

Wi-Fi Kit Quick Guide

V1.00

1 Default IP, Username and Password

IP address:	NVR	192.168.1.30
	IPC	192.168.1.13
Username:	admin	
Password:	123456	

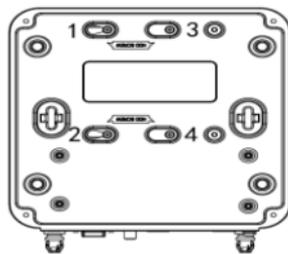
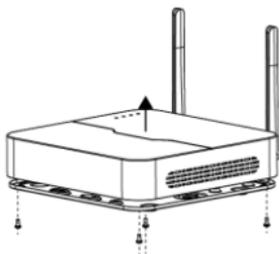
NOTE!

For security, you are strongly recommended to set a strong password of at least nine characters including all three elements: digits, letters and special characters.

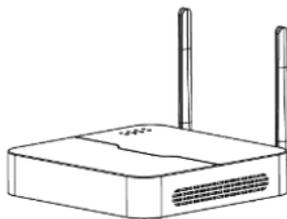
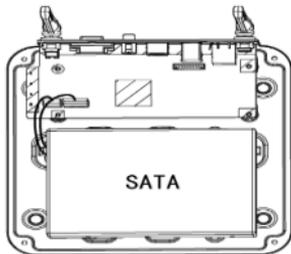
2 Disk Installation

The illustrations are for reference only. The actual device may vary.

1. Loosen the screws and remove the cover.
2. Secure the disk by fixing the screws to the screw holes shown in the figure.



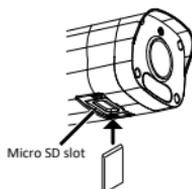
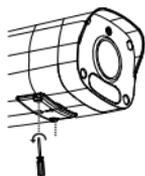
3. Connect data cables and power cables to the disk.
4. Put the cover back in place and tighten the screws.



3 (Optional) Install SD Card

Some camera models support Micro SD card. You need to open the bottom cover to install the SD card. Do not hot plug the Micro SD card after it is inserted. Otherwise the camera or the SD card might be damaged.

1. Open the bottom cover.
2. Insert the SD card properly.



4 Connect the Kit

The following part shows an example. The actual device may vary.

1. Connect the NVR to a monitor with a VGA or HDMI cable (not included in the kit).
2. Plug a mouse into the USB interface on the NVR.
3. Connect the NVR and the camera to power.

Figure 4-1 NVR Interfaces

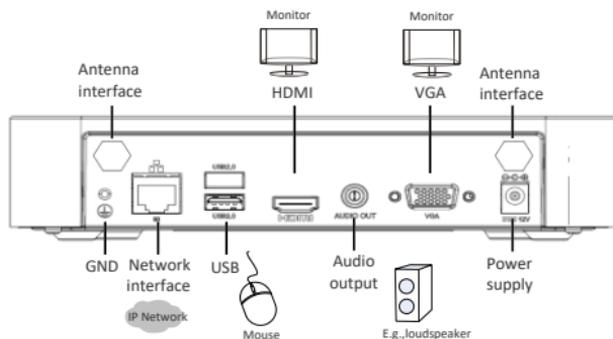
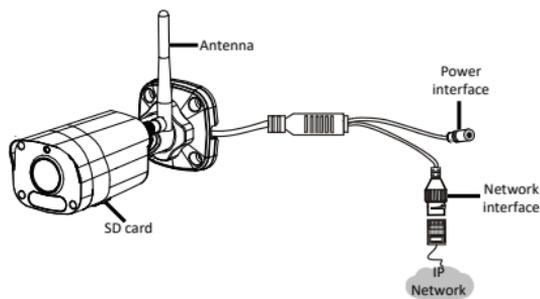


Figure 4-2 IPC Interfaces



5 Device Operation

5.1 Startup and Shutdown

Make sure the cables are connected correctly and the device is grounded properly. Use a power supply that meets requirements.

5.1.1 Startup

Connect the devices to power to start up the devices.

5.1.2 Shutdown

Click  > **Shutdown** on the screen toolbar in live view page.



CAUTION!

Do not disconnect power when the NVR is operating or shutting down.

5.2 Wi-Fi Configuration

The camera will get online and start live view on the NVR once the NVR and camera are connected to power. Follow the steps to change Wi-Fi settings.

1. Right-click on the NVR and then choose **Menu > Network > Wi-Fi AP**.
2. Change settings as needed:
 - SSID: MAC address by default, you can change as needed.

- Password: The default is the last eight digits of the serial number. You are strongly recommended to change into a strong password.
- Region, Channel: Signal interference varies with region and channel. You are recommended to choose a channel with less signal interference.
- Wireless NIC IP: The IP address of wireless NIC. The NVR assigns IP address to connected devices based on the start and end IP address range.

SSID	NVR
Password	Admin12345
Region	MKX
Channel	13 Auto
Wireless NIC IP	172 . 16 . 0 . 1
Start IP	172 . 16 . 0 . 100
End IP	172 . 16 . 0 . 254

No	Camera ID	Status	IP	Model	MAC Address	Signal Strength
1	D2	Added	172.16.0.109	IPUS-8208S-1080P-B	00:95:69:18:58:2c	
2	D1	Added	172.16.0.104	IPUS-8208S-1080P-B	00:95:69:15:36:a8	

Note: Follow local laws and regulations governing Wi-Fi usage to choose region.

Refresh QR Code Pair One-Click Pair Apply Exit



CAUTION!

The NVR's wireless NIC IP must be in a different network segment with its LAN IP address.

3. Click **Apply**.



NOTE!

After SSID or password are changed on the NVR, the new SSID or password will be synchronized to online cameras. For offline cameras, the changed settings cannot be synchronized, and you need to pair the camera with the NVR again. See 5.3 Pair Devices Again for details.

5.3 Pair Devices Again

If you change Wi-Fi settings on the NVR when cameras are offline, you need to pair devices again. Choose one of the following methods as needed.



NOTE!

The following methods are also applicable if you pair a camera not in the kit with the NVR.

- One-Click Pair
 1. Connect the camera and the NVR to the same switch (or connect the camera to the NVR with a network cable), and connect the devices to power.
 2. Right-click on the NVR and then choose **Menu > Network > Wi-Fi AP**.
 3. Press the RESET button on the back of the camera to restore factory default settings.
-



NOTE!

The reset button only works in 1-10 minutes after the camera is powered on. If you fails to press the button within the time range, you need to power off the camera and then on again to restore the defaults.

4. Click **One-Click Pair**.
-



NOTE!

This function works within 3 minutes after the camera restores defaults. So, if the camera is not paired successfully within this time, please restart the camera or try other methods.

5. Wait for the camera to get online.

- QR Code Pair
 1. Connect the camera to power.
 2. Press the RESET button on the back of the camera to restore factory default settings.
 3. Right-click on the NVR and then choose **Menu > Network > Wi-Fi AP**.
 4. Click **QR Code Pair**, and follow the on-screen instructions to scan the QR code.

5. Wait for the camera to get online.

- Use EZView

Please refer to 8.5 Pair Camera and NVR for detailed steps.

6 Install Devices

6.1 Wi-Fi Signal Connectivity

The antenna sends Wi-Fi signals in all directions around it. Wi-Fi connectivity is the best when antennas are parallel with each other, and is the weakest when the top of an antenna points directly to the top of another. Please arrange the antennas properly to improve Wi-Fi connectivity.

Figure 6-1 Installation with Strongest Signal

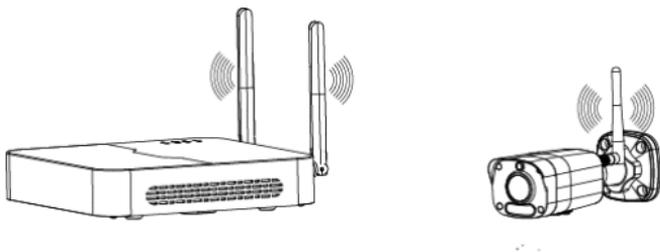
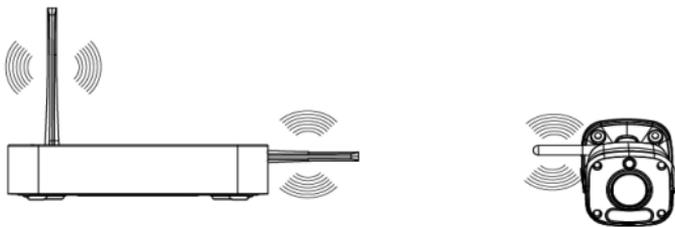


Figure 6-2 Installation with Weakest Signal



6.2 Install the Camera

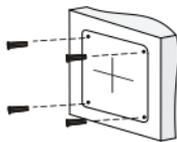
The following part takes wall mount as an example. Make sure the wall is strong

enough to support the weight of the camera. Please prepare hardware accessories in advance.

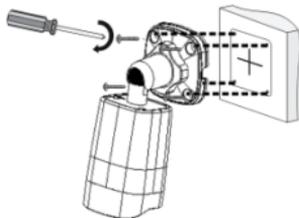
1. Paste positioning stickers on the wall and drill 30mm-depth guide holes using a Φ 6-6.5mm drill bit.



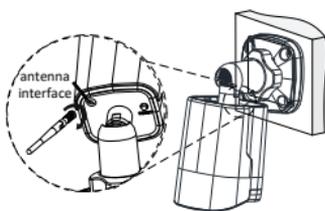
2. Knock the plastic rivets into the guide holes and ensure that they are tightened up.



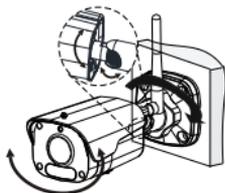
3. Screw the locknut to loosen the universal joint, and attach your camera to the wall.



4. Rotate the antenna to the antenna interface in clockwise direction.



5. Adjust the monitoring direction.



6. Connect the camera to power to start up.

7 Playback

In the preview page, select the desired window, then right click and select **Playback** to play the recording of the current day.



NOTE!

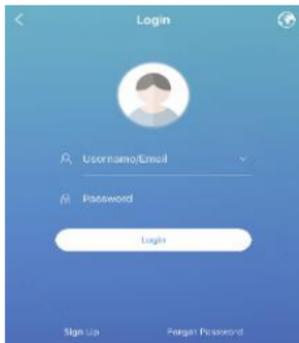
- A 7*24 recording schedule is enabled by default. To set a recording schedule manually, right click and select **Menu > Storage > Recording** and then set recording type and time based on your needs.
- If you choose **Event** type recording, you need to enable the corresponding alarm function and configure alarm-triggered recording/snapshot first.

8 EZView

Please download EZView on the App Store (iOS) or on Google Play (Android) first.

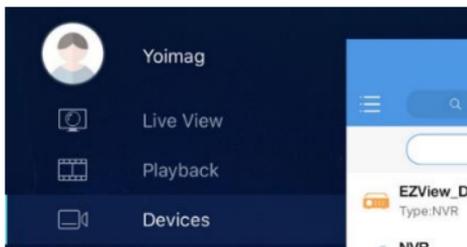
8.1 Sign Up an Account

1. Tap  in the upper right corner and choose **International** service area.
2. Tap **Sign Up** and follow the steps to complete sign up.



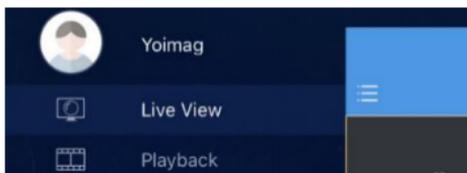
8.2 Add Devices

After logging in to your account, tap  > **Devices > Add**, then select a way to add devices. It's recommended to choose **Scan** and scan the QR code on the device body.



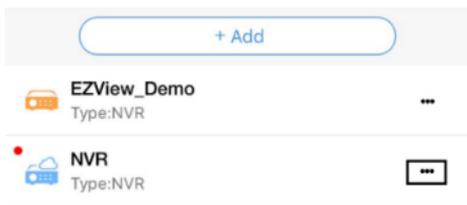
8.3 Live View/Playback

Tap  > **Live View/Playback**. Tap  in a window, then select a device to start live view or playback. You can also tap  in the upper-right corner and select device(s).



8.4 Share Devices

Tap  > **Devices**, select the desired device and tap **Share**, then complete the sharing settings. You may also share the device by generating a QR code.



8.5 Pair Camera and NVR

1. Connect the camera to power, and connect your mobile phone to NVR's Wi-Fi network.
2. Press the RESET button on the back of the camera to restore factory default settings.

3. Tap  > **Local Config** > **Device Wi-Fi Configuration**, enter the Wi-Fi password and tap **Start** to add the camera to the NVR.



Device Wi-Fi Configuration	
Wi-Fi	NVR
Password	Admin12345 
Security	WPA/WPA2 >

Follow the steps to configure Wi-Fi and add cameras to NVR.

1. Connect your mobile phone to the NVR's Wi-Fi.
2. Enter the Wi-Fi password and then tap <Start>.
3. Wait patiently for 5 mins (may be longer) and then check on the NVR whether the cameras are added.

Start

9 Web Login

Before you begin, check that your PC is connected to your NVR through network.

1. Open the browser on your PC, enter the IP address in the address bar, then press **Enter**. Install the plugin as required at first login. Close your browser during the installation.
2. In the login page, enter the correct username and password, then click **Login**.

Disclaimer and Safety Warnings

Copyright Statement

No part of this manual may be copied, reproduced, translated or distributed in any form or by any means without prior consent in writing from our company (referred to as us hereafter).

The product described in this manual may contain proprietary software owned by our company and its possible licensors. Unless permitted, no one is allowed to copy, distribute, modify, abstract, decompile, disassemble, decrypt, reverse engineer, rent, transfer, or sublicense the software in any form or by any means.

Trademark Acknowledgements



The terms HDMI and HDMI High-Definition Multimedia Interface, and the HDMI Logo are trademarks or registered trademarks of HDMI Licensing LLC in the United States and other countries.

All other trademarks, products, services and companies in this manual or the product described in this manual are the property of their respective owners.

Export Compliance Statement

Our company complies with applicable export control laws and regulations worldwide, including that of the People's Republic of China and the United States, and abides by relevant regulations relating to the export, re-export and transfer of hardware, software and technology. Regarding the product described in this manual, our company asks you to fully understand and strictly abide by the applicable export laws and regulations worldwide.

Privacy Protection Reminder

Our company complies with appropriate privacy protection laws and is committed to protecting user privacy. You may want to read our full privacy policy at our website and get to know the ways we process your personal information. Please be aware, using the product described in this manual may involve the collection of personal information such as face, fingerprint, license plate number, email, phone number, GPS. Please abide by your local laws and regulations while using the product.

About This Manual

- This manual is intended for multiple product models, and the photos, illustrations, descriptions, etc. in this manual may be different from the actual appearances, functions, features, etc. of the product.
- This manual is intended for multiple software versions, and the illustrations and descriptions in this manual may be different from the actual GUI and functions of the software.
- Despite our best efforts, technical or typographical errors may exist in this manual. Our company cannot be held responsible for any such errors and reserves the right to change the manual without prior notice.
- Users are fully responsible for the damages and losses that arise due to improper operation.
- Our company reserves the right to change any information in this manual without any prior notice or indication. Due to such reasons as product version upgrade or regulatory requirement of relevant regions, this manual will be periodically updated.

Disclaimer of Liability

- To the extent allowed by applicable law, in no event will our company be liable for any special, incidental, indirect, consequential damages, nor for any loss of profits, data, and documents.
- The product described in this manual is provided on an "as is" basis. Unless required by applicable law, this manual is only for informational purpose, and all statements, information, and recommendations in this manual are presented without warranty of any kind, expressed or implied, including, but not limited to, merchantability, satisfaction with quality, fitness for a particular purpose, and noninfringement.
- Users must assume total responsibility and all risks for connecting the product to the Internet, including, but not limited to, network attack, hacking, and virus. We strongly recommend that users take all necessary measures to enhance the protection of network, device, data and personal information. Our company disclaims any liability related thereto but will readily

provide necessary security related support.

- To the extent not prohibited by applicable law, in no event will our company and its employees, licensors, subsidiary, affiliates be liable for results arising out of using or inability to use the product or service, including, not limited to, loss of profits and any other commercial damages or losses, loss of data, procurement of substitute goods or services; property damage, personal injury, business interruption, loss of business information, or any special, direct, indirect, incidental, consequential, pecuniary, coverage, exemplary, subsidiary losses, however caused and on any theory of liability, whether in contract, strict liability or tort (including negligence or otherwise) in any way out of the use of the product, even if our company has been advised of the possibility of such damages (other than as may be required by applicable law in cases involving personal injury, incidental or subsidiary damage).
- To the extent allowed by applicable law, in no event shall our total liability to you for all damages for the product described in this manual (other than as may be required by applicable law in cases involving personal injury) exceed the amount of money that you have paid for the product.

Network Security

Please take all necessary measures to enhance network security for your device.

The following are necessary measures for the network security of your device:

- **Change default password and set strong password:** You are strongly recommended to change the default password after your first login and set a strong password of at least nine characters including all three elements: digits, letters and special characters.
- **Keep firmware up to date:** It is recommended that your device is always upgraded to the latest version for the latest functions and better security. Visit our official website or contact your local dealer for the latest firmware.

The following are recommendations for enhancing network security of your device:

- **Change password regularly:** Change your device password on a regular basis and keep the password safe. Make sure only the authorized user can log in to the device.
- **Enable HTTPS/SSL:** Use SSL certificate to encrypt HTTP communications and ensure data security.
- **Enable IP address filtering:** Allow access only from the specified IP addresses.
- **Minimum port mapping:** Configure your router or firewall to open a minimum set of ports to the WAN and keep only the necessary port mappings. Never set the device as the DMZ host or configure a full cone NAT.
- **Disable the automatic login and save password features:** If multiple users have access to your computer, it is recommended that you disable these features to prevent unauthorized access.
- **Choose username and password discretely:** Avoid using the username and password of your social media, bank, email account, etc, as the username and password of your device, in case your social media, bank and email account information is leaked.
- **Restrict user permissions:** If more than one user needs access to your system, make sure each user is granted only the necessary permissions.
- **Disable UPnP:** When UPnP is enabled, the router will automatically map internal ports, and the system will automatically forward port data, which results in the risks of data leakage.

Therefore, it is recommended to disable UPnP if HTTP and TCP port mapping have been enabled manually on your router.

- **SNMP:** Disable SNMP if you do not use it. If you do use it, then SNMPv3 is recommended.
- **Multicast:** Multicast is intended to transmit video to multiple devices. If you do not use this function, it is recommended you disable multicast on your network.
- **Check logs:** Check your device logs regularly to detect unauthorized access or abnormal operations.
- **Physical protection:** Keep the device in a locked room or cabinet to prevent unauthorized physical access.
- **Isolate video surveillance network:** Isolating your video surveillance network with other service networks helps prevent unauthorized access to devices in your security system from other service networks.

Safety Warnings

The device must be installed, serviced and maintained by a trained professional with necessary safety knowledge and skills. Before you start using the device, please read through this guide carefully and make sure all applicable requirements are met to avoid danger and loss of property.

Storage, Transportation, and Use

- Store or use the device in a proper environment that meets environmental requirements, including and not limited to, temperature, humidity, dust, corrosive gases, electromagnetic radiation, etc.
- Make sure the device is securely installed or placed on a flat surface to prevent falling.
- Unless otherwise specified, do not stack devices.
- Ensure good ventilation in the operating environment. Do not cover the vents on the device. Allow adequate space for ventilation.
- Protect the device from liquid of any kind.
- Make sure the power supply provides a stable voltage that meets the power requirements of the device. Make sure the power supply's output power exceeds the total maximum power of all the connected devices.
- Verify that the device is properly installed before connecting it to power.
- Do not remove the seal from the device body without consulting **our company** first. Do not attempt to service the product yourself. Contact a trained professional for maintenance.
- Always disconnect the device from power before attempting to move the device.
- Take proper waterproof measures in accordance with requirements before using the device outdoors.

Power Requirements

- Install and use the device in strict accordance with your local electrical safety regulations.
- Use a UL certified power supply that meets LPS requirements if an adapter is used.
- Use the recommended cordset (power cord) in accordance with the specified ratings.
- Only use the power adapter supplied with your device.
- Use a mains socket outlet with a protective earthing (grounding) connection.
- Ground your device properly if the device is intended to be grounded.

Battery Use Caution

- When battery is used, avoid:
 - Extremely high or low temperature and air pressure during use, storage and transportation;

- Battery replacement.
- Use the battery properly. Improper use of the battery such as the following may cause risks of fire, explosion or leakage of flammable liquid or gas.
 - Replace battery with an incorrect type;
 - Dispose of a battery into fire or a hot oven, or mechanically crushing or cutting of a battery;
- Dispose of the used battery according to your local regulations or the battery manufacturer's instructions.

Avertissement de l'utilisation de la batterie

- Lorsque utiliser la batterie, évitez:
 - Température et pression d'air extrêmement élevées ou basses pendant l'utilisation, le stockage et le transport.
 - Remplacement de la batterie.
- Utilisez la batterie correctement. Mauvaise utilisation de la batterie comme celles mentionnées ici, peut entraîner des risques d'incendie, d'explosion ou de fuite liquide de gaz inflammables.
 - Remplacer la batterie par un type incorrect;
 - Disposer d'une batterie dans le feu ou un four chaud, écraser mécaniquement ou couper la batterie;
- Disposer la batterie utilisée conformément à vos règlements locaux ou aux instructions du fabricant de la batterie.
- **Personal safety warnings:**
 - Chemical Burn Hazard. This product contains a coin cell battery. Do NOT ingest the battery. It can cause severe internal burns and lead to death.
 - Keep new and used batteries away from children.
 - If the battery compartment does not close securely, stop using the product and keep it away from children.
 - If you think batteries might have been swallowed or placed inside any part of the body, seek immediate medical attention.
- **Avertissements de sécurité personnelle:**
 - Risque de brûlure chimique. Ce produit contient une batterie de cellules. N'ingérer pas la batterie. Si la batterie de cellule est avalée, elle peut causer de graves brûlures internes en seulement 2 heures et peut entraîner la mort.
 - Gardez les batteries nouvelles ou utilisées à l'écart des enfants.
 - Si le compartiment de la batterie ne se ferme pas en toute sécurité, cessez d'utiliser le produit et gardez-le à l'écart des enfants.
 - Si vous pensez que des piles ont pu être avalées ou placées à l'intérieur d'une partie du corps, consultez immédiatement un médecin.

Regulatory Compliance

FCC Statements

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Caution: The user is cautioned that changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help..

RF Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20cm between the radiator and any part of your body.

LVD/EMC/RE Directive



This product complies with the European Low Voltage Directive 2014/35/EU, EMC Directive 2014/30/EU and RE Directive 2014/53/EU.

WEEE Directive-2012/19/EU



The product this manual refers to is covered by the Waste Electrical & Electronic Equipment (WEEE) Directive and must be disposed of in a responsible manner.

Battery Directive-2013/56/EC



Battery in the product complies with the European Battery Directive 2013/56/EC. For proper recycling, return the battery to your supplier or to a designated collection point.