



Network Video Recorder

Quick Start Guide








Foreword

General

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

Safety Instructions

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

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
V1.1.0	Updated local operations and some configuration settings.	September 2024
V1.0.0	First release.	July 2020

Privacy Protection Notice

As the NVR user or data controller, you might collect personal data of others such as face, audio, 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. Slight differences might be found between the manual and the product.

- We are not liable for losses incurred due to operating the product in ways that are not in compliance with the manual.
- The manual will be updated according to the latest laws and regulations of related jurisdictions. For detailed information, see the paper user's manual, use our CD-ROM, scan the QR code or visit our official website. The manual is for reference only. Slight differences might be found between the electronic version and the paper version.
- All designs and software are subject to change without prior written notice. Product updates might result in some differences appearing between the actual product and the manual. Please contact customer service for the latest program and supplementary documentation.
- There might be errors in the print or deviations in the description of the functions, operations and technical data. If there is any doubt or dispute, we reserve the right of 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 company names in the manual are properties of their respective owners.
- Please visit our website, contact the supplier or customer service if any problems occur while using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Important Safeguards and Warnings

This section introduces content covering the proper handling of the Device, hazard prevention, and prevention of property damage. Read carefully before using the Device, and comply with the guidelines when using it.

Transportation Requirements



Transport the Device under allowed humidity and temperature conditions.

Storage Requirements



Store the Device under allowed humidity and temperature conditions.

Installation Requirements



Stability Hazard

Possible result: The rack might fall down and cause serious personal injury.


Preventive measures (including but not limited to):

- Before extending the rack to the installation position, read the installation instructions.
- When the Device is installed on the slide rail, do not place any load on it.
- Do not retract the slide rail while the Device is installed on it.




-  Rotating Fan Blades Hazard

Avoid touching the fan blades, especially when they are moving.

-  Before installation, disconnect all the power cords.
- Do not connect the power adapter to the Device while the adapter is powered on.
- Strictly comply with the local electric safety code and standards. Make sure the ambient voltage is stable and meets the power supply requirements of the Device.
- Use the power adapter and cables provided with the Device. We assume no responsibility for injuries or damage caused by using the incorrect power adapter and cables.



-  Reliably ground the grounding terminal of the Device to improve safety. The grounding terminal differs depending on the device, and some devices do not have grounding terminals. Process the situation according to the device model.

- The Device must be installed in a location that only professionals can access. Non-professionals are not allowed to enter the installation area.
- The Device must be reliably grounded by professionals. They must install the grounding conductor in the building floor and verify the grounding connection of the output receptacle.
- Do not place the Device in a place exposed to sunlight or near heat sources.
- Keep the Device away from dampness, dust, and soot.
- Install the Device on a stable surface to prevent it from falling.
- Put the Device in a well-ventilated place, and do not block its ventilation.
- The Device is a class I electrical appliance. Make sure that the power supply of the Device is connected to a power socket with protective earthing.
- Use power cords that conform to your local requirements, and are rated specifications.
- Before connecting the power supply, make sure the input voltage matches the server power requirement.
- When installing the Device, make sure that the power plug can be easily reached to cut off the power.
- It is prohibited for non-professionals and unauthorized personnel to open the device casing.
- Affix the controller securely to the building before use.

Operation Requirements



- The Device or remote control contains button batteries. Do not swallow the batteries due to the risk of chemical burns.

Possible result: The swallowed button battery can cause serious internal burns and death within 2 hours.

Preventive measures (including but not limited to):

- ◇ Keep new and used batteries out of reach of children.
 - ◇ If the battery compartment is not securely closed, stop using the product immediately and keep out of reach of children.
 - ◇ Seek immediate medical attention if a battery is believed to be swallowed or inserted inside any part of the body.
- Battery Pack Precautions

Preventive measures (including but not limited to):

- ◇ Do not transport, store or use the batteries in high altitudes with low pressure and environments with extremely high and low temperatures.
- ◇ Do not dispose the batteries in fire or a hot oven, or mechanically crush or cut the batteries to avoid an explosion.
- ◇ Do not leave the batteries in environments with extremely high temperatures to avoid explosions and leakage of flammable liquid or gas.
- ◇ Do not subject the batteries to extremely low air pressure to avoid explosions and the leakage of flammable liquid or gas.



Place the Device in a location that children cannot easily access.



- This is a class 1 laser device. You can only insert modules that meet the requirements of class 1 lasers.

- Do not drop or splash liquid onto the Device, and make sure that there is no object filled with liquid on the Device to prevent liquid from flowing into it.
- Put the Device in a well-ventilated place, and do not block its ventilation.
- Operate the Device within the rated range of power input and output.
- Do not disassemble the Device without professional instruction.
- Transport, use and store the Device under allowed humidity and temperature conditions.

Maintenance Requirements



Replacing unwanted batteries with the wrong type of new batteries might result in explosion.

Preventive measures (including but not limited to):

- Replace unwanted batteries with new batteries of the same type and model to avoid the risk of fire and explosion.
- Dispose of the old batteries as instructed.



The appliance coupler is a disconnection device. Keep it at a convenient angle when using it. Before repairing or performing maintenance on the device, first disconnect the appliance coupler.

Table of Contents

Foreword.....	I
Important Safeguards and Warnings.....	III
1 Local Operations.....	1
1.1 Starting the NVR.....	1
1.2 Initializing the NVR.....	1
1.3 Configuring Network.....	3
1.4 Adding IP Camera.....	4
1.4.1 Initializing IP Camera.....	4
1.4.2 Adding IP Camera by Search Result.....	10
1.4.3 Manually Adding IP Camera.....	11
1.5 Configuring Recorded Video Storage Schedule.....	13
1.6 Configuring P2P Settings.....	13
1.6.1 Enabling P2P Function.....	14
1.6.2 Adding the NVR to Smart Phone Client.....	14
1.7 Live View.....	16
1.8 Recording Playback.....	18
2 Logging in to Web.....	19
Appendix 1 Security Recommendation.....	20

1 Local Operations

1.1 Starting the NVR

Before starting the NVR, make sure that:

- The rated input voltage matches the NVR's power requirements.
- The power wire connection is ready.
- For device security, connect the NVR 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 NVR

This topic shows how to initialize the NVR 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 NVR.

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 NVR after initialization.

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**.

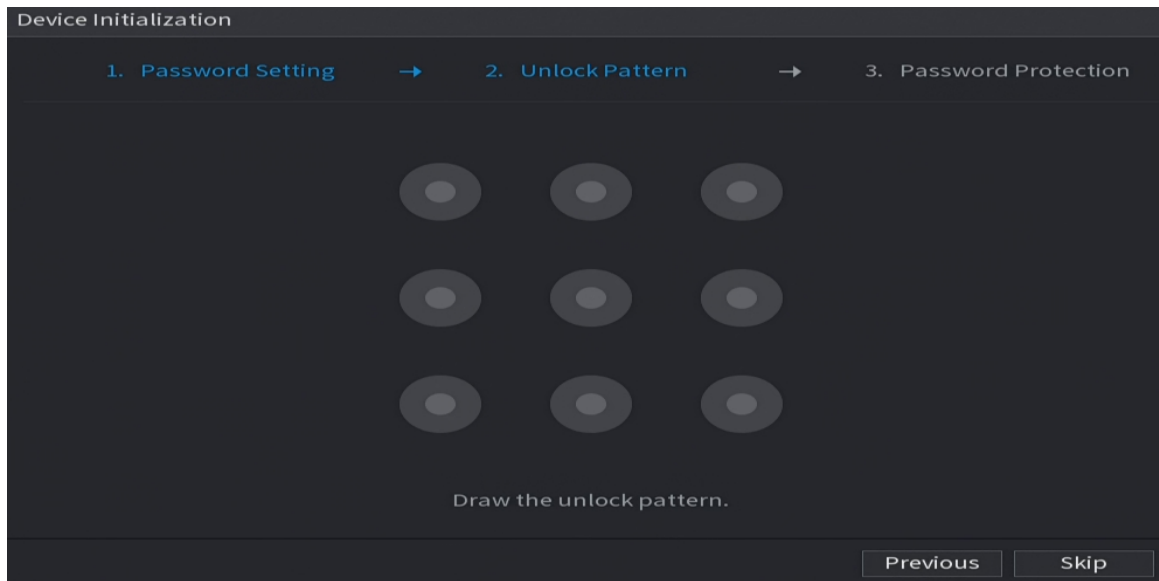
Step 5 Configure the password information for device administrator, and then click **Next**.

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	<p>Enter a prompt question that will help you recall the password for your device.</p>  <p>On the login interface, click  and the prompt will be displayed to help you reset the password.</p>

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

Figure 1-1 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.

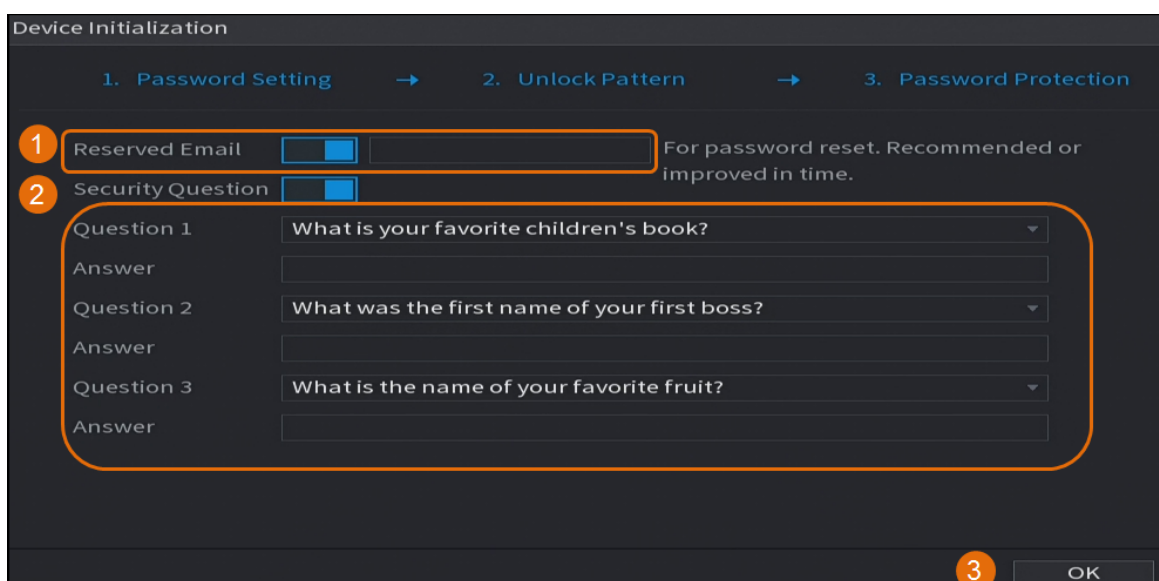
Step 7 (Optional) Apply reserved email and security questions to the NVR.



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 1-2 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 NVR.

Procedure

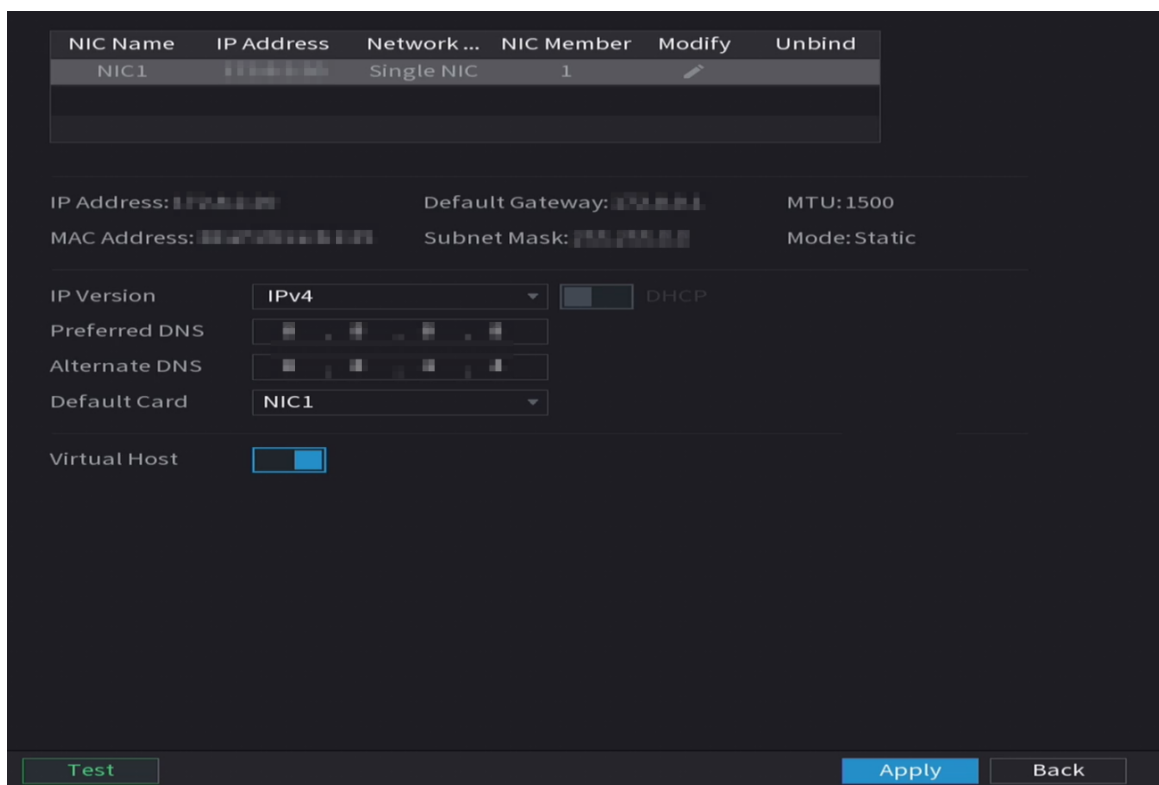
Step 1 Select **Main Menu > NETWORK > TCP/IP**.

Step 2 Configure parameters.



You can also configure network parameters in the Startup Wizard.

Figure 1-3 TCP/IP



NIC Name	IP Address	Network ...	NIC Member	Modify	Unbind
NIC1	192.168.1.100	Single NIC	1		

IP Address: 192.168.1.100 Default Gateway: 192.168.1.1 MTU: 1500

MAC Address: 08:00:27:00:00:00 Subnet Mask: 255.255.255.0 Mode: Static

IP Version: IPv4 ☒ DHCP

Preferred DNS: 192.168.1.1

Alternate DNS: 192.168.1.1


Default Card: NIC1

Virtual Host: ☒

Test Apply Back

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 NVR.

Parameter	Description
DHCP	<p>Enable the DHCP function. The IP address, subnet mask and default gateway are not available for configuration once DHCP is enabled.</p> <ul style="list-style-type: none"> • 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	<p>Enter the IP address and configure the corresponding subnet mask and default gateway.</p> <p> IP address and default gateway must be in the same network segment.</p>
Subnet Mask	
Default Gateway	
Preferred DNS	Enter the IP address of DNS.
Alternate DNS	Enter the IP address of alternate DNS.
MTU	<p>Enter a value for network card. The value ranges from 1280 byte to 1500 byte. The default is 1500.</p> <p>The suggested MTU values are as below.</p> <ul style="list-style-type: none"> • 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 Adding IP Camera

You can add an IP camera by search result or by manually entering IP information.



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

1.4.1 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 NVR, otherwise the connection will fail. The initialization will change IP camera's login password and IP address.



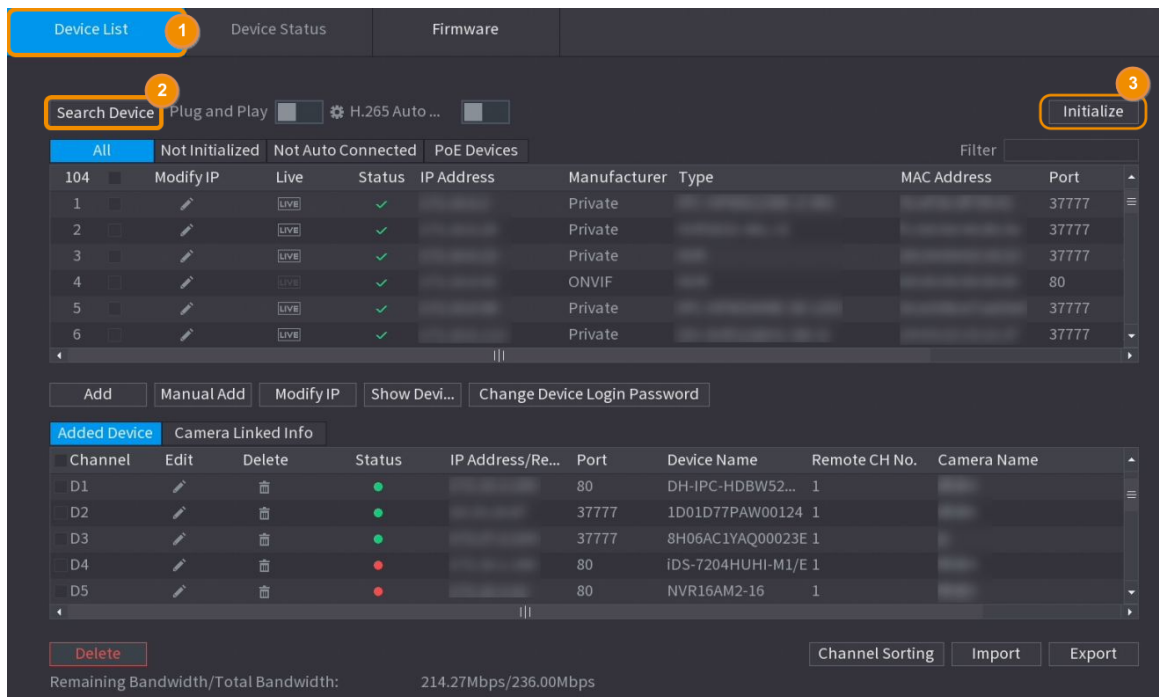
When you connect a camera that has not been initialized to the NVR through PoE port, the NVR will automatically initialize the camera. And the camera adopts the password and email information of the NVR by default.

Procedure

Step 1 Select **Main Menu > REMOTE DEVICE > Add Device > Video Device > Device List**.

Step 2 Click **Not Initialized**, and then click **Search Device**.

Figure 1-4 Search uninitialized device



The screenshot shows the 'Device List' tab in the Dahua NVR web interface. The interface includes a search bar, a table of devices, and an 'Initialize' button. The table shows columns for Channel, Edit, Delete, Status, IP Address, Port, Device Name, Remote CH No., and Camera Name. The 'Status' column shows 'Not Initialized' for the first six devices. The 'Initialize' button is highlighted with a red circle and the number 3.

Channel	Edit	Delete	Status	IP Address	Port	Device Name	Remote CH No.	Camera Name
D1			Not Initialized		80	DH-IPC-HDBW52...	1	
D2			Not Initialized		37777	1D01D77PAW00124	1	
D3			Not Initialized		37777	8H06AC1YAQ00023E	1	
D4			Not Initialized		80	IDS-7204HUHI-M1/E	1	
D5			Not Initialized		80	NVR16AM2-16	1	

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

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

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



This check box is selected by default.

Figure 1-5 Apply device settings

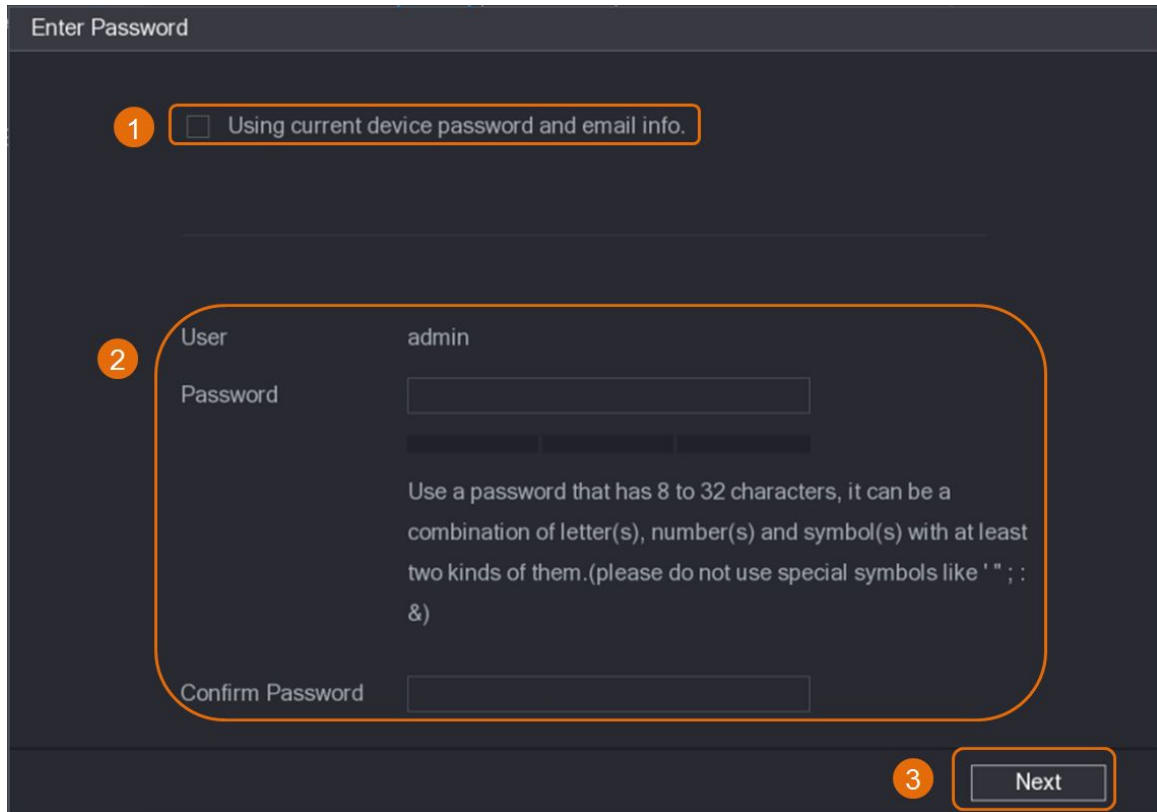
Enter Password

1 ☒ Using current device password and email info.

2 Next

2. Click **Next**.
- Manually set password and email information.
 1. Cancel **Using current device password and email info..**

Figure 1-6 Set password



Enter Password

1 ☐ Using current device password and email info.

2

User admin

Password

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

Confirm Password

3 Next

2. Set password.

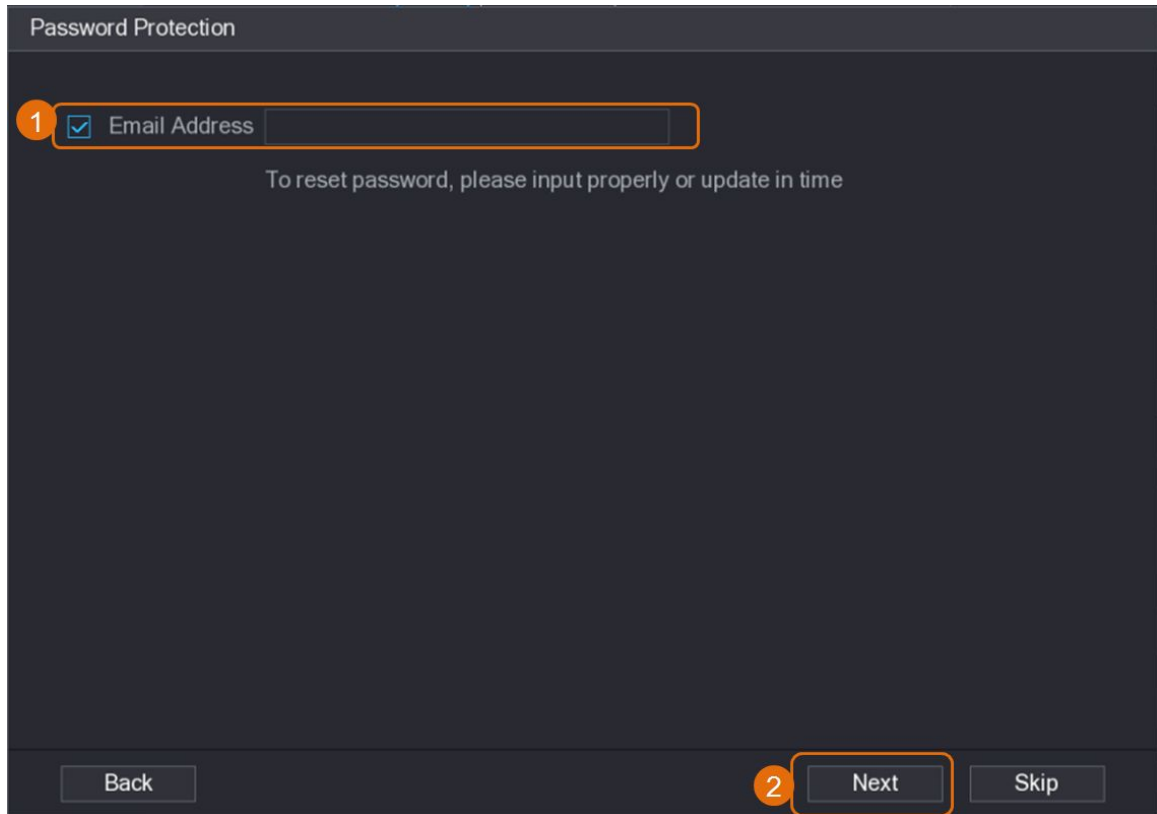
Table 1-3 Password

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 "&").
Confirm Password	
	Enter a strong password according to the password strength bar indication.

3. Click **Next**.

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

Figure 1-7 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 NVR will incrementally add the value on to the fourth section of the IP address when allocate IP addresses for those cameras.

Figure 1-8 Configure IP address

Modify IP

Checked Device No.: 1

☐ DHCP
 ☒ STATIC

IP Address

192.168.1.254

Subnet Mask

255.255.255.0

Default Gateway

192.168.1.1

Username

admin

Password

Incremental Value

1

1	Serial No.	IP Address
1		192.168.1.254

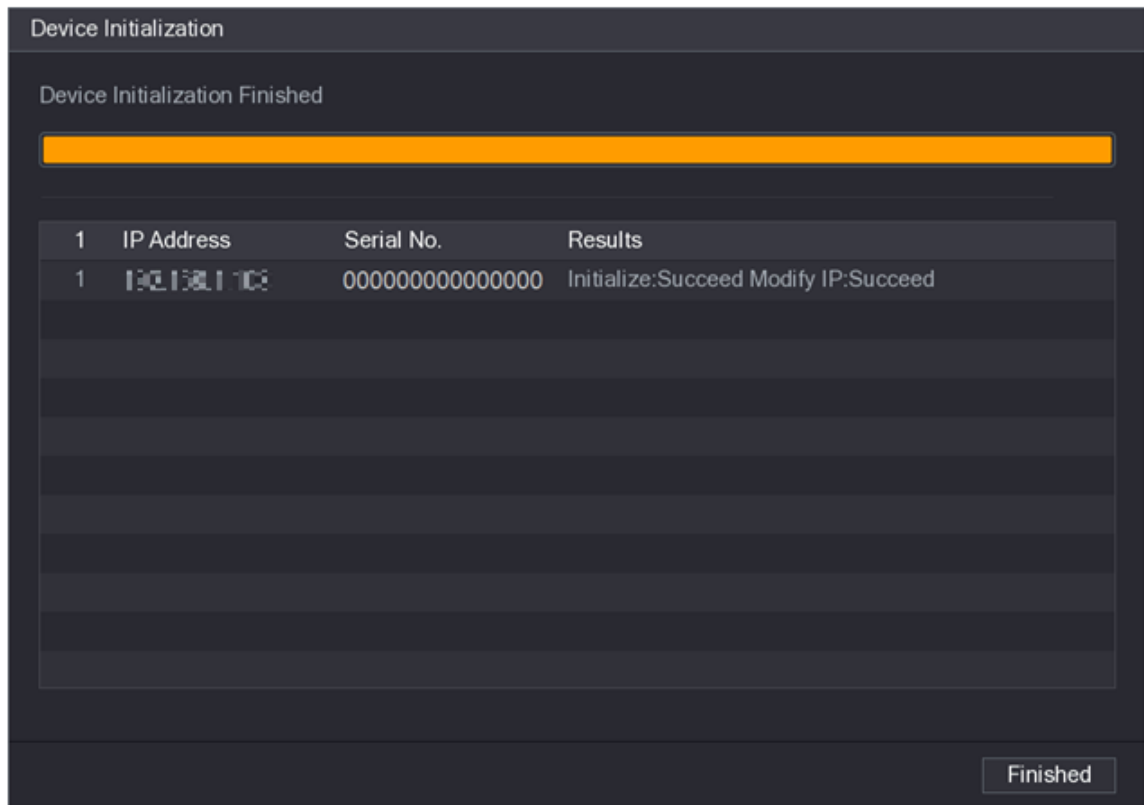
OK

Cancel

Step 6 Click **OK**.

Wait 1–2 minutes for the initialization to complete.

Figure 1-9 Device initialization



Step 7 Click **Finished**.

1.4.2 Adding IP Camera by Search Result

Prerequisites

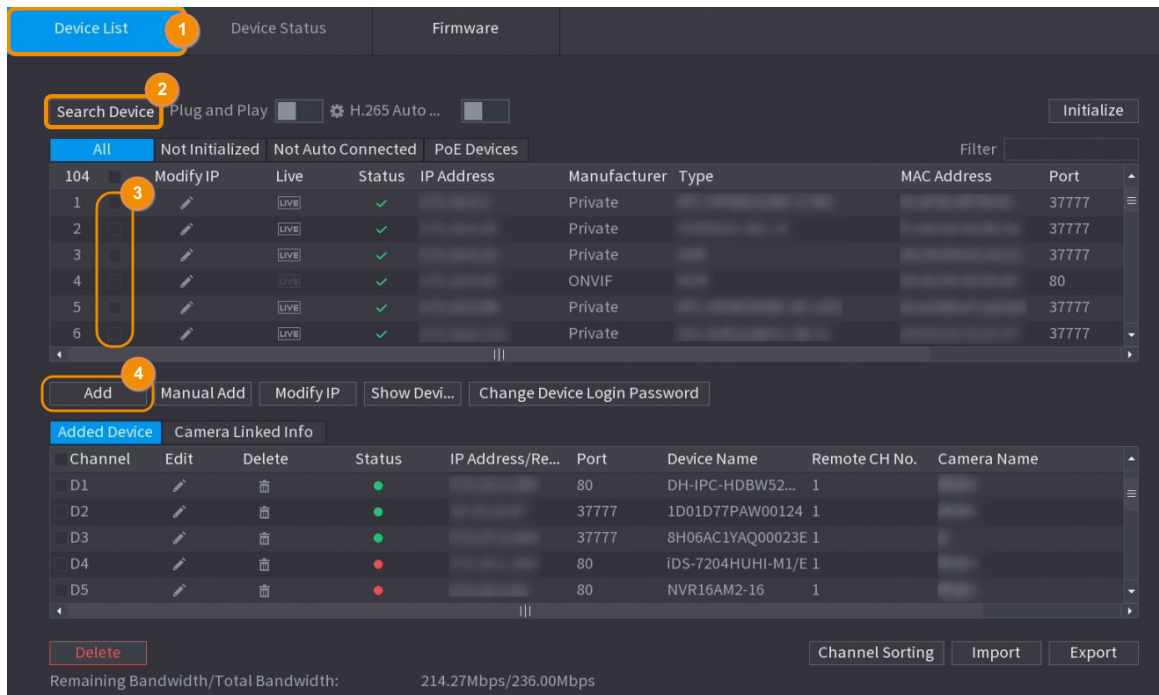
Make sure that the cameras you want to add have already been initialized and connected to the right network.

Procedure

Step 1 Select **Main Menu > REMOTE DEVICE > Add Device > Video Device > Device List**.

Step 2 Click **Search Device**.

Figure 1-10 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 boxes of the target camera, and then click **Add** to add more than one camera to **Added Device** list.

Results

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

1.4.3 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** > **REMOTE DEVICE** > **Add Device** > **Video Device** > **Device List**.
- Step 2** Click **Manual Add**.
- Step 3** In the **Manual Add** dialog box, configure parameters.

Figure 1-11 Configure manual add parameters

Manual Add

Channel

D3

Manufacturer

Private

IP Address

192.168.1.1

TCP Port

37777

Username

admin

Password

Total Channels

1

Remote CH No.

D1


Decode Strategy


General

Connect

Setting

Table 1-4 Remote channel parameters

Parameter	Description
Channel	Select the channel that you want use on the Device to connect the remote device.
Manufacturer	<p>Select the manufacturer of the remote device.</p> <p> Please connect the Imou camera to the Device through the ONVIF protocol, otherwise the Imou camera added through private protocols cannot be connected.</p>
Registration ID	Enter the registration ID of the remote device.
IP Address	Enter the IP address of the remote device.
RTSP Port	Enter the RTSP port number. The default value is 554.
HTTP Port	Enter the HTTP port number. The default value is 80.
TCP Port	The default value is 37777. You can enter the value as needed.
Username	Enter the username of the remote device.
Password	Enter the password of the user for the remote device.
Total Channels	<p>Click Connect to get the total number of channels of the remote device.</p> <p>For the remote device with multiple channels, you can choose the connected number of channels as needed.</p>

Parameter	Description
Remote CH No.	Enter the remote channel number of the remote device.
Decode Strategy	Select Default , Realtime , or Fluent .
Protocol Type	<ul style="list-style-type: none"> • If the remote device is added through private protocol, the default type is TCP. • If the remote device is added through ONVIF protocol, the system supports Auto , TCP, UDP, or MULTICAST. • If the remote device is added through other manufacturers, the system supports TCP and UDP.
Encryption	<p>If the remote device is added through ONVIF protocol, select the Encrypt checkbox and then the system will provide encryption protection to the data being transmitted.</p>  <p>To use this function, make sure that the HTTPS function is enabled for the remote IP camera.</p>


Step 4 Click **OK**.

1.5 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.
 - Drawing: Press and hold the left button of the mouse and drag the mouse to draw the period.
 - Editing: Click  to configure the period, and then click **OK**.
4. Click **Apply**.



The configured record schedule can come into effect only when the auto record function is enabled. For details to enable auto record, see User's Manual.

1.6 Configuring P2P Settings

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



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

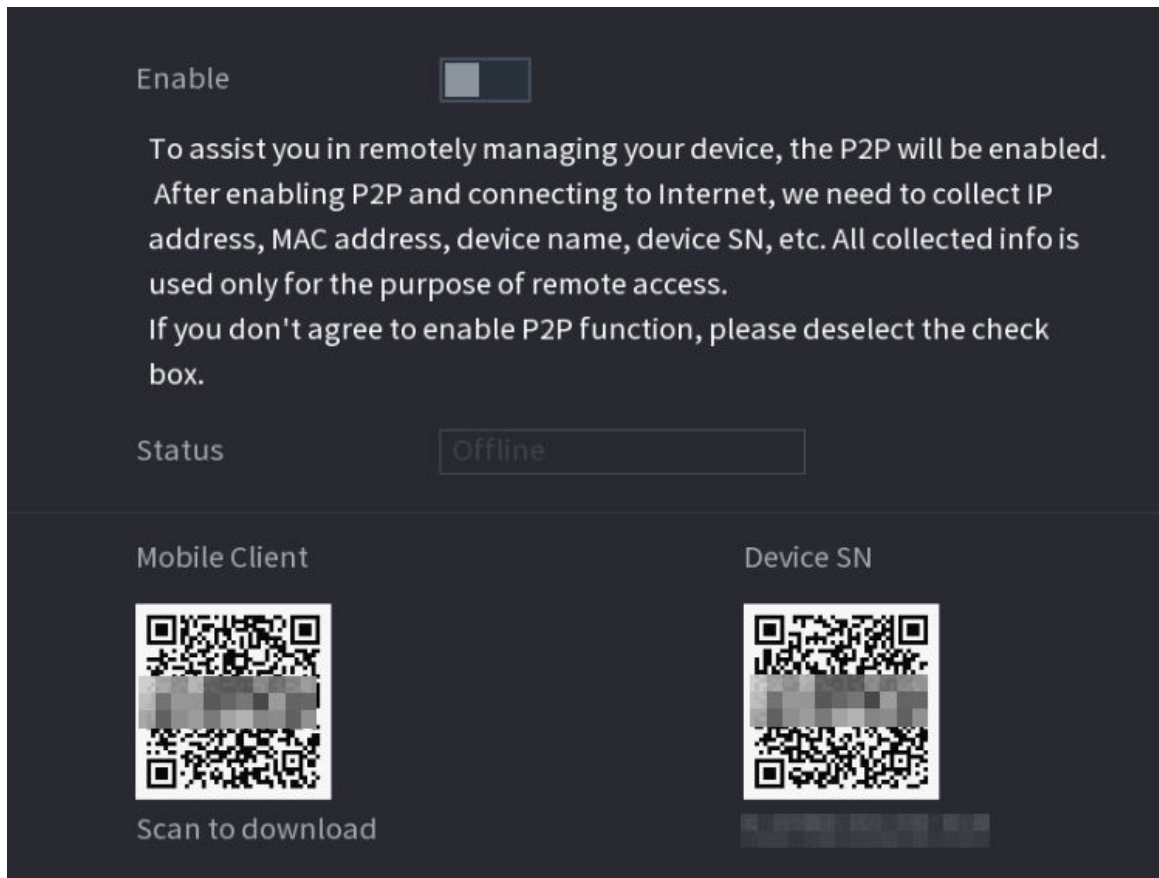
1.6.1 Enabling P2P Function

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 1-13 P2P




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

Step 3 Click **Apply**

1.6.2 Adding the NVR to Smart Phone Client

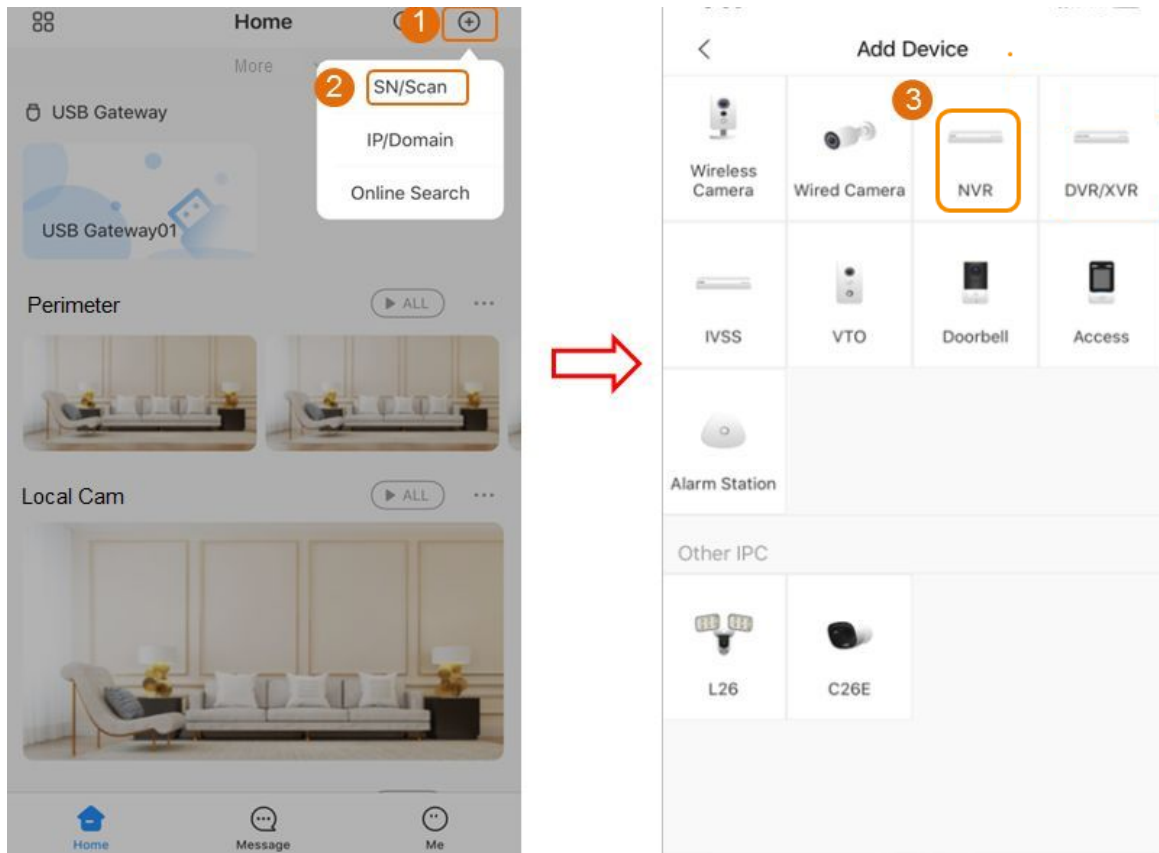
This topic takes adding the NVR to smart phone client as an example for smart phone management.

Procedure

Step 1 Open the application and tap .

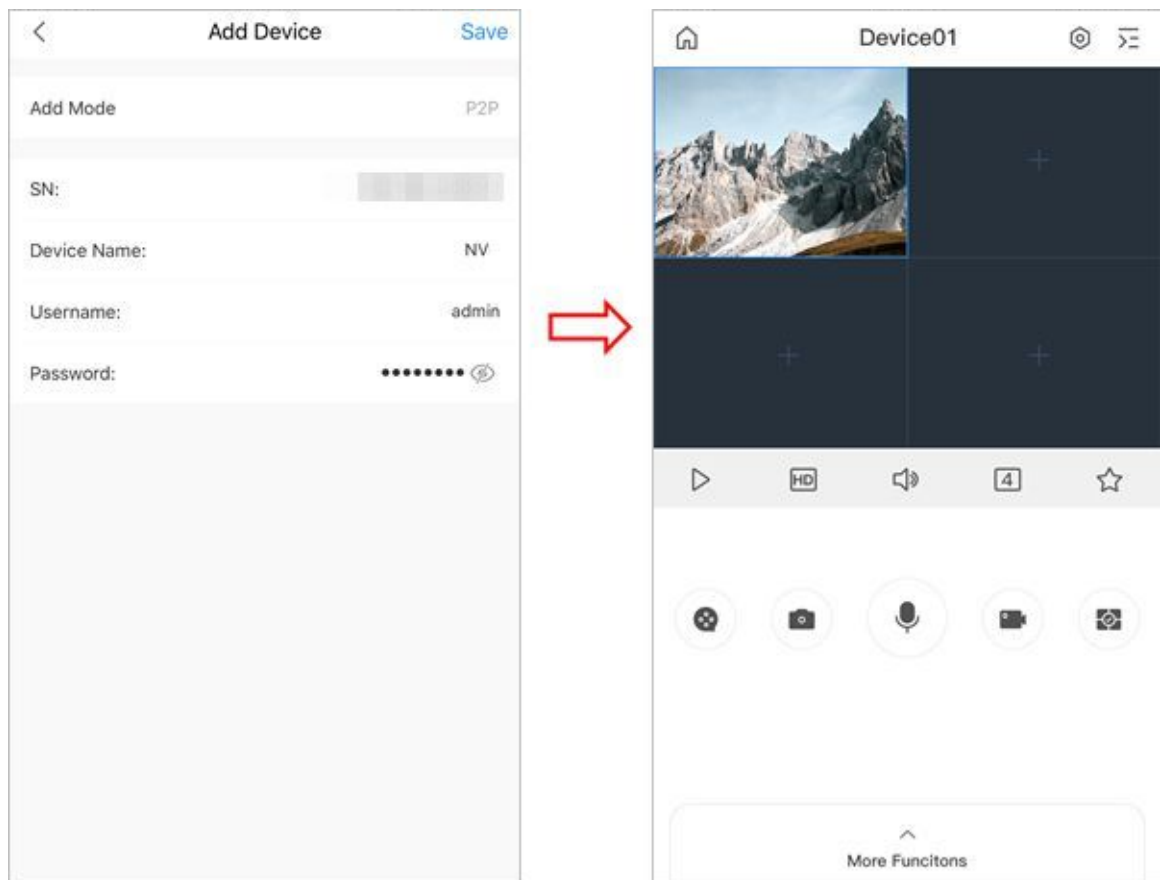
Step 2 Select **SN/Scan**.

Figure 1-14 Add device



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

Figure 1-15 Start live view



1.7 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 1-16 Live view









Live View Screen

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

- On the live view page, you can view the live video of each channel. The corresponding channel displays date, time, and channel name after you overlay the corresponding information.
- 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.

Table 1-6 Icon description

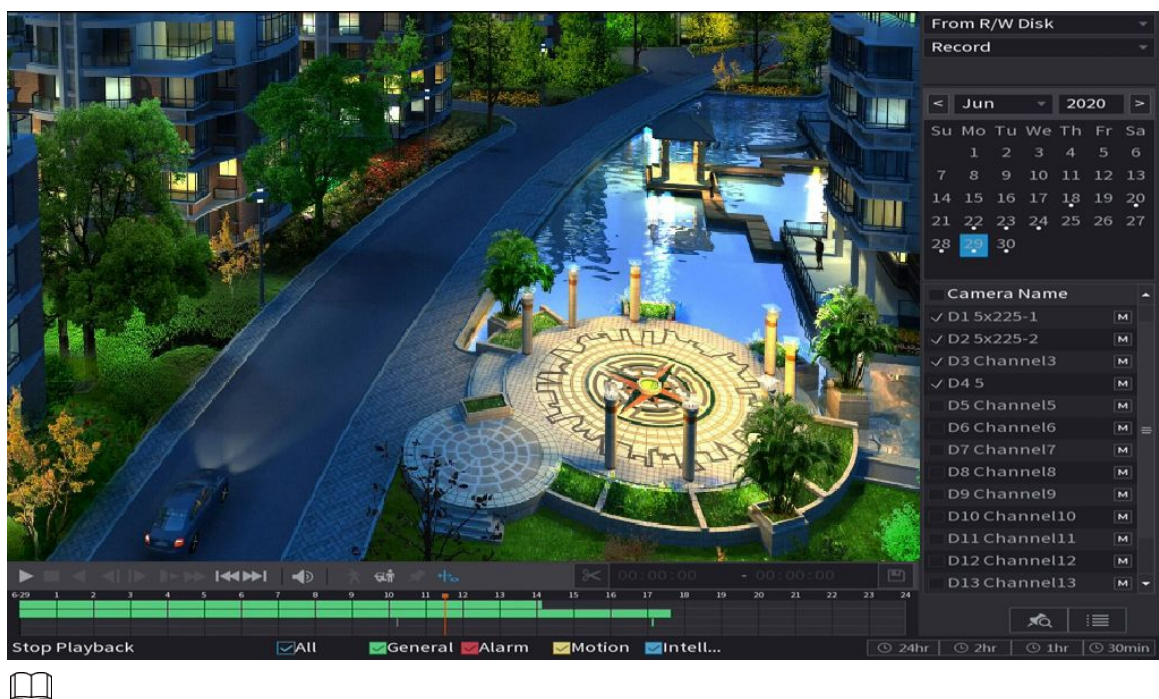
Icon	Description
	The current channel is recording.
	Motion detection alarm occurs.
	Video loss alarm occurs.
	The current channel is in monitor lock status.

Icon	Description
	<p>The Device connects to the network camera remotely.</p> <p></p> <p>This function is available on select models.</p>

1.8 Recording Playback

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


Figure 1-17 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.

2 Logging in to Web

The web provides most of the functions on local GUI. You can log in to web to manage the NVR 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 NVR, and then press Enter key.
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 logout function

The account logout 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 Allow list**

It is recommended that you turn on the allow list 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 allow list.

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;
- Establish 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).

ENABLING A SMARTER SOCIETY AND BETTER LIVING

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.

Address: No. 1399, Binxing Road, Binjiang District, Hangzhou, P. R. China | Website: www.dahuasecurity.com | Postcode: 310053

Email: dhoverseas@dhvisiontech.com | Tel: +86-571-87688888 28933188