

Quick Start Guide & Manual



16 Channel 1080P DVR PENDVR-ELE16M-AI



MOBILE APPS

FREE MOBILE APPS
FOR ANDRIOD AND IOS



FREE TECH SUPPORT

FAST SERVICE SUPPORT

Quick Start Guide

Foreword

Welcome

Thank you for purchasing our Digital Video Recorder (DVR).

This Quick Start Guide (hereinafter referred to be "the Guide") will help you become familiar with our DVR in a short time. Please read the Guide carefully before starting using your DVR and properly keep it for future reference.

Important Safeguards and Warnings

Operation Requirement

- Do not place or install the Device in a place exposed to sunlight or near the heat source.
- Keep the Device away from dampness, dust or soot.
- Keep the Device installed horizontally on the stable place to prevent it from falling.
- Do not drop or splash liquid onto the Device, and make sure there is no object filled with liquid on the Device to prevent liquid from flowing into the Device.
- Install the Device in a well-ventilated place, and do not block the ventilation of the Device.
- Operate the device within the rated range of power input and output.
- Do not disassemble the Device.
- Transport, use and store the Device under the allowed humidity and temperature conditions.

Electrical Safety

- Improper battery use might result in fire, explosion, or inflammation.
- When replacing battery, make sure the same model is used.
- Use the recommended power cables in the region and conform to the rated power specification.
- Use the power adapter provided with the Device; otherwise, it might result in people injury and device damage.
- The power source shall conform to the requirement of the Safety Extra Low Voltage (SELV) standard, and supply power with rated voltage which conforms to Limited power Source requirement according to IEC60950-1. Please note that the power supply requirement is subject to the device label.
- Connect the device (I-type structure) to the power socket with protective earthing.
- The appliance coupler is a disconnection device. When using the coupler, keep the angle for easy operation.

Safety Instructions

The following categorized signal words with defined meaning might appear in the Guide.

Signal Words	Meaning
--------------	---------

Signal Words	Meaning
 CAUTION	Indicates a potential risk which, if not avoided, could result in property damage, data loss, lower performance, or unpredictable result.
 NOTE	Provides additional information as the emphasis and supplement to the text.

Privacy Protection Notice

As the device user or data controller, you might collect personal data of others such as face, fingerprints, car plate number, Email address, phone number, GPS and so on. You need to be in compliance with the local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures include but not limited to: providing clear and visible identification to inform data subject the existence of surveillance area and providing related contact.

About the Guide

- The Guide is for reference only. If there is inconsistency between the Guide and the actual product, the actual product shall prevail.
- We are not liable for any loss caused by the operations that do not comply with the Guide.
- The Guide would be updated according to the latest laws and regulations of related regions. For detailed information, see the paper manual, CD-ROM, QR code or our official website. If there is inconsistency between paper User's Manual and the electronic version, the electronic version shall prevail.
- All the designs and software are subject to change without prior written notice. The product updates might cause some differences between the actual product and the Guide. Please contact the customer service for the latest program and supplementary documentation.
- There still might be deviation in technical data, functions and operations description, or errors in print. If there is any doubt or dispute, please refer to our final explanation.
- Upgrade the reader software or try other mainstream reader software if the Guide (in PDF format) cannot be opened.
- All trademarks, registered trademarks and the company names in the Guide are the properties of their respective owners.
- Please visit our website, contact the supplier or customer service if there is any problem occurred when using the device.
- If there is any uncertainty or controversy, please refer to our final explanation.

Table of Contents

Foreword	I
1 Quick Start	1
1.1 Unpacking the Accessories.....	1
1.2 Checking the Components.....	1
1.3 Installing Hard Disk Drive (HDD)	2
1.4 Booting up.....	4
2 The Grand Tour for Rear Panel.....	6
3 Local Configurations	8
3.1 Initializing DVR.....	8
3.2 Resetting Password	9
3.3 Adding Remote Device	12
3.4 Configuring Recording Storage Schedule	13
3.5 Playing Back Recorded Video	14
3.6 Configuring P2P Settings.....	15
3.6.1 Entering P2P Interface.....	15
3.6.2 Adding DVR into Cell Phone Client	16
3.7 Logout	18
4 Web Login	19

 NOTE

The actual appearance or quantity might be different depending on the model you purchased.

1.1 Unpacking the Accessories



1.2 Checking the Components

When you receive the DVR, please check against the following checking list. If any of the items are missing or damaged, contact the local retailer or after-sales engineer immediately.

Sequence	Checking items		Requirement
1	Package	Appearance	No obvious damage.
		Packing materials	No broken or distorted positions that could be caused by hit.
2	Labels	Labels on the device	Not torn up.  NOTE Do not tear up or throw away the labels; otherwise the warranty services are not ensured. You need to provide the serial number of the product when calling the after-sales service.
3	Device	Appearance	No obvious damage.
		Data cables, power cables, fan cables, and mainboard	No loose connection.

1.3 Installing Hard Disk Drive (HDD)

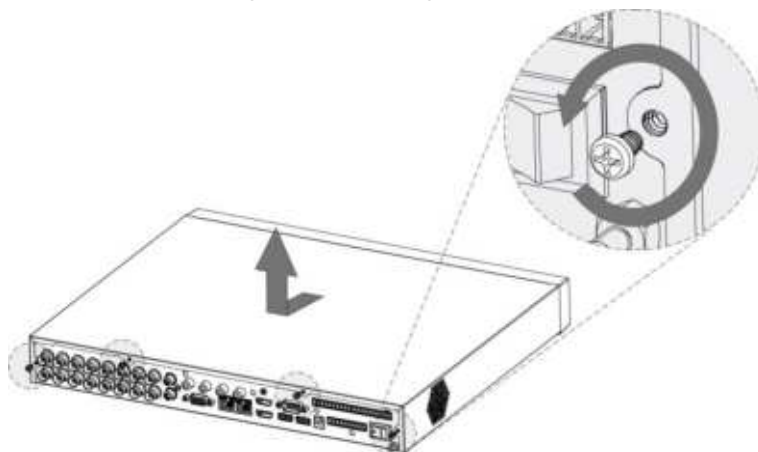
Please check whether the HDD is already installed for the first use. Please use enterprise HDD or surveillance HDD instead of PC HDD.

NOTE

Shut down the DVR and unplug the power cable before opening the cover to replace the HDD.

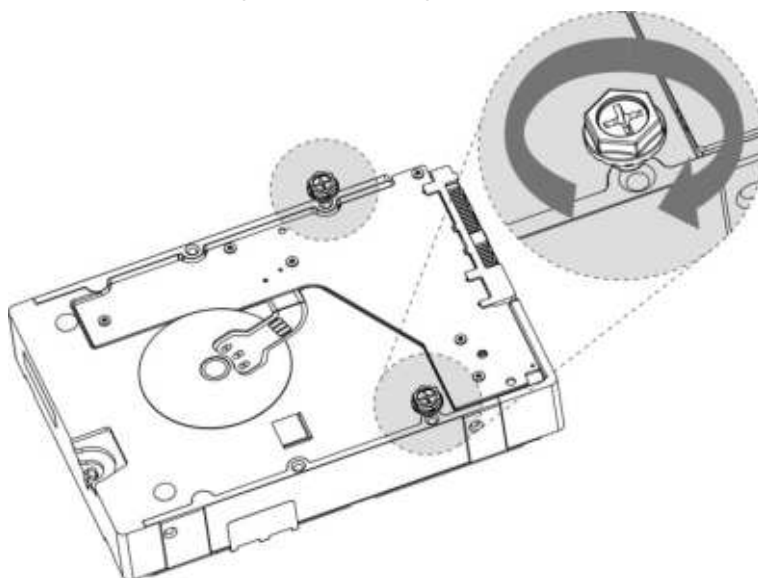
Step 1 Remove the screws to take off the cover.

Figure 1-1 Taking off cover



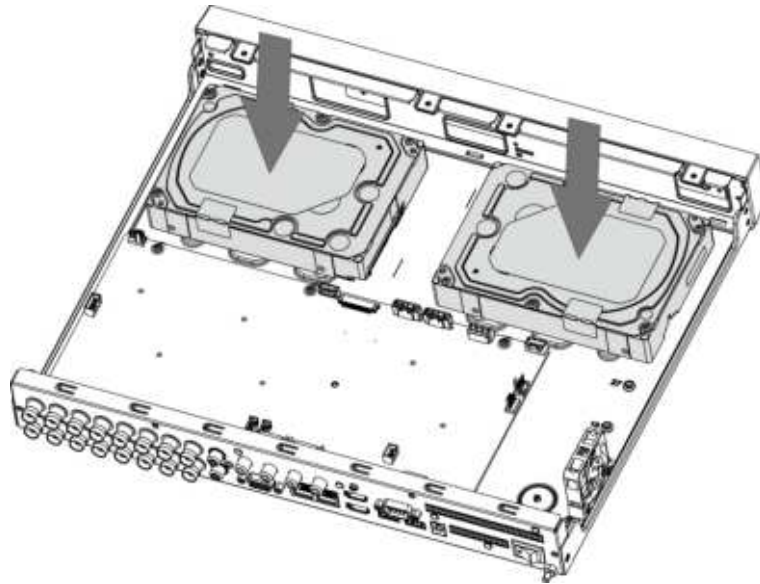
Step 2 Put two screws on the HDD and twist one turn.

Figure 1-2 Putting in screws



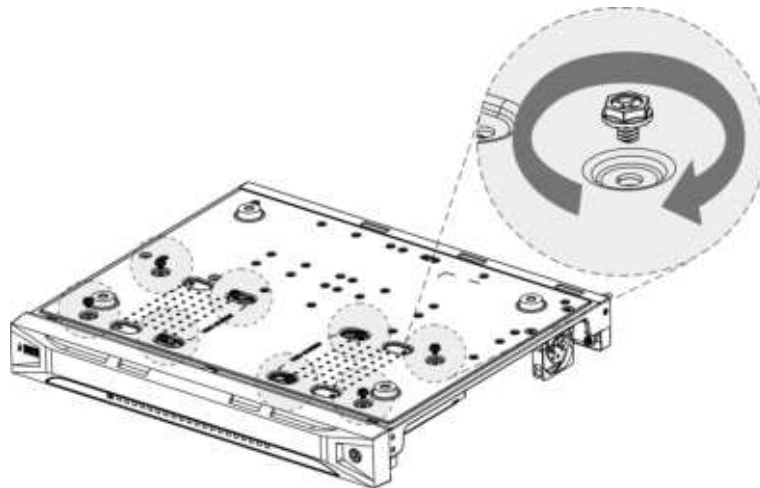
Step 3 Align the two screws with the holes on the device.

Figure 1-3 HDD placement



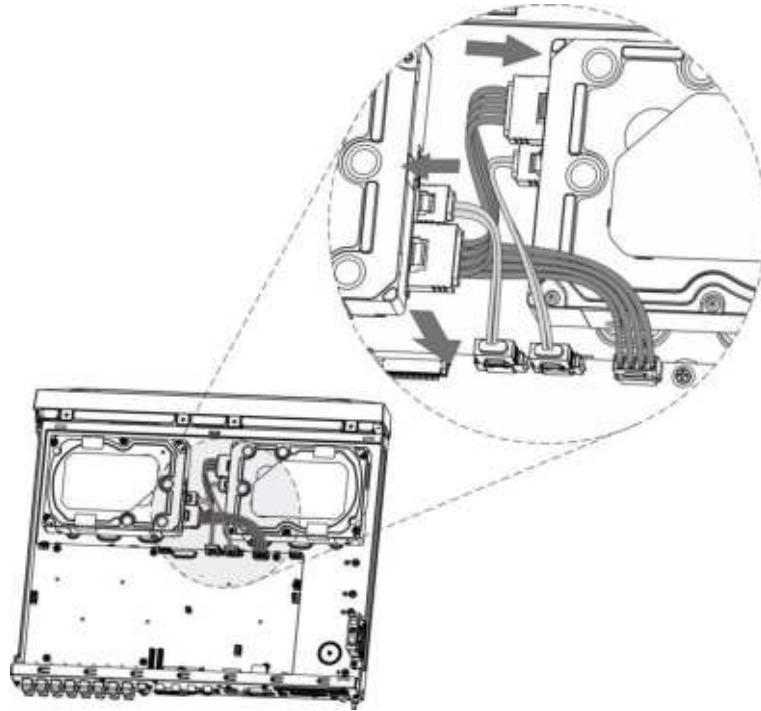
Step 4 Turn the device and put in the other two screws, and then fasten all screws to fix the HDD to the device.

Figure 1-4 HDD fixing to device



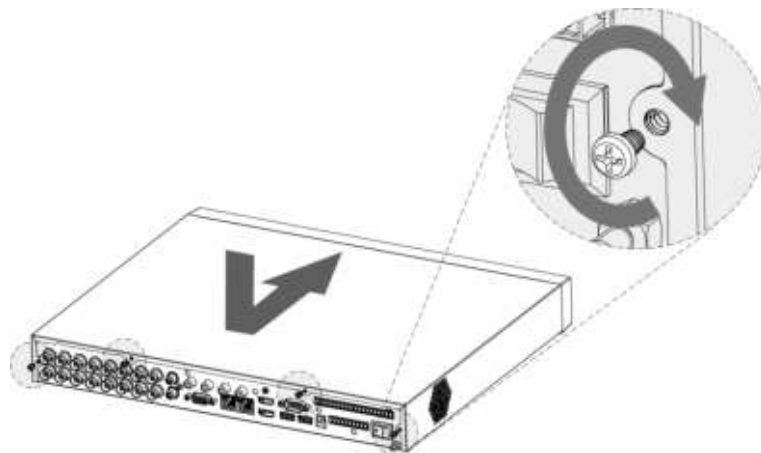
Step 5 Use power cable and data cable to connect the device and HDD.

Figure 1-5 Cables connection



Step 6 Put back the cover and fasten the screws.

Figure 1-6 Installation completed



1.4 Booting up



CAUTION

- Ensure the input voltage corresponds to the power requirement of the DVR. Turn on the DVR after the power cable is properly connected.
- To protect the DVR, connect the DVR with the power cable first, and then connect to the power source.
- To ensure the stable work of the DVR and the connected external devices such as camera and to prolong the HDD service life, please refer to the related international standard to use the power source that provides stable voltage with less ripple interference. UPS power source is recommended.

Step 1 Connect the DVR to a display.

Step 2 Plug in the power cable to the DVR.

Step 3 Press the power button to turn on the DVR. The power indicator glows.

On the connected display, the live view screen is displayed. If you turn on the DVR during the time period that is configured for recording, the system starts recording after it is turned on, and you will see the icon indicating recording status in specific channels.

2 The Grand Tour for Rear Panel

NOTE

The actual appearance might be different depending on the model you purchased.

The following figure shows the rear panel of the DVR.

Figure 2-1 Rear panel

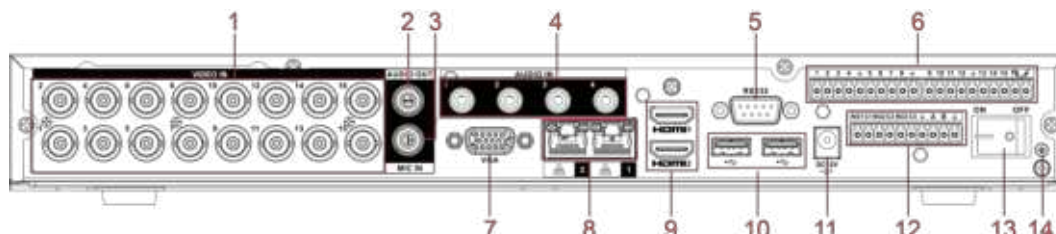


Table 2-1 Port description

No.	Port Name	Function
1	Video input port	Connects to analog camera to input video signal.
2	Audio output port	Outputs audio signal to the devices such as the sound box.
3	MIC IN	Two-way talk input port which receives analog audio signal output from the devices such as microphone and pickup.
4	Audio input port	Receives audio signal output from the devices such as microphone.
5	RS-232 debug COM	The port is used for general COM debug to configure IP address or transfer transparent COM data.
6	Alarm input port 1–16	4 groups of alarm input ports (Group 1: port 1 to port 4; Group 2: port 5 to port 8; Group 3: port 9 to port 12; Group 4: port 13 to port 16). These ports receive the signal from the external alarm source. There are two types: NO (normal open) and NC (normal close). NOTE When your alarm input device is using external power, please make sure the input device and the DVR connect to the same ground.
	⏏	Ground terminal.
7	VGA port	Outputs analog video data to the connected display with VGA port.
8	Network port	Connects to Ethernet port.
9	HDMI port	High definition audio and video signal output port. The port outputs the uncompressed high definition video and multi-channel audio data to the connected display with HDMI port.
10	USB port	Connects to the external devices such as keyboard, mouse, and USB storage device.

No.	Port Name	Function
11	Power input port	Inputs power.
12	Alarm output port 1–5 (NO1–NO5; C1–C5; NC5)	• 5 groups of alarm output ports (Group 1: port NO1–C1, Group 2: port NO2–C2, Group 3: port NO3–C3, Group 4: port NO4–C4, Group 5: port NO5, C5, NC5). These ports output alarm signal to the alarm device. Please make sure power supply to the external alarm device. • NO: Normal open alarm output port. • C: Alarm output public end. • NC: Normal close alarm output port.
13	Power button	Turns on/off the DVR.
14		Ground.

3 Local Configurations

Please read the following notes prior to using your DVR.

NOTE

- The interfaces in the Guide are used for introducing the operations and only for reference. The actual product shall govern.
- For details about operations of the DVR, see *User's Manual*.
- To enter the Main Menu, right-click on the live view screen to display the shortcut menu, and then click **Main Menu** and login the system.

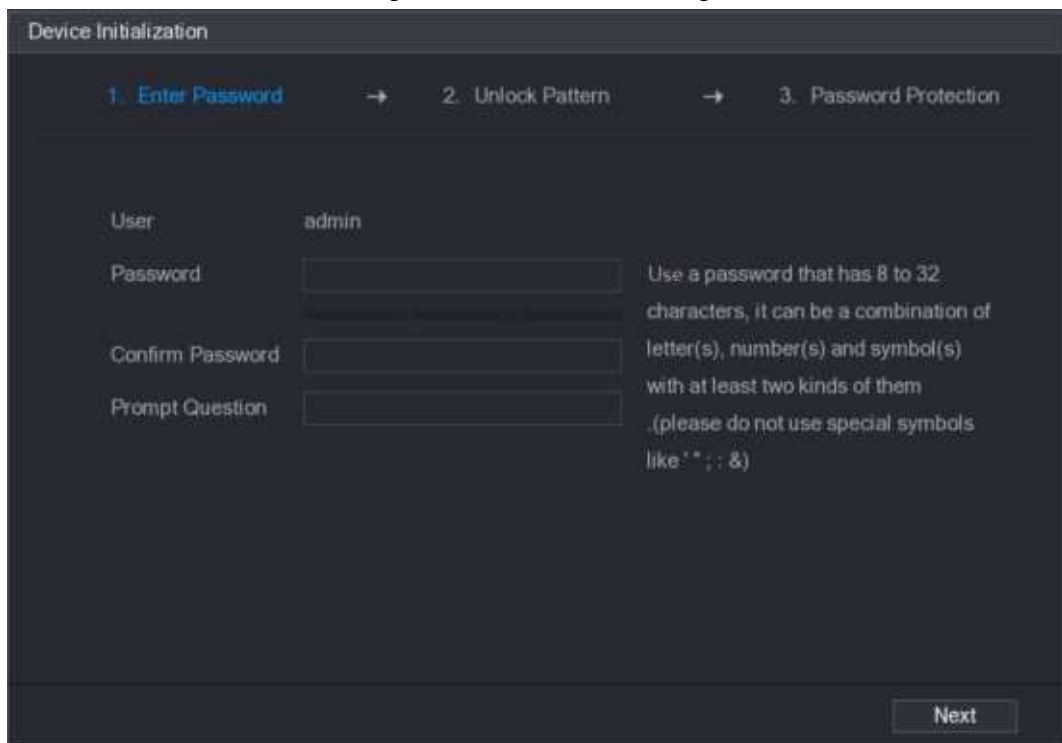
3.1 Initializing DVR

When booting up for the first time, the **Device Initialization** interface is displayed, see Figure 3-1. You need to configure the password information for the **admin** (by default). If needed, you can also configure the unlock pattern and password protection mode, see Figure 3-2 and Table 3-1.

NOTE

- The new password can be set from 8 characters through 32 characters and contains at least two types from number, letter and special characters (excluding "", "", ";", ":" and "&"). Please enter a strong password according to the password strength bar indication.
- To secure your DVR, it is strongly recommended to properly keep the password for admin and modify it periodically.

Figure 3-1 Password setting



The screenshot shows the 'Device Initialization' screen with a progress bar at the top indicating three steps: 1. Enter Password (active), 2. Unlock Pattern, and 3. Password Protection. Below the progress bar, the 'User' field is set to 'admin'. There are three input fields: 'Password', 'Confirm Password', and 'Prompt Question'. To the right of these fields, a text box provides instructions: 'Use a password that has 8 to 32 characters, it can be a combination of letter(s), number(s) and symbol(s) with at least two kinds of them. (please do not use special symbols like " " ; : &)'. A 'Next' button is located at the bottom right of the screen.

Figure 3-2 Password protection

Table 3-1 Password protection mode description

Password Protection Mode	Description
Email Address	Enter the reserved email address. In the Email Address box, enter an email address for password reset. In case you forgot password, enter the security code that you will get from this reserved email address to reset the password of admin.
Security Questions	Configure the security questions and answers. In case you forgot password, enter the answers to the questions can make you reset the password.
 NOTE If you want to configure the email or security questions function later or you want to change the configurations, select Main Menu > ACCOUNT > USER .	

3.2 Resetting Password

You can reset the password by the following methods when you forgot the password for admin account.

- If the password reset function is enabled, you can use mobile phone to scan the QR code to reset the password.
- If the password reset function is disabled, there are two situations:
 - ◇ If you configured security questions, you can find back the password by the security questions.
 - ◇ If you did not configure the security questions, you can only use the reset button on the mainboard to restore the Device to factory default.



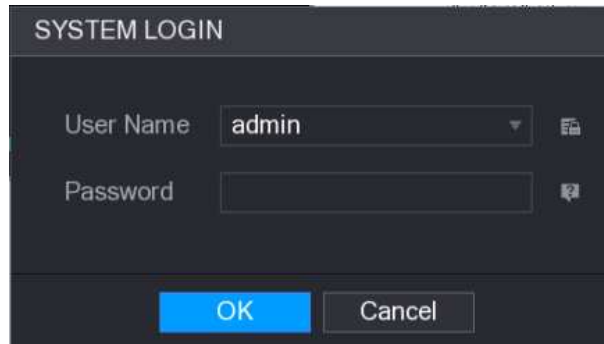
NOTE

Not all models are provided with reset button.

Step 1 Enter the login interface.

- If you have configured unlock pattern, the unlock pattern login interface is displayed. Click **Forgot Pattern**, the password login interface is displayed. See Figure 3-3.
- If you did not configure unlock pattern, the password login interface is displayed. See Figure 3-3.

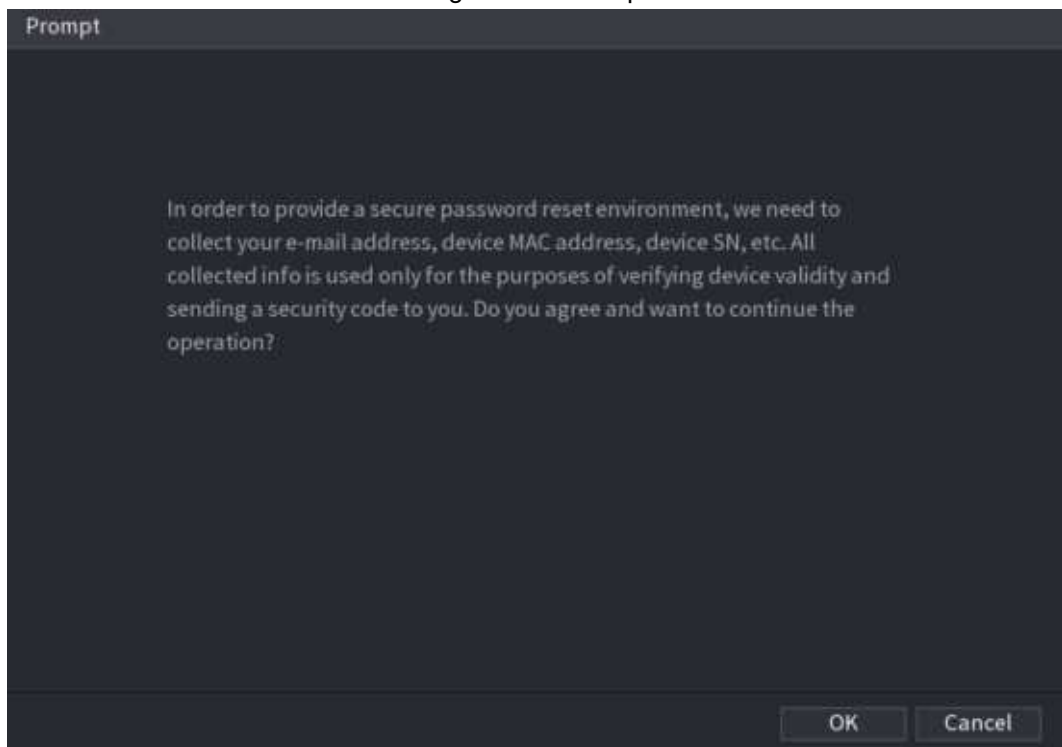
Figure 3-3 System login

A dark-themed dialog box titled "SYSTEM LOGIN". It contains two input fields: "User Name" with the text "admin" and a dropdown arrow, and "Password" which is empty. To the right of each field is a small icon (a key for User Name and a key with a slash for Password). At the bottom are two buttons: "OK" (highlighted in blue) and "Cancel".

Step 2 Click .

- If you did not set the reserved email address, the email entering interface is displayed. Enter the email address, and then click **Next**, the **Prompt** message interface is displayed. See Figure 3-4.
- If you have set the reserved email address, the **Prompt** message interface is displayed. See Figure 3-4.

Figure 3-4 Prompt

A dark-themed dialog box titled "Prompt". It contains a paragraph of text: "In order to provide a secure password reset environment, we need to collect your e-mail address, device MAC address, device SN, etc. All collected info is used only for the purposes of verifying device validity and sending a security code to you. Do you agree and want to continue the operation?". At the bottom are two buttons: "OK" and "Cancel".

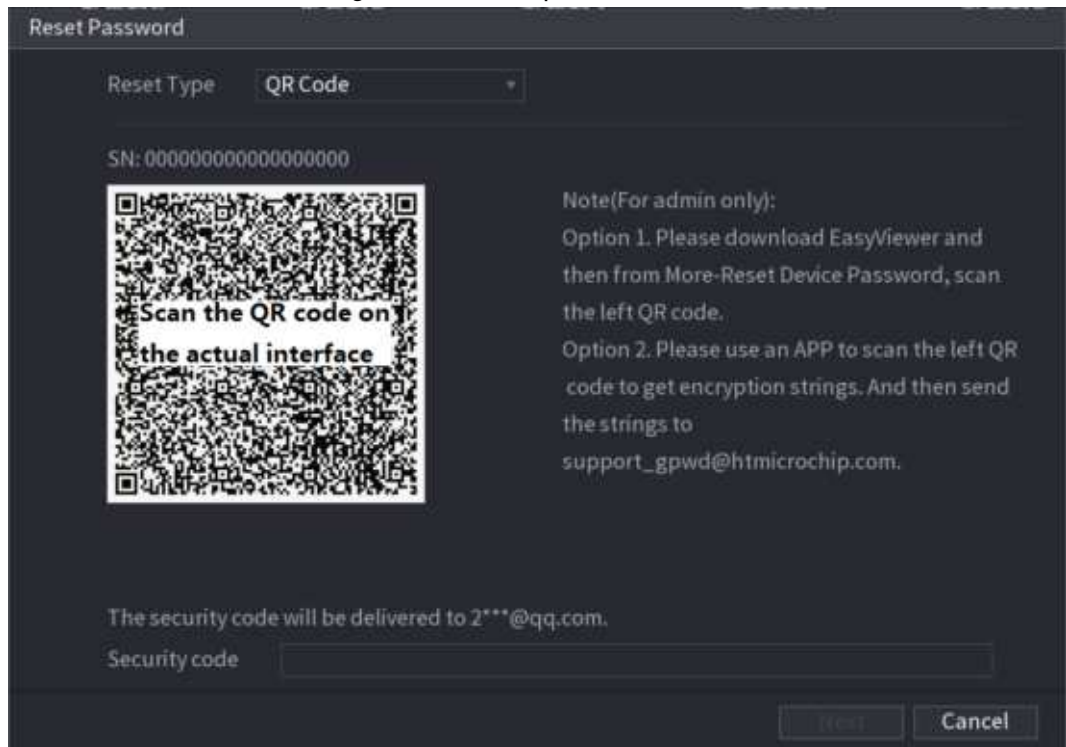
Step 3 Click **OK**.

The **Reset Password** interface is displayed. See Figure 3-5.

NOTE

After clicking **OK**, the system will collect your information for password reset, and the information includes but not limited to email address, MAC address, and device serial number. Please read the prompt carefully before clicking **OK**.

Figure 3-5 Reset password



Step 4 Reset the password.

- QR code
Scan the QR code on the actual interface, and then follow the onscreen instructions to get the security code in your reserved email address. In the **Security code** box, enter the security code.

CAUTION

- You can get the security code twice by scanning the same QR code. If you need to get the security code once again, please refresh the interface.
- Please use the security code received in your email box to reset the password within 24 hours; otherwise the security code becomes invalid.
- Security questions
 - 1) On the **Reset password** interface as shown in Figure 3-4, in the **Reset Type** list, select **Security Questions**, the **Security Questions** interface is displayed. See Figure 3-6.

NOTE

If you did not configure the security questions before, in the **Reset Type** list, there is no **Security Questions**.

- 2) In the **Answer** box, enter the correct answers.

Figure 3-6 Security questions

Reset Password

Reset Type: **Security Questions**

Question 1: What is your favorite children's book?
Answer:

Question 2: What was the first name of your first boss?
Answer:

Question 3: What is the name of your favorite fruit?
Answer:

Next Cancel

Step 5 Click **Next** and then follow the onscreen instructions to complete the password resetting.

3.3 Adding Remote Device

You can add remote devices by adding the IP address.

NOTE

This function is available after having configured the channel type as IP channel by selecting

Main Menu > CAMERA > CHANNEL TYPE.

Step 1 Select **Main Menu > CAMERA > REGISTRATION > Registration.**

The **Registration** interface is displayed.

Step 2 Click **IP Search.**

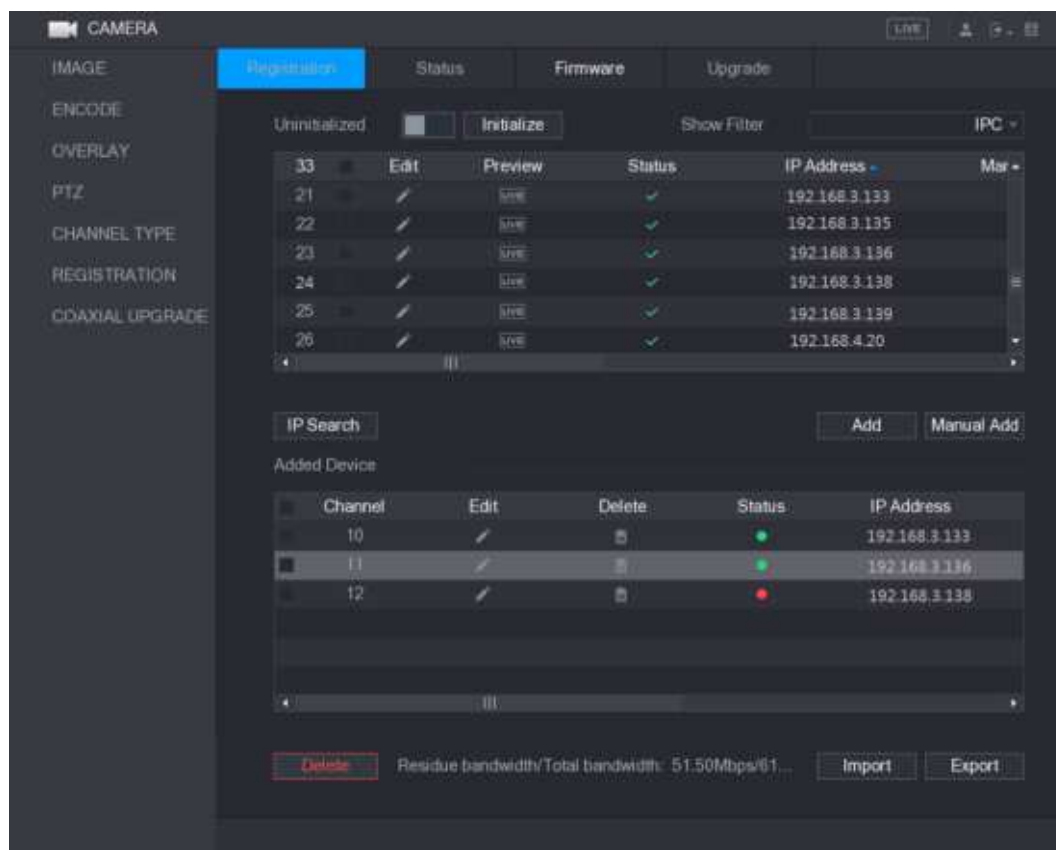
The searched devices are displayed.

Step 3 Add the device by either of the following ways.

- Double-click the device, or select the check box of the device and then click **Add.**
- Click **Manual Add**, configure the parameters and then click **Apply.**

The device is displayed in the **Added Device** area. See Figure 3-7.

Figure 3-7 Added device

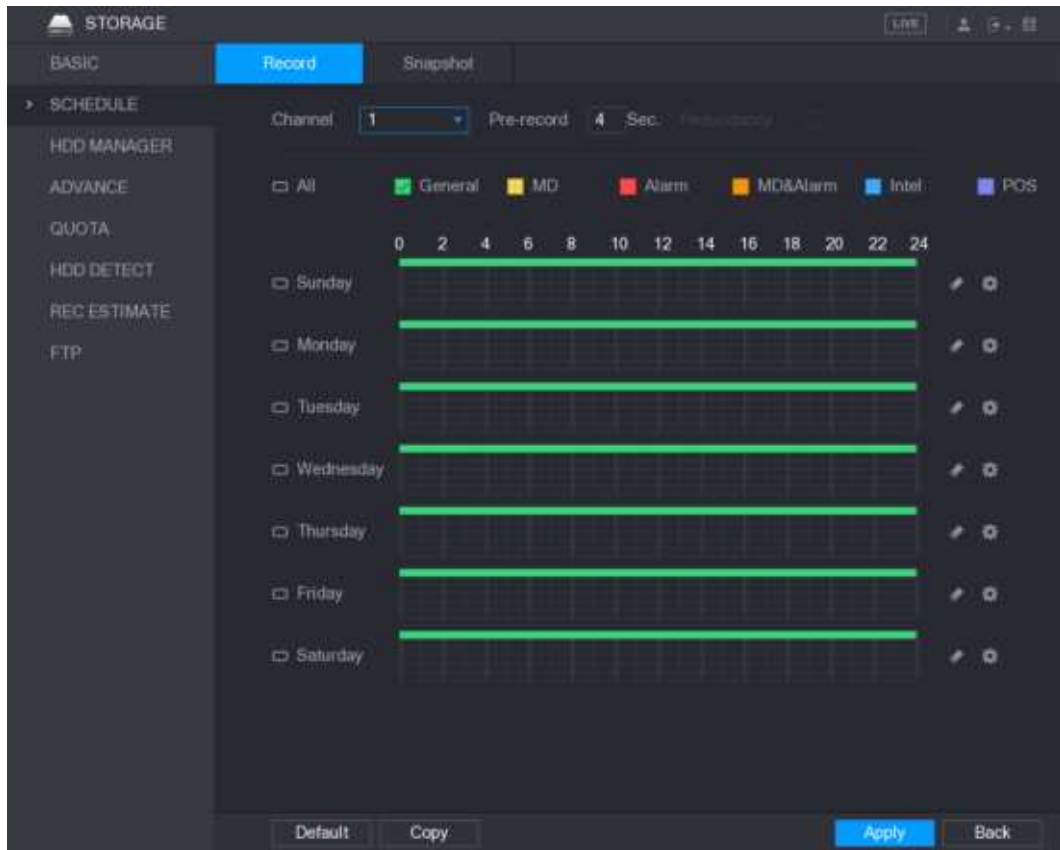


3.4 Configuring Recording Storage Schedule

Select **Main Menu > STORAGE > SCHEDULE > Record**, the **Record** interface is displayed, see Figure 3-8.

The default setting is 24 hours recording for all channels. You can modify the settings if needed.

Figure 3-8 Record storage configuration



3.5 Playing Back Recorded Video

You can search for and play back the recorded videos saved on the DVR.

Step 1 Select **Main Menu > VIDEO**.

The video search interface is displayed. See Figure 3-9.

Figure 3-9 Recorded video



Step 2 Select the source as **From R/W HDD** or **From I/O Device** from where you want to search for the recorded video.

Step 3 In the search type list, select **RECORD**.

Step 4 In the calendar area, select a date.

Step 5 In the **CAM NAME** list, select a channel.

Step 6 Click .

The system starts playing recorded video.

3.6 Configuring P2P Settings

You can add the DVR into your cell phone client or the platform to manage. For details, please refer to the P2P operation manual.

NOTE

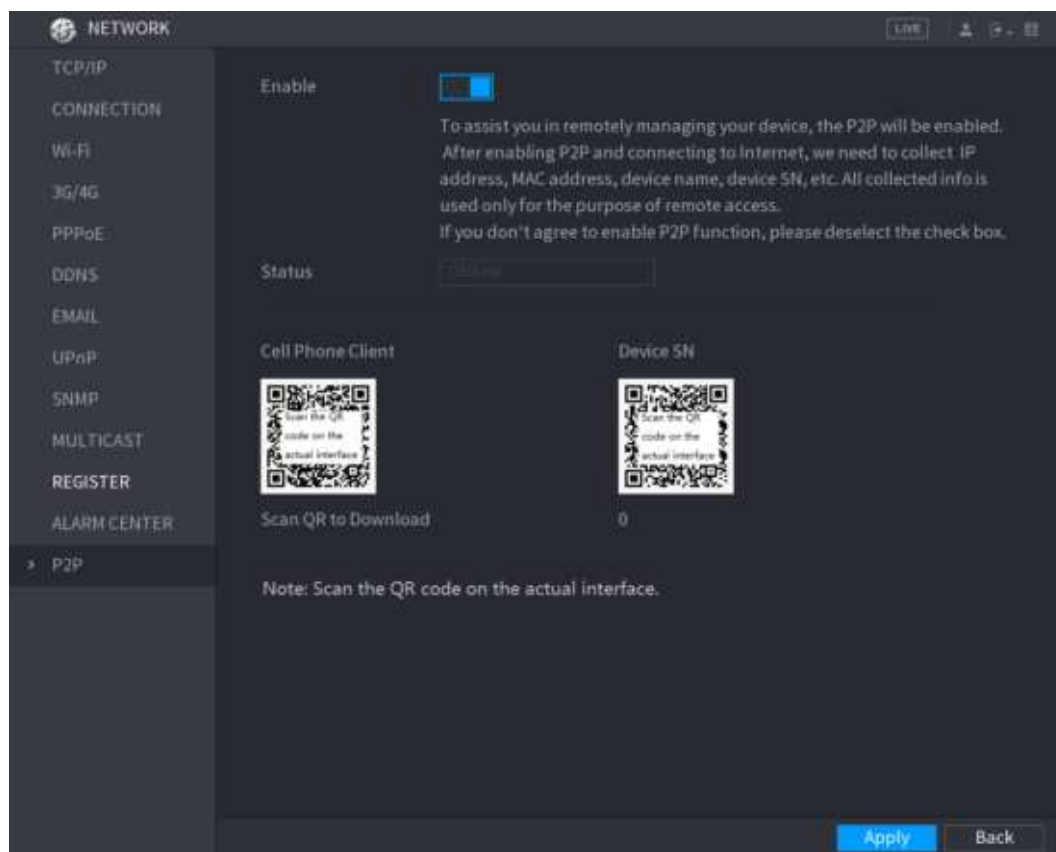
Make sure the DVR is connected into the Internet, and if yes, in the **Status** box of the P2P interface, it shows **Online**.

3.6.1 Entering P2P Interface

Step 1 Select **Main Menu > NETWORK > P2P**.

The **P2P** interface is displayed. See Figure 3-10.

Figure 3-10 P2P interface



Step 2 Enable the P2P function.

Step 3 Click **Apply**.

You can start adding the DVR into Cell Phone Client or the platform.

3.6.2 Adding DVR into Cell Phone Client

To use P2P function, take adding device into Cell Phone Client as an example.



You can also enter the QR code interface by clicking  on the top right of the interfaces after you have entered the Main Menu.

Step 1 Use your cell phone to scan the QR code under **Cell Phone Client** to download the application.

Step 2 On your cell phone, open the application, and then tap , the menu is displayed.

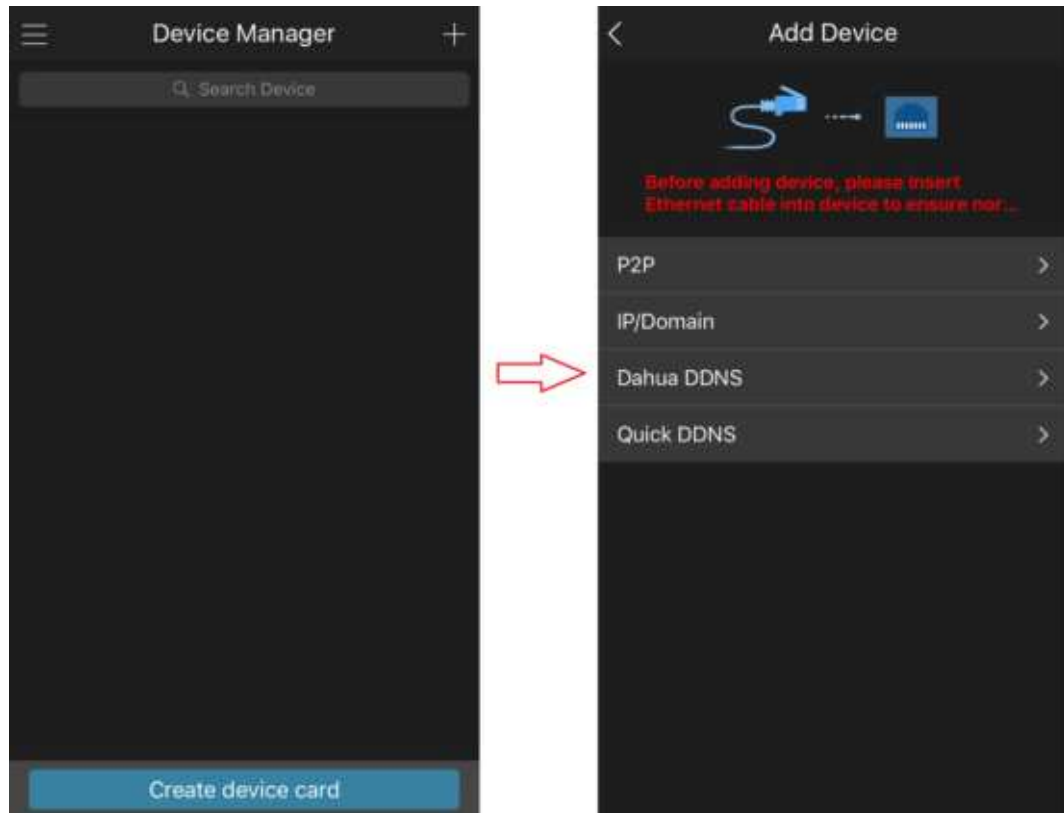
Step 3 Tap **Device Manager** >  > **Add Device**.

The **Add Device** interface is displayed. See Figure 3-11.



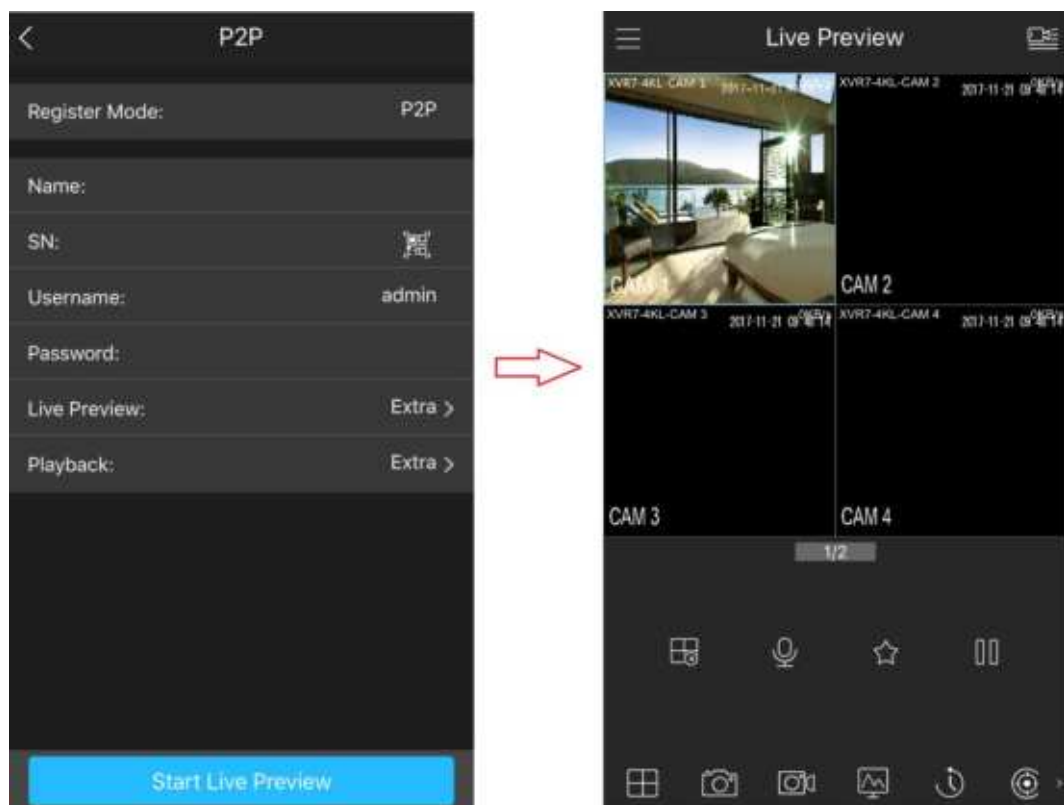
- If the DVR has not been initialized, follow the onscreen instructions to perform initialization first.
- You can add wireless device or wired device. The Guide takes adding wired device as an example.

Figure 3-11 Add device



Step 4 Tap **P2P**, enter a name for the DVR, the username and password, scan the QR code under **Device SN**, and then tap **Start Live Preview**. The DVR is added and displayed on the live view interface of the cell phone. See Figure 3-12.

Figure 3-12 Live view



3.7 Logout

On the top right of the Main Menu interface or any interface after you have entered the Main Menu, click .

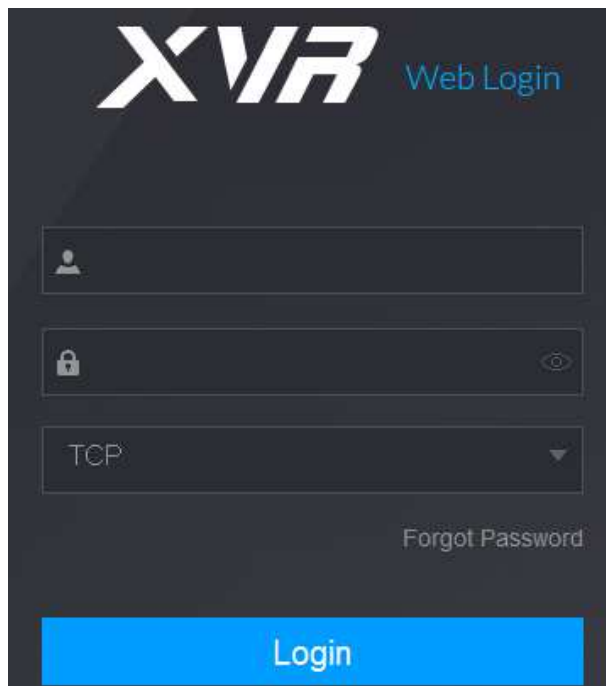
- Select **Logout**, you will log out the DVR.
- Select **Reboot**, the DVR will be rebooted.
- Select **Shutdown**, the DVR will be turned off.

You can also press the power button on the DVR to turn it off.

4 Web Login

Open the browser, enter the IP address of the DVR, and then press **Enter**. The **Login in** dialog box is displayed. See Figure 4-1. Properly enter the user name and password to login the web. For details, see *User's Manual*.

Figure 4-1 Login

The image shows the XVR Web Login interface. At the top, the 'XVR' logo is in white and 'Web Login' is in blue. Below the logo, there are three input fields: a username field with a person icon, a password field with a lock icon and a toggle eye icon, and a protocol dropdown menu currently set to 'TCP'. To the right of the protocol dropdown is a 'Forgot Password' link. At the bottom, there is a large blue 'Login' button.

NOTE

- Device initialization is required at the first login.
- The default administrator account is **admin**. The password is the one that was configured during initializing settings. To security your account, it is recommended to keep the password properly and change it periodically.
- You can select the protocol type as **TCP**, **UDP**, or **MULTICAST** depending on the networking structure. The default is **TCP**.
- If you forgot the password, click **Forgot Password** to reset the password.
- When entering the **Live** interface for the first time, follow the onscreen instructions "Please install plugins first!" to install the plugins.

Manual

Regulatory Information

The regulatory information herein might vary according to the model you purchased. Some information is only applicable for the country or region where the product is sold.

FCC Information



Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

FCC conditions:

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operation.

FCC compliance:

This equipment has been tested and found to comply with the limits for a digital device, pursuant to part 15 of the FCC Rules. This equipment generate, uses and can radiate radio frequency energy and, if not installed and used in accordance with the guide, may cause harmful interference to radio communication.

- For class A device, these limits are designed to provide reasonable protection against harmful interference in a commercial environment. 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.
- For class B device, these limits are designed to provide reasonable protection against harmful interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
 - Reorient or relocate the receiving antenna.
 - Increase the separation between the equipment and receiver.
 - Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
 - Consult the dealer or an experienced radio/TV technician for help.

Foreword

General

This user's manual (hereinafter referred to be "the Manual") introduces the functions and operations of the DVR devices (hereinafter referred to as "the Device").

Safety Instructions

The following categorized signal words with defined meaning might appear in the Manual.

Signal Words	Meaning
 DANGER	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
 WARNING	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
 CAUTION	Indicates a potential risk which, if not avoided, could result in property damage, data loss, lower performance, or unpredictable result.
 TIPS	Provides methods to help you solve a problem or save you time.
 NOTE	Provides additional information as the emphasis and supplement to the text.

Revision History

No.	Version	Revision Content	Release Time
4	V1.0.6	Added some models.	May 2020
3	V1.0.5	Updated to 4.0 UI version.	February 2020
2	V1.0.4	Added disarm function, HDD database function, and SMD preview function. Optimizes Smart Search function, available to filtering human and vehicle.	September 2019
1	V1.0.0	First release.	October 2018

Privacy Protection Notice

As the device user or data controller, you might collect personal data of others such as face, fingerprints, car plate number, Email address, phone number, GPS and so on. You need to be

in compliance with the local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures include but not limited to: providing clear and visible identification to inform data subject the existence of surveillance area and providing related contact.

About the Manual

- The manual is for reference only. If there is inconsistency between the manual and the actual product, the actual product shall prevail.
- We are not liable for any loss caused by the operations that do not comply with the manual.
- The manual would be updated according to the latest laws and regulations of related regions. For detailed information, see the paper manual, CD-ROM, QR code or our official website. If there is inconsistency between paper manual and the electronic version, the electronic version shall prevail.
- All the designs and software are subject to change without prior written notice. The product updates might cause some differences between the actual product and the manual. Please contact the customer service for the latest program and supplementary documentation.
- There still might be deviation in technical data, functions and operations description, or errors in print. If there is any doubt or dispute, please refer to our final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and the company names in the manual are the properties of their respective owners.
- Please visit our website, contact the supplier or customer service if there is any problem occurred when using the device.
- If there is any uncertainty or controversy, please refer to our final explanation.

Safeguards and Warnings

This chapter describes the contents covering proper handling of the Device, hazard prevention, and prevention of property damage. Read these contents carefully before using the Device, comply with them when using, and keep it well for future reference.

Operation Requirement

- Do not place or install the Device in a place exposed to sunlight or near the heat source.
- Keep the Device away from dampness, dust or soot.
- Keep the Device installed horizontally on the stable place to prevent it from falling.
- Wall-mounting is not supported.
- Do not drop or splash liquid onto the Device, and make sure there is no object filled with liquid on the Device to prevent liquid from flowing into the Device.
- Install the Device in a well-ventilated place, and do not block the ventilation of the Device.
- Operate the device within the rated range of power input and output.
- Do not disassemble the Device.
- Transport, use and store the Device under the allowed humidity and temperature conditions.

Electrical Safety

- Use the battery of specified manufacturer; otherwise there might result in explosion. When replacing battery, make sure the same type is used. Improper battery use might result in fire, explosion, or inflammation.
- Follow the instructions to dispose of the used battery.
- Use the recommended power cables in the region and conform to the rated power specification.
- Use the power adapter provided with the Device, or adapter meets the LPS standard; otherwise, it might result in people injury and device damage.
- The power source shall conform to the requirement of the Safety Extra Low Voltage (SELV) standard, and supply power with rated voltage which conforms to Limited power Source requirement according to IEC60950-1. Please note that the power supply requirement is subject to the device label.
- Connect the device (I-type structure) to the power socket with protective earthing.
- The appliance coupler is a disconnection device. When using the coupler, keep the angle for easy operation.

Table of Contents

Regulatory Information	I
Foreword	II
Safeguards and Warnings	IV
1 Introduction	1
1.1 Overview	1
1.2 Functions.....	1
2 Getting Started	3
2.1 Checking the Components.....	3

3.3 Remote Control Operations	19
3.4 Mouse Operations.....	21
4 Connecting Basics	23
4.1 Typical Connection Diagram	23
4.2 Connecting to Video and Audio Input and Output	24
4.2.1 Video Input.....	24
4.2.2 Video Output.....	24
4.2.3 Audio Input.....	24
4.2.4 Audio Output	25
4.3 Connecting to Alarm Input and Output	25
4.3.1 Introducing Alarm Port	26
4.3.2 Alarm Input.....	26
4.3.3 Alarm Output.....	27
4.3.4 Alarm Output Relay Parameters.....	27
5 Local Configurations	28
5.1 Initial Settings.....	28
5.1.1 Booting up.....	28
5.1.2 Initializing the Device	28
5.1.3 Resetting Password.....	32
5.1.4 Setting Up with the Startup Wizard.....	39
5.2 Live View.....	55
5.2.1 Live View Screen	55
5.2.2 Live View Control bar.....	56
5.2.3 Navigation Bar	60
5.2.4 Shortcut Menu	61
5.2.5 AI Preview Mode.....	62
5.2.6 Channel Sequence	64
5.2.7 Color Setting	66
5.2.8 Live View Display.....	68
5.2.9 Configuring Tour Settings	72
5.2.10 Quick Operation Bar	75
5.3 Entering Main Menu	77
5.4 Controlling PTZ Cameras	79
5.4.1 Configuring PTZ Connection Settings	79
5.4.2 Working with PTZ Control Panel	81
5.4.3 Configuring PTZ Functions.....	83
5.4.4 Calling PTZ Functions	85
5.4.5 Calling OSD Menu	87
5.5 Configuring Camera Settings.....	88
5.5.1 Configuring Image Settings	88
5.5.2 Configuring Encode Settings.....	91
5.5.3 Configuring Snapshot Settings	93
5.5.4 Configuring Encode Enhancement.....	94
5.5.5 Configuring Overlay Settings.....	95
5.5.6 Configuring Covered Area Settings	96
5.5.7 Configuring Channel Type	97
5.5.8 Upgrading Coaxial Camera	98

5.6 Configuring Remote Devices	99
5.6.1 Adding Remote Devices	99
5.6.2 Managing Remote Devices	111
5.7 Configuring Record Settings	113
5.7.1 Enabling Record Control	114
5.7.2 Configuring Recorded Video Storage Schedule.....	115
5.8 Configuring Snapshot Settings	115
5.8.1 Configuring Snapshot Trigger	115
5.8.2 Configuring Snapshot Storage Schedule	117
5.8.3 Backing up Snapshots to FTP	117
5.9 Playing Back Video	118
5.9.1 Enabling Record Control	118
5.9.2 Instant Playback	119
5.9.3 Main Interface of Video Playback.....	119
5.9.4 Smart Search	126
5.9.5 Showing AI Rule during Playback	126
5.9.6 Marking and Playing Back Video.....	127
5.9.7 Playing Back Snapshots	130
5.9.8 Playing Back Splices	130
5.9.9 Using the File List	130
5.10 Alarm Events Settings.....	132
5.10.1 Alarm Information.....	132
5.10.2 Alarm Input Settings	133
5.10.3 Alarm Output Settings.....	139
5.10.4 Video Detection	143
5.10.5 System Events.....	152
5.10.6 Configuring Disarming.....	155
5.11 AI Function	156
5.11.1 For Pro AI Series.....	156
5.11.2 For Lite AI Series	194
5.12 IoT Function	229
5.12.1 Configuring Sensor Settings.....	229
5.12.2 Configuring Temperature and Humidity Camera.....	236
5.12.3 Configuring Wireless Siren	248
5.13 Configuring POS Settings	248
5.13.1 Searching the Transaction Records	249
5.13.2 Configuring POS Settings.....	249
5.14 Configuring Backup Settings	251
5.14.1 Finding USB Device	251
5.14.2 Backing up Files	252
5.15 Network Management.....	253
5.15.1 Configuring Network Settings.....	253
5.15.2 Configuring Network Testing Settings	270
5.16 Configuring Account Settings.....	274
5.16.1 Configuring User Account.....	275
5.16.2 Configuring Group Account	280
5.16.3 Configuring ONVIF Users.....	284

5.17 Audio Management	285
5.17.1 Configuring Audio Files.....	285
5.17.2 Configuring Playing Schedule for Audio Files	287
5.18 Storage Management.....	288
5.18.1 Configuring Basic Settings	288
5.18.2 Configuring the Recording and Snapshot Schedule	289
5.18.3 Configuring Disk Manager	289
5.18.4 Configuring Record.....	291
5.18.5 Configuring Advance Settings	291
5.18.6 Configuring Disk Quota	293
5.18.7 Configuring HDD Detecting Settings	294
5.18.8 Configuring Record Estimate	297
5.18.9 Configuring FTP Storage Settings.....	299
5.19 Security Center	301
5.19.1 Security Status.....	301
5.19.2 System Service.....	302
5.19.3 Attack Defense.....	306
5.19.4 CA Certificate.....	311
5.19.5 Audio/Video Encryption	314
5.19.6 Security Warning	316
5.20 Configuring System Settings	319
5.20.1 Configuring General System Settings	319
5.20.2 Configuring RS-232 Settings.....	320
5.20.3 Configuring System Maintenance Settings	321
5.20.4 Exporting and Importing System Settings	322
5.20.5 Restoring Default Settings.....	324
5.20.6 Updating the Device	325
5.21 Viewing Information	328
5.21.1 Viewing Version Details	328
5.21.2 Viewing Log Information	328
5.21.3 Viewing Event Information.....	330
5.21.4 Viewing Network Information.....	331
5.21.5 Viewing HDD Information	333
5.21.6 Viewing Channel Information.....	334
5.21.7 Viewing Data Stream Information	335
5.22 Logout the Device	336
6 Web Operations.....	337
6.1 Connecting to Network.....	337
6.2 Logging in the Web	337
6.3 Introducing Web Main Menu	338
7 FAQ	340
Appendix 1 Glossary.....	346
Appendix 2 HDD Capacity Calculation.....	348
Appendix 3 Compatible Backup Devices	350
Appendix 3.1 Compatible USB list.....	350
Appendix 3.2 Compatible SD Card list	351
Appendix 3.3 Compatible Portable HDD list.....	351

Appendix 3.4 Compatible USB DVD List	351
Appendix 3.5 Compatible SATA DVD List.....	351
Appendix 3.6 Compatible SATA HDD List	352
Appendix 4 Compatible CD/DVD Burner List	357
Appendix 5 Compatible Displayer List.....	358
Appendix 6 Compatible Switcher	359
Appendix 7 Earthing	360
Appendix 7.1 What Is the Surge	360
Appendix 7.2 The Earthing Modes	361
Appendix 7.3 Thunder Proof Ground Method in the Monitor System	362
Appendix 7.4 The Shortcut Way to Check the Electric System by Digital Multimeter.....	363
Appendix 8 RJ45-RS-232 Connection Cable Definition	366
Appendix 9 Cybersecurity Recommendations	368

1 Introduction

1.1 Overview

The Device is an excellent digital monitor product for security industry. The embedded LINUX OS assures the stable operation. The H.265 and G.711 technologies assure the high quality image and low bit stream. The frame-by-frame play function displays more details for analysis, and provides the functions such as record, playback, and monitor and assures the synchronization for audio and video. The Device also adopts the advanced control technology and great network data transmission capability.

The Device adopts embedded design to achieve high security and reliability. It can work in the local end and, with strong networking capability it can get connected to the professional surveillance software (Smart PSS) to form a security network to show its powerful remote monitoring function.

The Device is applicable to the areas such as bank, telecom, electricity, traffic, intelligent residential district, factory, warehouse, resources, and water conservancy facilities.

1.2 Functions



The functions might be different depending on the software and hardware versions of the model you purchased.

AI Function

- Support face detection that analyzes the attributes such as age, gender, glasses, beard, mask, and then make structured of these data to store for quick search.
- Support face recognition that compares the captured face snapshot with the face library and link the configured alarms (face detection should be enabled).
- Support searching by picture that is convenient for finding the target picture from database.
- Support 16 channel IVS function that includes tripwire and intrusion detection. The IVS function can avoid wrong alarms by filtering the factors such as rains, light, and animals.
- Calculate the quantity of detected humans within 24 hours.
- Detect the vehicles passing by within 24 hours.

Real-time Surveillance

- Support VGA port and HDMI port to realize the surveillance through monitors.
- Support HDMI, VGA, and TV output at the same time.

IoT Management

Provide specific management module for IoT features including humidity and temperature data reports and alarms linkage.

Sensor Integration

Integrate coaxial cameras with diverse array of sensors such as temperature, humidity and wireless alarm devices.

Storage Management

- Special data format to guarantee data security and avoid the risk of modifying data viciously.
- Support digital watermark.

Compression Format

Support multiple-channel audio and video signal. An independent hardware decodes the audio and video signal from each channel to maintain video and audio synchronization.

Backup Function

- Support backup operation through USB port (such as USB storage disk, portable HDD, and burner).
- Client-end user can download the file from local HDD through network to backup.

Record & Playback

- Support each channel real-time record independently, and simultaneously support the functions such as search, backward play, network monitor, record search, and download.
- Support various playback modes: slow play, fast play, backward play and frame by frame play.
- Support time title overlay so that you can view event accurate occurred time.
- Support zooming in the selected area in the live view.

Network Operation

Support network remote real-time monitor, remote record search and remote PTZ control.

Alarm Activation

- Several relay alarm outputs to realize alarm activation and on-site light control.
- The alarm input port and output port have the protection circuit to guarantee the Device safety.

Communication Port

- RS-485 port can realize alarm input and PTZ control.
- RS-232 port can connect to keyboard, COM port of PC or the matrix control.
- Standard Ethernet port can realize network remote access function.
- The dual-network port has the multi-address, fault tolerance, load balance setup mode.

PTZ Control

Support PTZ decoder through RS-485 port.

Intelligent Operation

- Support mouse operation function.
- Support "copy and paste" function for the same settings.

UPnP (Universal Plug and Play)

Establish mapping connection between LAN and WAN through UPnP protocol.

Camera Self-adaptive

Auto-recognize and work with the PAL or NTSC camera and HD camera.

2 Getting Started

2.1 Checking the Components



The actual appearance, component, or quantity might be different depending on the model you purchased.

When you receive the Device, please check against the following checking list. If any of the items are missing or damaged, contact the local retailer or after-sales engineer immediately.

No.	Checking Items		Requirement
1	Package	Appearance	No obvious damage.
		Packing materials	No broken or distorted positions that could be caused by hit.
2	Labels	Labels on the device	Not torn up.  Do not tear up or throw away the labels; otherwise the warranty services are not ensured. You need to provide the serial number of the product when you call the after-sales service.
3	Device	Appearance	No obvious damage.
		Data cables, power cables, fan cables, mainboard	No connection loose.

3.3 Remote Control Operations



Please note the remote control is not our standard accessory and might not be included in the accessory bag. It is supplied dependent on the model you purchased.

Figure 3-12

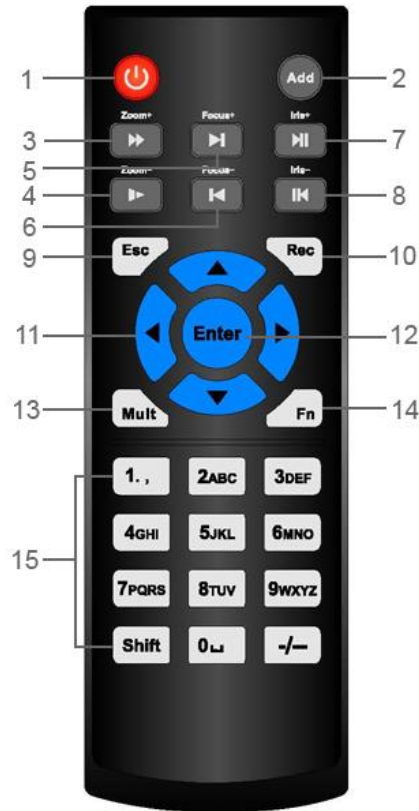


Table 3-12

No.	Name	Function
1	Power button	Press this button to boot up or shut down the device.
2	Address	Press this button to input device serial number, so that you can control the Device.
3	Forward	Multi-step forward speed and normal speed playback.
4	Slow motion	Multi-step slow motion speed or normal playback.
5	Next record	In playback state, press this button to play back the next video.
6	Previous record	In playback state, press this button to play back the previous video.
7	Play/Pause	- In normal playback state, press this button to pause playback. - In pause state, press this button to resume to normal playback. - In live view window interface, press this button to enter video search menu.
8	Reverse/pause	In the reverse playback state, press this button to pause reverse playback. In the reverse playback pause state, press this button to resume to playback reversing state.
9	Esc.	Go back to previous menu or cancel current operation (close front interface or control).

No.	Name	Function
10	Record	- Start or stop record manually. - In record interface, use the direction buttons to select the channel that you want to record. - Press this button for at least 1.5 seconds, and the manual record interface will be displayed.
11	Direction keys	Switch between current activated controls by going left or right. In playback state, the keys control the playback progress bar. Aux function (such as operating the PTZ menu).
12	Enter/menu key	- Confirms an operation. - Go to the OK button. - Go to the menu.
13	Multiple-window switch	Switch between multiple-window and one-window.
14	Fn	- In single-channel monitoring mode, press this button to display the PTZ control and color setting functions. - Switch the PTZ control menu in PTZ control interface. - In motion detection interface, press this button with direction keys to complete setup. - In text mode, press and hold this button to delete the last character. To use the clearing function: Long press this button for 1.5 seconds. - In HDD menu, switch HDD recording time and other information as indicated in the pop-up message.
15	Alphanumeric keys	- Input password, numbers. - Switch channel. - Press Shift to switch the input method.

3.4 Mouse Operations



The operations are based on the considerations for right-handed users.

Table 3-13

Operation	Function
Click left mouse button	Password input dialogue box pops up if you have not logged in yet. In live view window interface, you can go to the main menu.
	When you have selected one menu item, click it to view menu content.
	Implement the control operation.
	Modify check box or motion detection status.
	Click combo box to pop up drop-down list.
	In text box, click the corresponding button on the panel to enter a numeral or English character (small/capitalized). In English input mode: Click  to enter a backspace and click .

Operation	Function
	to delete the previous character.  In numeral input mode: Click  to clear and click  to delete the previous character. 
Double-click left mouse button	Implement special control operations such as double-click one item in the file list to play back the video. In multiple-window mode, double-click one channel to view in full-window. Double-click current video again to go back to previous multiple-window mode.
Right-click	Right-click in live view window interface, the shortcut menu is displayed. For different series product, the shortcut menu may vary. Exit current menu without saving the modification.
Click scroll wheel button	In numeral input box: Increase or decrease numeral value. Switch the items in the combo box. Page up or page down.
Point to select and move	Select current control and move it.
Dragging a selection box with left mouse button	Select motion detection zone. Select privacy mask zone.

4 Connecting Basics

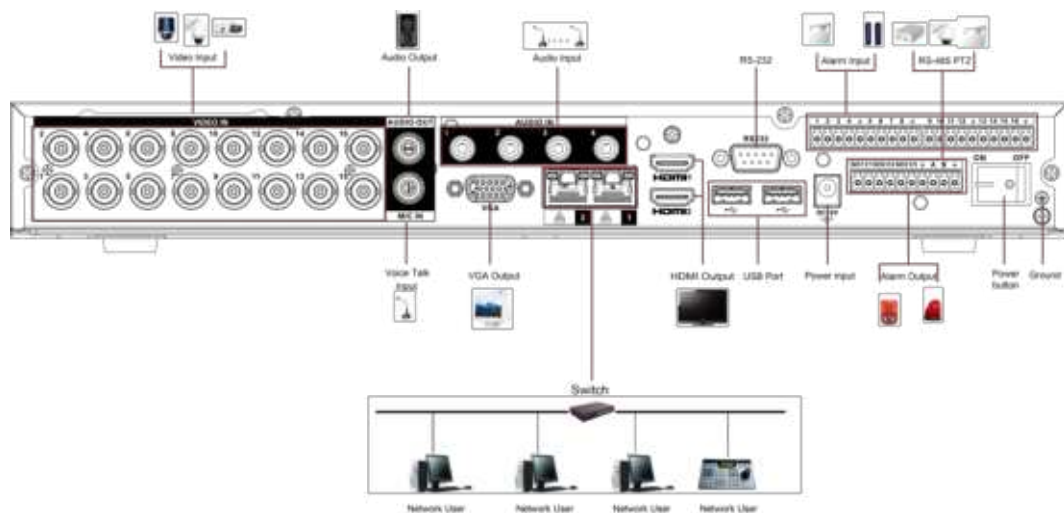
This chapter introduces the typical connection diagrams and ports connections.

4.1 Typical Connection Diagram



The following figure is for reference only. The actual product shall prevail.

Figure 4-1



4.2 Connecting to Video and Audio Input and Output

4.2.1 Video Input

The video input interface is BNC. The input video format includes: PAL/NTSC BNC ($1.0V_{P-P}$, 75Ω).

The video signal should comply with your national standards.

The input video signal shall have high SNR, low distortion; low interference, natural color, and suitable lightness.

Guarantee the stability and reliability of the camera signal

The camera shall be installed in a cool, dry place away from the conditions such as direct sunlight, inflammable, and explosive substances.

The camera and the DVR should have the same grounding to ensure the normal operation of the camera.

Guarantee stability and reliability of the transmission line

Please use high quality, sound shielded BNC. Please select suitable BNC model according to the transmission distance.

If the distance is too long, you should use twisted pair cable, and you can add video compensation devices or use optical fiber to ensure video quality.

You should keep the video signal away from the strong electromagnetic interference, especially the high tension current.

Keep connection lugs in well contact

The signal line and shielded wire should be fixed firmly and in well connection. Avoid dry joint, lap welding, and oxidation.

4.2.2 Video Output

Video output includes a BNC ($1.0V_{P-P}$, 75Ω) output, a VGA output, and HDMI output. System supports BNC, VGA and HDMI output at the same time.

When you are using pc-type monitor to replace the monitor, please pay attention to the following points:

- To defer aging, do not allow the pc monitor to run for a long time.
- Regular demagnetization will keep device maintain proper status.
- Keep it away from strong electromagnetic interference devices.

Using TV as video output device is not a reliable substitution method. You also need to reduce the working hour and control the interference from power supply and other devices. The low quality TV may result in device damage.

4.2.3 Audio Input

This series of products audio input port adopt BNC port.

Due to high impedance of audio input, please use active sound pick-up.

Audio transmission is similar to video transmission. Try to avoid interference, dry joint, loose contact and it shall be away from high tension current.

4.2.4 Audio Output

The audio output signal parameter is usually over 200mv 1K Ω (BNC or RCA). It can directly connect to low impedance earphone, active sound box or amplifier-drive audio output device.

If the sound box and the pick-up cannot be separated spatially, it is easy to arouse squeaking. In this case you can adopt the following measures:

- Use better sound pick-up with better directing property.
- Reduce the volume of the sound box.
- Using more sound-absorbing materials in decoration can reduce voice echo and improve acoustics environment.
- Adjust the layout of speaker and pickup to reduce squeaking.

4.3 Connecting to Alarm Input and Output

Please read the followings before connecting.

Alarm input

- Make sure alarm input mode is grounding alarm input.
- Grounding signal is needed for alarm input.
- Alarm input needs the low level voltage signal.
- Alarm input mode can be either NC (Normally Closed) or NO (Normally Open).
- When you are connecting two DVRs or you are connecting one DVR and one other device, use a relay to separate them.

Alarm output

The alarm output port should not be connected to high power load directly (It shall be less than 1A) to avoid high current which might result in relay damage. Use the contactor to realize the connection between the alarm output port and the load.

How to connect PTZ decoder

- Ensure the decoder has the same grounding with DVR; otherwise the PTZ might not be controlled. Shielded twisted wire is recommended and the shielded layer is used to connect to the grounding.
- Avoid high voltage. Ensure proper wiring and some thunder protection measures.
- For too long signal wires, 120 Ω should be parallel connected between A, B lines on the far end to reduce reflection and guarantee the signal quality.
- “485 A, B” of DVR cannot parallel connect with “485 port” of other device.
- The voltage between of A, B lines of the decoder should be less than 5V.

Make sure the front-end device has soundly earthed

Improper grounding might result in chip damage.

4.3.1 Introducing Alarm Port



The alarm input ports are dependent on the model you purchased.

Figure 4-2

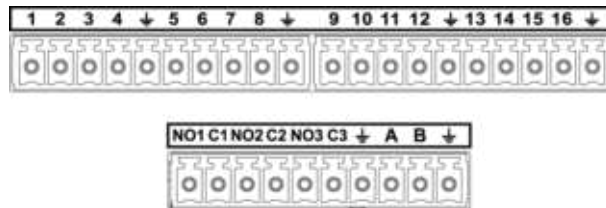


Table 4-1

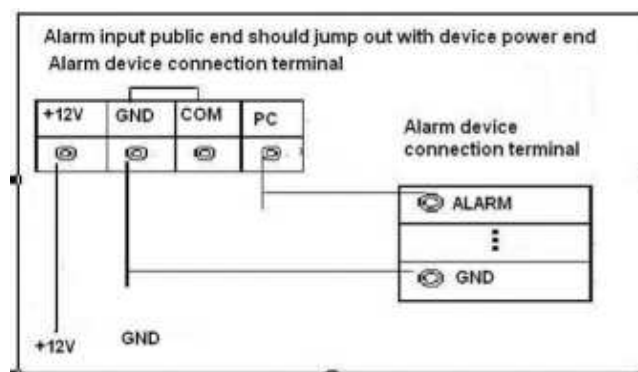
Icon	Description
1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	ALARM 1 to ALARM 16. The alarm becomes active in low voltage.
NO1 C1, NO2 C2, NO3 C3	There are four groups of normally open activation output (on/off button).
	Ground cable.
485 A/B	485 communication port. They are used to control devices such as decoder. 120Ω should be parallel connected between A, B lines if there are too many PTZ decoders.

4.3.2 Alarm Input

Refer to the following figure for more information.

- Grounding alarm inputs which includes NO (Normally Open) and NC (Normally Closed) type.
- Parallel connect COM end and GND end of the alarm detector (Provide external power to the alarm detector).
- Parallel connect the Ground of the DVR and the ground of the alarm detector.
- Connect the NC port of the alarm sensor to the DVR alarm input (ALARM).
- Use the same ground with that of DVR if you use external power to the alarm device.

Figure 4-3



4.3.3 Alarm Output

- Provide external power to external alarm device.
- To avoid overloading, read the following relay parameters table carefully.
- RS-485 A/B cable is for the A/B cable of the PTZ decoder.

4.3.4 Alarm Output Relay Parameters



Refer to the actual product for relay model information.

Table 4-2

Model		HFD23/005-1ZS	HRB1-S-DC5V
Material of the touch		AgNi+ gold-plating	AuAg10/AgNi10/CuNi30
Rating (Resistance Load)	Rated switch capacity	30V DC 1A/125V AC 0.5A	24V DC 1A/125V AC 2A
	Maximum switch power	62.5VA/30W	250VA/48W
	Maximum switch voltage	125V AC/60V DC	125V AC/60V DC
	Maximum switch currency	2A	2A
Insulation	Between touches	400VAC 1 minute	500VAC 1 minute
	Between touch and winding	1000VAC 1 minute	1000VAC 1 minute
Turn-on Time		5ms maximum	5ms maximum
Turn-off Time		5ms maximum	5ms maximum
Longevity	Mechanical	1×10^7 times (300 times/MIN)	5×10^6 times (300 times/MIN)
	Electrical	1×10^5 times (30 times/MIN)	2.5×10^4 times (30 times/MIN)
Working Temperature		-30℃—+70℃	-40℃—+70℃

5 Local Configurations

Read the following notes prior to using the Device.



- The interfaces in the Manual are used for introducing the operations and only for reference. The actual interface might be different dependent on the model you purchased. If there is inconsistency between the Manual and the actual product, the actual product shall govern.
- The Manual is a general document for introducing the product, so there might be some functions described for the Device in the Manual not apply to the model you purchased.
- Conventions for mouse operations on a menu.
 - ◇ Click: On the menu, left-click the mouse once on an option to enter the option setting.
 - ◇ Right-click: On any interface, right-click the mouse once to return to the previous level. For details about mouse operations, see "3.4 Mouse Operations."

5.1 Initial Settings

5.1.1 Booting up



- Ensure the input voltage corresponds to the power requirement of the Device. Power on the Device after the power cable is properly connected.
- To protect the Device, connect the Device with the power cable first, and then connect to the power source.
- To ensure the stable work of the Device and the external devices connected to the Device and to prolong the HDD life, it is recommended to refer to the national related standard to use the power source that provides stable voltage with less interference from ripples. UPS power source is recommended.

Step 1 Connect the Device to the monitor.

Step 2 Plug in the power cable to the Device.

Step 3 Press the power button to turn on the Device. The power indicator light is on.

On the connected monitor, the live view screen is displayed by default. If you turn on the Device during the time period that is configured for recording, the system starts recording after it is turned on, and you will see the icon indicating recording status is working in the specific channels.

5.1.2 Initializing the Device

When booting up for the first time, you need to configure the password information for **admin** (by default).

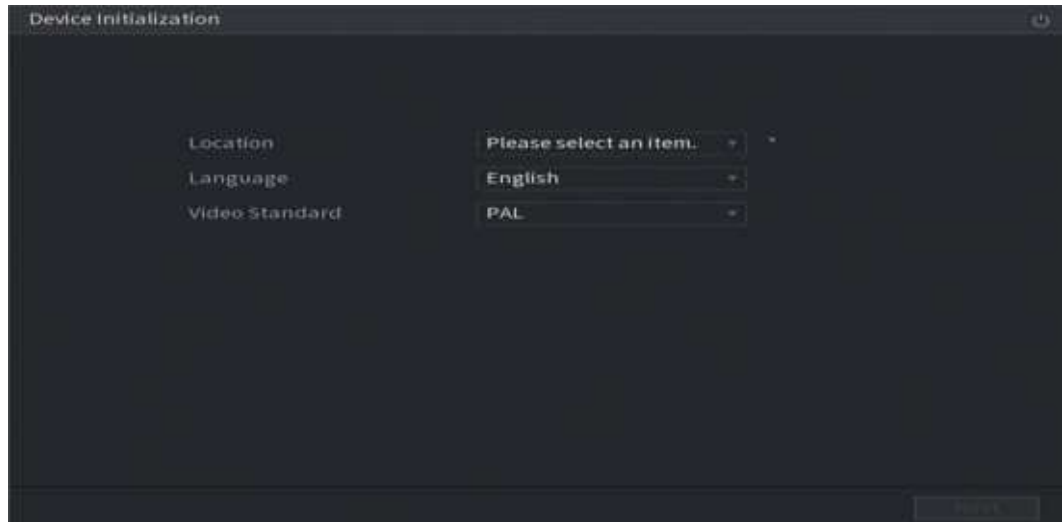


To secure the Device, it is strongly recommended for you to properly keep the password for admin and modify it regularly.

Step 1 Turn on the Device.

The **Location, Language** and **Video Standard** interface is displayed. See Figure 5-1.

Figure 5-1

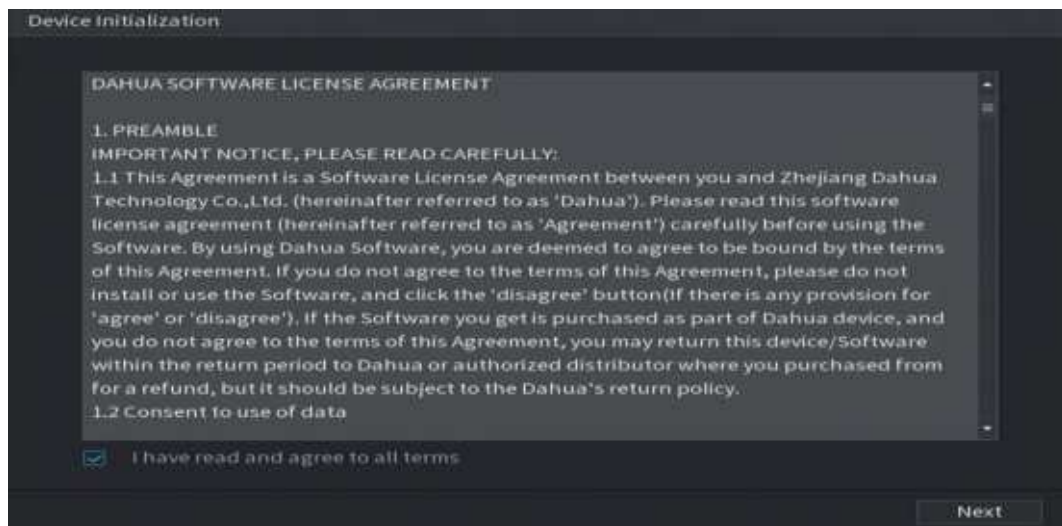


Step 2 Select your location from the drop-down list, then language and video standard will match your location automatically. You can change the language and video standard manually.

Step 3 Click **Next**.

The **Dahua Software License Agreement** interface is displayed. See Figure 5-2.

Figure 5-2



Step 4 Tick the check box that **I have read and agree to all terms**, and then click **Next**.

The **System Zone** and **System Time** interface is displayed. See Figure 5-3.

Figure 5-3

The screenshot shows the 'Device Initialization' window. It has a dark background. At the top, the title 'Device Initialization' is in a light gray bar. Below the title, there are two configuration items: 'Time Zone' with a dropdown menu showing '(UTC+04:00) Yerevan' and a small downward arrow, and 'System Time' with two input fields showing '2020 -01 -08' and '13 : 11 : 35'. At the bottom right, there is a 'Next' button.

Step 5 Select system zone, configure system time, and then click **Next**.
The **Enter Password** interface is displayed.

Figure 5-4

The screenshot shows the 'Device Initialization' window at the '1. Password Setting' step. At the top, there is a progress bar with three steps: '1. Password Setting' (highlighted in blue), '2. Unlock Pattern', and '3. Password Protection', connected by right-pointing arrows. Below the progress bar, there are four input fields: 'Username' (with the value 'admin'), 'Password', 'Confirm Password', and 'Password Hint'. To the right of these fields, there is a text box explaining the password requirements: 'Password must be 8 to 32 characters, including at least two of the following categories: numbers, uppercase letters, lowercase letters and special characters. (Characters like ' ', ':', and ';' cannot be included in)'. At the bottom right, there is a 'Next' button.

Step 6 Configure the password information for admin. For details, see Table 5-1.

Table 5-1

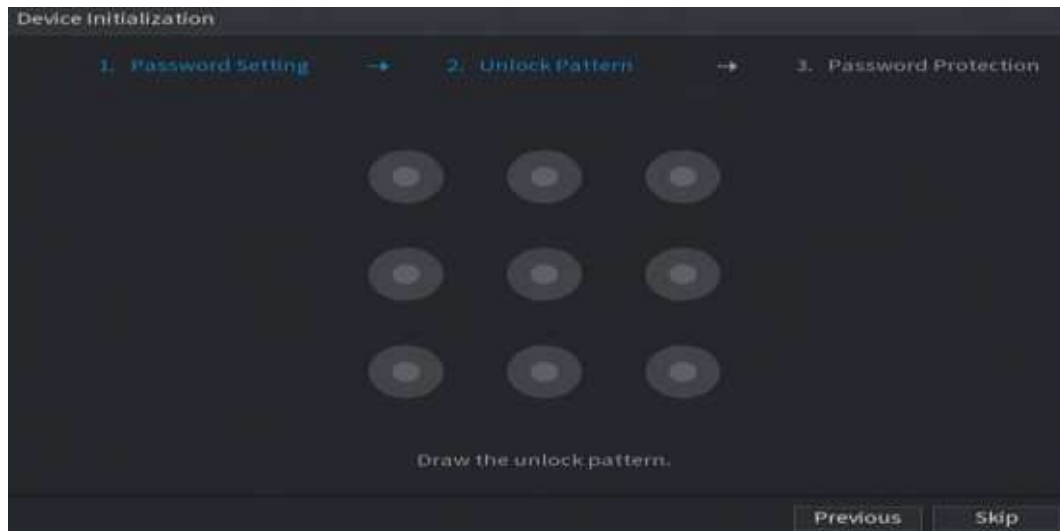
Parameter	Description
User	By default, the user is admin .
Password	In the Password box, enter the password for admin.
Confirm Password	The new password can be set from 8 characters through 32 characters and contains at least two types from number, letter and special characters (excluding "", "", ":", "." and "&").

Parameter	Description
Prompt Hint	In the Prompt Hint box, enter the information that can remind you of the password.  On the login interface, click , the prompt will display to help you find back the password.

Step 7 Click **Next**.

The **Unlock Pattern** interface is displayed.

Figure 5-5



Step 8 Draw an unlock pattern.

After the setting is completed, the **Password Protection** interface is displayed. See Figure 5-6.



- The pattern that you want to set must cross at least four points.
- If you do not want to configure the unlock pattern, click **Skip**.
- Once you have configured the unlock pattern, the system will require the unlock pattern as the default login method. If you skip this setting, enter the password for login.

Figure 5-6



Step 9 Configure the protection parameters for password. For details, see Table 5-2.

After configuration, if you forget the password for admin user, you can reset the password through the reserved email address or security questions. For details about resetting the password, see 5.1.3

If you do not want to configure the settings, disable the email address and security questions functions on the interface.

Table 5-2

Password Protection Mode	Description
Reserved Email	Enter the reserved email address. In the Reserved Email box, enter an email address for password reset. If you forget the password, enter the security code that you will get from this reserved email address to reset the password of admin.
Security Questions	Configure the security questions and answers. If you forget the password, enter the answers to the questions can make you reset the password.
 If you want to configure the email or security questions function later or you want to change the configurations, select Main Menu > ACCOUNT > Password Reset .	

Step 10 Click **OK** to complete the settings.

The **End-User License Agreement** interface is displayed.

Step 11 Select **I have read and agree to all terms** check box.

Step 12 Click **Next**.

The **Startup Wizard** interface is displayed. For details about quick settings during startup, see 5.1.4.

5.1.3 Resetting Password

You can reset the password by the following methods when you forget the password for admin account.

- If the password reset function is enabled, you can use mobile phone to scan the QR code to reset the password. For details, see "5.1.3.2 Resetting Password on Local Interface."
- If the password reset function is disabled, there are two situations:
 - ◇ If you configured security questions, you can find back the password by the security questions.
 - ◇ If you did not configure the security questions, you can only use the reset button on the mainboard to restore the Device to factory default. For details, see "5.1.3.3 Using Reset Button on the Mainboard."



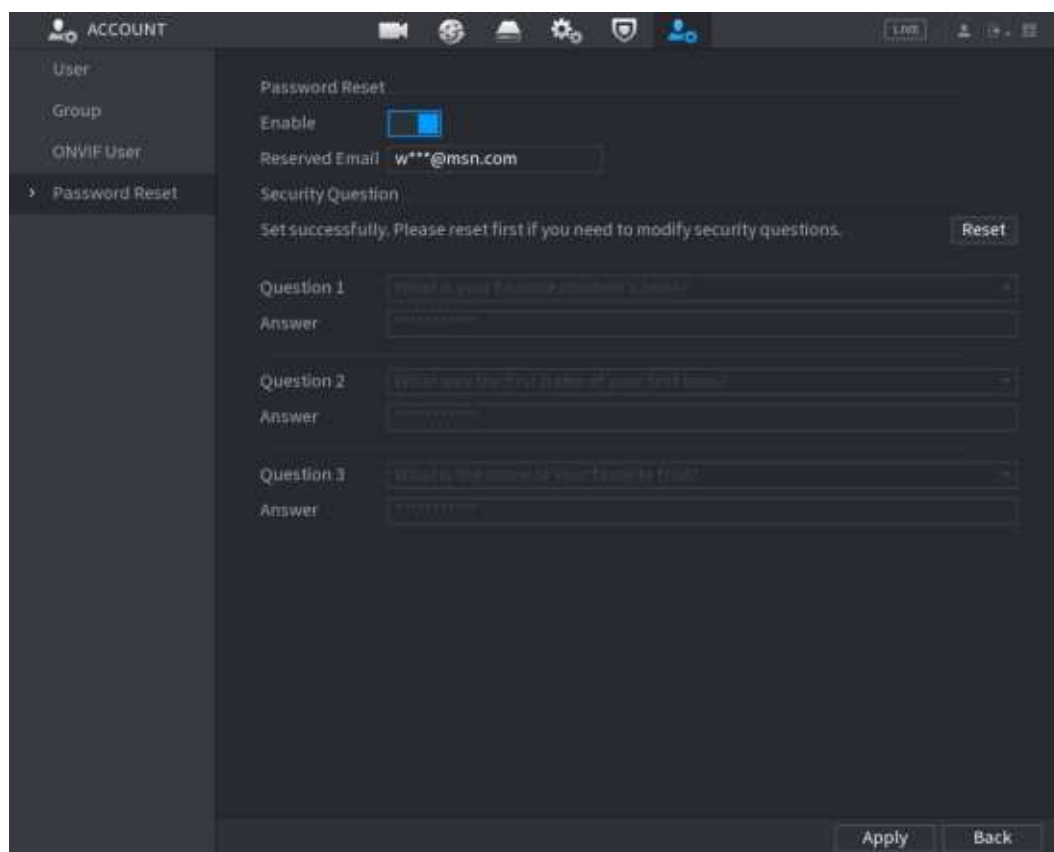
Not all models are provided with reset button.

5.1.3.1 Enabling Password Reset Function

Step 1 Select **Main Menu > Account > Password Reset**.

The **Password Reset** interface is displayed.

Figure 5-7



Step 2 Enable the Password Reset function.



This function is enabled by default.

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

When Password reset function is disabled, you can retrieve password through following ways:

- You can retrieve password through resetting password on local interface or using Reset button on the mainboard when the device supports Reset button.
- You can only retrieve password through resetting password on local interface (make sure that security questions are preset) when the device does not support Reset button.

5.1.3.2 Resetting Password on Local Interface

Step 1 Enter the login interface.

- If you have configured unlock pattern, the unlock pattern login interface is displayed. See Figure 5-8. Click **Forgot Pattern**, the password login interface is displayed. See Figure 5-9.
- If you did not configure unlock pattern, the password login interface is displayed.

See Figure 5-9. Click  to display the password with plaintext.



To login from other user account, on the unlock pattern login interface, click **Switch User**; or on the password login interface, in the **User Name** list, select other users to login.

Figure 5-8

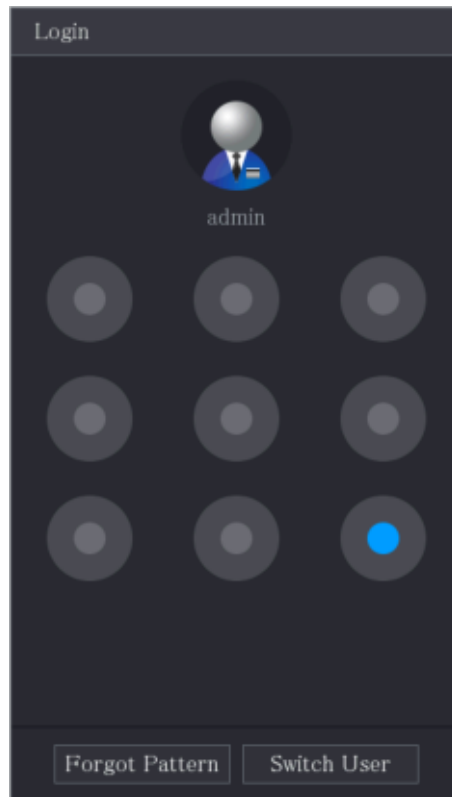
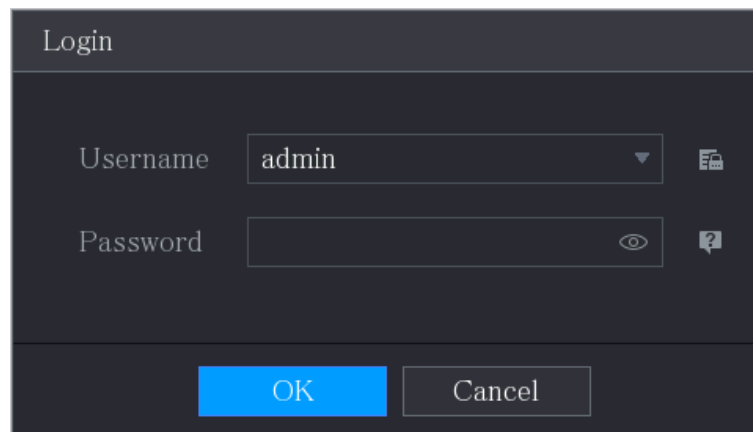


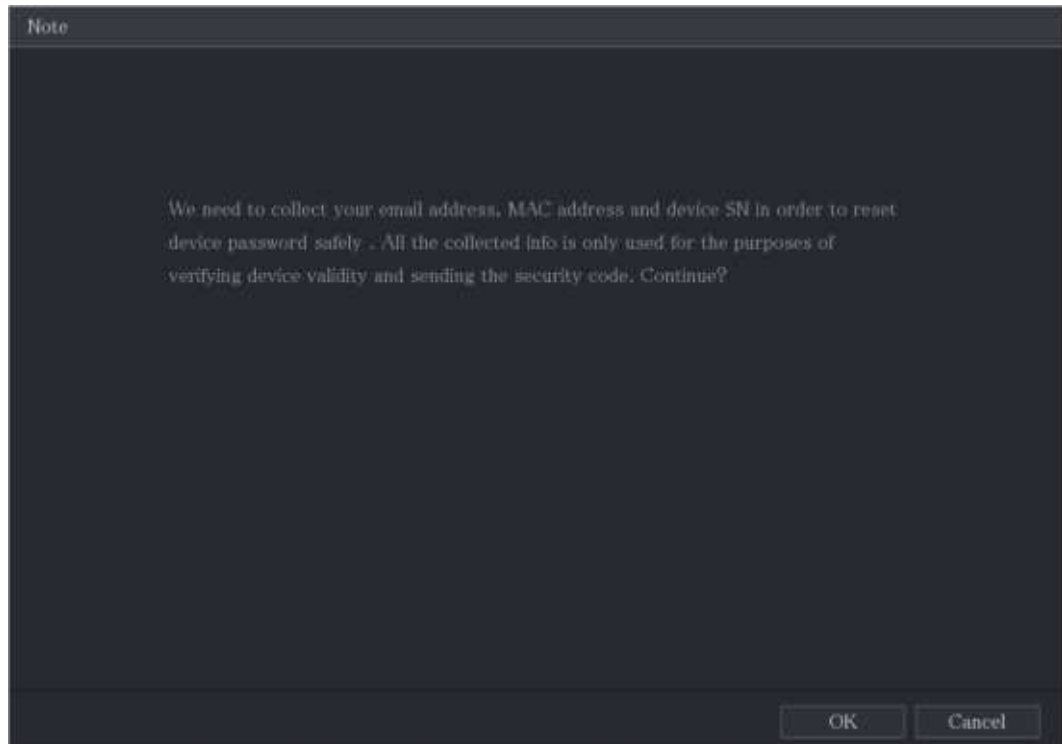
Figure 5-9



Step 2 Click .

- If you have set the reserved email address, the **Prompt** message interface is displayed.
- If you did not set the reserved email address, the email entering interface is displayed. See Step 3. Enter the email address, and then click **Next**, the **Prompt** message interface is displayed.

Figure 5-10



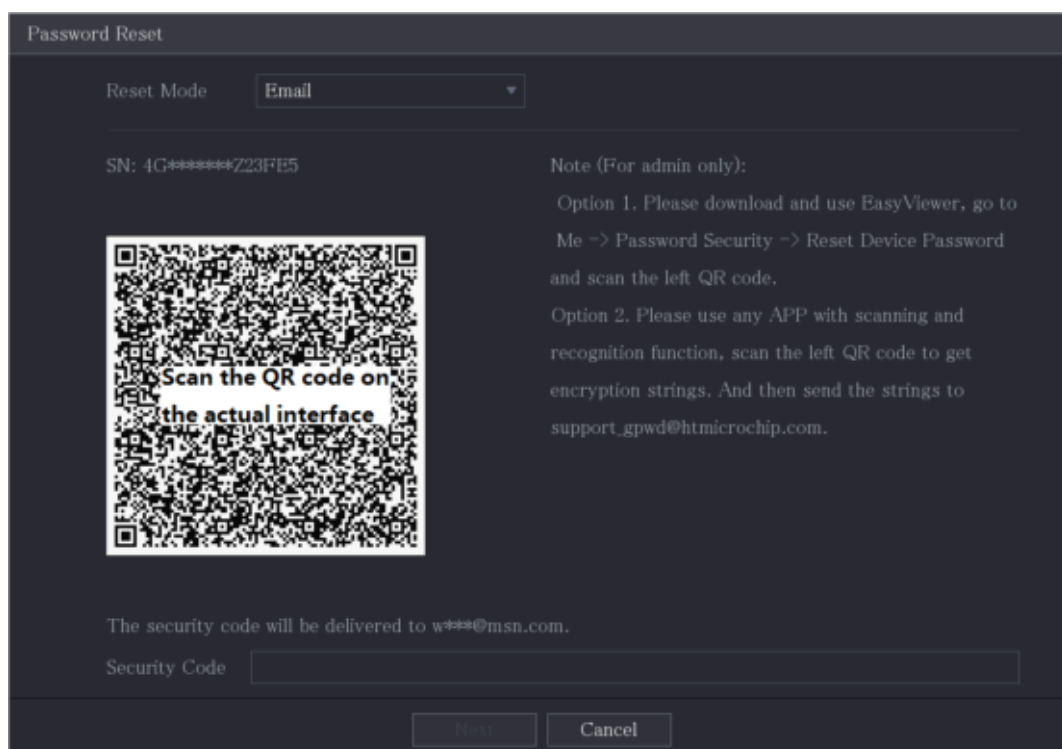
Step 3 Click **OK**.

The **Password Reset** interface is displayed.



After clicking **OK**, the system will collect your information for password reset, and the information includes but not limited to email address, MAC address, and device serial number. Read the prompt carefully before clicking **OK**.

Figure 5-11



Step 4 Reset the password.

- QR code

Follow the onscreen instructions to get the security code in your reserved email address. In the **Security code** box, enter the security code.



- You can get the security code twice by scanning the same QR code. If you need to get the security code once again, refresh the interface.
 - Use the security code received in your email box to reset the password within 24 hours; otherwise the security code becomes invalid.
- Security questions
- 1) On the **Reset password** interface as shown in Step 3, in the **Reset Type** list, select **Security Questions**, the Security Questions interface is displayed.



If you did not configure the security questions before, in the **Reset Type** list, there will be no **Security Questions**.

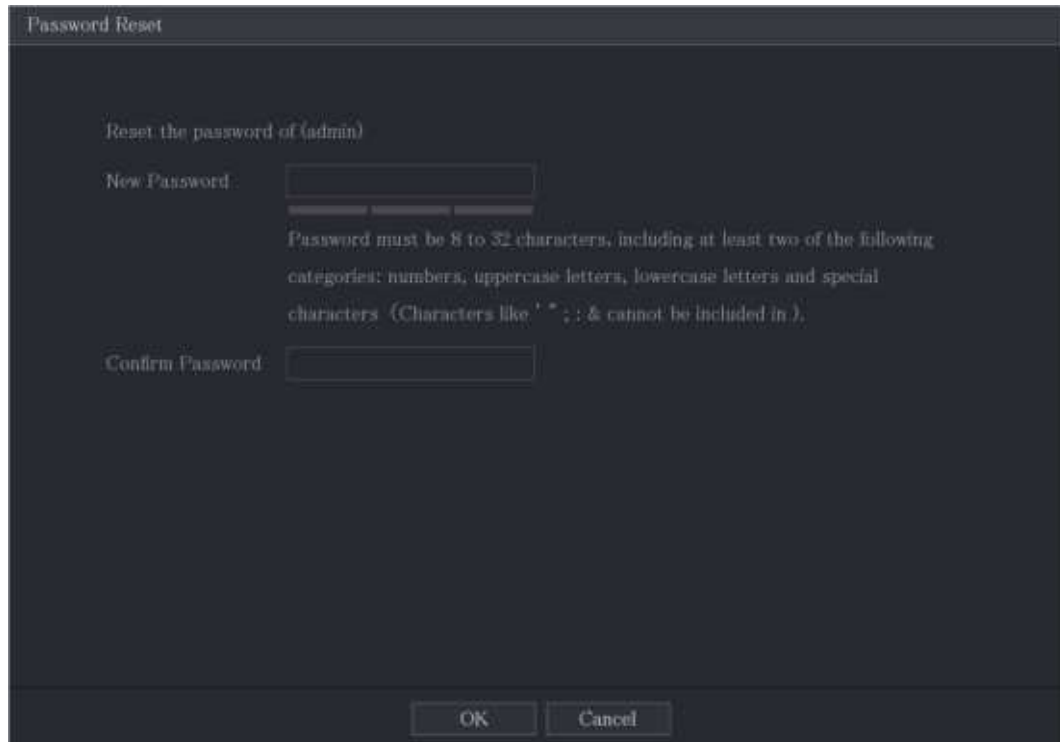
- 2) In the **Answer** box, enter the correct answers.

Figure 5-12

Step 5 Click **Next**.

The new password resetting interface is displayed.

Figure 5-13



The image shows a 'Password Reset' dialog box. At the top, it says 'Reset the password of (admin)'. Below this, there is a 'New Password' label followed by a text input field. Underneath the input field, a note specifies: 'Password must be 8 to 32 characters, including at least two of the following categories: numbers, uppercase letters, lowercase letters and special characters (Characters like ' * ; : & cannot be included in)'. Below the note is a 'Confirm Password' label followed by another text input field. At the bottom right of the dialog, there are two buttons: 'OK' and 'Cancel'.

Step 6 In the **New Password** box, enter the new password and enter it again in the **Confirm Password** box.

Step 7 Click **Save**. The password resetting is started.

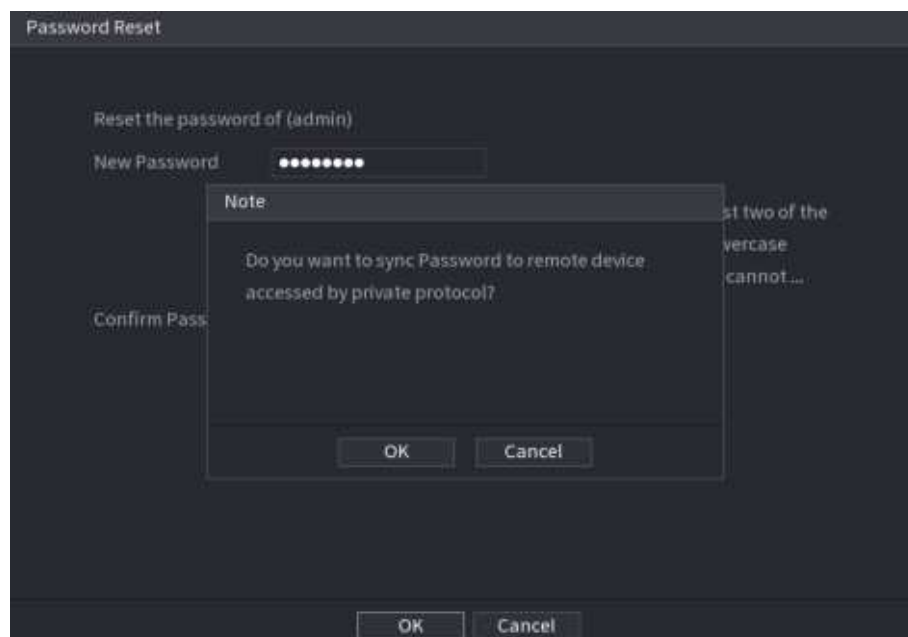
After resetting is completed, a pop-up message is displayed.

Step 8 Click **OK**.

A pop-up message is displayed asking if you want to sync the password with the remote devices, see Figure 5-14.

- Click **Cancel**, the resetting is finished.
- Click **OK**, the Sync Info interface is displayed.

Figure 5-14



The image shows the 'Password Reset' dialog box with a 'Note' pop-up window. The 'New Password' field is filled with dots. The 'Note' pop-up window has the title 'Note' and the text: 'Do you want to sync Password to remote device accessed by private protocol?'. It also has 'OK' and 'Cancel' buttons. The background dialog box is partially visible, showing the 'Confirm Password' label and the 'OK' and 'Cancel' buttons at the bottom.



This message appears only when there are digital channels instead of only analog channels.

Figure 5-15



5.1.3.3 Using Reset Button on the Mainboard

You can always use the reset button on the mainboard to reset the Device to the factory default.

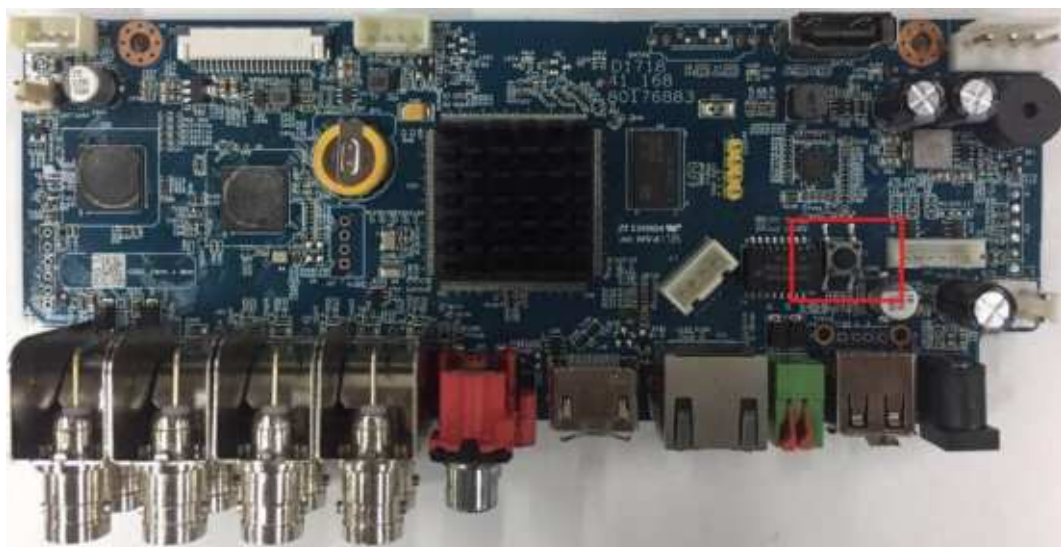


Not all models are provided with reset button.

Step 1 Disconnect the Device from power source, and then remove the cover panel. For details about removing the cover panel, see "2.2 Installing HDD."

Step 2 Find the reset button on the mainboard, and then press and hold the reset button for 5 seconds to 10 seconds. See Figure 5-16 for the location of the reset button.

Figure 5-16



Step 3 Reboot the Device.

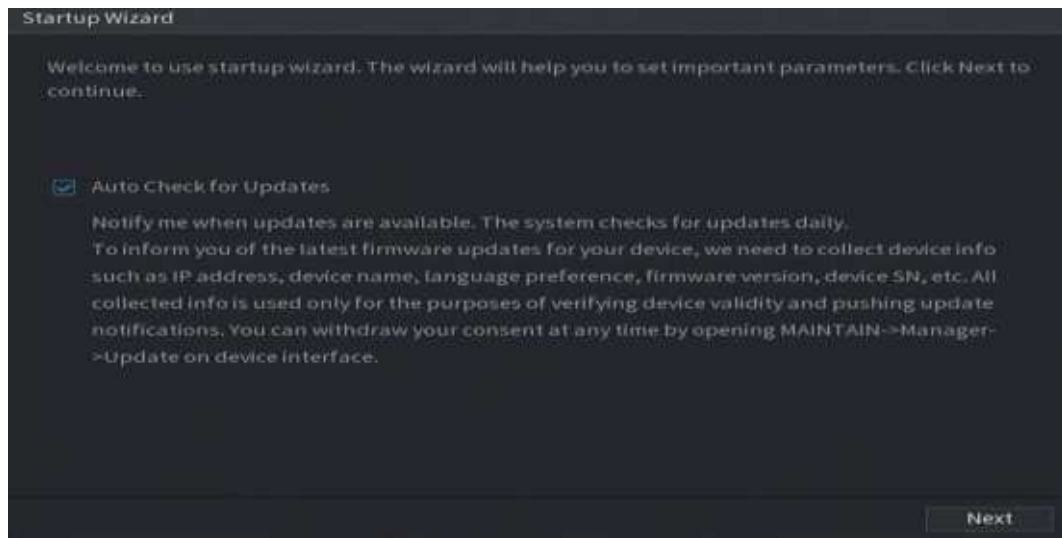
After the Device is rebooted, the settings have been restored to the factory default. You can start resetting the password.

5.1.4 Setting Up with the Startup Wizard

5.1.4.1 Entering Startup Wizard

The Startup Wizard helps you configure the basic settings to set up the Device. After you have initialized the Device, the **Startup Wizard** interface is displayed.

Figure 5-17



- If you select the **Auto-check for updates** check box, the system will notify you automatically when updates are available.
- After the auto-check function is enabled, to notify you to update timely, the system will collect the information such as IP address, device name, firmware version, and device serial number. The collected information is only used to verify the legality of the Device and push upgrade notices.
- If you clear the **Auto-check for updates** check box, the system will not perform automatic checks.

5.1.4.2 Configuring General Settings

You can configure the general settings for the Device such as Device name, language, and settings for instant playback.

You can also configure general settings by selecting **Main Menu > SYSTEM > General > Basic**.

Step 1 On the **Startup Wizard** interface, click **Next**.

The **Basic** interface is displayed.

Figure 5-18

The screenshot shows a 'Basic' settings window with the following parameters:

- Device Name: XVR
- Device No.: 8
- AI Mode: SMD
- Language: English
- Video Standard: PAL
- Instant Playback: 5 min.
- Logout Time: 10 min.
- Navigation Bar: ☐
- Mouse Sensitivity: A slider between 'Slow' and 'Fast'.
- Buttons: 'Previous' and 'Next' at the bottom right.
- Feature: 'Non-login User Permission' button next to Logout Time.

Step 2 Configure the basic settings parameters.

Table 5-3

Parameter	Description
Device Name	In the Device Name box, enter the Device name.
Device No.	In the Device No. box, enter a number for the Device.
AI Mode	Select SMD, Face or IVS&SMD for AI function in 5.11.2 For Lite AI Series. - When SMD is selected, only SMD is available. - When Face is selected, only face detection and face recognition are available. - When IVS&SMD is selected, only IVS and SMD are available.  This parameter is supported on select models. SMD, face detection, face recognition and IVS cannot be enabled simultaneously on those models.
Language	In the Language list, select a language for the Device system.
Video Standard	In the Video Standard list, select PAL or NTSC according to your actual situation.
Instant Playback	In the Instant Playback box, enter the time length for playing back the recorded video. The value ranges from 5 to 60. On the live view control bar, click the instant playback button to play back the recorded video within the configured time.
Logout Time	In the Logout Time box, enter the standby time for the Device. The Device automatically logs out when it is not working for the configured time period. You need to login the Device again.

Parameter	Description
	The value ranges from 0 to 60. 0 indicates there is not standby time for the Device. Click Monitor Channel(s) when logout . You can select the channels that you want to continue monitoring when you logged out.
Navigation Bar	Enable the navigation bar. When you click on the live view screen, the navigation bar is displayed.
Mouse Pointer Speed	Adjust the speed of double-click by moving the slider. The bigger the value is, the faster the double-clicking speed must be.

5.1.4.3 Configuring Date and Time Settings

You can configure the system time, choose the time zone, set the daylight saving time, and enable the NTP server.

You can also configure date and time settings by selecting **Main Menu > SYSTEM > General > Date & Time**.

Step 1 After you have configured the general settings, on the **General** interface, click **Next**.
The **Date & Time** interface is displayed.

Figure 5-19

Step 2 Configure the settings for date and time parameters.

Table 5-4

Parameter	Description
System Time	In the System Time box, enter time for the system. Click the time zone list, you can select a time zone for the system, and the time in adjust automatically.  Do not change the system time randomly; otherwise the recorded video cannot be searched. It is recommended to avoid the recoding period or stop recording first before you change the system time.
Time Zone	In the Time Zone list, select a time zone for the system.

Parameter	Description
Date Format	In the Date Format list, select a date format for the system.
Date Separator	In the Date Separator list, select a separator style for the date.
Time Format	In the Time Format list, select 12-HOUR or 24-HOUR for the time display style.
DST	Enable the Daylight Saving Time function. Click Week or click Date .
Start Time	Configure the start time and end time for the DST.
End Time	
NTP	Enable the NTP function to sync the Device time with the NTP server.  If NTP is enabled, device time will be automatically synchronized with server.
Server Address	In the Server Address box, enter the IP address or domain name of the corresponding NTP server. Click Manual Update , the Device starts syncing with the server immediately.
Port	The system supports TCP protocol only and the default setting is 123.
Interval	In the Interval box, enter the amount of time that you want the Device to sync time with the NTP server. The value ranges from 0 to 65535.

5.1.4.4 Configuring Network Settings

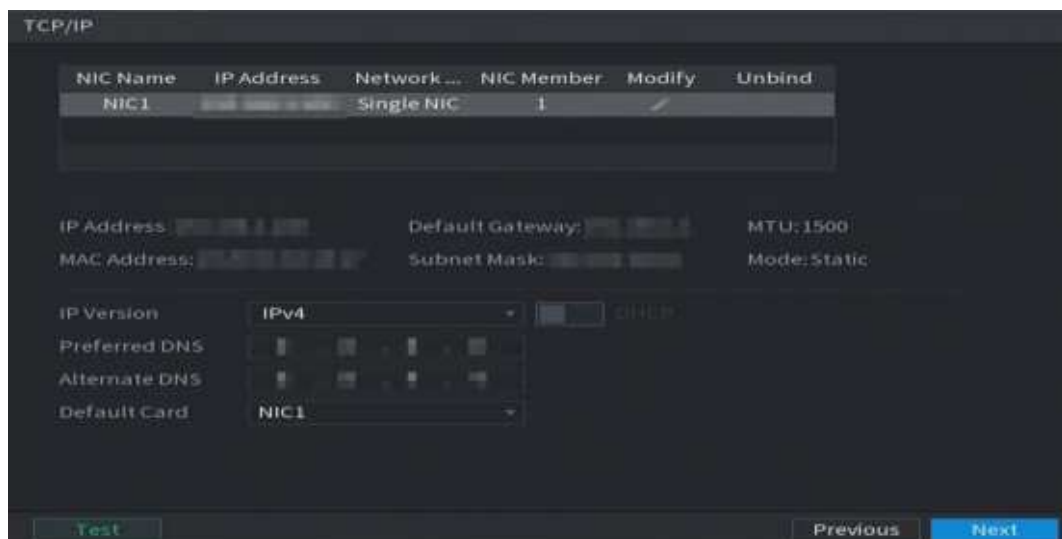
You can configure the basic network settings such as net mode, IP version, and IP address of the Device.

You can also configure network settings by selecting **Main Menu > NETWORK > TCP/IP**.

Step 1 After you have configured the date and time settings, on the **Date & Time** interface, click **Next**.

The **NETWORK** interface is displayed.

Figure 5-20



Step 2 Configure the settings for network parameters.

Table 5-5

Parameter	Description
IP Version	In the IP Version list, you can select IPv4 or IPv6 . Both versions are supported for access.
MAC Address	Displays the MAC address of the Device.
DHCP	Enable the DHCP function. The IP address, subnet mask and default gateway are not available for configuration once DHCP is enabled. • If DHCP is effective, the obtained information will display in the IP Address box, Subnet Mask box and Default Gateway box. If not, all values show 0.0.0.0. • If you want manually configure the IP information, disable the DHCP function first. • If PPPoE connection is successful, the IP address, subnet mask, default gateway, and DHCP are not available for configuration.
IP Address	Enter the IP address and configure the corresponding subnet mask and default gateway.  IP address and default gateway must be in the same network segment.
Subnet Mask	
Default Gateway	
DNS DHCP	Enable the DHCP function to get the DNS address from router.
Preferred DNS	In the Preferred DNS box, enter the IP address of DNS.
Alternate DNS	In the Alternate DNS box, enter the IP address of alternate DNS.
MTU	In the MTU box, enter a value for network card. The value ranges from 1280 byte through 1500 byte. The default is 1500. The suggested MTU values are as below. • 1500: The biggest value of Ethernet information package. This value is typically selected if there is no PPPoE or VPN connection, and it is also the default value of some routers, network adapters and switches. • 1492: Optimized value for PPPoE. • 1468: Optimized value for DHCP. • 1450: Optimized value for VPN.
Test	Click Test to test if the entered IP address and gateway are interworking.

5.1.4.5 Configuring P2P Settings

You can add the Device into your cell phone client or the platform to manage.

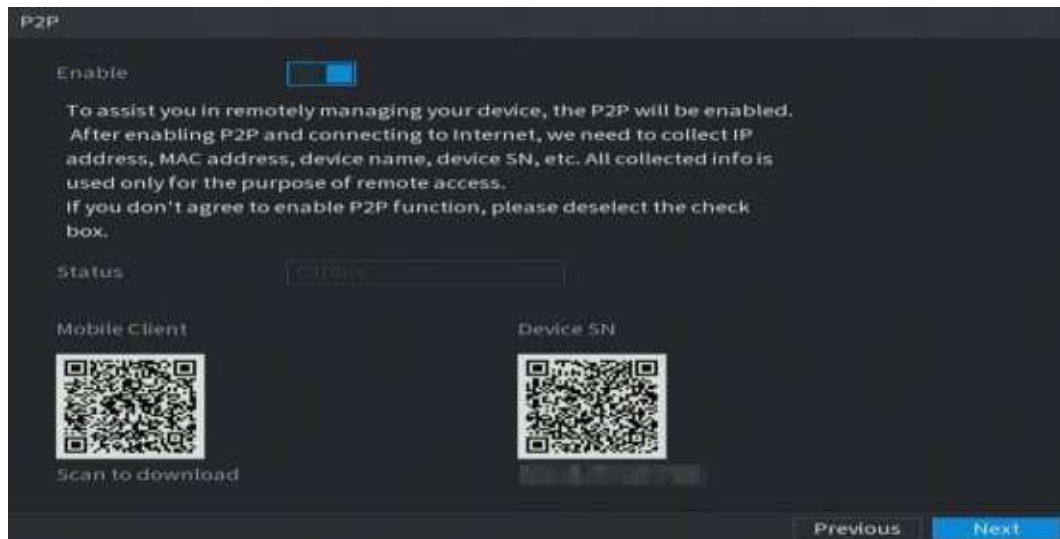
You can also configure P2P function by selecting **Main Menu > Network > P2P**.



Make sure the DVR is connected into the Internet, and if yes, in the **Status** box of the P2P interface, it shows **Online**.

Step 1 After you have configured the network settings, on the **Network** interface, click **Next**. The **P2P** interface is displayed.

Figure 5-21



Step 2 Enable the P2P function.



After the P2P function is enabled and connected to the Internet, the system will collect your information for remote access, and the information includes but not limited to email address, MAC address, and device serial number.

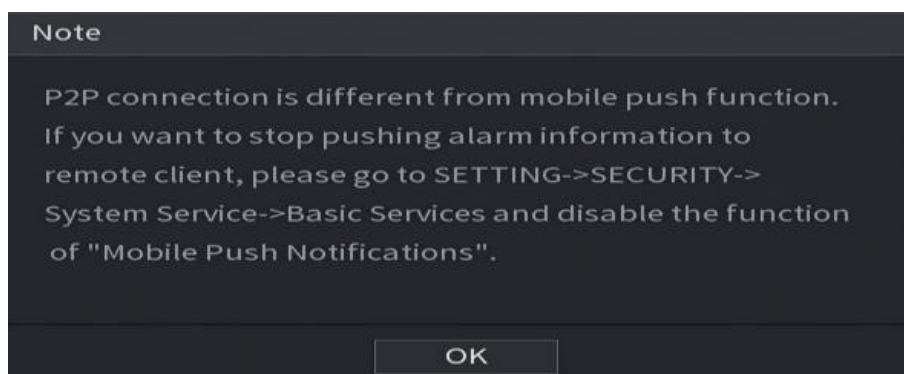
You can start adding the device.

- Cell Phone Client: Use your mobile phone to scan the QR code to add the device into the Cell Phone Client, and then you can start accessing the Device.
- Platform: Obtain the Device SN by scanning the QR code. Go to the P2P management platform and add the Device SN into the platform. Then you can access and manage the device in the WAN. For details, refer to the P2P operation manual.



- You can also enter the QR code of Cell Phone Client and Device SN by clicking  on the top right of the interfaces after you have entered the Main Menu.
- If selection of this function is canceled, the **Note** interface is displayed. See Figure 5-22. Choose to enable it or not according to your actual need.

Figure 5-22



To use this function, take adding device into Cell Phone Client as an example.

Adding Device into Cell Phone Client

Step 1 Use your cell phone to scan the QR code under Cell Phone Client to download the application.

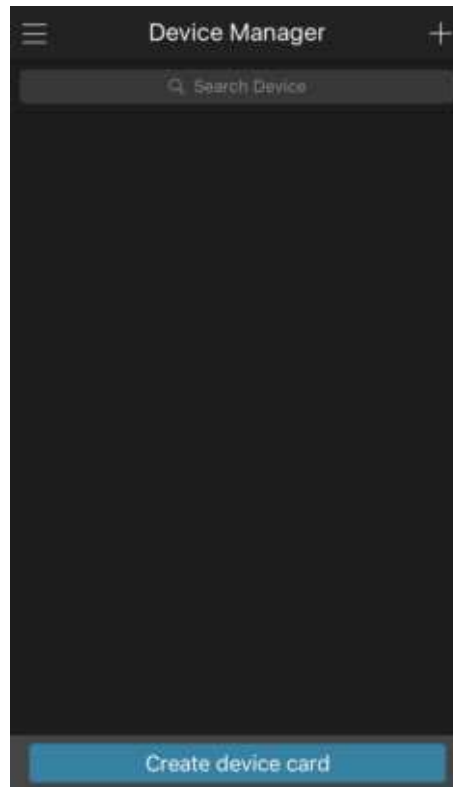
Step 2 On your cell phone, open the application, and then tap .

The menu is displayed. You can start adding the device.

1) Tap **Device Manager**.

The **Device Manager** interface is displayed.

Figure 5-23



2) Tap  on the top right corner.

The interface requiring device initialization is displayed. A pop-up message reminding you to make sure the Device is initialized is displayed.

3) Tap **OK**.

◇ If the Device has not been initialized, Tap **Device Initialization** to perform initializing by following the onscreen instructions.

◇ If the Device has been initialized, you can start adding it directly.

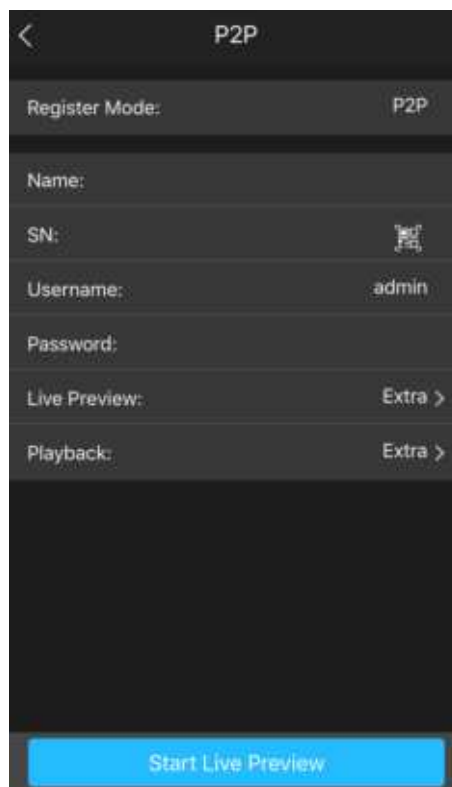
4) Tap **Add Device**.

The Add Device interface is displayed.



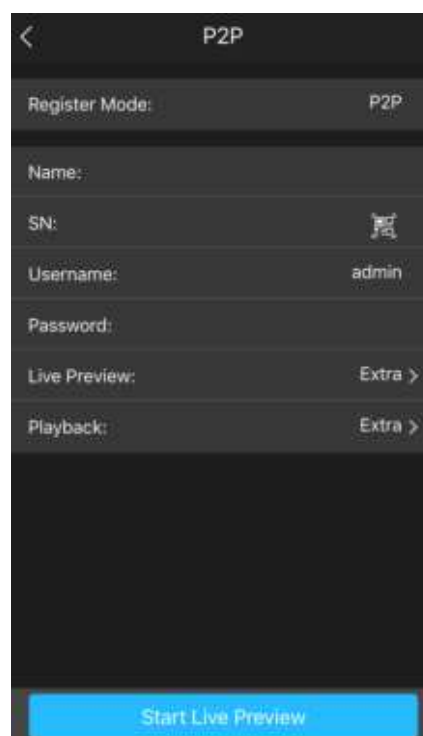
You can add wireless device or wired device. The Manual takes adding wired device as an example.

Figure 5-24



- 5) Tap **P2P**.
The **P2P** interface is displayed.

Figure 5-25



- 6) Enter a name for the DVR, the username and password, scan the QR code under **Device SN**.
7) Tap **Start Live Preview**.
The Device is added and displayed on the live view interface of the cell phone.

Figure 5-26



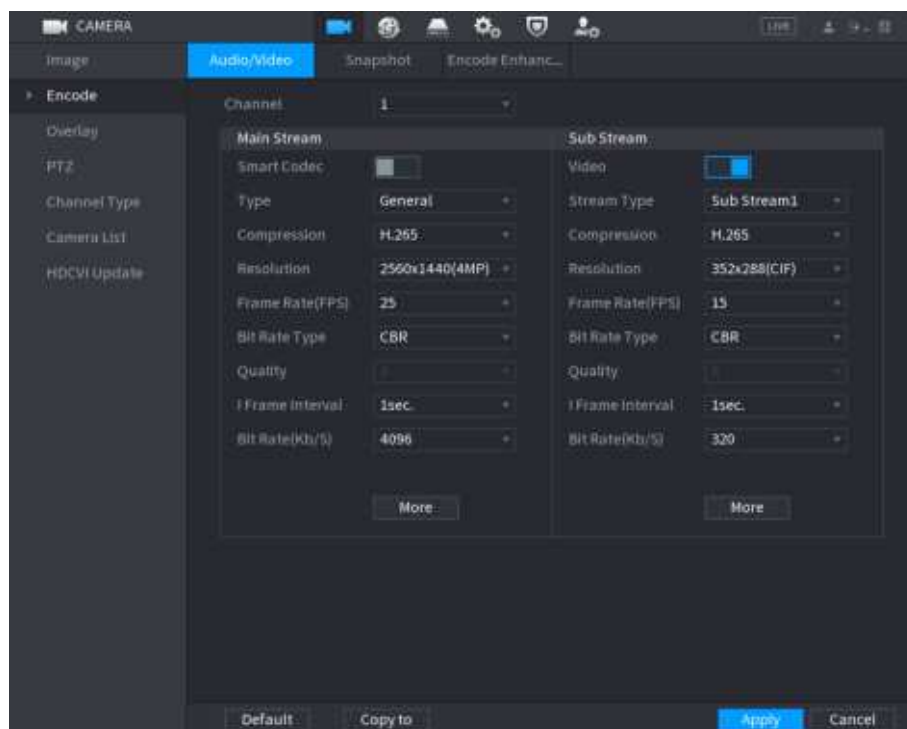
5.1.4.6 Configuring Encode Settings

You can configure the settings of main stream and sub stream for the Device.

You can also configure encode settings by selecting **Main Menu > CAMERA > Encode > Audio/Video**.

Step 1 After you have configured the P2P settings, on the **Audio/Video** interface, click **Next**.
The **Encode** interface is displayed.

Figure 5-27



Step 2 Configure the settings for the main/sub streams parameters. See Table 5-6.

Table 5-6

Parameter	Description
Channel	In the Channel list, select the channel that you want to configure the settings for.
Smart Codec	Enable the smart codec function. This function can reduce the video bit stream for non-important recorded video to maximize the storage space.
Type	• Main Stream: In the Type list, select General, MD (Motion Detect), or Alarm. • Sub Stream: This setting is not configurable.
Compression	In the Compression list, select the encode mode. • H.265: Main profile encoding. This setting is recommended. • H.264H: High profile encoding. Low bit stream with high definition. • H.264: Main profile encoding. • H.264B: Baseline profile encoding. This setting requires higher bit stream compared with other settings for the same definition.
Resolution	In the Resolution list, select resolution for the video. The maximum video resolution might be different dependent on your device model.
Frame Rate (FPS)	Configure the frames per second for the video. The higher the value is, the clearer and smoother the image will become. Frame rate changes along with the resolution. Generally, in PAL format, you can select the value from 1 through 25; in NTSC format, you can select the value from 1 through 30. However, the actual range of frame rate that you can select depends on the capability of the Device.
Bit Rate Type	In the Bit Rate Type list, select CBR (Constant Bit Rate) or VBR (Variable Bit Rate). If you select CBR , the image quality cannot be configured; if you select VBR , the image quality can be configured.
Quality	This function is available if you select VBR in the Bit Rate List. The bigger the value is, the better the image will become.
I Frame Interval	The interval between two reference frames.
Bit Rate (Kb/S)	In the Bit Rate list, select a value or enter a customized value to change the image quality. The bigger the value is, the better the image will become.
Video	Enable the function for sub stream.
Audio	Click More, the More interface is displayed. • Audio: This function is enabled by default for main stream. You need to manually enable it for sub stream 1. Once this function is enabled, the recorded video file is composite audio and video stream. • Audio Source: In the Audio Source list, you can select Local and HDCVI. ◇ Local: The audio signal is input from Audio In port. ◇ HDCVI: The audio signal is input from HDCVI camera.
Audio Source	
Compression	

Parameter	Description
	Compression: In the Compression list, select a format that you need.

5.1.4.7 Configuring Snapshot Settings

You can configure the basic snapshot settings such as quantity of snapshot each time, channel(s) to take snapshot, and image size and quality of snapshot.

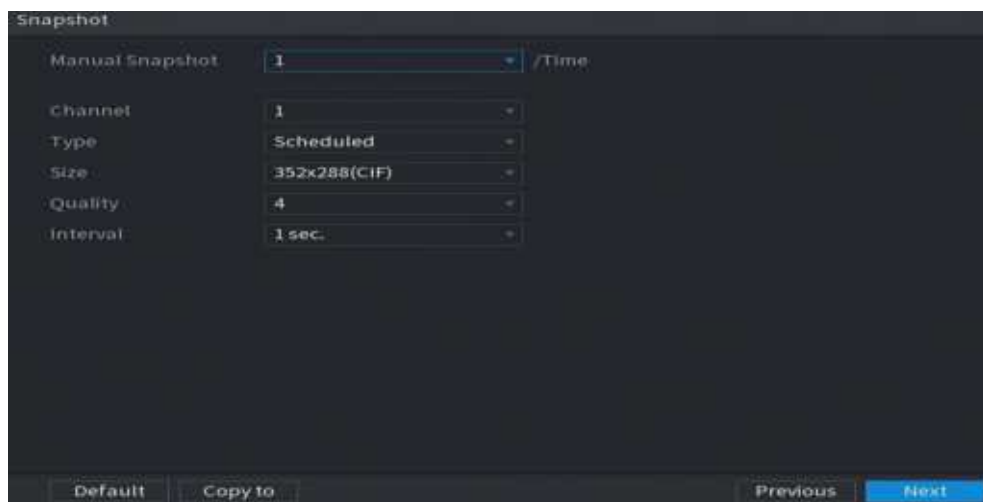
You can also configure general settings by selecting **Main Menu > CAMERA > Encode > Snapshot**.

For more information about snapshot settings, see "5.8 Configuring Snapshot Settings."

Step 1 After you have configured the encode settings, on the **Encode** interface, click **Next**.

The **Snapshot** interface is displayed.

Figure 5-28



Step 2 Configure the settings for the snapshot parameters. See Table 5-7.

Table 5-7

Parameter	Description
Manual Snapshot	In the Manual Snapshot list, select how many snapshots you want to take each time.
Channel	In the Channel list, select the channel that you want to configure the settings for.
Type	In the Mode list, you can select Human Face, Event, or General as the event type for which you want to take a snapshot. Scheduled: The snapshot is taken during the scheduled period. Event: The snapshot is taken when there is an alarm event occurs, such as motion detection event, video loss, and local alarms. Face Snapshot: The snapshot is taken when the face is detected. The face detection function is support only with the Channel 1.
Size	In the Size list, select a value for the image. The bigger the value is, the better the image will become.

Parameter	Description
Quality	Configure the image quality by 6 levels. The higher the level is, the better the image will become.
Interval	Configure or customize the snapshot frequency.

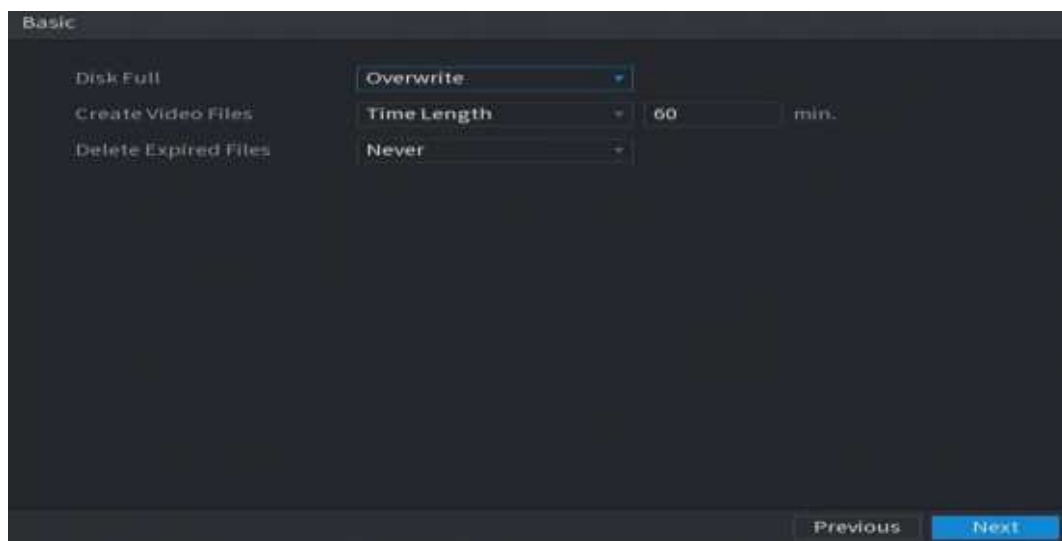
5.1.4.8 Configuring Basic Storage Settings

You can configure the settings for the situations when HDD is full, file length and time length of recorded video, and the settings if to auto-delete the old files.

You can also configure basic storage settings by selecting **Main Menu > STORAGE > Basic**.

Step 1 After you have configured the encode settings, on the **Snapshot** interface, click **Next**. The **Basic** interface is displayed.

Figure 5-29



Step 2 Configure the basic storage settings parameters.

Table 5-8

Parameter	Description
Disk Full	Configure the settings for the situation when all the read/write discs are full, and there are no more free discs. • Select Stop to stop recording • Select Overwrite to overwrite the recorded video files always from the earliest time.  The locked recorded video files will not be overwritten.
Create Video Files	Configure the time length and file length for each recorded video.
Delete Expired Files	Configure whether to delete the old files and if yes, in the Delete Expired Files list, select Custom to configure the time length for how long you want to keep the old files.

5.1.4.9 Configuring Recorded Video Storage Schedule

You can configure the schedule for the recorded video such as channels to record, alarm settings, and the armed period.

You can also configure recorded video storage settings by selecting **Main Menu > STORAGE > Schedule > Record**.

Step 1 After you have configured the basic storage settings, on the **Basic** interface, click **Next**. The **Record** interface is displayed.

Figure 5-30



Step 2 Configure the record settings parameters.

Table 5-9

Parameter	Description
Channel	In the Channel list, select a channel to record the video.
Pre-record	In the Pre-record list, enter the amount of time that you want to start the recording in advance.
Redundancy	If there are several HDDs installed to the Device, you can set one of the HDDs as the redundant HDD to save the recorded files into different HDDs. In case one of the HDDs is damaged, you can find the backup in the other HDD. • Select Main Menu > STORAGE > Disk Manager, and then set a HDD as redundant HDD. • Select Main Menu > STORAGE > Schedule > Record, and then select the Redundancy check box. ◇ If the selected channel is not recording, the redundancy function takes effect next time you record no matter you select the check box or not. ◇ If the selected channel is recording, the current recorded files will be packed, and then start recording according to the new schedule.  • Not all models support this function. • The redundant HDD only back up the recorded videos but not snapshots.

Parameter	Description
Event type	Select the check box of the event type which includes General , Motion (motion detect, video loss, tempering, diagnosis), Alarm (IoT alarms, local alarms, alarms from alarm box, IPC external alarms, IPC Offline alarms), M&A , Intelligent (IVS events, face detection), and POS .
Period	Define a period during which the configured recording setting is active.  The system only activates the alarm in the defined period.
Copy	Click Copy to to copy the settings to other channels.

Step 3 Define the video recording period by drawing or editing. By default, it is active all the time.

- Define the period by drawing.
- 1) Select the check box of event type.

Figure 5-31



- 2) Define a period. The system supports maximum six periods.
 - ◇ Define for the whole week: Click  next to **All**, all the icon switches to , you can define the period for all the days simultaneously.
 - ◇ Define for several days of a week: Click  before each day one by one, the icon switches to . You can define the period for the selected days simultaneously.
- 3) On the timeline, drag to define a period. The Device starts recoding the selected event type in the defined period.

Figure 5-32



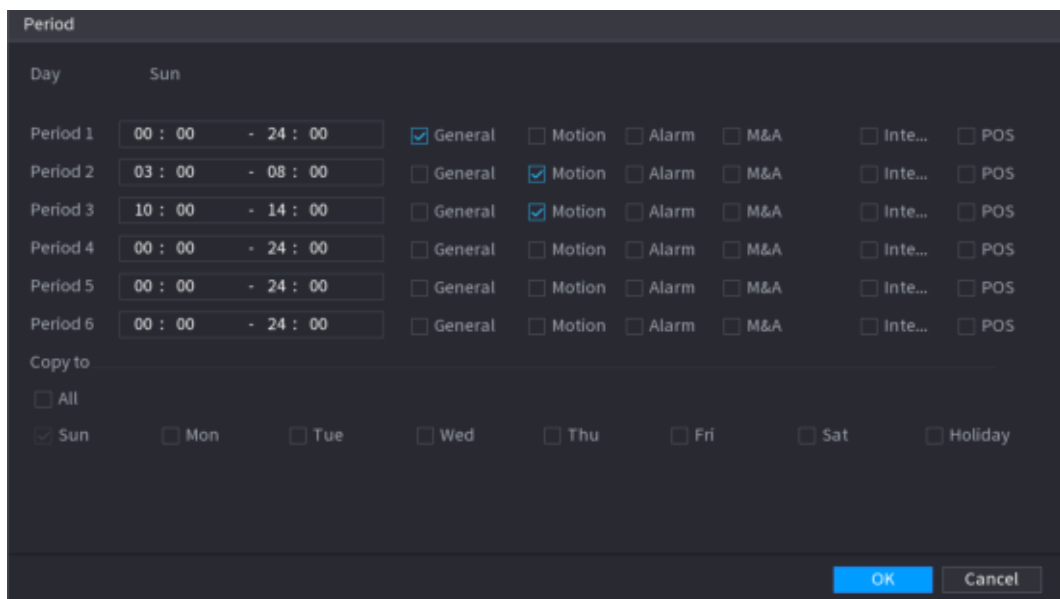
The color bar indicates the event type that is effective in a defined period:



- Recording priority in case of event types are overlapped: **M&A > Alarm > Intelligent > Motion > General**.
 - Select the check box of event type, and then click  to clear the defined period.
 - When selecting MD&Alarm, the MD and Alarm check boxes will be cleared respectively.
 - Define the period by editing. Take Sunday as an example.
- 4) Click .

The **Period** interface is displayed.

Figure 5-33



Day	Sun
Period 1	00 : 00 - 24 : 00 ☒ General ☐ Motion ☐ Alarm ☐ M&A ☐ Inte... ☐ POS
Period 2	03 : 00 - 08 : 00 ☐ General ☒ Motion ☐ Alarm ☐ M&A ☐ Inte... ☐ POS
Period 3	10 : 00 - 14 : 00 ☐ General ☒ Motion ☐ Alarm ☐ M&A ☐ Inte... ☐ POS
Period 4	00 : 00 - 24 : 00 ☐ General ☐ Motion ☐ Alarm ☐ M&A ☐ Inte... ☐ POS
Period 5	00 : 00 - 24 : 00 ☐ General ☐ Motion ☐ Alarm ☐ M&A ☐ Inte... ☐ POS
Period 6	00 : 00 - 24 : 00 ☐ General ☐ Motion ☐ Alarm ☐ M&A ☐ Inte... ☐ POS

Copy to

☐ All

☒ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat ☐ Holiday

OK Cancel

- 5) Enter the time frame for the period and select the event check box.
- ◇ There are six periods for you to set for each day.
 - ◇ Under **Copy to**, select **All** to apply the settings to all the days of a week, or select specific day(s) that you want to apply the settings to.
- 6) Click **OK** to save the settings.

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



- Click **Copy** to copy the settings to other channels.
- After configuring the recording schedule settings, you need to perform the following operations to start recording according to the defined schedule.
 - ◇ Enable the alarm event and configure the settings for the recording channel. For details, see "5.10 Alarm Events Settings."
 - ◇ You need to enable the recording function, see "5.9.1 Enabling Record Control."

5.1.4.10 Configuring Snapshot Storage Schedule

You can configure the storage schedule for the snapshot such as channels to take snapshot, alarm settings, and the armed period.

You can also configure snapshot storage settings by selecting **Main Menu > STORAGE > Schedule > Snapshot**.

Step 1 After you have configured the video recording settings, on the **Record** interface, click **Next**.

The **Snapshot** interface is displayed.

Figure 5-34



Step 2 Configure the snapshot settings parameters.

Table 5-10

Parameter	Description
Channel	In the Channel list, select a channel to take a snapshot.
Event type	Select the check box of the event type which includes General , Motion , Alarm , M&A , Intelligent , and POS .
Period	Define a period during which the configured snapshot setting is active. For details about defining a period, see "5.1.4.9 Configuring Recorded Video Storage Schedule."
Copy	Click Copy to to copy the settings to other channels.

Step 3 Click **OK**.

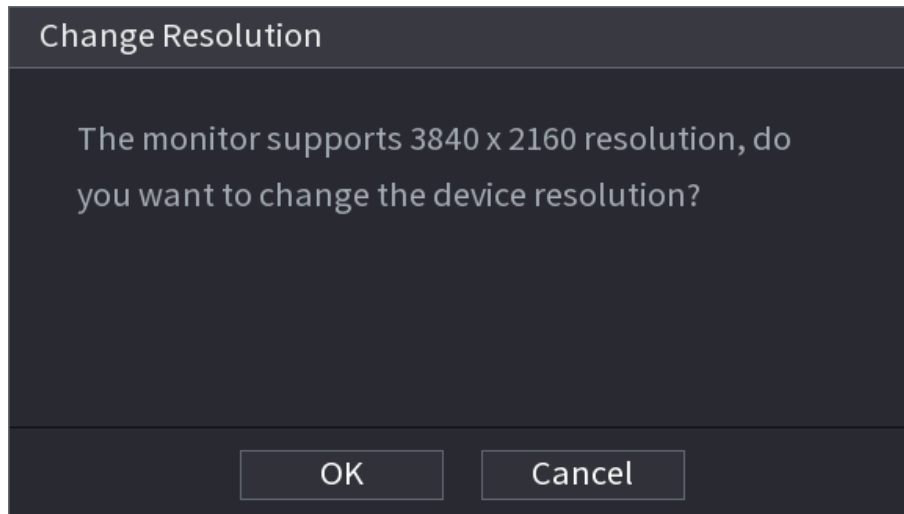
A pop-up message is displayed.

Step 4 Click **OK**.

The live view screen is displayed. The setting up with startup wizard is completed. You can start using the Device.

Step 5 (Optional) After the setting with startup wizard is completed, if the connected HDMI display resolution is inconsistent with default resolution (1280*1024), a dialog box will pop up. Choose to switch the resolution or not.

Figure 5-35



5.2 Live View

After you logged in the Device, the live view is displayed. The number of channels displayed depends on your model.

To enter the live view screen from other interfaces, click  on the top right of the screen.

Figure 5-36



5.2.1 Live View Screen

You can view the live video from the connected cameras through each channel on the screen.

- By default, the system time, channel name and channel number are displayed on each channel window. This setting can be configured by selecting **Main Menu > CAMERA > Overlay > Overlay**.

- The figure in the bottom right corner represents channel number. If the channel position is changed or the channel name is modified, you can recognize the channel number by this figure and then perform the operations such as record query and playback.

For the icons displayed on each channel, see Table 5-11.

Table 5-11

Icon	Function
	Indicates recording status. This icon displays when the video is being recorded.
	This icon displays when the motion detection occurs in the scene.
	This icon displays when the video loss is detected.
	This icon displays when the channel monitoring is locked.

TIPS

To switch the position of two channels, point to one of the two channels, and then drag the window to the other channel.

5.2.2 Live View Control bar

The live view control bar provides you access to perform the operations such as playback, zoom, real-time backup, manual snapshot, voice talk, adding remote devices, and streams switch.

When you move the pointer to the top middle position of a channel window, the live view control bar is displayed. See Figure 5-37 for analog channel and Figure 5-38 for digital channel.



If there is not operation for six seconds after the control bar is displayed, the control bar hides automatically.

Figure 5-37



Figure 5-38



Table 5-12

No.	Function	No.	Function	No.	Function
1	Instant Playback	4	Manual Snapshot	7	Camera Registration
2	Digital Zoom	5	Mute	/	/
3	Instant Record	6	Audio Talk	/	/

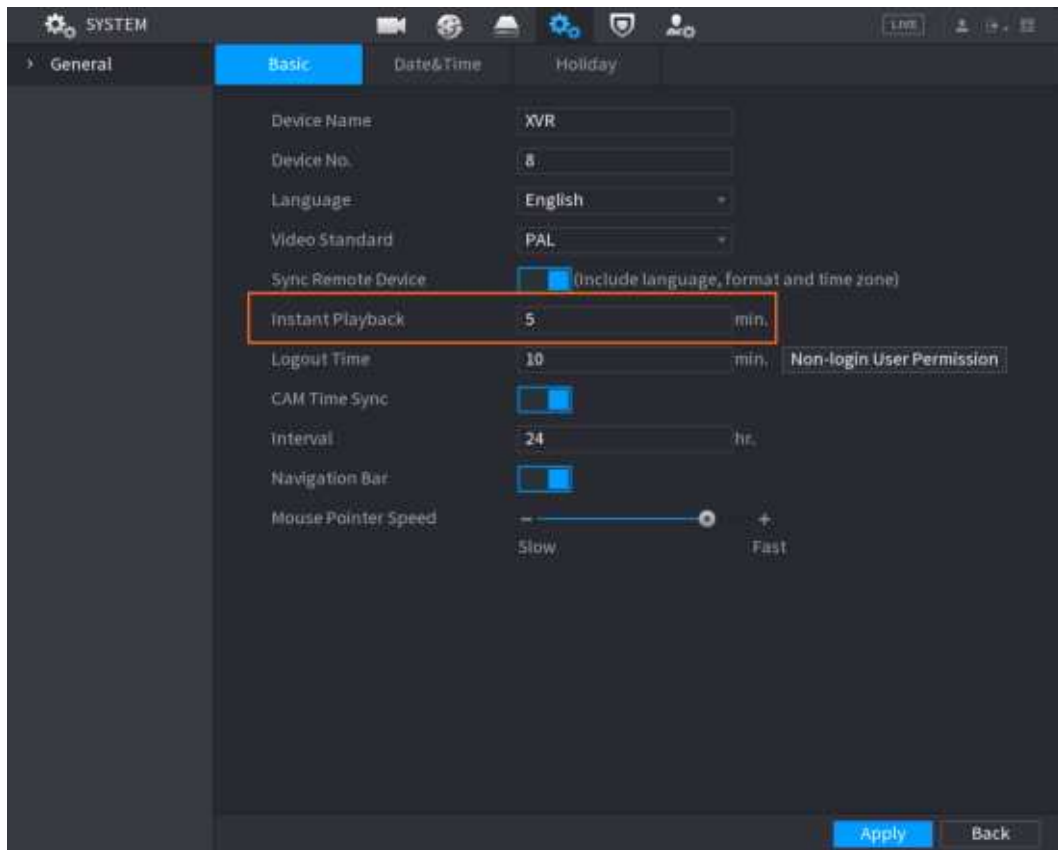
5.2.2.1 Instant Playback

You can play back the previous five minutes to sixty minutes of the recorded video.

By clicking , the instant playback interface is displayed. The instant playback has the following features:

- Move the slider to choose the time you want to start playing.
- Play, pause and close playback.
- The information such as channel name and recording status icon are shielded during instant playback and will not display until exited.
- During playback, screen split layout switch is not allowed.
- To change the playback time, select **Main Menu > SYSTEM > General > Basic**, in the **Instant Play** box, enter the time you want to play back.

Figure 5-39



5.2.2.2 Digital Zoom

You can enlarge a specific area of the image to view the details by either of the following two ways.

- Click , the icon switches to . Hold down the left mouse button to select the area you want to enlarge. The area is enlarged after the left mouse button is released.
 - Point to the center that you want to enlarge, rotate the wheel button to enlarge the area.
- 
- For some models, when the image is enlarged in the first way described previously, the selected area is zoomed proportionally according to the window.
 - When the image is in the enlarged status, you can drag the image toward any direction to view the other enlarged areas.
 - Right-click on the enlarged image to return the original status.

5.2.2.3 Instant Record

You can record the video of any channel and save the clip into a USB storage device.

By clicking , the recording is started. To stop recording, click this icon again. The clip is automatically saved into the connected USB storage device.

5.2.2.4 Manual Snapshot

You can take one to five snapshots of the video and save into a USB storage device.

By clicking , you can take snapshots. The snapshots are automatically saved into the connected USB storage device. You can view the snapshots on your PC.



To change the quantity of snapshots, select **Main Menu > CAMERA > ENCODE > Snapshot**, in the **Manual Snap** list, select the snapshot quantity.

5.2.2.5 Mute (Analog channel only)

You can mute the video sound by clicking . This function is supported in single-channel view.

5.2.2.6 White Light (Supported on camera with white light function)

Click  to manually control the camera to turn on the white light function.

5.2.2.7 Siren (Supported on camera with siren function)

Click  to manually control the camera to generate alarm sound.

5.2.2.8 Two-way Talk (Digital channel only)

You can perform the voice interaction between the Device and the remote device to improve efficiency of emergency. This function is supported only when the remotely connected IPC device supports bidirectional talk.

- Click , the icon switches to , the bidirectional talk of the remote device is turned on. The bidirectional talk of other digital channels is disabled.
- Click  to cancel the bidirectional talk. The bidirectional talk of other digital channels is resumed.

5.2.2.9 Adding Camera (Digital channel only)

You can view the information of remote devices and add new remote devices to replace the current connected devices.

By clicking , the **Camera List** interface is displayed. For details about adding the remote devices, see "5.6 Configuring Remote Devices."

5.2.3 Navigation Bar

You can access the functions to perform operations through the function icons on the navigation bar. For example, you can access Main Menu and switch window split mode.



The navigation bar is disabled by default. It does not appear in the live view screen until it is enabled. To enable it, select **Main Menu > SYSTEM > General > Basic**, enable the Navigation Bar, and then click **Apply**.

Figure 5-40



Table 5-13

Icon	Function
	Open Main Menu .
	Expand or condense the navigation bar.
	Select view layout.
	Go to the previous screen.
	Go to the next screen.
	Enable tour function. The icon switches to
	Open the PTZ control panel. For details, see "5.4 Controlling PTZ Cameras."
	Open the Image interface. This function is supported only in single-channel layout.
	Open the record search interface. For detail, see "5.9 Playing Back Video."
	Open the Alarm Status interface to view the device alarm status. For details, see "5.21.3 Viewing Event Information."
	Open the CHANNEL INFO interface to display the information of each channel.
	Open the Camera List interface. For details, see "5.6.1 Adding Remote Devices."
	Open the Network interface. For details, see "5.15.1 Configuring Network Settings."
	Open the Disk Manager interface. For details, see "5.18.3 Configuring Disk Manager."

Icon	Function
	Open the USB Management interface. For details about USB operations, see "5.14.2 Backing up Files", "5.21.2 Viewing Log Information", "5.20.4 Exporting and Importing System Settings", "5.20.6 Updating the Device."

5.2.4 Shortcut Menu

You can quickly access some function interfaces such as main menu, record search, PTZ setting, color setting and select the view split mode.

Right-click on the live view screen, the shortcut menu is displayed. For details about the functions of shortcut menu, see Table 5-14.



After you access any interface through shortcut menu, you can return to the previous screen by right-clicking on the current screen.

Figure 5-41

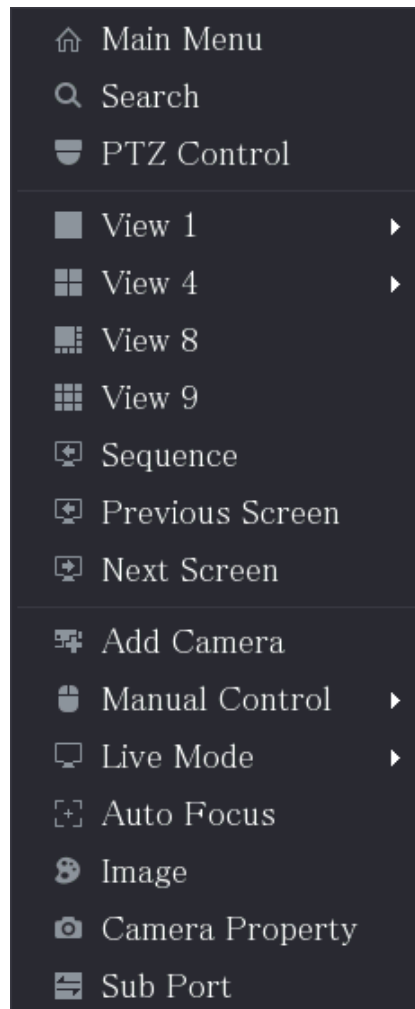


Table 5-14

Function	Description
Main Menu	Open Main Menu interface.

Function	Description
Search	Open the PLAYBACK interface where you can search and play back record files.
PTZ	Open the PTZ interface.
View Layout	Configure the live view screen as a single-channel layout or multi-channel layout.
Previous Screen	Click Previous Screen to go to the previous screen. For example, if you are using 4-split mode, the first screen is displaying the channel 1-4, click Next screen , you can view channel 5-8.
Next Screen	
Add Camera	Open the Camera List interface. For details, see "5.6 Configuring Remote Devices."  This parameter displays on the right-click menu only after setting at least one channel to IP type in Main Menu > CAMERA > Channel Type.
Manual Control	• Select Record Mode, you can configure the recording mode as Auto or Manual, or stop the recording. You can also enable or disable snapshot function • Select Alarm Mode, you can configure alarm output settings.
Live Mode	• Select General, the layout of live view screen is as default. • Select Face, the detected face snapshots are displayed in the bottom of the live view screen.
Auto Focus	Point to the channel window and right-click on it to open the shortcut menu, and then click Auto Focus.  Not all cameras support this function.
Image	Open the Image interface where you can adjust the video image color.
Camera Property	Click to modify the camera properties.
Sub Port	Click to switch to extra screen control.

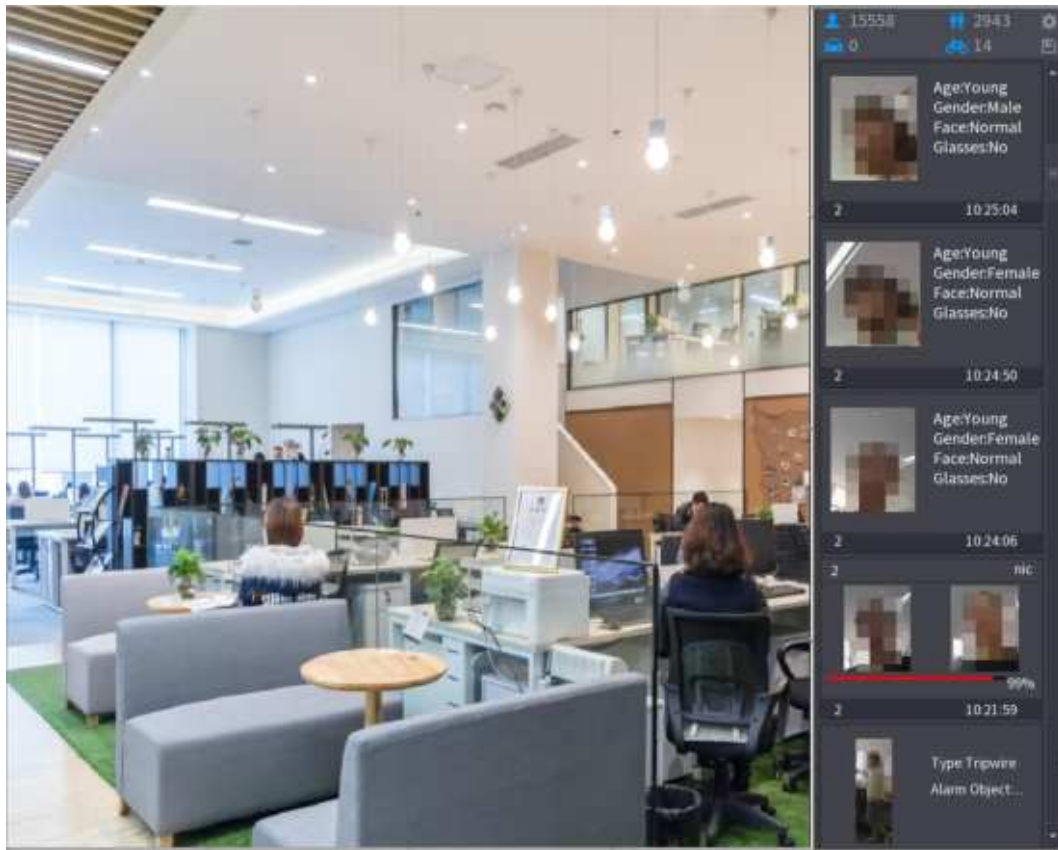
5.2.5 AI Preview Mode

You can view the detected faces snapshots and comparison results of detected faces and the faces in the library, and play back the recorded picture file.

To display the AI preview mode, the face detection function must be enabled. For details, see "5.11.1.1 Face Detection."

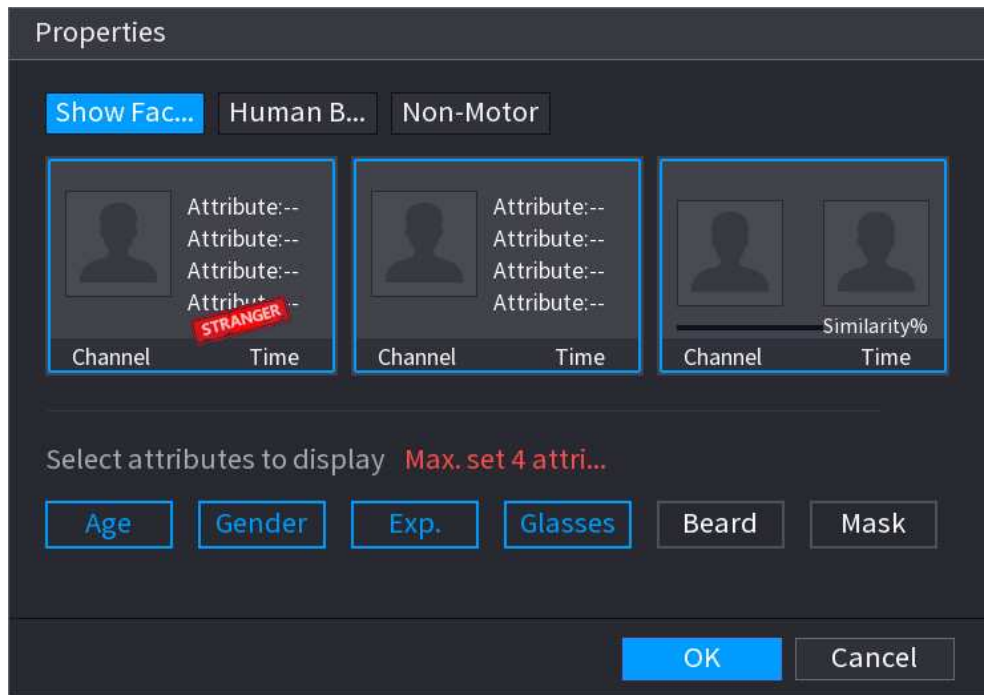
Right-click on the live view screen to display the shortcut menu, and then select **Live Mode > AI Mode**, the AI preview mode interface is displayed.

Figure 5-42



-  **15558**: Indicates the quantity of detected faces from 0 A.M. to midnight.
-  **2943**: Indicates the quantity of detected humans 0 A.M. to midnight.
-  **0**: Indicates the quantity of detected motor vehicles 0 A.M. to midnight.
-  **14**: Indicates the quantity of detected non-motor vehicles 0 A.M. to midnight.
- : Click this icon and then select the face attributes that you want to display on the AI preview mode. Maximum four attributes are supported to display. See Figure 5-43.
- : Click this icon to export counting report in .csv format. The report information includes date, starting time, ending time, and the number of human, vehicle and face. The title of report is named as "device name_ XVR_AI_Statistics_starting time_ending time.csv".

Figure 5-43



5.2.6 Channel Sequence

You can adjust the channel sequence displayed on live interface on actual needs.



The live view interface displays the default channel sequence after restoring factory defaults.

Step 1 Right-click on the live view interface and select **Sequence**.

The **Sequence** interface is displayed.



- The system displays the maximum number of window splits supported by the DVR after **selecting** Sequence.
- The Sequence interface displays only the channel name and channel number of added remote devices.  represents the remote device is online, and  represents the remote device is offline.

Figure 5-44 Sequence

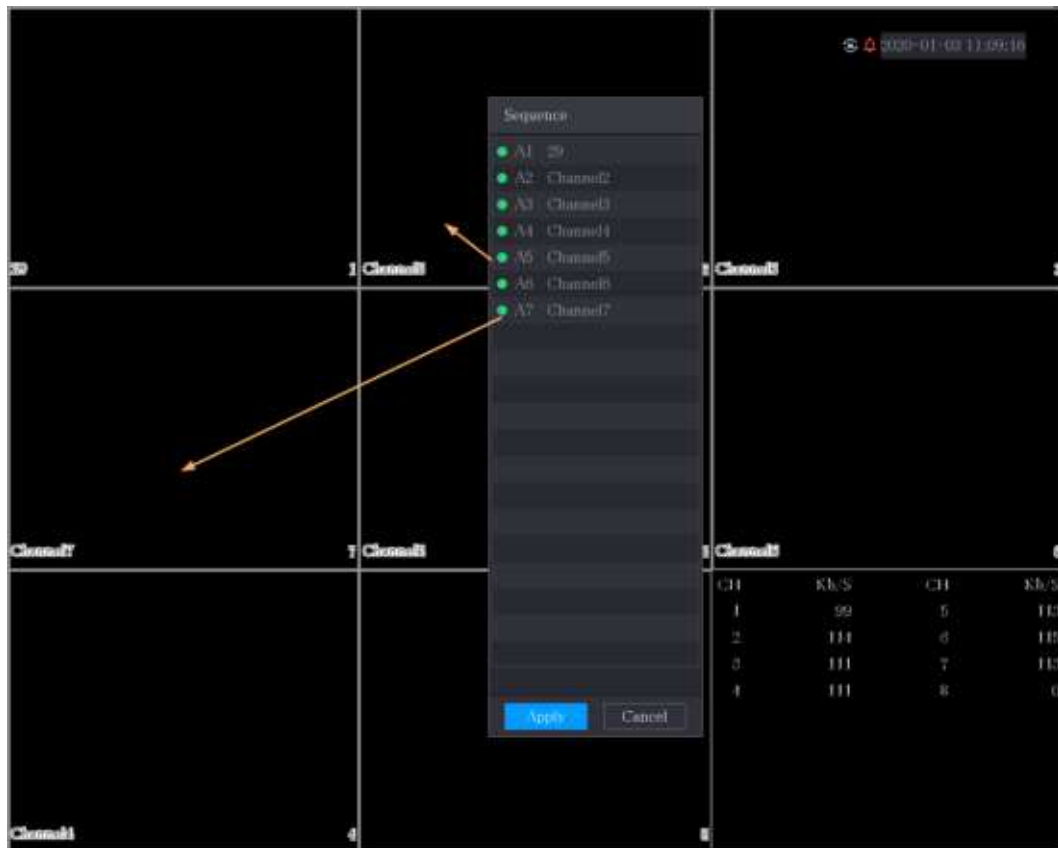
[illegible]

Step 2 Adjust channel sequence.

- Drag a channel to the target window split.
- Drag a window split to another to change the sequence.

You can view the channel sequence according to the channel number on the lower-right corner of the window split.

Figure 5-45 Adjusted Sequence



5.2.7 Color Setting

You can adjust the video image color effect such as sharpness, brightness, and contrast. The parameters are different according to the connected camera type. Take analog channel as an example.



Parameters displayed on the interface vary from different cameras, the actual interface shall prevail.

In the live view screen, right-click on the analog channel to see the shortcut menu, and then select **Image**, the **Image** interface is displayed.

For details, see "5.5.1 Configuring Image Settings."

Figure 5-46

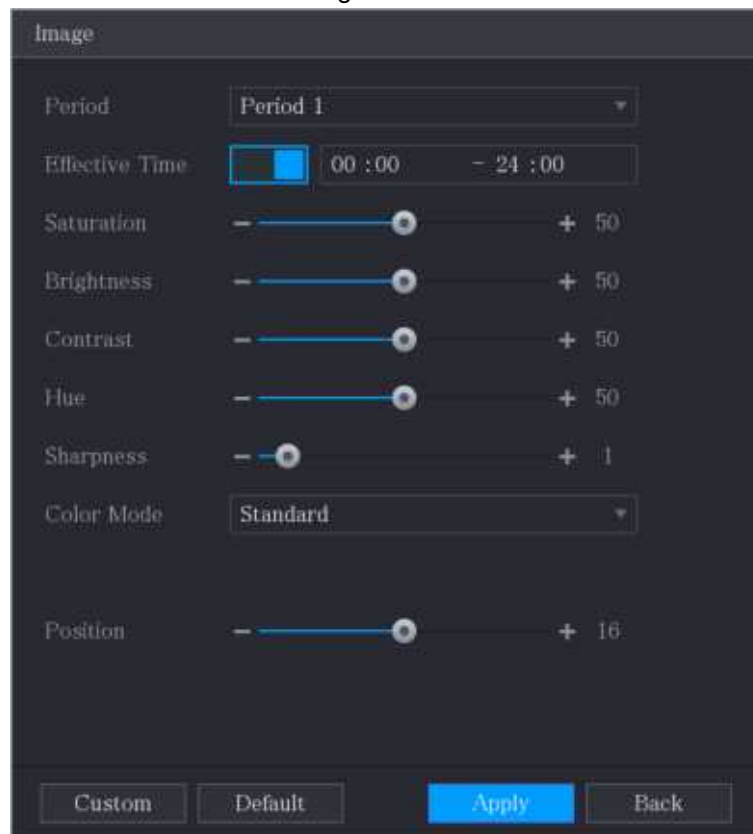


Table 5-15

Parameter	Description
Period	Divide 24 hours into two periods and configure the corresponding color settings.
Effective Time	Enable the function and then set the effective time for each period.
Sharpness	Adjust the sharpness of image edge. The bigger the value is, the more obvious the image edge, and the noise is also greater. The value ranges from 1 to 15. The default value is 1.
Hue	Adjust the hue of image. The value ranges from 0 to 100. The default value is 50.
Brightness	Adjust the image brightness. The value ranges from 0 to 100. The default value is 50. The bigger the value is, the brighter the image will become. You can adjust this value when the image as a whole looks dark or bright. However, the image is likely to become dim if the value is too big. The recommended range is between 40 and 60.
Contrast	Adjust the image contrast. The bigger the value is, the more obvious the contrast between the light area and dark area will become. You can adjust this value when the contrast is not obvious. However, if the value is too big, the dark area is likely to become darker and the light area over exposed. If the value is too small, the image is likely to become dim. The value ranges from 0 to 100. The default value is 50. The recommended range is between 40 and 60.

Parameter	Description
Saturation	Adjust the color shades. The bigger the value, the lighter the color will become. This value does not influence the general image lightness. The value ranges from 0 to 100. The default value is 50. The recommended range is between 40 and 60.
Color Mode	In the Color Mode list, you can select Standard, Soft, Bright, Vivid, Bank, Customized 1, Customized 2, Customized 3, and Customized 4. The sharpness, hue, brightness, contrast and saturation will adjust automatically according to the selected color mode.
EQ	Enhance the image effect. Adjust the effect value. - Click , image is adjusted to the optimized effect automatically. - Click , the current effect setting will be locked.  Only HD analog channel supports this function.
Position	Adjust the display position of the image in the channel window. The value indicates pixel. The default value is 16.  This function is only supported by analog channel.
Custom	You can customize four color modes. - Click Custom. The Custom Color interface is displayed. - In the Color Mode list, select Custom 1, for example. Then configure the settings for sharpness, hue, brightness, contrast and saturation. If you select All, the configuration will applies to all four customized color modes. - Click OK. - On the Image interface, in the Color Mode list, you can select the customized color mode.

5.2.8 Live View Display

5.2.8.1 Configuring Display Settings

You can configure the display effect such as displaying time title and channel title, adjusting image transparency, and selecting the resolution.

Step 1 Select **Main Menu > DISPLAY > Display**.

The **Display** interface is displayed.

Figure 5-47

Step 2 Configure the settings for the display parameters.

Table 5-16

Parameter		Description
Main Screen	Output Port	Indicates the main screen port.
	Time Title	Select the Time Title check box, the current system time displays in each channel window in live view screen. To hide the time, clear the check box.
	Channel Title	Select the Channel Title check box, the channel name, channel number and recording status display in each channel window in live view screen. To hide the time, clear the check box.
	Original Ratio	Select the Original Ratio check box, the video image displays in its actual size in the channel window.
	AI Rule	Select the AI Rule check box to enable AI rule showing function. It is enabled by default. .
	SMD Preview	Display the SMD rule box while preview. It is disabled by default.
	Live Audio	Select the Live Audio check box to enable the audio adjustment function in the channel window on the live view screen.
	Volume	Move the slider to adjust the volume of live audio.
	Transparency	Configure the transparency of the graphical user interface

Parameter		Description
		(GUI). The higher the value, the more transparent the GUI becomes.
	Resolution	Select resolution for the video. The default resolution for VGA port and HDMI port is 1280×1024.  Some of the resolution options might not be supported on the HDMI port.
	Live Mode	- General: No information is displayed on the channel window. - AI Mode: Displays the detected face snapshots.  Not all models support this function.
Sub Screen	Enable	Enable extra screen function. After this function is enabled, you can select which port as extra screen port, and the other port automatically becomes the main screen port.
	Output Port	Select the VGA port or HDMI port as the port connected by a secondary monitor. For example, if you select HDMI port as the extra screen port, the VGA port automatically becomes the main screen port.
	Resolution	Select resolution for the video. The default resolution for VGA port and HDMI port is 1280×720.  Some of the resolution options might not be supported on the HDMI port.
	Show Message	After it is enabled, the sub screen will display alarm message when an alarm is triggered.
 - The main menu does not display on the extra screen. - If you do not enable the extra screen function, both the VGA port and HDMI port display the same image.		

5.2.8.2 Configuring Zero-Channel Settings

You can view several video sources on one channel on the web end.

Step 1 Select **Main Menu > DISPLAY > Zero-Channel**.

The **Zero-Channel** interface is displayed.

Figure 5-48

Step 2 Configure the settings for the zero-channel parameters.

Table 5-17

Parameter	Description
Enable	Enable zero-channel function.
Compression	In the Compression list, select the video compression standard according to the device capability. The default is H.265.
Resolution	In the Resolution list, select the video resolution. The default is 704×576 (D1).
Frame Rate (FPS)	Select a value between 1 and 25 for PAL standard, and between 1 and 30 for NTSC standard. The actual arrange is decided and selected dependent on the Device capability.
Bit Rate (Kb/S)	The default value is 1024Kb/S. The actual arrange is decided and selected dependent on the Device capability and frame rate.

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

In the live interface on the web, click  to select one of the multi-channel modes, and then you can view the local video image.

5.2.8.3 Configuring TV



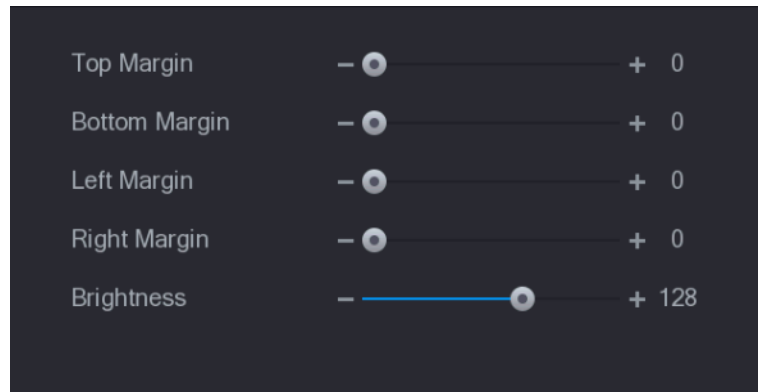
Not all models support this function.

You can adjust the border margins in top, bottom, left and right directions as well as the brightness of the monitor connected to the Video out port of the Device.

Step 1 Select **Main Menu > DISPLAY > TV Adjust**.

The **TV Adjust** interface is displayed.

Figure 5-49



Step 2 Configure the parameters according to your actual situation.

Step 3 Click **Apply** to complete the settings.

5.2.9 Configuring Tour Settings

You can configure a tour of selected channels to repeat playing videos. The videos display in turn according to the channel group configured in tour settings. The system displays one channel group for a certain period and then automatically changes to the next channel group.

Step 1 Select **Main Menu > DISPLAY > Tour Setting**.

The **Tour** interface is displayed. There are **Main Screen** tab and **Sub Screen** tab, see Figure 5-50 and Figure 5-51.

Figure 5-50

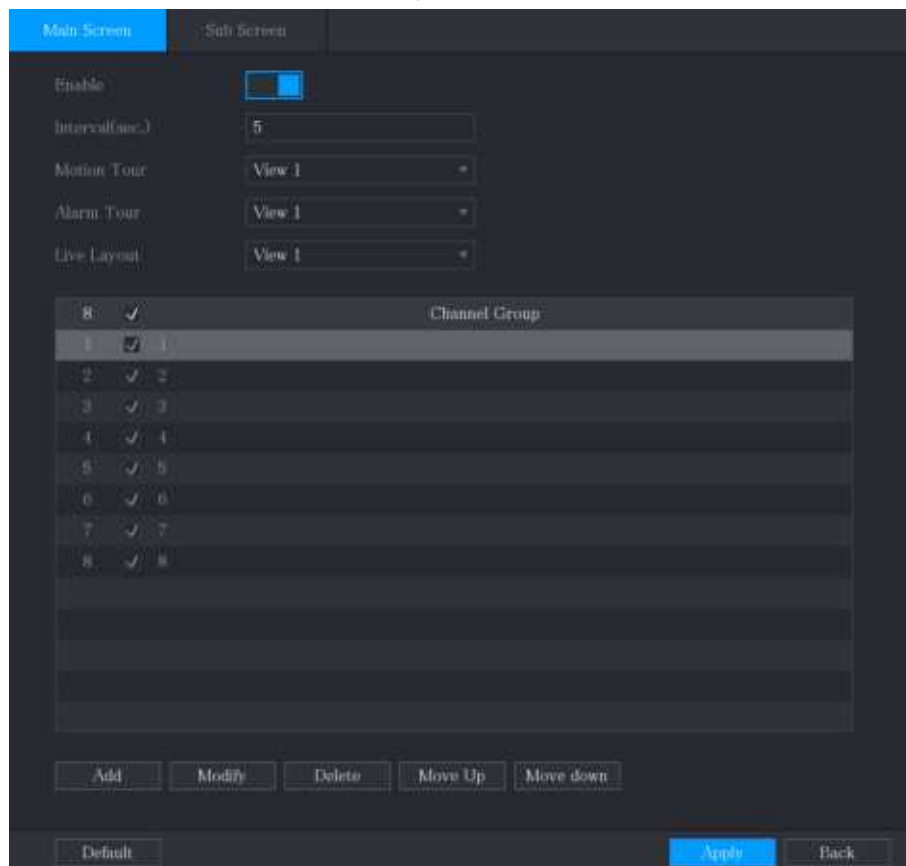


Figure 5-51

The screenshot shows the 'Sub Screen' configuration window. It includes an 'Enable' checkbox, an 'Interval (Sec.)' input field set to 5, and a 'Live Layout' dropdown set to 'View 1'. Below these is a 'Channel Group' list with 7 items, each with a checkbox and a number. At the bottom, there are buttons for 'Add', 'Modify', 'Delete', 'Move Up', 'Move down', 'Default', 'Apply', and 'Back'.

Step 2 Configure the settings for the tour parameters for both Main Screen and Extra Screen.

Table 5-18

Parameter	Description
Enable	Enable tour function.
Interval (Sec.)	Enter the amount of time that you want each channel group displays on the screen. The value ranges from 5 seconds to 120 seconds, and the default value is 5 seconds.
Motion Tour, Alarm Tour	Select the View 1 or View 8 for Motion Tour and Alarm Tour (system alarm events).
Live Layout	In the Live Layout list, select View 1 , View 4 , View 8 , or other modes that are supported by the Device.
Channel Group	Display all channel groups under the current Window Split setting. - Add a channel group: Click Add, in the pop-up Add Group channel, select the channels to form a group, and then click Save. - Delete a channel group: Select the check box of any channel group, and then click Delete. - Edit a channel group: Select the check box of any channel group and then click Modify, or double-click on the group. The Modify Channel Group dialog box is displayed. You can regroup the channels. - Click Move up or Move down to adjust the position of channel group.

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

TIPS

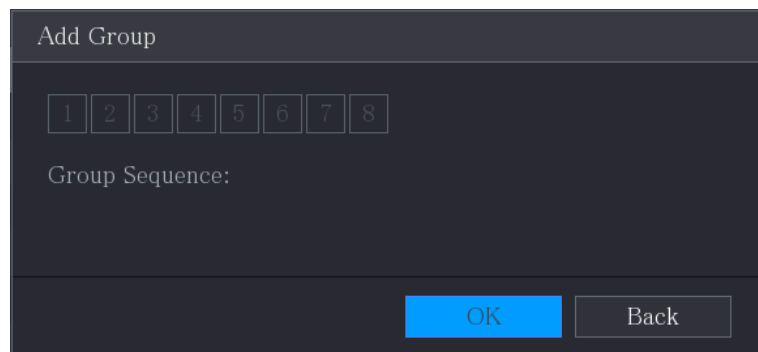
- On the top right of the live view screen, use the left mouse button or press Shift to switch between  (image switching is allowed) and  (image switching is not allowed) to turn on/off the tour function.
- On the navigation bar, click  to enable the tour and click  to disable it.

Adding a Channel Group

Step 1 Click **Add**.

The **Add Group** interface is displayed.

Figure 5-52



Step 2 Select the channels that you want to group for tour. See Figure 5-53.



If you want to select more than one channel, in the **Live Layout** list, do not select **View**

1.

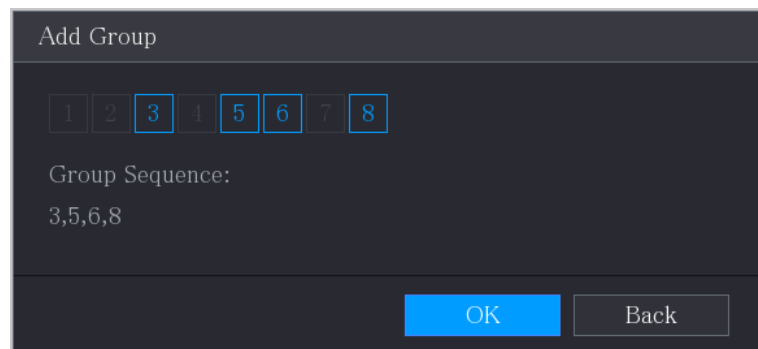


Figure 5-53

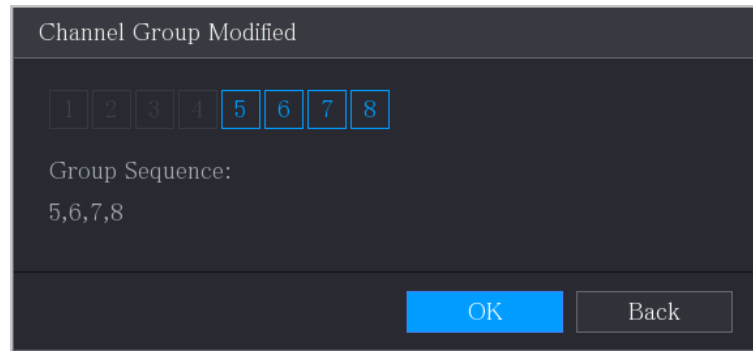
Step 3 Click **OK** to complete the settings.

Modifying a Channel Group

Double-click on a channel group, the **Channel Group Modified** interface is displayed.

You can modify channel group and click **OK** to complete the settings.

Figure 5-54



5.2.10 Quick Operation Bar

You can quickly access to the function modules on function tiles and setting menu through shortcut icons on quick operation bar.

This topic uses **ALARM** and **CAMERA** as examples to show you how to quickly access to other modules.

Shortcut Icons on Function Titles

Click **ALARM** to enter the **ALARM** interface.

Figure 5-55

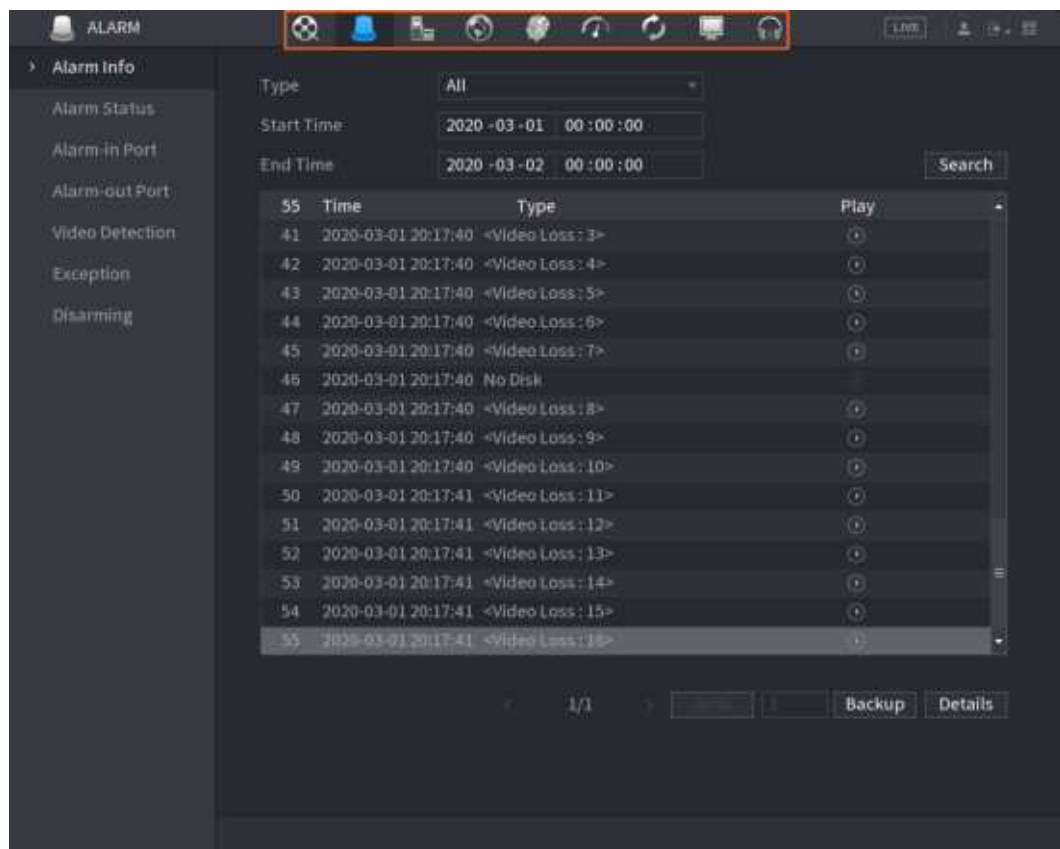


Table 5-19

Icon	Description
	Click to jump to SEARCH interface.
	Click to jump to ALARM interface.
	Click to jump to AI interface.
	Click to jump to POS interface.
	Click to jump to NETWORK interface.
	Click to jump to MAINTAIN interface.
	Click to jump to BACKUP interface.
	Click to jump to DISPLAY interface.
	Click to jump to AUDIO interface.

Shortcut Icons on Setting Menu

Click **CAMERA** to enter the **CAMERA** interface.

Figure 5-56

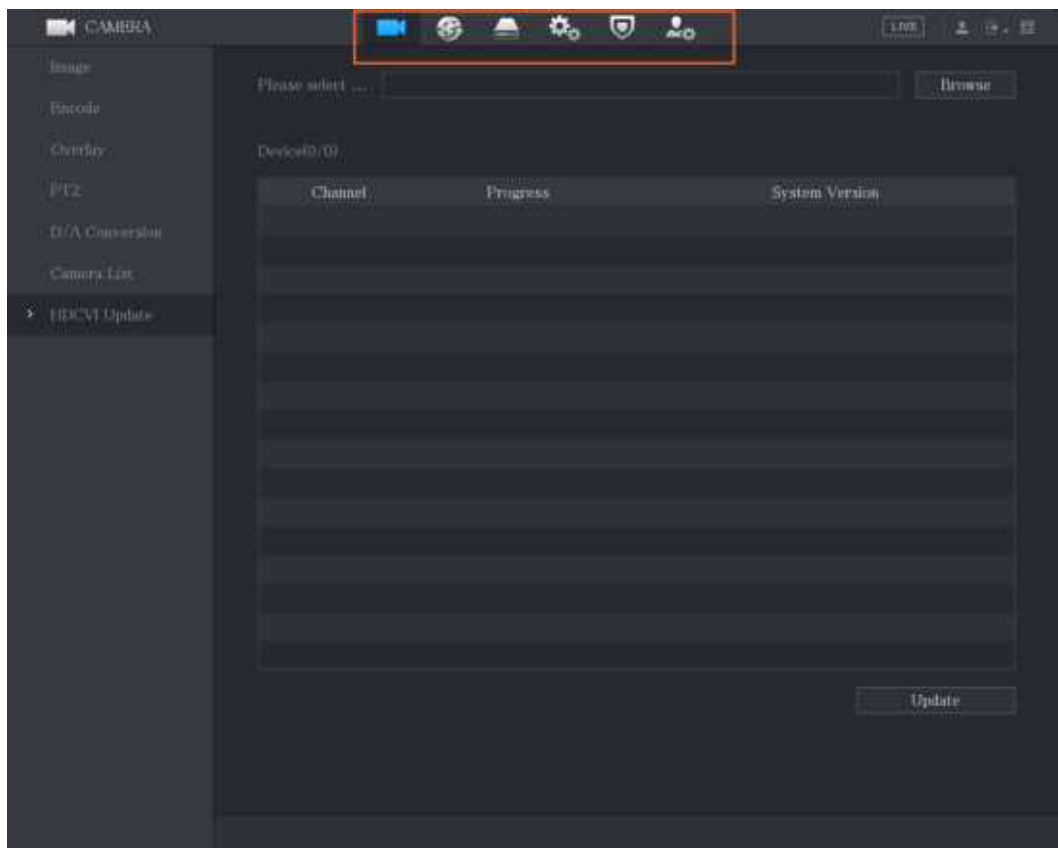


Table 5-20

Icon	Description
	Click to jump to CAMERA interface.
	Click to jump to NETWORK interface.
	Click to jump to STORAGE interface.
	Click to jump to SYSTEM interface.
	Click to jump to SECURITY interface.
	Click to jump to ACCOUNT interface.

5.3 Entering Main Menu

Right-click on the live view screen, the shortcut menu is displayed, Click Main Menu and then login the system. The Main Menu is displayed, see Figure 5-57.

Figure 5-57



Table 5-21

No.	Icon	Description
1	Function tiles	Includes nine function tiles: SEARCH, ALARM, SMART DETECTION, POS, IoT, MAINTAIN, BACKUP, DISPLAY and AUDIO. Click each tile to open the configuration interface of the tile. ● SEARCH: Search for and play back the recorded video saved on the Device. ● ALARM: Search for alarm information and configure alarm event actions. ● SMART DETECTION: Search SMD, face detection, and IVS information, and configure related settings. ● POS: You can connect the Device to the POS (Point of Sale) machine and receive the information from it. ● IoT: IoT live video preview, search, export reports, and configure function settings. ● MAINTAIN: You can view log and system information, test network and do other maintenance work. ● BACKUP: Search and back up the video files to the external storage device such as USB storage device. ● DISPLAY: Configure the display effect such as displaying content, image transparency, and resolution, and enable the zero-channel function. ● AUDIO: Manage audio files and configure the playing schedule. The audio file can be played in response to an alarm event if the voice prompts function is enabled.
2	Switch icon	 indicates the current page of main menu. Click  to switch to the next page or click  or  to turn page.
3	Setting menu	Includes six configurations through which you can configure camera settings, network settings, storage settings, system settings, account settings, and view information.
4	Live	Click  to go to the live view screen.
5		When you point to  , the current user account is displayed.
6		Click  , select Logout , Reboot , or Shutdown according to your actual situation.

No.	Icon	Description
7		Displays Cell Phone Client and Device SN QR Code. - Cell Phone Client: Use your mobile phone to scan the QR code to add the device into the Cell Phone Client, and then you can start accessing the Device from your cell phone. - Device SN: Obtain the Device SN by scanning the QR code. Go to the P2P management platform and add the Device SN into the platform. Then you can access and manage the device in the WAN. For details, refer to the P2P operation manual. You can also configure P2P function in the local configurations. See "5.1.4.5 Configuring P2P Settings."

5.4 Controlling PTZ Cameras

PTZ is a mechanical platform that carries a camera and a protective cover and performs overall control remotely. A PTZ can move in both horizontal and vertical direction to provide all-around view to the camera.



Before operating PTZ, ensure the network connection between PTZ and the Device.

5.4.1 Configuring PTZ Connection Settings

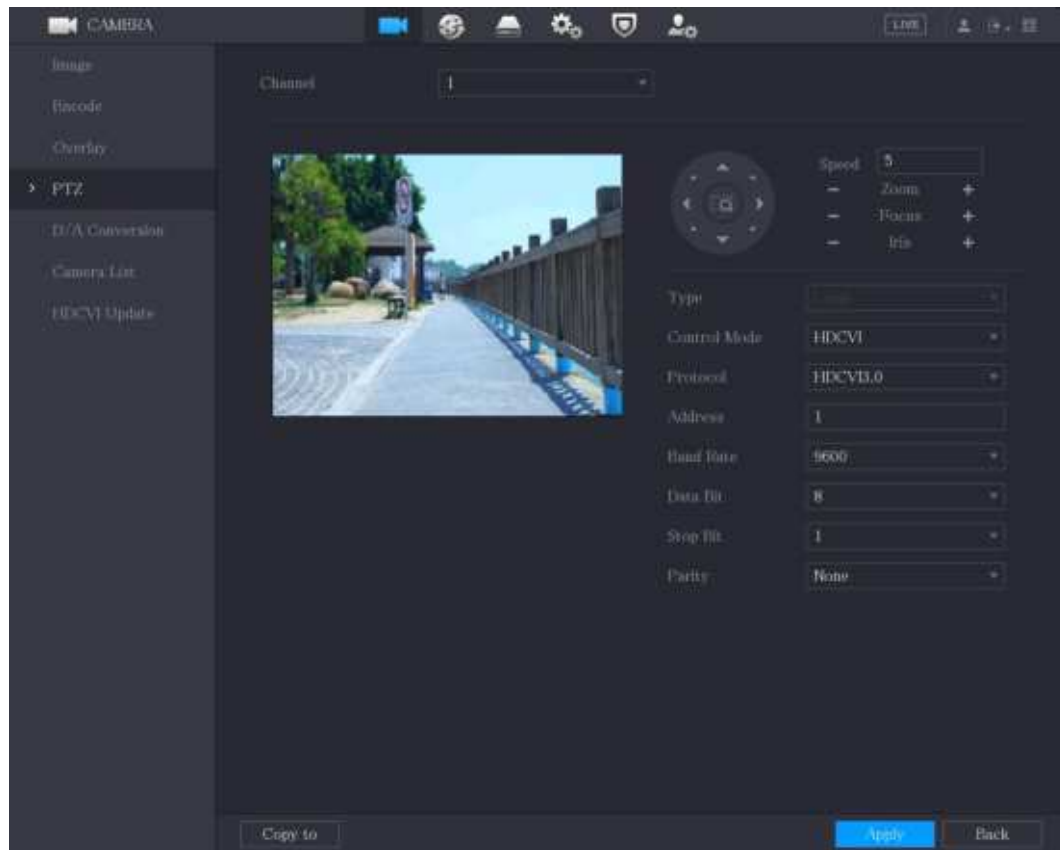
You need to configure the PTZ connection settings before use.

- Local connection: RS-485 Port for connecting speed dome or coaxial cable for connecting coaxial camera.
- Remote connection: local area network.

Step 1 Select **Main Menu > CAMERA > PTZ**.

The **PTZ** interface is displayed.

Figure 5-58



Step 2 Configure the settings for the PTZ connection parameters.

Table 5-22

Parameter	Description
Channel	In the Channel list, select the channel that you want to connect the PTZ camera to.
Type	- Local: Connect through RS-485 port or coaxial cable. - Remote: Connect through network by adding IP address of PTZ camera to the Device.
Control Mode	In the Control Mode list, select Serial Port or HDCVI . For HDCVI series product, select HDCVI . The control signal is sent to the PTZ through the coaxial cable. For the serial mode, the control signal is sent to the PTZ through the RS-485 port.
Protocol	In the Protocol list, select the protocol for the PTZ camera. For example, select HDCVI3.0 .
Address	In the Address box, enter the address for PTZ camera. The default is 1.  The entered address must be the same with the address configured on the PTZ camera; otherwise the PTZ camera cannot be controlled from the Device.
Baud Rate	In the Baud Rate list, select the baud rate for the PTZ camera. The default is 9600.
Data Bits	The default value is 8.
Stop Bits	The default value is 1.
Parity	The default value is NONE.

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



Click **Copy** to copy the settings to other channels.

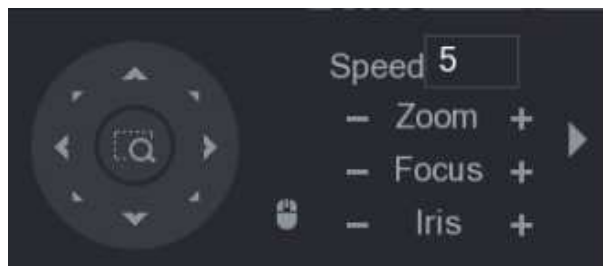
5.4.2 Working with PTZ Control Panel

PTZ control panel performs the operations such as directing camera in eight directions, adjusting zoom, focus and iris settings, and quick positioning.

Basic PTZ Control Panel

Right-click on the live view screen and then select **PTZ**. The PTZ control panel is displayed.

Figure 5-59



The functions with buttons in gray are not supported by the system.

Table 5-23

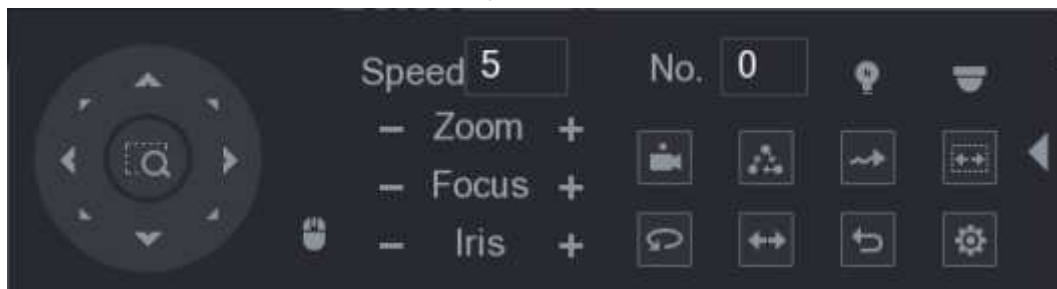
Parameter	Description
Speed	Controls the movement speed. The bigger the value is, the faster the movement will be.
Zoom	 : Zoom out.  : Zoom in.
Focus	 : Focus far.  : Focus near.
Iris	 : Image darker.  : Image brighter.
PTZ movement	Supports eight directions.

Parameter	Description
	Fast positioning button. - Positioning: Click  to enter the fast positioning screen, and then click anywhere on the live view screen, the PTZ will turn to this point and move it to the middle of the screen. - Zooming: On the fast positioning screen, drag to draw a square on the view. The square supports zooming. - Dragging upward is to zoom out, and dragging downward is to zoom in. - The smaller the square, the larger the zoom effect.  Not all models support this function and can only be controlled through mouse operations.
	Click  , you can control the four directions (left, right, up, and down) PTZ movement through mouse operation.
	Click  to open the expanded PTZ control panel.

Expanded PTZ Control Panel

On the basic PTZ control panel, click  to open the expanded PTZ control panel to find more options.

Figure 5-60



- The functions with buttons in gray are not supported by the system.
- Right-click once to return to the interface of PTZ basic control panel.

Table 5-24

Icon	Function	Icon	Function
	Preset		Pan
	Tour		Flip
	Pattern		Reset

	Scan		Click the Auxiliary Config icon to open the PTZ functions settings interface.
	Auxiliary		Click the Enter Menu icon to open the MENU OPERATION interface.

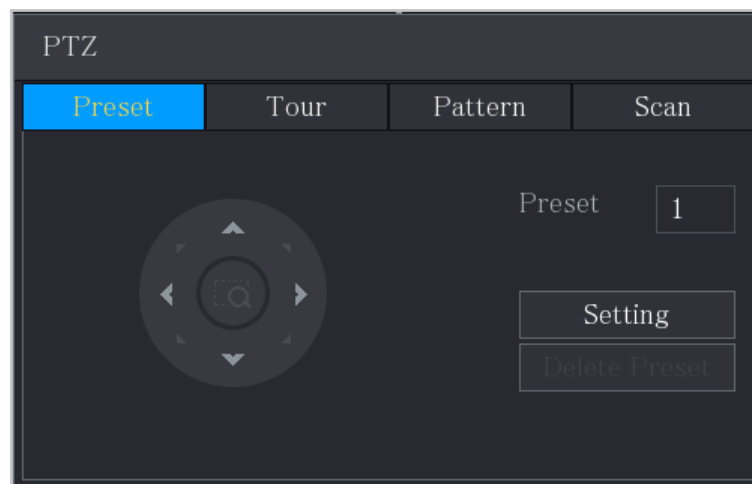
5.4.3 Configuring PTZ Functions

5.4.3.1 Configuring Presets

Step 1 On the Expanded PTZ Control Panel, click .

The **Preset** interface is displayed.

Figure 5-61



Step 2 Click the direction arrows to the required position.

Step 3 In the **Preset** box, enter the value to represent the required position.

Step 4 Click **Setting** to complete the preset settings.

5.4.3.2 Configuring Tours

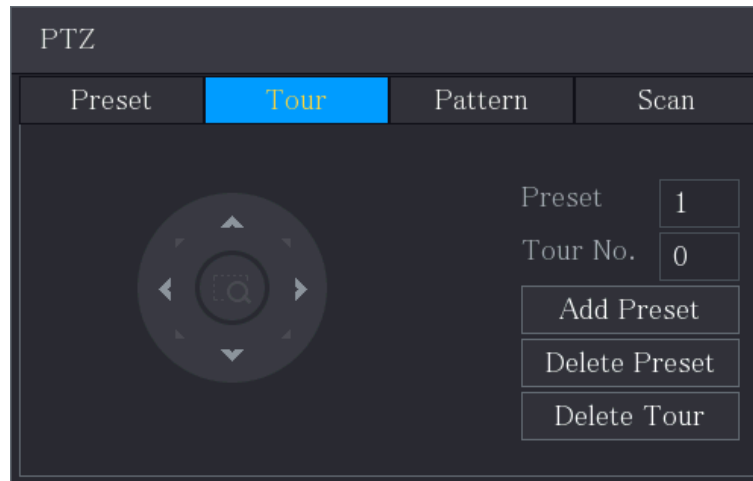
Step 1 On the Expanded PTZ Control Panel, click .

The **PTZ** interface is displayed.

Step 2 Click the **Tour** tab.

The **Tour** interface is displayed.

Figure 5-62



Step 3 In the **Tour No.** box, enter the value for the tour route.

Step 4 In the **Preset** box, enter the preset value.

Step 5 Click **Add Preset**.

A preset will be added for this tour.



- You can repeat adding more presets.
- Click **Delete Preset** to delete the preset for this tour. This operation can be repeated to delete more presets. Some protocols do not support deleting.

5.4.3.3 Configuring Patterns

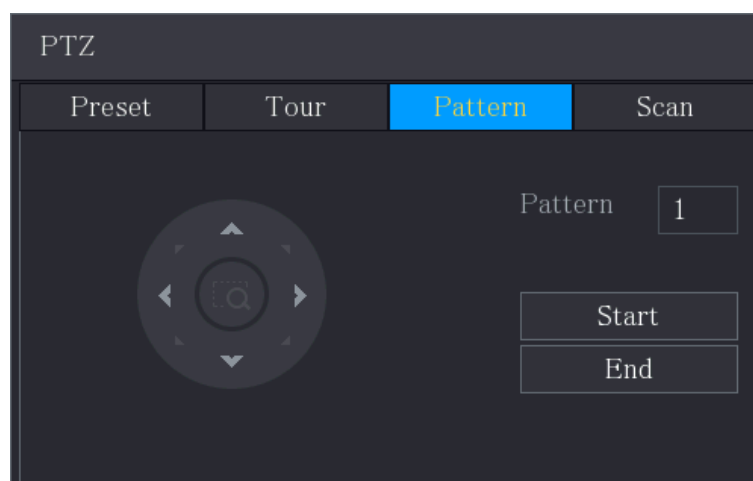
Step 1 On the Expanded PTZ Control Panel, click .

The **PTZ** interface is displayed.

Step 2 Click the **Pattern** tab.

The **Pattern** interface is displayed.

Figure 5-63



Step 3 In the **Pattern** box, enter the value for pattern.

Step 4 Click **Start** to perform the directions operations. You can also go to the PTZ Control Panel to perform the operations of adjusting zoom, focus, iris, and directions.

Step 5 On the **PTZ** interface, click **End** to complete the settings.

5.4.3.4 Configuring Scan

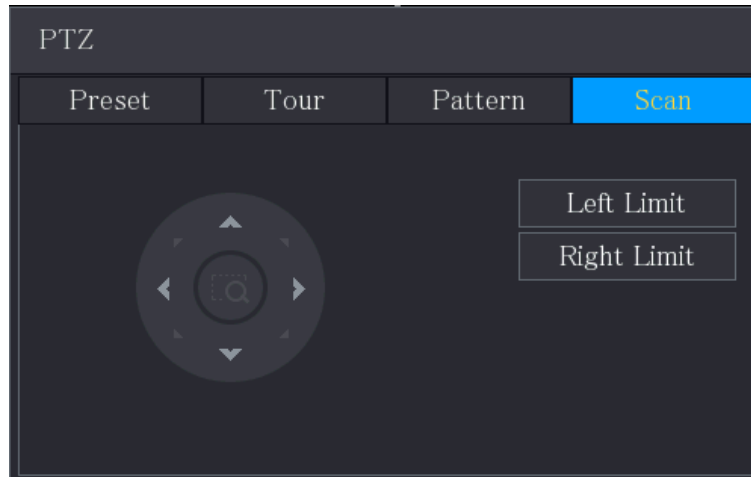
Step 1 On the Expanded PTZ Control Panel, click .

The **PTZ** interface is displayed.

Step 2 Click the **Scan** tab.

The **Scan** interface is displayed.

Figure 5-64

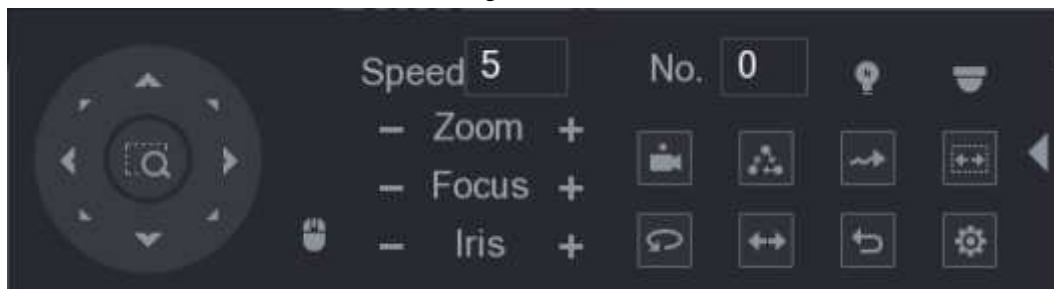


Step 3 Click the direction arrows to position the left and right limits.

5.4.4 Calling PTZ Functions

After you have configured the PTZ settings, you can call the PTZ functions for monitoring from the Expanded PTZ Control Panel.

Figure 5-65



5.4.4.1 Calling Presets

Step 1 On the expanded PTZ Control Panel, in the **No.** box, enter the value of the preset that you want to call.

Step 2 Click  to call the preset.

Step 3 Click  again to stop calling the preset.

5.4.4.2 Calling Tours

Step 1 On the Expanded PTZ Control Panel, in the **No.** box, enter the value of the tour that you want to call.

Step 2 Click  to call the tour.

Step 3 Click  again to stop calling the tour.

5.4.4.3 Calling Patterns

Step 1 On the Expanded PTZ Control Panel, in the **No.** box, enter the value of the pattern that you want to call.

Step 2 Call  to call the pattern.

The PTZ camera moves according to the configured pattern repeatedly.

Step 3 Click  again to stop calling the pattern.

5.4.4.4 Calling AutoScan

Step 1 On the Expanded PTZ Control Panel, in the **No.** box, enter the value of the border that you want to call.

Step 2 Click .

The PTZ camera performs scanning according to the configured borders.

Step 3 Click  again to stop auto scanning.

5.4.4.5 Calling AutoPan

Step 1 On the Expanded PTZ Control Panel, click  to start moving in horizontal direction.

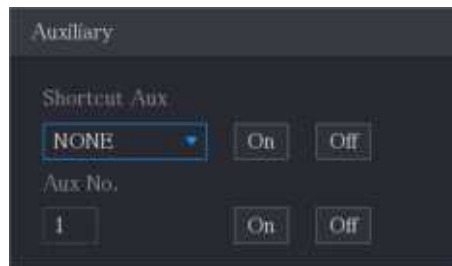
Step 2 Click  again to stop moving.

5.4.4.6 Using AUX Button

On the Expanded PTZ Control Panel, click , the AUX setting interface is displayed.

- In the **Shortcut Aux** list, select the option that corresponds to the applied protocol.
- In the **Aux No.** box, enter the number that corresponds to the AUX switch on the decoder.

Figure 5-66



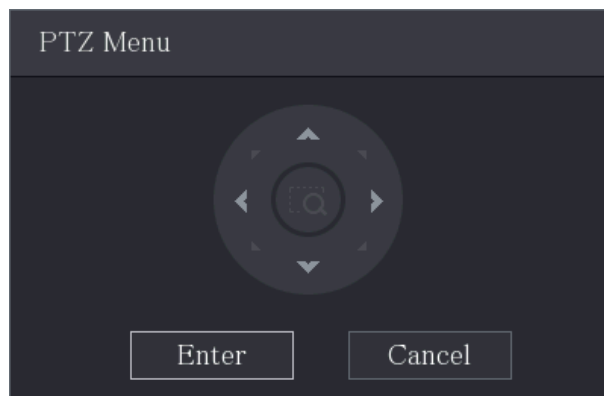
5.4.5 Calling OSD Menu

For the coaxial camera, you can call the OSD menu through the Expanded PTZ Control Panel.

Step 1 On the Expanded PTZ Control Panel, click .

The **PTZ Menu** interface is displayed.

Figure 5-67



Step 2 Click **Enter**.

The OSD menu is displayed.

Figure 5-68



Step 3 On the **PTZ Menu** interface, click the arrow button to select the onscreen parameters.

Step 4 Click **Enter** to complete the settings.

5.5 Configuring Camera Settings

5.5.1 Configuring Image Settings

You can configure the image settings such as saturation, contrast, brightness, sharpness for each connected camera.

Step 1 Select **Main Menu > CAMERA > Image**.

The **Image** interface is displayed. See Figure 5-69 for analog channel and Figure 5-70 for digital channel.

Figure 5-69

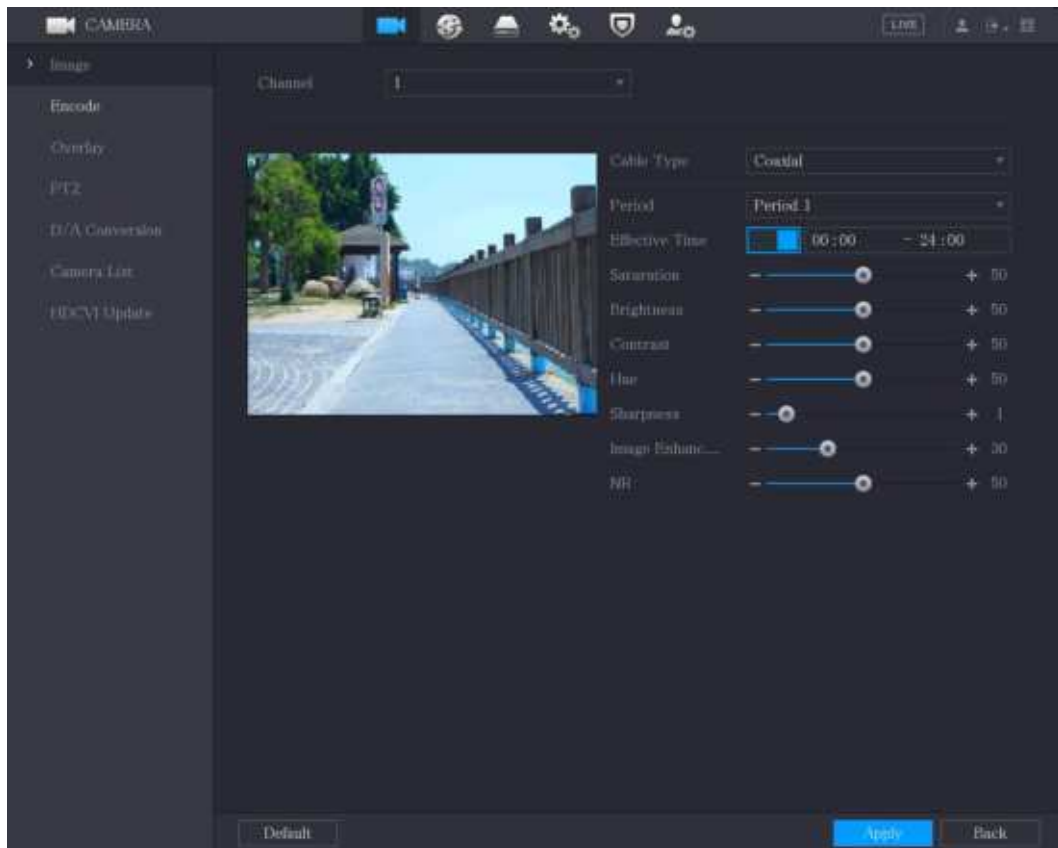
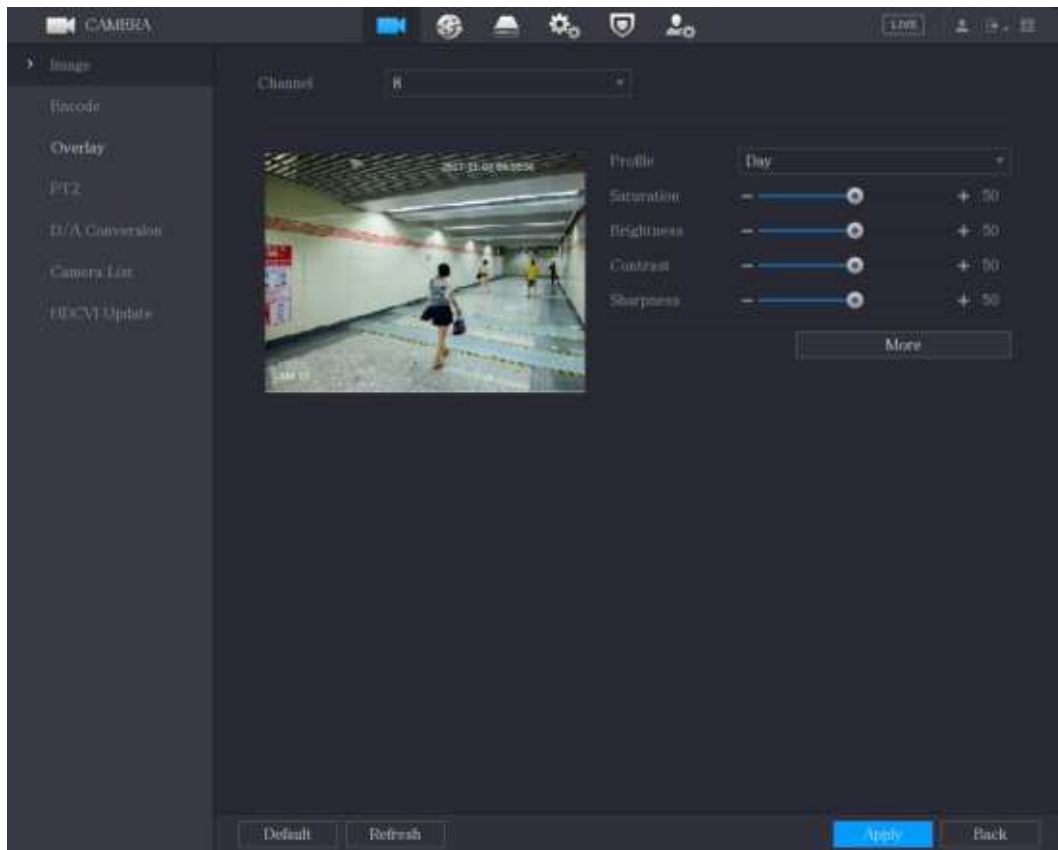


Figure 5-70



Step 2 Configure the settings for the image parameters.

On the digital channel interface, click **More** to display more parameters.

Table 5-25

Parameter	Description
Channel	In the Channel list, select the channel that you want to configure.
Cable Type	In the Cable Type list, select the cable type that the camera uses.  Not all models support this function.
Period	In the Period list, select a time period for the image settings. The image settings will be only used during the selected period.
Effective Time	Enable the effective function. In the Effective Time box, enter the start time and end time for the period you selected.
Saturation	Adjusts the color shades. The bigger the value, the lighter the color will become. This value does not influence the general image lightness. The value ranges from 0 to 100. The default value is 50. The recommended range is between 40 and 60.

Parameter	Description
Contrast	Adjusts the image contrast. The bigger the value is, the more obvious the contrast between the light area and dark area will become. You can adjust this value when the contrast is not obvious. However, if the value is too big, the dark area is likely to become darker and the light area over exposed. If the value is too small, the image is likely to become dim. The value ranges from 0 to 100. The default value is 50. The recommended range is between 40 and 60.
Brightness	Adjusts the image brightness. The bigger the value is, the brighter the image will become. You can adjust this value when the image as a whole looks dark or bright. However, the image is likely to become dim if the value is too big. The value ranges from 0 to 100. The default value is 50. The recommended range is between 40 and 60.
Hue	Adjusts the hue of image. The value ranges from 0 to 100. The default value is 50.
Sharpness	Adjusts the sharpness of image edge. The bigger the value is, the more obvious the image edge, and the noise is also greater. The value ranges from 1 to 15. The default value is 1.
Image Enhance	Adjusts the image definition. The bigger the value is, the clearer the image will become, but there will be more noises.
NR	Reduces the noises from image. The bigger the value is, the better the image will become.
Config File	In the Config File list, select Day, Night, Normal, or Switch By Period. The system configures the parameters correspondingly. • Day: Apply the configuration during daytime. • Night: Apply the configuration during nighttime. • Normal: Apply the configuration during day and night. • Switch by Period: If you select this option, you need to configure the sunrise time and sunset time where you are located.
Mirror	Enable the function, the left and right side of the video image will be switched. It is disabled by default.
3D Denoise	This function specially applies to the image which frame rate is configured as 2 at least. It reduces the noises by making use of the information between two frames. The bigger the value is, the better the effect.
Flip	In the Flip list, you can select 180° to change the video image display. By default, the setting is No Flip .
Light	In the Light list, select Close or Enable to use the backlight compensation or not.

Parameter	Description
Scene Mode	Configure the white balance to adjust the general hue of the image. The default setting is Auto. - Auto: Automatically apply white balance to different colors to make the image color display normally. - Sunny: Apply the threshold value to sunny environment. - Night: Apply the threshold value to night. - Customized: Manually adjust the Red Gain and Blue Gain values.
Day & Night	Configure the color and black&white mode of the image. This setting is not affected by the configuration files. The default setting is Auto. - Color: The camera outputs color image only. - Auto: Depends on the camera, such as overall brightness and whether there is an IR light, either color image or black&white image is output. - B/W: The camera outputs Black and white image only. - By Time: The camera outputs image according to the configured sunrise time and sunset time.

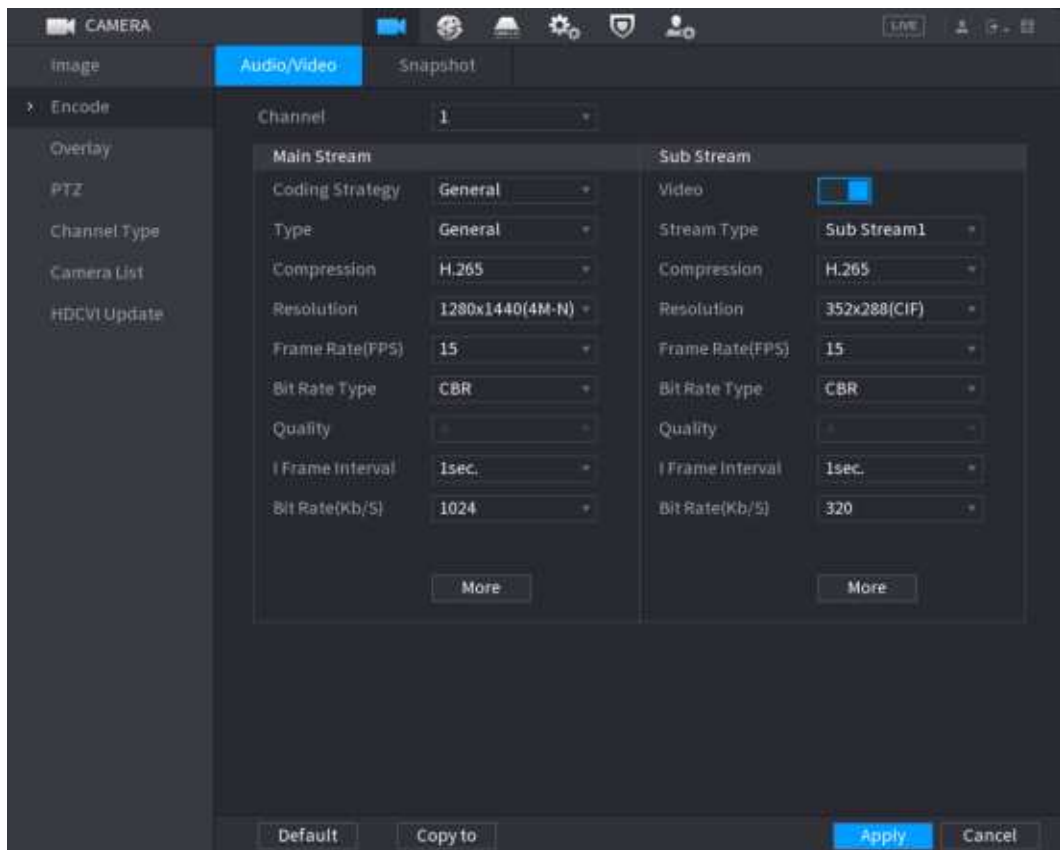
Step 3 Click **Apply** to complete the settings.

5.5.2 Configuring Encode Settings

Step 1 Select **Main Menu > CAMERA > Encode > Audio/Video**.

The **Audio/Video** interface is displayed.

Figure 5-71



Step 2 Configure the settings for the main/sub streams parameters.

Table 5-26

Parameter	Description
Channel	In the Channel list, select the channel that you want to configure the settings for.
Coding Strategy	- General: Uses general coding strategy. - Smart Codec: Enables the smart codec function. This function can reduce the video bit stream for non-important recorded video to maximize the storage space. - AI Codec: Enables the AI codec function. This function can reduce the video bit stream for non-important recorded video to maximize the storage space.
Type	- Main Stream: In the Type list, select General, Motion, or Alarm. - Sub Stream: This setting is not configurable.
Compression	In the Compression list, select the encode mode. - H.265: Main profile encoding. This setting is recommended. - H.264H: High profile encoding. Low bit stream with high definition. - H.264: General profile encoding. - H.264B: Baseline profile encoding. This setting requires higher bit stream compared with other settings for the same definition.
Bit Rate Type	In the Bit Rate Type list, select resolution for the video. The maximum video resolution might be different dependent on your device model.
Frame Rate (FPS)	Configure the frames per second for the video. The higher the value, the clearer and smoother the image will become. Frame rate changes along with the resolution. Generally, in PAL format, you can select the value from 1 through 25; in NTSC format, you can select the value from 1 through 30. However, the specific range of frame rate that you can select depends on the capability of the Device.
Quality	This function is available if you select VBR in the Bit Rate List. The higher the value, the better the image will become.
I Frame Interval	The interval between two reference frames.
Bit Rate (Kb/S)	In the Bit Rate list, select a value or enter a customized value to change the image quality. The bigger the value is, the better the image will become.
Video	Enable the function for sub stream.
Audio	Click More, the More interface is displayed. Audio: This function is enabled by default for main stream. You need to manually enable it for sub stream 1. Once this function is enabled, the recorded video file is composite audio and video stream.
Audio Source	
	Audio Source: In the Audio Source list, you can select LOCAL and HDCVI.

Parameter	Description
Compression	◇ LOCAL: The audio signal is input from Audio input port. ◇ HDCVI: The audio signal is input from HDCVI camera. ● Audio Format: In the Compression list, select a format that you need.

Step 3 Click **Apply** to complete the settings.



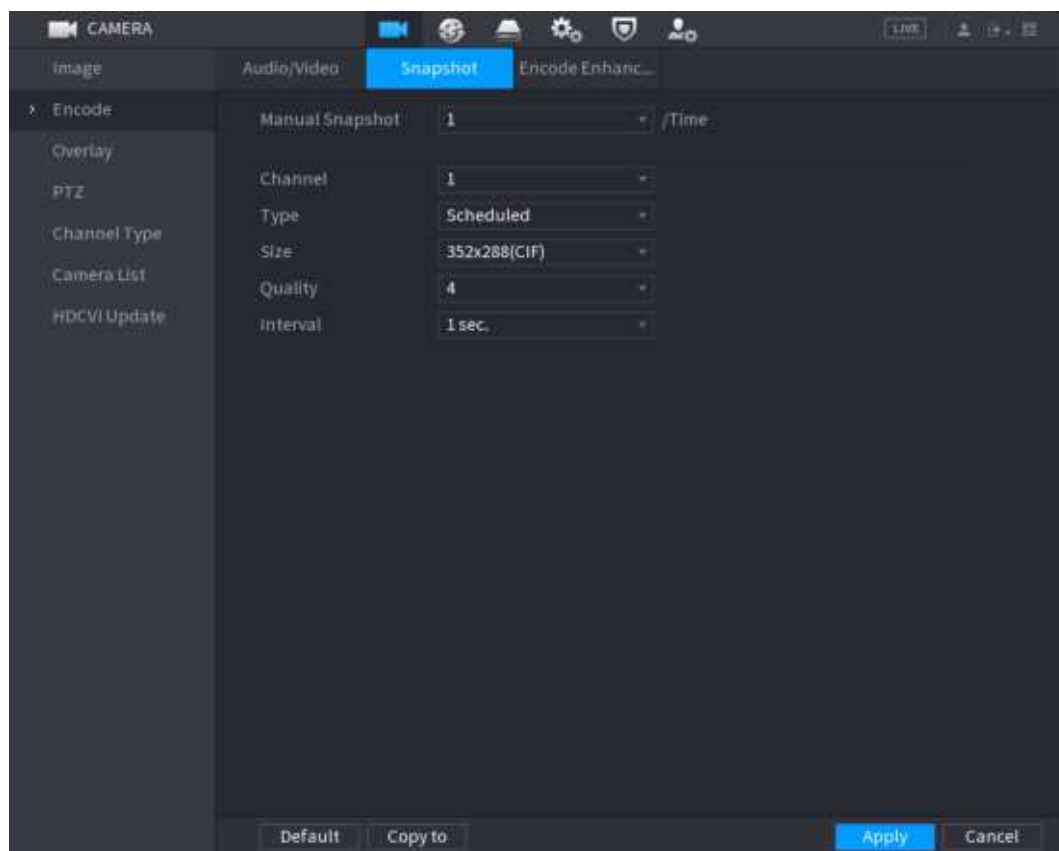
Click **Copy to** to copy the settings to other channels.

5.5.3 Configuring Snapshot Settings

Step 1 Select **Main Menu > CAMERA > Encode > Snapshot**.

The **Snapshot** interface is displayed.

Figure 5-72



Step 2 Configure the settings for the snapshot parameters.

Table 5-27

Parameter	Description
Manual Snapshot	In the Manual Snapshot list, select how many snapshots you want to take each time.
Channel	In the Channel list, select the channel that you want to configure the settings for.
Type	In the Type list, you can select Scheduled, Event, or Face Snapshot as the event type for which you want to take a snapshot. ● Scheduled: The snapshot is taken during the scheduled period.

Parameter	Description
	• Event: The snapshot is taken when there is an alarm event occurs, such as motion detection event, video loss, and local alarms. • Face Snapshot: The snapshot is taken when the face is detected. The face detection function is support only with the Channel 1.
Size	In the Size list, select a value for the image. The bigger the value is, the better the image will become.
Quality	Configures the image quality by 6 levels. The higher the level, the better the image will become.
Interval	Configures or customizes the snapshot frequency. You can select 1 second per one snapshot to 7 seconds per one snapshot. The maximum is 3600 seconds per one snapshot.

Step 3 Click **Apply** to complete the settings.



Click **Copy to** to copy the settings to other channels.

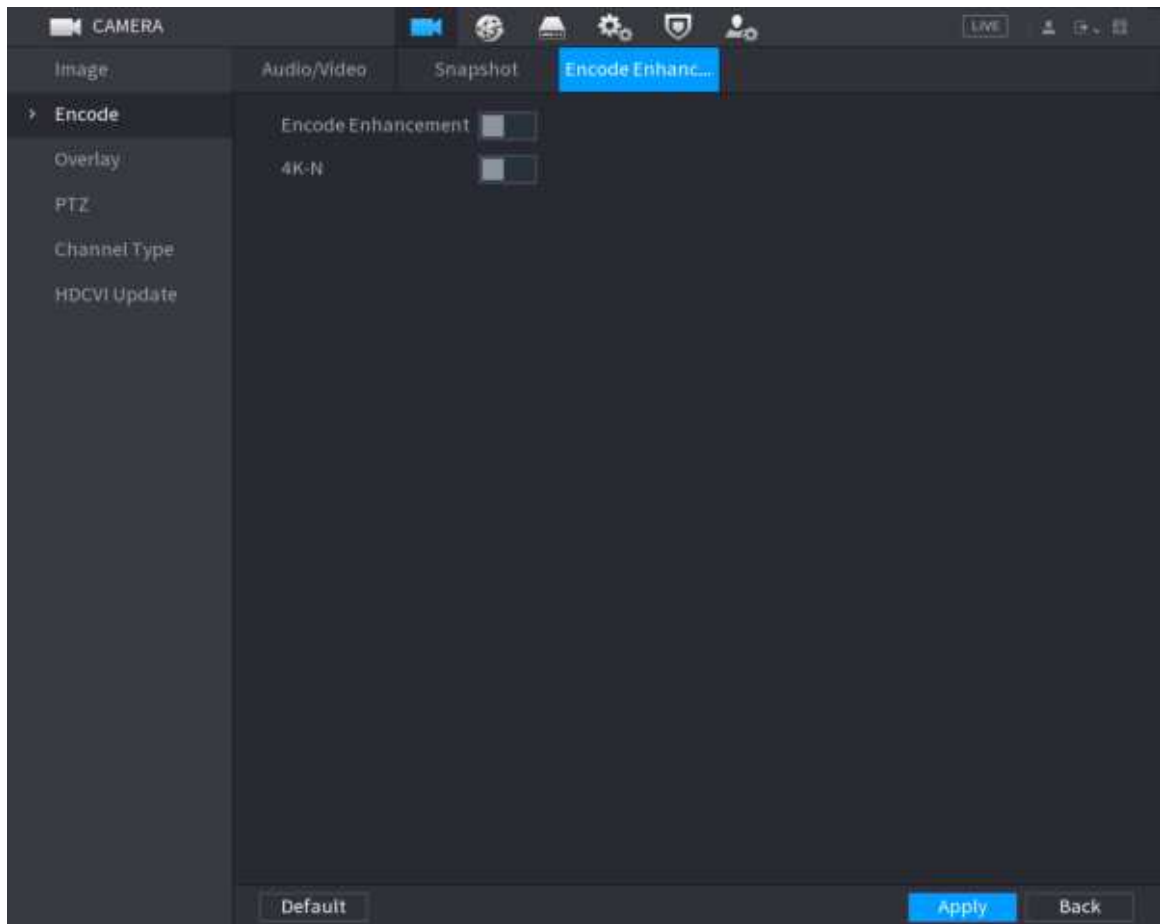
5.5.4 Configuring Encode Enhancement

You can enable this function and get more FPS in encode settings (see "5.5.2 Configuring Encode Settings"). In the meantime, you will not be able to use extra screen function (see "5.2.8.1 Configuring Display Settings") and AI functions (see "5.11 AI Function").

Select **Main Menu > CAMERA > Encode > Encode Enhancement**.

The **Encode Enhancement** interface is displayed.

Figure 5-73



Click the switch to enable it.

When connecting to the new generation 4K cameras, you can enable **4K-N** to switch 4K non-live view to 4K-N live view and encoding.

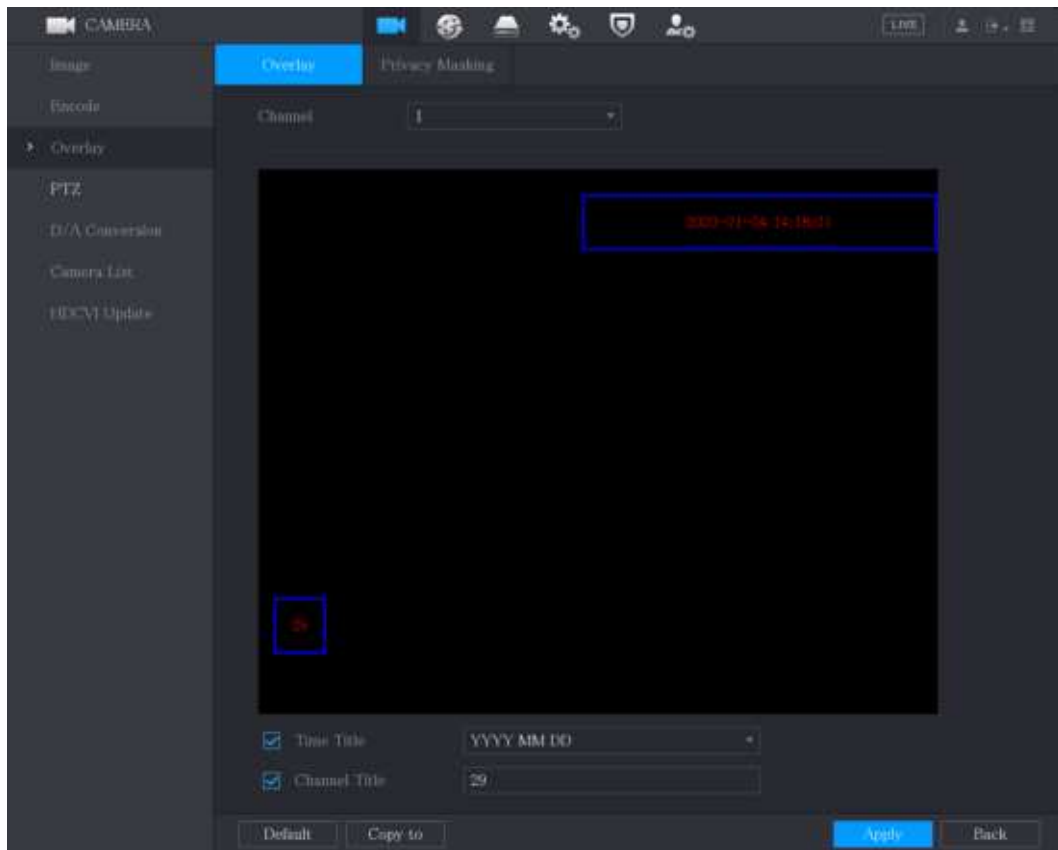
5.5.5 Configuring Overlay Settings

You can configure to display system time and channel name on each channel window in the live view screen.

Step 1 Select **Main Menu > CAMERA > Overlay > Overlay**.

The **Overlay** interface is displayed.

Figure 5-74



Step 2 Configure the settings for the text overlay parameters.

Table 5-28

Parameter	Description
Channel	In the Channel list, select the channel that you want to configure the settings for.
Time Title	Select the Time Title check box to display the system time on each channel window in the live view screen. In the Time Title list, select time display style.
Channel Title	Select the Channel Title check box to display the channel name on each channel window in the live view screen. In the Channel Title box, enter the name for the selected channel.

Step 3 Click **Apply** to complete the settings.

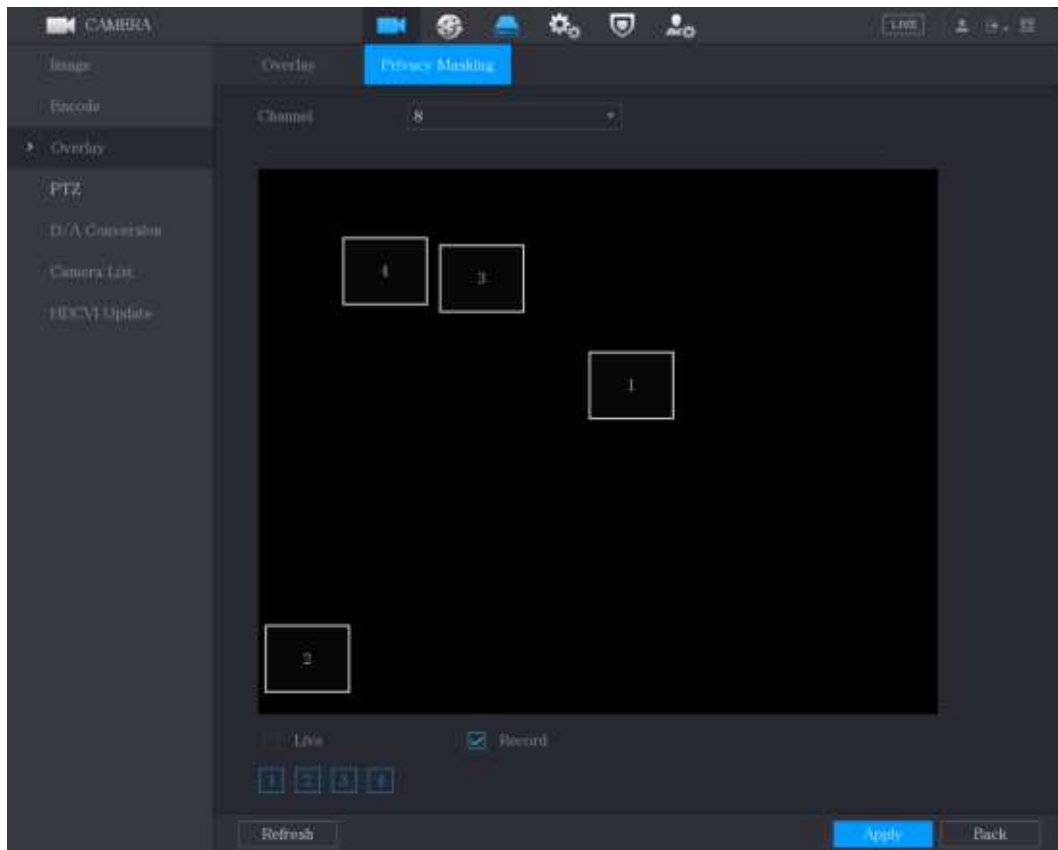


Click **Copy to** to copy the settings to other channels.

5.5.6 Configuring Covered Area Settings

Step 1 Select **Main Menu > CAMERA > Overlay > Privacy Masking**.
The **Privacy Masking** interface is displayed.

Figure 5-75



Step 2 Configure the settings for the covered area parameters.

Table 5-29

Parameter	Description
Channel	In the Channel list, select the channel that you want to configure the settings for.
Live	- Preview: Select the Live check box to apply the configured covered block to the selected channel window in the live view screen. - Record: Select the Record check box to apply the configured covered block to the selected channel window during recording. To configure covering block, do the following: - Select the Live check box or the Record check box, or select the both. The "1, 2, 3, 4" buttons are activated. - Click the buttons to select blocks. A triangle solid black block is displayed. - Drag the block to the area that you want to cover and adjust the size of the block. You can configure total 4 covered blocks.
Record	

Step 3 Click **Apply** to complete the settings.

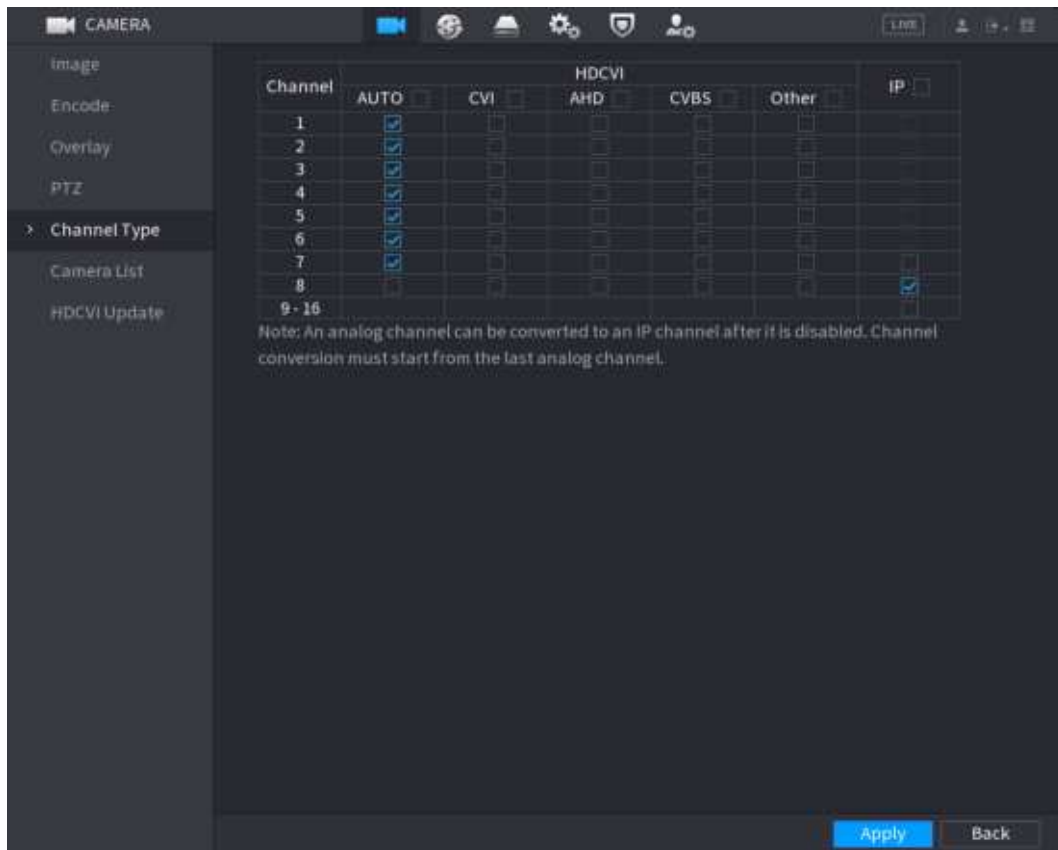
5.5.7 Configuring Channel Type

You can configure the channel type as **Analog** or **IP** channel.

Step 1 Select **Main Menu > CAMERA > Channel Type**.

The **Channel Type** interface is displayed.

Figure 5-76



Step 2 Configure the channels.

- Analog Channel: Select the transmission medium such as CVI, AHD, CVBS, and then follow the onscreen instructions to complete the settings.
- IP Channel: You can enable the IP channels by disabling the corresponding analog channels. The Device also provides expanded IP channels for your use, such as the **17–64** channels in Figure 5-76.



- The 17–64 channels are only for IP camera and the range changes dependent on the model you purchased.
- The channel selection for analog camera or IP camera are in sequence, for example, if you want to select channels for IP camera, you need to select from the last channel number Channel **16** first, which means, you cannot jump to select the channel **15** directly until you have selected the channel **16**.

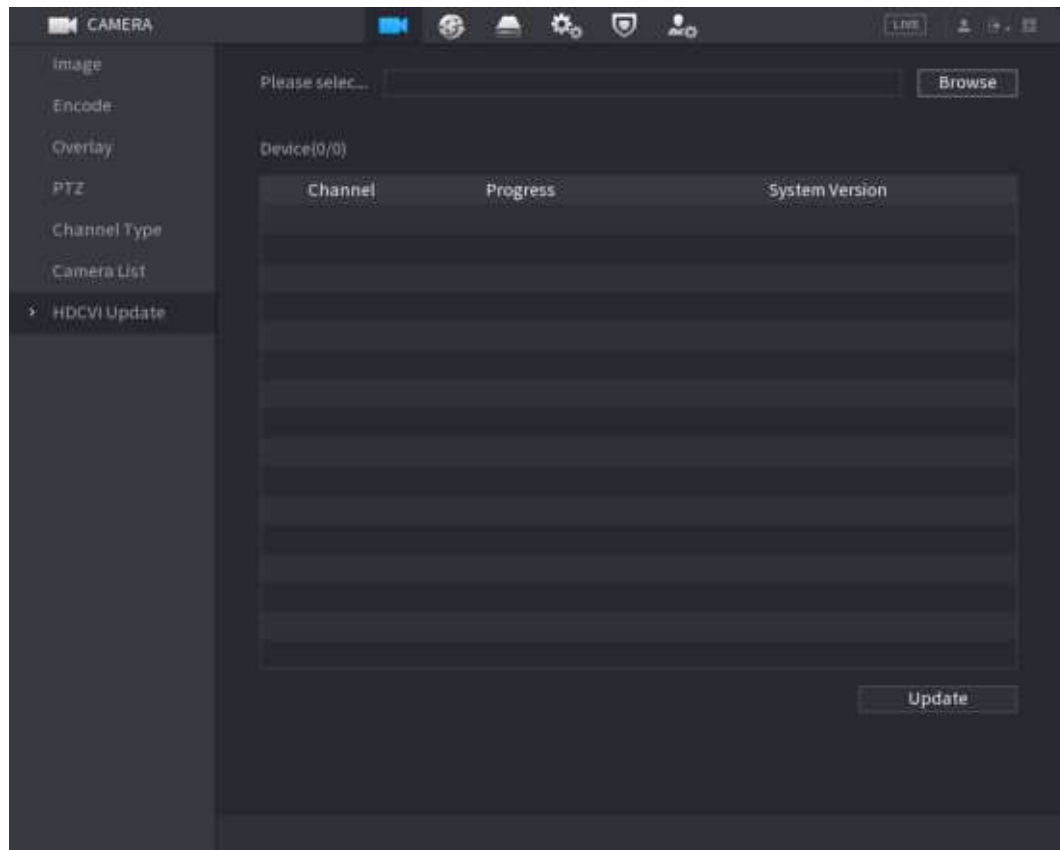
Step 3 Click **Apply** and follow the onscreen instructions to complete the settings.

5.5.8 Upgrading Coaxial Camera

Step 1 Select **Main Menu > CAMERA > HDVCI Update**.

The **HDVCI Update** interface is displayed.

Figure 5-77



Step 2 Click **Browse**.

The **Browse** interface is displayed.

Step 3 Select the upgrade file and then click **OK**.

The **HDVCI Update** interface is displayed.



You need to insert the USB storage device that contains the upgrading files.

Step 4 Select the check box of the channel that you want to upgrade.

Step 5 Click **Update**.

If the upgrading is successful, the system pops up a message indicating the upgrading is completed.

5.6 Configuring Remote Devices

5.6.1 Adding Remote Devices



This function is available after you have configured the channel type as IP channel as described in previous section, see "5.5.7 Configuring Channel Type."

You can add remote devices by adding the IP address.

Select **Main Menu > CAMERA > Camera List > Add Camera**, the **Add Camera** interface is displayed.

Figure 5-78

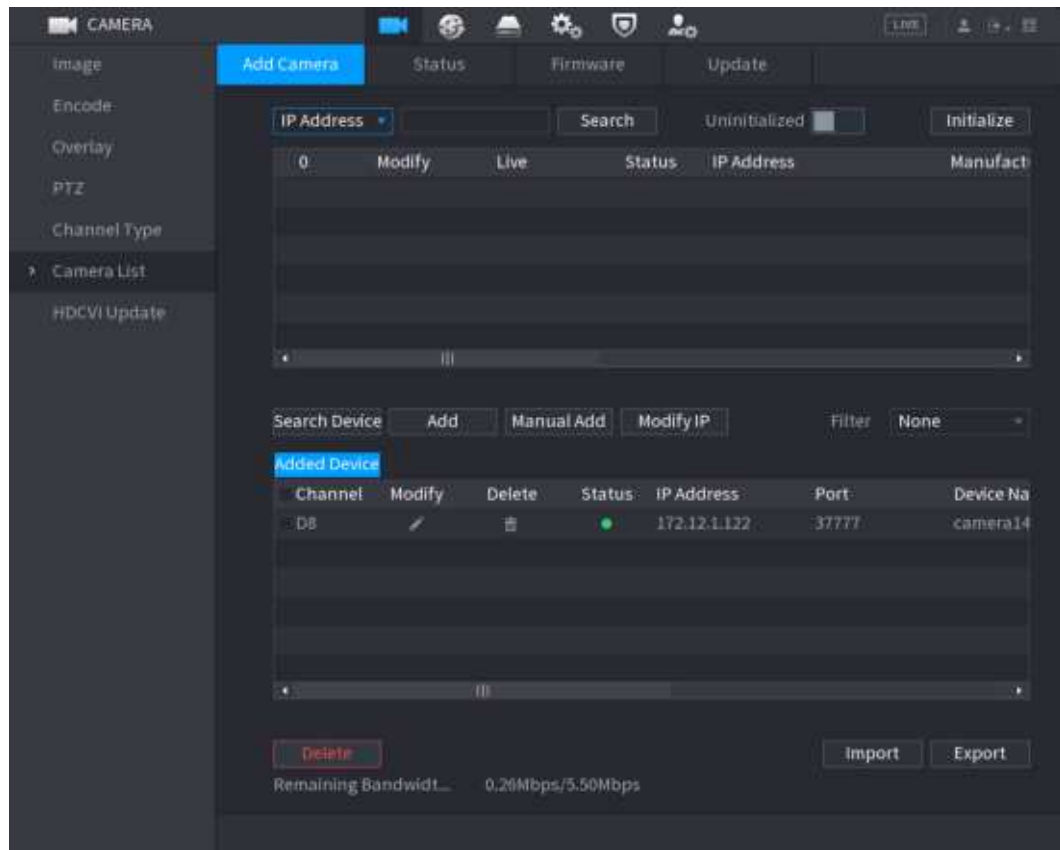


Table 5-30

Parameter	Description
Uninitialized	Enable the Uninitialized function, the uninitialized devices out of the searched devices are displayed in the searched device list.
Initialize	Select the uninitialized device from the uninitialized device list, and the click Initialize to start initializing device.
Filter	In the Filter list, select the remote device type that you want to display in the searched device list. - None: Display all types of devices. - IPC: Display the front-end devices. - DVR: Display all storage devices such as NVR, DVR and HCVR. - OTHER: Display the devices that do not belong to IPC or DVR type.
Searched Device List	Displays the searched devices. You can view the device information such as status, IP address.
Search	Click Search, the searched devices display in the searched device list. To adjust the display sequence, in the title line, you can click the IP address, Type or Device Name text. For example, click the IP address text, the sequence icon  is displayed.  is displayed next to the added device.
Add	In the Searched Device List area, select the device that you want to add.

Parameter	Description
Manual Add	Add the device by manually configuring settings such as IP address, channel selection. For details, see "5.6.1.3 Adding Remote Devices Manually."
Added Device List	Displays the added devices. You can edit and delete the device, and view the device information.
Delete	Select the check box of the added device, and then click Delete to delete the added device.
Import	Select the searched devices and then click Import to import the devices in batches.
Export	Select the added devices and then click Export . The exported devices information is saved into the USB storage device.

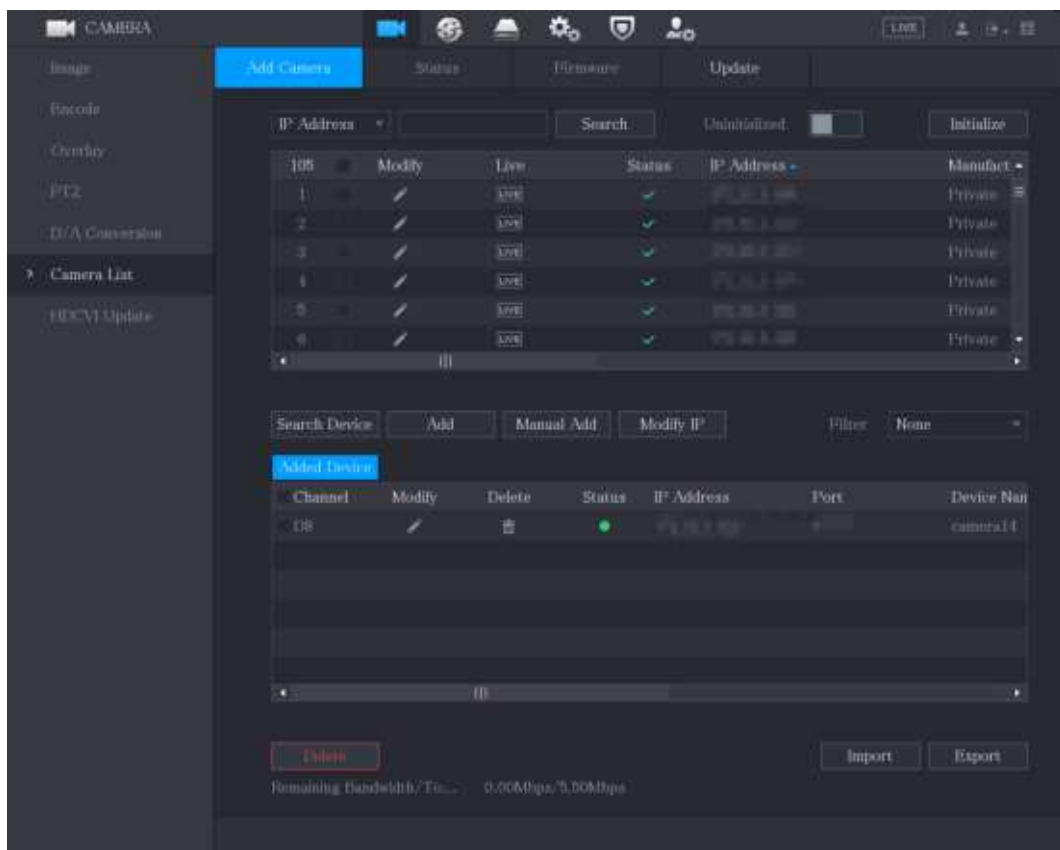
5.6.1.1 Initializing Remote Devices

You can reset the password and IP address of the remote devices through initializing.

Step 1 Click **Search Device**.

The devices found are displayed in the table.

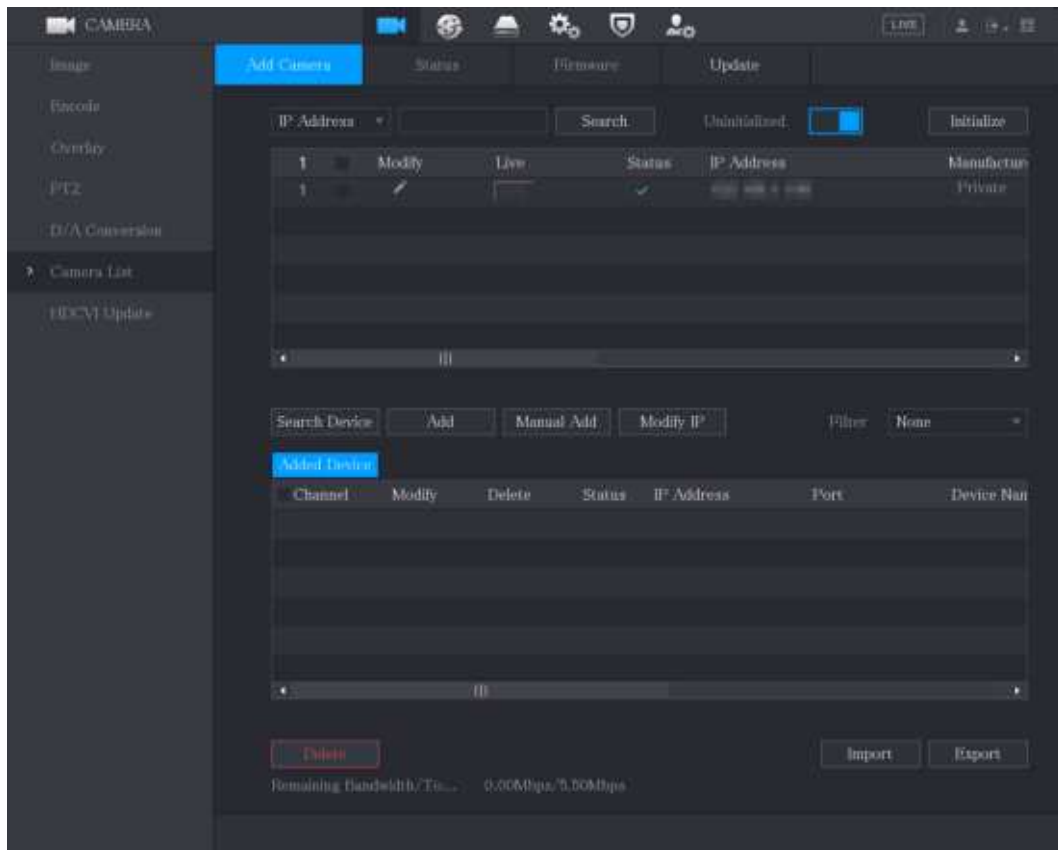
Figure 5-79



Step 2 Enable the Initialized function.

The uninitialized devices are displayed.

Figure 5-80

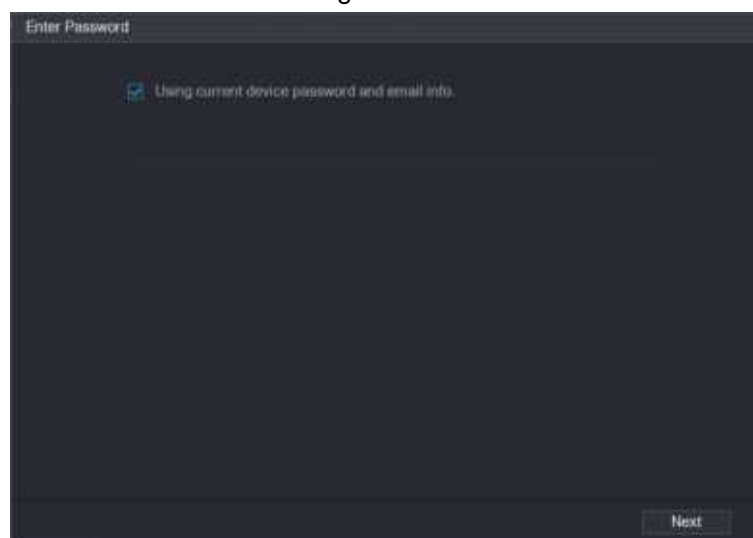


Step 3 Select the uninitialized device that you want to initialize.

Step 4 Click **Initialize**.

The **Enter Password** interface is displayed.

Figure 5-81



Step 5 Configure the password and email information.



If you select the **Using current device password and email info** check box, the remote device automatically uses the current password and email information, so you do not need to set the password and email address again and can go to Step 6.

1) Clear the Using current device password and email info check box.

The password setting interface is displayed.

Enter Password

☐ Using current device password and email info.

Useradmin

Password

Use a password that has 8 to 32 characters, it can be a combination of letter(s), number(s) and symbol(s) with at least two kinds of them (please do not use special symbols like " " ; , . ! ~)

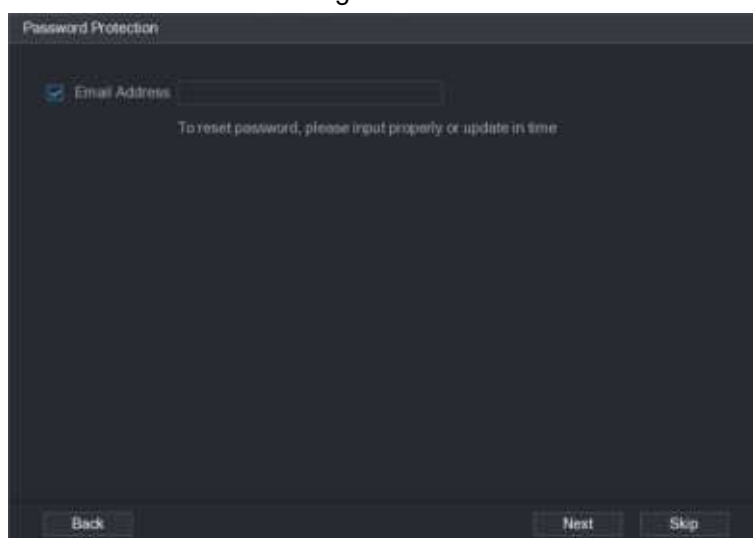
Confirm Password

Next

- Table 5-31

Parameter	Description
User	The default is admin.
Password	The new password can be set from 8 characters through 32 characters and contains at least two types from number, letter and special characters (excluding "", "", ";", ":" and "&"). Please enter a strong password according to the password strength bar indication.
Confirm Password	

- Figure 5-83



- 

Step 6 Click **Next**.

Local Configurations 103

Figure 5-84

The screenshot shows a 'NETWORK' configuration window. At the top, it says 'Checked Device No.: 1'. Below this, there are two radio buttons: 'DHCP' (unselected) and 'STATIC' (selected). Under the 'STATIC' option, there are four input fields for 'IP Address', 'Subnet Mask', 'Default Gateway', and 'Incremental Value'. The 'IP Address' field is currently set to '192.168.1.1', 'Subnet Mask' is '255.255.255.0', 'Default Gateway' is '192.168.1.1', and 'Incremental Value' is '1'. Below these fields is a table with two columns: 'IP Address' and 'Subnet Mask'. The first row shows '1' in the 'IP Address' column and '192.168.1.1' in the 'Subnet Mask' column. At the bottom of the window, there are three buttons: 'Back', 'Next', and 'Skip'.

Step 7 Configure the IP address.

- Select the **DHCP** check box, you do not need to enter the IP address information, because the system will allocate one IP address to the remote device.
- Select the **STATIC** check box, you need to enter the IP address, subnet mast, default gateway, and incremental value. The system will allocate the IP address to the remote devices by progressively increasing the last part of the IP address when initializing devices in batches.

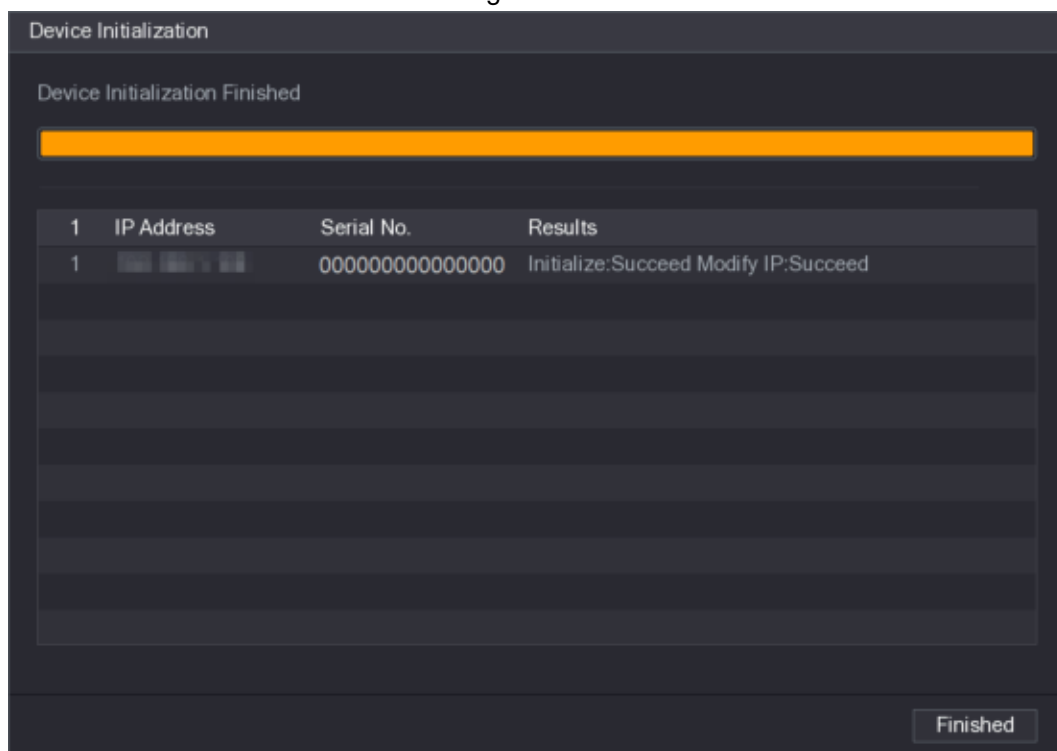


When configuring IP address for multiple remote devices which were not in the same network segment, these remote devices will belong to the same network segment after configuration.

Step 8 Click **Next**.

The initializing is started. After the process is completed, see Figure 5-85.

Figure 5-85

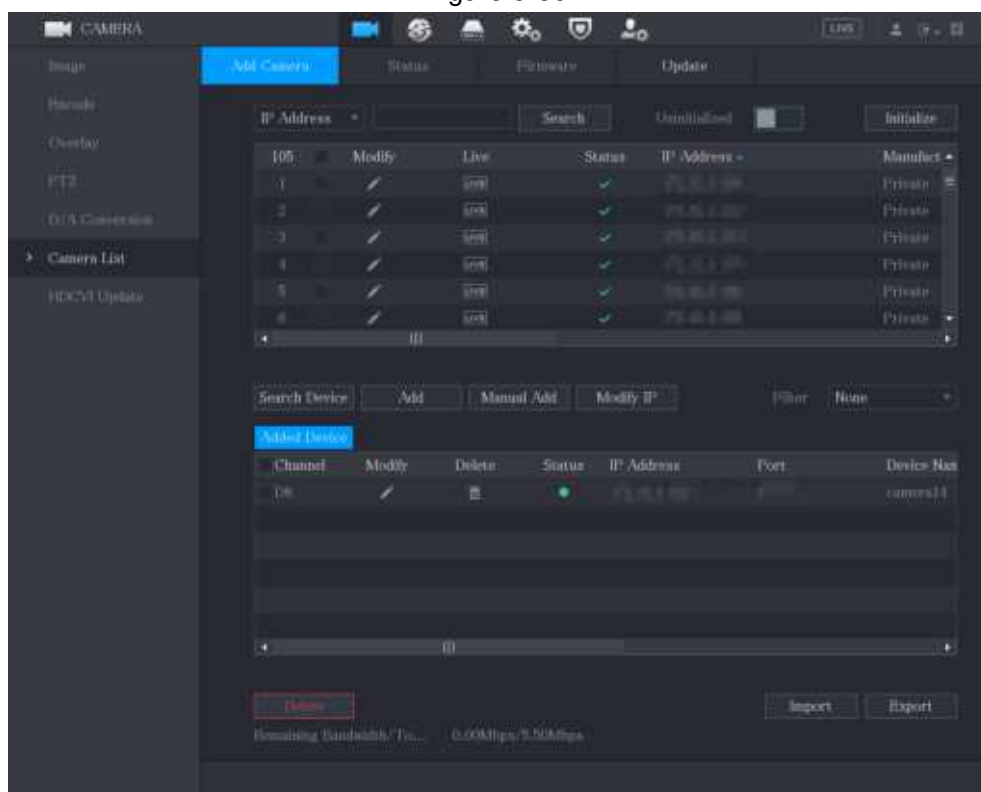


Step 9 Click **Finished** to complete the settings.

5.6.1.2 Adding Remote Devices Automatically

Step 1 On the **Registration** interface, click **Device Search**
The devices found are displayed.

Figure 5-86



Step 2 Select the check box of the device.

Step 3 Click **Add**.

The device is added into the **Added Device** area.



- You can also double-click the device to add it into the **Added Device** area.
- You can add devices in batches.

5.6.1.3 Adding Remote Devices Manually

Step 1 On the **Add Camera** interface, click **Manual Add**.

The **Manual Add** interface is displayed.

Figure 5-87

Step 2 Configure the settings for the manual adding device parameters.

Table 5-32

Parameter	Description
Channel	In the Channel list, select the channel that you want use on the Device to connect the remote device.
Manufacturer	In the Manufacturer list, select the manufacturer of the remote device.
IP Address	In the IP Address box, enter the IP address of remote device. The default is 192.168.0.0 which the system cannot connect to.
RTSP Port	The default value setting is 554. You can enter the value according to your actual situation.
HTTP Port	The default value setting is 80. You can enter the value according to your actual situation. If you enter other value, for example, 70, and then you should enter 70 after the IP address when logging in the Device by browser.
TCP Port	The default value setting is 37777. You can enter the value according to your actual situation.
User Name	Enter the user name of the remote device.

Parameter	Description
Password	Enter the password of the user for the remote device.
Remote CH No.	Enter the remote channel number of the remote device that you want to add.
Decoder Strategy	In the Decoder Strategy list, select Default , Realtime , or Fluent .
Protocol Type	- If the remote device is added through private protocol, the default type is TCP. - If the remote device is added through ONVIF protocol, the system supports Auto, TCP, UDP, or MULTICAST. - If the remote device is added through other manufacturers, the system supports TCP and UDP.
Encryption	If the remote device is added through ONVIF protocol, enabling the Encryption check box will provide encryption protection to the data being transmitted.  To use this function, the HTTPS function should be enabled for the remote IP camera.

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



- Only one device can be added manually at one time.
-  indicates successful connection and  indicates connection failed.

5.6.1.4 Modifying or Deleting Remote Devices

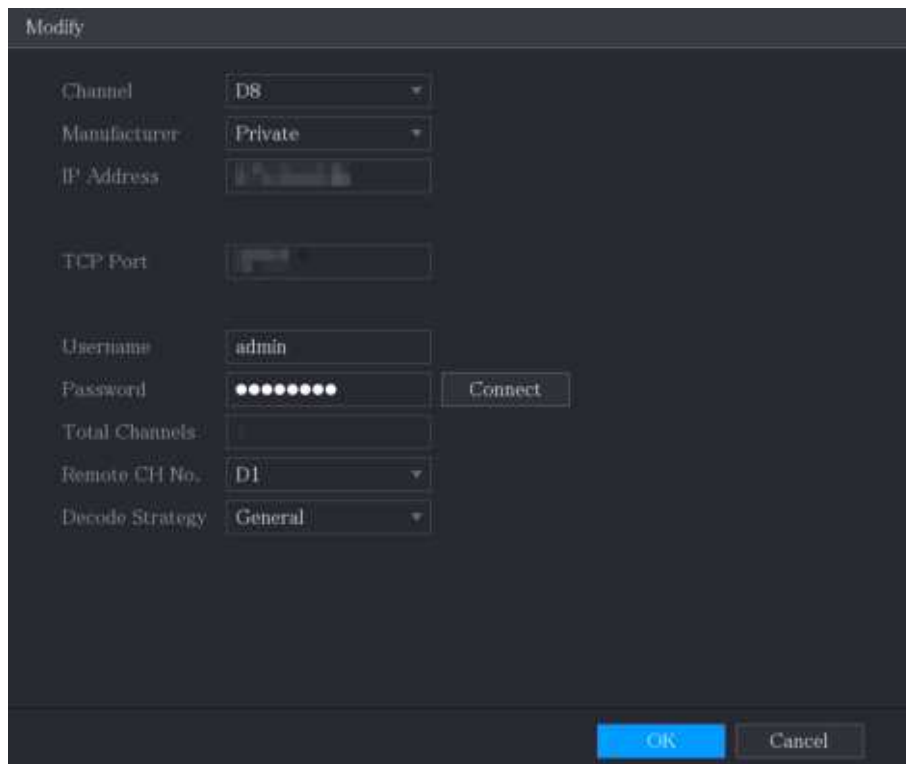
You can modify and delete the added devices.

- To modify the remote devices, do the following:

Step 1 Click  or double-click a device.

The **Modify** interface is displayed.

Figure 5-88



Step 2 In the **Channel** list, select the channel that you want to modify settings for.

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

- To delete one or more added devices, do the following:
 - ◇ Click  to delete one device.
 - ◇ Select the check box of the devices that you want to delete, and then click **Delete**.

5.6.1.5 Modifying IP Address

You can modify a single IP address or multiple IP addresses of remote devices at one time.



You can only modify the IP address of initialized cameras.

- To modify a single IP address, do the following:

Step 1 In the Searched Device list area, click  for the device that you want to modify IP.

The **Modify IP** interface is displayed.

Figure 5-89

Modify IP

Selected Device Quantity: 1

☐ DHCP ☒ Static

Username: admin Password:

IP Address: . . . Incremental Value: 1

Subnet Mask: . . .

Default Gateway: . . .

1	SN	IP Address
1		

OK Cancel

Step 2 Configure the settings for IP address, subnet mask, default gateway, user name, and password.

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

- To modify IP address in batches, do the following:

Step 1 In the Searched Device list area, select the devices that you want to modify IP address in batches.

Step 2 Click .

The **Modify IP** interface is displayed.

Figure 5-90

Modify IP

Selected Device Quantity: 4

☐ DHCP ☒ Static

Username: admin Password:

IP Address: . . . Incremental Value: 1

Subnet Mask: . . .

Default Gateway: . . .

4	SN	IP Address
1		
2		
3		
4		

OK Cancel

Step 3 Set incremental value.



The system will add the incremental value to the fourth segment of IP addresses of selected devices.

Step 4 Configure the settings for start IP address (the IP address is allocated in sequence), subnet mask, default gateway, user name, and password.

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

5.6.1.6 Exporting IP Address

You can export the added IP address to the USB storage device.



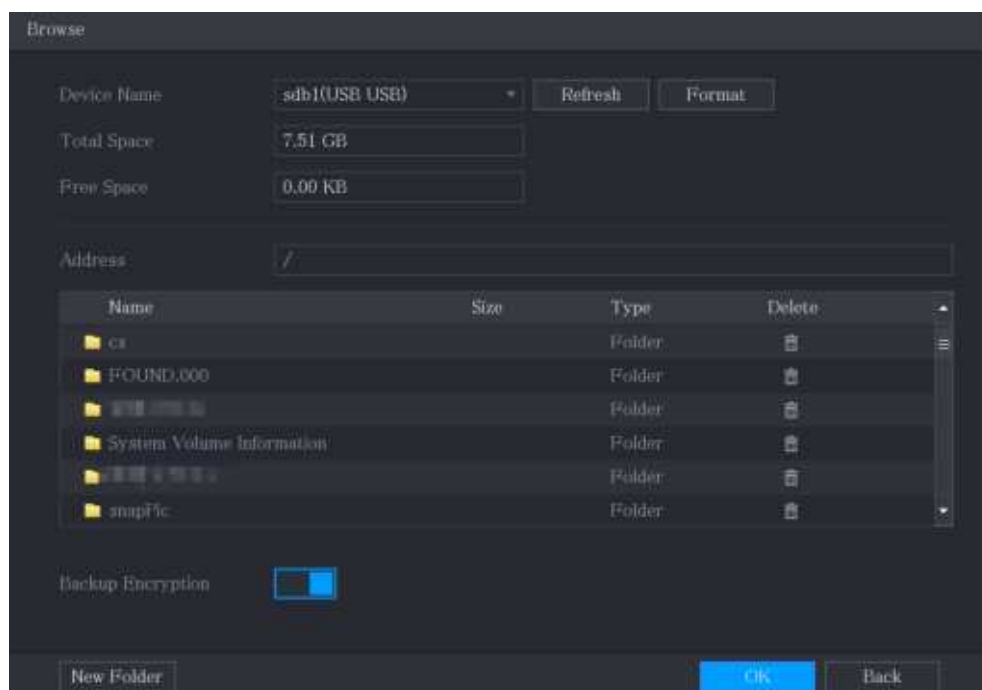
The exported information is saved in .csv file, which includes IP address, port number, channel number, manufacturer, user name, and password.

Step 1 Insert the USB storage device to the USB port of the Device.

Step 2 Click **Export**.

The **Browse** interface is displayed.

Figure 5-91



Step 3 Configure the save path.

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

A pop-up message indicating "Successfully exported" is displayed.

Step 5 Click **OK**.



When exporting IP address, the **Backup Encryption** check box is selected by default. The file information includes IP address, port, channel number, manufacturer, user name, and password.

- If you select the **Backup Encryption** check box, the file format is .backup.
- If you clear the **Backup Encryption** check box, the file format is .csv. In this case, there might be a risk of data leakage.

5.6.1.7 Importing IP Address

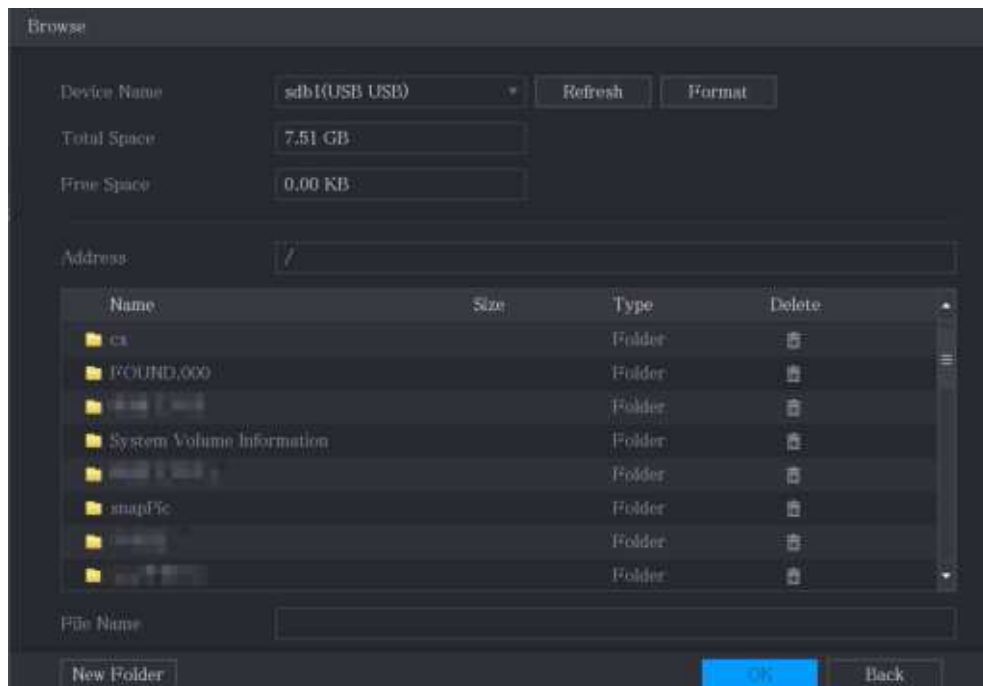
You can add remote devices by importing IP address information.

Step 1 Insert the USB storage device to the USB port of the Device.

Step 2 Click **Import**.

The **Browse** interface is displayed.

Figure 5-92



Step 3 Select the file that you want to import.

Step 4 Click **OK** to start importing.

After importing is completed, a pop-up message indicating "The import succeeded" is displayed.



If the IP address that you want to import already exists in the Device, the system will pop up a message to ask you whether to overwrite the existing content.

- Click OK to replace the existing one.
- Click Cancel to add it as a separate device in the Added Device area.



- You can edit the exported .csv file and be cautious not to change the file format; otherwise the file cannot be imported as it will be judged as invalid.
- The language of .csv file must match the Device language.
- The import and export through customized protocol is not supported.

5.6.2 Managing Remote Devices

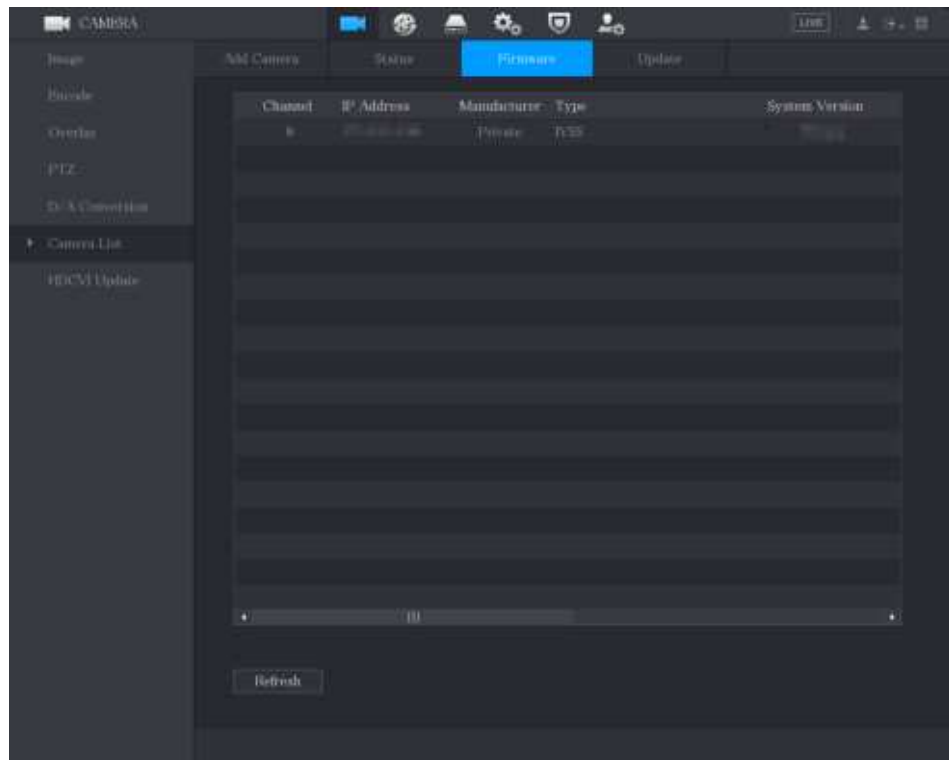
You can view the status of remote devices and upgrade.

5.6.2.1 Viewing Status

You can view the device information such as connection status, IP address, motion detection, video loss detection, camera name, and manufacturer.

Select **Main Menu > CAMERA > Camera List > Status**, the **Status** interface is displayed.

Figure 5-93

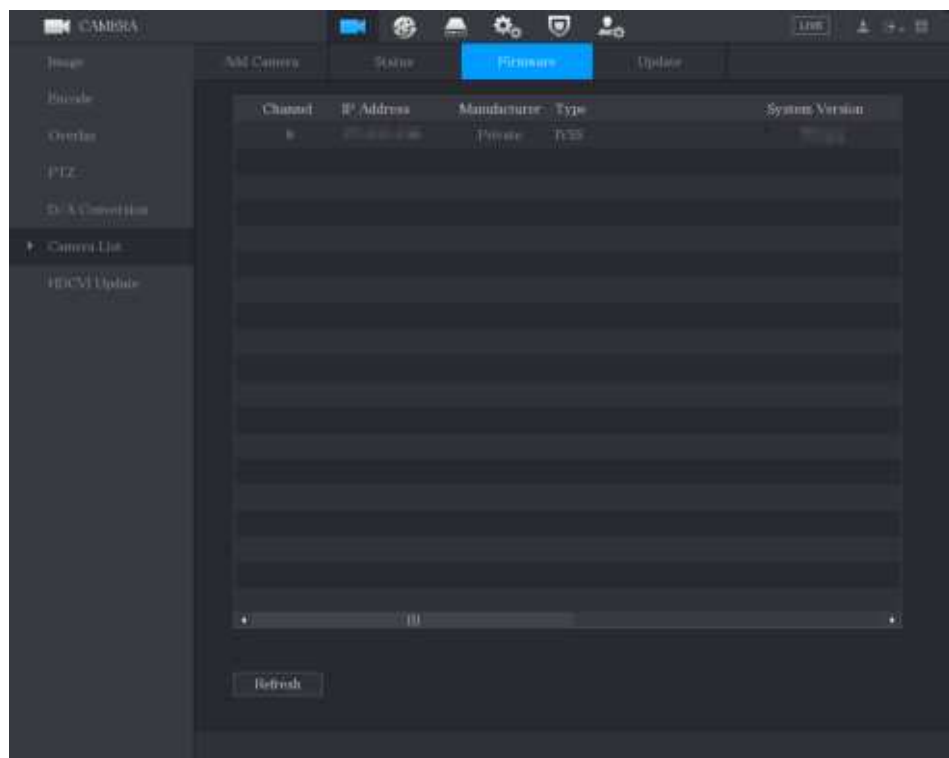


5.6.2.2 Viewing Firmware Information

You can view the device firmware information such as channel number, IP address, manufacturer, system version, video input, audio input, and alarm in.

Select **Main Menu > CAMERA > Camera List > Firmware**, the **Firmware** interface is displayed.

Figure 5-94

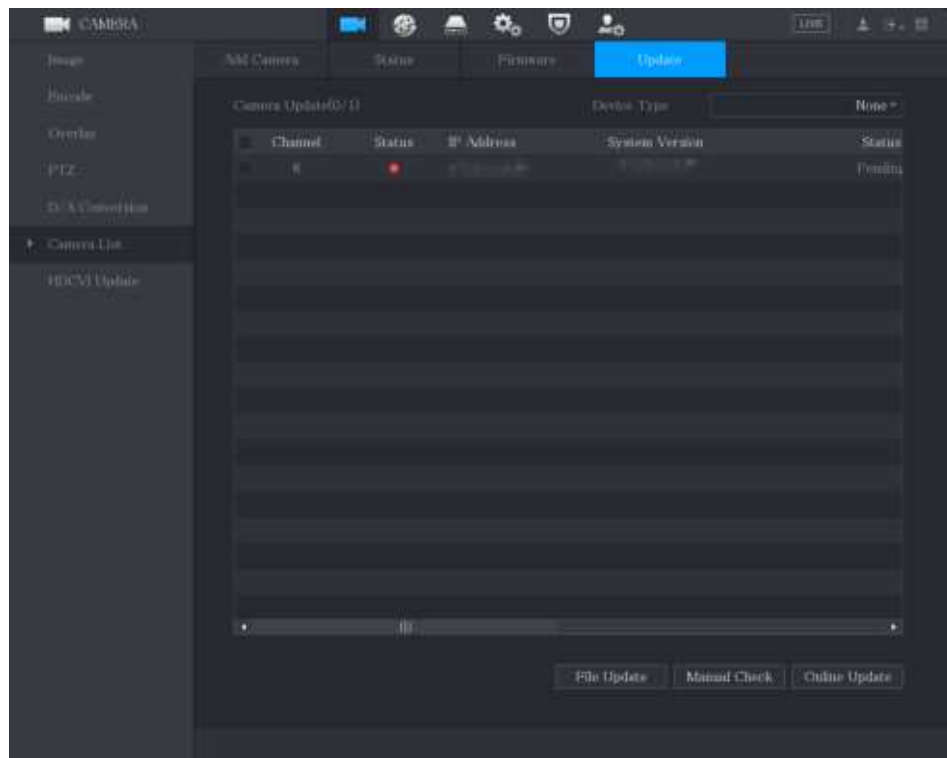


5.6.2.3 Upgrading Remote Devices

Step 1 Select **Main Menu > CAMERA > Camera List > Update**.

The **Update** interface is displayed.

Figure 5-95



Step 2 Upgrade the device.

- File Update

- 1) Insert a USB storage device containing the upgrade files into the USB port of the Device.

- 2) Select the devices that you want to upgrade.

- 3) Click **File Update**.

The **File Update** interface is displayed.

- 4) Select the upgrading files and click **Apply**.

- Online Update

- 1) Click **Detect** or select the check box the device that you want to upgrade and click **Manual Check**.

The system starts detecting if there is a new version on the online server.

- 2) Select the check box of all the devices that have new version.

- 3) Click **Online Update**.



- The system will pop up a message to indicate if the upgrading is successful.
- You can use the Type list to filter the devices so that you can find the devices quickly.

5.7 Configuring Record Settings

You can record video manually or automatically and configure the recording settings to main stream and sub stream respectively.

5.7.1 Enabling Record Control



- Manual recording operation requires the user have the permission to access **STORAGE** settings.
- Check to ensure the HDD installed in the Device has been formatted properly.

To enter the record control interface, do the following:

Step 1 Right-click on the live view screen, the shortcut menu is displayed. On the shortcut menu, select **Manual Control > Record Control**.

The **Record Mode** interface is displayed.

Figure 5-96

Step 2 Configure the settings for the record control parameters.

Table 5-33

Parameter	Description
Channel	Displays all the analog channels and the connected digital channels. You can select a single channel or select All .
Main Stream/Sub Stream	• Auto: Automatically record according to the record type and recording time as configured in the recording schedule. • Manual: Keep general recording for 24 hours for the selected channel. • Stop: Do not record.
Snapshot	Enable or disable the scheduled snapshot for the corresponding channels.

Step 3 Click **Apply**.

5.7.2 Configuring Recorded Video Storage Schedule

You need to configure the storage schedule for the recorded video so that the recorded video can be saved. For details, see "5.1.4.9 Configuring Recorded Video Storage Schedule."

5.8 Configuring Snapshot Settings

5.8.1 Configuring Snapshot Trigger

The snapshot is divided into scheduled snapshot, event triggered snapshot, and face detection triggered snapshot. When the both are enabled, the event triggered snapshot has the priority.

- If there is no alarm event, the system performs scheduled snapshot.
- If there is any alarm event, the system performs event triggered snapshot.

5.8.1.1 Configuring Scheduled Snapshot

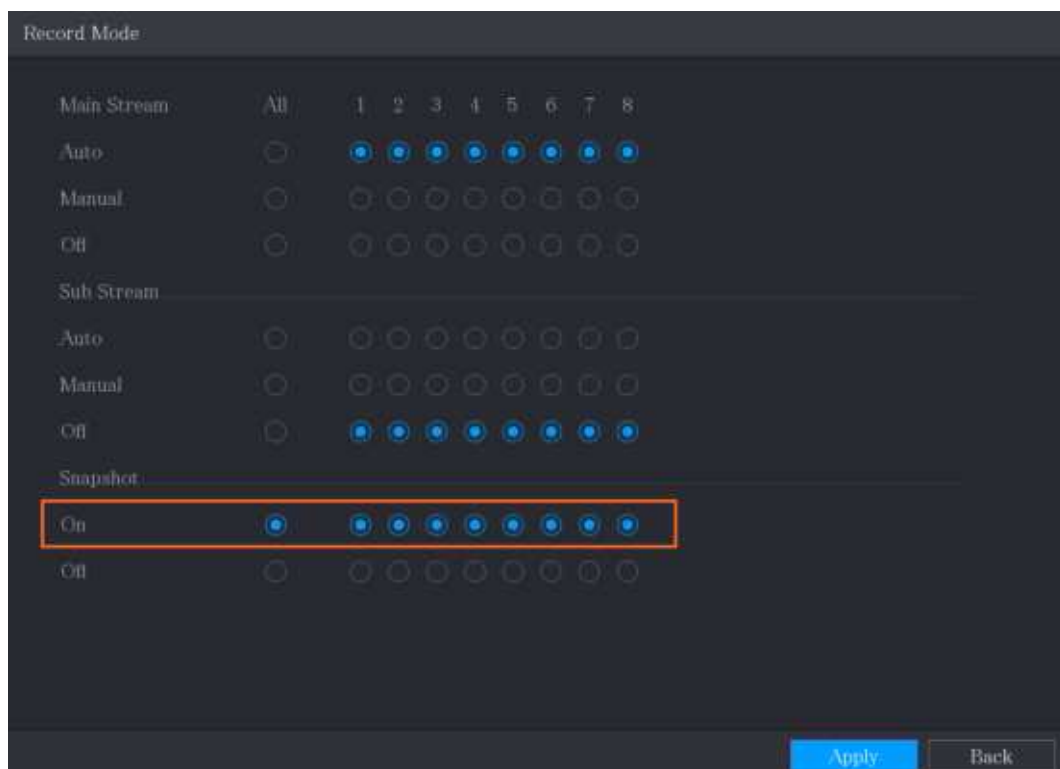
Step 1 Right-click on the live view screen, the shortcut menu is displayed.

Step 2 On the shortcut menu, select **Manual Control > Record Control**.

The **Record Mode** interface is displayed.

Step 3 In the **Snapshot** area, enable the snapshot for the channels if needed.

Figure 5-97



Step 4 Select **Main Menu > CAMERA > Encode > Snapshot**.

The **Snapshot** interface is displayed.

Step 5 In the **Type** list, select **Scheduled**, and then configure other parameters.

Figure 5-98

The screenshot shows the 'Snapshot' configuration tab. At the top, there are three tabs: 'Audio/Video', 'Snapshot' (selected), and 'Encode Enhanc...'. Below the tabs, there are several configuration options: 'Manual Snapshot' (set to 1), 'Channel' (set to 1), 'Type' (set to Scheduled and highlighted with a red box), 'Size' (set to 352x288(CIF)), 'Quality' (set to 4), and 'Interval' (set to 1 sec.).

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

- If you have configured the snapshot schedule, the configuration has been completed.
- If you have not configured the snapshot schedule, see "5.1.4.10 Configuring Snapshot Storage Schedule."

5.8.1.2 Configuring Event Triggered Snapshot

Step 1 Select **Main Menu > CAMERA > Encode > Snapshot**.

The **Snapshot** interface is displayed.

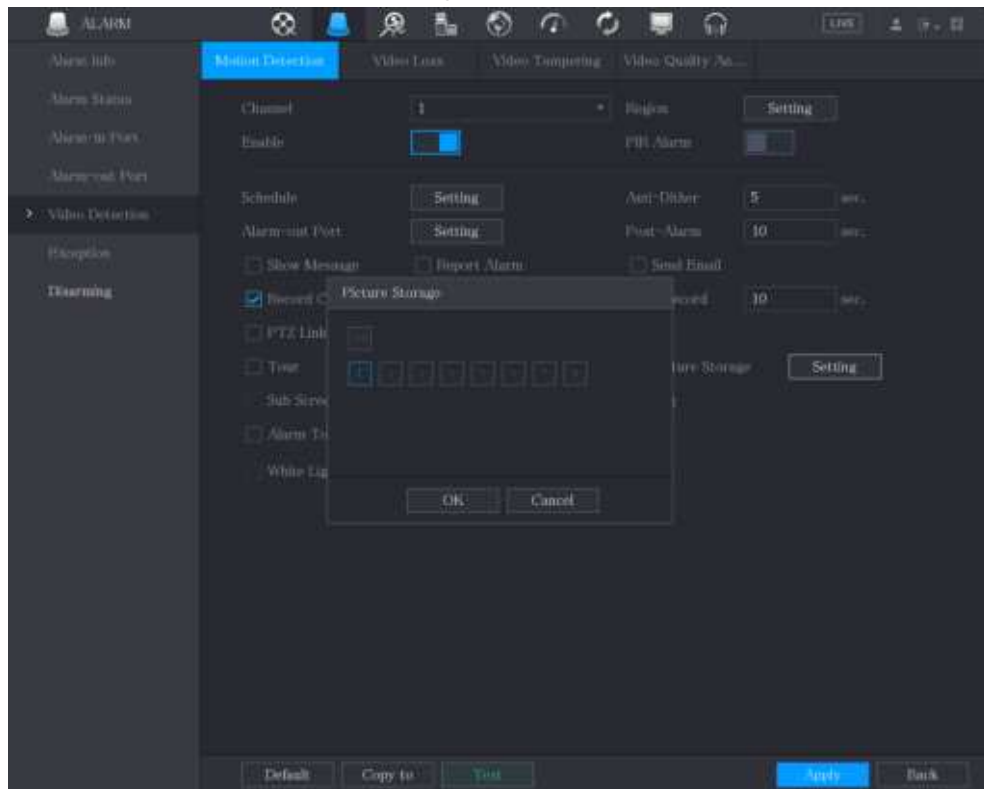
Step 2 In the **Type** list, select **Event**, and then configure other parameters.

Figure 5-99

The screenshot shows the 'Snapshot' configuration tab. At the top, there are three tabs: 'Audio/Video', 'Snapshot' (selected), and 'Encode Enhanc...'. Below the tabs, there are several configuration options: 'Manual Snapshot' (set to 1), 'Channel' (set to 1), 'Type' (set to Event and highlighted with a red box), 'Size' (set to 352x288(CIF)), 'Quality' (set to 4), and 'Interval' (set to 1 sec.).

Step 3 Select **Main Menu > ALARM > Video Detection**, and select the event type to configure, for example, select the **Motion Detection** tab.

Figure 5-100



Step 4 Click **Setting** next to **Picture Storage** check box and select the corresponding channel

Step 5 Click **Apply**.

5.8.2 Configuring Snapshot Storage Schedule

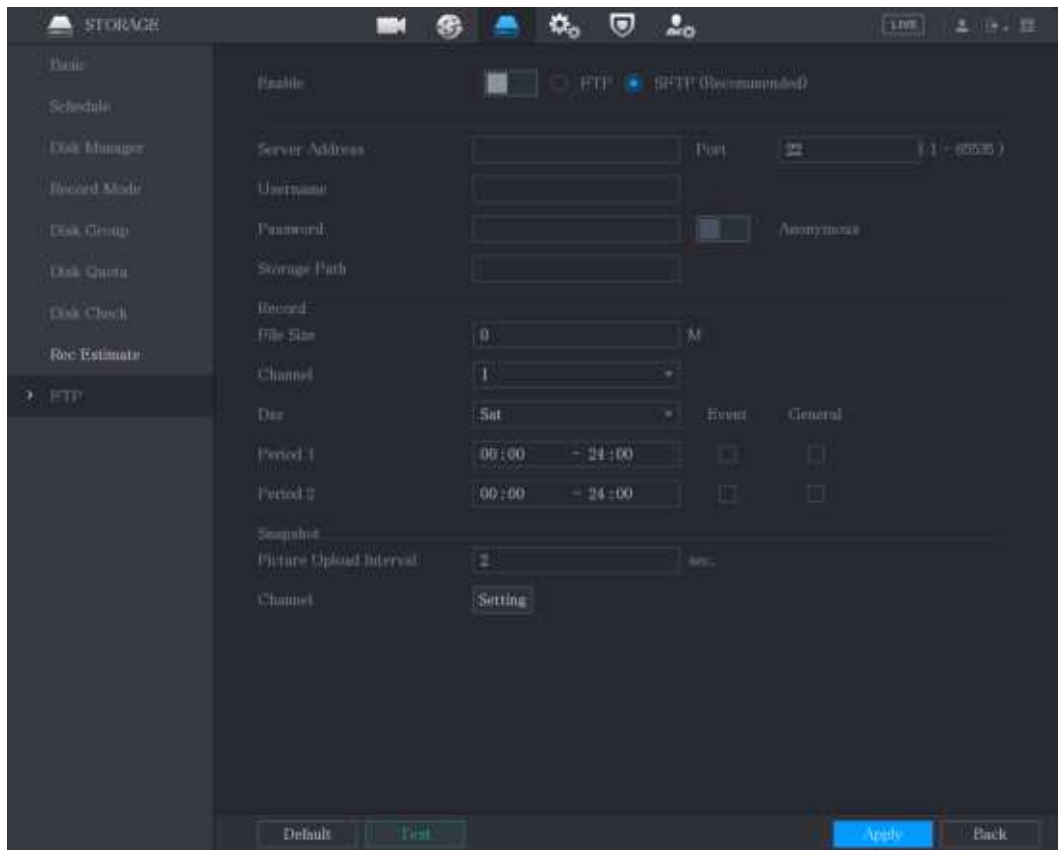
You need to configure the storage schedule for the snapshot so that the snapshot can be saved. For details, see "5.1.4.10 Configuring Snapshot Storage Schedule."

5.8.3 Backing up Snapshots to FTP

Step 1 Select **Main Menu > STORAGE > FTP**.

The **FTP** interface is displayed.

Figure 5-101



Step 2 Enable the FTP function and configure the parameters. For details, see "5.18.9 Configuring FTP Storage Settings."

The snapshots will be uploaded to FTP for backup.

5.9 Playing Back Video

5.9.1 Enabling Record Control



- Manual recording operation requires the user have the permission to access **STORAGE** settings.
- Check to ensure the HDD installed in the Device has been formatted properly.

To enter the record control interface, do the following:

Step 1 Right-click on the live view screen, the shortcut menu is displayed. On the shortcut menu, select **Manual Control > Record Mode**. The **Record Mode** interface is displayed.

Figure 5-102

The screenshot shows a 'Record Mode' configuration window. It has three main sections: 'Main Stream', 'Sub Stream', and 'Snapshot'. Each section has a mode selector (All, Auto, Manual, Off) and a grid of 8 channels. In the 'Main Stream' section, 'All' is selected, and all 8 channels are set to 'Auto'. In the 'Sub Stream' section, 'Off' is selected, and all 8 channels are set to 'Off'. In the 'Snapshot' section, 'Off' is selected, and all 8 channels are set to 'Off'. At the bottom right, there are 'Apply' and 'Back' buttons.

Step 2 Configure the settings for the record control parameters.

Table 5-34

Parameter	Description
Channel	Displays all the analog channels and the connected digital channels. You can select a single channel or select All .
Main Stream/Sub Stream	• Auto: Automatically record according to the record type and recording time as configured in the recording schedule. • Manual: Keep general recording for 24 hours for the selected channel. • Stop: Do not record.
Snapshot	Enable or disable the scheduled snapshot for the corresponding channels.

5.9.2 Instant Playback

You can use the instant playback function to play back the previous five minutes to sixty minutes of the recorded video in any channel. For details about instant playback function, see "5.2.2.1 Instant Playback."

5.9.3 Main Interface of Video Playback

You can search for and play back the recorded video saved on the Device.

Select **Main Menu > Search**, the video search interface is displayed.

Figure 5-103

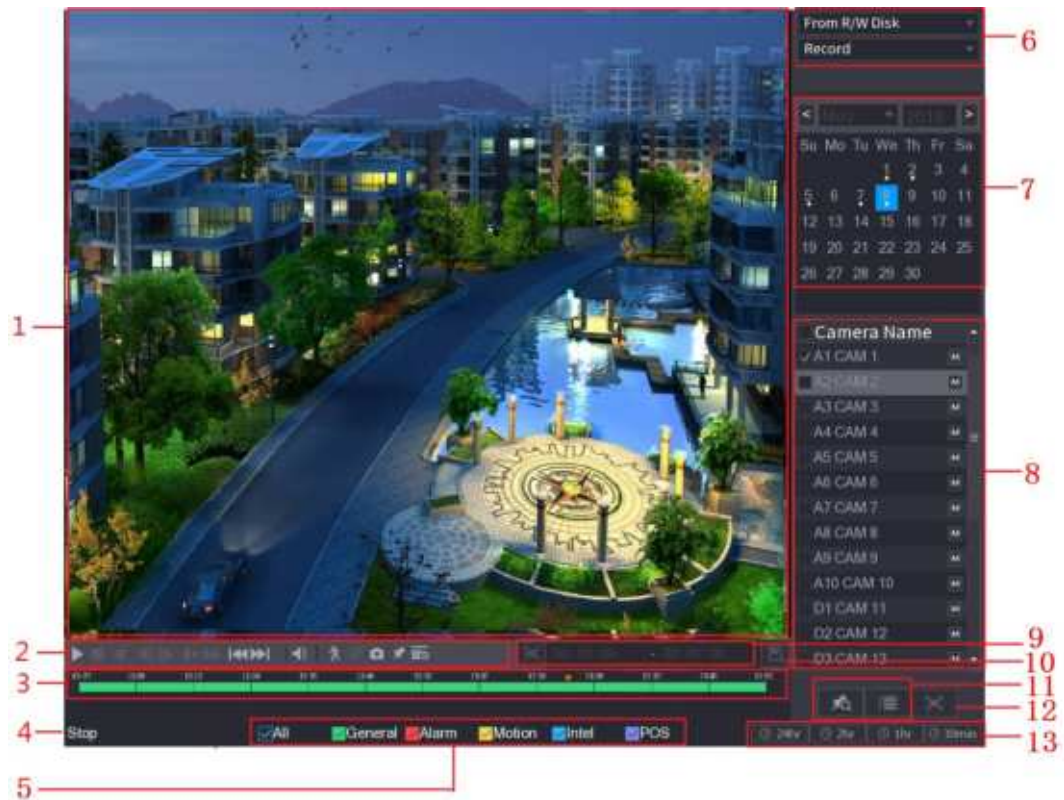


Table 5-35

No.	Function	Description
1	Display Window	Display the searched recorded video or picture. Supports simultaneously playing in single-channel, 4-channel, 9-channel, and 16-channel.  When playing back in a single channel, click and hold to select the area that you want to enlarge. The area is enlarged after the left mouse button is released. To exit the enlarged status, right-click on the image.
2	Playback Controls Bar	Playback control buttons. For details about the control buttons, see "5.9.3.1 Introducing Playback Controls."

No.	Function	Description
3	Time Bar	Display the type and time period of the current recorded video. • In the 4-channel layout, there are four time bars are displayed; in the other view layouts, only one time bar is displayed. • Click on the colored area to start playback from a certain time. • In the situation when you are configuring the settings, rotate the wheel button on the time bar, the time bar is zooming in from 0. In the situation when playback is ongoing, rotate the wheel button on the time bar, the time bar is zooming from the time point where the playback is located. • Time bar colors: Green indicates general type; Red indicates external alarm; Yellow indicates motion detection; Blue indicates intelligent events; Purple indicates POS events. • For some models, when you are clicking on the blank area in the time bar, the system automatically jumps to the next time point where there is a recorded video located. • Click and hold the time bar, and the mouse pointer shall change to a hand icon, and then you can drag to view the playback of the target time. • You can drag the vertical orange line on the time bar to rapidly view the playback in iframe format. • When playing back video in one channel mode, you can move mouse pointer to time bar to display thumbnail pictures for the video of target time. • When playing back video, you can select other channels as needed. The time bar of newly added channels will be added up to the time bar of earlier base channels. The type and time period of newly added channels are the same with early base channels.
4	Play Status	Includes two playback status: Play and Stop .
5	Record type	Select the check box to define the recording type to search for.
6	Search type	Select the content to play back: Record , Picture , Subperiod . For details about the selecting search type, see "5.9.3.2 Selecting Search Type."
7	Calendar	Click the date that you want to search, the time bar displays the corresponding record. The dates with record or snapshot have a small solid circle under the date.

No.	Function	Description
8	View Layout and Channel Selection	In the Camera Name list, select the channel(s) that you want to play back. - The window split is decided by how you select the channel(s). For example, if you select one channel, the playback is displayed in the single-channel view; if you select two to four channels, the playback is displayed in the four-channel view. The maximum is eight channels. - Click  to switch the streams.  indicates main stream, and  indicates sub stream.
9	Video Splice	Splice a section of recorded video and save it. For details about splicing a recorded video, see "5.9.3.3 Clipping Recorded Video."
10	Backup	Back up the recorded video files. For details, see "5.9.3.4 Backing up Recorded Video."
11	List Display	This area includes Tag List and File List. : Click the Tag List button, the marked recorded video list is displayed. Double-click the file to start playing. : Click the File List button, the searched recorded video list is displayed. You can lock the files. For details, see "5.9.9 Using the File List."
12	Full Screen	Click  to display in full screen. In the full screen mode, point to the bottom of the screen, the time bar is displayed. Right-click on the screen to exit full screen mode.
13	Time Bar Unit	You can select 24hr, 2hr, 1hr, or 30min as the unit of time bar. The time bar display changes with the setting.

5.9.3.1 Introducing Playback Controls Bar

You can perform the operations such as control the speed of playback, add mark, and take snapshots through the playback controls bar.

Figure 5-104



The play backward function and playback speed are dependent on the product version. The actual product shall govern. You can also contact the technical support to consult the hardware version information.

Table 5-36

Icon	Function
	Play/Pause. During playing back, you can switch between play and pause.
	Stop. During playing back, you can click the Stop button to stop playback.
	Play Backward. - During playing back, click the Play Backward button to backward play the recorded video, the button switches to ; click  to stop playing backward. - During playing back, click  to start playing forward.
	Previous Frame/Next Frame. - When the playback is paused, click  or click  to play single-frame recorded video. - When playing back single-frame recorded video, click  to start playing forward.
	Slow Playback. - During playing back, click  to set the speed of slow playback as SlowX1/2, SlowX1/4, SlowX1/8, or SlowX1/16. - During fast playback, click  to slow down the speed of fast playback.
	Fast Playback. - During playing back, click  to set the speed of fast playback as FastX2, FastX4, FastX8, or FastX16. - During slow playback, click  to speed up slow playback.
	Previous Day/Next Day. Click  or click  to play the previous day or next day of the current recorded video.
	Adjust volume of playback.
	Enable smart search function. For details about using the smart search, see "5.9.4 Smart Search."
	Add filter criteria of smart search. You can select Human , Vehicle , or uncheck. For details about using the smart search, see "5.9.4 Smart Search."

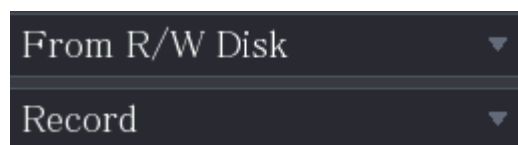
Icon	Function
	In the full screen mode, click  to take a snapshot and save into the USB storage device or mobile HDD.
	Add Mark for the recorded view. For details about adding mark, see "5.9.6 Marking and Playing Back Video."
	Show or hide POS information. During single-channel playback, click  to show or hide POS information on the screen.
	During playback, click this icon to display or hide AI rulers. For more details, see "5.9.5 Showing AI Rule during Playback."
	Show playback video in full screen.

5.9.3.2 Selecting Search Type

You can search the recorded videos, splice, or snapshots from HDD or external storage device.

- **From R/W Disk:** Recorded videos or snapshots playback from HDD of the Device.

Figure 5-105



- **From I/O Device:** Recorded videos playback from external storage device.
Click **Browse**, select the save path of recorded video file that you want to play.

Double-click the video file or click  to start playing.

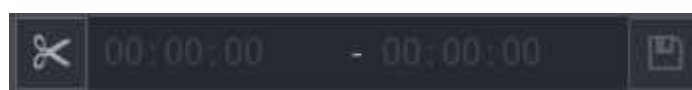
Figure 5-106



5.9.3.3 Clipping Recorded Video

During playback, clip sections of recorded video and save to the USB storage device. For the video clip interface, see Figure 5-107.

Figure 5-107



Step 1 Select a recorded video that you want to play.

- Click  to start playing from the beginning.

- Double-click anywhere in the time bar colored area to start playback.

Step 2 Click on the time bar to select the start time, and then click  to start clipping.

Step 3 Click on the time bar to select the end time, and then click  to stop clipping.

Step 4 Click .

The **BACKUP** dialog box is displayed. You can back up the files.



- You can clip the video of a single-channel or multiple channels.
- Maximum 1024 files can be backed up at one time.
- The files that are selected in the **File List** cannot be clipped.

5.9.3.4 Backing up Recorded Video

You can back up the recorded video file or splice video file into the USB storage device.

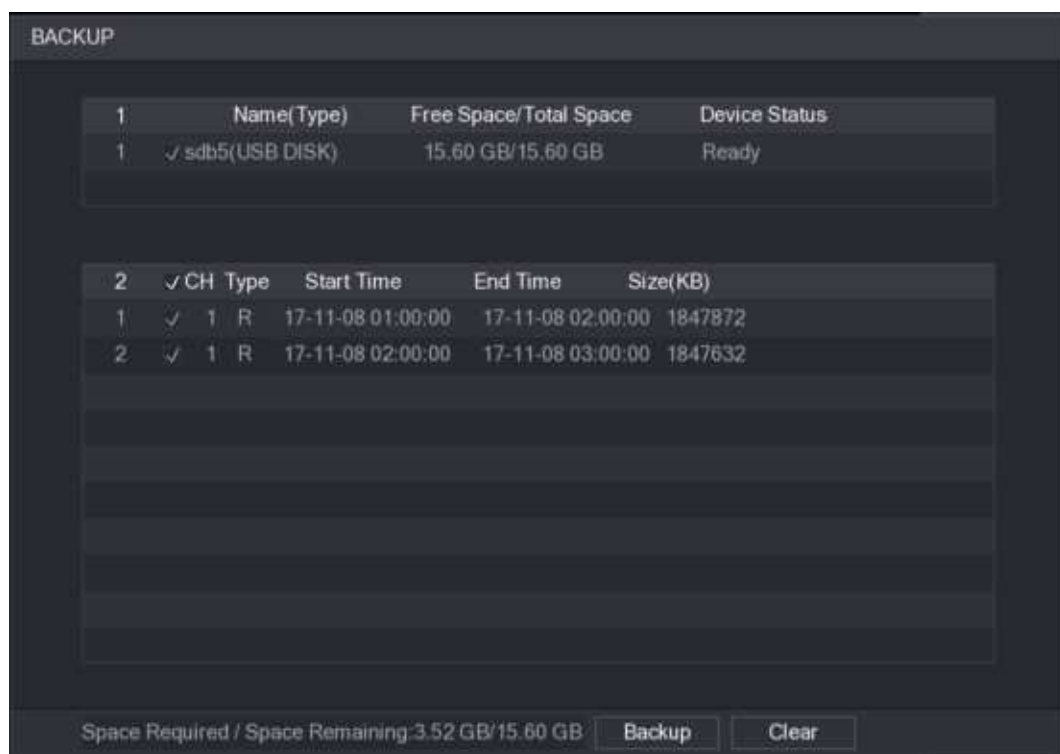
Step 1 Select the recorded video file that you want to back up. You can select the following two types of files:

- Recorded video file: Click , the **File List** area is displayed. Select the file(s) that you want to back up.
- Splice video file. For details about splicing video file, see "5.9.3.3 Clipping Recorded Video."

Step 2 Click .

The **BACKUP** dialog box is displayed.

Figure 5-108



Step 3 Click **Backup**.



If you do not want to back the file, clear the check box.

5.9.4 Smart Search

During playback, you can analyze a certain area to find if there was any motion detection event occurred. The system will display the images with motion events of the recorded video.



Not all models support this function.

To use the Smart Search function, you need to enable the motion detection for the channel by selecting **Main Menu > ALARM > Video Detection > Motion Detection**.

To use the Smart Search function, do the following:

Step 1 Select **Main Menu > SEARCH**, the video search interface is displayed.

Step 2 In the **Camera Name** list, select the channel(s) that you want to play.

Step 3 Click  or double-click anywhere in the time bar colored area to start playback.

Step 4 Click .

The grid is displayed on the screen.



- Only single-channel supports smart search.
- If multi-channels are selected, double-click on the channel window to display this channel only on the screen, and then you can start using smart search function.

Step 5 Drag the pointer to select the searching area.



The grid area supports 22×18(PAL) and 22×15(NTSC).

Step 6 Click  to add filter criteria. You can check **Human** box, **Vehicle** box, or uncheck.

- Human: Display the motion alarm of human during selected time and searching area.
- Vehicle: Display the motion alarm of vehicle during selected time and searching area.
- Unchecking: Display the general motion alarm which includes both human and vehicle, during selected time and searching area.

Step 7 Click .

The screen starts playing back the motional splices of recorded video for the selected searching area.

Step 8 Click  to exit the smart searching while playback.

5.9.5 Showing AI Rule during Playback

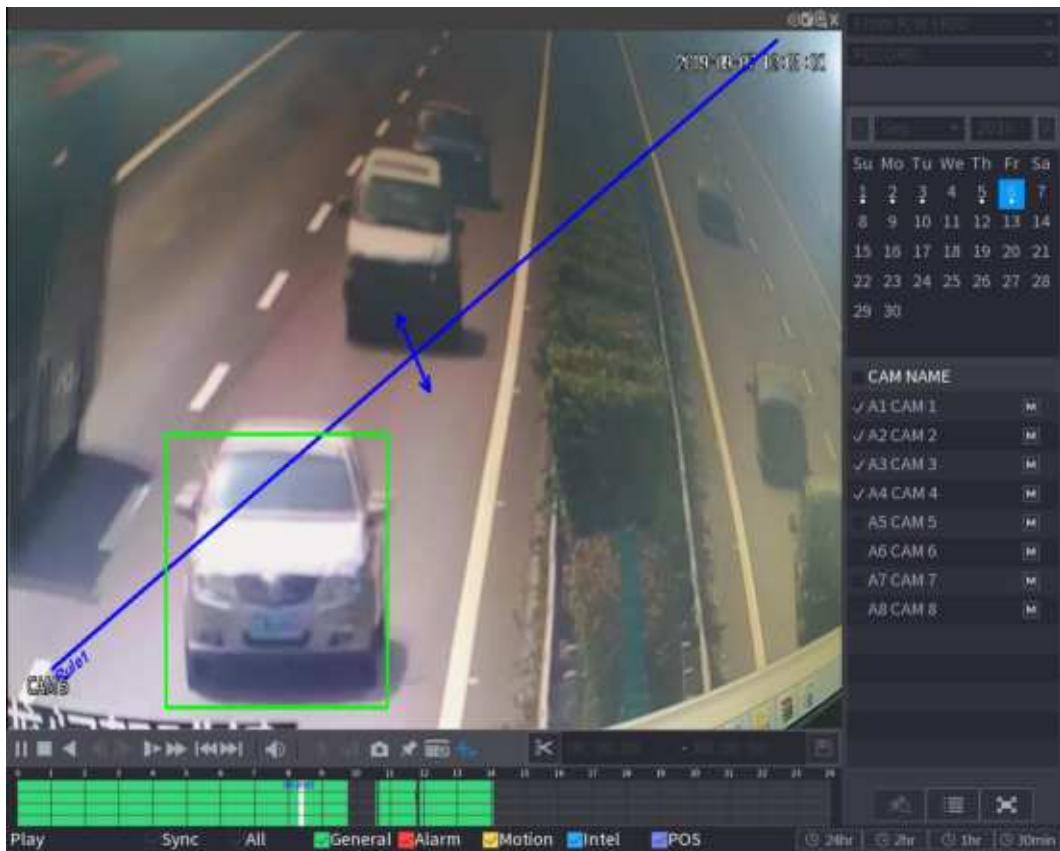
To use the AI rule showing function, do the following:

Step 1 Select **Main Menu > SEARCH**, the video search interface is displayed.

Step 2 In the **Camera Name** list, select the channel(s) that you want to play.

Step 3 Click  or double-click anywhere in the time bar colored area to start playback.
You can see the AI rule during playback. This function is enabled by default.

Figure 5-109



Click  to hide AI rule.

5.9.6 Marking and Playing Back Video

You can mark the recording for somewhere important. Then you can easily find the marked recording by searching time and mark name.

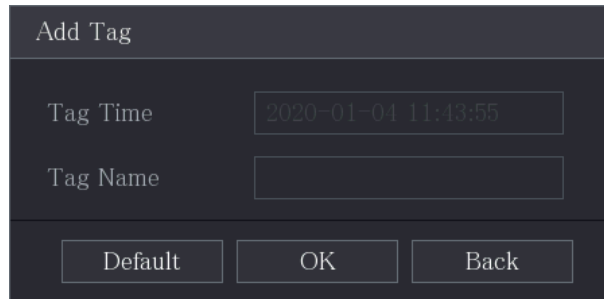
Marking a Video

Step 1 Select **Main Menu > SEARCH**, the video search interface is displayed.

Step 2 In the playback mode, click .

The **Add Tag** dialog box is displayed.

Figure 5-110

A dark-themed dialog box titled "Add Tag". It contains two input fields: "Tag Time" with the value "2020-01-04 11:43:55" and "Tag Name" which is empty. At the bottom, there are three buttons: "Default", "OK", and "Back".

Add Tag	
Tag Time	2020-01-04 11:43:55
Tag Name	
Default OK Back	

Step 3 In the **Tag Name** box, enter a name.

Step 4 Click **OK**.

This marked video file displays in the **Tag List**.

Playing Back Marked Video



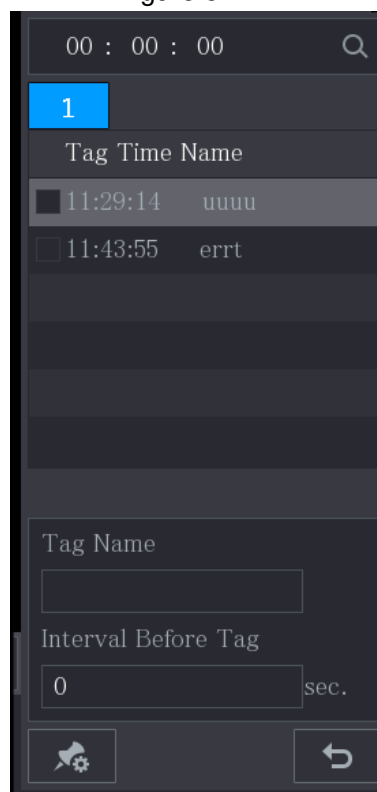
This function is supported on single-channel playback.

Step 1 In the **Camera Name** list, select one channel.

Step 2 Click .

The Mark List interface is displayed.

Figure 5-111

A dark-themed interface titled "Mark List". At the top, there is a search bar with the text "00 : 00 : 00" and a magnifying glass icon. Below the search bar is a list of items. The first item is "1" in a blue box. Below it is a section titled "Tag Time Name" containing two entries: "11:29:14 uuuu" and "11:43:55 errt". At the bottom, there is a section titled "Tag Name" with an empty input field, and a section titled "Interval Before Tag" with a value of "0" and the unit "sec.". At the very bottom, there are two icons: a magnifying glass and a circular arrow.

Step 3 Double-click the file that you want to play back.

To search the marked video by time, in the **SEARCH** box on the top of the interface, enter the time, and then click .

Playing Back Time before the Tag

You can configure to play N seconds of the tagged video before the tagged time.

Step 1 In the **Tag Name** box, enter the name of a tagged video.

Step 2 In the **Interval Before Tag** box, enter N seconds.

Step 3 Click .

The playback starts from N seconds before the tagged time.

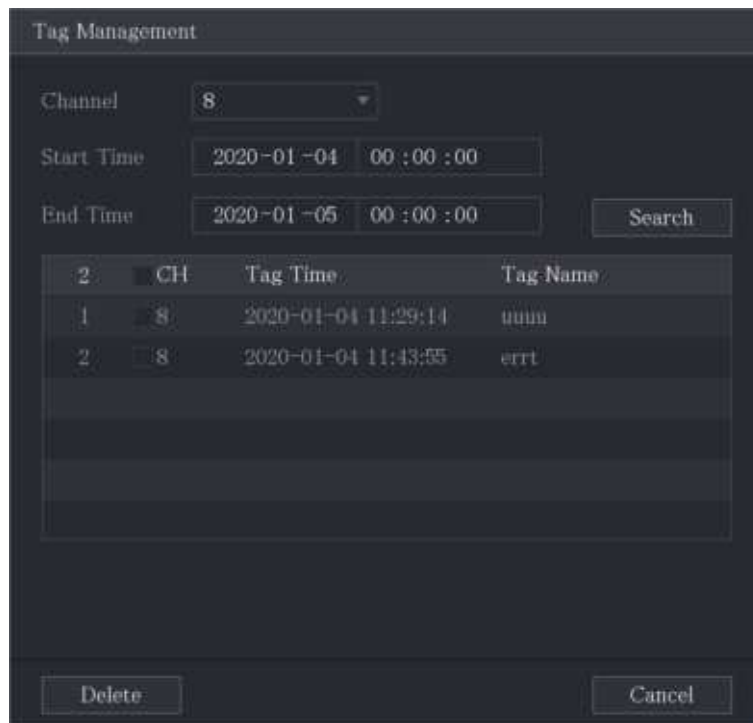


If there is N seconds exist before the marked time, the playback starts from N seconds before the tagged time. If there is not, it plays back as much as there is.

Managing Tagged Video

On the **Tag List** interface, click , the **Tag Management** interface is displayed.

Figure 5-112



The screenshot shows the 'Tag Management' dialog box. It has a title bar 'Tag Management'. Below it, there are input fields for 'Channel' (set to 8), 'Start Time' (2020-01-04 00:00:00), and 'End Time' (2020-01-05 00:00:00). A 'Search' button is to the right of the 'End Time' field. Below these fields is a table with columns: 'ID', 'CH', 'Tag Time', and 'Tag Name'. The table contains two rows of data. At the bottom of the dialog are 'Delete' and 'Cancel' buttons.

ID	CH	Tag Time	Tag Name
1	8	2020-01-04 11:29:14	uun
2	8	2020-01-04 11:43:55	errt

- Be default, it manages all the tagged videos of the selected channel.
- To search the tagged video, select channel number from the **Channel** list, enter time in **Start Time** box and **End Time** box, and then click **Search**.
- All the tagged videos display in time order.
- To modify the name of tagged video, double-click a tagged video, the **Modify Tag** dialog box is displayed.
- To delete the marked video, select the tagged video, and then click **Delete**.



After opening the **Tag Management** interface, the playback will pause until exiting this interface.

If the marked video that was in playing back is deleted, the playback will start from the first tagged video in the **Tag List**.

5.9.7 Playing Back Snapshots

You can search and play back the snapshots.

Step 1 Select **Main Menu > SEARCH**, the video search interface is displayed.

Step 2 In the **Search Type** list, select **Picture**.

Step 3 In the **Channel** list, select a channel number.

Step 4 In the **Calendar** area, select a date.

Step 5 Click .

The system starts playing snapshots according to the configured intervals.

5.9.8 Playing Back Splices

You can clip the recorded video files into splices and then play back at the same time to save your time.

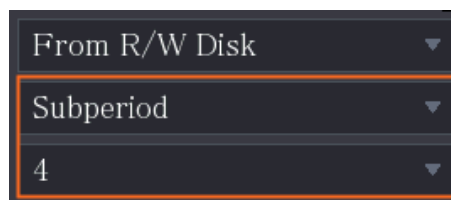


Not all models support this function.

Step 1 Select **Main Menu > SEARCH**, the video search interface is displayed.

Step 2 In the **Search Type** list, select **Subperiod**; In the Split Mode list, select **4, 9, or 16**.

Figure 5-113



Step 3 In the **Calendar** area, select a date.

Step 4 In the **Camera Name** list, select a channel.



Only single-channel supports this function.

Step 5 Start playing back splices.

- Click , the playback starts from the beginning.
- Double-click anywhere on the time bar, the playback starts from where you click.

Figure 5-114



Every recorded video file must be at least five minutes. If a recorded video file is less than 20 minutes but still choose to split into four windows, the system will automatically adjust the windows quantity to ensure every splice is more than five minutes, and in this case it is possible that there are no images are displaying in some windows.

5.9.9 Using the File List

You can view all the recorded videos within a certain period from any channel in the **File List**.

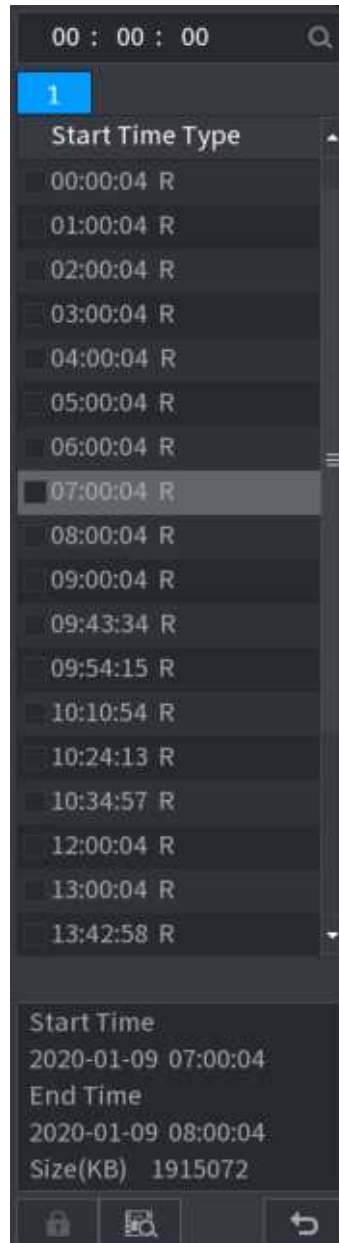
Step 1 Select **Main Menu > VIDEO**, the video search interface is displayed.

Step 2 Select a channel(s).

Step 3 Click .

The **File List** interface is displayed.

Figure 5-115



Step 4 Start playback.

- Click , the playback starts from the first file by default.
- Click any file, the system plays back this file.



- In the time box on the top of the file list interface, you can enter the specific time to search the file that you want to view.
- In the File List area, there are 128 files can be displayed.
- File type: **R** indicates general recorded video; **A** indicates recorded video with external alarms; **M** indicates recorded video with motion detection events; **I** indicates recorded video with intelligent vents.

- Click  to return to the interface with calendar and CAM NAME list.

Locking and Unlocking the Recorded Video

- To lock the recorded video, on the **File List** interface, select the check box of the recorded video, and then click . The locked video will not be covered.

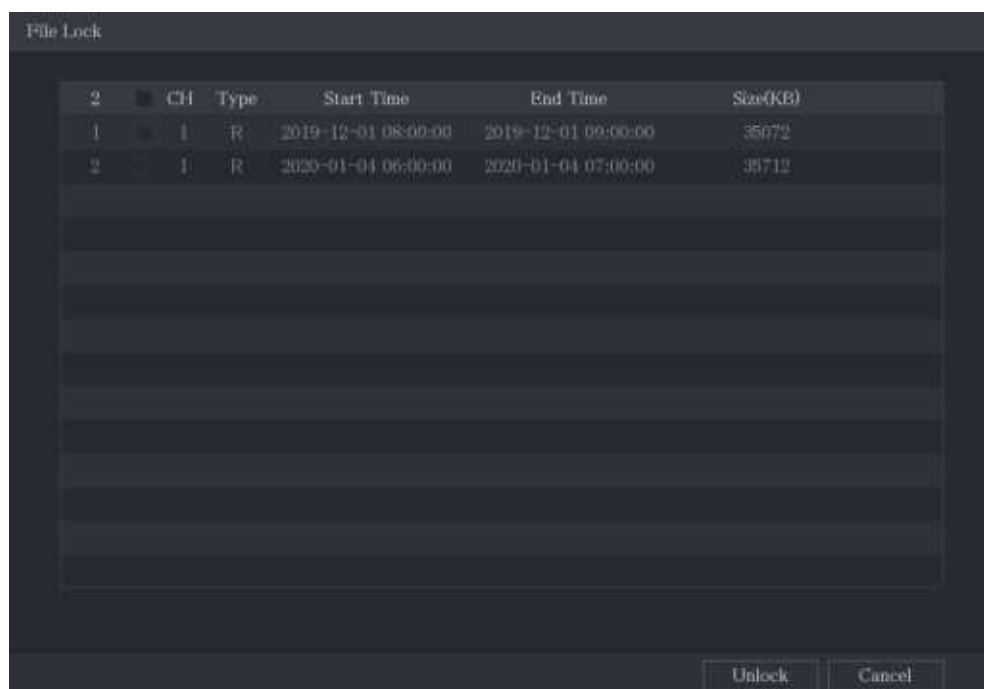
- To view the locked information, click , the **File Lock** interface is displayed.



The recorded video that is under writing or overwriting cannot be locked.

- To unlock the recorded video, in the **File Lock** interface, select the video, and then click **Unlock**.

Figure 5-116



5.10 Alarm Events Settings

5.10.1 Alarm Information

You can search, view and back up the alarm information.

Step 1 Select **Main Menu > ALARM > Alarm Info**.

The **Alarm Info** interface is displayed.

Figure 5-117

	Type	Start Time	End Time	Search
Type	All	2020-01-04 00:00:00	2020-01-05 00:00:00	Search

13	Time	Type	Search
1	2020-01-04 00:41:27	<Tampering : 8>	⊕
2	2020-01-04 00:41:29	<Tampering : 8>	⊕
3	2020-01-04 09:05:33	<Tampering : 8>	⊕
4	2020-01-04 09:05:34	<Tampering : 8>	⊕
5	2020-01-04 12:33:15	<Tampering : 8>	⊕
6	2020-01-04 12:33:16	<Tampering : 8>	⊕
7	2020-01-04 13:31:34	<Network Disconnection Event : 1>	⊕
8	2020-01-04 13:31:39	<CAM Offline Alarm : 8>	⊕
9	2020-01-04 14:04:04	<Network Disconnection Event : 1>	⊕
10	2020-01-04 14:04:29	<CAM Offline Alarm : 8>	⊕
11	2020-01-04 15:12:09	<CAM Offline Alarm : 8>	⊕
12	2020-01-04 16:23:43	<Network Disconnection Event : 1>	⊕
13	2020-01-04 16:23:53	<Network Disconnection Event : 1>	⊕

< 1/1 > Backup Details

Step 2 In the **Type** list, select the event type; In the **Start Time** box and **End Time** box, enter the specific time.

Step 3 Click **Search**.

The search results are displayed.

Step 4 Click **Backup** to back up the search results into the external storage device.



- Click  to play the recorded video of alarm event.
- Select an event and click **Details** to view the detailed information of the event.

5.10.2 Alarm Input Settings

Connect the alarm input and output ports by referring to "4.3 Connecting to Alarm Input and Output." You can configure the alarm settings for each channel individually or apply the settings to all channels and then save the settings.

5.10.2.1 Configuring Local Alarms

You can connect the alarm device to the alarm input port of the Device. When the alarm is activated on the alarm device, the alarm information will be uploaded to the Device, and then the Device outputs the local alarms in the way that you configure in this section.

Step 1 Select **Main Menu > ALARM > Alarm-in Port > Local**.

The **Local** interface is displayed.

Figure 5-118

Step 2 Configure the settings for the local alarms.

Table 5-37

Parameter	Description
Alarm-in Port	Select the channel number.
Alarm Name	Enter the customized alarm name.
Enable	Enable or disable the local alarm function.
Device Type	In the Device Type list, select NO or select NC as the voltage output type.
Schedule	Click Setting to display setting interface. Define a period during which the motion detection is active. For details, see "Setting Motion Detection Period" section in "5.10.4.1 Configuring Motion Detection Settings."
Anti-Dither	Configure the time period from end of event detection to the stop of alarm.
Alarm-out Port	Click Setting to display setting interface. - Local Alarm: Enable alarm activation through the alarm devices connected to the selected output port. - Extension Alarm: Enable alarm activation through the connected alarm box. - Wireless Siren: Enable alarm activation through devices connected by USB gateway or camera gateway.
Post-Alarm	Set a length of time for the Device to delay turning off alarm after the external alarm is cancelled. The value ranges from 0 seconds to 300 seconds, and the default value is 10 seconds.
Show Message	Select the Show Message check box to enable a pop-up message in your local host PC.

Parameter	Description
Report Alarm	Select the Report Alarm check box to enable the system to upload the alarm signal to the network (including alarm center) when an alarm event occurs.
Send Email	Select the Send Email check box to enable the system to send an email notification when an alarm event occurs.  To use this function, make sure the email function is enabled in Main Menu > NETWORK > Email.
Record Channel	Select the channel(s) that you want to record. The selected channel(s) starts recording after an alarm event occurs.  The recording for local alarm recording and auto recording must be enabled. For details, see "5.1.4.9 Configuring Recorded Video Storage Schedule" and "5.9.1 Enabling Record Control."
PTZ Linkage	Click Setting to display the PTZ interface. Enable PTZ linkage actions, such as selecting the preset that you want to be called when an alarm event occurs.
Post Record	Set a length of time for the Device to delay turning off recording after the alarm is cancelled. The value ranges from 10 seconds to 300 seconds, and the default value is 10 seconds.
Tour	Select the Tour check box to enable a tour of the selected channels.
Picture Storage	Select the Snapshot check box to take a snapshot of the selected channel.  To use this function, select Main Menu > CAMERA > Encode > Snapshot, in the Type list, select Event.
Sub Screen	Select the check box to enable the function. When an alarm event occurs, the extra screen outputs the settings configured in Main Menu > DISPLAY > Tour Setting > Sub Screen.  • Not all models support this function. • To use this function, extra screen shall be enabled.
Video Matrix	Select the check box to enable the function. When an alarm event occurs, the video output port outputs the settings configured in Main Menu > DISPLAY > Tour Setting.  Not all models support this function.
Buzzer	Select the check box to activate a buzzer noise at the Device.
Log	Select the check box to enable the Device to record a local alarm log.

Step 3 Click **Apply** to complete the settings.



- Click **Default** to restore the default setting.
- Click **Copy to**, in the **Copy to** dialog box, select the additional channel(s) that you want to copy the local alarm settings to, and then click **Apply**.

5.10.2.2 Configuring Alarms from Alarm Box

You can connect the alarm box to the RS-485 port of the Device. When the alarm is detected by the alarm box, the alarm information will be uploaded to the Device, and then the Device outputs the alarms in the way that you configure in this section.

Step 1 Select **Main Menu > ALARM > Alarm-in Port > Alarm Box**.

The **Alarm Box** interface is displayed.

Figure 5-119

Step 2 In the **Alarm Box** list, select the alarm box number corresponding to the address number configured by the DIP switch on the Alarm Box.

Step 3 In the **Alarm-in Port** list, select the alarm input port on the Alarm Box.

Step 4 Configure the settings for other parameters of the Alarm Box. For details, see Table 5-37.

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



Click **Default** to restore the default setting.

5.10.2.3 Configuring Alarms from External IP Cameras

Step 1 Select **Main Menu > ALARM > Alarm-in Port > CAM Ext**.

The **CAM Ext** interface is displayed.

Figure 5-120

Step 2 Configure the alarm input settings from the external IPC. For details, see Table 5-37.

Step 3 Click **Apply** to complete the settings.



- Click **Default** to restore the default setting.
- Click **Copy to** to copy the settings to other channels.
- Click **Refresh** to refresh configured settings.

5.10.2.4 Configuring Alarms for IP Camera Offline

You can configure the alarm settings for the situation when the IP camera is offline.

Step 1 Select **Main Menu > ALARM > Alarm-in Port > CAM Offline**.

The **CAM Offline** interface is displayed.

Figure 5-121

Step 2 Configure the alarm input settings from the offline IPC.

Step 3 Click **Apply** to complete the settings.

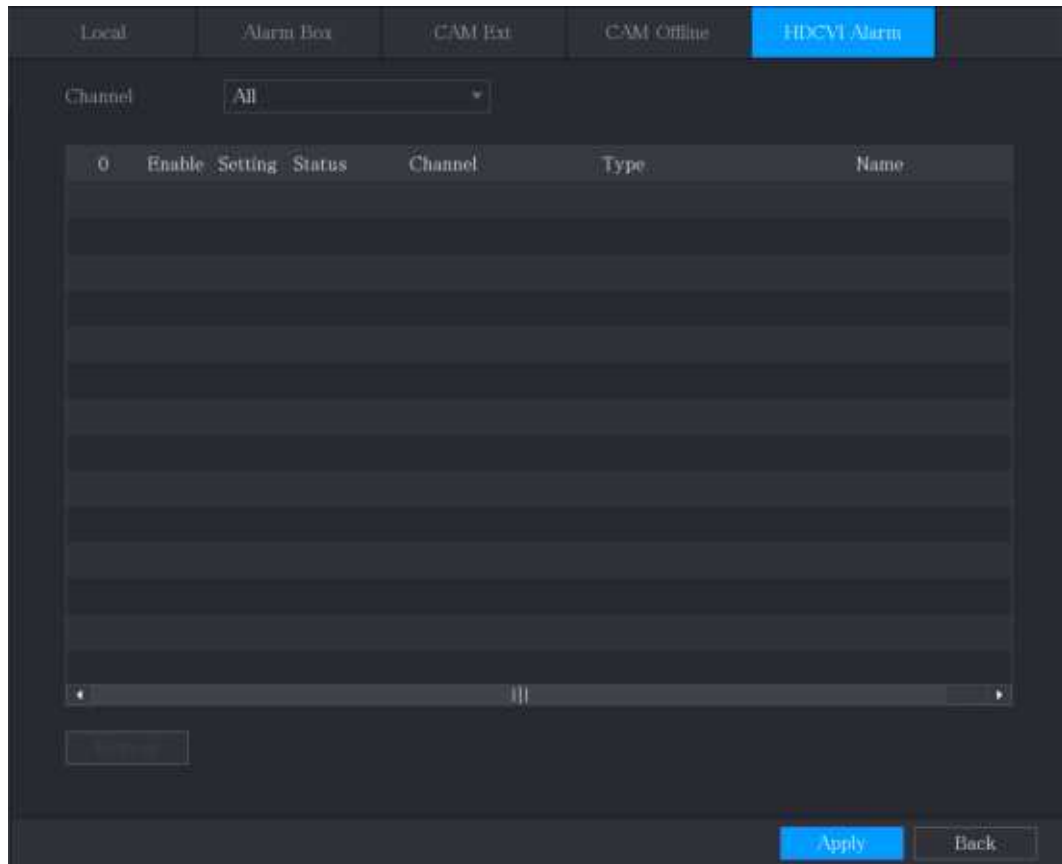


- Click **Default** to restore the default setting.
- Click **Copy to** to copy the settings to other channels.

5.10.2.5 Configuring Alarms from HDCVI Devices

Step 1 Select **Main Menu > ALARM > Alarm-in Port > HDCVI Alarm**.
The **HDCVI Alarm** interface is displayed.

Figure 5-122



Step 2 In the **Channel** list, select a channel or **All**.

Step 3 Click .

Step 4 Configure the settings for other parameters of the Alarm Box. For details, see Table 5-37.

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

Step 6 Click **Apply** to complete the settings.

5.10.3 Alarm Output Settings

5.10.3.1 Configuring Alarm Output

When the Device activates alarms, the connected alarm device generates alarms in the way that you can configure in this section. You can connect to the output port of the Device or connect wirelessly.

- **Auto**: When an alarm event is triggered on the Device, the connected alarm device generates alarms.
- **Manual**: The alarm device is forced to keep generating alarms.
- **Stop**: The alarm output function is not enabled.

Step 1 Select **Main Menu > ALARM > Alarm-out Port > Alarm Mode**.

The **Alarm Mode** interface is displayed.

Figure 5-123

Step 2 Configure the settings for the alarm output. For details, see Table 5-38.

Table 5-38

Parameter		Description
Local Alarm	Alarm Type	Select alarm type for each alarm output port.
	Status	Indicates the status of each alarm output port.
Extension Alarm	Alarm Box	Select the alarm box number corresponding to the address number configured by the DIP switch on the Alarm Box.
	Alarm Type	Select the alarm type for each alarm output ports.
	Status	Indicates the status of each alarm output port.
Alarm Reset		Click OK to clear all alarm output status.

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

5.10.3.2 Configuring White Light

When the motion detection alarm is activated, the system links the camera to generate white light alarm.



To use this function, connect at least one white light camera to your Device.

Step 1 Select **Main Menu > ALARM > Alarm-out Port > White Light**.

The **White Light** interface is displayed.

Figure 5-124

Step 2 Configure the settings for the white light parameters.

Table 5-39

Parameter	Description
Channel	In the Channel list, select a channel that is connected to a white light camera.
Delay	Set a length of time for the Device to delay turning off alarm after the alarm is cancelled. The value ranges from 5 seconds to 30 seconds, and the default value is 5 seconds.
Mode	Set the alarm mode of white light to be Always on or Flicker .
Flicker Frequency	When setting the alarm mode of white light to be Flash , you can select the flash frequency from Low , Middle , and High .

Step 3 Click **Apply** to complete the settings.

5.10.3.3 Configuring Siren

When the motion detection alarm is activated, the system links the camera to generate sound alarm.



To use this function, connect at least one camera that supports audio function.

Step 1 Select **Main Menu > ALARM > Alarm-out Port > Siren**.

The **Siren** interface is displayed.

Figure 5-125

Step 2 Configure the settings for the siren parameters.

Table 5-40

Parameter	Description
Channel	In the Channel list, select a channel that is connected to a camera that supports audio function.
Play	Click Play to manually trigger the IP camera to play audio file.
Delay	Set a length of time for the Device to delay turning off alarm after the alarm is cancelled. The value ranges from 5 seconds to 30 seconds, and the default value is 5 seconds.
Audio Clip	Select the audio clip for the siren sound. The default setting is Clip 1 .
Volume	Select the volume for the audio clip. You can select the flash frequency from Low , Middle , and High .
Update Audio Clip	Import the upgrade audio file (.bin) to upgrade the alarm audio file of the camera. For details, see "Upgrade Audio File of Camera"

Step 3 Click **Apply** to complete the settings.

Upgrade Audio File of Camera



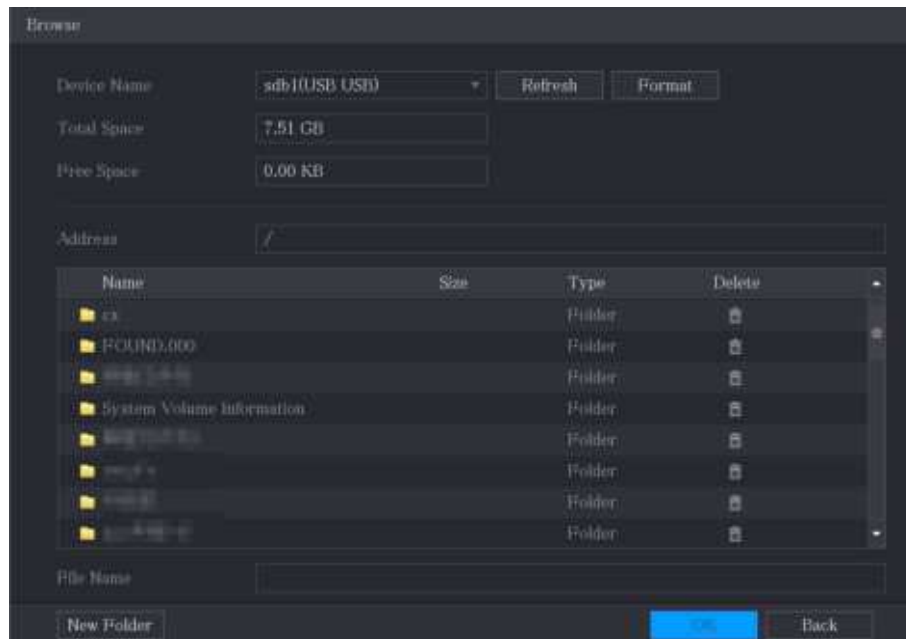
This function is supported only on the local interface.

Step 1 Prepare a USB device or other external storage device and plug it into the Device.

Step 2 Click **Browse**.

The **Browse** interface is displayed.

Figure 5-126



Step 3 Select the upgrade audio file (.bin).

Step 4 Click **OK** to return to the Siren interface.

Step 5 Click **Upgrade** to upgrade the alarm audio file of the camera.

5.10.4 Video Detection

Video detection adopts computer vision and image processing technology. The technology analyzes the video images to detect the obvious changes such as moving objects and blurriness. The system activates alarms when such changes are detected.

5.10.4.1 Configuring Motion Detection Settings

When the moving object appears and moves fast enough to reach the preset sensitivity value, the system activates the alarm.

Step 1 Select **Main Menu > ALARM > Video Detection > Motion Detection**.

The **Motion Detection** interface is displayed.

Figure 5-127

Step 2 Configure the settings for the motion detection parameters.

Table 5-41

Parameter	Description
Channel	In the Channel list, select a channel to set the motion detection.
Region	Click Setting to define the motion detection region.
Enable	Enable or disable the motion detection function.
PIR Alarm	PIR function helps enhancing the accuracy and validity of motion detect. It can filter the meaningless alarms that are activated by the objects such as falling leaves, flies. The detection range by PIR is smaller than the field angle. PIR function is enabled by default if it is supported by the cameras. Enabling PIR function will get the motion detect to be enabled automatically to generate motion detection alarms; if the PIR function is not enabled, the motion detect just has the general effect.  - Only when the channel type is CVI, the PIR function can be enabled. - If the camera does not support PIR function, it will be unusable. - If the Device does not support PIR function, it will not be displayed on the interface.
Schedule	Define a period during which the motion detection is active.

Parameter	Description
Anti-Dither	Configure the time period from end of event detection to the stop of alarm.
Alarm-out Port	Click Setting to display setting interface. - General Alarm: Enable alarm activation through the alarm devices connected to the selected output port. - External Alarm: Enable alarm activation through the connected alarm box. - Wireless Siren: Enable alarm activation through devices connected by USB gateway or camera gateway.
Post-Alarm	Set a length of time for the Device to delay turning off alarm after the external alarm is cancelled. The value ranges from 0 seconds to 300 seconds, and the default value is 10 seconds. If you enter 0, there will be no delay.
Show Message	Select the Show Message check box to enable a pop-up message in your local host PC.
Report Alarm	Select the Report Alarm check box to enable the system to upload the alarm signal to the network (including alarm center) when an alarm event occurs.
Send Email	Select the Send Email check box to enable the system to send an email notification when an alarm event occurs.  To use this function, make sure the email function is enabled in Main Menu > NETWORK > Email.
Record Channel	Select the channel(s) that you want to record. The selected channel(s) starts recording after an alarm event occurs.  The recording for motion detection and auto recording function must be enabled. For details, see "5.1.4.9 Configuring Recorded Video Storage Schedule" and "5.9.1 Enabling Record Control."
PTZ Linkage	Click Setting to display the PTZ interface. Enable PTZ linkage actions, such as selecting the preset that you want to be called when an alarm event occurs.  Motion Detect can only activate PTZ preset.
Post Record	Set a length of time for the Device to delay turning off recording after the alarm is cancelled. The value ranges from 10 seconds to 300 seconds, and the default value is 10 seconds.
Tour	Select the Tour check box to enable a tour of the selected channels.
Picture Storage	Select the Snapshot check box to take a snapshot of the selected channel.  To use this function, select Main Menu > CAMERA > Encode > Snapshot, in the Type list, select Event.

Parameter	Description
Sub Screen	Select the check box to enable the function. When an alarm event occurs, the extra screen outputs the settings configured in Main Menu > DISPLAY > Tour > Sub Screen .  - Not all models support this function. - To use this function, extra screen shall be enabled.
Video Matrix	Select the check box to enable the function. When an alarm event occurs, the video output port outputs the settings configured in Main Menu > DISPLAY > Tour .  Not all models support this function.
Buzzer	Select the check box to activate a buzzer noise at the Device.
Log	Select the check box to enable the Device to record a local alarm log.
Alarm Tone	Select to enable audio broadcast/alarm tones in response to a motion detection event.
White Light	Select the check box to enable white light alarm of the camera.
Siren	Select the check box to enable sound alarm of the camera.

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



- Click **Default** to restore the default setting.
- Click **Copy to**, in the **Copy to** dialog box, select the additional channel(s) that you want to copy the motion detection settings to, and then click **Apply**.
- Click **Test** to test the settings.

Setting the Motion Detection Region

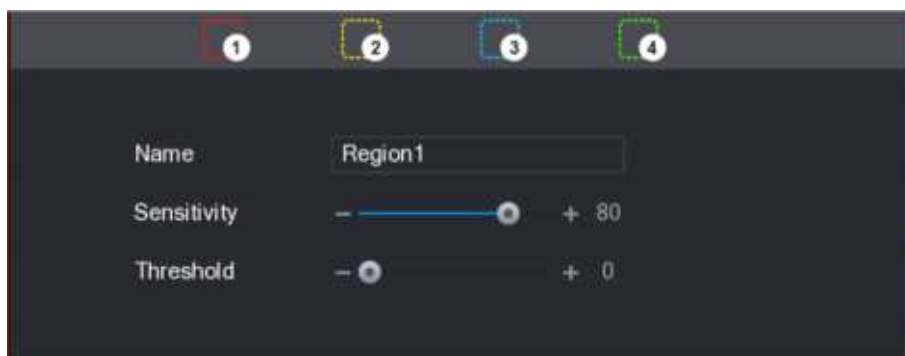
Step 1 Next to **Region**, click **Setting**.

The region setting screen is displayed.

Step 2 Point to the middle top of the interface.

The setting interface is displayed.

Figure 5-128



Step 3 Configure the regions settings. You can configure totally four regions.

- Select one region, for example, click .
- Drag on the screen to select the region that you want to detect.
The selected area shows the color that represents the region.
- Configure the parameters.

Table 5-42

Parameter	Description
Name	Enter a name for the region.
Sensitivity	Every region of every channel has an individual sensitivity value. The bigger the value is, the easier the alarms can be activated.
Threshold	Adjust the threshold for motion detect. Every region of every channel has an individual threshold.



When anyone of the four regions activates motion detect alarm, the channel where this region belongs to will activate motion detect alarm.

Step 4 Right-click on the screen to exit the region setting interface.

Step 5 On the **Motion Detection** interface, click **Apply** to complete the settings.

Setting Motion Detection Period



The system only activates the alarm in the defined period.

Step 1 Next to **Schedule**, click **Setting**.

The **Setting** interface is displayed..

Figure 5-129



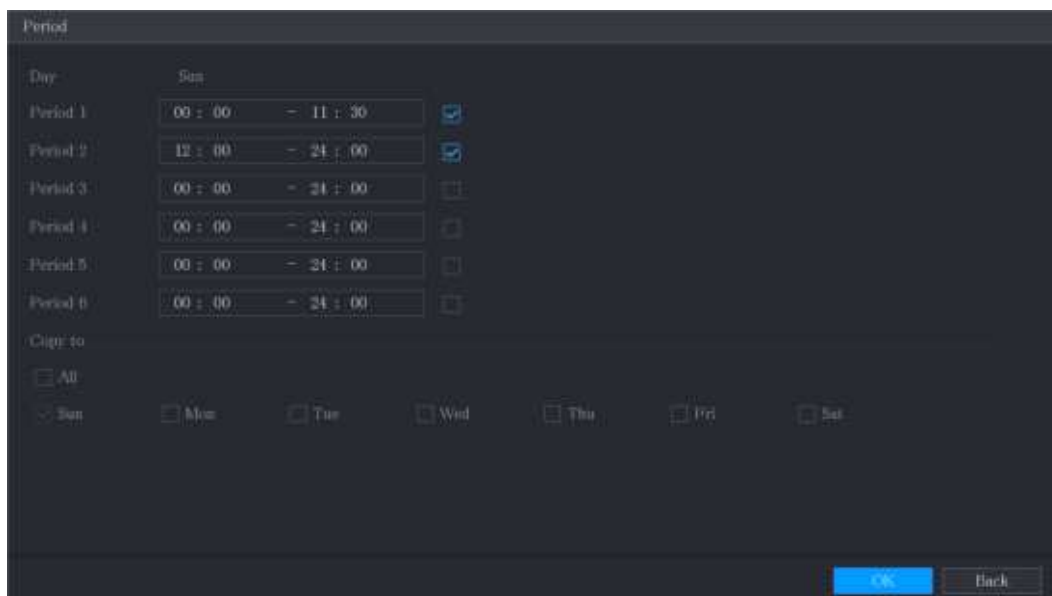
Step 2 Define the motion detection period. By default, it is active all the time.

- Define the period by drawing.
 - ◇ Define for a specified day of a week: On the timeline, click the half-hour blocks to select the active period.
 - ◇ Define for several days of a week: Click  before each day, the icon switches to . On the timeline of any selected day, click the half-hour blocks to select the active periods, all the days with  will take the same settings.

- ◇ Define for all days of a week: Click **All**, all  switches to . On the timeline of any day, click the half-hour blocks to select the active periods, all the days will take the same settings.
 - Define the period by editing. Take Sunday as an example.
- 1) Click .

The **Period** interface is displayed.

Figure 5-130



- 2) Enter the time frame for the period, and then select the check box to enable the settings.
 - ◇ There are six periods for you to set for each day.
 - ◇ Under **Copy to**, select **All** to apply the settings to all the days of a week, or select specific day(s) that you want to apply the settings to.
- 3) Click **OK** to save the settings.

Step 3 On the **Motion Detection** interface, click **Apply** to complete the settings.

5.10.4.2 Configuring Video Loss Settings

When the video loss occurs, the system activates the alarm.

Step 1 Select **Main Menu > ALARM > Video Detection > Video Loss**.

The **Video Loss** interface is displayed.

Figure 5-131

Step 2 To configure the settings for the video loss detection parameters, see “5.10.4.1 Configuring Motion Detection Settings.”



For PTZ activation, different from motion detection, the video loss detection can activate PTZ preset, tour, and pattern.

Step 3 Click **Apply** to complete the settings.



- Click **Default** to restore the default setting.
- Click **Copy to**, in the **Copy to** dialog box, select the additional channel(s) that you want to copy the motion detection settings to, and then click **Apply**.

5.10.4.3 Configuring Tampering Settings

When the camera lens is covered, or the video is displayed in a single color because of the causes such as sunlight status, the monitoring cannot be continued normally. To avoid such situations, you can configure the tampering alarm settings.

Step 1 Select **Main Menu > ALARM > Video Detection > Video Tampering**.

The Video **Tampering** interface is displayed.

Figure 5-132

Step 2 To configure the settings for the tampering detection parameters, see “5.10.4.1 Configuring Motion Detection Settings.”



For PTZ activation, different from motion detection, the video loss detection can activate PTZ preset, tour, and pattern.

Step 3 Click **Apply** to complete the settings.



- Click **Default** to restore the default setting.
- Click **Copy to**, in the **Copy to** dialog box, select the additional channel(s) that you want to copy the motion detection settings to, and then click **Apply**.

5.10.4.4 Configuring Video Quality Analytics



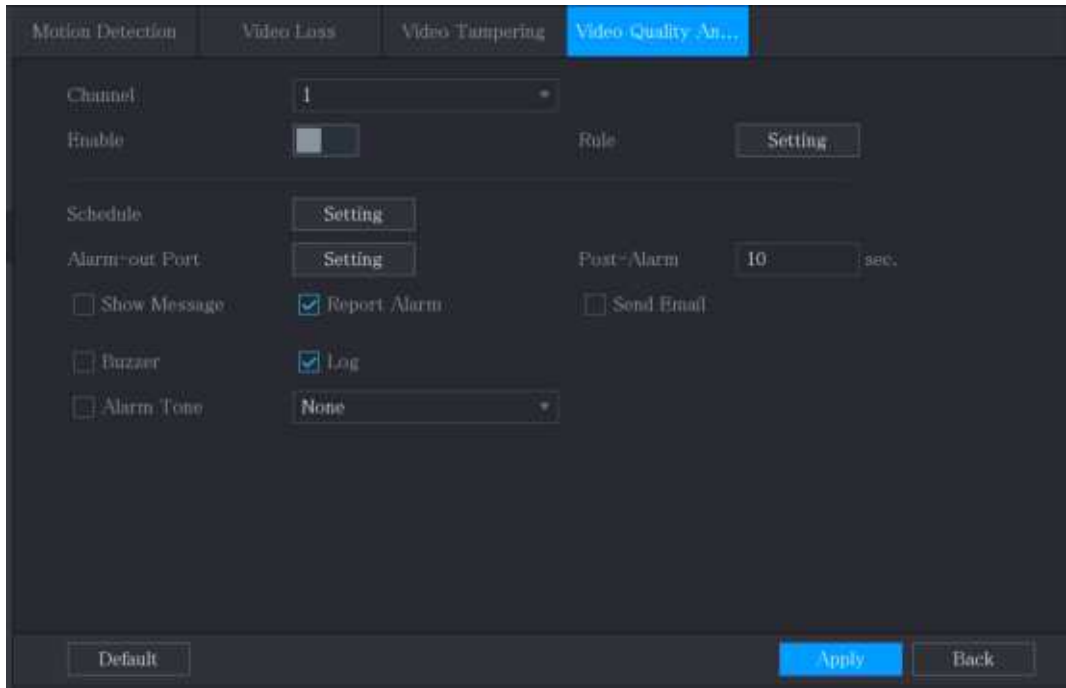
This function can be used only when it is supported by the camera.

When the video appear the conditions such as blurry, overexposed, or the color changes, the system activates the alarm.

Step 1 Select **Main Menu > ALARM > Video Detection > Video Quality Analytics**.

The **Video Quality Analytics** interface is displayed.

Figure 5-133



Step 2 To configure the settings for the diagnosis parameters, see "5.10.4.1 Configuring Motion Detection Settings."

Step 3 Click **Apply** to complete the settings.



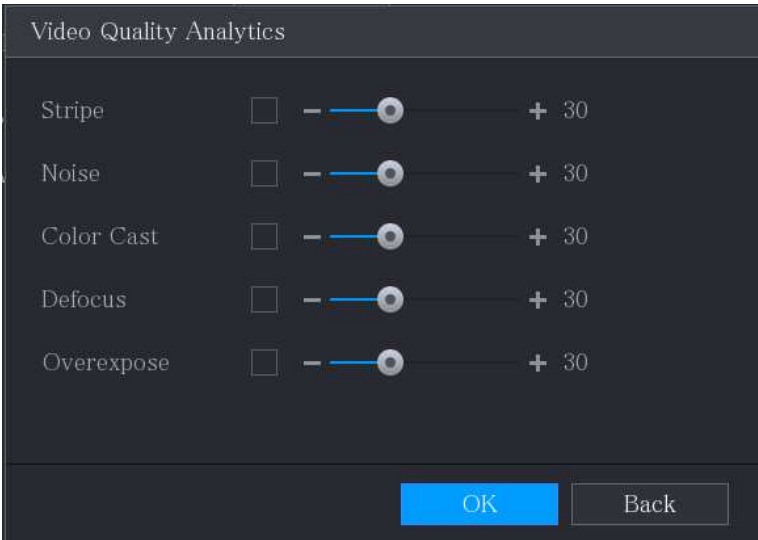
Click **Default** to restore the default setting.

Setting the Types for Diagnosing Targets

Step 1 Next to **Rule**, click **Setting**.

The **Video Quality Analytics** interface is displayed.

Figure 5-134



Step 2 Select the items that you want to diagnose and set the threshold (30 by default).

Table 5-43

Parameter	Description
-----------	-------------

Parameter	Description
Stripe	A horizontal, vertical or diagonal stripe that might appear in the video because of device aging or electronic interruption. Such stripe brings visual interruption.
Noise	Video noises such as blurriness or quality reduction that is caused by optical distortion or device problem during camera shooting.
Color Cast	Variances in the normal proportions of RGB colors.
Defocus	Blurry video is caused during camera shooting, transferring and processing. Such condition is a common image quality reduction problem and defined as out of focus.
Overexposure	The video brightness refers to the intensity of image pixel. The range is between 0 (the darkest black) and 255 (the brightest white). If the brightness exceeds the threshold, the image is over exposed.

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

The system returns to the **Video Quality Analytics** interface.

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



Click **Default** to restore the default setting.

5.10.5 System Events

You can configure the alarm output for three types of system event (HDD, Network, and User). When there is an abnormal system event occurs, the system activates alarms in the way that you configure in this section.

5.10.5.1 Configuring HDD Event Settings

Step 1 Select **Main Menu > ALARM > Exception > Disk**.

The **Disk** interface is displayed.

Figure 5-135

The screenshot shows a configuration window for the 'Disk' event. At the top, there are tabs for 'Disk' and 'Network'. Under the 'Disk' tab, the 'Event Type' is a dropdown menu currently showing 'No Disk'. Below it is an 'Enable' toggle switch that is turned on. Further down, there is a 'Setting' button next to the 'Alarm-out Port' label. To the right of this is a 'Post-Alarm' field with the value '10' and a unit 'sec.'. Below these are three checkboxes: 'Show Message', 'Report Alarm', and 'Send Email', all of which are currently unchecked. Below these are two more checkboxes: 'Buzzer' (unchecked) and 'Log' (checked). At the bottom of this section is an 'Alarm Tone' dropdown menu set to 'None'. At the very bottom right of the window are 'Apply' and 'Back' buttons.

Step 2 Configure the settings for the HDD event.

Table 5-44

Parameter	Description
Event Type	In the Event Type list, select No Disk , Disk Error , or Low Space as the event type.
Enable	Enable or disable the HDD event detection function.
Alarm-out Port	Click Setting to display setting interface. - Local Alarm: Enable alarm activation through the alarm devices connected to the selected output port. - Extension Alarm: Enable alarm activation through the connected alarm box. - Wireless Siren: Enable alarm activation through devices connected by USB gateway or camera gateway.
Post-Alarm	Set a length of time for the Device to delay turning off alarm after the external alarm is cancelled. The value ranges from 10 seconds to 300 seconds, and the default value is 10 seconds.
Show Message	Select the Show Message check box to enable a pop-up message in your local host PC.
Report Alarm	Select the Report Alarm check box to enable the system to upload the alarm signal to the network (including alarm center) when an alarm event occurs.
Send Email	Select the Send Email check box to enable the system to send an email notification when an alarm event occurs.  To use this function, make sure the email function is enabled in Main Menu > NETWORK > Email .
Buzzer	Select the check box to activate a buzzer noise at the Device.

Parameter	Description
Log	Select the check box to enable the Device to record a local alarm log.
Alarm Tone	Select to enable audio broadcast/alarm tone in response to a HDD alarm event.

Step 3 Click **Apply** to complete the settings.

5.10.5.2 Configuring Network Event Settings

Step 1 Select **Main Menu > ALARM > Exception > Network**.

The **Network** interface is displayed.

Figure 5-136

Step 2 Configure the settings for the Network event.

Table 5-45

Parameter	Description
Event Type	In the Event Type list, select Office , IP Conflict , or MAC Conflict as the event type.
Enable	Enable or disable the Network event detection function.
Alarm-out Port	Click Setting to display setting interface. - General Alarm: Enable alarm activation through the alarm devices connected to the selected output port. - External Alarm: Enable alarm activation through the connected alarm box. - Wireless Siren: Enable alarm activation through devices connected by USB gateway or camera gateway.
Post-Alarm	Set a length of time for the Device to delay turning off alarm after the external alarm is cancelled. The value ranges from 10 seconds to 300 seconds, and the default value is 10 seconds.

Parameter	Description
Show Message	Select the Show Message check box to enable a pop-up message in your local host PC.
Send Email	Select the Send Email check box to enable the system to send an email notification when an alarm event occurs.  To use this function, make sure the email function is enabled in Main Menu > NETWORK > Email .
Buzzer	Select the check box to activate a buzzer noise at the Device.
Log	Select the check box to enable the Device to record a local alarm log.
Post Record	Continue to record for some time after the alarm is ended. The value ranges from 10 seconds to 300 seconds.
Alarm Tone	Select to enable audio broadcast/alarm tones in response to a network alarm event.

Step 3 Click **Apply** to complete the settings.

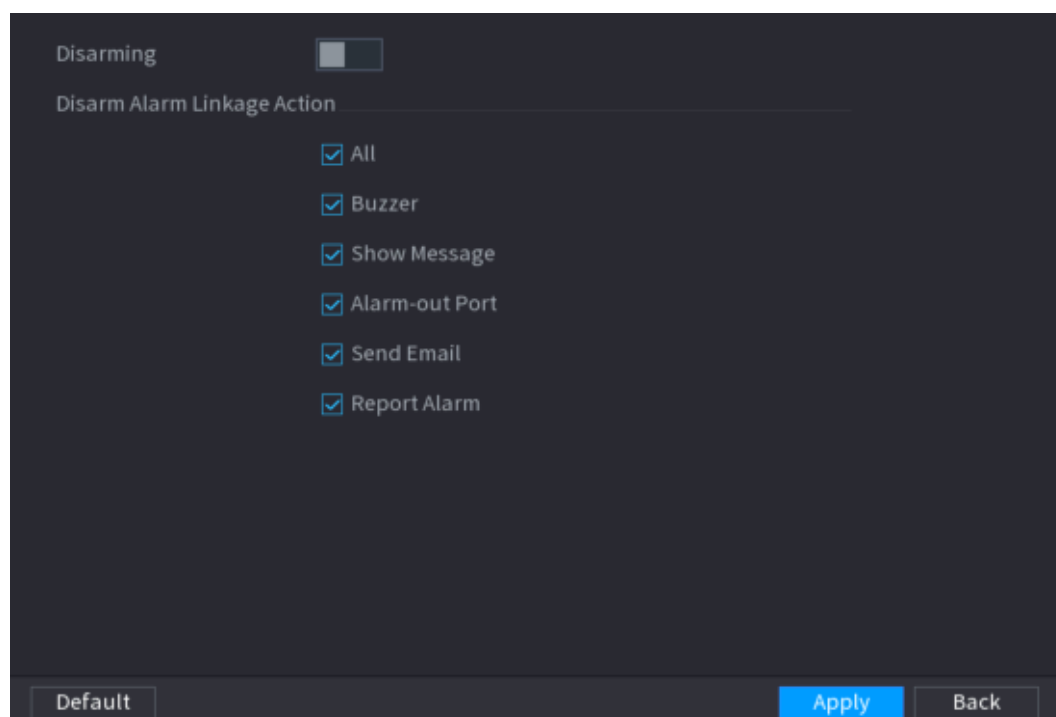
5.10.6 Configuring Disarming

You can disarm all alarm linkage actions as needed.

Step 1 Select **Main Menu > ALARM > Disarming**.

Step 2 Click  to enable disarming.

Figure 5-137



Step 3 Select alarm linkage actions to disarm.



All alarm linkage actions will be disarmed when you select **All**.

Step 4 Click **Apply**.

5.11 AI Function

5.11.1 For Pro AI Series



The faces are fuzzily processed to comply with relevant regulations.

AI module provides face detection, face recognition, IVS functions, and video structuring. These functions take effect after they are configured and enabled. It adopts deep learning and can realize precision alarms.

- Face detection: The Device can analyze the faces captured by the camera and link the configured alarms.
- Face recognition: The Device can compare the captured faces with the face library and then link the configured alarms.
- IVS: The IVS function processes and analyzes the human and vehicle images to extract the key information to match with the preset rules. When the detected behaviors match with the rules, the system activates alarms. The IVS function can avoid wrong alarms by filtering the factors such as rains, light, and animals.
- Video structuring: The device can detect and extract key features from the human bodies and non-motor vehicles in the video, and then build a structured database. You can search any target you need with these features. For example, you can search any people who wears yellow short sleeve shirt. See more details in "5.11.1.4 Video Structuring."

5.11.1.1 Face Detection

The Device can analyze the pictures captured by the camera to detect whether the faces are on the pictures. You can search and filter the recorded videos the faces and play back.



If you select AI by device, then among face detection and recognition, IVS function, and video structuring, you can use one of them at the same time for the same channel.

5.11.1.1.1 Configuring Face Detection Parameters

The alarms are generated according to the configured parameters.

Step 1 **Main Menu > AI > Parameters > Face Detection.**

The **Face Detection** interface is displayed.

Figure 5-138

Step 2 In the **Channel** list, select a channel that you want to configure face detection function, and then enable it.

Step 3 Configure the parameters.

Table 5-46

Parameter	Description
Type	You can select from AI by Camera and AI by Device. AI by Camera: This option requires certain AI cameras. The camera will do all the AI analysis, and then give the results to the DVR. AI by Device: The camera only transmits normal video stream to the DVR, and then the DVR will do all the AI analysis.
Rule	Click View Setting to draw areas to filter the target. You can configure two filtering targets (maximum size and minimum size). When the target is smaller than the minimum size or larger than the maximum size, no alarms will be activated. The maximum size should be larger than the minimum size.
Schedule	Define a period during which the detection is active. For details, see "Setting Motion Detection Period" section in "5.10.4.1 Configuring Motion Detection Settings."

Parameter	Description
Alarm-out Port	Click Setting to display setting interface. - General Alarm: Enable general alarm and select the alarm output port. - Ext. Alarm: Connect the alarm box to the Device and then enable it. - Wireless Siren: Connect the wireless gateway to the Device and then enable it. For details, see "5.12 IoT Function." When an alarm event occurs, the system links the peripheral alarm devices connected to the selected output port.
Post-Alarm	Set a length of time for the Device to delay turning off alarm after the external alarm is cancelled. The value ranges from 0 seconds to 300 seconds. If you enter 0, there will be no delay.
Show Message	Select the Show Message check box to enable a pop-up alarm message in your local host PC.
Report Alarm	Select the Report Alarm check box to enable the system to upload the alarm signal to the network (including alarm center) when an alarm event occurs.  - Not all models support this function. - The corresponding parameters in the alarm center should be configured. For details, see "5.15.1.12 Configuring Alarm Center Settings."
Send Email	Select the Send Email check box to enable the system to send an email notification when an alarm event occurs.  To use this function, make sure the email function is enabled in Main Menu > NETWORK > Email.
Record Channel	Select the channel(s) that you want to record. The selected channel(s) starts recording after an alarm event occurs.  The recording for intelligence event and auto recording function must be enabled. For details, see "5.1.4.9 Configuring Recorded Video Storage Schedule" and "5.9.1 Enabling Record Control."
PTZ Linkage	Click Setting to display the PTZ interface. Enable PTZ linkage actions, such as selecting the preset that you want to be called when an alarm event occurs.  To use this function, the PTZ operations must be configured. For details, see "5.4 Controlling PTZ Cameras."
Post Record	Set a length of time for the Device to delay turning off recording after the alarm is cancelled. The value ranges from 10 seconds to 300 seconds.

Parameter	Description
Tour	Select the Tour check box to enable a tour of the selected channels.  - To use this function, the tour setting must be configured. - After the tour is ended, the live view screen returns to the view layout before tour started.
Picture Storage	Select the Picture Storage check box to take a snapshot of the selected channel.  To use this function, make sure the snapshot function is enabled for Intel in Main Menu > STORAGE > Schedule > Snapshot.
Video Matrix	Select the check box to enable the function. When an alarm event occurs, the video output port outputs the settings configured in "Main Menu > DISPLAY > TOUR > Extra Screen."  - Not all models support this function. - The extra screen must be enabled to support this function.
Buzzer	Select the check box to activate a buzzer noise at the Device.
Log	Select the check box to enable the Device to record a local alarm log.
Alarm Tone	Select to enable audio broadcast in response to a face detection event.
White Light	Select the check box to enable the white light alarm of the camera.
Siren	Select the check box to enable the sound alarm of the camera.

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

5.11.1.1.2 Searching for and Playing Detected Faces

You can search the detected faces and play back.

Step 1 Select **Main Menu > AI > AI Search > Face Detection**.

The **Face Detection** interface is displayed.

Figure 5-139

Channel: 1

Start Time: 2020-03-02 00:00:00

End Time: 2020-03-03 00:00:00

Gender: All

Age: All

Glasses: All

Beard: All

Mouth Mask: All

Expression: All

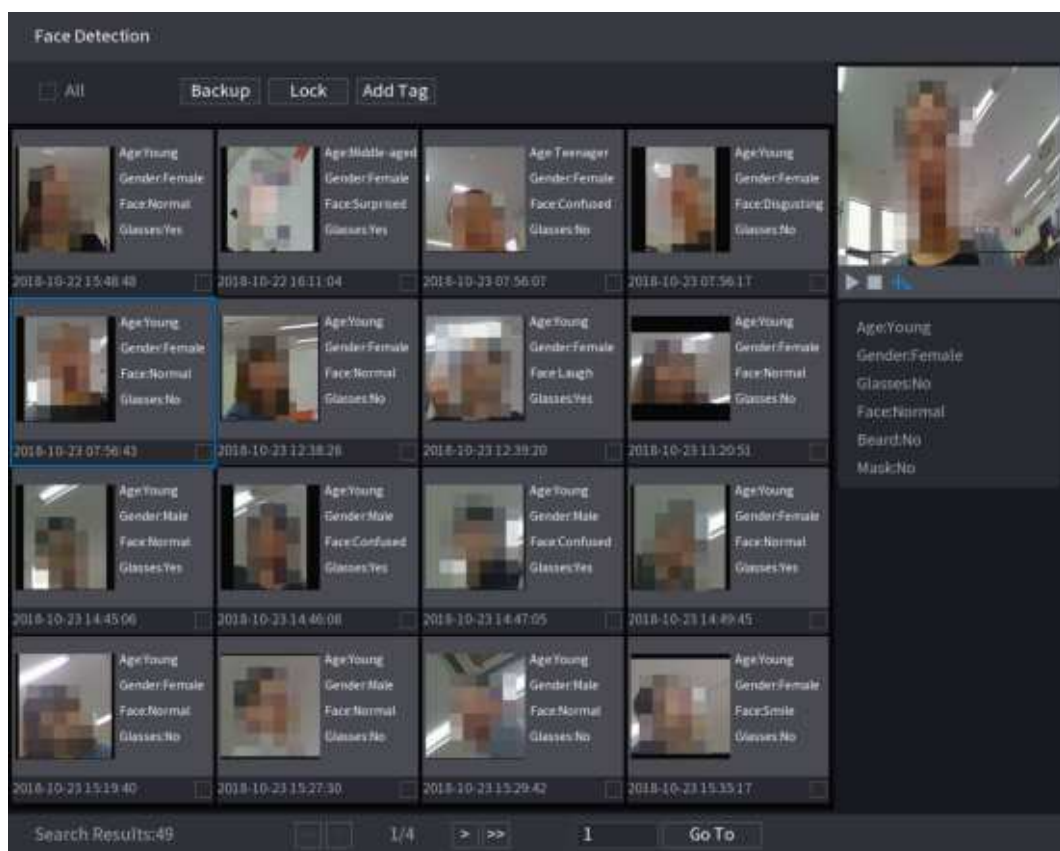
Smart Search

Step 2 Select the channel, enter the start time and end time, and set for the gender, age, glasses, beard, and mask.

Step 3 Click **Smart Search**.

The results are displayed.

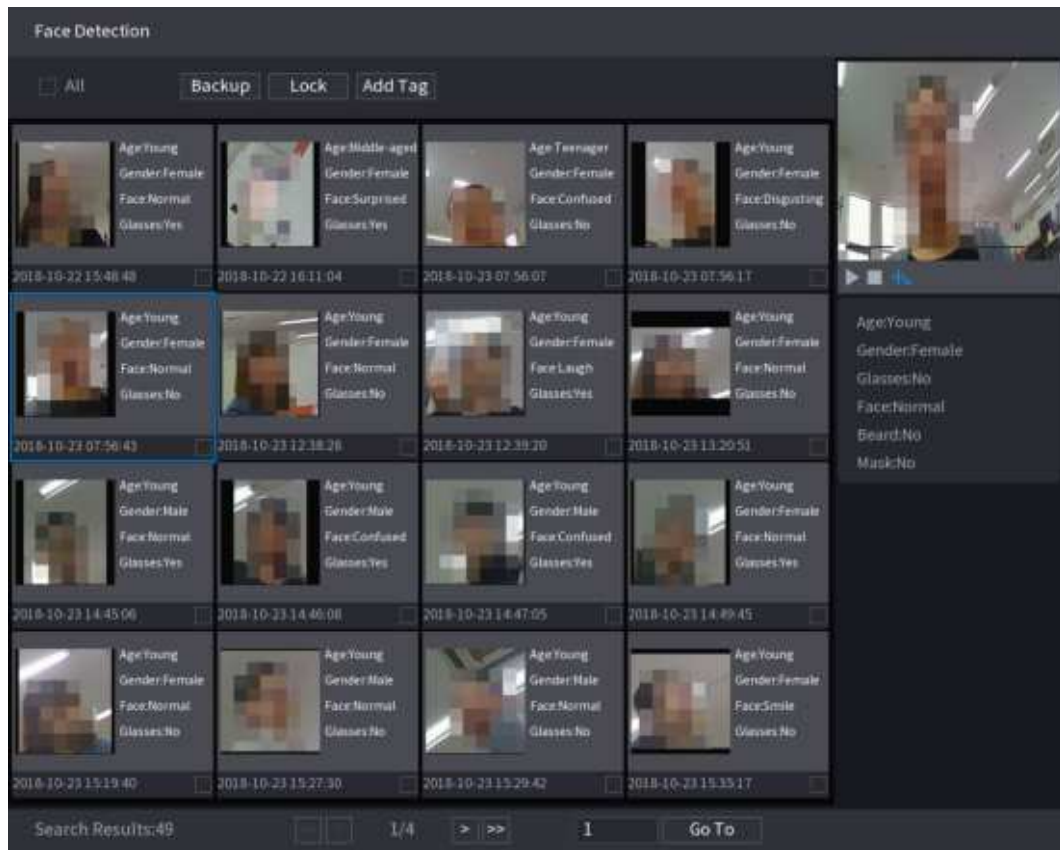
Figure 5-140



Step 4 Select the face that you want to play back.

The picture with registered information is displayed.

Figure 5-141



Step 5 Click  to start playing back the recorded detected face snapshots.

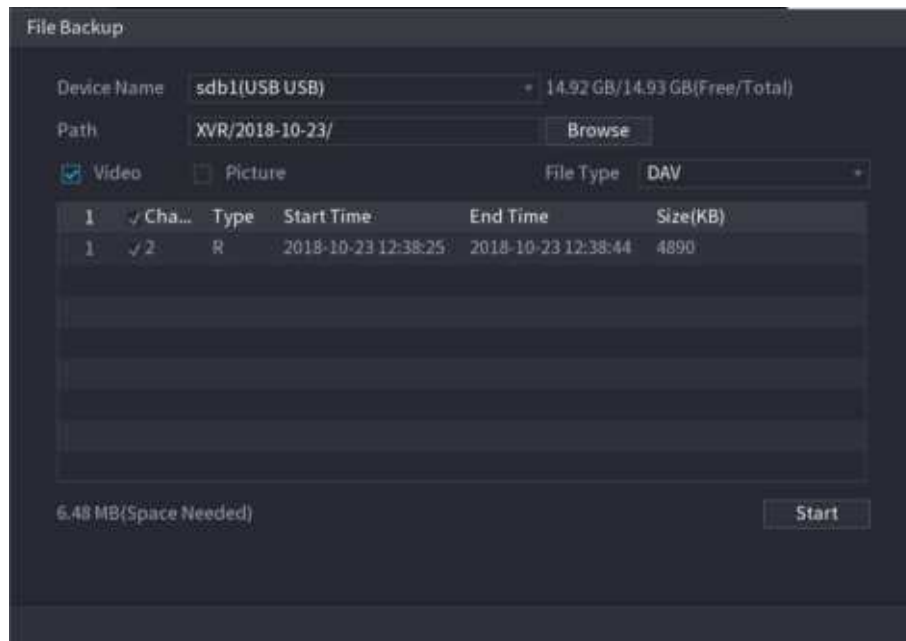


Double-click on the playing interface to switch between full screen playing and thumbnail playing.

You can also do the following operations to the recorded files.

- To export the database file (.csv) to the external storage device, select files, click **Export**, and then select the save path.
- To back up the recorded files to the external storage device, select files, click **Backup**, select the save path and file type, and then click **Start**.

Figure 5-142



- To lock the files to make it unable to be overwritten, select the files, and then click **Lock**.
- To add a mark to the file, select the files and then click **Add Tag**.

5.11.1.2 Face Recognition

Face recognition applies to AI preview mode and smart search.

- AI preview mode: Supports comparing the detected faces with the face library, and display the comparison results.
- Smart search: Supports faces searching by faces attributes or portraits.



- If you select AI by device, then among face detection and recognition, IVS function, and video structuring, you can use one of them at the same time for the same channel.
- Before enabling face recognition function for a channel, the face detection must be enabled first for this channel.

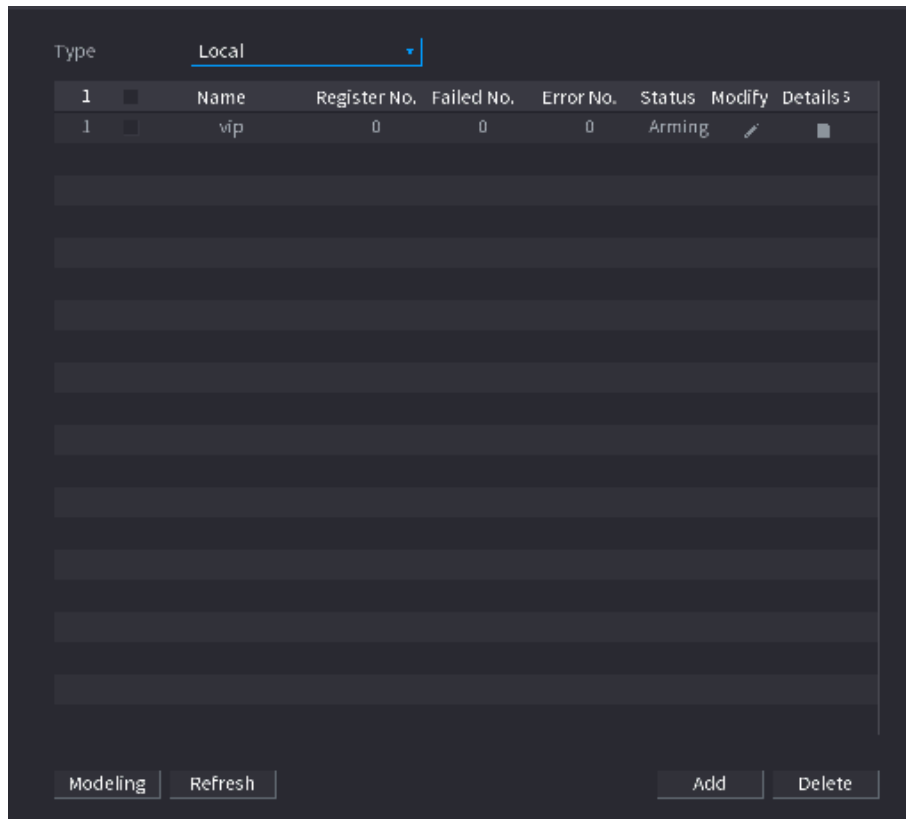
5.11.1.2.1 Face Library Management

You should create a face library for comparing the detected faces and the faces in the library. The Device supports creating maximum 20 libraries and registering 100,000 faces.

Creating a Face Library

- Step 1 Select **Main Menu > AI > Database > Face Database Config**.
The **Face Database Config** interface is displayed.

Figure 5-143



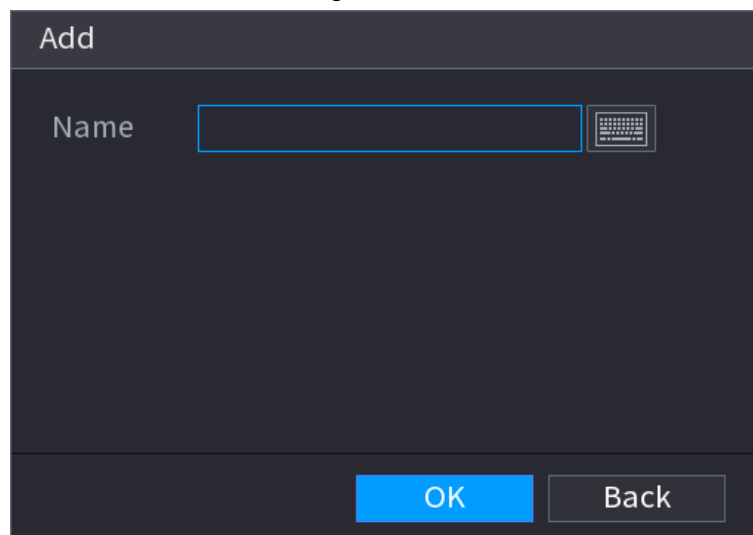
Step 2 At **Type**, you can select **Local** or **Remote**.

- **Local**: Viewing the existing face databases or adding new one on the DVR.
- **Remote**: If you have face recognition camera, you can select this to view the existing face databases or adding new one on the camera.

Click **Add**.

The **Add** interface is displayed.

Figure 5-144



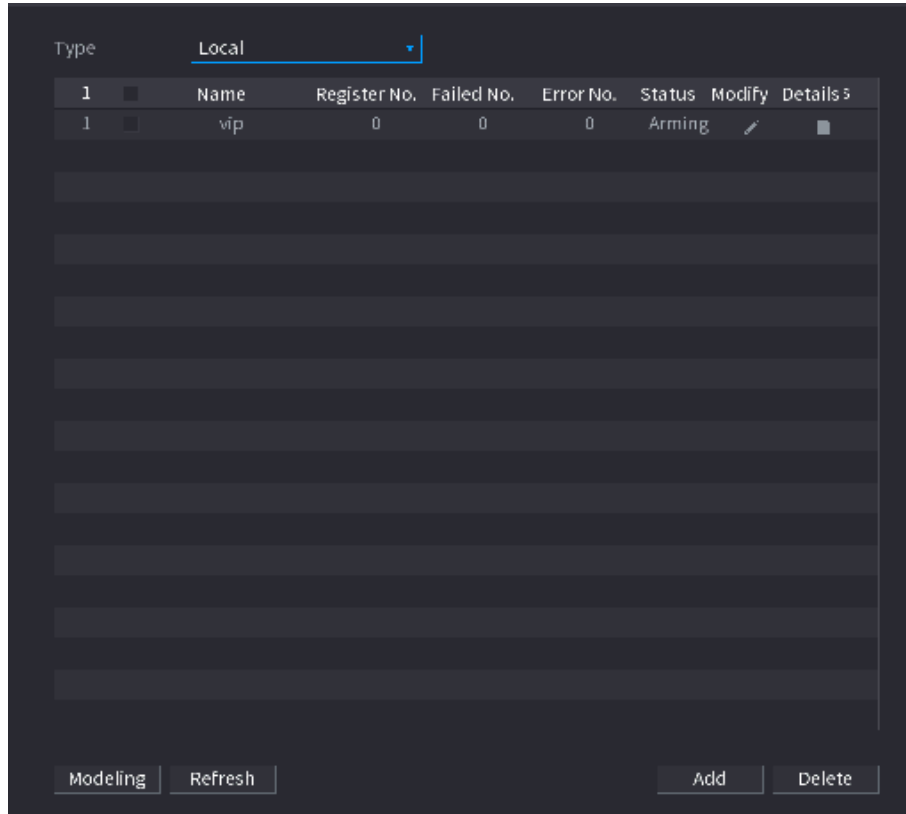
Step 3 Enter the face library name, and then click **OK**.

The created library is displayed.

- Click to modify library name.

- Click  to view the library details and add new faces to the library. For details, see "Adding Face Pictures."
- Select the library, and then click **Modeling**. The system will extract the attributes of face pictures in the library for the future comparison.
- Select the library, and then click **Delete** to delete the library.

Figure 5-145



Adding Face Pictures

You can add face pictures to the existing libraries one by one or by batch, or add from the detected faces.



To add face pictures one by one or by batch, you need to get the pictures from the USB storage device. The picture size should be smaller than 256K with resolution between 200×200–6000×5000.

Adding One Face Picture

Step 1 Select **Main Menu > AI > Database > Face Database Config**.

The **Face Database Config** interface is displayed.

Step 2 Click  of the library that you want to configure.

The **Details** interface is displayed.

Figure 5-146

Details

Name Gender: All ID No. Model... All

☐ All

1/1 1

Step 3 Click **Register ID**.

The **Register ID** interface is displayed.

Figure 5-147

Register ID

Name

Gender ☒ Male ☐ Female

Birthday Year Month Date

Address

ID Type

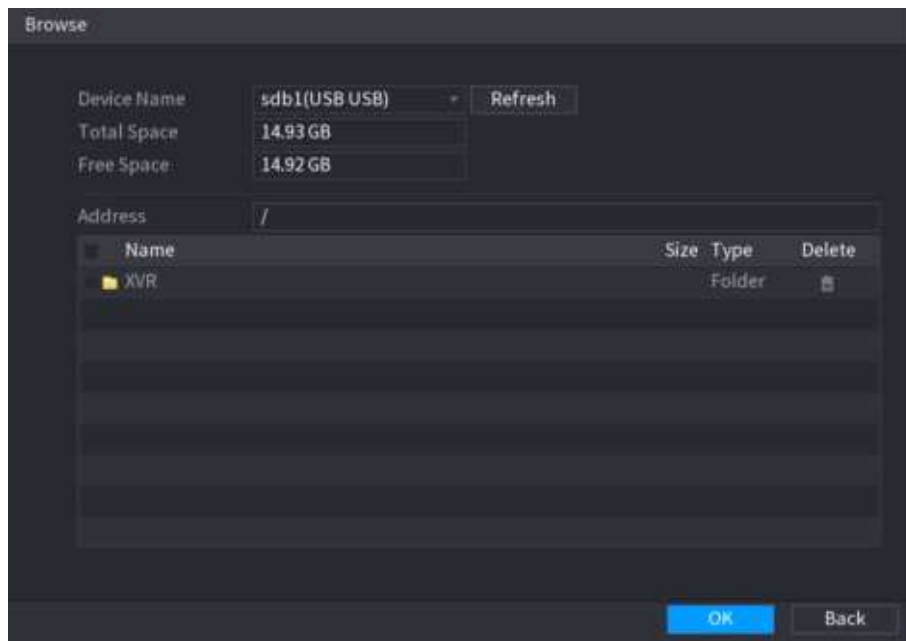
ID No.

Country

Step 4 Click  to add a face picture.

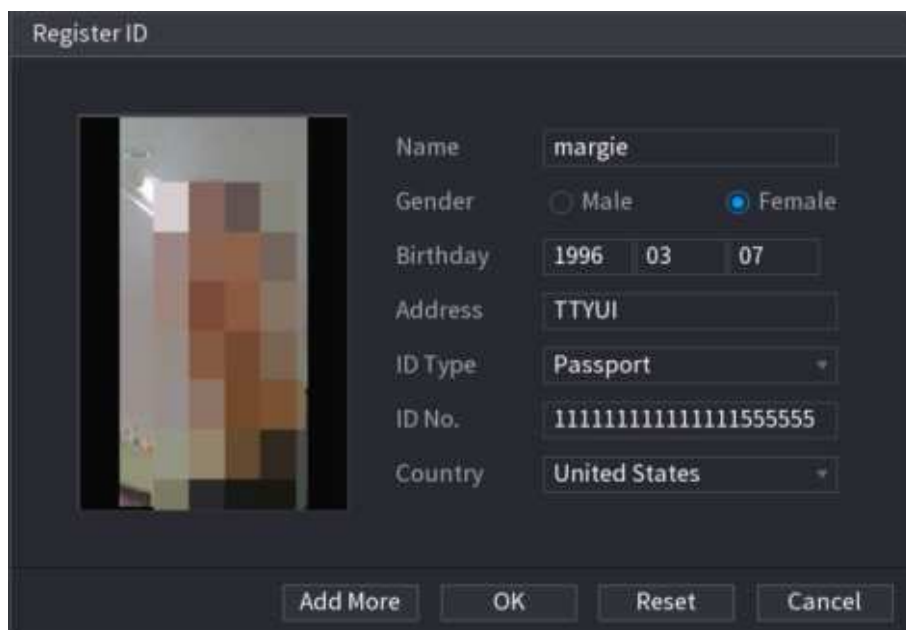
The **Browse** interface is displayed.

Figure 5-148



Step 5 Select a face picture and enter the registration information.

Figure 5-149



Step 6 Click **OK**.

The system prompts the registration is successful.

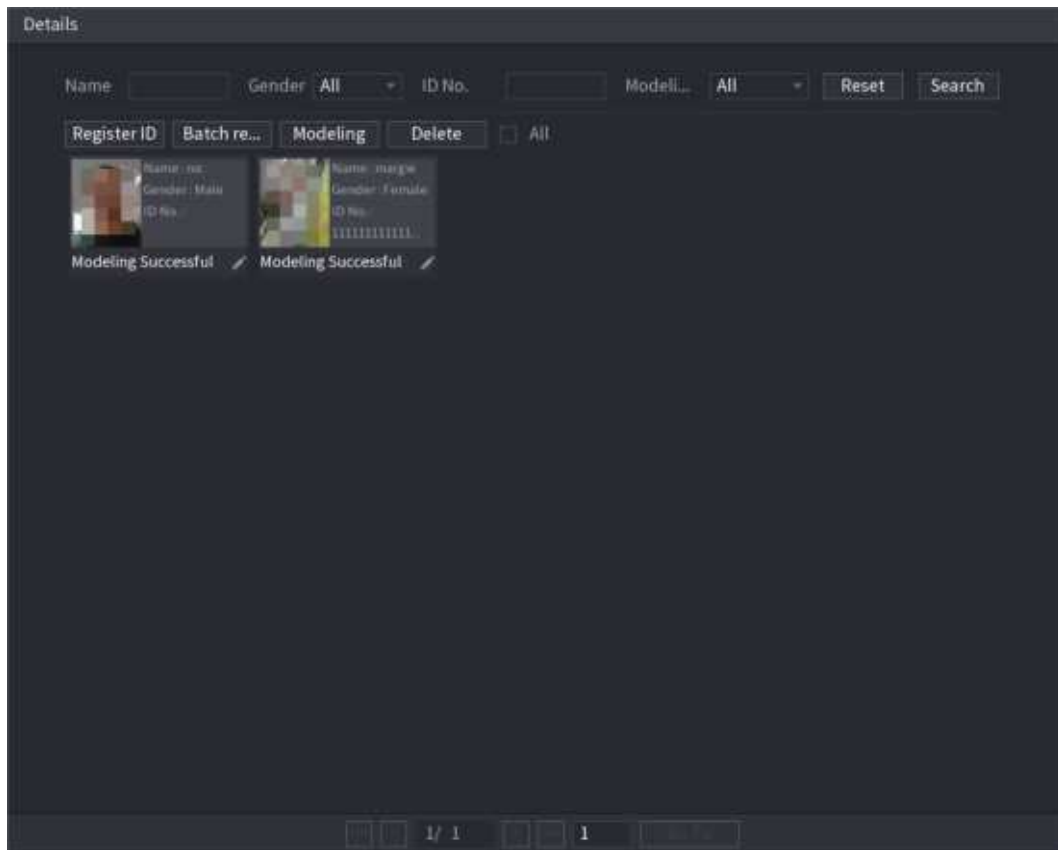
Step 7 On the **Details** interface, click **Search**.

The system prompts modeling is successful.



If the system prompts the message indicating modeling is in process, wait a while and then click **Search** again. If modeling is failed, the registered face picture cannot be used for face recognition.

Figure 5-150



Adding Face Pictures in Batch

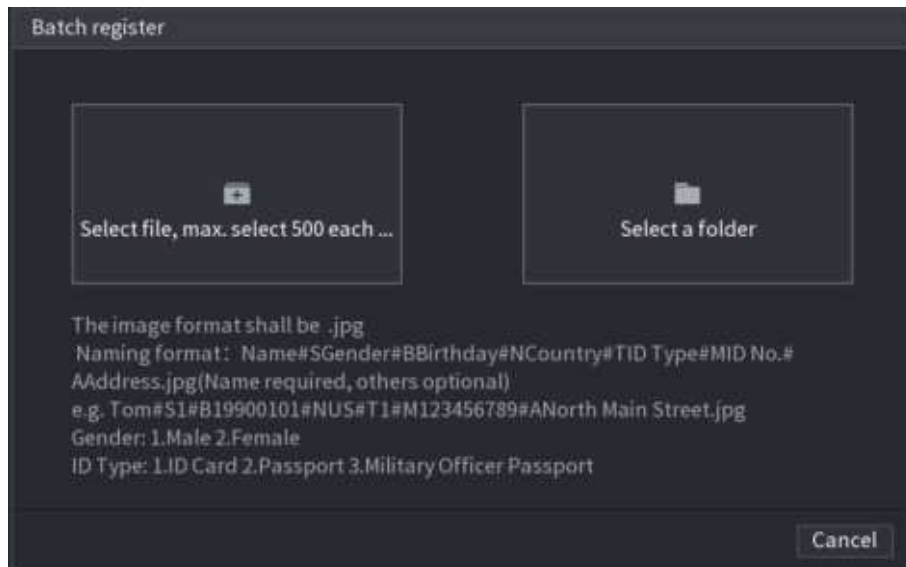
Step 1 Give a name to the face picture by referring to Table 5-47.

Table 5-47

Naming format	Description
Name	Enter the name.
Gender	Enter 1 or 2. 1 represents male, and 2 represents female.
Birthday	Enter numbers in the format of yyyy-mm-dd.
Country	Enter the abbreviation of country. For example, CN for China.
ID Type	1 represents ID card; 2 represents passport; 3 represents military officer password.
ID No.	Enter the ID number.
Address	Enter the address.

Step 2 On the **Details** interface, click **Batch register**.
The **Batch register** interface is displayed.

Figure 5-151



Step 3 Click **Select file, max select 500 each time** or **Select a folder** to import face pictures.

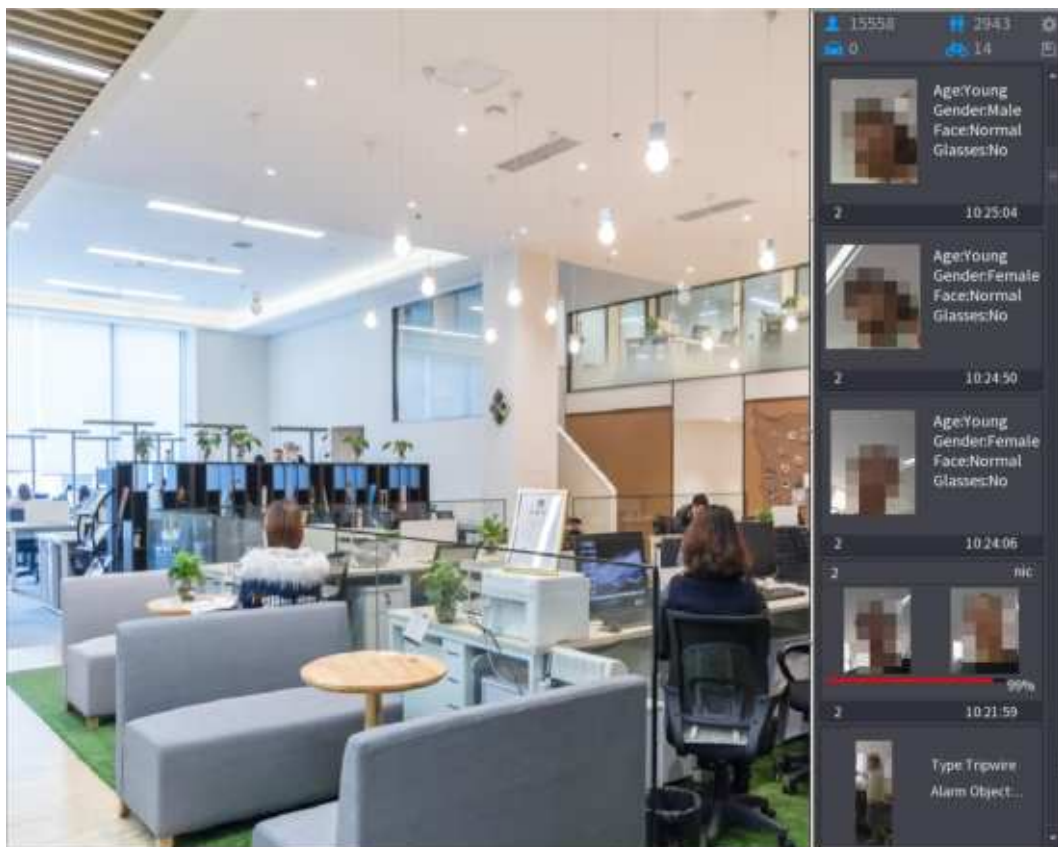
Step 4 Click **OK** to complete batch registration.

Adding the Detected Faces

Step 1 Right-click on the live view screen, and then select **Live Mode > AI Mode**.

The AI Mode live view screen is displayed.

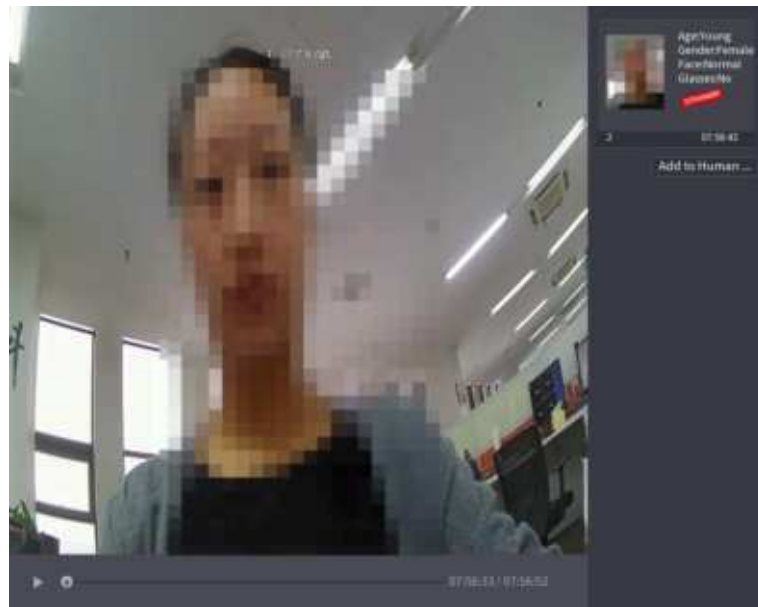
Figure 5-152



Step 2 Double-click the detected face snapshot that you want to add.

The snapshot playing back interface is displayed.

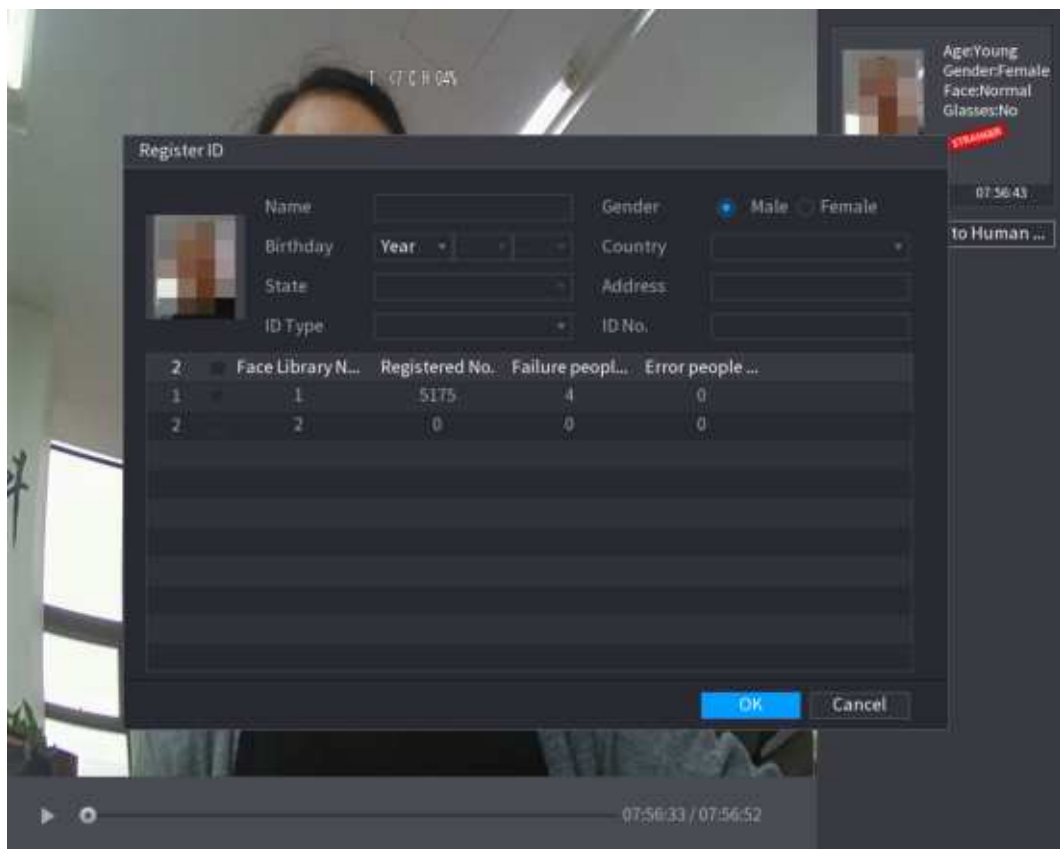
Figure 5-153



Step 3 Click **Add to Human Face Database**.

The **Register ID** interface is displayed.

Figure 5-154



Step 4 Select the face library and enter the ID information.

Step 5 Click **OK** to complete registration.

5.11.1.2.2 Face Recognition Configuration

You can compare the detected faces with the faces in the library to judge if the detected face belongs to the library. The comparison result will be displayed on the AI mode live view screen and smart search interface, and link the alarms.

Step 1 Select **Main Menu > AI > Parameters > Face Recognition**.

The **Face Recognition** interface is displayed.

Figure 5-155

The screenshot shows the 'Face Recognition' configuration window. At the top, there is a 'Channel' dropdown menu set to '1' and an 'Enable' checkbox. Below these are 'Schedule' and 'Target Face Data...' buttons, both labeled 'Setting'. A 'Stranger Alarm' checkbox is also present. The main area contains a table with columns: '0', 'Enable', 'Name', 'Similarity', 'Modify Parameters', and 'Delete'. The table is currently empty. At the bottom, there are 'Default', 'Apply', and 'Back' buttons.

Step 2 In the **Channel** list, select a channel that you want to configure face recognition function, and then enable it.

Step 3 Set the **Schedule**. For details, see "5.10.4.1 Configuring Motion Detection Settings."

Step 4 Set the **Target Face Database**.

1) Click **Setting**.

The **Face Database** interface is displayed.

Figure 5-156

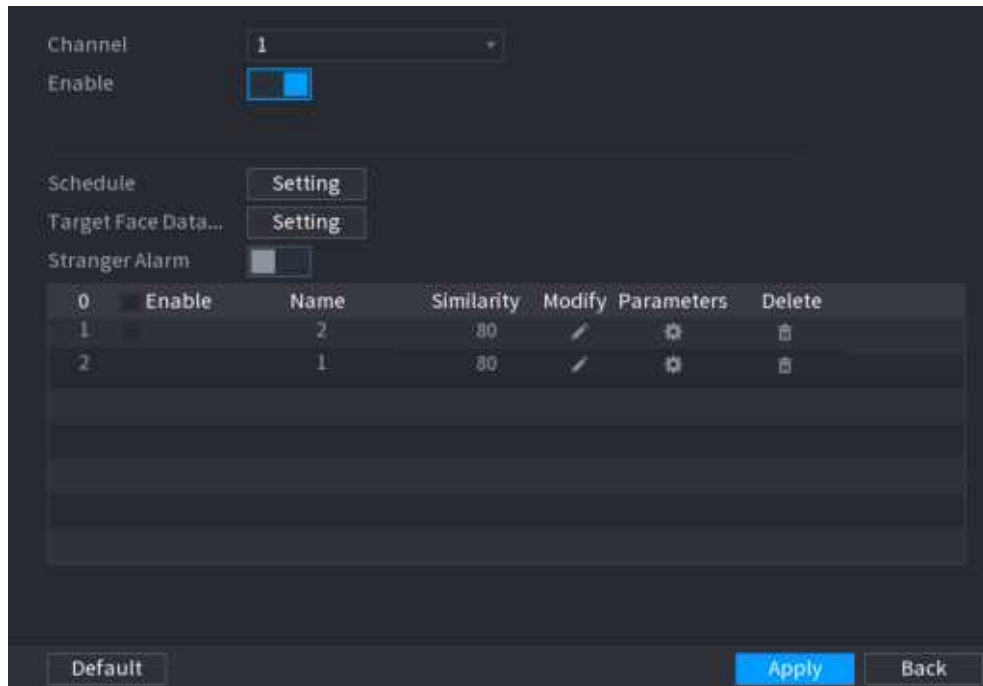
The screenshot shows the 'Face Database' window. It features a table with columns: '0', 'Name', 'Register No.', 'Failed No.', and 'Error No.'. The table is empty. At the bottom right, there are 'OK' and 'Cancel' buttons.

2) Select one or multiple face libraries.

3) Click **OK**.

The selected face library is listed.

Figure 5-157



Step 5 Configure the added face library.

- Click to modify the similarity. The lower the number is, the easier the alarm linkage will trigger.
- Click to delete the face library.
- Click to set the alarm linkage. For details, see Table 5-46.

After setting is completed, click **OK**.

Step 6 (Optional) Enable the **Stranger Mode**.

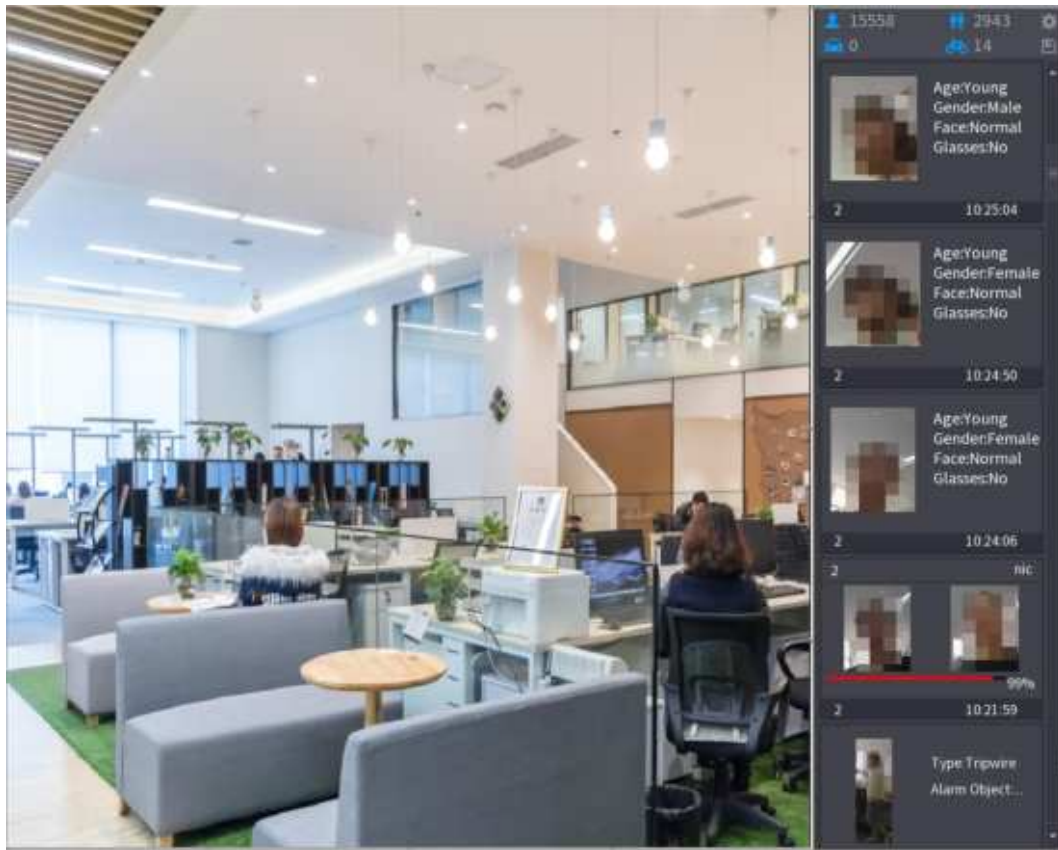
- 1) Enable the Stranger mode (☒). When the detected faces do not belong to the face library, the system remarks the face as "Stranger."
- 2) Click **Setting** to set the alarm linkage. For details, see Table 5-46.
- 3) After setting is completed, click **OK**.

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

After the face recognition function is enabled, right-click on the live view screen, and then select **Live Mode > AI Mode**. The AI mode live view screen is displayed. See Figure 5-158.

- If the detected face belongs to the enabled face library, the similarity result is displayed.
- If the detected face does not belong to the enabled face library, the face will be remarked as "Stranger."

Figure 5-158



5.11.1.2.3 Smart Search for Face Recognition

You can compare the detected faces with the face library and play back.

- Search by attributes: Search the face library by the face attributes.
- Search by picture: Search the face library by uploading face pictures.

Searching by Attributes

Step 1 Select **Main Menu > AI > AI Search > Face Recognition > Search by Attributes**.
The **Search by Attributes** interface is displayed.

Figure 5-159

Search by Attribute Search by Picture

Channel 1

Start Time 2020 -03 -02 00 :00 :00

End Time 2020 -03 -03 00 :00 :00

Gender All

Age All

Glasses All

Beard All

Mouth Mask All

Expression All

Similarity 80 %

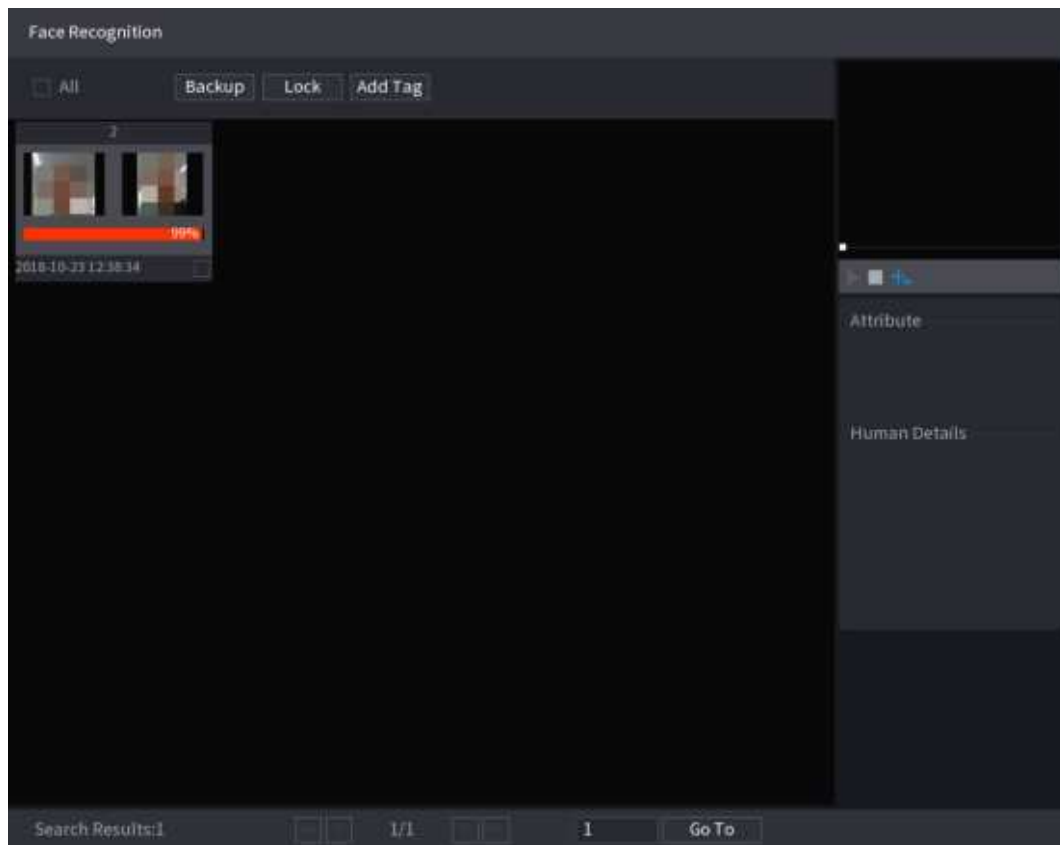
Smart Search

Step 2 Select the channel and set the parameters such as start time, end time, gender, age, glasses, beard, mask, and similarity according to your requirement.

Step 3 Click **Smart Search**.

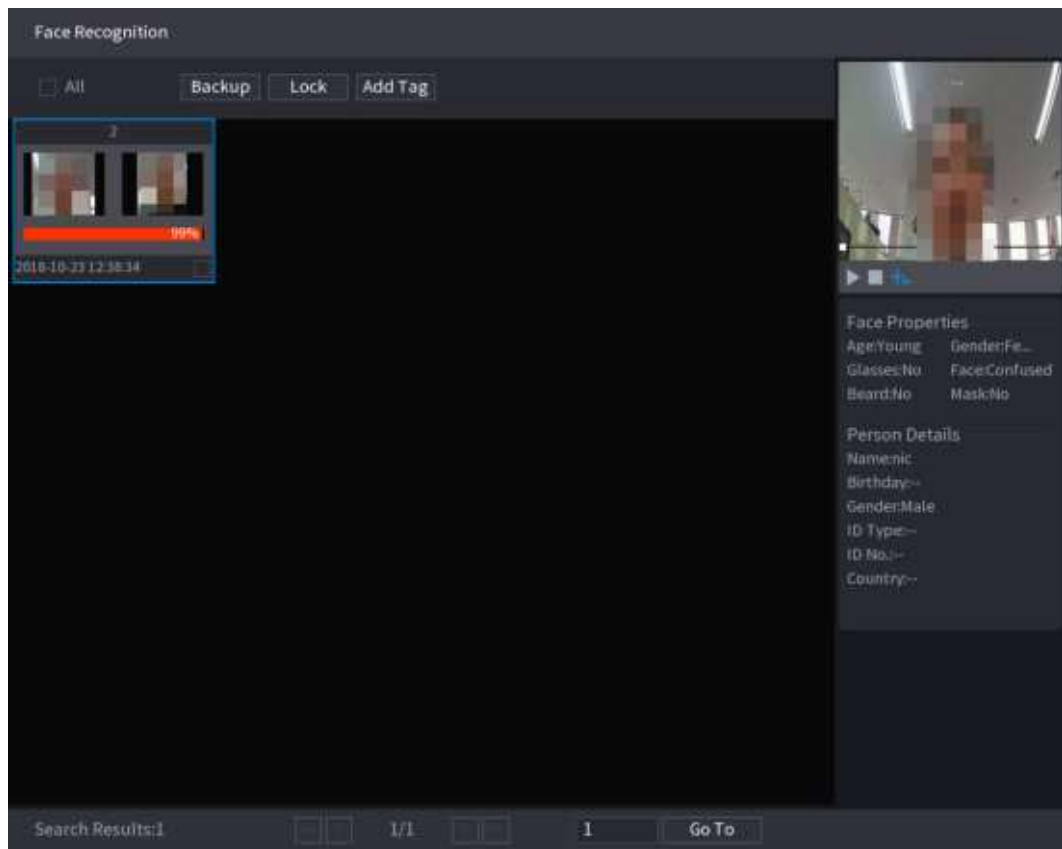
The search result is displayed.

Figure 5-160



- Step 4** Click the picture that you want to play back.
The picture with registered information is displayed.

Figure 5-161



- Step 5** Click  to play back the recorded video.

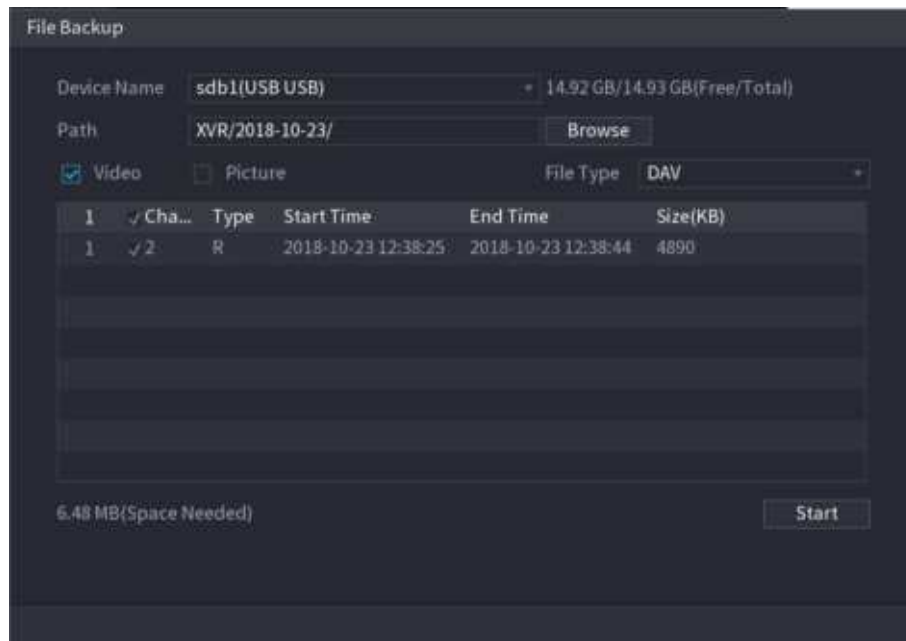


Double-click on the playing interface to switch between full screen playing and thumbnail playing.

You can also do the following operations to the recorded files.

- To export the database file (.csv) to the external storage device, select files, click **Export**, and then select the save path.
- To back up the recorded files to the external storage device, select files, click **Backup**, select the save path and file type, and then click **Start**.

Figure 5-162

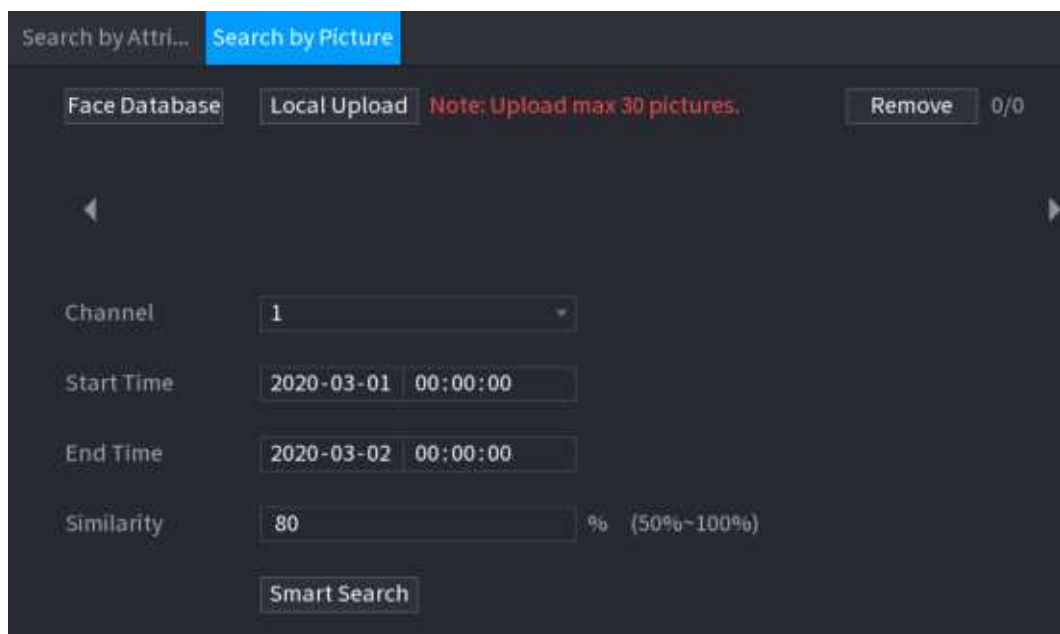


- To lock the files to make it unable to be overwritten, select the files, and then click **Lock**.
- To add a mark to the file, select the files and then click **Add Tag**.

Search by Picture

Step 1 Select **Main Menu > AI > AI Search > Face Recognition > Search by Picture**.
The **Search by Picture** interface is displayed.

Figure 5-163



Step 2 Upload face pictures from **Face Database** or **Local Upload**.

NOTE

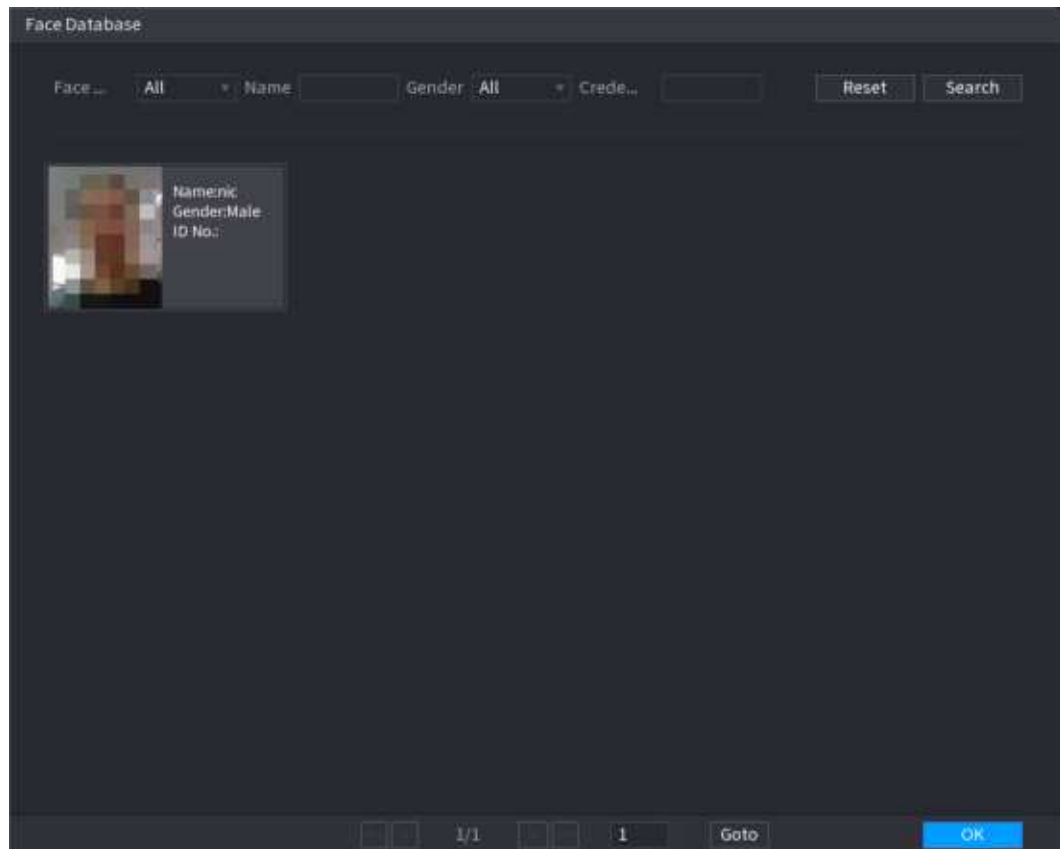
Maximum 30 pictures can be uploaded at one time, and the system support searching 8 pictures at one time.

- Face Database

- 1) Click **Face Database**.

The **Face Database** interface is displayed.

Figure 5-164



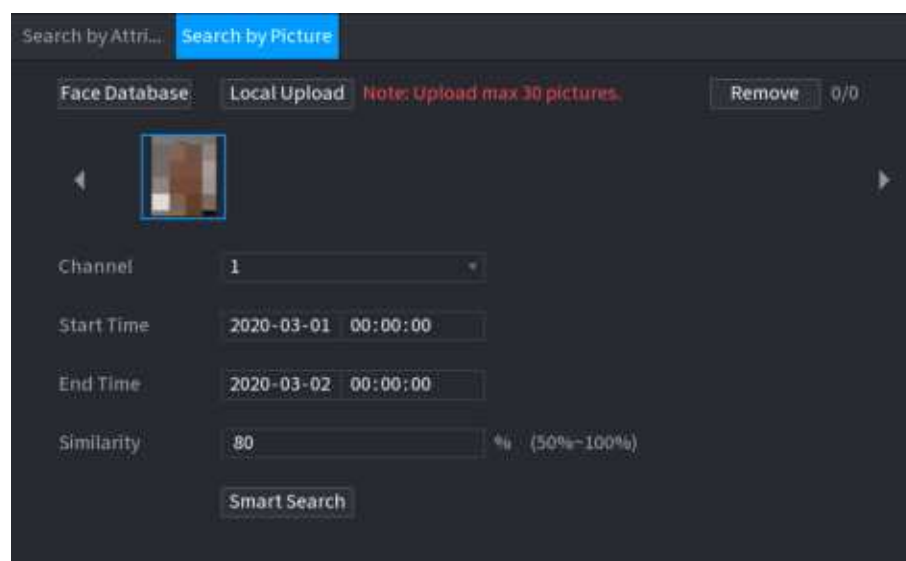
- 2) Set the searching parameters by selecting the face library and gender, and entering name and ID No. according to your actual requirement.
- 3) Click **Search** to display the results that satisfy the requirement.



Click **Reset** to clear the searching parameters.

- 4) Select the picture and then click **OK**.
The picture is displayed on the Search by Picture interface.

Figure 5-165



- Local Upload

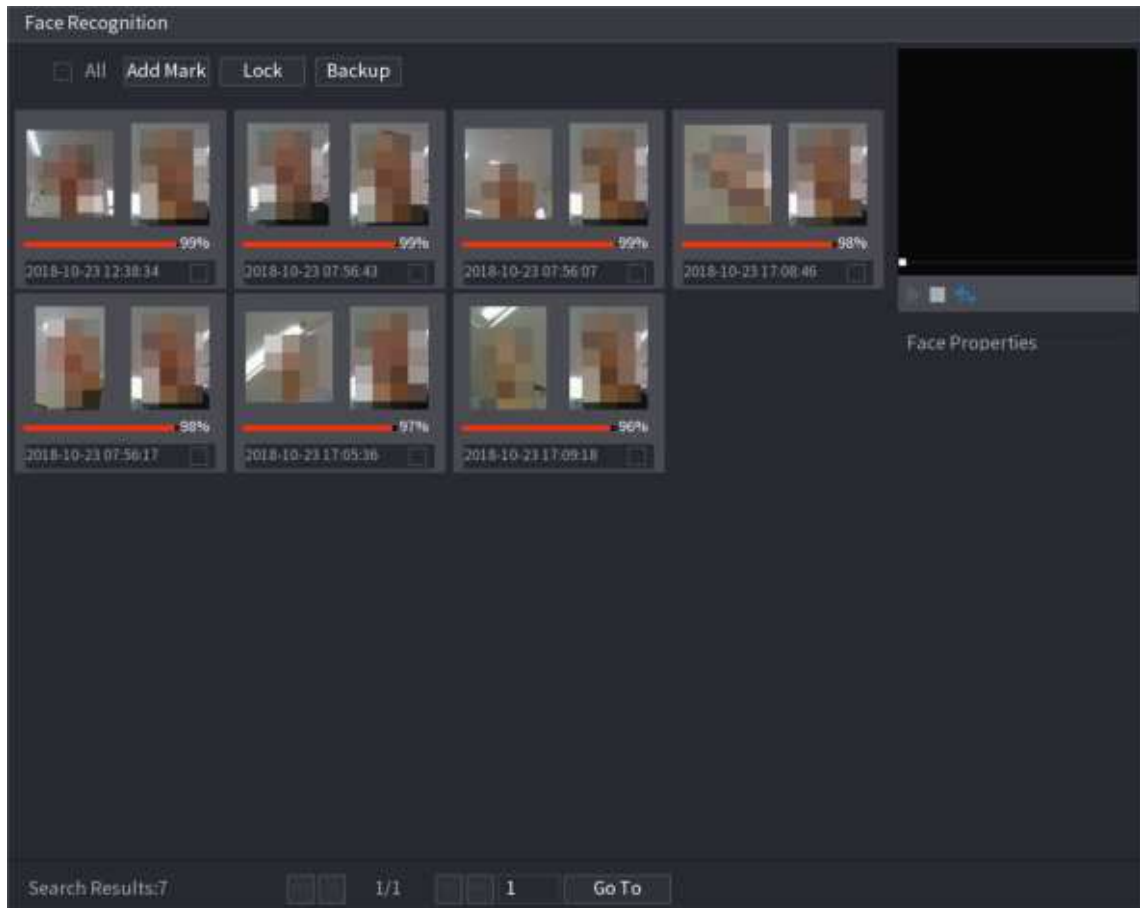
Plug the USB storage device (with face pictures) to the Device, and then click **Local Upload**. Then select the picture from the USB storage device, and then click **OK**. The selected face pictures are uploaded.

Step 3 After the face pictures are uploaded, continue to configure other parameters (channel, start time, end time, and similarity).

Step 4 Click **Smart Search**.

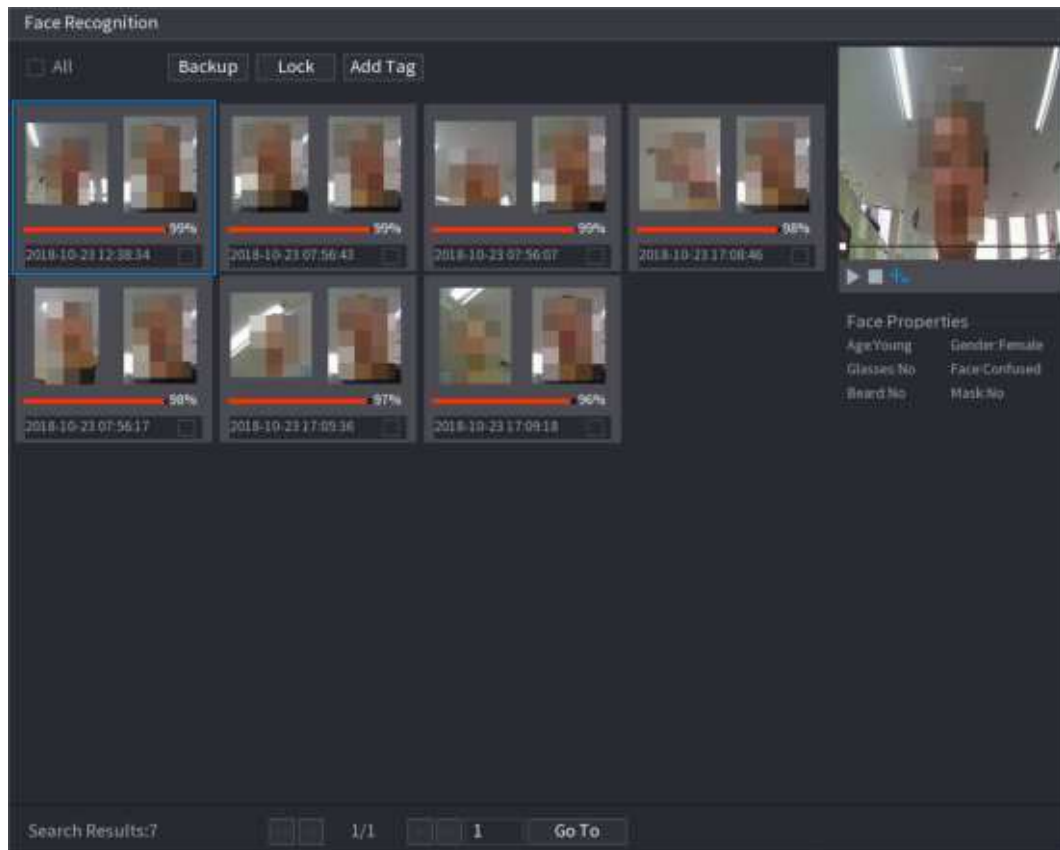
The searching results are displayed.

Figure 5-166



Step 5 Select the face picture that you want to play back.

Figure 5-167



Step 6 Click  to play back the recorded video.

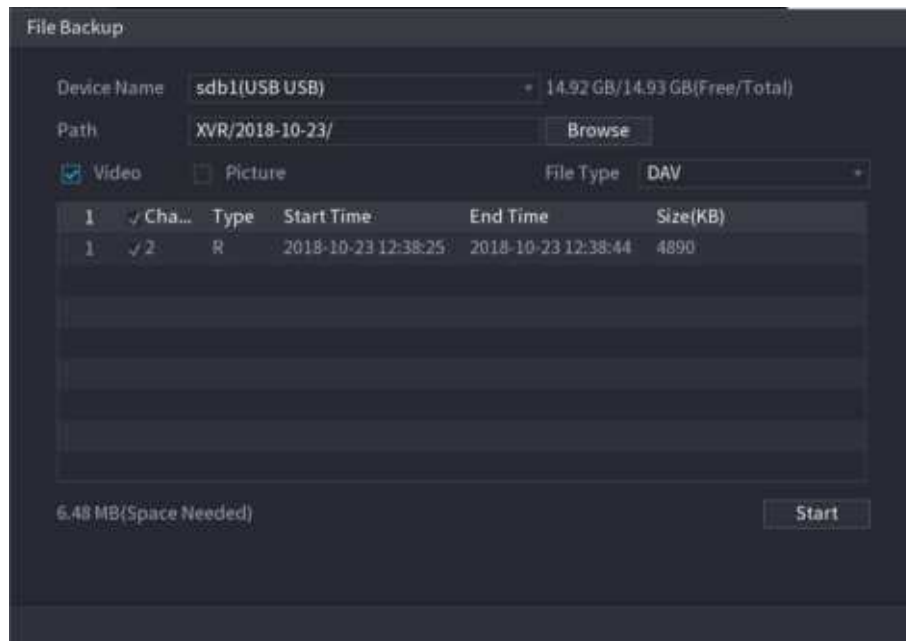


Double-click on the playing interface to switch between full screen playing and thumbnail playing.

You can also do the following operations to the recorded files.

- To add a mark to the file, select the files and then click **Add Tag**.
- To lock the files to make it unable to be overwritten, select the files, and then click **Lock**.
- To back up the recorded files to the external storage device, select files, click **Backup**, select the save path and file type, and then click **Start**.

Figure 5-168



5.11.1.3 IVS Function

The IVS function processes and analyzes the images to extract the key information to match with the preset rules. When the detected behaviors match with the rules, the system activates alarms.



If you select AI by device, then among face detection and recognition, IVS function, and video structuring, you can use one of them at the same time for the same channel.

5.11.1.3.1 Configuring IVS Parameters

The alarms are generated according to the configured parameters.

Step 1 Select **Main Menu > AI > Parameters > IVS**.

The **IVS** interface is displayed.

Figure 5-169

0	Enable	Name	Type	Draw	Trigger	Delete	F

Add

Default Apply Back

Step 2 In the **Channel** list, select the channel number that you want to configure the IVS function.

Step 3 At **Type**, you can select from **AI by Camera** and **AI by Device**.

- **AI by Camera:** This option requires certain AI cameras. The camera will do all the AI analysis, and then give the results to the DVR.
- **AI by Device:** The camera only transmits normal video stream to the DVR, and then the DVR will do all the AI analysis.

Step 4 Click **Add**.

One line of rule is displayed.

Figure 5-170

1	Enable	Name	Type	Draw	Parameters	Delete	F
1	☐	Rule1	Tripwire				F

Add

Step 5 Configure the parameters for the rule that you selected.

Step 6 Select the check box of the rule to enable it.

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

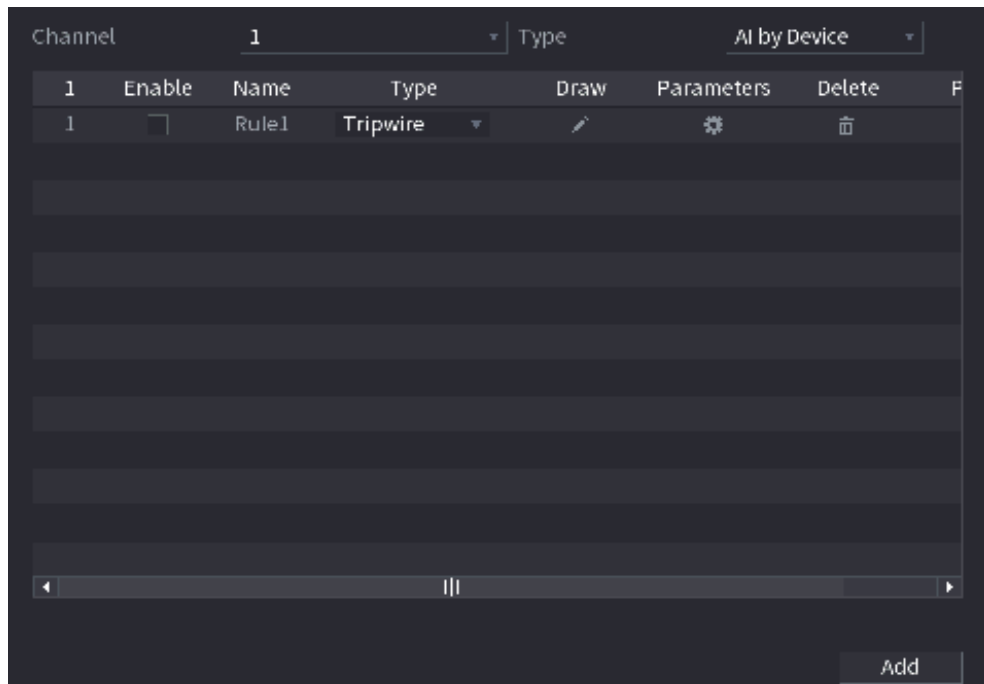
Configuring Tripwire Rules

When the target object crosses the tripwire in the defined direction, the system activates alarms.

- The tripwire can be configured as a straight line or broken line.
- Supports detecting one-way or two-way tripwire crossing.
- Supports multiple tripwires in the same scenario to meet the complexity.
- Supports size filtering for target.

Step 1 On the rule line that you added, in the **Type** list, select **Tripwire**.

Figure 5-171



Step 2 Draw a tripwire.

- 1) In the **Channel** list, select the channel that you want to configure the rules for.
- 2) Click .

The monitoring screen to configure the tripwire rules is displayed.

Figure 5-172



3) Configure the settings for the parameters of drawing rules.

Table 5-48

Parameter	Description
Name	Enter the customized rule name.
Direction	Set the direction of the tripwire. You can choose A to B (left to right), B to A (right to left), and Both .
Target Filter	Click  to draw areas to filter the target. You can configure two filtering targets (maximum size and minimum size). When the target that is crossing the tripwire is smaller than the minimum size or larger than the maximum size, no alarms will be activated. The maximum size should be larger than the minimum size.
Effective Target	Enable the AI Recognition function (). By default, Human and Motor Vehicle are selected for alarm object.

4) Drag to draw a tripwire. The tripwire can be a straight line, broken line or polygon.

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

Step 3 Click  to set the actions to be triggered.

The **Trigger** interface is displayed.

Figure 5-173

Step 4 Configure the triggering parameters.

Table 5-49

Parameter	Description
Schedule	Define a period during which the detection is active. For details, see "Setting Motion Detection Period" section in "5.10.4.1 Configuring Motion Detection Settings."
Alarm-out Port	Click Setting to display setting interface. - General Alarm: Enable general alarm and select the alarm output port. - Ext. Alarm: Connect the alarm box to the Device and then enable it. - Wireless Siren: Connect the wireless gateway to the Device and then enable it. For details, see "5.12 IoT Function." When an alarm event occurs, the system links the peripheral alarm devices connected to the selected output port.
Post-Alarm	Set a length of time for the Device to delay turning off alarm after the external alarm is cancelled. The value ranges from 0 seconds to 300 seconds. If you enter 0, there will be no delay.
Show Message	Select the Show Message check box to enable a pop-up alarm message in your local host PC.
Report Alarm	Select the Report Alarm check box to enable the system to upload the alarm signal to the network (including alarm center) when an alarm event occurs.  - Not all models support this function. - The corresponding parameters in the alarm center should be configured. For details, see "5.15.1.12 Configuring Alarm Center Settings."

Parameter	Description
Send Email	Select the Send Email check box to enable the system to send an email notification when an alarm event occurs.  To use this function, make sure the email function is enabled in Main Menu > NETWORK > EMAIL.
Record Channel	Select the channel(s) that you want to record. The selected channel(s) starts recording after an alarm event occurs.  The recording for intelligence event and auto recording function must be enabled. For details, see "5.1.4.9 Configuring Recorded Video Storage Schedule" and "5.9.1 Enabling Record Control."
PTZ Linkage	Click Setting to display the PTZ interface. Enable PTZ linkage actions, such as selecting the preset that you want to be called when an alarm event occurs.  To use this function, the PTZ operations must be configured. For details, see "5.4 Controlling PTZ Cameras."
Post-Record	Set a length of time for the Device to delay turning off recording after the alarm is cancelled. The value ranges from 10 seconds to 300 seconds.
Tour	Select the Tour check box to enable a tour of the selected channels.  • To use this function, the tour setting must be configured. • After the tour is ended, the live view screen returns to the view layout before tour started.
Picture Storage	Select the Picture Storage check box to take a snapshot of the selected channel.  To use this function, make sure the snapshot function is enabled for Intel in Main Menu > STORAGE > Schedule > Picture Storage.
Video Matrix	Select the check box to enable the function. When an alarm event occurs, the video output port outputs the settings configured in "Main Menu > DISPLAY > Tour > Sub Screen."  • Not all models support this function. • The extra screen must be enabled to support this function.
Buzzer	Select the check box to activate a buzzer noise at the Device.
Log	Select the check box to enable the Device to record a local alarm log.
Alarm Tone	Select to enable audio broadcast in response to a face detection event.

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

Step 6 Select the **Enable** check box, and then click **Apply**.

The tripwire detecting function is active. When the target object crosses the tripwire in the defined direction, the system activates alarms.

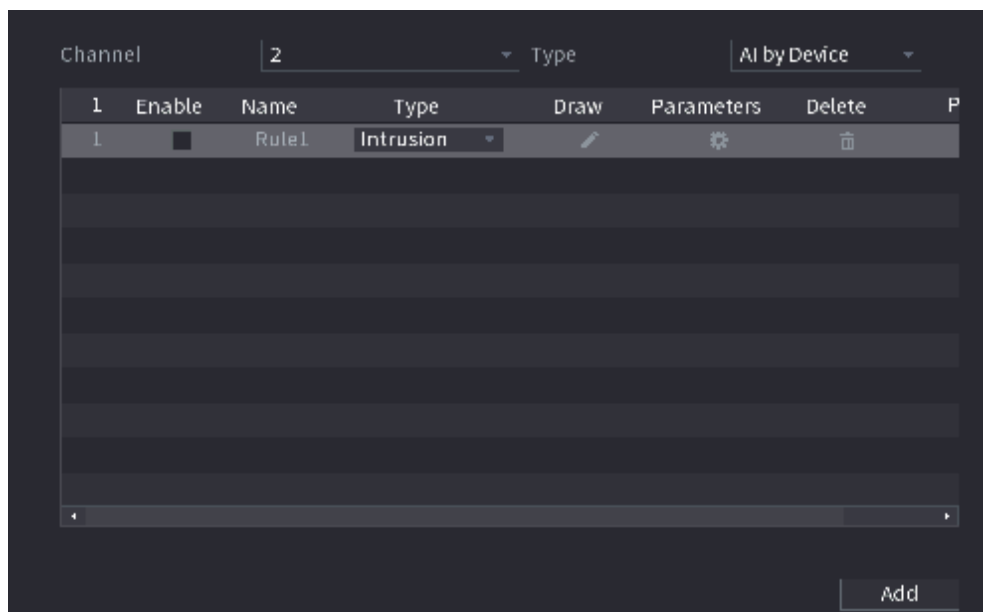
Configuring Intrusion Rules

When the target enters and leaves the defined detection area, or the target appears in the defined area, the system activates alarms.

- You can define the shape and quantity of intrusion areas.
- Supports detecting the behaviors that enter and leave the intrusion areas.
- Supports detecting the behaviors that are moving in the intrusion areas. The quantity of areas and lasting time can be configured.
- Supports size filtering for target.

Step 1 On the rule line that you added, in the **Type** list, select **Intrusion**.

Figure 5-174



Step 2 Draw an area.

- 1) In the **Channel** list, select the channel that you want to configure the rules for.
- 2) Click

The monitoring screen to configure the intrusion rules is displayed.

Figure 5-175



3) Configure the settings for the parameters of drawing rules.

Table 5-50

Parameter	Description
Name	Enter the customized rule name.
Action	Configure the actions that are defined as intrusion. You can select the Appear check box and the Cross check box.
Direction	In the Direction list, select the direction of crossing the configured area. You can select Enter&Exit , Enter , and Exit .
Target Filter	Click  to draw areas to filter the target.  You can configure two filtering targets (maximum size and minimum size). When the target that is crossing the tripwire is smaller than the minimum size or larger than the maximum size, no alarms will be activated. The maximum size should be larger than the minimum size.
Effective Target	Enable the AI Recognition function (). By default, Human and Motor Vehicle are selected for alarm object.

4) Drag to draw an area.

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

Step 3 Click  to set the actions to be triggered. For details, see Table 5-49.

Step 4 Select the **Enable** check box, and then click **Apply**.

The intrusion detecting function is active. When the target enters and leaves the area, or the target appears in the defined area, the system activates alarms.

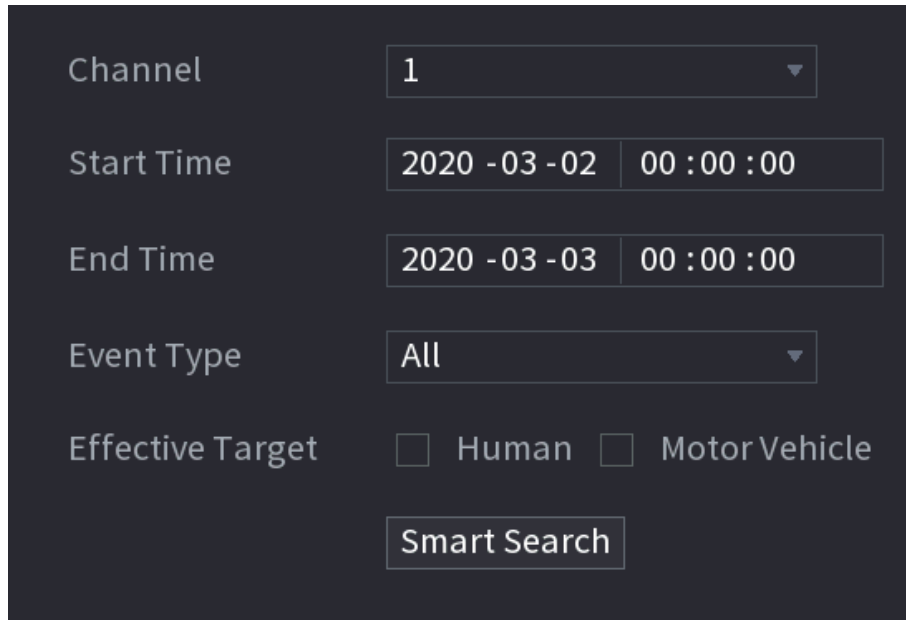
5.11.1.3.2 Smart Search for IVS Function

You can search for the intelligent events and play back.

Step 1 Select **Main Menu > AI > SMART SEARCH > IVS**.

The **IVS** interface is displayed.

Figure 5-176



The screenshot displays the IVS Smart Search interface with the following fields and controls:

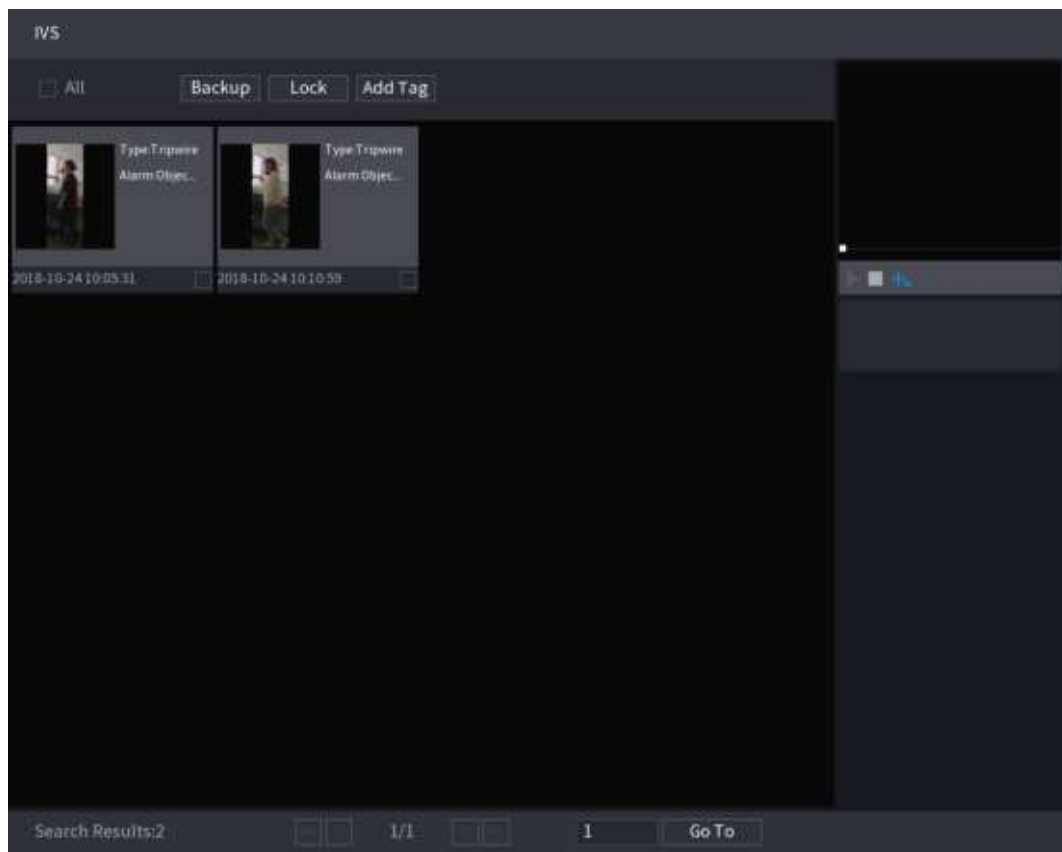
- Channel:** A dropdown menu currently showing '1'.
- Start Time:** A date and time selector showing '2020 -03 -02' and '00 :00 :00'.
- End Time:** A date and time selector showing '2020 -03 -03' and '00 :00 :00'.
- Event Type:** A dropdown menu currently showing 'All'.
- Effective Target:** Two checkboxes labeled 'Human' and 'Motor Vehicle', both of which are currently unchecked.
- Smart Search:** A button located at the bottom of the form.

Step 2 In the **Channel** list, select the channel that you want to search for the events, and then set other parameters such as start time, end time, event type, and alarm object.

Step 3 Click **Smart Search**.

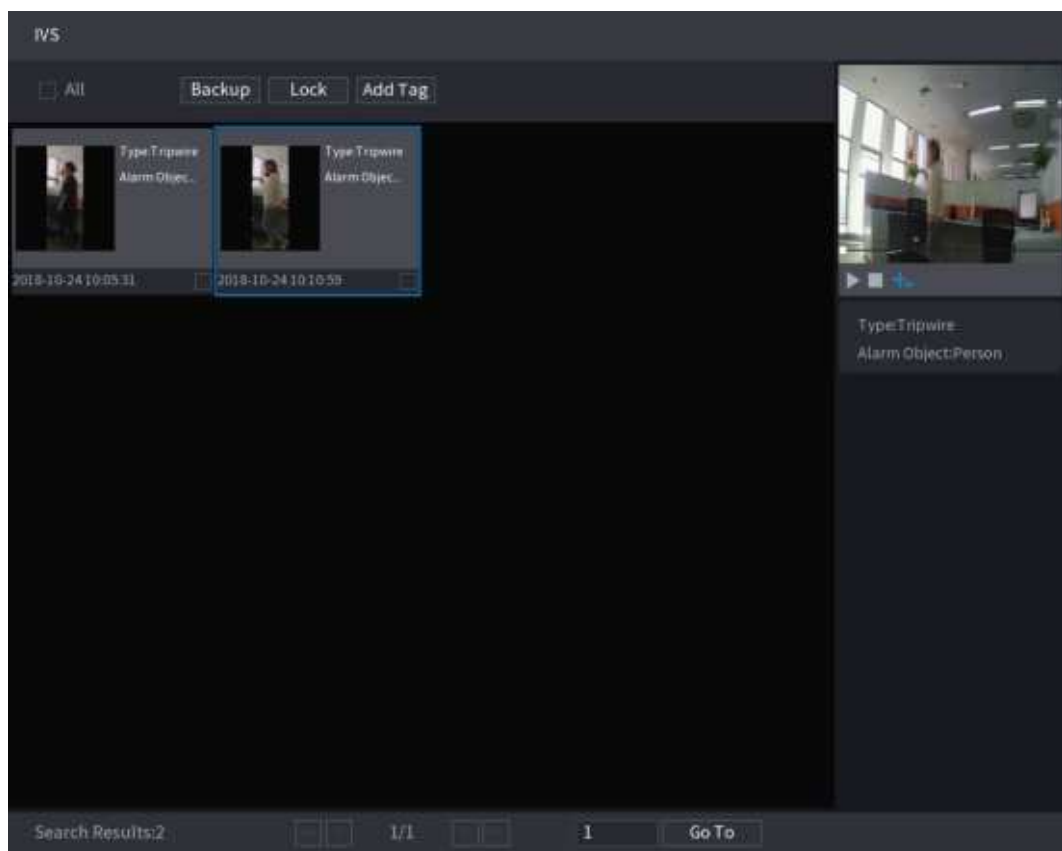
The results that satisfy the searching conditions are displayed.

Figure 5-177



Step 4 Click the picture that you want to play back.

Figure 5-178



Step 5 Click  to play back the recorded video.

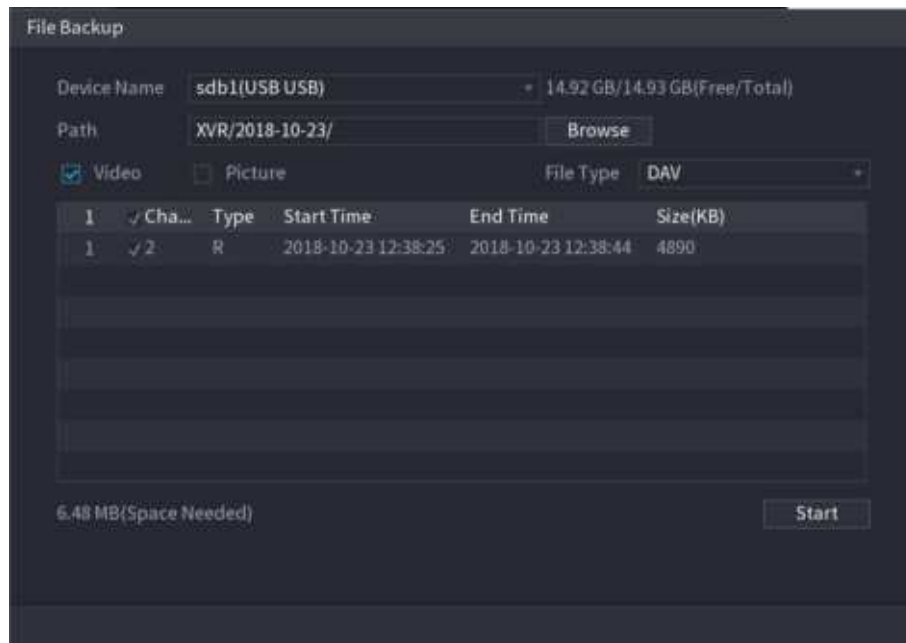


Double-click on the playing interface to switch between full screen playing and thumbnail playing.

You can also do the following operations to the recorded files.

- To back up the recorded files to the external storage device, select files, click **Backup**, select the save path and file type, and then click **Start**.

Figure 5-179



- To lock the files to make it unable to be overwritten, select the files, and then click **Lock**.
- To add a mark to the file, select the files and then click **Add Tag**.

5.11.1.4 Video Structuring

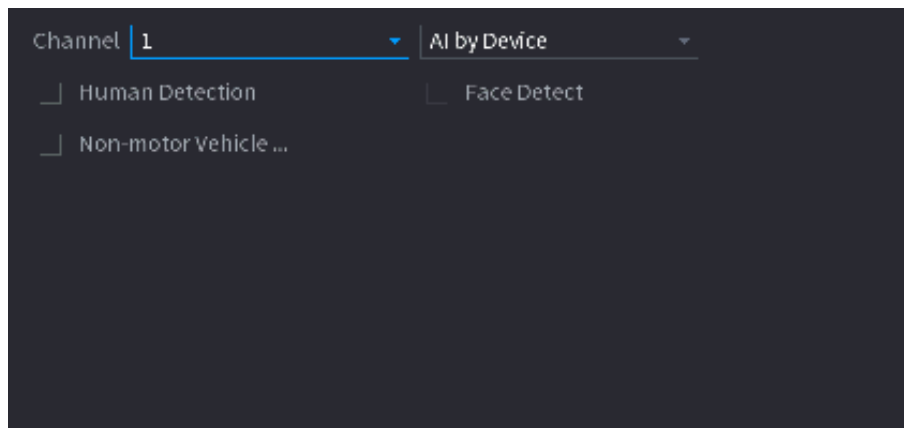
The device can detect and extract key features from the human bodies and non-motor vehicles in the video, and then build a structured database. You can search any target you need with these features.

5.11.1.4.1 Configuring Video Structuring

Step 1 Select **Main Menu > AI > Parameters > Video Structuring**.

The **Video Structuring** interface is displayed.

Figure 5-180



Step 2 In the **Channel** list, select a channel that you want to configure video structuring function, and then enable it.

Step 3 At **Type**, you can select from **AI by Camera** and **AI by Device**.

- **AI by Camera:** This option requires certain AI cameras. The camera will do all the AI analysis, and then give the results to the DVR.
- **AI by Device:** The camera only transmits normal video stream to the DVR, and then the DVR will do all the AI analysis.

Step 4 You can select from **Human Detection**, **Face Detect**, and **Non-motor Vehicle**.

- **Human Detection:** Select this option, and then the device will analyze all the human body features in the video, including Top, Top Color, Bottom, Bottom Color, Hat, Bag, Gender, Age, and Umbrella. You can search the target you need with these features. See "Human Body Detection" in "5.11.1.4.2 Smart Search for Video Structuring."
- **Face Detect:** You need to select **Human Detection** first, and then you can select this option. If you select this option, and there is any human face appears in the video, then there will be an extra face image and some extra face features in the human body detection results, including Glasses, Expression, Mask, and Beard. You can search the target you need with these features. See "Human Body Detection" in "5.11.1.4.2 Smart Search for Video Structuring."
- **Non-motor Vehicle:** Select this option, and then the device will analyze all the non-motor vehicle features in the video, including Type, Vehicle Color, People Number, and Helmet. You can search the target you need with these features. See "Non-motor Vehicle Detection" in "5.11.1.4.2 Smart Search for Video Structuring."

Step 5 Click **Apply**.

5.11.1.4.2 Smart Search for Video Structuring

You can search the target you need with human body features or non-motor vehicle features

Human Body Detection

Step 1 Select **Main Menu > AI > SMART SEARCH > Human Body Detection**.

The **Human Body Detection** interface is displayed.

Figure 5-181

Channel	1
Start Time	2019 -05 -13 00 :00 :00
End Time	2019 -05 -13 23 :59 :59
Top	All
Top Color	All
Bottom	All
Bottom Color	All
Hat	All
Bag	All
Gender	All
Age	All
Umbrella	All
Smart Se...	

Step 2 Select the channel and the time, and then select one or multiple features from **Top**, **Top Color**, **Bottom**, **Bottom Color**, **Hat**, **Bag**, **Gender**, **Age**, or **Umbrella**.

Step 3 Click **Smart Search**. The search result is displayed.

- If you only selected **Human Body Detection** and did not select **Face Detection** in "5.11.1.4.1 Configuring Video Structuring", there will be only human body features displayed in the results.

Figure 5-182

HUMAN BODY DETECTION

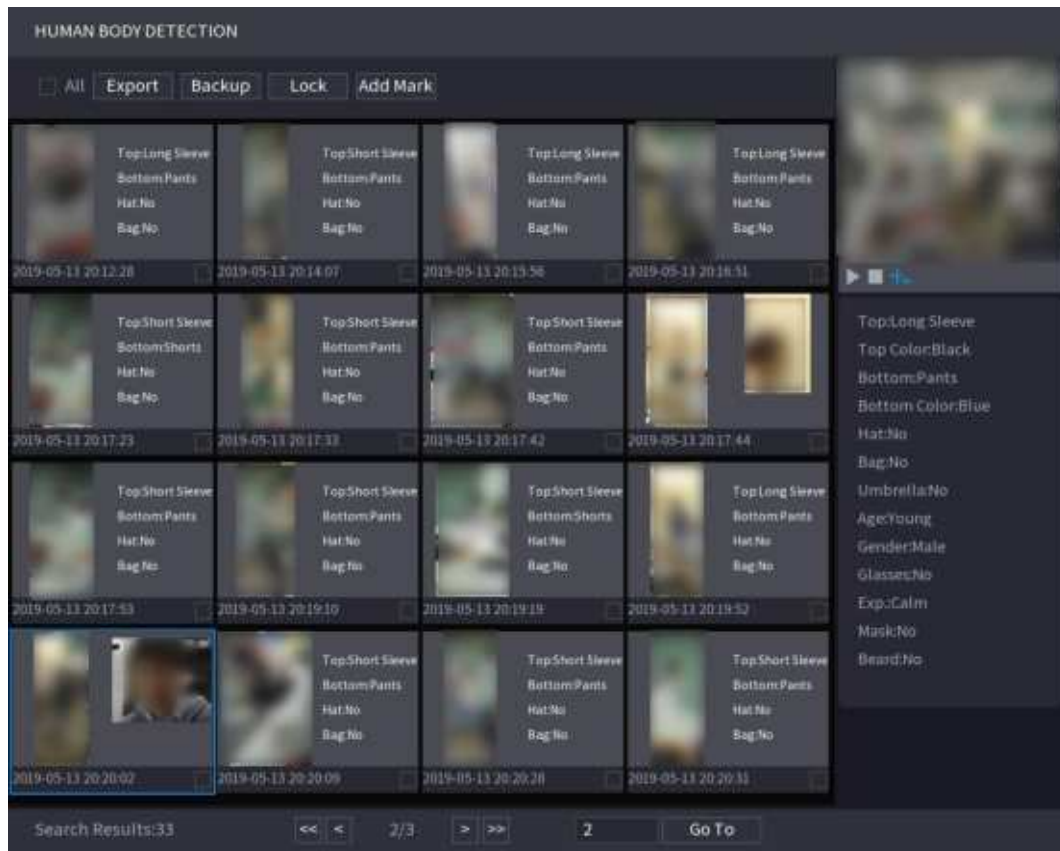
☐ All

 Top:Long Sleeve Bottom:Pants Hat:No Bag:No 2019-05-13 20:12:28	 Top:Short Sleeve Bottom:Pants Hat:No Bag:No 2019-05-13 20:14:07	 Top:Long Sleeve Bottom:Pants Hat:No Bag:No 2019-05-13 20:15:58	 Top:Long Sleeve Bottom:Pants Hat:No Bag:No 2019-05-13 20:16:51	 Top:Long Sleeve Top Color:Black Bottom:Pants Bottom Color:Blue Hat:No Bag:No Umbrella:No Age:Young Gender:Male
 Top:Short Sleeve Bottom:Shorts Hat:No Bag:No 2019-05-13 20:17:23	 Top:Short Sleeve Bottom:Pants Hat:No Bag:No 2019-05-13 20:17:38	 Top:Short Sleeve Bottom:Pants Hat:No Bag:No 2019-05-13 20:17:42	 Top:Short Sleeve Bottom:Pants Hat:No Bag:No 2019-05-13 20:19:10	
 Top:Short Sleeve Bottom:Pants Hat:No Bag:No 2019-05-13 20:17:53	 Top:Short Sleeve Bottom:Pants Hat:No Bag:No 2019-05-13 20:19:10	 Top:Short Sleeve Bottom:Shorts Hat:No Bag:No 2019-05-13 20:19:18	 Top:Long Sleeve Bottom:Pants Hat:No Bag:No 2019-05-13 20:19:52	
 Top:Short Sleeve Bottom:Pants Hat:No Bag:No 2019-05-13 20:19:10	 Top:Short Sleeve Bottom:Pants Hat:No Bag:No 2019-05-13 20:20:09	 Top:Short Sleeve Bottom:Pants Hat:No Bag:No 2019-05-13 20:20:20	 Top:Short Sleeve Bottom:Pants Hat:No Bag:No 2019-05-13 20:20:31	

Search Results:33 << < 2/3 > >> 2 Go To

- If you selected **Human Body Detection** and **Face Detection** in "5.11.1.4.1 Configuring Video Structuring", and there is any human face appears in the video, there will be extra face features displayed in the results.

Figure 5-183



Step 4 Select one or multiple results, and then you can

- Click **Export** to export them to the USB device
- Click **Backup** to make backup in the DVR
- Click **Lock** so that they don't get overwritten or deleted
- Click **Add Tag** to name them as needed.

Non-motor Vehicle Detection

Step 1 Select **Main Menu > AI > AI Search > Non-motor Vehicle Detection**.

The **Non-motor Vehicle Detection** interface is displayed.

Figure 5-184

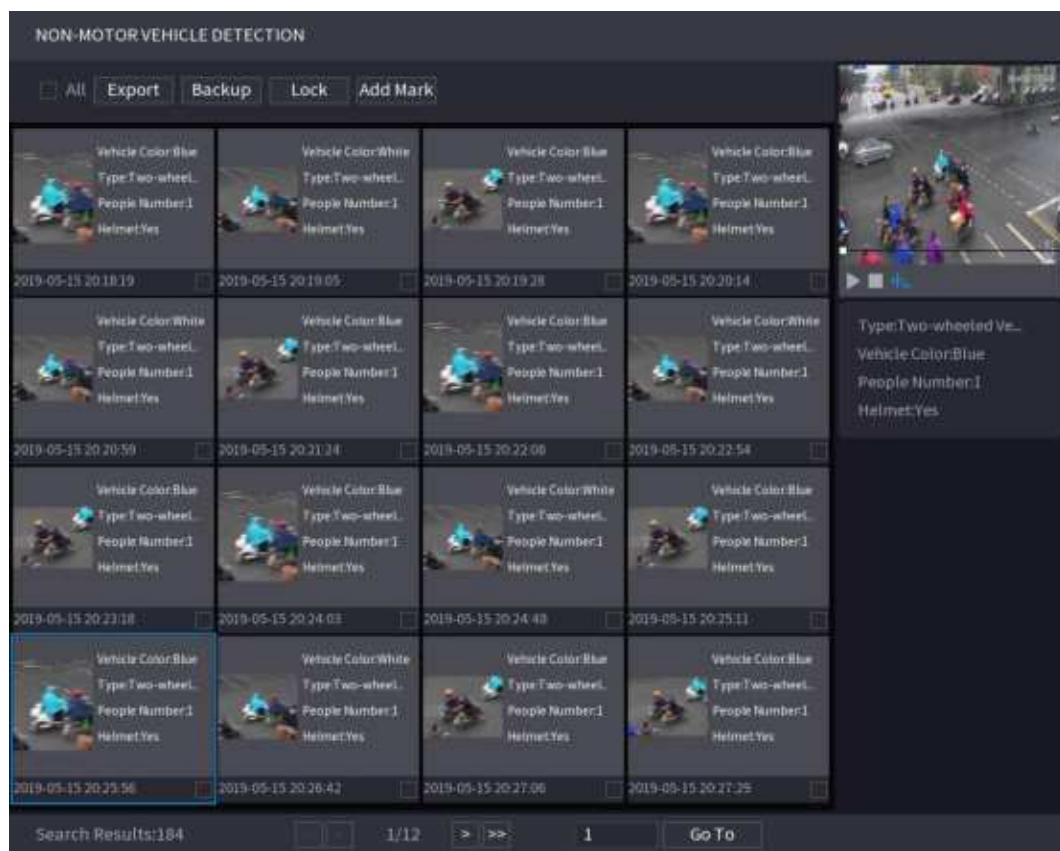
Channel	1
Start Time	2019 -05 -13 00 :00 :00
End Time	2019 -05 -13 23 :59 :59
Type	All
Vehicle Color	All
People Number	All
Helmet	All
Smart Se...	

Step 2 Select the channel and the time, and then select one or multiple features from **Type**, **Vehicle Color**, **People Number**, or **Helmet**.

Step 3 Click **Smart Search**.

The search result is displayed.

Figure 5-185



Step 4 Select one or multiple results, and then you can

- Click **Export** to export them to the USB device
- Click **Backup** to make backup in the DVR

- Click **Lock** so that they don't get overwritten or deleted
- Click **Add Tag** to name them as needed.

5.11.2 For Lite AI Series

AI module provides SMD (Smart Motion Detection) and IVS functions. These functions take effect after they are configured and enabled. It adopts deep learning and can realize precision alarms. You can only enable one of them to the same channel at the same time.

- SMD: The device can detect and classify humans and vehicles in the image.
- IVS: The IVS function processes and analyzes the human and vehicle images to extract the key information to match with the preset rules. When the detected behaviors match with the rules, the system activates alarms. The IVS function can avoid wrong alarms by filtering the factors such as rains, light, and animals.
- Face detection: The Device can analyze the faces captured by the camera and link the configured alarms. This function is available for XVR5X-I and XVR 7X-I series only.
- Face recognition: The Device can compare the captured faces with the face library and then link the configured alarms. This function is available for XVR 7X-I series only.



SMD, face detection, face recognition and IVS cannot be enabled simultaneously on select models. For details, see 5.1.4.2 Configuring General Settings.

5.11.2.1 SMD

The device can detect and classify humans and vehicles in the image.

5.11.2.1.1 Configuring SMD Parameters

Step 1 Select **Main Menu > AI > Parameters > SMD**.

The **SMD** interface is displayed.

Figure 5-186

Step 2 In the **Channel** list, select a channel that you want to configure face detection function, and then enable it.

Step 3 Configure the parameters.

Table 5-51

Parameter	Description
Channel	In the Channel list, select a channel to set the motion detection.
Enable	Enable or disable the motion detection function.
Sensitivity	Set the sensitivity for smart motion detection.
Effective Target	Select human or motor vehicle or both.
Schedule	Define a period during which the motion detection is active.
Anti-Dither	Configure the time period from end of event detection to the stop of alarm.
Alarm-out Port	Click Setting to display setting interface. - General Alarm: Enable alarm activation through the alarm devices connected to the selected output port. - External Alarm: Enable alarm activation through the connected alarm box. - Wireless Siren: Enable alarm activation through devices connected by USB gateway or camera gateway.
Post-Alarm	Set a length of time for the Device to delay turning off alarm after the external alarm is cancelled. The value ranges from 0 seconds to 300 seconds, and the default value is 10 seconds. If you enter 0, there will be no delay.
Show Message	Select the Show Message check box to enable a pop-up message in your local host PC.
Report Alarm	Select the Report Alarm check box to enable the system to upload the alarm signal to the network (including alarm center) when an alarm event occurs.
Send Email	Select the Send Email check box to enable the system to send an email notification when an alarm event occurs.  To use this function, make sure the email function is enabled in Main Menu > NETWORK > Email .
Record Channel	Select the channel(s) that you want to record. The selected channel(s) starts recording after an alarm event occurs.  The recording for motion detection and auto recording function must be enabled. For details, see "5.1.4.9 Configuring Recorded Video Storage Schedule" and "5.9.1 Enabling Record Control."
PTZ Linkage	Click Setting to display the PTZ interface. Enable PTZ linkage actions, such as selecting the preset that you want to be called when an alarm event occurs.  Motion Detect can only activate PTZ preset.

Parameter	Description
Post Record	Set a length of time for the Device to delay turning off recording after the alarm is cancelled. The value ranges from 10 seconds to 300 seconds, and the default value is 10 seconds.
Tour	Select the Tour check box to enable a tour of the selected channels.
Picture Storage	Select the Snapshot check box to take a snapshot of the selected channel.  To use this function, select Main Menu > CAMERA > Encode > Snapshot , in the Type list, select Event .
Sub Screen	Select the check box to enable the function. When an alarm event occurs, the extra screen outputs the settings configured in Main Menu > DISPLAY > Tour > Sub Screen .  • Not all models support this function. • To use this function, extra screen shall be enabled.
Video Matrix	Select the check box to enable the function. When an alarm event occurs, the video output port outputs the settings configured in Main Menu > DISPLAY > Tour .  Not all models support this function.
Buzzer	Select the check box to activate a buzzer noise at the Device.
Log	Select the check box to enable the Device to record a local alarm log.
Alarm Tone	Select to enable audio broadcast/alarm tones in response to a motion detection event.
White Light	Select the check box to enable white light alarm of the camera.
Siren	Select the check box to enable sound alarm of the camera.

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

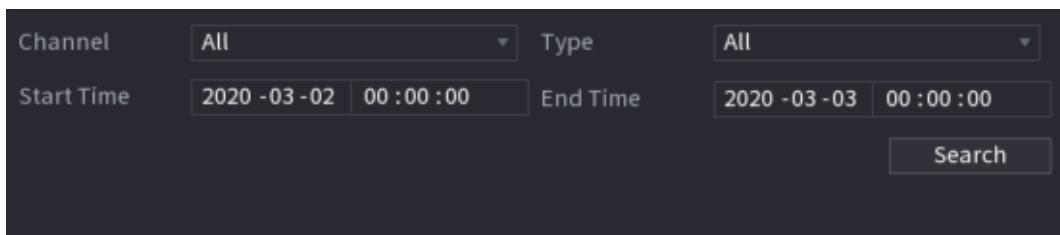
5.11.2.1.2 Searching for SMD Reports

You can search the detection history by channel, object type, and time.

Step 1 Select **Main Menu > AI > AI Search > SMD**.

The **SMD** interface is displayed.

Figure 5-187



The screenshot shows a search interface with the following fields:

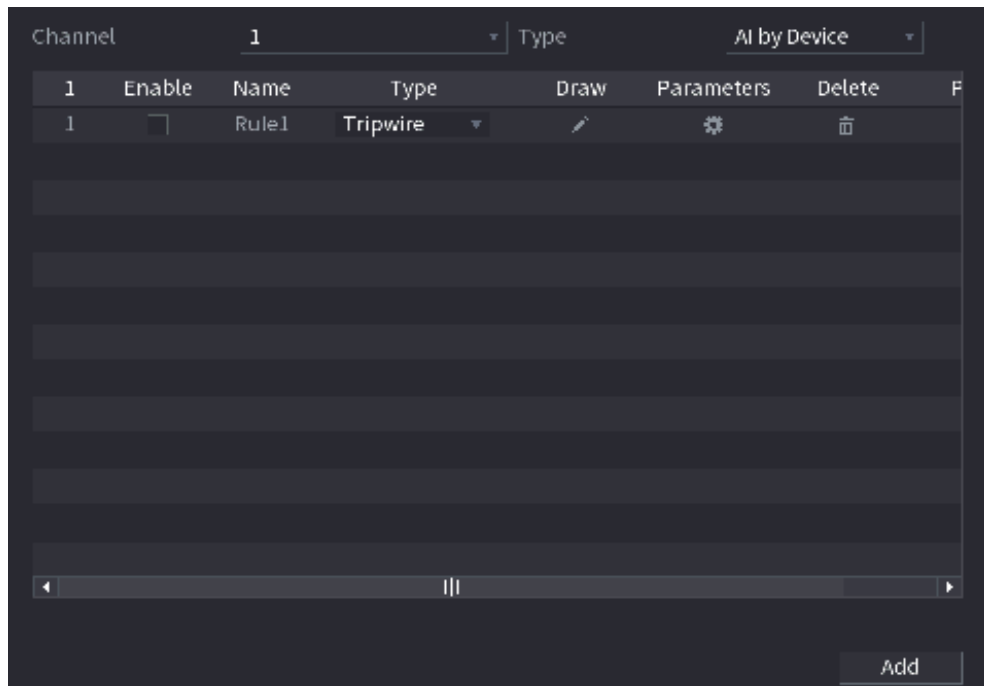
- Channel:** A dropdown menu currently set to "All".
- Type:** A dropdown menu currently set to "All".
- Start Time:** A date and time input field showing "2020 -03 -02 00 :00 :00".
- End Time:** A date and time input field showing "2020 -03 -03 00 :00 :00".
- Search:** A button located at the bottom right of the form.

Step 2 Select the channel, enter the start time and end time, and select the object type you need.

Step 3 Click **Search**.

The results are displayed.

Figure 5-189



Step 4 Configure the parameters for the rule that you selected.

Step 5 Select the check box of the rule to enable it.

Step 6 Click **Apply** to complete the settings.

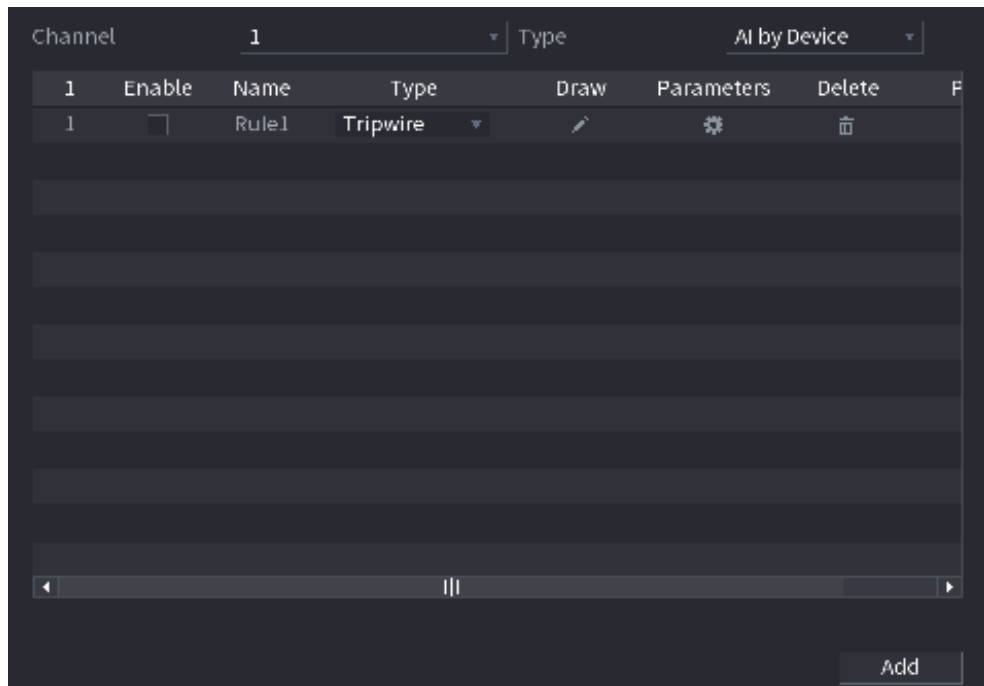
Configuring Tripwire Rules

When the target object crosses the tripwire in the defined direction, the system activates alarms.

- The tripwire can be configured as a straight line or broken line.
- Supports detecting one-way or two-way tripwire crossing.
- Supports multiple tripwires in the same scenario to meet the complexity.
- Supports size filtering for target.

Step 1 On the rule line that you added, in the **Type** list, select **Tripwire**.

Figure 5-190



Step 2 Draw a tripwire.

1) In the **Channel** list, select the channel that you want to configure the rules for.

2) Click

The monitoring screen to configure the tripwire rules is displayed.

Figure 5-191



3) Configure the settings for the parameters of drawing rules.

Table 5-52

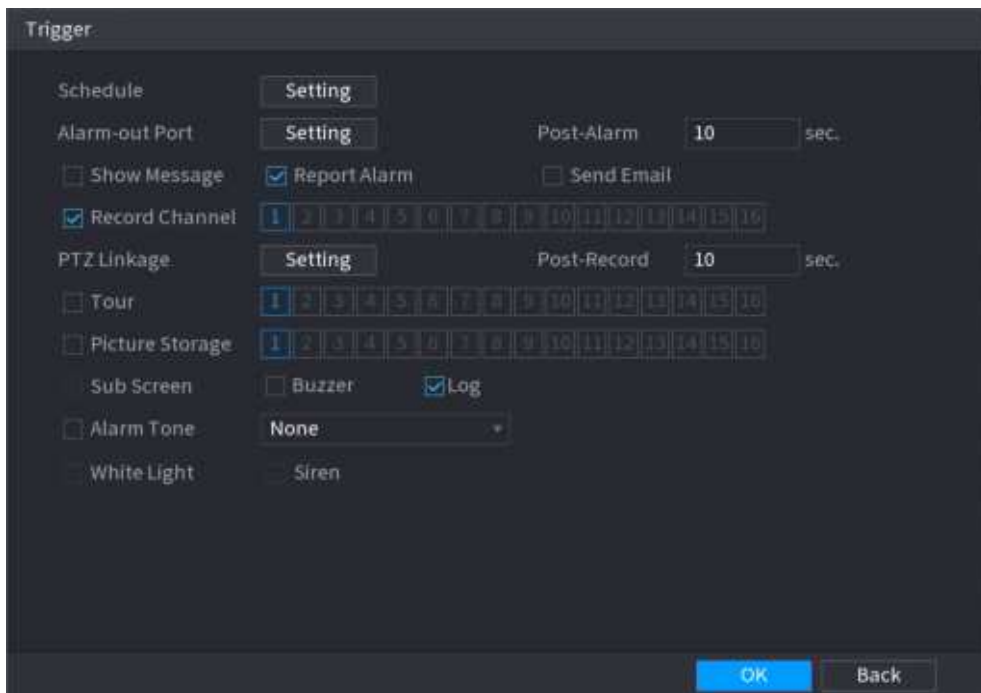
Parameter	Description
Name	Enter the customized rule name.
Direction	Set the direction of the tripwire. You can choose A to B (left to right), B to A (right to left), and Both .
Target Filter	Click  to draw areas to filter the target. You can configure two filtering targets (maximum size and minimum size). When the target that is crossing the tripwire is smaller than the minimum size or larger than the maximum size, no alarms will be activated. The maximum size should be larger than the minimum size.
Effective Target	Enable the AI Recognition function (). By default, Human and Motor Vehicle are selected for alarm object.

- 4) Drag to draw a tripwire. The tripwire can be a straight line, broken line or polygon.
- 5) Click **OK** to save the settings.

Step 3 Click  to set the actions to be triggered.

The **Trigger** interface is displayed.

Figure 5-192



Step 4 Configure the triggering parameters.

Table 5-53

Parameter	Description
Schedule	Define a period during which the detection is active. For details, see "Setting Motion Detection Period" section in "5.10.4.1 Configuring Motion Detection Settings."

Parameter	Description
Alarm-out Port	Click Setting to display setting interface. - General Alarm: Enable general alarm and select the alarm output port. - Ext. Alarm: Connect the alarm box to the Device and then enable it. Wireless Siren: Connect the wireless gateway to the Device and then enable it. For details, see "5.12 IoT Function." When an alarm event occurs, the system links the peripheral alarm devices connected to the selected output port.
Post-Alarm	Set a length of time for the Device to delay turning off alarm after the external alarm is cancelled. The value ranges from 0 seconds to 300 seconds. If you enter 0, there will be no delay.
Show Message	Select the Show Message check box to enable a pop-up alarm message in your local host PC.
Report Alarm	Select the Report Alarm check box to enable the system to upload the alarm signal to the network (including alarm center) when an alarm event occurs.  - Not all models support this function. - The corresponding parameters in the alarm center should be configured. For details, see "5.15.1.12 Configuring Alarm Center Settings."
Send Email	Select the Send Email check box to enable the system to send an email notification when an alarm event occurs.  To use this function, make sure the email function is enabled in Main Menu > NETWORK > Email.
Record Channel	Select the channel(s) that you want to record. The selected channel(s) starts recording after an alarm event occurs.  The recording for intelligence event and auto recording function must be enabled. For details, see "5.1.4.9 Configuring Recorded Video Storage Schedule" and "5.9.1 Enabling Record Control."
PTZ Linkage	Click Setting to display the PTZ interface. Enable PTZ linkage actions, such as selecting the preset that you want to be called when an alarm event occurs.  To use this function, the PTZ operations must be configured. For details, see "5.4 Controlling PTZ Cameras."
Post-Record	Set a length of time for the Device to delay turning off recording after the alarm is cancelled. The value ranges from 10 seconds to 300 seconds.

Parameter	Description
Tour	Select the Tour check box to enable a tour of the selected channels.  - To use this function, the tour setting must be configured. - After the tour is ended, the live view screen returns to the view layout before tour started.
Picture Storage	Select the Snapshot check box to take a snapshot of the selected channel.  To use this function, make sure the snapshot function is enabled for Intel in Main Menu > STORAGE > Schedule > Snapshot.
Video Matrix	Select the check box to enable the function. When an alarm event occurs, the video output port outputs the settings configured in "Main Menu > DISPLAY > Tour > Sub Screen."  - Not all models support this function. - The extra screen must be enabled to support this function.
Buzzer	Select the check box to activate a buzzer noise at the Device.
Log	Select the check box to enable the Device to record a local alarm log.
Alarm Tone	Select to enable audio broadcast in response to a face detection event.

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

Step 6 Select the **Enable** check box, and then click **Apply**.

The tripwire detecting function is active. When the target object crosses the tripwire in the defined direction, the system activates alarms.

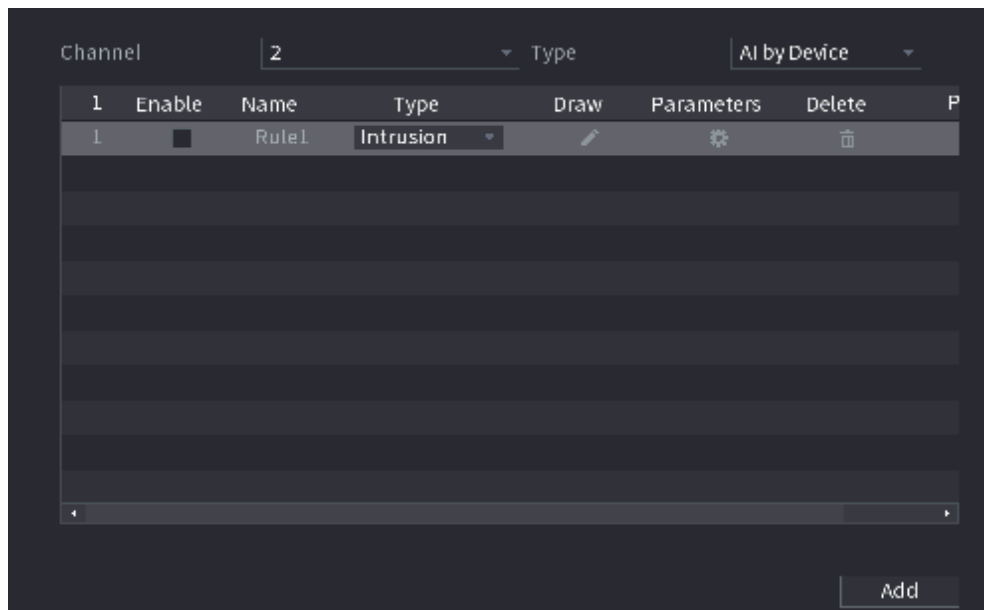
Configuring Intrusion Rules

When the target enters and leaves the defined detection area, or the target appears in the defined area, the system activates alarms.

- You can define the shape and quantity of intrusion areas.
- Supports detecting the behaviors that enter and leave the intrusion areas.
- Supports detecting the behaviors that are moving in the intrusion areas. The quantity of areas and lasting time can be configured.
- Supports size filtering for target.

Step 1 On the rule line that you added, in the **Type** list, select **Intrusion**.

Figure 5-193



Step 2 Draw an area.

1) In the **Channel** list, select the channel that you want to configure the rules for.

2) Click

The monitoring screen to configure the intrusion rules is displayed.

Figure 5-194



3) Configure the settings for the parameters of drawing rules.

Table 5-54

Parameter	Description
Name	Enter the customized rule name.
Action	Configure the actions that are defined as intrusion. You can select the Appear check box and the Cross check box.
Direction	In the Direction list, select the direction of crossing the configured area. You can select Enter&Exit , Enter , and Exit .
Target Filter	Click  to draw areas to filter the target.  You can configure two filtering targets (maximum size and minimum size). When the target that is crossing the tripwire is smaller than the minimum size or larger than the maximum size, no alarms will be activated. The maximum size should be larger than the minimum size.
Effective Target	Enable the AI Recognition function (). By default, Human and Motor Vehicle are selected for alarm object.

- 4) Drag to draw an area.
- 5) Click **OK** to save the settings.

Step 3 Click  to set the actions to be triggered. For details, see Table 5-53.

Step 4 Select the **Enable** check box, and then click **Apply**.

The intrusion detecting function is active. When the target enters and leaves the area, or the target appears in the defined area, the system activates alarms.

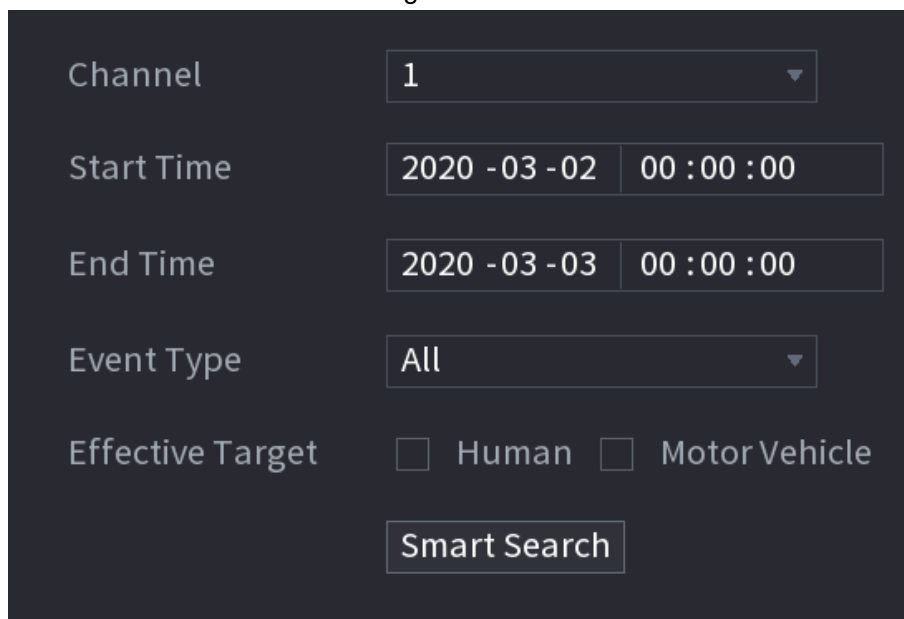
5.11.2.2.2 Smart Search for IVS Function

You can search for the intelligent events and play back.

Step 1 Select **Main Menu > AI > AI Search > IVS**.

The **IVS** interface is displayed.

Figure 5-195



The screenshot shows a dark-themed interface for the IVS Smart Search function. It includes the following elements:

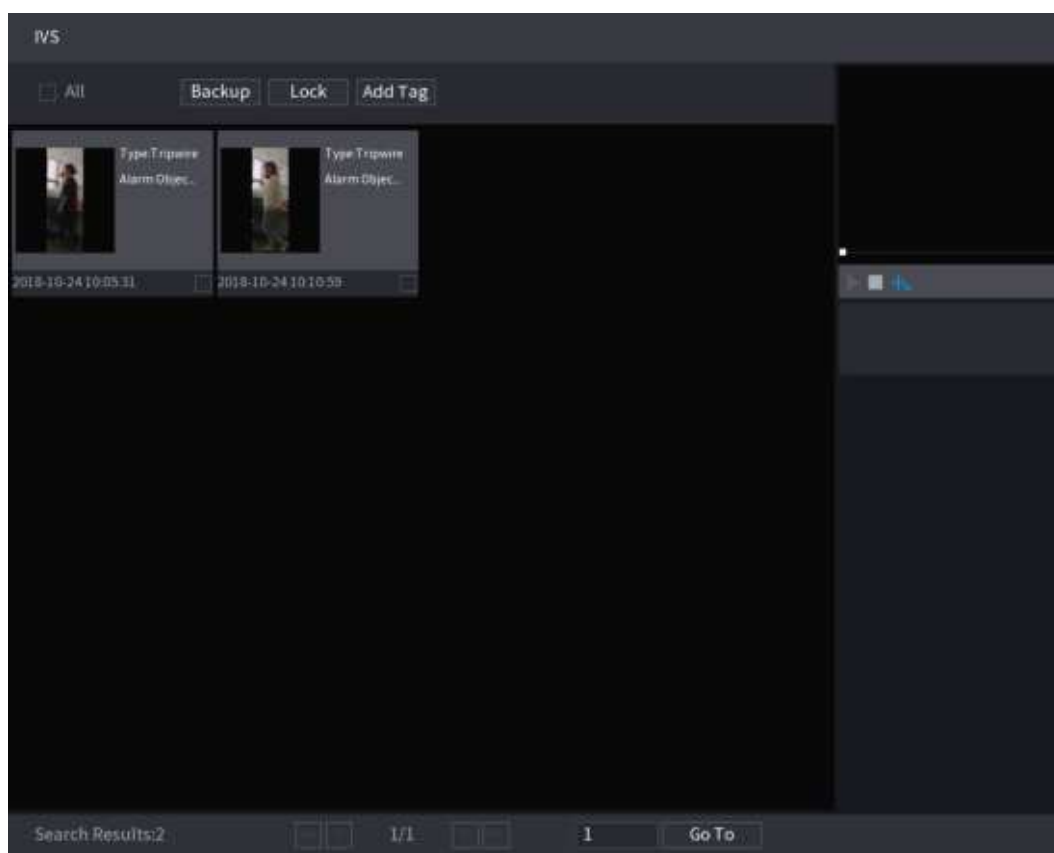
- Channel:** A dropdown menu currently set to '1'.
- Start Time:** Two input fields showing '2020 -03 -02' and '00 :00 :00'.
- End Time:** Two input fields showing '2020 -03 -03' and '00 :00 :00'.
- Event Type:** A dropdown menu currently set to 'All'.
- Effective Target:** Two checkboxes labeled 'Human' and 'Motor Vehicle', both of which are currently unchecked.
- Smart Search:** A prominent button at the bottom center of the form.

Step 2 In the **Channel** list, select the channel that you want to search for the events, and then set other parameters such as start time, end time, event type, and alarm object.

Step 3 Click **Smart Search**.

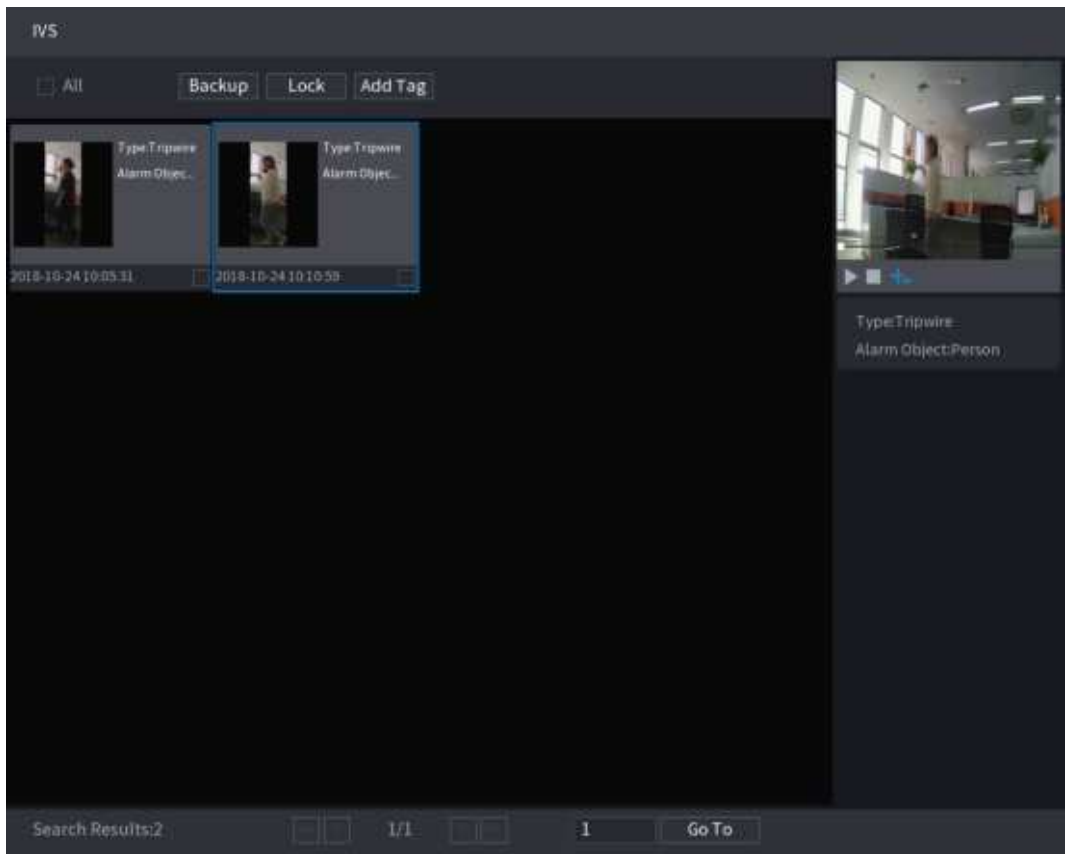
The results that satisfy the searching conditions are displayed.

Figure 5-196



Step 4 Click the picture that you want to play back.

Figure 5-197



Step 5 Click  to play back the recorded video.

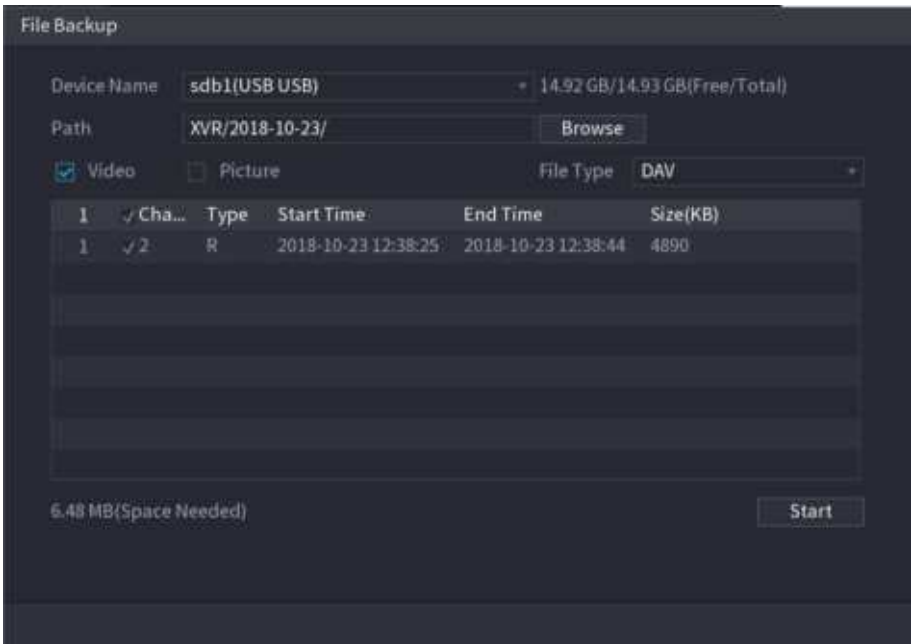


Double-click on the playing interface to switch between full screen playing and thumbnail playing.

You can also do the following operations to the recorded files.

- To back up the recorded files to the external storage device, select files, click **Backup**, select the save path and file type, and then click **Start**.

Figure 5-198



- To lock the files to make it unable to be overwritten, select the files, and then click **Lock**.
- To add a mark to the file, select the files and then click **Add Tag**.

5.11.2.3 Face Detection (For XVR5X-I and XVR7X-I series only)

Some series of devices can analyze the pictures captured by the camera to detect whether the faces are on the pictures. You can search and filter the recorded videos the faces and play back.



If you select AI by device, then among face detection and recognition, IVS function, you can use one of them at the same time for the same channel.

5.11.2.3.1 Configuring Face Detection Parameters

The alarms are generated according to the configured parameters.

Step 1 Select **Main Menu > AI > Parameters > Face Detection**.

The **Face Detection** interface is displayed.

Figure 5-199

Step 2 In the **Channel** list, select a channel that you want to configure face detection function, and then enable it.

Step 3 Configure the parameters.

Table 5-55

Parameter	Description
Rule	Click View Setting to draw areas to filter the target. You can configure two filtering targets (maximum size and minimum size). When the target is smaller than the minimum size or larger than the maximum size, no alarms will be activated. The maximum size should be larger than the minimum size.
Schedule	Define a period during which the detection is active. For details, see "Setting Motion Detection Period" section in "5.10.4.1 Configuring Motion Detection Settings."
Alarm-out Port	Click Setting to display setting interface. - General Alarm: Enable general alarm and select the alarm output port. - Ext. Alarm: Connect the alarm box to the Device and then enable it. - Wireless Siren: Connect the wireless gateway to the Device and then enable it. For details, see "5.12 IoT Function." When an alarm event occurs, the system links the peripheral alarm devices connected to the selected output port.
Post-Alarm	Set a length of time for the Device to delay turning off alarm after the external alarm is cancelled. The value ranges from 0 seconds to 300 seconds. If you enter 0, there will be no delay.
Show Message	Select the Show Message check box to enable a pop-up alarm message in your local host PC.
Report Alarm	Select the Report Alarm check box to enable the system to upload the alarm signal to the network (including alarm center) when an alarm event occurs.  - Not all models support this function. - The corresponding parameters in the alarm center should be configured. For details, see "5.15.1.12 Configuring Alarm Center Settings."
Send Email	Select the Send Email check box to enable the system to send an email notification when an alarm event occurs.  To use this function, make sure the email function is enabled in Main Menu > NETWORK > Email .
Record Channel	Select the channel(s) that you want to record. The selected channel(s) starts recording after an alarm event occurs.  The recording for intelligence event and auto recording function must be enabled. For details, see "5.1.4.9 Configuring Recorded Video Storage Schedule" and "5.9.1 Enabling Record Control."

Parameter	Description
PTZ Linkage	Click Setting to display the PTZ interface. Enable PTZ linkage actions, such as selecting the preset that you want to be called when an alarm event occurs.  To use this function, the PTZ operations must be configured. For details, see "5.4 Controlling PTZ Cameras."
Post Record	Set a length of time for the Device to delay turning off recording after the alarm is cancelled. The value ranges from 10 seconds to 300 seconds.
Tour	Select the Tour check box to enable a tour of the selected channels.  • To use this function, the tour setting must be configured." • After the tour is ended, the live view screen returns to the view layout before tour started.
Picture Storage	Select the Picture Storage check box to take a snapshot of the selected channel.  To use this function, make sure the snapshot function is enabled for Intel in Main Menu > STORAGE > Schedule > Snapshot.
Video Matrix	Select the check box to enable the function. When an alarm event occurs, the video output port outputs the settings configured in Main Menu > DISPLAY > TOUR > Extra Screen.  • Not all models support this function. • The extra screen must be enabled to support this function.
Buzzer	Select the check box to activate a buzzer noise at the Device.
Log	Select the check box to enable the Device to record a local alarm log.
Alarm Tone	Select to enable audio broadcast in response to a face detection event.
White Light	Select the check box to enable the white light alarm of the camera.
Siren	Select the check box to enable the sound alarm of the camera.

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

5.11.2.3.2 Searching for and Playing Detected Faces

You can search the detected faces and play back.

Step 1 Select **Main Menu > AI > AI Search > Face Detection**.

The **Face Detection** interface is displayed.

Figure 5-200

Channel: 1

Start Time: 2020-03-02 00:00:00

End Time: 2020-03-03 00:00:00

Gender: All

Age: All

Glasses: All

Beard: All

Mouth Mask: All

Expression: All

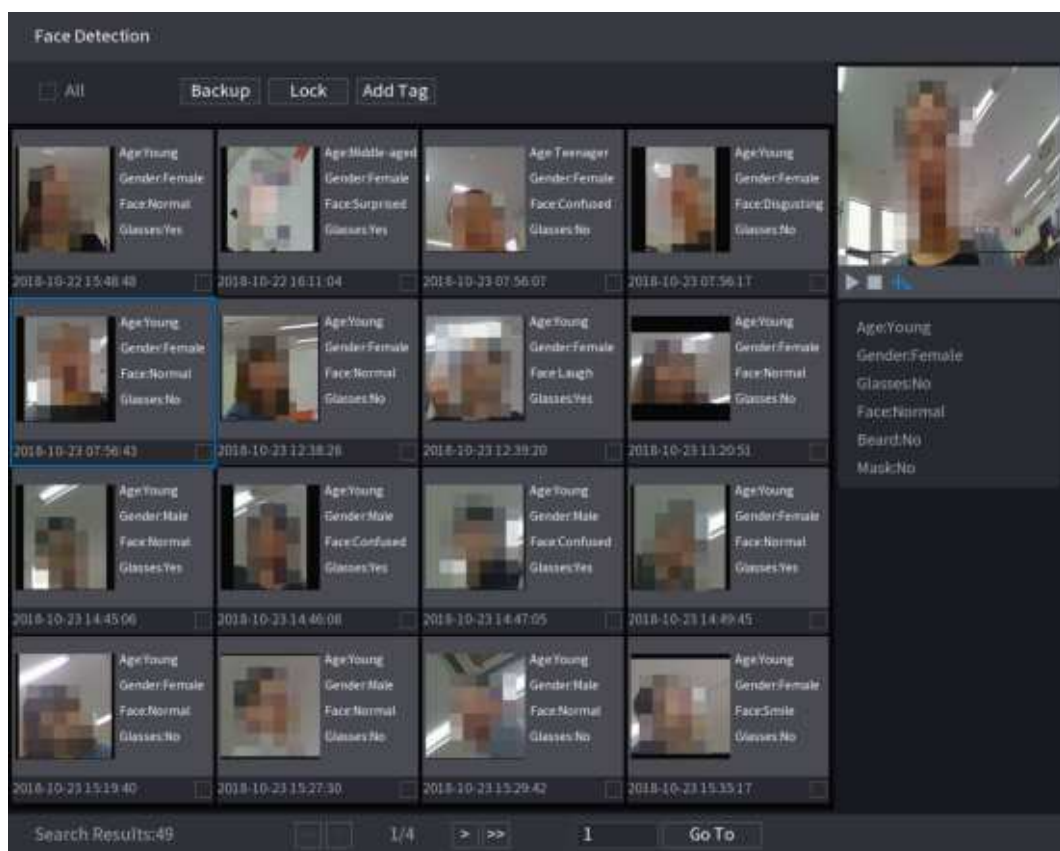
Smart Search

Step 2 Select the channel, enter the start time and end time, and set for the gender, age, glasses, beard, and mask.

Step 3 Click **Smart Search**.

The results are displayed.

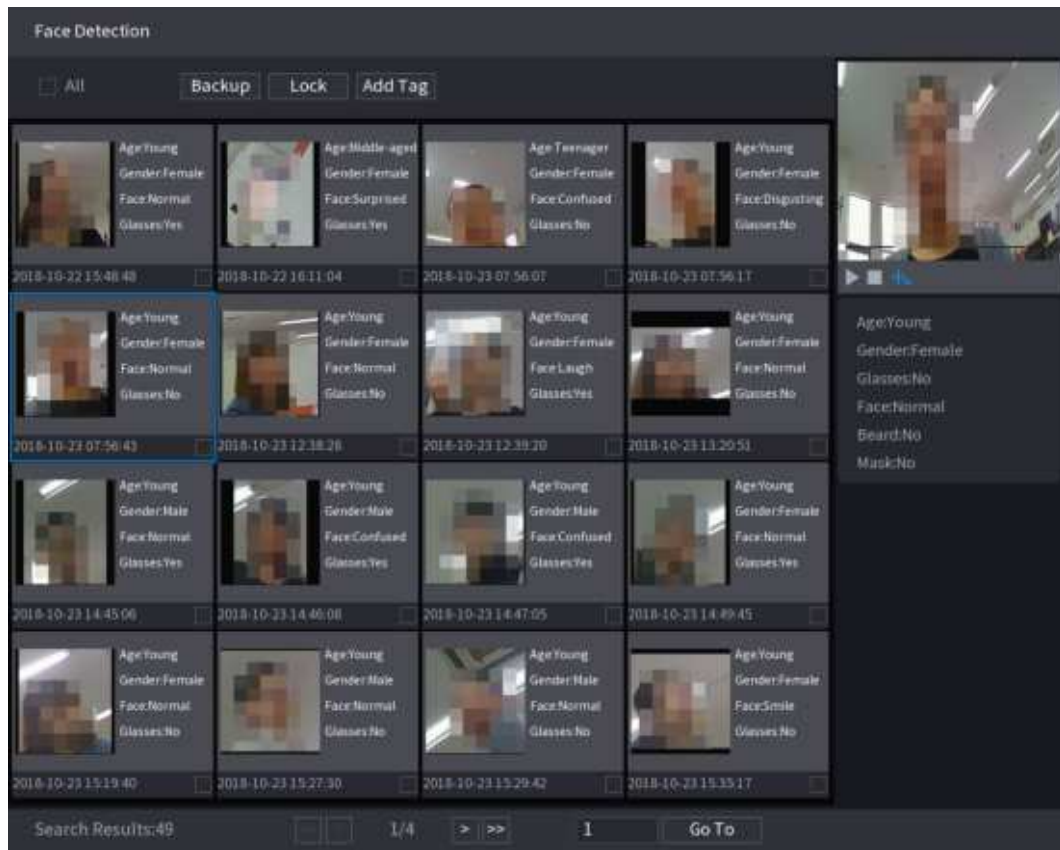
Figure 5-201



Step 4 Select the face that you want to play back.

The picture with registered information is displayed.

Figure 5-202



Step 5 And then click  to start playing back the recorded detected face snapshots.

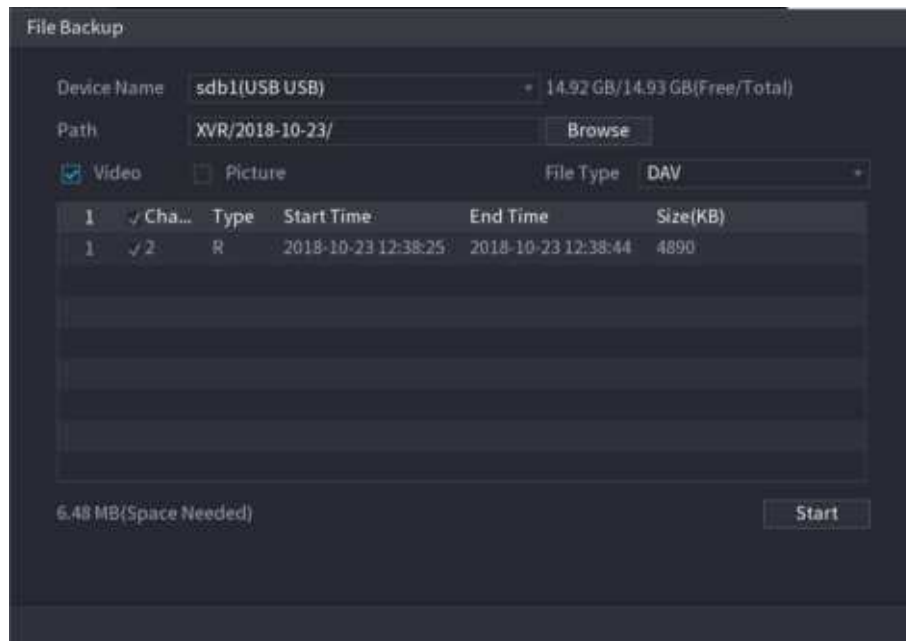


Double-click on the playing interface to switch between full screen playing and thumbnail playing.

You can also do the following operations to the recorded files.

- To export the database file (.csv) to the external storage device, select files, click **Export**, and then select the save path.
- To back up the recorded files to the external storage device, select files, click **Backup**, select the save path and file type, and then click **Start**.

Figure 5-203



- To lock the files to make it unable to be overwritten, select the files, and then click **Lock**.
- To add a mark to the file, select the files and then click **Add Tag**.

5.11.2.4 Face Recognition (For XVR7X-I series only)

Face recognition applies to AI preview mode and smart search.

- AI preview mode: Supports comparing the detected faces with the face library, and display the comparison results.
- Smart search: Supports faces searching by faces attributes or portraits.



- If you select AI by device, then among face detection and recognition, IVS function, you can use one of them at the same time for the same channel.
- Before enabling face recognition function for a channel, the face detection must be enabled first for this channel.

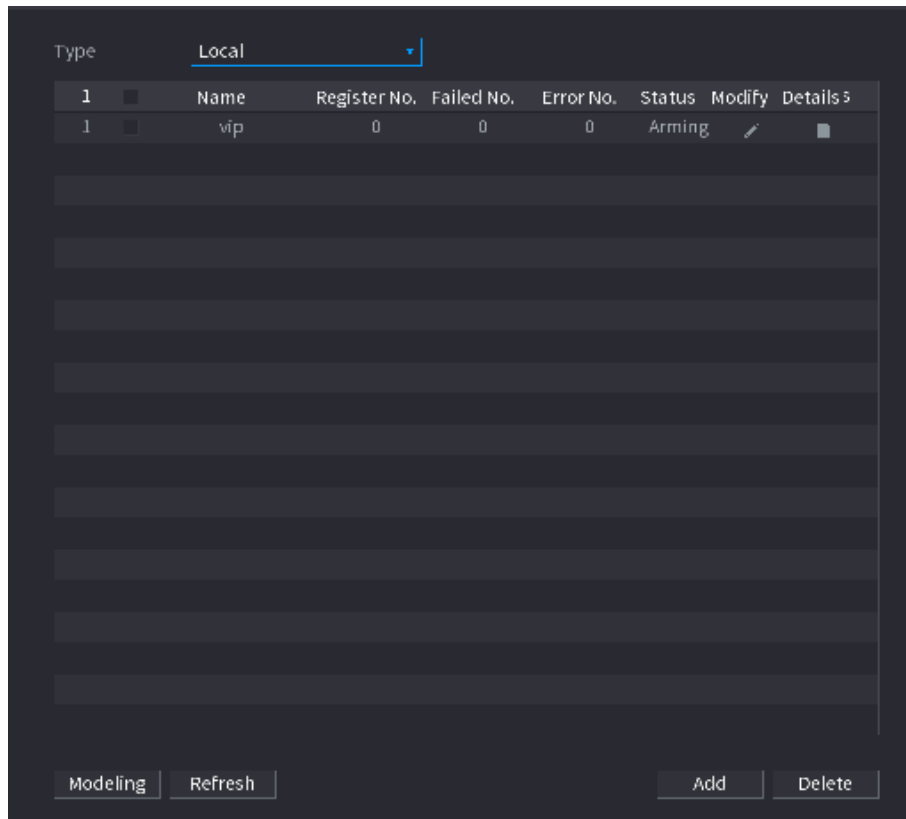
5.11.2.4.1 Face Library Management

You should create a face library for comparing the detected faces and the faces in the library. The Device supports creating maximum 20 libraries and registering 100,000 faces.

Creating a Face Library

- Step 1 Select **Main Menu > AI > Database > Face Database Config**.
The **Face Database Config** interface is displayed.

Figure 5-204



Step 2 At **Type**, you can select **Local** or **Remote**.

- **Local**: Viewing the existing face databases or adding new one on the DVR.
- **Remote**: If you have face recognition camera, you can select this to view the existing face databases or adding new one on the camera.

Click **Add**.

The **Add** interface is displayed.

Figure 5-205

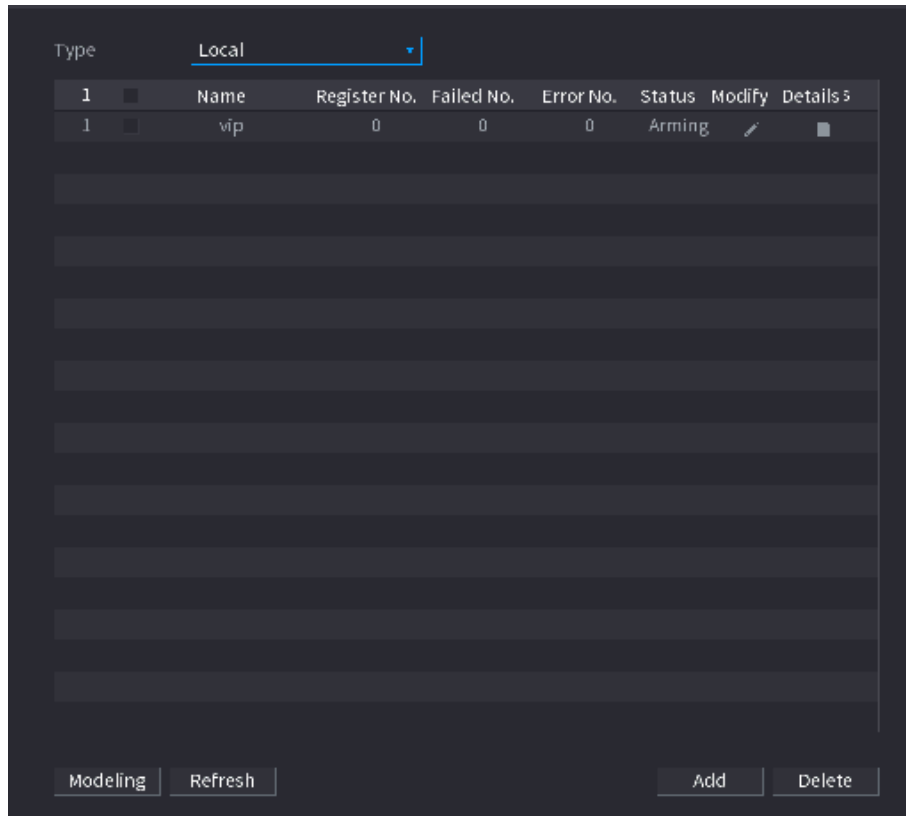
Step 3 Enter the face library name, and then click **Save**.

The created library is displayed.

- Click  to modify library name.

- Click  to view the library details and add new faces to the library. For details, see "Adding Face Pictures."
- Select the library, and then click **Modeling**. The system will extract the attributes of face pictures in the library for the future comparison.
- Select the library, and then click **Delete** to delete the library.

Figure 5-206



Adding Face Pictures

You can add face pictures to the existing libraries one by one or by batch, or add from the detected faces.



To add face pictures one by one or by batch, you need to get the pictures from the USB storage device. The picture size should be smaller than 256K with resolution between 200×200–6000×5000.

Adding One Face Picture

Step 1 Select **Main Menu > AI > Database > Face Database Config**.

The **Face Database Config** interface is displayed.

Step 2 Click  of the library that you want to configure.

The **Details** interface is displayed.

Figure 5-207

Details

Name Gender: All ID No. Model... All

☐ All

1/1 1

Step 3 Click **Register ID**.

The **Register ID** interface is displayed.

Figure 5-208

Register ID

Name

Gender ☒ Male ☐ Female

Birthday Year Month Date

Address

ID Type

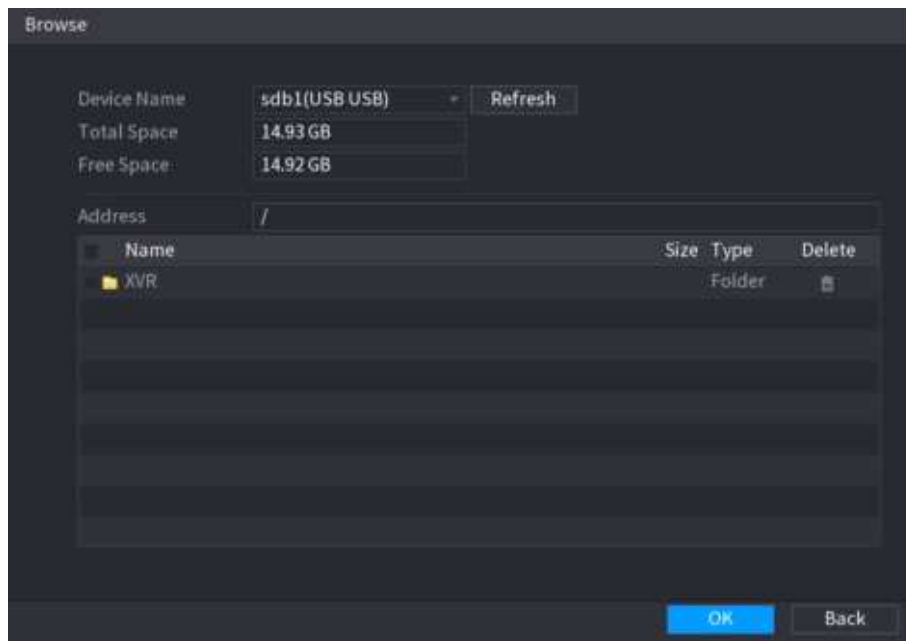
ID No.

Country

Step 4 Click  to add a face picture.

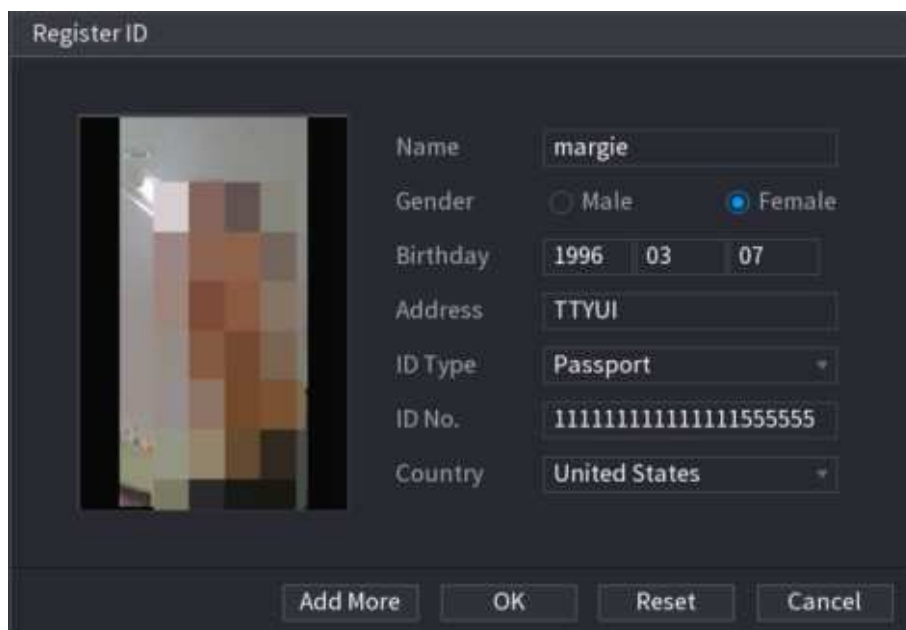
The **Browse** interface is displayed.

Figure 5-209



Step 5 Select a face picture and enter the registration information.

Figure 5-210



Step 6 Click **OK**.

The system prompts the registration is successful.

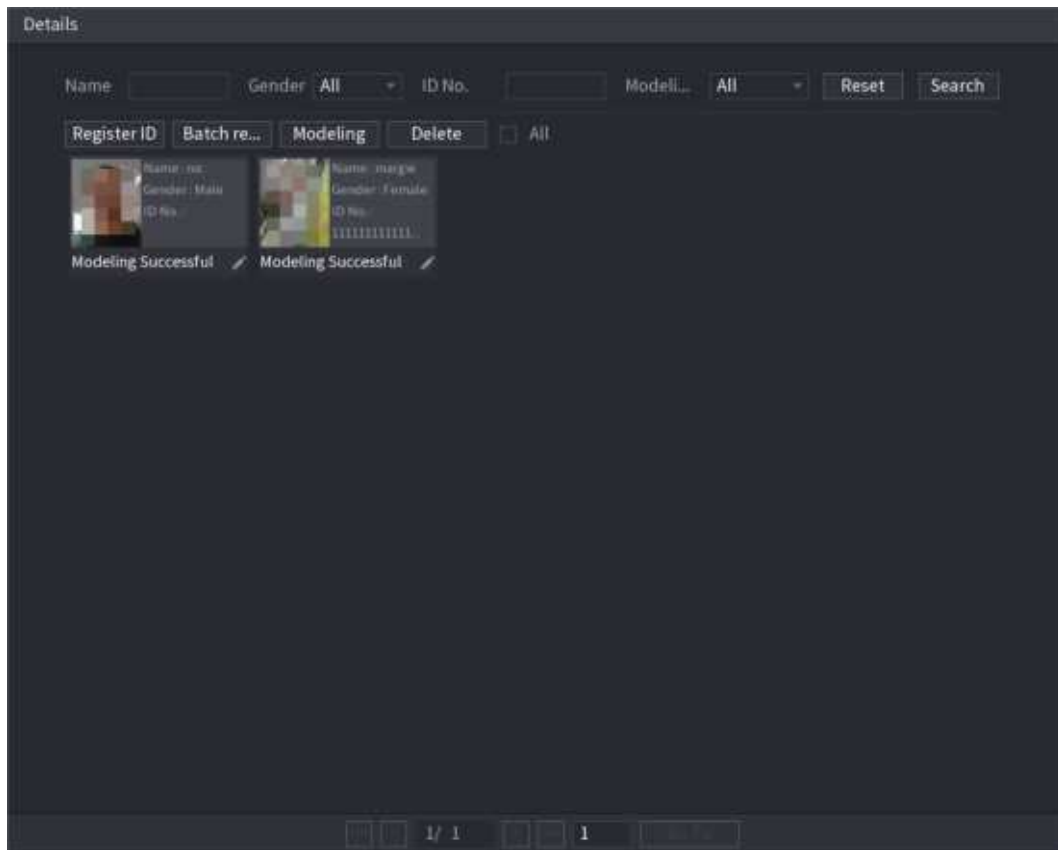
Step 7 On the **Details** interface, click **Search**.

The system prompts modeling is successful.



If the system prompts the message indicating modeling is in process, wait a while and then click **Search** again. If modeling is failed, the registered face picture cannot be used for face recognition.

Figure 5-211



Adding Face Pictures in Batches

Step 1 Give a name to the face picture by referring to Table 5-56.

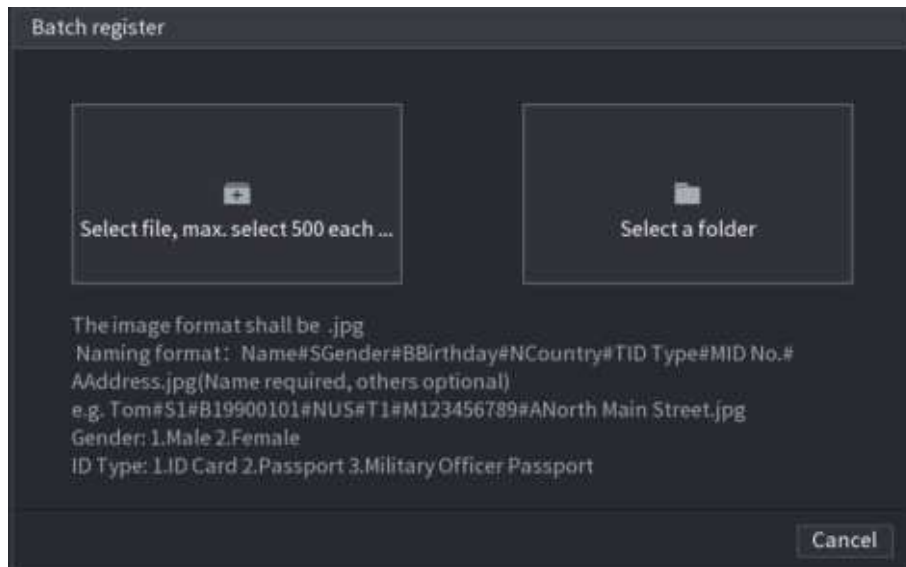
Table 5-56

Naming format	Description
Name	Enter the name.
Gender	Enter 1 or 2. 1 represents male, and 2 represents female.
Birthday	Enter numbers in the format of yyyy-mm-dd.
Country	Enter the abbreviation of country. For example, CN for China.
ID Type	1 represents ID card; 2 represents passport; 3 represents military officer password.
ID No.	Enter the ID number.
Address	Enter the address.

Step 2 On the **Details** interface, click **Batch register**.

The **Batch register** interface is displayed.

Figure 5-212



Step 3 Click **Select file, max select 500 each time** or **Select a folder** to import face pictures.

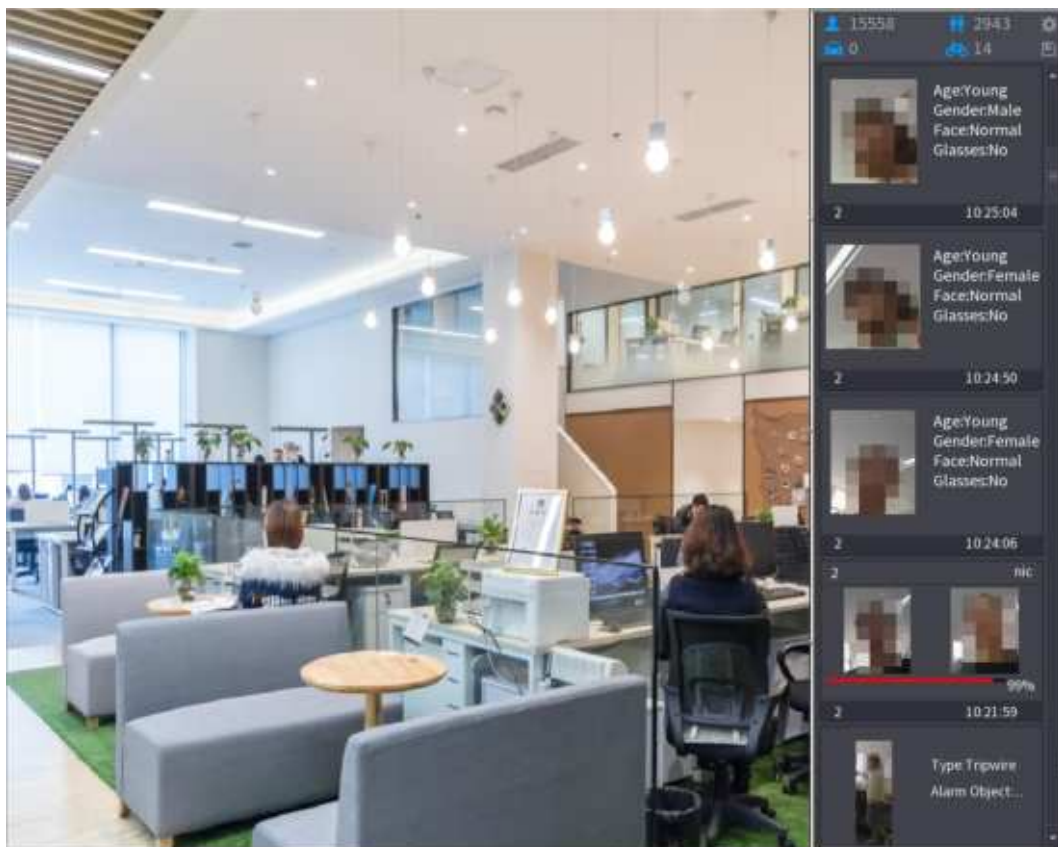
Step 4 Click **OK** to complete batch registration.

Adding the Detected Faces

Step 1 Right-click on the live view screen, and then select **Live Mode > AI Mode**.

The AI Mode live view screen is displayed.

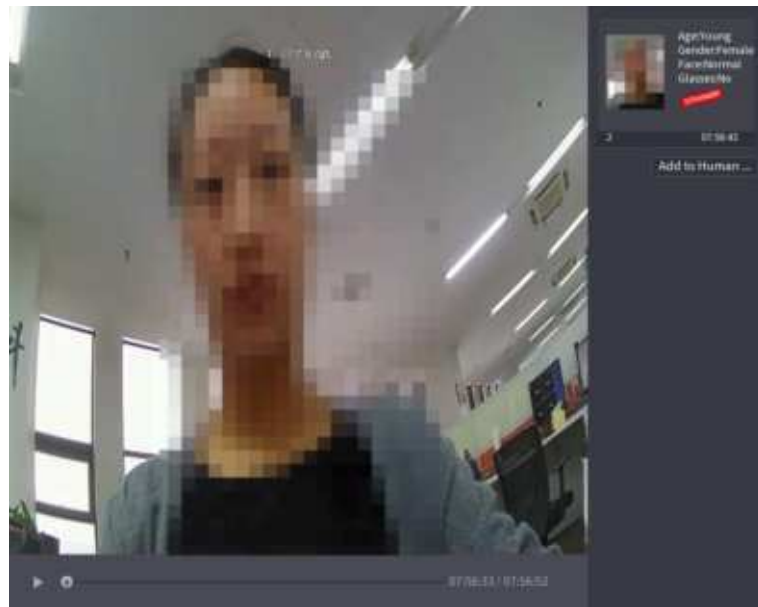
Figure 5-213



Step 2 Double-click the detected face snapshot that you want to add.

The snapshot playing back interface is displayed.

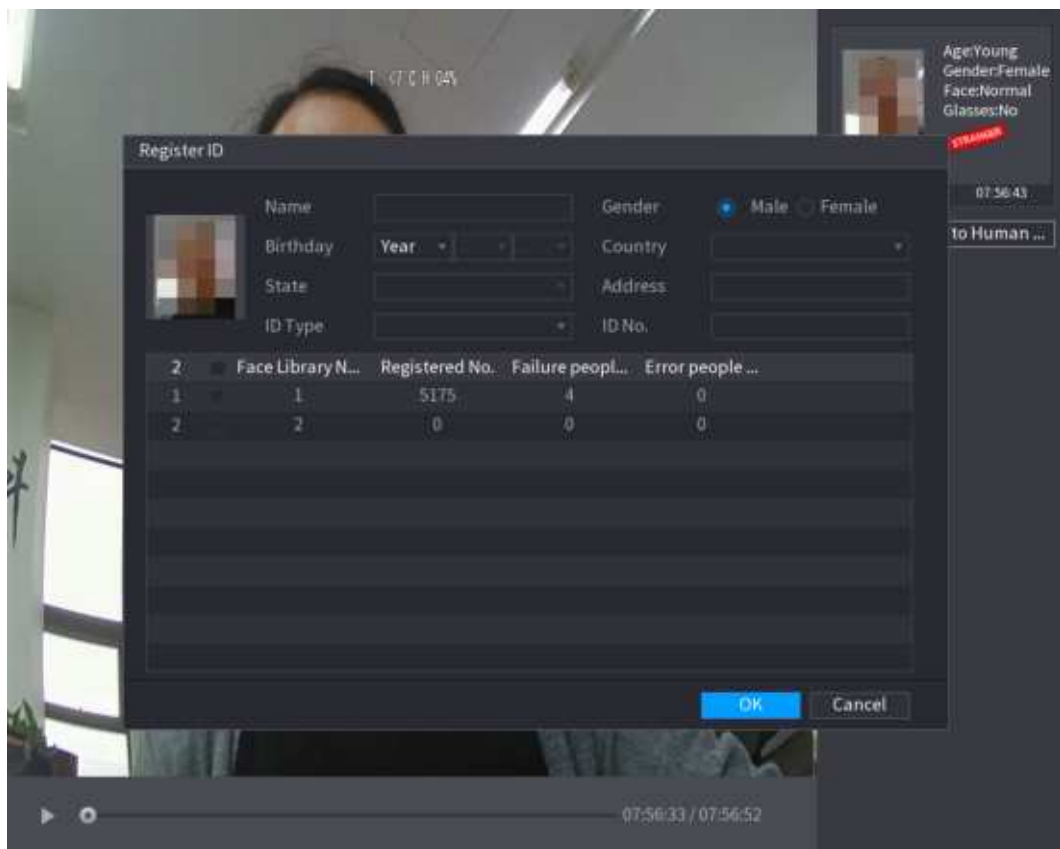
Figure 5-214



Step 3 Click **Add to Human Face Database**.

The **Register ID** interface is displayed.

Figure 5-215



Step 4 Select the face library and enter the ID information.

Step 5 Click **OK** to complete registration.

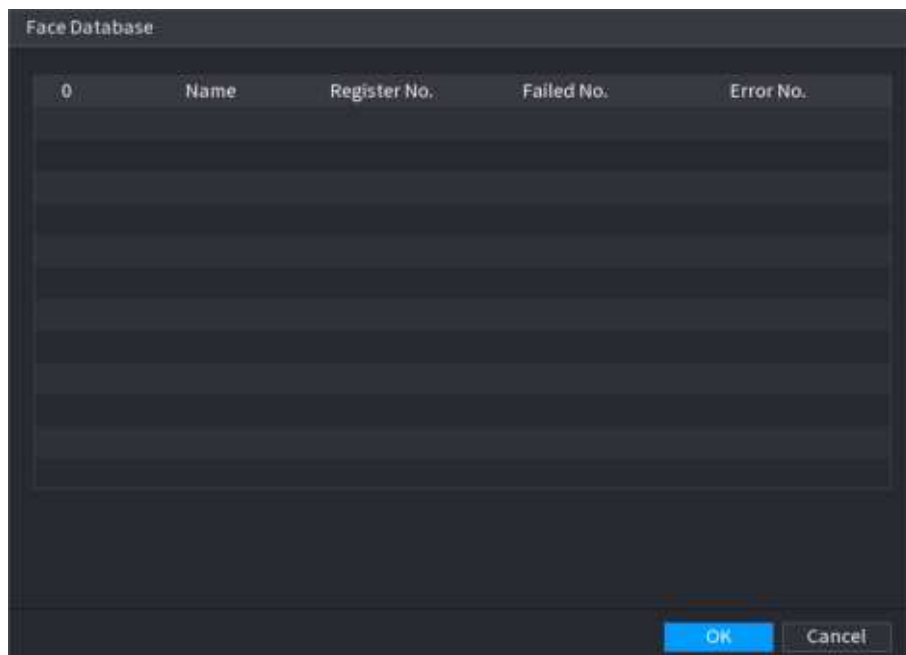
5.11.2.4.2 Face Recognition Configuration

You can compare the detected faces with the faces in the library to judge if the detected face belongs to the library. The comparison result will be displayed on the AI mode live view screen and smart search interface, and link the alarms.

Step 1 Select **Main Menu > AI > Parameters > Face Recognition**.

The **Face Recognition** interface is displayed.

Figure 5-216



Step 2 In the **Channel** list, select a channel that you want to configure face recognition function, and then enable it.

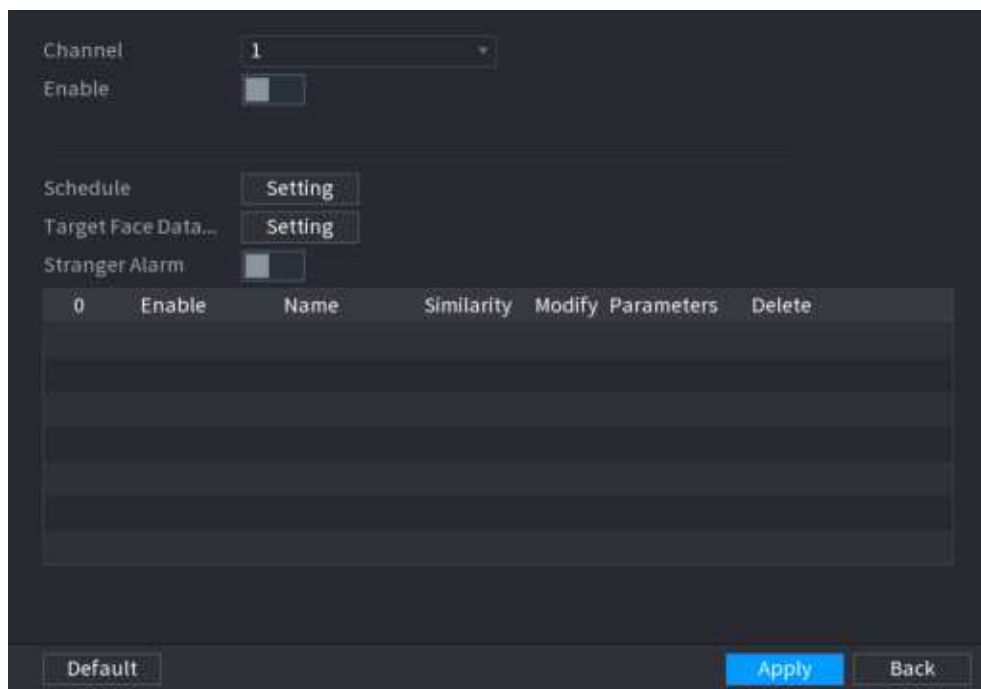
Step 3 Set the **Period**. For details, see "5.10.4.1 Configuring Motion Detection Settings."

Step 4 Set the **Target Face Database**.

1) Click **Setting**.

The **Face Library** interface is displayed.

Figure 5-217

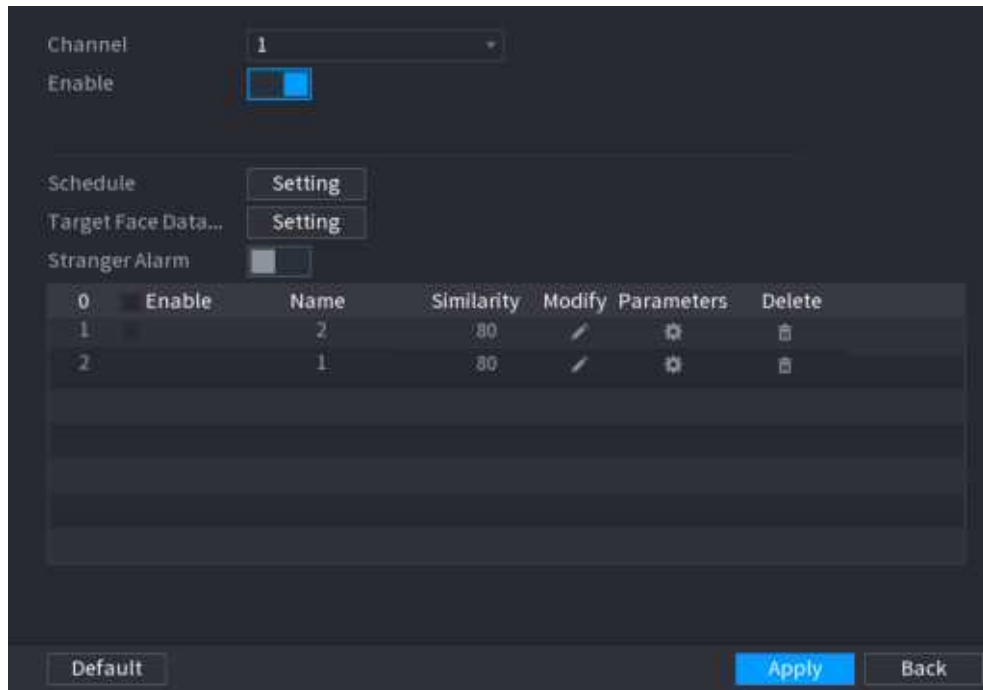


2) Select one or multiple face libraries.

3) Click **OK**.

The selected face library is listed.

Figure 5-218



Step 5 Configure the added face library.

- Click to modify the similarity. The lower the number is, the easier the alarm linkage will trigger.
- Click to delete the face library.
- Click to set the alarm linkage. For details, see Table 5-46.

After setting is completed, click **OK**.

Step 6 (Optional) Enable the **Stranger Mode**.

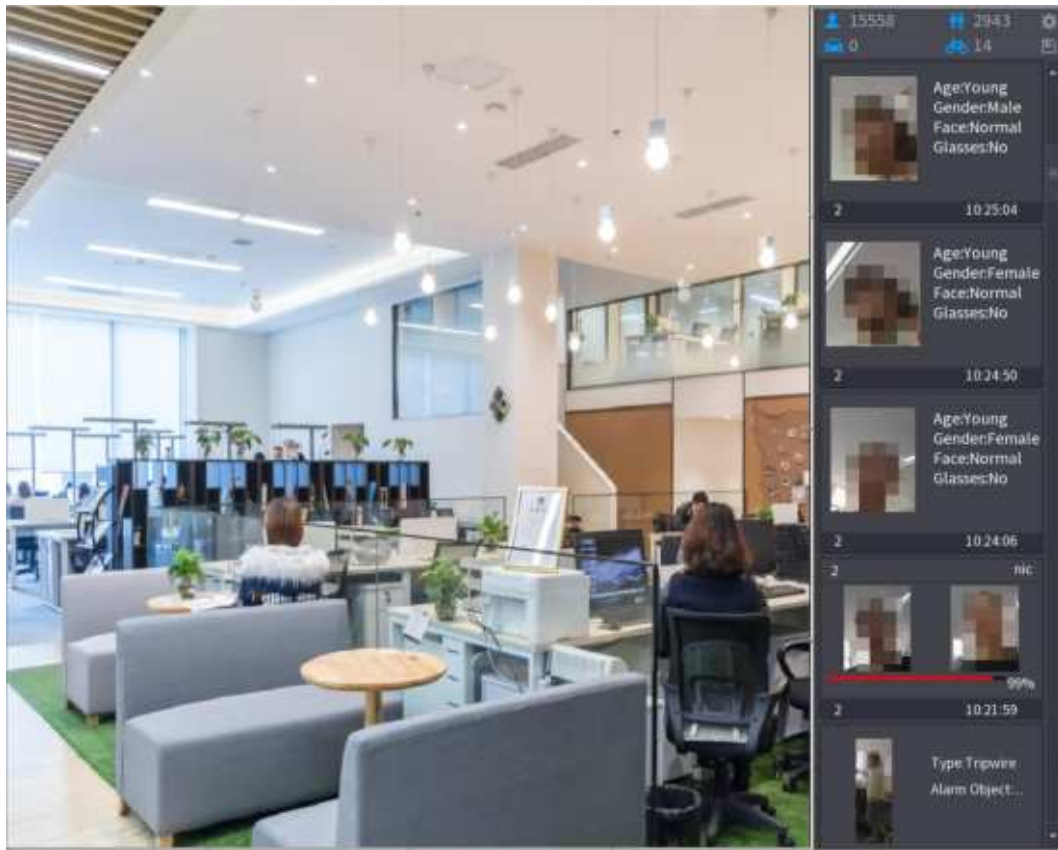
- 1) Enable the Stranger mode (☒). When the detected faces do not belong to the face library, the system remarks the face as "Stranger."
- 2) Click **Setting** to set the alarm linkage. For details, see Table 5-46.
- 3) After setting is completed, click **OK**.

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

After the face recognition function is enabled, right-click on the live view screen, and then select **Preview Mode > AI Mode**. The AI mode live view screen is displayed.

- If the detected face belongs to the enabled face library, the similarity result is displayed.
- If the detected face does not belong to the enabled face library, the face will be remarked as "Stranger."

Figure 5-219



5.11.2.4.3 Smart Search for Face Recognition

You can compare the detected faces with the face library and play back.

- Search by attributes: Search the face library by the face attributes.
- Search by picture: Search the face library by uploading face pictures.

Searching by Attributes

Step 1 Select **Main Menu > AI > AI Search > Face Recognition > Search by Attributes**.
The **Search by Attributes** interface is displayed.

Figure 5-220

Search by Attribute Search by Picture

Channel 1

Start Time 2020 -03 -02 00 :00 :00

End Time 2020 -03 -03 00 :00 :00

Gender All

Age All

Glasses All

Beard All

Mouth Mask All

Expression All

Similarity 80 %

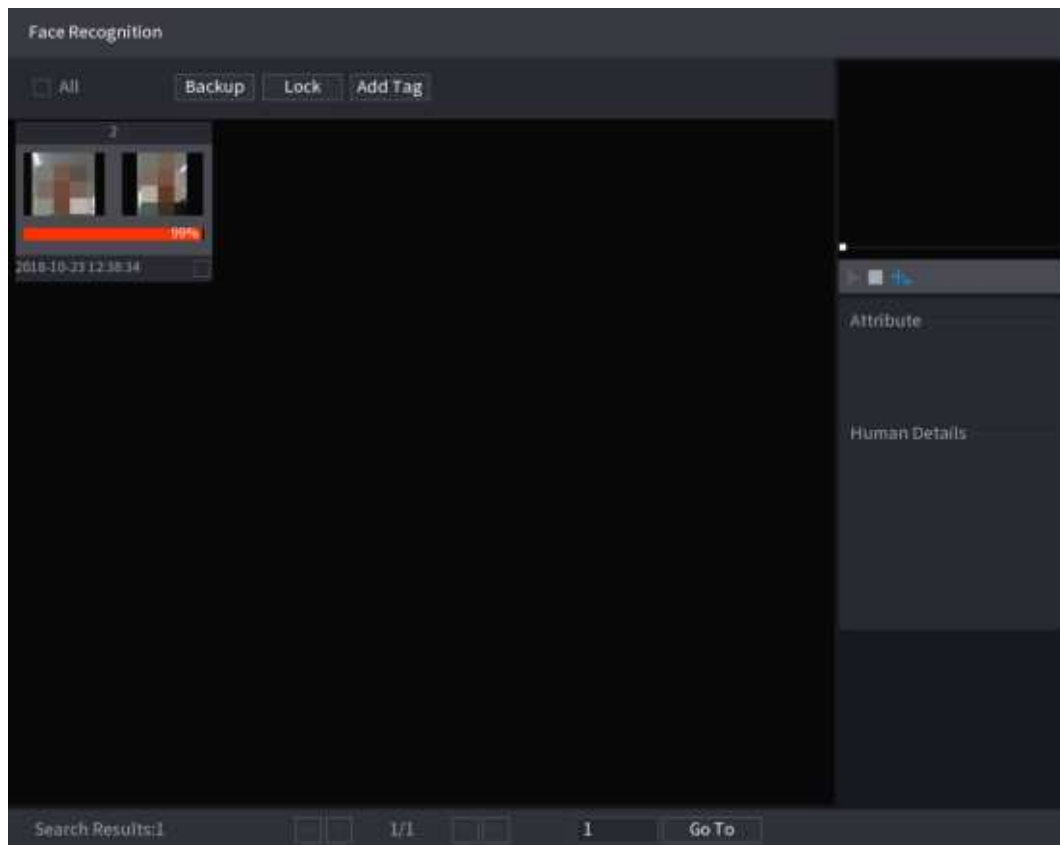
Smart Search

Step 2 Select the channel and set the parameters such as start time, end time, gender, age, glasses, beard, mask, and similarity according to your requirement.

Step 3 Click **Smart Search**.

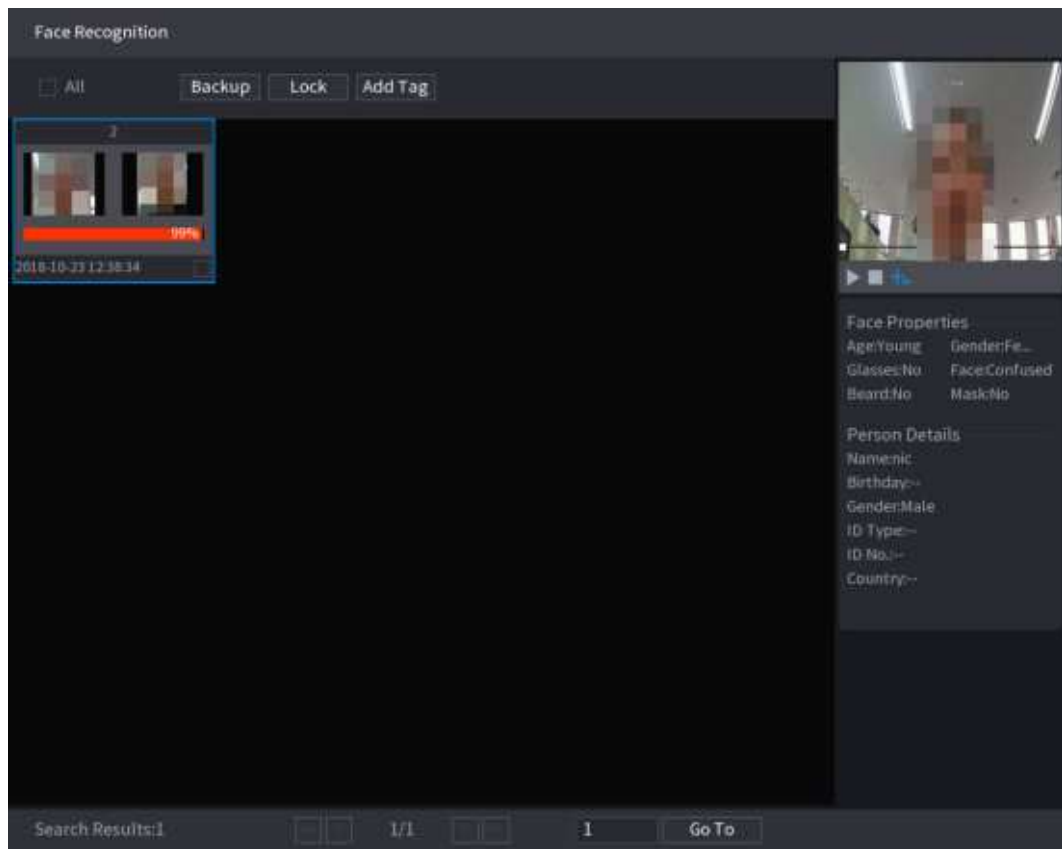
The search result is displayed.

Figure 5-221



- Step 4** Click the picture that you want to play back.
The picture with registered information is displayed.

Figure 5-222



- Step 5** Click  to play back the recorded video.

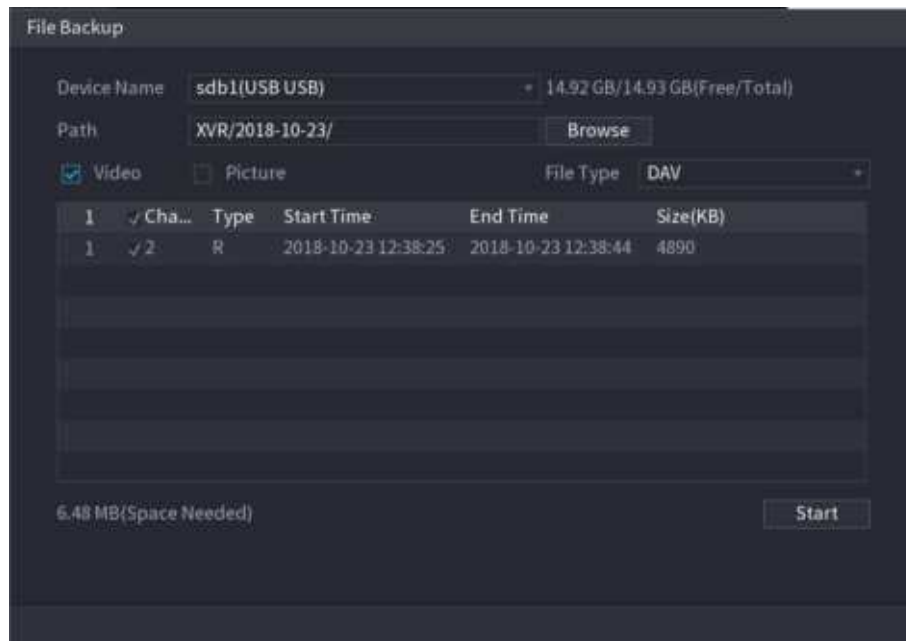


Double-click on the playing interface to switch between full screen playing and thumbnail playing.

You can also do the following operations to the recorded files.

- To export the database file (.csv) to the external storage device, select files, click **Export**, and then select the save path.
- To back up the recorded files to the external storage device, select files, click **Backup**, select the save path and file type, and then click **Start**.

Figure 5-223

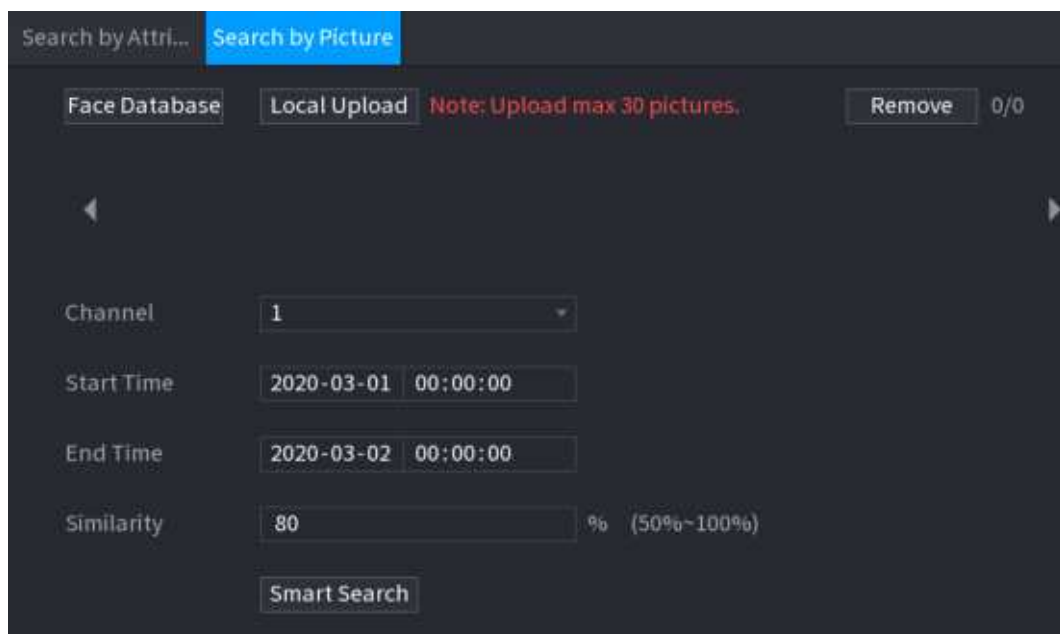


- To lock the files to make it unable to be overwritten, select the files, and then click **Lock**.
- To add a mark to the file, select the files and then click **Add Mark**.

Search by Picture

Step 1 Select **Main Menu > AI > AI Search > Face Recognition > Search by Picture**.
The **Search by Picture** interface is displayed.

Figure 5-224



Step 2 Upload face pictures from **Face Database** or **Local Upload**.



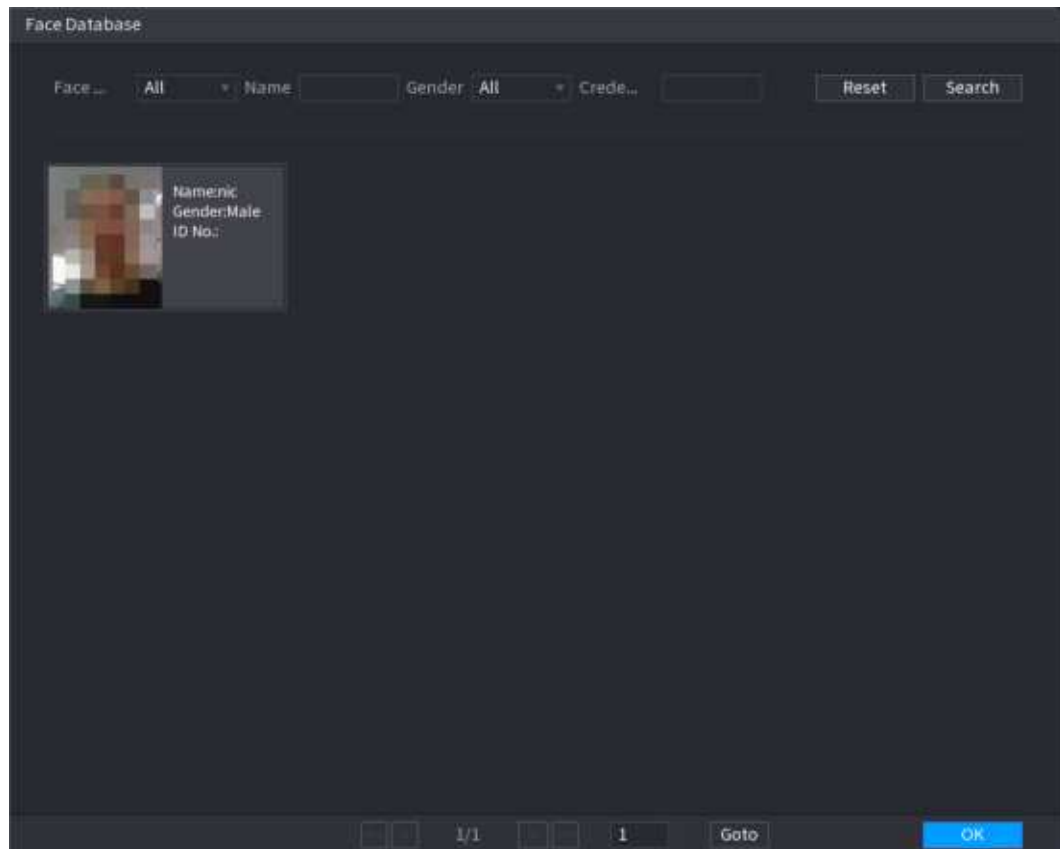
Maximum 30 pictures can be uploaded at one time, and the system support searching 8 pictures at one time.

- Face Database

- 1) Click **Face Database**.

The **Face Database** interface is displayed.

Figure 5-225



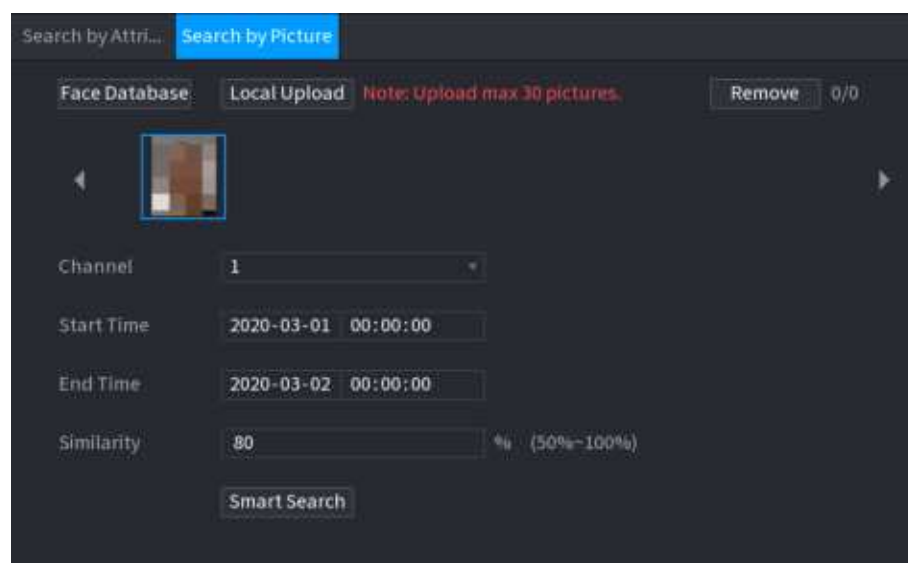
- 2) Set the searching parameters by selecting the face library and gender, and entering name and ID No. according to your actual requirement.
- 3) Click **Search** to display the results that satisfy the requirement.



Click **Reset** to clear the searching parameters.

- 4) Select the picture and then click Save.
The picture is displayed on the Search by Picture interface.

Figure 5-226



- Local Upload

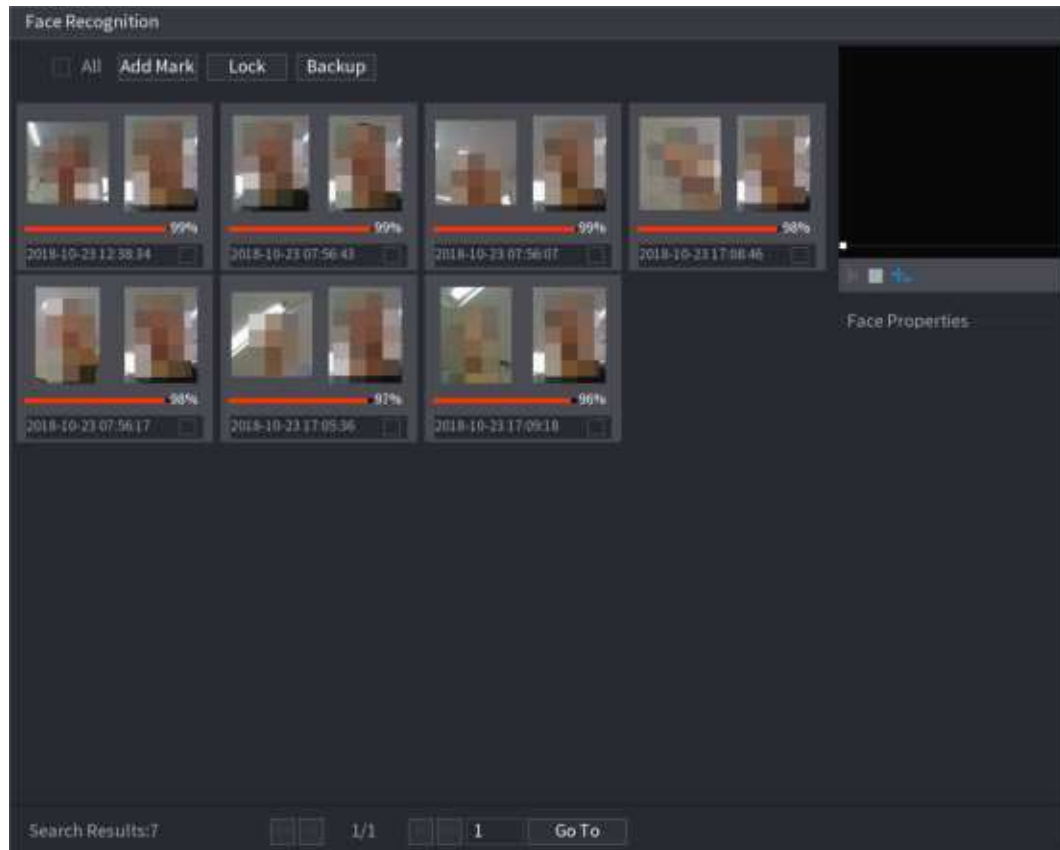
Plug the USB storage device (with face pictures) to the Device, and then click **Local Upload**. Then select the picture from the USB storage device, and then click **OK**. The selected face pictures are uploaded.

Step 3 After the face pictures are uploaded, continue to configure other parameters (channel, start time, end time, and similarity).

Step 4 Click **Smart Search**.

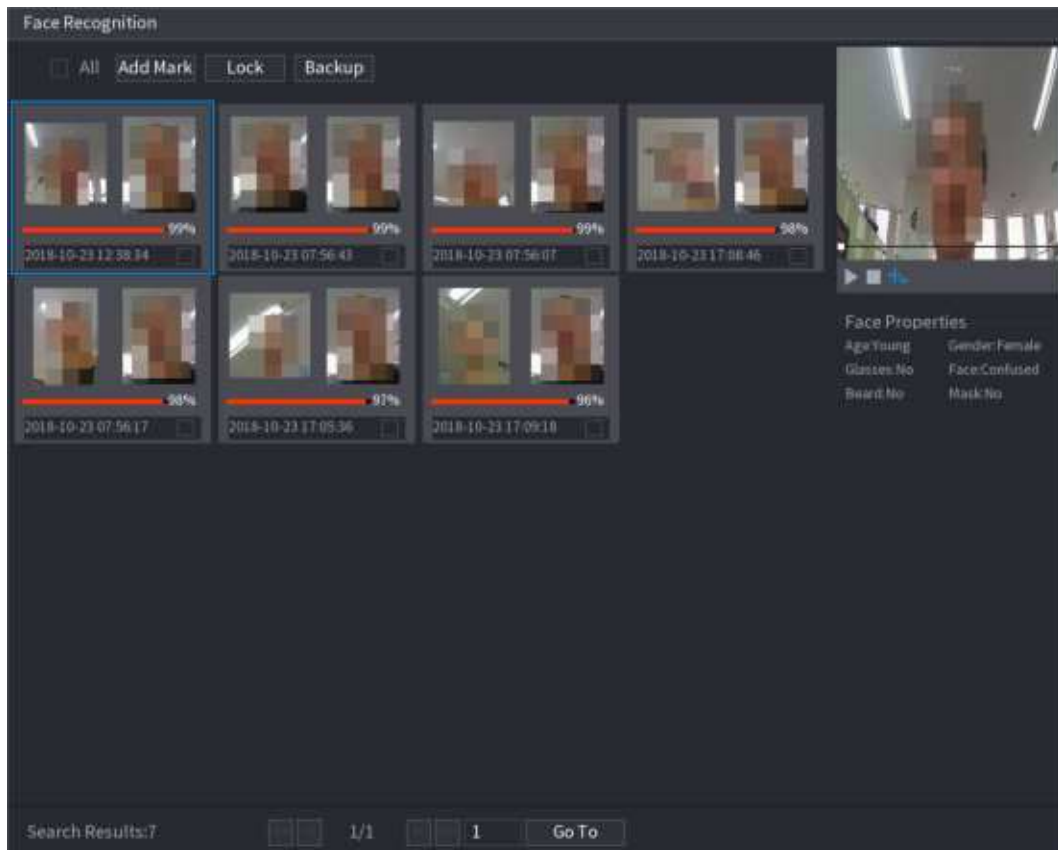
The searching results are displayed.

Figure 5-227



Step 5 Select the face picture that you want to play back.

Figure 5-228



Step 6 Click  to play back the recorded video.

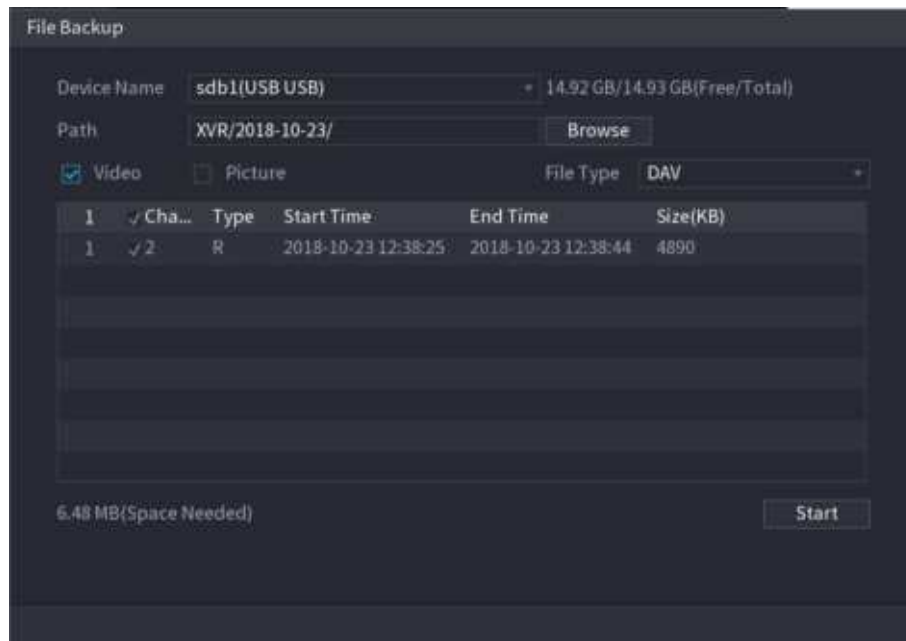


Double-click on the playing interface to switch between full screen playing and thumbnail playing.

You can also do the following operations to the recorded files.

- To add a mark to the file, select the files and then click **Add Mark**.
- To lock the files to make it unable to be overwritten, select the files, and then click **Lock**.
- To back up the recorded files to the external storage device, select files, click **Backup**, select the save path and file type, and then click **Start**.

Figure 5-229



5.12 IoT Function

5.12.1 Configuring Sensor Settings

You can connect external sensors wirelessly through the Device with USB gateway or through connecting to a camera gateway. After connection, you can activate alarm events through external sensors.

5.12.1.1 Connecting Sensor through Device

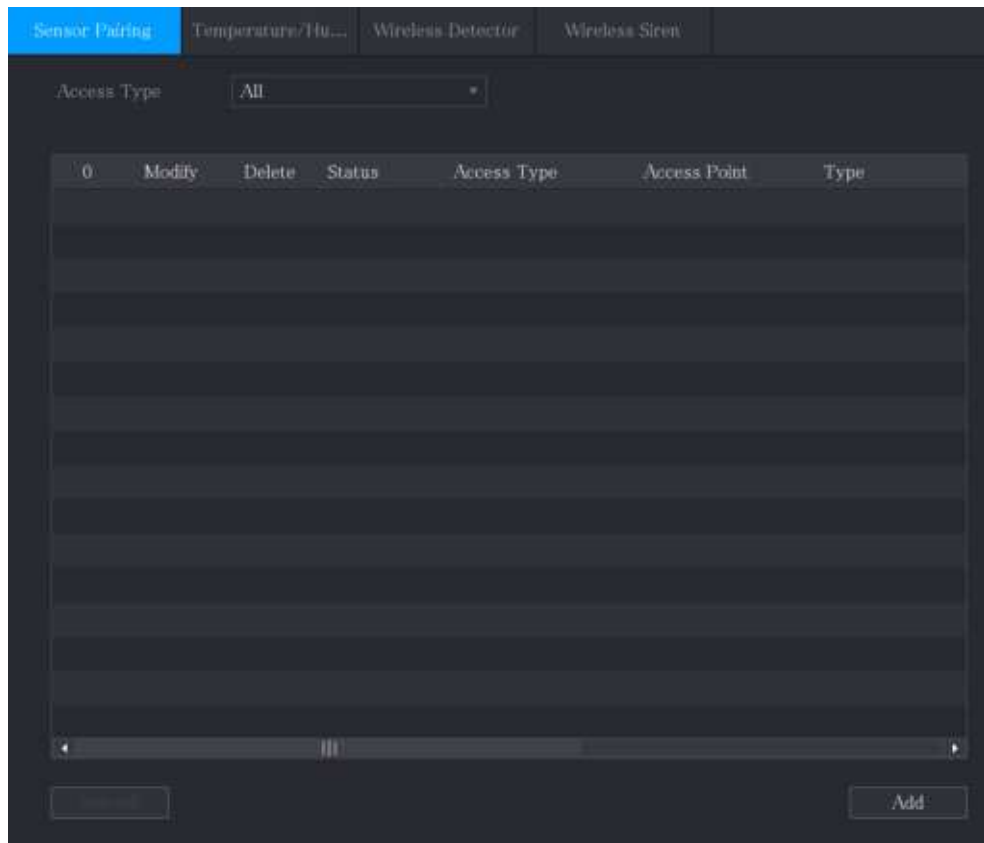


Only the Device with USB gateway supports this function.

Step 1 Select **Main Menu > IoT > Management > Sensor Pairing**.

The **Sensor Pairing** interface is displayed.

Figure 5-230



Step 2 In the **Access Type** list, select **USB Gateway**.

Step 3 Click **Add**.

The **Add** interface is displayed.

Figure 5-231

The screenshot shows the 'Add' configuration page. It has a title bar 'Add'. Below it, there are several form fields: 'Access Type' (dropdown menu set to 'USB Gateway'), 'Add Mode' (dropdown menu set to 'Pair' with a 'Pair' button next to it), 'Access Point' (dropdown menu set to 'USB Gateway-1'), 'SN' (text input field), 'Name' (text input field), 'Type' (text input field), 'Category' (text input field), and 'Status' (text input field). At the bottom right, there is a 'Back' button.

Step 4 Click **Pair**.

The Device starts pairing with the sensor.

Add

Access Type

USB Gateway

Add Way

Pair

Pair

Access Point

USB Gateway-1

Serial No.

3J01837AAZ00008

Name

USB-Panic Button-1

Type

Panic Button

Class

Alarm In

Status

Connected

Back

[illegible]

5.12.1.2 Connecting Sensor through Camera with Gateway

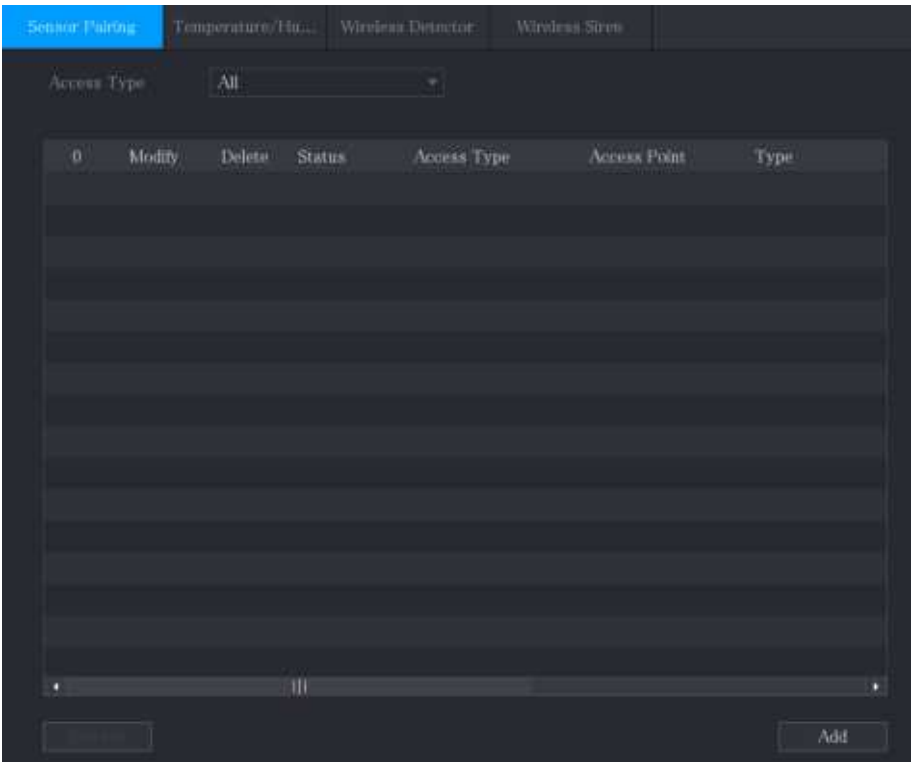


Only the camera with gateway supports this function.

Step 1 Select **Main Menu > IoT > Management > Sensor Pairing**.

The **Sensor Pairing** interface is displayed.

Figure 5-234



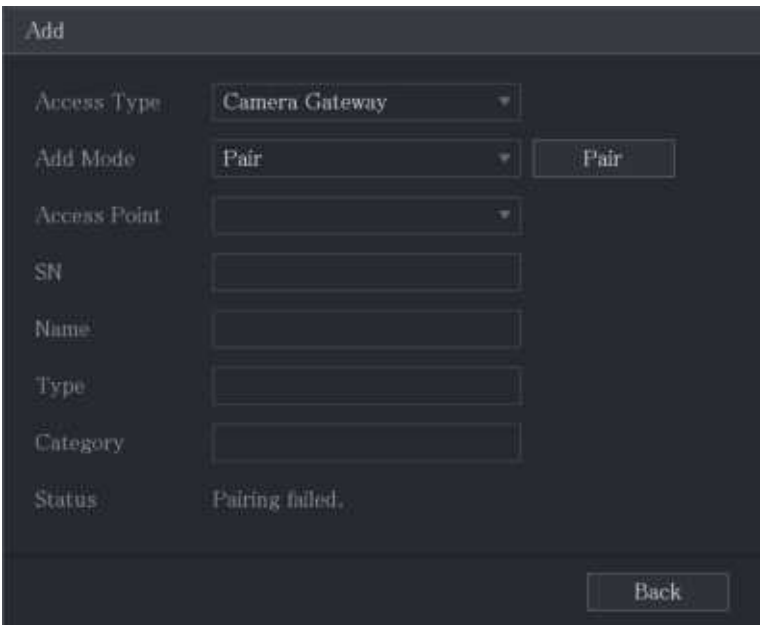
Step 2 In the **Access Type** list, select **Camera Gateway**.

Step 3 In the **Channel** list, select the channel that is connected to the camera.

Step 4 Click **Add**.

The **Add** interface is displayed.

Figure 5-235



Step 5 Click **Pair**.

The Device starts pairing with the sensor.

After pairing is completed, see Figure 5-236.

Figure 5-236

Add

Access Type

Camera Gateway

Add Mode

Pair

Pair

Access Point

Chn6-Air

SN

3J01837AAZ00008

Name

Chn6-Panic Button-1

Type

Panic Button

Category

Alarm In

Status

Pairing failed.

Back

Step 6 Click **Back** to exit the pairing interface.

The added sensor information is displayed.



Click  to modify the sensor name; click  to delete sensor information.

Figure 5-237

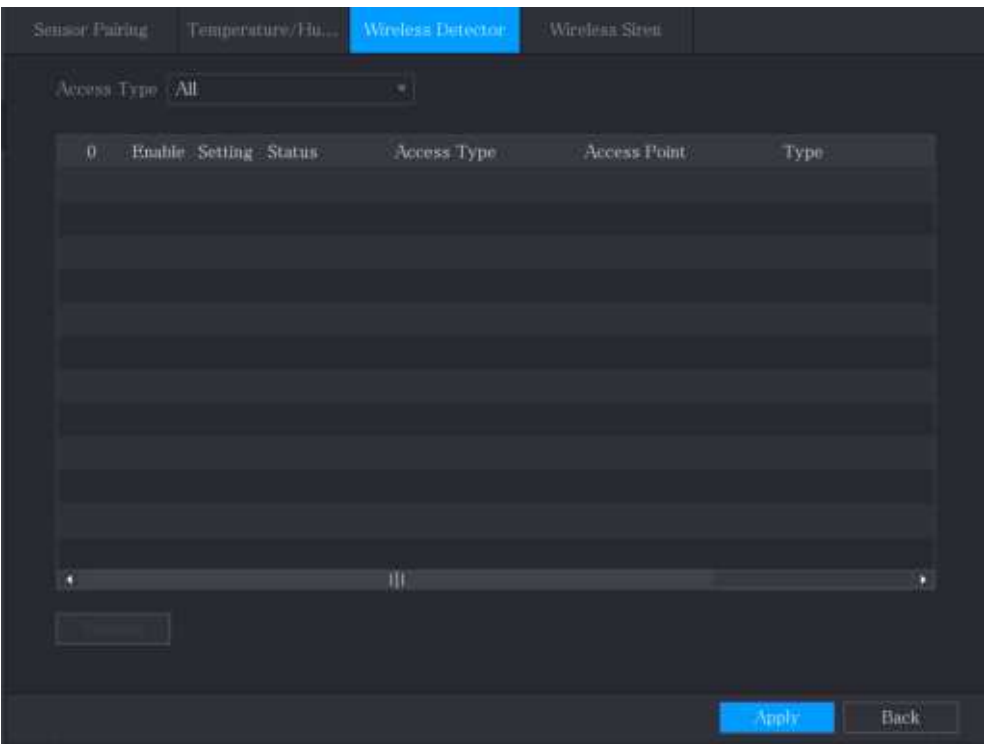
[illegible]

5.12.1.3 Configuring Alarm Linkage

Step 1 Select **Main Menu > IoT > Management > Wireless Detector**.

The **Wireless Detector** interface is displayed.

Figure 5-238



Step 2 In the **Access Type** list, select **USB Gateway**, **Camera Gateway**, or **All**.

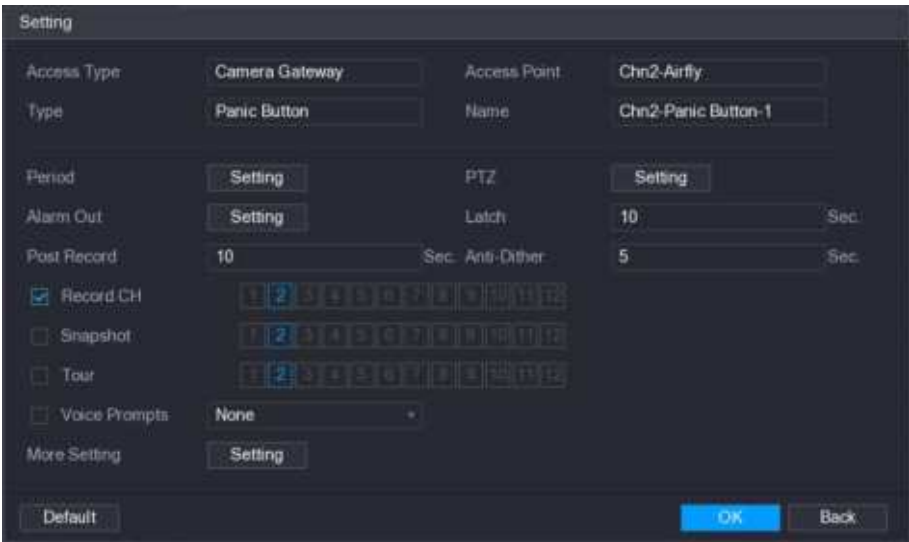


When **Access Type** is **Camera Gateway**, you can select **Channel** to filter the status of present wireless detector.

Step 3 Click .

The **Setting** interface is displayed.

Figure 5-239



Step 4 Configure the settings for alarm linkage.

Table 5-57

Parameter	Description
Name	Enter the customized alarm name.
Schedule	Click Setting to display setting interface. Define a period during which the motion detection is active. For details, see "Setting Motion Detection Period" section in "5.10.4.1 Configuring Motion Detection Settings."
PTZ Linkage	Click Setting to display the PTZ interface. Enable PTZ linkage actions, such as selecting the preset that you want to be called when an alarm event occurs.
Alarm-out Port	Click Setting to display setting interface. - Local Alarm: Enable alarm activation through the alarm devices connected to the selected output port. - Extension Alarm: Enable alarm activation through the connected alarm box. - Wireless Siren: Enable alarm activation through devices connected by USB gateway or camera gateway.
Post-Alarm	Set a length of time for the Device to delay turning off alarm after the external alarm is cancelled. The value ranges from 0 seconds to 300 seconds, and the default value is 10 seconds.
Post Record	Set a length of time for the Device to delay turning off recording after the alarm is cancelled. The value ranges from 10 seconds to 300 seconds, and the default value is 10 seconds.
Anti-Dither	Configure the time period from end of event detection to the stop of alarm.
Record Channel	Select the channel(s) that you want to record. The selected channel(s) starts recording after an alarm event occurs.  The recording for alarm and auto recording must be enabled. For details, see "5.1.4.9 Configuring Recorded Video Storage Schedule" and "5.9.1 Enabling Record Control."
Snapshot	Select the Snapshot check box to take a snapshot of the selected channel.  To use this function, select Main Menu > CAMERA > Encode > Snapshot , in the Type list, select Event .
Tour	Select the Tour check box to enable a tour of the selected channels.
Alarm Tone	Select to enable audio broadcast/voice prompts in response to a local alarm event.

Parameter	Description
More Setting	• Show Message: Select the Show Message check box to enable a pop-up message in your local host PC. • Buzzer: Select the check box to activate a buzzer noise at the Device. • Video Matrix: Select the check box to enable the function. When an alarm event occurs, the video output port outputs the settings configured in "Main Menu > DISPLAY > Tour."  Not all models support this function. • Send Email: Enable the system to send an email notification when an alarm event occurs.  To use this function, make sure the email function is enabled in Main Menu > NETWORK > Email. • Log: Select the check box to enable the Device to record a local alarm log. • Extra screen: Select the check box to enable the function. When an alarm event occurs, the extra screen outputs the settings configured in Main Menu > DISPLAY > Tour > Sub Screen.  • Not all models support this function. • To use this function, extra screen shall be enabled.

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

Step 6 On the **Wireless Detector** interface, click **Apply** to complete the settings.

5.12.2 Configuring Temperature and Humidity Camera

You can view, search and export the temperature and humidity data of camera with such sensors and configure the alarm event settings.

To use this function, please make sure there is at least one camera with temperature and humidity sensor has been connected to the Device.

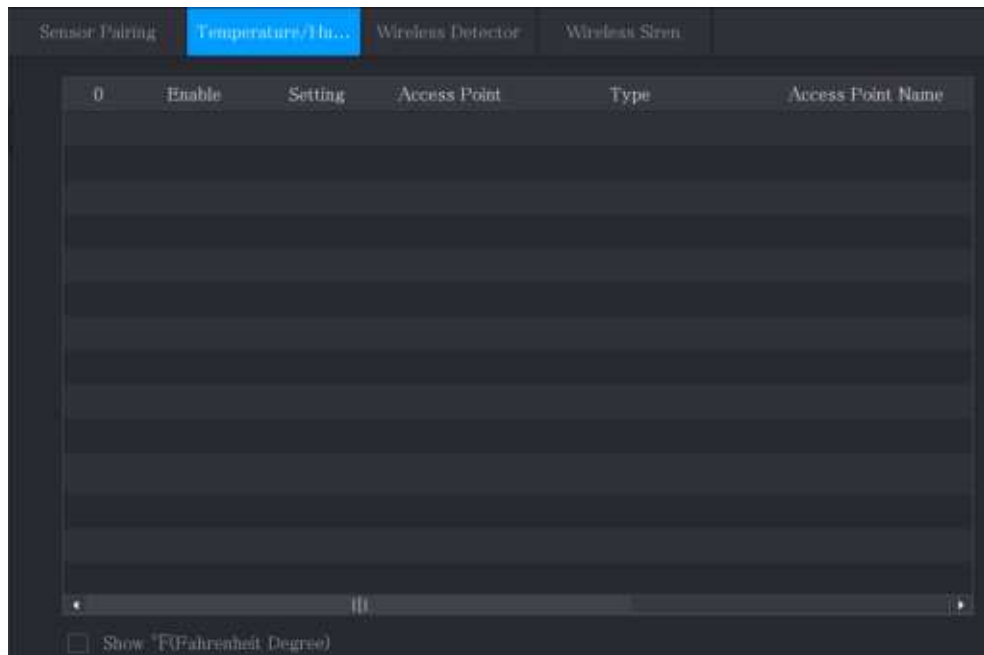
5.12.2.1 Enabling Detecting Function

You should enable the IoT function the first time when you enter this interface.

Step 1 On the main menu, select **IoT > Management > Temperature/Humidity.**

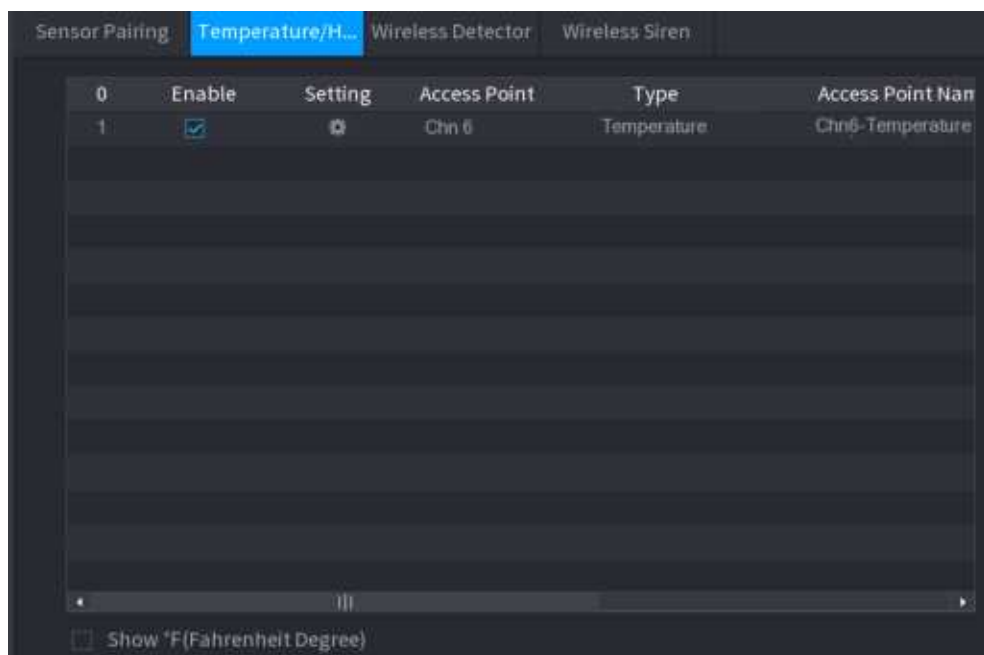
The **Temperature/Humidity** interface is displayed.

Figure 5-240



Step 2 Select the **Enable** check boxes to enable IoT function.

Figure 5-241



The Device starts detecting the temperature and humidity data from the camera and display on the **Realtime Display** interface.

Step 3 (Optional) Set temperature displaying mode.

When **Show °F (Fahrenheit Degree)** is selected, the temperature will be displayed by Fahrenheit degree in **Realtime Display** tab.

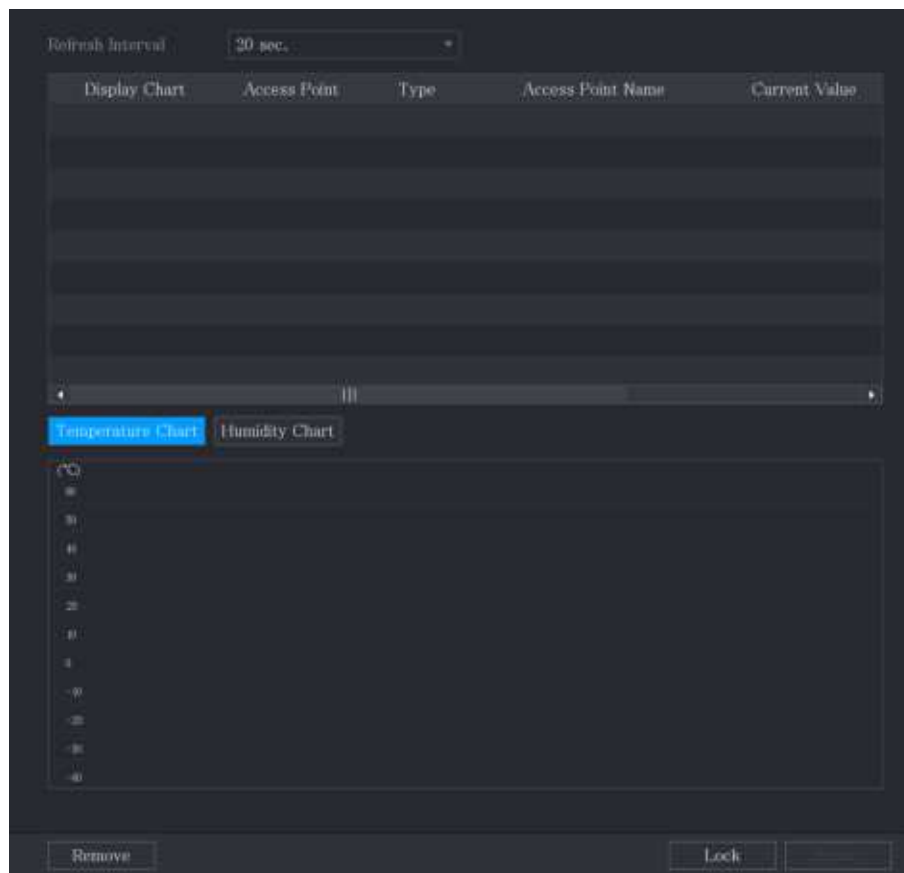
5.12.2.2 Viewing Temperature and Humidity Data

You can view the temperature and humidity data on the **Realtime Display** interface after the IoT function is enabled.

In the **Refresh Interval** box, select data refresh interval. For example, you can select **5 Sec**.

You can also display the temperature and humidity data in graphical way by selecting the **Display Chart** check box to. See Figure 5-242 for humidity data in graphical way.

Figure 5-242



Click **Remove** to delete the data.

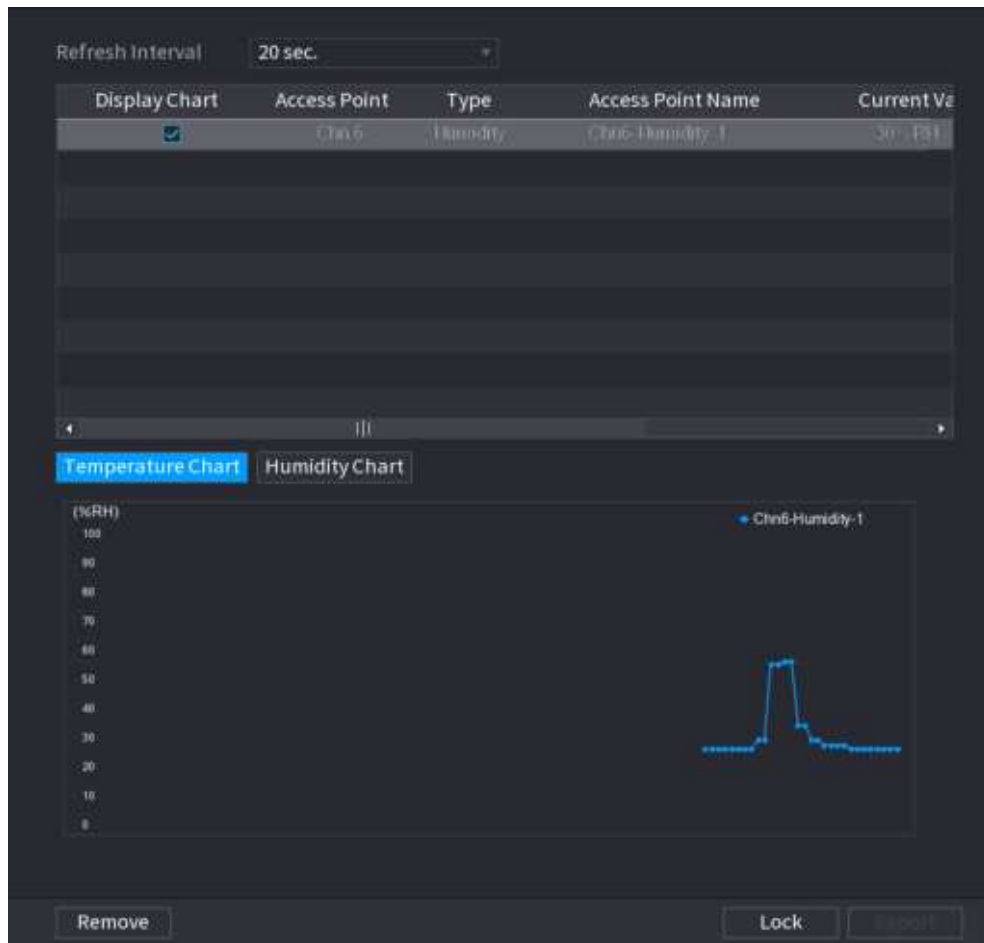
5.12.2.3 Exporting Temperature and Humidity Data

You can export the temperature and humidity data in .BMP format. Take exporting humidity data as an example.

Step 1 Prepare a USB device and plug it into the Device.

Step 2 On the **Realtime Display** interface, click the **Humidity** tab.

Figure 5-243



- Step 3** Click **Lock** to lock the data.
The export button is enabled.
- Step 4** Click **Export**. The system starts exporting the data.
After exporting is finished, a **Message** dialog box is displayed.
- Step 5** Click **OK**.
You can find the exported data on your USB device.

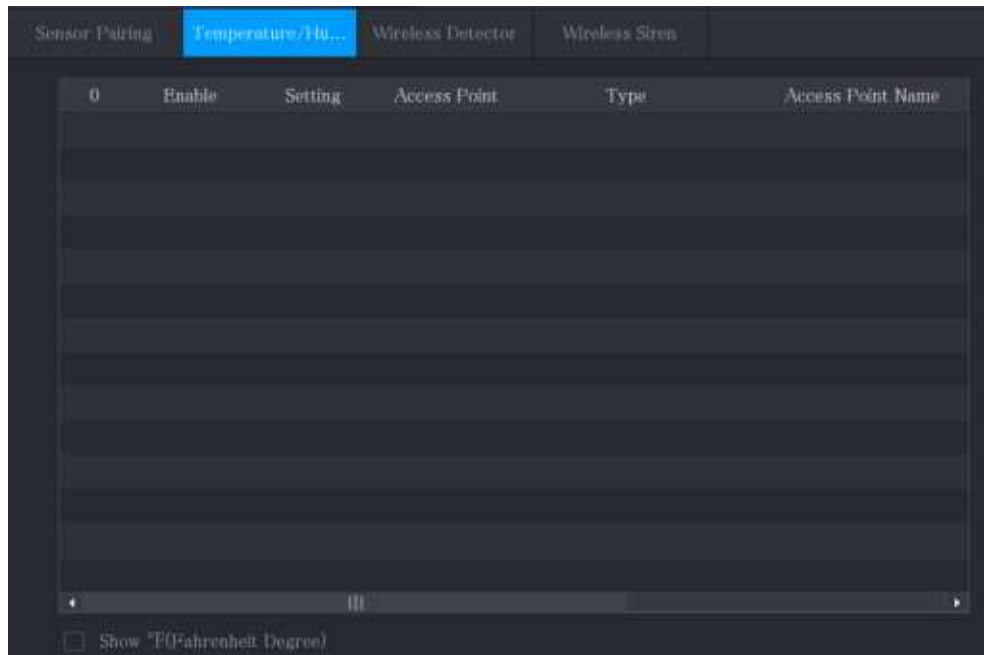
5.12.2.4 Configuring Alarm Linkage

You can configure alarm linkage settings for temperature and humidity data.

5.12.2.4.1 Configuring Alarm Linkage for Temperature Data

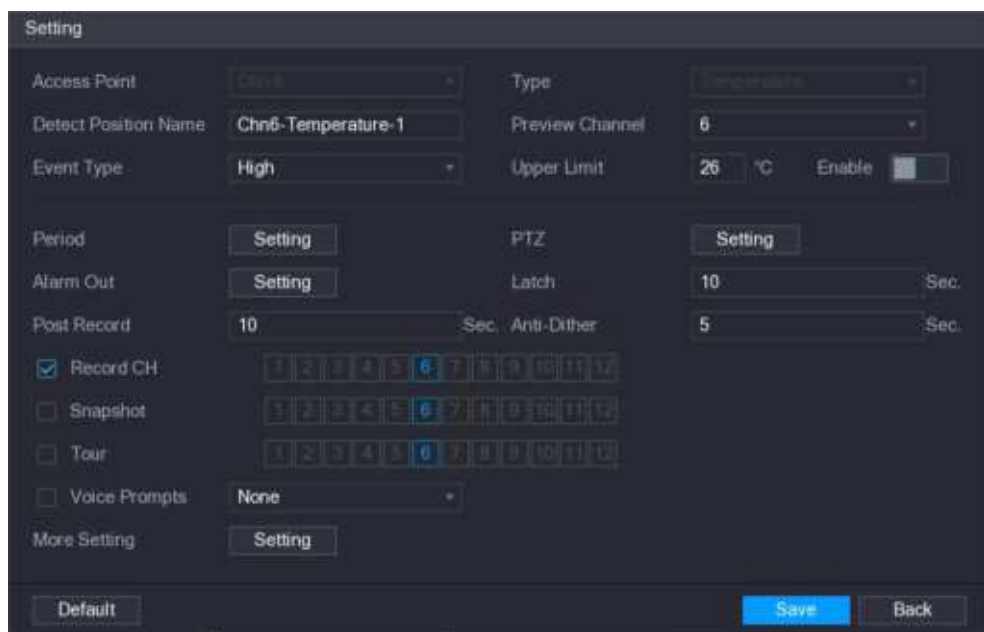
- Step 1** On the main interface, select **IoT > Management > Temperature/Humidity**.
The **Temperature/Humidity** interface is displayed.

Figure 5-244



Step 2 On the temperature information line, click .
The **Setting** interface is displayed.

Figure 5-245



Step 3 Configure the settings for alarm linkage.

Table 5-58

Parameter	Description
Access Point	Indicates the channel that the camera is connected to.
Type	Temperature by default.
Detect Position Name	Set the detect position name.
Preview Channel	Select the channel that you want to preview to help monitor the channel of access point. This channel could be the channel of access point or any other channels according to your actual situation.
Event Type	Select event type as High or Low , and set the upper and low temperature limit respectively. For example, select event type as High and set upper limit as 28 , the alarm occurs when the temperature reaches 28°C.
Upper Limit	
Enable	Enable the alarm function.
Schedule	Define a period during which the alarm setting is active. For more information about setting the period, see "5.10.4.1 Configuring Motion Detection Settings."
Alarm-out Port	Click Setting to display setting interface. - General Alarm: Enable alarm activation through the alarm devices connected to the selected output port. - External Alarm: Enable alarm activation through the connected alarm box. - Wireless Siren: Enable alarm activation through devices connected by USB gateway or camera gateway.
PTZ Linkage	Click Setting to display the PTZ interface. Enable PTZ linkage actions, such as selecting the preset that you want to be called when an alarm event occurs.
Post-Alarm	Set a length of time for the Device to delay turning off alarm after the external alarm is cancelled. The value ranges from 0 seconds to 300 seconds, and the default value is 10 seconds. If you enter 0, there will be no delay.
Post Record	Set a length of time for the Device to delay turning off recording after the alarm is cancelled. The value ranges from 10 seconds to 300 seconds, and the default value is 10 seconds.
Anti-Dither	Configure the time period from end of event detection to the stop of alarm.
Snapshot	Select the check box to take a snapshot of the selected channel.  To use this function, make sure the snapshot is enabled motion detect alarms in Main Menu > STORAGE > Schedule > Snapshot .

Parameter	Description
Record Channel	Select the channel(s) that you want to record. The selected channel(s) starts recording after an alarm occurs.  The recording for IoT alarms and auto recording function must be enabled. For details, see "5.1.4.9 Configuring Recorded Video Storage Schedule" and "5.9.1 Enabling Record Control."
Tour	Select the check box to enable a tour of the selected channels.  To use this function, make sure the tour is enabled and configured in Main Menu > DISPLAY > Tour.
Alarm Tone	Select to enable audio broadcast/alarm tones in response to a temperature alarm event.
More Setting	• Show Message: Select the Show Message check box to enable a pop-up message in your local host PC. • Buzzer: Select the check box to activate a buzzer noise at the Device. • Video Matrix: Select the check box to enable the function. When an alarm event occurs, the video output port outputs the settings configured in "Main Menu > DISPLAY > Tour."  Not all models support this function. • Send Email: Enable the system to send an email notification when an alarm event occurs.  To use this function, make sure the email function is enabled in Main Menu > NETWORK > Email. • Log: Select the check box to enable the Device to record a local alarm log. • Extra screen: Select the check box to enable the function. When an alarm event occurs, the extra screen outputs the settings configured in Main Menu > DISPLAY > Tour > Sub Screen.  • Not all models support this function. • To use this function, extra screen shall be enabled.

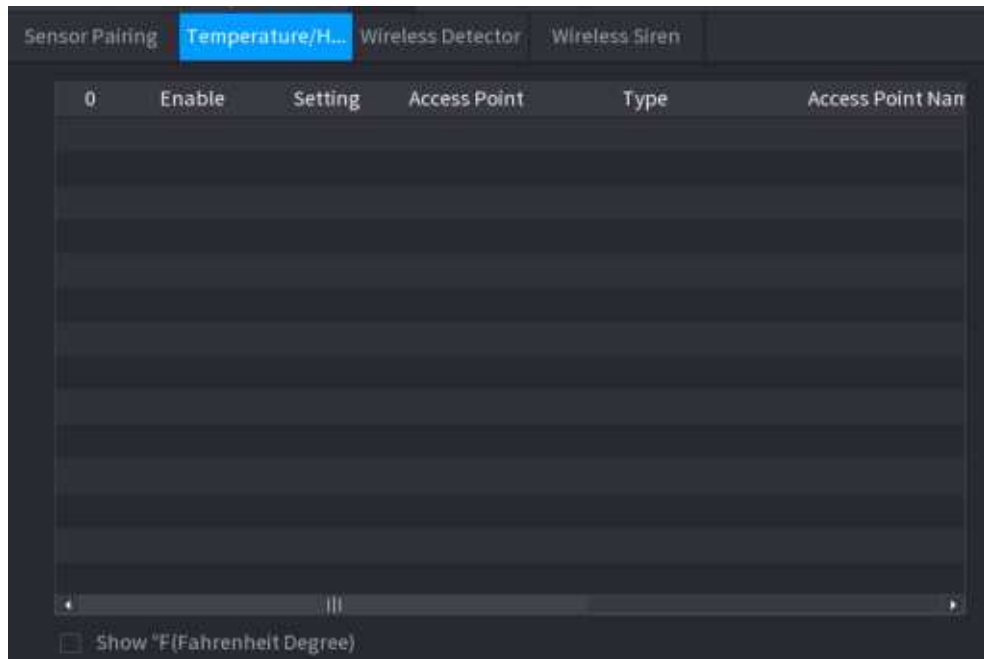
Step 4 Click **Save** to save the settings.

5.12.2.4.2 Configuring Alarm Settings for Humidity Data

You can configure the alarm event by setting the humidity data.

Step 1 On the main interface, select **IoT > Management > Temperature/Humidity**.
The **Temperature/Humidity** interface is displayed.

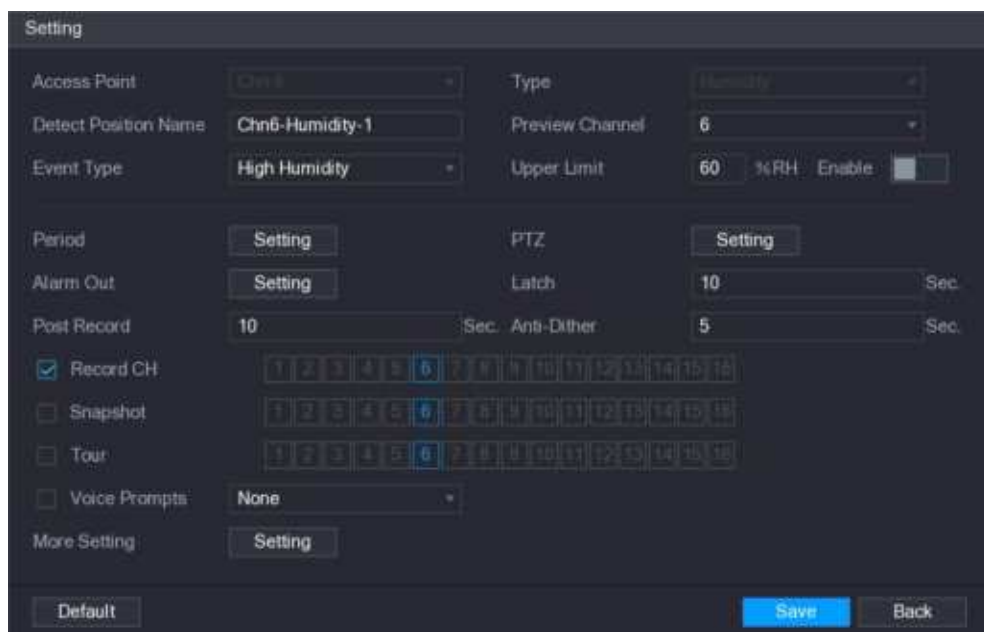
Figure 5-246



Step 2 On the humidity information line, click .

The **Setting** interface is displayed.

Figure 5-247



Step 3 Configure the settings for the following parameters.

Table 5-59

Parameter	Description
Access Point	Indicates the channel that the camera is connected to.
Type	Humidity by default.
Detect Position Name	Set the detect position name.
Preview Channel	Select the channel that you want to preview to help monitor the channel of access point. This channel could be the channel of access point or any other channels according to your actual situation.
Event Type	Select event type as High Humidity or Low Humidity , and set the upper and low humidity limit respectively. For example, select event type as High Humidity and set upper limit as 60 , the alarm occurs when the humidity reaches 60%RH.
Upper Limit	
Enable	Enable the alarm function.
Schedule	Define a period during which the alarm setting is active. For more information about setting the period, see "5.10.4.1 Configuring Motion Detection Settings."
Alarm-out Port	Click Setting to display setting interface. - General Alarm: Enable alarm activation through the alarm devices connected to the selected output port. - External Alarm: Enable alarm activation through the connected alarm box. - Wireless Siren: Enable alarm activation through devices connected by USB gateway or camera gateway.
PTZ Linkage	Click Setting to display the PTZ interface. Enable PTZ linkage actions, such as selecting the preset that you want to be called when an alarm event occurs.
Post-Alarm	Set a length of time for the Device to delay turning off alarm after the external alarm is cancelled. The value ranges from 0 seconds to 300 seconds, and the default value is 10 seconds. If you enter 0, there will be no delay.
Post Record	Set a length of time for the Device to delay turning off recording after the alarm is cancelled. The value ranges from 10 seconds to 300 seconds, and the default value is 10 seconds.
Anti-Dither	Configure the time period from end of event detection to the stop of alarm.
Snapshot	Select the check box to take a snapshot of the selected channel.  To use this function, make sure the snapshot is enabled motion detect alarms in Main Menu > STORAGE > Schedule > Snapshot .

Parameter	Description
Record Channel	Select the channel(s) that you want to record. The selected channel(s) starts recording after an alarm occurs.  The recording for IoT alarms and auto recording function must be enabled. For details, see "5.1.4.9 Configuring Recorded Video Storage Schedule" and "5.9.1 Enabling Record Control."
Tour	Select the check box to enable a tour of the selected channels.  To use this function, make sure the tour is enabled and configured in Main Menu > DISPLAY > Tour.
Alarm Tone	Select to enable audio broadcast/voice prompts in response to a temperature alarm event.
More Setting	• Show Message: Select the Show Message check box to enable a pop-up message in your local host PC. • Buzzer: Select the check box to activate a buzzer noise at the Device. • Video Matrix: Select the check box to enable the function. When an alarm event occurs, the video output port outputs the settings configured in "Main Menu > DISPLAY > Tour."  Not all models support this function. • Send Email: Enable the system to send an email notification when an alarm event occurs.  To use this function, make sure the email function is enabled in Main Menu > NETWORK > Email. • Log: Select the check box to enable the Device to record a local alarm log.

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

5.12.2.5 Searching IoT Information

You can search and backup all your IoT data.

To back up the data, you should prepare a USB device and plug it into the Device.

Step 1 On the main interface, select **IoT > IOT Search**.

Figure 5-248

Step 2 Configure the parameters settings.

Table 5-60

Parameter	Description
Access Point	Indicates the channel that the camera is connected to.
Display Type	In the Display Type list, select List or Diagram .
Type	Select the information type that you want to search. You can select Humidity or Temperature .
Status	Select the information state that you want to search. This option is available when you select List in the Display Type list.
Start Time	Enter the start time and end time for the information that you want to search.
End Time	

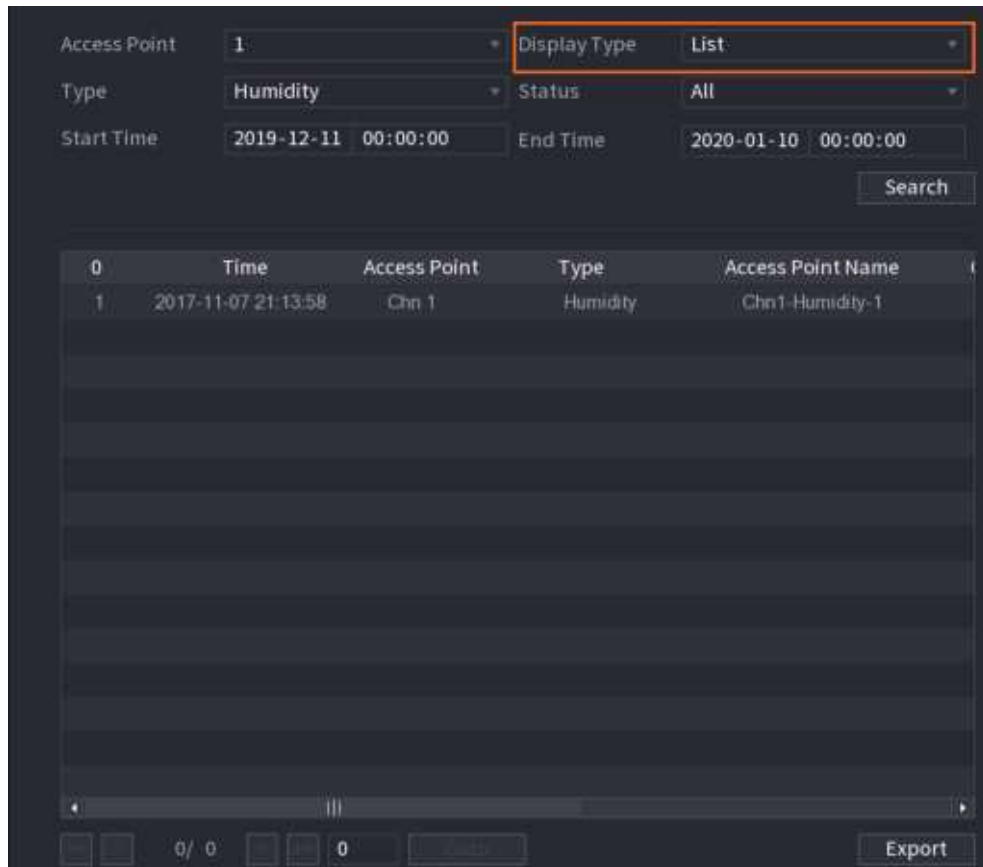
Step 3 Click **Search**.

The system starts search according to your parameters settings. After searching is finished, the result displays. For the data displayed in list, see Figure 5-249.



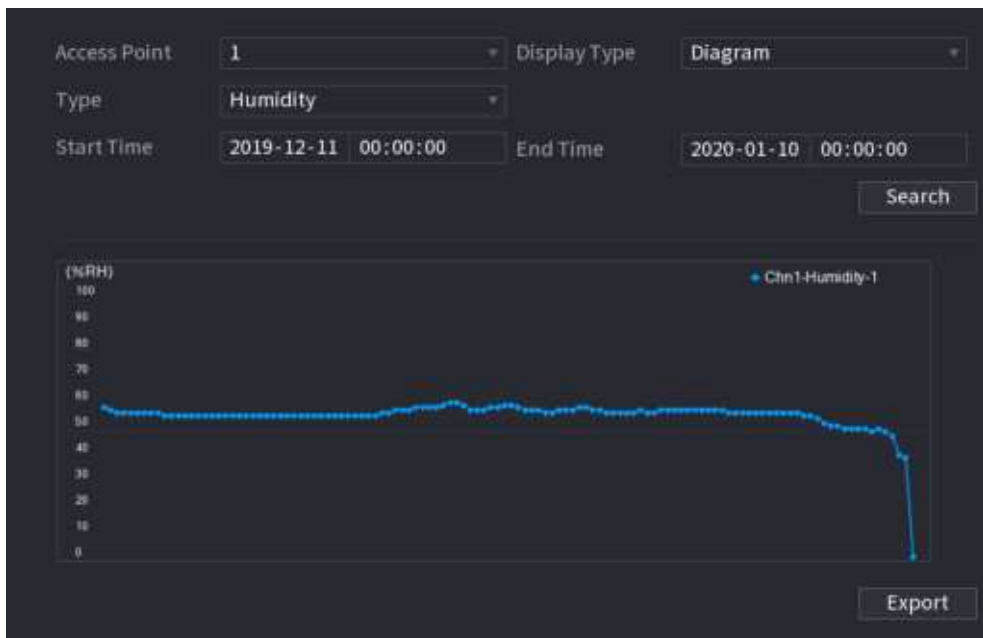
Click **Goto** to switch result pages.

Figure 5-249



- For the data displayed in graph, see Figure 5-250.

Figure 5-250



Step 4 Click **Export**. The system starts exporting the data.
After exporting is finished, a **Message** dialog box is displayed.

Step 5 Click **OK**.
You can find the exported data on your USB device.

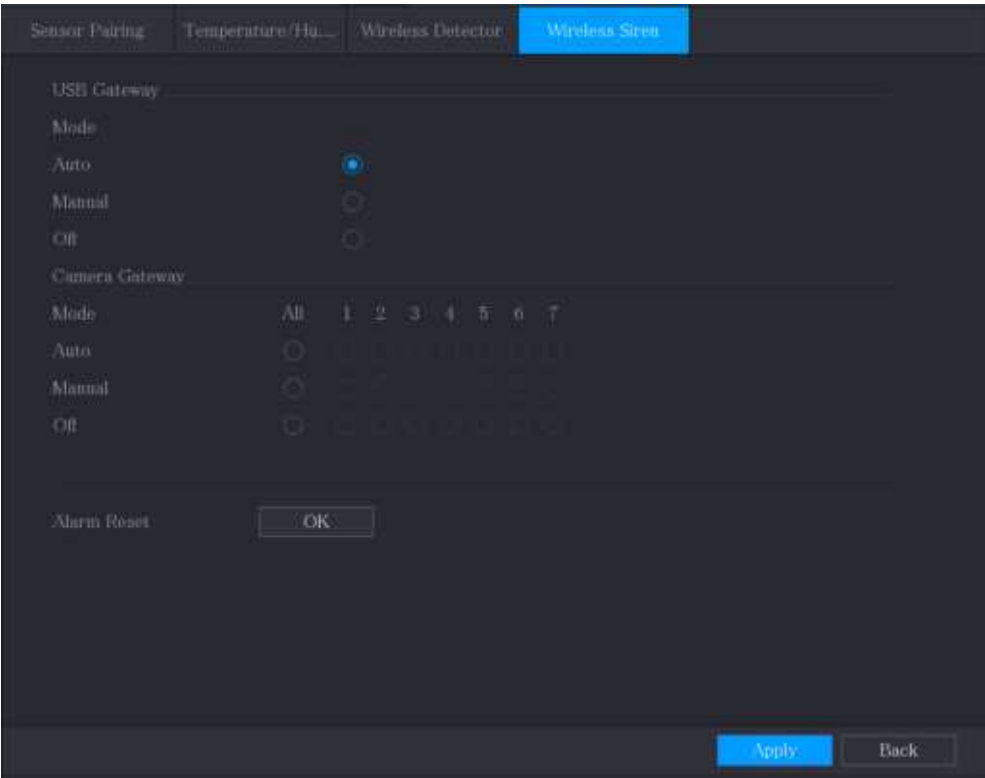
5.12.3 Configuring Wireless Siren

You can connect the wireless siren to the Device, when there is an alarm event activated on the Device, the wireless siren generate alarms.

Step 1 Select **Main Menu > IoT > Management > Wireless Siren**.

The **Wireless Siren** interface is displayed.

Figure 5-251



Step 2 Configure the settings for the wireless alarm output.

Table 5-61

Parameter	Description
USB Gateway, Camera Gateway	● Auto: Automatically activate alarm if the alarm output function for wireless siren is enabled for specific events. For example, if you want to enable the alarm output through wireless siren for motion detection, see "Alarm Output" parameter in Table 5-41. ● Manual: Activate alarm immediately. ● Off: Do not activate alarm.
Alarm Release	Click OK to clear all alarm output status of wireless siren.

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

5.13 Configuring POS Settings

You can connect the Device to the POS (Point of Sale) machine and receive the information from it. This function applies to the scenarios such as supermarket POS machine. After connection is established, the Device can access the POS information and display the overlaid text in the channel window.



Playing POS information in the local playback and viewing the POS information in the live view screen only support single-channel mode and four-channel mode. Displaying monitoring screen and playing back in the web support multi-channel mode.

5.13.1 Searching the Transaction Records



The system supports fuzzy search.

Step 1 Select **Main Menu > POS > POS Search**.

The **POS Search** interface is displayed.

Figure 5-252

Step 2 In the **POS Search** box, enter the information such as transaction number on your receipt, amount, or product name.

Step 3 In the **Start Time** box and **End Time** box, enter the time period that you want to search the POS transaction information.

Step 4 Click **Search**.

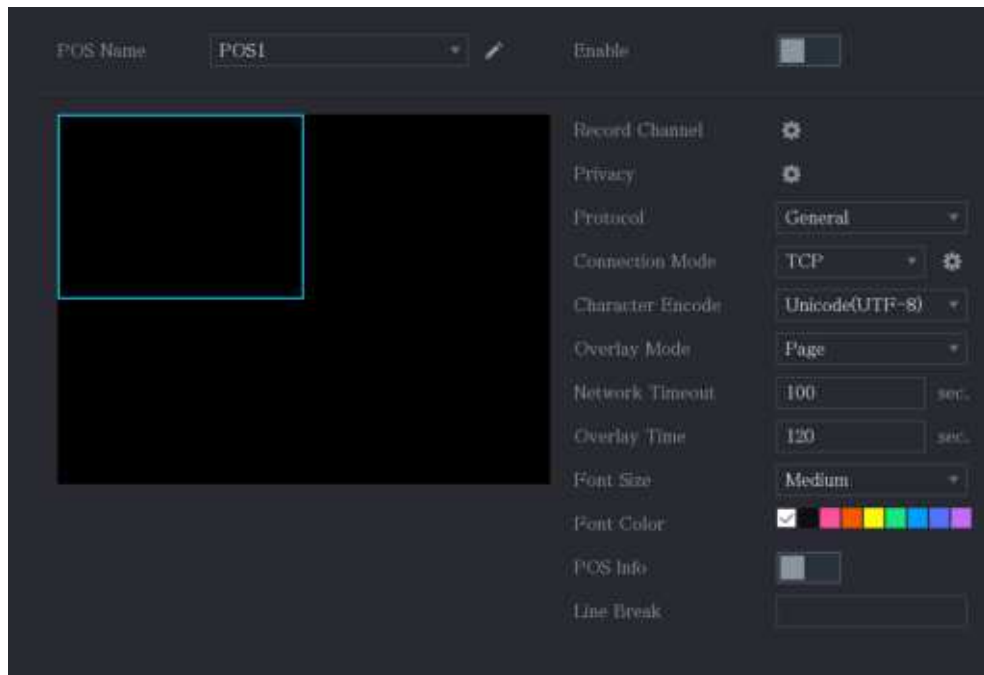
The searched transaction results display in the table.

5.13.2 Configuring POS Settings

Step 1 Select **Main Menu > POS > POS Setting**.

The **POS Setting** interface is displayed.

Figure 5-253



Step 2 Configure the settings for the POS parameters.

Table 5-62

Parameter	Description
POS Name	In the POS Name list, select the POS machine that you want to configures settings for. Click  to modify the POS name.  The POS name supports 21 Chinese characters or 63 English characters.
Enable	Enable the POS function.
Record Channel	Select the channel(s) that you want to record. The selected channel(s) starts recording after an alarm occurs.  The recording for POS alarms and auto recording function must be enabled. For details, see "5.1.4.9 Configuring Recorded Video Storage Schedule" and "5.9.1 Enabling Record Control."
Privacy	Enter the privacy content.
Protocol	Select POS by default. Different machine corresponds to different protocol.
Connection Mode	In the Connect Type list, select the connection protocol type. Click , the IP Address interface is displayed. In the Source IP box, enter the IP address (the machine that is connected to the Device) that sends messages.
Character Encode	Select a character encoding mode.

Parameter	Description
Overlay Mode	In the Overlay Mode list, Select Page or ROLL. • Page means to turn a page when there are 16 lines of overlay information. • ROLL means to roll up the interface when there are 16 lines of overlay information. The first line disappears each time.  When local preview mode is 4-split, overlay information is substituted when there are 8 lines.
Network Timeout	When the network is not working correctly and cannot be recovered after the entered timeout limit, the POS information will not display normally. After the network is recovered, the latest POS information will be displayed.
Overlay Time	Enter the time that how long you want to keep the POS information displaying. For example, enter 5, the POS information disappear from the screen after 5 seconds.
Font Size	In the Font Size list, select Small , Medium , or Large as the text size of POS information
Font Color	In the color bar, click to select the color for the text size of POS information.
POS Info	Enable the POS Info function, the POS information displays in the live view screen.
Line Break	It does not need to configure. The system goes to a new line 1s after no data is received. If you enter a line delimiter, the system goes to a new line when overlay information identifies the line delimiter (hexadecimal). For example, if line delimiter is F and overlay information is 123156789, the local preview and web overlay information is displayed as: <pre>123 6789</pre>

Step 3 Click **Apply** to complete the settings.

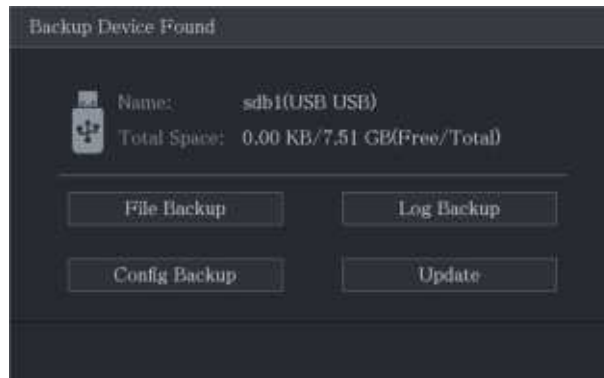
5.14 Configuring Backup Settings

5.14.1 Finding USB Device

When you inset a USB storage device into the USB port of the Device, the Device detects the USB storage device and pops up **Find USB device** interface, which provides you a shortcut to perform backup and upgrading operations. See Figure 5-254.

For details, see "5.14.2 Backing up Files", "5.21.2 Viewing Log Information", "5.20.4 Exporting and Importing System Settings", and "5.20.6 Updating the Device."

Figure 5-254



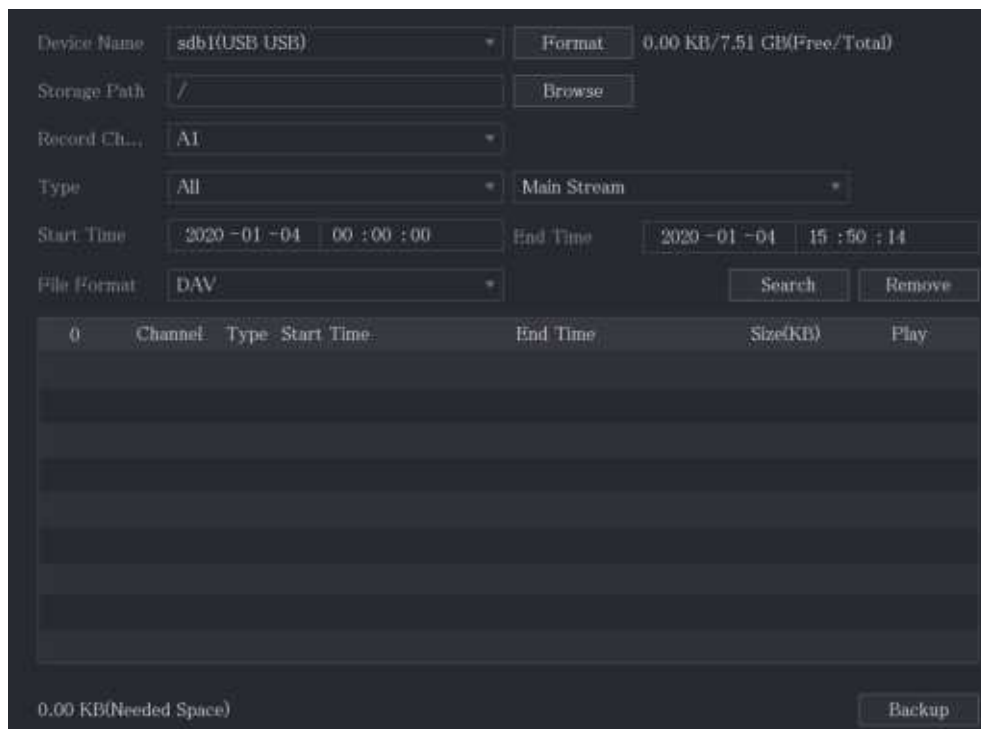
5.14.2 Backing up Files

You can back up the recorded videos and snapshots.

Step 1 Select **Main Menu > Backup**.

The **Backup** interface is displayed.

Figure 5-255



Step 2 Configure the settings for the backup parameters.

Table 5-63

Parameter	Description
Device Name	In the Device Name list, select the device that you want to back up the files to.
Format	Click Format, the Format interface is displayed. - If the capacity of external storage device is less than 2TB, you can select FAT32 or NTFS to format it. - If the capacity of external storage device is equal to or more than 2TB, you can only select NTFS to format it.

Parameter	Description
Path	Click Browse , the Browse interface is displayed. Select the route where you want to search for the files.
Record Channel	In the Record Channel list, select the channel where you want to search for the files.
Type	In the Type list, select the file type that you want to search.
Start Time	Enter the start time and end time for the files that you want to search.
End Time	
File Format	In the File Format list, select the file format as DAV or MP4 that you want to search.

Step 3 Click **Search** to search the files that meet the configured settings.

The searched results will display in the table.

Step 4 Select the files that you want to back up.

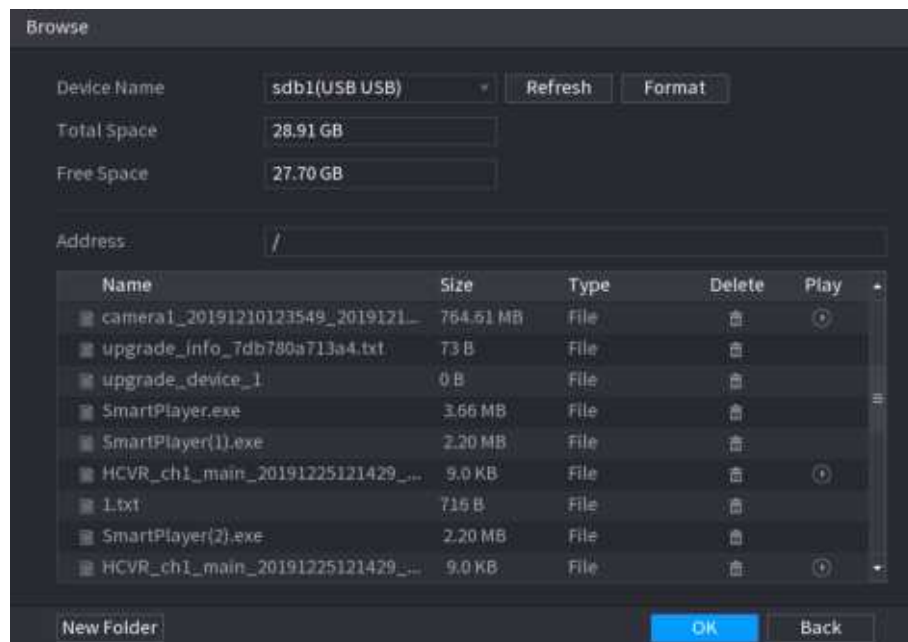
Step 5 Click **Backup** to back up the selected files to the configured path.



Click **Remove** to remove all the searched results.

The system will display a backup progress bar. A dialog box will be prompted When backup is completed.

Figure 5-256



Step 6 Click **OK**.

5.15 Network Management

5.15.1 Configuring Network Settings

You can ensure the network interworking between the Device and other devices through configuring the network settings.

5.15.1.1 Configuring TCP/IP Settings

You can configure the settings for the Device such as IP address, DNS according to the networking plan.

Select **Main Menu > NETWORK > TCP/IP**, the **TCP/IP** interface is displayed.

For details about parameter settings, see "5.1.4.4 Configuring Network Settings."

Figure 5-257

The screenshot displays the TCP/IP configuration interface. At the top, there is a table with columns: NIC Name, IP Address, Network Mode, NIC Member, Modify, and Unbind. The first row shows 'NIC1' with a 'Single NIC' mode and member '1'. Below the table, the configuration fields are organized into sections. The first section includes 'IP Address', 'Default Gateway', and 'MTU: 1500'. The second section includes 'MAC Address', 'Subnet Mask', and 'Mode: Static'. The third section includes 'IP Version' (set to 'IPv4'), 'Preferred DNS', 'Alternate DNS', and 'Default Card' (set to 'NIC1'). At the bottom, there are three buttons: 'Test', 'Apply', and 'Back'.

5.15.1.2 Configuring Port Settings

You can configure the maximum connection accessing the Device from Client such as WEB, Platform, and Mobile Phone and configure each port settings.

Step 1 Select **Main Menu > NETWORK > Port**.

The **Port** interface is displayed.

Figure 5-258

The screenshot shows a configuration window titled 'NETWORKS' with a sidebar on the left containing various network-related options: TCP/IP, Port, Wi-Fi, 3G/4G, PPPoE, EDMS, UPnP, Email, SRMP, Multicast, Alarm Center, Registrar, and P2P. The 'Port' option is selected. The main area displays several parameters with their current values and ranges in parentheses:

- Max Connection: 128 (0 - 128)
- TCP Port: 37777 (1025 - 65535)
- UDP Port: 37778 (1025 - 65535)
- HTTP Port: 80 (1 - 65535)
- HTTPS Port: 443 (1 - 65535)
- RTSP Port: 554 (1 - 65535)
- NTP Server Port: 123 (1 - 65535)
- POS Port: 38800 (1025 - 65535)

At the bottom right, there are 'Apply' and 'Back' buttons.

Step 2 Configure the settings for the connection parameters.



The parameter setting can take effect without need to reboot the device.

Table 5-64

Parameter	Description
Max Connection	The allowable maximum clients accessing the Device at the same time, such as WEB, Platform, and Mobile Phone. Select a value between 1 and 128. The default value setting is 128.
TCP Port	The default value setting is 37777. You can enter the value according to your actual situation.
UDP Port	The default value setting is 37778. You can enter the value according to your actual situation.
HTTP Port	The default value setting is 80. You can enter the value according to your actual situation. If you enter other value, for example, 70, and then you should enter 70 after the IP address when logging in the Device by browser.
RTSP Port	The default value setting is 554. You can enter the value according to your actual situation.
POS Port	Data transmission. The value range is from 1 through 65535. The default value is 38800.
NTP Server Port	The default value setting is 123. You can enter the value according to your actual situation.

HTTPS Port	HTTPS communication port. The default value setting is 443. You can enter the value according to your actual situation.
------------	---

Step 3 Click **Apply** to complete the settings.

5.15.1.3 Configuring Wi-Fi Connection Settings

You can make wireless connection between the Device and the other devices in the same network through Wi-Fi settings, facilitating the devices connection and mobility.

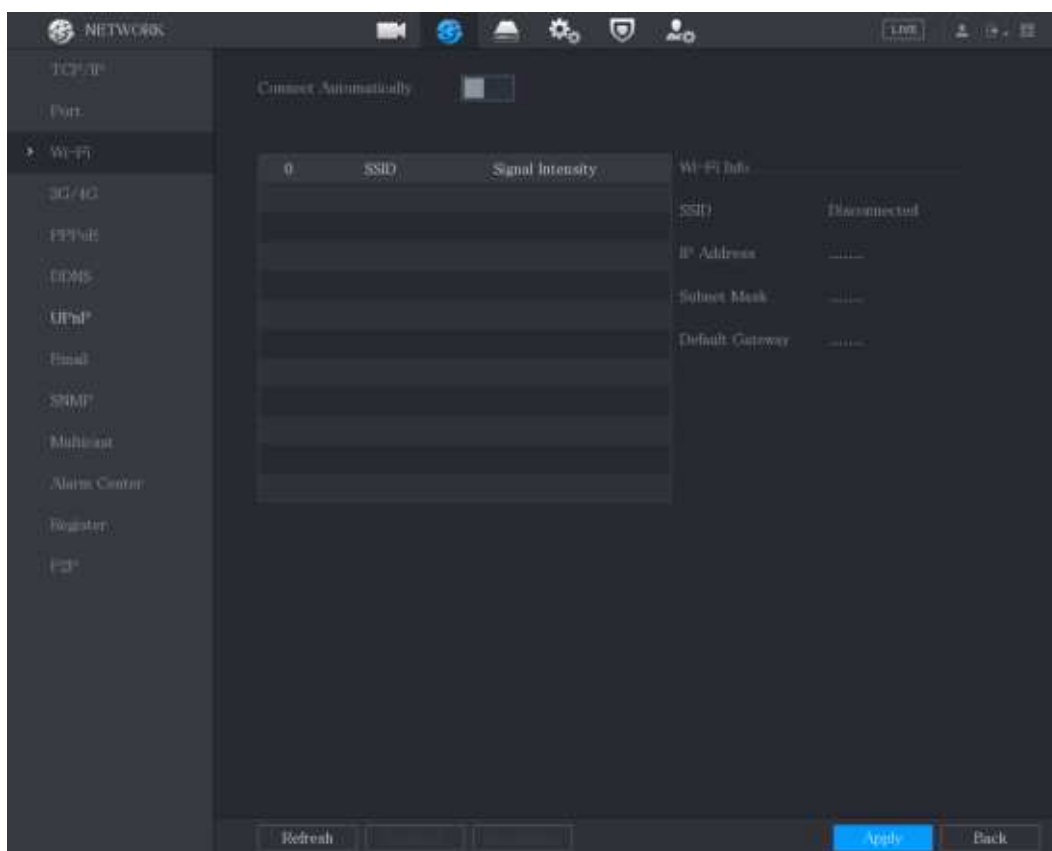


Only the Device with Wi-Fi module supports this function.

Step 1 Select **Main Menu > NETWORK > Wi-Fi**.

The **Wi-Fi** interface is displayed.

Figure 5-259



Step 2 Configure the settings for the Wi-Fi connection parameters.

Table 5-65

Parameter	Description
Connect Automatically	Enable Connect Automatically . After the Device is restarted, it will automatically connect to the nearest hotspot that had been connected successfully.
Refresh	Refresh the hotspot list. The self-adaption function such as adding password is supported if such setting was once configured.

Connect	In the hotpots list, select a hotspot, and then click Connect. - To reconnect the same hotspot, disconnect first and then reconnect. - To connect to other hotspot, disconnect from the current connected hotspot first, and then connect to the other hotspot.
Disconnect	To disconnect from a hotspot, click Disconnect .

Step 3 Click **Apply** to complete the settings.

After the Device is connected to a Wi-Fi hotspot, in the **Wi-Fi Info** area, the current hotspot, IP address, subnet mask, and default gateway are displayed.

5.15.1.4 Configuring 3G/4G Settings

You can connect a wireless 3G/4G module to the USB port of the Device and then access the Device with the IP address provided by the module.



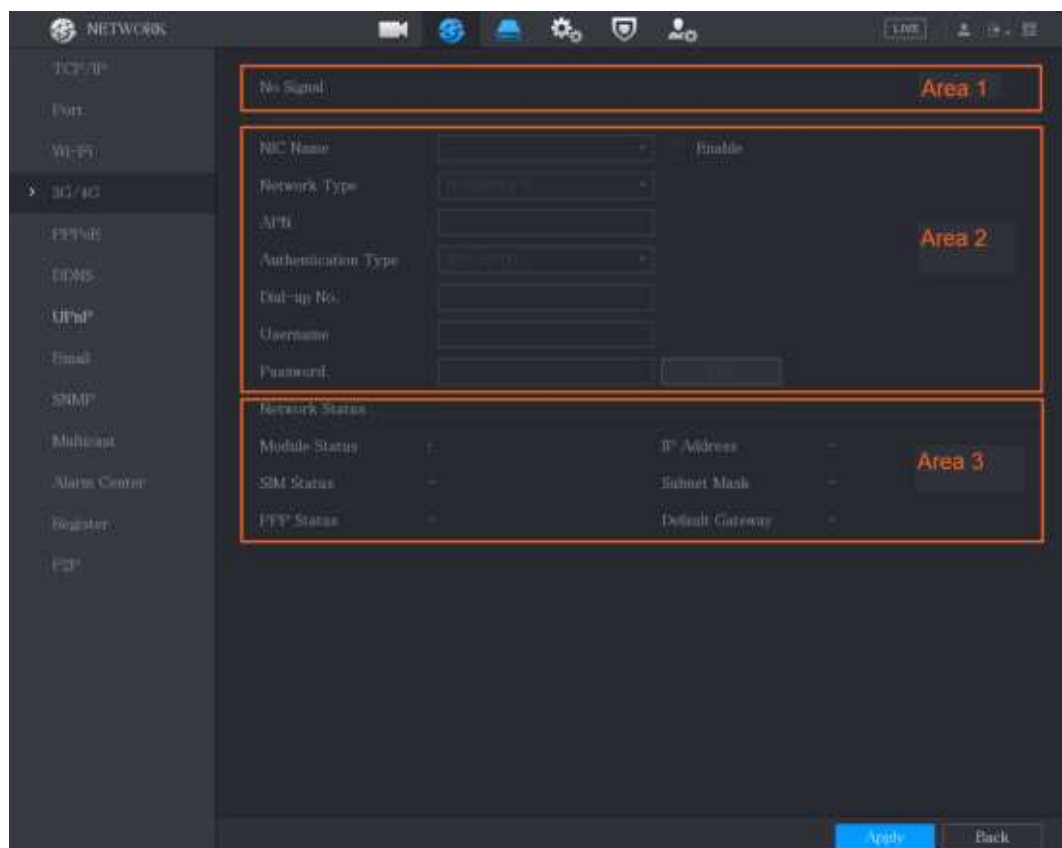
Not all models support this function.

Step 1 Connect the wireless 3G/4G module to the USB port of the Device.

Step 2 Select **Main Menu > NETWORK > 3G/4G**.

The **3G/4G** interface is displayed.

Figure 5-260



The 3G/4G interface is consisted of three areas:

- Area 1: Displays the signal strength.
- Area 2: Displays the module configurations.
- Area 3: Displays the connection state.



The information of Area 2 will display after the 3G/4G module is connected; while the information of Area 1 and Area 3 will display only after the 3G/4G function is enabled.

Step 3 The Device starts identifying the wireless module and displays the recognized information for the parameters in Area 2.

Table 5-66

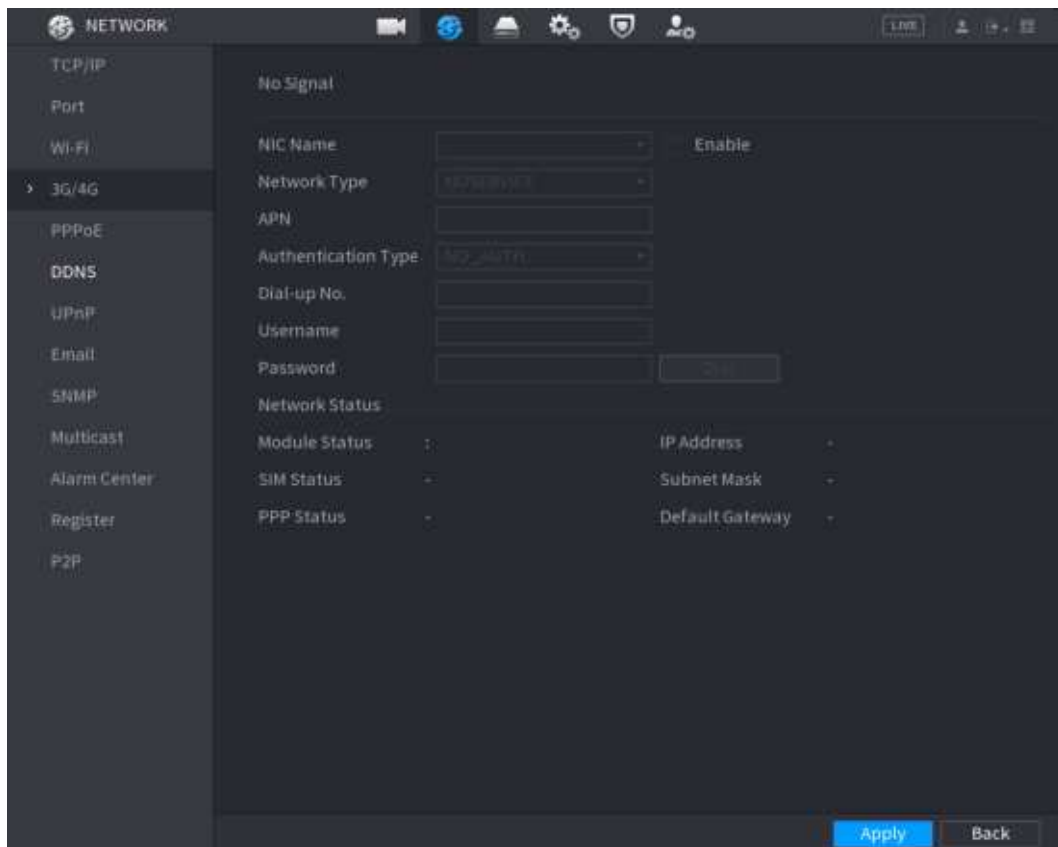
Parameter	Description
NIC Name	Displays the name of Ethernet card.
Network Type	Displays the network type. Different type represents different supplier.
APN	Displays the default APN number.
Dial-up No.	Displays the default dial No.
Authentication Type	Authentication mode. You can select PAP , CHAP , or NO_AUTH .
Username, Password	Enter the username and password for authentication.

Step 4 Select the **Enable** check box.

Step 5 Click **Dial** to start connecting.

After the connection is established, the result is displayed in the **Wireless Network** area.

Figure 5-261



Step 6 Click **Apply** to complete the settings.

Supported 3G/4G Modules by the Device

- China Mobile 3G/4G: ZTE MF832S
- China Mobile 4G: ZTE MF832S

- China Unicom 3G: ZTE MF667S, HUAWEI E353U-1
- China Telecom 4G: HUAWEI EC122, ZTE AC2736



- If the Device is connected to China Telecom 3G/4G network, you can login the Device with the public IP address through the PC of public internet (The HTTP port is not configured as 80). If the Device is connected to China Unicom or China Mobile 3G network, which are defined as private network, therefore you cannot login the Device through PC that is connected to public internet.
- The Ethernet card names that are displayed on the 3G/4G interface are not constant, and they could be ppp5, ppp6, ppp7 or ppp8 and are different depending on the USB2.0 port on the Device that is connected to the 3G module.
- If you dial to connect to 3G/4G network, you have to keep trying till succeeded. The default gateway could be switched depending on the priority of Ethernet cards.
- The China Unicom and China Mobile 3G/4G modules in USB flash disk style do not support EDGE mode for the moment.

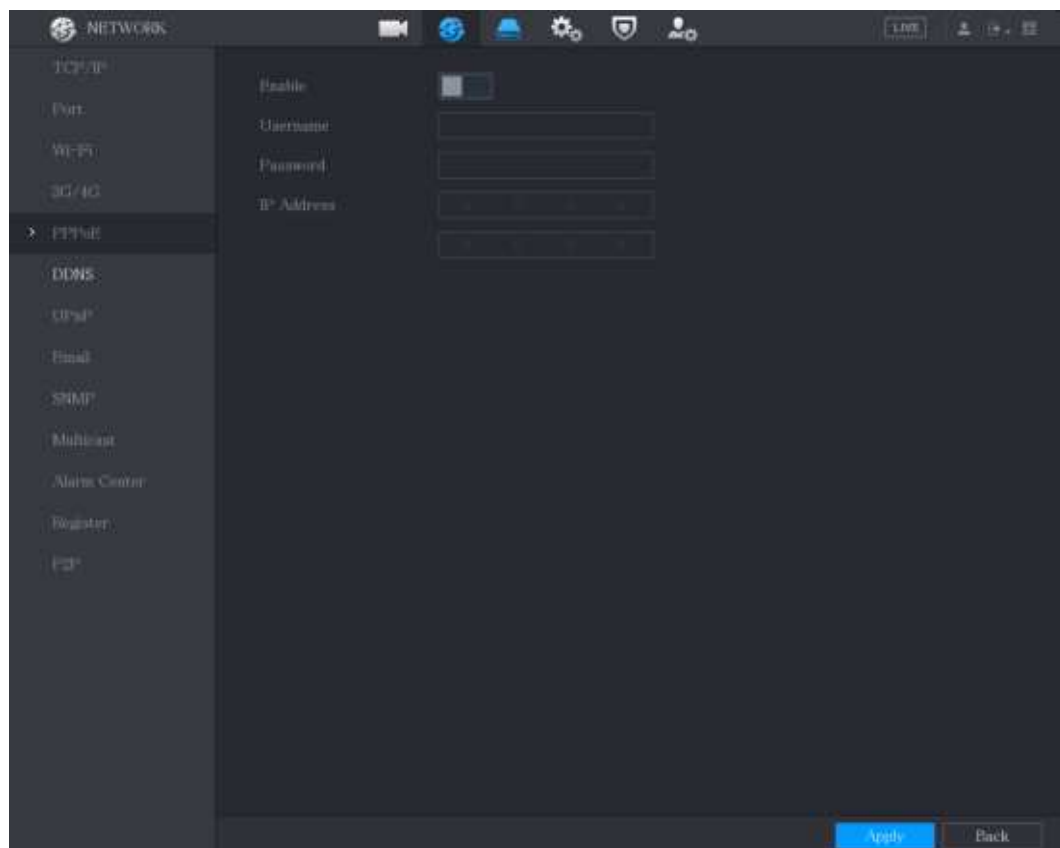
5.15.1.5 Configuring PPPoE Settings

PPPoE is another way for the Device to access the network. You can establish network connection by configuring PPPoE settings to give the Device a dynamic IP address in the WAN. To use this function, firstly you need to obtain the user name and password from the Internet Service Provider.

Step 1 Select **Main Menu > NETWORK > PPPoE**.

The **PPPoE** interface is displayed.

Figure 5-262



Step 2 Enable the PPPoE function.

Step 3 In the **Username** box and **Password** box, enter the user name and password accordingly provided by the Internet Service Provider.

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

The system pops up a message to indicate the successfully saved. The IP address appears on the PPPoE interface. You can use this IP address to access the Device.



When the PPPoE function is enabled, the IP address on the **TCP/IP** interface cannot be modified.

5.15.1.6 Configuring DDNS Settings

When the IP address of the Device changes frequently, the DDNS function can dynamically refresh the correspondence between the domain on DNS and the IP address, ensuring you access the Device by using the domain.

Preparing for Configuration

Confirm if the Device supports the DDNS Type and log in the website provided by the DDNS service provider to register the information such as domain from PC located in the WAN.



After you have registered and logged in the DDNS website successfully, you can view the information of all the connected devices under this user name.

Configuring Steps

Step 1 Select **Main Menu > NETWORK > DDNS**.

The **DDNS** interface is displayed.

Figure 5-263

Step 2 Configure the settings for the DDNS parameters.

Table 5-67

Parameter	Description
Enable	Enable the DDNS function.  After enabling DDNS function, the third-party might collect your Device information.
Type	Type and address of DDNS service provider.
Server Address	- Type: DynDNS DDNS; address: members.dyndns.org - Type: NO-IP DDNS; address: dynupdate.no-ip.com - Type: CN99 DDNS; address: members.3322.org
Domain Name	The domain name for registering on the website of DDNS service provider.
User Name	Enter the user name and password obtained from DDNS service provider. You need to register (including user name and password) on the website of DDNS service provider.
Password	
Interval	Enter the amount of time that you want to update the DDNS.

Step 3 Click **Apply** to complete the settings.

Enter the domain name in the browser on your PC, and then press **Enter**.

If the web interface of the Device is displayed, the configuration is successful. If not, the configuration is failed.

5.15.1.7 Configuring EMAIL Settings

You can configure the email settings to enable the system to send the email as a notification when there is an alarm event occurs.

Step 1 Select **Main Menu > NETWORK > Email**.

The **Email** interface is displayed.

Figure 5-264

Step 2 Configure the settings for the email parameters.

Table 5-68

Parameter	Description
Enable	Enable the email function.  There might be risk of sending data to specified email address after it is enabled.
SMTP Server	Enter the address of SMTP server of sender's email account.
Port	Enter the port value of SMTP server. The default value setting is 25. You can enter the value according to your actual situation.
Username	Enter the user name and password of sender's email account.
Password	
Anonymous	If enable the anonymity function, you can login as anonymity.
Receiver	In the Receiver list, select the number of receiver that you want to receive the notification. The Device supports up to three mail receivers.
Email Address	Enter the email address of mail receiver(s).

Parameter	Description
Sender	Enter the sender's email address. It supports maximum three senders separated by comma.
Subject	Enter the email subject. Supports Chinese, English and Arabic numerals. It supports maximum 64 characters.
Attachment	Enable the attachment function. When there is an alarm event, the system can attach snapshots as an attachment to the email.
Encryption Type	Select the encryption type: NONE , SSL , or TLS .  For SMTP server, the default encryption type is TLS .
Sending Interval (sec.)	This is the interval that the system sends an email for the same type of alarm event, which means, the system does not send an email upon any alarm event. This setting helps to avoid the large amount of emails caused by frequent alarm events. The value ranges from 0 to 3600. 0 means that there is no interval.
Health Mail	Enable the health test function. The system can send a test email to check the connection.
Sending Interval (Min.)	This is the interval that the system sends a health test email. The value ranges from 30 to 1440. 0 means that there is no interval.
Test	Click Test to test the email sending function. If the configuration is correct, the receiver's email account will receive the email.  Before testing, click Apply to save the settings.

Step 3 Click **Apply** to complete the settings.

5.15.1.8 Configuring UPnP Settings

You can map the relationship between the LAN and the WAN to access the Device on the LAN through the IP address on the WAN.

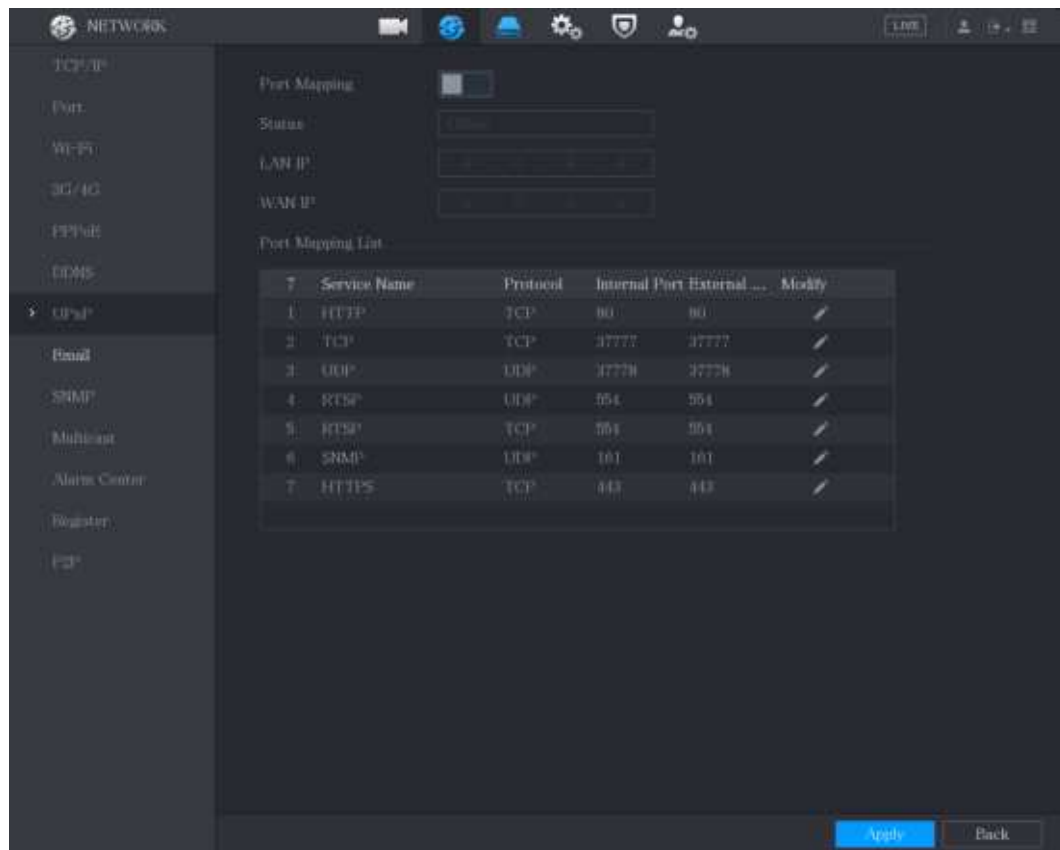
Preparation for Configuration

- Login the router to set the WAN port to enable the IP address to connect into the WAN.
- Enable the UPnP function at the router.
- Connect the Device with the LAN port on the router to connect into the LAN.
- Select **Main Menu > NETWORK > TCP/IP**, configure the IP address into the router IP address range, or enable the DHCP function to obtain an IP address automatically.

Configuration Steps

Step 1 Select **Main Menu > NETWORK > UPnP**.
The **UPnP** interface is displayed.

Figure 5-265



Step 2 Configure the settings for the UPnP parameters.

Table 5-69

Parameter	Description
Port Mapping	Enable the UPnP function. After it is enabled, the intranet services and ports shall be mapped to extranet, proceed with caution.
Status	Indicates the status of UPnP function. - Offline: Failed. - Online: Succeeded.
LAN IP	Enter IP address of router on the LAN. After mapping succeeded, the system obtains IP address automatically without performing any configurations.
WAN IP	Enter IP address of router on the WAN. After mapping succeeded, the system obtains IP address automatically without performing any configurations.

Parameter	Description
Port Mapping List	The settings in PAT table correspond to the UPnP PAT table on the router. • Service Name: Name of network server. • Protocol: Type of protocol. • Int. Port: Internal port that is mapped on the Device. • Ext. Port: External port that is mapped on the router.  • To avoid the conflict, when setting the external port, try to use the ports from 1024 through 5000 and avoid popular ports from 1 through 255 and system ports from 256 through 1023. • When there are several devices in the LAN, reasonably arrange the ports mapping to avoid mapping to the same external port. • When establishing a mapping relationship, ensure the mapping ports are not occupied or limited. • The internal and external ports of TCP and UDP must be the same and cannot be modified. • Click  to modify the external port.

Step 3 Click **Apply** to complete the settings.

In the browser, enter http://WAN IP: External IP port. You can visit the LAN Device.

5.15.1.9 Configuring SNMP Settings



Not all models support this function.

You can connect the Device with some software such as MIB Builder and MG-SOFT MIB Browser to manage and control the Device from the software.

Preparation for Configuration

- Install the software that can manage and control the SNMP, such as MIB Builder and MG-SOFT MIB Browser
- Obtain the MIB files that correspond to the current version from the technical support.

Configuration Steps

Step 1 Select **Main Menu > NETWORK > SNMP**.

The **SNMP** interface is displayed.

Figure 5-266

The screenshot shows the 'SNMP' configuration page in a network management system. The left sidebar contains a list of protocols: TCP/IP, Port, Wi-Fi, 3G/4G, PPPoE, EDMS, CPsP, Email, **SNMP**, Multicast, Alarm Center, Register, and P2P. The main configuration area for SNMP includes the following fields:

- Enable:** A checkbox that is currently checked.
- Version:** Radio buttons for V1, V2, and V3 (Recommended), with V3 selected.
- SNMP Port:** A text box containing '161'.
- Read Community:** An empty text box.
- Write Community:** An empty text box.
- Trap Address:** An empty text box.
- Trap Port:** A text box containing '162'.
- Read-Only Username:** A text box containing 'Public'.
- Read/Write Username:** A text box containing 'Private'.
- Authentication Type:** A dropdown menu set to 'MD5'.
- Authentication Password:** Two empty text boxes for password input.
- Encryption Type:** A dropdown menu set to 'CBC-DES'.
- Encryption Password:** Two empty text boxes for password input.

'Apply' and 'Back' buttons are located at the bottom right of the configuration area.

Step 2 Configure the settings for the SNMP parameters.

Table 5-70

Parameter	Description
Enable	Enable the SNMP function.
Version	Select the check box of SNMP version(s) that you are using. The default version is V3 . There is a risk of select V1 or V2.
SNMP Port	Indicates the monitoring port on the agent program.
Read Community	Indicates the read/write strings supported by the agent program.
Write Community	
Trap Address	Indicates the destination address for the agent program to send the Trap information.
Trap Port	Indicates the destination port for the agent program to send the Trap information.
Read-Only Username	Enter the user name that is allowed to access the Device and has the "Read Only" permission.
Read/Write Username	Enter the user name that is allowed to access the Device and has the "Read and Write" permission.
Authentication Type	Includes MD5 and SHA. The system recognizes automatically.
Authentication Password	Enter the password for authentication type and encryption type. The password should be no less than eight characters.

Parameter	Description
Encryption Password	
Encryption Type	In the Encryption Type list, select an encryption type. The default setting is CBC-DES.

Step 3 Compile the two MIB files by MIB Builder.

Step 4 Run MG-SOFT MIB Browser to load in the module from compilation.

Step 5 On the MG-SOFT MIB Browser, enter the Device IP that you want to manage, and then select the version number to query.

Step 6 On the MG-SOFT MIB Browser, unfold the tree-structured directory to obtain the configurations of the Device, such as the channels quantity and software version.

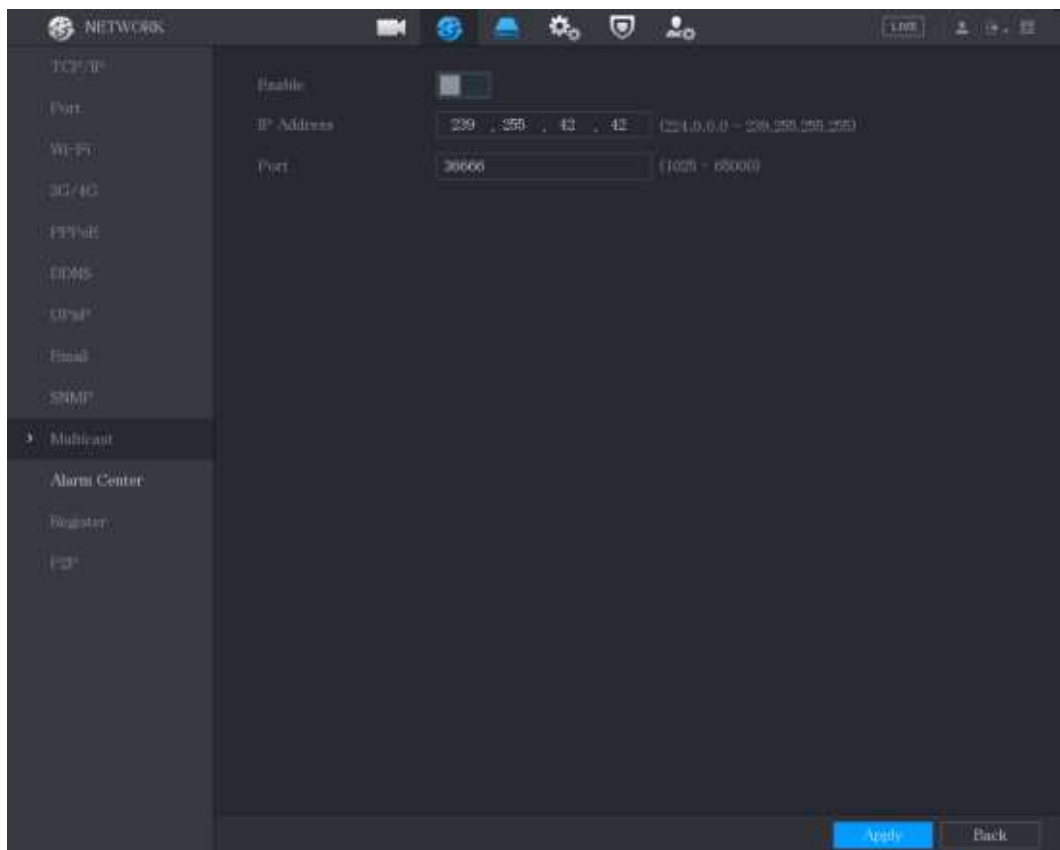
5.15.1.10 Configuring Multicast Settings

When you access the Device from the network to view the video, if the access is exceeded, the video will not display. You can use the multicast function to group the IP to solve the problem.

Step 1 Select **Main Menu > NETWORK > Multicast**.

The **Multicast** interface is displayed.

Figure 5-267



Step 2 Configure the settings for the multicast parameters.

Table 5-71

Parameter	Description
Enable	Enable the multicast function.

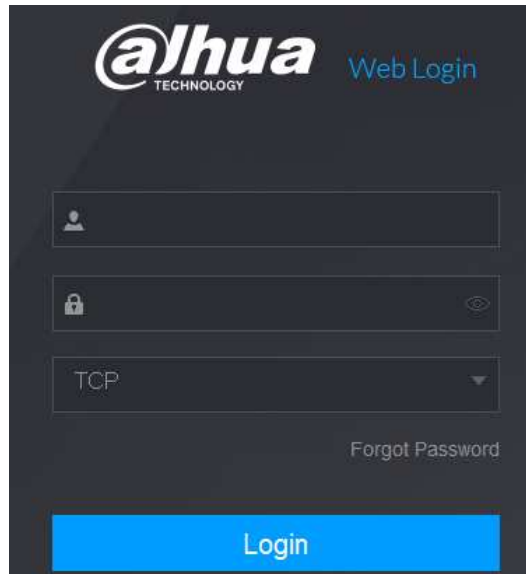
IP Address	Enter the IP address that you want to use as the multicast IP. The IP address ranges from 224.0.0.0 through 239.255.255.255.
Port	Enter the port for the multicast. The port ranges from 1025 through 65000.

Step 3 Click **Apply** to complete the settings.

You can use the multicast IP address to login the web.

On the web login dialog box, in the **Type** list, select **MULTICAST**. The web will automatically obtain the multicast IP address and join. Then you can view the video through multicast function.

Figure 5-268



5.15.1.11 Configuring Register Settings

You can register the Device into the specified proxy server which acts as the transit to make it easier for the client software to access the Device.

Step 1 Select **Main Menu > NETWORK > Register**.

The **Register** interface is displayed.

Figure 5-269

The screenshot shows the 'Register' configuration page within the 'NETWORK' settings. The sidebar on the left lists various network and system settings. The main configuration area contains the following fields:

- Enable:** A checkbox that is currently unchecked.
- No.:** A dropdown menu with the value '1' selected.
- Server Address:** A text input field containing '0.0.0.0'.
- Port:** A text input field containing '8000', with a range indicator '(1 ~ 65535)' to its right.
- Sub-Device ID:** A text input field containing '0'.

At the bottom right of the configuration area, there are two buttons: 'Apply' (highlighted in blue) and 'Back'.

Step 2 Configure the settings for the register parameters.

Table 5-72

Parameter	Description
Enable	Enable the register function.
No.	The default value is 1.
Server IP Address	Enter the server IP address or the server domain that you want to register to.
Port	Enter the port of the server.
Sub Service ID	This ID is allocated by the server and used for the Device.

Step 3 Click **Apply** to complete the settings.

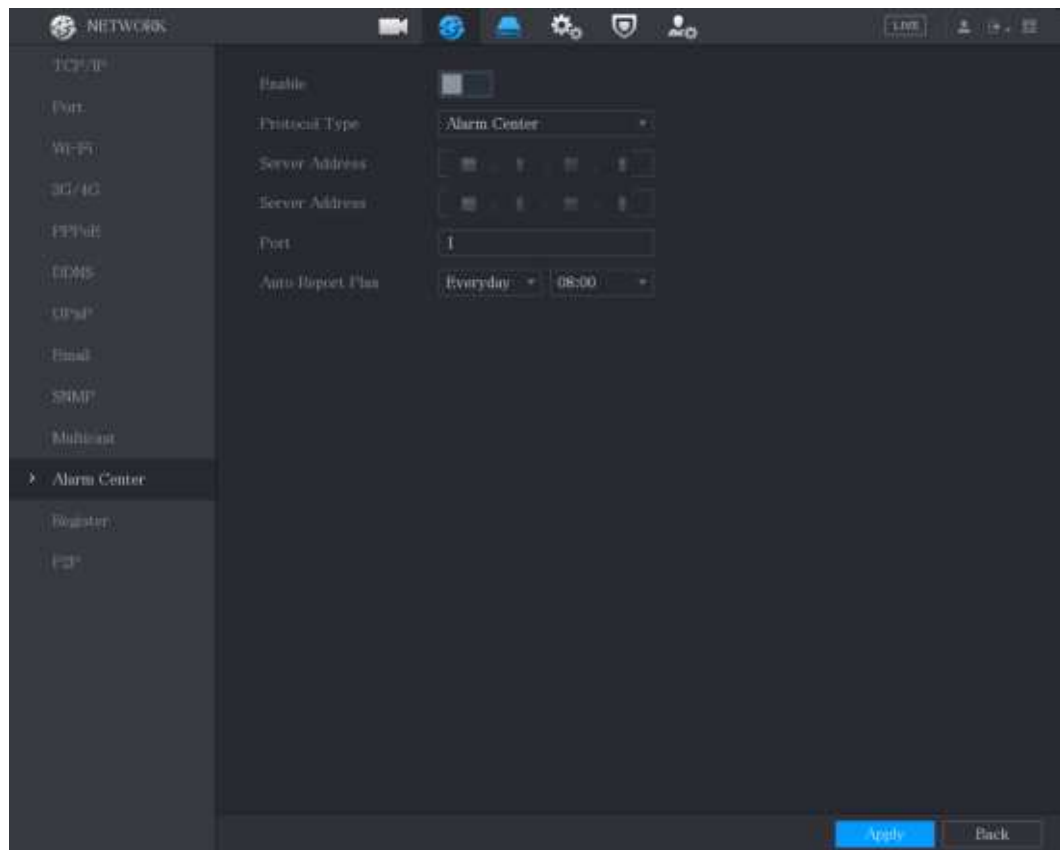
5.15.1.12 Configuring Alarm Center Settings

You can configure the alarm center server to receive the uploaded alarm information. To use this function, the **Report Alarm** check box must be selected. For details about alarm event settings, see "5.10 Alarm Events Settings."

Step 1 Select **Main Menu > NETWORK > Alarm Center**.

The **Alarm Center** interface is displayed.

Figure 5-270



Step 2 Configure the settings for the alarm center parameters.

Table 5-73

Parameter	Description
Enable	Enable the alarm center function.
Protocol Type	In the Protocol Type list, select protocol type. The default is ALARM CENTER .
Server Address	The IP address and communication port of the PC installed with alarm client.
Port	
Auto Report Plan	In the Auto Report Plan list, select time cycle and specific time for uploading alarm.

Step 3 Click **Apply** to complete the settings.

5.15.1.13 Configuring P2P Settings

You can manage the devices by using P2P technology to download the application and register the devices. For details, see "5.1.4.5 Configuring P2P Settings."

5.15.2 Configuring Network Testing Settings

5.15.2.1 Testing the Network

You can test the network connection status between the Device and other devices.

Step 1 Select **Main Menu > MAINTAIN > Network > Test**.
The **Network Test** interface is displayed.

Figure 5-271

Name	IP	Packet Sniffer Size	Packet Sniffer Backup
LAN1	192.168.1.100	0KB	

Step 2 In the **Destination IP** box, enter the IP address.

Step 3 Click **Test**.

After testing is completed, the test result is displayed. You can check the evaluation for average delay, packet loss, and network status.

Figure 5-272

Online User Network Load **Test**

Network Test

Destination IP:

Test Result: Average Delay: 1.0ms Packet Loss Rate: 0%
Network Status: OK

Packet Sniffer Backup

Device Name:

Address:

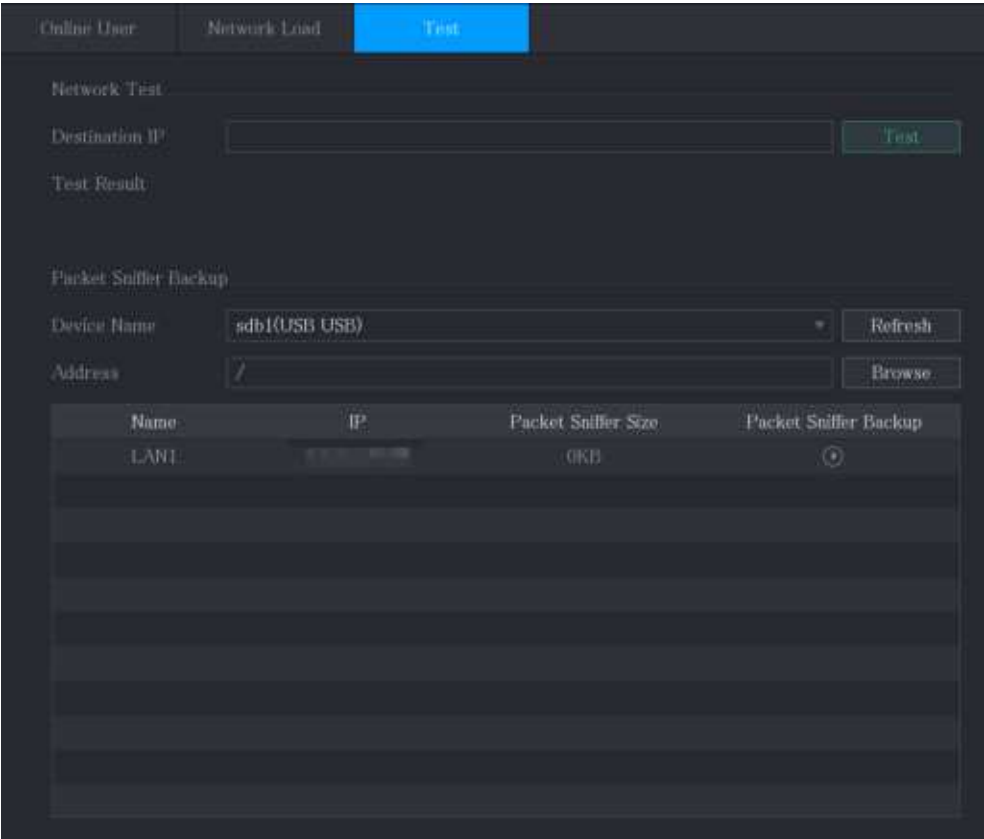
Name	IP	Packet Sniffer Size	Packet Sniffer Backup
LAN1	192.168.1.1	0KB	Refresh

5.15.2.2 Capturing Packet and Backing up

Packet capture means the operations such as capturing, resending, and editing data that are sent and received during network transmission. When there is network abnormality, you can perform packet capturing and back up into the USB storage device. This date can be provided to the technical support for analyzing the network condition.

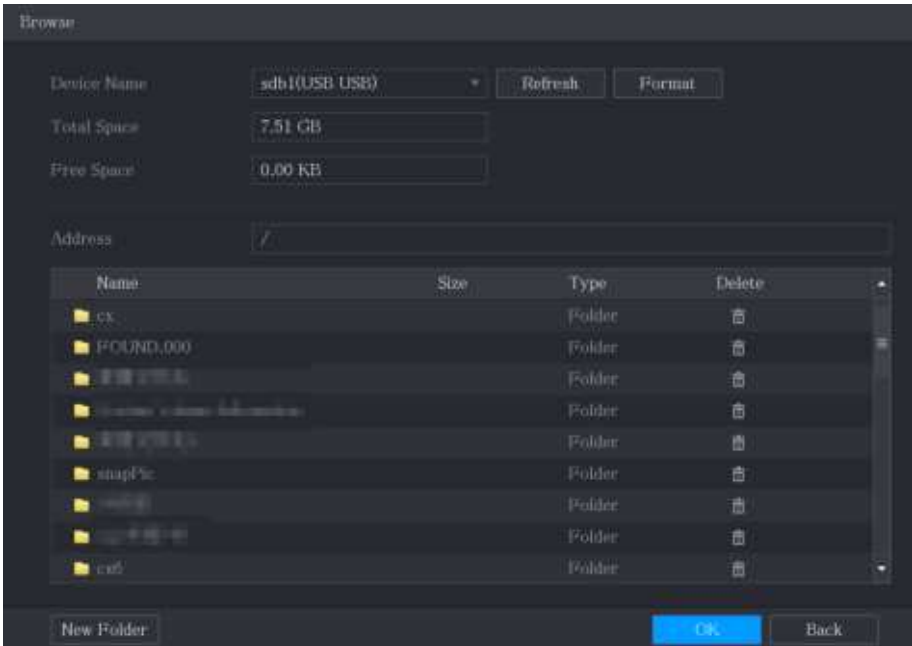
- Step 1 Select **Main Menu > MAINTAIN > Network > Test**.
The **Test** interface is displayed.

Figure 5-273



- Step 2 Connect a USB storage device to the Device.
- Step 3 Click **Refresh**.
The Device starts detecting the USB storage device and displays its name in the **Device Name** box.
- Step 4 Select the route of the data that you want to capture and back up.
- 1) In the **Packet Sniffer Backup** area, click **Browse**.
The **Browse** interface is displayed.

Figure 5-274



2) Select the route.



- If there are several USB storage devices are connected to the Device, you can select from the **Device Name** list.
- Click Refresh to total space, free space and the file list in the selected USB storage device.
- In the case of insufficient capacity, click  to delete the needless files.
- Click **New Folder** to create a new folder in the USB storage device.

3) Click **OK** to save the route selection settings.

The **Test** interface is displayed again.

Step 5 Click  to start packet capturing and backing up.

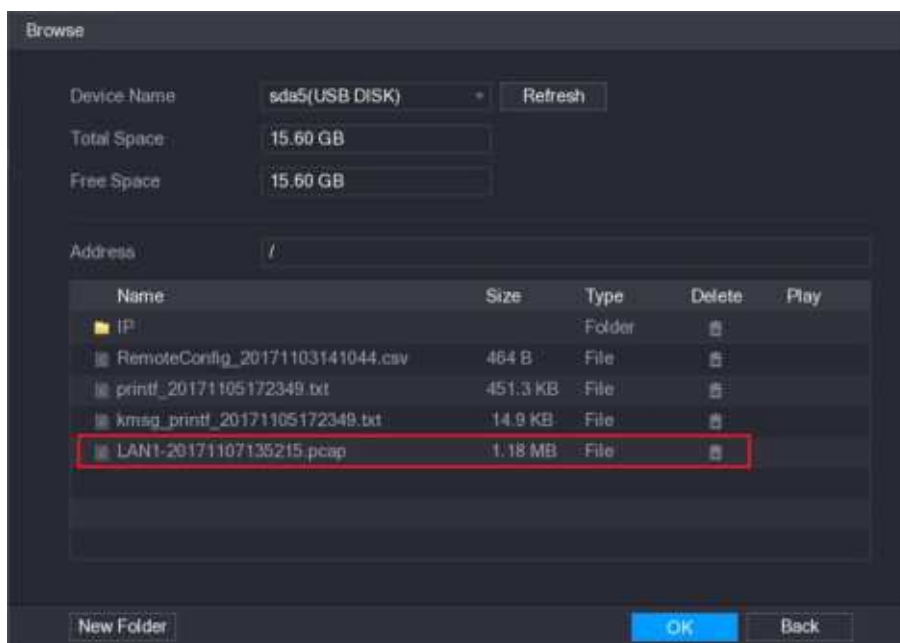


- Only the data packet of one LAN can be captured at one time.
- After capturing starts, you can exit the **Test** interface to perform other operations such as web login and monitoring.

Step 6 Click  to stop capturing.

The backup data is saved in the selected route under the naming style "LAN name-time.pcap." You can open it by using Wireshark software.

Figure 5-275



5.16 Configuring Account Settings

You can add, modify and delete user accounts, groups, and ONVIF users, and set security questions for admin account.



- The user name supports 31 characters and group name supports 15 characters. The user name can be consisted of letter, number, "_", "@", ".".

- You can set maximum 64 users and 20 groups. The group name by "User" and "Admin" cannot be deleted. You can set other groups and define the relevant permissions. However, the admin account cannot be set randomly.
- You can manage the account by user and group and the name cannot be repeated. Every user must belong to a group, and one user only belongs to one group.

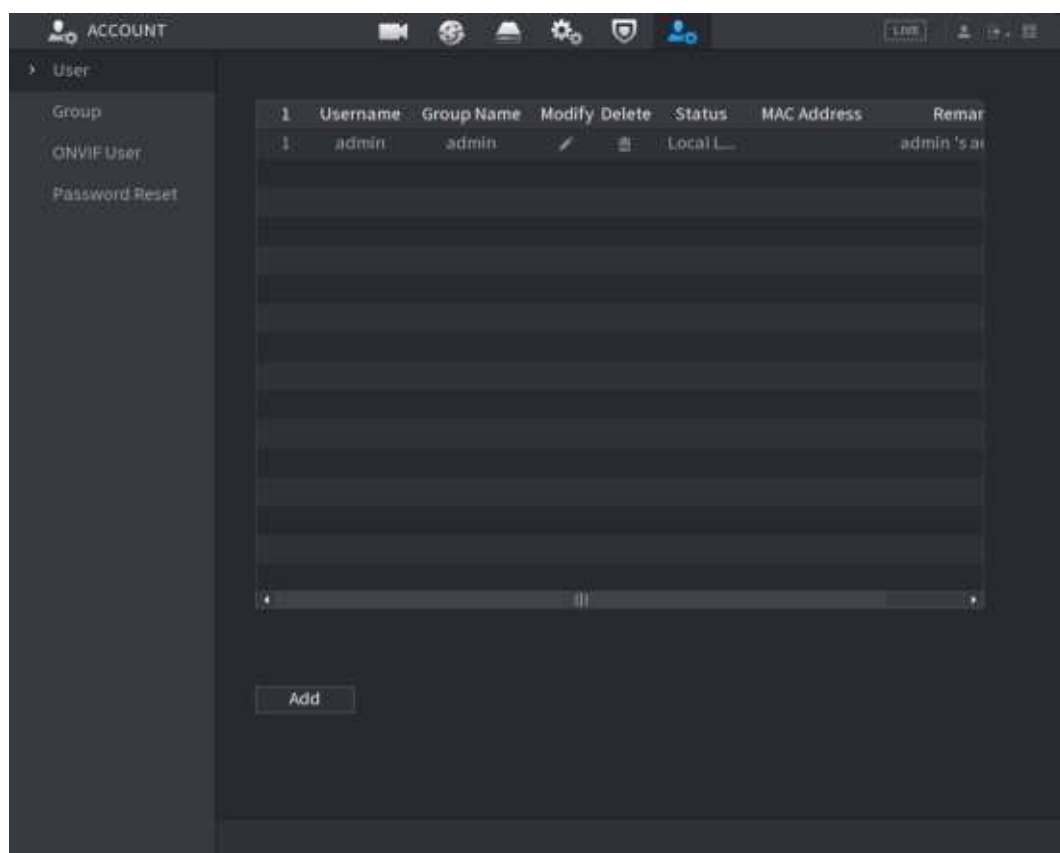
5.16.1 Configuring User Account

5.16.1.1 Adding a User Account

Step 1 Select **Main Menu > ACCOUNT > User**.

The **User** interface is displayed.

Figure 5-276



Step 2 Click **Add**.

The **Add** interface is displayed.

Figure 5-277

Step 3 Configure the settings for the parameters of adding a user account.

Table 5-74

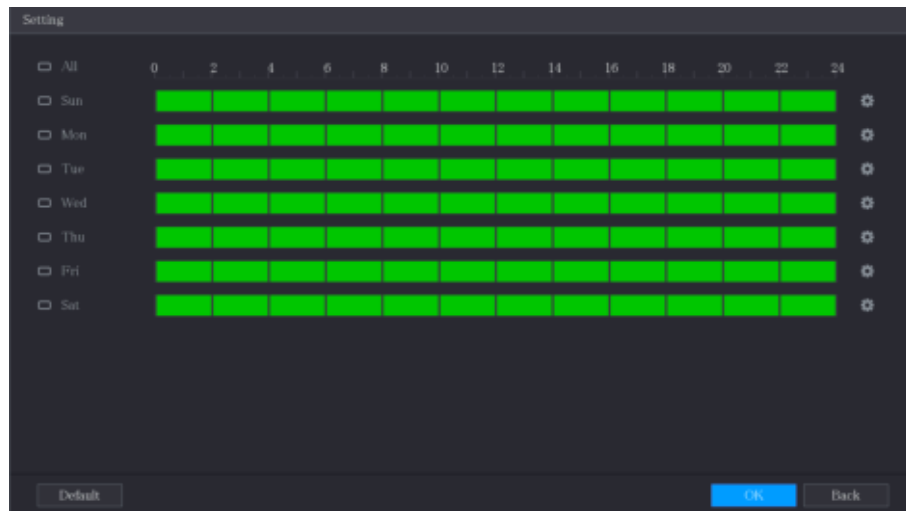
Parameter	Description
Username	Enter a user name and password for the account.
Password	
Confirm Password	Re-enter the password.
Remarks	Optional. Enter a description of the account.
User MAC	Enter user MAC address
Group	Select a group for the account. The user rights must be within the group permission.
Period	Click Setting to display Setting interface. Define a period during which the new account can login the device. The new account cannot login the device during the time beyond the set period.
Permission	In the Permission area, select the check boxes in the System tab, Playback tab, and Monitor tab. To manage the user account easily, when defining the user account authority, it is recommended not to give the authority to the common user account higher than the advanced user account.

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

Setting Permitted Period

Step 1 Next to **Period**, click **Setting**.
The **Set** interface is displayed.

Figure 5-278



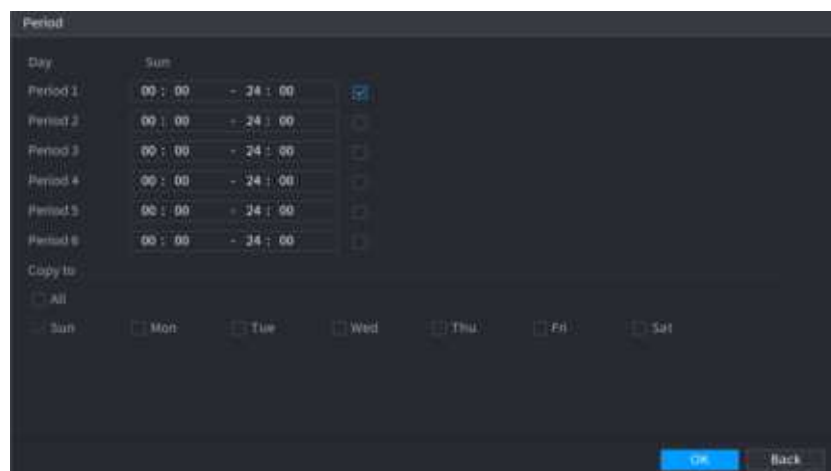
Step 2 Define the permitted period. By default, it is active all the time.

- Define the period by drawing.
 - ◇ Define for a specified day of a week: On the timeline, click the half-hour blocks to select the active period.
 - ◇ Define for several days of a week: Click  before each day, the icon switches to . On the timeline of any selected day, click the half-hour blocks to select the active periods, all the days with  will take the same settings.
 - ◇ Define for all days of a week: Click **All**, all the  switches to . On the timeline of any day, click the half-hour blocks to select the active periods, all the days will take the same settings.
- Define the period by editing. Take Sunday as an example.

- 1) Click .

The **Period** interface is displayed.

Figure 5-279



- 2) Enter the time frame for the period and select the check box to enable the settings.
 - ◇ There are six periods for you to set for each day.

- ◇ Under **Copy**, select **All** to apply the settings to all the days of a week, or select specific day(s) that you want to apply the settings to.

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

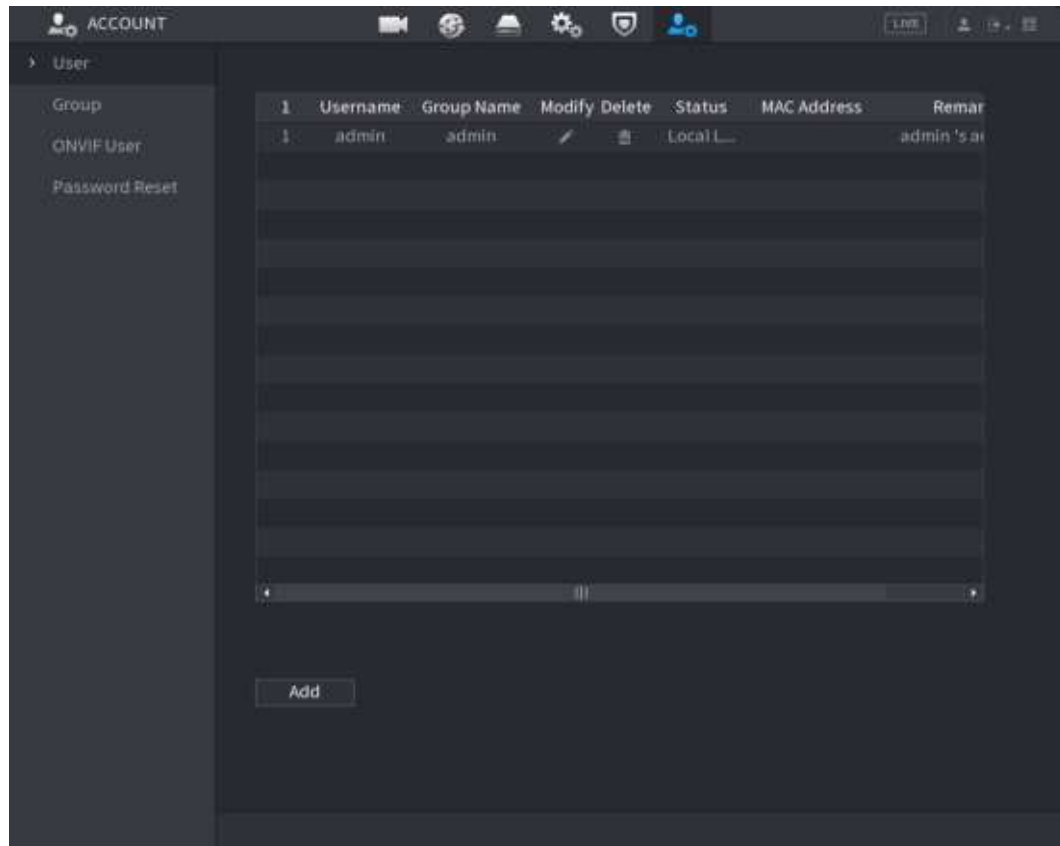
Step 3 Click **OK**.

5.16.1.2 Modify a User Account

Step 1 Select **Main Menu > ACCOUNT > User**.

The **User** interface is displayed.

Figure 5-280



Step 2 Click  for the user account that you want to modify.

The **Modify** interface is displayed.

Figure 5-281

The screenshot shows a 'Modify' window for a user account. The 'Username' field is set to 'admin'. The 'Modify Password' section has a toggle switch. There are input fields for 'Old Password', 'New Password', 'Confirm Password', and 'Password Hint'. The 'User MAC' field is empty. The 'Group' field is set to 'admin'. The 'Remarks' field contains 'Login to system'. The 'Unlock Pattern' toggle is turned on, and there is a small icon next to it. Below the input fields are three buttons: 'System', 'Search', and 'Live'. Underneath these buttons is a grid of checkboxes for permissions: 'All', 'ACCOUNT', 'STORAGE', 'SECURITY', 'SYSTEM', 'EVENT', 'BACKUP', 'SYSTEM INFO', 'NETWORK', 'MAINTENANCE', 'MANUAL CONTROL', and 'CAMERA'. All these checkboxes are checked. At the bottom right are 'OK' and 'Back' buttons.

Step 3 Change the settings for password, user name, user group, user MAC, memo, period, and authority.



The new password can be set from 8 digits through 32 digits and contains at least two types from number, letter and special characters (excluding "", "", "", ".", "." and "&").

For the admin account, you enable/disable the unlock pattern and modify password hint.

- To use the unlock pattern, enable **Unlock Pattern**, click , draw a pattern in the **Unlock Pattern** interface, and then click **Save** to save the setting.
- Enter password hint text in **Password Hint** box.

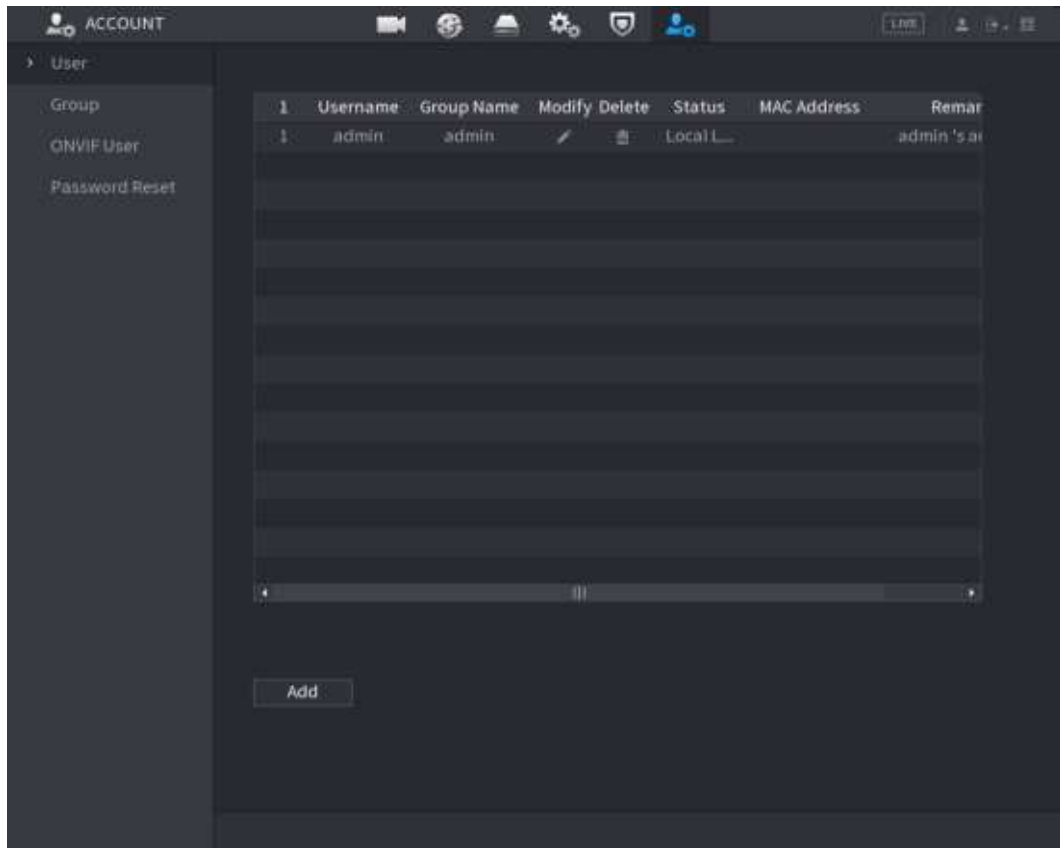
Step 4 Click **OK** to complete the settings.

5.16.1.3 Deleting a User Account

Step 1 Select **Main Menu > ACCOUNT > User**.

The **User** interface is displayed.

Figure 5-282



Step 2 Click  for the user account that you want to delete.

A **Message** is displayed.

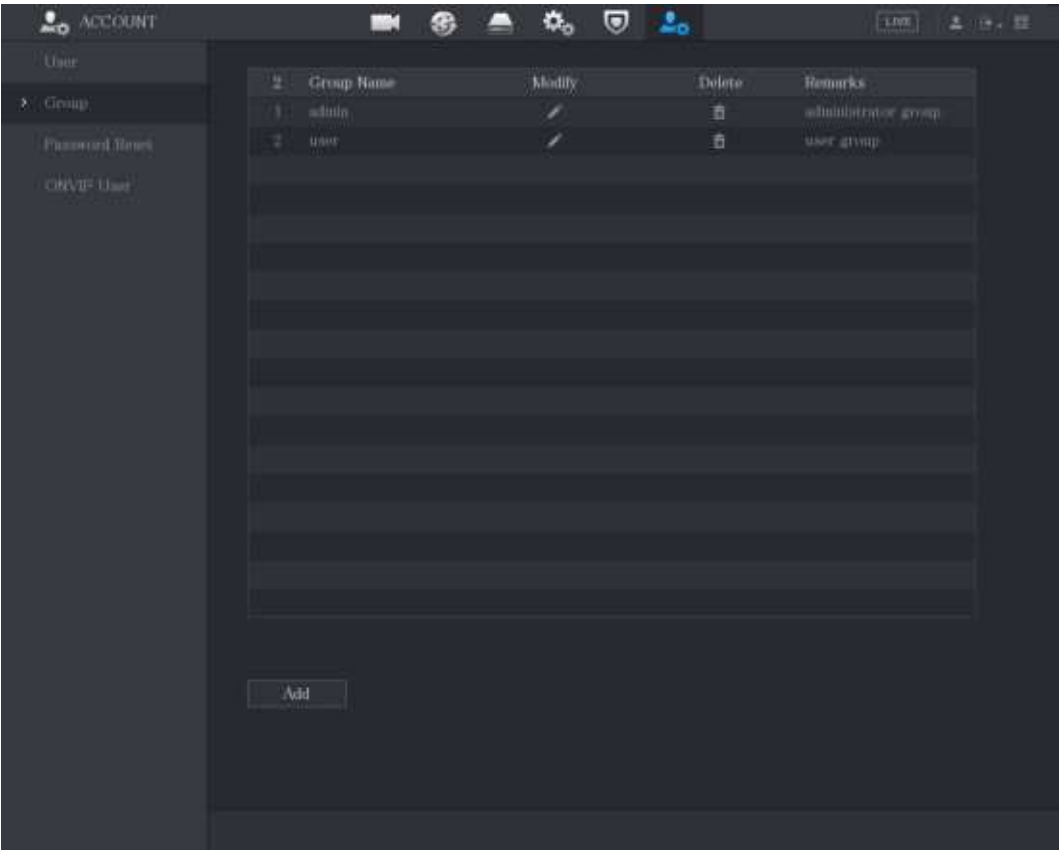
Step 3 Click **OK** to delete a user account.

5.16.2 Configuring Group Account

5.16.2.1 Adding a Group

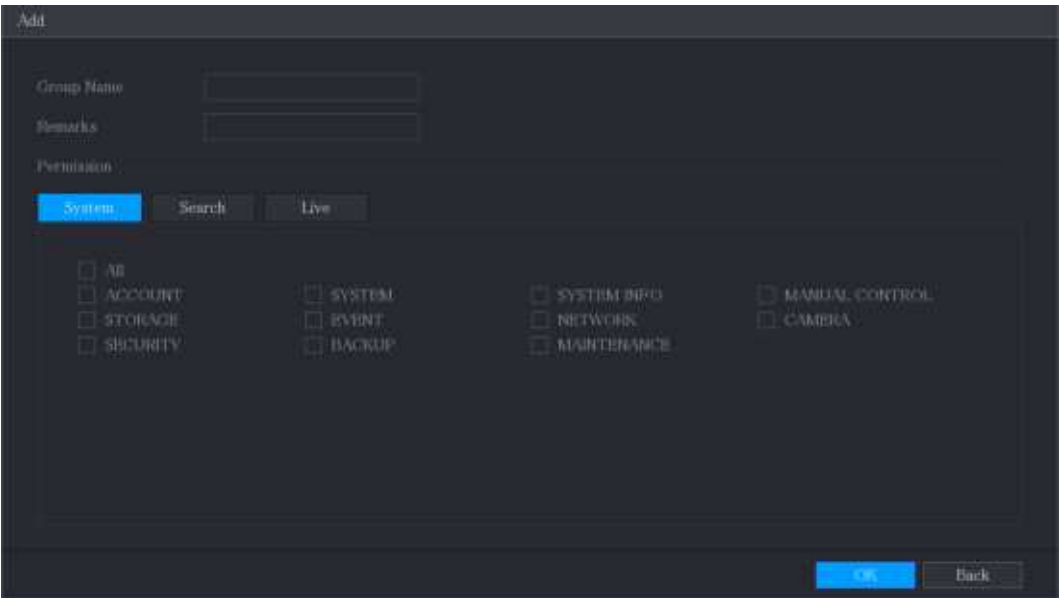
Step 1 Select **Main Menu > ACCOUNT > Group**.
The **GROUP** interface is displayed.

Figure 5-283



Step 2 Click **Add**.
The **Add** interface is displayed.

Figure 5-284



Step 3 Configure the settings for the parameters of adding a group.

Table 5-75

Parameter	Description
Group Name	Enter a name for the group.

Parameter	Description
Remarks	Optional. Enter a description of the account.
Permission	In the Permission area, select the check boxes in the System tab, Playback tab, and Monitor tab.

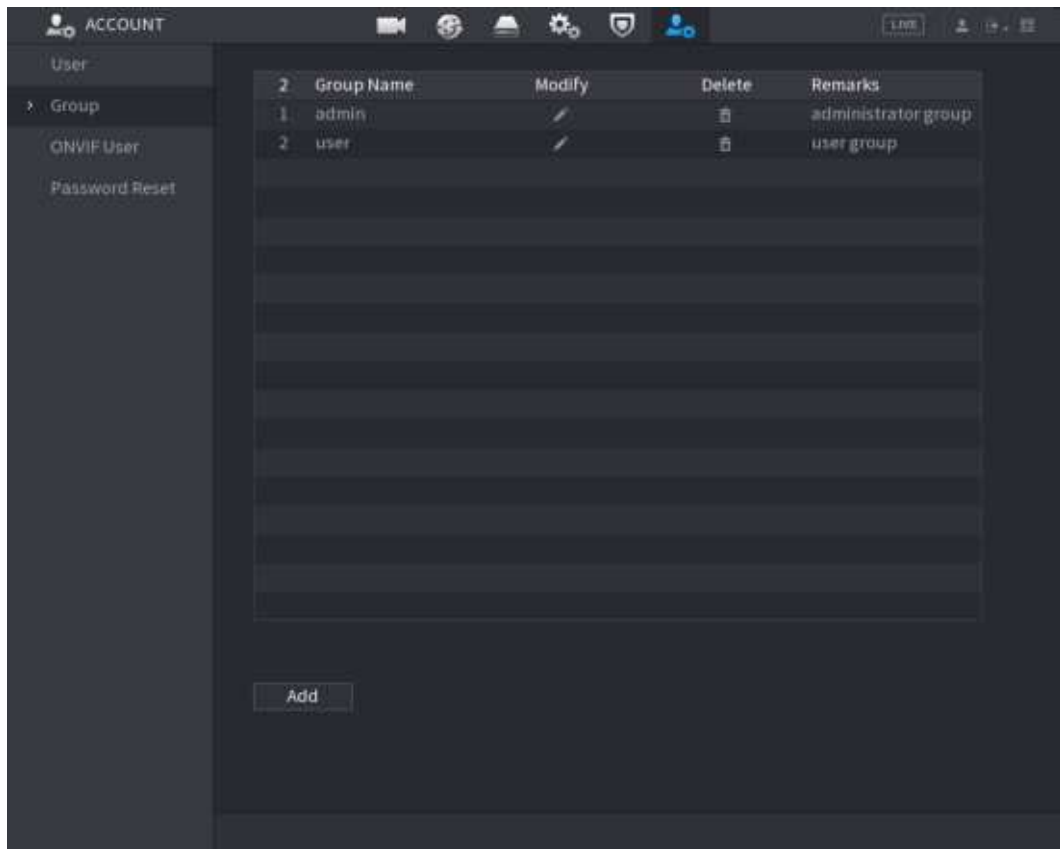
Step 4 Click **OK** to complete the settings.

5.16.2.2 Modifying a Group

Step 1 Select **Main Menu > ACCOUNT > Group**.

The **Group** interface is displayed.

Figure 5-285



Step 2 Click  for the group account that you want to modify.

Step 3 The **Modify** interface is displayed.

Figure 5-286

Modify

Group

user

Group Name

user

Remarks

user group

Permission

System

Search

Live

☐ All
 ☐ ACCOUNT
 ☐ STORAGE
 ☐ SECURITY

☐ SYSTEM
 ☐ EVENT
 ☐ BACKUP

☐ SYSTEM INFO
 ☐ NETWORK
 ☐ MAINTENANCE

☒ MANUAL CONTROL
 ☐ CAMERA

OK

Back

Step 4 Change the settings for group name, memo, and authority.

Step 5 Click **OK** to complete the settings.

5.16.2.3 Deleting a Group

Step 1 Select **Main Menu > ACCOUNT > Group**.

The **Group** interface is displayed.

Figure 5-287

ACCOUNT

User

Group

ONVIF User

Password Reset

2

Group Name

Modify

Delete

Remarks

1

admin

administrator group

2

user

user group

Add

Step 2 Click  for the user account that you want to delete.

A **Message** is displayed.

Step 3 Click **OK** to delete a group.

5.16.3 Configuring ONVIF Users

The device manufactured by other company can connect to the Device through ONVIF protocol by an authorized ONVIF account.

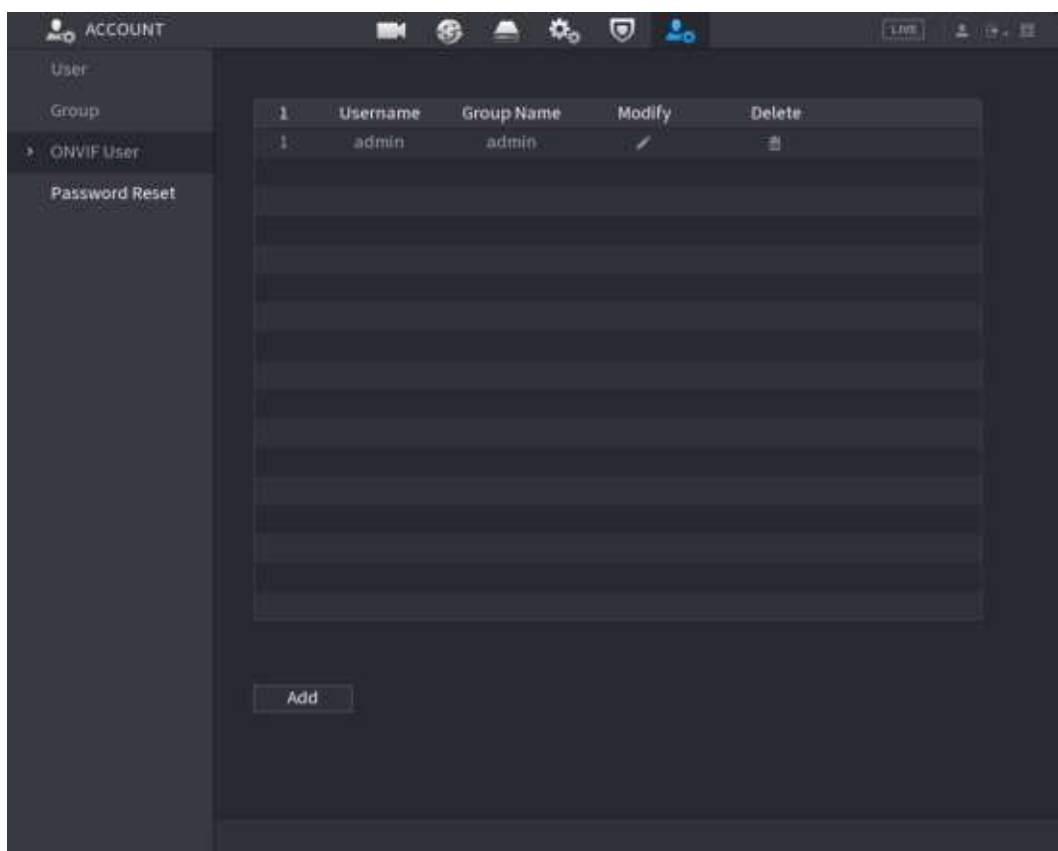


The admin account is created for ONVIF users right after the Device has been initialized

Step 1 Select **Main Menu > ACCOUNT > ONVIF User**.

The **ONVIF User** interface is displayed.

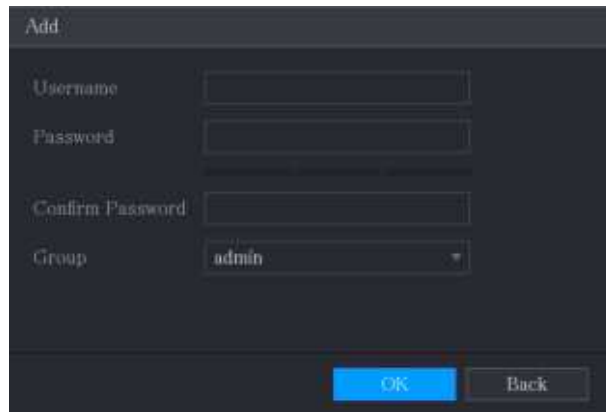
Figure 5-288



Step 2 Click **Add**.

The **Add** interface is displayed. See Figure 5-289.

Figure 5-289



Step 3 Enter user name, password, and select the group that you want this account to belong to.

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



Click  to modify the account; Click  to delete the account.

5.17 Audio Management

Audio management function manages audio files and configures the playing schedule. When there is an alarm event, the audio file can be activated.

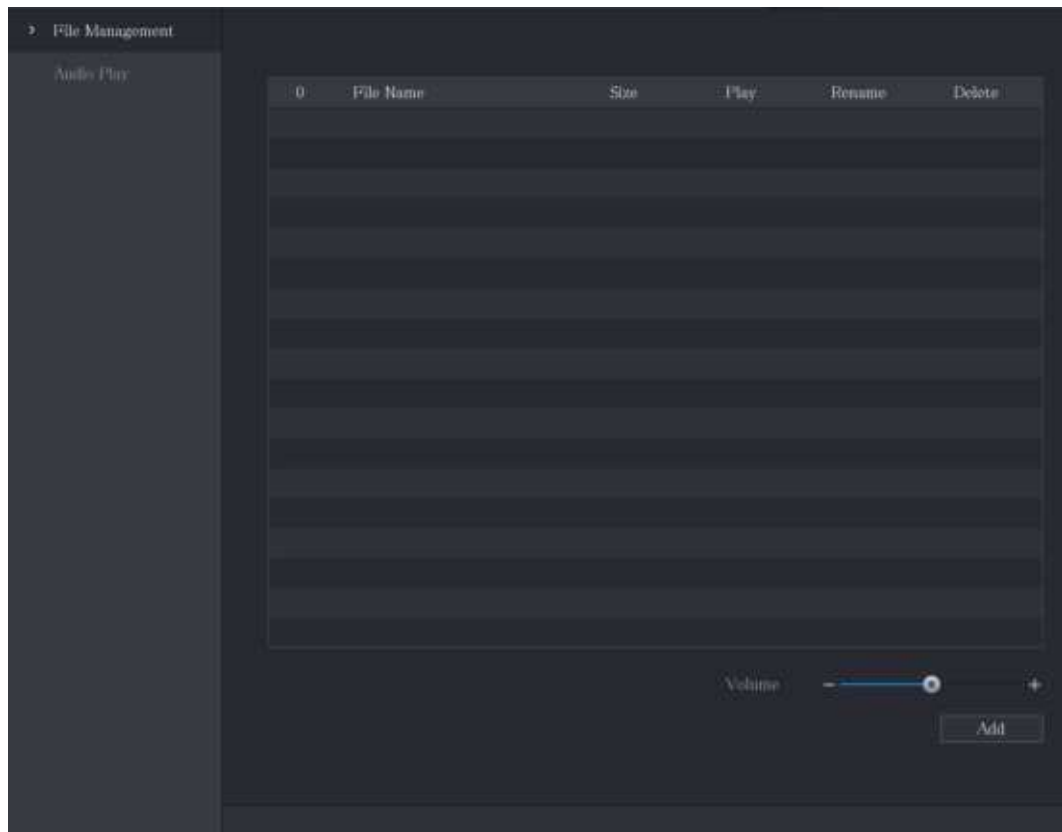
5.17.1 Configuring Audio Files

You can add audio files, listen to audio files, rename and delete audio files, and configure the audio volume.

Step 1 Select **Main Menu > AUDIO > File Management**.

The **File Management** interface is displayed.

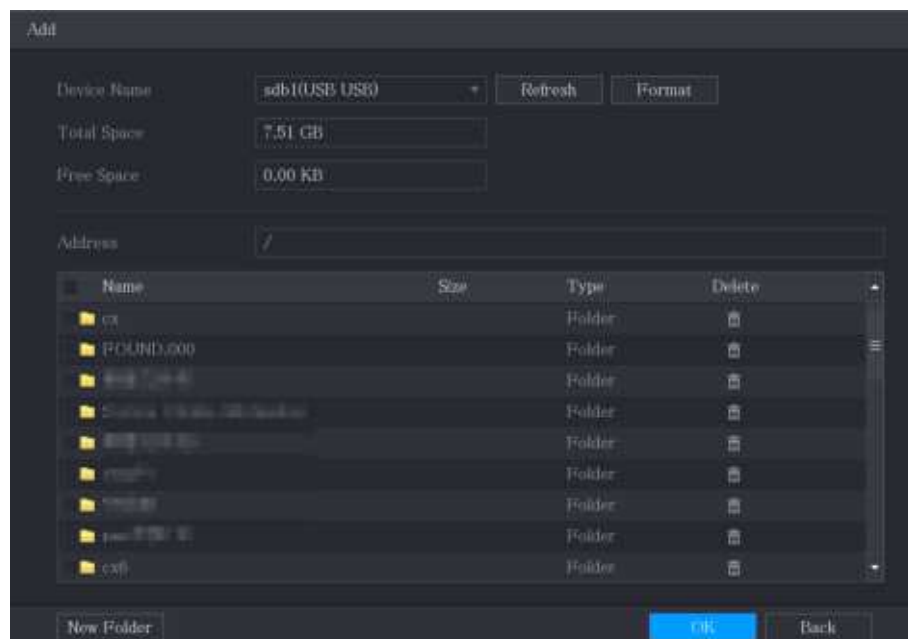
Figure 5-290



Step 2 Click **Add**.

The **Add** interface is displayed.

Figure 5-291

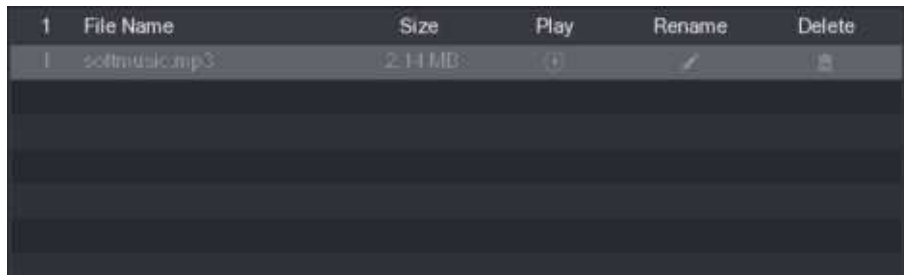


Step 3 Select the audio files that you want to import.

Step 4 Click **OK** to start importing audio files from the USB storage device.

If the importing is successful, the audio files will display in the **File Management** interface.

Figure 5-292



The imported audio files are automatically saved into the HDD, so you do not need to connect to the USB storage device to get the file next time.

- Click  to play the audio file.
- Click  to rename the audio file.
- Click  to delete the audio file.
- To decrease or increase the playing volume, move the slider to the left or to the right.

5.17.2 Configuring Playing Schedule for Audio Files

You can configure the settings to play the audio files during the defined time period.

Step 1 Select **Main Menu > AUDIO > Audio Play**.

The **Audio Play** interface is displayed.

Figure 5-293



Step 2 Configure the settings for the schedule parameters.

Table 5-76

Parameter	Description
Period	In the Period box, enter the time. Select the check box to enable the settings. You can configure up to six periods.
File Name	In the File Name list, select the audio file that you want to play for this configured period.

Interval	In the Interval box, enter the time in minutes for how often you want to repeat the playing.
Repeat	Configure how many times you want to repeat the playing in the defined period.
Output Port	Includes two options: MIC and Audio. It is MIC by default. The MIC function shares the same port with talkback function and the latter has the priority.



- The finish time for audio playing is decided by audio file size and the configured interval.
- Playing priority: Alarm event > Talkback > Trial listening > Audio file.

Step 3 Click **Apply** to complete the settings.

5.18 Storage Management

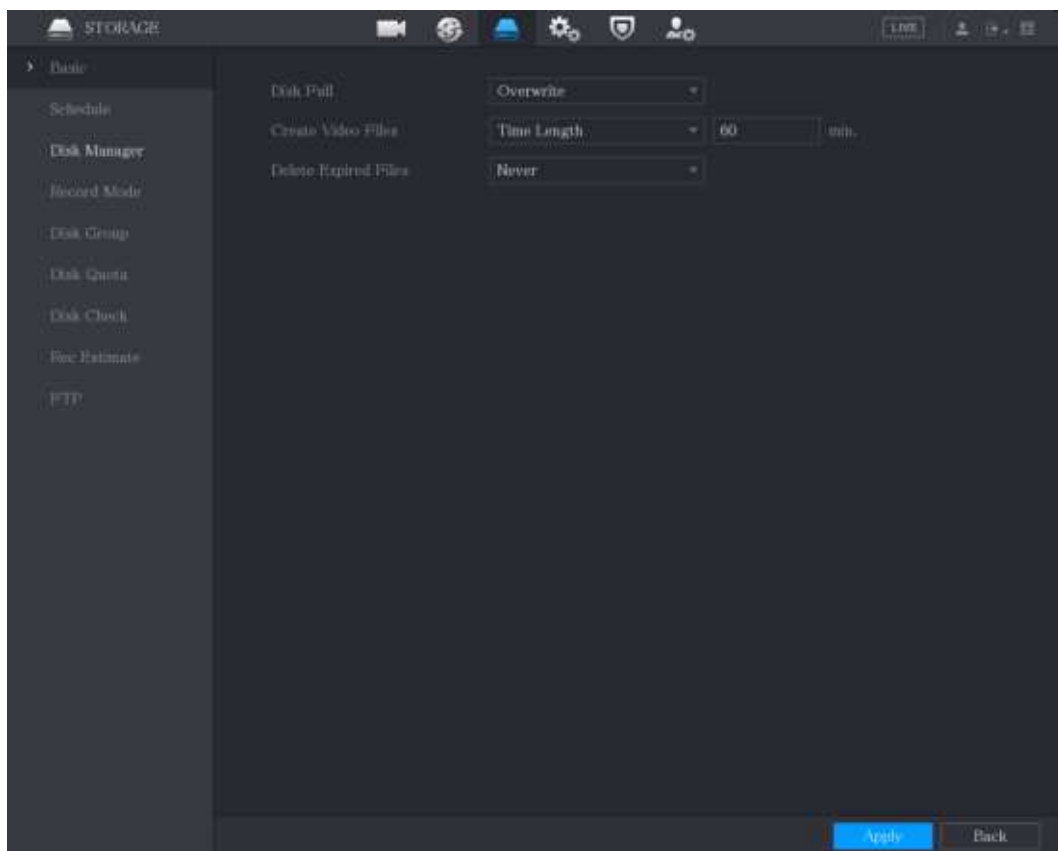
Storage management function manages the stored resources such as recorded video files and storage space. The function aims at providing easier operation and improving the storage efficiency.

5.18.1 Configuring Basic Settings

Step 1 Select **Main Menu > STORAGE > Basic**.

The **Basic** interface is displayed.

Figure 5-294



Step 2 Configure the settings for the basic settings parameters.

Table 5-77

Parameter	Description
Disk Full	Configure the settings for the situation all the read/write discs are full. • Select Stop to stop recording • Select Overwrite to overwrite the recorded video files always from the earliest time.
Create Video Files	Configure the time length and file length for each recorded video.
Delete Expired Files	Configure whether to delete the old files and if yes, configure the days.

Step 3 Click **Apply** to complete the settings.

5.18.2 Configuring the Recording and Snapshot Schedule

The system starts recording and taking snapshot according to the configured schedule. For details, see "5.1.4.9 Configuring Recorded Video Storage Schedule" and "5.1.4.10 Configuring Snapshot Storage Schedule."

5.18.3 Configuring Disk Manager

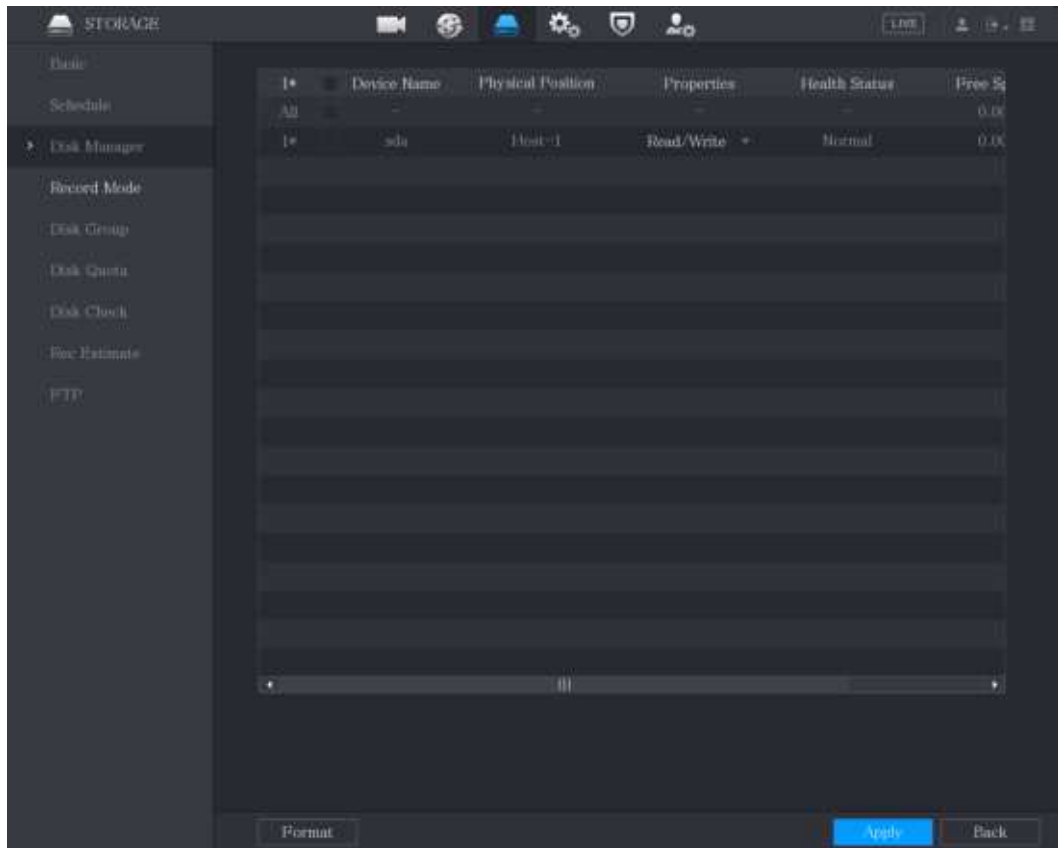
You can view the HDD information, format HDD, and configure the HDD type through HDD manager.

Step 1 Select **Main Menu > STORAGE > Disk Manager**.

The **Disk Manager** interface is displayed.

In the table, you can view the information of current HDD, such as device name, HDD type, status, total space and free space, and serial number of the HDD port.

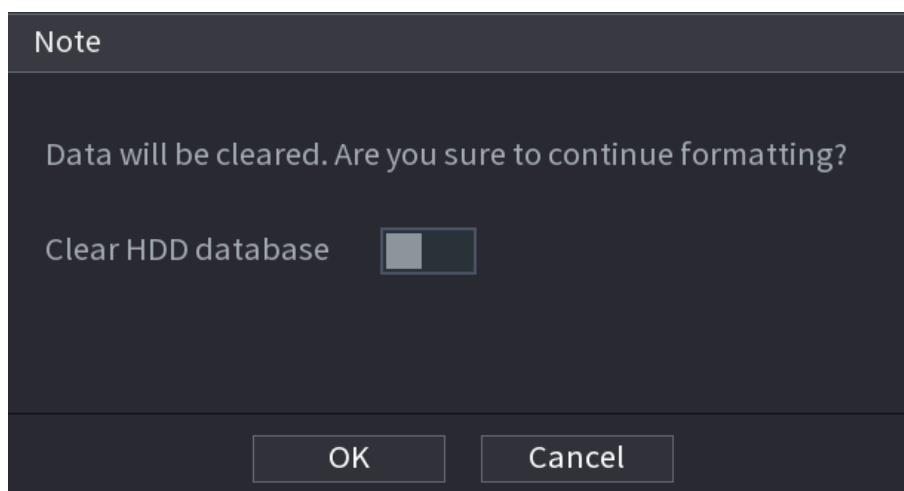
Figure 5-295



Step 2 Configuring the settings for the HDD manager.

- HDD type setting: In the **Properties** list, select **Read/Write**, **Read Only**, and then click **Apply** to save the settings.
- HDD format: Select the HDD that you want to format, click **Format**, and enable **Clear HDD database** in the pop-up message, click **OK** and enter the password of admin user in the prompted dialog box, click **OK** and then following the on-screen instructions to complete formatting.
- Formatting HDD will erase all data on the disk, proceed with caution.

Figure 5-296



5.18.4 Configuring Record

Record type includes auto and manual record. You can configure record type of main stream and sub stream. See "5.7 Configuring Record Settings".

5.18.5 Configuring Advance Settings

Create HDD group, and save main stream, sub stream and snapshot of designated channels to the HDD group.

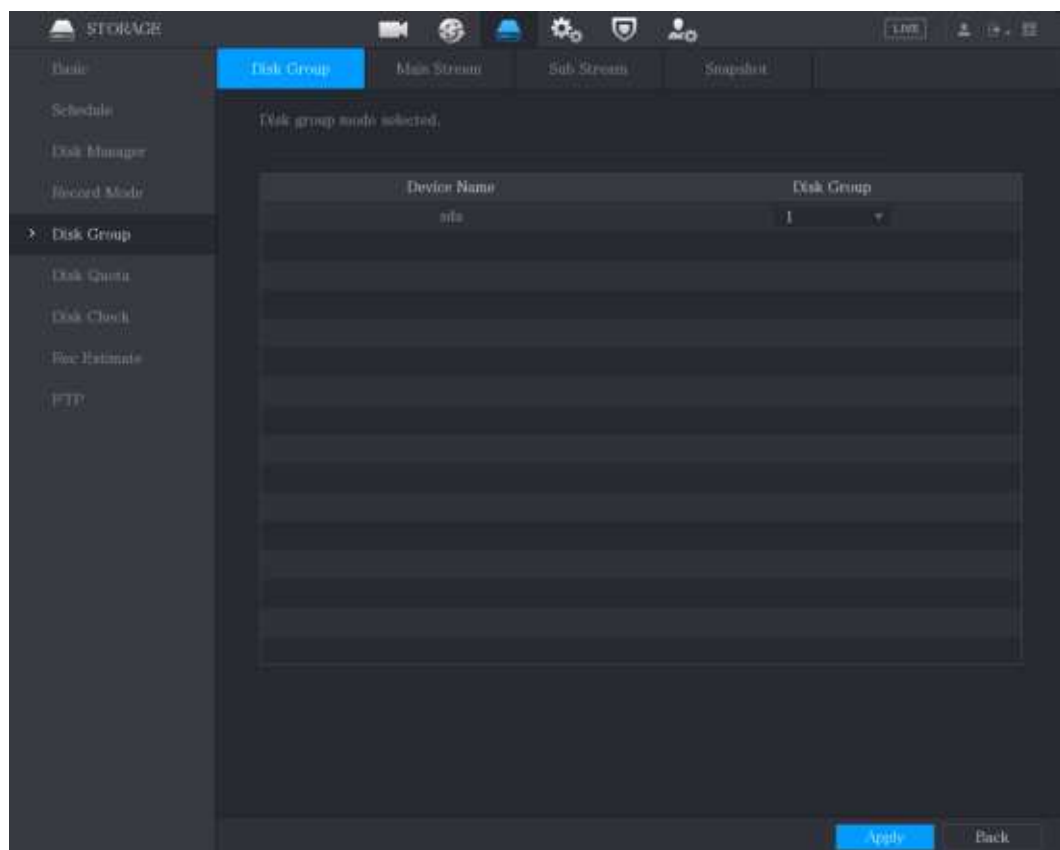


- If the interface displays that "Current HDD Mode is Quota Group", click "Change to HDD Group Mode", and then configure HDD group.
- You can enable either HDD Group Mode or Quota Group. The system prompts to reboot the device each time when you switch the mode.

Step 1 Select **Main Menu > STORAGE > Disk Group > Disk Group.**

The **Disk Group** interface is displayed.

Figure 5-297



Step 2 Select group for each HDD, and then click **Apply** to complete the settings.

Step 3 After configuring HDD group, click **Main Stream**, **Sub Stream** and **Snapshot** tabs respectively, to configure the saving of main stream, sub stream and snapshot information of different channels to different HDD groups.

Figure 5-298

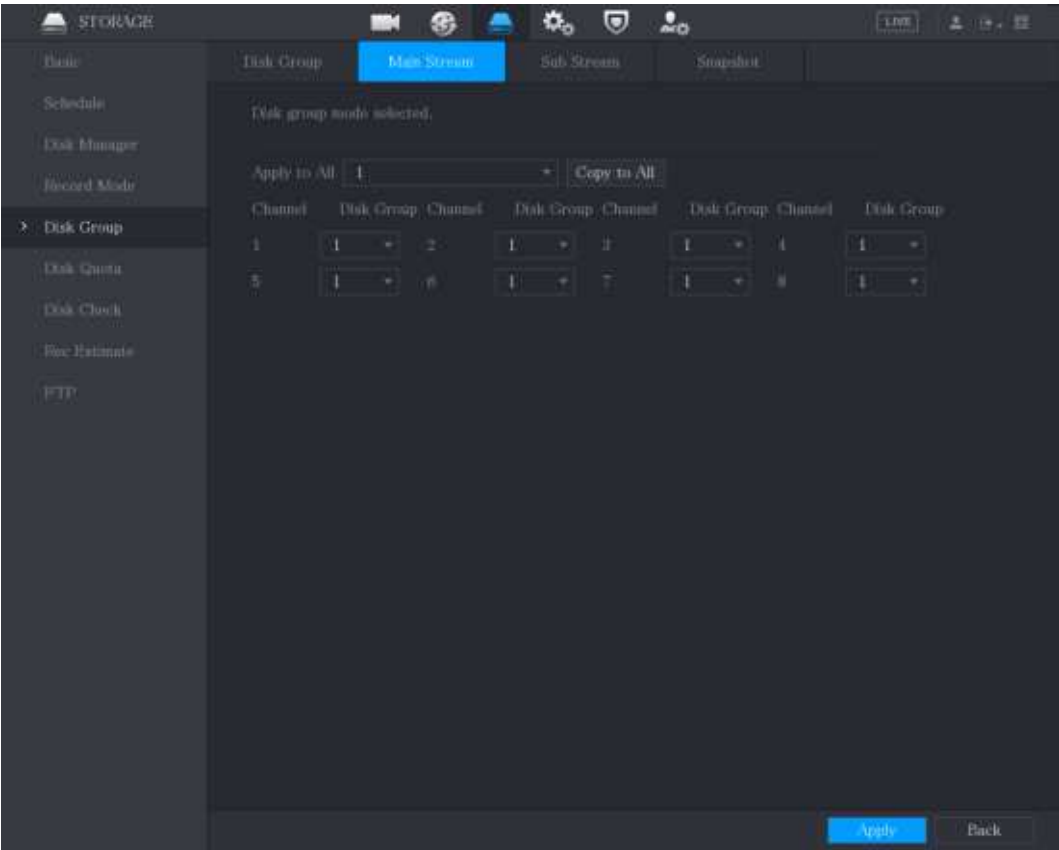


Figure 5-299

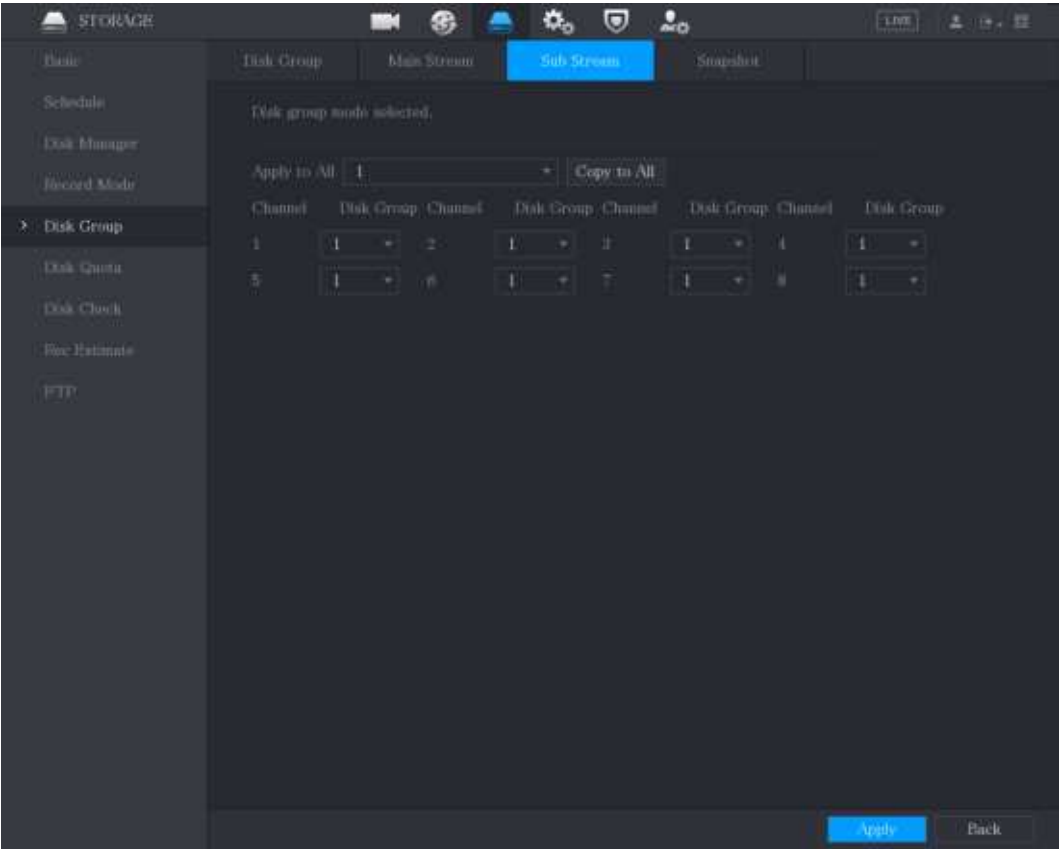
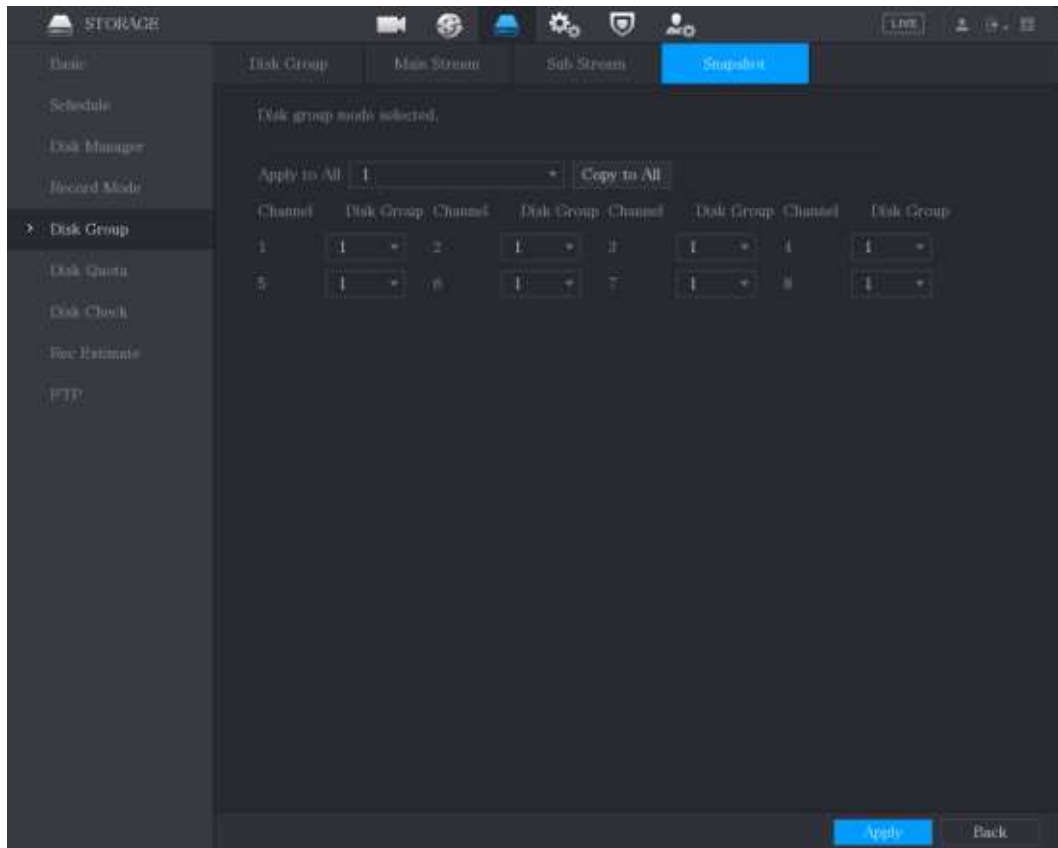


Figure 5-300



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

5.18.6 Configuring Disk Quota

By configuring quota, allocate fixed storage capacity to each channel, and distribute the storage space of each channel reasonably.

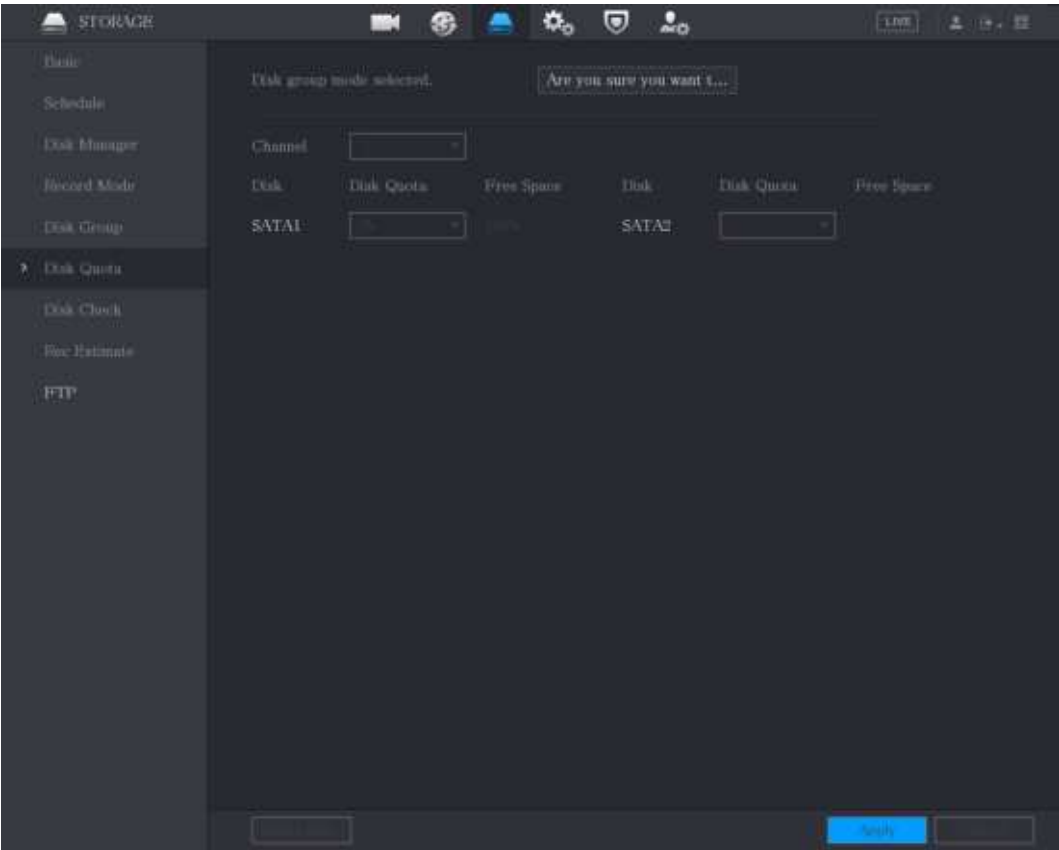


- If the interface displays that "Current HDD Mode is HDD Group", click "Change to Quota Mode", and then configure quota.
- You can enable either HDD Group Mode or Quota Group. The system prompts to reboot the device each time when you switch the mode.

Step 1 Select **Main Menu > STORAGE > Disk Quota**.

The **Disk Quota** interface is displayed.

Figure 5-301



Step 2 Select the channels you want to configure, and select quota from the drop-down list of corresponding HDD.

Step 3 Click **Apply** to complete the settings.



Click **Quota Statistics** to view the quota of each channel in HDD. See Figure 5-302.

Figure 5-302

Quota Statistics		
1	Channel	Disk Quota
1	Other	2.72 TB

5.18.7 Configuring HDD Detecting Settings



Not all models support this function.

HDD detecting function detects the current status of HDD to let you know the HDD performance and replace the defective HDD.

5.18.7.1 Checking HDD

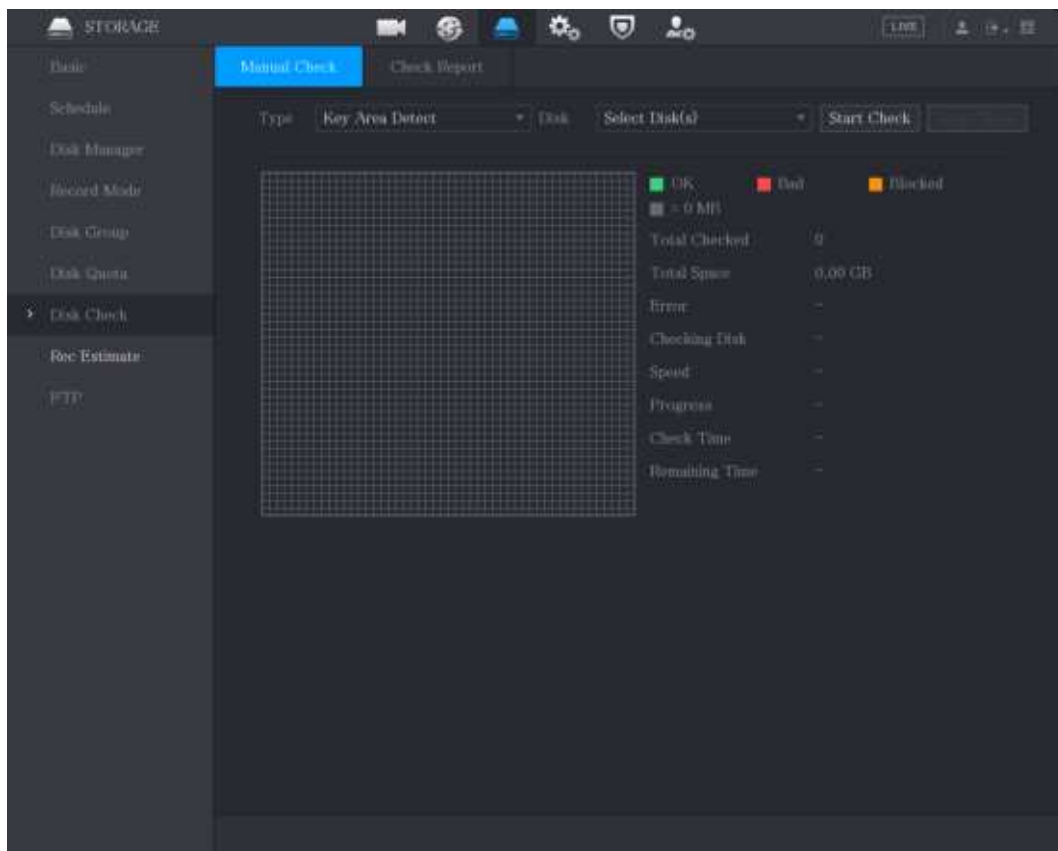
You can detect HDD by key area detect and global detect.

- Key area detect: Detect the files saved in HDD. The detected bad track can be repaired by formatting. If there are no files in HDD, the system cannot detect the bad track.
- Global detect: Detect the whole HDD through Windows, which takes time and might affect the HDD that is recording the video.

Step 1 Select **Main Menu > STORAGE > Disk Check > Manual Check**.

The **Manual Check** interface is displayed.

Figure 5-303



Step 2 In the **Type** list, select **Key Area Detect** or **Global Check**; and in the **Disk** list, select the HDD that you want to detect.

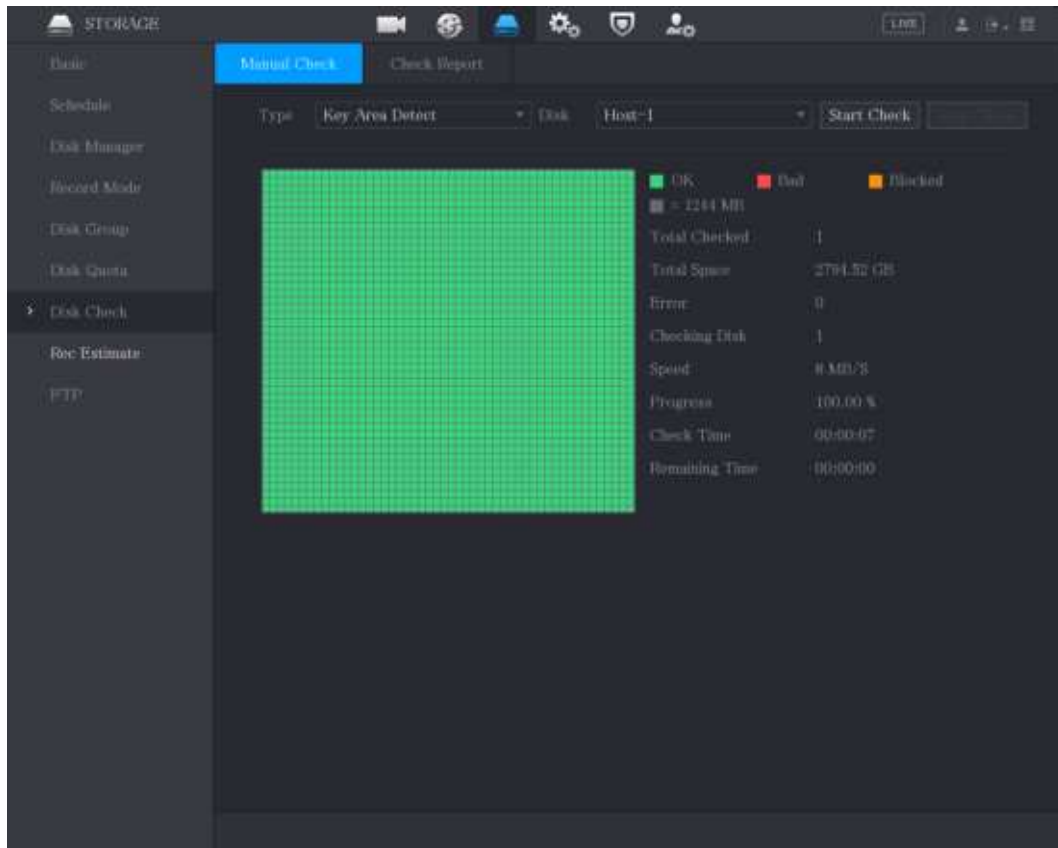
Step 3 Click **Start Check**.

The system starts detecting the HDD. After detecting is completed, see Figure 5-304.



During detecting, click **Pause** to pause detecting, click **Continue** to restart detecting, and click **Stop Detect** to stop detecting.

Figure 5-304



5.18.7.2 View Detecting Results

After the detecting is completed, you can view the detecting reports to find out the problem and replace the defective HDD to avoid data loss.

Step 1 Select **Main Menu > STORAGE > Disk Check > Check Report**.

The **Check Report** interface is displayed.

Figure 5-305

The screenshot shows the 'Check Report' tab in the 'STORAGE' application. It displays a table with the following data:

ID	Disk No.	Check Type	Start Time	Total Space	Error
1	Host-1	Quick Check	2020-01-05 19:37:32	2794.52 GB	0

Step 2 Click .

The **Details** interface is displayed. You can view detecting results and S.M.A.R.T reports.

Figure 5-306

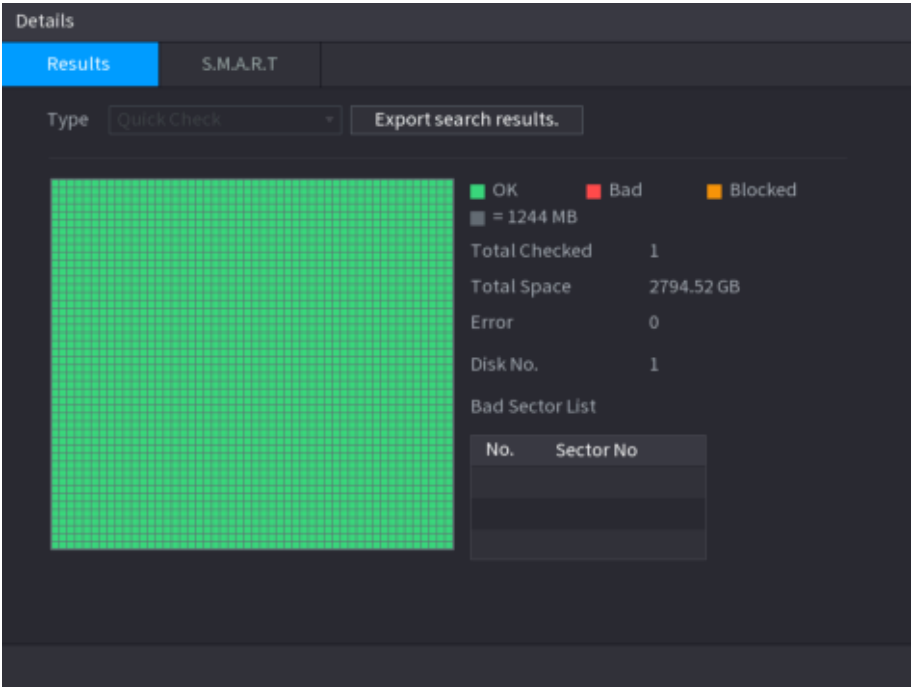
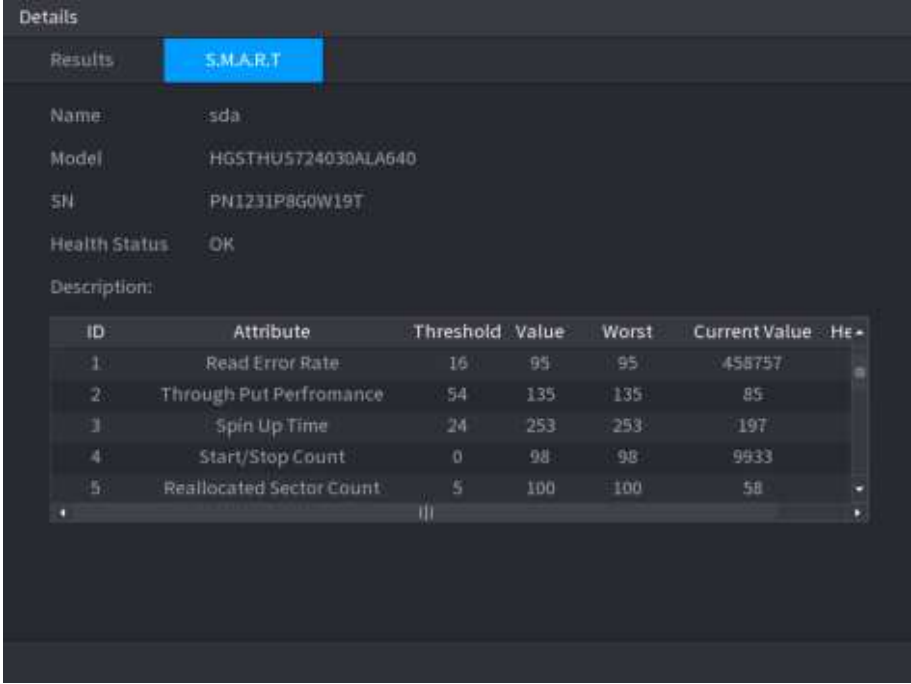


Figure 5-307



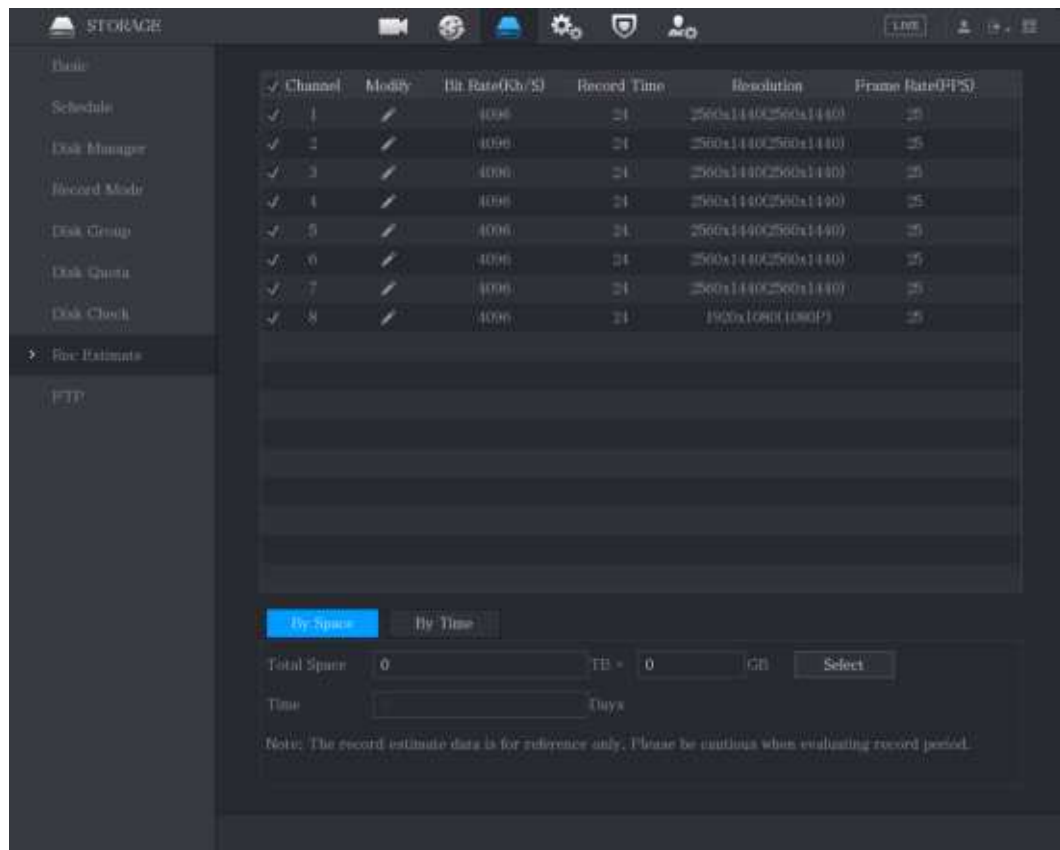
5.18.8 Configuring Record Estimate

Record estimate function can calculate how long you can record video according to the HDD capacity, and calculate the required HDD capacity according to the record period.

Step 1 Select **Main Menu > STORAGE > Rec Estimate**.

The **Rec Estimate** interface is displayed.

Figure 5-308



Step 2 Click .

The **Modify** dialog box is displayed.

You can configure the resolution, frame rate, bit rate and record time for the selected channel.

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

Then the system will calculate the time period that can be used for storage according to the channels settings and HDD capacity.



Click **Copy to** to copy the settings to other channels.

Calculating Recording Time

Step 1 On the **Rec Estimate** interface, click the **By Space** tab.

The **By Space** interface is displayed.

Figure 5-309



Step 2 Click **Select**.

The **Select Disk(s)** interface is displayed.

- Step 3** Select the check box of the HDD that you want to calculate.
In the **By Time** tab, in the **Time** box, the recording time is displayed.

Figure 5-310

Calculating HDD Capacity for Storage

- Step 1** On the **Rec Estimate** interface, click the **By Time** tab.
The **By Time** interface is displayed.

Figure 5-311

- Step 2** In the **Time** box, enter the time period that you want to record.
In the **Total Space** box, the required HDD capacity is displayed.

Figure 5-312

5.18.9 Configuring FTP Storage Settings

You can store and view the recorded videos and snapshots on the FTP server.

Preparation for Configuration

Purchase or download a FTP server and install it on your PC.



For the created FTP user, you need to set the write permission; otherwise the upload of recorded videos and snapshots might be failed.

Configuration Steps

- Step 1** Select **Main Menu > STORAGE > FTP**.
The **FTP** interface is displayed.

Figure 5-313

The screenshot shows the 'STORAGE' configuration window with the 'FTP' tab selected. The 'Enable' checkbox is checked, and 'SFTP (Recommended)' is selected under 'FTP type'. The 'Server Address' field is empty, and the 'Port' is set to 22. The 'Username' and 'Password' fields are empty, and the 'Anonymous' checkbox is checked. The 'Storage Path' field is empty. The 'Record' section shows 'File Size' as 0 M, 'Channel' as 1, and 'Dir' as Sun. The 'Period 1' and 'Period 2' fields are both set to 00:00 - 24:00. The 'Snapshot' section shows 'Picture Upload Interval' as 2 sec. The 'Channel' dropdown is set to 'Setting'. At the bottom, there are buttons for 'Default', 'Test', 'Apply', and 'Back'.

Step 2 Configure the settings for the FTP settings parameters.

Table 5-78

Parameter	Description
Enable	Enable the FTP upload function.
FTP type	- FTP: Plaintext transmission. - SFTP: Encrypted transmission (recommended)
Server Address	IP address of FTP server.
Port	- FTP: The default is 21. - SFTP: The default is 22.
Anonymous	Enter the user name and password to login the FTP server.
Username	
Password	
Storage Path	Create folder on FTP server. - If you do not enter the name of remote directory, system automatically creates the folders according to the IP and time. - If you enter the name of remote directory, the system creates the folder with the entered name under the FTP root directory first, and then automatically creates the folders according to the IP and time.

Parameter	Description
File Size	Enter the length of the uploaded recorded video. • If the entered length is less than the recorded video length, only a section of the recorded video can be uploaded. • If the entered length is more than the recorded video length, the whole recorded video can be uploaded. • If the entered length is 0, the whole recorded video will be uploaded.
Picture Upload Interval (Sec.)	• If this interval is longer than snapshot interval, the system takes the recent snapshot to upload. For example, the interval is 5 seconds, and snapshot interval is 2 seconds per snapshot, the system uploads the recent snapshot every 5 seconds. • If this interval is shorter than snapshot interval, the system uploads the snapshot per the snapshot interval. For example, the interval is 5 seconds, and snapshot interval is 10 seconds per snapshot, the system uploads the snapshot every 10 seconds. • To configure the snapshot interval, select Main Menu > CAMERA > Encode > Snapshot.
Channel	Select the channel that you want to apply the FTP settings.
Day	Select the week day and set the time period that you want to upload the recorded files. You can set two periods for each week day.
Period 1, Period 2	
Record type	Select the record type (Alarm, Intel, MD, and General) that you want to upload. The selected record type will be uploaded during the configured time period.

Step 3 Click **Test**.

The system pops up a message to indicate success or failure. If failed, check the network connection or configurations.

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

5.19 Security Center

You can set security options to strengthen device security and use the device in a much safer way.

5.19.1 Security Status

Security scanning helps get a whole picture of device security status. You can scan user, service and security module status for detailed information about the security status of the device.

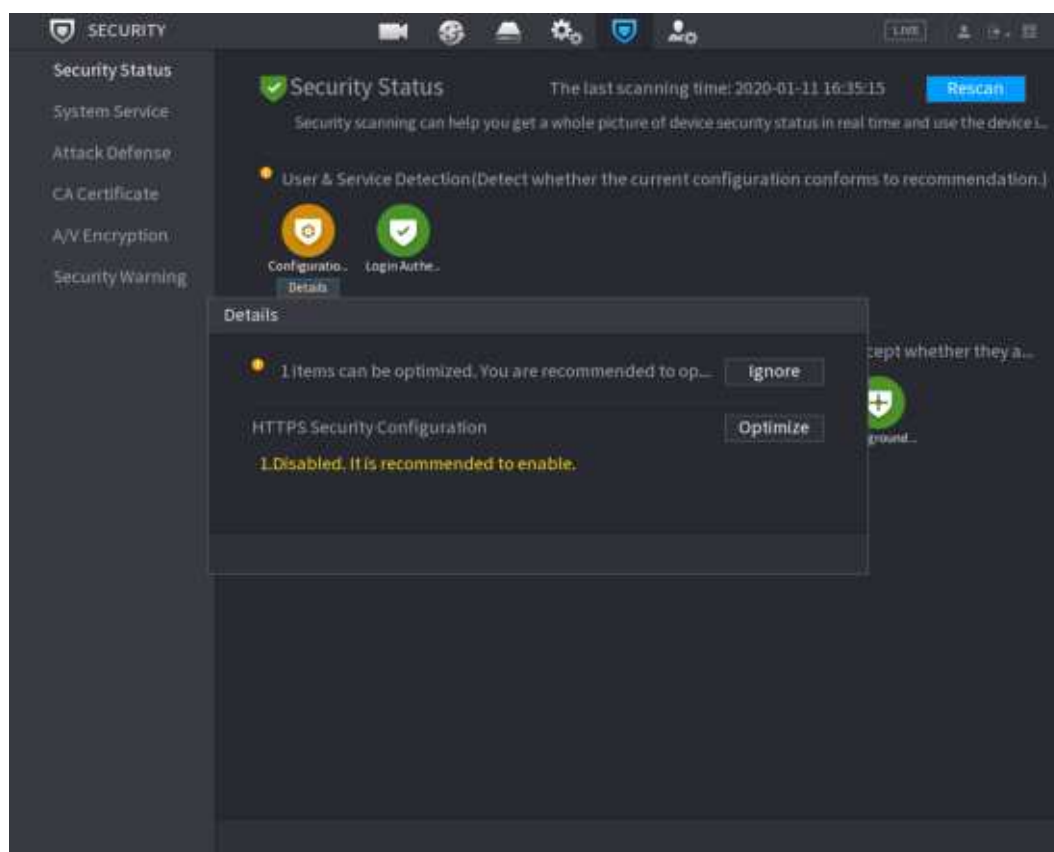
Detecting User and Service



Green icon represents a healthy status of the scanned item, and orange icon represents a risky status.

- Login authentication: When there's a risk in the login authentication, the icon will be in orange to warn risk. You can click **Details** to see the detailed risk description.
- Configuration Security: When there's a risk in the device configuration, the icon will be in orange to warn risk. You can click **Details** to see the detailed risk description.

Figure 5-314



Scanning Security Modules

This area shows the running status of security modules. For details about the security modules, move mouse pointer on the icon to see the on-screen instructions.

Scanning Security Status

You can click **Rescan** to scan security status.

5.19.2 System Service

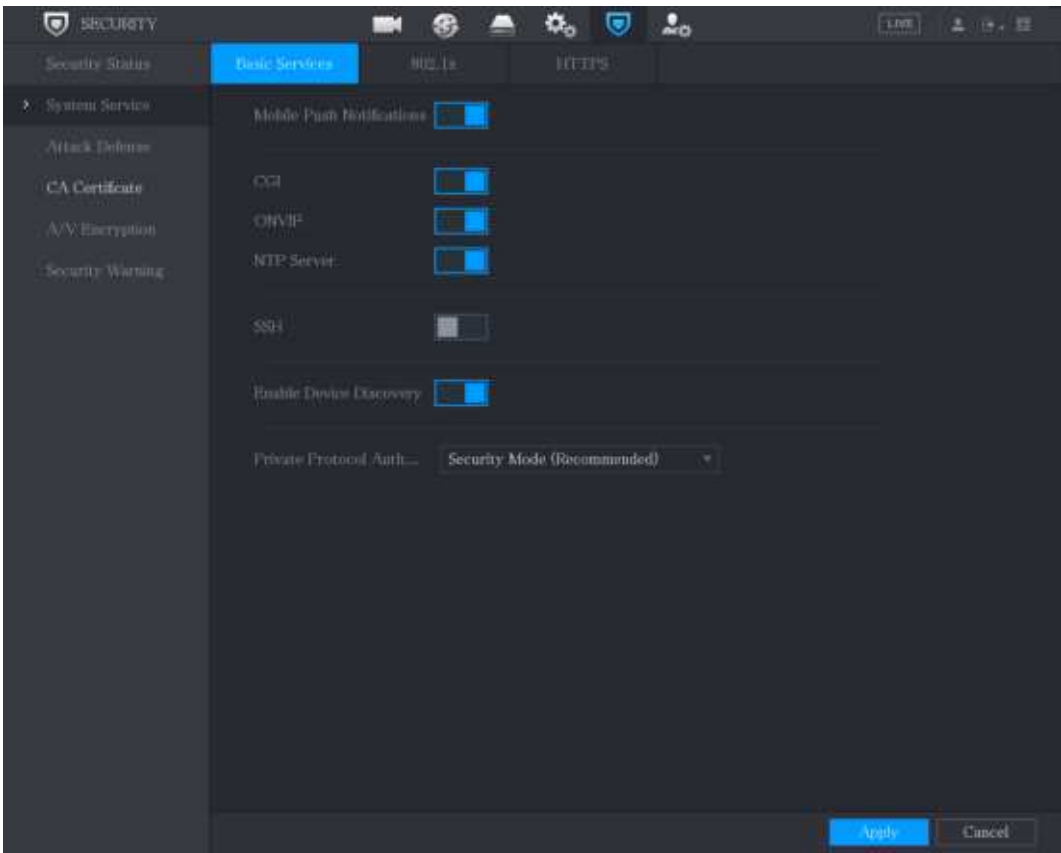
You can set DVR basic information such as basic services, 802.1x and HTTPS.

5.19.2.1 Basic Services

Step 1 Select **Main Menu > SECURITY > System Service > Basic Services**.

The **Basic Services** interface is displayed.

Figure 5-315



Step 2 Select **Basic Services** and configure parameters.



There might be safety risk when **Mobile Push Notifications**, **CGI**, **ONVIF**, **SSH** and **NTP Server** is enabled.

Table 5-79

Parameter	Description
Mobile Push Notifications	After enabling this function, the alarm triggered by the NVR can be pushed to a mobile phone. This function is enabled by default.  There might be safety risk if this service is enabled. Disable this function when it is not in use.

Parameter	Description
CGI	If this function is enabled, the remote devices can be added through the CGI protocol. This function is enabled by default.  There might be safety risk if this service is enabled. Disable this function when it is not in use.
ONVIF	If this function is enabled, the remote devices can be added through the ONVIF protocol. This function is enabled by default.  There might be safety risk if this service is enabled. Disable this function when it is not in use.
NTP Server	After enabling this function, a NTP server can be used to synchronize the device. This function is enabled by default.
SSH	After enabling this function, you can use SSH service. This function is disabled by default.  There might be safety risk if this service is enabled. Disable this function when it is not in use.
Enable Device Discovery	After enabling this function, the device can be searched by other devices.
Private Protocol Authentication Mode	• Security Mode (Recommended): Uses Digest access authentication when connecting to DVR. • Compatible Mode: Select this mode when the client does not support Digest access authentication.

Step 3 Click **Apply** to complete the settings.

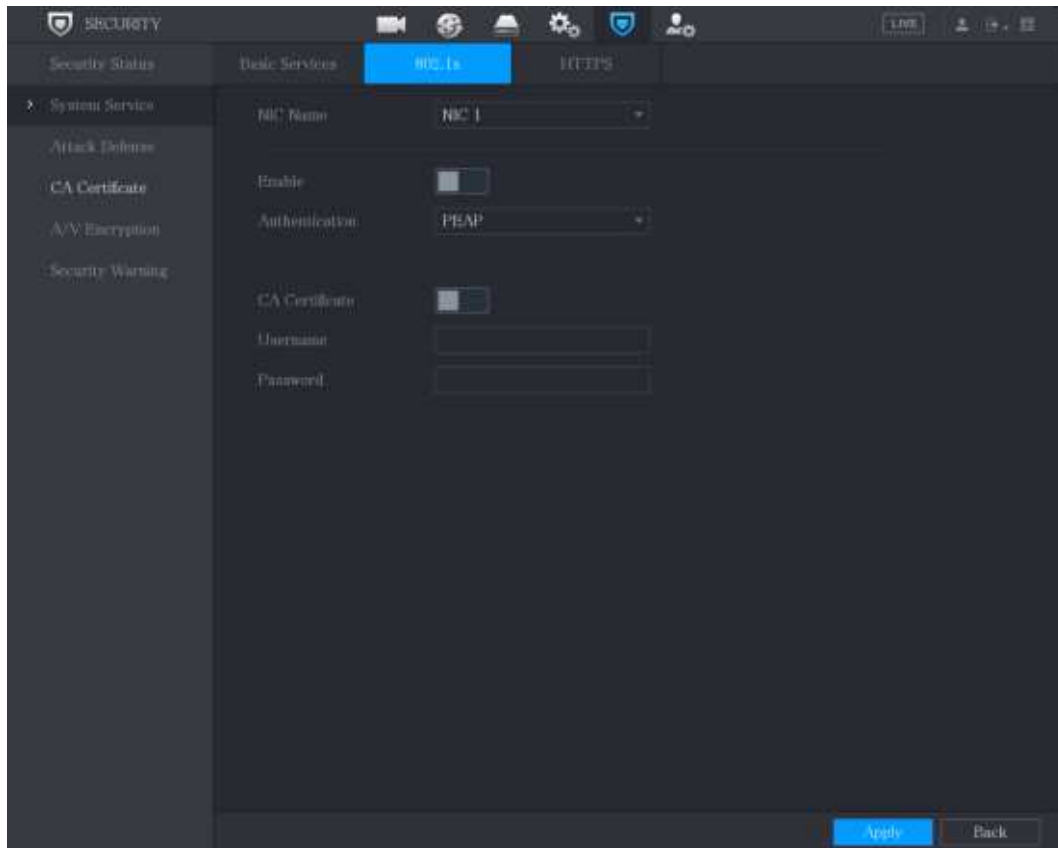
5.19.2.2 802.1x

The device needs to pass 802.1x certification to enter the LAN.

Step 1 Select **Main Menu > SECURITY > System Service > 802.1x**.

The **802.1x** interface is displayed.

Figure 5-316



Step 2 Select the Ethernet card you want to certify.

Step 3 Select **Enable** and configure parameters.

Table 5-80

Parameter	Description
NIC Name	Select a NIC.
Authentication	• PEAP: protected EAP protocol. • TLS: Transport Layer Security. Provide privacy and data integrity between two communications application programs.
CA Certificate	Enable it and click Browse to import CA certificate from flash drive. For details about importing and creating a certificate, see 5.19.4.
Username	The username shall be authorized at server.
Password	Password of the corresponding username.

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

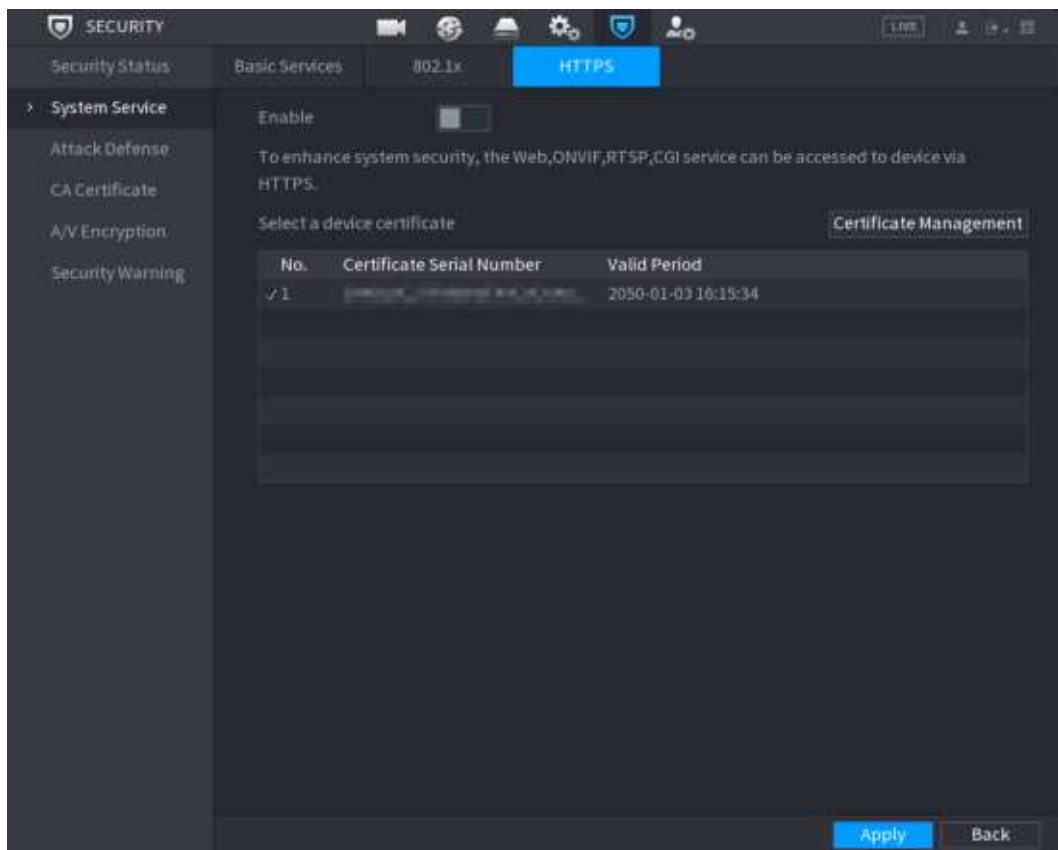
5.19.2.3 HTTPS

We recommend that you enable HTTPS function to enhance system security.

Step 1 Select **Main Menu > SECURITY > System Service > HTTPS**.

The **HTTPS** interface is displayed.

Figure 5-317



Step 2 Select **Enable** to enable HTTPS function.

Step 3 Click **Certificate Management** to create or import a HTTPS certificate from USB drive.
For details about importing or creating a CA certificate, see 5.19.4.

Step 4 Select a HTTPS certificate.

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

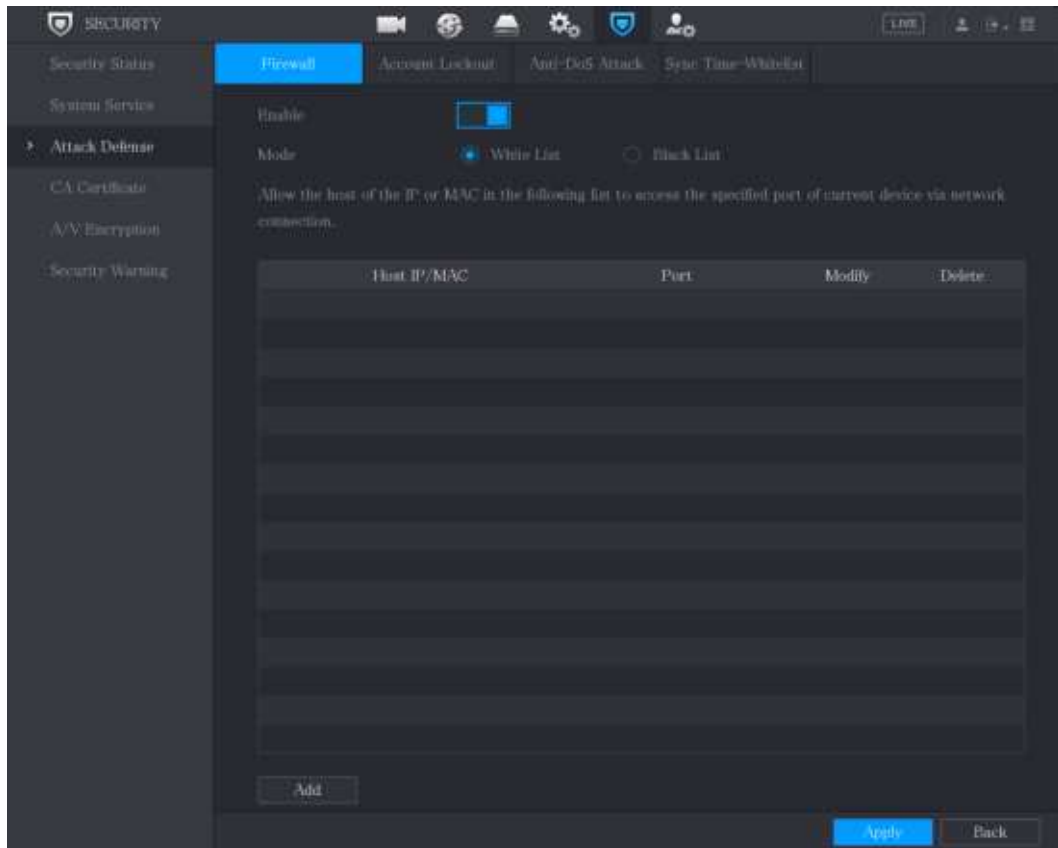
5.19.3 Attack Defense

5.19.3.1 Firewall

Step 1 Select **Main Menu > SECURITY > Attack Defense > Firewall**.

The **Firewall** interface is displayed.

Figure 5-318



Step 2 Select **Enable** to enable firewall.

Step 3 Configure the parameters.

Table 5-1 Firewall parameters

Parameter	Description
Mode	Mode can be configured when Type is Network Access. - If White List is enabled, you can visit device port successfully with IP/MAC hosts in the white list. - If Black List is enabled, you cannot visit device port with IP/MAC hosts in black list.
Add	When Type is Network Access, you can configure IP Address, IP Segment and MAC Address.
Type	You can select IP address, IP segment and MAC address.
IP Address	Enter IP Address, Start Port and End Port that is allowed or forbidden.  When Type is IP Address, they can be configured. Start Port and End Port can be configured only in Network Access Type.
Start Port	
End Port	

Parameter	Description
Start Address/End Address	Enter Start Address and End Address of IP Segment.  When Type is IP Segment, they can be configured.
MAC Address	Enter MAC Address that is allowed or forbidden  When Type is MAC Address, it can be configured.

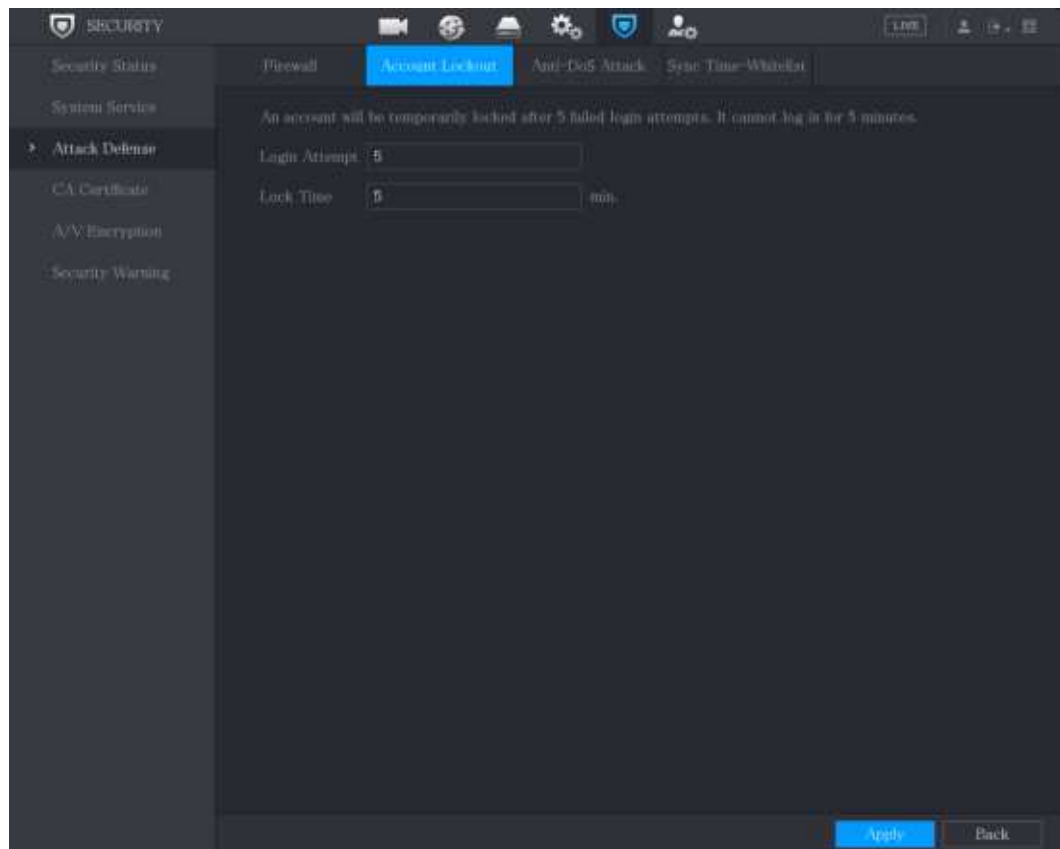
Step 4 Click **Apply** to complete the settings.

5.19.3.2 Account Lockout

Step 1 Select **Main Menu > SECURITY > Attack Defense > Account Lockout**.

The **Account Lockout** interface is displayed.

Figure 5-319



Step 2 Set parameters.

Table 5-81

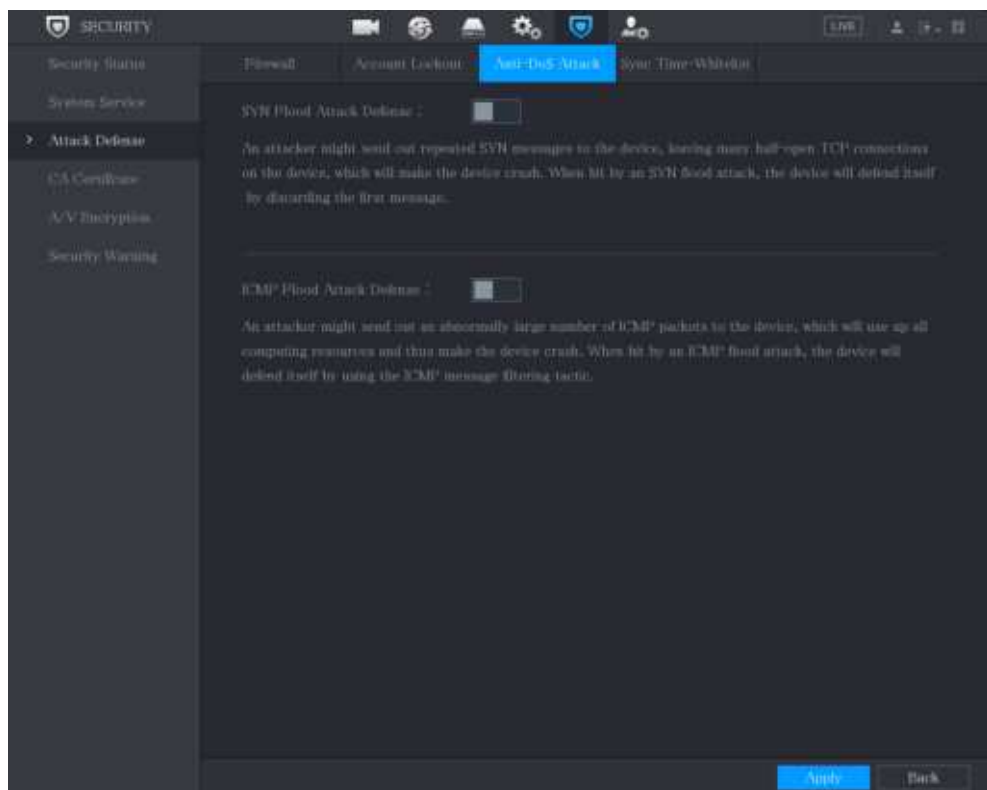
Parameter	Description
Attempt(s)	Set the maximum number of allowable wrong password entries. The account will be locked after your entries exceed the maximum number. Value range: 5–30. Default value: 5.
Lock Time	Set how long the account is locked for. Value range: 5–120 minutes. Default value: 5 minutes.

Step 3 Click **Apply** to complete the settings.

5.19.3.3 Anti-Dos Attack

You can enable **SYN Flood Attack Defense** and **ICMP Flood Attack Defense** to defend the device against Dos attack. See Figure 5-320.

Figure 5-320



5.19.3.4 Sync Time-Whitelist

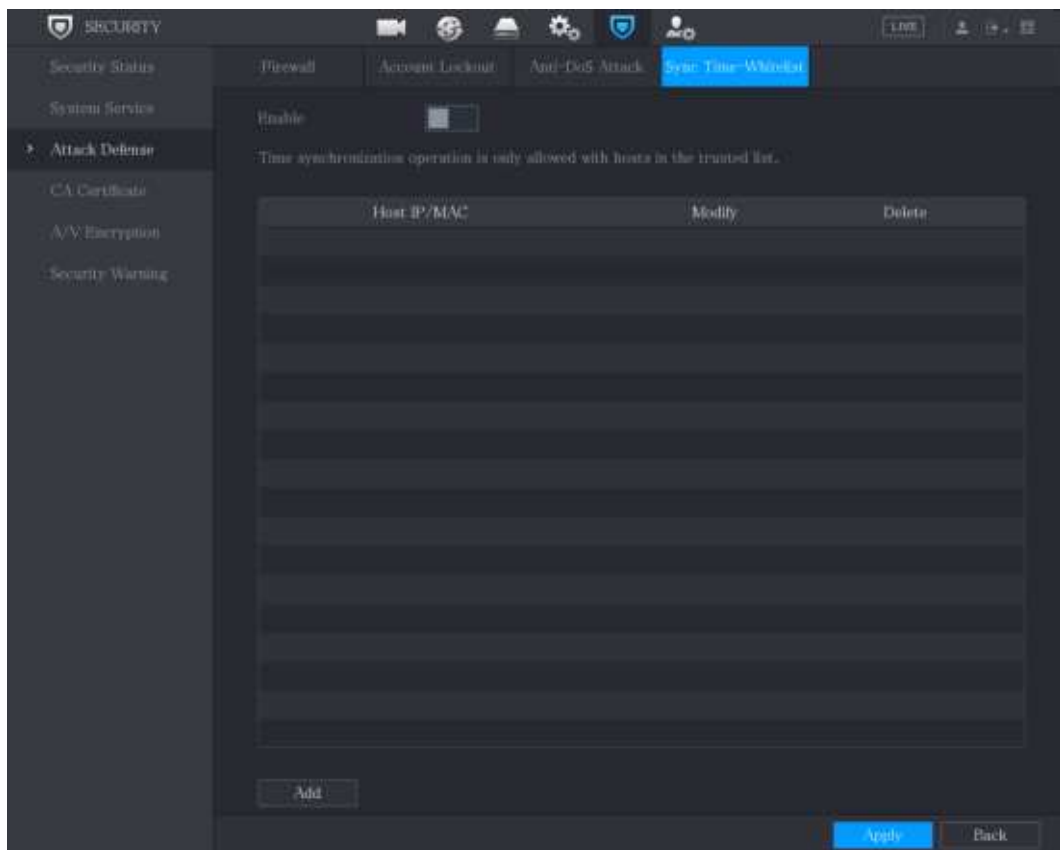


The synchronization is only allowed with hosts in the trusted list.

Step 1 Select **Main Menu > SECURITY > Attack Defense > Sync Time-Whitelist**.

The **Sync Time-Whitelist** interface is displayed.

Figure 5-321



Step 2 Select **Enable** to enable **Sync Time-Whitelist** function.

Step 3 Configure the parameters.

Table 5-82

Parameter	Description
Add	You can add trusted hosts for time synchronization.
Type	Select IP address or IP segment for hosts to be added.
IP Address	Input the IP address of a trusted host.  When Type is IP Address, it can be configured
Start Address	Input the start IP address of trusted hosts.  When Type is IP Segment, it can be configured
End Address	Input the end IP address of trusted hosts.  When Type is IP Segment, it can be configured

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

5.19.4 CA Certificate

You can create or import device certificate and install trusted CA Certificate.

5.19.4.1 Device Certificate

Create Certificate

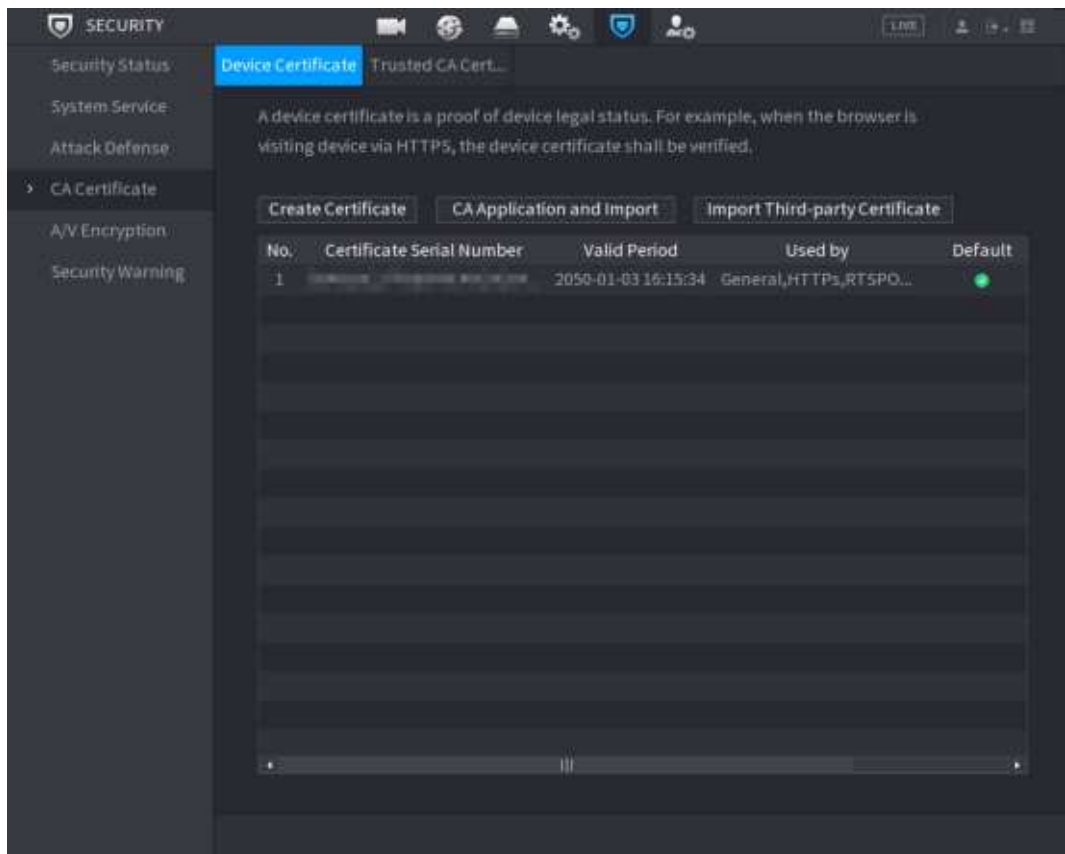
1. Select **Main Menu > SECURITY > CA Certificate > Device Certificate**.

The **Device Certificate** interface is displayed.



- Click  to download the certificate to local storage.
- Click  to delete the certificate. The deleted certificate cannot be restored, proceed with caution.

Figure 5-322



2. Configure parameters.

Table 5-83

Parameter	Description
County	This parameter is user defined.
State	This parameter is user defined.
City Name	This parameter is user defined.

Parameter	Description
Valid Period	Input a valid period for the certificate.
Organization	This parameter is user defined.
Organization Unit	This parameter is user defined.
Domain Name	Input the IP address of the certificate.

3. Click **Create**.

CA Application and Import

Follow the on-screen instructions to finish CA application and import.



Insert a USB flash drive before operating.

Figure 5-323

CA Application and Import

Procedure:

Step 1: Select 'Create a Certificate Request' to generate a certificate request file.

Step 2: Submit the certificate request file to a third-party CA institution to apply for a certificate.

Step 3: Select 'Import a Certificate' and then import the CA certificate issued by the third-party institution.

Type: **Create Certificate R...** Import Certificate

Country:

Province:

City Name:

Valid Period:

Organization:

Organization Unit:

Domain Name:

Create Cancel

Import Third-Party Certificate

Insert the USB flash drive with third-party certificate before importing.

1. Select **Import Third-party Certificate**.

Figure 5-324

The screenshot shows a dark-themed dialog box titled "Import Third-party Certificate". It has three input fields: "Path", "Private Key", and "Private Key Password". The "Path" and "Private Key" fields have "Browse" buttons next to them. At the bottom right, there are "Import" and "Cancel" buttons.

2. Configure Parameters.

Table 5-2 Importing third-party certificate

Parameter	Description
Path	Click Browse to find the third-party certificate path on the USB drive.
Private Key	Click Browse to find the third-party certificate private key on the USB drive.
Private Key Password	Input the password of encrypted private key. When the private key is not encrypted, you don't need to this parameter.

3. Click **Create**.

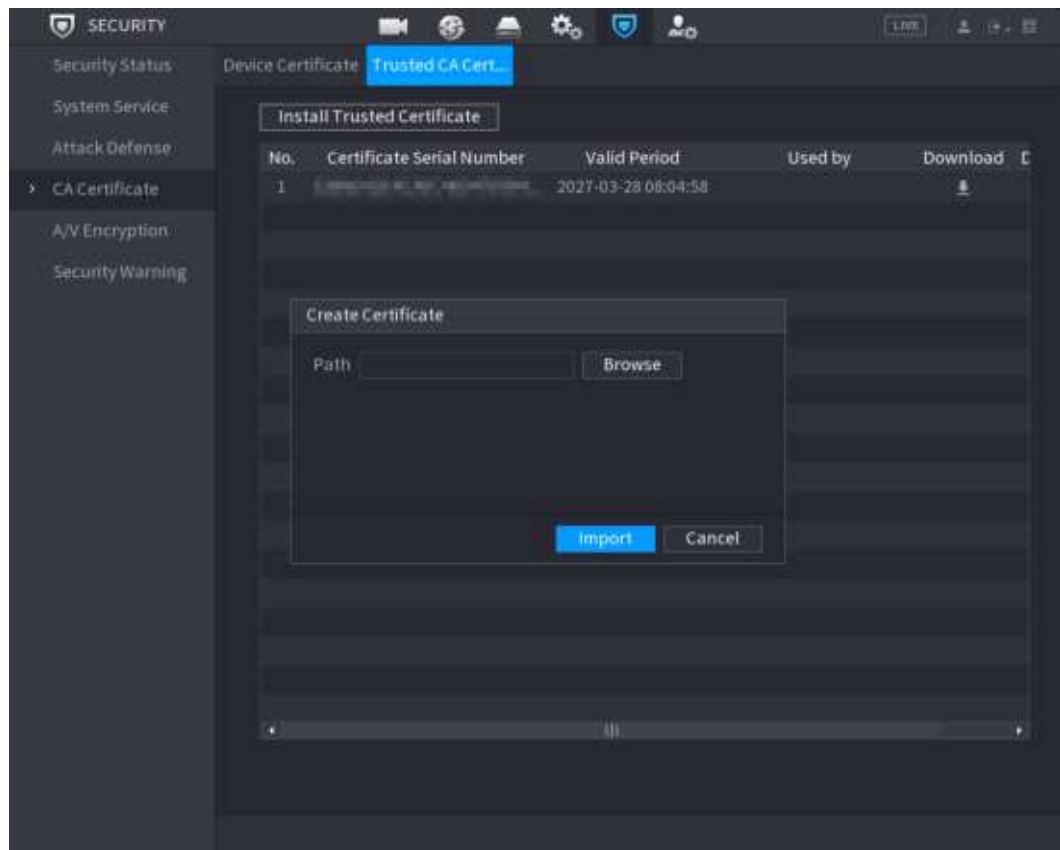
5.19.4.2 Trusted CA Certificate

Step 1 Select **Main Menu > SECURITY > CA Certificate > Trusted CA Certificate**.

Step 2 Click **Install Trusted Certificate**.

The **Create Certificate** is displayed.

Figure 5-325



Step 3 Click **Browse** to select the certificate that you want to install.

Step 4 Click **Import**.

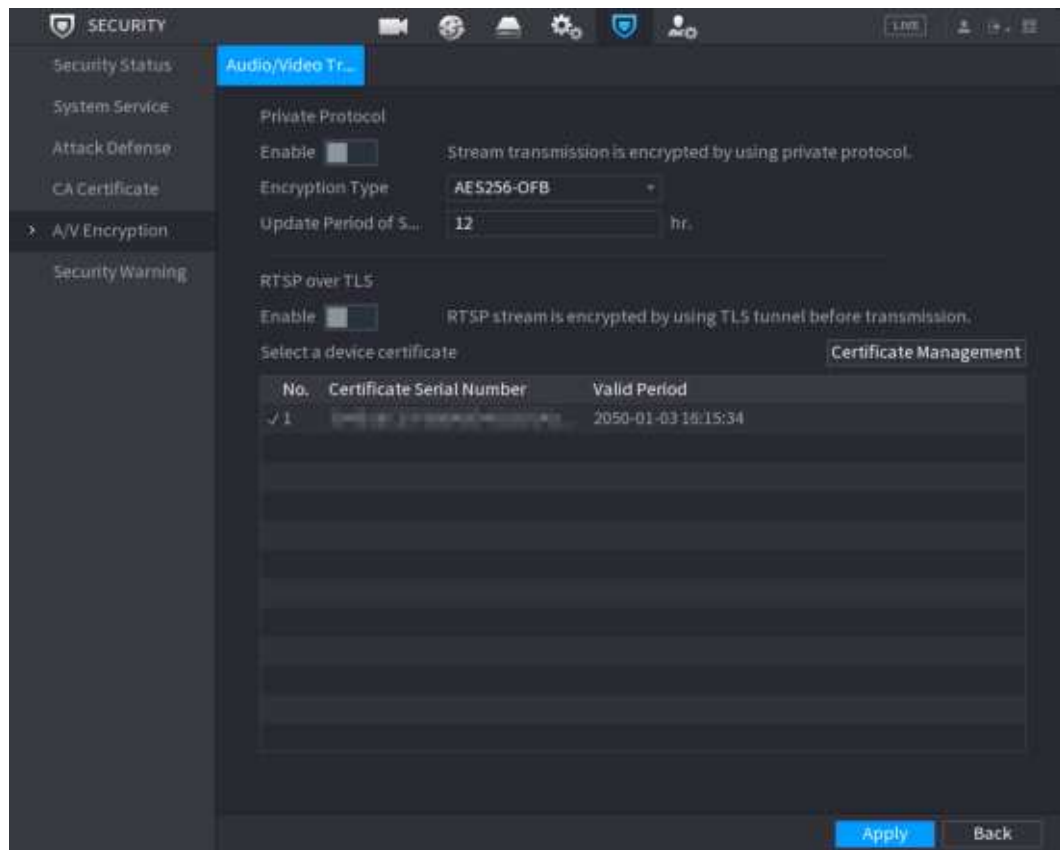
5.19.5 Audio/Video Encryption

The device supports audio and video encryption during data transmission.

Step 1 Select **Main Menu > SECURITY > A/V Encryption > Audio/Video Transmission**.

The **Audio/Video Transmission** interface is displayed.

Figure 5-326



Step 2 Configure parameters.

Table 5-84

Area	Parameter	Description
Private Protocol	Enable	Enables stream frame encryption by using private protocol. There might be safety vulnerability if this service is disabled.
	Encryption Type	Use the default setting.
	Update Period of Secret Key	Secret key update period. Value range: 0–720 hours. 0 means never update the secret key. Default value: 12.
RTSP over TLS	Enable	Enables RTSP stream encryption by using TLS. There might be data breach if this service is disabled. We recommend that you enable this function.
	Select a device certificate	Select a device certificate for RTSP over TLS.

Area	Parameter	Description
	Certificate Management	For details about certificate management, see 5.19.4.1.

Step 3 Click **Apply** to complete the settings.

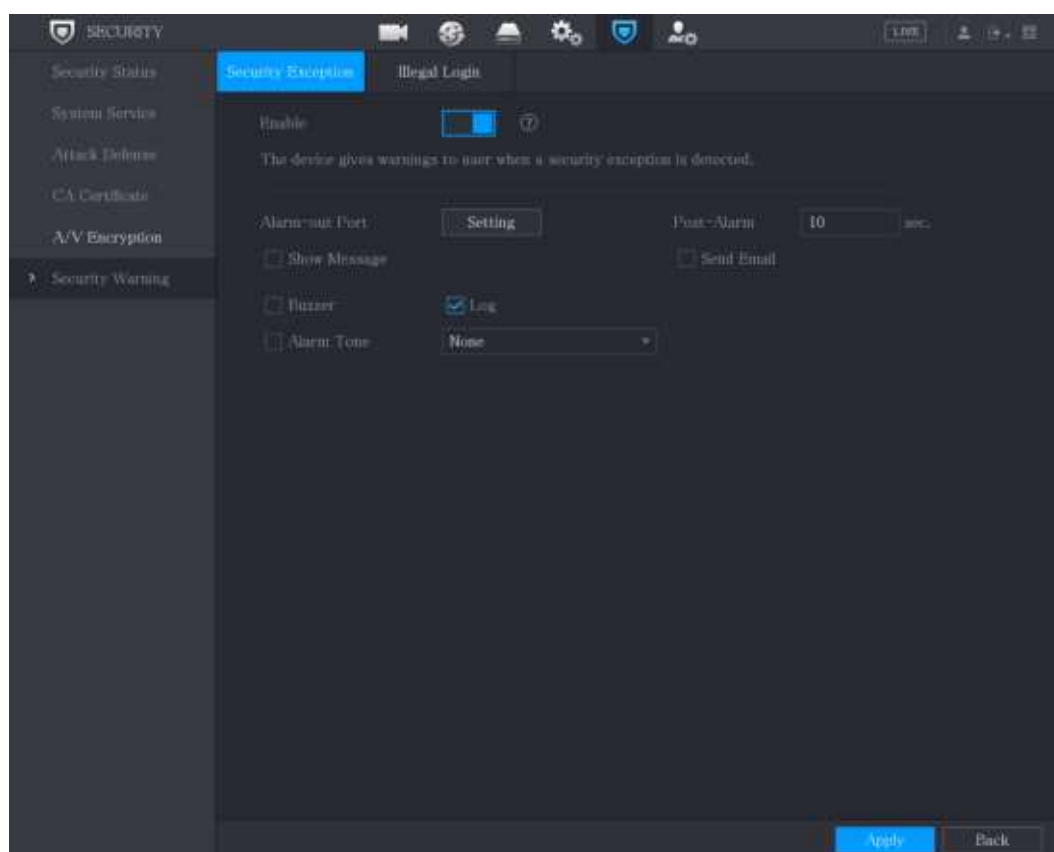
5.19.6 Security Warning

5.19.6.1 Security Exception

Step 1 Select **Main Menu > SECURITY > Security Warning > Security Exception**.

The **Security Exception** interface is displayed.

Figure 5-327



Step 2 Select **Enable** and configure parameters.

Table 5-85

Parameter	Description
Alarm-out Port	The alarm device (such as lights, sirens, etc.) is connected to the alarm output port. When an alarm occurs, the NVR device transmits the alarm information to the alarm device.
Post-Alarm	When the alarm ends, the alarm extended for a period of time. The time range is from 0 seconds to 300 seconds.

Parameter	Description
Show Message	Check box to enable a pop-up message in your local host PC.
Buzzer	Select the check box to activate the buzzer when an alarm occurs.
Alarm Tone	Check the box and then select the corresponding audio file from the dropdown list. System plays the audio file when the alarm occurs.  See 5.17 to add audio file first.
Log	Select the check box, the NVR device records the alarm information in the log when an alarm occurs.
Send Email	Select the check box. When an alarm occurs, the NVR device sends an email to the set mailbox to notify the user.  To use this function, make sure the email function is enabled in Main Menu > NETWORK > Email.
②	Security Event monitoring explanation. It indicates the type of attacks that can trigger security exception. • Unauthorized executable program trying to run • Web URL brute-force attack • Session connection overload • Session ID brute-force attack

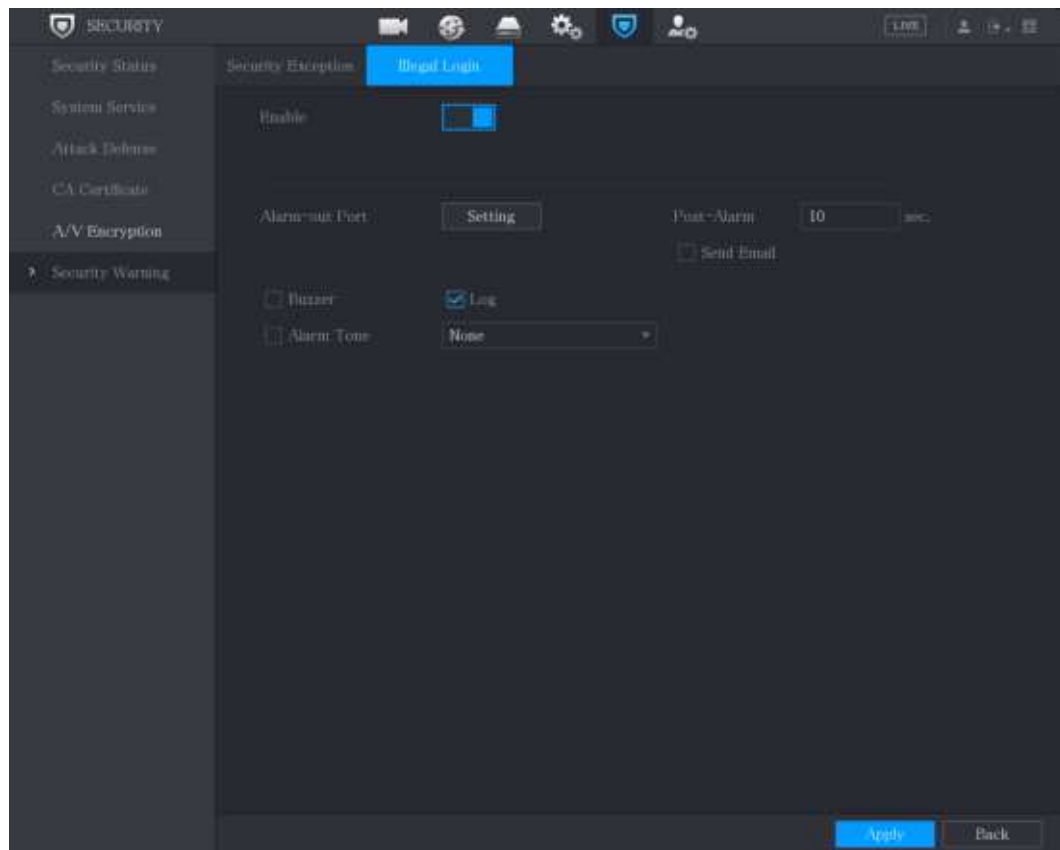
Step 3 Click **Apply** to complete the settings.

5.19.6.2 Illegal Login

Step 1 Select **Main Menu > SECURITY > Security Warning > Illegal Login**.

The **Illegal Login** interface is displayed.

Figure 5-328



Step 2 Select **Enable** and configure parameters.

Table 5-86

Parameter	Description
Alarm-out Port	The alarm device (such as lights, sirens) is connected to the alarm output port. When an alarm occurs, the NVR device transmits the alarm information to the alarm device.
Post-Alarm	When the alarm ends, the alarm extended for a period of time. The time range is from 0 seconds through 300 seconds.
Buzzer	Select the check box to activate the buzzer when an alarm occurs.
Alarm Tone	Check the box and then select the corresponding audio file from the dropdown list. System plays the audio file when the alarm occurs.  See 5.17 to add audio file first.
Log	Select the check box, the NVR device records the alarm information in the log when an alarm occurs.
Send Email	Select the check box. When an alarm occurs, the NVR device sends an email to the set mailbox to notify the user.  To use this function, make sure the email function is enabled in Main Menu > NETWORK > Email .

5.20 Configuring System Settings

5.20.1 Configuring General System Settings

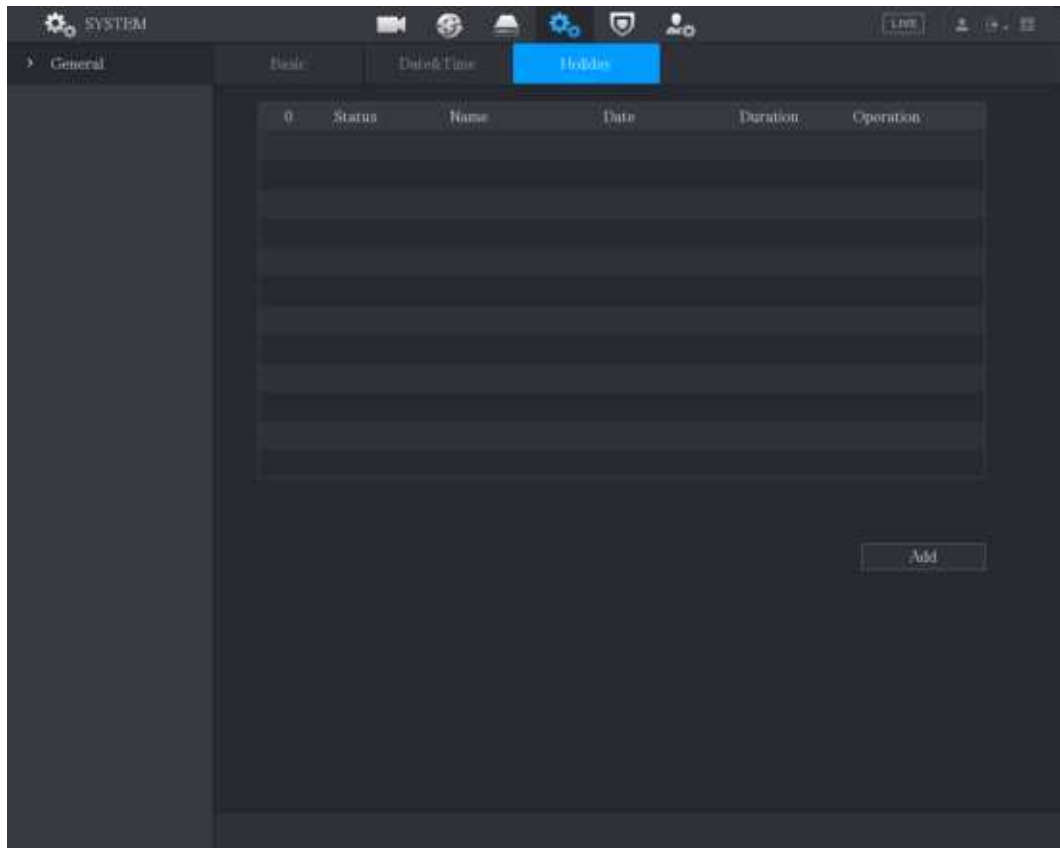
You can configure the device basic settings, time settings, and holiday settings.

To configure the holiday settings, do the following:

Step 1 Select **Main Menu > SYSTEM > General > Holiday**.

The **Holiday** interface is displayed.

Figure 5-329



Step 2 Click **Add**.

The **Add** interface is displayed.

Figure 5-330

The 'Add' dialog box contains the following fields and options:

- Name:** A text input field.
- Effective Mode:** Radio buttons for ☐ Once and ☒ Always.
- Period:** Radio buttons for ☒ Date and ☐ Week.
- Start Time:** A time selection field showing 01:07.
- End Time:** A time selection field showing 01:07.
- Add More:** A checkbox that is currently unchecked.
- Buttons:** 'Add' and 'Cancel' buttons at the bottom right.

Step 3 Configure the holiday name, repeat mode, time range according to your actual situation.

Step 4 Click **Add**.

The added holiday information is displayed.



Enable the **Add More** function, so you can continue adding holiday information.

Figure 5-331

The 'Holiday' page displays a table with the following columns: ID, Status, Name, Date, Duration, and Operation. The first row shows a holiday with ID 1, Status 'On', Name 'xx', Date '1.5', and Duration '1 Days'. Below the table is an 'Add' button.

ID	Status	Name	Date	Duration	Operation
1	On	xx	1.5	1 Days	

5.20.2 Configuring RS-232 Settings

You can configure serial port function, Baud rate and other parameters.



Only some series products support this RS-232.

Select **Main Menu > SYSTEM > RS232**.

The **RS232** interface is displayed.

Figure 5-332



Table 5-87

Parameter	Description
Function	Select serial port control protocol. • Console: Upgrade the program and debug with the console and mini terminal software. • Keyboard: Control this Device with special keyboard. • Adapter: Connect with PC directly for transparent transmission of data. • Protocol COM: Configure the function to protocol COM, in order to overlay card number. • PTZ Matrix: Connect matrix control. It is Console by default.
Baud Rate	Select Baud rate, which is 115200 by default.
Data Bits	It ranges from 5 to 8, which is 8 by default.
Stop Bits	It includes 1 and 2.
Parity	It includes none, odd, even, mark and null. It is none by default.

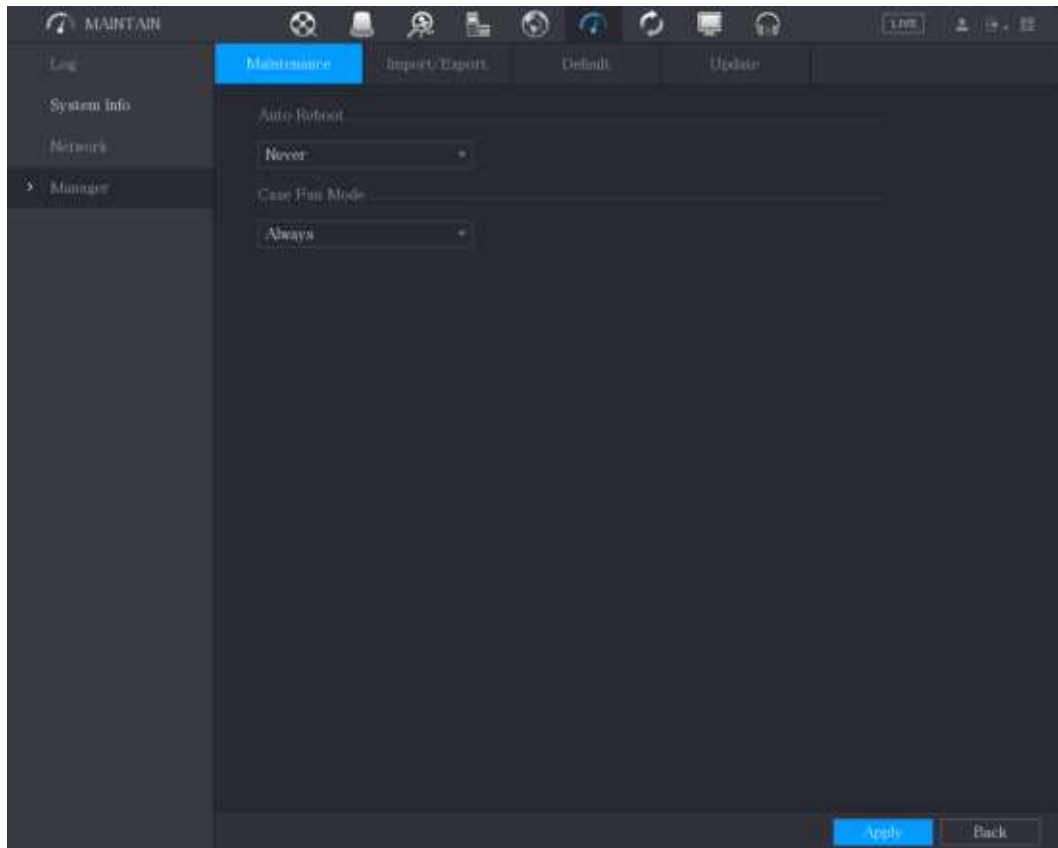
5.20.3 Configuring System Maintenance Settings

When the Device has been running for a long time, you can configure the auto reboot when the Device is not working. You can also configure the case fan mode to reduce noise and extend the service life.

Step 1 Select **Main Menu > MAINTAIN > Manager > Maintenance**.

The **Maintenance** interface is displayed.

Figure 5-333



Step 2 Configure the settings for the system maintenance parameters.

Table 5-88

Parameter	Description
Auto Reboot	In the Auto Reboot list, select the reboot time.
Case Fan Mode	In the Case Fan Mode list, you can select Always or Auto. If you select Auto, the case fan will stop or start according to the external conditions such as the Device temperature.  Not all models support this function, and it is only supported on the local configuration interface.

Step 3 Click **Apply** to complete the settings.

5.20.4 Exporting and Importing System Settings

You can export or import the Device system settings if there are several Devices that require the same setup.

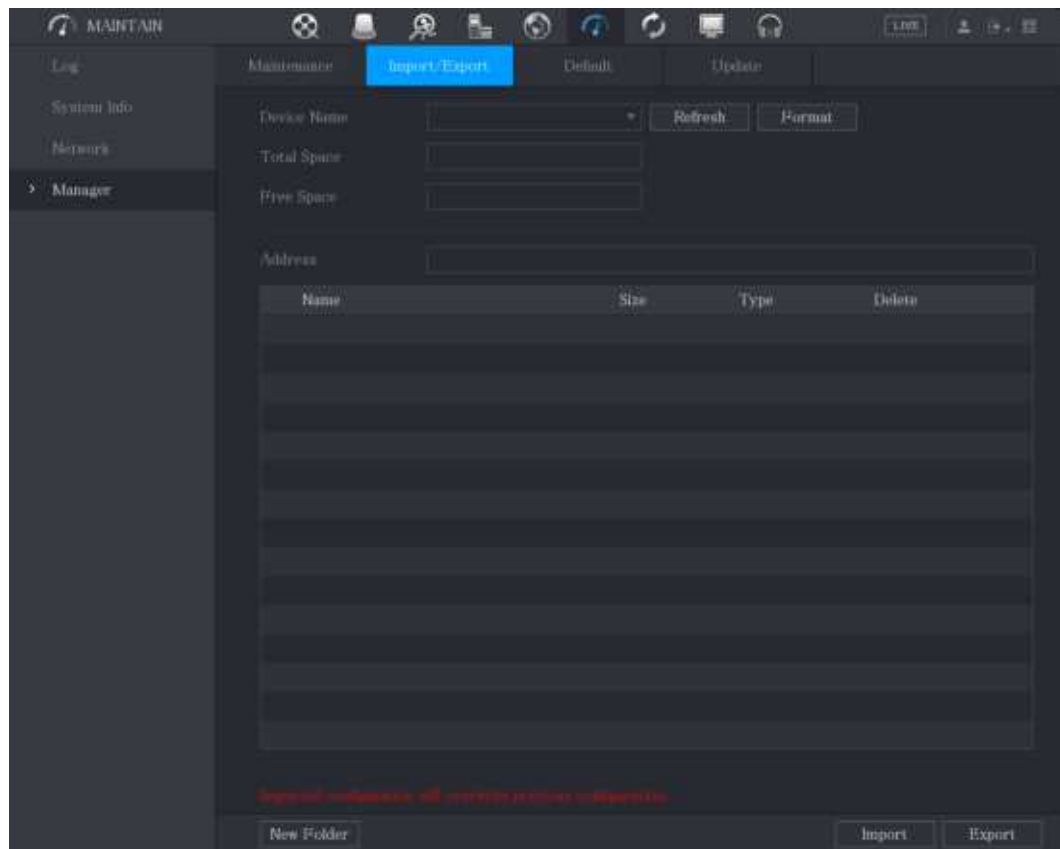


- The **IMP/EXP** interface cannot be opened if the backup operation is ongoing on the other interfaces.
- When you open the **IMP/EXP** interface, the system refreshes the devices and sets the current directory as the first root directory.
- Click **Format** to format the USB storage device.

Exporting System Settings

- Step 1 Select **Main Menu > MAINTAIN > Manager > Import/Export**.
The **Import/Export** interface is displayed.

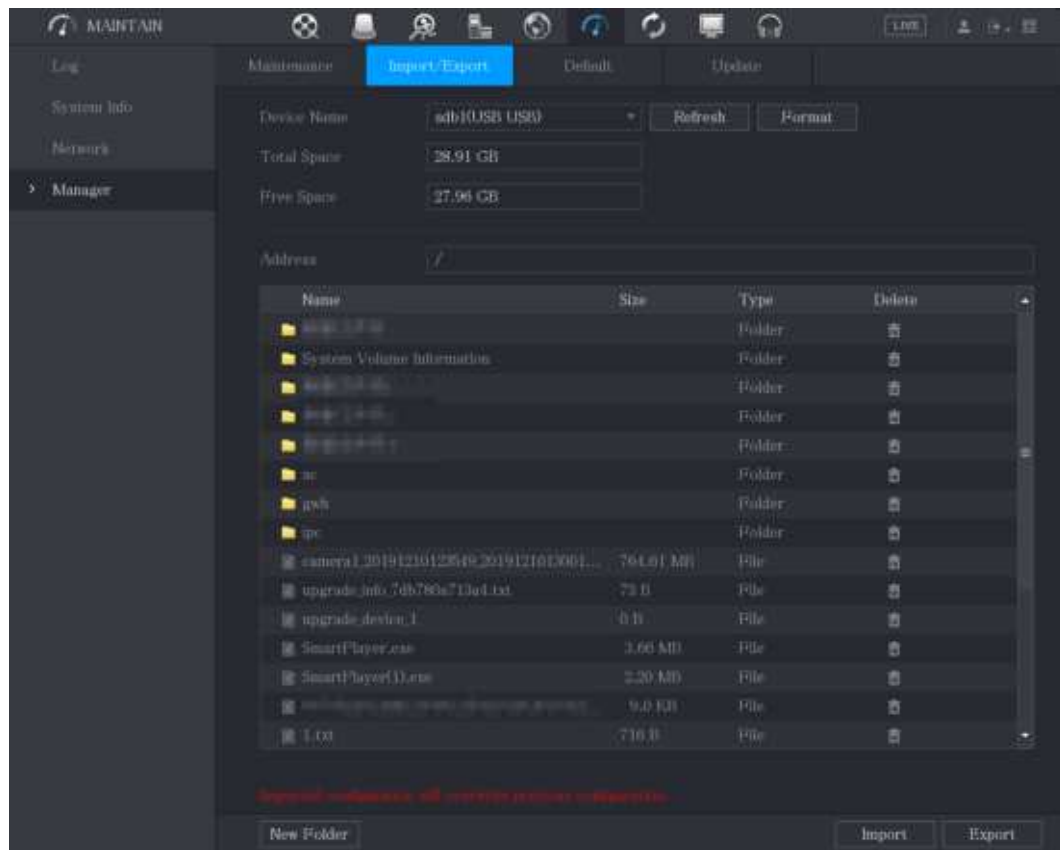
Figure 5-334



- Step 2 Insert a USB storage device into one of the USB ports on the Device.

- Step 3 Click **Refresh** to refresh the interface.
The connected USB storage device is displayed.

Figure 5-335



Step 4 Click **Export**.

There is a folder under the name style of "Config_[YYYYMMDDhhmmss]". Double-click this folder to view the backup files.

Importing System Settings

Step 1 Insert a USB storage device containing the exported configuration files from another Device) into one of the USB ports on the Device.

Step 2 Select **Main Menu > SYSTEM > Import/Export**.

The **Import/Export** interface is displayed.

Step 3 Click **Refresh** to refresh the interface.

The connected USB storage device is displayed.

Step 4 Click on the configuration folder (under the name style of "Config_[YYYYMMDDhhmmss]") that you want to import.

Step 5 Click **Import**.

The Device will reboot after the imported is succeeded.

5.20.5 Restoring Default Settings



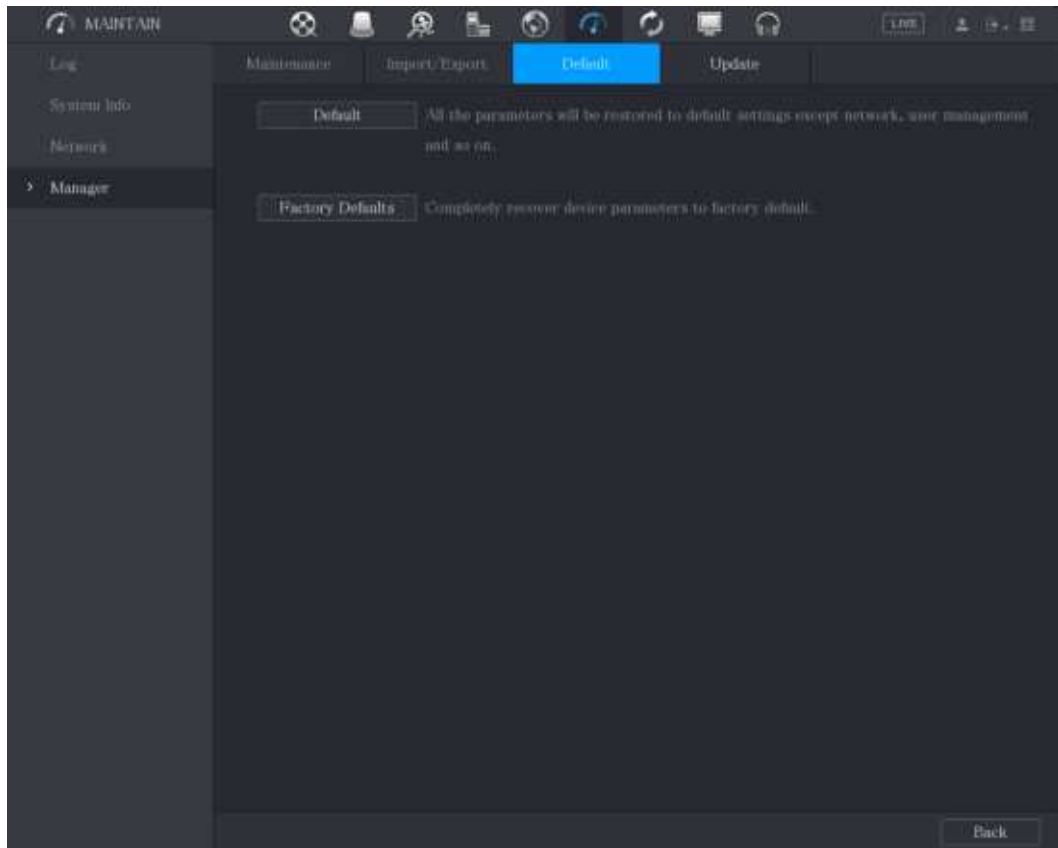
Only Admin account supports this function.

You can select the settings that you want to restore to the factory default.

Step 1 Select **Main Menu > MAINTAIN > Manager > Default**.

The **Default** interface is displayed.

Figure 5-336



Step 2 Restore the settings.

- Click **Default** to restore all parameters to default settings except parameters such as network, user management.
- Click **Factory Default**, select **OK** and then enter the password of admin user in the prompted dialog box to completely recover device parameters to factory default.

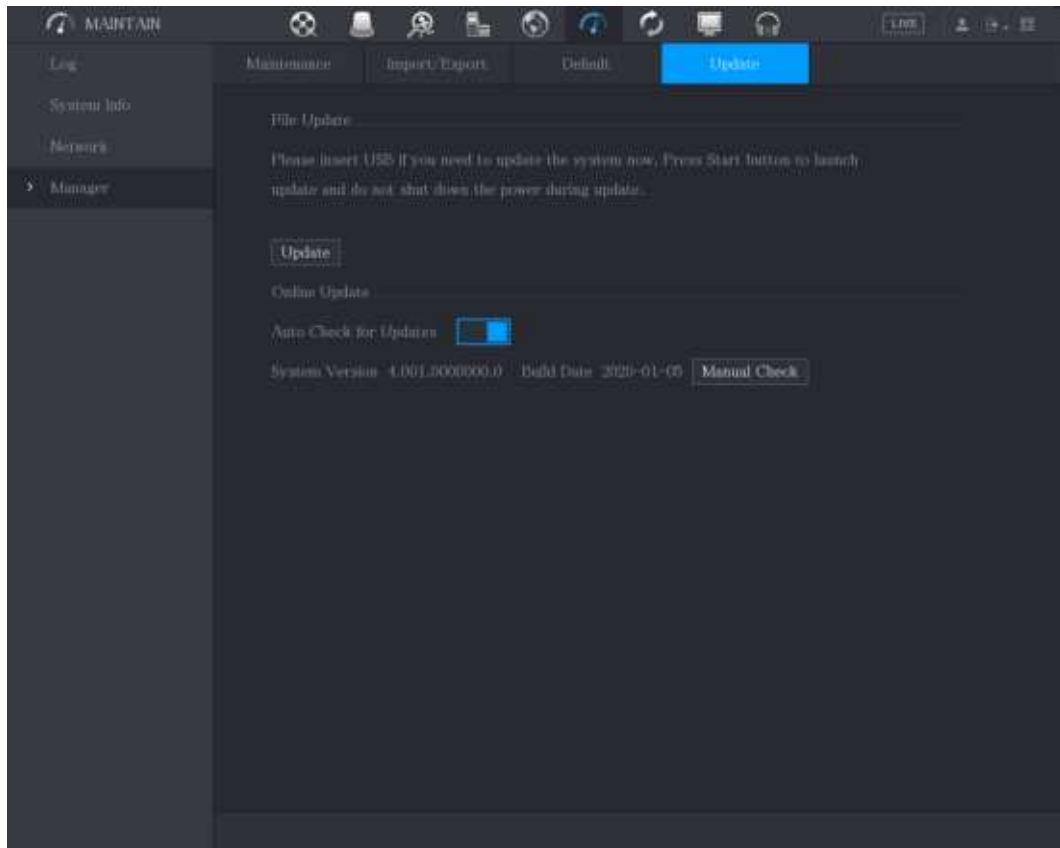
5.20.6 Updating the Device

5.20.6.1 Updating File

Step 1 Insert a USB storage device containing the upgrade files into the USB port of the Device.

Step 2 Select **Main Menu > MAINTAIN > Manager > Update**.
The **Update** interface is displayed.

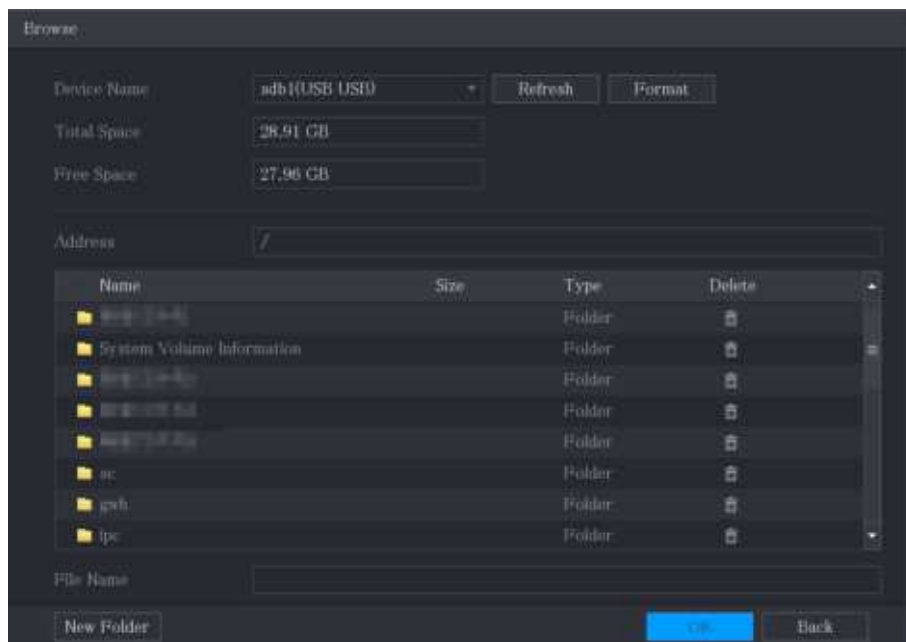
Figure 5-337



Step 3 Click **Upgrade**.

The **Upgrade** interface is displayed.

Figure 5-338



Step 4 Click the file that you want to upgrade.

The selected file is displayed in the **Address** box.

Step 5 Click **OK**.

5.20.6.2 Performing Online Upgrade

When the Device is connected to Internet, you can use online upgrade function to upgrade the system.

Before using this function, you need to check whether there is any new version by auto check or manual check.

- Auto check: The Device checks if there is any new version available at intervals.
- Manual check: Perform real-time check whether there is any new version available.

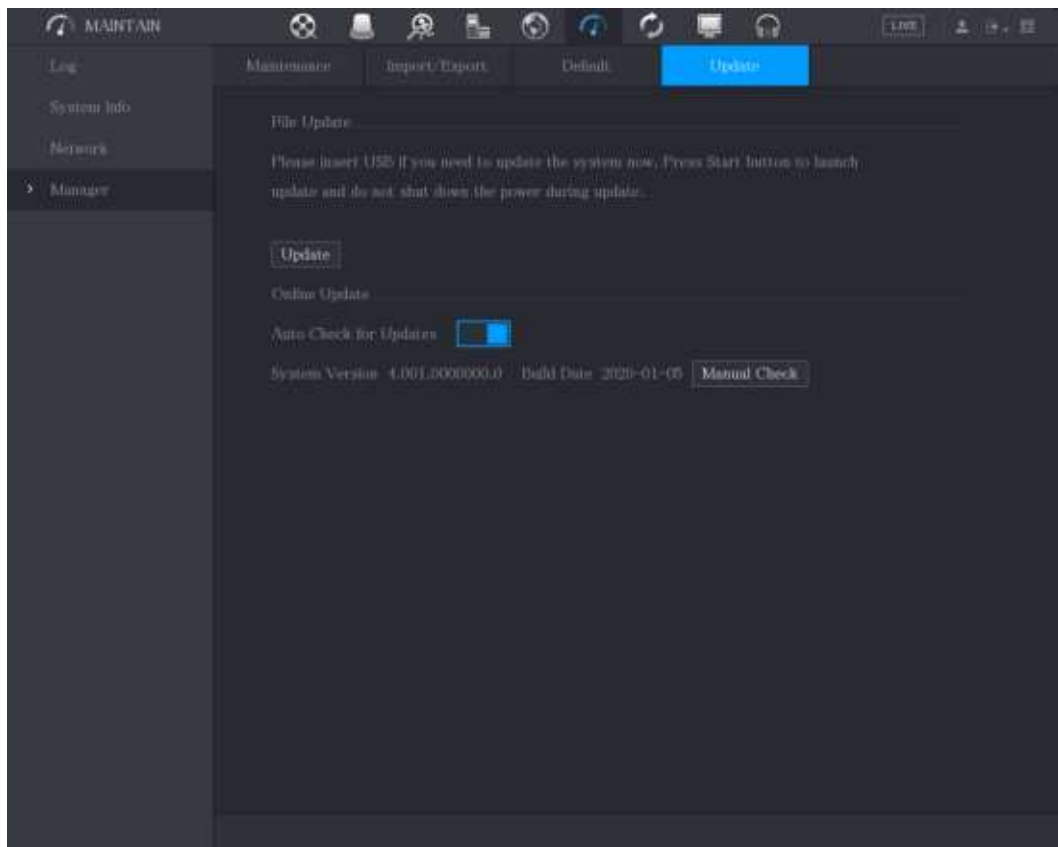


Ensure the correct power supply and network connection during upgrading; otherwise the upgrading might be failed.

Step 1 Select **Main Menu > MAINTAIN > Manager > Update**.

The **Update** interface is displayed.

Figure 5-339



Step 2 Check whether there is any new version available.

- Auto check : Enable Auto-check for updates.
- Manual check: Click **Manual Check**.

The system starts checking the new versions. After checking is completed, the check result is displayed.

- If the "It is the latest version" text is displayed, you do not need to upgrade.
- If the text indicating there is a new version, go the step 3.

Step 3 Click **Upgrade now**.

5.20.6.3 Uboot Upgrading



- Under the root directory in the USB storage device, there must be "u-boot.bin.img" file and "update.img" file saved, and the USB storage device must be in FAT32 format.
- Make sure the USB storage device is inserted; otherwise the upgrading cannot be performed.

When starting the Device, the system automatically check whether there is a USB storage device connected and if there is any upgrade file, and if yes and the check result of the upgrade file is correct, the system will upgrade automatically. The Uboot upgrade can avoid the situation that you have to upgrade through +TFTP when the Device is halted.

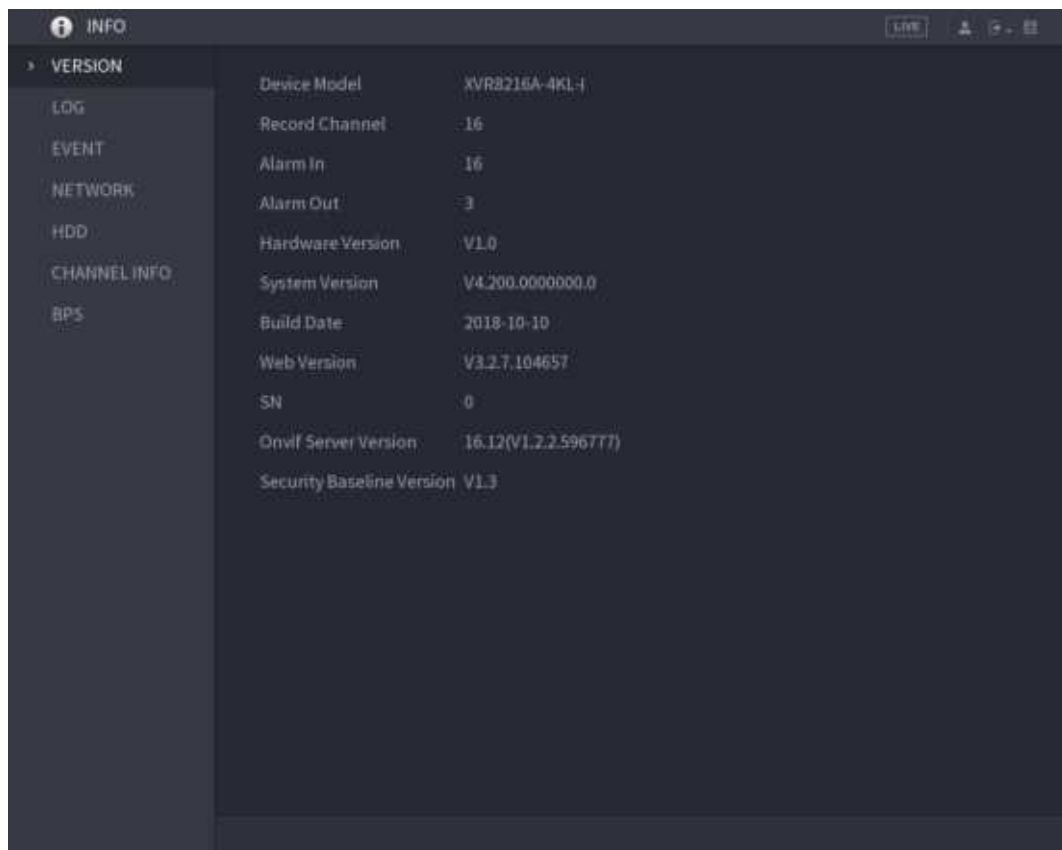
5.21 Viewing Information

You can view the information such as log information, HDD information, and version details

5.21.1 Viewing Version Details

You can view the version details such as device model, system version, and build date.

Select **Main Menu > INFO > VERSION**, the **VERSION** interface is displayed.



5.21.2 Viewing Log Information

You can view and search the log information.

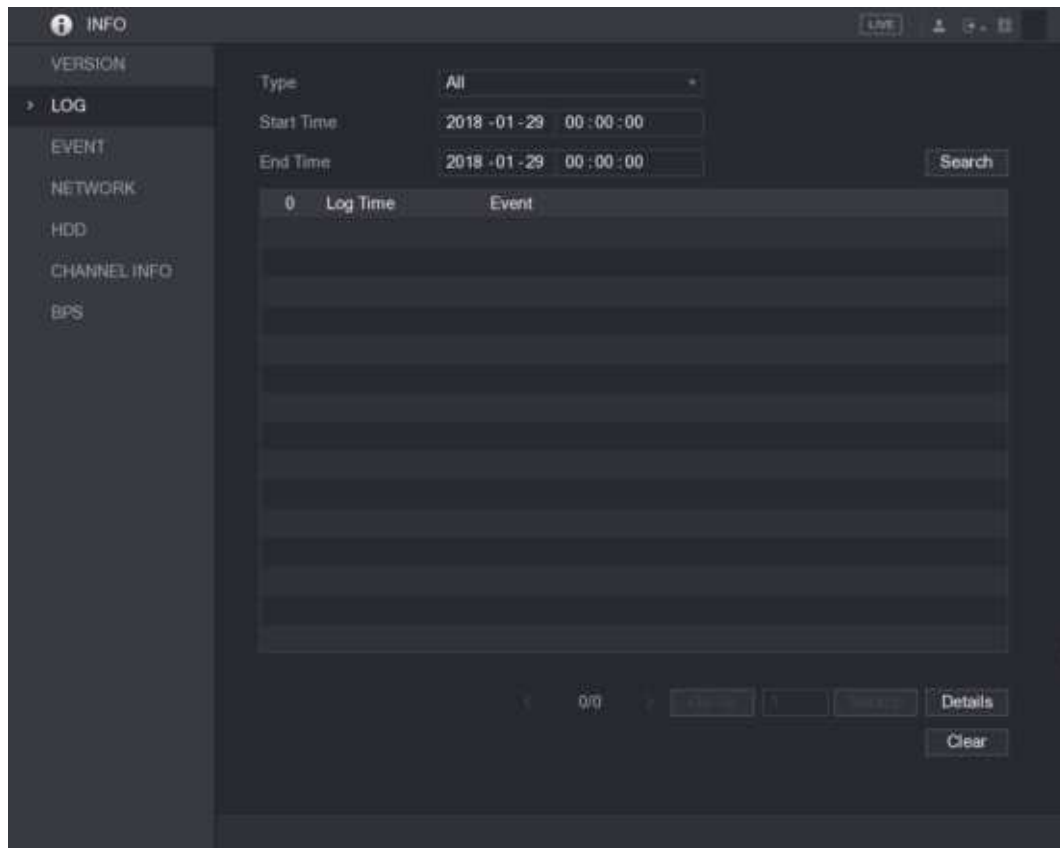


- If there is no HDD installed, the system can save up to 10,000 logs.
- If there is HDD installed and has been formatted, the system can save up to 500,000 logs.
- If there is HDD installed, the logs about system operations are saved in the memory of the Device and other types of logs are saved into the HDD. If there is no HDD installed, the other types of logs are also saved in the memory of the Device.
- When formatting the HDD, the logs will not be lost. However, if you take out the HDD from the Device, the logs might be lost.

Step 1 Select **Main Menu > INFO > LOG**.

The **LOG** interface is displayed.

Figure 5-340

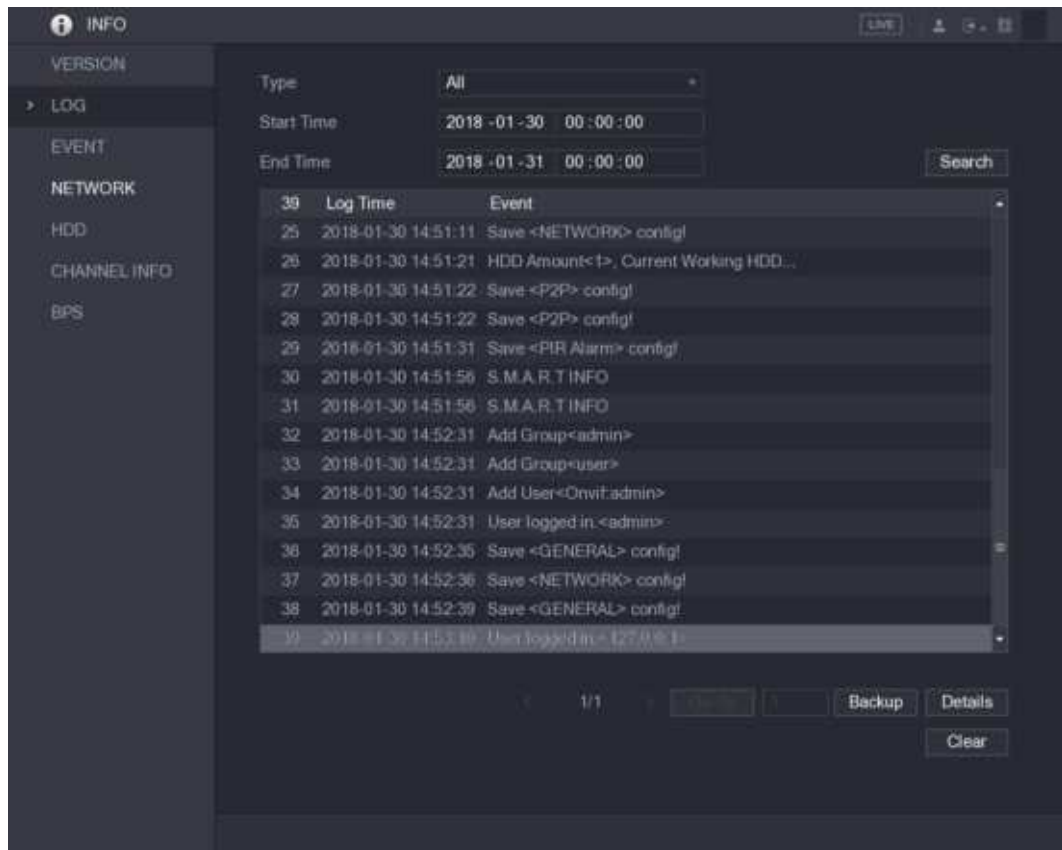


Step 2 In the **Type** list, select the log type that you want to view (**System, Config, Storage, Record, Account, Clear, Playback, and Connection**) or select **All** to view all logs.

Step 3 In the **Start Time** box and **End Time** box, enter the time period to search, and then click **Search**.

The search results are displayed.

Figure 5-341



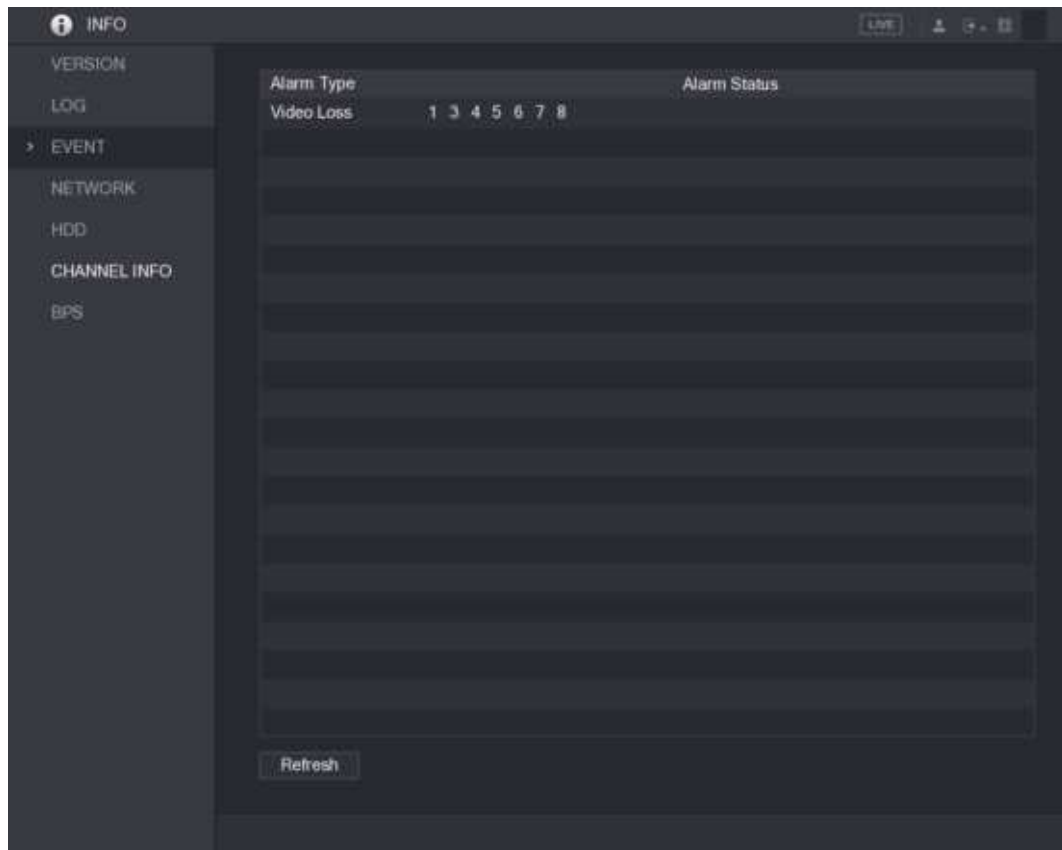
- Click **Details** or double-click the log that you want to view, the **Detailed Information** interface is displayed. Click **Next** or **Previous** to view more log information.
- Click **Backup** to back up the logs into the USB storage device.
- Click **Clear** to remove all logs.

5.21.3 Viewing Event Information

You can view the event information of the Device and channel.

Select **Main Menu > INFO > EVENT**, the **EVENT** interface is displayed.

Figure 5-342



5.21.4 Viewing Network Information

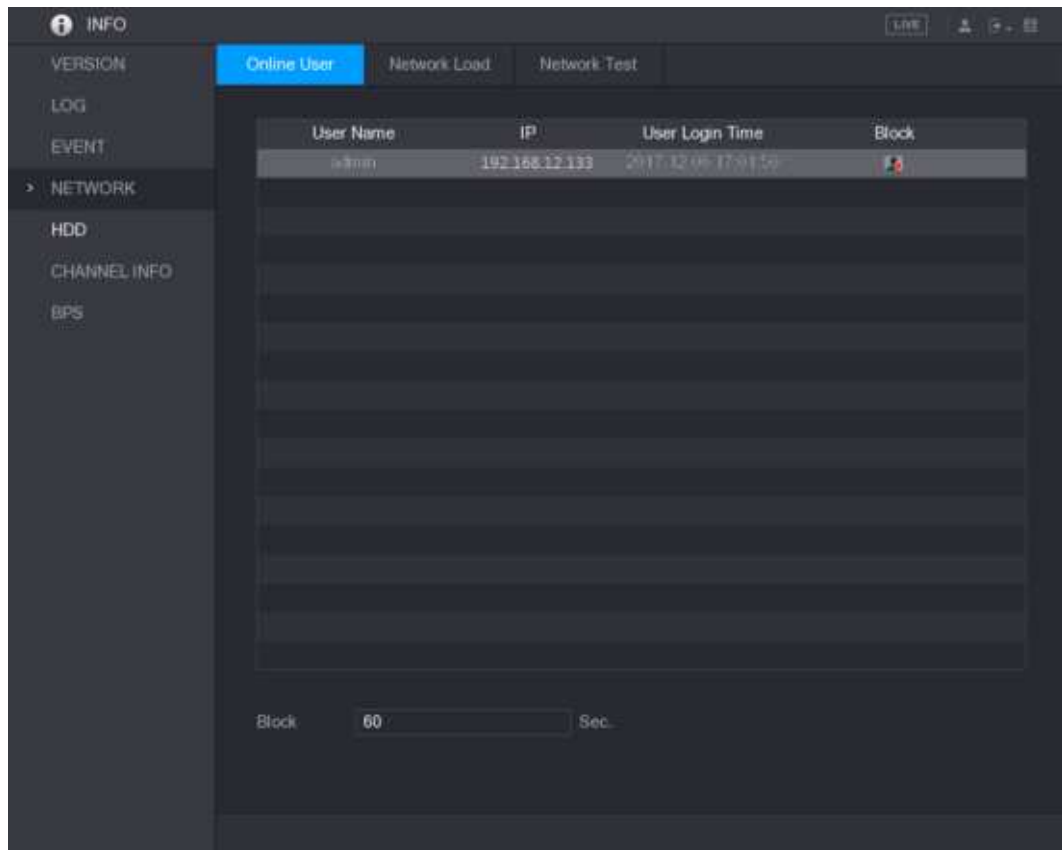
You can view the online users, network data transmission details, and test network. For details about testing network, see "5.15.2.1 Testing the Network."

5.21.4.1 Viewing Online Users

You can view the online user information and block any user for a period of time.

Select **Main Menu > INFO > NETWORK > Online users**, the **Online users** interface is displayed.

Figure 5-343



To block an online user, click  and then enter the time that you want to block this user. The maximum value you can set is 65535.

The system detects every 5 seconds to check whether there is any user added or deleted, and update the user list timely.

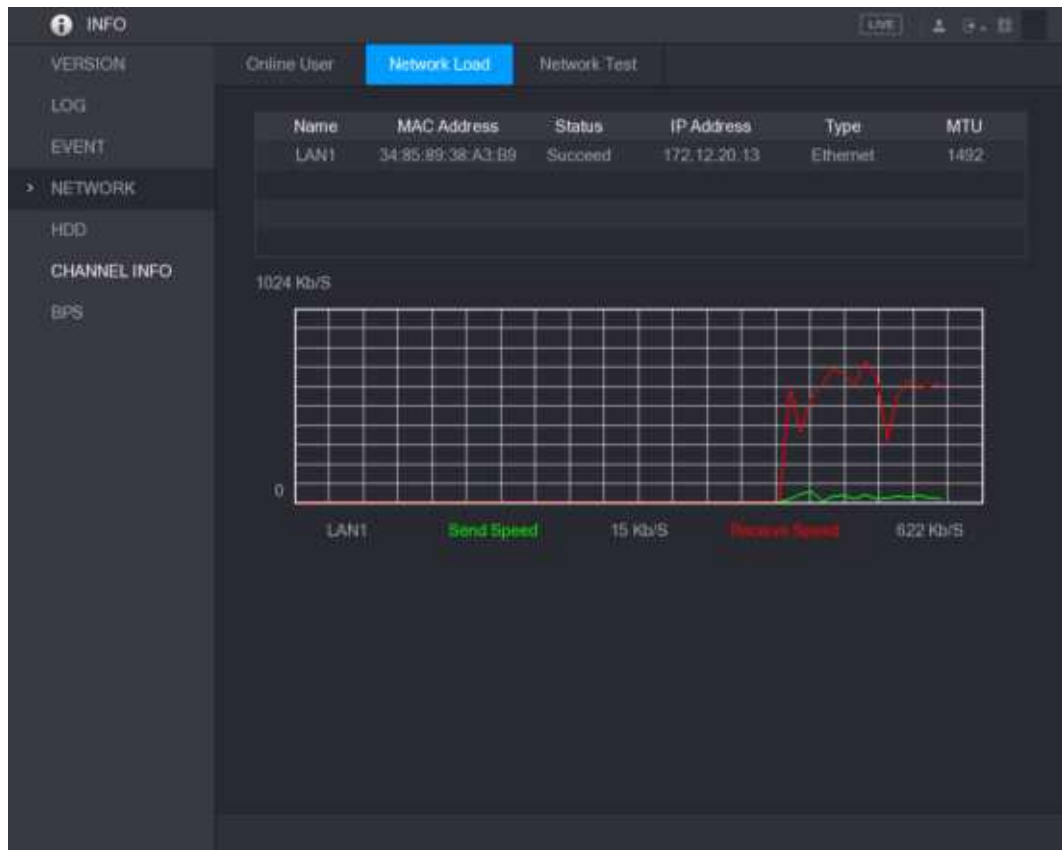
5.21.4.2 Viewing the Network Load

Network load means the data flow which measures the transmission capability. You can view the information such as data receiving speed and sending speed.

Step 1 Select **Main Menu > INFO > NETWORK > Network Load**.

The **Network Load** interface is displayed.

Figure 5-344



Step 2 Click the LAN name that you want to view, for example, LAN1.
The system displays the information of data sending speed and receiving speed.



- The default display is LAN1 load.
- Only one LAN load can be displayed at one time.

5.21.5 Viewing HDD Information

You can view the HDD quantity, HDD type, total space, free space, status, and S.M.A.R.T information.

Select **Main Menu > INFO > HDD**, the **HDD** interface is displayed.

Figure 5-345

1*	Device Name	Physical Position	Type	Total Space	Free Space
1*	sda	main board-1	Read/Write	2.72 TB	0.00 MB

Table 5-89

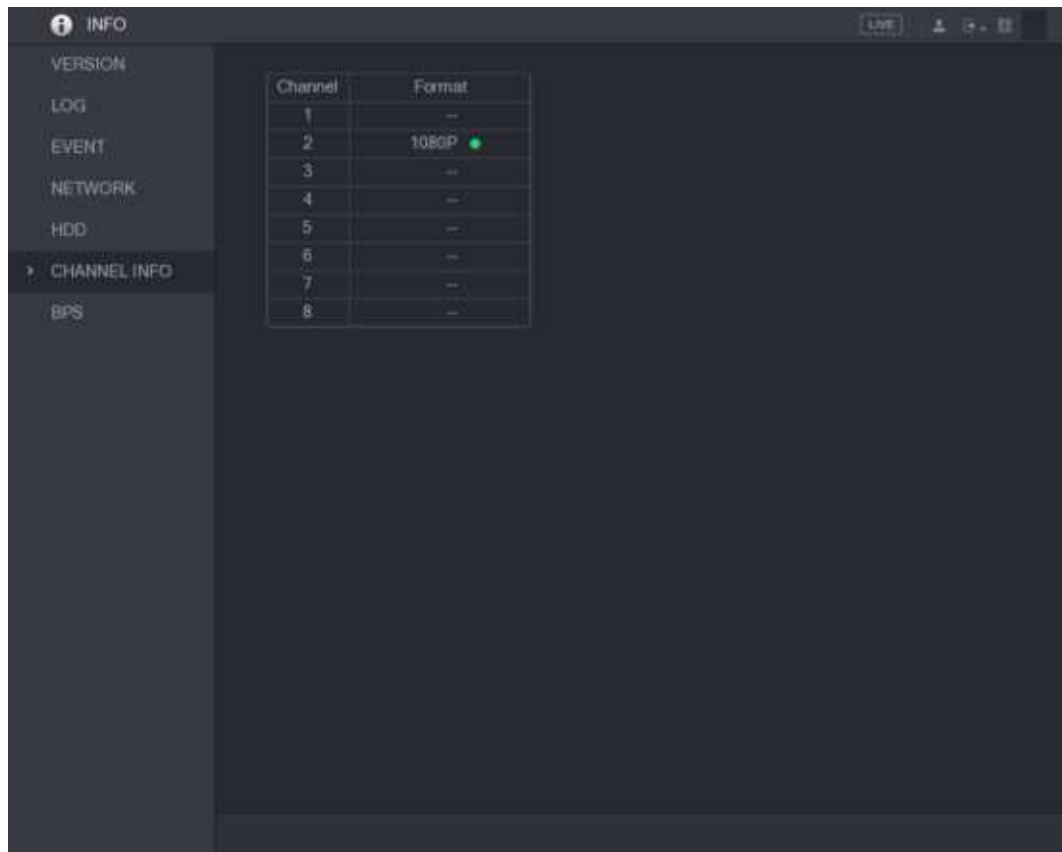
Parameter	Description
No.	Indicates the number of the currently connected HDD. The asterisk (*) means the current working HDD.
Device Name	Indicates name of HDD.
Physical Position	Indicates installation position of HDD.
Type	Indicates HDD type.
Total Space	Indicates the total capacity of HDD.
Free Space	Indicates the usable capacity of HDD.
Status	Indicates the status of the HDD to show if it is working normally.
S.M.A.R.T	View the S.M.A.R.T reports from HDD detecting.

5.21.6 Viewing Channel Information

You can view the camera information connected to each channel.

Select **Main Menu > INFO > CHANNEL INFO**, the **CHANNEL INFO** interface is displayed.

Figure 5-346

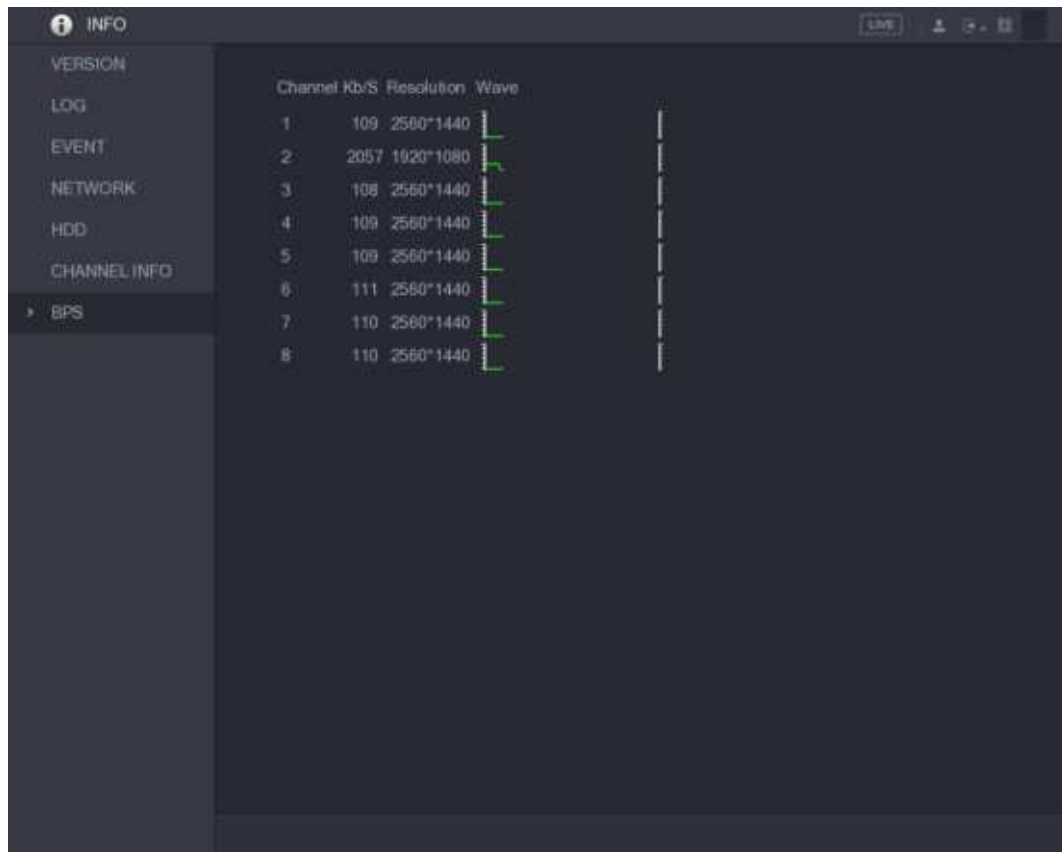


5.21.7 Viewing Data Stream Information

You can view the real-time data stream rate and resolution of each channel.

Select **Main Menu > INFO > BPS**, the **BPS** interface is displayed.

Figure 5-347



5.22 Logout the Device

On the top right of the Main Menu interface or on any interface after you have entered the Main

Menu, click .

- Select **Logout**, you will log out the device.
- Select **Reboot**, the Device will be rebooted.
- Select **Shutdown**, the Device will be turned off.

6 Web Operations



- The interfaces in the Manual are used for introducing the operations and only for reference. The actual interface might be different dependent on the model you purchased. If there is inconsistency between the Manual and the actual product, the actual product shall govern.
- The Manual is a general document for introducing the product, so there might be some functions described for the Device in the Manual not apply to the model you purchased.
- Besides Web, you can use our Smart PSS to login the device. For detailed information, please refer to Smart PSS user's manual.

6.1 Connecting to Network



- The factory default IP of the Device is 192.168.1.108.
- The Device supports monitoring on different browsers such as Safari, fire fox, Google on Apple PC to perform the functions such as multi-channel monitoring, PTZ control, and device parameters configurations.

Step 1 Check to make sure the Device has connected to the network.

Step 2 Configure the IP address, subnet mask and gateway for the PC and the Device. For details about network configuration of the Device, see "5.1.4.4 Configuring Network Settings."

Step 3 On your PC, check the network connection of the Device by using "ping ***.***.***.***". Usually the return value of TTL is 255.

6.2 Logging in the Web

Step 1 Open the IE browser, enter the IP address of the Device, and then press Enter. The Login in dialog box is displayed.

Figure 6-1

The image shows a 'Web Login' dialog box with a dark background. It contains three input fields: a username field with a person icon, a password field with a lock icon and a toggle eye icon, and a protocol dropdown menu currently set to 'TCP'. At the bottom is a large blue 'Login' button.

Step 2 Enter the user name and password.



- The default administrator account is **admin**. The password is the one that was configured during initial settings. To security your account, it is recommended to keep the password properly and change it regularly.
- Click  to display the password.

Step 3 Click **Login**.

6.3 Introducing Web Main Menu

After you have logged in the Web, the main menu is displayed.

Figure 6-2



Table 6-1

No.	Icon	Description
1		Includes configuration menu through which you can configure camera settings, network settings, storage settings, system settings, account settings, and view information.
2	None	Displays system date and time.
3		When you point to  , the current user account is displayed.
4		Click  , select Logout , Reboot , or Shutdown according to your actual situation.

No.	Icon	Description
5		Displays Cell Phone Client and Device SN QR Code. • Cell Phone Client: Use your mobile phone to scan the QR code to add the device into the Cell Phone Client, and then you can start accessing the Device from your cell phone. • Device SN: Obtain the Device SN by scanning the QR code. Go to the P2P management platform and add the Device SN into the platform. Then you can access and manage the device in the WAN. For details, please refer to the P2P operation manual. You can also configure P2P function in the local configurations. See "5.1.4.5 Configuring P2P Settings."
6		Displays the web main menu.
7	None	Includes eight function tiles: LIVE, VIDEO, ALARM, IoT, AI, BACKUP, DISPLAY, and AUDIO. Click each tile to open the configuration interface of the tile. • LIVE: You can perform the operations such as viewing real-time video, configuring channel layout, setting PTZ controls, and using smart talk and instant record functions if needed. • VIDEO: Search for and play back the recorded video saved on the Device. • ALARM: Search for alarm information and configure alarm event actions. • AI: Configure face detection, face recognition, and IVS functions. • IoT: You can view, search and export the temperature and humidity data of camera and configure the alarm event settings. • BACKUP: Search and back up the video files to the local PC or external storage device such as USB storage device. • DISPLAY: Configure the display effect such as displaying content, image transparency, and resolution, and enable the zero-channel function. • AUDIO: Manage audio files and configure the playing schedule. The audio file can be played in response to an alarm event if the voice prompts function is enabled.

1. DVR cannot boot up properly.

There are following possibilities:

- Input power is not correct.
- Power connection is not correct.
- Power switch button is damaged.
- Program upgrade is wrong.
- HDD malfunction or something wrong with HDD jumper configuration.
- Seagate DB35.1, DB35.2, SV35 or Maxtor 17-g has compatibility problem. Please upgrade to the latest version to solve this problem.
- Front panel error.
- Main board is damaged.

2. DVR frequently shuts down or stops running.

There are following possibilities:

- Input voltage is not stable or it is too low.
- HDD malfunction or something wrong with jumper configuration.
- Button power is not enough.
- Front video signal is not stable.
- Working environment is too harsh, too much dust.
- Hardware malfunction.

3. Hard disk cannot be detected.

There are following possibilities:

- HDD is broken.
- HDD jumper is damaged.
- HDD cable connection is loose.
- Main board SATA port is broken.

4. There is no video output whether it is one-channel, multiple-channel or all-channel output.

There are following possibilities:

- Program is not compatible. Please upgrade to the latest version.
- Brightness is 0. Please restore factory default setup.
- There is no video input signal or it is too weak.
- Check privacy mask setup or your screen saver.
- DVR hardware malfunctions.

5. Real-time video color is distorted.

There are following possibilities:

- When using BNC output, NTSC and PAL setup is not correct. The real-time video becomes black and white.
- DVR and monitor resistance is not compatible.
- Video transmission is too long or degrading is too huge.
- DVR color or brightness setup is not correct.

6. Cannot search local records.

There are following possibilities:

- HDD jumper is damaged.
- HDD is broken.
- Upgraded program is not compatible.
- The recorded file has been overwritten.
- Record function has been disabled.

7. Video is distorted when searching local records.

There are following possibilities:

- Video quality setup is too low.
- Program read error, bit data is too small. There is mosaic in the full screen. Please restart the DVR to solve this problem.
- HDD data jumper error.
- HDD malfunction.
- DVR hardware malfunctions.

8. No audio under monitor state.

There are following possibilities:

- It is not a power picker.
- It is not a power acoustics.
- Audio cable is damaged.
- DVR hardware malfunctions.

9. There is audio under monitor state but no audio under playback state.

There are following possibilities:

- Setup is not correct. Please enable audio function.
- Corresponding channel has no video input. Playback is not continuous when the screen is blue.

10. System time is not correct.

There are following possibilities:

- Setup is not correct.
- Battery contact is not correct or voltage is too low.
- Crystal oscillator is broken.

11. Cannot control PTZ on DVR.

There are following possibilities:

- Front panel PTZ error.
- PTZ decoder setup, connection or installation is not correct.
- Cable connection is not correct.
- PTZ setup is not correct.
- PTZ decoder and DVR protocol is not compatible.
- PTZ decoder and DVR address is not compatible.
- When there are several decoders, please add 120 Ohm between the PTZ decoder A/B cables furthest end to delete the reverberation or impedance matching. Otherwise the PTZ control is not stable.
- The distance is too far.

12. Motion detection function does not work.

There are following possibilities:

- Period setup is not correct.
- Motion detection zone setup is not correct.
- Sensitivity is too low.

- For some versions, there is hardware limit.

13. Cannot log in client-end or web.

There are following possibilities:

- For Windows 98 or Windows ME user, please update your system to Windows 2000 sp4. Or you can install client-end software of lower version. Please note right now, our DVR is not compatible with Windows VISTA control.
- ActiveX control has been disabled.
- No dx8.1 or higher. Please upgrade display card driver.
- Network connection error.
- Network setup error.
- Password or user name is invalid.
- Client-end is not compatible with DVR program.

14. There is only mosaic no video when preview or playback video file remotely.

There are following possibilities:

- Network fluency is not good.
- Client-end resources are limit.
- There is multiple-cast group setup in DVR. This mode can result in mosaic. Usually we do not recommend this mode.
- There is privacy mask or channel protection setup.
- Current user has no right to monitor.
- DVR local video output quality is not good.

15. Network connection is not stable.

There are following possibilities:

- Network is not stable.
- IP address conflict.
- MAC address conflict.
- PC or DVR network card is not good.

16. Burn error /USB back error.

There are following possibilities:

- Burner and DVR are in the same data cable.
- System uses too much CPU resources. Please stop record first and then begin backup.
- Data amount exceeds backup device capacity. It might result in burner error.
- Backup device is not compatible.
- Backup device is damaged.

17. Keyboard cannot control DVR

There are following possibilities:

- DVR serial port setup is not correct.
- Address is not correct.
- When there are several switchers, power supply is not enough.
- Transmission distance is too far.

18. Alarm signal cannot be disarmed.

There are following possibilities:

- Alarm setup is not correct.
- Alarm output has been open manually.
- Input device error or connection is not correct.
- Some program versions might have this problem. Please upgrade your system.

19. Alarm function is null.

There are following possibilities:

- Alarm setup is not correct.
- Alarm cable connection is not correct.
- Alarm input signal is not correct.
- There are two loops connect to one alarm device.

20. Remote control does not work.

There are following possibilities:

- Remote control address is not correct.
- Distance is too far or control angle is too small.
- Remote control battery power is low.
- Remote control is damaged or DVR front panel is damaged.

21. Record storage period is not enough.

There are following possibilities:

- Camera quality is too low. Lens is dirty. Camera is installed against the light. Camera aperture setup is not correct.
- HDD capacity is not enough.
- HDD is damaged.

22. Cannot playback the downloaded file.

There are following possibilities:

- There is no media player.
- No DXB8.1 or higher graphic acceleration software.
- There is no DivX503Bundle.exe control when you play the file transformed to AVI via media player.
- No DivX503Bundle.exe or ffdshow-2004 1012 .exe in Windows XP OS.

23. Forgot local menu operation password or network password

Please contact your local service engineer or our sales person for help. We can guide you to solve this problem.

24. When I login via HTTPS, a dialogue says the certificate for this website is for other address.

Please create server certificate again.

25. When I login via HTTPS, a dialogue says the certificate is not trusted.

Please download root certificate again.

26. When I login via HTTPS, a dialogue says the certificate has expired or is not valid yet.

Please make sure your PC time is the same as the device time.

27. I connect the general analog camera to the device, there is no video output.

There are following possibilities:

- Check camera power supplying, data cable connection and other items.
- This series device does not support the analog camera of all brands. Please make sure the device supports general standard definition analog camera.

28. I connect the standard definition analog camera or the coaxial camera to the device, there is no video output.

There are following possibilities:

- Check camera power supplying, or camera data cable connection.

- For the product supports analog standard definition camera/HD camera, you need to go to the **Main Menu > CAMERA > CHANNEL TYPE** to select corresponding channel type and then restart the DVR.

29. I cannot connect to the IP channel.

There are following possibilities:

- Check the camera is online or not.
- Check IP channel setup is right or not (such as IP address, user name, password, connection protocol, and port number).
- The camera has set the whitelist (Only the specified devices can connect to the camera).

30. After I connected to the IP channel, the one-window output is OK, but there is no multiple-window output.

There are following possibilities:

- Check the sub stream of the camera has been enabled or not.
- Check the sub stream type of the camera is H.264 or not.
- Check the device supports camera sub stream resolution or not (such as 960H, D1, and HD1).

31. After I connected to the IP channel, the multiple-window output is OK, but there is no one-window output.

There are following possibilities:

- Check there is video from the IP channel or not. Please go to the **Main Menu > INFO > BPS** to view bit stream real-time information.
- Check the main stream of the camera has been enabled or not.
- Check the main stream type of the camera is H.264 or not.
- Check the device supports camera main stream resolution or not (such as 960H, D1, and HD1).
- Check camera network transmission has reached the threshold or not. Please check the online user of the camera.

32. After I connected to the IP channel, there is no video output in the one-window or the multiple-window mode. But I can see there is bit stream.

There are following possibilities:

- Check the main stream/sub stream type of the camera is H.264 or not.
- Check the device supports camera main stream/sub stream resolution or not (such as 1080P, 720P, 960H, D1, and HD1).
- Check the camera setup. Please make sure It supports the products of other manufacturers.

33. DDNS registration failed or cannot access the device domain name.

There are following possibilities:

- Check the device is connected to the WAN. Please check the device has got the IP address if the PPPoE can dial. If there is a router, please check the router to make sure the device IP is online.
- Check the corresponding protocol of the DDNS is enabled. Check the DDNS function is OK or not.
- Check DNS setup is right or not. Default Google DNS server is 8.8.8.8, 8.8.5.5. You can use different DNS provided by your ISP.

34. I cannot use the P2P function on my cell phone or the WEB.

There are following possibilities:

- Check the device P2P function is enabled or not. (Main menu->Setting->Network->P2P)
- Check the device is in the WAN or not.
- Check cell phone P2P login mode is right or not.
- It is the specified device P2P login port or not when you are using P2P client.
- Check user name or password is right or not.
- Check P2P SN is right or not. You can use the cell phone to scan the QR code on the device P2P interface (**Main Menu > Network > P2P**), or you can use the version information of the WEB to confirm. (For some previous series products, the device SN is the main board SN, it might result in error.)

35. I connect the standard definition camera to the device, there is no video output.

There are following possibilities:

- Check the DVR supports standard definition signal or not. Only some series product supports analog standard definition signal, coaxial signal input.
- Check channel type is right or not. For the product supports analog standard definition camera/HD camera, you need to go to the **Main Menu > CAMERA > CHANNEL TYPE** to select corresponding channel type (such as analog) and then restart the DVR. In this way, the DVR can recognize the analog standard definition.
- Check camera power supplying, or camera data cable connection.

36. I cannot connect to the IP camera.

There are following possibilities:

- Check DVR supports IP channel or not. Only some series products support A/D switch function, it can switch analog channel to the IP channel to connect to the IP camera. From **Main Menu > CAMERA > CHANNEL TYPE**, select the last channel to switch to the IP channel. Some series product products support IP channel extension, it supports N+N mode.
- Check the IPC and the DVR is connected or not. Please go to the **Main Menu > CAMERA > REGISTRATION** to search to view the IP camera is online or not. Or you can go to the **Main Menu > INFO > NETWORK > Network Test**, you can input IP camera IP address and then click the Test button to check you can connect to the IP camera or not.
- Check IP channel setup is right or not (such as IP address, manufacturer, port, user name, password, and remote channel number).

Daily Maintenance

- Please use the brush to clean the board, socket connector and the chassis regularly.
- The device shall be soundly earthed in case there is audio/video disturbance. Keep the device away from the static voltage or induced voltage.
- Please unplug the power cable before you remove the audio/video signal cable, RS-232 or RS-485 cable.
- Do not connect the TV to the local video output port (VOUT).It might result in video output circuit.
- Always shut down the device properly. Please use the shutdown function in the menu, or you can press the power button in the front panel for at least three seconds to shut down the device. Otherwise it might result in HDD malfunction.
- Please make sure the device is away from the direct sunlight or other heating sources. Please keep the sound ventilation.
- Please check and maintain the device regularly.

Appendix 1 Glossary

The abbreviations in this glossary are related to the Manual.

Abbreviations	Full term
BNC	Bayonet Nut Connector
CBR	Constant Bit Rate
CIF	Common Intermediate Format
DDNS	Dynamic Domain Name Service
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DST	Daylight Saving Time
DVR	Digital Video Recorder
FTP	File Transfer Protocol
HDD	Hard Disk Drive
HDMI	High Definition Multimedia Interface
HTTP	Hyper Text Transfer Protocol
IoT	Internet of Things
IP	Internet Protocol
IVS	Intelligent Video System
LAN	Local Area Network
MAC	Media Access Control
MTU	Maximum Transmission Unit
NTP	Network Time Protocol
NTSC	National Television Standards Committee
ONVIF	Open Network Video Interface Forum
PAL	Phase Alteration Line
PAT	Port Address Translation
POS	Point of Sale
PPPoE	Point-to-Point Protocol over Ethernet
PSS	Professional Surveillance Software
PTZ	Pan Tilt Zoom
RCA	Radio Corporation of American
RTSP	Real Time Streaming Protocol
S.M.A.R.T	Self-Monitoring-Analysis and Reporting Technology
SATA	Serial Advanced Technology Attachment
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
UDP	User Datagram Protocol
UPnP	Universal Plug and Play
VBR	Variable Bit Rate

Abbreviations	Full term
VGA	Video Graphics Array
WAN	Wide Area Network

Appendix 2 HDD Capacity Calculation

Calculate total capacity needed by each DVR according to video recording (video recording type and video file storage time).

Step 1 According to Formula (1) to calculate storage capacity q_i that is the capacity of each channel needed for each hour, unit MB.

$$\text{Formula (1): } q_i = d_i \div 8 \times 3600 \div 1024$$

In the formula: d_i means the bit rate, unit Kbit/s

Step 2 After video time requirement is confirmed, according to Formula (2) to calculate the storage capacity m_i , which is storage of each channel needed unit MB.

$$\text{Formula (2): } m_i = q_i \times h_i \times D_i$$

In the formula:

- h_i means the recording time for each day (hour)
- D_i means number of days for which the video shall be kept

Step 3 According to Formula (3) to calculate total capacity (accumulation) q_T that is needed for all channels in the DVR during **scheduled video recording**.

$$\text{Formula (3): } q_T = \sum_{i=1}^c m_i$$

In the formula: c means total number of channels in one DVR

Step 4 According to Formula (4) to calculate total capacity (accumulation) q_T that is needed for all channels in DVR during **alarm video recording (including motion detection)**.

$$\text{Formula (4): } q_T = \sum_{i=1}^c m_i \times a\%$$

In the formula: $a\%$ means alarm occurrence rate

You can refer to the following table for the file size in one hour per channel. (All the data listed below are for reference only.)

Bit Stream Size (max)	File Size	Bit Stream Size (max)	File Size
96Kbps	42MB	128Kbps	56MB
160Kbps	70MB	192Kbps	84MB
224Kbps	98MB	256Kbps	112MB
320Kbps	140MB	384Kbps	168MB
448Kbps	196MB	512Kbps	225MB

Bit Stream Size (max)	File Size	Bit Stream Size (max)	File Size
640Kbps	281MB	768Kbps	337MB
896Kbps	393MB	1024Kbps	450MB
1280Kbps	562MB	1536Kbps	675MB
1792Kbps	787MB	2048Kbps	900MB

Appendix 3 Compatible Backup Devices

Appendix 3.1 Compatible USB list

Manufacturer	Model	Capacity
Sandisk	Cruzer Micro	512MB
Sandisk	Cruzer Micro	1GB
Sandisk	Cruzer Micro	2GB
Sandisk	Cruzer Freedom	256MB
Sandisk	Cruzer Freedom	512MB
Sandisk	Cruzer Freedom	1GB
Sandisk	Cruzer Freedom	2GB
Kingston	DataTraveler II	1GB
Kingston	DataTraveler II	2GB
Kingston	DataTraveler	1GB
Kingston	DataTraveler	2GB
Maxell	USB Flash Stick	128MB
Maxell	USB Flash Stick	256MB
Maxell	USB Flash Stick	512MB
Maxell	USB Flash Stick	1GB
Maxell	USB Flash Stick	2GB
Kingax	Super Stick	128MB
Kingax	Super Stick	256MB
Kingax	Super Stick	512MB
Kingax	Super Stick	1GB
Kingax	Super Stick	2GB
Netac	U210	128MB
Netac	U210	256MB
Netac	U210	512MB
Netac	U210	1GB
Netac	U210	2GB
Netac	U208	4GB
Teclast	Ti Cool	128MB
Teclast	Ti Cool	256MB
Teclast	Ti Cool	512MB
Teclast	Ti Cool	1GB
Sandisk	Cruzer Micro	2GB
Sandisk	Cruzer Micro	8GB
Sandisk	Ti Cool	2GB
Sandisk	Hongjiao	4GB
Lexar	Lexar	256MB

Manufacturer	Model	Capacity
Kingston	Data Traveler	1GB
Kingston	Data Traveler	16GB
Kingston	Data Traveler	32GB
Aigo	L8315	16GB
Sandisk	250	16GB
Kingston	Data Traveler Locker+	32GB
Netac	U228	8GB

Appendix 3.2 Compatible SD Card list

Manufacturer	Standard	Capacity	Card type
Transcend	SDHC6	16GB	Big
Kingston	SDHC4	4GB	Big
Kingston	SD	2GB	Big
Kingston	SD	1GB	Big
Sandisk	SDHC2	8GB	Small
Sandisk	SD	1GB	Small

Appendix 3.3 Compatible Portable HDD list

Manufacturer	Model	Capacity
YDStar	YDstar HDD box	40GB
Netac	Netac	80GB
Iomega	Iomega RPHD-CG" RNAJ50U287	250GB
WD Elements	WCAVY1205901	1.5TB
Newsmy	Liangjian	320GB
WD Elements	WDBAAR5000ABK-00	500GB
WD Elements	WDBAAU0015HBK-00	1.5TB
Seagate	FreeAgent Go(ST905003F)	500GB
Aigo	H8169	500GB

Appendix 3.4 Compatible USB DVD List

Manufacturer	Model
Samsung	SE-S084
BenQ	LD2000-2K4

Appendix 3.5 Compatible SATA DVD List

Manufacturer	Model
LG	GH22NS30

Manufacturer	Model
Samsung	TS-H653 Ver.A
Samsung	TS-H653 Ver.F
Samsung	SH-224BB/CHXH
SONY	DRU-V200S
SONY	DRU-845S
SONY	AW-G170S
Pioneer	DVR-217CH

Appendix 3.6 Compatible SATA HDD List



Please upgrade the DVR firmware to latest version to ensure the accuracy of the table below.

Here we recommend HDD of 500GB to 4TB capacity.

Manufacturer	Series	Model	Capacity	Port Mode
Seagate	Video 3.5	ST1000VM002	1TB	SATA
Seagate	Video 3.5	ST2000VM003	2TB	SATA
Seagate	Video 3.5	ST3000VM002	3TB	SATA
Seagate	Video 3.5	ST4000VM000	4TB	SATA
Seagate	SV35	ST1000VX000	1TB	SATA
Seagate	SV35	ST2000VX000	2TB	SATA
Seagate	SV35	ST3000VX000	3TB	SATA
Seagate	SV35 (Support HDD data recovery offered by Seagate)	ST1000VX002	1TB	SATA
Seagate	SV35 (Support HDD data recovery offered by Seagate)	ST2000VX004	2TB	SATA
Seagate	SV35 (Support HDD data recovery offered by Seagate)	ST3000VX004	3TB	SATA
Seagate	SkyHawk HDD	ST1000VX001	1TB	SATA
Seagate	SkyHawk HDD	ST1000VX005	1TB	SATA
Seagate	SkyHawk HDD	ST2000VX003	2TB	SATA
Seagate	SkyHawk HDD	ST2000VX008	2TB	SATA
Seagate	SkyHawk HDD	ST3000VX006	3TB	SATA
Seagate	SkyHawk HDD	ST3000VX010	3TB	SATA
Seagate	SkyHawk HDD	ST4000VX000	4TB	SATA
Seagate	SkyHawk HDD	ST4000VX007	4TB	SATA
Seagate	SkyHawk HDD	ST5000VX0001	5TB	SATA
Seagate	SkyHawk HDD	ST6000VX0001	6TB	SATA
Seagate	SkyHawk HDD	ST6000VX0023	6TB	SATA
Seagate	SkyHawk HDD	ST6000VX0003	6TB	SATA
Seagate	SkyHawk HDD	ST8000VX0002	8TB	SATA
Seagate	SkyHawk HDD	ST8000VX0022	8TB	SATA

Manufacturer	Series	Model	Capacity	Port Mode
Seagate	SkyHawk HDD	ST100000VX0004	10TB	SATA
Seagate	SkyHawk HDD (Support HDD data recovery offered by Seagate)	ST1000VX003	1TB	SATA
Seagate	(Support HDD data recovery offered by Seagate)	ST2000VX005	2TB	SATA
Seagate	(Support HDD data recovery offered by Seagate)	ST3000VX005	3TB	SATA
Seagate	(Support HDD data recovery offered by Seagate)	ST4000VX002	4TB	SATA
Seagate	(Support HDD data recovery offered by Seagate)	ST5000VX0011	5TB	SATA
Seagate	(Support HDD data recovery offered by Seagate)	ST6000VX0011	6TB	SATA
Seagate	(Support HDD data recovery offered by Seagate)	ST8000VX0012	8TB	SATA
WD	WD Green	WD10EURX (EOL)	1TB	SATA
WD	WD Green	WD20EURX (EOL)	2TB	SATA
WD	WD Green	WD30EURX (EOL)	3TB	SATA
WD	WD Green	WD40EURX (EOL)	4TB	SATA
WD	WD Purple	WD10PURX	1TB	SATA
WD	WD Purple	WD20PURX	2TB	SATA
WD	WD Purple	WD30PURX	3TB	SATA
WD	WD Purple	WD40PURX	4TB	SATA
WD	WD Purple	WD50PURX	5TB	SATA
WD	WD Purple	WD60PURX	6TB	SATA
WD	WD Purple	WD80PUZX	8TB	SATA
WD	WD Purple	WD10PURZ	1TB	SATA
WD	WD Purple	WD20PURZ	2TB	SATA
WD	WD Purple	WD30PURZ	3TB	SATA
WD	WD Purple	WD40PURZ	4TB	SATA
WD	WD Purple	WD50PURZ	5TB	SATA
WD	WD Purple	WD60PURZ	6TB	SATA
WD	WD Purple	WD80PURZ	8TB	SATA
WD	WD Purple	WD4NPURX	4TB	SATA
WD	WD Purple	WD6NPURX	6TB	SATA
TOSHIBA	Mars	DT01ABA100V	1TB	SATA
TOSHIBA	Mars	DT01ABA200V	2TB	SATA

Manufacturer	Series	Model	Capacity	Port Mode
TOSHIBA	Mars	DT01ABA300V	3TB	SATA
TOSHIBA	Sonance	MD03ACA200V	2TB	SATA
TOSHIBA	Sonance	MD03ACA300V	3TB	SATA
TOSHIBA	Sonance	MD03ACA400V	4TB	SATA
TOSHIBA	Sonance	MD04ABA400V	4TB	SATA
TOSHIBA	Sonance	MD04ABA500V	5TB	SATA
Seagate	Constellation ES series (SATA interface)	ST1000NM0033	1TB	SATA
Seagate	Constellation ES series (SATA interface)	ST2000NM0033	2TB	SATA
Seagate	Constellation ES series (SATA interface)	ST3000NM0033	3TB	SATA
Seagate	Constellation ES series (SATA interface)	ST4000NM0033	4TB	SATA
Seagate	Constellation ES series (SATA interface)	ST1000NM0055	1TB	SATA
Seagate	Constellation ES series (SATA interface)	ST2000NM0055	2TB	SATA
Seagate	Constellation ES series (SATA interface)	ST3000NM0005	3TB	SATA
Seagate	Constellation ES series (SATA interface)	ST4000NM0035	4TB	SATA
Seagate	Constellation ES series (SATA interface)	ST6000NM0115	6TB	SATA
Seagate	Constellation ES series (SATA interface)	ST8000NM0055	8TB	SATA
Seagate	Constellation ES series (SATA interface)	ST10000NM0016	10TB	SATA
Seagate	Constellation ES series (SATA interface)	ST4000NM0024	4TB	SATA
Seagate	Constellation ES series (SATA interface)	ST6000NM0024	6TB	SATA
Seagate	Constellation ES series (SAS interface)	ST1000NM0023	1TB	SATA
Seagate	Constellation ES series (SAS interface)	ST2000NM0023	2TB	SATA
Seagate	Constellation ES series (SAS interface)	ST3000NM0023	3TB	SATA
Seagate	Constellation ES series (SAS interface)	ST4000NM0023	4TB	SATA
Seagate	Constellation ES series (SAS interface)	ST6000NM0014	6TB	SATA
Seagate	Constellation ES series (SAS interface)	ST1000NM0045	1TB	SATA

Manufacturer	Series	Model	Capacity	Port Mode
Seagate	Constellation ES series (SAS interface)	ST2000NM0045	2TB	SATA
Seagate	Constellation ES series (SAS interface)	ST3000NM0025	3TB	SATA
Seagate	Constellation ES series (SAS interface)	ST4000NM0025	4TB	SATA
Seagate	Constellation ES series (SAS interface)	ST6000NM0095	6TB	SATA
Seagate	Constellation ES series (SAS interface)	ST6000NM0034	6TB	SATA
Seagate	Constellation ES series (SAS interface)	ST8000NM0075	8TB	SATA
WD	WD RE series (SATA interface)	WD1003FBYZ	1TB	SATA
WD	WD RE series (SATA interface)	WD1004FBYZ (replace WD1003FBYZ)	1TB	SATA
WD	WD RE series (SATA interface)	WD2000FYYZ	2TB	SATA
WD	WD RE series (SATA interface)	WD2004FBYZ (replace WD2000FYYZ)	2TB	SATA
WD	WD RE series (SATA interface)	WD3000FYYZ	3TB	SATA
WD	WD RE series (SATA interface)	WD4000FYYZ	4TB	SATA
WD	WD (SATA interface)	WD2000F9YZ	2TB	SATA
WD	WD (SATA interface)	WD3000F9YZ	3TB	SATA
WD	WD (SATA interface)	WD4000F9YZ	4TB	SATA
WD	WD (SATA interface)	WD4002FYYZ	4TB	SATA
WD	WD (SATA interface)	WD6001FSYZ	6TB	SATA
WD	WD (SATA interface)	WD6002FRYZ	6TB	SATA
WD	WD (SATA interface)	WD8002FRYZ	8TB	SATA
HITACHI	Ultrastar series (SATA interface)	HUS724030ALA640	3TB	SATA
HITACHI	Ultrastar series (SATA interface)	HUS726060ALE610	6TB	SATA
HITACHI	Ultrastar series (SATA interface)	HUH728060ALE600	6TB	SATA
HITACHI	Ultrastar series (SATA interface)	HUH728080ALE600	8TB	SATA
HITACHI	Ultrastar series (SAS interface)	HUS726020AL5210	2TB	SATA
HITACHI	Ultrastar series (SAS interface)	HUS726040AL5210	4TB	SATA

Manufacturer	Series	Model	Capacity	Port Mode
HITACHI	Ultrastar series (SAS interface)	HUS726060AL5210	6TB	SATA
Seagate	Pipeline HD Mini	ST320VT000	320GB	SATA
Seagate	Pipeline HD Mini	ST500VT000	500GB	SATA
Seagate	Pipeline HD Mini	ST2000LM003 (EOL)	2TB	SATA
TOSHIBA	2.5-inch PC series	MQ01ABD050V	500GB	SATA
TOSHIBA	2.5-inch PC series	MQ01ABD100V	1TB	SATA
SAMSUNG	HN-M101MBB	HN-M101MBB (EOL)	1TB	SATA
Seagate	2.5-inch enterprise series	ST1000NX0313	1TB	SATA
Seagate	2.5-inch enterprise series	ST2000NX0253	2TB	SATA

Appendix 4 Compatible CD/DVD Burner List



Please upgrade the DVR firmware to latest version to ensure the accuracy of the table below.

And you can use the USB cable with the model recommended to set USB burner.

Manufacturer	Model	Port Type	Type
Sony	DRX-S50U	USB	DVD-RW
Sony	DRX-S70U	USB	DVD-RW
Sony	AW-G170S	SATA	DVD-RW
Samsung	TS-H653A	SATA	DVD-RW
Panasonic	SW-9588-C	SATA	DVD-RW
Sony	DRX-S50U	USB	DVD-RW
BenQ	5232WI	USB	DVD-RW

Appendix 5 Compatible Displayer List

Please refer to the following table form compatible displayer list.

Brand	Model	Dimension (Unit: inch)
BENQ (LCD)	ET-0007-TA	19-inch (wide screen)
DELL (LCD)	E178FPc	17-inch
BENQ (LCD)	Q7T4	17-inch
BENQ (LCD)	Q7T3	17-inch
HFNOVO (LCD)	LXB-L17C	17-inch
SANGSUNG (LCD)	225BW	22-inch (wide screen)
HFNOVO (CRT)	LXB-FD17069HB	17-inch
HFNOVO (CRT)	LXB-HF769A	17-inch
HFNOVO(CRT)	LX-GJ556D	17-inch
Samsung (LCD)	2494HS	24-inch
Samsung (LCD)	P2350	23-inch
Samsung (LCD)	P2250	22-inch
Samsung (LCD)	P2370G	23-inch
Samsung (LCD)	2043	20-inch
Samsung (LCD)	2243EW	22-inch
Samsung (LCD)	SMT-1922P	19-inch
Samsung (LCD)	T190	19-inch
Samsung (LCD)	T240	24-inch
LG (LCD)	W1942SP	19-inch
LG (LCD)	W2243S	22-inch
LG (LCD)	W2343T	23-inch
BENQ (LCD)	G900HD	18.5-inch
BENQ (LCD)	G2220HD	22-inch
PHILIPS (LCD)	230E	23-inch
PHILIPS (LCD)	220CW9	23-inch
PHILIPS (LCD)	220BW9	24-inch
PHILIPS (LCD)	220EW9	25-inch

Appendix 6 Compatible Switcher

Brand	Model	network working mode
D-Link	DES-1016D	10/100M self-adaptive
D-Link	DES-1008D	10/100M self-adaptive
Ruijie	RG-S1926S	Five network modes: • AUTO • HALF-10M • FULL-10M • HALF-100M • FULL-100M
H3C	H3C-S1024	10/100M self-adaptive
TP-LINK	TL-SF1016	10/100M self-adaptive
TP-LINK	TL-SF1008+	10/100M self-adaptive

Appendix 7.1 What Is the Surge

Surge is a short current or voltage change during a very short time. In the circuit, it lasts for microsecond. In a 220V circuit, the 5KV or 10KV voltage change during a very short time (about microseconds) can be called a surge. The surge comes from two ways: external surge and internal surge.

- The external surge: The external surge mainly comes from the thunder lightning. Or it comes from the voltage change during the on/off operation in the electric power cable.
- The internal surge: The research finds 88% of the surge from the low voltage comes from the internal of the building such as the air conditioning, elevator, electric welding, air compressor, water pump, power button, duplicating machine and other device of inductive load.

The lightning surge is far above the load level the PC or the micro devices can support. In most cases, the surge can result in electric device chip damage, PC error code, accelerating the part aging, data loss and etc. Even when a small 20 horsepower inductive engine boots up or stops, the surge can reach 3000V to 5000V, which can adversely affect the electronic devices that use the same distribution box.

To protect the device, you need to evaluate its environment, the lightning affection degree objectively. Because surge has close relationship with the voltage amplitude, frequency, network structure, device voltage-resistance, protection level, ground and etc. The thunder proof work shall be a systematic project, emphasizing the all-round protection (including building, transmission cable, device, ground and etc.). There shall be comprehensive management and the measures shall be scientific, reliable, practical and economic.

Considering the high voltage during the inductive thundering, the International Electrotechnical Commission (IEC) standard on the energy absorbing step by step theory and magnitude classification in the protection zone, you need to prepare multiple precaution levels.

You can use the lightning rod, lightning strap or the lightning net to reduce the damage to the building, personal injury or the property.

The lightning protection device can be divided into three types:

- Power lightning arrester: There are 220V single-phase lightning arrester and 380V three-phase lightning arrester (mainly in parallel connection, sometimes use series connection) You can parallel connect the power lightning arrester in the electric cable to reduce the short-time voltage change and release the surge current. From the BUS to the device, there are usually three levels so that system can reduce the voltage and release the current step by step to remove the thunderstorm energy and guarantee the device safety. You can select the replaceable module type, the terminal connection type and portable socket according to your requirement.
- Signal lightning arrester: This device is mainly used in the PC network, communication system. The connection type is serial connection. Once you connected the signal lightning

arrestor with the signal port, it can cut the channel of the thunderstorm to the device, and on the other hand, it can discharge the current to the ground to guarantee the device proper work. The signal lightning arrester has many specifications, and widely used in many devices such as telephone, network, analog communication, digital communication, cable TV and satellite antenna. For all the input port, especially those from the outdoor, you need to install the signal lightning arrester.

- **Antenna feed cable lightning arrester:** It is suitable for antenna system of the transmitter or the device system to receive the wireless signal. It uses the serial connection too.

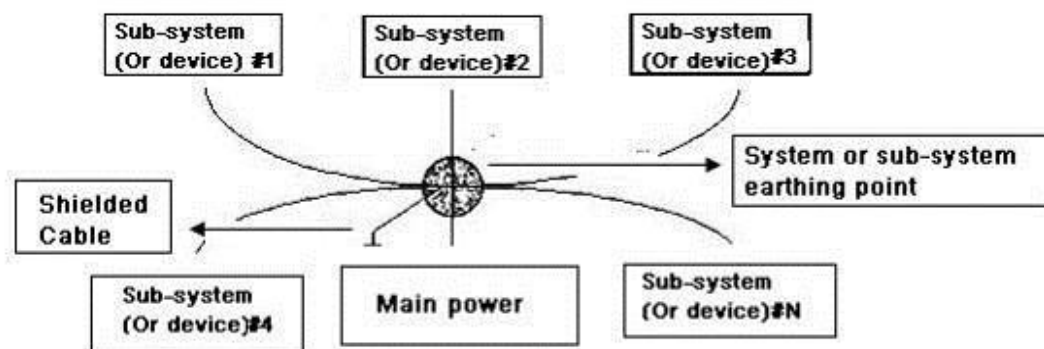
Please note, when you select the lightning arrester, please pay attention to the port type and the earthing reliability. In some important environment, you need to use special shielded cable. Do not parallel connect the thunder proof ground cable with the ground cable of the lightning rod. Please make sure they are far enough and grounded respectively.

Appendix 7.2 The Earthing Modes

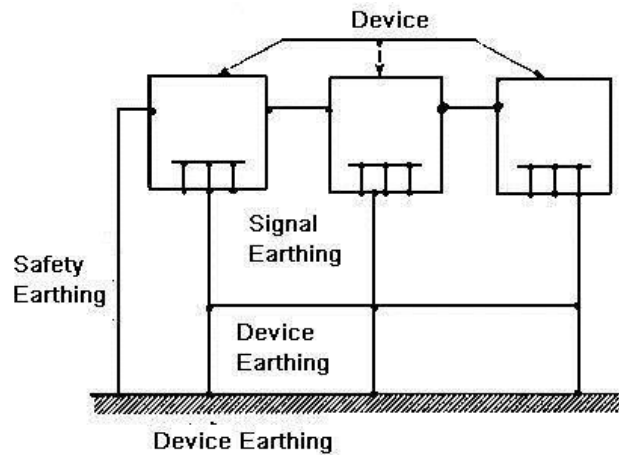
We all know the earthing is the most complicated technology in the electromagnetism compatibility design since there is no systematic theory or module. The earthing has many modes, but the selection depends on the system structure and performance.

The following are some successfully experience from our past work.

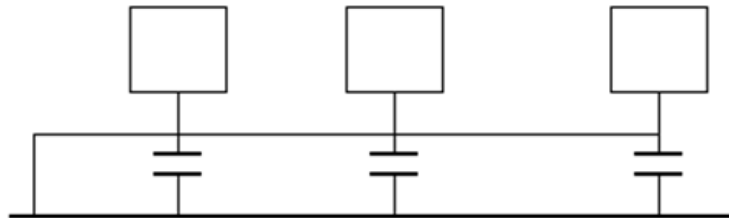
- **One-point ground:** In the following figure you can see there is a one-point ground. This connection provides common point to allow signal to be transmitted in many circuits. If there is no common point, the error signal transmission occurred. In the one-point ground mode, each circuit is just grounded only and they are connected at the same point. Since there is only one common point, there is no circuit and so, there is no interference.



- **Multiple-point ground:** In the following figure, you can see the internal circuit uses the chassis as the common point. While at the same time, all devices chassis use the earthing as the common point. In this connection, the ground structure can provide the lower ground resistance because when there are multiple-point grounds; each ground cable is as short as possible. And the parallel cable connection can reduce the total conductance of the ground conductor. In the high-frequency circuit, you need to use the multiple-point ground mode and each cable needs to connect to the ground. The length shall be less than the $1/20$ of the signal wavelength.



- **Mixed ground:** The mixed ground consists of the features of the one-point ground and multiple-point ground. For example, the power in the system needs to use the one-point ground mode while the radio frequency signal requires the multiple-point ground. So, you can use the following figure to earth. For the direct current (DC), the capacitance is open circuit and the circuit is one-point ground. For the radio frequency signal, the capacitance is conductive and the circuit adopts multiple-point ground.



When connecting devices of huge size (the device physical dimension and connection cable is big comparing with the wave path of existed interference), then there are possibility of interference when the current goes through the chassis and cable. In this situation, the interference circuit path usually lies in the system ground circuit.

When considering the earthing, you need to think about two aspects: One is the system compatibility, and the other is the external interference coupling into the earth circuit, which results in system error. For the external interference is not regular, it is not easy to resolve.

Appendix 7.3 Thunder Proof Ground Method in the Monitor System

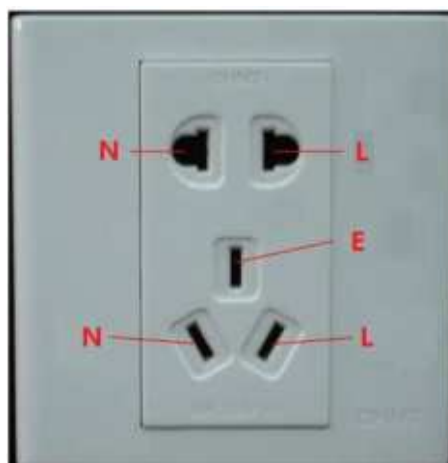
- The monitor system shall have sound thunder proof earthing to guarantee personnel safety and device safety.
- The monitor system working ground resistance shall be less than 1Ω .
- The thunder proof ground shall adopt the special ground cable from the monitor control room to the ground object. The ground cable adopts copper insulation cable or wire and its ground section shall be more than 20mm^2 .
- The ground cable of the monitor system cannot short circuit or mixed connected with the strong alternative current cable.
- For all the ground cables from the control room to the monitor system or ground cable of other monitor devices, please use the copper resistance soft cable and its section shall be

more than 4 mm².

- The monitor system usually can adopt the one-point ground.
- Please connect the ground end of 3-pin socket in the monitor system to the ground port of the system (protection ground cable)

Appendix 7.4 The Shortcut Way to Check the Electric System by Digital Multimeter

For 220V AC socket, from the top to the bottom, E (ground cable), N (neutral cable), L (live cable). Please refer to the following figure.



There is a shortcut way to check these three cables connection are standard or not (not the accurate check).



In the following operations, the multimeter range shall be at 750V.

For E (earth cable)

Turn the digital multimeter to 750V AC, use your one hand to hold the metal end, and then the other hand insert the pen to the E port of the socket. See the following figure. If the multimeter shows 0, then you can see current earth cable connection is standard. If the value is more than 10, then you can know there is inductive current and the earth cable connection is not proper.



For L (live cable)

Turn the digital multimeter to 750V AC, use your one hand to hold the metal end, and then the other hand insert the pen to the L port of the socket. See the following figure. If the multimeter shows 125, then you can see current live cable connection is standard. If the value is less than 60, then you can know current live cable connection is not proper or it is not the live cable at all.



For N (Neutral cable)

Turn the digital multimeter to 750V AC, use your one hand to hold the metal end, and then the other hand insert the pen to the N port of the socket. See the following figure. If the multimeter shows 0, then you can see current N cable connection is standard. If the value is more than 10, then you can see there is inductive current and the neutral cable connection is not proper. If the value is 120, then you can know that you have misconnected the neutral cable to the live cable.



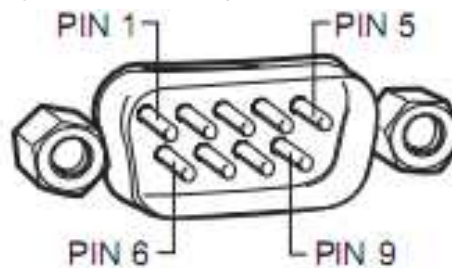
Appendix 8 RJ45-RS-232 Connection Cable

Definition

Here we are going to make standard RS-232 port and standard RJ45 (T568B).
Please refer to the following figure for RJ45 cable definition.

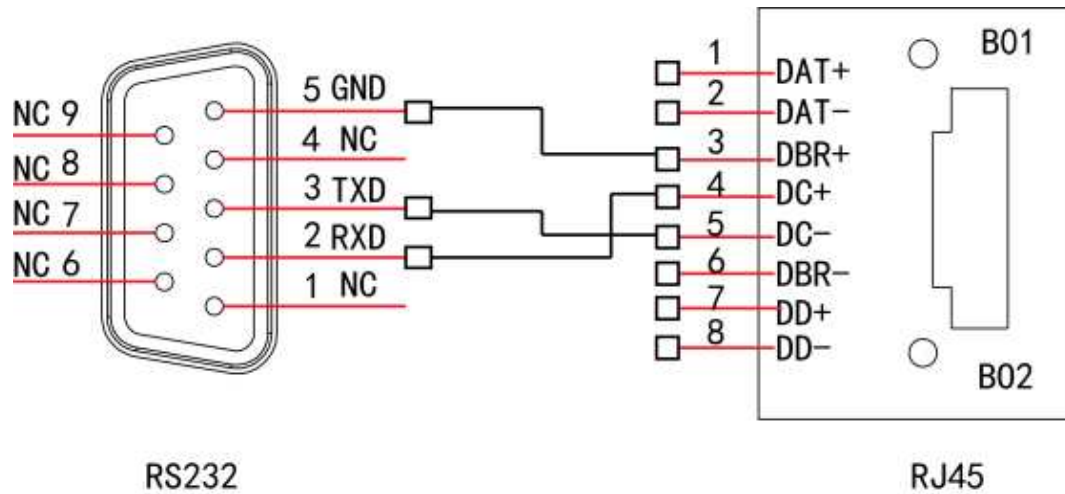


Please refer to the following figure for RS-232 pin definition.



Cross Connection

Please refer to the following figure for connection information.

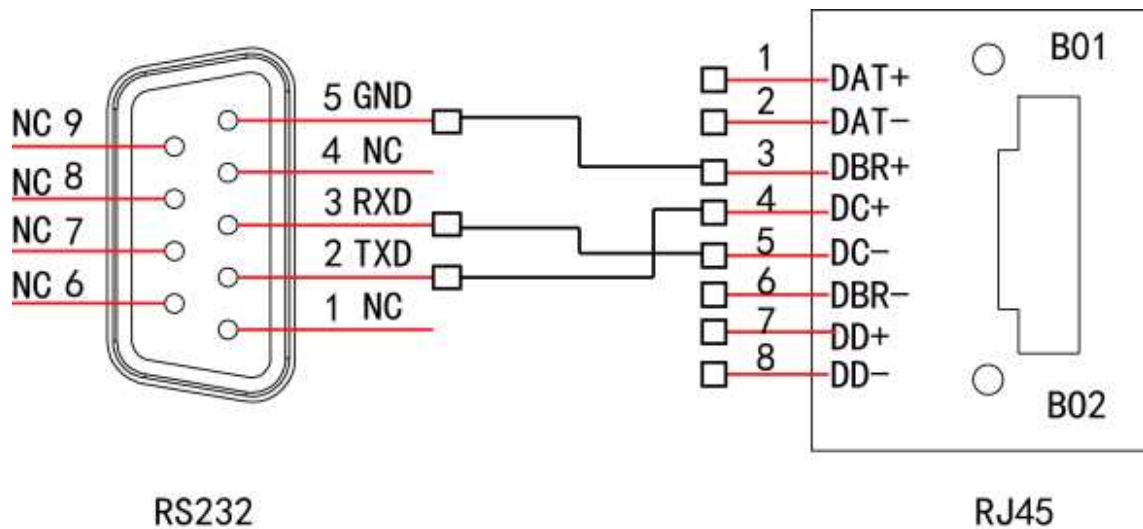


Please refer to the following table for detailed crossover cable connection information.

RJ45 (T568B)	RJ45 (Network cable)	RS-232	Signal Description
4	Blue	2	RXD
5	White and blue	3	TXD
3	White and green	5	GND

Straight Connection

Please refer to the following figure for straight cable connection information.



Please refer to the following table for straight connection information.

RJ45 (T568B)	RJ45 (Network cable)	RS-232	Signal Description
4	Blue	3	RXD
5	White and blue	2	TXD
3	White and green	5	GND

Appendix 9 Cybersecurity Recommendations

Mandatory actions to be taken towards cybersecurity

1. Change Passwords and Use Strong Passwords:

The number one reason systems get “hacked” is due to having weak or default passwords. It is recommended to change default passwords immediately and choose a strong password whenever possible. A strong password should be made up of at least 8 characters and a combination of special characters, numbers, and upper and lower case letters.

2. Update Firmware

As is standard procedure in the tech-industry, we recommend keeping NVR, DVR, and IP camera firmware up-to-date to ensure the system is current with the latest security patches and fixes.

“Nice to have” recommendations to improve your network security

1. Change Passwords Regularly

Regularly change the credentials to your devices to help ensure that only authorized users are able to access the system.

2. Change Default HTTP and TCP Ports:

- Change default HTTP and TCP ports for systems. These are the two ports used to communicate and to view video feeds remotely.
- These ports can be changed to any set of numbers between 1025-65535. Avoiding the default ports reduces the risk of outsiders being able to guess which ports you are using.

3. Enable HTTPS/SSL:

Set up an SSL Certificate to enable HTTPS. This will encrypt all communication between your devices and recorder.

4. Enable IP Filter:

Enabling your IP filter will prevent everyone, except those with specified IP addresses, from accessing the system.

5. Change ONVIF Password:

On older IP Camera firmware, the ONVIF password does not change when you change the system’s credentials. You will need to either update the camera’s firmware to the latest revision or manually change the ONVIF password.

6. Forward Only Ports You Need:

- Only forward the HTTP and TCP ports that you need to use. Do not forward a huge range of numbers to the device. Do not DMZ the device’s IP address.
- You do not need to forward any ports for individual cameras if they are all connected to a recorder on site; just the NVR is needed.

7. Disable Auto-Login on SmartPSS:

Those using SmartPSS to view their system and on a computer that is used by multiple people should disable auto-login. This adds a layer of security to prevent users without the appropriate credentials from accessing the system.

8. Use a Different Username and Password for SmartPSS:

In the event that your social media, bank, email, etc. account is compromised, you would not want someone collecting those passwords and trying them out on your video surveillance system. Using a different username and password for your security system will make it more difficult for someone to guess their way into your system.

9. Limit Features of Guest Accounts:

If your system is set up for multiple users, ensure that each user only has rights to features and functions they need to use to perform their job.

10. UPnP:

- UPnP will automatically try to forward ports in your router or modem. Normally this would be a good thing. However, if your system automatically forwards the ports and you leave the credentials defaulted, you might end up with unwanted visitors.
- If you manually forwarded the HTTP and TCP ports in your router/modem, this feature should be turned off regardless. Disabling UPnP is recommended when the function is not used in real applications.

11. SNMP:

Disable SNMP if you are not using it. If you are using SNMP, you should do so only temporarily, for tracing and testing purposes only.

12. Multicast:

Multicast is used to share video streams between two recorders. Currently there are no known issues involving Multicast, but if you are not using this feature, deactivation can enhance your network security.

13. Check the Log:

If you suspect that someone has gained unauthorized access to your system, you can check the system log. The system log will show you which IP addresses were used to login to your system and what was accessed.

14. Physically Lock Down the Device:

Ideally, you want to prevent any unauthorized physical access to your system. The best way to achieve this is to install the recorder in a lockbox, locking server rack, or in a room that is behind a lock and key.