Network Video Recorder
Quick Start Guide

V1.0.1

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.

Table of Contents

General

This quick start guide (hereinafter referred to be "the Guide") introduces the functions and operations of the Network Video Recorder (NVR) devices (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.
⚡ ELECTRICITY	Indicates dangerous high voltage. Take care to avoid coming into contact with electricity.
☀ LASER BEAM	Indicates a laser radiation hazard. Take care to avoid exposure to a laser beam.
ESD	Electrostatic Sensitive Devices. Indicates a device that is sensitive to electrostatic discharge.
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.

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 include 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 govern.

- We are not liable for any loss caused by the operations that do not comply with the Guide.

- 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

- 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 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.
- 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.

1 Hardware Installation and Connection

1.1 Preparation Work

DANGER

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

SN	Name		Contents
1	Whole package	Appearance	There is any visible damage or not.
		Package	There is any accidental clash during transportation or not.
2	Front panel and rear panel	The model on the front panel	Check the model with the purchase order.
		The label on the rear panel.	It is neat and clean or not. 📖 **Note** Do not tear off, or discard the label. Usually we need you to represent the serial number when we provide the service after sales.
3	Case	Appearance	There is any visible damage or not.
		Check the data cable, power cable, fan cable, main board and etc.	Check the connection is secure or not. 📖 **Note** Contact your local retailer or our service engineer if the connection is loosen.

1.2 HDD Installation

DANGER

Shut down the device and then unplug the power cable before you open the case to replace the HDD!
All figures listed below for reference only!

For the first time to install, please check the HDD has been installed or not.

Refer to the user manual for HDD space information and recommended HDD brand. Please use HDD of 7200rpm or higher. **Usually we do not recommend the PC HDD.**

①Use the screwdriver to loose the screws of the rear panel and then remove the front cover.

②Put the HDD to the HDD bracket in the chassis and then line up the four screws to the four holes in the HDD. Use the screwdriver to fix the screws firmly to secure HDD on the HDD bracket

③Connect to the HDD data cable to the main board and the HDD port respectively. Loosen the power cable of the chassis and connect another end of the power cable to the HDD port.

④After connect the cable, put the front cover back to the device and then fix screws of the rear panel.

2 Front Panel/Rear Panel

Note

- Follow figures listed here for reference only. Please refer to the actual product for detailed information.
- Refer to the user's manual for detailed information.

The front panel is shown as in Figure 2-1.
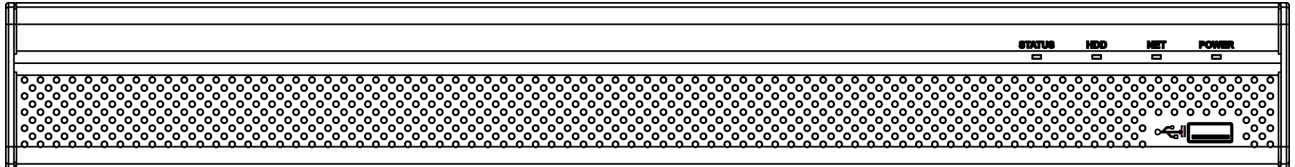
Figure 2-1

Please refer to the following sheet for front panel button information.

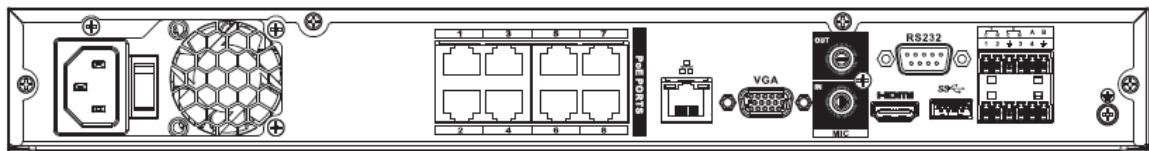| Icon	Name	Function
STATUS	Status indicator light	The blue light is on when the device is malfunction.
HDD	HDD status indicator light	The blue light is on when the HDD is malfunction.
NET	Network status indicator light	The blue light is on when the network connection is abnormal.
POWER	Power status indicator light	The blue light is on when the power connection is OK.
⟵	USB2.0 port	Connect to peripheral USB 2.0 storage device, mouse, burner and etc.

The rear panel is shown as in Figure 2-2.

Figure 2-2

Please refer to the following sheet for detailed information.

Icon	Port Name	Function
	Network port	10M/100M/1000Mbps self-adaptive Ethernet port. Connect to the network cable.
HDMI	High Definition Media Interface	High definition audio and video signal output port. It transmits uncompressed high definition video and multiple-channel data to the HDMI port of the display device. HDMI version is 1.4.
SS⟵	USB3.0 port	USB3.0 port. Connect to mouse, USB storage device, USB burner and etc.
RS-232	RS-232 debug COM.	It is for general COM debug to configure IP address or transfer transparent COM data.

Icon	Port Name	Function
VGA	VGA video output port	VGA video output port. Output analog video signal. It can connect to the monitor to view analog video.
MIC IN	Audio input port	Bidirectional talk input port. It is to receive the analog audio signal output from the devices such as microphone, pickup.
MIC OUT	Audio output port	Audio output port. It is to output the analog audio signal to the devices such as the sound box. ● Bidirectional talk output. ● Audio output on 1-window video monitor. ● Audio output on 1-window video playback.
1～8	Alarm input port 1～8	● There are two groups. The first group is from port 1 to port 4; the second group is from port 5 to port 8. They are to receive the signal from the external alarm source. There are two types; NO (normal open)/NC (normal close). ● When your alarm input device is using external power, please make sure the device and the NVR have the same ground.
⏚	GND	Alarm input ground port.
NO1～NO3	Alarm output port 1～3	● 3 groups of alarm output ports. (Group 1：port NO1 ～ C1,Group 2:port NO2 ～ C2,Group 3:port NO3 ～ C3）).Output alarm signal to the alarm device. Please make sure there is power to the external alarm device. ● NO：Normal open alarm output port. ● C：Alarm output public end.
C1～C3		
A	RS-485 communication port	RS485_A port. It is the cable A. You can connect to the control devices such as speed dome PTZ.
B		RS485_B.It is the cable B. You can connect to the control devices such as speed dome PTZ.
DC 12V ⏚Ⓒ⏚	Power input port	Input DC 12V/4A.
Power switch	/	Power on/off button.
PoE PORTS	/	Bult-in Switch. Support PoE. It provides power to the network camera. The 8 PoE series product supports total 48V 120W.

3 Connection

📖**Note**

- The following figure for reference only. Please refer to the actual product for detailed information.
- Refer to the user's manual for detailed information.
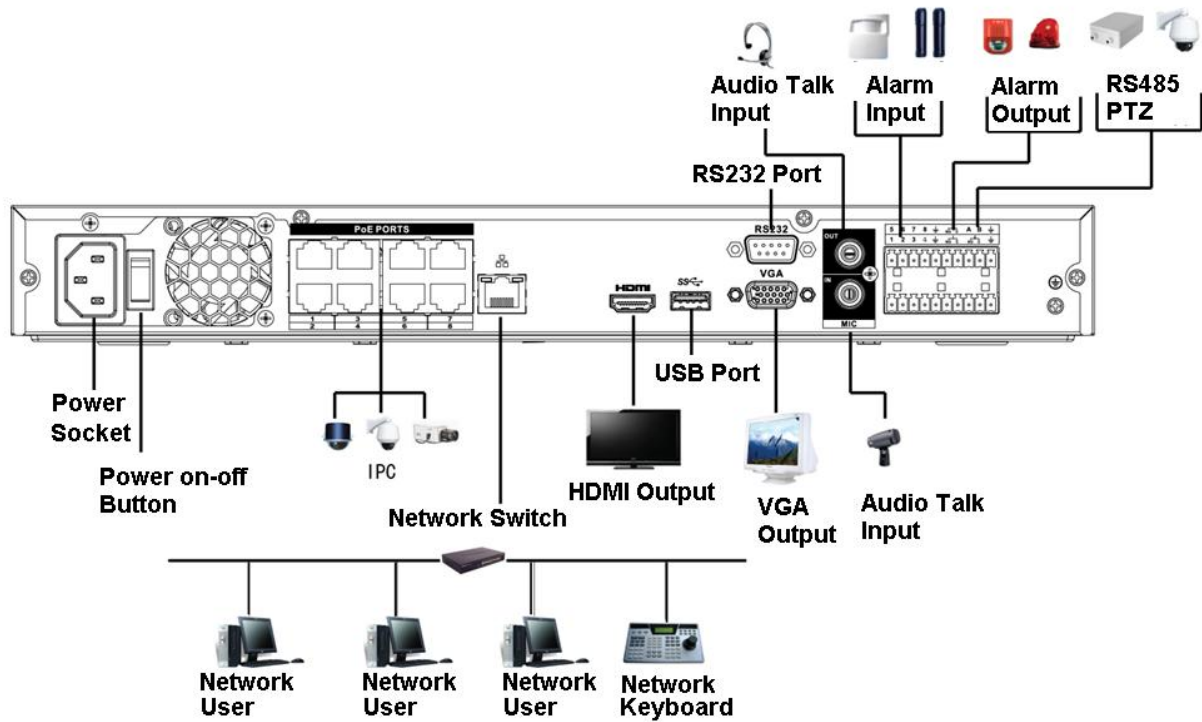
Device cable connection is shown as in Figure 3-1.

Figure 3-1

4 GUI Operation

4.1 Boot up

⚠ **DANGER**

Before the boot up, please make sure:

- **For device security, please connect the NVR to the power adapter first and then connect the device to the power socket.**
- **The rated input voltage matches the device power on-off button. Please make sure the power wire connection is OK. Then click the power on-off button.**
- **Always use the stable current, if necessary UPS is a best alternative measure.**

Please follow the steps listed below to boot up the device.

Step 1 Connect the device to the monitor and then connect a mouse.

Step 2 Connect power cable.

Step 3 Click the power button at the front or rear panel and then boot up the device. After device booted up, the system is in multiple-channel display mode by default.

4.2 Device Initialization

If it is your first time to use the device, please set a login password of **admin** (system default user).

🕮 **Note**

For your device safety, please keep your login password of **admin** well after the initialization steps, and change the password regularly.

Please follow the steps listed below.

Step 1 Boot up NVR.

Device displays device initialization interface. See Figure 4-1.
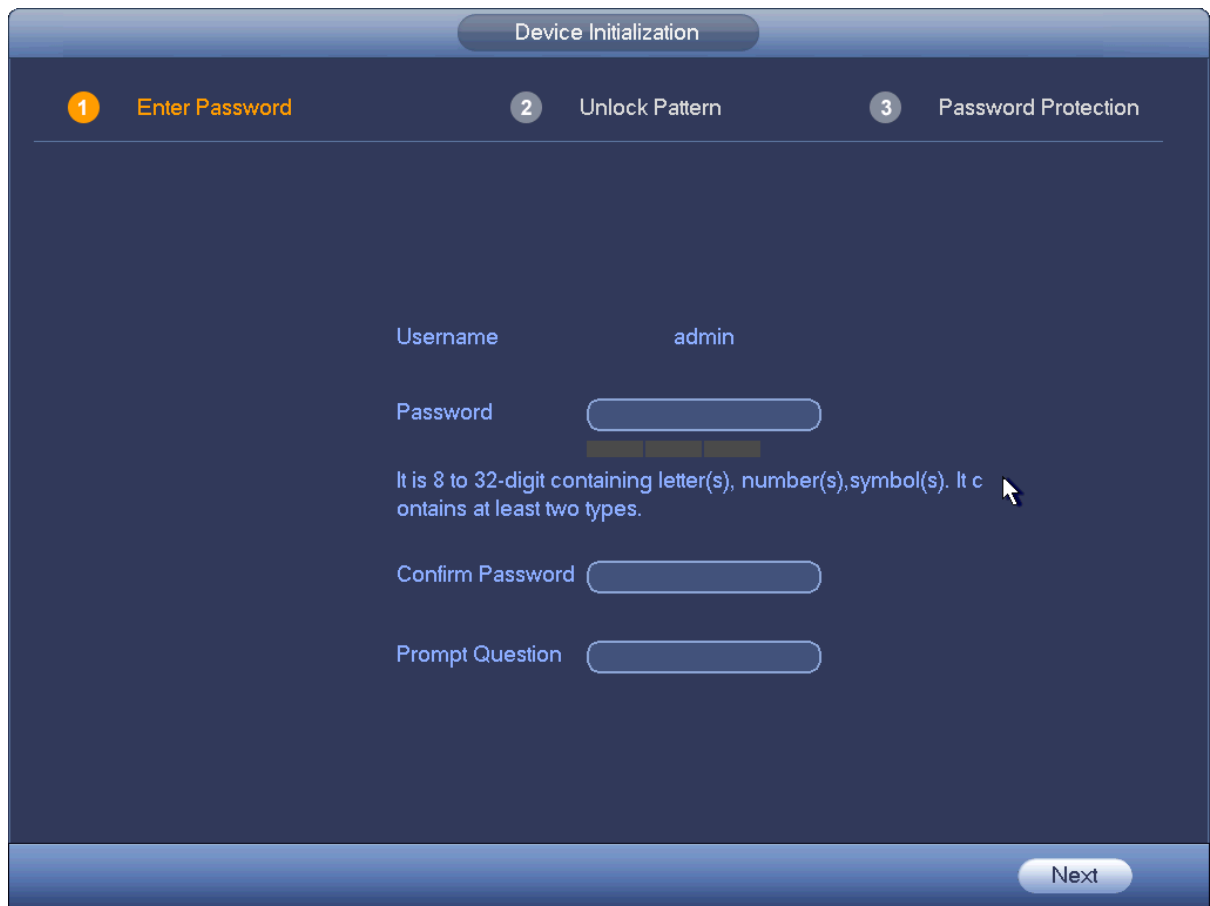
Figure 4-1

Step 2 Set login password of **admin**.
- User name: The default user name is **admin**.
- Password/confirm password: The password ranges from 8 to 32 digitals. It can contain letters, numbers and special characters (excluding "'","""","':","':","&") . The password shall contain at least two categories. Usually we recommend the strong password.

- Prompt question: If you set the prompt question here. On the login interface, click [icon], device can display the corresponding prompt question for you to remind the password.

⚠ **WARNING**

STRONG PASSWORD RECOMMENDED-For your device own safety, please create a strong password of your own choosing. We also recommend you change your password periodically especially in the high security system.

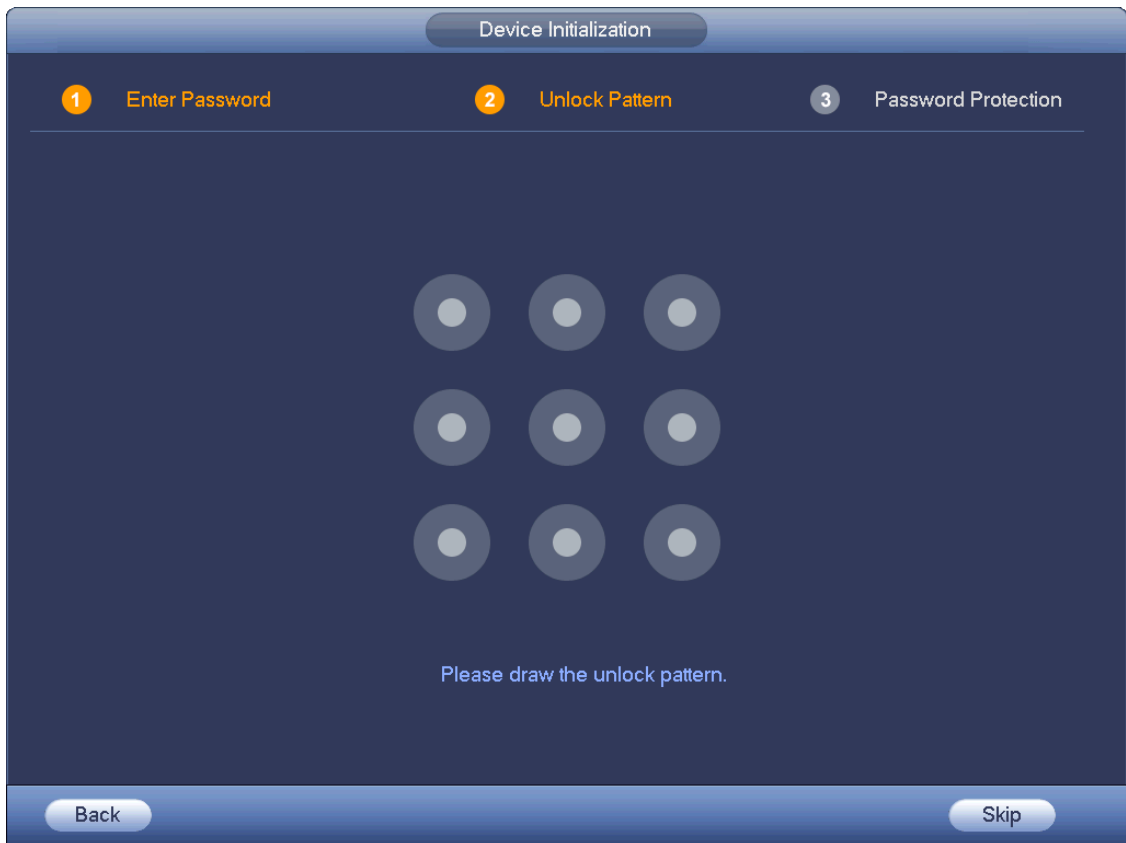Step 3 Click Next, device goes to the following interface. See Figure 4-2.

7

Figure 4-2

Step 4 Set unlock pattern.

After set unlock pattern, device goes to password protection interrface. See Figure 4-3.

📖 **Note**

- Device adopts unlock pattern to login by default if you have set pattern here. If there is no unlock pattern, please input the password to login.
- Click Skip if there is no need to set unlock pattern.

Figure 4-3

Step 5 Set security questions.

📖 **Note**

- After setting the security questions here, you can use the email you input here or answer the security questions to reset **admin** password. Refer to user's manual for detailed information.
- Cancel the email or security questions box and then click Next button to skip this step.

- Email: Input an email address for reset password purpose. In case you forgot password in the future, input the security code you got on the assigned email to reset the password of admin. If you have not input email here or you need to update the email information, please go to the main menu->Setting->System->Account to set. Refer to user's manual for detailed information.
- Security question: Set security questions and corresponding answers. Properly answer the questions to reset admin password. In case you have not input security question here or you need to update the security question information, please go to the main menu->Setting->System->Account->Security question to set. Refer to user's manual for detailed information.

📖 **Note**

If you want to reset password by answering security questions, please go to the local menu interface.

Step 6 Click OK to complete the device initialization setup.

Device goes to startup wizard interface. Refer to user's manual for Startup wizard detailed information.

4.3 Reset Password

If you forgot **admin** password, you can reset the password by email or by answering the security questions (local menu only).

Please follow the steps listed below.

Step 1 Go to the device login interface. See Figure 4-4 or Figure 4-5. .

- If you have set unlock pattern, device displays unlock pattern login interface. See Figure 4-4. Click "Forgot unlock pattern", device goes to Figure 4-5.
- If you have not set unlock pattern, device displays password interface. See Figure 4-5.

📖 **Note**

Click Switch user button or click the user name and then select a user from the dropdown list, you can login via other account.
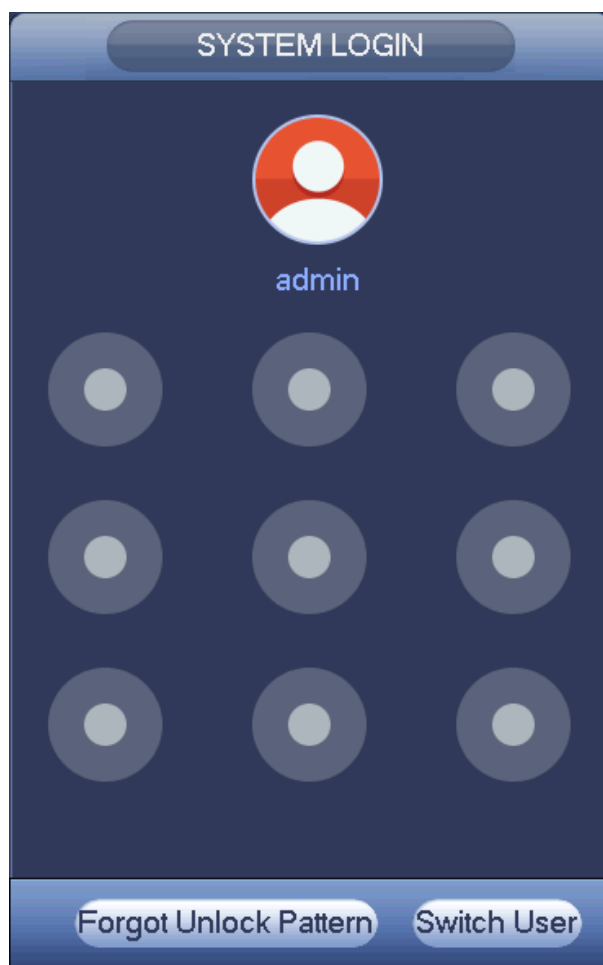
Figure 4-4

Figure 4-5

Step 2 Click .

- If you have not input email address information when you are initializing the device, the interface is shown as in Figure 4-6. Please input an email address and then click Next button, devices goes to Figure 4-7.
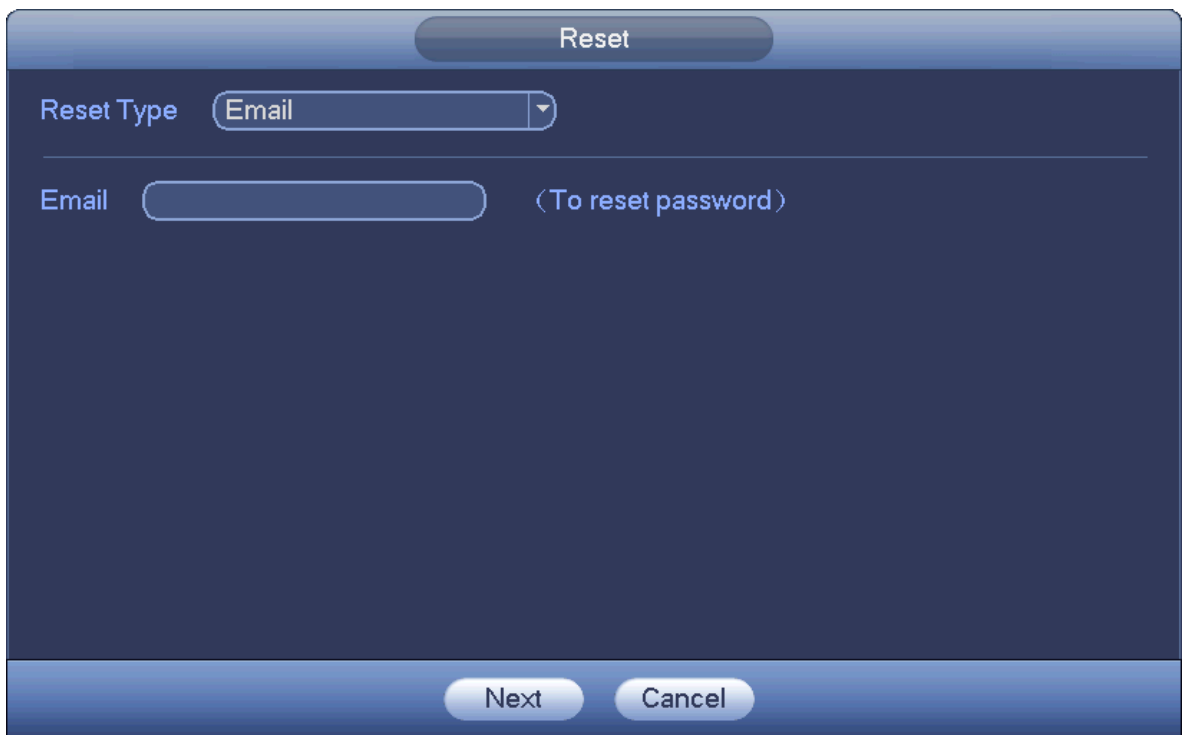- If you have input email when you are initializing the device, device goes to Figure 4-7.

Figure 4-6

Figure 4-7

Step 3 Reset login password.

There are two ways to reset the password: Scan QR code and reset by email/security questions.

- **Email**

In Figure 4-7, follow the prompts on the interface to scan the QR code, and then input the security code you get via the assigned email.

 Warning

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

- **Security questions**

In Figure 4-6., select security question from the drop down list. Device displays security question interface. See Figure 4-8. Please input the correct answers here.
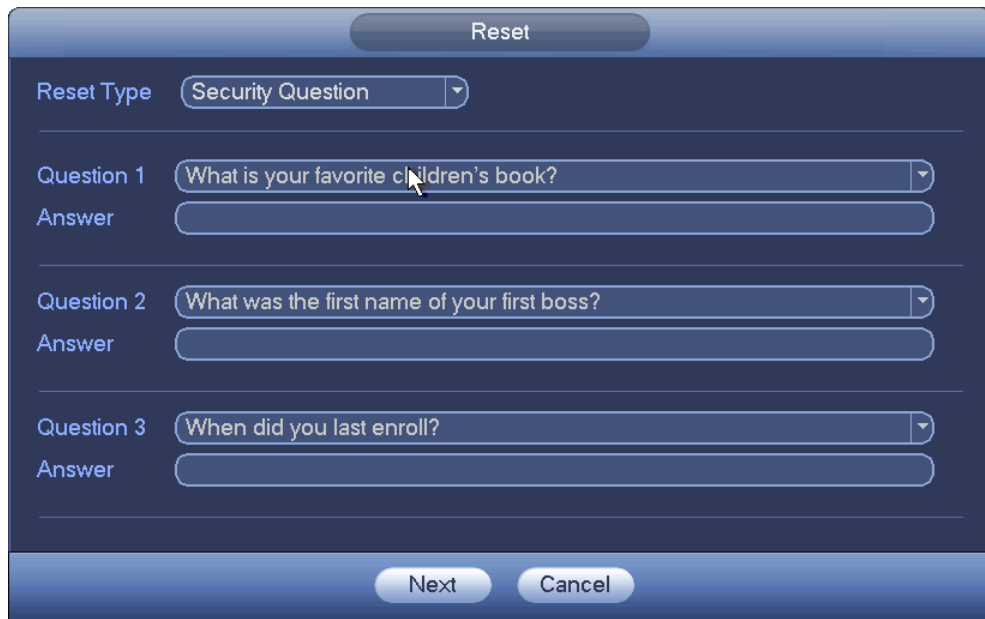
Figure 4-8

Step 4 Click Next button.

Device displays reset password interface. See Figure 4-9.
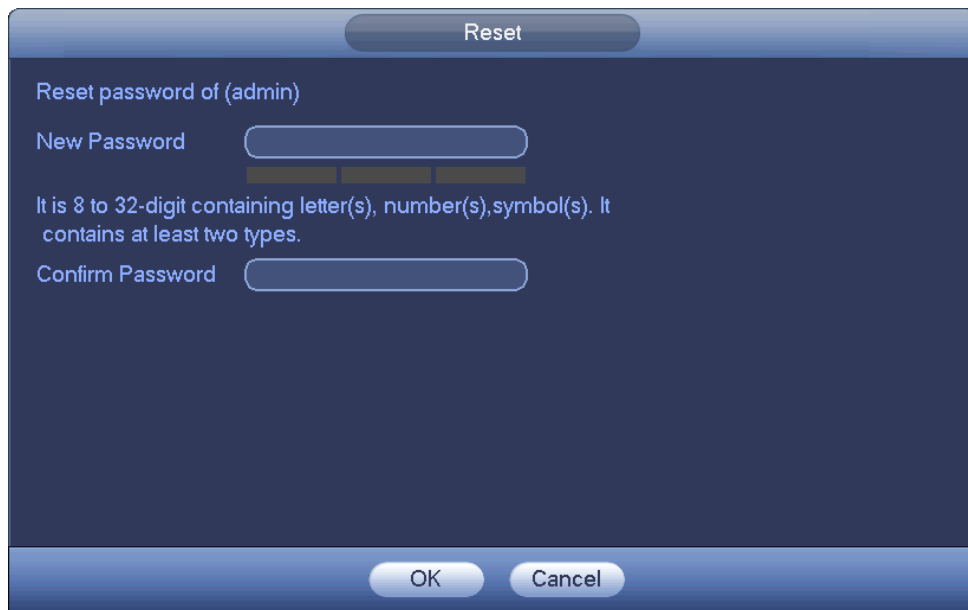
Figure 4-9

Step 5 Input new password and then confirm.

⚠️ **WARNING**

STRONG PASSWORD RECOMMENDED-For your device own safety, please create a strong password of your own choosing. The password shall be at least 8-digit containing at least two types of the following categories: letters, numbers and symbols. We also recommend you change your password periodically especially in the high security system.

Step 6 Click OK button to complete the setup.

4.4 Startup Wizard

After you successfully initialize the device, it goes to startup wizard. Here you can quickly configure your device. It includes smart add, general setup, basic network setup, camera registration, P2P, and schedule interface.

Please follow the steps listed below.

Step 1 Boot up the device.

Device goes to startup wizard if you have successfully initialized the device. See Figure 4-10.

📖 **Note**

- Check the Startup button here, device goes to startup wizard again when it boots up the next time. Cancel the Startup button, device goes to the login interface directly when it boots up the next time.
- Check the box to enable smart add function, and then click the Next button. Device now adds the camera. Refer to chapter 4.5 Smart Add for detailed information. Please note this function is for some series product only.
- Click the Cancel button, device goes to login interface. Device is in multiple-window preview mode by default. Refer to user's manual for detailed information.
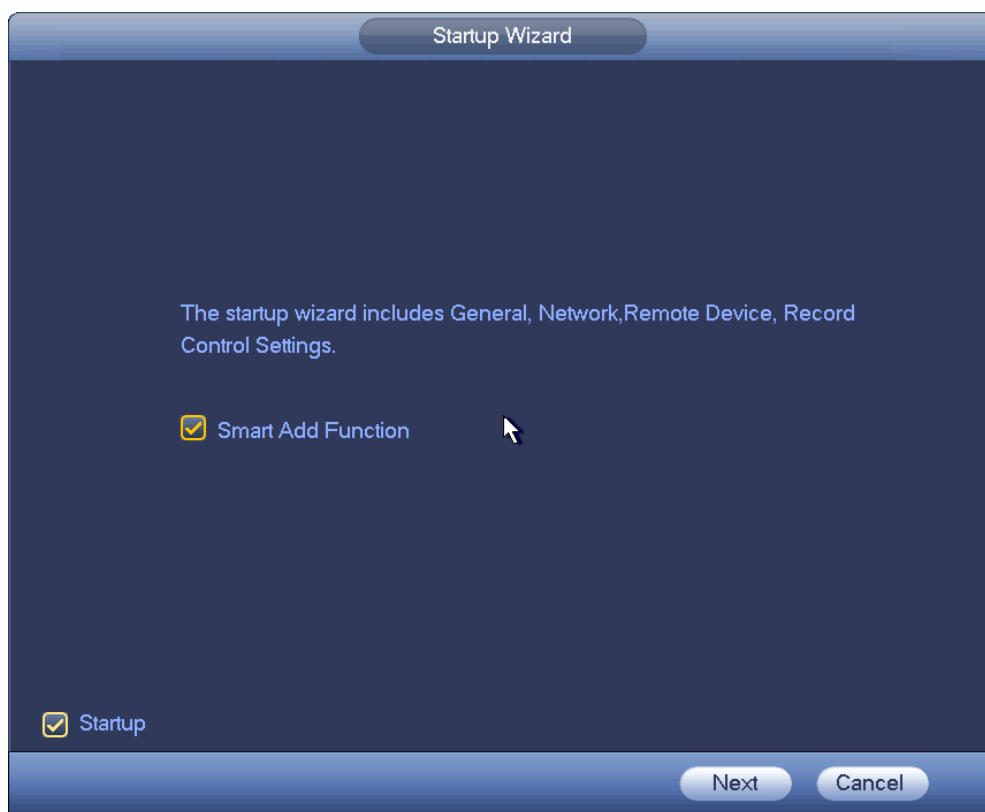
Figure 4-10

Step 2 Click Next button.

- Device displays unlock pattern login interface if you have set unlock pattern. See Figure 4-11. Click forgot pattern, device goes to password login interface. See
- If you have not set unlock pattern, device displays password login interface. See Figure 4-12.
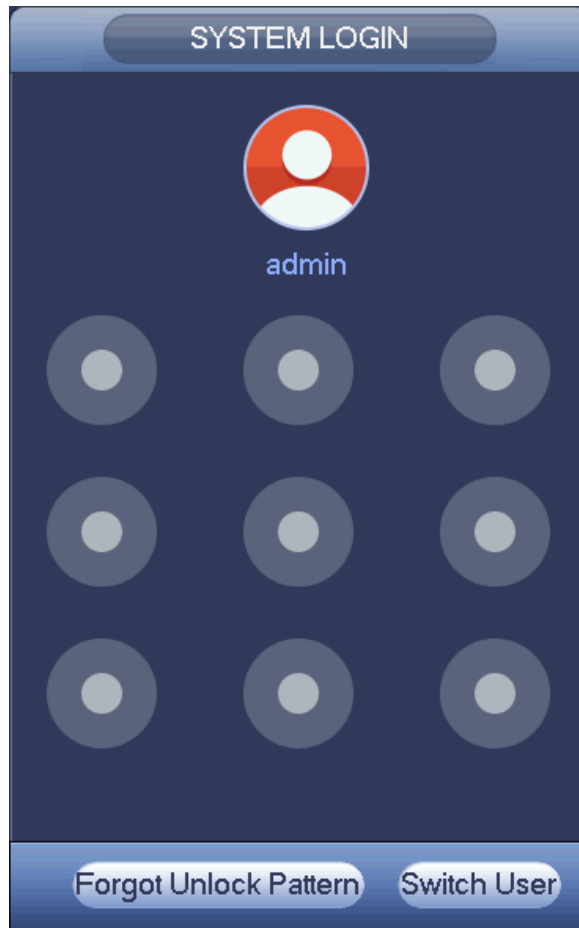
Figure 4-11

Figure 4-12

Step 3 Draw unlock pattern or input login password.

Warning

- The account becomes locked after five times login failure by default. After each login failure, you can see the remaining login attempts.
- Refer to user's manual (Main menu->Setting->Event->Abnormality->User) to set login attempt times (1-10) and account lock time (1 to 30 minutes).

Step 4 Click OK button.

Device goes to startup wizard, now you can quickly configure the device. Refer to the user's manual for detailed information.

4.5 Smart Add

When the network camera(s) and the device are in the same router or switch, you can use smart add function to add network cameras to the device. See Figure 4-13.

There are two ways to go to the smart add interface. Refer to the user's manual for detailed information.

- From the startup wizard, click Smart add button and then click Next.
- On the preview interface, right click mouse and then select Smart add.
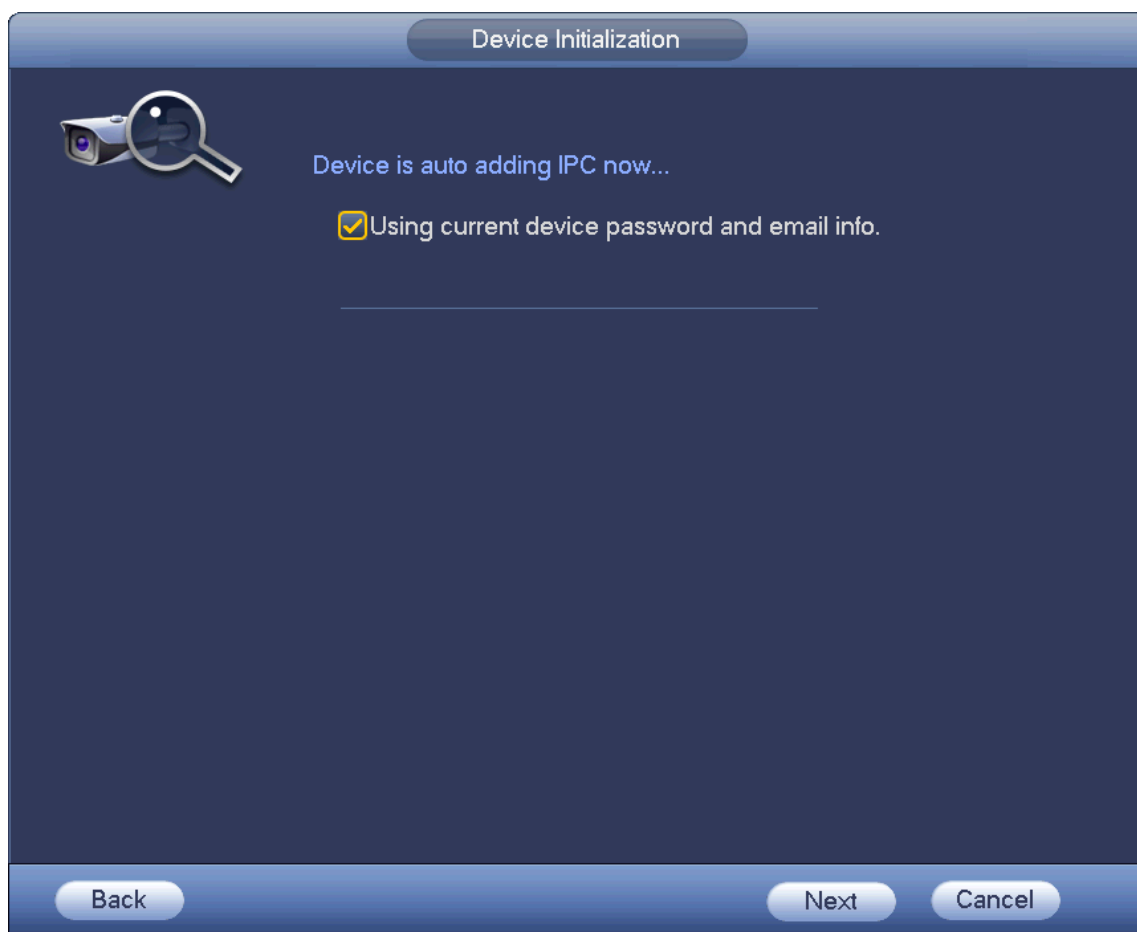
Figure 4-13

4.6 Registration

Here you can add network camera, change network camera IP address and etc.

Step 1 There are two ways to go to Registration interface. See Figure 4-14.

- From main menu->Setting->Camera->Registration, you can go to the registration interface.
- On the preview interface, right click mouse and then select Registration.

Figure 4-14

Step 2 Add network camera.

● Device search: Click the button; you can search all network cameras in the same network segment. See Figure 4-15. Double click a camera or check the camera box and then click Add button, you can add a device to the list.

📖 **Note**

●The device in the added device list is not shown in the search result column.

●In (IP Address ▾), select IP address or the MAC address from the dropdown list and then input the corresponding information, click Search button to view the results.

●Status in the search list can display the remote device has been initialized or not. That is to say, the remote device has set the password of **admin**. 📹 means the remote device has initialized. Cherck Uninitialized box to search the unitialized devices. Refer to the user's manual for detailed informaiton.

Figure 4-15

● Manual Add: Click Manual Add button, you can set the corresponding network camera information and then select the channel you want to add. See Figure 4-16.
   ✧ Manufacturer: Please select from the dropdown list.

📖**Note**

Different series products may support different manufactures, please refer to the actual product.
   ✧ CAM name: Set the channel name and then click Save button.

📖**Note**

Make sure you have successfully added the remote device and the connection status is 🟢 if you want to change channel name. .
   ✧ IP address: Input remote device IP address.
   ✧ RTSP port: Input RTSP port of the remote device. The default setup is 554.

📖**Note**

Skip this item if the manufacture is private or customize.

✧ HTTP port: Input HTTP port of the remote device. The default setup is 80.

📖**Note**

Skip this item if the manufacture is private or customize.
 ✧ TCP port: Input TCP port of the remote device. The default setup is 37777.
 ✧ User name/password: The user name and password to login the remote device.
 ✧ Channel No.: Input channel amount or click the Connect button to get the channel amount of the remote device.

📖**Note**

We recommend click Connect button to get remote device channel amount, the manual add operation may result in failure if the input channel amount is not right.
 ✧ Remote channel No.: After getting the remote device channel amount, click Setup to select a channel.

📖**Note**

Click to select one or more remote channel numbers here.
 ✧ Channel: The local channel number you want to add. One channel name has corresponding one channel number.
 ✧ Decode buffer: There are three items: realtime,local,fluent.
 ✧ Service type: There are four items: auto/TCP/UDP/MULTICAST(ONVIF device only)

📖**Note**

 ✧ The default connection mode is TCP if the connection protocol is private.
 ✧ There are three items:TCP/UDP/MULTICAST if the connection protocol is ONVIF.
 ✧ There are two items: TCP/UDP if the connection protocol is from the third-party.

Figure 4-16

Step 3 Click OK to add the camera to the device.

📖 **Note**

Click ✏️ to change the remote device information. Click ❌ to delete remote device. .

4.7 Schedule

All channels are record continuously by default. You can set customized record period and record type.


Figure 4-17

Step 1 From main menu->Setting->Schedule->Record.
          Enter schedule interface. See Figure 4-18.

Figure 4-18

Step 2 Set parameters.

- Channel: Please select the channel number first. You can select "all" if you want to set for the whole channels.

✧ 🔗: Sync connection icon. Select icon ▢ of several dates, all checked items can be edited or together. Now the icon is shown as 🔗.

✧ ⬜: Click it to delete a record type from one period.

- Record Type: Please check the box to select corresponding record type. There are five types: Regular/MD (motion detect)/Alarm/MD&Alarm/IVS.
- Week day: There are eight options: ranges from Saturday to Sunday and all.
- Holiday: It is to set holiday setup. Please note you need to go to the General interface (Main Menu->Setting->System->General) to add holiday first. Otherwise you cannot see this item.
- Pre-record: System can pre-record the video before the event occurs into the file. The value ranges from 1 to 30 seconds depending on the bit stream.
- Redundancy: System supports redundancy backup function. It allows you backup recorded file in two disks. You can highlight Redundancy button to activate this function. Please note, before enable this function, please set at least one HDD as redundant. (Main menu->Setting->Storage->HDD Manager). Please note this function is null if there is only one HDD.
- ANR: It is to save video to the SD card of the network camera in case the network connection fails. The value ranges from 0s～43200s. After the network connection resumed,

21

the system can get the video from the SD card and there is no risk of record loss.

● Period setup: Click button ⚙ after one date or a holiday, you can see an interface shown as in Figure 4-19.There are five record types: regular, motion detection (MD), Alarm, MD & alarm and IVS.

Figure 4-19

Please following the steps listed below to draw the period manually.

　　a) Select a channel you want to set. See Figure 4-20.

Figure 4-20

　　b) Set record type. See Figure 4-21.

Figure 4-21

📖 **Note**

● When the record type is MD (motion detect), alarm, MD&Alarm, IVS, please enable the channel record function when corresponding alarm occurs. For example, when the alarm type is MD, from main menu->Setting->Event->Video Detect->Motion Detect, please select the record channel and enable record function. See Figure 4-22.
● When the record type is MD (motion detect), alarm, MD&Alarm, IVS, refer to user's manual to enable the corresponding record function first.
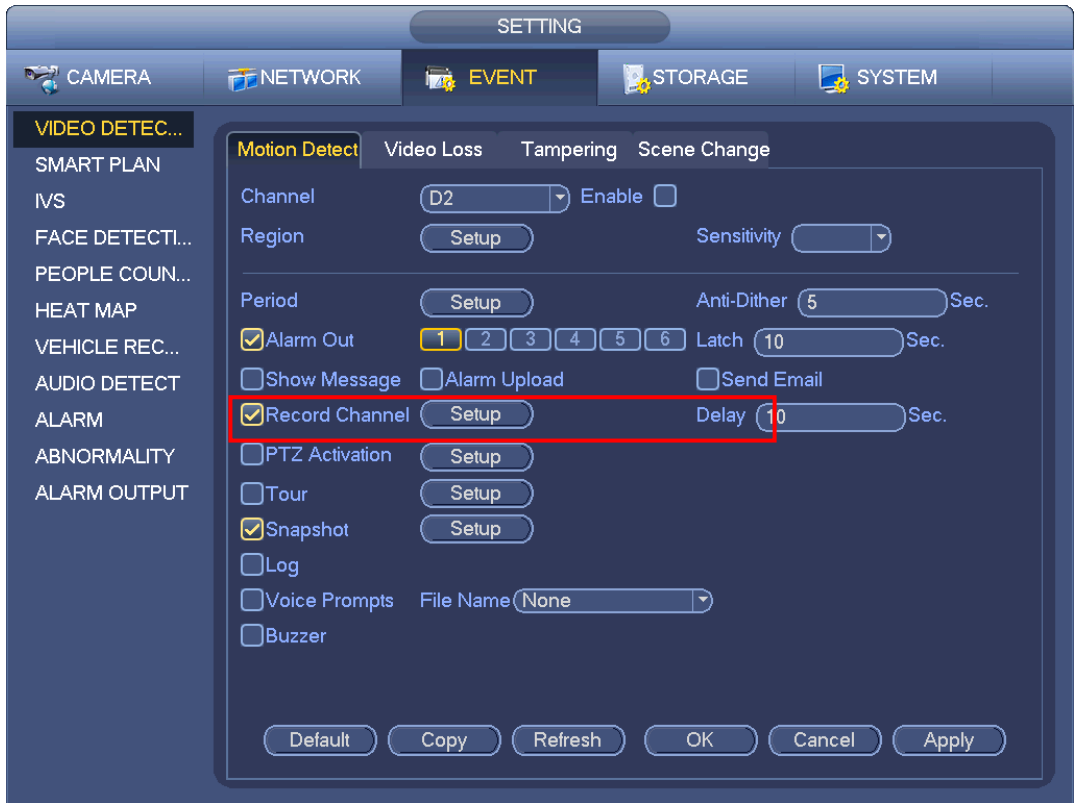
Figure 4-22

c) Please draw manually to set record period. There are six periods in one day. See Figure 4-23.

📖 **Note**

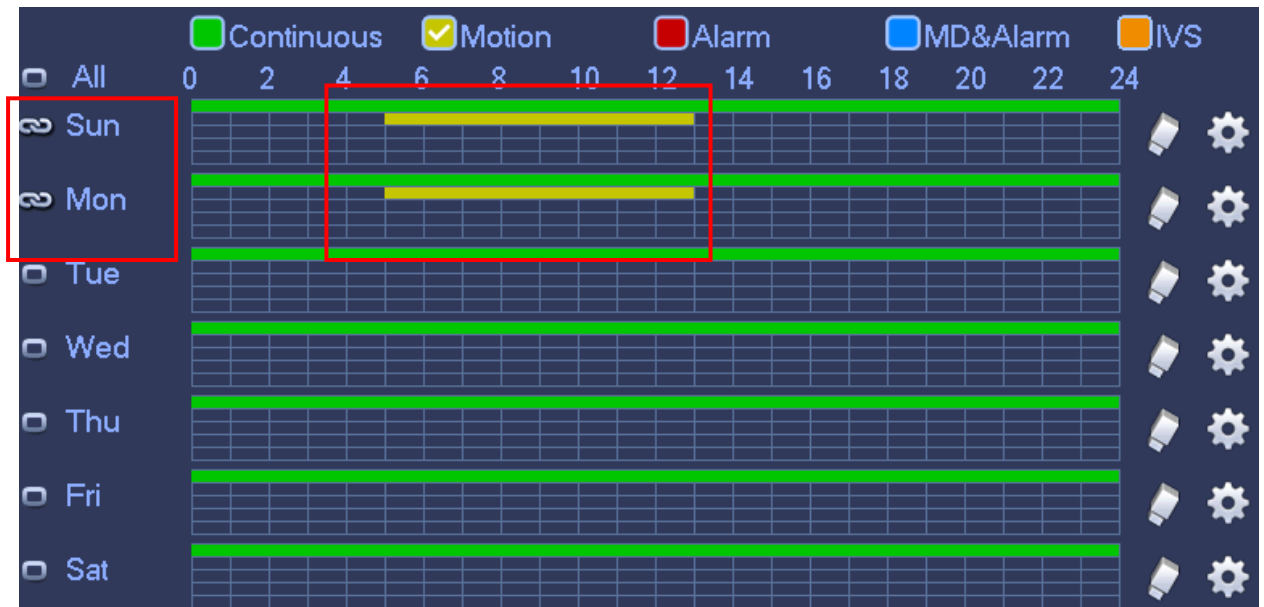If you have added a holiday, you can set the record period for the holiday.

Figure 4-23

Step 3 Click Apply button to save schedule record settings.

📖 **Note**

Please enable auto record function so that the record plan can become activated. Refer to user's manual Record control for detailed information.

4.8 Instant Playback

Move you mouse to the top center of the video of current channel, you can see system pops up the preview control interface. See Figure 4-24.

Click ![icon], device plays the record file previous 5 to 60 minutes of the current channel.

SN	Icon	Name
1		Instant playback
2		Digital zoom
3		Instant backup
4		Manual snapshot
5		Audio talk
6		Remote Device
7		Switch bit streams

Figure 4-24

5 Web Operation

If it is your first time to login the device, please initialize your device first. Refer to the user's manual for detailed information.

Device supports remote access, management via the PC.

📖 **Note**

- Slight difference may be found on user interface. Please refer to the actual product for detailed information.
- Device supports various browsers such as Safari, Chrome and etc.
- Use ChromeApp to login the WEB if the Chrome version is 45 or higher. Go to the Chrome online store to download the ChromeApp installation package.

5.1 Network Connection

Step 1 PC and NVR connection is OK.

Step 2 Set PC IP address, NVR IP address, subnet mask and gateway.

- Set the IP address of the same section for the PC and NVR. Input corresponding gateway and subnet mask if there are routers.)
- The device default IP address is 192.168.1.108.

Step 3 Check the PC and device connection is OK or not. Refer to the following two ways to check the network connection is OK or not. When the PC and device network connection is OK, login the WEB via the PC.

- On PC, use order ping ***.***.***.***(NVR IP address) to check connection is OK or not. Login Usually the TTL value is 255.
- Login the device local menu, from setting->Network->Network test and then input PC IP address. Check the connection is OK or not.

Step 4 Login the WEB. Refer to chapter 5.2 Login for detailed information.

5.2 Login

Step 1 Open the browser and input NVR address in the address column. Click Enter button. Enter login interface. See Figure 5-1.

Figure 5-1

Step 2 Input user name and password.

📖 **Note**

- Device default user name is **admin**. The password is that you set during initialization process. For your device safety, please change the admin password regularly and keep it well.
- In case you forgot password, click Forgot password to reset. Refer to the user's manual for detailed information.

Step 3 Click Login.

Enter preview interface. See Figure 5-2. Refer to the user's manual for detailed information.

📖 **Note**

- Click Install the plug-in to install if it is your first time to login the WEB.
- Before upgrade the new WEB version, there are two ways to delete the controls.
- Go to "C:\Program Files\webrec\WEB30\WebPlugin" and then run WEB uninstall tool such as "uninst.exe". System auto delete old controls.
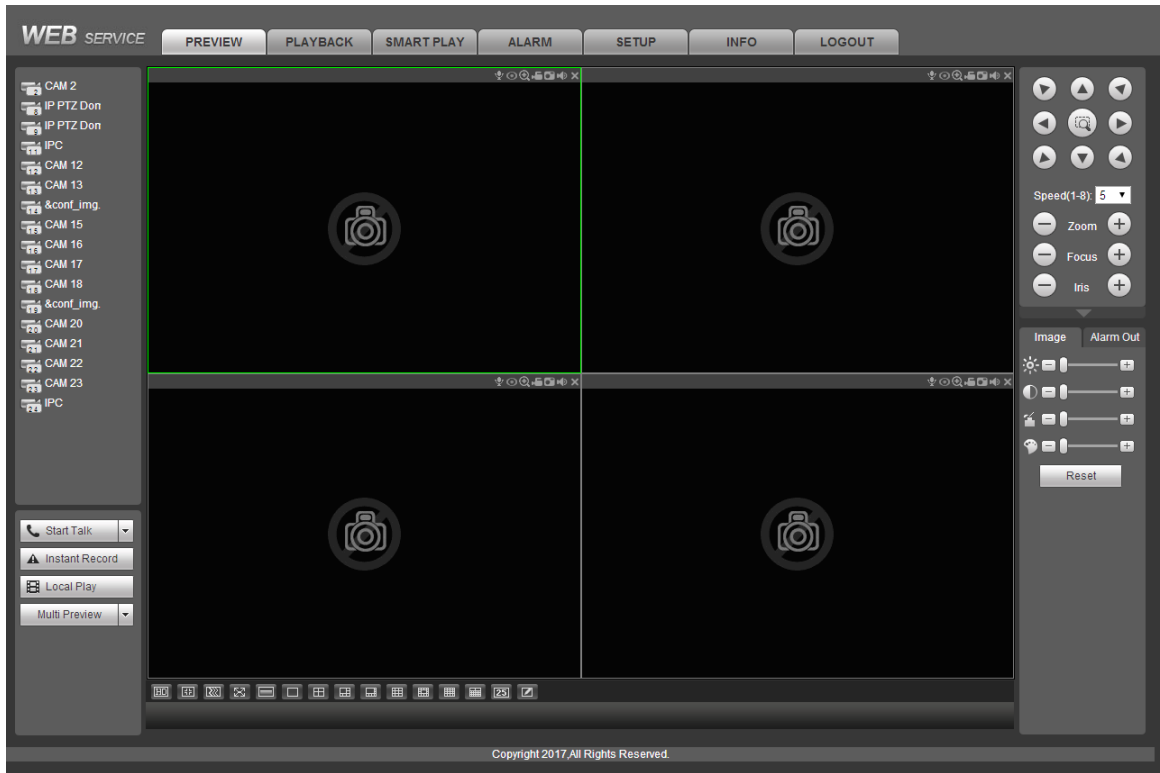- Go to "C:\Program Files\webrec" and then delete Single folder.

Figure 5-2

6 P2P

Step 1 Use cell phone to scan the client QR code and download the APP. See Figure 6-1.

📖 **Note**

- There are two ways to get QR code.
- Refer to the device package box to get the cell phone client QR code.
- Login the device local menu, and from main menu->Setting->Network->P2P, or login the WEB, from Setup->Network->TCP/IP->P2P to get the client QR code and the device SN QR code.

Figure 6-1

Step 2 After installation, run the APP and then select Live preview to go to the main interface. Add the device via the cell phone.

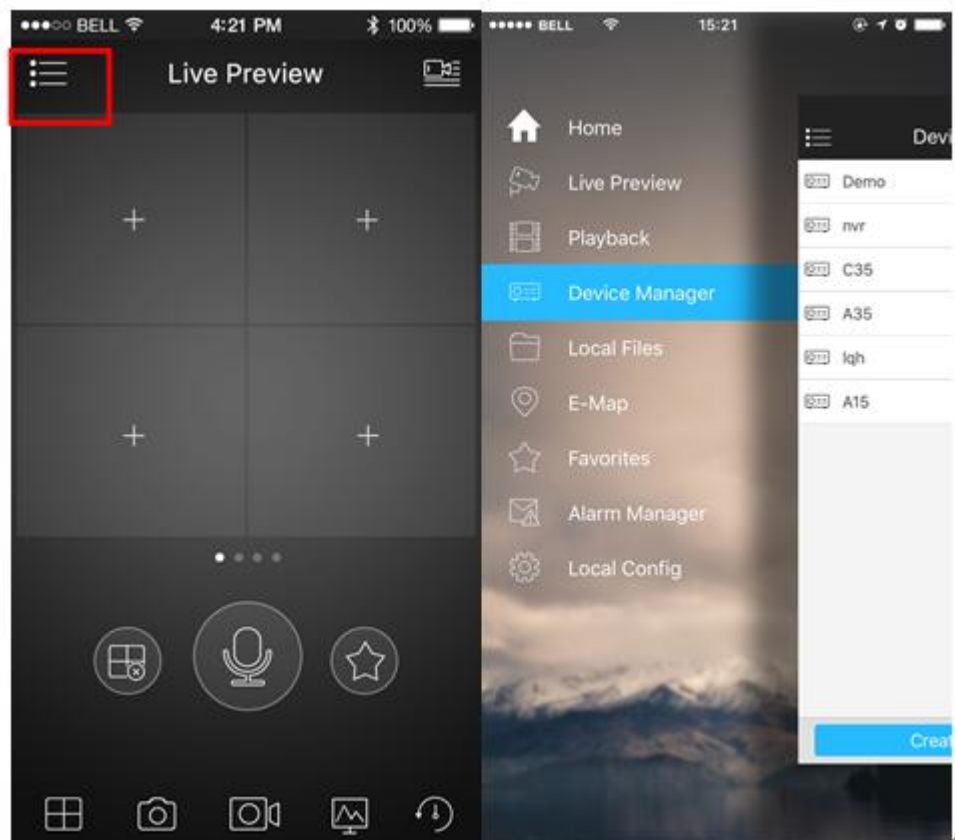1) Tap and then tap Device Manager. See Figure 6-2.

Figure 6-2

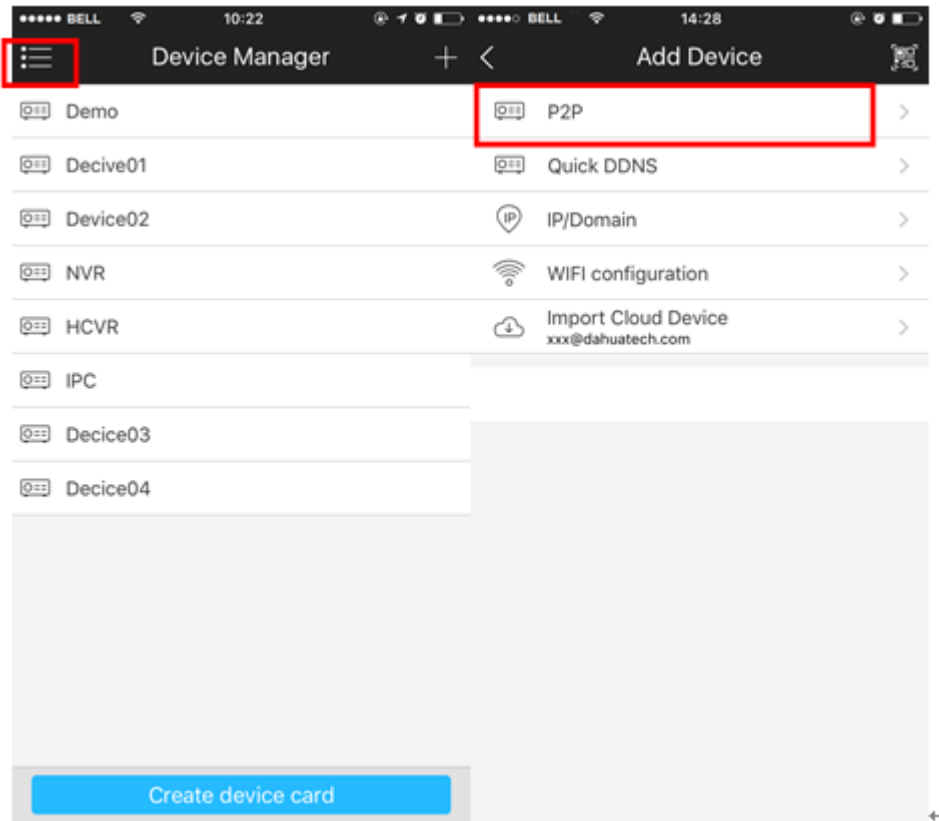2) Tap P2P to add the device. See Figure 6-3.

Figure 6-3

3) Scan the device label or the device SN on the device local menu to add the device. See Figure 6-4.

Figure 6-4

a) After scan, you can view the product SN. Click the Start live preview button, now you can see live view on the cell phone. See Figure 6-5.
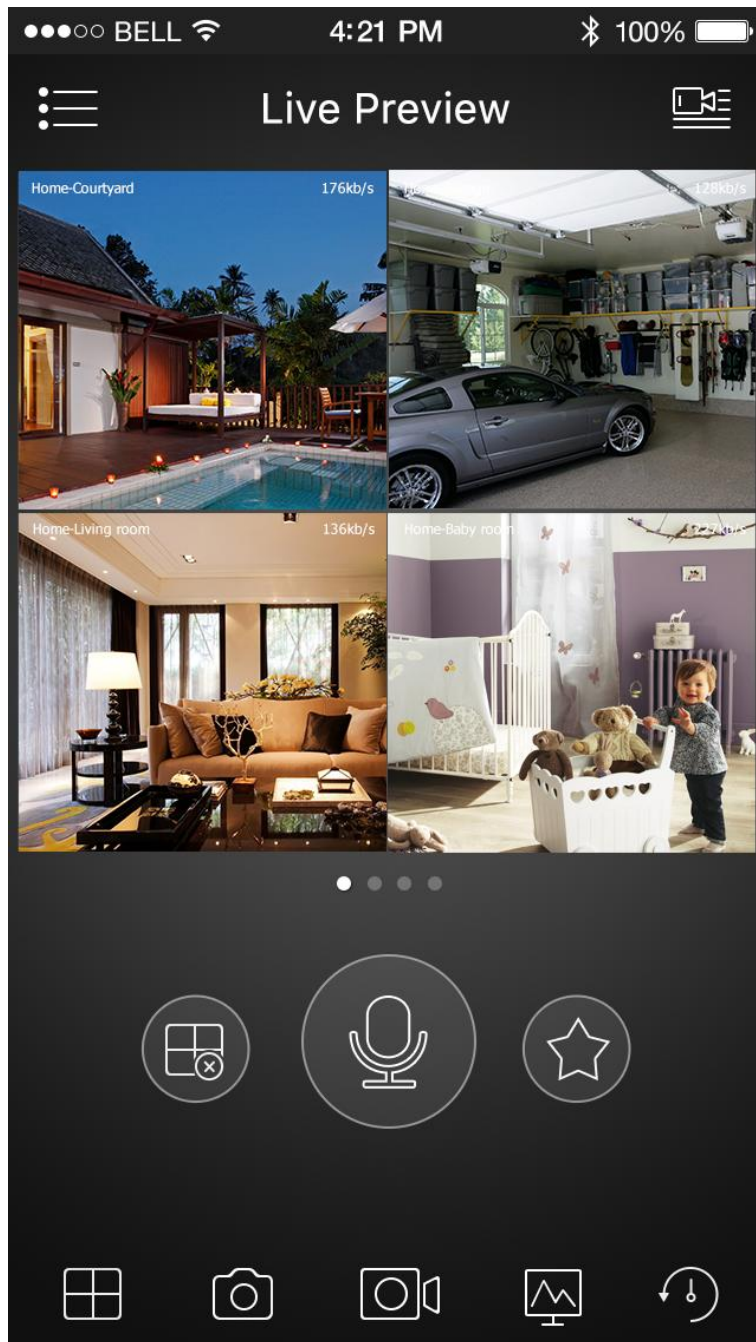
Figure 6-5

For detailed operation information, please refer to the *User's Manual*.

📖 **Note**

- Slight difference may be found in user interface.
- All the designs and software here are subject to change without prior written notice.
- All trademarks and registered trademarks are the properties of their respective owners.
- If there is any uncertainty or controversy, please refer to the final explanation of us.
- Please visit our website or contact your local service engineer for more information.