

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 RESPONSIBILITIES 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
1.1	FRONTPANEL.....	1
1.2	REARPANEL	1
1.3	USB MOUSE OPERATION	2
1.4	HDD INSTALLATION	2
2	GETTING STARTED.....	4
2.1	START UP THE DEVICE	4
2.2	ACTIVATE THE DEVICE	4
2.3	CONFIGURE UNLOCK PATTERN FOR LOGIN.....	6
2.4	LOGIN TO THE DEVICE.....	6
2.4.1	<i>Log in via Unlock Pattern.....</i>	<i>6</i>
2.4.2	<i>Log in via Password</i>	<i>7</i>
2.5	ENTER WIZARD TO CONFIGURE QUICK BASIC SETTINGS	8
2.6	ENTER MAIN MENU	10
2.7	SYSTEM OPERATION	11
2.7.1	<i>Log out</i>	<i>11</i>
2.7.2	<i>Shut Down the Device</i>	<i>11</i>
2.7.3	<i>Reboot the Device</i>	<i>11</i>
3	LIVE VIEW	11
3.1	INTRODUCTION OF LIVE VIEW.....	11
3.1.1	<i>Quick Setting Toolbar in Live View Mode:.....</i>	<i>12</i>
3.2	DIGITAL ZOOM	13
3.3	LIVE VIEW STRATEGY	13
3.4	PTZ CONTROL WIZARD.....	14
3.4.1	<i>Configure PTZ Parameters</i>	<i>14</i>
3.4.2	<i>Set PTZ Presets, Patrols & Patterns.....</i>	<i>15</i>
3.4.3	<i>Auxiliary Functions.....</i>	<i>20</i>
4	PLAYBACK	21
4.1	INSTANT PLAYBACK	21

4.2	PLAY NORMAL VIDEO	21
4.3	PLAY SMART SEARCHED VIDEO	22
4.4	PLAY CUSTOM SEARCHED FILES.....	23
4.5	PLAY TAG FILES	24
4.6	PLAY EVENT FILES.....	26
4.7	PLAY BY SUB-PERIODS	27
4.8	PLAY LOG FILES.....	27
4.9	PLAY EXTERNAL FILE	28
4.10	PLAYBACK OPERATIONS	28
4.10.1	<i>Set Play Strategy in Smart/Custom Mode</i>	28
4.10.2	<i>Edit Video Clips</i>	28
4.10.3	<i>Thumbnails View</i>	28
4.10.4	<i>Fast View</i>	29
4.10.5	<i>Digital Zoom</i>	29
5	FILE MANAGEMENT	29
5.1	SEARCH AND EXPORT ALL FILES.....	29
5.1.1	<i>Search Files</i>	29
5.1.2	<i>Export Files</i>	30
5.2	SEARCH AND EXPORT HUMAN FILES	31
5.2.1	<i>Search Files</i>	31
5.2.2	<i>Export Human Files</i>	32
5.3	SEARCH AND EXPORT VEHICLE FILES	32
5.3.1	<i>Search Vehicle Files</i>	32
5.3.2	<i>Export Vehicle Files</i>	33
6	SMART ANALYSIS	33
6.1	PEOPLE COUNTING.....	33
6.2	HEAT MAP.....	34
7	CAMERA MANAGEMENT.....	35
7.1	CONFIGURE SIGNAL INPUT CHANNEL	35
7.1.1	<i>Configuring 5 MP Long Distance Transmission</i>	35
7.1.2	<i>Add the IP Cameras</i>	36
7.2	CAMERA CONFIGURE OSD SETTINGS.....	37
7.3	CONFIGURE PRIVACY MASK	38
7.4	CONFIGURE THE VIDEO PARAMETERS	39

7.4.1	Main Stream.....	39
7.4.2	Sub-Stream	40
8	STORAGE	40
8.1	CONFIGURING RECORD SCHEDULE.....	40
8.2	STORAGE DEVICE	42
8.2.1	Manage Local HDD	42
8.2.2	Add a Network Disk	44
8.3	STORAGE MODE	45
8.3.1	Configure HDD Quota	45
8.3.2	Configure HDD Group	45
8.3.3	Advanced	46
8.3.4	Cloud Storage.....	46
9	SYSTEM CONFIGURATION	50
9.1	CONFIGURE GENERAL SETTINGS.....	50
9.2	MANAGE USER ACCOUNTS	51
9.2.1	Add a User	51
9.2.2	Set Permission for a User	53
9.2.3	Edit the Admin User	54
9.2.4	Set Local Live View Permission.....	55
9.2.5	Delete a User.....	56
9.3	NETWORK SETTINGS.....	56
9.3.1	Configure TCP/IP Settings	56
9.3.2	Configure Advanced Settings	60
9.4	EVENT SETTINGS.....	63
9.4.1	Configuring Motion Detection	63
9.4.2	Configure Video Tampering Alarm.....	66
9.4.3	Configure Video Loss Alarm	66
9.4.4	Configure Exceptions Alarm	67
9.5	CONFIGURE LIVE VIEW SETTINGS	68
9.5.1	General Settings.....	68
9.5.2	Configure Live View Layout.....	69
9.5.3	Configure Channel-Zero Encoding.....	69
9.6	CONFIGURE HOLIDAY RECORDING	70
10	SYSTEM MANAGEMENT	71

10.1	VIEWING SYSTEM INFORMATION	71
10.2	SEARCH & EXPORT LOG FILES	71
10.2.1	<i>Search the Log Files</i>	71
10.2.2	<i>Export the Log Files</i>	72
10.3	IMPORT/EXPORT DEVICE CONFIGURATION FILES	73
10.4	UPGRADE SYSTEM.....	73
10.4.1	<i>Upgrade by Local Backup Device</i>	73
10.4.2	<i>Upgrade by FTP</i>	74
10.4.3	<i>Upgrade by Online Upgrade</i>	74
10.4.4	<i>Upgrade Camera</i>	75
10.5	RESTORE DEFAULT SETTINGS	75
10.6	NETWORK DETECTION	76
10.6.1	<i>Network Traffic Monitoring</i>	76
10.6.1	<i>Test Network Detection</i>	76
10.7	STORAGE DEVICE MAINTENANCE	77
10.7.1	<i>S.M.A.R.T. Detection</i>	77
10.7.2	<i>Bad Sector Detection</i>	78
10.8	SECURITY MANAGEMENT	79
10.8.1	<i>RTSP Authentication</i>	79
10.8.2	<i>ISAPI Service</i>	79
10.8.3	<i>HTTP Authentication</i>	79
10.8.4	<i>Managing ONVIF User Accounts</i>	80
11	FREQUENTLY ASKED QUESTIONS	81

1 Introduction

1.1 Front Panel

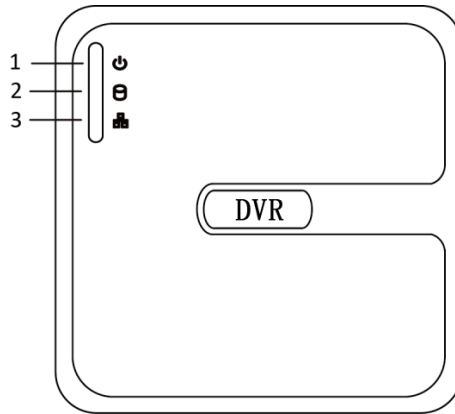


Figure 1.1 Front Panel

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

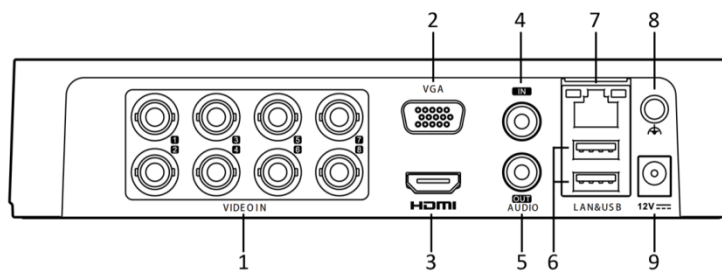


Figure1.2 Rear Panel

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 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.

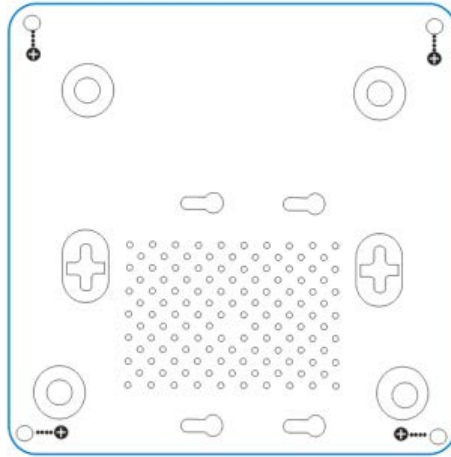


Figure1.3 Device bottom

2. Connect the data cable and power cable.

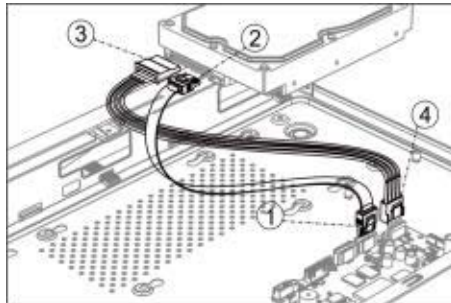


Figure1.4 HDD line

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.

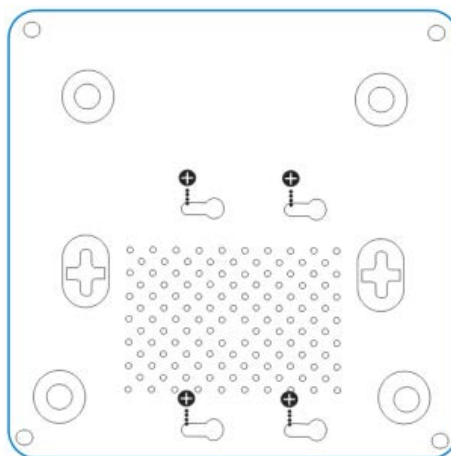


Figure1.5 Fixed HDD

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

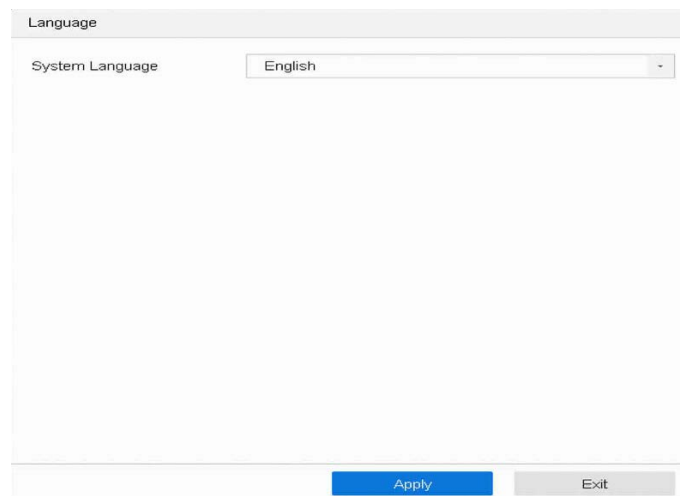


Figure 2.1 Set OSD Language

2. Enter the admin password twice.

admin

Strong

Reserved E-mail Settings ?

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

OK

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.

Reserved E-mail Settings

Reserved E-mail

OK Cancel

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.

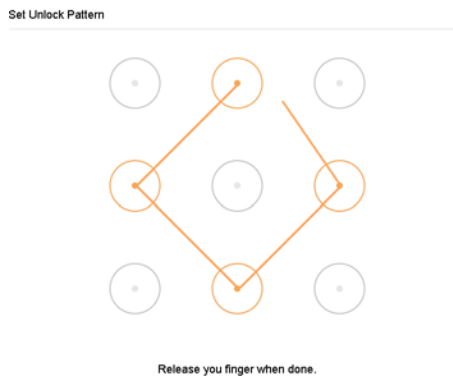


Figure 2.4 Draw the Pattern

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.

2.5 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 2.7 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 2.8 Network Settings

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

Label	Status	Type	Capacity	Free Space	Edit	Delete
1	RW	Local	2794.52GB	2765.00GB		

Figure 2.9 HDD Management

4. To initialize the HDD, click the **Init** button. Initialization removes all the data saved in the HDD.
5. Click **Next**. You enter the **Camera Setup** 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.

 **NOTE**

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

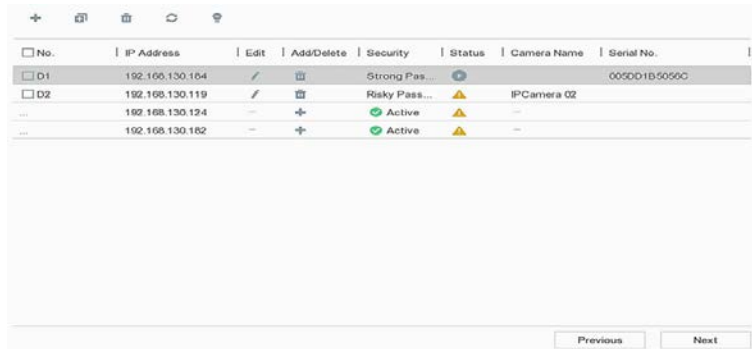


Figure 2.10 Search for IP Cameras

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

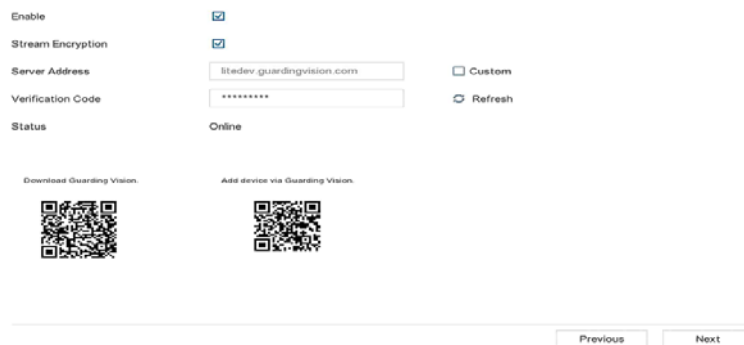



Figure 2.11 Guarding Vision P2P Connect Access

2. Click **Next** to enter the **Change Password** interface to create the new admin password if required.



Figure 2.12 Change Password

 **NOTE**

You can enter click the  to show the characters input.

- 1) Check the checkbox of **New Admin Password**.
- 2) Enter the original password in the text field of **Admin Password**
- 3) Input the same password in the text field of **New Password** and **Confirm**.
- 4) Check the **Unlock Pattern** to enable the unlock pattern login.

 **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. Click **OK** 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
	Smart Analysis
	Camera Management
	Storage 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.



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**




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.

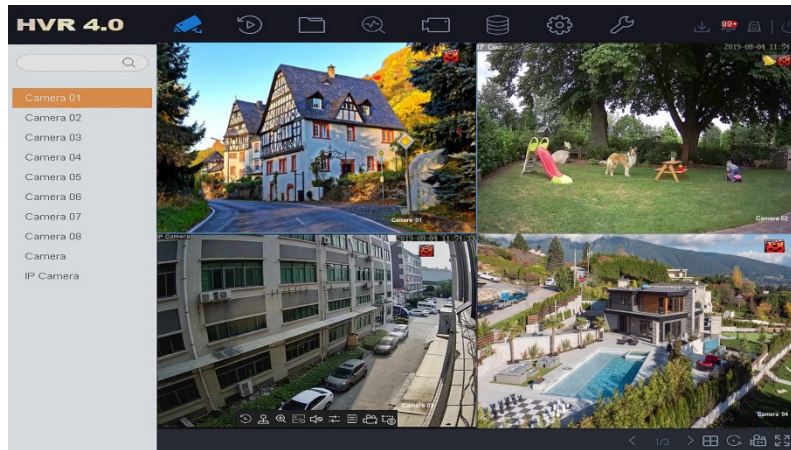


Figure 3.1 Live view windows

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		Live View Strategy
	PTZ Control		Information
	Digital Zoom		Enable/Disable Manual Record
	Image Settings		Switch to sub
	Mute/Audio on		


 Instant Playback only shows the record in last five minutes. If no record is found, it means there is no record during the last five minutes.


 The quick PTZ Control settings toolbar in the live view interface.

 Digital Zoom is for zooming in the live image. You can zoom in the image to different proportions (1 to 16X) by moving the sliding bar. You can also scroll the mouse wheel to control the zoom in/out.

 Image Settings icon can be selected to enter the Image Settings menu.

 The live view strategy to **Real-time**, **Balanced** or **Fluency** . Only support IP camera.

 Move the mouse onto the Information icon to show the real-time stream information, including the frame rate, bit rate, resolution and stream type.

 Switch between main stream and sub stream, only support IP camera. (Maximum support 2 channels 5mp)

3.2 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 3.3 Digital Zoom

3.3 Live View Strategy

Steps

1. In the live view mode, click  to enter the digital zoom operation interface in full screen

mode.


2. Select the live view strategy to **Real-time**, **Balanced** or **Fluency**.

3.4 PTZ Control Wizard

Before you start

Please make sure the connected IP camera supports the PTZ function and is properly connected.

Steps

1. Click  on the quick settings toolbar in the live view interface. The PTZ control wizard will pop up as below.

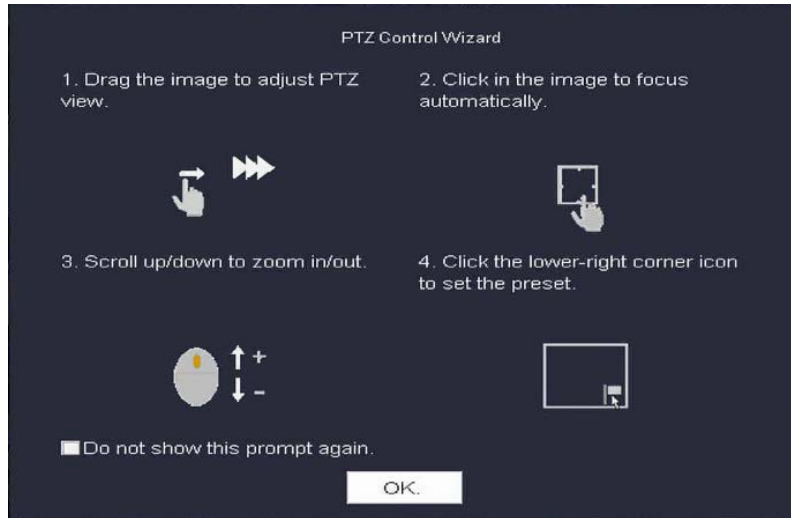


Figure 3.4 Digital Zoom


2. Follow the wizard to adjust the PTZ view, focus, and zoom in/out the camera.
3. (Optional) Check *Do not show this prompt again*.
4. Click **OK** to exit.

3.4.1 Configure PTZ Parameters

Purpose:

Follow the procedure to set the parameters for PTZ. The configuration of the PTZ parameters should be done before you control the PTZ camera.

Steps

1. Click  on the quick settings toolbar in the live view interface. The PTZ control panel displays on the right of the interface.
2. Click **PTZ Parameters Settings** to set the PTZ parameters.

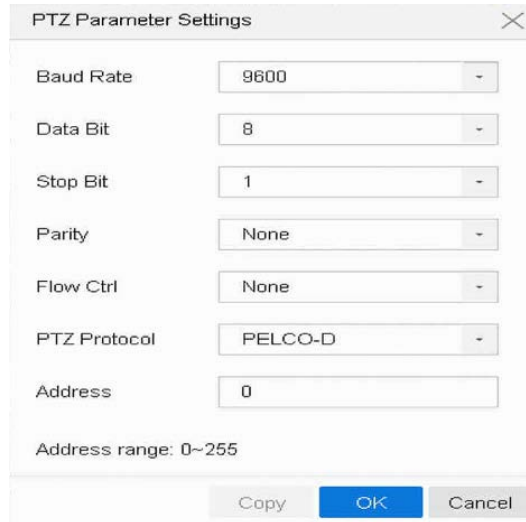


Figure 3.5 PTZ Parameters Settings

3. Edit the parameters of the PTZ camera.
4. Click **OK** to save the settings.



All the parameters should be exactly the same as the PTZ camera parameters.

3.4.2 Set PTZ Presets, Patrols & Patterns

Before you start:

Please make sure that the presets, patrols and patterns should be supported by PTZ protocols.

3.4.2.1 Set a Preset

Purpose:

Follow the steps to set the preset location which you want the PTZ camera to point to when an event takes place.

Steps



1. Click  on the quick settings toolbar in the live view interface.
2. Use the directional buttons on the PTZ control panel to wheel the camera to the location where you want to set preset, and the zoom and focus operations can be recorded in the preset as well.
3. Click  in the lower right corner of live view to set the preset.



Figure 3.6 Set Preset

4. Select the preset No. (1~255) from the drop-down list.
5. Enter the preset name in the text field.
6. Click **Apply** to save the preset.
7. Repeat steps 2-6 to save more presets.
8. (Optional) Click **Cancel** to cancel the location information of the preset.


- (Optional) Click  in the lower right corner of live view to view the configured presets.



Figure 3.7 View the Configured Presets

3.4.2.2 Call a Preset

Purpose:

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

Steps



- Click  on the quick settings toolbar in the live view interface.
- Click  in the lower right corner of live view.
- Select the preset No. from the drop-down list.
- Click **Call** to call it.



Figure 3.8 Call Preset (1)


- Or click  in the lower right corner of live view, and click the configured preset to call it.




Figure 3.9 Call Preset (2)

3.4.2.3 Set a Patrol

Purpose:

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

Steps

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

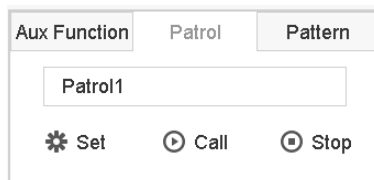


Figure 3.10 Patrol Configuration

- Select the patrol No. in the text field.
- Click **Set** to enter the Patrol Settings interface.

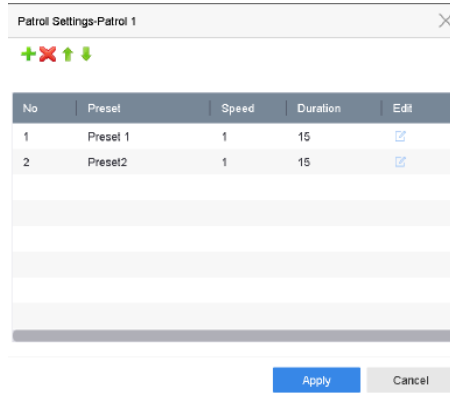


Figure 3.11 Patrol Settings

- 5 Click to add key point for the patrol.

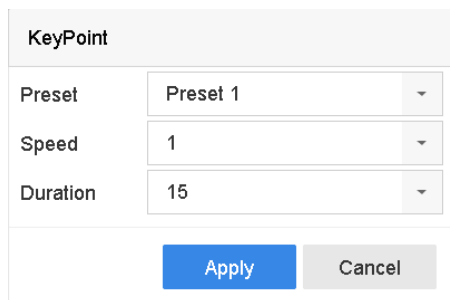


Figure 3.12 Key Point Configuration

- A. Configure key point parameters.

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

Speed: It defines the speed at which the PTZ will move from one key point to the next.

Duration: It refers to the time span to stay at the corresponding key point.

- B. Click **Apply** to save the key points to the patrol.

- 6 (Optional) Click to edit the added key point.

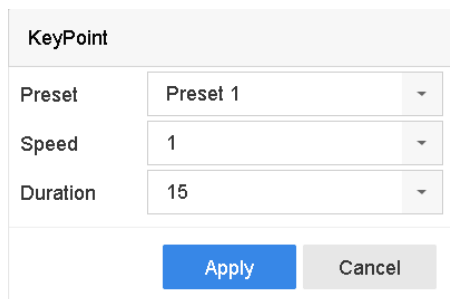


Figure 3.13 Edit Key Point

- 7 (Optional) Select a key point and click to delete it.

- 8 (Optional) Click or to adjust the key point order.

- 9 Click **Apply** to save the settings of the patrol.


- 10 Repeat steps 3-9 to set more patrols.

3.4.2.4 Call a Patrol

Purpose:

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

Steps

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

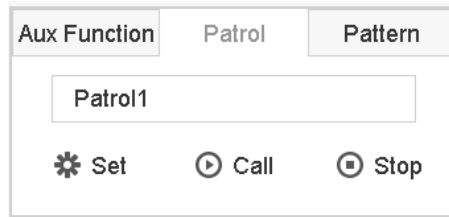


Figure 3.14 Patrol Configuration


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

3.4.2.5 Set a Pattern

Purpose:

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

Steps

1. Click  on the quick settings toolbar in the live view interface.
The PTZ control panel displays on the right of the interface.
2. Click **Pattern** to configure pattern.

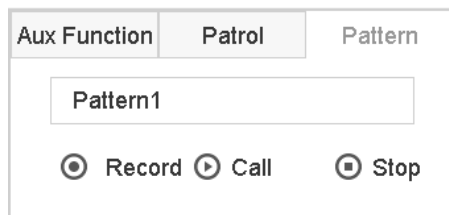


Figure 3.15 Pattern Configuration

3. Select the pattern No. in the text field.
4. Set the pattern.
 - a. Click **Record** to start recording.
 - b. Click corresponding buttons on the control panel to move the PTZ camera.
 - c. Click **Stop** to stop recording.

The movement of the PTZ is recorded as the pattern.


5. Repeat steps 3-4 to set more patterns.

3.4.2.6 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.
The PTZ control panel displays on the right of the interface.
2. Click **Pattern** to configure pattern.

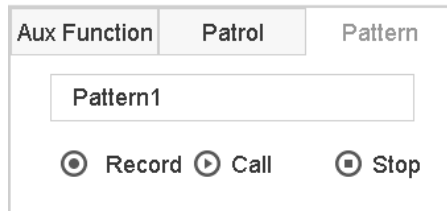


Figure 3.16 Pattern Configuration

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

3.4.2.7 Set Linear Scan Limits

Before you start:

Please make sure the connected IP camera supports the PTZ function, and is properly connected.


Purpose:

The linear scan can be enabled to trigger the scan in the horizontal direction in the predefined range.



This function is supported by some certain models.

Steps

1. Click  on the quick settings toolbar in the live view interface.
The PTZ control panel displays on the right of the interface.
2. Click the directional buttons to wheel the camera to the location where you want to set the limit, and click **Left Limit** or **Right Limit** to link the location to the corresponding limit.




The speed dome starts linear scan from the left limit to the right limit, and you must set the left limit on the left side of the right limit, as well the angle from the left limit to the right limit should be no more than 180°.

3.4.2.8 Call Linear Scan

Purpose:

Follow the procedure to call the linear scan in the predefined scan range.

Steps

1. Click  on the quick settings toolbar in the live view interface.
2. Click **Linear Scan** to start the linear scan and click it again to stop it.
3. (Optional) Click **Restore** to clear the defined left limit and right limit data.

 **NOTE**


Reboot the camera to take the settings into effect.

3.4.2.9 One-touch Park

Purpose:

For some certain model of the speed dome, it can be configured to start a predefined park action (scan, preset, patrol and etc.) automatically after a period of inactivity (park time).

Steps

1. Click  on the quick settings toolbar in the live view interface.
2. Click Park (Quick Patrol), Park (Patrol 1) or Park (Preset 1) to activate the park action.

Park (Quick Patrol): The dome starts patrol from the predefined preset 1 to preset 32 in order after the park time. The undefined preset will be skipped.

Park (Patrol 1): The dome starts moving according to the predefined patrol 1 path after the park time.

Park (Preset 1): The dome moves to the predefined preset 1 location after the park time.

The park time can only be set via the speed dome configuration interface. The value is 5s by default.


3. Click Stop Park (Quick Patrol), Stop Park (Patrol 1) or Stop Park (Preset 1) to inactivate it.

3.4.3 Auxiliary Functions

Purpose:

You can operate the auxiliary functions including light, wiper, and center on the PTZ control panel.

Steps

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

Click **Aux Function**.

Click the icons to operate the aux functions. See the table for the description of the icons.

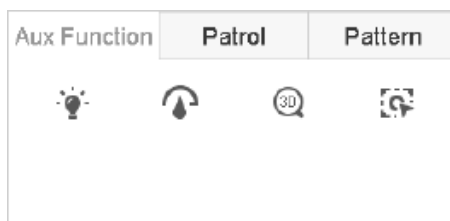





Figure 3.17 Aux Function Configuration

Description of Aux Functions Icons

Icon	Description
	Light on/off
	Wiper on/off
	Center

4 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.

4.1 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.

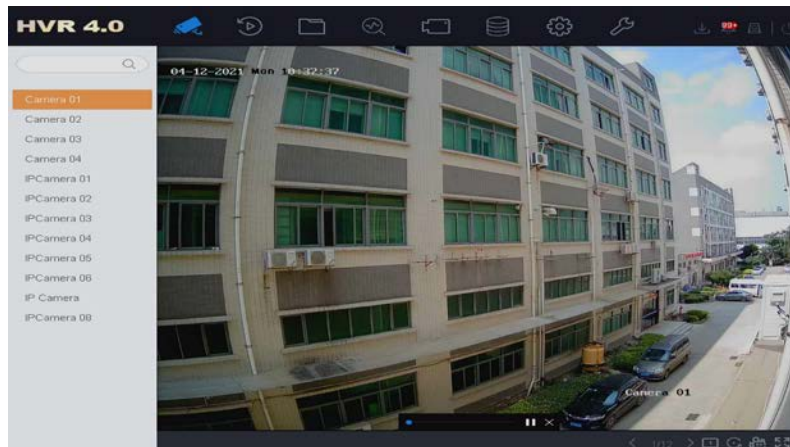



Figure 4.1 Playback Interface

4.2 Play 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 Chapter [4.10 Playback Operations](#).

- Click the channel(s) to execute simultaneous playback of multiple channels.



Figure 4.2 Playback Interface



Figure 4.3 Toolbar of Playback

4.3 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 4.4 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

- 1 Click  the icon.
- 2 Click on the image to specify the start point and end point of the line.

2) Intrusion Detection

- 1 Click  the icon.
- 2 Specify 4 points to set a quadrilateral region for intrusion detection. Only one region can be set.

3) Motion Detection

- 1 Click the  icon
- 2 Hold the mouse on the image to draw the detection area manually.
- 3 Click Search  to search the matched video and start to play it.

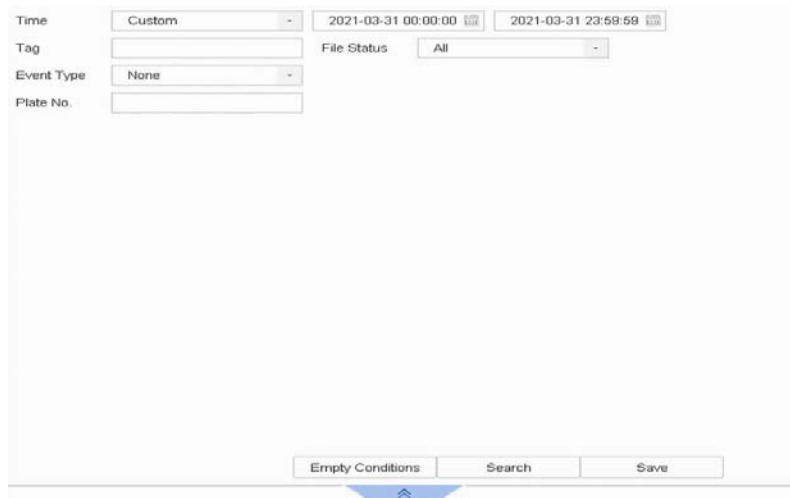
4.4 Play Custom Searched Files

Purpose:

You can play the files by custom search with different conditions.

Steps

1. Go to Playback.
2. Select a camera or cameras from the list.
3. Click **Custom Search** on the left bottom to enter the **Search Condition** interface.
4. Enter the search conditions for the files, e.g., time, file status, event type, etc.



The screenshot shows a 'Custom Search' interface with the following elements:

- Time:** A dropdown menu set to 'Custom'.
- Tag:** An empty text input field.
- Event Type:** A dropdown menu set to 'None'.
- Plate No.:** An empty text input field.
- Date Range:** Two date and time selectors: '2021-03-31 00:00:00' and '2021-03-31 23:59:59'.
- File Status:** A dropdown menu set to 'All'.
- Buttons:** 'Empty Conditions', 'Search', and 'Save' buttons at the bottom.

Figure 4.5 Custom Search

- 5 Click Search.

Index	Channel	Start/End Time	File Type	View	Lock
1	A1	31-03-2021 08:42:04~31-03-2021 08:46:41	Video		
2	A1	31-03-2021 08:46:35~31-03-2021 09:21:44	Video		
3	A1	31-03-2021 09:28:23~31-03-2021 09:57:40	Video		

Total: 28 P: 1/8

Figure 4.6 Custom Searched Video Files

- 6 On the search results interface, select a file and click to start playing the video.
- 7 **Export Playback Files.** [See 5.1.2 Export File](#)

You can click to return to search interface.

4.5 Play Tag Files

Purpose:

Video tag allows you to record related information like people and location of a certain time point during playback. You can use video tag(s) to search for video files and position time point.

Before playing back by tag:

Add Tag Files

Steps

1. Go to Playback.
2. Search and play back the video file(s).
3. Click to add the tag.
4. Edit the tag information.
5. Click **OK**.



NOTE

Max. 64 tags can be added to a single video file.

Edit Tag Files

Steps

1. Go to Playback.
2. Click **Tag**.

The available tags are white marked and displayed in the time bar.

3. Point the white marked tag in the time bar to access the tag information.

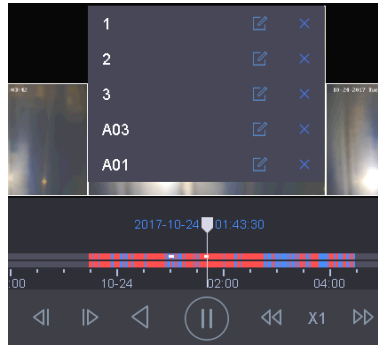


Figure 4.7 Edit Tag Files

4. Click  to edit the tag name.
5. Click **OK**.

Play Tag Files

Steps

1. Go to Playback.
2. Click **Custom Search** on the left bottom to enter the Search Condition interface.
3. Enter the search conditions for the tag files, including the time and the tag keyword.

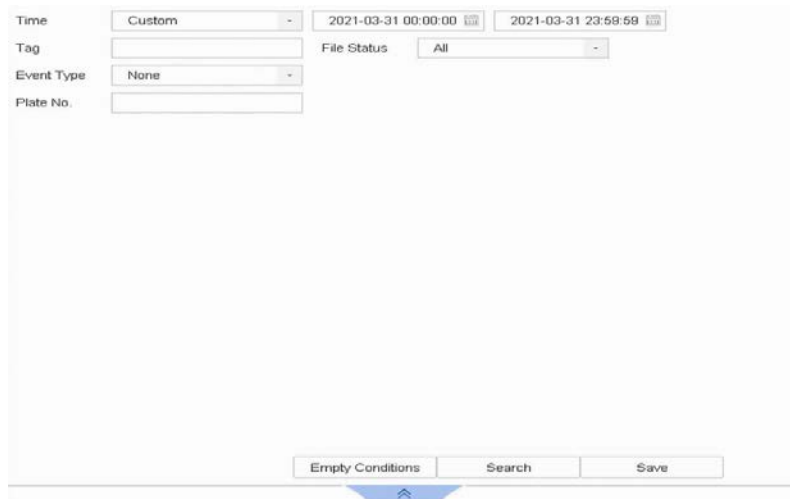


Figure 4.8 Tag Search

4. Click Search.

The screenshot shows a search results interface with a table of video files. At the top, there are tabs for 'All', 'Video', and 'Picture', and an 'Export' button. Below the tabs, the search criteria are 'D2 26-03-2021 15:11:00 ~ 26-03-2021 18:15:47'. The table has columns for Index, Channel, Start/End Time, File Type, View, and Lock. There are four rows of video files, all of type 'Video' from channel 'D2'. At the bottom, there is a pagination control showing 'Total: 4 P: 1/1' and a 'Go' button.

Index	Channel	Start/End Time	File Type	View	Lock
1	D2	26-03-2021 15:11:13~26-03-2021 15:17:48	Video	▶	🔒
2	D2	26-03-2021 15:18:42~26-03-2021 15:18:55	Video	▶	🔒
3	D2	26-03-2021 15:19:40~26-03-2021 15:20:04	Video	▶	🔒
4	D2	26-03-2021 15:20:48~26-03-2021 16:15:42	Video	▶	🔒

Figure 4.9 Searched Tag Files

5. On the search results interface, select a tag file and click to start playing the video.

6. **Export Playback Files.** [See 5.1.2 Export File](#)

You can click  to return to search interface.

4.6 Play Event Files

Purpose:

Play back video files on one or several channels searched by event type (e.g., alarm input, motion detection, line crossing detection, face detection, vehicle detection, etc.).




Steps

1. Go to **Playback..**
2. Click **Custom Search** on the left bottom to enter the Search Condition interface.
3. Enter the search conditions for the event files, e.g., time, event type, file status, vehicle information (for vehicle detection event), etc.
4. Click Search.
5. On the search results interface, select an event video file/picture file and double click to start playing the video.

This screenshot is identical to the one in Figure 4.9, showing the search results interface with a table of video files. The search criteria are 'D2 26-03-2021 15:11:00 ~ 26-03-2021 18:15:47'. The table has columns for Index, Channel, Start/End Time, File Type, View, and Lock. There are four rows of video files, all of type 'Video' from channel 'D2'. At the bottom, there is a pagination control showing 'Total: 4 P: 1/1' and a 'Go' button.

Index	Channel	Start/End Time	File Type	View	Lock
1	D2	26-03-2021 15:11:13~26-03-2021 15:17:48	Video	▶	🔒
2	D2	26-03-2021 15:18:42~26-03-2021 15:18:55	Video	▶	🔒
3	D2	26-03-2021 15:19:40~26-03-2021 15:20:04	Video	▶	🔒
4	D2	26-03-2021 15:20:48~26-03-2021 16:15:42	Video	▶	🔒

Figure 4.10 Event Files


- You can click  or  button to play 30s backward or forward.
 - Export Playback Files.** [See 5.1.2 Export File](#)
- You can click  to return to search interface.

4.7 Play by Sub-periods

Purpose:

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

Steps

- Go to Playback.
- Select  icon at the left bottom corner to enter the sub-period playing mode.
- Select a camera.
- Set the start time and end time for searching video.
- 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.

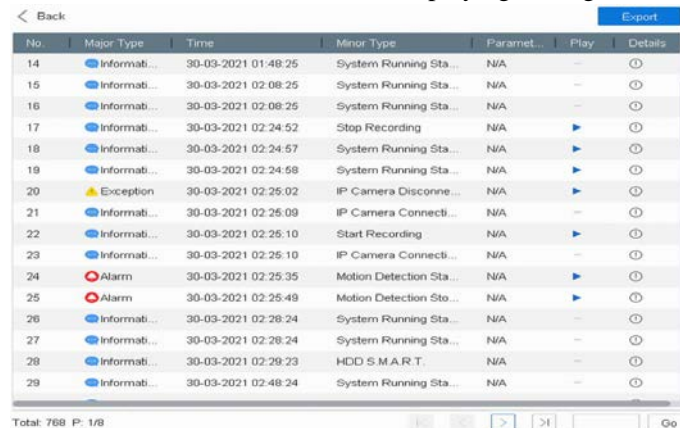
4.8 Play Log Files

Purpose:

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

Steps

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



No.	Major Type	Time	Minor Type	Paramet...	Play	Details
14	Informati...	30-03-2021 01:48:25	System Running Sta...	N/A	▶	ⓘ
15	Informati...	30-03-2021 02:08:25	System Running Sta...	N/A	▶	ⓘ
16	Informati...	30-03-2021 02:08:25	System Running Sta...	N/A	▶	ⓘ
17	Informati...	30-03-2021 02:24:52	Stop Recording	N/A	▶	ⓘ
18	Informati...	30-03-2021 02:24:57	System Running Sta...	N/A	▶	ⓘ
19	Informati...	30-03-2021 02:24:58	System Running Sta...	N/A	▶	ⓘ
20	Exception	30-03-2021 02:25:02	IP Camera Disconn...	N/A	▶	ⓘ
21	Informati...	30-03-2021 02:25:09	IP Camera Connect...	N/A	▶	ⓘ
22	Informati...	30-03-2021 02:25:10	Start Recording	N/A	▶	ⓘ
23	Informati...	30-03-2021 02:25:10	IP Camera Connect...	N/A	▶	ⓘ
24	Alarm	30-03-2021 02:25:35	Motion Detection Sta...	N/A	▶	ⓘ
25	Alarm	30-03-2021 02:25:49	Motion Detection Sta...	N/A	▶	ⓘ
26	Informati...	30-03-2021 02:28:24	System Running Sta...	N/A	▶	ⓘ
27	Informati...	30-03-2021 02:28:24	System Running Sta...	N/A	▶	ⓘ
28	Informati...	30-03-2021 02:29:23	HDD S.M.A.R.T.	N/A	▶	ⓘ
29	Informati...	30-03-2021 02:48:24	System Running Sta...	N/A	▶	ⓘ

Figure 4.11 System Log Search Interface

4.9 Play External File



Purpose:

You can play files from the external storage devices.

Before You Start:

Connect the storage device with the video files to your device.

Steps


- 1 Go to Playback.
- 2 Click  the icon at the left bottom corner.
- 3 Select and click the  button or double click to play the file.

4.10 Playback Operations

4.10.1 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 4.12 Play Strategy

4.10.2 Edit Video Clips

You can take video clips during the playback and export the clips.

In the video playback mode, Click  to start video clipping operation.



: Set the start time and end time of the video clipping.



: Export the video clips to the local storage device.

4.10.3 Thumbnails View

With the thumbnails view on the playback interface, you can conveniently locate the required video files on the time bar.

In the video playback mode, move the mouse to the time bar to get the preview thumbnails of the video files.



Figure 4.13 Thumbnails View

You can select and click on a required thumbnail to enter the full-screen playback.


4.10.4 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.

4.10.5 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 to 16X).



Figure 4.14 Digital Zoom

5 File Management

Click  to start instant File Management

5.1 Search and Export All Files

5.1.1 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.

Time: Custom | 2021-03-30 00:00:00 | 2021-03-30 23:59:59
Camera: [All] Camera
Tag: | File Status: All
Event Type: None
Plate No.:
Empty Conditions | Search | Save

Figure 5.1 Search All Files1

5.1.2 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 [5.1.1 Search Files](#).
2. Click **Export** to export the selected file(s) to a backup device. You can click **Select All** to select all files.

Index	Channel	Start/End Time	File Type	View	Lock
1	D2	26-03-2021 15:14:19~26-03-2021 15:14:48	Video	▶	—
2	D2	26-03-2021 15:38:08~26-03-2021 15:38:12	Video	▶	—
3	D2	26-03-2021 15:41:13~26-03-2021 15:41:20	Video	▶	—
4	D2	26-03-2021 15:41:24~26-03-2021 15:41:30	Video	▶	—
5	D2	26-03-2021 15:43:08~26-03-2021 15:43:14	Video	▶	—
6	D2	26-03-2021 15:43:18~26-03-2021 15:43:24	Video	▶	—
7	D2	26-03-2021 16:02:49~26-03-2021 16:02:55	Video	▶	—
8	D2	26-03-2021 16:02:59~26-03-2021 16:03:05	Video	▶	—
9	D2	26-03-2021 16:04:19~26-03-2021 16:04:25	Video	▶	—
10	D2	26-03-2021 16:04:30~26-03-2021 16:04:36	Video	▶	—
11	D2	26-03-2021 16:11:24~26-03-2021 16:11:45	Video	▶	—
12	D2	26-03-2021 16:13:01~26-03-2021 16:13:12	Video	▶	—
13	D2	26-03-2021 16:13:13~26-03-2021 16:13:57	Video	▶	—
14	D2	26-03-2021 16:14:03~26-03-2021 16:14:26	Video	▶	—
15	D2	26-03-2021 16:14:26~26-03-2021 16:14:32	Video	▶	—

Total: 16 P: 1/1

Figure 5.2 Search All Files2

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

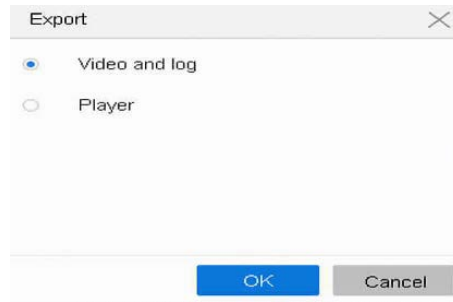


Figure 5.3 Search All Files3

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

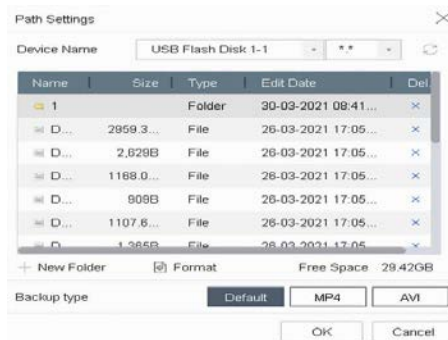

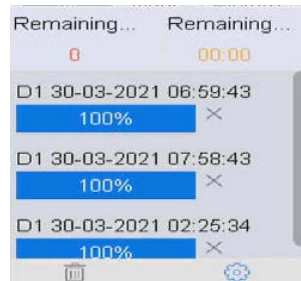



Figure 5.4 Backup Path settings



You can click  to view export progress.



You can click  to return to search interface.

5.2 Search and Export Human Files

5.2.1 Search Files

Purpose:

Specify detailed conditions to search human pictures and videos.

Before you start

Configure human body detection function for the cameras you want to search and export human pictures and videos.

Steps

1. Go to File Management > Human Files.
2. Select **Time** and **Camera** to search.

3. Click **Search** to display results. The matched files are displayed in thumbnail or list.
4. Select **Target Picture** or **Source Picture** in menu bar to display related pictures only.
 - **Target Picture:** Display the search results of people close-up.
 - **Target Picture:** Display the search results of people close-up.



Figure 5.5 Search Human Files

5.2.2 Export Human 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 for the human files to export. For details, see [5.2.1 Search Human Files](#).
2. Click to select files and click **Export**.
3. Select the file to export as **Video and Log** and click **OK**.
4. Click **OK** to export files to backup device. [See 5.1.2 Export File](#)

5.3 Search and Export Vehicle Files

5.3.1 Search Vehicle Files

Purpose:

Specify detailed conditions to search vehicle pictures and videos.

Before you start

Configure vehicle detection function for the cameras you want to search and export vehicle pictures and videos.

Steps

1. Go to File Management > Vehicle Files.
2. Specify detailed conditions, including **Time**, **Camera**, **Plate No.**, and **Area/Country**.
3. Click **Search** to display results. The matched files are displayed in thumbnail or list.
4. Select **Target Picture** or **Source Picture** in menu bar to display related pictures only. Select **Video** or **Picture** to specify the file type.

- **Target Picture:** Display the search results of vehicle close-up.
- **Source Picture:** Display the search results of original picture captured by camera.



Figure 5.6 Search Vehicle Files

5.3.2 Export Vehicle 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 for the vehicle files to export. For details, see [5.3.1 Search Vehicle Files](#).
2. Click to select files and click **Export**.
3. Select the file to export as **Video and Log** and click **OK**.
4. Click **OK** to export files to backup device. [See 5.1.2 Export File](#)

6 Smart Analysis

With the configured VCA detection, the device supports the smart analysis for people counting and heat map.

6.1 People Counting

Purpose:

The Counting is used to calculate the number of people entered or left a certain configured area and form in daily/weekly/monthly/annual reports for analysis.

Steps

1. Go to Smart Analysis > Counting.
2. Select a camera.
3. Select the report type to Daily Report, Weekly Report, Monthly Report, or Annual Report as you desired.

4. Set the **Date** to analyze. Then it will generate the people counting graphic.
5. (Optional) Click **Export** to export the report in excel format.

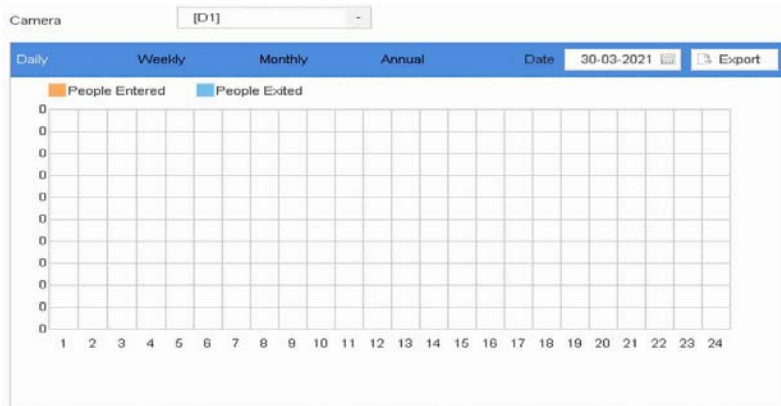


Figure 6.1 People Counting Interface

6.2 Heat Map

Purpose:

Heat Map is a graphical representation of data. The heat map function is used to analyze how many people visited and stayed in a specific area.

Before You Start

The Heat Map function must be supported by the connected IP camera and the corresponding configuration must be set.

Steps

1. Go to Smart Analysis > Heat Map.
2. Select a camera.
3. Select the report type to Daily Report, Weekly Report, Monthly Report, or Annual Report as you desired.
4. Set the **Data** to analyze.
5. Click **Counting**. Then, there will generate the result graphic in different colors.
6. (Optional) Click **Export** to export the statistics report in excel format.

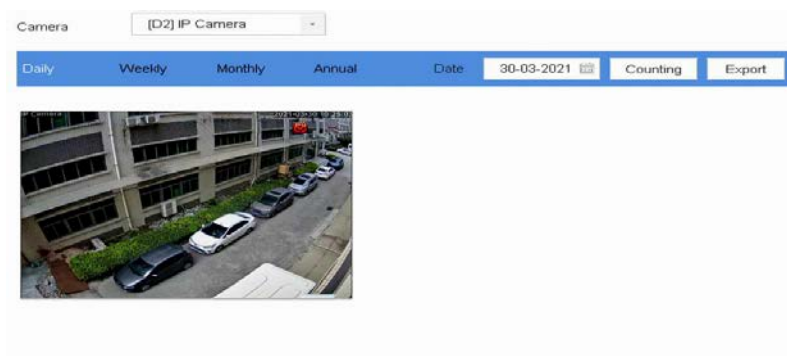


Figure 6.2 Heat Map Interface



As shown in the figure above, red color block (255, 0, 0) indicates the most welcome area, and

blue color block (0, 0, 255) indicates the less-popular area.


7 Camera Management

7.1 Configure Signal Input Channel

Purpose

You can configure the analog and IP signal input types.

Steps

1. Click  on the main menu bar.
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.

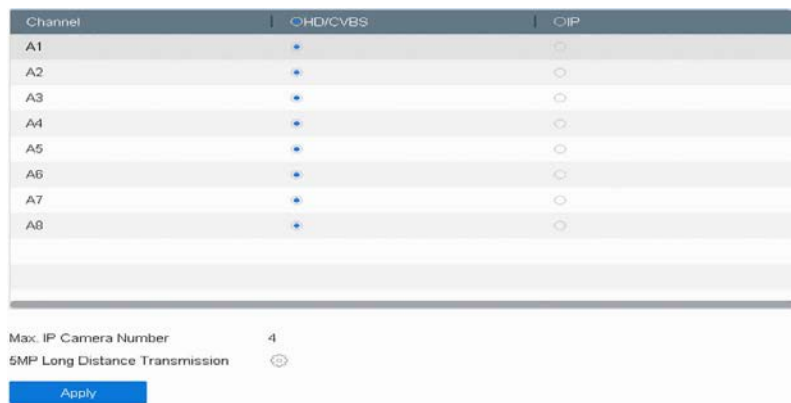


Figure 7.1 Signal Input Status

7.1.1 Configuring 5 MP Long Distance Transmission

You can configure 5 MP long distance transmission on the Signal Input Status interface.

Steps



1. Click  on the main menu bar.
2. Click Camera > Analog.
3. Click  to enter the 5 MP Long Distance Transmission Settings interface.
4. Select channel(s) to enable 5 MP Long Distance Transmission.
5. Click **OK**.
6. Click **Apply** to save the settings.



Figure 7.2 5 MP Long Distance Transmission Settings

7.1.2 Add the IP Cameras

7.1.2.1 Add the IP Camera Manually

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.

Before you start:

Ensure the network connection is valid and correct, and the IP camera to add has already been activated.

Steps



1. Click  on the main menu bar.
2. Click **Camera > IP Camera > Custom Add** on the title bar or click  in the idle channel window to enter the Add IP Camera interface.
3. Enter IP address, protocol, management port, and other information of the IP camera to add.
4. Enter the login user name and password of the IP camera.
5. Click **Add** to finish the adding of the IP camera.
6. (Optional) Click **Continue to Add** to continue to add other IP cameras.



Figure 7.3 Add IP Camera

7.1.2.2 Add the Automatically Searched Online IP Cameras

Steps

1. On the **IP Camera** interface, click the **Number of Unadded Online Device** to expand the panel.
2. Select the automatically searched online devices.
3. Click **Custom Add**.

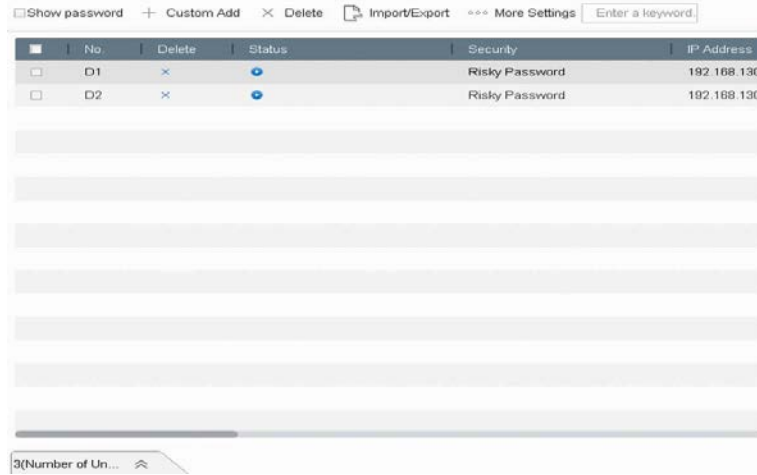


Figure 7.4 Add IP Camera

 **NOTE**


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

7.2 Camera Configure OSD Settings

Purpose:

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

Steps

1. Click  on the main menu bar.
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.

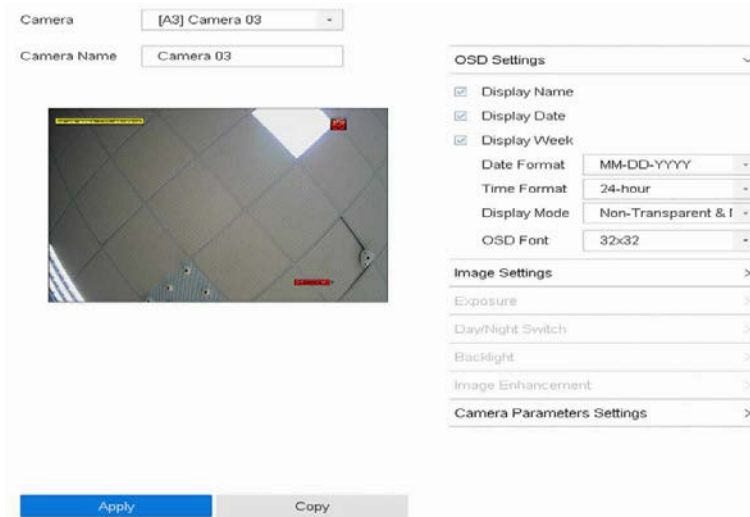



Figure 7.5 OSD Configuration Interface

7.3 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. Click  on the main menu bar.
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.

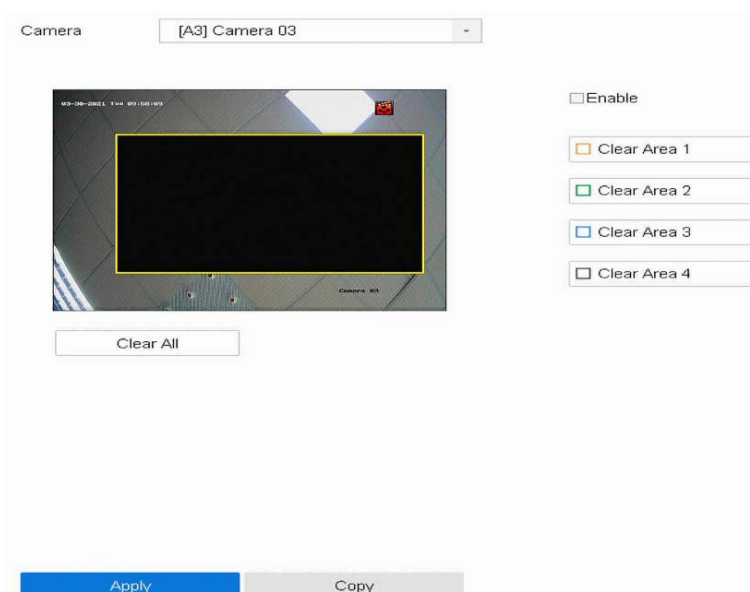


Figure 7.6 Privacy Mask Settings Interface



Up to 4 privacy masks zones can be configured and the size of each area can be adjusted.

Related Operation:


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.

7.4 Configure the Video Parameters

7.4.1 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. Click  on the main menu bar.
2. Click Video Parameters> Main Steam
3. Select the camera from the drop-down list.
4. Click **Apply** to save the settings.

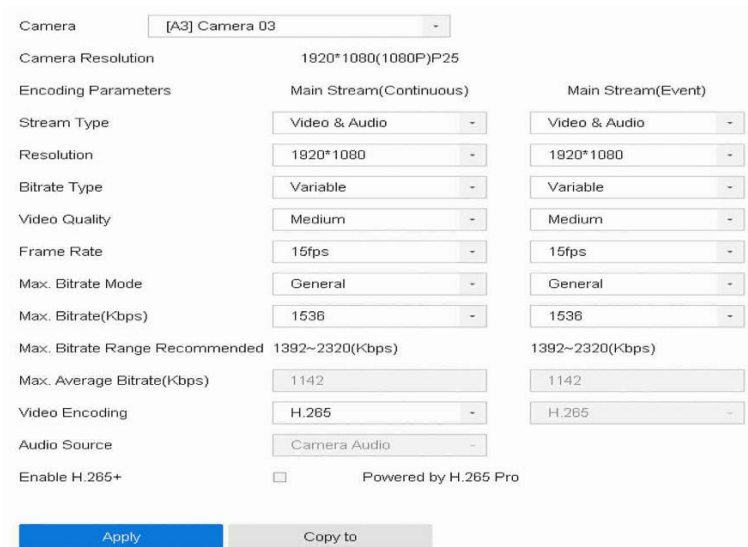


Figure 7.7 Main Stream Settings Interface

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.

Enable H.265+

H.265+ is an optimized encoding technology based on the standard H.265/HEVC compression. With H.265+, the video quality is almost the same as that of H.265/HEVC but with less transmission bandwidth and storage capacity required.

7.4.2 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.

The screenshot displays the 'Sub-Stream Settings Interface' for a camera. The settings are as follows:

Setting	Value
Camera	[A3] Camera 03
Stream Type	Video & Audio
Resolution (Max.: WD1)	960*576(WD1)
Bitrate Type	Constant
Video Quality	Medium
Frame Rate	12fps
Max. Bitrate Mode	Custom(32-3072)
Max. Bitrate (Kbps) (Max.: 3M)	464
Max. Bitrate Range Recommended	589~948(Kbps)
Video Encoding	H.265

At the bottom of the interface, there are two buttons: 'Apply' (highlighted in blue) and 'Copy to' (greyed out).

Figure 7.8 Sub-Stream Settings Interface

8 Storage

Before startup of the device, install and connect the HDD to the device.

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 **Storage > Schedule. Record > Enable Schedule** to enter record schedule settings page.
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.

Camera No. [A1] Camera 01

Enable Schedule

Advanced

Continuous Event Motion Alarm Edit

M | A M & A None

0 2 4 6 8 10 12 14 16 18 20 22 24

Mon	Motion																								1
Tue	Motion																								2
Wed	Motion																								3
Thu	Motion																								4
Fri	Motion																								5
Sat	Motion																								6
Sun	Motion																								7

*Note: Operation is invalid when the number of time segments exceeds the limit (8).

Apply Copy to

Figure 8.1 Record Schedule Settings

Different recording types are configurable.

Continuous: scheduled recording

Event: recording triggered by all event triggered alarm.

Motion: recording triggered by motion detection.

Alarm: recording triggered by alarm.

M/A: recording triggered by either motion detection or alarm.

M&A: recording triggered by motion detection and alarm.

None: No recording video

- ① Drag the mouse on the time bar to set the record schedule.
- ② Click **Advanced** to configure advanced record parameters

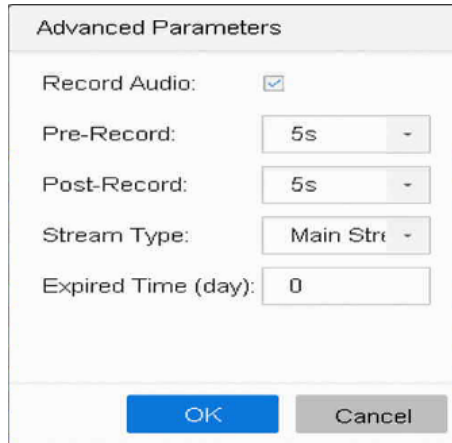


Figure 8.2 Advanced Record Settings

- ❖ **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.

- ③ Click **OK** to save the settings.
- ④ If you want to copy the record schedule settings of the current camera to other cameras, click **Copy to** to copy the settings.
- ⑤ Click **Apply** to save the settings

8.2 Storage Device

8.2.1 Manage Local HDD

8.2.1.1 Configure HDD Group

Multiple HDDs can be managed in groups. Video from specified channels can be recorded onto a particular HDD group through HDD settings.

Steps

1. Go to **Storage > Storage Device**.
2. Select the HDD to set the group.

3. Click  to enter Local HDD Settings interface.

		Total Capacity 1863.03GB		Free Space 1702.00GB				
Label	Capacity	Status	Property	Type	Free Space	Group	Edit	Delete
5	931.52GB	Normal	R/W	Local	871.00GB	2		
7	931.52GB	Normal	R/W	Local	831.00GB	1		

Figure 8.3 Storage Device

Local HDD Settings

HDD No. 5

HDD Property R/W Read-only Redundan...

Group 1 2 3 4 5 6 7 8

9 10 11 12 13 14 15 16

HDD Capacity 931.52GB

Figure 8.4 Local HDD Settings

4. Select a group number for the HDD.
5. Click **OK**.


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

1. Go to **Storage → Storage Mode** .
2. Select group number from the list.
3. Select related camera(s) to save videos and pictures on the HDD group.
4. Click **Apply**.

8.2.1.2 Configure the HDD Property

HDD property can be set as R/W, Read-only, or Redundant.

Steps

1. Go to **Storage → Storage Device** .
2. Click  of desired HDD.
3. Select HDD **Property**.

R/W

HDD supports both read and write.

Read-only

Files in read-only HDD will not be overwritten.

Redundant

Save the videos and pictures not only in the R/W HDD but also in the redundant HDD. It effectively enhances the data safety and reliability. Ensure at least another HDD which is in Read/Write status exists.

4. Click **OK**.

8.2.1.3 Configure the HDD Quota

Each camera can be configured with an allocated quota for storing videos or pictures.

Steps

1. Go to Storage → Storage Mode .
2. Select **Mode** as **Quota**.
3. Select a camera to set quota.
4. Enter the storage capacity in the text fields of **Max. Record Capacity (GB)** and **Max. Picture Capacity (GB)**.
5. Click **Copy to** to copy the quota settings of the current camera to other cameras.
6. Click **Apply**.

8.2.2 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 Storage → Storage Device .
2. Click **Add**.
3. Select **NetHDD** type.
4. Enter **NetHDD IP** address and click **Search** to search the available NetHDD.
5. Select the desired NetHDD.
6. Click **OK**.
7. The added NetHDD will be displayed in the HDD list. Select the newly added NetHDD and click **Init**.

Custom Add	
NetHDD	NetHDD 1
Type	NAS
NetHDD IP	192 . 168 . 130 . 155
NetHDD Directory	/adc/device/1

Search

OK Cancel

Figure 8.5 Add NetHDD

8.3 Storage Mode

8.3.1 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 Storage > 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.

Mode	<input checked="" type="radio"/> Quota <input type="radio"/> Group
Camera	[A1] Camera 01
Used Record Capacity	2048.00MB
Used Picture Capacity	0B
HDD Capacity (GB)	1863
Max. Record Capacity (GB)	0
Max. Picture Capacity (GB)	0
Free Quota Space 1863 GB	
<input type="button" value="Apply"/> <input type="button" value="Copy to"/>	

Figure 8.6 Storage Mode-HDD Quota



NOTE

When the quota capacity is set to **0**, all cameras will use the total capacity of HDD for record and picture capture.

8.3.2 Configure HDD Group

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

Steps

1. Go to Storage> 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.

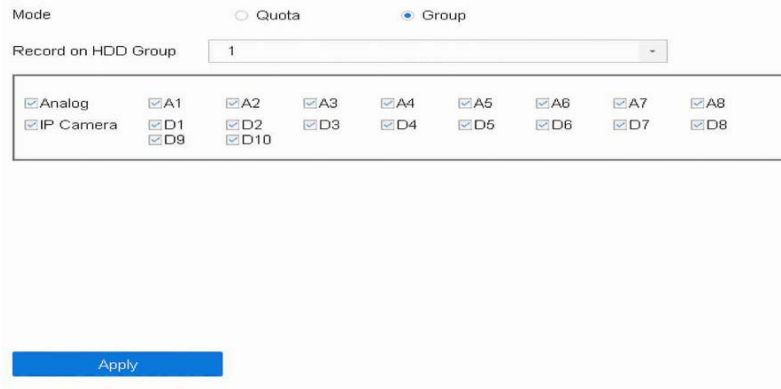


Figure 8.7 Storage Mode-HDD Group



Reboot the device to activate the new storage mode settings.

8.3.3 Advanced

- Go to Menu > Record > Advanced.



Figure 8.8 Advanced Interface

8.3.4 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 > 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 or Drop Box.


Enable Cloud Storage

Cloud Type

Authorization Code

Status **Offline**

Use a QR code scanner app to scan the QR code to log in the selected cloud to get the authorization code.



Camera

Upload Type

Enable Event Upload

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

Figure 8.9 Cloud Storage Interface(1)

4. According to the prompts, you are required to use a mobile browser to scan the QR code to log in the selected cloud to get the authentication code. And then copy the authentication code to **Authentication Code**.
5. Click **Apply** and then back to the main menu.

Note: For OneDrive, it can't return the code directly, you need to get the code from address bar after clicking ok of 'failed to receive auth token'.



Figure 8.10 OneDrive Interface

6. Enter the cloud storage interface again about 20s later. When **Status** shows online, it indicates the successful registration.
7. Input the code into the Authorization Code, then it will turn to be online.


Enable Cloud Storage

Cloud Type

Authorization Code

Status online

Use a QR code scanner app to scan the QR code to log in the selected cloud to get the authorization code.



Camera

Upload Type

Enable Event Upload

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

Figure 8.11 Cloud Storage Interface(2)

8. Tick the Enable Event Upload box.

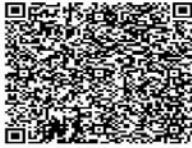
Enable Cloud

Cloud Type

Authorization Code

Status Offline

Use a QR code scanner app to scan the QR code to log in the selected cloud to get the authorization code.



Camera

Upload Type

Enable Event Upload

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

Figure 8.12 Cloud Storage Interface(3)

9. Configure the Record Schedule and choose the Sub stream or Double Stream as stream type in Storage->Schedule-> Record-> Advanced.



Figure 8.13 Record Schedule

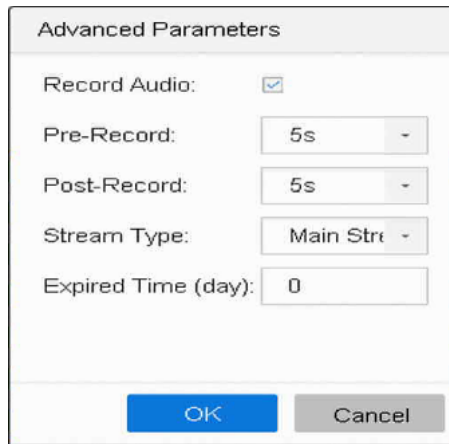


Figure 8.14 Sub stream

- Configure the event and check the checkbox **Upload Captured Pictures To Cloud** in the linkage action of event.(System—Event-Normal Event—Motion Detection—Linkage Action)

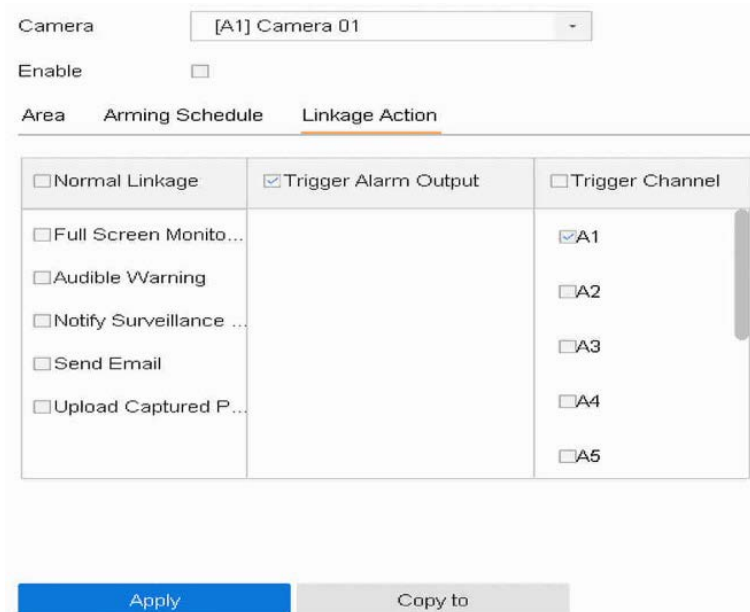


Figure 8.15 Cloud Linkage Action

11. Trigger the event, then videos or pictures will be uploaded to your cloud storage, in the **snapshot** folder.



Figure 8.16 cloud snapshot

9 System Configuration

9.1 Configure General Settings

Purpose:

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

Steps

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



Figure 9.1 General Settings Interface

2. Configure the following settings.

Resolution: 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.

Enhanced IP Mode:

Enabling Enhanced IP Mode will allow you to connect to the maximum number of cameras and make Smart Event unavailable in analog channel.

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

9.2 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.

9.2.1 Add a User

Steps

1. Go to System > User.



No.	User Name	Security	Priority	User's MAC Address	Permission
1	admin	Weak Password	Admin	00:00:00:00:00:00	

Figure 9.2 User Management Interface

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

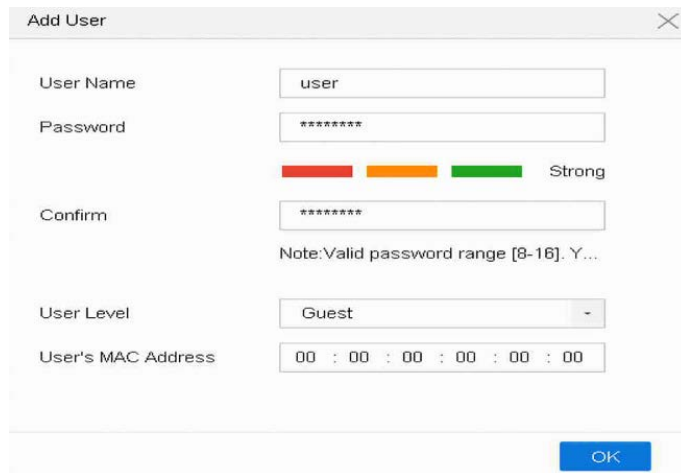


Figure 9.3 Add User

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



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.

Operator: The *Operator* user level has permission of Two-way Audio in Remote Configuration and all operating permission in Camera Configuration by default.

Guest: The Guest user has no permission of Two-way Audio in Remote Configuration and only has the local/remote playback in the Camera Configuration by default.

- **User's MAC Address:** The MAC address of the remote PC which logs onto the device. If it is configured and enabled, it only allows the remote user with this MAC address to access the device.

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.

No.	User Name	Security	Priority	User's MAC Address	Permission
1	admin	Weak Password	Admin	00:00:00:00:00:00	—
2	user	Strong Password	Guest	00:00:00:00:00:00	✔
3	a1	Weak Password	Guest	00:00:00:00:00:00	✔


Figure 9.4 User List

9.2.2 Set Permission for a User

Purpose:

For the added user, you can assign the different permissions, including the local and remote operation for the device.

Steps

1. Go to System > User.
2. Select a user from the list and then click the  button to enter the permission settings interface.

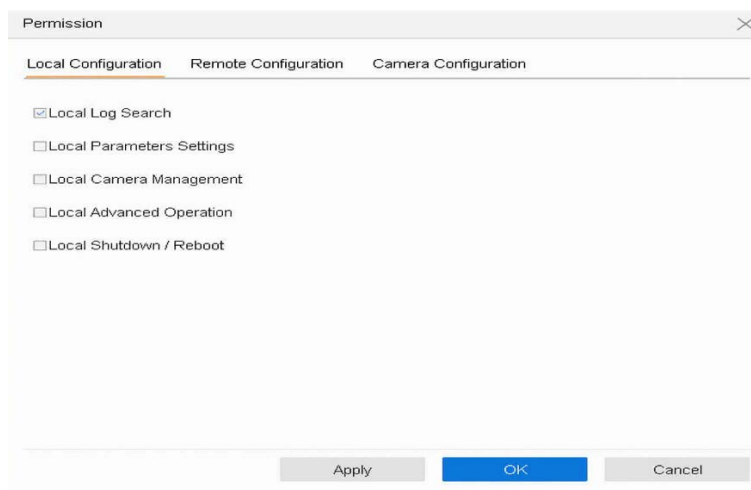


Figure 9.5 User Permission Settings Interface

3. Set the operating permission of Local Configuration, Remote Configuration and Camera Configuration for the user.

9.2.2.1 Local Configuration

Local Log Search: Searching and viewing logs and system information of device.

Local Parameters Settings: Configuring parameters, restoring factory default parameters and importing/exporting configuration files.

Local Camera Management: The adding, deleting and editing of IP cameras.

Local Advanced Operation: Operating HDD management (initializing HDD, setting HDD property), upgrading system firmware, clearing I/O alarm output.

Local Shutdown Reboot: Shutting down or rebooting the device.

9.2.2.2 Remote Configuration

Remote Log Search: Remotely viewing logs that are saved on the device.

Remote Parameters Settings: Remotely configuring parameters, restoring factory default parameters and importing/exporting configuration files.

Remote Camera Management: Remote adding, deleting and editing of the IP cameras.

Remote Serial Port Control: Configuring settings for RS-232 and RS-485 ports.

Remote Video Output Control: Sending remote button control signal.

Two-Way Audio: Realizing two-way radio between the remote client and the device.

Remote Alarm Control: Remotely arming (notify alarm and exception message to the remote client) and controlling the alarm output.

Remote Advanced Operation: Remotely operating HDD management (initializing HDD, setting HDD property), upgrading system firmware, clearing I/O alarm output.

Remote Shutdown/Reboot: Remotely shutting down or rebooting the device.

9.2.2.3 Camera Configuration

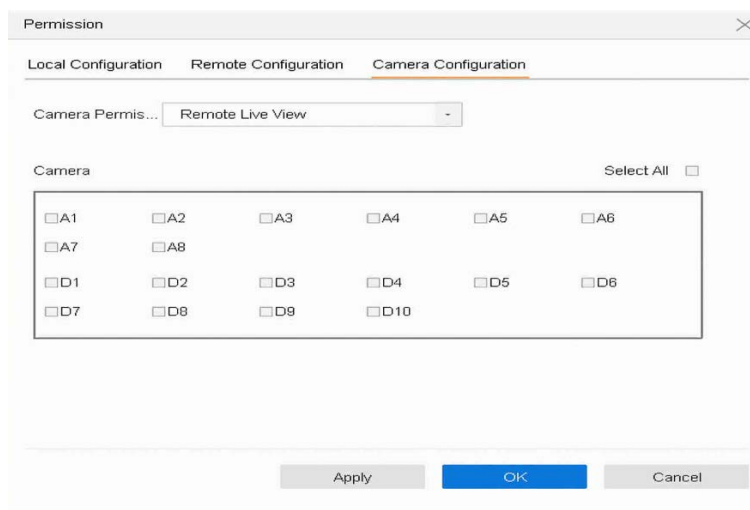


Figure 9.6 Enable Live View Permission

Remote Live View: Remotely viewing live video of the selected camera (s).

Local Manual Operation: Locally starting/stopping manual recording and alarm output of the selected camera (s).

Remote Manual Operation: Remotely starting/stopping manual recording and alarm output of the selected camera (s).

Local Playback: Locally playing back recorded files of the selected camera (s).

Remote Playback: Remotely playing back recorded files of the selected camera (s).

Local PTZ Control: Locally controlling PTZ movement of the selected camera (s).

Remote PTZ Control: Remotely controlling PTZ movement of the selected camera (s).

Local Video Export: Locally exporting recorded files of the selected camera (s).

➤ Click **OK** to save the settings.

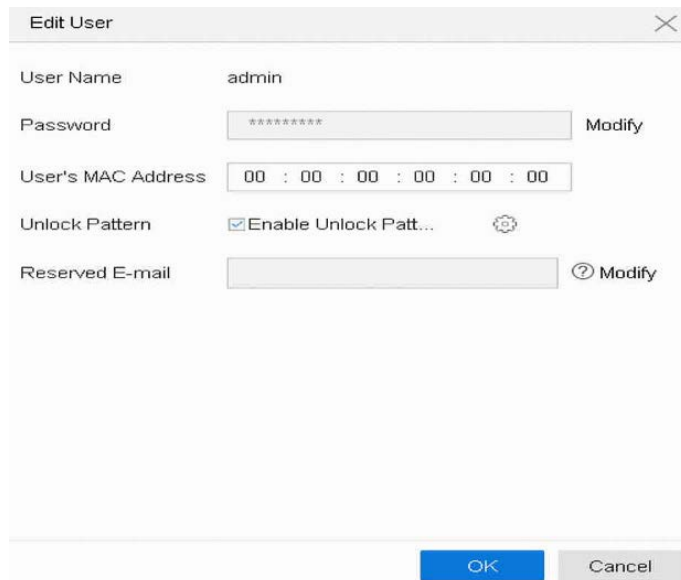
9.2.3 Edit the Admin User

Purpose:

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

Steps

1. Go to System > User.
2. Select the admin user from the list.
3. Click **Modify**.



The screenshot shows a dialog box titled "Edit User" with a close button (X) in the top right corner. The dialog contains the following fields and options:

- User Name:** admin
- Password:** A text box containing "*****" with a "Modify" button to its right.
- User's MAC Address:** A text box containing "00 : 00 : 00 : 00 : 00 : 00".
- Unlock Pattern:** A checkbox labeled "Enable Unlock Patt..." which is checked, followed by a gear icon.
- Reserved E-mail:** A text box with a "? Modify" button to its right.

At the bottom of the dialog, there are two buttons: "OK" (highlighted in blue) and "Cancel".

Figure 9.7 Edit Admin User

4. Edit the admin user information as demand, including the new admin password (strong password is required), and MAC address.
5. Edit the unlock pattern for the admin user account.
 - Check **Enable Unlock Pattern** to enable the use of unlock pattern when logging in to the device.
 - Use the mouse to draw a pattern among the 9 dots on the screen, and release the mouse when the pattern is done.
6. Configure security question for password resetting.
7. Configure reserved email for password resetting
8. Click **OK** to save the settings.

9.2.4 Set Local Live View Permission

Steps

1. Go to System > User.
2. Select Live View Permission on Lock Screen
3. Select cameras to live view.
4. Click **OK**.

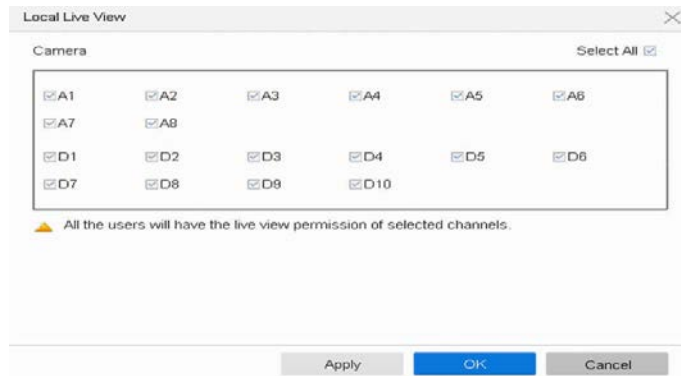


Figure 9.8 Enable Live View Permission

9.2.5 Delete a User

Purpose:

The admin user account has the permission to delete the operator/guest user account.

Steps

1. Go to System > User.
2. Select a user from the list.
3. Click **Delete** to delete the selected user account.

9.3 Network Settings

9.3.1 Configure TCP/IP Settings

Purpose

TCP/IP settings must be properly configured before operating the device over network.

9.3.1.1 Configure TCP/IP

Steps

1. Go to System > Network > TCP/IP.
2. Select Net-Fault Tolerance or Multi-Address Mode under Working Mode..

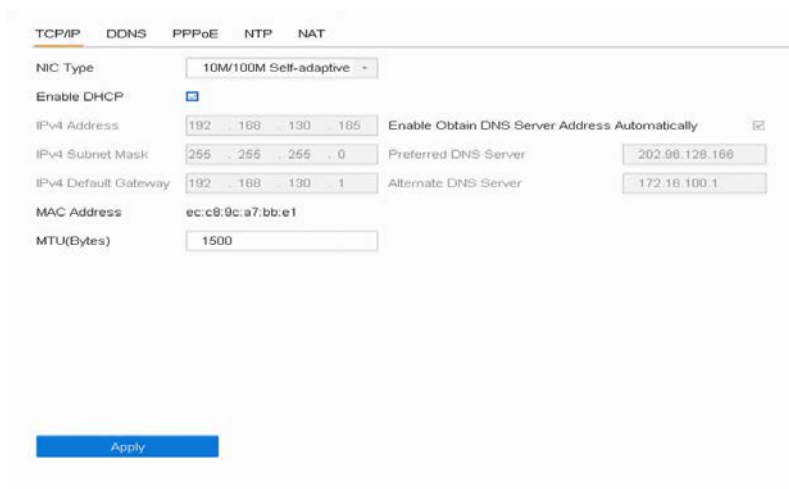


Figure 9.9 TCP/IP Settings

Net-Fault Tolerance: The two NIC cards use the same IP address, and you can select the main NIC to LAN1 or LAN2. By this way, in case of one NIC card failure, the device will automatically enable the other standby NIC card so as to ensure the normal running of the whole system.

Load Balance: By using the same IP address and two NIC cards share the load of the total bandwidth, which enables the system to provide two Gigabit network capacity.

Multi-address Mode: The parameters of the two NIC cards can be configured independently. You can select LAN1 or LAN2 under Select NIC for parameter settings. You can select one NIC card as default route. And then the system is connecting with the extranet the data will be forwarded through the default route.

3. Configure other IP settings as needed.
 - Check **Enable DHCP** to obtain IP settings automatically if a DHCP server is available in the network.
 - Valid range of MTU value is 500 to 1500.
4. Click **Apply**.

9.3.1.2 Configure DDNS

Purpose

You can set Dynamic DNS service for network access. Different DDNS modes are available:

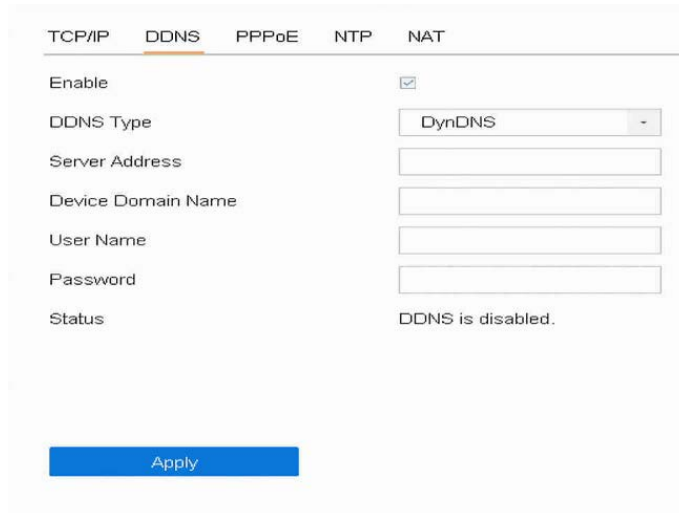
DynDNS, PeanutHull, and NO-IP.

Before You Start

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

Steps

1. Go to System > Network > TCP/IP > 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**.

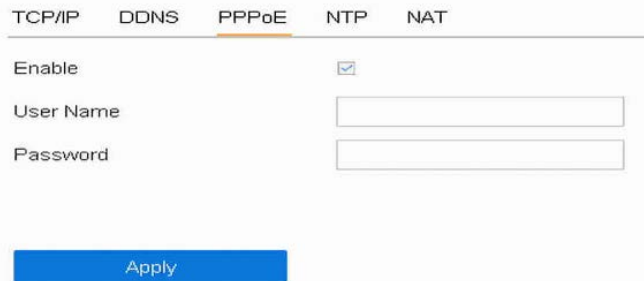


The screenshot shows the DDNS configuration page. At the top, there are tabs for TCP/IP, DDNS (which is selected and highlighted in orange), PPPoE, NTP, and NAT. Below the tabs, there is a form with the following fields: 'Enable' with a checked checkbox, 'DDNS Type' with a dropdown menu set to 'DynDNS', 'Server Address', 'Device Domain Name', 'User Name', and 'Password', each with an empty text input field. At the bottom, there is a blue 'Apply' button. The status at the bottom right of the form reads 'DDNS is disabled.'

Figure 9.10 DDNS Settings

9.3.1.2.1.1 Configure PPPoE

- If the device is connected to Internet through PPPoE, you need to configure user name and password accordingly under **System > Network > TCP/IP > PPPoE**.
- Contact your Internet service provider for details about PPPoE service.



The screenshot shows the PPPoE configuration page. At the top, there are tabs for TCP/IP, DDNS, PPPoE (which is selected and highlighted in orange), NTP, and NAT. Below the tabs, there is a form with the following fields: 'Enable' with a checked checkbox, 'User Name', and 'Password', each with an empty text input field. At the bottom, there is a blue 'Apply' button.

Figure 9.11 PPPoE Settings

9.3.1.2.1.2 Configure NTP

Purpose

Connection to a network time protocol (NTP) server can be configured on your device to ensure the accuracy of system date and time.

Steps

1. Go to System > Network > TCP/IP > NTP.
2. Check **Enable**.
3. Configure NTP settings as need.

TCP/IP DDNS PPPoE **NTP** NAT

Enable

Interval (min)

NTP Server

NTP Port

Figure 9.12 NTP Settings

Interval (min): Time interval between two time synchronizations with NTP server.

NTP Server: IP address of the NTP server.

NTP Port: Port of the NTP server.

4. Click **Apply**.

9.3.1.2.1.3 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 **System > Network > TCP/IP > 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.

TCP/IP DDNS PPPoE NTP **NAT**

Enable

Mapping Type

Port Type	Edit	External Port	External IP Address	Port	UPnP Status
HTTP Port	<input type="button" value="Edit"/>	80	0.0.0.0	80	Inactive
RTSP Port	<input type="button" value="Edit"/>	554	0.0.0.0	554	Inactive
Server Port	<input type="button" value="Edit"/>	8000	0.0.0.0	8000	Inactive
HTTPS Port	<input type="button" value="Edit"/>	443	0.0.0.0	443	Inactive
Cloud P2P Co...	<input type="button" value="Edit"/>	9010	0.0.0.0	9010	Inactive
Cloud P2P Da...	<input type="button" value="Edit"/>	9020	0.0.0.0	9020	Inactive

Figure 9.13 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.

9.3.2 Configure Advanced Settings

9.3.2.1 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

The device must be connected to a local area network (LAN) that contains an SMTP mail server. The network must be connected to either an intranet or the Internet depending on the location of the e-mail accounts to send notification.

Steps

1. Go to System > Network > Advanced > Email.
2. Configure the following Email settings.

Setting	Value
Enable Server Authentication	<input type="checkbox"/>
User Name	
Password	
SMTP Server	
SMTP Port	25
Enable SSL/TLS	<input type="checkbox"/>
Sender	
Sender's Address	
Select Receivers	Receiver 1
Receiver	
Receiver's Address	
Enable Attached Picture	<input type="checkbox"/>
Interval	2s

Figure 9.14 Email Settings

Enable 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.

Enable Attached Picture: Check to enable the function if you want to send email with attached alarm images. The interval is the time between two adjacent alarm images.

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

9.3.2.2 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 System > Network > Advanced > Platform Access.

The screenshot shows the 'Platform Access' configuration page. It includes a dropdown for 'Access Type' (Guarding Vision), a checked 'Enable' checkbox, a text input for 'Server Addr...' (litedev.sgp.guardingvisic) with a 'Custom' checkbox, an unchecked 'Enable Stream ...' checkbox, a text input for 'Verification Code' (ism111111), and a 'Status' field (Online). Below these is a 'Guarding Vision ...' field (Unlinked) and an 'Unbind' button. Two QR codes are displayed with instructions to scan them via the Guarding Vision app or to download the smartphone app. An 'Apply' button is located at the bottom left.

Figure 9.15 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**.

- (Optional) Check **Custom** and enter the server address as needed. The default server address is dev.guardingvision.com.
- (Optional) Check **Enable Stream Encryption** and verification code will be required for remote access and live view.
- Click **Apply**. After configuration, you can access and manage the DVR by your mobile phone

9.3.2.3 Configure Ports

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

- Go to **System > Network > Advanced > More Settings** and configure port settings as needed.

Email	Platform Access	More Settings
Alarm Host IP		<input type="text"/>
Alarm Host Port		<input type="text" value="0"/>
Server Port		<input type="text" value="8000"/>
HTTP Port		<input type="text" value="80"/>
Multicast IP		<input type="text"/>
RTSP Port		<input type="text" value="554"/>
Output Bandwidth Limit		<input type="checkbox"/>
Output Bandwidth (Mbps)		<input type="text" value="2"/>

Figure 9.16 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.

9.4 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.

9.4.1 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 System > Event > Normal Event > Motion Detection.
2. Select the camera to configure the motion detection.
3. Check **Enable**

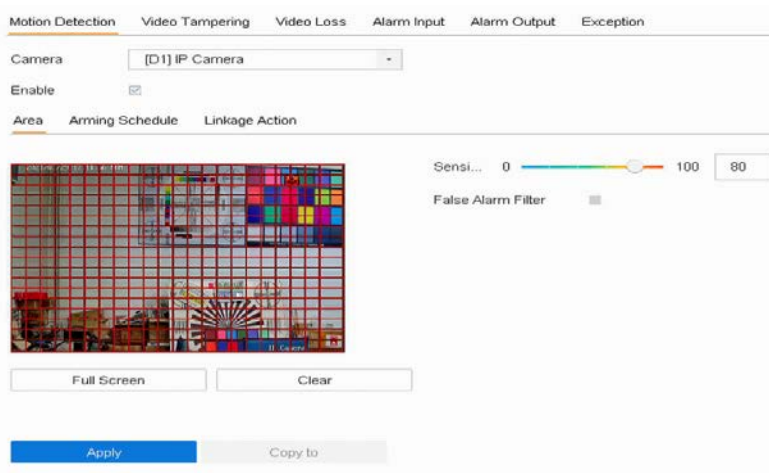


Figure 9.17Set Motion Detection

9.4.1.1 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.

9.4.1.2 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.

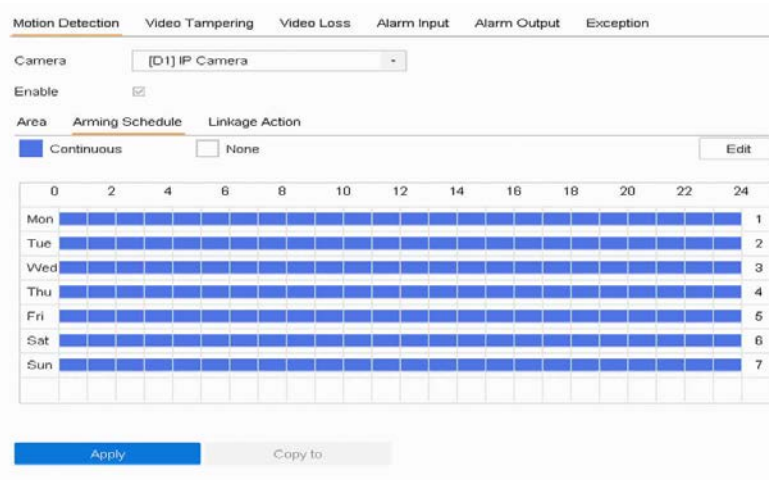


Figure 9.18 Arming Schedule

9.4.1.3 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.

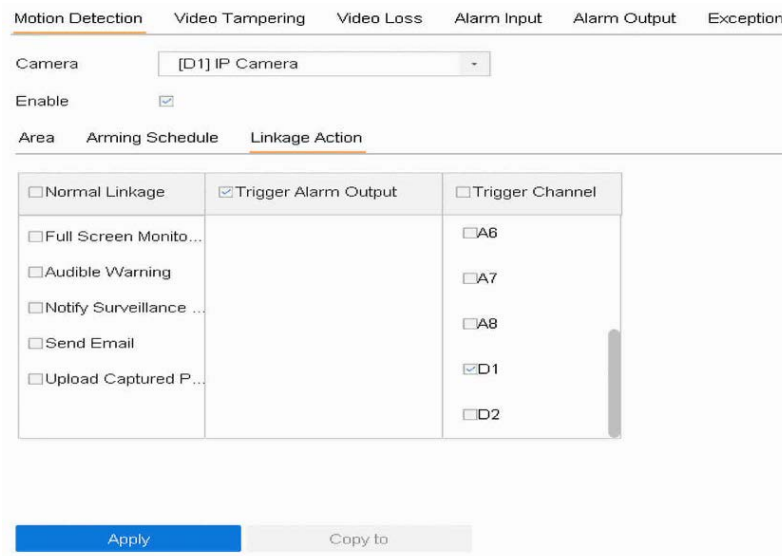


Figure 9.19 Motion Detection-Linking Method

9.4.1.3.1.1 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.

9.4.1.3.1.2 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.

Trigger Alarm Output
 A->1
 A->2
 A->3
 A->4

Figure 9.20 Motion Detection-Trigger Alarm Output

9.4.1.3.1.3 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.

Trigger Channel
 A1
 A2
 A3
 A4
 A5

Figure 9.21 Motion Detection-Alarm Linked Recording

9.4.2 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. Set the arming schedule. Refer to Chapter [9.4.1.2 Configure Arming Schedule](#).
7. Set the linkage actions. Refer to Chapter [9.4.1.3 Configure Arming Linkage Actions](#).

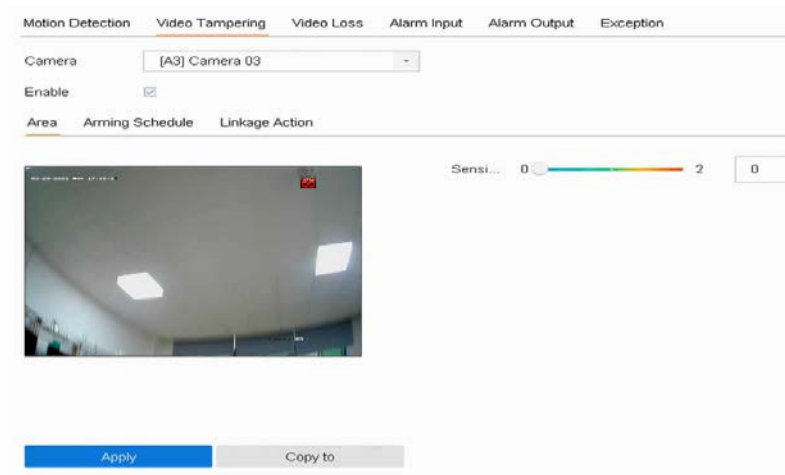


Figure 9.22 Set Video Tampering Setting

9.4.3 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 System> Event>Normal Event>Video Tampering.
2. Select the camera to configure the video tampering detection.
3. Check **Enable**.
4. Set the arming schedule. Refer to Chapter [9.4.1.2 Configure Arming Schedule](#).
5. Set the linkage actions. Refer to Chapter [9.4.1.3 Configure Arming Linkage Actions](#).

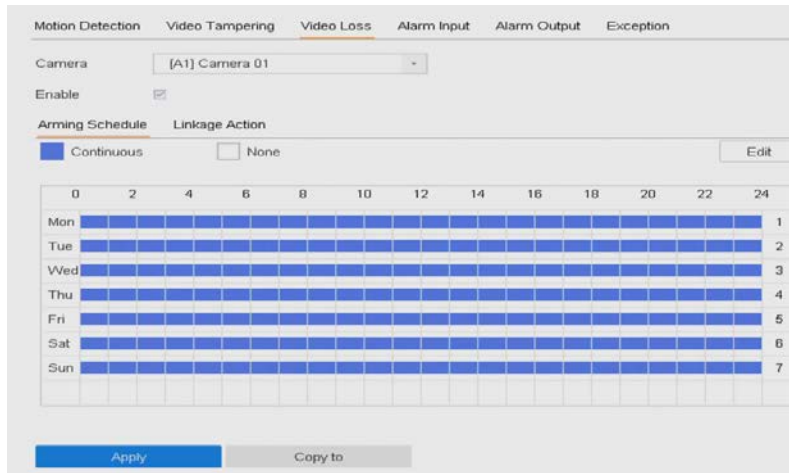



Figure 9.23 Set Video Loss Detection

9.4.4 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>System> 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.

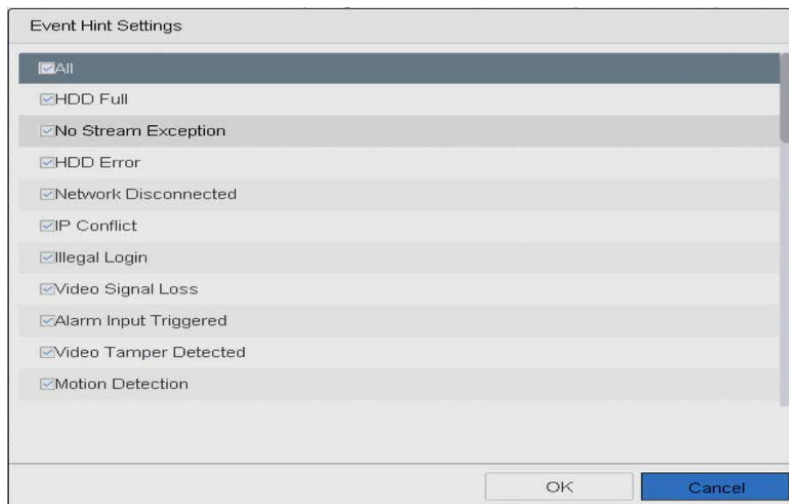


Figure 9.24 Event Hint Settings

5. Select the exception type from the drop-down list to set the linkage actions.
6. Set the normal linkage and alarm output triggering. Refer to [9.4.1.3 Configure Arming Linkage Actions](#).

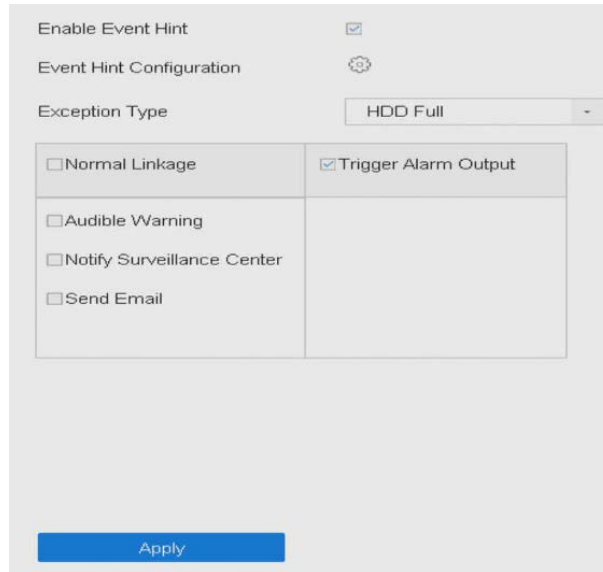


Figure 9.25 Exceptions Handling

9.5 Configure Live View Settings

9.5.1 General Settings

Live View settings can be customized. 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 System → Live View → General .
2. Configure the live view parameters.



Figure 9.23 Live View-General

Video Output Interface

Select the video output to configure.

Live View Mode

Select the display mode for Live View, e.g., 2*2, 1*5, etc.

Dwell Time

The time in seconds to wait between switching of cameras when using auto-switch in Live View.

Enable Audio Output

Enable/disable audio output for the selected video output.

Volume

Adjust the Live View volume, 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 **OK**.

9.5.2 Configure Live View Layout

Steps

1. Go to 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.

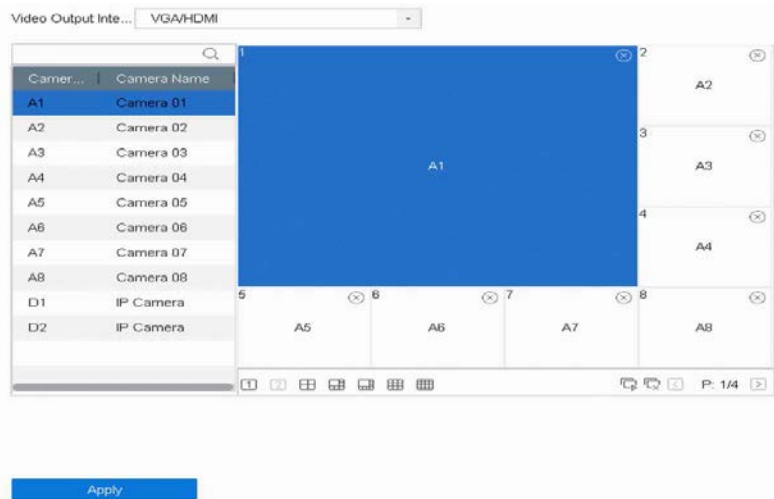




Figure 9.24 Live View Layout

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.

9.5.3 Configure Channel-Zero Encoding

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

Steps

1. Go to System → Live View → Channel-Zero.
2. Check Enable Channel-Zero Encoding.

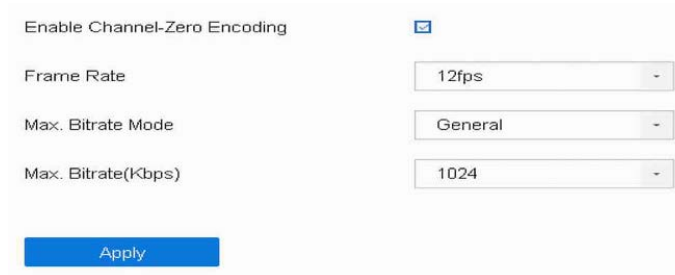


Figure 9.25 Live View- Channel-Zero Encoding


- 3 . Configure **Frame Rate**, **Max. Bitrate Mode**, and **Max. Bitrate**. A higher frame rate and bitrate require higher bandwidth
- 4 . Click **Apply**.

You can view all the channels on one screen via CMS or web browser.

9.6 Configure Holiday Recording

You may want to have different plan for recording on holiday, this function allows you to set the recording schedule on holiday for the year.

Steps

1. Go to System → Holiday .
2. Select a holiday item from the list.
3. Click  to edit the selected holiday.
4. Check Enable.
5. Set Holiday Name, Mode, Start Date, and End Date.
6. Click **OK**.
7. Set the schedule for holiday recording. Refer to **Configure Plan Recording** for details.

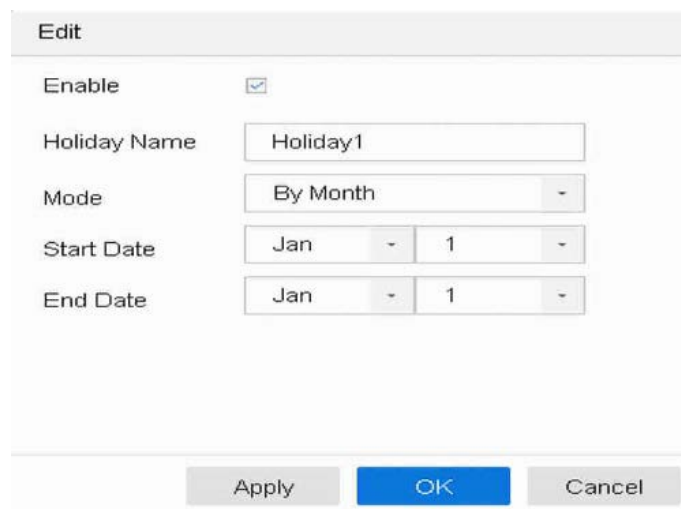


Figure 9.26 Edit Holiday Settings

10 System Management

10.1 Viewing System Information

Steps

1. Go to Menu > Maintenance > System Info.
2. You can click Device Info, Camera, Record, Alarm, Network and HDD to view the system information of the device.

10.2 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.

10.2.1 Search the Log Files

Steps

1. Go to Maintenance > Log Information.
2. Set the log search conditions.

The screenshot shows the Log Search Interface with the following elements:

- Time:** 2021-03-30 00:00:00 - 2021-03-30 23:59:59
- Search:** A blue button to initiate the search.
- Major Type:** A dropdown menu set to 'All'.
- Minor Type:** A checkbox labeled 'Select All'.
- Export All:** A grey button to export the search results.
- Log Entries List:** A scrollable list of log entries, each with a checkbox:
 - Alarm Input
 - Alarm Output
 - Motion Detection Started
 - Motion Detection Stopped
 - Video Tampering Detection Started
 - Video Tampering Detection Stopped
 - Video Quality Diagnostics Alarm Started
 - Video Quality Diagnostics Alarm Stopped
 - Line Crossing Detection Alarm Started
 - Line Crossing Detection Alarm Stopped
 - Intrusion Detection Alarm Started
 - Intrusion Detection Alarm Stopped
 - Audio Loss Exception Alarm Started
 - Audio Loss Exception Alarm Stopped
 - Sudden Change of Sound Intensity Alarm Started
 - Sudden Change of Sound Intensity Alarm Stopped

Figure 10.1 Log Search Interface

3. Click **Search** to start search log files.

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

No.	Major Type	Time	Minor Type	Paramet...	Play	Details
1	Informati...	30-03-2021 00:08:24	System Running Sta...	N/A	--	ⓘ
2	Informati...	30-03-2021 00:08:24	System Running Sta...	N/A	--	ⓘ
3	Informati...	30-03-2021 00:28:24	System Running Sta...	N/A	--	ⓘ
4	Informati...	30-03-2021 00:28:24	System Running Sta...	N/A	--	ⓘ
5	Informati...	30-03-2021 00:29:15	HDD S.M.A.R.T.	N/A	--	ⓘ
6	Informati...	30-03-2021 00:48:24	System Running Sta...	N/A	--	ⓘ
7	Informati...	30-03-2021 00:48:24	System Running Sta...	N/A	--	ⓘ
8	Informati...	30-03-2021 01:08:24	System Running Sta...	N/A	--	ⓘ
9	Informati...	30-03-2021 01:08:24	System Running Sta...	N/A	--	ⓘ
10	Informati...	30-03-2021 01:28:24	System Running Sta...	N/A	--	ⓘ
11	Informati...	30-03-2021 01:28:24	System Running Sta...	N/A	--	ⓘ
12	Informati...	30-03-2021 01:29:18	HDD S.M.A.R.T.	N/A	--	ⓘ
13	Informati...	30-03-2021 01:48:25	System Running Sta...	N/A	--	ⓘ
14	Informati...	30-03-2021 01:48:25	System Running Sta...	N/A	--	ⓘ
15	Informati...	30-03-2021 02:08:25	System Running Sta...	N/A	--	ⓘ
16	Informati...	30-03-2021 02:08:25	System Running Sta...	N/A	--	ⓘ

Figure 10.2 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.

10.2.2 Export the Log Files

Connect a storage device to your device.

Steps

1. Search the log files. Refer to Chapter 10.2.1 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.

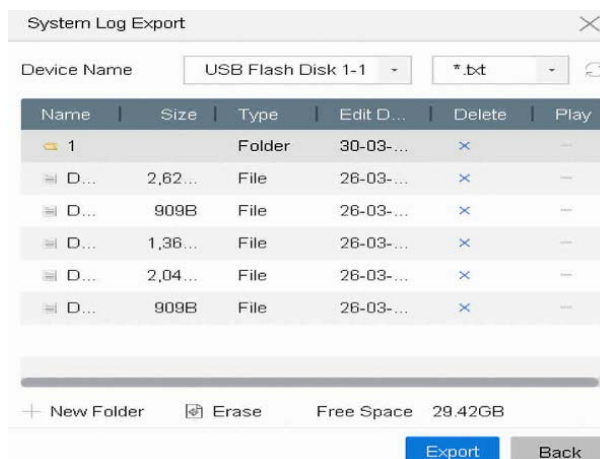


Figure 10.3 Export Log Files

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.

10.3 Import/Export Device 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.

Before You Start

Connect a storage device to your device. To import the configuration file, the storage device must contain the file.

Steps

1. Go to Maintenance → Import/Export .

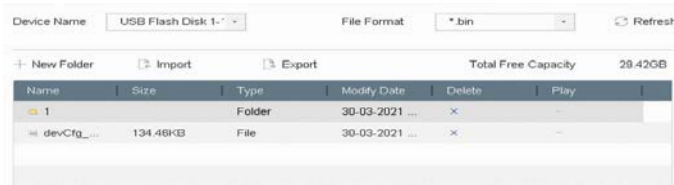


Figure 10.4 Import/Export Config File

2. Click the **IP Camera Import/Export** tab, and the content of detected plugged external device appears.
3. Export or import the IP camera configuration files.
 - Click **Export** to export configuration files to the selected local backup device.
 - To import a configuration file, select the file from the selected backup device and click **Import**.

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

10.4 Upgrade System

Your device firmware can be upgraded with a local backup device or remote FTP server.

10.4.1 Upgrade by Local Backup Device

Connect your device to a local storage device that contains the firmware update file.

Steps

1. Go to Maintenance → Upgrade .
2. Click **Local Upgrade** to enter the local upgrade interface.
3. Select the firmware update file from the storage device.
4. Click **Upgrade** to start upgrading.



Figure 10.5 Local Upgrade Interface

After the upgrade is completed, the device will reboot automatically to activate the new firmware.

10.4.2 Upgrade by FTP

Before You Start

Ensure the network connection of the PC (running FTP server) and the device are valid and correct. Run the FTP server on the PC and copy the firmware into the corresponding directory of your PC.

Steps

1. Go to Maintenance → Upgrade .
2. Click **FTP** to enter the local upgrade interface.
3. Enter FTP Server Address.
4. Click **Upgrade** to start upgrading.
5. After the upgrading is complete, reboot the device to activate the new firmware.

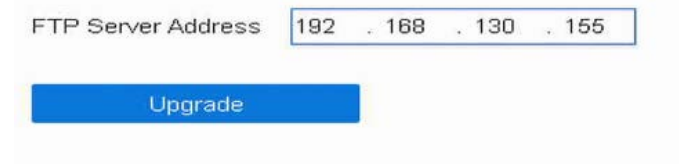


Figure 10.6 FTP Upgrade Interface

10.4.3 Upgrade by Online Upgrade

After logging the device into guarding vision, the device would periodically check for the latest firmware from guarding vision. If an upgrade firmware is available, the device will notify you when you log in. You can also manually check for the latest firmware.

Before You Start:

Ensure the device has successfully connected to guarding vision, and it requires to install at least one read-write HDD for firmware downloading.

Steps

1. Go to Maintenance > Upgrade > Online Upgrade.
2. Click **Check Upgrade** to manually check and download the latest firmware from guarding vision.



Figure 10.7 Online Upgrade Interface

The device will automatically check for the latest firmware every 24 hours. If it detects available upgrade firmware, the device will notify you when you log in.

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

4. Click Upgrade Now.

10.4.4 Upgrade Camera

You can upgrade multiple connected analog cameras supporting Turbo HD or AHD signal simultaneously with DVR.

Steps

1. Go to Maintenance > Upgrade > Camera Upgrade.

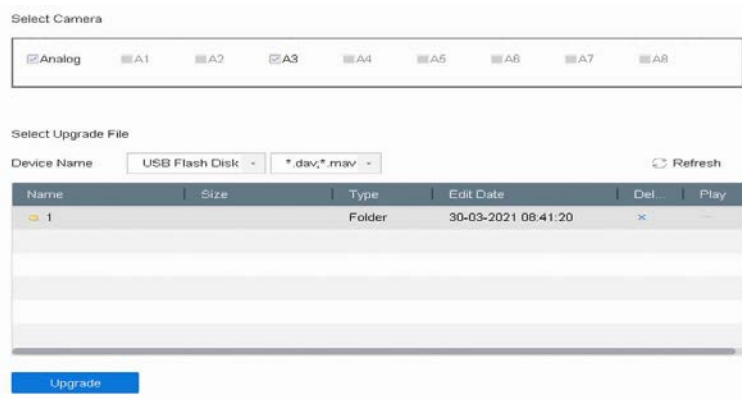


Figure 10.8 Camera Upgrade Interface

2. Check the analog camera(s) for upgrading.

The analog camera must support Turbo HD or AHD signal

3. Select the update file from the backup device.

4. Click **Upgrade** to start upgrading.

10.5 Restore Default Settings

Steps

1. Go to Maintenance → Default .

2. Select the restore type from the following three options.



Figure 10.9 Restore Default Settings

Restore Defaults

Restore all parameters, except the network (including IP address, subnet mask, gateway, MTU, NIC working mode, default route, server port, etc.) and user account parameters, to the factory default settings.

Factory Defaults

Restore all parameters to the factory default settings.

Restore to Inactive

Restore the recorder to inactive status.

The device will reboot automatically after restoring to the default settings.

10.6 Network Detection

10.6.1 Network Traffic Monitoring

Network traffic monitoring is the process of reviewing, analyzing and managing network traffic for any abnormality or process that can affect network performance, availability and/or security.

Steps

1. Go to Maintenance → Network → Traffic .
2. You can view the real-time network traffic status, including MTU (Maximum Transmission Unit), and network throughput.

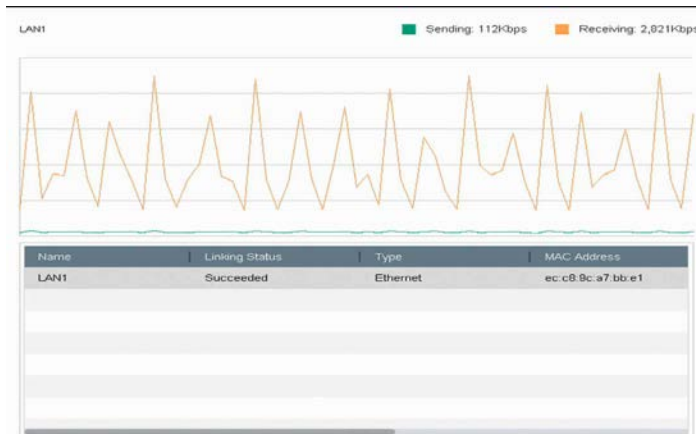


Figure 10.10 Network Traffic

10. 6. 1 Test Network Detection

Before You Start

10.6.1.1 Test Network Delay and Packet Loss

Network delay is caused by slow response of the device when oversized data information is not limited during transmission under certain network protocol, e.g. TCP/IP. Packet loss test is for testing network packet loss rate that is the ratio of lost data packet and total number of transmitted data packet.

Steps

1. Go to Maintenance → Network → Network Detection .
2. Select a network card in Select NIC.
3. Enter the destination IP address in Destination Address.
4. Click Test.

Network Delay, Packet Loss Test

Select NIC:

Destination Address:

Network Packet Export

Device Name:

LAN1	192.168.130.185	1,126Kbps	<input type="button" value="Export"/>
------	-----------------	-----------	---------------------------------------

Figure 10.11 Test Network Delay and Packet Loss

10.6.1.2 Export Network Packet

After the recorder accessing network, you can use USB flash drive to export network packet.

Steps

1. Insert the USB flash drive.
2. Go to **Maintenance** → **Network** → **Network Detection** .
3. Select network card in **Select NIC**.
4. Select the USB flash drive in **Device Name**. You can click **Refresh** if the connected local backup device cannot be displayed.
5. **Optional:** Click **Status** to view the network status.
6. Click **Export**.

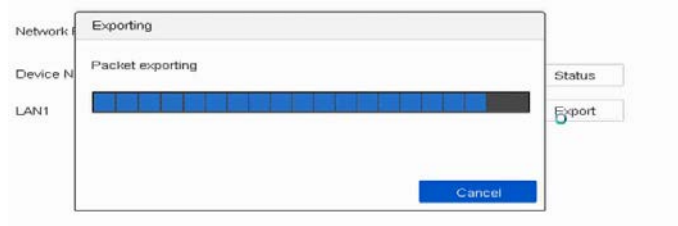


Figure 10.12 Export Network Packet

It will export 1 MB data each time as default.

10.6.1.3 Network Resource Statistics

The remote access, including web browser and client software, will consume output bandwidth. You can view the real-time bandwidth statistics.

Steps

1. Go to **Maintenance** → **Network** → **Network Stat** .
2. View the bandwidth statistics, including **IP Camera**, **Remote Live View**, **Remote Play**, **Net Total Idle**, etc.
3. **Optional:** Click **Refresh** to obtain the latest data.

Type	bandwidth
IP Camera	4,096Kbps
Remote Live View	0bps
Remote Playback	0bps
Net Total Idle	92Mbps

Figure 10.13 Network Resource Statistics

10.7 Storage Device Maintenance

10.7.1 S.M.A.R.T. Detection

HDD detection functions such as the adopting of the S.M.A.R.T. and the Bad Sector Detection techniques. S.M.A.R.T. (Self-Monitoring, Analysis and Reporting Technology) are HDD monitoring systems to detect various reliability indicators in the hopes of anticipating failures.

Steps

1. Go to **Maintenance** → **HDD Operation** → **Bad Sector Detection** .

2. Select the HDD to view its S.M.A.R.T. information list.
3. Select the self-test types as Short Test, Expanded Test, or the Conveyance Test.
4. Click Self-Test to start the S.M.A.R.T. HDD self-evaluation.

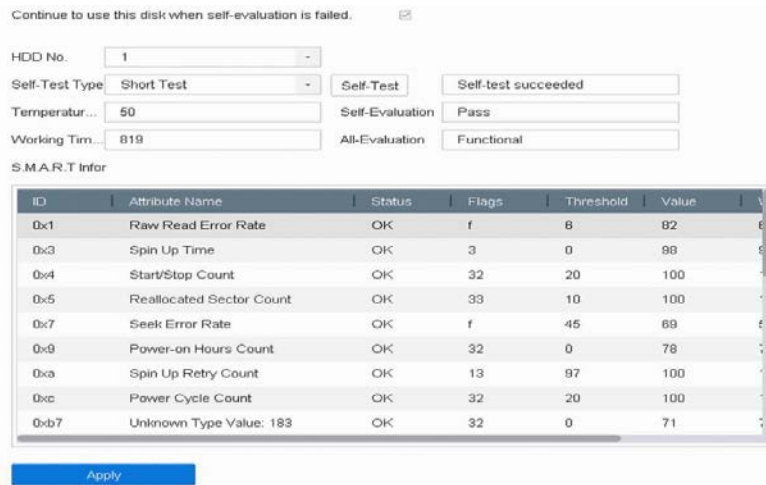


Figure 10.14 S.M.A.R.T. Settings Interface

To use the HDD even when the S.M.A.R.T. checking has failed, check **Continue to use the disk when self-evaluation is failed.**

10.7.2 Bad Sector Detection

Steps

1. Go to **Maintenance** → **HDD Operation** → **Bad Sector Detection** .
2. Select the HDD No. you want to configure in the dropdown list.
3. Select **All Detection** or **Key Area Detection** as the detection type.
4. Click **Self-Test** to start the detection.

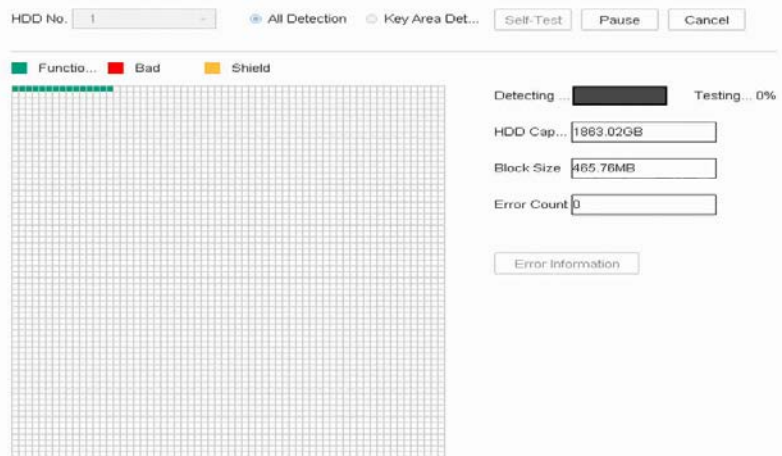


Figure10.15 Bad Sector Detection

- You can pause/resume or cancel the detection.
- After testing has been completed, you can click **Error information** to see the detailed damage information.


10.8 Security Management

10.8.1 RTSP Authentication

You can specifically secure the stream data of live view by setting the RTSP authentication.

Steps

1. Go to Maintenance → System Service → System Service .
2. Select RTSP Authentication Type.
3. Click Apply.
4. Restart the device to take effect the settings.



The screenshot shows a configuration window for RTSP authentication. At the top, there is a checkbox labeled 'Enable RTSP' which is checked. Below it, there is a dropdown menu labeled 'RTSP Authentication Type' with the word 'digest' selected and a small downward arrow on the right side of the menu.

Figure10.16 RTSP Authentication

Two authentication types are selectable, if you select **digest**, 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.

10.8.2 ISAPI Service

ISAPI (Internet Server Application Programming Interface) is an open protocol based on HTTP, which can realize the communication between the system devices (e.g., network camera, NVR, etc.). The device is as a server, the system can find and connect the device.

Steps

1. Go to Maintenance → System Service → System Service .
2. Check Enable ISAPI.
3. Click Apply.
4. Restart the device to take effect the settings.

10.8.3 HTTP Authentication

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

Steps

1. Go to Maintenance → System Service → System Service .
2. Check the Enable HTTP to enable the HTTP service.
3. Select the digest as the HTTP Authentication in the drop-down list.
4. Click Apply to save the settings.



The screenshot shows a configuration window for HTTP authentication. At the top, there is a checkbox labeled 'Enable HTTP' which is checked. Below it, there is a dropdown menu labeled 'HTTP Authentication Type' with the word 'digest' selected and a small downward arrow on the right side of the menu.

Figure10.17 HTTP Authentication

Restart the device to take effect the settings.

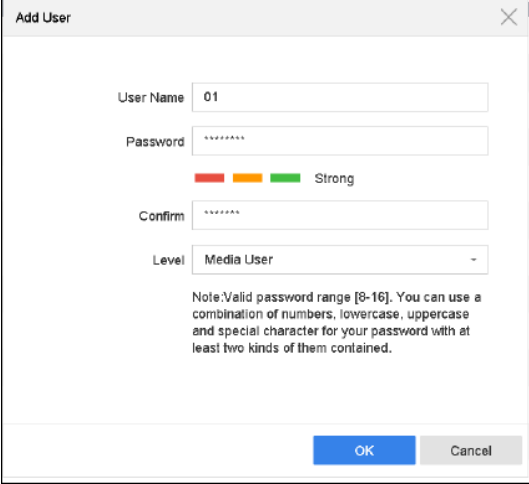
Two authentication types are selectable: **digest** and **digest/basic**. For security reasons, it is recommended to select **digest** as the authentication type.

10.8.4 Managing ONVIF User Accounts

For the third-party camera connection to the device via ONVIF, you can enable ONVIF function and manage the user accounts.

Steps

1. Go to Maintenance > **System Service** > **ONVIF**.
2. Check **Enable ONVIF** to enable the ONVIF access management.
3. Click **Add** to enter the Add User interface.
4. Edit the user name, and enter the strong password.
5. Select the user level to **Media User**, **Operator** and **Admin**.
6. Click **OK** to save the settings.



The screenshot shows a dialog box titled "Add User". It contains the following fields and elements:

- User Name:** A text input field containing "01".
- Password:** A password input field with asterisks. Below it is a strength indicator with three colored bars (red, orange, green) and the word "Strong".
- Confirm:** A password input field with asterisks.
- Level:** A dropdown menu showing "Media User".
- Note:** A text block at the bottom stating: "Note: Valid password range [8-16]. You can use a combination of numbers, lowercase, uppercase and special character for your password with at least two kinds of them contained."
- Buttons:** "OK" and "Cancel" buttons at the bottom right.

Figure10.18 Add User

Result:

The added user accounts have the permission to connect other devices to the device via ONVIF protocol.

11 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.