AI Network Video Recorder

Quick Start Guide

V1.0.0

Cybersecurity Recommendations

Mandatory actions to be taken towards cybersecurity

1. Change Passwords and Use Strong Passwords:

The number one reason systems get “hacked” is due to having weak or default passwords. It is recommended to change default passwords immediately and choose a strong password whenever possible. A strong password should be made up of at least 8 characters and a combination of special characters, numbers, and upper and lower case letters.

2. Update Firmware

As is standard procedure in the tech-industry, we recommend keeping NVR, DVR, and IP camera firmware up-to-date to ensure the system is current with the latest security patches and fixes.

“Nice to have” recommendations to improve your network security

1. Change Passwords Regularly

Regularly change the credentials to your devices to help ensure that only authorized users are able to access the system.

2. Change Default HTTP and TCP Ports:

● Change default HTTP and TCP ports for systems. These are the two ports used to communicate and to view video feeds remotely.

● These ports can be changed to any set of numbers between 1025-65535. Avoiding the default ports reduces the risk of outsiders being able to guess which ports you are using.

3. Enable HTTPS/SSL:

Set up an SSL Certificate to enable HTTPS. This will encrypt all communication between your devices and recorder.

4. Enable IP Filter:

Enabling your IP filter will prevent everyone, except those with specified IP addresses, from accessing the system.

5. Change ONVIF Password:

On older IP Camera firmware, the ONVIF password does not change when you change the system’s credentials. You will need to either update the camera’s firmware to the latest revision or manually change the ONVIF password.

6. Forward Only Ports You Need:

● Only forward the HTTP and TCP ports that you need to use. Do not forward a huge range of numbers to the device. Do not DMZ the device's IP address.

● You do not need to forward any ports for individual cameras if they are all connected to a recorder on site; just the NVR is needed.

7. Disable Auto-Login on SmartPSS:

Those using SmartPSS to view their system and on a computer that is used by multiple people should disable auto-login. This adds a layer of security to prevent users without the appropriate credentials from accessing the system.

8. Use a Different Username and Password for SmartPSS:

In the event that your social media, bank, email, etc. account is compromised, you would not want someone collecting those passwords and trying them out on your video surveillance system. Using a different username and password for your security system will make it more difficult for someone to guess their way into your system.

9. Limit Features of Guest Accounts:

If your system is set up for multiple users, ensure that each user only has rights to features and functions they need to use to perform their job.

10. UPnP:

● UPnP will automatically try to forward ports in your router or modem. Normally this would be a good thing. However, if your system automatically forwards the ports and you leave the credentials defaulted, you may end up with unwanted visitors.

● If you manually forwarded the HTTP and TCP ports in your router/modem, this feature should be turned off regardless. Disabling UPnP is recommended when the function is not used in real applications.

11. SNMP:

Disable SNMP if you are not using it. If you are using SNMP, you should do so only temporarily, for tracing and testing purposes only.

12. Multicast:

Multicast is used to share video streams between two recorders. Currently there are no known issues involving Multicast, but if you are not using this feature, deactivation can enhance your network security.

13. Check the Log:

If you suspect that someone has gained unauthorized access to your system, you can check the system log. The system log will show you which IP addresses were used to login to your system and what was accessed.

14. Physically Lock Down the Device:

Ideally, you want to prevent any unauthorized physical access to your system. The best way to achieve this is to install the recorder in a lockbox, locking server rack, or in a room that is behind a lock and key.

15. Connect IP Cameras to the PoE Ports on the Back of an NVR:

Cameras connected to the PoE ports on the back of an NVR are isolated from the outside world and cannot be accessed directly.

16. Isolate NVR and IP Camera Network

The network your NVR and IP camera resides on should not be the same network as your public computer network. This will prevent any visitors or unwanted guests from getting access to the same network the security system needs in order to function properly.

General

This quick start guide (hereinafter referred to be "the Guide") 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 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

No.	Version	Revision Content	Release Time
1	V1.0.0	First Release.	

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 Guide

- The Guide is for reference only. If there is inconsistency between the Guide 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 Guide.
- The Guide 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 Guide. 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 Guide (in PDF format) cannot be opened.
- All trademarks, registered trademarks and the company names in the Guide 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 Guide carefully before use to prevent danger and property loss. Strictly conform to the Guide during application and keep it properly after reading.

Operating Requirement

- Install the POE front-end device indoors.
- The device does not support wall mount.
- Don’t place and install the device in an area exposed to direct sunlight or near heat generating device.
- Don’t 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.
- Don’t 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.
- Don’t 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

Cybersecurity Recommendations ..... **I**
Foreword ..... **III**
Important Safeguards and Warnings ..... **V**
1 Checking the Components **1**
2 Installing HDD **2**
2.1 1-HDD 2
2.2 2-HDD 4
3 Connection **7**
4 GUI Operations **8**
4.1 Booting Up 8
4.2 Initializing the Device 8
4.3 Modifying IP Address 11
4.4 Camera Registration 12
4.5 Schedule 13
4.6 Record Playback 14
4.7 Shut Down 15
5 Web Operations **16**
6 P2P **17**

1 Checking the Components

CAUTION

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. **NOTE** 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. **NOTE** 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.

CAUTION

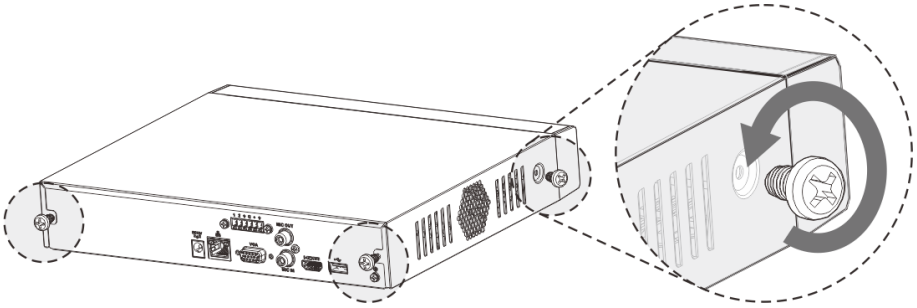
Shut off the power before you replace the HDD.

For the first time installation, make sure 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

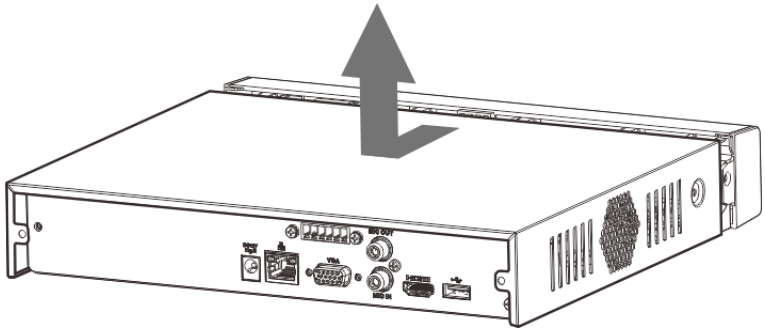
Step 1 Remove the fixing screws of the case cover (including the two screws on the rear panel and two screws on the left and right panels).

Figure 2-1 Installing HDD (1)



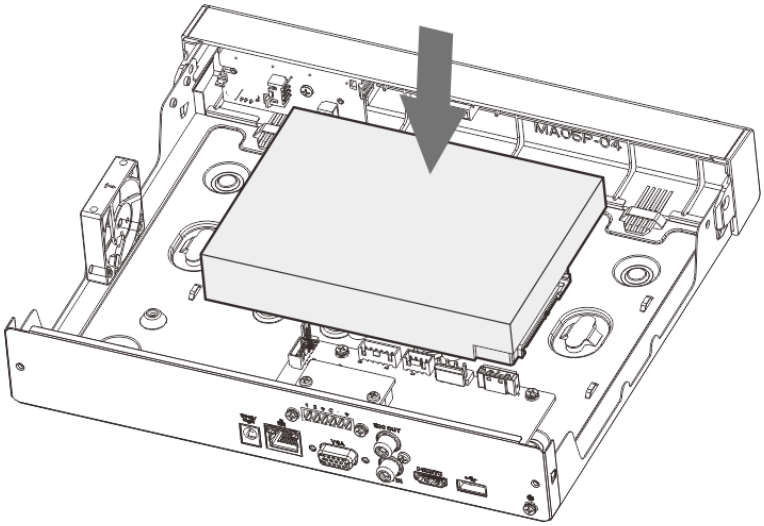
Step 2 Remove the case cover along the direction shown in the following arrow.

Figure 2-2 Installing HDD (2)



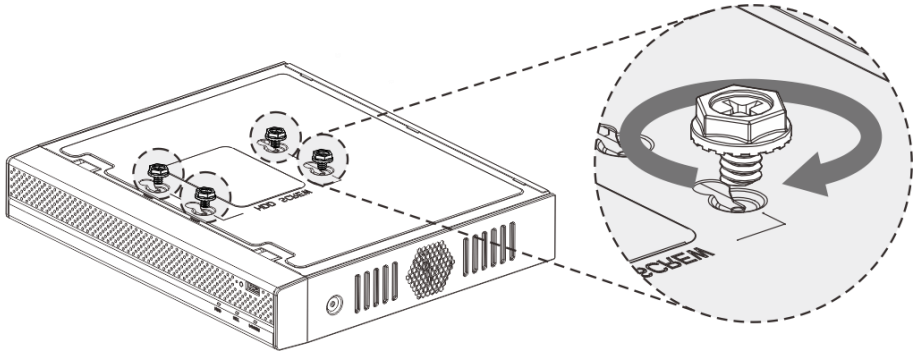
Step 3 Match the four holes on the baseboard to place the HDD.

Figure 2-3 Installing HDD (3)



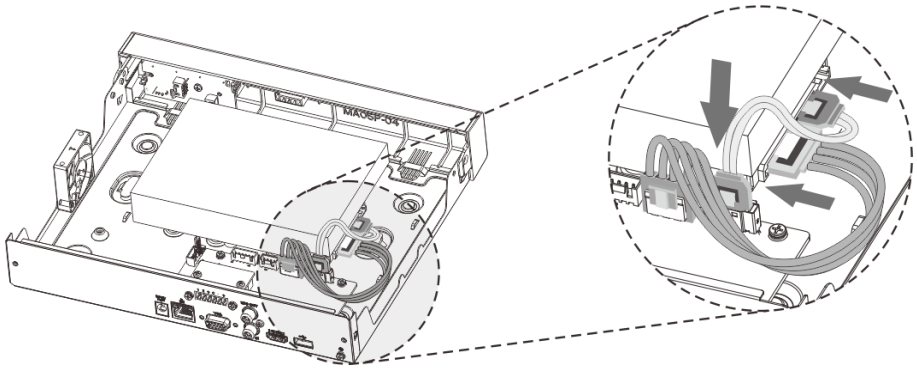
Step 4 Turn the Device upside down, match the screws with the holes on the HDD and then fasten them. The HDD is fixed to the baseboard

Figure 2-4 Installing HDD (4)



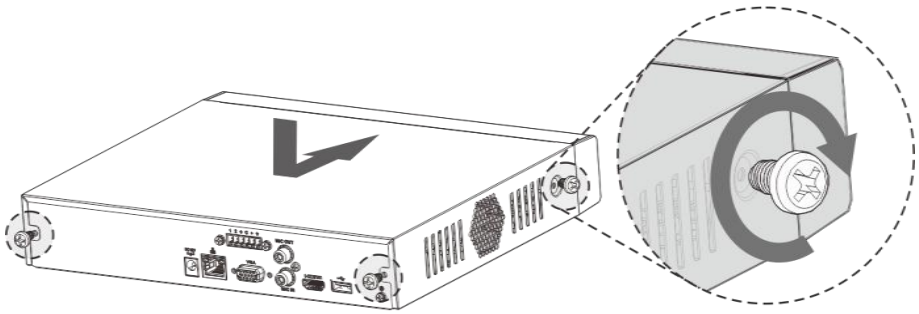
Step 5 Connect the HDD data cable and power cable to the Device.

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.

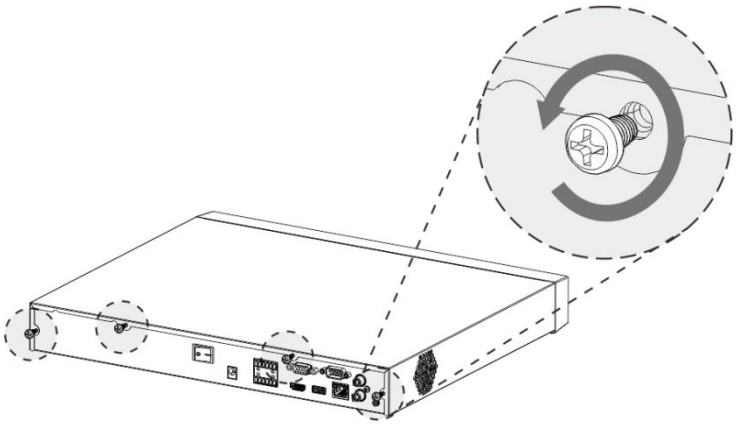
Figure 2-6 Installing HDD (6)



2.2 2-HDD

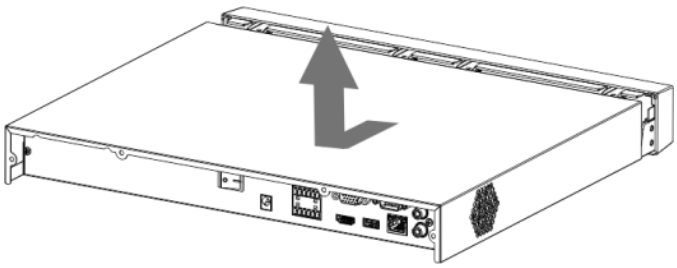
Step 1 Remove the four fixing screws on the rear panel.

Figure 2-7 Installing HDD (1)



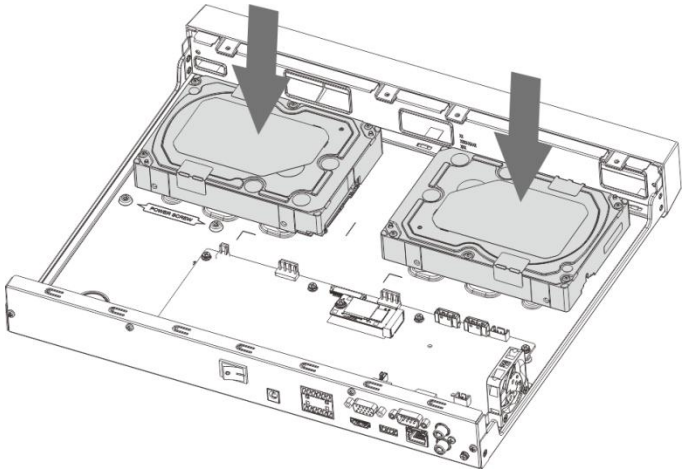
Step 2 Remove the case cover along the direction shown in the following arrow.

Figure 2-8 Installing HDD (2)



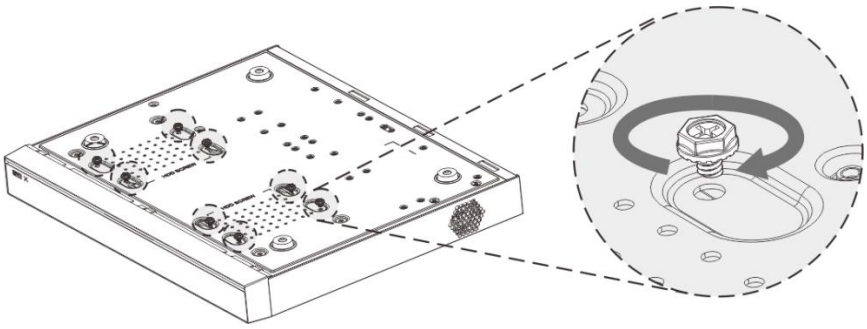
Step 3 Match the four holes on the baseboard to place the HDD.

Figure 2-9 Installing HDD (3)



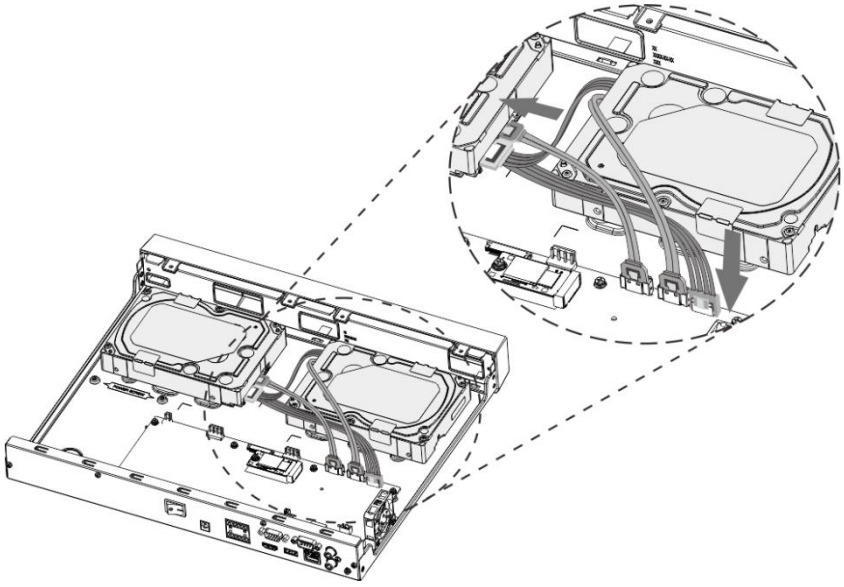
Step 4 Turn the Device upside down, match the screws with the holes on the HDD and then fasten them. The HDD is fixed to the baseboard

Figure 2-10 Installing HDD (4)



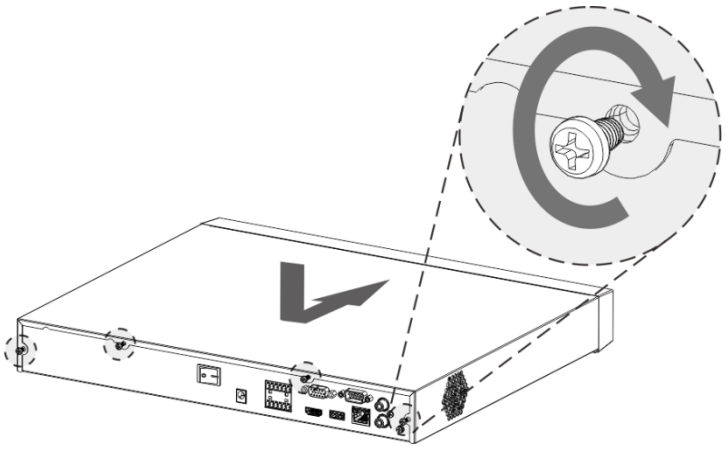
Step 5 Connect the HDD data cable and power cable to the Device.

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)

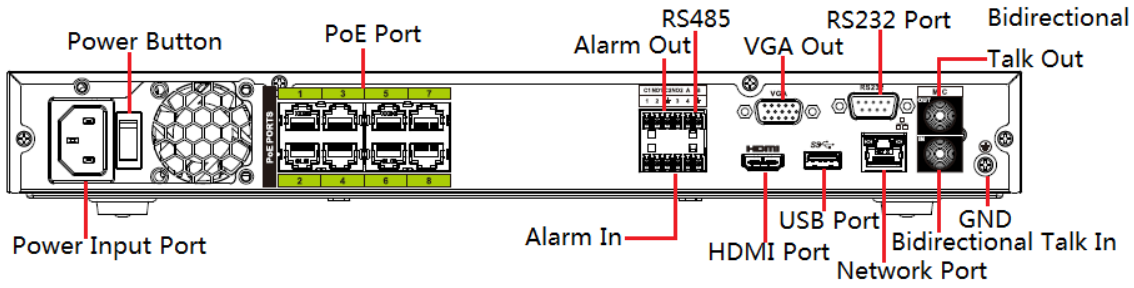


3 Connection

NOTE

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

NOTE

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

CAUTION

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.

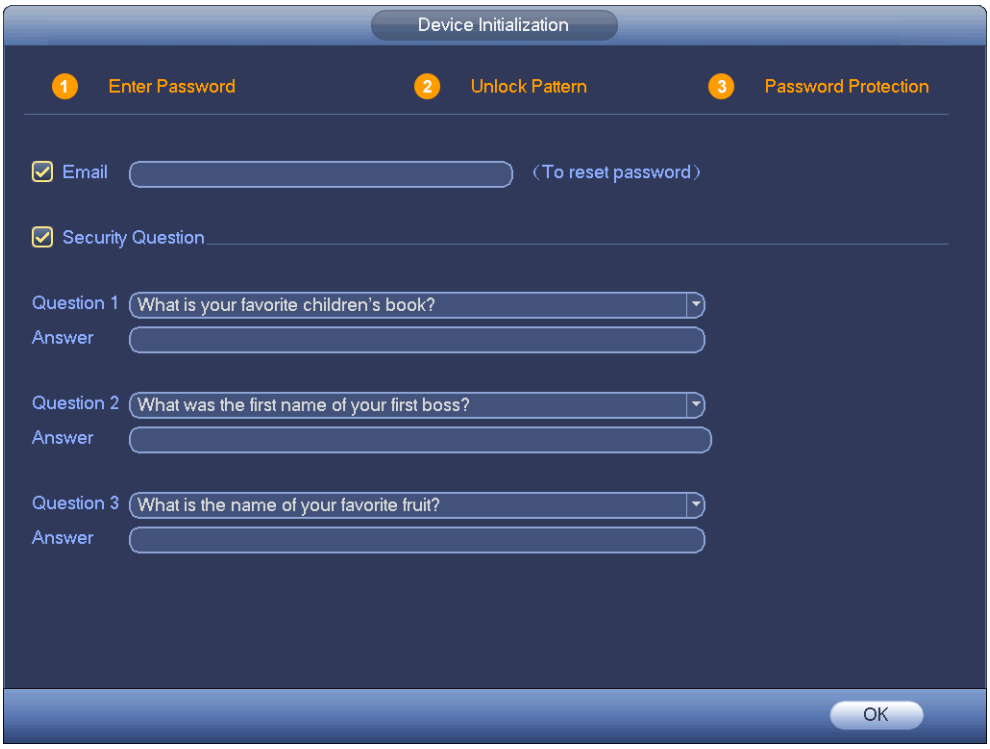
Step 3 Configure the unlock pattern or click **Skip**.

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

NOTE

- 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.

NOTE

- 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.
NOTE 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

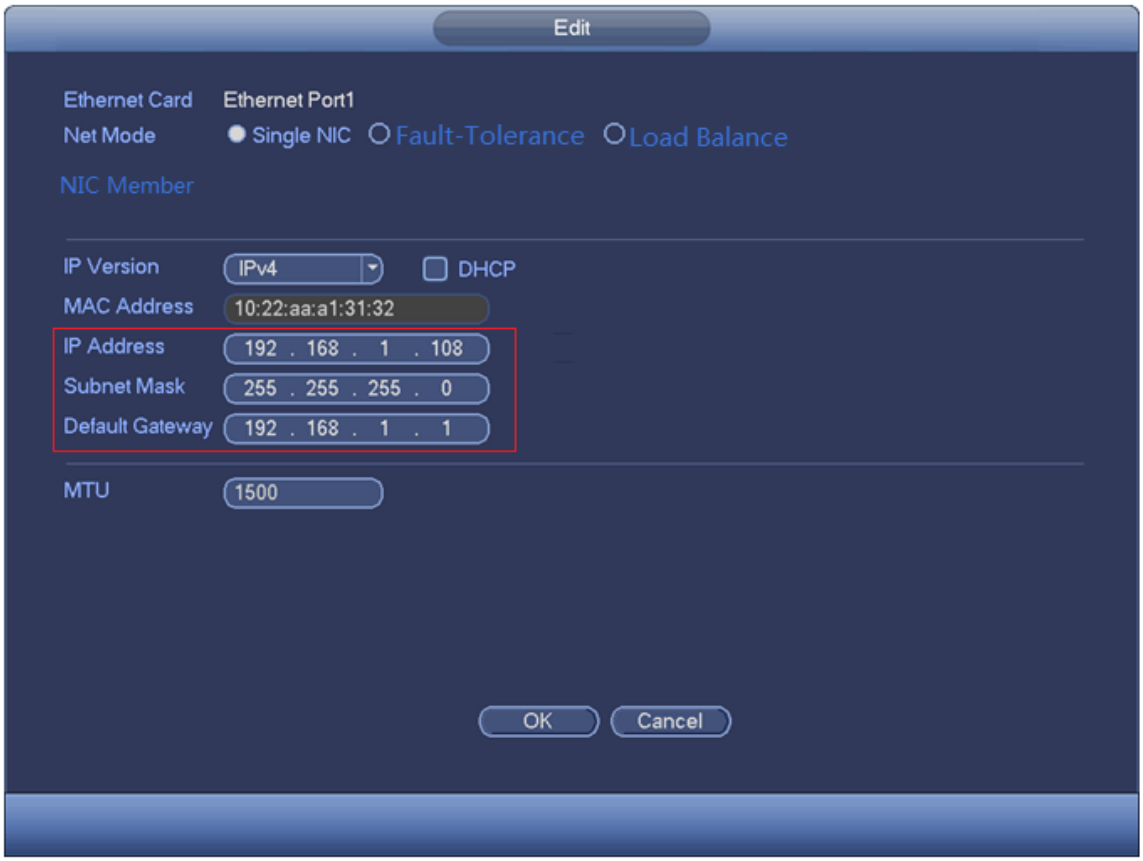
Step 1 Select **Main Menu** > **SETTING** > **NETWORK** > **TCP/IP**.
The TCP/IP interface is displayed. See Figure 4-3.

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** > **SETTING** > **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.

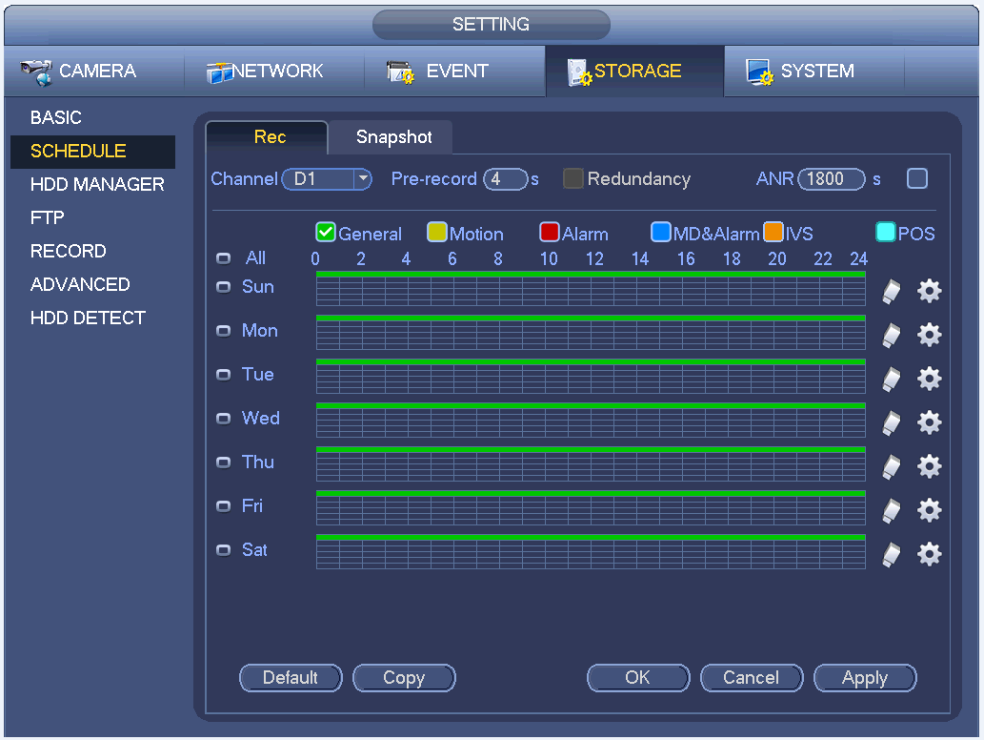
Figure 4-5 Registration

4.5 Schedule

Select **Main Menu** > **SETTING** > **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

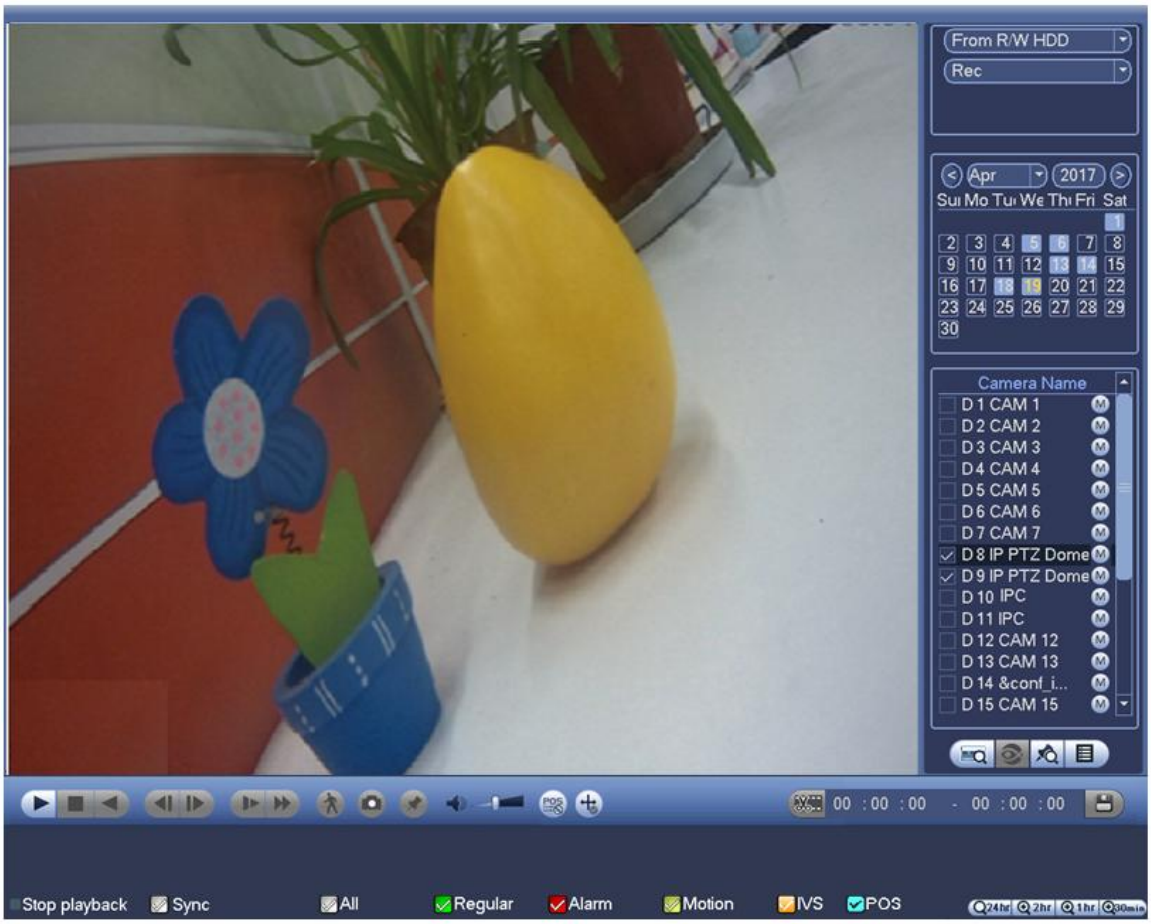


4.6 Record Playback

Select **Main Menu** > **Search** 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

Select **Main Menu** > **SHUT DOWN** and the **SHUT DOWN** interface is displayed. Click **Shut down**.

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.

NOTE

- 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*.

NOTE

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** > **SETTING** > **NETWORK** > **P2P**.
- Log in the Web interface and select **SETUP** > **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 cell phone APP.

NOTE

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

Figure 6-2 Device Manager