wisstar+

USER MANUAL

WP-N6632-M4

www.wisstar.net

info@wisstar.net

User Manual

About this Manual

This Manual is applicable to Network Video Recorder (NVR).

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 OUR COMPANY 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 OUR COMPANY, 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 OUR COMPANY 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. OUR COMPANY SHALL NOT TAKE ANY RESPONSIBILITES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER ATTACK, HACKER ATTACK, VIRUS INSPECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, OUR COMPANY 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. OUR COMPANY 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

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. OUR COMPANY 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
	Provides additional information to emphasize or supplement important points of the main text.
	Indicates a potentially hazardous situation, which if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
	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 or 12 VDC according to the IEC60950-1 standard. Please refer to technical specifications for detailed information.
- Do not connect several devices to one power adapter as adapter overload may cause over-heating or a fire hazard.
- Please make sure that the plug is firmly connected to the power socket.
- If smoke, odor or noise rise from the device, turn off the power at once and unplug the power cable, and then please contact the service center.

Preventive and Cautionary Tips

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

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

TABLE OF CONTENTS

Chapter 1 Introduction

1.1 IR Remote Control Operations

The device may also be controlled with the included IR remote control, shown in Figure 1-1.

NOTE

Batteries (2×AAA) must be installed before operation.

The IR remote is set at the factory to control the device (using default Device ID# 255) without any additional steps. Device ID# 255 is the default universal device identification number shared by the devices. You may also pair an IR Remote to a specific device by changing the Device ID#, as follows:

Pairing (Enabling) the IR Remote to a Specific Device (optional)

You can pair an IR Remote to a specific device by creating a user-defined Device ID#. This feature is useful when using multiple IR Remotes and devices.

On the device:

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

Step 2 Type a number (255 digits maximum) into the Device No. field.

On the IR Remote:

Step 3 Press the DEV button.

Step 4 Use the Number buttons to enter the Device ID# that was entered into the device.

Step 5 Press Enter button to accept the new Device ID#.

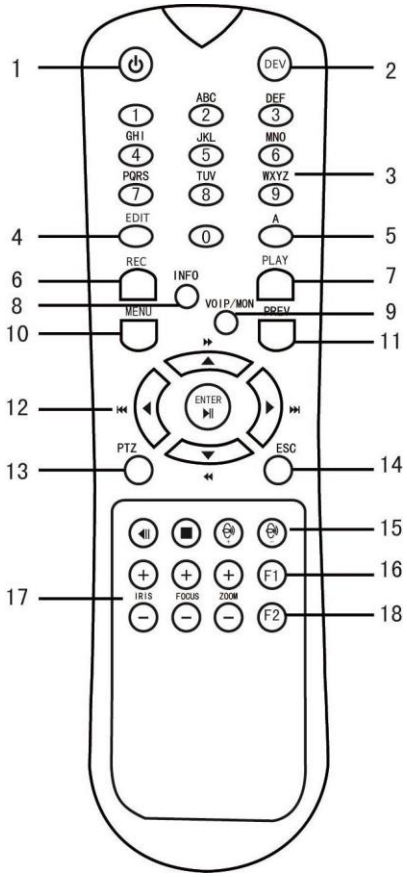


Figure 1-1 Remote Control

Unpairing (Disabling) an IR Remote from a Device

To unpair an IR Remote from a device so that the unit cannot control any device functions, proceed as follows:

Press the DEV key on the IR Remote. Any existing Device ID# will be erased from the unit's memory and it will no longer function with the device.

NOTE

(Re)-enabling the IR Remote requires pairing to a device. See "Pairing the IR Remote to a Specific device (optional)," above.

The keys on the remote control closely resemble the ones on the front panel. See the table 1.4.

Table 1-1 IR Remote Functions

No.	Name	Function Description
1	**POWER ON/OFF**	•To Turn Power On: -If User Has Not Changed the Default device Device ID# (255): 1.Press Power On/Off button (1). -If User Has Changed the device Device ID#: 1.Press DEV button. 2.Press Number buttons to enter user-defined Device ID#. 3.Press Enter button. 4.Press Power button to start device. •To Turn device Off: -If User Is Logged On: 1.Hold Power On/Off button (1) down for five seconds to display the "Yes/No" verification prompt. 2.Use Up/Down Arrow buttons (12) to highlight desired selection. 3.Press Enter button (12) to accept selection. -If User Is *Not* Logged On: 1.Hold Power On/Off button (1) down for five seconds to display the user name/password prompt. 2.Press the Enter button (12) to display the on-screen keyboard. 3.Input the user name. 4.Press the Enter button (12) to accept input and dismiss the on-screen keyboard. 5.Use the Down Arrow button (12) to move to the "Password" field. 6.Input password (use on-screen keyboard or numeric buttons (3) for numbers). 7.Press the Enter button (12) to accept input and dismiss the on-screen keyboard. 8.Press the OK button on the screen to accept input and display the Yes/No" verification prompt (use Up/Down Arrow buttons (12) to move between fields) 9.Press Enter button (12) to accept selection. User name/password prompt depends on device is configuration. See "System Configuration" section.

2	**DEV**	Enable IR Remote: Press DEV button, enter device Device ID# with number keys, press Enter to pair unit with the device
		Disable IR Remote: Press DEV button to clear Device ID#; unit will no longer be paired with the device
3	**Numerals**	Switch to the corresponding channel in Live View or PTZ Control mode
		Input numbers in Edit mode
4	**EDIT**	Delete characters before cursor
		Check the checkbox and select the ON/OFF switch
5	**A**	Adjust focus in the PTZ Control menu
		Switch on-screen keyboards (upper and lower case alphabet, symbols, and numerals)
6	**REC**	Enter Manual Record setting menu
		Call a PTZ preset by using the numeric buttons in PTZ control settings
		Turn audio on/off in Playback mode
7	**PLAY**	Go to Playback mode
		Auto scan in the PTZ Control menu
8	**INFO**	Reserved
9	**VOIP**	Switches between main and spot output Zooms out the image in PTZ control mode
10	**MENU**	Return to Main menu (after successful login)
		N/A
		Show/hide full screen in Playback mode
12	**DIRECTION**	Navigate between fields and menu items
		Use Up/Down buttons to speed up/slow down recorded video, and Left/Right buttons to advance/rewind 30 secs in Playback mode
		Cycle through channels in Live View mode
		Control PTZ camera movement in PTZ control mode
	ENTER	Confirm selection in any menu mode

		Checks checkbox
		Play or pause video in Playback mode
		Advance video a single frame in single-frame Playback mode
		Stop/start auto switch in auto-switch mode
13	**PTZ**	Enter PTZ Control mode
14	**ESC**	Go back to previous screen
		N/A
15	**RESERVED**	Reserved
16	**F1**	Select all items on a list
		N/A
		Switch between play and reverse play in Playback mode
17	**PTZ Control**	Adjust PTZ camera iris, focus, and zoom
18	**F2**	Cycle through tab pages
		Switch between channels in Synchronous Playback mode

Troubleshooting Remote Control:

NOTE

Make sure you have installed batteries properly in the remote control. And you have to aim the remote control at the IR receiver in the front panel.

If there is no response after you press any button on the remote, follow the procedure below to troubleshoot.

Step 1 Go to **System** > **General** by operating the front control panel or the mouse.

Step 2 Check and remember device ID#. The default ID# is 255. This ID# is valid for all the IR remote controls.

Step 3 Press the DEV button on the remote control.

Step 4 Enter the device ID# you set in step 2.

Step 5 Press the ENTER button on the remote.

If the Status indicator on the front panel turns blue, the remote control is operating properly. If the Status indicator does not turn blue and there is still no response from the remote, please check the following:

- Batteries are installed correctly and the polarities of the batteries are not reversed.
- Batteries are fresh and not out of charge.
- IR receiver is not obstructed.
- No fluorescent lamp is used nearby

If the remote still can’t function properly, please change a remote and try again, or contact the device provider.

1.2 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:

Step 1 Plug USB mouse into one of the USB interfaces on the front panel of the device.

Step 2 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:

Table 1-2 Description of the Mouse Control

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.

Chapter 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.

Start up the device:

Step 1 Check the power supply is plugged into an electrical outlet. It is HIGHLY recommended that an Uninterruptible Power Supply (UPS) be used in conjunction with the device. The Power indicator LED on the front panel should be red, indicating the device gets the power supply.

Step 2 Press the POWER button on the front panel. The Power indicator LED should turn blue indicating that the unit begins to start up.

Step 3 After startup, the Power indicator LED remains blue. A splash screen with the status of the HDD appears on the monitor. The row of icons at the bottom of the screen shows the HDD status. 'X' means that the HDD is not installed or cannot be detected.

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.

Step 1 Input the same password in the text field of **Create New Password** and **Confirm New Password**.

NOTE

You can click the  to show the characters input.

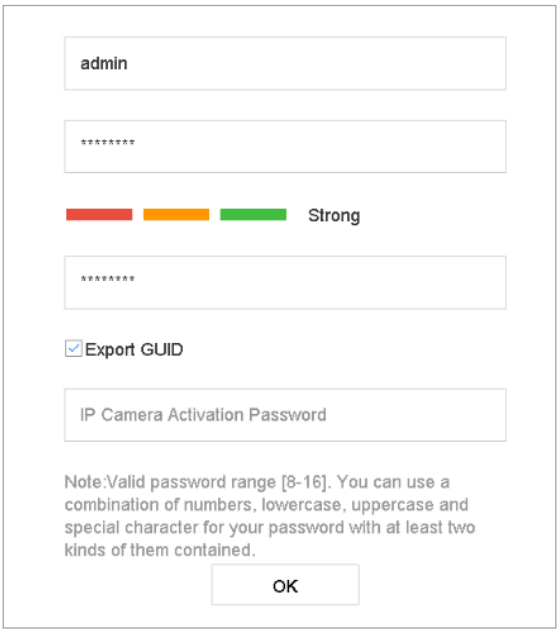


Figure 2-1 Setting Admin Password

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.

Step 2 In the **IP Camera Activation** text field, enter the password to activate the IP camera (s) connected to the device.

Step 3 Optionally, check the **Export GUID** to export the GUID for future password resetting.

Step 4 Click **OK** to save the password and activate the device.

NOTE

- After the device is activated, you should properly keep the password.
- When you have enabled the **Export GUID**, continue to export the GUID file to the USB flash driver for the future password resetting.
- You can duplicate the password to the IP cameras that are connected with default protocol.

2.3 Configure Unlock Pattern for Login

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

Step 1 After the device is activated, you can enter the following interface to configure the device unlock pattern.

Step 2 Use the mouse to draw a pattern among the 9 dots on the screen. Release the mouse when the pattern is done.

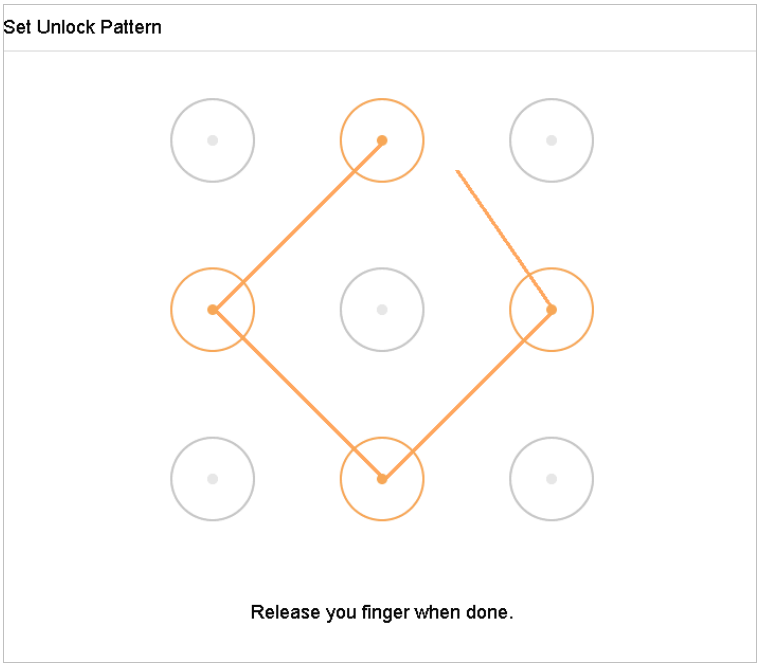


Figure 2-2 Draw the Pattern

NOTE

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

Step 3 Draw the same pattern again to confirm it. When the two patterns match, the pattern is configured successfully.

NOTE

If the two patterns are different, you must set the pattern again.

2.4 Login to the Device

2.4.1 Log in via Unlock Pattern

NOTE

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

Step 1 Please configure the pattern first before unlocking. Please refer to Chapter 2.2 Step 2In the **IP Camera Activation** text field, enter the password to activate the IP camera (s) connected to the device.

Step 2 Optionally, check the **Export GUID** to export the GUID for future password resetting.

Step 3 Click **OK** to save the password and activate the device.

NOTE

- After the device is activated, you should properly keep the password.
- When you have enabled the **Export GUID**, continue to export the GUID file to the USB flash driver for the future password resetting.
- You can duplicate the password to the IP cameras that are connected with default protocol.
- Configure Unlock Pattern for Login.

Step 4 Right click the mouse on the screen and select the menu to enter the interface.

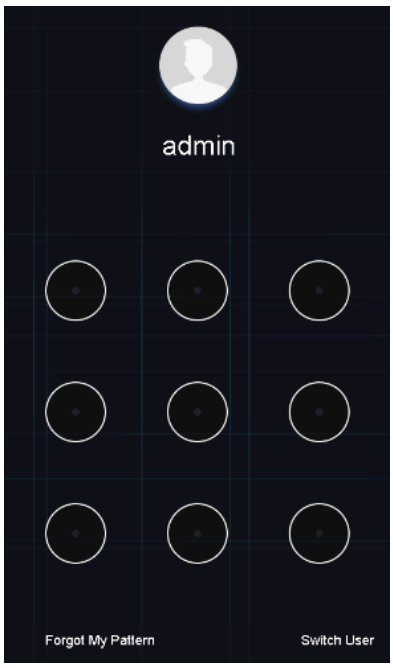


Figure 2-3 Draw the Unlock Pattern

Step 5 Draw the pre-defined pattern to unlock to enter the menu operation.

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.

Step 1 Select the **User Name** in the dropdown list.

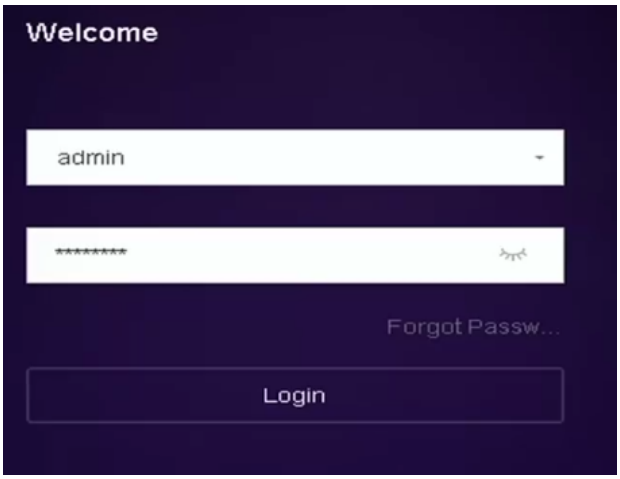


Figure 2-4 Login Interface

Step 2 Input password.

Step 3 Click **Login** to log in.

NOTE

When you forget the password of the admin, you can click **Forgot Password** to reset the password.

NOTE

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

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.

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

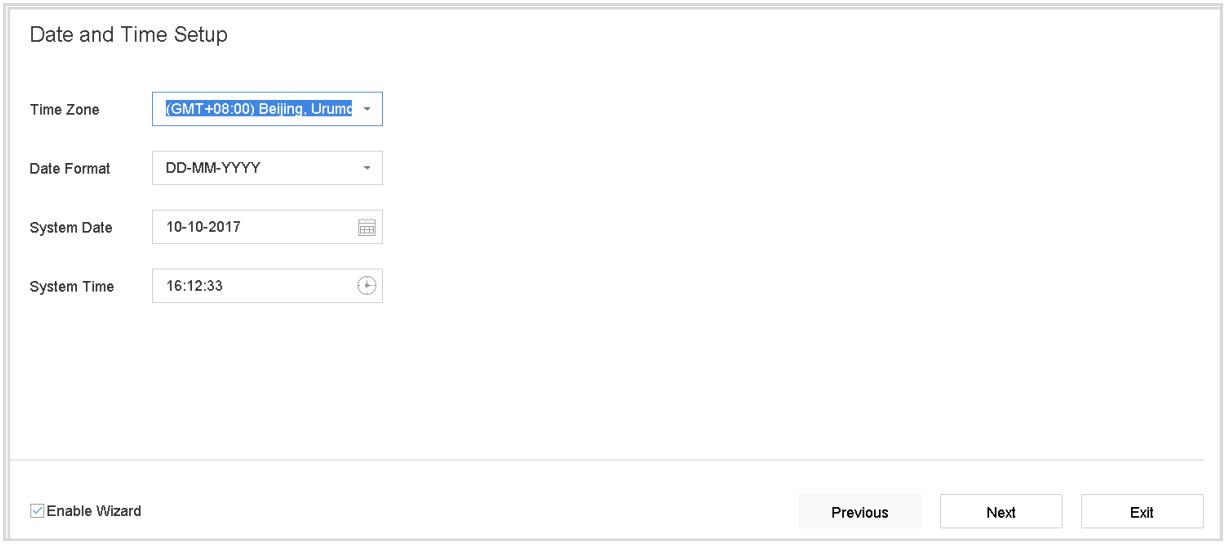


Figure 2-5 Date and Time Settings

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

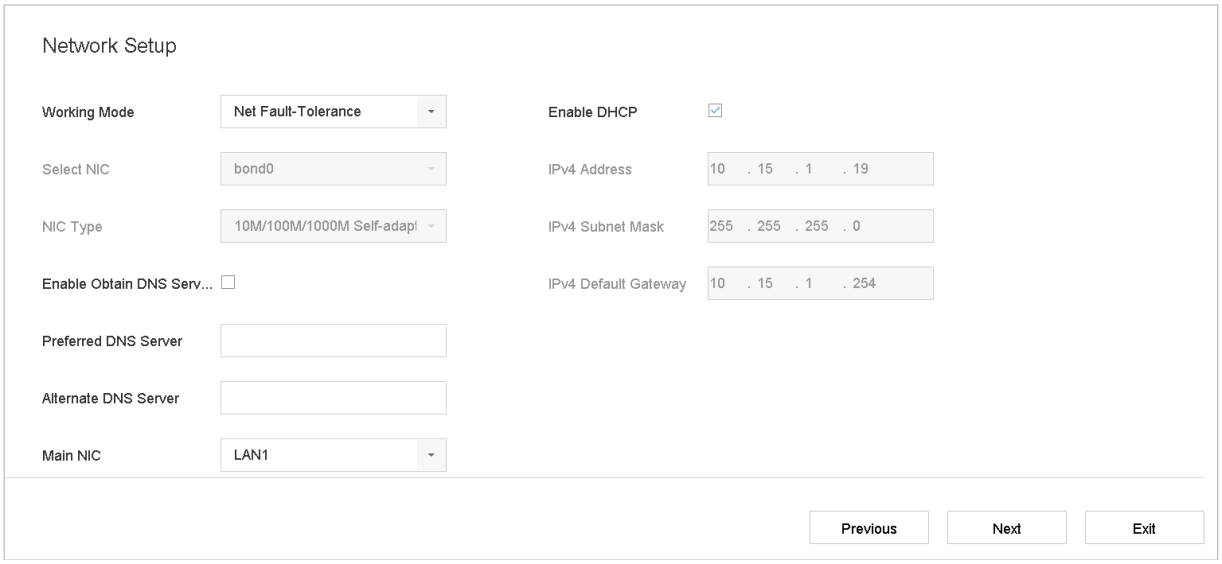


Figure 2-6 Network Settings

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

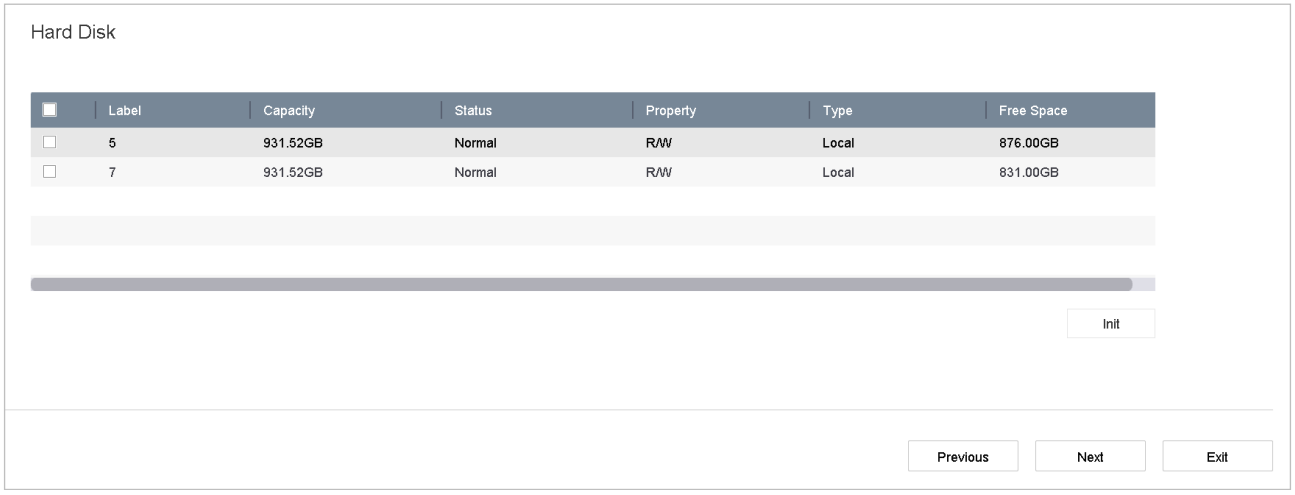


Figure 2-7 HDD Management

Step 4 To initialize the HDD, click the **Init** button. Initialization removes all the data saved in the HDD.

Step 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.

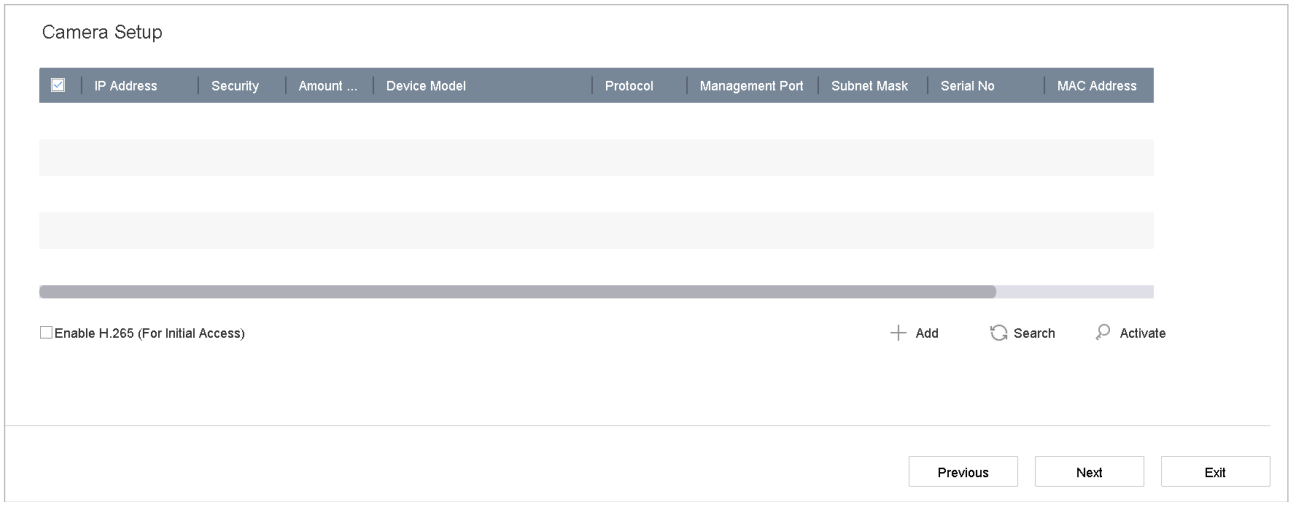


Figure 2-8 Search for IP Cameras

Step 6 Enter the Platform Access and configure the Guarding Vision settings.

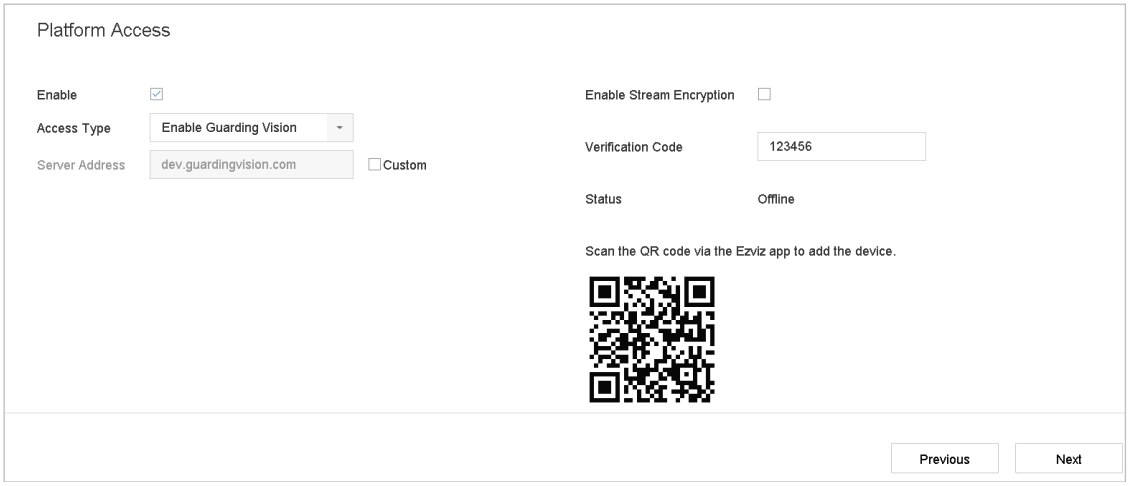


Figure 2-9 Guarding Vision Access

Step 7 Click **Next** to enter the **Change Password** interface to create the new admin password if required.

Figure 2-10 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.

Step 8 Click **OK** to complete the startup Setup Wizard.

2.6 Enter Main Menu

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.

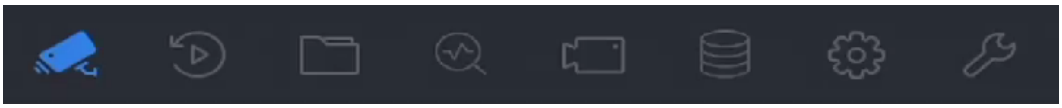


Figure 2-11 Main Menu Bar

Table 2-1 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 log in again.

Step 1 Click  on the menu bar.

Step 2 Click **Logout**.

NOTE

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

2.7.2 Shut Down the Device

Step 1 Click  on the menu bar.

Step 2 Click the **Shutdown** button.

Step 3 Click the **Yes** button.

NOTE

Do not press the POWER button again when the system is shutting down.

2.7.3 Reboot the Device

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

Step 1 Click  on the menu bar.

Step 2 Click **Reboot** to reboot the device.

Chapter 3 Camera Management

3.1 Add the IP Cameras

3.1.1 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.

Step 1 Click  on the main menu bar to enter the Camera Management.

Step 2 Click the **Custom Add** tab on the title bar or click  in the idle channel window to enter the Add IP Camera interface.

Step 3 Enter IP address, protocol, management port, and other information of the IP camera to add.

Step 4 Enter the login user name and password of the IP camera.

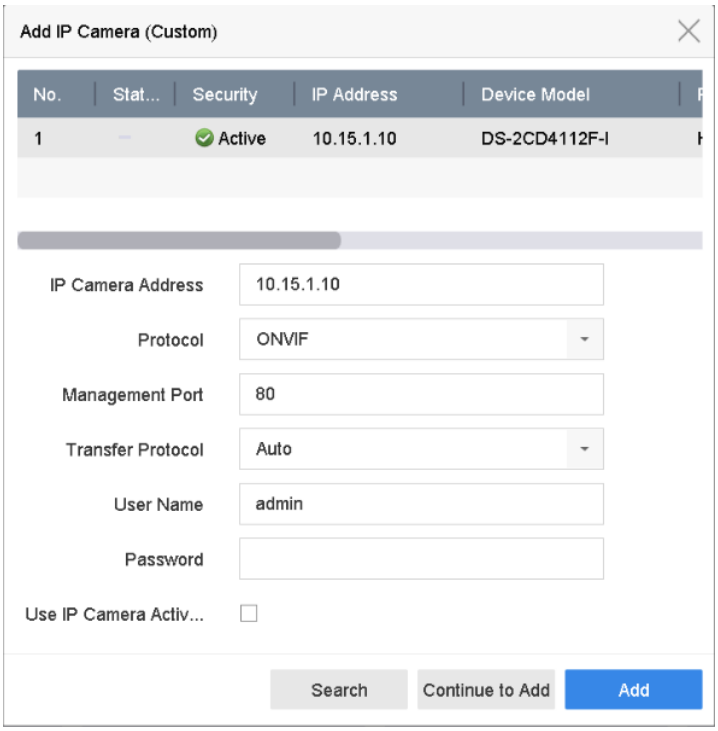


Figure 3-1 Add IP Camera

Step 5 Click **Add** to finish the adding of the IP camera.

Step 6 (Optional) Click **Continue to Add** to continue to add other IP cameras.

3.1.2 Add the Automatically Searched Online IP Cameras

Step 1 On the Camera Management interface, click the **Online Device** panel to expand the Online Device interface.

Step 2 Select the automatically searched online device.

Step 3 Click **Add** to add the camera which has the same login password with the device.

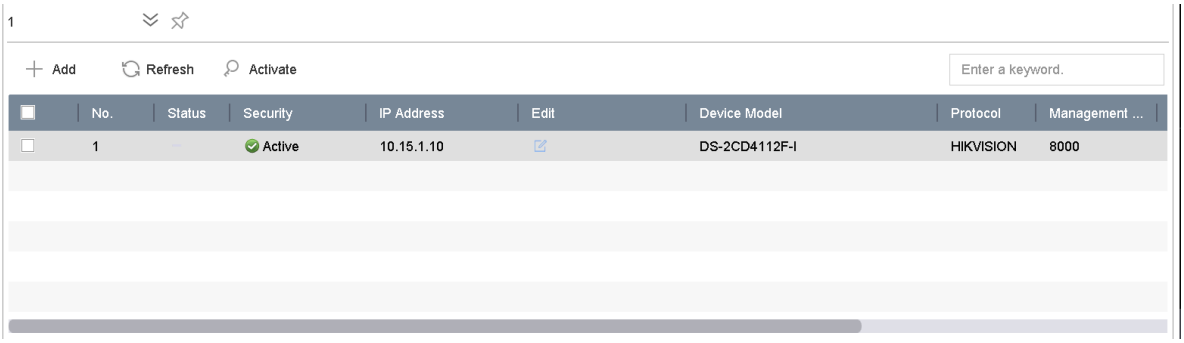


Figure 3-2 Add IP Camera

NOTE

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

3.2 Manage Cameras for PoE Device

NOTE

This chapter is only applicable for models with PoE funciton.

Purpose:

The PoE interfaces enables the device system to pass electrical power safely, along with data, on Ethernet cabling to the connected PoE cameras. Supported PoE camera number varies with device model

If you disable the PoE interface, you can also connect to the online network cameras. And the PoE interface supports the Plug-and-Play function.

For example, if you want to connect 6 network cameras via PoE interfaces and 2 online cameras, you must disable 2 PoE interfaces in the Edit IP Camera menu.

Follow the steps to add network cameras for device supporting PoE function.

3.2.1 Add PoE Cameras

Step 1 Connect PoE cameras to device PoE ports with network cables.

Step 2 Go to **Camera > Camera > IP Camera** to view camera image and information.

3.2.2 Add Non-PoE IP Cameras

You can disable the PoE interface by selecting the manual while the current channel can be used as a normal channel and the parameters can also be edited.

Step 1 Go to **Camera > Camera > IP Camera**.

Step 2 Position the cursor on a window with no linked IP camera and click the  button.

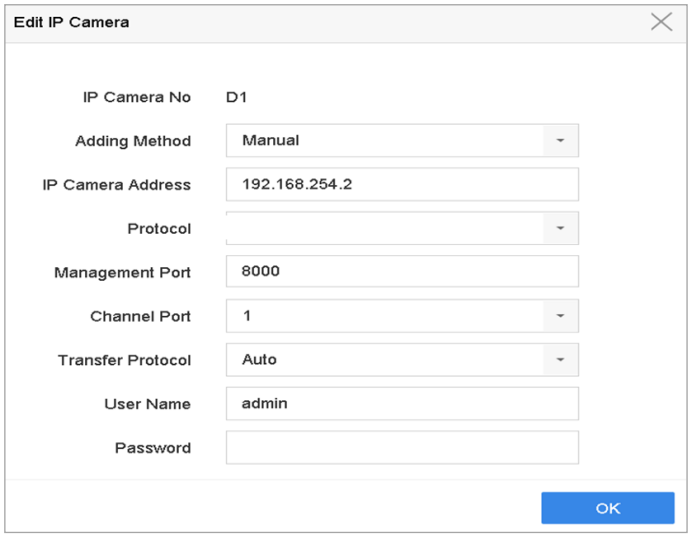


Figure 3-3 Edit IP Camera

Step 3 Select Adding Method as **Manual**.

- **Plug-and-Play:** The camera is physically connected to the PoE interface. Its parameters cannot be edited. You can go to **System > Network > TCP/IP** to change IP address of PoE port. .
- **Manual:** Add IP camera without physical connection via network.

Step 4 Enter the IP address, the user name and password of administrator manually.

Step 5 Click **OK**.

3.2.3 Configure PoE Interface

Purpose:

When it requires long-distance PoE transmission (100 to 300 m), you can enable long distance mode for the PoE channel.

Step 1 Go to **Camera > Camera >PoE Settings**.

Step 2 Enable or disable long network cable mode by selecting **Long Distance** or **Short Distance** radio.

- **Long Distance**: Long-distance (100 to 300 meters) network transmissions via POE interface.
- **Short Distance**: Short-distance (< 100 meters) network transmission via POE interface.

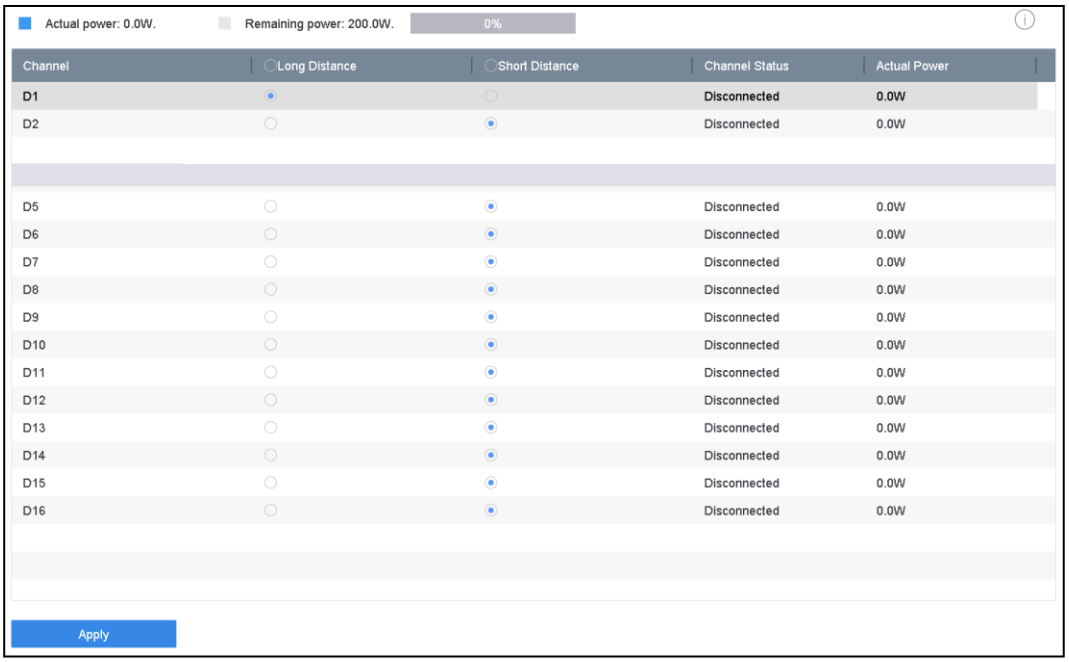


Figure 3-4 PoE Settings

NOTE

- The PoE ports are enabled with the short distance mode by default.
- The bandwidth of IP camera connected to the PoE via long network cable (100 to 300 meters) cannot exceed 6 MP.
- The allowed max. long network cable may be less than 300 meters depending on different IP camera models and cable materials.
- When the transmission distance reaches 100 to 250 meters, you must use the CAT5E or CAT6 network cable to connect with the PoE interface.
- When the transmission distance reaches 250 to 300 meters, you must use the CAT6 network cable to connect with the PoE interface.

Step 3 Click **Apply**.

3.3 Enable the H.265 Stream Access

The device can automatically switch to the H.265 stream of IP camera (which supports H.265 video format) for the initial access.

Step 1 Go to **More Settings** > **H.265 Auto Switch Configuration** at the top taskbar.

Step 2 Check the checkbox of **Enable H.265 (For Initial Access)**.

Step 3 Click **OK**.

3.4 Upgrade the IP Camera

The IP camera can be remotely upgraded through the device.

NOTE

Plug the U-flash drive with the IP camera's firmware upgrade file to the device.

Step 1 On the camera management interface, select a camera.

Step 2 Go to **More Settings** > **Upgrade** at the top taskbar.

Step 3 Select the firmware upgrade file from the U-flash drive.

Step 4 Click **Upgrade**.

Result:

The IP camera will reboot automatically after the upgrading completes.

3.5 Configure the Customized Protocols

Purpose

To connect the network cameras which are not configured with the standard protocols, you can configure the customized protocols for them. The system provides 16 customized protocols.

Step 1 Go to **More Settings** > **Protocol** at the top taskbar to enter the protocol management interface.

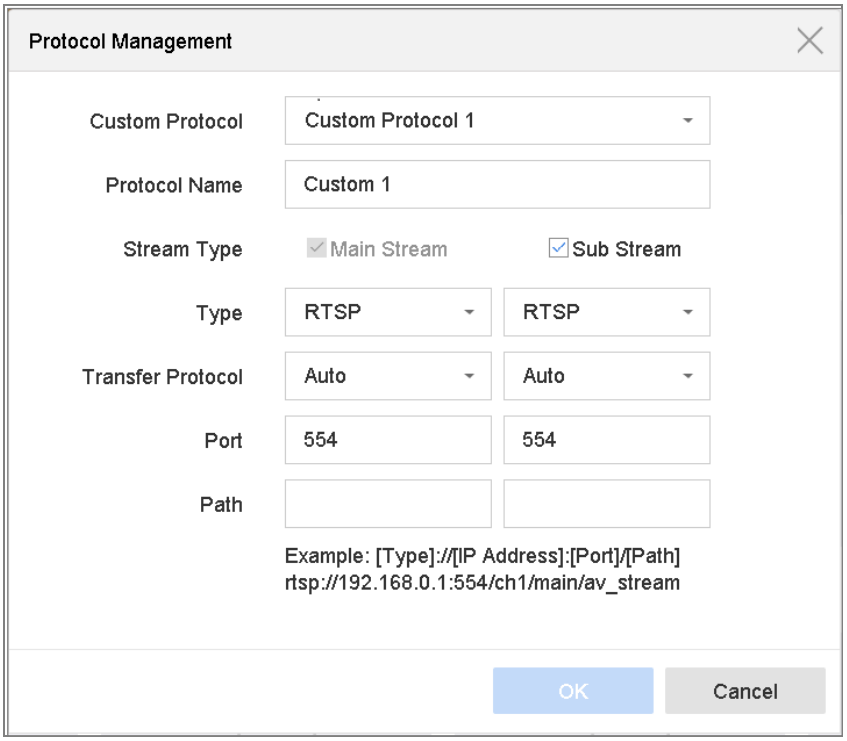


Figure 3-5 Protocol Management

Step 2 Select the protocol type of transmission and choose the transfer protocols.

- **Type:** The network camera adopting custom protocol must support getting stream through standard RTSP.
- **Path:** you have to contact the manufacturer of the network camera to consult the URL (uniform resource locator) for getting main stream and sub-stream.
- The format of the URL is: [Type]://[IP Address of the network camera]:[Port]/[Path].
- ***Example:*** rtsp://192.168.1.55:554/ch1/main/av_stream.

NOTE

The protocol type and the transfer protocols must be supported by the connected IP camera.

Step 3 Click **OK** to save the settings.

Result:

After adding the customized protocols, you can see the protocol name is listed in the drop-down list.

Chapter 4 IoT

IoT (Internrt of Things) feature allows you to build connections between your video recorder and IoT devices, including access control and alarm devices. Video recorder will receive alarms from connected IoT devices. You can configure linkage actions like triggering recording and full screen monitoring, when IoT alarm occurs.

4.1 Add IoT Device

NOTE

Maximum IoT channel number is the half of maximum network camera number of your video recorder.

4.1.1 Add Access Control Device

Purpose

Add alarm host and video intercom devices to receive their alarms. You can configure linkage actions like triggering recording and full screen monitoring, when an alarm occurs.

Before your start

Install access control devices. Ensure network communication between access control devices and video recorder is well.

Step 1 Go to **Business Application > IoT > Access Control > Device Management**.

Step 2 Click **Add**.

Figure 4-1 Access Control

Step 3 Enter access control device information. **Device IP**, **Port**, **User Name**, and **Password** must be the same with access control device.

Step 4 (Optional) For device with multiple access control channels or video channels, check the access control channel and video channel as your desire.

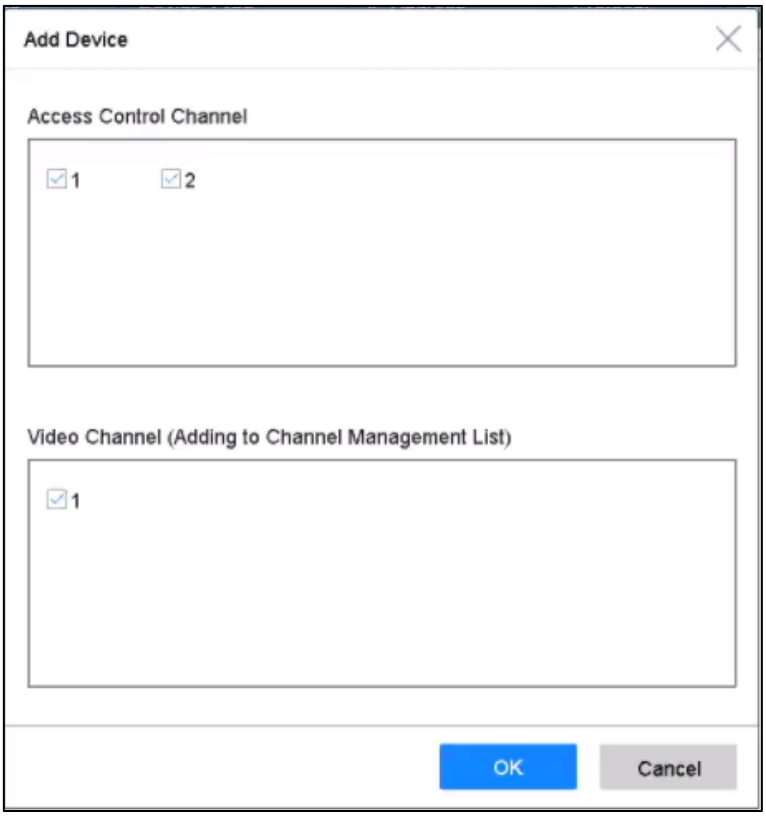


Figure 4-2 Add Device

Step 5 Click **Add**.

Related operations:

- Click to view the live video of related channel.

NOTE

For access control devices without the video channel. You need to select trigger channel in linkage action configuration first. For details, refer to *4.2 Configure Linkage Action*.

- Click to edit added access control device information.

4.1.2 Add Alarm Device

Purpose

Add alarm devices of Luminite, GJD, or OPTEX manufacturer to receive their alarms. You can configure linkage actions like triggering recording and full screen monitoring, when an alarm occurs.

Before your start

Install alarm devices. Ensure network communication between alarm devices and video recorder is well.

Step 1 Go to **Business Application > IoT > Alarm > Device Management**.

Step 2 Click **Add**.

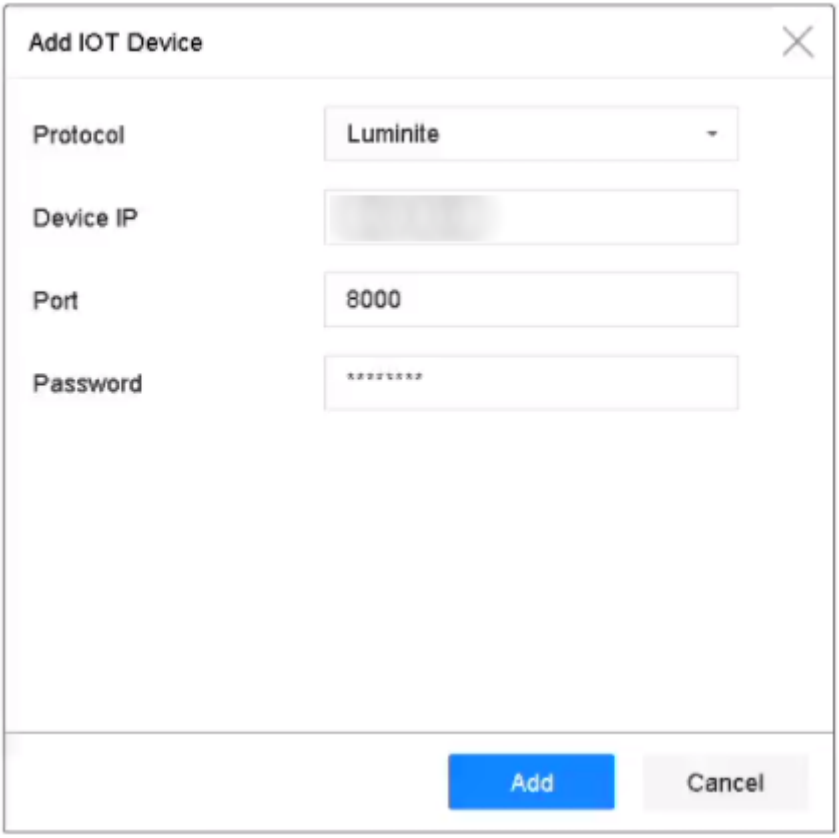


Figure 4-3 Alarm Device

Step 3 Enter access control device information. The information must be the same with alarm device to add.

Step 4 Click **Add**.

Related operations:

- Click to view the live video of related channel.

NOTE

You need to select trigger channel in linkage action configuration first. For details, refer to *4.2 Configure Linkage Action*.

- Click to edit added alarm device information.

4.2 Configure Linkage Action and Arming Schedule

Purpose

Configure the linkage actions and arming schedule for access control or alarm devices. Linkage actions will be triggered when the designate alarm occurs.

Step 1 Click  of an added IoT device.

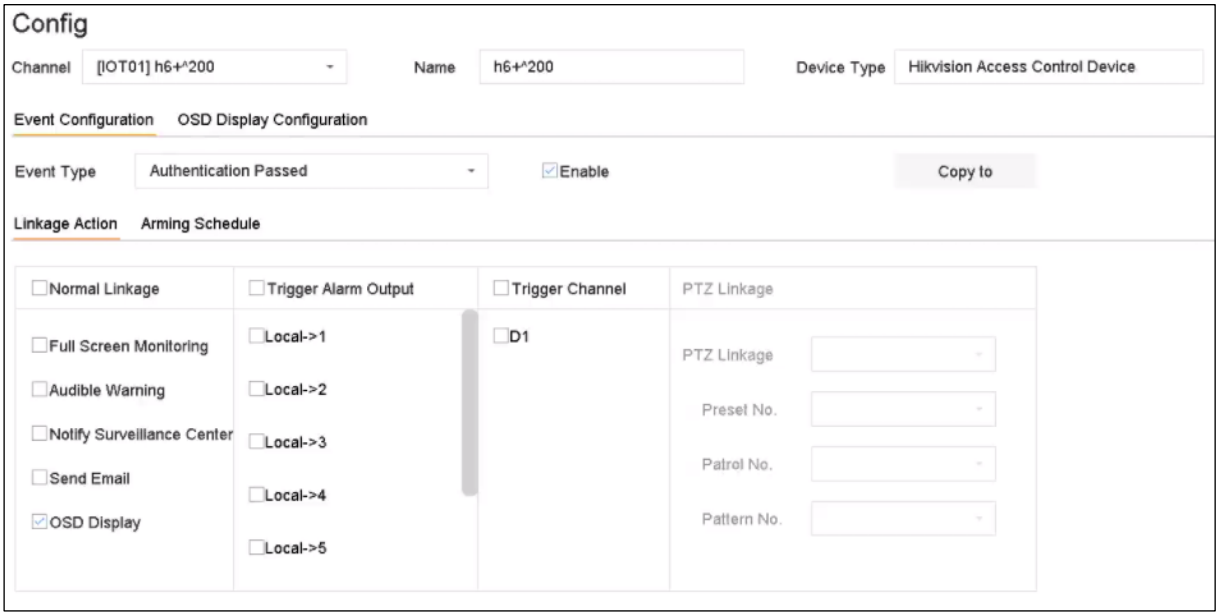


Figure 4-4 Configure IoT

Step 2 Select **Event Type.** The following configuration is only valid for the selected event type.

Step 3 Check **Enable**.

Step 4 Check linkage actions as your desire. For detailed steps, refer to *11.2 Configure Alarm Linkage Actions*.

Full Screen Monitoring and **OSD Display** are only valid for the selected **Trigger Channel**.

Step 5 Click **Arming Schedule**.

Step 6 Configure arming schedule. For detailed steps, refer to *11.1 Configure Arming Schedule*. Linkage action is only valid during the set schedule.

Step 7 Click **Apply**.

4.3 Configure OSD

Purpose

You can display alarm information received from IoT devices on live view image.

Step 1 Click  of an added IoT device.

Step 2 Check **OSD Display** on Event Configuration interface.

Step 3 Select **Trigger Channel**.

Step 4 Click **OSD Display Configuration**.

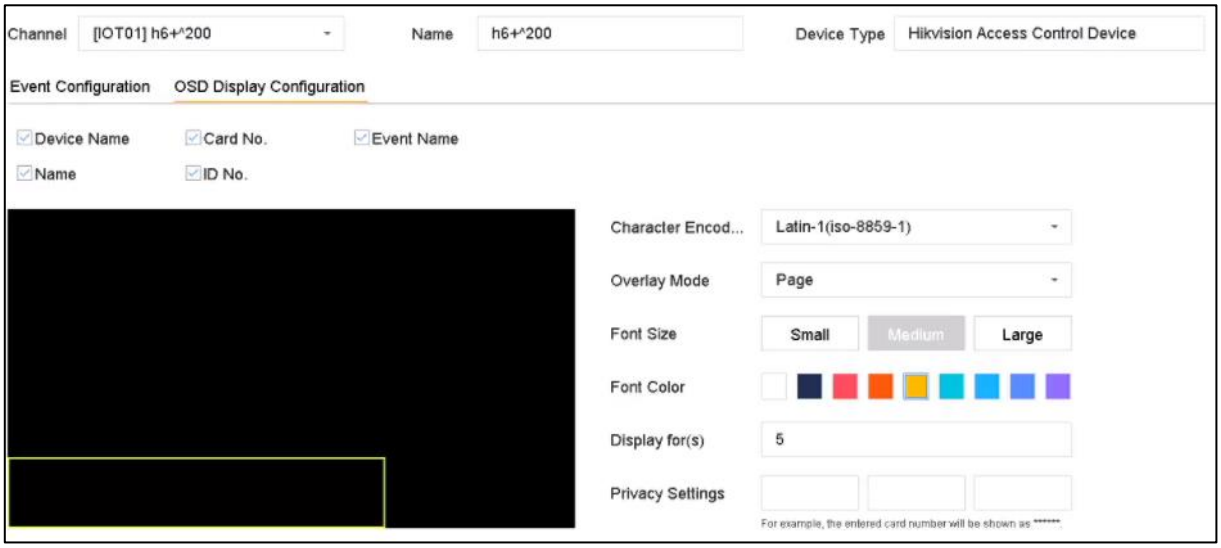


Figure 4-5 OSD Configuration

Step 5 Select items, including **Device Name**, **Card No.**, **Event Name**, **Name**, and **ID No.**, to display on live view image. The items are only for access control devices.

Step 6 Configure OSD properties.

- **Overlay Mode**:

  − **Scroll**: The OSD will automatically scroll to show the new alarm information.

  − **Page**: When the current OSD cannot show more alarm information, it will automatically turn to new page

- **Privacy Settings**: Enter privacy information you want to mask. Masked privacy information will be replaced by *. Privacy information includes **Event**, **Device**, **Card**, **Name**, and **ID**.

Step 7 Adjust the quadrilateral of yellow frame on the preview window to adjust IoT OSD size and position.

Step 8 Click **Apply**.

4.4 Search IoT Record

Purpose

Search alarms by time, by event type, or by channel.

Step 1 Go to event record interface.

- Access control: Go to **Business Application > IoT > Access Control > Card Swiping Record**.
- Alarm device: Go to **Business Application > IoT > Alarm > Search Data.**

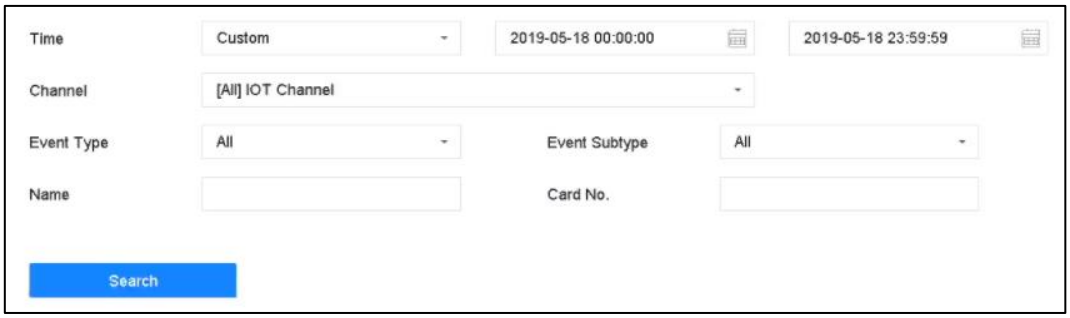


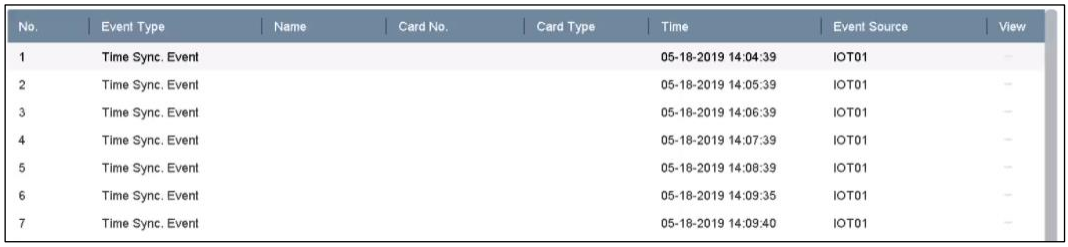
Figure 4-6 Search Event Record (Access Control)

Figure 4-7 Search Event Record (Alarm Device)

Step 2 Specify search conditions.

Name and **Card No.**: When card swiping event occurs, the access control device will upload card name and card No. to video record. You can search event by card name or card No.

Step 3 Click **Search.**



No.	Event Type	Name	Card No.	Card Type	Time	Event Source	View
1	Time Sync. Event				05-18-2019 14:04:39	IOT01	
2	Time Sync. Event				05-18-2019 14:05:39	IOT01	
3	Time Sync. Event				05-18-2019 14:06:39	IOT01	
4	Time Sync. Event				05-18-2019 14:07:39	IOT01	
5	Time Sync. Event				05-18-2019 14:08:39	IOT01	
6	Time Sync. Event				05-18-2019 14:09:35	IOT01	
7	Time Sync. Event				05-18-2019 14:09:40	IOT01	

Figure 4-8 Search Result (Access Control)

No.	Channel	Time	Main Type	Sub Type	Status	Data	View
1	IOT03	05-18-2019 14:49:56	GJD Alarm Event	PIR Detection alarm			

Figure 4-9 Search Result (Alarm Device)

4.5 IoT Video/Picture

Purpose

Configure the event recording or capturing schedule for the selected trigger channel, the channel will automatically record videos or capture pictures when IoT alarm occurs.

4.5.1 Configure Event Recording/Capturing

Purpose:

The video recorder can record videos or capture pictures when an IoT alarm occurs.

Step 1 Click  of an added IoT device.

Step 2 Select desired **Event Type**.

Step 3 Check **Enable**.

Step 4 Check **Trigger Channel** you want to record event videos or capture pictures when an alarm occurs.

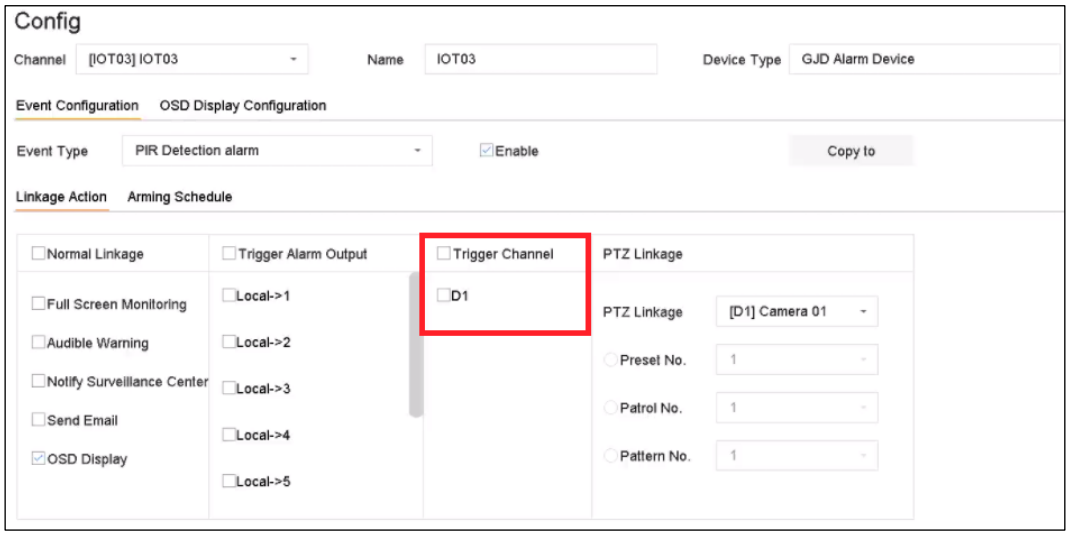


Figure 4-10 Trigger Channel

Step 5 Click **Apply**.

Step 6 Configure event recording or capturing schedule. Choose from:

- Recording
  1) Go to **Storage > Schedule > Record**.
  2) Select **Camera No.** and check **Enable Schedule**. The camera should be the camera you select in step 4.
  3) Select the recording type as **Event**.
  4) Drag the mouse on the time bar to set the event detection recording schedule. Refer to *8.4 Configure Recording Schedule* for details.
  5) Click **OK**.
- Capturing
  1) Go to **Storage > Schedule > Capture**.
  2) Select **Camera No.** and check **Enable Schedule**. The camera should be the camera you select in step 4.
  3) Select the capturing type as **Event**.

4) Drag the mouse on the time bar to set the event detection capturing schedule. Refer to *8.4 Configure Recording Schedule* for details.
5) Click **OK**.

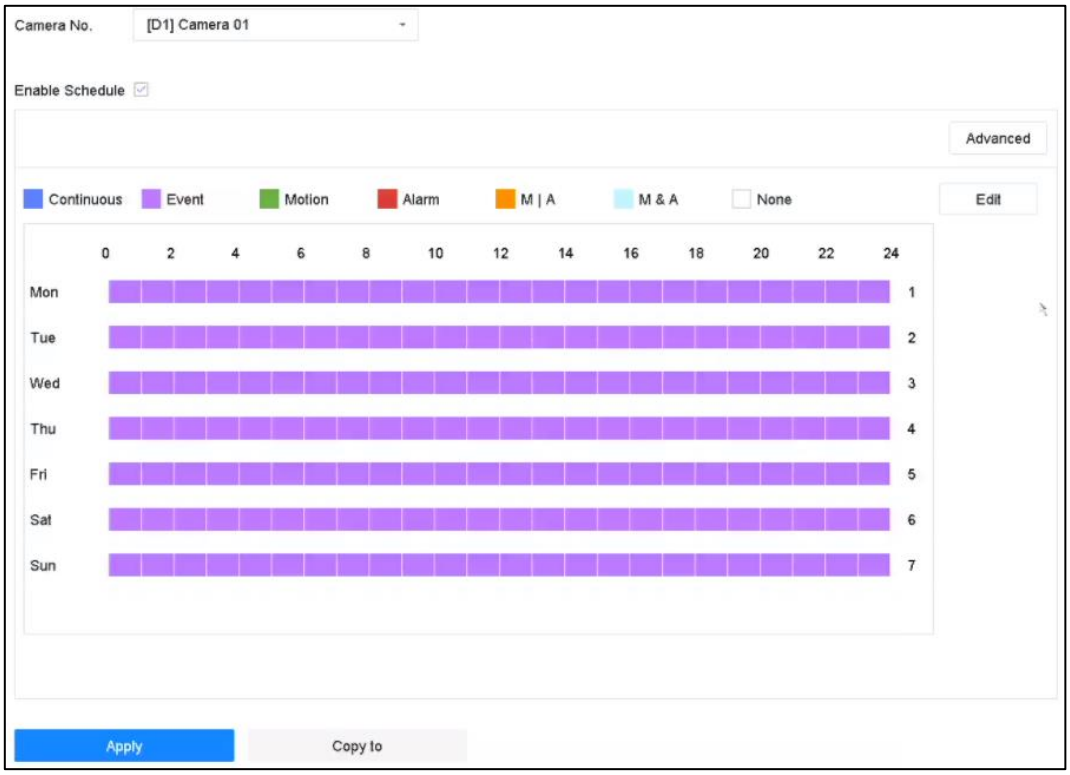


Figure 4-11 Event Recording

Step result:

When an alarm occurs, the selected trigger channel will start event recording.

4.5.2 Search IoT Video/Picture

Purpose

Search IoT event triggered videos or pictures.

Step 1 Go to **File Management > All Files**.

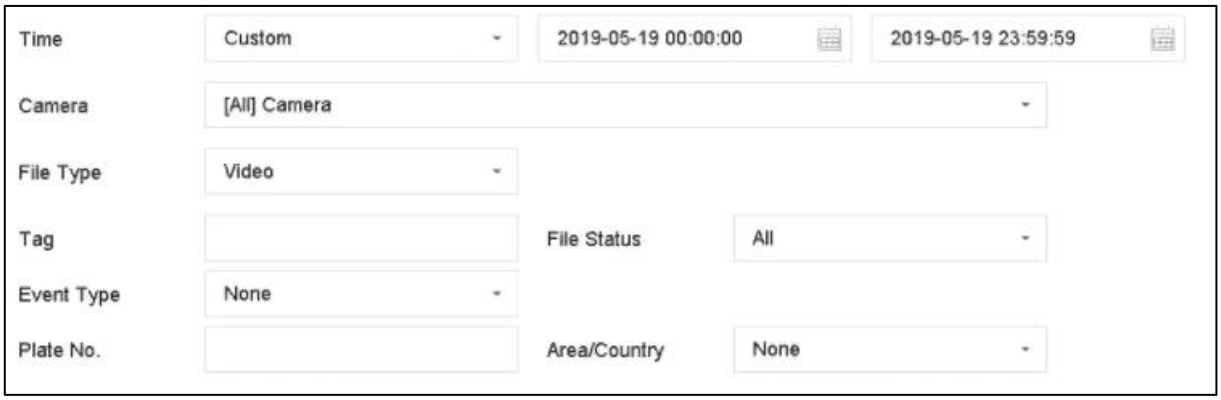


Figure 4-12 Search Event Video/Picture

Step 2 Set search conditions.

- **Camera**: Select it as the selected trigger channels in IoT linkage action configuration.
- **Event Type**: Select the desired IoT event.
- **File Type**: You can search the IoT video or picture.

Step 3 Click **Search**.

Chapter 5 Camera Settings

5.1 Configure OSD Settings

Purpose:

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

Step 1 Go to **Camera** >**Display.**

Step 2 Select the camera from the drop-down list.

Step 3 Edit the name in the **Camera Name** text field.

Step 4 Check the checkbox of the **Display Name**, **Display Date** and **Display Week** if you want to show the information on the image.

Step 5 Set the date format, time format, and display mode.

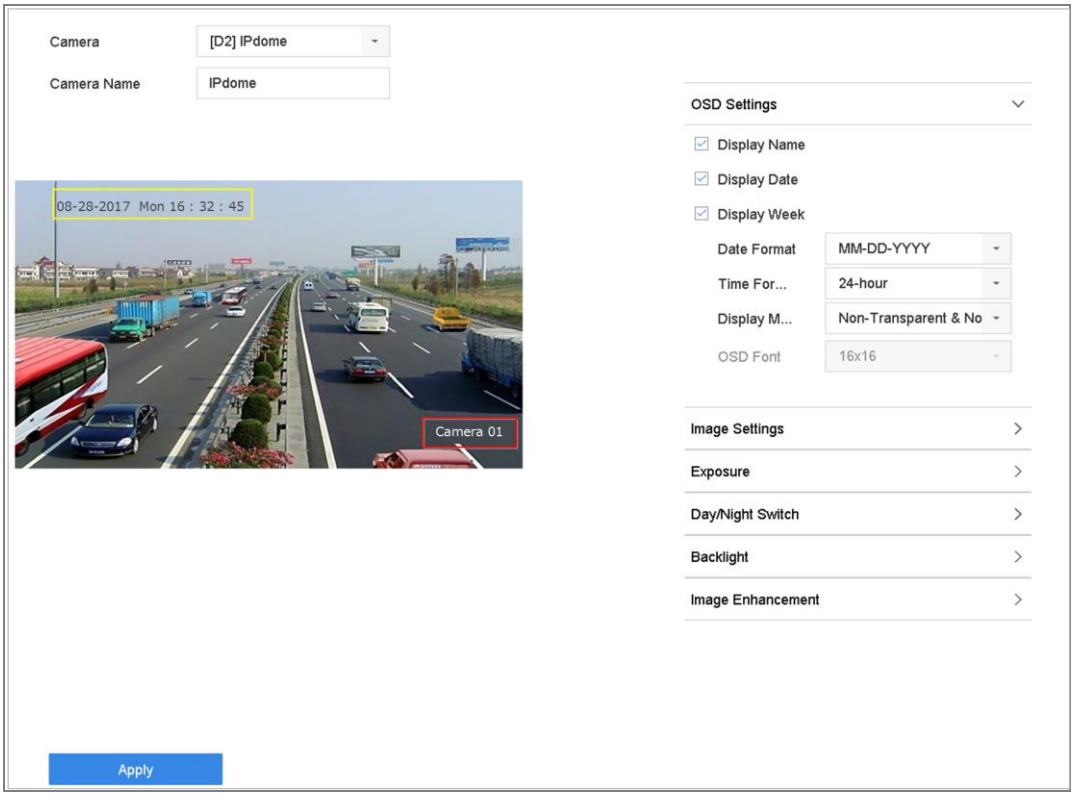


Figure 5-1 OSD Configuration Interface

Step 6 You can use the mouse to click and drag the text frame on the preview window to adjust the OSD position.

Step 7 Click the **Apply** button to apply the settings.

5.2 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.

Step 1 Go to **Camera** >**Privacy Mask**.

Step 2 Select the camera to set privacy mask.

Step 3 Click the checkbox of **Enable** to enable this feature.

Step 4 Use the mouse to draw a zone on the window. The zones will be marked with different frame colors.

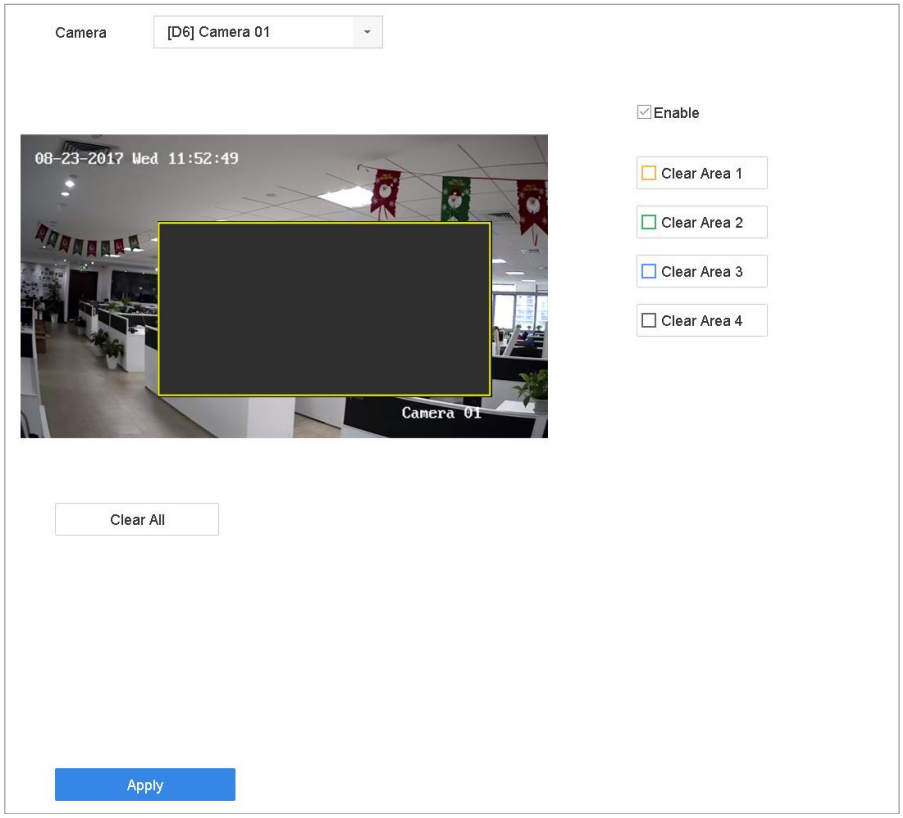


Figure 5-2 Privacy Mask Settings Interface

NOTE

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.

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

5.3 Configure the Video Parameters

Purpose:

You can customize the image parameters including the brightness, contrast, saturation for the live view and recording effect.

Step 1 Go to **Camera**>**Display.**

Step 2 Select the camera from the drop-down list.

Step 3 Adjust the slider or click on the up/down arrow to set the value of the brightness, contrast or saturation.

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

5.4 Configure the Day/Night Switch

The camera can be set to day, night or auto switch mode according to the surrounding illumination conditions.

Step 1 Go to **Camera**>**Display.**

Step 2 Select the camera from the drop-down list.

Step 3 Select the day/night switch mode to **Day**, **Night**, **Auto** or **Auto-Switch**.

- **Auto**: The camera switches between the day mode and the night mode according to the illumination automatically.
  - The sensitivity ranges from 0 to 7, and the higher sensitivity results in the more easily to trigger the mode switch.
  - The switch time refers to the interval time between the day/night switch. You can set it from 5 sec to 120 sec.
- **Auto-Switch**: The camera switches the day mode and the night mode according to the start time and end time you set.

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

5.5 Configure Other Camera Parameters

For the connected camera, you can configure the camera parameters including the exposure mode, backlight and image enhancement.

Step 1 Go to **Camera**>**Display.**

Step 2 Select the camera from the drop-down list.

Step 3 Configure the camera parameters.

- Exposure: Set the exposure time (1/10000 to 1 sec) of camera. The larger exposure value results in the brighter image.
- Backlight: Set the wide dynamic range (0 to 100) of the camera. When the surrounding illumination and the object have larger difference in brightness, you should set the WDR value.
- Image Enhancement: For optimized image contrast enhancement.

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

Chapter 6 Live View

Live view shows you the video image getting from each camera in real time.

6.1 Start Live View

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

- You can select a window and double click a camera from the list to play the video from the camera in the selected window.
- Use the toolbar at the playing window bottom to realize the capture, instant playback, audio on/off, digital zoom, live view strategy, show information and start/stop recording, etc.

6.1.1 Digital Zoom

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

Step 1 In the live view mode, click  from the toolbar to enter the digital zoom interface.

Step 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 6-1 Digital Zoom

6.1.2 Live View Strategy

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

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

6.1.3 Switch Main/Auxiliary Port

Only the image displaying at the main port can enter main menu and achieve device operation.

You can click  in Live View mode to switch the main/auxiliary port.

6.1.4 3D Positioning

3D Positioning is for zooming in/out the specific area of live image.

Step 1 In the live view mode, click  .

Step 2 Click  .

Step 3 Operate the zoom in/out in the image.

- **Zoom in**

  Use the left key of mouse to click on the desired position in the video image and drag a rectangle area in the lower right direction to realize zoom in.

- **Zoom out**

  Use the left key of mouse to drag a rectangle area in the upper left direction to move the position to the center and enable the rectangle area to zoom out.

6.2 Target Detection

In live view mode, the target detection function can achieve smart detection, facial detection, vehicle detection, and human body detection during the last 5 seconds and the following 10 seconds.

Step 1 In the live view mode, click **Target Detection** tab to enter the target detection interface.

Step 2 Select different detection types: smart detection (), vehicle detection (), face detection () and human body detection ().

Step 3 You can select the historical analysis () or the real-time analysis () to obtain the results.

Figure 6-2 Target Detection

Step 4 Optionally, you can select channels that require picture capture. The unselected channels will not capture picture.

1. Click  at the left bottom of live view interface.
2. Select channel(s), the checked channel(s) will capture picture. All channels are selected as default.
3. Click **Finish**.

Step 5 The smart analysis results of the detection are displayed in the list. Optionally, click a result in list to play the related video.

6.3 Configure Live View Settings

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

Step 1 Go to **System** > **Live View** > **General**.

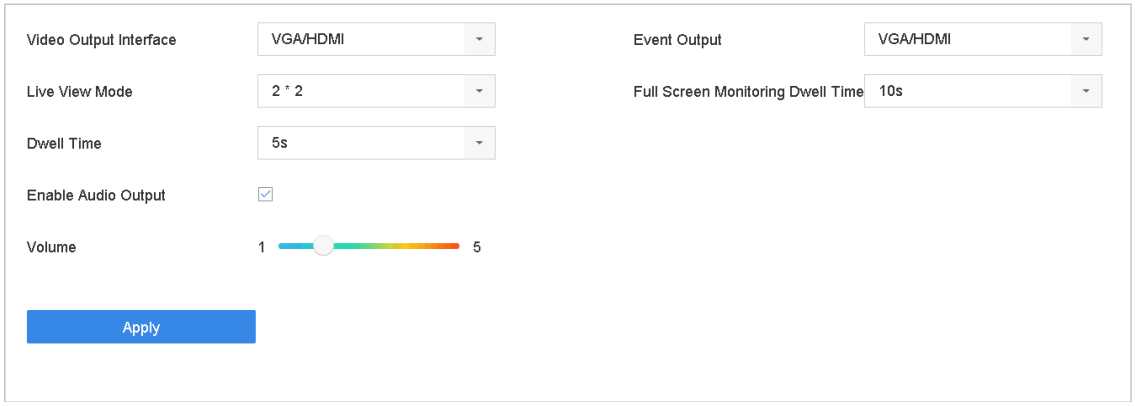


Figure 6-3 Live View-General

Step 2 Configure the live view parameters.

- **Video Output Interface:** Select the video output to configure.
- **Live View Mode:** Select the display mode for live view, e.g., 2*2, 1*5, etc.
- **Dwell Time:** The time in seconds to dwell between switching of cameras when enabling auto-switch in Live View.
- **Enable Audio Output:** Enable/disable audio output for the selected video output.
- **Volume:** Adjust the volume of live view, playback and two-way audio for the selected output interface.
- **Event Output:** Select the output to show event video.
- **Full Screen Monitoring Dwell Time:** Set the time in seconds to show alarm event screen.

Step 3 Click **OK** to save the settings.

6.4 Configure Live View Layout

Step 1 Go to **System**> **Live View**>**View Settings**.

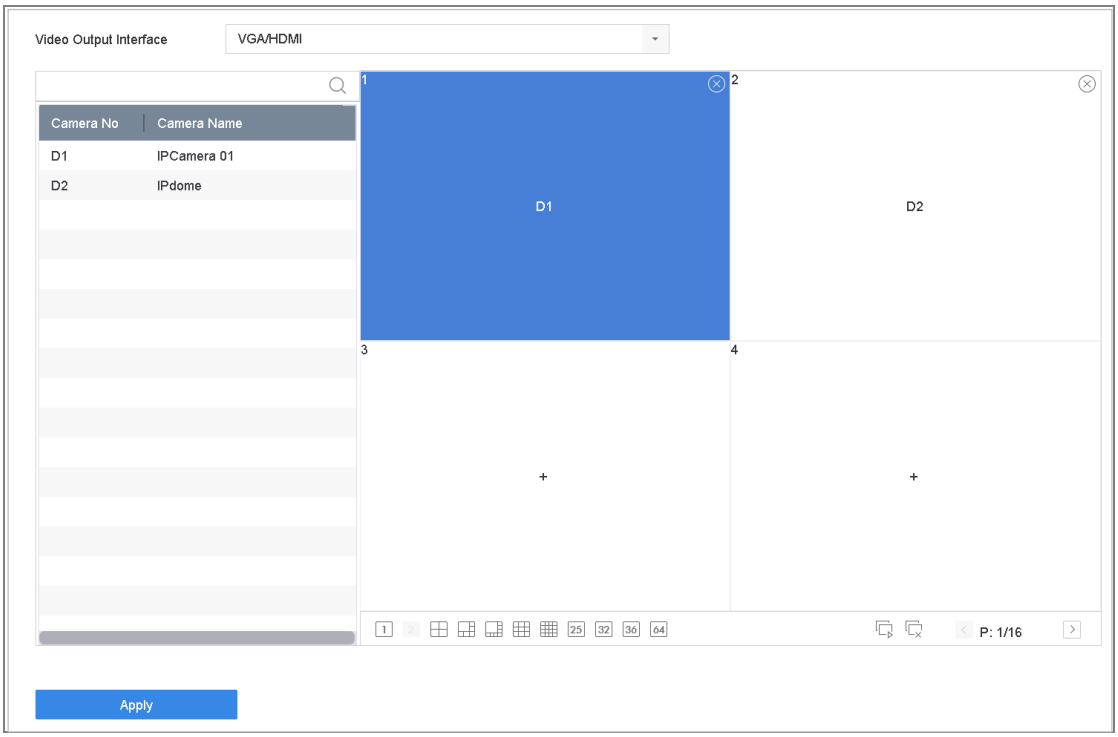


Figure 6-4 Live View

Step 2 Select the video output interface, e.g., HDMI/ VGA or channel-zero.

Step 3 Select a window division mode from the toolbar.

Step 4 Select a division window, and double-click on the camera from the list to set the camera to the window.

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

NOTE

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.

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

6.5 Configure Auto-Switch of Cameras

You can set the auto-switch of cameras to play in different display modes.

Step 1 Go to **System** > **Live View** > **General**.

Step 2 Set the video output interface, live view mode and dwell time.

- **Video Output Interface:** Select the video output interface.
- **Live View Mode:** Select the display mode for live view, e.g., 2*2, 1*5, etc.
- **Dwell Time:** The time in seconds to dwell between switching of cameras when enabling auto-switch. The range is from 5s to 300s.

Step 3 Go to **View Settings** to set the view layout.

Step 4 Click **OK** to save the settings.

6.6 Configure Channel-zero Encoding

Purpose:

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

Step 1 Go to **System**>**Live View**>**General**.

Step 2 Select the video output interface to **Channel-Zero**.

Step 3 Go to **System**>**Live View**>**Channel-Zero**.

Step 4 Check the checkbox to enable the channel-zero.

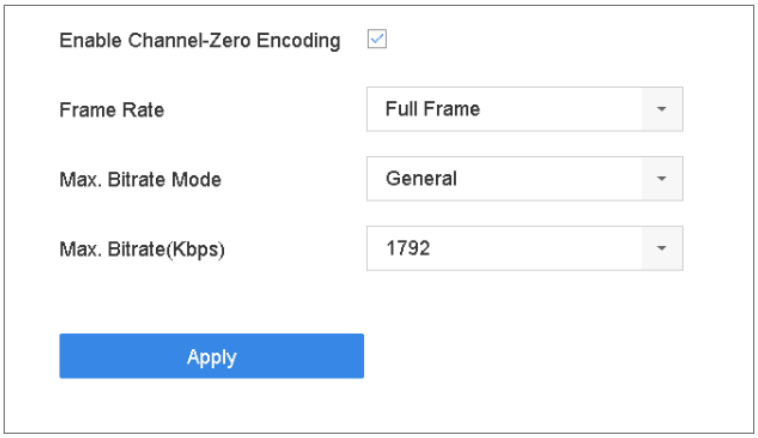


Figure 6-5 Live View- Channel-Zero Encoding

Step 5 Configure the **Frame Rate**, **Max. Bitrate Mode** and Max. Bitrate. The higher frame rate and bitrate settings result in the higher requirement of bandwidth.

Step 6 Click **Apply.**

Result:

You can view all of the channels in one screen using the CMS or web browser.

Chapter 7 PTZ Control

7.1 PTZ Control Wizard

Before you start

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

Purpose

Follow the PTZ control wizard to guide you through the basic PTZ operation.

Step 1 Click  on the quick settings toolbar of the PTZ camera live view. The PTZ control wizard pops up as below.

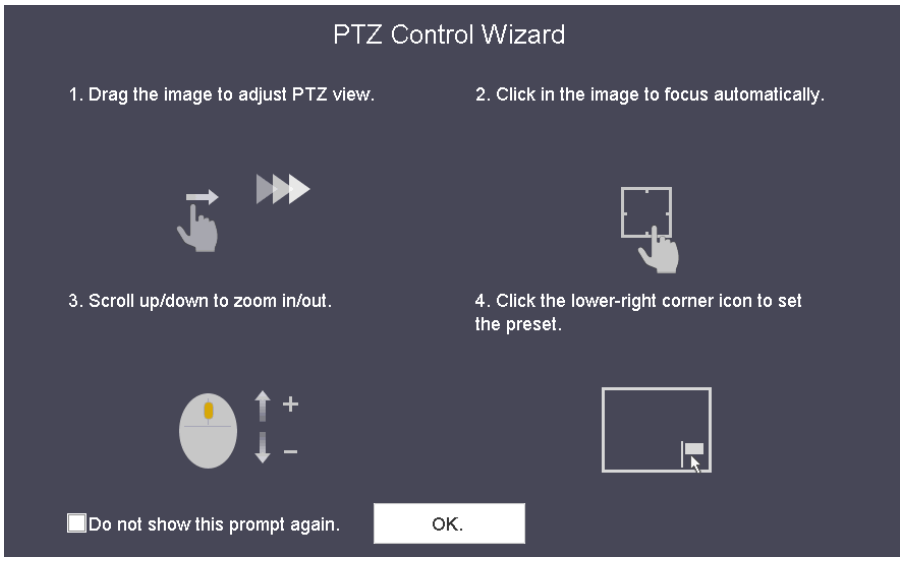


Figure 7-1 PTZ Control Wizard

Step 2 Follow the wizard to adjust the PTZ view, focus, and zoom in/out the camera.

Step 3 (Optional) Check *Do not show this prompt again.*

Step 4 Click **OK** to exit.

7.2 ConfigurePTZ 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.

Step 1 Click  on the quick settings toolbar of the PTZ camera live view. The PTZ control panel displays on the right of the interface.

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

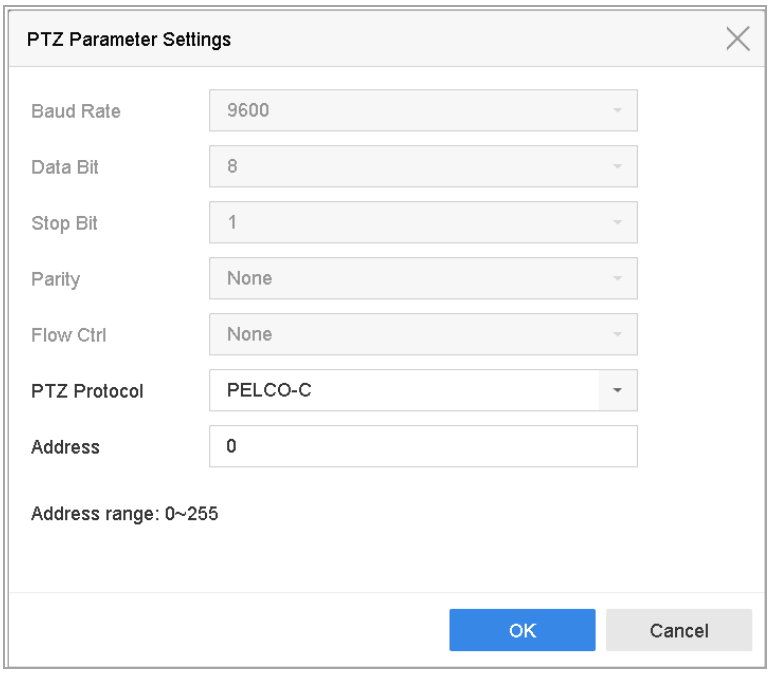


Figure 7-2 PTZ Parameters Settings

Step 3 Edit the parameters of the PTZ camera.

NOTE

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

Step 4 Click **OK** to save the settings.

7.3 Set PTZ Presets, Patrols & Patterns

Before you start:

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

7.3.1 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.

Step 1 Click on the quick settings toolbar of the PTZ camera live view.

The PTZ control panel displays on the right of the interface.

Step 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.

Step 3 Click  in the lower right corner of live view to set the preset.

Figure 7-3 Set Preset

Step 4 Select the preset No. (1~255) from the drop-down list.

Step 5 Enter the preset name in the text field.

Step 6 Click **Apply** to save the preset.

Step 7 Repeat steps 2-6 to save more presets.

Step 8 (Optional) Click **Cancel** to cancel the location information of the preset.

Step 9 (Optional) Click  in the lower right corner of live view to view the configured presets.

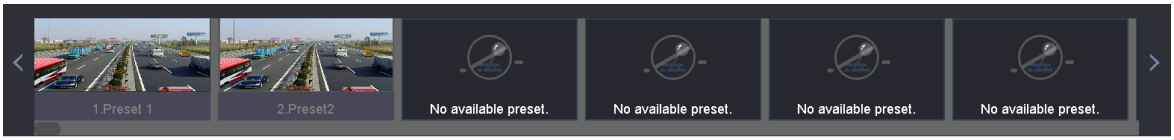


Figure 7-4 View the Configured Presets

7.3.2 Call a Preset

Purpose:

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

Step 1 Click  on the quick settings toolbar of the PTZ camera live view.

Step 2 Click  in the lower right corner of live view.

Step 3 Select the preset No. from the drop-down list.

Step 4 Click **Call** to call it.

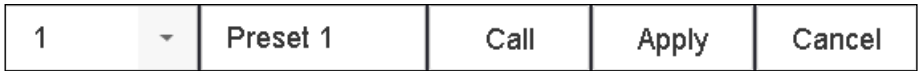


Figure 7-5 Call Preset (1)

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

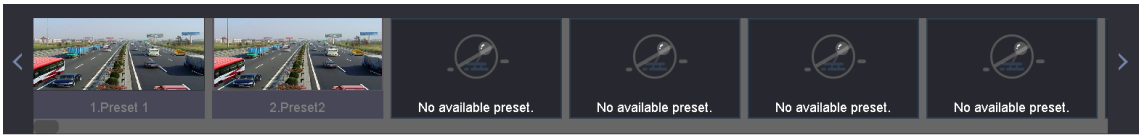


Figure 7-6 Call Preset (2)

7.3.3 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.

Step 1 Click  on the quick settings toolbar of the PTZ camera live view.

The PTZ control panel displays on the right of the interface.

Step 2 Click **Patrol** to configure patrol.

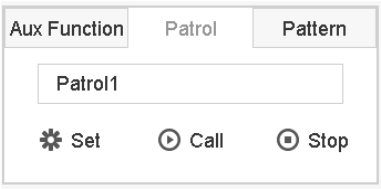


Figure 7-7 Patrol Configuration

Step 3 Select the patrol No. in the text field.

Step 4 Click **Set** to enter the Patrol Settings interface.

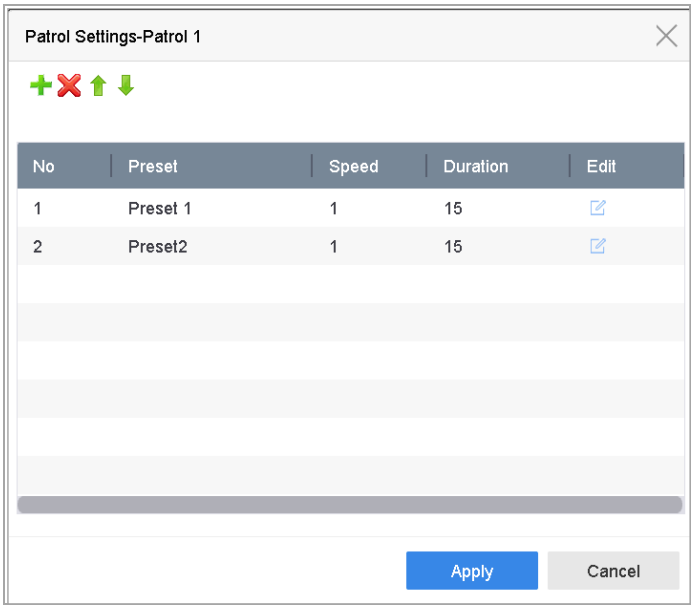


Figure 7-8 Patrol Settings

Step 5 Click  to add key point for the patrol.

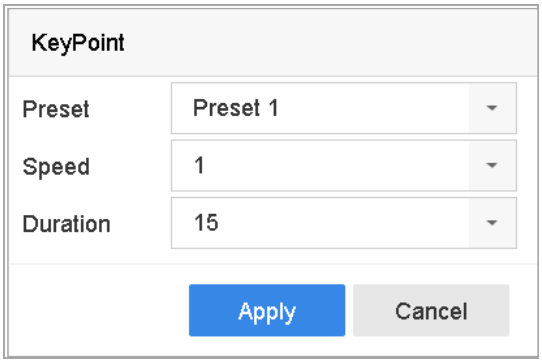


Figure 7-9 Key Point Configuration

1) 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.

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

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

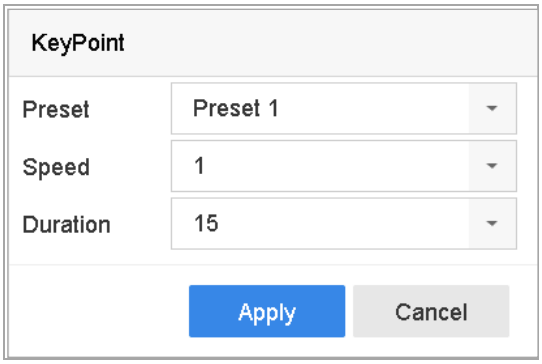


Figure 7-10 Edit Key Point

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

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

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

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

7.3.4 Call a Patrol

Purpose:

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

Step 1 Click on the quick settings toolbar of the PTZ camera live view.

The PTZ control panel displays on the right of the interface.

Step 2 Click **Patrol** on the PTZ control panel.

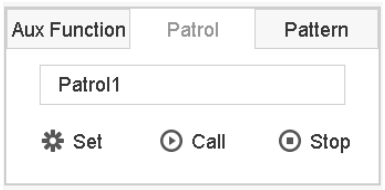


Figure 7-11 Patrol Configuration

Step 3 Select a patrol in the text field.

Step 4 Click **Call** to call it.

Step 5 (Optional) Click **Stop** to stop calling it.

7.3.5 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.

Step 1 Click  on the quick settings toolbar of the PTZ camera live view.

The PTZ control panel displays on the right of the interface.

Step 2 Click **Pattern** to configure pattern.

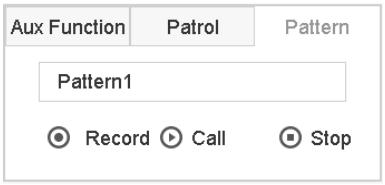


Figure 7-12 Pattern Configuration

Step 3 Select the pattern No. in the text field.

Step 4 Set the pattern.

1) Click **Record** to start recording.
2) Click corresponding buttons on the control panel to move the PTZ camera.
3) Click **Stop** to stop recording.

The movement of the PTZ is recorded as the pattern.

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

7.3.6 Call a Pattern

Purpose:

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

Step 1 Click  on the quick settings toolbar of the PTZ camera live view.

The PTZ control panel displays on the right of the interface.

Step 2 Click **Pattern** to configure pattern.

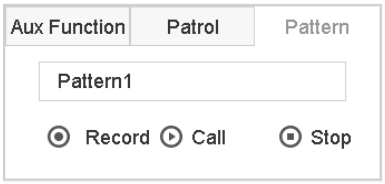


Figure 7-13 Pattern Configuration

Step 3 Select a pattern in the text field.

Step 4 Click **Call** to call it.

Step 5 (Optional) Click **Stop** to stop calling it.

7.3.7 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.

NOTE

This function is supported by some certain models.

Step 1 Click  on the quick settings toolbar of the PTZ camera live view.

The PTZ control panel displays on the right of the interface.

Step 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.

NOTE

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 180º.

7.3.8 Call Linear Scan

NOTE

Before operating this function, make sure the connected camera supports the linear scan.

Purpose:

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

Step 1 Click  on the quick settings toolbar of the PTZ camera live view.

The PTZ control panel displays on the right of the interface.

Step 2 Click **Linear Scan** to start the linear scan and click it again to stop it.

Step 3 (Optional) Click **Restore** to clear the defined left limit and right limit data.

NOTE

Reboot the camera to take the settings into effect.

7.3.9 One-touch Park

NOTE

Before operating this function, make sure the connected camera supports the linear scan.

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).

Step 1 Click  on the quick settings toolbar of the PTZ camera live view.

The PTZ control panel displays on the right of the interface.

Step 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.

NOTE

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

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

7.4 Auxiliary Functions

Before you start

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

Purpose

You can operate the auxiliary functions including light, wiper, 3D positioning, and center on the PTZ control panel.

Step 1 Click  on the quick settings toolbar of the PTZ camera live view.

The PTZ control panel displays on the right of the interface.

Step 2 Click **Aux Function**.

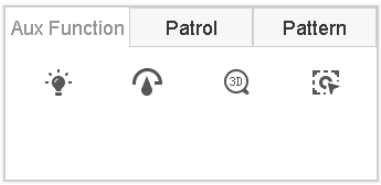


Figure 7-14 Aux Function Configuration

Step 3 Click the icons to operate the aux functions. See the table for the description of the icons.

Table 7-1 Description of Aux Functions Icons

Icon	Description
	Light on/off
	Wiper on/off
	3D positioning
	Center

Chapter 8 Storage

8.1 Storage Device Management

8.1.1 Install the HDD

Before startup of the device, install and connect the HDD to the device. Refer to the Quick Start Guide for the installation instructions.

8.1.2 Add the Network Disk

You can add the allocated NAS or disk of IP SAN to device, and use it as network HDD. Up to 8 network disks can be added.

Adding NAS

Step 1 Go to **Storage** > **Storage Device**.

Step 2 Click **Add** to enter the Custom Add interface.

Step 3 Select the NetHDD from the drop-down list.

Step 4 Select the type to NAS.

Step 5 Enter the NetHDD IP address in the text field.

Step 6 Click **Search** to search the available NAS disks.

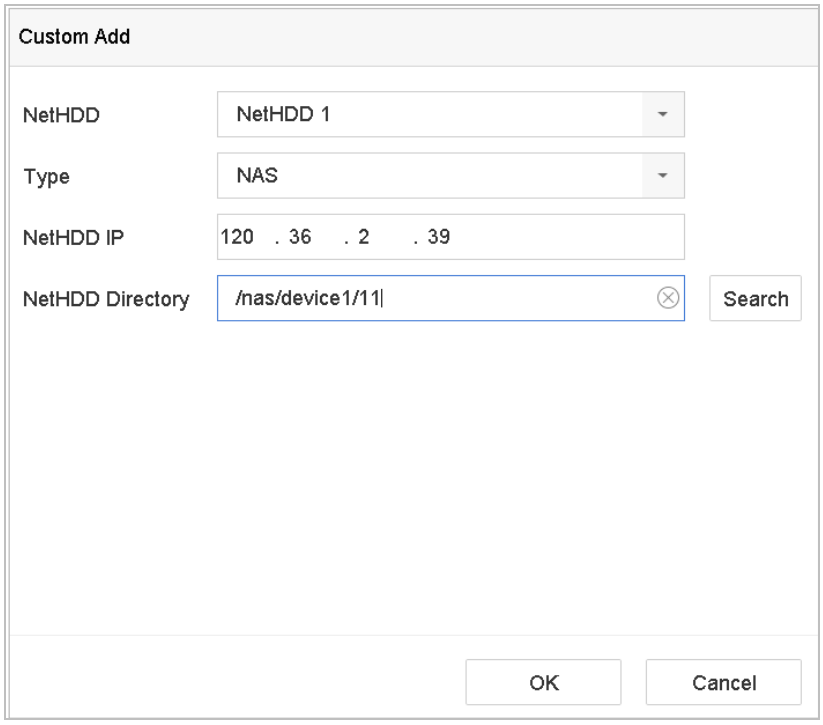


Figure 8-1 Add NAS Disk

Step 7 Select the NAS disk from the list shown below, or you can manually enter the directory in the text field of NetHDD Directory.

Step 8 Click the **OK** to complete the adding of the NAS disk.

Result:

After having successfully added the NAS disk, return to the HDD Information menu. The added NetHDD will be displayed in the list.

Adding IP SAN

Step 1 Go to **Storage** > **Storage Device**.

Step 2 Click **Add** to enter the Custom Add interface.

Step 3 Select the NetHDD from the drop-down list.

Step 4 Select the type to IP SAN.

Step 5 Enter the NetHDD IP address in the text field.

Step 6 Click **Search** to search the available IP SAN disks.

Step 7 Select the IP SAN disk from the list shown below.

Step 8 Click **OK** to complete the adding of the IP SAN disk.

Up to 1 IP SAN disk can be added.

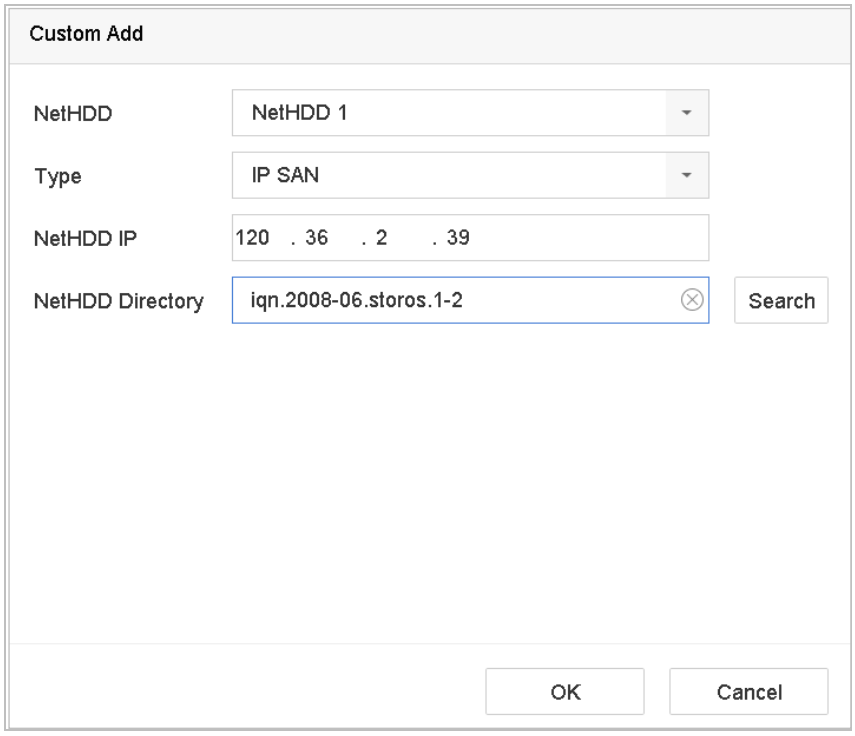


Figure 8-2 Add IP SAN Disk

Result:

After having successfully added the IP SAN disk, return to the HDD Information menu. The added NetHDD will be displayed in the list.

NOTE

If the installed HDD or NetHDD is uninitialized, please select it and click the **Init** button for initialization.

8.1.3 Configure eSATA for Data Storage

When there is an external eSATA device connected to device, you can configure eSATA for the data storage, and you can manage the eSATA in the device.

Step 1 Click **Storage**>**Advanced**.

Step 2 Select the eSATA type to Export or Record/Capture from the dropdown list of **eSATA**.

Export: use the eSATA for backup.

Record/Capture: use the eSATA for record/capture. Refer to the following steps for operating instructions.

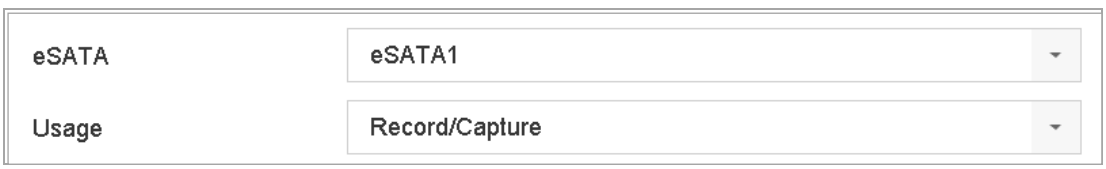


Figure 8-3 Set eSATA Mode

Step 3 When the eSATA type is selected to Record/Capture, enter the storage device interface.

Step 4 Edit the property of the selected eSATA, or initialize it is required.

8.2 Storage Mode

8.2.1 Configure HDD Group

Purpose:

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

Step 1 Go to **Storage**> **Storage Device**.

Step 2 Check the checkbox to select the HDD to set the group.

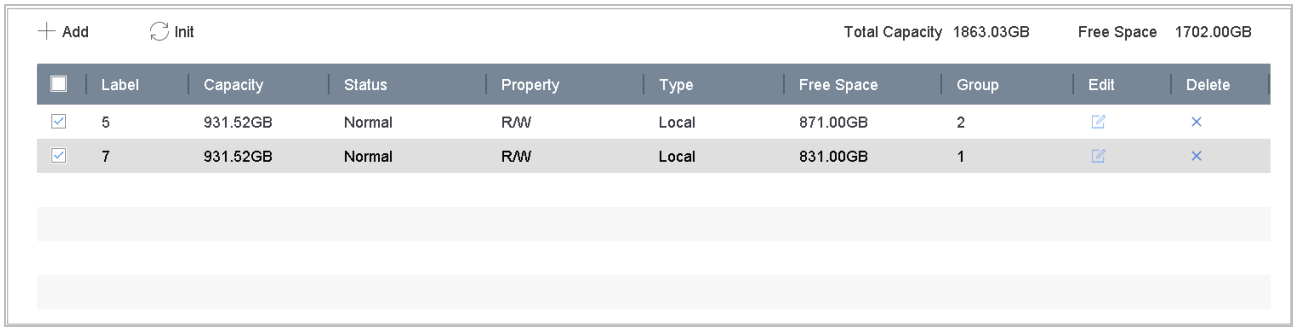


Figure 8-4 Storage Device

Step 3 Click  to enter the Local HDD Settings interface.

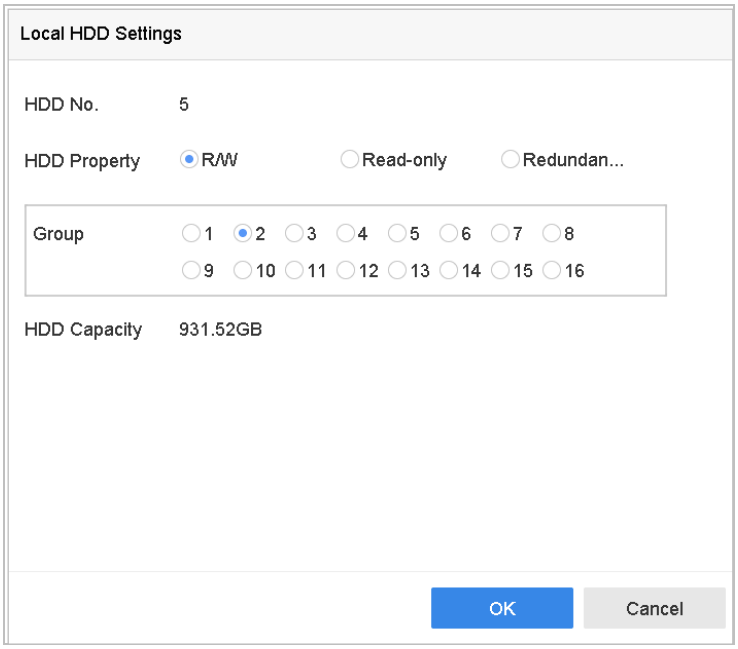


Figure 8-5 Local HDD Settings

Step 4 Select the Group number for the current HDD.

Step 5 Click **OK**.

NOTE

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

Step 6 Go to **Storage**> **Storage Mode**.

Step 7 Check the checkbox of **Group** tab.

Step 8 Select the group No. from the list.

Step 9 Check the checkbox to select the IP camera (s) to record/capture on the HDD group.

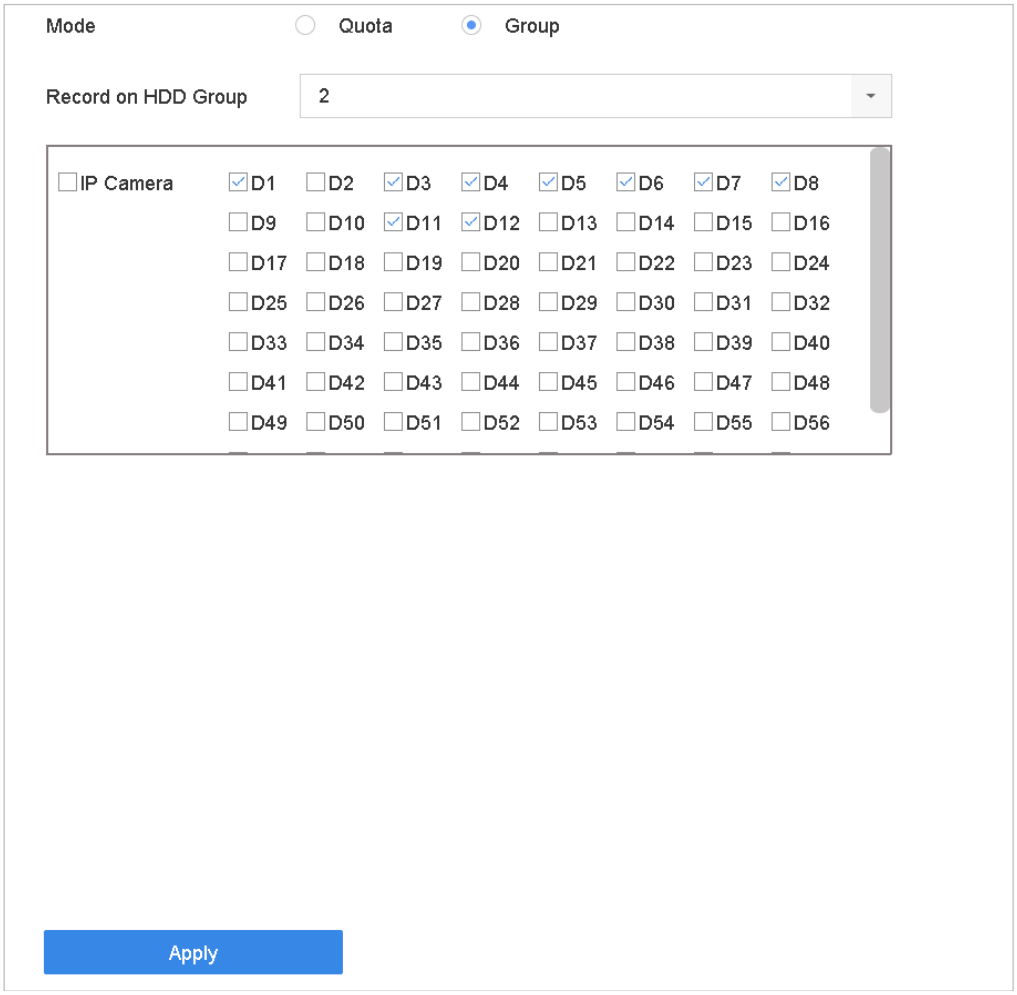


Figure 8-6 Storage Mode-HDD Group

Step 10 Click **Apply**.

NOTE

Reboot the device to activate the new storage mode settings.

8.2.2 Configure HDD Quota

Purpose:

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

Step 1 Go to **Storage**> **Storage Mode**.

Step 2 Check the checkbox of **Quota** tab.

Step 3 Select a camera to set quota.

Step 4 Enter the storage capacity in the text fields of **Max. Record Capacity (GB)** and **Max. Picture Capacity (GB)**.

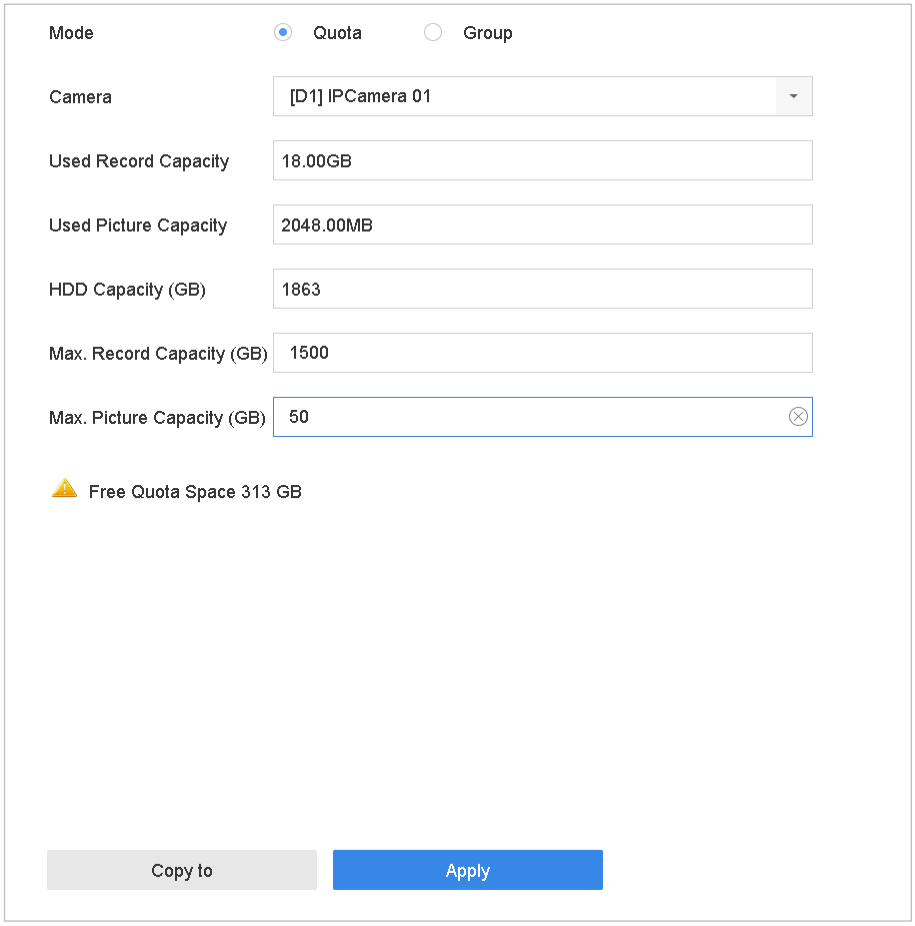


Figure 8-7 Storage Mode-HDD Quota

Step 5 (Optional) You can click **Copy to** if you want to copy the quota settings of the current camera to other cameras.

Step 6 Click the **Apply** button to apply the settings.

NOTE

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

NOTE

Reboot the device to activate the new storage mode settings.

8.3 Recording Parameters

8.3.1 Main Stream

The 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.

Frame Rate (FPS - Frames Per Second): 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+ Mode: The H.264+ mode helps to ensure the high video quality with a lowered bitrate. It can effectively reduces the need of bandwith and HDD storage space.

NOTE

A higher resolution, frame rate and bitrate setting will provide you the better video quality, but it will also require more internet bandwidth and use more storage space on the hard disk drive.

8.3.2 Sub-Stream

The sub-stream is a second codec that runs alongside the mainstream. It allows you to reduce the outgoing internet bandwidth without sacrificing your direct recording quality.

The sub-stream is often exclusively used by smartphone applications to view live video. Users with limited internet speeds may benefit most from this setting.

8.3.3 Picture

The picture refers to the live picture capture in continuous or event recording type.

Picture Quality: set the picture quality to low, medium or high. The higher picture quality results in more storage space requirement.

Interval: the interval of capturing live picture.

8.3.4 ANR

ANR (Automatic Network Replenishment) function which enables the IP camera to save the recording files in the local storage when the network is disconnected, and when the network is resumed, it uploads the files to the device.

Enable the ANR (Automatic Network Replenishment) function via the web browser (**Configuration** > **Storage** > **Schedule Settings** > **Advanced**).

8.3.5 Configure Advanced Recording Settings

Step 1 Go to **Storage** > **Schedule Settings > Record Schedule/Capture Schedule**.

Step 2 Check the checkbox of **Enable** to enable scheduled recording.

Step 3 Click **Advanced** to set the recording parameters.

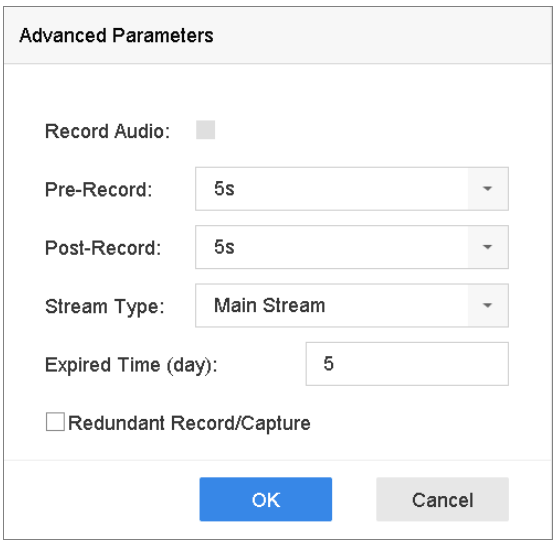


Figure 8-8 Advanced Record Settings

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.

Redundant Record/Capture: By enabling redundant record or capture you save the record and captured picture in the redundant HDD. See *Chapter Configure Redundant Recording and Capture*.

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.

Step 4 Click **OK** to save the settings.

8.4 Configure Recording Schedule

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

Before you start

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

Refer to the *Quick Start Guide* for the HDD installation.

Refer to *Chapter 8.1.2* Add the Network Disk for network HDD connections.

Step 1 Go to **Storage** > **Recording Schedule**.

Step 2 Select a camera.

Step 3 Check the **Enable Schedule**.

Step 4 Select a **Record Type**. The record type can be Continuous, Motion Detection, Alarm, Motion | Alarm, Motion & Alarm, and Event.

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.

Step 5 Select a day and click-and-drag the mouse on the time bar to set the record schedule.

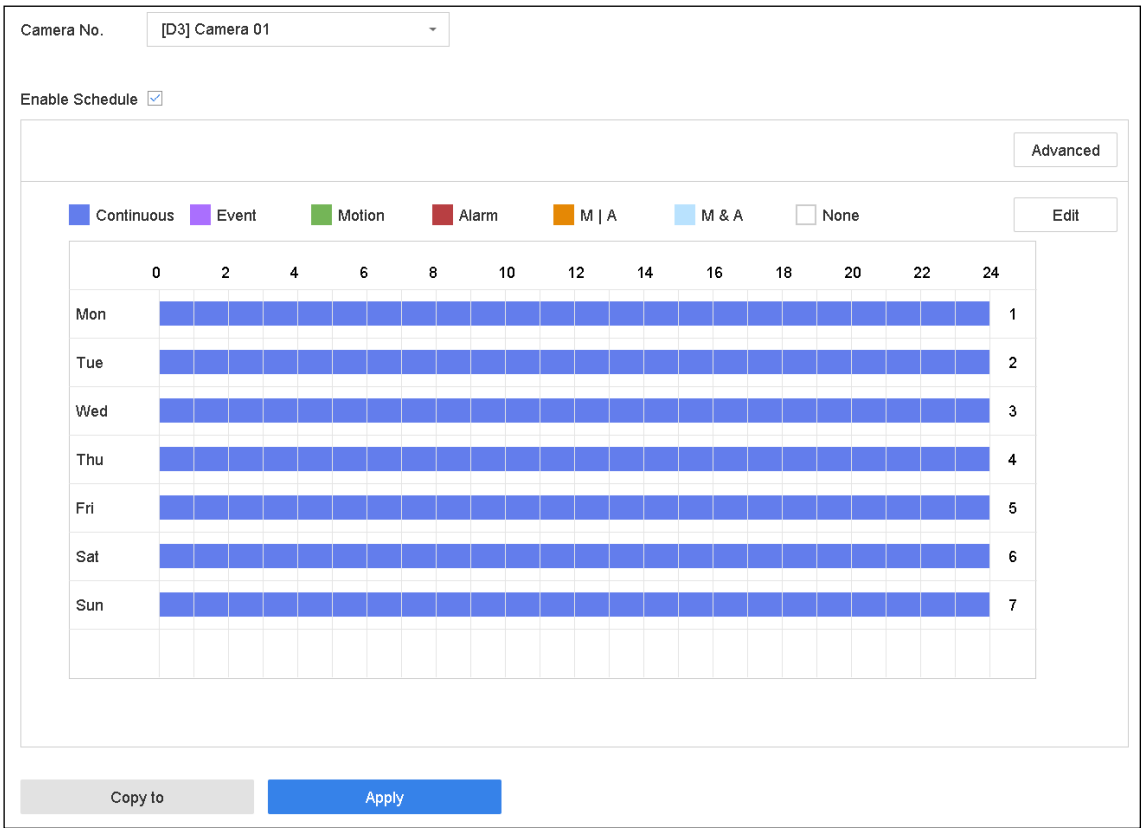


Figure 8-9 Record Schedule

Step 6 Repeat the above steps to schedule recording or capture for other days in the week.

NOTE

The all-day continuous recording is configured for the device by factory default.

Step 7 (Optional) Copy the schedule settings of the one day to the other days of the week or holiday.

1) Click the  tab.
2) Select the day (s) to duplicate with the same schedule settings.
3) Click **OK**.

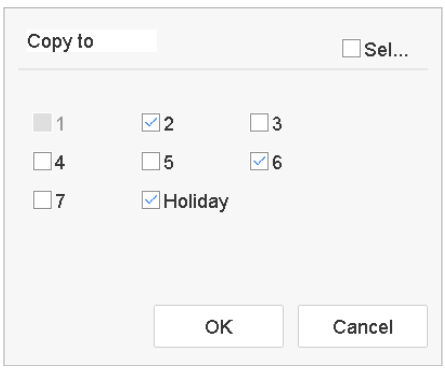


Figure 8-10 Copy Schedule to Other Days

Step 8 Click **Apply** to save the settings.

NOTE

To enable Motion, Alarm, M | A (motion or alarm), M & A (motion and alarm) and Event triggered recording and capture, you must configure the motion detection settings, alarm input settings and other events as well. Please refer to Chapter 11 Event and Alarm Settings and Chapter 12

for details for details.

8.5 Configure Continuous Recording

Step 1 Go to **Camera** > **Encoding Parameters** > **Recording Parameters**.

Step 2 Set the continuous main stream/sub-stream recording parameters for the camera.

Step 3 Go to **Storage** > **Recording Schedule**.

Step 4 Select the recording type to **Continuous**.

Step 5 Drag the mouse on the time bar to set the continuous recording schedule. Refer to Chapter 8.4 Configure Recording Schedule for details.

8.6 Configure Motion Detection Triggered Recording

You can configure the recording triggered by the motion detection event.

Step 1 Go to **System** > **Event > Normal Event > Motion Detection**.

Step 2 Configure the motion detection and select the channel (s) to trigger the recording when motion event occurs. Refer to Chapter 11.3 Configure Motion Detection Alarm for details.

Step 3 Go to **Camera** > **Encoding Parameters** > **Recording Parameters**.

Step 4 Set the event main stream/sub-stream recording parameters for the camera.

Step 5 Go to **Storage** > **Recording Schedule**.

Step 6 Select the recording type to **Motion**.

Step 7 Drag the mouse on the time bar to set the motion detection recording schedule. Refer to Chapter 8.4 Configure Recording Schedule for details.

8.7 Configure Event Triggered Recording

You can configure the recording triggered by the motion detection, motion detection and alarm, face detection, vehicle detection, line crossing detection, etc.

Step 1 Go to **System** > **Event**.

Step 2 Configure the event detection and select the channel (s) to trigger the recording when event occurs. Refer to Chapter 11 Event and Alarm Settings and Chapter 12

for details.

Step 3 Go to **Camera** > **Encoding Parameters** > **Recording Parameters**.

Step 4 Set the event main stream/sub-stream recording parameters for the camera.

Step 5 Go to **Storage** > **Recording Schedule**.

Step 6 Select the recording type to **Event**.

Step 7 Drag the mouse on the time bar to set the event detection recording schedule. Refer to Chapter 8.4 Configure Recording Schedule for details.

8.8 Configure Alarm Triggered Recording

You can configure the recording triggered by the motion detection, face detection, vehicle detection, line crossing detection, etc.

Step 1 Go to **System** > **Event** > **Normal Event > Alarm Input**.

Step 2 Configure the alarm input and select the channel (s) to trigger the recording when alarm occurs.

Refer to Chapter 11 Event and Alarm Settings and Chapter 12

for details for details.

Step 3 Go to **Camera** > **Encoding Parameters** > **Recording Parameters**.

Step 4 Set the event main stream/sub-stream recording parameters for the camera.

Step 5 Go to **Storage** > **Recording Schedule**.

Step 6 Select the recording type to **Alarm**

Step 7 Drag the mouse on the time bar to set the alarm recording schedule. Refer to Chapter 8.4 Configure Recording Schedule for details.

8.9 Configure Picture Capture

The picture refers to the live picture capture in continuous or event recording type.

Step 1 Go to **Camera** > **Encoding Parameters** > **Capture**.

Step 2 Set the picture parameters.

- **Resolution**: set the resolution of the picture to capture.
- **Picture Quality**: set the picture quality to low, medium or high. The higher picture quality results in more storage space requirement.
- **Interval**: the interval of capturing live picture.

Step 3 Go to **Storage** > **Capture Schedule**.

Step 4 Select the camera to configure the picture capture.

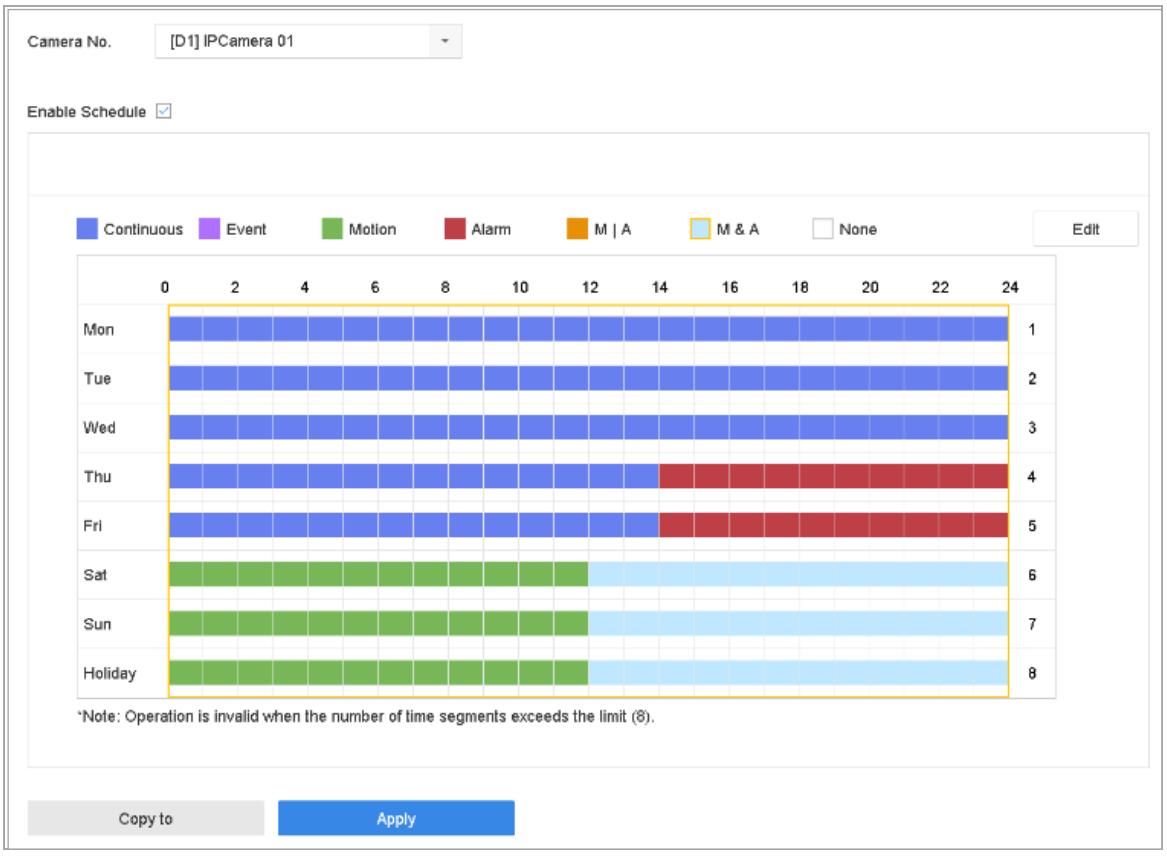


Figure 8-11 Set Picture Capture Schedule

Step 5 Set the picture capture schedule. Refer to Chapter 8.4 Configure Recording Schedule for details.

8.10 Configure Holiday Recording and Capture

Purpose:

Follow the steps to configure the record or capture schedule on holiday for that year. You may want to have different plan for recording and capture on holiday.

Step 1 Go to **System** > **Holiday Setting**s.

Step 2 Select a holiday item from the list and click .

Step 3 Check the **Enable** to configure the holiday.

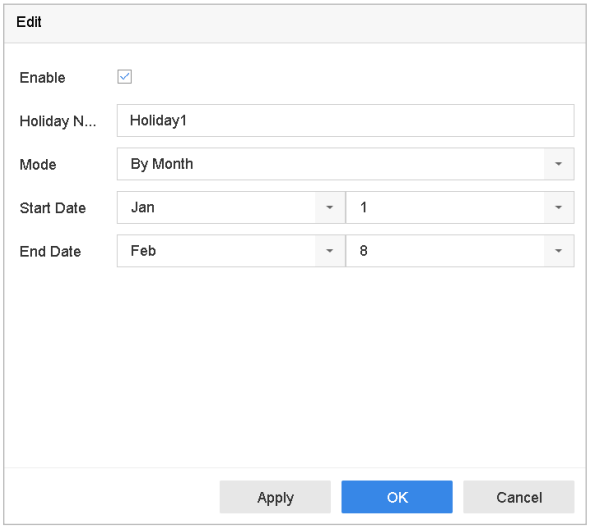


Figure 8-12 Edit Holiday Settings

1) Edit the holiday name.
2) Select the mode to by date, by week or by month.
3) Set the start and end date of the holiday.
4) Click **OK**.

Step 4 Set the schedule for the holiday recording. Refer to Chapter 8.4 Configure Recording Schedule for details.

8.11 Configure Redundant Recording and Capture

Purpose:

Enabling redundant recording and capture, which means saving the record files and captured pictures not only in the R/W HDD but also in the redundant HDD, will effectively enhance the data safety and reliability. .

NOTE

You must set the storage mode to *Group* before you set the HDD property to Redundancy. For detailed information, please refer to Chapter 8.2.1 Configure HDD Group. There should be at least another HDD which is in Read/Write status.

Step 1 Go to **Storage** > **Storage Device**.

Step 2 Select a **HDD** from the list and Click  to enter the Local HDD Settings interface.

Step 3 Set the HDD property to **Redundancy**.

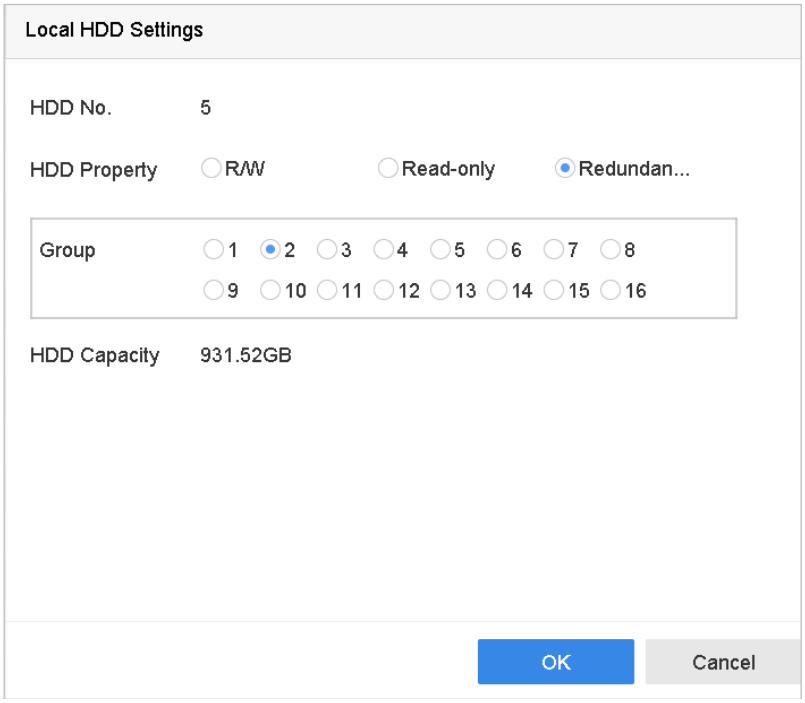


Figure 8-13 HDD Property-Redundancy

Step 4 Go to **Storage** > **Schedule Settings > Record Schedule/Capture Schedule**.

Step 5 Click **Advanced** to set the camera recording parameters.

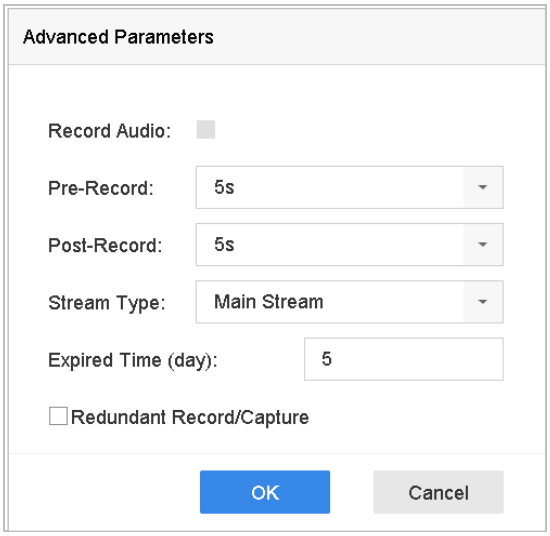


Figure 8-14 Record Parameters

Step 6 Check the checkbox of **Redundant Record/Capture**.

Step 7 Click **OK** to save settings.

Chapter 9 File Management

9.1 Search and Export All Files

9.1.1 Search Files

Purpose

Specify detailed conditions to search videos and pictures.

Step 1 Go to **File Management** > **All Files**.

Step 2 Specify detailed conditions, including time, camera, event type, etc.

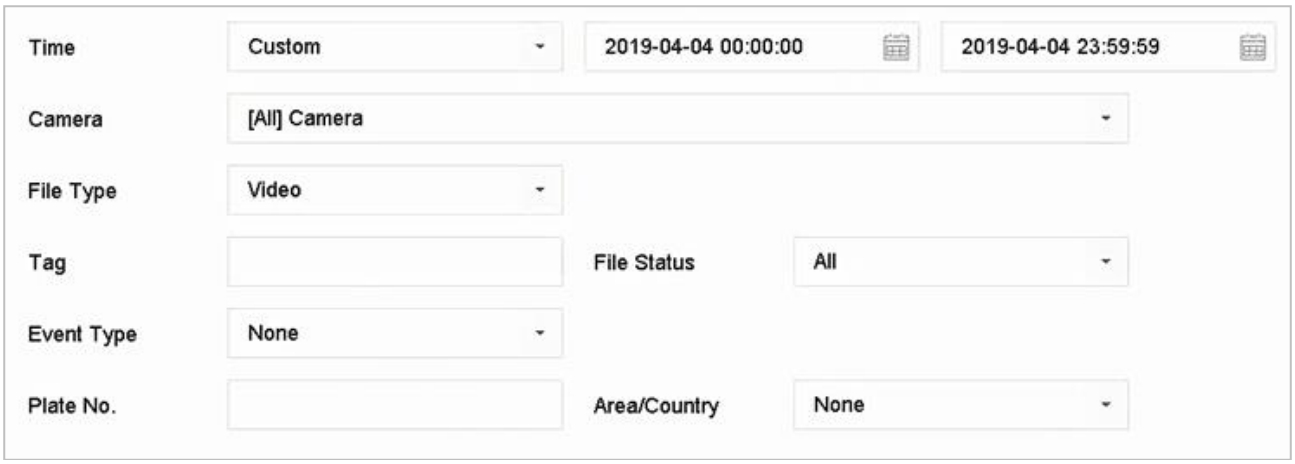


Figure 9-1 Search All Files

Step 3 Click **Search** to display results. The matched files will be displayed.

9.1.2 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.

Step 1 Search files to export. For details, see *9.1.1 Search Files*.

Step 2 Click to select files and click **Export**.

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

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

9.2 Search and Export Human Files

9.2.1 Search Human 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.

Step 1 Go to **File Management** > **Human Files**.

Step 2 Select **Time** and **Camera** to search.

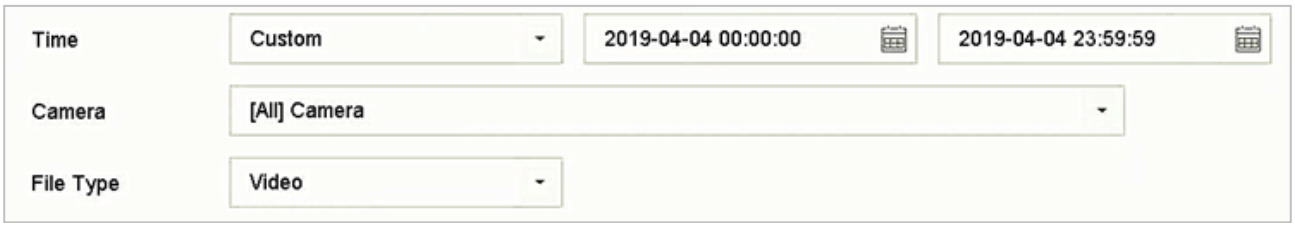


Figure 9-2 Search Human Files

Step 3 Click **Search** to display results. The matched files are displayed in thumbnail or list.

Step 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.
- **Source Picture**: Display the search results of original picture captured by camera.

9.2.2 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.

Step 1 Search for the human files to export. For details, see *9.2.1 Search Human Files*.

Step 2 Click to select files and click **Export**.

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

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

9.3 Search and Export Vehicle Files

9.3.1 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.

Step 1 Go to **File Management** > **Vehicle Files**.

Step 2 Specify detailed conditions, including **Time, Camera**, **Plate No.**, and **Area/Country**.

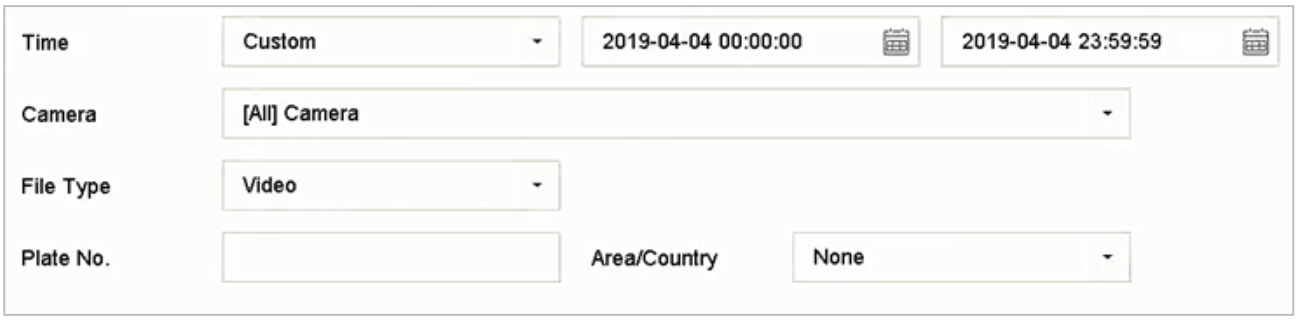


Figure 9-3 Search Vehicle Files

Step 3 Click **Search** to display results. The matched files are displayed in thumbnail or list.

Step 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.

9.3.2 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.

Step 1 Search for the vehicle files to export. For details, see *9.3.1 Search Vehicle Files*.

Step 2 Optionally, Check **Backup License Plate Statistics Info** to export license plate statistics information later.

Step 3 Select files as your desire.

Step 4 Click **Export**.

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

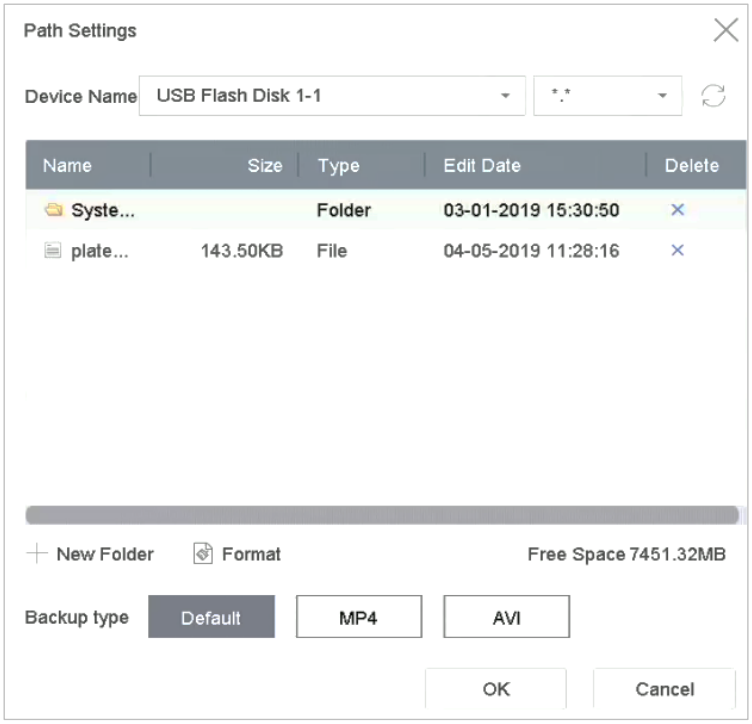


Figure 9-4 Export Vehicle File

Step 6 Click **OK** to export files to backup device.

9.4 Search History Operation

9.4.1 Save Search Condition

Purpose

You can save the search conditions for future reference and quick search.

Step 1 Go to **File Management** > **All Files/People Appearance File/Vehicle File**.

Step 2 Set the search conditions.

Step 3 Click **Save**.

Step 4 Enter a name in text field and click **Finished**. The saved search conditions will be displayed in search history list.

9.4.2 Call Search History

Purpose:

You can quickly search files by calling search history.

Step 1 Go to **File Management** > **All Files/Human Files/Vehicle Files**.

Step 2 Click a search conditon to quickly search files.

Chapter 10 Playback

10.1 Play Video Files

10.1.1 Instant Playback

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.

Step 1 On the live view window of the selected camera, move the cursor to the window bottom to access the toolbar.

Step 2 Click  to start instant playback.

Figure 10-1 Playback Interface

10.1.2 Play Normal Video

Step 1 Go to **Playback.**

Step 2 Check one or more cameras in the camera list to start playing the video.

Step 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 10.2 Playback Operations 8.2.
- Click the channel(s) to execute simultaneous playback of multiple channels.

Figure 10-2 Playback Interface

NOTE

The playing speed of 256X is supported.

10.1.3 Play Smart Searched Video

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.

NOTE

The smart playback must be in the single-channel playing mode.

Step 1 Go to **Playback**.

Step 2 Start playing the video of camera.

Step 3 Click **Smart**.

Step 4 From the toolbar at the bottom of the playing window, click the motion/line crossing/ intrusion icon for search.

Figure 10-3 Playback by Smart Search

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

- **Line Crossing Detection**

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

- **Intrusion Detection**

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

- **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.

10.1.4 Play Custom Searched Files

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

Step 1 Go to **Playback**.

Step 2 Select a camera or cameras from the list.

Step 3 Click **Custom Search** on the left bottom to enter the Search Condition interface.

Step 4 Enter the search conditions for the files, e.g., time, file status, event type, etc.

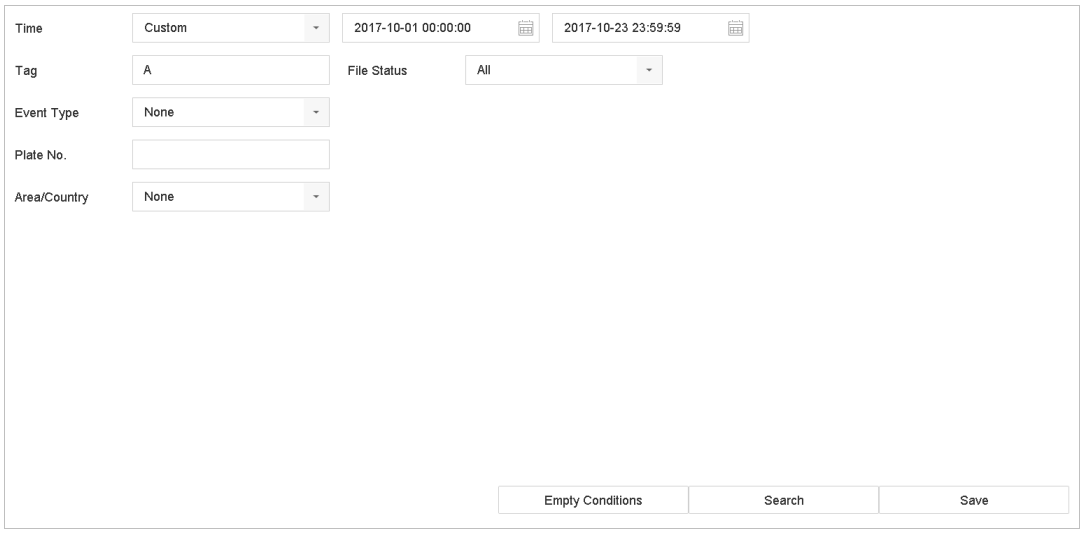


Figure 10-4 Custom Search

Step 5 Click **Search.**

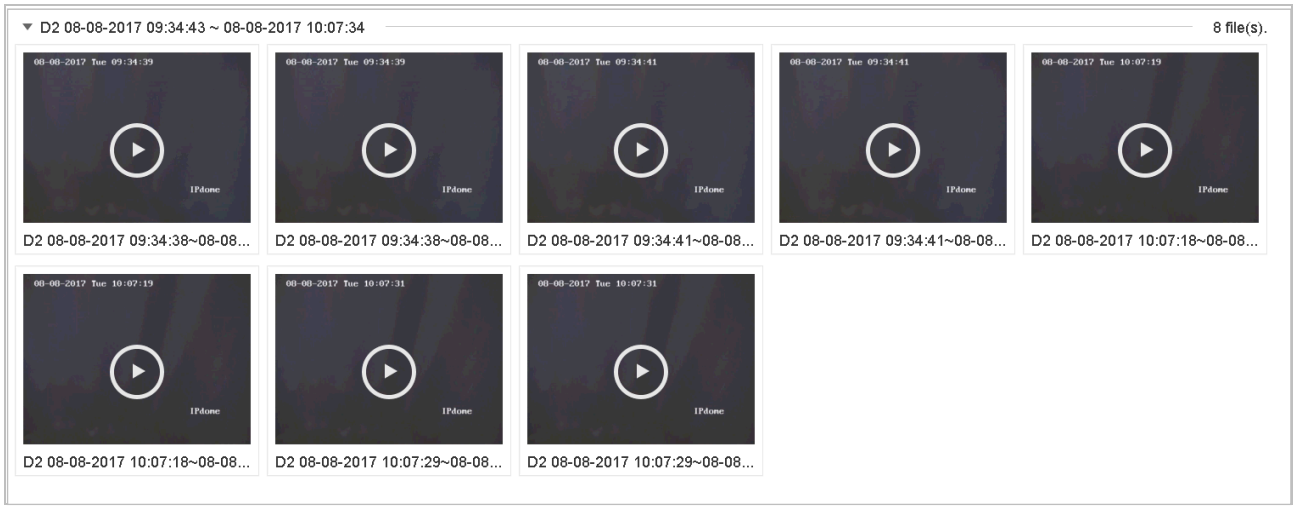


Figure 10-5 Custom Searched Video Files

Step 6 On the search results interface, select a file and click to start playing the video.

10.1.5 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

Step 1 Go to **Playback**.

Step 2 Search and play back the video file(s).

Step 3 Click  to add the tag.

Step 4 Edit the tag information.

Step 5 Click **OK**.

NOTE

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

Edit Tag Files

Step 1 Go to Playback.

Step 2 Click **Tag**.

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

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

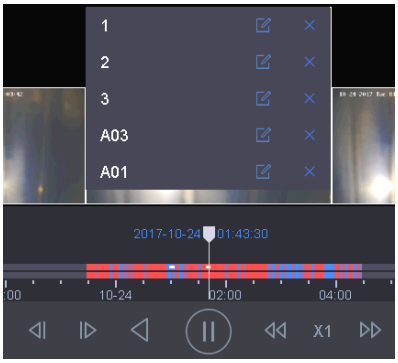


Figure 10-6 Edit Tag Files

Step 4 Click  to edit the tag name.

Step 5 Click **OK**.

Play Tag Files

Step 1 Go to **Playback**.

Step 2 Click **Custom Search** on the left bottom to enter the Search Condition interface.

Step 3 Enter the search conditions for the tag files, including the time and the tag keyword.

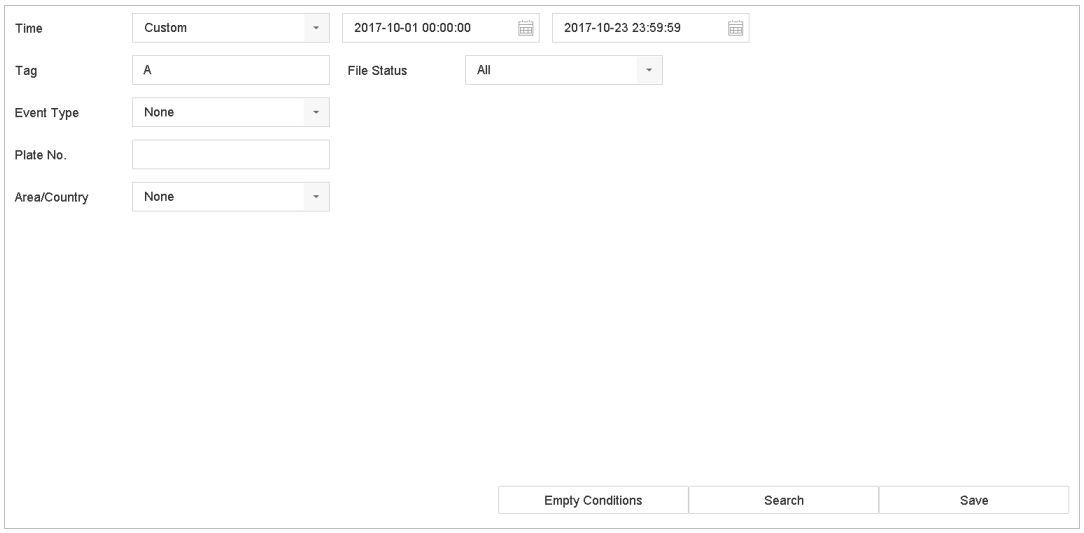


Figure 10-7 Tag Search

Step 4 Click **Search.**

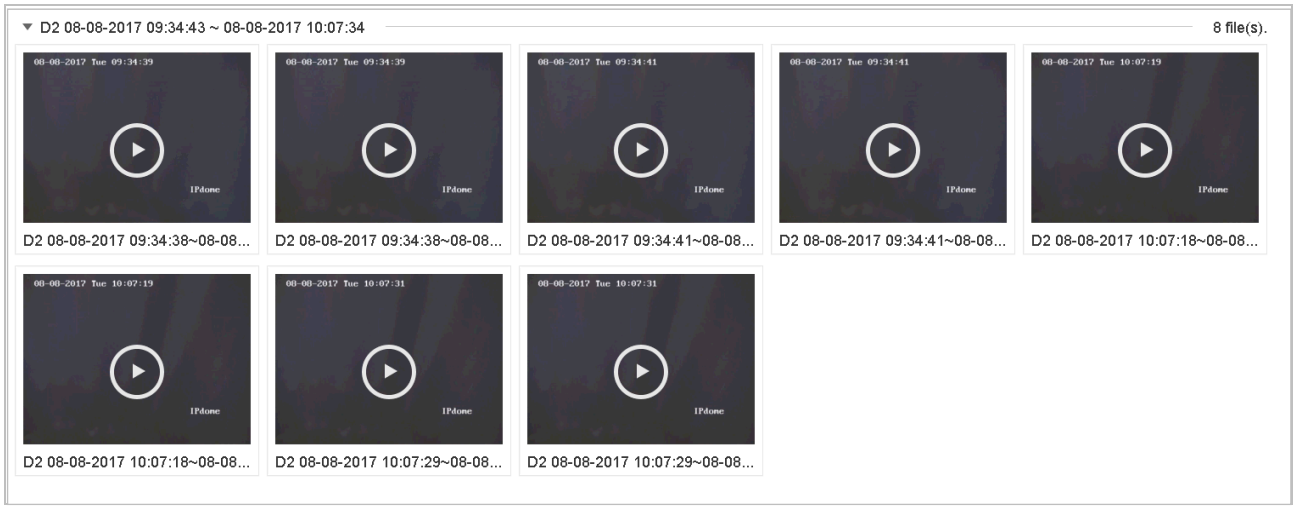


Figure 10-8 Searched Tag Files

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

10.1.6 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.).

Step 1 Go to **Playback**.

Step 2 Click **Custom Search** on the left bottom to enter the Search Condition interface.

Step 3 Enter the search conditions for the event files, e.g., time, event type, file status, vehicle information (for vehicle detection event), etc.

Step 4 Click **Search.**

Step 5 On the search results interface, select an event video file/picture file and double click to start playing the video.

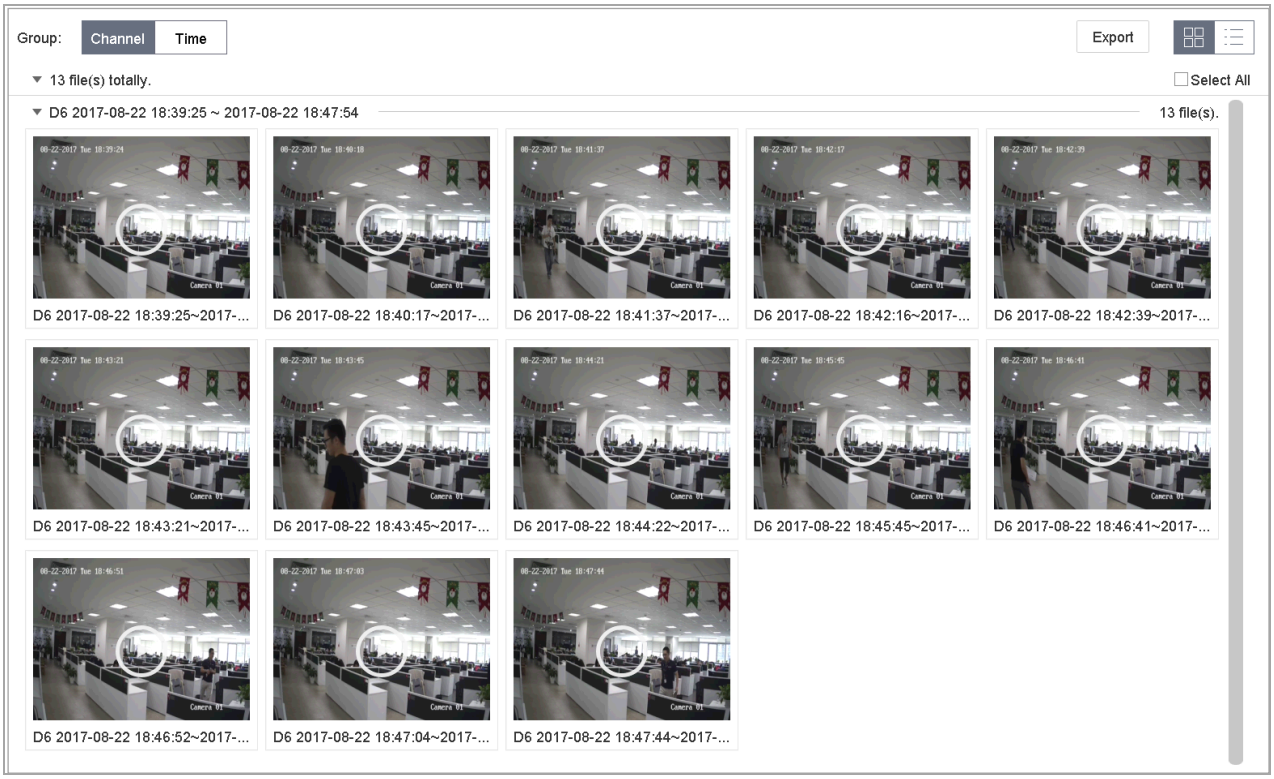


Figure 10-9 Event Files

You can click  or  button to play 30s backward or forward.

NOTE

- Refer to Chapter 11 Event and Alarm Settings and Chapter 12

for details for event and alarm settings.

- Refer to Chapter 8.7 Configure Event Triggered Recording for the event triggered recording/capture settings.

10.1.7 Play by Sub-periods

Purpose:

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

Step 1 Go to **Playback**.

Step 2 Select  icon at the left bottom corner to enter the sub-period playing mode.

Step 3 Select a camera.

Step 4 Set the start time and end time for searching video.

Step 5 Select the different multi-period at the right bottom corner, e.g., 4-Period.

NOTE

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

10.1.8 Play Log Files

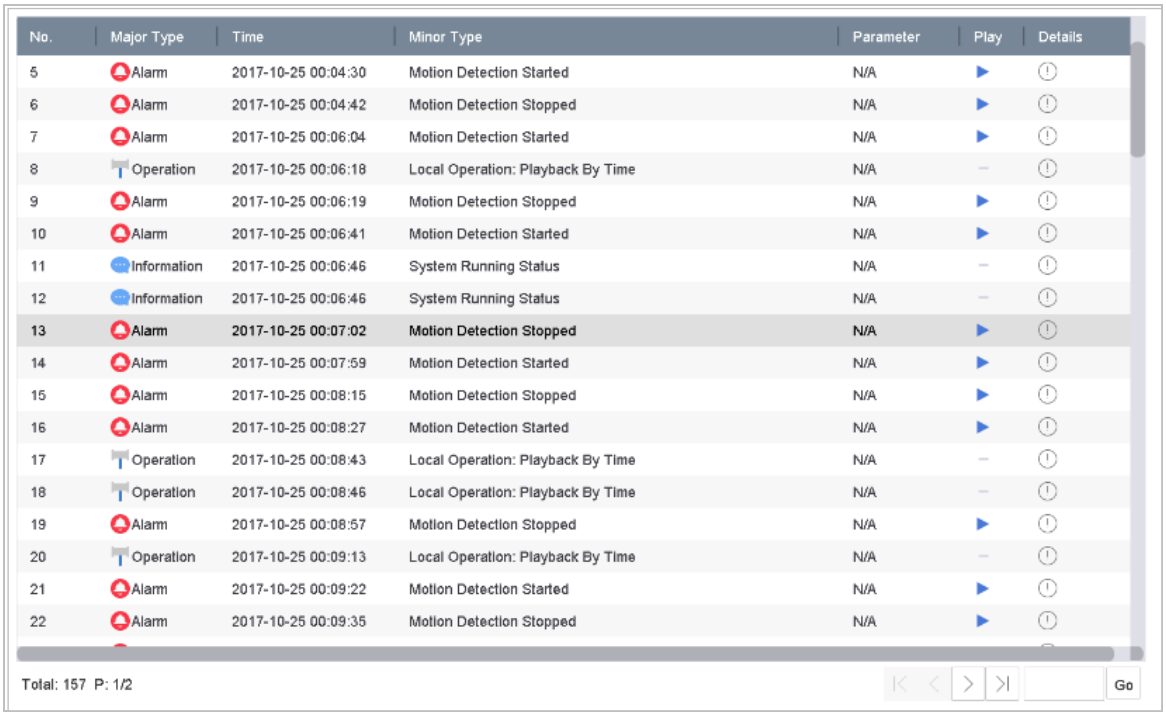
Purpose:

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

Step 1 Go to **Maintenance**>**Log Information**.

Step 2 Click **Log Search** tab to enter Playback by System Logs.

Step 3 Set search time and type and click **Search**.



No.	Major Type	Time	Minor Type	Parameter	Play	Details
5	Alarm	2017-10-25 00:04:30	Motion Detection Started	N/A		
6	Alarm	2017-10-25 00:04:42	Motion Detection Stopped	N/A		
7	Alarm	2017-10-25 00:06:04	Motion Detection Started	N/A		
8	Operation	2017-10-25 00:06:18	Local Operation: Playback By Time	N/A		
9	Alarm	2017-10-25 00:06:19	Motion Detection Stopped	N/A		
10	Alarm	2017-10-25 00:06:41	Motion Detection Started	N/A		
11	Information	2017-10-25 00:06:46	System Running Status	N/A		
12	Information	2017-10-25 00:06:46	System Running Status	N/A		
13	Alarm	2017-10-25 00:07:02	Motion Detection Stopped	N/A		
14	Alarm	2017-10-25 00:07:59	Motion Detection Started	N/A		
15	Alarm	2017-10-25 00:08:15	Motion Detection Stopped	N/A		
16	Alarm	2017-10-25 00:08:27	Motion Detection Started	N/A		
17	Operation	2017-10-25 00:08:43	Local Operation: Playback By Time	N/A		
18	Operation	2017-10-25 00:08:46	Local Operation: Playback By Time	N/A		
19	Alarm	2017-10-25 00:08:57	Motion Detection Stopped	N/A		
20	Operation	2017-10-25 00:09:13	Local Operation: Playback By Time	N/A		
21	Alarm	2017-10-25 00:09:22	Motion Detection Started	N/A		
22	Alarm	2017-10-25 00:09:35	Motion Detection Stopped	N/A		

Total: 157 P: 1/2 Go

Figure 10-10 System Log Search Interface

Step 4 Choose a log with video file and click to start playing the log file.

10.1.9 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.

Step 1 Go to **Playback**.

Step 2 Click at the left bottom corner.

Step 3 Select and click the button or double click to play the file.

10.2 Playback Operations

10.2.1 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.

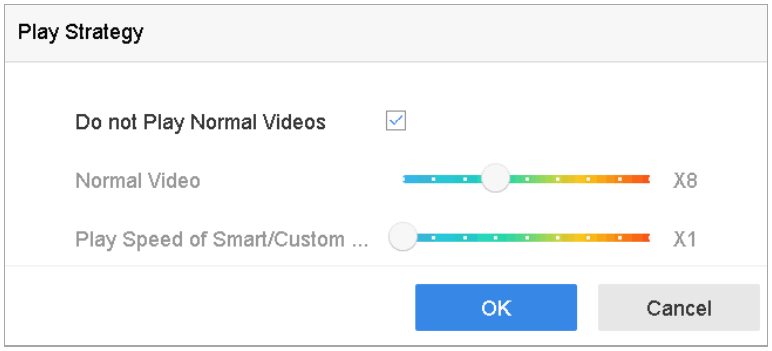


Figure 10-11 Play Strategy

10.2.2 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.

10.2.3 Switch between Main Stream and Sub-Stream

You can switch between the main stream and the sub-stream during the playback.

 : Play the video in main stream.

 : Play the video in sub-stream.

NOTE

The encoding parameters for the main stream and sub-stream can be configured in **Storage** > **Encoding Parameters**.

10.2.4 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.

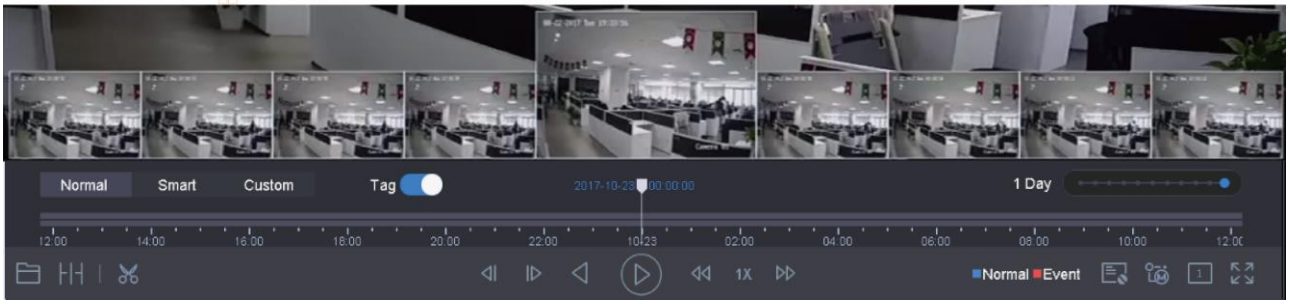


Figure 10-12 Thumbnails View

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

10.2.5 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.

10.2.6 Digital Zoom

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

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

Figure 10-13 Digital Zoom

Chapter 11 Event and Alarm Settings

11.1 Configure Arming Schedule

Step 1 Select **Arming Schedule**.

Step 2 Click Edit.

Step 3 Select a day of the week and set the time period. Up to eight time periods can be set each day.

NOTE

Time periods shall not be repeated or overlapped.

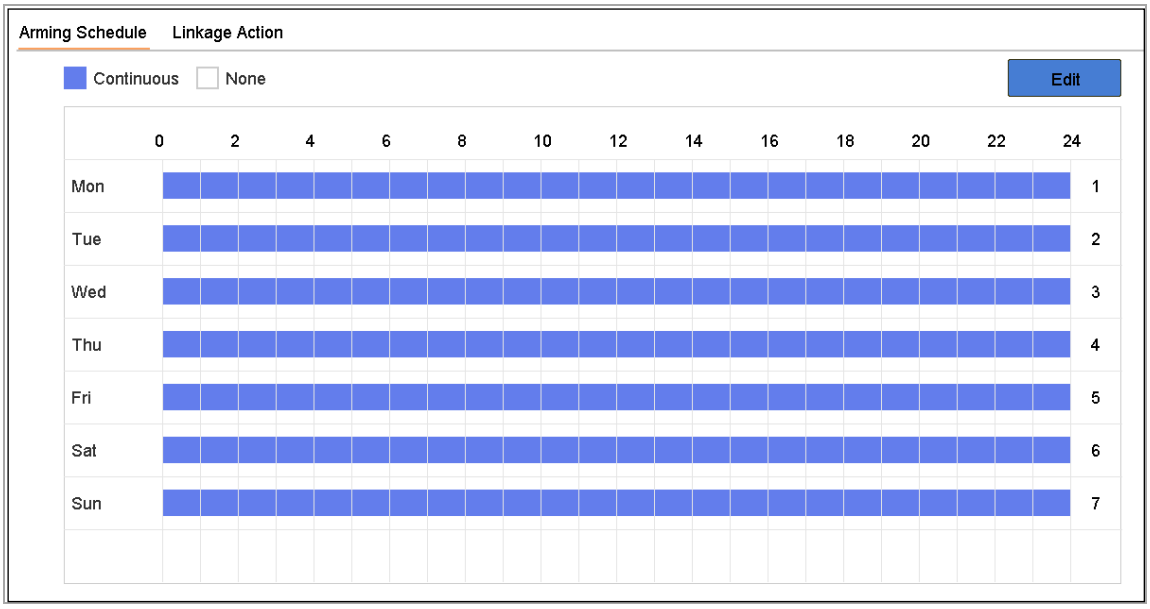


Figure 11-1 Set Arming Schedule

Step 4 (Optional) You can click **Copy** to copy the current day arming schedule settings to other day(s).

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

11.2 Configure Alarm Linkage Actions

Step 1 Click **Linkage Action** to set the alarm linkage actions.

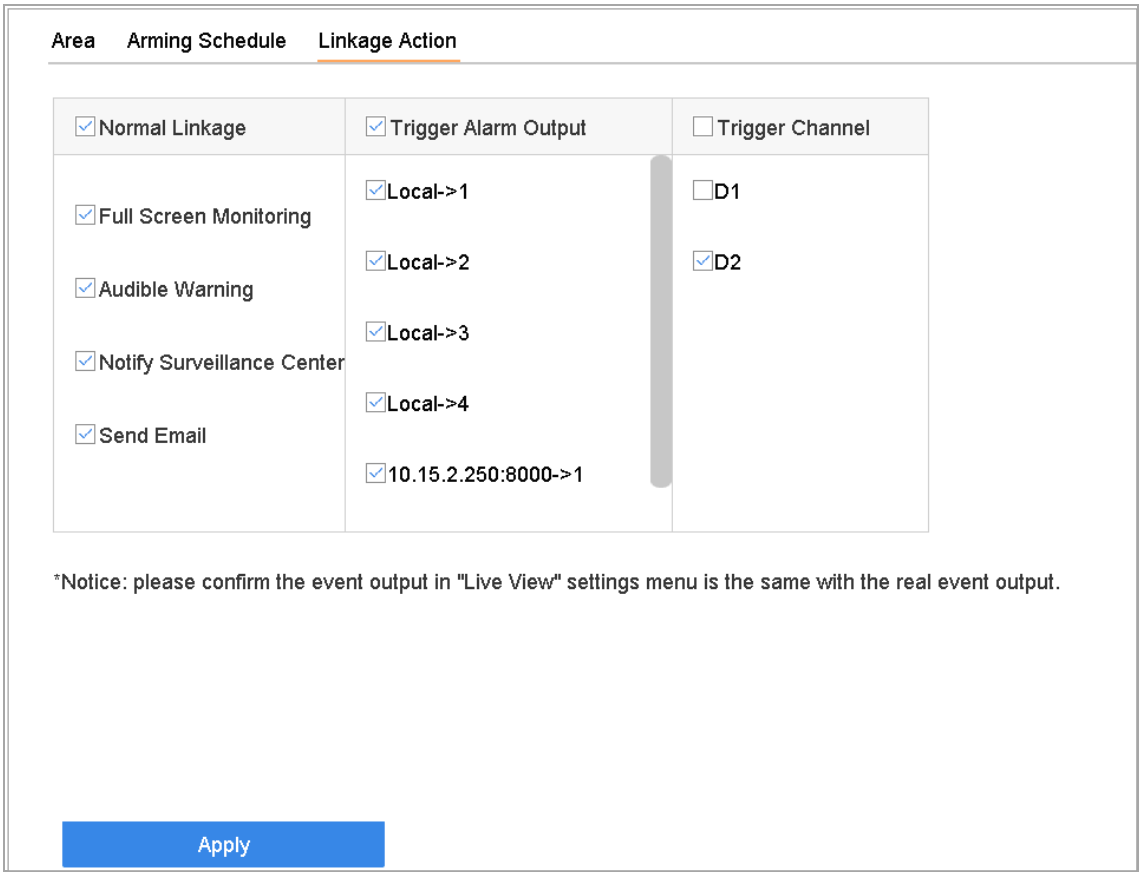


Figure 11-2 Set Linkage Actions

Step 2 Select the normal linkage actions, trigger alarm output or trigger recording channel.

- **Full Screen Monitoring**

When an alarm is triggered, the local monitor displays in full screen the video image from the alarming channel configured for full screen monitoring.

If alarms are triggered simultaneously in several channels, their full-screen images will be switched at an interval of 10 seconds (default dwell time). A different dwell time can be set by going to **System>Live View > Full Screen Monitoring Dwell Time**.

Auto-switch will terminate once the alarm stops and back to the live view interface.

NOTE

You must select the channel(s) in **Trigger Channel** settings you want to trigger full screen monitoring.

- **Audible Warning**

It will trigger an audible *beep* when an alarm is detected.

- **Notify Surveillance Center**

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

NOTE

The alarm signal will be transmitted automatically at detection mode when remote alarm host is configured.

- **Send Email**

It will send an email with alarm information to the user when an alarm is detected.

Please refer to 14.8 Configure Email for details of Email configuration.

Step 3 Check the checkbox to select the alarm output when an alarm is triggered.

NOTE

To trigger an alarm output when an event occurs, please refer to Chapter 11.6.3 Configure Alarm Output to set the alarm output parameters.

Step 4 Click **Trigger Channel** and select one or more channels which will start to record/capture or perform full-screen monitoring when motion alarm is triggered.

NOTE

You have to set the recording schedule to realize this function. Please refer to Refer to Chapter 8.4 Configure Recording Schedule for settings of the recording schedule.

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

11.3 Configure Motion Detection Alarm

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

Step 1 Go to **System**> **Event**>**Normal Event>Motion Detection.**

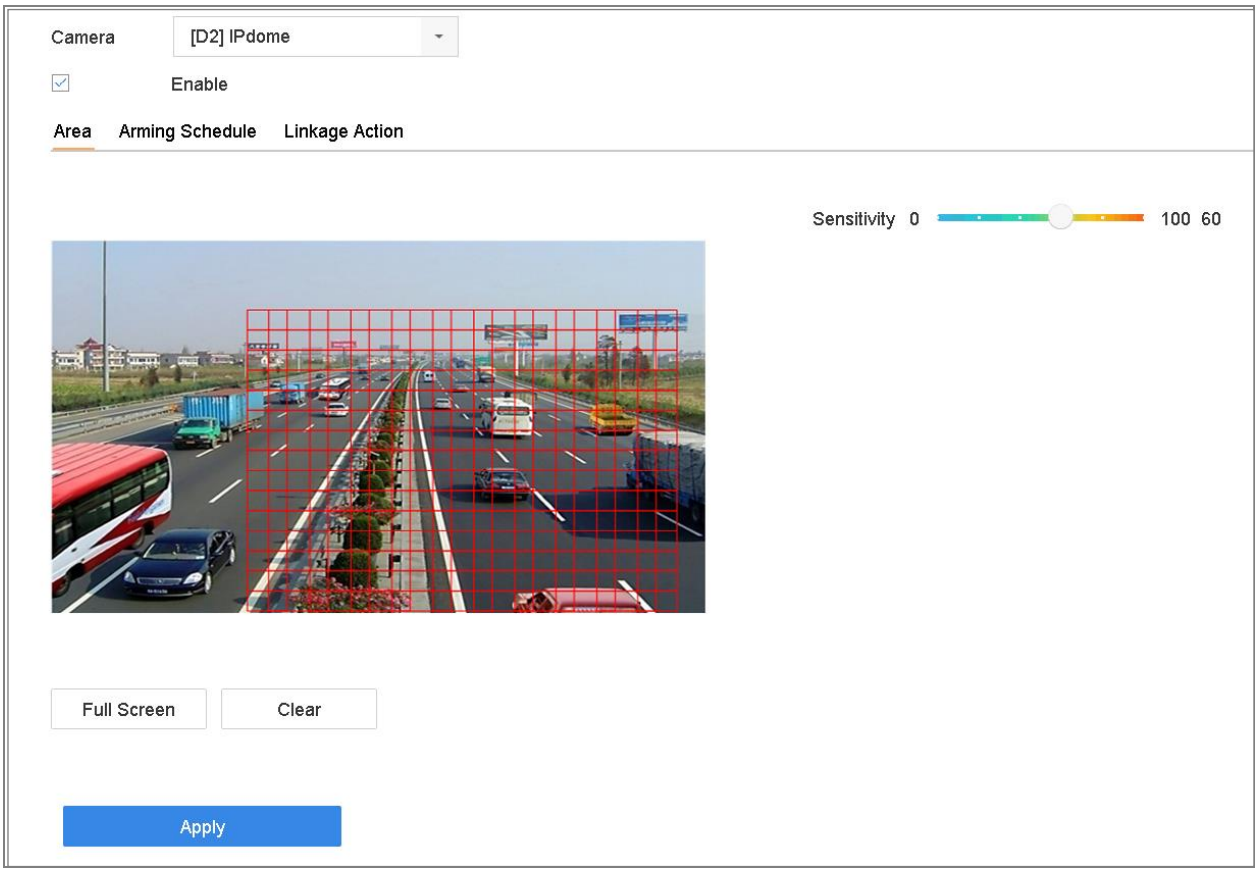


Figure 11-3 Set Motion Detection

Step 2 Select the camera to configure the motion detection.

Step 3 Check **Enable**.

Step 4 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.

Step 5 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.

Step 6 Set the arming schedule. Refer to Chapter 11.1 Configure Arming Schedule.

Step 7 Set the linkage actions. Refer to Chapter 11.2 Configure Alarm Linkage Actions.

11.4 Configure Video Loss Alarm

Purpose:

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

Step 1 Go to **System**> **Event**>**Normal Event>Video Loss**

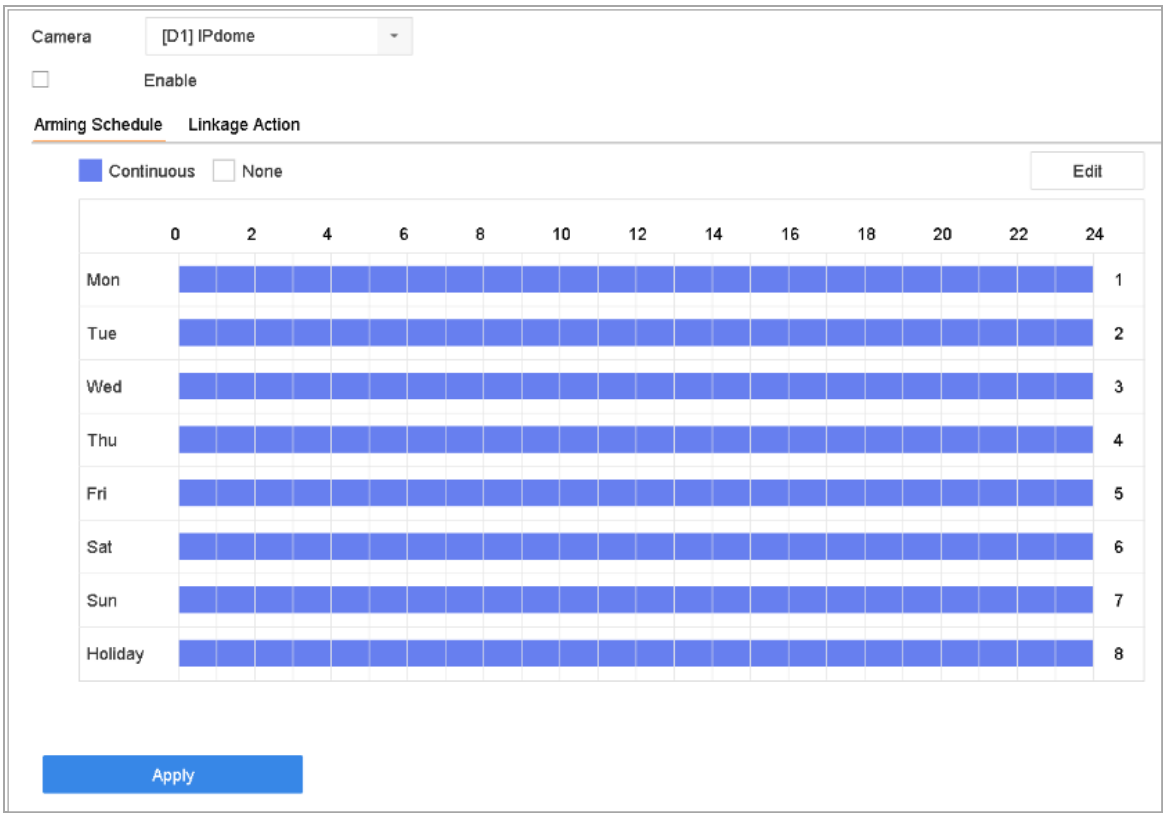


Figure 11-4 Set Video Loss Detection

Step 2 Select the camera to configure the video loss detection.

Step 3 Check **Enable**.

Step 4 Set the arming schedule. Refer to Chapter 11.1 Configure Arming Schedule.

Step 5 Set the linkage actions. Refer to Chapter 11.2 Configure Alarm Linkage Actions.

11.5 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).

Step 1 Go to **System**> **Event**>**Normal Event>Video Tampering.**

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

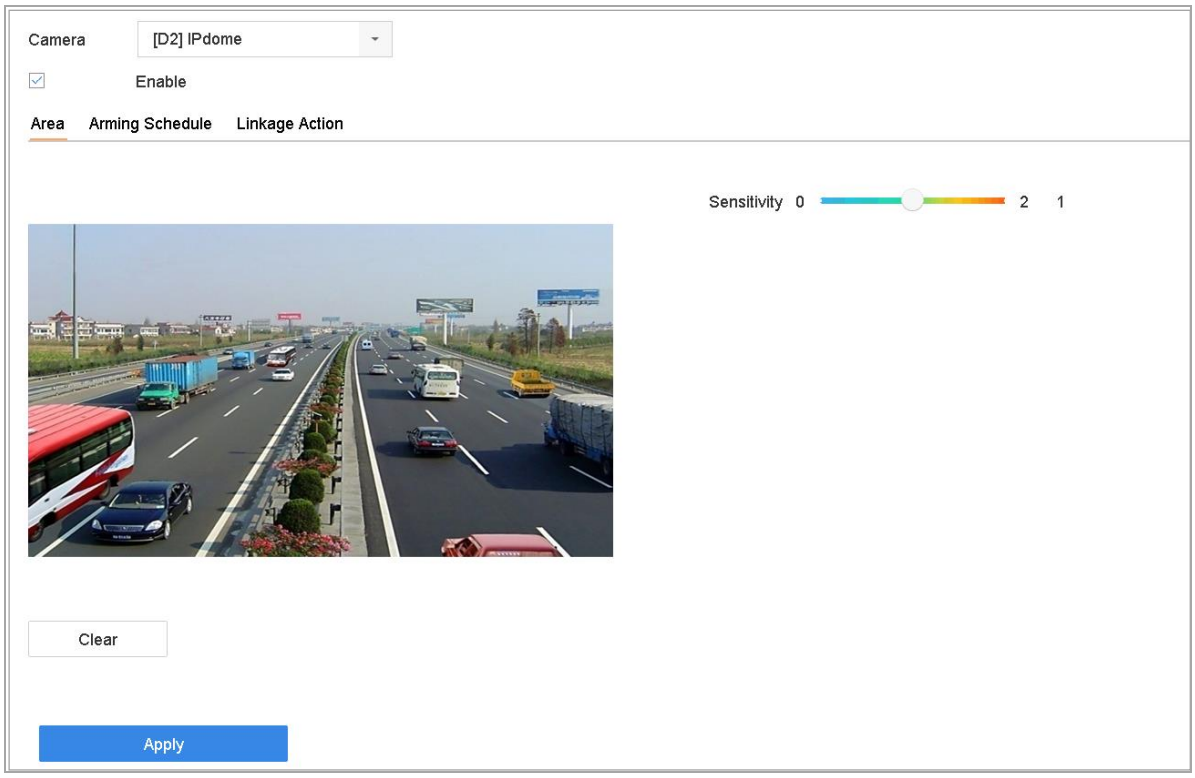


Figure 11-5 Set Video Tampering Setting

Step 3 Check **Enable**.

Step 4 Set the video tampering area. Use the mouse to click and drag on the preview screen to draw the customized video tampering area.

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

Step 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.

Step 6 Set the arming schedule. Refer to Chapter 11.1 Configure Arming Schedule.

Step 7 Set the linkage actions. Refer to Chapter 11.2 Configure Alarm Linkage Actions.

11.6 Configure Sensor Alarms

Purpose:

Set the handling action of an external sensor alarm.

11.6.1 Configure Alarm Input

Step 1 Go to **System**> **Event**>**Normal Event>Alarm Input**

Step 2 Select an alarm input item from the list and click  .

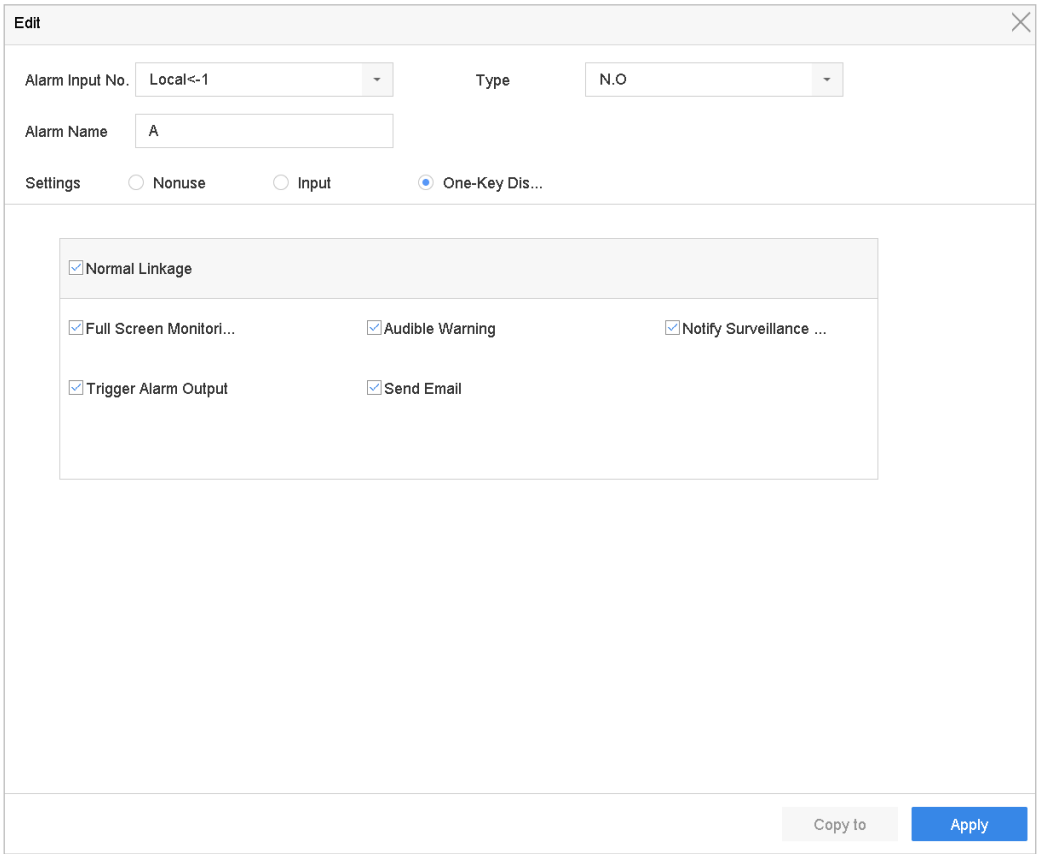


Figure 11-6 Alarm Input

Step 3 Select the alarm input type to N.C or N.O.

Step 4 Edit the alarm name.

Step 5 Check the radio button of **Input**.

Step 6 Set the arming schedule. Refer to Chapter 11.1 Configure Arming Schedule.

Step 7 Set the linkage actions. Refer to Chapter 11.2 Configure Alarm Linkage Actions.

11.6.2 Configure One-Key Disarming

The one-key disarming enables the device to disarm the alarm input 1 by one-key operation.

Step 1 Go to **System**> **Event**>**Normal Event>Alarm Input**

Step 2 Select the alarm input1 item from the list and click .

Step 3 Select the alarm input type to N.C or N.O.

Step 4 Edit the alarm name.

Step 5 Check the radio button of **Enable One-Key Disarming**.

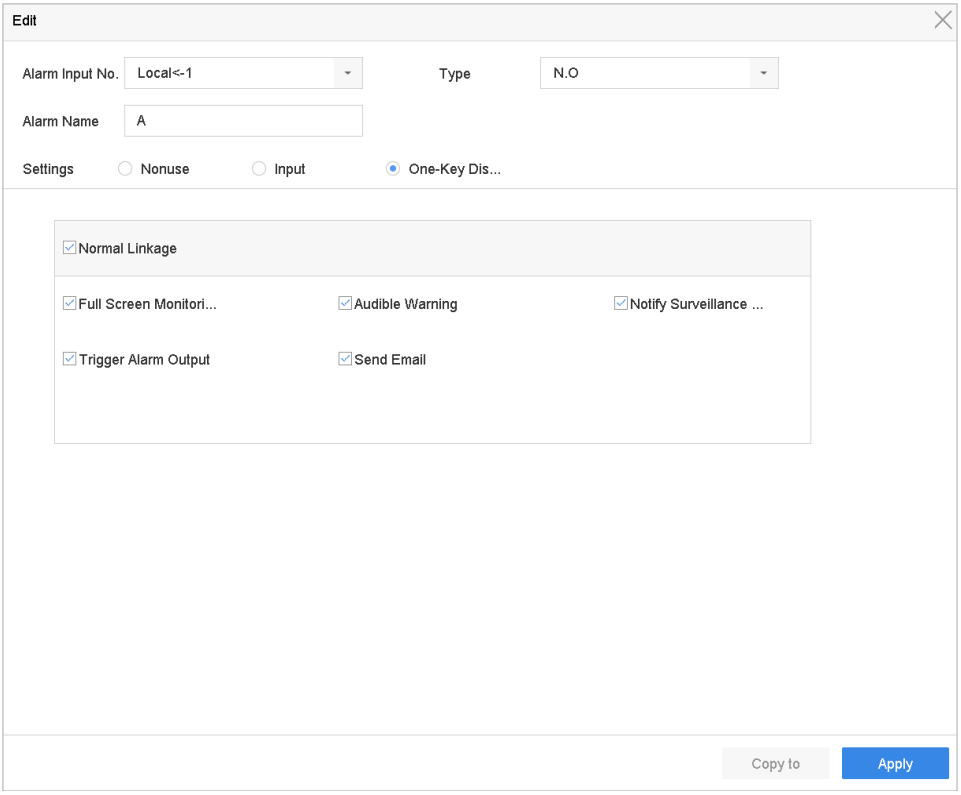


Figure 11-7 One-Key Alarm Disarming

Step 6 Select the alarm linkage action (s) you want to disarm for the local alarm input1.

NOTE

When the alarm input 1 (Local<-1) is enabled with one-key disarming, the other alarm input settings are not configurable.

Step 7 Click **Apply** to save the settings.

11.6.3 Configure Alarm Output

Trigger an alarm output when an alarm is triggered.

Step 1 Go to **System**> **Event**>**Normal Event>Alarm Output**.

Step 2 Select an alarm output item from the list and click .

Step 3 Edit the alarm name.

Step 4 Select the dwell time (the alarm duration) from 5s to 600s, or **Manually Clear**.

Manually Clear: you should manually clear the alarm when the alarm occurs. Refer to 11.9 Trigger or Clear Alarm Output Manually for detailed instructions.

Step 5 Set the arming schedule. Refer to Chapter 11.1 Configure Arming Schedule.

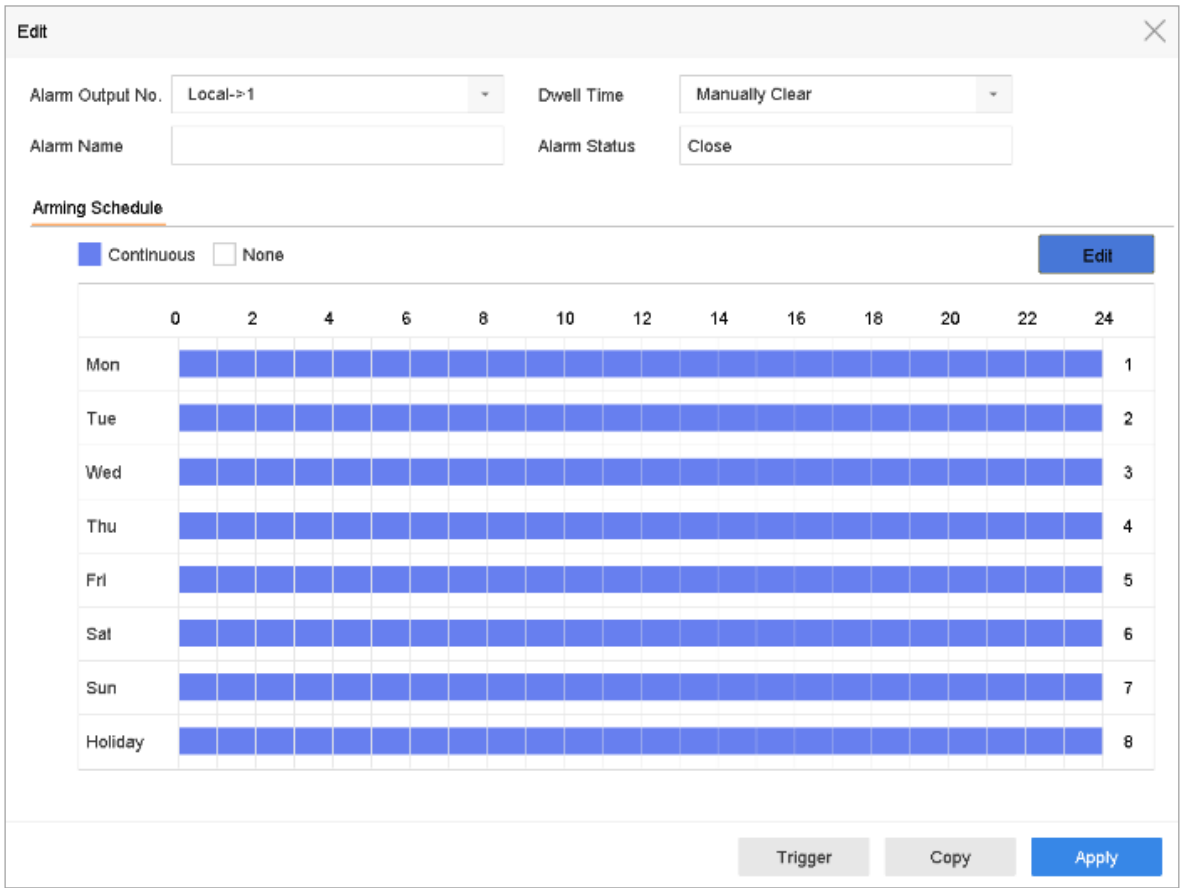


Figure 11-8 Alarm Output

Step 6 (Optional) You can click **Copy** to copy the same settings to other alarm output (s).

11.7 Configure Exceptions Alarm

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

Step 1 Go to **System> Event>Normal Event>Exception**.

Step 2 (Optional) Enable the event hint if you want to display the event hint in the live view window.

1) Check the checkbox of **Enable Event Hint.**

2) Click  to select the exception type (s) to take the event hint.

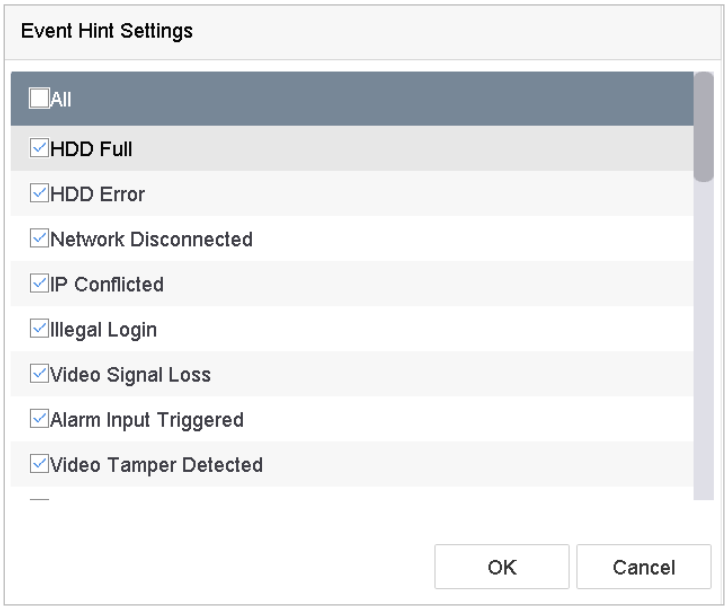


Figure 11-9 Event Hint Settings

Step 3 Select the excetion type from the drop-down list to set the linkage actions.

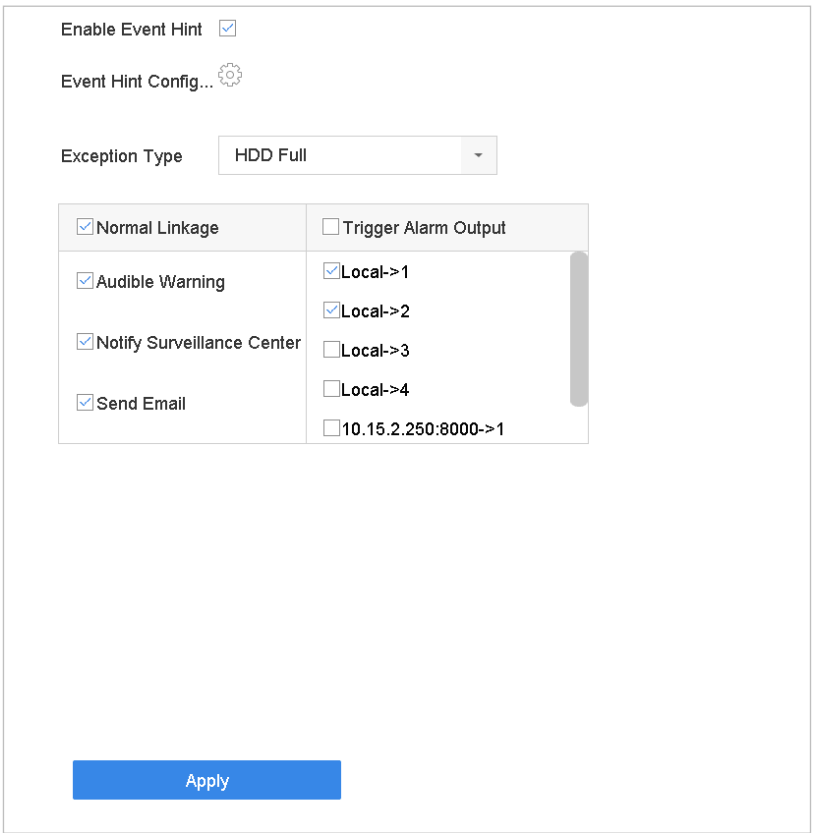


Figure 11-10 Exceptions Handling

Step 4 Set the normal linkage and alarm output triggering. Refer to 11.2 Configure Alarm Linkage Actions.

Step 5 Click **Apply**.

11.8 Configure Combined Alarm

Purpose

Combined alarm combines events with alarm input. The combined alarm will be triggered when it receives alarms from both alarm input and events. Event types include motion detection, video tampering detection, and other smart events such as line crossing detection, intrusion detection, etc.

Before you start

Ensure the channel has been assigned with event alarm as your desire, and the alarm input has been configured (refer to 11.6.1 Configure Alarm Input).

Step 1 Go to **System** > **Event** > **Normal Event** > **Alarm Input**.

Step 2 Select an alarm input item from the list and click .

Step 3 Select **Settings** as **Input**.

Step 4 Click **Combined Alarm**.

Step 5 Select channel as your desire.

Step 6 Select **Combined Alarm Event**.

Step 7 Click **Apply**.

NOTE

The combined alarm arming schedule and linkage action are the same as the selected event(s).

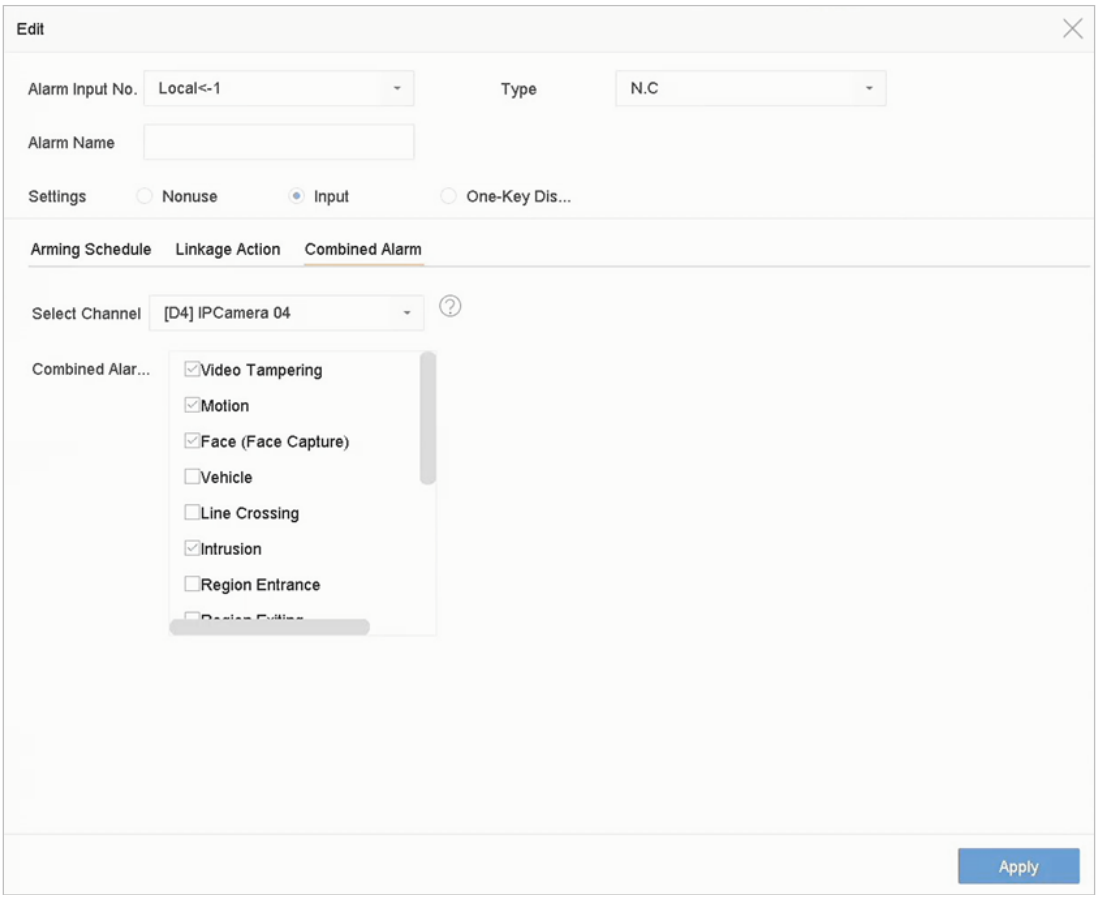


Figure 11-11 Combined Alarm

11.9 Trigger or Clear Alarm Output Manually

Purpose:

Sensor alarm can be triggered or cleared manually. When the **Manually Clear** is selected for the dwell time of an alarm output, the alarm can be cleared only by clicking **Clear** button.

Step 1 Go to **System**> **Event**>**Normal Event>Alarm Output**.

Step 2 Select the alarm output you want to trigger or clear.

Step 3 Click **Trigger/Clear** to trigger or clear an alarm output.

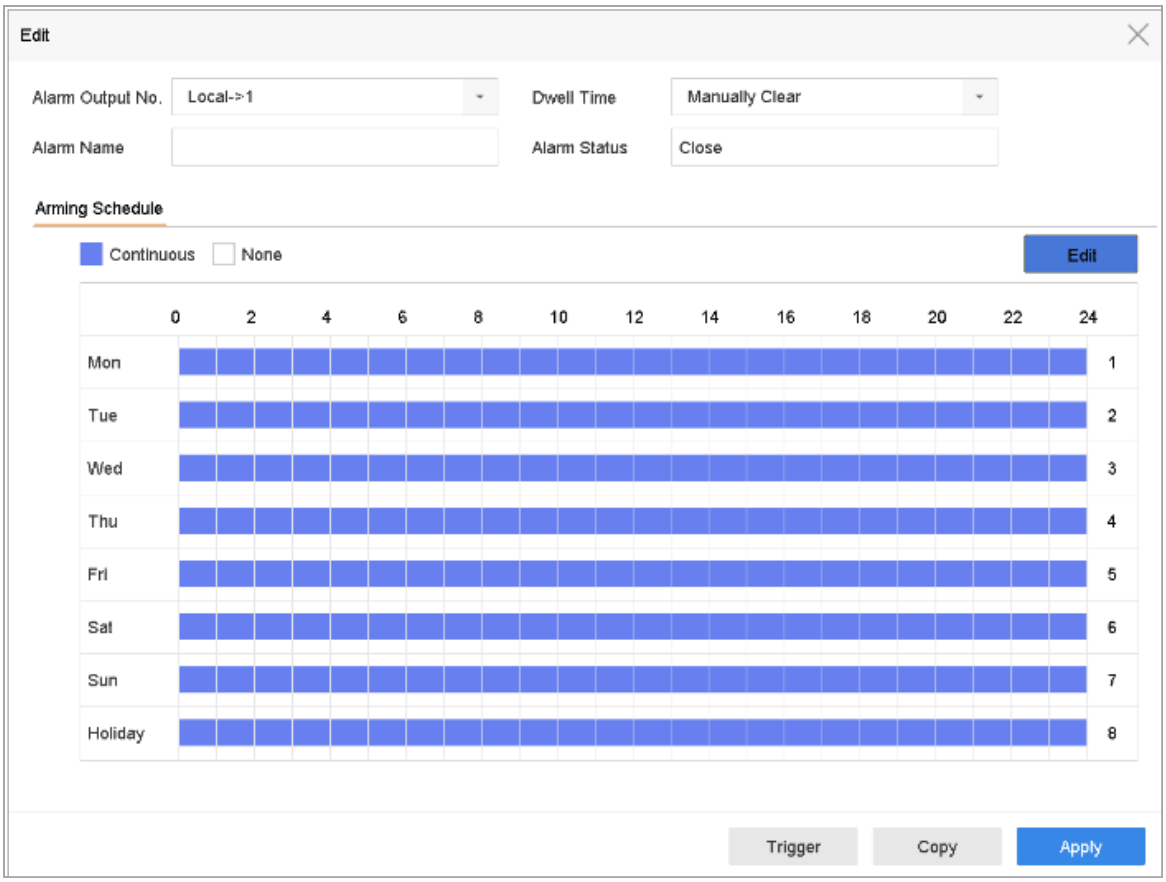


Figure 11-12 Alarm Output

Chapter 12 VCA Event Alarm

The device supports receiving the VCA detections sent by connected IP cameras. Enable and configure the VCA detection on the IP camera settings interface first.

NOTE

- VCA detections must be supported by the connected IP camera.
- Refer to the User Manual of Network Camera for the detailed instructions for the VCA detection.

12.1 Face Detection

Purpose:

Face detection function detects the face appears in the surveillance scene. Linkage actions will be triggered when a human face is detected.

Step 1 Go to **System > Event > Smart Event**.

Step 2 Click **Face Detection**.

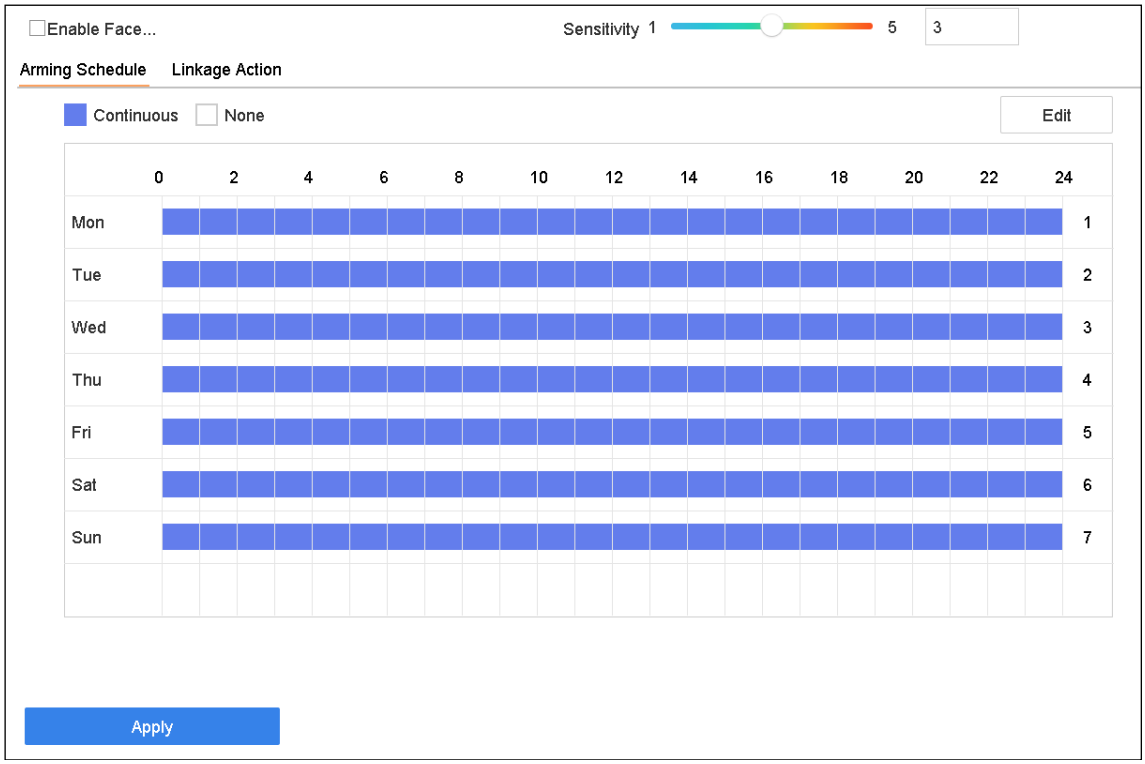


Figure 12-1 Face Detection

Step 3 Select a camera to configure.

Step 4 Check **Enable Face Detection**.

Step 5 Optionally, check **Save VCA Picture** to save the captured pictures of face detection.

Step 6 Drag the **Sensitivity** slider to set the detection sensitivity. Sensitivity range: [1-5]. The higher the value is, the more easily the face can be detected.

Step 7 Set the arming schedule. Refer to Chapter 11.1 Configure Arming Schedule.

Step 8 Set the linkage actions. Refer to Chapter 11.2 Configure Alarm Linkage Actions.

Step 9 Click **Apply**.

12.2 Vehicle Detection

Purpose:

Vehicle Detection is available for the road traffic monitoring. In Vehicle Detection, the passed vehicle can be detected and the picture of its license plate can be captured. You can send alarm signal to notify the surveillance center and upload the captured picture to FTP server.

Step 1 Go to **System > Event > Smart Event**.

Step 2 Click **Vehicle**.

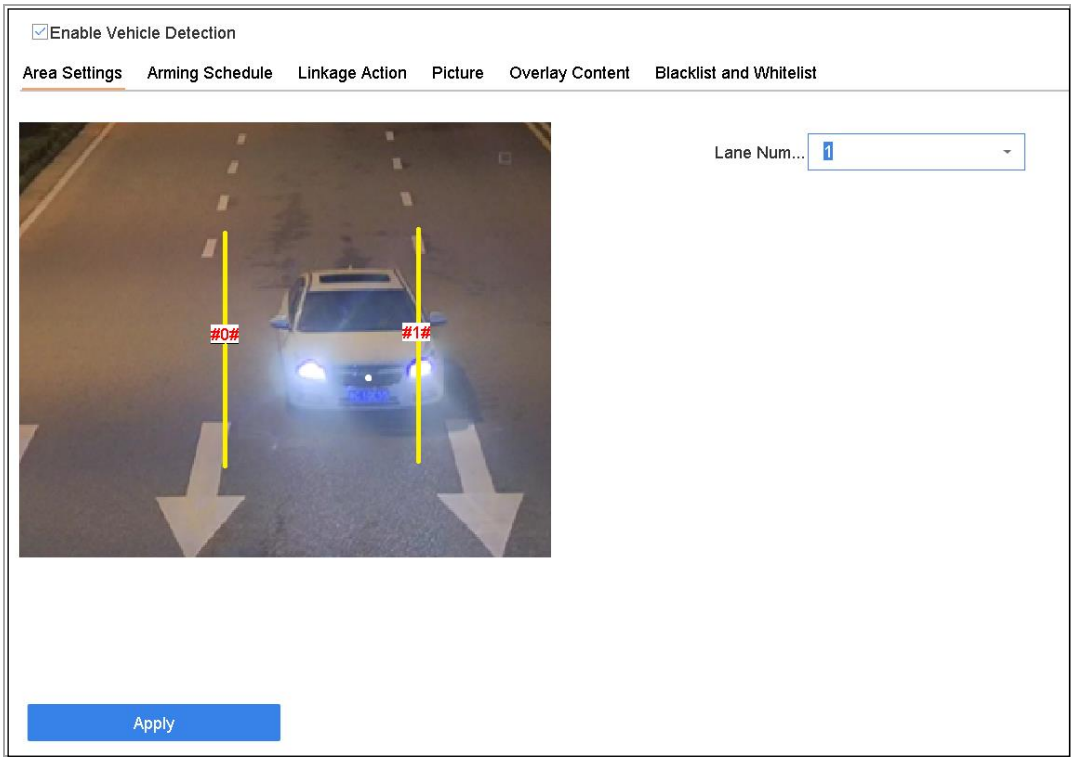


Figure 12-2 Vehicle Detection

Step 3 Select a camera to configure.

Step 4 Check **Enable Vehicle Detection**.

Step 5 Optionally, check **Save VCA Picture** to save the captured pictures of vehicle detection.

Step 6 Set the arming schedule. Refer to Chapter 11.1 Configure Arming Schedule.

Step 7 Set the linkage actions. You can configure the linkage action for black list, whitelist and other license plate respectively. Refer to Chapter 11.2 Configure Alarm Linkage Actions.

Step 8 Configure rules, including **Area Settings, Picture, Overlay Content**, and **Blacklist and Whitelist**.

Area Settings: Up to 4 lanes are selectable.

Blacklist and Whitelist: You can export the file first to see its format, and edit it and import it to the device.

Step 9 Click **Apply**.

NOTE

Refer to the User Manual of Network Camera for the detailed instructions for the vehicle detection.

12.3 Line Crossing Detection

Purpose:

Line crossing detection detects people, vehicles, and objects crossing a set virtual line. The detection direction can be set as bidirectional, from left to right or from right to left.

Step 1 Go to **System > Event > Smart Event**.

Step 2 Click **Line Crossing**.

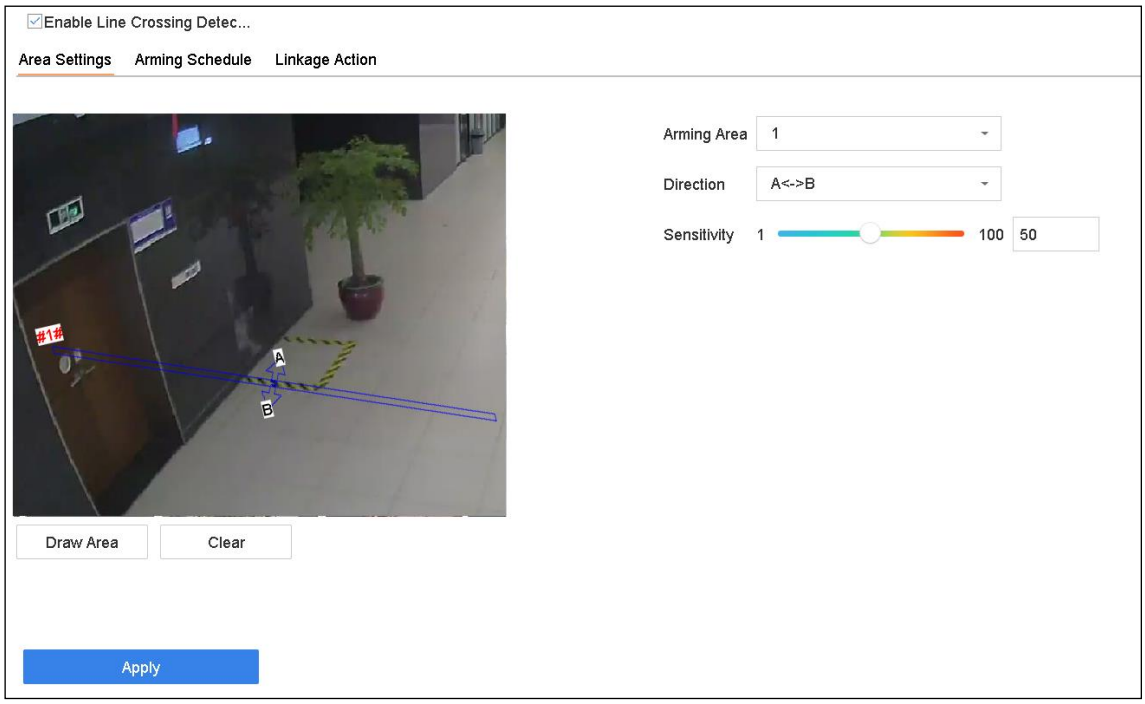


Figure 12-3 Line Crossing Detection

Step 3 Select a camera to configure.

Step 4 Check **Enable Line Crossing Detection** checkbox.

Step 5 Optionally, check **Save VCA Picture** to save the captured pictures of line crossing detection.

Step 6 Follow the steps to set the line crossing detection rules and detection areas.

1) Select an **Arming Area** to configure. Up to 4 arming regions are selectable.

Select the **Direction** as **A<->B**, **A->B**, or **A<-B**.

A<->B: Only the arrow on the B side shows. When an object goes across the configured line with both direction can be detected and alarms are triggered.

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

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

Drag the **Sensitivity** slider to set the detection sensitivity. Sensitivity range: sensitivity. The higher the value is, the more easily the detection alarm can be triggered.

Click Draw Region and set two points in the preview window to draw a virtual line.

Step 7 Set the arming schedule. Refer to Chapter 11.1 Configure Arming Schedule.

Step 8 Set the linkage actions. Refer to Chapter 11.2 Configure Alarm Linkage Actions.

Step 9 Click **Apply**.

12.4 Intrusion Detection

Purpose:

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

Step 1 Go to **System > Event > Smart Event**.

Step 2 Click **Intrusion**.

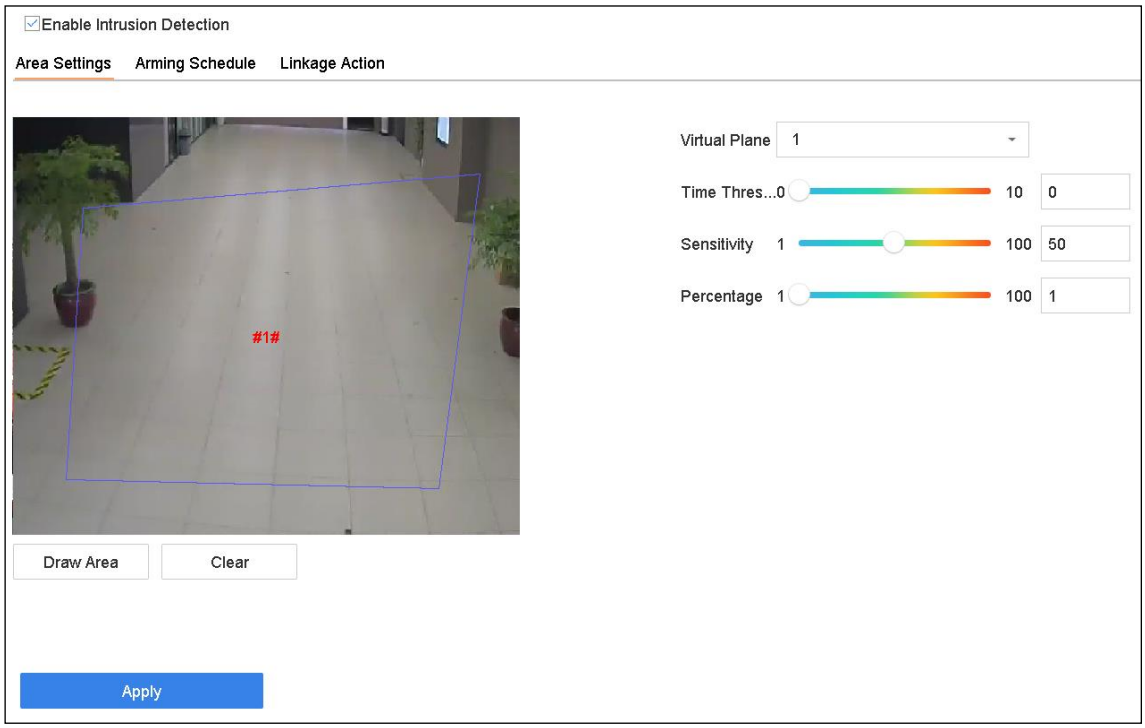


Figure 12-4 Intrusion Detection

Step 3 Select a camera to configure.

Step 4 Check **Enable Intrusion Detection**.

Step 5 Optionally, check **Save VCA Picture** to save the captured pictures of intrusion detection.

Step 6 Follow the steps to set the detection rules and detection areas.

1) Select a **Virtual Panel** to configure. Up to 4 virtual panels are selectable.

Drag the sliders to set Time Threshold, Sensitivity, and Percentage.

Time Threshold: The threshold for the time of the object loitering in the region. When the duration of the object in the defined detection area is longer than the threshold, device will trigger an alarm. Its range is [1s-10s].

Sensitivity: The size of the object that can trigger the alarm. The higher the value is, the more easily the detection alarm can be triggered. Its range is [1-100].

Percentage: The ratio of the in-region part of the object that can trigger the alarm. For example, if the percentage is 50%, when the object enters the region and occupies half of the whole region, device will trigger an alarm. Its range is [1-100].

Click **Draw Area** and draw a quadrilateral in the preview window by specifying four vertexes of the detection region.

Step 7 Set the arming schedule. Refer to Chapter 11.1 Configure Arming Schedule.

Step 8 Set the linkage actions. Refer to Chapter 11.2 Configure Alarm Linkage Actions.

Step 9 Click **Apply**.

12.5 Region Entrance Detection

Purpose:

Region entrance detection function detects objects that enter a pre-defined virtual region from the outside place.

Step 1 Go to **System Management > Event Settings > Smart Event**.

Step 2 Click **Region Entrance Detection**.

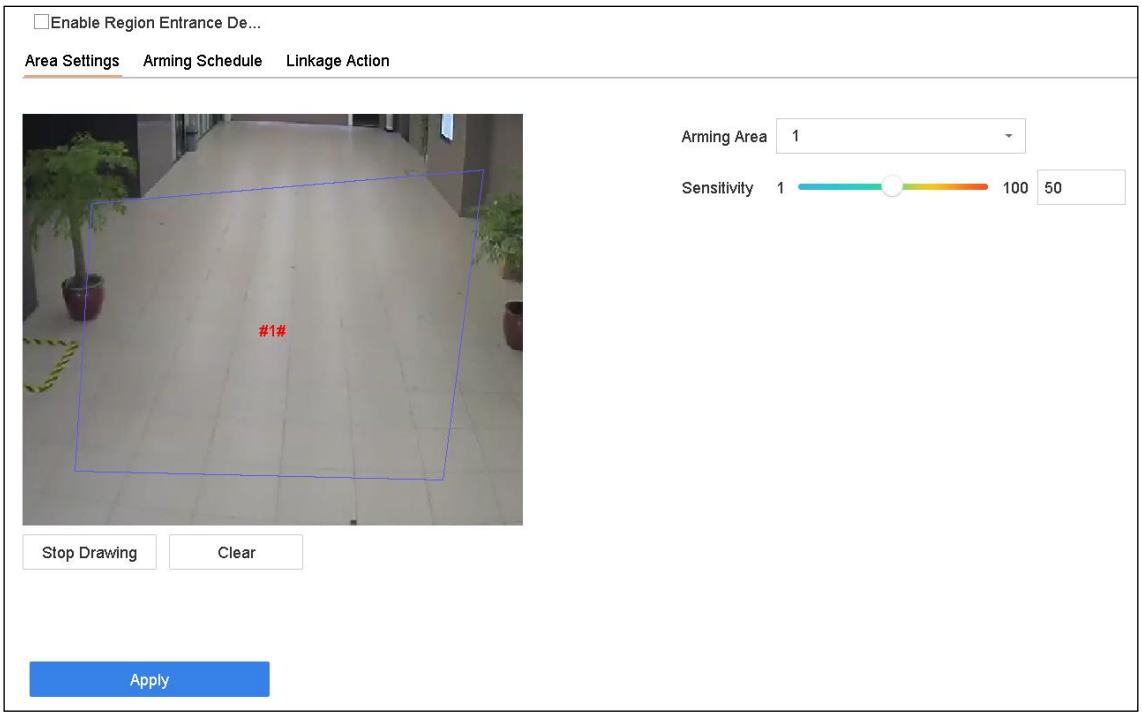


Figure 12-5 Region Entrance Detection

Step 3 Select a camera to configure.

Step 4 Check **Enable Region Entrance Detection** checkbox.

Step 5 Optionally, check **Save VCA Picture** checkbox to save the captured pictures of region entrance detection.

Step 6 Follow the steps to set the detection rules and detection areas.

1) Select an **Arming Area** to configure. Up to 4 regions are selectable.

Drag the sliders to set Sensitivity.

Sensitivity: The higher the value is, the more easily the detection alarm can be triggered. Its range is [0-100].

Click **Draw Area** and draw a quadrilateral in the preview window by specifying four vertexes of the detection region.

Step 7 Configure **Arming Schedule** and **Linkage Action**.

Step 8 Click **Apply**.

12.6 Region Exiting Detection

Purpose:

Region exiting detection function detects objects that exit from a pre-defined virtual region.

Step 1 Go to **System > Event > Smart Event**.

Step 2 Click **Region Exiting**.

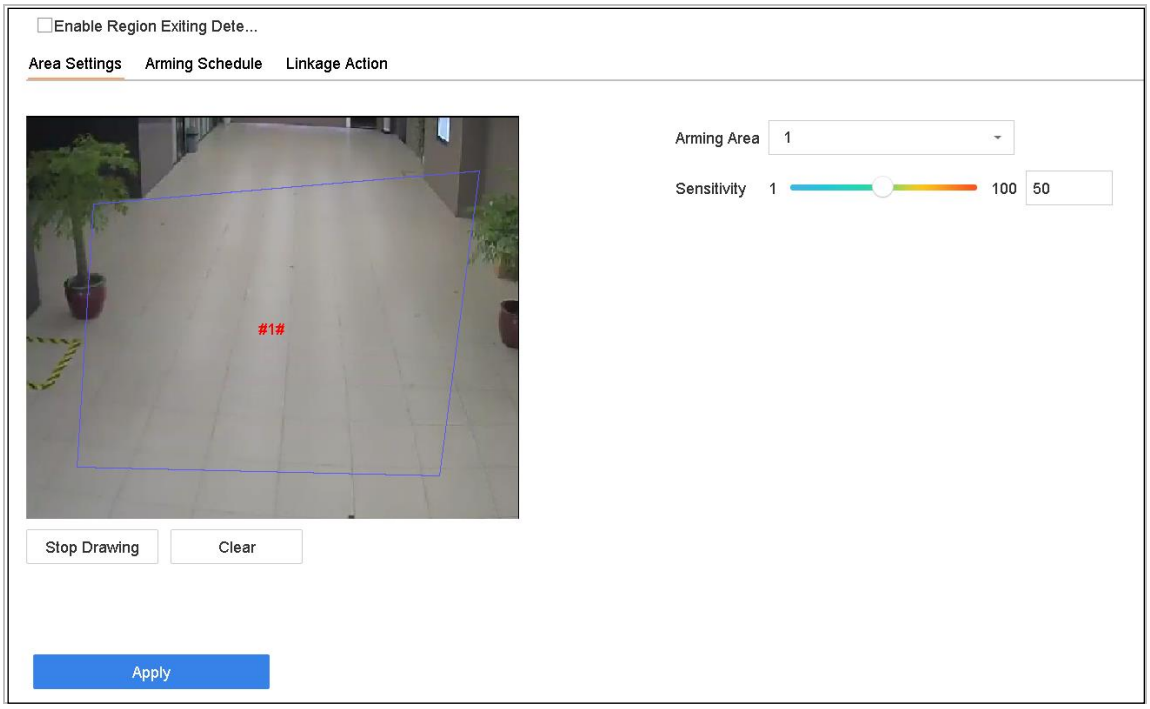


Figure 12-6 Region Exiting Detection

Step 3 Select a **Camera** to configure.

Step 4 Check **Enable Region Exiting Detection**.

Step 5 Optionally, check **Save VCA Picture** to save the captured pictures of region exiting detection.

Step 6 Follow the steps to set the detection rules and detection areas.

1) Select an **Arming Area** to configure. Up to 4 regions are selectable.

Drag the sliders to set Sensitivity.

Sensitivity: The higher the value is, the more easily the detection alarm can be triggered. Its range is [0-100].

Click **Draw Area** and draw a quadrilateral in the preview window by specifying four vertexes of the detection region.

Step 7 Set the arming schedule. Refer to Chapter 11.1 Configure Arming Schedule.

Step 8 Set the linkage actions. Refer to Chapter 11.2 Configure Alarm Linkage Actions.

Step 9 Click **Apply**.

12.7 Loitering Detection

Purpose

Loitering detection is used to detect whether a target stays within a specified area longer than the set time and trigger alarm for linked actions.

Step 1 Go to **System > Event > Smart Event**.

Step 2 Select a camera to configure.

Step 3 Click **Loitering**.

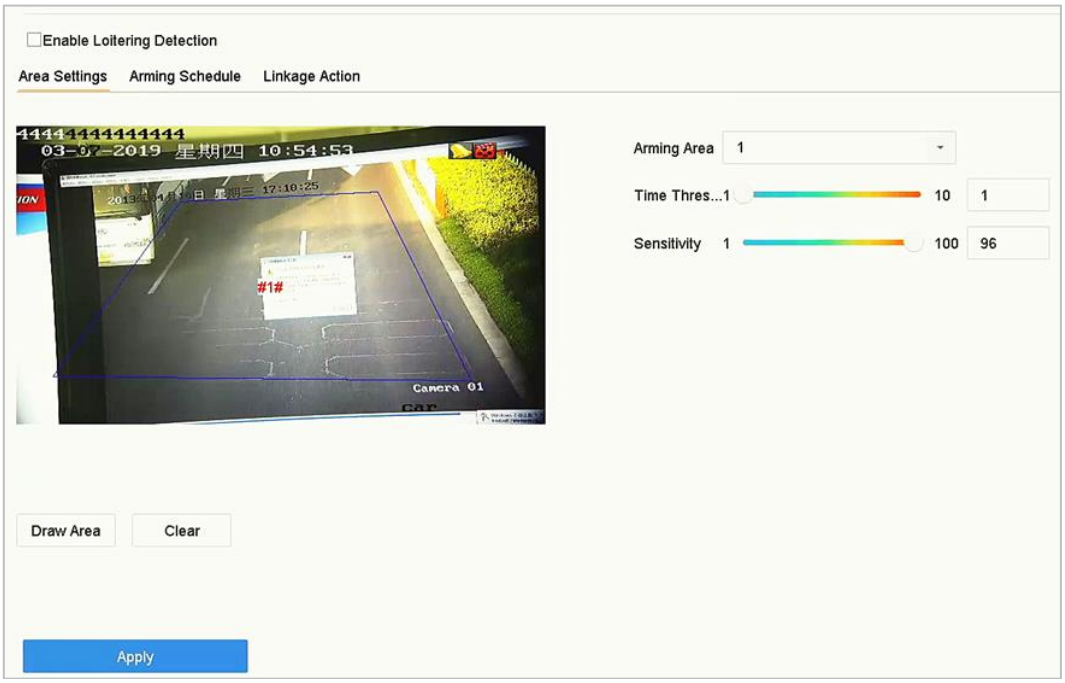


Figure 12-7 Loitering Detection

Step 4 Check **Enable Loitering Detection**.

Step 5 Optionally, check **Save VCA Picture** to save the captured loitering detection pictures.

Step 6 Set loitering detection parameters.

1) Select **Arming Area**. Up to 4 areas are selectable.

Set **Time Threshold (s)**.

Time Threshold: The time of car staying in the region. If the value is 10, an alarm is triggered after the car has stayed in the region for 10s. Its range is [1s-10s].

Set **Sensitivity**.

Sensitivity: Similarity of the background image to the object. The higher the value, the easier the detection alarm will be triggered.

Step 7 Set the arming schedule. Refer to Chapter 11.1 Configure Arming Schedule.

Step 8 Set the linkage actions. Refer to Chapter 11.2 Configure Alarm Linkage Actions.

Step 9 Click **Apply**.

12.8 People Gathering Detection

Purpose

People gathering detection is used to detect whether the density of human bodies within a specified area exceeds the set value and trigger alarm for linked actions.

Step 1 Go to **System > Event > Smart Event**.

Step 2 Select a camera to configure.

Step 3 Click **People Gathering**.

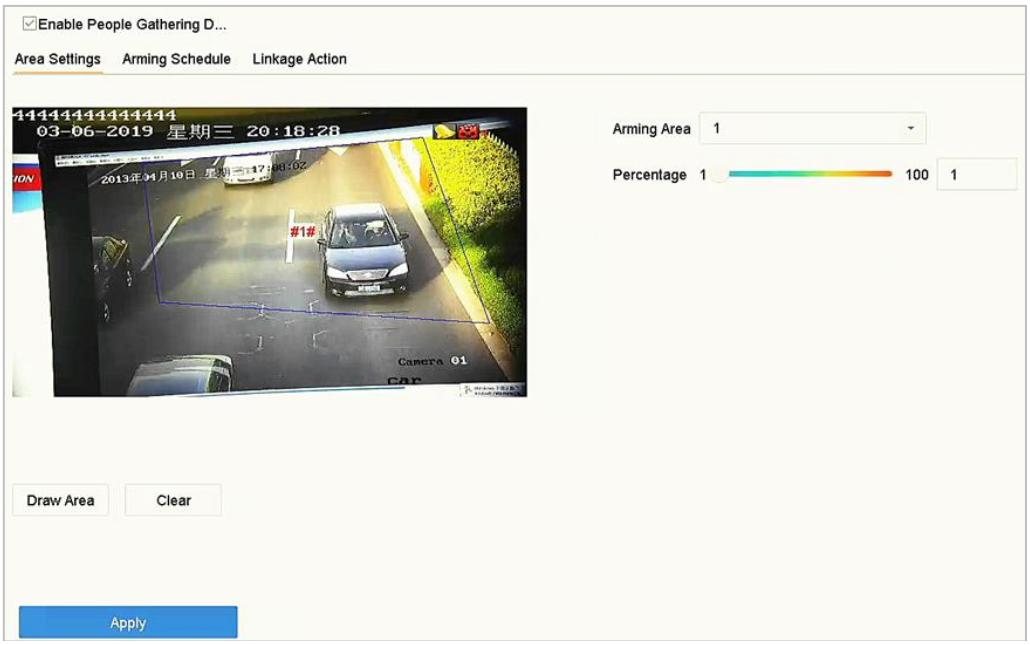


Figure 12-8 People Gathering Detection

Step 4 Check **Enable People Gathering Detection**.

Step 5 Optionally, check **Save VCA Picture** to save the captured people gathering detection pictures.

Step 6 Set people gathering detection parameters.

1) Select **Arming Area**. Up to 4 areas are selectable.

Click **Draw Area** to draw a quadrilateral in the preview window by specifying four vertices of the area.

Set Percentage.

Percentage: The percentage refers to the density of human bodies within the area. If it exceeds the threshold value, the device will trigger alarm.

Step 7 Set the arming schedule. Refer to Chapter 11.1 Configure Arming Schedule.

Step 8 Set the linkage actions. Refer to Chapter 11.2 Configure Alarm Linkage Actions.

Step 9 Click **Apply**.

12.9 Fast Moving Detection

Purpose

Fast moving detection is used to detect suspicious running and chasing, over speed and fast moving. It will trigger alarm when an object is moving fast and send notification to arming host so that necessary actions can be taken in advance.

Step 1 Go to **System > Event > Smart Event**.

Step 2 Select a camera to configure.

Step 3 Click **Fast Moving**.

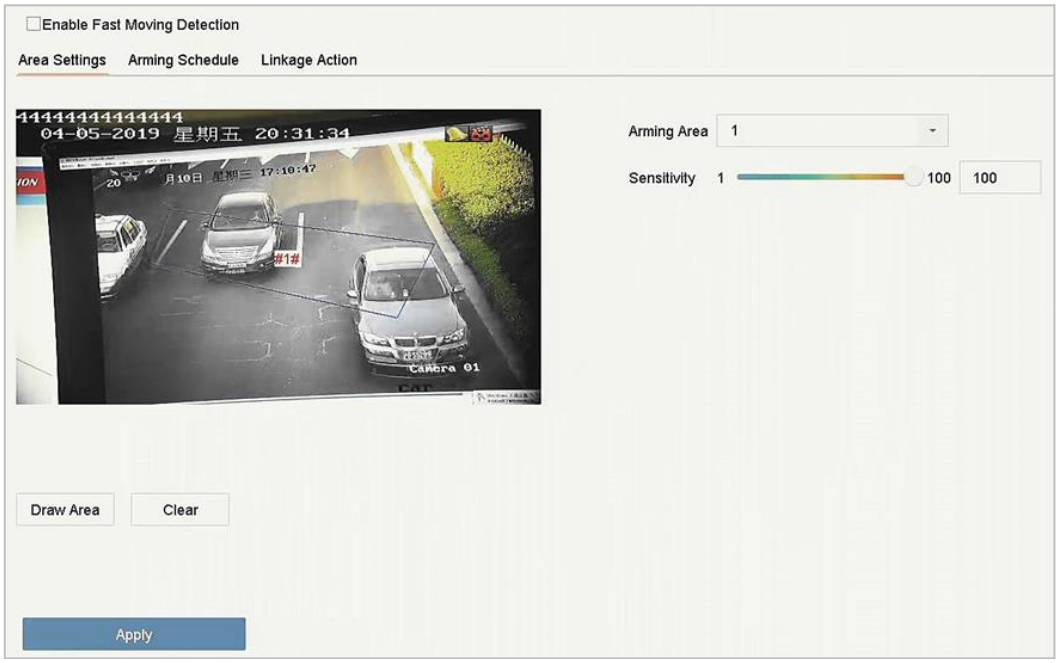


Figure 12-9 Fast Moving Detection

Step 4 Check **Enable Fast Moving**.

Step 5 Optionally, check **Save VCA Picture** to save the captured fast moving detection pictures.

Step 6 Set fast moving detection parameters.

1) Select **Arming Area**. Up to 4 areas are selectable.

Click **Draw Area** to draw a quadrilateral in the preview window by specifying four vertices of the area.

Set Sensitivity.

Sensitivity: Similarity of the background image to the object. The higher the value, the easier the detection alarm will be triggered.

Step 7 Set the arming schedule. Refer to Chapter 11.1 Configure Arming Schedule.

Step 8 Set the linkage actions. Refer to Chapter 11.2 Configure Alarm Linkage Actions.

Step 9 Click **Apply**.

12.10 Parking Detection

Purpose

Parking detection is used to detect parking violation in set area, applied in expressway and one-way street.

Step 1 Go to **System > Event > Smart Event**.

Step 2 Select a camera to configure.

Step 3 Click **Parking**.

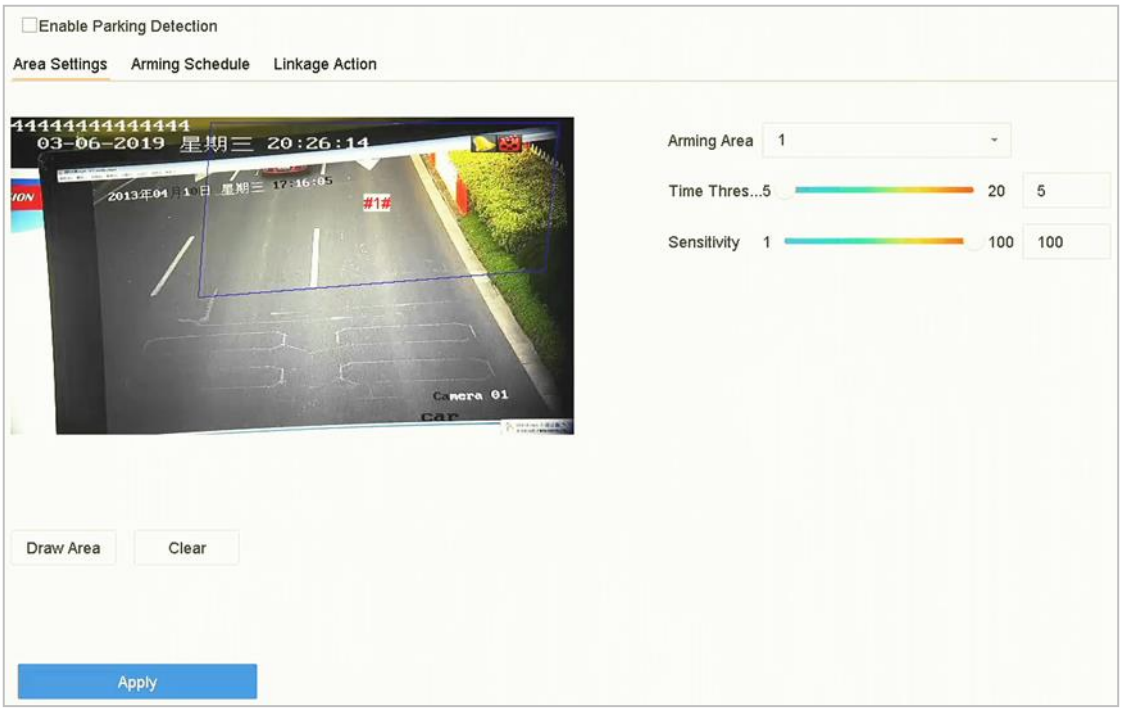


Figure 12-10 Parking Detection

Step 4 Check **Enable Parking Detection**.

Step 5 Optionally, check **Save VCA Picture** to save the captured parking detection pictures.

Step 6 Set parking detection parameters.

6) Select **Arming Area**. Up to 4 areas are selectable.

6) Set **Time Threshold (s).**

Time Threshold: The time of car staying in the region. If the value is 10, an alarm is triggered after the car has stayed in the region for 10s. Its range is [5s-20s].

7) Set **Sensitivity**.

Sensitivity: Similarity of the background image to the object. The higher the value, the easier the detection alarm will be triggered.

Step 7 Set the arming schedule. Refer to Chapter 11.1 Configure Arming Schedule.

Step 8 Set the linkage actions. Refer to Chapter 11.2 Configure Alarm Linkage Actions.

Step 9 Click **Apply**.

12.11 Unattended Baggage Detection

Purpose:

Unattended baggage detection function detects the objects left over in the pre-defined region such as the baggage, purse, dangerous materials, etc., and a series of actions can be taken when the alarm is triggered.

Step 1 Go to **System > Event > Smart Event**.

Step 2 Click **Unattended Baggage**.

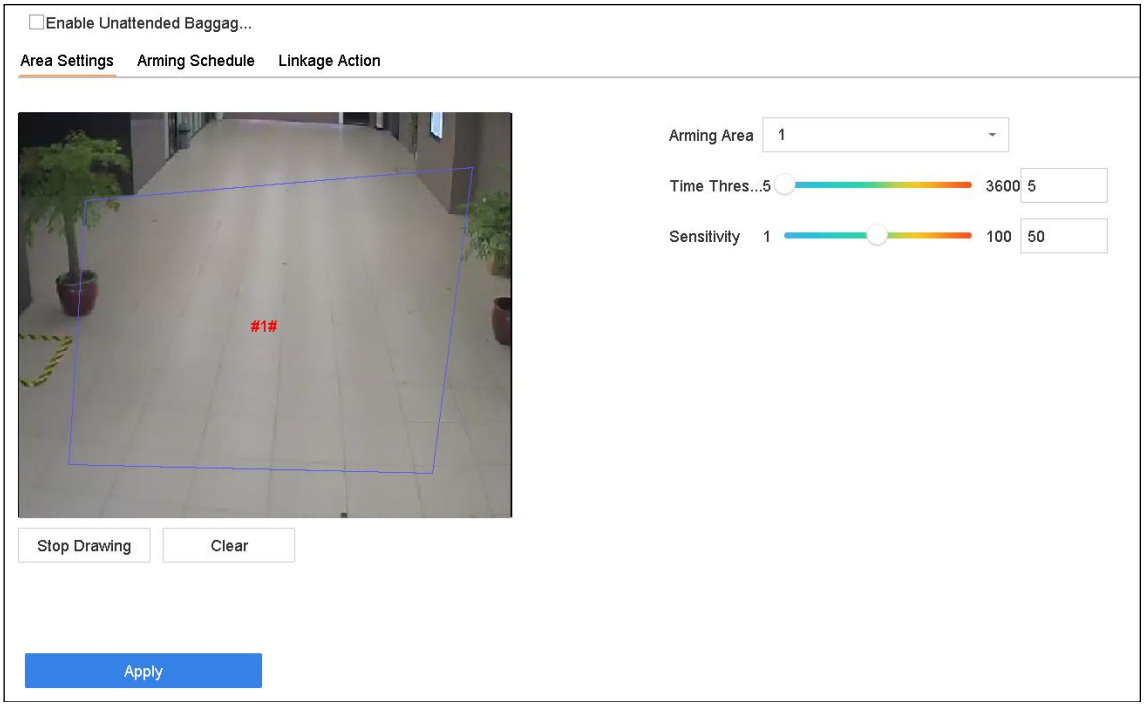


Figure 12-11 Unattended Baggage Detection

Step 3 Select a camera to configure.

Step 4 Check **Enable Unattended Baggage Detection**.

Step 5 Optionally, check **Save VCA Picture** to save the captured pictures of unattended baggage detection.

Step 6 Follow the steps to set the detection rules and detection areas.

1) Select an **Arming Region** to configure. Up to 4 regions are selectable.
2) Drag the sliders to set **Time Threshold** and **Sensitivity**.

   Time Threshold: The time of the objects left over in the region. If the value is 10, alarm is triggered after the object is left and stayed in the region for 10s. Its range is [5s-20s].

   Sensitivity: Similarity degree of the background image. The higher the value is, the more easily the detection alarm can be triggered.

3) Click **Draw Region** and draw a quadrilateral in the preview window by specifying four vertexes of the detection region.

Step 7 Set the arming schedule. Refer to Chapter 11.1 Configure Arming Schedule.

Step 8 Set the linkage actions. Refer to Chapter 11.2 Configure Alarm Linkage Actions.

Step 9 Click **Apply**.

12.12 Object Removal Detection

Purpose:

Object removal detection function detects the objects removed from the pre-defined region, such as the exhibits on display, and a series of actions can be taken when the alarm is triggered.

Step 1 Go to **System > Event > Smart Event**.

Step 2 Click **Object Removable**.

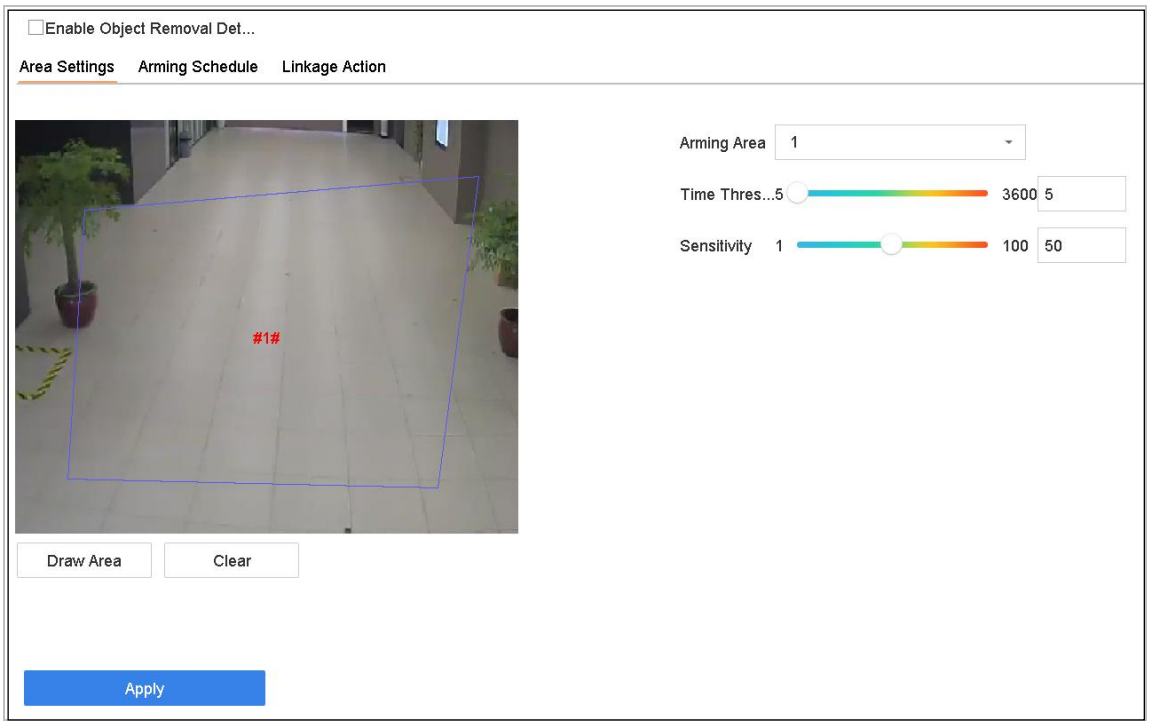


Figure 12-12 Object Removal Detection

Step 3 Select a camera to configure.

Step 4 Check **Enable Object Removable Detection**.

Step 5 Optionally, check **Save VCA Picture** to save the captured pictures of object removable detection.

Step 6 Follow the steps to set the detection rules and detection areas.

1) Select an **Arming Area** to configure. Up to 4 regions are selectable.
Drag the sliders to set **Time Threshold and Sensitivity**.

Time Threshold: The time of the objects removed from the region. If the value is 10, alarm is triggered after the object disappeared from the region for 10s. Its range is [5s-20s].

Sensitivity: The similarity degree of the background image. Usually, when the sensitivity is high, a very small object taken from the region can trigger the alarm.

Click **Draw Area** and draw a quadrilateral in the preview window by specifying four vertexes of the detection region.

Step 7 Set the arming schedule. Refer to Chapter 11.1 Configure Arming Schedule.

Step 8 Set the linkage actions. Refer to Chapter 11.2 Configure Alarm Linkage Actions.

Step 9 Click **Apply**.

12.13 Audio Exception Detection

Purpose:

Audio exception detection detects the abnormal sounds in the surveillance scene, such as the sudden increase/decrease of the sound intensity.

Step 1 Go to **System > Event > Smart Event**.

Step 2 Click **Audio Exception**.

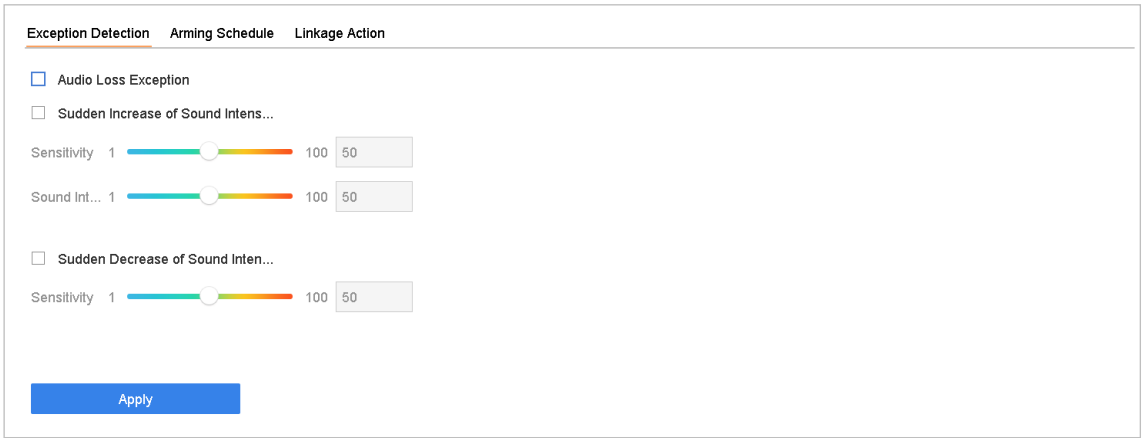


Figure 12-13 Audio Exception Detection

Step 3 Select a camera to configure.

Step 4 Optionally, check **Save VCA Picture** to save the captured pictures of audio exception detection.

Step 5 Follow the steps to set the detection rules.

1) Select **Exception Detection**.
2) Check **Audio Loss Exception, Sudden Increase of Sound Intensity Detection,** or **Sudden Decrease of Sound Intensity Detection.**

Audio Loss Exception: Detects the sound steep rise in the surveillance scene. You can set the detection sensitivity and threshold for sound steep rise. You need to configure its **Sensitivity** and **Sound Intensity Threshold**.

Sensitivity: The smaller the value is, the more severe the change should be to trigger the detection. Range [1-100].

Sound Intensity Threshold: It can filter the sound in the environment. The louder the environment sound, the higher the value should be. Adjust it according to the environment. Range [1-100].

Sudden Decrease of Sound Intensity Detection: Detects the sound steep drop in the surveillance scene. You need set the detection sensitivity [1-100].

Step 6 Set the arming schedule. Refer to Chapter 11.1 Configure Arming Schedule.

Step 7 Set the linkage actions. Refer to Chapter 11.2 Configure Alarm Linkage Actions.

Step 8 Click **Apply**.

12.14 Sudden Scene Change Detection

Purpose:

Scene change detection detects the change of surveillance environment affected by the external factors, such as the intentional rotation of the camera.

Step 1 Go to **System > Event > Smart Event**.

Step 2 Click **Sudden Scene Change**.

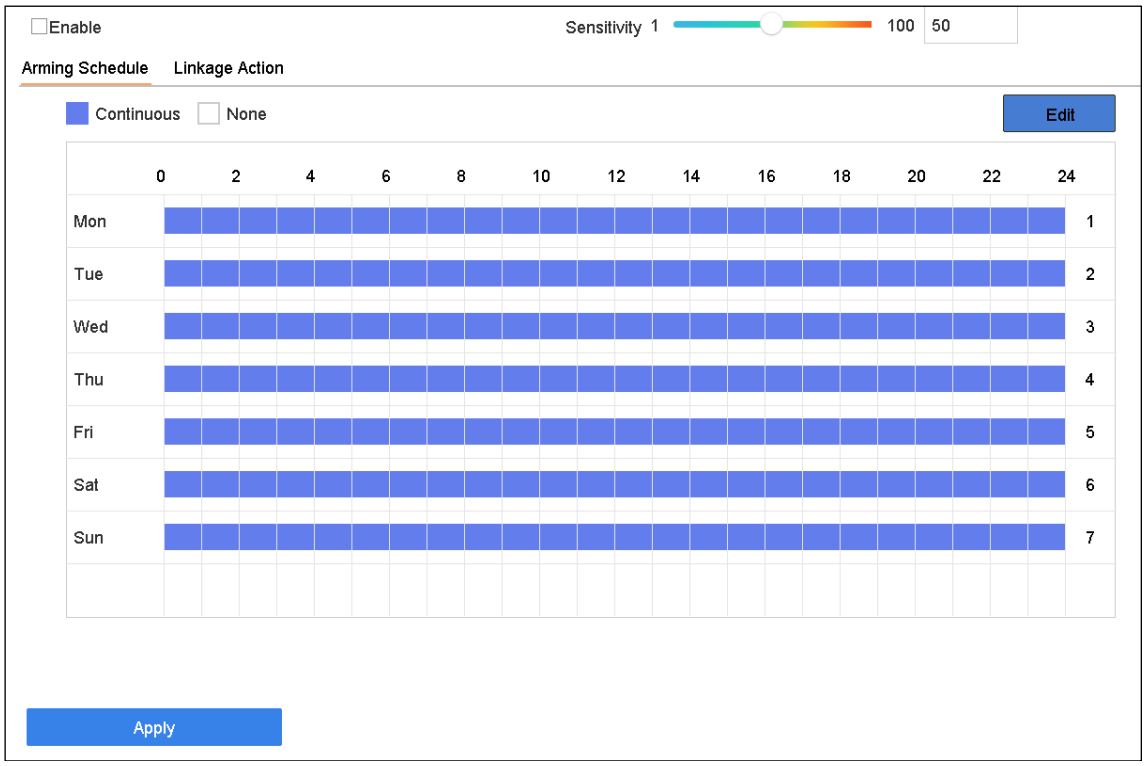


Figure 12-14 Sudden Scene Change

Step 3 Select a camera to configure.

Step 4 Check **Enable Sudden Scene Change Detection**.

Step 5 Optionally, check **Save VCA Picture** to save the captured pictures of sudden scene change detection.

Step 6 Drag the **Sensitivity** slider to set the detection sensitivity. Sensitivity range: [1-100]. The higher the value is, the more easily the change of scene can trigger the alarm.

Step 7 Set the arming schedule. Refer to Chapter 11.1 Configure Arming Schedule.

Step 8 Set the linkage actions. Refer to Chapter 11.2 Configure Alarm Linkage Actions.

Step 9 Click **Apply**.

12.15 Defocus Detection

Purpose:

The image blur caused by defocus of the lens can be detected.

Step 1 Go to **System > Event > Smart Event**.

Step 2 Click **Defocus**.

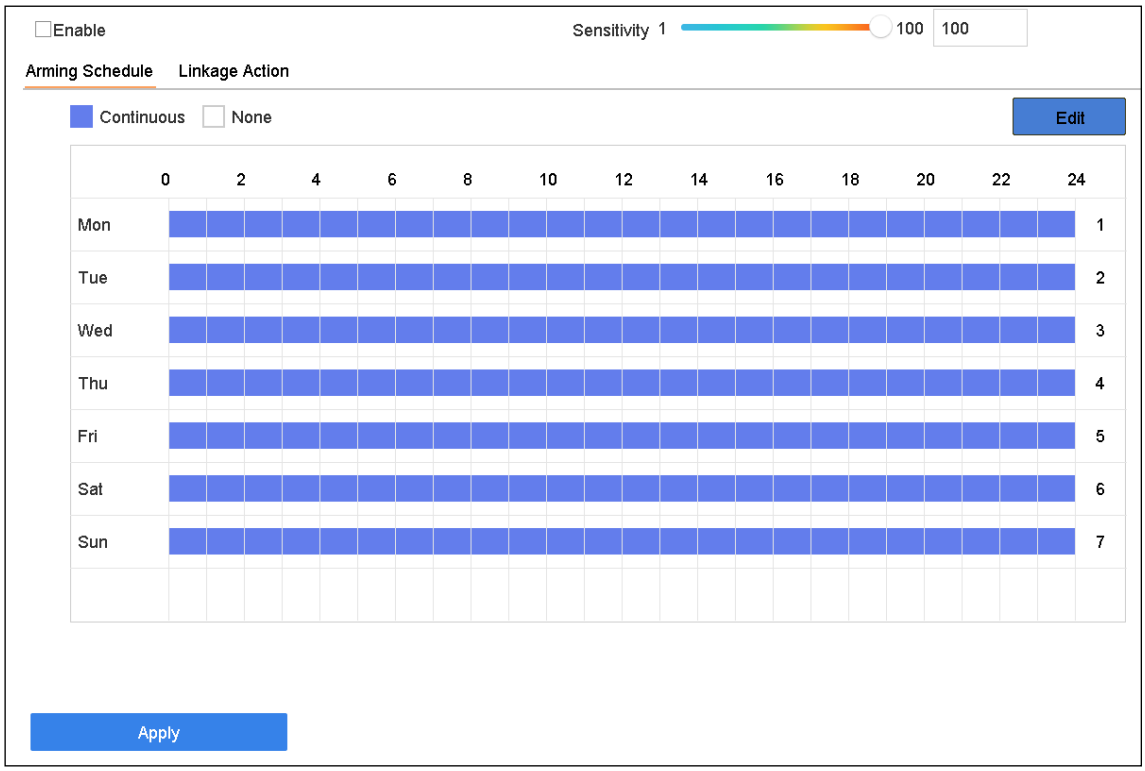


Figure 12-15 Defocus Detection

Step 3 Select a camera to configure.

Step 4 Check **Enable Defocus Detection**.

Step 5 Optionally, check **Save VCA Picture** to save the captured pictures of defocus detection.

Step 6 Drag the **Sensitivity** slider to set the detection sensitivity. Sensitivity range: [1-100]. The higher the value is, the more easily the defocus image can be detected.

Step 7 Set the arming schedule. Refer to Chapter 11.1 Configure Arming Schedule.

Step 8 Set the linkage actions. Refer to Chapter 11.2 Configure Alarm Linkage Actions.

Step 9 Click **Apply**.

12.16 PIR Alarm

Purpose:

A PIR (Passive Infrared) alarm is triggered when an intruder moves within the detector vision field. The heat energy dissipated by a person, or any other warm blooded creature such as dogs, cats, etc., can be detected.

Step 1 Go to **System > Event > Smart Event**.

Step 2 Click **PIR Alarm**.

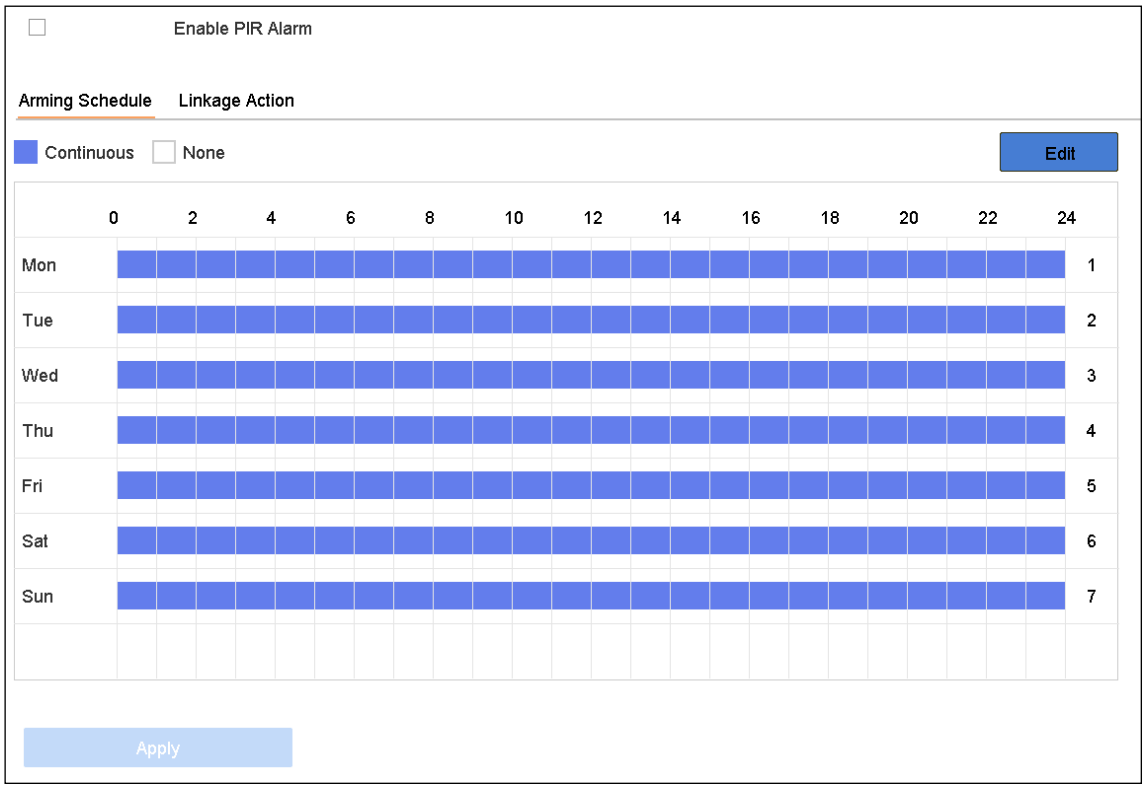


Figure 12-16 FIR Alarm

Step 3 Select a camera to configure.

Step 4 Check **PIR Alarm**.

Step 5 Optionally, check **Save VCA Picture** to save the captured pictures of PIR alarm.

Step 6 Set the arming schedule. Refer to Chapter 11.1 Configure Arming Schedule.

Step 7 Set the linkage actions. Refer to Chapter 11.2 Configure Alarm Linkage Actions.

Step 8 Click **Apply**.

Chapter 13 Smart Analysis

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

13.1 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.

Step 1 Go to **Smart Analysis** > **Counting**.

Step 2 Select the camera.

Step 3 Select the report type to **Daily Report, Weekly Report, Monthly Report**, or **Annual Report**.

Step 4 Set the **Date** to analyze. Then the people counting graphic will show.

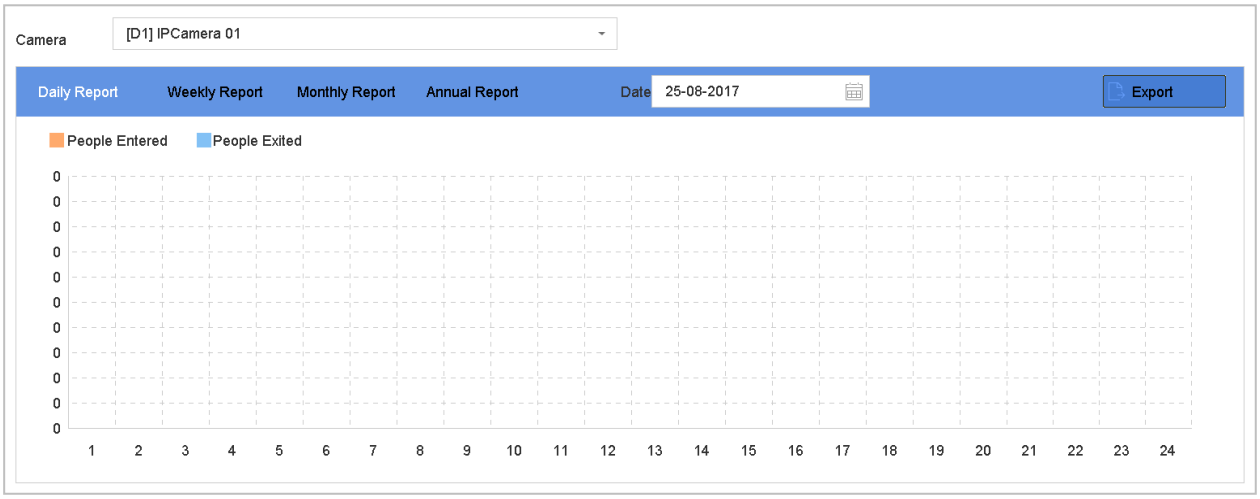


Figure 13-1 People Counting Interface

Step 5 (Optional) Click **Export** to export the report in excel format.

13.2 Heat Map

Purpose:

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

The heat map function must be supported by the connected IP camera and the corresponding configuration must be set.

Step 1 Go to **Smart Analysis > Heat Map**.

Step 2 Select a camera.

Step 3 Select the report type as **Daily Report, Weekly Report, Monthly Report**, or **Annual Report.**

Step 4 Set the **Data** to analyze.

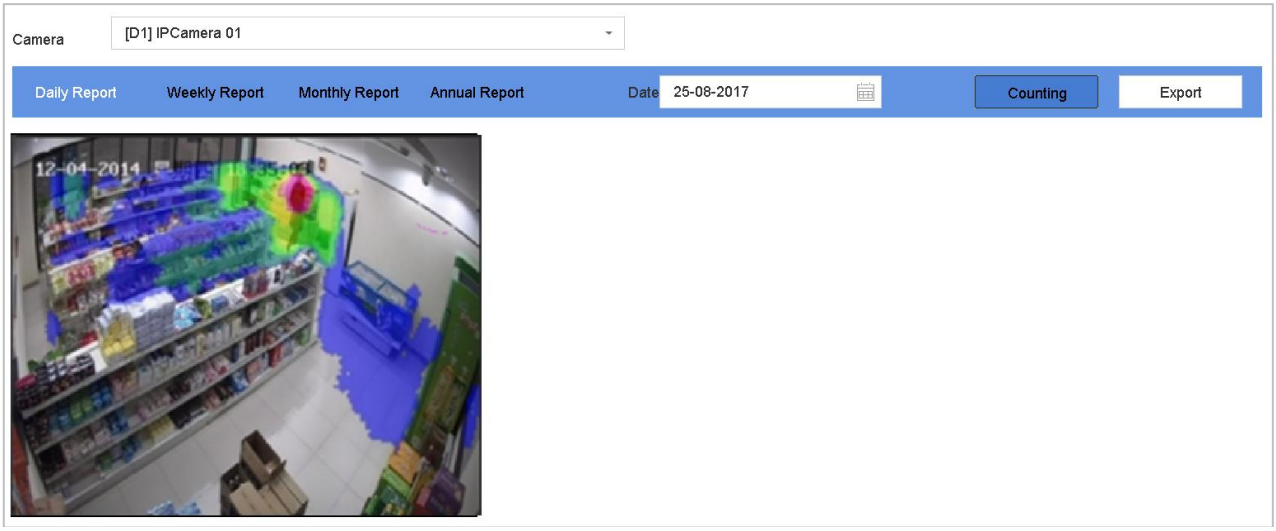


Figure 13-2 Heat Map Interface

Step 5 Click **Counting**. Then the results displayed in graphics marked in different colors will show.

NOTE

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.

Step 6 (Optional) Click **Export** to export the statistics report in excel format.

Chapter 14 Network Settings

14.1 Configure TCP/IP Settings

Purpose

TCP/IP settings must be properly configured before you can operate the device over network.

14.1.1 Device with Dual Network Interface

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

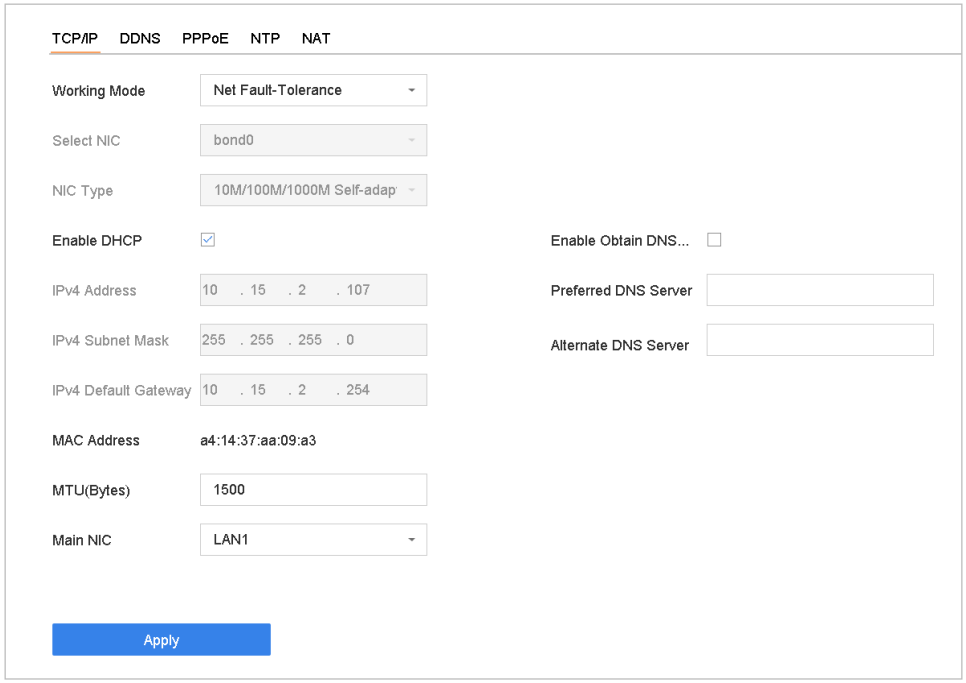


Figure 14-1 TCP/IP Settings

Step 2 Select **Net-Fault Tolerance** or **Multi-Address Mode** under Working Mode.

- **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.
- **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.

Step 3 Configure other IP settings as needed.

NOTE

- 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 9676.

Step 4 Click **Apply**.

14.1.2 Device with a Single Network Interface

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

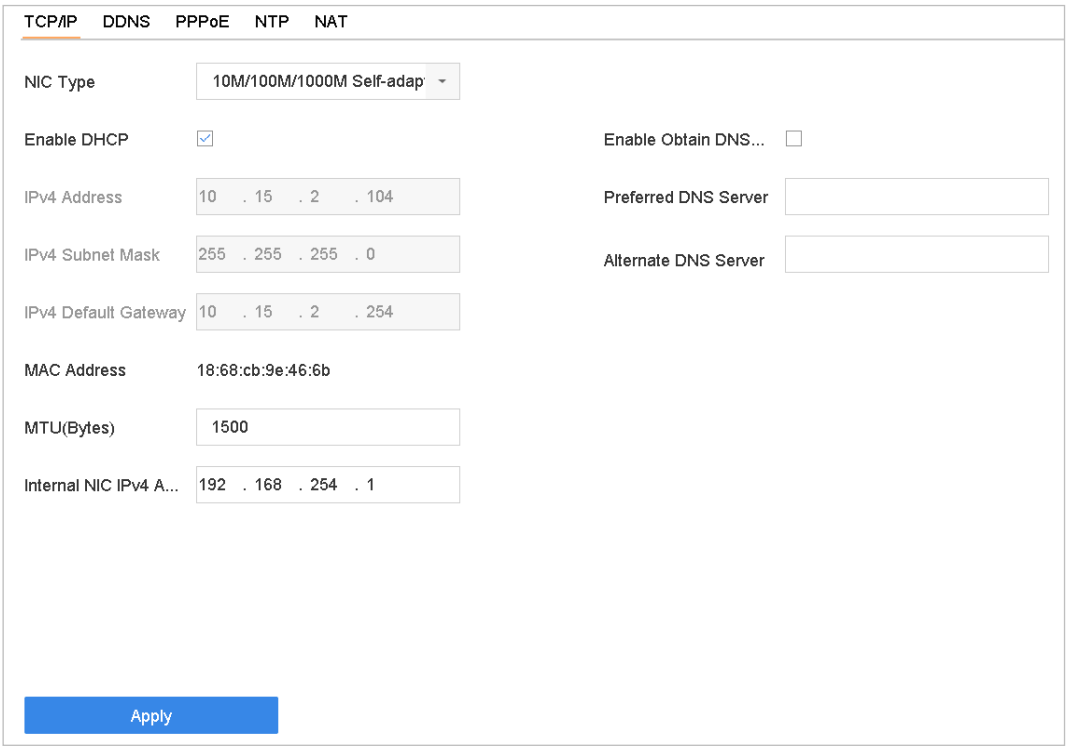


Figure 14-2 TCP/IP Settings

Step 2 Configure network parameters as needed.

NOTE

- 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 9676.

Step 3 Click **Apply**.

14.2 Configure Guarding Vision

Purpose

Guarding Vision 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 system.

Step 1 Go to **System** > **Network** > **Advanced** > **Platform Access**.

Step 2 Check **Enable** to activate the function. Then the service terms will pop up.

1) Enter the verification code in **Verification Code**.

Scan the QR code to read the service terms and privacy statement.

Check The Guarding Vision service will require internet access. Please read Service Terms and Privacy Statement before enabling the service if you agree the service terms and privacy statement.

Click **OK** to save the settings.

NOTE

- Guarding Vision is disabled by default.
- The verification code is empty by default. It must contain 6 to 12 letters or numbers, and it is case sensitive.

Step 3 (Optional) Check **Custom** to enter the server address as your desire.

Step 4 (Optional) Check **Enable Stream Encryption**, verification code is required for remote access and live view.

Step 5 (Optional) Click **Unbind** if the device requires to unbind with the current Guarding Vision account.

Step 6 Click **Apply**.

What to do next:

After configuration, you can access and manage your devices through Guarding Vision app or website.

14.3 Configure EHome

Purpose

EHome protocol is non-open and push-mode protocol based on TCP/UDP, which can realize the communication between the system and mobile devices (e.g., body camera, MNVR, etc.). The system is as a server and you can register the device to the system. The protocol is suitable for the application of dynamic device IP address.

Step 1 Go to **System** > **Network** > **Advanced** > **Platform Access**.

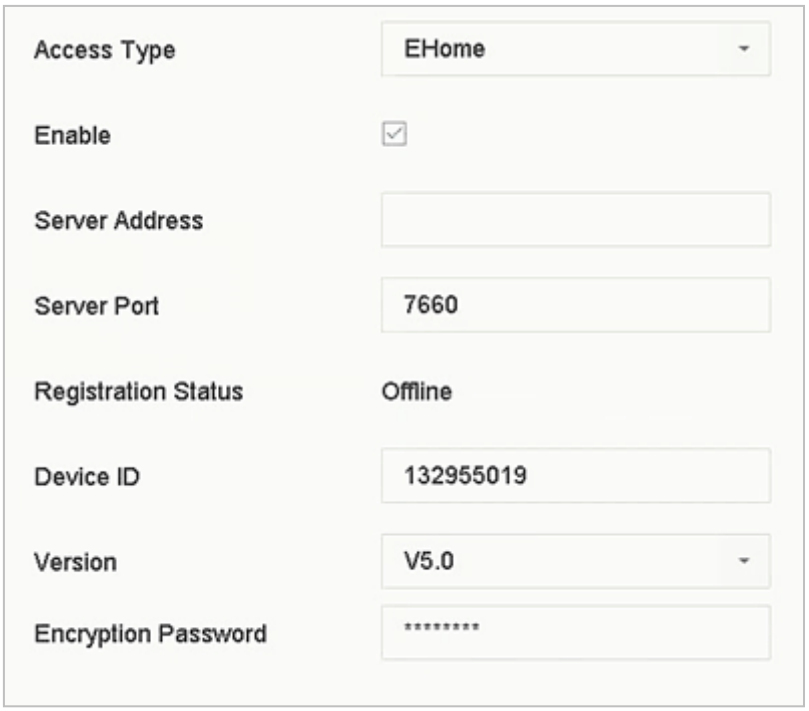


Figure 14-3 EHome Settings

Step 2 Select **Access Type** as EHome.

Step 3 Check **Enable**.

NOTE

Enabling EHome will disable Guarding Vision platform access.

Step 4 Set the related parameters, including **Server Address**, **Server Port**, **Device ID**, **Version**, and **Encryption Password**.

- **Server Address**: The platform server IP address.
- **Server Port**: The platform server port, ranges from 1024 to 65535. The actual port shall be provided by the platform.
- **Device ID**: The Device ID shall be provided by the platform.
- **Version**: EHome protocol version, only V5.0 is available.
- **Encryption Password**: Encryption password is required when using EHome V5.0 version, it provides more secure communication between the device and platform. Enter it for verification after the device is registered to the EHome platform.

Step 5 Click **Apply** to save the settings and restart the device.

What to do next:

You can see the registration status (online or offline) after the device is restarted.

14.4 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.

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

Step 2 Check **Enable**.

Step 3 Select **DynDNS** under **DDNS Type**.

NOTE

PeanutHull and NO-IP are also available under DDNS Type, and required information should be entered accordingly.

Step 4 Enter **Server Address** for **DynDNS** (i.e. members.dyndns.org).

Step 5 Under **Device Domain Name**, enter the domain name obtained from the DynDNS website.

Step 6 Enter the **User Name** and **Password** registered in the DynDNS website.

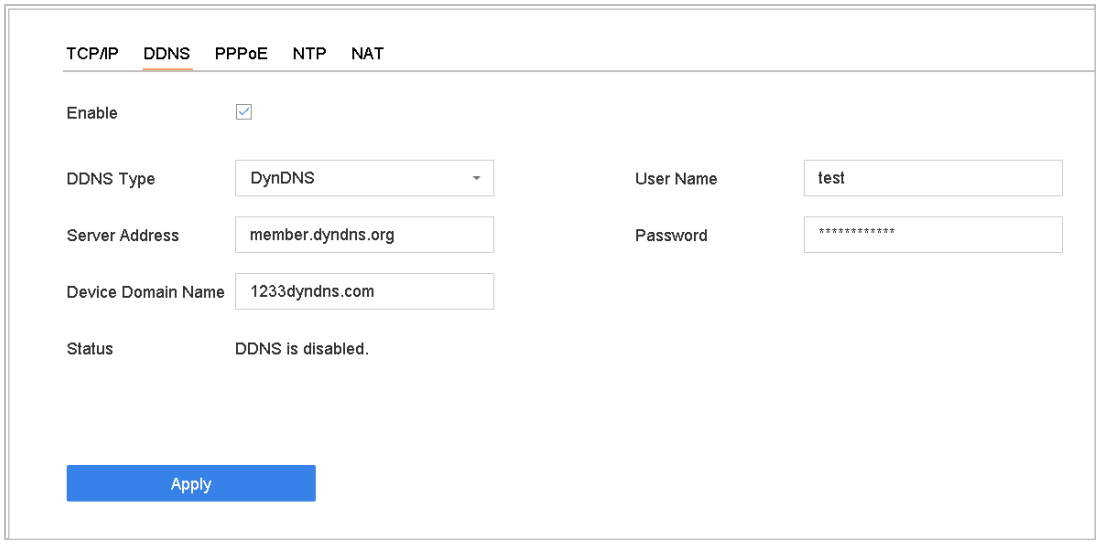


Figure 14-4 DDNS Settings

Step 7 Click **Apply**.

14.5 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**.

NOTE

Contact your Internet service provider for details about PPPoE service.

14.6 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.

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

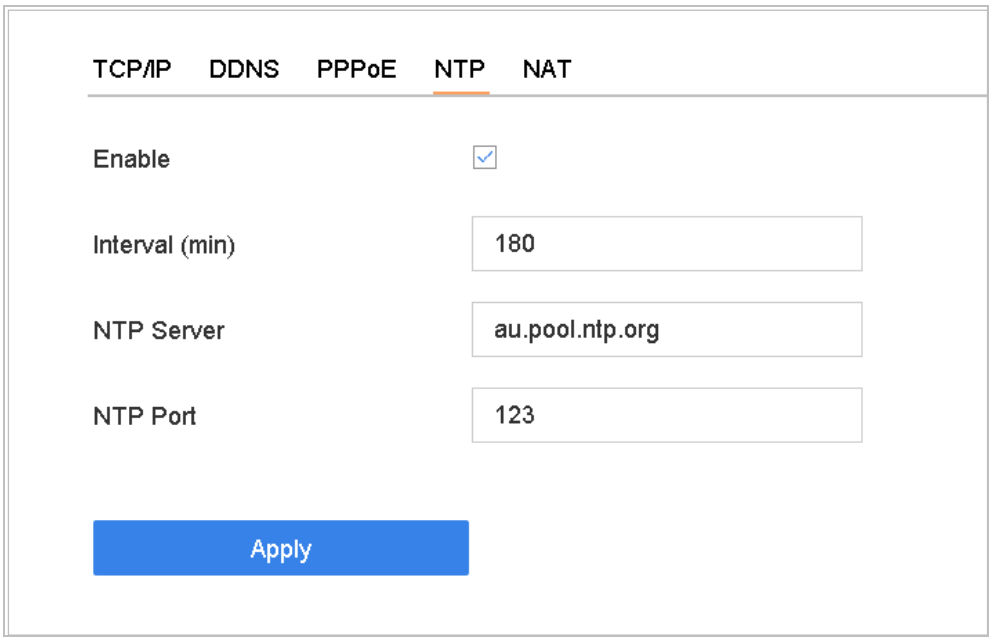


Figure 14-5 NTP Settings

Step 2 Check **Enable**.

Step 3 Configure NTP settings as need.

- **Interval (min)**: Time interval between two time synchronization with NTP server.
- **NTP Server**: IP address of the NTP server.
- **NTP Port**: Port of the NTP server.

Step 4 Click **Apply**.

14.7 Configure SNMP

Purpose

You can configure SNMP settings to get device status and parameter information.

Before You Start

Download the SNMP software to receive device information via SNMP port. By setting the trap address and port, the device is allowed to send alarm event and exception message to the surveillance center.

Step 1 Go to **System** > **Network** > **Advanced** > **SNMP**.

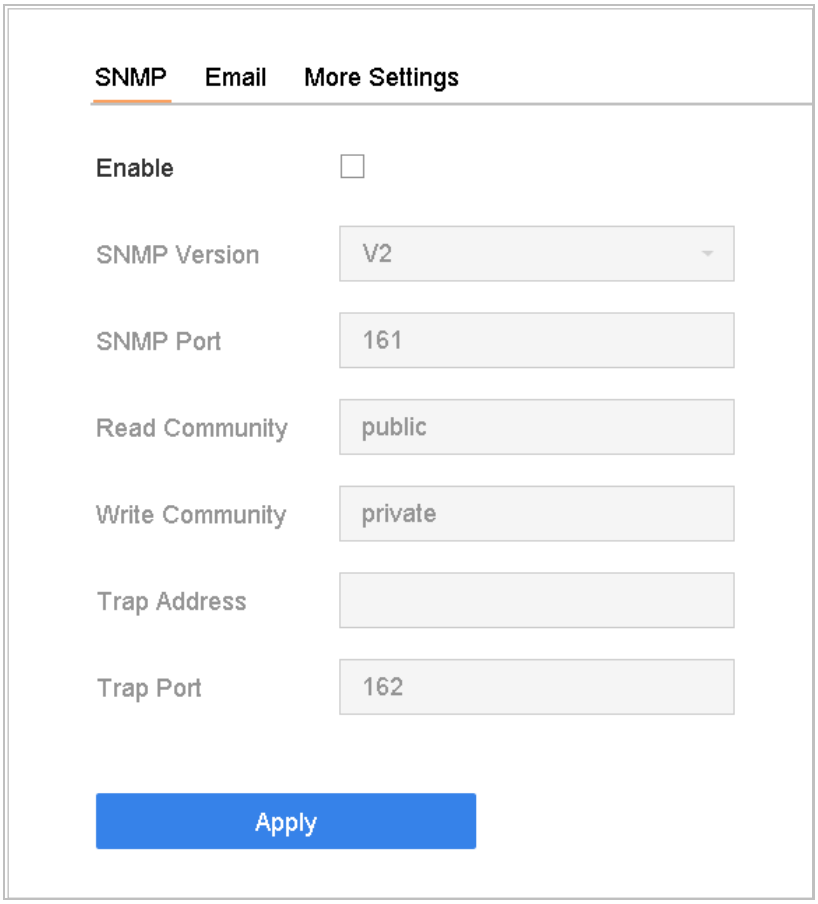


Figure 14-6 SNMP Settings

Step 2 Check **Enable**. A message will pop up to prompt possible security risk and click **Yes** to continue.

Step 3 Configure the SNMP settings as needed.

- **Trap Address**: IP address of the SNMP host.
- **Trap Port**: Port of the SNMP host.

Step 4 Click **Apply**.

14.8 Configure Email

Purpose

The system can be configured to send an Email notification to all designated users when a specified event occur, 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 also be connected to either an intranet or the Internet depending on the location of the e-mail accounts to which you want to send notification.

Step 1 Go to **System** > **Network** > **Advanced** > **Email**.

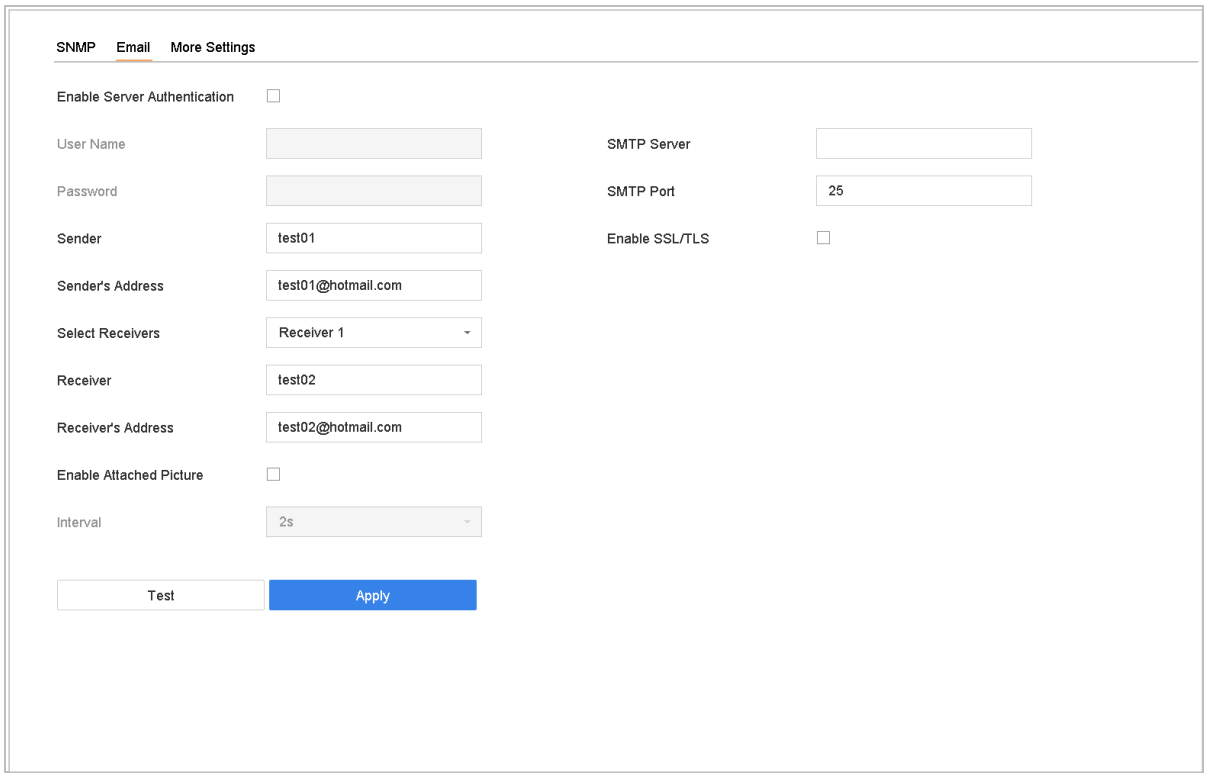


Figure 14-7 Email Settings

Step 2 Configure the following 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.

Step 3 Click **Apply**.

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

14.9 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.

- **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 (e.g., iVMS-4200) 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 an 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 to control streaming media servers. The port is 554 by default.
- **Enhanced SDK Service Port**: The enhanced SDK service adopts TLS protocol over the SDK service that provides safer data transmission. The port is 8443 by default.

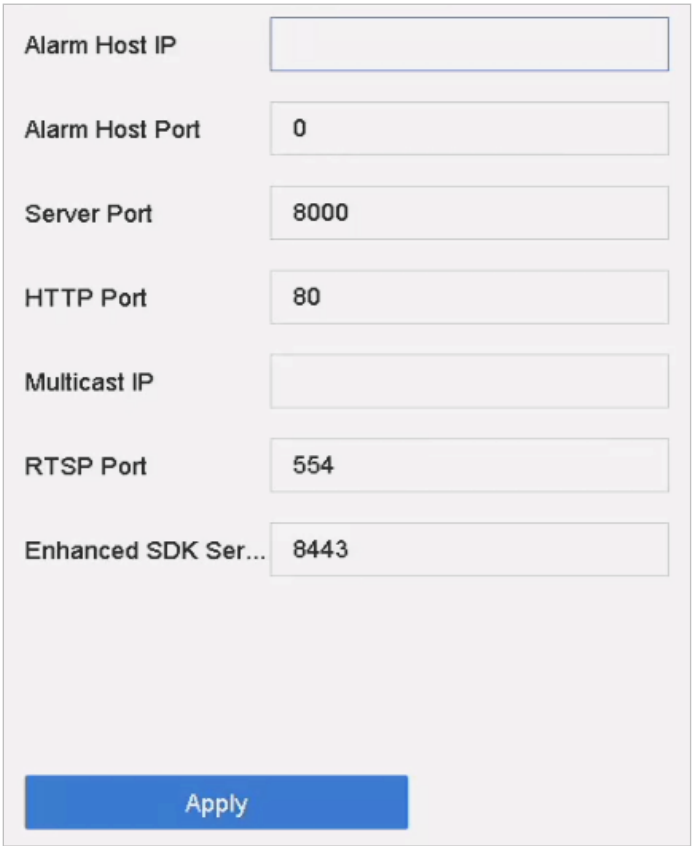


Figure 14-8 Port Settings

Chapter 15 User Management and Security

15.1 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 users and configure user parameters.

15.1.1 Add a User

Step 1 Go to **System** > **User**.

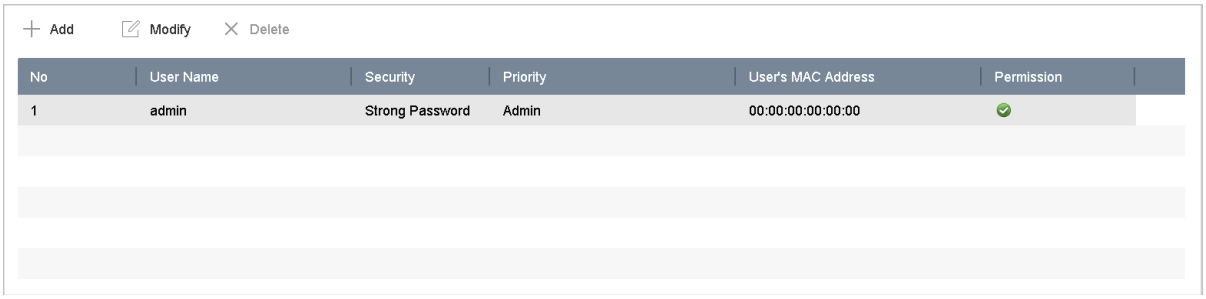


Figure 15-1 User Management Interface

Step 2 Click **Add** to enter the operation permission interface.

Step 3 Input the admin password and click **OK**.

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

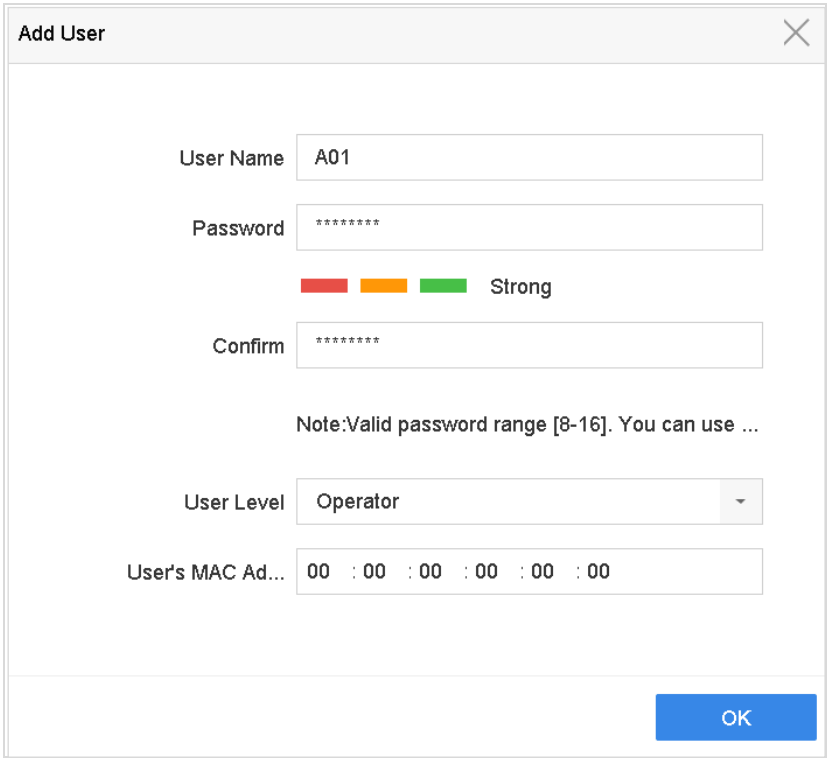


Figure 15-2 Add User

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. We also recommend that you reset your password regularly. Especially in the high security systems, 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:** An *Operator* user level has Two-way Audio permission in Remote Configuration and all operating permissions 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 that logs onto the device. If it is configured and enabled, it allows only the remote user with this MAC address to access the device.

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

Step 6 In the User Management interface, the added new user is displayed on the list.

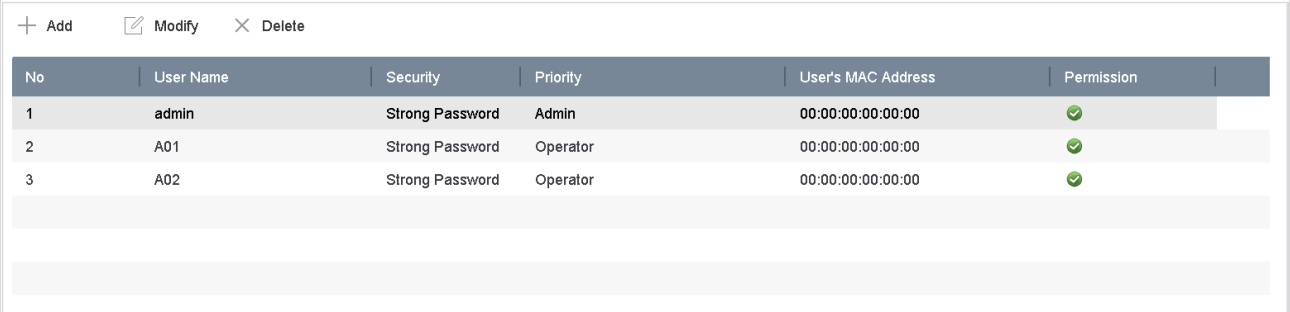


Figure 15-3 User List

15.1.2 Edit the Admin User

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

Step 1 Go to **System** > **User**.

Step 2 Select the admin user from the list.

Step 3 Click **Modify**.

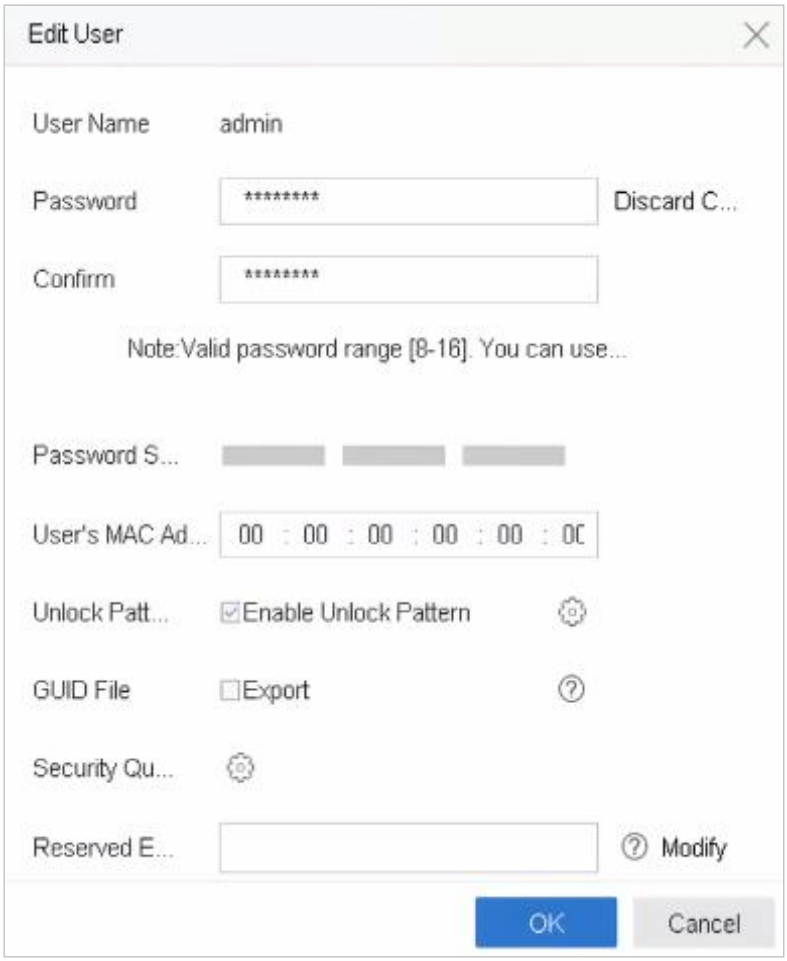


Figure 15-4 Edit User (Admin)

Step 4 Edit the admin user information as desired, including a new admin password (strong password is required) and MAC address.

Step 5 Edit the unlock pattern for the admin user account.

1) Check **Enable Unlock Pattern** to enable the use of an unlock pattern when logging in to the device.
2) Use the mouse to draw a pattern among the 9 dots on the screen, and release the mouse when the pattern is done.

Step 6 Check **Export** of **Export GUID** to export the GUID file for the admin user account.

NOTE

When the admin password is changed, export the new GUID to the connected USB flash disk in the Import/Export interface for the future password resetting.

Step 7 Configure security question for password resetting.

Step 8 Configure reserved email for password resetting.

Step 9 Click **OK** to save the settings.

15.1.3 Edit an Operator/Guest User

You can edit the user information, including user name, password, permission level, and MAC address. Check **Change Password** to change the password, and input the new password in the text field of **Password** and **Confirm**. A strong password is recommended.

Step 1 Go to **System** > **User**.

Step 2 Select a user from the list and click **Modify**.

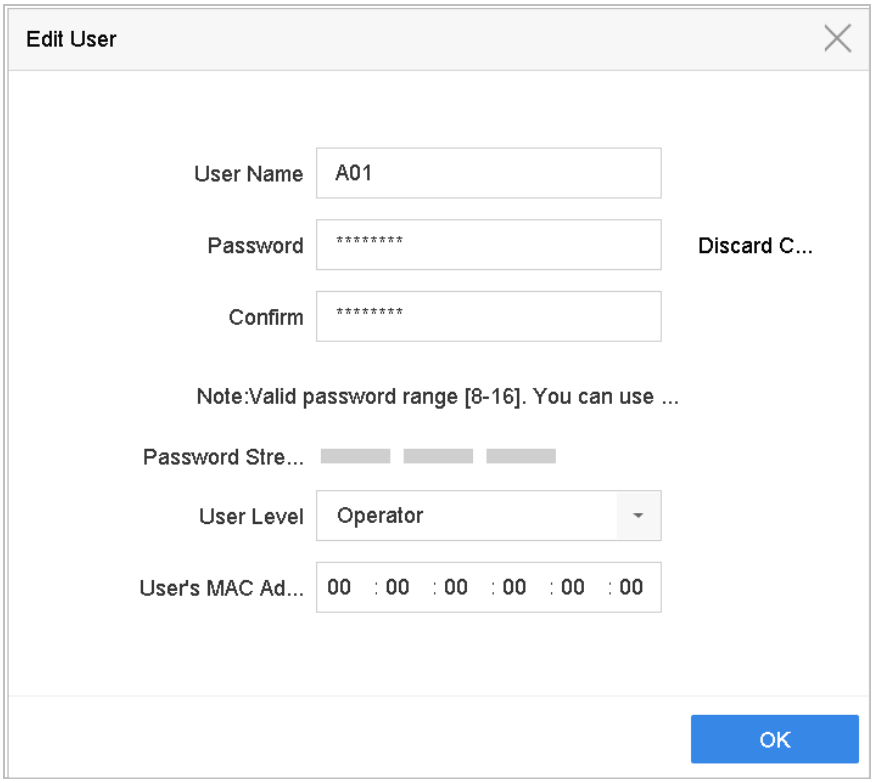


Figure 15-5 Edit User (Operator/Guest)

Step 3 Edit the user information as desired, including the new password (strong password is required) and MAC address.

15.1.4 Delete a User

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

Step 1 Go to **System** > **User**.

Step 2 Select a user from the list.

Step 3 Click **Delete** to delete the selected user account.

15.2 Manage User Permissions

15.2.1 Set User Permissions

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

Step 1 Go to **System** > **User**.

Step 2 Select a user from the list, and then click  to enter the permission settings interface.

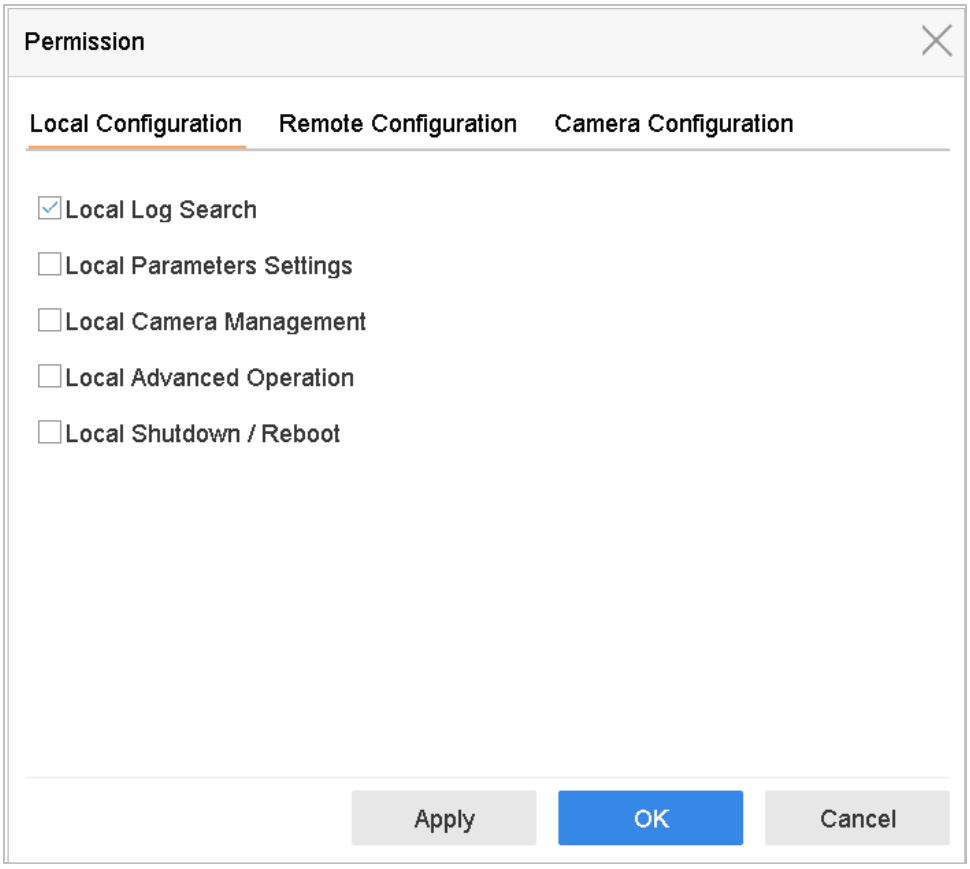


Figure 15-6 User Permission Settings Interface

Step 3 Set the user's operating permissions for Local Configuration, Remote Configuration, and Camera Configuration for the user.

- 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: 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.

- 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 port settings.

Remote Video Output Control: Sending remote button control signals.

Two-Way Audio: Operating the 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.

- Camera Configuration

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). Available for double verification function, refer to 15.2.4 Set Double Verification Permission for Non-Admin Users for details.

Remote Playback/Download: Remotely playing back or downloading recorded files of the selected camera(s). Available for double verification function, refer to 15.2.4 Set Double Verification Permission for Non-Admin Users for details.

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). Available for double verification function, refer to 15.2.4 Set Double Verification Permission for Non-Admin Users for details.

Local Live View: View live video of the selected camera(s) in local.

Step 4 Click **OK** to save the settings.

NOTE

Only the admin user account has the permission to restore factory default parameters.

15.2.2 Set Local Live View Permission for Non-Admin Users

The admin user can assign to normal users (Operator or Guest) the live view permission for specific cameras.

Step 1 Go to **System** > **User**.

Step 2 Click .

Step 3 Input admin password and click **OK**.

Step 4 Select cameras that a non-admin user can view locally and click **OK.**

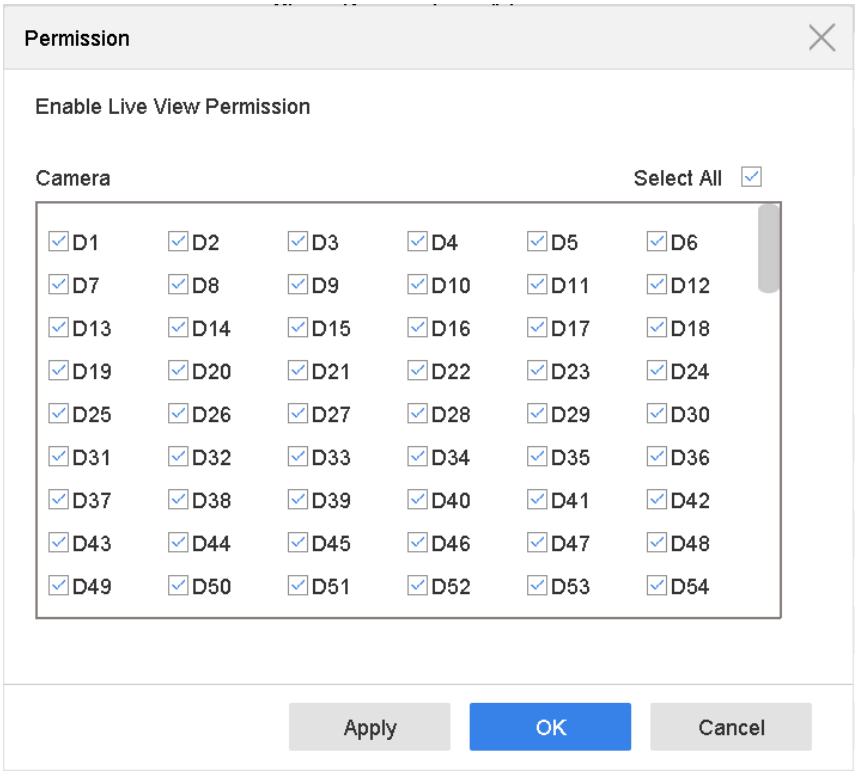


Figure 15-7 Set Live View Permissions

Step 5 Click  of non-admin user.

Step 6 Click the **Camera Configuration** tab.

Step 7 Select Camera Permission as **Local Live View**.

Step 8 Select cameras to display in Live View.

Step 9 Click **OK**.

15.2.3 Set Live View Permission on Lock Screen

The admin user can set live view permission for specific cameras in the screen lock status of device.

Step 1 Go to **System** > **User**.

Step 2 Click **Live View Permission on Lock Screen**.

Step 3 Input admin password and click **Next.**

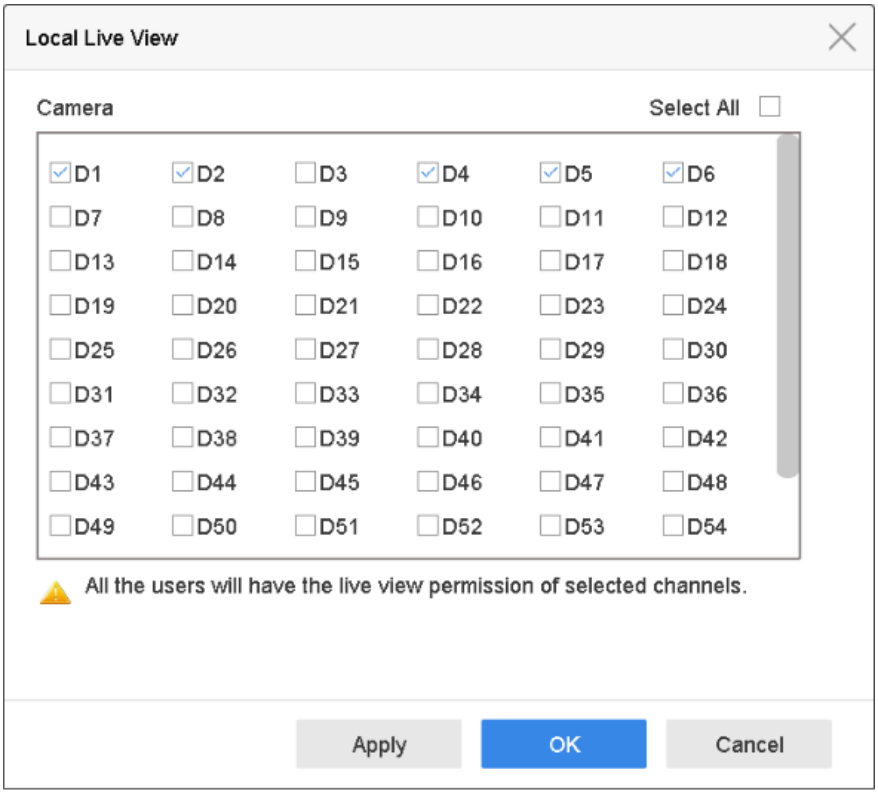


Figure 15-8 Set Live View Permissions on Lock Screen

Step 4 Set the permissions.

- Select the camera (s) to allow live view when the current user account is in logout status.
- Deselect the camera (s) to forbidden the camera (s) being viewed when the current user account is in logout status.

Step 5 Click **OK**.

NOTE

- The *admin* user can set this permission for user accounts.
- When the normal user (Operator or Guest) has no local live view permission for specific camera (s) (refer to 15.2.2 Set Local Live View Permission for Non-Admin Users), the live view permission for such camera (s) on lock screen status cannot be configured (live view not allowed by default).

15.2.4 Set Double Verification Permission for Non-Admin Users

After double verification is enabled in the channel, a non-admin user must be verified by an authorized user to get the permission. Only admin has the authorization to set double verification.

Step 1 Go to **Maintenance** > **System Service** > **Double Verification Settings**.

Step 2 Check **Enable Double Verification**.

Step 3 Set double verification user. The double verification is different from the system user. You can add up to 8 double verification users.

4. Click **Add** to add a double verification user.
5. Enter the admin password.
6. Set the user parameters, including user name, password, camera permission, etc.
7. Click **OK**.

Figure 15-9 Set Double Verification User

Step 4 Click **Apply**.

Step 5 Go to **System** > **User**.

Step 6 Click to edit user permission.

Step 7 Select **Camera Permission**. Only **Local Playback**, **Remote Playback/Download**, and **Local Video Export** are available for double verification.

Step 8 Select the channel(s) that requires double verification.

Step 9 Click **OK**.

15.3 Configure Password Security

15.3.1 Export GUID File

The GUID file may help you to reset password when you forget password.

Step 1 Select to export GUID file when you are activating the device, or editing the admin user account.

Step 2 Insert the U flash disk to your device, and export the GUID file to the U flash disk.

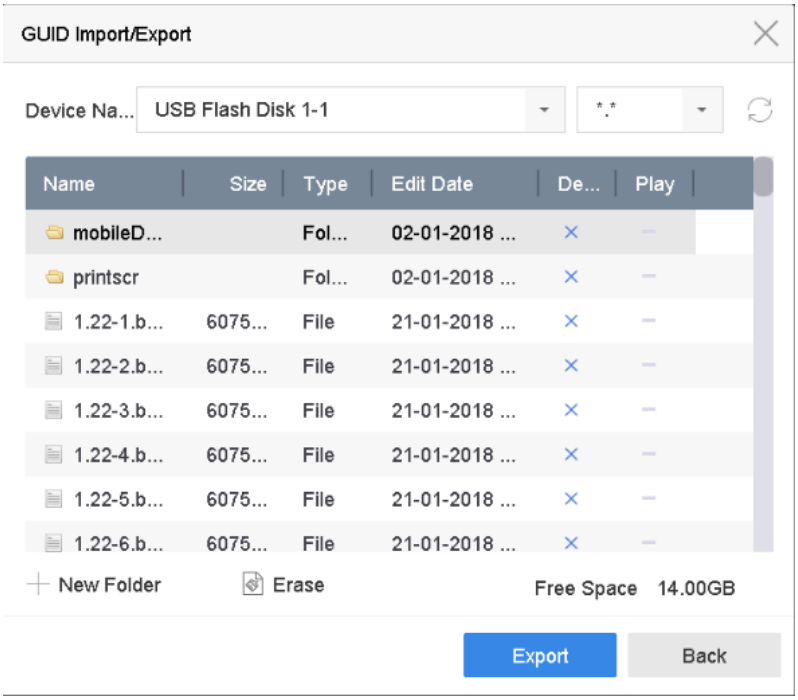


Figure 15-10 Export GUID File

NOTE

Please keep your GUID file properly for future password resetting.

15.3.2 Configure Security Questions

The security question configuration may help you to reset password when you forget your password or encounter security issues.

Step 1 Click **Security Question Configuration** when you are activating the device, or editing the admin user account.

Step 2 Select three security questions from the drop-down list and input the answers.

Step 3 Click **OK**.

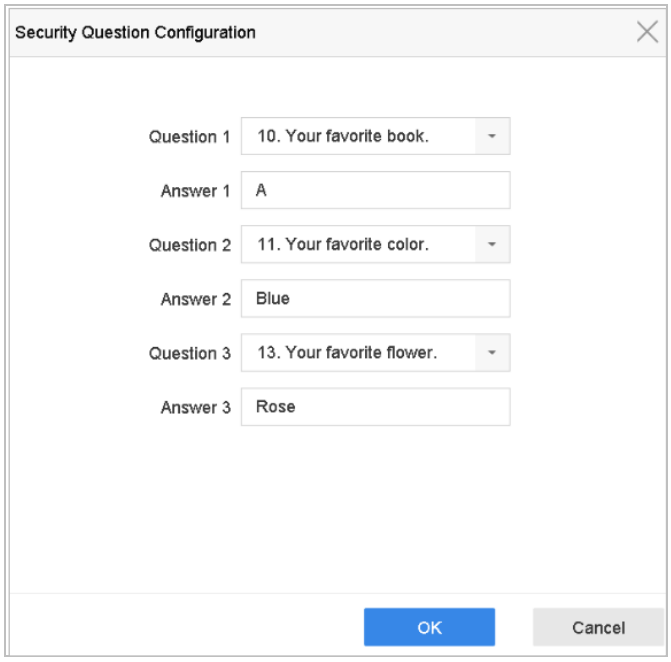


Figure 15-11 Configure Security Questions

15.3.3 Configure Reserved Email

Purpose:

The reserved email will help you to reset password when you forget your password.

Step 1 Check **Reserved E-mail** when you are activating the device, or click **Modify** when you are editing the admin user account.

Step 2 Enter reserved email address.

Step 3 Click **OK.**

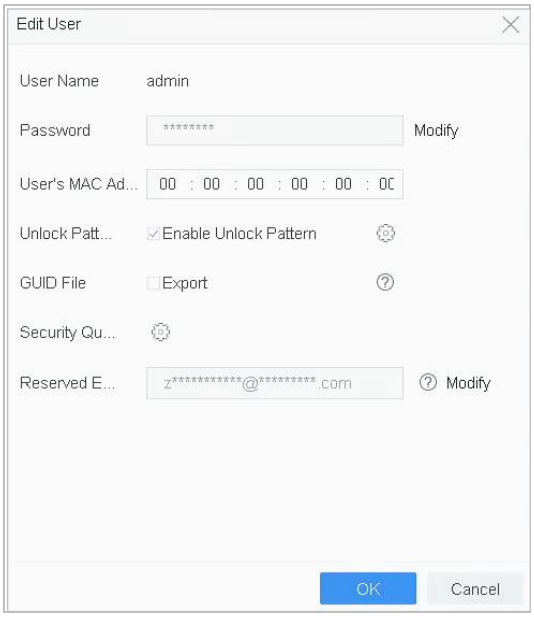


Figure 15-12 Configure Reserved Email

15.4 Reset Password

When you forget the admin password, you can reset the password by importing the GUID file, answering security questions, or entering verification code from your reserved email .

15.4.1 Reset Password by GUID

Before You Start

The GUID file must be exported and saved in the local U flash disk after you have activated the device or edited the admin user account. (Refer to Chapter 15.3.1 Export GUID File).

Step 1 On the user login interface, click **Forgot Password**.

Step 2 Select the password resetting type to **Verify by GUID**.

NOTE

Please insert the U flash disk stored with the GUID file to the NVR before resetting password.

Step 3 Select the GUID file from the U flash disk and click **Import** to import the file to the device.

NOTE

If you have imported the wrong GUIE file for 7 times, you will be not allowed to reset the password for 30 minutes.

Step 4 After the GUID file is successfully imported, enter the reset password interface to set the new admin password.

Step 5 Click **OK** to set the new password. You can export the new GUID file to the U flash disk for future password resetting.

NOTE

When the new password is set, the original GUID file will be invalid. The new GUID file should be exported for future password resetting. You can also enter the User>User Management interface to edit the admin user and export the GUID file.

15.4.2 Reset Password by Security Questions

Before You Start

You have configured the security questions when you activate the device or edit the admin user account. (Refer to Chapter 15.3.2 Configure Security Questions).

Step 1 On the user login interface, click **Forgot Password**.

Step 2 Select the password resetting type to **Verify by Security Question**.

Step 3 Input the correct answers of the three security questions.

Step 4 Click **OK**.

NOTE

If the answers mismatch, the verification is failed.

Step 5 Create the new admin password on the **Reset Password** interface.

15.4.3 Reset Password by Reserved Email

Before You Start

Ensure you have configured the reserved email when you are activating the device or editing the admin user account. (Refer to 15.3.3 Configure Reserved Email)

Step 1 On the user login interface, click **Forgot Password**.

Step 2 Select the password resetting type to **Verify by Reserved Email**.

Step 3 Click **OK**.

Step 4 Obtain the verification code. There are two ways to get the verification code.

- Use Guarding Vision app to scan the QR code.
- Send the QR code to email server.

2) Insert a USB flash drive to your device.
3) Click **Export** to export the QR code to USB flash drive.
4) Email the QR code to *pw_recovery@device-service.com* as attachment.

Step 5 Check your reserved email, and you will receive a verification code within 5 minutes.

Step 6 Enter the verification code.

Step 7 Click **OK** to set the new password.

Chapter 16 System Service Maintenance

16.1 Storage Device Maintenance

16.1.1 Configure Disk Clone

Purpose:

Select the HDDs to clone to eSATA HDD.

Before you start:

Connect an eSATA disk to the device.

Step 1 Go to **Maintenance > HDD Operation > HDD Clone**.

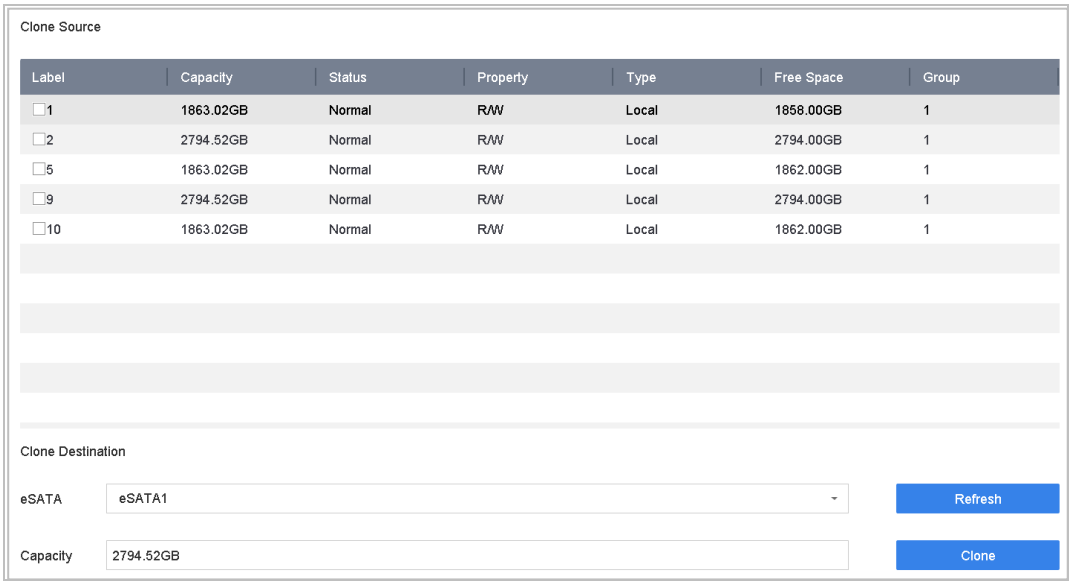


Figure 16-1 HDD Clone

Step 2 Check the HDD to clone. The capacity of selected HDD must match the capacity of clone destination.

Step 3 Click **Clone**.

Step 4 Click **Yes** on popup message box to continue clone.

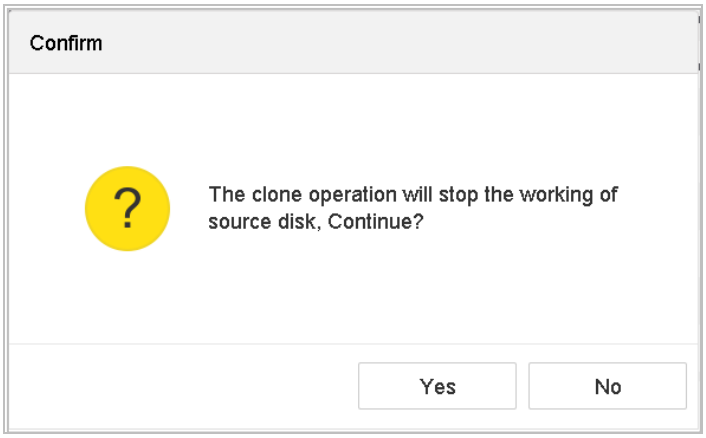


Figure 16-2 Message Box

16.1.2 S.M.A.R.T Detection

Purpose:

The device provides the HDD detection function such as the adopting of the S.M.A.R.T. and the Bad Sector Detection technique. The S.M.A.R.T. *(*Self-Monitoring, Analysis and Reporting Technology*)* is a monitoring system for HDD to detect and report on various indicators of reliability in the hopes of anticipating failures.

Step 1 Go to **Maintenance** > **HDD Operation** > **S.M.A.R.T.**.

Step 2 Select the HDD to view its S.M.A.R.T information list.

Step 3 Select the self-test types as **Short Test**, **Expanded Test** or the **Conveyance Test**.

Step 4 Click **Self-Test** to start the S.M.A.R.T. HDD self-evaluation.

Step 5 The related information of the S.M.A.R.T. is shown on the interface. You can check the HDD status.

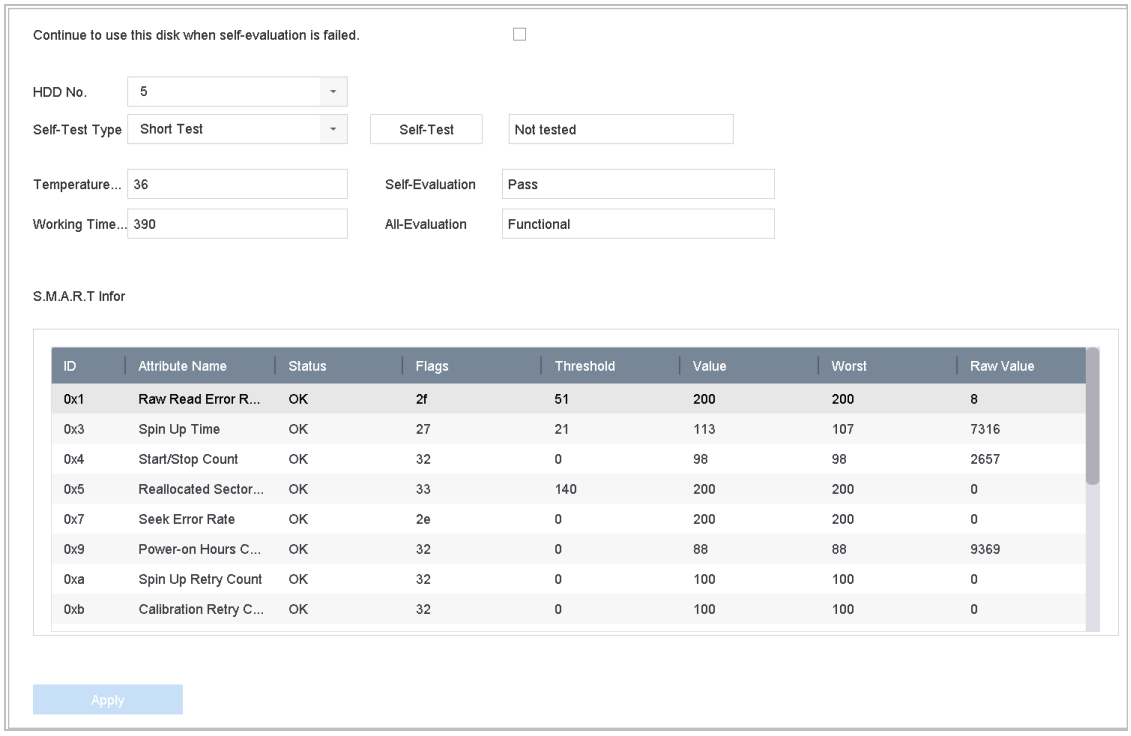


Figure 16-3 S.M.A.R.T Settings Interface

NOTE

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

16.1.3 Bad Sector Detection

Step 1 Go to **Maintenance** > **HDD Operation** > **Bad Sector Detection**.

Step 2 Select the HDD No. in the dropdown list you want to configure.

Step 3 Select **All Detection** or **Key Area Detection** as the detection type.

Step 4 Click the **Self-Test** button to start the detection.

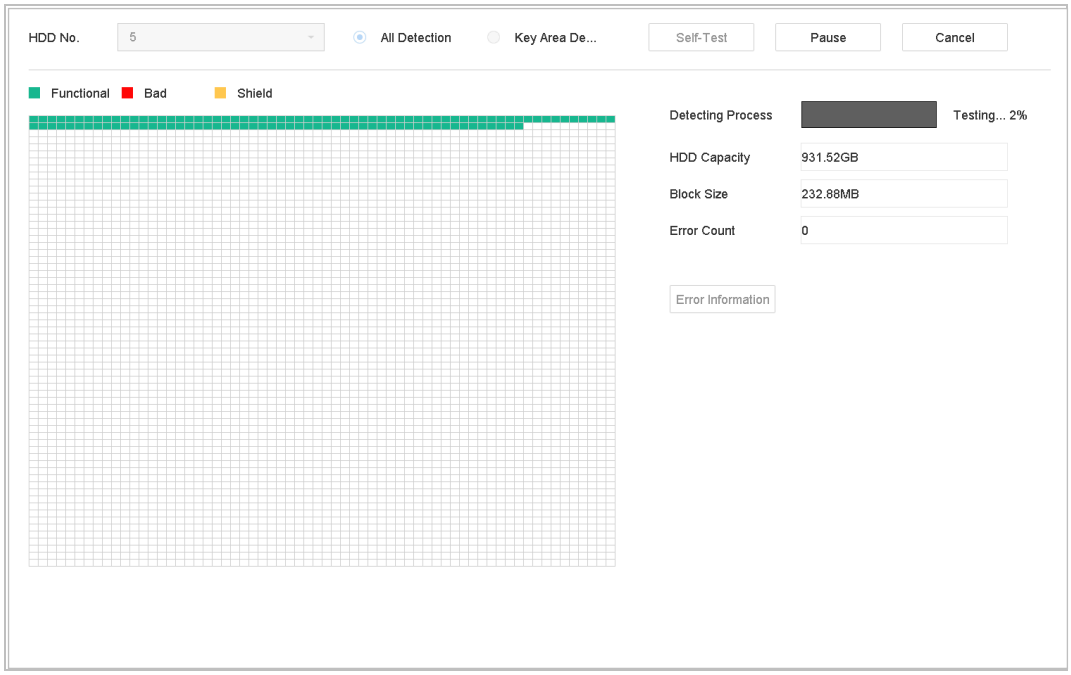


Figure 16-4 Bad Sector Detection

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

16.1.4 HDD Health Detection

Purpose:

You can view the health status of Seagate HDD that generated after October 1th, 2017 and capacity ranges from 4 TB to 8 TB. The function helps you to troubleshoot HDD problems. Compared with S.M.A.R.T function, health detection shows HDD status with more details.

Step 1 Go to **Maintenance > HDD Operation > Health Detection**.

Figure 16-5 Health Detection

Step 2 Click a HDD to view details.

16.1.5 Repair Database

Purpose

Repairing database will rebuild all databases. It might help to improve your system speed after upgrade.

Step 1 Go to **Storage** > **Storage Device**.

Step 2 Select the drive.

Step 3 Click **Repair Database**.

Step 4 Click **Yes**.

NOTE

- Repairing database will rebuild all databases. Existing data will not be affected, but local search and playback functions will not be available during the process, you can still achieve search and playback functions remotely via web browser, client software, etc.
- Do not pull out drive, or shut down the device during the process.
- You can see the repairing progress at **Status**.

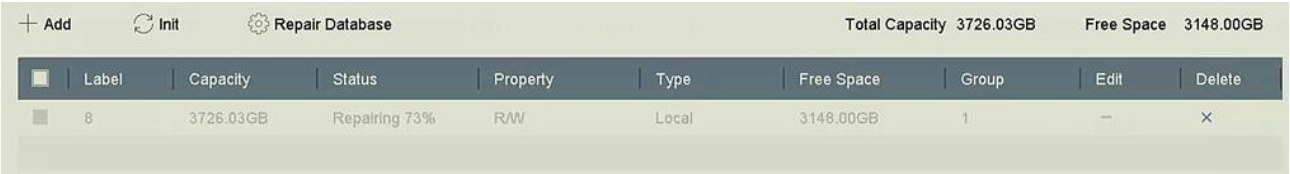


Figure 16-6 Repair Database

16.2 Search & Export Log Files

Purpose:

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

16.2.1 Search the Log Files

Step 1 Go to **Maintenance** > **Log Information**.

Step 2 Set the log search conditions, including the Time, Major Type and Minor Type.

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

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

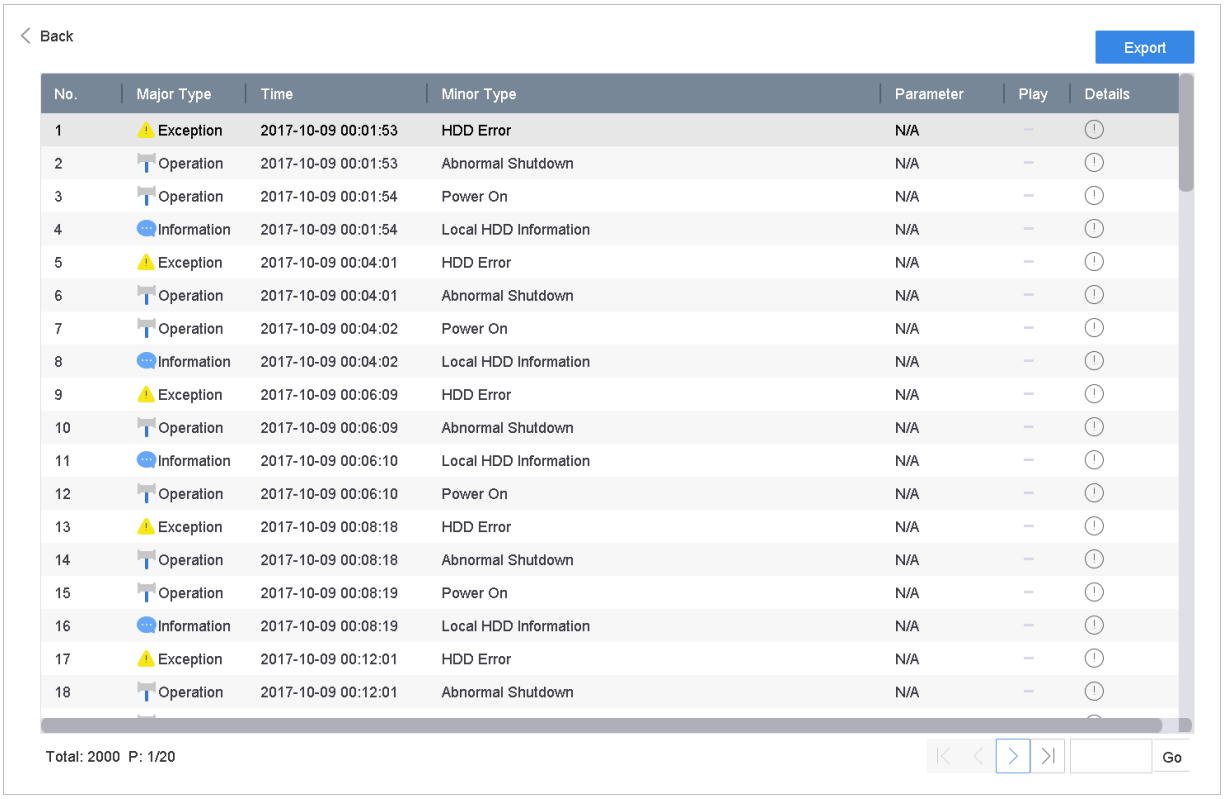


Figure 16-7 Log Search Results

NOTE

Up to 2000 log files can be displayed each time.

Related Operation:

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

16.2.2 Export the Log Files

Before You Start:

Connect a storage device to your device.

Step 1 Search the log files. Refer to Chapter 16.2.1 Search the Log Files.

Step 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.

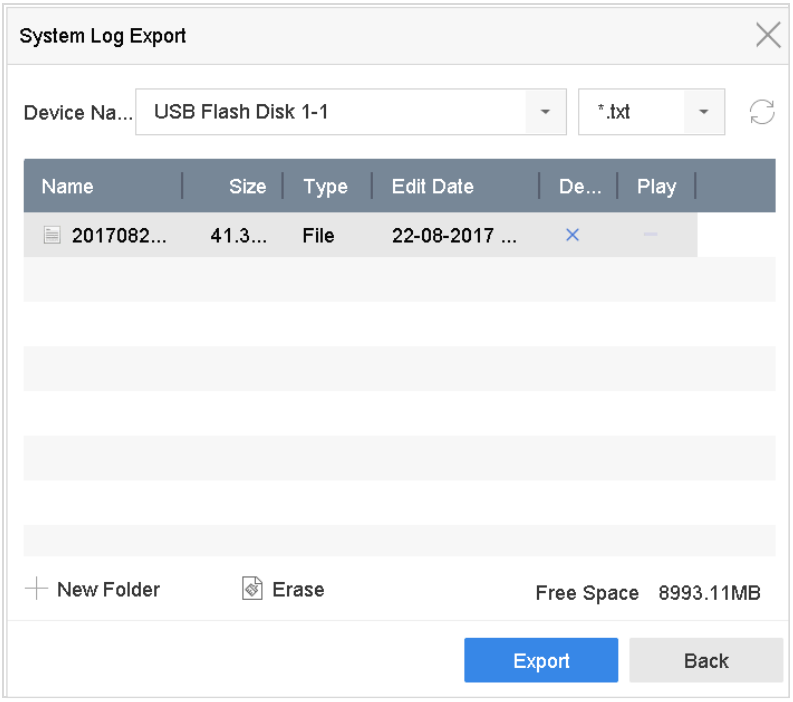


Figure 16-8 Export Log Files

Step 3 On the Export interface, select the storage device from the dropdown list of **Device Name**.

Step 4 Select the format of the log files to be exported. Up to 15 formats are selectable.

Step 5 Click the **Export** to export the log files to the selected storage device.

Related Operation:

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

16.3 Import/Export IP Camera Configuration Files

Purpose:

The information of added IP camera can be generated into an excel file and exported to the local device for backup, including the IP address, manage port, password of admin, etc.. And the exported file can be edited on your PC, like adding or deleting the content, and copy the setting to other devices by importing the excel file to it.

Before You Start:

Connect a storage device to your device. For importing the configuration file, the storage device must be with the file.

Step 1 Go to **Camera** > **IP Camera Import/Export**.

Step 2 Click the **IP Camera Import/Export** tab, and the content of detected plugged external device appears.

Step 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 the **Import** button.

NOTE

After the importing process is completed, you must reboot the device to activate the settings.

16.4 Import/Export Device Configuration Files

Purpose:

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.

Connect a storage device to your device. For importing the configuration file, the storage device must be with the file.

Before You Start:

Connect a storage device to your device. For importing the configuration file, the storage device must be with the file.

Step 1 Go to **Maintenance** >**Import/Export**

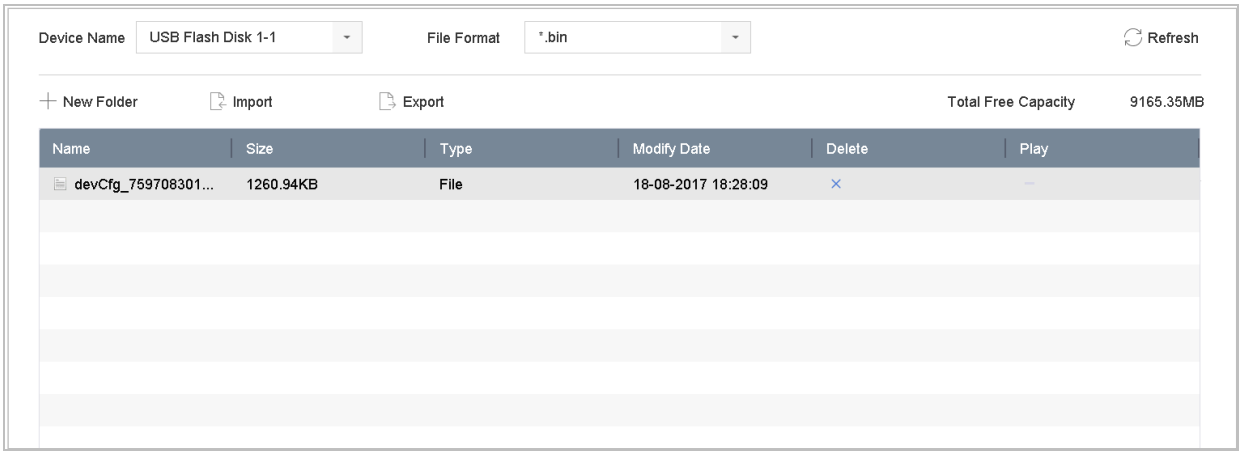


Figure 16-9 Import/Export Config File

Step 2 Export or import the device 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 the **Import** button.

NOTE

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

16.5 Configure System Services

16.5.1 Network Security Settings

Set HTTP Authentication

Purpose

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

Step 1 Go to **System** > **System Service** > **System Service**.

Figure 16-10 HTTP Authentication

Step 2 Check **Enable HTTP** to enable the HTTP service.

Step 3 Select **HTTP Authentication**.

NOTE

Two authentication types are selectable, for security reasons, it is recommended to select **digest** as the authentication type.

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

Step 5 Restart the device to take effect the settings.

NOTE

Two authentication types are selectable, for security reasons, it is recommended to select **digest** as the authentication type.

Disable HTTP

Purpose

The admin user account can disable the HTTP service from the GUI or the web browser.

After the HTTP is disabled, all the related services, including the ISAPI, Onvif and Gennetc, will terminate as well.

Step 1 Go to **System** > **System Service** > **System Service**.

Step 2 Uncheck **Enable HTTP** to disable the HTTP service.

Step 3 Click **Apply** to save the settings.

Step 4 Restart the device to take effect the settings.

RTSP Authentication

Purpose

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

Step 1 Go to **System** > **System Service** > **System Service**.

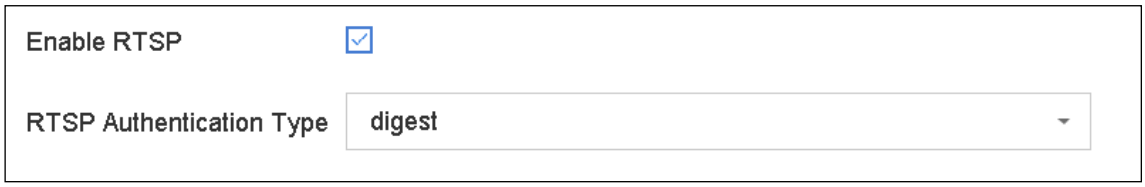


Figure 16-11 RTSP Authentication

Step 2 Select the authentication type.

NOTE

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.

Step 3 Click **Apply** to save the settings.

Step 4 Restart the device to take effect the settings.

Enable ISAPI

Purpose

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.

Step 1 Go to **System** > **System Service** > **System Service**.

Step 2 Check **Enable ISAPI**.

Step 3 Click **Apply** to save the settings.

Step 4 Restart the device to take effect the settings.

Enable IP Camera Occupation Detection

Purpose

The function is able to detect the IP camera status. If the IP camera has been added by other device, it will show as  when you search available IP cameras in **Number of Unadded Online Device.**

Step 1 Go to **System** > **System Service** > **System Service**.

Step 2 Check **Enable IP Camera Occupation Detection**.

Step 3 Click **Apply** to save the settings.

Step 4 Restart the device to take effect the settings.

Enable SDK Service

Purpose

SDK service is used for developing applications of hardware platform, software framework, operating system, etc.

Step 1 Go to **System** > **System Service** > **System Service**.

Step 2 Check **Enable SDK Service**.

Step 3 Click **Apply** to save the settings.

Step 4 Restart the device to take effect the settings.

Enable Enhanced SDK Service

Purpose

The enhanced SDK service adopts TLS protocol over the SDK service that provides safer data transmission.

Step 1 Go to **System** > **System Service** > **System Service**.

Step 2 Check **Enable SDK Service**.

Step 3 Click **Apply** to save the settings.

Step 4 Restart the device to take effect the settings.

IP/MAC Address Filter

Purpose:

The address filter decides whether to allow or forbid specific IP/MAC address to get access to your device.

Step 1 Go to **Maintenance** > **System Service** > **Address Filter**.

Step 2 Check **Enable**.

Step 3 Select **Restriction Mode**. Choose to filter by IP address or MAC Address.

Step 4 Select **Restriction Type**. The device mechanism will allow or forbid specific IP/MAC address to get access to your device.

Step 5 Set **Restriction List**. You can add, edit or delete address.

Step 6 Click **Apply** to save the settings.

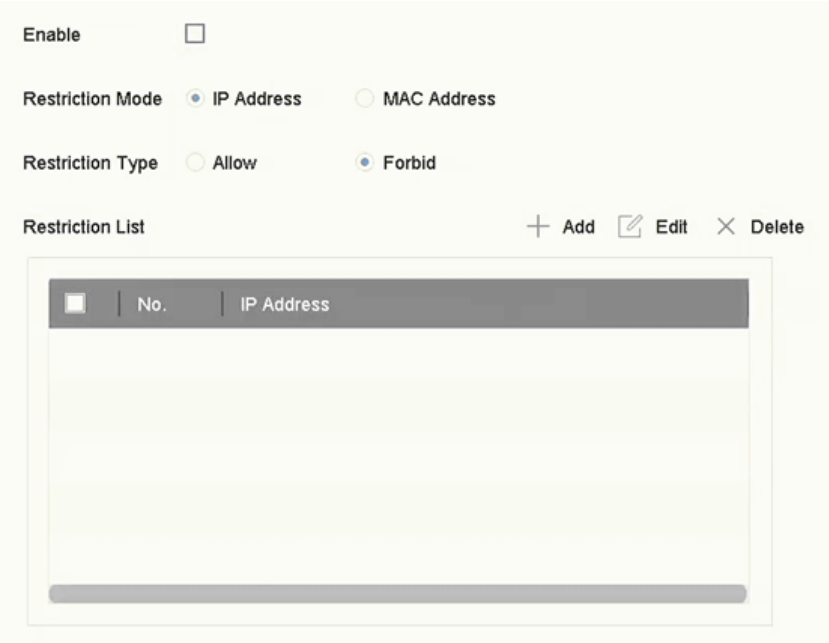


Figure 16-12 Address Filter

16.5.2 Manage ONVIF User Accounts

Purpose

ONVIF protocol allows the connection with third-party cameras. The added user accounts have the permission to connect other devices via ONVIF protocol.

Step 1 Go to **System** > **System Service** > **ONVIF**.

Step 2 Check **Enable ONVIF** to enable the ONVIF access management.

NOTE

ONVIF protocol is disabled by default.

Step 3 Click **Add**.

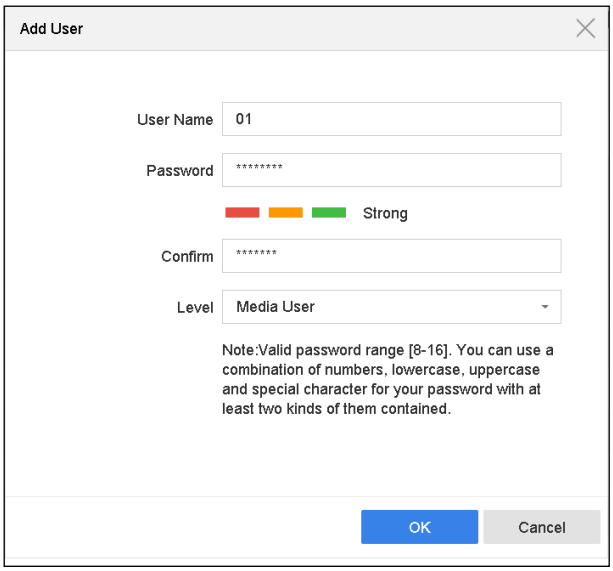


Figure 16-13 Add User

Step 4 Enter the user name, and 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.

Step 5 Select the user level to **Media User**, **Operator**, or **Admin**.

Step 6 Click **OK** to save the settings.

16.6 Upgrade System

Purpose:

The firmware on your device can be upgraded by local backup device or remote FTP server.

16.6.1 Upgrade by Local Backup Device

Before You Start:

Connect your device with a local storage device with update firmware file.

Step 1 Go to **Maintenance**>**Upgrade**.

Step 2 Click the **Local Upgrade** tab to enter the local upgrade interface.

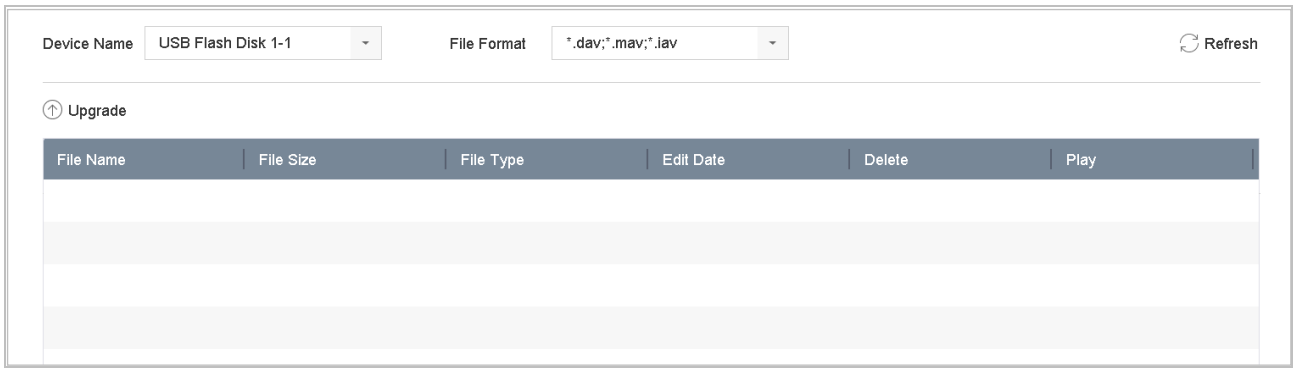


Figure 16-14 Local Upgrade Interface

Step 3 Select the update file from the storage device.

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

Step 5 After the upgrading is complete, the device will reboot automatically to activate the new firmware.

16.6.2 Upgrade by FTP

Before you start:

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

Step 1 Go to **Maintenance**>**Upgrade**.

Step 2 Click the **FTP** tab to enter the local upgrade interface.

Figure 16-15 FTP Upgrade Interface

Step 3 Enter the FTP Server Address in the text field.

Step 4 Click the **Upgrade** button to start upgrading.

Step 5 After the upgrading is complete, reboot the device to activate the new firmware.

16.7 Restore Default Settings

Step 1 Go to **Maintenance** > **Default**.

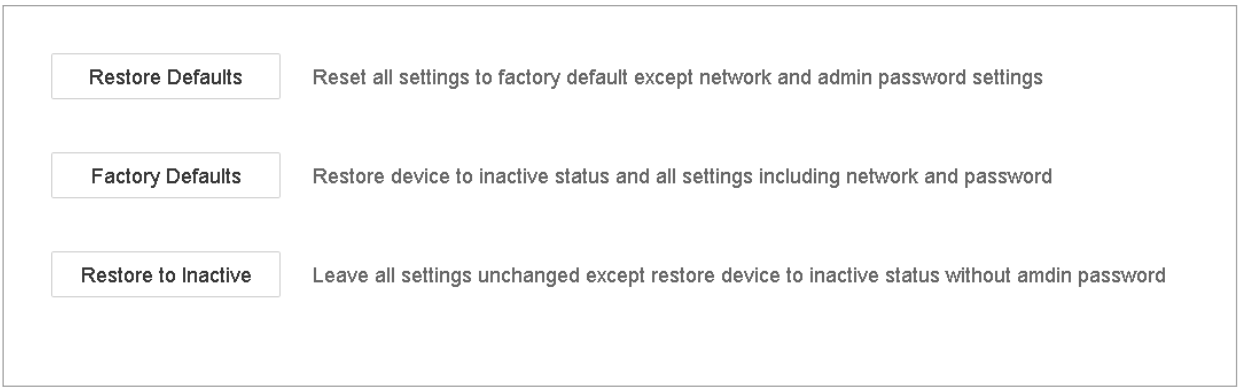


Figure 16-16 Restore Defaults

Step 2 Select the restoring type from the following three options.

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 device to the inactive status.

NOTE

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

Chapter 17 General System Settings

17.1 Configure General Settings

Purpose:

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

Step 1 Go to System > General.

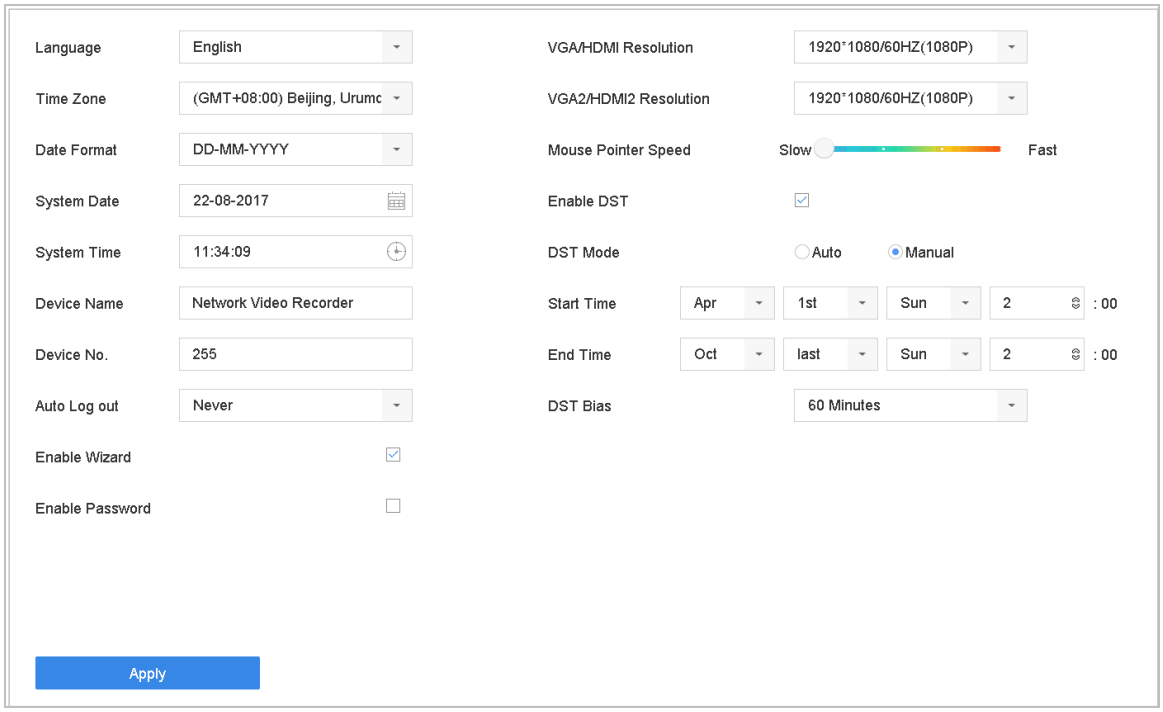


Figure 17-1 General Settings Interface

Step 2 Configure the following settings.

Language: The default language used is *English*.

Output Standard: Select the output standard to NTSC or PAL, which must be the same with the video input standard.

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.

Mouse Pointer Speed: Set the speed of mouse pointer; 4 levels are configurable.

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

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

Step 3 Click the **Apply** button to save the settings.

17.2 Configure Date & Time

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

Step 2 Configure the date and time.

Time Zone: Select the time zone.

Date Format: Select the date format.

System Date: Select the system date.

System Time: Set the system time.

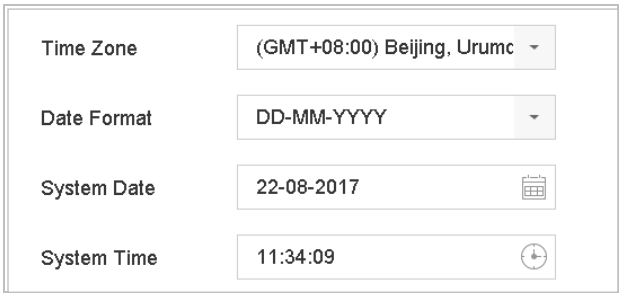


Figure 17-2 Date and Time Settings

Step 3 Click the **Apply** button to save the settings.

17.3 Configure DST Settings

The DST (daylight saving time) refers to the period of the year when clocks are moved one period ahead. In some areas worldwide, this has the effect of creating more sunlit hours in the evening during months when the weather is the warmest.

We advance our clocks ahead a certain period (depends on the DST bias you set) at the beginning of DST, and move them back the same period when we return to standard time (ST).

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

Step 2 Check the **Enable DST**.

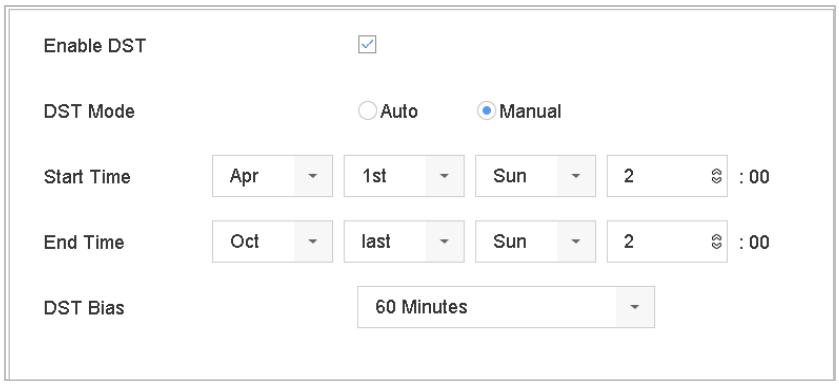


Figure 17-3 DST Settings Interface

Step 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.

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

17.4 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.

17.4.1 Add a User

Step 1 Go to **System** > **User**.

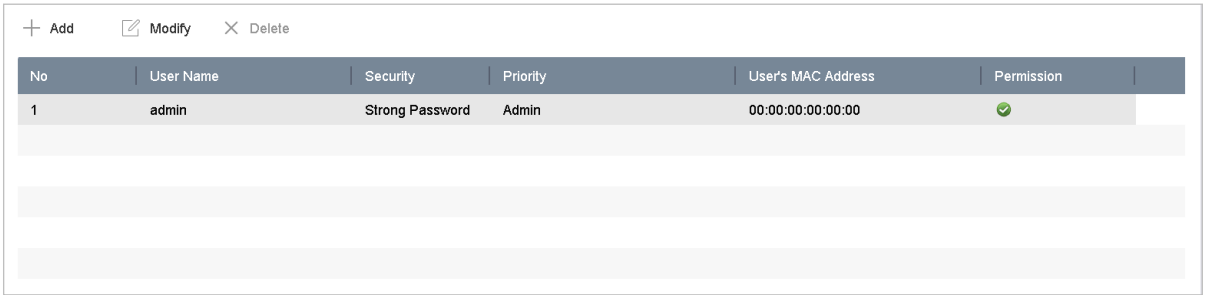


Figure 17-4 User Management Interface

Step 2 Click **Add** to enter the operation permission interface.

Step 3 Enter the admin password and click **OK**.

Step 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**.

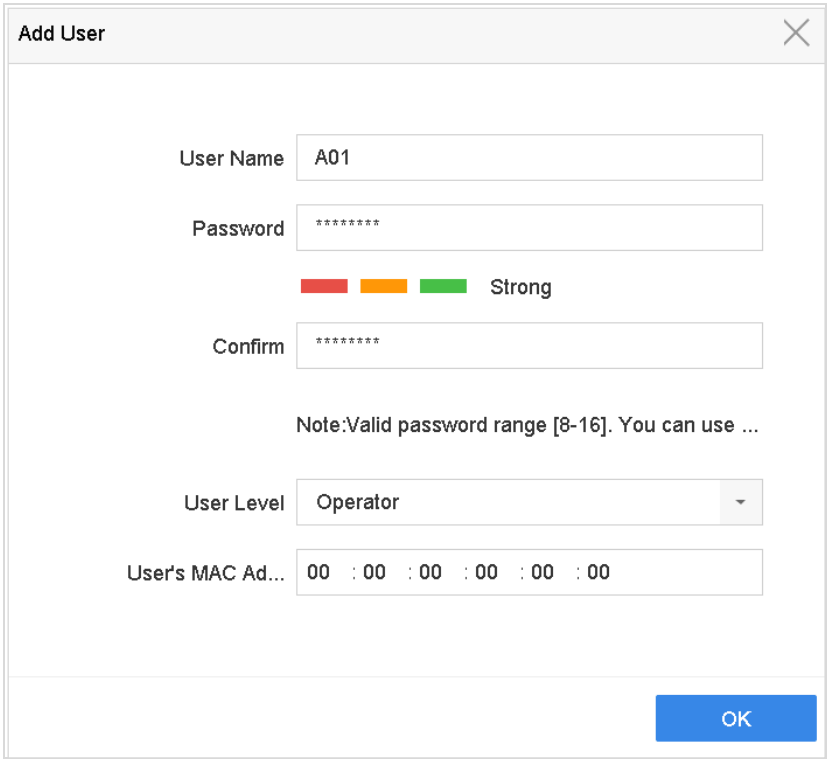


Figure 17-5 Add User

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.

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

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

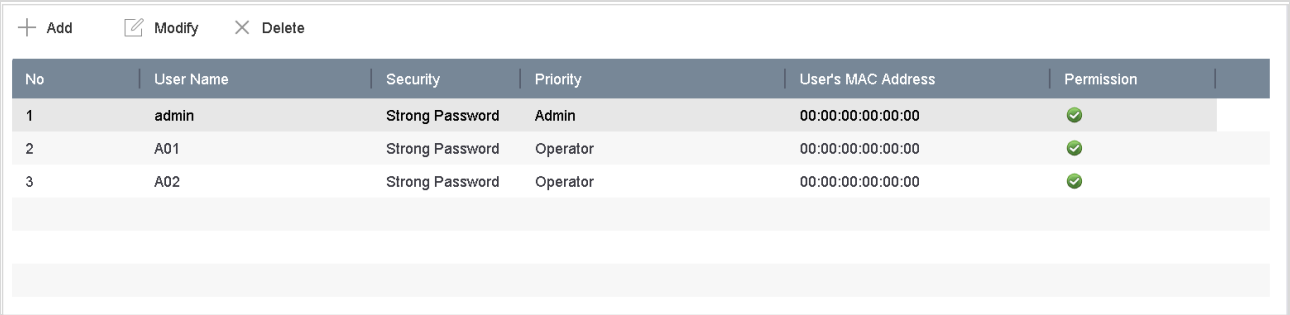


Figure 17-6 User List

17.4.2 Set the Permission for a User

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

Step 1 Go to **System** > **User**.

Step 2 Select a user from the list and then click the button to enter the permission settings interface.

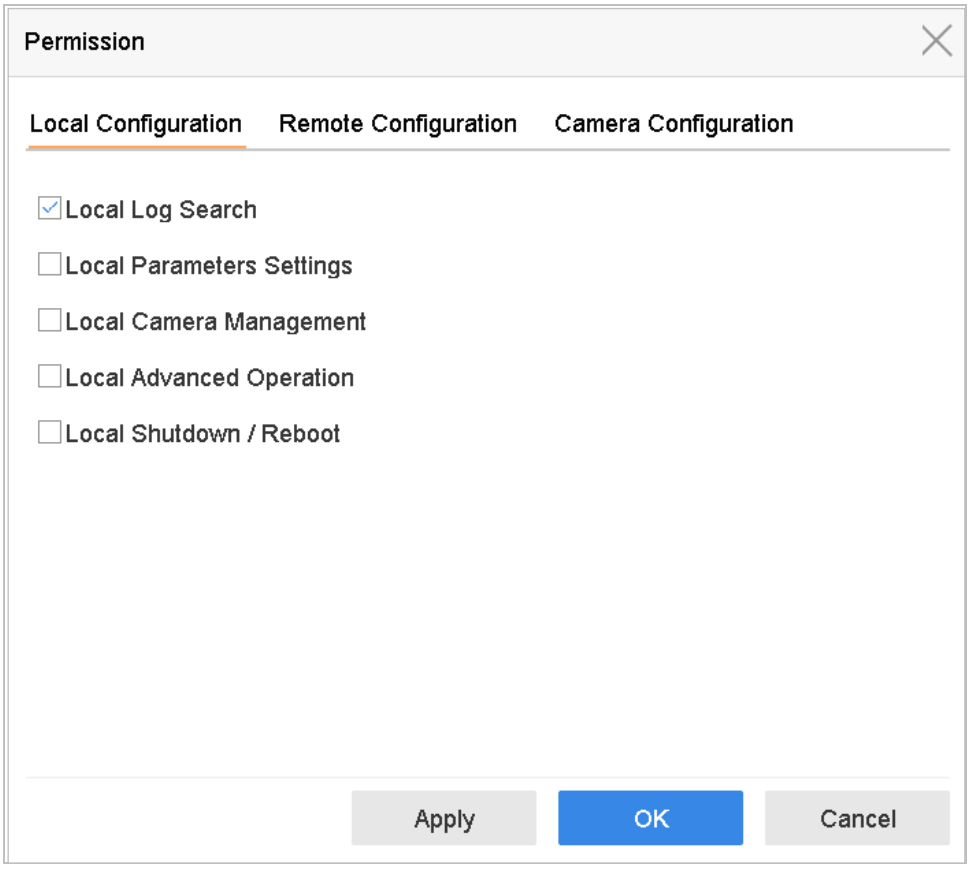


Figure 17-7 User Permission Settings Interface

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

- **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.

- **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.

- Camera Configuration

  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).

  Local Live View: View live video of the selected camera(s) in local.

Step 4 Click **OK** to save the settings.

NOTE

Only the admin user account has the permission of restoring factory default parameters.

17.4.3 Set Local Live View Permission for Non-Admin Users

Step 1 Go to **System** > **User**.

Step 2 Click of admin user.

Step 3 Enter admin password and click **OK**.

Step 4 Select cameras that non-admin user can view in local and click **OK.**

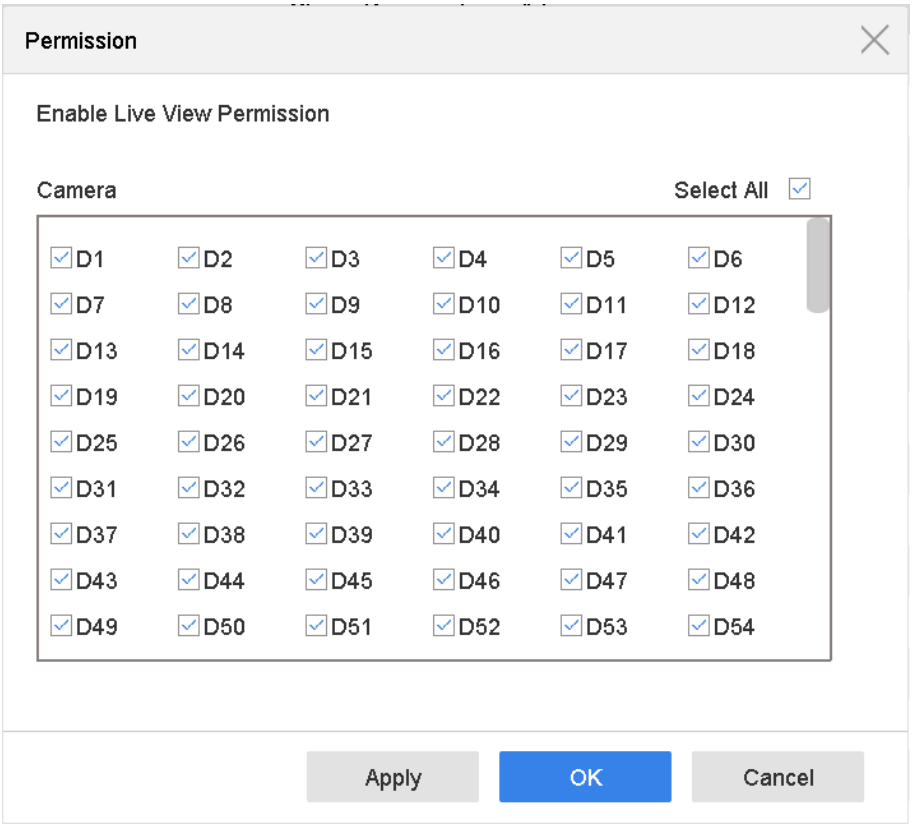


Figure 17-8 Enable Live View Permission

Step 5 Click  of non-admin user.

Step 6 Enter **Camera Configuration** tab.

Step 7 Select Camera Permission as **Local Live View**.

Step 8 Select cameras to live view.

Step 9 Click **OK**.

17.4.4 Edit the Admin User

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

Step 1 Go to **System** > **User**.

Step 2 Select the admin user from the list and click **Modify**.

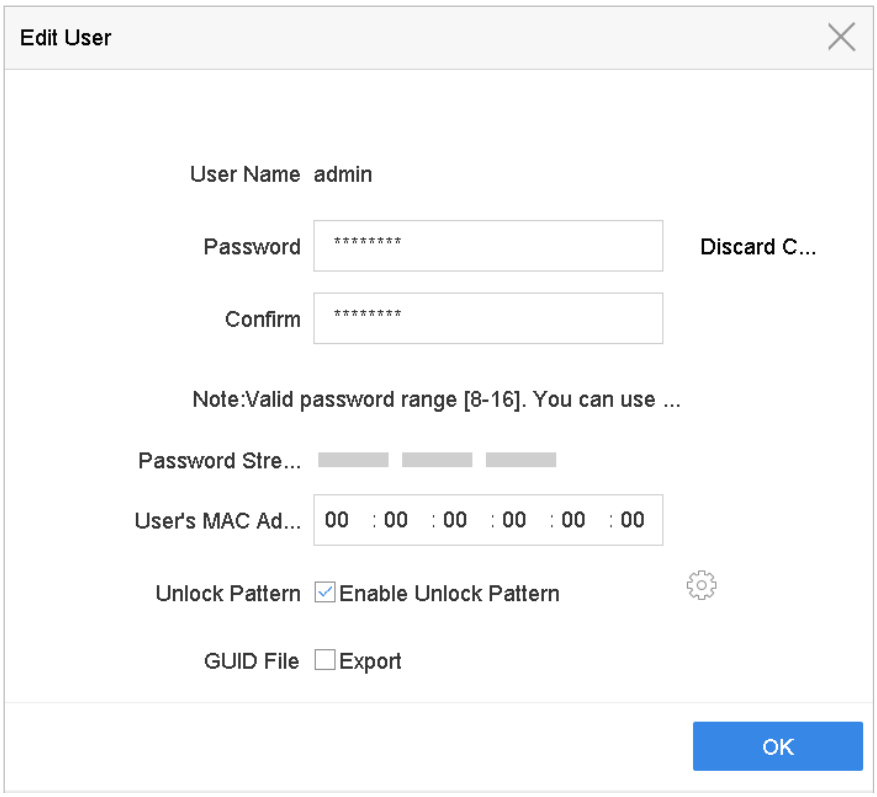


Figure 17-9 Edit User (Admin)

Step 3 Edit the admin user information as demand, including the new admin password (strong password is required), and MAC address.

Step 4 Edit the unlock pattern for the admin user account.

5) Check the checkbox of **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.

NOTE

Step 5 Please refer to Chapter 2.2 Step 2In the **IP Camera Activation** text field, enter the password to activate the IP camera (s) connected to the device.

Step 6 Optionally, check the **Export GUID** to export the GUID for future password resetting.

Step 7 Click **OK** to save the password and activate the device.

NOTE

- After the device is activated, you should properly keep the password.
- When you have enabled the **Export GUID**, continue to export the GUID file to the USB flash driver for the future password resetting.
- You can duplicate the password to the IP cameras that are connected with default protocol.

Configure Unlock Pattern for Login for detailed instructions.

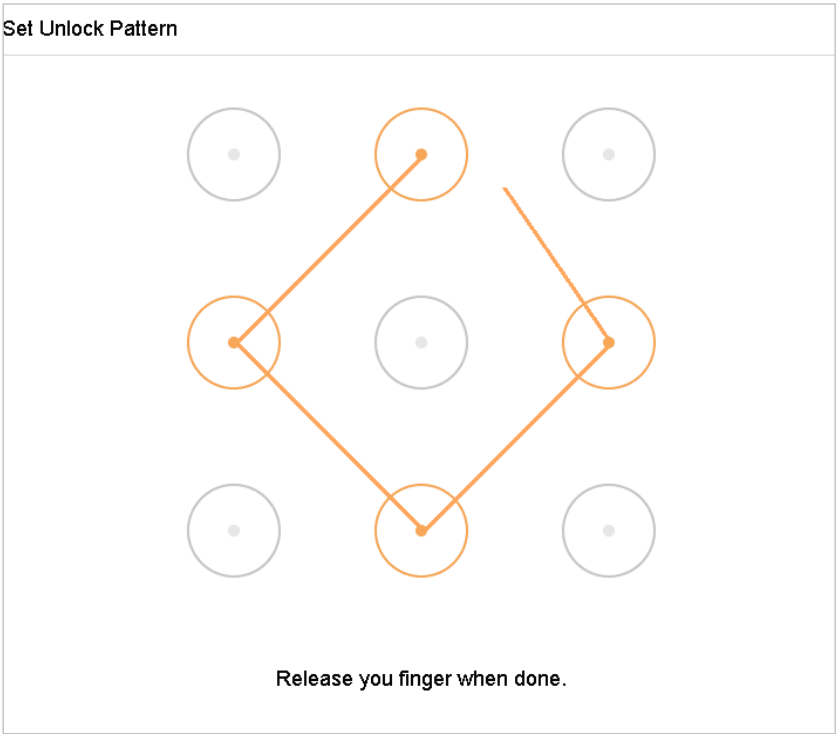


Figure 17-10 Set Unlock Patter for Admin User

Step 8 Click the of **Export GUID** to enter the reset password interface to export the GUID file for the admin user account.

When the admin password is changed, you can export the new GUID to the connected U flash disk in the Import/Export interface for the future password resetting.

Step 9 Click the **OK** button to save the settings.

Step 10 For the **Operator** or **Guest** user account, you can also click the button on the user management interface to edit the permission.

17.4.5 Edit the Operator/Guest User

You can edit the user information, including user name, password, permission level and MAC address. Check the checkbox of **Change Password** if you want to change the password, and input the new password in the text field of **Password** and **Confirm**. A strong password is recommended.

Step 1 Go to **System** > **User**.

Step 2 Select a user from the list and click **Modify**.

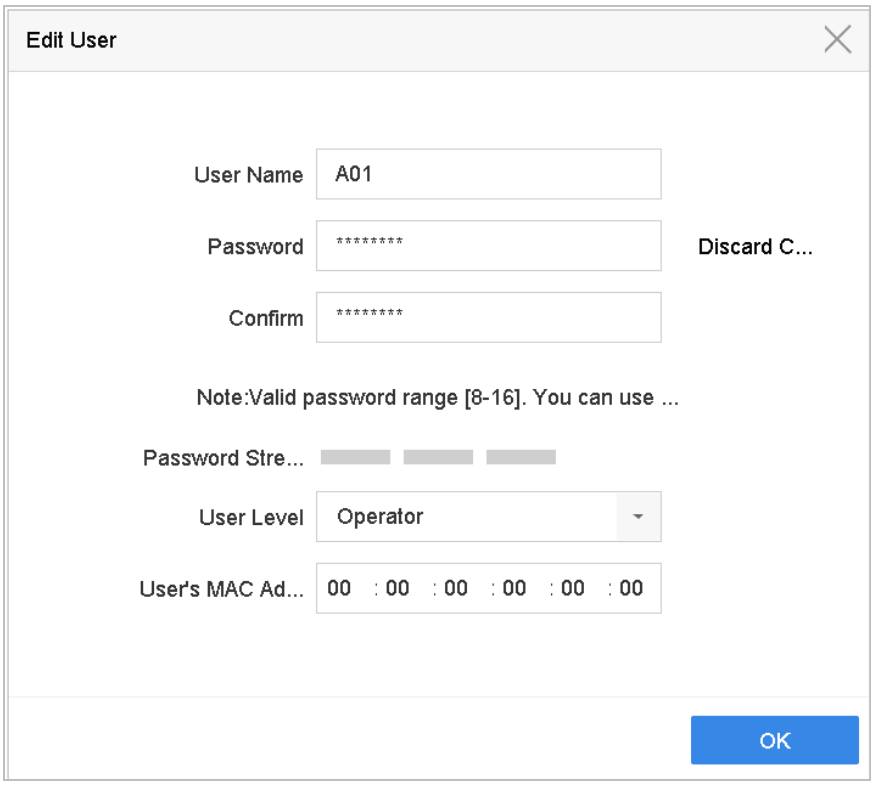


Figure 17-11 Edit User (Operator/Guest)

Step 3 Edit the user information as demand, including the new password (strong password is required), and MAC address.

17.4.6 Delete a User

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

Step 1 Go to **System** > **User**.

Step 2 Select a user from the list.

Step 3 Click **Delete** to delete the selected user account.

Chapter 18 Appendix

18.1 Glossary

- **HDD:** Acronym for Hard Disk Drive. A storage medium which stores digitally encoded data on platters with magnetic surfaces.
- **DHCP:** Dynamic Host Configuration Protocol (DHCP) is a network application protocol used by devices (DHCP clients) to obtain configuration information for operation in an Internet Protocol network.
- **HTTP:** Acronym for Hypertext Transfer Protocol. A protocol to transfer hypertext request and information between servers and browsers over a network
- **DDNS:** Dynamic DNS is a method, protocol, or network service that provides the capability for a networked device, such as a router or computer system using the Internet Protocol Suite, to notify a domain name server to change, in real time (ad-hoc) the active DNS configuration of its configured hostnames, addresses or other information stored in DNS.
- **PPPoE:** Stands for "Point-to-Point Protocol over Ethernet." PPPoE is a network configuration used for establishing a PPP connection over an Ethernet protocol.
- **Hybrid device:** A hybrid device is a combination of a DVR and device.
- **NTP:** Acronym for Network Time Protocol. A protocol designed to synchronize the clocks of computers over a network.
- **NTSC:** Acronym for National Television System Committee. NTSC is an analog television standard used in such countries as the United States and Japan. Each frame of an NTSC signal contains 525 scan lines at 60Hz.
- **Device:** Acronym for Network Video Recorder. A device can be a PC-based or embedded system used for centralized management and storage for IP cameras, IP Domes and other devices.
- **PAL:** Acronym for Phase Alternating Line. PAL is also another video standard used in broadcast televisions systems in large parts of the world. PAL signal contains 625 scan lines at 50Hz.
- **PTZ:** Acronym for Pan, Tilt, Zoom. PTZ cameras are motor driven systems that allow the camera to pan left and right, tilt up and down and zoom in and out.
- **USB:** Acronym for Universal Serial Bus. USB is a plug-and-play serial bus standard to interface devices to a host computer.

18.2 Troubleshooting

- **No image displayed on the monitor after starting up normally.**

Possible Reasons:

- No VGA or HDMI connections.
- Connection cable is damaged.
- Input mode of the monitor is incorrect.

Step 1 Verify the device is connected with the monitor via HDMI or VGA cable.

Step 2 If not, please connect the device with the monitor and reboot.

Step 3 Verify the connection cable is good.

Step 4 If there is still no image display on the monitor after rebooting, please check if the connection cable is good, and change a cable to connect again.

Step 5 Verify Input mode of the monitor is correct.

Step 6 Please check the input mode of the monitor matches with the output mode of the device (e.g. if the output mode of device is HDMI output, then the input mode of monitor must be the HDMI input). And if not, please modify the input mode of monitor.

Step 7 Check if the fault is solved by the step 1 to step 3.

Step 8 If it is solved, finish the process.

If not, please contact the engineer from our company to do the further process.

- **There is an audible warning sound "Di-Di-Di-DiDi" after a new bought device starts up.**

Possible Reasons:

- No HDD is installed in the device.
- The installed HDD has not been initialized.
- The installed HDD is not compatible with the device or is broken-down.

Step 9 Verify at least one HDD is installed in the device.

- If not, please install the compatible HDD.

NOTE

Please refer to the *Quick Start Guide* for the HDD installation steps.

- If you don't want to install a HDD, go to Menu>System> Event>Normal Event>Exception, and uncheck the Audible Warning checkbox of "HDD Error".

Step 10 Verify the HDD is initialized.

6) Go to Menu>Storage>Storage Device.

If the status of the HDD is “Uninitialized”, please check the checkbox of corresponding HDD and click the “Init” button.

Step 11 Verify the HDD is detected or is in good condition.

7) Select Menu>Storage>Storage Device.

8) If the HDD is not detected or the status is “Abnormal”, please replace the dedicated HDD according to the requirement.

Step 12 Check if the fault is solved by the step 1 to step 3.

If it is solved, finish the process.

If not, please contact the engineer from our company to do the further process.

- **The status of the added IP camera displays as “Disconnected” when it is connected through Private Protocol. Select “Menu>Camera>Camera>IP Camera” to get the camera status.**

Possible Reasons:

- Network failure, and the device and IP camera lost connections.
- The configured parameters are incorrect when adding the IP camera.
- Insufficient bandwidth.

Step 13 Verify the network is connected.

9) Connect the device and PC with the RS-232 cable.

Open the Super Terminal software, and execute the ping command. Input “ping IP” (e.g. ping 172.6.22.131).

NOTE

Simultaneously press **Ctrl** and **C** to exit the ping command.

If there exists return information and the time value is little, the network is normal.

Step 14 Verify the configuration parameters are correct.

10) Go to Menu>Camera.

Verify the following parameters are the same with those of the connected IP devices, including IP address, protocol, management port, user name and password.

Step 15 Verify the whether the bandwidth is enough.

11) Go to Menu>Maintenance>Net Detect>Network Stat..

Check the usage of the access bandwidth, and see if the total bandwidth has reached its limit.

Step 16 Check if the fault is solved by the step 1 to step 3.

If it is solved, finish the process.

If not, please contact the engineer from our company to do the further process.

- **The IP camera frequently goes online and offline and the status of it displays as "Disconnected".**

  Possible Reasons:

  − The IP camera and the device versions are not compatible.

  − Unstable power supply of IP camera.

  − Unstable network between IP camera and device.

  − Limited flow by the switch connected with IP camera and device.

Step 17 Verify the IP camera and the device versions are compatible.

12) Go to Menu>Camera, and view the firmware version of connected IP camera.

Go to Menu>Maintenance>System Info>Device Info and view the firmware version of device.

Step 18 Verify power supply of IP camera is stable.

13) Verify the power indicator is normal.

When the IP camera is offline, please try the ping command on PC to check if the PC connects with the IP camera.

Step 19 Verify the network between IP camera and device is stable.

When the IP camera is offline, connect PC and device with the RS-232 cable.

Open the Super Terminal, use the ping command and keep sending large data packages to the connected IP camera, and check if there exists packet loss.

NOTE

Simultaneously press **Ctrl** and **C** to exit the ping command.

Example: Input ping 172.6.22.131 –l 1472 –f.

Step 20 Verify the switch is not flow control.

Check the brand, model of the switch connecting IP camera and device, and contact with the manufacturer of the switch to check if it has the function of flow control. If so, please turn it down.

Step 21 Check if the fault is solved by the step 1 to step 4.

If it is solved, finish the process.

If not, please contact the engineer from our company to do the further process.

- **No monitor connected with the device locally and when you manage the IP camera to connect with the device by web browser remotely, of which the status displays as Connected. And then you connect the device with the monitor via VGA or HDMI interface and reboot the device, there is black screen with the mouse cursor.**

Connect the device with the monitor before startup via VGA or HDMI interface, and manage the IP camera to connect with the device locally or remotely, the status of IP camera displays as Connect. And then connect the device with the CVBS, and there is black screen either.

Possible Reasons:

After connecting the IP camera to the device, the image is output via the main spot interface by default.

Step 22 Enable the output channel.

Step 23 Go to Menu>System>Live View>General, and select video output interface in the drop-down list and configure the window you want to view.

NOTE

- The view settings can only be configured by the local operation of device.
- Different camera orders and window-division modes can be set for different output interfaces separately, and digits like “D1”and “D2” stands for the channel number, and “X” means the selected window has no image output.

Step 24 Check if the fault is solved by the above steps.

If it is solved, finish the process.

If not, please contact the engineer from our company to do the further process.

- **Live view stuck when video output locally.**

Possible Reasons:

− Poor network between device and IP camera, and there exists packet loss during the transmission.

− The frame rate has not reached the real-time frame rate.

Step 25 Verify the network between device and IP camera is connected.

- When image is stuck, connect the RS-232 ports on PC and the rear panel of device with the RS-232 cable.
- Open the Super Terminal, and execute the command of “**ping** *192.168.0.0* **–l 1472 –f**” (the IP address may change according to the real condition), and check if there exists packet loss.

NOTE

Simultaneously press **Ctrl** and **C** to exit the ping command.

Step 26 Verify the frame rate is real-time frame rate.

Go to Menu>Camera>Encoding Parameters, and set the Frame rate to Full Frame.

Step 27 Check if the fault is solved by the above steps.

If it is solved, finish the process.

If not, please contact the engineer from our company to do the further process.

- **Live view stuck when video output remotely via the Internet Explorer or platform software.**

Possible Reasons:

- Poor network between device and IP camera, and there exists packet loss during the transmission.
- Poor network between device and PC, and there exists packet loss during the transmission.
- The performances of hardware are not good enough, including CPU, memory, etc..

Step 28 Verify the network between device and IP camera is connected.

14) When image is stuck, connect the RS-232 ports on PC and the rear panel of device with the RS-232 cable.

Open the Super Terminal, and execute the command of "**ping** *192.168.0.0* **–l 1472 –f**" (the IP address may change according to the real condition), and check if there exists packet loss.

NOTE

Simultaneously press **Ctrl** and **C** to exit the ping command.

Step 29 Verify the network between device and PC is connected.

1) Open the cmd window in the Start menu, or you can press "windows+R" shortcut key to open it.
2) Use the ping command to send large packet to the device, execute the command of "ping 192.168.0.0 –l 1472 –f" (the IP address may change according to the real condition), and check if there exists packet loss.

NOTE

Simultaneously press **Ctrl** and **C** to exit the ping command.

Step 30 Verify the hardware of the PC is good enough.

Simultaneously press **Ctrl**, **Alt** and **Delete** to enter the windows task management interface, as shown in the following figure.

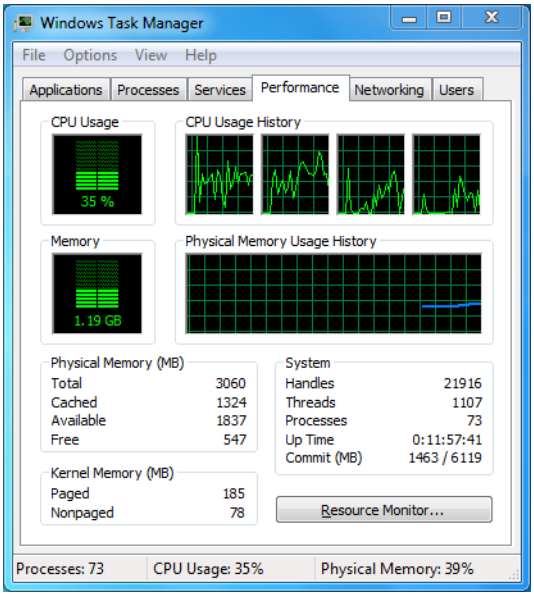


Figure 18-1 Windows task management interface

- Select the “Performance” tab; check the status of the CPU and Memory.
- If the resource is not enough, please end some unnecessary processes.

Step 31 Check if the fault is solved by the above steps.

If it is solved, finish the process.

If not, please contact the engineer from our company to do the further process.

- **When using the device to get the live view audio, there is no sound or there is too much noise, or the volume is too low.**

Possible Reasons:

- Cable between the pickup and IP camera is not connected well; impedance mismatches or incompatible.
- The stream type is not set as “Video & Audio”.
- The encoding standard is not supported with device.

Step 32 Verify the cable between the pickup and IP camera is connected well; impedance matches and compatible.

Log in the IP camera directly, and turn the audio on, check if the sound is normal. If not, please contact the manufacturer of the IP camera.

Step 33 Verify the setting parameters are correct.

Go to Menu>Camera>Encoding Parameters, and set the Stream Type as “Audio & Video”.

Step 34 Verify the audio encoding standard of the IP camera is supported by the device.

The device supports G722.1 and G711 standards, and if the encoding parameter of the input audio is not one of the previous two standards, you can log in the IP camera to configure it to the supported standard.

Step 35 Check if the fault is solved by the above steps.

If it is solved, finish the process.

If not, please contact the engineer from our company to do the further process.

- **The image gets stuck when device is playing back by single or multi-channel.**

Possible Reasons:

- Poor network between device and IP camera, and there exists packet loss during the transmission.
- The frame rate is not the real-time frame rate.
- The device supports up to 16-channel synchronize playback at the resolution of 4CIF, if you want a 16-channel synchronize playback at the resolution of 720p, the frame extracting may occur, which leads to a slight stuck.

Step 36 Verify the network between device and IP camera is connected.

1) When image is stuck, connect the RS-232 ports on PC and the rear panel of device with the RS-232 cable.
2) Open the Super Terminal, and execute the command of "**ping** *192.168.0.0* **–l 1472 –f**" (the IP address may change according to the real condition), and check if there exists packet loss.

NOTE

Simultaneously press the **Ctrl** and **C** to exit the ping command.

Step 37 Verify the frame rate is real-time frame rate.

Select "Menu > Record > Parameters > Record", and set the Frame Rate to "Full Frame".

Step 38 Verify the hardware can afford the playback.

Reduce the channel number of playback.

Go to Menu>Camera>Encoding Parameters, and set the resolution and bitrate to a lower level.

Step 39 Reduce the number of local playback channel.

Go to Menu>Playback, and uncheck the checkbox of unnecessary channels.

Step 40 Check if the fault is solved by the above steps.

If it is solved, finish the process.

If not, please contact the engineer from our company to do the further process.

- **No record file found in the device local HDD, and prompt "No record file found".**

Possible Reasons:

- The time setting of system is incorrect.
- The search condition is incorrect.
- The HDD is error or not detected.

Step 41 Verify the system time setting is correct.

Go to Menu>System>General, and verify the "Device Time" is correct.

Step 42 Verify the search condition is correct.

Go to playback interface, and verify the channel and time are correct.

Step 43 Verify the HDD status is normal.

Go to Menu>Storage>Storage Device to view the HDD status, and verify the HDD is detected and can be read and written normally.

Step 44 Check if the fault is solved by the above steps.

If it is solved, finish the process.

If not, please contact the engineer from our company to do the further process.

040210051090416

wisstar+

www.wisstar.net

info@wisstar.net