ATM Digital Video Recorder

User Manual

About this Document

- This Document includes instructions for using and managing the Product. Pictures, charts, images and all other information hereinafter are for description and explanation only.
- The information contained in the Document is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of the Document at the Hikvision website (***https://www.hikvision.com***). Unless otherwise agreed, Hangzhou Hikvision Digital Technology Co., Ltd. or its affiliates (hereinafter referred to as "Hikvision") makes no warranties, express or implied.
- Please use the Document with the guidance and assistance of professionals trained in supporting the Product.

About this Product

- This product can only enjoy the after-sales service support in the country or region where the purchase is made.
- If the product you choose is a video product, please scan the following QR code to obtain the "Initiatives on the Use of Video Products", and read it carefully.

Acknowledgment of Intellectual Property Rights

- Hikvision owns the copyrights and/or patents related to the technology embodied in the Products described in this Document, which may include licenses obtained from third parties.
- Any part of the Document, including text, pictures, graphics, etc., belongs to Hikvision. No part of this Document may be excerpted, copied, translated, or modified in whole or in part by any means without written permission.
- HIKVISION and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions.
- Other trademarks and logos mentioned are the properties of their respective owners.
- HDMI The terms HDMI and HDMI High-Definition Multimedia Interface, and the HDMI Logo are trademarks or registered trademarks of HDMI Licensing Administrator, Inc. in the United States and other countries.

LEGAL DISCLAIMER

- TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS DOCUMENT AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED "AS IS" AND "WITH ALL FAULTS AND ERRORS". HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF

BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.

- YOU ACKNOWLEDGE THAT THE NATURE OF THE INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INFECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.
- YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.
- IN THE EVENT OF ANY CONFLICTS BETWEEN THIS DOCUMENT AND THE APPLICABLE LAW, THE LATTER PREVAILS.

Regulatory Information

FCC Information

Please take attention that changes or modification not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.
FCC compliance: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

FCC Conditions

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

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

EU Conformity Statement

This product and - if applicable - the supplied accessories too are marked with "CE" and comply therefore with the applicable harmonized European standards listed under the EMC Directive 2014/30/EU, the RoHS Directive 2011/65/EU.

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

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

Industry Canada ICES-003 Compliance

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

Applicable Model

This manual is applicable to the following model.

Series	Model
iDS-7200AHQHI-M	iDS-7204AHQHI-M1

Symbol Conventions

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

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

Safety Instruction

- Proper configuration of all passwords and other security settings is the responsibility of the installer and/or user.
- In the use of the product, you must be in strict compliance with the electrical safety regulations of the nation and region. Please refer to technical specifications for detailed information.
- Input voltage should meet both the SELV (Safety Extra Low Voltage) and the Limited Power Source with 100 VAC to 240 VAC or 12 VDC according to the IEC60950-1 standard. Please refer to technical specifications for detailed information.
- Do not connect several devices to one power adapter as adapter overload may cause over-heating or a fire hazard.
- Please make sure that the plug is firmly connected to the power socket.
- If smoke, odor or noise rises from the device, turn off the power at once and unplug the power cable, and then please contact the service center.

Preventive and Cautionary Tips

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

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

Contents

Chapter 1 Basic Operation

1.1 Activate Your Device

1.1.1 Default User and IP Address

- Default administrator account: admin.
- Default IPv4 address: 192.168.1.64.

1.1.2 Activate via Local Menu

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

Steps

1. Enter the admin password twice.

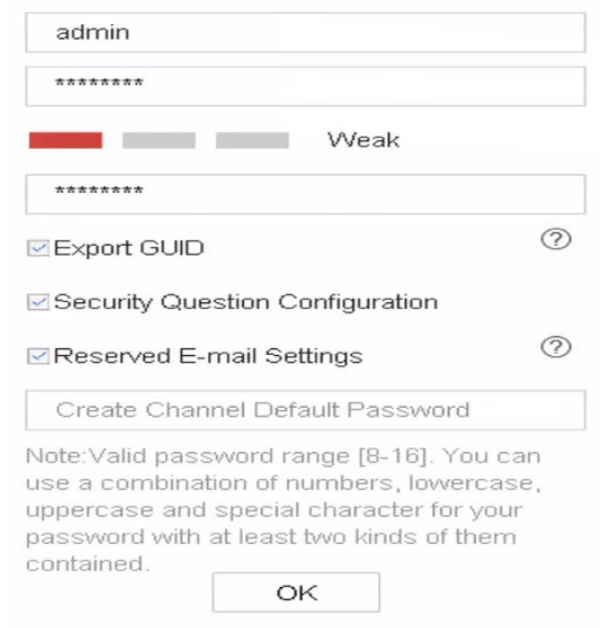

Figure 1-1 Activate via Local Menu

Warning

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

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

2. Enter the password to activate the IP cameras.
3. **Optional:** Check **Export GUID**, **Security Question Configuration**, or **Reserved E-mail Settings**.
4. Click **OK**.

Note

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

What to do next

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

1.1.3 Activate via SADP

SADP software is used for detecting the online device, activating the device, and resetting its password.

Before You Start

Get the SADP software from the supplied disk or the official website, and install the SADP according to the prompts.

Steps

1. Connect your video recorder power supply to an electrical outlet and turn on it.
2. Run the SADP software to search the online recorders.
3. Check the recorder status from the device list, and select the inactive recorder.

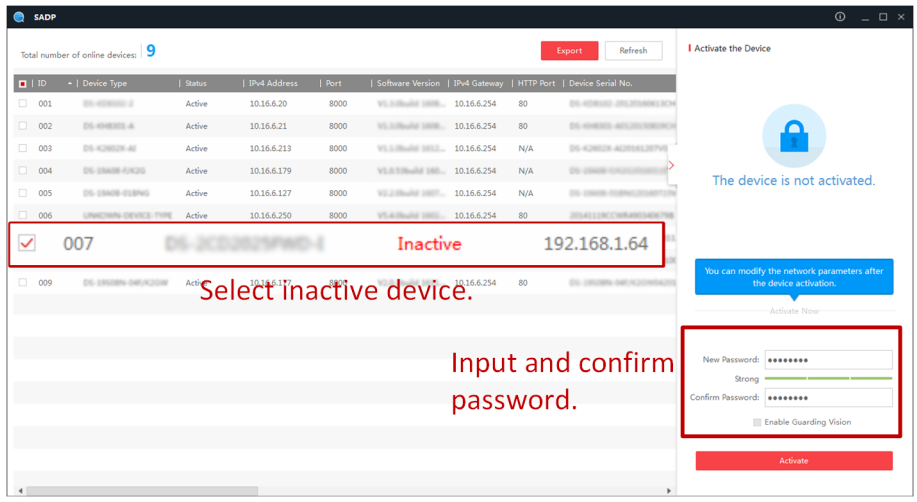

Figure 1-2 Activate via SADP

4. Create and input the new password in the password field, and confirm the password.

Note

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

5. Click **Activate**.

1.1.4 Activate via Client Software

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

Before You Start

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

Steps

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

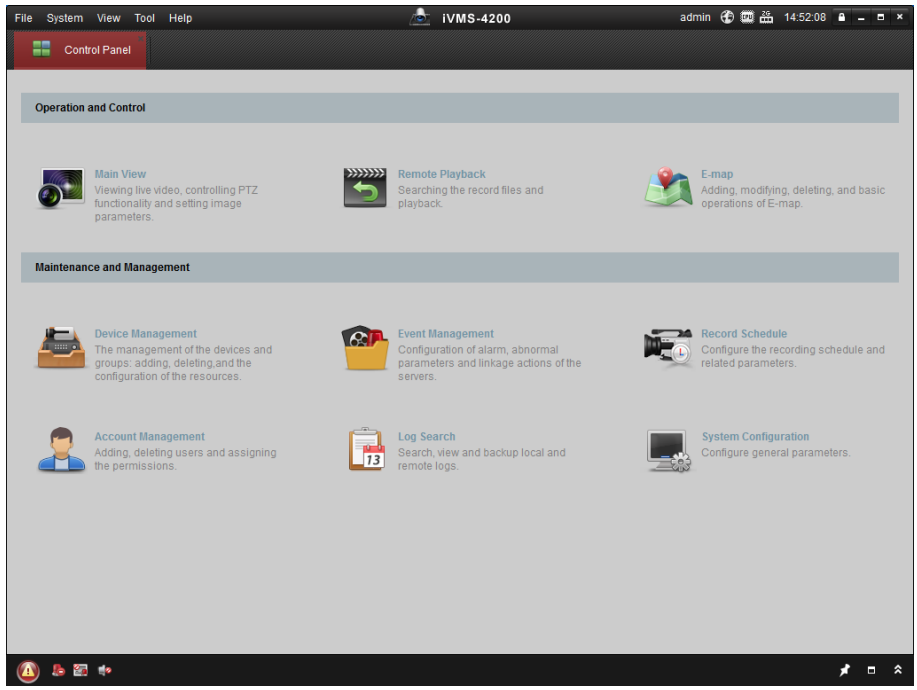

Figure 1-3 Control Panel

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

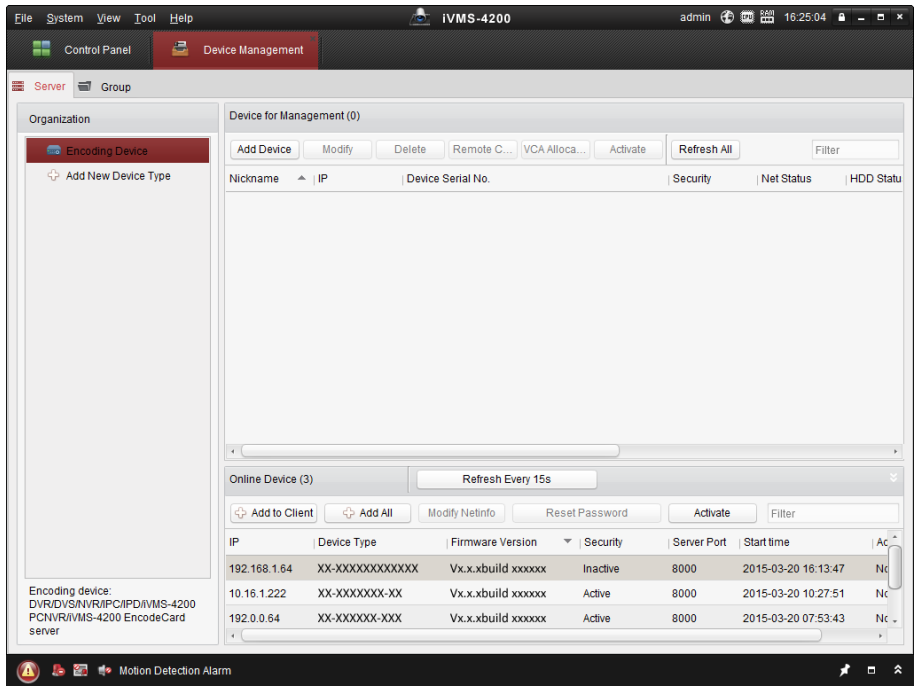

Figure 1-4 Device Management Interface

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

Note

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

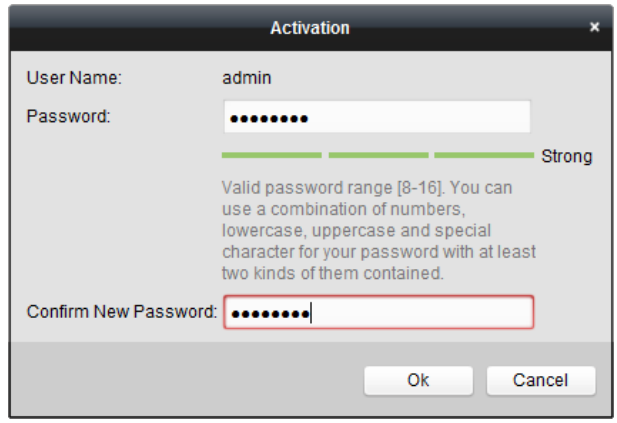

Figure 1-5 Activation

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

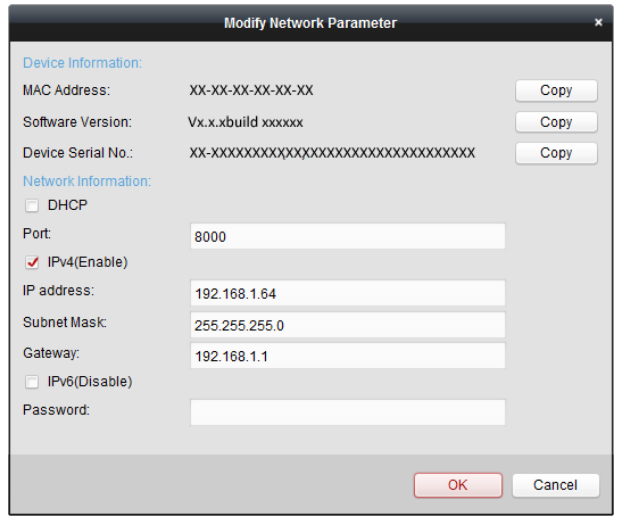

Figure 1-6 Modify Network Parameters

8. Change the recorder IP address to the same subnet with your computer.
   - Modify the IP address manually.
   - Check **Enable DHCP**.
9. Input the password to activate your IP address modification.

1.1.5 Activate via Web Browser

You can get access to the recorder via web browser. You may use one of the following listed web browsers: Internet Explorer 6.0 and above, Apple Safari, Mozilla Firefox, and Google Chrome. The supported resolutions include 1024*768 and above.

Steps

1. Enter the IP address in web browser, and then press **Enter**.

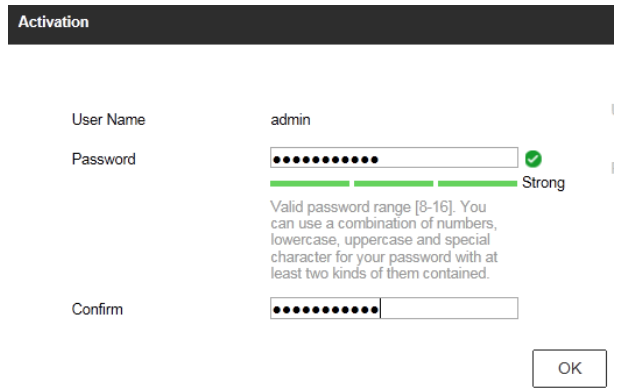

Figure 1-7 Web Browser Activation

2. Set the password for the admin user account.

Note

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

3. Click **OK**.

1.2 Configure TCP/IP Settings

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

Steps

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

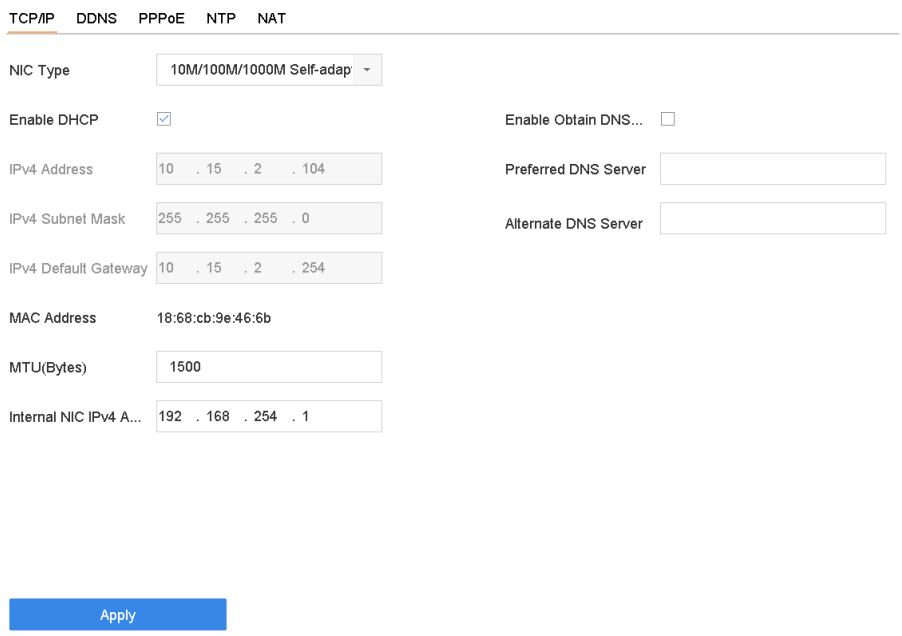

Figure 1-8 TCP/IP Settings

2. Configure network parameters as needed.

Note

- Check **Enable DHCP** to obtain IP settings automatically if a DHCP server is available on the network.
- Valid MTU value range is 500 to 9676.

3. Click **Apply**.

1.3 Add Network Camera

1.3.1 Configure Signal Input

You can configure the analog and IP signal input types, disabling one analog channel can add one IP channel.

Steps

1. Go to **Camera → Camera → Analog** .

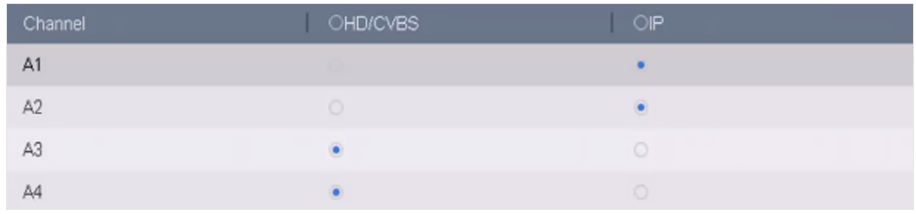

Figure 1-9 Signal Input Type

2. Select signal input type as **HD/CVBS** or **IP** for each channel.

   HD/CVBS

   Four types of analog signal inputs including Turbo HD, AHD, HDCVI, and CVBS can be connected randomly for the channel.

   IP

   Network camera can be connected for the channel.

3. Click **Apply**. You can view the maximum network camera accessible number in **Max. IP Camera Number**.

1.3.2 Add Automatically Searched Online Network Camera

Steps

1. Click on the main menu.
2. Click **Number of Unadded Online Device** at the bottom.
3. Select the automatically searched online network cameras.
4. Click **Add** to add the camera which has the same login password with the video recorder.

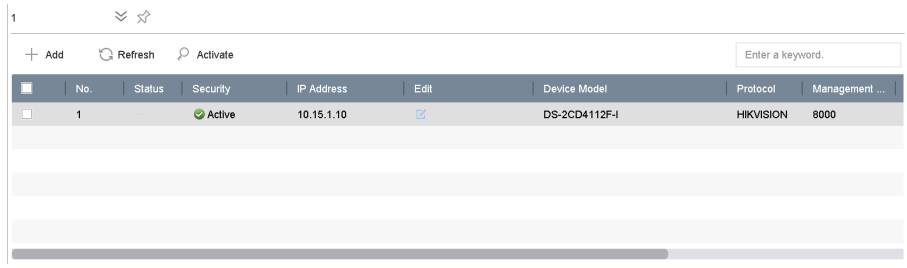

Figure 1-10 Add Automatically Searched Online Network Camera

Note

If the network camera to add has not been activated, you can activate it in the network camera list of camera management interface.

1.3.3 Add Network Camera Manually

Before you view live video or record video files, you must add network cameras to the device.

Before You Start

Ensure the network connection is valid and correct, and the network camera is activated.

Steps

1. Click on the main menu.
2. Click **Custom Adding**.
3. Set **IP Camera Address**, **Protocol**, **Management Port**, **Transfer Protocol**, **User Name**, and **Password**. Management port ranges from 1 to 65535.

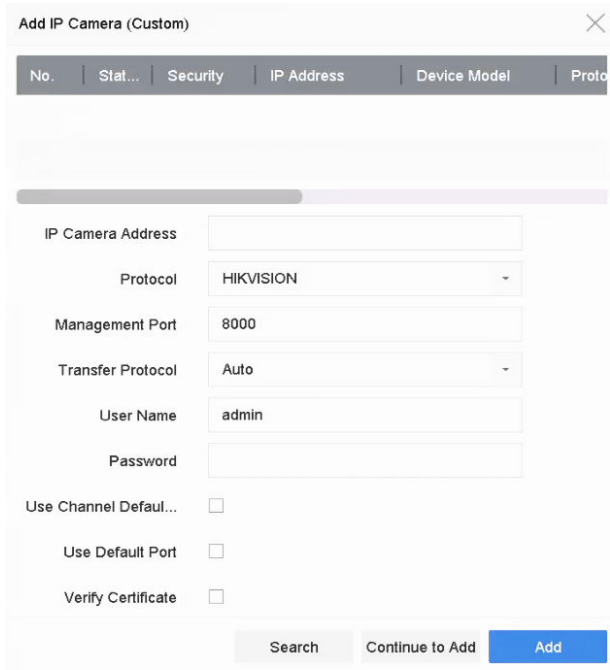

Figure 1-11 Add Network Camera

4. **Optional:** Check **Use Channel Default Password** to use the default password to add the camera.
5. **Optional:** Check **Use Default Port** to use the default management port to add the camera. For SDK service, the default port value is 8000. For enhanced SDK service, the default value is 8443.

Note

The function is only available when you use HIKVISION protocol.

6. **Optional:** Check **Verify Certificate** to verify the camera with certificate. The certificate is a form of identification for the camera that provides more secure camera authentication. It requires to import the network camera certificate to the NVR first when you use this function. For details, refer to .

Note

The function is only available when you use HIKVISION protocol.

7. Click **Add**.
8. **Optional:** Check **Continue to Add** to add other network cameras.

1.4 Platform Access

1.4.1 Configure Hik-Connect

Hik-Connect provides mobile phone application and platform service to access and manage your video recorder, which enables you to get a convenient remote access to the surveillance system.

Steps

1. Go to **System → Network → Advanced → Platform Access** .
2. Check **Enable** to activate the function. Then the service terms will pop up.
   1) Enter **Verification Code**.
   2) Scan the QR code to read the service terms and privacy statement.
   3) Check **The Hik-Connect service will require internet access. Please read Service Terms and Privacy Statement before enabling the service.** if you agree the service terms and privacy statement.
   4) Click **OK**.

   Note

   - Hik-Connect is disabled by default.
   - The verification code is empty by default. It must contain 6 to 12 letters or numbers, and it is case sensitive.
3. **Optional:** Configure following parameters.
   - Check **Custom** and enter **Server Address** as your desire.
   - Check **Enable Stream Encryption**, verification code is required for remote access and live view.
   - Click **Unbind** if your video recorder requires to unbind with the current Hik-Connect account.
4. Click **Apply**.

What to do next

You can access and manage your video recorder through Hik-Connect app or ***www.hik-connect.com*** .

Chapter 2 Live View

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

2.1 Start Live View

Click on the main menu bar to enter the Live View.

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

2.1.1 Configure Live View Settings

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

Steps

1. Go to **System → Live View → General** .

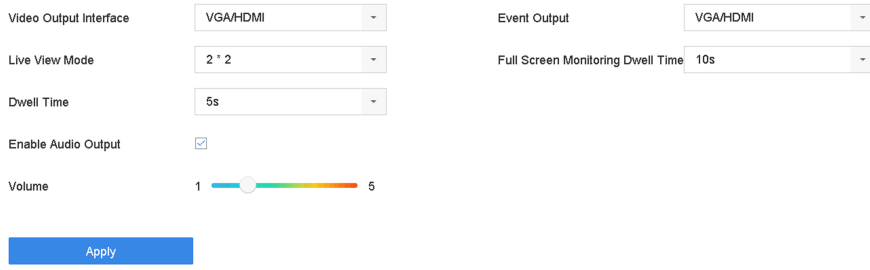

Figure 2-1 Live View-General

2. Configure the live view parameters.

Video Output Interface

Select the video output to configure.

Live View Mode

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

Dwell Time

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

Enable Audio Output

Enable/disable audio output for the selected video output.

Volume

Adjust the Live View volume, playback and two-way audio for the selected output interface.

Event Output

Select the output to show event video.

Full Screen Monitoring Dwell Time

Set the time in seconds to show alarm event screen.

3. Click **OK**.

2.1.2 Configure Live View Mode

Steps

1. Go to **System → Live View → View** .
2. Select the video output interface.
3. Select a layout or custom layout from the toolbar.
4. Select a division window, and double-click on a camera in the list to link the camera to the window.

Note

- You can also click-and-drag the camera to the desired window on the Live View interface to set the camera order.
- You can enter the number in the text field to quickly search the camera from the list.

5. Click **Apply**.
6. **Optional:** Click to start live view for all channels, or click to stop all live view channels.

2.2 Digital Zoom

Digital Zoom zooms into the live image in different magnifications (1x to 16x).

Steps

1. Start live view, click from the toolbar.
2. Move the sliding bar or scroll the mouse wheel to zoom in/out the image to different magnifications (1x to 16x).

Figure 2-2 Digital Zoom

2.3 PTZ Control

2.3.1 Configure PTZ Parameters

Follow these procedures to set the PTZ parameters. The PTZ parameters configuration must be done before you can control the PTZ camera.

Steps

1. Click on the quick settings toolbar of the PTZ camera's Live View.
2. Click **PTZ Parameters Settings** to set the PTZ parameters.

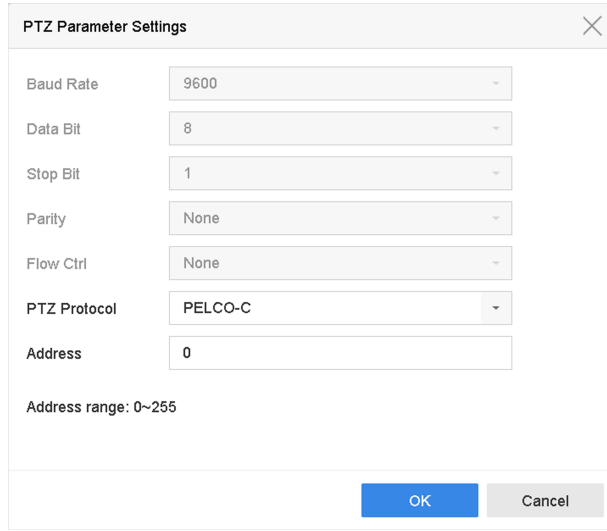

Figure 2-3 PTZ Parameters Settings

3. Edit the PTZ parameters.

Note

All the parameters should be exactly match the PTZ camera parameters.

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

2.3.2 Set a Preset

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

Steps

1. Click on the quick settings toolbar of the PTZ camera's live view.
2. Click directional buttons to wheel the camera to a location.
3. Adjust the zoom, focus and iris status.
4. Click in the lower right corner of Live View to set the preset.

Figure 2-4 Set Preset

5. Select the preset No. (1 to 255) from the drop-down list.
6. Enter the preset name.
7. Click **Apply** to save the preset.
8. **Optional:** Click **Cancel** cancel the location information of the preset.
9. **Optional:** Click in the lower right corner of Live View to view the configured presets.

Figure 2-5 View the Configured Presets

2.3.3 Call a Preset

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

Steps

1. Click on the quick settings toolbar of the PTZ camera's Live View.
2. Click in the lower right corner of Live View to set the preset.
3. Select the preset No. from the drop-down list.
4. Click **Call** to call it, or click in the lower right corner of Live View, and click the configured preset to call it.

Figure 2-6 Call Preset (1)

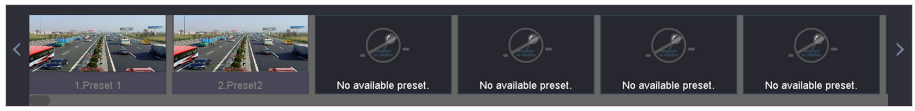

Figure 2-7 Call Preset (2)

2.3.4 Set a Patrol

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

Steps

1. Click on the quick settings toolbar of the PTZ camera's live view.
2. Click **Patrol** to configure patrol.

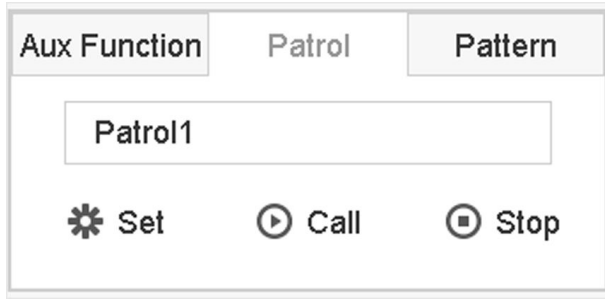

Figure 2-8 Patrol Configuration

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

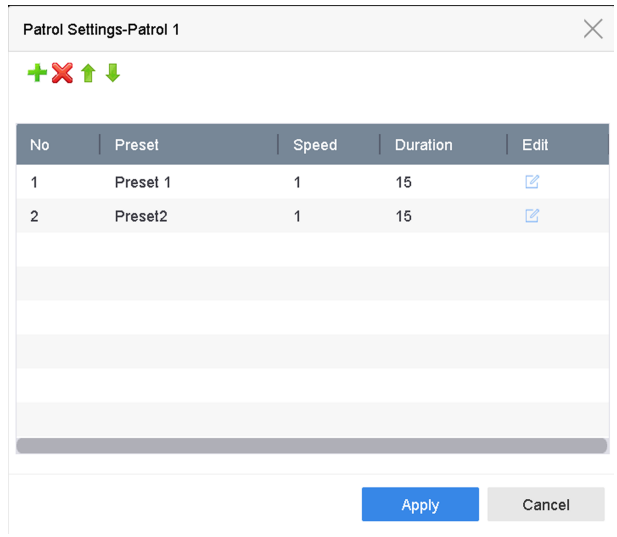

Figure 2-9 Patrol Settings

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

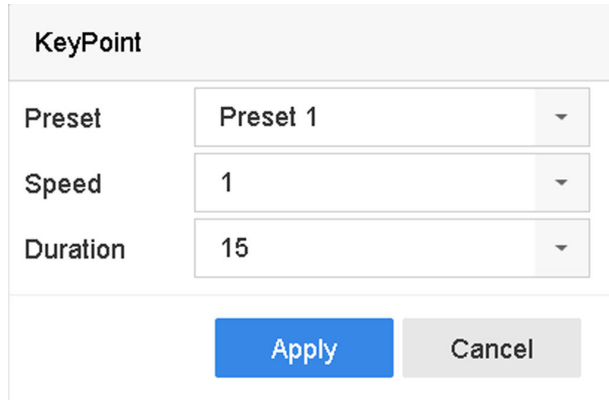

Figure 2-10 Key Point Configuration

1) Configure key point parameters.

Preset

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

Speed

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

Duration

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

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

6. Other Operation is as follows.

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

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

2.3.5 Call a Patrol

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

Steps

1. Click on the quick settings toolbar of the PTZ camera's live view.
2. Click **Patrol** on the PTZ control panel.

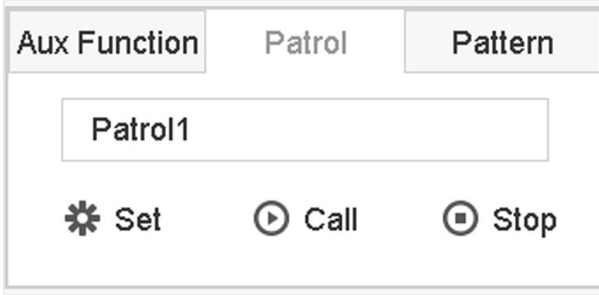

Figure 2-11 Patrol Configuration

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

2.3.6 Set a Pattern

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

Steps

1. Click on the quick settings toolbar of the PTZ camera's live view.
2. Click **Pattern** to configure a pattern.

Figure 2-12 Pattern Configuration

3. Select the pattern No.
4. Set the pattern.
   1) Click **Record** to start recording.
   2) Click corresponding buttons on the control panel to move the PTZ camera.
   3) Click **Stop** to stop recording. The PTZ movement is recorded as the pattern.

2.3.7 Call a Pattern

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

Steps

1. Click on the quick settings toolbar of the PTZ camera's live view.
2. Click **Pattern** to configure pattern.

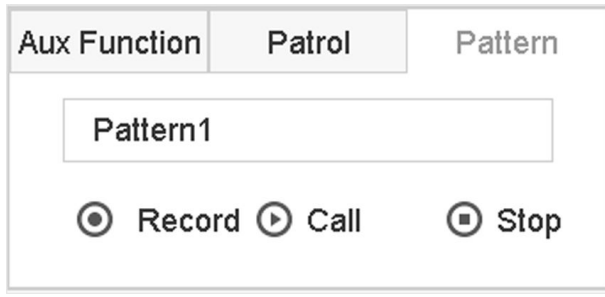

Figure 2-13 Pattern Configuration

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

2.3.8 Set Linear Scan Limit

Linear Scan trigger a scan in the horizontal direction in the predefined range.

Before You Start

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

Note

This function is supported only by some certain models.

Steps

1. Click on the quick settings toolbar of the PTZ camera's live view.
2. Click directional buttons to wheel the camera to a location, and click **Left Limit** or **Right Limit** to link the location to the corresponding limit.

   Note

   The speed dome linear scans from the left limit to the right limit, and you must set the left limit on the left side of the right limit. Also, the angle from the left limit to the right limit must be no more greater than 180º.

2.3.9 One-Touch Park

Certain speed dome models can be configured to start a predefined park action (scan, preset, patrol and etc.) automatically after a period of inactivity (park time).

Before You Start

Before operating this function, make sure the connected camera supports linear scan and is in HIKVISION protocol.

Steps

1. Click on the quick settings toolbar of the PTZ camera's live view.
2. Click **Park (Quick Patrol)**, **Park (Patrol 1)**, or **Park (Preset 1)** to activate the park action.

   Park (Quick Patrol)

   The dome starts patrolling from the predefined preset 1 to preset 32 in order after the park time. Undefined presets will be skipped.

   Park (Patrol 1)

   The dome starts moving according to the predefined patrol 1 path after the park time.

   Park (Preset 1)

   The dome moves to the predefined preset 1 location after the park time.

   Note

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

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

Chapter 3 Recording and Playback

3.1 Recording

3.1.1 Configure Recording Parameters

Go to **Camera → Video Parameters** .

Main Stream

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

Frame Rate (FPS - Frames Per Second)

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

Resolution

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

Bitrate

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

Enable H.264+

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

Enable H.265+

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

Note

- A higher resolution, frame rate and bit rate setting will provide you the better video quality, but it will also require more internet bandwidth and use more storage space on the hard disk drive.
- H.264+ or H.265+ encoding technology is only available for certain models.

Sub-Stream

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

Picture

The picture refers to the live picture capture in continuous or event recording type. (**Storage → Capture Schedule → Advanced**

Picture Quality

Set the picture quality to low, medium or high. The higher picture quality results in more storage space requirement.

Interval

The interval of capturing live picture.

Capture Delay Time

The duration of capturing pictures.

3.1.2 Enable the H.265 Stream Access

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

Go to **Camera → More Settings → H.265 Auto Switch Configuration** to enable the function.

3.1.3 Manual Recording

You can click  to manually start/stop recording videos at live view.

3.1.4 Configure Plan Recording

The camera would automatically start/stop recording according to the configured recording schedule.

Before You Start

- Ensure you have installed the HDDs to the device or added the network disks before storing the video files, pictures and log files.
- Before enabling **Motion**, **Alarm**, **M | A** (motion or alarm), **M & A** (motion and alarm), **Event**, and **Smart ATM** triggered recording and capture, you must configure the motion detection settings, alarm input settings and other events as well. Refer to ***Event*** for details.

Steps

1. Go to **Storage → Schedule → Record** .
2. Select a camera.
3. Check **Enable Schedule**.
4. Select a recording type.

   Continuous

   Scheduled recording.

   Event

   Recording triggered by all event triggered alarm.

   Motion

   Recording triggered by motion detection.

   Alarm

   Recording triggered by alarm.

   M/A

   Recording triggered by either motion detection or alarm.

   M&A

   Recording triggered by motion detection and alarm.

   Smart ATM

   Recording triggered by smart ATM.
5. Drag the cursor on time bar to set the record schedule.

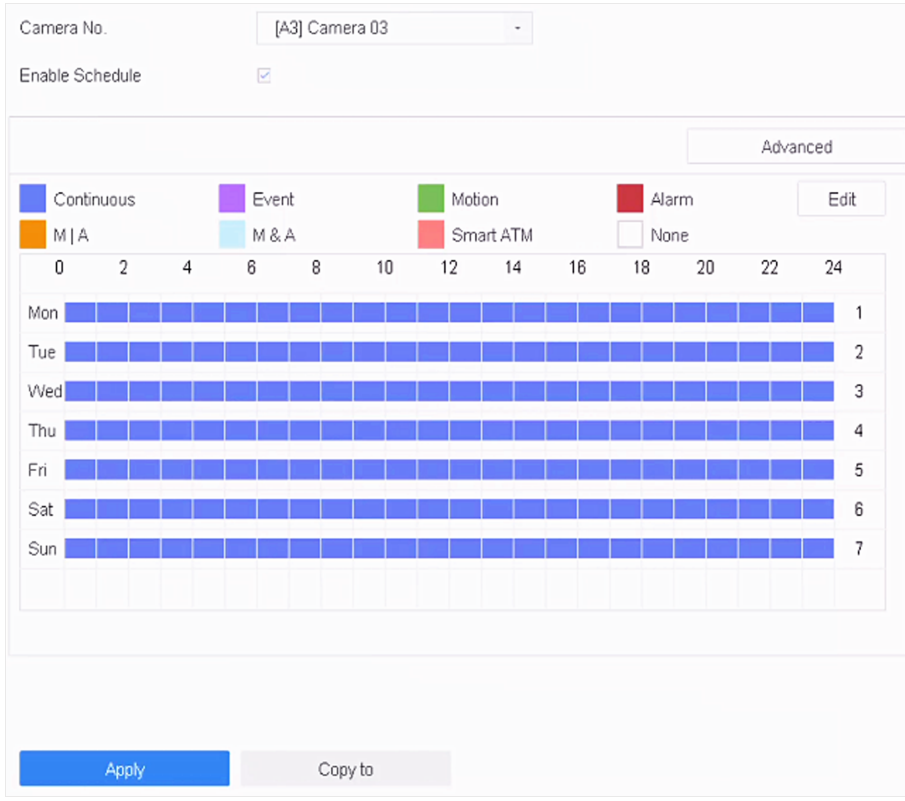

Figure 3-1 Record Schedule

Note

- You can repeat the above steps to set schedule recording or capture for each day in the week.
- Continuous recording is applied to each day by default.

6. **Optional:** Copy the recording schedule to other camera(s).
   1) Click **Copy to**.
   2) Select camera(s) to duplicate with the same schedule settings.
   3) Click **OK**.
7. Click **Apply**.

3.1.5 Configure Holiday Recording

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

Steps

1. Go to **System → Holiday** .
2. Select a holiday item from the list.
3. Click to edit the selected holiday.
4. Check **Enable**.

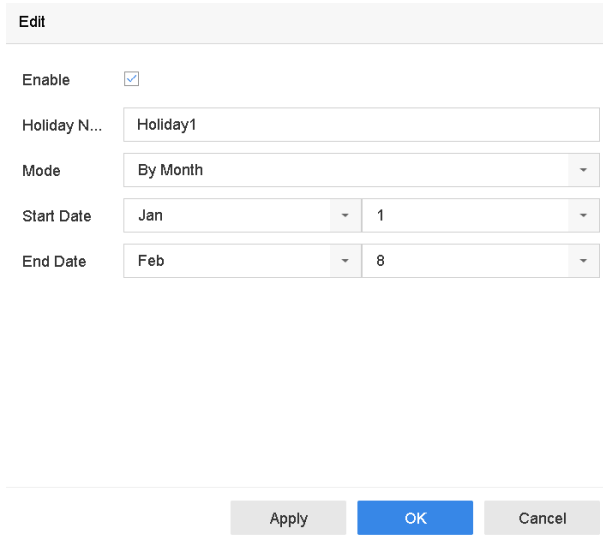

Figure 3-2 Edit Holiday Settings

5. Set **Holiday Name**, **Mode**, **Start Date**, and **End Date**.
6. Click **OK**.
7. Set the schedule for holiday recording. Refer to ***Configure Plan Recording*** for details.

3.1.6 Configure 1080p Lite Mode

When **1080P Lite Mode** is enabled, the encoding resolution at 1080P Lite (real-time) is supported. If not, up to 1080P (non-real-time) is supported.

Go to **Storage → Advanced** to enable or disable **1080P Lite Mode**.

3.2 Playback

3.2.1 Instant Playback

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

After selecting the camera on **Live View**, you can move the cursor to the window bottom to access the toolbar, and click to start instant playback.

Figure 3-3 Playback Interface

3.2.2 Play Normal Video

Go to **Playback**, select date and camera(s), and use the toolbar at the bottom to perform playback operations. Refer to ***Playback Operations*** . You can click camera(s) to execute simultaneous playback of multiple camera(s).

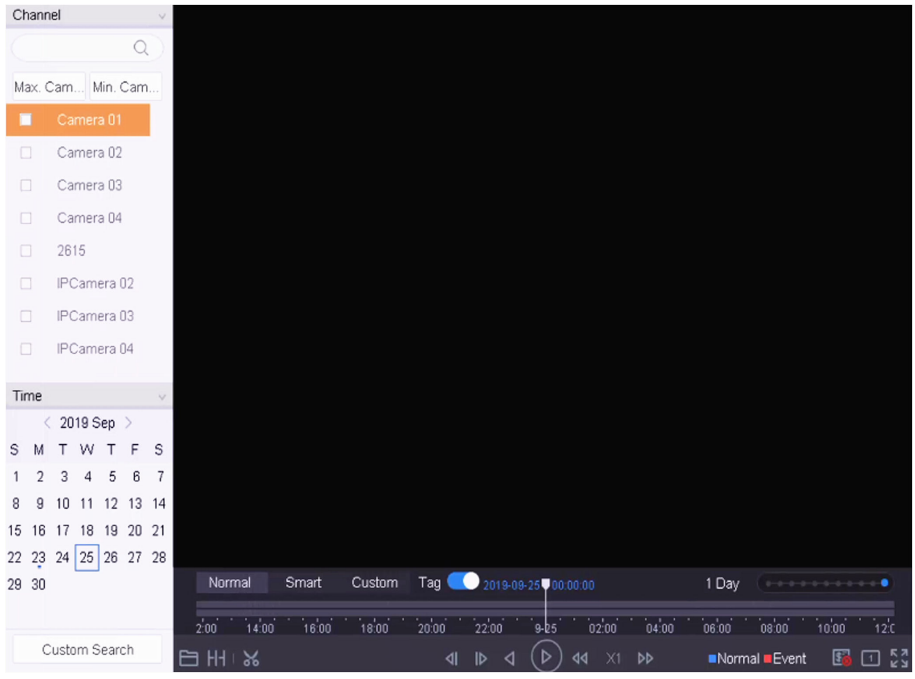

Figure 3-4 Play Normal Video Interface

3.2.3 Play Custom Searched Files

You can play video by customized search conditions.

Steps

1. Go to **Playback**.
2. Select camera(s) from the list.
3. Click **Custom Search** on the left bottom.
4. Enter search conditions, including **Time**, **File Status**, **Event Type**, etc.

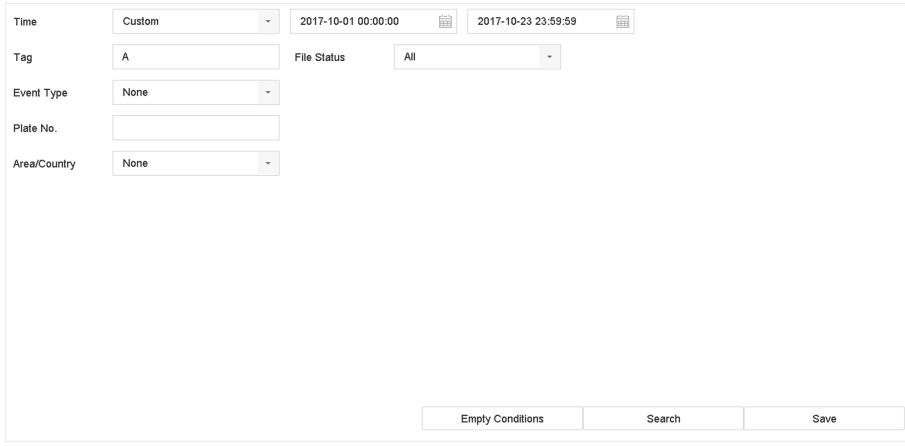

Figure 3-5 Custom Search

5. Click **Search**.

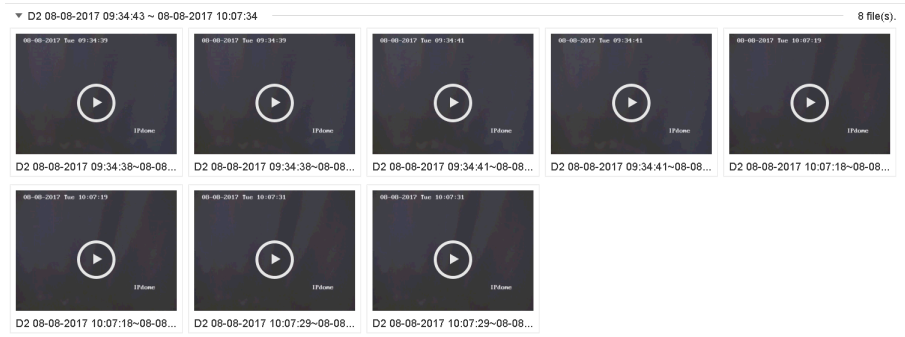

Figure 3-6 Custom Searched Video Files

6. Select a file and start playing the video on search results interface.

3.2.4 Play Tag Files

Video tag allows you to record information, such as people and locations of a certain time point, during playback. You can use video tag(s) to search video files and position time point.

Add Tag Files

Steps

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

Note

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

Play Tag Files

Steps

1. Go to **Playback**.
2. Click **Custom Search** at the left bottom.
3. Enter search conditions, including time and tag keyword.

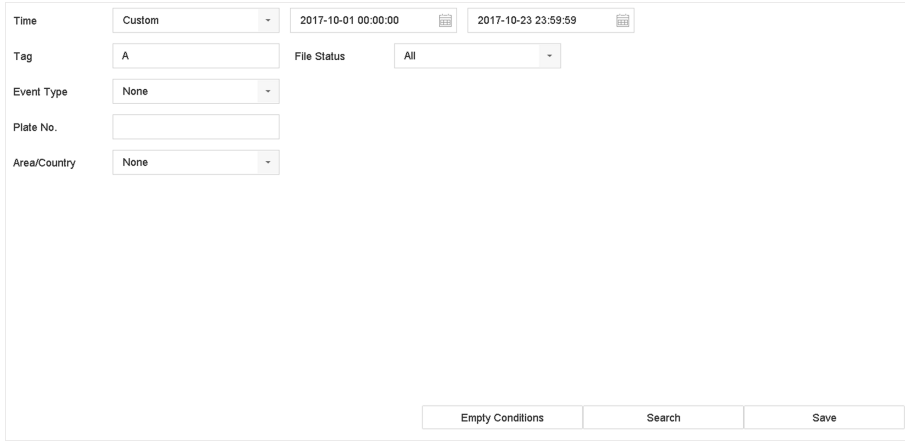

Figure 3-7 Tag Search

4. Click **Search**.

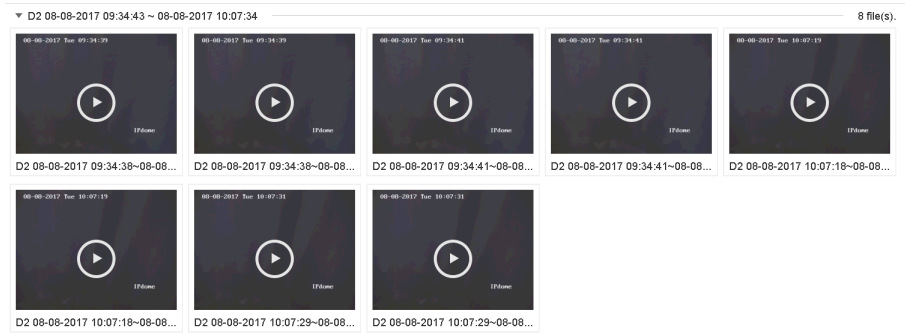

Figure 3-8 Searched Tag Files

5. Select a tag file, and play the video on the search results interface.

3.2.5 Play by Sub-periods

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

Steps

1. Go to **Playback**.
2. Click at the lower-left corner.
3. Select a camera.
4. Set the start time and end time for searching video.
5. Select the different multi-period at the lower-right corner, e.g., 4-Period.

Note

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

3.2.6 Play External Files

You can play files from external storage devices.

Before You Start

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

Steps

1. Go to **Playback**.
2. Click at the lower-left corner.
3. Click , or double-click the file to play it.

3.3 Playback Operations

3.3.1 Edit Video Clips

You can cut and export video clips during playback.

Steps

1. Go to **Playback**
2. Click at the bottom toolbar.
3. Set the start time and end time. You can click to set the time period, or set a time segment on time bar.
4. Click to save the video clip to a storage device.

Chapter 4 Event

4.1 Normal Event Alarm

4.1.1 Configure Motion Detection Alarms

Motion detection enables the device to detect the moving objects in the monitored area and trigger alarms.

Steps

1. Go to **System → Event → Normal Event → Motion Detection** .
2. Select a camera.
3. Check **Enable**.
4. Set the motion detection area.

Full screen	Click to set the full-screen motion detection for the image.
Customized area	Drag on the preview screen to draw the customized motion detection area(s).

5. Set **Sensitivity** (0-100). The sensitivity allows you to calibrate how readily movement triggers the alarm. A higher value results in the more readily to triggers motion detection.
6. Set the arming schedule. Refer to ***Configure Arming Schedule*** .
7. Set linkage actions. Refer to ***Configure Linkage Actions*** .

4.1.2 Configure Video Loss Alarms

Video loss detection detects video loss of a channel and takes alarm response action(s).

Steps

1. Go to **System → Event → Normal Event → Video Loss** .
2. Select a camera.
3. Check **Enable**.
4. Set the arming schedule. Refer to ***Configure Arming Schedule*** .
5. Set linkage actions. Refer to ***Configure Linkage Actions*** .

4.1.3 Configure Video Tampering Alarms

Video tampering detection triggered an alarm when the camera lens is covered and takes alarm response action(s).

Steps

1. Go to **System → Event → Normal Event → Video Tampering** .

2. Select a camera.
3. Check **Enable**.
4. Set the video tampering area. Drag on the preview screen to draw the customized video tampering area.
5. Set **Sensitivity** (0-2). 3 levels are available. The sensitivity calibrates how readily movement triggers the alarm. A higher value more readily triggers the video tampering detection.
6. Set the arming schedule. Refer to ***Configure Arming Schedule*** .
7. Set linkage actions. Refer to ***Configure Linkage Actions*** .

4.1.4 Configure Sensor Alarms

Set the handling action of an external sensor alarm.

Steps

1. Go to **System → Event → Normal Event → Alarm Input** .
2. Select an alarm input item from the list and click
3. Select the alarm input type.
4. Edit the alarm name.
5. Check **Input**.
6. Set the arming schedule. Refer to ***Configure Arming Schedule*** .
7. Set linkage actions. Refer to ***Configure Linkage Actions*** .

4.1.5 Configure Exceptions Alarms

Exception events can be configured to take the event hint in the Live View window and trigger alarm output and linkage actions.

Steps

1. Go to **System → Event → Normal Event → Exception** .
2. **Optional:** Enable the event hint to display it in the live view window.
   1) Check **Enable Event Hint**.
   2) Click to select the exception type(s) to take the event hint.

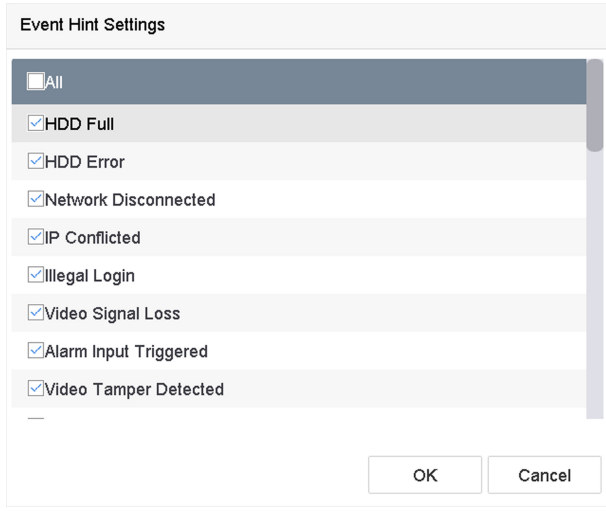

Figure 4-1 Event Hint Settings

3. Select an exception type.

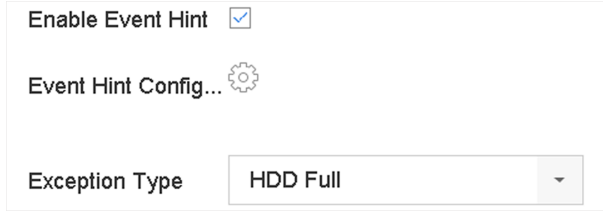

Figure 4-2 Exceptions Handling

4. Set the linkage actions. Refer to ***Configure Linkage Actions*** .

4.2 Smart ATM Event Alarm

Two smart ATM modes are supported: panel mode, and human face mode. You can only enable one mode for the same analog camera.

Enable smart ATM event alarm will cost 2-ch IP camera connection resources.

4.2.1 Panel Mode

Panel mode supports the following smart ATM protection rule types: human entrance, operation timeout, sticking scrip, and installing scanner. Eight rules can be set for the mode per channel. You can set the alarm response actions once the configured rule is triggered.

Steps

1. Go to **System → Event → Smart ATM Event** .

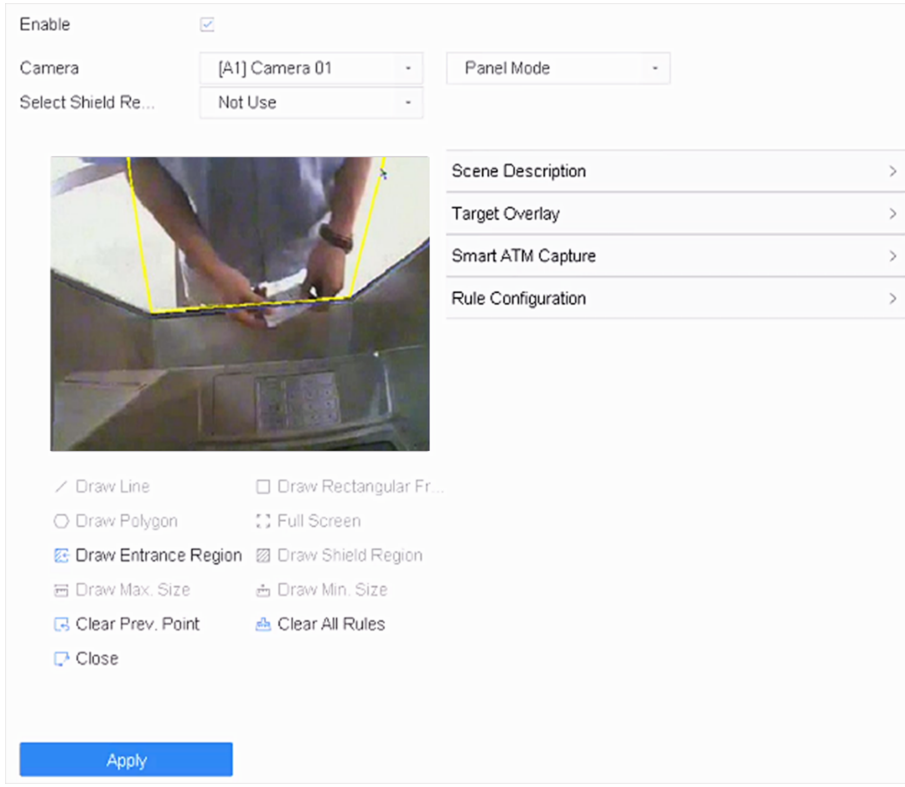

Figure 4-3 Panel Mode

2. Check **Enable**.
3. Select an analog camera.
4. Select **Panel Mode**.
5. Set **Scene Description**.

   Mounting Location

   The camera mounting location.

   Mounting Type

   The camera mounting type.

   Standing Region Contained in Scene

   Whether the scene contains the human standing region.
6. Set **Smart ATM Capture** parameters for captured image.
7. Set **Target Overlay**. Target frames or rules can be overlaid on captured image.
8. Set **Rule Configuration**.
   1) Check **Enable** of the selected rule.
   2) Double click the rule, or click .
   3) Set **Name**, **Type**, **Alarm Duration**, etc.

      Duration

It will alarm if the selected rule type continues for the configured duration. For **Operation Timeout**, it ranges from 4 to 6000 seconds. For **Sticking Scrip** and **Installing Scanner**, it ranges from 4 to 60 seconds.

Alarm Duration

Alarm duration after the selected type is triggered.

4) Click **OK**.

Note

Rules of different types can be enabled together for the panel mode.

9. Draw the rule region.

Human Entrance	Click **Draw Entrance Region** to draw the region.
Operation Timeout	Click **Draw Entrance Region**, **Draw Rectangular Frame**, **Draw Polygon**, or **Full Screen** to draw the region.
Sticking Scrip	Click **Draw Entrance Region**, **Draw Rectangular Frame**, **Draw Polygon**, or **Full Screen** to draw the region.
Installing Scanner	Click **Draw Entrance Region**, **Draw Rectangular Frame**, **Draw Polygon**, or **Full Screen** to draw the region.

10. Click of the selected rule to set alarm response actions. Refer to ***Configure Linkage Actions*** and ***Configure Arming Schedule*** for details.

11. Optional: Set the shield region. The shield region is used to shield environment interferences or other influences which may cause false alarms.

1)Select a shield region in **Select Shield Region**.

2)Click **Draw Shield Region**.

3)Click on the live view image to draw points of the region. You can click **Clear Prev. Point** to clear the point that was previously drawn.

4)Click **Close** and the system will close the region automatically.

12. Click **Apply**.

4.2.2 Human Face Mode

Human face mode supports the following smart ATM protection rule types: normal human face, abnormal human face, multiple human faces, wearing sunglasses, and using mobile phone. Only one rule can be set for the mode, the rule can contain one or more ATM protection rule types. You can set the alarm response actions once the configured rule is triggered.

Steps

1. Go to **System → Event → Smart ATM Event** .

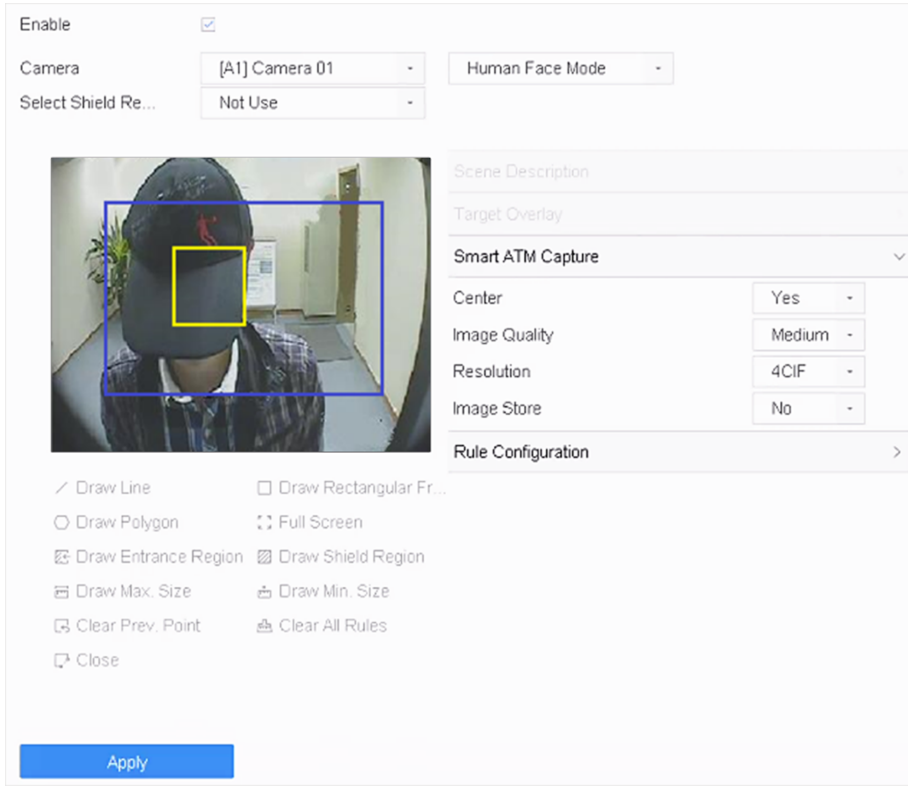

Figure 4-4 Human Face Mode

2. Check **Enable**.
3. Select an analog camera.
4. Select **Human Face Mode**.
5. Set **Smart ATM Capture** parameters for captured image.
6. Set **Rule Configuration**.
   1) Check **Enable** of the selected rule.
   2) Double click the rule, or click .
   3) Set **Name**, **Type**, **Alarm Duration**.
   4) Click **OK**.
7. Draw the human face detection region. It is recommended to click **Full Screen** to the draw detection region as full-screen.
8. **Optional:** Click **Draw Max. Size/Draw Min. Size** to draw the maximum/minimum filtering size of the human face.

Note

- It is recommended to use 0 for size filtering, which the device will automatically calculate and set the filtering size.
- The max. face size should be larger than the min. face size.

9. **Optional:** Set the shield region. The shield region is used to shield environment interferences or other influences which may cause false alarms.

1) Select a shield region in **Select Shield Region**.
2) Click **Draw Shield Region**.
3) Click on the live view image to draw points of the region. You can click **Clear Prev. Point** to clear the point that was previously drawn.
4) Click **Close** and the system will close the region automatically.

10. Click of the selected rule to set alarm response actions. Refer to ***Configure Linkage Actions*** and ***Configure Arming Schedule*** for details.

11. Click **Apply**.

4.3 VCA Event Alarm

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

Note

- VCA detections must be supported by the connected IP camera.
- Refer to the network camera user manual for detailed VCA detection instructions.

4.3.1 Facial Detection

The facial detection detects the face appearing in the surveillance scene. Linkage actions can be triggered when a human face is detected.

Steps

1. Go to **System → Event → Smart Event** .

2. Click **Face Detection**.

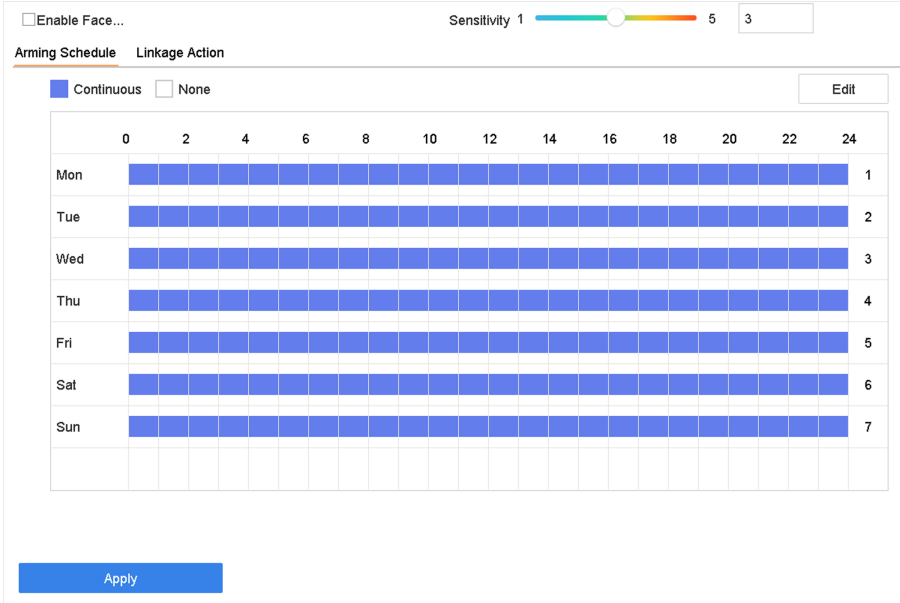

Figure 4-5 Facial Detection

3. Select a camera to configure.
4. Check **Enable Face Detection**.
5. **Optional:** Check **Save VCA Picture** to save the captured pictures of face detection.
6. Set the detection sensitivity. Sensitivity range: [1-5]. The higher the value is, the more easily the face will be detected.
7. Set the arming schedule. Refer to ***Configure Arming Schedule***
8. Set linkage actions. Refer to ***Configure Linkage Actions***
9. Click **Apply**.

4.3.2 Vehicle Detection

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

Steps

1. Go to **System → Event → Smart Event** .
2. Select a camera to configure.
3. Click **Vehicle**.

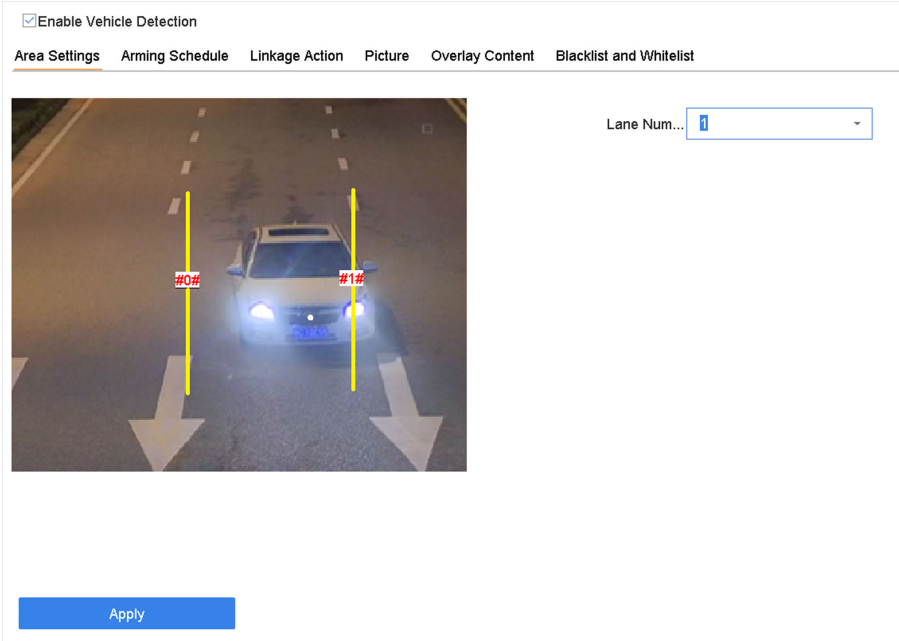

Figure 4-6 Vehicle Detection

4. Check **Enable Vehicle Detection**.
5. **Optional:** Check **Save VCA Picture** to save the captured vehicle detection pictures.
6. Set the arming schedule.Refer to ***Configure Arming Schedule***
7. Set the linkage actions. Refer to ***Configure Linkage Actions***
8. Configure rules, including **Area Settings**, **Picture**, **Overlay Content**, and **Blacklist and Whitelist**.

   Area Settings

   Up to 4 lanes are selectable.

   Blacklist and Whitelist

   You can export the file first to see its format, and edit it and import it to the device.
9. Click **Apply**.

Note

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

4.3.3 Line Crossing Detection

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

Steps

1. Go to **System → Event → Smart Event** .
2. Click **Line Crossing**.

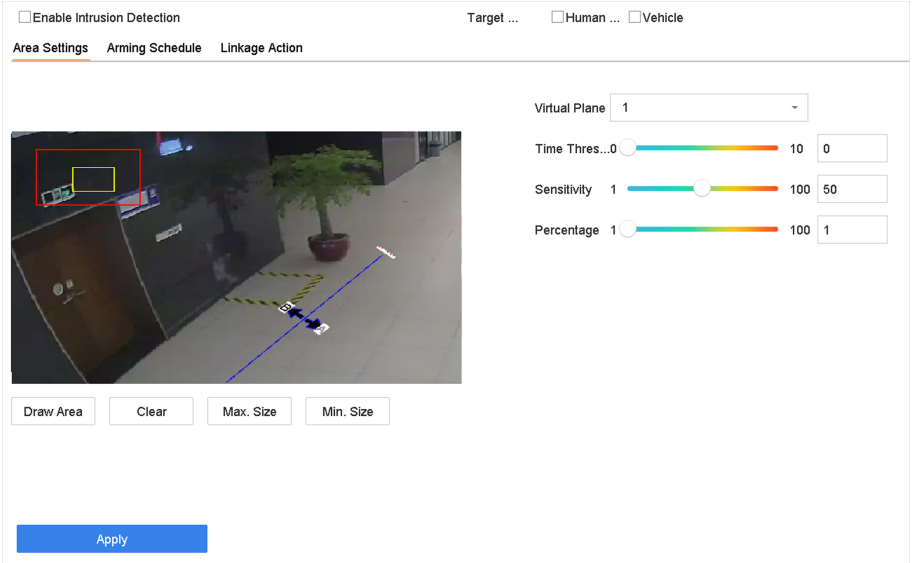

Figure 4-7 Line Crossing Detection

3. Select a camera.
4. Check **Enable Line Crossing Detection**.
5. **Optional:** Check **Save VCA Picture** to save the captured pictures of line crossing detection.
6. Set the line crossing detection rules and detection areas.
   1) Select an arming area.
   2) Select **Direction** as **A<->B**, **A->B**, or **A<-B**.

      A<->B

      Only the arrow on the B side shows. When an object goes across the configured line with both directions can be detected and alarms are triggered.

      A->B

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

      B->A

      Only the object crossing the configured line from the B side to the A side can be detected.
   3) Set the detection sensitivity. The higher the value is, the more easily the detection alarm can be triggered.
   4) Click **Draw Region**.
   5) Draw a virtual line in the preview window.
7. **Optional:** Draw the maximum size/minimum size for targets. Only the targets in the size ranging from max.size to min. size will trigger line crossing detection.
   1) Click **Max. Size/Min. Size**.
   2) Draw an area in preview window.
   3) Click **Stop Drawing**.
8. Set the arming schedule. Refer to ***Configure Arming Schedule*** .
9. Set linkage actions. Refer to ***Configure Linkage Actions*** .
10. Click **Apply**.

4.3.4 Intrusion Detection

The Intrusion detection function detects people, vehicles or other objects that enter and loiter in a pre-defined virtual region. Specific actions can be taken when an alarm is triggered.

Steps

1. Go to **System → Event → Smart Event** .
2. Click **Intrusion**.

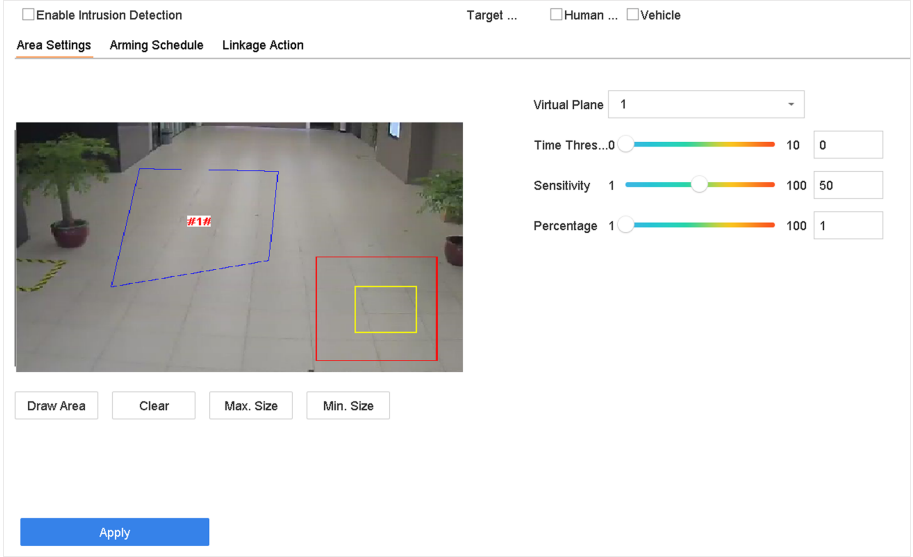

Figure 4-8 Intrusion Detection

3. Check **Enable Intrusion Detection**.
4. **Optional:** Check **Save VCA Picture** to save the captured intrusion detection pictures.
5. Set the detection rules and detection areas.
   1) Select a virtual panel. Up to 4 virtual panels are selectable.
   2) Set **Time Threshold**, and **Sensitivity**.

      Time Threshold

      The time an object loiter in the region. When the duration of the object in the defined detection area exceeds the threshold, the device will trigger an alarm.

      Sensitivity

      The size of the object that can trigger the alarm. The higher the value is, the more easily the detection alarm will be triggered.
   3) Click **Draw Area**.
   4) Draw a quadrilateral in the preview window.
6. **Optional:** Draw the maximum size/minimum size for targets. Only the targets in the size ranging from max.size to min. size will trigger line crossing detection.
   1) Click **Max. Size/Min. Size**.
   2) Draw an area in preview window.
   3) Click **Stop Drawing**.

7. Set the arming schedule. Refer to ***Configure Arming Schedule*** .
8. Set linkage actions. Refer to ***Configure Linkage Actions*** .
9. Click **Apply**.

4.3.5 Region Entrance Detection

Region entrance detection detects objects that enter a predefined virtual region.

Steps

1. Go to **System Management → Event Settings → Smart Event** .
2. Click **Region Entrance Detection**.

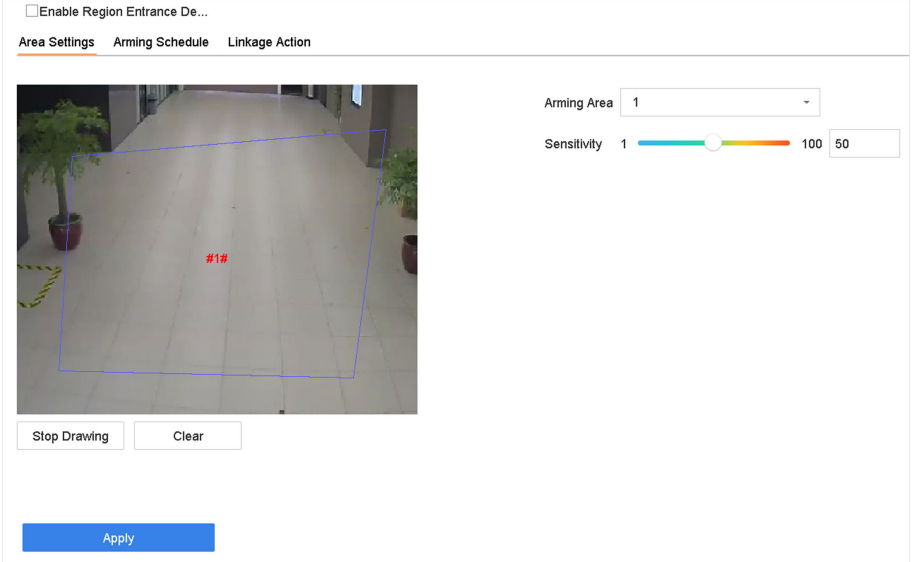

Figure 4-9 Region Entrance Detection

3. Select a camera.
4. Check **Enable Region Entrance Detection**.
5. **Optional:** Check **Save VCA Picture** to save the captured pictures of region entrance detection pictures.
6. Set detection rules and detection areas.
   1) Select **Arming Region**. Up to 4 regions are selectable.
   2) Set **Sensitivity**. The higher the value is, the easier the detection alarm will be triggered. Its range is [0-100].
   3) Click **Draw Region**, and draw a quadrilateral in the preview window.
7. Set the arming schedule. Refer to ***Configure Arming Schedule*** .
8. Set linkage actions. Refer to ***Configure Linkage Actions*** .
9. Click **Apply**.

4.3.6 Region Exiting Detection

Region exiting detection detects objects that exit from a predefined virtual region.

Steps

1. Go to **System → Event → Smart Event** .
2. Click **Region Exiting**.

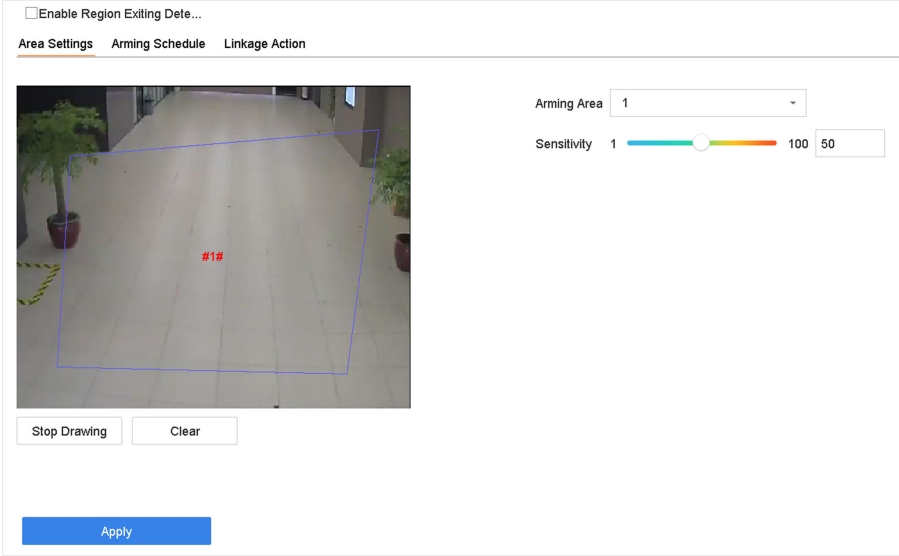

Figure 4-10 Region Exiting Detection

3. Select a camera.
4. Check **Enable Region Exiting Detection**.
5. **Optional:** Check **Save VCA Picture** to save the captured region exiting detection pictures.
6. Follow these steps to set the detection rules and detection areas.
   1) Select **Arming Region**. Up to 4 regions are selectable.
   2) Set **Sensitivity**. The higher the value is, the more easily the detection alarm will be triggered. Its range is [0-100].
   3) Click **Draw Region** and draw a quadrilateral in the preview window.
7. Set the arming schedule. Refer to ***Configure Arming Schedule*** .
8. Set linkage actions. Refer to ***Configure Linkage Actions*** .
9. Click **Apply**.

4.3.7 Defocus Detection

Image blur caused by lens defocus can be detected.

Steps

1. Go to **System → Event → Smart Event** .
2. Click **Defocus**.

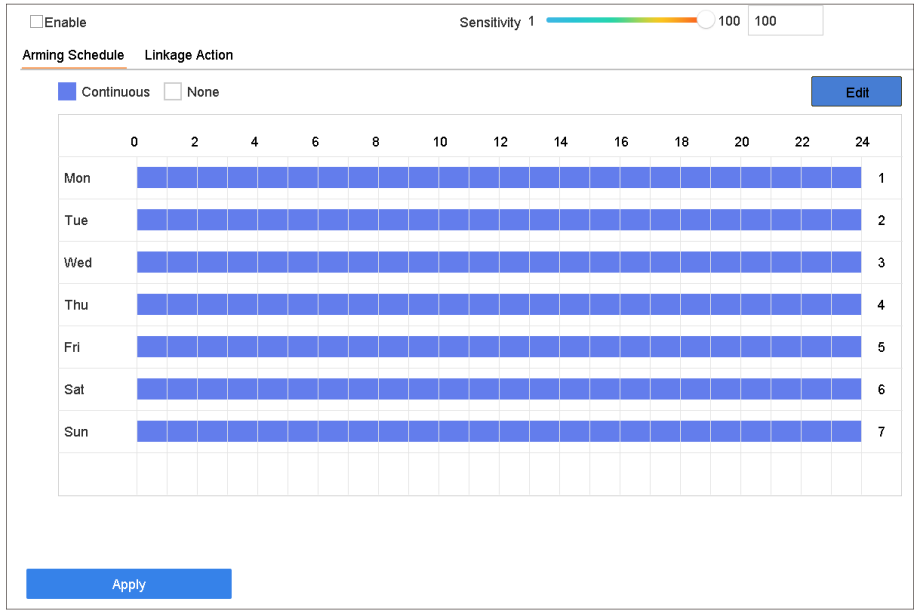

Figure 4-11 Defocus Detection

3. Select a camera to configure.
4. Check **Enable**.
5. **Optional:** Check **Save VCA Picture** to save the captured defocus detection pictures.
6. Drag the **Sensitivity** slider to set the detection sensitivity.

Note

Sensitivity range: [1-100]. The higher the value, the more easily the defocus image will be detected.

7. Set the arming schedule.Refer to ***Configure Arming Schedule*** .
8. Set the linkage actions. Refer to ***Configure Linkage Actions*** .
9. Click **Apply**.

4.3.8 Object Removal Detection

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

Steps

1. Go to **System → Event → Smart Event** .
2. Click **Object Removable**.

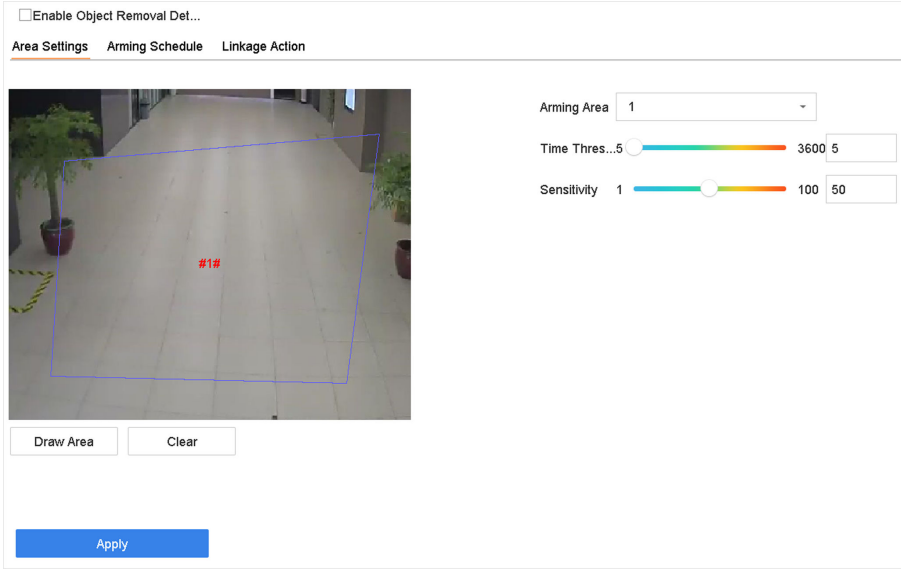

Figure 4-12 Object Removal Detection

3. Select a camera to configure.
4. Check **Enable Object Removable Detection**.
5. **Optional:** Check **Save VCA Picture** to save the captured object removable detection pictures.
6. Follow these steps to set the detection rules and detection areas.
   1) Select Arming Region. Up to 4 regions are selectable.
   2) Drag the sliders to set **Time Threshold** and **Sensitivity**.

      Time Threshold

      The time of the objects removed from the region. If the value is 10, alarm will be triggered after the object disappears from the region for 10s. Its range is [5s-20s].

      Sensitivity

      The similarity degree of the background image. If the sensitivity is high, a very small object taken from the region will trigger the alarm.
   3) Click **Draw Area** and draw a quadrilateral in the preview window by specifying four vertices of the detection region.
7. Set the arming schedule.Refer to ***Configure Arming Schedule*** .
8. Set the linkage actions. Refer to ***Configure Linkage Actions*** .
9. Click **Apply**.

4.3.9 Audio Exception Detection

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

Steps

1. Go to **System → Event → Smart Event** .
2. Click **Audio Exception**.

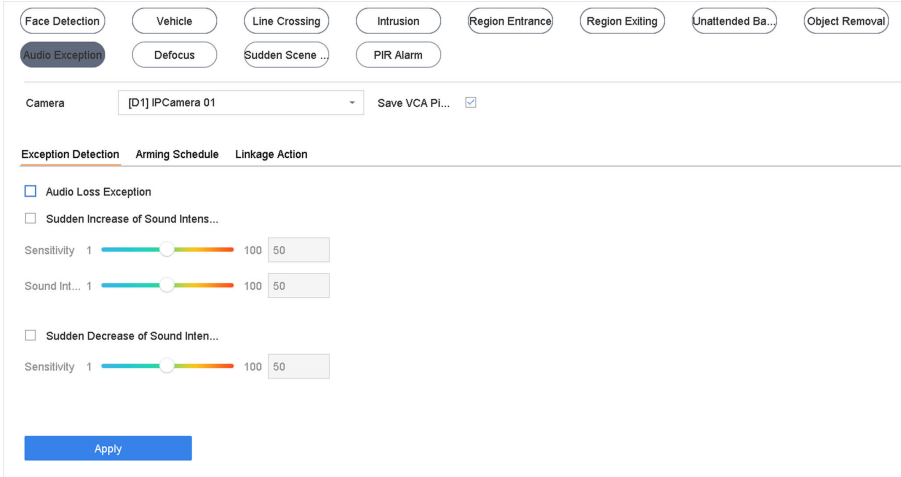

Figure 4-13 Audio Exception Detection

3. Select a camera to configure.
4. **Optional:** Check **Save VCA Picture** to save the captured audio exception detection pictures.
5. Set the detection rules:
   1) Select **Exception Detection**.
   2) Check **Audio Loss Exception**,**Sudden Increase of Sound Intensity Detection**,and/or **Sudden Decrease of Sound Intensity Detection**.

      Audio Loss Exception

      Detects a steep sound rise in the surveillance scene. You can set the detection sensitivity and threshold for steep sound rise by configuring its **Sensitivity** and **Sound Intensity Threshold**

      Sensitivity

      The smaller the value, the more severe the change must be to trigger the detection. Range [1-100].

      Sound Intensity Threshold

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

      Sudden Decrease of Sound Intensity Detection

      Detects a steep sound drop in the surveillance scene. You need set the detection sensitivity [1-100].
6. Set the arming schedule. Refer to ***Configure Arming Schedule*** .
7. Set the linkage actions. Refer to ***Configure Linkage Actions*** .
8. Click **Apply**.

4.3.10 Sudden Scene Change Detection

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

Steps

1. Go to **System → Event → Smart Event** .
2. Click **Sudden Scene Change**.

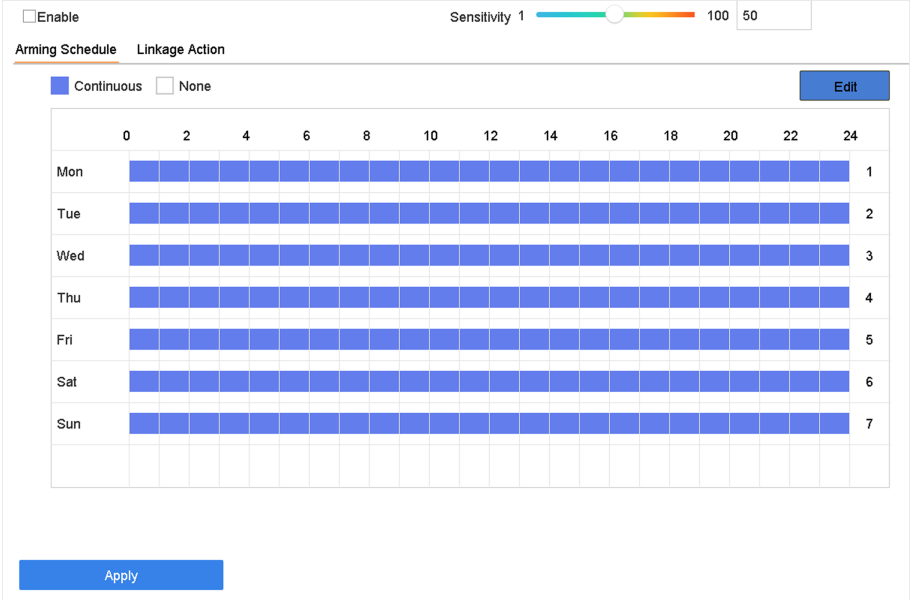

Figure 4-14 Sudden Scene Change

3. Select a camera to configure.
4. Check **Enable**.
5. **Optional:** Check **Save VCA Picture** to save the captured sudden scene change detection pictures.
6. Drag the **Sensitivity** slider to set the detection sensitivity.

Note

Sensitivity range: [1-100]. The higher the value, the more easily the change of scene can trigger the alarm.

7. Set the arming schedule.Refer to ***Configure Arming Schedule*** .
8. Set the linkage actions. Refer to ***Configure Linkage Actions*** .
9. Click **Apply**.

4.3.11 Unattended Baggage Detection

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

Steps

1. Go to **System → Event → Smart Event** .
2. Click **Unattended Baggage**.

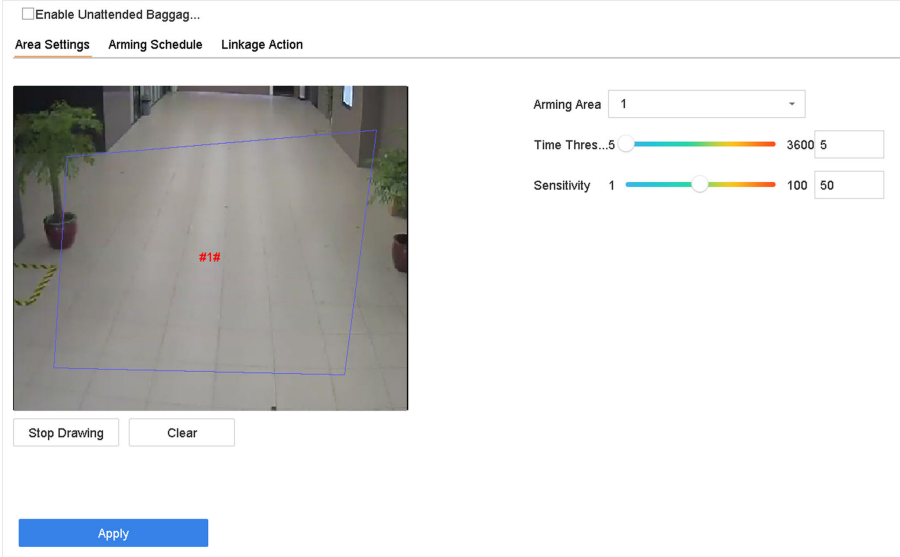

Figure 4-15 Unattended Baggage Detection

3. Select a camera.
4. Check **Enable Unattended Baggage Detection**.
5. **Optional:** Check **Save VCA Picture** to save the captured unattended baggage detection pictures.
6. Set the detection rules and detection areas.
   1) Select **Arming Region**. Up to 4 regions are selectable.
   2) Drag the sliders to set **Time Threshold** and **Sensitivity**.

      Time Threshold

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

      Sensitivity

      Similarity of the background image to the object. The higher the value, the easier the detection alarm will be triggered.
   3) Click **Draw Region** and draw a quadrilateral in the preview window.
7. Set the arming schedule. Refer to ***Configure Arming Schedule*** .
8. Set linkage actions. Refer to ***Configure Linkage Actions*** .
9. Click **Apply**.

4.3.12 PIR Alarm

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

Steps

1. Go to **System → Event → Smart Event** .
2. Click **PIR Alarm**.

Figure 4-16 PIR Alarm

3. Select a camera to configure.
4. Check **PIR Alarm**.
5. **Optional:** Check **Save VCA Picture** to save the captured of PIR alarm pictures.
6. Set the arming schedule.Refer to ***Configure Arming Schedule*** .
7. Set the linkage actions. Refer to ***Configure Linkage Actions*** .
8. Click **Apply**.

4.3.13 Target Detection

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

Steps

1. In Live View mode, click Target Detection to enter the target detection interface.

2. Select different detection types: smart detection ( ), vehicle detection ( ), face detection ( ), and human body detection ( ).
3. Select the historical analysis ( ) or real-time analysis ( ) to obtain the results.

Note

The smart analysis results of the detection are displayed in the list. Click a result in list to play the related video.

4.4 Configure Arming Schedule

Steps

1. Click **Arming Schedule**.
2. Click **Edit**.
3. Select a day of the week and set the time period. Up to eight time periods can be set each day.

Note

Time periods cannot repeat or overlapped.

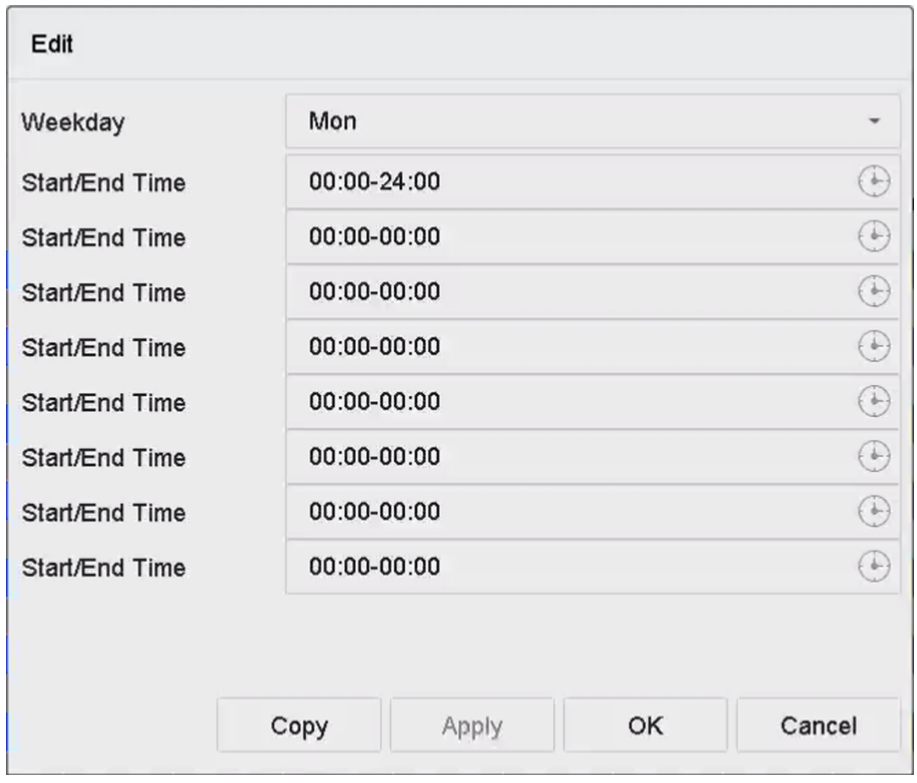

Figure 4-17 Set Arming Schedule

4. You can click **Copy** to copy the current day arming schedule settings to other day(s).
5. Click **Apply** to save the settings.

4.5 Configure Linkage Actions

Alarm linkage actions will be activated when an alarm or exception occurs, including Event Hint Display, Full Screen Monitoring, Audible Warning (buzzer), Notify Surveillance Center, Trigger Alarm Output, and Send Email.

4.5.1 Configure Auto-Switch Full Screen Monitoring

When an alarm is triggered, the local monitor displays in full screen the video image from the alarming channel configured for full screen monitoring. And when the alarm is triggered simultaneously in several channels, you must configure the auto-switch dwell time.

Note

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

Steps

1. Go to **System → View → General** .
2. Set the event output and dwell time.

   Event Output

   Select the output to show the event video.

   Full Screen Monitoring Dwell Time

   Set the time in seconds to show the alarm event screen. If alarms are triggered simultaneously in several channels, their full-screen images will be switched at an interval of 10 seconds (default dwell time).
3. Go to the **Linkage Action** interface of the alarm detection (e.g., motion detection, video tampering, face detection, etc.).
4. Select the **Full Screen Monitoring** alarm linkage action.
5. Select the channel(s) in **Trigger Channel** for full screen monitoring.

4.5.2 Configure Audio Warning

The audio warning has the system to trigger an audible beep when an alarm is detected.

Steps

1. Go to **System → View → General** .
2. Enable the audio output and set the volume.
3. Go to **Linkage Action** interface of the alarm detection (e.g., motion detection, video tampering, face detection, etc.).
4. Select the **Audio Warning** alarm linkage action.

4.5.3 Notify Surveillance Center

The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).

Steps

1. Go to **System → Network → Advanced → More Settings** .
2. Set the alarm host IP and alarm host port.
3. Go to **Linkage Action** interface of the alarm detection (e.g., motion detection, video tampering, face detection, etc.).
4. Select **Notify Surveillance Center**.

4.5.4 Configure Email Linkage

The system can send an email with alarm information to a user or users when an alarm is detected.

Steps

1. Go to **System → Network → Advanced → Email** .
2. Set the email parameters.
3. Click **Apply**.
4. Go to the **Linkage Action** interface of the alarm detection (e.g., motion detection, video tampering, face detection, etc.).
5. Select **Send Email** alarm linkage action.

4.5.5 Configure PTZ Linkage

The system can trigger the PTZ actions (e.g., call preset/patrol/pattern) when the alarm event, or VCA detection events occurs.

Before You Start

Make sure the connected PTZ or speed dome connected supports PTZ linkage.

Steps

1. Go to **Linkage Action** interface of the alarm input or VCA detection (e.g., face detection, line crossing detection, intrusion detection, etc.).
2. Select the **PTZ Linkage**.
3. Select the camera to perform the PTZ actions.
4. Select the preset/patrol/pattern No. to call when the alarm events occur.

Note

You can set only one PTZ type for the linkage action each time.

Chapter 5 Camera Settings

5.1 Configure Image Parameters

You can customize image parameters, including day/night switch, backlight, contrast, and saturation in **Camera → Display** .

Image Settings

Customize the image parameters including brightness, contrast, and saturation.

Exposure

Set the camera exposure time (1/10000 to 1 sec). A larger exposure value results in a brighter image.

Day/Night Switch

Set the camera to day, night, or auto switch mode according to time or the surrounding illumination condition. When the light diminishes at night, the camera can switches to night mode with high quality black and white image.

Backlight

Set the camera's wide dynamic range (0 to 100). When the surrounding illumination and the object have large differences in brightness, you can set the WDR value to balance the brightness level of the whole image.

Image Enhancement

For optimized image contrast enhancement that reduces noise in video stream.

5.2 Configure OSD Settings

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

Steps

1. Go to **Camera → Display** .
2. Select a camera as your desire.
3. Edit name in **Camera Name**.
4. Check **Display Name**, **Display Date** and **Display Week** to show the information on the image.
5. Set the date format, time format, and display mode.

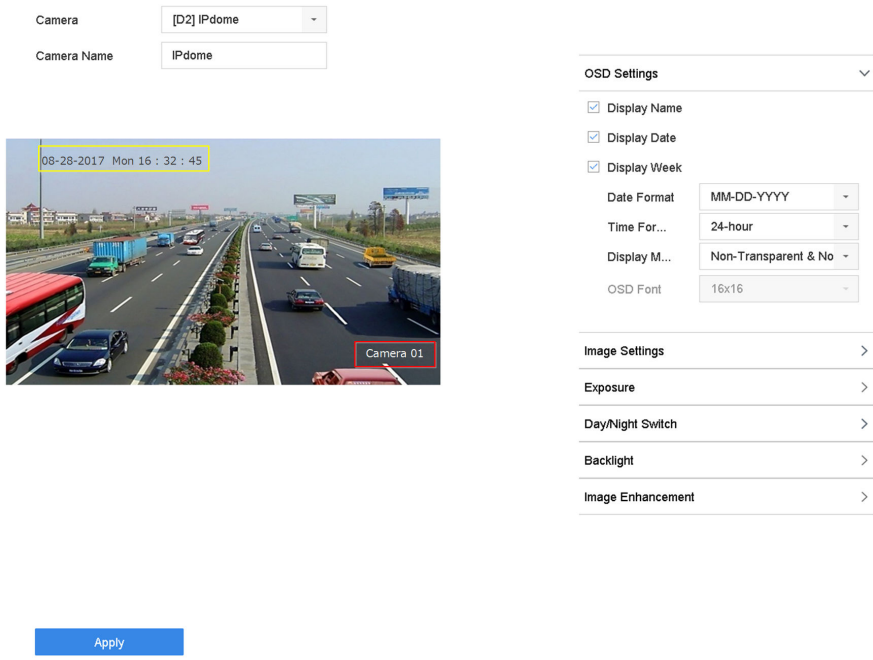

Figure 5-1 OSD Configuration Interface

6. Drag the text frame on the preview window to adjust the OSD position.
7. Click **Apply**.

5.3 Configure Privacy Mask

The privacy mask protects personal privacy by concealing parts of the image from kive view or recording with a masked area.

Steps

1. Go to **Camera → Privacy Mask** .
2. Select a camera to set privacy mask.
3. Check **Enable**.
4. Draw a zone on the window. The zone will be marked by different frame colors.

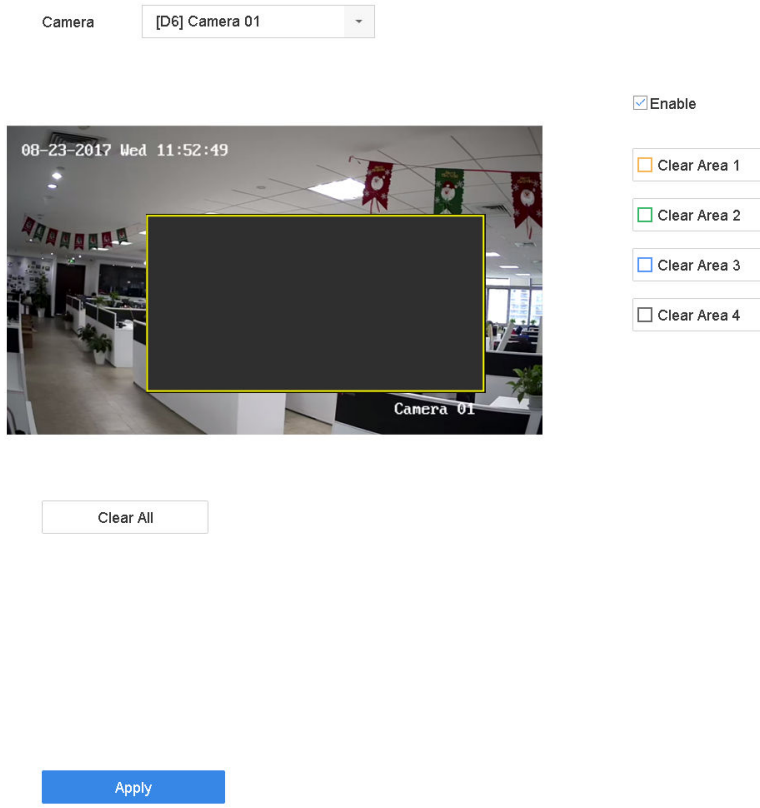

Figure 5-2 Privacy Mask Settings Interface

Note

- Up to 4 privacy masks zones can be configured and the size of each area can be adjusted.
- You can clear the configured privacy mask zones on the window by clicking the corresponding clear zone 1 to 4 icons on the right of the window, or click **Clear All** to clear all zones.

5. Click **Apply**.

Chapter 6 Storage

6.1 Manage Local HDD

6.1.1 Configure HDD Group

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

Steps

1. Go to **Storage → Storage Mode** .
2. Select **Mode** as **Group**.
3. Click **Apply**.
4. Go to **Storage → Storage Device** .
5. Select a HDD.

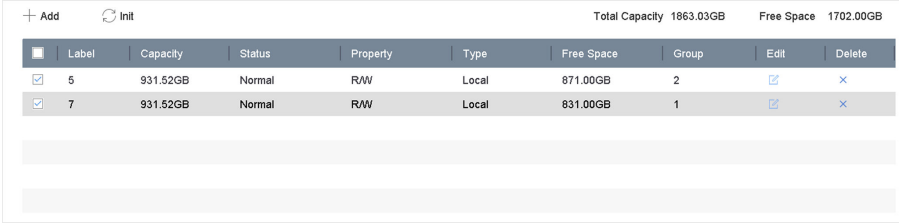

Figure 6-1 Storage Device

6. Click to enter Local HDD Settings interface.

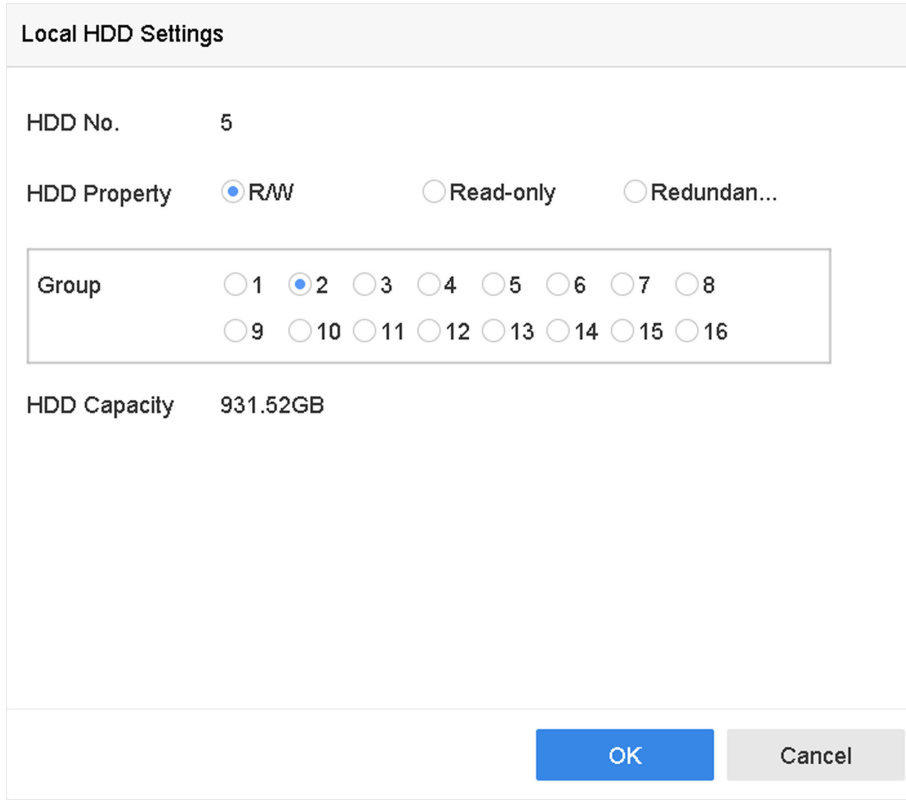

Figure 6-2 Local HDD Settings

7. Select a group number for the HDD.
8. Click **OK**.

Note

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

9. Go to **Storage → Storage Mode** .
10. Select group number from the list.
11. Select related camera(s) to save videos and pictures on the HDD group.
12. Click **Apply**.

6.1.2 Configure the HDD Property

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

Before You Start

Set the storage mode to Group. For detailed steps, refer to ***Configure HDD Group***

Steps

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

R/W

HDD supports both read and write.

Read-only

Files in read-only HDD will not be overwritten.

Redundant

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

4. Click **OK**.

6.1.3 Configure the HDD Quota

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

Steps

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

Note

- When the quota capacity is set to 0, all cameras will use the total capacity of HDD for videos and pictures.
- Reboot the video recorder to activate the new settings.

6.2 Add a Network Disk

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

Steps

1. Go to **Storage → Storage Device** .
2. Click **Add**.

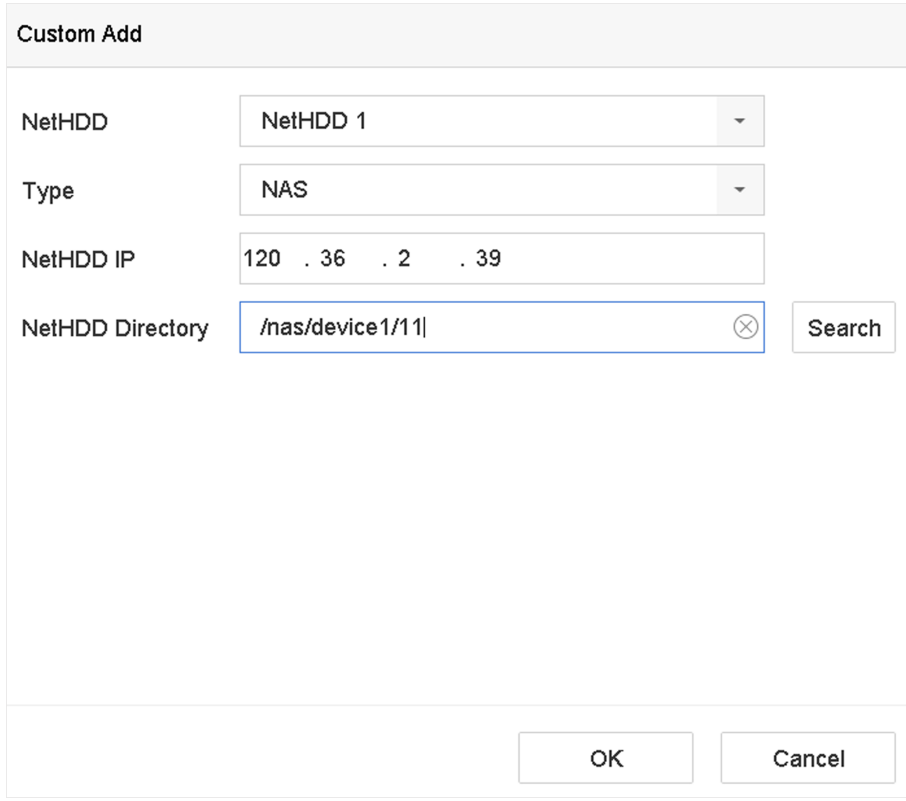

Figure 6-3 Add NetHDD

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

Chapter 7 Network Settings

7.1 Configure TCP/IP Settings

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

Steps

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

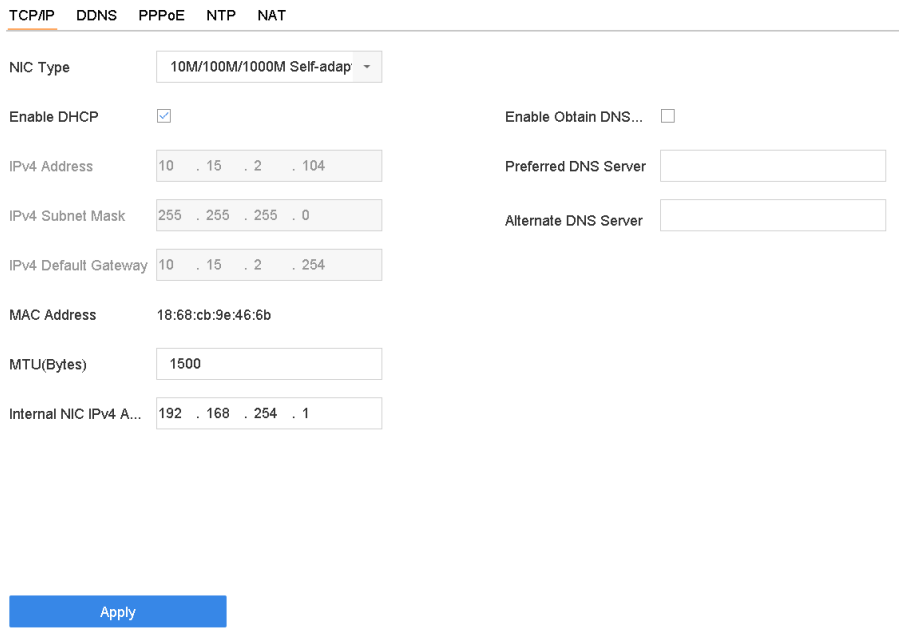

Figure 7-1 TCP/IP Settings

2. Configure network parameters as needed.

Note

- Check **Enable DHCP** to obtain IP settings automatically if a DHCP server is available on the network.
- Valid MTU value range is 500 to 9676.

3. Click **Apply**.

7.2 Configure DDNS

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

Before You Start

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

Steps

1. Go to **System → Network → TCP/IP → DDNS**

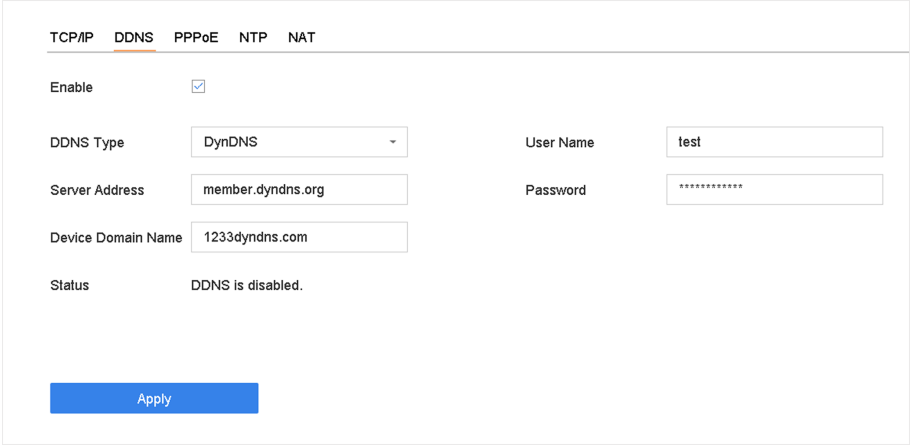

Figure 7-2 DDNS Settings

2. Check **Enable**.
3. Select **DDNS Type** as DynDNS.
4. Enter Server Address for DynDNS (i.e., members.dyndns.org).
5. Under Device Domain Name, enter the domain name obtained from the DynDNS Website.
6. Enter **User Name** and **Password** registered in the DynDNS Website.
7. Click **Apply**.

7.3 Configure PPPoE

If the device is connected to the Internet through PPPoE, you need to configure the user name and password accordingly under **System → Network → TCP/IP → PPPoE** .

Note

Contact your Internet service provider for details about PPPoE service.

7.4 Configure NTP

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

Steps

1. Go to **System → Network → TCP/IP → NTP** .

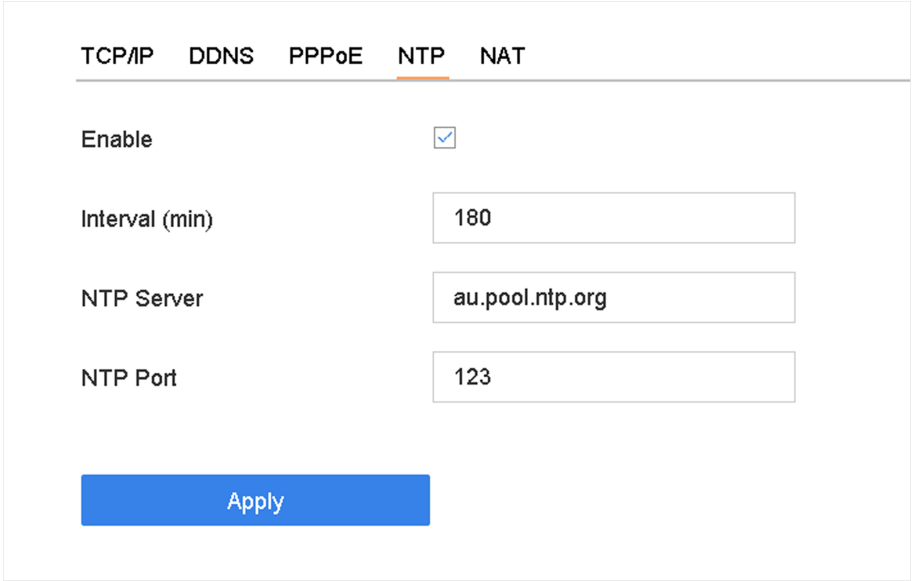

Figure 7-3 NTP Settings

2. Check **Enable**.
3. Configure NTP settings as need.

   Interval (min)

   Time interval between two time synchronization with NTP server.

   NTP Server

   IP address of the NTP server.

   NTP Port

   Port of the NTP server.
4. Click **Apply**.

7.5 Configure Port

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

Steps

1. Go to **System → Network → Advanced → More Settings** .

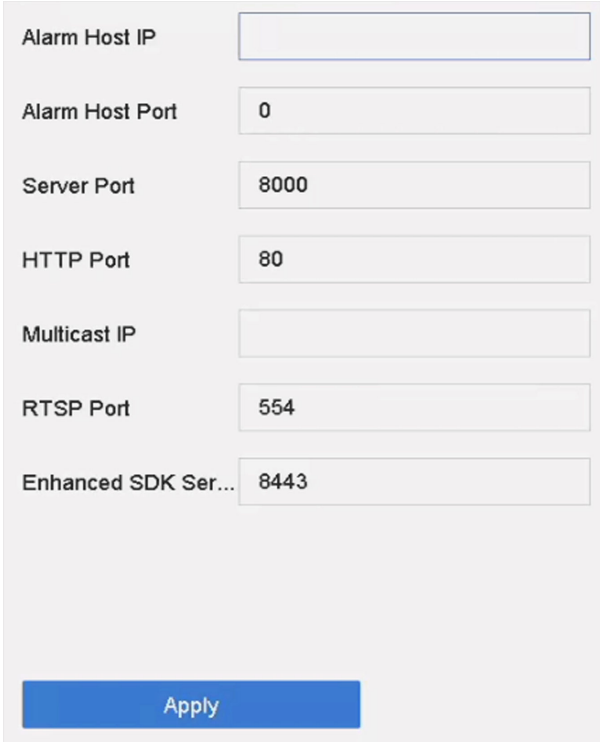

Figure 7-4 Port Settings

2. configure port settings as needed.

Alarm Host IP/Port

With a remote alarm host configured, the device will send the alarm event or exception message to the host when an alarm is triggered. The remote alarm host must have the client management system (CMS) software installed.The alarm host IP refers to the IP address of the remote PC on which the CMS software (e.g., iVMS-4200) is installed, and the alarm host port (7200 by default) must be the same as the alarm monitoring port configured in the software.

Server Port

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

HTTP Port

HTTP port (80 by default) should be configured for remote Web browser access.

Multicast IP

Multicast can be configured to enable Live View for cameras that exceed the maximum number allowed through network. A multicast IP address covers Class-D IP ranging from 224.0.0.0 to 239.255.255.255 and it is recommended to use an IP address ranging from 239.252.0.0 to 239.255.255.255. When adding a device to the CMS software, the multicast address must be the same as that of the device.

RTSP Port

RTSP (Real Time Streaming Protocol) is a network control protocol designed to control streaming media servers. The port is 554 by default.

Enhanced SDK Service Port

The enhanced SDK service adopts TLS protocol over the SDK service that provides safer data transmission. The port is 8443 by default.

3. Click **Apply**.

7.6 Configure Port Mapping (NAT)

Two ways are provided for port mapping to realize the remote access via the cross-segment network, UPnP™ and manual mapping.

Before You Start

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

Universal Plug and Play (UPnP™) can permit the device seamlessly discover the presence of other network devices on the network and establish functional network services for data sharing, communications, etc. You can use the UPnP™ function to enable the fast connection of the device to the WAN via a router without port mapping.

Steps

1. Go to **Menu → Configuration → Network → NAT** .

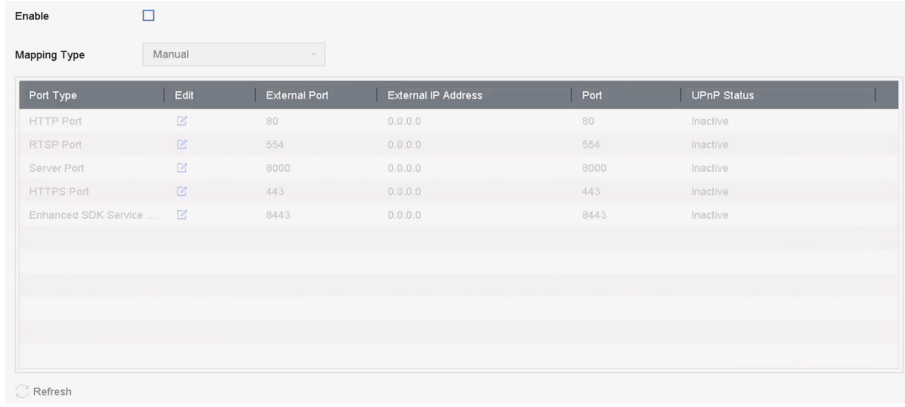

Figure 7-5 Port Mapping Setting

2. Check **Enable**.
3. Select **Mapping Type** as **Manual** or **Auto**.
   - Auto:If you select **Auto**, the port mapping items are read-only, and the external ports are set by the router automatically.
   - Manual:If you select **Manual**, you can edit the external port on your demand by clicking to activate **External Port Settings**.

Note

- You can use the default port No., or change it according to actual requirements.
- External Port indicates the port No. for port mapping in the router.
- The value of the RTSP port No. should be 554 or between 1024 and 65535, while the value of the other ports should be between 1 and 65535 and the value must be different from each other. If multiple devices are configured for the UPnP™ settings under the same router, the value of the port No. for each device should be unique.

4. Enter the virtual server setting page of router; fill in the blank of **Internal Source Port** with the internal port value, the blank of **External Source Port** with the external port value, and other required contents.

Note

- Each item should be corresponding with the device port, including server port, http port, RTSP port and https port.
- The virtual server setting interface below is for reference only, it may be different due to different router manufactures. Please contact the manufacture of router if you have any problems with setting virtual server.

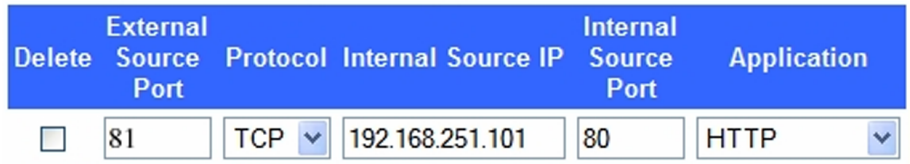

Figure 7-6 Setting Virtual Server Item

7.7 Configure ONVIF

ONVIF protocol allows the connection with third-party cameras. The added user accounts have the permission to connect other devices via ONVIF protocol.

Steps

1. Go to **System → System Service → ONVIF** .
2. Check **Enable ONVIF** to enable the ONVIF access management.

Note

ONVIF protocol is disabled by default.

3. Click **Add**.
4. Enter **User Name**, and **Password**

Caution

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

5. Select **Level** as **Media User**,**Operator** or **Admin**.
6. Click **OK**.

Chapter 8 ATM Settings

8.1 Network Interception

The transaction information of ATM, including transaction card No, transaction amount, transaction behaviour, etc., can be captured by monitoring the data package of the network communication.

Before You Start
Connect the device and the ATM (Automatic Teller Machine) to the network properly.

Steps
1. Go to **System → ATM Settings** .
2. Check **Enable ATM**.
3. Select **Input** as **Network Interception**.
4. Enter the ATM IP address.
5. Select a protocol. If you select **Custom**, refer to ***Custom Protocol Settings*** for details.
6. Click **Apply**.

8.2 Serial Port Interception

The transaction information, including transaction card No, transaction amount, transaction behaviour, etc., can be captured by monitoring the data package of the serial port communication.

Before You Start
Connect the device and the ATM (Automatic Teller Machine) via the serial port properly.

Steps
1. Go to **System → ATM Settings** .
2. Check **Enable ATM**.
3. Select **Input** as **Serial Port Interception**.
4. Select a protocol. If you select **Custom**, click **RS-232** to set **Protocol**, **Baud Rate**, **Data Bit**, etc. Refer to ***Custom Protocol Settings*** for custom parameter setting details.
5. Click **Apply**.

8.3 Network Protocol

TCP connection is established between the device and ATM in server/client mode. The transaction information, including transaction card No, transaction amount, transaction behavior, etc., will be sent from the ATM to the device.

Before You Start
Connect the device and the ATM (Automatic Teller Machine) to the network properly.

Steps
1. Go to **System → ATM Settings** .
2. Check **Enable ATM**.
3. Select **Input** as **Network Protocol**.
4. Set **Interception Port**. The interception port is 10000 by default.
5. Select a protocol.
6. Click **Apply**.

8.4 Serial Port Protocol

The transaction information, including transaction card No, transaction amount, transaction behaviour, etc., will be sent from the ATM to the device.

Before You Start
Connect the device and the ATM (Automatic Teller Machine) via the serial port properly.

Steps
1. Go to **System → ATM Settings** .
2. Check **Enable ATM**.
3. Select **Input** as **Serial Port Protocol**.
4. Set **Protocol**, **Baud Rate**, **Data Bit**, etc.
5. Click **Apply**.

8.5 Custom Protocol Settings

8.5.1 Configure Data Package

The start/end tag can be set to locate the data package in the captured message. You can also filter the specified content as your desire.

Steps
1. Click **Data Package**.

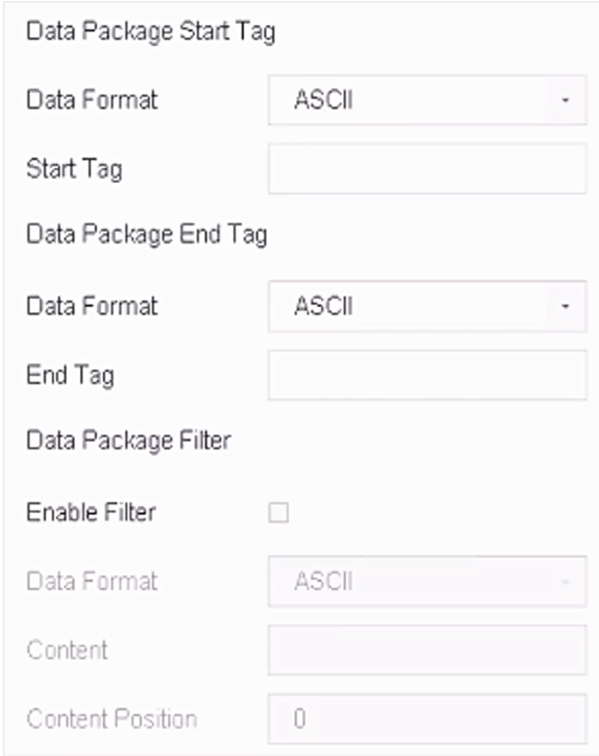

Figure 8-1 Data Package

2. Set **Data Format** in **Data Package Start Tag**.
3. Set **Start Tag** for the data package according to **Data Format**.
4. Set **Data Format** in **Data Package End Tag**.
5. Set **End Tag** for the data package according to **Data Format**.
6. **Optional:** Filter specified content.
   1) Check **Enable Filter**.
   2) Select a format in **Data format**.
   3) Enter the content in **Content**.
   4) Set **Content Position**
7. Click **OK**.

8.5.2 Configure Transaction Information

The device can analyze the transaction information which is contained in the captured message, including the card No., transaction behavior, transaction amount and serial No.

Steps

1. Click **Transaction Information**.

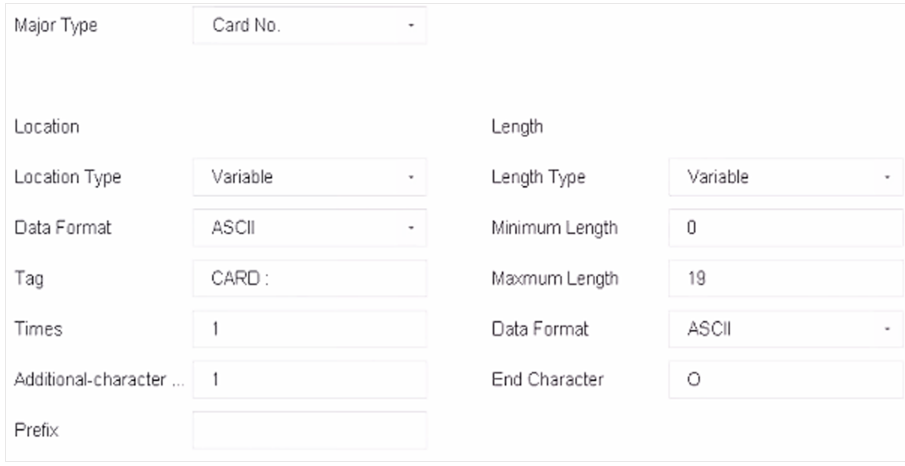

Figure 8-2 Transaction Information

2. Set **Major Type**.
3. Set **Minor Type**.

Note

When **Major Type** is set as **Transaction Behaviour**, 8 minor types are selectable: **Card In**, **Card Out**, **Overlay**, **Query**, **Withdrawal**, **Deposit**, **Change Password**, and **Transfer**.

4. Set location parameters to locate the selected transaction information in the captured message.
   - Set **Location Type** as **Variable**, and set **Data Format**, **Tag**, **Times** and **Additional-character Offset**.
   - Set **Location Type** as **Fixed**, and set **Fixed Offset**.
5. Set the length of the selected transaction information if **Major Type** is not set as **Transaction Behaviour**.
   - Set **Length Type** as **Variable**, and set the minimum length and maximum length for the transaction information, and then select data format and set the end character.
   - Set **Length Type** as **Fixed**, and set the fixed length value.
   - Set **Length Type** as **Auto**, set the length digits and length position, and then the length of the transaction information will be obtained from the message automatically.
6. Set **Prefix**, **Data Format**, and **Action Code**.
7. Click **OK**.

What to do next

You can click at lower-right corner of live view/playback to display transaction information.

8.5.3 Configure Trigger Channel

You can select the channels for the text overlay of transaction information and command triggered recording.

Steps

1. Click **Trigger Channel**.

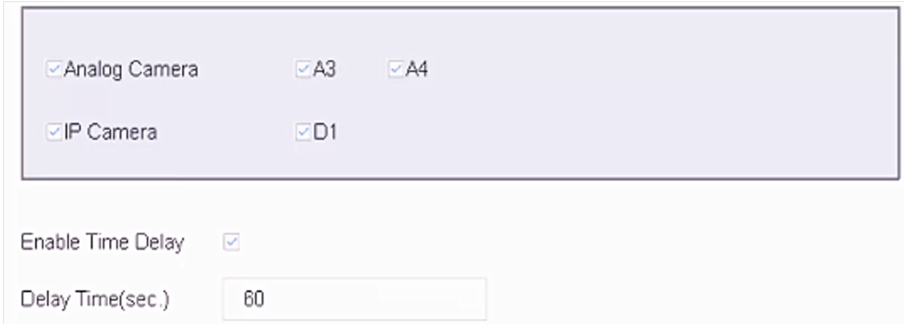

Figure 8-3 Trigger Channel

2. Select analog camera(s) or IP camera(s) for the text overlay of transaction information and command triggered recording.
3. Check **Enable Time Delay**.
4. Set **Delay Time** for menu display if there is no Card In or Card Out in the transaction information. The default value is 60, the range is from 0 to 65535.
5. Click **OK**.

8.5.4 Configure Overlay Position

You can configure the position of transaction text overlay on the display window.

Steps

1. Click **Overlay Position**.

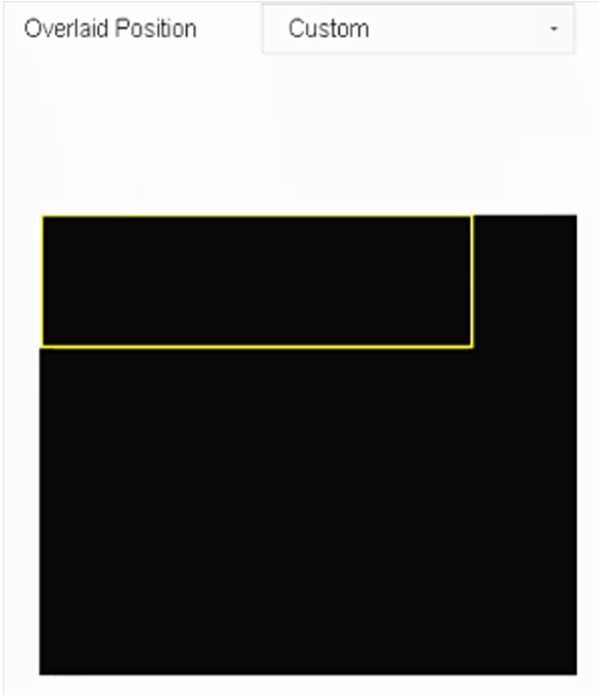

Figure 8-4 Overlay Position

2. Set whether to overly transaction information on the image.

None It will not overlay transaction information on the image.

Custom It will overlay transaction information on the image. You can drag the yellow rectangle to a desirable position.

3. Click **OK**.

Chapter 9 File Management

9.1 Search Files

Specify detailed conditions to search videos and pictures.

Steps

1. Go to **File Management → All Files/Human Files/Vehicle Files** .
2. Specify detailed conditions, including time, camera, event type, etc.

Note

- For All Files,select **Time**,**Camera**,**File Type**,**Event type**.
- For Human Files, select **Time**, **Camera** and **File Type** to search.
- For Vehicle Files,select **Time**,**Camera**,**File Type**,**Plate No.**,**Area/Country**.

3. Click **Search** to display results.The matched files will be displayed.
4. Select **Target Picture** or **Source Picture** in the menu bar to display related pictures only.
   - Target Picture:Display the search results of vehicle close-ups.
   - Source Picture:Display the search results of original pictures captured by camera.

9.2 Search History Operation

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

Steps

1. Go to **File Management → All Files/Human Files/Vehicle Files** .
2. Set the search conditions.
3. Click **Save**.
4. Enter a name in text field and click **Finished**. The saved search conditions will be displayed in **Search Condition** list.

Note

You can quickly search files by clicking a search condition.

9.3 Export Files

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

Steps

1. Search files to export.
2. Click files to select and click **Export**.
3. **Optional:** Check **Backup License Plate Statistics Info** to export license plate statistics information later.

   Note

   Only for vehicle files.

4. Select the file to export as **Video and log** and click **OK**.
5. Click **OK** to export files to backup devcie.

Chapter 10 User Management and Security

10.1 Manage User Accounts

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

10.1.1 Add a User

Steps

1. Go to **System → User** .
2. Click **Add** to enter the operation permission interface.
3. Input the admin password and click **OK**.
4. In the Add User interface, enter the information for a new user.

Caution

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

User Level

Set the user level to Operator or Guest. Different user levels have different operating permission.

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

User's MAC Address

The MAC address of the remote PC that logs onto the device. If it is configured and enabled, it allows only the remote user with this MAC address to access the device.

5. Click **OK**.
   In the User Management interface, the added new user is displayed on the list.

10.1.2 Edit the Admin User

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

Steps

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

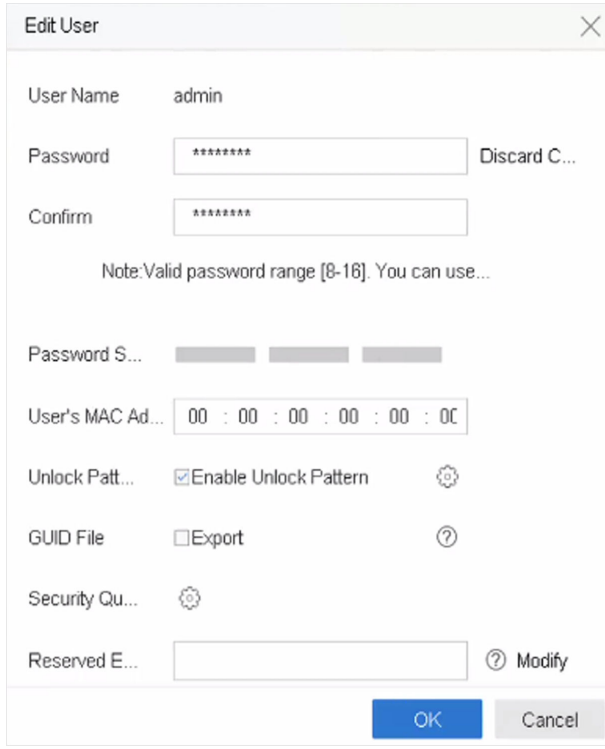

Figure 10-1 Edit User (Admin)

4. Edit the admin user information as desired, including a new admin password (strong password is required) and MAC address.
5. Edit the unlock pattern for the admin user account.
   1) Check **Enable Unlock Pattern** to enable the use of an unlock pattern when logging in to the device.
   2) Use the mouse to draw a pattern among the 9 dots on the screen, and release the mouse when the pattern is done.
6. Check **Export** of **GUID File** to export the GUID file for the admin user account.

Note

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

7. Configure security question for password resetting.
8. Configure reserved email for password resetting.

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

10.1.3 Edit an Operator/Guest User

You can edit the user information, including user name, password, permission level, and MAC address.

Steps

1. Go to **System → User** .
2. Select a user from the list and click **Modify**.

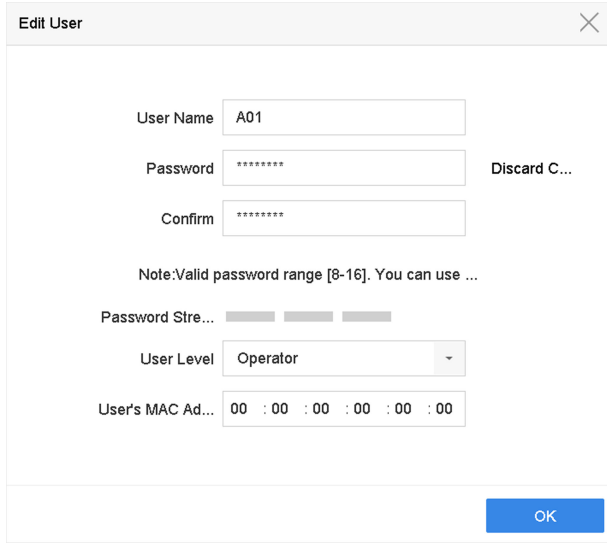

Figure 10-2 Edit User (Operator/Guest)

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

10.2 Manage User Permissions

10.2.1 Set User Permissions

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

Steps

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

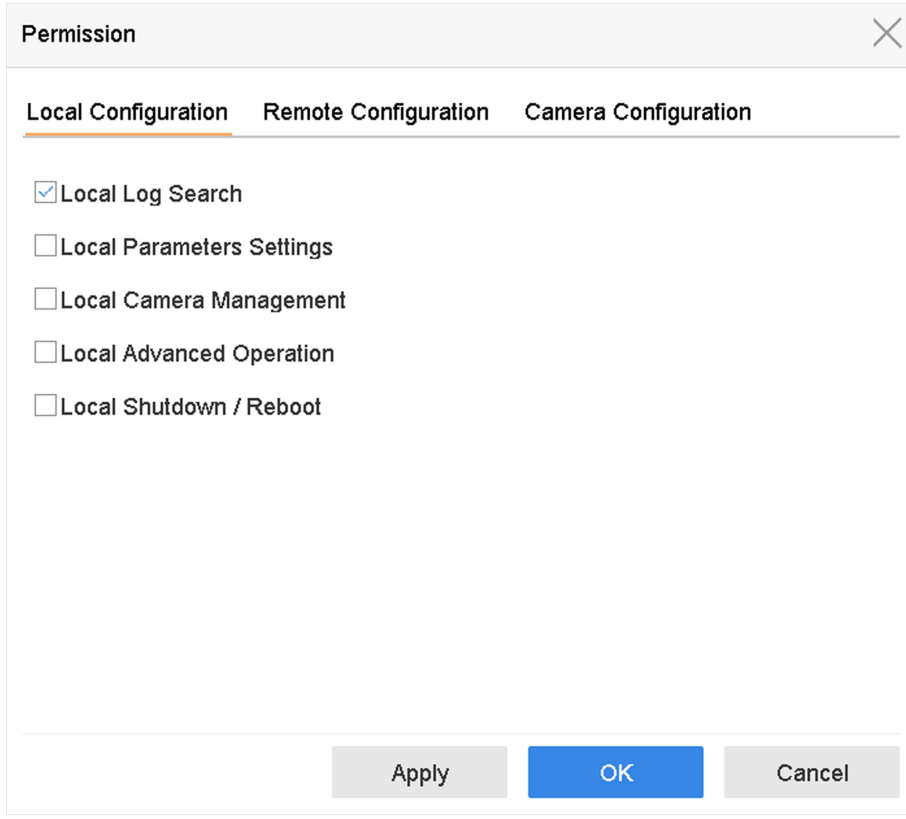

Figure 10-3 User Permission Settings Interface

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

1) Set Local Configuration

Local Log Search

Searching and viewing logs and system information of device.

Local Parameters Settings

Configuring parameters, restoring factory default parameters, and importing/exporting configuration files.

Local Camera Management

Adding, deleting, and editing of IP cameras.

Local Advanced Operation

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

Local Shutdown Reboot

Shutting down or rebooting the device.

2) Set Remote Configuration

Remote Log Search

Remotely viewing logs that are saved on the device.

Remote Parameters Settings

Remotely configuring parameters, restoring factory default parameters, and importing/exporting configuration files.

Remote Camera Management

Remote adding, deleting, and editing of the IP cameras.

Remote Serial Port Control

Configuring settings for RS-232 and RS-485 port settings.

Remote Video Output Control

Sending remote button control signals.

Two-Way Audio

Operating the two-way radio between the remote client and the device.

Remote Alarm Control

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

Remote Advanced Operation

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

Remote Shutdown/Reboot

Remotely shutting down or rebooting the device.

3) Set Camera Configuration

Remote Live View

Remotely viewing live video of the selected camera(s).

Local Manual Operation

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

Remote Manual Operation

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

Local Playback

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

Remote Playback

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

Local PTZ Control

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

Remote PTZ Control

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

Local Video Export

Locally exporting recorded files of the selected camera(s).

Local Live View

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

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

10.2.2 Set Live View Permission on Lock Screen

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

- The admin user can set this permission for user accounts.
- When the normal user (Operator or Guest) has no local live view permission for specific camera (s), the live view permission for such camera (s) on lock screen status cannot be configured (live view not allowed by default).

Steps

1. Go to **System → User** .
2. Click **Live View Permission on Lock Screen**.
3. Input admin password and click **Next**.

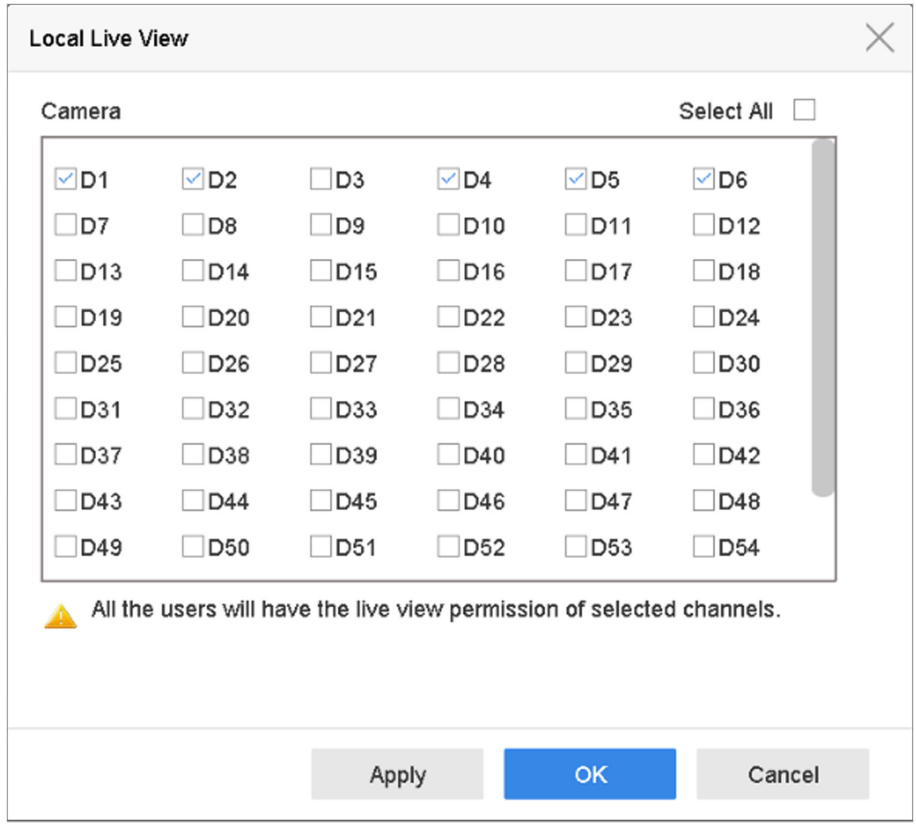

Figure 10-4 Set Live View Permissions on Lock Screen

4. Set the permissions.Select the camera (s) to allow live view when the current user account is in logout status.
5. Click **OK**.

10.3 Configure Password Security

10.3.1 Export GUID File

The GUID file can help you to reset password when you forget password. Please keep it properly.

Steps

1. Check **Export** and click **OK** to export GUID file when you are activating the device, or editing the admin user account.
2. Insert a USB flash drive to your device.and export the GUID file to the USB flash drive.

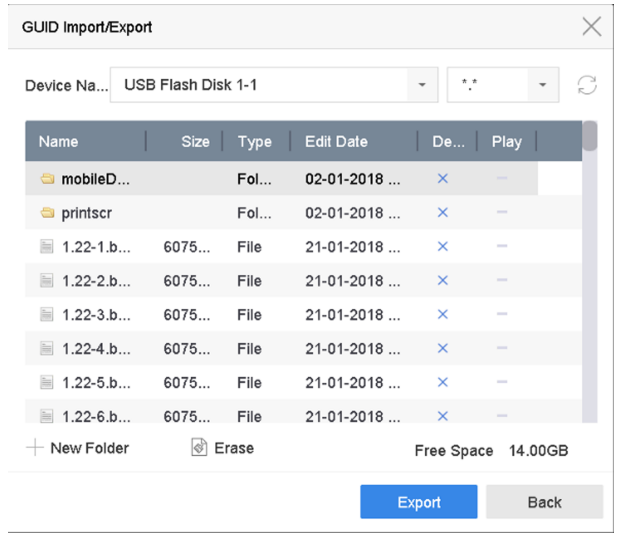

Figure 10-5 Export GUID File

3. Select a Device.
4. Select a directory on the device.
5. Click **Export**.

10.3.2 Configure Security Questions

The security questions can help you to reset password when you forget your password, or encounter security issues.

Steps

1. Click **Security Question Configuration** when you are activating the device, or editing the admin user account.
2. Select three security questions from the drop-down list and input the answers.

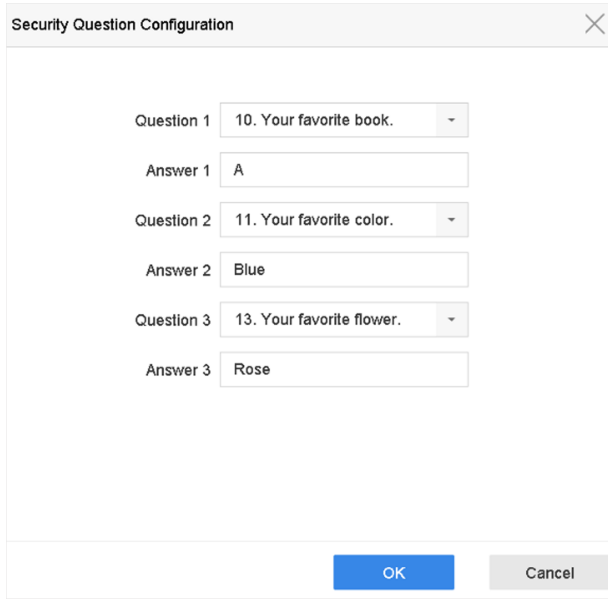

Figure 10-6 Configure Security Questions

3. Click **OK**.

10.3.3 Configure Reserved Email

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

Steps

1. Check **Reserved E-mail** when you are activating the device, or click **Modify** when you are editing the admin user account.
2. Enter reserved email address.

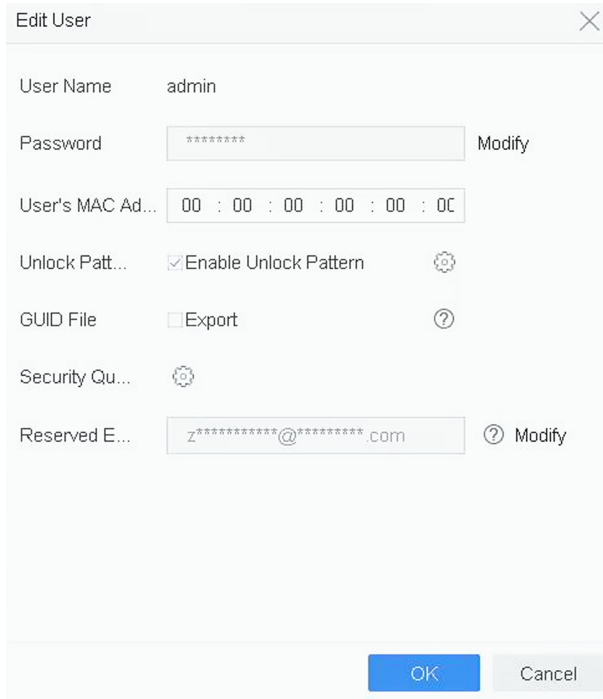

Figure 10-7 Configure Reserved Email

3. Click **OK**.

10.4 Reset Password

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

10.4.1 Reset Password by GUID

Before You Start

The GUID file must be exported and saved in the local U flash disk after you have activated the device or edited the admin user account.

Steps

1. On the user login interface, click **Forgot Password**.
2. On **Password Reset Type** , Select **Verify by GUID**.

Note

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

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

Note

If you have imported the wrong GUID file for 7 times, you will be not allowed to reset the password for 30 minutes.

4. After the GUID file is successfully imported, enter the reset password interface to set the new admin password.
5. Click **OK** to set the new password. You can export the new GUID file to the U flash disk for future password resetting.

Note

When the new password is set, the original GUID file will be invalid. The new GUID file should be exported for future password resetting. You can also enter **User → User Management** to edit the admin user and export the GUID file.

10.4.2 Reset Password by Security Questions

Before You Start

You have configured the security questions when you activate the device or edit the admin user account. (Refer to Chapter 17.3.2 Configure Security Questions).

Steps

1. On the user login interface, click **Forgot Password**.
2. Select the **password resetting type** as **Verify by Security Question** .
3. Input the correct answers of the three security questions.
4. Click **OK**.
5. Create the new admin password on the Reset Password interface.

10.4.3 Reset Password by Reserved Email

Before You Start

Ensure you have configured the reserved email when you are activating the device or editing the admin user account. (Refer to ***Configure Reserved Email***)

Steps

1. On the user login interface, click **Forgot Password**.
2. On the password reset type interface,Select **Verify by Reserved Email**.
3. Click **OK**.
4. Click **Next** if you accept the legal disclaimer. You can use a smartphone to scan the QR code and read the legal disclaimer.
5. Obtain the verification code. There are two ways to get the verification code.
   - Use Hik-Connect app to scan the QR code.
   - Send the QR code to email server.

a. Insert a USB flash drive to your device.
b. Click **Export** to export the QR code to USB flash drive.
c. Email the QR code to ***pw_recovery@hikvision.com*** as attachment.

6. Check your reserved email, and you will receive a verification code within 5 minutes.
7. Enter the verification code.
8. Click **OK** to set the new password.

Chapter 11 System Management

11.1 Configure Device

Steps

1. Go to **System → General** .
2. Configure the following settings.

Language

The default language used is English.

Output Standard

Set the output standard to NTSC or PAL, which must be the same as the video input standard.

Resolution

Configure video output resolution.

Device Name

Edit device name.

Device No.

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

Auto Logout

Set the timeout time for menu inactivity. E.g., when the timeout time is set to 5 minutes, then the system will exit from the current operation menu to Live View screen after 5 minutes of menu inactivity.

Mouse Pointer Speed

Set the speed of the mouse pointer; 4 levels are configurable.

Enable Wizard

Enable/disable the Wizard when the device starts up.

Enable Password

Enable/disable the use of the login password.

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

11.2 Configure Time

11.2.1 Manual Time Synchronization

Steps

1. Go to **System → General** .
2. Configure the date and time.
3. Click **Apply** to save the settings.

11.2.2 NTP Synchronization

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

Steps

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

   Interval (min)

   Time interval between two time synchronization with NTP server

   NTP Server

   IP address of the NTP server

   NTP Port

   Port of the NTP server
4. Click **Apply**

11.2.3 DST Synchronization

DST (daylight saving time) refers to the period of the year when clocks are moved one period ahead. In some areas worldwide, this has the effect of creating more sunlit hours in the evening during months when the weather is the warmest.

We advance our clocks ahead a certain period (depends on the DST bias you set) at the beginning of DST, and move them back the same period when we return to standard time (ST).

Steps

1. Go to **System → General** .
2. Check **Enable DST**.
3. Set **DST mode** as **Auto** or **Manual**.

   Auto

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

   Manual

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

4. Set the DST Bias. Set the time (30/60/90/120 minutes) offset from the standard time.
5. Click **Apply** to save the settings.

11.3 Network Detection

11.3.1 Network Traffic Monitoring

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

Steps

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

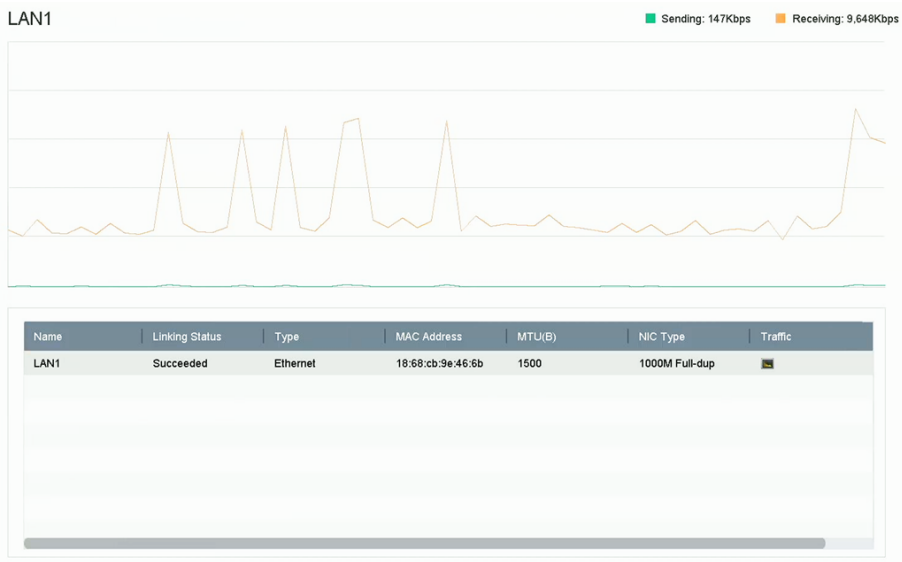

Figure 11-1 Network Traffic

11.3.2 Test Network Delay and Packet Loss

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

Steps

1. Go to **Maintenance → Network → Detection** .
2. Select a network card in **Select NIC**.

3. Enter the destination IP address in **Destination Address**.
4. Click **Test**.

Figure 11-2 Test Network Delay and Packet Loss

11.3.3 Export Network Packet

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

Before You Start
Prepare a USB flash drive to export network packet.

Steps
1. Insert the USB flash drive.
2. Go to **Maintenance → Network → Detection** .
3. Select network card in **Select NIC**.
4. Select the USB flash drive in **Device Name**. You can click **Refresh** if the connected local backup device cannot be displayed.

Figure 11-3 Export Network Packet

5. **Optional:** Click **Status** to view the network status.
6. Click **Export**.

Note
It will export 1 MB data each time as default.

11.3.4 Network Resource Statistics

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

Steps
1. Go to **Maintenance → Network → Stat** .

Figure 11-4 Network Resource Statistics

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

11.4 Storage Device Maintenance

Enter a short description of your concept here (optional).

This is the start of your concept.

11.4.1 Bad Sector Detection

Steps

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

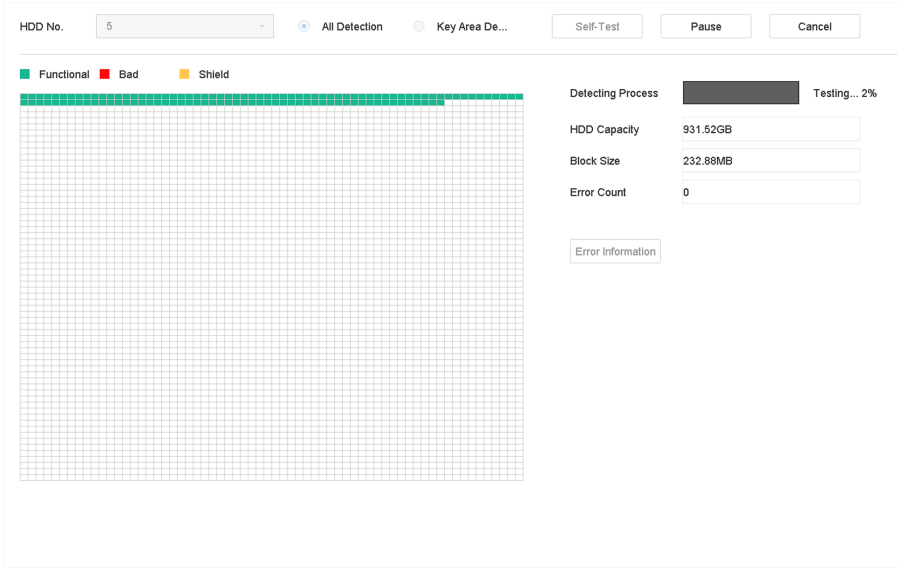

Figure 11-5 Bad Sector Detection

Note

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

11.4.2 Repair Database

Repairing database will rebuild all databases. It might help to improve your system speed after upgrade.

Steps

1. Go to **Storage → Storage Device** .
2. Select the drive.
3. Click **Repair Database**.
4. Click **Yes**.

Note

- Repairing database will rebuild all databases. Existing data will not be affected, but local search and playback functions will not be available during the process, you can still achieve search and playback functions remotely via web browser, client software, etc.
- Do not pull out the drive, or shut down the device during the process.
- You can see the repairing progress at **Status**.

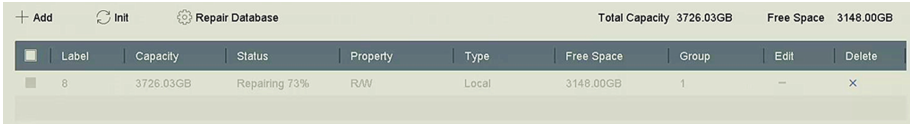

Figure 11-6 Repair Database

11.5 Upgrade System

11.5.1 Upgrade Device

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

Upgrade by Local Backup Device

Before You Start

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

Steps

1. Go to **Maintenance → Upgrade** .
2. Click **Local Upgrade** to enter the local upgrade interface.

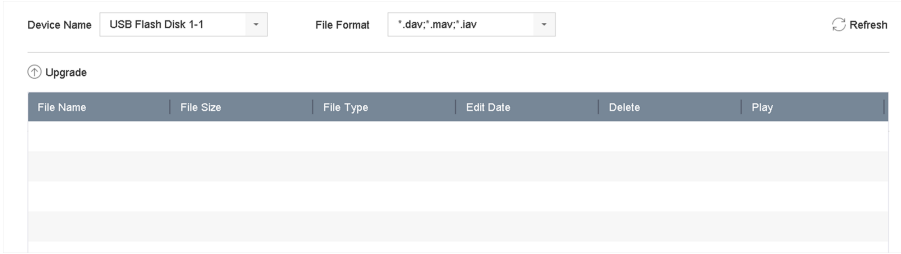

Figure 11-7 Local Upgrade Interface

3. Select the firmware update file from the storage device.
4. Click **Upgrade** to start upgrading.

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

Upgrade by FTP

Before You Start

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

Steps

1. Go to **Maintenance → Upgrade** .
2. Click **FTP** to enter the local upgrade interface.

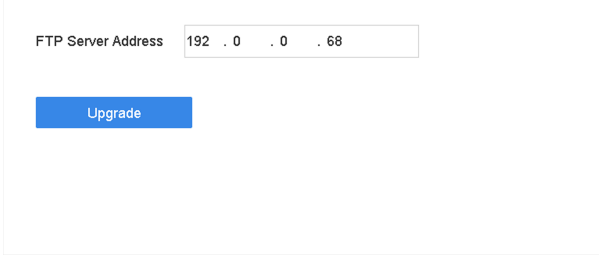

Figure 11-8 FTP Upgrade Interface

3. Enter **FTP Server Address**.
4. Click **Upgrade** to start upgrading.
5. After the upgrading is complete, reboot the device to activate the new firmware.

Upgrade by Hik-Connect

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

Before You Start
Ensure the device has successfully connected to Hik-Connect, and it requires to install at least one read-write HDD for firmware downloading.

Steps
1. Go to **Maintenance → Upgrade → Online Upgrade** .
2. Click **Check Upgrade** to manually check and download the latest firmware from Hik-Connect.

   Note

   The device will automatically check for the latest firmware every 24 hours. If it detects available upgrade firmware, the device will notify you when you log in.
3. **Optional:** You can switch on **Download Latest Package Automatically** to automatically download the latest firmware package.
4. Click **Upgrade Now**.

11.5.2 Upgrade Analog Cameras

You can upgrade connected analog cameras that support Turbo HD or AHD signal.

Steps
1. Go to **Maintenance → Upgrade → Camera Upgrade** .
2. Select camera(s) as your desire.
3. Select the external storage device.
4. Select the upgrade file.
5. Click **Upgrade**.

11.5.3 Upgrade IP Cameras

The IP camera can be remotely upgraded through the device.

Before You Start
Ensure you have inserted the USB flash drive to the device, and it contains the IP camera upgrade firmware.

Steps
1. On the camera management interface, select a camera.
2. Go to **More Settings → Upgrade** .
3. Select the firmware upgrade file from the USB flash drive.

4. Click **Upgrade**.

   The IP camera will reboot automatically after the upgrading completes.

11.6 Import/Export Device Configuration Files

The device configuration files can be exported to a local device for backup; and the configuration files of one device can be imported to multiple devices if they are to be configured with the same parameters.

Before You Start

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

Steps

1. Go to **Maintenance → Import/Export** .

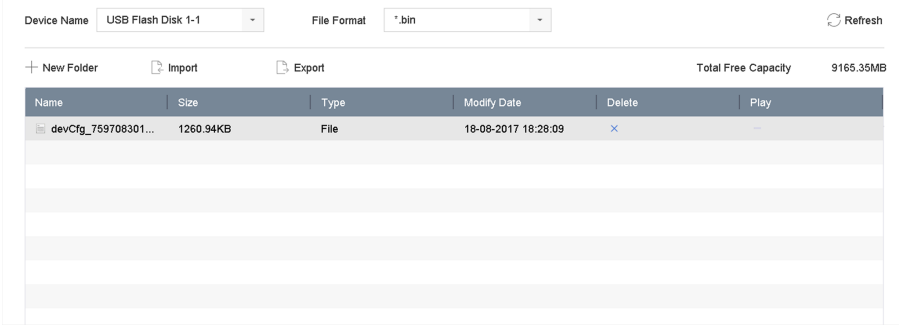

Figure 11-9 Import/Export Config File

2. Export or import the device configuration files.
   - Click **Export** to export configuration files to the selected local backup device.
   - To import a configuration file, select the file from the selected backup device and click **Import**.

Note

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

11.7 Search & Export Log Files

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

Steps

1. Go to **Maintenance → Log Information** .

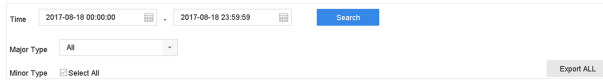

Figure 11-10 Log Search Interface

2. Set the log search conditions, including the time, major type and minor type.
3. Click **Search** to start searching the log files.
4. The matched log files will be displayed on the list, as shown below.

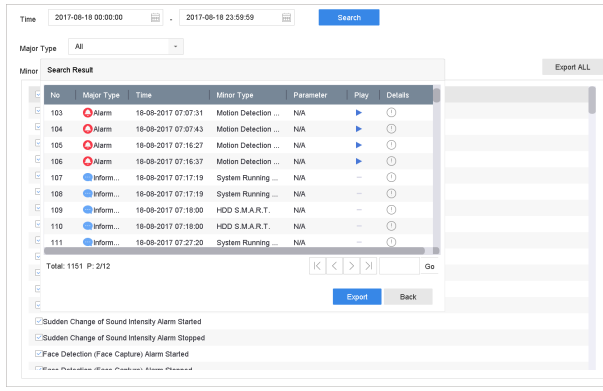

Figure 11-11 Log Search Results

Note

Up to 2,000 log files can be displayed each time.

5. Related Operation:

	Click or double-click it to view detailed information.
	Click it to view the related video file.
Export/Export ALL	Click it to export all the system logs to the storage device.

11.8 Restore Default Settings

Steps

1. Go to **Maintenance → Default** .

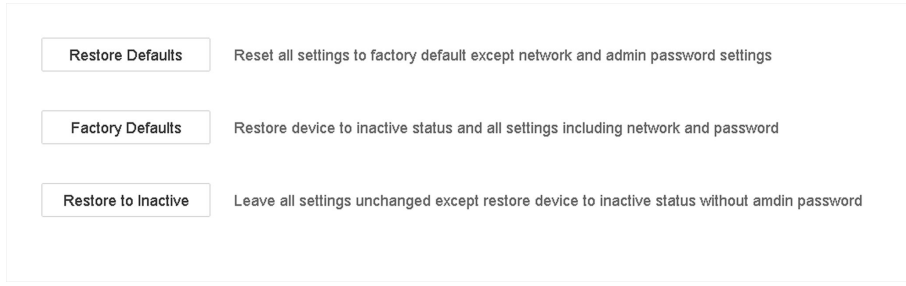

Figure 11-12 Restore Default Settings

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

Restore Defaults

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

Factory Defaults

Restore all parameters to the factory default settings.

Restore to Inactive

Restore the recorder to inactive status.

Note

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

11.9 Security Management

Enter a short description of your concept here (optional).

This is the start of your concept.

11.9.1 HTTP Authentication

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

Steps

1. Go to **System → System Service → System Service** .

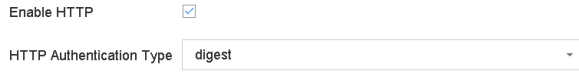

Figure 11-13 HTTP Authentication

2. Check **Enable HTTP**.
3. Select **HTTP Authentication Type**.

Note

Two authentication types are selectable, for security reasons, it is recommended to select **digest** as the authentication type.

4. Click **Apply** to save the settings.
5. Restart the device to take effect the settings.

11.9.2 ISAPI Service

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

Steps

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

11.9.3 RTSP Authentication

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

Steps

1. Go to **System → System Service → System Service** .

Figure 11-14 RTSP Authentication

2. Select **RTSP Authentication Type**.

Note

Two authentication types are selectable, if you select **digest**, only the request with digest authentication can access the video stream by the RTSP protocol via the IP address. For security reasons, it is recommended to select **digest** as the authentication type.

3. Click **Apply**.
4. Restart the device to take effect the settings.


See Far, Go Further