Network Video Recorder 1U POE KIT

Quick Start Guide V.1.02

Table Of Contents

Getting Started

A. Inspecting the Components 1

B. Rear Panel Identification 2

Device Setup

A. Booting Up 3

B. Device Initialization 3

C. Startup Wizard 4-5

Web Operation

A. Accessing Web Interface 5

Remote Access

A. P2P setup to Phone App 6

AI and IVS

A. Intelligent Motion Detect (iMD) 7

B. Perimeter Protection 7

C. Onboard POE Information 8

Appendices 8-9

A. FAQ

B. Cybersecurity Recommendations

www.icrealtime.com

IMPORTANT SAFEGUARDS AND WARNINGS

Operating Requirement

- Install the PoE front-end device indoors.
- The Device does not support wall mount.
- Do not place and install the device in an area exposed to direct sunlight or near heat generating 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

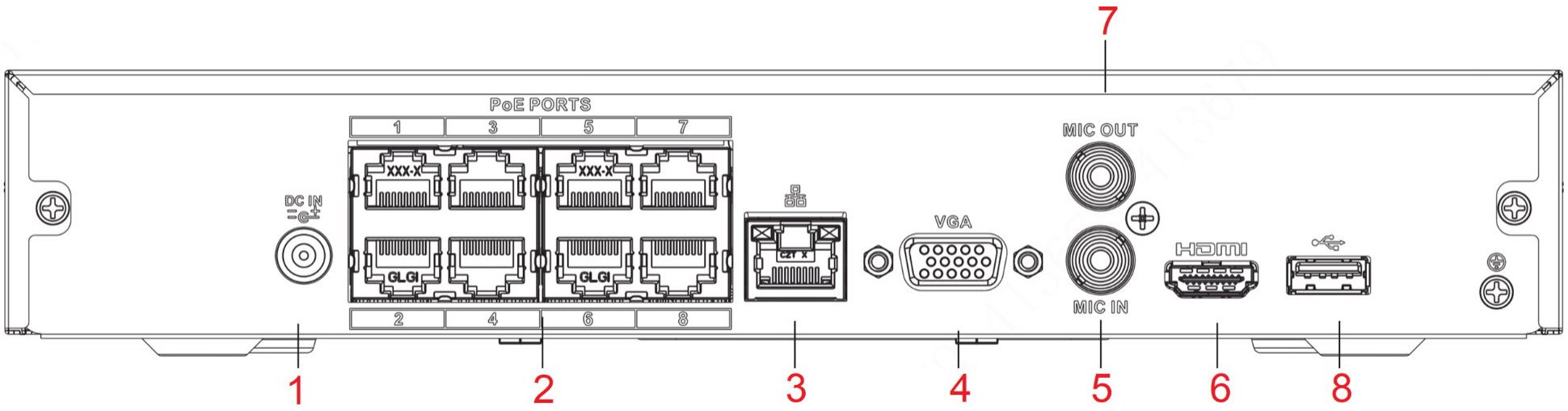
- Improper battery use might result in fire, explosion, or inflammation.
- When replacing battery, make sure the same model is used.
- Use the recommended power cables in the region and conform to the rated power specification
- Use the power adapter provided otherwise, it may result in injury and device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

1B. Rear Panel Identification

The actual appearance may differ depending on the model purchased.



1. **Power Input Port**
2. **PoE ports (for IP camera connection; See Page 7, Section 5C)**
3. **Ethernet Port (to local network)**
4. **VGA Port**
5. **Audio Input**
6. **HDMI Port**
7. **Audio Output (for 2 way talk)**
8. **USB Port**

2A. BOOTING UP

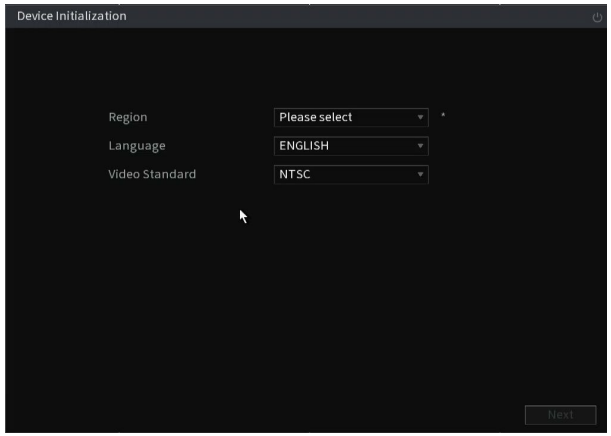
Prerequisites

- System is being supplied appropriate power.
- A network cable is connected to a router for local and remote access.
- A mouse and display are connected to the machine to interact with the menus.

2B. DEVICE INITIALIZATION

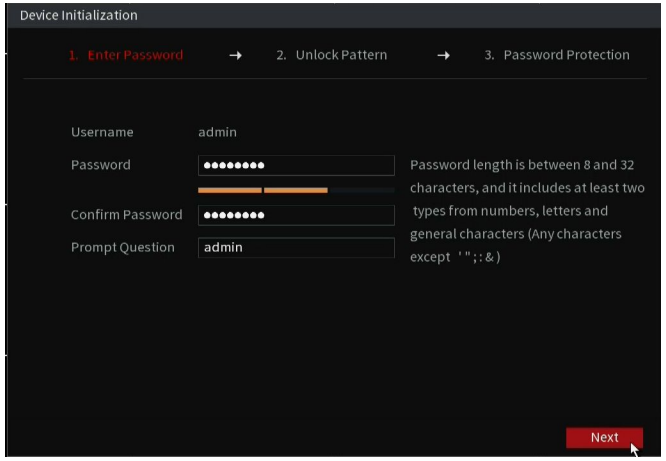
1.1 - Region Settings

- Select region and appropriate language then click next.



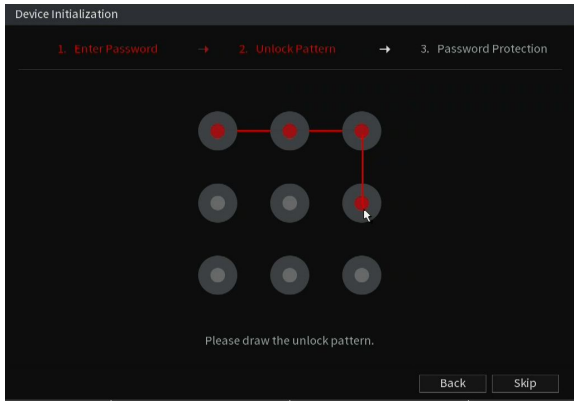
1.2 - Security

- Create a password at least 8 characters long and has at least two character types,
- A prompt question can act as a password hint.

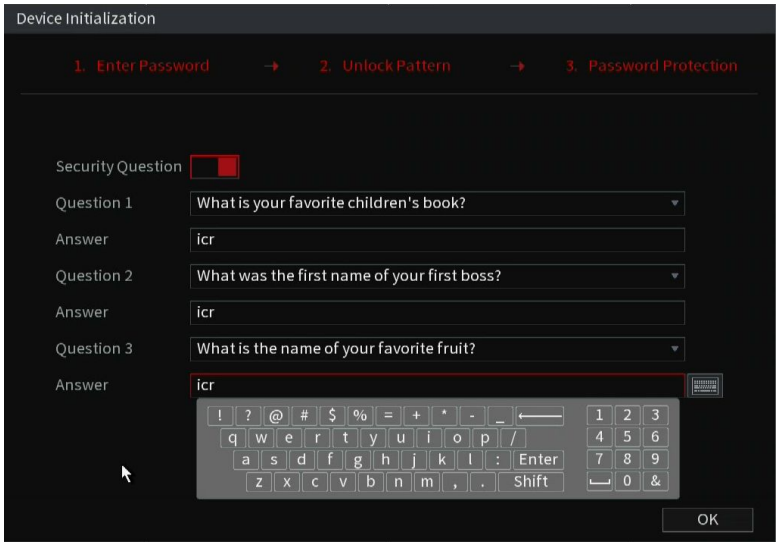


DEVICE INITIALIZATION (cont.)

- Draw an unlock pattern to use in place of a password.
- Click skip if you do not want to use an unlock pattern.



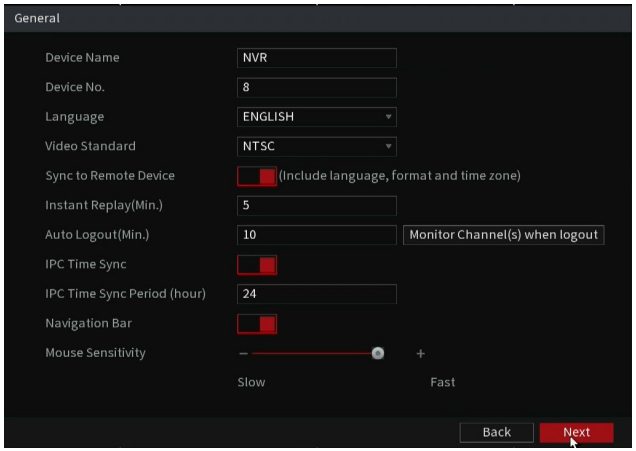
- Answer security questions to reset password in case password is lost.
- A factory reset will be necessary if the password was forgotten at a later date and security questions were not answered.



2C STARTUP WIZARD

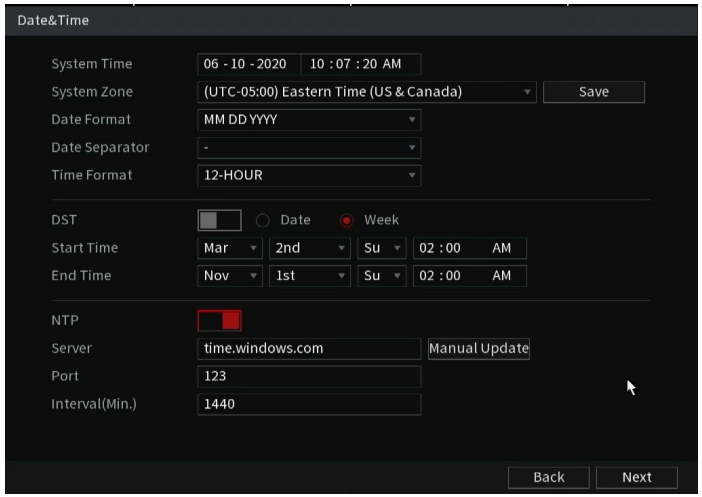
1.1 - General Settings

- General settings can be left at default.
- Change Auto Logout to 0 minutes to always stay logged in.
- *Monitor Channels when logout* controls the cameras that can be viewed when there is no user logged in the local interface.



1.2 - Timezone

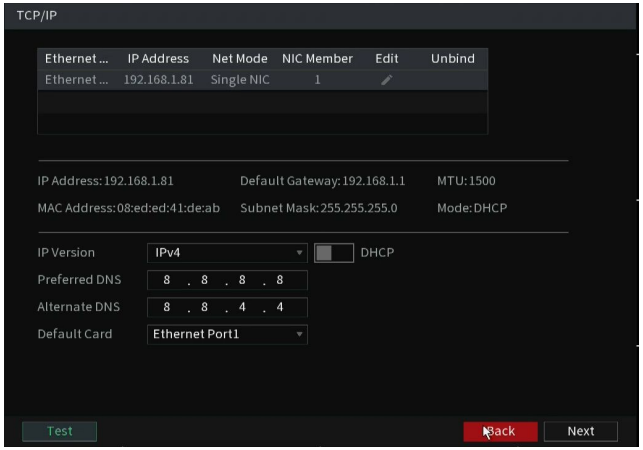
- Select appropriate time zone (UTC/GMT).
- Enable Daylight Savings Time (DST) if applicable. DST settings should be set to week with a start time of Mar 2nd Sun and an end time of Nov 1st Sun.



STARTUP WIZARD (cont.)

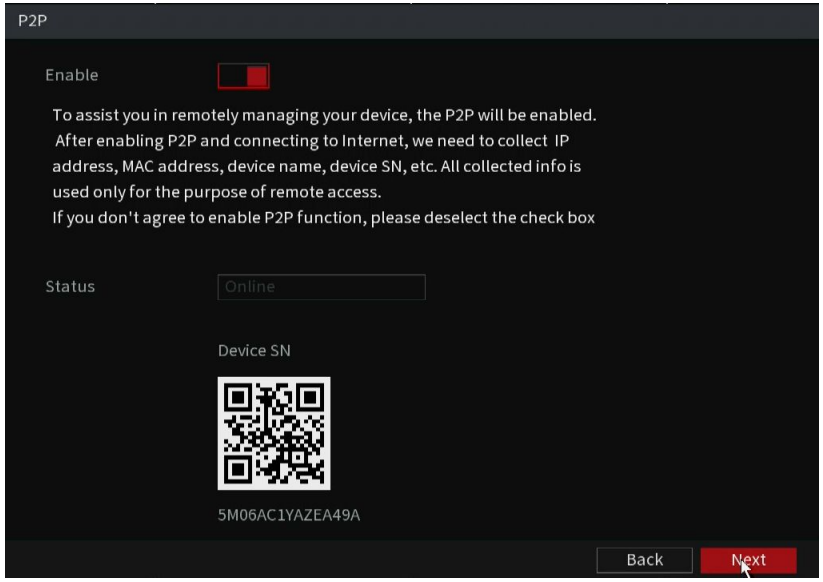
1.3 - Network

- Leave machine on DHCP so it gets assigned an IP address from the router. You may set on static after it has acquired an IP from the local network.
- Disable DHCP and program IP address manually if using a static IP address.



1.4 - P2P

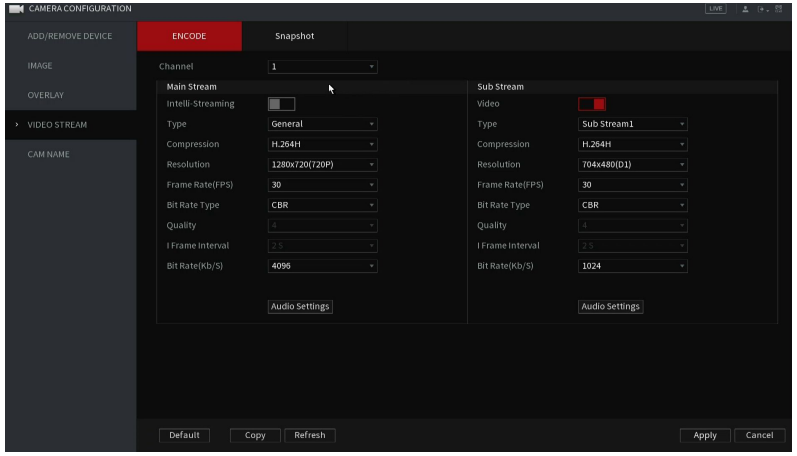
- Keep P2P enabled for easy remote access.



STARTUP WIZARD (cont)

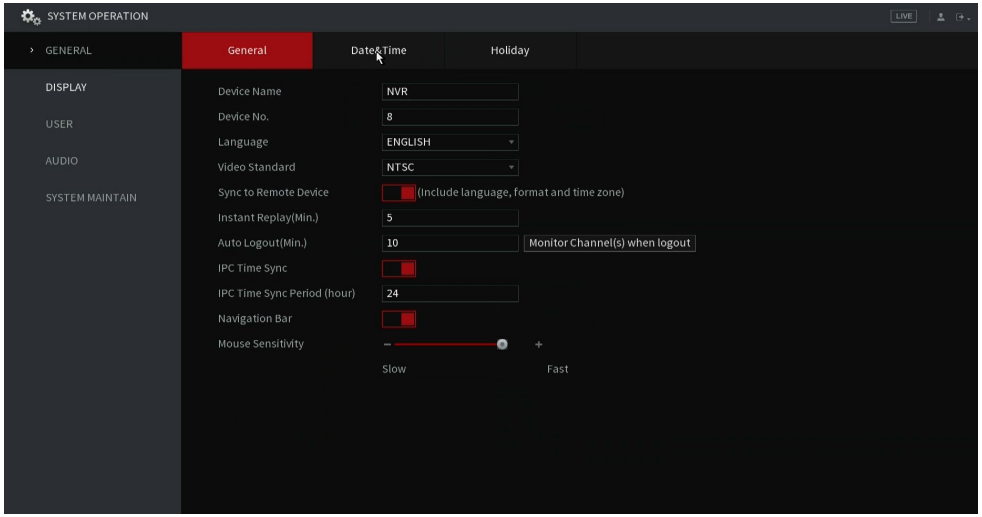
1.5 - Encode Settings (optional)

- Lower encode settings to optimize maximum recording time.
- Recommended values are: H.265, 15FPS, VBR, 6(Best).



1.6 - Basic (optional)

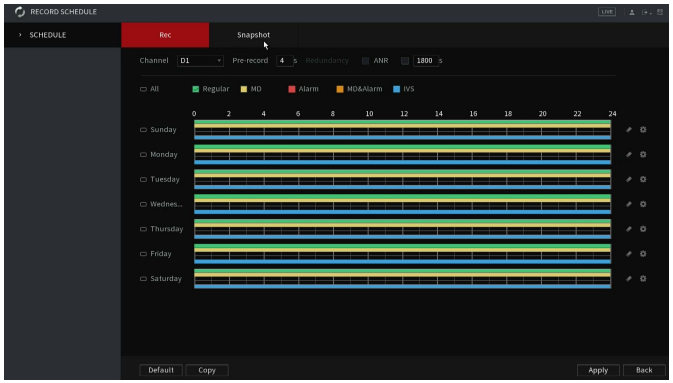
- Basic settings can be left on default.
- Auto delete old files only applies to system logs.



STARTUP WIZARD (cont)

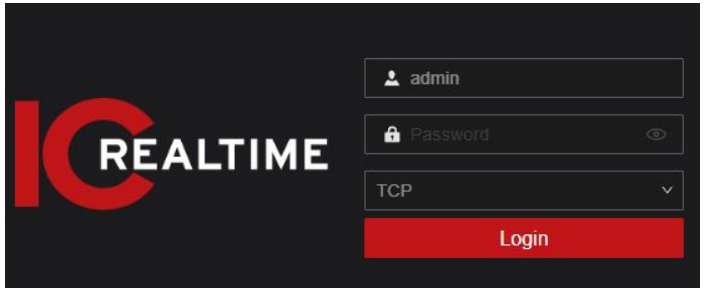
1.7- Record & Snapshot Schedule (optional)

- Click any of the setup icons to the right of the timeline
- Select the checkbox for Motion/MD within period 1 then copy settings to every day of the week.
- Use the copy button to apply settings to appropriate channels.



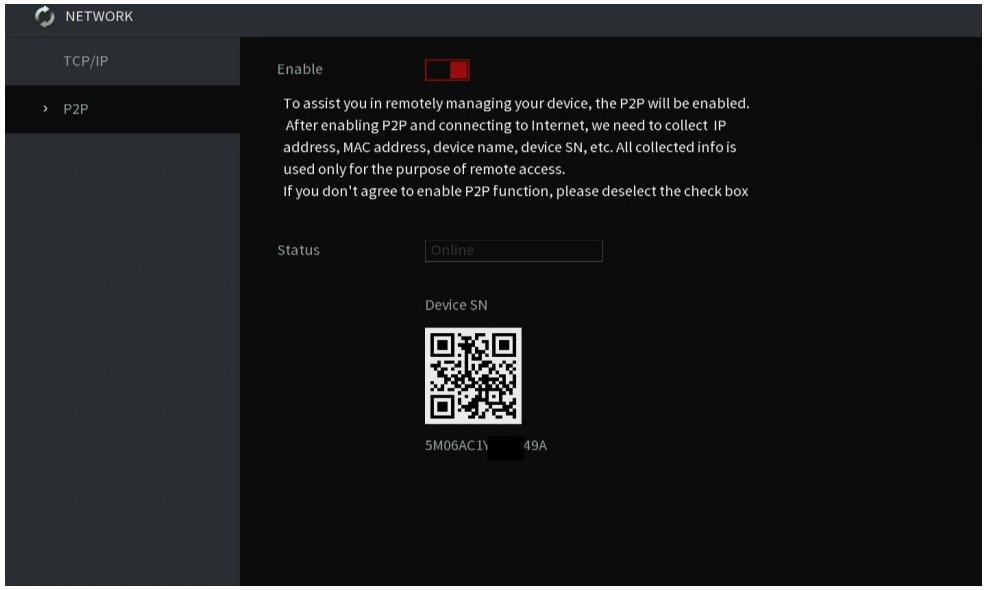
3A. Accessing Web Interface:

- Open the browser and enter the IP address of the Device into the address bar. Press Enter key. The Login interface is displayed.
- Enter the username (admin) and the password that was set up.
- Click Login.

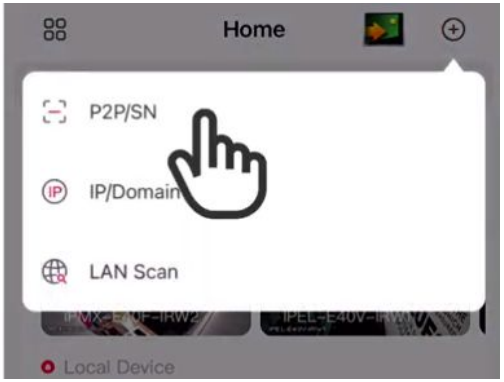


4A. P2P setup to Phone App:

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



- 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.

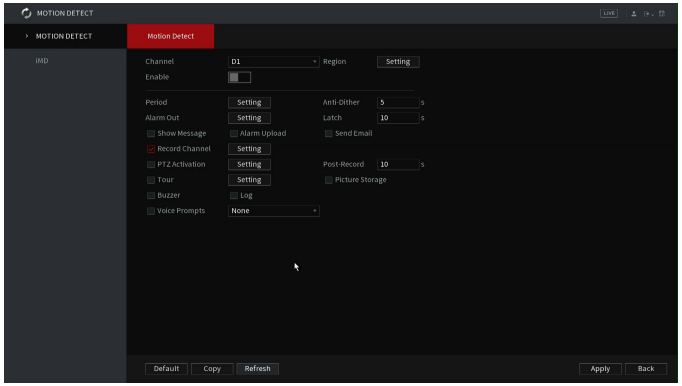
5A. Intelligent Motion Detect

Prerequisites

- Only IC Realtime cameras with Intelligent Motion Detect are compatible with this feature on the NVR
- A mouse and display are connected to the machine to interact with the menus or you are accessing via Web Interface. (See Section 3A).

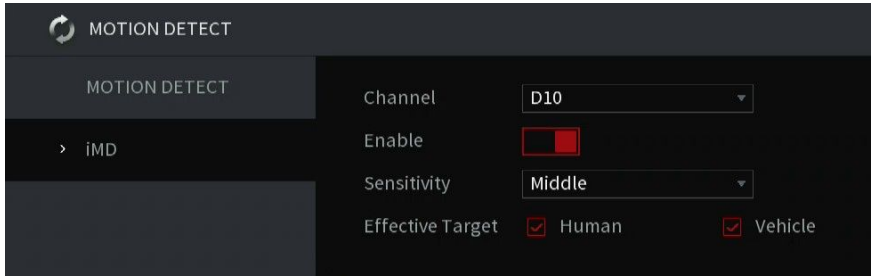
5.1 - Enabling Motion Detect

- Go to **Main Menu -> Basic Settings** then **Motion Detect**.
- Select the appropriate channel from the drop down and click "**enable**".
- Under Region, click "**Setting**." This section will allow you to mask off areas you do not want to trigger motion. Any area that is highlighted will trigger and areas that are transparent will not trigger motion. You can also configure the Sensitivity and Threshold.
- Click "**Apply**" when finished.



5.2 - Enabling Intelligent Motion Detect

- Go to **Main Menu -> Basic Settings -> Motion Detect -> iMD**
- Select the appropriate channel from the drop down and click "enable".
- You can check in whether you want motion detect to only trigger Human Targets, Vehicles, or both.
- Click "**Apply**"when finished.



5B. Perimeter Protection

Prerequisites

- Only IC Realtime cameras with Perimeter Protection are compatible with this feature on the NVR
- A mouse and display are connected to the machine to interact with the menus or you are accessing via Web Interface. (See Section 3A)

5.1 - Enabling Smart Plan and IVS

- Go to **Main Menu -> Advanced Settings -> Alert Center -> Intelligence** then **"Smart Plan"**.
- Select the appropriate channel from the drop down. Select the icon that looks light a light bulb for IVS. If you do not have this option, your camera may be incompatible.
- Click "**Apply**" when finished.

5.2 - Enabling Perimeter Protection

- Go to **Main Menu -> Advanced Settings -> Alert Center-> Parameters> IVS**
- Select the appropriate channel from the drop down and click "enable".
- Create and IVS Rules by clicking "+" then create a rule. See here for IVS setup.
- Under **Effective Target,** you can check in whether you want Perimeter Protection to only trigger Human Targets, Vehicles, or both.
- Click "**Apply**"when finished.

5C. Built-in POE Switch Information:

- The NVR's built-in POE is primarily **designed for use with IC Realtime cameras**. Third-party IPC plugged in via ONVIF are not guaranteed to work due to manufacturer's variance.

- Please check the specification sheet for the PoE budget of the NVR built-in POE. Be mindful when using devices that require more than standard POE, such as baluns or POE+/ Hi-POE cameras.

- Cameras plugged into the NVR poe should be set to **DHCP**. By default, the switch is in **Route Mode**, meaning it will automatically assign IP address to the cameras plugged in. The cameras will adopt a 10.1.1.X IP scheme. This scheme can be changed under **Settings > Advanced Settings > network > Switch.**

- **PoE ports are bound to corresponding channels**. For example, when an IPC is connected to PoE port 1, it will be assigned to Channel 1.

- If an IPC is connected to PoE port number in which the corresponding channel has been occupied (by manually adding another camera), the IPC plugged in to that port will be assigned to the next open channel

- **Bridge Mode** (only available in some models) allows the network port and the POE ports to be on the same network segment. Cameras plugged into the built-in POE will acquire IP from the local network (that is plugged into the network port of the NVR). Do not connect a switch/ router to the NVR built-in POE. For models that support **Bridge Mode**, this can be toggle under **Settings > Advanced Settings > network > Switch.**

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. Verify all cables are secure and there is link light activity on the Ethernet Port. 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 or premium version of the app from the Play Store or the App Store. Search IC Realtime and you'll get results for IC View (free) and ICRSS Pro (premium).
Can I set up the machine without a display connected?	Yes. You can access the machine's configuration page from a computer by typing its IP address into a web browser.
I cannot 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 Time**
   - According to the standard procedure in Tech-industry, we recommend to keep your equipment (such as NVR, DVR, IP camera, etc.) firmware up-to-date to ensure the system is equipped with the latest security patches and fixes. When the equipment is connected to the public network, it is recommended to enable the "auto-check for updates" function to obtain timely information of firmware updates released by the manufacturer
   - We suggest that you download and use the latest version of client software.

"Nice to have" recommendations to improve your equipment network security:

- **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.