Safety Instruction

- Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.
- In the use of the product, you must be in strict compliance with the electrical safety regulations of the nation and region.
- Firmly connect the plug to the power socket. Do not connect several devices to one power adapter. Power off the device before connecting and disconnecting accessories and peripherals.
- Shock hazard! Disconnect all power sources before maintenance.
- The equipment must be connected to an earthed mains socket-outlet.
- The socket-outlet shall be installed near the equipment and shall be easily accessible.
- ϟ indicates hazardous live and the external wiring connected to the terminals requires installation by an instructed person.
- Never place the equipment in an unstable location. The equipment may fall, causing serious personal injury or death.
- Input voltage should meet the SELV (Safety Extra Low Voltage) and the LPS (Limited Power Source) according to the IEC62368.
- High touch current! Connect to earth before connecting to the power supply.
- If smoke, odor or noise rise from the device, turn off the power at once and unplug the power cable, and then please contact the service center.
- Use the device in conjunction with an UPS, and use factory recommended HDD if possible.
- This product contains a coin/button cell battery. If the battery is swallowed, it can cause severe internal burns in just 2 hours and can lead to death.
- This equipment is not suitable for use in locations where children are likely to be present.
- CAUTION: Risk of explosion if the battery is replaced by an incorrect type.
- Improper replacement of the battery with an incorrect type may defeat a safeguard (for example, in the case of some lithium battery types).
- Do not dispose of the battery into fire or a hot oven, or mechanically crush or cut the battery, which may result in an explosion.
- Do not leave the battery in an extremely high temperature surrounding environment, which may result in an explosion or the leakage of flammable liquid or gas.
- Do not subject the battery to extremely low air pressure, which may result in an explosion or the leakage of flammable liquid or gas.
- Dispose of used batteries according to the instructions.
- Keep body parts away from fan blades and motors. Disconnect the power source during servicing.
- Keep body parts away from motors. Disconnect the power source during servicing.

Preventive and Cautionary Tips

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

- The device is designed for indoor use only. Install it in a well-ventilated, dust-free environment without liquids.
- 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.
- The equipment shall not be exposed to dripping or splashing and that no objects filled with liquids shall be placed on the equipment, such as vases.
- No naked flame sources, such as lighted candles, should be placed on the equipment.
- The ventilation should not be impeded by covering the ventilation openings with items, such as newspapers, table-cloths, curtains, etc. The openings shall never be blocked by placing the equipment on a bed, sofa, rug or other similar surface.
- For certain models, ensure correct wiring of the terminals for connection to an AC mains supply.
- For certain models, the equipment has been designed, when required, modified for connection to an IT power distribution system.
- 🔋 identifies the battery holder itself and identifies the positioning of the cell(s) inside the battery holder.
- + identifies the positive terminal(s) of equipment which is used with, or generates direct current. + identifies the negative terminal(s) of equipment which is used with, or generates direct current.
- Keep a minimum 200 mm (7.87 inch) distance around the equipment for sufficient ventilation.
- For certain models, ensure correct wiring of the terminals for connection to an AC mains supply.
- Use only power supplies listed in the user manual or user instruction.
- The USB port of the equipment is used for connecting to a mouse, keyboard, USB flash drive, or Wi-Fi dongle only.
- Use only power supplies listed in the user manual or user instruction.
- Do not touch the sharp edges or corners.
- When the device is running above 45 °C (113 °F), or its HDD temperature in S.M.A.R.T. exceeds the stated value, please ensure the device is running in a cool environment, or replace HDD(s) to make the HDD temperature in S.M.A.R.T. below the stated value.

Contents

Chapter 1 Basic Operation

1.1 Activate Your Device

1.1.1 Default User and IP Address

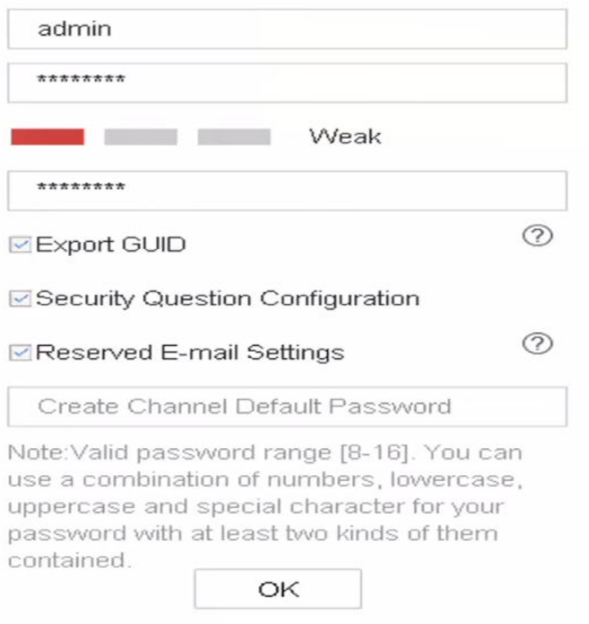
- Default administrator account: admin.
- Default IPv4 address: 192.168.1.64.

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.



admin

****

Weak

****

☑ Export GUID

☑ Security Question Configuration

☑ Reserved E-mail Settings

Create Channel Default Password

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

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 change your password regularly, especially in the high security system, changing 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

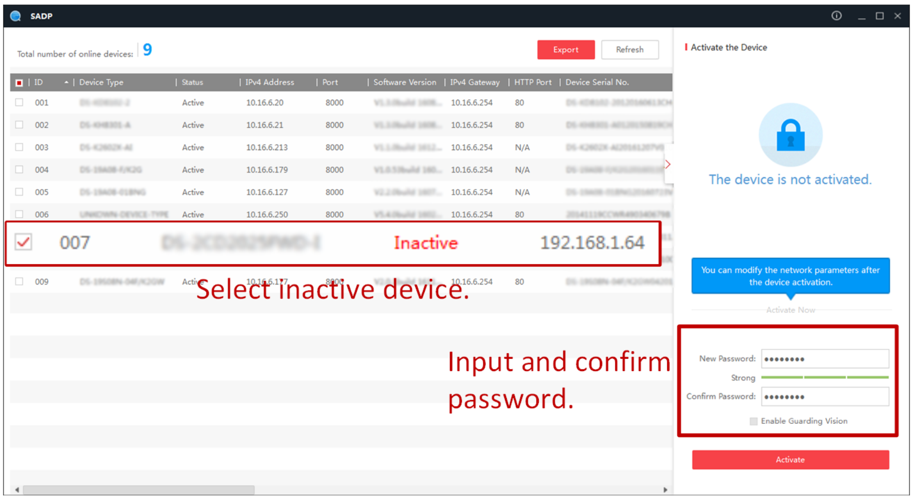
SADP software is used for detecting the online device, activating the device, and resetting its password.

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.



SADP

Total number of online devices: 9

ID	Device Type	Status	IPv4 Address	Port	Software Version	IPv4 Gateway	HTTP Port	Device Serial No.
□ 001	[illegible]	Active	10.16.6.20	8000	[illegible]	10.16.6.254	80	[illegible]
□ 002	[illegible]	Active	10.16.6.21	8000	[illegible]	10.16.6.254	80	[illegible]
□ 003	[illegible]	Active	10.16.6.213	8000	[illegible]	10.16.6.254	N/A	[illegible]
□ 004	[illegible]	Active	10.16.6.179	8000	[illegible]	10.16.6.254	N/A	[illegible]
□ 005	[illegible]	Active	10.16.6.127	8000	[illegible]	10.16.6.254	N/A	[illegible]
□ 006	[illegible]	Active	10.16.6.250	8000	[illegible]	10.16.6.254	80	[illegible]
☑ 007	[illegible]	Inactive	192.168.1.64					
□ 009	[illegible]	Active	10.16.6.177	8000	[illegible]	10.16.6.254	80	[illegible]

Select inactive device.

Input and confirm password.

Activate the Device

The device is not activated.

You can modify the network parameters after the device activation.

Activate Now

New Password: ••••••••

Strong

Confirm Password: ••••••••

□ Enable Guarding Vision

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 change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.

5. Click **Activate**.

1.1.4 Activate via Client Software

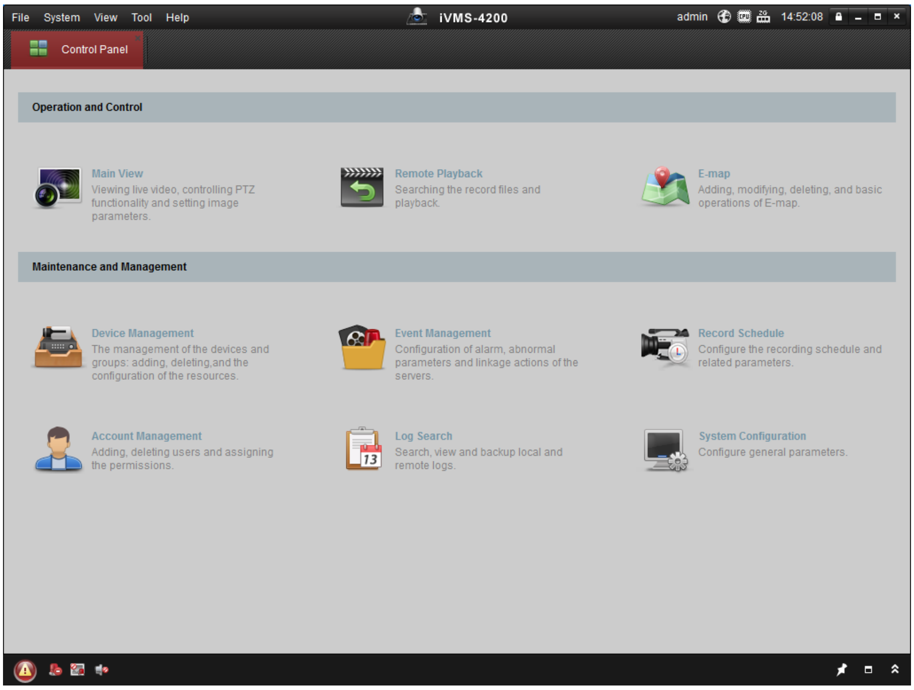
The client software is versatile video management software for multiple kinds of devices.

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.



Operation and Control

Main View
Viewing live video, controlling PTZ functionality and setting image parameters.

Remote Playback
Searching the record files and playback.

E-map
Adding, modifying, deleting, and basic operations of E-map.

Maintenance and Management

Device Management
The management of the devices and groups: adding, deleting,and the configuration of the resources.

Event Management
Configuration of alarm, abnormal parameters and linkage actions of the servers.

Record Schedule
Configure the recording schedule and related parameters.

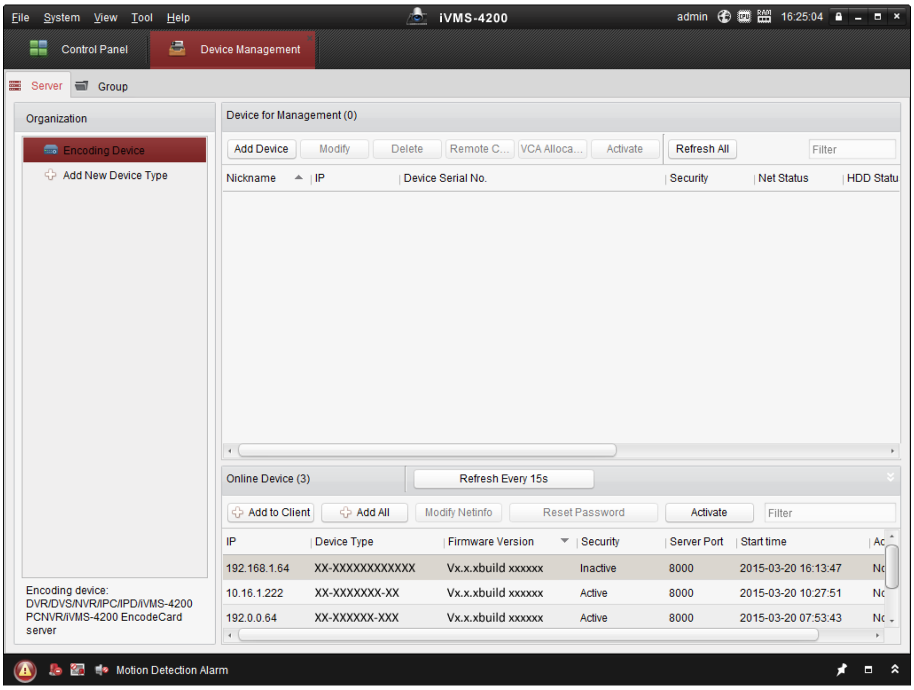
Account Management
Adding, deleting users and assigning the permissions.

Log Search
Search, view and backup local and remote logs.

System Configuration
Configure general parameters.

Figure 1-3 Control Panel

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



Encoding device:
DVR/DVS/NVR/IPC/IPD/iVMS-4200 PCNVR/iVMS-4200 EncodeCard server

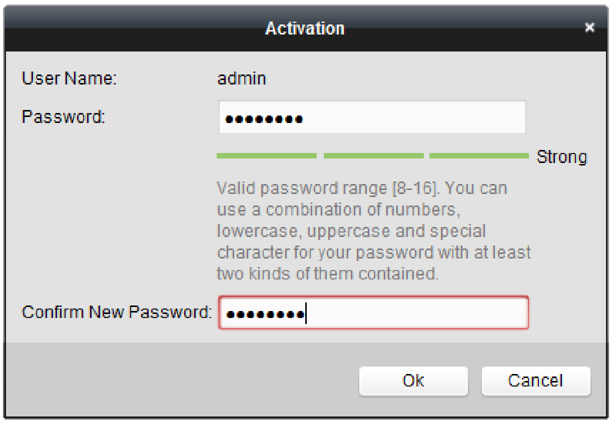
IP	Device Type	Firmware Version	Security	Server Port	Start time	Ac
192.168.1.64	XX-XXXXXXXXXXXX	Vx.x.xbuild xxxxxx	Inactive	8000	2015-03-20 16:13:47	Nc
10.16.1.222	XX-XXXXXXX-XX	Vx.x.xbuild xxxxxx	Active	8000	2015-03-20 10:27:51	Nc
192.0.0.64	XX-XXXXXX-XXX	Vx.x.xbuild xxxxxx	Active	8000	2015-03-20 07:53:43	Nc

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 change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.



User Name: admin

Password: ••••••••

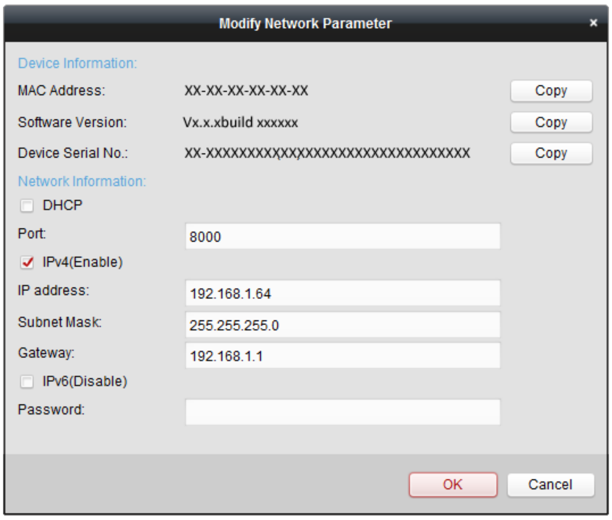
Strong

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

Confirm New Password: ••••••••

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.



Device Information:

MAC Address: XX-XX-XX-XX-XX-XX

Software Version: Vx.x.xbuild xxxxxx

Device Serial No.: XX-XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Network Information:

☐ DHCP

Port: 8000

☑ IPv4(Enable)

IP address: 192.168.1.64

Subnet Mask: 255.255.255.0

Gateway: 192.168.1.1

☐ IPv6(Disable)

Password:

Figure 1-6 Modify Network Parameters

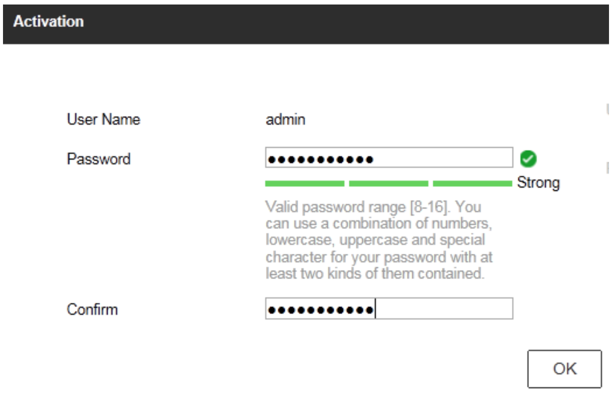
8. Change the recorder IP address to the same subnet with your computer.
   - Modify the IP address manually.
   - Check **Enable DHCP**.
9. Input the password to activate your IP address modification.

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**.



Activation

User Name admin

Password ●●●●●●●●●●● Strong

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

Confirm ●●●●●●●●●●●

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 change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.

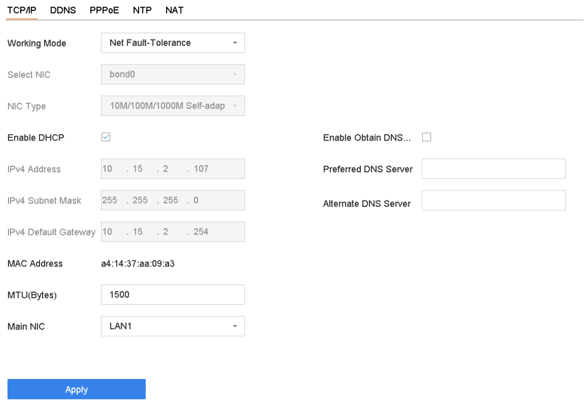
3. Click **OK**.

1.2 Configure TCP/IP Settings

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

Steps

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



Working Mode: Net Fault-Tolerance

Select NIC: bond0

NIC Type: 10M/100M/1000M Self-adap

Enable DHCP ☑

Enable Obtain DNS... □

IPv4 Address: 10 . 15 . 2 . 107

Preferred DNS Server:

IPv4 Subnet Mask: 255 . 255 . 255 . 0

Alternate DNS Server:

IPv4 Default Gateway: 10 . 15 . 2 . 254

MAC Address: a4:14:37:aa:09:a3

MTU(Bytes): 1500

Main NIC: LAN1

Figure 1-8 TCP/IP Settings

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

   Net-Fault Tolerance

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

   Multi-Address Mode

   The parameters of the two NIC cards can be configured independently. You can select LAN1 or LAN2 under Select NIC for parameter settings. Select one NIC card as the default route. When the system connects with the extranet, the data will be forwarded through the default route.

3. Configure other IP settings as needed.
4. Click **Apply**.

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.

1.3 Configure HDD

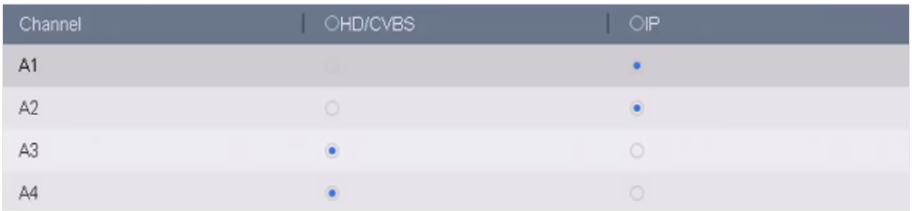
Ensure the video recorder storage media is well. You can install at least one HDD and initialize it, or create a RAID and initialize it.

1.4 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** .



Channel	○HD/CVBS	○IP
A1	○	●
A2	○	●
A3	●	○
A4	●	○

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**.

1.5 Configure Enhanced IP Mode

Enabling enhanced IP mode will allow you to connect to the maximum number of cameras, but disable 2K/4K output resolution, and make perimeter protection, human or vehicle detection of motion detection, facial detection and face picture comparison functions unavailable in analog channel.

Go to **System → General** , and check **Enhanced IP Mode**.

1.6 Connect PoC Camera

The devices of /P series can detect the connected PoC cameras automatically, manage the power consumption via the coaxial communication, and provide power to the cameras via coaxitron.

Before You Start

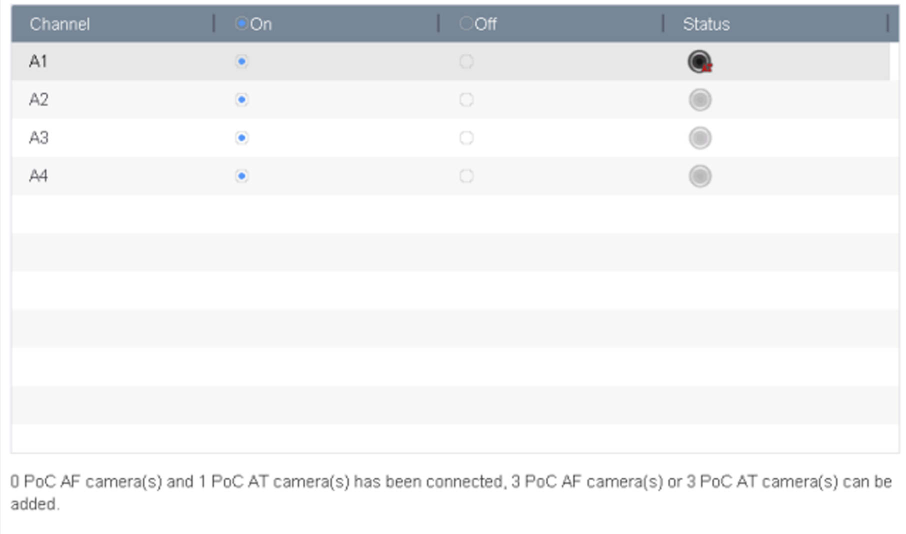
- Ensure your device supports PoC (Power over Coaxitron) cameras connection.
- Connect the PoC camera to the DVR.

Steps

1. Go to **Menu → Camera → PoC Status** .
2. Turn on the PoC for the channel(s) as your desire.
3. Check the status of connected PoC camera.

- If the power consumption of the DVR is lower than that of AF camera, when AF or AT camera is connected, there is no video and “Insufficient Power for PoC” is overlaid on the live view image.
- If the power consumption of the DVR is higher than that of the AF camera and lower than that of the AT camera, when AF camera is connected, it is powered on normally; when AT camera is connected, it is powered on and then powered off, and there is no video and “Insufficient Power for PoC” is overlaid on the live view image.
- If the power consumption of the DVR is higher than that of the AT camera, when AF or AT camera is connected, it is powered on normally.

4. Check the connected AF or AT camera number and the connectable camera number.



Channel	○On	○Off	Status
A1	◉	○	●
A2	◉	○	◉
A3	◉	○	◉
A4	◉	○	◉

0 PoC AF camera(s) and 1 PoC AT camera(s) has been connected, 3 PoC AF camera(s) or 3 PoC AT camera(s) can be added.

Figure 1-10 PoC Status

Note

- Only Hikvision PoC camera is supported.
- The maximum connectable AT/AF camera number varies with different models.

Warning

Please turn off the PoC function if the camera does not support PoC, or the camera is not produced by Hikvision. Otherwise, it may result in permanent damage to the camera or DVR.

1.7 Add Network Camera

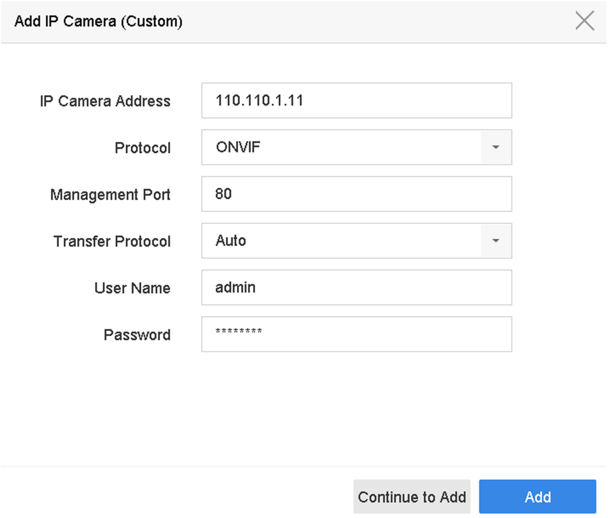
Before you can get live video or record the video files, you must add the network cameras to the connection list of the device.

Before You Start

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

Steps

1. Click ▭ on the main menu bar.
2. Click **Custom Add** tab on the title bar.



Add IP Camera (Custom)

IP Camera Address	110.110.1.11
Protocol	ONVIF
Management Port	80
Transfer Protocol	Auto
User Name	admin
Password	********

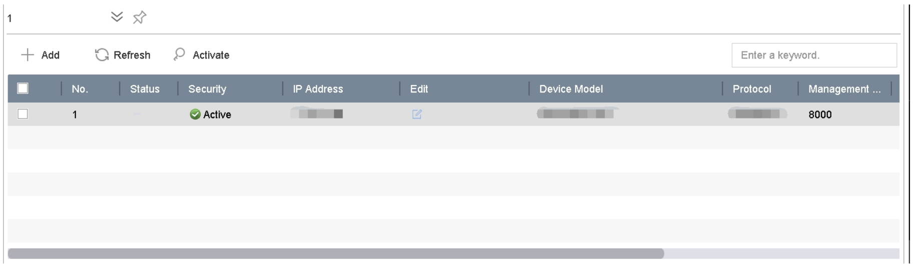
Figure 1-11 Add IP Camera

3. Enter IP address, protocol, management port, and other IP camera information to add.
4. Enter the login user name and password of the IP camera.
5. Click **Add** to finish the adding of the IP camera.
6. **Optional:** Click **Continue to Add** to continue to add additional IP cameras.

1.7.1 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.



□	No.	Status	Security	IP Address	Edit	Device Model	Protocol	Management ...
□	1		✓ Active	[redacted]		[redacted]	[redacted]	8000

Figure 1-12 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.

1.7.2 Add Network Camera Manually

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

Before You Start

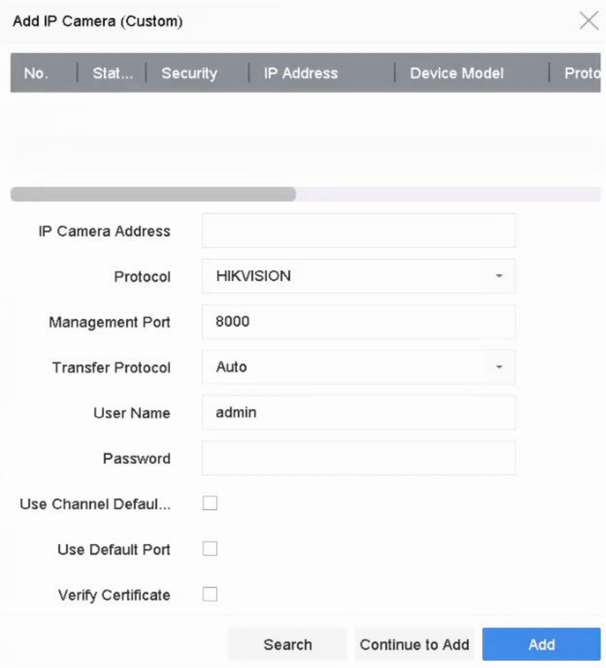
Ensure the network connection is valid and correct, and the network camera is activated.

Steps

1. Click on the main menu.
2. Click **Custom Add**.
3. Set the parameters. For example, **IP Camera Address**, **Protocol**, etc.

Note

Management port ranges from 1 to 65535.



Add IP Camera (Custom)

No.	Stat...	Security	IP Address	Device Model	Proto

IP Camera Address	
Protocol	HIKVISION
Management Port	8000
Transfer Protocol	Auto
User Name	admin
Password	
Use Channel Defaul...	□
Use Default Port	□
Verify Certificate	□

Figure 1-13 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 device first when you use this function. For details, refer to .

Note

The enhanced SDK service is only available when you use HIKVISION protocol.

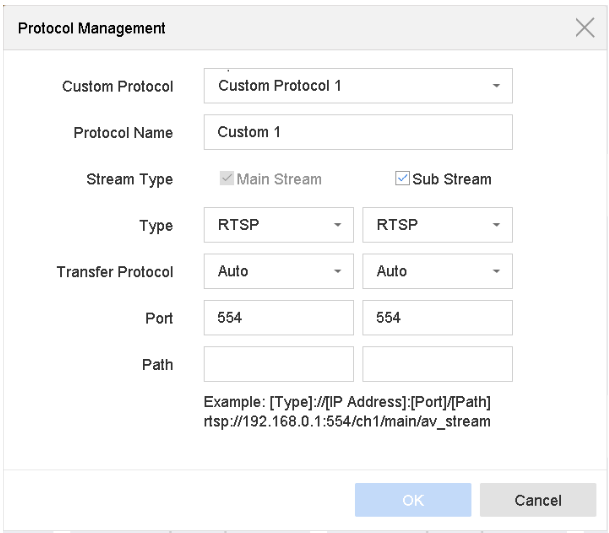
7. Click **Add**.
8. **Optional:** Check **Continue to Add** to add other network cameras.

1.7.3 Add Network Camera via Customized Protocol

For network cameras that are not using standard protocols, you can configure customized protocols to add them. The system provides 16 customized protocols.

Steps

1. Go to **More Settings → Protocol** .



Protocol Management

Custom Protocol: Custom Protocol 1

Protocol Name: Custom 1

Stream Type: ☑ Main Stream ☑ Sub Stream

Type: RTSP | RTSP

Transfer Protocol: Auto | Auto

Port: 554 | 554

Path:

Example: [Type]://[IP Address]:[Port]/[Path]
rtsp://192.168.0.1:554/ch1/main/av_stream

Figure 1-14 Protocol Management

2. Set protocol parameters.

Type

The network camera adopting custom protocol must support getting stream through standard RTSP.

Path

Contact the manufacturer of network camera for the URL (Uniform Resource Locator) of getting main stream and sub-stream.

Note

The protocol type and the transfer protocol must be supported by the network camera to add.

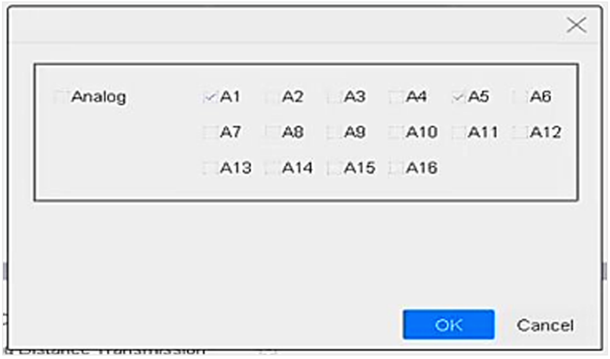
3. Click **OK**.
4. Click **Custom Add** to add cameras.
5. Set the parameters.
6. Click **OK**.

1.8 Configure 5 MP Long Distance Transmission

For HUHI and HTHI series DVR, you can configure 5 MP long distance transmission on the Signal Input Status interface.

Steps

1. Go to **Camera → Camera → Analog** .
2. Click ⚙ to enter the 5 MP Long Distance Transmission Settings interface.



□ Analog ☑ A1 □ A2 □ A3 □ A4 ☑ A5 □ A6
□ A7 □ A8 □ A9 □ A10 □ A11 □ A12
□ A13 □ A14 □ A15 □ A16

Figure 1-15 5 MP Long Distance Transmission Settings

3. Select channel(s) to enable 5 MP Long Distance Transmission.
4. Click **OK**.
5. Click **Apply**.

1.9 Connect to Platform

1.9.1 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 with 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:** Check **Custom** and enter **Server Address** as your desire.
4. **Optional:** Check **Enable Stream Encryption**, then verification code is required for remote access and live view.
5. Bind your device with a Hik-Connect account.
   1) Use a smart phone to scan the QR code, and download Hik-Connect app. You can also download it from ***https://appstore.hikvision.com*** , or the QR code below. Refer to *Hik-Connect Mobile Client User Manual* for details.

Figure 1-16 Download Hik-Connect

   2) Use Hik-Connect to scan the device QR, and bind the device.

Note

If the device is already bound with an account, you can click **Unbind** to unbind with the current account.

6. Click **Apply**.

What to do next

You can access your video recorder via Hik-Connect.

Chapter 2 Camera Settings

2.1 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

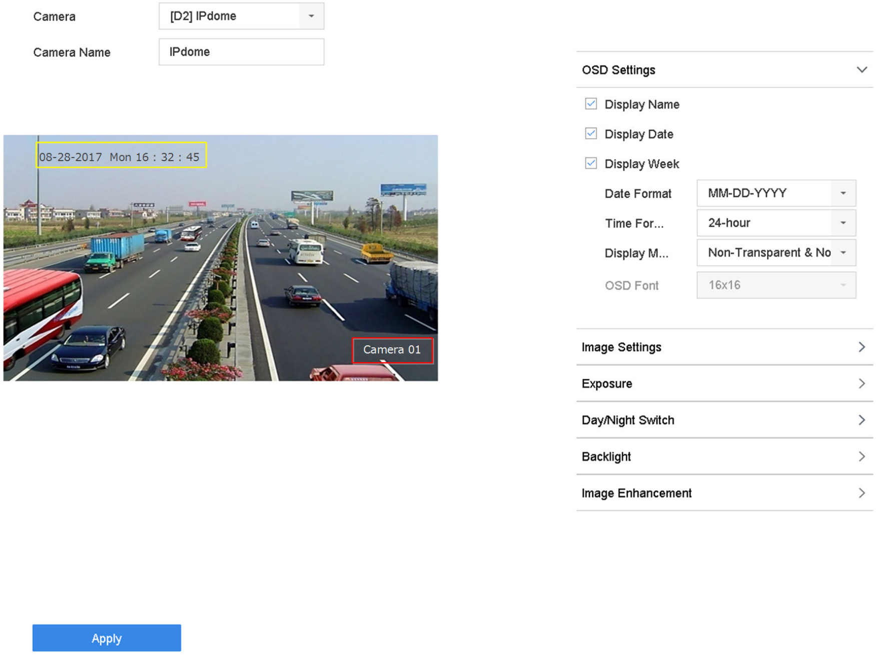
For optimized image contrast enhancement that reduces noise in video stream.

2.2 Configure OSD

You can configure the OSD (On-screen Display) 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.



Camera: [D2] IPdome

Camera Name: IPdome

OSD Settings

☑ Display Name

☑ Display Date

☑ Display Week

Date Format: MM-DD-YYYY

Time For...: 24-hour

Display M...: Non-Transparent & No

OSD Font: 16x16

Figure 2-1 OSD Settings

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

2.3 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.

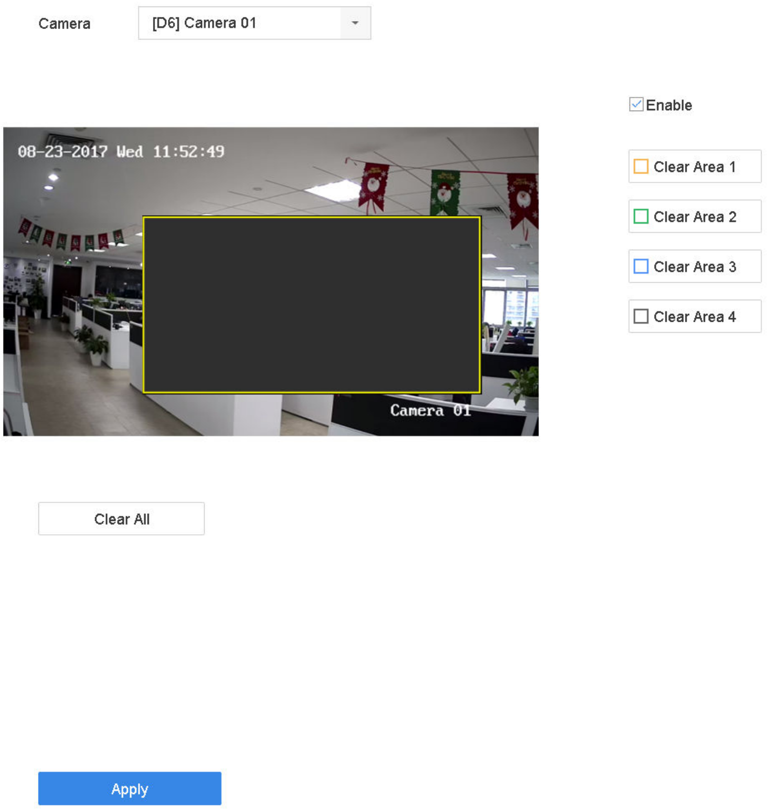


Figure 2-2 Privacy Mask Settings

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**.

2.4 Import/Export IP Camera Configuration Files

The IP camera information, including the IP address, manage port, password of admin, etc., can be saved in Microsoft Excel format and backed up to the local device. The exported file can be edited on a PC, including adding or deleting the content, and copying the setting to other devices by importing the Excel file to it.

Before You Start

When importing the configuration file, connect the storage device that contains the configuration file to the device.

Steps

1. Go to **Camera → IP Camera Import/Export** .

2. Click **IP Camera Import/Export**, and the detected external device contents appear.
3. Export or import the IP camera configuration files.
   - Click **Export** to export the 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 the importing process is completed, you must reboot the device to activate the settings.

2.5 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.

Chapter 3 Live View

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

3.1 Start Live View

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

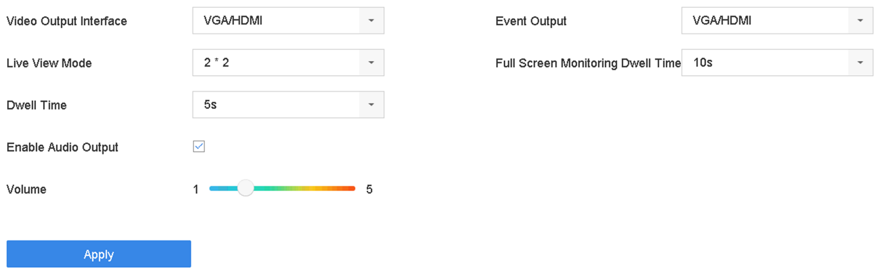
- Select a window and double click a camera from the list to play the video from the camera in the selected window.
- Use the toolbar at the playing window bottom to realize the capture, instant playback, audio on/off, digital zoom, live view strategy, show information and start/stop recording, etc.

3.1.1 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** .



Video Output Interface: VGA/HDMI

Event Output: VGA/HDMI

Live View Mode: 2 * 2

Full Screen Monitoring Dwell Time: 10s

Dwell Time: 5s

Enable Audio Output: ☑

Volume: 1 — 5

Figure 3-1 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**.

3.1.2 Configure Auto-Switch of Cameras

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

Steps

1. Go to **System → Live View → General** .
2. Set **Video Output Interface**, **Live View Mode**, and **Dwell Time**.

Video Output Interface

Select the video output interface.

Live View Mode

Select the display mode for live view, e.g., 2*2, 1*5, etc.

Dwell Time

The time in seconds to dwell between switching of cameras when enabling auto-switch. The range is from 5s to 300s.

3. Go to **View Settings** to set the view layout.
4. Click **OK** to save the settings.

3.1.3 Configure Live View Layout

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

Configure Custom Live View Layout

Steps

1. Go to **System → Live View → View** .
2. Click **Set Custom Layout**.
3. Click + on the Custom Layout Configuration interface.
4. Edit the layout name.
5. Select a window division mode from the toolbar.

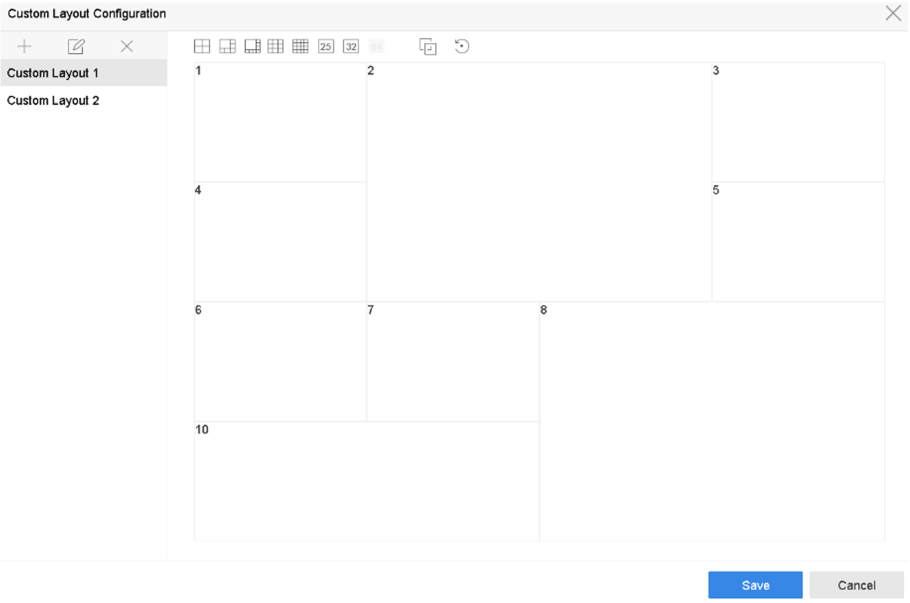


Figure 3-2 Configure Live View Layout

6. Select multiple windows and click to joint the windows. The selected windows must be in rectangle area.
7. Click **Save**.

   The successfully configured layout is displayed in the list.
8. **Optional:** Select a live view layout from the list and click to edit the name, or click to delete the name.

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

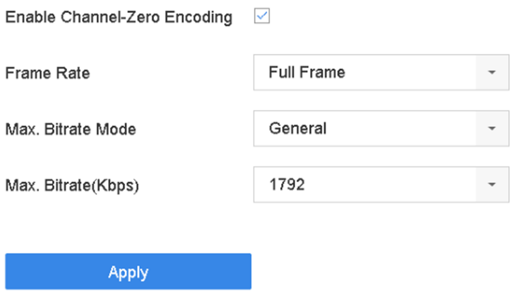
   - You can also click-and-drag the camera to the desired window on the Live View interface to set the camera order.
   - You can enter the number in the text field to quickly search the camera from the list.
5. Click **Apply**.
6. **Optional:** Click to start live view for all channels, or click to stop all live view channels.

3.1.4 Configure Channel-Zero Encoding

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

Steps

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



Enable Channel-Zero Encoding ☑

Frame Rate: Full Frame

Max. Bitrate Mode: General

Max. Bitrate(Kbps): 1792

Figure 3-3 Channel-Zero Encoding

3. Configure **Frame Rate**, **Max. Bitrate Mode**, and **Max. Bitrate**.

Note

The higher frame rate and bitrate require the higher bandwidth.

4. Click **Apply**.

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

3.1.5 Use an Auxiliary Monitor

Certain features of the Live View are also available while in an Aux monitor. Features include:

Single Screen

Switch to a full screen display of the selected camera. Camera can be selected from a dropdown list.

Multi-screen

Switch between different display layout options. Layout options can be selected from a dropdown list.

Next Screen

When displaying less than the maximum number of cameras in Live View, clicking this feature will switch to the next set of displays.

Playback

Enter into Playback mode.

PTZ Control

Enter PTZ Control mode.

Main Monitor

Enter Main operation mode.

Note

In the live view mode of the main output monitor, the menu operation is not available while Aux output mode is enabled.

3.2 Digital Zoom

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

Steps

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

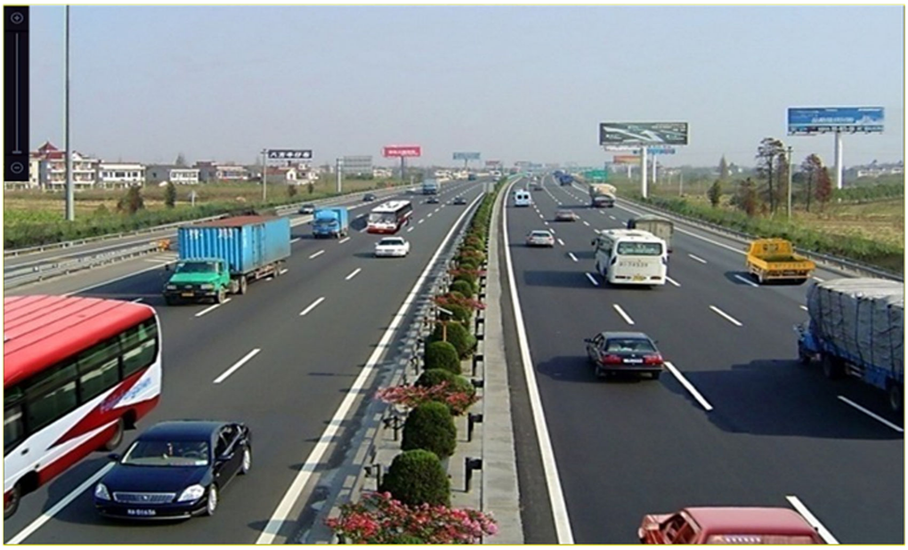


Figure 3-4 Digital Zoom

3.3 Live View Strategy

Steps

1. In the live view mode, click ⇄ to enter the digital zoom operation interface in full screen mode.
2. Select the live view strategy to **Real-time**, **Balanced** or **Fluency**.

3.4 Facial Recognition

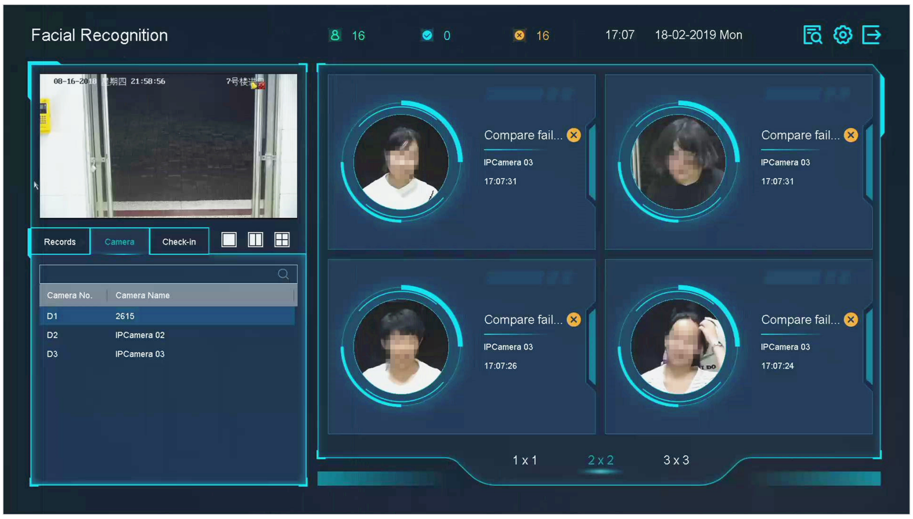
You can enter facial recognition interface to view real-time facial recognition and stranger recognition results.

Before You Start

Ensure you have configured facial detection and face picture comparison function, refer to for details.

Steps

1. Go to live view interface, and click ☺ in toolbar.
2. Click □, ◫, or ⊞ to set window division.
3. Select a window as you desired.
4. Double click a camera from the camera list on the left bottom.



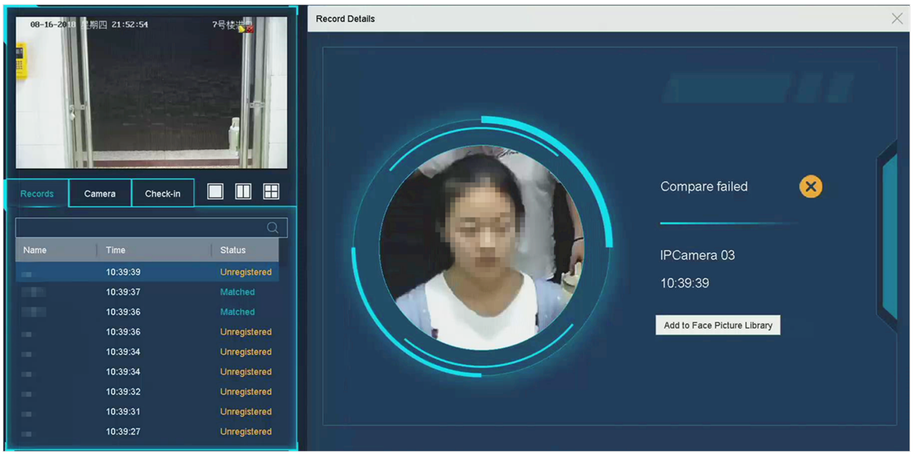
Camera No.	Camera Name
D1	2615
D2	IPCamera 02
D3	IPCamera 03

Figure 3-5 Facial Recognition

5. Click **Records** to view the real-time facial recognition records of selected camera. The records will also be shown in the window on the right. You can view the facial detection number at the top, including the total number, succeeded number and failed number.
6. **Optional:** For the unregistered face picture, you can double click it in records list, and add it to face picture library.

Note

For guest and operator user, it requires Local Parameters Settings permission to add unregistered face picture to face picture library.



Name	Time	Status
[redacted]	10:39:39	Unregistered
[redacted]	10:39:37	Matched
[redacted]	10:39:36	Matched
[redacted]	10:39:36	Unregistered
[redacted]	10:39:34	Unregistered
[redacted]	10:39:34	Unregistered
[redacted]	10:39:32	Unregistered
[redacted]	10:39:31	Unregistered
[redacted]	10:39:27	Unregistered

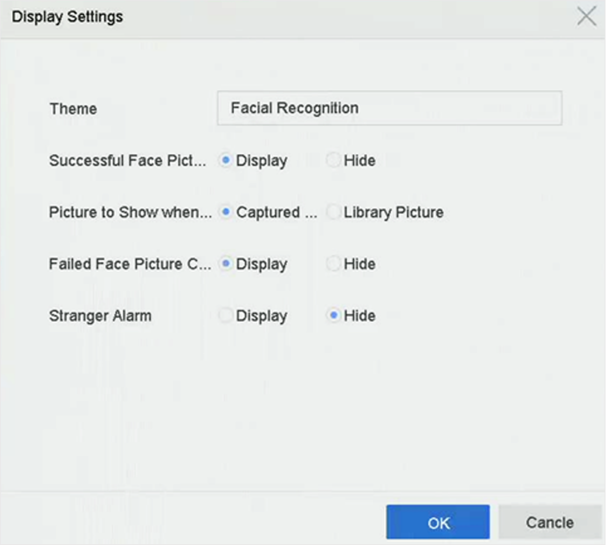
Compare failed

IPCamera 03

10:39:39

Figure 3-6 Add Unregistered Face Picture

7. **Optional:** Click **Check-in** to view face picture library check-in record, including **Total No.**, **Checked In** and **Unchecked In**.
8. **Optional:** Click ⚙ on the upper right corner to configure the display settings as you desired.



Theme: Facial Recognition

Successful Face Pict... ● Display ○ Hide

Picture to Show when... ● Captured ... ○ Library Picture

Failed Face Picture C... ● Display ○ Hide

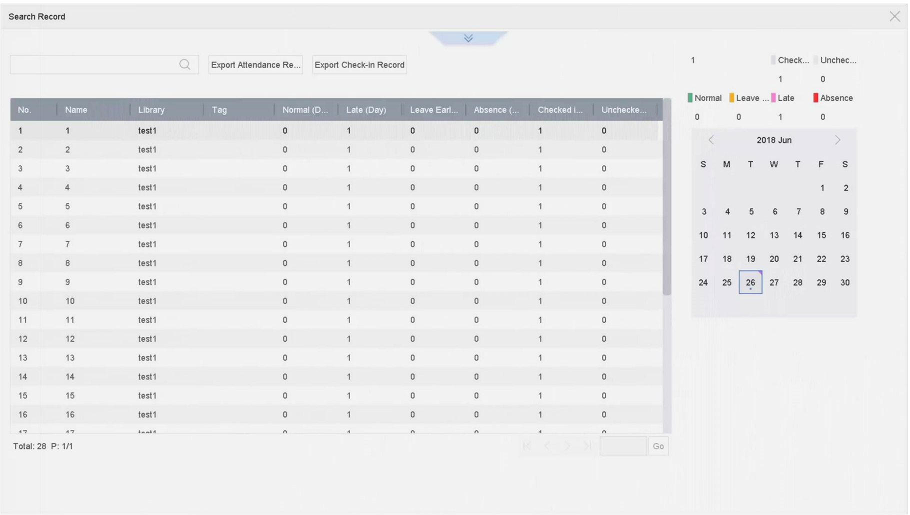
Stranger Alarm ○ Display ● Hide

Figure 3-7 Facial Recognition Display Settings

9. **Optional:** Click 🔍 on the upper right corner to search and export record.
   1) Set the search parameters as you desired.
   2) Click **Search**.
   3) Click **Export Attendance Record** or **Export Check-in Record**.

Note

- Ensure you have inserted USB flash drive before export.
- You can click a record to review the attendance information of this individual in calendar.
- For guest and operator user, it requires "Local Video Export permission" (in "Camera Permission") to search and export record.



Search Record

No.	Name	Library	Tag	Normal (D...	Late (Day)	Leave Earl...	Absence (...	Checked i...	Unchecke...
1	1	test1		0	1	0	0	1	0
2	2	test1		0	1	0	0	1	0
3	3	test1		0	1	0	0	1	0
4	4	test1		0	1	0	0	1	0
5	5	test1		0	1	0	0	1	0
6	6	test1		0	1	0	0	1	0
7	7	test1		0	1	0	0	1	0
8	8	test1		0	1	0	0	1	0
9	9	test1		0	1	0	0	1	0
10	10	test1		0	1	0	0	1	0
11	11	test1		0	1	0	0	1	0
12	12	test1		0	1	0	0	1	0
13	13	test1		0	1	0	0	1	0
14	14	test1		0	1	0	0	1	0
15	15	test1		0	1	0	0	1	0
16	16	test1		0	1	0	0	1	0
17	17	test1		0	1	0	0	1	0

Total: 28 P: 1/1

1		Check...	Unchec...
		1	0
🟩 Normal	🟧 Leave ...	🟪 Late	🟥 Absence
0	0	1	0

2018 Jun

S	M	T	W	T	F	S
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30

Figure 3-8 Face Recognition Search Record

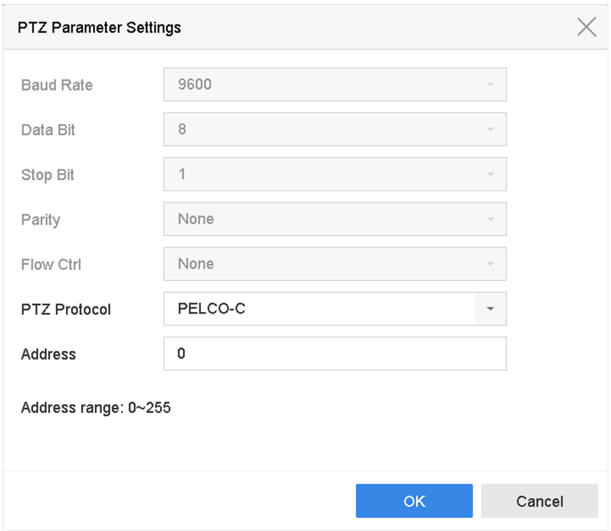
3.5 PTZ Control

3.5.1 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.
2. Click **PTZ Parameters Settings** to set the PTZ parameters.



PTZ Parameter Settings

Baud Rate	9600
Data Bit	8
Stop Bit	1
Parity	None
Flow Ctrl	None
PTZ Protocol	PELCO-C
Address	0

Address range: 0~255

Figure 3-9 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.

3.5.2 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.

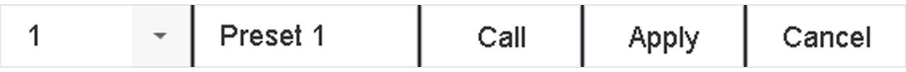


Figure 3-10 Set Preset

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** to cancel the location information of the preset.
9. **Optional:** Click in the lower right corner of Live View to view the configured presets.

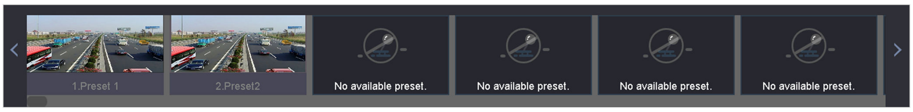


Figure 3-11 View the Configured Presets

3.5.3 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.

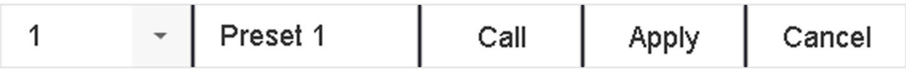


Figure 3-12 Call Preset (1)

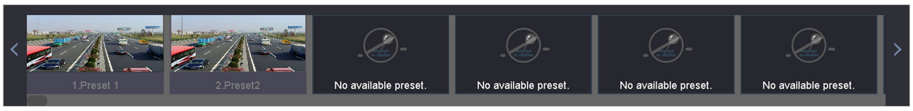


Figure 3-13 Call Preset (2)

3.5.4 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.

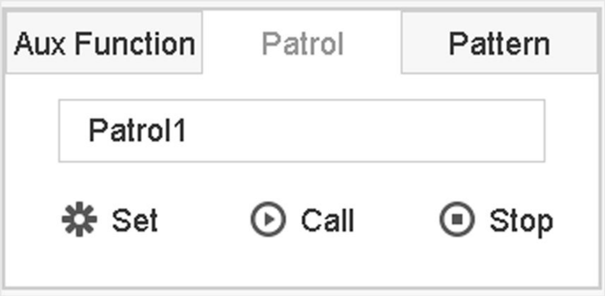
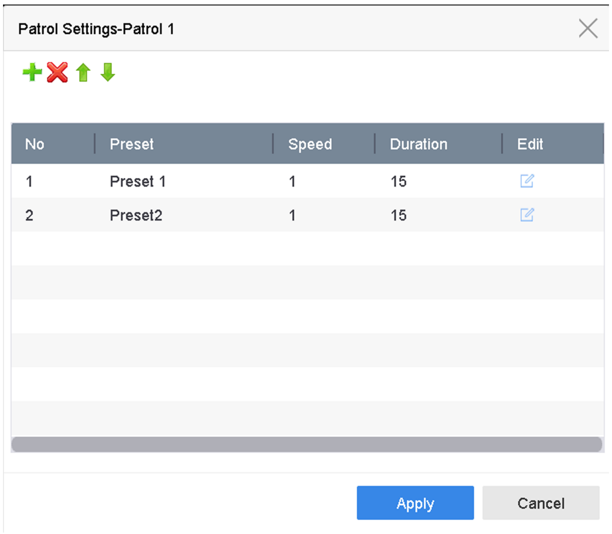


Figure 3-14 Patrol Configuration

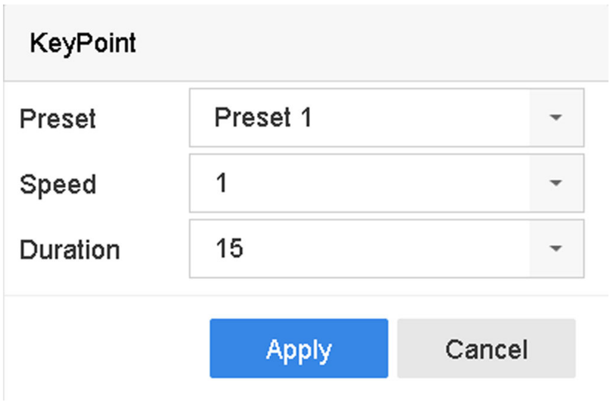
3. Select the patrol No.
4. Click **Set**.


Patrol Settings-Patrol 1

No	Preset	Speed	Duration	Edit
1	Preset 1	1	15	✎
2	Preset2	1	15	✎

Figure 3-15 Patrol Settings

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



KeyPoint

Preset: Preset 1

Speed: 1

Duration: 15

Figure 3-16 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.

Table 3-1 Operation Description

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.

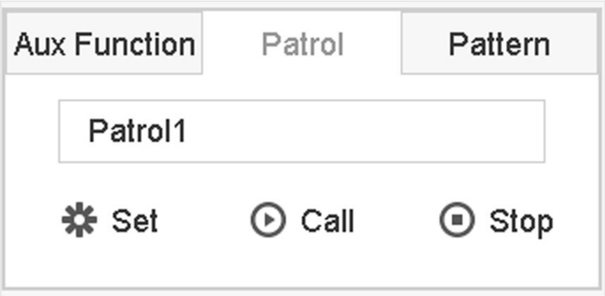
3.5.5 Call a Patrol

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.



Patrol1

Figure 3-17 Patrol Configuration

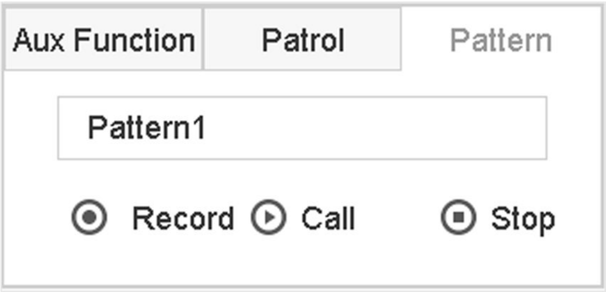
3. Select a patrol.
4. Click **Call** to start the patrol.
5. **Optional:** Click **Stop** to stop the patrol.

3.5.6 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.



Pattern1

Figure 3-18 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.

3.5.7 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.

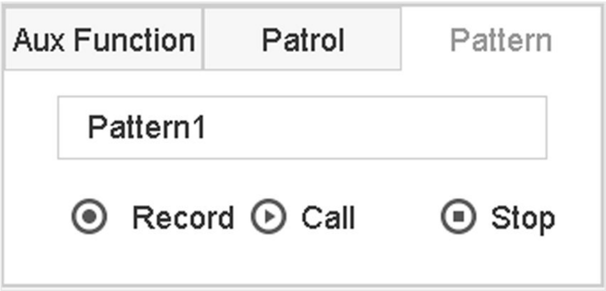


Figure 3-19 Pattern Configuration

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

3.5.8 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 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 not greater than 180º.

3.5.9 One-Touch Park

Certain speed dome models can be configured to start a predefined park action (scan, preset, patrol, 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.

3.5.10 Auxiliary Functions

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

Before You Start

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

Steps

1. Click on the quick settings toolbar of the PTZ camera's live view. The PTZ control panel displays on the right of the interface.
2. Click **Aux Function**.

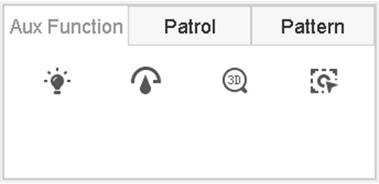


Figure 3-20 Aux Function Configuration

3. Click the icons to operate the aux functions. See the table for the icon descriptions.

Table 3-2 Description of Aux Functions Icons

Icon	Description
💡	Light on/off
💧	Wiper on/off
3D	3D positioning
⛶	Center

Chapter 4 Recording and Playback

4.1 Recording

4.1.1 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.

Audio

The audio input signal source.

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.
- For DS-7100HQHI-K, DS-7204/7208/7216HQHI-K, DS-710HUHI-K, DS-7200HUHI-K, DS-7200HTHI-K, iDS-7200HQHI-K1/S(B), iDS-7200HQHI-K2/4S(B), iDS-7200HUHI-K/4S(B), iDS-7200HQHI-M, iDS-7200HUHI-M, and /E series , you can select the input signal source from analog camera. It will transmit audio via coaxial cable.
- Before selecting **Audio** as **Camera**, ensure the camera supports to transmit audio via coaxial cable.
- It will make the local audio input signal unavailable if you select **Audio** as **Camera**.

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.

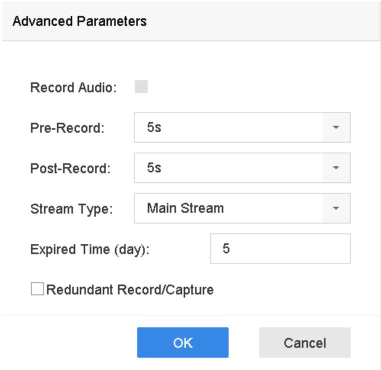
Capture Delay Time

The duration of capturing pictures.

Configure Advanced Recording Parameters

Steps

1. Go to **Storage → Schedule → Record** .
2. Check **Enable Schedule** to enable scheduled recording.
3. Click **Advanced** to set the advanced parameters.


Advanced Parameters

Record Audio: □

Pre-Record: 5s

Post-Record: 5s

Stream Type: Main Stream

Expired Time (day): 5

□ Redundant Record/Capture

Figure 4-1 Advanced Record Settings

Record Audio

Enable or disable audio recording.

Pre-record

The time you set to record before the scheduled time or event. For example, when an alarm triggers the recording at 10:00, and if you set the pre-record time as 5 seconds, the camera records at 9:59:55.

Post-record

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

Stream Type

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

Expired Time

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

Redundant Record/Capture

By enabling redundant record or capture you save the record and captured picture in the redundant HDD.

4.1.2 Enable 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.

4.1.3 Manual Recording

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

4.1.4 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) and **Event** triggered recording and capture, you must configure the motion detection settings, alarm input settings and other events as well. Refer to 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

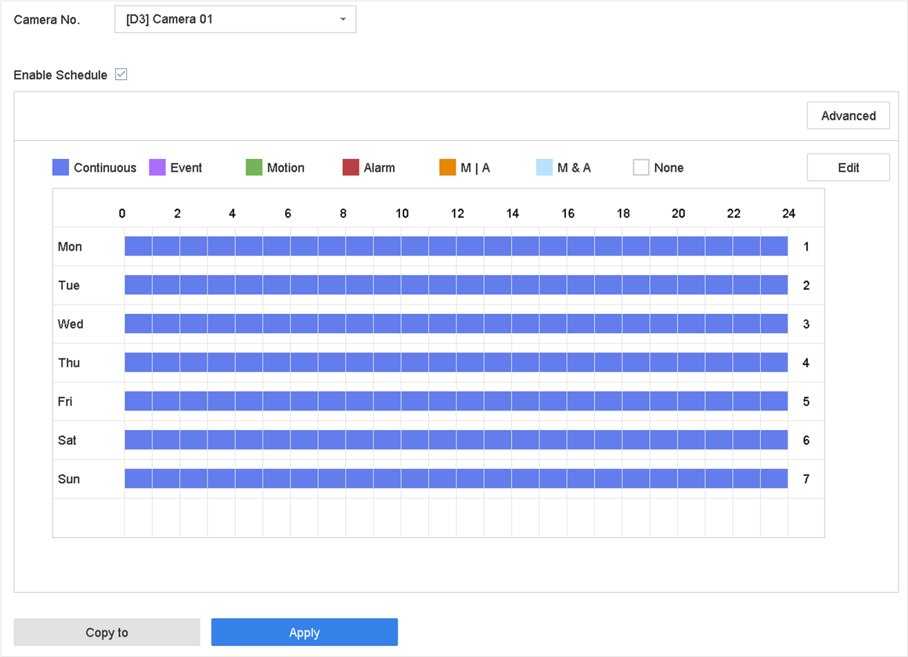
   Recording triggered by either motion detection or alarm.

   M&A

   Recording triggered by motion detection and alarm.

   POS

   Recording triggered by POS and alarm.
5. Drag the cursor on time bar to set the record schedule.



Camera No. [D3] Camera 01

Enable Schedule ☑

Figure 4-2 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**.

4.1.5 Configure Continuous Recording

The device can continuously record the video within the configured time schedule.

Steps

1. Go to **Camera → Encoding Parameters → Recording Parameters** .
2. Set the continuous main stream/sub-stream recording parameters for the camera.
3. Go to **Storage → Recording Schedule** .
4. Drag the mouse on the time bar to set the continuous recording schedule. Refer to ***Configure Plan Recording*** for details.

4.1.6 Configure Motion Detection Triggered Recording

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

Steps

1. Go to **System → Event → Normal Event → Motion Detection** .
2. Configure the motion detection and select the channel (s) to trigger the recording when motion event occurs. Refer to ***Configure Linkage Actions*** for details.
3. Go to **Camera → Encoding Parameters → Recording Parameters** .
4. Set the event main stream/sub-stream recording parameters for the camera.
5. Go to **Storage → Recording Schedule** .
6. Select the recording type to **Motion**.
7. Drag the mouse on the time bar to set motion detection recording schedule. Refer to ***Configure Plan Recording*** for details.

4.1.7 Configure Event Triggered Recording

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

Steps

1. Go to **System → Event** .
2. Configure the event detection and select the channel(s) to trigger the recording when event occurs. Refer to ***Event*** for details.
3. Go to **Camera → Encoding Parameters → Recording Parameters** .
4. Set the event main stream/sub-stream recording parameters for the camera.
5. Go to **Storage → Recording Schedule** .
6. Select the recording type to **Event**.
7. Drag the mouse on the time bar to set the event detection recording schedule. Refer to ***Configure Plan Recording*** for details.

4.1.8 Configure Alarm Triggered Recording

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

Steps

1. Go to **System → Event → Normal Event → Alarm Input** .
2. Configure the alarm input and select the channel(s) to trigger the recording when alarm occurs. Refer to ***Event*** for details.
3. Go to **Camera → Encoding Parameters → Recording Parameters** .
4. Set the event main stream/sub-stream recording parameters for the camera.
5. Go to **Storage → Recording Schedule** .
6. Select the recording type to **Alarm**.

7. Drag the mouse on the time bar to set the alarm recording schedule. Refer to ***Configure Plan Recording*** for details.

4.1.9 Configure Picture Capture

The picture refers to the live picture capture in continuous or event recording type. Only certain models support this function.

Steps

1. Go to **Camera → Encoding Parameters → Capture** .
2. Set the picture parameters.

   Resolution

   Set the resolution of the picture to capture.

   Picture Quality

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

   Interval

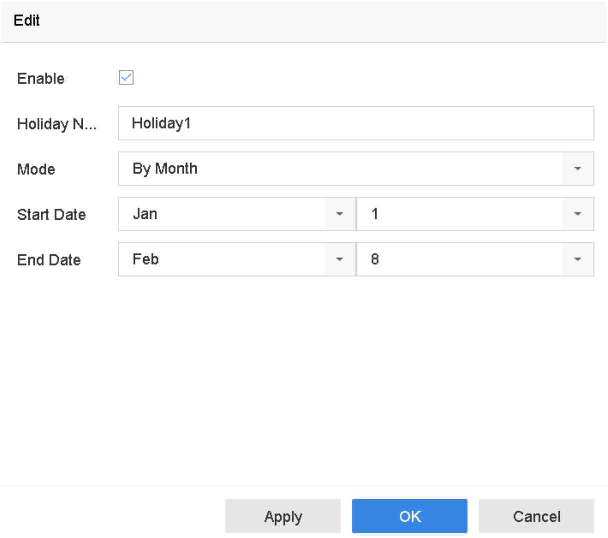
   The interval of capturing live picture.
3. Go to **Storage → Capture Schedule** .
4. Select the camera to configure the picture capture.
5. Set the picture capture schedule. Refer to ***Configure Plan Recording*** for details.

4.1.10 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**.


Edit

Enable ☑

Holiday N... Holiday1

Mode By Month

Start Date Jan 1

End Date Feb 8

Figure 4-3 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.

4.1.11 Configure Redundant Recording and Capture

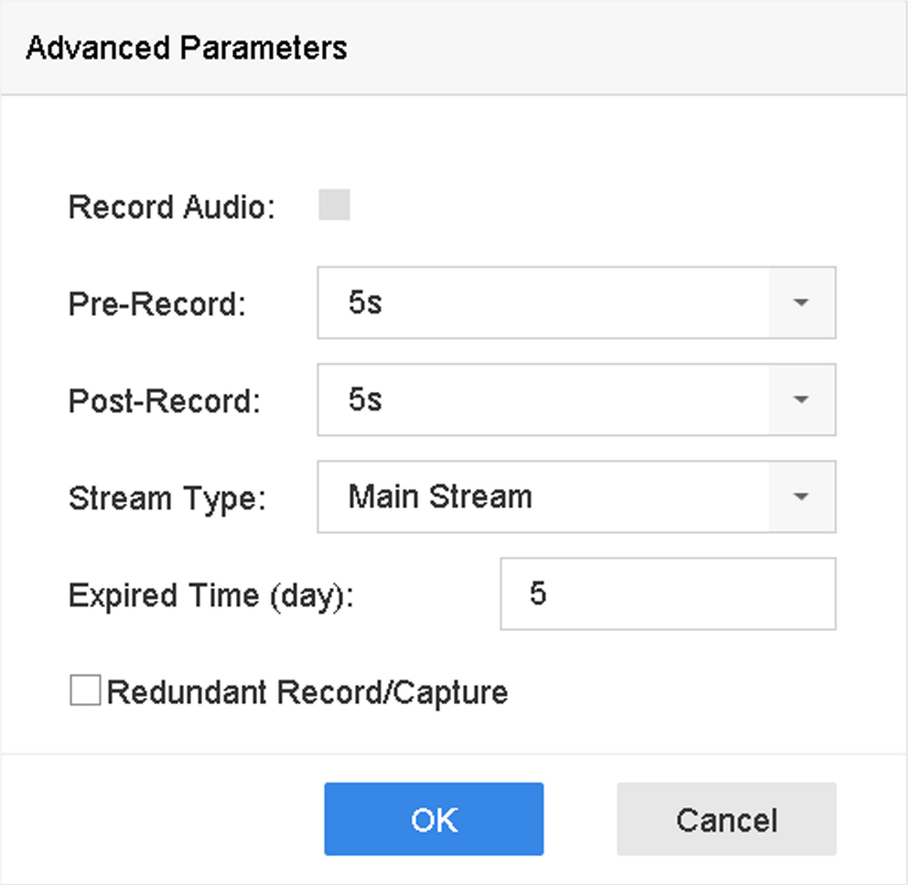
Enabling redundant recording and capture, which means saving the record files and captured pictures not only in the R/W HDD but also in the redundant HDD, will effectively enhance the data safety and reliability.

Before You Start

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

Steps

1. Go to **Storage → Storage Device** .
2. Select a HDD from the list and click ✎ to enter the **Local HDD Settings** interface.
3. Set the HDD property to **Redundancy**.
4. Go to **Storage → Schedule Settings → Record Schedule/Capture Schedule** .
5. Click **Advanced** to set the camera recording parameters.


Advanced Parameters

Record Audio: □

Pre-Record: 5s

Post-Record: 5s

Stream Type: Main Stream

Expired Time (day): 5

□ Redundant Record/Capture

Figure 4-4 Record Parameters

6. Check **Redundant Record/Capture**.
7. Click **OK** to save settings.

4.1.12 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**.

4.2 Playback

4.2.1 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.

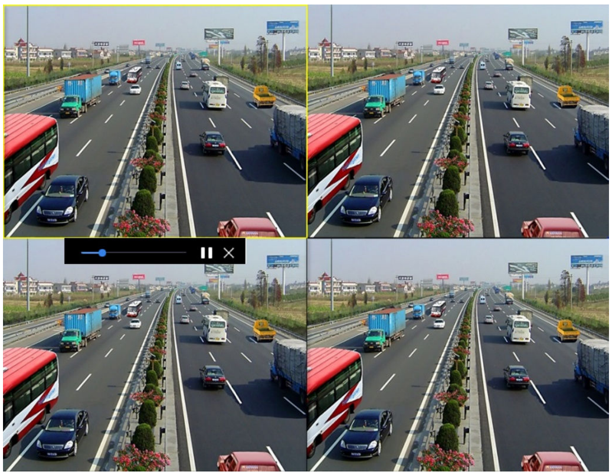


Figure 4-5 Playback

4.2.2 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).

Note

256x playing speed is supported.

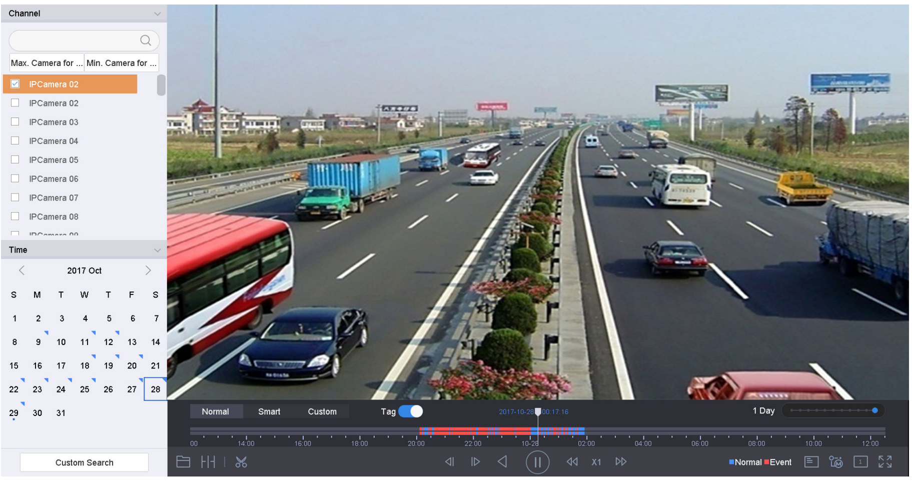


Figure 4-6 Play Normal Video Interface

4.2.3 Play Smart Searched Video

In smart playback mode, the device can analyze videos that containing motion, line, or intrusion detection information, and mark them in red.

Go to **Playback**, click **Smart**, then select detection event such as line crossing detection (⟍) or intrusion detection (□) in the toolbar at the bottom, and play the video as your desire.

For certain analog cameras that have enabled human and vehicle of motion detection, you can click 👤 or 🚗 to search human and vehicle targets. When you are playing back videos that contain human or vehicle targets, the device cannot use the videos (that contain human or vehicle targets) to apply a double analysis of line crossing detection (⟍) or intrusion detection (□).

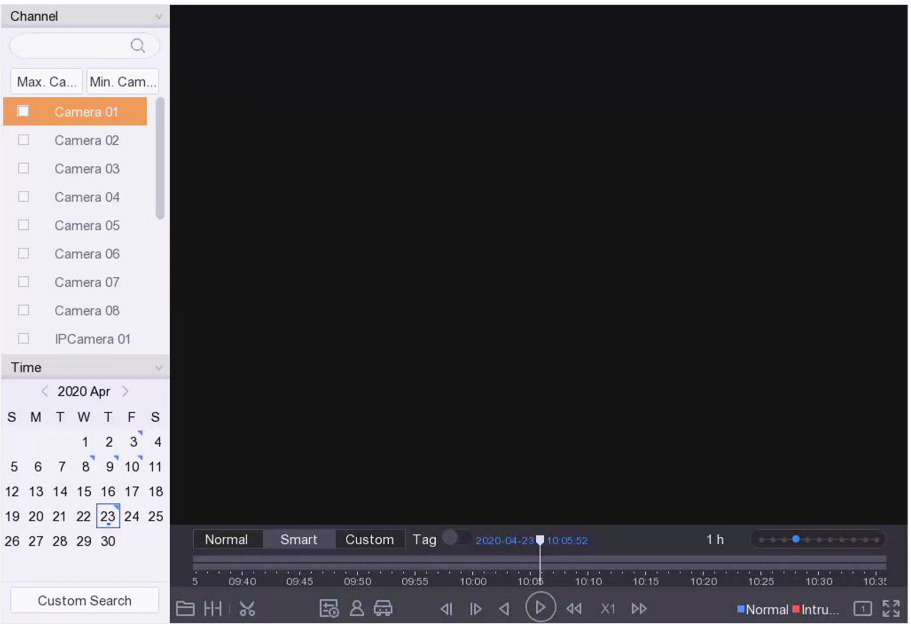


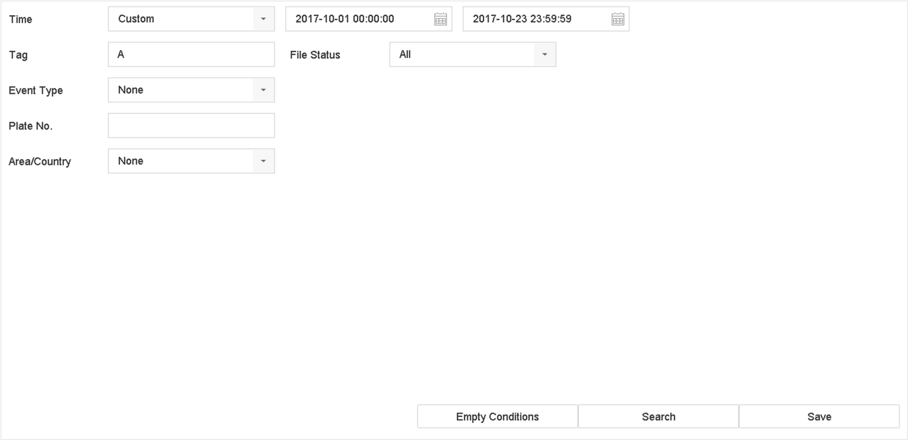
Figure 4-7 Payback by Smart Search

4.2.4 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.



Time: Custom | 2017-10-01 00:00:00 | 2017-10-23 23:59:59

Tag: A

File Status: All

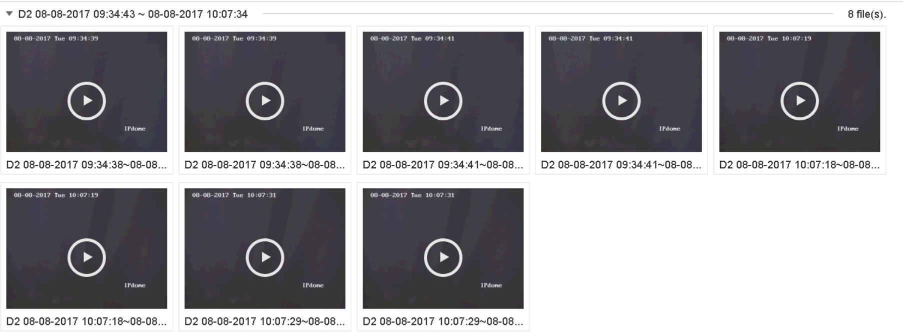
Event Type: None

Plate No.:

Area/Country: None

Figure 4-8 Custom Search

5. Click **Search**.



▾ D2 08-08-2017 09:34:43 ~ 08-08-2017 10:07:34

8 file(s).

D2 08-08-2017 09:34:38~08-08...

D2 08-08-2017 09:34:38~08-08...

D2 08-08-2017 09:34:41~08-08...

D2 08-08-2017 09:34:41~08-08...

D2 08-08-2017 10:07:18~08-08...

D2 08-08-2017 10:07:18~08-08...

D2 08-08-2017 10:07:29~08-08...

D2 08-08-2017 10:07:29~08-08...

Figure 4-9 Custom Searched Video Files

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

4.2.5 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**.

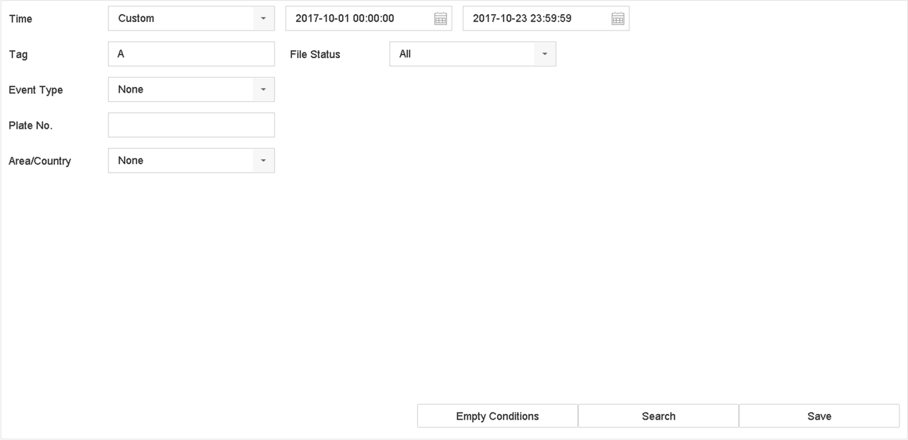
Note

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.



Time: Custom, 2017-10-01 00:00:00, 2017-10-23 23:59:59

Tag: A

File Status: All

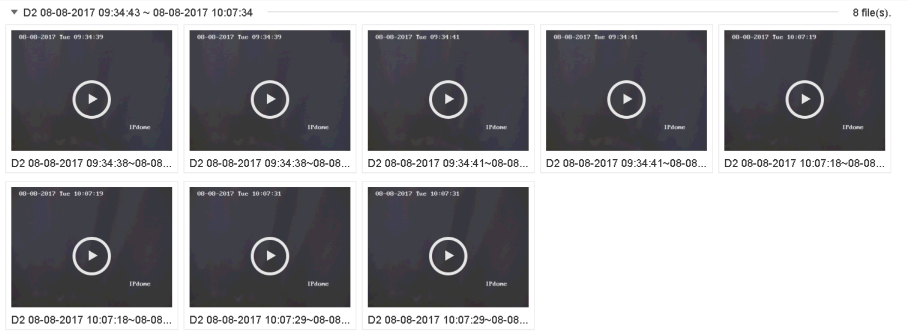
Event Type: None

Plate No.:

Area/Country: None

Figure 4-10 Tag Search

4. Click **Search**.



▼ D2 08-08-2017 09:34:43 ~ 08-08-2017 10:07:34 8 file(s).

D2 08-08-2017 09:34:38~08-08...

D2 08-08-2017 09:34:38~08-08...

D2 08-08-2017 09:34:41~08-08...

D2 08-08-2017 09:34:41~08-08...

D2 08-08-2017 10:07:18~08-08...

D2 08-08-2017 10:07:18~08-08...

D2 08-08-2017 10:07:29~08-08...

D2 08-08-2017 10:07:29~08-08...

Figure 4-11 Searched Tag Files

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

4.2.6 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

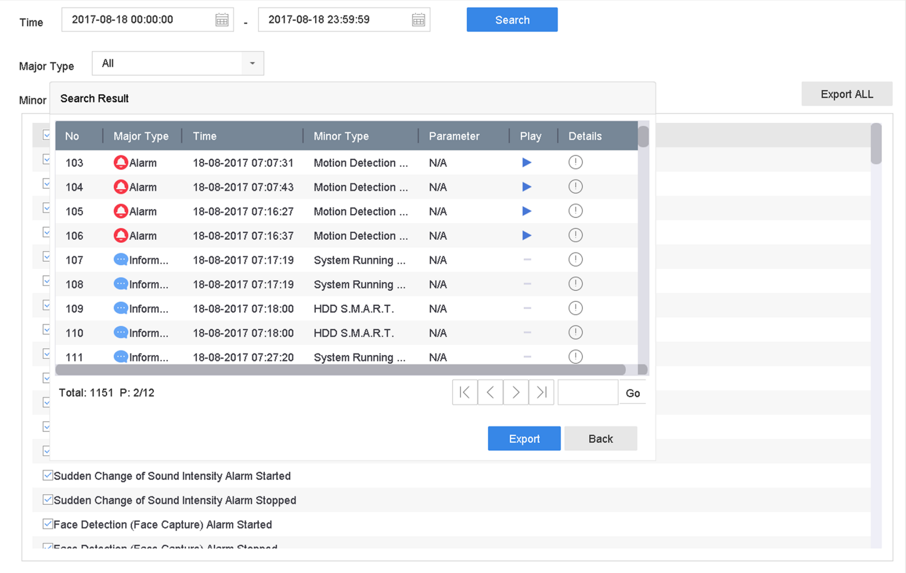
According to the defined number of split-screens, the video files on the selected date can be divided into average segments for playback. E.g., if there are video files existing between 16:00 and 22:00, and the 6-screen display mode is selected, then it can play the video files for 1 hour on each screen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

4.2.7 Play Log Files

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

Steps

1. Go to **Maintenance → Log Information** .
2. Click **Log Search** .
3. Set search time and type and click **Search**.



Time 2017-08-18 00:00:00 - 2017-08-18 23:59:59

Major Type All

Minor

Search Result

No	Major Type	Time	Minor Type	Parameter	Play	Details
103	Alarm	18-08-2017 07:07:31	Motion Detection ...	N/A	▶	ⓘ
104	Alarm	18-08-2017 07:07:43	Motion Detection ...	N/A	▶	ⓘ
105	Alarm	18-08-2017 07:16:27	Motion Detection ...	N/A	▶	ⓘ
106	Alarm	18-08-2017 07:16:37	Motion Detection ...	N/A	▶	ⓘ
107	Inform...	18-08-2017 07:17:19	System Running ...	N/A	–	ⓘ
108	Inform...	18-08-2017 07:17:19	System Running ...	N/A	–	ⓘ
109	Inform...	18-08-2017 07:18:00	HDD S.M.A.R.T.	N/A	–	ⓘ
110	Inform...	18-08-2017 07:18:00	HDD S.M.A.R.T.	N/A	–	ⓘ
111	Inform...	18-08-2017 07:27:20	System Running ...	N/A	–	ⓘ

Total: 1151 P: 2/12

☑ Sudden Change of Sound Intensity Alarm Started

☑ Sudden Change of Sound Intensity Alarm Stopped

☑ Face Detection (Face Capture) Alarm Started

Figure 4-12 System Log Search Interface

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

4.2.8 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.

4.3 Playback Operations

4.3.1 Normal/Important/Custom Video

During the playback, you can select the following three modes to play the video.

Normal

Video files from the continuous recording.

Important

Video files from the event and alarm recording triggered recording.

Custom

Video files searched by custom conditions.

4.3.2 Set Play Strategy in Important/Custom Mode

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

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

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

Note

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

4.3.3 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.

4.3.4 Switch between Main Stream and Sub-Stream

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

Icon	Description
Ⓜ	Play the video in main stream.
Ⓢ	Play the video in sub-stream.

Note

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

4.3.5 Thumbnails View

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

In the playback mode, position the cursor on time bar to get preview thumbnails.

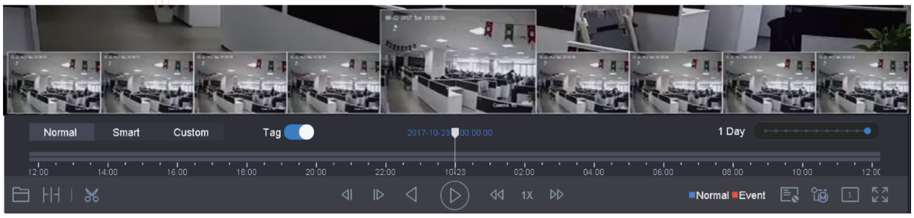


Figure 4-13 Thumbnails View

You can click a thumbnail to enter the full-screen playback.

4.3.6 Fast View

Hold the mouse to drag on the time bar to get a fast view of the video files.

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

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

4.3.7 Digital Zoom

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

Steps

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

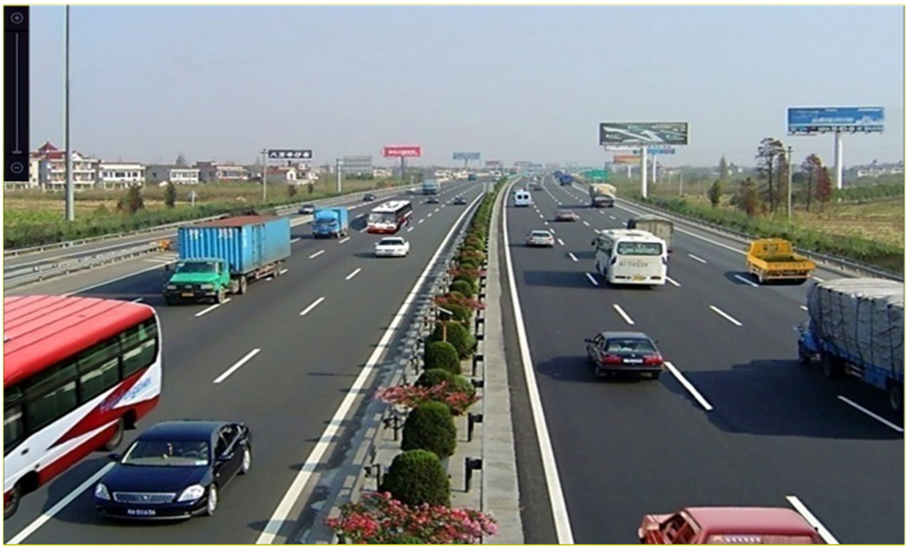


Figure 4-14 Digital Zoom

Chapter 5 Smart Analysis

5.1 Engine Configuration

Each engine processes a specified VCA type as its working mode. You can configure the engine working mode as your desire.

Steps

Note

The chapter is only available for certain models of iDS series.

1. Go to **Smart Analysis → Smart Analysis → Engine Configuration** .
2. Configure each engine usage. You can view the engine temperature and linked channel status of each function.

   Note

   If the engine has been bound with channel(s), switching engine working mode will unbind the engine and channel(s), and cancel the related smart event of the channel.

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

5.2 Task Configuration

You can view the task status in task configuration. Smart analysis results are used for filtering the pictures when searching interested human body and vehicle pictures.

Before You Start

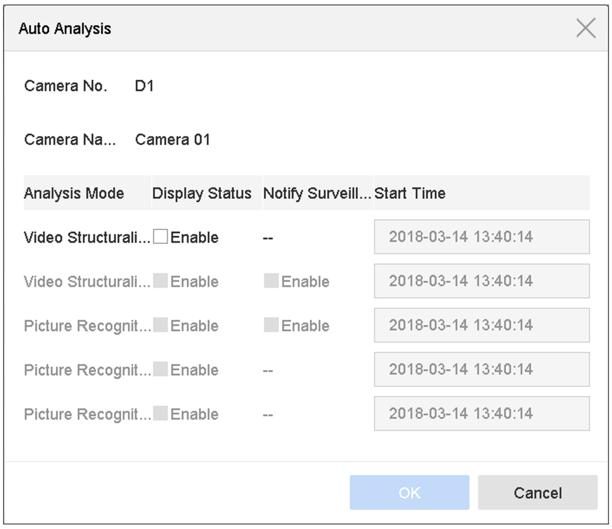
Check **Save VCA Pictures** for human body detection/vehicle detection, line crossing detection, intrusion detection, region entrance, or region exiting.

Steps

Note

The chapter is only available for certain models of iDS series.

1. Go to **Smart Analysis → Smart Analysis → Task Configuration** .
2. Check cameras to enable corresponding analysis mode. Ensure engine is available for the selected analysis mode.
3. Enable auto analysis.



Auto Analysis

Camera No. D1

Camera Na... Camera 01

Analysis Mode	Display Status	Notify Surveill...	Start Time
Video Structurali...	□ Enable	--	2018-03-14 13:40:14
Video Structurali...	□ Enable	□ Enable	2018-03-14 13:40:14
Picture Recognit...	□ Enable	□ Enable	2018-03-14 13:40:14
Picture Recognit...	□ Enable	--	2018-03-14 13:40:14
Picture Recognit...	□ Enable	--	2018-03-14 13:40:14

Figure 5-1 Auto Analysis

1) Click **Edit**.
2) **Optional:** Check Enable of Display Status and Notify Surveillance Center.
3) Set **Start Time** of video to analyze.
4) Click **OK**.

4. Check cameras and click **Enabled** to start analyzing.

   Task status includes 3 conditions: Disabled, Waiting, and Enabled.

   - Disabled: No analysis task is enabled on the camera.
   - Waiting: The analysis task of the camera is enabled. Device is waiting to analyze data.
   - Enabled: The analysis task of the camera is enabled and device is analyzing data of the camera.

5. **Optional:** For Non-Real-Time Face Picture Comparison analysis mode, click **View Record** to view the progress of each day.

5.3 Configure Enhanced VCA Mode

Enabling enhanced VCA mode will maximize the connectable channel number for line crossing detection and intrusion detection. However, it will disable 2K/4K HDMI output resolution and 4 MP/5 MP/8 MP signal input for HUHI-K series. And for HQHI-K series, it will disable CVBS output and channel-zero encoding.

Go to **System → General** , and check **Enhanced VCA Mode**.

5.4 Face Picture Comparison

The device supports the face picture comparison alarm and face capture for the connected camera based on face recognition feature.

Go to **Smart Analysis → Smart Analysis → Engine Configuration** . Configure at least one engine usage as **Facial Recognition**. Refer to ***Engine Configuration*** for details.

Note

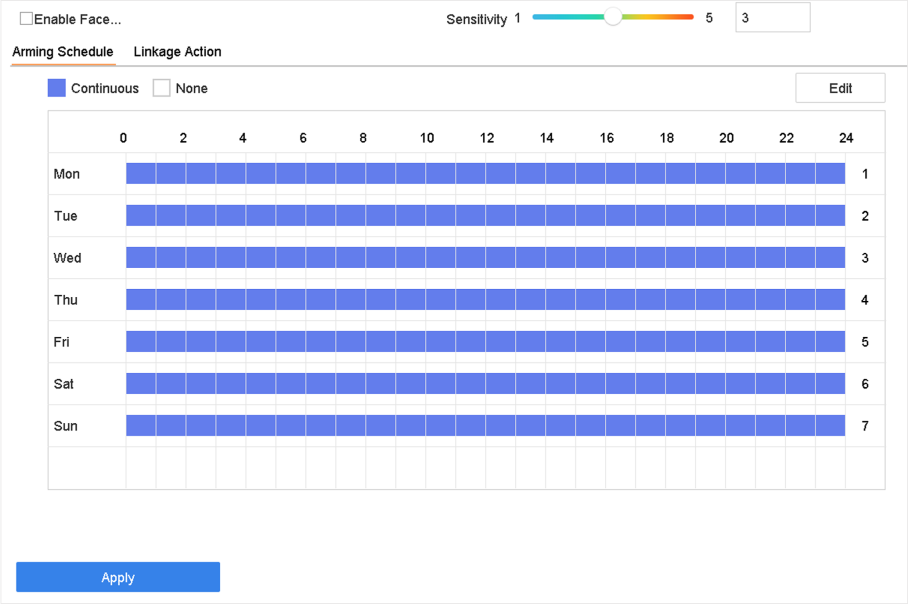
The chapter is only available for certain models of iDS series.

5.4.1 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**.



□ Enable Face...

Sensitivity 1 — 5: 3

Figure 5-2 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**.

5.4.2 Face Picture Library Management

Face picture library is mainly used for face picture storage and face picture comparison.

Add a Face Picture Library

You can create face picture libraries via local GUI or Hik-Connect app. Here we take the operations on local GUI as an example.

Steps

1. Go to **Smart Analysis → Face Picture Database** .
2. Click + .
3. Enter the face picture library name.
4. Click **OK**.

Note

You can click ✎ or × to edit the library name or delete the library.

Upload Face Pictures to the Library

Face picture comparison is based on face pictures in the library. You can upload a single face picture or import multiple face pictures to the library.

Before You Start

- Ensure the picture format is JPEG or JPG.
- For each picture, ensure it only has one face.
- Import all pictures to a backup device in advance.

Steps

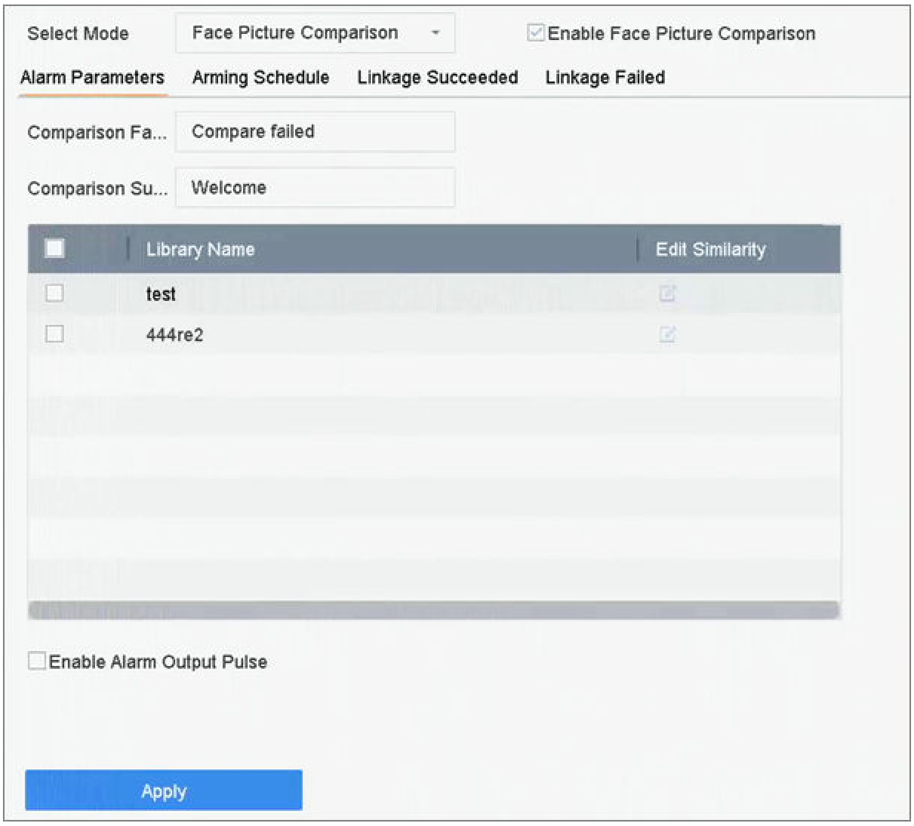
1. Select a face picture library in the list.
2. Click **Add** or **Import Face Picture Library**.
3. Import picture(s).
   - **Add**: Select a picture to import and click **Import**.
   - **Import Face Picture Library**: Select multiple pictures to import and click **Import**.
4. **Optional:** Select pictures and click **Copy to** to copy the uploaded pictures of the current library to other library.
5. **Optional:** Select a picture and click **Edit** to modify the picture information.
6. **Optional:** Select a picture from the list and click **Delete** to delete the picture.
7. **Optional:** Select a library and click **Export Face Picture Library** to export library to backup device.
8. **Optional:** Click ⊞ or ☰ to view by figure or list.

5.4.3 Configure Face Picture Comparison

Compare detected face pictures with specified face picture library. Trigger alarm when comparison succeeded.

Steps

1. Go to **System → Event → Smart Event → Face Picture Comparison** .



Select Mode: Face Picture Comparison

☑ Enable Face Picture Comparison

Comparison Fa...: Compare failed

Comparison Su...: Welcome

□	Library Name	Edit Similarity
□	test	✎
□	444re2	✎

□ Enable Alarm Output Pulse

Figure 5-3 Face Picture Comparison

2. Select a camera.
3. Select **Mode** as **Face Picture Comparison**.
4. Check **Enable Face Picture Comparison**.
5. **Optional:** Set **Comparison Failed Prompt**, **Comparison Succeeded Prompt**, and **Enable Alarm Output Pulse**.

   Comparison Failed Prompt

   It will display the prompt in live view **Target Detection** (with **Facial Detection** checked) or **Facial Recognition** when face picture comparison failed. You can click ☺ in live view to enter Facial Recognition interface.

   Comparison Succeeded Prompt

   It will display the prompt in **Facial Recognition** when face picture comparison succeeded. You can click ☺ in live view to enter Facial Recognition interface.

Enable Alarm Output Pulse

It is usually linked with a gate. When a person is passing a gate, if the comparison succeeded, it will trigger a pulse to open the gate. The pulse is between 100 to 900 ms. You can set **Alarm Output Pulse (ms)** in **System → Event → Normal Event → Alarm Output** .

6. Select face picture libraries and set similarity.
7. Set the arming schedule. Refer to ***Configure Arming Schedule*** .
8. Set the linkage actions when face picture comparison succeeded or failed. Refer to ***Configure Linkage Actions*** .
9. Click **Apply** to save the settings.

5.4.4 Face Picture Search

Search by Face Picture Comparison Event

Search face picture by face picture comparison results.

Steps

1. Go to **Smart Analysis → Smart Search → Face Search → Search by Event** .
2. Set the start time and end time.
3. Select a channel.
4. Select **Event Type** as **Face Picture Comparison**.
5. Click **Start Search**. The search result list displays 1 channel.
6. Click **Channel** to select a channel as your desire. It will display search results for the selected channel.

What to do next

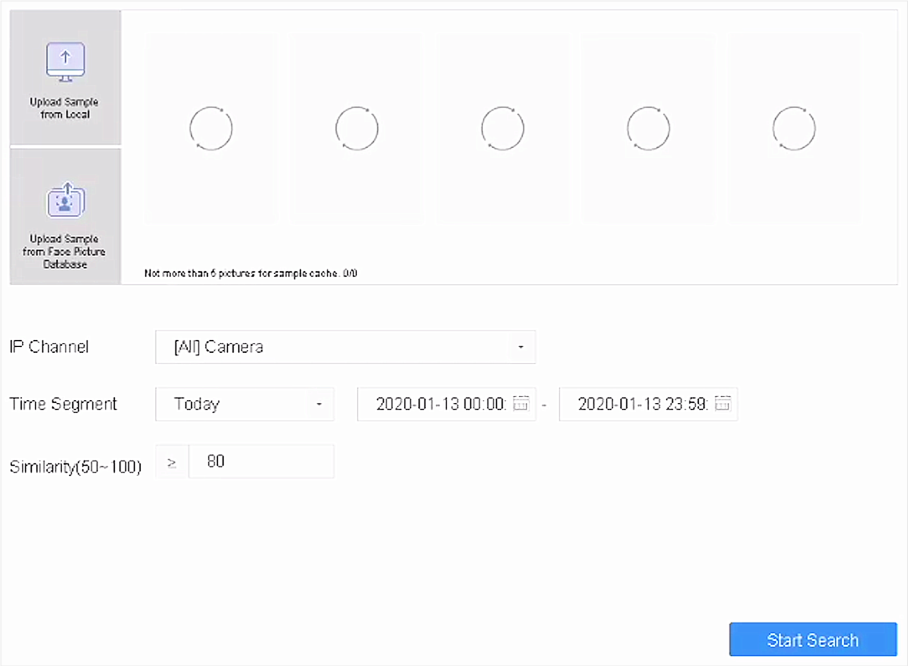
Refer to ***View Searching Result*** .

Search by Uploaded Picture

You can search the face pictures by uploaded picture.

Steps

1. Go to **Smart Analysis → Smart Search → Face Search → Search by Picture** .



Not more than 6 pictures for sample cache. 0/0

IP Channel [All] Camera

Time Segment Today 2020-01-13 00:00 - 2020-01-13 23:59

Similarity(50~100) ≥ 80

Figure 5-4 Search by Uploaded Picture

2. Select a channel.
3. Select face pictures for search.
    - Click **Upload Sample from Local** and select face pictures from your local directory.
    - Click **Upload Sample from Face Picture Database** and select face pictures from created face picture libraries.
4. Set the start time and end time.
5. Set the **Similarity** value (range: 0 to 100). Device will analyze the similarity between samples and face pictures in library and show pictures the similarity of which are higher than the set one.
6. Click **Start Search**. The search result list displays 1 channel.
7. Click **Channel** to select a channel as your desire. It will display search results for the selected channel.

What to do next

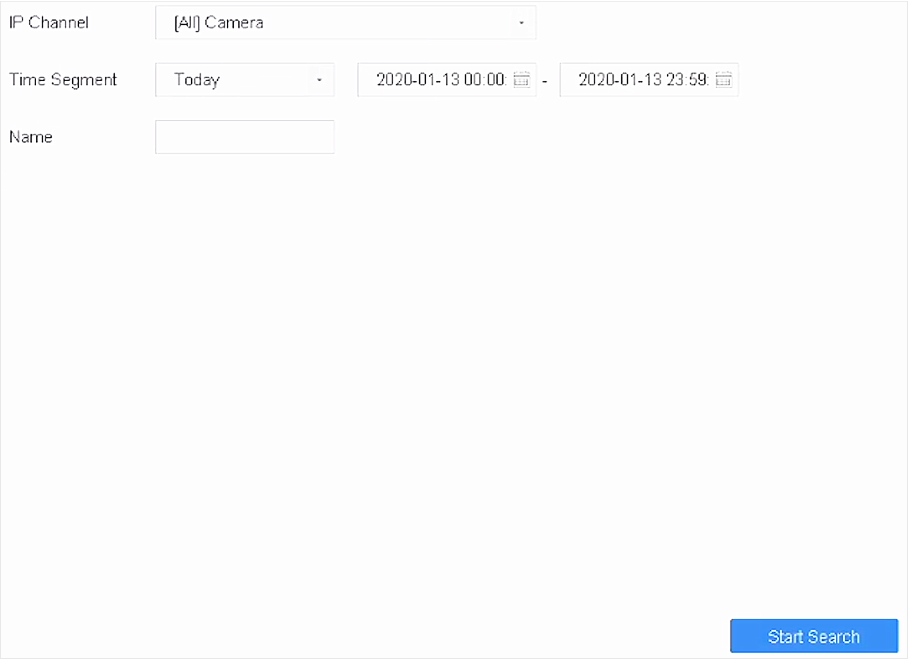
Refer to ***View Searching Result*** .

Search by Personal Name

Search face picture by personal name.

Steps

1. Go to **Smart Analysis → Smart Search → Face Search → Search by Name** .



IP Channel [All] Camera

Time Segment Today 2020-01-13 00:00 - 2020-01-13 23:59

Name

Figure 5-5 Search by Personal Name

2. Set the start time and end time of the face pictures to search.
3. Select a channel.
4. Enter a name.
5. Click **Start Search**. The search result list displays 1 channel.
6. Click **Channel** to select a channel as your desire. It will display search results for the selected channel.

What to do next

Refer to ***View Searching Result*** .

Search by Appearance

Search face picture by appearance.

Steps

1. Go to **Smart Analysis → Smart Search → Face Search → Search by Appearance** .
2. Set search conditions.
3. Click **Start Search**. The search result list displays 1 channel.
4. Click **Channel** to select a channel as your desire. It will display search results for the selected channel.

What to do next

Refer to ***View Searching Result*** .

View Searching Result

- Double click a file to view the related video.
- Click **Add to Face Database** to add the selected file(s) to a face picture library.
- Click **Add to Sample** to add the select file(s) as sample picture(s). You can use the sample picture(s) to search other pictures. Refer to ***Search by Uploaded Picture*** .
- Click **Export** to export the selected file(s) to a backup device. You can click **Select All** to select all files.

Note

- You can click ▣ to view export progress.
- You can click ︾ to return to search interface.

5.5 Perimeter Protection

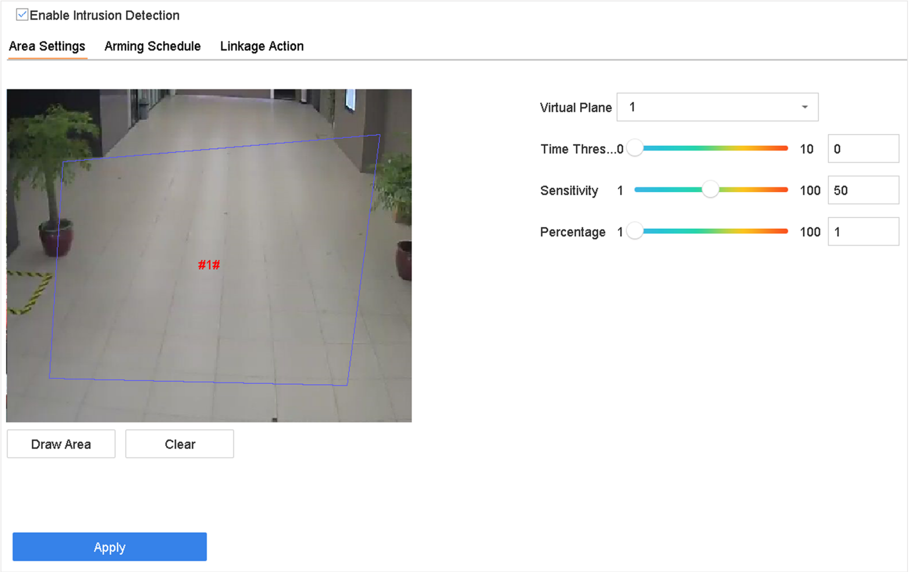
For certain models of iDS series. Go to **Smart Analysis → Smart Analysis → Engine Configuration** . Configure at least one engine usage as **Perimeter Protection**. Refer to ***Engine Configuration*** for details.

5.5.1 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**.



☑Enable Intrusion Detection

Area Settings | Arming Schedule | Linkage Action

Virtual Plane: 1

Time Thres...: 0 – 10, 0

Sensitivity: 1 – 100, 50

Percentage: 1 – 100, 1

Figure 5-6 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. Set the arming schedule. Refer to ***Configure Arming Schedule*** .
7. Set linkage actions. Refer to ***Configure Linkage Actions*** .
8. Click **Apply**.

Note

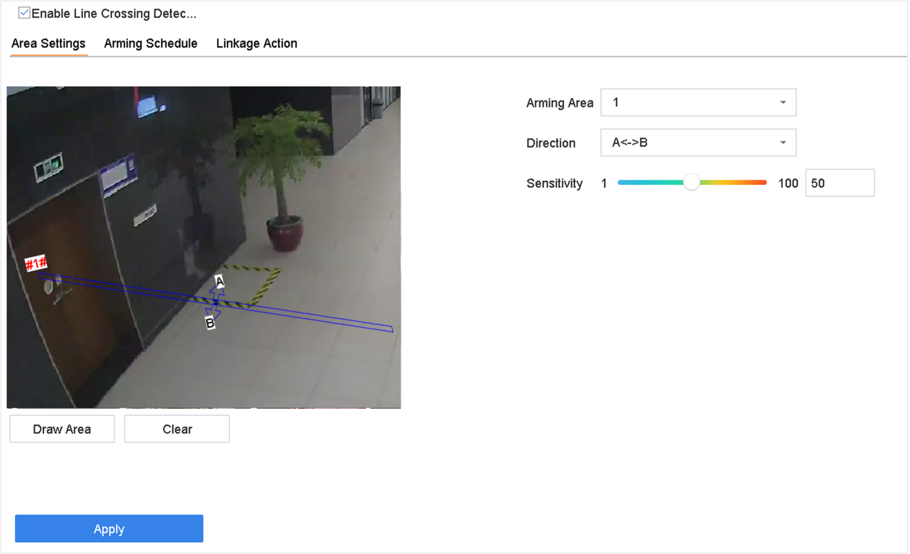
For iDS-7200 series, you can set **Target Detection** as **Human** or **Vehicle**. Only the target of selected type will trigger the alarm.

5.5.2 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**.



☑Enable Line Crossing Detec...

Area Settings | Arming Schedule | Linkage Action

Arming Area: 1

Direction: A<->B

Sensitivity: 1 — 100, 50

Figure 5-7 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. Set the arming schedule. Refer to ***Configure Arming Schedule*** .

8. Set linkage actions. Refer to ***Configure Linkage Actions*** .
9. Click **Apply**.

Note

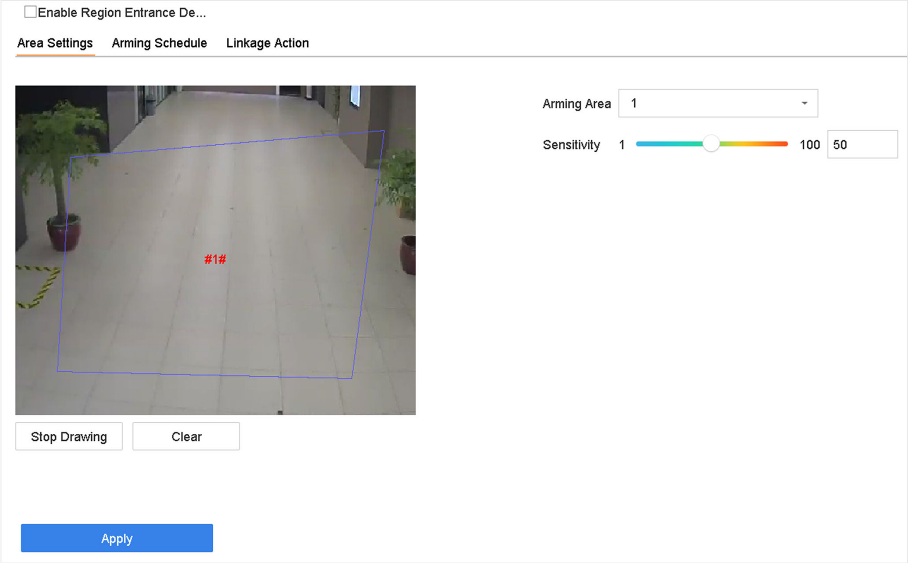
For iDS-7200 series, you can set **Target Detection** as **Human** or **Vehicle**. Only the target of selected type will trigger the alarm.

5.5.3 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**.



☐Enable Region Entrance De...

Area Settings | Arming Schedule | Linkage Action

Arming Area: 1

Sensitivity: 1 – 100, 50

Figure 5-8 Region Entrance Detection

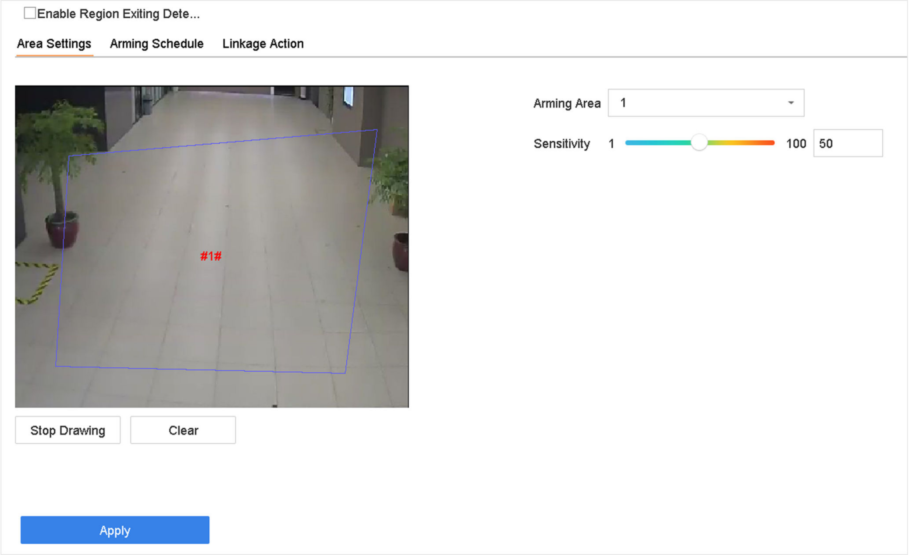
3. Select a camera.
4. Check **Enable Region Entrance Detection**.
5. **Optional:** Check **Save VCA Picture** to save the captured pictures of region entrance detection pictures.
6. Set detection rules and detection areas.
   1) Select **Arming Region**. Up to 4 regions are selectable.
   2) Set **Sensitivity**. 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**.

5.5.4 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**.



□Enable Region Exiting Dete...

Arming Area: 1

Sensitivity: 1 – 100, 50

Figure 5-9 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**.

5.6 Human Body Detection

Go to **Smart Analysis → Smart Analysis → Engine Configuration** . Configure at least one engine usage as **Picture Recognition-Human Body**. Refer to ***Engine Configuration*** for details.

Go to **Smart Analysis → Smart Analysis → Task Configuration** to enable the task for camera. For details, refer to ***Task Configuration*** for details.

Note

The chapter is only available for certain models of iDS series.

5.6.1 Human Body Detection

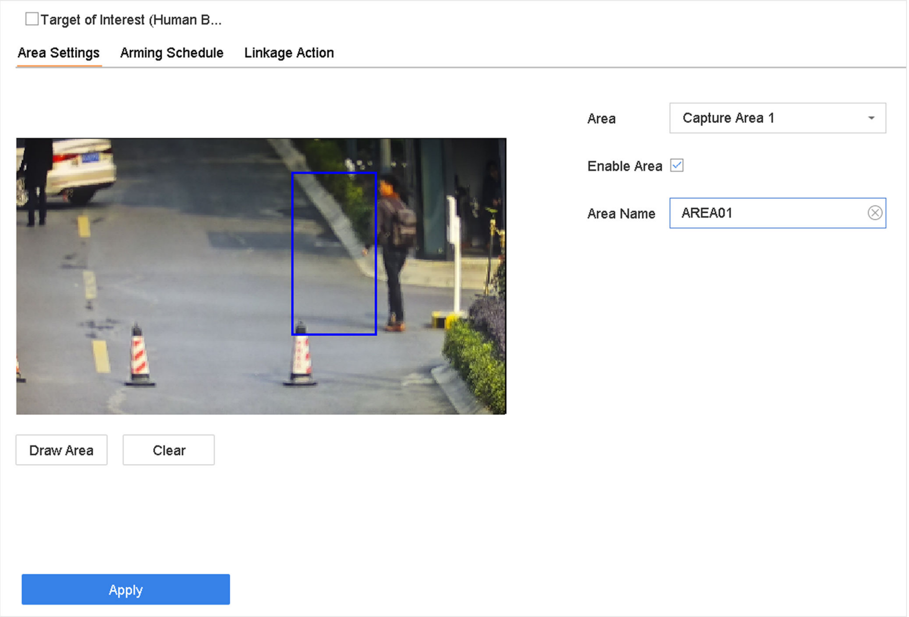
The human body detection enables to detect the human body appearing in the monitoring scene, and capture the human body pictures.

Before You Start

The connected camera supports the human body detection.

Steps

1. Go to **System → Event → Smart Event** .
2. Click **Human Body**.
3. **Optional:** For IP camera does not support human body detection, Check **Enable Local Human Body Detection**. Then the device will consume its decoding resource to execute human body detection. Before enabling the function, go to **Smart Analysis → Smart Analysis → Engine Configuration** to select at least one engine as **Video Structuralization-Real-Time**.
4. Enabling the function will change smart events supported by the camera.
5. Select the camera to configure the human body detection.
6. Check **Save VCA Picture** to save the captured pictures of human body detection.
7. Check **Target of Interest (Human Body)** to discard non-human body pictures and videos which are not triggered by human body detection. The feature is only available for local human body detection.
8. Set detection area.


□ Target of Interest (Human B...

Area: Capture Area 1

Enable Area ☑

Area Name: AREA01

Figure 5-10 Human Body Detection

1) Select the detection area to configure from the Area drop-down list. Up to 8 detection areas are selectable.
2) Check **Enable Area** to enable the selected detection area.
3) Edit the area name in **Scene Name**. The scene name can contain up to 32 characters.
4) Click **Draw Area** to draw a quadrilateral in the preview window and then click **Stop Drawing**.

9. Set the arming schedule. Refer to ***Configure Arming Schedule*** .

10. Set linkage actions. Refer to ***Configure Linkage Actions*** .

11. Click **Apply** to activate the settings.

5.6.2 Human Body Search

Search by Appearance

Search human body pictures according to manually specified search conditions.

Steps

1. Go to **Smart Analysis → Smart Search → Human Body Detection → Search by Appearance** .
2. Specify search conditions.
3. Click **Start Search**. The search result list displays 1 channel.
4. Click **Channel** to select a channel as your desire. It will display search results for the selected channel.
5. **Optional:** Export search results.
   1) Select result file(s) from the search result interface, or check **Select All** to select all files.
   2) Click **Export** to export the selected file(s) to a backup device.

Note

- You can click ▣ to view export progress.
- You can click ︾ to return to search interface.

Search by Uploaded Picture

To increase search accuracy, upload several pictures of one person to compare with captured human body pictures.

Before You Start

Import human body pictures in a USB flash drive and connect it to device.

Steps

Note

- When there are multiple targets existing in the same picture, up to 30 target pictures can be analyzed and displayed.
- The maximum allowed picture size is 3840*2160.
- The picture must be in JPG or JPEG format.
- The picture name (with the suffix) cannot exceed 64 characters.
- Ensure the picture you uploaded is clear and recognizable.

1. Go to **Smart Analysis → Smart Search → Human Body Detection → Search by Picture** .
2. Select a channel.
3. Click **Upload Sample**.
4. Click **Upload Sample from Local** and select face pictures from your local directory.
5. Set the start time and end time.
6. Select a picture in USB flash drive, and click **Import**.
7. Select related pictures, and click **Upload**.
8. Specify search conditions.

   Similarity

   Device will analyze the similarity between samples and face pictures in library and show pictures the similarity of which are higher than the set one.
9. Click **Start Search**. The search result list displays 1 channel.
10. **Optional:** Export search results.

    1)Select result file(s) from the search result interface, or check **Select All** to select all files.

    2)Click **Export** to export the selected file(s) to a backup device.

    Note

    - You can click ▣ to view export progress.
    - You can click ︾ to return to search interface.

Add Search Result as Sample Picture

You can add searched human body pictures as sample pictures. And then search human body pictures by the sample pictures.

Steps

1. Search human body pictures.
2. In search result interface, click to select a picture and click **Add to Sample**.
3. Return to search condition settings interface, the selected sample will be listed.

5.7 Motion Detection

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 detection areas and rules.
    1) Click **Draw Area** to draw the detection area(s) on the preview screen.
    2) Right-click the mouse, and click **Stop Drawing** to finish drawing.
    3) 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.
    4) **Optional:** For certain analog PIR cameras, check **False Alarm Filter** to reduce alarms.
    5) **Optional:** For certain iDS M and iDS K (B) series devices, it can analyze analog camera videos that contain human and vehicle. Check **Human** or **Vehicle** under an analog camera. Only the target of selected type will trigger the alarm, which can reduce false alarms that are caused by other objects.

Note

- **Target Detection** of motion detection is conflicted with PIR alarm, hence **False Alarm Filter** and **Target Detection** of **Human** and **Vehicle** cannot be enabled at the same time.
- **Target Detection** of motion detection may also be conflicted with enhanced IP mode, and smart events like facial detection, face picture comparison, perimeter protection (line crossing detection and intrusion detection).

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

5.8 Vehicle Detection

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

5.8.1 Configure 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.

Steps

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

   Area Settings

   Up to 4 lanes are selectable.

   Blocklist and Allowlist

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

9. Click **Apply**.

Note

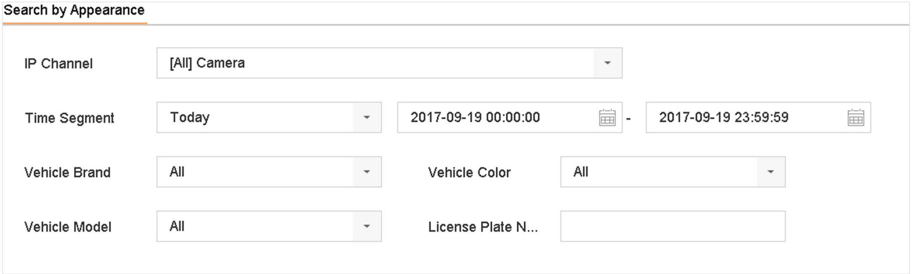
Refer to the Network Camera User Manual for detailed instructions for the vehicle detection.

5.8.2 Vehicle Search

You can search and view the matched vehicle pictures.

Steps

1. Go to **Smart Analysis → Smart Search → Vehicle Search** .
2. Select the IP camera for the vehicle search.
3. Set search conditions.



Search by Appearance

IP Channel: [All] Camera

Time Segment: Today 2017-09-19 00:00:00 - 2017-09-19 23:59:59

Vehicle Brand: All

Vehicle Color: All

Vehicle Model: All

License Plate N...:

Figure 5-11 Vehicle Search

4. Click **Start Search**. The search result list displays 1 channel.
5. Click Channel to select a channel as your desire. It will display search results for the selected channel.
6. Export search results.
   1) Select result file(s) from the search result interface, or check **Select All** to select all files.
   2) Click **Export** to export the selected file(s) to a backup device.

Note

You can click to view export progress.

5.9 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

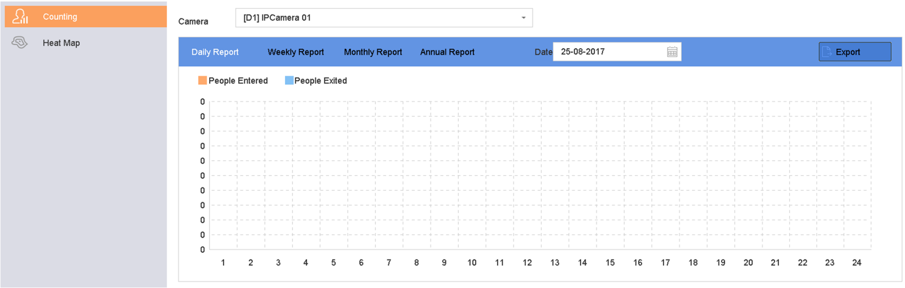
The smart analysis results of the detection are displayed in the list. Click a result in list to play the related video.

5.10 People Counting

Counting calculates the number of people entering or leaving a certain configured area and creates daily/weekly/monthly/annual reports for analysis.

Steps

1. Go to **Smart Analysis → Counting** .
2. Select the camera(s).
3. Select the report type.
4. Set **Date** to analyze. The people counting graphic will show.



Camera [D1] IPCamera 01

Date 25-08-2017

Figure 5-12 People Counting Interface

5. **Optional:** Click **Export** to export the report in Microsoft Excel format.

5.11 Heat Map

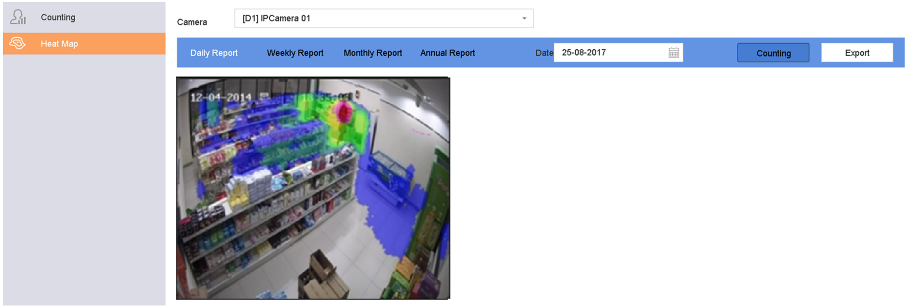
Heat Map is a graphical representation of data. The heat map function is used to analyze how many people visited and stayed in a specific area.

Before You Start

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

Steps

1. Go to **Smart Analysis → Heat Map** .
2. Select a camera.
3. Select the report type.
4. Set **Date** to analyze.



Camera [D1] IPCamera 01

Date 25-08-2017

Figure 5-13 Heat Map Interface

5. Click **Counting**. The results will be displayed in graphics marked in different colors.

Note

As shown in the figure above, red color block (255, 0, 0) indicates the most trafficked area, and blue color block (0, 0, 255) indicates the less-popular area.

6. **Optional:** Click **Export** to export the statistics report in Microsoft Excel format.

Chapter 6 Event

6.1 Normal Event Alarm

6.1.1 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*** .

6.1.2 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*** .

6.1.3 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**.

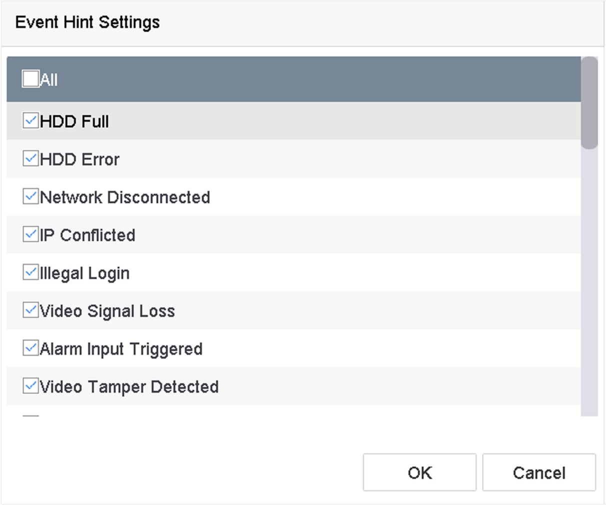
6. Set the arming schedule. Refer to ***Configure Arming Schedule*** .
7. Set linkage actions. Refer to ***Configure Linkage Actions*** .

6.1.4 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.



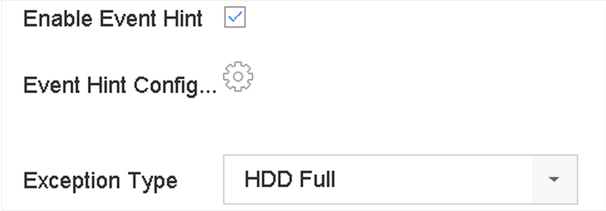
Event Hint Settings

☐ All
☑ HDD Full
☑ HDD Error
☑ Network Disconnected
☑ IP Conflicted
☑ Illegal Login
☑ Video Signal Loss
☑ Alarm Input Triggered
☑ Video Tamper Detected

OK   Cancel

Figure 6-1 Event Hint Settings

3. Select an exception type.



Enable Event Hint ☑

Event Hint Config... ⚙

Exception Type: HDD Full

Figure 6-2 Exceptions Handling

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

6.2 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

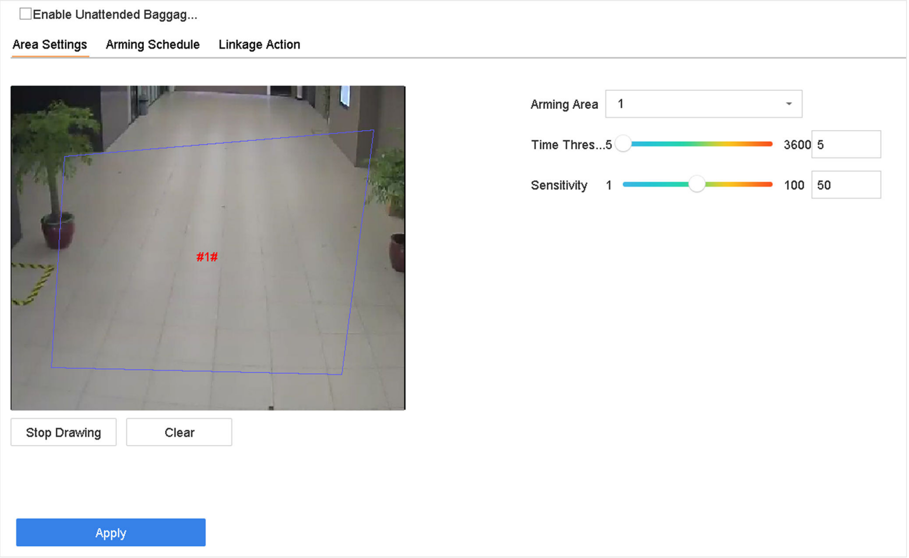
- VCA detections must be supported by the connected IP camera.
- Refer to the network camera user manual for detailed VCA detection instructions.

6.2.1 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**.



□ Enable Unattended Baggag...

Arming Area: 1

Time Thres...: 5 — 3600, 5

Sensitivity: 1 — 100, 50

Figure 6-3 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.

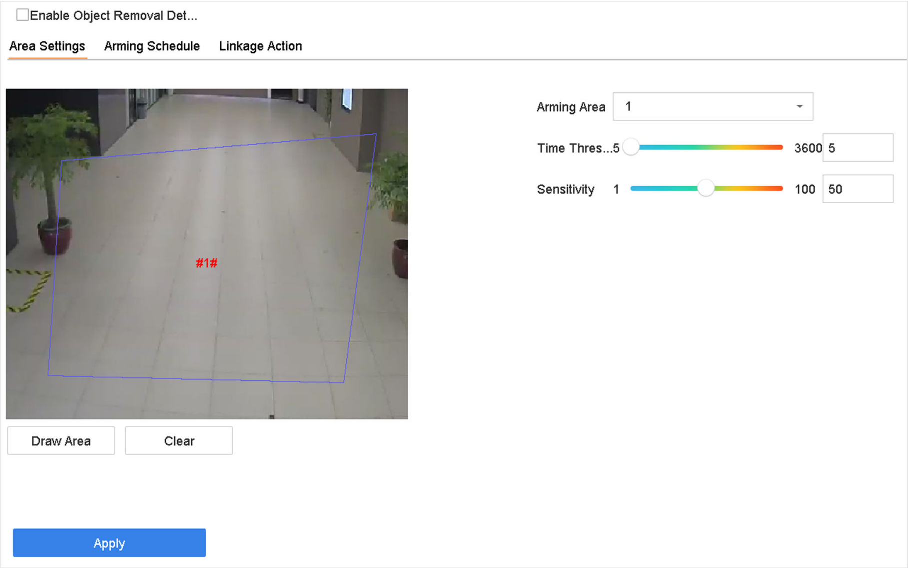
3) Click **Draw Region** and draw a quadrilateral in the preview window.
7. Set the arming schedule. Refer to ***Configure Arming Schedule*** .
8. Set linkage actions. Refer to ***Configure Linkage Actions*** .
9. Click **Apply**.

6.2.2 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**.



□Enable Object Removal Det...

Arming Area: 1

Time Thres...5 — 3600: 5

Sensitivity 1 — 100: 50

Figure 6-4 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**.

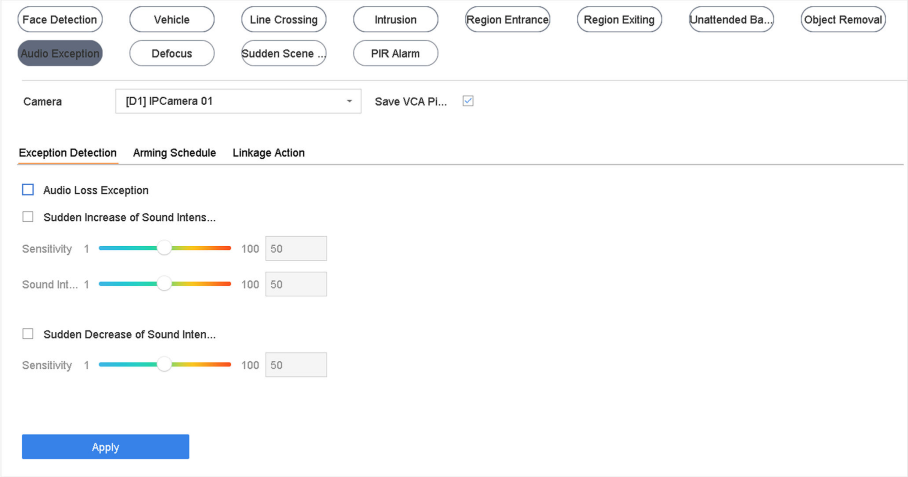
6.2.3 Audio Exception Detection

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**.



Camera [D1] IPCamera 01 Save VCA Pi... ☑

□ Audio Loss Exception

□ Sudden Increase of Sound Intens...

Sensitivity 1 100 50

Sound Int... 1 100 50

□ Sudden Decrease of Sound Inten...

Sensitivity 1 100 50

Figure 6-5 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].

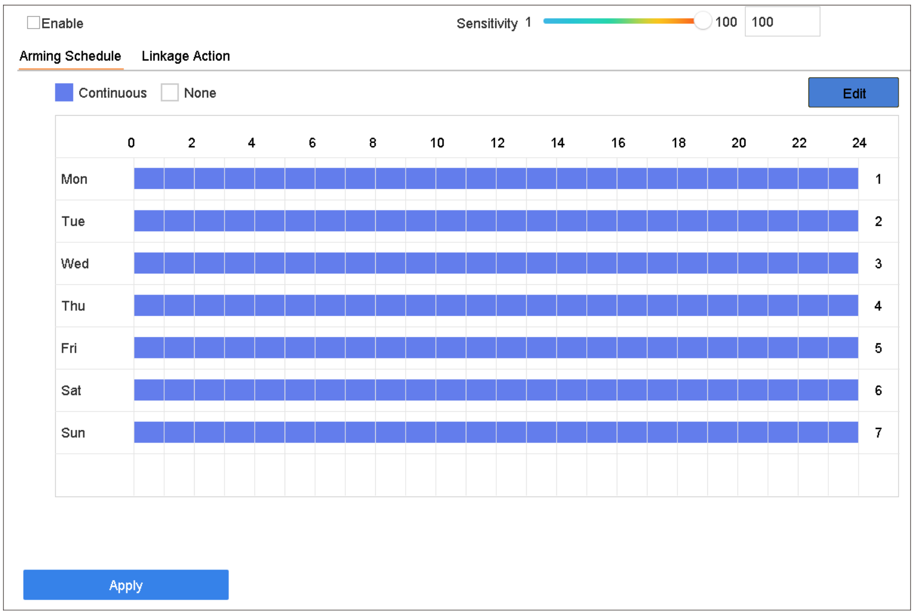
6. Set the arming schedule. Refer to ***Configure Arming Schedule*** .
7. Set the linkage actions. Refer to ***Configure Linkage Actions*** .
8. Click **Apply**.

6.2.4 Defocus Detection

Image blur caused by lens defocus can be detected.

Steps

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



□Enable

Sensitivity 1 100 100

Figure 6-6 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*** .

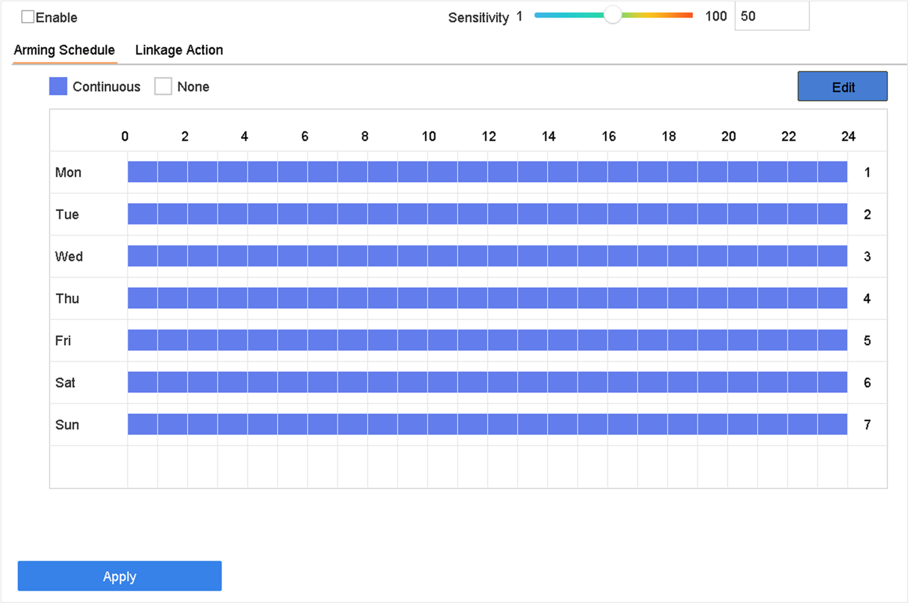
8. Set the linkage actions. Refer to ***Configure Linkage Actions*** .
9. Click **Apply**.

6.2.5 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**.



☐ Enable

Sensitivity 1 — 100 50

Figure 6-7 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**.

6.2.6 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**.

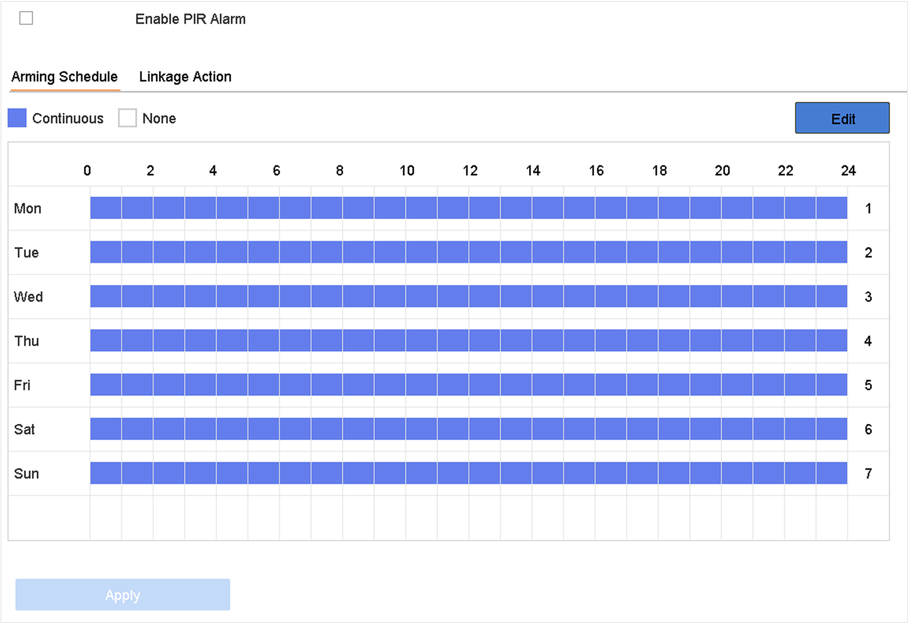


Figure 6-8 PIR Alarm

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**.

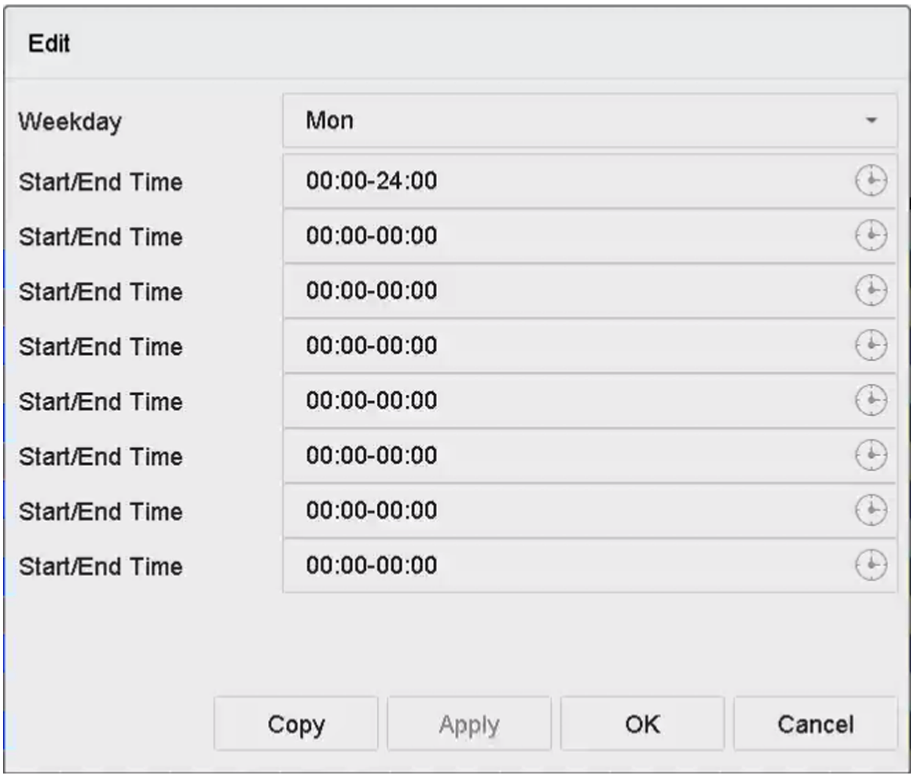
6.3 Configure Arming Schedule

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.



Edit

Weekday: Mon

Start/End Time: 00:00-24:00

Start/End Time: 00:00-00:00

Start/End Time: 00:00-00:00

Start/End Time: 00:00-00:00

Start/End Time: 00:00-00:00

Start/End Time: 00:00-00:00

Start/End Time: 00:00-00:00

Start/End Time: 00:00-00:00

Figure 6-9 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.

6.4 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.

6.4.1 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 → Live 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.

6.4.2 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.

6.4.3 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**.

6.4.4 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.

6.4.5 Trigger Alarm Output

The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.

Steps

1. Go to **Linkage Action** interface of the alarm detection (e.g., motion detection, face detection, line crossing detection, intrusion detection, etc.).
2. In **Trigger Alarm Outputs** Area, Select the alarm output (s) to trigger.
3. Go to **System → Event → Normal Event → Alarm Output** .
4. Select an alarm output item from the list.

6.4.6 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.

6.4.7 Configure Audio and Light Alarm Linkage

For certain cameras, you can set the alarm linkage action as audio alarm or light alarm.

Before You Start

- Ensure your camera supports audio and light alarm linkage.
- Ensure the audio output and volume are properly configured.

Steps

1. Go to the linkage action interface of the alarm detection (e.g., motion detection).
2. Set **Audio and Light Alarm Linkage** as your desire.
3. Click **Apply**.

Note

You can use Hik-Connect to record customized voice messages, and send voice messages to cameras. The customized voice messages can be used for audio linkage.

Chapter 7 File Management

7.1 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.

7.2 Export Files

Export files for backup purposes to a USB device, or eSATA HDD.

Steps

1. Search files. Refer to ***Search Files*** for details.
2. Select files.
3. Click **Export**.
4. **Optional:** For vehicle files, check **Backup License Plate Statistics Info** to export license plate statistics information later.
5. Select the file to export as **Video and log** and click **OK**.
6. Select the backup device and folder path.
7. Click **OK**.

7.3 Smart Search

You can search human body files, face files and vehicles in **File Management → Smart Search** . Refer to ***Human Body Search Face Picture Search*** , and ***Vehicle Search*** for details.

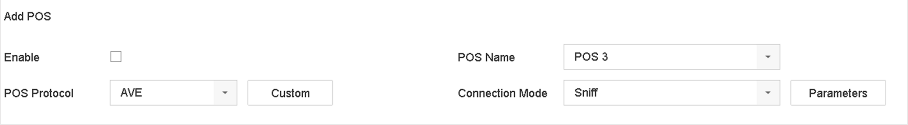
Chapter 8 POS Configuration

The device can be connected to a POS machine/server, and receive a transaction message to overlay on the image during Live View or playback, as well as trigger a POS event alarm.

8.1 Configure POS Connection

Steps

1. Go to **System → POS** .
2. Click **Add**.



Add POS

Enable □

POS Name POS 3

POS Protocol AVE

Connection Mode Sniff

Figure 8-1 POS Settings

3. Select a POS device from the drop-down list.
4. Check **Enable**.

Note

The number of POS devices supported by each device is the half of its number of channel, e.g., 8 POS devices are supported for the DS-9616NI-I8 model.

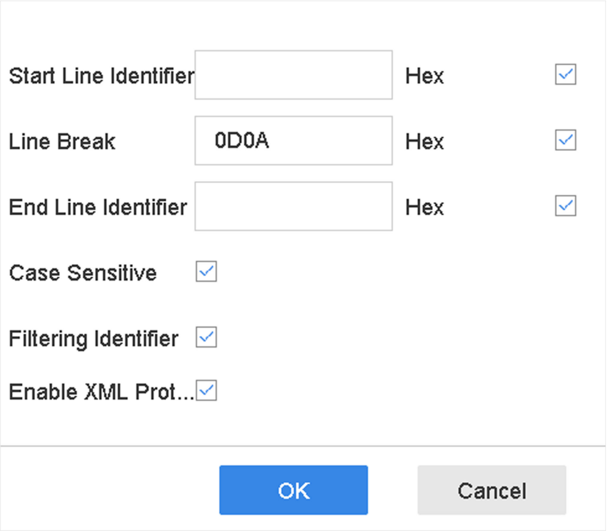
5. Select **POS Protocol**.

Note

When a new protocol is selected, reboot the device to activate the new settings.

Universal Protocol

Click **Advanced** to expand more settings when selecting the universal protocol. You can set the start line identifier, line break tag, and end line tag for the POS overlay characters, and the case-sensitive property of the characters. You can also optionally check the filtering identifier and the XML protocol.



Start Line Identifier Hex ☑

Line Break 0D0A Hex ☑

End Line Identifier Hex ☑

Case Sensitive ☑

Filtering Identifier ☑

Enable XML Prot... ☑

Figure 8-2 Universal Protocol Settings

EPSON

The fixed start and end line tag are used for EPSON protocol.

AVE

The fixed start and end line tag are used for AVE protocol. Serial port and virtual serial port connection types are supported.

Click **Custom** to configure the AVE settings. Select **Rule** as **VSI-ADD** or **VNET** . Set the address bit of the POS message to send. Click **OK** to save the settings.

NUCLEUS

Click the **Custom** to configure the NUCLEUS settings.

Enter the employee No., shift No., and the terminal No. in the field. The matching message sent from the POS device will be used as the valid POS data.

Note

The NUCLEUS protocol must be used in the RS-232 connection communication.

6. Select **Connection Mode** and click **Parameters** to configure the parameters for each connection mode.

TCP Connection

When using TCP connection, the port must be set from 1 to 65535, and the port for each POS machine must be unique.

Set the **Allowed Remote IP Address** of the device sending the POS message.

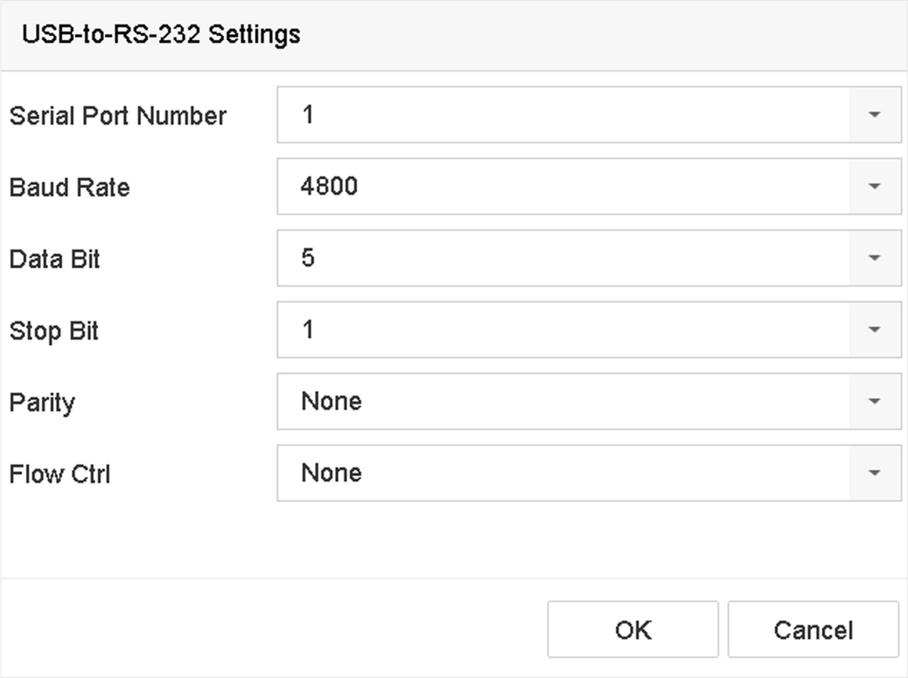
UDP Connection

When using UDP connection, the port must be set from 1 to 65535, and the port for each POS machine must be unique.

Set the **Allowed Remote IP Address** of the device sending the POS message.

USB-to-RS-232 Connection

Configure the USB-to-RS-232 convertor port parameters, including the port serial number, baud rate, data bit, stop bit, parity, and flow ctrl.



USB-to-RS-232 Settings

Serial Port Number	1
Baud Rate	4800
Data Bit	5
Stop Bit	1
Parity	None
Flow Ctrl	None

Figure 8-3 USB-to-RS-232 Settings

RS-232 Connection

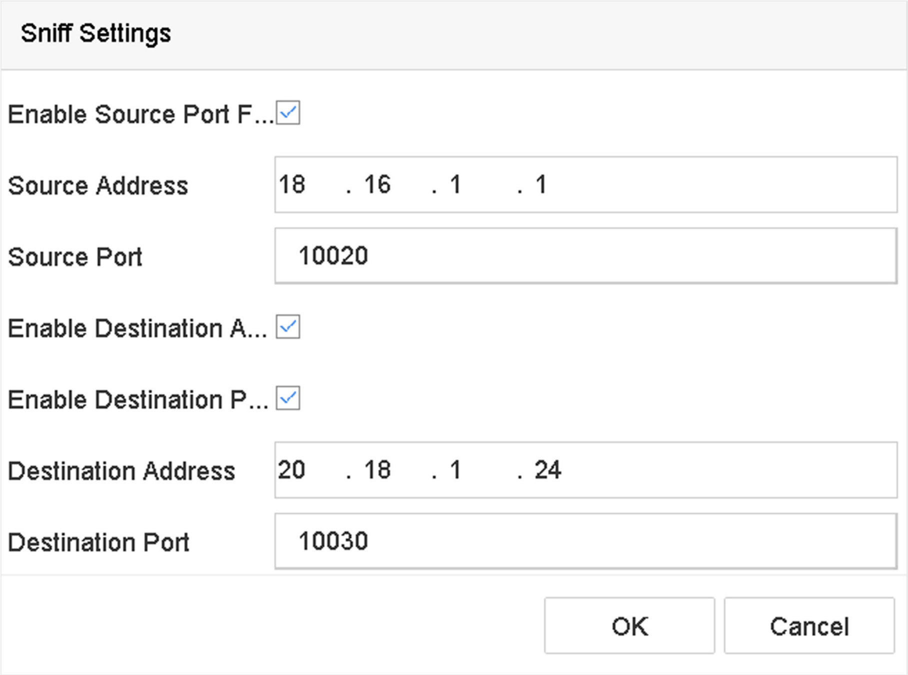
Connect the device and the POS machine via RS-232. The RS-232 settings can be configured in **Menu → Configuration → RS-232** . The Usage must be set to Transparent Channel.

Multicast Connection

When connecting the device and the POS machine via Multicast protocol, set the multicast address and port.

Sniff Connection

Connect the device and the POS machine via Sniff. Configure the source address and destination address settings.



Sniff Settings

Enable Source Port F... ☑

Source Address: 18 . 16 . 1 . 1

Source Port: 10020

Enable Destination A... ☑

Enable Destination P... ☑

Destination Address: 20 . 18 . 1 . 24

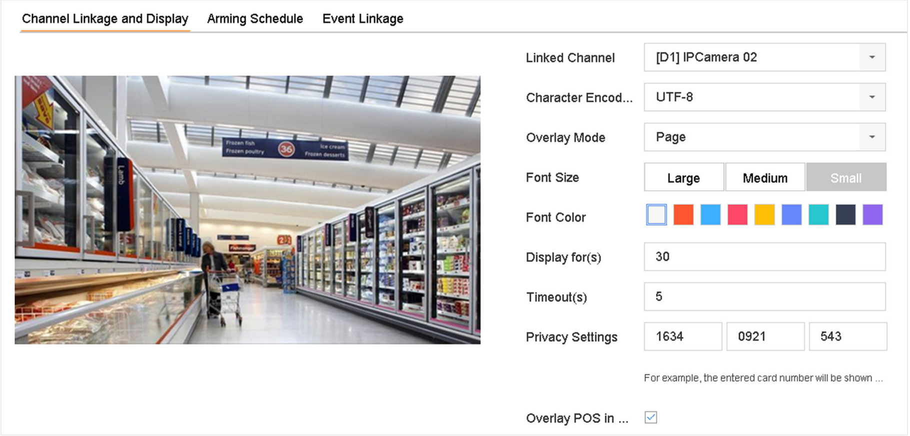
Destination Port: 10030

Figure 8-4 Sniff Settings

8.2 Configure POS Text Overlay

Steps

1. Go to **System → POS** .
2. Click **Channel Linkage and Display**.



Linked Channel: [D1] IPCamera 02

Character Encod...: UTF-8

Overlay Mode: Page

Font Size: Large | Medium | Small

Font Color: □ 🟥 🟦 🟥 🟨 🟦 🟦 ⬛ 🟪

Display for(s): 30

Timeout(s): 5

Privacy Settings: 1634 | 0921 | 543

For example, the entered card number will be shown ...

Overlay POS in ... ☑

Figure 8-5 Overlay Character Settings

3. Select **linked channel** to overlay the POS characters.
4. Set the characters overlay for the enabled POS.
   - Character encoding format: currently the Latin-1 format is available
   - Overlay mode of the characters to display in scrolling or page mod

- Font size and font color
- Display time (sec) of the characters. The value ranges 5 -3600 sec.
- Timeout of POS event. The value ranges 5 -3600 sec. When the device has not received the POS message within the defined time, the transaction ends.

5. In **Privacy Settings**, set the POS privacy information to not display on the image, e.g., the card number, user name, etc.

   The defined privacy information will be displayed using ***on the image instead.
6. Check **Overlay POS in Live View**. When this feature is enabled, the POS information is overlaid on the Live View image.

   Note

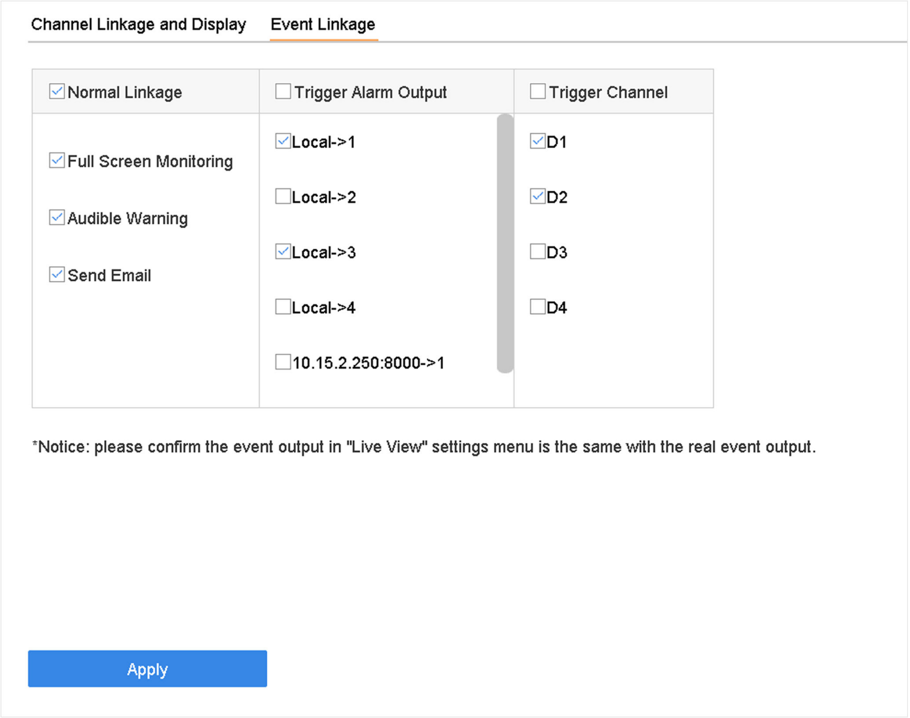
   Drag the frame to adjust the textbox size and position on POS settings interface preview screen.
7. Click **Apply** to activate the settings.

8.3 Configure POS Alarm

A POS event can trigger channels to start recording, or trigger full screen monitoring or an audio warning, notifying the surveillance center, send e-mail, etc.

Steps

1. Go to **Storage → Recording Schedule** .
2. Set the POS event's arming schedule.
3. Go to **System → POS** .
4. Click **Event Linkage** on the POS adding or editing interface.



☑ Normal Linkage	□ Trigger Alarm Output	□ Trigger Channel
☑ Full Screen Monitoring	☑ Local->1	☑ D1
☑ Audible Warning	□ Local->2	☑ D2
☑ Send Email	☑ Local->3	□ D3
	□ Local->4	□ D4
	□ 10.15.2.250:8000->1	

*Notice: please confirm the event output in "Live View" settings menu is the same with the real event output.

Figure 8-6 Set Trigger Cameras of POS

5. Select the normal linkage actions.
6. Select one or more alarm output(s) to trigger.
7. Select one or more channels to record or become full-screen monitoring when a POS alarm is triggered.
8. Click **Apply** to save the settings.

Chapter 9 Storage

9.1 Storage Device Management

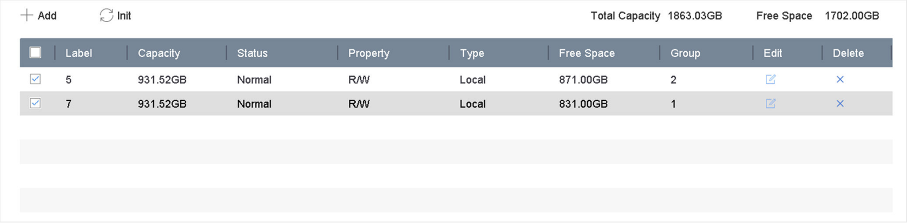
9.1.1 Manage Local HDD

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.

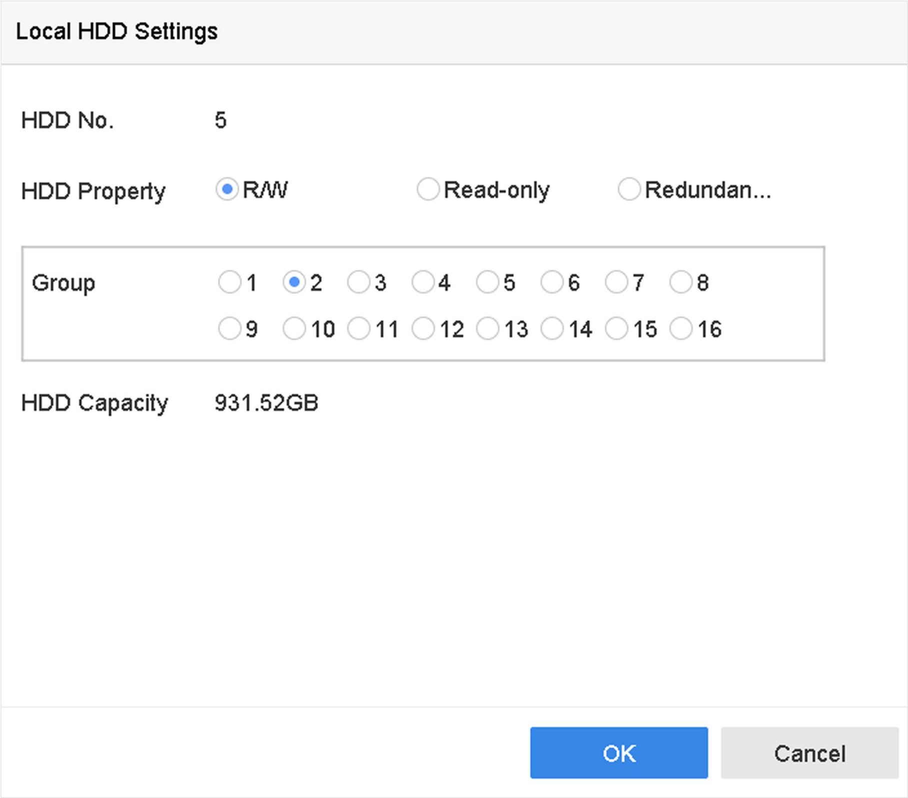


Total Capacity 1863.03GB Free Space 1702.00GB

□	Label	Capacity	Status	Property	Type	Free Space	Group	Edit	Delete
☑	5	931.52GB	Normal	R/W	Local	871.00GB	2	✎	×
☑	7	931.52GB	Normal	R/W	Local	831.00GB	1	✎	×

Figure 9-1 Storage Device

6. Click ✎ to enter Local HDD Settings interface.



Local HDD Settings

HDD No. 5

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

Group ○ 1 ● 2 ○ 3 ○ 4 ○ 5 ○ 6 ○ 7 ○ 8 ○ 9 ○ 10 ○ 11 ○ 12 ○ 13 ○ 14 ○ 15 ○ 16

HDD Capacity 931.52GB

Figure 9-2 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**.

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**.

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

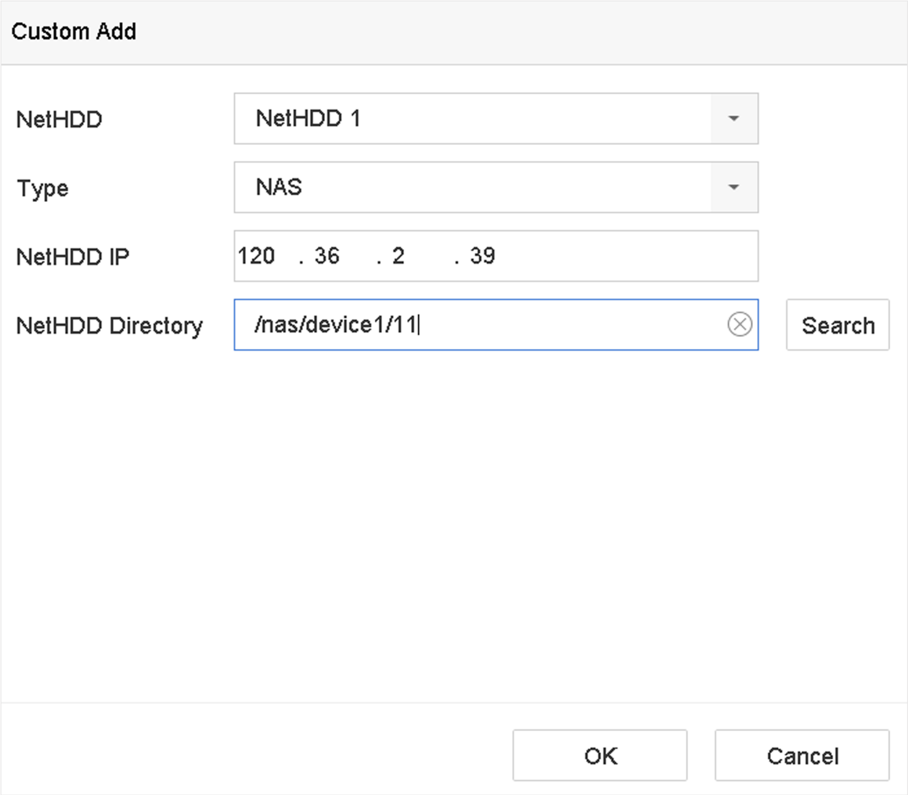
- When the quota capacity is set to 0, all cameras will use the total capacity of HDD for videos and pictures.
- Reboot the video recorder to activate the new settings.

9.1.2 Add a Network Disk

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

Steps

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



Custom Add

NetHDD: NetHDD 1

Type: NAS

NetHDD IP: 120 . 36 . 2 . 39

NetHDD Directory: /nas/device1/11

Figure 9-3 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**.

9.1.3 Manage eSATA

Configure eSATA for Data Storage

When there is an external eSATA device connected to your video recorder, you can configure the eSATA usage as data storage and manage the eSATA.

Steps

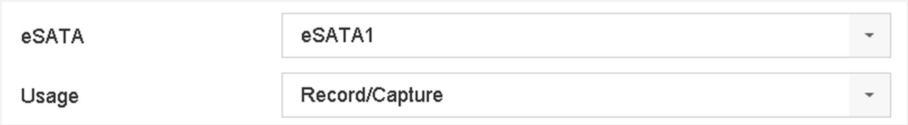
1. Go to **Storage → Advanced** .
2. Select eSATA **Usage** as **Export** or **Record/Capture**.

   Export

   Use the eSATA for backup.

Record/Capture

Use the eSATA for record/capture. Refer to the following steps for operating instructions.



eSATA	eSATA1
Usage	Record/Capture

Figure 9-4 eSATA Mode

What to do next

If eSATA usage is set as **Record/Capture**, enter the storage device interface to edit its property or initialize it.

Configure eSATA for Auto Backup

If you made an automatic backup plan, the video recorder will back up the local videos of 24 hours ahead of the backup start time to eSATA.

Before You Start

Ensure the device has correctly connected with an external eSATA hard drive, and its usage type is set as **Export**. Refer to ***Manage eSATA*** for details.

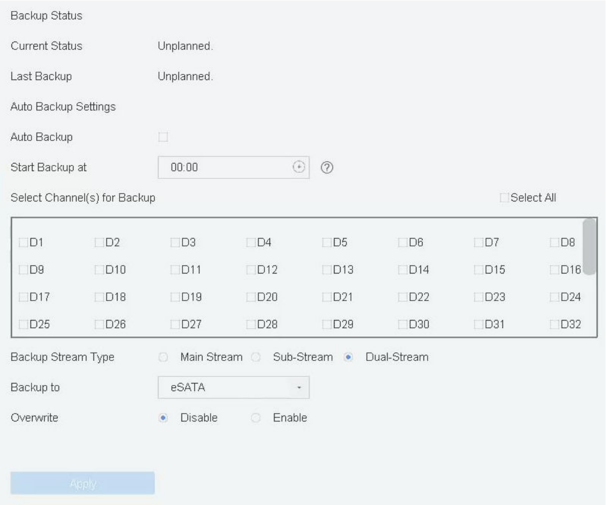
Steps

1. Go to **Storage → Auto Backup** .
2. Check **Auto Backup**.
3. Set the backup start time in **Start Backup at**.

Note

If the day experiences a failed backup, the video recorder will back up the videos 48 hours ahead of the backup start time in the next day.

4. Select channels for backup.
5. Select **Backup Stream Type** as your desire.
6. Select **Overwrite** type.
   - **Disable**: When HDD is full, it will stop writing.
   - **Enable**: When HDD is full, it will continue to write new files by deleting the oldest files.
7. Click **Apply**.



Backup Status

Current Status Unplanned.

Last Backup Unplanned.

Auto Backup Settings

Auto Backup □

Start Backup at 00:00

Select Channel(s) for Backup □Select All

□D1	□D2	□D3	□D4	□D5	□D6	□D7	□D8
□D9	□D10	□D11	□D12	□D13	□D14	□D15	□D16
□D17	□D18	□D19	□D20	□D21	□D22	□D23	□D24
□D25	□D26	□D27	□D28	□D29	□D30	□D31	□D32

Backup Stream Type ○ Main Stream ○ Sub-Stream ● Dual-Stream

Backup to eSATA

Overwrite ● Disable ○ Enable

Figure 9-5 Configure eSATA for Auto Backup

9.2 Disk Array

A disk array is a data storage virtualization technology that combines multiple physical disk drives into a single logical unit. Also known as a "RAID", an array stores data over multiple HDDs to provide enough redundancy so that data can be recovered if one disk fails. Data is distributed across the drives in one of several ways called "RAID levels", based the redundancy and performance required.

9.2.1 Create a Disk Array

The video recorder supports software-based disk arrays. Enable the RAID function as required, and ensure each HDD capacity is not less than 4 TB. Two ways are available for creating an array: one-touch configuration and manual configuration.

One-Touch Creation

One-touch configuration creates the disk array. By default, the array type created by one-touch configuration is RAID 5.

Before You Start

Install at least 3 HDDs. If more than 10 HDDs are installed, 2 arrays will be created. To maintain reliability and stability running of the HDDs, it is recommended to use of enterprise-level HDDs of the same model and capacity.

Steps

1. Go to **Storage → Advanced** .
2. Check **Enable RAID**.

3. Click **Apply** and reboot the device to have settings take effect.
4. After reboot, go to **Storage → RAID Setup → Physical Disk** .
5. Click **One-touch Config**.
6. Edit **Array Name** and click **OK** to start configuring.

Note

If you install 4 or more HDDs, a hot spare disk for array rebuilding will be created.

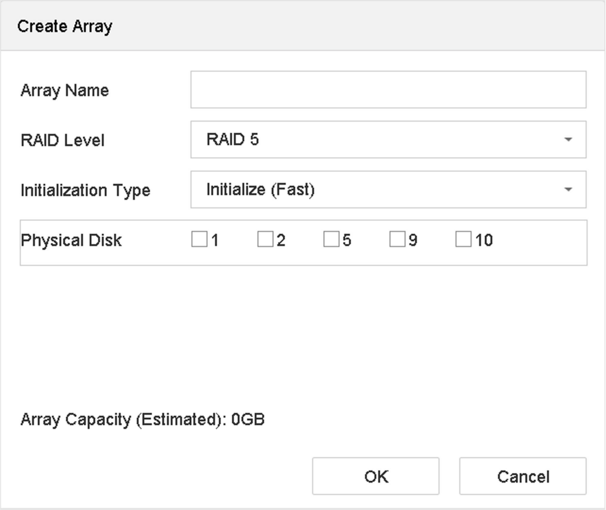
7. **Optional:** The video recorder will automatically initialize the created array. Go to **Storage → RAID Setup → Array** to view the information of the created array.

Manual Creation

Manually create a RAID 0, RAID 1, RAID 5, RAID 6, or RAID 10 array.

Steps

1. Go to **Storage → Advanced** .
2. Check **Enable RAID**.
3. Click **Apply** and reboot the device to have settings take effect.
4. After reboot, go to **Storage → RAID Setup → Physical Disk** .
5. Click **Create**.



Create Array

Array Name

RAID Level: RAID 5

Initialization Type: Initialize (Fast)

Physical Disk: □1 □2 □5 □9 □10

Array Capacity (Estimated): 0GB

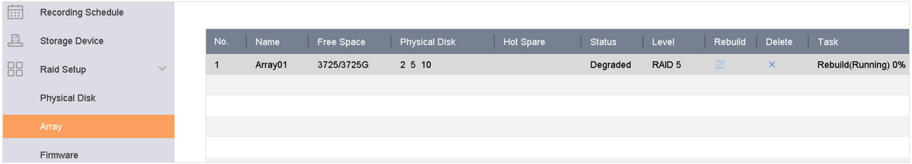
Figure 9-6 Create Array

6. Enter **Array Name**.
7. Select **RAID Level** as required.
8. Select the physical disks to constitute the array.

Table 9-1 The Required Number of HDDs

RAID Level	The Required Number of HDDs
RAID 0	At least 2 HDDs.
RAID 1	At least 2 HDDs.
RAID 5	At least 3 HDDs.
RAID 6	At least 4 HDDs.
RAID 10	The number of HDD must be an even ranges from 4 to 16.

9. Click **OK**.
10. **Optional:** The video recorder will automatically initialize the created array. Go to **Storage → RAID Setup → Array** to view the information of the created array.



No.	Name	Free Space	Physical Disk	Hot Spare	Status	Level	Rebuild	Delete	Task
1	Array01	3725/3725G	2 5 10		Degraded	RAID 5	✎	×	Rebuild(Running) 0%

Figure 9-7 Array List

9.2.2 Rebuild an Array

The array status includes Functional, Degraded, and Offline. To ensure the high security and reliability of the data stored in an array, take immediate and proper maintenance of the arrays according its status.

Functional

No disk loss in the array.

Offline

The number of lost disks has exceeded the limit.

Degraded

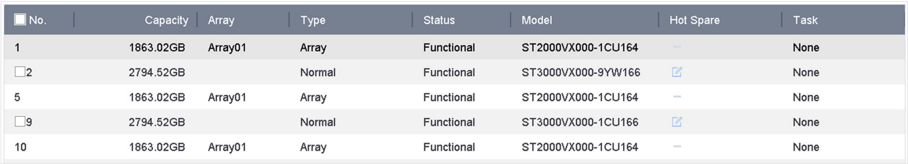
If any HDD fails in the array, the array degrades. Restore it to Functional status by rebuilding the array.

Configure a Hot Spare Disk

The hot spare disk is required for the disk array automatic rebuilding.

Steps

1. Go to **Storage → RAID Setup → Physical Disk** .



□ No.	Capacity	Array	Type	Status	Model	Hot Spare	Task
1	1863.02GB	Array01	Array	Functional	ST2000VX000-1CU164	—	None
□2	2794.52GB		Normal	Functional	ST3000VX000-9YW166	✎	None
5	1863.02GB	Array01	Array	Functional	ST2000VX000-1CU164	—	None
□9	2794.52GB		Normal	Functional	ST3000VX000-1CU166	✎	None
10	1863.02GB	Array01	Array	Functional	ST2000VX000-1CU164	—	None

Figure 9-8 Physical Disk

2. Click ✎ of an available HDD to set it as the hot spare disk.

Automatically Rebuild an Array

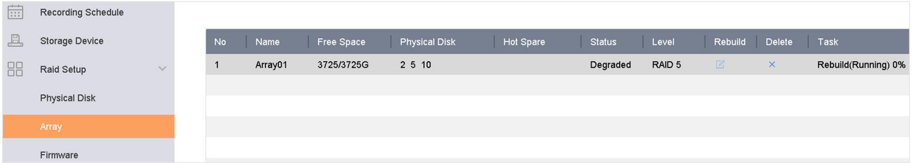
The video recorder can automatically rebuild degraded arrays with the hot spare disks.

Before You Start

Create hot spare disks. For details, refer to ***Configure a Hot Spare Disk*** .

Steps

1. Go to **Storage → RAID Setup → Array** .



No	Name	Free Space	Physical Disk	Hot Spare	Status	Level	Rebuild	Delete	Task
1	Array01	3725/3725G	2 5 10		Degraded	RAID 5	✎	×	Rebuild(Running) 0%

Figure 9-9 Array List

Manually Rebuild an Array

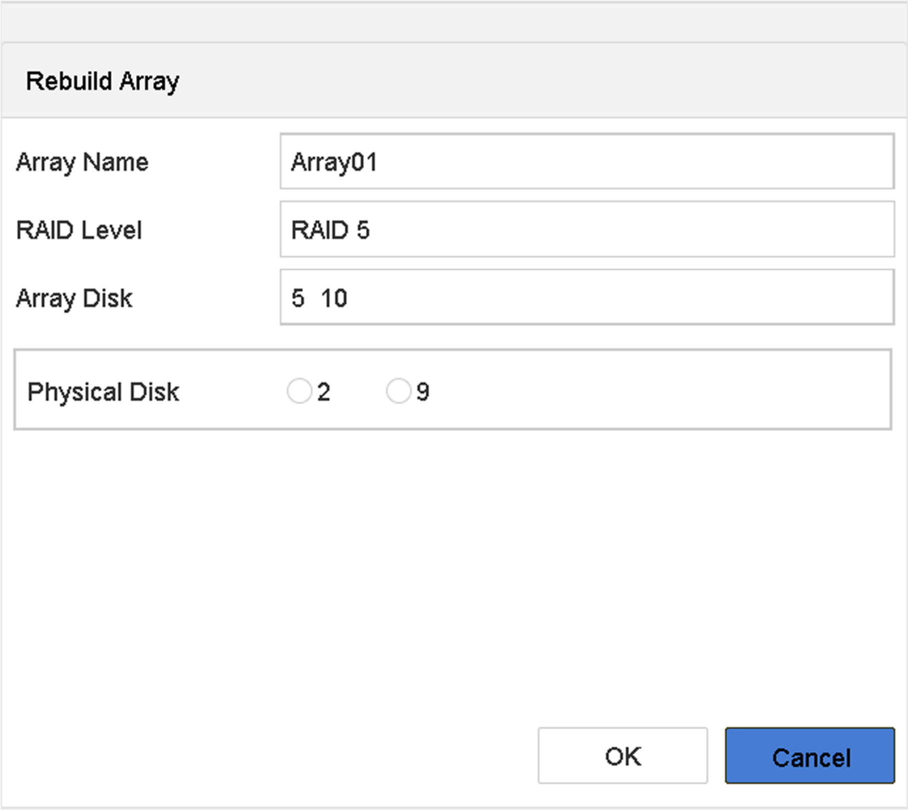
If no hot spare disks are configured, rebuild a degraded array manually.

Before You Start

At least one available physical disk must exist to rebuild an array.

Steps

1. Go to **Storage → RAID Setup → Array** .
2. Click ✎ of the degraded array.



Rebuild Array

Array Name: Array01

RAID Level: RAID 5

Array Disk: 5 10

Physical Disk ○ 2 ○ 9

Figure 9-10 Rebuild Array

3. Select the available physical disk.
4. Click **OK**.
5. Click **OK** on the pop up message box "Do not unplug the physical disk when it is under rebuilding."

Chapter 10 Network Settings

10.1 Configure DDNS

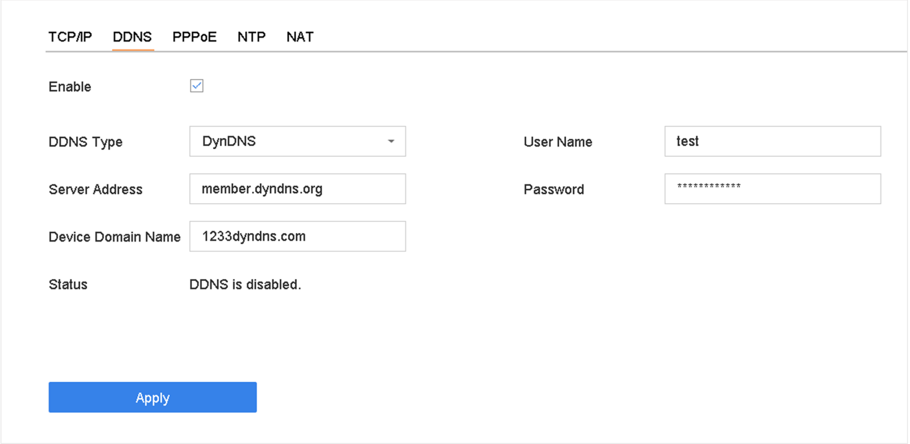
You can set Dynamic DNS service for network access. Different DDNS modes are available: DynDNS, PeanutHull, and NO-IP.

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**



Enable	☑		
DDNS Type	DynDNS	User Name	test
Server Address	member.dyndns.org	Password	************
Device Domain Name	1233dyndns.com		
Status	DDNS is disabled.		

Figure 10-1 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**.

10.2 Configure PPPoE

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

Contact your Internet service provider for details about PPPoE service.

10.3 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.

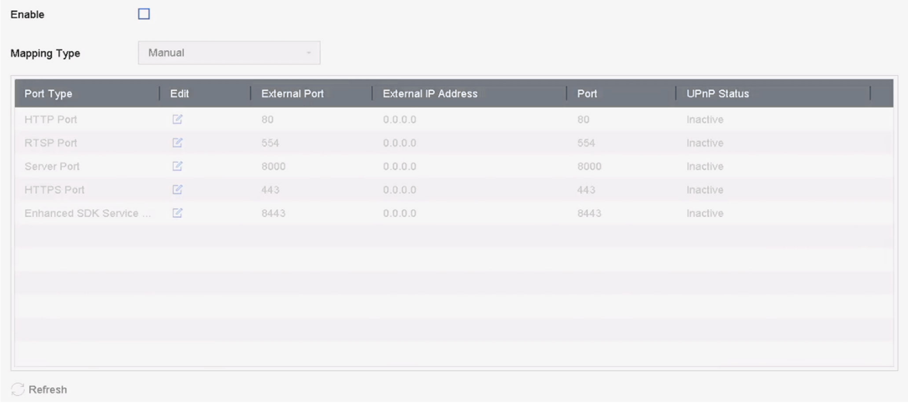
Before You Start

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 **System → Network → TCP/IP → NAT** .



Enable □

Mapping Type: Manual

Port Type	Edit	External Port	External IP Address	Port	UPnP Status
HTTP Port	✎	80	0.0.0.0	80	Inactive
RTSP Port	✎	554	0.0.0.0	554	Inactive
Server Port	✎	8000	0.0.0.0	8000	Inactive
HTTPS Port	✎	443	0.0.0.0	443	Inactive
Enhanced SDK Service ...	✎	8443	0.0.0.0	8443	Inactive

Figure 10-2 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

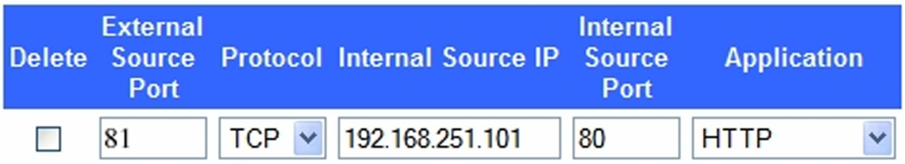
- You can use the default port No., or change it according to actual requirements.
- External Port indicates the port No. for port mapping in the router.
- The value of the RTSP port No. should be 554 or between 1024 and 65535, while the value of the other ports should be between 1 and 65535 and the 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.



Delete	External Source Port	Protocol	Internal Source IP	Internal Source Port	Application
□	81	TCP	192.168.251.101	80	HTTP

Figure 10-3 Set Virtual Server Item

10.4 Configure Wi-Fi

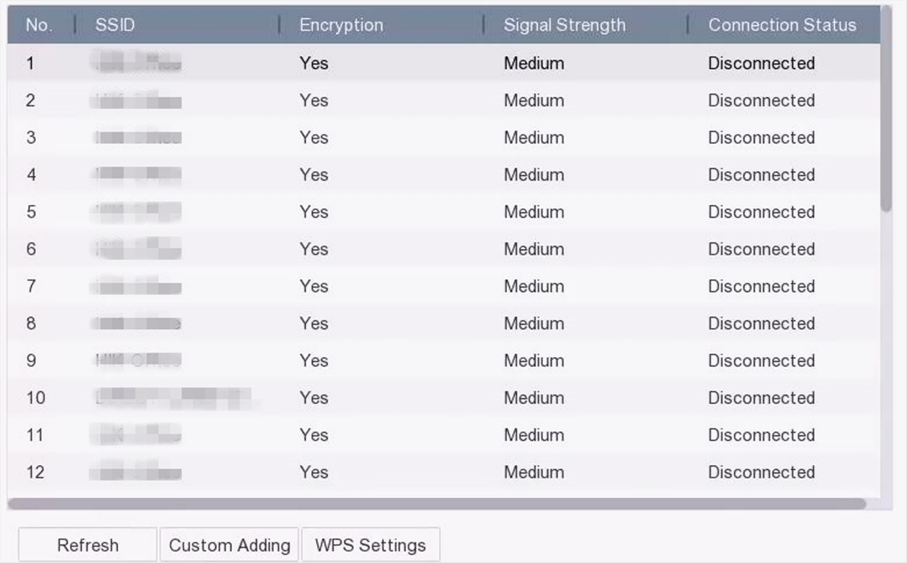
You can use a Wi-Fi dongle to connect your device to a wireless network.

Before You Start

Prepare a suitable Wi-Fi dongle, and insert it in to the USB interface at the rear panel.

Steps

1. Go to **System → Network → TCP/IP → Wi-Fi** .



No.	SSID	Encryption	Signal Strength	Connection Status
1	[redacted]	Yes	Medium	Disconnected
2	[redacted]	Yes	Medium	Disconnected
3	[redacted]	Yes	Medium	Disconnected
4	[redacted]	Yes	Medium	Disconnected
5	[redacted]	Yes	Medium	Disconnected
6	[redacted]	Yes	Medium	Disconnected
7	[redacted]	Yes	Medium	Disconnected
8	[redacted]	Yes	Medium	Disconnected
9	[redacted]	Yes	Medium	Disconnected
10	[redacted]	Yes	Medium	Disconnected
11	[redacted]	Yes	Medium	Disconnected
12	[redacted]	Yes	Medium	Disconnected

Figure 10-4 Connect to a Wireless Network

2. Check **Enable Wi-Fi**.
3. Connect to a wireless network.

Connect to an Automatically Searched Wireless Network

a. Double click the wireless network from the list as you desired.
b. Set wireless network parameters.
c. Click **OK**.

Connect to a Customized Wireless Network

a. Click **Custom Adding**.
b. Set wireless network parameters.
c. Click **OK**.

Connect to a Wireless Network with WPS (Wi-Fi Protected Setup)

a. Click **WPS Settings**.
b. Check **Enable WPS**.
c. Set wireless network parameters.
d. Click **Apply**.

After connecting to an available wireless network, you can view the connection result in **Connection Status**.

4. Go to **System → Network → TCP/IP → TCP/IP** .
5. Set **Select NIC** and **Default Route** as **WLAN0**.
6. Set other network parameters.
7. Click **Apply**.

10.5 Configure SNMP

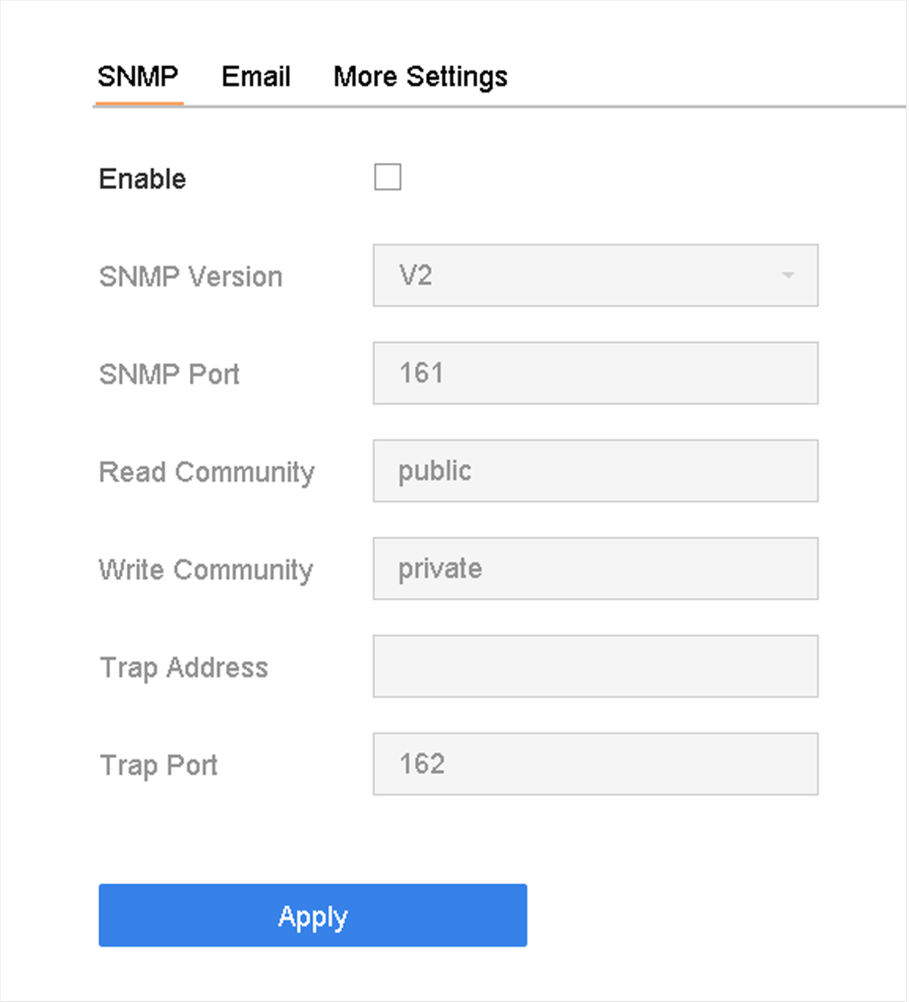
You can configure SNMP settings to get device status and parameter information.

Before You Start

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

Steps

1. Go to **System → Network → Advanced → SNMP** .



Enable ☐

SNMP Version V2

SNMP Port 161

Read Community public

Write Community private

Trap Address

Trap Port 162

Figure 10-5 SNMP Settings

2. Check **Enable**. A message will pop up to notify about a possible security risk. Click **Yes** to continue.
3. Configure the SNMP settings as needed.

   Trap Address

      SNMP host IP address.

   Trap Port

      Port of the SNMP host.
4. Click **Apply**.

10.6 Configure Email

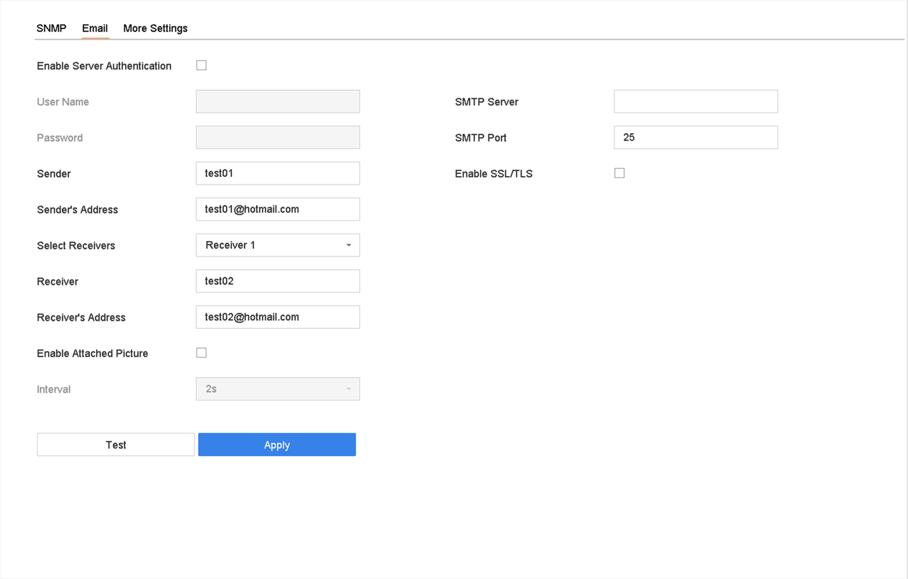
The system can be configured to send an e-mail notification to all designated users when a specified event occurs such as when an alarm or motion event is detected, or the administrator password is changed, etc.

Before You Start

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

Steps

1. Go to **System → Network → Advanced → Email** .



Enable Server Authentication ☐
User Name
Password
Sender test01
Sender's Address test01@hotmail.com
Select Receivers Receiver 1
Receiver test02
Receiver's Address test02@hotmail.com
Enable Attached Picture ☐
Interval 2s
SMTP Server
SMTP Port 25
Enable SSL/TLS ☐

Figure 10-6 Email Settings

2. Configure the email settings.

Enable Server Authentication

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

SMTP Server

The IP address of SMTP Server or host name (e.g., smtp.263xmail.com).

SMTP Port

The SMTP port. The default TCP/IP port used for SMTP is 25.

Enable SSL/TLS

Check to enable SSL/TLS if required by the SMTP server.

Sender

The sender's name.

Sender's Address

The sender's address.

Select Receivers

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

Receiver

The receiver's name.

Receiver's Address

The e-mail address of the user to be notified.

Enable Attached Picture

Check to send e-mail with attached alarm images. The interval is the time between sending two subsequent alarm images.

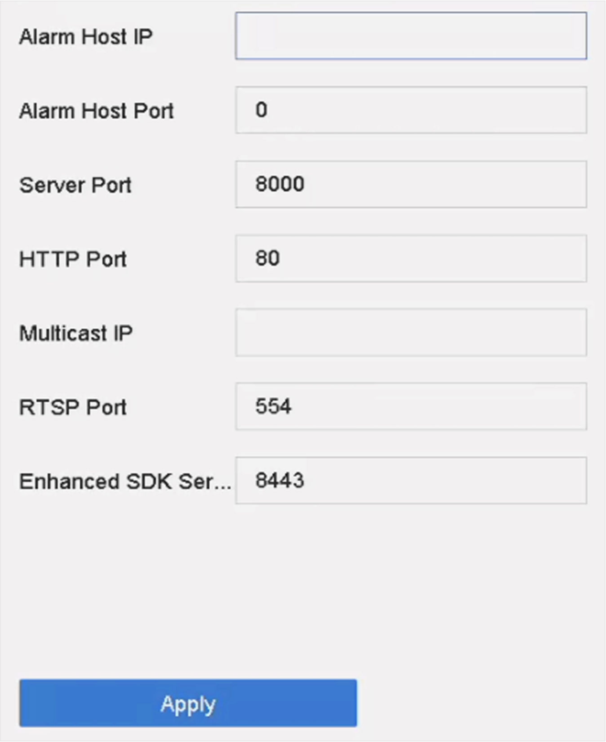
3. Click **Apply**.
4. **Optional:** Click **Test** to send a test email.

10.7 Configure Port

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

Steps

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



Alarm Host IP	
Alarm Host Port	0
Server Port	8000
HTTP Port	80
Multicast IP	
RTSP Port	554
Enhanced SDK Ser...	8443

Figure 10-7 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**.

10.8 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 **Maintenance → 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 11 User Management and Security

11.1 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.

11.1.1 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**.

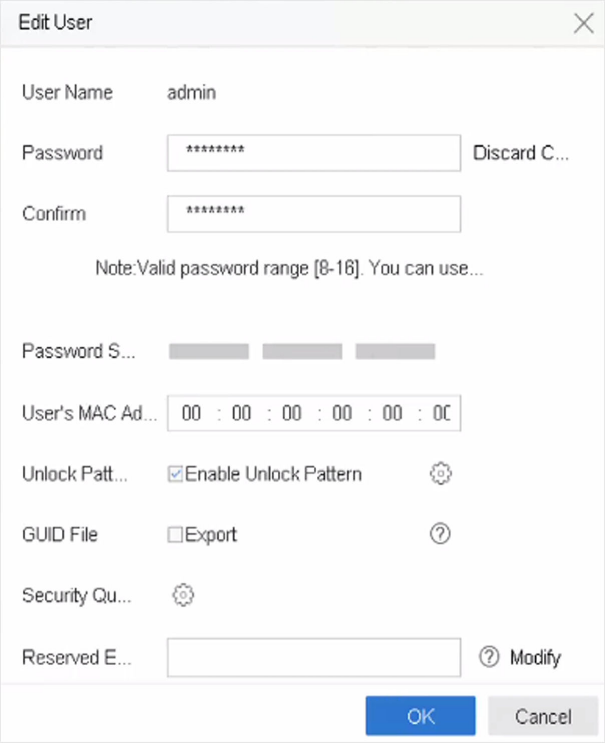
   In the User Management interface, the added new user is displayed on the list.

11.1.2 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**.



Edit User

User Name admin

Password ******** Discard C...

Confirm ********

Note:Valid password range [8-16]. You can use...

Password S...

User's MAC Ad... 00 : 00 : 00 : 00 : 00 : 0C

Unlock Patt... ☑Enable Unlock Pattern

GUID File □Export

Security Qu...

Reserved E... Modify

Figure 11-1 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 drive 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.

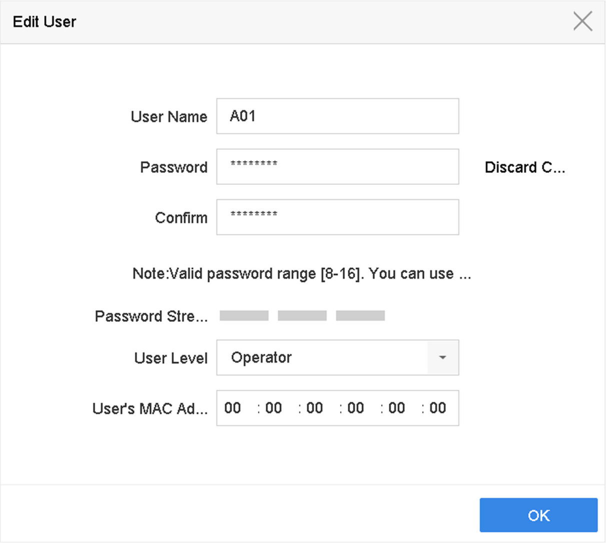
11.1.3 Edit an Operator/Guest User

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**.



Edit User

User Name: A01

Password: ********

Discard C...

Confirm: ********

Note:Valid password range [8-16]. You can use ...

Password Stre...

User Level: Operator

User's MAC Ad...: 00 : 00 : 00 : 00 : 00 : 00

OK

Figure 11-2 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**.

11.2 Manage User Permissions

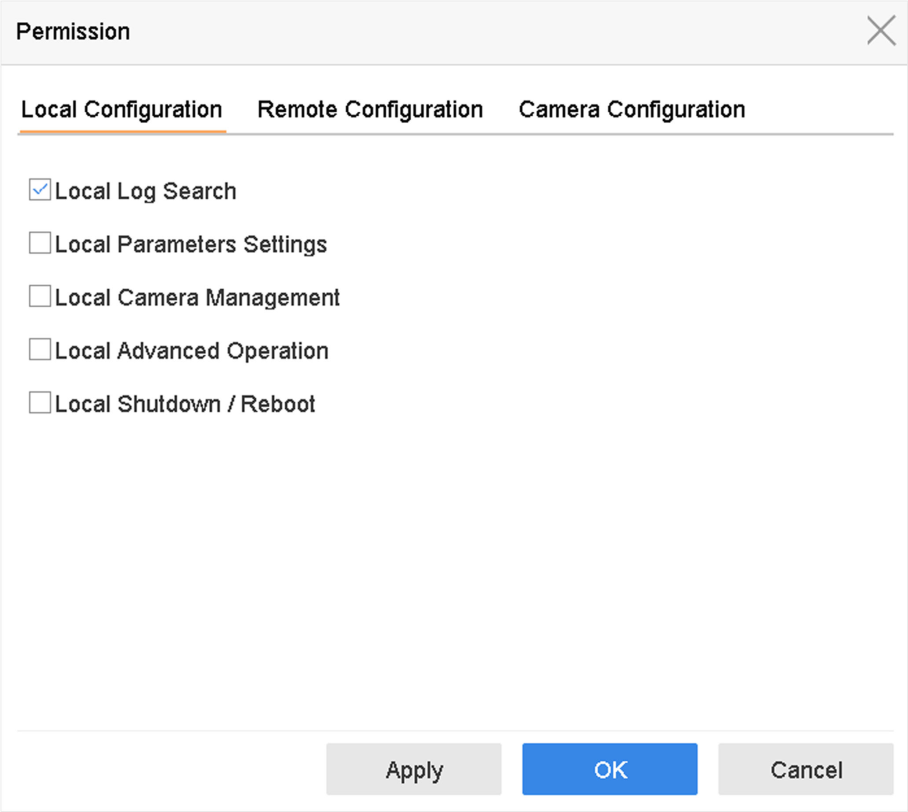
11.2.1 Set User Permissions

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.


Permission

Local Configuration | Remote Configuration | Camera Configuration

☑ Local Log Search

□ Local Parameters Settings

□ Local Camera Management

□ Local Advanced Operation

□ Local Shutdown / Reboot

Figure 11-3 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.

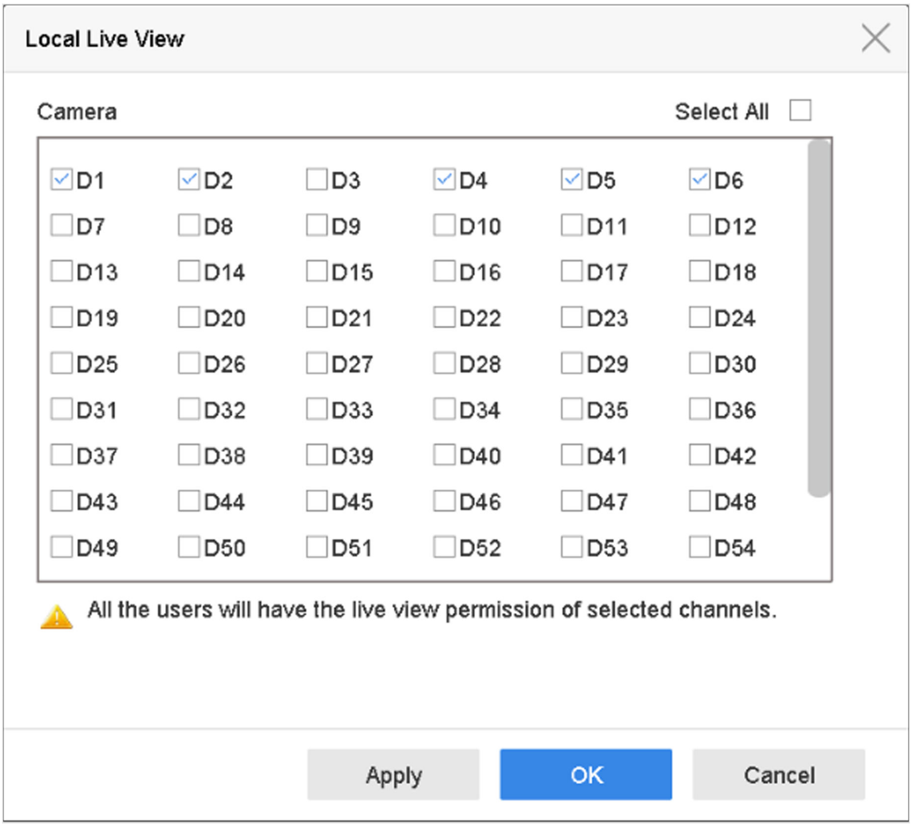
11.2.2 Set Live View Permission on Lock Screen

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**.



Local Live View

Camera   Select All □

☑D1	☑D2	□D3	☑D4	☑D5	☑D6
□D7	□D8	□D9	□D10	□D11	□D12
□D13	□D14	□D15	□D16	□D17	□D18
□D19	□D20	□D21	□D22	□D23	□D24
□D25	□D26	□D27	□D28	□D29	□D30
□D31	□D32	□D33	□D34	□D35	□D36
□D37	□D38	□D39	□D40	□D41	□D42
□D43	□D44	□D45	□D46	□D47	□D48
□D49	□D50	□D51	□D52	□D53	□D54

⚠ All the users will have the live view permission of selected channels.

Figure 11-4 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**.

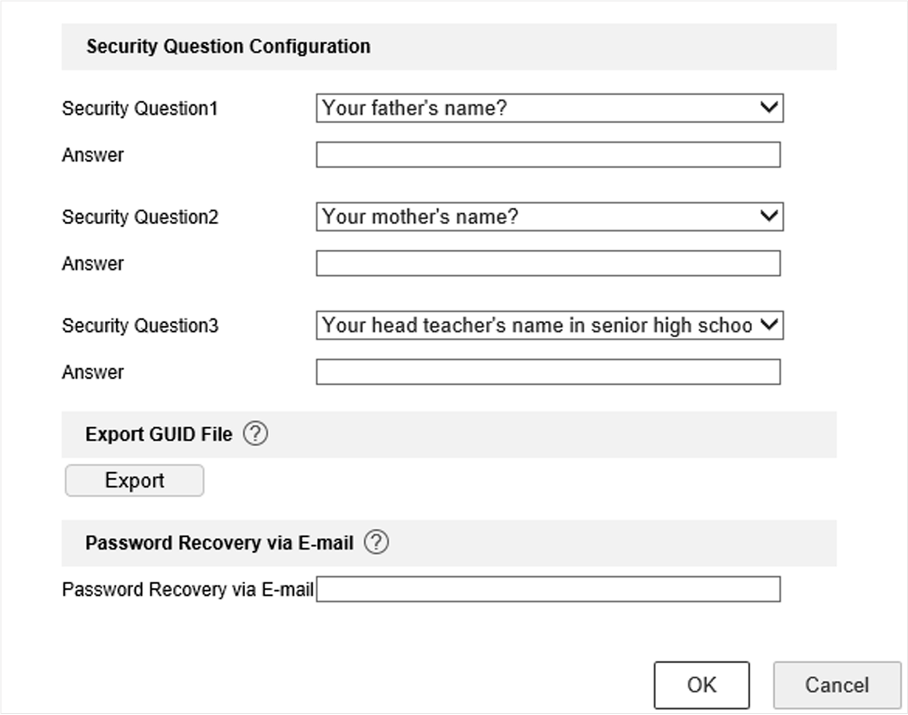
11.3 Configure Password Security

11.3.1 Export GUID File

The GUID file can help you to reset password when you forget it. You can export GUID file via web browser. Please keep the GUID file properly.

Before You Start
Ensure you are on the same network segment with your device.

Steps
1. Go to **Configuration → System → User Management → User Management** .
2. Select the admin user.
3. Click **Account Security Settings**.
4. Click **Modify**.



Security Question Configuration

Security Question1: Your father's name?

Answer

Security Question2: Your mother's name?

Answer

Security Question3: Your head teacher's name in senior high schoo

Answer

Export GUID File

Password Recovery via E-mail

Password Recovery via E-mail

Figure 11-5 Export GUID File

5. Click **Export** in **Export GUID File**.
6. Enter the admin password.
7. Save the GUID file to a directory as your desire.

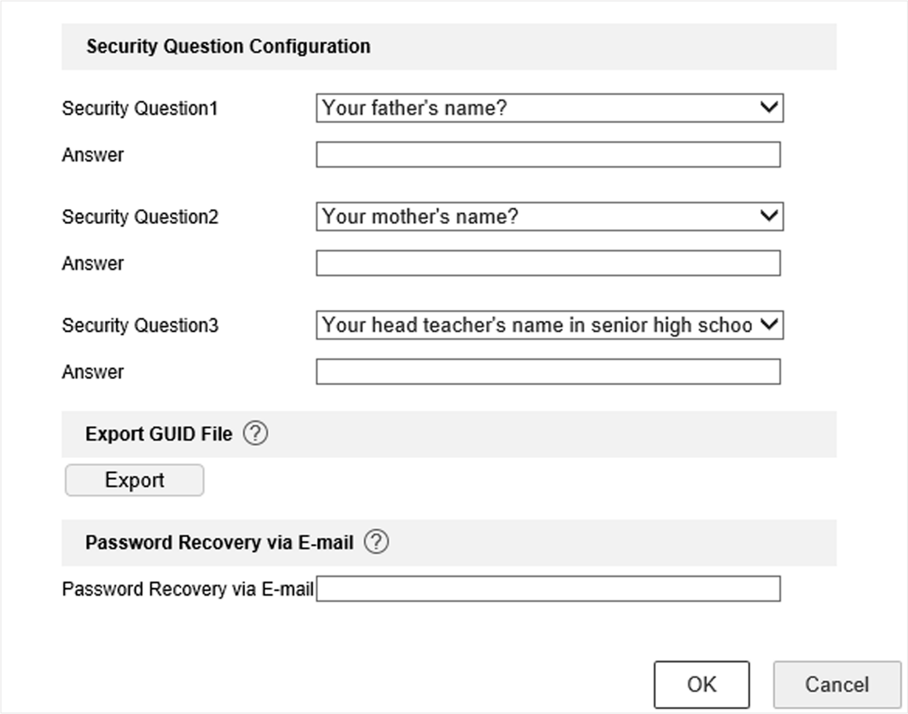
11.3.2 Configure Security Questions

The security questions can help you to reset password when you forget your password, or encounter security issues. You can configure security questions via web browser.

Before You Start
Ensure you are on the same network segment with your device.

Steps

1. Go to **Configuration → System → User Management → User Management** .
2. Select the admin user.
3. Click **Account Security Settings**.
4. Click **Modify**.



Security Question Configuration

Security Question1: Your father's name?

Answer:

Security Question2: Your mother's name?

Answer:

Security Question3: Your head teacher's name in senior high schoo

Answer:

Export GUID File

Password Recovery via E-mail

Password Recovery via E-mail:

Figure 11-6 Configure Security Questions

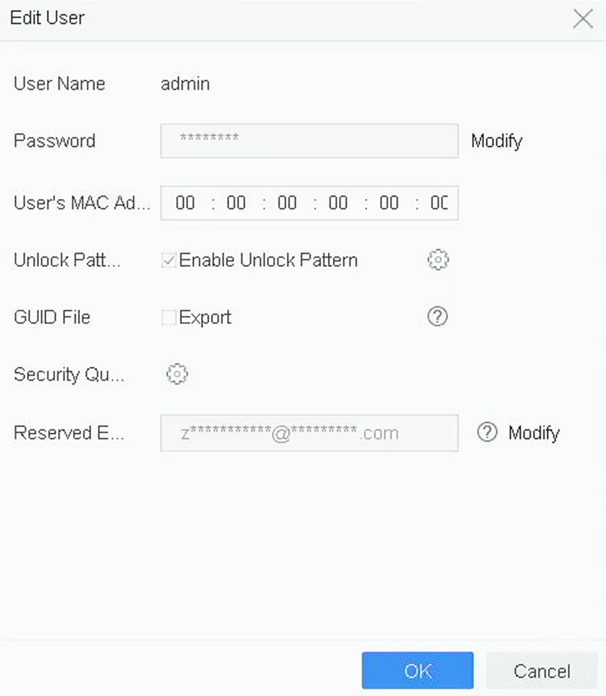
5. Set the security questions.
6. Click **OK**.
7. Enter the admin password.
8. Click **OK**.

11.3.3 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.



Edit User

User Name admin

Password ******** Modify

User's MAC Ad... 00 : 00 : 00 : 00 : 00 : 0C

Unlock Patt... ☑ Enable Unlock Pattern

GUID File □ Export

Security Qu...

Reserved E... z***********@*********.com Modify

Figure 11-7 Configure Reserved Email

3. Click **OK**.

11.4 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.

11.4.1 Reset Password by GUID

You can reset password by GUID via web browser.

Before You Start

Ensure you have the correct GUID file.

Steps

1. On the user login interface, click **Forgot password**.
2. Select **Verification Mode** as **GUID File Verification**.
3. Click **Browse** to locate the GUID file.
4. Click **Next**.

5. Enter a new password.

⚠ **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 change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.

6. Confirm the new password.
7. Click **Next**.

11.4.2 Reset Password by Security Questions

You can reset password by answering security questions via web browser.

Before You Start

Ensure you have configured the security questions when you activate the device or edit the admin user account.

Steps

1. On the user login interface, click **Forgot password**.
2. Select **Verification Mode** as **Security Question Verification**.
3. Enter the answers of each question.
4. Click **Next**.
5. Enter a new password.

⚠ **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 change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.

6. Click **Next**.

11.4.3 Reset Password by Hik-Connect

Before You Start

Ensure your device has enabled Hik-Connect, and bound with a registered Hik-Connect account.

Steps

1. On the user login interface, click **Forgot Password**.
2. On the password reset type interface, select **Verify by Hik-Connect**.

3. Log in to Hik-Connect app with the account that has bound with your device.
4. Use Hik-Connect to scan the QR code. Thereafter, you will have a verification code from Hik-Connect.
5. Enter the verification code.
6. Click **OK**.

11.4.4 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 12 System Management

12.1 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.

12.2 Configure Time

12.2.1 Manual Time Synchronization

Steps

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

12.2.2 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**

12.2.3 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.

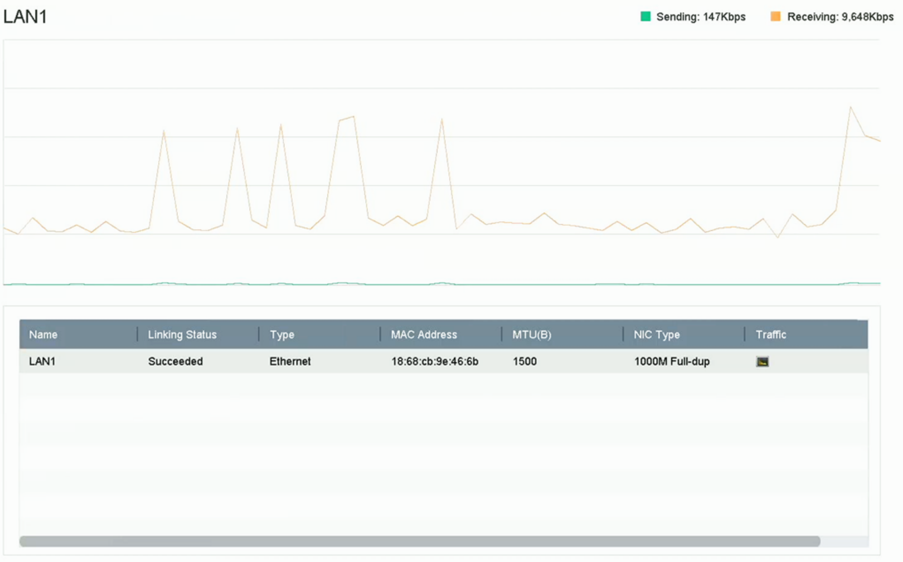
12.3 Network Detection

12.3.1 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.



Name	Linking Status	Type	MAC Address	MTU(B)	NIC Type	Traffic
LAN1	Succeeded	Ethernet	18:68:cb:9e:46:6b	1500	1000M Full-dup	▨

Figure 12-1 Network Traffic

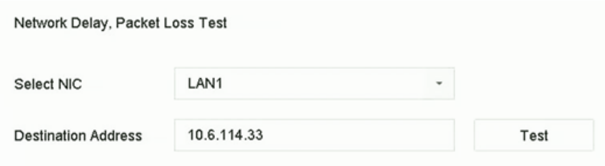
12.3.2 Test Network Delay and Packet Loss

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**.



Network Delay, Packet Loss Test

Select NIC: LAN1

Destination Address: 10.6.114.33

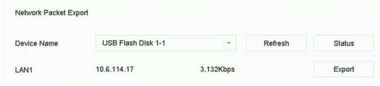
Figure 12-2 Test Network Delay and Packet Loss

12.3.3 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.



Network Packet Export

Device Name: USB Flash Disk 1-1

LAN1 10.6.114.17 3,132Kbps

Figure 12-3 Export Network Packet

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

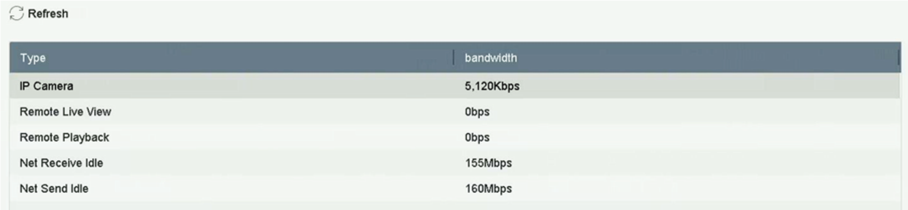
Note

It will export 1 MB data each time as default.

12.3.4 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** .



Refresh

Type	bandwidth
IP Camera	5,120Kbps
Remote Live View	0bps
Remote Playback	0bps
Net Receive Idle	155Mbps
Net Send Idle	160Mbps

Figure 12-4 Network Resource Statistics

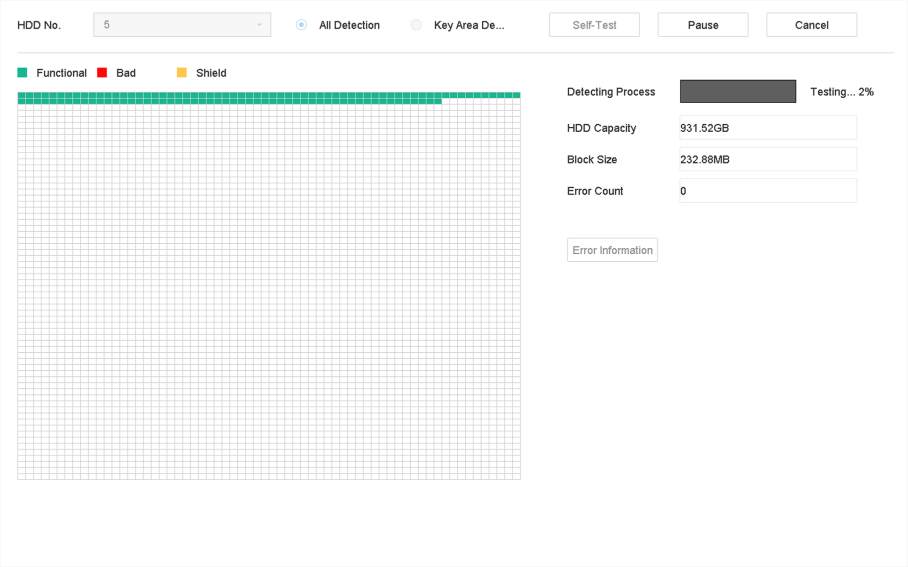
2. View the bandwidth statistics, including **IP Camera**, **Remote Live View**, **Remote Play**, **Net Total Idle**, etc.
3. **Optional:** Click **Refresh** to obtain the latest data.

12.4 Storage Device Maintenance

12.4.1 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.



HDD No. 5 ● All Detection ○ Key Area De... Self-Test Pause Cancel

🟩 Functional 🟥 Bad 🟨 Shield

Detecting Process Testing... 2%

HDD Capacity 931.52GB

Block Size 232.88MB

Error Count 0

Error Information

Figure 12-5 Bad Sector Detection

Note

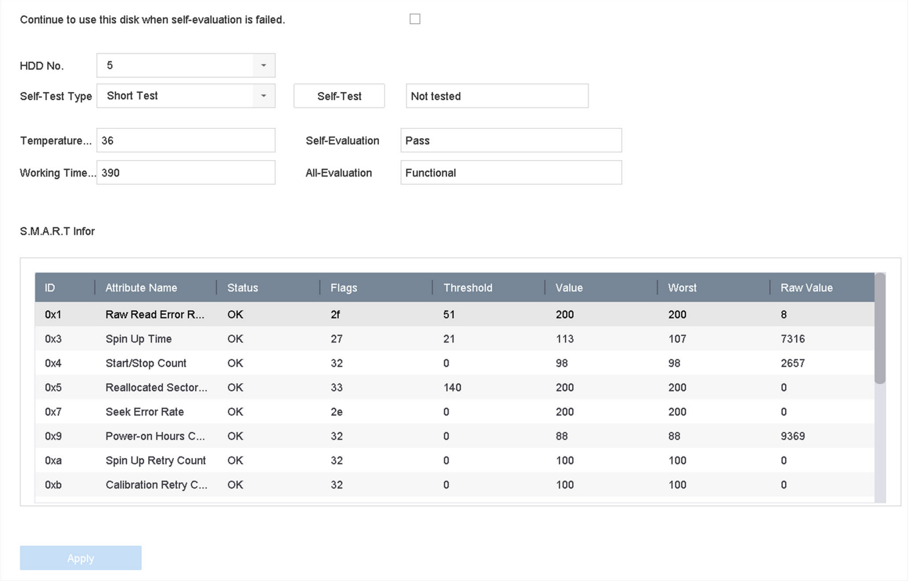
- You can pause/resume or cancel the detection.
- After testing has been completed, you can click **Error information** to see the detailed damage information.

12.4.2 S.M.A.R.T. Detection

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

Steps

1. Go to **Maintenance → HDD Operation → S.M.A.R.T** .
2. Select the HDD to view its S.M.A.R.T. information list.
3. Set **Self-Test Type**.
4. Click **Self-Test** to start the S.M.A.R.T. HDD self-evaluation.



Continue to use this disk when self-evaluation is failed. □

HDD No. 5

Self-Test Type Short Test

Not tested

Temperature... 36

Self-Evaluation Pass

Working Time... 390

All-Evaluation Functional

S.M.A.R.T Infor

ID	Attribute Name	Status	Flags	Threshold	Value	Worst	Raw Value
0x1	Raw Read Error R...	OK	2f	51	200	200	8
0x3	Spin Up Time	OK	27	21	113	107	7316
0x4	Start/Stop Count	OK	32	0	98	98	2657
0x5	Reallocated Sector...	OK	33	140	200	200	0
0x7	Seek Error Rate	OK	2e	0	200	200	0
0x9	Power-on Hours C...	OK	32	0	88	88	9369
0xa	Spin Up Retry Count	OK	32	0	100	100	0
0xb	Calibration Retry C...	OK	32	0	100	100	0

Figure 12-6 S.M.A.R.T. Settings Interface

Note

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

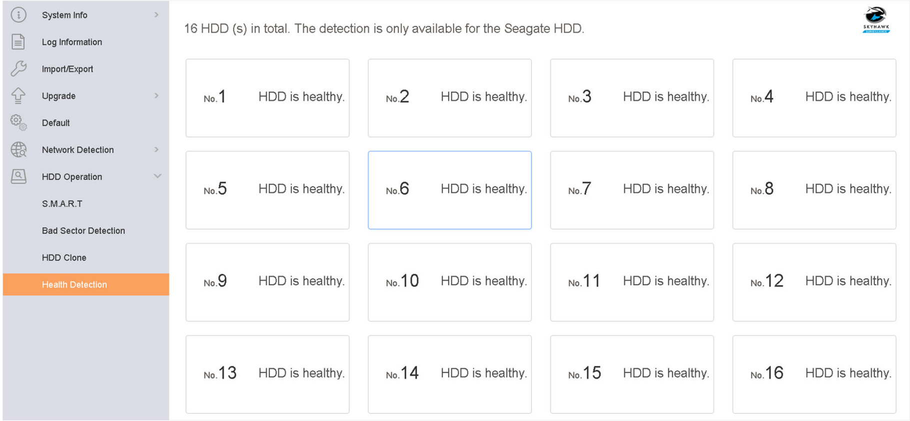
The related information of the S.M.A.R.T. is shown, and you can check the HDD status.

12.4.3 HDD Health Detection

You can view the health status of a 4 TB to 8 TB Seagate HDD that generated after October 1, 2017. Use this function to help troubleshoot HDD problems. Health Detection shows a more detailed HDD status than the S.M.A.R.T. function.

Steps

1. Go to **Maintenance → HDD Operation → Health Detection** .



16 HDD (s) in total. The detection is only available for the Seagate HDD.

No.1 HDD is healthy.	No.2 HDD is healthy.	No.3 HDD is healthy.	No.4 HDD is healthy.
No.5 HDD is healthy.	No.6 HDD is healthy.	No.7 HDD is healthy.	No.8 HDD is healthy.
No.9 HDD is healthy.	No.10 HDD is healthy.	No.11 HDD is healthy.	No.12 HDD is healthy.
No.13 HDD is healthy.	No.14 HDD is healthy.	No.15 HDD is healthy.	No.16 HDD is healthy.

Figure 12-7 Health Detection

2. Click a HDD to view details.

12.4.4 Configure Disk Clone

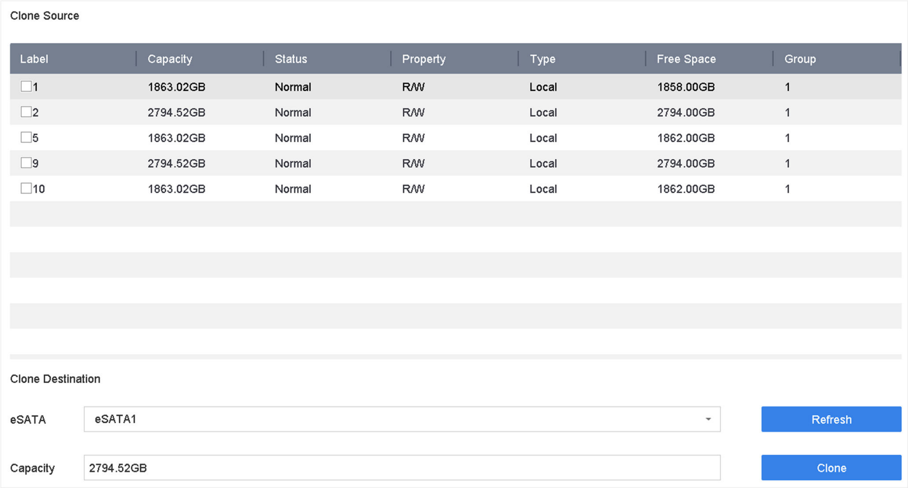
Select the HDDs to clone to the eSATA HDD.

Before You Start

Connect an eSATA disk to the device.

Steps

1. Go to **Maintenance → HDD Operation → HDD Clone** .



Clone Source

Label	Capacity	Status	Property	Type	Free Space	Group
□1	1863.02GB	Normal	R/W	Local	1858.00GB	1
□2	2794.52GB	Normal	R/W	Local	2794.00GB	1
□5	1863.02GB	Normal	R/W	Local	1862.00GB	1
□9	2794.52GB	Normal	R/W	Local	2794.00GB	1
□10	1863.02GB	Normal	R/W	Local	1862.00GB	1

Clone Destination

eSATA: eSATA1

Capacity: 2794.52GB

Figure 12-8 HDD Clone

2. Check the HDD to clone. The capacity of the selected HDD must match the capacity of the clone destination.
3. Click **Clone**.
4. Click **Yes** on the pop up message box to create the clone.

12.4.5 Repair Database

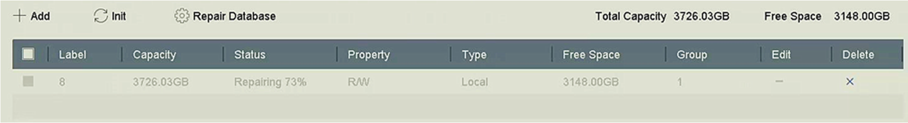
Repairing database will rebuild all databases. It might help to improve your system speed after upgrade.

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**.



Total Capacity 3726.03GB Free Space 3148.00GB

□	Label	Capacity	Status	Property	Type	Free Space	Group	Edit	Delete
■	8	3726.03GB	Repairing 73%	R/W	Local	3148.00GB	1	–	×

Figure 12-9 Repair Database

12.5 Upgrade Device

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

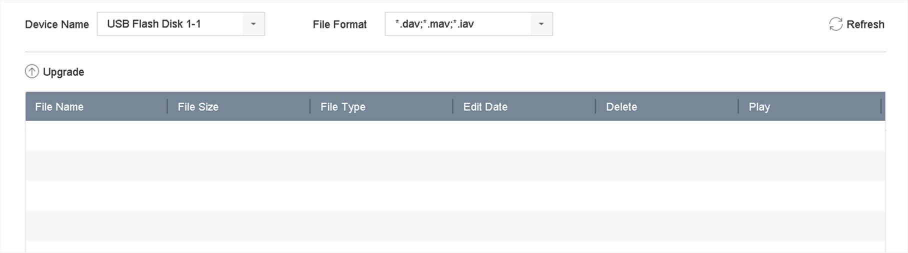
12.5.1 Upgrade by Local Backup Device

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.



Device Name: USB Flash Disk 1-1

File Format: *.dav;*.mav;*.iav

File Name	File Size	File Type	Edit Date	Delete	Play

Figure 12-10 Local Upgrade

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.

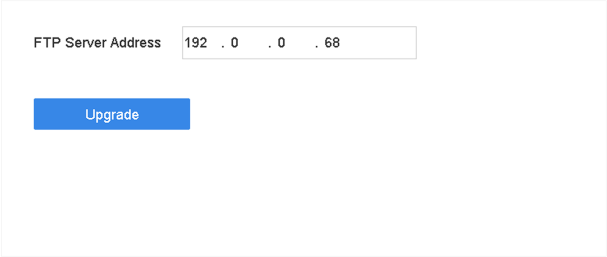
12.5.2 Upgrade by FTP

Before You Start

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

Steps

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



FTP Server Address 192 . 0 . 0 . 68

Figure 12-11 FTP Upgrade

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.

12.5.3 Upgrade by Web Browser

You can upgrade the device by web browser

After logging in to the device via web browser, go to **Configuration → System → Maintenance → Upgrade** . Click **Browse** to upload the firmware, and upgrade the device.

12.5.4 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**.

12.6 Import/Export Device Configuration Files

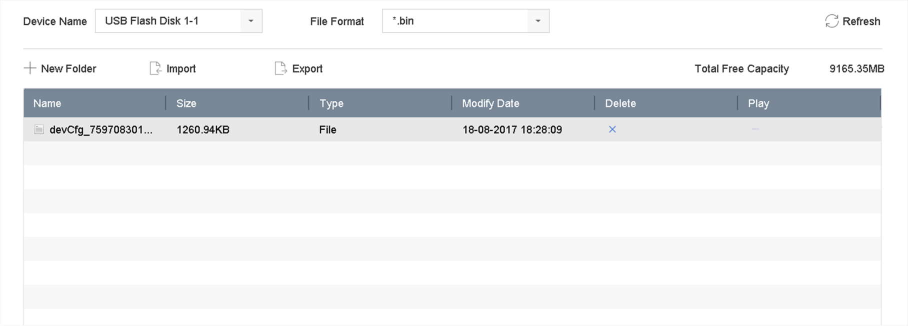
The device configuration files can be exported to a local device for backup; and the configuration files of one device can be imported to multiple devices if they are to be configured with the same parameters.

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** .



Device Name: USB Flash Disk 1-1

File Format: *.bin

Total Free Capacity: 9165.35MB

Name	Size	Type	Modify Date	Delete	Play
devCfg_759708301...	1260.94KB	File	18-08-2017 18:28:09	×	-

Figure 12-12 Import/Export Configuration 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

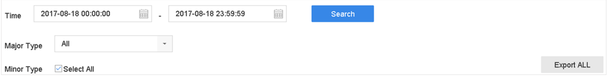
After having finished importing configuration files, the device will reboot automatically.

12.7 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** .



Time: 2017-08-18 00:00:00 - 2017-08-18 23:59:59

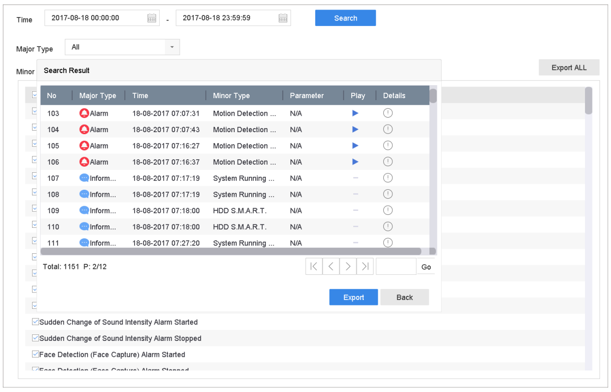
Major Type: All

Minor Type: ☑ Select All

Figure 12-13 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.



Time 2017-08-18 00:00:00 - 2017-08-18 23:59:59 Search

Major Type All

Minor

Search Result

Export ALL

No	Major Type	Time	Minor Type	Parameter	Play	Details
103	Alarm	18-08-2017 07:07:31	Motion Detection ...	N/A	▶	ⓘ
104	Alarm	18-08-2017 07:07:43	Motion Detection ...	N/A	▶	ⓘ
105	Alarm	18-08-2017 07:16:27	Motion Detection ...	N/A	▶	ⓘ
106	Alarm	18-08-2017 07:16:37	Motion Detection ...	N/A	▶	ⓘ
107	Inform...	18-08-2017 07:17:19	System Running ...	N/A	–	ⓘ
108	Inform...	18-08-2017 07:17:19	System Running ...	N/A	–	ⓘ
109	Inform...	18-08-2017 07:18:00	HDD S.M.A.R.T.	N/A	–	ⓘ
110	Inform...	18-08-2017 07:18:00	HDD S.M.A.R.T.	N/A	–	ⓘ
111	Inform...	18-08-2017 07:27:20	System Running ...	N/A	–	ⓘ

Total: 1151 P: 2/12 Go

Export Back

☑Sudden Change of Sound Intensity Alarm Started

☑Sudden Change of Sound Intensity Alarm Stopped

☑Face Detection (Face Capture) Alarm Started

Figure 12-14 Log Search Results

Note

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

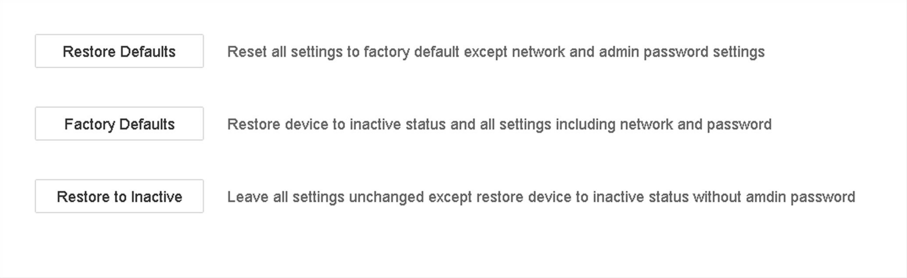
5. Related Operation:

ⓘ	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.

12.8 Restore Default Settings

Steps

1. Go to **Maintenance → Default** .



Restore Defaults | Reset all settings to factory default except network and admin password settings

Factory Defaults | Restore device to inactive status and all settings including network and password

Restore to Inactive | Leave all settings unchanged except restore device to inactive status without amdin password

Figure 12-15 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.

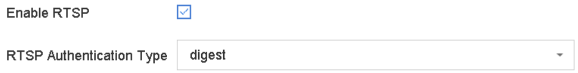
12.9 Security Management

12.9.1 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** .



Enable RTSP ☑

RTSP Authentication Type: digest

Figure 12-16 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.

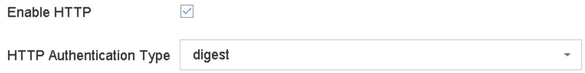
3. Click **Apply**.
4. Restart the device to take effect the settings.

12.9.2 HTTP Authentication

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

Steps

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



Enable HTTP ☑

HTTP Authentication Type: digest

Figure 12-17 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.

12.9.3 Disable SADP Services

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

Go to **System → System Service → System Service** , and uncheck **Enable SADP** to disable the service.

Chapter 13 Appendix

13.1 List of Applicable Power Adapter

Only use power adapters listed below.

Power Adapter Model	Specifications	Manufacturer
MSA-C1500IC12.0-18P-DE	12 V, 1.5 A	0000201935 MOSO Technology Co., Ltd.
ADS-25FSG-12 12018GPG	CE, 100 to 240 VAC, 12 V, 1.5 A, 18 W, Φ5.5 × 2.1 × 10	0000200174 Shenzhen Honor Electronic Co., Ltd.
MSA-C1500IC12.0-18P-US	12 V, 1.5 A	0000201935 MOSO Technology Co., Ltd.
TS-A018-120015AD	100 to 240 VAC, 12 V, 1.5 A, 18 W, Φ5.5 × 2.1 × 10	0000200878 Shenzhen Transin Technologies Co., Ltd.
MSA-C2000IC12.0-24P-DE	12 V, 2 A	0000201935 MOSO Technology Co., Ltd.
ADS-24S-12 1224GPG	CE, 100 to 240 VAC, 12 V, 2 A, 24 W, Φ2.1	0000200174 Shenzhen Honor Electronic Co., Ltd.
MSA-C2000IC12.0-24P-US	US, 12 V, 2 A	0000201935 MOSO Technology Co., Ltd.
ADS-26FSG-12 12024EPCU	US, 12 V, 2 A	0000200174 Shenzhen Honor Electronic Co., Ltd.
KPL-040F-VI	12 V, 3.33 A, 40 W	0000203078 Channel Well Technology Co., Ltd.
MSA-Z3330IC12.0-48W-Q	12 V, 3.33 A	0000201935 MOSO Technology Co., Ltd.
MSP-Z1360IC48.0-65W	48 V, 1.36 A	0000201935 MOSO Technology Co., Ltd.
KPL-050S-II	48 V, 1.04 A	0000203078 Channel Well Technology Co., Ltd.

13.2 Glossary

Dual-Stream

Dual-stream is a technology used to record high resolution video locally while transmitting a lower resolution stream over the network. The two streams are generated by the DVR, with the main stream having a maximum resolution of 1080P and the sub-stream having a maximum resolution of CIF.

DVR

Acronym for Digital Video Recorder. A DVR is device that is able to accept video signals from analog cameras, compress the signal and store it on its hard drives.

HDD

Acronym for Hard Disk Drive. A storage medium which stores digitally encoded data on platters with magnetic surfaces.

DHCP

Dynamic Host Configuration Protocol (DHCP) is a network application protocol used by devices (DHCP clients) to obtain configuration information for operation in an Internet Protocol network.

HTTP

Acronym for Hypertext Transfer Protocol. A protocol to transfer hypertext request and information between servers and browsers over a network.

PPPoE

PPPoE, Point-to-Point Protocol over Ethernet, is a network protocol for encapsulating Point-to-Point Protocol (PPP) frames inside Ethernet frames. It is used mainly with ADSL services where individual users connect to the ADSL transceiver (modem) over Ethernet and in plain Metro Ethernet networks.

DDNS

Dynamic DNS is a method, protocol, or network service that provides the capability for a networked device, such as a router or computer system using the Internet Protocol Suite, to notify a domain name server to change, in real time (ad-hoc) the active DNS configuration of its configured hostnames, addresses or other information stored in DNS.

Hybrid DVR

A hybrid DVR is a combination of a DVR and NVR.

NTP

Acronym for Network Time Protocol. A protocol designed to synchronize the clocks of computers over a network.

NTSC

Acronym for National Television System Committee. NTSC is an analog television standard used in such countries as the United States and Japan. Each frame of an NTSC signal contains 525 scan lines at 60Hz.

NVR

Acronym for Network Video Recorder. An NVR can be a PC-based or embedded system used for centralized management and storage for IP cameras, IP Domes and other DVRs.

PAL

Acronym for Phase Alternating Line. PAL is also another video standard used in broadcast televisions systems in large parts of the world. PAL signal contains 625 scan lines at 50Hz.

PTZ

Acronym for Pan, Tilt, Zoom. PTZ cameras are motor driven systems that allow the camera to pan left and right, tilt up and down and zoom in and out.

USB

Acronym for Universal Serial Bus. USB is a plug-and-play serial bus standard to interface devices to a host computer.

13.3 Communication Matrix

Please scan the QR code below to view the communication matrix document.

Figure 13-1 Communication Matrix

13.4 Device Command

Please scan the QR code below to view the device command document.

Figure 13-2 Device Command

13.5 Frequently Asked Questions

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

Reason

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

Solution

1. Go to **Camera → Video Parameters → Sub-Stream** . Select the channel, and turn down the resolution and max. bitrate (resolution shall be less than 720p, max. bitrate shall be less than 2048 Kbps).

   Note

   If your video recorder notifies not support this function, you can log in to the camera, and adjust video parameters via web browser.

2. Properly set the sub-stream resolution and max. bitrate (resolution shall be less than 720p, max. bitrate shall be less than 2048 Kbps), then delete the channel and add it back again.

13.5.2 Why is the video recorder notifying risky password after a network camera is added?

Reason

The camera password is too weak.

Solution

Change the camera password.

Warning

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

13.5.3 Why is the video recorder notifying the stream type is not supported?

Reason

The camera encoding format mismatches with the video recorder.

Solution

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

13.5.4 How to improve the playback image quality?

Reason

Recording parameter settings are inappropriate.

Solution

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

13.5.5 Why is analog channel having "NO VIDEO" overlaid on live view?

Reason

1. The video in connector is loose, which results in weak video signal.
2. Video in/out standard mismatch.
3. Transmission distance too long.
4. Cable damage causes weak video signal.
5. The video in connector of video recorder is broken.

Solution

1. Ensure connectors are connected firmly.
2. Go to **System → General** . Ensure the output standard is correct.

3. Ensure the distance between analog camera and video recorder has not exceeded the limit.
4. Ensure the cable is not damaged.
5. Try other BNC connectors if they are working normally.

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

Solution

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

13.5.7 Why is the timeline at playback not constant?

Reason

1. When the video recorder is using event recording, it only records video when event occurs. Hence the video may not be continuous.
2. Exception occurs, such as the device offline, HDD error, record exception, network camera offline, etc.

Solution

1. Ensure the recording type is continuous recording.
2. Go to **Maintenance → Log Information** . Search the log file during the video time period. See if there are unexpected events, such as HDD error, record exception, etc.

13.5.8 Why is the video recorder notifying the network is unreachable when a network camera is being added?

Reason

1. The IP address or port of network camera is incorrect.
2. The network between video recorder and camera is disconnected.

Solution

1. Go to **Camera → Camera → IP Camera** . Click ✎ of the selected camera, and edit its IP address and port. Ensure the video recorder and camera is using the same port.
2. Go to **Maintenance → Network → Detection** . Enter the IP address of network camera in **Destination Address**, and click **Test** to see if the network is reachable.

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

Reason

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

Solution

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

13.5.10 Why is the video recorder notifying IP conflict?

Reason

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

Solution

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

13.5.11 Why is image getting stuck when playing back by single or multi-channel cameras?

Reason

HDD read/write exception.

Solution

Export the video, and play it with other devices. If it plays normally on other device, change your HDD, and try again.

13.5.12 Why does my video recorder make a beeping sound after booting?

Reason

1. The front panel is not fastened (for the device which its front panel is removable).
2. HDD error, or do not have HDD.

Solution

1. If it makes continuous beeps, and your device's front panel is removable, ensure the front panel is fastened.
2. If it makes non-continuous beeps (3 long, 2 short), take HDD error as an example, check if the device has installed HDD. If not, you can go to **System → Event → Normal Event → Exception** , and uncheck **Event Hint Configuration** to disable HDD error event hint.
   Check if the HDD is initialized. If not, go to Storage > Storage Device to initialize the HDD.
   Check if the HDD is broken. You can change it, and try again.

13.5.13 Why is there no recorded video after the motion detection is set?

Reason

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

Solution

1. The recording schedule is setup correctly by following the steps listed in Configuring Record/ Capture Schedule.
2. The motion detection area is configured correctly. The channels are being triggered for motion detection (See Configuring Motion Detection).
3. Check if the device has installed HDD.
   Check if the HDD is initialized. If not, go to Storage > Storage Device to initialize the HDD.
   Check if the HDD is broken. You can change it, and try again.

13.5.14 Why is the device not able to control PTZ camera via coaxitron?

Reason

1. The camera does not support coaxitron.
2. The coaxitron protocol is incorrect.
3. The signal is affected by video optical transceiver.

Solution

1. Ensure the video input signal is HDTVI, and the camera supports coaxitron.
2. Ensure coaxitron protocol parameters are correct, such as baud rate and address.
3. Remove the video optical transceiver, and try again.

13.5.15 Why does the PTZ seem unresponsive via RS-485?

Reason

1. The RS-485 cable is not properly connected.
2. The RS-485 interface is broken.
3. The control protocol is not correct.

Solution

1. Check if RS-485 cable is properly connected.
2. Change RS-485 interface, and try again.
3. Ensure control protocol is Pelco.

13.5.16 Why is the video sound quality not good?

Reason

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

Solution

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