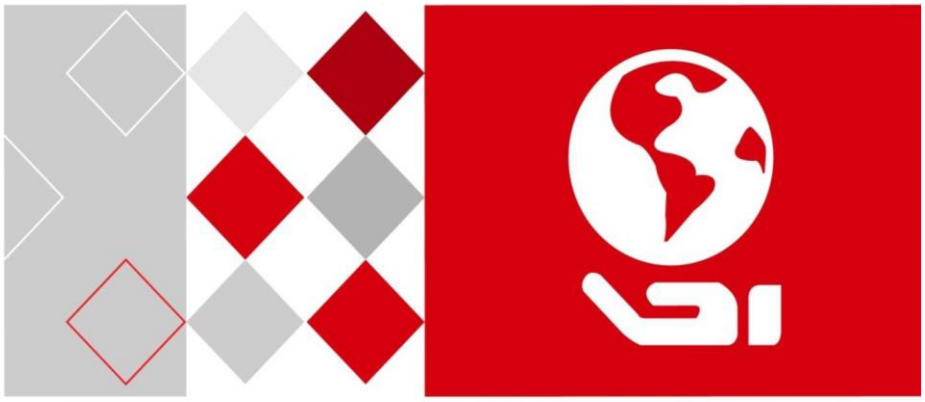


Digital Video Recorder
User Manual

Quick Start Guide

About this Manual

This Manual is applicable to Turbo HD Digital Video Recorder (DVR).

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.

Please use this user manual under the guidance of professionals.

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 ISMART 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 ISMART, 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 ISMART 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. ISMART 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, ISMART 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. ISMART 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.

Symbol Conventions

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

Symbol	Description
NOTE	Provides additional information to emphasize or supplement important points of the main text.
WARNING	Indicates a potentially hazardous situation, which if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
DANGER	Indicates a hazard with a high level of risk, which if not avoided, will result in death or serious injury.

Safety Instructions

- Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.
- In the use of the product, you must be in strict compliance with the electrical safety regulations of the nation and region. Please refer to technical specifications for detailed information.
- Input voltage should meet both the SELV (Safety Extra Low Voltage) and the Limited Power Source with 100~240 VAC, 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.

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.
- The USB interface can only connect to mouse, keyboard or USB flash drive.
- Ensure to use the attached power adaptor only and not to change the adaptor randomly.

TABLE OF CONTENTS

1 Introduction

1.1 Front Panel

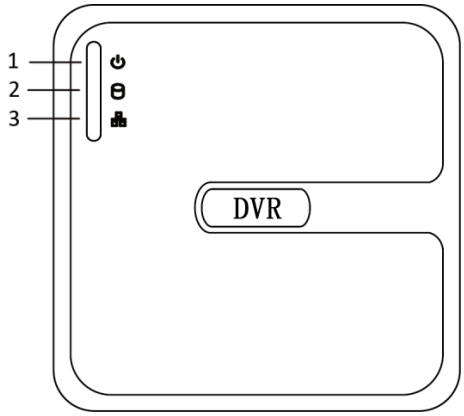


Figure 1.1 Front Panel

Front Panel Description：

NO.	Icon	Description
1		Turns red when DVR is powered up.
2		Turns red when data is being read from or written to HDD.
3		Flickers blue when network connection is functioning properly.

1.2 Rear Panel

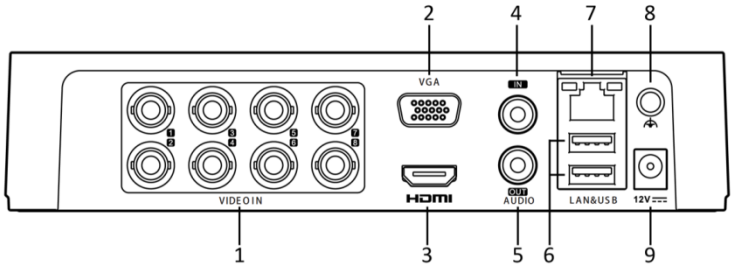


Figure1.2 Rear Panel

Rear Panel Description：

Index	Description	Index	Description
1	Video and Coaxial Audio In	6	USB Interface
2	VGA Interface	7	LAN Network Interface
3	HDMI Interface	8	GND
4	AUDIO IN	9	12 VDC Power Input
5	AUDIO OUT		

1.3 USB Mouse Operation

A regular 3-button (Left/Right/Scroll-wheel) USB mouse can also be used with this device. To use a USB mouse:

Plug USB mouse into one of the USB interfaces on the front panel of the device. The mouse should automatically be detected. If in a rare case that the mouse is not detected, the possible reason may be that the two devices are not compatible, please refer to the recommended the device list from your provider.

The operation of the mouse:

Name	Action	Description
Left-Click	Single-Click	Live view: Select channel and show the quick set menu. Menu: Select and enter.
	Double-Click	Live view: Switch between single-screen and multi- screen.
	Click and Drag	PTZ control: pan, tilt and zoom. Video tampering, privacy mask and motion detection: Select target area. Digital zoom-in: Drag and select target area. Live view: Drag channel/time bar
Right-Click	Single-Click	Live view: Show menu. Menu: Exit current menu to upper level menu.
Scroll-Wheel	Scrolling up	Live view: Previous screen. Menu: Previous item.
	Scrolling down	Live view: Next screen. Menu: Next item.

1.4 Input Method Description

Figure1.3 Soft Keyboard

Description of the buttons on the soft keyboard:

Icon	Description	Icon	Description
0...	Number	A...	English letter
	Lowercase/Uppercase		Backspace
123 ABC	Switch the keyboard		Space
	Positioning the cursor		Enter
#+=	Symbols		Reserved

1.5 HDD Installation

Before you start

Before installing a hard disk drive (HDD), please make sure the power is disconnected from the device. A factory recommended HDD should be used for the installation.

Tools Required: Cross screwdriver

Fix-on-bottom installation is applicable when you need to install and fix the HDD on the device bottom.

Steps

1. Remove the cover from device by unfastening the screws on panels.

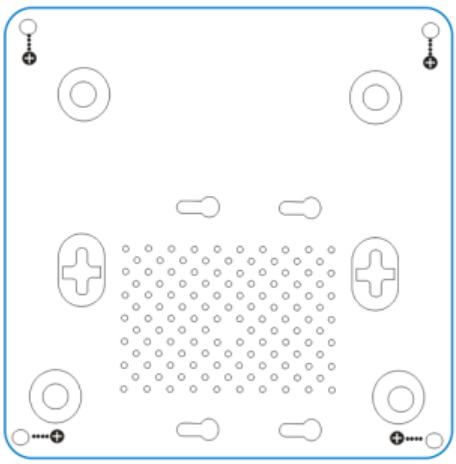


Figure1.3 Device bottom

2. Connect the data cable and power cable.

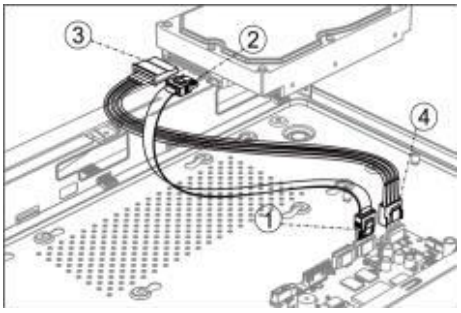


Figure1.4 HDD line

3. Connect one end of data cable to the device motherboard

1) Connect the other end of data cable to HDD.

2) Connect one end of power cable to HDD.

3) Connect the other end of power cable to the device motherboard.

4) Set the device up, match HDD screw threads with the reserved holes on the device bottom, and fix HDD with screws.

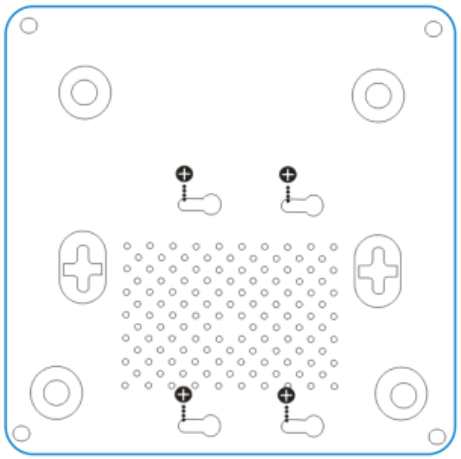


Figure1.5 Fixed HDD

4. Reinstall the device cover and fasten screws.

2 Getting Started

2.1 Start up the Device

Purpose:

Proper startup and shutdown procedures are crucial to expanding the life of the device.

Before you start:

Check that the voltage of the extra power supply is the same with the device's requirement, and the ground connection is working properly.

Connect the device power supply interface and electrical socket with delivered power cable. The Power button on the front panel should be red, indicating the device is receiving the power.

2.2 Activate the Device

Purpose:

For the first-time access, you need to activate the device by setting an admin password. No operation is allowed before activation. You can also activate the device via Web Browser, SADP, or Client Software.

Steps

1. Choose an OSD language

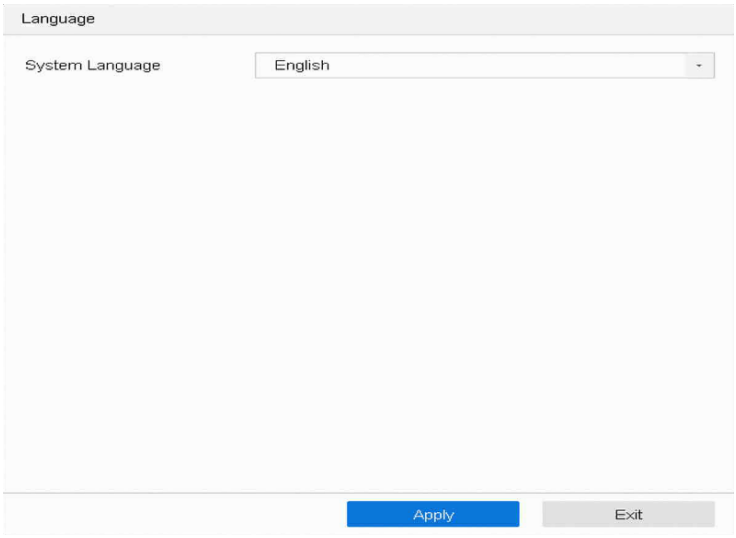


Figure 2.1 Set OSD Language

2. Enter the admin password twice.

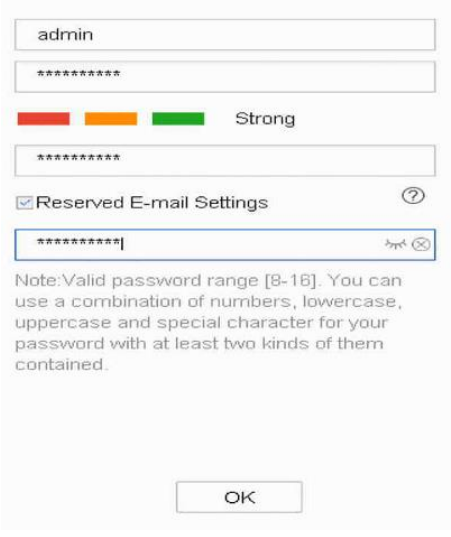


Figure 2.2 Set Admin Password

WARNING

We highly recommend you create a strong password of your own choosing (Using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers, and special characters.) in order to increase the security of your product.

And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

3. Enter the password to activate the IP camera(s) connected to the device.
4. Optionally, check Export GUID, Security Question Configuration, or Reserved E-mail Settings for password resetting in the future.
5. Click OK.

What to do next:

1) When you have enabled **Export GUID**, continue to export the GUID file to the USB flash drive for the future password resetting.
2) When you have enabled Security Question Configuration, continue to set the security questions for the future password resetting.
3) When you have enabled **Reserved E-mail Settings**, continue to set the reserved email for the future password resetting.

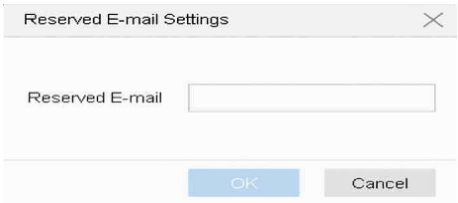


Figure 2.3 Set the Reserved Email

NOTE

- **After the device is activated, you should properly keep the password.**
- **You can duplicate the password to the IP cameras that are connected with default protocol.**

2.3 Configure Unlock Pattern for Login

Purpose:

For the admin user, you can configure the unlock pattern for device login.

Steps

1. After the device is activated, you can enter the following interface to configure the device unlock pattern.
2. Use the mouse to draw a pattern among the 9 dots on the screen. Release the mouse when the pattern is done.
3. Draw the same pattern again to confirm it. When the two patterns match, the pattern is configured successfully.

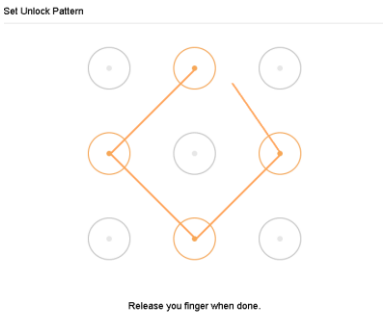


Figure 2.4 Draw the Pattern

NOTE

- **Connect at least 4 dots to draw the pattern.**
- **Each dot can be connected for once only.**

2.4 Login to the Device

2.4.1 Log in via Unlock Pattern

Only the *admin* user has the permission to unlock the device.

Please configure the pattern first before unlocking. Please refer to 2.2 Activate the Device.

Steps

1. Right click the mouse on the screen and select the menu to enter the interface.
2. Draw the pre-defined pattern to unlock to enter the menu operation.

Figure 2.5 Draw the Unlock Pattern

NOTE

- If you have forgotten your pattern, you can select the **Forgot My Pattern** or **Switch User** option to enter the normal login dialog box.
- When the pattern you draw is different from the pattern you have configured, you should try again.
- If you have drawn the wrong pattern for more than 5 times, the system will switch to the normal login mode automatically.

2.4.2 Log in via Password

Purpose:

If device has logged out, you must login the device before operating the menu and other functions.

Steps

1. Select the **User Name** in the dropdown list.
2. Input password
3. Click **OK** to log in.

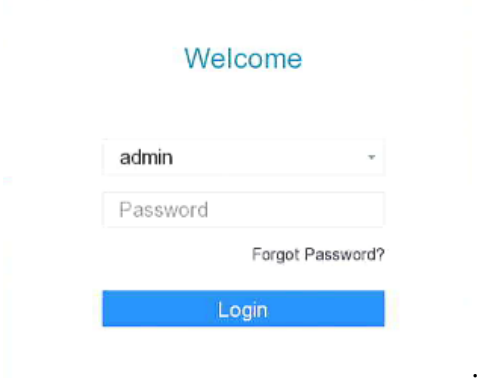


Figure 2.6 Login Interface

NOTE

- When you forget the password of the admin, you can click **Forgot Password** to reset the password.
- In the Login dialog box, if you enter the wrong password 7 times, the current user account will be locked for 60 seconds.

2.4.3 User Logout

Purpose:

After logging out, the monitor turns to the live view mode and if you want to perform some operations, you need to enter the user name and password to log in again.

Steps

1. Enter the **Power Off** menu.

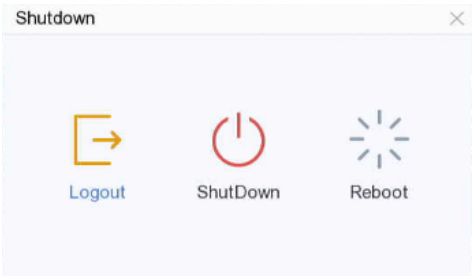


Figure 2.7 Logout

2. Click **Logout**.

NOTE

After you have logged out of the system, menu operation on the screen is invalid. It is required to input a user name and password to unlock the system.

2.5 Enter Wizard to Configure Quick Basic Settings

Purpose:

By default, the Setup Wizard starts once the device has loaded.

The Setup Wizard can walk you through some important settings of the device. If you don't want to use the Setup Wizard at that moment, click the **Exit** button.

Steps

1. Configure the date and time on the Date and Time Setup interface.

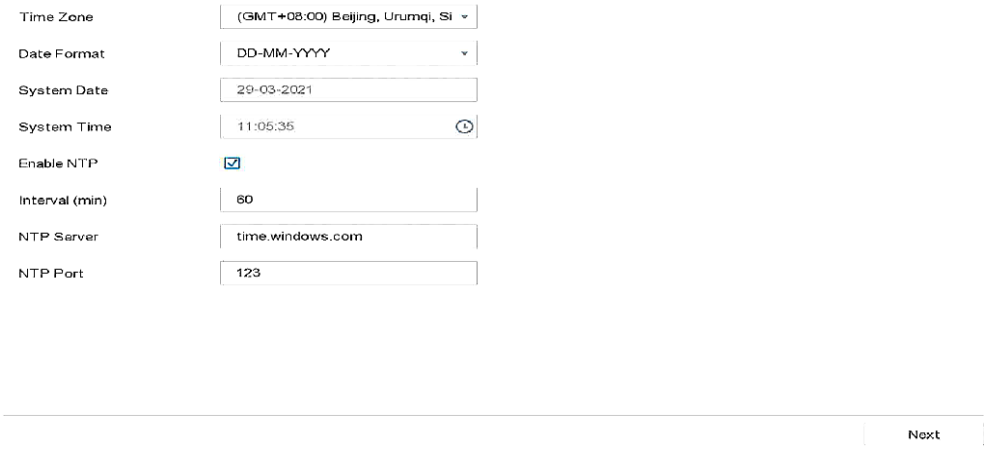


Figure 2.8 Date and Time Settings

2. After the time settings, click **Next** to enter the Network Setup Wizard window, as shown in the following figure.

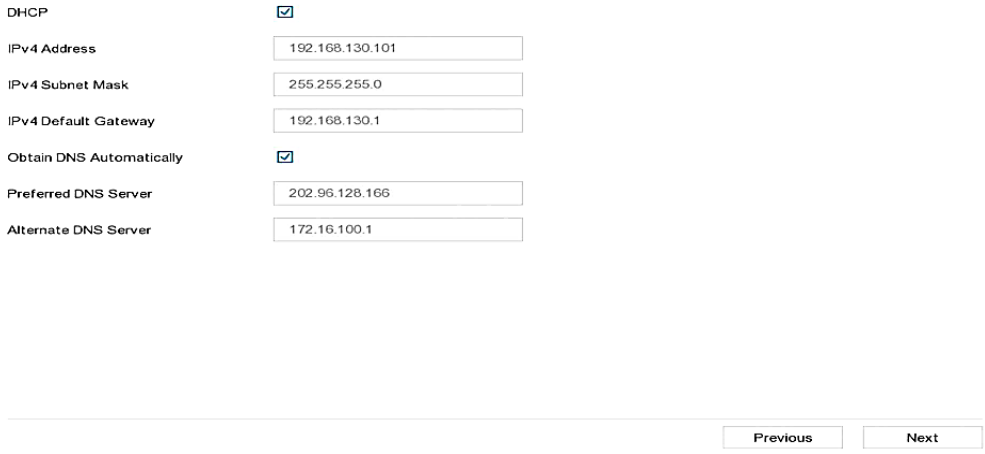


Figure 2.9 Network Settings

3. Enter the Platform Access and configure the Guarding Vision P2P-Connect settings.

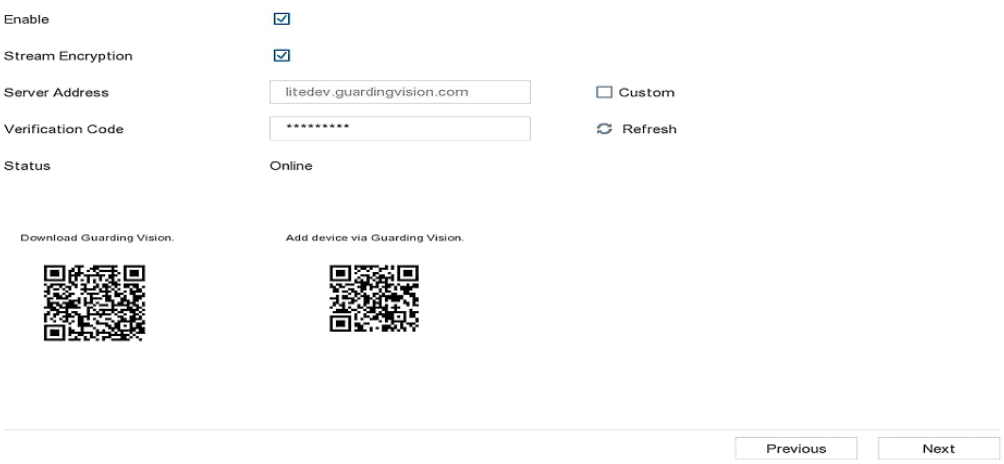


Figure 2.10 Guarding Vision P2P Connect Access

4. Click **Next**. You enter the **Add Camera** interface to add the IP cameras.

1) Click **Search** to search the online IP Camera. Before adding the camera, make sure the IP camera to be added is in active status.

2) Click the **Add** to add the camera.

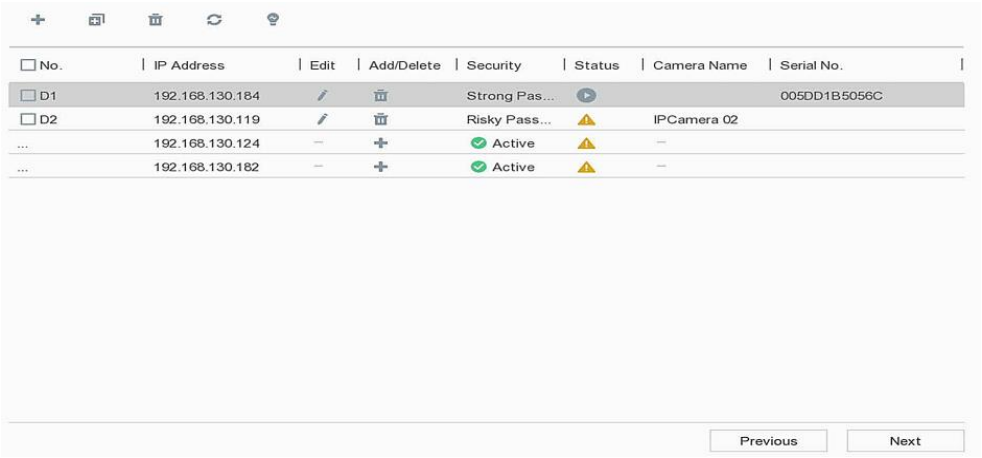


Figure 2.11 Add IP Cameras

NOTE

If the camera is in inactive status, you can select the camera from the list and click **Activate** to activate the cameras.

5. Click **Next** after you configured the network parameters, which takes you to the **HDD Management** window.

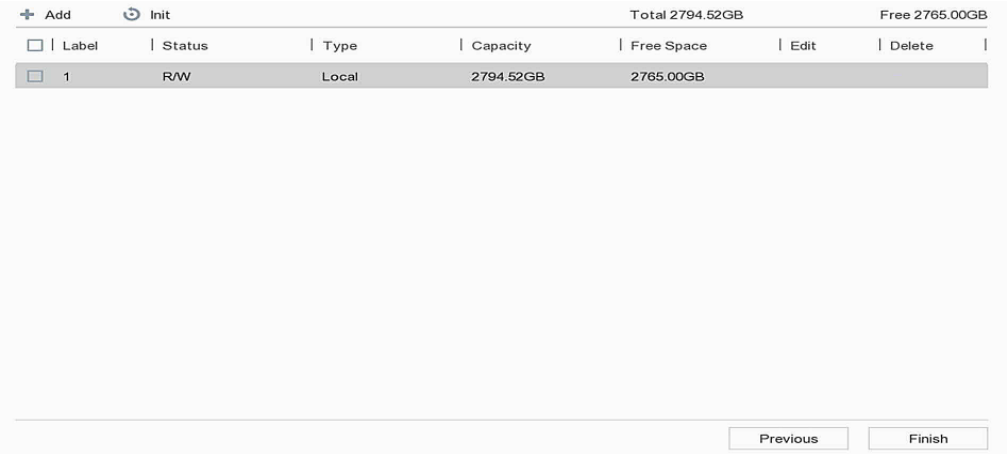


Figure 2.12 HDD Management

6. To initialize the HDD, click the **Init** button. Initialization removes all the data saved in the HDD.
7. Click **Finish** to complete the startup Setup Wizard.

2.6 Enter Main Menu

Purpose:

After you have completed the wizard, you can right click on the screen to enter the main menu bar. Refer to the following figure and table for the description of main menu and sub-menus.

Figure 2.13 Main Menu Bar

Description of Icons:

Icon	Description
	Live View
	Playback
	File Management
	System Management
	System Maintenance

2.7 System Operation

2.7.1 Log out

Purpose:

After logging out, the monitor turns to the live view mode and if you want to perform any

operations, you need to enter user name and password to log in again.

Steps

1. Click on the menu bar
2. Click Logout.

NOTE

After you have logged out the system, menu operation on the screen is invalid. It is required to input a user name and password to unlock the system.

2.7.2 Shut Down the Device

Steps

1. Click on the menu bar
2. Click the **Shutdown**.
3. Click the **Yes**

NOTE

Do not conduct power off operation again when the system is shutting down.

2.7.3 Reboot the Device

Purpose:

From the Shutdown menu, you can also reboot the device.

Steps

1. Click on the menu bar
2. Click **Reboot** to reboot the device.

3 Live View

3.1 Introduction of Live View

Live view shows you the video image getting from each camera in real time. Live view shows you the video image getting from each camera in real time. The DVR will automatically enter Live View mode when powered on. It is also at the very top of the menu hierarchy.

➢ Click  on the main menu bar to enter the live view.

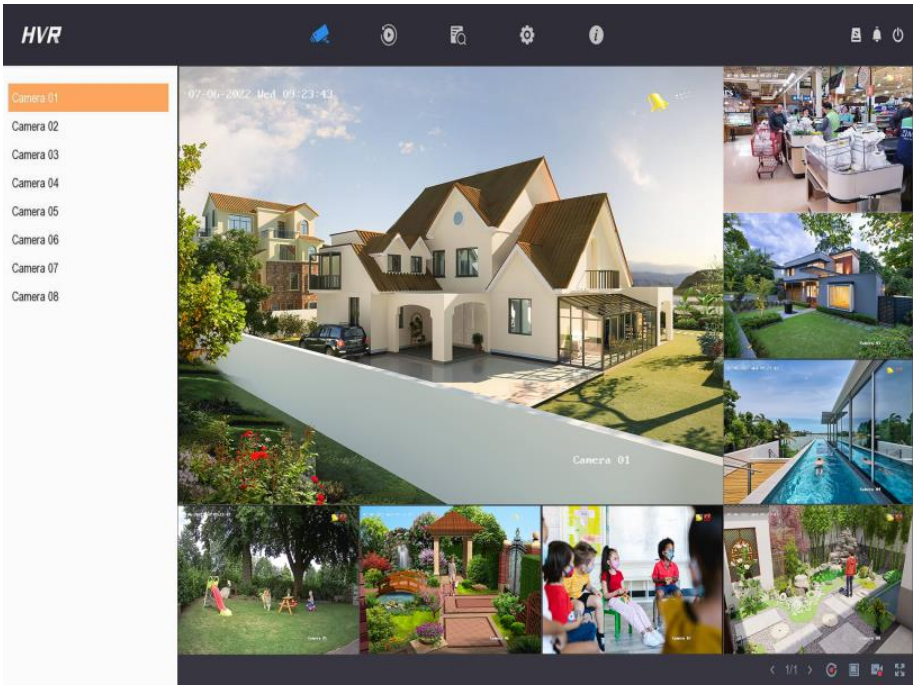
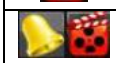


Figure 3.1 Live view windows

Live View Icons

In the live view mode, there are icons at the right top of the screen for each channel, showing the status of the record and alarm in the channel, so that you can know whether the channel is recorded, or whether there are alarms occur as soon as possible.

Description of Live View Icons:

Icons	Description
	Alarm (video loss, tampering, motion detection, VCA or sensor alarm
	Record (manual record, schedule record, motion detection or alarm triggered record)
	Alarm & Record.
	Event/Exception (motion detection, sensor alarm or exception information.

3.1.1 Quick Setting Toolbar in Live View Mode:

On the screen of each channel, there is a quick setting toolbar which shows when you click the screen.

Figure 3.2 Quick Setting Toolbar

Description of Quick Setting Toolbar Icons:

Icons	Description	Icons	Description
	Instant Playback		Mute/Audio on
	PTZ Control		Enable/Disable Manual Record
	Digital Zoom	A1	Channel information

3.2 Adjusting Live View Settings

Purpose:

Live View settings can be customized according to different needs. You can configure the output interface, dwell time for screen to be shown, mute or turning on the audio, the screen number for each channel, etc.

Device & System from Switch to Expert Mode/Easy Mode in the lower left corner of the menu and you can set the functions of the DVR.

Steps

1. Enter the **Configuration>System>Live Vie>General** Settingsinterface.

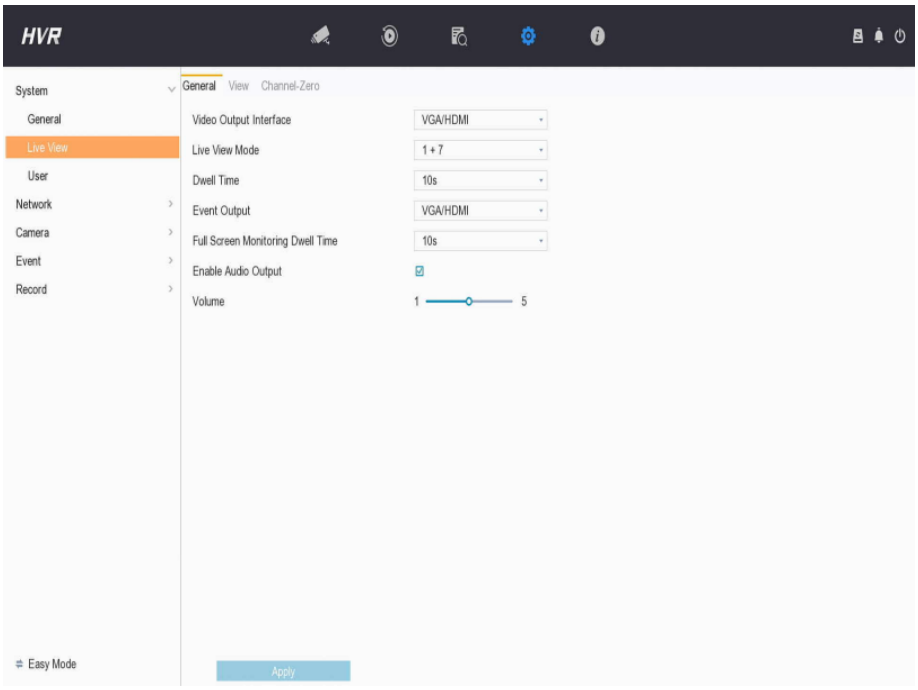


Figure 3.3 Live View-General

The settings available in this menu include:

Video Output Interface: Selects the output to configure the settings.

Live View Mode: Selects the display mode to be used for Live View.

Dwell Time: The time in seconds to *dwell* between switching of channels when enabling auto-switch in Live View.

Enable Audio Output: Enables/disables audio output for the selected camera in the live view mode.

Volume: Adjust the volume of the audio output.

Event Output: Designates the output to show event video. If available, you can select a different video output interface from the Video Output Interface when an event occurs

Full Screen Monitoring Dwell Time: The time in seconds to show alarm event screen.

2. Enter the **Configuration>System>Live View>View** Settings interface.

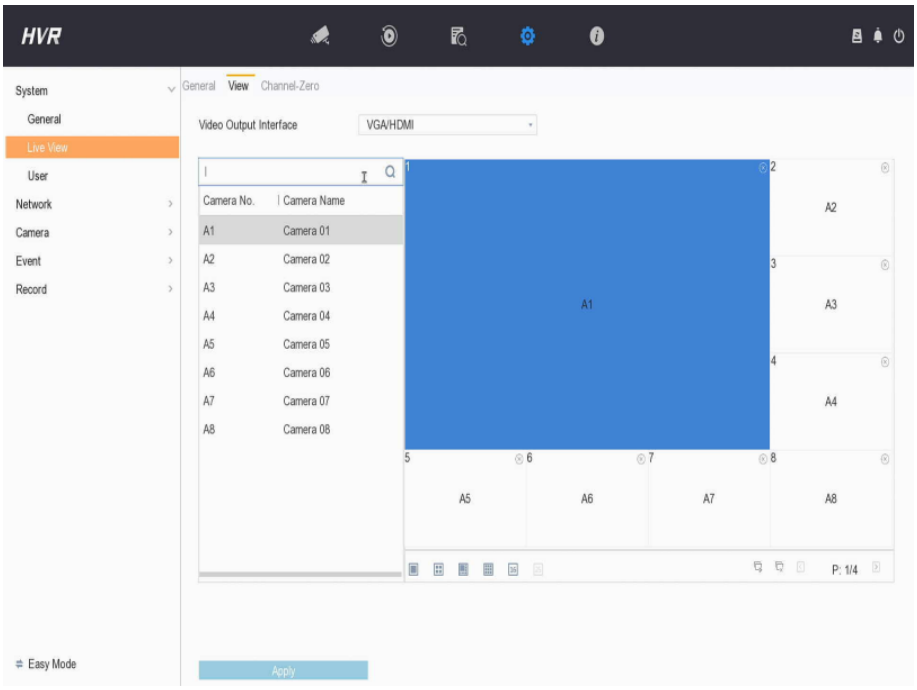


Figure 3.4 Live View-Camera Order

1) Click a window to select it, and then double-click a camera name in the camera list you would like to display. Setting an 'X' means the window will not display any camera.

2) You can also click  to start live view of all channels in order and click  to stop live view of all channels. Click or to go to the previous or next page.

3) Click the **Apply** button.

3. Enter the **Configuration>System>Live View> Channel-Zero** Settings interface.

1) Check the checkbox to enable the channel-zero.

2) Configure the **Frame Rate**, **Max. Bitrate Mode** and Max. Bitrate. The higher frame rate and bitrate settings result in the higher requirement of bandwidth.

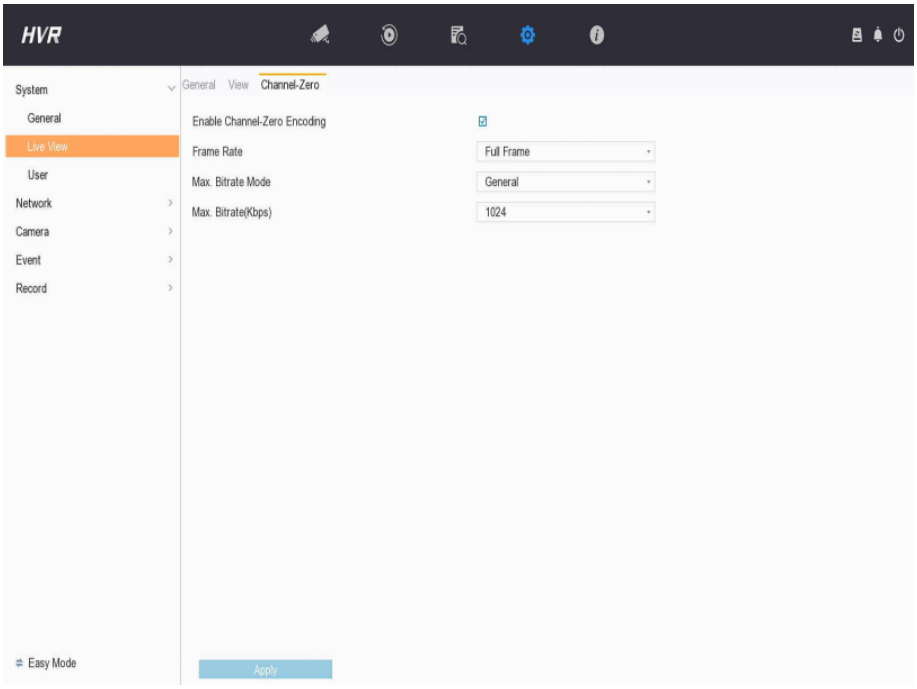


Figure 3.5 Live View- Channel-Zero

3) Click **Apply.**

3.3 Digital Zoom

Purpose:

Digital Zoom is for zooming in the live image. You can zoom in the image to different proportions (1 to 16X).

Steps

1. In the live view mode, click  from the toolbar to enter the digital zoom interface.
2. You can move the sliding bar or scroll the mouse wheel to zoom in/out the image to different proportions (1 to 16X).

Figure 3.5 Digital zoom

4 PTZ Control Wizard

4.1 Configuring PTZ Settings

Before you start

Follow the procedure to set the parameters for PTZ. You should configure the PTZ parameters before controlling the PTZ camera.

Steps

1. Click  on the quick settings toolbar in the live view interface.

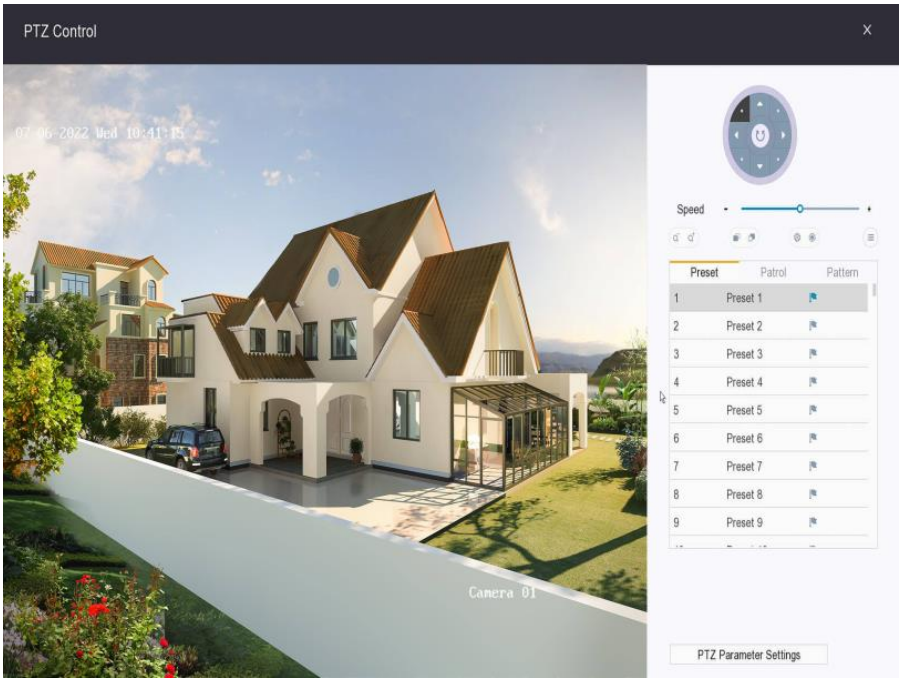


Figure 4.1 PTZ settings

2. Click the **PTZ Parameters Settings** button to set the PTZ parameters.

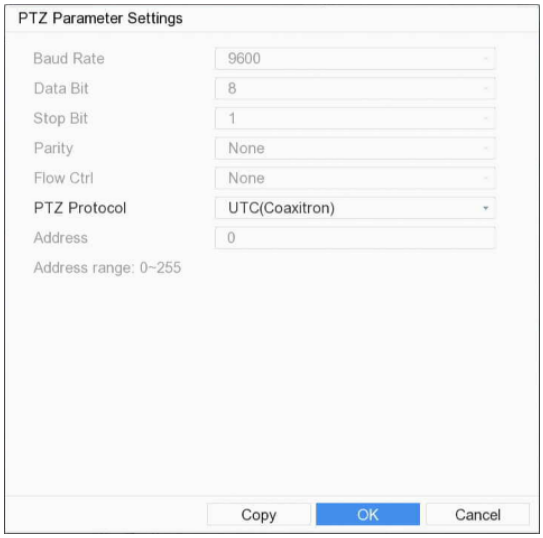


Figure 4.2 PTZ Parameters Settings

3. Edit the PTZ parameters.
4. (Optional) Click **Copy** button to copy the settings to the other channels. Select the channels you want to copy to and click **OK** to return to the **PTZ Parameters Settings** interface.

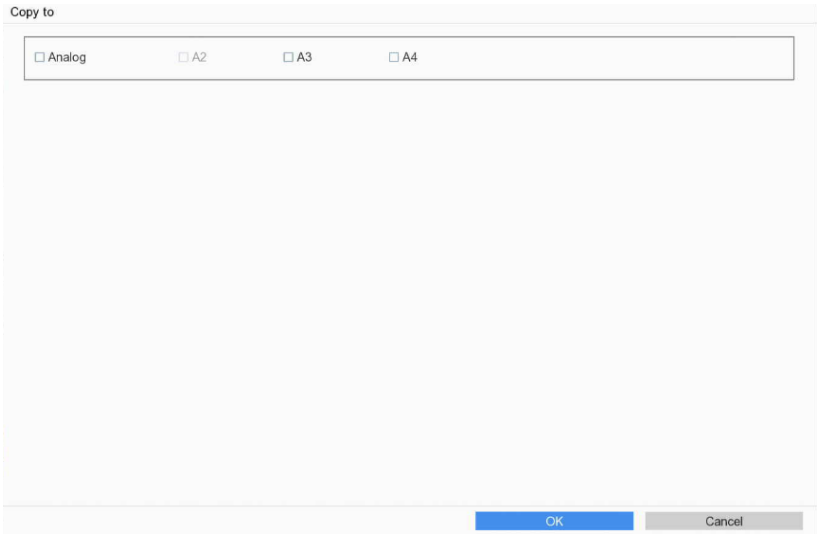


Figure 4.3 Copy to Other Channels

5. Click **OK** to save the settings.
6. (Optional) Check the checkbox of **Enable Omnicast Control** to enable the PTZ control of the selected camera.

4.2 Set a Preset

Before you start

Presets record the PTZ position and the status of zoom, focus, iris, etc. You can call a preset to quickly move the camera to the predefined position

Steps

1. Click  on the quick settings toolbar in the live view interface.

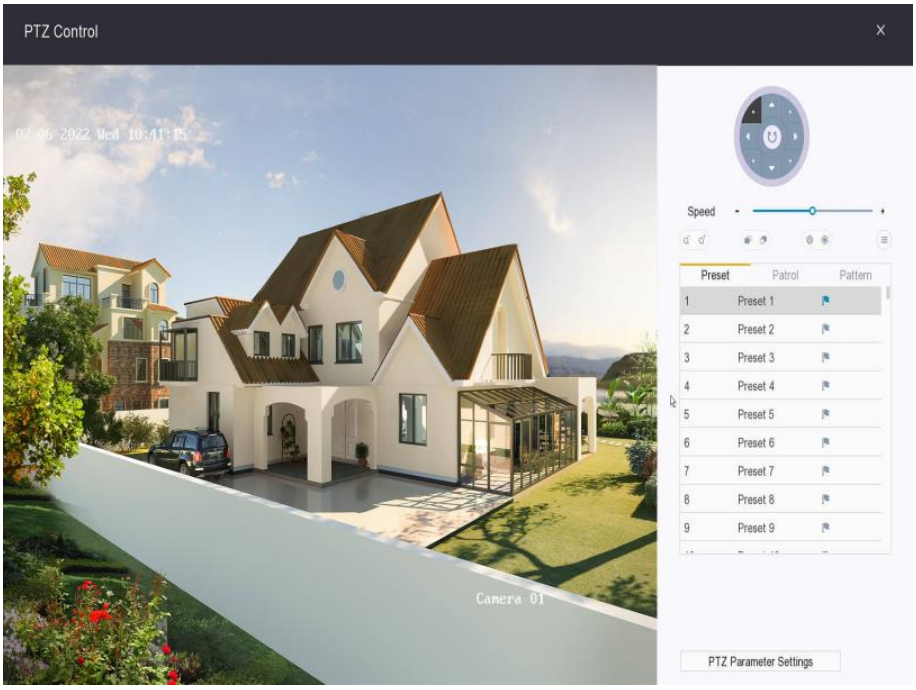


Figure 4.4 PTZ settings

2. Click directional buttons to wheel the camera to a location.
3. Adjust the zoom, focus and iris status.
4. Click in the lower right corner of Live View to set the preset

Figure 4.5 Set Preset

5. Select the preset No. (1 to 255) from the drop-down list.
6. Click the button save the preset.
7. Click the button to clear the location information of the preset.

4.3 Calling Presets

Purpose

This feature enables the camera to point to a specified position such as a window when an event takes place.

Steps

1. Click on the quick settings toolbar in the live view interface.
2. Click the **Call Preset** button to call it.

Figure 4.6 PTZ Panel-General

NOTE

When the Coaxitron camera/dome connected and the PTZ protocol is selected to UTC (Coaxitron), you can call the preset 95 to enter the menu of the connected Coaxitron camera/dome. Use the directional buttons on the PTZ control panel to operate the menu.

4.4 Set a Patrol

Purpose

Patrols can be set to move the PTZ to key points and have it stay there for a set duration before moving on to the next key point. The key points are correspond to the presets.

Steps

1. Click on the quick settings toolbar in the live view interface.
2. Click **Patrol** to configure patrol.

Figure 4.7 Patrol Configuration

3. Select the patrol No.
4. Click **Set**.

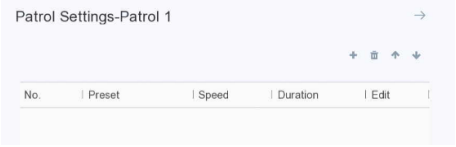


Figure 4.8 Patrol Settings

5. Click + to add a key point to the patrol.

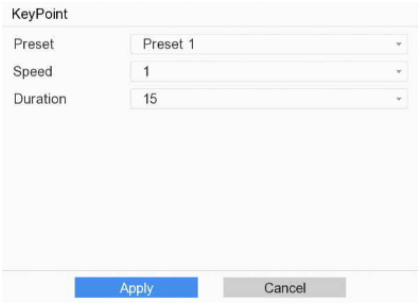


Figure 4.9 Key Point Configuration

1) Configure key point parameters.

Preset

Determines the order the PTZ will follow while cycling through the patrol.

Speed

Defines the speed the PTZ will move from one key point to the next.

Duration

Refers to the duration to stay at the corresponding key point.

2) Click **Apply** to save the key points to the patrol.

6. Other Operation is as follows.

Operation	Description	Operation	Description
	Select a key point to delete		Adjust the key point order
	Adjust the key point order		Edit the added key point

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

4.5 Call a Patrol

Calling a patrol makes the PTZ move according to the predefined patrol path.

Steps

1. Click  on the quick settings toolbar in the live view interface.
2. Click **Patrol** on the PTZ control panel.

Figure4.10 Patrol Configuration

3. Select a patrol.
4. Click **Call** to start the patrol.
5. **Optional:** Click **Stop Call** to stop the patrol.

4.6 Set a Pattern

Patterns can be set by recording the movement of the PTZ. You can call the pattern to make the PTZ move according to the predefined path.

Steps

1. Click on the quick settings toolbar in the live view interface.
2. Click **Pattern** to configure a pattern.

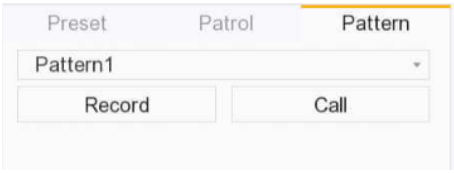


Figure 3.13 Pattern Configuration

3. Select the pattern No.
4. Set the pattern.

1) Click **Record** to start recording.

2) Click corresponding buttons on the control panel to move the PTZ camera.

3) Click **Stop** to stop recording. The PTZ movement is recorded as the pattern.

4.7 Call a Pattern

Purpose:

Follow the procedure to move the PTZ camera according to the predefined patterns.

Steps

1. Click on the quick settings toolbar in the live view interface.
2. Click **Pattern** to configure pattern.

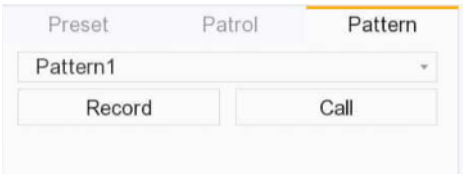


Figure 4.11 Pattern Configuration

3. Select a pattern in the text field.
4. Click **Call** to call it.
5. (Optional) Click **Stop Call** to stop calling it.

5 Playback

Purpose:

The recorded video files and pictures on the hard disk can be played back in the following modes: instant playback, all-day playback for the specified channel, and playback by normal/event/smart/tag/system logs/sub-periods/external file search/picture.

5.1 Instant Playback

Purpose:

Instant Playback enables the device to play the recorded video files in last five minutes. If no video is found, it means there is no recording during the last five minutes.

Steps

1. On the live view window of the selected camera, move the cursor to the window bottom to access the toolbar.
2. Click to start instant playback.

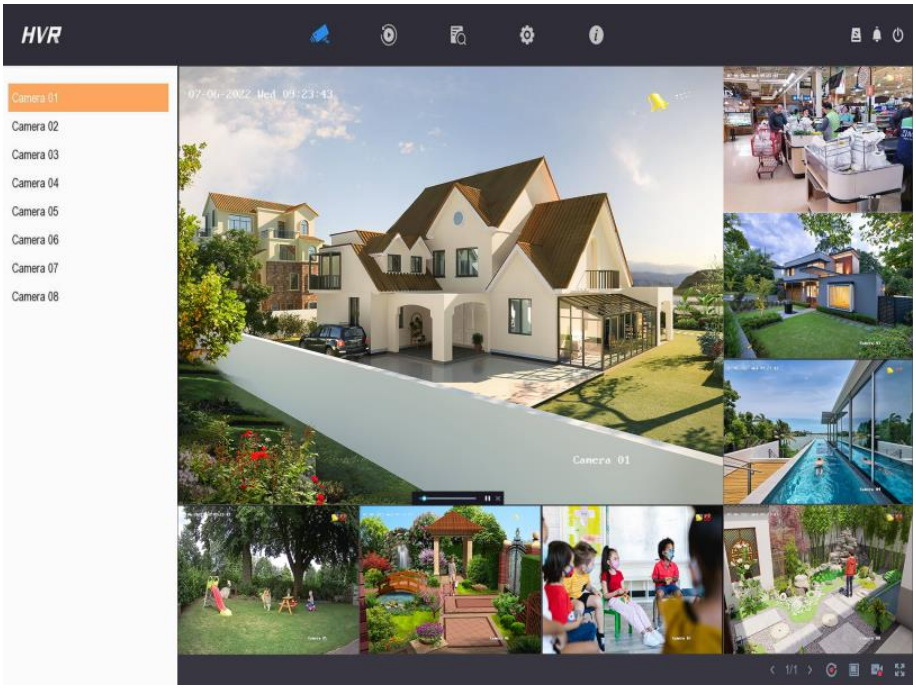


Figure 5.1 Playback Interface

5.2 Play Normal Video

5.2.1 Playback Normal Video

Purpose:

In the normal playback mode, you can achieve the advanced playback operations which will satisfy more complicated requirements

Steps

1. Click to start instant File Management

2. Select one or more cameras in the **Channel** list to start playing the video.
3. Select a date in the calendar.

- Use the toolbar in the bottom part of playback interface to control the playing and realize a series of operations. Refer to Chapter5.6 Playback Operations.
- Click the channel(s) to execute simultaneous playback of multiple channels.

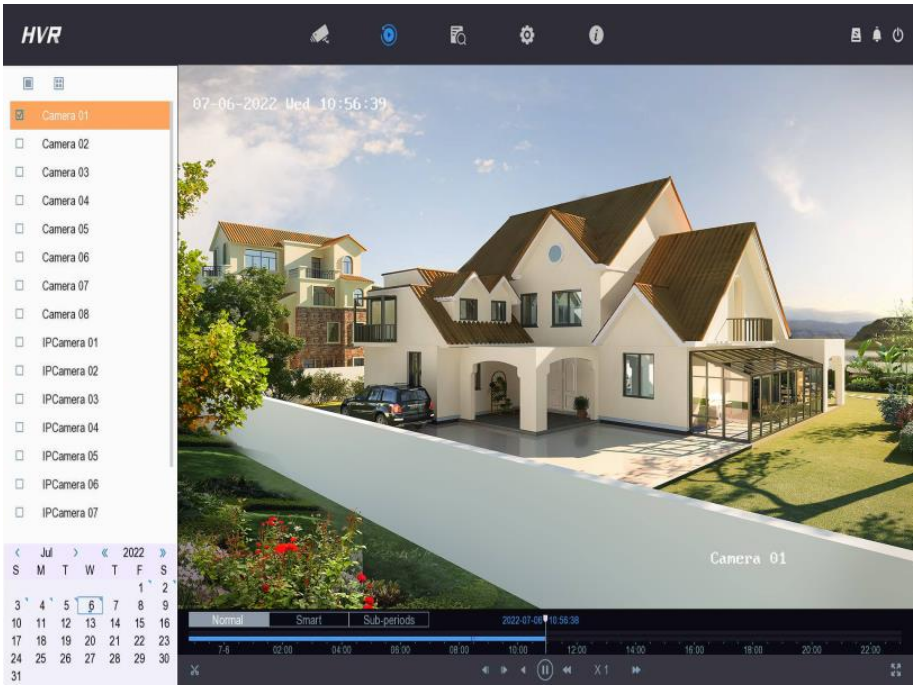


Figure 5.2 Playback Interface

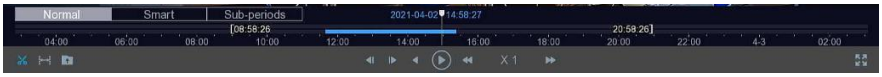


Figure 5.3 Toolbar of Playback

5.2.2 Backing up Video Clips

Purpose:

You may also select video clips in playback mode to export directly during Playback, using USB devices (USB flash drives, USB HDDs, USB writer), or SATA writer.

Steps

1. Go to Playback
2. During playback, use buttons and in the playback toolbar to Set the start time and end time.

Figure 5.4 clip time search

3. Click to save the video clip to a storage device.
4. Click the button to enter the **Export Clip** interface.

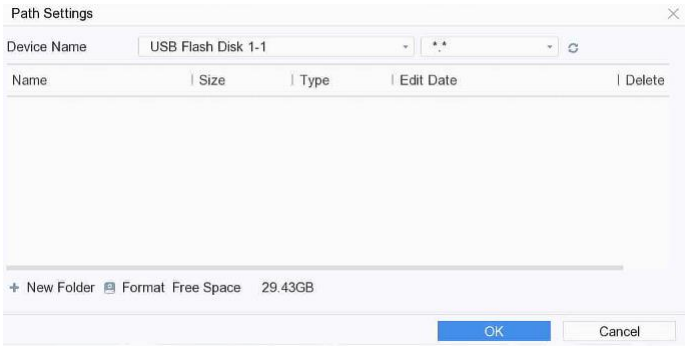


Figure 5.5 Backup Path settings

5. Select the file to export as **Video and Log** and click **OK**.

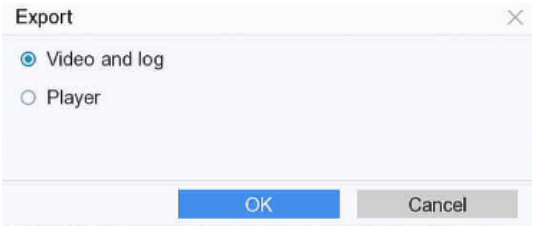


Figure 5.6 select file type

You can click to view export progress.

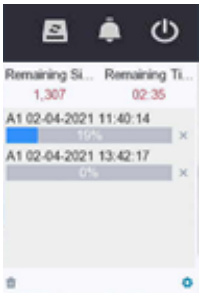


Figure 5.7 File backup progress

5.3 Play Smart Searched Video

Purpose:

In the smart playback mode, the device can analyze the video containing the motion, line or intrusion detection information, mark it in red color and play the smart searched video.

Steps

1. Go to Playback.
2. Start playing the video of camera.
3. Click **Smart**.
4. From the toolbar at the bottom of the playing window, click the motion/line crossing/intrusion icon for search.

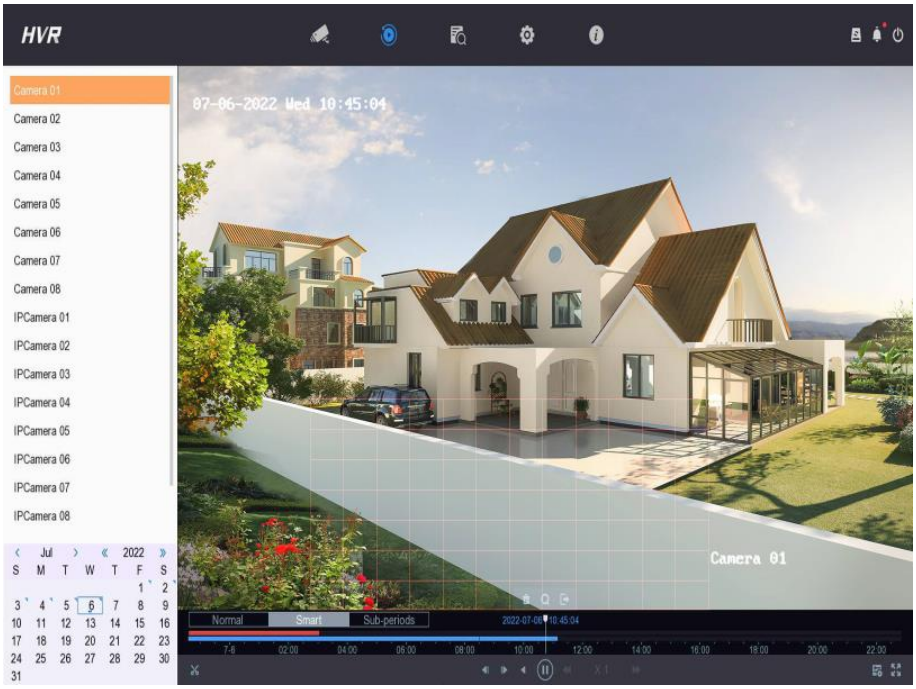


Figure 5.8 Playback by Smart Search

5. Set the rules and areas for smart search of line crossing detection, intrusion detection or motion detection event triggered recording.

1. Line Crossing Detection

❶ Click the icon.

❷ Click on the image to specify the start point and end point of the line.

2. Intrusion Detection

❶ Click the icon.

❷ Specify 4 points to set a quadrilateral region for intrusion detection. Only one region can be set.

3. Motion Detection

❶ Click the icon

❷ Hold the mouse on the image to draw the detection area manually.

❸ Click Search to search the matched video and start to play it.

Backing up Video Clips Refer to Chapter Backing up Video Clips

5.4 Play by Sub-periods

Purpose:

The video files can be played in multiple sub-periods simultaneously on the screens.

Steps

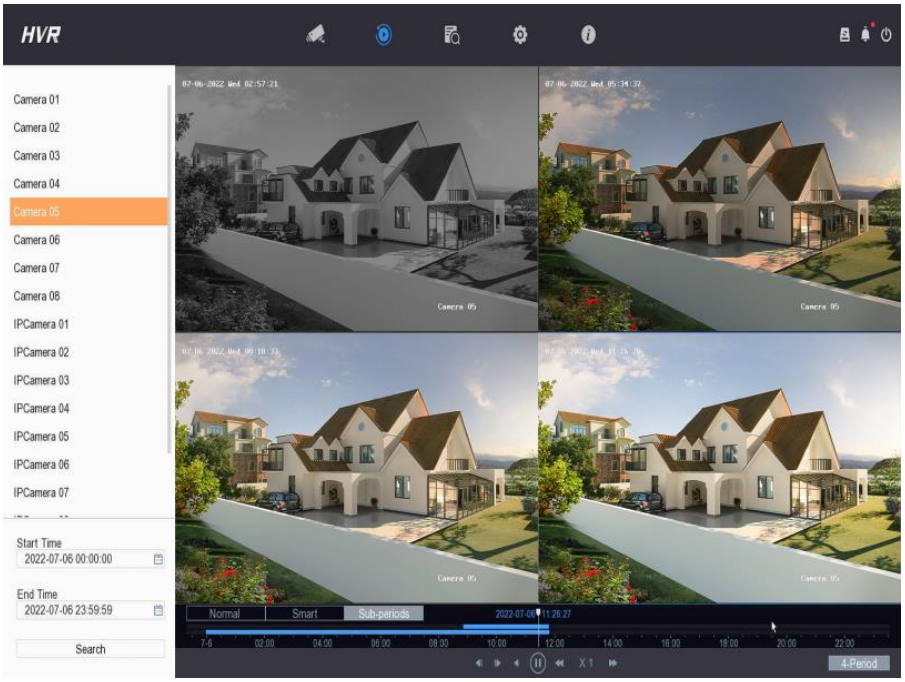


Figure 5.9 Playback by sub-periods Search

1. Go to Playback.
2. Select Sub-periods icon at the left bottom corner to enter the sub-period playing mode.
3. Select a camera.
4. Set the start time and end time for searching video.
5. Select the different multi-period at the right bottom corner, e.g., 4-Period.

NOTE

According to the defined number of split-screens, the video files on the selected date can be divided into average segments for playback. E.g., if there are video files existing between 16:00 and 22:00, and the 6-screen display mode is selected, then it can play the video files for 1 hour on each screen simultaneously.

5.5 Play Log Files

Purpose:

Play back record file(s) associated with channels after searching system logs.

Steps

1. Go to Maintenance>More>Log Information.
2. Click **Log Search** tab to enter Playback by System Logs.
3. Set search time and type and click **Search**.
4. Choose a log with video file and click to start playing the log file.

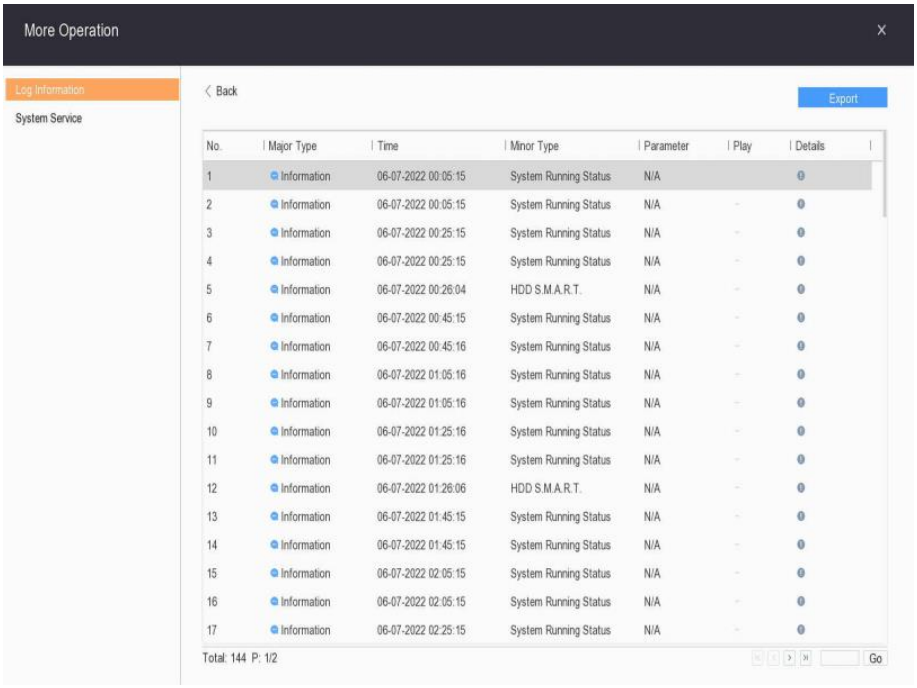


Figure 5.10 System Log Search Interface

5.6 Playback Operations

5.6.1 Set Play Strategy in Smart/Custom Mode

Purpose:

When you are in the smart or custom video playback mode, you can set the playing speed separately for the normal video and the smart/custom video, or you can select to skip the normal video.

In the Smart/Custom video playback mode , Click  to set the play strategy.

- When **Do not Play Normal Videos** is checked, the device will skip the normal video and play the smart (motion/line crossing/intrusion) video and the custom (searched video) only in the normal speed (X1).
- When **Do not Play Normal Videos** is unchecked, you can set the play speed for the normal video the smart/custom video separately. The speed range is from X1 to XMAX.

NOTE

You can set the speed in the single-channel play mode only.

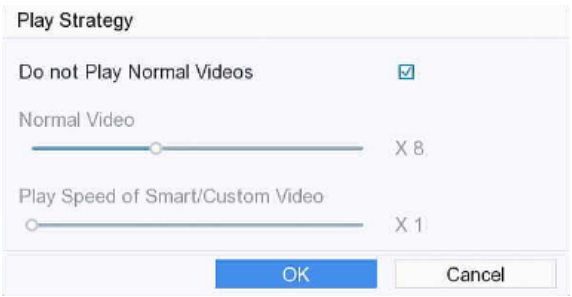


Figure 5.11 Play Strategy

5.6.2 Fast View

You can hold the mouse to drag on the time bar to get the fast view of the video files.

In the video playback mode, use the mouse to hold and drag through the playing time bar to fast view the video files.

Release the mouse to the required time point to enter the full-screen playback.

5.6.3 Digital Zoom

In the video playback mode, click from the toolbar to enter the digital zoom interface.

You can move the sliding bar or scroll the mouse wheel to zoom in/out the image to different proportions (1 to16X).

Figure 5.12 Digital Zoom

6 File Management

Click to start instant File Management

6.1 Search and Export All Files

6.1.1 Search Files

Purpose:

Specify detailed conditions to search videos and pictures

Steps

1. Go to File Management > All Files.
2. Specify detailed conditions, including time, camera, event type, etc.
3. Click **Search** to display results. The matched files will be displayed.

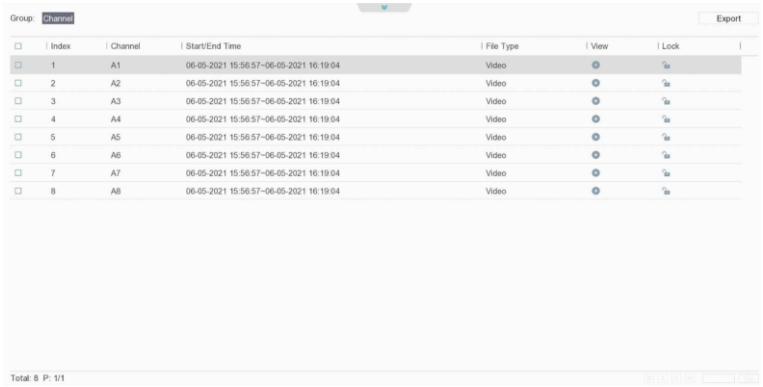


Figure 6.1 Search All Files

6.1.2 Export Files

Purpose

Export files for backup purposes using USB device (USB flash drive, USB HDD, USB optical disc drive), SATA optical disc drive or eSATA HDD.

Steps

1. Search files to export. For details, see *6.1.1 Search Files.*
2. Click **Export** to export the selected file(s) to a backup device. You can click select all files.

Figure 6.2 Search backup Files

3. Click **OK** to export files to backup device.

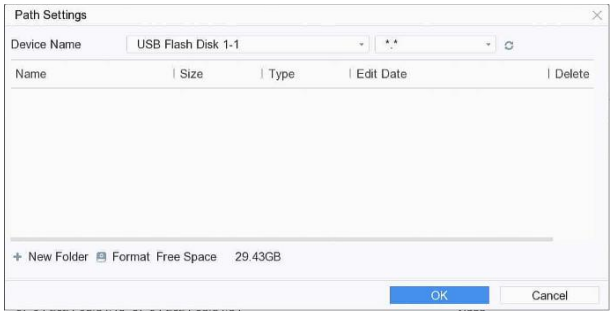


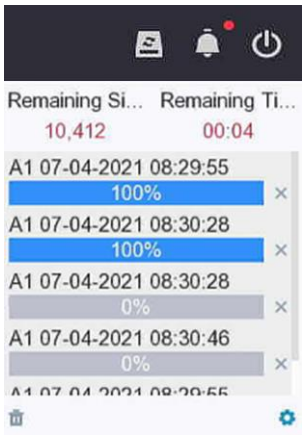
Figure 6.3 Backup Path settings

4. Select the file to export as **Video and Log** and click **OK**.

Figure 6.4 Select Export file type

NOTE

You can click to view export progress.



You can click  to return to search interface.

7 System Configuration

You are able to configure the DVR for Channel, Record, Alarm, Network, Device & System from Switch to Expert Mode/Easy Mode in the lower left corner of the menu and you can set the functions of the DVR.

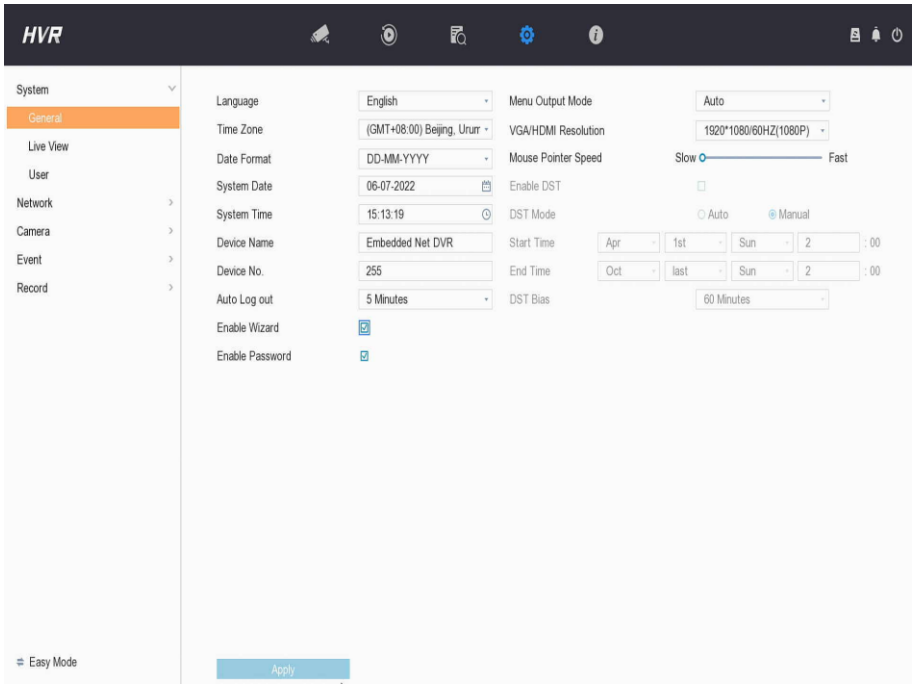


Figure 7.1 configuration Manu

7.1 System General Settings

Purpose:

You can configure the BNC output standard, VGA output resolution, mouse pointer speed through the System > General interface.

7.1.1 General Settings

Steps

1. Go to **Menu>Configuration>System > General.**

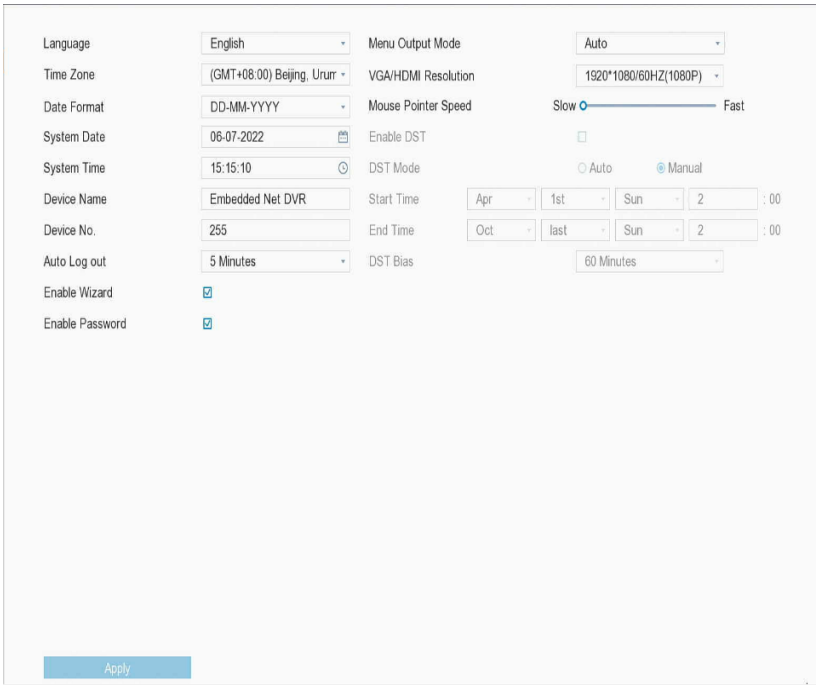


Figure 7.2 General Settings Interface

2. Configure the following settings.

Menu Output Mode: Configure the resolution of the video output.

Device Name: Edit the name of the device

Device No.: Edit the serial number of the device. The Device No. can be set in the range of 1~255, and the default No. is 255. The number is used for the remote and keyboard control.

Auto Logout: Set timeout time for menu inactivity. E.g., when the timeout time is set to *5 Minutes*, then the system will exit from the current operation menu to live view screen after 5 minutes of menu inactivity.

Enable Wizard: Enable/disable the Wizard when the device starts up.

Enable Password: Enable/disable the use of the login password.

Time Zone: Select the time zone.

Date Format: Select the date format.

System Date: Select the system date.

System Time: Set the system time.

Enable DST:

3. Select the DST mode to **Auto** or **Manual**.

Auto: Automatically enable the default DST period according to the local DST rules.

Manual: Manually set the start time and end time of the DST period, and the DST bias.

DST Bias: Set the time (30/60/90/120 minutes) offset from the standard time.

Example: The DST begins at 2:00 a.m. on the second Sunday of March and ends at 2:00 a.m. on the first Sunday of November, with 60 minutes ahead.

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

7.1.2 Manage User Accounts

Purpose:

The *Administrator* user name is *admin* and the password is set when you start the device for the first time. The *Administrator* has the permission to add and delete user and configure user parameters.

7.1.2.1 *Add a User*

Steps

1. Go to **Menu>Configuration>System > User**

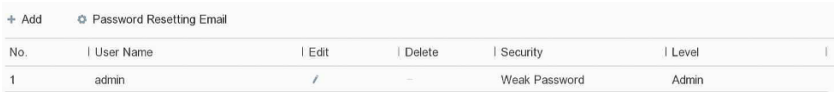


Figure 7.3 User Management Interface

2. Click **Add** to enter the operation permission interface.
3. Enter the admin password and click **Next**.

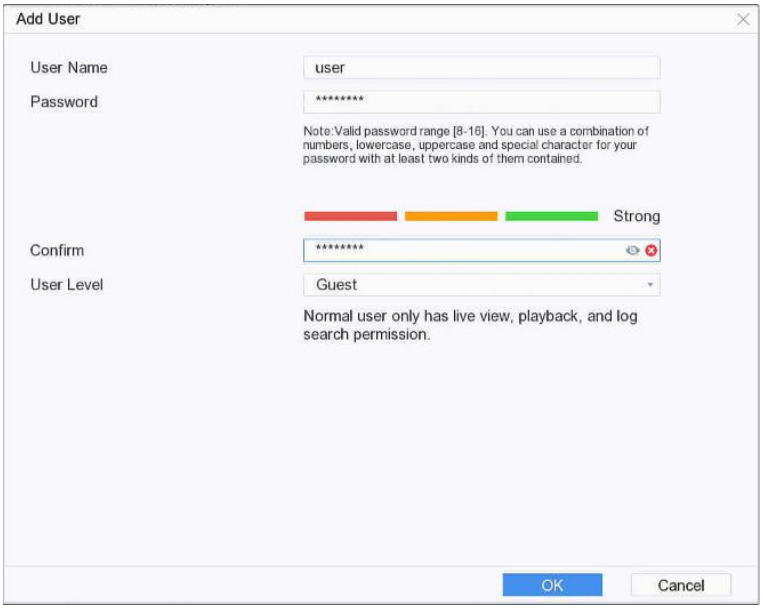


Figure 7.4 Add User

4. In the Add User interface, enter the information for new user, including **User Name**, **Password**, **Confirm** (password), **User Level** (Operator/Guest).

WARNING

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

- **User Level:** Set the user level to Operator or Guest. Different user levels have different operating permission.

Guest: The Guest user has no permission of Two-way Audio in Remote Configuration and Normal user only has live view, playback, and log search permission.

5. Click **OK** to finish the new user account adding.

Result: In the User Management interface, the added new user is displayed on the list.

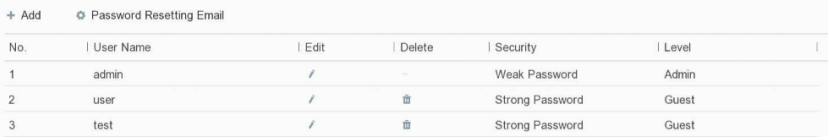


Figure 7.5 User Permission Settings Interface

7.1.2.2 *Edit the Admin User*

Purpose:

For the admin user account, you can modify your password and unlock pattern.

Steps

1. Go to **Menu>Configuration>System > User**.
2. Select the admin user from the list.
3. Click the icon to enter the **Edit User** interface, as shown below.

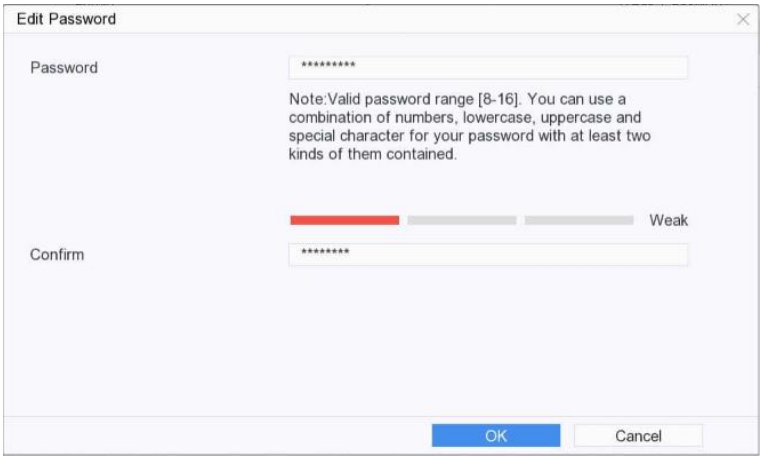


Figure7.6 Edit Admin User

4. Edit the admin user information as demand, including the new admin password (strong

password is required).

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

7.1.2.3 *Deleting a User*

Steps

1. Go to **Menu>Configuration>System > User**.
2. Select the user to be deleted from the list, as shown below.

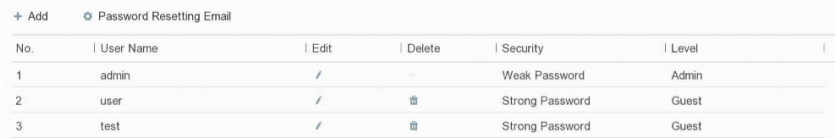


Figure 7.7 User List

3. Click to delete the selected user account.

7.1.2.4 *Set Password Resetting Email*

Steps

1. Go to Menu>Configuration>System > User.
2. Select the admin user from the list.
3. Click the icon to enter the **Password Resetting Email** interface, as shown below.

Figure 7.8 set password resetting email

4. Click **OK**.

7.1.3 Configure Live View Settings

7.1.3.1 *Live View General Settings*

Purpose:

Live View settings can be customized according to different needs. You can configure the output interface, dwell time for screen to be shown, mute or turning on the audio, the screen number for each channel, etc.

Steps

1. Go to **Menu>Configuration>System > Live View>General**.

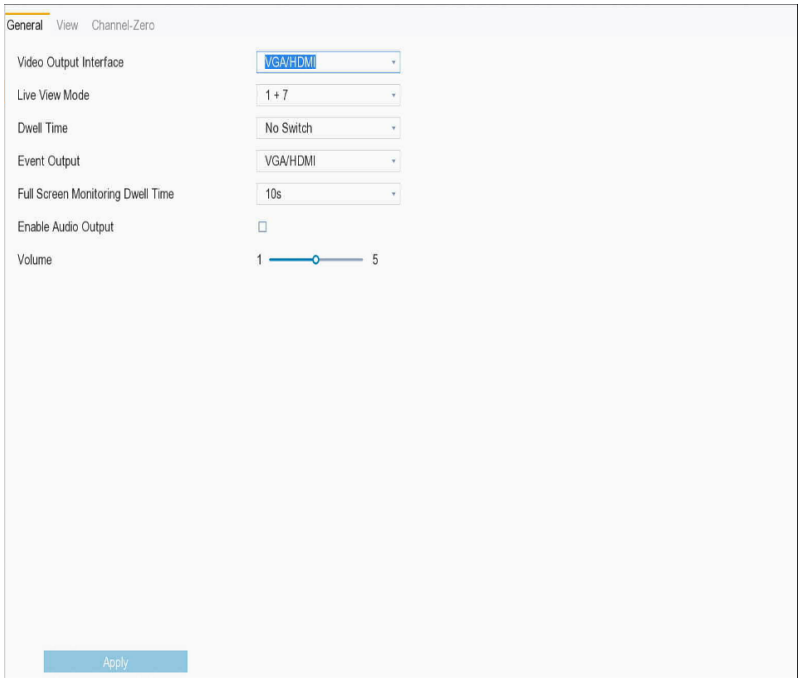


Figure 7.9 Live View-General

2. Configure the live view parameters.

- **Video Output Interface**: Select the video output to configure.
- **Live View Mode**: Select the display mode for live view, e.g., 2*2, 1*7, etc.
- **Dwell Time**: The time in seconds to dwell between switching of cameras when enabling auto-switch in Live View.
- **Enable Audio Output**: Enable/disable audio output for the selected video output.
- **Volume**: Adjust the volume of live view, playback and two-way audio for the selected output interface.
- **Event Output**: Select the output to show event video.
- **Full Screen Monitoring Dwell Time**: Set the time in seconds to show alarm event screen.

3. Click **Apply** to save the setting

7.1.3.2 *Configure Live View Layout*

Steps

1. Go to **Menu>Configuration>System > Live View>View.**
2. Select the video output interface, e.g., HDMI/ VGA or channel-zero.
3. Select a window division mode from the toolbar.
4. Select a division window, and double-click on the camera from the list to set the camera to the window.

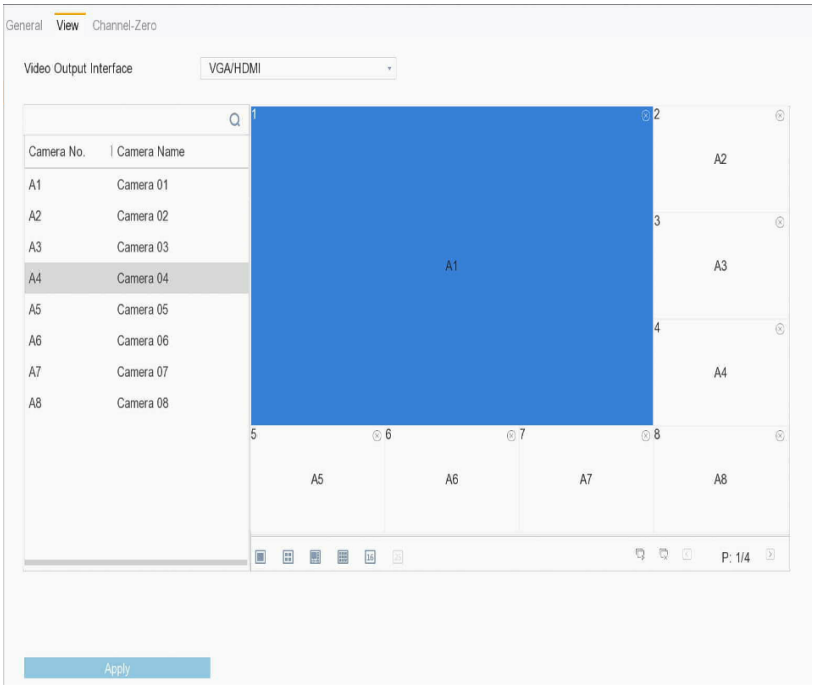


Figure 7.10 Live View

You can enter the number in the text field to quickly search the camera from the list.

You can also click-and-drag the camera to the desired window on the live view interface to set the camera order

Related Operation:

- Click button to start live view for all the channels.
- Click to stop all the live view.

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

7.1.3.3 *Configure Live View channel-Zero*

Purpose:

You can enable the channel-zero encoding when 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.

1. Enter the **Configuration>System>Live View> Channel-Zero** Settingsinterface.
2. Check the checkbox to enable the channel-zero.
3. Configure the **Frame Rate**, **Max. Bitrate Mode** and Max. Bitrate. The higher frame rate and bitrate settings result in the higher requirement of bandwidth.
4. Click **Apply.**

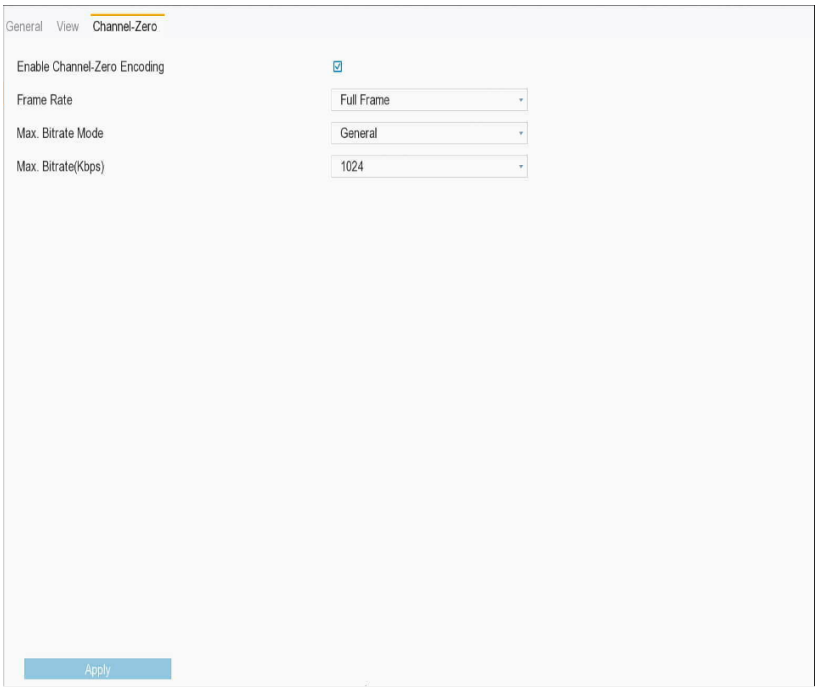


Figure 7.11 Live View Channel-Zero

7.2 Network Settings

7.2.1 Network General Setting

7.2.1.1 *Configure TCP/IP Settings*

Steps

Go to **Menu>Configuration> > Network >General> TCP/IP**

1. Select Net-Fault Tolerance or Multi-Address Mode under Working Mode.

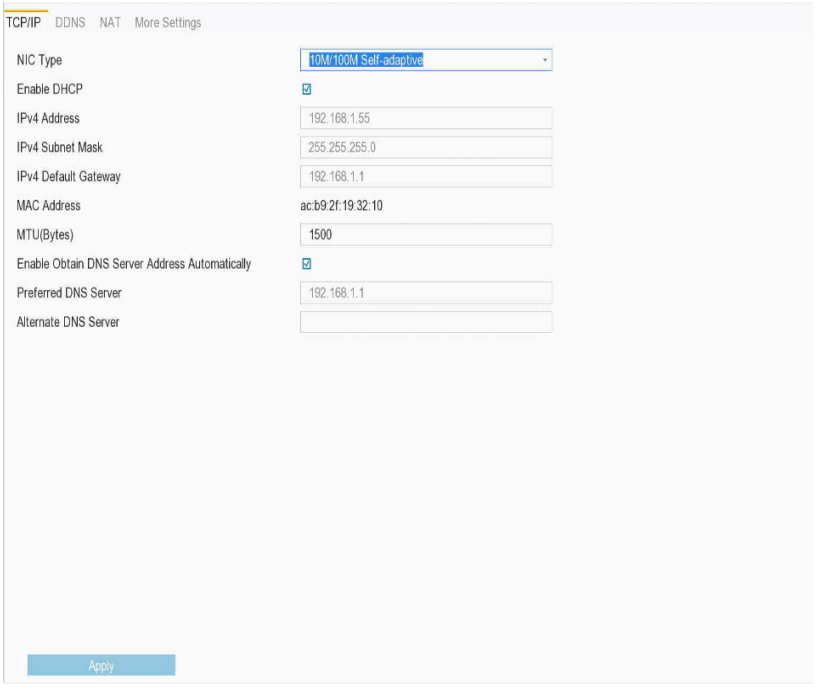


Figure 7.12 TCP/IP Setting

On the **General Settings** interface, you can configure the following parameters: NIC Type, IPv4 Address, IPv4 Gateway, TU, DNS Server and Main NIC.

2. Configure other IP settings as needed
3. Check **Enable DHCP** to obtain IP settings automatically if a DHCP server is available in the network.
4. Click **Apply**.

7.2.1.2 *Configure DDNS*

Purpose

You can set Dynamic DNS service for network access. Different DDNS modes are available: **DynDNS**, **PeanutHull,** and **NO-IP**.

Before You Start

You must register DynDNS, PeanutHull and NO-IP services with your ISP before configuring DDNS settings.

Steps

1. Go to **Menu>Configuration> > Network >General> > DDNS.**
2. Check **Enable**.
3. Select DynDNS under DDNS Type.
4. Enter **Server Address** for **DynDNS** (i.e. members.dyndns.org).
5. Under **Device Domain Name**, enter the domain name obtained from the DynDNS website.
6. Enter the **User Name** and **Password** registered in the DynDNS website.
7. Click **Apply**.

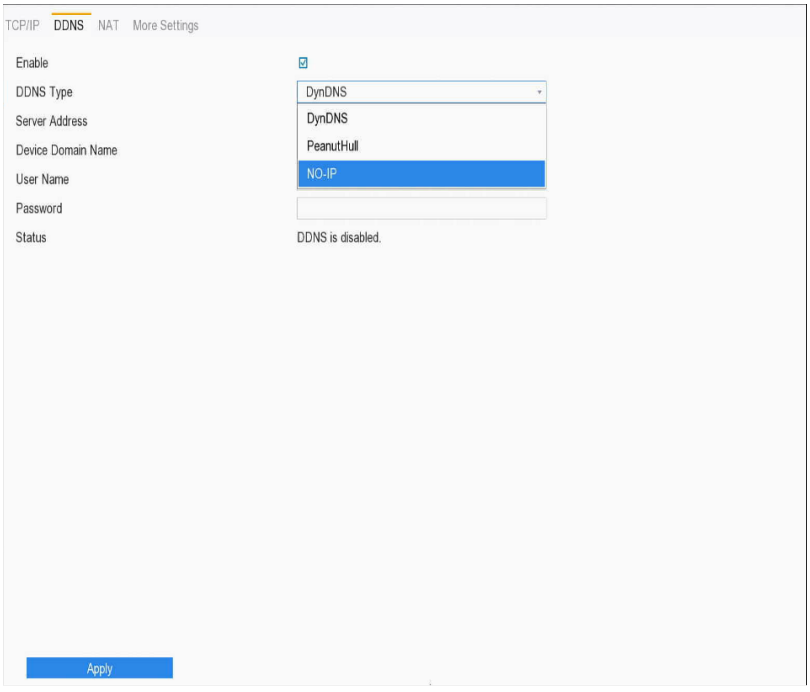


Figure 7.13 DDNS Settings

7.2.1.3 *Configure NAT*

Purpose:

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

Steps

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

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

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

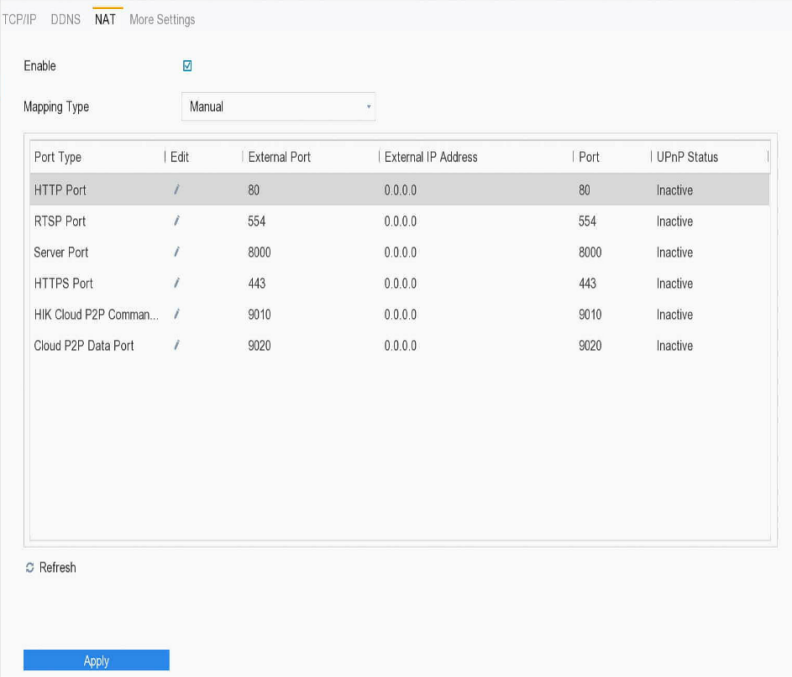


Figure 7.14 NAT Settings

4. 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.

Cloud P2P Command Port: The default port number is 9010.

Cloud P2P Data Port: The default port number is 9020.

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

7.2.1.4 *Configure Ports*

You can configure different types of ports to enable relevant functions.

Go to **Menu>Configuration> > Network >General> > More Settings** and configure port settings as needed.

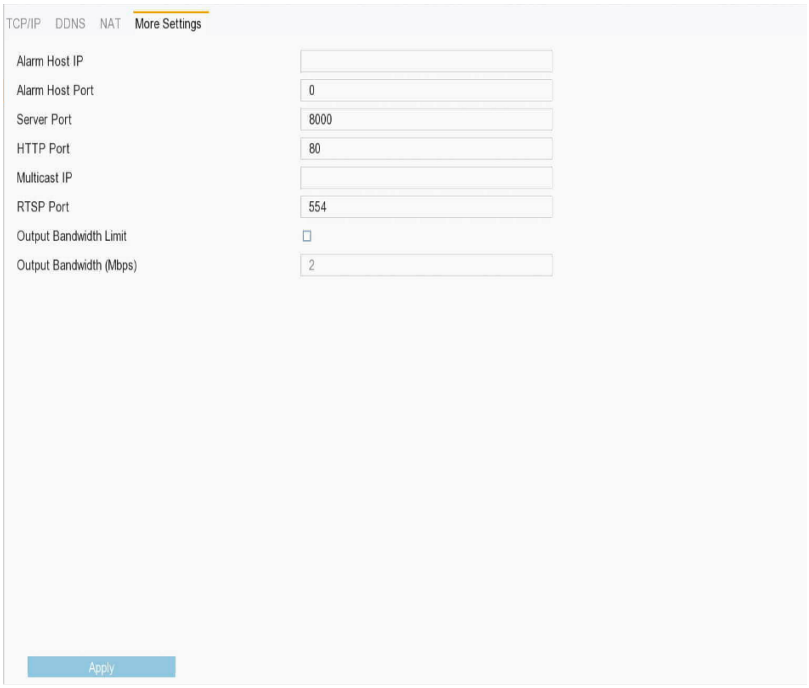


Figure 7.15 Port Settings

Alarm Host IP/Port: 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 client management system (CMS) software installed.

The **Alarm Host IP** refers to the IP address of the remote PC on which the CMS software is installed, and the **Alarm Host Port** (7200 by default) must be the same as the alarm monitoring port configured in the software.

Server Port: Server port (8000 by default) should be configured for remote client software access and its valid range is 2000 to 65535.

HTTP Port: HTTP port (80 by default) should be configured for remote web browser access.

Multicast IP: Multicast can be configured to enable live view for cameras that exceed the maximum number allowed through network. A multicast IP address covers Class-D IP ranging from 224.0.0.0 to 239.255.255.255 and it is recommended to use the IP address ranging from 239.252.0.0 to 239.255.255.255.

When adding a device to the CMS software, the multicast address must be the same as that of the device.

RTSP Port: RTSP (Real Time Streaming Protocol) is a network control protocol designed for use in entertainment and communications systems to control streaming media servers. The port is 554 by default.

Output Bandwidth Limit: You can check the checkbox to enable output bandwidth limit.

Output Bandwidth: After enable the output bandwidth limit, input the output bandwidth.

The output bandwidth limit is used for the remote live view and playback.

The default output bandwidth is the maximum limit.

7.2.2 Configure Platform

Purpose

Guarding Vision Connect provides mobile phone application and platform service to access and manage your connected devices, which enables you to get a convenient remote access to the surveillance

Steps

1. Go to **Menu>Configuration> > Network > Platform Access**.

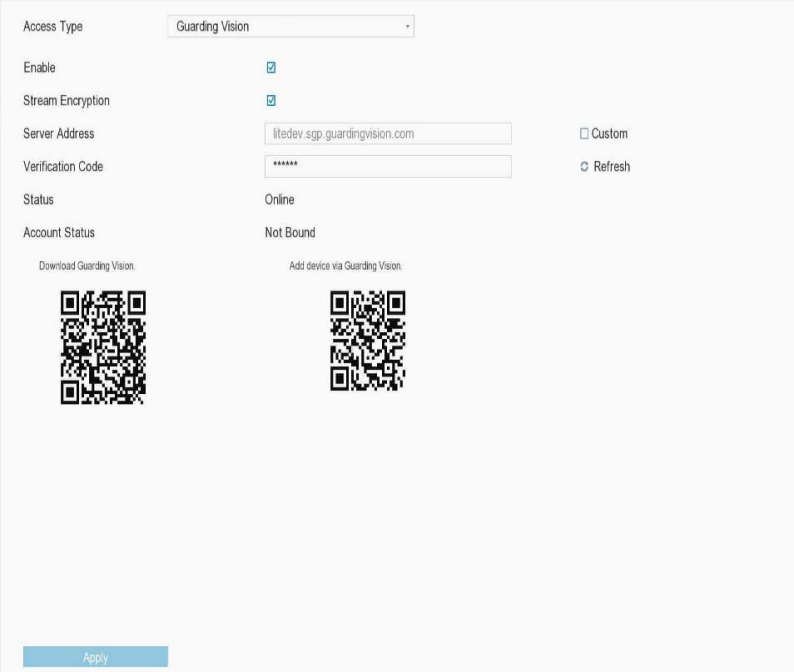


Figure 7.16 Platform Settings

2. Check **Enable** and a **Service Terms** window will pop up. Create your verification code, check to agree to the service terms and click **OK**.
3. (Optional) Check **Custom** and enter the server address as needed. The default server address is litev.sgp .guardingvision.com.
4. (Optional) Check **Enable Stream Encryption** and verification code will be required for remote access and live view.
5. Click **Apply**. After configuration, you can access and manage the DVR by your mobile phone

7.2.3 Configure Email

Purpose

The system can send an Email to designated users when a specified event occurs, such as an alarm or motion event is detected, or the administrator password is changed, etc.

Before You Start

Witch to Expert Mode/Easy Mode in the lower left corner of the menu.

Steps

1. Go to **Menu>Configuration> > Network > Email**.
2. Configure the following Email settings.

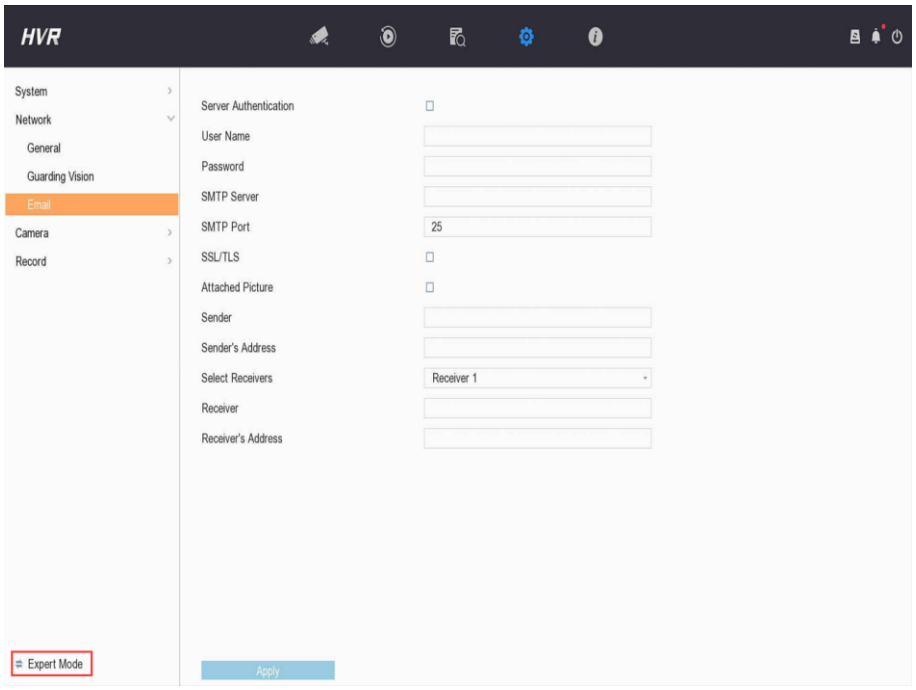


Figure 7.17 Email Settings

Server Authentication: Check to enable the function if the SMTP server requires user authentication and enter user name and password accordingly.

SMTP Server: The IP address of SMTP Server 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/TLS: Check to enable SSL/TLS if required by the SMTP server.

Sender: The name of the sender.

Sender's Address: Sender's Address.

Select Receivers: Select the receiver. Up to 3 receivers can be configured.

Receiver: The name of the receiver.

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

3. Click **Apply**.
4. (Optional) Click **Test** to send a test email.

7.3 Camera Settings

7.3.1 Configure Signal Input Channel

Purpose

You can configure the analog and IP signal input types.

Steps

1. Go to **Menu>Configuration> > Camera.**

2. Click **Camera > Analog**
3. Check the checkbox to select different signal input types: HD/CVBS and IP. If you select **HD/CVBS**, four types of analog signal inputs including Turbo HD, AHD, HDCVI, and CVBS can be connected randomly for the selected channel. If you select **IP**, IP camera can be connected for the selected channel.
4. Click **Apply** to save the settings.

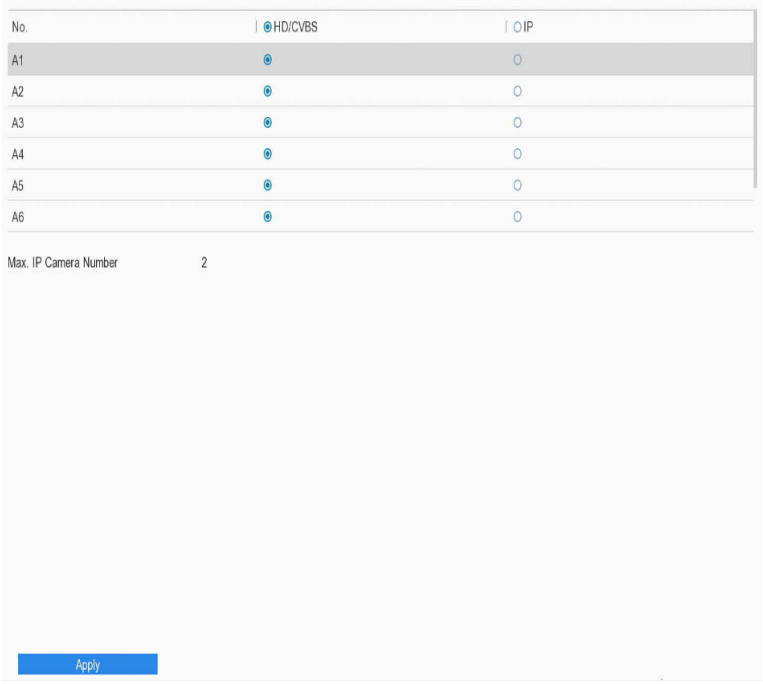


Figure 7.18 Signal Input Status

7.3.2 Add Online the IP Cameras

Purpose:

Before you can get live video or record the video files, you should add the network cameras to the connection list of the device.

Steps

1. Go to **Menu>Configuration> > Camera.**
2. Click Camera > IP Camera
3. On the **IP Camera** interface, click the **Online Device** to expand the panel.
4. Select the automatically searched online devices.
5. Click **Add** to finish the adding of the IP camera.

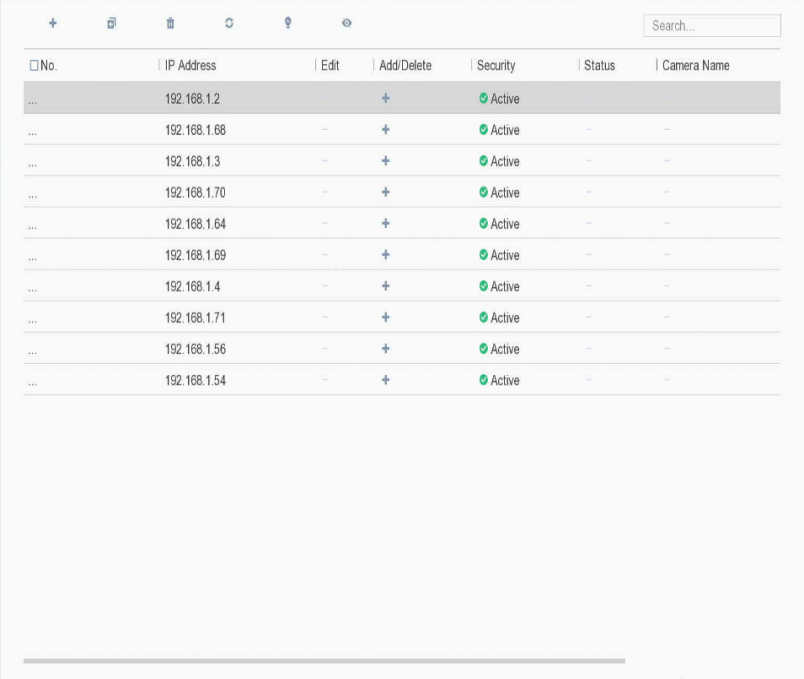


Figure 7.19 Add IP Camera

If the IP camera to add has not been activated, you can activate it from the IP camera list on the camera management interface.

7.3.3 Configure OSD Settings

Purpose:

You can configure the OSD (On-screen Display) settings for the camera, including date/time, camera name, etc.

Steps

1. Go to **Menu>Configuration> > Camera.**
2. Click **Display.**
3. Select the camera from the drop-down list.
4. Edit the name in the **Camera Name** text field.
5. Check the checkbox of the **Display Name**, **Display Date** and **Display Week** if you want to show the information on the image.
6. Set the date format, time format, and display mode.
7. You can use the mouse to click and drag the text frame on the preview window to adjust the OSD position.
8. Click the **Apply** button to apply the settings.

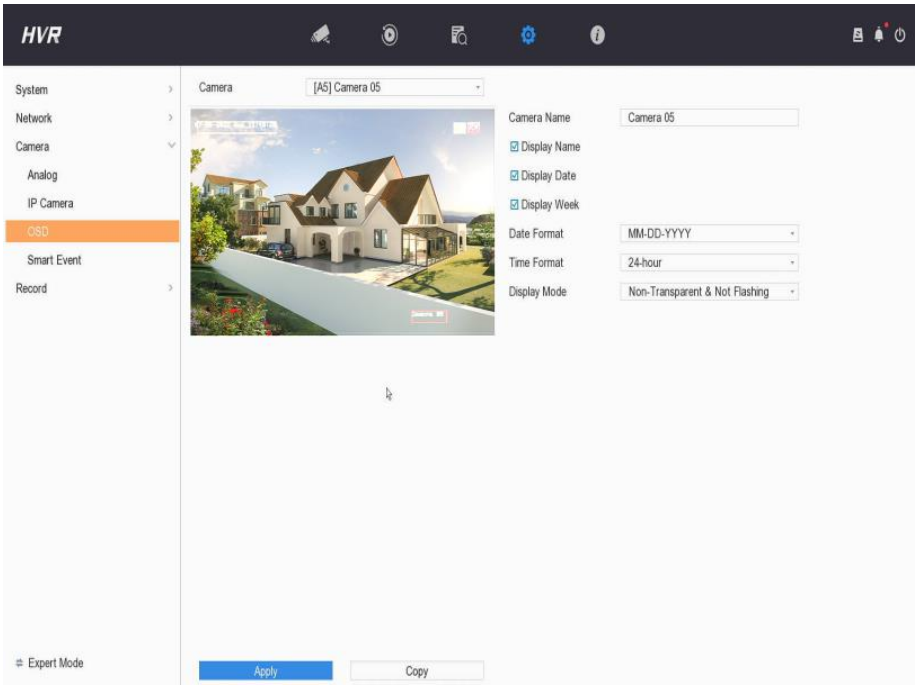


Figure 7.20 OSD Configuration Interface

7.3.4 Configure Privacy Mask

Purpose:

The privacy mask can be used to protect personal privacy by concealing parts of the image from view or recording with a masked area.

Steps

1. Go to **Menu>Configuration> Camera.**
2. Click **Privacy Mask**.
3. Select the camera to set privacy mask.
4. Click the checkbox of **Enable** to enable this feature.
5. Use the mouse to draw a zone on the window. The zones will be marked with different frame colors.
6. The configured privacy mask zones on the window can be cleared by clicking the corresponding Clear Zone1-4 icons on the right side of the window, or click **Clear All** to clear all zones.
7. Click **Apply** to save the settings.

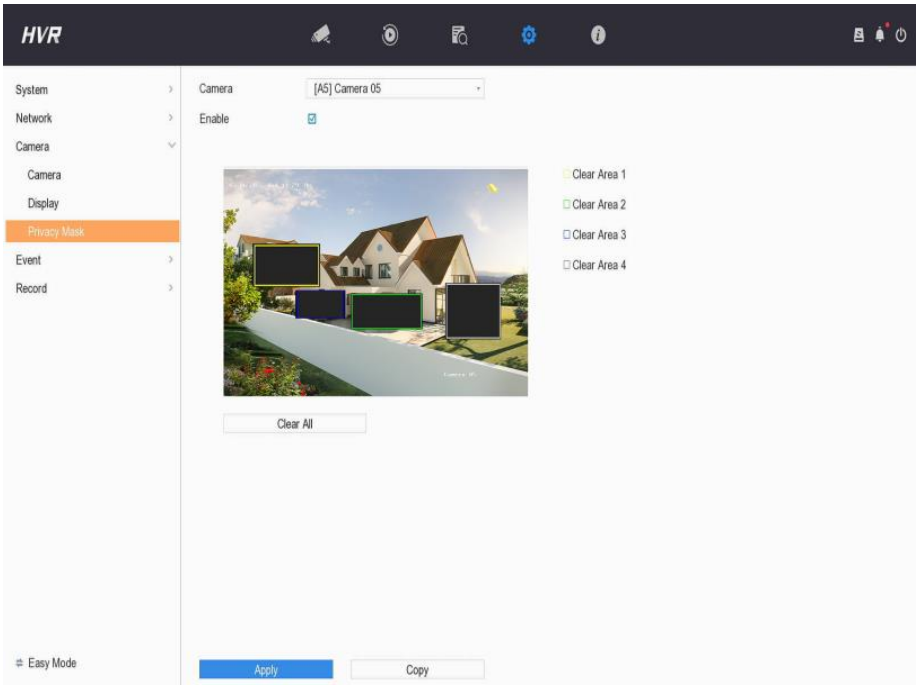


Figure 7.21 Privacy Mask Settings Interface

7.4 Event Settings

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.

7.4.1 Configuring Motion Detection

Purpose:

The motion detection enables the device to detect the moving objects in the monitoring area and trigger the alarm.

Steps

1. Go to **Menu>Configuration> Event > Normal Event > Motion Detection**.
2. Select the camera to configure the motion detection.
3. Check **Enable**

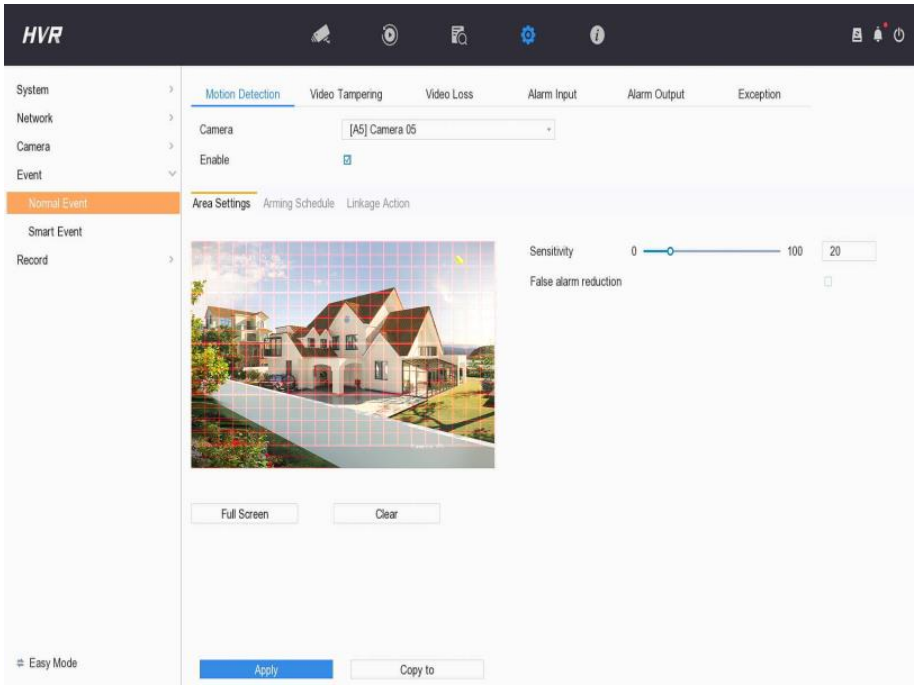


Figure7.22 Set Motion Detection

7.4.1.1 *Area*

Steps

1. Set the motion detection area.

   - Full screen: click to set the full-screen motion detection for the image.
   - Customized area: use the mouse to click and drag on the preview screen to draw the customized motion detection area (s).

You can click **Clear** to clear the current motion detection area settings and draw again.

2. Set sensitivity (0-100). The sensitivity allows you to calibrate how readily movement triggers the alarm. The higher value results in the more readily to trigger the motion detection.

7.4.1.2 *Arming Schedule*

Steps

1. Select the Arming Schedule tab.
2. Choose one day of a week and set the time segment. Up to eight time periods can be set within each day. Time periods shall not be repeated or overlapped.
3. Click **Apply** to save the settings.

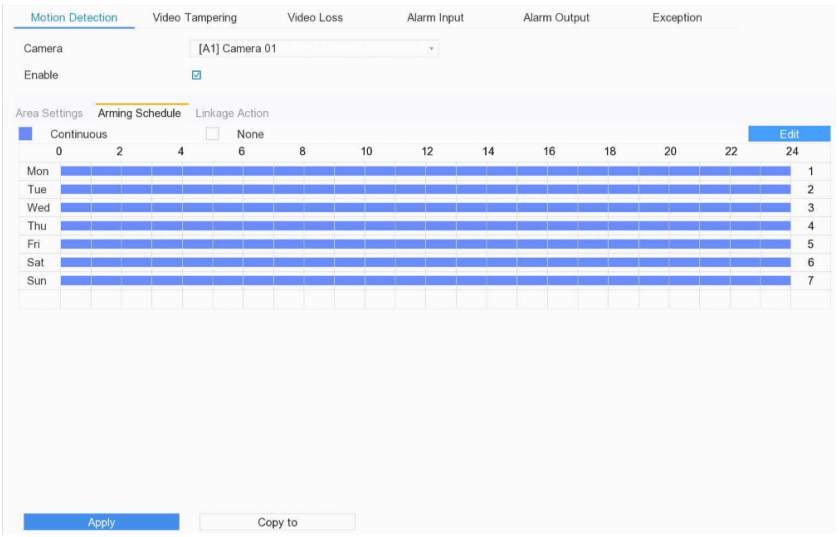


Figure 7.23 Arming Schedule

7.4.1.3 *Linkage Action*

Steps

1. Click Linkage Method tab.
2. Select the alarming linkage method(s) including Full Screen Monitoring， Audible Warning, Notify Surveillance Center, Send Email and Upload Pictures to Cloud.

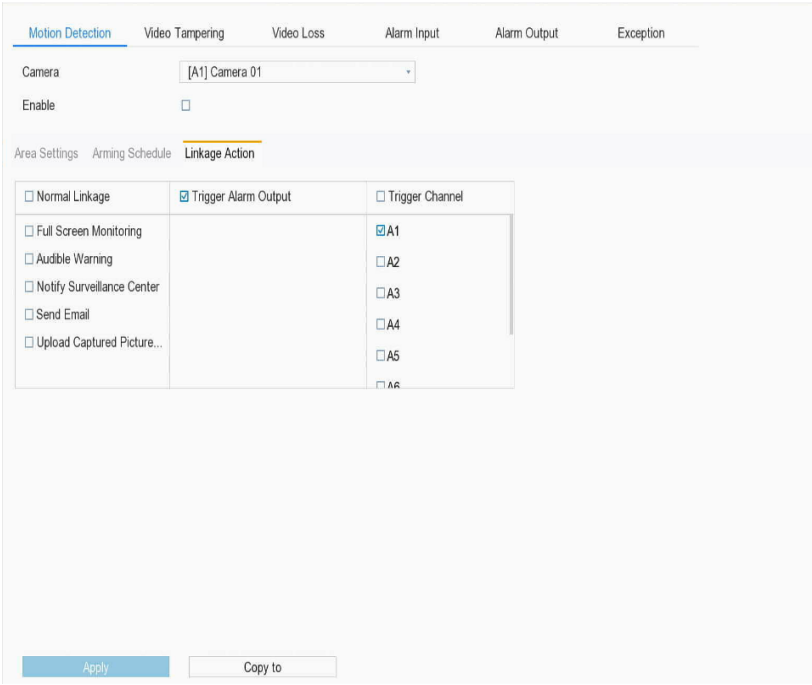


Figure 7.24 Motion Detection-Linking Method

7.4.1.3.1.1 Normal linkage

Full Screen Monitoring

If alarms are triggered simultaneously in several channels, their full-screen images will be switched at an interval of 10 seconds

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.

Upload Pictures to Cloud

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

7.4.1.3.1.2 Trigger Alarm Output

- Select the channel you want to trigger an external alarm output when a motion detection event occurs. To trigger an external alarm output when an event occurs, you need to go to the Alarm Output Settings to set the related parameters.

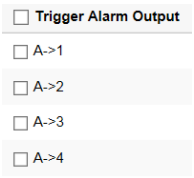


Figure 7.25 Motion Detection-Trigger Alarm Output

7.4.1.3.1.3 Trigger Channel

Steps

1. Select the channel you want to trigger recording when a motion detection event occurs.
2. Click **Apply** to save the settings.

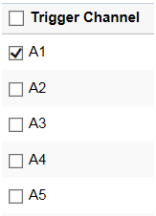


Figure 7.26 Motion Detection-Alarm Linked Recording

7.4.2 Configure Video Tampering Alarm

Purpose:

The video tampering detection enables to trigger alarm when the camera lens is covered and take alarm response action(s).

Steps

1. Go to **System > Event > Normal Event >Video Tampering**.
2. Select the camera to configure the video tampering detection.
3. Check **Enable**.
4. Set the video tampering area. Use the mouse to click and drag on the preview screen to draw the customized video tampering area.
5. Set sensitivity level (0-2). 3 levels are available. The sensitivity allows you to calibrate how readily movement triggers the alarm. The higher value results in the more readily to trigger the video tampering detection.
6. Click **Apply** to save the settings

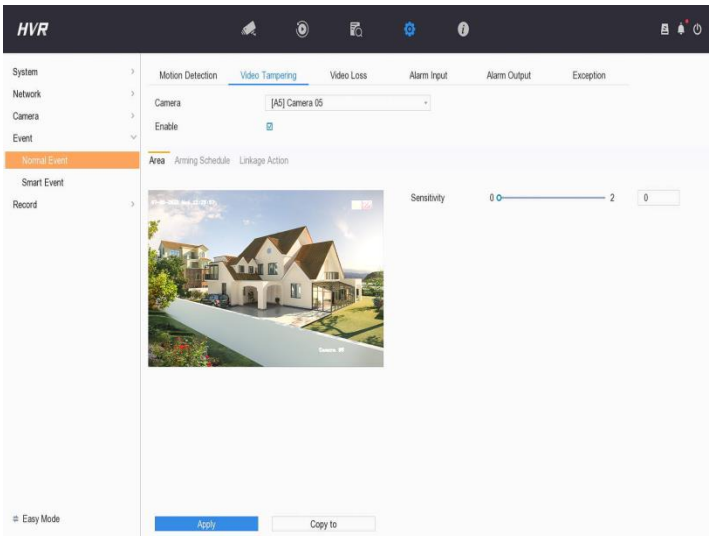


Figure 7.27 Set Video Tampering Setting

7. Set the arming schedule. Refer to Chapter 7.4.1.2 Configure Arming Schedule.
8. Set the linkage actions. Refer to Chapter 7.4.1.3 Configure Alarm Linkage Actions.

7.4.3 Configure Video Loss Alarm

Purpose:

The video loss detection enables to detect video loss of a channel and take alarm response action(s).

Steps

1. Go to **Menu>Configuration> Event > Normal Event >Video Loss.**
2. Select the camera to configure the video loss detection.
3. Check **Enable**.
4. Set the arming schedule. Refer to Chapter 7.4.1.2 Configure Arming Schedule.
5. Set the linkage actions. Refer to Chapter 7.4.1.3 Configure Alarm Linkage Actions.

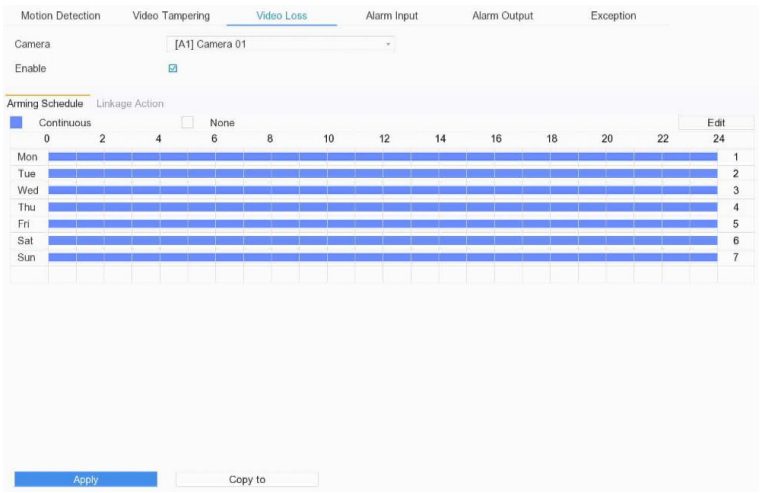


Figure 7.28 Set Video Loss Detection

7.4.4 Configure Exceptions Alarm

Purpose:

The exception events can be configured to take the event hint in the live view window, trigger alarm output and linkage actions.

Steps

1. Go to **Menu>Configuration> Event > Normal Event >Exception.**
2. (Optional) Enable the event hint if you want to display the event hint in the live view window.
3. Check **Enable Event Hint.**
4. Click  to select the exception type (s) to take the event hint.

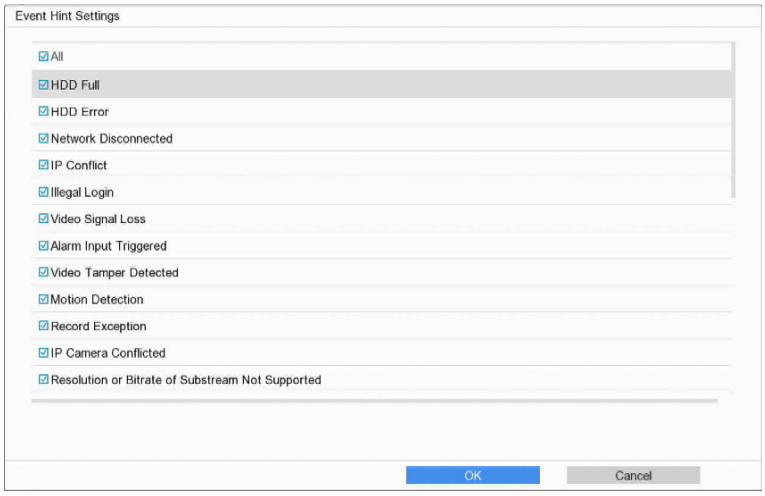


Figure 7.29 Event Hint Settings

5. Select the exception type from the drop-down list to set the linkage actions.

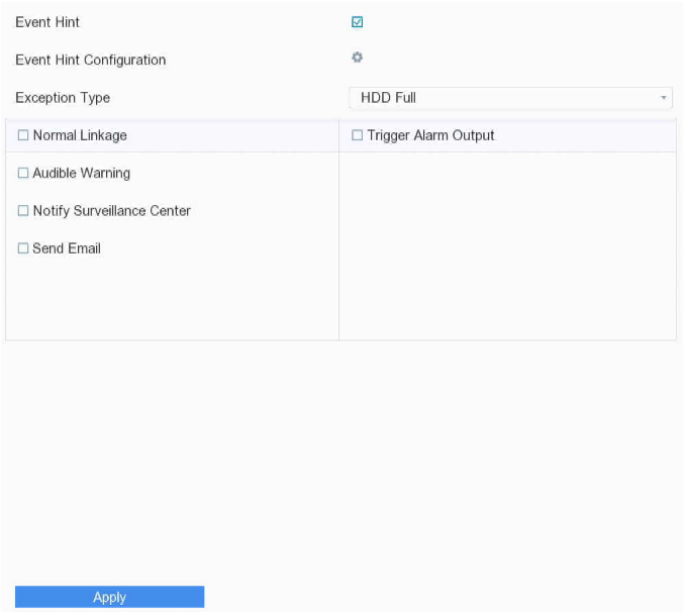


Figure 7.30 Exceptions Handling

6. Set the normal linkage and alarm output triggering. Refer to 7.4.1.3 Configure Alarm Linkage Actions.

7.5 Configure Recording

Purpose:

Set the record schedule, and then the camera automatically starts/stops recording according to the configured schedule.

Before you start

Make sure you have installed the HDDs to the device or added the network disks before you storing the video files, pictures and log files.

7.5.1 Recording Schedule

Steps

1. Go to **Menu>Configuration** > **Record** >**Schedule.**
2. Select a camera.
3. Check Enable.
4. Select a Record type. The record type can be Continuous、 Event and None.

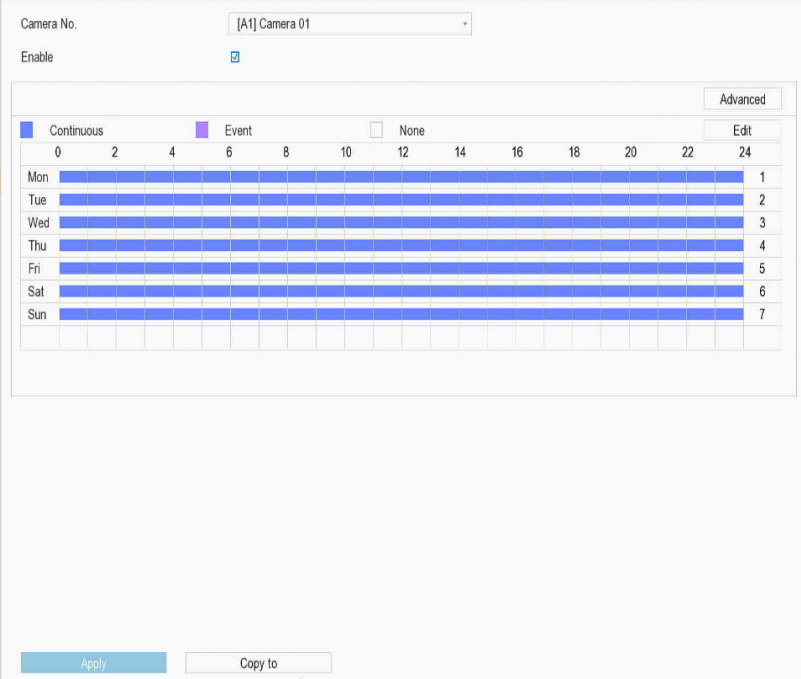


Figure 7.31 Record Schedule Settings

Different recording types are configurable.

Continuous: scheduled recording

Event: recording triggered by all event triggered alarm.

None: Don't recording video

5. Drag the mouse on the time bar to set the record schedule.
6. Click **Advanced** to configure advanced record parameters

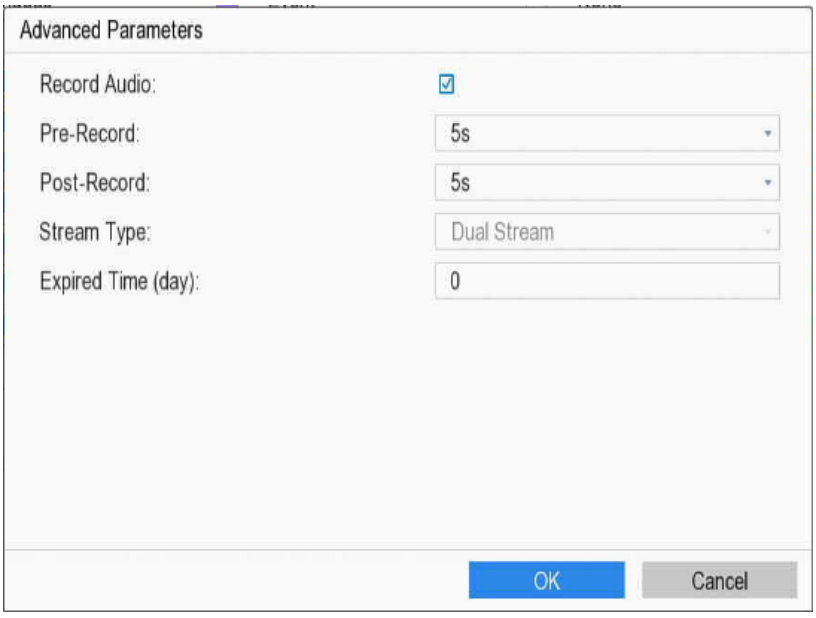


Figure 7.32 Advanced Record Settings

Record Audio: Check the checkbox to enable or disable audio recording.

Pre-record: The time you set to record before the scheduled time or event. For example, when an

alarm triggers the recording at 10:00, and if you set the pre-record time as 5 seconds, the camera records at 9:59:55.

Post-record: The time you set to record after the event or the scheduled time. For example, when an alarm triggered recording ends at 11:00, and if you set the post-record time as 5 seconds, it records till 11:00:05.

Expired Time: The expired time is period for a recorded file to be kept in the HDD. When the deadline is reached, the file will be deleted. If you set the expired time to 0, the file will not be deleted. The actual keeping time for the file should be determined by the capacity of the HDD.

Stream Type: Main stream and sub-stream are selectable for recording. When you select sub-stream, you can record for a longer time with the same storage space.

7. Click **OK** to save the settings.
8. If you want to copy the record schedule settings of the current camera to other cameras, click **Copy to** to copy the settings.
9. Click **Apply** to save the settings

7.5.2 Recording Parameters

7.5.2.1 *Main Steam*

Main stream refers to the primary stream that affects data recorded to the hard disk drive and will directly determine your recording quality and image size. Comparing with the sub-stream, the main stream can provide a higher quality video with higher resolution and frame rate.

Steps

1. Go to **Menu>Configuration** > **Record** >**Parameter**>**Main Steam.**
2. Select the camera from the drop-down list.
3. Click **Apply** to save the settings.

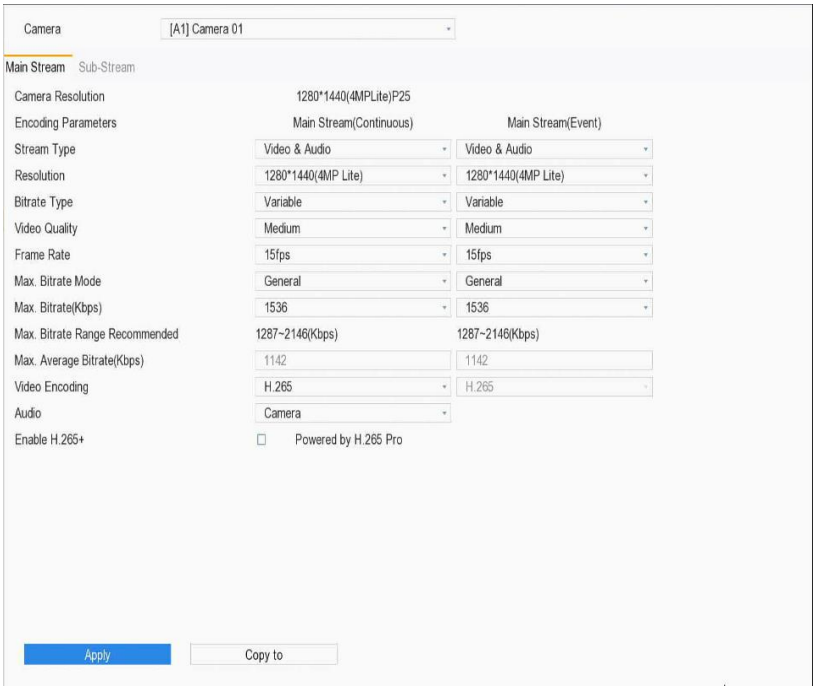


Figure 7.33 Main Stream Settings Interface

Frame Rate (FPS - Frames Per Second)

It refers to how many frames are captured each second. A higher frame rate is advantageous when there is movement in the video stream, as it maintains image quality throughout.

Resolution

Image resolution is a measure of how much detail a digital image can hold. The greater the resolution, the greater the level of detail. Resolution can be specified as the number of pixel-columns width) by the number of pixel-rows (height), e.g., 1024 ×768.

Bitrate

The bit rate (in Kbit/s or Mbit/s) is often referred to as speed, but actually defines the number of bits/time unit and not distance/time unit.

Enable H.264+

H.264+ combines intelligent analysis technology with predictive encoding, noise suppression, and long-term bit rate control to realize a lower bit rate, which plays a significant role in cutting storage costs and provides a higher return value for the investment.

7.5.2.2 *Sub-Stream*

Sub-stream is a second codec that runs alongside the main stream. It allows you to reduce the outgoing internet bandwidth without sacrificing your direct recording quality. Sub-stream is often exclusively used by apps to view live video. Users with limited internet speeds may benefit most from this setting.

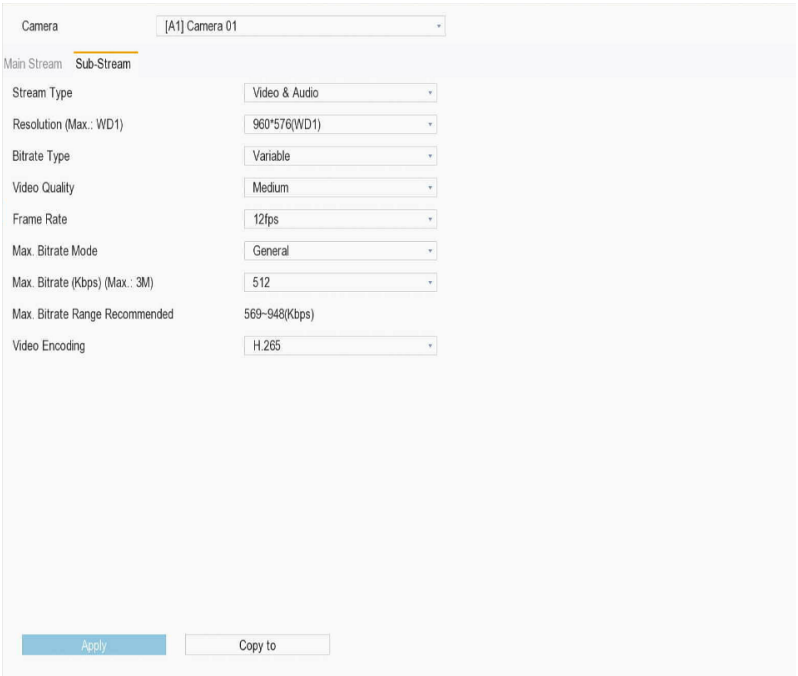


Figure 7.34 Sub-Stream Settings Interface

7.5.3 Add a Network Disk

You can add the allocated NAS or IP SAN disk to the device, and use it as a network HDD. Up to 2 network disks can be added.

Steps

1. Go to **Menu>Configuration** > **Record** >**Storage**
2. Click **Add**.

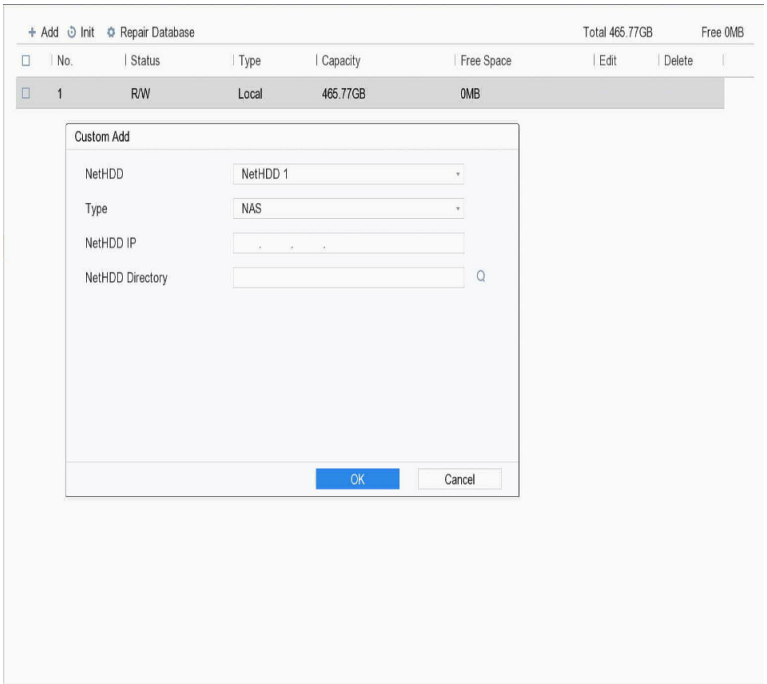


Figure 7.35 Add Net HDD

3. Select **Net HDD** type.
4. Enter **Net HDD IP** address and click to search the available Net HDD.
5. Select the desired Net HDD.
6. Click **OK**.
7. The added Net HDD will be displayed in the HDD list. Select the newly added Net HDD and click **Init**.

7.5.4 Storage Mode

7.5.4.1 *Configure HDD Quota*

Purpose:

Each camera can be configured with allocated quota for the storage of recorded files or captured pictures.

Steps

1. Go to **Menu>Configuration > Record >Storage Mode.**
2. Select **Mode** to **Quota**.

3. Select a camera to set quota
4. Enter the storage capacity of Max. Record Capacity (GB) and Max. Picture Capacity (GB).
5. (Optional) You can click **Copy to** if you want to copy the quota settings of the current camera to other cameras.
6. Click **Apply** to apply the settings. Reboot the device to activate the new storage mode settings.

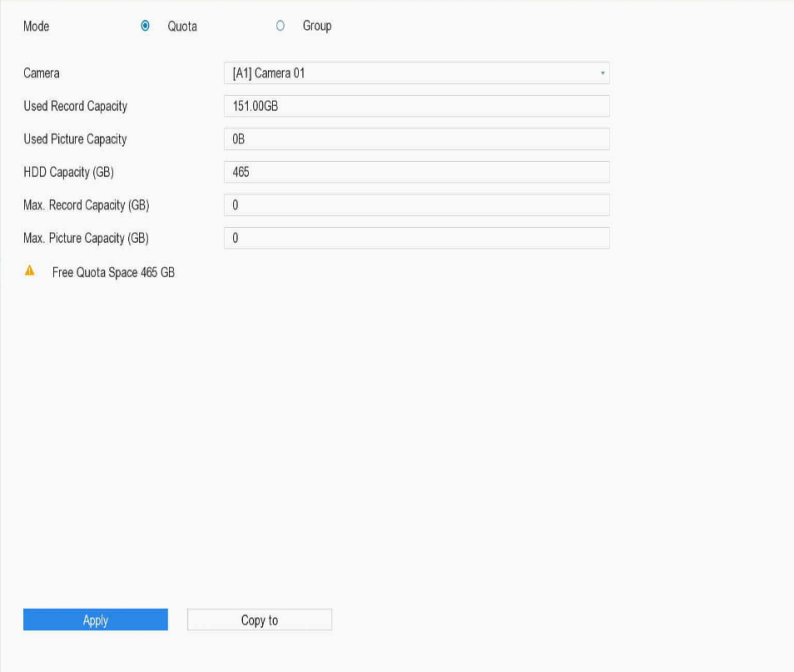


Figure 7.36 Storage Mode-HDD Quota

7.5.4.2 *Configure HDD Group*

Regroup the cameras for HDD if the HDD group number is changed.

Steps

1. Go to **Menu>Configuration > Record >Storage Mode.**
2. Select **Mode** to **Group**.
3. Select the group No. from **Record on HDD Group**.
4. Select the IP camera(s) to record/capture on the HDD group.
5. Click **Apply**.

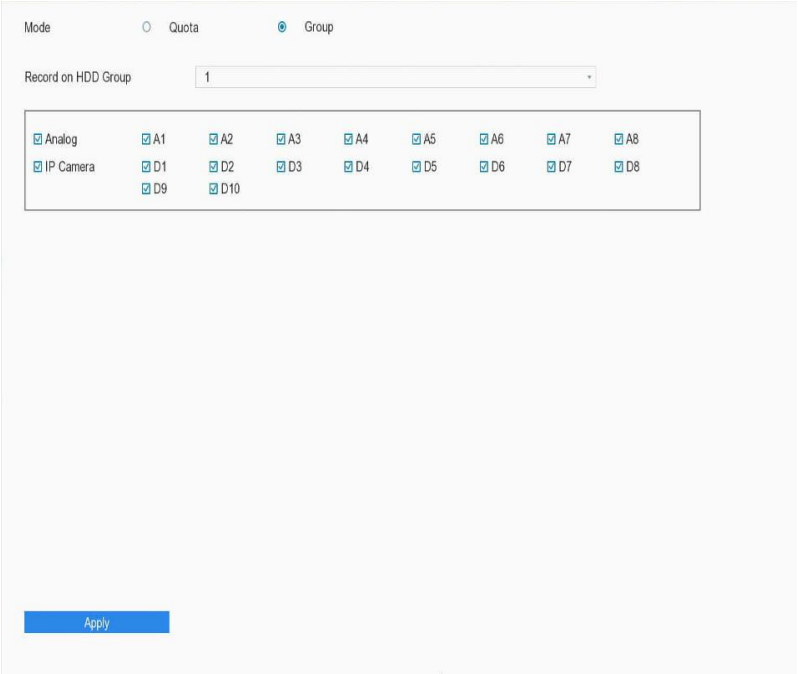


Figure 7.37 Storage Mode-HDD Group

7.5.5 Advanced Settings

Steps

1. Go to **Menu>Configuration** > **Record** >**Advanced Settings**.

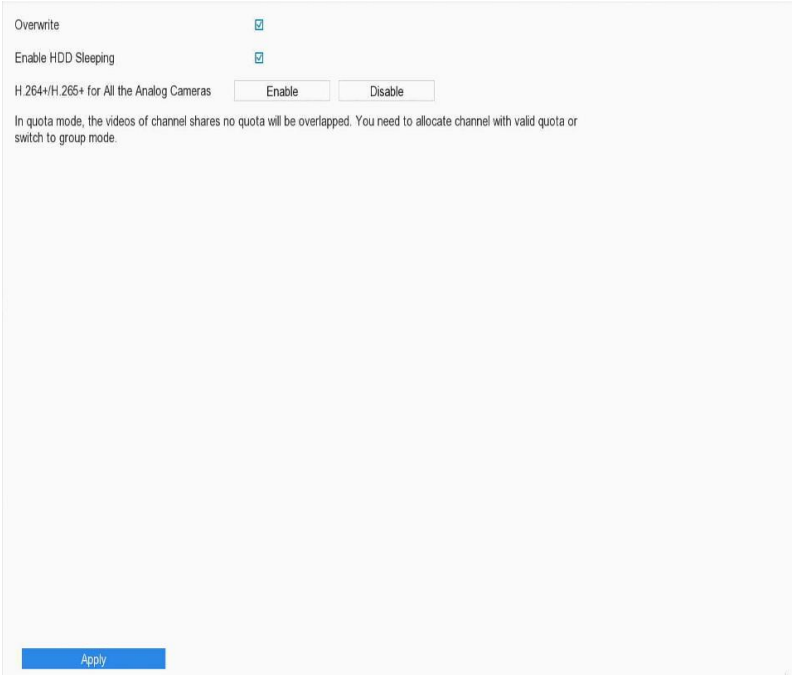


Figure 7.38 Advanced Settings

2. **Overwrite**: Use this option to overwrite the old recordings on the HDD when the HDD is full.

3. **Enable HDD Sleeping:** The HDDs which are free of working for a long time will be set to sleep.

4. **H.264+/H.265+ for All Analog Cameras**

① Click **Enable** button, the following attention box pops up to remind you that H.264+/H.265+ is already enabled for all analog cameras.

② Click **Disable** to disable H.264+/H.265+ for all the analog cameras and the following attention box pops up.

7.5.6 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

Steps

1. Go to **Configuration > Record> Cloud Storage**.
2. Check **Enable Cloud Storage** checkbox to enable the feature.
3. Select the **Cloud Type** from the drop-down list to Drop Box.

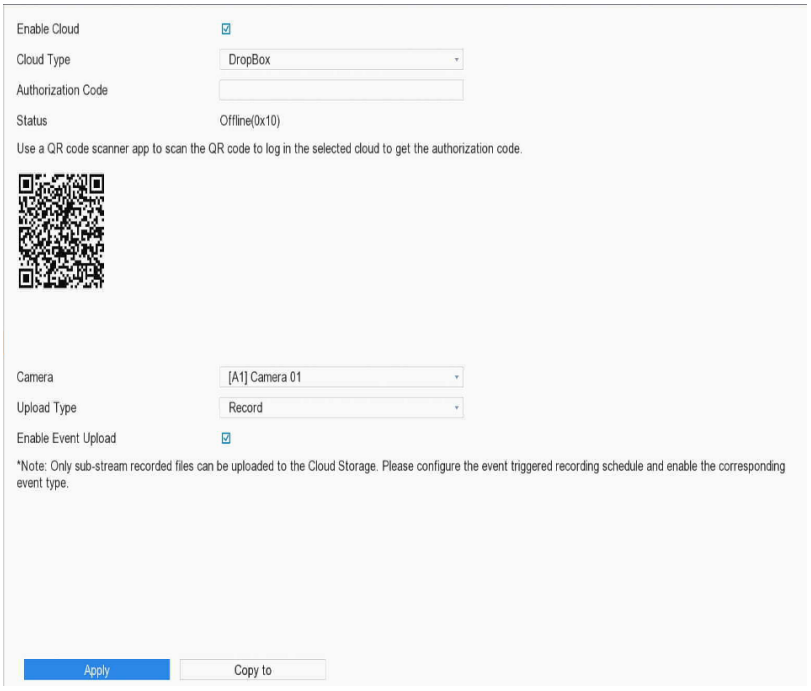


Figure 7.39 Cloud Storage Settings

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* 7.4.1.3 Configure Alarm Linkage Actions.

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.

8 System Maintenance

8.1 System Information

Steps

1. Go to **Menu > Maintenance**.
2. You can click Device Info to view the system information of the device.

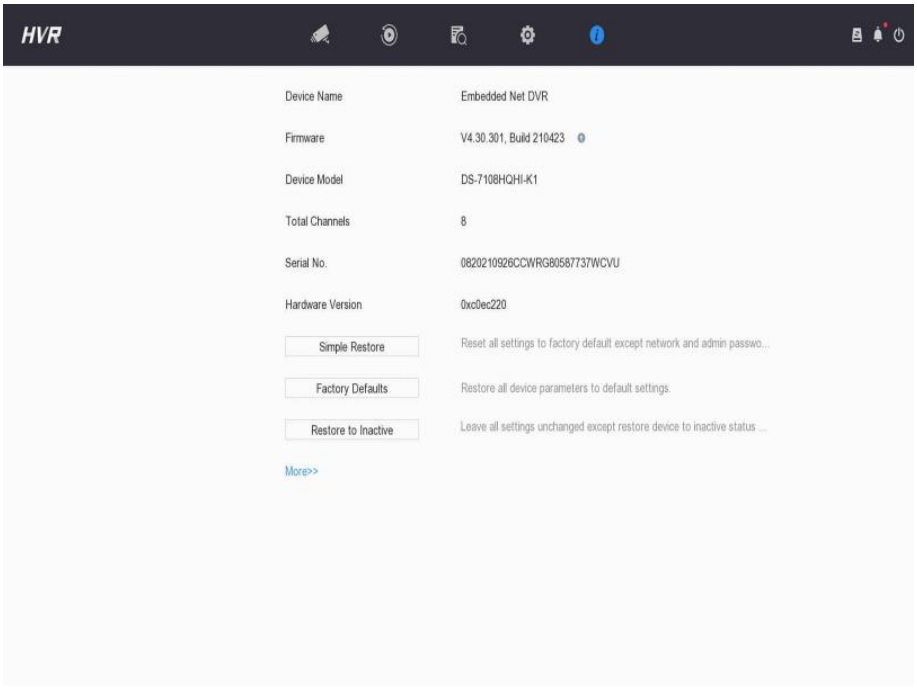


Figure 8.1 system information

8.2 Restoring Default Settings

Steps

1. Go to **Menu > Maintenance.**
2. Select the restoring type from the following three options

Simple Restore: Reset all settings to factory default except network and admin password settings.

Factory Defaults: Restore all parameters to the factory default settings.

Restore to Inactive: Restore the device to the inactive status.

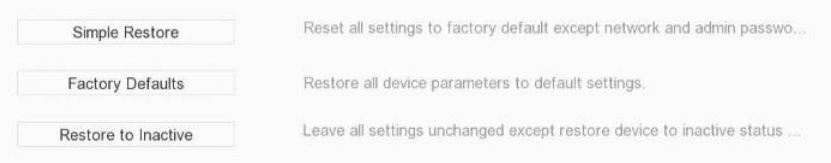


Figure 8.2 Restore Defaults

8.3 Upgrade System

8.3.1 Upgrade by Local Backup Device

Steps

1. Go to **Menu > Maintenance.**
2. Click to enter the Device Upgrade interface

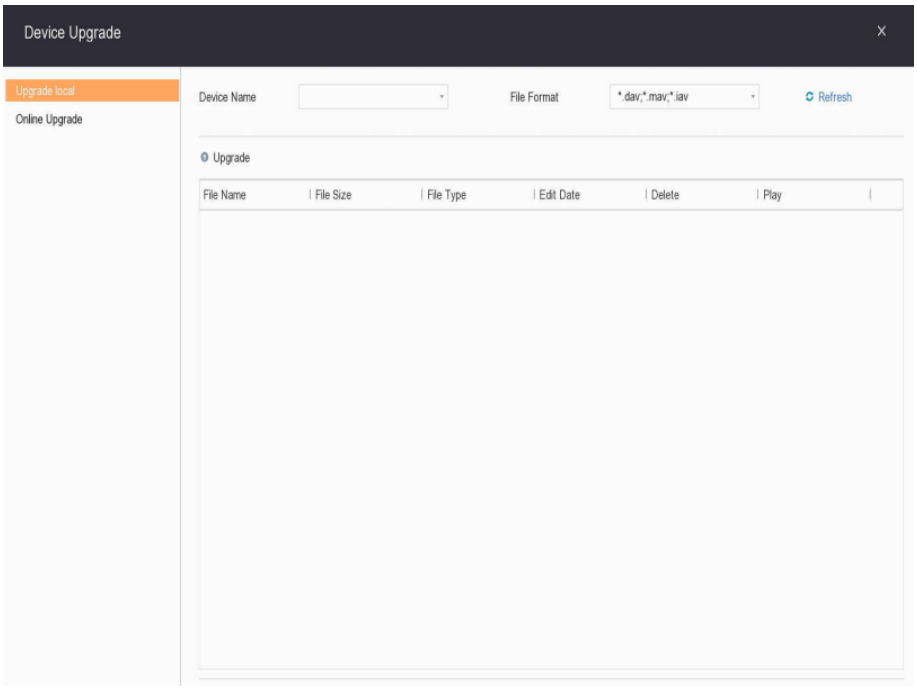


Figure 8.2 Device Upgrade

8.3.1.1 *Local Upgrade*

1. Select the update file from the backup device.
2. Click **Upgrade** to start upgrading.
3. The device will reboot automatically after the upgrading is completed

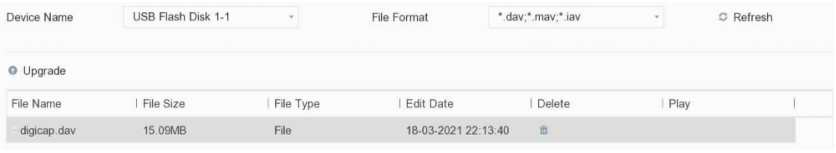


Figure 8.3 local Upgrade

8.3.1.2 *Online Upgrade*

1. Click **Test Upgrade** to manually check and download the latest firmware.
2. If new firmware version is available, click **Yes** to download the firmware at the pup up window.

Figure 8.4 Online Upgrade

3. (Optional) You can switch on **Download Latest Package Automatically** to automatically download the latest firmware package.
4. Click Upgrade Now.

8.4 Search & Export Log Files

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

8.4.1 Search the Log Files

Steps

1. Go to **Menu > Maintenance.**
2. Click More>> to enter the More Operation interface.
3. Select **log information.**
4. Click **Search** to start search log files.

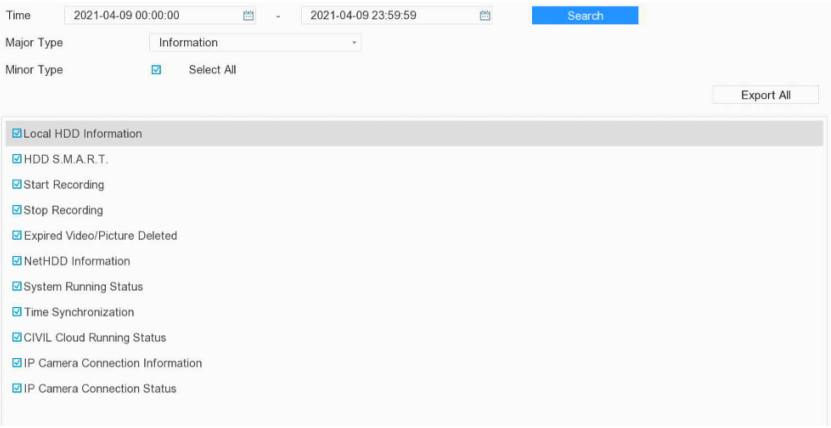


Figure 8.5 Log Search Interface

The matched log files will be displayed in the list shown below.

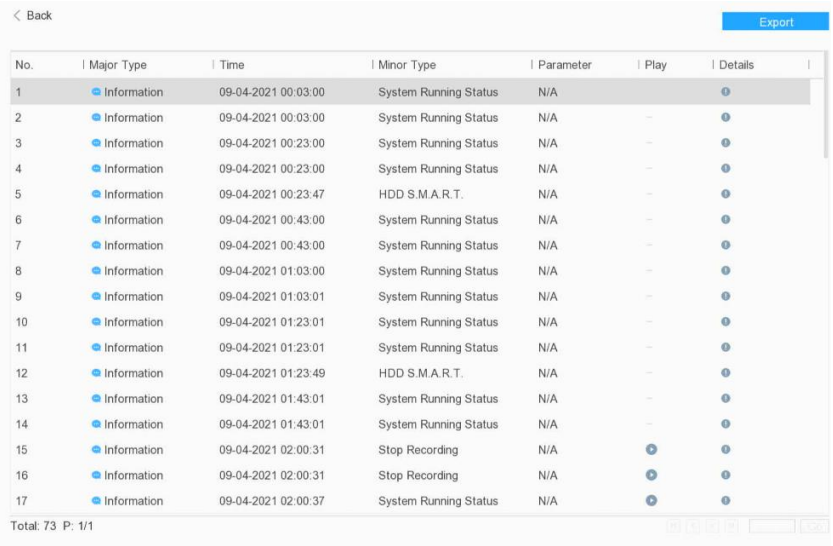


Figure 8.6 Log Search Results

Up to 2000 log files can be displayed each time.

Related Operation:

- Click or double click it to view its detailed information.
- Click to view the related video file.

8.4.2 Export the Log Files

Connect a storage device to your device.

Steps

1. Search the log files. Refer to Chapter 8.4.1 Search the Log Files.
2. Select the log files you want to export, and click **Export** Or you can click **Export ALL** on the Log Search interface to export all the system logs to the storage device.

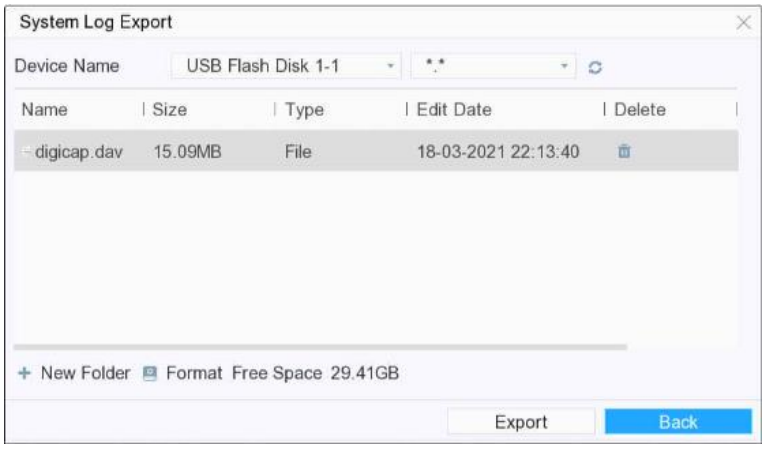


Figure 8.7 Export Log Files

3. Select the storage device from the dropdown list of **Device Name**.
4. Select the format of the log files to be exported. Up to 15 formats are selectable.
5. Click **Export** to export the log files to the selected storage device.

Related Operation:

- Click **New Folder** to create new folder in the storage device.
- Click **Format** to format the storage device before log export.

8.5 System Service

Purpose

You can disable SADP service to enhance the access security, e.g., when you are in the untrusted network environment.

Steps

1. Go to **Menu > Maintenance.**
2. Click More>> to enter the More Operation interface.
3. Select **System Service.**

Figure 8.8 Network Security Settings

Enable RTSP:

You can specifically secure the stream data of live view by setting the RTSP authentication. Two authentication types are selectable: **digest** and **digest/basic**. If you select **digest**, as the RTSP authentication, only the request with digest authentication can access the video stream by the RTSP protocol via the IP address. For security reasons, it is recommended to select digest as the authentication type.

HTTP Authentication:

If you need to enable the HTTP service, you can set the HTTP authentication to enhance the access security.

Two authentication types are selectable: **digest** and **digest/basic**. For security reasons, it is recommended to select digest as the authentication type.

9 Frequently Asked Questions

1. Why is there a part of channels displaying “No Resource” or turning black screen in multi-screen of live view?

Reason

1. Sub-stream resolution or bitrate settings is inappropriate.
2. Connecting sub-stream failed.

Solution

1. Go to **Camera → Video Parameters → Sub-Stream** . Select the channel, and turn down the resolution and max. bitrate (resolution shall be less than 720p, max. bitrate shall be less than 2048 Kbps).
2. Properly set the sub-stream resolution and max. bitrate (resolution shall be less than 720p, max. bitrate shall be less than 2048 Kbps), then delete the channel and add it back again.

2. Why is the video recorder notifying not support the stream type?

Reason

The camera encoding format mismatches with the video recorder.

Solution

If the camera is using H.265/MJPEG for encoding, but video recorder does not support H.265/ MJPEG, change the camera encoding format to the same as video recorder.

3. How to improve the playback image quality?

Reason

Recording parameter settings are inappropriate.

Solution

Go to **Camera → Video Parameters** . Increase resolution and max. bitrate, and try again.

4. How to confirm the video recorder is using H.265 to record video?

Solution

Check if the encoding type at live view toolbar is H.265.

5. Why is the timeline at playback not constant?

Reason

1. When the video recorder is using event recording, it only records video when event occurs. Hence the video may not be continuous.

2. Exception occurs, such as the device offline, HDD error, record exception, network camera offline, etc.

Solution

1. Ensure the recording type is continuous recording.

2. Go to **Maintenance → Log Information** . Search the log file during the video time period. See if

there are unexpected events, such as HDD error, record exception, etc.

6. Why is the IP address of network camera being changed automatically?

Reason

When network camera and video recorder are using the same switch but in different subnet, the video recorder will change the IP address of network camera to the same subnet as itself.

Solution

When adding camera, click **Custom Add** to add camera.

7. Why is the video recorder notifying IP conflict?

Reason

The video recorder uses the same IP address as other devices.

Solution

Change the IP address of video recorder. Ensure it is not the same as other devices.

8. Why is there no recorded video after setting the motion detection?

Reason

1. The recording schedule is incorrect.
2. The motion detection event setting is incorrect.
3. HDD exception.

Solution

1. The recording schedule is setup correctly by following the steps listed in Configuring Record/Capture Schedule.
2. The motion detection area is configured correctly. The channels are being triggered for motion detection (See Configuring Motion Detection).
3. Check if the device has installed HDD.

Check if the HDD is initialized. If not, go to Storage > Storage Device to initialize the HDD.

Check if the HDD is broken. You can change it, and try again.

9. Why is the sound quality not good in recording video?

Reason

1. The audio input device does not have a good effect in sound collection.
2. Interference in transmission.
3. The audio parameter is not properly set.

Solution

1. Check if the audio input device is working properly. You can change another audio input device, and try again.
2. Check the audio transmission line. Ensure all lines are well connected or welded, and there is no electromagnetic interference.
3. Adjust the audio volume according to the environment and audio input device.