Digital Video Recorder

Quick Start Guide



V1.0.0

Foreword

General

This quick start guide (hereinafter referred to as "the Manual") introduces the functions and operations of the DVR device (hereinafter referred to as "the DVR").

Safety Instructions

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

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

Revision History

Version	Revision Content	Release Time
V1.0.0	First release.	July 2020

Privacy Protection Notice

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

About the Manual

- The Manual is for reference only. If there is inconsistency between the Manual and the actual product, the actual product shall prevail.
- We are not liable for any loss caused by the operations that do not comply with the Manual.

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

Important Safeguards and Warnings

The following description is the correct application method of the DVR. Read the Manual carefully before use to prevent danger and property loss. Strictly conform to the Manual during application and keep it properly after reading.

Operating Requirements

- Do not place and install the DVR in an area exposed to direct sunlight or near heat generating device.
- Do not install the DVR in a humid, dusty or fuliginous area.
- Keep its horizontal installation, or install it at stable places, and prevent it from falling.
- Do not drip or splash liquids onto the DVR; do not put on the DVR anything filled with liquids, in order to prevent liquids from flowing into the DVR.
- Install the DVR at well-ventilated places; do not block its ventilation opening.
- Use the DVR only within rated input and output range.
- Do not dismantle the DVR arbitrarily.
- Transport, use and store the DVR within allowed humidity and temperature range.

Power Requirements

- Use batteries according to requirements. Otherwise, it may result in fire, explosion or burning risks of batteries!
- To replace batteries, only the same type of batteries can be used.
- Dispose the exhausted batteries according to the instructions.
- Use electric wires within rated specifications recommended by local regulations.
- Use standard power adapter matched with this DVR. Otherwise, the user shall undertake resulting personnel injuries or DVR damages.
- Use power supply that meets SELV (safety extra low voltage) requirements, and supply power with rated voltage that conforms to Limited Power Source in IEC60950-1. For specific power supply requirements, refer to device labels.
- Products with category I structure shall be connected to grid power output socket, which is equipped with protective grounding.
- Appliance coupler is a disconnecting device. During normal use, keep an angle that facilitates operation.

Table of Contents

Foreword I
Important Safeguards and Warnings III
1 Local Operations 1
1.1 Starting the DVR 1
1.2 Initializing the DVR 1
1.3 Configuring Network 4
1.4 Configuring Encode Setting 6
1.5 Adding IP Camera 8
1.5.1 Changing Channel Type 9
1.5.2 Initializing IP Camera 10
1.5.3 Adding IP Camera by Search Result 15
1.5.4 Manually Adding IP Camera 17
1.6 Configuring Recorded Video Storage Schedule 20
1.7 Configuring P2P Settings 20
1.7.1 Enabling P2P Function 20
1.7.2 Adding the DVR to Smart Phone Client 21
1.8 Smart Motion Detection 23
1.9 Live View 26
1.10 Recording Playback 27
2 Logging in to Web 29
Appendix 1 Security Recommendation 30

1 Local Operations

1.1 Starting the DVR

Before starting the DVR, make sure that:

- The rated input voltage matches the DVR's power requirements.
- The power wire connection is ready.
- For device security, connect the DVR to the power adapter first and then connect it to the power socket.
- Always use stable current. It is recommended to use UPS as the power source.

1.2 Initializing the DVR

This topic shows how to initialize the DVR before use.

Background Information

When booting up for the first time, you need to configure the password information for **admin** (by default). To guarantee device security, we strongly recommend you properly keep the login password and regularly modify it.

Procedure

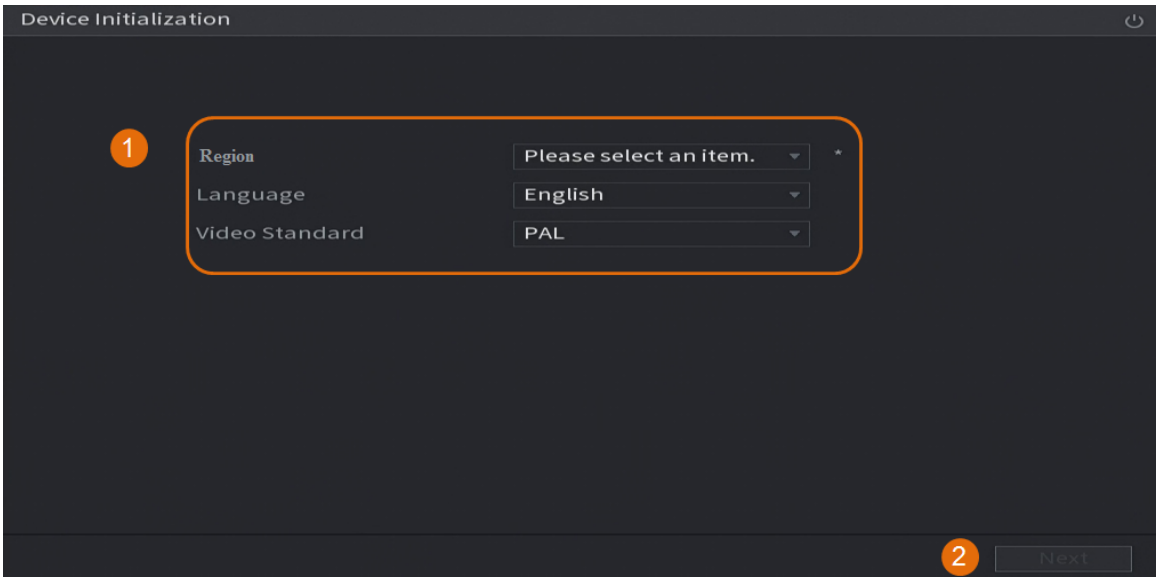
Step 1 Turn on the DVR.

The system enters device initialization interface.

Step 2 From the drop-down lists, select region, language and video standard as needed and click **Next**.

You can change these settings on setting pages of the DVR after initialization.

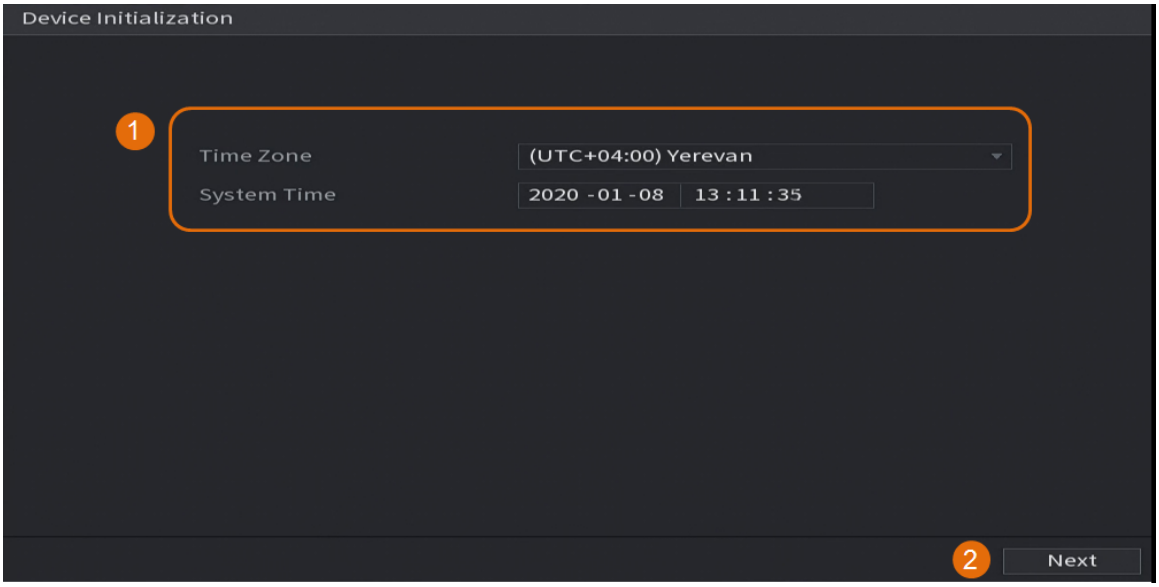
Figure 1-1 Set region, language and video standard



Step 3 Read the Software License Agreement and select **I have read and agree to all terms** , and then click **Next**.

Step 4 Select time zone and configure system time, and then click **Next**.

Figure 1-2 Configure time zone and system time



Step 5 Configure the password information for device administrator, and then click **Next**.

Figure 1-3 Configure password information

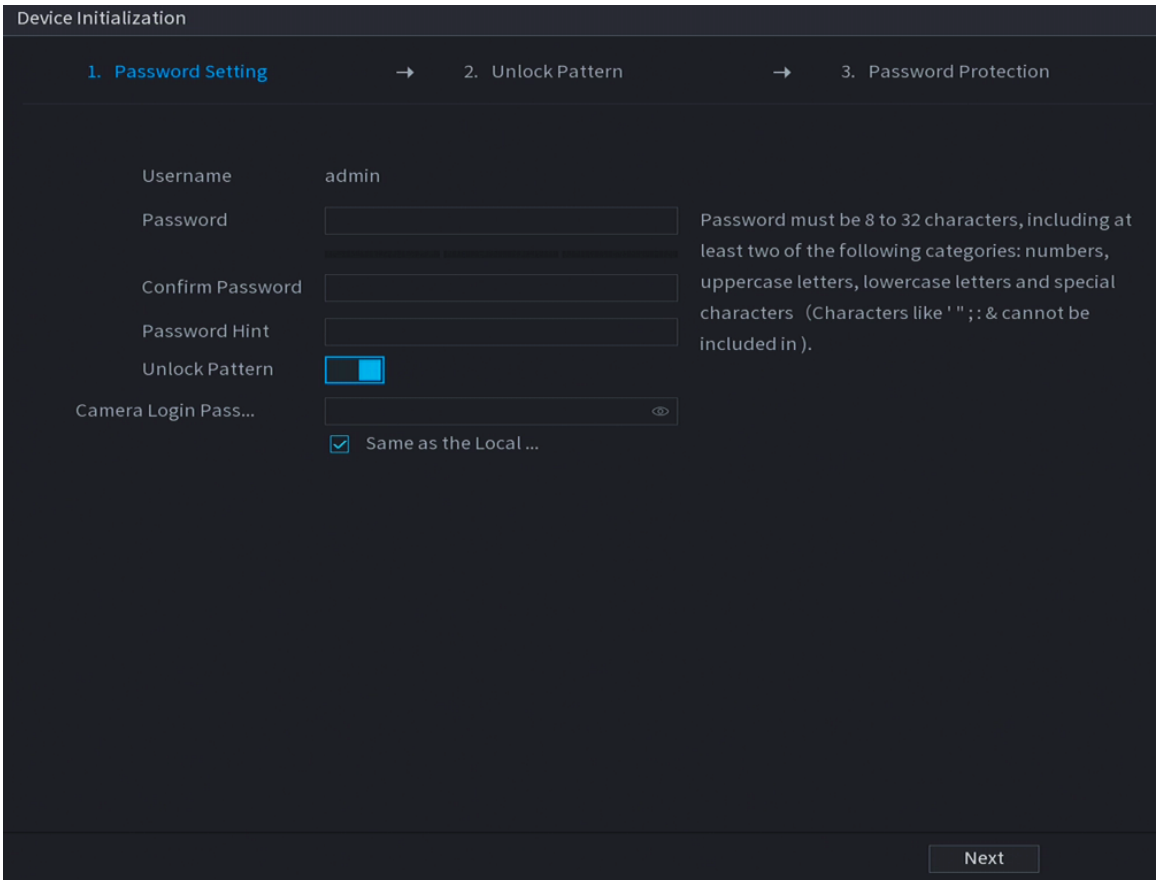
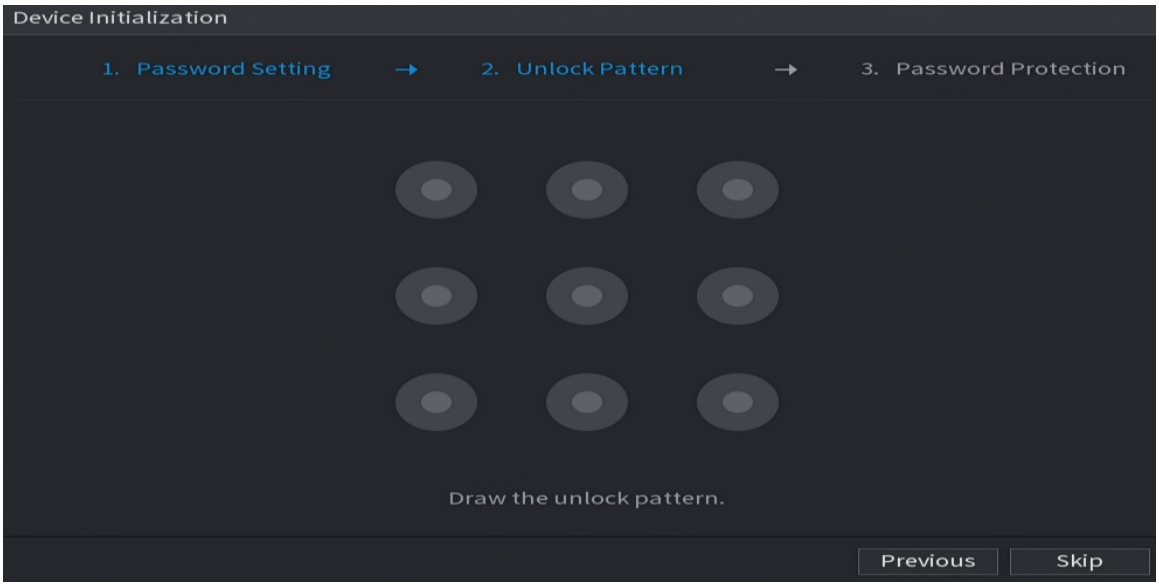


Table 1-1 Password information

Parameter	Description
Username	By default, the username is **admin** and you cannot change it.
Password	Enter a new password for device administrator in **Password** field, and confirm the password in the next field.
Confirm Password	
Password Hint	Enter a prompt question that will help you recall the password for your device. On the login interface, click  and the prompt will be displayed to help you reset the password.

Step 6 (Optional) Use mouse to draw an unlock pattern, and then draw it again for confirmation.

Figure 1-4 Draw an unlock pattern



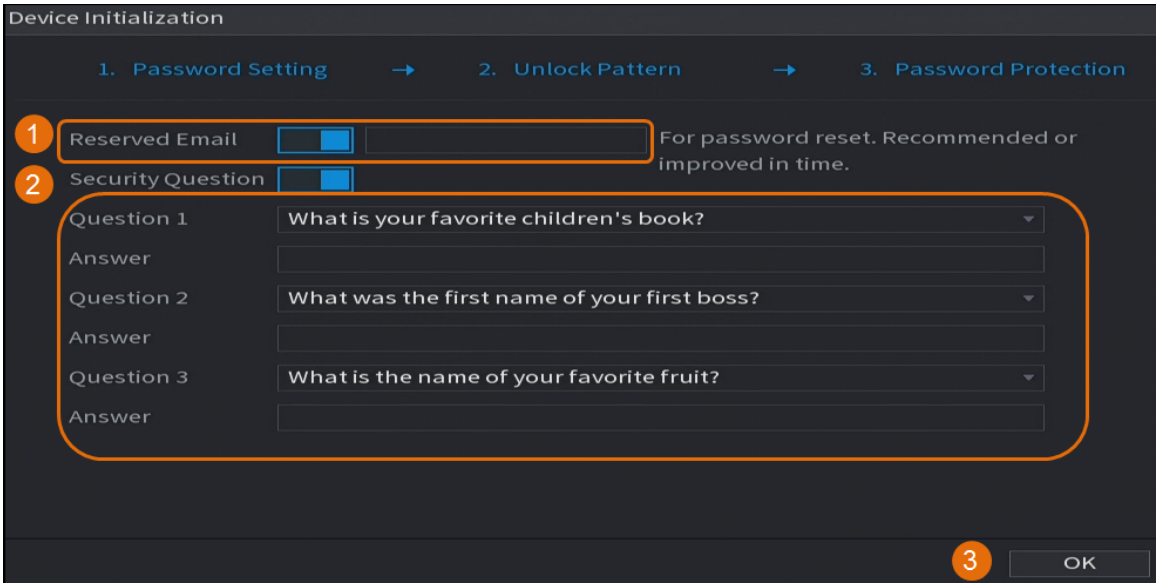
- The pattern that you want to set must cross at least four points.
- If you do not want to configure the unlock pattern, click **Skip**.
- Once you have configured the unlock pattern, it will be used as the default authentication method. If you skip this setting, enter the password for login.

Step 7 (Optional) Apply reserved email and security questions to the DVR.

After configuration, if you forgot the password for admin user, you can reset the password through the linked email address or security questions.

- Enable **Reserved Email** and enter the email address.
- Enable **Security Question** and select questions from the drop-down lists for **Question 1**, **Question 2**, and **Question 3**, and then enter the answers to those questions.

Figure 1-5 Apply reserved email and security questions



Step 8 Click **OK**.

1.3 Configuring Network

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

Procedure

Step 1 Select **Main Menu** > **NETWORK** > **TCP/IP**.

Step 2 Configure parameters.

You can also configure network parameters in the Startup Wizard.

Figure 1-6 TCP/IP

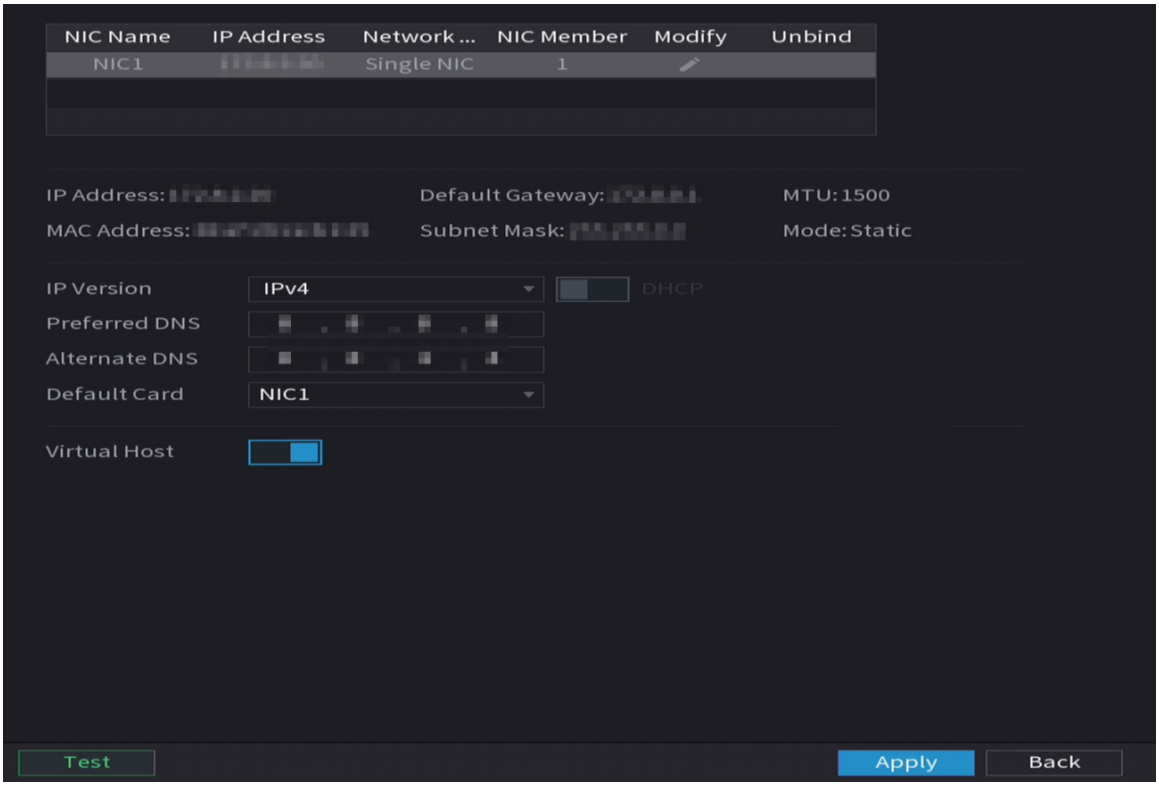


Table 1-2 TCP/IP parameters

Parameter	Description
IP Version	In the **IP Version** list, you can select **IPv4** or **IPv6**. Both versions are supported for access.
MAC Address	Displays the MAC address of the DVR.
DHCP	Enable the DHCP function. The IP address, subnet mask and default gateway are not available for configuration once DHCP is enabled. • If DHCP is effective, the obtained information will be displayed in the **IP Address**, **Subnet Mask** and **Default Gateway**. If not, all values show 0.0.0.0. • If PPPoE connection is successful, the IP address, subnet mask, default gateway, and DHCP are not available for configuration.
IP Address	Enter the IP address and configure the corresponding subnet mask and default gateway. IP address and default gateway must be in the same network segment.
Subnet Mask	
Default Gateway	
Preferred DNS	Enter the IP address of DNS.
Alternate DNS	Enter the IP address of alternate DNS.

Parameter	Description
MTU	Enter a value for network card. The value ranges from 1280 byte to 1500 byte. The default is 1500. The suggested MTU values are as below. ● 1500: The biggest value of Ethernet information package. This value is typically selected if there is no PPPoE or VPN connection, and it is also the default value of some routers, network adapters and switches. ● 1492: Optimized value for PPPoE. ● 1468: Optimized value for DHCP. ● 1450: Optimized value for VPN.
Test	Click **Test** to test if the entered IP address and gateway are interworking.

Step 3 Click **OK**.

1.4 Configuring Encode Setting

This topic shows how to set encode settings for each channel.

Procedure

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

Step 2 Configure the parameters of the main/sub streams.

Figure 1-7 Audio/Video

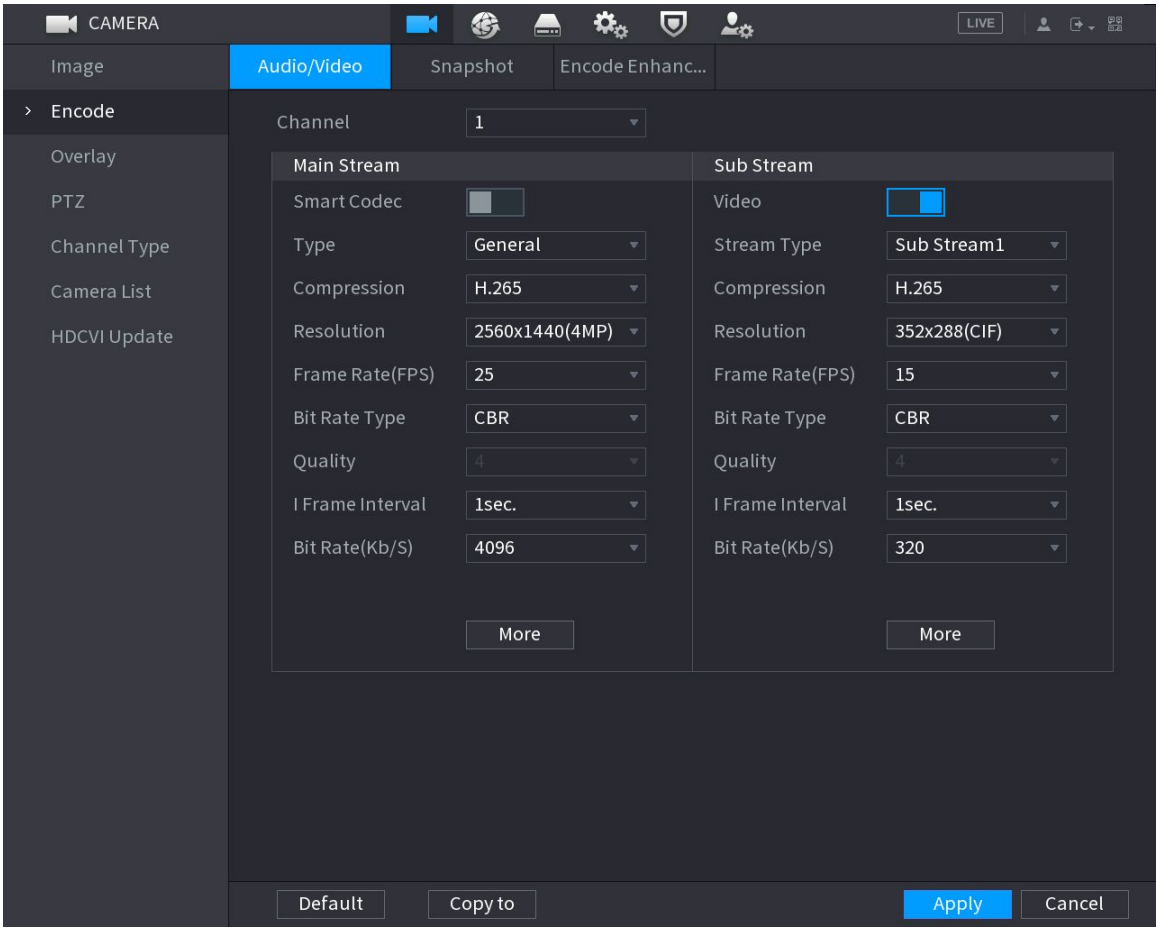


Table 1-3 Audio/Video parameters

Parameter	Description
Channel	In the **Channel** list, select the channel that you want to configure the settings for.
Smart Codec	Enable the smart codec function. This function can reduce the video bit stream for non-important recorded video to maximize the storage space.
Type	• Main Stream: From the **Type** drop-down list, select **General**, **Motion**, or **Alarm**. • Sub Stream: This setting is not configurable.
Compression	In the **Compression** list, select the encode mode. • H.265: Main profile encoding. This setting is recommended. • H.264H: High profile encoding. Low bit stream with high definition. • H.264: General profile encoding. • H.264B: Baseline profile encoding. This setting requires higher bit stream compared with other settings for the same definition.

Parameter	Description
Resolution	From the Resolution list, select a resolution for video output. The maximum video resolution may vary model to model.
Bit Rate Type	From the **Bit Rate Type** drop-down list, select resolution for the video. The maximum video resolution might be different dependent on your device model.
Frame Rate (FPS)	Configure the frames per second for the video. The higher the value, the clearer and smoother the image will become. Frame rate changes along with the resolution. Generally, in PAL format, you can select the value from 1 to 25; in NTSC format, you can select the value from 1 to 30. However, the specific range of frame rate that you can select depends on the capability of the DVR.
Quality	This function is available if you select **VBR** in the **Bit Rate** List. The higher the value, the better the image will become.
I Frame Interval	The interval between two reference frames.
Bit Rate (Kb/S)	From the **Bit Rate** drop-down list, select a value or enter a customized value to change the image quality. The bigger the value is, the better the image will become.
Video	Enable the function for sub stream.
Audio Audio Source Compression	Click **More**, the **More** interface is displayed. ● Audio: This function is enabled by default for main stream. You need to manually enable it for sub stream 1. Once this function is enabled, the recorded video file is composite audio and video stream. ● Audio Source: In the **Audio Source** list, you can select **LOCAL** and **HDCVI**. ◇ **LOCAL**: The audio signal is input from Audio input port. ◇ **HDCVI**: The audio signal is input from HDCVI camera. ● Audio Format: From the **Compression** drop-down list, select a format as needed.

Step 3 Click **Apply**.

You can click **Copy to** to copy the settings to other channels.

1.5 Adding IP Camera

You can add an IP camera by search result or by manually entering IP information. Before adding IP camera, you shall change at least one analog channel to IP channel.

Cameras you want to add must be in the same network with the DVR.

1.5.1 Changing Channel Type

You can convert channel type to IP channel when you need to add IP camera to the DVR.

Background Information

All channels of the DVR are set as analog channels by default, and you can convert them to IP channels.

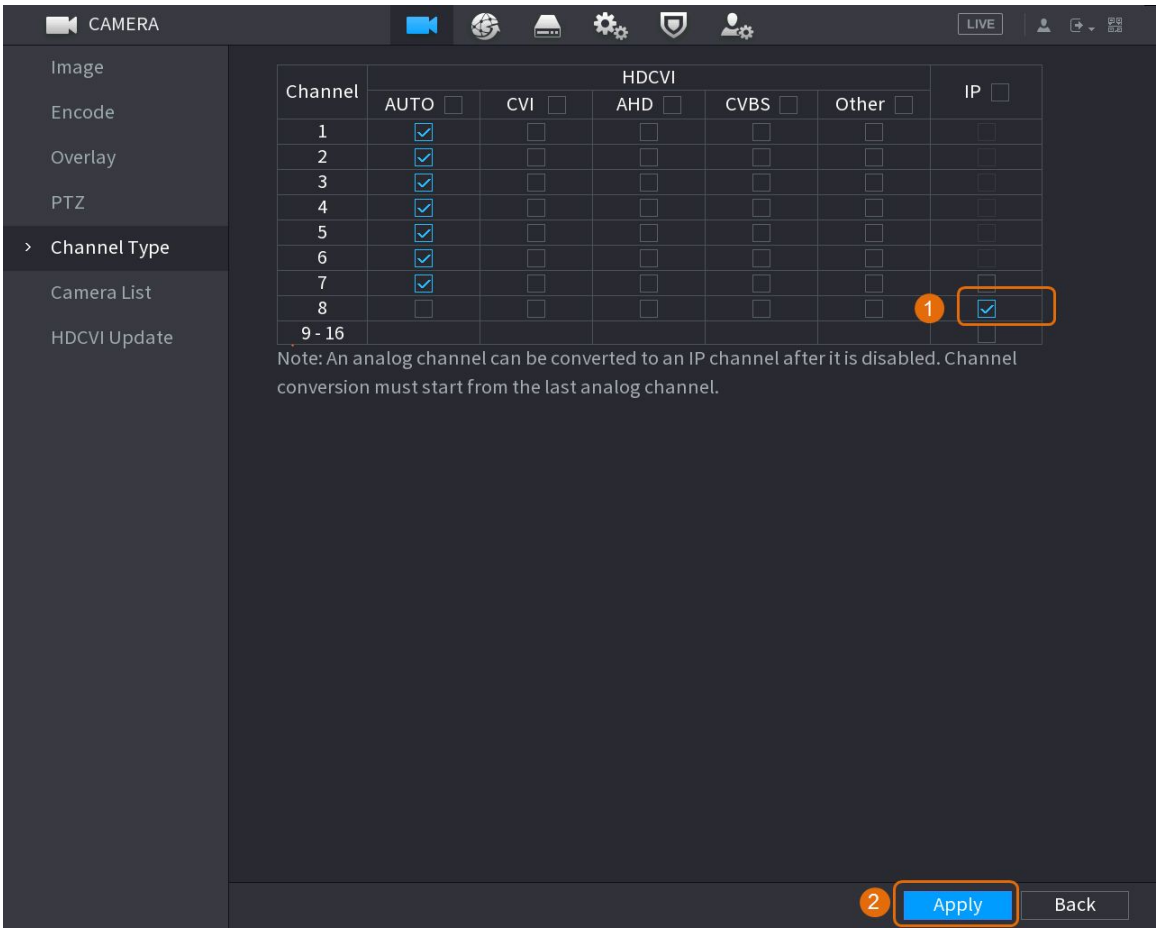
Procedure

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

Step 2 Select the check box(es) in **IP** column.

- The channel selection for analog camera or IP camera are in sequence, for example, if you want to convert channels for IP cameras, you need to select from the last channel number Channel **8** first, which means, you cannot select channel **7**directly until you have selected channel **8**.
- In the case of the following figure, the 9–16 channels are only for IP cameras and the range varies with the model you purchased. The actual product shall prevail.

Figure 1-8 Select IP channel



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

1.5.2 Initializing IP Camera

The topic shows how to initialize new cameras or the cameras after restoring factory defaults.

Background Information

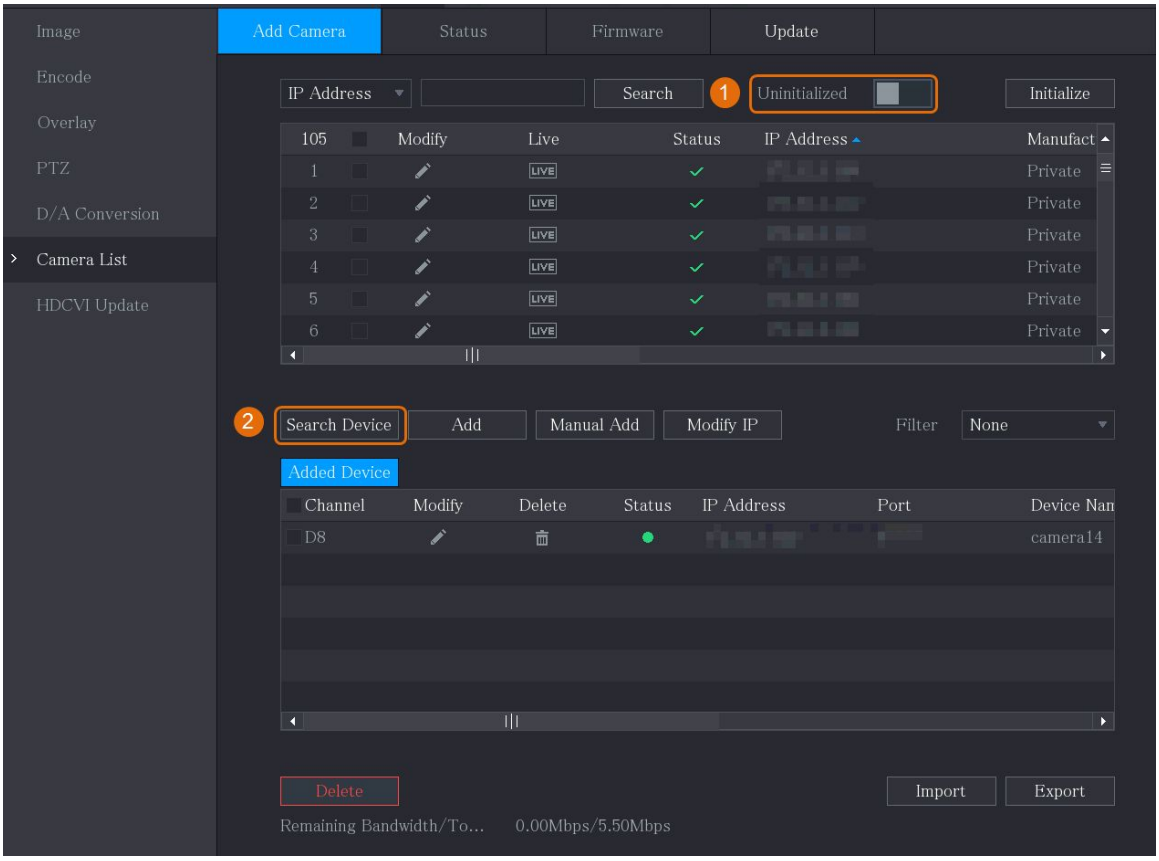
The IP camera shall be initialized before connecting to an DVR, otherwise the connection will fail. The initialization will change IP camera's login password and IP address.

Procedure

Step 1 Select **Main Menu** > **Camera** > **Camera List** > **Add Camera**.

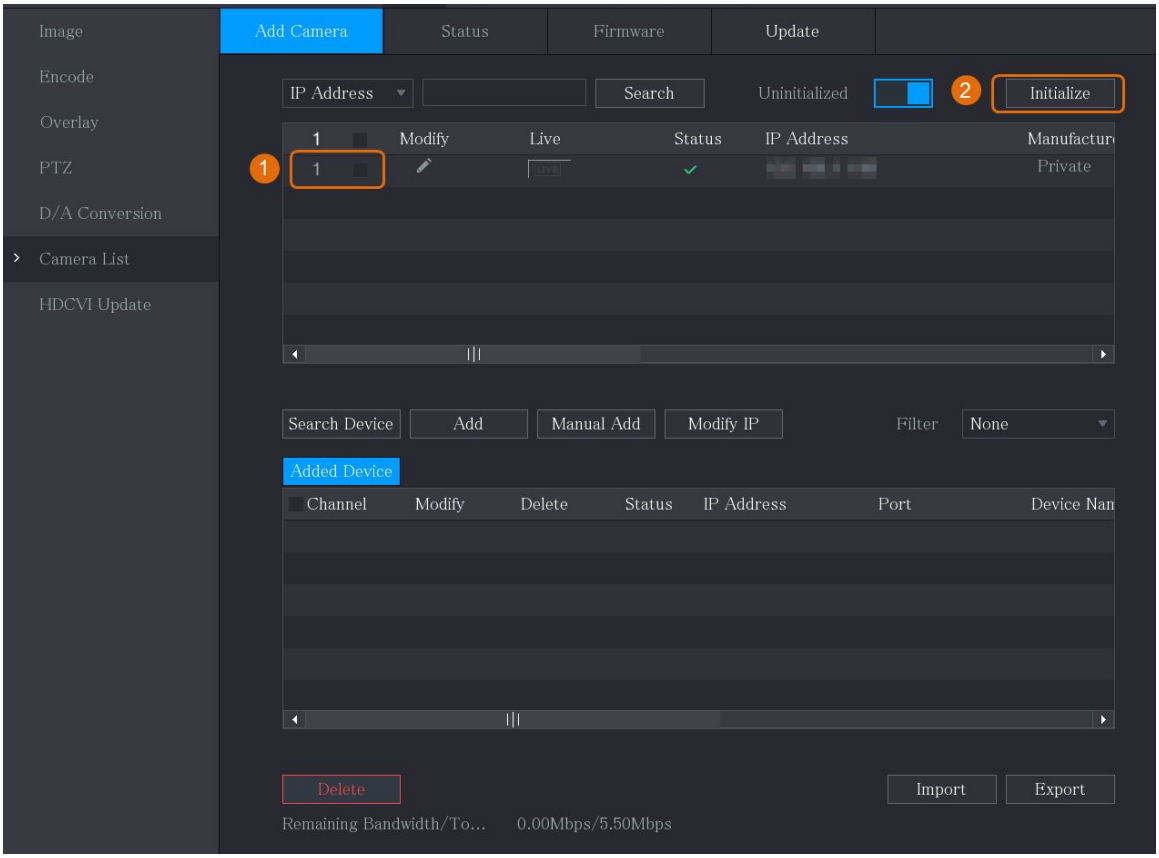
Step 2 Enable **Uninitialized** , and then click **Search Device**.

Figure 1-9 Search uninitialized device



Step 3 Select the camera to be initialized and then click **Initialize**.

Figure 1-10 Initialize the camera

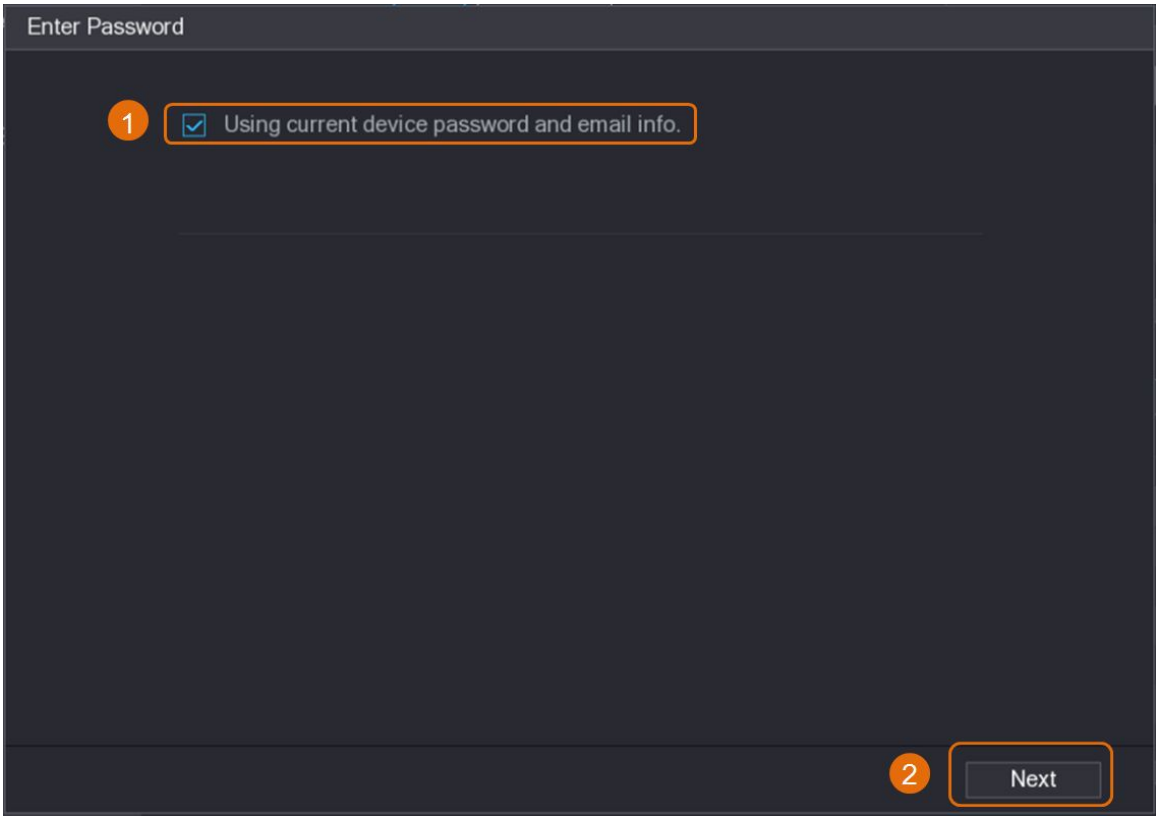


Step 4 Apply password and email information to the IP camera.

- Use the DVR's settings.
  1. Select **Using current device password and email info.**.

     This check box is selected by default.

Figure 1-11 Apply device settings

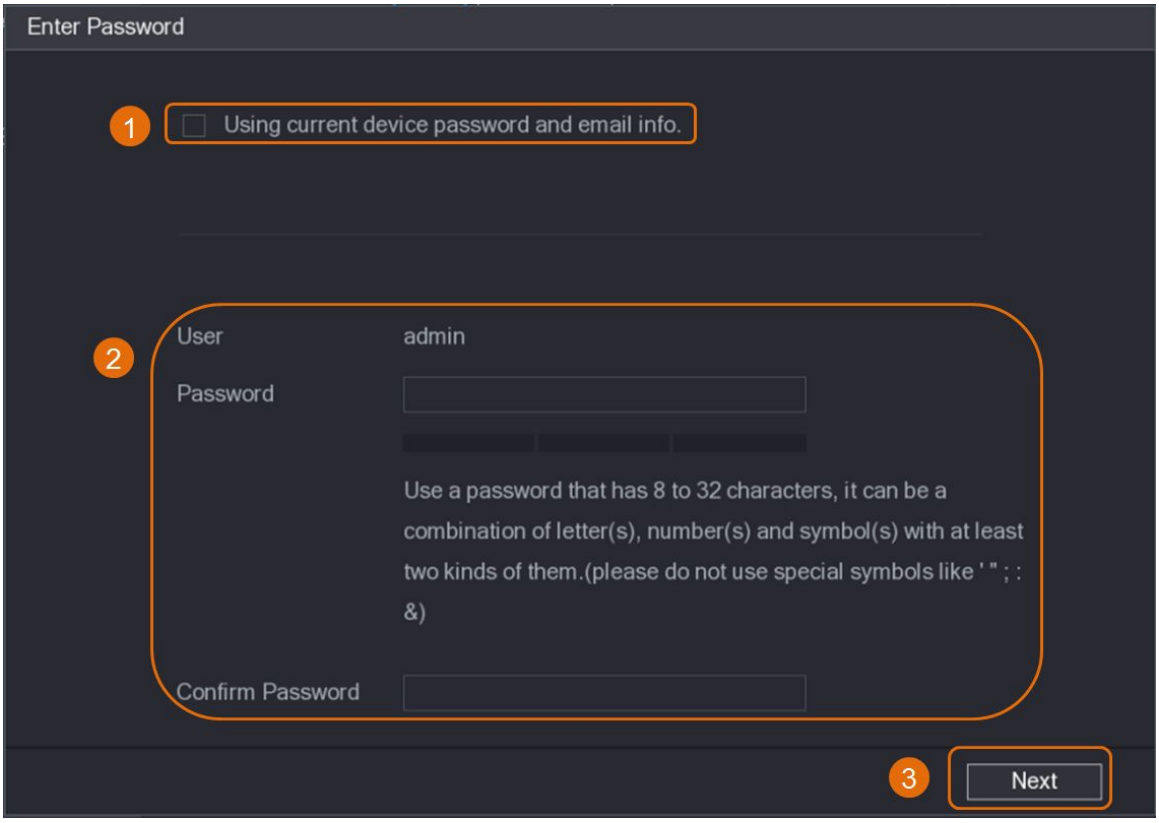


2. Click **Next**.

- Manually set password and email information.

1. Cancel **Using current device password and email info.**.

Figure 1-12 Set password



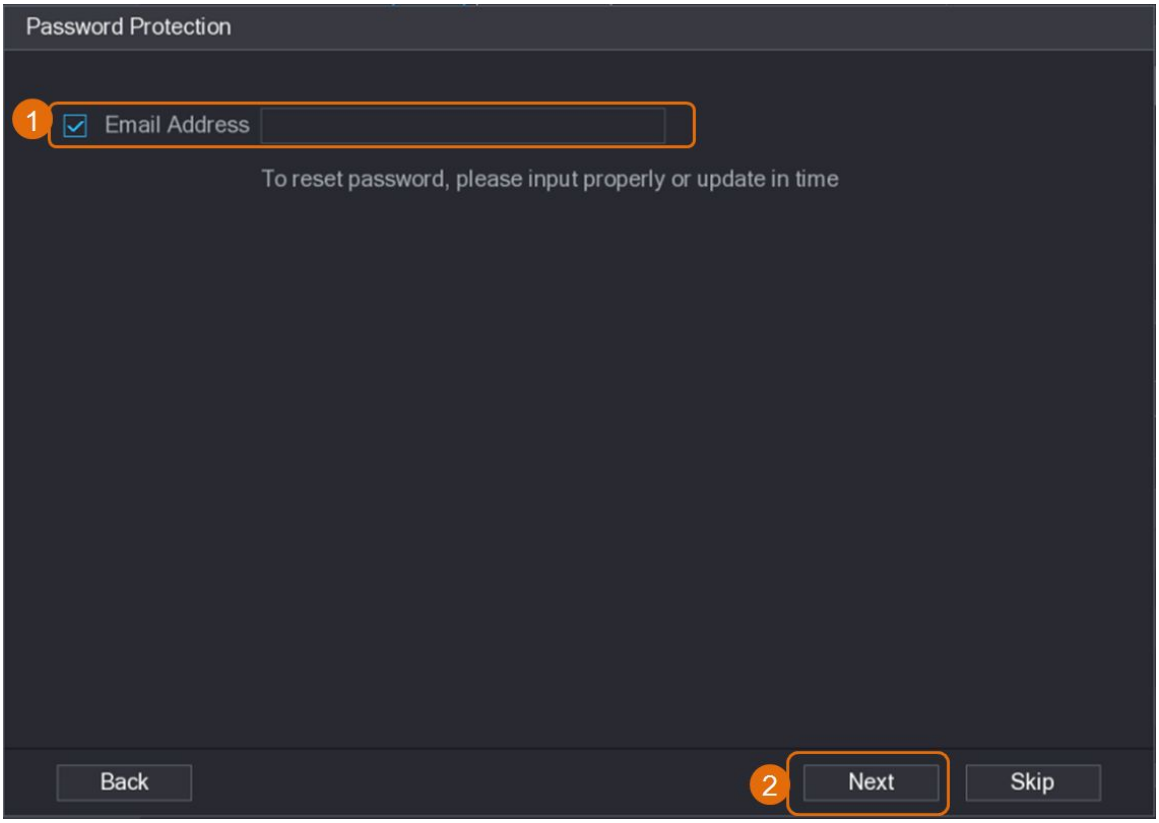
2. Set password.

Table 1-4 Password

Parameter	Description
User	The default value is **admin** that cannot be changed.
Password	The new password can be set from 8 characters to 32 characters and contains at least two types from numbers, letters and special characters (excluding"'", """, ";", ":" and "&"). Enter a strong password according to the password strength bar indication.
Confirm Password	

3. Click **Next**.
4. Enter an email address and click **Next**.

Figure 1-13 Set email information

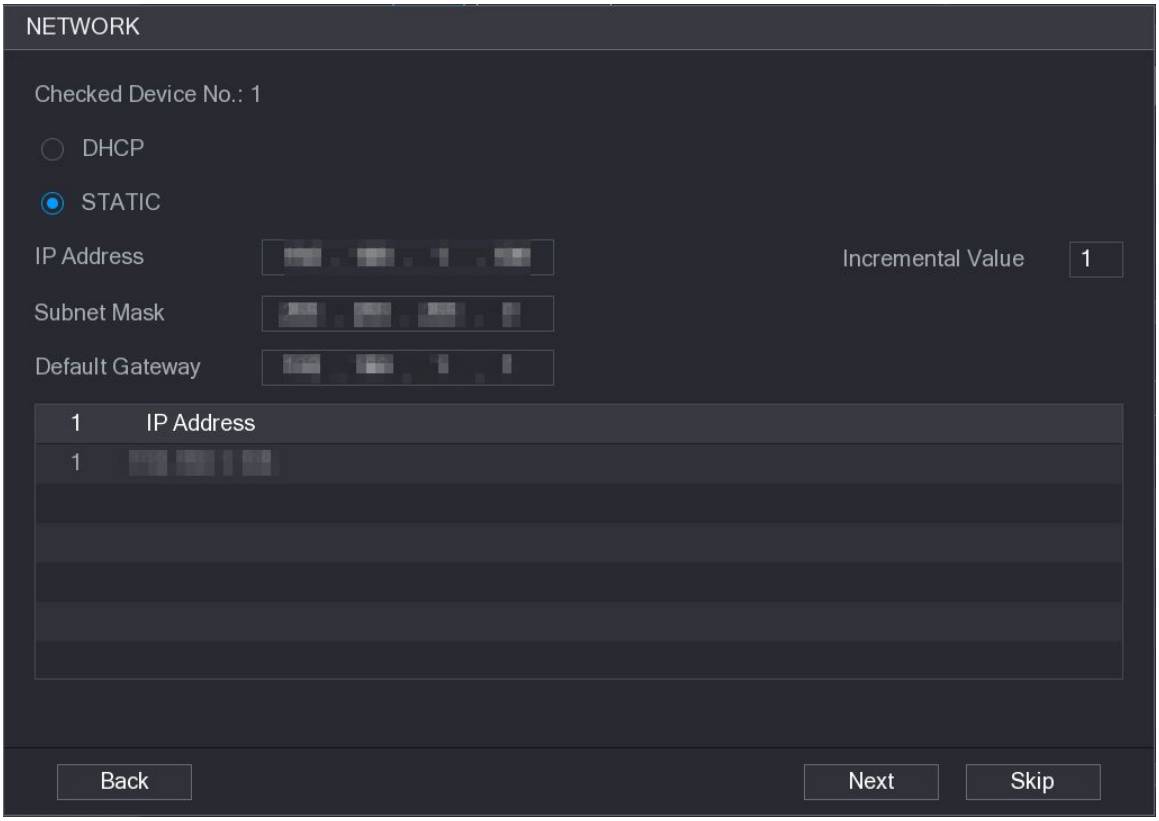


Step 5 Configure camera IP address.

- Select **DHCP** if there is a DHCP server deployed.
- Select **Static**, and then input IP address, subnet mask, default gateway and incremental value.

Set the incremental value when you need to change IP addresses of multiple cameras at one time. The DVR will incrementally add the value on to the fourth section of the IP address when allocate IP addresses for those cameras.

Figure 1-14 Configure IP address



Step 6 Click **Next**.

Wait 1–2 minutes for the initialization to complete.

Step 7 Click **Finished**.

1.5.3 Adding IP Camera by Search Result

Prerequisites

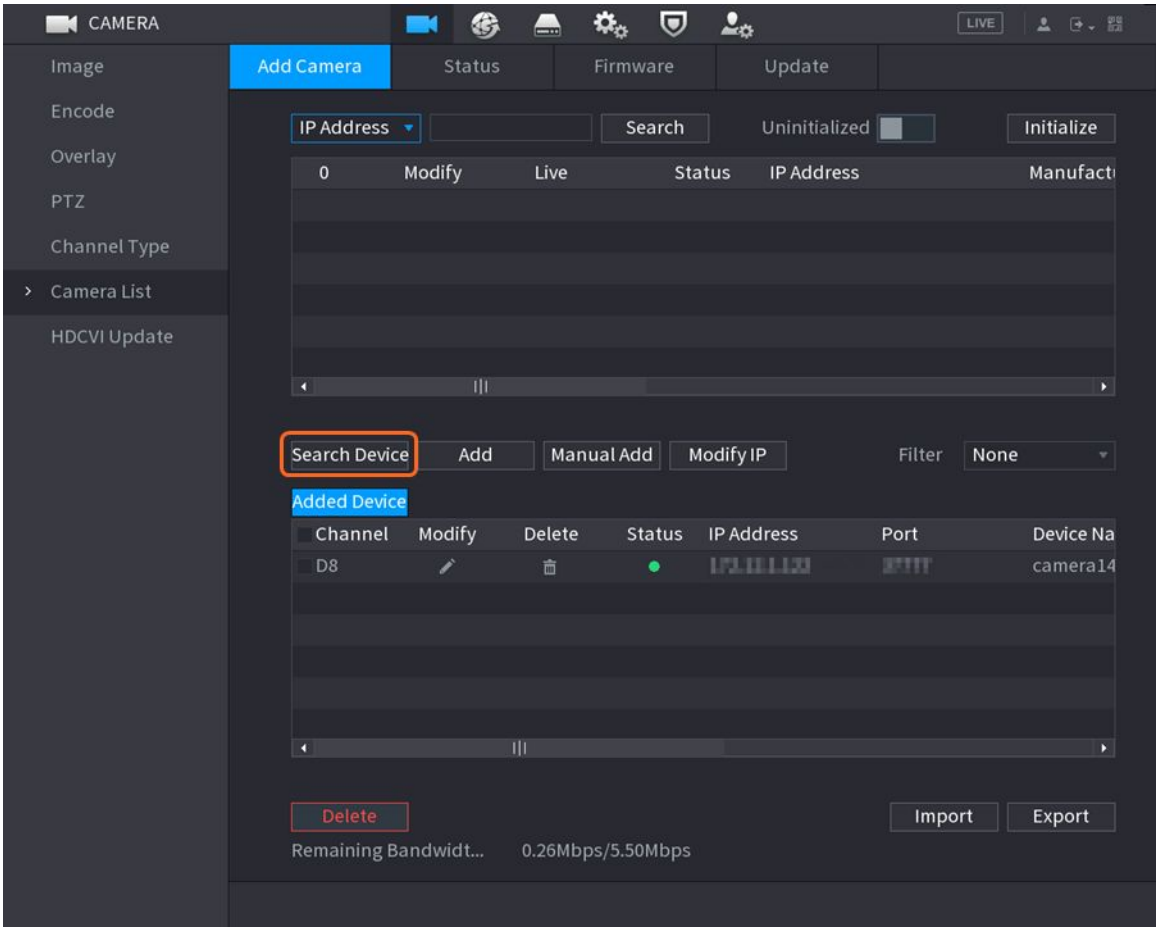
Make sure that the cameras you want to add have already been initialized and connected to the right network.

Procedure

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

Step 2 Click **Search Device**.

Figure 1-15 Search device



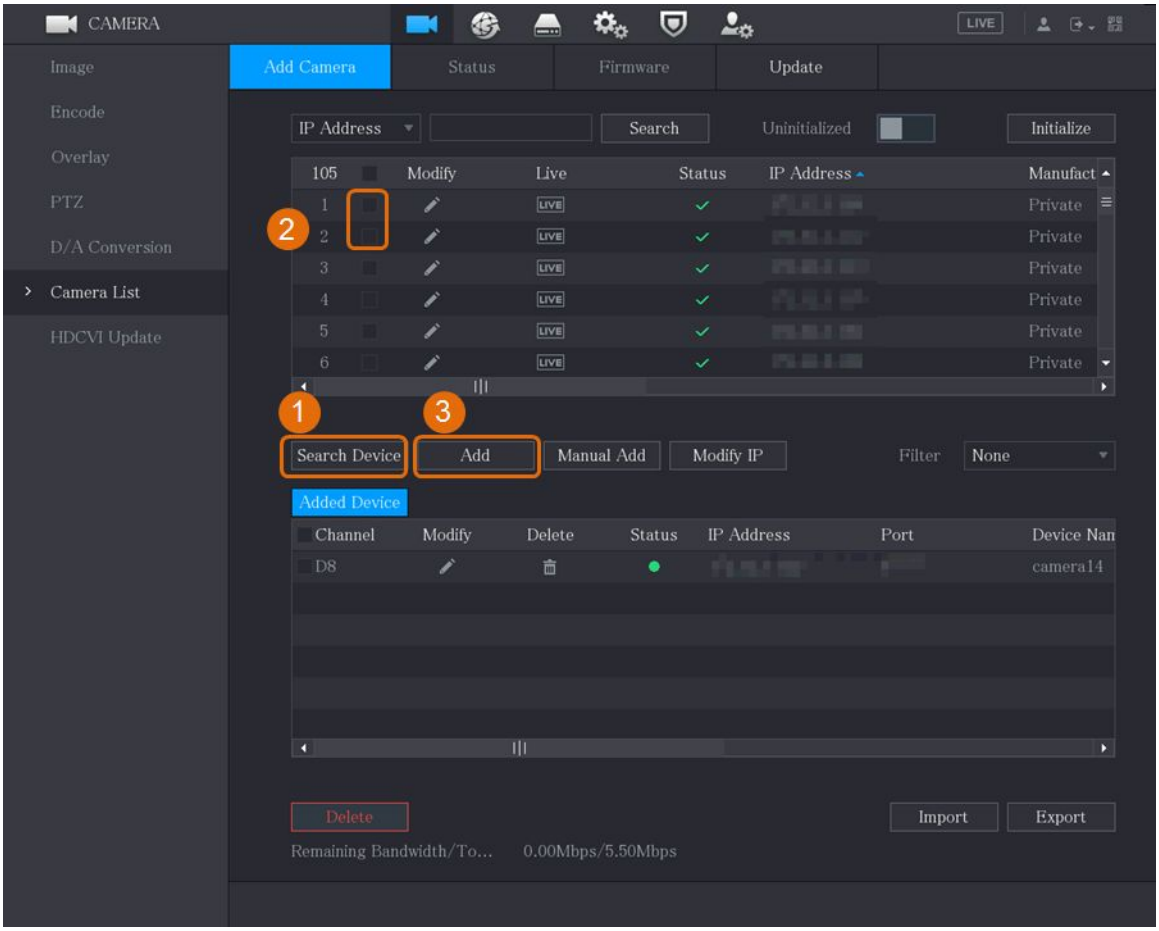
Step 3 Add IP cameras.

- Add by double-click: Double-click the target camera to add it to **Added Device** list.

  You can only add one camera by search result at one time.
- Add by check box: Select the check box of the target camera, and then click **Add** to add it to **Added Device** list.

  You can select more than one check box and add cameras in batches.

Figure 1-16 Add IP camera by search result



Results

- If the status of the added camera is green (), it indicates the camera is properly added to the DVR.
- If the status of the added camera is red (), it indicates connection failure between the camera and the DVR. Check the parameters of the camera such as password, protocol and channel number, and then try adding it again.

1.5.4 Manually Adding IP Camera

You can add an IP camera by IP information at one time.

Prerequisites

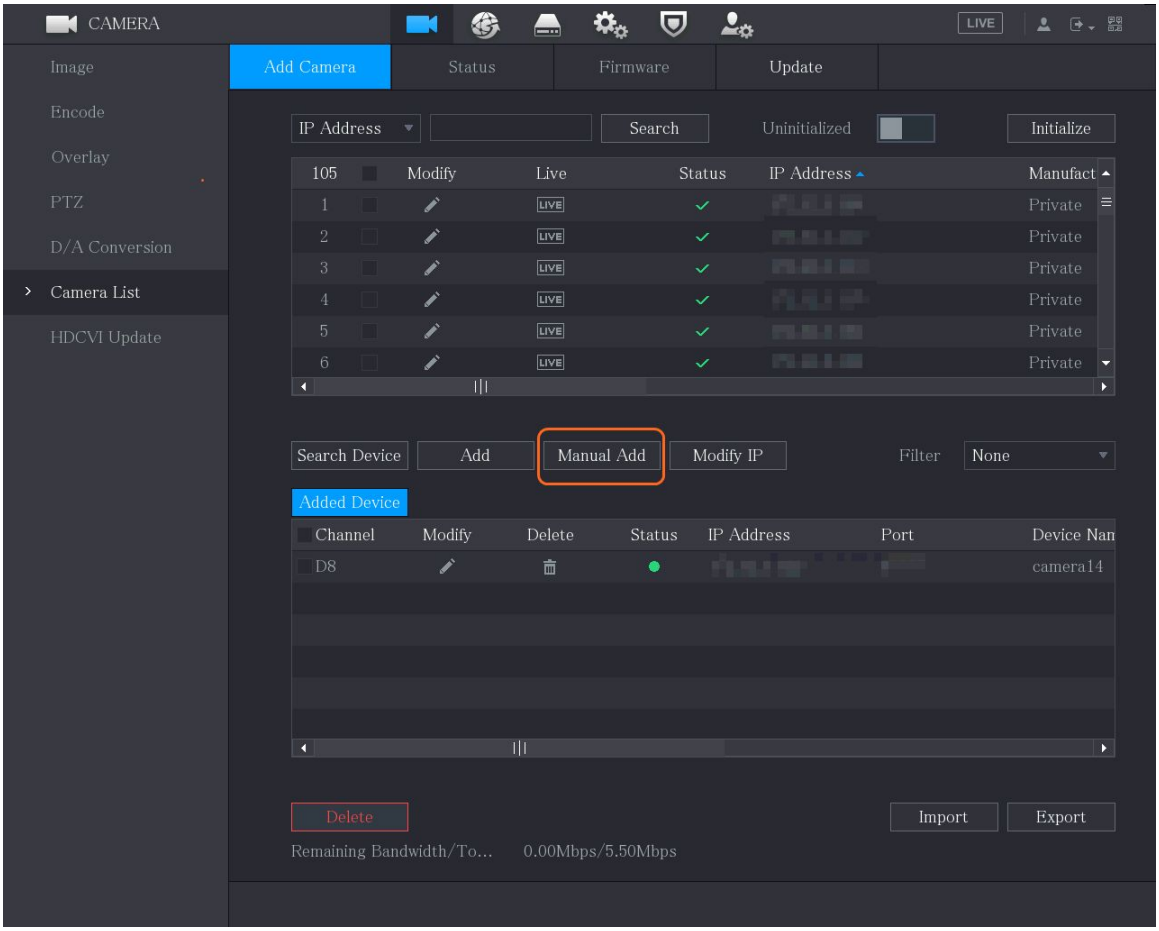
Make sure that the cameras you want to add have already been initialized and connected to the right network.

Procedure

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

Step 2 Click **Manual Add**.

Figure 1-17 Manual add



Step 3 In the **Manual Add** dialog box, configure parameters.

Figure 1-18 Configure manual add parameters

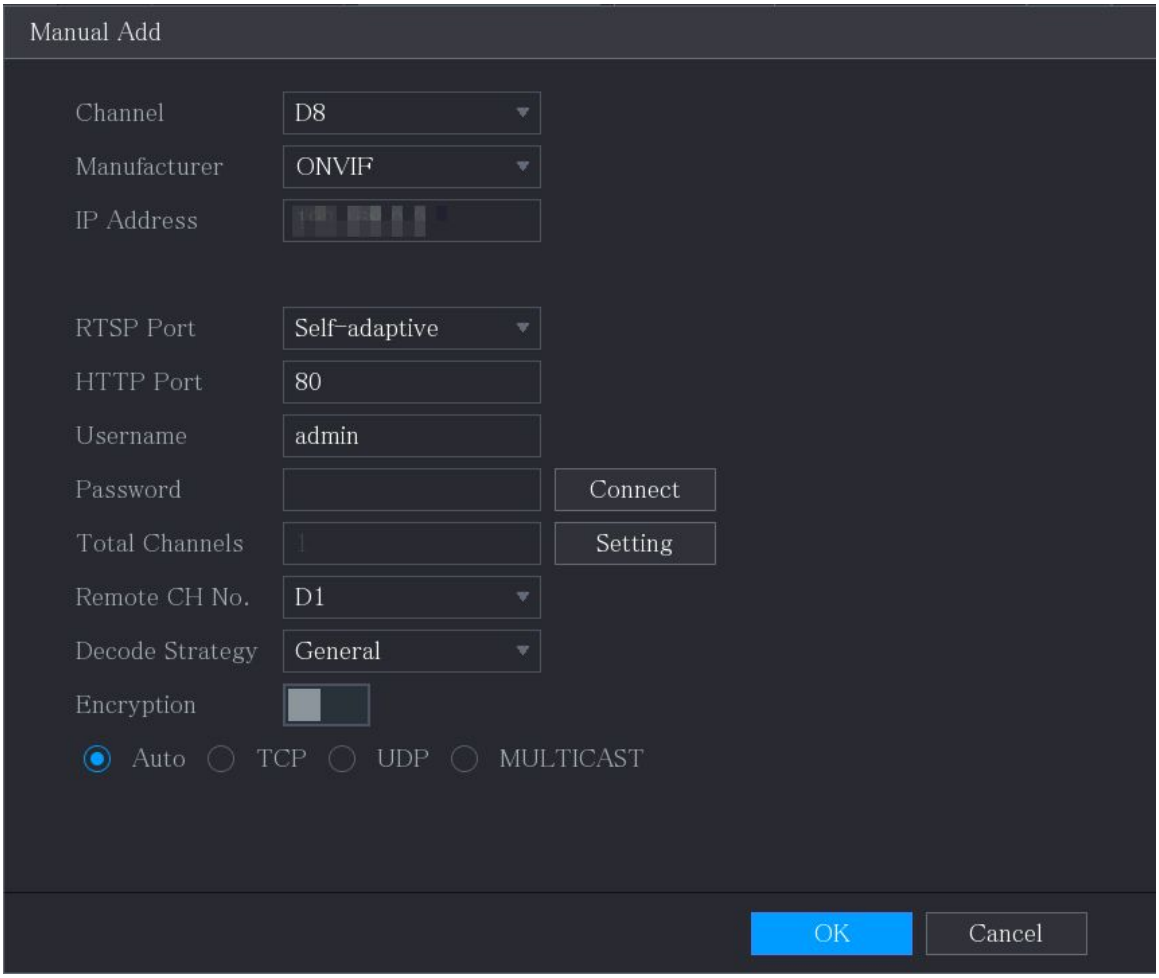


Table 1-5 Manual add parameters

Parameter	Description
Channel	From the **Channel** drop-down list, select the channel that you want use on the DVR to connect the remote device.
Manufacturer	From the **Manufacturer** drop-down list, select the manufacturer of the remote device.
IP Address	In the **IP Address** field, enter the IP address of the IP camera. Change the default value (192.168.0.0) which the system cannot connect to.
RTSP Port	The default value is 554. You can change the value as needed.
HTTP Port	The default value is 80. You can change the value as needed. If you enter another value, for example, 70, and then you should enter 70 after the IP address when logging in to the DVR by browser.
TCP Port	The default value is 37777. You can change the value as needed.

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

Step 4 Click **OK**.

1.6 Configuring Recorded Video Storage Schedule

By default, all cameras continuously record videos 24 hours a day. You can modify the settings as needed.

You can also configure storage schedule in the Startup Wizard.

1. Select **Main Menu** > **STORAGE** > **Schedule** > **Record**.
2. Configure parameters.
3. Set the schedule by drawing or editing.
4. Click **Apply**.

1.7 Configuring P2P Settings

You can use the QR code to connect a smart phone to the DVR for management.

Make sure that the DVR has been connected to the Internet, and if yes, in the **Status** box of the P2P interface, it shows **Online**.

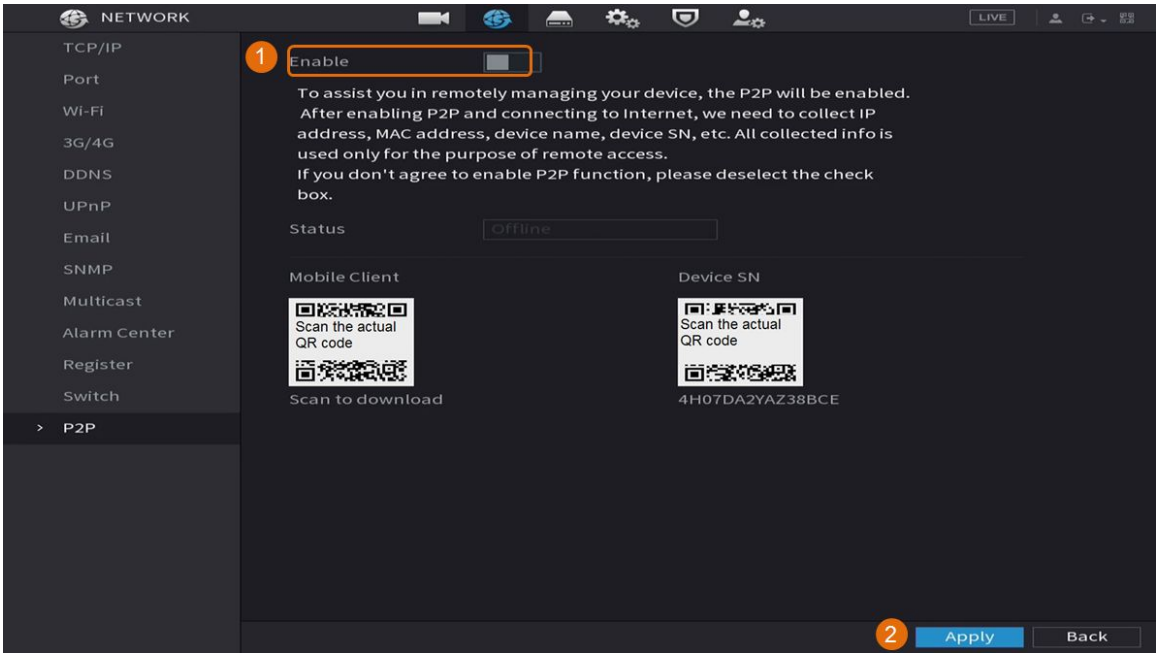
1.7.1 Enabling P2P Function

You need to enter P2P interface to enable P2P function and scan the QR code to download the smart phone application.

Procedure

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

Figure 1-20 P2P



Step 2 Click **Enable** to enable P2P function.

Step 3 Click **Apply**

1.7.2 Adding the DVR to Smart Phone Client

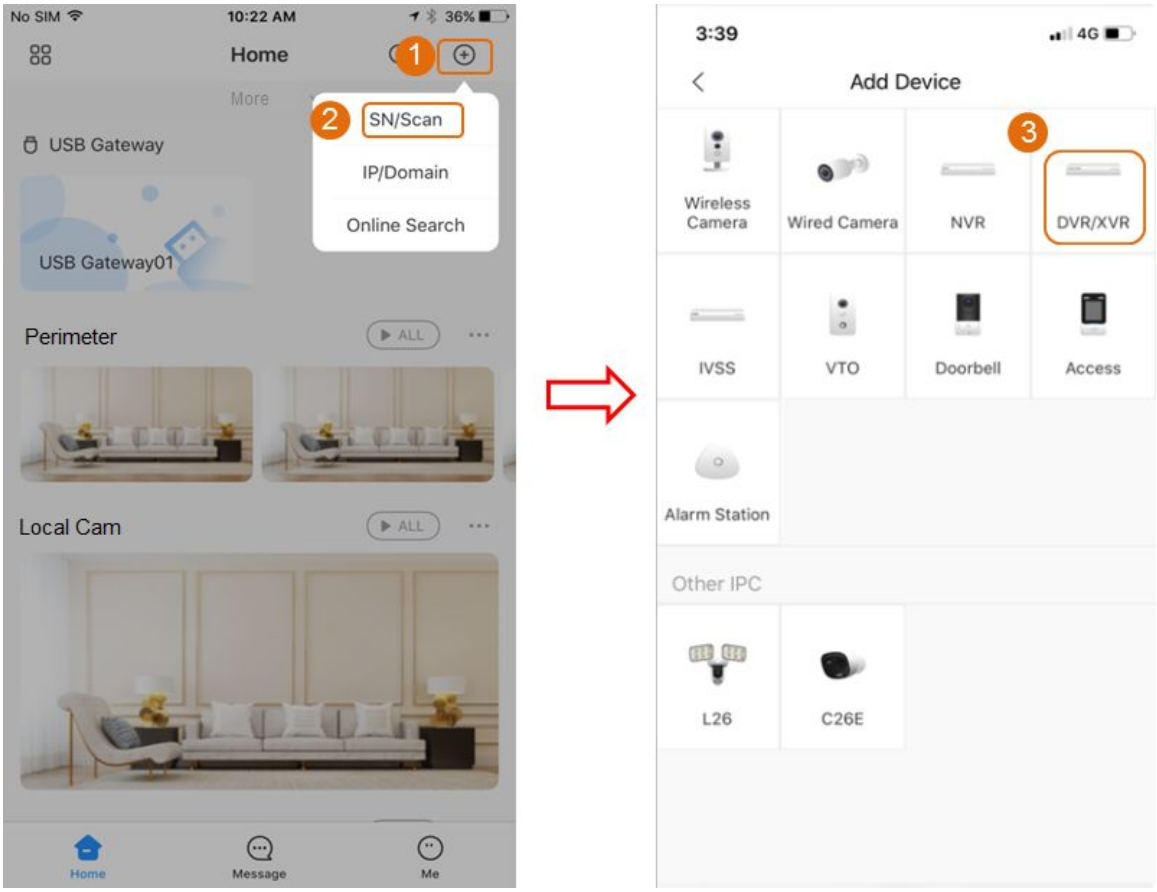
This topic takes adding the DVR to smart phone client as an example for smart phone management.

Procedure

Step 1 Open the application and tap .

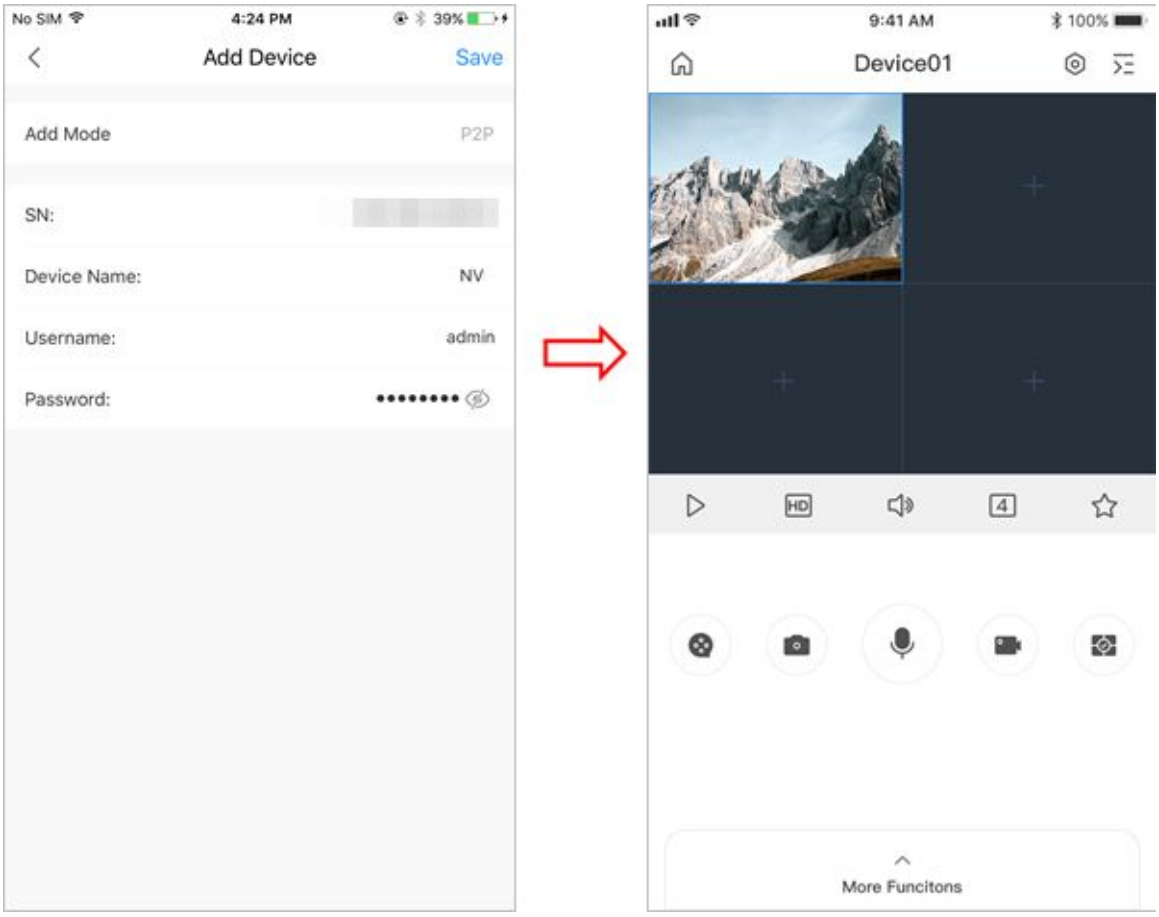
Step 2 Select **SN/Scan**.

Figure 1-21 Add device



Step 3 Select **DVR/XVR**, enter a name and password for the DVR, and then tap **Save**.

Figure 1-22 Start live view



1.8 Smart Motion Detection

This topic shows how to configure Smart Motion Detection (SMD).

Background Information

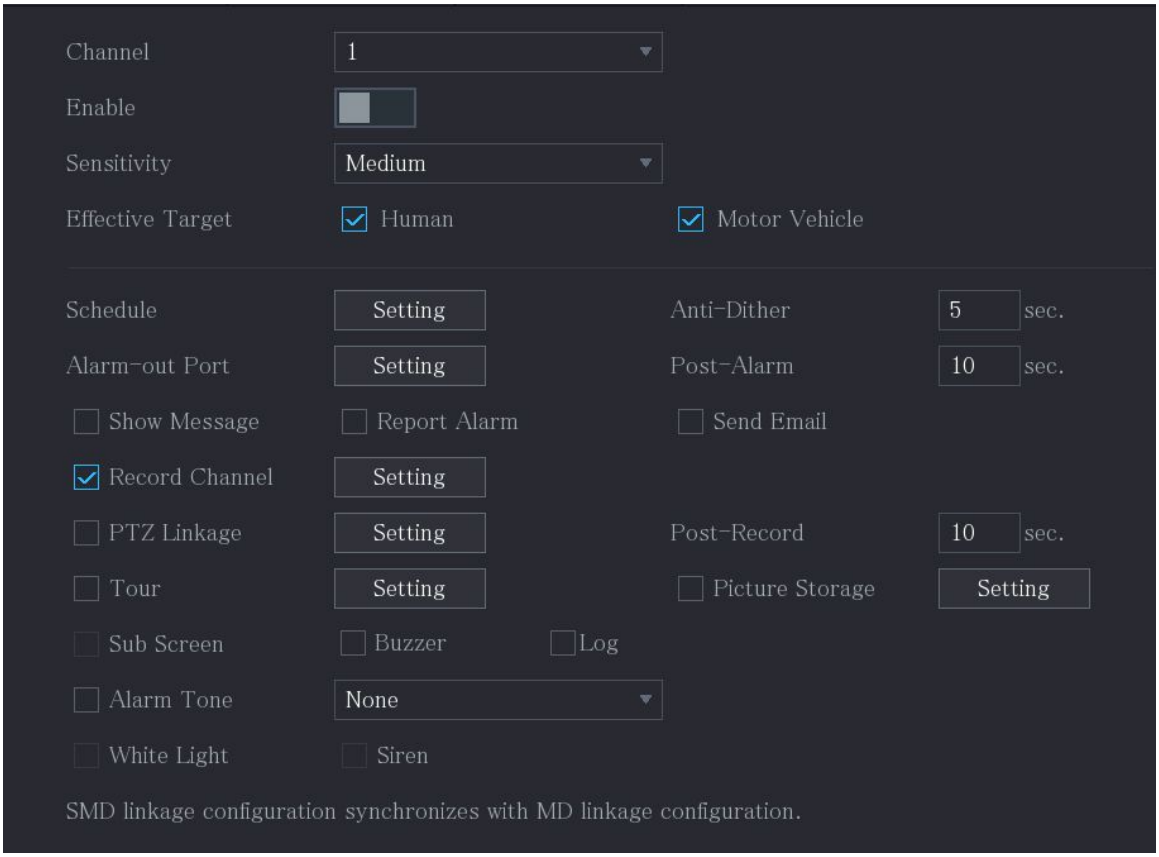
The Smart Motion Detection (SMD) is an ideal monitoring feature for low populated areas where you want an alert for human or vehicles anywhere in the scene without having to set rules and draw lines.

Procedure

Step 1 Select .

The **SMD** interface is displayed.

Figure 1-23 SMD



Step 2 Select the channel and enable.

Step 3 Set parameters.

Parameter	Description
Channel	In the **Channel** list, select a channel to set the motion detection.
Enable	Enable or disable SMD function.
Sensitivity	Set sensitivity, including high, middle, and low. The higher the sensitivity is, the bigger alarm probability will be, the bigger false alarm rate will be. The system selects middle by default.
Effective Target	Select alarm object, including person and vehicle.
Schedule	Define a period during which the motion detection is active.
Anti-Dither	Configure the time period from end of event detection to the stop of alarm.
Alarm-out Port	Click **Setting** to display setting interface. • General Alarm: Enable alarm activation through the alarm devices connected to the selected output port. • External Alarm: Enable alarm activation through the connected alarm box. • Wireless Siren: Enable alarm activation through devices connected by USB gateway or camera gateway.

Parameter	Description
Post-Alarm	Set a length of time for the Device to delay turning off alarm after the external alarm is cancelled. The value ranges from 0 seconds to 300 seconds, and the default value is 10 seconds. If you enter 0, there will be no delay.
Show Message	Select the **Show Message** check box to enable a pop-up message in your local host PC.
Report Alarm	Select the **Report Alarm** check box to enable the system to upload the alarm signal to the network (including alarm center) when an alarm event occurs.
Send Email	Select the **Send Email** check box to enable the system to send an email notification when an alarm event occurs.  To use this function, make sure that the email function is enabled in **Main Menu** > **NETWORK** > **EMAIL**.
Record Channel	Select the channel(s) that you want to record. The selected channel(s) starts recording after an alarm event occurs.  The recording for motion detection and auto recording function must be enabled.
PTZ Linkage	Click **Setting** to display the PTZ interface.  Motion Detect can only activate PTZ preset.
Post Record	Set a length of time for the Device to delay turning off recording after the alarm is cancelled. The value ranges from 10 seconds to 300 seconds, and the default value is 10 seconds.
Tour	Select the **Tour** check box to enable a tour of the selected channels.
Picture Storage	Select the **Snapshot** check box to take a snapshot of the selected channel.  To use this function, select **Main Menu** > **CAMERA** > **Encode** > **Snapshot**, in the **Type** list, select **Event**.
Sub Screen	Select the check box to enable the function. When an alarm event occurs, the extra screen outputs the settings configured in **Main Menu** > **DISPLAY** > **Tour** > **Sub Screen**.  • Not all models support this function. • To use this function, extra screen shall be enabled.
Buzzer	Select the check box to activate a buzzer noise at the Device.
Log	Select the check box to enable the Device to record a local alarm log.

Parameter	Description
Alarm Tone	Select to enable audio broadcast/alarm tones in response to a motion detection event.
White Light	Select the check box to enable the white light alarm of the camera.
Siren	Select the check box to enable the sound alarm of the camera.

Step 4 Click **Apply** to save configuration.

1.9 Live View

After you logged in, the system goes to multiple-channel live view mode by default. You can view the monitoring video of each channel. Note that the number of displayed window may vary model to model.

To enter the live view screen from other interfaces, click LIVE at the upper-right of the screen.

Figure 1-24 Live view



Live View Screen

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

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

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

For the icons displayed on each channel, see "Icon description".

Table 1-7 Icon description

Icon	Description
	Video is being recorded.
	Motion detection occurs in the scene.
	Video loss is detected.
	Channel monitoring is locked.

1.10 Recording Playback

To play back a recording, you can select **Main Menu** > **Playback** or right-click the live view interface and select **Search**.

Figure 1-25 Playback main interface



For details about the instructions on playback main interface, see User's Manual.

Instant Playback

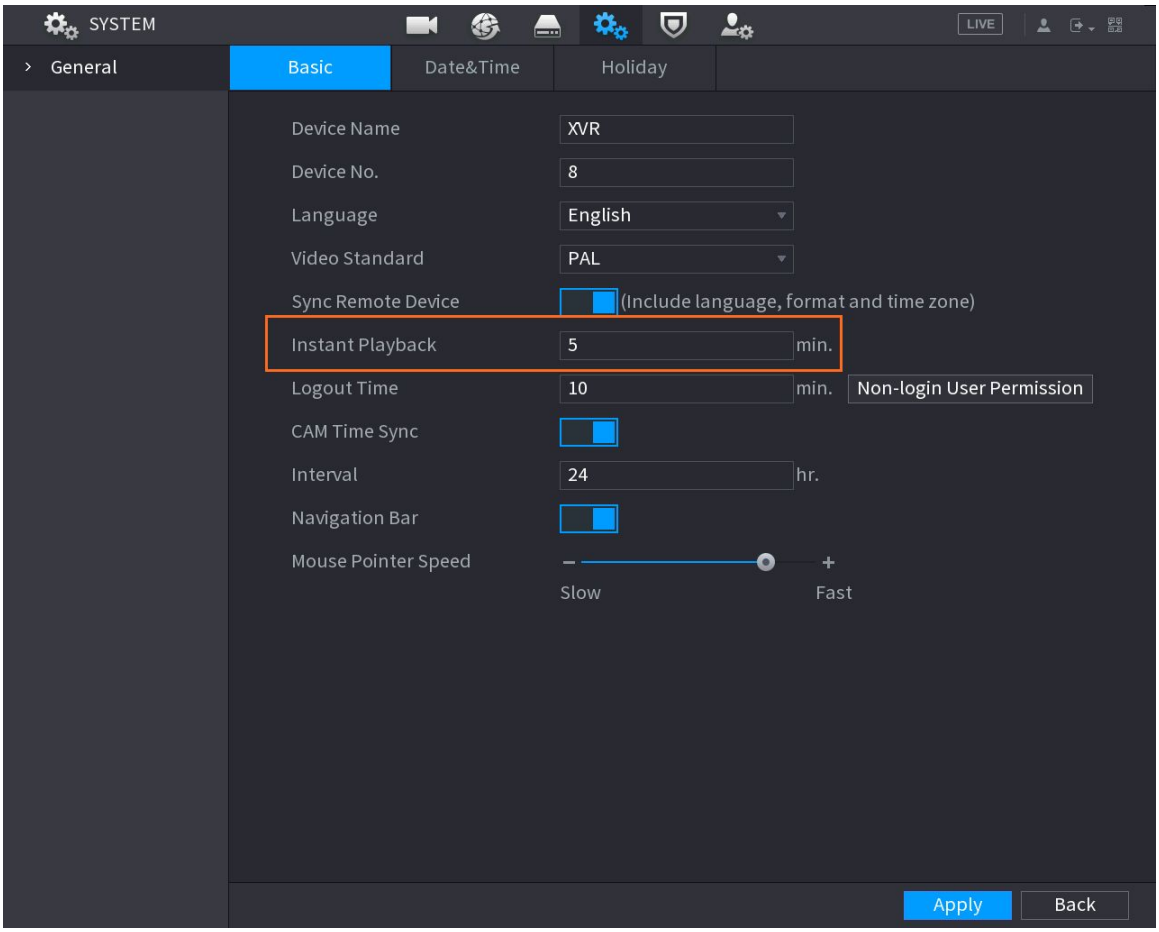
You can play back the previous 5 minutes to 60 minutes of the recorded video.

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

- Move the slider to choose the time you want to start playing.
- Play, pause and close playback.
- The information such as channel name and recording status icon are shielded during instant playback and will not display until exited.
- During playback, screen split layout switch is not allowed.

To change the playback time, select **Main Menu** > **SYSTEM** > **General** > **Basic**, in the **Instant Play** box, enter the time you want to play back.

Figure 1-26 Set instant playback time



Smart Search Playback

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

This function is for some series product only.

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

2 Logging in to Web

The web provides most of the functions on local GUI. You can log in to web to manage the DVR as needed.

Slight difference might be found on the interfaces of different models. Following figures are for reference only. The actual product shall govern.

1. Open the browser and enter the IP address of the DVR, and then press Enter key.

   The factory default IP of the Device is 192.168.1.108.
2. Enter the username and password.
3. Click **Login**.

Appendix 1 Security Recommendation

Account Management

1. **Use complex passwords**

   Please refer to the following suggestions to set passwords:

   - The length should not be less than 8 characters;
   - Include at least two types of characters: upper and lower case letters, numbers and symbols;
   - Do not contain the account name or the account name in reverse order;
   - Do not use continuous characters, such as 123, abc, etc.;
   - Do not use repeating characters, such as 111, aaa, etc.
2. **Change passwords periodically**

   It is recommended to periodically change the device password to reduce the risk of being guessed or cracked.
3. **Allocate accounts and permissions appropriately**

   Appropriately add users based on service and management requirements and assign minimum permission sets to users.
4. **Enable account lockout function**

   The account lockout function is enabled by default. You are advised to keep it enabled to protect account security. After multiple failed password attempts, the corresponding account and source IP address will be locked.
5. **Set and update password reset information in a timely manner**

   The device supports password reset function. To reduce the risk of this function being used by threat actors, if there is any change in the information, please modify it in time. When setting security questions, it is recommended not to use easily guessed answers.

Service Configuration

1. **Enable HTTPS**

   It is recommended that you enable HTTPS to access web services through secure channels.
2. **Encrypted transmission of audio and video**

   If your audio and video data contents are very important or sensitive, it is recommended to use encrypted transmission function in order to reduce the risk of your audio and video data being eavesdropped during transmission.
3. **Turn off non-essential services and use safe mode**

   If not needed, it is recommended to turn off some services such as SSH, SNMP, SMTP, UPnP, AP hotspot etc., to reduce the attack surfaces.

   If necessary, it is highly recommended to choose safe modes, including but not limited to the following services:

   - SNMP: Choose SNMP v3, and set up strong encryption and authentication passwords.
   - SMTP: Choose TLS to access mailbox server.
   - FTP: Choose SFTP, and set up complex passwords.
   - AP hotspot: Choose WPA2-PSK encryption mode, and set up complex passwords.
4. **Change HTTP and other default service ports**

   It is recommended that you change the default port of HTTP and other services to any port between 1024 and 65535 to reduce the risk of being guessed by threat actors.

Network Configuration

1. **Enable Allowlist**

   It is recommended that you turn on the allowlist function, and only allow IP in the allow list to access the device. Therefore, please be sure to add your computer IP address and supporting device IP address to the allowlist.
2. **MAC address binding**

   It is recommended that you bind the IP address of the gateway to the MAC address on the device to reduce the risk of ARP spoofing.
3. **Build a secure network environment**

   In order to better ensure the security of devices and reduce potential cyber risks, the following are recommended:

   - Disable the port mapping function of the router to avoid direct access to the intranet devices from external network;
   - According to the actual network needs, partition the network: if there is no communication demand between the two subnets, it is recommended to use VLAN, gateway and other methods to partition the network to achieve network isolation;
   - Stablish 802.1x access authentication system to reduce the risk of illegal terminal access to the private network.

Security Auditing

1. **Check online users**

   It is recommended to check online users regularly to identify illegal users.
2. **Check device log**

   By viewing logs, you can learn about the IP addresses that attempt to log in to the device and key operations of the logged users.
3. **Configure network log**

   Due to the limited storage capacity of devices, the stored log is limited. If you need to save the log for a long time, it is recommended to enable the network log function to ensure that the critical logs are synchronized to the network log server for tracing.

Software Security

1. **Update firmware in time**

   According to the industry standard operating specifications, the firmware of devices needs to be updated to the latest version in time in order to ensure that the device has the latest functions and security. If the device is connected to the public network, it is recommended to enable the online upgrade automatic detection function, so as to obtain the firmware update information released by the manufacturer in a timely manner.
2. **Update client software in time**

   It is recommended to download and use the latest client software.

Physical Protection

It is recommended that you carry out physical protection for devices (especially storage devices), such as placing the device in a dedicated machine room and cabinet, and having access control

and key management in place to prevent unauthorized personnel from damaging hardware and other peripheral equipment (e.g. USB flash disk, serial port).