# Network Video Recorder

## Quick Start Guide

**V1.1.1**

# 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.

I

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

# Foreword

## General

This quick start guide (hereinafter referred to be "the Guide") introduces the functions and operations of the NVR (EZ-IP 2.0) 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 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.<br>📖 **Note**<br><br>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.<br>📖 **Note**<br><br>Contact your local retailer or our service engineer if the connection is loosen. |

# 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!**

## 2.1 Smart 1U Series

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. **We do not recommend the PC HDD.**



①. Loosen the screws of the bottom of the chassis.



② Place the HDD in accordance with the four holes in the bottom.



③ Turn the device upside down and then secure the screws firmly.



④ Connect the HDD cable and power cable to the HDD and the mainboard respectively.



⑤ Put the cover back and then fix the screws of the rear panel. The installation is complete.
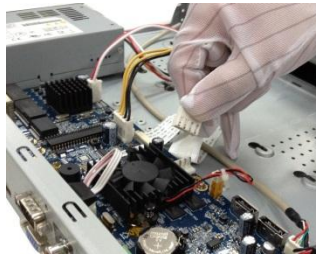
## 2.2 Compact 1U and 1U Series

For the first time to install, please check the HDD has been installed or not.
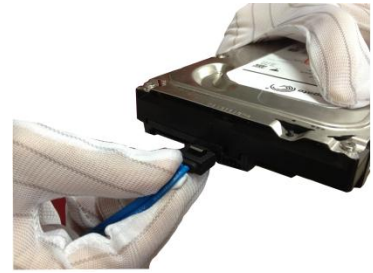Refer to the user manual for HDD space information and recommended HDD brand. Please use HDD of 7200rpm or higher. **We do not recommend the PC HDD.**

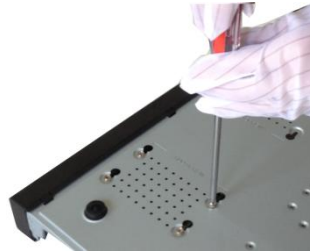① Loosen the screws of the upper cover and side panel.



② Connect the one end of the HDD data cable and the power cable to the mainboard.



③ Connect the other end of the HDD data cable and the power cable to the HDD.



④ Place the HDD in accordance with the four holes on the bottom of the chassis.



⑤ Turn the device upside down; fix the screws to secure the HDD on the bottom of the chassis.



⑥ Put the cover in accordance with the clip and then fix the screws on the rear panel and side panel.

# 3 Rear Panel

Follow figures listed here for reference only. Please refer to the actual product for detailed information.

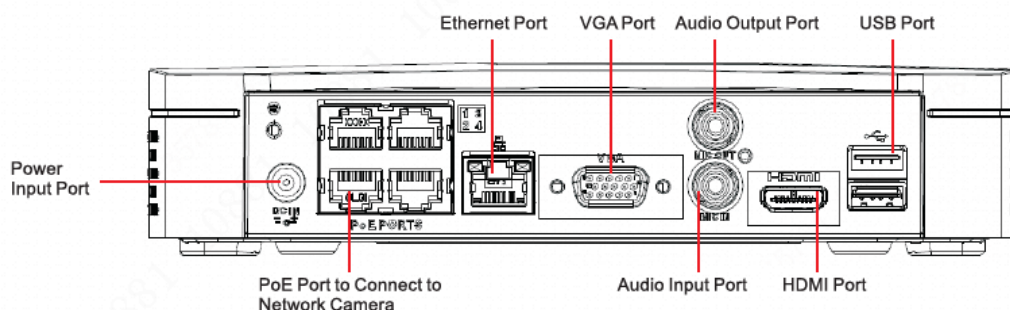## 3.1 Smart 1U Series

The front panel is shown as in Figure 3-1.



Figure 3-1

## 3.2 Compact 1U and 1U Series

The front panel is shown as in Figure 3-2.
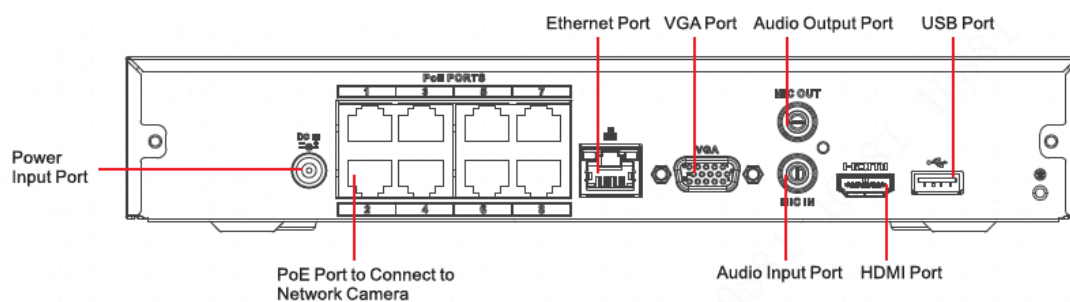


Figure 3-2

 Note

Please check the icon on the rear panel carefully. Please refer to the actual product for detailed information.

● If the icon is ![DC 12V icon], it inputs DC 12V power. If the icon is ![DC 48V icon], it inputs the DC 48V power.

● The 4PoE series product supports 48V 50W total power. The 8PoE series products supports 48V 80W total power.

4

# 4 GUI Operation

📖 **Note**

Slight difference may be found on the user interface. All figures listed below for reference only.

## 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 🔲, device can display the corresponding prompt question for you to remind the password.

⚠️ **WARNING**

**STRONG PASSWORD RECOMMENDED-For your device 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.
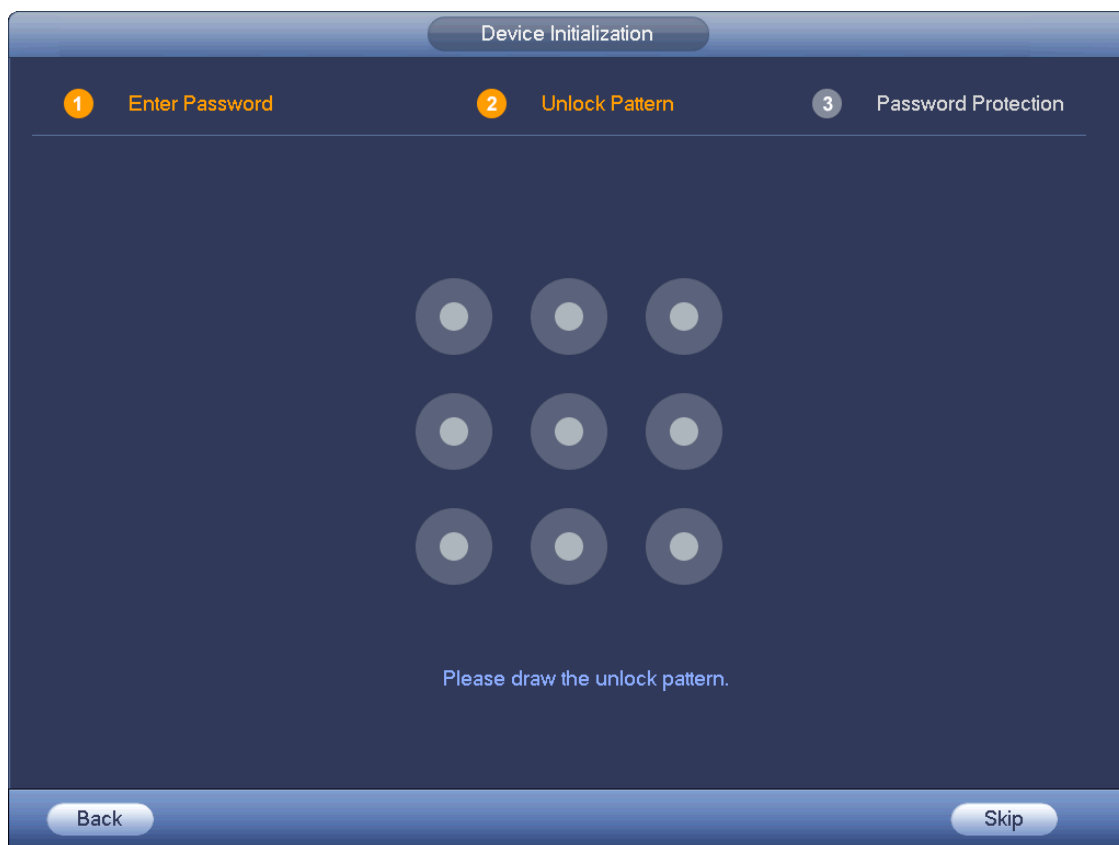
6

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.

7

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.

● 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**.

● 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  Change IP Address

8

📖 **Note**

Different series products have different Ethernet adapter amount and type. Please refer to the actual product.

From Main menu->Setting->Network->TCP/IP, enter TCP/IP interface. See Figure 4-4.
It is to change default IP address (192.168.1.108).



Figure 4-4

## 4.4  Camera Registration

From Main menu->Setting->Camera->Registration, enter Registration interface. Or on the preview interface, right click mouse and then select Camera Registration. Enter the Registration interface. See Figure 4-5.
Click Device search and then double click the searched device on the list, or check the box before the searched device name and then click Add button. Click OK to complete the add operation.

Figure 4-5

## 4.5 Schedule

From Main menu->Setting->Storage->Schedule, enter schedule interface. See Figure 4-6.
After device first booted up, all channels are record continuously by default. Device supports customized record period and record type.

Figure 4-6

## 4.6 Playback

From Main menu->Search, or on the preview interface right click mouse and then select search item, enter the following interface. See Figure 4-7.

It is to search and playback the video record file or image. Please refer to the user's manual for detailed information.
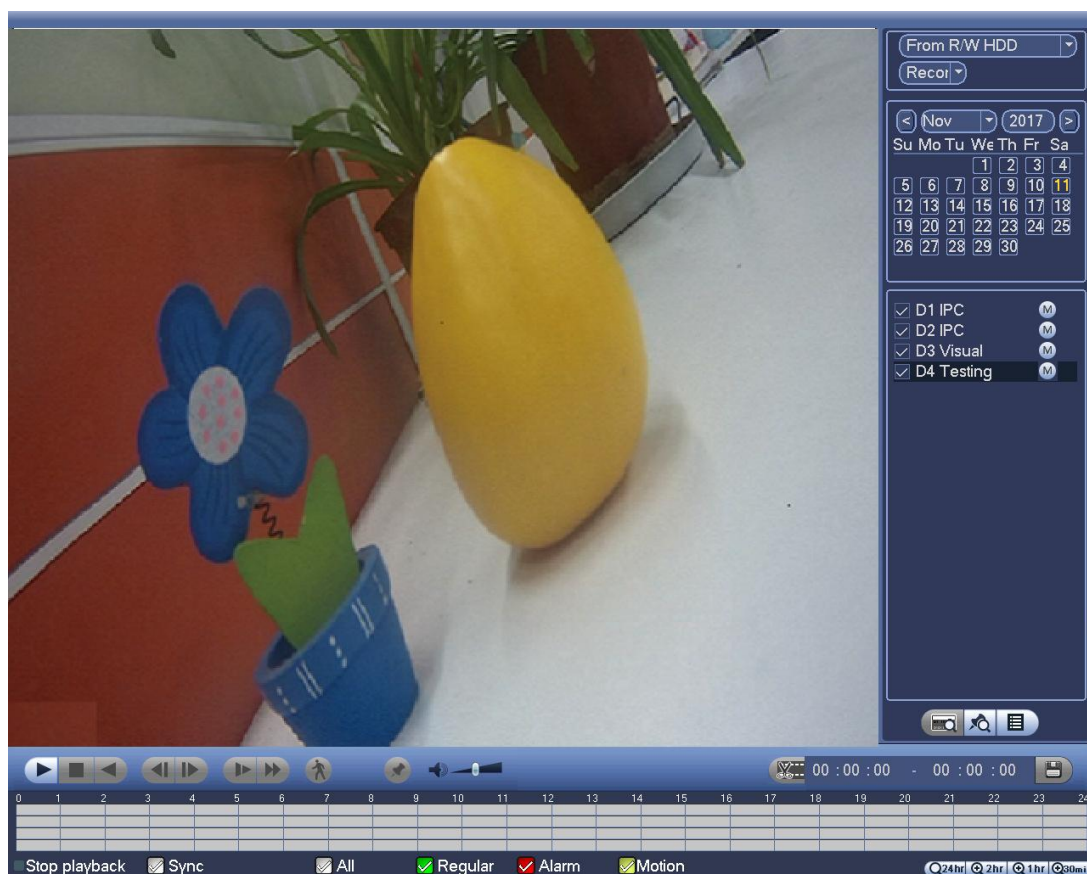
Figure 4-7

## 4.7 Shut down

From Main menu->shut down, enter the shutdown interface. Click Shut down.

# 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.**

## 5.1 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 regularlay and keep it well.
- In case you forgot passowrd, click Forgot password to reset. Refer to the user's manual for detailed informaiton.

Step 3 Click Login.
Enter preview interface. See Figure 5-2. Refer to the user's manual for detailed information.

### 📖 Note

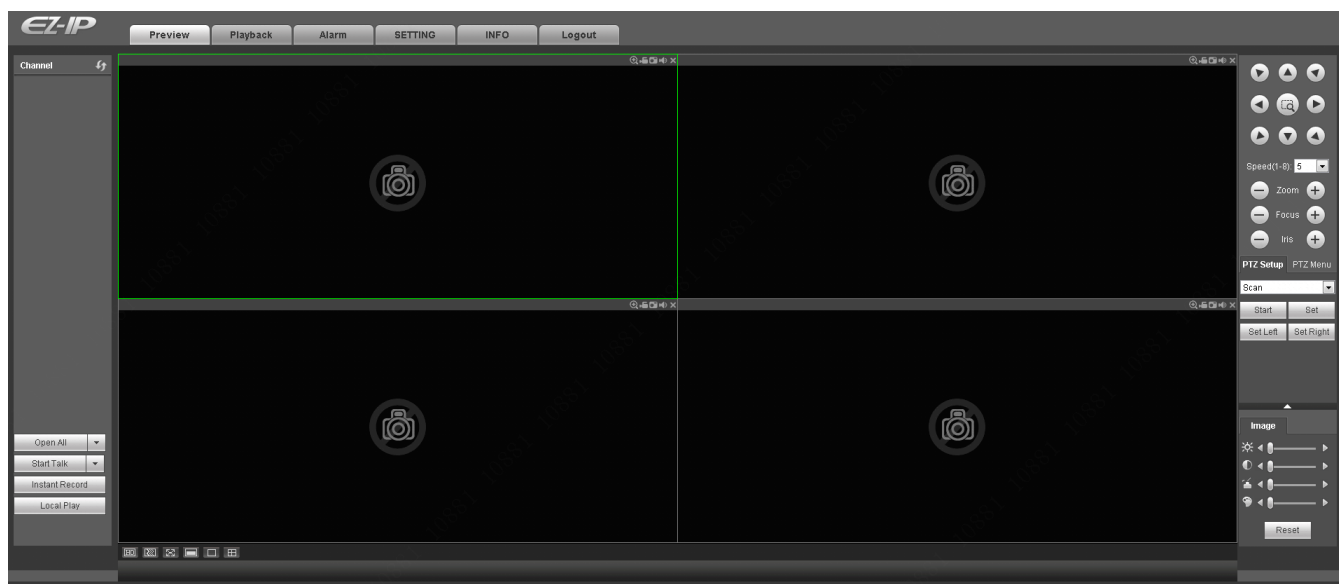- Click Install the plug-in to install if it is your first time to login the WEB.

Figure 5-2

14

# 6 P2P

Step 1 Use cell phone to scan the client QR code and download the APP.

## 📖 **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.

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.

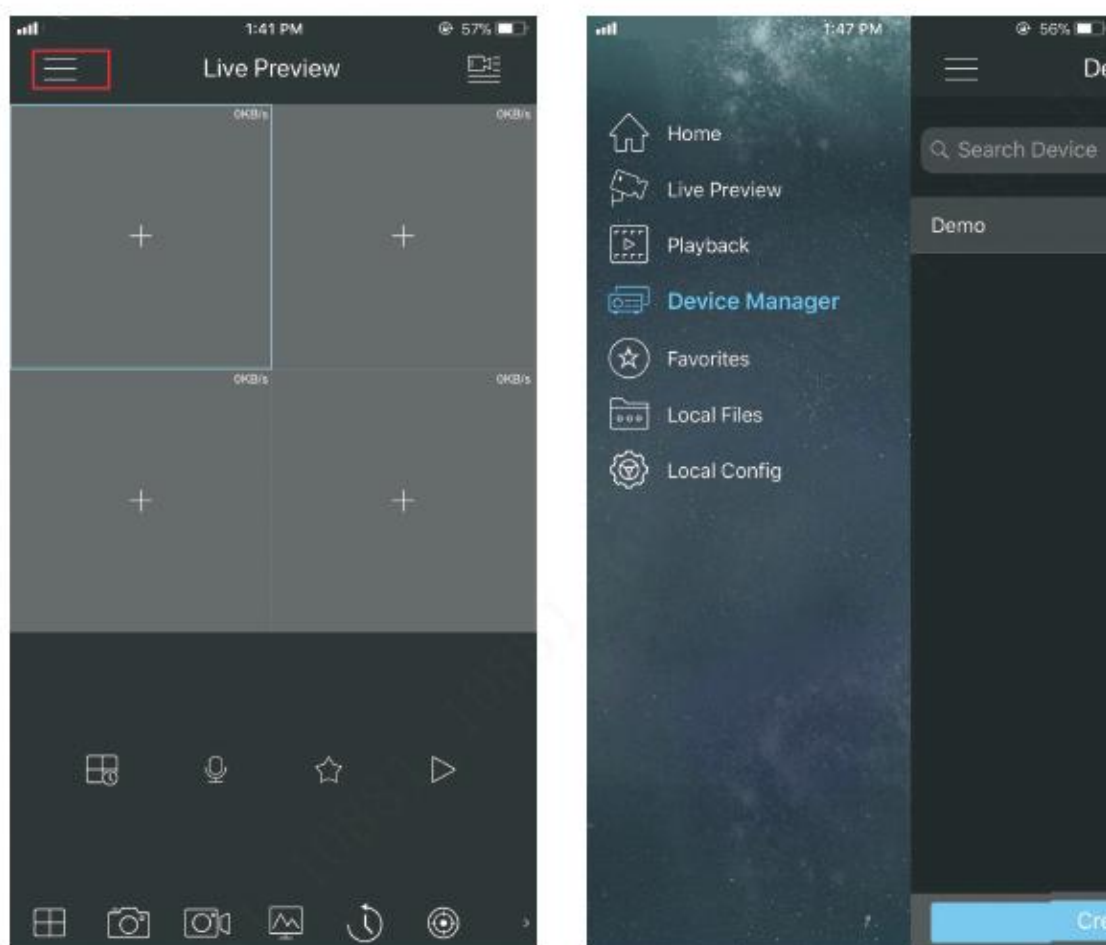1) Tap 📋 and then tap Device Manager. See Figure 6-1.



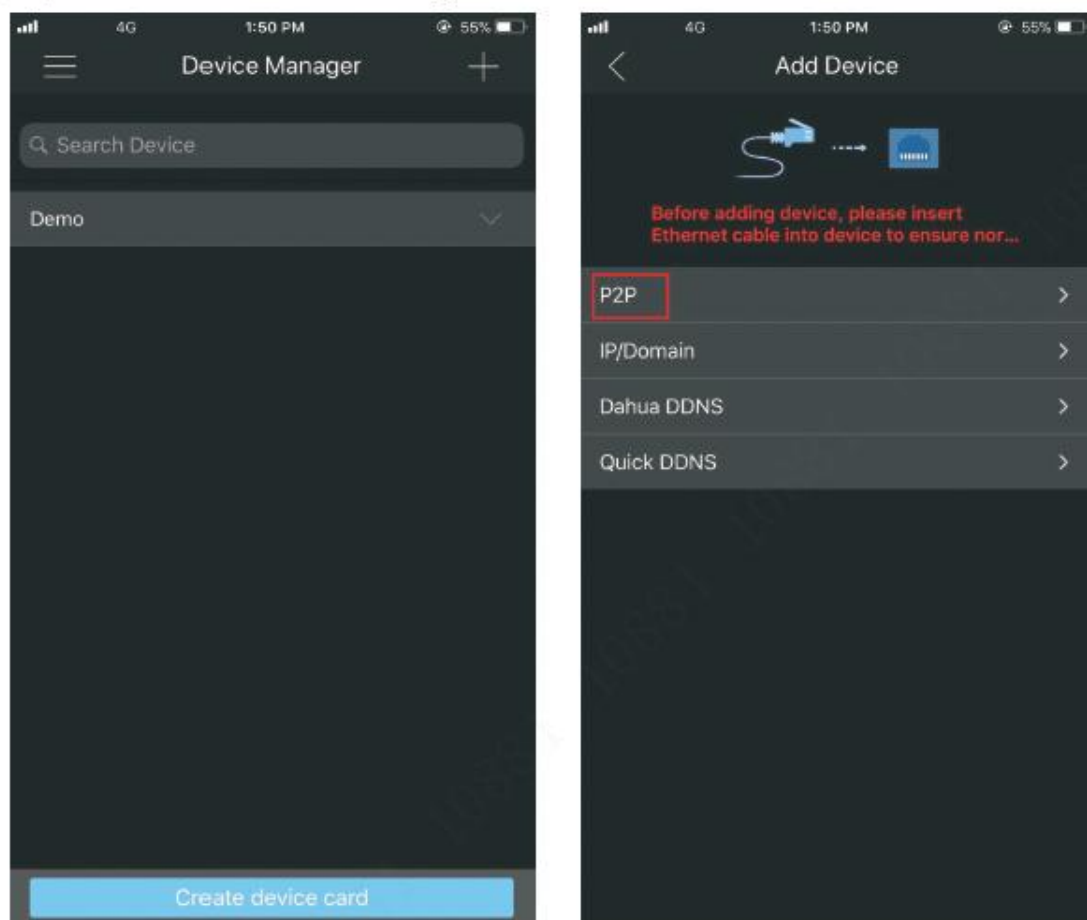Figure 6-1

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



Figure 6-2

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



Figure 6-3

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 6-4.
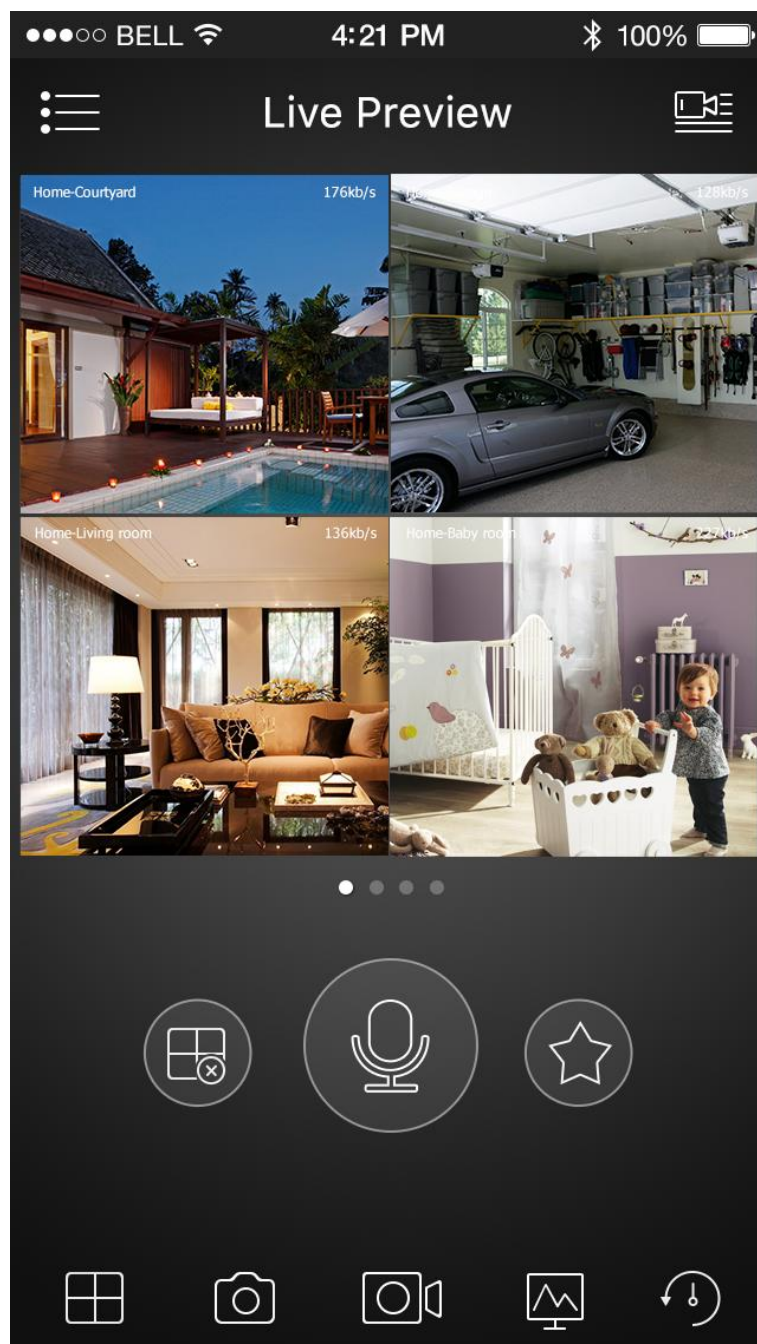
Figure 6-4

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.**

17