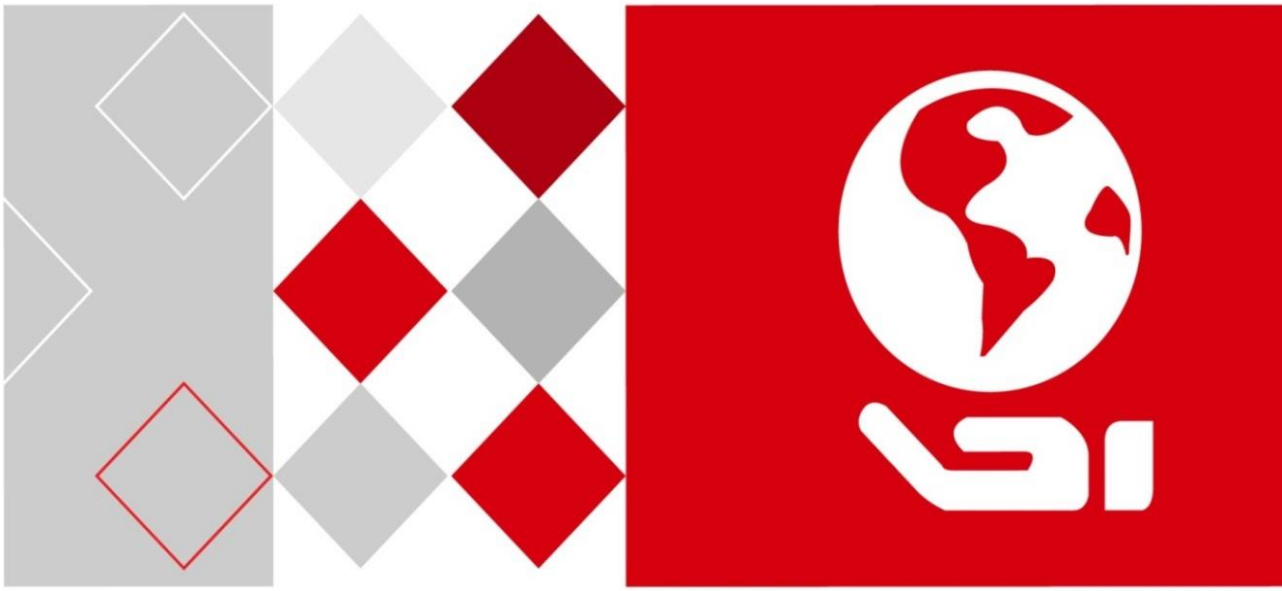


DS-6700HUHI-K Series Encoder

User Manual

UD07058B

User Manual

About this Manual

This Manual is applicable to DS-6700HUHI-K Series Encoder.

The Manual includes instructions for using and managing the product. Pictures, charts, images and all other information hereinafter are for description and explanation only. The information contained in the Manual is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version in the company website (http://overseas.hikvision.com/en/).

Please use this user manual under the guidance of professionals.

Trademarks Acknowledgement

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

Legal Disclaimer

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

REGARDING TO THE PRODUCT WITH INTERNET ACCESS, THE USE OF PRODUCT SHALL BE WHOLLY AT YOUR OWN RISKS. HIKVISION SHALL NOT TAKE ANY RESPONSIBILITES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER ATTACK, HACKER ATTACK, VIRUS INSPECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.

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

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

Regulatory Information

FCC Information

Please take attention that changes or modification not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

FCC compliance: This equipment has been tested and found to comply with the limits for a Class 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 2014/30/EU, the LVD Directive 2014/35/EU, the RoHS Directive 2011/65/EU.

2012/19/EU (WEEE directive): Products marked with this symbol cannot be disposed of as unsorted municipal waste in the European Union. For proper recycling, return this product to your local supplier upon the purchase of equivalent new equipment, or dispose of it at designated collection points. For more information see: www.recyclethis.info

2006/66/EC (battery directive): This product contains a battery that cannot be disposed of as unsorted municipal waste in the European Union. See the product documentation for specific battery information. The battery is marked with this symbol, which may include lettering to indicate cadmium (Cd), lead (Pb), or mercury (Hg). For proper recycling, return the battery to your supplier or to a designated collection point. For more information see: www.recyclethis.info

Industry Canada ICES-003 Compliance

This device meets the CAN ICES-3 (A)/NMB-3(A) standards requirements.

Applicable Models

This manual is applicable to the models listed in the following table.

Series	Model
DS-6700HUHI-K	DS-6704HUHI-K
	DS-6708HUHI-K
	DS-6716HUHI-K

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
	Provides additional information to emphasize or supplement important points of the main text.
	Indicates a potentially hazardous situation, which if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
	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 to 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

Product Key Features

General

- Self-adaptive HDTVI/HDCVI/AHD/CVBS signal input
- Connectable to the Coaxitron camera/dome with long transmission distance
- 5 MP/4 MP HDTVI video input and live view
- Independent configuration for each channel, including resolution, frame rate, bit rate, image quality, etc
- Encoding for both video stream and video and audio stream; audio and video synchronization during composite stream encoding
- Watermark technology

Monitoring

- Motion detection, video-tampering detection, video exception alarm, video loss alarm and VCA alarm functions
- Privacy mask
- Several PTZ protocols supported; PTZ preset, patrol and pattern

HDD Management

- 1 SATA interface for DS-6704HUHI-K, and 2 SATA interfaces for DS-6708/6716HUHI-K
- Each disk with a maximum of 8 TB storage capacity
- S.M.A.R.T. and bad sector detection
- HDD sleeping function
- HDD property: redundancy, read-only, read/write (R/W)
- HDD group management
- HDD quota management; different capacity can be assigned to different channels

Recording and Playback

- Holiday recording schedule configuration
- Cycle and non-cycle recording modes
- Normal and event video encoding parameters
- Multiple recording types: continuous, alarm, motion, motion | alarm, motion & alarm and VCA
- 8 recording time periods with separated recording types
- Pre-record and post-record for motion detection triggered recording, and pre-record time for schedule and manual recording
- Searching record files by events (alarm input/motion detection)
- Locking and unlocking of record files
- Redundant recording
- Searching and playing back record files by camera number, recording type, start time, end time, etc.
- Smart playback to go through less effective information (only supported by client software)
- Reverse playback

- Supports pause, fast forward, slow forward, skip forward, and skip backward when playback, locating by dragging the mouse on the progress bar

Alarm and Exception

- Configurable arming time of alarm input/output
- Alarm for video loss, motion detection, video tampering, abnormal signal, video input/recording resolution mismatch, illegal login, network disconnected, IP confliction, record exception, HDD error, and HDD full, etc.
- Alarm triggers, audio alarm, notifying surveillance center, sending email and alarm output
- VCA detection alarm (audio exception detection, scene change detection, line crossing detection, and intrusion detection)
- Supports coaxial alarm

Network Functions

- 1 self-adaptive 10M/100M/1000M network interface
- IPv6 is supported
- TCP/IP protocol, PPPoE, DHCP, DNS, DDNS, NTP, SADP, SMTP, SNMP, NFS, iSCSI, UPnP™, HTTPS, and ONVIF are supported
- Support access by Hik-Connect
- TCP, UDP and RTP for unicast
- Auto/Manual port mapping by UPnP™
- Remote search, playback, download, locking and unlocking the record files, and downloading files broken transfer resume
- Remote parameters setup; remote import/export of device parameters
- Remote viewing of the device status, system logs and alarm status
- Remote keyboard operation
- Remote HDD formatting and program upgrading
- Remote system restart and shutdown
- Alarm and exception information can be sent to the remote host
- Remotely start/stop recording
- Remotely start/stop alarm output
- Remote PTZ control
- Remote JPEG capture
- Two-way audio and voice broadcasting
- Embedded WEB server

Development Scalability

- SDK for Windows and Linux system
- Source code of application software for demo
- Development support and training for application system

Chapter 1 Introduction

1.1 Front Panel

Figure 1. 1 DS-6704HUHI-K Front Panel

Figure 1. 2 DS-6708/6716HUHI-K Front Panel

Table 1. 1 Indicator Description

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

1.2 Rear Panel

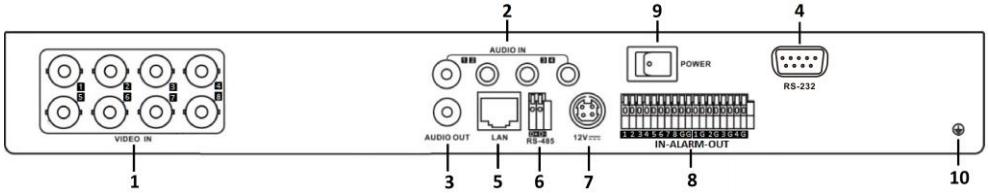


Figure 1. 3 DS-6708HUHI-K Rear Panel

NOTE

The rear panel of DS-6704/6716HUHI-K provides 4/16 video input interfaces.

Table 1. 2 Interface Description

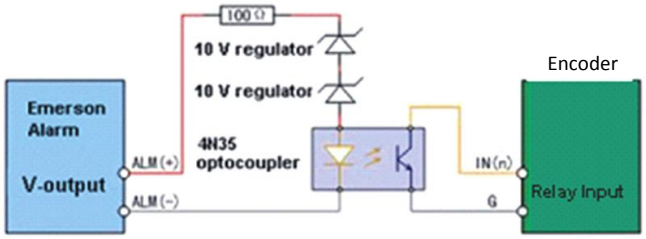
	Description
1	VIDEO IN
2	AUDIO IN, RCA Connector
3	AUDIO OUT, RCA Connector
4	RS-232 Serial Interface
5	LAN Network Interface
6	RS-485 Serial Interface
7	12 VDC Power Input
8	Alarm In/Out
9	Power Switch
10	GND

1.3 Alarm Connections

1.3.1 Alarm Input Connections

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

Alarm input connections for Emerson Alarm:



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

Figure 1. 4 Alarm Input Connections for Emerson Alarm

Alarm input connections for Normal Alarm:

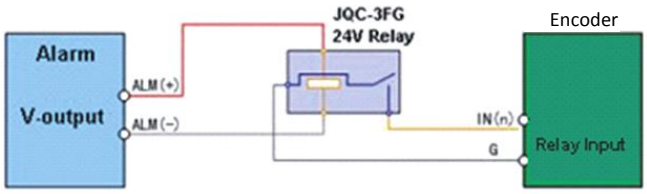


Figure 1. 5 Alarm Input Connections for Normal Alarm

1.3.2 Alarm Output Connections

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

Alarm output connections diagram:

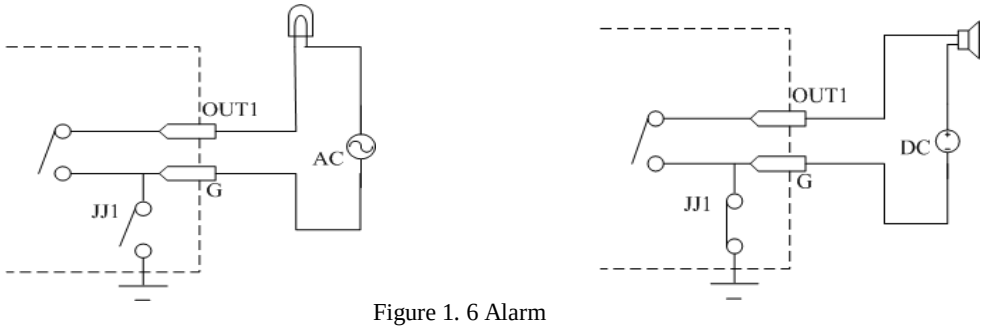


Figure 1. 6 Alarm Output Connections

Please note the different connections of JJ1 shown above.

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

Chapter 2 Activation

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

2.1 Activating via Web Browser

Steps:

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

NOTE

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

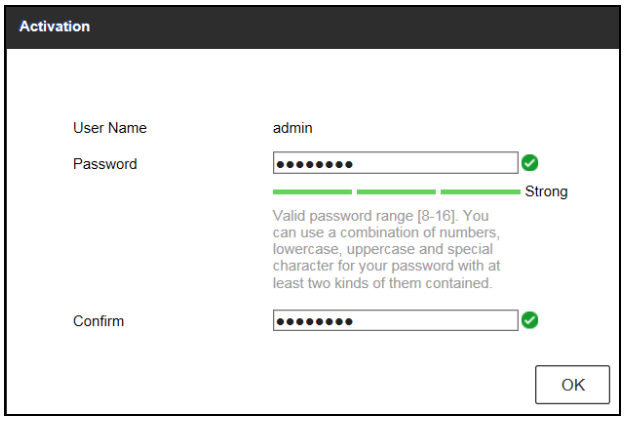


Figure 2. 1 Activation

3. Create a password and input the password into the **Password** text 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 then the window pops up as below.

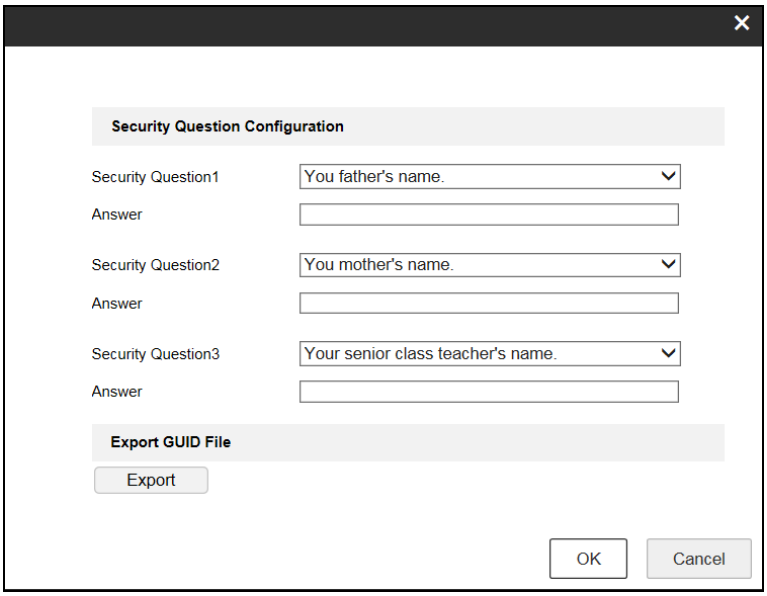


Figure 2. 2 Security Question Configuration and Export GUID File

6. (Optional) Configure the security questions or export the GUID file. Refer to *Chapter 11.1.4 Configuring Security Questions* and *Chapter 11.1.5 Exporting GUID File*. Or click **Cancel** to skip the configuration.

2.2 Activating via Client Software

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

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

Steps:

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

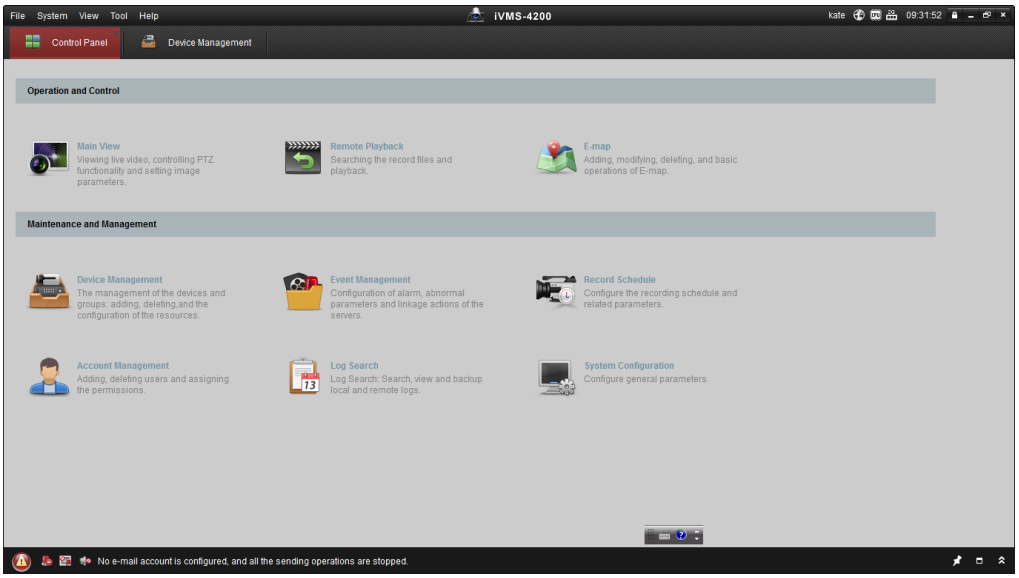


Figure 2. 3 Control Panel

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

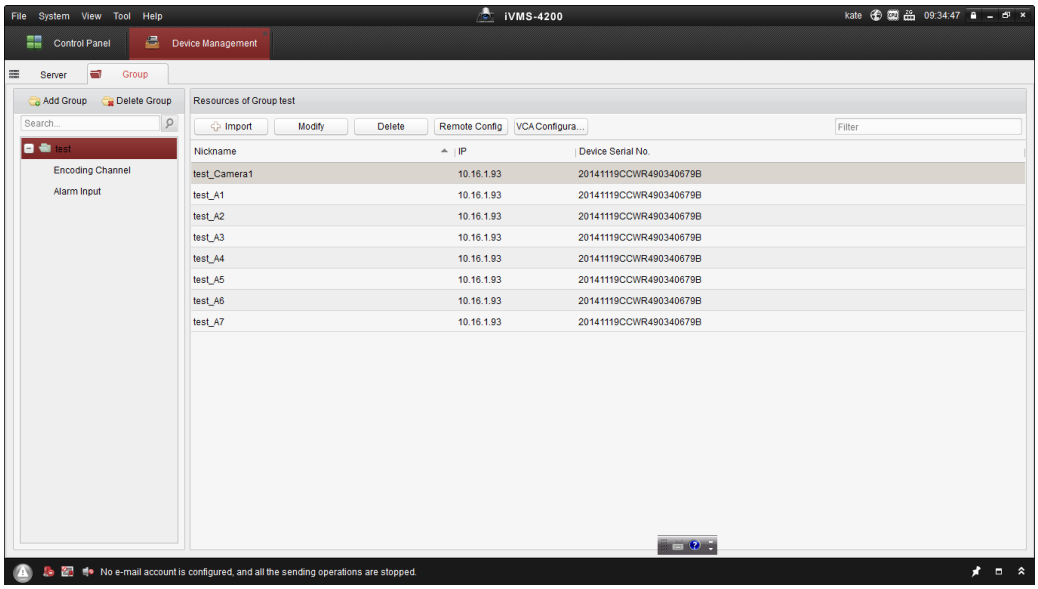


Figure 2. 4 Control Panel

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

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

Figure 2. 5 Activation Interface (Client Software)

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

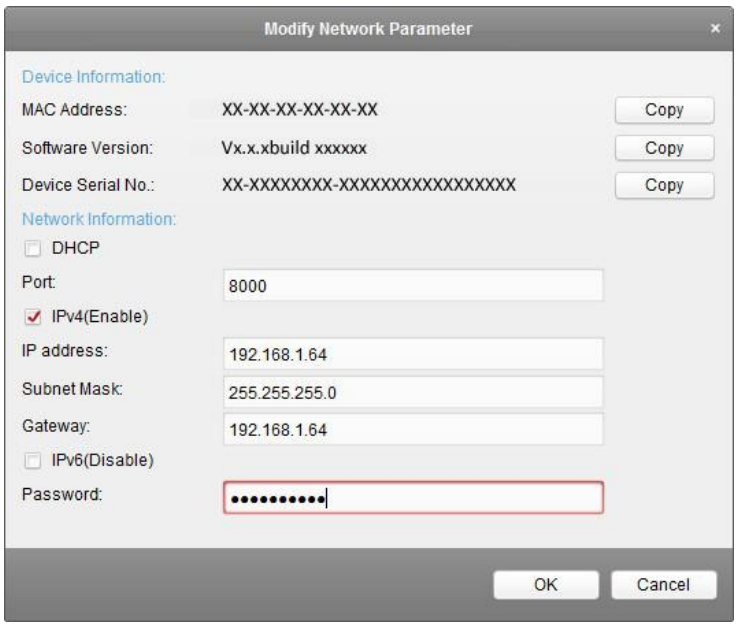


Figure 2. 6 Modifying the Network Parameters

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 3 Getting Started via WEB Browser

The device 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 2*.
- 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*.

3.1 Login

Steps:

1. Open WEB browser, input the IP address of the device and then press the **Enter** key on PC. The system will display the login interface.

NOTE

When the HTTPS feature is enabled, the system uses the HTTPS login mode (e.g., https://192.0.0.64) by default. 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.

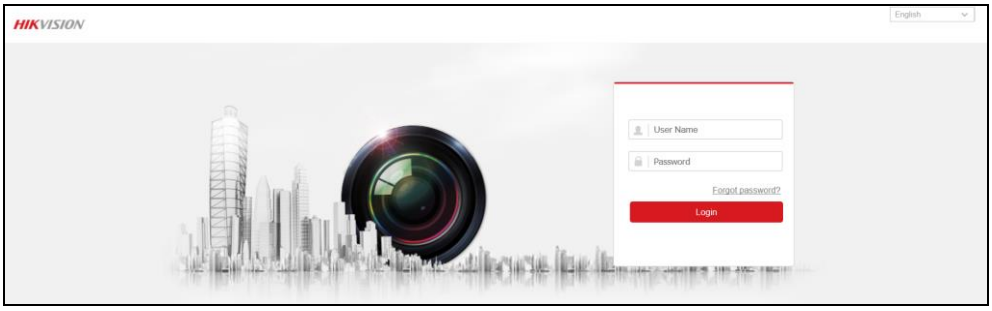


Figure 3. 1 Login Page

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 30 seconds.

3. On the main page, you need to download and install the plug-in.
   (1) Click on the live view panel by following the hints on the screen.

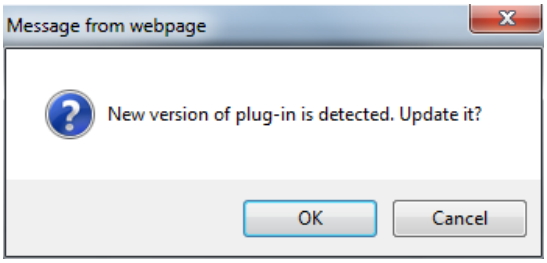


Figure 3. 2 Download and Install Plug-in

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

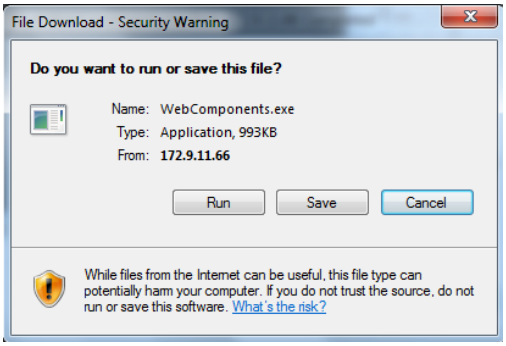


Figure 3. 3 Run Web Components

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

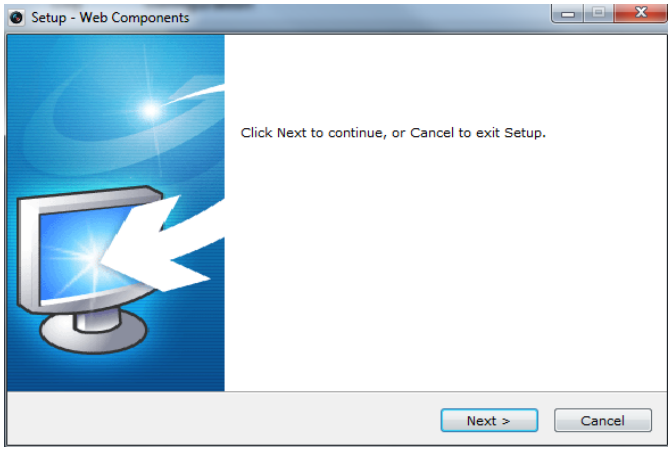


Figure 3. 4 Click Next

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

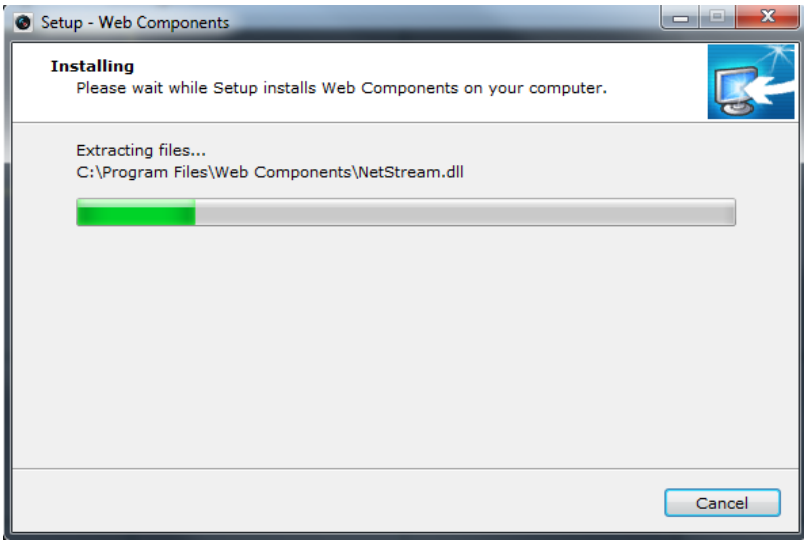


Figure 3. 5 Install the Web Components

3.2 Resetting Password

Purpose

If you forget the password of the device, you can set a new password by answering security questions or importing GUID file.

Before you start

Set the security questions and answers, or export the GUID file first in user management. Refer to *Chapter 11.1.4 Configuring Security Questions* and *Chapter 11.1.5 Exporting GUID File* for reference.

1. On the login page, click **Forgot password?** to enter the verification page.
2. Select the **Verification Mode**.
   - **Security Question Verification**: Answer the security questions listed on the page.

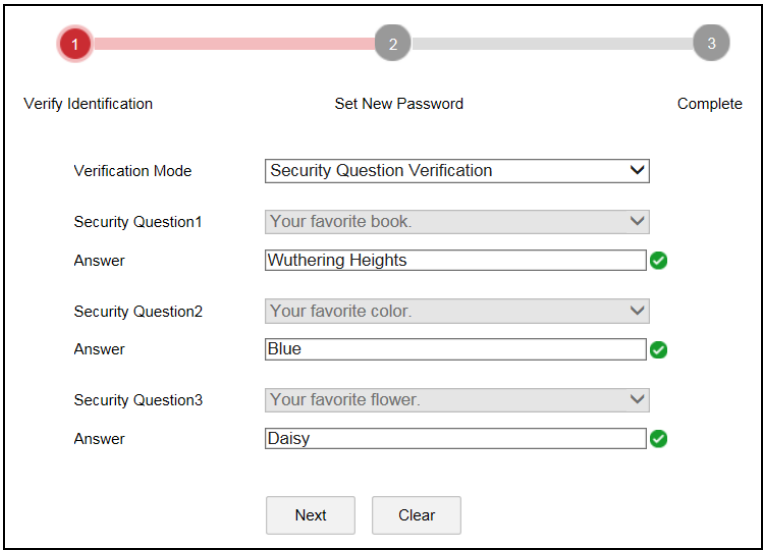


Figure 3. 6 Security Question Verification

   - **GUID File Verification**: Click **Browse** to select the exported GUID file.

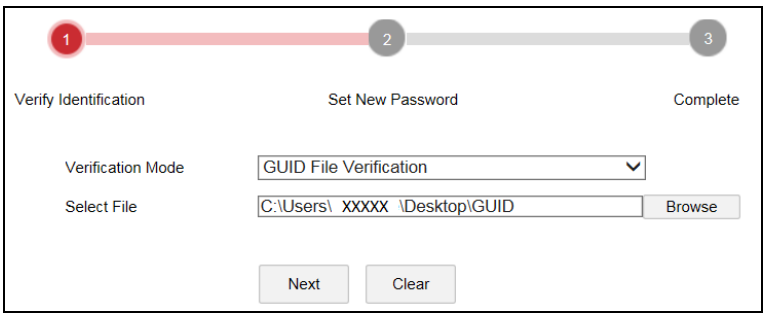


Figure 3. 7 GUID File Verification

3. Click **Next** to set new password.

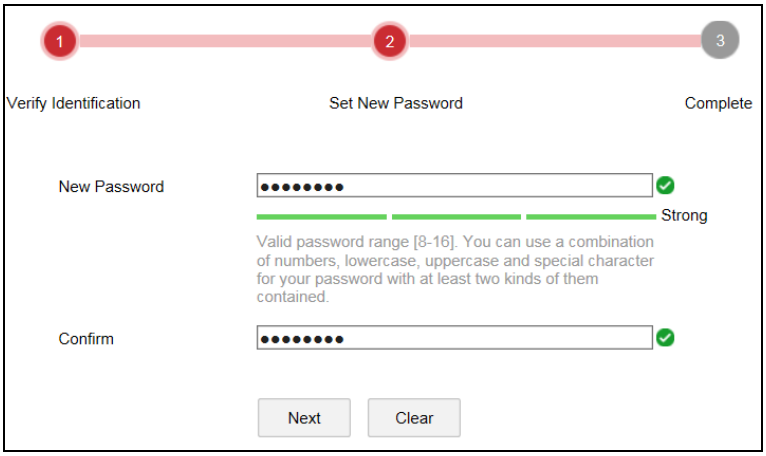


Figure 3. 8 Set New Password

4. Click **Next** and the password is modified. It will jump to the login interface.

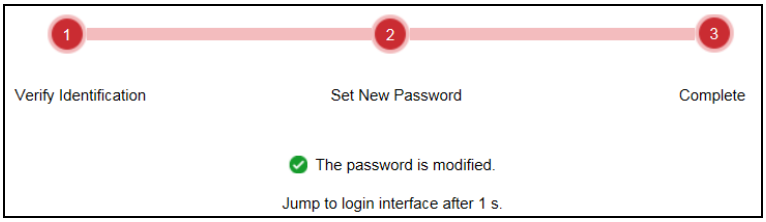


Figure 3. 9 Password Modified

3.3 Main Page Introduction

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

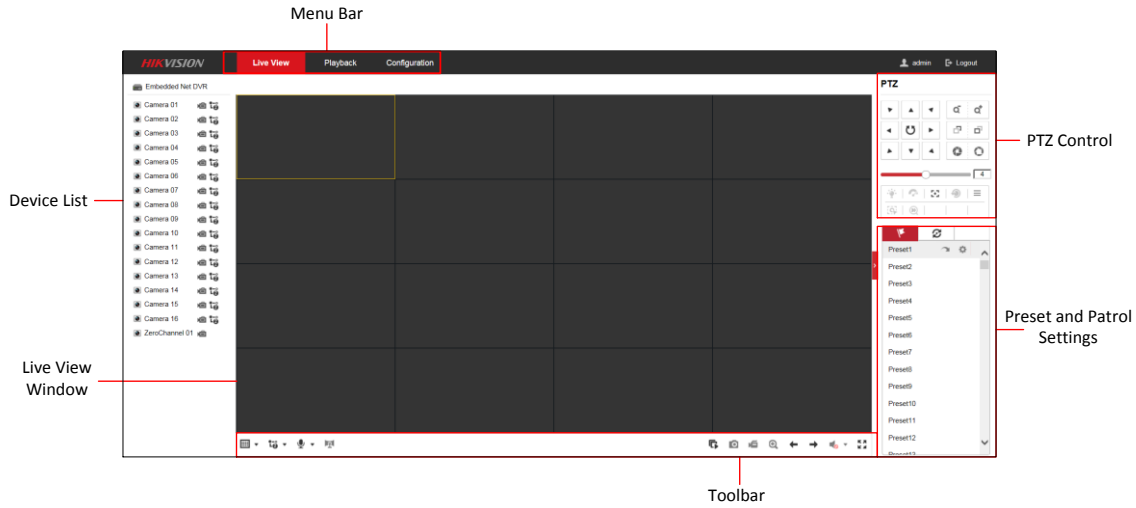


Figure 3. 10 Main Page

Description of the live view page:

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

Device List: Display the connected encoder and its channels.

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

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

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

Preset and Patrol Settings: Set and call the preset/patrol for the camera (supports PTZ function).

Chapter 4 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.

4.1 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.

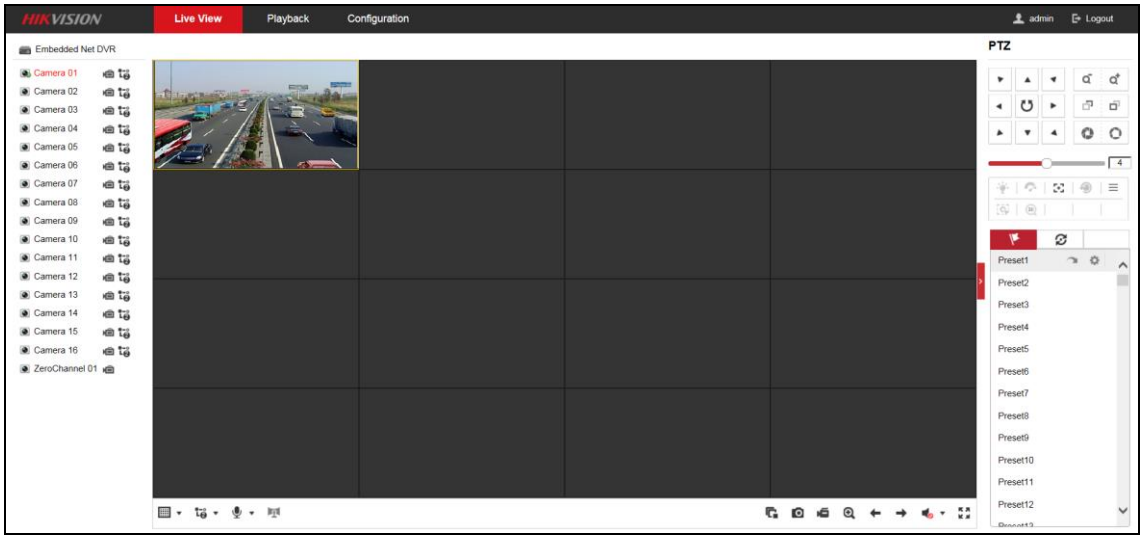


Figure 4. 1 Start Live View

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

Refer to the following table for the description of icons on the live view toolbar:

Table 4. 1 Description of Toolbar

Icon	Description
	Select the window-division mode with 1/4/9/16 split screens
/	Start/Stop live view
	Select main stream or sub-stream
/	Start/Stop two-way audio
	Capture pictures in live view mode
/	Manually start/stop recording

	Enable e-PTZ
/	Previous/Next page
/	Audio on/off
	Switch to full-screen live view mode.

NOTE

Before using two-way audio function or recording with audio, please select the **Video Type** to **Video & Audio** on *Chapter 6.2 Configuring Video/Audio Settings.*

4.1.1 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:

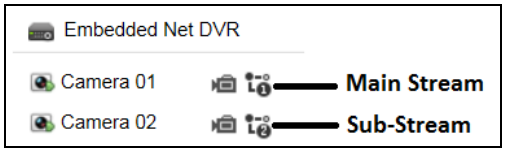


Figure 4. 2 Main Stream/Sub-Stream for Live View

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

4.1.2 Full-screen Mode

You can click on the toolbar or double click on the live video to switch to the full-screen view mode. If you click to switch to the full-screen mode, then press ESC on the keyboard to switch back to the normal mode.

If you double click to switch to the full-screen mode, then double click again to switch back to the normal mode.

Please refer to the following section for more information:

1. Capturing pictures on *Chapter 4.2 Capturing the Picture.* .
2. Configuring recording on *Chapter 8 Record Settings.*
3. Setting the image quality of live view on *Chapter 5.1 Local Configuration.*
4. Setting the saving path for the recorded video files and captured pictures on *Chapter 5.1Local Configuration.*
5. Setting the OSD text on live video on *Chapter 6.1.2 Configuring OSD Settings*.

4.2 Capturing the Picture

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

When the picture is captured, the note message box will appear at the lower right corner to show you the saving path.

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

4.3 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 device respectively.
2. The baud rate, PTZ control and address configured in the **RS-485 Settings** interface (**Configuration > System > System Settings**), as shown below, must be the same with the parameters of the connected pan/tilt unit or speed dome.

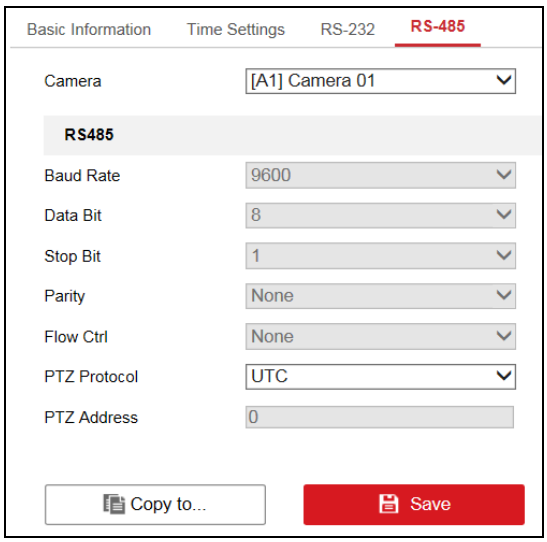


Figure 4. 3 RS-485 Settings

4.3.1 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 4. 4 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 4. 2 Description of PTZ Control Buttons

Button	Description
	Zoom in/out
	Focus near/far
	Iris +/-
	Light on/off
	Wiper on/off
4	Adjust speed of pan/tilt movement
	Auxiliary focus
	Initialize lens
	Adjust speed of pan/tilt movements
	Start Manual Tracking
	Start 3D Zoom

4.3.2 Setting/Calling a Preset

Setting a Preset:

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

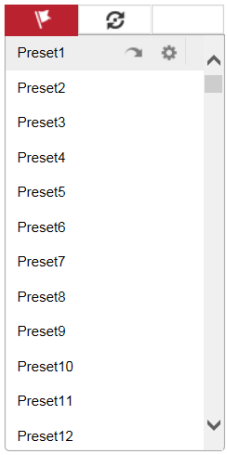


Figure 4. 5 Set a Preset

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 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.

Linking to Alarm:

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

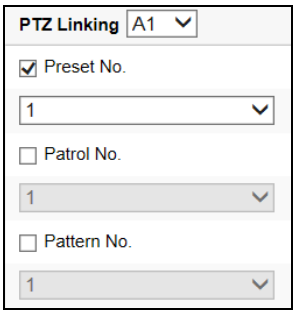


Figure 4. 6 PTZ Linking

Please refer to *Chapter 7.1.2 Configuring Alarm Input* for the PTZ Linking settings (**Configuration>Event>Basic Event>Alarm Input>Linkage Method**).

4.3.3 Setting/Calling a Patrol

Setting a Patrol:

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

Figure 4. 7 Patrol Settings

3. Click to edit the patrol.
4. Click to add patrol path.

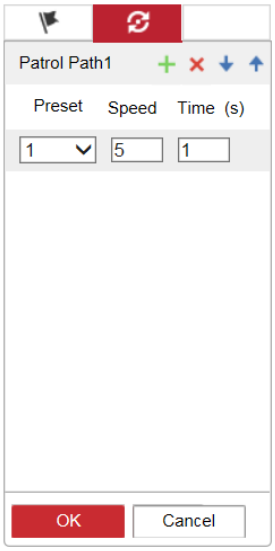


Figure 4. 8 Add Patrol Path

5. Configure patrol parameters, including the preset No., duration of staying for one preset and speed of patrol.
   Preset: determines the order at which the PTZ will follow while cycling through the patrol.
   Time: refers to the time span to stay at the corresponding key point. The time can be set from 1 to 30 sec.
   Speed: defines the speed at which the PTZ will move from one key point to the next. The speed can be set from 1 to 40.
6. Click **OK** to save the path to the current patrol.
7. Repeat the above step 3 to 6 to add more patrol paths.
8. (Optional) Click to edit the existing patrol path, or click to delete it.
9. Repeat the above steps to configure other patrols.

Calling a Patrol:

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

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

4.4 Configuring Channel-Zero Encoding

Purpose:

Sometimes you need to get a remote view of many channels in real time from web browser or CMS (Client Management System) software, in order to decrease the bandwidth requirement without affecting the image quality, channel-zero encoding is supported as an option for you.

Steps:

1. Go to **Configuration > Video/Audio > Channel-Zero**.

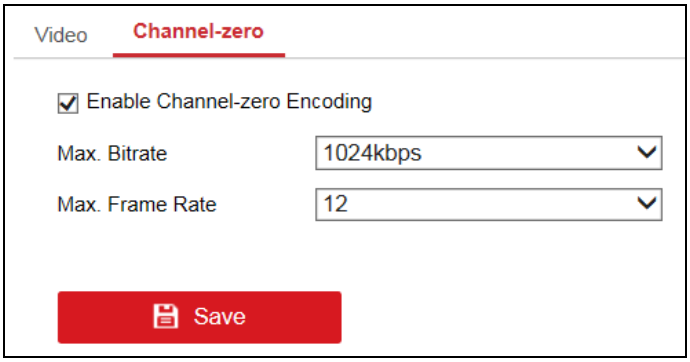


Figure 4. 9 Channel-Zero Settings

2. Check **Enable Channel-zero Encoding**.
3. Configure the **Max. Bitrate** and **Max. Frame Rate**.
4. Click **Save** to save the settings.

   After you set the Channel-Zero encoding, you can get a view in the remote client or web browser of 16 channels in one screen.

Chapter 5 Device Configuration

5.1 Local Configuration

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

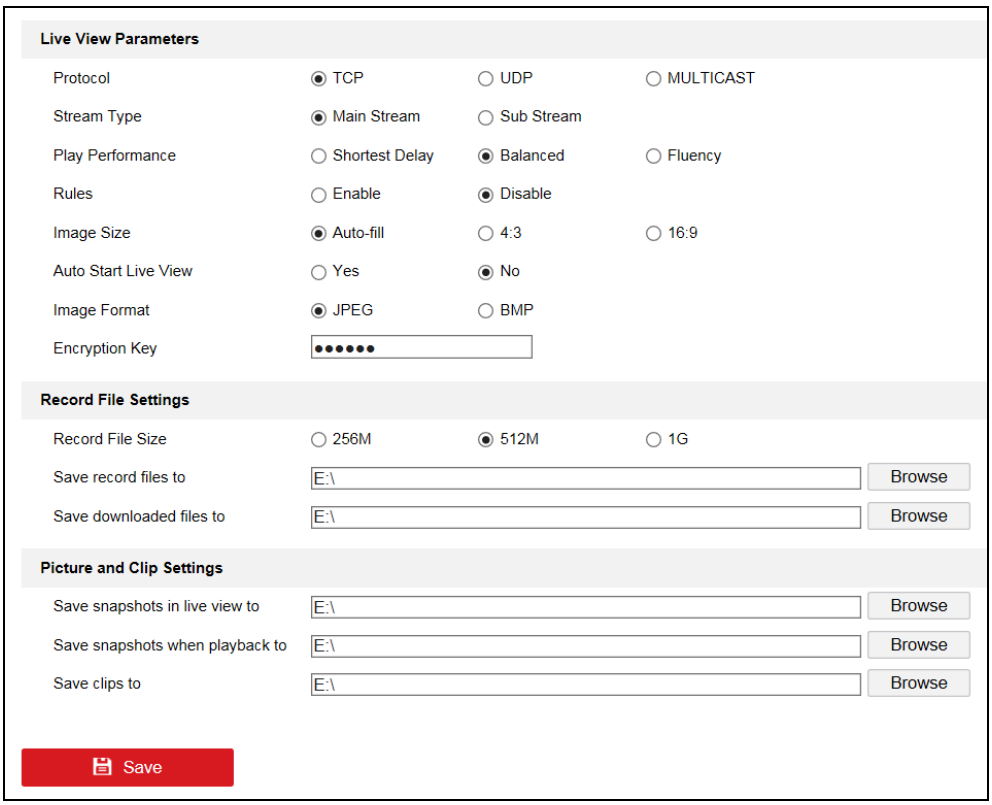


Figure 5. 1 Local Configuration

Configure the following settings:

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

- **UDP:** It provides more real-time audio and video streams.
- **TCP:** It ensures complete deliver of streaming data and better video quality, yet its real-time effect is not so good.
- **MULTICAST:** It's recommended to select MCAST type when using the Multicast function. For detailed information about Multicast, refer to *Chapter 5.3.1 Configuring TCP/IP Settings*.

Stream Type: Select the stream type to main stream or sub-stream used for live view by web browser. Please refer to *Chapter 6.2 Configuring Video/Audio Settings* for the parameters settings of the main stream and sub-stream respectively.

Play Performance: Set the play performance to Shortest Delay, Balanced, or Fluency.

Rules: 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*

7.1.1 Configuring Motion Detection.

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

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

Image Format: Select the image format for picture capture.

Encryption Key: Enter the encryption key.

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

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

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

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.

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

5.2 System Configuration

5.2.1 Viewing Device Information

Go to **Configuration > System > System Settings > Basic Information** to enter the Device Information page of the encoder.

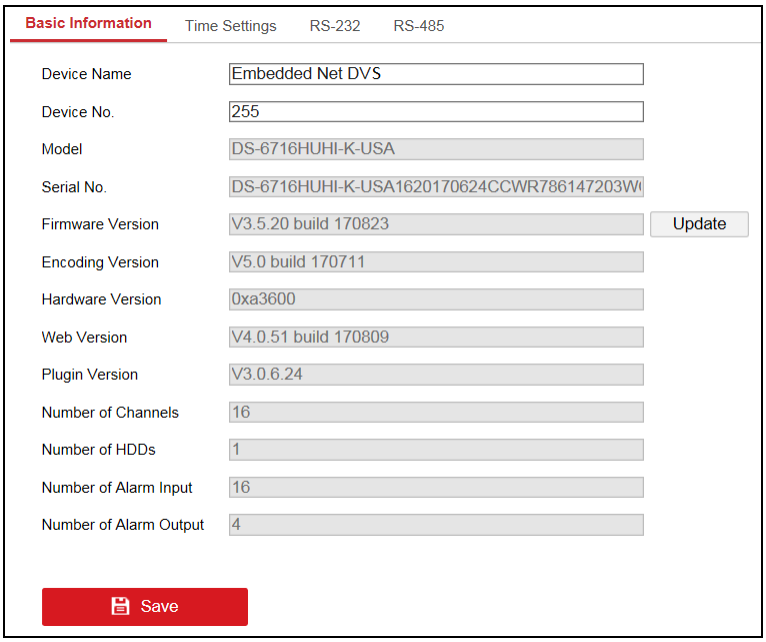


Figure 5. 2 1 Device Information

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

5.2.2 Configuring Time Settings

Steps:

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

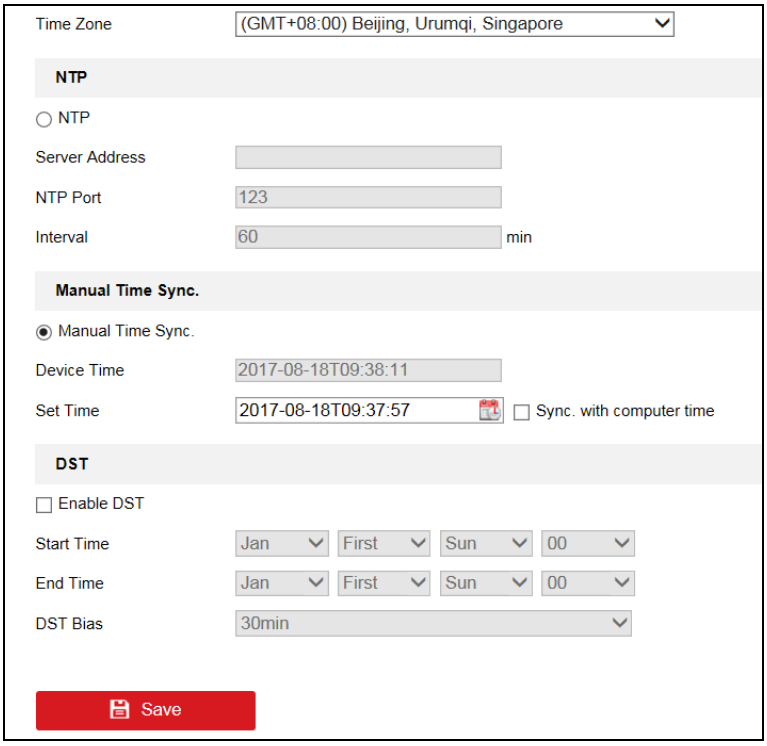


Figure 5. 3 Time Settings

2. Select the **Time Zone** that is closest to the device's location from the drop-down menu.
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 clicking the radio button, and configure the following settings:

Server Address: IP address of NTP server.

NTP Port: Port of NTP server.

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

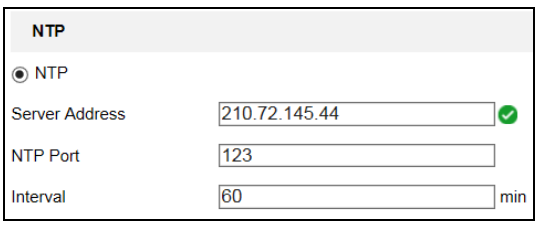


Figure 5. 4 Time Sync by NTP Server

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 Manually**

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

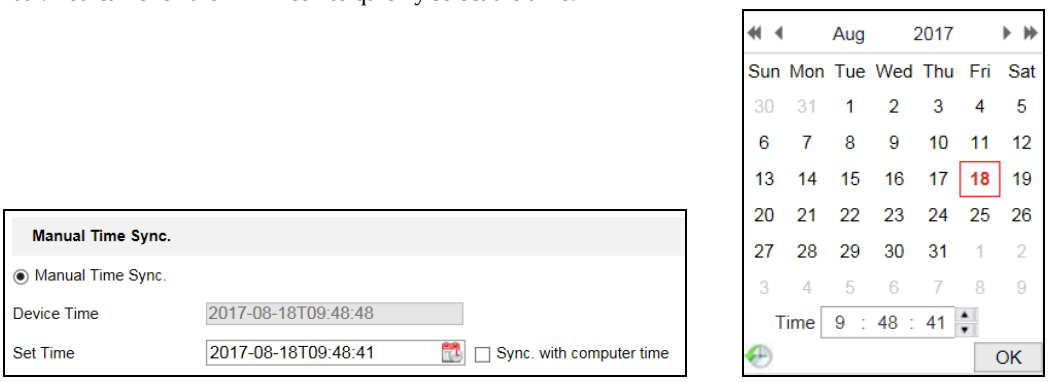


Figure 5. 5 Manual Time Sync.

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

- Check **Enable DST** to enable the DST function and set the date of the DST period.

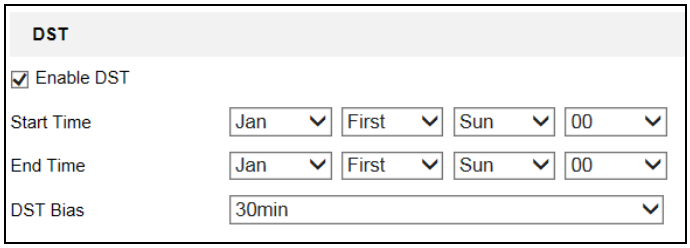


Figure 5. 6 DST Settings

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

5.2.3 Configuring RS-232 Serial Port

The RS-232 serial port can be used in two ways:

- Parameters Configuration: Connect a computer to the camera through the serial port. Device parameters can be configured by using software such as HyperTerminal. The serial port parameters must be the same as the serial port parameters of the camera.
- Transparent Channel: Connect a serial device directly to the camera. The serial device will be controlled remotely by the computer through the network.

Steps:

1. Go to **Configuration**> **System** > **System Settings** > **RS-232**.

2. Configure the Baud Rate, Data Bit, Stop Bit, Parity, Flow Control, and Usage.

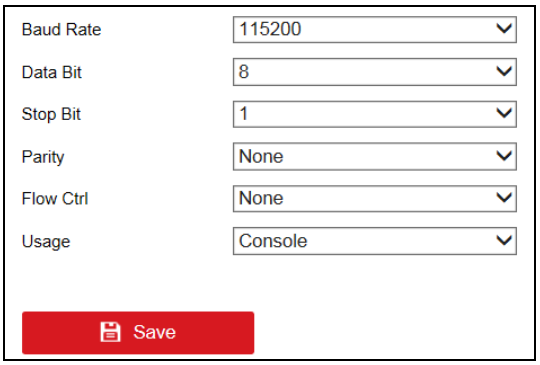


Figure 5. 7 RS-232 Settings

NOTE

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

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

5.2.4 Configuring RS-485 Serial Port

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. Go to **Configuration** > **System** > **System Settings** > **RS-485**.

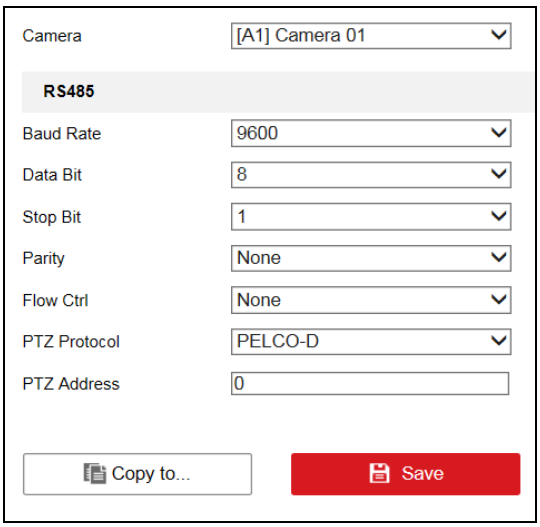


Figure 5. 8 RS-485 Settings

2. Set the RS-485 parameters.

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

NOTE

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

3. (Optional) Click **Copy to** to copy the same settings to other cameras.

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

5.3 Network Configuration

5.3.1 Configuring TCP/IP Settings

Network settings must be properly configured before operating device over network.

Steps:

1. Go to **Configuration** > **Network** > **Basic Settings** > **TCP/IP** to enter the TCP/IP Settings page.

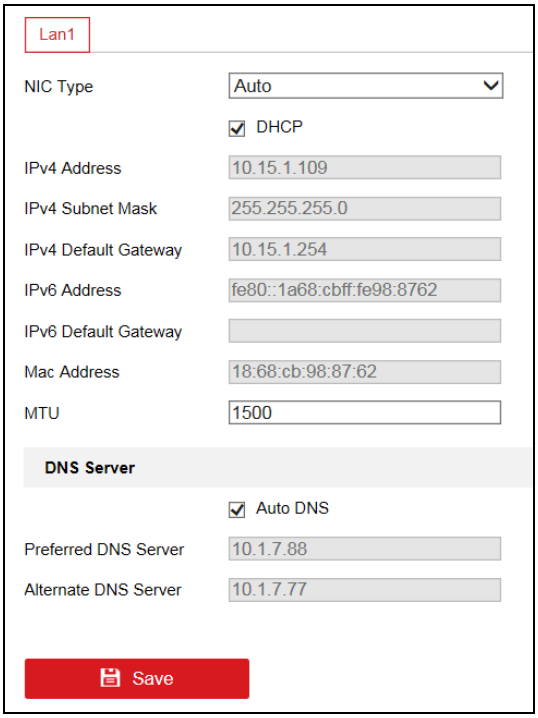


Figure 5. 9 TCP/IP Settings

2. Configure the NIC settings, including the NIC Type, IPv4 or IPv6 Address, IPv4 Subnet Mask, IPv4 or IPv6

Default Gateway, MAC Address, and MTU settings.

NOTE

The valid value range of MTU is 500 to 1500.

3. If the DHCP server is available, you can check **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. Or check **Auto DNS** to automatically obtain the IP address.

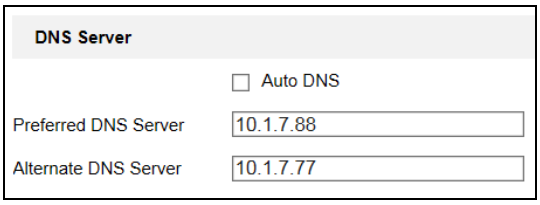


Figure 5. 10 DNS Server Settings

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

5.3.2 Configuring Port Settings

Purpose:

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

Steps:

1. Go to **Configuration > Network > Basic Settings > Port** to enter the Port Settings page.

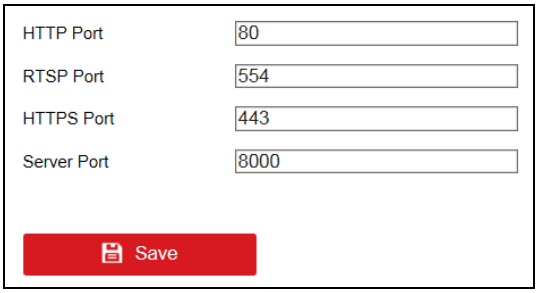


Figure 5. 11 Port Settings

2. Set the HTTP port, RTSP port, HTTPS port, and Server Port 8000 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.

   Server Port: The default port number is 8000.
3. Click **Save** to save the settings.

NOTE

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

5.3.3 Configuring DDNS Settings

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

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

Steps:

1. Go to **Configuration > Network > Basic Settings > DDNS** to enter the DDNS Settings page.
2. Check **Enable DDNS** to enable this feature.
3. Select **DDNS Type**. Three different DDNS types are selectable: DynDNS, PeanutHull, and NO-IP.

- **DynDNS:**

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

(2) Enter the **Domain** obtained from the DynDNS website.

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

(4) Confirm the password.

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

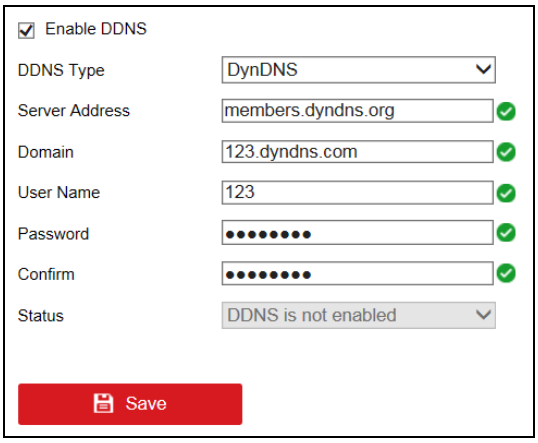


Figure 5. 12 DynDNS Settings

- **PeanutHull:**

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

(2) Confirm the password.

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

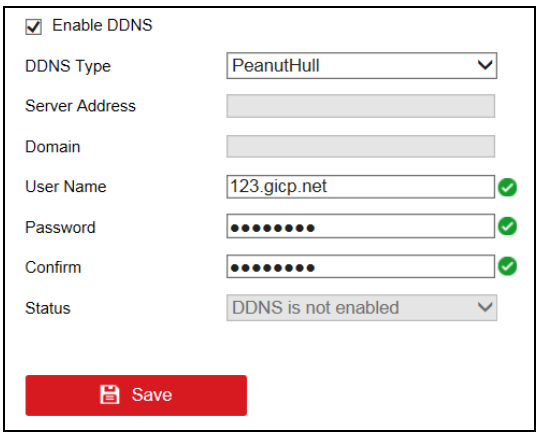


Figure 5. 13 PeanutHull Settings

- **NO-IP:**
  (1) Enter the **Server Address** as www.noip.com.
  (2) Enter the **Domain** you registered.
  (3) Enter the **User Name** and **Password**.
  (4) Confirm the password.
  (5) Click Sa**ve** and then you can view the camera with the domain name.

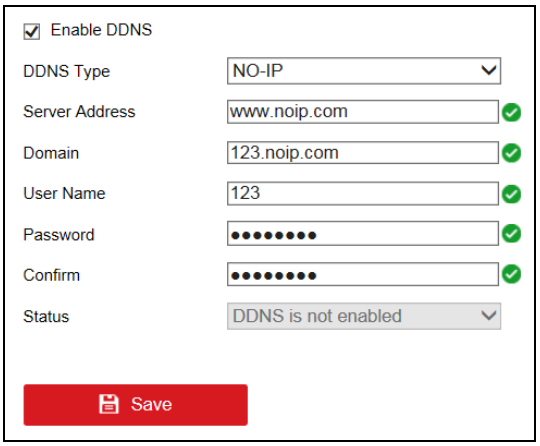


Figure 5. 14 NO-IP Settings

NOTE

Reboot the device to make the settings take effect.

5.3.4 Configuring PPPoE Settings

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

Steps:

1. Go to **Configuration > Network > Basic Settings > PPPoE Settings** to enter the PPPoE settings page.

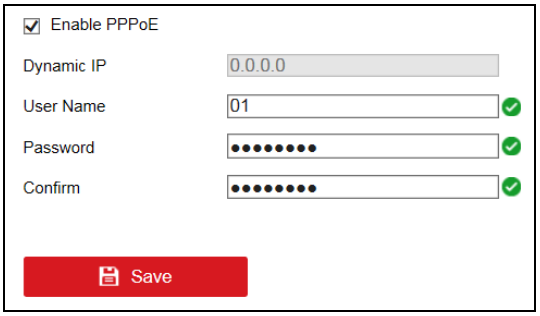


Figure 5. 15 PPPoE Settings

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

NOTE

The user name and password should be assigned by your ISP.

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

5.3.5 Configuring Email Settings

Purpose:

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

Before you start

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

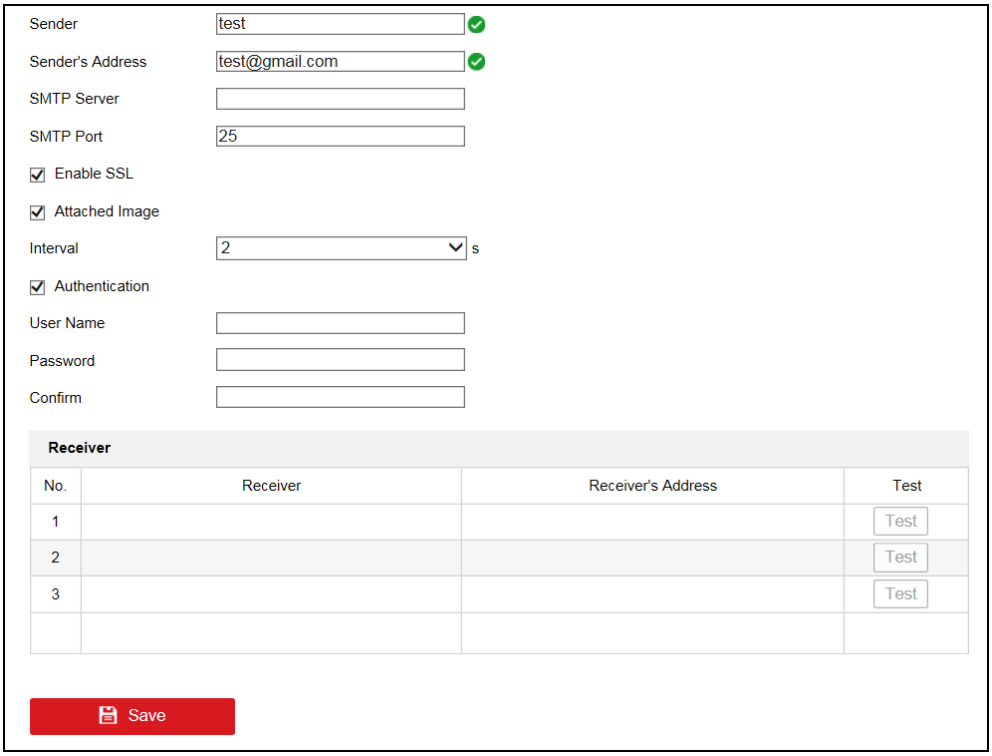


Figure 5. 16 Email Settings

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

Interval: The interval refers to the time 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.

The **Receiver** table: Select the receiver to which the email is sent. Up to 3 receivers can be configured.

Receiver: The name of user to be notified.

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

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 *Chapter 7.1.1 Configuring Motion Detection*, *Chapter 7.1.2 Configuring Alarm Input*, *Chapter 7.1.4 Configuring Video Loss Alarm*, *Chapter 7.1.5 Configuring Video Tempering Alarm* and *Chapter 7.1.6 Handling Exception.*

5.3.6 Configuring UPnP™ Settings

Purpose:

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

Before you start:

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

Steps:

1. Go to **Configuration > Network > Basic Settings > NAT** to enter the NAT settings page.
2. Check **Enable UPnP™** to enable the function.
3. Select the **Port Mapping Mode** to Automatic or Manual.

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

   When you select **Manual**, you can customize the value of the external port.

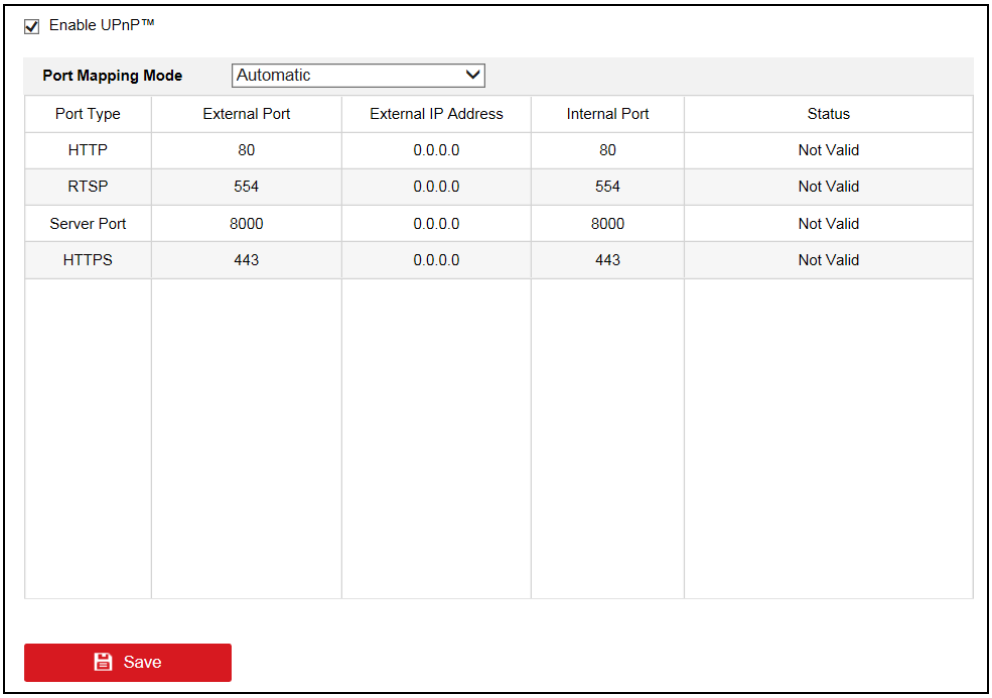


Figure 5. 17 UPnPTM Settings-Auto

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

5.3.7 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 page.
2. Check **Enable** to enable the function.
3. 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.

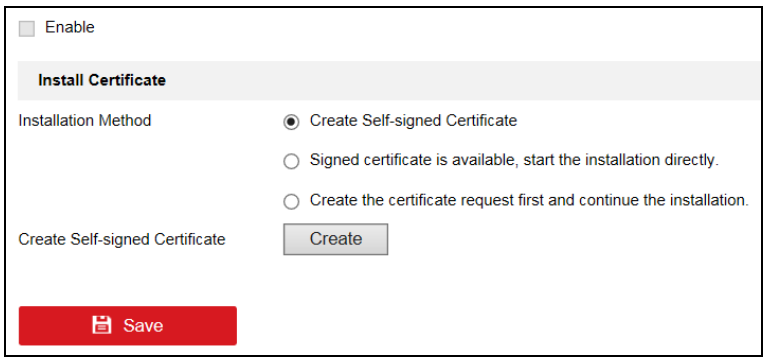


Figure 5. 18 Create Self-signed Certificate

(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** 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.

4. There will be the certificate information after your successfully creating and installing the certificate.

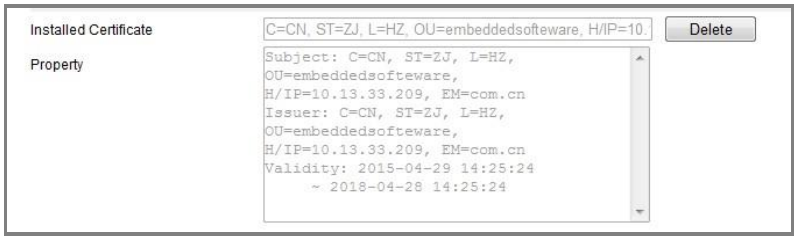


Figure 5. 19 Installed Certificate

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

5.3.8 Configuring Hik-Connect

Purpose:

Hik-Connect provides the mobile phone application and the service platform page (www.hik-connect.com) to access and manage your connected encoder, which enables you to get a convenient remote access to the surveillance system.

NOTE

The Hik-Connect can be enabled via operation on SADP software, GUI and Web browser. We introduce the operation steps on GUI in this section.

Steps:

1. Go to **Configuration > Network > Advanced Settings > Platform Access** to enter the Hik-Connect Settings page.

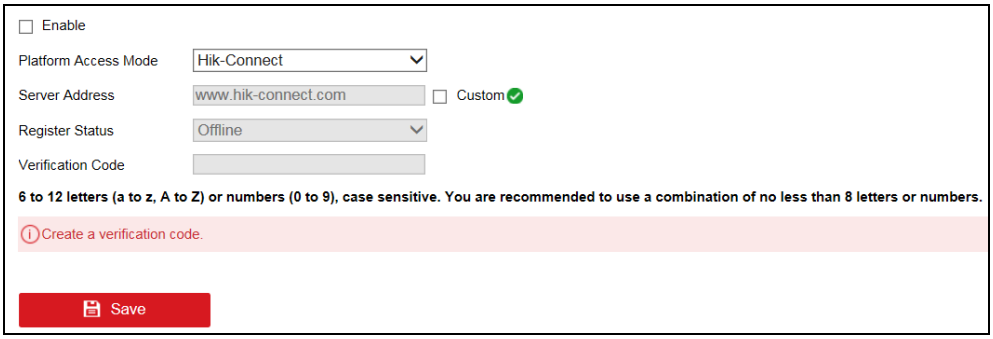


Figure 5. 20 Hik-Connect Settings

2. Check the **Enable** checkbox to activate the function.

Then the Service Terms page pops up as below.

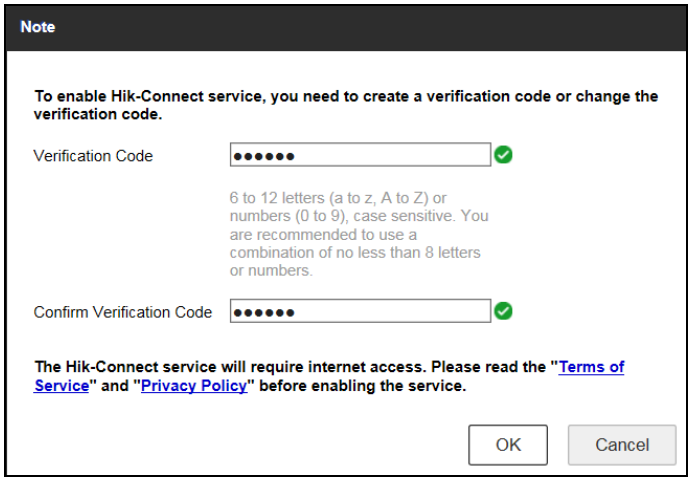


Figure 5. 21 Service Terms

1) Create the verification code in the **Verification Code** text field.
2) Confirm the verification code.
3) Read **Terms of Service** and **Privacy Policy** before enabling the service.
4) Click **OK** to save the settings and return to the Hik-Connect page.

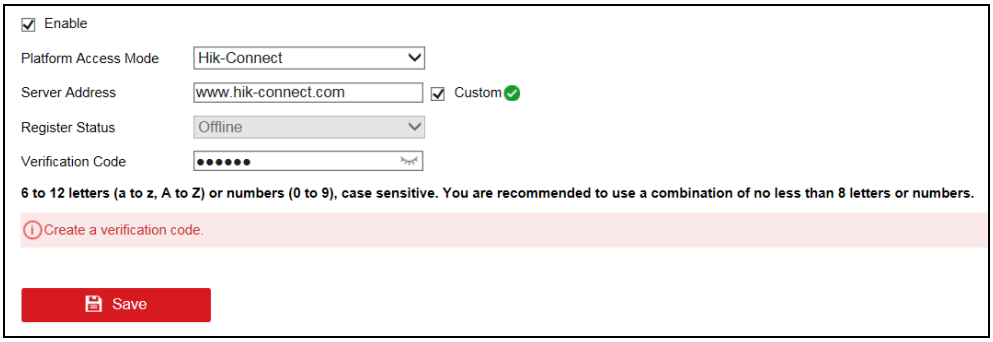


Figure 5. 22 Hik-Connect Settings

NOTE

- Hik-Connect is disabled by default.
- The verification code is empty when the device leaves factory.
- The verification code must contain 6 to 12 letters or numbers and is case sensitive.
- Every time you enable Hik-Connect, the Service Terms page pops up and you should read Terms of Service and Privacy Policy before enabling it.

3. If you want to customize the server, enable **Custom** and enter the **Server Address** in the text field.
4. Click **Save** to save the settings.
   After configuration, you can access and manage the encoder by your mobile phone on which the Hik-Connect application is installed or by the website (www.hik-connect.com).

NOTE

Please refer to the help file on the official website (www.hik-connect.com) and the *Hik-Connect Mobile Client User Manual* for adding the device to Hik-Connect and more operation instructions.

5.3.9 Configuring Multicast Address

Purpose:

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

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

Steps:

1. Go to **Configuration** > **Network** > **Advanced Settings** > **Other** to enter the multicast address settings interface.

Figure 5. 23 Multicast Address Settings

2. Enter the multicast address in the text filed.
3. Click **Save** to save the settings.

NOTE

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

5.3.10 Configuring Remote Alarm Host

Purpose:

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

Steps:

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

Figure 5. 24 Remote Alarm Host

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

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

Chapter 6 Camera Settings

6.1 Configuring Image

6.1.1 Configuring Display Settings

Purpose:

You can configure the scene, brightness, contrast, saturation, etc. in the display settings.

Steps:

1. Go to **Configuration > Image > Display Settings** to enter the Display Settings page.

Figure 6. 1 Display Settings

2. Select the camera from the drop-down list.
3. Select the **Scene** according to different light conditions. Four scenes 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.
4. Set the image parameters of the camera.

   Brightness describes bright of the image, which ranges from 0 to 255.

   Contrast describes the contrast of the image, which ranges from 0 to 255.

   Saturation describes the colorfulness of the image color, which ranges from 0 to 255.

   Hue describes the degree to which a stimulus can be described as similar to or different from stimuli that are described as red, green, blue, and yellow, which ranges from 0 to 255.

   Sharpness describes the edge contrast of the image, which ranges from 0 to 15.

   Denoising describes the process of removing noise from a signal, which ranges from 0 to 5.
5. (Optional) Click **Default** to restore the image parameters to the default settings.

6.1.2 Configuring OSD Settings

Purpose:

You can customize the camera name, time/date format, display mode, and OSD size displayed on the live view.

Steps:

1. Go to **Configuration > Image > OSD Settings**.

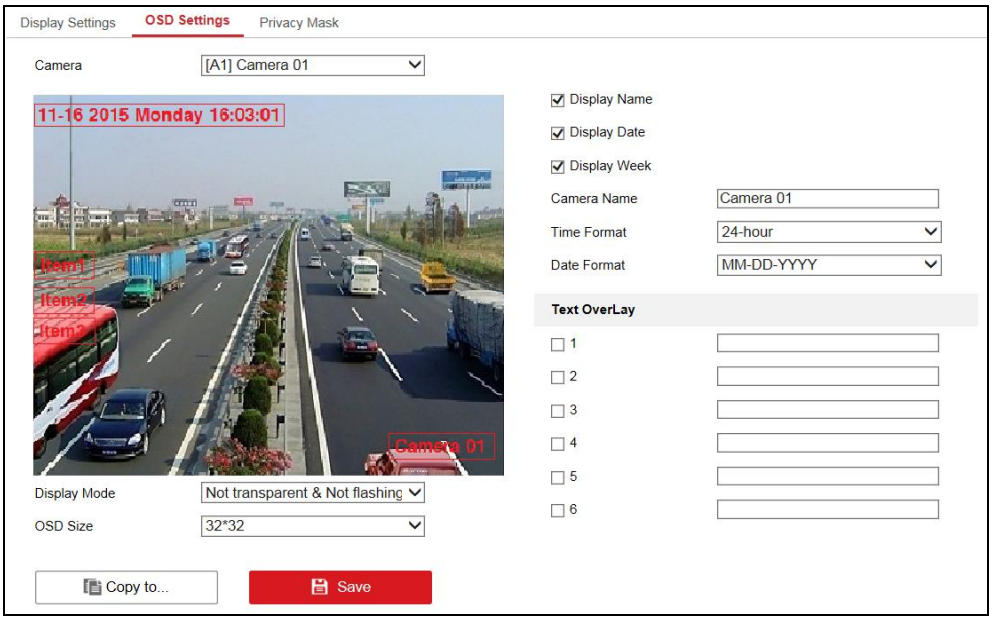


Figure 6. 2 OSD Settings

2. Check the corresponding checkbox to select the display of camera name, date or week if required.
3. Edit the camera name in the text field of **Camera Name**.
4. Select from the drop-down list to set the time format, date format, display mode, and OSD size.
5. Configure the text overlay settings.
   (1) Check the checkbox in front of the textbox to enable the on-screen display.
   (2) Input the characters in the textbox.

   NOTE

   Up to 6 text overlays are configurable.
6. Use the mouse to click and drag text frames in the live view window to adjust their positions.
7. (Optional) Click **Copy to** to copy the same settings to other cameras.
8. Click **Save** to save the settings.

6.1.3 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. Go to **Configuration > Image > Privacy Mask** to enter the privacy mask settings page.

2. Select the camera to configure privacy mask.
3. Check the checkbox of **Enable Privacy Mask** to enable this function.

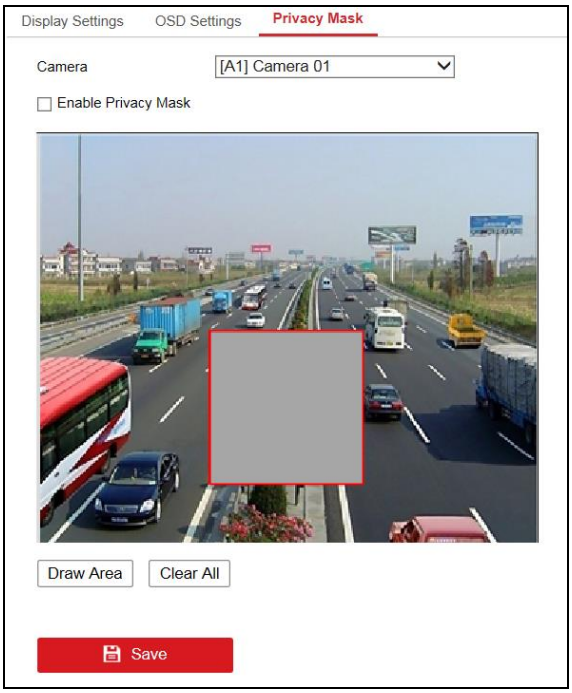


Figure 6. 3 Privacy Mask Settings

4. Click **Draw Area**.
5. Draw the mask area by clicking and dragging the mouse in the live video image.

NOTE

Up to four privacy mask areas can be configured.

6. When finishing the area setting, click **Stop Drawing** to finish drawing.

   You can click **Clear All** to clear all of the areas you set without saving it.
7. Click **Save** to save the settings

6.2 Configuring Video/Audio Settings

Steps:

1. Go to **Configuration > Video/Audio > Video** to enter the Video Settings page.

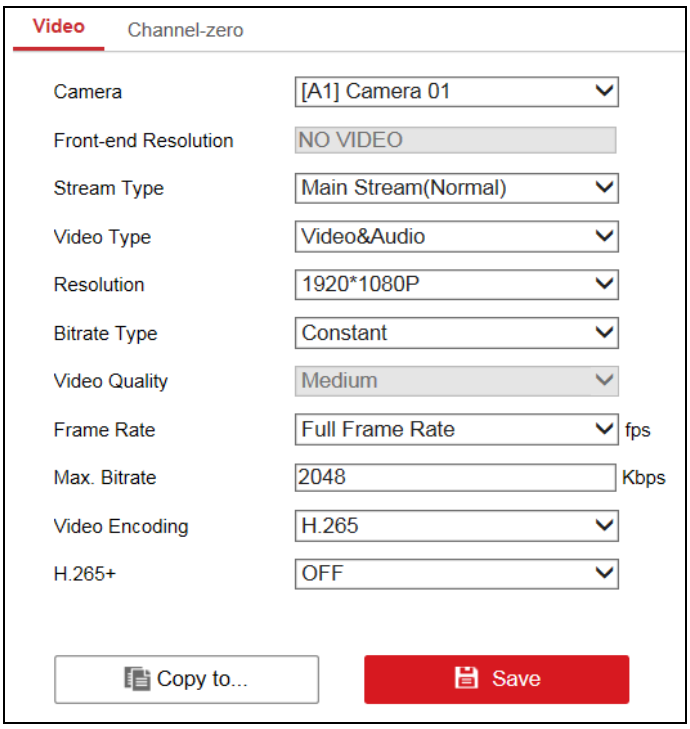


Figure 6. 4 Video Settings

2. Select the camera from the drop-down list to configure.
3. View the **Front-end Resolution**.
4. 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 view with good bandwidth, and the sub-stream can be used for live view when the bandwidth is low. Refer to the *Chapter 5.1 Local Configuration* for changing the main stream to sub-stream for live view.
5. 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: Select the frame rate.

   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: Select or customize the maximum bit rate for recording.

   Video Encoding: You can configure H.264 or H.265 for the main stream (continuous) of cameras.

   H.264+/H.265+: Select ON or OFF to enable or disable H.264+/H.265+. Enabling it helps to ensure the high

video quality with a lowered bitrate.

- The cameras support enabling H.264+/H.265+ if the video encoding is H.264/H.265 for the main stream.
- For the connnected camera, the H.264+ or H.265+ should be supported by the camera.
- Reboot the device to activate the new settings after enabling H.264+ or H.265+.

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

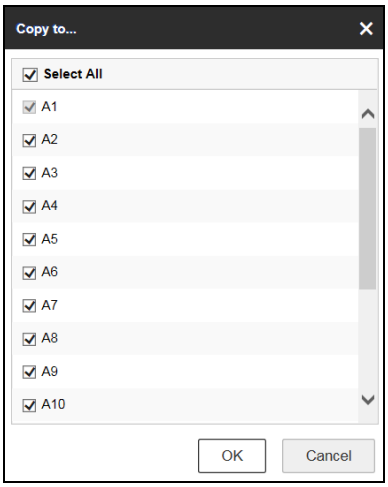


Figure 6. 5 Copy to Camera

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

Chapter 7 Event Settings

7.1 Configuring Basic Events

Purpose:

You can configure the basic events by following the instructions in this section, including motion detection, video tampering, alarm input, alarm output, and exception, etc. These events can trigger the linkage methods, such as Notify Surveillance Center, Send Email, Trigger Alarm Output, etc.

7.1.1 Configuring Motion Detection

Purpose:

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

Steps:

1. Go to **Configuration> Event > Basic Event > Motion** to enter the motion detection settings page.
2. Select the camera to configure the motion detection.
3. Check **Enable Motion Detection**.
4. (Optional) Check **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. Set the motion detection area.
   (1) Click **Area Settings** tab.

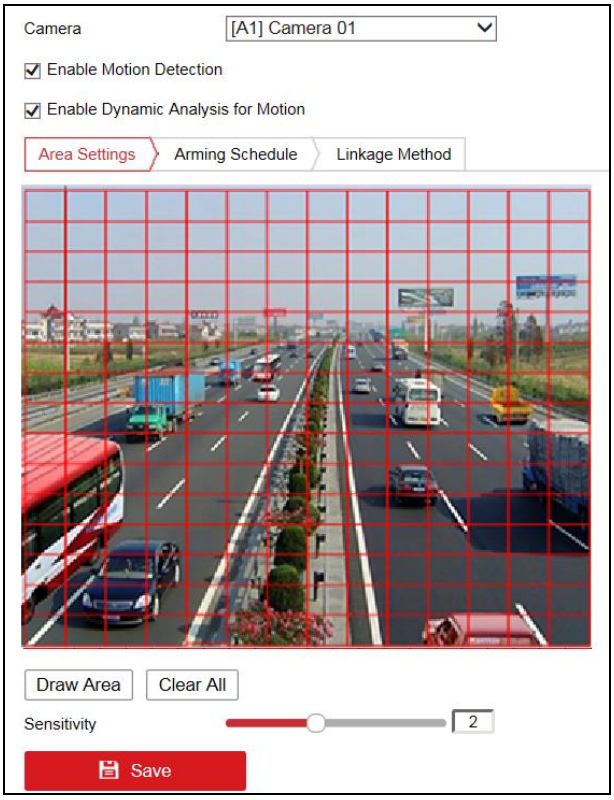


Figure 7. 1 Motion Detection-Area Settings

(2) Click **Draw Area**. Draw motion detection area by dragging the mouse in the live video image.

NOTE

By default, the full screen motion detection is configured.

(3) Click **Stop Drawing** to finish drawing.

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

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

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

6. Set the arming schedule for motion detection.

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

Figure 7. 2 Motion Detection-Arming Schedule Settings

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

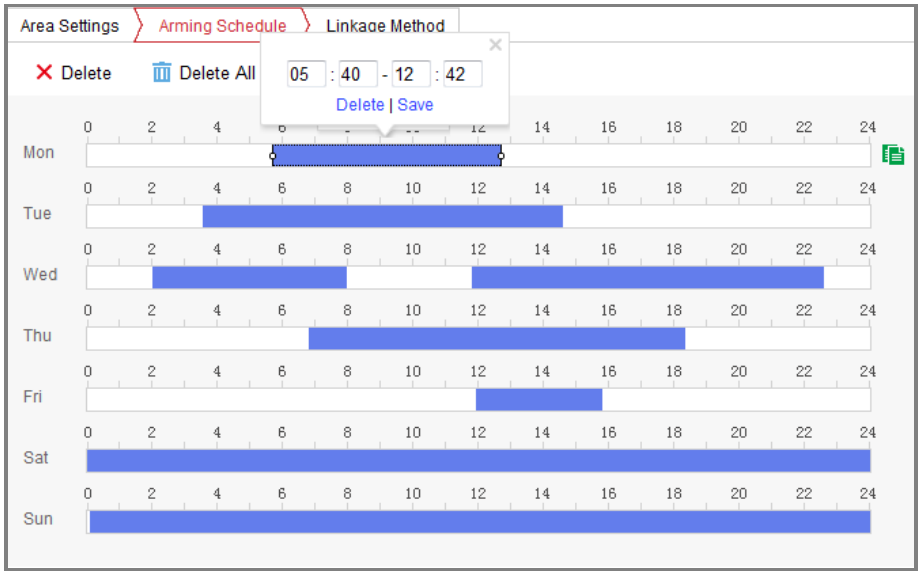


Figure 7. 3 Motion Detection-Edit Arming Schedule

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) (Optional) Move the mouse to the end of each day, and click to copy the current settings to other days.

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

7. Set the alarm actions taken for motion detection.

(1) Click **Linkage Method** tab.

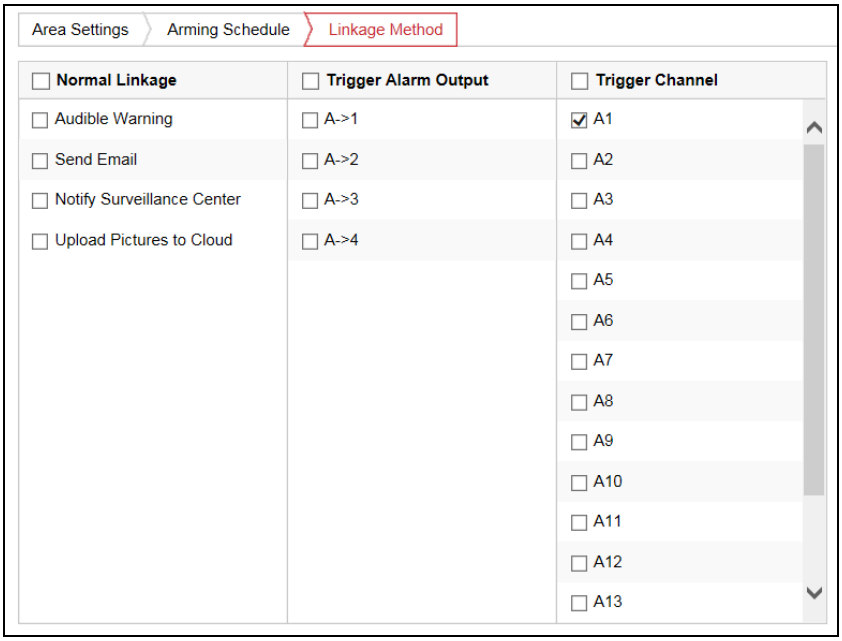


Figure 7. 4 Motion Detection-Linking Method

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

- **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 *Section Configuring Email Settings.*

- **Upload Pictures to Cloud**

Capture the image when an alarm is triggered and upload the picture to cloud.

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

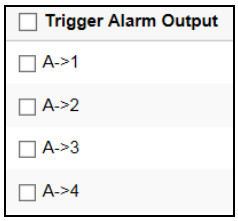


Figure 7. 5 Motion Detection-Trigger Alarm Output

NOTE

To trigger an external alarm output when an event occurs, you need to go to the Alarm Output Settings to set the related parameters. Refer to *Chapter 7.1.3 Configuring Alarm Output* for reference.

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

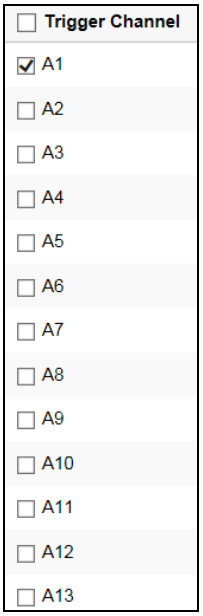


Figure 7. 6 Motion Detection-Alarm Linked Recording

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

7.1.2 Configuring Alarm Input

Steps:

1. Go to **Configuration> Event > Basic Event > Alarm Input** to enter the Alarm Input Settings page.
2. Select the **Alarm Input No.**
3. Select the **Alarm Type**. The alarm type can be NO (Normally Open) and NC (Normally Closed).
4. Enter the **Alarm Name**.
5. Check **Enable Alarm Input Handling**.
6. Click **Arming Schedule** tab to set the arming schedule for the alarm input. Please refer to *Step 6* in *Chapter 7.1.1 Configuring Motion Detection*.

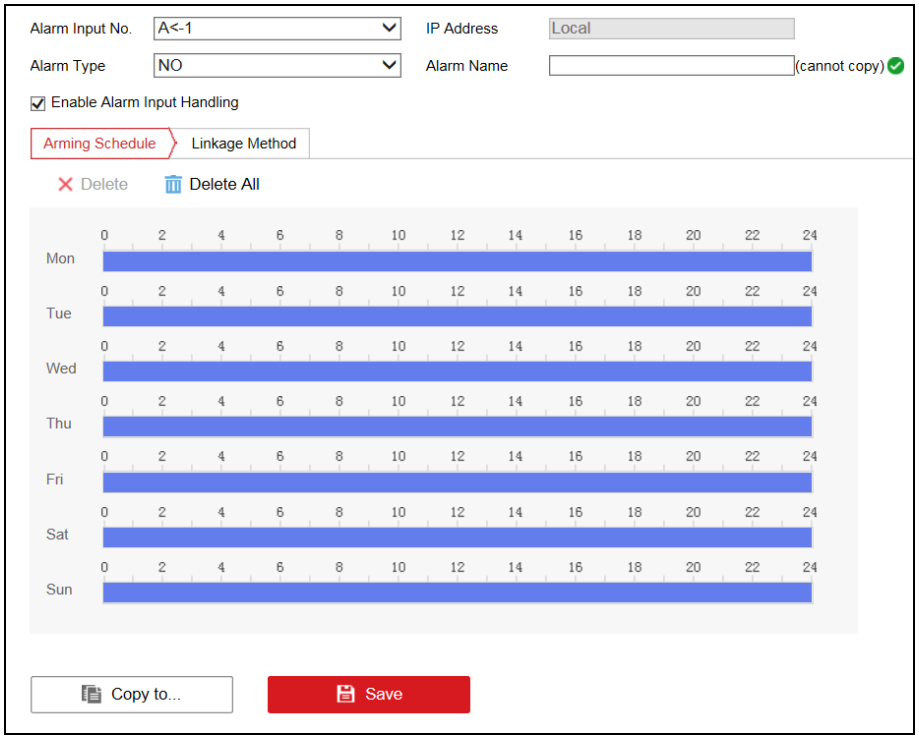


Figure 7. 7 Alarm Input Settings-Arming Schedule

7. Click the **Linkage Metho**d tab to set the actions taken for the alarm input. Please refer to *Step 7* in *Chapter 7.1.1 Configuring Motion Detection*.

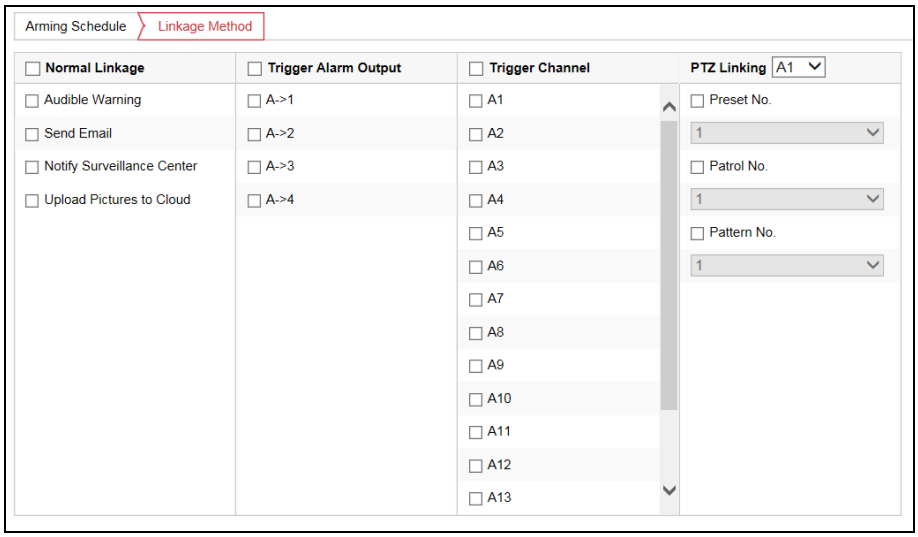


Figure 7. 8 Alarm Input Settings-Linkage Method

8. You can also select the PTZ linking for the alarm input if your camera is installed with a pan/tilt unit.
   (1) Select the PTZ Linking channel.
   (2) Check the relative checkbox to enable preset calling, patrol calling or pattern calling.
9. (Optional) Click **Copy to** to copy your settings to other alarm inputs.
10. Click **Save** to save the settings.

7.1.3 Configuring Alarm Output

Steps:

1. Go to **Configuration> Event > Basic Event > Alarm Output** to enter the Alarm Output Settings page.

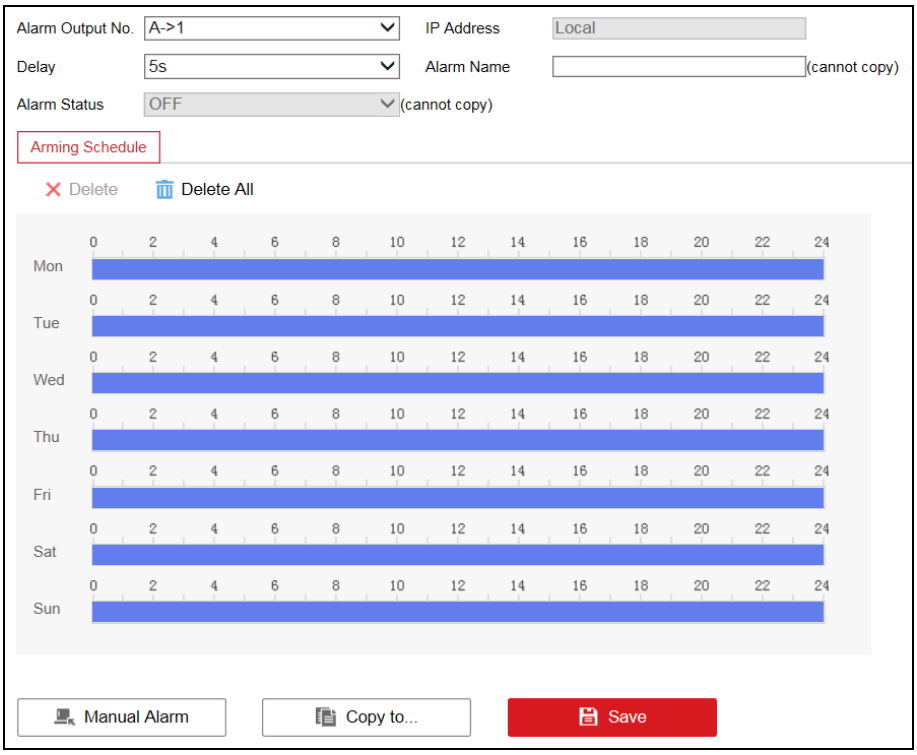


Figure 7. 9 Motion Detection-Alarm Output Settings

2. Select the **Alarm Output No.**
3. Set the **Delay** time 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 **Arming Schedule** tab to set the arming schedule for the alarm input. Please refer to *Step 6* in *Chapter 7.1.1 Configuring Motion Detection*.
5. (Optional) Click **Copy to** to copy your settings to other alarm outputs.
6. Click **Save** to save the settings.

7.1.4 Configuring Video Loss Alarm

Steps:

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

Figure 7. 10 Video Loss Alarm Settings

2. Select the camera to configure the video loss alarm.
3. Check **Enable Video Loss Detection**.
4. Set the arming schedule for video loss detection. Please refer to *Step 6* in *Chapter 7.1.1 Configuring Motion Detection.*
5. Set the actions taken for video loss detection. Please refer to *Step 7* in *Chapter 7.1.1 Configuring Motion Detection.*
6. Click **Save** to save the settings.

7.1.5 Configuring Video Tempering Alarm

Purpose:

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

Steps:

1. Go to **Configuration> Event > Basic Event > Video Tempering**.
2. Select the camera to configure the video tampering detection alarm.

Figure 7. 11 Video Tempering Alarm Settings

3. Check **Enable Video Tempering**.
4. Set the tamper-proof area. Please refer to *Step 5* in *Chapter 7.1.1 Configuring Motion Detection*.
5. Set the arming schedule for tamper-proof. Please refer to *Step 6* in *Chapter 7.1.1 Configuring Motion Detection.*
6. Set the actions taken for the tamper-proof alarm. Please refer to *Step 7* in *Chapter 7.1.1 Configuring Motion Detection.*
7. Click **Save** to save the settings.

7.1.6 Handling Exception

The exception type can be HDD full, HDD error, network disconnected, IP address conflicted, illegal login, and record exception.

Steps:

1. Go to **Configuration> Event > Basic Event > Exception**.
2. Check the checkbox to set the actions taken for the exception alarm. Please refer to *Step 7* in *Chapter 7.1.1 Configuring Motion Detection*.

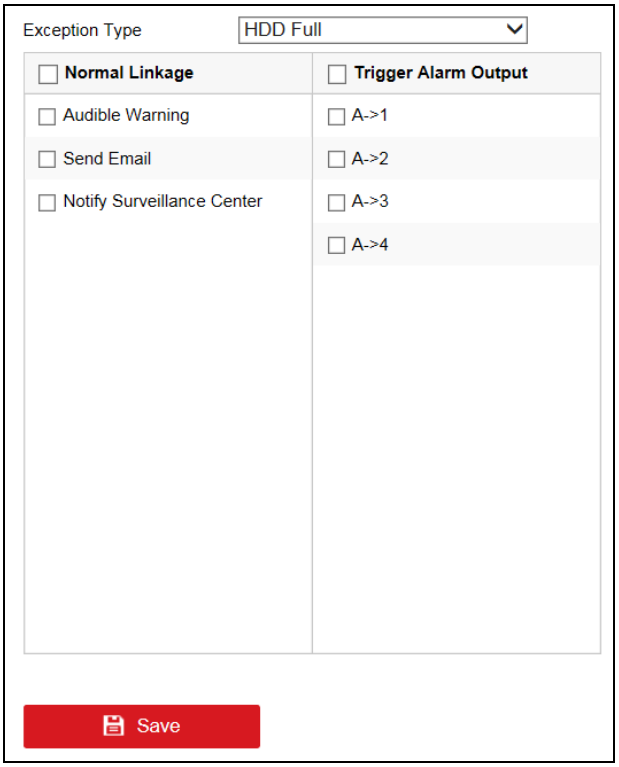


Figure 7. 12 Handling Exceptions

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

7.2 Configuring Smart Event

You can configure the smart events by following the instructions in this section, including audio exception detection, scene change detection, intrusion detection, and line crossing detection. These events can trigger the linkage methods, such as Notify Surveillance Center, Send Email, Trigger Alarm Output, etc.

7.2.1 Configuring Audio Exception Detection

Purpose:

Audio exception detection function detects the abnormal sounds in the surveillance scene, such as the sudden increase/decrease of the sound intensity, and some certain actions can be taken when the alarm is triggered.

Audio exception detection function varies according to different camera models.

Steps:

1. Go to **Configuration > Event > Smart Event > Audio Exception Detection**.

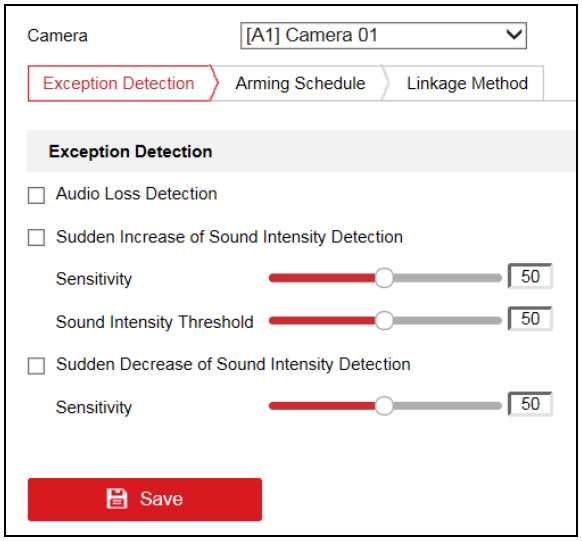


Figure 7. 13 Audio Exception Detection

2. Select the **Camera**.
3. Check the checkbox of **Audio Loss Detection** to enable the audio loss detection function.
4. Check the checkbox of **Sudden Increase of Sound Intensity Detection** to detect the sound steep rise in the surveillance scene. You can set the detection sensitivity and threshold for sound steep rise.
5. Check the checkbox of **Sudden Decrease of Sound Intensity Detection** to detect the sound steep drop in the surveillance scene. You can set the detection sensitivity and threshold for sound steep drop.
   - **Sensitivity**: Range [1-100], the smaller the value is, the more severe the change should be to trigger the detection.
   - **Sound Intensity Threshold**: Range [1-100], it can filter the sound in the environment, the louder the environment sound, the higher the value should be. You can adjust it according to the real environment.
6. Click **Arming Schedule** to set the arming schedule. Refer to *Step 6* in *Chapter 7.1.1 Configuring Motion Detection.*
7. Click **Linkage Method** to set the linkage methods for audio exception. Refer to *Step 7* in *Chapter 7.1.1 Configuring Motion Detection*.
8. Click **Save** to save the settings.

7.2.2 Configuring Intrusion Detection

Purpose:

Intrusion detection function detects people, vehicle or other objects which enter and loiter in a pre-defined virtual region, and some certain actions can be taken when the alarm is triggered.

NOTE

Intrusion detection function varies according to different camera models.

Steps:

1. Go to **Configuration> Event > Smart Event > Intrusion Detection**.

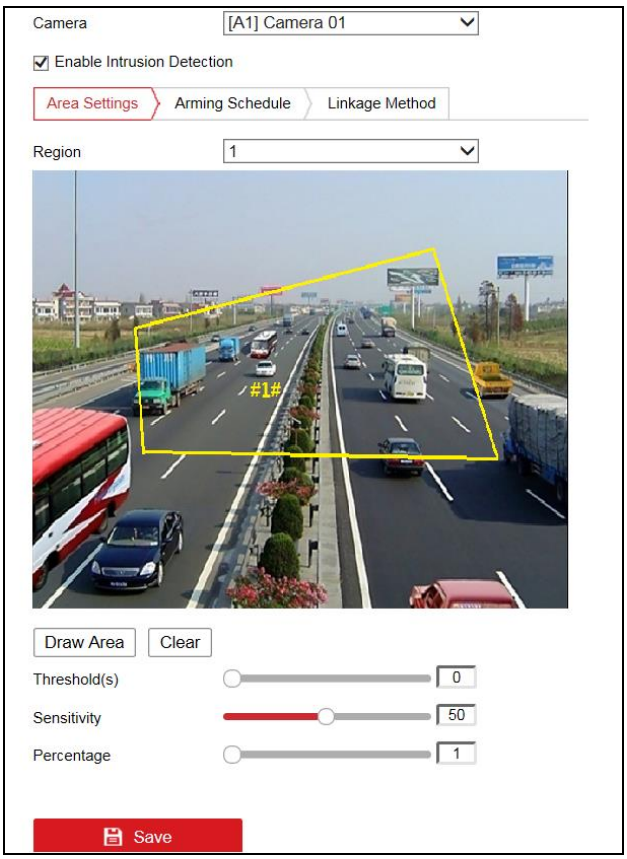


Figure 7. 14 Intrusion Detection

2. Select the **Camera**.
3. Check the checkbox of **Enable Intrusion Detection** to enable the function.
4. Select a region number from the drop-down list of **Region**.

   Region: A pre-defined vertexes area on the live view image. Targets, such as, people, vehicle or other objects, who enter and loiter in the region will be detected and trigger the set alarm.
5. Click **Area Settings** tab and click **Draw Area** to start the region drawing.
6. Click on the live video to specify the four vertexes of the detection region, and right click to complete drawing.
7. Click **Stop Drawing** when finish drawing.
8. Set the time threshold for intrusion detection.

   Threshold: Range [0-2s], the threshold for the time of the object loitering in the region. If you set the value as 0, alarm is triggered immediately after the object entering the region.
9. Drag the slider to set the sensitivity value.

   Sensitivity: Range [1-100]. It stands for the percentage of the body part of an acceptable target that goes across the pre-defined line.

   Sensitivity = S1/ST*100

   S1 stands for the target body part that goes across the pre-defined line. ST stands for the complete target body.

   Example: if you set the value as 60, the action can be counted as a line crossing action only when 60 percent or more body part goes across the line.

NOTE

The **Sensitivity** of the detection is supported by certain camera models. Refer to actual display for details.

10. Drag the slider to set the percentage.

    Percentage: Range [1-100]. Percentage defines the ratio of the in-region part of the object which can trigger the alarm. For example, if the percentage is set as 50%, when the object enters the region and occupies half of the whole region, the alarm is triggered.

11. Repeat the above steps to configure other regions. Up to 4 regions can be set. You can click the **Clear** button to clear all pre-defined regions.
12. Click **Arming Schedule** to set the arming schedule. Refer to *Step 6* in *Chapter 7.1.1 Configuring Motion Detection.*
13. Click **Linkage Method** to select the linkage methods for intrusion detection. Refer to *Step 7* in *Chapter 7.1.1 Configuring Motion Detection*.
14. Click **Save** to save the settings.

7.2.3 Configuring Line Crossing Detection

Purpose:

Line crossing detection function detects people, vehicle or other objects which cross a pre-defined virtual line, and some certain actions can be taken when the alarm is triggered.

NOTE

Line crossing detection function varies according to different camera models.

Steps:

1. Go to **Configuration > Event > Smart Event > Line Crossing Detection**.

Figure 7. 15 Line Crossing Detection

2. Select the **Camera**.
3. Check the checkbox of **Enable Line Crossing Detection** to enable the function.
4. Click **Area Settings** tab and select the line from the drop-down list.
5. Click **Draw Area**, and a virtual line is displayed on the live video.
6. Drag the line, and you can locate it on the live video as desired. Click on the line, two red squares are displayed on each end, and you can click-and-drag one of the red squares to define the shape and length of the line.
7. Select the direction for line crossing detection. And you can select the directions as A<->B, A ->B, and B->A.

   A<->B: The object going across the plane with both directions can be detected and alarms are triggered.

   A->B: Only the object crossing the configured line from the A side to the B side can be detected.

   B->A: Only the object crossing the configured line from the B side to the A side can be detected.
8. Click **Stop Drawing** when finish drawing.
9. Drag the slider to set the sensitivity value.

   Sensitivity: Range [1-100]. It stands for the percentage of the body part of an acceptable target that goes across the pre-defined line.

   Sensitivity = S1/ST*100

   S1 stands for the target body part that goes across the pre-defined line. ST stands for the complete target body.

   Example: if you set the value as 60, the action can be counted as a line crossing action only when 60 percent or more body part goes across the line.

   NOTE

   The **Sensitivity** of the detection is supported by certain models. Refer to actual display for details.
10. Repeat the above steps to configure other lines. Up to 4 lines can be set. You can click **Clear** to clear all pre-defined lines.
11. Click the **Arming Schedule** tab to set the arming schedule. Refer to *Step 6* in *Chapter 7.1.1 Configuring Motion Detection*.
12. Click the **Linkage Method** tab to set the linkage methods. Refer to *Step 7* in *Chapter 7.1.1 Configuring Motion Detection*.
13. Click **Save** to save the settings.

7.2.4 Configuring Scene Change Detection

Purpose:

Scene change detection function detects the change of surveillance environment affected by the external factors; such as the intentional rotation of the camera and some certain actions can be taken when the alarm is triggered.

Steps:

1. Go to **Configuration > Event > Smart Event > Scene Change Detection**.

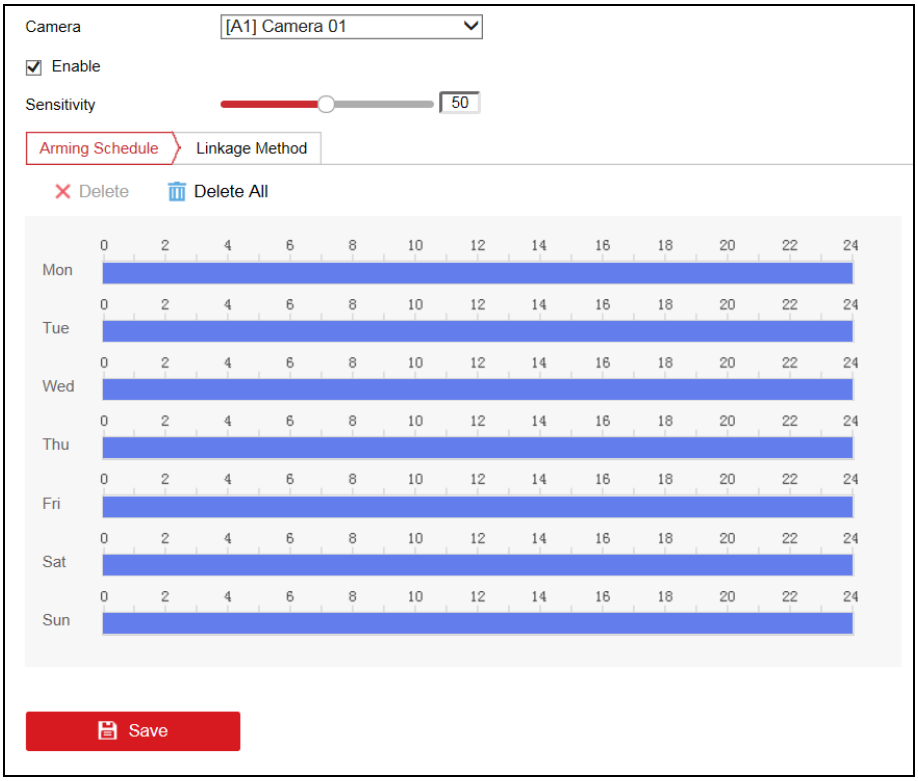


Figure 7. 16 Scene Change Detection

2. Select the **Camera**.
3. Check **Enable** to enable scene change detection.

NOTE

For the analog cameras, the line crossing detection and intrusion detection conflict with sudden scene change detection. You can only enable one function. If you have enabled line crossing detection or intrusion detection, when you enable sudden scene change detection and save the settings, the following attention box pops up as below.

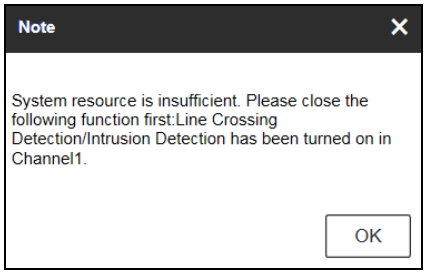


Figure 7. 17 Note

4. Drag the slider to set the sensitivity value.

   Sensitivity: Range [1-100]. The higher the value is, the more easily the change of scene can trigger the alarm.
5. Click the **Arming Schedule** to set the arming schedule. Refer to *Step 6* in *Chapter 7.1.1 Configuring Motion Detection.*
6. Click the **Linkage Method** tab to set the linkage methods. Refer to *Step 7* in *Chapter 7.1.1 Configuring*

Motion Detection.

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

Chapter 8 Record Settings

Before you start

Make sure the encoder is connected with HDD or network disk, and the HDD or network disk has been initialized for the first time to use.

8.1 Configuring Record Schedule

Purpose:

Set the record schedule, and then the camera will automatically start/stop recording according to the configured schedule.

Steps:

1. Go to **Configuration > Storage > Schedule Settings > Record Schedule** to enter record schedule settings page.

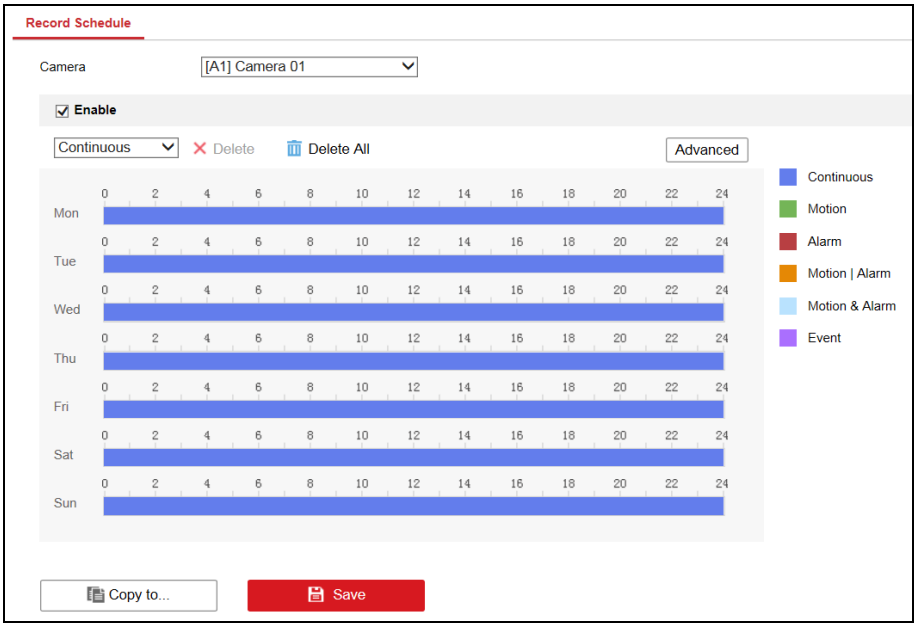


Figure 8. 1 Record Schedule Settings

2. Select the **Camera** to configure the record schedule.
3. Check the checkbox of **Enable** to enable scheduled recording.
4. Select a **Record Type**. The record type can be Continuous, Motion Detection, Alarm, Motion | Alarm, Motion & Alarm, and Event.
   - **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 Detection**, 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 *Chapter 7.1.1 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. Refer to *Chapter 7.1.2 Configuring Alarm Input*.

- **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. Refer to *Chapter 7.1.1 Configuring Motion Detection* and *Chapter 7.1.2 Configuring Alarm Input*.

- **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/capture schedule, you have to configure the settings on the **Motion Detection** and **Alarm Input Settings** interfaces. Refer to *Chapter 7.1.1 Configuring Motion Detection* and *Chapter 7.1.2 Configuring Alarm Input*.

- **Event:**

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

5. Drag the mouse on the time bar to set the record schedule.
6. Click **Advanced** to configure advanced record parameters**.**
   - **Pre-record:** The Pre-Record time can be configured as No Pre-Record, 5 s, 10 s, 15 s, 20 s, 25 s 30 s, or not limited.
   - **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.
   - **Record Audio:** Enable or disable the audio record.
   - **Stream Type:** Select the Main Stream, Sub-Stream, or Dual-Stream for analog camera recording.
   - **Expired Time:** The expired time is the longest time for a record file to be kept in the HDD, if the deadline is reached, the file will be deleted. You can set the expired time to 0, and then the file will not be deleted. The actual keeping time for the file should be determined by the capacity of the HDD.

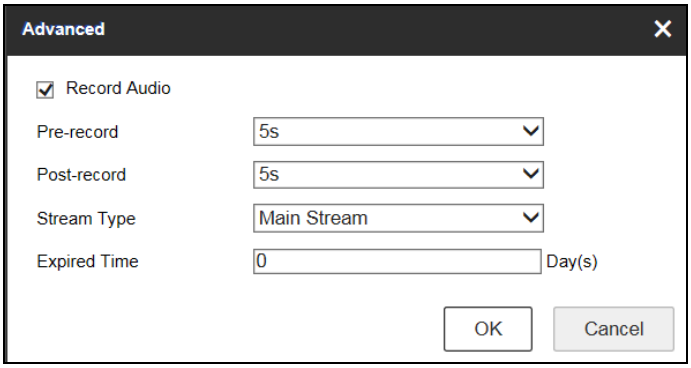


Figure 8. 2 Advanced Settings

7. If you want to copy the record schedule settings of the current camera to other cameras, click **Copy to** to copy

the settings.

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

8.2 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. Go to **Configuration> Storage > Advanced Settings> Holiday** to enter holiday settings page.

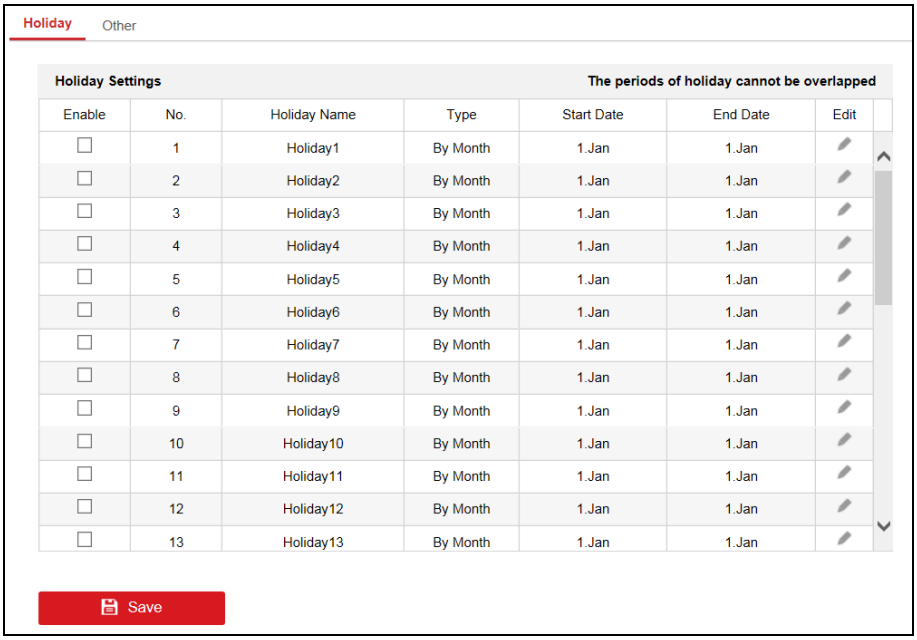


Figure 8. 3 Holiday Settings

2. Select an item from the list and click to edit the holiday.
   (1) Edit the **Holiday Name**.
   (2) Select the holiday type from the drop-down list to by month, by week or by date.
   (3) Set the **Start Date** and **End Date**.
   (4) Click **OK** to save the settings and return to the Holiday Settings page.

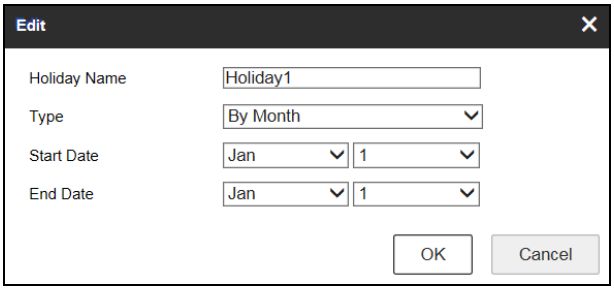


Figure 8. 4 Edit Holiday

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

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

Chapter 9 HDD Management

9.1 Initializing HDD

Purpose:

A newly installed hard disk drive (HDD) must be initialized before it can be used with your encoder.

Steps:

1. Go to **Configuration > Storage > Storage Management > HDD Management**.

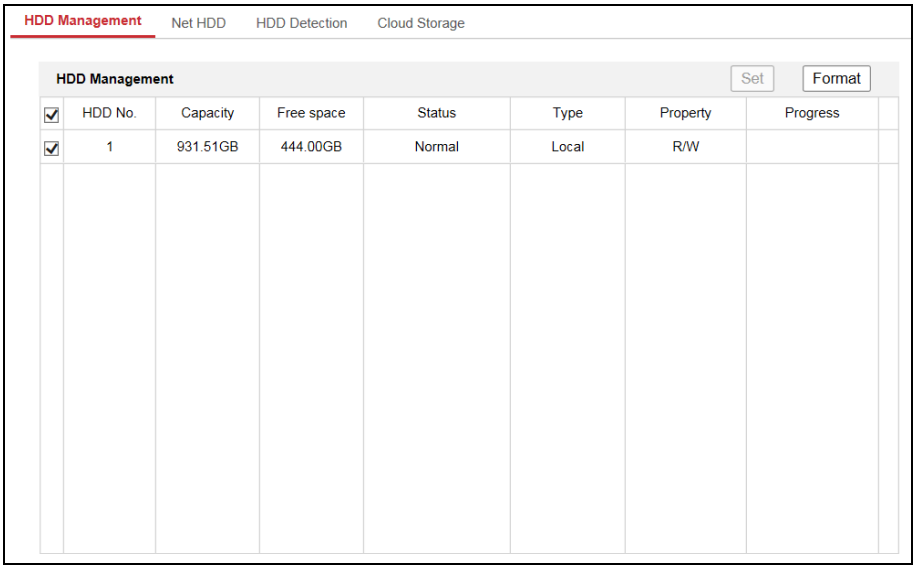


Figure 9. 1 HDD Management

2. Check the HDD information such as the capacity, free space, status, type, property, etc.
3. Select HDD to be initialized.
4. Click **Format** to initialize it.

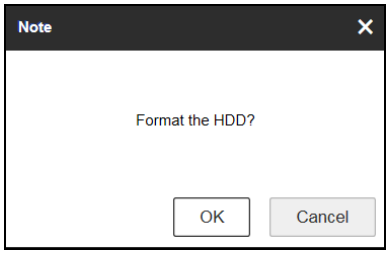


Figure 9. 2 Confirm Initialization

5. Click **OK** to start initialization.

   After the HDD has been initialized, the status of the HDD will change from *Uninitialized* to *Normal*.

NOTE

Initializing the HDD will erase all data on it.

9.2 Configuring Net HDD

For the models with SATA disks connected, the configuration of network disk is selectable.

Before you start:

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

Steps:

1. Go to **Configuration** > **Storage** > **Storage Management** > **Net HDD**.

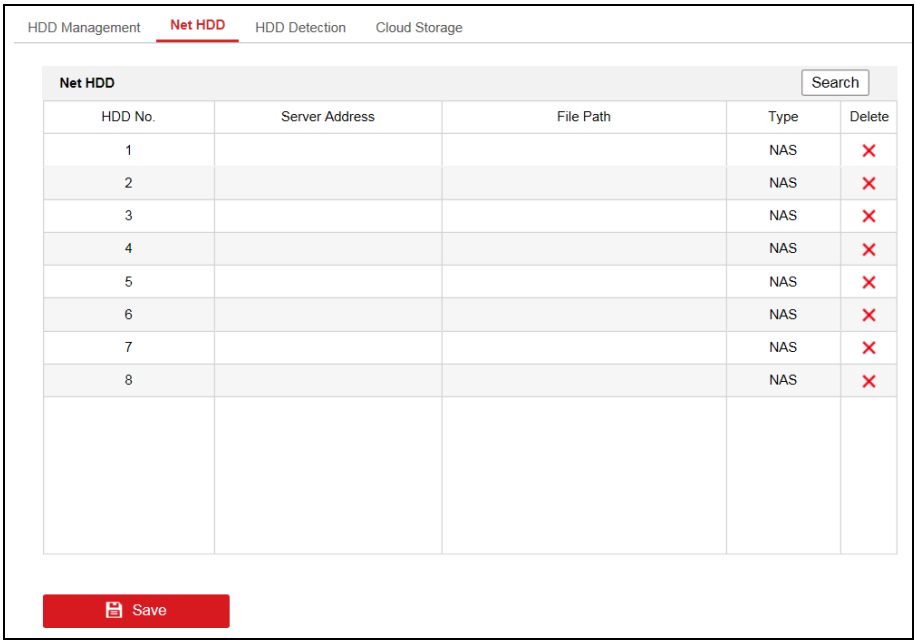


Figure 9. 3 Net HDD

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.
   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.
   4) Select the searched NAS or IP SAN disk from the list and click **OK** to add it.

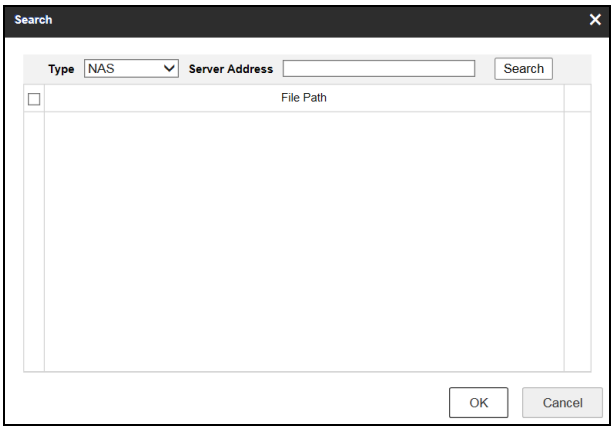


Figure 9. 4 Search Net HDD

3. 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: 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: 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 **Save** to add the configured network disk.

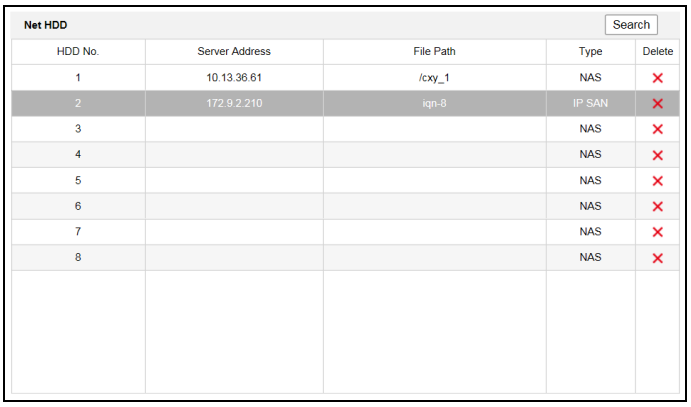


Figure 9. 5 Added Net HDD

5. Initialize the added network disk.

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

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

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

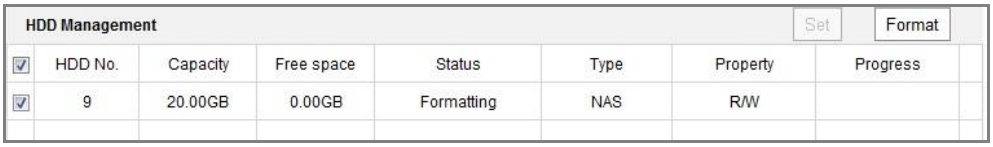


Figure 9. 6 Initial Disk

   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.

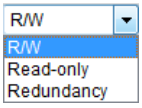


Figure 9. 7 Set HDD Property

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 and 1 IP SAN disk can be connected.

9.3 Checking S.M.A.R.T. Information

Purpose:

The S.M.A.R.T. *(*Self-Monitoring, Analysis and Reporting Technology*)* is a monitoring system for HDD to detect *a*nd report on various indicators of reliability in the hopes of anticipating failures.

Steps:

1. Go to **Configuration** > **Storage** > **Storage Management** > **HDD Detection**.
2. Click the **S.M.A.R.T. Settings** tab to enter the page.
3. Select the HDD to view its S.M.A.R.T. information list, as shown below.

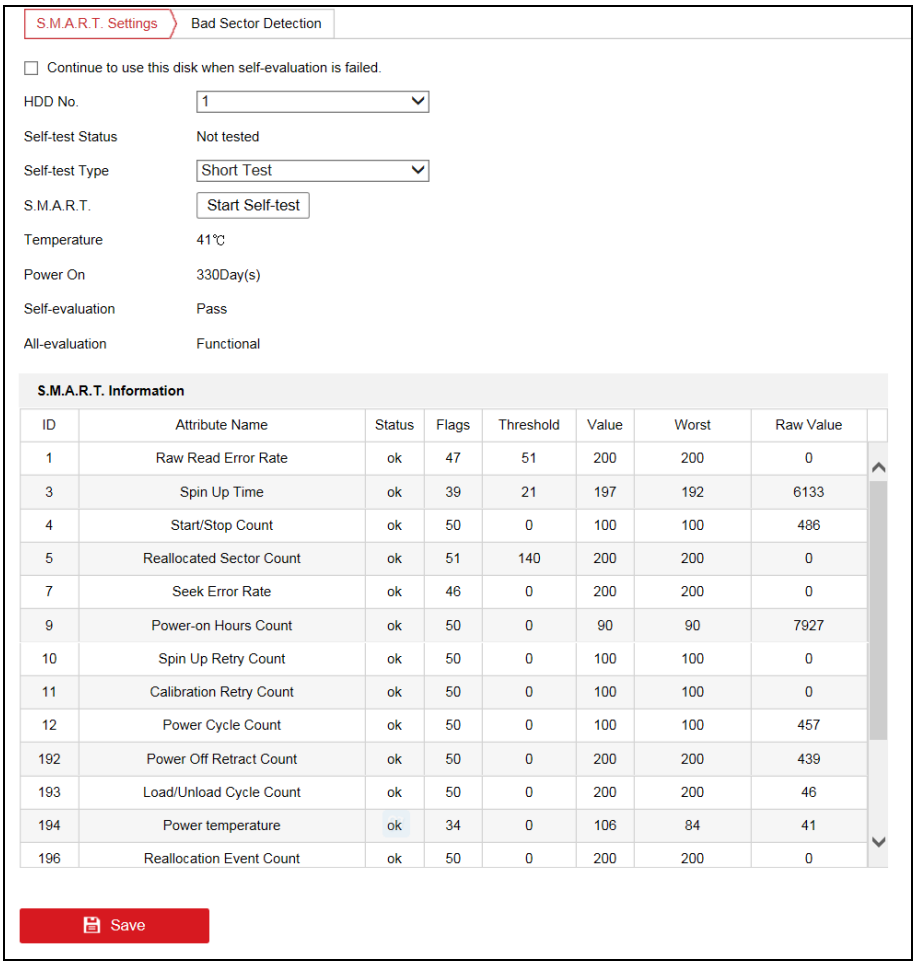


Figure 9. 8 S.M.A.R.T. Information

NOTE

If you want to use the HDD even when the S.M.A.R.T. checking is failed, you can check the checkbox before the **Continue to use this disk when self-evaluation is failed** item.

9.4 Detecting Bad Sector

Purpose

You can detect the bad sector of the HDD to check the status of the HDD.

1. Go to **Configuration** > **Storage** > **Storage Management** > **HDD Detection**.
2. Click the **Bad Sector Detection** tab to enter the page.
3. Select a HDD.
4. Select the **Test Type**.
5. Click **Start detect** to start detecting.

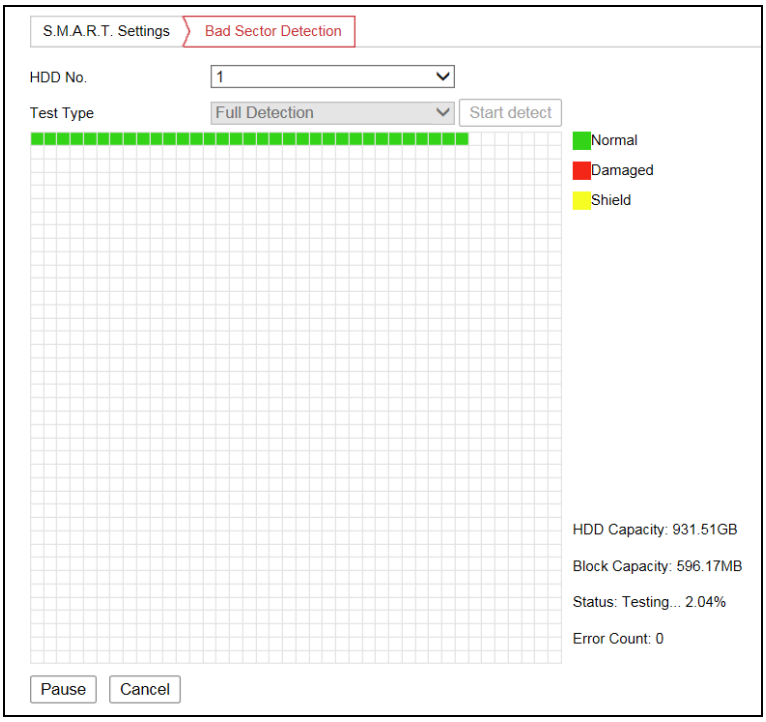


Figure 9. 9 Bad Sector Detection

6. (Optional) Click **Pause** to pause the detection or click **Cancel** to cancel the detection.

9.5 Configuring Cloud Storage

Purpose:

The cloud storage facilitates you to upload and download the recorded files at any time and any place, which can highly enhance the efficiency.

1. Go to **Configuration** > **Storage** > **Storage Management** > **Cloud Storage**.
2. Check **Enable Cloud Storage** checkbox to enable the feature.
3. Select the **Cloud Type** from the drop-down list to One Drive, Google Drive or Drop Box.

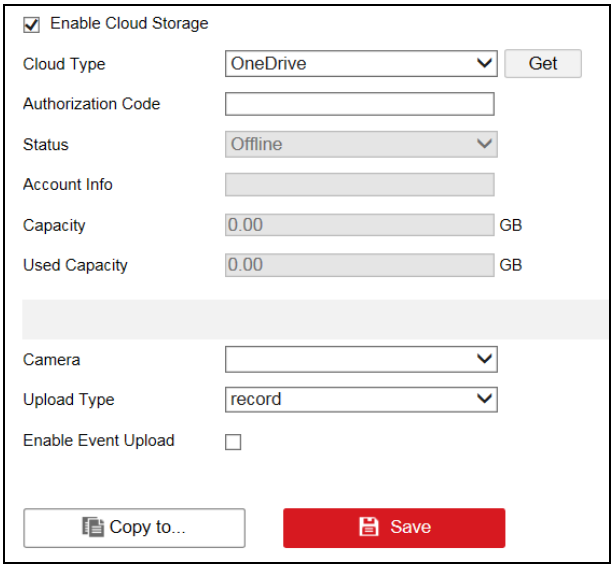


Figure 9. 10 Cloud Storage

4. Click **Get** to get the authentication code. And then copy the authentication code to the **Authentication Code** text filed.
5. Click **Save** to save the settings.
6. Enter the cloud storage page again about 20s later. When the **Status** shows online, it indicates the successful registration.
7. Configure the recording schedule. For detailed recording schedule, refer to *Chapter 8.1 Configuring Record Schedule*.
8. Upload the event triggered recording files to the cloud storage.
   1) Enter the cloud storage page, and select the camera you have set in the recording schedule interface.
   2) Select the **Upload Type**.
   3) Check the **Enable Event Upload** checkbox.
   4) Click **Save** to save the settings.

NOTE

- Only the sub-stream recorded files can be uploaded to the Cloud Storage.
- Please configure the event triggered recording schedule and enable the corresponding event type.

9. (Optional) Click **Copy to** to copy the cloud storage settings to other cameras.
10. Click **Save** to save the settings.

9.6 Configuring Other Settings

Purpose:

You can enable HDD sleeping and overwriting, and edit the packet time.

Steps:

1. Go to **Configuration** > **Storage** > **Advanced Settings** > **Other**.

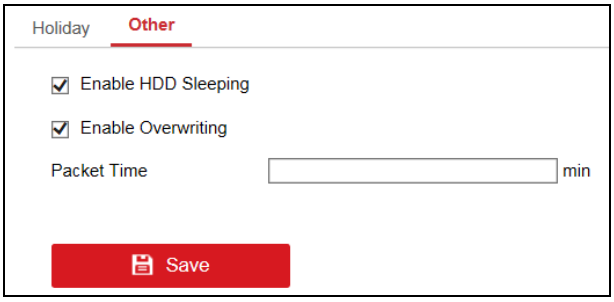


Figure 9. 11 Other Settings

2. Check **Enable HDD Sleeping**, thus to decrease the power consumption of the device and extend the life of the HDDs if the HDDs are free of working for a long time.
3. Check **Enable Overwriting** to enable HDD overwriting.
4. Enter the **Packet Time**. It ranges from 1 to 300 min.
5. Click **Save** to save the settings.

Chapter 10 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 page.

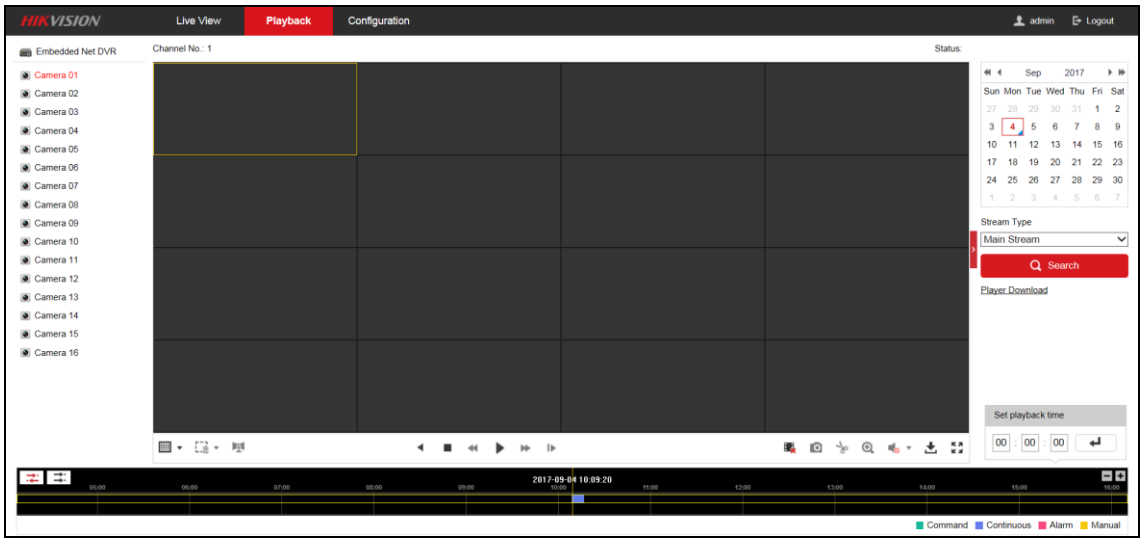


Figure 10. 1 Playback Page

2. Click the camera from the device list for playback.
3. Select the date from the calendar.
4. Select the **Stream Type**.
5. Click **Search**.

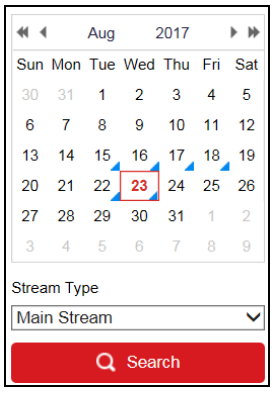


Figure 10. 2 Select Date and Stream Type for Search

6. Click ▶ to play the video file searched on the current date.
7. Click the icons on the toolbar to operate in playback mode.

Figure 10. 3 Playback Toolbar

Table 10. 1 Description of Toolbar Icons

Icon	Operation	Icon	Operation
	Select window-division mode		Reverse playback
/	Play/Pause		Stop playing
	Slow forward		Fast forward
	Play by single frame		Stop all channels from playing
	Capture pictures in playback mode		Download video files
/	Start/Stop clipping video files	/	Audio on/off
	Enable e-PTZ		Full screen

8. Drag the progress bar with the mouse to locate the exact playback point. Or input the time and click to locate the playback point.

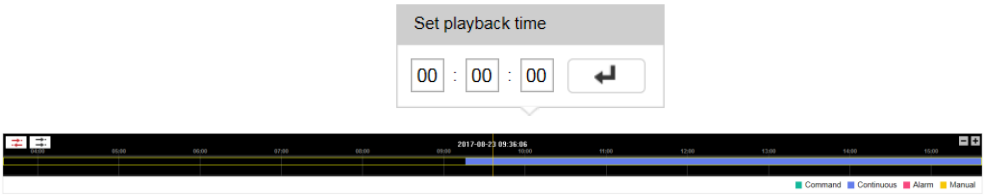


Figure 10. 4 Progress Bar

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

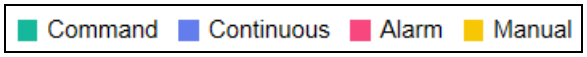


Figure 10. 5 Video Types

9. (Optional) Click to realize synchronous playback. Up to 4 cameras can be played back simultaneously. Click to stop synchronous playback.

Chapter 11 User Management

11.1 User Management

Go to **Configuration > System > User Management > User Management** to enter the User Management page.

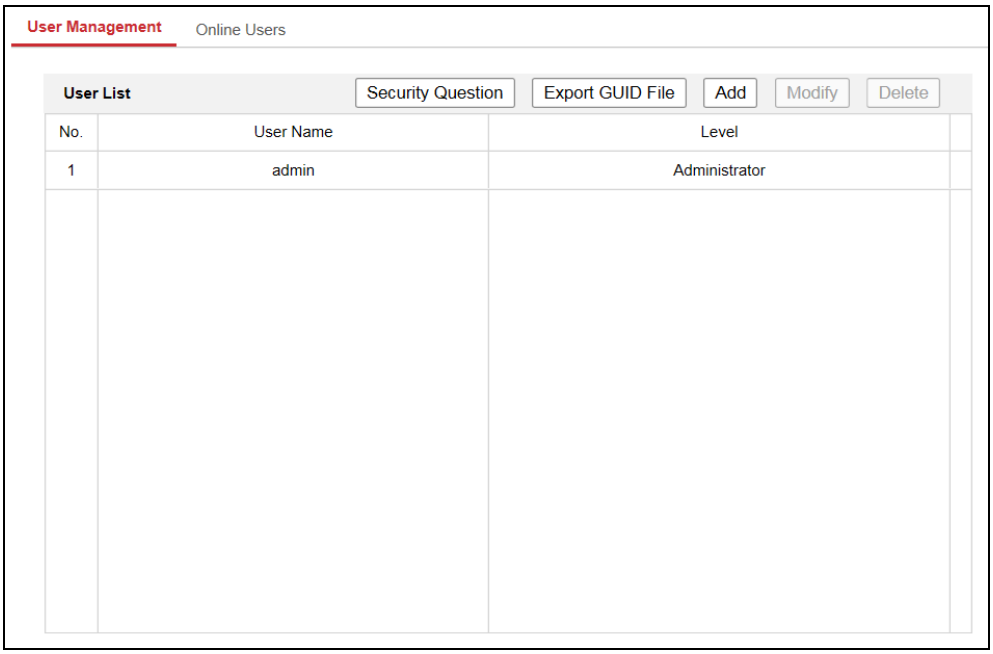


Figure 11. 1 User Management

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

11.1.1 Adding a User

Steps:

1. Click **Add** to enter the Add User page.
2. Edit the **User Name**.
3. Select the **Level** to **Operator** or **User**.
4. Enter the **Admin Password**.
5. Enter the **Password** of the added user.
6. Confirm the same password.

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

monthly or weekly can better protect your product.

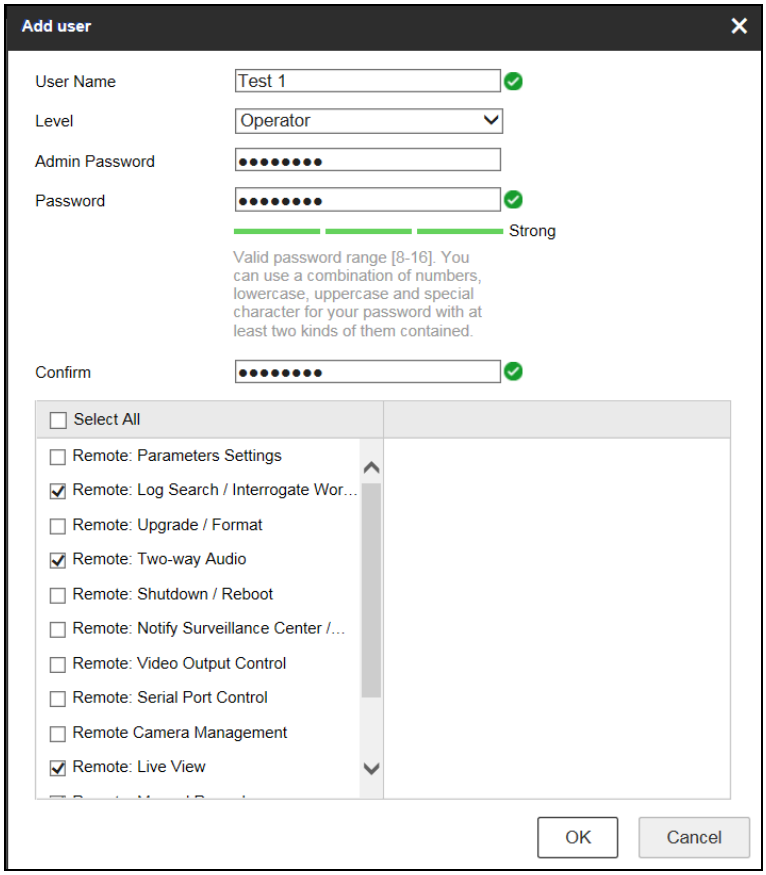


Figure 11. 2 Add a User

Different user level is given 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.

7. Configure the user permissions for the created user account.
8. Click **OK** to add the user.

Figure 11. 3 Added User

11.1.2 Modifying a User

Steps:

1. Select a user account from the list on the User Management page to be modified.

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

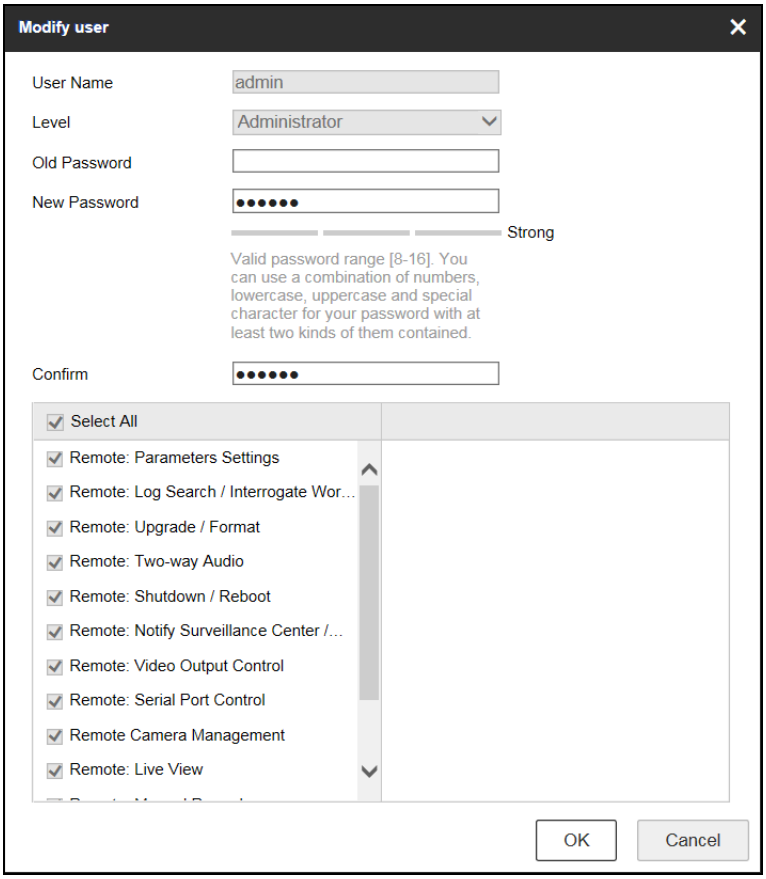


Figure 11. 4 Modify the Admin

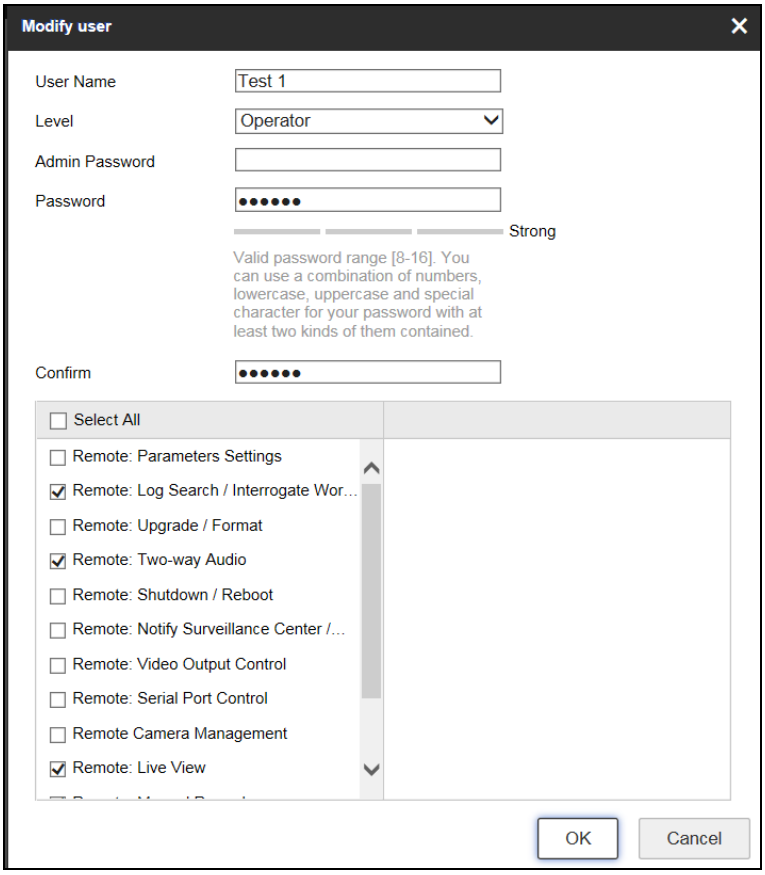


Figure 11. 5 Modify the Operator

3. Modify the editable parameters. You are highly recommended to use the strong password.
4. Configure the user permission for the user.
5. Click **OK** to save the settings.

NOTE

You need the admin password to modify the admin user or operator.

11.1.3 Deleting a User

Steps:

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

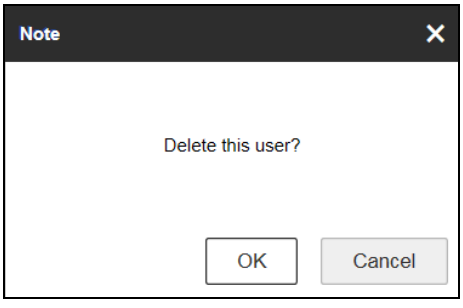


Figure 11. 6 Delete a User

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

11.1.4 Configuring Security Questions

Purpose:

You can set the security question for the admin and other users. In case of forgetting the password, you can retrieve the password by answering the security questions.

Steps:

1. Go to **Configuration > System > User Management > User Management**.
2. Select a user from the user list.
3. Click **Security Question** and the window pops up as below.

Figure 11. 7 Confirm the Admin Password

4. Enter the **Admin Password**.
5. Click **OK** to enter the Security Question Configuration page.

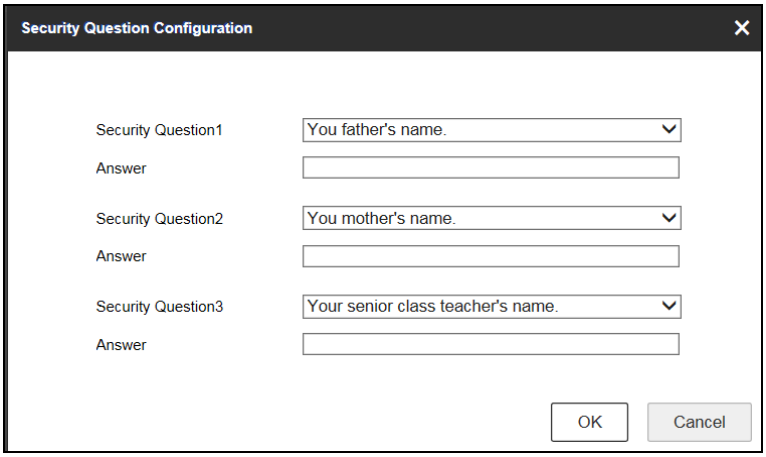


Figure 11. 8 Security Question Configuration

6. Select the **Security Question** and enter the answer in the **Answer** text field.
7. Click **OK** to save the settings.

11.1.5 Exporting GUID File

Purpose:

You can export GUID file to the USB flash drive for retrieving the forgotten password.

Steps:

1. Go to **Configuration > System > User Management > User Management**.
2. Click **Export GUID File** and the window pops up as below.

Figure 11. 9 Confirm the Admin Password

3. Enter the **Admin Password** and click **OK**.
4. Select the directory to save the GUID file. Then the note window pops up as below.

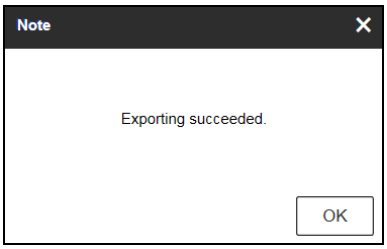


Figure 11. 10 Note

5. Click **OK** to finish exporting GUID file.

11.2 Online Users

Purpose:

You can see the current users who are visiting the device through this interface. User information, such as user name, level, IP address, and operation time, is displayed in the User List.

Click **Refresh** to refresh the list.

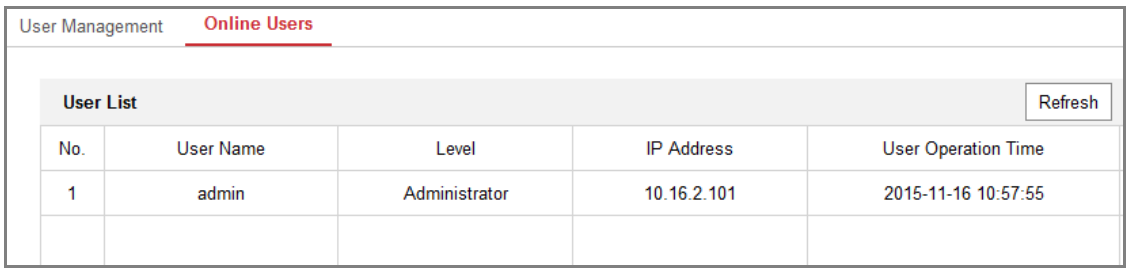


Figure 11. 11 View the Online Users

Chapter 12 Log Search, Maintenance and Security Settings

12.1 Searching Log

Purpose

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

Before you start

The log function can be realized only when the encoder is connected with HDD or network disk. And make sure the HDD or network disk has been initialized for the first time to use.

Steps:

1. Go to **Configuration > System > Maintenance > Log**.
2. Set the log search conditions to refine your search, including the **Major Type**, **Minor Type**, **Start Time** and **End Time**.
3. Click **Search** to start searching log files.
4. The matched log files will be displayed on the list shown below.

NOTE

Up to 2000 log files can be displayed each time.

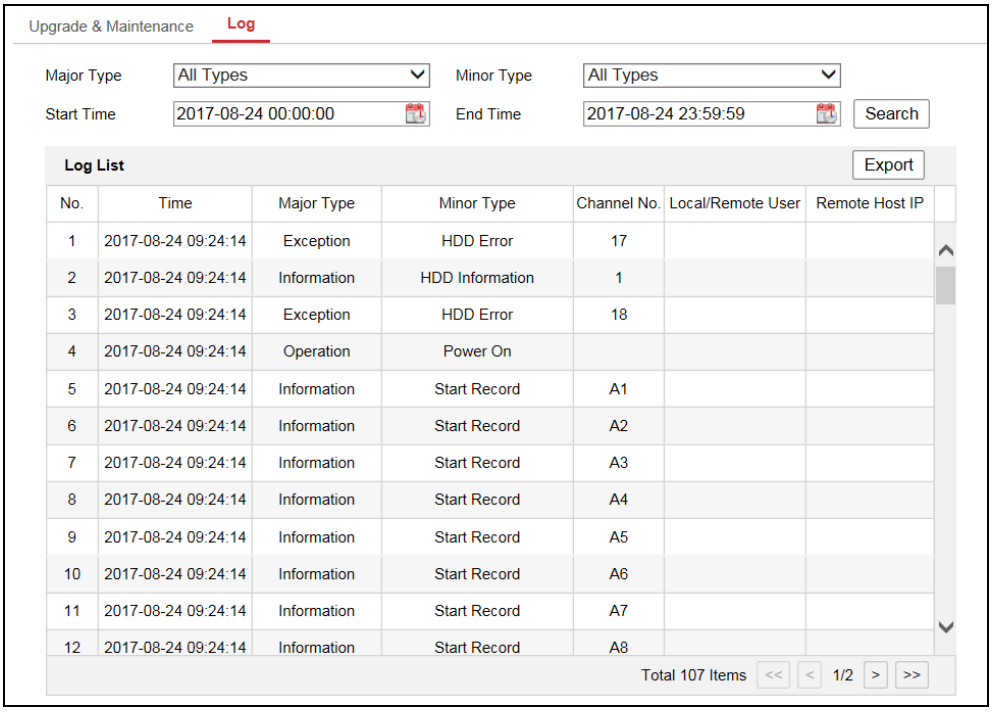


Figure 12. 1 Search Log

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

12.2 Maintenance

Go to **Configuration > System > Maintenance > Upgrade & Maintenance** to enter the Maintenance page of the encoder.

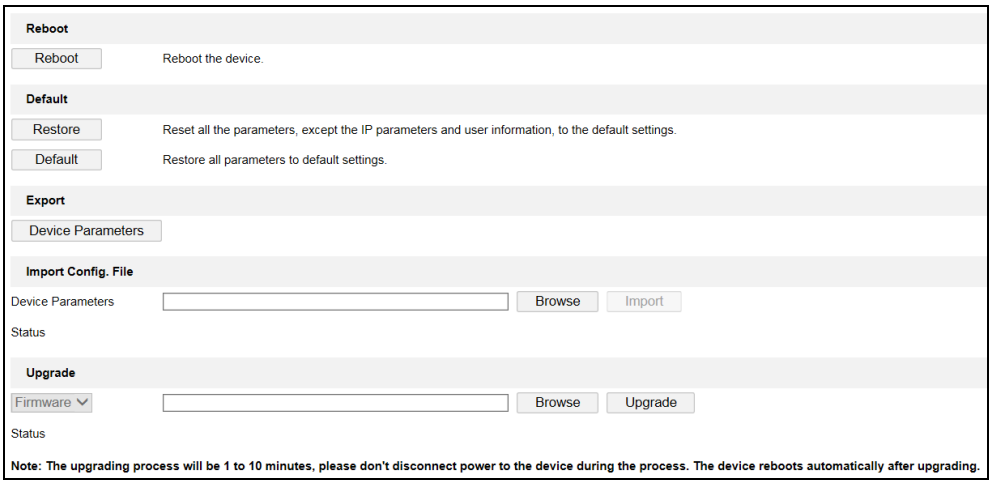


Figure 12. 2 Maintenance

12.2.1 Rebooting the Device

Steps:

1. Go to **Configuration > System > Maintenance > Upgrade & Maintenance > Reboot.**

Figure 12. 3 Reboot the Device

2. Click **Reboot** and the window pops up as below.

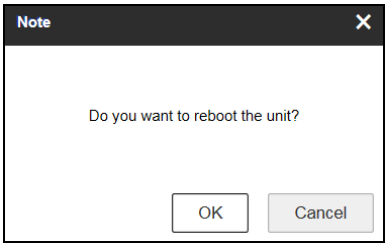


Figure 12. 4 Note

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

12.2.2 Restoring Default Settings

Steps:

1. Go to **Configuration > System > Maintenance > Upgrade & Maintenance > Default.**

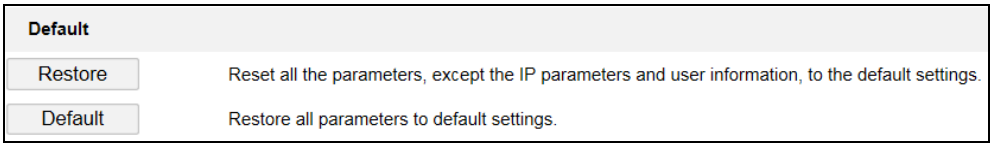


Figure 12. 5 Restore Default Settings

2. Click **Restore** or **Default** to restore device parameters.

- **Restore**: Restore the device to the default settings for the parameters except the IP address, subnet mask, gateway and port.
- **Default**: Restore the device to the default settings for all parameters.

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

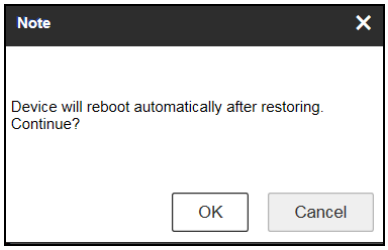


Figure 12. 6 Pop-up Message Box

12.2.3 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 devices if they are to be configured with the same parameters.

- On the **Configuration > System > Maintenance > Upgrade & Maintenance > Import Config. File** page, click **Browse** to select the file from the selected backup device and then click **Import** to import a configuration file.

NOTE

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

- On the **Configuration > System > Maintenance > Upgrade & Maintenance > Export** page, click **Device Parameters** to export configuration files to the selected local backup device.

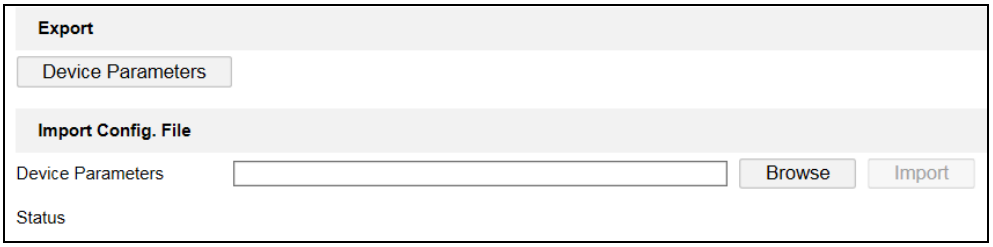


Figure 12. 7 Import/Export Config Files

12.2.4 Upgrading the System

On the **Configuration** > **System** > **Maintenance** > **Upgrade & Maintenance** > **Upgrade** page, click **Browse** to select the local update file and then click **Upgrade** to start remote upgrade.

Figure 12. 8 Remote Upgrade

12.3 Configuring Security Settings

Purpose:

To enable the remote login, and improve the data communication security, the encoder provides the security service for better user experience.

Steps:

1. Go to **Configuration** > **System** > **Security** > **Security Service**.

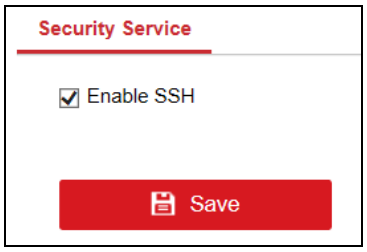


Figure 12. 9 Security Service

2. Check **Enable SSH** to enable the data communication security.
3. Click **Save** to save the settings.

Chapter 13 Specification

Table 13. 1 Specification

Model		DS-6704HUHI-K	DS-6708HUHI-K	DS-6716HUHI-K
Video/Audio input/output	Video input	4-ch	8-ch	16-ch
		BNC interface (1.0 Vp-p, 75 Ω), supporting coaxitron connection		
	HDTVI input	5 MP, 4 MP, 3 MP, 1080p30, 1080p25, 720p60, 720p50, 720p30, 720p25		
	AHD input	1080p25, 1080p30, 720p25, 720p30		
	HDCVI input	1080p25, 1080p30, 720p25, 720p30		
	CVBS input	PAL/NTSC		
	Audio input	4-ch, RCA (2.0 Vp-p, 1 KΩ)		
	Audio output	1-ch, RCA (Linear, 1 KΩ)		
	Synchronous playback	4-ch	8-ch	16-ch
Video/Audio encoding	Video compression	H.265+/H.265/H.264+/H.264		
	Audio compression	G.711u		
	Main stream	5 MP/4 MP/3 MP/1080p/720p/WD1/4CIF/VGA/CIF		
	Frame rate	Main stream: 5 MP@12fps/4 MP@15fps/3 MP@18fps 1080p/720p/WD1/4CIF/VGA/CIF@25fps (P)/30fps (N)		
		Sub-stream: WD1/4CIF/CIF@25fps (P)/30fps (N)		
	Video bit rate	32 Kbps to 10 Mbps		
	Audio bit rate	64 Kbps		
	Dual stream	Support		
Network management	Network protocols	TCP/IP, PPPoE, DHCP, DNS, DDNS, NTP, SADP, SMTP, SNMP, NFS, iSCSI, UPnP™, HTTPS, ONVIF profile S		
Storage	SATA	1 SATA interface	2 SATA interfaces	
	Capacity	Up to 8 TB capacity for each disk		
External interface	Two-way audio input	1-ch, RCA (2.0 Vp-p, 1 KΩ) (using the 1st audio input)		
	Network interface	1, RJ45 10M/100M/1000M self-adaptive Ethernet interface		
	Serial interface	RS-485 (half-duplex); RS-232		
	Alarm in/out	4/1	8/4	16/4
General	Power supply	12 VDC		
	Consumption (without HDD)	≤ 10 W	≤ 20 W	≤ 25 W
	Working temperature	-10 ℃ to +55 ℃ (+14 ℉ to +131 ℉)		
	Working humidity	10% to 90%		
	Dimensions (W × D × H)	315 × 242 × 45 mm (12.4 × 9.5 × 1.8 inch)	380 × 320 × 48 mm (15.0 × 12.6 × 1.9 inch)	
	Weight (without HDD)	≤ 1.16 kg (2.6 lb)	≤ 1.78 kg (3.9 lb)	≤ 2 kg (4.4 lb)

Chapter 14 FAQ

- **Why cannot ping the Encoder?**

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

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

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

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

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

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

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

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

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

First Choice for Security Professionals

www.hikvision.com