

NVR Quick Start Guide

Version 1.0.0

Contents

Hardware Setup 6
NVR Initialization 7
Main Menu Overview 11
Adjusting Camera Settings for Maximum Resolution, FPS, and Bitrate 12
IVS, Motion Detection, and Recording Setup 13
Setting Up Email Alerts 15
Setting Up AI Events 19
Playback 26
Computer Access Setup 26
Remote access not working? (Troubleshooting steps) 28
Amcrest View Pro 2 Setup 29
References & Contact Information 31

Welcome

Thank you for purchasing an Amcrest NVR.

Before installation and operation, please read the below safeguards and warnings carefully.

This document provides a quick setup and overview of your Amcrest NVR and its features. **For access to a full user manual or further information regarding your device please visit:** http://amcrest.com/support

Important Safeguards and Warnings

- All installations and operations of the device should conform to your local electrical safety codes.
- We assume no liability or responsibility for any of the fires or electrical shocks caused by improper handling or installation.
- We are not liable for any problems caused by unauthorized modifications or attempted repair.
- Do not submerge the device in water or install in areas with high levels of moisture or humidity.
- Handle with care, avoid dropping or placing the device in unsecure areas.
- The NVR does not have rack mount compatibility and should be used on flat surfaces.

Check Packaging

When you receive the NVR system in the packaging, unpack it, and check all sides of the NVR to see if there is any physical damage. The protective materials used for the packaging of the NVR will protect most accidental damage during transportation, but to ensure that your equipment is operating as expected, it is recommended to inspect the product before proceeding.

On the NVR, check that the label on the bottom is not damaged. The serial number and model number of the unit is needed to add the device to other Amcrest applications.

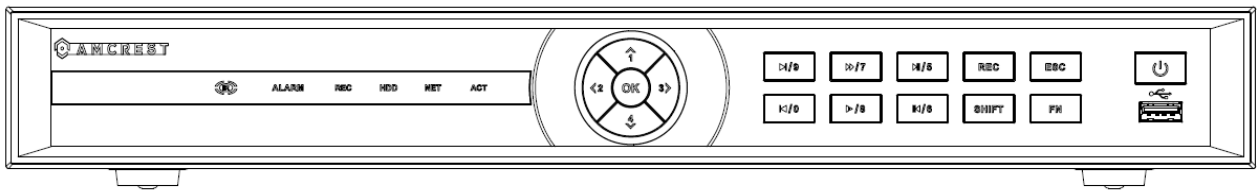
Please note that most Amcrest cameras come defaulted to H.264 encoding for maximum compatibility when accessing your device in a web browser, or other third-party applications. However, for optimal performance, the device's compression and bitrate can be updated to H.265 compression after the device has been initialized.

H.265 provides a more advanced technology than H.264 and allows the device to reduce file sizes which in turn helps to reduce required bandwidth without sacrificing frames per second (FPS) or resolution.

For more information on adjusting compression and bitrates, please refer to page 18, "*Adjusting Camera Settings for Maximum Resolution, FPS, and Bitrate*".

Front Panel

NV42XXX-EI Series



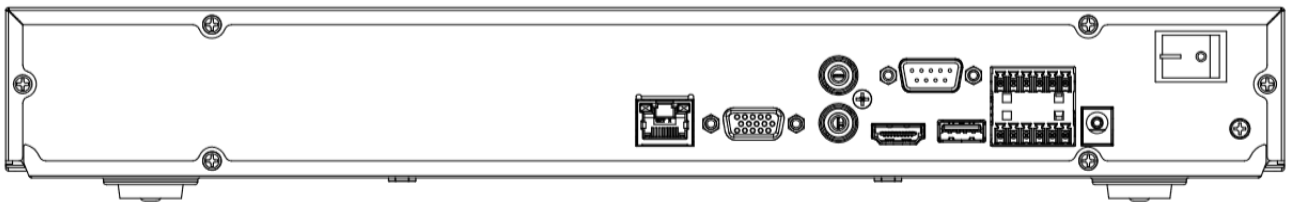
Button	Icon	Description
Power Button		Press and hold this button for five seconds to shut off or power on the NVR. Use the switch on the back of the NVR to initially power the device.
USB		Front panel USB 2.0 Port.
Up/1, Down/4	▲、▼	Activate current control, modify setup, move up and down in a menu Increase/decrease numeric functions. Tilt camera up and down using PTZ menu (if applicable).
Left/2, Right/3	◀、▶	Move left or right in a menu. When viewing playback, use these buttons to scan forwards or backwards.
Enter	OK	Confirm a current operation Go to default button Go to menu
Escape	ESC	Go to previous menu or cancel a current operation. When using playback, used to restore real-time monitor mode.
Record	REC	Manually stop/start a recording. Use the directional keys or numeric keys to select the recording channel.
Shift	SHIFT	In a textbox, click this button to switch between numeric characters or provide capitalization to a word, etc.
Play/Pause/5	▶ II	Click this button to pause or resume playback. In text mode, input number 5.
Reverse Playback/ Pause/6	II ◀	During playback or pause mode, click this button to reverse playback. In reverse playback, click this button to pause. In text mode, input number 6.
Fast Forward/7		Various fast speeds and normal playback. In text mode, input number 7
Slow Motion/8		Multiple slow play speeds or normal playback. In text mode, input number 8.
Next/9	▶|	In playback mode, press to playback the next video. In menu setup, go downward in a dropdown list. In text mode, input number 9.
Previous/0	|◀	In playback mode, press this button to playback the previous video. In text mode, input number 0.

Function	FN	One-window monitor mode, click this button to display assistant function: PTZ control and image color. Backspace function: in numeric control or text control, press and hold for 2 seconds to delete the previous character before the cursor. In motion detection setup, working with FN and direction keys to realize setup. In text mode, press this button to switch between numeric, capitalization, etc.

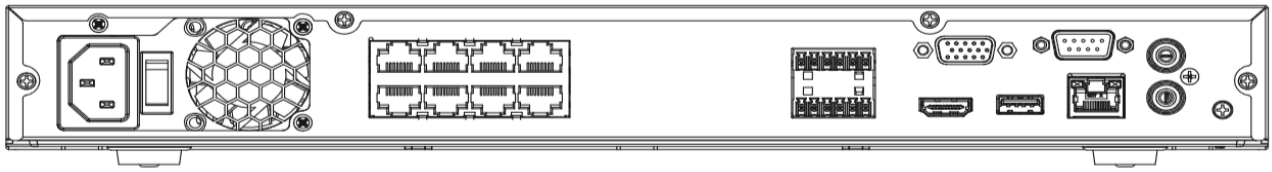
Rear Panel

The rear panel of the NVR may differ from model to model.

Non-PoE ports



PoE Ports.



	USB 2.0 port	USB 2.0 port. Connect a mouse, USB storage device, etc.
	Network port	10M/100Mbps self-adaptive Ethernet port.
HDMI	HDMI Output	High-definition audio and video signal output port.
VGA	VGA video output port	VGA video output port. Outputs analog video signal. This connects to the monitor to view analog video.
	GND	Ground end
	Power Port	DC12V, DC48V Depending on model.
MIC IN	Audio input port	Bidirectional talk input port. This is used to receive the analog audio signal from the device such as a microphone.
MIC Out	Audio output port	Audio output port. This is used to output the analog audio signal to devices such as an external RCA speaker. Bidirectional talk output. Audio output on 1-window video monitoring. Audio output on 1-window video playback.
PoE Ports	PoE ports	Built-in switch on certain compatible devices. For PoE series products, you can use this port to provide power to a PoE camera.

Hardware Setup

Before setting up the NVR, you will need the following items. These items may not be included:

A computer monitor, or TV with either an HDMI or VGA input
A power strip with room for 4 large power plugs
A hard drive for storing video recordings.
A USB flash drive formatted to FAT 32 for importing/exporting configure or image files.

It is recommended to connect all components *before* mounting any of the cameras. This is to ensure all components are working properly before they are physically installed. If any components are not functioning, please contact Amcrest Support: https://amcrest.com/contact

There will be two parts to this section:
Hard drive installation
Setting up the cable connections

A hard drive must be installed to record or save *any* footage. If no hard drive is installed, you can only view the cameras from the NVR. If a microSD card is installed in the camera, you can still view the recordings from the microSD card using the Amcrest View Pro application and accessing the camera directly, however, no recordings will be retained to the NVR if a hard drive is not installed.

Hard drive installation

A hard drive can be installed if you want to record and save data to the NVR. Having a hard drive allows you to configure and use the recording functionality of the NVR to store and view AI events.

The hard drive used in these NVRs must be no larger than 16TB (Terabytes). For more information, please review the technical specifications or visit: https://amcrest.com/support

To install your hard drive, the following is needed:

A medium sized (regular) Phillips-head screwdriver - *not included.*
A hard drive - *not included.*
Four hard drive fastening screws – *included.*

Note: **Before installing the hard drive, make sure the NVR is powered off with the power cable disconnected.**

1. Loosen the screws of the upper cover and side panel using a Phillips head screwdriver.
2. Attach the four screws hard drive screws to the hard drive (sold separately). Do not overtighten, only turn a max of three times.
3. Place the hard drive into the NVR in accordance with the four holes at the bottom of the NVR casing.
4. Turn the NVR upside down and tighten the hard drive screws firmly to the casing of the NVR.
5. Connect the hard drive cabling and power cables to the hard drive.
6. Put the cover back onto the NVR in accordance with the clip and secure it back onto the NVR.

Setting Up the Cables

The following instructions will show you how to set up the cables for the NVR, cameras, as well as a monitor or TV screen.

To set up the cable connections, there are 5 steps:

1. Connect a monitor or TV screen to your NVR. The NVR is compatible with any monitor or screen that uses a VGA or HDMI connection. For the purposes of this guide, we will use a VGA connection. Take a VGA cable and connect one end to the VGA port on your monitor/screen and the other end to the VGA port on the back panel of your NVR.
2. Connect an Ethernet cable to your router.
   Then, connect the other end of the cable to the Ethernet port on the back of the NVR.
3. Connect the cameras to the same network as the NVR ensuring the cameras are properly connected and powered via the network. Please note, if using a model with POE connections on the back, connect the POE cameras directly to the back of the NVR using an Ethernet cable.
4. Connect the NVR's power adapter into the power port on the back of the NVR.
   Note: If your NVR has a 3-prong power cord, connect the input of the cord into the power input of the NVR.
5. Connect the other end of the power cable into a wall outlet or power strip to turn on the NVR. Some models may feature a power switch on the back which may need to be turned on to power the device.

NVR Initialization

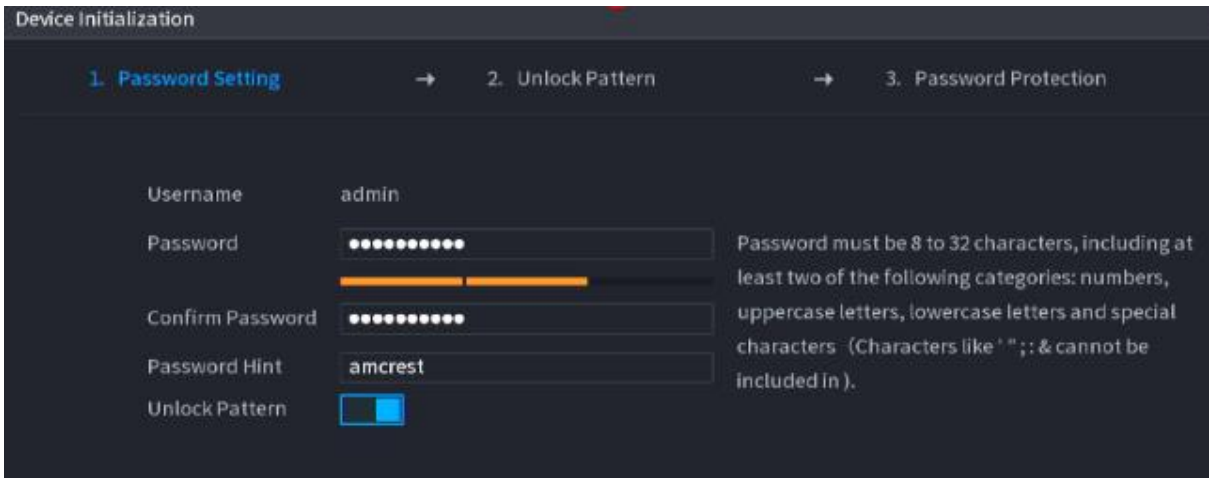
After applying power to the NVR, the system will turn on. Allow the NVR to finish loading. The **Device Initialization** screen will appear. Please note, the initialization screen may be different than what is displayed based on the model you are using however the same concepts will apply. Select your location, language, and video standard then click **Next** to continue.

Select your time zone as well as current date and time. Click **Next** to continue.

Enter Password

Create a new admin password for your NVR. The password for your device should be between 8 and 32 characters. A combination of letters, numbers, and symbols are recommended when setting up your password.

Note: Please do not use special symbols like ' " ; : &



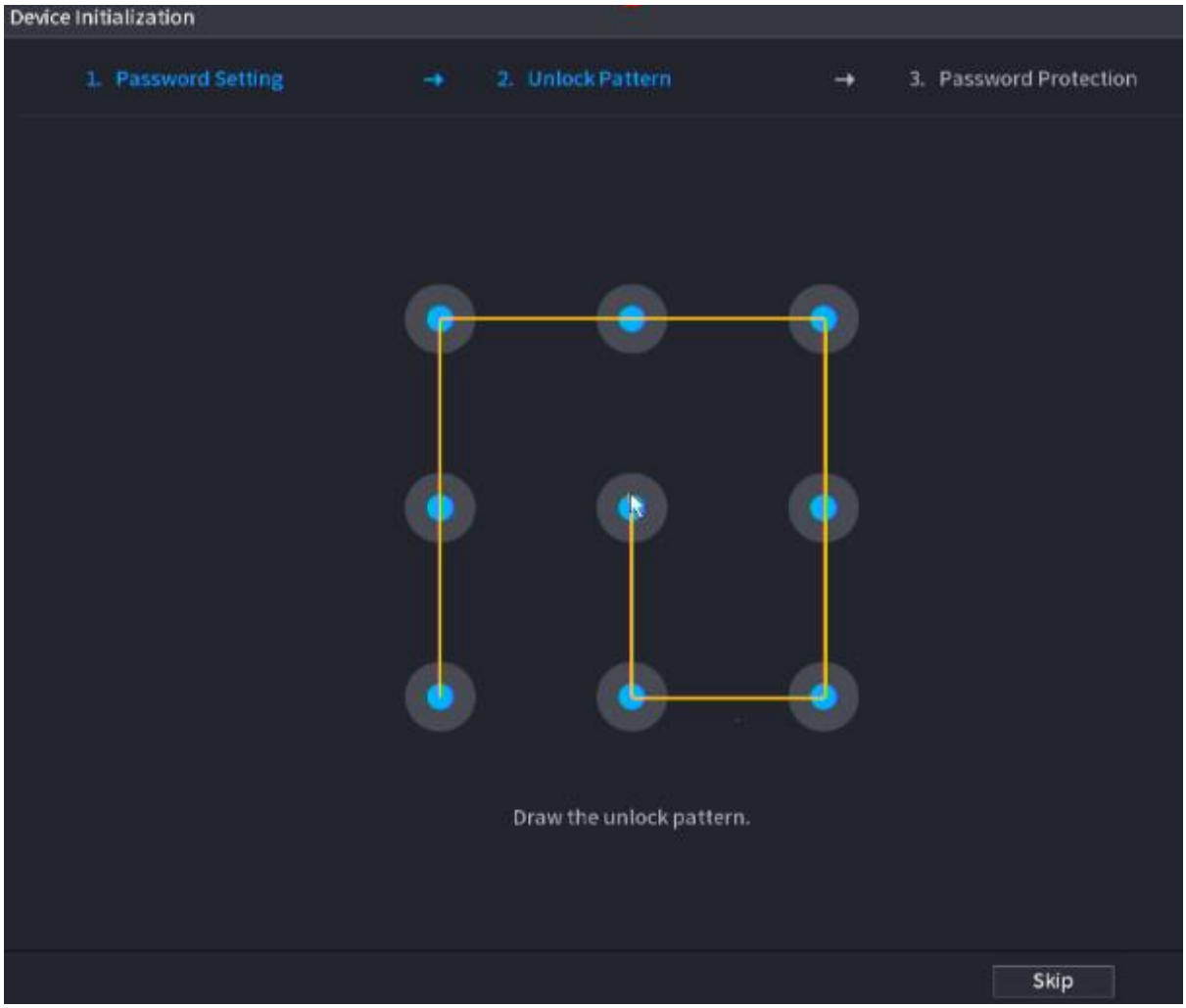
Once you have entered a new password for your device, confirm the password in the next field.

Lastly, you will be asked to enter a prompt question for your account. This is useful if you have forgotten your password and would like an easier way of recovering your password. Please use a prompt question that will help you remember the password for your device.

After you have completed this section, click **Next** to continue.

Unlock Pattern

This is an optional security measure for your device and is only available in the local user interface. To set an unlock pattern, use your mouse to draw a design that you will remember**.** Draw the pattern again to confirm. If you do not want to assign an unlock pattern, you can click '**Skip**' to skip this process.

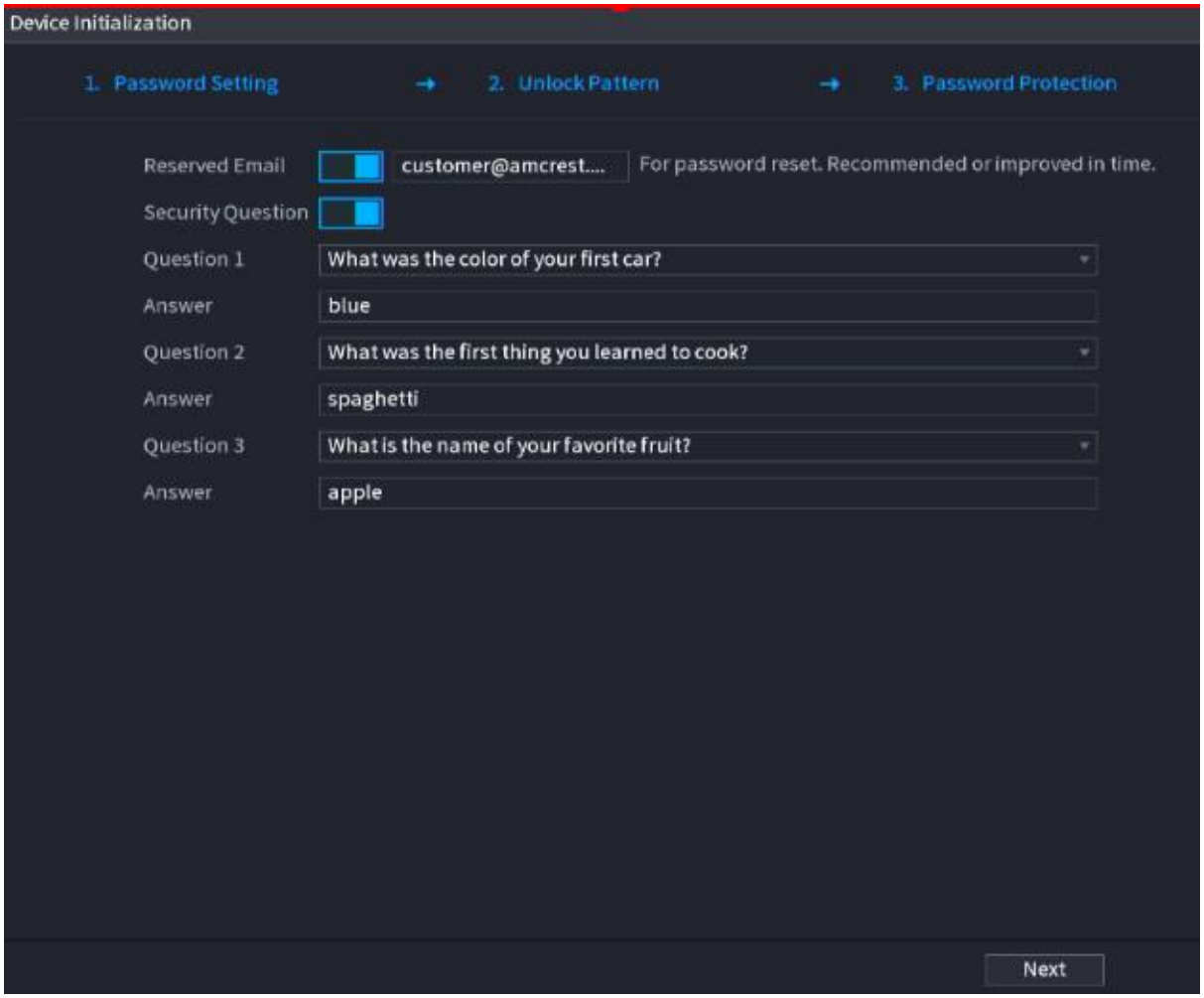


If you have been assigned an unlock pattern, you will need to draw the pattern again to confirm your assigned unlock pattern.

Password Protection

Additional means of password protection and retrieval can be set up in this menu. If you would like to reset your password using your email, make sure the email address checkbox is enabled and enter a valid email address in the **Email Address** field. The email address will be retained in the system.

If you do not want to use an email address, you can disable the email address option. As a secondary means of recovering your password, you can apply security questions to your NVR. To add a question, select a question from the drop-down menus for **Question 1, Question 2,** and **Question 3** and enter the answers to those questions in the **Answer** fields.



Once this section is complete, click on the **Save** or **Next** button to save your information to the device.

Startup Wizard Walkthrough

The first page of the Startup Wizard will appear which allows you to setup any General, Network, Remote Devices, and Record Control Settings for the NVR. By default, the NVR's IP address will be set to DHCP which means your network has already automatically assigned an IP address to the NVR. For optimal performance it is highly recommended to set the device IP to static to ensure the IP of the device does not change. To set the device to a static IP, click on the **Modify** (pencil icon) for the NIC card and disable the DHCP toggle switch to set the NVR's network mode to static. Click **OK** then click **Next** to continue.

Note: Most Amcrest products are H.265 compatible. H.265 provides more advanced technology than H.264 and allows the device to reduce file sizes which in turn helps to reduce required bandwidth **without sacrificing frames per second (FPS) or resolution**. However, for maximum compatibility when accessing your device in a web browser, or other third-party applications, our H.265 compatible products will come **factory default to H.264.**

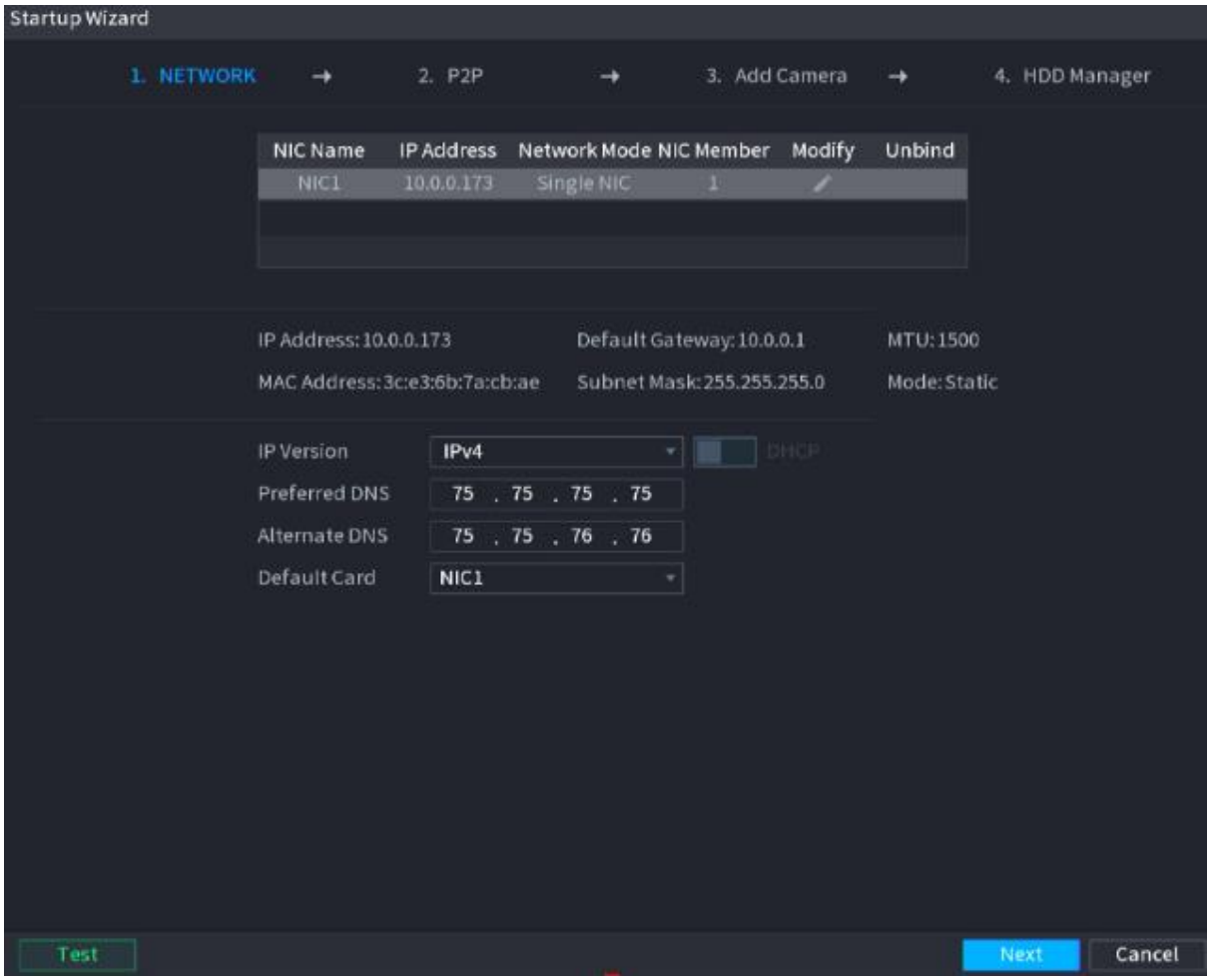
For optimal performance, the device's compression can be upgraded to H.265 during the camera registration process.

Network

Unless you have a specific reason to change these settings, it is best to leave them as they are. Please note, **the IP address for the NVR will be the address used to access your NVR's web user interface on a laptop or PC**, please disable DHCP to set the NVR to a static IP.

Click the **Test** to test the overall health and status of your network connection once complete, click the **Back** button to return to the previous menu.

To continue with the startup wizard, click **Next.**



P2P

The next screen that appears is the P2P screen. This screen allows you to connect your NVR to your mobile device via the Amcrest View Pro app. The P2P status should read as "Online". To download the app, use your mobile device's camera and scan the **Cell Phone Client** QR code. When using the app, use the SN QR Code for quick access to the serial number for your NVR.

Click the **Next** to continue.

Add Camera

The next screen that appears is the **Add Camera** screen. This is where you can begin adding cameras to the NVR. If the cameras are not directly connected to the back of the NVR, please make sure they are active and on the same network as the NVR before proceeding.

To begin adding a device, click on **Device Search** to allow the NVR to scan for connected devices on your network.

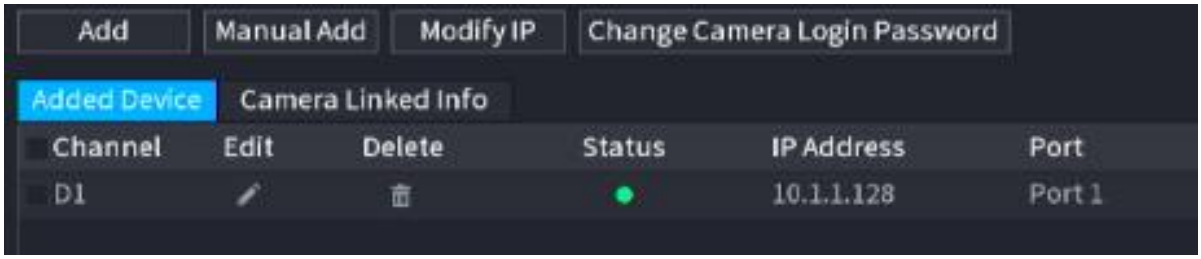
A list of applicable connected devices will show on the screen. Select your devices by clicking on the checkbox next to the device and click **Add** to add the device into the **Added Devices** menu.

If the status of your camera is red, it indicates the camera is not properly connected to the NVR. This could be because the password for the camera is not entered properly in the system.
To modify the password for your camera, click on the edit icon (pencil) located in the **Edit** column in the **Added Device** menu.

Select the **Password** field and use the onscreen keyboard to enter the password for your camera. Once the password has been entered, click **Connect** then click **Save** to continue.

Note: If this is a new device and a password has not been added the password will be **admin.**

Once the password has been properly set the **Status** indicator will turn green indicating the camera has been properly added.



As previously stated, our H.265 compatible products will come **factory defaulted to H.264 compression**, but for increased performance, the camera's settings can be automatically switched to H.265 compression. Switching to H.265 compression reduces bandwidth **without sacrificing frames per second or resolution**. To activate H.265 compression, click on the **H.265 Auto Switch**.

For more information on H.265 compression, please visit: amcrest.com/support

Click on **Next** to proceed.

HDD Manager

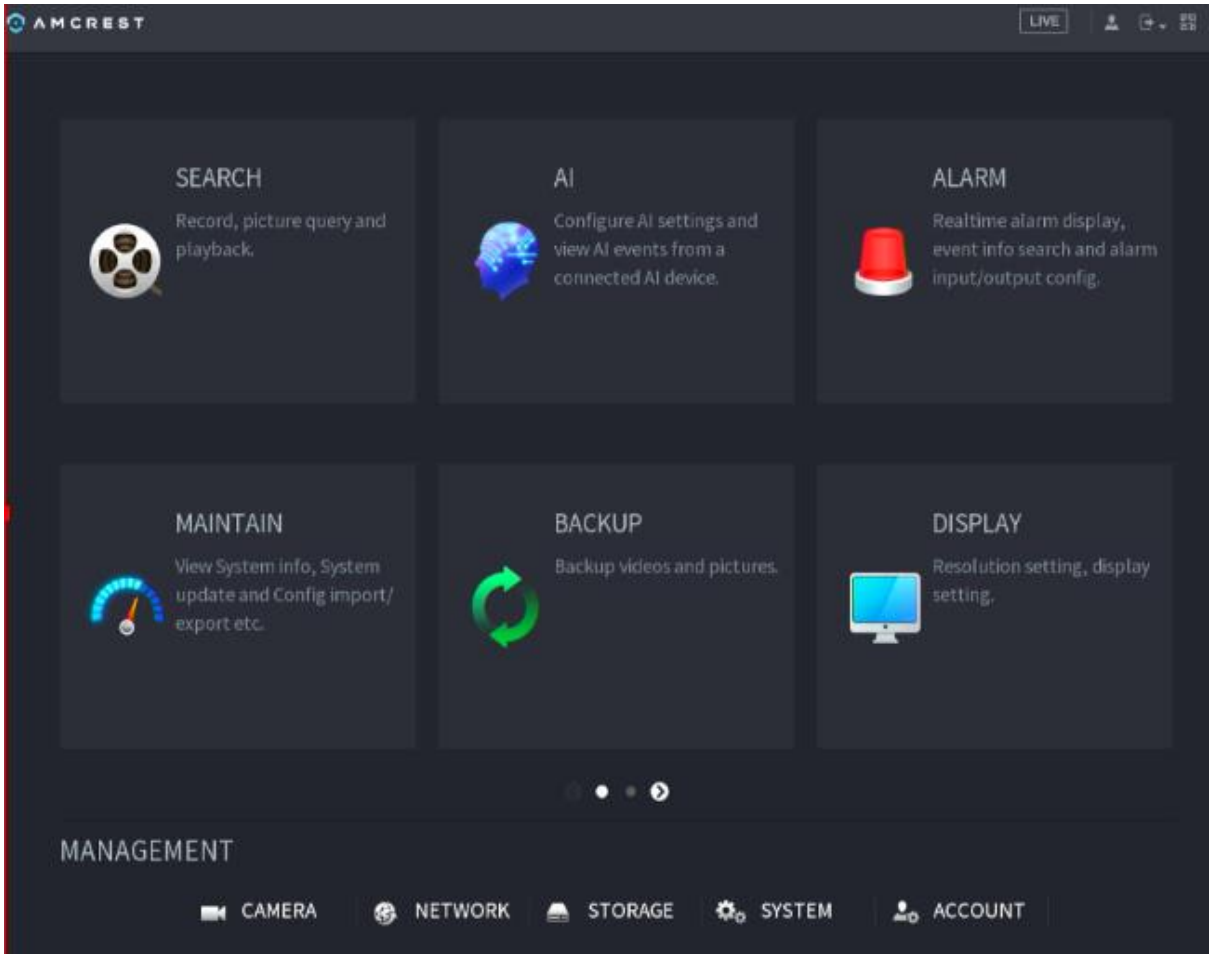
The HDD manager may not be applicable to all models however this screen allows you to view the status or format any hard drives that are connected inside the NVR. This is typically used for devices that have multiple hard drives.

To format a hard drive, select a hard drive from the list and click **Format**. Select the **Clear HDD database** toggle switch and click OK to proceed. Enter the NVR's password that you created previously and click OK. The NVR will then format the selected hard drive. If you would like to format other hard drives, please select the drive from the list and repeat the process.

The next screen you will see will be the video wall screen which will display all connected devices. Right click on the video wall and click on the '**Main Menu**' from the selections to access the main menu.

Main Menu Overview

The screenshot below is the main menu screen for the Amcrest NVR console interface:



Below are short descriptions for each of the menu items on the main menu:

SEARCH: View, search, and play recorded videos.
AI: Manage and view artificial intelligence and face recognition information and settings.
ALARM: View and search for live alarm information. Configure alarm event actions.
MAINTAIN: View system information, system updates. Import/export configuration files, etc.
BACKUP: Search and backup files using a USB flash drive.
DISPLAY: Configure resolution and display settings.
AUDIO: Configure audio announcements and import audio files.

Management

CAMERA: Add, search, review or edit settings for each camera, including video settings (e.g. quality, bit rate, color, etc.).
NETWORK: Review and edit TCP/IP, connection, DDNS, Email settings, etc. (e.g., P2P, UPnP, Multicast, etc.)
STORAGE: Set motion detection IVS schedules, as well as access the hard drive management interface, FTP, etc.
SYSTEM: Review and edit general system settings such as, video standards, date & time, as well as adjust firewall settings.
ACCOUNT: Add or remove shared user settings, groups, as well as ONVIF users. Reset security questions and update reset password email.

Adjusting Camera Settings for Maximum Resolution, FPS, and Bitrate

Most Amcrest products are H.265 compatible. H.265 provides more advanced technology than H.264 and allows the camera to reduce file sizes which in turn helps to reduce required

bandwidth **without sacrificing frames per second (FPS) or resolution**. However, for maximum compatibility when accessing your device in a web browser, or other third-party applications, our H.265 compatible products will come **factory default to H.264.** For optimal performance, the device's settings can be upgraded to H.265 compression if needed.

Please note, for higher performance as well when using H.265 compression it is recommended to adjust bitrate. The bitrate is the number of bits that are processed per unit time by the system and helps the system to create a tradeoff between bandwidth and image quality.

How to Adjust to H.265 Compression
If the auto switch for H.265 compression was not selected in the camera registration process, the setting can be adjusted manually. On the **Main Menu**, under **Management**, click on **Camera**.

In the **Camera** menu, select **Encode** and click on the **Compression** drop down menu and select **H.265**.

Click **Apply** to save your settings.

Adjusting Bitrate
Since H.265 compression uses roughly 30% less resources than H.264, the camera will typically come defaulted to a preset bitrate when switching to H.265. For instance, when switching to H.265 on a 4K camera, the bitrate may be defaulted to 8192 Kb/S, however, adjusting the bitrate to a lower value may help to increase the overall efficiency of the camera while viewing playback or watching live view.

To adjust the bitrate, access the **Encode** menu and click on the **Bit Rate (Kb/S)** dropdown menu. A list of preset bitrates will be displayed as well as a **Customized** selection which will allow you to set a customized bitrate if needed.

Please note, when using a 4K camera, it is recommended to keep the bitrate around **1792 Kb/S**, however, different values may be applicable depending on your specific network requirements. Please refer to the table below regarding recommended resolution and bitrates and custom thresholds.

Resolution	Recommended Bitrate	Custom Bitrate Threshold
2MP (1080P)	Default Settings	Default Settings
3MP	Default Settings	Default Settings
4MP	Default Settings	Default Settings
5MP	1536 Kb/S	1792 Kb/S
8MP (4K)	1792 - 2048 Kb/S	1825 Kb/S

Note: Adjusting the bitrate to anything lower than the recommended bitrates above may result in degradation to recordings or to live view. For the best results, if you are adjusting multiple cameras, it is highly recommended to adjust each camera **individually**. This may be a trial-and-error process since most network environments are unique and may vary, however, the bitrate should range between 1792-2048 Kb/S if using a 4K camera. An optimal customized bitrate should be around 1825 Kb/S. Click **Apply** to save the new bitrate settings.

IVS, Motion Detection, and Recording Setup

This section will cover how to set up a recording schedule for your NVR. This is applicable to regular (24/7 recordings), motion detection, and IVS recordings. IVS stands for intelligent video system analytics and is the basis for all AI rules associated with your device. This section will also cover how to set up a recording schedule, email alerts with snapshots, etc.

Note: **The NVR can only be set up to save recordings or IVS information if a hard drive has already been installed**. **However, email alerts with snapshots can still work without a hard drive installed.**

The following setup processes will be shown using the NVR's built-in interface. However, these same steps can also be done through the web interface on a computer. For more information on how to access your device from a web browser, please refer to section, *"Computer Access Setup".* Despite the difference in appearance, the settings pages have similar organizational structures.

Enabling Recording Options

This menu should be verified to ensure that all recording protocols are enabled. This menu details, per channel, which streams are enabled or disabled in the NVR. Please note, the interface shown may differ model to model, however the same concepts will apply. To access this menu, please refer to the information provided below.

1. On the main menu, click on **Storage**.

2. Click on **Record** or **Record Mode**. This menu displays all active channels and streams being used for recording. If using snapshots, ensure the **Snapshot** radio button is enabled on each stream. To apply the settings to all channels, click on the **All** radio button.

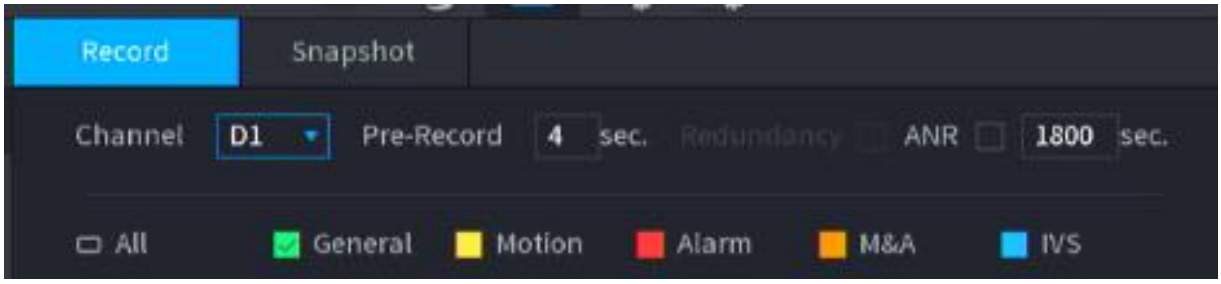
3. Click on **Apply** to save the settings to your device.

Setting Up Recording Schedules

1. From the Main Menu, click on **STORAGE** in the **MANAGEMENT** section:

Make sure you are on the **SCHEDULE** > **REC** page. This is where you can configure your video recording schedules. To configure a snapshot schedule, click on the **Snapshot** tab. All video events will be saved and accessible via the playback menu, if a hard drive is installed, whereas snapshot events can be emailed. For more information on how to set up Email snapshots, please refer to section, *"Setting Up Email Alerts".* By default, **Regular** (24/7), **MD** (Motion Detection) and **IVS** recording types will be activated for all days as indicated by the different colored bars available in this menu.

To choose a channel (or camera) for which to configure, click the number next to **Channel**, then select either a single channel or **All** if you would like the schedule to apply to all channels currently connected to your NVR:



By default, the NVR will have the schedule for each recording type to record 24/7. Also note that the NVR uses military time from 00:00 to 24:00 hours instead of 12 a.m. to 12 a.m.

To edit a recording schedule, select a recording option from the colored boxes. Each recording option is color coded: Green: Regular (24/7 recording), Yellow: MD (Motion Detection), Red: (Alarm), Orange: MD&Alarm (a combination of motion detection and alarm recordings), and IVS. Select which recording type you would like to modify and then use your mouse to adjust the time via the time bar for your specific recording type.

Click the eraser icon to the right of any day if you would like to clear the entire row of blocks.

To add or remove motion detection blocks to the grid, mark the yellow checkbox next to **MD**, then click individual cells or click-and-drag for multiple blocks.

To the left of each day, there are small boxes which can be marked to 'link' days together. This is useful if you want to save time by instantly making changes to multiple days simultaneously.
In the below example, Sunday and Monday are linked, so any blocks that are added or removed for Sunday will automatically and immediately reflect the same for Monday and vice versa.

The same concept applies when configuring other recording schedule types such as IVS.

Another way to configure recording schedules is by manually setting time periods. Click the "gear" icon to the far right of any day to open the **Period** page.

Here, the periods (Periods 1 - 6) will be displayed in chronological order. You can set either **Regular**, **MD, Alarm, MD&Alarm or IVS**, checkboxes. You can also copy the period settings over to other days by checking them individually or checking **All**. Make sure to click **Save** when finished.

Now that you have finished configuring the recording schedules, you may need to copy these settings over to other channels (or cameras). By default, D1 (Channel 1) will be selected unless you immediately selected **All** in the channel window previously. Please note, you can copy these settings directly over to another channel by clicking **Copy.**

In the **Copy** window, you can select individual channels for any cameras you have added to the NVR or select **All**:

Click **Save** when finished.

When finished on this screen, click **Apply** to save your changes.

Setting Up Email Alerts

Setting up Email alerts will allow you to receive snapshots of events via your email. These events can be motion detection, IVS, Face Detection, or other events captured by your device. Each event type must have the "**Send Email**" option enabled to allow the feature to send snapshots to your email. To set up email alerts, please refer to the information provided below.

1. On the Main Menu, click on **Network** located in the **Management** section.
2. Select **Email** and **Enable** the toggle switch.
3. Enter the SMTP information for your email. In this example we will be using Gmail, however other email services can also be used. If using Gmail, type in "**smtp.gmail.com**"
4. Enter a port number. This is based on the type of encryption used by your email service. In this example we will be using port **465**, which uses an **SSL** encryption type. If using **TLS**, the port number will be **587**.
5. Enter the email address you will be using in the **Username** field.
6. Enter the password for the email address in the **Password** field.
7. In the **Receiver** field, enter your email address. Enter that same email address in the **Sender** field.

8. Update the subject line for your alerts in the **Subject** field. The default subject line will be NVR Alert however this can be changed to anything you would like to use.
9. Make sure the **Attachment** toggle switch is enabled to enable snapshots to be sent.

10. Click **Apply** and **Test** to verify connectivity. Once the test has been successfully sent, click **Save** to continue.

11. Check your email to see if you received the email test.
Now, whenever your camera detects motion, you will get email alerts sent to the email that was set up in the system.

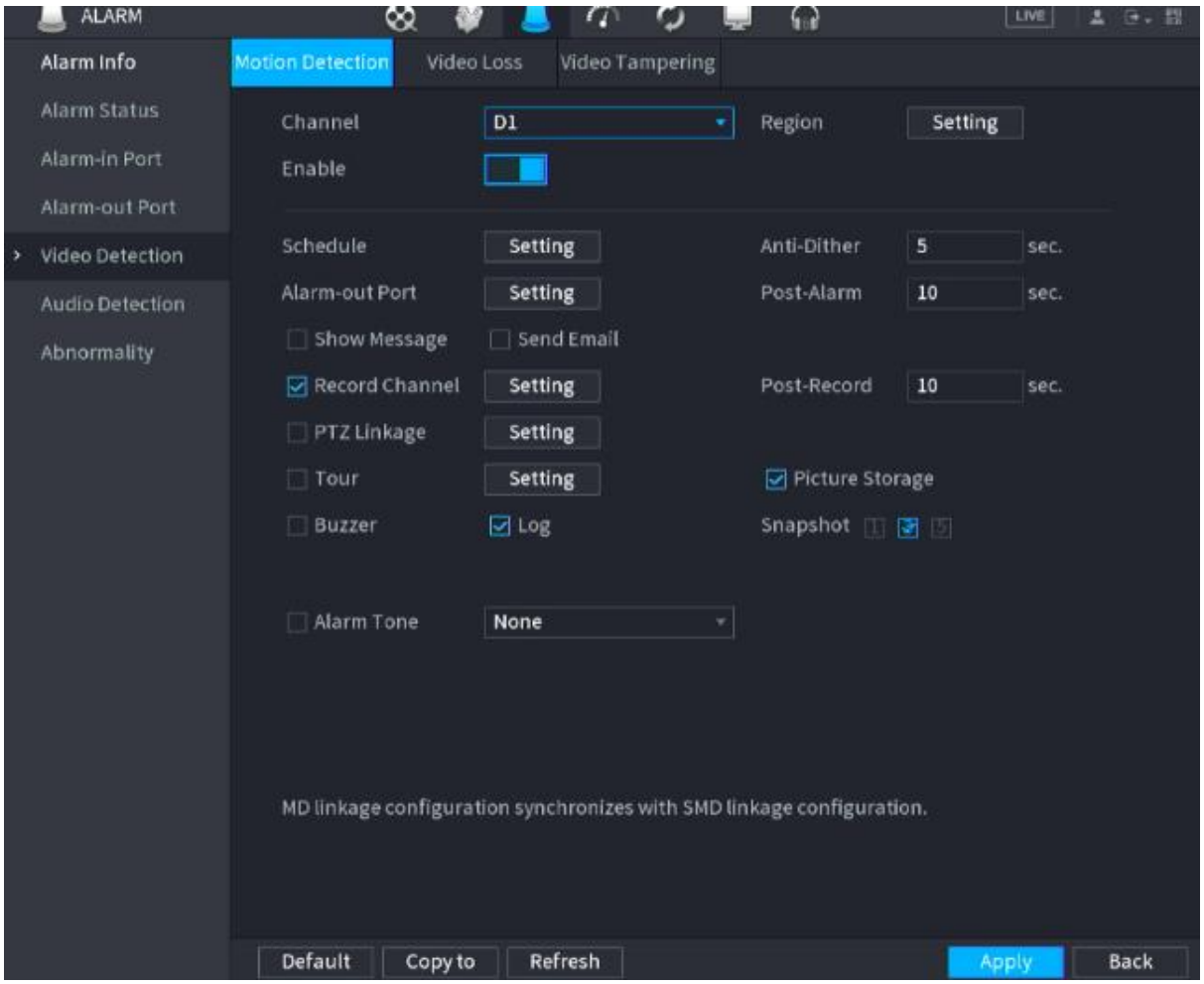
This will include an email with a snapshot of what was seen when the event was triggered.

Setting Up Motion Alerts

Motion detection events are different from IVS or other AI events as they do not use AI algorithms to function and can be used in conjunction with IVS or other rules as they are separate features in the system. For more information on configuring motion detection, please refer to the information below.

1. On the Main menu, click on **Alarm**

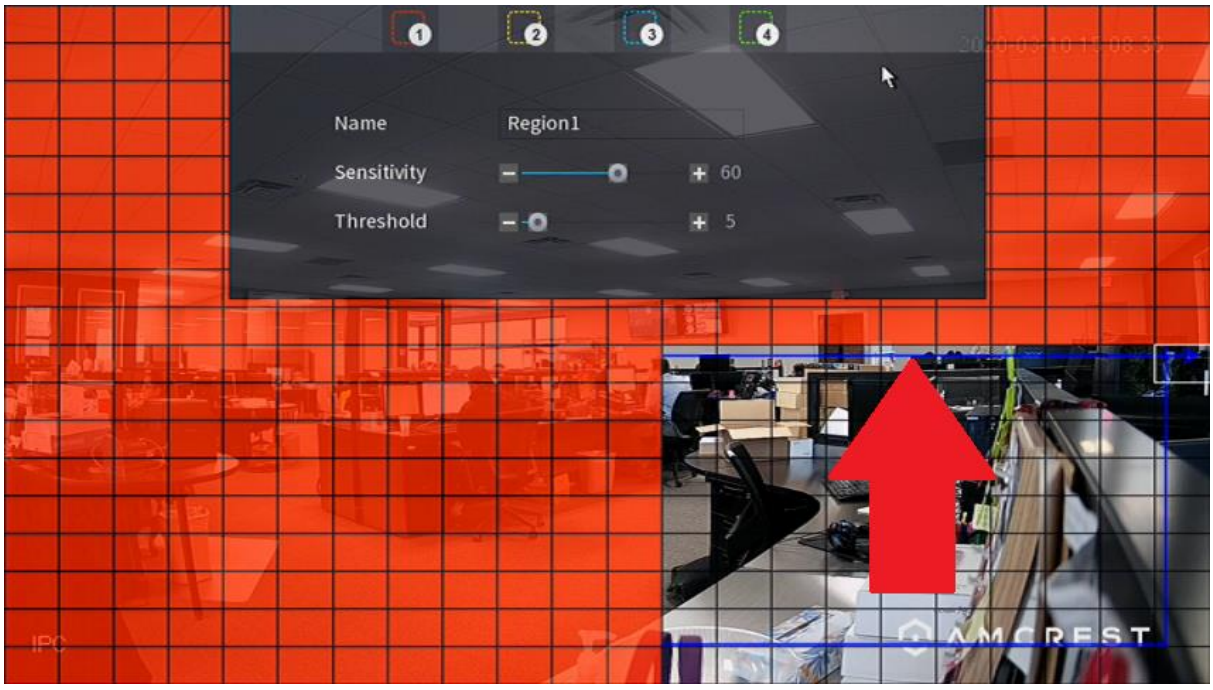
2. Select **Video Detection** to access the **Motion Detect** menu. This is the main configuration page for your motion detection settings. Select which channel you are configuring from the Channel drop down menu.



3. Ensure the toggle switch for motion detection is enabled and adjust any motion detection settings or motion schedules accordingly.

Adjusting Region Settings

You can set up “regions“ for motion detection using the region grid on your NVR. By default, the entire area of view for your cameras will be highlighted with red blocks indicating that all areas of the live view screen will have active motion detection. However, to prevent false events from occurring, you can use your mouse to block out certain areas.



If you hover your mouse pointer over the top-center edge of this window, another small window will appear with options to configure **sensitivity** and **threshold** settings as well as to choose from up to **four regions**.

Sensitivity - is the measure of how many pixels on the screen need to change before being considered motion. **0** is the lowest value and **100** is the highest.

In plain English: Sensitivity is the difference between a squirrel running up a tree, versus a big dog running up to and barking at that tree. A squirrel would trigger motion detection at a *higher* sensitivity because it takes *less change or movement to qualify as motion*. But the dog would trigger motion detection at a *lower* sensitivity because it takes *more change or movement to qualify as motion*.

Threshold - is the degree of movement that needs to occur before the motion is defined as a motion event and is triggered. **0** is the lowest value and **100** is the highest.

In plain English: Threshold is the difference between a car driving quickly on a street and a car driving into the field of view, slowing down, and turning into a driveway. The car driving past *would not* trigger motion detection based on a certain threshold setting, but the parking car *would* trigger motion detection with that *same* threshold setting. The *higher* the threshold, the *more time* motion needs to occur before motion detection is triggered. The *lower* the threshold, the *less time* motion needs to occur before motion detection is triggered.

If sensitivity is set to 100 and threshold to 0, motion detection will be triggered by almost any change in the field of view, large or small. But if sensitivity is set to 0 and threshold to 100, motion detection will be extremely difficult to trigger.

The **four regions** are all different colors, so you can customize the field of view of any camera to your specific preferences.

To choose another region, hover your mouse pointer near the top center of the region window, and a small window will appear. Keep your mouse pointer inside that small window and select either region 2, 3, or 4:

You will be able to click individual blocks or click-and-drag an area with the newly selected color to highlight portions of the screen. Each new region (or color) has its own unique sensitivity and threshold settings. The different regions/colors can also overlap one another. To exit the region setting screen, right click your mouse on the interface.

Adjusting Motion Detection Schedules

Motion detection schedules work the same as the schedules outlined in section: "*Setting Up Recording Schedules."* To adjust a motion detection schedule, click on **Period** and use your mouse to adjust the timeline. Click on the settings (gear) icon to set multiple periods. Click on **Save** to save your schedule.



3. Click on the **"Send Email"** checkbox. To enable the NVR to send an email once a motion is detected.
4. Click on **Apply** to save the settings to your system.

Once you have set up your settings for one channel, you can copy them to other channels in the system. If you did not select **All** after clicking **Channel** as previously described, click **Copy**, select channels to copy to, then click **Save**.
Click **Save** to save all the settings made on this page. Click **Apply** in the Motion Detect menu to finish saving your motion detection settings to your device.

Setting Up AI Events

The AI menu allows the user to manage and view artificial intelligence, ANPR, IVS, face recognition information, etc. AI features available on the device can be controlled either by the device or using an AI camera depending on its features.

There are 2 AI types, **AI by Camera**, which allows the NVR to use the **camera's** built-in AI features (if applicable), or **AI by Device**, which allows the system to use the **NVR's** built-in AI features. Since most AI cameras differ model-to-model we will cover what is available via the NVR using the AI by device protocol.

Note: If using a non-AI camera, please use the AI by Device protocol to set an AI function.

The NVR provides the following AI features built in; Face Detection, Face Recognition, IVS features, such as tripwire and intrusion, SMD (human and vehicle detection), and heat map. **Other AI features such as people counting and ANPR (license plate reading) will be controlled by an IPC only.**

Set a Smart Plan

A Smart Plan will not be available if using a non-AI camera or an AI camera that supports only certain features not supported by the NVR. AI features such as IVS and Heat Map can be used simultaneously, however, Face Detection, People Counting, etc. will have to be used separately. A smart plan must be enabled for an AI feature to be activated.

Setting Up Face Detection

Face detection is used to allow your device to detect face events. This feature can be used either by the NVR or by the camera (if supported). For more information on setting up face detection, please refer to the information provided below.

1: Access the **Smart Plan** menu and select the channel you would like to configure from the **Channel** drop down menu. Click on the **Face Detection** icon and then click **Apply**. If using a non-AI camera, or a camera that does not support face detection, a smart plan may not be available for the specific channel.

2. Click on the **Face Detection** menu located in the **Parameters** section and select which channel to configure from the Channel drop down menu. Next, choose which face detection type you will be using from the **Type** drop down menu. In this example we will be using **AI by Device**, however, you can choose AI by Camera to use the camera's built-in face detection settings, if applicable. Enable the face detection toggle switch.

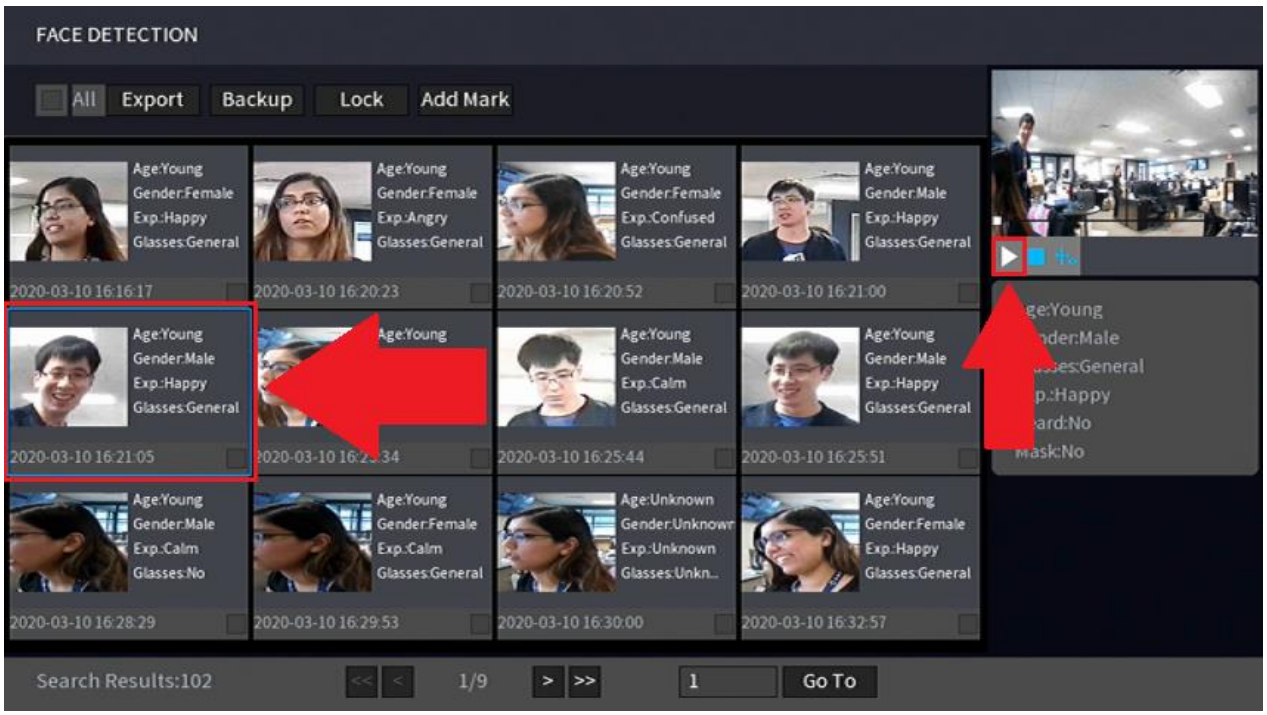
3. It is best to leave the **Rule** settings as default, however, they can be adjusted by clicking on the **Setting** button. Use your mouse to adjust the minimum (Min) and maximum (Max) size of the face detection area.

4. When triggered, the face detection event will be retained in the face detection smart search menu or snapshots of the event can be emailed to you. To have a snapshot of the event emailed to you, set up email alerts as described in section: *Setting Up Email Alerts* and click on the **"Send Email"** checkbox. Click **Apply** to save the setting.

Viewing Face Detection Data

All face detection data retained by the system can be accessed via the **Face Detection** option located in the **Smart Search** menu. Enter a start and end date and time for the event you would like to view in the Smart Search interface and click **Smart Search**.

A display of all face detection data will be displayed along with facial attributes. Click on the event you would like to view, and a clip of the event will be displayed in the built-in player. Click on the play icon to view the event.



Storing a Face Detection Event

Face detection events can be stored on a USB flash drive. Insert the flash drive into a USB port on the device then click the check box next to the event you wish to store. If you would like to store all files, click on the **All** checkbox at the top of the interface. Click **Backup** to store the event, or multiple events to the USB flash drive. There will be a “File Type” drop down menu, select MP4 from the file type menu and click **Start**.

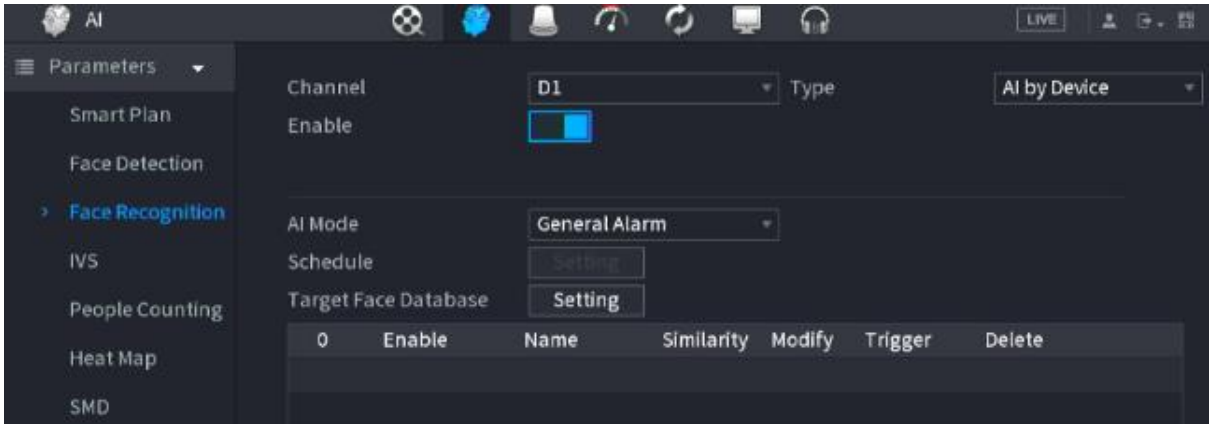
Once the backup process is complete, click **Save**. The files will be stored onto your USB flash drive and the MP4 recordings can be viewed on a computer.

Using Face Recognition

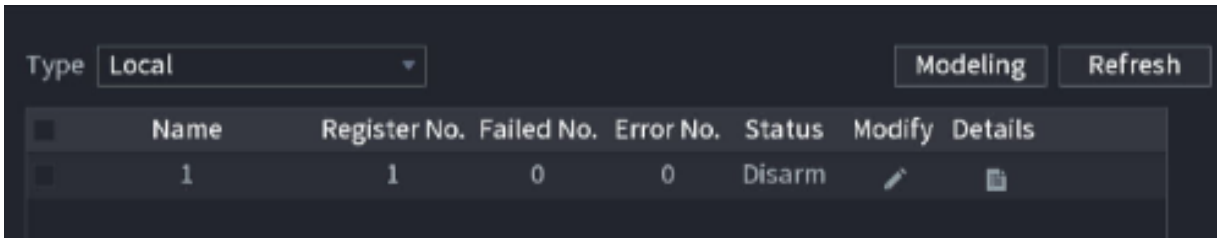
Face recognition is used in conjunction with face detection to locate and determine facial similarities detected by the system. Images are registered in a face library, by the user, and accessed via a face recognition smart search tool that is built into the NVR. **A USB flash drive with applicable images (in jpeg format) should be inserted into a USB port on the NVR if you are importing images locally.**

1. Ensure **Face Detection** is enabled and access the **Face Recognition** menu.

2. Click on the **Face Recognition** option in the **Parameters** menu and verify the correct channel (camera) is being used. Click on the **Enable** toggle switch to enable the feature. Click on **Apply**.



3. Click on the **Database** option located in the AI menu and click on **Add** to begin registering images to a face library. **A face library must be registered for this feature to function properly.** Enter a name for your face library and click **Save.**
The library will now be saved to the database. Click on the **Details** section to begin adding images into the to the face library.



If you have a single image to add click **Register ID**, if you have multiple images to add click on **Batch register**. Follow the on-screen prompts to add the images into the library. Once the images have been successfully modeled into the database, left click on the interface to exit.

4. Navigate back to the **Face Recognition** menu in the **Parameters** section and click on the **Setting** option in the **Target Face Database** field. Select the face library you just created and click **Save** to insert the library of registered images into the interface.

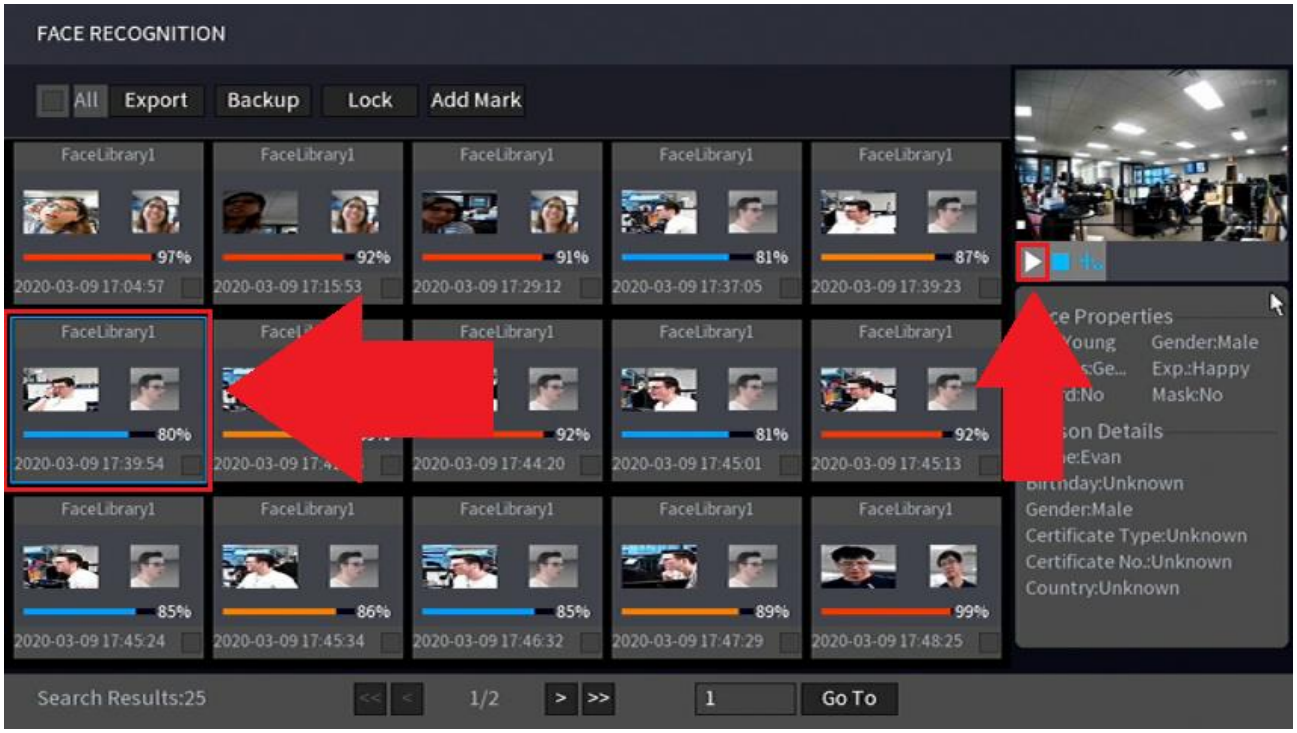
5. Select an AI mode from the **AI Mode** drop down menu. **Common Mode** allows the device to use the images registered in the face library as a reference. Enabling the **Stranger Alarm** to alert the system once an unrecognized face is detected. Click **Apply** to save the settings to your system.

Note: To adjust **Common Mode** settings, click on the **Trigger** (gear) icon and select which additional options you would like to apply to this feature. Be sure to click **Apply** to save the settings to your device.

Viewing Face Recognition Data

All face recognition data retained by the system can be accessed via the **Face Recognition** option located in the **Smart Search** menu. A search by attributes or a search by image can be performed. Searching by attributes will load all face recognition data found in the system whereas searching by an image will filter and display only the faces chosen by the user.

To search by attributes, enter the start and end time of the event in the interface and then click **Smart Search**. The interface will display all face recognition data. To view the event, click on the event you would like to view then click the play button in the interface.



To view specific face recognition data by image, click on the **Search by Image** tab located in the **Face Recognition** interface.

If searchable images are already uploaded into a face library click on **Face Library** and select an image from the interface, then click **Save** to begin a search. If you would like to add images locally click **Local Upload** and follow the on-screen prompts to upload images. A USB flash drive with applicable images (in jpeg format) can be used to upload images to the NVR. Once an image has been loaded, enter the start and end time of the event, and click **Smart Search.**

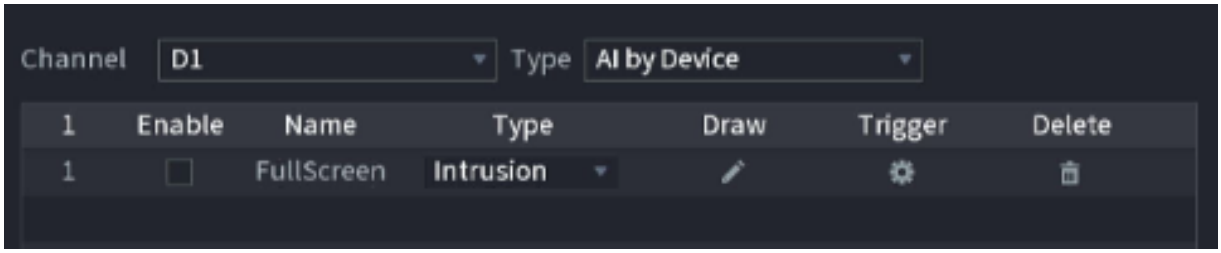
The system will display all face recognition data based on the image selected. All face recognition data can be backed up locally using a USB flash drive.

Setting Up IVS and Heat Map

Both IVS rules and Heat Map features can be used simultaneously in the system, however the NVR does not have built-in heat map features and can only be applied if the camera supports this feature. However, the NVR does have built-in IVS, the IVS rules on the NVR are controlled either by camera or by the NVR. The NVR currently has 2 built-in IVS features available (Tripwire and Intrusion) whereas some Amcrest AI cameras may have additional IVS features. For more information on how to set up IVS and heat map, please refer to the information provided below.

Note: Please make sure to completely disable any face detection, face recognition, people counting or other AI features when using IVS rules. If using an AI camera that supports this feature be sure to use AI by Camera in the IVS menu and enable the IVS or heat map smart plan.

1. Click on the **IVS** option located in the **Parameters** menu and verify the correct channel is being used. If you are using AI features available on the camera side, select AI by Camera, in this example we will be using **AI by Device** to highlight key features of the NVR. Click **Add** to add an IVS rule.



IVS Features Available by Device

Any camera, whether AI or non-AI, connected to the NVR can take advantage of the NVRs built-in AI features, including IVS. For more information on the built-in IVS features please refer to the information provided below.

Tripwire: Allows the device to trigger an event if an object, such as a human or vehicle, crosses a set tripwire line.
Intrusion: Allows the device to trigger an event if an object, such as a human or vehicle, appears or crosses a set intrusion area.

Note: For more information about the AI features available on your device, please consult the full user manual for your specific model camera or visit: https://amcrest.com/support

3. Click on the **Type** drop down menu to select an available IVS rule. Once a rule is selected, click on the **Draw** (pencil) icon, to begin configuring the rule.

4. Use your mouse to draw an area or line on the interface. Click on the interface and use your mouse to draw an area or line, click your mouse on the interface when done, then right click to set the area or line to the system.

If you would like to add a name for the rule, enter a name in the **Name** box. The **Direction** drop down menu allows you to choose a direction in which the rule will be triggered. Object filters can be enabled for accuracy. Click **Save**.

The Target Filter option is used to set a minimum or maximum detection area. It is recommended to leave this as default; however, it can be modified. Use the Clear (trash can) icon to remove a drawn area or line. The AI Recognition toggle switch enables object filtering options that allow you the ability to determine if a human or vehicle has entered the area. If Person is chosen, the rule will only be triggered if a human figure is detected. If Vehicle is chosen, the rule will only be triggered if a vehicle is detected by the system. Both object filtering options can be used simultaneously if needed.

5. If you would like to add multiple rules to the device, click on **Add** and repeat the IVS setup process for the rule. Click **Apply** once all IVS rules are set.

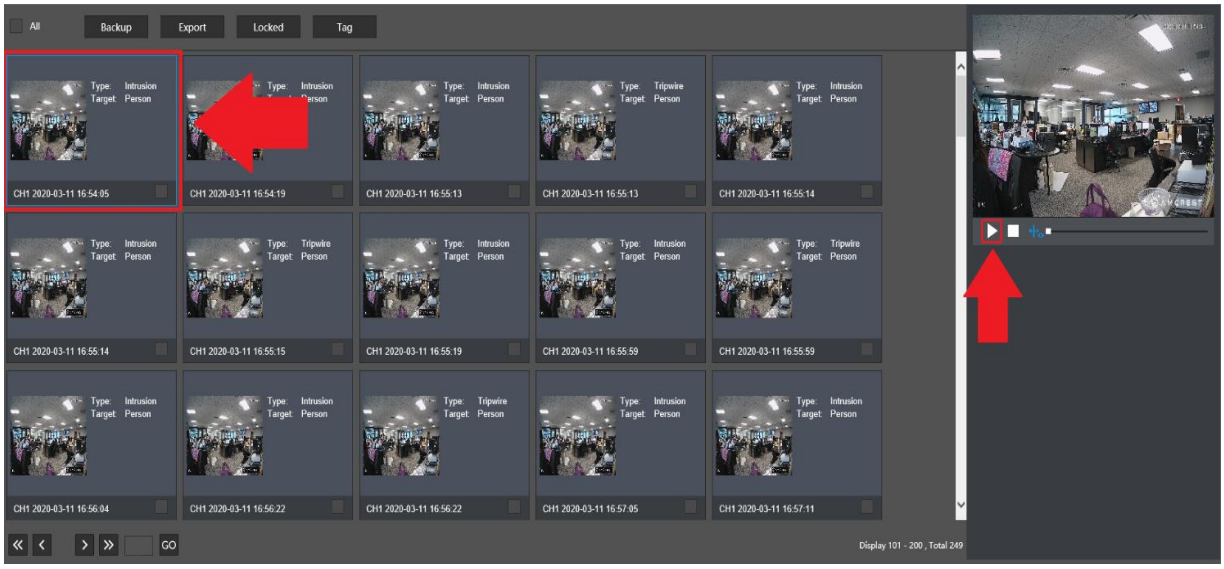
Use the Trigger (gear) icon to apply any additional settings to an IVS rule, such as enabling email snapshots, etc. To delete an IVS rule, click on the delete (trash can) icon.

Note: Once an IVS rule is triggered the line or area visible on the live view screen will flash.

Viewing IVS Data

Any IVS data retained on the system can be viewed using the IVS Smart Search interface or via the playback menu if an IVS schedule is set in the system. To learn more about recordings schedules, please refer to section *"Setting Up Recording Schedules".*

1. To view IVS data using the IVS smart search interface, click on the **IVS** option located in the Smart Search menu. Enter the start and end time of the event and click **Smart Search**. A layout of all IVS events will be displayed. To view the event, select the event from the interface and click the play button. The event can also be stored using a USB flash drive.



Using Heat Map

Heat Map is a tool used to determine the overall crowd flow (density) over a certain amount of time in a specific area. Heat map provides a color-coded layout of the density with red being the highest level to blue which is the lowest level. For more information on how to use a heat map, please refer to the information provided below.

1. Ensure the **Heat Map** icon is enabled in the **Smart Plan** menu. Click **Apply**. Please note, if the camera you are using does not support heat map, the feature will not be available in the NVR.

2. Enable the Heat Map toggle switch to turn on the feature. Click **Apply.**

Note: A schedule can be set for this feature by clicking on the **Setting** button in the **Period** field. This will allow the feature only to function during specific times set by the user.

3. To view Heat Map data, click on the **Smart Search** option and click on **Heat Map**. Enter a start and end time into the interface and click **Search**. The heat map period cannot exceed one month of reporting. All heat map data will appear in the interface.

Note: To back up a heat map image, click on **Export** then click **Save**. This will save a BMP image to an external USB flash drive.

Using People Counting

People Counting is used to provide a statistic based on the number of people who enter and exit a certain area. This feature cannot be used in conjunction with IVS or any other AI features associated with your device. For more information on using people counting please refer to the information provided below.

1. Enable the **People Counting** icon in the **Smart Plan** menu. Please note, if the camera you are using does not support People Counting, the feature will not be available in the NVR. Click **Apply**.

2. Click on the **People Counting** option located in the **Parameters** menu. Ensure the correct channel is being used and click on the **Enable** toggle switch to enable the feature. Click **Apply**.

3. To update any information regarding people counting. Click on the **RULE** button located in the Rule field of the interface. It is best to leave this area as default; however, you can modify the name, direction, or target filtering of the feature. Target filtering allows you to modify the detection area based on a minimum and maximum setting on the screen. Right click on the interface to exit.

4. Use the interface to apply any additional settings such as sending an email snapshot of the event ("**Send Email**"), etc. Click **Apply** when finished.

Viewing People Counting Data

People counting data shows the number of people reported by the system entering or exiting the area within a specified amount of time. This information is displayed graphically using a histogram or a line graph and can be exported to a USB flash drive if needed. For more information on how to view people counting data please refer to the information provided below.

1. Click on the **People Counting** option located in the **Smart Search** menu. Enter the start and end time of the report in the **Start Time** and **End Time** fields.

2. Reports can be pulled in daily, monthly, or yearly increments. Click on the **Report Type** drop down menu to access additional reports if needed. Click **Search** to view statistics.

3. A chart will be displayed in the interface showing how many people have entered or exited the area. You can use the Histogram/Polygon buttons to switch between different report types.

4. An excel spreadsheet of this data can be exported and backed up via a USB flash drive. To export this data to a USB flash drive, insert a USB flash drive into a USB port on the NVR. Click **Export** in the interface. Click **Save**, this will export the excel sheet to your flash drive.

ANPR

The ANPR option allows the user to sync vehicle block and allow lists as well as view license plate data if a license plate reader camera is applied to the NVR. Please note, this option is only applicable to license plate reader cameras, all other models that do not support ANPR will not be compatible with this option.

Please note, this option is only for license plate detail retention. The camera must be set up for ANPR first before applying it to the NVR for retention. **All other ANPR camera settings, such as LPR capture areas, will have to be modified in the license plate camera directly using a web user interface**.

Using ANPR

The capture area and other settings must be applied on the camera side before enabling this feature in the NVR. If any license plate numbers have been placed on the allow or block lists in the camera, please select Sync Vehicle Blocklist/Allowlist.

The additional notification options will apply to all events, block list events, or allow list events if needed. Select the notification type or any other applicable settings, then click **Apply** to save.

Once ANPR data is captured, click on the **Smart Search** and access the **License Plate Data** option to view the events. Enter the date and time range of the event and click **Search**. A list of LPR data will be shown. Select an event to view, use the play option to view the event. Events can be backed up on a USB drive or thumb drive if needed to export locally.

Playback

Motion detection and IVS recordings can be accessed in the **Playback** option on the main menu. **A hard drive must be installed to access and view recordings from this menu.** To access the playback interface, click on the **Playback** option located in the main menu.

To view recordings from the search menu, select the camera you wish to view from the **Camera Name** section by clicking on a checkbox next to the device.

A timeline of the recordings will appear in the interface.

Click the **Play** button () to play all recordings available on the timeline.

Additionally, all days with recordings available will be highlighted in the calendar portion of the interface with a dot.
To select specific days/months or years, use the navigation arrows provided in the calendar. A file list of recordings can also be shown by clicking on the **File List** icon () located in the interface. Once clicked, a list of recordings will be shown based on the time the events were recorded.

Note: In the File List menu, "**R**" stands for regular/continuous recordings, "**M**" stands for Motion Detection recordings, and "**I**" stands for IVS recordings.

To play a recording from the File List menu, double click on the file you want to view. The recording will automatically begin to play in the interface.

How To Upgrade System Firmware

Keeping the firmware on your NVR up to date is an important part of overall system health. For security purposes, it is highly recommended to upgrade the firmware on your device every time a new firmware is available. To locate the most up to date firmware for your NVR please visit https://amcrest.com/firmware

Upgrading the firmware for your NVR can be done locally, using a USB flash drive, or via a web browser using the web user interface. For more information on how to access the web user interface please see section, *"Computer Access Setup".*

Upgrading the Firmware Locally

1. Insert a USB flash drive into your computer and go to https://amcrest.com/firmware
2. Locate the most up to date firmware for your device and download it to your computer. Save the file to your USB flash drive.
3. Insert the USB flash drive into a USB port on your NVR.
4. On the NVR, go to **Operation** and click on **System Maintain,** then click on the **Upgrade** tab.
5. Click on **System Upgrade**.
6. Locate the firmware file that is on the USB flash drive and then click **Save**.
7. Allow the system to be upgraded. The device may reset after the firmware update is complete.

Computer Access Setup

There are 2 ways to access your NVR from a computer, locally or remotely.

Local Access: Logging into your NVR's web interface from a computer or laptop connected to the same network as your NVR (home, office, etc.).
Remote Access: Logging into your NVR's web interface from a computer or laptop connected to a network outside of your home or business network (coffee shop, work computer, etc.)

Local access is preferred by those who do not want to make their NVR accessible from outside their network. *However, there are several options available for remote access that use standardized and secure network protocols including SSL, TLS, DDNS, etc.* Most other users require remote network access by way of their smartphones, tablets, laptops, or computers, wherever they are.

The following section will cover both means of access (local and remote). Keep in mind that any user can have *both* local *and* remote access simultaneously if they choose.

This device features the latest in JavaScript technology which allows you to access your device using a wide variety of web browsers including Google Chrome, Firefox, Safari, and other mainstream web browsers using a PC or Mac computer. To access the web UI using a web browser, please refer to the information provided below.

Locate the IP address for your device using the Amcrest IP Config Tool. The Amcrest IP Config Tool can be downloaded at the following web page: amcerest.com/downloads.

In the All Downloads menu, click on IP Config Software to begin the free download. Once the download has completed installing, locate the IP address associated with the device you would like to view in the browser.

Enter this IP address into the browser and press enter to load the web user interface. Please note, if this is your first time accessing the interface, please follow the prompts in the device initialization screen to access your device.

Enter the login credentials for your device. If this is the first time accessing the device, the username and password will both be **admin.** Click on **Login**. Once logging in you will be taken to the main menu interface.

Accessing the Web User Interface

To access the web user interface (web UI) for your NVR, open a web browser and type the IP address for your NVR into the browser and press Enter. This will pull up the Device Initialization screen. Set a location, language and video standard then click **Next** to continue.

Choose your Time Zone and System Time then click **Next** to continue.

Enter Password

Like accessing the NVR directly, if you are accessing the NVR for the first time you will need to enter a password for the device. Enter a password. Click **Next** to continue.

Next, it is recommended to secure your NVR with an Email address and security questions. The Email address entered can be used for password recovery purposes in case a password is forgotten or needs to be reset.

Enter a valid email address and then select and answer the security questions provided in the dropdown menu. Click **OK** when done.

When the NVR has been setup successfully you will hear a beep from the NVR and a prompt in the browser letting you know that the initialization is complete. You will then be taken to the login screen. Enter the **username** and **password** for your NVR then click **Login**.

Note: Please allow all permissions to allow the plugins to function in your browser. Once the plugins are allowed the main menu screen will appear.

Accessing the Web User Interface Remotely

For the purposes of this guide, we will outline the most common method for setting up web access. Port forwarding using the HTTP protocol and using Dynamic Domain Name Server (DDNS) is the easiest way to set up stable remote access.

For this method, you should have direct access to your router as well as the ability to port forward the device using the router's built-in interface.
Below is a step-by-step walk through those details on how to set up the NVR for remote web access using DDNS.

1. Log into the web UI and go to **Management>>Network>>Connection.** In the Connection tab, note the HTTP Port information for your NVR.
It is recommended to ensure the port number is at least 5 digits long to prevent any port conflicts. You can change the port to any 5-digit number that is less than 65535 (e.g., 12345) by clicking the number field and entering a new port number. Write it down, then click **Save**.
2. The system will need to be rebooted for this change to take effect. Click **OK**.
3. Once the NVR has come back online, log back into the web UI and navigate back to the Connection menu to verify the HTTP port has been updated properly.

4. Access your router's user interface and port forward the device using the HTTP port information displayed in the system. Every router's port forwarding protocols are unique. For more information on how to port forward your specific device, please visit portforward.com or refer to the user manual for your specific router.

Note: When port forwarding the NVR in your router, make sure to use the TCP, UDP and updated HTTP protocols displayed in the NVR. If DDNS is not an option, the device can be accessed remotely using the public IP address for your network and the HTTP port used that was port forwarded in your router. To locate your public IP address and verify the connectivity of your system, please visit: canyouseeme.org

5. Click on the **DDNS** menu located in the **Network** tab in the left panel. In the DDNS menu, click on the Enable checkbox to enable DDNS. Make sure the **AMCREST DDNS** type is selected and a domain name for the NVR (one you create) is entered in the Domain Name field. As an example, the Domain Name will be in the following format: mynewnvr.amcrestddns.co

Click **Save** once the DDNS information is entered.

Accessing the Device Remotely
After setting up the NVR in the previous steps provided, open a web browser, and enter in the DDNS domain name address previously setup for your NVR.

For example, if the DDNS domain name is http://abc123456789.amcrestddns.com and your HTTP Port is 12345, the URL would be http://abc123456789.amcrestddns.com:12345

Remote access not working? (Troubleshooting steps)

Please contact Amcrest Support via one of the following options:

Visit http://amcrest.com/contact and use the email form

Call Amcrest Support using one of the following numbers
Toll Free: (888) 212-7538
International Callers (Outside of US): +1-713-893-8956
USA: 713-893-8956
Canada: 437888-0177

UK: 203-769-2757

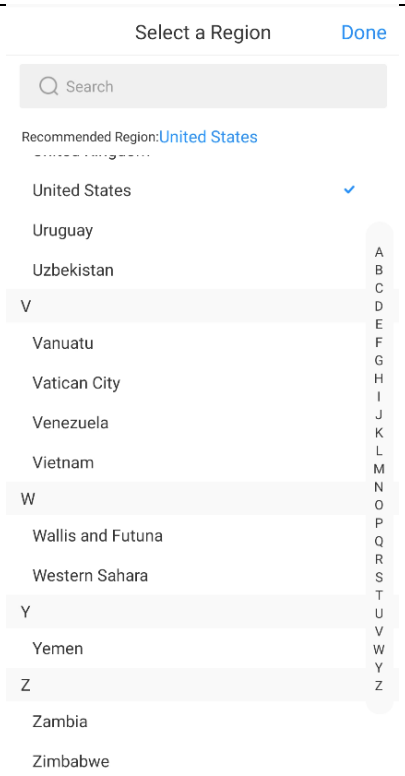
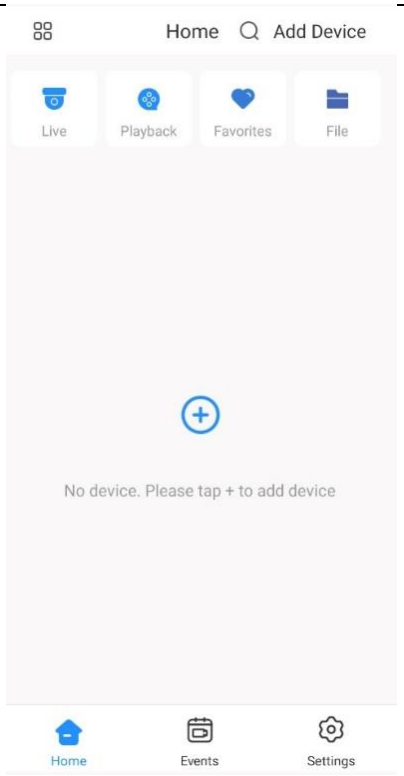
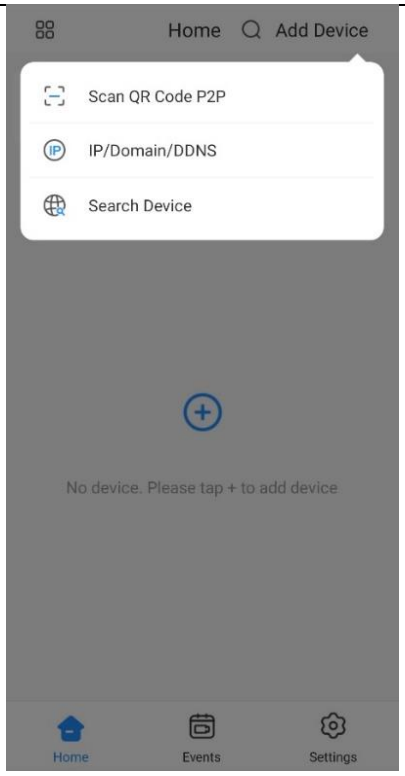
Upgrading the Firmware Using a Web User Interface.

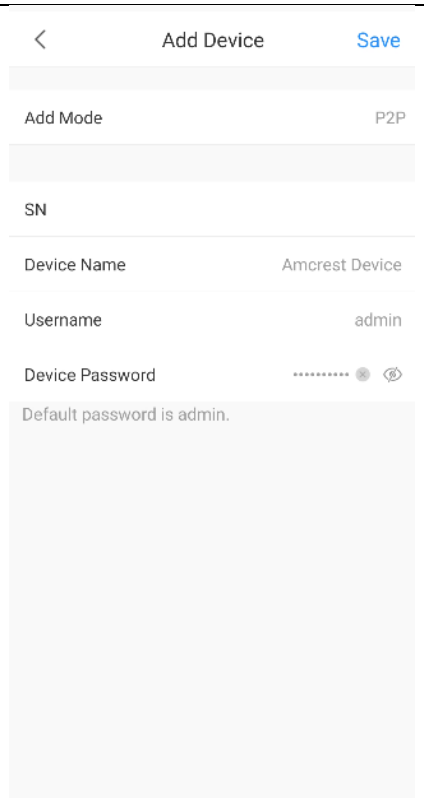
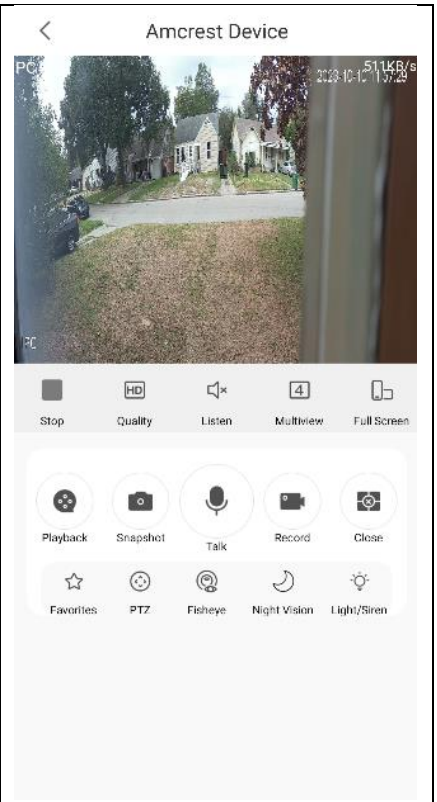
1. Log into your NVR via a web browser and click on **Operation**.
2. In the **Operation** menu, click on **System Maintain** then click on the **Upgrade** tab.
3. Click on **Download the latest Firmware** button to access the firmware downloads page.
4. Choose your model device and download the firmware file.
5. In the **Upgrade** menu, click **Browse** to access the firmware file and load it into the system.
6. Click on **System Upgrade** and allow the system to upgrade. The system may reset after the firmware file has finished downloading. The system is now up to date.

Amcrest View Pro 2 Setup

The following steps will continue the app setup process for an Android phone and, though the iPhone version of the app has slightly different steps, most of this process is identical and easy. Download and install the Amcrest View Pro 2 app for the App Store or Google Play Store.

Open the app on your mobile device and allow the app to load.

		
1. Select your country of origin and click **Done**.	2. Tap Add Device or the "+" icon to begin adding your device.	3. Tap **Scan QR Code P2P**.

		
4. Scan the QR code and tap DVR/NVR.	5. Create a name for the device, enter the username and password. Click **Save**.	6. The device has been successfully added to the app.

Note: To locate the serial number, you must either have physical access to the NVR or computer access to the web interface to access the P2P menu. The SN QR code will be the serial number for your device. For more information regarding the Amcrest View Pro app, please visit: https://amcrest.com/support

FCC Statement

1. 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.
2. The user's manual or instruction manual for an intentional or unintentional radiator shall caution the user that changes, or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment. In cases where the manual is provided only in a form other than paper, such as on a computer disk or over the Internet, the information required by this section may be included in the manual in that alternative form, provided the user can reasonably be expected to have the capability to access information in that form.
3. (b) For a Class B digital device or peripheral, the instructions furnished the user shall include the following or similar statement, placed in a prominent location in the text of the manual: 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.

4. RF exposure warning

This equipment must be installed and operated in accordance with provided instructions and the antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter. End-users and installers must be provided with antenna installation instructions and transmitter operating conditions for satisfying RF exposure compliance.

IC Warning Statement

This device complies with Industry Canada's license-exempt RSSs. Operation is subject to the following two conditions:

(1) This device may not cause interference; and
(2) This device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

This equipment complies with IC RSS-102 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.

Pour se conformer aux exigences de conformité CNR 102 RF exposition, une distance de séparation d'au moins 20 cm doit être maintenue entre l'antenne de cet appareil ettoutes les personnes.

References & Contact Information

To view setup videos for many of the steps outlined in this guide, go to http://amcrest.com/videos
For more supplemental information, a full user manual, or to view articles related to your device visit http://amcrest.com/support
For contact information please visit us at https://amcrest.com/contact or reach out to us directly at 1-888-212-7538

This quick start guide is for reference only. Slight differences may be found in the user interface.
All the designs and software here are subject to change without prior written notice.
All trademarks and registered trademarks mentioned are the properties of their respective owners.