AI Network Video Recorder

Quick Start Guide

V1.0.0

Foreword

General

This quick start guide (hereinafter referred to be "the Manual") introduces the functions and operations of the AI NVR device (hereinafter referred to be "the Device").

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 2019

Privacy Protection Notice

As the device user or data controller, you might collect personal data of others such as face, fingerprints, car plate number, Email address, phone number, GPS and so on. 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. Please 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, please 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.
- Please visit our website, contact the supplier or customer service if there is any problem occurred when using the device.
- If there is any uncertainty or controversy, please refer to our final explanation.

Important Safeguards and Warnings

The following description is the correct application method of the Device. 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 Requirement

- Install the POE front-end device indoors.
- The device does not support wall mount.
- Do not place and install the device in an area exposed to direct sunlight or near heat generating device.
- Do not install the device 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 device; don’t put on the device anything filled with liquids, in order to prevent liquids from flowing into the device.
- Install the device at well-ventilated places; don’t block its ventilation opening.
- Use the device only within rated input and output range.
- Do not dismantle the device arbitrarily.
- Transport, use and store the device within allowed humidity and temperature range.

Power Requirement

- Make sure to use the designated battery type. Otherwise there might be explosion risk.
- Make sure to 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.
- Make sure to dispose the exhausted batteries according to the instructions.
- The product shall use electric wires (power wires) recommended by this area, which shall be used within its rated specification.
- Make sure to use standard power adapter matched with this Device. Otherwise, the user shall undertake resulting personnel injuries or Device 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, please 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, please keep an angle that facilitates operation.

Table of Contents

1 Checking the Components

All the installation and operations here should conform to the local electric safety rules.

When you receive the Device, please check against the following checking list. If any of the items are missing or damaged, contact the local retailer or after-sales engineer immediately.

Sequence	Checking items		Requirement
1	Package	Appearance	No obvious damage.
		Packing materials	No broken or distorted positions that could be caused by hit.
		Accessories	No missing.
2	Labels	Labels on the Device	● Device model conforms to the purchase order. ● Not torn up. Do not tear up or throw away the labels; otherwise the warranty services are not ensured. You need to provide the serial number of the product when you call the after-sales service.
3	Device	Appearance	No obvious damage.
		Data cables, power cables, fan cables, mainboard	No connection loose. If there is any loose, please contact the company after-sales service in time.

2 Installing HDD

The following figures are for reference only. The actual product shall govern.

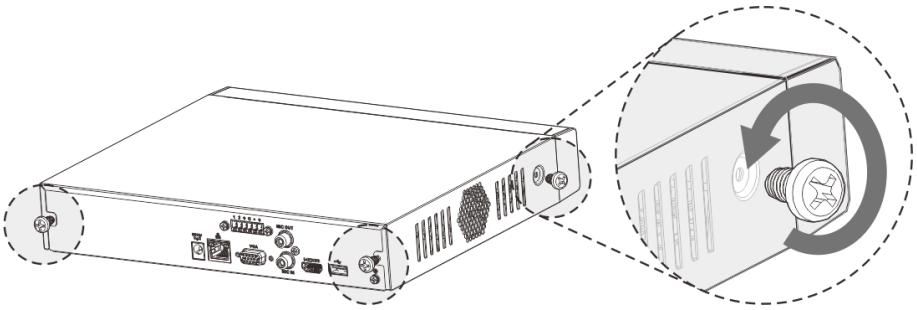
Shut off the power before you replace the HDD.

For the first time installation, check whether the HDD has been installed or not. We recommend to use HDD of enterprise level or surveillance level. It is not recommended to use PC HDD

2.1 1-HDD

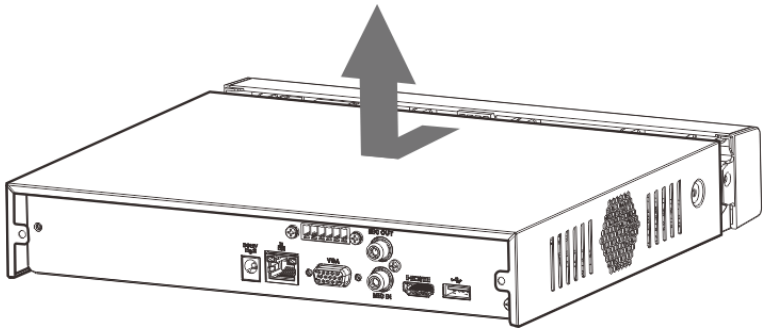
Step 1 Remove the fixing screws of the case cover (including the two screws on the rear panel and two screws on the left and right panels).

Figure 2-1 Installing HDD (1)



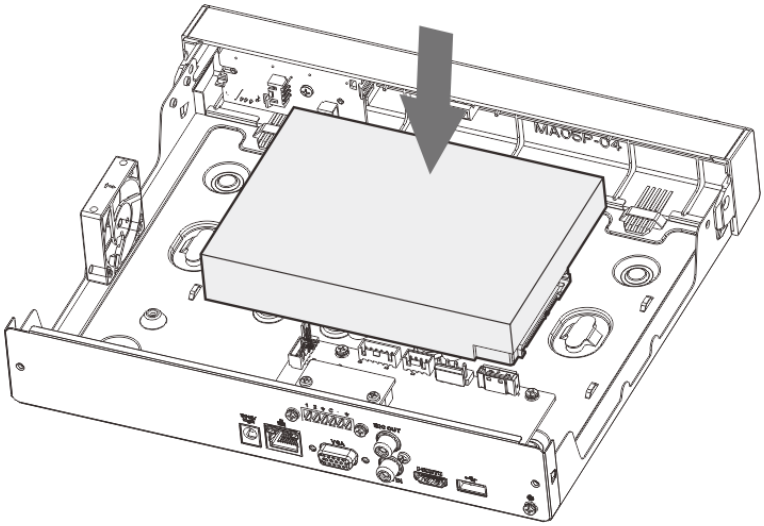
Step 2 Remove the case cover along the direction shown in the following arrow.

Figure 2-2 Installing HDD (2)



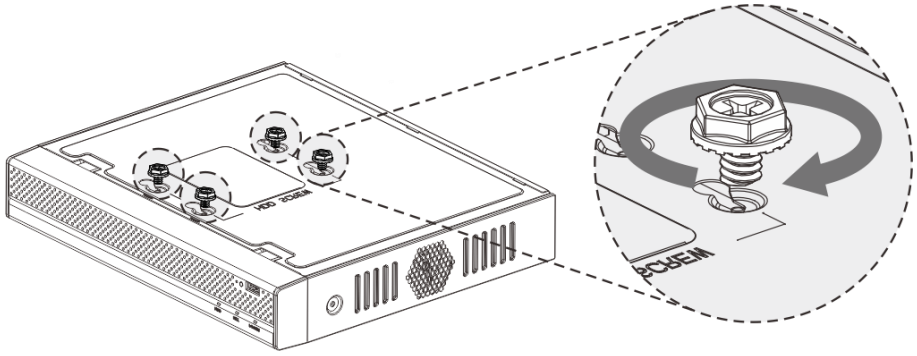
Step 3 Match the four holes on the baseboard to place the HDD.

Figure 2-3 Installing HDD (3)



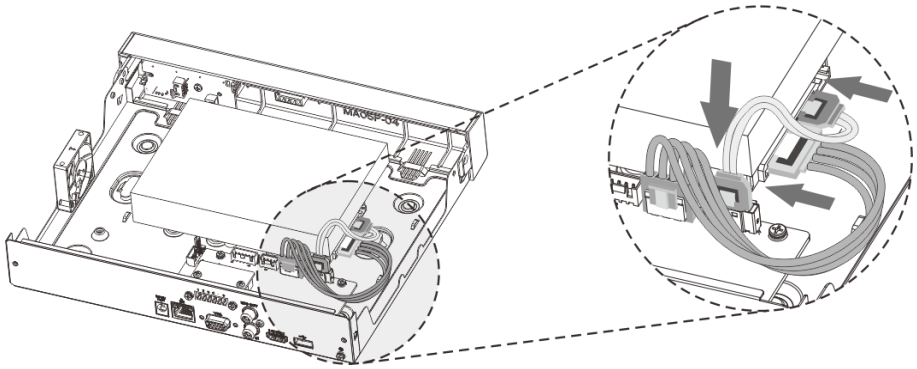
Step 4 Turn the Device upside down, match the screws with the holes on the HDD and then fasten them. The HDD is fixed to the baseboard.

Figure 2-4 Installing HDD (4)



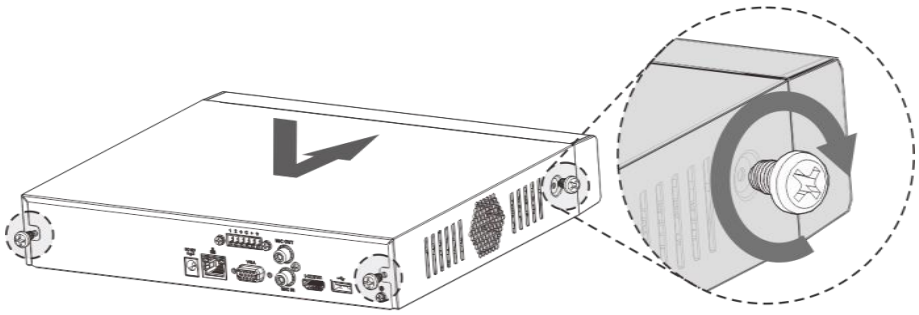
Step 5 Connect the HDD data cable and power cable to the Device.

Figure 2-5 Installing HDD (5)



Step 6 Put back the cover and fasten the screws on the rear panel and side panels to complete the installation.

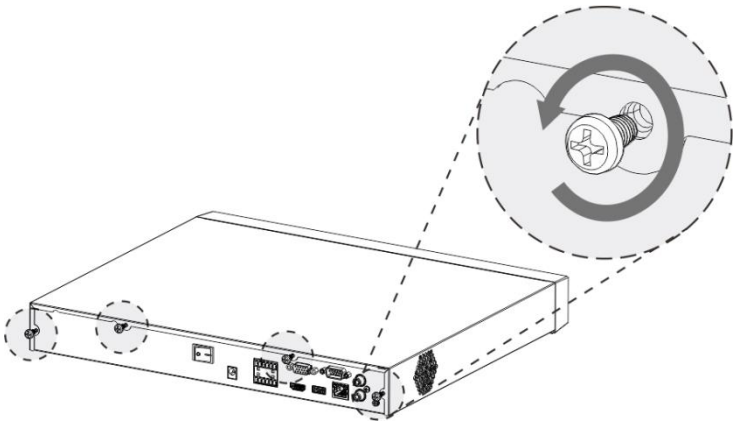
Figure 2-6 Installing HDD (6)



2.2 2-HDD

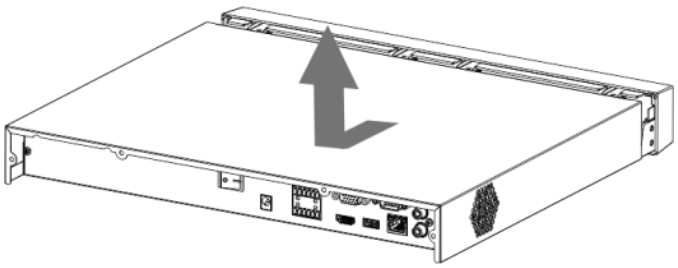
Step 1 Remove the four fixing screws on the rear panel.

Figure 2-7 Installing HDD (1)



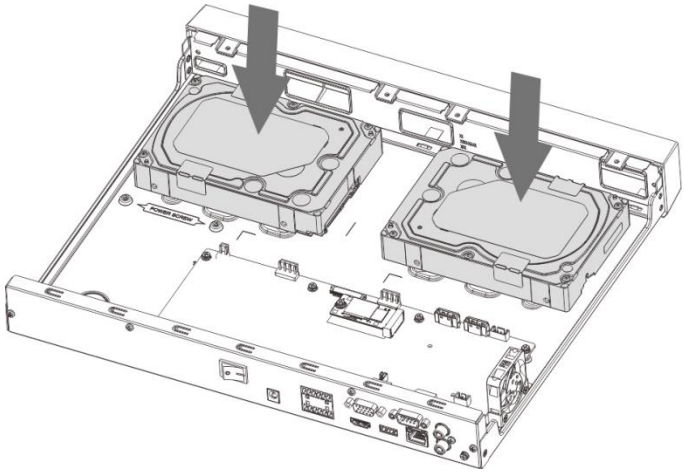
Step 2 Remove the case cover along the direction shown in the following arrow.

Figure 2-8 Installing HDD (2)



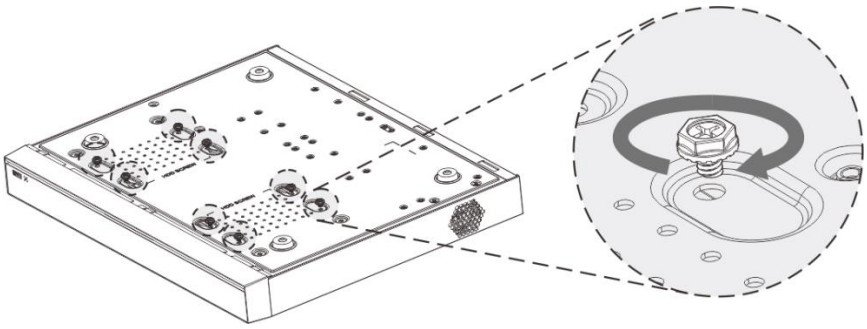
Step 3 Match the four holes on the baseboard to place the HDD.

Figure 2-9 Installing HDD (3)



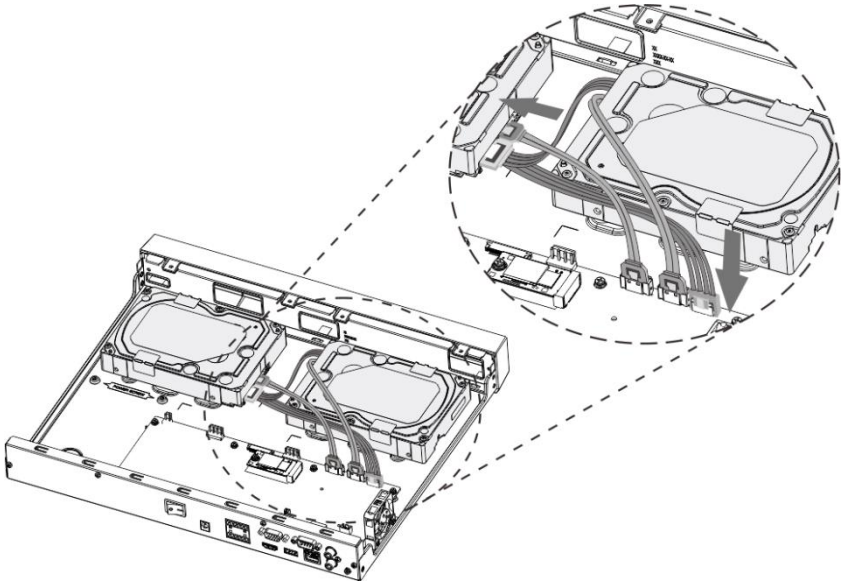
Step 4 Turn the Device upside down, match the screws with the holes on the HDD and then fasten them. The HDD is fixed to the baseboard.

Figure 2-10 Installing HDD (4)



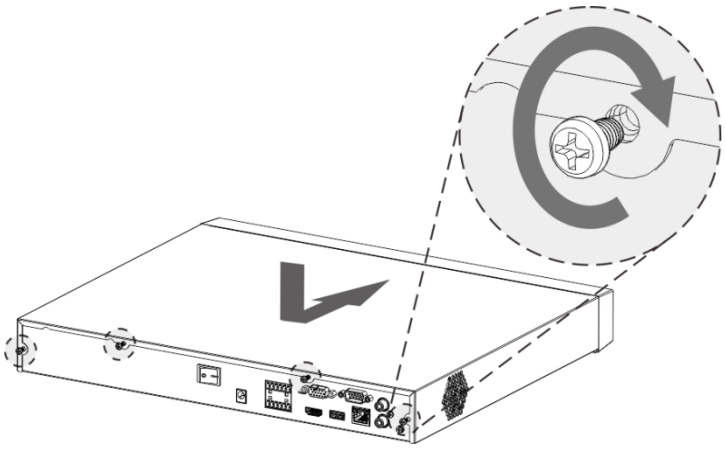
Step 5 Connect the HDD data cable and power cable to the Device.

Figure 2-11 Installing HDD (5)



Step 6 Put back the cover and fasten the four screws on the rear panel to complete the installation.

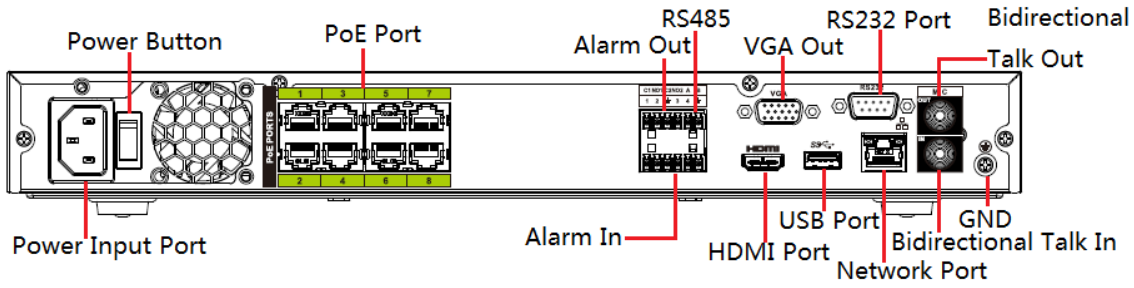
Figure 2-12 Installing HDD (6)



3 Connection

The following figure is for reference only. The actual product shall govern. For details, see *User's Manual*.

Figure 3-1 Connection sample



4 GUI Operations

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

4.1 Booting Up

Before the boot up, please make sure:

- The rated input voltage shall match with the device power requirement. Make sure the power wire connection is ready and then turn on the power button.
- For device security, connect the Device to the power adapter first and then connect it to the power socket.
- Always use the stable current. It is recommended to use UPS.
- Device of some series does not have the power on-off button. You can boot up the Device once the power is connected.

Connect the Device to the monitor, plug into the power socket, and then press the power button to boot up the Device.

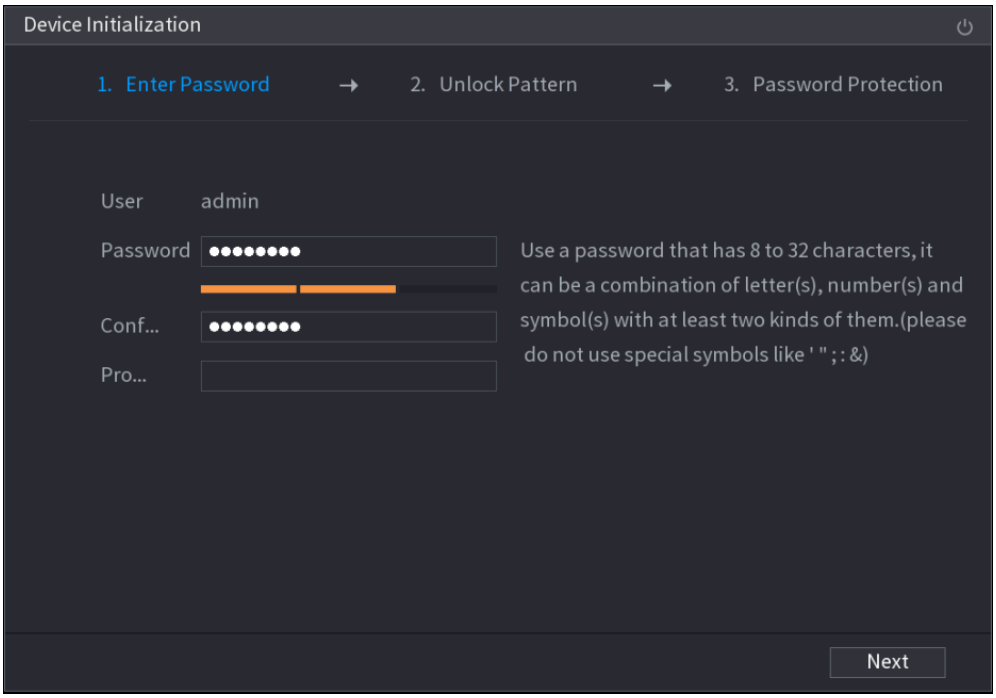
4.2 Initializing the Device

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

Step 1 Turn on the Device.

The **Device Initialization** interface is displayed. See Figure 4-1.

Figure 4-1 Enter password



Step 2 Configure the password, confirm the password, and then enter the prompt question.

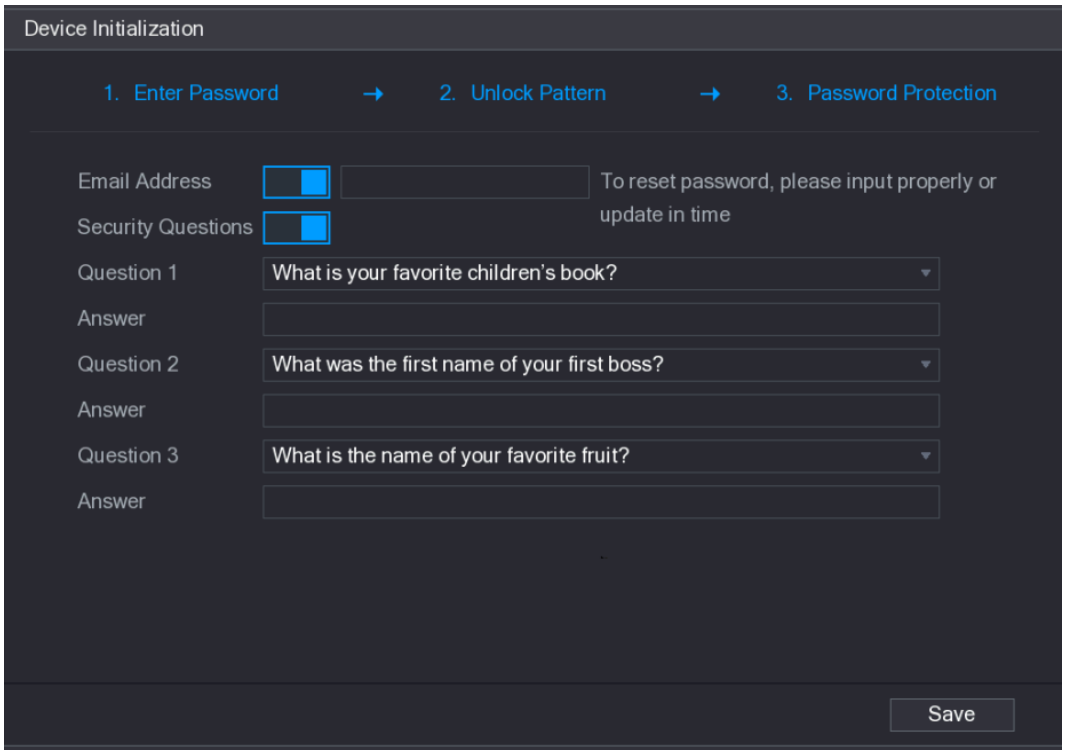
The password can be set from 8 characters through 32 characters and contain at least two types from number, letter and special character (excluding"'", """, ";", ":" and "&"). It is recommended to set a password of high security according to the prompt.

Step 3 Configure the unlock pattern or click **Skip**.

After setting unlock pattern, the password protection setting interface is displayed. See Figure 4-2.

- Once you have configured the unlock pattern, the system will require the unlock pattern as the default login method. If you skip this setting, enter the password for login.

Figure 4-2 Password protection



Step 4 Configure password protection. For details, see Table 4-1.

- After configuration, if you forgot the password for admin user, you can reset the password through the reserved email address or security questions. For details about resetting the password, see *User's Manual*.
- If you do not want to configure the settings, disable the email address and security questions functions on the interface.

Table 4-1 Password protection parameter description

Password Protection Mode	Description
Email Address	Enter the reserved email address. In the **Email Address** box, enter an email address for password reset. In case you forgot password, enter the security code that you will get from this reserved email address to reset the password of admin.
Security Questions	Configure the security questions and answers. In case you forgot password, entering the answers to the questions can make you reset the password.
If you want to configure the email or security questions fucntion later or you want to change the configurations, select **Main Menu > ACCOUNT > USER**.	

Step 5 Click **OK** to complete the settings.

The **Startup Wizard** interface is displayed. For details, see *User's Manual*.

4.3 Modifying IP Address

Step 1 Select **Main Menu** > **NETWORK** > **TCP/IP**.
The TCP/IP interface is displayed. See Figure 4-3.

Step 2 Click .
The **Edit** interface is displayed. See Figure 4-4.

Step 3 Modify the IP address according to the actual network plan (the default IP address is 192.168.1.108).

Figure 4-3 TCP/IP

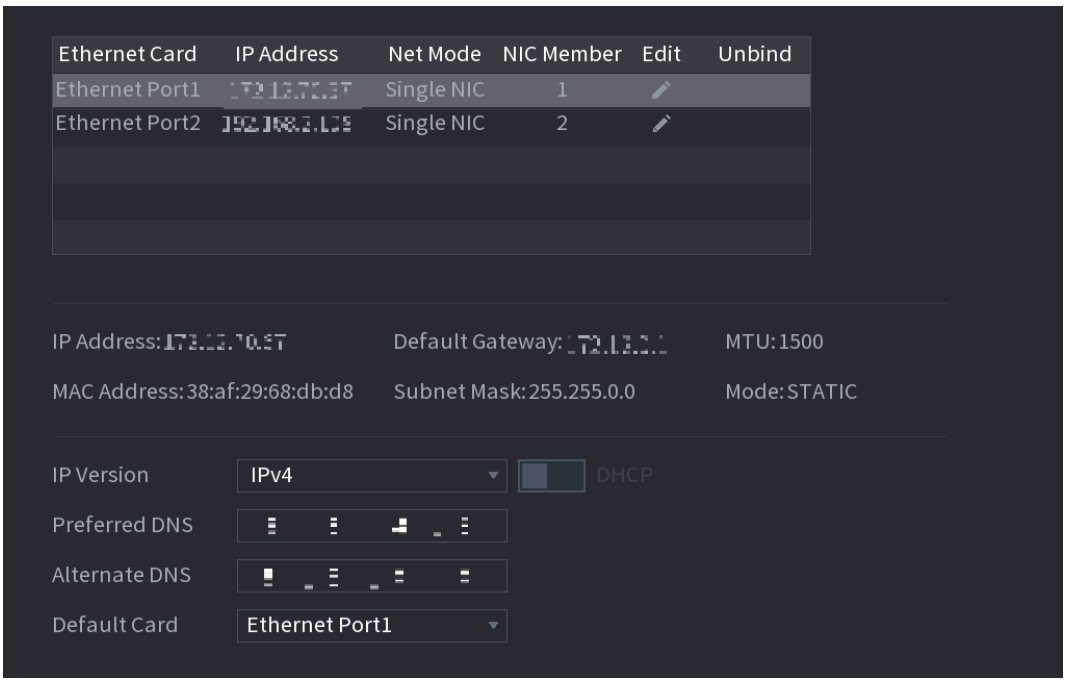
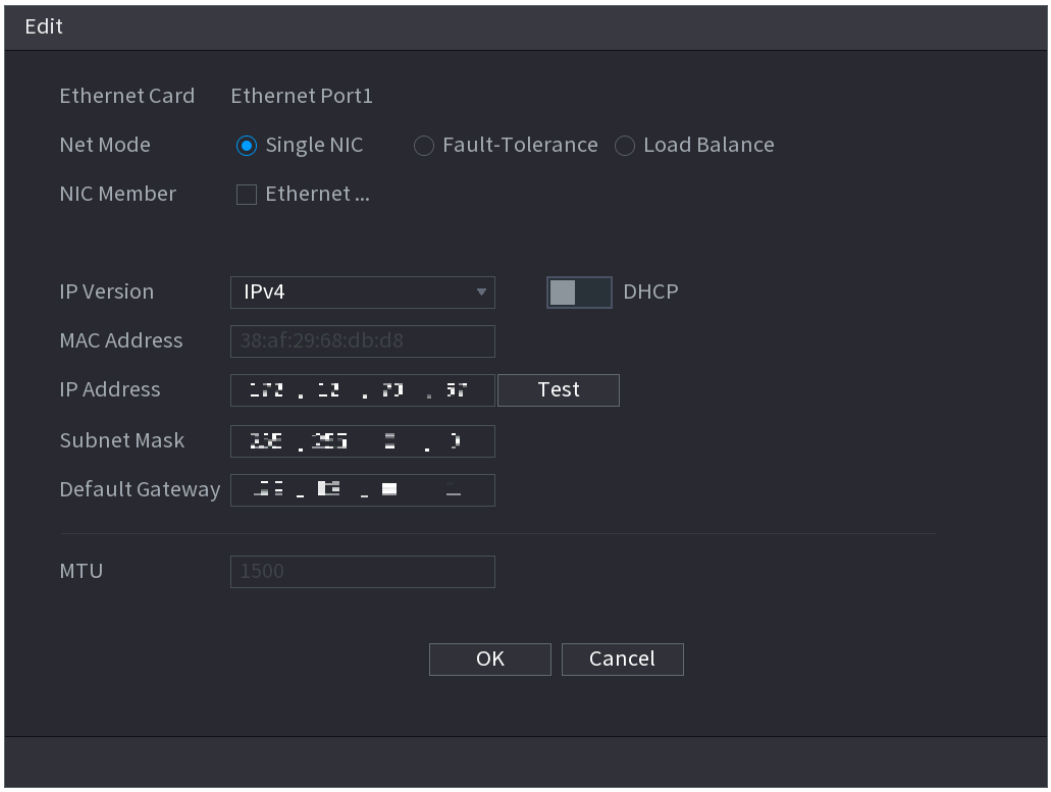


Figure 4-4 Edit



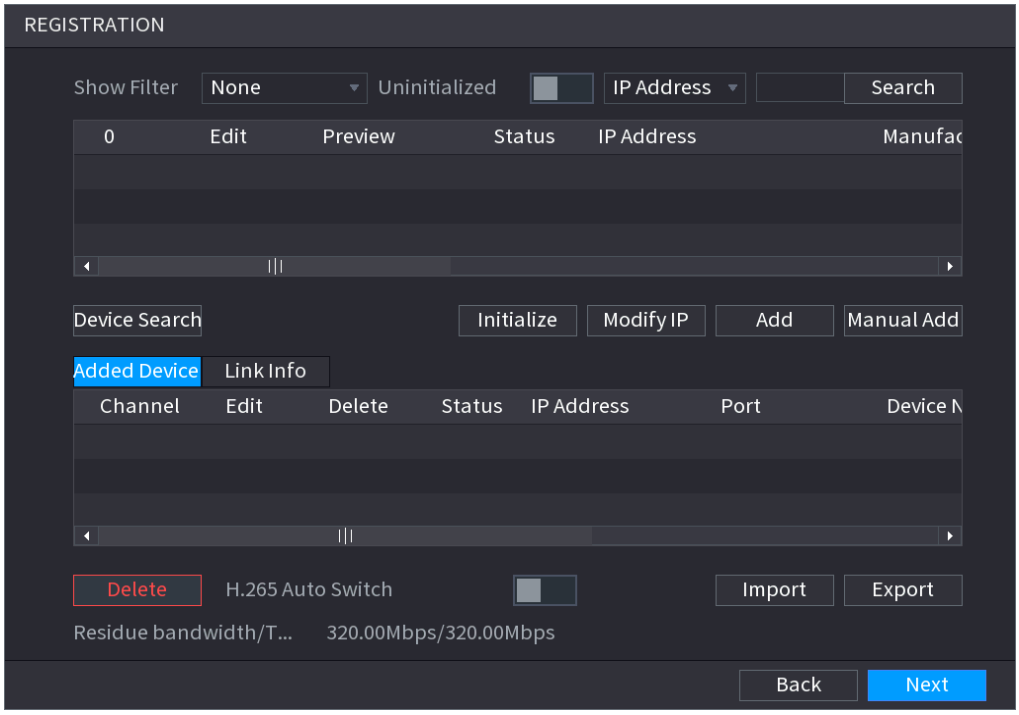
4.4 Camera Registration

Select **Main Menu** > **CAMERA** > **Registration**. The **Registration** interface is displayed. See Figure 4-5.

You can register remote devices through the following two ways:

- Click **Device Search**. In the result list, double-click the remote device or select the check box in front of the device, and then click **Add** to register the remote device.
- Click **Manual Add** and enter the IP address of the remote device to register it.

Figure 4-5 Registration

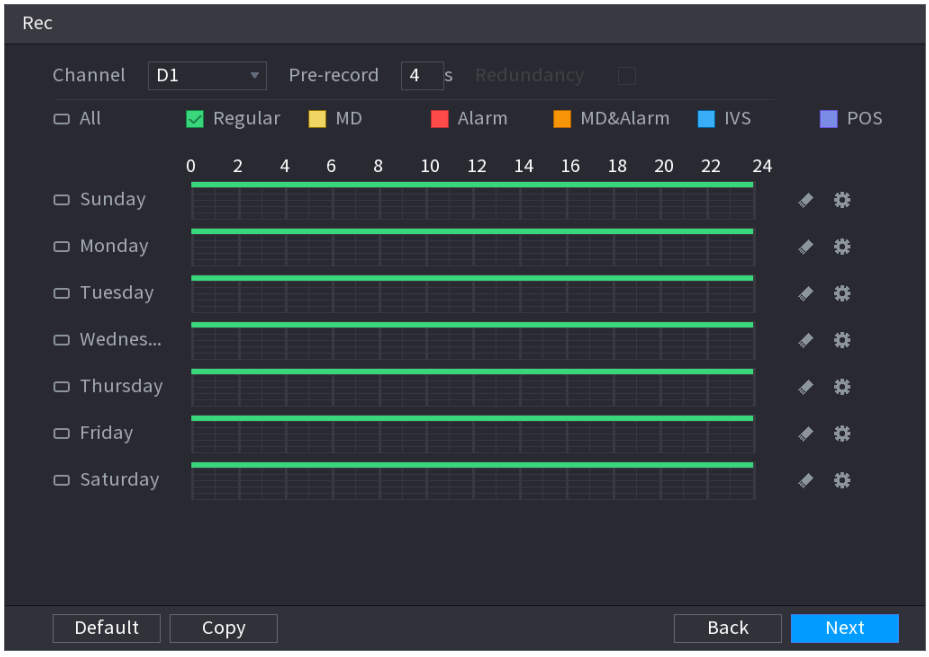


4.5 Schedule

Select **Main Menu** > **STORAGE** > **SCHEDULE** > **Rec**. The **Rec** interface is displayed. See Figure 4-6.

According to the actual needs, drag the mouse in the time figure to draw the period or click to configure the record time.

Figure 4-6 Schedule



4.6 Record Playback

Select **Main Menu** > **PLAYBACK** or right click on the preview interface and select **Search**. The record search interface is displayed. See Figure 4-7.

The system can play back records according to the select criteria such as record type, record time and channel.

Figure 4-7 Record search

4.7 Shut Down

Click  at the top right corner and then select **Shutdown**.

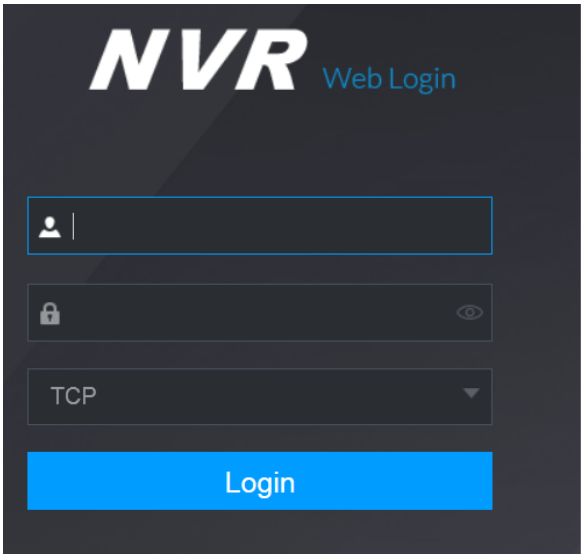
5 Web Operations

If it is your first time to log in the Device, you shall initialize the Device first. For detailed information, see *User's Manual*.

Step 1 Open the browser and enter the IP address of the Device into the address bar. Press Enter key.

The **Login** interface is displayed. See Figure 5-1.

Figure 5-1 Login



Step 2 Enter the username and password.

- The default username is admin, and the login password is the one you set in device initialization. To ensure device security, it is recommended to modify the admin password regularly and keep it properly.
- If you forgot the admin login password, click **Forgot password** to reset it. For detailed information, see *User's Manual*.

Step 3 Click **Login**.

The **Preview** interface is displayed. On the Web interface, you can perform operations such as system settings, device management and network settings. For details, see *User's Manual*.

When you log in Web for the first time, install the control according to system prompts.

6 P2P

Step 1 Scan the QR code with the cell phone to download and install the mobile app.

You can get the mobile app QR code and device SN QR code through the following two ways:

- Log in the local interface and select **Main Menu** > **NETWORK** > **P2P**.
- Log in the Web interface and select **Main Menu** > **NETWORK** > **TCP/IP** > **P2P**.

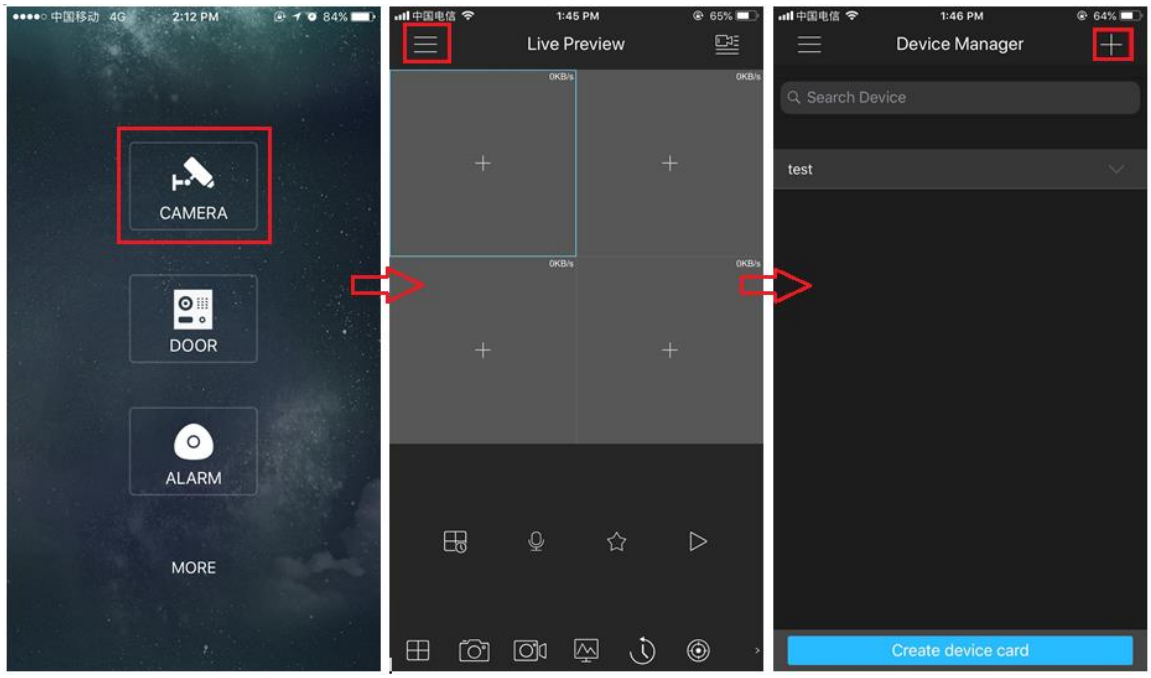
Figure 6-1 Mobile app QR code

Step 2 Register device on the mobile app.

After registering the device successfully, you can view the monitor screen on the mobile phone app.

The following figures are for reference only. The actual product shall govern. For detailed information, see *User's Manual*.

Figure 6-2 Device Manager



Appendix 1 Cybersecurity Recommendations

Cybersecurity is more than just a buzzword: it's something that pertains to every device that is connected to the internet. IP video surveillance is not immune to cyber risks, but taking basic steps toward protecting and strengthening networks and networked appliances will make them less susceptible to attacks. Below are some tips and recommendations on how to create a more secured security system.

Mandatory actions to be taken for basic equipment network security:

1. **Use Strong 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; character types include 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 overlapped characters, such as 111, aaa, etc.;

2. **Update Firmware and Client Software in Time**

   - According to the standard procedure in Tech-industry, we recommend to keep your equipment (such as NVR, DVR, IP camera, etc.) firmware up-to-date to ensure the system is equipped with the latest security patches and fixes. When the equipment is connected to the public network, it is recommended to enable the "auto-check for updates" function to obtain timely information of firmware updates released by the manufacturer.
   - We suggest that you download and use the latest version of client software.

"Nice to have" recommendations to improve your equipment network security:

1. **Physical Protection**

   We suggest that you perform physical protection to equipment, especially storage devices. For example, place the equipment in a special computer room and cabinet, and implement well-done access control permission and key management to prevent unauthorized personnel from carrying out physical contacts such as damaging hardware, unauthorized connection of removable equipment (such as USB flash disk, serial port), etc.

2. **Change Passwords Regularly**

   We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.

3. **Set and Update Passwords Reset Information Timely**

   The equipment supports password reset function. Please set up related information for password reset in time, including the end user's mailbox and password protection questions. If the information changes, please modify it in time. When setting password protection questions, it is suggested not to use those that can be easily guessed.

4. **Enable Account Lock**

   The account lock feature is enabled by default, and we recommend you to keep it on to guarantee the account security. If an attacker attempts to log in with the wrong password several times, the corresponding account and the source IP address will be locked.

5. **Change Default HTTP and Other Service Ports**

   We suggest you to change default HTTP and other service ports into any set of numbers between 1024~65535, reducing the risk of outsiders being able to guess which ports you are using.

6. **Enable HTTPS**

   We suggest you to enable HTTPS, so that you visit Web service through a secure communication channel.

7. **Enable Whitelist**

   We suggest you to enable whitelist function to prevent everyone, except those with specified IP addresses, from accessing the system. Therefore, please be sure to add your computer's IP address and the accompanying equipment's IP address to the whitelist.

8. **MAC Address Binding**

   We recommend you to bind the IP and MAC address of the gateway to the equipment, thus reducing the risk of ARP spoofing.

9. **Assign Accounts and Privileges Reasonably**

   According to business and management requirements, reasonably add users and assign a minimum set of permissions to them.

10. **Disable Unnecessary Services and Choose Secure Modes**

    If not needed, it is recommended to turn off some services such as SNMP, SMTP, UPnP, etc., to reduce risks.

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

    - SNMP: Choose SNMP v3, and set up strong encryption passwords and authentication passwords.
    - SMTP: Choose TLS to access mailbox server.
    - FTP: Choose SFTP, and set up strong passwords.
    - AP hotspot: Choose WPA2-PSK encryption mode, and set up strong passwords.

11. **Audio and Video Encrypted Transmission**

    If your audio and video data contents are very important or sensitive, we recommend that you use encrypted transmission function, to reduce the risk of audio and video data being stolen during transmission.

    Reminder: encrypted transmission will cause some loss in transmission efficiency.

12. **Secure Auditing**

    - Check online users: we suggest that you check online users regularly to see if the device is logged in without authorization.
    - Check equipment log: By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.

13. **Network Log**

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

14. **Construct a Safe Network Environment**

    In order to better ensure the safety of equipment and reduce potential cyber risks, we recommend:

    - Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.

- The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.
- Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.