HLX-IP5M-B102EW-AI
5MP POE AI Bullet Camera
User Manual

Version 1.0.0

Contents

Installation Guide 3
Web User Interface Access 4
Live View 5
Playback 5
Settings 7
Camera 7
Audio 11
Network 11
Event 17
Storage 24
Destination 27
System 29
Information 31

Welcome

Thank you for purchasing a Helix camera!

This user manual is designed to be a reference tool for the installation and operation of your camera. This camera uses POE (Power-Over-Ethernet) to provide both power (802.3af) and data to the camera using a POE switch or injector using a standard Ethernet cable.

Important Security Warning

To keep your camera secure and prevent unauthorized access, please make sure to follow the steps below:



• Never use the default password for your camera. Always ensure that your password is at least 810 characters long and
contains a combination of lowercase characters, uppercase characters as well as numbers.

Overview

This fixed lens 5MP outdoor security camera delivers stunning ultra-high-definition video in 5-megapixel resolution, at 20 frames per second. It features a super wide 2.8mm angled lens which provides a wide 93.2° viewing angle. The camera features three different night vision modes which allows the camera to view objects at night up to 98ft away. It features an IR mode, which allows the camera to use IR LEDs to see at night, a white light mode, which allows the camera to use white light LEDs to achieve color night vision, and a smart illumination mode, which allows the camera to use IR LED to see at night, however, when a motion is detected, the deterrent LEDs will flash.

The camera also features a built-in microphone, on-board motion detection, built-in AI features, such as IVS, which can be used for enhanced perimeter protection, and smart motion detection which allows the camera to detect only humans in the area. The camera also features flexible storage options to store recordings to a microSD card (up to 256GB), SFTP/FTP, NAS, NVR, or using the Amcrest Cloud (optional). The device can be accessed using a web browser or using the Helix Pro app on a mobile device.

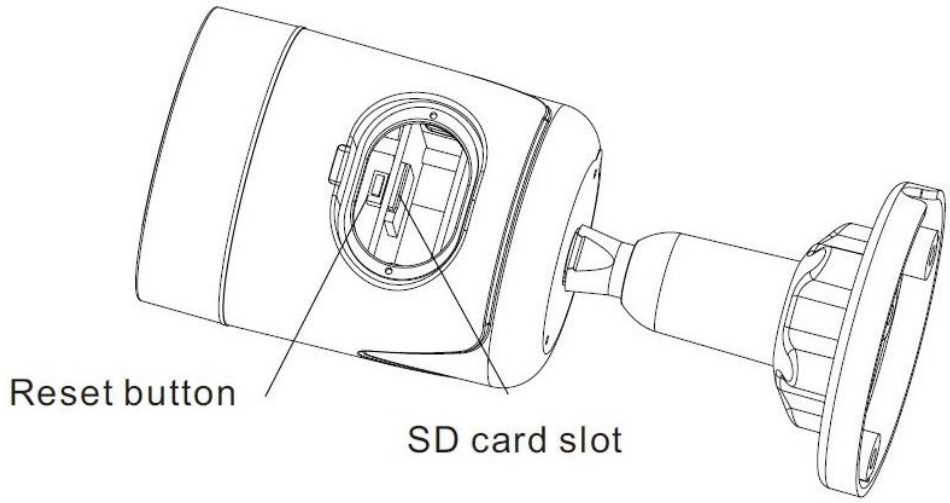
Installation Guide

Follow the steps and use the diagram in this section to install your camera.

MicroSD Card Installation

A microSD card can be used to store and view local recordings/snapshots. This camera requires a class 10 or above microSD card formatted to FAT32 to function. The camera can handle a max of 256GB of microSD card storage.

1. Remove the cover on the bottom of the camera using a Phillips Head screwdriver.
2. Locate the provided microSD card slot and insert the microSD card. The factory reset button will also be provided in this area.



3. Place the cover back onto the camera and secure it using the screwdriver.

Physical Installation

Before installing your camera, please make sure the installation surface can support at least 3 times the weight of the camera. To install the camera onto a wall, follow the steps below:

1. Place the installation template (sticker) onto the mounting surface.
2. Use a drill to drill the provided installation holes and insert the wall anchors. Please note, if running cables through the installation surface, a 1" paddle bit can be used to pull the wires through.
3. Connect any wiring to the camera then align the holes on the base of the camera with the wall anchors. Use the provided screws to secure the camera to the mounting surface.
4. Position the camera to the desired position. Use the locking mechanism on the base of the camera to adjust and secure the camera.

Accessing The Camera

The camera can be accessed using a laptop, desktop or mobile device. When accessing the camera for the first time, please make sure the camera is on the same network as a computer or mobile device. If using a mobile device, please make sure to download the Helix Pro app from the App or Play stores before proceeding.

Web User Interface Access

This camera features the latest JavaScript technology which allows you to access it using a wide variety of web browsers including Google Chrome, Firefox, Safari, or other mainstream web browsers using your PC or Mac **without the use of a plugin**.

To access your camera from your computer you will need to first locate the camera's IP address. To locate the camera's IP address, it is highly recommended to download our free Helix IP Config Tool.

In the All-Downloads menu, select the **Helix 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. Open the web browser and enter this IP address into the browser. Press Enter to access the web user interface. Enter the username and password (admin) for your camera and click **Login. Provide a new password for the camera and click Enter** to access the web UI.

Live View

By default, the interface opens on the Live View tab. The live view menu allows the user to see a live video feed from the camera. Use the Playback, Cloud Storage, and Settings, options to access these features. For more information on the features provided in the Live View menu, please refer to the details provided below.

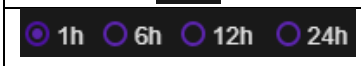
Main Stream: Displays the mainstream feed of the camera.
Sub Stream: Displays the sub stream feed of the camera (640x360). The stream will automatically switch to sub stream if the resources of the browser are too low.
Logout: Log the user out of the interface.

Button	Function Name	Function Description
	Snapshot	Manually take a snapshot of the live feed. The event will be downloaded to the default destination provided in the browser you are using.
	Record	Manually record a video of the live feed. The event (.mp4) will be downloaded to the default destination provided in the browser.
	Image Settings	Adjust image encode settings (takes you to the Encode menu).
	Audio	Listen to audio from the camera's built-in microphone.
	Motion Detected	Will be displayed once the camera detects a motion event
	Mic	Provides 2-way talk for applicable devices (not applicable).
	PTZ	Provides pan/tilt/zoom options for applicable devices (not applicable).
	Download Backup	Provides a list of upcoming event downloads. Click **Clear** to clear the download queue.
	Help	Provides quick access to the help center.

Button	Function Name	Function Description
	Wide Screen	Sets the aspect ratio of the stream to wide screen (16:9)
	Standard	Sets the aspect ratio of the stream to standard size (4:3)
	All	Sets the stream to fit the interface provided in the browser.
	Full Screen	View the stream in full screen.

Playback

The Playback menu allows the user to view and download recorded events that have been stored on a microSD card. This includes scheduled recordings, alarm records, snapshots, IVS events, etc.

File Type	Use this option to select between video recordings (.mp4) or snapshots (.jpg) of events.
< >	Use the provided arrows to select a date range of events. If events are present, the day in the calendar will be highlighted.
Scheduled Record	Use this record type to filter and view only continuous recording events.
Alarm Record	Use this record type to filter and view only alarm events.
IVS Event	Use this record type to filter and view only IVS events.
	Use the quick select option to jump to a specific area of the playback timeline. Click **Go** to jump to the selected portion of the timeline.
File List	Click this option to view all the recordings provided on a selected day. Recordings can be downloaded from the interface in this menu.
	Click this option to rewind the recording while it is being played.
	Use these options to pause or play the recording.
	Use this option to rewind the recording 3x faster.
	Use this option to fast forward the recording 3x faster.
	Use this option to manually take a snapshot of the recording. The event will be downloaded to the default destination provided in the browser you are using.
	Use this option to manually take a recording of the event being played. The event (.mp4) will be downloaded to the default destination provided in the browser.
	Use this option to listen to audio from the recording.
	Use this option to apply a start and end time of
	Use these options to set the timeline in a 1 hour, 6 hour, 12 hour, or 24 hour format.
Timeline	Use the timeline to scroll through events.

Cloud Storage

The Cloud Storage tab allows the user quick access to the Amcrest Cloud website (https://amcrestcloud.com). Amcrest Cloud allows you to access your device from anywhere in the world. **This is an optional cloud storage service provided by Amcrest** for your Helix device. Please note, you will need an Amcrest Cloud account before setting up your camera with Amcrest Cloud. You can register for an account in the cloud app or from the website at https://amcrest.com/cloud/



Note: The camera must be set up in the web UI **first** before you add it to the cloud. It cannot be added fresh out the box. To ensure the camera connects to the cloud, a reboot of your camera is recommended.

Settings

The Settings tab allows the user to view, update, and manage camera settings. This can include, encode, network, event, storage, system and other information related to your device.

Camera

This menu tab allows the user to change different camera settings including configuration, encode, and audio settings.

Configuration

The Configuration menu allows the user to configure image profiles for normal, day, and night usage. Below is an explanation for each of the fields on the Configuration tab in the Configuration menu item:

Image

The image tab allows the user to set picture, exposure, backlight compensation, night vision, and other image settings related to the camera.

Profile Management: Use this dropdown menu to select between automatic or scheduled profile settings. If using a scheduled profile, if using a daytime profile, enter a start and end time for the profile. If using a nighttime profile, select At Night to only apply at night. Click Apply to apply profile settings.

Picture

Brightness: This slider is used to adjust playback and record video window brightness. The value ranges from 0 to 100. The default value is 50. The larger the number, the brighter the video is. When you input the value here, the bright section and the dark section of the video will be adjusted accordingly. You can use this function when the whole video is too dark or too bright. Please note the video may become hazy if the value is too high. The recommended value ranges from 40 to 60.

Sharpness: This slider is used to adjust the sharpness of the video. The value ranges from 0 to 100. The larger the value is, the clearer the edges are and vice versa. Note: The higher the value, the higher likelihood of picture noise occurring. The default value is 50 and the recommended value ranges from 40 to 60.

Contrast: This slider is used to adjust playback and recorded video window contrast. The value ranges from 0 to 100. The default value is 50. The larger the number is, the higher the contrast is. You can use this function when the whole video brightness is OK, but the contrast is not correct. Please note the video may become hazy if the value is too low. If this value is too high, the dark section may lack brightness while the bright section may overexpose. The recommended value ranges from 40 to 60.

Saturation: This slider is used to adjust playback and record video image saturation. The value ranges from 0 to 100. The default value is 50. The larger the number, the stronger the color is. This value has no effect on the general brightness of the whole video. The video color may become too strong if the value is too high. For the grey part of the video, distortion may occur if the white balance is not accurate. Please note the video may not be clear if the value is too low. The recommended value ranges from 40 to 60.

Exposure

This menu allows the user to adjust exposure settings. By default, the camera will be set to automatically control exposure settings, however, the camera's exposure settings can be set to manual which will manually control the shutter speed. The shutter speed (exposure time) can be set from 1/5 – 1/20000 if needed.

BLC Mode

This menu allows the user to adjust back light compensation settings such as wide dynamic range, HLC, BLC, and defog.

WDR: Wide Dynamic Range makes multiple scans of a scene to provide one balanced and unwashed image that is clear for the user. Select this option if needed and use the provided slider to adjust the sensitivity.

HLC: Highlight compensation is a feature that came out of necessity due to overexposure from strong light sources like headlights or spotlights. Select this option if needed and use the provided slider to adjust the sensitivity.

BLC: Backlight compensation: Default will use the whole image to balance the lighting settings, and Customized will allow you to balance the lighting settings from the target area. Select this option if needed and use the provided slider to adjust the sensitivity.

Defog: Defog allows the camera to compensate the image to increase visibility in foggy or hazy weather conditions.

White Balance

This menu allows the user to adjust white balance settings. By default, this will be set to auto, which will allow the camera to automatically adjust the red and blue gain options for optimal use, however, the user can set this to manual if needed. If set to manual, use the **Red Gain** and **Blue Gain** sliders to manually adjust the white balance sensitivity of the area.



Scene

This menu allows the user to adjust and scene and image orientation of the live feed. For more details, please refer to the information below.

Scene: Use this dropdown menu to select whether the camera is in an indoor or outdoor environment.
Flip: Use this option to flip or rotate the feed.

Normal: The camera is at a normal (0°) viewing angle.
Horizontal: The camera is mirrored in a horizontal viewing angle.
Vertical: The camera is flipped at a 180° viewing angle.
Horizontal + Vertical: the image is flipped and mirrored at a 180° viewing angle.

Night Vision

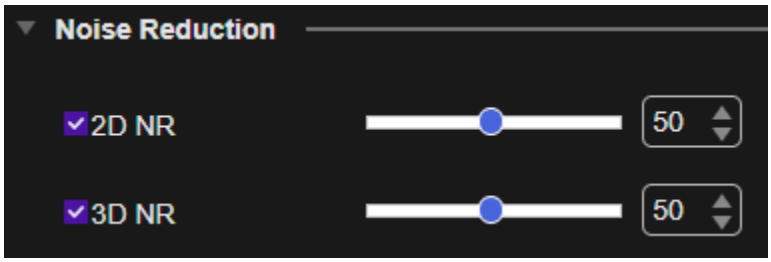
This menu allows the user to set night vision settings. The camera comes equipped with different night vision modes, for more details please refer to the information provided below.

Night Vision Settings: This dropdown box allows the user to select whether to turn the IR light on or off.

Smart Illumination: Allows the camera to switch on the IR LEDs, however once an object is detected the deterrent LEDs will flash.
White Light: Allows the camera to switch on the white light LED for color night vision.
IR Mode: Allows the camera to switch on the IR LEDs for B&W night vision.
Schedule: Allows the camera's night vision settings to only be activated during a start and end time set by the user.

Noise Reduction

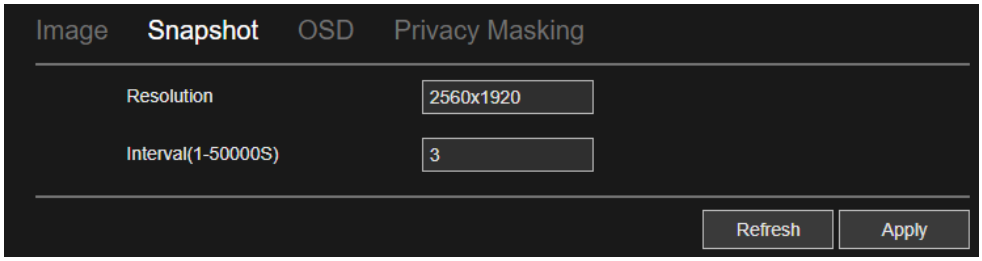
This menu allows the user to enable, disable, or adjust 2D and 3D noise reduction settings. Select 2D or 3D noise reduction options, use the sliders to adjust the sensitivity for each option.



To reset to default settings, click the **Reset Defaults** button. To Apply the settings, click the **Apply** button.

Snapshot

The snapshot tab allows the user to view snapshot resolution as well as the intervals (in seconds) in which the snapshots will be retained.



To refresh the interface, click the **Refresh** button. To Apply the settings, click the **Apply** button.

OSD

The OSD tab allows you to view, adjust, and modify overlays on your device, this includes the Helix logo overlay, date & time, device name, etc. The overlay will be displayed on the screen, select the overlay on the screen and use your mouse to place it on the screen.

Logo: Use this option to enable or disable the Helix logo overlay on the live feed.
Date & Time: Use this option to enable or disable the date & time overlay on the live feed.
Device Name: Add a name for the device and view it on the live feed.
Additional custom overlays can be added as well if needed. Select an overlay slot and align left or right. Enter text into the field and use your mouse to place it on the screen.

To reset to default settings, click the **Reset Defaults** button. Click the **Refresh** button to refresh the interface. To Apply the settings, click the **Apply** button.

Privacy Masking

Privacy Masking allows the user to place up to four privacy masks on the interface. This allows the user to block certain areas on the feed that wish to remain blocked or private. To add a privacy mask, click and hold your mouse on the interface, then drag over the selected area.



To refresh the interface, click the **Refresh** button. To remove all privacy masks, click **Remove All**. Click **Apply** to Apply the overlay settings.

Encode

The Encode menu allows the user to view and adjust encode settings. For more details, please refer to the information provided below.

Encode Type: This option allows the user to select between different compression types including H.264, H.265, and MJPEG.
Video Encode Level: This option allows the user to choose between a low, medium, or high-quality level.
Resolution: Use this dropdown menu to select a video resolution for the mainstream feed of the camera.
Frame Rate (FPS): Use this dropdown menu to select a frame rate for your device. The default will be 20 fps.
I Frame Interval: This field allows the user to set the P frame amount between two I frames. The value ranges from 1 to 60 seconds. The default value is 50.
Bit Rate Control: This dropdown box allows the user to select a bit rate type. The system supports two-bit rate types: CBR and VBR. In VBR mode, video quality can be set.
Bit Rate: This dropdown box allows the user to select a bit rate. This can range from 512kbps – 6144kbps.
Smart Encode: Smart codec is a function in most Helix cameras which aims to reduce bandwidth consumption without losing visible image quality by intelligently increasing compression where it will not make a visible difference in the scene.

Sub Stream is a lower quality stream that allows the feed to take up less resources and bandwidth when streaming. The Mainstream and the Sub Stream have the same fields. Sub Stream can be enabled by checking the box next to Enable.

To reset to default settings, click the **Reset Defaults** button. To refresh the screen, click on **Refresh**. To Apply the settings, click the **Apply** button.

Audio

This menu allows the user to modify audio settings for the camera. Below is an explanation for each of the fields on the Audio menu:

Microphone Type: The camera has a built-in microphone; this will be the default microphone type.
Microphone Volume: Use this slider to increase or decrease the microphone volume.
Speaker Type: The camera does not support two-way audio.
Speaker Volume: Use this slider to increase or decrease the speaker volume (if applicable).
Encode Mode: Select between AAC, G711.a, G711.u, and PCM audio formats.
Sampling Frequency: The default sampling frequency of the device will be 8000.

To reset to default settings, click the **Reset Defaults** button. To refresh the screen, click on **Refresh**. To Apply the settings, click the **Apply** button.

Network

This menu allows the user to modify, update, or adjust network settings associated with your camera. This includes TCP/IP, HTTPS, SMTP, and other network related settings.

TCP/IP

TCP/IP stands for Transmission Control Protocol/Internet Protocol and it is the language/protocol that allows communication between an internet-connected device, whether on a local network or the Internet. This screen allows for TCP/IP settings to be modified for the camera to establish a connection to the network.

Mode: Switch between a DHCP or static IP mode.
IP Address: Displays the current IP address of the device.
Subnet Mask: Displays the current subnet mask of the device.
Gateway: Displays the default gateway associated with your device.
Obtain DNS automatically: Enable or disable the ability to allow the camera to automatically obtain a DNS.
DNS1: Displays the preferred DNS server IP address.
DNS2: Displays the alternate DNS server IP address.
MTU(800 – 1500): Controls the largest size of data packets that the camera can send over the network. The default value is 1500.

To reset to default settings, click the **Reset Defaults** button. To refresh the page, click the **Refresh** button. To Apply the settings, click the **Apply** button.

P2P

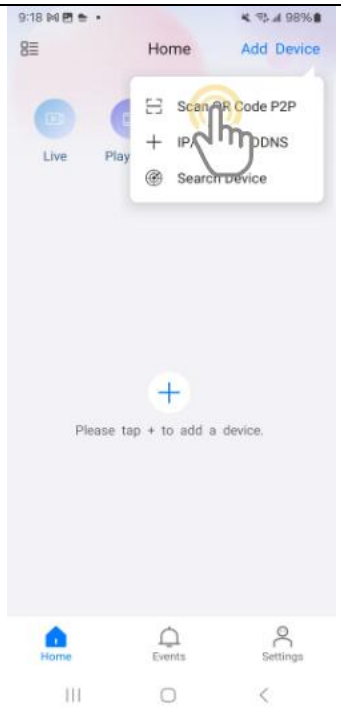
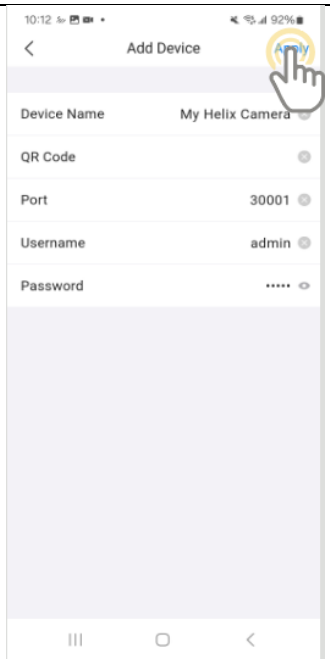
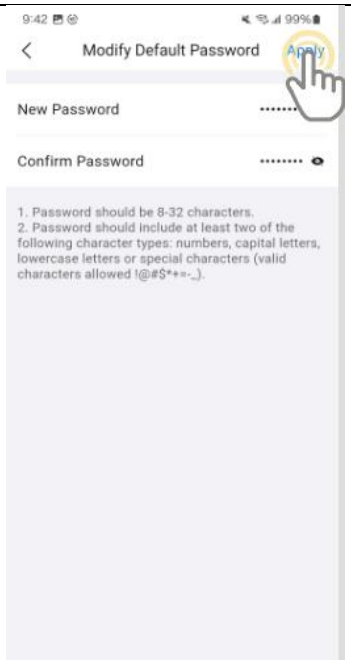
The P2P menu provides the user with a QR code to connect their camera to various apps using P2P, such as the Helix Pro app. P2P must be enabled and active to function. Below is an explanation of the fields on the P2P settings tab:

Enable: This option allows the user to enable the P2P feature for the camera. This feature must be enabled for the camera to connect to a smartphone or tablet via the Helix Pro app. It is enabled by default.
Status: This field displays the status of the P2P connection. Once the camera is connected to a device, this field should display the word Online.
S/N: This field displays the Token ID for the camera. The Token ID can be used to manually enter the camera's information on a mobile or tablet device in case the QR code scanning feature cannot be used.
QR Code: This image is a Quick Response (QR) code. By scanning this image using the Helix Pro app, this camera can establish a connection with the app.

To reset to default settings, click the **Reset Defaults** button. To refresh the page, click the **Refresh** button. To Apply the settings, click the **Apply** button.

Helix Pro App

To add your Helix camera into the Helix Pro app, follow these steps:

	
Open the app, tap **Add Device**, and select **Scan QR Code P2P**.	Scan the QR code on the device or manually enter the serial number by selecting **Manually Enter QR Code**.
	
Enter a name for the device in the Device Name field. Enter the default password (**admin**) for the camera in the Password field. Tap **Apply**.	Enter a new password for the camera and tap **Apply**.

Connection

The Connection menu allows the user to view and modify connection ports related to the camera.

HTTP Port: Designates the Hypertext Transfer Protocol (HTTP) port number. The default value is 80.
RTSP Port: Designates the Real Time Streaming Protocol (RTSP) port number. The default value is 554.
HTTPS Port: Designates the Hypertext Transfer Protocol Secure (HTTPS) port number. The default value is 443.
Max Connection: This field displays the maximum number of connections allowed for the camera.

To refresh the page, click the **Refresh** button. To Apply the settings, click the **Apply** button.

ONVIF

The ONVIF menu allows the user to access and configure various functionalities through a standardized protocol. This is useful if you want to integrate your camera with third-party software or NVRs that also support ONVIF.

Protocol Name: Displays the protocol used (ONVIF)
Protocol Version: Displays the ONVIF version.
Protocol Software: Displays the ONVIF software version.
ONVIF UUID: Displays the UUID (Universally Unique Identifier) for the ONVIF protocol.
Profile_G: Enable or disable the ability to connect to third party devices that support Profile_G interoperability.
Media2: Enable or disable the ability to connect to third party devices that support Media2 interoperability.
Authentication: Enable or disable the ability to provide additional authentication when using ONVIF protocol.
RTSP: Enable or disable the ability for the camera to connect using an RTSP protocol. The RTSP URL format will be as follows: rtsp://ip:port/channel ID/stream ID

To refresh the page, click the **Refresh** button. To Apply the settings, click the **Apply** button.

RTMP

RTMP stands for **real-time messaging protocol**. It provides a high-performance transmission of video, and data from an encoder such as an IP camera to a server, which distributes the signal across the internet. Below is an explanation of the options provided in this menu.

Protocol Name: Displays the protocol used (RTMP)
Protocol Version: Displays the RTMP version.
Protocol Software: Displays the RTMP software version.
Enable: Enable/disable the RTMP protocol (mainstream bitrate should be lower than 2048 kbps).
Audio: Enable/disable Audio in the RTMP stream (Audio format must be AAC).
IP Address: Enter a custom address for the RTMP protocol (URL/Stream Key)
StreamID: Displays which stream is being used for the RTMP protocol.
Status: Displays the status of the RTMP stream.

To reset to default settings, click the **Reset Defaults** button. To refresh the page, click the **Refresh** button. To Apply the settings, click the **Apply** button.

DDNS

DDNS stands for Dynamic Domain Name Server. This technology is used to automatically update name servers in real time to help the camera maintain a persistent address despite changes in location or configuration. What this

means is that even when the camera is restarted, moved, or reconfigured, it can keep the same IP address, thus allowing remote users uninterrupted access to the camera, rather than having to request a new IP address to use for remote access anytime a change is made.

To use this feature, users will need to set up an account with a DDNS service. The camera supports a variety of DDNS services such as HelixDDNS, NO-IP DDNS, CN99 DDNS, and Dyndns DDNS. Based on which service is selected, different options may show on this screen. For the purposes of this guide, HelixDDNS will be used. HelixDDNS is a free DDNS service. Ensure the device has been properly port forwarded in your router (HTTP port) and access the web UI. Access the DDNS menu and click Enable. Select the DDNS protocol and enter a unique domain name for the device (DomainName/helixddns.com). Click **Test** to test the connection.



Once the test is complete, click **Apply** to Apply the domain name. To refresh the page, click the **Refresh** button.

IP Filter

This screen allows for the filtering of IP addresses, either blocking them, or granting them access to the camera. This feature helps make the camera more secure by limiting remote access only to approved users. Below is an explanation of fields on the IP Filter settings screen:

IP Filter: This option allows the user to enable the IP Filter feature for trusted sites.
Rule Type: Select if the IP will be blocked or allowed.
Block List: Use the "+" and "-" icons to add or remove an IP from the block list. Add an IP segment (start IP and end IP) to the list. To remove, select the IP from the block list and click the "-" icon. To edit an IP segment, click the Edit option and edit the IP segment manually.

To reset to default settings, click the **Reset Defaults** button. To refresh the page, click the **Refresh** button. To Apply the settings, click the **Apply** button.

SMTP (Email)

This screen allows for the configuring of email settings to permit the camera to send emails when an alarm is triggered. To automatically set the SMTP protocol, select Google, Outlook.com, Comcast, Yahoo, or Other if needed. Below is an explanation of fields on the SMTP (Email) settings screen:

SMTP Server: SMTP stands for Simple Mail Transfer Protocol. This will display SMPT server details. For instance, if using Gmail, the protocol will be "smtp.gmail.com".
SMTP Server Port: This field allows the user to enter the port that corresponds to the selected SMTP server.
Username: This field allows the user to enter the SMTP username (Email address for admin user).
Password: This field allows the user to enter the password associated with the SMTP username. If using Gmail, please make sure to enter the generated app password provided by Google in this field.
Sender: This field allows the user to enter the sender email address. This email address will be the one that sends out all emails pertaining to the alerts and alarm emails sent by the camera.
Email Title: This field allows the user to define the subject line of the email that is sent to the receivers.
Attachment: This option allows a snapshot of the event to be attached to the email notification.

Recipients: This field allows the user to enter the receiver email addresses. These email addresses are the ones that will receive any emails pertaining to alert and alarm emails sent by the camera. Up to 3 email addresses can be entered in this field.

SSL Encryption: Select which authentication type is being used for the SMTP port.

SSL: Secure Socket Layer. This was the original encryption protocol used for securing communication channels. (Port: 465)

TLS: Allows an initially unencrypted connection to be upgraded to a secure one using TLS. Uses port 587 for SMTP.

OFF: Provides no encryption on email alert notifications.

Sending Intervals: This field allows the user to define, in minutes, how long the system should wait between sending emails. This prevents multiple emails from being sent out.

Test: Click this option to test the SMTP connection. A test email notification will be sent to your email to verify the connection. Please make sure to select Apply to Apply SMTP settings before testing.

To reset to default settings, click the **Reset Defaults** button. To refresh the page, click the **Refresh** button. To Apply the settings, click the **Apply** button.

UPnP

UPnP stands for Universal Plug and Play, and it is a protocol used to easily connect devices to the internet. In the case of this camera, it allows the camera to connect to the router in an easy manner to quickly allow for remote access. Below is an explanation of fields on the UPnP settings screen:

UPnP Enable: This option allows the user to enable the UPnP function.

Mode: This dropdown menu allows the user to set UPnP modes:

Manual: Allows the user to set customized UPnP port numbers.

Auto: Allows the device to set UPnP settings automatically.

HTTP Port: Enter the HTTP port of the UPnP mapping.

HTTPS Port: Enter the HTTPS port of the UPnP mapping.

RTSP Port: Enter the RTSP port of the UPnP mapping if needed.

Client Port: Enter the UPnP client port.

To refresh the page, click the **Refresh** button. To Apply the settings, click the **Apply** button.

SNMP

SNMP stands for Simple Network Management Protocol. It's a tool used to manage and monitor network devices like Helix IP cameras. It can be used to monitor device information by allowing authorized software to collect info about the camera, like its model, IP address, and video resolution, configuration changes, etc.

Helix cameras typically support SNMP versions 1, 2, and 3. For security reasons, it's recommended to use SNMPv3, which offers encryption and authentication. Enable an SNMP option and enter the requested details into the interface.

SNMPV1: The original version of Simple Network Management Protocol, it uses unencrypted communication in plain text and provides a less secure weaker authentication method with minimal security.

SNMPV2C: A variant of SNMPv2 that offers some minor improvements over SNMPv1, but still has significant security limitations.

SNMPV3: The third version of Simple Network Management Protocol, represents a significant leap in security compared to SNMPv1 and SNMPv2c. It provides more secure communication and stronger authentication by encrypting data transmission using algorithms such as AES.

To refresh the page, click the **Refresh** button. To Apply the settings, click the **Apply** button.

HTTPS

Hypertext Transfer Protocol Secure (https) is a combination of the Hypertext Transfer Protocol (HTTP) with the Secure Socket Layer (SSL)/Transport Layer Security (TLS) protocol. This menu allows the user to enable a secure HTTPS/SSL connection. Please make sure that a root certificate has been created and applied before enabling HTTPS. To refresh the page, click the **Refresh** button. To Apply the settings, click the **Apply** button.

Certification

This option allows the user to create a root cert to allow a secure HTTPS/SSL connection in the web browser. To create a root certificate, enter the country, state or province, city, etc. and click **Create Cert**. The device will reboot. Log back into the device and access the HTTPS menu, click **Certification** then click **Export** to export the cert to your computer.

Once the cert has been installed and applied to your computer, navigate back to the web interface, and access the HTTPS menu. Click on the **Enable** option in the HTTPS menu, click **Apply** and allow the device to reboot and enable HTTPS in the browser.

Upload

This option allows the user to upload a customized HTTPS root certificate and key that will apply the HTTPS cert to the camera. A self-signed certificate (created by yourself) can work within your network. However, for a secure internet connection, a certificate from a trusted Certificate Authority (CA) is highly recommended. Upload the cert and key and click **Apply**, allow the device to reboot and enable HTTPS in the browser.

Event

This menu allows the user to change different settings for triggering events such as motion detection, audio detection IVS, etc.

Motion Detection

The motion detection menu allows the user to set and enable settings for motion detection such as setting motion detection areas, email notifications, and schedules.

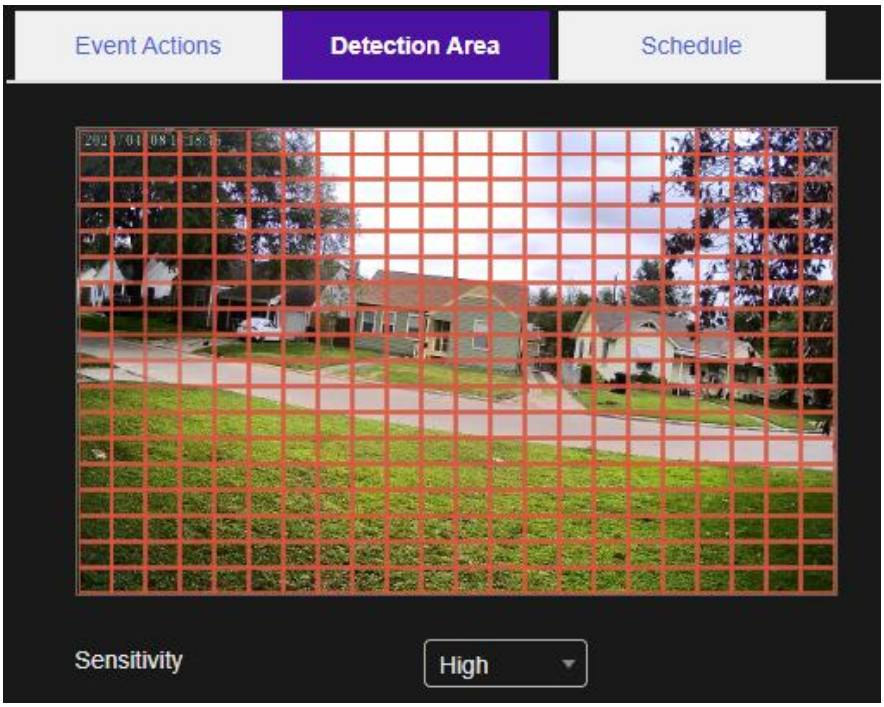
Event Actions

Enable: Enable or disable motion detection.
Send Email: Enable the camera to send an email when a motion detection alarm is triggered.
Snapshot: Enable the camera to take a snapshot when a motion detection alarm is triggered.
Record: Enable the camera to record video when a motion detection alarm is triggered.
Record Time: The amount of time the motion event will record.

To reset to default settings, click the **Reset Defaults** button. To refresh the page, click the **Refresh** button. To Apply the settings, click the **Apply** button.

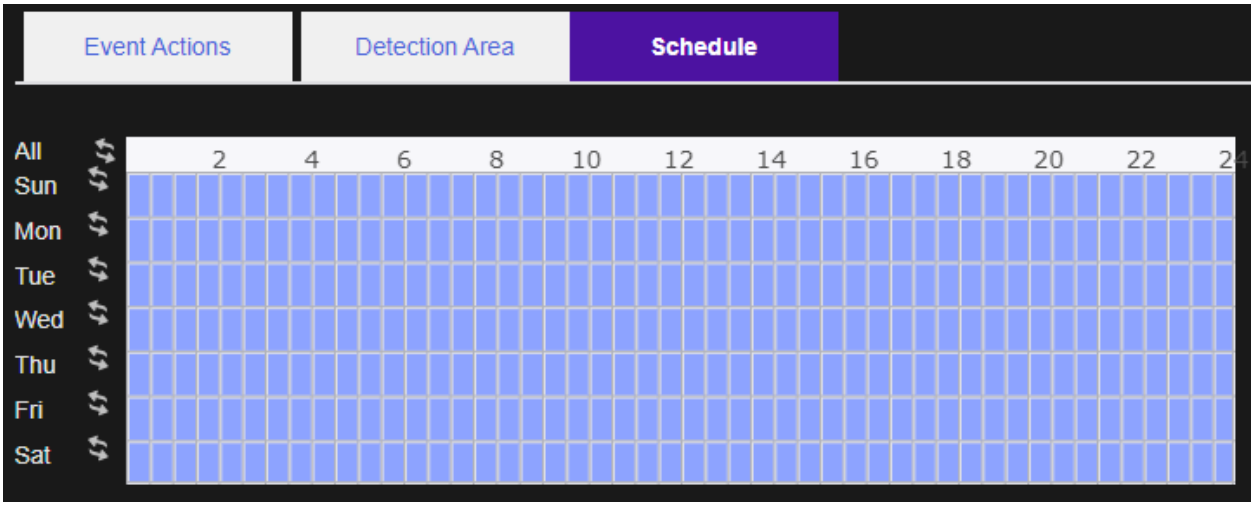
Detection Area

This menu allows the user to set areas in which motion detection will apply or not apply. The grid will display all areas that are applicable to motion detection. Use your mouse to remove or customize detection areas if needed. The sensitivity dropdown menu will allow the motion detection to be set to highest, high, medium, and low. Please note, the higher the sensitivity the more notifications you may receive.

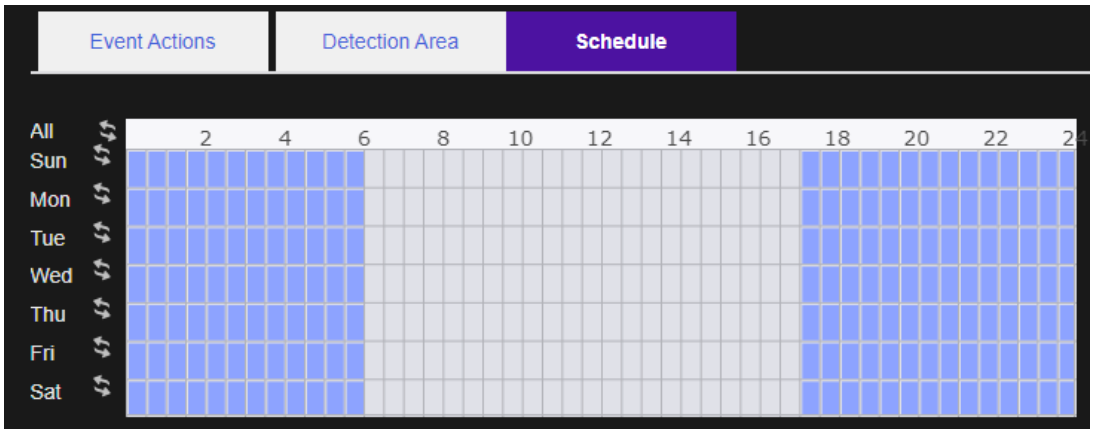


Schedule

This menu allows the user to set a motion detection schedule. This will allow motion detection to only apply on a specific date & time if needed.



Click and drag to set motion detection for certain dates and times. For instance, if you would like motion detection to only apply at 6am till 5pm all week, click and drag the applicable area on the interface and click **Apply**.



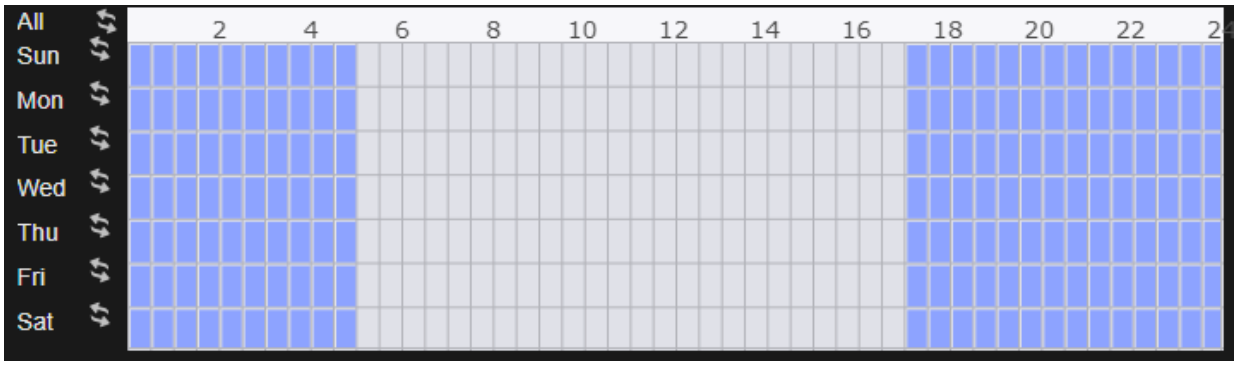
To remove a schedule, click the icon. This can apply to the whole schedule or specific days if needed.

To reset to default settings, click the **Reset Defaults** button. To refresh the page, click the **Refresh** button. To Apply the settings, click the **Apply** button.

Audio Detection

This menu allows the user to modify audio detection settings. Below is a screenshot of the Audio Detection screen: Below is an explanation of the fields on the **Audio Detection** tab:

Rise: Enable or disable audio detection.
Send Email: This option allows the user to enable the camera to send an email when an audio detection alarm is triggered.
Snapshot: This option allows the user to enable the camera to take a snapshot when an audio detection alarm is triggered.
Record: This option allows the user to enable the camera to record video when an audio detection alarm is triggered.
Record Time: The amount of time the audio event will record video.
Schedule: This menu allows the user to set an audio detection schedule. This will allow audio detection to only apply on a specific date & time if needed.



To reset to default settings, click the **Reset Defaults** button. To refresh the page, click the **Refresh** button. To Apply the settings, click the **Apply** button.

IVS

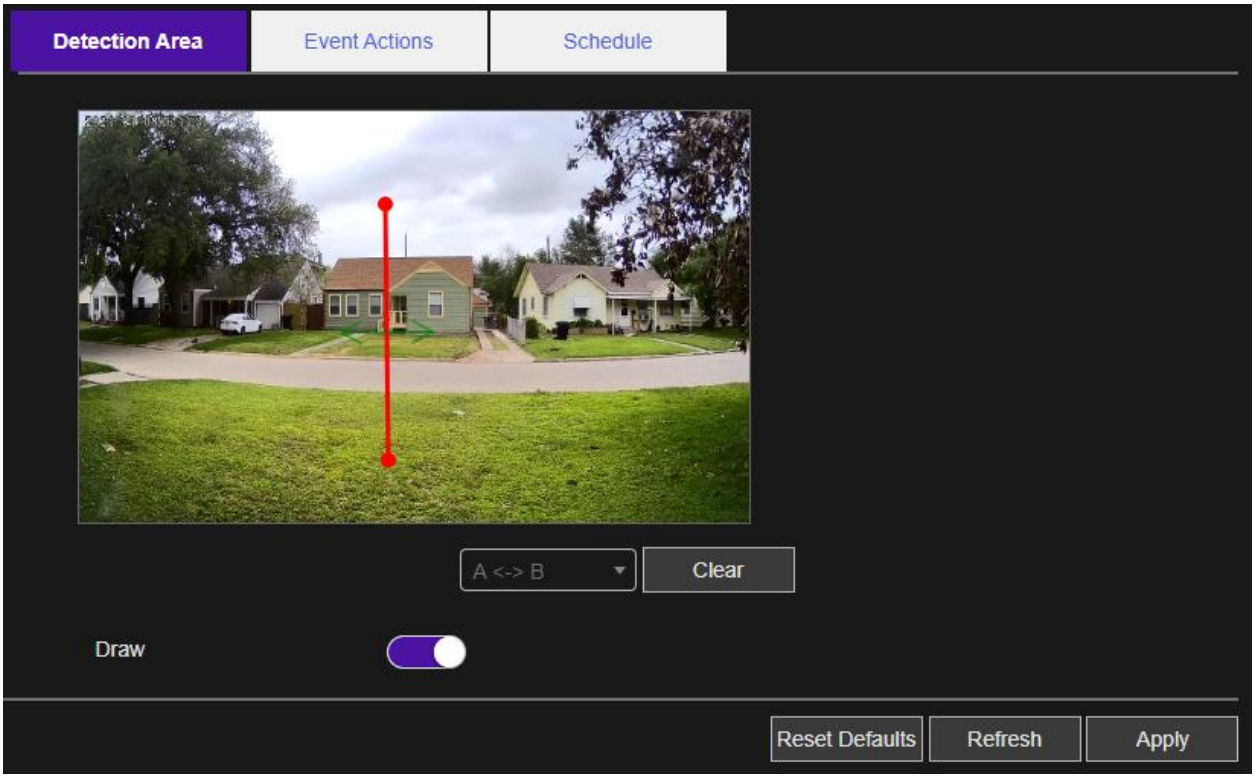
IVS stands for Intelligent Video Surveillance, the features provided in the IVS menu allow the camera to use deep learning algorithms to analyze video footage and provides more advanced security features than traditional motion detection. Features such as tripwire and intrusion provide more advanced perimeter protection while features such as human detection will only alert you if a human is detected decreasing false alerts.

Tripwire

Tripwire allows the camera to trigger an event if an object crosses the set tripwire line. Click **Enable** to enable the tripwire feature then click **Apply**.

Detection Area

This option allows the user to set a tripwire detection line. To set a tripwire line, click **Draw** and use your mouse to draw a detection line. Use the directional dropdown menu to set which direction the object will be going for the tripwire to be triggered. It can be set left, right, or in both directions (A<->B). Click the Clear option to remove the detection line.



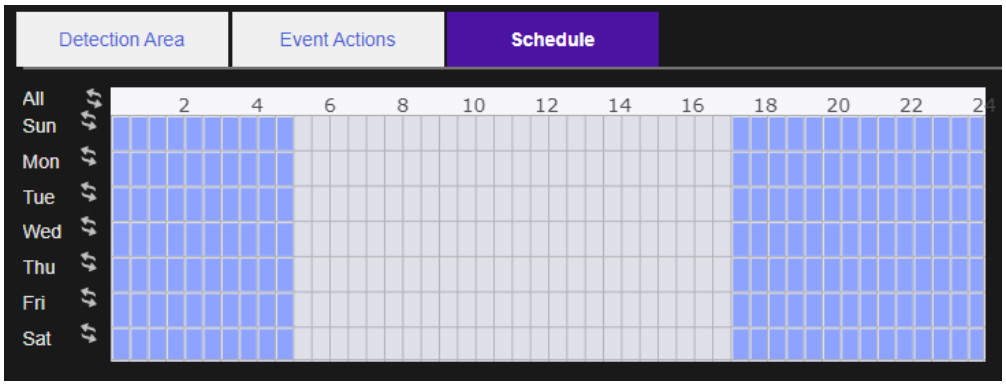
Event Actions

This option allows the user to set actions such as email notifications and record.

Send Email: Allows the user to enable the camera to send an email when an IVS event is triggered.
Snapshot: Allows a snapshot of the IVS event to be sent via email when triggered.
Record: Allows the event to be recorded to a microSD card after the event is triggered.
Record Time: The amount of time the event will record after it has been triggered.

Schedule

This option allows the user to set an IVS schedule. This will allow the rule to only be triggered at specific dates & times customized by the user. For instance, if you would like an IVS rule to only apply at 6am till 5pm all week, click and drag the applicable area on the interface and click **Apply**.



To remove a schedule, click the icon. This can apply to the whole schedule or specific days if needed.

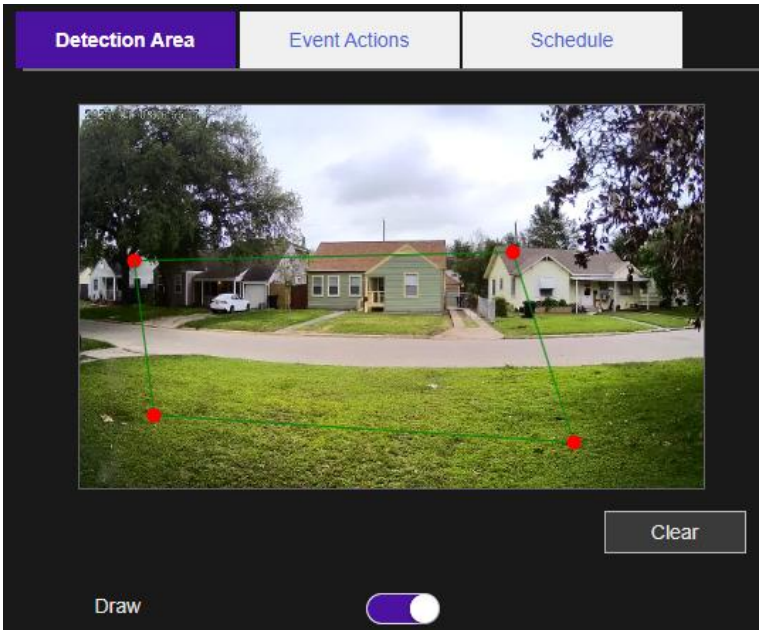
To reset to default settings, click the **Reset Defaults** button. To refresh the page, click the **Refresh** button. To Apply the settings, click the **Apply** button.

Intrusion

Intrusion allows the camera to trigger an event if an object appears or crosses a set intrusion area set by the user. Click **Enable** to enable the feature then click **Apply**.

Detection Area

This option allows the user to set a detection area. By default, the detection area will be set to full screen, however, to adjust the area click **Draw** and use your mouse to set a customized detection area. Click **Apply**.



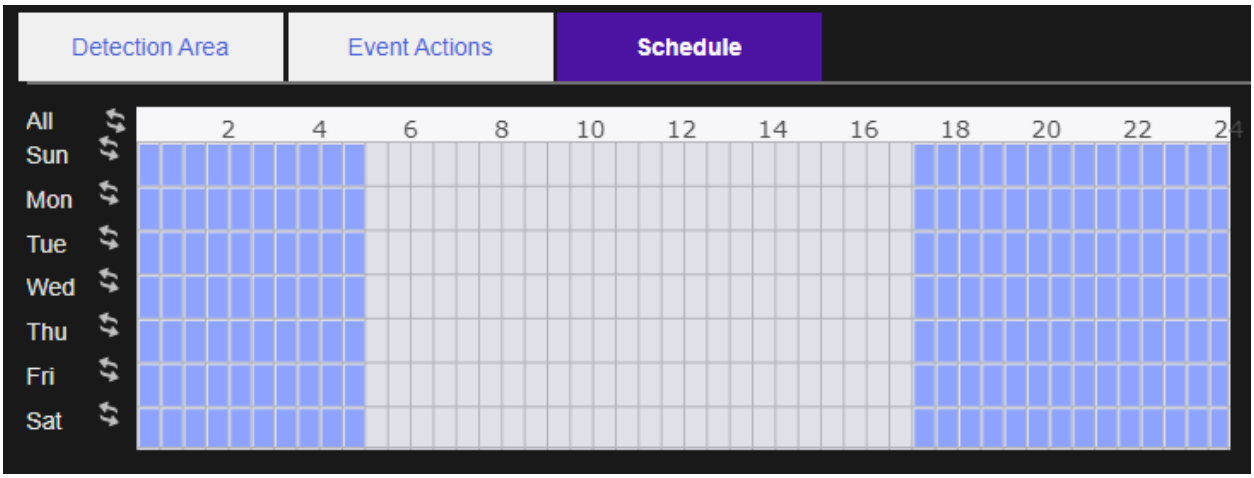
Event Actions

This option allows the user to set actions such as email notifications and record.

Send Email: Allows the user to enable the camera to send an email when an IVS event is triggered.
Snapshot: Allows a snapshot of the IVS event to be sent via email when triggered.
Record: Allows the event to be recorded to a microSD card after the event is triggered.
Record Time: The amount of time the event will record after it has been triggered.

Schedule

This option allows the user to set an IVS schedule. This will allow the rule to only be triggered at specific dates & times customized by the user. For instance, if you would like an IVS rule to only apply at 6am till 5pm all week, click and drag the applicable area on the interface and click **Apply**.



To remove a schedule, click the icon. This can apply to the whole schedule or specific days if needed.

To reset to default settings, click the **Reset Defaults** button. To refresh the page, click the **Refresh** button. To Apply the settings, click the **Apply** button.

Human Detection

This option uses an advanced algorithm to differentiate between human and non-human shapes within a scene and send notifications only when a person is detected decreasing false alerts. To begin setting up this feature, click **Enable** then click **Apply**.

Detection Area

This option allows the user to set a detection area. By default, the detection area will be set to full screen, however, to adjust the area click **Draw** and use your mouse to set a customized detection area. Click **Apply**.

Event Actions

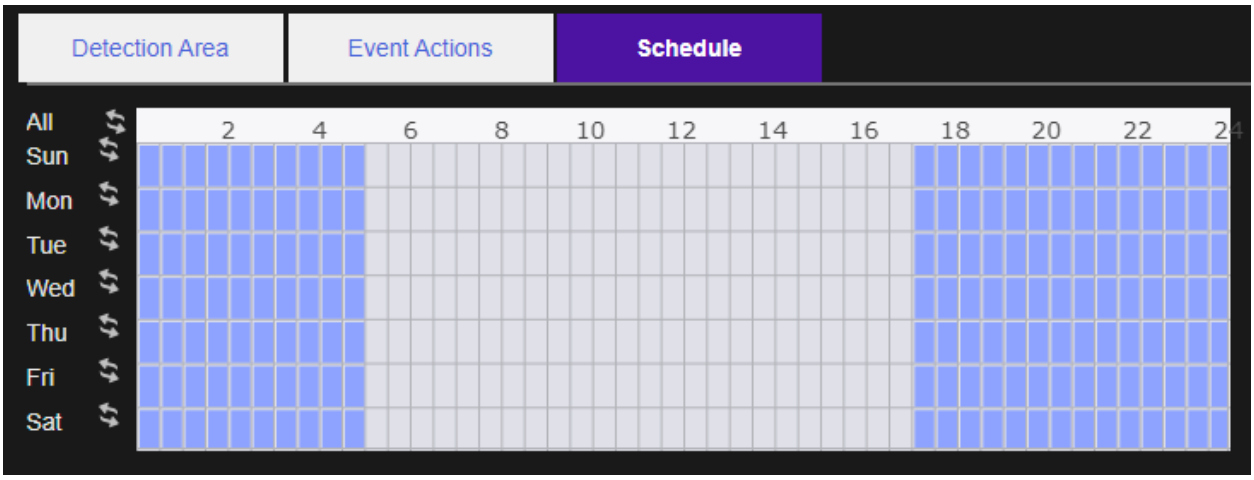
This option allows the user to set actions such as email notifications and record.

Send Email: Allows the user to enable the camera to send an email when an event is triggered.
Snapshot: Allows a snapshot of the event to be sent via email when triggered.

Record: Allows the event to be recorded to a microSD card after the event is triggered.
Record Time: The amount of time the event will record after it has been triggered.

Schedule

This option allows the user to set a human detection schedule. This will allow the rule to only be triggered at specific dates & times customized by the user. For instance, if you would like a rule to only apply from 6am till 5pm all week, click and drag the applicable area on the interface and click **Apply**.

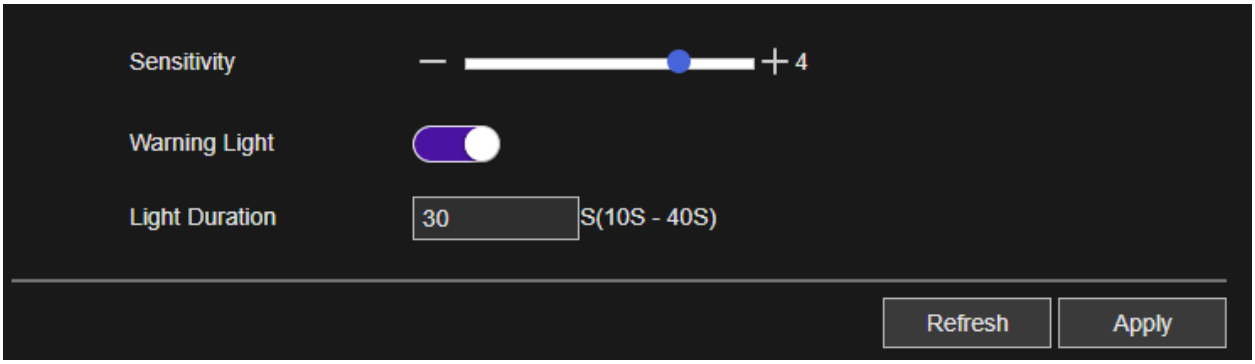


To remove a schedule, click the icon. This can apply to the whole schedule or specific days if needed.

To reset to default settings, click the **Reset Defaults** button. To refresh the page, click the **Refresh** button. To Apply the settings, click the **Apply** button.

IVS Settings

This option allows the user to adjust the sensitivity of set IVS or human detection events as well as set active deterrents (if applicable) such as an onboard warning light and set light duration if needed. Please note, the sensitivity will be set to default (4) however can be adjusted between 1 and 5, 5 being the most sensitive. To activate an active deterrent, enable the Warning Light option and set a light duration for the deterrent.



To refresh the page, click the **Refresh** button. To Apply the settings, click the **Apply** button.

Abnormality

This menu allows the user to adjust abnormality event settings. This menu has 4 tabs: SD Card, Network, or login failures.

SD Card

This tab allows the user to set the camera's response to an SD card related abnormality. Below is an explanation of the fields on the **SD Card** settings tab:

Event Type: This dropdown box allows the user to select which SD card abnormality to set event triggers for. The 3 options are No SD Card and SD Card Error,
Enable: This option enables the SD Card abnormality trigger for the camera.
Send Email: This option allows the user to enable the camera to send an email when an SD Card abnormality is detected.

To reset to default settings, click the **Reset Defaults** button. To refresh the page, click the **Refresh** button. To Apply the settings, click the **Apply** button.

Network

This tab allows the user to set the camera's response to a Network related abnormality. Below is an explanation of the fields on the **Network** settings tab:

Event Type: This dropdown box allows the user to select which Network abnormality to set event triggers for. The 2 options are Disconnected and IP Conflict.
Enable: This option enables the Network abnormality trigger for the camera.
Record: This option allows the user to enable the camera to record video when a network abnormality is detected.
Record Delay: This field specifies in seconds how long the delay between alarm activation and recording should be.

To reset to default settings, click the **Reset Defaults** button. To refresh the page, click the **Refresh** button. To Apply the settings, click the Apply button.

Login Failure

This tab allows the user to set the camera's response to an Illegal Access related abnormality. Below is an explanation of the fields on the **Login Failure** settings tab:

Enable: This option enables the login failure abnormality trigger for the camera.
Login Attempts (3-30): This field allows the user to specify how many failed login attempts must be attempted to trigger a login failure abnormality event.
Send Email: This option allows the user to enable the camera to send an email when a login failure is triggered.

To reset to default settings, click the **Reset Defaults** button. To refresh the page, click the **Refresh** button. To Apply the settings, click the **Apply** button.

Storage

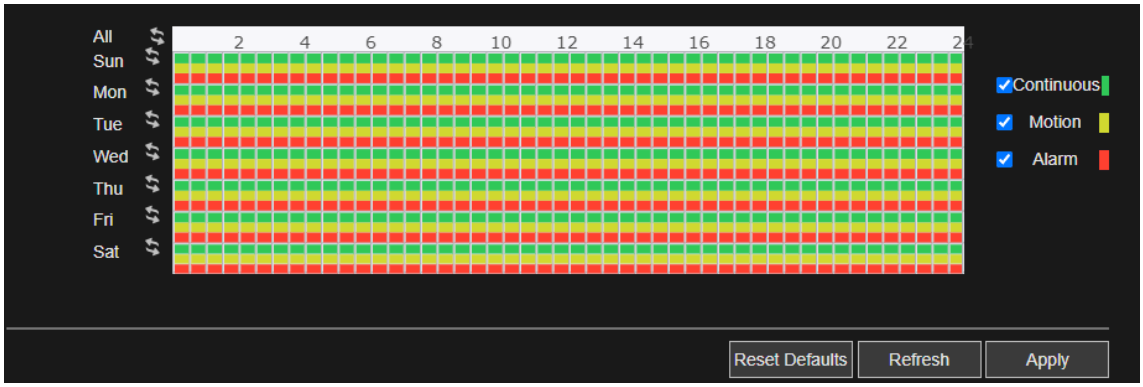
This menu section allows the user to change storage settings for the camera.

Schedule

The schedule menu manages the recording schedule for the camera including all continuous, motion, and alarm schedules.

Record Schedule

This tab is where video recording settings are configured. Below is a screenshot of the Record Schedule menu:



Below is an explanation of the fields on the Record Schedule settings tab:

These options allow the user to select which recording type they want to configure on the schedule. There are 3 types of recordings:

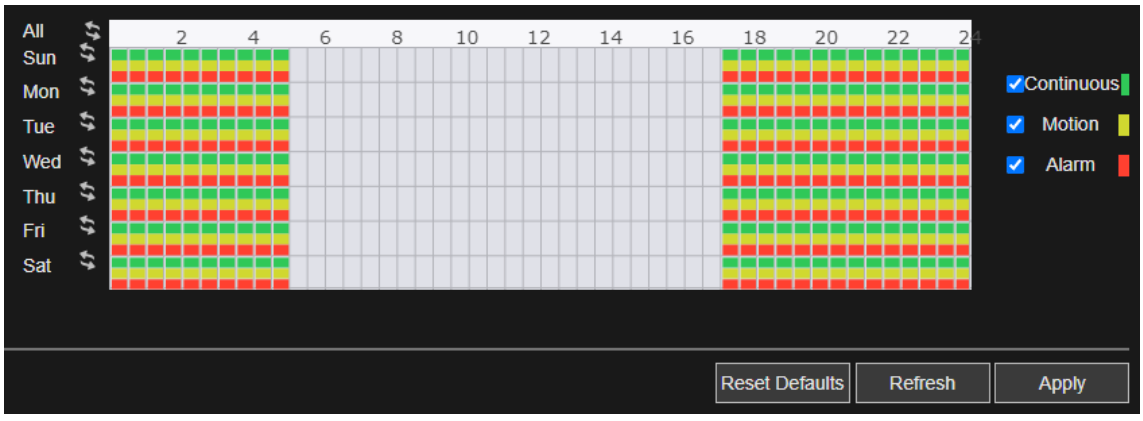
These options allow the user to select which recording type they want to configure on the schedule. There are 3 types of recordings:

Continuous: The camera captures all footage for the specified time period. Continuous snapshot schedules are represented by the color green.

Motion: The camera captures all motion detection events for a specified time period. Motion event schedules are represented by the color yellow.

Alarm: The camera will capture all alarm events. Alarm schedules are represented by the color red.

To adjust a video recording schedule, select a record type then click and drag on the time bar for the desired date. To edit multiple days at once, drag the cursor further up or down to cover the other days. For instance, if you would like a rule to only apply from 6am till 5pm all week, click and drag the applicable area on the interface and click **Apply**.

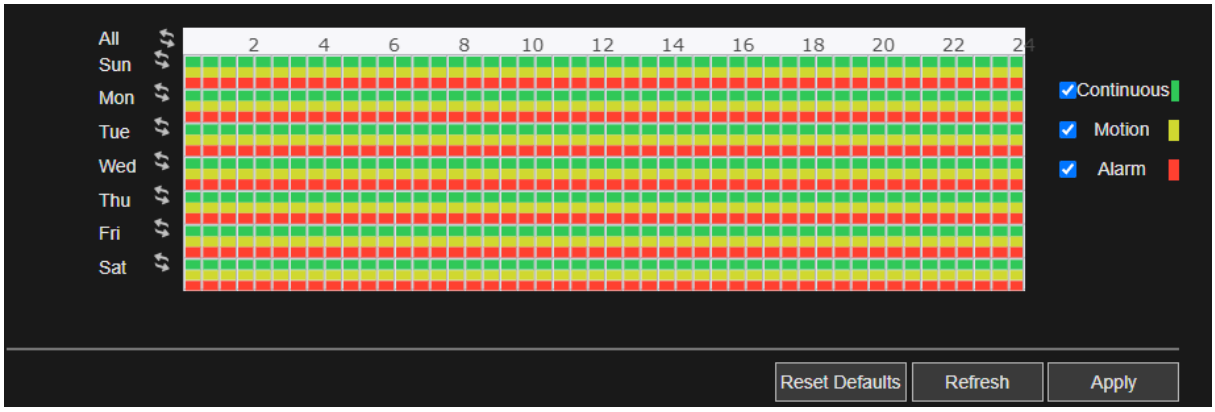


To remove a schedule, click the icon. This can apply to the whole schedule or specific days if needed.

To reset to default settings, click the **Reset Defaults** button. To refresh the page, click the **Refresh** button. To Apply the settings, click the **Apply** button.

Snapshot Schedule

This tab is where snapshot recording settings are configured Below is a screenshot of the Record Schedule menu:



Below is an explanation of the fields on the Snapshot Schedule settings tab:

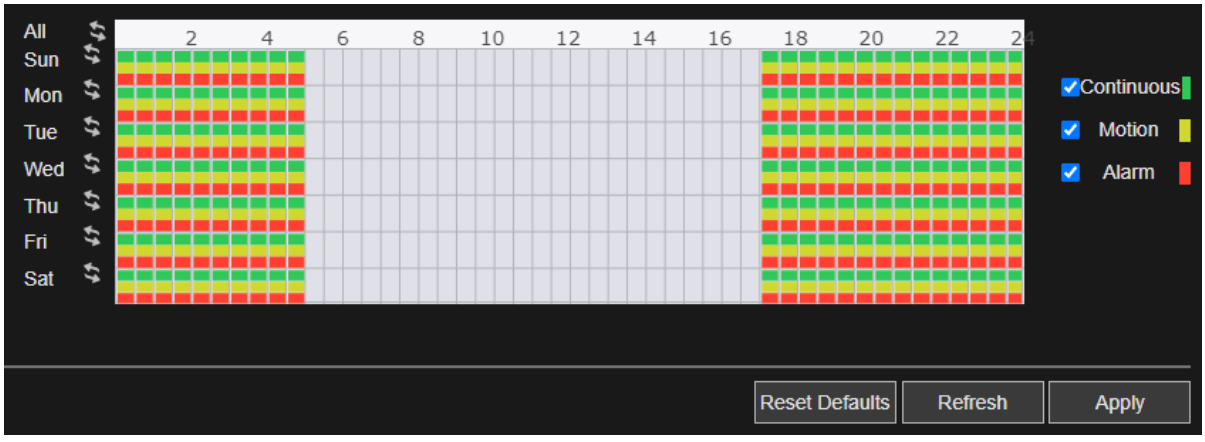
These options allow the user to select which recording type they want to configure on the schedule. There are 3 types of recordings:

Continuous: The camera captures all footage for the specified time period. Continuous snapshot schedules are represented by the color green.

Motion: The camera captures snapshots of all motion detection events for a specified time period. Motion snapshot schedules are represented by the color yellow.

Alarm: The camera will capture snapshots of all alarm events. Alarm snapshot schedules are represented by the color red.

To adjust a snapshot recording schedule, select a record type then click and drag on the time bar for the desired date. To edit multiple days at once, drag the cursor further up or down to cover the other days. For instance, if you would like a rule to only apply from 6am till 5pm all week, click and drag the applicable area on the interface and click **Apply**.



To remove a schedule, click the icon. This can apply to the whole schedule or specific days if needed.

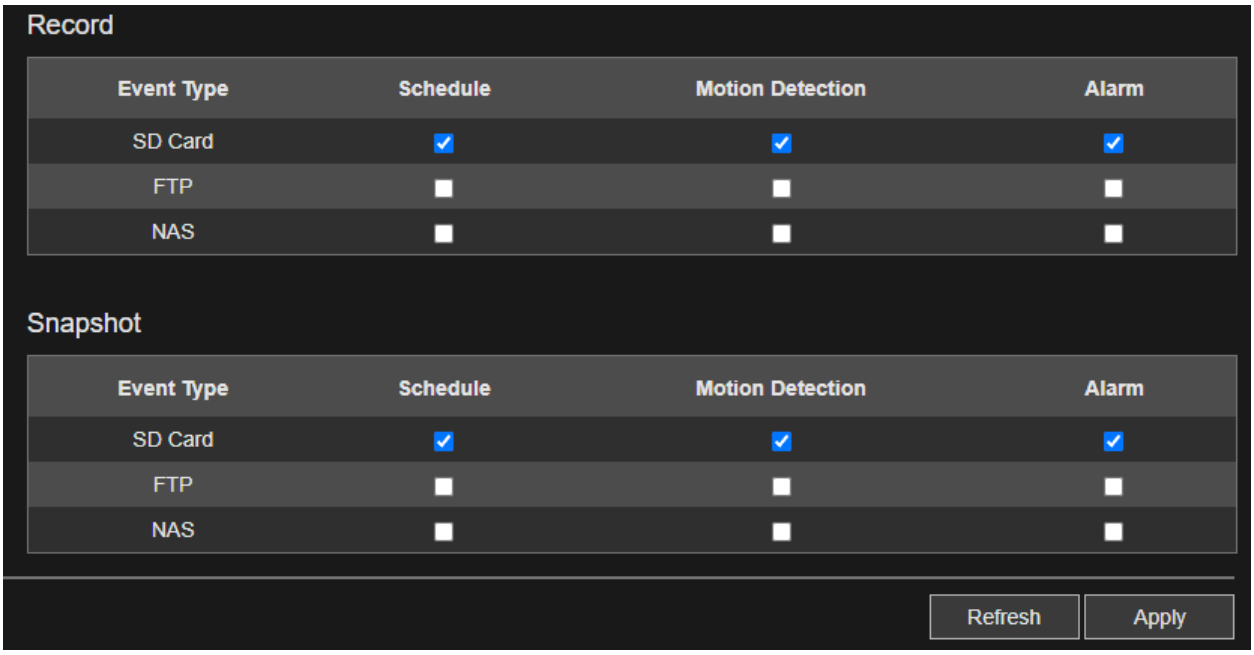
To reset to default settings, click the **Reset Defaults** button. To refresh the page, click the **Refresh** button. To Apply the settings, click the **Apply** button.

Destination

This menu controls where recorded media is stored. There are 4 tabs in this menu: Path, SD Card, FTP, and NAS.

Path

This tab is where the user can designate a path for recorded video and snapshots to reside in. Below is a screenshot of the Path tab:



Below is an explanation of the fields on the **Path** settings tab:

Event Type: This column designates storage options available to the camera. The options are SD Card, FTP, and NAS.
Schedule: This option allows a schedule to be enabled for the record path.
Motion Detect: This option allows motion detection record types to be sent to the record path.
Alarm: This option allows alarm record types to be sent to the record path.

To reset to default settings, click the **Reset Defaults** button. To refresh the page, click the **Refresh** button. To Apply the settings, click the **Apply** button.

SD Card

This tab is where the user can change SD card settings. Below is an explanation of the fields on the SD Card settings tab:

SD Card Status: Specifies if a format is needed or the current status of the microSD card.
SD Card SN Code: Displays the serial number details of the microSD card (if applicable).
SD Card Capacity: This column shows the available memory on the microSD card.
Used Space: The amount of storage used on the microSD card.
Picture Capacity: The amount of storage designated for snapshots.
Picture Used Space: The amount of storage used for snapshots on the microSD card.
Format: This button formats the microSD card.

FTP

This tab allows the user to set events to be stored onto an SFTP or FTP server. By default, this option will be set using an SFTP protocol as it is the most secure method, however, an FTP server address can be set as well. Please note, if saving events to an FTP, please make sure the FTP option is enabled in the Path tab before proceeding. Below is an explanation of the fields provided in this menu.

Enable: Enable an SFTP, FTPS, or FTP protocol.
Server Address: Enter the IP address of the SFTP, FTPS, or FTP server.
Port: Enter the port number of the SFTP, FTPS, or FTP server. SFTP port will be 22, FTP or FTPS ports will be 21.
Username: Enter the username of the SFTP, FTPS, or FTP server.
Password: Enter the password associated with the SFTP, FTPS, or FTP server.
Path Enter the directory information for the SFTP, FTPS, or FTP folder.
Test: Test the connection between the camera and the SFTP, FTPS, or FTP server.

To refresh the page, click the **Refresh** button. To Apply the settings, click the **Apply** button.

NAS

This tab is where the user can change NAS settings. Before proceeding, please make sure the NAS option is selected in the Path menu. Below is an explanation of the fields on the NAS settings tab:

Enable: Enable the NAS protocol.
Server Address: Enter the server address of the NAS.
Record Directory: Enter the directory information in which the events will be stored.
Protocol: Select a NAS protocol (NFS or CIFS) used to store the events to the NAS.

To reset to default settings, click the **Reset Defaults** button. To refresh the page, click the **Refresh** button. To Apply the settings, click the **Apply** button.

Record Control

This menu is where general recording settings are configured.

StreamID: Choose between mainstream or substream feed details.
Max Limit (48-512M): Displays the maximum amount of MBs per recording.
Audio: Enable or disable audio in video recordings.
Recording Overwrite: Enable or disable the ability to overwrite old recordings if the storage device is full.

To refresh the page, click the **Refresh** button. To Apply the settings, click the **Apply** button.

Cloud Storage

This menu redirects the user to the Amcrest Cloud web site. At this website (amcrestcloud.com) users can register for new accounts as well as view or modify existing accounts.

System

This menu section allows the user to change general settings for the camera.

General

This tab is where the user can configure some basic camera settings. Below is an explanation of the fields on the **General** settings tab:

Device Name: Displays the serial number associated with the device.
Video Standard: This dropdown box allows the user to select either the NTSC or PAL video standard.
Video refresh frequency: Displays the current I-frame interval related to video compression.

To refresh the page, click the **Refresh** button. To Apply the settings, click the **Apply** button.

Date & Time

This tab is where the user can configure the date and time settings for the camera. Below is an explanation of the fields on the Date & Time settings tab:

Time Zone: This dropdown box allows the user to change the time zone used in the camera.
Date & Time: This field allows the user to enter the date and time manually. Clicking the PC Sync button allows the camera to sync with the computer's date & time.
Date Format: Displays the format in which the date will be displayed in the interface.
Time Format: Displays the format in which the time will be displayed in the interface.
NTP Server: This option allows the user to enable the camera's synchronization with an NTP server.
- **NTP Server**: This field allows the user to enter an NTP server.
- **NTP Port**: This field allows the user to enter the port number for the NTP server.

Frequency of Checks. Minimum 10s: This field allows the user to enter in the update period time. This number designates how frequently the camera pings the NTP server to ensure it has the correct time.
DST: This option allows the user to enable daylight savings time for the camera.
- **Start Time**: These dropdown boxes and fields allow the user to enter in the start time for DST.
- **End Time**: These dropdown boxes and fields allow the user to enter in the end time for DST.
- **Offset Time:** This dropdown menu allows you to specify how long of an offset the DST settings will take.

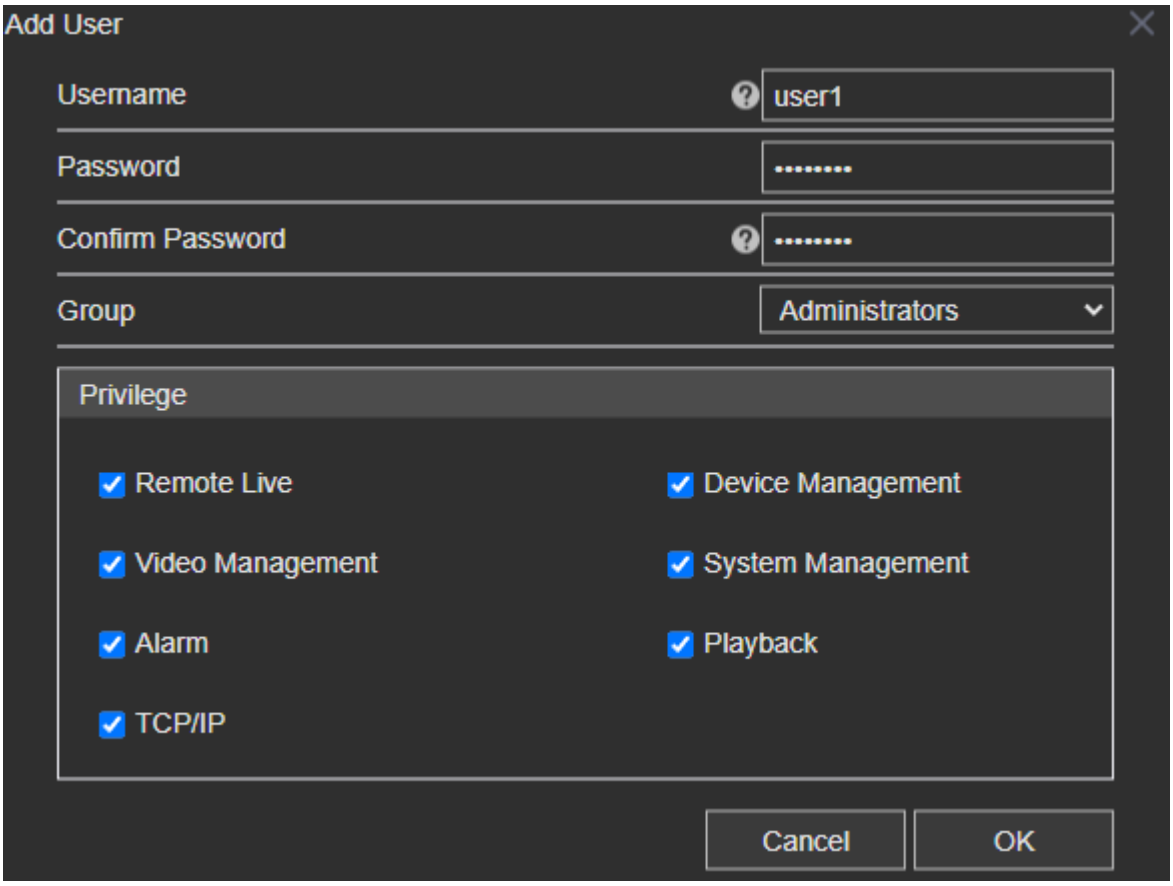
To refresh the page, click the **Refresh** button. To Apply the settings, click the **Apply** button.

Manage Users

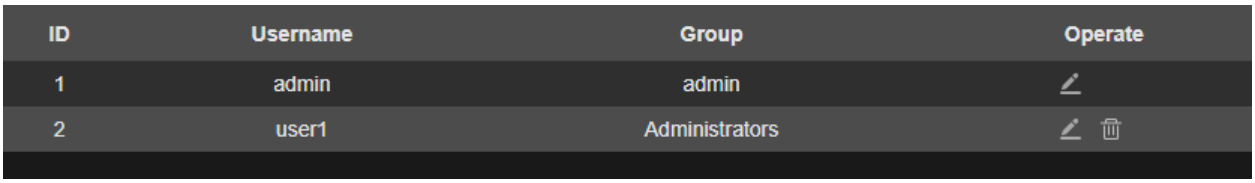
This menu allows the user to change the user accounts on the camera. By default, the camera only has the admin account which has all rights/authorities. Additional accounts can be created on this screen.

ID: The number of accounts applied to the device.
Username: Displays the username associated with the user.
Group: Displays which group the user is associated with (administrator, operator, or media user).

Operate: Allows the user to edit user details.
Add: Add new users to the camera. This is the menu you can add new users, set user groups, as well as assign specific privileges for new users.



To delete a user, click on the trashcan icon next to the user's name and remove.

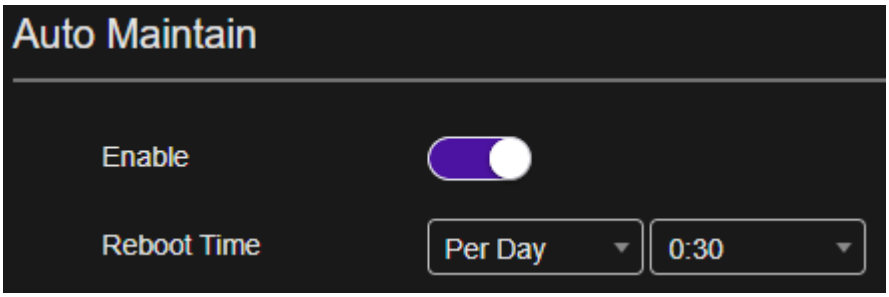


Reboot/Reset

This screen allows the user to reset the camera and all its settings to the factory settings. Below is an explanation of the items listed in this field:

Reboot: Click this option to reboot the camera. Please note, this will not set the camera to factory default, it will only reboot the camera.
Reset: Click this option to restore camera defaults or set the camera back to factory default. Please note, restoring camera defaults will not set the camera back to factory default settings. It will simply set all features to default, the username and password for the device will remain the same. Select the factory default option and click OK to reset the camera back to factory default settings.

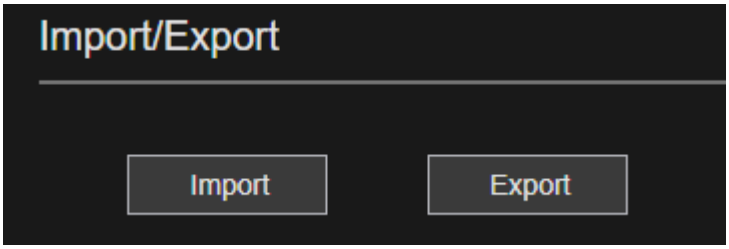
Auto Maintain: This option will allow the camera to automatically reboot at specified times. Click the enable button to enable the feature and select a reboot time if needed.



To refresh the page, click the **Refresh** button. To apply the settings, click the **Apply** button.

Import/Export

This screen allows the user to import or export settings from the camera. To export the settings, click the Export button. The settings file will be downloaded to your device. Click the **Import** button, select the exported file and import the settings back into the camera.



Firmware

This menu allows the user to upgrade the camera's firmware.

Update: Click this option to import the downloaded firmware file into the interface. The device will begin upgrading once it is applied. Please note, when upgrading do not close the browser or turn off the camera. The camera will automatically reset once the update is complete. The latest firmware version will be displayed in the interface.
Get Latest: Click this option to automatically be sent to the firmware downloads page.

Information

This menu section allows the user to view information about the camera for reference purposes.

Information

This screen allows the user to see various information about the camera, software versions, as well as other details related to the camera such as the serial number (S/N), device name, type, model, firmware version, etc.

Log

This screen is where the camera's activity log is kept. To view logs for a specific time period, modify the start time and end time fields, choose the type of event (system, setting, data, event, record, manage users, clear log), and click search.

To back up the log, click the Backup button. To clear the log, click the **Clear** button.

Online Users

This screen allows the user to see which users are online. Click **Refresh** to refresh this table.

Logout

Clicking the logout button will log you out of the interface and return you to the main login page.

Remote Web Access Setup

There are two main methods for setting up remote access: UPnP/DDNS, and Port Forwarding.

UPnP/DDNS Remote Web Access Setup

Using Universal Plug and Play (UPnP) and Dynamic Domain Name Server (DDNS) functionality is the easiest way to setup stable remote access. For this method, your router should support the uPnP networking protocol and the protocol should be enabled. Please refer to your router manufacturer's documentation to learn how to enable uPnP on your router.

Below is a step-by-step walkthrough that details how to set up a Helix camera for Remote Web Access using UPnP and DDNS:

1. Login to your camera's web interface, open the main menu then go to Setup -> Network.
2. Using the left-hand menu, go to the Connection menu, and write down the HTTP port. It is recommended to ensure the port number is at least 5 digits long to prevent any port conflicts. If need be, change the port to a 5digit number that is less than 65535, note the number down, and click Apply before proceeding to the next step.
3. The system will prompt you to reset the camera. Click OK and wait for the camera to restart.
4. Restarting the camera may cause the device to use another IP address. Use the included IP Config tool to find the IP address as detailed previously in this document.
5. Login to your camera, open the main menu then go to Setup -> Network.
6. Click the Connections menu item on the left-hand menu and ensure that the HTTP port has changed.
7. Click the DDNS menu item on the left-hand menu, select HelixDDNS from the drop-down box, click the option next to Server Type, and then click the Apply button on the bottom right.
8. To set a custom DDNS name, fill out the Domain Name field and click Apply.
9. Write down the entire Domain Name field, including the white text that says HelixDDNS.com
10. Click the UPnP menu item on the left-hand menu and click the enable option at the top.
11. While in the UPnP menu, double click the HTTP port, and change both the internal and external HTTP ports to match the number that was used in step 2.
12. Uncheck the last 4 options in the PAT table on the UPnP menu.
13. Click apply, then exit this menu to go back to the main menu, then re-enter the UPnP menu, and ensure the UPnP status says, "Mapping Successful".
14. Open a web browser and enter in the DDNS domain name address from step 9, enter in a colon, then type the port number from step 4 on to the end.

a. For example, if the DDNS domain name is http://abc123456789.helixDDNS.com and your HTTP Port is 33333, the URL would be http://abc123456789.helixDDNS.com:33333

15. The browser may prompt you to install a plugin. Click install to download the plugin, and then click on the plugin installation file to install the plugin.
16. If the browser prompts you to allow the plugin to work on the computer, hit Allow to ensure the plugin can run successfully.
17. Enter in login details into the username and password fields and click login.

Port Forwarding Remote Web Access Setup

Port Forwarding is an alternative method to setting up remote access for Helix cameras. This method should only be used if the UPnP/DDNS Remote Access method did not work.

Below is a step-by-step walkthrough that details how to setup the camera for Remote Web Access using Port Forwarding:

1. Login to your camera, open the main menu then go to Settings -> Network.
2. Open the TCP/IP settings screen.
3. By default, the camera has the mode set to DHCP. Ensure that DHCP is selected. The IP Address, Subnet Mask, Default Gateway, Preferred DNS, and Alternate DNS should all be 0s if DHCP is selected.
4. Click Apply to Apply these settings. This should now open the main menu.
5. From the main menu, go to **Settings -> Network**.
6. On the TCP/IP settings screen, the IP Address, Subnet Mask, Default Gateway, Preferred DNS, and Alternate DNS should all be populated.
7. Click the radio button next to Static, to change the mode to Static.
8. Write down the IP Address that is currently in the IP address field.
9. Click the **Apply** button.
10. Using the left-hand menu, go to the Connection menu, and write down the TCP, UDP, and HTTP port number. It is recommended to ensure that these port numbers are at least 5 digits long to prevent any port conflicts. If need be, change each of these port numbers to a 5-digit number that is less than 65535, note the numbers down, and click Apply before proceeding to the next step.
11. Go to http://www.canyouseeme.org/ and check to ensure each of the port numbers specified in step 10 is open.
12. Write down the manufacturer name, brand, and model name for the router that the camera is connected to, and then proceed to http://www.portforward.com on your web browser.
13. Open the port forwarding guide section on the left-hand side menu.
14. Find the router brand name in the list and click it.
15. Find the router model number and click it.
16. Click the Default Guide link near the middle of the page.
17. This guide will help you take the step necessary to port forward on the router. Follow these steps, and then return to the camera.
18. Login to your camera, open the main menu then go to Setup -> Network.
19. Click the DDNS menu item on the left-hand menu, pick helixDDNS from the drop-down box, click the option next to Server Type, and then click the Apply button on the bottom right.
20. To set a custom DDNS name, fill out the Domain Name field and click Apply.
21. Write down the entire Domain Name field, including the white text that says helixtDDNS.com
22. Open a web browser and enter in the DDNS domain name address from step 21, enter in a colon, then type the HTTP port number from step 10 on to the end.
    For example, if the DDNS domain name is http://abc123456789.helixDDNS.com and your HTTP Port is 33333, the URL would be http://abc123456789.helixDDNS.com:33333
23. Enter in login details into the username and password fields and click login.

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.

Appendix A: Toxic or Hazardous Materials or Elements

Component Name	**Toxic or Hazardous Materials or Elements**					
	Pb	**Hg**	**Cd**	**Cr VI**	**PBB**	**PBDE**
Sheet Metal	O	O	O	O	O	O
Plastic Parts	O	O	O	O	O	O
Circuit Board	O	O	O	O	O	O
Fastener	O	O	O	O	O	O
Wire and Cable/Ac Adapter	O	O	O	O	O	O
Packing Material	O	O	O	O	O	O
Accessories	O	O	O	O	O	O

O: Indicates that the concentration of the hazardous substance in all homogeneous materials in the parts is below the relevant threshold of the SJ/T11363-2006 standard.

X: Indicates that the concentration of the hazardous substance of at least one of all homogeneous materials in the parts is above the relevant threshold of the SJ/T11363-2006 standard. During the environmental-friendly use period (EFUP) period, the toxic or hazardous substance or elements contained in products will not leak or mutate so that the use of these (substances or elements) will not result in any severe environmental pollution, any bodily injury or damage to any assets. The consumer is not authorized to process such kind of substances or elements, please return to the corresponding local authorities to process according to your local government statutes.

O: Indicates that the concentration of the hazardous substance in all homogeneous materials in the parts is below the relevant threshold of the SJ/T11363-2006 standard.
X: Indicates that the concentration of the hazardous substance of at least one of all homogeneous materials in the parts is above the relevant threshold of the SJ/T11363-2006 standard. During the environmental-friendly use period (EFUP) period, the toxic or hazardous substance or elements contained in products will not leak or mutate so that the use of these (substances or elements) will not result in any severe environmental pollution, any bodily injury or damage to any assets. The consumer is not authorized to process such kind of substances or elements, please return to the corresponding local authorities to process according to your local government statutes.

Note:
This user manual 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.