Mobile Network Video Recorder MNVR-EL04

Quick Start Guide V.1.00

Table Of Contents

IMPORTANT SAFEGUARDS AND WARNINGS

Operating Requirement

- Install the PoE front-end device inside a vehicle.
- The Device support in-dash automotive installation
- Do not place and install the device in an area exposed to direct sunlight or near heat generating devices.
- 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

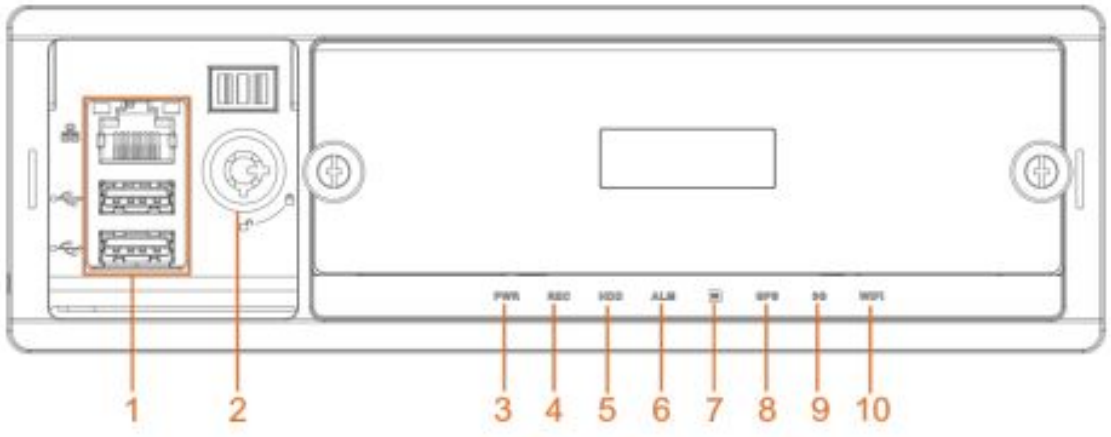
- Improper battery use might result in fire, explosion, or inflammation.
- When replacing battery, make sure the same model is used.
- Use the recommended power cables in the region and conform to the rated power specification
- Use the power adapter provided otherwise, it may result in injury and device 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.

1A. Inspecting the Components

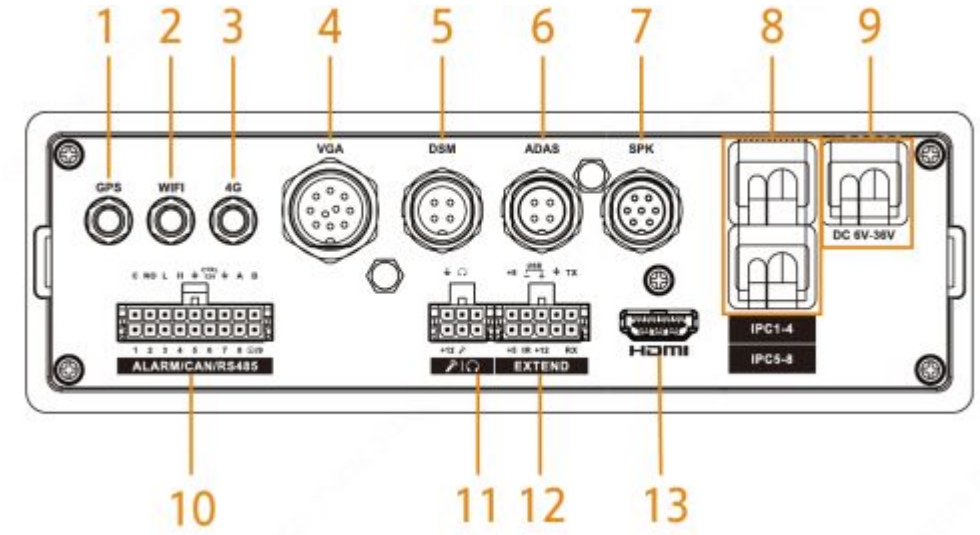
Items	Detail	Inspect
Package	• Appearance • Packing Materials • Accessories	• Any obvious damage on box • Broken or distorted positions due to physical abuse • The accessory box should have all materials (ie: Security Key, extra cables, connectors, Power cord)
Labels	• Labels Containing the Serial Number are located on Device and in box	• The serial numbers on the Labels are in vital in tracking the device in our database. Ensure they are not torn or lost.
Device	• Appearance • Data, power, and fan cables, mainboard	• Any obvious damage • Loose connections

1A. Front/ Rear Panel Identification

The actual appearance may differ depending on the model purchased.



1. (Inside Panel) **USB port x2, RJ45 network port**
2. (Inside Panel) **Device lock/unlock (on/off button)-**
NOTE: if left in unlocked position, the NVR will not boot/shut down if operating.
3. Power indicator light
4. Record indicator light
5. HDD indicator light
6. Alarm indicator light
7. IR (if equipped)
8. GPS status indicator
9. 4G status indicator
10. Wi-Fi status indicator

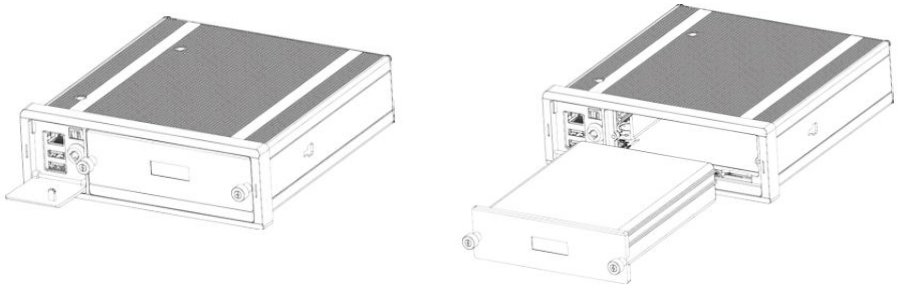


1. GPS port
2. WIFI antenna port
3. 4G antenna port
4. VGA port
5. Driver Status Monitor (DSM) camera input
6. Advanced Driver Assistance Systems (ADAS) camera input
7. SPK port
8. IPC Connection (Standard POE only)
9. Power cable
10. Alarm input/output port
11.Voice talk port
12. Extension port
13. HDMI interface

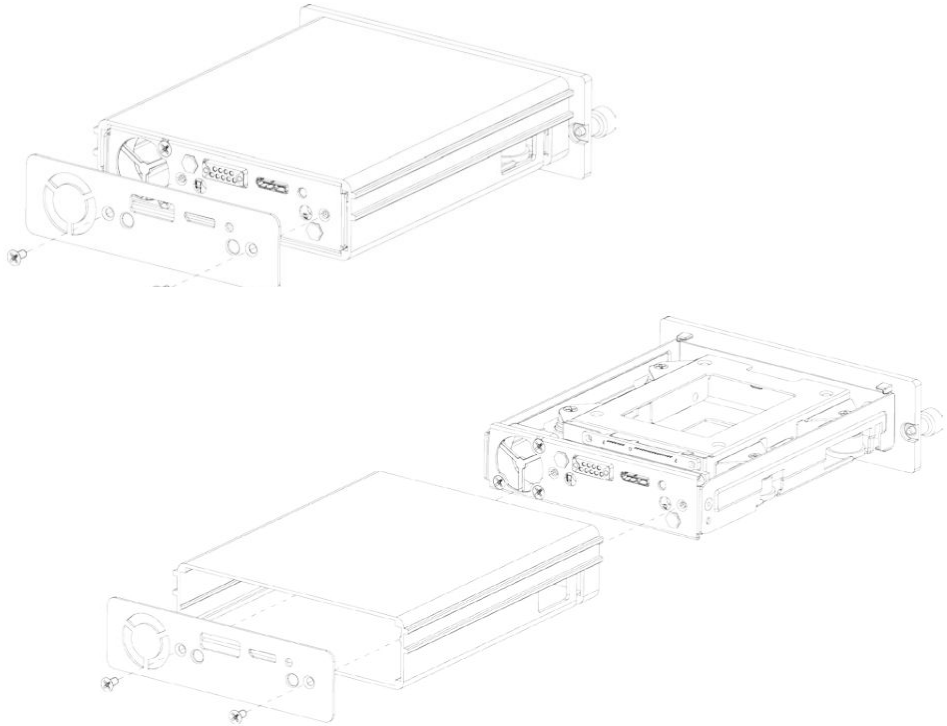
2A. Initial Setup

2.1 - HDD Install

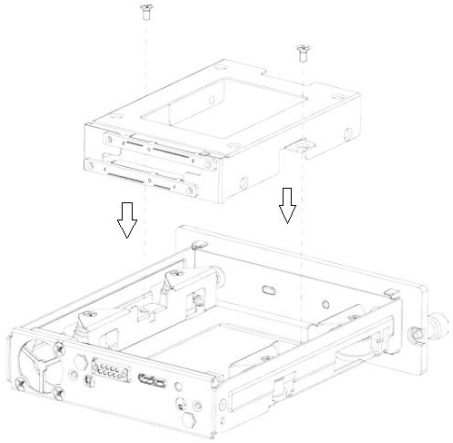
1. Press to open the side panel and unlock the HDD bay using the supplied Key
2. Loosen the two screws at the front panel and take out the HDD carrier along the guide rail.



3. Loosen two screws on the back panel of the HDD carrier, take out the rear carrier panel, and remove the HDD carrier enclosure.
4. Loosen two screws of the HDD holder and remove the HDD tray.



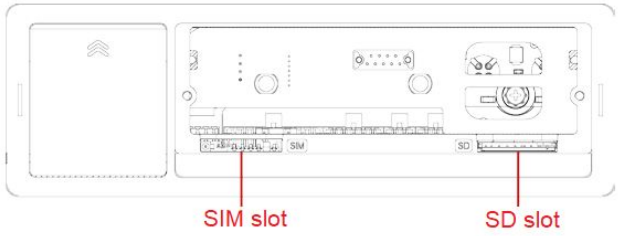
5. Loosen two screws of the HDD holder and remove the HDD tray.
6. Use four screws to install each HDD and the HDD holder, and replace the HDD holder back to the Recorder.



2.2 - SIM Card Install

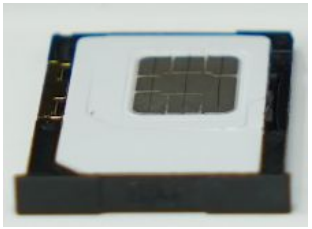
(**NOTE**: Some models like **MNVR-EL04** support **only Verizon Plans**)

1. Press to open the side panel and unlock the HDD bay using the supplied Key
2. Remove the HDD carrier as per previous instructions. Identify the SIM card slot.



3. Using a small pointed tool, push in the white button on the lower left side of the SD card slot. This allows SIM card tray to pop out the slot to be removed.

4. Remove the Tray and install a SIM card into the tray. Replace the tray back into the slot firmly. (SIM card will be facing down when installed)



2.3 - Connecting Antennas

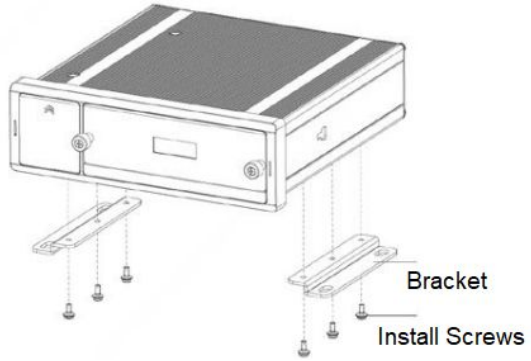
- Three antennas are included in the accessory box and screw into the respective ports in the back of the MNVR and are required for their respective use..
- The flat-ended antennae is for 4G. This is recommended to be installed vertically attached to near the windshield.

- The GPS Antenna is recommended to be installed on the roof of the vehicle.

- The WiFi Antenna is recommended to be installed near the windshield or on the roof of the vehicle.

2.4 - Vehicle Mounting and Installation

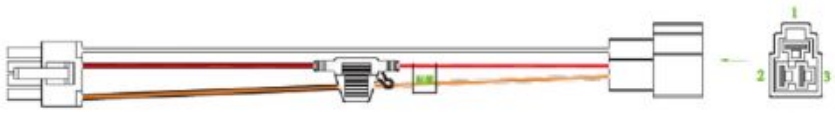
1. Place washers onto the install screws.
2. Using the install screws with washers, mount bracket to the bottom of the Recorder respectively.



3. Install the MNVR onto the vehicle 9we recommend the vehicle to be off).
4. Drill holes on the vehicle according to the installation dimensional drawing.
5. Use screws to install the Device onto the vehicle.
6. Connect all the necessary cabling to the back of the MNVR (minus power cable).

2.5 - Powering the MNVR

- Before connecting the power cable, v**erify with a multimeter: whether the input voltage is between 6V DC and 36V DC**. The NVR will become damaged if it is out of this range.
- **Check Polarity!** Please make sure that the positive and negative poles of the power are connected correctly. If not, the device may be damaged.
- The diameter of the power cable should be more than 1.0 mm2. Use recommended power cables and automotive nylon latching connector.
- When connecting the cables to the device, make sure that the main power switch of the vehicle is turned off and the key of the vehicle is placed in the off state.
- **The MNVR power cable should be connected to the ground wire. ACC signal, and constant electricity.**



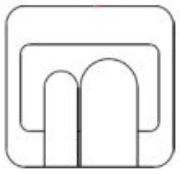
2.6 - Power Cable

1. Enable the main power switch on the vehicle, then confirm vehicle power output with a multimeter while the Key position is on **OFF, ACC/ Accessory** and **ON** position to verify power behavior.
   When the multimeter detects voltage, remove the car key. If the voltage changes to 0V, it means that the measured signal is ACC on the car
2. Turn off the main power switch on the vehicle, and place the key in the OFF state.
3. Connect the power cable according to the main power switch installation mode.

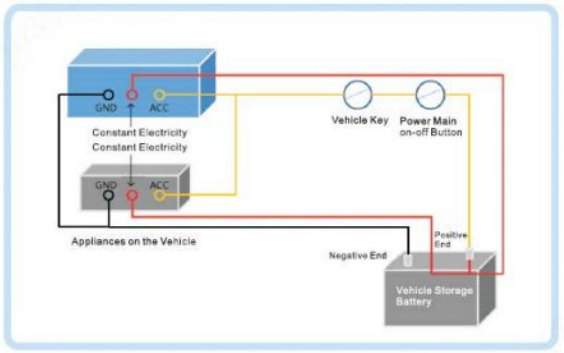
2.7 - Connecting Power

Note: Connect power only when the Key is set to **OFF** position.

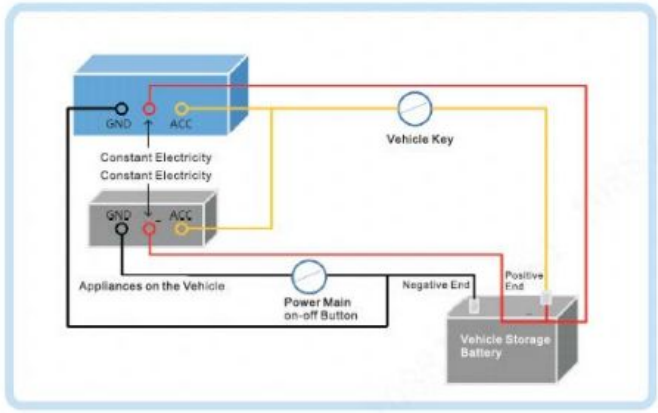
1. Note the Power Cable connections. Connect one end of the power cable to the power port of the device (the left port in the figure) or directly use the power cable from the device.
2. Connect the other end to the vehicle battery (the right port in the figure).
3. The **red wire with fuse is positive pole** of the power (normal live).
4. The **black wire is the grounding** cable. The **orange wire is the ACC signal** (Key live).



- Vehicle main power switch installed on the positive pole of the vehicle battery



- Vehicle main switch installed on the negative pole of the vehicle battery

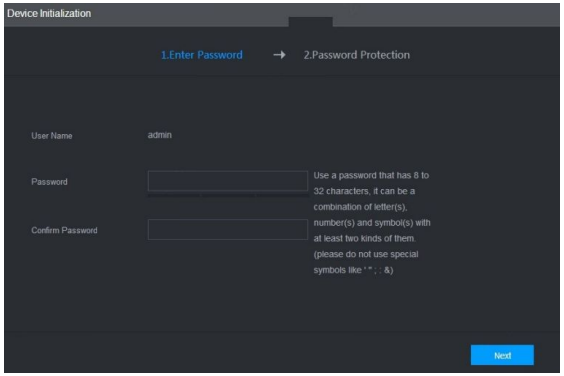


3B. Startup and Initialization

3.1- User Interface Access

Once the MNVR is powered (Key on **ACC** or **ON**) and the HDD lock is engaged, you can access the interface via HDMI port in the back of the unit or using the Web UI (Requires laptop and ethernet cable plugged into the front).

- Press the side panel on the front of the NVR to open it and access the RJ45 Network and USB port. You can plug in a mouse in the USB if accessing via HDMI. Plug in an ethernet cable from the NVR RJ45 port to a laptop if accessing the web UI.
- The MNVR will be on 192.168.1.108/199 by default.
- When first accessing the MNVR, you will be prompted to create a password for the **admin** account.

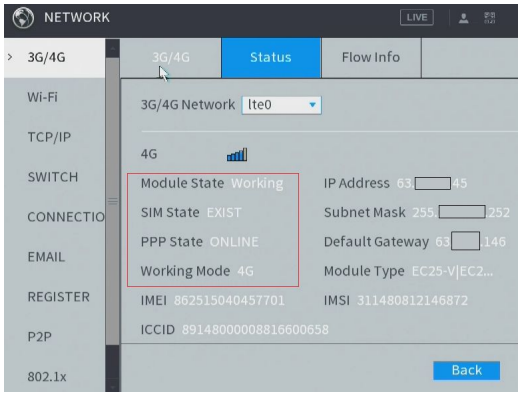


3.2- SIM Card Status

The MNVR IMIEE will be required to create a mobile data plan and link with a SIM card.

- If using 4G, make sure the 4G antenna is installed.
- The IMIEE of the MNVR can be located from **Main Menu > Info**

If equipped with an activated SIM card, you can check the Status under **Main Menu > Network > 3G/4G**



3C. Adding IP Cameras:

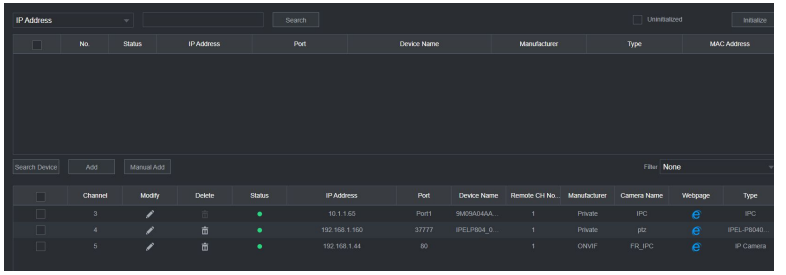
3.3- Connecting IP Cameras

The MNVR is equipped with standard PoE ports (PoE+/ Hi PoE are not supported) for IPC camera connection. Cameras plugged into the MNVR PoE will be assigned a 10.1.1.X IP from the NVR internal switch and will occupy channels 3-6.

- Cameras will be plugged into the RJ45 breakout cables from the back of the MNVR. See the **Red** arrows below.

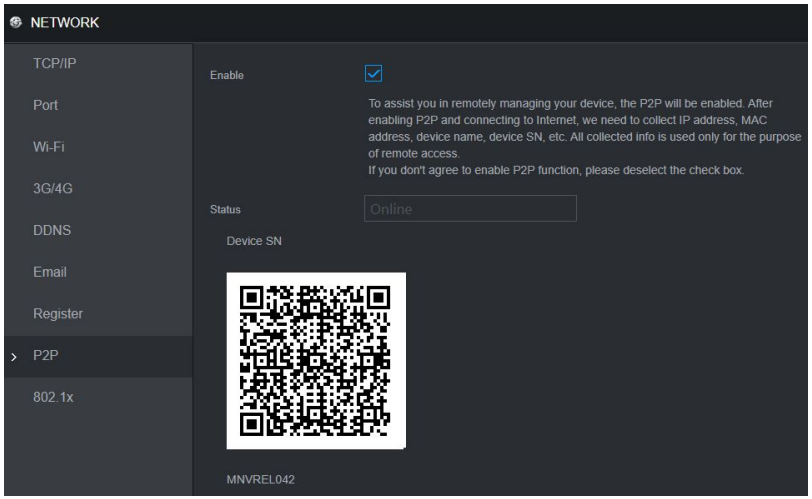
- The MNVR comes with RJ45 connection protectors. They are recommended to be installed as shown below.

- IC Realtime cameras are recommended for the MNVR as they are plug and play.
- Cameras should be set to **DHCP**. If initialized already, the cameras are recommended to be setup with the same login credentials as the NVR.
- For remote device management, access the MNVR **web UI** and go to **Main Menu,** Click **Setting** > **Camera** > **Camera List** to view the camera management section.

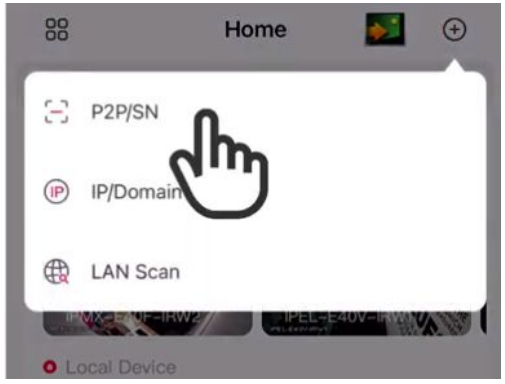


4A. P2P setup to Phone App:

- Log in to the local or web interface and select **Main Menu> NETWORK>P2P.**
- Enable the P2P checkbox. The Status should be: **Online**.

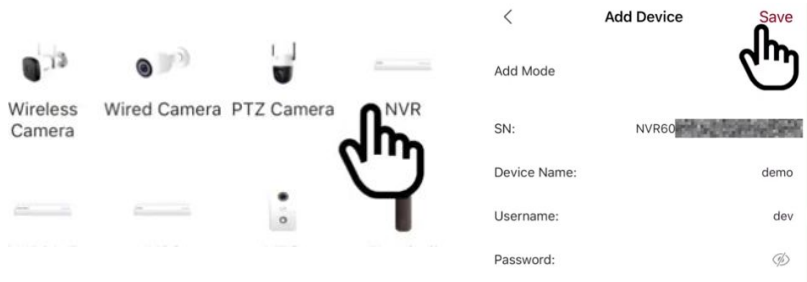


- Open the phone app (**IC View+**). On the Home Page, tap on the "**+**" icon on the upper right then tap on **P2P**.



- The app will use your phone camera to scan for the QR code or you can input the Serial Number manually.

- Select the Device type (**NVR**).
- Input the correct username and password as well as a device name to identify the recorder. Tap on **Save** to connect to your Recorder.

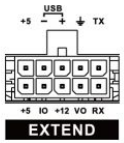


4A. MNVR Port Explanations

- VGA Interface

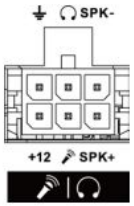
No.	Function	No.	Function	No.	Function
1	+12V/1A output	5	Audio output	9	VGA line sync
2	Ground line	6	VGA_B	10	VGA line sync
3	VGA_G	7	VGA_R	-	-
4	RXD_232	8	TXD_232	-	-

- Extension Ports



Name	Function
+5	USB +5V (bottom line)
+5	USB +5V (upper line)
-	USB data- and USB data+ that connect to USB port.
+	
IO	Reserved, used for expand customization.
+12	+12V/1A output.
⏚	Ground
VO	AV video output
RX	RS-232 serial port sender and receiver that connects to RS-232 port
TX	

- Audio/ Voice Ports



Name	Function
+12	+12V output
⏚	Ground
	Mic In that can connect to microphone.
	Mic Out that can connect to earphone.
SPK+	Speak positive pole
SPK-	Speak negative pole

5A. FAQ

P2P says Offline even though I followed the steps in the guide	The machine may not have pulled an IP address from the router/ SIM. Verify all cables are installed securely and SIM card carrier is activated with an active plan through Verizon. You can also change the DNS servers to DHCP instead of the default 8.8.8.8
I want to access my recorder from my phone	You can download our free app from the Play Store or the App Store. Search IC Realtime and you'll get results for IC View+
Can I set up the machine without a display connected?	Yes. You can access the MNVR configuration page from a computer by typing its IP address into a web browser or P2P. MNVR must be connected via Ethernet or a remote SIM plan.
I can not login through the web browser	IC Realtime recorders that are not HTML5 compatible have to use Internet Explorer to initialize the plugin. If you're already using Internet Explorer, reinstall the plugin by deleting the "*webrec*" and "*webplugin.exe*" folders within *C:\Program Files and/or C:\Program Files (x86)* see here for more information
My IP cameras won't connect/ show image	You may need to Initialize the camera before the NVR can connect to it. This is done in the Registration section or by logging into the camera Web GUI. See here for more camera registration information: Remote Device Registration
I need more in-depth help regarding configuration	IC Realtime has a Help Center that covers a variety of topics: https://icrealtime.com/help-center/categories

5C. Appendix: 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.**

Here are some recommendations:

- 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 include the account name or the account name in reverse order
- Do not use continuous characters such as 123, abc, etc.
- Do not use repeated characters such as 111, aaa, etc

2. **Update Firmware and Client Software in Regularly**

- 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:

- **Physical Protection.** We suggest that you ensure physical protection to equipment, especially storage devices. For example, place the equipment in a special computer room and rack cabinet, as well as implementing strong 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.
  -
- **Change Passwords Regularly.** We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.

- **Maintain and Update Password Reset Information.** The equipment supports password reset function. Please set up related information for password reset, including the end user's mailbox and password protection questions. If the information changes, please modify it accordingly. When setting password protection questions, it is suggested not to use those that can be easily guessed.
  -
- **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

- **Change Default HTTP and Other Service Ports.** It is recommended 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.

- **Enable HTTPS.** It is recommended to enable HTTPS, so that you visit Web service through a secure communication channel.

- **Enable Whitelist**. It is recommended 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.

- **MAC Address Reservation/ Binding.** It is recommended to bind the IP and MAC address of the gateway to the equipment, thus reducing the risk of ARP spoofing.

- **Assign Accounts and Privileges Responsibly.** In accordance to business and management requirements, add users and assign a minimum set of permissions to them.

- **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

- **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.

- **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.

- **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

- **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.