NVR Quick Start Guide

Version 1.0.0

Contents

Welcome 3
Hardware Setup 4
NVR Initialization 5
Main Menu 9
IVS, Motion Detection, and Recording Setup 9
Setting Up Email Alerts 11
Setting Up IVS Events 12
Playback 13
Computer Access Setup 13
How To Upgrade System Firmware 15
Helix Pro App Setup 15

Welcome

Thank you for purchasing a Helix NVR.

Before installation and operation, please read the safeguards and warnings below carefully. This document provides a quick setup and overview of your Helix NVR and its features

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 it 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

The following items should be included with your device.

Component	Quantity
Network Video Recorder	1
Quick Start Guide	1
Mouse	1
Power Adapter (if applicable)	1
Power Cord	1
HDD Phillips Head Screws	Included

Device Ports

The ports and indicator LEDs may be different depending on the model of the NVR.

Front Panel

Port Name	Description
PWR Indicator	Power status indicator. When the NVR is on the indicator will be solid. When the NVR is off the indicator will be off.
HDD Indicator	Hard drive status indicator. This indicator flashes when data is being transmitted.
USB 2.0	Supports a connection for a USB mouse or back up flash drive.
USB 2.0	Supports a connection for a USB mouse or back up flash drive.

Rear Panel

	Description
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.
	Supports RJ45 100Mbps self-adaptive network Ethernet port.
Audio	External audio in or audio out ports (may differ model to model).
VGA	VGA video output port. Outputs analog video signal. This connects to the monitor to view analog video.
HDMI	High-definition audio and video signal output port.
	Power switch. Turn the NVR on or off.
Power Input	Power adapter input (Please refer to the specs sheet for your specific model for more details on power requirements.)
USB 2.0	Supports a connection for a USB mouse or back up flash drive.

Hardware Setup

Before setting up the NVR, you may require the following items. These items may not be included with your NVR:

A computer monitor, or TV with either an HDMI or VGA input.
A power strip with room for additional power adapters (if needed).
A hard drive for storing video recordings.
A USB flash drive formatted to FAT 32 to import/export config or image files (if needed).

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.

Hard Drive Installation

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 Helix Pro application and accessing the camera directly over the network, however, no recordings will be retained in the NVR if a hard drive is not installed.

To install your hard drive, you will need the following items:

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

Note: **Before installing the hard drive, make sure the NVR is turned off and disconnected from power.**

1. Use a Phillips head screwdriver to remove the screws on the NVR to remove the cover if necessary.
2. Attach the hard drive screws to the hard drive (sold separately). Do not overtighten, only turn a max of two to three times.
3. Place the hard drive into the NVR in accordance with the installation holes or any brackets.
4. Turn the NVR upside down and tighten the hard drive screws firmly to the casing of the NVR if needed.
5. Connect the hard drive cabling to the hard drives to provide power and data to the hard drives
6. Put the cover back onto the NVR 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.

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 an HDMI connection. Take a HDMI cable and connect one end to the HDMI port on your monitor/screen and the other end to the HDMI 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.
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.

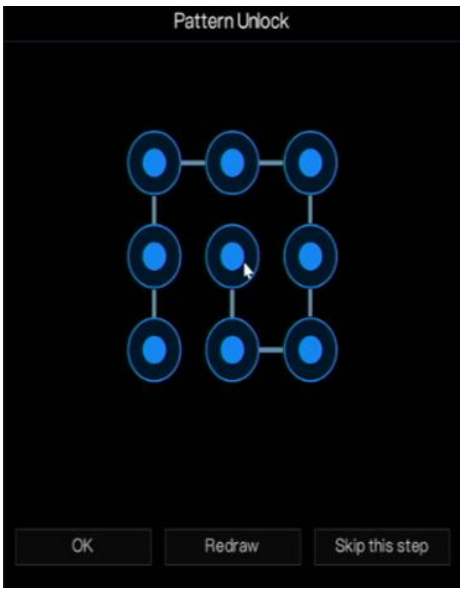
NVR Initialization

After applying power to the NVR, the system will turn on. Allow the NVR to finish loading. The **Activation** screen will appear. **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 ' " ; : &

Pattern Unlock

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 this step**' to skip the process.



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

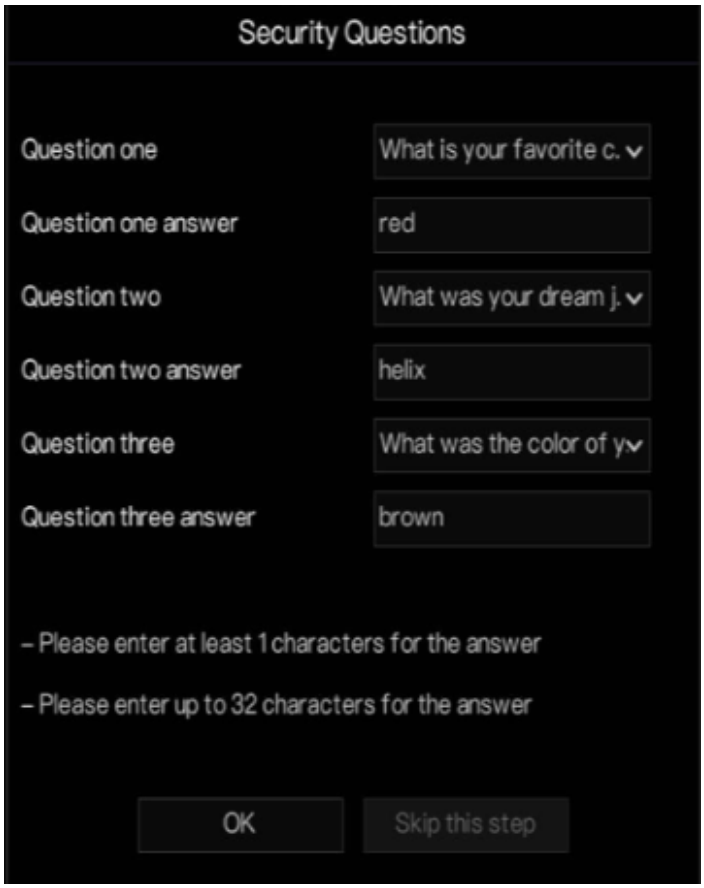
Email For Password Recovery

If you would like to reset your password using your email, enter a valid email address in the **Email Address** field. The email address will be retained in the system and can be used to recover your password. Click **OK** to continue.

Note: If you do not want to use an email for password recovery, click **Skip this step**.

Security Questions

As another 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 each field and enter the answers to those questions in the answer fields. Click **OK** to continue.



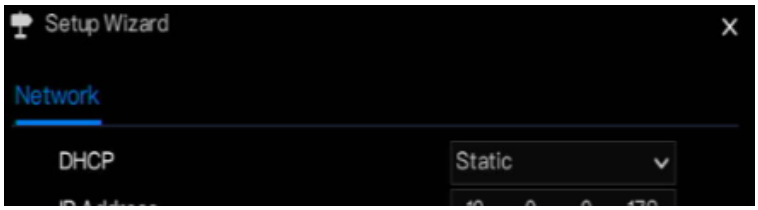
Note: If you do not want to apply security questions, click **Skip this step**.

Startup Wizard Walkthrough

The Startup Wizard allows you to set up any network, general info (date & time, time zone, DST), cameras, as well as manage any connected hard drives applied to the NVR.

Network

By default, the NVR's network mode will be set to DHCP which means your network has 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 DHCP dropdown menu and select **Static**.

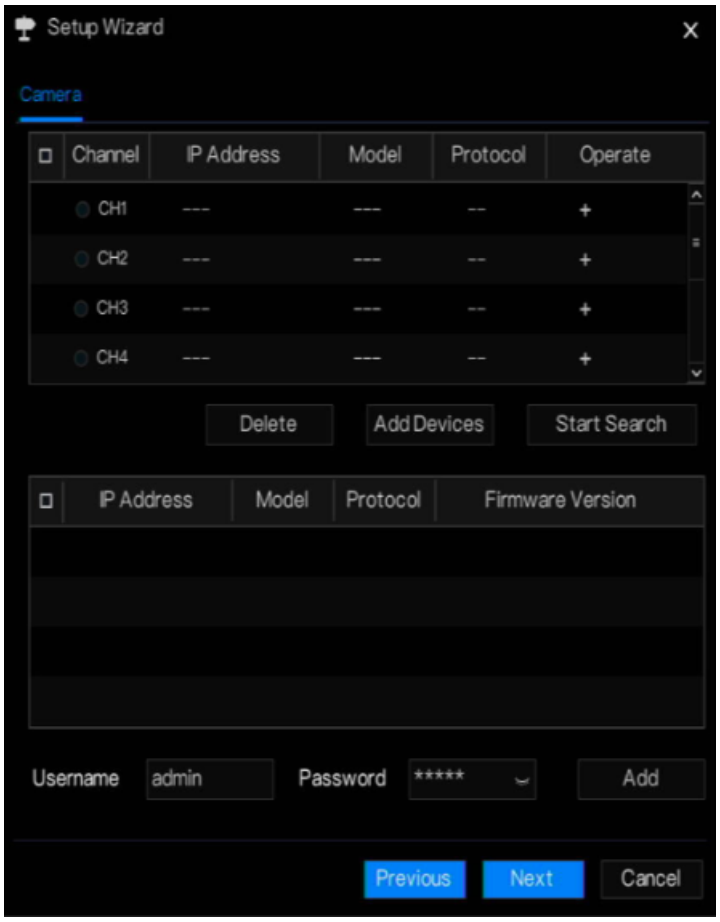


The NVR's IP address will be the address used to access your device using a web browser and use the web user interface. It is recommended to notate the IP address of your device if needed. Click **Next** to continue.

Camera

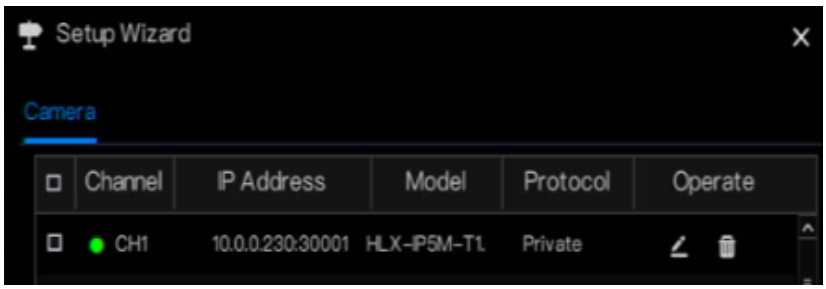
The next screen that appears is the **Camera** screen. This is where you can start adding cameras to the NVR. If the cameras are not directly connected to the back of the NVR, please make sure they are active and on the same network as the NVR before proceeding. The NVR can add third party cameras; however, most will use a separate protocol such as ONVIF, RTSP, etc. with limited features.

To begin adding a device, click on **Start Search** to allow the NVR to scan for connected devices on your network. A list of applicable devices will be displayed, select your devices by clicking on the checkbox next to them and click **Add**.



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 **Operate** column next to the device.

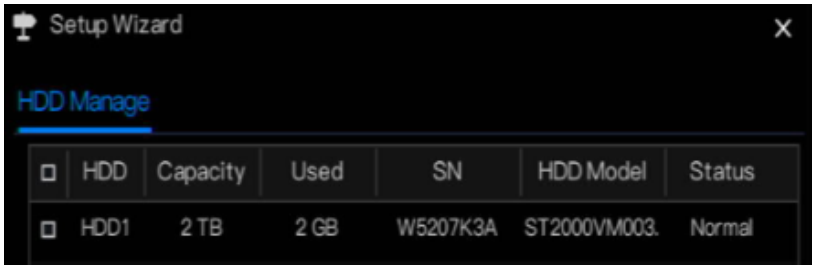
Select the **Password** field and enter the password for your camera. Once the password has been entered, click **OK**. The status indicator will turn green indicating the camera has been properly added and ready for use within the system.



Once all devices have been properly added to the system, click on **Next** to continue.

HDD Manage

The HDD manage menu allows you to view the status or format any hard drives that are connected inside the NVR.



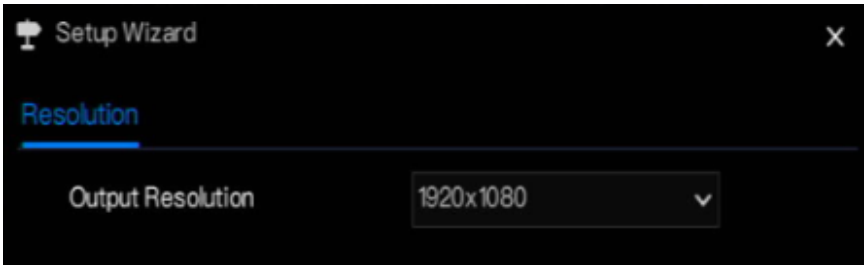
To format a hard drive, select a hard drive from the list and click **Format**. Click **OK** to allow the NVR to format the hard drive. Please note, all data on the hard drive will be lost after formatting. Click **OK** once formatting is complete. Click **Next** to continue.

P2P

The P2P menu allows you to connect your NVR to your mobile device using the Helix Pro app. The P2P status should read as “Online”. The Helix Pro app is available on both the Google Play and App Store. When adding the device into the app, scan the provided QR code in this menu and follow the instructions in the mobile app. Click the **Next** to continue.

Resolution

The resolution menu allows you to set the video output resolution of the NVR, from the device to the monitor. By default, this will be set to 1080p, however, can be modified if needed. Click Finish to complete the setup wizard.



Main Menu

The video wall will be displayed after the device has been activated. To access the main menu, right click on the video wall to display the main menu options.



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

CHANNEL: Add, search, review or edit settings for each camera, including video settings (e.g. quality, bit rate, color, etc.).
STORAGE: Set general, motion, or IVS schedules, as well as access the hard drive management interface, FTP, etc.
NETWORK: Review and edit network settings such as TCP/IP, DDNS, Email settings, etc. (e.g., P2P, UPnP, SNMP, etc.)
ALARM: Set motion, audio, IVS detection, set alarm in and out parameters (if applicable) and abnormality settings (e.g., hard drive, IP conflict, or network connection alarms).
SYSTEM: Review and edit general system settings such as passwords, firmware, date & time, as well as adding shared user accounts, etc.

IVS, Motion Detection, and Recording Setup

This section will cover how to set up a recording schedule for your NVR. This is applicable to continuous (24/7 recordings), motion detection, and IVS recordings. 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 procedures will be shown using the NVR's built-in local interface. However, these same steps can also be done using the web user interface on a computer in a web browser. For more information on how to access your device from a web browser, please refer to section, *"Computer Access Setup, pg. 13".* Please note, despite the difference in appearance, the settings pages have similar organizational structures.

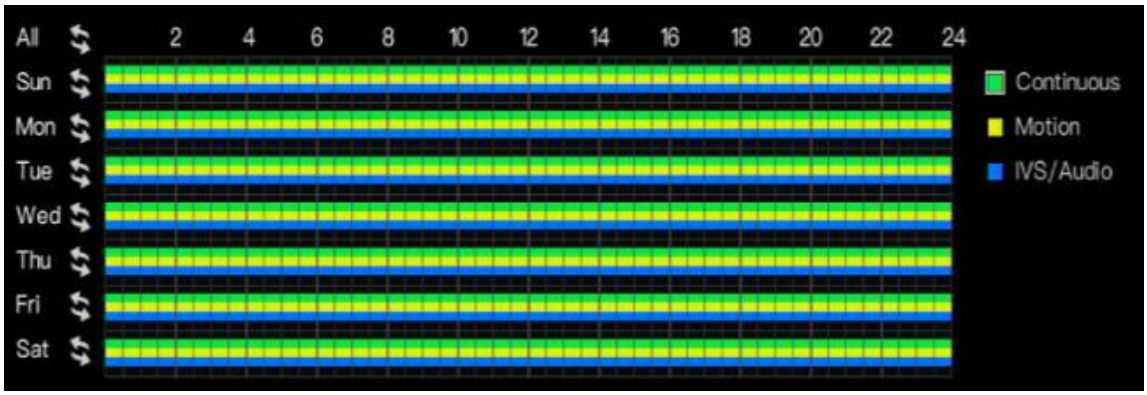
Setting Up Recording Schedules

1. From the **Main Menu**, locate the **Storage** menu and click **Schedule**.

Make sure you are in the **Record** tab in the schedule menu. 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 in the playback menu, if a hard drive is installed,

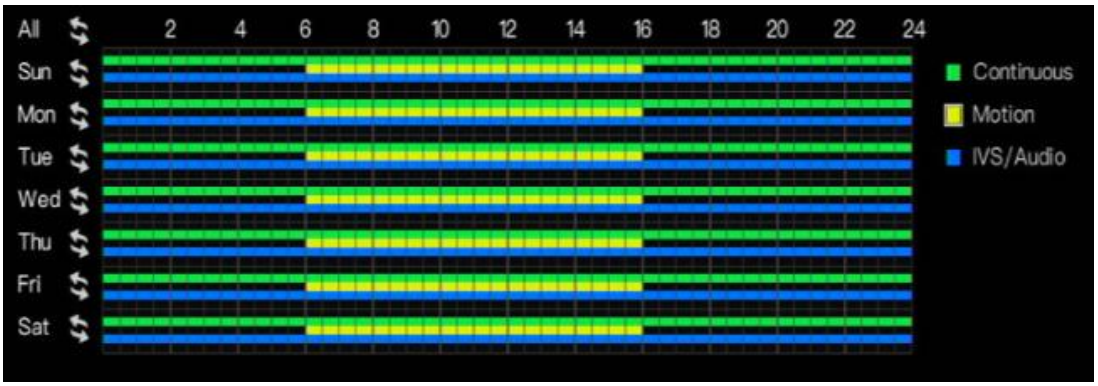
whereas snapshot events can be emailed. For more information on how to set up Email snapshots, please refer to section, *"Setting Up Email Alerts pg. 11".* By default, **Continuous** (24/7), **Motion** (Motion Detection) and **IVS/Audio (IVS & Audio Detection)** recording types will be activated for all days as indicated by the different colored bars available in this menu. To choose a channel (or camera) to configure, click the channel number next to **Channel**.

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.

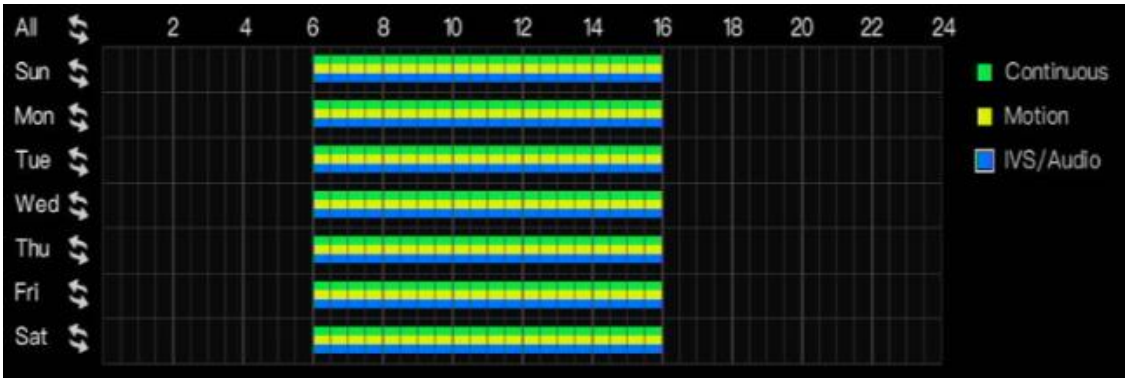


To edit a recording schedule, select a recording option from the colored boxes. Each recording option is color coded: Green: Continuous (24/7 recording), Yellow: Motion (Motion Detection), and IVS/Audio (IVS & Audio Detection). Select which recording type you would like to modify and use your mouse to adjust the time using the time bar for your specific recording type.

For instance, if you want to only record motion events between 0600 – 1600 (6am – 4pm) and have it applied to all days of the week, select the motion record type (yellow) and use your mouse to highlight the areas before 0600 and after 1600.



If you want to apply this schedule to other record types, select the record type and use your mouse to adjust the time bar. Click **Apply** to save the schedule.



Note: To restore a schedule back to default, select a record type and click the  icon.

Setting Up Email Alerts

Setting up email alerts will allow you to receive snapshots of events using your email. Each feature 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, locate the Network section and click **Email**.
2. 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**"
3. Enter a port number into the SMTP Server Port field. 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**.
4. Enter the email address you will be using in the **Username** field.
5. Enter the password for the email address in the **Password** field (please refer to your email provider's guides for how to allow third party apps or devices.
6. In the **Receiver** field, enter your email address. Enter that same email address in the **Email Sender** field.
7. Click **Apply** and **Test** to verify connectivity. A test email should be sent to the email address you entered. Once the test has been successfully sent, click **Apply.** to continue.

Setting Up Motion Detection

Motion detection events are different from IVS as they do not use AI algorithms to function. Once an object is detected, a recording or snapshot of the event will be retained to the hard drive. For more information on configuring motion detection, please refer to the information below.

1. On the **Main Menu**, locate the **Alarm** section and click **Motion Detection**.

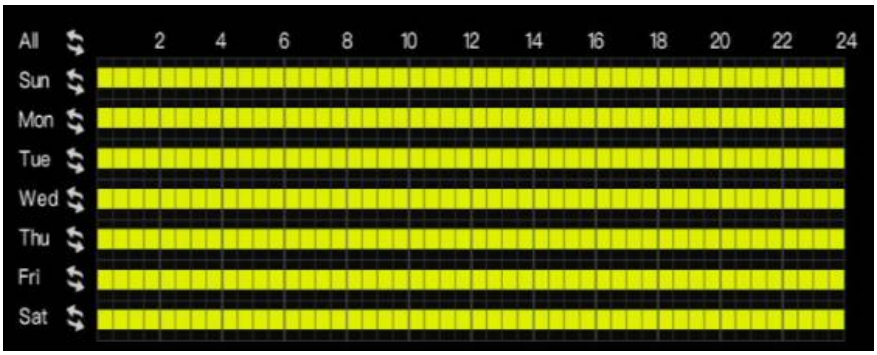
2. Select which channel to apply the rule and make sure the option is enabled. The detection area will be set to cover the entire area; however, you can use your mouse to customize and block out certain areas if needed in the **Detection Area** tab.

Sensitivity - is the measure of how many pixels on the screen need to change before being considered motion. By default, it will be set to medium, however, it can range from low to highest. Please note, adjusting the sensitivity higher than medium may cause more false alerts as the detection area will become more sensitive to movement.

3. Set any additional event actions such as sending an email of the event, buzzer, full screen, etc. and set a motion detection schedule if needed.

Adjusting Motion Detection Schedules

Motion detection schedules work the same as the schedules outlined in section: "*Setting Up Recording Schedules, pg. 9"* To adjust a motion detection schedule, click on the **Schedule** tab and use your mouse to adjust the timeline. Click **Apply** to save the schedule.



Setting Up IVS Events

The NVR does not have built-in AI features, such as IVS, however, it is supported by **a Helix camera** that supports IVS. IVS features supported by the NVR are tripwire, intrusion, and human/vehicle detection. Additional IVS settings, such as a warning light, can be enabled in the IVS setting menu. For more information on setting up IVS events, please refer to the information provided below.

1. On the main menu, locate the **Alarm** section and select **IVS**. Select a channel you would like to apply the rules to and click **Apply**.

Tripwire: Allows the device to trigger an event if an object crosses a set tripwire line.
Intrusion: Allows the device to trigger an event if an object appears or crosses a set area.
Human/Vehicle Detection: Allows the device to trigger an event if only a human or vehicle crosses a set detection area.

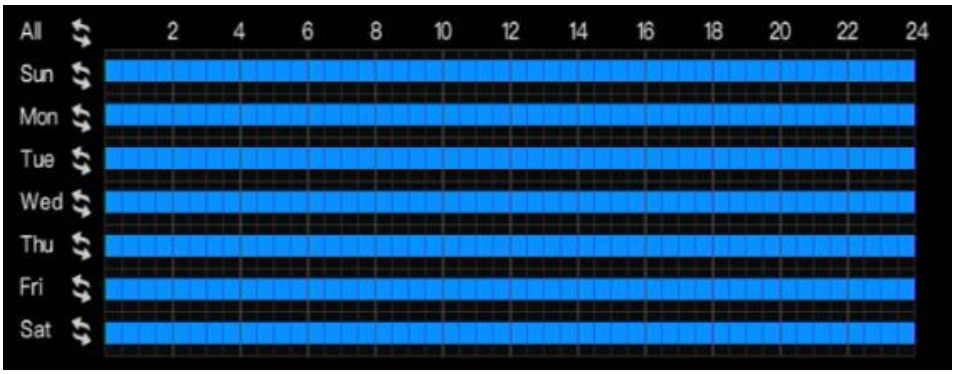
Note: Not all Helix cameras will support vehicle detection.

2. Use your mouse to draw a detection line or area on the interface and set which direction the object will travel for the rule to be triggered if needed. Click **Apply** once the detection line or areas have been drawn.

3. Set any additional event actions such as sending an email of the event, buzzer, full screen, etc. and set an IVS schedule if needed.

Adjusting IVS Schedules

IVS schedules work the same as the schedules outlined in section: "*Setting Up Recording Schedules, pg. 9."* To adjust an IVS schedule, click on the **Schedule** tab and use your mouse to adjust the timeline. Click on **Apply** to save your schedule.

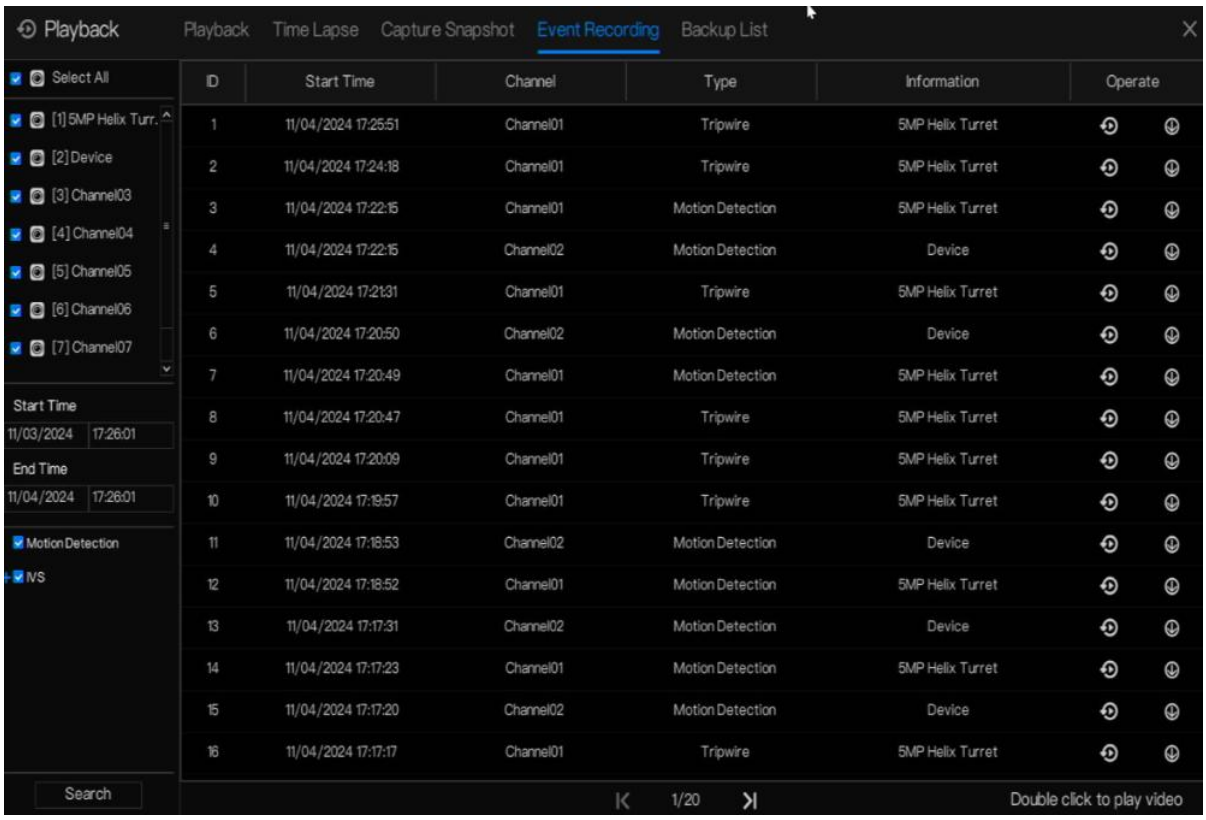


Playback

Recordings and snapshots of the events can be accessed in the **Playback** menu. **A hard drive must be installed to access and view recordings from this menu.** To access the playback menu, access the video wall menu and select the playback icon ( ) in the bottom panel.

To view recordings, select the camera or cameras you wish to view. Use the calendar to select applicable dates and times that apply to the events. A timeline of the recordings for the selected channels will appear in the timeline.
Different record types will be displayed as different colors, continuous (green), motion detection (yellow), and IVS/Audio (blue). Use the timeline options to scroll or manually view the recordings.

A list of all recordings can be located and viewed locally in the **Event Recording** menu.



Enter a start and end date & time range for the events and click **Search**. To play the event you can double click the video or click the playback icon ( ). If a USB flash drive is installed, you can download the file locally by clicking the download icon ( ).

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, laptops, or computers.

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 JavaScript technology which allows you to access it 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 user interface (web UI) using a web browser, please refer to the information provided below.

Locate the IP address for your device using the Helix IP Config Tool. This free software is available on our official web site.

The IP address for your NVR can also be found in the TCP/IP tab in the network menu. Enter this IP address into the browser and press enter to load the web user interface. 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 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 in a web browser and click the **Setting** gear wheel option.
2. Select **Network** and access the **Connection** menu.
3. Enter a port number into the HTTP Port field. The default port is 80, however, 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 and click **Apply**.
4. The system will automatically reboot, once the NVR comes back online it can be accessed again using the following format, "IPaddress:port number"
5. Access your router's user interface and port forward the device using the HTTP port information you entered 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 updated HTTP port number assigned to 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

6. Click on the **DDNS** menu located in the **Network** tab in the left panel. Enable DDNS and make sure the default protocol is selected. Enter a domain name for the NVR (one you create) in the **Domain Name** field. Click **Apply** once the DDNS details are entered. Click **Test** to test and confirm the DDNS connection is successful.

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

Upgrading the Firmware Using a Web User Interface.

1. Log into your NVR using a web browser and click on the Setting gear wheel option.
2. Click **System** and select the **Update** option.
3. Click Update and select the latest firmware file you downloaded to your computer.
4. Open the file, the NVR will automatically begin to update. Allow the device to update and reboot to complete the firmware update process.

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.

Upgrading the firmware for your NVR can be done locally, using a USB flash drive, or using the web user interface in a web browser. For more information on how to access the web user interface please see section, *"Computer Access Setup, pg. 13".*

Upgrading the Firmware Locally

1. Insert a USB flash drive into your computer.
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, locate the System menu and select **Firmware**.
5. Click **Upgrade**.
6. Select the firmware file listed in the Update menu and click **OK**.
7. Allow the system to be upgraded. The device may reset after the firmware update is complete.

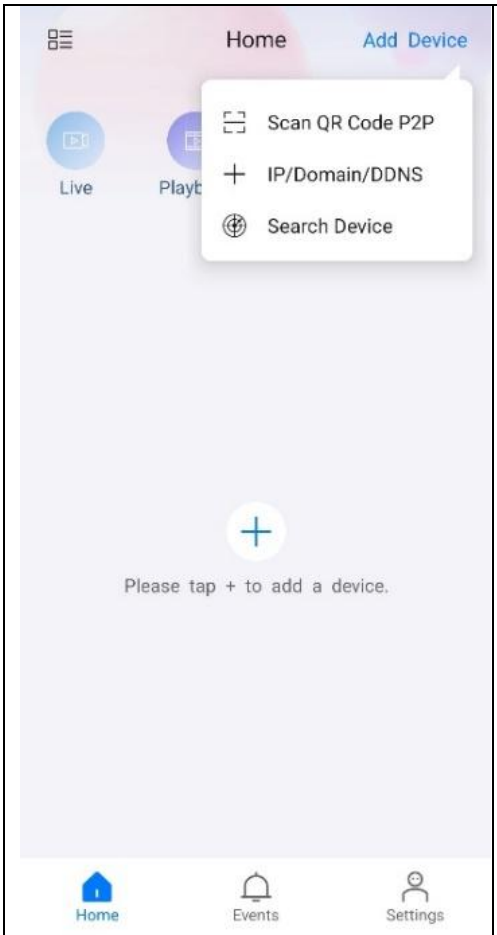
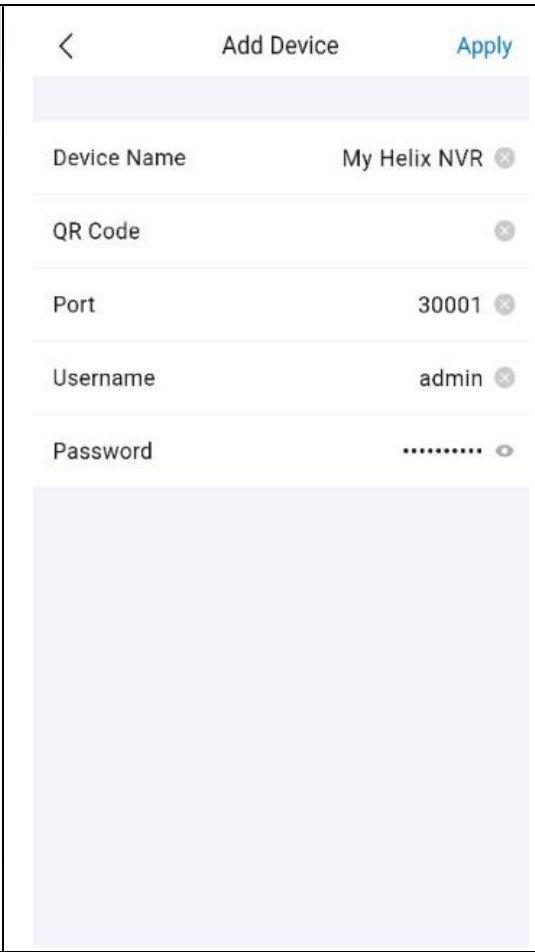
Upgrading the Firmware in a Web Browser

This may be the easiest and most convenient way of upgrading the firmware on your NVR. To begin, please refer to the information below on how to access your device in a web browser.

Helix Pro App Setup

The following steps will provide steps for setting up your Helix device in the Helix Pro app. The setup process for an Android phone and iOS version may be slightly different but most of this process is identical and easy.

Download and install the Helix Pro app from the App Store or Google Play Store. Open the app on your mobile device and allow the app to load. Please make sure your mobile device is on the same network as your NVR and the NVR is initialized before adding it to the app.

	
1. Open the app, tap **Add Device**, and select **Scan QR Code P2P**.	2. Scan the QR code or enter the UUID for the device manually. Enter a name for your device and password, then tap **Apply** to add the NVR to the app.

Note: To locate the QR code details, you must either have physical access to the NVR or access to the web interface using a web browser to access the P2P menu. The QR code details will be on the device or in the P2P menu.

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.