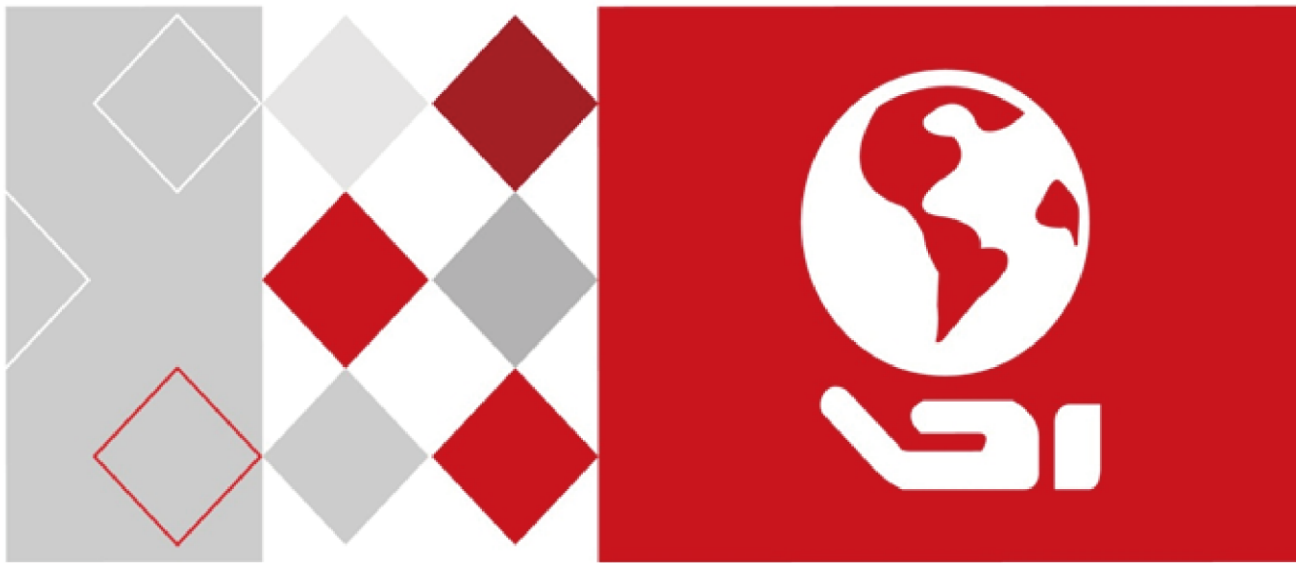# HIKVISION
HiWatch Series

Network Video Recorder

User Manual

Legal Information

COPYRIGHT ©2020 Hangzhou Hikvision Digital Technology Co., Ltd.

About this Manual

The Manual includes instructions for using and managing the Product. Pictures, charts, images and all other information hereinafter are for description and explanation only. The information contained in the Manual is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version in the company website (***https://www.hi-watch.eu/***). Please use this Manual with the guidance and assistance of professionals trained in supporting the Product.

Trademarks

HIKVISION and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions. Other trademarks and logos mentioned below are the properties of their respective owners.

HDMI™: The terms HDMI and HDMI High-Definition Multimedia Interface, and the HDMI Logo are trademarks or registered trademarks of HDMI Licensing Administrator, Inc. in the United States and other countries.

Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS MANUAL AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED "AS IS" AND "WITH ALL FAULTS AND ERRORS". HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.

YOU ACKNOWLEDGE THAT THE NATURE OF INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INSPECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.

YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS.

YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.

IN THE EVENT OF ANY CONFLICTS BETWEEN THIS MANUAL AND THE APPLICABLE LAW, THE LATER PREVAILS.

Regulatory Information

FCC Information

Please take attention that changes or modification not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

FCC compliance: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Conditions

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

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

EU Conformity Statement

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

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

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

Industry Canada ICES-003 Compliance

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

This device complies with Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions:

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

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radioexempts de licence. L'exploitation est autorisée aux deux conditions suivantes :

1. l'appareil ne doit pas produire de brouillage, et
2. l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

Under Industry Canada regulations, this radio transmitter may only operate using an antenna of atype and maximum (or lesser) gain approved for the transmitter by Industry Canada. To reducepotential radio interference to other users, the antenna type and its gain should be so chosen thatthe equivalent isotropically radiated power (e.i.r.p.) is not more than that necessary for successful communication.

Conformément à la réglementation d'Industrie Canada, le présent émetteur radio peutfonctionner avec une antenne d'un type et d'un gain maximal (ou inférieur) approuvé pourl'émetteur par Industrie Canada. Dans le but de réduire les risques de brouillage radioélectrique àl'intention des autres utilisateurs, il faut choisir le type d'antenne et son gain de sorte que lapuissance isotrope rayonnée équivalente (p.i.r.e.) ne dépasse pas l'intensité nécessaire à l'établissement d'une communication satisfaisante.

This equipment should be installed and operated with a minimum distance 20cm between the radiator and your body.

Cet équipement doit être installé et utilisé à une distance minimale de 20 cm entre le radiateur et votre corps.

Applicable Model

This manual is applicable to the following models.

Table 1-1 Applicable Model

Series	Model
HWN-2100MH-W(C)	HWN-2104MH-W(C)
	HWN-2108MH-W(C)
HWN-2100MH-W	HWN-2104MH-W
	HWN-2108MH-W

Symbol Conventions

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

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

Safety Instruction

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

Preventive and Cautionary Tips

Before connecting and operating your device, please be advised of the following tips:
● Ensure recorder is installed in a well-ventilated, dust-free environment.
● Recorder is designed for indoor use only.
● Keep all liquids away from the device.
● Ensure environmental conditions meet factory specifications.
● Ensure recorder is properly secured to a rack or shelf. Major shocks or jolts to the recorder as a result of dropping it may cause damage to the sensitive electronics within the recorder.
● Use the device in conjunction with an UPS if possible.
● Power down the recorder before connecting and disconnecting accessories and peripherals.
● A factory recommended HDD should be used for this device.
● Improper use or replacement of the battery may result in hazard of explosion. Replace with the same or equivalent type only. Dispose of used batteries according to the instructions provided by the battery manufacturer.
● When installing the device into a cabinet over 2U height, it is suggested to use rack shelf to bear the weight. If the cabinet height is over 4U, it is suggested to use slide rails or rack shelf to bear the weight.
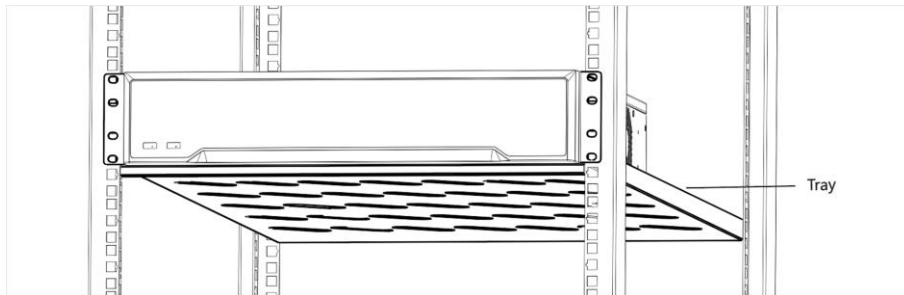
Contents

Chapter 1 Get Started

1.1 Startup and Activation

1.1.1 Startup, Shutdown and Reboot

Proper startup and shutdown procedures are crucial to expand the life of your device.

Startup Your Device

Ensure the voltage of the extra power supply satisfies the requirement, and the ground connection is working properly.
Plug the power supply into an electrical outlet. It is HIGHLY recommended that an Uninterruptible Power Supply (UPS) is used in conjunction with the device.
Press the power button on the panel. The power indicator LED would be lighted up which indicating the device begins to start up.

Shut Down Your Device

Go to **Menu** → **Shutdown**. Click **Shutdown**, and click **Yes**.
If your device has a power button on the front panel, you can also hold the power button for 3 seconds, and then enter the admin user name and password to shut down your device.

[i]**Note**

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

Reboot Your Device

Go to **Menu** → **Shutdown**. Click **Reboot**, and your device will restart.

Figure 1-1 Startup, Shutdown and Reboot

1.1.2 Activate Your Device

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 password in **Create New Password** and **Confirm New 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.
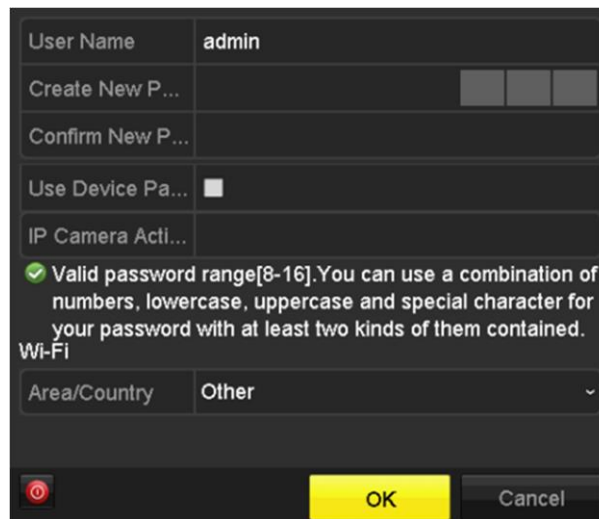
Figure 1-2 Set Admin Password

2. Check **Use Device Password to Active IP Camera**, or enter the password in **IP Camera Activation** to activate the IP camera(s) connected to the device.
3. Set **Area/Country**.
4. Click **OK**.

What to do next

Export the GUID file to the USB flash driver for the future password resetting.

1.1.3 Login and Logout

User Login

You have to log in to the device before operating the menu and other functions.

Steps

1. Select a user account.
2. Enter the password for the selected user.
3. Click **Login**.
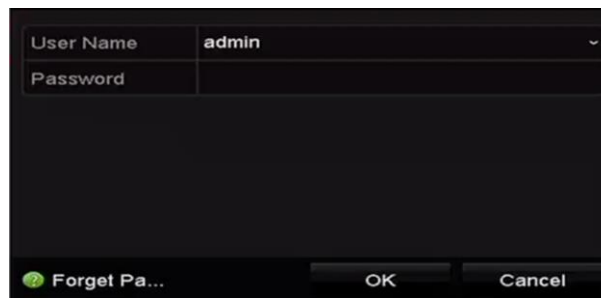
Figure 1-3 Login

- For the admin, if you have entered the wrong password for 7 times, the account will be locked for 60 seconds.
- For the operator, if you have entered the wrong password for 5 times, the account will be locked for 60 seconds.

User Logout

After logging out, the monitor turns to the live view mode and if you want to perform any operations, you need to enter user name and password log in again.

Go to **Menu → Shutdown**. Click **Logout**.

Figure 1-4 Logout

1.1.4 Set Unlock Pattern

For the admin user, you can set the unlock pattern for device login after it is activated.

Steps

1. Use mouse to draw a pattern among the 9 dots on the screen. Release the mouse when the pattern is done.
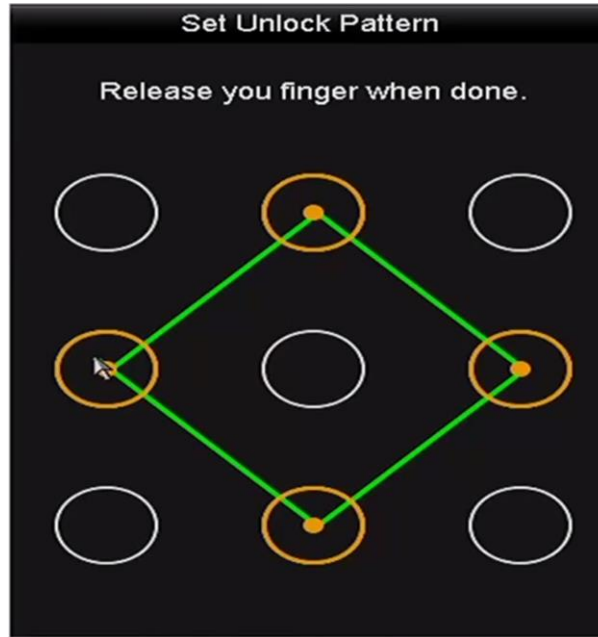
Figure 1-5 Set Unlock Pattern

Note
- The pattern shall have 4 dots at least.
- Each dot can be connected for once only.

2. Draw the same pattern again to confirm it.

Note

You can go to **Menu** → **Configuration** → **User**, and click 📝 to edit or disable the unlock pattern.

1.2 Add Network Cameras

1.2.1 Activate the IP Camera

Before adding the camera, make sure the IP camera to add is in active status.

Steps

1. Enter the IP camera management interface.
   – Select the **Add IP Camera** option from the right-click menu in live view mode.
   – click **Menu → Camera → Camera**

ⓘ**Note**

For the IP camera detected online in the same network segment, the Password status shows whether it is active or inactive.
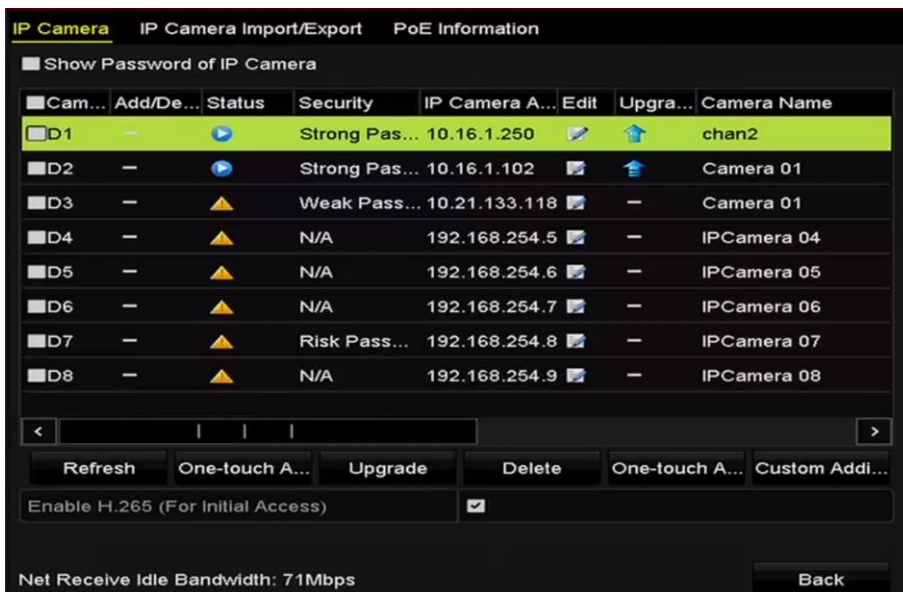
Figure 1-6 IP Camera Management Interface

2. Click the inactive icon of the camera to enter the following interface to activate it. You can also select multiple cameras from the list and click the **One-touch Activate** to activate the cameras in batch.
3. Set the password of the camera to activate it.

   Use IP Camera Activation Password

   The camera(s) will use the password which you have set during the device activation.

   Create New Password

If **IP Camera Activation Password** is not used, you shall create a new password for the camera.
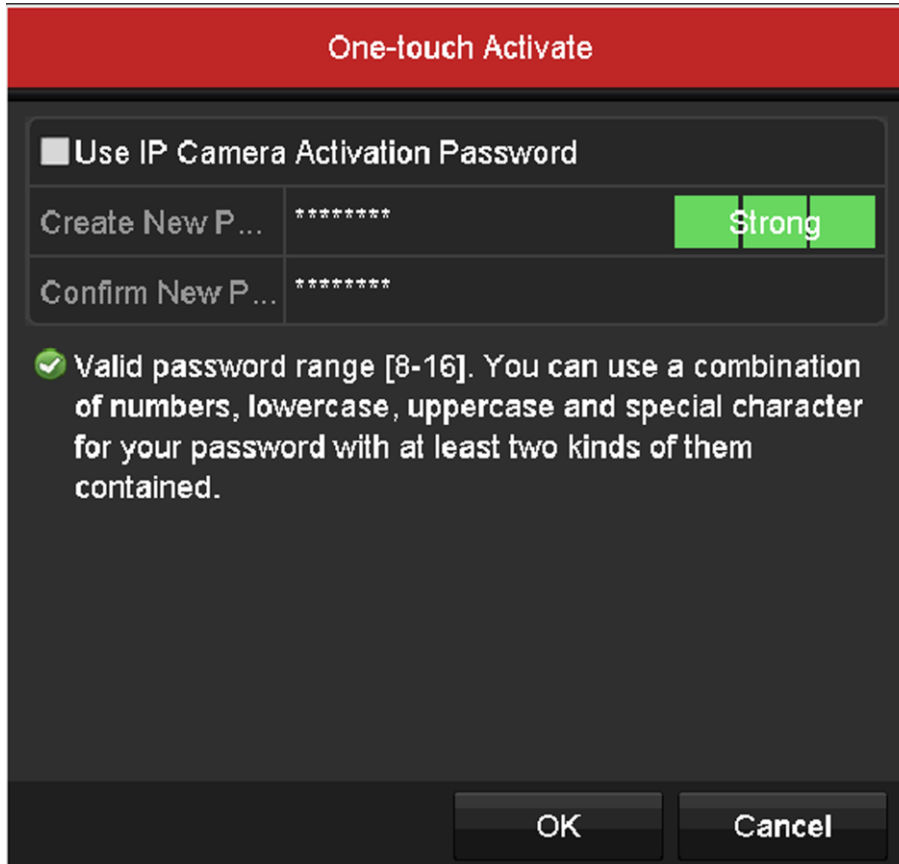
Figure 1-7 Set New Password

Warning

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

4. Click **OK**.
   The security status of camera will be changed to **Active**.

1.2.2 Add Wi-Fi Cameras

You can use Wi-Fi match function to search Wi-Fi cameras that are not activated, and add them to the device automatically.
Select **Wi-Fi Match** from the right-click menu in live view mode, and the device will search and add

Wi-Fi cameras. The process will take about 2 minutes. The Wi-Fi camera will use **IP Camera Activation Password** as its password. (Refer to ***Activate Your Device***.)

☐**i**Note

- It is recommended to keep the distance between Wi-Fi camera and device within 50 meters.
- Only certain Wi-Fi camera models and versions support this function.
- Ensure the Wi-Fi camera is powered on, not activated, and has not been connected with other devices via network cable.

1.2.3 Wi-Fi Auto-Switch

When adding Wi-Fi cameras to a Wi-Fi NVR, Wi-Fi Auto-Switch (For Initial Access) can synchronize Wi-Fi parameters to the IP camera.

1.2.4 Add Online IP Cameras

The main function of the NVR is to connect the network cameras and record the video got from it. So before you can get a live view or record of the video, you should add the network cameras to the connection list of the device.

Before You Start

Ensure the network connection is valid and correct. For detailed checking and configuring of the network.

Steps

1. Adding the IP Cameras.
   – OPTION 1
     1. Click to select an idle window in the live view mode.
     2. Click the ➕ in the center of the windw to pop up the adding IP camera interface.
     3. Select the detected IP camera and click the **Add** button to add it directly, and you can click the **Search** button to refresh the online IP camera manually. Or you can choose to custom add the IP camera by editing the parameters in the corresponding textfiled and then click the **Add** button to add it.

Network Video Recorder User Manual

Figure 1-8 Quick Adding IP Camera Interface

− OPTION 2
1. Select the **Add IP Camera** option from the right-click menu in live view mode or click **Menu → Camera → Camera** to enter the IP camera management interface.
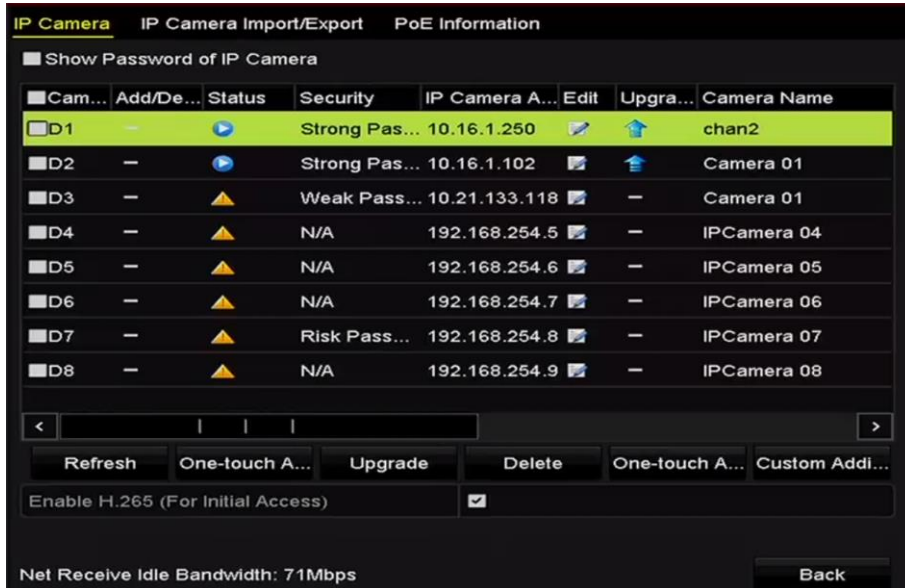
Figure 1-9 Adding IP Camera Interface

2. The online cameras with same network segment will be detected and displayed in the camera list.
3. Select the IP camera from the list and click the button to add the camera. Or you can click the **One-touch Adding** button to add all cameras (with the same login password) from

the list.

Note

Make sure the camera to add has already been activated.

4. (For the encoders with multiple channels only) check the **Channel Port** checkbox in the pop-up window, as shown in the following figure, and click **OK** to add multiple channels.
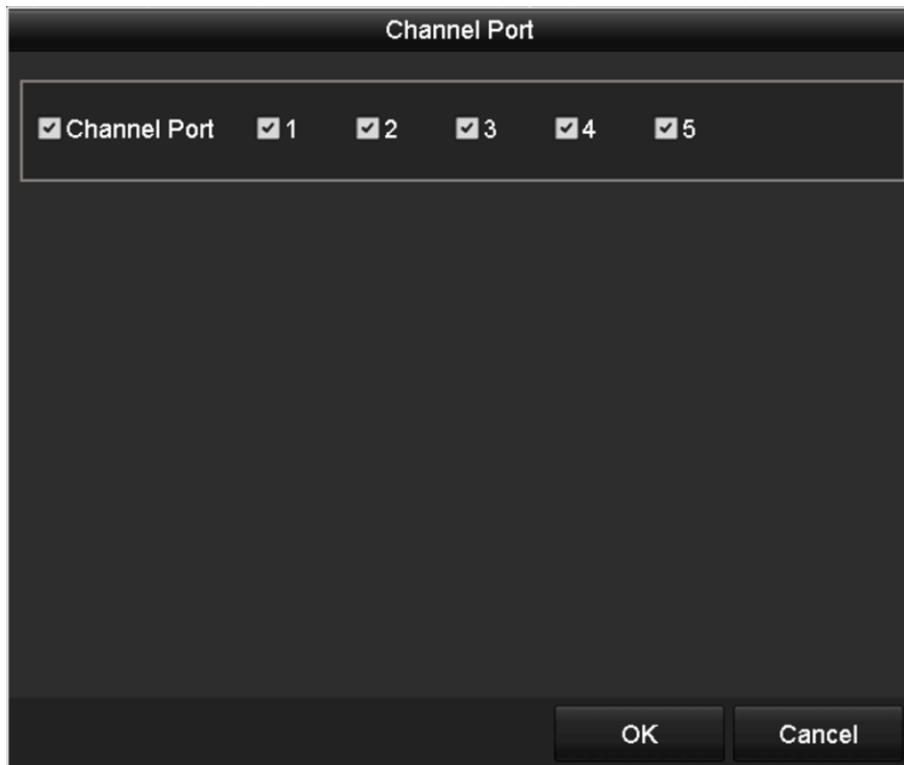
Figure 1-10 Selecting Multiple Channels

– OPTION 3
   1. On the IP Camera Management interface, click the **Custom Adding** button to pop up the Add IP Camera (Custom) interface.
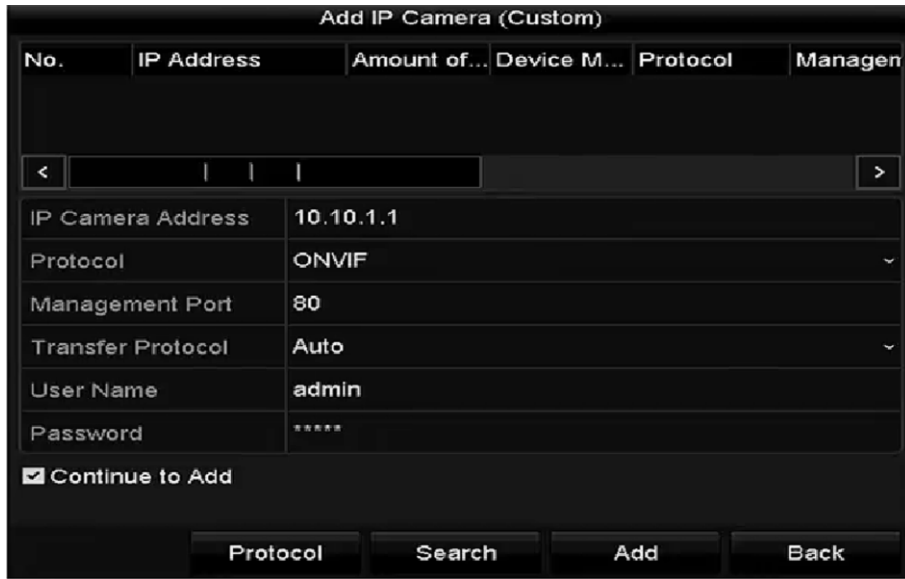
Figure 1-11 Custom Adding IP Camera Interface

2. You can edit the IP address, protocol, management port, and other information of the IP camera to be added.

ℹ️**Note**

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

3. **Optional:** Check the checkbox of **Continue to Add** to add other IP cameras.
4. Click **Add** to add the camera. The successfully added cameras are listed in the interface.

Table 1-1 Description of Icons

Icon	Description	Icon	Description
	Edit basic parameters of the camera.		Add the detected IP camera.
	The camera is disconnected; you can click the icon to get the exception information of camera.		Delete the IP camera.
	Play the live video of the connected camera.		Advanced settings of the camera.
	Upgrade the connected IP camera.	Security	Show the security status of the camera to be active/inactive or the password strength (strong/medium/weak/risk

Icon	Description	Icon	Description
			)

ⅰNote

For the added IP cameras, the Security status shows the security level of the password of camera: strong password, weak password and risk password.

1.2.5 Show the Password of Added IP Camera

For the admin login user account, you can check the checkbox of **Show Password of IP Camera** to enable the show the passwords of the successfully added IP cameras in the list.
You must enter the admin password to confirm permission.

1.2.6 Edit the Connected IP Cameras and Configure Customized Protocols

After the adding of the IP cameras, the basic information of the camera lists in the page, you can configure the basic setting of the IP cameras.

Steps

1. Click 📝 to edit the parameters; you can edit the IP address, protocol and other parameters.
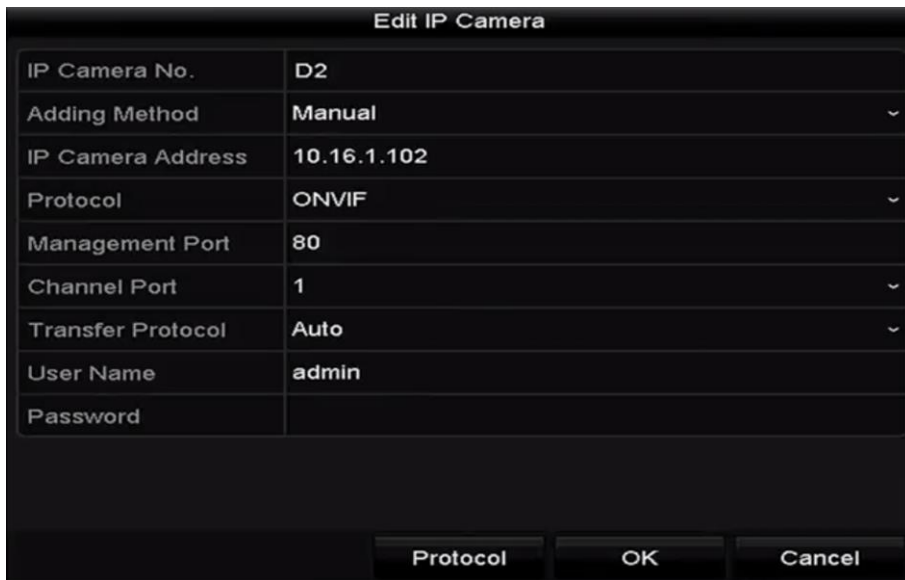
Figure 1-12 Edit the Parameters

    Channel Port

      If the connected device is an encoding device with multiple channels, you can choose the

channel to connect by selecting the channel port No. in the dropdown list.
2. Click **OK** to save the settings and exit the editing interface.
3. Edit advanced parameters.
   1) Drag the horizontal scroll bar to the right side and click 📷.
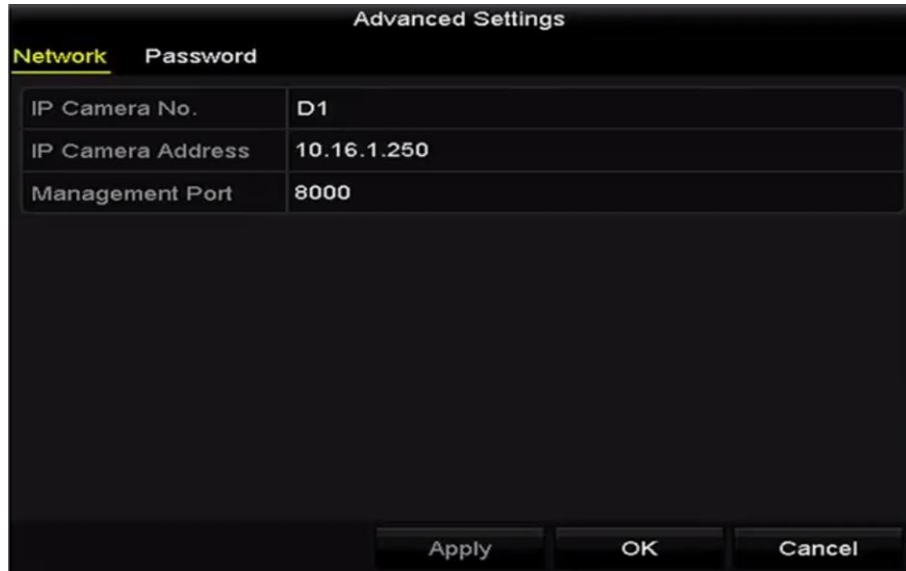
Figure 1-13 Paramerters Configuration of the Camera

2) You can edit the network information and the password of the camera.
3) Click **OK** to save the settings and exit the interface.

⎕**i** **Note**

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

4. Configuring the customized protocols.
   1) Click **Protocol** in the custom adding IP camera interface to enter the protocol management interface.

Figure 1-14 Protocol Management Interface

ℹ️**Note**

There are 16 customized protocols provided in the system, you can edit the protocol name; and choose whether to enable the sub-stream.

---

2) Choose the protocol type of transmission and choose the transfer protocols.

ℹ️**Note**

Before customizing the protocol for the network camera, you have to contact the manufacturer of the network camera to consult the URL (uniform resource locator) for getting main stream and sub-stream.

The format of the URL is: [Type]://[IP Address of the network camera]:[Port]/[Path]. Example: rtsp://192.168.1.55:554/ch1/main/av_stream.

● Protocol Name: Edit the name for the custom protocol.
● Enable Substream: If the network camera does not support sub-stream or the sub-stream is not needed leave the checkbox empty.
● Type: The network camera adopting custom protocol must support getting stream through standard RTSP.
● Transfer Protocol: Select the transfer protocol for the custom protocol.
● Port: Set the port No. for the custom protocol.

● Path: Set the resource path for the custom protocol. E.g., ch1/main/av_stream.

⬛**Note**

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

After adding the customized protocols, you can see the protocol name.
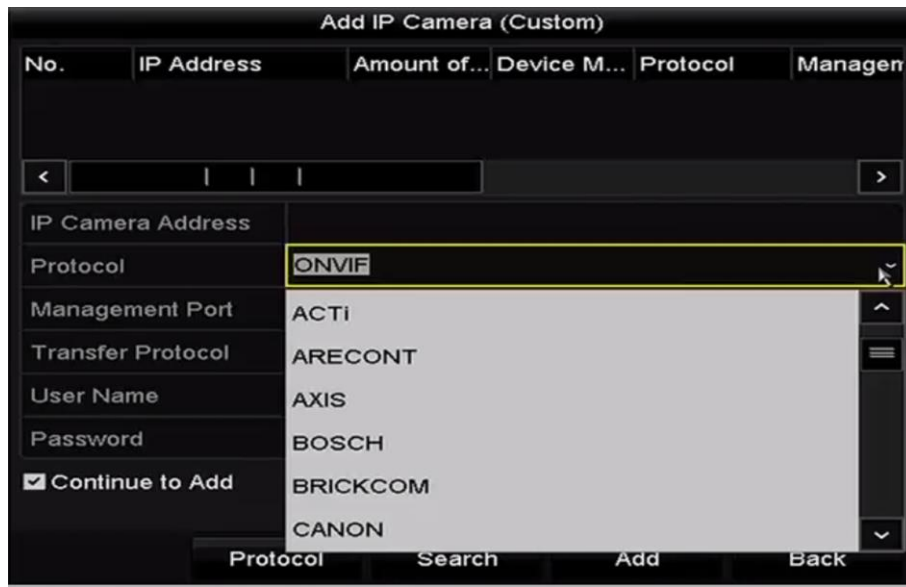
Figure 1-15 Protocol Setting

3) Choose the protocols you just added to validate the connection of the network camera.

1.3 Configure Hik-Connect

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

Steps

1. Go to **Menu → Configuration → Network → Platform Access**.
2. Check **Enable**. The service terms will pop up.
   1) Enter the verification code in **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** to save the settings.

ⓘ**Note**

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

3. Optional: Configure following parameters.
   - Check **Custom** and enter **Server Address** as your desire.
   - Check **Enable Stream Encryption**, then verification code is required for remote access and live view.
4. 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.

5. Click **Apply**.

What to do next

After configuration, you can access and manage your devices through Hik-Connect app or website.

Chapter 2 Camera Settings

2.1 Configure Camera as Repeater

The connected Wi-Fi cameras can be set as repeaters to extend the wireless network connection distance.

Before You Start

- Ensure your Wi-Fi cameras support this function.
- Before installing Wi-Fi cameras, you have to configure the repeater function first.

Steps

1. Add Wi-Fi cameras to the device through wireless network. Refer to **Add Network Cameras** for details.
2. Go to **Menu → Camera → IP Camera**.

Figure 2-1 Configure Camera as Repeater

3. Turn on the switch(s) in **Repeater Status** of Wi-Fi camera(s) as your desire.

> ⓘ**Note**
>
> - The repeater camera and repeated camera shall both enable this function.
> - Only two layers are allowed for the topology.

4. Optional: Click **Enable Repeater** or **Disable Repeater** to enable or disable the repeater function of all cameras.

What to do next

Install your Wi-Fi cameras to the destinations. Thereafter, Wi-Fi cameras will automatically form a

logical network topology according to Wi-Fi signal strength, you can view the connection topology and status in **Menu → Camera → Camera Topology**.
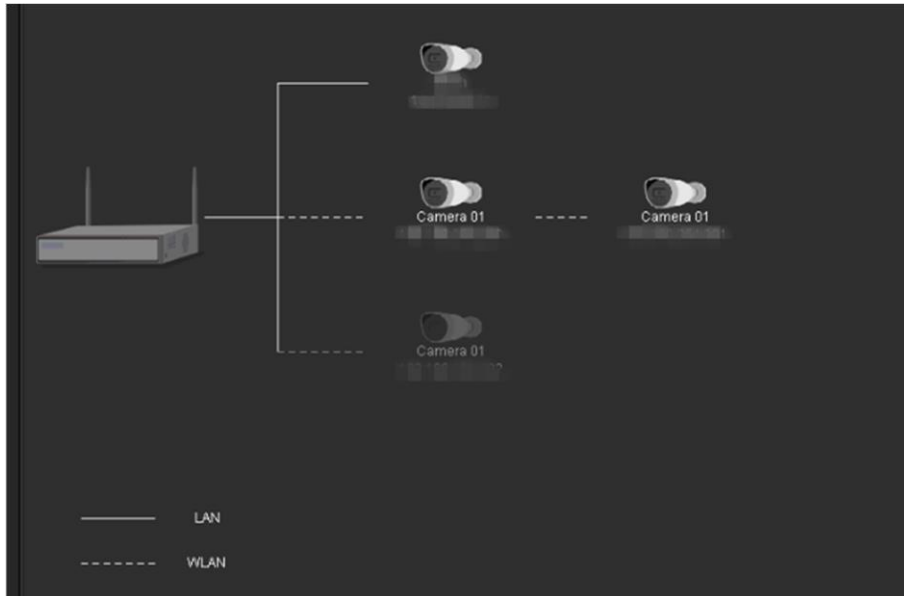
Figure 2-2 Camera Topology

2.2 Configure OSD Settings

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

Steps

1. Go to **Menu → Camera → OSD**.
2. Select a camera.
3. Edit **Camera Name**.
4. Select **Display Name**, **Display Date**, or **Display Week** as your desire
5. Set **Date Format**, **Time Format**, and **Display Mode**.

Figure 2-3 OSD Configuration

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

2.3 Configure Privacy Mask

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

Steps

1. Go to **Menu → Camera → Image**.

Figure 2-4 Image Settings

2. Select a camera to set image parameters.
3. Adjust the slider, or click on the up/down arrow to set brightness, contrast, or saturation.
4. Set **Enable Rotate** to **Clockwise 270 degrees** or **OFF**. When **OFF** is selected, the image is restored to original.
5. Select **Mirror Mode**to**Left-Right**, **Up-Down**, **Center** or **OFF**. When **OFF** is selected, the image is restored to original.

Note

- The Rotate and Mirror functions must be supported by the connected IP camera
- The image parameters adjustment can affect both the live view and the recording quality.

6. Click **Apply**.

2.4 Configure Video Parameters

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

Steps

1. Go to **Menu → Camera → Image → Image Settings**.
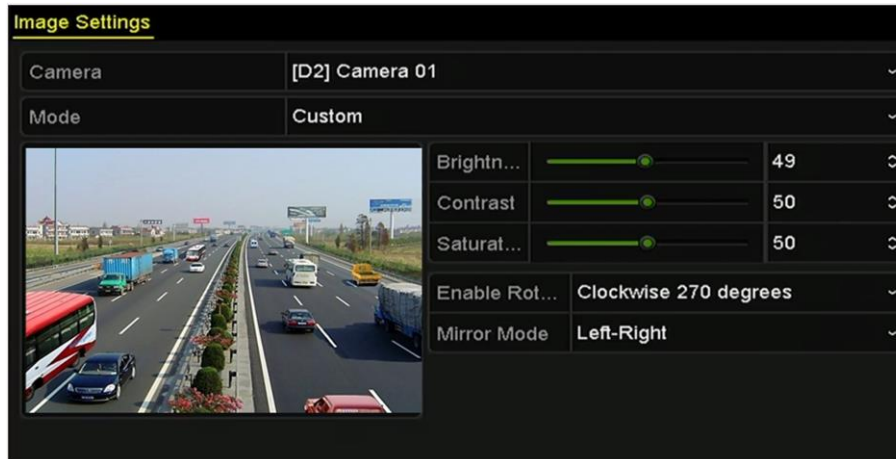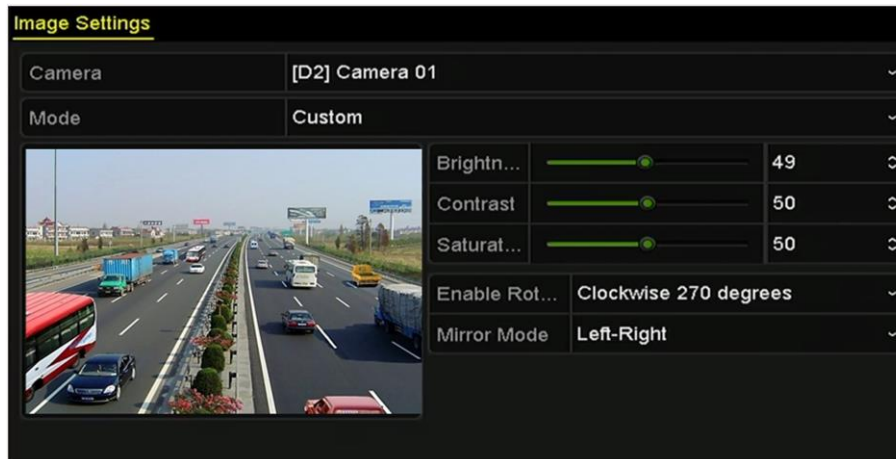
Figure 2-5 Image Settings

2. Select a camera.
3. Adjust the slider or click on the up/down arrow to set the value of the brightness, contrast or saturation.
4. Set **Enable Rotate** to **Clockwise 270 degrees** or **OFF**. When **OFF** is selected, the image is restored to original.
5. Set **Mirror Mode** to **Left-Right**, **Up-Down**, **Center** or **OFF**. When **OFF** is selected, the image is restored to original.

⊡**Note**

● Rotate and Mirror functions must be supported by the connected IP camera.
● The image parameters adjustment can affect both the live view and the recording quality.

6. Click **Apply**.

Chapter 3 Live View

3.1 Introduction of Live View

Live view shows you the video image getting from each camera in real time. The NVR automatically enters Live View mode when powered on. It is also at the very top of the menu hierarchy, thus pressing the ESC many times (depending on which menu you're on) brings you to the Live View mode.
Live View Icons

In the live view mode, there are icons at the upper-right of the screen for each channel, showing the status of the record and alarm in the channel, so that you can know whether the channel is recorded, or whether there are alarms occur as soon as possible.

Table 3-1 Description of Live View Icons

Icons	Description
🔔	Alarm (video loss, video tampering, motion detection, VCA and sensor alarm)
🎲	Record (manual record, schedule record, motion detection, VCA and alarm triggered record)
🔔🎲	Alarm and Record
⚠	Event/Exception (motion detection, VCA, sensor alarm or exception information, appears at the lower-left corner of the screen. Please refer to*Set Alarm Response Actions* for details.)

3.2 Operations in Live View Mode

In live view mode, there are many functions provided.
The functions are listed below.

Single Screen

showing only one screen on the monitor.

Multi-screen

showing multiple screens on the monitor simultaneously.

Auto-switch

the screen is auto switched to the next one. And you must set the dwell time for each screen on the configuration menu before enabling the auto-switch.

Start Recording

continuous record and motion detection record are supported.

Output Mode

select the output mode as Standard, Bright, Gentle or Vivid.

Add IP Camera

the shortcut to the IP camera management interface.

Playback

playback the recorded videos for current day.

Aux Monitor

the NVR checks the connection of the output interfaces to define the main and auxiliary output interfaces. The priority level for the main and aux output is HDMI > VGA.

When both the HDMI and VGA are connected, the HDMI is used as main output and the VGA is used as the aux output.

When the aux output is enabled, the main output cannot perform any operation, and you can do some basic operation on the live view mode for the Aux output.

3.2.1 Use the Mouse in Live View

Table 3-2 Mouse Operation in Live View

Name	Description
Common Menu	Quick access to the sub-menus which you frequently visit.
Menu	Enter the main menu of the system by right clicking the mouse.
Single Screen	Switch to the single full screen by choosing channel number from the dropdown list.
Multi-screen	Adjust the screen layout by choosing from the dropdown list.
Previous Screen	Switch to the previous screen.
Next Screen	Switch to the next screen.
Start/Stop Auto-switch	Enable/disable the auto-switch of the screens.
Start Recording	Start continuous recording or motion detection recording of all channels.
Add IP Camera	Enter the IP Camera Management interface, and manage the cameras.
Playback	Enter the playback interface and start playing back the video of the selected channel immediately.
PTZ	Enter the PTZ control interface.

Name	Description
Output Mode	Four modes of output supported, including Standard, Bright, Gentle and Vivid.
Aux Monitor	Switch to the auxiliary output mode and the operation for the main output is disabled.

Note

- The dwell time of the live view configuration must be set before using **Start Auto-switch**.
- If you enter Aux monitor mode and the Aux monitor is not connected, the mouse operation is disabled; you need to switch back to the Main output with the MAIN/AUX button on the front panel or remote.
- If the corresponding camera supports intelligent function, the Reboot Intelligence option is included when right-clicking mouse on this camera.
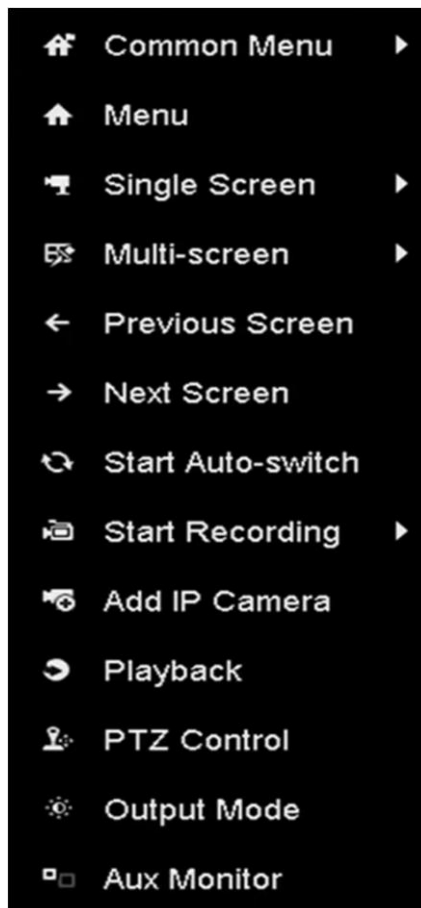

Figure 3-1 Right-click Menu

3.2.2 Use an Auxiliary Monitor

Certain features of the Live View are also available while in an Aux monitor.
● 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.

3.2.3 Quick Setting Toolbar in Live View Mode

On the screen of each channel, there is a quick setting toolbar which shows when you single click the mouse in the corresponding screen.

Figure 3-2 Quick Setting Toolbar

Table 3-3 Description of Live View Icons

Icon	Description	Icon	Description	Icon	Description
	Enable/Disable Manual Record		Instant Playback		Mute/Audio on
	Capture		PTZ Control		Digital Zoom
	Image Settings		Live View Strategy		Information
	Main/Sub-Stream		Close		

 Instant Playback only shows the record in last five minutes. If no record is found, it means there is no record during the last five minutes.
 Digital Zoom is for zooming in the live image. You can zoom in the image to different proportions (1 to16X) by moving the sliding bar from   to . You can also scroll the mouse

wheel to control the zoom in/out.

Figure 3-3 Digital Zoom

Image Settings icon can be selected to enter the Image Settings menu.
You can set the image parameters like brightness, contrast, saturation and hue according to the actual demand.

Figure 3-4 Image Settings- Customize

Live View Strategy can be selected to set strategy, including Real-time, Balanced, Fluency.
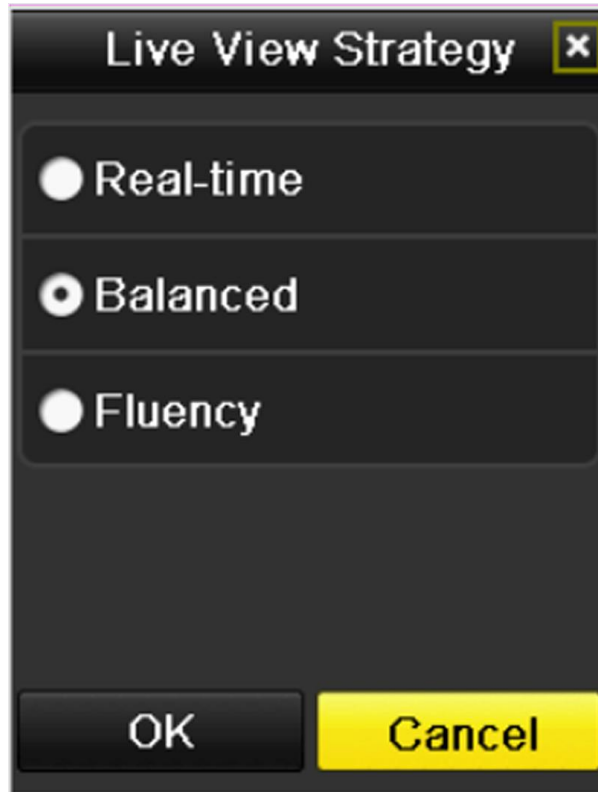
Figure 3-5 Live View Strategy

Face detection function can be used to detect the human faces in live view mode and save in HDD. When there are human faces with the specified size detected in the front of the camera, the device will capture the human face and save in HDD.

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

Figure 3-6 Information

3.3 Adjust Live View Settings

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

Steps

1. Enter the Live View Settings interface. Go to **Menu → Configuration → Live View**.
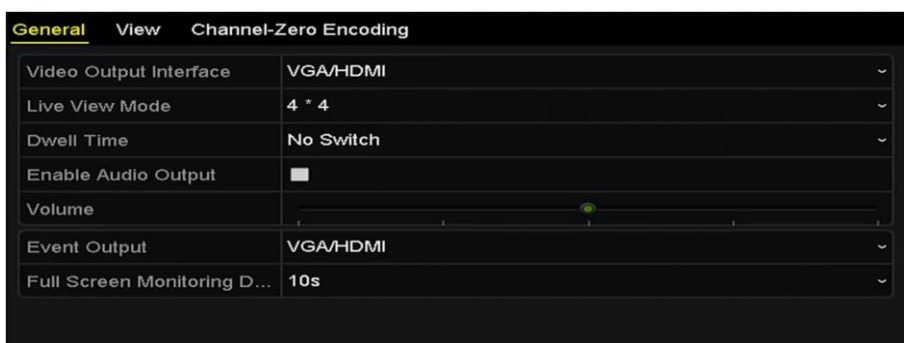
Figure 3-7 Live View-General

The settings available in this menu include:

Video Output Interface

   Select the video output to configure the live view parameters.

Live View Mode

Select the display mode to be used for live view.

Dwell Time

The time in seconds to dwell between switching of channels when enabling auto-switch in Live View.

Enable Audio Output

Enables/disables audio output for the selected video output.

Volume

Adjust the volume of live view, playback and two-way audio for the selected output interface.

Event Output

Designates the output to show event video.

Full Screen Monitoring Dwell Time

The time in seconds to show alarm event screen.

2. Set cameras order.
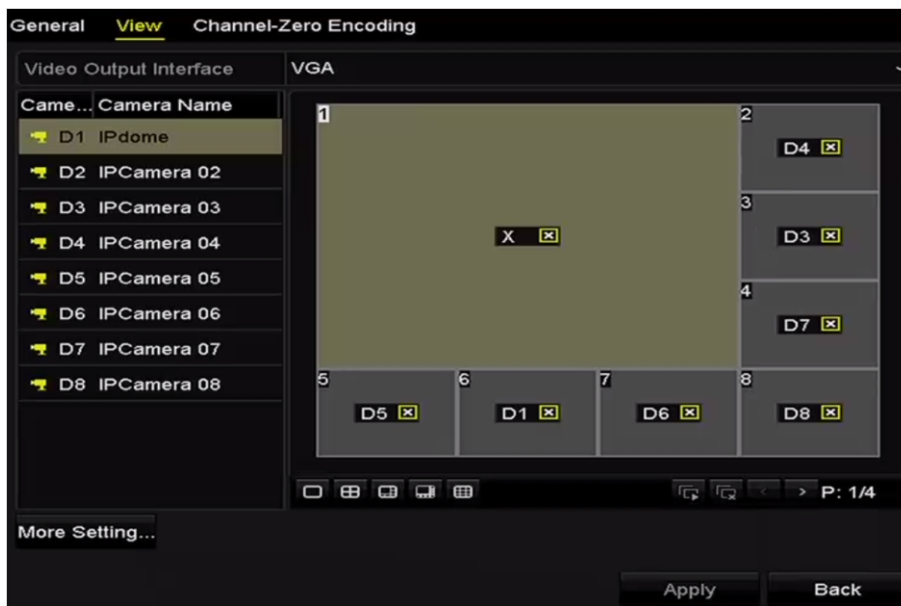
Figure 3-8 Live View-Camera Order

1) Select a View mode in [icons], including 1/4/6/8/16-window division modes are supported depending on different models.

2) Select the small window, and double-click on the channel number to display the channel on the window.

3) You can click [icon] button to start live view for all the channels and click [icon] to stop all the live view.

4) click **Apply** to save the setting.

Note

You can also click-and-drag the camera to the desired window on the live view interface to set the camera order.

3. Set the stream type for live view of camera.
   1) Click **More Settings** to enter the more settings interface.
   2) Select the camera to configure from the list.
   3) Select the stream type asmain stream, sub-stream or Auto.
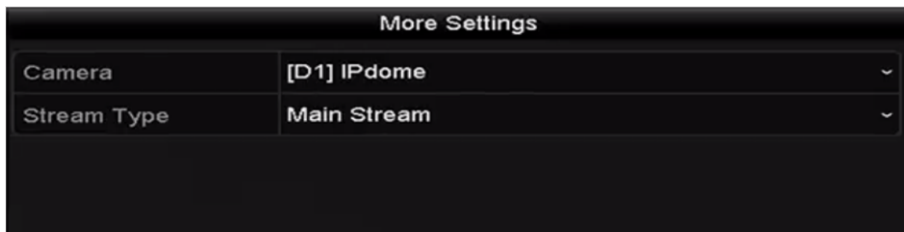
Figure 3-9 Stream Type Settings

   4) Click **Apply** to save the settings.
   5) Optional: You can click **Copy** to copy the stream type settings of the current camera to other camera (s).

3.4 Channel-Zero Encoding

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

Steps

1. Enter **Live View** Settings interface. Go to **Menu → Configuration → Live View**.
2. Select **Channel-Zero Encoding**.

Figure 3-10 Live View- Channel-Zero Encoding

3. Check **Enable Channel Zero Encoding**.
4. Configure **Frame Rate**, **Max. Bitrate Mode** and **Max. Bitrate**.

Result

After you set the Channel-Zero encoding, you can get a view in the remote client or web browser of 16 channels in one screen.

3.5 PTZ Control

3.5.1 Configure PTZ Settings

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

Steps

1. Enter the PTZ Settings interface. Go to **Menu → Camera → PTZ**.

Figure 3-11 PTZ Settings

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

Figure 3-12 PTZ- General

3. Choose the camera for PTZ setting.
4. Enter the parameters of the PTZ camera.

⊡**Note**

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

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

3.5.2 Set PTZ Presets, Patrols & Patterns

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

Customize Presets

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

Steps

1. Enter the PTZ Control interface. Go to **Menu** → **Camera** → **PTZ**.

Figure 3-13 PTZ Settings

2. Use the directional button to wheel the camera to the location where you want to set preset; and the zoom and focus operations can be recorded in the preset as well.
3. Enter the preset No. (1~255) in the preset text field, and click **Set** to link the location to the preset.

   Repeat the steps2-3 to save more presets.

4. Optional: Click **Clear** to clear the location information of the preset, or click **Clear All** to clear the location information of all the presets.

Call Presets

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

Steps

1. Click **PTZ** in the lower-right corner of the PTZ setting interface, or press the PTZ button on the front panel, or click the PTZ Control icon in the quick setting bar, or select the PTZ option in the right-click menu to show the PTZ control panel.
2. Choose **Camera**.
3. Click to show the general settings of the PTZ control.

Figure 3-14 PTZ Panel - General

4. Click to enter the preset No. in the corresponding text field.

5. Click **Call Preset** to call it.

Customize Patrols

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

Steps

1. Enter the PTZ Control interface. Go to **Menu → Camera → PTZ**.

Figure 3-15 PTZ Settings

2. Select patrol No. in the drop-down list of patrol.
3. Click **Set** to add key points for the patrol.

Figure 3-16 Key point Configuration

4. Configure key point parameters, such as the key point No., duration of staying for one key point and speed of patrol.

ℹ️**Note**

The key point is corresponding to the preset.

Key Point No.

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

Duration

   refers to the time span to stay at the corresponding key point.

Speed

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

5. Click **Add** to add the next key point to the patrol, or you can click **OK** to save the key point to the patrol.
6. Optional: You can delete all the key points by clicking **Clear** for the selected patrol, or click**Clear All** to delete all the key pints for all patrols.

Call Patrols

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

Steps

1. Click **PTZ** in the lower-right corner of the PTZ setting interface, or press the PTZ button on the front panel, or click the PTZ Control icon ![icon] in the quick setting bar, or select the PTZ option in the right-click menu to show the PTZ control panel.
2. Click the ![button] button to show the general settings of the PTZ control.

Figure 3-17 PTZ Panel - General

3. Select a patrol and click **Call Patrol** to call it.
4. You can click **Stop Patrol** to stop calling it.

Customize Patterns

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

Steps

1. Go to **Menu → Camera → PTZ**, and enter the PTZ Control interface.

Figure 3-18 PTZ Settings

2. Choose pattern number.
3. Click **Start** and click corresponding buttons in the control panel to move the PTZ camera, and click **Stop** to stop it.

The movement of the PTZ is recorded as the pattern.

Call Patterns

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

Steps

1. Click **PTZ** in the lower-right corner of the PTZ setting interface, or press the PTZ button on the front panel, or click the PTZ Control icon in the quick setting bar, or select the PTZ option in the right-click menu to show the PTZ control panel.
2. Click to show the general settings of the PTZ control.

Figure 3-19 PTZ Panel - General

3. Click **Call Pattern** to call it.

4. Click **Stop Pattern** to stop calling it.

Customize Linear Scan Limit

The Linear Scan can be enabled to trigger the scan in the horizantal direction in the predefined range.

ⓘ**Note**

This function is supported by some certain models.

Steps

1. Go to **Menu → Camera → PTZ**, enter the PTZ Control interface.

Figure 3-20 PTZ Settings

2. Use the directional button to wheel the camera to the location where you want to set the limit, and click **Left Limit** or **Right Limit** to link the location to the corresponding limit.

⚠️**Note**

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

Call Linear Scan

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

Before You Start

Make sure the connected camera supports the linear scan and is in HIKVISION protocol.

Steps

1. Click **PTZ** in the lower-right corner of the PTZ setting interface, or press the PTZ button on the front panel, or click 🖥 in the quick setting bar to enter the PTZ setting menu in live view mode.
2. Click ▶ to show the one-touch function of the PTZ control.

Figure 3-21 PTZ Panel - One-touch

3. Click **Linear Scan** to start the linear scan and click the Linear Scan button again to stop it
4. You can click **Restore** to clear the defined left limit and right limit data and the dome needs to reboot to make settings take effect.

3.5.3 PTZ Control Panel

To enter the PTZ control panel, there are two ways supported.
● Option 1: In the PTZ settings interface, click the **PTZ** button on the lower-right corner which is next to the Back button.
● Option 2:In the Live View mode, you can press the PTZ Control button on the front panel or on the remote control, or choose , or select the PTZ option in the right-click menu.
  Click **Configuration** on the control panel, and you can enter the PTZ Settings interface.

Note

In PTZ control mode, the PTZ panel will be displayed when a mouse is connected with the device. If no mouse is connected, the PTZ appears in the lower-left corner of the window, indicating that this camera is in PTZ control mode.

Figure 3-22 PTZ Panel1

Figure 3-23 PTZ Panel2

Figure 3-24 PTZ Panel3

Table 3-4 Description of the PTZ panel icons

Icon	Description	Icon	Description	Icon	Description
	Direction button and the auto-cycle button	+	Zoom+, Focus+, Iris+	−	Zoom-, Focus-, Iris-
	The speed of the PTZ movement		Light on/off		Wiper on/off
3D	3D Positioning		Image Centralization		Menu
PTZ Control	Switch to the PTZ control interface	One-touch	Switch to the one-touch control interface	General	Switch to the general settings interface
	Previous item		Next item		Start pattern / patrol
	Stop the patrol / pattern movement	x	Exit		Minimize windows

Chapter 4 Recording

4.1 Configure Parameters

By configuring the parameters you can define the parameters which affect the image quality, such as the transmission stream type, the resolution and so on.

Before You Start

Make sure that the HDD has already been installed. If not, please install a HDD and initialize it. (**Menu → HDD → General**)
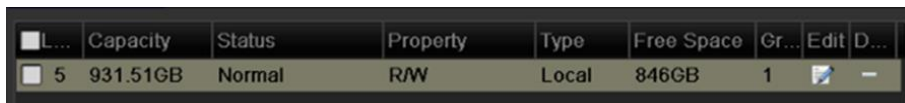
Figure 4-1 HDD-General

1. Check the storage mode of the HDD.If the HDD mode is **Quota**, please set the maximum record capacity and maximum picture capacity. For detailed information, see *Configure Quota Mode*.

Steps

1. Enter the Record settings interface to configure the recording parameters: **Menu → Record → Parameters**.
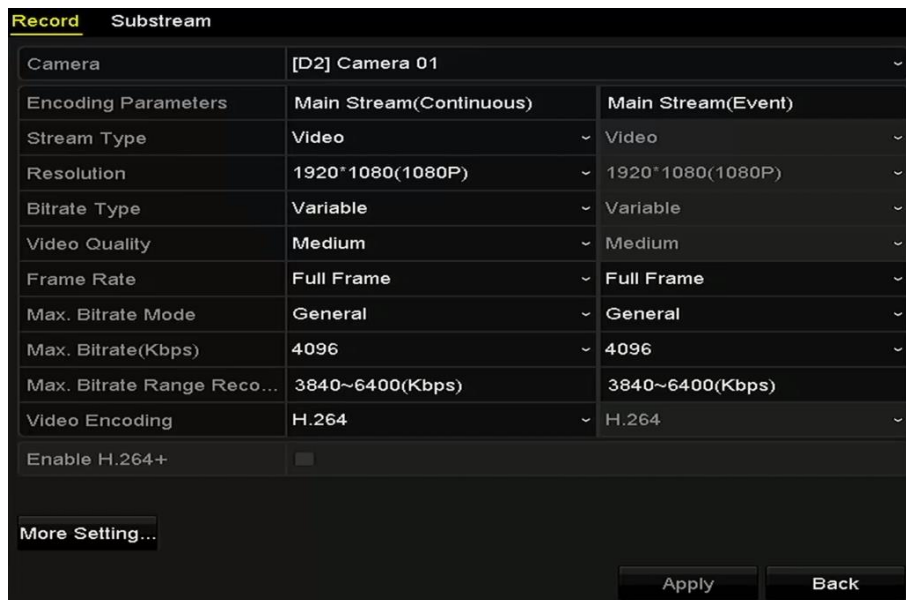
Figure 4-2 Recording Parameters

2. Set recording parameters.
    1. Select **Record**. You can configure the stream type, the resolution, and other parameters on

your demand.

Video Encode

select the video encoding to H.265 or H.264.

Enable H.264+ Mode

check the checkbox to enable. Once enabled, the **Max. Bitrate Mode**, **Max. Bitrate(Kbps)** and **Max. Bitrate Range Recommend** are not configurable. Enabling it helps to ensure the high video quality with a lowered bitrate.

☐**i Note**

The H.265 and H.264+ should be supported by the connected IP camera.

2. Click **More Settings** to set the advanced parameters for recording and then click **OK** to finish editing.
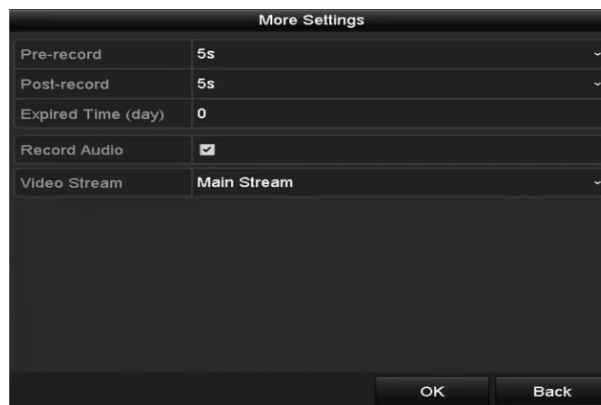
Figure 4-3 More Settings

Pre-record

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

Post-record

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

Expired Time

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

Redundant Record/Capture

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

Record Audio

Check the checkbox to enable or disable audio recording.

Video Stream

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

3. Click **Apply**.
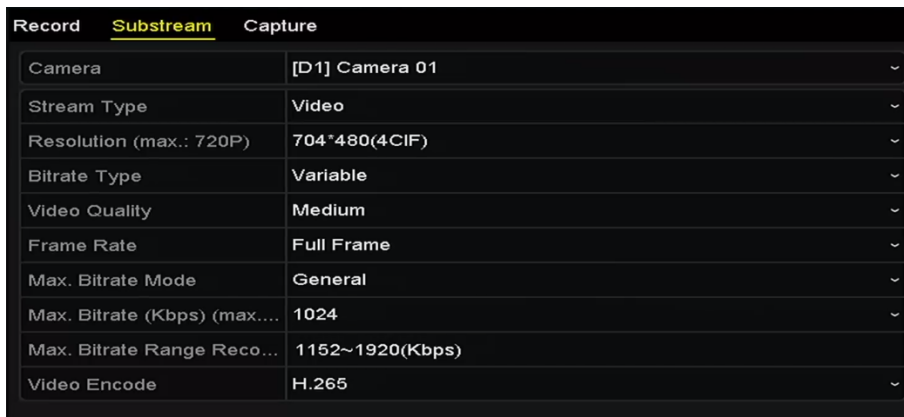
ℹ️**Note**

● The **redundant record/capture** is used when you want to save the record files or captured pictures in the redundant HDD.
● The parameters of **Main Stream (Event)** are read-only.
● You can enable the ANR (Automatic Network Replenishment) function via the web browser (**Configuration** → **Storage** → **Schedule Settings** → **Advanced**) to save the video files in the IP camera when the network is disconnected, and synchronize the files to the NVR when the network is resumed.

---

3. Set Sub-stream Parameters.
    1. Enter the **Substream** tab page.

Record	Substream	Capture
Camera	[D1] Camera 01	
Stream Type	Video	
Resolution (max.: 720P)	704*480(4CIF)	
Bitrate Type	Variable	
Video Quality	Medium	
Frame Rate	Full Frame	
Max. Bitrate Mode	General	
Max. Bitrate (Kbps) (max....	1024	
Max. Bitrate Range Reco...	1152~1920(Kbps)	
Video Encode	H.265	

Figure 4-4 Sub-stream Parameters

    2. Configure the parameters of the camera.
    3. Click **Apply**.

4.2 Configure Recording Schedule

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

we take the record schedule procedure as an example, and the same procedure can be applied to configure schedule for both recording and capture. To schedule the automatic capture, you need to choose the Capture tab in **Schedule** interface.

Steps
1. Go to **Menu** → **Record** → **Schedule**.
2. Configure recording schedule.
    1. Select **Record Schedule**. Different recording types are marked in different color icons.

    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.

    ⎕ⓘNote
    You can delete the set schedule by clicking **None**.

    2. Choose the camera you want to configure.
    3. Select the check box after **Enable Schedule**.
    4. Click **Edit** or click on the color icon under the edit button and draw the schedule line on the panel.
    ● Edit the schedule.
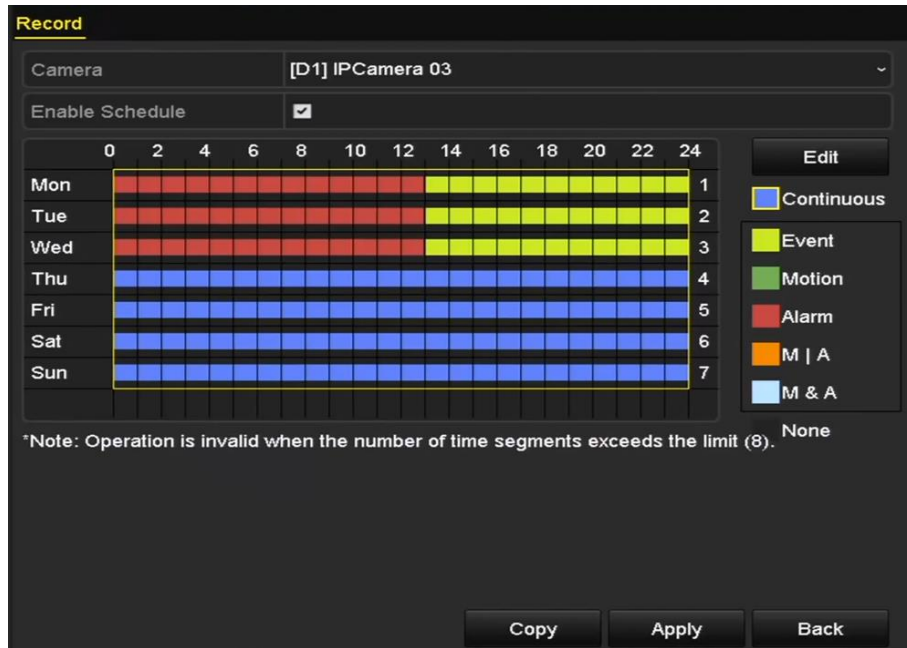
Figure 4-5 Recording Schedule Interface

ⓘ**Note**

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

● In the message box, you can choose the day to which you want to set schedule.
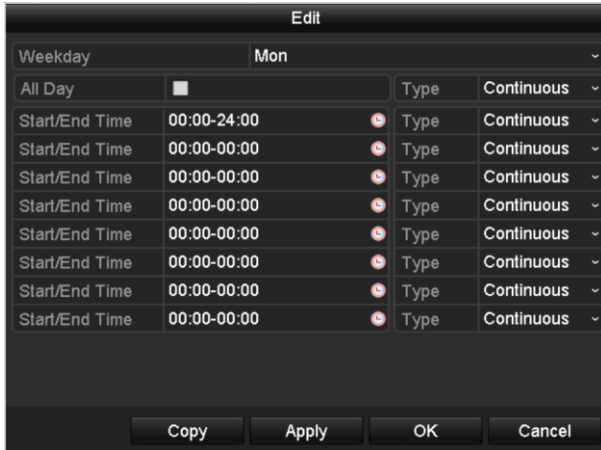
You can click 🕐 to set the accurate time

of the schedule.
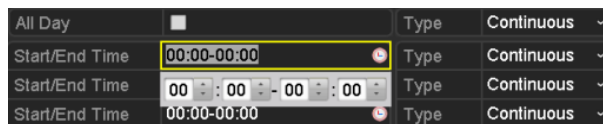● To schedule an all-day recording, check **All Day**.

Figure 4-6 Edit Schedule

● To arrange other schedule, set **Start/End time** for each period.

> ⓘ**Note**
>
> Up to 8 periods can be configured for each day. And the time periods can't be overlapped each other.

- Select the record type.

> ⓘ**Note**
>
> ○ To enable **Motion**, **Alarm**, **M | A** (motion or alarm), **M & A** (motion and alarm) and VCA (Video Content Analysis) triggered recording and capture, you must configure the motion detection settings, alarm input settings or VCA settings as well. For detailed information, refer to *Set Motion Detection Alarm* and *VCA Alarm*.
> ○ The VCA settings are only available to the smart IP cameras. Repeat the above edit schedule steps to schedule recording or capture for other days in the week. If the schedule can also be applied to other days, click **Copy**.
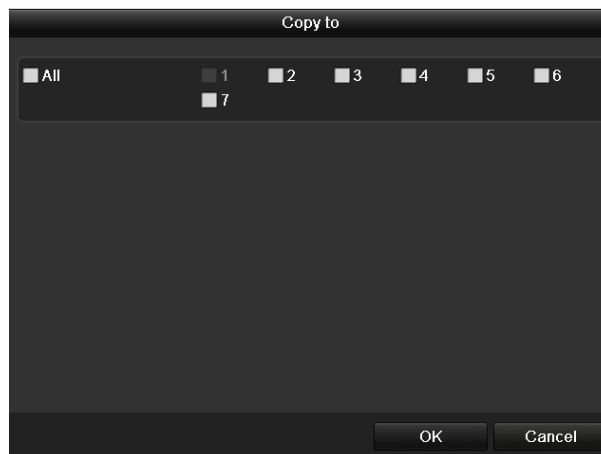
Figure 4-7 Copy Schedule to Other Days

- Click **OK** to save setting and back to upper level menu.
- Click **Apply** in the Record Schedule interface to save the settings.
- Draw the schedule.
  - Click on the color icons, you can choose the schedule type as continuous or event.
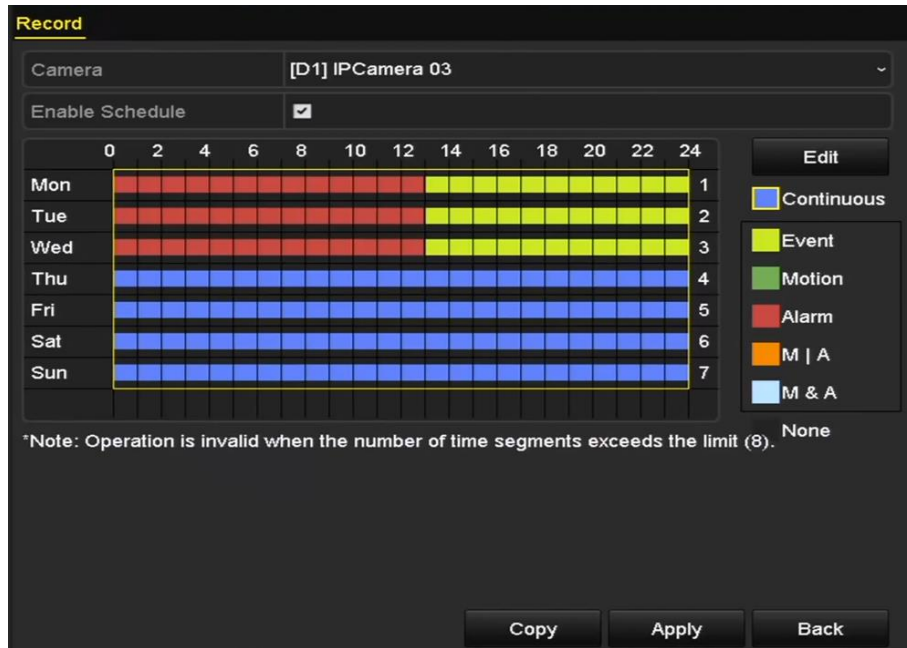
Figure 4-8 Draw the Schedule

● Click the **Apply** button to validate the settings.

3. Optional: If the settings can also be used to other channels, click **Copy**, and then choose the channel to which you want to copy.
4. Click **Apply** to save the settings.

Figure 4-9 Copy Schedule to Other Channels

4.3 Configure Motion Detection Recording

Follow the steps to set the motion detection. In the live view mode, once a motion detection event takes place, the NVR can analyze it and take alarm response actions. Enabling motion

detection function can trigger certain channels to start recording, or trigger full screen monitoring, audio warning, notify the surveillance center and so on. In this chapter, you can follow the steps to schedule a record which triggered by the detected motion.

Steps

1. Go to **Menu → Camera → Motion**.

Figure 4-10 Motion Detection

2. Configure Motion Detection.
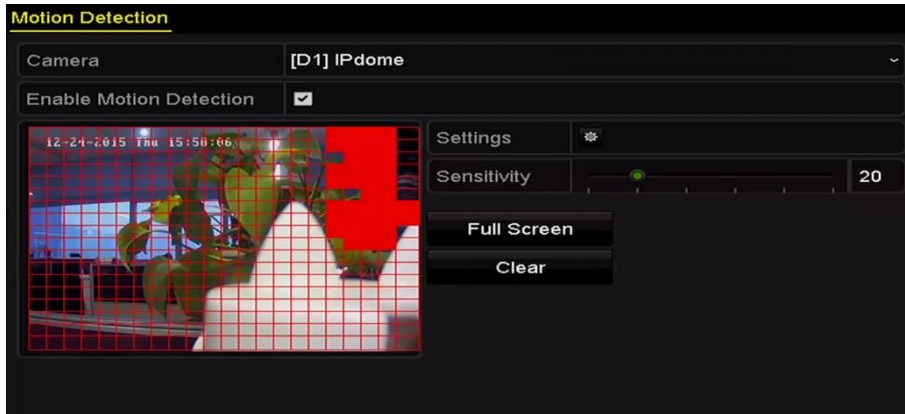   1) Choose camera you want to configure.
   2) Check the checkbox after **Enable Motion Detection**.
   3) Drag and draw the area for motion detection by mouse. If you want to set the motion detection for all the area shot by the camera, click **Full Screen**. To clear the motion detection area, click **Clear**.
   4) Click **Settings**, and the message box for channel information pops up.
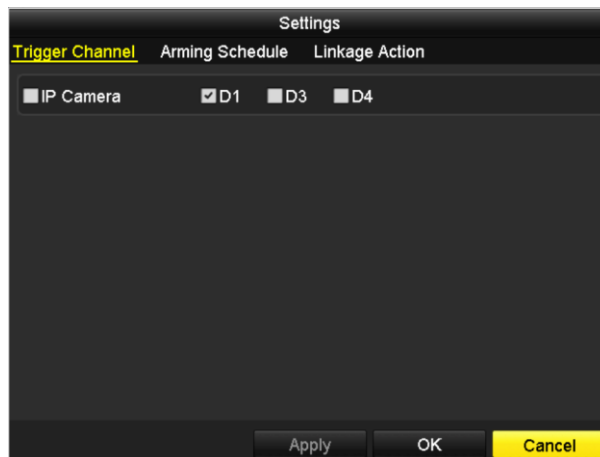
Figure 4-11 Motion Detection Handling

1. Select the channels which you want the motion detection event to trigger recording.
2. Click **Apply** to save the settings.
3. Click **OK** to back to the upper level menu.
4. Exit the Motion Detection menu.

3. Edit the Motion Detection Record Schedule. For the detailed information of schedule configuration, see **Configure Recording Schedule**.

4.4 Configure Alarm Triggered Recording

Follow the procedure to configure alarm triggered recording.

Steps

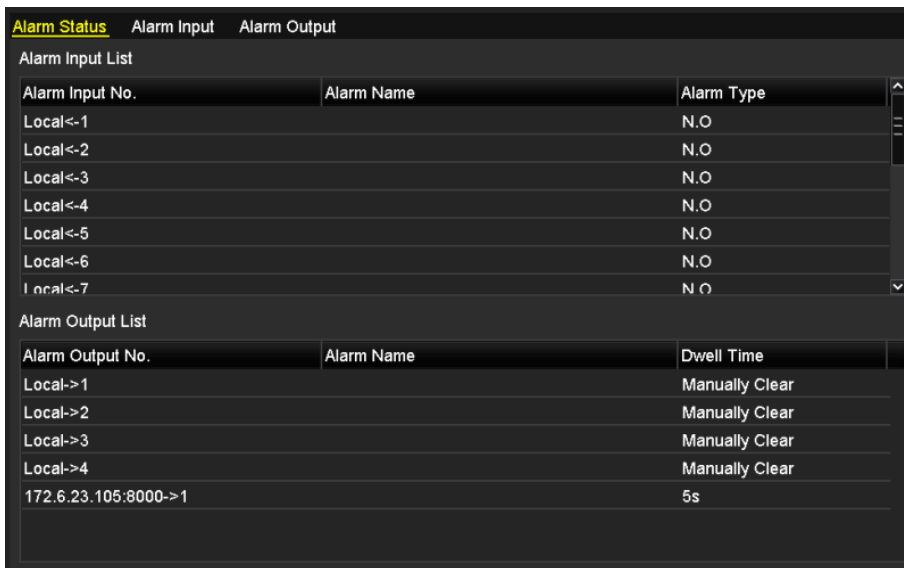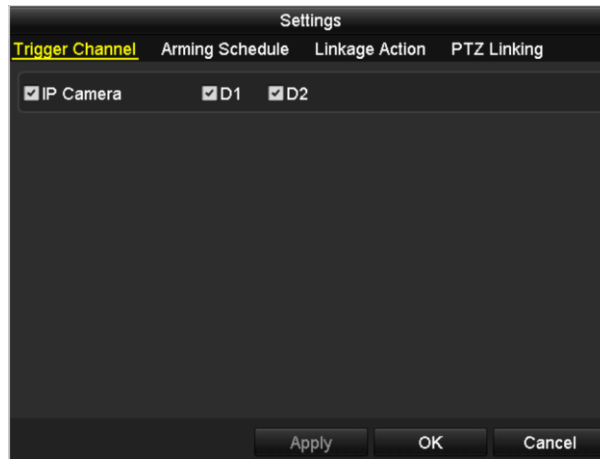1. Go to **Menu** → **Configuration** → **Alarm**.

Figure 4-12 Alarm Settings

2. Click **Alarm Input**.

Figure 4-13 Alarm Settings- Alarm Input

1) Select Alarm Input number and configure alarm parameters.
2) Choose **N.O** (normally open) or **N.C** (normally closed) for alarm type.
3) Check the checkbox.
4) Click **Settings**.

Figure 4-14 Alarm Settings

1. Choose the alarm triggered recording channel.
2. Check the checkbox to select channel.
3. Click **Apply** to save settings.
4. Click **OK** to back to the upper level menu.

5) Repeat the above steps to configure other alarm input parameters.
6) If the settings can also be applied to other alarm inputs, click **Copy** and choose the alarm input number.
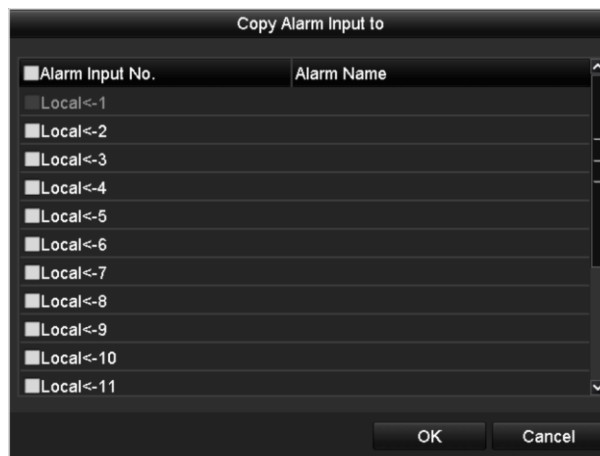
Figure 4-15 Copy Alarm Input

3. Edit the Alarm triggered record in the Record/Capture Schedule setting interface. For the detailed information of schedule configuration, see ***Configure Recording Schedule***.

4.5 Configure VCA Event Recording

The event triggered recording can be configured through the menu. Then events include the motion detection, alarm and VCA events (face detection/face capture, line crossing detection,

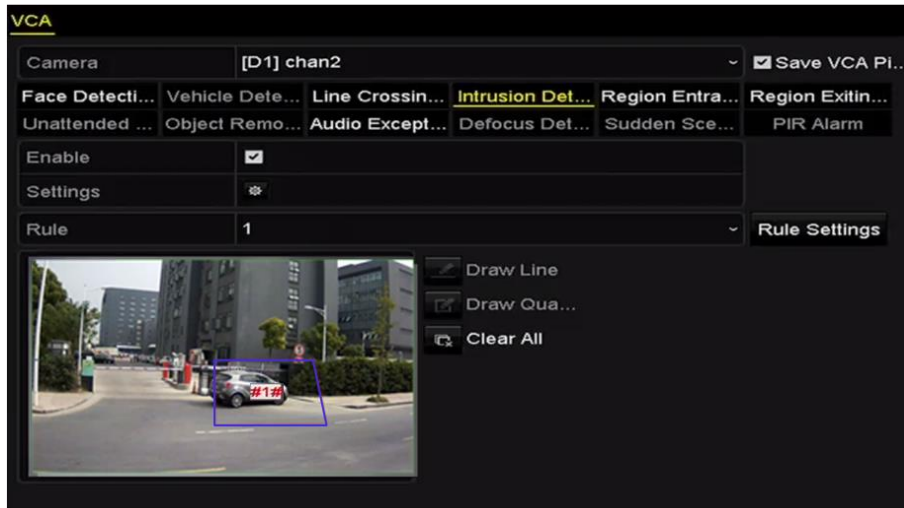intrusion detection, region entrance detection, region exiting detection, loitering detection, people gathering detection, fast moving detection, parking detection, unattended baggage detection, object removal detection, audio loss exception detection, sudden change of sound intensity detection, and defocus detection).

Steps

1. Go to **Menu → Camera → VCA**.

Figure 4-16 VCA Settings

2. Configure the detection rules for VCA events. For details, please refer to ***Chapter 9 VCA Alarm***.
3. Click   to configure the alarm linkage actions for the VCA events.
4. Select **Trigger Channel** and select one or more channels which will start to record when VCA alarm is triggered.
5. Click **Apply** to save the settings.
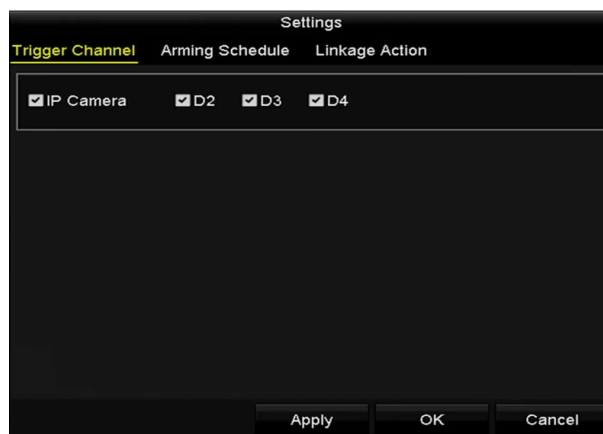
Figure 4-17 Set Trigger Camera of VCA Alarm

 Note

The PTZ Linking function is only available for the VCA settings of IP cameras.

6. Go to **Menu → Record → Schedule → Record Schedule**, and then set VCA as the record type. For details, see step 2 in ***Configure Recording Schedule***.

4.6 Manual Recording

Follow the steps to set parameters for the manual recording and continuous capture. Using manual recording and continuous capture, you need to manually cancel the record and capture. The manual recording and manual continuous capture is prior to the scheduled recording and capture.

Steps

1. Go to **Menu → Manual**.

Figure 4-18 Manual Record

2. Enable the Manual Recording.
   1) Select **Record**.
   2) Click the status button before camera number to change [OFF] to [ON].
3. Disable manual record.Click the status button to change [ON] to [OFF].

> **Note**
>
> [ON] means that the channel is configured the record schedule.After rebooting, all the manual records enabled will be canceled.

4.7 Configure Redundant Recording

Enabling redundant recording, 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.

Steps

1. Go to **Menu → HDD**.

Figure 4-19 HDD General

2. Select the HDD and click [icon] to enter the Local HDD Settings interface.
   1) Set the HDD property to Redundancy.

Figure 4-20 HDD General-Editing

2) Click **Apply** to save the settings.
3) Click **OK** to back to the upper level menu.

[i]**Note**

You must set the Storage mode in the HDD advanced settings to Group before you set the HDD property to Redundant. For detailed information, please refer to . There should be at least another HDD which is in Read/Write status.

3. Go to **Menu → Record → Parameters**.
   1) Select **Record**.
   2) Click **More Settings**.

Figure 4-21 Record Parameters

3) Select Camera you want to configure in the drop-down list.

4) Check the checkbox of **Redundant Record/Capture**.

5) Click **OK** to save settings and back to the upper level menu.

6) Repeat the above steps for configuring other channels.

4.8 Configure Holiday Recording

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

Steps

1. Go to **Menu → Record → Holiday**.

Figure 4-22 Holiday Settings

2. Enable Edit Holiday schedule.
   1) Click ![edit icon] to enter the Edit interface.

Figure 4-23 Edit Holiday Settings

2) Check the checkbox after **Enable Holiday**.
3) Select **Mode** from the dropdown list.
4) There are three different modes for the date format to configure holiday schedule.
5) Set the start and end date.
6) Click **Apply** to save settings.
7) Click **OK** to exit the Edit interface.

3. Enter Record/Capture Schedule settings interface to edit the holiday recording schedule. See *Configure Recording Schedule*.

4.9 Files Protection

You can lock the recording files or set the HDD property to Read-only to protect the record files from being overwritten.

4.9.1 Lock the Recording Files

Lock File when Playback

Steps

1. Go to **Menu → Playback**.
2. Check the checkbox of channel(s) in the channel list and then double-click to select a date on the calendar.

Figure 4-24 Normal/Smart Playback

3. During playback, click [icon] to lock the current recording file.

[i]**Note**

In the multi-channel playback mde, clicking [icon] will lock all the record files related to the playback channels.

4. You can click [icon] to pop up the file management interface. Click the Locked File tab to check and export the locked files.

Figure 4-25 Locked File Management

In the File Management interface, you can also click to change it to to unlock the file and the file is not protected.

Lock File when Export

Steps

1. Go to **Menu → Export**.
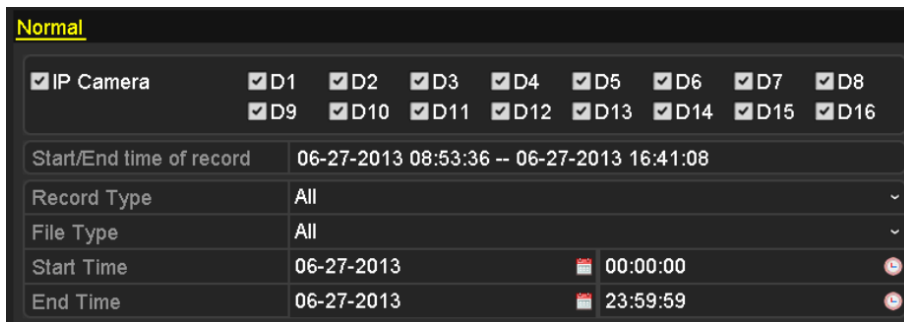
Figure 4-26 Export

2. Select the channels you want to search.
3. Configure the record type, file type start/end time.
4. Click **Search** to show the results.

Figure 4-27 Export- Search Result

5. Protect the record files.
    1) Find the record files you want to protect, and then click ![icon] which will turn to![icon], indicating that the file is locked.

ⓘ**Note**

The record files of which the recording is still not completed cannot be locked.

---

    2) Click ![icon] to change it to ![icon] to unlock the file and the file is not protected.

4.9.2 Set HDD Property to Read-only

Steps

1. Go to **Menu → HDD**.
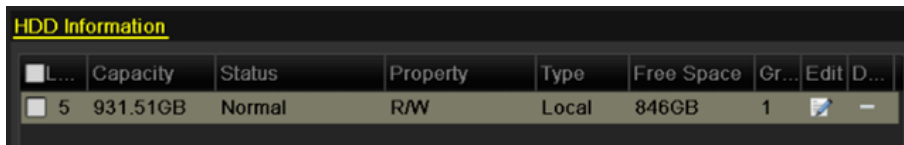
Figure 4-28 HDD General

2. Click ![icon] to edit the HDD you want to protect.

Figure 4-29 HDD General- Editing

ⓘ**Note**

To edit HDD property, you need to set the storage mode of the HDD to Group.

3. Set the HDD property to Read-only.
4. Click **OK** to save settings and back to the upper level menu.

ⓘ**Note**

● You cannot save any files in a Read-only HDD. If you want to save files in the HDD, change the property to R/W.
● If there is only one HDD and is set to Read-only, the NVR can't record any files. Only live view mode is available.
● If you set the HDD to Read-only when the NVR is saving files in it, then the file will be saved in next R/W HDD. If there is only one HDD, the recording will be stopped.

Chapter 5 Playback

5.1 Play Back Record Files

5.1.1 Instant Playback

Play back the recorded video files of a specific channel in the live view mode. Channel switch is supported.

Before You Start

Enter the prerequisites here (optional).

Enter the context of your task here (optional).

Steps

1. Choose a channel in live view mode.
2. click ![icon] in the quick setting toolbar.

Note

In the instant playback mode, only record files recorded during the last five minutes on this channel will be played back.

Figure 5-1 Instant Playback Interface

5.1.2 Play Back by Normal Search

5.1.3 Play Back by Smart Search

The smart playback function provides an easy way to get through the less effective information. When you select the smart playback mode, the system will analyze the video containing the motion, line or intrusion detection information, mark it with green color and play it in the normal speed while the video without motion will be played in the 16-time speed. The smart playback rules and areas are configurable.

Steps

1. Go to **Menu → Playback**.
2. Select the **Normal/Smart** in the drop-down list on the top-left side.
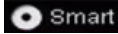
> ℹ️**Note**
>
> The main stream or sub stream for recording is configurable in **Menu → Record → Parameters**.

3. Select a camera in the camera list.
4. Select a date in the calendar and click ▶ on the left toolbar to play the video file.

Figure 5-2 Playback by Smart Search

5. Click ⊙ Smart radio button to switch to the playback by smart search.
6. Set the rules and areas for smart search of line crossing detection, intrusion detection or motion detection event triggered recording.
   - Line Crossing Detection:Select ↘ , and click on the image to specify the start point and end point of the line.
   - Intrusion Detection:Click ◇ , and specify 4 points to set a quadrilateral region for intrusion detection. Only one region can be set.
   - Motion Detection:Click ▦ , and then hold the mouse on the image to draw the detection area

manually. You can also click ⊞ to set the full screen as the detection area.

7. Optional: You can click ▼ to filter the searched video files by setting the target characters, including the gender and age of the human and whether he/she wears glasses.

Figure 5-3 Set Result Filter

5.1.4 Play Back by Event Search

Play back record files on one or several channels searched out by event type (e.g., alarm input, motion detection and VCA).

Steps

1. Go to **Menu → Playback**.
2. Select **Event** in the drop-down list on the top-left side.
3. Select the major type to **Alarm Input**, **Motion**, or **VCA** as the event type.

ℹ️**Note**

We take playback by VCA as the example in the following instructions.

Figure 5-4 Event Search Interface

4. Select the minor type of VCA from the drop-down list.
5. Select the camera (s) for searching, and set the Start time and End time.

6. Click **Search** to get the search result information. You may refer to the right-side bar for the result.

7. Select a result item and click ![play icon] to play back the file.

ℹ️Note

Pre-play and post-play can be configured.

8. Optional: Enter the Synch Playback interface to select the camera (s) for synchronous playback.
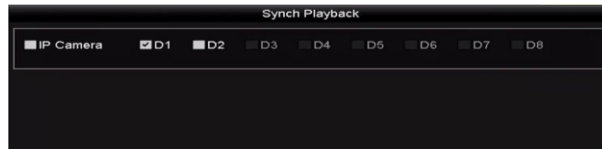
Figure 5-5 Synch Playback Interface

9. Enter the playback interface.The toolbar in the bottom part of playback interface can be used to control playing process.You can click ![left arrow] or ![right arrow] to select the previous or next event.

Figure 5-6 Interface of Playback by Event

5.1.5 Play Back by Tag

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

Before Playing Back by Tag

Steps

1. Go to **Menu → Playback**.
2. Search and play back the record file(s).

Figure 5-7 Interface of Playback by Time

● Click [icon] to add default tag.

Click [icon] to add customized tag and input tag name.

---

[i]**Note**

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

---

3. Tag management.Click [icon] to enter the File Management interface and click **Tag** to manage the tags. You can check, edit, and delete tag(s).

Figure 5-8 Tag Management Interface

Play Back by Tag

Steps

1. Select **Tag** from the drop-down list in the Playback interface.
2. Select the stream to Main Stream or Sub Stream.
3. Choose channels, edit start time and end time, and then click **Search** to enter Search Result interface.

📖**Note**

You can enter keyword to search the tag on your command.

---

4. Click ⓞ to play back the selected tag file.

Figure 5-9 Interface of Playback by Tag

5.1.6 Play Back by System Logs

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

Steps

1. Go to **Menu → Maintenance → Log Information**.
2. Click **Log Search** to enter Playback by System Logs.
3. Set search time and type and click **Search**.
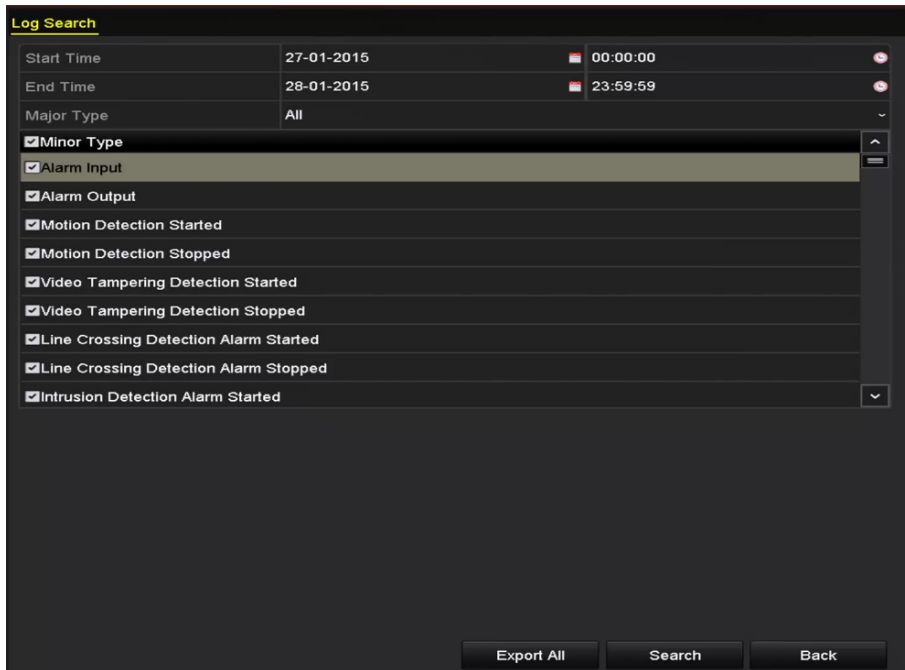
Figure 5-10 System Log Search Interface

4. Choose a log with record file and click ⊙ to enter Playback interface.
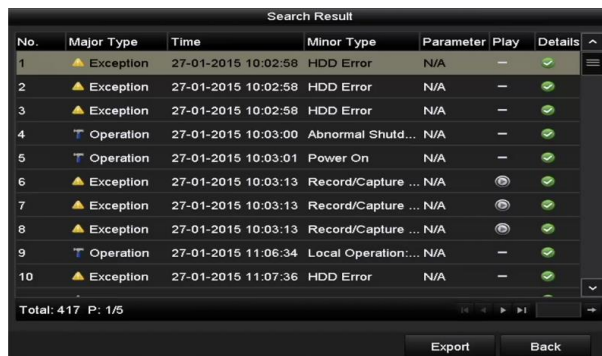
Figure 5-11 Result of System Log Search

The toolbar in the bottom part of Playback interface can be used to control playing process.

Figure 5-12 Interface of Playback by Log

5.1.7 Play Back External File

Perform the following steps to look up and play back files in the external devices.

Steps

1. Go to **Menu → Playback**.
2. Select **External File** in the drop-down list on the top-left side.

⃞**i**Note

- The files are listed in the right-side list.
- You can click 🔄 Refresh to refresh the file list.

---

3. Select and click ⊚ to play back it. And you can adjust the playback speed by clicking ⏩ and ⏪.

Figure 5-13 Interface of External File Playback

5.1.8 Play Back by Sub-periods

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

Steps

1. Go to **Menu → Playback**.
2. Select **Sub-periods** at the upper-left corner.
3. Select a date and start playing the video file.
4. Set **Split-screen Number**. Up to 16 screens are available.

Figure 5-14 Sub-periods Playback

⊡**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.

5.2 Auxiliary Functions of Playback

5.2.1 Play Back Frame by Frame

Play video files frame by frame, in case of checking image details of the video when abnormal events happen.
Go to Playback interface.
● If you choose playback of the record file: click ⏪ until the speed changes to Single frame and one click on the playback screen represents playback of one frame.
● If you choose reverse playback of the record file: click ⏪ until the speed changes to Single frame and one click on the playback screen represents reverse playback of one frame. It is also feasible to use ⏸ in toolbar.

5.2.2 Fast View

You can hold the mouse to drag on the time bar to get the fast view of the video files.

Steps

1. Enter the playback interface and start to play the video files.
2. Use the mouse to hold and drag through the playing time bar to fast view the video files.
3. Release the mouse to the required time point to enter the full-screen playback.

⊡**Note**

The fast view is supported only in the 1X single-camera playback mode.

5.2.3 Digital Zoom

Steps

1. Click 🔍 on the playback control bar to enter Digital Zoom interface.
2. You can zoom in the image to different proportions (1 to16X) by moving the sliding bar from ⊖ to . You can also scroll the mouse wheel to control the zoom in/out.

Figure 5-15 Draw Area for Digital Zoom

3. Right-click the image to exit the digital zoom interface.

5.2.4 File Management

You can manage the video clips, captured pictures in playback, locked files and tags you have

added in the playback mode.

Steps

1. Enter the playback interface.
2. Click ⚙ on the toolbar to enter the file management interface.

Figure 5-16 File Management

3. You can view the saved video clips, lock/unlock the files and edit the tags which you added in the playback mode.
4. If required, select the items and click **Export All** or **Export** to export the clips/pictures/files/tags to local storage device.

Chapter 6 Backup
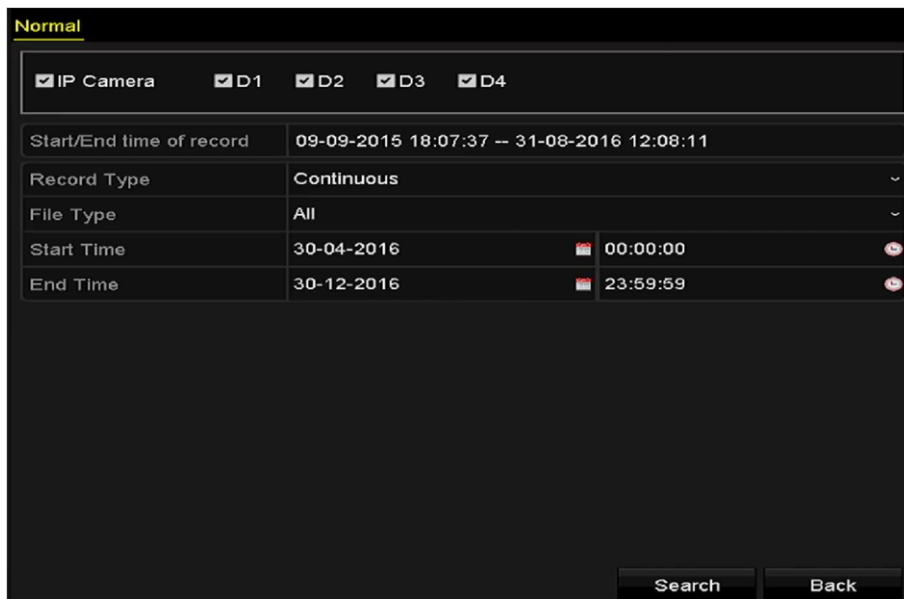
6.1 Back up Record Files

6.1.1 Back up by Normal Video Search

The record files can be backup to various devices, such as USB devices (USB flash drives, USB HDDs, USB writer), or SATA writer.

Steps

1. Go to **Menu → Export → Normal**.
2. Select the cameras to search.
3. Set search condition and click **Search** to enter the search result interface. The matched video files or pictures are displayed in Chart or List display mode.

Figure 6-1 Normal Video Search for Backup

4. Select video files or pictures from the Chart or List to export.

ⓘNote

The size of the currently selected files is displayed in the lower-left corner of the window.

Figure 6-2 Result of Normal Video Search for Backup

5. Export the video files or picture files. Click **Export All** to export all the files.Or you can select recording files you want to back up, and click **Export** to enter Export interface.

ⓘNote

If the inserted USB device is not recognized:
- Click **Refresh**.
- Reconnect device.
- Check for compatibility from vendor.

You can also format USB flash drives or USB HDDs via the device.

Figure 6-3 Export by Normal Video Search using USB Flash Drive

The backup of video files using USB writer or SATA writer has the same operating instructions. Please refer to steps described above.

6.1.2 Back up by Event Search

Back up event-related record files using USB devices (USB flash drives, USB HDDs, USB writer), SATA writer or eSATA HDD. Quick Backup and Normal Backup are supported.

Steps

1. Go to **Menu → Export → Event**.
2. Select the cameras to search.
3. Select the event type to alarm input, motion, or VCA.
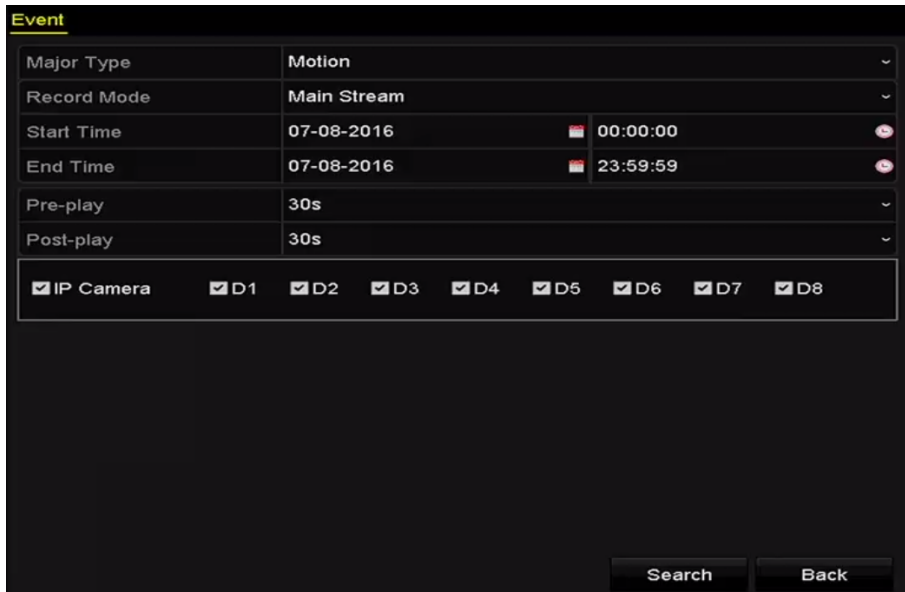
Figure 6-4 Event Search for Backup

4. Set the search conditions and click **Search** to enter the search result interface. For the POS event type, you can also set the Keyword and enable the Case Sensitivity (upper case and lower case) to search the video files with the key word contained POS information.
5. The matched video files are displayed in Chart or List display mode. Select video files from the Chart or List interface to export.
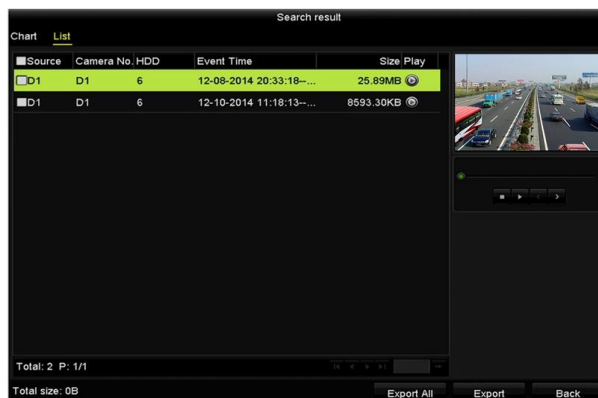
Figure 6-5 Result of Event Search

6. Export the video files. Please refer to *Back up by Normal Video Search*.

6.1.3 Back up Video Clips

You may also select video clips in playback mode to export directly during Playback, using USB devices (USB flash drives, USB HDDs, USB writer), SATA writer or eSATA HDD.

Steps

1. Enter Playback interface.
2. During playback, use ![icon] or ![icon] in the playback toolbar to start or stop clipping record file (s); or use ![icon] to capture pitcures.
3. Click ![icon] to enter the file management interface.

Figure 6-6 Video Clips or Captured Pictures Export Interface

4. Export the video clips or captured pictures in playback.Please refer to *Back up by Normal Video Search* for details.

6.2 Manage Backup Devices

Management of USB flash drives, USB HDDs and eSATA HDDs.

Steps

1. Enter the Export interface.

Figure 6-7 Storage Device Management

2. Backup device management.
    ● Click **New Folder** if you want to create a new folder in the backup device.
    ● Select a record file or folder in the backup device and click 🗑 if you want to delete it.
    ● Click **Erase** if you want to erase the files from a re-writable CD/DVD.
    ● Click **Format** button to format the backup device.

ⓘNote

If the inserted storage device is not recognized:
    ● Click **Refresh**.
    ● Reconnect device.
    ● Check for compatibility from vendor.

Chapter 7 Event and Alarm

7.1 Normal Event Alarm

7.1.1 Set Motion Detection Alarm

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

Steps

1. Go to **Menu → Camera → Motion** and choose a camera you want to set up motion detection.
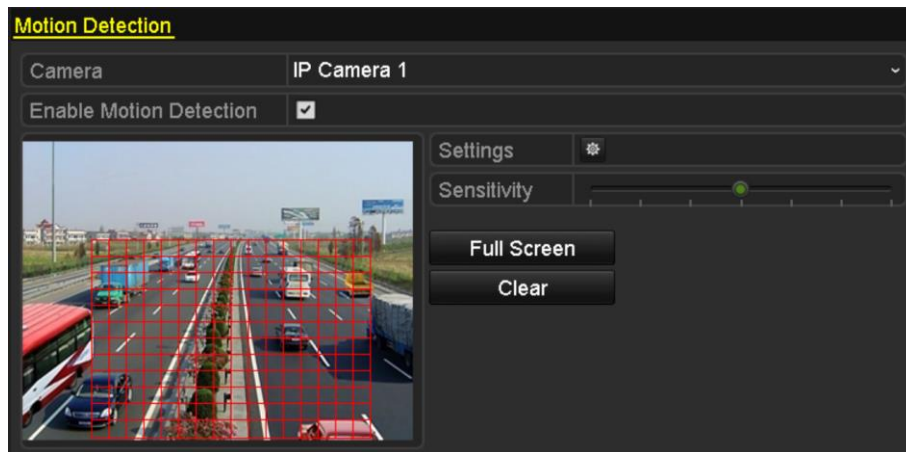
Figure 7-1 Motion Detection Setup Interface

2. Set up detection area and sensitivity.Tick **Enable Motion Detection**, use the mouse to draw detection area(s) and drag the sensitivity bar to set sensitivity.Click ⚙ and set alarm response actions.

3. Click **Trigger Channel** and select one or more channels which will start to record/capture or become full-screen monitoring when motion alarm is triggered, and click **Apply** to save the settings.

Figure 7-2 Set Trigger Camera of Motion Detection

4. Set up arming schedule of the channel.
   1) Select Arming Schedule tab to set the arming schedule of handling actions for the motion detection.
   2) Choose one day of a week and up to eight time periods can be set within each day.
   3) Click **Apply** to save the settings.

⎕**i Note**

   Time periods shall not be repeated or overlapped.

Figure 7-3 Set Arming Schedule of Motion Detection

5. Click **Handling** to set up alarm response actions of motion alarm.
6. If you want to set motion detection for another channel, repeat the above steps or just click **Copy** in the Motion Detection interface to copy the above settings to it.

7.1.2 Set Sensor Alarms

Set the handling action of an external sensor alarm.

Steps

1. Go to **Menu → Configuration → Alarm** and select an alarm input..

Figure 7-4 Alarm Status Interface of System Configuration

2. Set up the handling action of the selected alarm input.Check **Enable** and click **Settings** to set up its alarm response actions.

Figure 7-5 Alarm Input Setup Interface

3. Enable the one-key disarming for local alarm input 1 (Local<-1).
    1) Check **Enable One-Key Disarming**.
    2) Click **Settings** to enter the linkage action settings interface.
    3) Select the alarm linkage action (s) you want to disarm for the local alarm input1. The selected linkage actions include the Full Screen Monitoring, Audible Warning, Notify Surveillance Center, Send Email and Trigger Alarm Output.

4. Select **Trigger Channel** and select one or more channels which will start to record/capture or become full-screen monitoring when an external alarm is input, and click Apply to save the settings.
5. Select **Arming Schedule** to set the arming schedule of handling actions.

Settings			
Trigger Channel	Arming Schedule	Linkage Action	PTZ Linking
Week	Mon		
1	00:00-24:00		
2	00:00-00:00		
3	00:00-00:00		
4	00:00-00:00		
5	00:00-00:00		
6	00:00-00:00		
7	00:00-00:00		
8	00:00-00:00		
	Copy	Apply	OK	Cancel
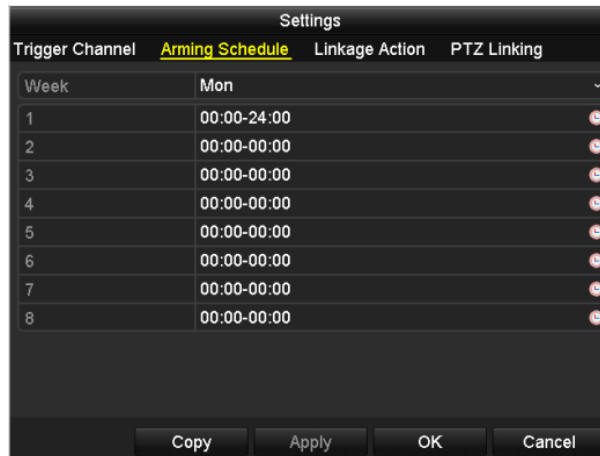
Figure 7-6 Set Arming Schedule of Alarm Input

Choose one day of a week and Max. eight time periods can be set within each day, and click **Apply** to save the settings.

Note

Time periods shall not be repeated or overlapped.
Repeat the above steps to set up arming schedule of other days of a week. You can also use **Copy** to copy an arming schedule to other days.

6. Select **Linkage Action** to set up alarm response actions of the alarm input.
7. Optional: Select PTZ Linking tab and set PTZ linkage of the alarm input.Set PTZ linking parameters and click **OK** to complete the settings of the alarm input.

Note

Make sure the PTZ or speed dome connected supports PTZ linkage.
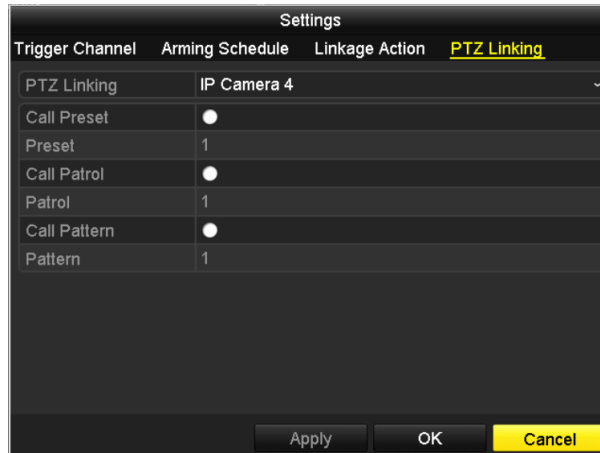
Figure 7-7 Set PTZ Linking of Alarm Input

8. If you want to set handling action of another alarm input, repeat the above steps.Or you can click **Copy** on the Alarm Input Setup interface and check the checkbox of alarm inputs to copy the settings to them.
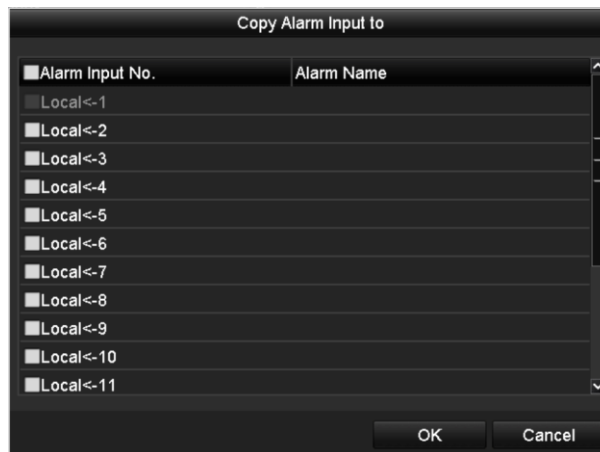
Figure 7-8 Copy Settings of Alarm Input

7.1.3 Detect Video Loss Alarm

Detect video loss of a channel and take alarm response action(s).

Steps

1. Go to **Menu → Camera → Video Loss**.
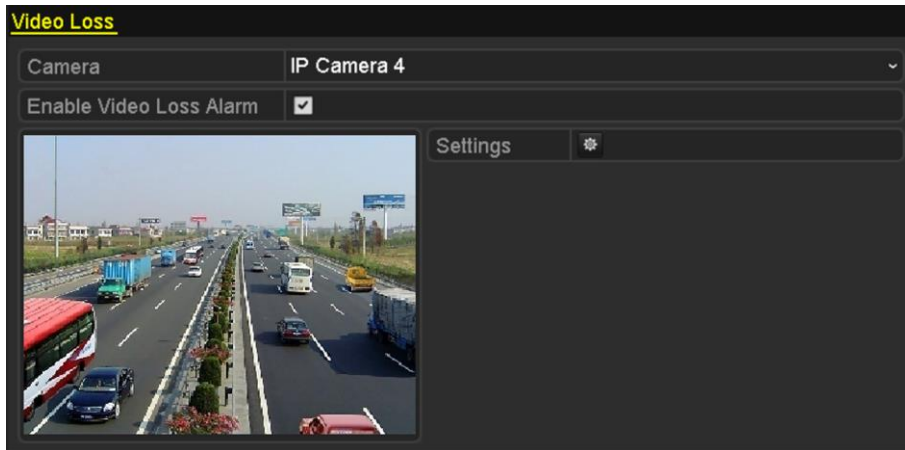
Figure 7-9 Video Loss Setup

2. Select a channel you want to detect.
3. Check **Enable Video Loss Alarm**.
4.   Click Settings button to set up handling action of video loss.
5. Set up arming schedule of the handling actions.
   1) Select **Arming Schedule**.
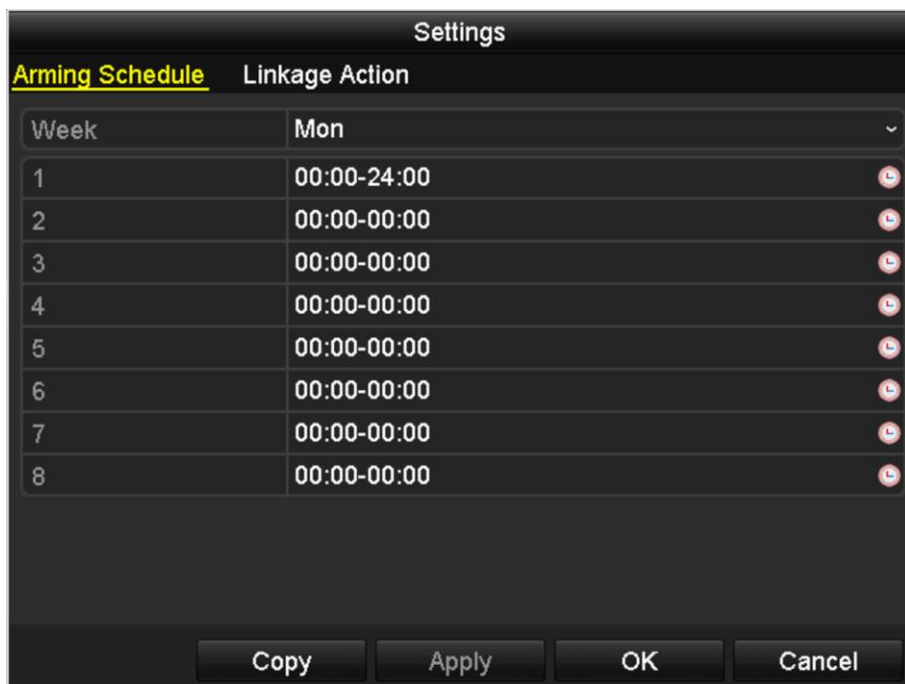
Figure 7-10 Set Arming Schedule of Video Loss

2) Choose one day of a week and up to eight time periods can be set within each day.

ⓘNote

Time periods shall not be repeated or overlapped.

---

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

6. Select **Linkage Action** to set up alarm response action of video loss (please refer to Setting Alarm Response Actions).
7. Click **OK** to complete the video loss settings of the channel.

7.1.4 Detect Video Tampering Alarm

Trigger alarm when the lens is covered and take alarm response action(s).

Steps

1. Enter **Menu → Camera → Video Tampering**.
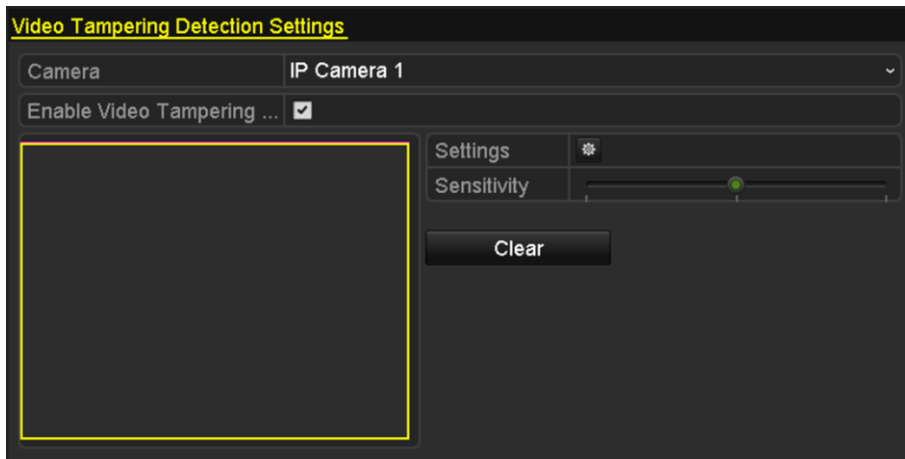
Figure 7-11 Video Tampering Setting

2. Select a channel you want to detect.
3. Check **Enable Video Tampering Detection**.
4. Drag the sensitivity bar to set a proper sensitivity level. Use the mouse to draw an area you want to detect video tampering.
5. Click button to set up handling action of video tampering.
6. Set arming schedule and alarm response actions of the channel.
   1) Click **Arming Schedule**.
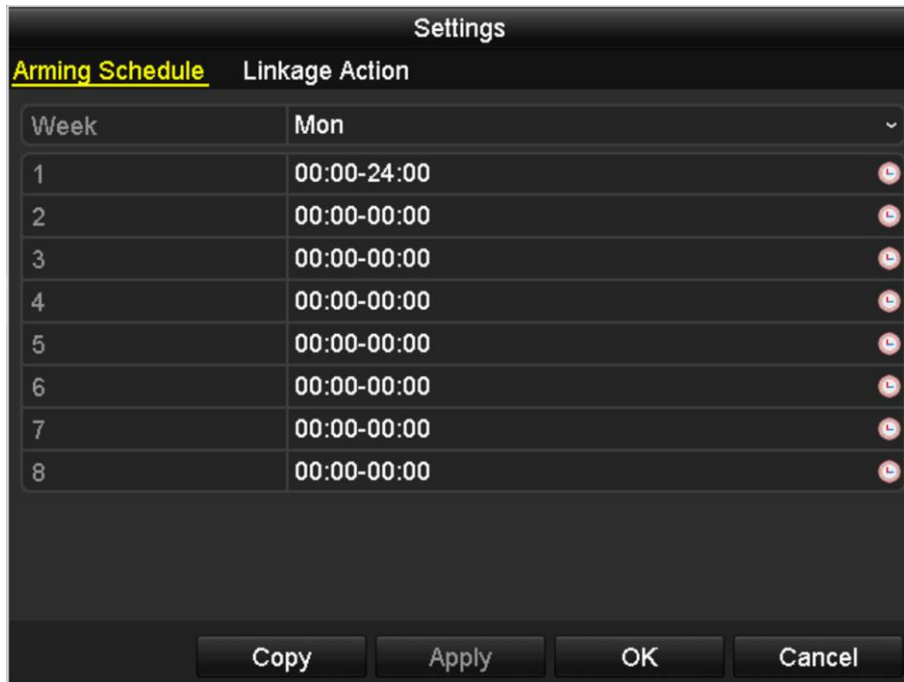
Figure 7-12 Set Arming Schedule of Video Tampering

2) Choose one day of a week and Max. eight time periods can be set within each day.

ⓘ**Note**

Time periods shall not be repeated or overlapped.

3) Click **Apply** to save the settings.
7. Select **Linkage Action** to set up alarm response action of video tampering alarm (please refer to Setting Alarm Response Actions).
8. Click **OK** to complete the video loss settings of the channel.

7.1.5 Handle Exceptions Alarm

Exception settings refer to the handling action of various exceptions, e.g.

● HDD Full: The HDD is full.
● HDD Error: Writing HDD error or unformatted HDD.
● Network Disconnected: Disconnected network cable.
● IP Conflicted: Duplicated IP address.
● Illegal Login: Incorrect user ID or password.
● Record/Capture Exception: No space for saving recorded files or captured images.
● Hot Spare Exception: Disconnected with the working device.

Steps

1. Go to **Menu → Configuration → Exceptions**.
2. Choose the Alarm trigger methods as you demand.

Figure 7-13 Exceptions Setup

7.1.6 Set Alarm Response Actions

Alarm response 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.

Steps

1. Go to **Menu → Configuration → Exceptions**.
2. Check **Enable Event Hint**.

> **Note**
>
> When an event or exception happens, a hint can be displayed on the lower-left corner of live view image. And you can click the hint icon to check the details. Besides, the event to be displayed is configurable.

3. Set the type of event to be displayed on the image.

Figure 7-14 Event Hint Settings

4. Choose the linkage action.

Full Screen Monitoring

When an alarm is triggered, the local monitor (VGA, HDMI or BNC monitor) display in full screen the video image from the alarming channel configured for full screen monitoring. If alarms are triggered simultaneously in several channels, their full-screen images will be switched at an interval of 10 seconds (default dwell time). A different dwell time can be set by going to **Menu** → **Configuration** → **Live View**.

Auto-switch will terminate once the alarm stops and you will be taken back to the Live View interface.

ⓘNote

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

Audible Warning

Trigger an audible beep when an alarm is detected.

Notify Surveillance Center

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

ⓘNote

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

Send Email

Send an email with alarm information to a user or users when an alarm is detected. Refer to *Configure Email* for details.

Trigger Alarm Output

Trigger an alarm output when an alarm is triggered. Refer to ***Trigger Alarm Output*** for details.

5. Click **OK**.

7.1.7 Trigger Alarm Output

Trigger an alarm output when an alarm is triggered.

Steps

1. Go to **Menu → Configuration → Alarm → Alarm Output**.
2. Select an alarm output and set alarm name and dwell time. Click **Schedule** to set the arming schedule of alarm output.

Note

If **Dwell Time** is set as **Manually Clear**, you can clear it only by going to **Menu → Manual → Alarm**.
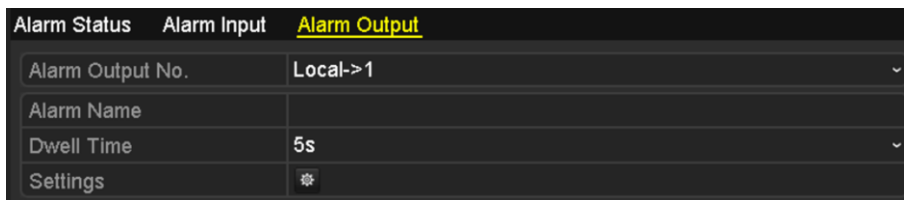
Figure 7-15 Alarm Output Setup

3. Set up arming schedule of the alarm output.

Choose one day of a week and up to 8 time periods can be set within each day.

Note

Time periods shall not be repeated or overlapped.

Figure 7-16 Set Arming Schedule of Alarm Output

4. Repeat the above steps to set up arming schedule of other days of a week. You can also use **Copy** to copy an arming schedule to other days.
5. Click **OK** to complete the video tampering settings of the alarm output No..
6. You can also copy the above settings to another channel.
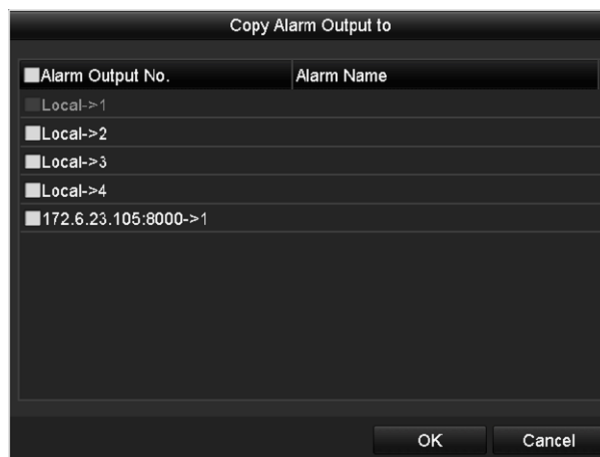
Figure 7-17 Copy Settings of Alarm Output

7.1.8 Trigger or Clear Alarm Output Manually

Sensor alarm can be triggered or cleared manually. If **Manually Clear** is selected in the dwell time of an alarm output, the alarm can be cleared only by clicking **Clear** in the following interface.

Steps

1. Go to **Menu → Manual → Alarm**
2. Select the alarm output you want to trigger or clear and make related operations.
   ● Click **Trigger/Clear** if you want to trigger or clear an alarm output.
   ● Click **Trigger All** if you want to trigger all alarm outputs.
   ● Click **Clear All** if you want to clear all alarm output.

7.2 VCA Alarm

The NVR supports the VCA detection alarm sent by IP camera. The VCA detection must be enabled and configured on the IP camera settings interface first.

Note
- All VCA detection must be supported by the connected IP camera.
- Please refer to the User Manual of Network Camera for the detailed instructions for the all VCA detection types.

7.2.1 Intrusion Detection

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

Steps
1. Enter **Menu → Camera → VCA**.
2. Select a camera to configure the VCA.

Note
You can check **Save VCA Picture** to save captured pictures of VCA detection.

3. Set **VCA detection type** as **Intrusion Detection**.
4. Check **Enable**.
5. Click to configure the trigger channel, arming schedule and linkage actions.
6. Click **Rule Settings** to set the intrusion detection rules. Set the following parameters.

Note
Up to 4 rules can be configured.

Threshold
Range [1s-10s], the threshold for the time of the object loitering in the region. When the duration of the object in the defined detection area is longer than the set time, the alarm will be triggered.

Sensitivity
Range [1-100]. The value of the sensitivity defines the size of the object which can trigger the alarm. The higher the value is, the more easily the detection alarm can be triggered.

Percentage
Range [1-100]. Percentage defines the ratio of the in-region part of the object which can

trigger the alarm. For example, if the percentage is set as 50%, when the object enters the region and occupies half of the whole region, the alarm is triggered.

7. Click and draw a quadrilateral in the preview window by specifying four vertexes of the detection region, and right click to complete drawing. Only one region can be configured.

Note

You can use the to clear the existing virtual line and re-draw it.
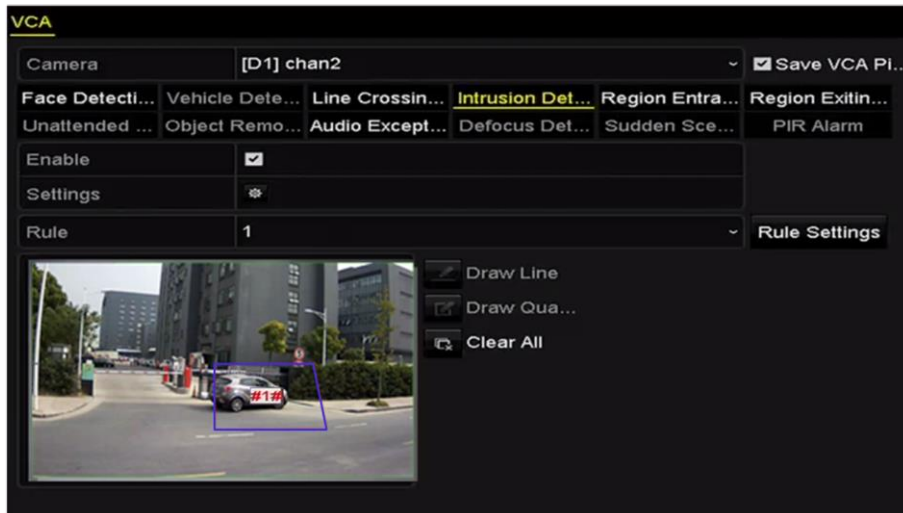
Figure 7-18 Draw Area for Intrusion Detection

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

7.2.2 Line Crossing Detection

This function can be used for detecting people, vehicles and objects cross a set virtual line. The line crossing direction can be set as bidirectional, from left to right or from right to left. And you can set the duration for the alarm response actions, such as full screen monitoring, audible warning, etc.

Steps

1. Enter **Menu → Camera → VCA**.
2. Select the camera to configure the VCA.

Note

You can check **Save VCA Picture** to save the captured pictures of VCA detection.

3. Select **VCA detection type** as **Line Crossing Detection**.
4. Check **Enable**.

5. Click to configure the trigger channel, arming schedule and linkage actions for the line crossing detection alarm.
6. Click **Rule Settings** to set the line crossing detection rules.

ⓘNote

Up to 4 rules can be configured.

---

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

   A<->B

   Only the arrow on the B side shows; when an object going across the configured line with both direction can be detected and alarms are triggered.

   A->B

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

   B->A

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

2) Click-and-drag the slider to set the detection sensitivity.

   Sensitivity

   Range [1-100]. The higher the value is, the more easily the detection alarm can be triggered.

3) Click **OK** to save the rule settings and back to the line crossing detection settings interface.
7. Click and set two points in the preview window to draw a virtual line.

ⓘNote

You can use the to clear the existing virtual line and re-draw it.
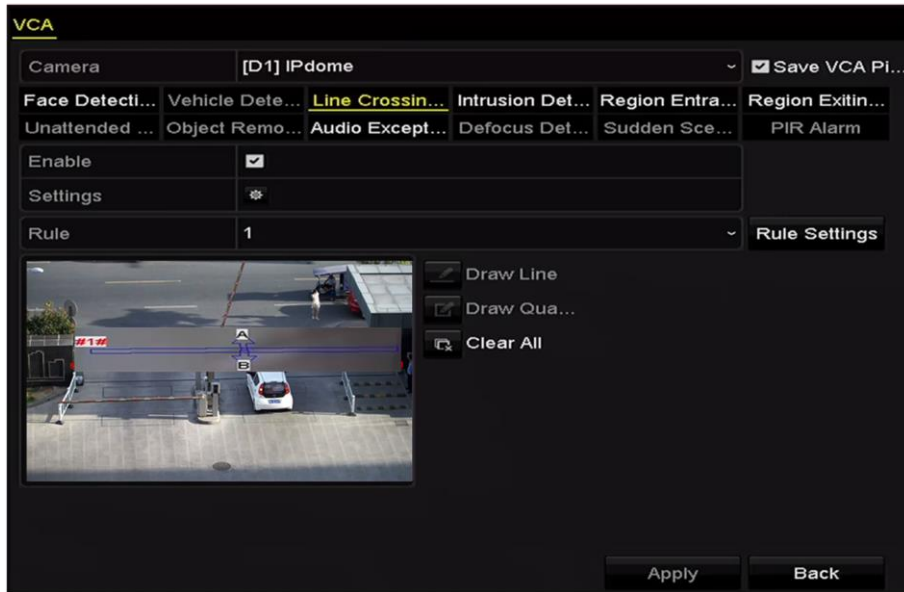
Figure 7-19 Draw Line for Line Crossing Detection

Chapter 8 Network Settings

8.1 Configure General Settings

Network settings must be properly configured before you operate NVR over network.

Steps

1. Go to **Menu** → **Configuration** → **Network**.
2. Select **General**.
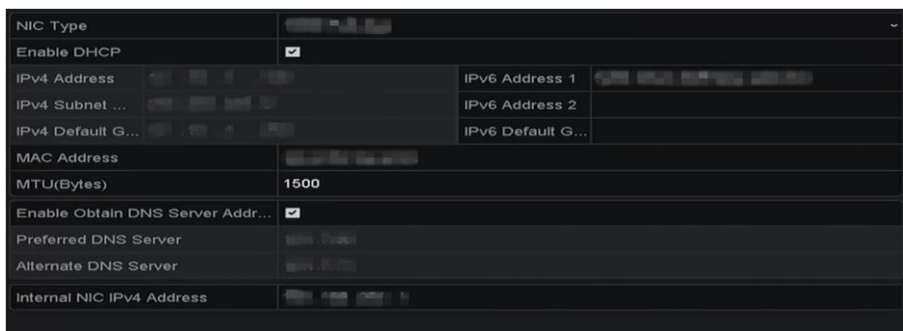
Figure 8-1 Network Settings

3. Configure related parameters.

   MTU

   The valid value range of MTU is 500 - 9676.

   DHCP

   If the DHCP server is available, you can check **Enable DHCP** to automatically obtain an IP address and other network settings from that server.

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

8.2 Configure Wi-Fi

The device can work as a wireless network router. Follow the steps to setup a network router.

Steps

1. Go to **Menu** → **Configuration** → **WIFI**.
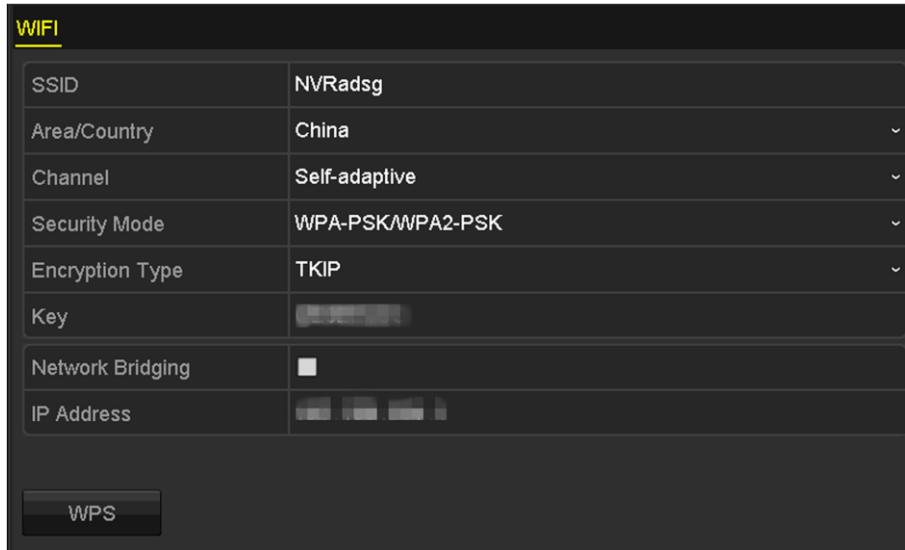
Figure 8-2 Wi-Fi Settings

2. Configure wireless network parameters, including **Network Bridging**, **SSID**, **Security Mode**, and **Key**.

Network Bridging

Enable device to create a single aggregate network from multiple communication networks or network segments.

SSID

It is the short for Service Set Identifier. SSID is the Wi-Fi name that the device provides.

Area/Country

Select where the router is used.

Channel

Select the best channel according to your situation.

Security Mode

Select the security protocol for the wireless network.

Encryption Type

It is used to protect information. TKIP and AES are selectable.

Key

Enter the encryption key.

WPS

It is the short of Wi-Fi Protected Setup. Click the button and then you can connect the wireless network without password for once.

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

8.3 Configure Advanced Settings

8.3.1 Configuring DDNS

You can set the Dynamic DNS (DDNS) for network access. Prior registration with your ISP is required before configuring the system to use DDNS.

Steps

1. Go to **Menu → Configuration → Network**.
2. Select **DDNS** to enter the DDNS Settings interface.
3. Check **Enable DDNS** to enable this feature.
4. Select **DDNS Type** as **DynDNS**, **PeanutHull**, or **NO-IP**.
5. Configure **Server Address,Device Domain Name,User Name,User Name**.
6. Click **Apply** to save and exit the interface.

8.3.2 Configure NTP Server

A Network Time Protocol (NTP) Server can be configured on your NVR to ensure the accuracy of system date/time.If the NVR is connected to a public network, you should use a NTP server that has a time synchronization function, such as the server at the National Time Center (IP Address: 210.72.145.44). If the NVR is setup in a more customized network, NTP software can be used to establish a NTP server used for time synchronization.

Steps

1. Go to **Menu →   Configuration →   Network → NTP**.
2. Check **Enable NTP**.
3. Configure the following NTP settings.

   Interval

   Time interval between the two synchronizing actions with NTP server. The unit is minute.The time synchronization interval can be set from1 to 10080min, and the default value is 60min.

   NTP Server

   IP address of NTP serve.r

   NTP Port

   Port of NTP server.

4. Click **Apply**.

8.3.3 Configure More Settings

Steps

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

2. Select **More Settings** to enter the More Settings interface.

Alarm Host IP	192.0.0.10
Alarm Host Port	7200
Server Port	8000
HTTP Port	80
Multicast IP	239.252.2.50
RTSP Port	554

Figure 8-3 Configure More Settings

3. Configure the remote alarm host, server port, HTTP port, multicast, RTSP port.

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 CMS (Client Management System) software installed. The Alarm Host IP refers to the IP address of the remote PC on which the CMS (Client Management System) software (e.g., iVMS-4200) is installed, and the Alarm Host Port must be the same as the alarm monitoring port configured in the software (default port is 7200).

Multicast IP

The multicast can be configured to realize live view for more than the maximum number of cameras through network. A multicast address spans the Class-D IP range of 224.0.0.0 to 239.255.255.255. It is recommended to use the IP address ranging from 239.252.0.0 to 239.255.255.255. When adding a device to the CMS (Client Management System) software, the multicast address must be the same as the device's multicast IP.

RTSP Port

The RTSP (Real Time Streaming Protocol) is a network control protocol designed for use in entertainment and communications systems to control streaming media servers. The default RTSP port is 554, and you can change it according to different requirements.

Server Port and HTTP Port

The Server Port should be set to the range of 2000-65535 and it is used for remote client software access. The HTTP port is used for remote IE access.The default Server Port is 8000 and the HTTP Port is 80, and you can change them according to different requirements.

4. Click **Apply** to save and exit the interface.

8.3.4 Configure Email

The system can be configured to send an email notification to all designated users if an alarm event is detected, etc., an alarm or motion event is detected or the administrator password is changed.

Before You Start

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

Steps

1. Go to **Menu → Configuration → Network**.
2. Set the IPv4 address, IPv4 subnet mask, IPv4 gateway and the preferred DNS server in the Network Settings menu.
3. Click **Apply** to save the settings.
4. Select the Email tab to enter the Email Settings interface.

Figure 8-4 Email Settings

5. Configure the following email settings.

Enable Server Authentication

Check it to enable the server authentication feature.

User Name

The user name of sender's account registered on the SMTP server.

Password

The password of sender's account registered on the SMTP server.

SMTP Server

The SMTP Server IP address 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

Click **Enable SSL/TLS** if required by the SMTP server.

Sender

The name of sender.

Sender's Address

The Email address of sender.

Select Receivers

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

Receiver

The name of user to be notified.

Receiver's Address

The Email address of user to be notified.

Enable Attached Picture

Check **Enable Attached Picture** if you want to send email with attached alarm images. The interval is the time of two adjacent alarm images. You can also set SMTP port and enable SSL here.

Interval

The interval refers to the time between two actions of sending attached pictures.

6. Click **Apply** to save the email settings.
7. You can click **Test** to test whether your email settings work.

8.3.5 Configuring 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.

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

Steps

1. Go to **Menu → Configuration → Network → NAT**.
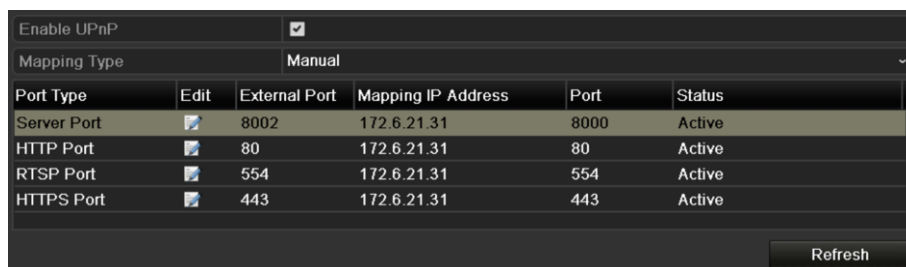
Figure 8-5 UPnP™ Settings

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

ⓘNote
- 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.

Figure 8-6 Setting Virtual Server Item

- Each item should be corresponding with the device port, including server port, http port, RTSP port and https port.
- The above virtual server setting interface 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.

8.4 Check Network Traffic

You can check the network traffic to obtain real-time information of NVR such as linking status, MTU, sending/receiving rate, etc.

Steps

1. Go to **Menu → Maintenance → Net Detect**.

Figure 8-7 Network Traffic

2. You can view the sending rate and receiving rate information on the interface. The traffic data is refreshed every 1 second.

8.5 Configure Network Detection

You can obtain network connecting status of NVR through the network detection function, including network delay, packet loss, etc.

8.5.1 Test Network Delay and Packet Loss

Steps

1. Go to **Menu → Maintenance → Net Detect**.
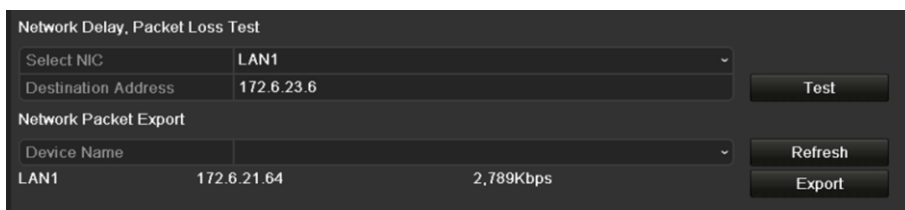2. Enter **Destination Address**.

Figure 8-8 Network Detection

3. Click **Test** to start testing network delay and packet loss.

Result

The testing result pops up on the window. If the testing is failed, the error message box will pop up as well.
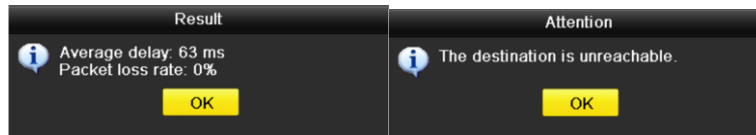
Figure 8-9 Testing Result of Network Delay and Packet Loss

8.5.2 Export Network Packet

The captured network data packet can be exported to USB flash drive, or other local backup devices.

Steps

1. Go to **Menu** → **Maintenance** → **Net Detect** → **Network Detection**.
2. Select a backup device in **Device Name**.

Note

Click **Refresh** if the connected local backup device cannot be displayed. When it fails to detect the backup device, please check whether it is compatible with the device. You can format the backup device if the format is incorrect.
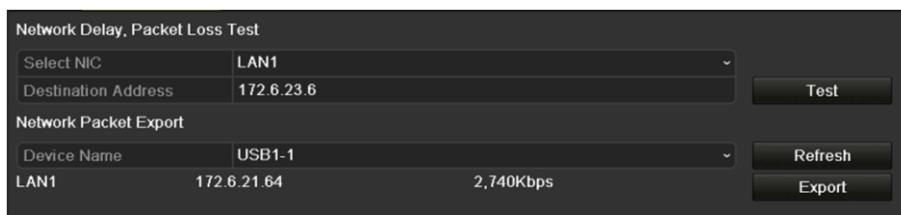
Figure 8-10 Export Network Packet

3. Click **Export** to start exporting.
4. Click **OK** after the exporting is completed.

Note

Up to 1 MB data can be exported each time.

8.5.3 Check the Network Status

You can check your network status, and quickly set the network parameters if the network is abnormal.
Go to **Menu** → **Maintenance** → **Net Detect** → **Network Detection**. Click **Status** at the lower- right corner.
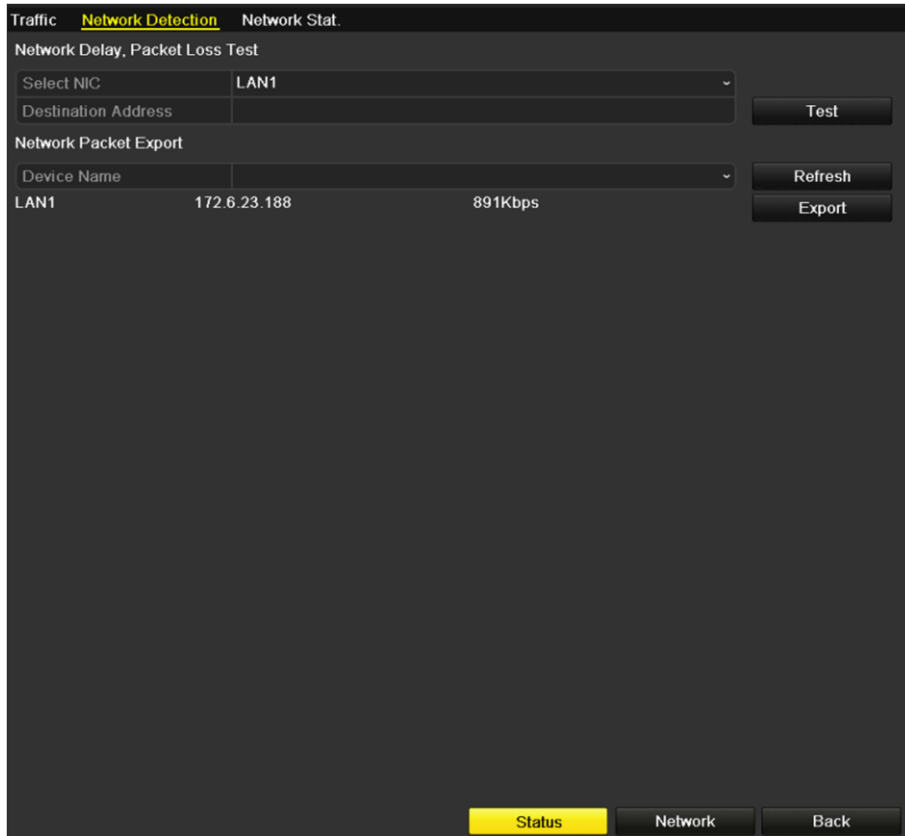
Figure 8-11 Network Status Checking

If the checking result is normal, you will receive a pop-up message. If the network status is not normal, you can click **Network** to set network parameters.

8.5.4 Check Network Statistics

You can check the network status to obtain the real-time network bandwidth information.
Go to **Menu → Maintenance → Net Detect → Network Stat.**. The bandwidth of **IP Camera**, **Remote Live View**, **Remote Playback**, **Net Receive Idle** and **Net Send Idle** will be listed.
You can click **Refresh** to get the latest status.

Figure 8-12 Network Stat.
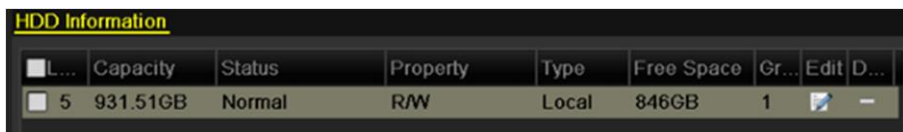
Chapter 9 HDD Management

9.1 Initialize HDDs

A newly installed hard disk drive (HDD) must be initialized before using it with your device. Initializing the HDD will erase all data on it.

Steps
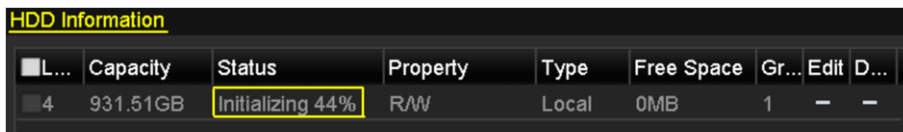
1. Go to **Menu → HDD → General**.

Figure 9-1 HDD Information

2. Select HDD(s) for initialization.
3. Click **Init**.
4. Click **OK** to start initialization.

Figure 9-2 HDD Status

After the HDD is initialized, its status will be changed from "Uninitialized" to "Normal".

9.2 Configure Quota Mode

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

Steps

1. Go to **Menu → HDD → Advanced**.

Figure 9-3 Storage Mode Settings

2. Set **Mode** as **Quota**.

3. Select a camera for quota.

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

5. Optional: Click **Copy** to copy the quota settings of the current camera to other cameras.

6. Click **Apply**.

⬚**i**Note

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

9.3 Configure HDD Error Alarms

You can configure the HDD error alarms when the HDD status is "Uninitialized" or "Abnormal".

Steps

1. Go to **Menu → Configuration → Exceptions**.

2. Set **Exception Type** as **HDD Error**.

3. Select HDD error alarm type(s).

Figure 9-4 Configure HDD Error Alarm

4. If you have checked **Trigger Alarm Output**, you shall select its alarm output.

5. Click **Apply**.

Chapter 10 System Management

10.1 View System Information

You can view the device information, device model, serial number, firmware, etc.
Go to **Menu → Maintenance → System Info**. You can view the system information in **Device Info**, **Camera**, **Record**, **Alarm**, **Network**, and **HDD**.

Figure 10-1 Device Information

ⓘ**Note**
You can add the device to your mobile client software (iVMS-4500) by scanning the QR code.

10.2 Configure General Settings

You can configure the BNC output standard, VGA output resolution, mouse pointer speed in **Menu**

→ **Configuration** → **General** → **General**.

Figure 10-2 General Settings

Language

The system language. Default language is **English**.

Output Standard

Set it to **NTSC** or **PAL**, it must be the same with the video input standard.

Resolution

You can configure the VGA resolution and HDMI resolution respectively. Up to 4K (3840 × 2160) resolution is selectable for the HDMI output.

Enable Wizard

Enable/disable the wizard when the device starts up.

Enable Password

Enable/disable the use of the login password.

10.3 Configure DST Settings

Daylight saving time (DST) is the practice of advancing clocks during the lighter months so that evenings have more daylight and mornings have less.
Go to **Menu** → **Configuration** → **General** → **DST Settings**. You can check **Auto DST Adjustment**, or check **Enable DST** to manually set the date of the DST period.

Figure 10-3 DST Settings

10.4 Manage User Accounts

The default user name for administrator is "admin", and you can set the password of admin during activation. Administrator has the permission to add, delete user, and configure user parameters.

10.4.1 Add a User

Steps

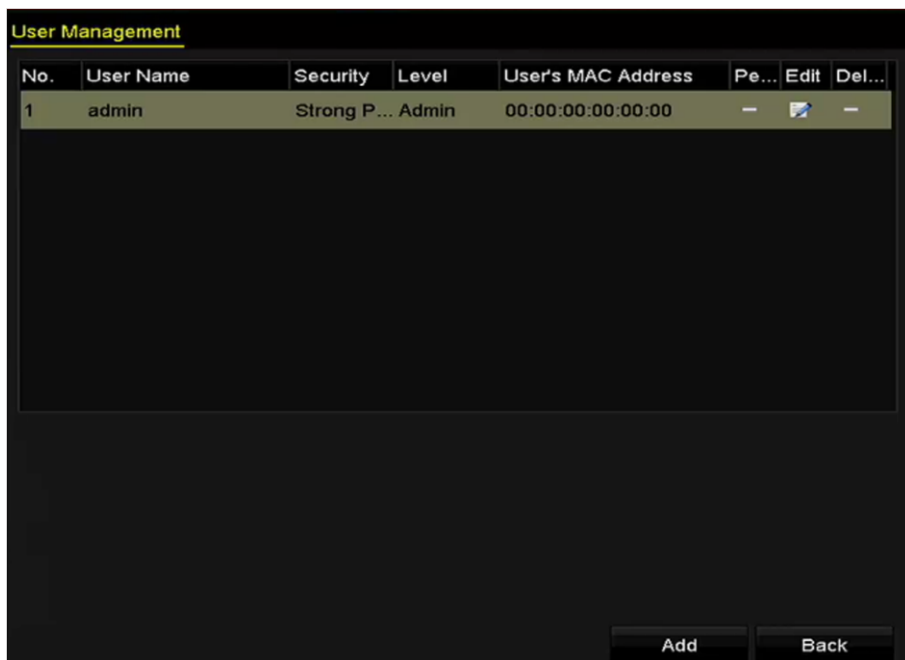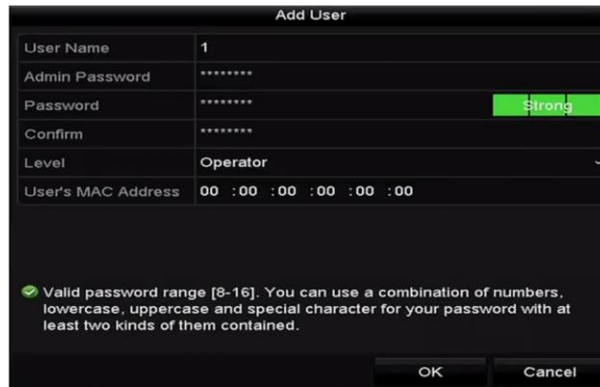1. Go to **Menu → Configuration → User → User Management**.

Figure 10-4 User Management

2. Click **Add**.

Figure 10-5 Add User

3. Set parameters for the new user.

   Password

   Set the password for the user.

   Level

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

   Operator

   Operator has the permission of Two-way Audio in Remote Configuration and all operating permission in Camera Configuration by default.

   Guest

   Guest 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

   If it is enabled, it only allows the specified MAC address to access your device.

⚠️**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.

4. Click **OK**.
   The added new user will be displayed on the user list.
5. Click ✅ of the user to set the user permission.
6. Set the operating permission of **Local Configuration**, **Remote Configuration** and **Camera Configuration**.

Local Configuration

Local Log Search

Searching and viewing logs and system information of your device.

Local Parameters Settings

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

Local Camera Management

Adding, deleting and editing of IP cameras.

Local Advanced Operation

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

Local Shutdown Reboot

Shutting down or rebooting the device.

Remote Configuration

Remote Log Search

Remotely viewing logs that are saved on the device.

Remote Parameters Settings

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

Remote Camera Management

Remote adding, deleting and editing of the IP cameras.

Remote Serial Port Control

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

Remote Video Output Control

Sending remote button control signal.

Two-Way Audio

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

Remote Alarm Control

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

Remote Advanced Operation

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

Remote Shutdown/Reboot

Remotely shutting down or rebooting the device.

Camera Configuration

Remote Live View

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

Local Manual Operation

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

Remote Manual Operation

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

Local Playback

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

Remote Playback

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

Local PTZ Control

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

Remote PTZ Control

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

Local Video Export

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

7. Click **OK**.

⎙**Note**
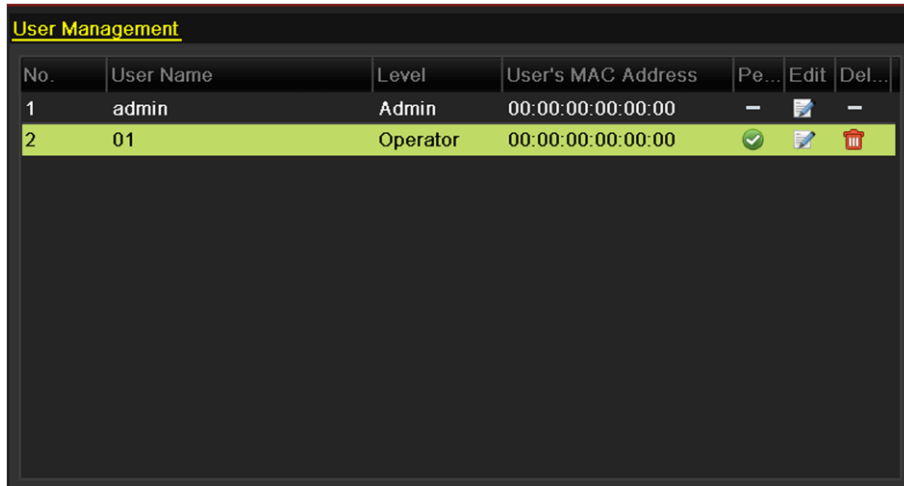
Only the admin user account has the permission of restoring factory default parameters.

10.4.2 Delete a User

Steps

1. Go to **Menu → Configuration → User → User Management**.

Figure 10-6 User List

2. Click of the user that requires to be deleted.
3. Enter the admin password,
4. Click **OK**.
5. Click **Yes** to confirm deleting this user.

10.4.3 Edit a User

For the added user accounts, you can edit the parameters.

Steps

1. Go to **Menu → Configuration → User → User Management**.
2. Select a user from the list.
3. Click .

Figure 10-7 Edit User (Operator/Guest)
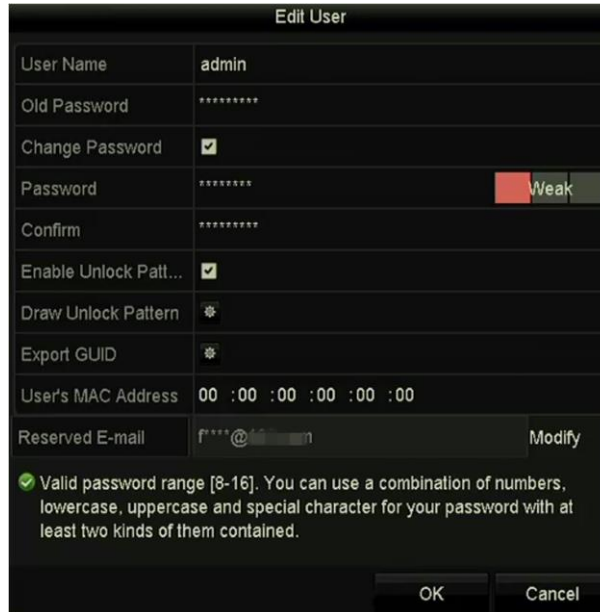
Figure 10-8 Edit User (Admin)

4. Edit the user password.

Operator and Guest

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

Admin

You can export GUID, and edit the password, unlock pattern, MAC address, and reserved email. You are allowed to edit the operator and guest permission by clicking ☑ on User Management interface.

10.5 Configure More Settings

You can configure the device name, device No., auto logout time, menu output mode, etc. Go to **Menu → Configuration → General → More Settings**.
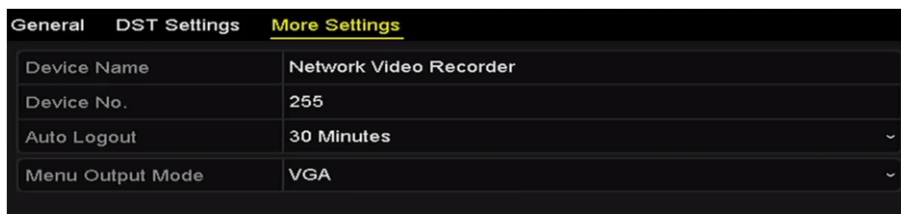
Figure 10-9 More Settings

Device No.

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

Auto Logout

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

Enable HDMI/VGA Simultaneous Output

You can set the simultaneous output for the HDMI and VGA. For devices with 16-ch IP video inputs, enable this function will make 4K resolution of HDMI unavailable.

Menu Output Mode

Choose to display the menu on HDMI or VGA. When **Auto** is selected, and both HDMI and VGA outputs are connected, the device will detect and set the HDMI as the menu output.

10.6 Search & Export Log Files

The operation, alarm, exception and information of the device can be stored in log files, which can be viewed and exported.

Steps

1. Go to **Menu → Maintenance → Log Information**.
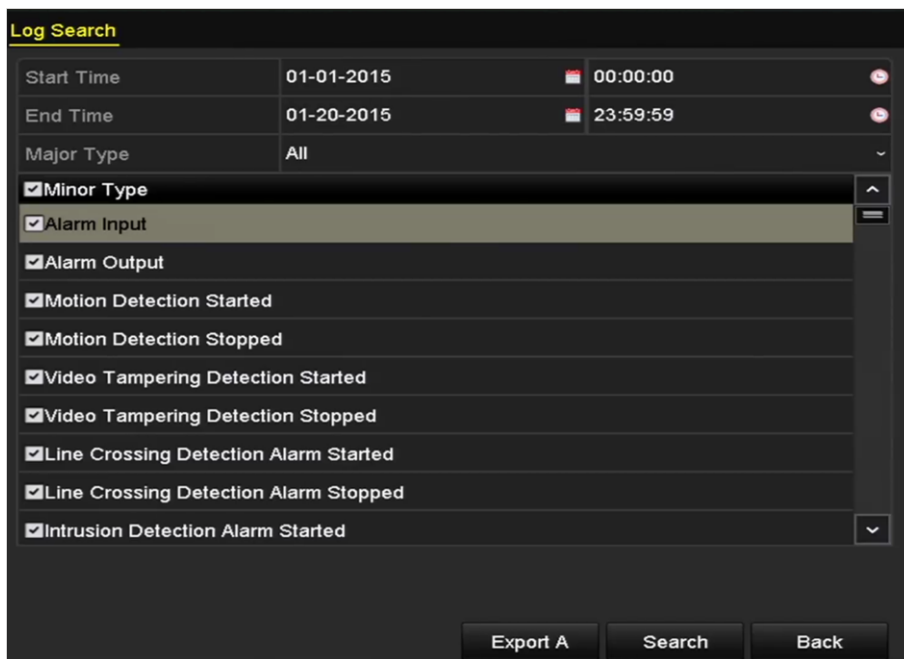
Figure 10-10 Log Search

2. Set the log search conditions
3. Click **Search**.

Figure 10-11 Log Search Results

ℹ️**Note**

Up to 2000 log files can be displayed each time.

The matched log files will be displayed on the search result list.

4. Optional: Click ✅ or double click the log to view its detailed information.
5. Optional: Click ⊚ to view the related video files if available.
6. Click **Export** to export the log files, or click **Export All** on the previous interface to export all log files to a USB flash drive.
   1) Select a USB flash drive in **Device Name**.
   2) Select a format of the log files.
   3) Optional: Click **New Folder** to create a new folder in the USB flash drive.
   4) Optional: Click **Format** to format the USB flash drive before exporting.
   5) Click **Export**.

ℹ️**Note**

Please connect the USB flash drive to the device before exporting log files.

10.7 Import/Export Configuration File

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

with the same parameters.

10.7.1 Import Configuration File

Before You Start

Prepare a USB flash drive that contains the configuration file, and insert it to the device.

Steps

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

Figure 10-12 Import/Export Config File

2. Select the USB flash drive from **Device Name**.
3. Select the configuration file.
4. Click **Import**.
5. Enter the admin password.
6. Click **OK**. The device will restart automatically.

10.7.2 Export Configuration File

Before You Start

Prepare a USB flash drive, and insert it into the device.

Steps

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

Figure 10-13 Import/Export Config File

2. Select the USB flash drive from **Device Name**.

3. Click **Export**.

4. Enter the admin password

5. Click **OK**.

10.8 Upgrade System

10.8.1 Upgrade by Local Backup Device

Use a local backup device, such as a USB flash drive, to upgrade your device.

Before You Start

● Prepare a local backup device, such as a USB flash drive.

● Ensure the local backup device contains the upgrade file, and insert it to the device.

Steps

1. Go to **Menu → Maintenance → Upgrade → Local Upgrade**.
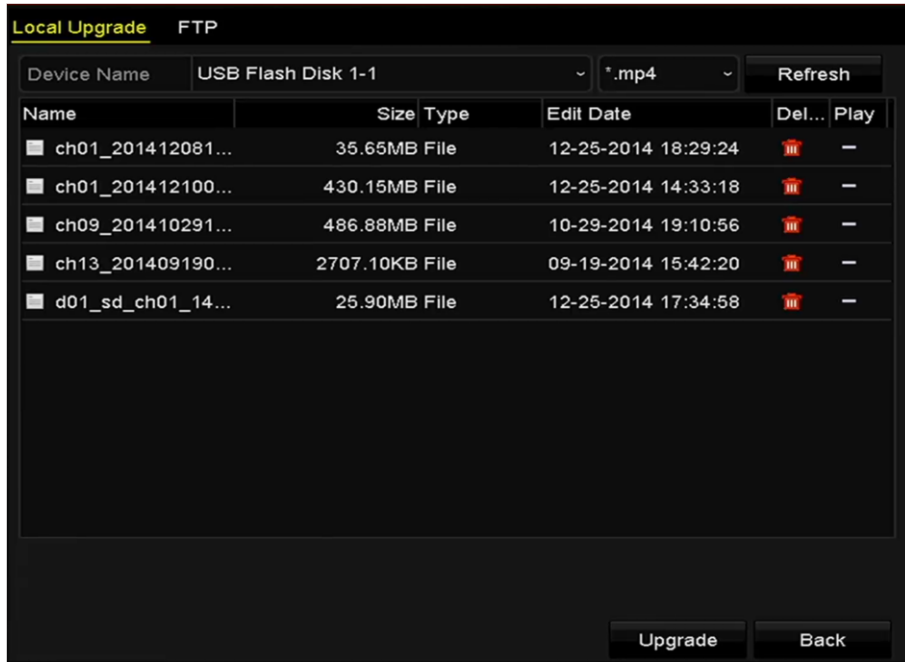
Figure 10-14 Local Upgrade

2. Select the backup device from **Device Name**.

3. Select the upgrade file.

4. Click **Upgrade**.

5. Waiting for the upgrade progress. The device will restart automatically.

10.8.2 Upgrade by FTP

You can upgrade your device via FTP.

Before You Start

● Ensure the network connection of the PC (running FTP server) and the device is valid and correct.

● Run the FTP server on the PC and copy the firmware into the corresponding directory of your PC.

Steps

1. Go to **Menu** → **Maintenance** → **Upgrade** → **FTP**.
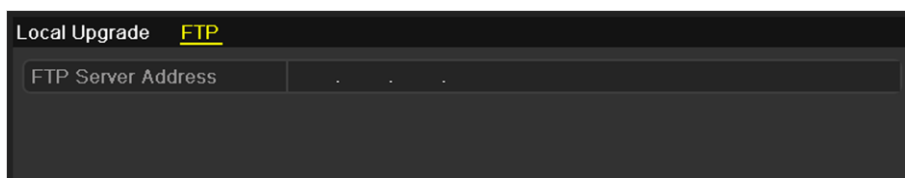
Figure 10-15 FTP Upgrade

2. Enter the FTP server address.

3. Click **Upgrade**.

4. Waiting for the upgrade progress. The device will restart automatically.

10.9 Reset Password by GUID

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

Steps

1. On the user login interface, click **Forgot Password**.
2. Select the password resetting type to **Verify by GUID**.
3. Insert the USB flash drive that contains GUID file.
4. Select the GUID file from the USB flash drive.
5. Click **Import** to import the file to the device
6. After the GUID file is successfully imported, enter the reset password interface to set the new admin password.
7. Click **OK** to set the new password.

> **Note**
>
> When the new password is set, the original GUID file will be invalid.

What to do next

You can export the new GUID file to the USB flash drive for future password resetting.

10.10 Restore Default Settings

Go to **Menu → Maintenance → Default**. Select a restore type from the following three options. The device will restart automatically after restoring to the default settings.

Restore Defaults

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

Factory Defaults

Restore all parameters to the factory default settings.

Restore to Inactive

Restore the device to the inactive status.

> **Note**
>
> **Factory Defaults** and **Restore to Inactivate** will restore added network cameras to factory settings.

Figure 10-16 Restore Defaults

Chapter 11 Appendix

11.1 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.
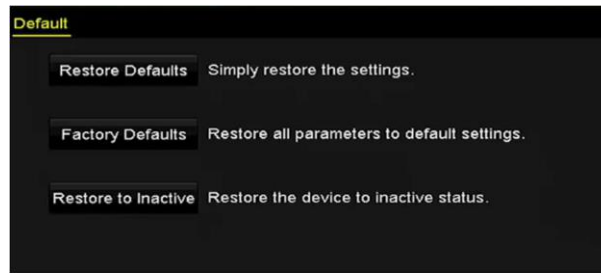
DVR

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.

11.2 Frequently Asked Questions

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

Reason

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

Solution

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

ⓘ**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.

11.2.2 Why is the video recorder notifying not support the stream type?

Reason

The camera encoding format mismatches with the video recorder.

Solution

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

11.2.3 Why is the video recorder notifying risky password after adding network camera?

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.

11.2.4 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.

11.2.5 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.

11.2.6 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.

11.2.7 When adding network camera, the video recorder notifies network is unreachable.

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.

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

Reason

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

Solution

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

11.2.9 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.

11.2.10 Why is image getting stuck when the video recorder is 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.

11.2.11 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.

11.2.12 Why is there no recorded video after setting the motion

detection?

Reason

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

Solution

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

11.2.13 Why is the sound quality not good in recording video?

Reason

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

Solution

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

See Far, Go Further