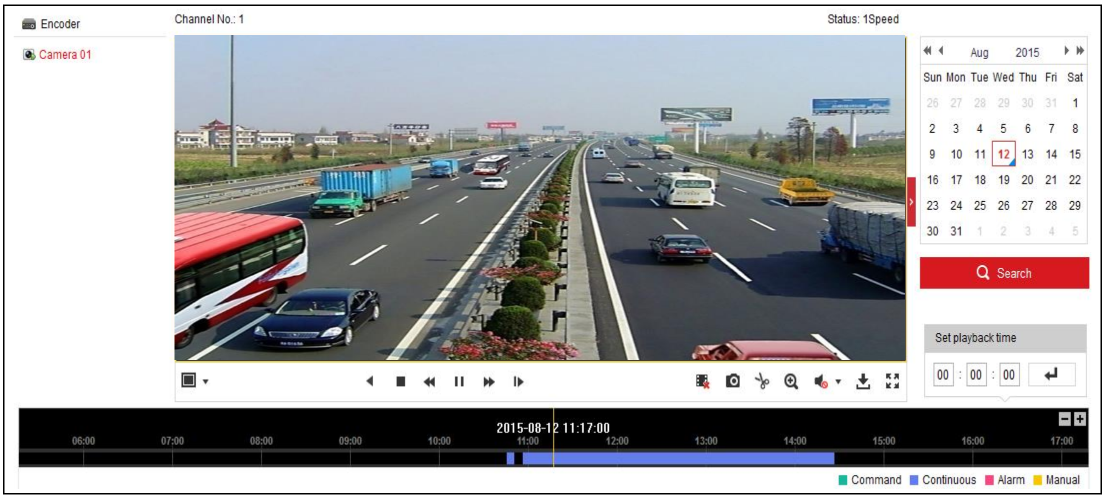


Figure 9. 2 Playback Interface

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

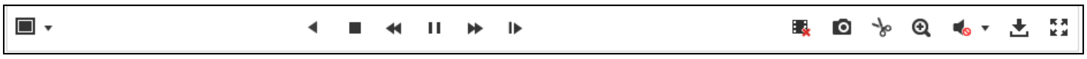


Figure 9. 3 Playback Toolbar

Table 1-1 Description of the buttons

Button	Operation	Button	Operation
◀	Reversed Play	📷	Capture a picture
▶/■	Stop	✂/✂	Start/Stop clipping video files
❚❚	Pause	🔊 ━━○━━━ / 🔇	Audio on and adjust volume/Mute
⏪	Speed down	⬇	Download
⏩	Speed up	❚▶	Playback by frame
🔍/🔍	Enable/Disable digital zoom	⛶	Switch to full-screen playback mode.
⊞ ▾	Select the window-division mode		

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

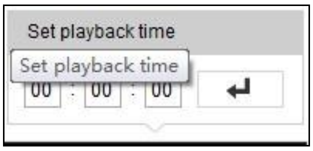


Figure 9. 4 Set the Playback Time

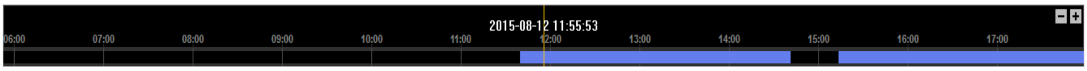


Figure 9. 5 Playback Timeline

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

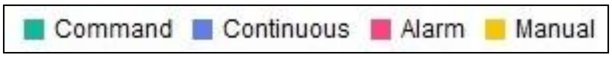
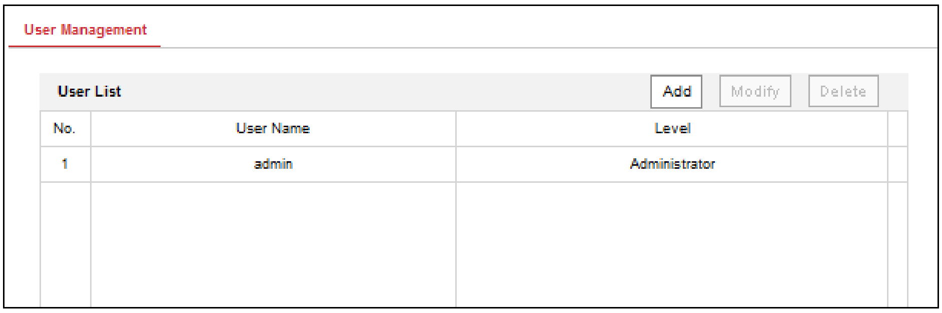


Figure 9. 6 Video Types

Chapter 10 Managing User Accounts

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



No.	User Name	Level
1	admin	Administrator

Figure 10. 1 User Information Interface

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

10.1 Adding a User

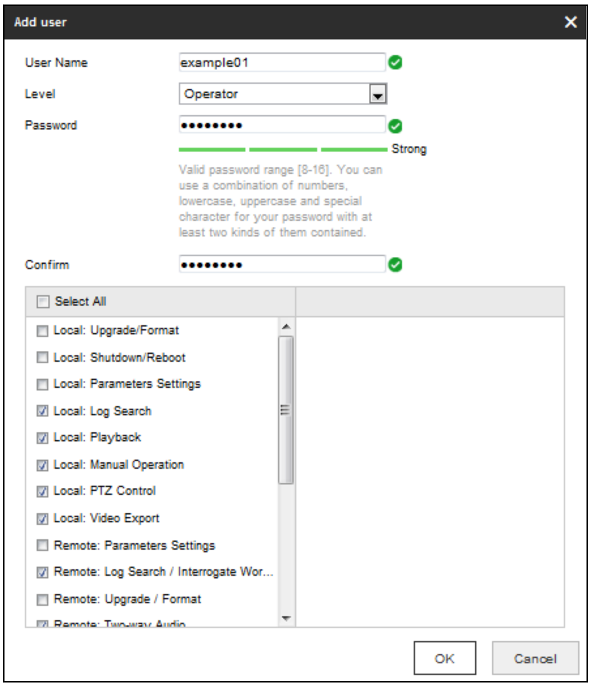
Steps:

1. Click **Add** to enter the Add user interface.
2. Edit the **User Name**.
3. Select the **Level** to **Operator** or **User**.

   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.
4. Set the **Password**, and confirm the same password.

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



Add user

User Name: example01

Level: Operator

Password: ••••••••

Strong

Valid password range [8-16]. You can use a combination of numbers, lowercase, uppercase and special character for your password with at least two kinds of them contained.

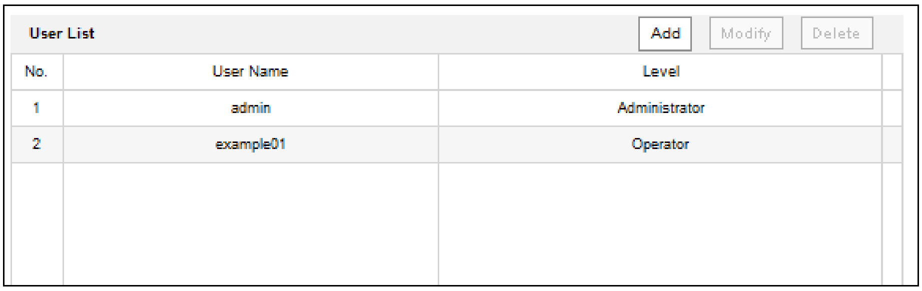
Confirm: ••••••••

□ Select All

- □ Local: Upgrade/Format
- □ Local: Shutdown/Reboot
- □ Local: Parameters Settings
- ☑ Local: Log Search
- ☑ Local: Playback
- ☑ Local: Manual Operation
- ☑ Local: PTZ Control
- ☑ Local: Video Export
- □ Remote: Parameters Settings
- ☑ Remote: Log Search / Interrogate Wor...
- □ Remote: Upgrade / Format
- ☑ Remote: Two-way Audio

Figure 10. 2 Add a User

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.



User List

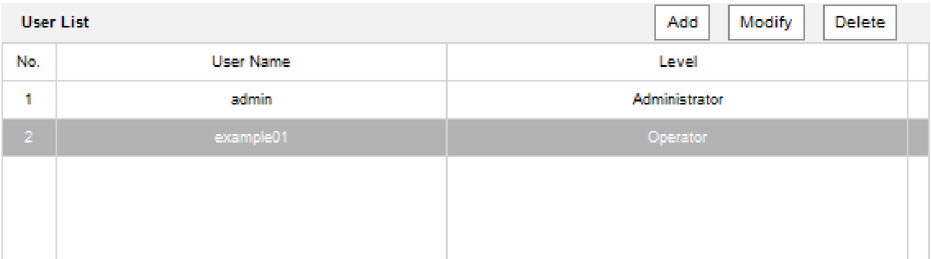
No.	User Name	Level
1	admin	Administrator
2	example01	Operator

Figure 10. 3 User List

10.2 Modifying a User

Steps:

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



User List

No.	User Name	Level
1	admin	Administrator
2	example01	Operator

Figure 10. 4 Select a User

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

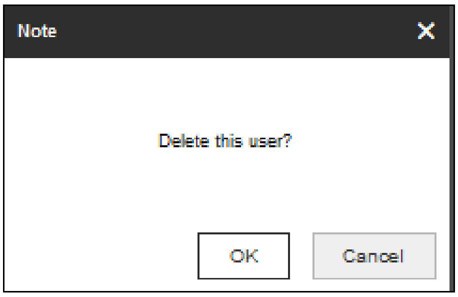
NOTE

You need the admin password to modify the admin user.

10.3 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:



Note

Delete this user?

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

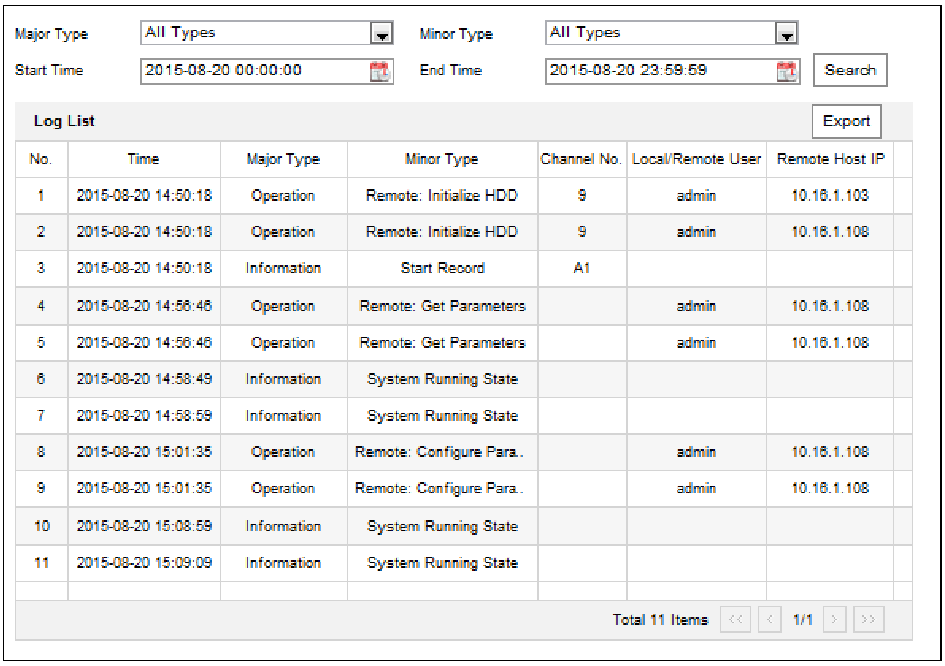
The Log function can be realized only when the Encoder is connected with Micro SD card or network disk. And make sure the disk has been initialized for the first time to use. Please refer to *Section Adding Network Disk* for details.

Steps:

1. Click **Configuration > System > Maintenance > Log** 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.



Major Type: All Types
Minor Type: All Types
Start Time: 2015-08-20 00:00:00
End Time: 2015-08-20 23:59:59

No.	Time	Major Type	Minor Type	Channel No.	Local/Remote User	Remote Host IP
1	2015-08-20 14:50:18	Operation	Remote: Initialize HDD	9	admin	10.16.1.103
2	2015-08-20 14:50:18	Operation	Remote: Initialize HDD	9	admin	10.16.1.108
3	2015-08-20 14:50:18	Information	Start Record	A1		
4	2015-08-20 14:56:46	Operation	Remote: Get Parameters		admin	10.16.1.108
5	2015-08-20 14:56:46	Operation	Remote: Get Parameters		admin	10.16.1.108
6	2015-08-20 14:58:49	Information	System Running State			
7	2015-08-20 14:58:59	Information	System Running State			
8	2015-08-20 15:01:35	Operation	Remote: Configure Para.		admin	10.16.1.108
9	2015-08-20 15:01:35	Operation	Remote: Configure Para.		admin	10.16.1.108
10	2015-08-20 15:08:59	Information	System Running State			
11	2015-08-20 15:09:09	Information	System Running State			

Figure 11. 1 Log Search Interface

5. You can click the **Export** button to save the searched log files to local directory.

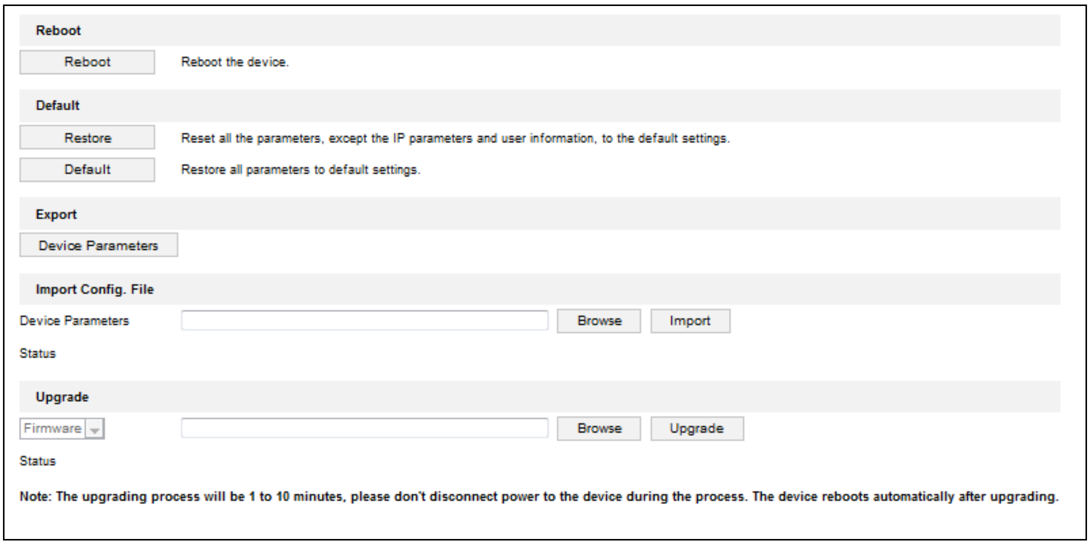
11.2 Viewing Device Information

Click **Configuration** > **System** > **System Settings** > **Basic Information** to enter the Device Information interface of the encoder:

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 Upgrade & Maintenance

Click **Configuration** > **System** > **Maintenance** > **Upgrade & Maintenance** to enter the Maintenance interface of the encoder:



Reboot

Reboot — Reboot the device.

Default

Restore — Reset all the parameters, except the IP parameters and user information, to the default settings.

Default — Restore all parameters to default settings.

Export

Device Parameters

Import Config. File

Device Parameters — Browse — Import

Status

Upgrade

Firmware — Browse — Upgrade

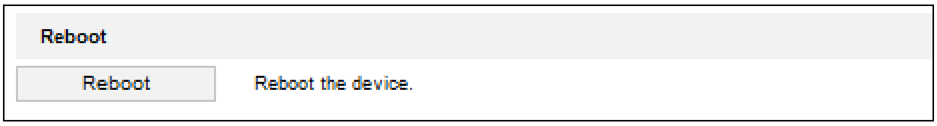
Status

Note: The upgrading process will be 1 to 10 minutes, please don't disconnect power to the device during the process. The device reboots automatically after upgrading.

Figure 11. 2 Maintenance Page

11.3.1 Rebooting the Device

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



Reboot

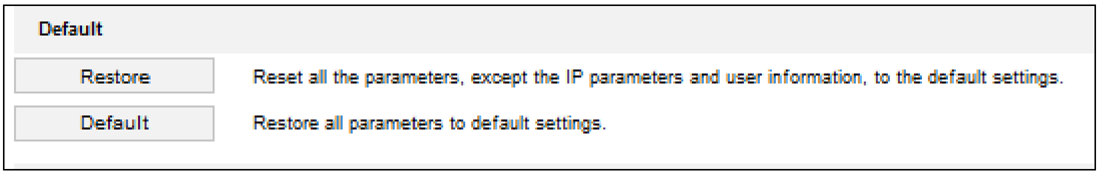
Reboot — Reboot the device.

Figure 11. 3 Reboot the Device

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

11.3.2 Restoring Default Settings

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



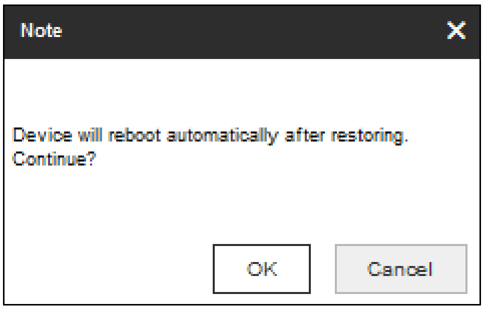
Default

Restore	Reset all the parameters, except the IP parameters and user information, to the default settings.
Default	Restore all parameters to default settings.

Figure 11. 4 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.



Note

Device will reboot automatically after restoring.
Continue?

Figure 11. 5 Pop-up Message Box

11.3.3 Importing/Exporting Configuration Files

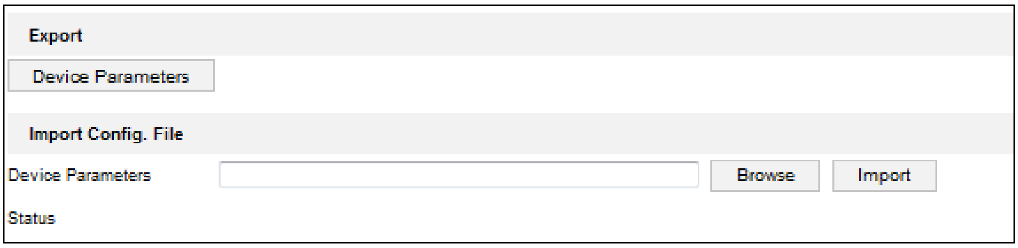
The configuration files of the device can be exported to local device for backup; and the configuration files of one device can be imported to multiple device devices if they are to be configured with the same parameters.

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



Export

Device Parameters

Import Config. File

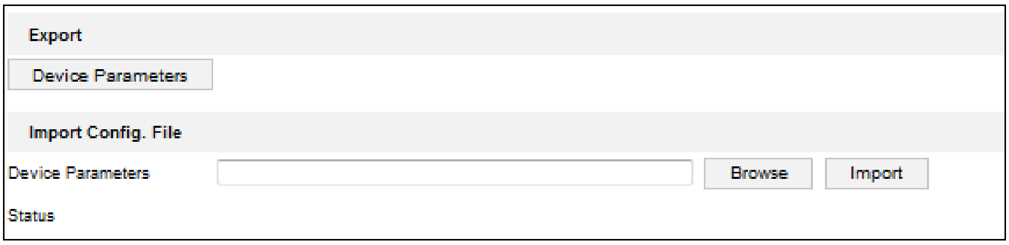
Device Parameters

Status

Figure 11. 6 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.



Export

Device Parameters

Import Config. File

Device Parameters

Browse

Import

Status

Figure 11. 7 Remote Upgrade

Chapter 12 Specifications

Model	DS-6701HFHI/V	
Video/Audio input/output	Video input	1-ch, VGA
		1-ch, HDMI
	Video input format/frame rate	**VGA:** UXGA (1600 × 1200)p/60Hz, 1080p/60Hz, 1080p/50Hz, SXGA (1280 × 1024)p/60Hz, 1440 × 900p/60 Hz, 1366 × 768p/60 Hz, 720p/60Hz, XGA (1024 × 768)p/75Hz, XGA (1024 × 768)p/60Hz, 800 × 600p/60Hz, 640 × 480p/60Hz **HDMI:** UXGA (1600 × 1200)p/60Hz, 1080p/60Hz, SXGA (1280 × 1024)p/60Hz, 720p/60Hz, XGA (1024 × 768)p/60Hz
	Video loop output	1-ch, VGA
	Audio input	1-ch, 3.5 mm interface (two-way audio multiplex)
	Audio output	1-ch, 3.5 mm interface (linear, 600Ω)
Video/Audio encoding/ decoding parameter	Video compression standard	H.264
	Video encoding resolution	UXGA/1080p/SXGA/720p/XGA/WD1/4CIF/CIF
	Video frame rate	1/16 FPS to full frame rate (full frame rate includes 25/30/50/60 frames, depending on input signal)
	Video bitrate	32 Kbps to 8192 Kbps, up to 16 Mbps
	Audio compression standard	G.711u/G.711a/AAC
	Audio bitrate	16Kbps/128Kbps
	Stream type	Video & audio/video
	Dual stream	Dual stream Sub stream resolution: WD1/4CIF/2CIF/CIF/QCIF
Storage	Network storage	NAS, iSCSI, IPSAN
	SD card	Micro SD card
	Maximum capacity	4 TB for network single hard disk, 128 GB for micro SD card
Network	Security	Password protection, HTTPS encryption
	Network protocol	IPv4/v6, HTTP, HTTPS, FTP, SMTP, RTMP, UPnP, SNMP, ONVIF, DNS, DynDNS, HiDDNS, EZVIZ Cloud P2P, NTP, RTSP, RTP/RTCP, TCP, UDP, IGMP, ICMP, DHCP, ARP
External interface	Two-way audio input	1, 3.5 mm interface (audio input multiplex)
	Network interface	1, RJ45 10/100 M self-adaptive Ethernet interface
	Serial interface	1, RS-485, half-duplex
		1, RS-232
	Alarm in	1-ch
	Alarm out	1-ch
	Restoration	Support
General	Power supply	12 VDC, 2-pin connector
	Consumption	≤ 6 W
	Working temperature	-10 ºC to +55 ºC (14 ºF to 131 ºF)
	Working humidity	10 to 90 %
	Dimensions (W × H × D)	114 × 47.5 × 127.5 mm (4.5" ×1.9" ×5.0")
	Weight	≤ 1 kg (2.2 lb)

Chapter 13 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?**

  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.

0101001050917