



Hunter Series Network Video Recorder

Quick Start Guide

V1.0.1






Foreword

General

This manual introduces the functions and operations of the NVR devices (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

No.	Version	Revision Content	Release Time
2	V1.0.1	<ul style="list-style-type: none"> Updated a figure in Schedule. Updated electrical safety. 	September 2019
1	V1.0.0	First release.	July 2019

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

Thank you for purchasing our Network Video Recorder (NVR).

This manual will help you become familiar with our NVR in a short time. Please read the manual carefully before starting using your NVR and properly keep it for future reference.

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.

Electrical Safety

- Improper battery use might result in fire, explosion, or inflammation.
- When replacing battery, make sure the same model is used.
- Use the recommended power cables in the region and conform to the rated power specification.
- Use the power adapter provided with the Device; otherwise, it might result in people injury and device damage.
- The power source shall conform to the requirement of the Safety Extra Low Voltage (SELV) standard, and supply power with rated voltage which conforms to Limited power Source requirement according to IEC60950-1. Please note that the power supply requirement is subject to the device label.
- Connect the device (I-type structure) to the power socket with protective earthing.
- The appliance coupler is a disconnection device. When using the coupler, keep the angle for easy operation.

Table of Contents

Foreword	I
Important Safeguards and Warnings	III
1 Quick Start	1
1.1 Checking the Components	1
1.2 Installing HDD	2
2 The Grand Tour	6
3 Connection	9
4 Local Configurations	10
4.1 Booting Up	10
4.2 Initializing the Device	10
4.3 Resetting Password	13
4.4 Startup Wizard	17
4.5 Registration	17
4.6 Schedule	18
4.7 Instant Playback	19
5 Web Operations	21
Appendix 1 Cybersecurity Recommendations	23



1 Quick Start



The Device does not support wall mount.

1.1 Checking the Components

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.

No.	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	<ul style="list-style-type: none"> Device model conforms to the purchase order. Not torn up.  <p>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 request the after-sales service.</p>
3	Device	Appearance	No obvious damage.
		Data cables, power cables, fan cables, mainboard	<p>No loose connection.</p>  <p>If there is any loose connection, please contact the company after-sales service in time.</p>

1.2 Installing HDD

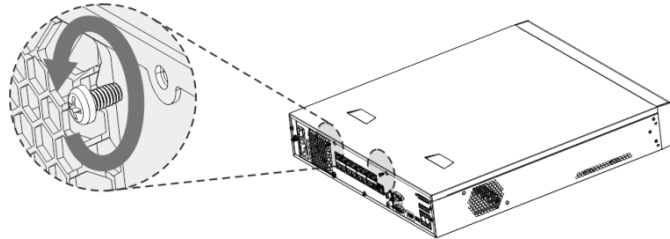
For the first time installation, check whether the HDD has been installed or not. We recommend to use HDD of enterprise level or surveillance level. It is not recommended to use PC HDD.



- Shut down the NVR and unplug the power cord before opening cover to replace the HDD.
- Different models have different HDD numbers. The actual product shall prevail.

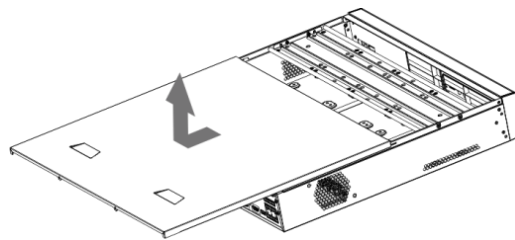
Step 1 Remove the fixing screws on the rear panel.

Figure 1-1 Remove the screws



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

Figure 1-2 Remove case cover



Step 3 Remove the screws on the sides of HDD bracket to take out the bracket.

- 4-HDD NVR has one HDD bracket. For the way to remove the bracket, see Figure 1-3.
- 8-HDD NVR has two HDD brackets. For the way to remove the brackets, see Figure 1-4.

Figure 1-3 Remove HDD bracket (4-HDD)

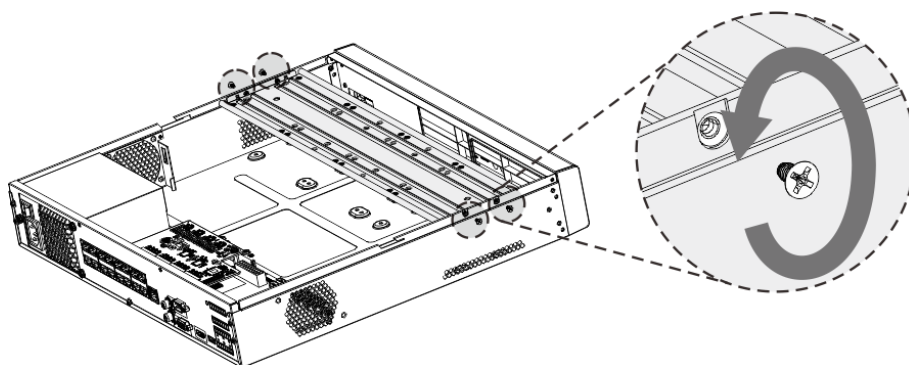
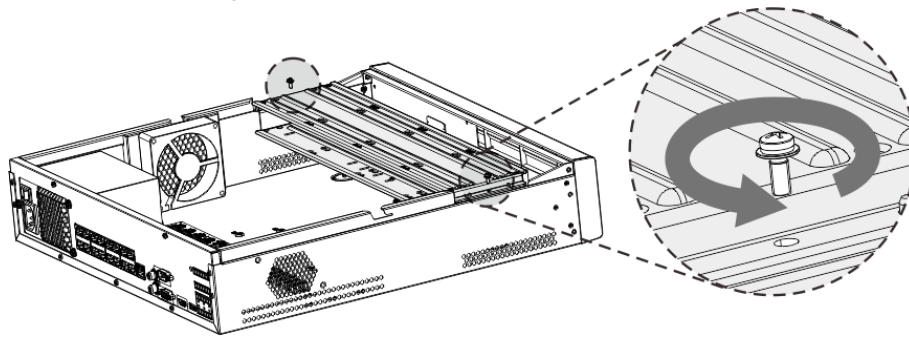
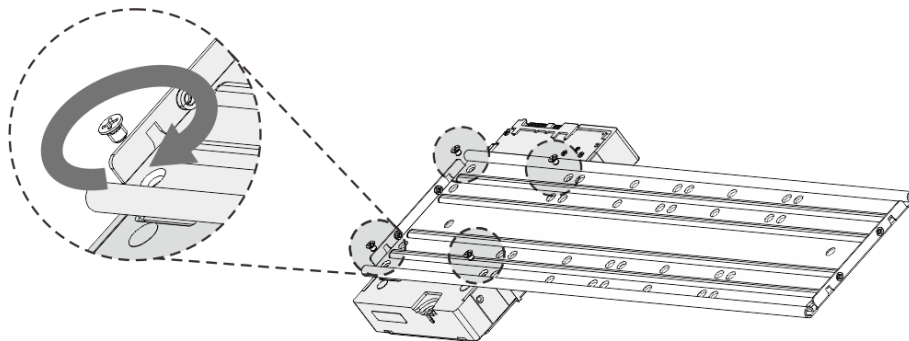


Figure 1-4 Remove HDD bracket (8-HDD)



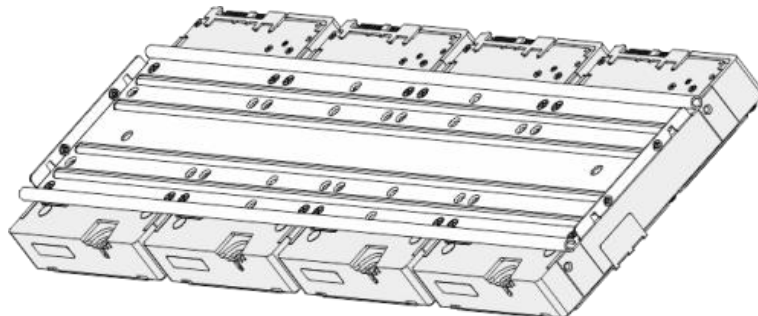
Step 4 Match the four screw holes on the HDD with the four holes on the bracket and then fasten the screws. The HDD is fixed to the bracket.

Figure 1-5 Fix the HDD (1)



Step 5 Refer to Step 4 to install other HDDs.

Figure 1-6 Fix the HDD (2)

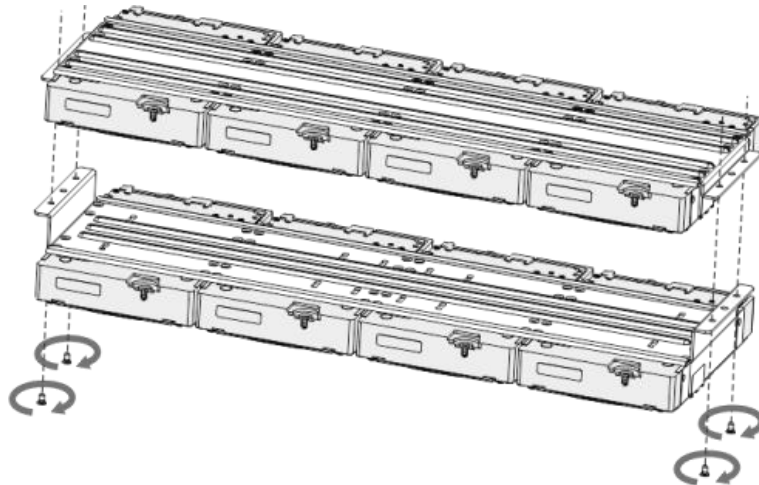


Step 6 Lock the two HDD brackets.



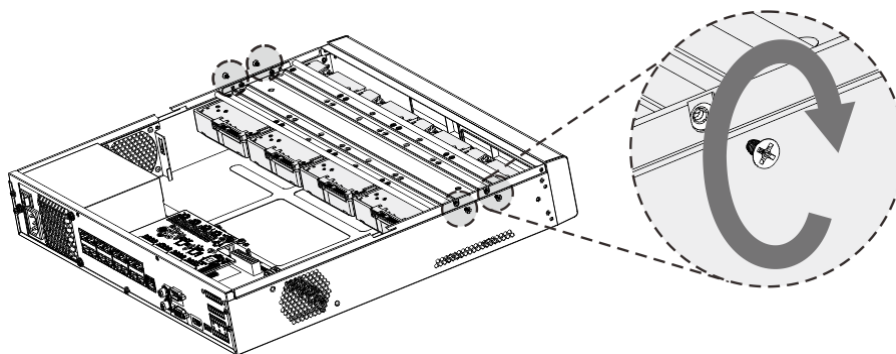
This step is required for 8-HDD devices only.

Figure 1-7 Lock two HDD brackets



Step 7 Place the bracket to the device and then fasten the screws on the sides of the bracket.

Figure 1-8 Fasten HDD bracket

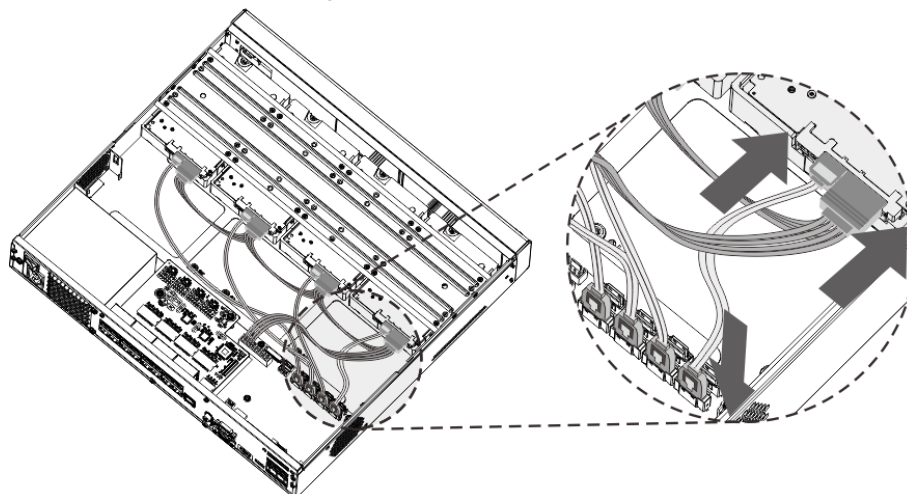


Step 8 Connect the HDD data cable and power cable to the device.



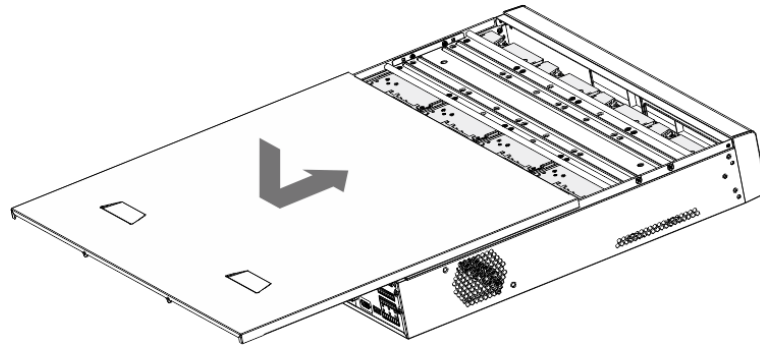
Figure 1-9 takes 4-HDD device as an example. The actual product shall prevail.

Figure 1-9 Connect cables



Step 9 Put back the cover and fasten the screws on the rear panel to complete the installation.

Figure 1-10 Complete installation



2 The Grand Tour



- The following figures are for reference only. The actual product shall prevail.
- See *User's Manual* for detailed information.

Figure 2-1 Front panel

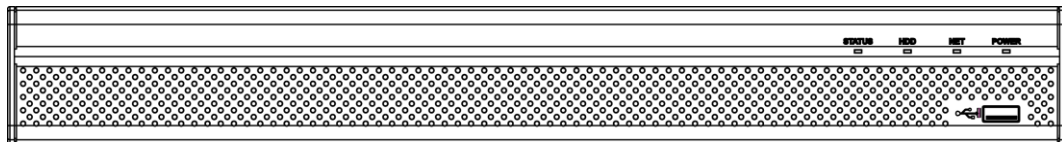


Table 2-1 Description of front panel functions


Icon	Name	Description
STATUS	Status indicator	After booting up the Device, the indicator glows blue.
HDD	HDD status indicator	<ul style="list-style-type: none"> • The indicator is off when the HDD is normal. • The indicator glows blue when the HDD is in malfunction.
NET	Network status indicator	<ul style="list-style-type: none"> • The indicator is off when the network is normal. • The indicator glows blue when the network is in malfunction.
POWER	Power status indicator	The indicator glows blue when the power supply is normal.
	USB 2.0 port	Connects to external devices such as USB storage device, keyboard and mouse.

Figure 2-2 Rear panel

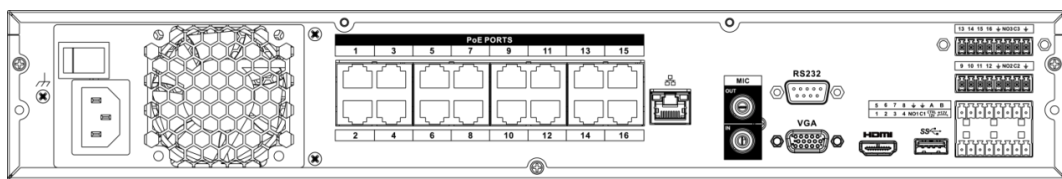







Table 2-2 Description of rear panel functions

Icon	Port Name	Function
	Power button	Turns on/off the NVR.
	Power input port	Input power.
MIC IN	Audio input port	Bidirectional talk input port. It is to receive analog audio signal from devices such as microphone, sound pickup.

Icon	Port Name	Function
MIC OUT	Audio output port	<p>Audio output port. It is to output analog audio signal to devices such as sound box.</p> <ul style="list-style-type: none"> ● Bidirectional talk output. ● Audio output for 1-window video monitor. ● Audio output for 1-window video playback.
1-16	Alarm input port (1-16)	<ul style="list-style-type: none"> ● There are four groups: 1-4, 5-8, 9-12 and 13-16. They receive signals from external alarm source. Alarm input includes two types; NO (normal open) and NC (normal close). ● When your alarm input device is using external power, make sure the device and the NVR have the same GND.
	GND	Alarm input ground port.
NO1-NO3	Alarm output port 1-3	<ul style="list-style-type: none"> ● Three groups of alarm output ports (NO1-C1; NO2-C2; NO3-C3). Output alarm signal to the external alarm device. Make sure power supply is available for the external alarm device. ● NO: Normal open alarm output port. ● C: Alarm output public end.
C1-C3		
A	RS-485 port	<ul style="list-style-type: none"> ● RS485_A port. Control cable A of the 485 device. It connects external devices such as speed dome and PTZ. ● RS485_B port. Control cable B of the 485 device. It connects external devices such as speed dome and PTZ.
B		
CTRL 12V	-	Controllable 12V power output. It is to control the on-off alarm relay output. It can be used to control the device alarm output. At the same time, it can also be used as the power input source of some devices such as alarm detector.
+12V	-	+12V power output port. It can provide power to some peripheral devices such as camera and alarm device. Make sure the power supply of peripheral device shall be below 1A.
	Network port	10M/100M/1000Mbps self-adaptive Ethernet port. Connect to the network cable.
eSATA	eSATA port	External SATA port. It can connect device with SATA port. You need to set HDD jumper when connecting a HDD.
USB port	USB port	Connect to devices such as mouse, USB storage device and USB burner.
RS-232	RS-232 port	It is for general COM debugging to configure IP address and transfer transparent COM data.
HDMI	HDMI port	High definition audio and video signal output port. It transmits uncompressed high definition video and multiple-channel audio data to display devices with HDMI

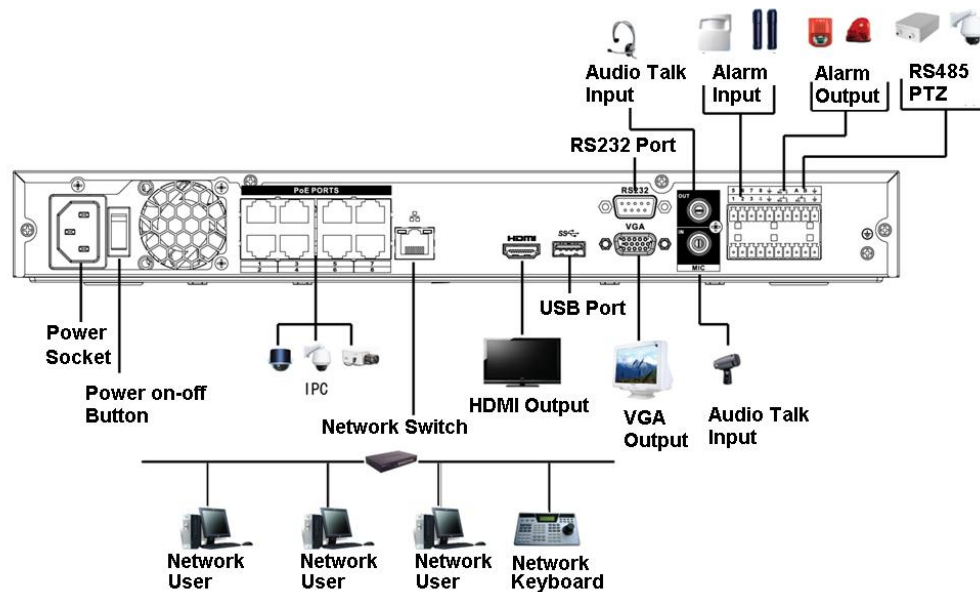
Icon	Port Name	Function
		port.
VGA	VGA port	VGA video output port. It can connect to the monitor to view analog video.
	GND	Ground.

3 Connection



- The following figure is for reference only. The actual product shall prevail.
- See User's Manual for detailed information.

Figure 3-1 Device connection



Error! Use the Home tab to apply 标题 1,I1,H1,Title1,Normal + Font:

Helvetica,Bold,Space Before 12 pt,Not Bold,Heading

One,h1,Head1,Head,1,Numbered,nu,Level 1 Head,1st level,Section

Head,Sec1,h11,1st level1,h12,1st level2,h13,1st level3,h14,1st level4,h15,1st leve 9

4 Local Configurations



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

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.

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.



Error! Use the Home tab to apply 标题 1, I1, H1, Title1, Normal + Font:

Helvetica, Bold, Space Before 12 pt, Not Bold, Heading One, h1, Head1, Head, 1, Numbered, nu, Level 1 Head, 1st level, Section Head, Sec1, h11, 1st level1, h12, 1st level2, h13, 1st level3, h14, 1st level4, h15, 1st level5 10

Figure 4-1 Enter password

Step 2 Configure the password information for admin. For details, see Table 4-1.

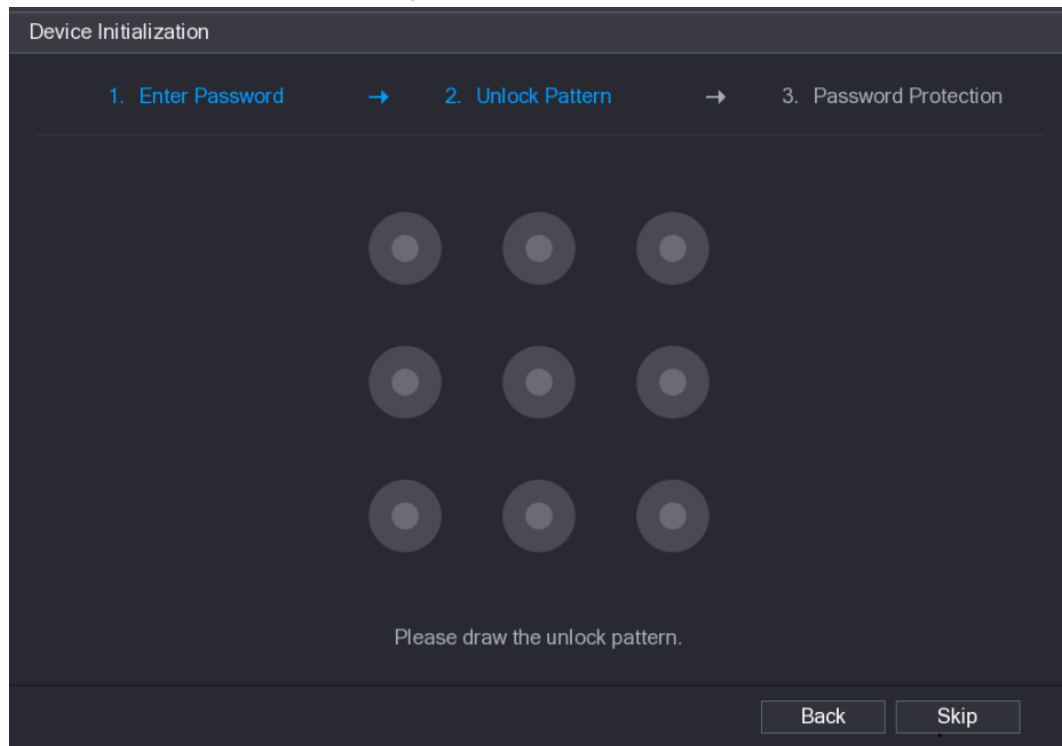
Table 4-1 Password information description

Parameter	Description
User	By default, the user is admin .
Password	In the Password box, enter the password for admin. The new password can be set from 8 characters through 32 characters and contain at least two types from number, letter and special characters (excluding "", "", ", ":", " and "&").
Confirm Password	
Prompt Question	In the Prompt Question box, enter the information that can remind you of the password.  On the login interface, click  and the prompt will display to help you reset the password.

Step 3 Click **Next**.

The **Unlock Pattern** setting interface is displayed. See Figure 4-2.

Figure 4-2 Unlock pattern

**Step 4** Draw an unlock pattern.

After setting unlock pattern, the password protection setting interface is displayed. See Figure 4-3.



- 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.
- If you do not want to configure the unlock pattern, click **Skip**.

Figure 4-3 Password protection

Device Initialization

1. Enter Password → 2. Unlock Pattern → 3. Password Protection

Email Address ☐ To reset password, please input properly or update in time

Security Questions ☐

Question 1 What is your favorite children's book? ▾

Answer

Question 2 What was the first name of your first boss? ▾

Answer

Question 3 What is the name of your favorite fruit? ▾

Answer

Save

Error! Use the Home tab to apply 标题 1,I1,H1,Title1,Normal + Font:

Helvetica,Bold,Space Before 12 pt,Not Bold,Heading

One,h1,Head1,Head,1,Numbered,nu,Level 1 Head,1st level,Section

Head,Sec1,h11,1st level1,h12,1st level2,h13,1st level3,h14,1st level4,h15,1st leve 12

Step 5 Configure the protection parameters for password. For details, see Table 4-2.



- 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 4-2 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 function later or you want to change the configurations, select Main Menu > ACCOUNT > USER .	

Step 6 Click **OK** to complete the settings.

The **Startup Wizard** interface is displayed. For details about quick settings during startup, see "4.4 Startup Wizard."


4.3 Resetting Password

If you forgot the admin password, you can reset the password by the following ways:

- When the password reset function is enabled, you can scan the QR code on the local interface to reset the password.
- When the password reset function is disabled, there are two situations:
 - ◇ If you configured security questions, you can reset the password by the security questions.
 - ◇ If you did not configure the security questions, you can only use the reset button on the mainboard to restore the Device to factory default.



Reset button is for some series product only.

Step 1 Click  on the login interface.

The **Reset Password** interface is displayed. See Figure 4-4.




- On the unlock pattern interface, click **Forgot Unlock Pattern** to switch to the password login interface, and then click .
- If you have not input email address in device initialization, the interface is shown as in Figure 4-5. Configure an email address, click **Next**, and then the Device goes to Figure 4-4.

Figure 4-4 Reset password (1)

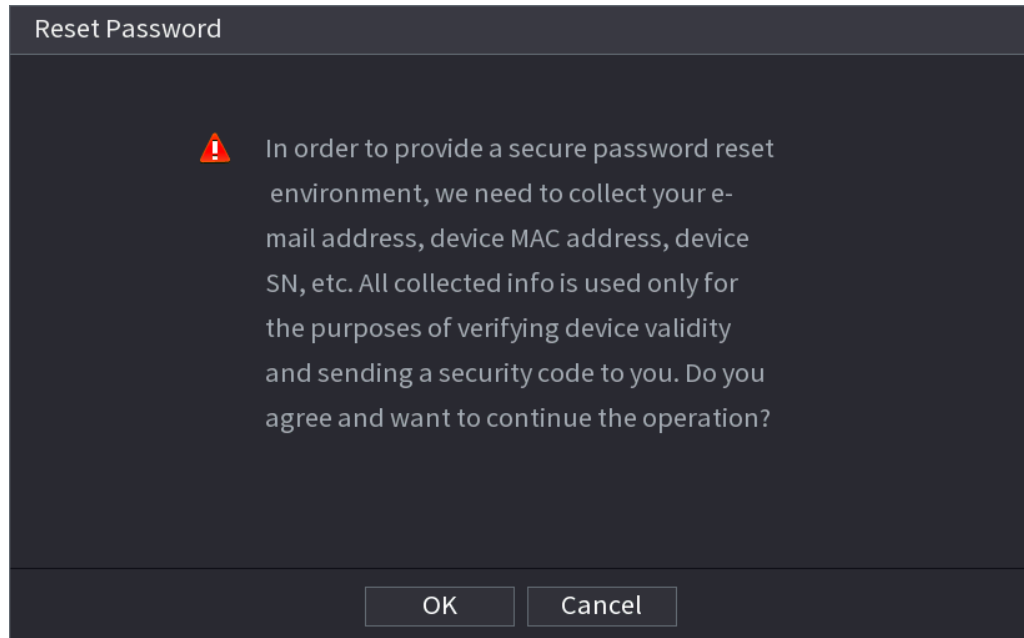
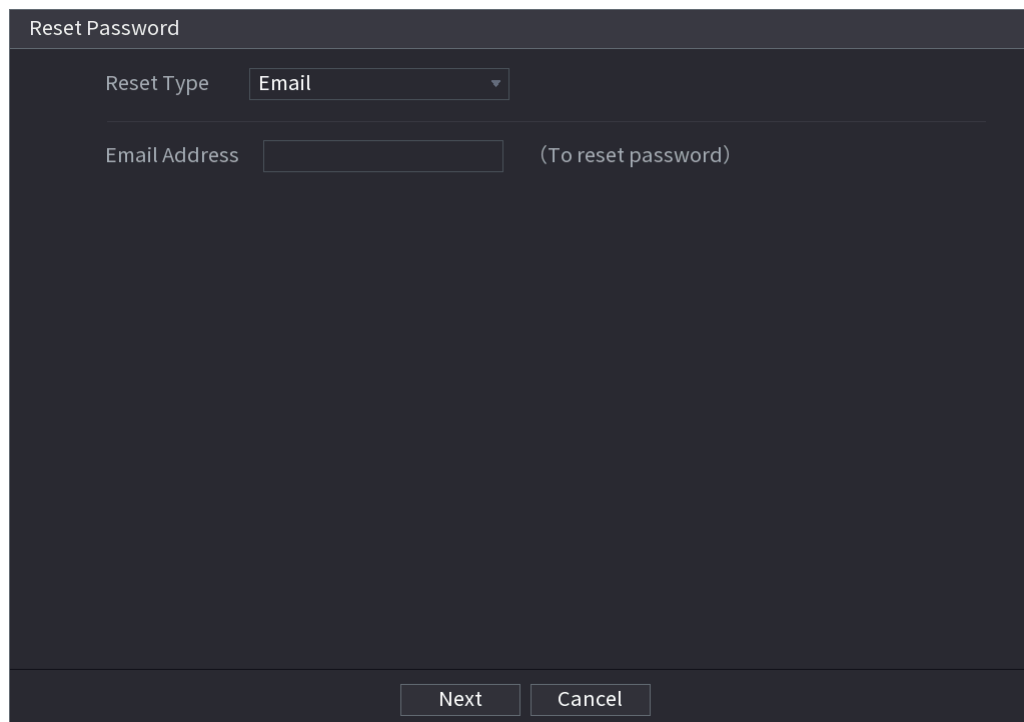


Figure 4-5 Reset password (2)



Step 2 Click **OK**.

The password resetting interface is displayed. See Figure 4-6.



After clicking OK, we will collect your personal information such as cell phone number, MAC address and device serial number. The collected information is used for verifying device legality and sending security code. Read the notice carefully and confirm if you agree with the collection or not.

Figure 4-6 Reset password (3)

Reset Password

Reset Type: Email

SN:

Scan the QR code on the actual interface

Note(For admin only):

Option 1. Please download EasyViewer and then from More-Reset Device Password, scan the left QR code.

Option 2. Please use an APP to scan the left QR code to get encryption strings. And then send the strings to support_gpwd@htmicrochip.com.

The security code will be delivered to 1***@qq.com.

Security code

Next Cancel

Step 3 Reset login password.

- Email

In Figure 4-6, follow the prompts on the interface to scan the QR code, and then enter the security code you get via the assigned email.



- For the same QR code, you can scan max twice to get two security codes. Refresh the QR code if you want to get security code again.
- The security code in your email is only valid for 24 hours.
- Security questions

In Figure 4-6, in the **Reset Type** drop-down list, select security question. The security question interface is displayed. See Figure 4-7. Enter the preset correct answers in the text boxes.

Error! Use the Home tab to apply 标题 1, I1, H1, Title1, Normal + Font: Helvetica, Bold, Space Before 12 pt, Not Bold, Heading

One, h1, Head1, Head, 1, Numbered, nu, Level 1 Head, 1st level, Section Head, Sec1, h11, 1st level1, h12, 1st level2, h13, 1st level3, h14, 1st level4, h15, 1st level 15

Figure 4-7 Reset password (4)

Reset Password

Reset Type: Security Questions

Question 1: What is your favorite children's book?
Answer:

Question 2: What was the first name of your first boss?
Answer:

Question 3: What is the name of your favorite fruit?
Answer:

Next Cancel

Step 4 Click **Next**.

The interface to set new password is displayed. See Figure 4-8.

Figure 4-8 Reset password (5)

Reset Password

Reset password of (admin)

New 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:

Save Cancel

Step 5 Enter the new password and confirm it.



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 6 Click **OK** to complete the settings.

Error! Use the Home tab to apply 标题 1, I1, H1, Title1, Normal + Font:

Helvetica, Bold, Space Before 12 pt, Not Bold, Heading

One, h1, Head1, Head, 1, Numbered, nu, Level 1 Head, 1st level, Section

Head, Sec1, h11, 1st level1, h12, 1st level2, h13, 1st level3, h14, 1st level4, h15, 1st leve 16

4.4 Startup Wizard



After completing all items on the startup wizard, the startup wizard automatically hides when booting up the Device next time.

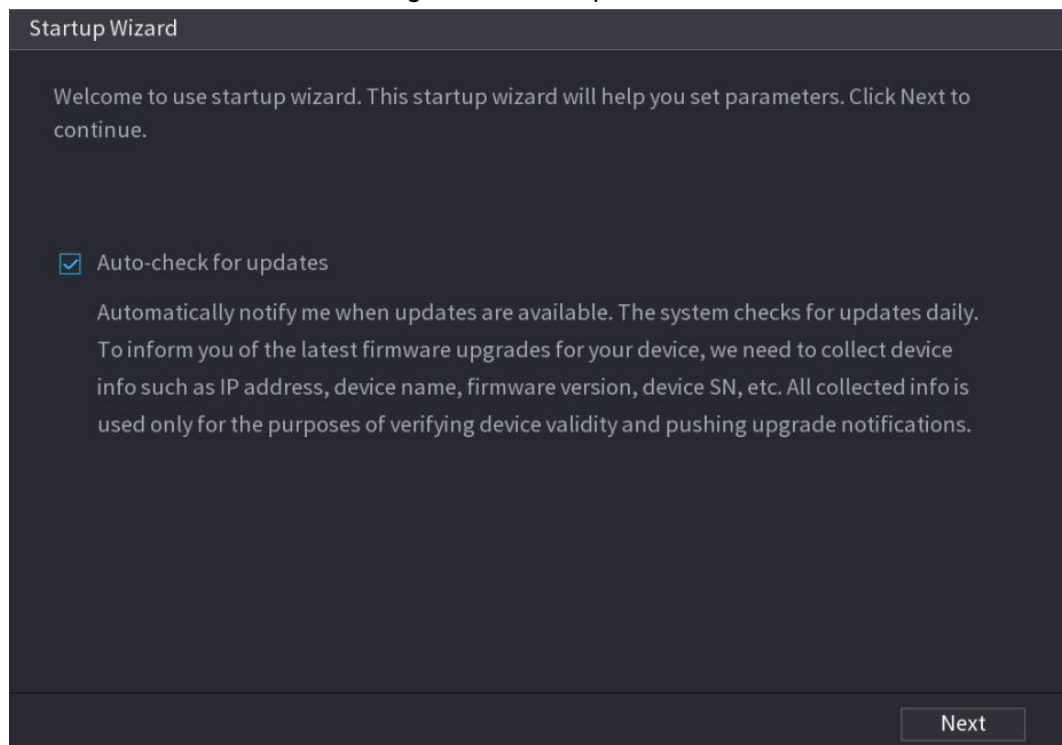
After you successfully initialize the Device, the **Startup Wizard** is displayed. See Figure 4-9. Click **Next**, log in the Device, and then you can enter the startup wizard to configure the Device quickly. For details, see *User's Manual*.

- Selecting the check box of **Auto-check for updates**, the Device automatically checks for new application every day.



After auto-check for updates is enabled, in order to inform you of the latest firmware upgrades, we will collect your personal information such as IP address, device name, firmware version and device SN. The collected information is used for verifying device legality and pushing upgrade notice.

Figure 4-9 Startup wizard



4.5 Registration

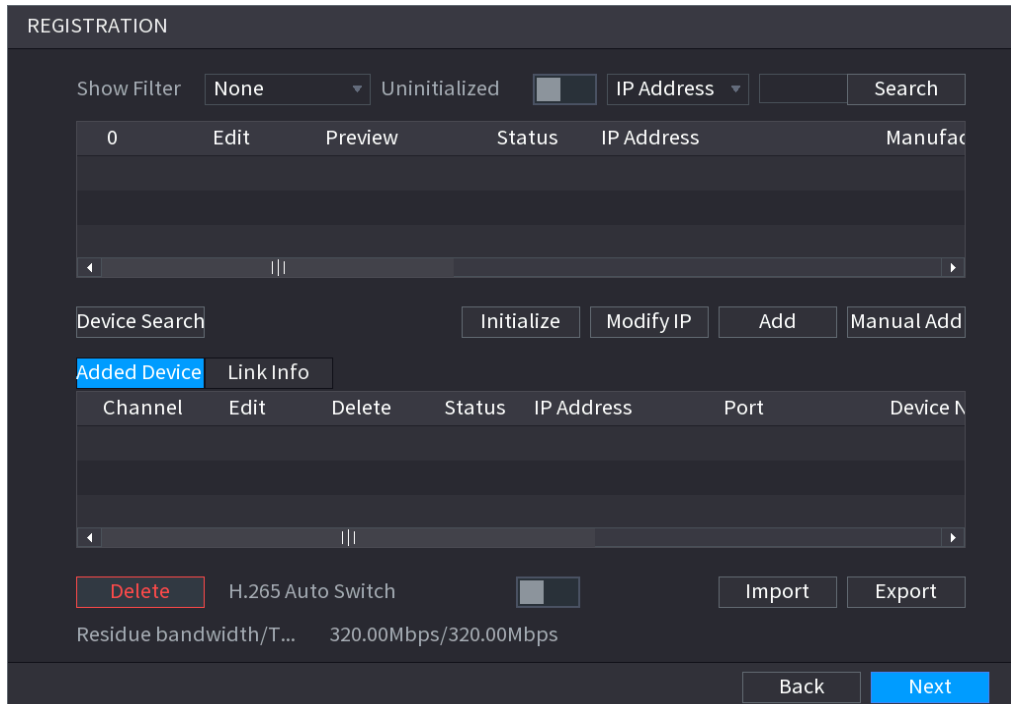
Select **Main Menu > CAMERA > Registration**. The **Registration** interface is displayed. See Figure 4-10.

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 4-10 Registration



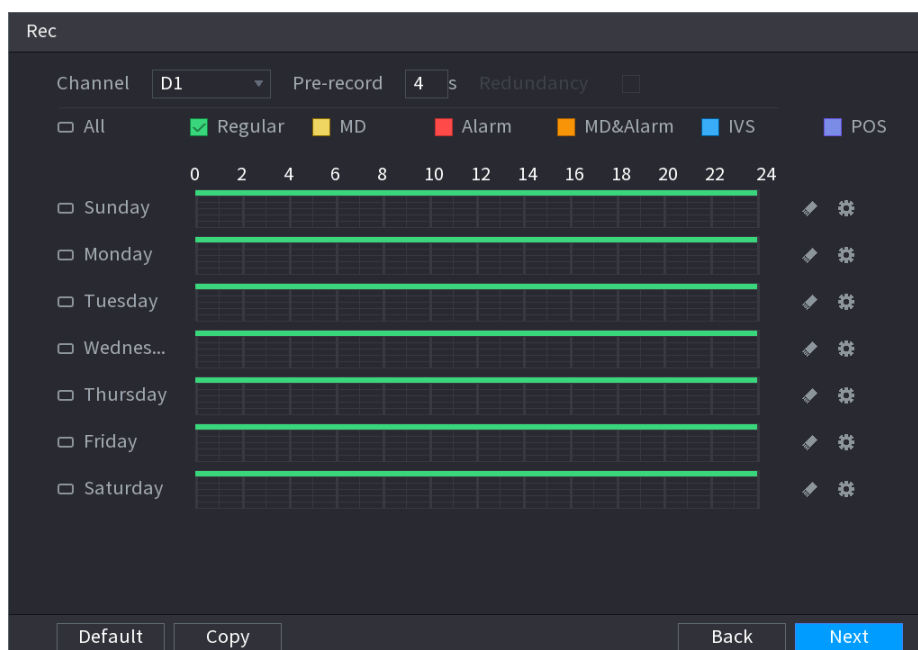
4.6 Schedule

All channels are 24-hour recording continuously by factory default. You can customize the record period and record type.

Step 1 Select **Main Menu > STORAGE > SCHEDULE > Rec.**

The **Rec** interface is displayed. See Figure 4-11.

Figure 4-11 Schedule



Error! Use the Home tab to apply 标题 1,I1,H1,Title1,Normal + Font:

Helvetica,Bold,Space Before 12 pt,Not Bold,Heading


One,h1,Head1,Head,1,Numbered,nu,Level 1 Head,1st level,Section

Head,Sec1,h11,1st level1,h12,1st level2,h13,1st level3,h14,1st level4,h15,1st leve 18

Step 2 Configure parameters such as channel, pre-record, ANR and record type.

- After setting one HDD to be redundant disk, select the **Redundancy** check box to realize video file backup. It is to save video files to different HDDs at the same time. Once one of the HDDs is damaged, there is still a backup file in another disk to ensure data reliability.
- Select the **ANR** check box to enable this function. When the IPC is out of network access, it keeps on recording and saves the records in the SD card. After the network is recovered, IPC transmits the records during the network outage back to the NVR device to ensure record integrity.

Step 3 Set the schedule period. It includes drawing and editing.

- Drawing: Press and hold down the left button of the mouse and drag the mouse in the time figure to draw the period.
- Editing: Click  to configure the period and then click **OK**.

Step 4 Click **Apply** or **OK** to save the settings.



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*.

4.7 Instant Playback








Move the mouse to the top center of the current channel preview interface and you can see the control bar. See Figure 4-12. Click  in the control bar and the system starts to reply the records 5 minutes to 60 minutes ago in the current channel.

Figure 4-12 Control bar



For icon description on the control bar, see Table 4-3.

Table 4-3 Control bar icon description

No.	Icon	Description
1		Instant playback
2		Digital zoom
3		Instant backup
4		Manual snapshot
5		Bidirectional talk
6		Switch bit streams

Error! Use the Home tab to apply 标题 1, I1, H1, Title1, Normal + Font:

Helvetica, Bold, Space Before 12 pt, Not Bold, Heading One, h1, Head1, Head, 1, Numbered, nu, Level 1 Head, 1st level, Section Head, Sec1, h11, 1st level1, h12, 1st level2, h13, 1st level3, h14, 1st level4, h15, 1st level5 20

5 Web Operations

You can log in to the web interface of the Device by browsers such as Safari, Firefox and Chrome.

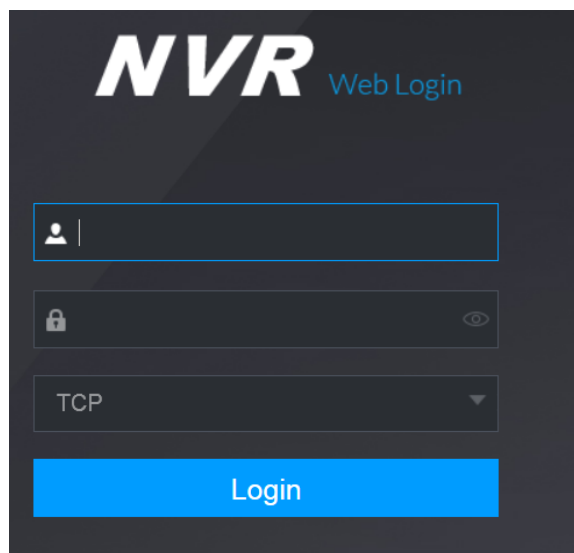


- Slight difference might be found on the interfaces of different models. Following figures are for reference only. The actual product shall prevail.
- Use ChromeApp to log in the web if the Chrome version is 45 or higher. Go to the Chrome online store to download the ChromeApp installation package.
- Before logging in to the web, make sure that the network connection between PC and the Device is ready.

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.

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 to the web for the first time, install the control according to system prompts.
- When you want to upgrade the control, delete the original control first. See the following two ways to delete the control:

Error! Use the Home tab to apply 标题 1, I1, H1, Title1, Normal + Font: Helvetica, Bold, Space Before 12 pt, Not Bold, Heading

One, h1, Head1, Head, 1, Numbered, nu, Level 1 Head, 1st level, Section

Head, Sec1, h11, 1st level1, h12, 1st level2, h13, 1st level3, h14, 1st level4, h15, 1st leve 21

- ◇ Enter C:\Program Files\webrec\WEB30\WebPlugin, and run the uninstall tool **uninst.exe**. The system automatically deletes the control.
- ◇ Enter C:\Program Files\webrec and delete the **Single** folder.

Error! Use the Home tab to apply 标题 1, l1, H1, Title1, Normal + Font:

Helvetica, Bold, Space Before 12 pt, Not Bold, Heading
One, h1, Head1, Head, 1, Numbered, nu, Level 1 Head, 1st level, Section
Head, Sec1, h11, 1st level1, h12, 1st level2, h13, 1st level3, h14, 1st level4, h15, 1st leve 22

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.