IP8M-DT3949EW-3AI-V2
8MP Dual Illumination Active Deterrence Fixed-focal Turret Camera
User Manual

Version 1.0.0
July 17th, 2023

Contents

Installation Guide 4
Initialization 4
Web User Interface 6
Main Menu 8
Playback 8
AI 14
Alarm 24
Maintain 30
Settings 39
Amcrest View Pro 40
Storage 46
Log 48

Welcome

Thank you for purchasing an Amcrest camera!

Here you can find information about your camera's features and functions and information to aid in troubleshooting. For access to the quick start guide and other support information, go to http://amcrest.com/support

To contact Amcrest support, visit http://amcrest.com/contact and use the email form.

Call Amcrest Support using one of the following numbers:
Toll Free: (888) 212-7538
International Callers (Outside of US): +1-713-893-8956
USA: +1-713-893-8956
Canada: 437-888-0177
UK: 203-769-2757

Important Security Warning

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



- Always make sure that your camera has the latest firmware as listed on www.amcrest.com/firmware
- 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, and numbers.

Overview

This 8MP dual illumination camera delivers stunning ultra-high-definition video in 8-megapixel resolution, at 30 frames per second. It features dual AI sensors with multi-spectral imaging technology that produces colorful images in low light conditions. The 2.8mm angled lenes provide a full 125° 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 human and vehicles in the area. The camera also has built-in red/blue flashing warning lights which can act as a deterrent once an object is detected as well as a built-in siren. 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. All these features can be accessed and customized using a web browser or even using the Amcrest View Pro app using a mobile device.

Installation Guide

Follow the steps and use the diagram in this section to install the POE cameras.

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. Locate the **Reset** cover on the top of the camera. This area will provide access to the factory reset button as well as the microSD card slot.

2. Remove the cover. If you are having trouble removing the cover, use the provided torx wrench to remove the camera's dome enclosure.

3. Locate the microSD card slot, and with the gold pins forward towards the lens, insert the microSD card into the slot.

4. Gently press in until you hear a click. This click indicates the microSD card has been properly secured.

5. Place the cover back onto the camera and secure it to the camera. If you have removed the dome enclosure, please put the enclosure back onto the camera and secure it tightly with the torx wrench.

Physical Installation

Note: Prior to installation ensure that the installation environment can support at least 3 times the weight of the camera.

1.Place the installation sticker onto the mounting surface.
2.Drill bottom holes according to the installation position map and insert the included wall anchors into the holes. If running wires through a wall/ceiling a 1" paddle bit can be used to drill the center portion of the sticker.
3.Use the included torx wrench to remove the security screw on the front of the casing. This will disassemble the camera from its case.
4.Align the holes on the bottom installation bracket to the wall anchors on your mounting surface. Run the wiring through the newly drilled hole or on the side of the camera keeping the camera and mounting bracket level with the mounting surface.
5.Use a Phillips head screwdriver (not included) to secure the bottom bracket and camera to the mounting surface.
6.Place the top portion of the casing over the camera and installation bracket and use the included torx wrench to tighten the security screw back onto the casing. Do not overtighten the security screw as it may not properly be secured if overtightened.

Initialization

This camera features the latest JS technology which allows the camera to be accessed both locally and remotely in most main web browsers. The camera can also be accessed on your mobile device using the Amcrest View Pro app, Amcrest Cloud, Blue Iris, etc.

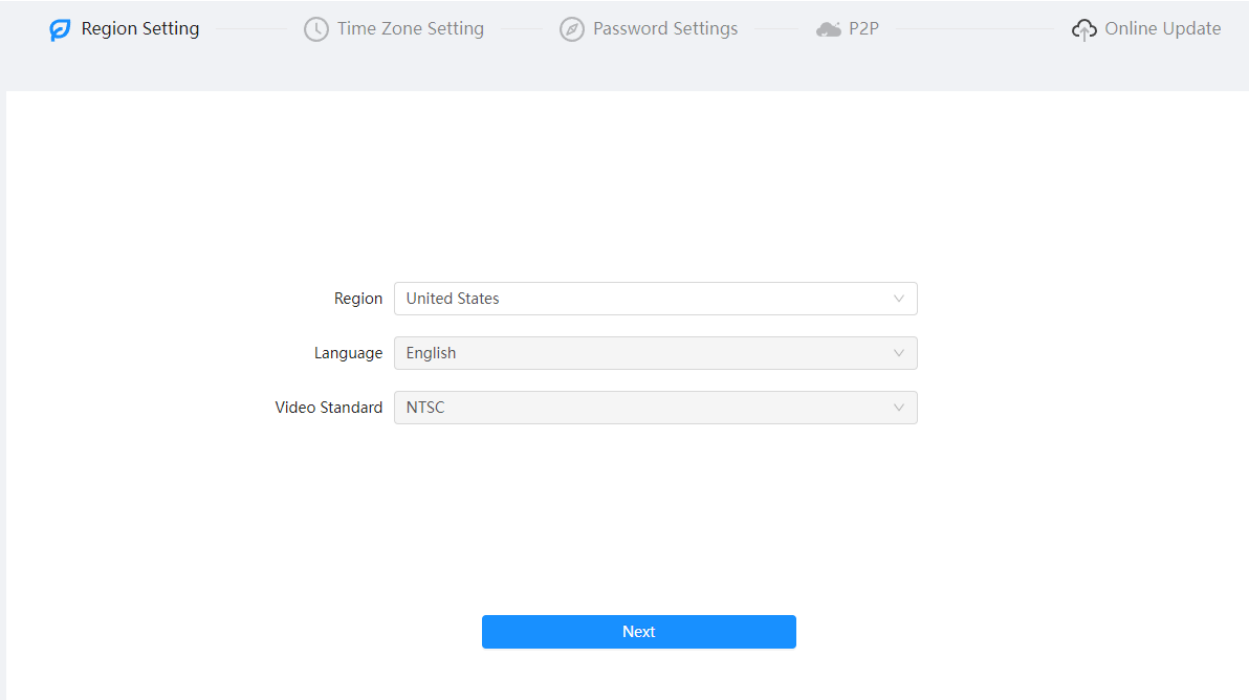
Web User Interface Access

The camera can be accessed in most mainstream web browsers including Chrome, Firefox, Edge, etc. using the camera's IP address. Please note, some features may require a .exe plugin and will not be compatible on Mac browsers. To locate the camera's IP address, it is highly recommended to download our free Amcrest IP Config Tool software. The Amcrest IP Config Tool can be downloaded at the following web page: amcrest.com/downloads

In the **All-Downloads** menu, click on **IP Config Software** to begin the free download. Once the download has completed installing, locate the IP address associated with the device you would like to view in the browser. Open the web browser and enter this IP address into browser. Press Enter to access the web user interface.

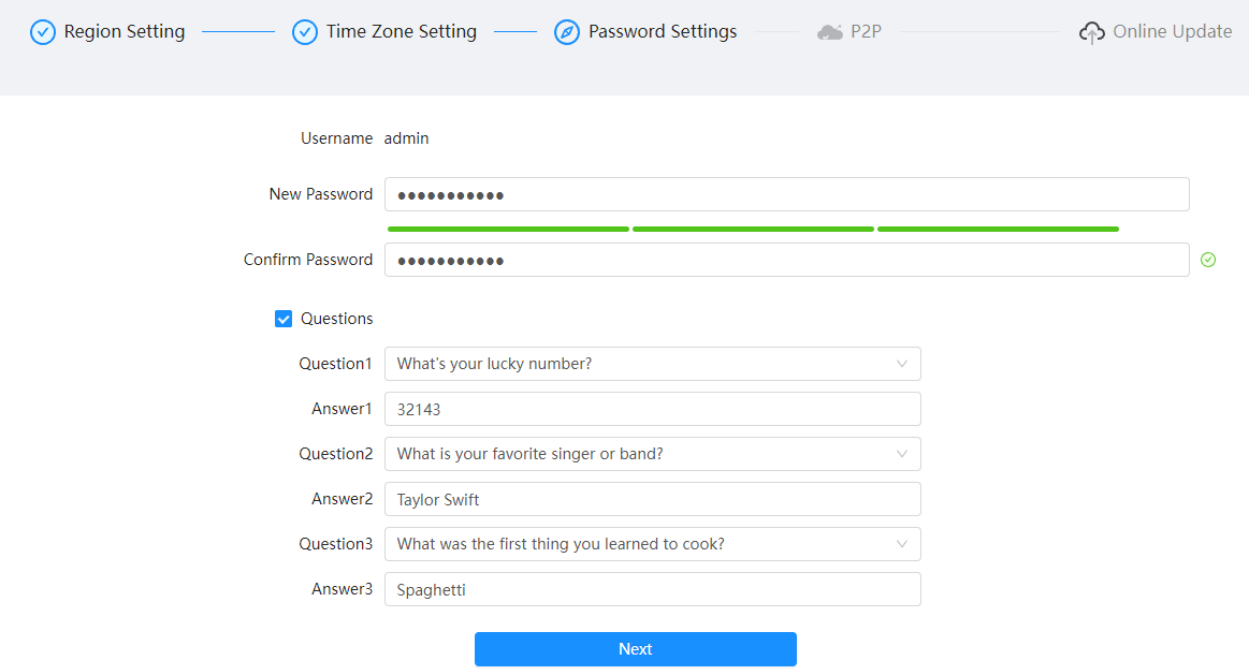
Device Initialization

After accessing the camera in a web UI, the device will need to be initialized. Verify your region settings on the interface, click **Next** to continue.



Verify the time zone settings. To sync the time & date to your computer's date & time settings, click Sync to PC. Click **Next** to continue.

Create a new admin password for your camera. This will be the password to access the device. The password should be between 8 and 32 characters with a combination of letters, numbers, and symbols are recommended when setting up your password. A list of security questions will be provided as well, these questions can be used in the future as a reference to reset your password if it has misplaced or forgotten. Click **Next** to continue.



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

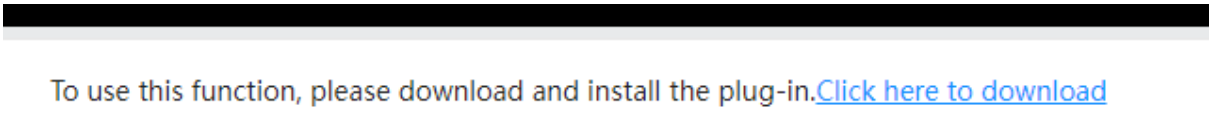
The P2P option will be enabled by default. This option allows you to connect your camera to your mobile device using the Amcrest View Pro app which is available in the App Store or Google Play store or by scanning the "Cell Phone Client" QR Code provided. Use the **Device SN** QR code for quick access to the serial number of your camera. Please note, **before adding your camera P2P into the view pro app to finish device initialization.**

For more information on how to add your camera to the Amcrest View Pro app, please refer to the "Amcrest View Pro" section provided below. Click Next to continue. The camera will be set automatically to automatically check for updates, you can enable or disable this option in the online update menu. When finished, click **Finish** to complete the initialization of your camera.

Web User Interface

After the device has been initialized you can now access the camera in the web browser. The camera can be accessed in most mainstream web browsers such as Chrome, Firefox, etc. However as previously described, some features may require a .exe plugin and are not compatible on Mac browsers. Enter the username and password for your camera and click **Login.**

To install the plugin, select "**Click here to download**" and download the .exe plugin to your computer. Install the plugin and allow the browser to refresh. If you do not want to install the plugin, click "**Close**".

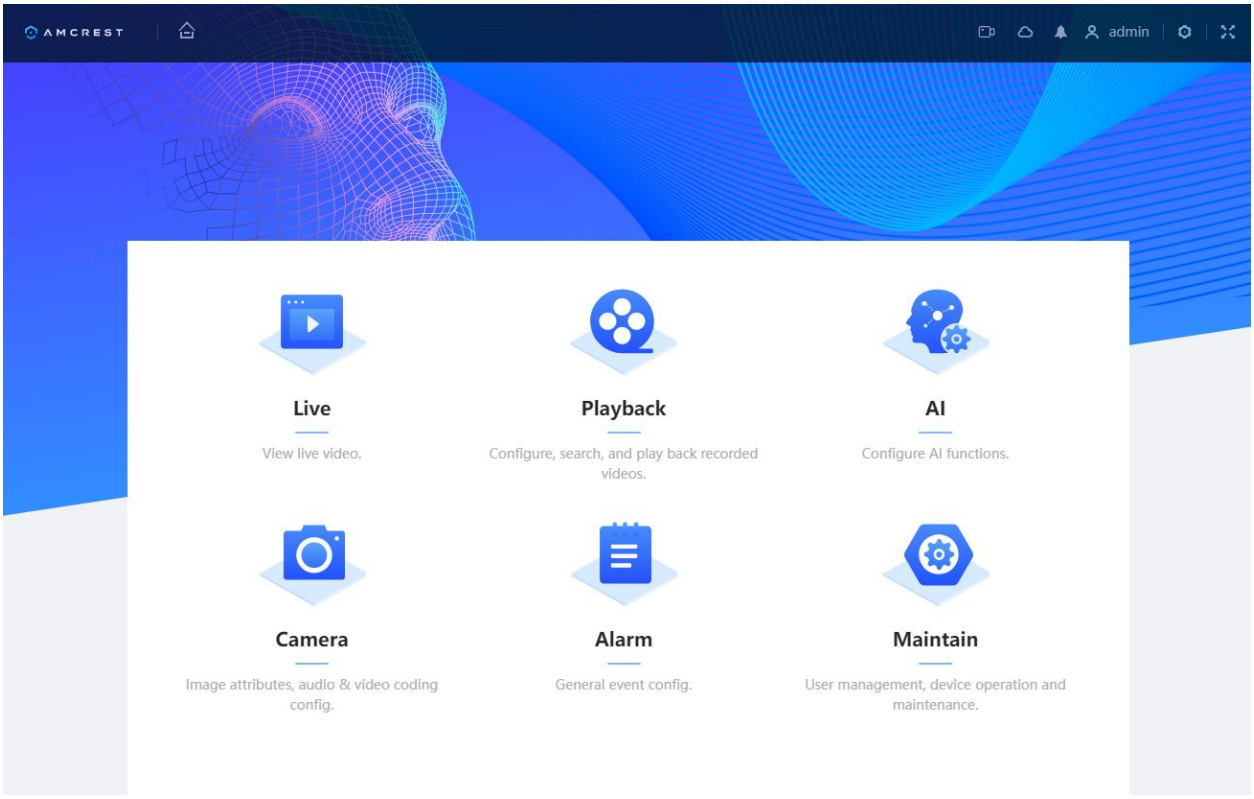


Live

The live menu allows you to access the panoramic view and features associated with your camera. For more information on the features provided in the live view menu, please refer to the table provided below.

Feature	Description
Video Stream	Provides access to the view of the mainstream and sub streams of the camera.
Image Adjustment	Adjust the brightness, contrast, saturation, and hue of the feed. Press the Reset button to return these to default. Default values are typically around 64.
	Adapt/Original Size. Switch between displaying the original size of the stream in its set resolution or adapting to the size of the monitor display the feed is being viewed on.
	W:H. Adjust the width and height of the live view feed between its original size or adaptive size, which removes the gray borders.
	Smoothness Adjustment. Adjust the fluency allows the camera to compensate for any network discrepancies to increase fluency of the stream.
	AI Rule. Enable or disable the AI rule overlays on the live view screen.
	Intelligence Area. Enable or disable intelligence overlays on the live view screen.
	Auxiliary Installation: Allows you to use an Amcrest camera as an auxiliary input for an Amcrest NVR. This means that you can use the camera to view live video, playback recorded video, and receive alarm notifications from other cameras that are connected to the same NVR.
	Warning Light: Allows the user to manually flash the red/blue warning LEDs.
	Siren: Allows the user to manually enable the onboard siren.
	Force Alarm1. Enable or disable an alarm being sent to an external alarm.
	Digital Zoom. Features 16x zoom. To use digital zoom, select the digital zoom icon, select an area on the live view screen you would like to view and release. (Requires Plugin)
	Snapshot. Click this button to take a manual snapshot of the live view screen.
	Triple Snapshot. Click this button to take 3 simultaneous manual snapshots of the live view screen.
	Record Control. Click this button to manually record a video of the live view screen. Click the button again to stop recording.
	Sound. Click this button to enable or disable audio output from the camera. This is only applicable if using an external RCA speaker on the audio out port found on the dongle wire connection.
	Talk. Click this button to activate the talk feature on the camera. This is only applicable if using an external RCA microphone on the audio in port found on the dongle wire connection.
	Full Screen: Sets the live feed into full screen mode.

Main Menu



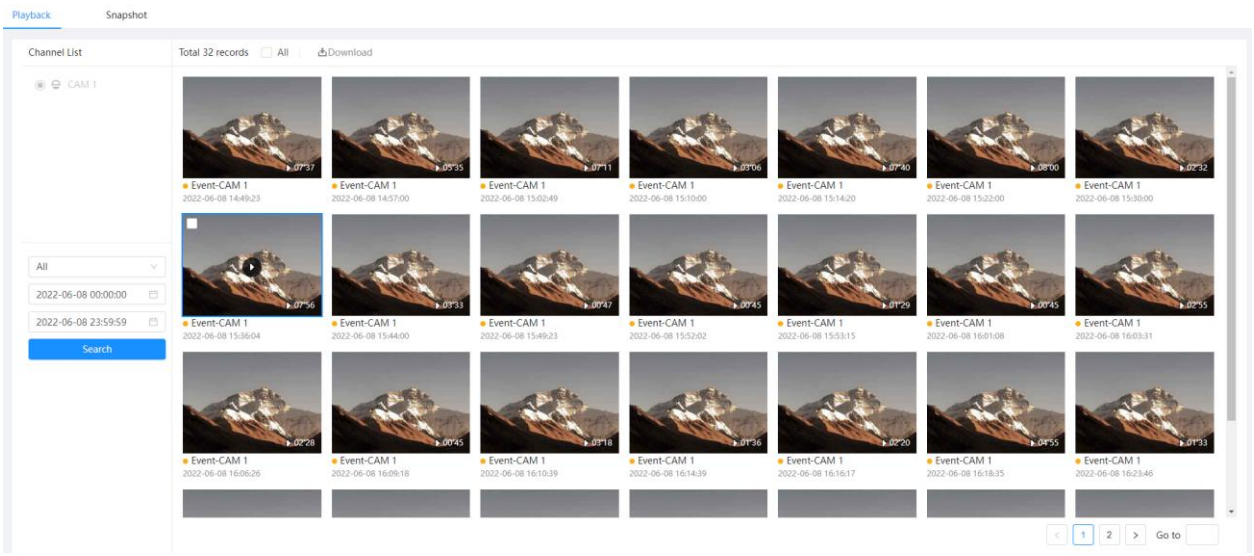
The main menu allows for quick access to the features and interfaces associated with your camera. For more information on the main menu options, please refer to the information provided below.

Top Banner

	Home. Return to the main menu from any selected tab or interface.
	Live. Return to the live view screen from any selected tab or interface.
	Cloud. Automatically directs the user to https://amcrestcloud.com
	Alarm. View or clean queued or already executed alarm types.
	Admin. Click to restart the camera or log out of the current user account.
	Setting. View Path, Network, Storage, and Log interfaces.
	Full Screen. Click to set the interface to full screen. Press Esc to return to original format.

Playback

The Playback menu allows the user to playback and download recorded video and snapshots that have been saved to a microSD card. Press the Search button to load recordings or snapshots based on a specified date and time.



Viewing a Recording

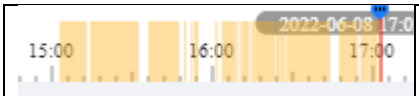
To view a recording, click on the “All” dropdown menu and select which record type you would like to view. There are several event record types that can be selected including a general record type, which will display all continuous recording events, an Event record type which will display all motion detection and other motion activated recordings, as well as an alarm (external alarm) and manual record types.

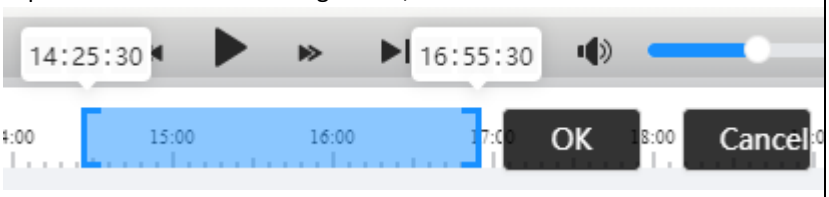
Select a record type from this menu and click on the start time option. A calendar will appear, choose the start date of the recording you would like to view then click “Select time”. The default start time will be set to 00:00:00, which is midnight, use the scroll-down options to select the exact hour, minute, and even seconds of the start of the event. In this example, we are using 15:05:02, which is 3:05 pm. Click **Ok** to set the start time.

Next, click on the end time option. A calendar will appear, choose the end date of the recording you would like to view and click “select time”. The default end time will be set to 23:59:59 which is roughly 1 second before midnight. Use the scroll down options to select the exact hour, minute, and even seconds for the end of the event. In this example, we are using 17:03 which is 5:03pm. Click **Ok** to set the end time.

Click **Search**. The interface will display the total number of events within the specified time frame.

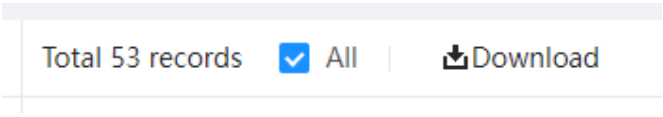
To view the event, hover your mouse over the selected event and click the play button. The list of events will be displayed in the left panel and the selected recording will start to play. For more information on the options provided in the playback menu, please refer to the information provided below.

	Timeline. Use the timeline to scroll through specific events in a designated time frame.
	Digital Zoom. While the event is playing, click on the digital zoom option to zoom in on a specific area of the recording.
	AI Rule. Use this option to enable or disable AI overlays in the recording.
	Intelligence Rule. Display intelligence rule overlays in the recording.

	Previous. Click to return to a previous recording found in the file list.
	Rewind. Use the rewind option while the recording is playing to rewind either in a 2x, 4x, 8x or 16x.
	Play/Pause. Use these options to start or pause the recording.
	Fast Forward. Use the fast forward option while the recording is playing to fast forward in 2x, 4x, 8x, or 16x.
	Next. Click to move to the next recording in the file list.
	Next Frame. Use this option when the recording is playing to scrub through the recording frame by frame.
	Triple Snapshot. Click this button to take a triple snapshot while the recording is playing.
	Snapshot. Click this button to take a snapshot while the recording is playing.
	Video Clip. User your mouse to set a range in the timeline in which a video clip can be saved. Once a range is set, click **OK**.  Select a download format, preferably .mp4, as well as a storage path for the clip. Click **Start Download** to download the clip to your computer.
	Full Screen. Click this button while the recording is playing to view it in full screen mode.

Download a Recording

Events can be downloaded directly from the playback menu to your computer. **Downloading a recording will require the use of a plugin**, please make sure it is installed on your computer before proceeding. The interface allows you to download a single event or multiple events if needed, if you would like to download all events, click on the "All" option located next to the total records field.



To download a recording, select an event ensuring it has a blue checkmark. After selecting the event, click the **Download** button to launch the download interface. The download interface will display the total number of events being downloaded, the event type, the start & end times, the duration of the event as well as the total size (MB) of the event. Click on **Browse** to select a download path and click **Start Download** to download the selected event or events to your computer.

Snapshot

The snapshot tab allows you to search and view snapshots of events, adjust the quality of the snapshot, set snapshot schedules, and set storage paths for snapshots.

Search Snapshots

This is the default menu and allows you to search and view snapshots that have been retained on a microSD card. Similar to viewing recordings, the record types can be located using a start and end date & time and downloaded to your computer.

To view a snapshot, click on the "All" dropdown menu and select which event type you would like to view. There are several event types that can be selected including a general event type, an event type that will display all motion detection snapshots, and other motion-activated event types, such as alarm (external alarm) and manual record types.

Select an event type from this menu and click on the start time option. A calendar will appear, choose a start date of the recording you would like to view then click "Select time". The default start time will be set to 00:00:00, which is midnight, use the scroll-down options to select the exact hour, minute, and even seconds of the start of the event. In this example, we are using 15:05:02, which is 3:05 pm. Click **Ok** to set the start time.

Next, click on the end time option. A calendar will appear, choose the end date of the event you would like to view and click "select time". The default end time will be set to 23:59:59 which is roughly 1 second before midnight. Use the scroll down options to select the exact hour, minute, and even seconds for the end of the event. In this example, we are using 17:03 which is 5:03pm. Click **Ok** to set the end time.

Click **Search**. The interface will display the total number of events within the specified time frame.

To view the snapshot, hover your mouse over the selected event and click the play button. The list of snapshots will be displayed in the left panel and the selected snapshot will be displayed in the interface. If you would like a slide show of each snapshot in the left panel played, click the Slide Show icon () at the bottom of the interface.

Downloading a Snapshot

Snapshots can be downloaded directly from the snapshot interface to your computer. The snapshots will be saved in jpg format. The interface allows you to download a single or multiple snapshots if needed, if you would like to download all the snapshots, click on the "All" option located next to the total records field.

To download a snapshot, select an event ensuring it has a blue checkmark next to the event. After selecting the event, click the **Download** button to launch the download interface.

The download interface will display the total number of snapshots being downloaded, the format type, the start time of the event, as well as the total size (MB) of the snapshot. Click on **Browse** to select a download path for the snapshots and click **Start Download** to download them to your computer.

Snapshot

This tab provides additional details pertaining to snapshots including the size, quality, and interface in which the snapshots will be retained. For a brief description of the features in this menu, please refer to the table below.

Type	Scheduled: Set settings for scheduled snapshot events only. Event: Set settings for motion activated snapshot events only.
Size	The resolution of the snapshot when it is viewed or downloaded.

Quality	The overall quality of the snapshot, the lower the quality the less clear the image will become. The default is 5 however can be modified from 1 – 6.
Interval	The amount of time in which snapshots will be retained. This can range from 1 – 7 seconds or can be customized between 1-50000 seconds.

Schedule

The schedule menu allows you to set a snapshot schedule which will provide the camera with a way to only retain snapshots during specific days or times.



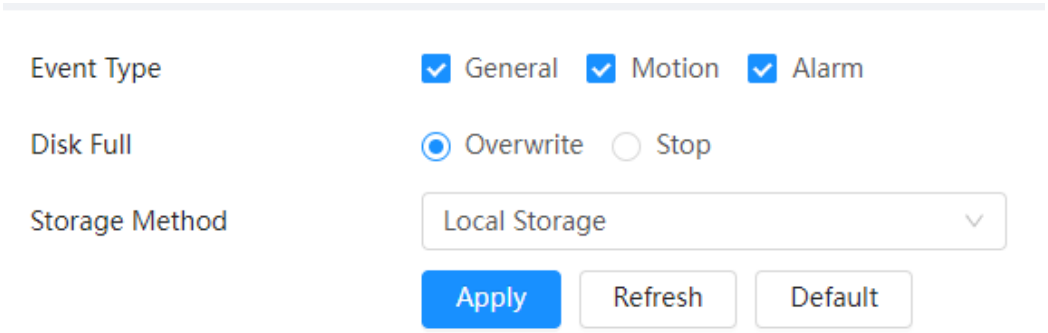
Below is an explanation of the fields on the Snapshot Schedule settings tab:

Record Type: These checkboxes allow the user to select which snapshot type they want to configure on the schedule. There are 3 types of snapshots:
General: General means that the camera will take snapshots during the specified time period. General recording is represented by the color green.
Motion: Motion Detection means that the camera only takes snapshots when the motion detection alarm is activated. Motion recording is represented by the color yellow.
Alarm: Alarm means that the camera only takes snapshots when an alarm is activated. Alarm recording is represented by the color red.
Snapshot Schedule: To specify a snapshot range, first select the type of snapshot desired, then click and drag on time bar for the desired date. To edit multiple days at once, drag the cursor further up or down to cover the other days.
Copy: Clicking this button opens a screen that allows for snapshot periods to be set for each day and for each snapshot type. There are a total of 6 periods that can be set.

Holiday: Provides a way to specify which days the schedule will not apply. To set a holiday, click the Holiday button and select Enable. On the calendar, select the dates in which the schedule will not apply and click OK. A separate holiday schedule can be applied, if a schedule is needed use your mouse to set the time & specified rule types. Click **Apply**.

Snapshot Control

This menu allows you to set a storage location to which snapshots will be sent. This can be set to local storage, which will send the snapshots to a microSD card (if installed) or via network storage which allows the snapshots to be sent using FTP or to an SFTP server.



Below is an explanation of the fields listed in this menu.

Event Type: These checkboxes allow the user to select which snapshot type they want to be sent to the storage method selected.

General: Pertains to 24/7, or continuous snapshot events.
Motion: Pertains to motion detection only snapshot events.
Alarm: Pertains to only if an alarm is activated

Disk Full: Allows the camera to overwrite or stop recording if the storage method is detected as full.
Storage Method: Choose the method in which snapshots are retained.

Local Storage: Snapshots will be stored in a microSD card (if installed).

Network Storage: Snapshots will be stored in a network storage option such as an FTP, NAS, or SFTP server.

Sending Snapshots Using Network Storage.

To send snapshots to an FTP server or NAS, select the network storage option from the storage method dropdown menu. Then select either FTP or NAS from the dropdown menu.

FTP

If using FTP, the recommended storage method would be SFTP. Please make sure a designated SFTP server is active before using this method. If an SFTP is not set up, please use FTP and set accordingly. Below is a description of the options provided in the SFTP or FTP mode menus.

Mode: Select between SFTP(Recommended) or FTP protocols.
Enable: Enables the SFTP or FTP protocol.
Sever IP: Enter the server IP of the SFTP or FTP server.

Port: Enter the port number associated with your SFTP or FTP server. Please note, if using SFTP, use port 22, if using FTP use port 21.
Username: Enter the username associated with the SFTP or FTP server.
Password: Enter the password associated with the SFTP or FTP server.
Storage Path: Enter the destination folder or path in which the events will be retained in the SFTP or FTP server.
Urgently store to local: If the SFTP or FTP server is unreachable, the files will be sent to local storage if a microSD card is installed.

Click **Apply** to set the SFTP or FTP settings. To refresh the interface, click **Refresh**. If you need to reset the settings back to default, click **Default**. After all credentials or entered, click **Test** to test the connection.

NAS

If using NAS, the protocol types are NFS or SMB. Please make sure a designated NAS is active before using this method. Below is a description of the options provided in the NAS interface of the camera.
Protocol Type: Select between NFS or SMB protocol types.
Enable: Use this toggle switch to enable the NAS feature.
Server IP: Enter the server IP address of your NAS system.
Storage Path: Enter the destination folder or path in which the events will be retained in the NAS.

Click **Apply** to save the settings. To refresh the interface, click **Refresh**. If you need to reset the settings back to default, click **Default**.

Auto Upload

The auto upload feature allows you to automatically upload the snapshots to a defined server using HTTP protocol once an alarm is triggered.

Upload Mode: The mode will be set to the default protocol, which is HTTP.
Enable: Enables the auto upload feature.
Add: Click add to begin setting the auto upload parameters.
Delete: Select the parameter from the interface and click delete to remove it.
No. The number is assigned to the parameters located in the interface.
IP/Domain: Double-click to enter the IP address of the defined server.
Port: Enter the port number of the defined server.
Event Type: Double-click to select which event types will be uploaded to the defined server.
Test: Click Test to test the connection between the camera and the defined server.
Delete: Click the trash can icon to delete the parameter. Click OK to remove it.

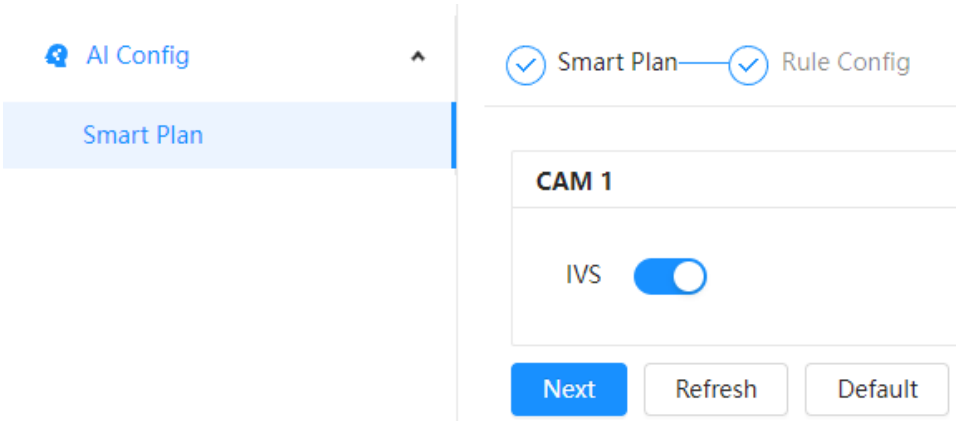
Click **Apply** to save the settings. To refresh the interface, click **Refresh**. If you need to reset the settings back to default, click **Default**.

AI

The AI menu allows the user to configure AI functions associated with your camera.

Smart Plan

A smart plan acts as a master switch for the AI features associated with your camera. Set the IVS toggle switch on and click **Next** to begin setting IVS rules.



Click the **Add Rule** option to begin applying the IVS rules into the interface.

Tripwire

Tripwire allows the camera to trigger an event if an object, such as a human or vehicle, crosses a set tripwire line. After adding the rule, the interface will show the rule as enabled, use your mouse to draw a detection line on the interface.

For a brief description of the features listed in this interface, please refer to the table below.

Rule	Description
	Rule: Used to begin drawing a detection line on the interface.
	Pixel: Used to measure and set the number of pixels in the target area on the live monitoring screen.
min	**Min. Size:** Used to determine the minimum size in which a target can be detected.
max	**Max. Size:** Used to determine the maximum size in which a target can be detected.
	Delete: Used to delete a parameter graphic on the interface.

Parameter	Description
Sensitivity	Adjust the sensitivity of the detection line drawn on the interface.
Direction	Allows the user 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)
Target Filter	Enable or disable the effective target options.
Effective Target	Enable human or vehicle detection options
Human	Enable human detection (only trigger when a human is detected).
Vehicle	Enable vehicle detection (only trigger when a vehicle is detected).
Schedule	Allows the user to set a schedule in which the IVS rule will be triggered
Alarm-out Port	If a local alarm is configured, enable this option to trigger the alarm if an event is triggered.

Post Alarm	The delay in between IVS events. The default is 10 seconds however this can be modified between 10~300 seconds.
Playback	Allow the user to store the recording locally and playback if a microSD card is inserted.
Post Record	The delay in which events will be recorded. The default is 10 seconds however this can be modified between 10~300 seconds.
Siren	Allow the camera to activate the onboard siren once an event is triggered.
Warning Light	Allow the camera to activate the red/blue warning LEDs once an event is triggered.
Flicker Frequency	Set the flicker frequency of the warning LEDs from low, medium, or high.
Stay Time	The amount of time the warning LEDs will flash after an event is detected.
Send Email	Enables the camera to send an email notification when an event is triggered
Snapshot	Allows a snapshot of the event to be sent in an email notification.

Click the Back option to return to the previous menu. Click **Apply** to save the settings. To refresh the interface, click **Refresh**. If you need to reset the settings back to default, click **Default**.

Intrusion

Intrusion allows the camera to trigger an event if an object, such as a human or vehicle, appears or crosses a set intrusion area set by the user. After adding the rule, the interface will display the rule as enabled, use your mouse to draw a detection area on the interface.

For a brief description of the features listed in this interface, please refer to the table below.

Rule	Description
	**Rule:** Used to begin drawing a detection area on the interface.
	**Pixel:** Used to measure and set the number of pixels in the target area on the live monitoring screen.
	**Min. Size:** Used to determine the minimum size in which a target can be detected.
	**Max. Size:** Used to determine the maximum size in which a target can be detected.
	**Delete:** Used to delete a parameter graphic on the interface.

Parameter	Description
Sensitivity	Adjust the sensitivity of the detection area drawn on the interface.
Action	Allows the user to choose a parameter filter that will activate a trigger if an object were to cross or appear in the set intrusion area. **Cross**: The rule will trigger when a target enters or exits the area. **Appears**: The rule will trigger when a target appears inside the area.
Direction	Allows the user to choose whether the rule will be triggered if an object enters, exits, or enters & exits a set line or area.
Target Filter	Enable or disable the effective target options.
Effective target	Enable human or vehicle detection options
Human	Enable human detection (only trigger when a human is detected).
Vehicle	Enable vehicle detection (only trigger when a vehicle is detected).
Schedule	Allows the user to set a schedule in which the IVS rule will be triggered

Alarm-out Port	If a local alarm is configured, enable this option to trigger the alarm if an event is triggered.
Post Alarm	The delay in between IVS events. The default is 10 seconds however this can be modified between 10~300 seconds.
Playback	Allow the user to store the recording locally and playback if a microSD card is inserted.
Post Record	The delay in which events will be recorded. The default is 10 seconds however this can be modified between 10~300 seconds.
Siren	Allow the camera to activate the onboard siren once an event is triggered.
Warning Light	Allow the camera to activate the red/blue warning LEDs once an event is triggered.
Flicker Frequency	Set the flicker frequency of the warning LEDs from low, medium, or high.
Stay Time	The amount of time the warning LEDs will flash after an event is detected.
Send Email	Enables the camera to send an email notification when an event is triggered
Snapshot	Allows a snapshot of the event to be sent in an email notification.

Click the Back option to return to the previous menu. Click **Apply** to save the settings. To refresh the interface, click **Refresh**. If you need to reset the settings back to default, click **Default**.

Camera

This menu allows the user to update or modify camera settings such as video, audio, or to manage image profiles.

Image

The image menu allows the user to configure image profiles as well as adjust the image, exposure, backlight, white balance, and other features associated with the camera. For more information, please refer to the information provided below.

Profiles

A profile allows the user to set when the image settings will be applied. The profile management section allows you to select between a general (24/7 profile option), schedule, or day/night profile type. Please note, if using a schedule profile type, use the Schedule option to set which months and days will apply to the selected profile.

Scheduling a Profile

To schedule a profile, select the Schedule button under profile management, then select the Schedule option at the bottom of the interface to begin setting a schedule. Use your mouse to select a profile type (color-coded options) and click and drag the timelines next to the specified month to select the month and hours in which the profile will apply.

Profile: This dropdown box allows the user to select which profile to apply. There are several profiles to choose between.
Day: Select this profile if surveillance will be outdoors in the sunlight. This will be the default profile.
Night: Select this profile if surveillance will be outdoors at nighttime.
General: Select this option to have the camera automatically switch between day/night profiles.
Front Light: Select this option if the camera is installed in an area with a light detected in the front area of the camera.
Back Light: Select this option if the camera is installed in an area with a light detected in the back area of the camera.
Strong Backlight: Select this profile if a strong backlight is detected by the camera.

Low Illuminance: Select this profile if the camera is in an area without a lot of light in the area.
Custom1: Set a custom profile in which the settings will apply.
Custom2: Set a custom profile in which the settings will apply.

Click **Apply** to save the settings. To refresh the interface, click **Refresh**. If you need to reset the settings back to default, click **Default**.

AI SSA

AI SSA (Scene Self-Adaption) is a technology that uses deep learning algorithms to intelligently identify multiple scenes and adjust to their optimal images. This helps to ensure that images are captured with the highest possible quality, regardless of the lighting conditions or other environmental factors.

Profile: This dropdown box allows the user to select which profile to apply. There are several profiles to choose between.
Mode: Enable or disable this option.

Click **Apply** to save the settings. To refresh the interface, click **Refresh**. If you need to reset the settings back to default, click **Default**.

Image

The image tab allows the user to configure image settings such as brightness, contrast, saturation, etc.

Style: Select between a standard, vivid, or soft image style. A soft style will display the actual color of the image. A standard style, which is the default style of the camera, will show a weaker hue with an increase in contrast. A vivid style will show the feed with greater hue and saturation.
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.
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 window 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.
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.
Gamma: This slider is used to adjust the gamma of the video. The larger the number, the brighter the video is. The default value is 50 and the recommended value ranges from 40 to 60.
Flip: Flips the image 0°, 90°, 180°, or 270°.

Mirror: Mirror the live feed left or right.

Click **Apply** to save the settings. To refresh the interface, click **Refresh**. If you need to reset the settings back to default, click **Default**.

Exposure

The exposure tab allows the user to configure exposure settings such as anti-flicker, exposure contrast, noise reduction settings, etc.

Anti-Flicker: These radio buttons allow the user to select what type of anti-flicker technology should be used for the video feed. The three options are 50 Hz, 60 Hz, and Outdoor. The desired option should offset any flickering effect caused by the electrical current used in the specific area.

Mode: This dropdown menu allows the user to modify certain exposure settings related to the device such as, gain priority, shutter priority or setting a manual gain setting.

Auto- This setting lets you select your shutter speed and have the gain adjust automatically. Selecting customized range will let you both the shutter speed an adjust the gain manually.

Gain Priority - This setting will maximize the gain for the ideal exposure. Low Noise Basically turns up the ISO to the best setting without sacrificing exposure timing.

Shutter Priority- This setting will maximize the fastest shutter speed and will sacrifice the gain in return.

Manual – This setting allows the user to manually adjust shutter and gain values, the recommended shutter value is 0-33.33ms and the recommended gain value is 0-50.

Exposure Compensation: Use this slider to control the brightness of the exposure. Please note, the higher the value is, the brighter the image will be, 50 will be the most compensation that can be used on this device.

3D NR: This radio button allows the user to turn the 3D Noise Reduction feature on or off.

3D NR Level: This slider allows the user to specify the 3D Noise Reduction level. The value ranges from 1-100.

2D NR Level: This slider allows the user to specify the 2D Noise Reduction level. 2D noise reduction will be active if 3D NR is disabled. The value ranges from 0 to 100.

Click **Apply** to save the settings. To refresh the interface, click **Refresh**. If you need to reset the settings back to default, click **Default**.

Backlight

The backlight tab allows the user to modify and configure backlight settings associated with the camera including, BLC, HLC, and WDR.

Mode: Use this dropdown menu to select between different backlight compensation modes.

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.

HLC: Highlight compensation is a feature that came out of necessity due to overexposure from strong light sources like headlights or spotlights.

WDR: Wide Dynamic Range makes multiple scans of a scene to provide one balanced and unwashed image that is clear for the user.

SSA: Smart Scene Adaptive, automatically evaluates and compensates for changes in the luminance of a scene.

Click **Apply** to save the settings. To refresh the interface, click **Refresh**. If you need to reset the settings back to default, click **Default**.

WB

The WB tab allows the user to modify and configure white balance settings. White balance is used to adjust colors to match the color of the light source so that white objects appear white. Please note, objects may be lit by a number of different light sources, including sunlight, incandescent bulbs, and fluorescent lighting.

Mode: Use this dropdown menu to select between different white balance modes.

Auto: Automatically determine proper white balance of a specified area.
Natural Preset mode for areas with large amounts of lights.
Street Lamp: Preset mode for darker areas to ensure color precision.
Outdoor: Preset mode for outdoor settings in natural or artificial light.
Manual: Manually adjust the red and blue values of the feed
Custom Area: Allows the user to select a specific region of the live feed to apply white balance settings.

Click **Apply** to save the settings. To refresh the interface, click **Refresh**. If you need to reset the settings back to default, click **Default**.

Day/Night

The day/night tab allows the user to set the camera to switch between color and black and white modes according to the environmental conditions.

Mode: Use this dropdown menu to select between different day/night modes.

Color: The camera will display a color image only.
B/W: The camera will display a black and white image only.

Click **Apply** to save the settings. To refresh the interface, click **Refresh**. If you need to reset the settings back to default, click **Default**.

Illuminator

The Illuminator tab allows the user to enable or disable night vision settings. The camera is set by default to automatically enable the onboard white light LEDs.

Profile: This dropdown box allows the user to select which profile to modify. The 3 options are Day, Night, and Normal.

Fill Light: This dropdown menu allows the user to select between various night vision modes.

IR Mode: Allows the camera to switch on the IR LEDs for B&W night vision.
White Light: Allows the camera to switch on the white light LED for color night vision.
Smart Illumination: Allows the camera to switch on the IR LEDs, however once an object is detected the deterrent LEDs will flash.

Mode: This dropdown box allows the user to select whether to turn the IR light on or off. (Auto only for smart illumination).

Auto – Sets the IRs to automatically turn on or off based on Day & Night conditions.
Manual – Manually turns the IRs on.
Off – Manually turns the IR LEDs off. Please note, IR LEDs will not turn on at all when this option is selected.

Brightness Upper Limit: Use this slider to adjust the amount of light provided by the white light LEDs. Ranges from 0 to 100.

Click **Apply** to save the settings. To refresh the interface, click **Refresh**. If you need to reset the settings back to default, click **Default**.

Defog

The defog tab allows the user to set the image quality to improve if being used in foggy or hazy conditions. This feature will be off by default however can be set to automatically be enabled if the conditions change.

Mode: Use this dropdown menu to select between different defog modes.

Auto: Automatically set to improve image quality in hazy or foggy conditions.
Manual: Will automatically switch between defog modes, however, the user can manually adjust the intensity of the defog mode between high, medium, and low.
Off: Disables defog mode.

Click **Apply** to save the settings. To refresh the interface, click **Refresh**. If you need to reset the settings back to default, click **Default**.

LDC

This menu allows the user to adjust the lens distortion correction. This allows the camera to straighten barrel distortion of the lens. Please note, when enabled, it will cut a considerable portion of the image. Below is an explanation of the features provided in this menu.

Profile: This dropdown box allows the user to select which profile to modify. The 3 options are Day, Night, and General.
LDC: Enable or disable lens distortion correction.

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

AFSA

AFSA, or AI Scene Self-Adaption, is a technology that uses deep learning algorithms to intelligently identify multiple scenes and adjust the camera settings accordingly to capture the highest quality images.

Click **Apply** to save the settings. To refresh the interface, click **Refresh**. If you need to reset the settings back to default, click **Default**.

Encode

This menu allows the user to change video settings for the camera's video feed including video overlays.

Compression: The camera supports H.264, H.264H, and H.265 compression types.
Encoding Strategy: Choose between a general, smart, or AI codec to improve video compressibility and reduce storage space. Please note, it is recommended to keep this as default (General).
Resolution: Change the mainstream resolution of the camera. The default resolution will be 12MP (4000*3000).
Frame Rate (FPS): Change the mainstream fps (frames per second) of the camera. The default is 25 fps.
Bit Rate Type: The camera supports two-bit rate types: CBR (constant) and VBR (variable). If using a variable bit rate type, the video quality of the camera can be adjusted.
Reference Bit Rate: This is the recommended bit rate value according to the resolution and frame rate.

Bit Rate: This dropdown box allows the user to select a bit rate or create a custom bit rate between 3 – 17664 Kb/s
I Frame Interval: This field allows the user to set the P frame amount between two I frames. The value ranges from 1 to 150 seconds. The default value is 50.
Watermark String: This field allows the user to set the watermark's text. The default string is Amcrest. The maximum length is 85 characters. This string can only include numbers, characters, and underscores.

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.

Click **Apply** to save the settings. To refresh the interface, click **Refresh**. If you need to reset the settings back to default, click **Default**.

Overlay

The overlay menu allows the user to set and configure overlay details associated with the camera. This includes privacy masking, channel titles, font properties, logo overlays, etc.

Privacy Masking

Privacy masking allows the user to set up to 4 distinct blocks on the live feed to block certain objects or areas on the screen. By default, 4 areas will already be set, use your mouse to adjust the area size and location of the privacy masking blocks. To clear the overlays, click "clear".

Enable: Enable privacy mask settings
Add: Add additional privacy masking blocks to the feed. Four is the max.

Clear: Clear all overlays from the feed. To delete a specific privacy mask overlay, click on the trash can icon next to the overlay selection in the interface.

Click **Apply** to save the settings. To refresh the interface, click **Refresh**. If you need to reset the settings back to default, click **Default**.

Channel Title

The channel title menu allows the user to change the input text and text alignment found on the interface. The camera can support up to 2 channel titles, to add an additional channel title, click the "+" symbol found on the interface and enter the text into the provided field. Use your mouse to adjust the location of the channel title on the interface.

Enable: Enable the channel title overlay
Input Text: Input and edit channel title text. Use the "+" icon to enter additional input text.
Text Alignment: Align the channel title text to the left or right of the editable banner.

Click **Apply** to save the settings. To refresh the interface, click **Refresh**. If you need to reset the settings back to default, click **Default**.

Time Title

The time title menu allows the user to enable or disable the time stamp overlay found on the live feed. The day of the week can be displayed as well using the "week display".

Enable: Enable or disable the time stamp overlay found on the live feed.
Week Display: Display the day of the week on the time stamp overlay.

Click **Apply** to save the settings. To refresh the interface, click **Refresh**. If you need to reset the settings back to default, click **Default**.

Location

The location menu allows the user to add an additional overlay to be displayed on the live feed. The camera can support up to 2 additional location titles, to add an additional location title, click the "+" symbol found on the interface and enter the text into the provided field. Use your mouse to adjust the location of the location title on the interface.

Enable: Enable the location overlay.
Input Text: Input and edit the location text. Use the "+" icon to enter additional input text.
Text Alignment: Align the location text to the left or right of the editable banner.

Click **Apply** to save the settings. To refresh the interface, click **Refresh**. If you need to reset the settings back to default, click **Default**.

Font Properties

The font properties menu allows the user to adjust the font size and color of the text found in the interface.
Font Size: Choose between different font sizes. By default, the font size will be set to general which allows the text to fit the screen size.
Color: Use the provided color pallet to set the color of the text.
Line Spacing: The amount of space between each text (1-1.5mm)
Click **Apply** to save the settings. To refresh the interface, click **Refresh**. If you need to reset the settings back to default, click **Default**.

Logo Overlay

The logo overlay menu allows the user to enable or disable the Amcrest logo found on the interface.

Enable: Enable or disable the Amcrest logo overlay.

Click **Apply** to save the settings. To refresh the interface, click **Refresh**. If you need to reset the settings back to default, click **Default**.

Custom Title

The Custom Title menu allows the user to enter and set a custom text overlay in live feed. The camera can support up to 2 additional custom titles, to add an additional custom title, click the "+" symbol found on the interface and enter the text into the provided field. Use your mouse to adjust the location of the custom title on the interface.

Enable: Enable the custom title overlay.
Input Text: Input and edit the custom title text. Use the "+" icon to enter additional input text.

Text Alignment: Align the custom title text to the left or right of the editable banner.

Click **Apply** to save the settings. To refresh the interface, click **Refresh**. If you need to reset the settings back to default, click **Default**.

Audio

The Audio menu allows the user to modify audio settings for the camera. There are no built-in audio devices for this camera such as a speaker or microphone.

Enable: Enable or disable audio on the main or sub stream.
Compression: This dropdown allows the user to modify audio
Sampling Frequency: This dropdown box allows the user to select a sampling frequency for the audio. Audio sampling allows for higher or lower sound quality.
Noise Filter: This option allows the user to enable or disable the noise filter. A noise filter helps provide a cleaner audio quality.
Microphone Volume: Use this slider to adjust the audio in function of the microphone.
Speaker Volume: Use this slider to adjust the audio out function of the speakers.

Click **Apply** to save the settings. To refresh the interface, click **Refresh**. If you need to reset the settings back to default, click **Default**.

Alarm Tone

The Alarm Tone tab allows the user to add a custom tone which can be applied to a siren or alarm once it has been triggered.

Add: Click **Add** to add a custom audio file into the interface. The audio file must be a .wav file.

Adding a Custom Audio File

The interface allows you to manually record or upload an audio file. To record a custom audio file, enter a name for the file and click the record button, click the stop button to stop recording and select the audio file in the interface. To upload a custom audio file, click the upload button and click the browse button to select the .wav file you would like to upload. Once the file is loaded, click Upload and select the audio file in the interface. 39

To select a custom audio file, select a tone from the interface, the alarm will automatically be applied to the camera. If the siren or audio linkage option in the rule is triggered the custom alarm will sound. To manually trigger the alarm, click on the () icon located in the live view menu.

Click **Apply** to save the settings. To refresh the interface, click **Refresh**. If you need to reset the settings back to default, click **Default.**

Alarm

The alarm menu allows the user to set motion detection, audio detection, alarm, and abnormality settings. Motion detection will be enabled by default in this menu.

Motion Detection

This tab allows the user to enable or disable motion detection settings. Below is a description of the features provided in this menu.

Parameter	Description
Enable	Enable or disable the feature.
Schedule	Allows the user to set a schedule in which the rule will be triggered. Motion detection will be set to trigger 24/7. However, to set a motion detection schedule, click Add Schedule. Use your mouse to set a schedule, per hour, per day if needed click Apply to set the setting.
Anti-dither	The time in which the camera will not capture any movement. After this end, the feature would inform the camera to begin recording the footage again.
Region	Allows the user to set regions in which motion detection will not be detected. The camera can set up to 4 different, color-coded regions. Use your mouse to adjust the area. This option also allows you to control the sensitivity and threshold of the detection area. **Sensitivity** is the amount of change required to increase the motion detected by a percentage. The lower the sensitivity, the more movement is required to trigger an alarm. **Threshold** is the level that the motion detection needs to reach to trigger an alarm. The lower the threshold, the more likely that motion will trigger an alarm. To designate a zone, click and drag the mouse over the area desired. When a colored box is displayed over the live feed, that area is now enabled for motion detection. After the motion detection zone is set, click the enter button to exit the motion detection screen. Remember to click the save button on the motion detection settings screen, otherwise the motion detection zones will not go into effect. Clicking the cancel button to leave the motion detection zone and will not save the zone setup.
Alarm-out Port	Enable or disable motion detection to trigger an external alarm (if applicable).
Post-alarm	The amount of time the event will end after it is triggered.
Playback	Allow the user to store the recording locally and playback if a microSD card is inserted.
Post-Record	The delay in which events will be recorded. The default is 10 seconds however this can be modified between 10~300 seconds.
Siren	Allows the camera to activate the onboard siren once an event is triggered.
Warning Light	Allow the camera to activate the red/blue warning LEDs once an event is triggered.
Flicker Frequency	Set the flicker frequency of the warning LEDs from low, medium, or high.
Stay Time	The amount of time the warning LEDs will flash after an event is detected.
Send Email	Enables the camera to send an email notification when an event is triggered
Snapshot	Allows a snapshot of the event to be sent in an email notification. Use the 1,3, and 5 snapshot options to choose whether 1, 3, or 5 images of the alert will be sent in an email notification.

Click **Apply** to save the settings. To refresh the interface, click **Refresh**. If you need to reset the settings back to default, click **Default**.

Video Tampering

This option allows the camera to trigger an event if the camera's lens is covered or if the video output becomes insufficient. Below is a description of the features provided in this menu.

Parameter	Description
Event Type	The type of event that is being reported (video tampering).
Enable	Enable or disable the feature.
Covered Area	The percentage of the area that is being monitored by the camera.
Duration	The amount of time the alarm is activated before it ends.
Anti-dither	The time in which the camera will not capture any movement. After this end, the feature would inform the camera to begin recording the footage again.
Schedule	Allows the user to set a schedule in which the feature will be triggered. Tampering will be set to trigger 24/7 however, to set a motion detection schedule, click Add Schedule. Use your mouse to set a schedule, per hour, per day if needed click Apply to set the setting.
Alarm-out Port	Enable or disable tampering to trigger an external alarm (if applicable).
Post-alarm	The amount of time the event will end after it is triggered.
Playback	Allow the user to store the recording locally and playback if a microSD card is inserted.
Post-Record	The delay in which events will be recorded. The default is 10 seconds however this can be modified between 10~300 seconds.
Send Email	Enables the camera to send an email notification when an event is triggered
Snapshot	Allows a snapshot of the event to be sent in an email notification.

Click **Apply** to save the settings. To refresh the interface, click **Refresh**. If you need to reset the settings back to default, click **Default**.

Audio Detection

This option allows the user to set event triggers based on audio thresholds such as a vague voice, tone changes, or any other sound intensity is detected. Below is a description of the features provided in this menu.

Parameter	Description
Audio Exception	Enable or disable the feature.
Intensity Change	Allows the alarm to trigger if the sound intensity is higher than the sensitivity and threshold settings. Intensity levels will be displayed in the graph below the sensitivity and threshold options.
Sensitivity	The amount of change required to increase the motion detected by a percentage. The lower the sensitivity, the more movement is required to trigger an alarm.
Threshold	The level that motion detection needs to reach to trigger an alarm. The lower the threshold, the more likely that motion will trigger an alarm.

Schedule	Allows the user to set a schedule in which the feature will be triggered. Audio detection will be set to trigger 24/7 however, to set a motion detection schedule, click Add Schedule. Use your mouse to set a schedule, per hour, per day if needed click Apply to set the setting.
Anti-dither	The time in which the camera will not capture any movement. After this end, the feature would inform the camera to begin recording the footage again.
Alarm-out Port	Enable or disable audio detection to trigger an external alarm (if applicable).
Post-alarm	The amount of time the event will end after it is triggered.
Playback	Allow the user to store the recording locally and playback if a microSD card is inserted.
Post-Record	The delay in which events will be recorded. The default is 10 seconds however this can be modified between 10~300 seconds.
Send Email	Enables the camera to send an email notification when an event is triggered
Snapshot	Allows a snapshot of the event to be sent in an email notification.

Click **Apply** to save the settings. To refresh the interface, click **Refresh**. If you need to reset the settings back to default, click **Default**.

Alarm

The alarm menu allows the user to set alarm configurations if an external alarm is connected to the device. External alarm connections are as follows:

Color	Description
Brown	Alarm_OUT1
Green	Alarm_OUT_GND
Blue	Alarm_IN1
Gray	Alarm_IN_GND

Below is a description of the features provided in this menu.

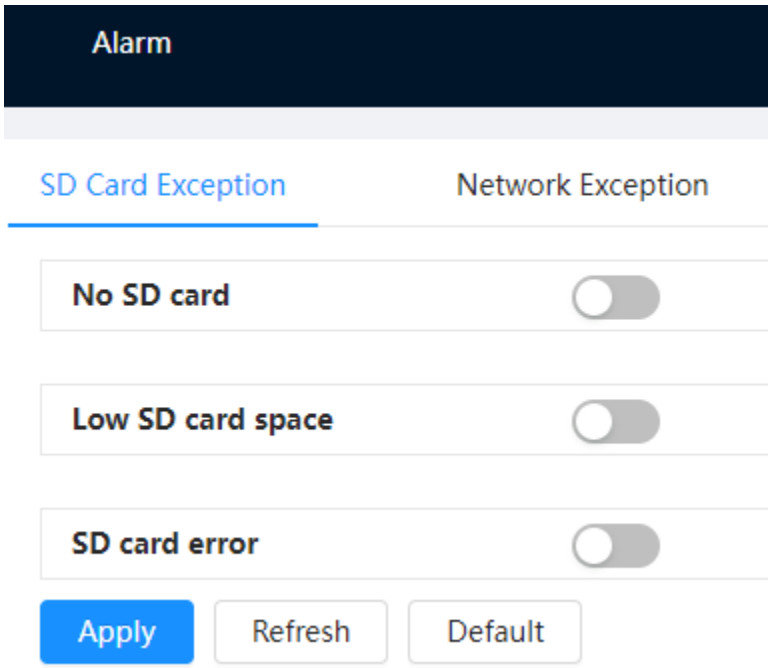
Parameter	Description
Enable	Enable or disable the feature.
Alarm-in Port	Allows the alarm to trigger if the sound intensity is higher than the sensitivity and threshold settings. Intensity levels will be displayed in the graph below the sensitivity and threshold options.
Schedule	Allows the user to set a schedule in which the feature will be triggered. Audio detection will be set to trigger 24/7 however, to set a motion detection schedule, click Add Schedule. Use your mouse to set a schedule, per hour, per day if needed click Apply to set the setting.
Anti-dither	The time in which the camera will not capture any movement. After this ends, the feature would inform the camera to begin recording the footage again.
Sensor Type	No (Normally Open) – This will allow the alarm to stay active until triggered. NC (Normally Closed) – This will allow the alarm to stay closed until triggered.
Alarm-out Port	Enable or disable an alarm to trigger an external alarm (if applicable).
Post-alarm	The amount of time the event will be end after it is triggered.

Playback	Allow the user to store the recording locally and playback if a microSD card is inserted.
Post-Record	The delay in which events will be recorded. The default is 10 seconds however this can be modified between 10~300 seconds.
Siren	Allows the camera to activate the onboard siren once an event is triggered.
Send Email	Enables the camera to send an email notification when an event is triggered
Snapshot	Allows a snapshot of the event to be sent in an email notification.

Click **Apply** to save the settings. To refresh the interface, click **Refresh**. If you need to reset the settings back to default, click **Default**.

Abnormality

This menu allows the user to adjust and set error configurations which will trigger a notification if an abnormality is detected.



SD Card Exception

This option allows the user to choose which errors will occur if the camera detects an abnormality with an inserted microSD card.

Parameter	Description
No SD card	Enable this option to trigger an event if no microSD card is inserted or detected by the camera.
Low SD card space	Enable this option to trigger an event if the space on the microSD card is low.
SD card error	Enable this

Click **Apply** to save the settings. To refresh the interface, click **Refresh**. If you need to reset the settings back to default, click **Default**.

Network Exception

This option allows the user to choose which errors will occur if the camera detects or determines a network or connection abnormality such as if the camera is offline or is experiencing an IP conflict.

Offline

This abnormality will be triggered if the camera is detected offline in the network.

Parameter	Description
Alarm-out Port	Enable or disable an alarm to trigger an external alarm (if applicable).
Alarm Channel	Choose alarm channel 1 or alarm channel 2 to be triggered.
Post-alarm	The amount of time the event will be end after it is triggered.
Playback	Allow the user to store the recording locally and playback if a microSD card is inserted.
Post-Record	The delay in which events will be recorded. The default is 10 seconds however this can be modified between 10~300 seconds.

IP Conflict

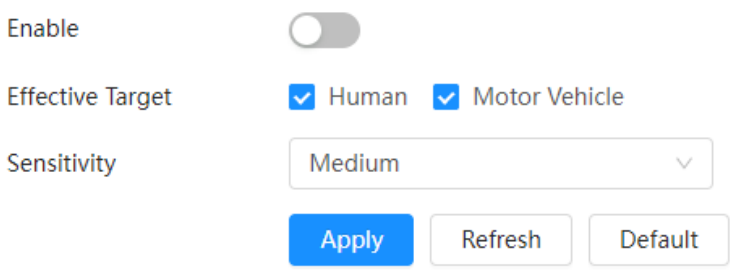
This abnormality will be triggered if the camera detects an IP conflict between the network and the camera if set to DHCP.

Parameter	Description
Alarm-out Port	Enable or disable an alarm to trigger an external alarm (if applicable).
Alarm Channel	Choose alarm channel 1 or alarm channel 2 to be triggered.
Post-alarm	The amount of time the event will be end after it is triggered.
Playback	Allow the user to store the recording locally and playback if a microSD card is inserted.
Post-Record	The delay in which events will be recorded. The default is 10 seconds however this can be modified between 10~300 seconds.

Click **Apply** to save the settings. To refresh the interface, click **Refresh**. If you need to reset the settings back to default, click **Default**.

Smart Motion Detection

Smart Motion Detection uses an advanced algorithm to differentiate between human and motor vehicle shapes within a scene and send alarms only when a person or vehicle is detected. This helps to reduce false alerts from objects such as leaves blowing on a tree, animals, or other unwanted objects.



This option works alongside basic motion detection, so any options enabled in the motion detection menu will apply to smart motion detection as well. To use this option, click the Enable option, select an effective target filter (human or vehicle), set the sensitivity (medium is recommended), then click **Apply**.

Disarming

The disarming feature allows you to temporarily disable the alarm and other security features of your camera. This can be useful if you need to enter or exit your property without triggering an alarm, or if you want to temporarily disable the system for maintenance.

Disarming: Enable or disable the feature.
Disarm by Period: Enable a schedule to be assigned to the feature.
Disarm Period: Set a schedule for the disarming feature. Click **Add Schedule** to set the schedule.
Event Notifications: Enable or disable notifications related to the disarming feature.
Disarm Alarm Linkage Action: Select which type of notification will be applied.

Click **Apply** to save the settings. To refresh the interface, click **Refresh**. If you need to reset the settings back to default, click **Default**.

Maintain

The maintain menu allows the user to set user management options, device operation, and maintenance options.

General

The basic menu allows you to view basic camera information such as the device name (serial number) as well as set different video standards such as NTSC and PAL.

Click **Apply** to save the settings. To refresh the interface, click **Refresh**. If you need to reset the settings back to default, click **Default**.

Date & Time

The date & time tab allows you to set and view date and time information as well as provides an option to sync the device to your current computer's date & time. Below is a description of the features provided in this menu.

Parameter	Description
Time	Allows the user to switch between setting a custom time or connecting to an NTP server.
System Time	Allows the user to manually set the date and time using a provided calendar.
Sync with PC	Allows the user to sync the device to the local PC's current date & time
Time Format	Allows the user to choose which format the date and time will be displayed. Please note, time can be displayed in 24-hour or 12-hour format.
Time Zone	Allows the user to choose a specific time zone which the camera is located.
DST	Allows the user to enable Daylight Savings Time options.
Enable	Enable DST settings.
Type	Select between date and week DST settings.
Start Time	The date in which DST will start (March 2nd)
End Time	The date in which DST will end (November 1st)

Click **Apply** to save the settings. To refresh the interface, click **Refresh**. If you need to reset the settings back to default, click **Default.**

Information

The information menu displays the current ONVIF, system, web, and algorithm version, that is currently being applied to the camera. Use the Online User tab to see who is currently accessing the camera.

Version

This menu provides an oversight of the current ONVIF, system (firmware), web, and algorithm version that is currently applied to the camera.

Online User

This menu will display a list of all users that are currently accessing or actively using the camera. To refresh the interface, click the **Refresh** button.

Account

The account menu allows users to add or modify shared users, set user groups, as well as add an ONVIF user.

User

The user tab allows the user to add or modify a shared user to the camera. This will allow another user the ability to access the camera based on specific limitations or permissions provided by the admin account. Below is a description of the features provided in this menu.

Parameter	Description
Add	Click the add button to add a shared user.
Delete	Select a user from the interface and click Delete to remove the user.
Anonymous Login	Allows admin to login using the IP address instead of a username and password. Please note, anonymous users only have preview authorities. If signed in as an anonymous user, click Logout to login with other usernames.
Interface	Displays the number of users, the username, group, password strength, remarks, restricted login details, and operation (edit/delete). Editing user details allows you to update the current password for a shared user as well as set account permissions related to the system, live view, or search options available.
Password Reset	Enable or disable the ability to perform a password reset.

Click **Apply** to save the settings. To refresh the interface, click **Refresh**. If you need to reset the settings back to default, click **Default.**

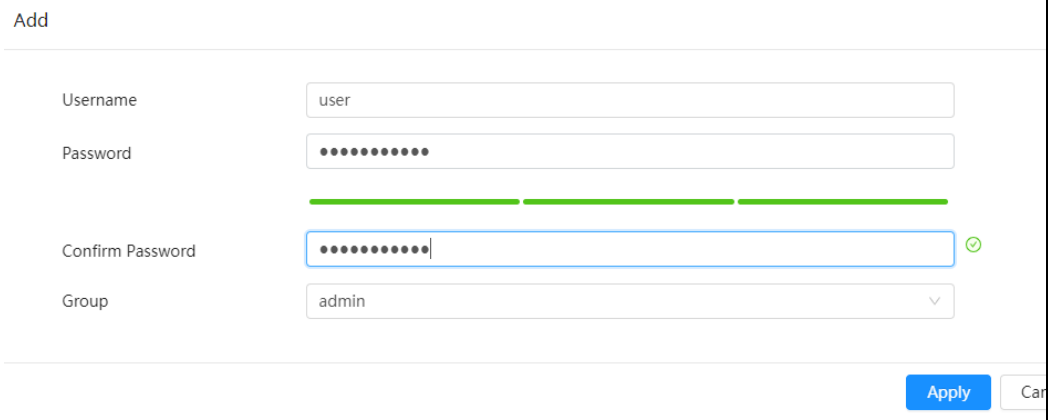
Group

The group tab allows the user to set or modify group details. Users can be assigned to specific groups within the interface if multiple users are applied. Please note, there will be two groups assigned by default, an admin group and a user group. Below is a description of the features provided in this menu.

Parameter	Description
Add	Click the add button to add a new user group. Enter a name for the group as well as any remarks pertaining to the group. Select which permissions will apply to this new group, this can be system, live, or search options. Click apply to set these permissions to the specific user group.
Delete	Select the group from the interface and click delete to remove it from the camera.
Operation	Used to edit or delete a user group. Click the edit button to edit the group's name, remarks, or system permissions. Click OK when finished.
Interface	Displays the group name, remarks pertaining to the group, as well as edit and delete options. Use the edit button to update the group name, remarks, or system permissions. Click OK when finished.

ONVIF User

The ONVIF user tab allows the user to set or modify any ONVIF user details related to the camera. This allows you to add, delete, or change the password of an ONVIF user. Below is a description of the features provided in this menu.

Parameter	Description
Add	Click the add button to add a new user group.  Enter a username and password for the ONVIF user, then use the group dropdown
Delete	Select the ONVIF user from the interface and click delete to remove them from the camera.
Operation	Used to edit or delete a user group. Click the edit button to edit the group's name, remarks, or system permissions. Click OK when finished.
Interface	Displays the ONVIF user's name, which group they are in, password strength, as well as edit and delete options. Click the edit option next to the ONVIF user to change the username or update the password for an existing ONVIF user.

Manager

The manager menu allows the user to set maintenance, import/export, and default settings to the camera. These options are available in separate tabs within the system.

Maintenance

The camera provides a few maintenance options such as the ability to automatically restart the camera as well as the ability to automatically delete old files if a microSD card is inserted. Below is a description of the features provided in this menu.

Restart System

Set the camera to automatically restart at a scheduled time.

Parameter	Description
Auto Restart	Enable or disable the camera from automatically restarting
Restart Time	Use the dropdown menu to select a day in which the camera will restart, then enter a time.

Delete Old Files

Set the camera to automatically delete old files based on the set number of days it has been stored on a microSD card. Please note, once files are deleted, they cannot be restored.

Parameter	Description
Auto Delete	Enable or disable the camera to delete old files.
Delete File	Once enabled, enter the number of days in which the camera keeps these files before they are deleted.

Click **Apply** to save the settings. To refresh the interface, click **Refresh**. If you need to reset the settings back to default, click **Default.**

Import/Export

This menu allows you to export or import a current configuration file for the camera. This option is useful if you need to perform a factory reset and would like to keep your current configuration. Below is a description of the features provided in this menu.

Parameter	Description
Export Configuration File	Click this option to download a configuration backup file to your computer.
File	Allows the user to select and import a configuration file to the camera. To import a config file, click Select File and load the config file to the interface. Click Import File to apply the configuration to the camera.

Default Settings

This menu allows you to reset your camera to its original default settings or factory reset the camera completed. Please note, performing a factory reset will revert all configurations to factory settings, this includes the admin's username and password. The default password for the camera is **admin.** Below is a description of the features provided in this menu.

Parameter	Description
Default	Click the Default option to restore all settings back to default.
Factory Defaults	Click the Factory Defaults option to restore all parameters, including admin username and password to factory settings.

Packet Capture

This option allows the camera to use a built-in packet sniffer to monitor the packet data flowing from the camera across the network. Optional IP ports can be used. However, to use this option, click on the play icon in the Packet Sniffer Backup field. The camera will begin the process, click the pause button when complete. A .pcap report will be downloaded to your computer when stopped.

Run Log

This menu allows the user to view and export log details related to the camera. Logs are based on the internal actions retained by the camera. To view a log, select the download option to download and view the log on your computer.

Security

This menu allows the user to perform a security scan as well as the current security status of the camera. If security is compromised, click the Details icon to provide optimization options. Below is a description of the features provided in this menu.

Parameter	Description
Security Status	Click the **Rescan** icon to perform a security scan of the camera. This will scan all security parameters and provide the current security status of the device.
Login Authentication	Detect whether the current login authentication mode conforms to the recommendation.
User Status	Detect whether a user password is as complicated as required.
Configuration Security	Detect whether the current Email, FTP, SFTP, HTTPS, etc. configuration conforms to the recommendation.
Audio/Video Transmission Encryption	Encrypt real-time live view and playback video streams during network transmission.
Trusted Protection	Based on trusted protection technology, ensure that the device runs in a trusted safe environment. • **Trusted Update:** Verify the upgrade firmware integrity and validity based on digital signature technology. • **Trusted Boot:** During start, make signature verification of firmware data, and ensure operating code and data is valid and effective. • **Trusted Execute:** Monitor real-time operating status, recognize, and reject execution of malicious programs, and protect the device from virus.
Security Warning	Immediately after detecting security abnormal behaviors, the device sends a security warning to remind the user timely.
Attack Defense	Monitor cyber-attacks in real-time and take effective defending measures to protect device network security.
Firmware Encryption	The officially released firmware is encrypted. After upgrade, it is encrypted for storage in system partition.

802.1x	Based on 802.1x technology and build network access control system to effectively block unauthorized hosts from accessing the protected private network. Please note, this should be disabled by default and may not be available in most devices.
Secure Shell	Based on mutual authentication by device administrator and third-party service, provide multi-factor authentication to prevent background terminal from malicious operation.
Configuration Files Security	Encrypt the device configuration file with a safe key and export it in an encrypted way. • **Encrypted Storage of Configuration:** The device makes encrypted storage of background configuration data to protect data security. • **Encrypted Exporting of Configuration:** The device can export configuration backup in an encrypted way by default.
CA Certificate	Centralized management of CA certificate helps you to use the certificate more normatively.
Log Security	Support recording logs by levels to ensure traceability of system operations and events.
Session Security	Monitor session interaction process in real-time, and recognize validity, authenticity, and security of session credentials. • **Auto Logout after Timeout:** If the client has no operation for a long time, the device will log out of this session automatically to avoid any security threats. • **Brute-force Access Prevention:** When the device detects continuous attempted access with wrong session credentials, the follow-up access of this host will be blocked to avoid session leakage. • **Anti-hijacking:** The device recognizes the binding between session credential and client host, rejects unmatched session requests and avoids session leakage.
Physical Backup	Based on physical backup, in case of physical damages, the device switches to backup device, and thus effectively improves operation continuity and robustness. **System Partition Backup:** If device firmware upgrading failed accidentally, when it is restarted, the device will automatically restore previous firmware data from backup partition, so that the device restores normal operation.

Attack Defense

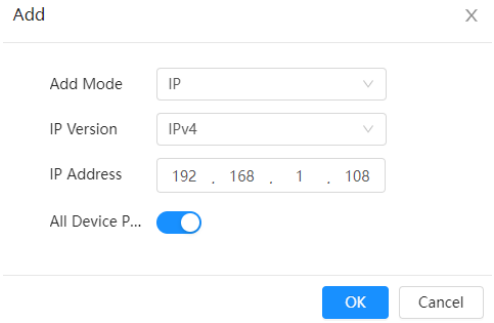
This menu allows you to set IP filters, account lockout details, as well as anti-DoS attack options which help to provide an added layer of security to your device.

IP Filter

The IP Filter menu allows users to whitelist and blacklist specific IP addresses. This feature helps make the camera more secure by limiting remote access to only approved users. Please note, that only source hosts whose IP/MAC are provided in the interface will be allowed to access the corresponding ports of the camera.

Below is a description of the features provided in this menu.

Parameter	Description
Enable	Enable or disable IP filtering
Mode	Select between an allowlist (whitelist) or blocklist (blacklist)

Add	Add an IP address to the interface. Enter the mode, IP version, and IP address and click OK. 
Delete	Select an IP from the interface and click delete to remove it the interface.
Interface	Displays the host IP/MAC, port number, and operation. Click the edit icon to edit a selected IP. Click the trashcan icon to remove the IP from the interface.

Click **Apply** to save the settings. To refresh the interface, click **Refresh**. If you need to reset the settings back to default, click **Default.**

Account Lockout

The account lockout menu allows the user to set how many attempts can be used before the user's account is locked as well as the duration of how long it will be locked for, please note, default will be 5 attempts, with a duration of 5 minutes. Click **Apply** to save the account lockout settings.

ONVIF users can also set their account login attempts separately as well. The default for an ONVIF user will be 30 times with a duration of 5 minutes. Click Apply to save the account lockout settings.

Click **Apply** to save the settings. To refresh the interface, click **Refresh**. If you need to reset the settings back to default, click **Default.**

Anti-DoS Attack

This menu provides additional tools such as SYN Flood Attack Defense and ICMP Flood Attack Defense to defend the device against DoS attacks. Below is a description of the features provided in this menu.

Parameter	Description
SYN Flood Attack Defense	Use the Enable/Disable toggle switch to enable or disable this feature. **Note:** An attacker might send out repeated SYN messages to the device, leaving many half-open TCP connections on the device, which will make the device crash. When hit by an SYN flood attack, the device will defend itself by discarding the first message.
ICMP Flood Attack Defense	Use the Enable/Disable toggle switch to enable or disable this feature. **Note:** An attacker might send out an abnormally large number of ICMP packets to the device, which will use up all computing resources and thus make the device crash. When hit by an ICMP flood attack, the device will defend itself by using the ICMP message filtering tactic.

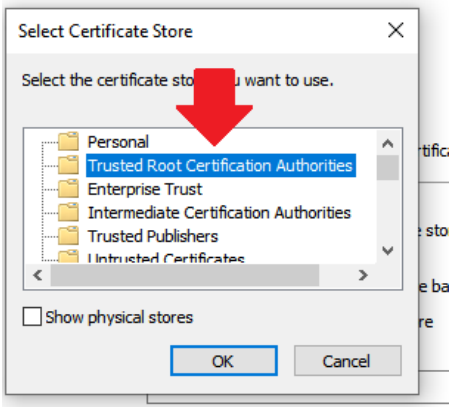
Click **Apply** to save the settings. To refresh the interface, click **Refresh**. If you need to reset the settings back to default, click **Default.**

CA Certificate

This menu allows the user to create or upload an unauthenticated certificate so you can log into the web browser through HTTPS with your PC. Please note that a device certificate is proof of the device's legal status. For example, when the user is visiting the device using HTTPS, the device certificate shall be verified.

There will be a device certificate installed by default, if you wish to upload your own HTTPS cert, click Install Device Certificate, and follow the provided prompts, please note, that not all third-party HTTPS certs will be applicable for this process. To use the default HTTPS cert, please refer to the information provided below.

Step 1: Click **Download** to download the default HTTPS cert and save it to your computer.
Step 2: Left click on the cert and click **Install Certificate**.
Step 3: Click **Local Machine** and click **Next**.
Step 4: Click the **Place all certificates in the following store** option and select **Browse**.
Step 5: Select the **Trusted Root Certification Authorities** folder and click **OK**. Click Next.



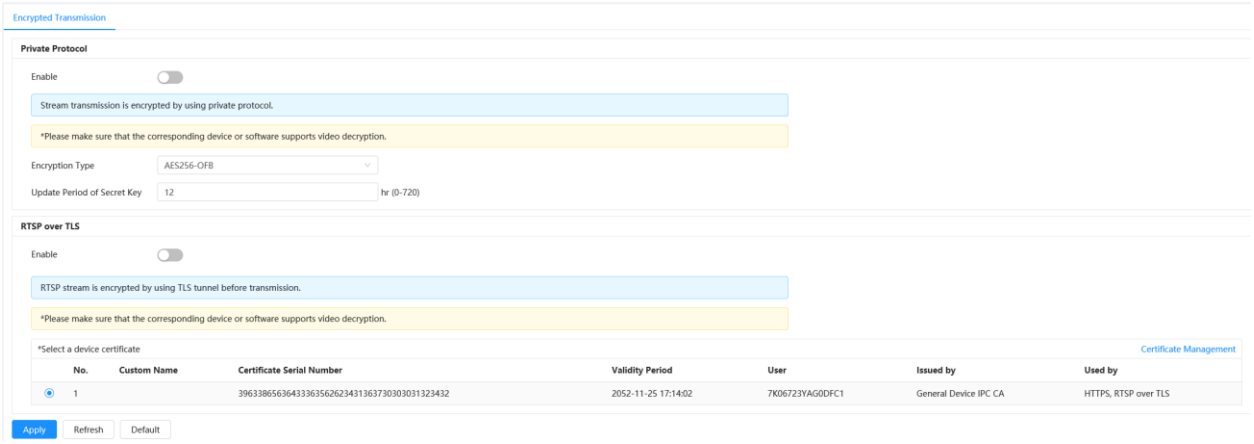
Step 6: Click **Finish**.
Step 7: In the web user interface of the camera, go to **Network** and access the **HTTPS** menu and **Enable** the function. Click **Apply**. The browser will automatically reset, and you will now be accessing the IP using HTTPS.

Trusted CA Certificates

A trusted CA certificate is used to verify the legal status of a host. For example, a switch CA certificate shall be installed for 802.1x authentication. If you would like to use these sources, click download and follow the same installation process as previously provided for device certifications.

A/V Encryption

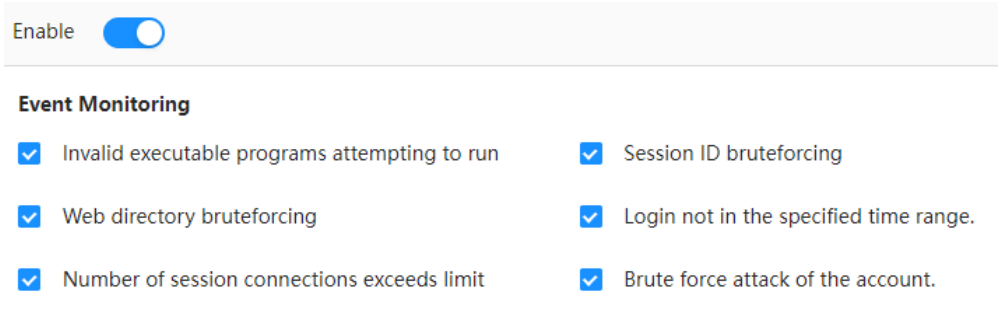
The device supports audio and video encryption. This option will be disabled by default however is recommended as the stream can be transmitted by using a private protocol. An RTSP stream can also be encrypted using a TLS tunnel before transmission. Please note, before enabling these features that the device or software you are using to view the stream supports video decryption.



Click **Apply** to save the settings. To refresh the interface, click **Refresh**. If you need to reset the settings back to default, click **Default.**

Security Warning

The security warning menu allows the user to detect device security statuses in real-time. This helps keep the user informed of any security exception events immediately to avoid any later security risks that may occur. Please note, if email alerts are set up, email notification of the event may be sent using the Event Linkage option and selecting Send Email. Alerts can also be sent using an external alarm output port.

Parameter	Description
Enable	Enable or disable the security feature. Once enabled, choose the specific event monitoring options you would like to apply.  **Note:** Security warning can detect device security status in real time, and keep you informed of the security exception events immediately, so that you can deal with them timely and avoid security risks.
Event Linkage	Use this option to enable an email to be sent if the feature is triggered.
Alarm-out Port	Enable or disable an alarm to trigger an external alarm (if applicable).
Alarm Channel	Choose alarm channel 1 or alarm channel 2 to be triggered.
Post-alarm	The amount of time the event will be end after it is triggered.

Click **Apply** to save the settings. To refresh the interface, click **Refresh**. If you need to reset the settings back to default, click **Default.**

Update

The update menu allows you to manually upgrade firmware directly into the interface. The latest firmware for your device can be found at amcrest.com/firmware.



To update firmware, download the .bin file from the amcrest firmware downloads page. Click Browse and locate the .bin file. Click Update and allow the firmware to upgrade. The browser will restart after the upgrade is complete.

Settings

To access additional settings, click on the settings icon. In this menu you can access the record path, network, storage, and log menus.

Path

The path menu allows the user to set a storage path for both recording and snapshot events. Below is a description of the features provided in this menu. **Requires a plugin to function.**

Parameter	Description
Live Record	Click Browser to set a storage path for manual live view recordings.
Playback Download	Click Browse to set a storage path for recordings downloaded from playback.
Video Clip	Click Browse to set a storage path for clipped videos.
Live Snapshot	Click Browse to set a storage path for manual snapshots from live view.
Playback Snapshot	Click Browse to set a storage path for snapshots stored in the playback menu.

Click **Apply** to save the settings. To refresh the interface, click **Refresh**. If you need to reset the settings back to default, click **Default.**

Network

The network menu allows the user to modify and configure network settings associated with the camera. These settings include TCP/IP settings, P2P, DDNS, Email, HTTPS, etc.

TCP/IP

The TCP/IP menu allows the user to set a static IP, view P2P status, as well as configure RTMP if needed. Below is a description of the features provided in this menu.

Parameter	Description
Host Name	The default name of the device is IPC, however can be modified.
ARP/Ping	Allows the IP address of the camera to be configured using ARP/ping commands.
NIC	Network Interface Card: Wired (Default) – Ethernet connection
Mode	Static vs DHCP: These radio buttons allow the user to choose between a static IP address, and a dynamic IP address. DHCP stands for Dynamic Host Configuration Protocol, and this enables the camera to automatically obtain an IP address from another network device such as a server or more commonly, a router. When the DHCP function is enabled, the user cannot modify the IP address, Subnet Mask, or Default Gateway, as these values are obtained from the DHCP function. To view the current IP address, DHCP needs to be disabled
Mac Address	Displays the MAC address of the device.
IP Version	Switch between IPv4 and IPv6 IP versions.
IP address	The current IP address of the camera.
Sub Mask	Displays the current sub mask of the gateway.
Default Gateway	Displays the current address format of the current gateway.
Preferred DNS	IP address of the preferred DNS.
Alternate DNS	IP address of the alternate DNS.

Click **Apply** to save the settings. To refresh the interface, click **Refresh**. If you need to reset the settings back to default, click **Default.**

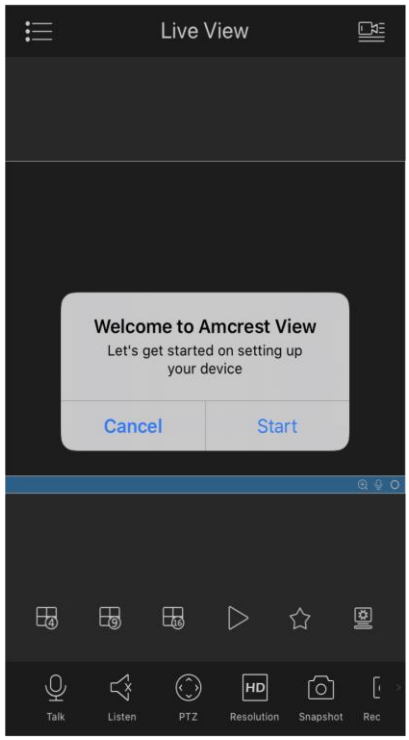
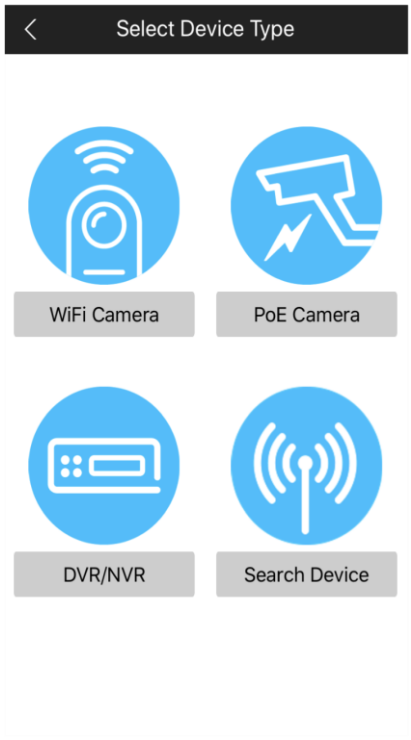
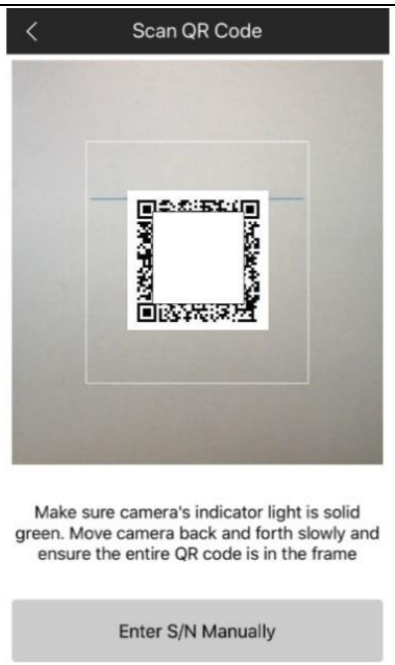
P2P

This feature will be enabled by default, use the provided QR code to add your camera to the Amcrest View app, Amcrest Cloud, AmcrestView.com, etc. If the QR code is unable to be used, the camera's serial number can be used to connect the device using P2P. Please note, this option will be enabled by default. After enabling the function and connecting to the Internet, we will collect device information such as IP address, MAC address, name, and serial number. The collected information is only used for remote access to the device. If you do not agree to enable the function, please cancel the selection of the check box.

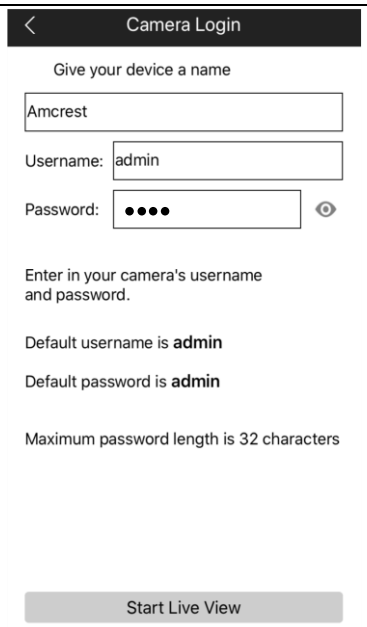
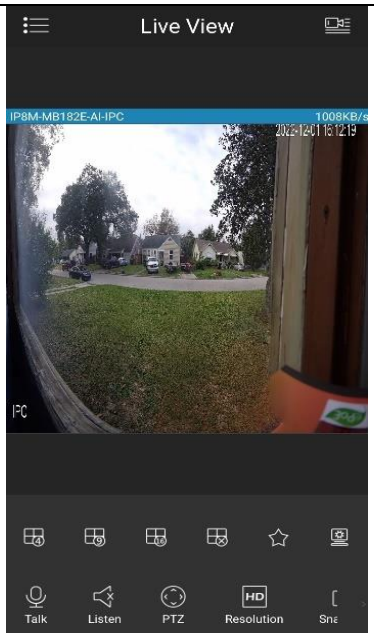
Click **Apply** to save the settings. To refresh the interface, click **Refresh**. If you need to reset the settings back to default, click **Default.**

Amcrest View Pro

After the app has been successfully downloaded to your mobile device, open the app and follow the instructions below to add the camera.

<table>
<tr>
<td>
</td>
<td>
</td>
</tr>
<tr>
<td>3. Tap “Start”.</td>
<td>4. Tap “POE Camera”.</td>
</tr>
<tr>
<td>
</td>
<td>
</td>
</tr>
<tr>
<td>5. Tap “P2P Connection”.

Note: IP/Domain/DDNS can be used to establish a DDNS connection. For more information on how to setup a DDNS connection, visit amcrest.com/support</td>
<td>6. Scan the QR code or enter the serial number of the device manually if the device’s QR code is not available.</td>
</tr>
</table>

	
7. Create a name for the device and enter a username and password. The default username and password will be admin. Tap **Start Live View**.	8. Update the default password for the device and tap **"Start Live View"** to view the device.

RTMP

The RTMP menu allows the user to stream live video to platforms such as YouTube which support RTMP streaming. Below is a description of the features provided in this menu.

Parameter	Description
Enable	Enable or disable RTMP streaming
Stream Type	Choose to stream the mainstream, sub stream1, and sub stream2
Address Type	Choose between a non-custom or custom RTMP address.
Encryption	Enable or disable RTMP stream encryption.
IP Address	Enter a RTMP IP address (if applicable).
Port	RTMP port number (default port number is 1935).
Custom address	Enter a custom address if using a custom address type. For example, if streaming to YouTube a custom address would be, "Stream URL/Stream key".

Click **Apply** to save the settings. To refresh the interface, click **Refresh**. If you need to reset the settings back to default, click **Default.**

Connection

The connection menu allows users to configure port connections associated with the camera. Below is a description of the features provided in this menu.

Parameter	Description
Max Connection	Allows the user to specify the maximum number of users that can be connected to the camera at the same time. The maximum number of users the camera can support at one time is 20.
TCP Port	This field designates the Transmission Control Protocol (TCP) port number. The default value is 37777.
UDP Port	This field designates the User Datagram Protocol (UDP) port number. The default value is 37778.
HTTP Port	This field designates the Hypertext Transfer Protocol (HTTP) port number. The default value is 80.
RTSP Port	This field designates the Real Time Streaming Protocol (RTSP) port number. The default value is 554.
HTTPS Port	This field designates the Hypertext Transfer Protocol Secure (HTTPS) port number. The default value is 443.

Click **Apply** to save the settings. To refresh the interface, click **Refresh**. If you need to reset the settings back to default, click **Default.**

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 AMCRESTDDNS, NO-IP DDNS, and Dyndns DDNS. Based on which service is selected, different options may show on this screen. For the purposes of this guide, AmcrestDDNS will be used. AmcrestDDNS is a free DDNS service provided by Amcrest, and it must be renewed every year.

Parameter	Description
Type	Use the dropdown menu to select a DDNS protocol. (NO-IP DDNS, AmcrestDDNS, Dyndns DDNS).
Server Address	The DDNS server's IP address format.
Domain Name	Enter a domain name for the DDNS address. Click Test to make sure it is available
Username	Enter the username of the DDNS server.
Password	Enter the password of the DDNS server.
Interval	The update cycle of the connection between the device and the DDNS server.

Click **Apply** to save the settings. To refresh the interface, click **Refresh**. If you need to reset the settings back to default, click **Default.**

Email

This menu allows the user to configure email settings to allow email notifications to be sent once a rule or feature that supports email alerts is triggered. Below is a description of the features provided in this menu.

Parameter	Description
Email Provider	Select an Email provider (Gmail will be the default provider).
Enable	Enable or disable email notifications
SMTP Server	The SMTP server protocol (smtp.gmail.com will be default).
Encryption Type	Choose between TLS or SSL encryption types.
Port	The port number of the encryption type used (TLS (587), SSL (465).
Anonymous	Enable or disable anonymous login.
Username	The email address that is being used to send email notifications.
Password	The password or generated app password. Please note, if using Gmail a generated password will be needed to allow email alerts to come through to your account. Please ensure 2 factor authentication is enabled on your email account and enter a generated password. To get a generated password from Gmail, please refer to the steps below: **Step 1:** Open Gmail and click on the account avatar/picture. **Step 2:** Click on **Manage Your Google Account** and click on **Security**. **Step 3:** Select App passwords. **Step 4:** Enter the password for your email and click Next. **Step 5:** Select an option from the provided dropdown menu and select Custom. Enter a name for the authentication and click Generate. **Step 6:** Enter the provided security password into the Password field located in the camera's interface.
Sender	The email address of the sender, this should be the same as the email address used in the username field.
Encryption Type	Select whether to use TLS or SSL encryption. This should match the previous encryption type menu.
Subject	The subject line of the email notification. Click on the "+" icon to choose whether this will display the device name, IP address, or event type. Click the Attachment icon to allow snapshots.
Receiver	The email address that will be used to receive the email notifications.
Health Mail	Allows the camera to send a test email to check the connectivity of the device.
Sending Interval	The amount of time in which a health email will be sent. The default is 60 minutes, however, can be modified from 30 – 1440 minutes.

Click **Apply** to save the settings. To refresh the interface, click **Refresh**. If you need to reset the settings back to default, click **Default.**

UPnP

UPnP stands for Universal Plug and Play, is a protocol that establishes mapping relations between a local area and wide area networks. This function enables the user to access a local area device through a wide area IP address. Below is a description of the features provided in this menu.

Parameter	Description
Enable	Enable or disable UPnP.
Enable Device Discovery	Enable or disable the ability to automatically discover the device on the network.

Router Status	Displays the current status of the mapping process.
Mode	Use the dropdown menu to select between a custom or default mapping mode.
Interface	Displays the HTTP, TCP, UDP, RTSP, HTTPS internal and external port status. Use the enable/disable toggle switch to enable or disable a specific protocol. Use the modify icon to edit the external port of a selected protocol.

Click **Apply** to save the settings. To refresh the interface, click **Refresh**. If you need to reset the settings back to default, click **Default.**

Basic Services

This menu allows the user to enable or disable IP hosts (devices with IP addresses) that are allowed to access the device. The options available in this menu are used to enhance network and data security. Please note, that only trusted site hosts will be allowed to access or log into the device's web interface.

Parameter	Description
Multicast/Broadcast Search	Enable or disable this function if multiple users are viewing the device simultaneously through the network using a multicast/broadcast protocol.
CGI, ONVIF, or Genetec	Enable or disable these functions to provide access to these protocols.
Mobile Push Notifications	Enable or disable push notifications from the device to occur.
Private Protocol	Enable or disable private protocol authentication.
Private Protocol Authentication Mode	Use the dropdown menu to select whether a private protocol is authenticated using security mode (recommended) or a compatible mode.
Online Log Backup	Enable or disable an online log to backup the camera's log.
TLSv1.1	Enable or disable the camera to be compatible with browsers that support TLSv1.1

Click **Apply** to save the settings. To refresh the interface, click **Refresh**. If you need to reset the settings back to default, click **Default.**

HTTPS

This menu allows the user to create or upload an authenticated certificate to allow the user to log into the device through a secure HTTPS IP address. For more information on how to set up HTTPS please refer to the Device Certificate section of this document. Below is a description of the features provided in this menu.

Parameter	Description
Enable	Enable or disable HTTPS service. Please note that HTTPS is a service entry based on Transport Layer Security (TLS). HTTPS provides web service, ONVIF access service, and RTSP access service.
Compatible with TLSv1.1 and earlier versions	Enable or disable the cert to be compatible with browsers that support TLSv1.1 or earlier TLS versions. Please note that there may be security risks if TLS of earlier versions is enabled.
Interface	Displays all current certificates associated with this device. Please note that it is recommended to use the default HTTPS cert provided in the device.
Certificate Management	Provides quick access to the Device Certificate menu. This allows you to edit and manage all certs related to HTTPS on this device.

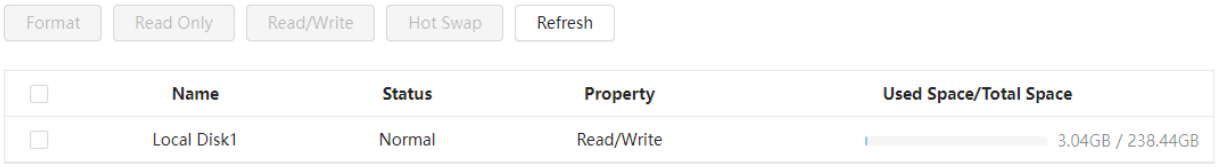
Click **Apply** to save the settings. To refresh the interface, click **Refresh**. If you need to reset the settings back to default, click **Default.** Click Download Root Certificate to store the root certificate on your computer.

Storage

The storage menu allows the user to view and modify storage options and settings such as local storage, FTP, and NAS settings.

Storage

This menu allows the user to view the status as well as used/total space available on an inserted microSD card. The features in this menu also allow you to format the microSD card, as well as set read/write permissions.



Storage Setting

This menu allows the user to manage and control storage settings as well as change the storage methods of the camera. Below is a description of the features provided in this menu.

Storage

Parameter	Description
Event Type	Choose which record types will be sent to a selected storage method. **General:** Continuous (24/7) record types **Motion:** Motion Detection record types **Alarm:** External alarm record types.
Disk Full	When a storage method is full, choose if the old data will be overwritten or if the camera will stop recording when its full.
Storage Method	Use this dropdown menu to choose a storage method. FTP: Set the camera to store events in an FTP or SFTP server. NAS: Set the camera to store events to a designated NAS server.

Click **Apply** to save the settings. To refresh the interface, click **Refresh**. If you need to reset the settings back to default, click **Default.**

Record Control

This menu allows the user to set general record options for the device. Below is a description of the features provided in this menu.

Parameter	Description
Max Duration	The time used for packing video files

Pre-Record	The amount of time that will be displayed before the detected event occurs.
Record Mode	Set the device to record automatically or manually. The record mode can be set to off as well if the recording is not applicable.
Record Stream	Set the device to record the mainstream, or sub-streams by default.

Click **Apply** to save the settings. To refresh the interface, click **Refresh**. If you need to reset the settings back to default, click **Default.**

Schedule

The schedule menu allows the user to set a recording schedule which will provide the camera with a way to only retain recordings during specific days or times. Use the mouse to modify recording schedules if needed for each day and time applicable.



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

Event Type: These checkboxes allow the user to select which record type they want to configure on the schedule. There are 3 types of snapshots:

General: General means that the camera will record during the specified time. A general recording is represented by green.

Motion: Motion Detection means that the camera only records when the motion detection alarm is activated. Motion recording is represented by yellow.

Alarm: Alarm means that the camera only records when an alarm is activated. Alarm recording is represented by the color red.
Copy: Clicking this button opens a screen that allows periods to be set for each day and for each record type. There are a total of 6 periods that can be set.
Holiday: Provides a way to specify which days the schedule will not apply. To set a holiday, click the Holiday button and select Enable. On the calendar, select the dates in which the schedule will not apply and click OK. A separate holiday schedule can be applied, if a schedule is needed use your mouse to set the time & specified rule types.
Click **Apply**.

Click **Apply** to save the settings. To refresh the interface, click **Refresh**. If you need to reset the settings back to default, click **Default.**

Log

The log menu allows users to view and back up local and remote logs. . Below is a description of the features provided in this menu.

Parameter	Description
Start time	Click this option and use the provided calendar to enter a start and end date of the log.
Type	Use this option to select a log type. If you would like all types to apply, select All.
Search	Click Search to view admin and system logs.
Interface	View the time, username, and type of log detected. Click the Details option to view log contents including the address and web type.
Backup	Click this option to download a text file of all logs to your computer.

Remote Log

The remote log menu allows the user to configure a remote log to access related logs by accessing a set IP address. Below is a description of the features provided in this menu.

Parameter	Description
Enable	Enable or disable a remote log.
Server Address	Enter the server IP address for the remote log.
Port	Enter the port number of the server IP.
Device No.	Enter the device number, the default device number is 22.

Click **Apply** to save the settings. To refresh the interface, click **Refresh**. If you need to reset the settings back to default, click **Default.**

Logout

To log out of the interface, click on the  icon and select logout. If you would like to restart the camera, select **Restart.**

FCC Statement

1. This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.
2. The user's manual or instruction manual for an intentional or unintentional radiator shall caution the user that changes, or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment. In cases where the manual is provided only in a form other than paper, such as on a computer disk or over the Internet, the information required by this section may be included in the manual in that alternative form, provided the user can reasonably be expected to have the capability to access information in that form.
3. (b) For a Class B digital device or peripheral, the instructions furnished the user shall include the following or similar statement, placed in a prominent location in the text of the manual: NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or

television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures: -- Reorient or relocate the receiving antenna. -- Increase the separation between the equipment and receiver. -- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected. -- Consult the dealer or an experienced radio/TV technician for help.
4. RF exposure warning This equipment must be installed and operated in accordance with provided instructions and the antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.

End-users and installers must be provided with antenna installation instructions and transmitter operating conditions for satisfying RF exposure compliance.

IC Warning Statement

This device complies with Industry Canada's license-exempt RSSs. Operation is subject to the following two conditions: (1) This device may not cause interference; and (2) This device must accept any interference, including interference that may cause undesired operation of the device. Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement. This equipment complies with IC RSS-102 radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20cm between the radiator and any part of your body. Pour se conformer aux exigences de conformité CNR 102 RF exposition, une distance de séparation d'au moins 20 cm doit être maintenue entre l'antenne de cet appareil ettoutes les personnes.

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(Case)	O	O	O	O	O	O
Plastic Parts (Panel)	O	O	O	O	O	O

Circuit Board	O	O	O	O	O	O
Fastener	O	O	O	O	O	O
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 substances 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 kinds of substances or elements, please return to the corresponding local authorities to process according to your local government statutes.

Note:
To view setup videos for many of the steps outlined in this guide, go to http://amcrest.com/videos
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.

To contact Amcrest support, please do one of the following:

Visit https://amcrest.com/contact and use the email form.
Call Amcrest Support using one of the following numbers:
Toll Free US: (888) 212-7538
International Callers (Outside of US): +1-713-893-8956
USA: 713-893-8956
Canada: 437-888-0177
UK: 203-769-2757