5MP POE Outdoor Security Turret Camera
User Manual

Version 1.0.0

Contents

Overview 3
Installation Guide 3
Camera Setup 4
AMLINK Pro App Setup 4
Web User Interface Setup 6
Live View 6
Storage 7
AI 13
Settings 16
System 17
Network 22
Video/Audio 28
Camera 31
Event 35
Storage 39

Welcome

Thank you for purchasing an AMLINK camera!

This user manual is designed to be a reference tool for the installation and operation of your camera.
Here you can find information about the camera's features, functions, and information to aid in troubleshooting.

For any additional information or how to contact us please visit: https://amlinksecurity.com/pages/contact

Important Security Warning

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

Overview

This 5MP security camera delivers stunning ultra-high-definition video in 5-megapixel resolution, at 20 frames per second. It features a fixed 2.8mm lens that provides a wide field of view to cover more area. 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 LEDs to achieve color night vision, and a smart light mode which allows the camera to activate the white light LEDs at night if an event is detected.

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 human/vehicle detection, which allows the camera to detect only human and vehicles in the area. The camera also features flexible storage options to store recordings to a microSD card (up to 256GB), SFTP/FTP, NAS, NVR, or using the AMLINK Cloud. All these features can be accessed and customized using a web browser or using the AMLINK Pro app on your 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 and remove the **Reset** cover on the camera. This area will provide access to the factory reset button as well as the microSD card slot.
2. Locate the microSD card slot and insert the microSD card into the slot.
3. Gently press in to secure the card.
4. Place the cover back onto the camera and secure it.

Physical Installation

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, drill the holes and insert the wall anchors.
2. Use the provided L-wrench to remove the bottom mounting plate.
3. Run wires of the camera through the mounting plate and align the mounting holes of the plate to the holes on the sticker surface.
4. Place a microSD card into the camera if needed and secure the microSD/Reset hatch back onto the camera.
5. Place the housing of the camera body back onto the camera and use the L-wrench to secure.
6. Move and adjust the angle of the camera manually and tighten the screw to secure.

Camera Setup

This section will provide information on how to set up and access your camera through the following methods:

AMLINK Pro app (iOS and Android)
Web User Interface Setup

AMLINK Pro App Setup

AMLINK cameras can be accessed on your mobile device using the AMLINK Pro app. This app is available in both the App Store and Google Play store.

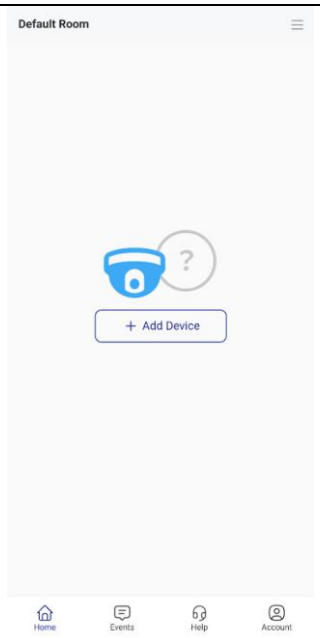
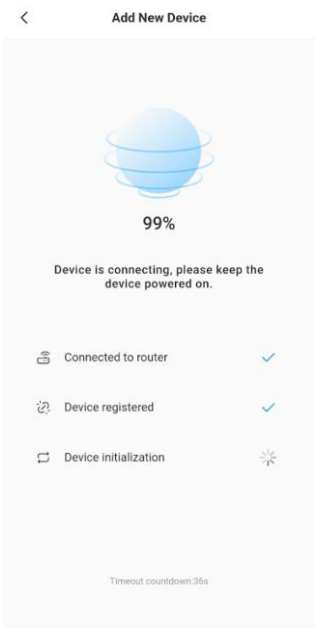
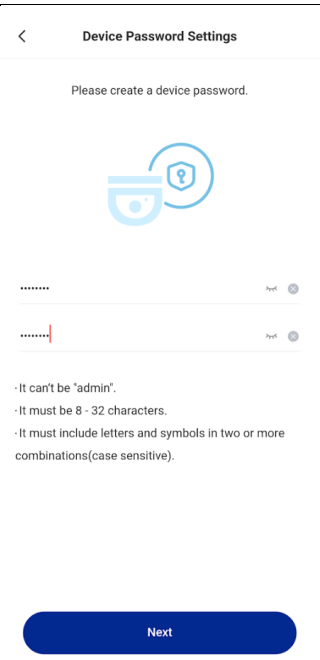
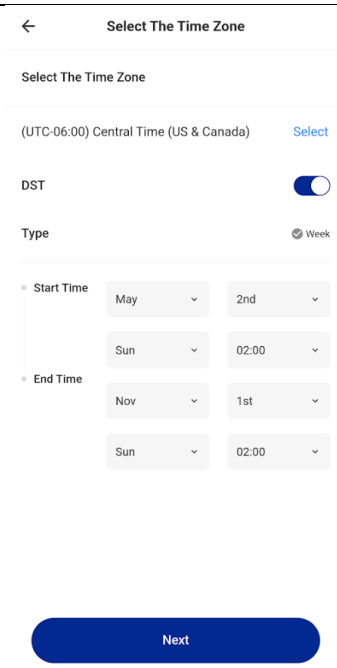
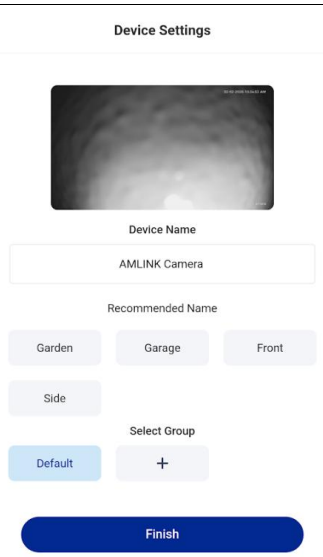
Registering An AMLINK Account

An AMLINK account will need to be created to begin adding devices. An email address and password will be required to create an account in the AMLINK app.

1. Tap **Create Account**.
2. Enter your email address and tap Get **Verification Code**. The app will send a verification code email to the provided email address.
3. Enter the verification code into the app and create a password for your account. Click **Finish**.

Adding a Camera

Before adding your camera, please make sure the device is connected to the same network as your mobile device. The camera should be receiving both power and data from the POE connection on your network using an Ethernet cable.

		
1. Open the app and log into your AMLINK account. Tap the "**+**" icon or "**+ Add Device**".	2. Select your camera from the **Add New Device** list and scan the QR code located on your device. Note: The serial number can be entered manually by tapping **Enter the SN manually**.	3. Allow the device to connect, register, and initialize
		
4. Enter a password for your device and confirm the password. Tap Next.	5. Select any time zone, daylight savings, or other info. Tap **Next**.	6. Enter a name for your device and tap **Finish**.

For more information about AMLINK Pro and its functionalities visit: https://amlinksecurity.com/support

AMLINK Cloud Storage Setup

A cloud storage plan can be used which provides a premium cloud storage option for your recordings. This is an optional service provided by AMLINK that can be applied per device using the AMLINK Pro app. To sign up for an AMLINK cloud storage plan, tap the cloud icon associated with your device, select a storage plan, and complete the in-app sign-up process.

For more information on the AMLINK cloud and its functionalities visit: https://amlinksecurity.com/support

Web User Interface Setup

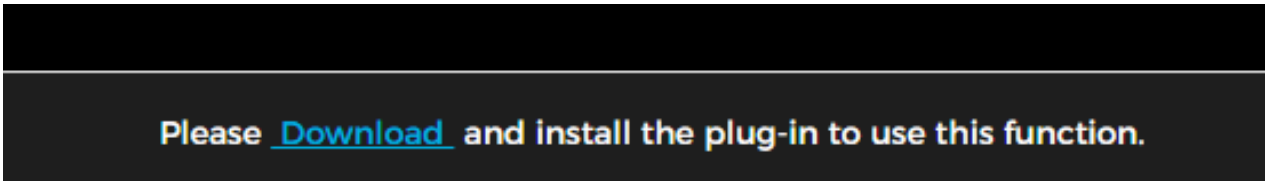
This camera features the latest technology which allows you to access your camera using a wide variety of web browsers including, Google Chrome, Firefox, Safari, or other mainstream browsers using your PC or Mac. For more information on how to access your camera using a web browser please refer to the information below.

First, locate the camera's IP address. To locate the camera's IP address, it is highly recommended to download our free AMLINK IP Config Tool software. For more information about the AMlink IP Config Tool, please visit https://amlinksecurity.com/support

Once the download has been completed installing on your computer, locate the IP address for your device. Open a web browser and enter the IP address to be taken to the device initialization page. Proceed with device initialization if needed. Enter the username and password for your device and click **Login**.

Live View

By default, the interface will open the **Live View** tab. The live view tab allows the user to see the video steam (mainstream or substream) of the camera, adjust image settings, manual snapshot, manual recordings, etc. A plugin is **not** needed; however, it can be installed to use other functions such as file path setting, etc.



Button	Function Name	Function Description
CH1	Mainstream/Substream	Switch between mainstream and substream video streams
Image Adjustment	Image Adjustment	**Brightness**: This slider is used to adjust the brightness of the stream. The value ranges from 0 to 100. The larger the number, the brighter the video. Please note the video may become hazy if the value is too high. **Contrast**: This slider is used to adjust the contrast of the stream. The value ranges from 0 to 100. The larger the number the higher the contrast. 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. **Saturation**: This slider is used to adjust the saturation of the stream. The value ranges from 0 to 100. The larger the number the stronger the color. 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. Please note the video may not be clear if the value is too low. **Hue:** This slider is used to shift the overall color spectrum of the stream. It is a color-correction tool that essentially "rotates" the colors on a standard color wheel to correct color imbalances or to achieve a specific visual look. **Reset:** Resets the image adjustments back to default settings.
	Warning Light	Click this to manually enable or disable the built-in warning light LED.
	Sound Alarm	Click this to manually enable or disable the built-in alarm siren.
	Digital Zoom	Click this option and use your mouse on the interface to digitally zoom in on an area. Click the icon again to exit.
	Snapshot	Click this to manually take a snapshot of the live view. The snapshot will be saved to the default file path for snapshots.
	Manual Record	Click this to manually record video. The video will be saved to the default file path of videos. Please make sure the plugin is installed to download as .mp4 format by default.
	Audio Output	Click this to enable or disable audio output from the camera. This feature allows the user to listen in on the audio the camera's microphone is picking up.
	Two-Way Talk	Click this option to speak and hear audio from the camera.
	W:H	Click this option to set the video feed format to wide or adaptive view.
	AI Rule	Click this option to enable or disable the AI overlays on live view.
	Full Screen	Click this option to set the live view to full screen. Click **Esc** to exit.
	QR Code	Click this to provide quick access to the device's serial number.
	Logout	Click this option to log out of the interface.
	Full Screen	Click this option to set the interface to full screen, click again to return to its original format.

Storage

The **Storage** tab allows the user to access storage settings related to FTP & NAS only. **Please use the AMLINK Pro mobile app to view playback or set recording schedules for microSD (local recording).** For more information on the AMLINK pro app, please visit amlinksecurity.com/support.

Video

This menu allows the user to set video recording, storage, and schedule settings for an FTP or NAS.

Recording Settings

The **Recording Settings** menu allows the user to set general video recording settings for an FTP or NAS storage path.

Max Duration: The maximum amount of time of a video recording.
Pre-Record: The amount of video footage from the moments **before** a recording is triggered by an event.

Full Disk: Set the camera to overwrite old video files or stop recording entirely after storage is full
Recording Stream: Set the camera to record either the mainstream or sub stream.

To save the settings, click the **Apply** button. To refresh the page, click the **Refresh** button. To reset to default settings, click the **Default** button.

Storage

The **Storage** menu allows the user to set video file storage paths to an FTP or NAS.

FTP: Allows the recordings to be stored to a SFTP or FTP server.
NAS: Allows the recordings to be stored to a NAS (if applicable).

Note: Only one network storage service can be enabled on the device at the same time, the configuration will be modified synchronously under video and pictures.

Setting Up SFTP or FTP

The FTP or SFTP option allows the camera to "push" files, specifically video clips and image snapshots, to a remote server. By default, the camera will be set to SFTP, however, it can be modified if needed.

Mode: Select between an SFTP or FTP protocol.
Enable: Enable the protocol.
Server Address: Enter the IP address of the SFTP or FTP server.
Port: Enter the port number of the SFTP or FTP server. SFTP port will be 22, FTP port will be 21.
Username: Enter the username of the SFTP or FTP server.
Password: Enter the password associated with the SFTP or FTP server.
Storage Directory: Enter the directory's information in which the events will be stored.
Directory Structure: These options are used to keep the large volume of files organized and easy to navigate.
- **Level 1 Directory:** Set as device name, device IP, or automatic (custom title).
- **Level 2 Directory:** Set as Date, File Type, or Channel No.
- **Level 3 Directory:** Set as File Type_Channel No., File Type, Date, or Channel No.

Test: Test the connection of camera to the SFTP or FTP server after all settings are applied.

To save the settings, click the **Apply** button. To refresh the page, click the **Refresh** button. To reset to default settings, click the **Default** button.

NAS

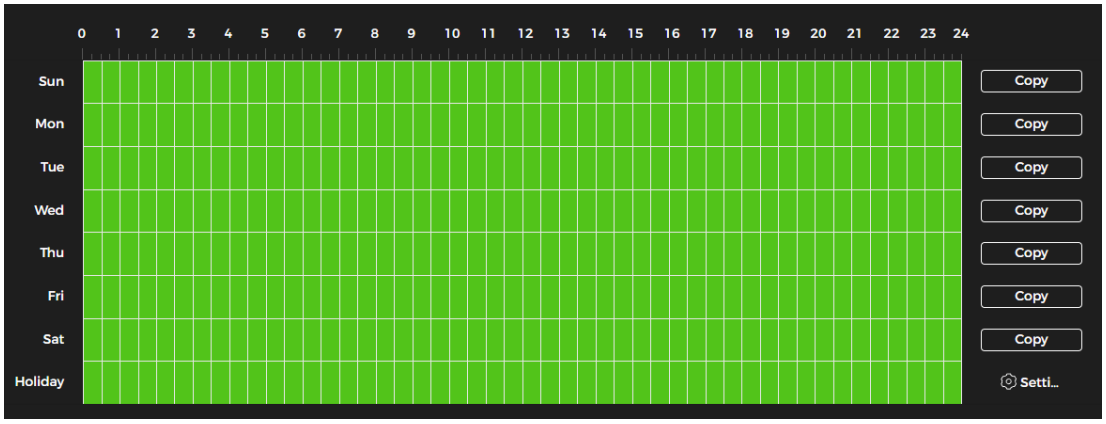
The **NAS** option allows the camera to record videos and save snapshots directly to a server or storage device on your network **without needing an NVR**. This turns your camera into a standalone recording system. It is essentially the "serverless" version of the NVR feature.

Enable: Enable the NAS protocol.
Server Address: Enter the server address of the NAS.
Remote Directory: Enter the directory information in which the events will be stored.

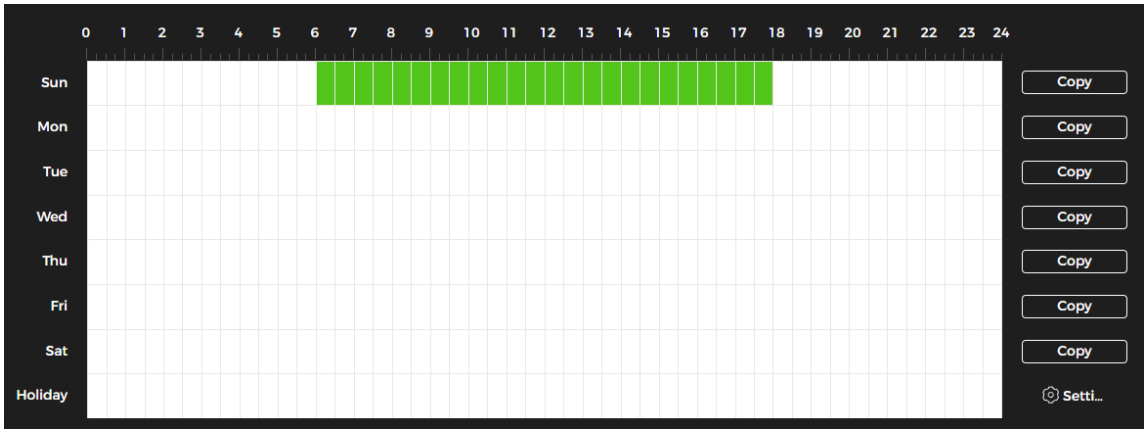
To save the settings, click the **Apply** button. To refresh the page, click the **Refresh** button. To reset to default settings, click the **Default** button.

Schedule

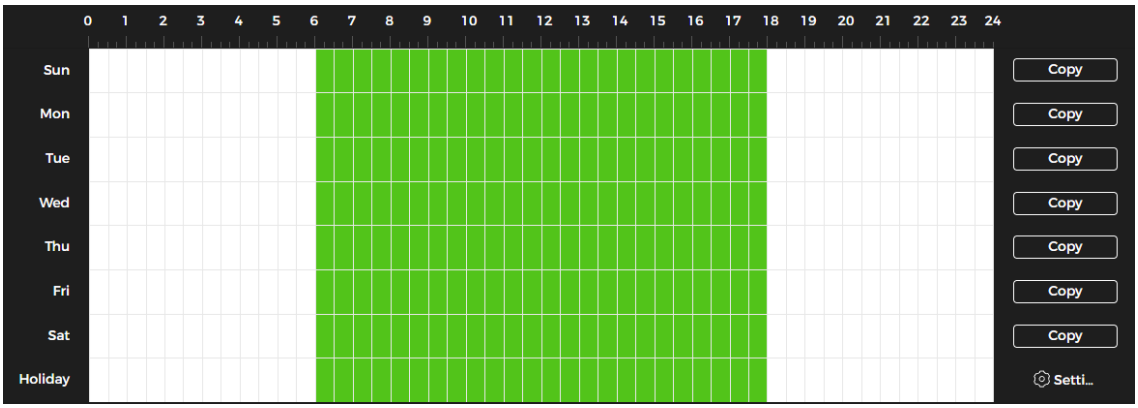
The **Schedule** menu allows you to manage the recording schedules for the camera. This includes all recording types (24/7 recordings) or event only recording types. By default, it will be set to continuously record.



To set a recording schedule, select an event type (all type or event only) and use your mouse on the interface to set the recording schedule. For instance, if you want the camera to only record on Sunday between 6am and 6pm, click the **Clear** option and use your mouse to set the schedule from 6 – 18 (6am – 6pm), Mon – Fri, and click **Apply**.



If you want the schedule to apply to all or multiple days of the week, click the **Copy** option next to the schedule just made and select which days you would like the schedule to apply to and click Apply to set the schedule.



Holiday

The **Holiday** option is a scheduling tool that allows you to set a specific recording or alarm behavior for certain dates that differ from your normal weekly routine. Essentially, it prevents your "Business Hours" schedule from running on days when you are not home or out of town.

To access the holiday settings, click the settings gear wheel icon( ) next to the “Holiday” column of the schedule and enable the holiday option. Select the start and end time of the holiday schedule in the provided calendar and click **OK**. This will set the camera to your holiday schedule.

To save the settings, click the **Apply** button. To refresh the page, click the **Refresh** button. To reset to default settings, click the **Default** button.

Snapshot Settings

The **Snapshot Settings** menu allows the user to set general snapshot settings such as the type, size, quality of snapshots, etc.

Type: Allows the user to select whether the settings will apply continuous (24/7) or event only snapshots.
Size: Determines the physical dimensions of the snapshot in pixels (resolution).
Quality: Determines the compression level and how much detail is preserved within the pixels of the snapshot versus how much the file is shrunk to save space. It can be set to low, medium, and high.
Full Disk: Set the camera to overwrite old snapshot files or stop after the storage path is full.
Recording Stream: Set the camera to record either the mainstream or sub stream.

To save the settings, click the **Apply** button. To refresh the page, click the **Refresh** button. To reset default settings, click the **Default** button.

Storage

The **Storage** menu allows the user to set snapshot file storage paths to an FTP or NAS.

FTP: Allows the recordings to be stored to a SFTP or FTP server.
NAS: Allows the recordings to be stored to a NAS (if applicable).

Note: Only one network storage service can be enabled on the device at the same time, the configuration will be modified synchronously under video and snapshots.

Setting Up SFTP or FTP

The FTP or SFTP option allows the camera to "push" files to a remote server. By default, the camera will be set to SFTP, however, it can be modified if needed.

Mode: Select between an SFTP or FTP protocol.
Enable: Enable the protocol.
Server Address: Enter the IP address of the SFTP or FTP server.
Port: Enter the port number of the SFTP or FTP server. SFTP port will be 22, FTP port will be 21.
Username: Enter the username of the SFTP or FTP server.
Password: Enter the password associated with the SFTP or FTP server.
Storage Directory: Enter the directory’s information in which the events will be stored.
Directory Structure: These options are used to keep the large volume of files organized and easy to navigate.

Level 1 Directory: Set as device name, device IP, or automatic (custom title).

Level 2 Directory: Set as Date, File Type, or Channel No.

Level 3 Directory: Set as File Type_Channel No., File Type, Date, or Channel No.

Customized Picture Name: Allows the user to define a specific naming convention for snapshots generated by the camera. For instance, **Default Name:** 20260210_084512_01.jpg, **Custom Name (e.g., "Front_Gate"):** Front_Gate_20260210_084512.jpg

Channel No.: Displays the channel number in the customized title.

Date & Time: Displays the date and time of the event in the customized title.

ms: Adds a three-digit millisecond value to the end of the customized title.

Device Name: Displays the name of the device in the customized title.

IP Address: Displays the IP address of the device in the customized title.

Snapshot Mode: Displays which modes were used (motion, schedule, manual etc.) captured the event.

Automatic: Tells the camera to name each file using its own pre-set identity (like the camera's name) followed by the exact date and time it was taken.

Test: Test the connection between the camera and the SFTP or FTP server.

To save the settings, click the **Apply** button. To refresh the page, click the **Refresh** button. To reset to default settings, click the **Default** button.

NAS

The **NAS** option allows the camera to save snapshots directly to a server or storage device on your network **without needing an NVR**. This turns your camera into a standalone recording system. It is essentially the "serverless" version of the NVR feature.

Enable: Enable the NAS protocol.

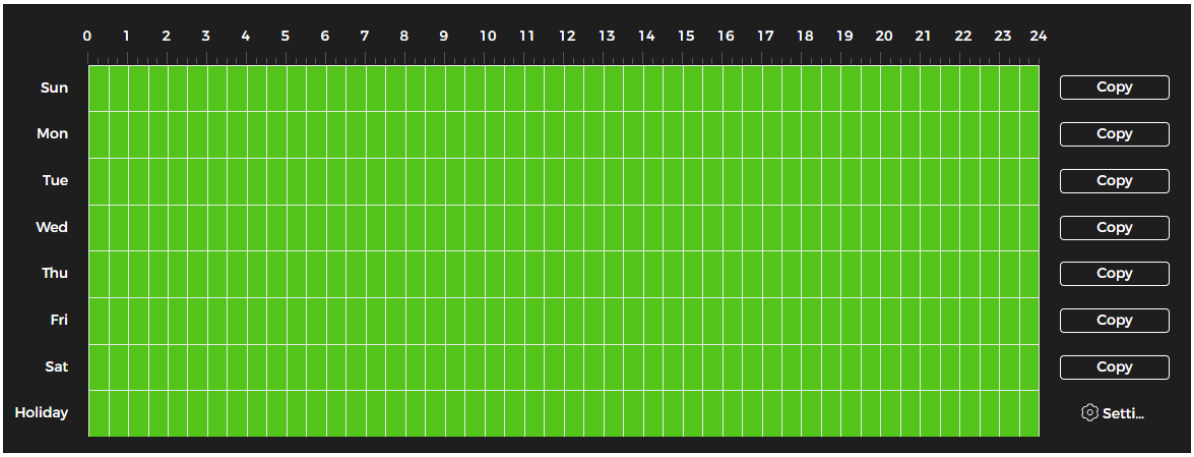
Server Address: Enter the server address of the NAS.

Remote Directory: Enter the directory information in which the events will be stored.

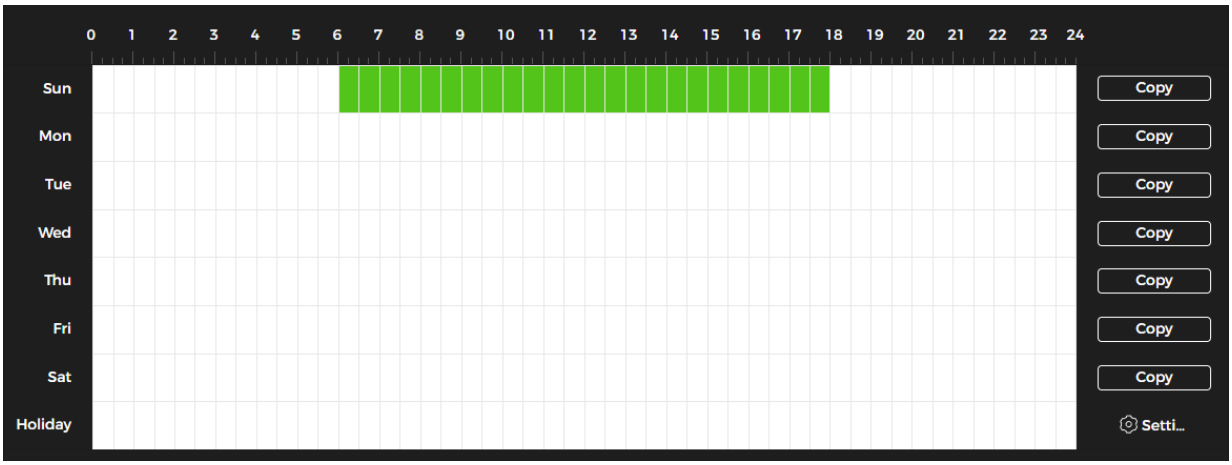
To save the settings, click the **Apply** button. To refresh the page, click the **Refresh** button. To reset to default settings, click the **Default** button.

Schedule

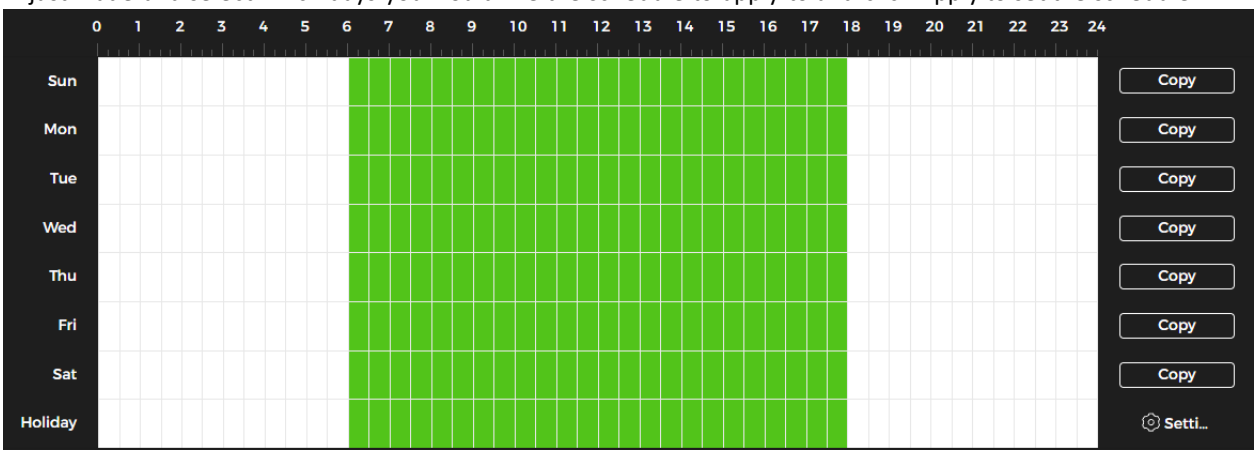
The **Schedule** menu allows you to manage snapshot schedules for the camera. This includes all snapshot types including 24/7 or event. By default, it will be set to continuously monitor.



To set a schedule, select an event type (all type or event only) and use your mouse on the interface to set the schedule. For instance, if you want the camera to only be active on Sunday between 6am and 6pm, click the **Clear** option and use your mouse to set the schedule from 6 – 18 (6am – 6pm), Mon – Fri, and click **Apply**.



If you want the schedule to apply to all or multiple days of the week, click the **Copy** option next to the schedule just made and select which days you would like the schedule to apply to and click Apply to set the schedule.



Holiday

The **Holiday** option is a scheduling tool that allows you to set a specific recording or alarm behavior for certain dates that differ from your normal weekly routine. Essentially, it prevents your "Business Hours" schedule from running on days when you are not home or out of town.

To access the holiday settings, click the settings gear wheel icon( ) next to the "Holiday" column of the schedule and enable the holiday option. Select the start and end time of the holiday schedule in the provided calendar and click **OK**. This will set the camera to your holiday schedule.

To save the settings, click the **Apply** button. To refresh the page, click the **Refresh** button. To reset to default settings, click the **Default** button.

AI

The **AI** menu allows the user to configure AI rules for the camera. This includes IVS features such as line crossing and area detection rules. Please note, IVS will conflict with HVD settings, enabling this feature will automatically disable HVD. To begin configuring IVS, please enable the IVS feature in the AI config menu and click **Next**. Select the + icon and choose an AI rule that you would like to configure.

Line Detection

The **Line Detection** menu allows the camera to trigger an event if an object, such as a human or vehicle, crosses the set tripwire line. Use your mouse to set a detection line.



Icon	Description
	Draw or modify a detection line.
	Used to measure and set the number of pixels in the target area.
	Delete a graphic or detection line from the live monitoring screen.
	Sets a minimum size in which an event will be triggered.
	Sets a maximum size in which an event will be triggered.

Enable: Enable or disable the AI rule.

Sensitivity: Set the overall sensitivity of the rule. The higher the sensitivity the more times the rule may be triggered. Use the slider to adjust the sensitivity.

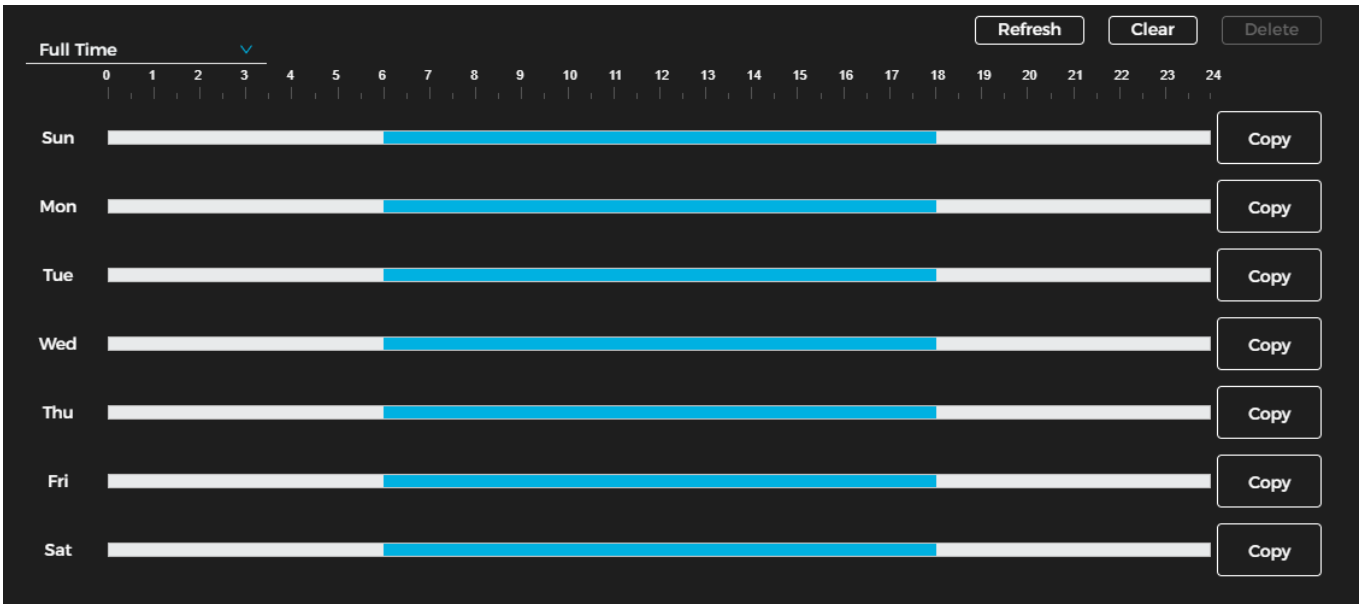
Direction: Set which direction the object will be going for the tripwire to be triggered. It can be set left, right, or in both directions (A<->B).

Object Filter: Allows the camera to be triggered only when a specific object, such as a human or vehicle, is detected. Both checkboxes can be activated at the same time if needed.

Human: This checkbox allows the camera to be triggered only when a human figure is detected.

Motor Vehicle: This checkbox allows the camera to be triggered only when a vehicle has been detected.

Schedule: Allows the user to set a schedule for the rule. Click the settings icon to begin setting the schedule. A full-time schedule will be set by default, however, to set multiple schedules, click the +Schedule option if needed. To set a schedule, click the clear option and use your mouse to set the schedule. For instance, if you want the schedule to only apply between 6am and 6pm, slide the slider between 6 and 18 (6am – 6pm). Click the Copy option to set the schedule to multiple days if needed. Click **Apply** to set the schedule.



Record: This option allows the user to enable the camera to record video when an event is triggered.
Recording Delay: This field specifies, in seconds, how long the delay between events should be. The default is 10 seconds however this can be modified between 10~300 seconds.
Siren: This option allows the user to enable the camera to trigger an audible siren sound once the rule is triggered.
Play Count: The number of times the alarm will play after it is triggered.
Audio File: The alarm sound that will be used once the alarm is triggered.
Warning Light: This option allows the user to enable the camera to trigger the white light LED to turn on once an object has been detected.
Mode: The default mode for the warning light will be set to Flicker, allowing the camera to flash when an event is detected.
Flicker Frequency: The speed of the white light LED flash (low, middle, or high)
Duration: How long will the flash last. Default is 10 seconds however it can range between 5 and 30.
Schedule: Set a schedule in which the flash will apply.
Brightness: Adjust the brightness of the warning light LED.
Send Email: This checkbox allows the user to enable the camera to send an email when an event is triggered.
Snapshot: This checkbox allows a snapshot of the event to be sent to registered email address once triggered.

To save the settings, click the **Apply** button. To refresh the page, click the **Refresh** button. To reset to default settings, click the **Default** button.

Area Detection

The **Area Detection** rule allows the camera to trigger an event if an object, such as a human or vehicle, appears or crosses a set area. Use your mouse to set a detection.



Icon	Description
	Draw or modify a detection area.
	Used to measure and set the number of pixels in the target area.
	Delete a graphic or detection line from the live monitoring screen.
MIN	Sets a minimum size in which an event will be triggered.
MAX	Sets a maximum size in which an event will be triggered.

Enable: Enable or disable the AI rule.

Sensitivity: Set the overall sensitivity of the rule. The higher the sensitivity the more times the rule may be triggered. Use the slider to adjust the sensitivity.

Action: : These checkboxes allow 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.

Inside: The rule will trigger when a target is inside the area (not applicable)

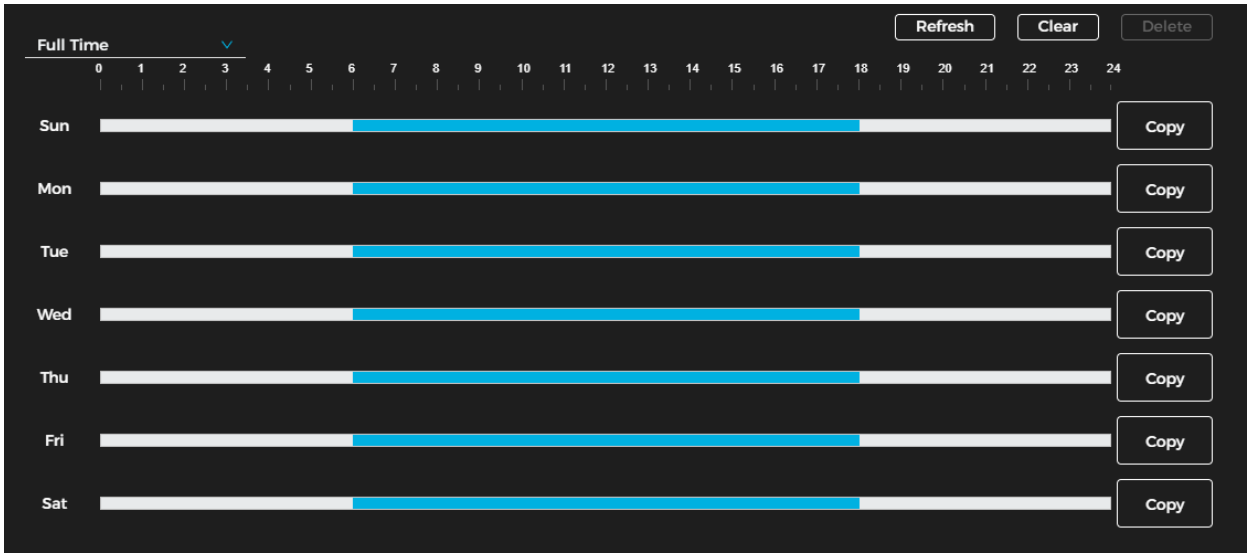
Direction: This dropdown menu allows the user to choose whether the rule will be triggered if an object enters, exits, or enters & exits a set line or area.

Object Filter: Allows the camera to be triggered only when a specific object, such as a human or vehicle, is detected. Both checkboxes can be activated at the same time if needed.

Human: This checkbox allows the camera to be triggered only when a human figure is detected.

Motor Vehicle: This checkbox allows the camera to be triggered only when a vehicle has been detected.

Schedule: Allows the user to set a schedule for the rule. Click the settings icon to begin setting the schedule. A full-time schedule will be set by default, however, to set multiple schedules, click the +Schedule option if needed. To set a schedule, click the clear option and use your mouse to set the schedule. For instance, if you want the schedule to only apply between 6am and 6pm, slide the slider between 6 and 18 (6am – 6pm). Click the Copy option to set the schedule to multiple days if needed. Click **Apply** to set the schedule.



Record: This option allows the user to enable the camera to record video when an event is triggered.
Recording Delay: This field specifies, in seconds, how long the delay between events should be. The default is 10 seconds however this can be modified between 10~300 seconds.
Siren: This option allows the user to enable the camera to trigger an audible siren sound once the rule is triggered.
Play Count: The number of times the alarm will play after it is triggered.
Audio File: The alarm sound that will be used once the alarm is triggered.
Warning Light: This option allows the user to enable the camera to trigger the white light LED to turn on once an object has been detected.
Mode: The default mode for the warning light will be set to Flicker, allowing the camera to flash when an event is detected.
Flicker Frequency: The speed of the white light LED flash (low, middle, or high)
Duration: How long will the flash last. Default is 10 seconds however it can range between 5 and 30.
Schedule: Set a schedule in which the flash will apply.
Brightness: Adjust the brightness of the warning light LED.
Send Email: This checkbox allows the user to enable the camera to send an email when an event is triggered.
Snapshot: This checkbox allows a snapshot of the event to be sent to registered email address once triggered.

To save the settings, click the **Apply** button. To refresh the page, click the **Refresh** button. To reset to default settings, click the **Default** button.

Settings

The **Settings** menu allows the user to update or modify system, network, video/audio, event, and other general settings related to your AMLINK camera.

Local Settings

The **Local Settings** menu allows the user to set local storage path settings for the camera including record and snapshot events. This option may require the use of the plugin to function. To set local storage path settings, click the **Browse** option and select a destination for the storage path.

To save the settings, click the **Apply** button. To refresh the page, click the **Refresh** button. To reset to default settings, click the **Default** button.

System

The **System** menu allows the user to adjust or modify date & time settings, access upgrade and maintenance features, user management, etc.

General Settings

The **General Settings** menu allows the user to view and modify the device name, language, video standard, as well as adjust any date & time settings for your device.

Device Name: Displays the name of the device. The name can be modified if needed by entering a new name for the camera in this field and selecting **Apply**.
Language: The default language of the device will be English.
Video Standard: Adjust between NTSC or PAL video standards.
Model: Displays the model number of the camera.
Audio Input: Displays how many audio inputs the device supports.
Audio Output: Displays how many audio outputs the device supports.
Serial No.: Displays the serial number of the device.
MAC: Displays the MAC address of the device.
Firmware Ver.: Displays the current firmware version applied to the device.
ONVIF Ver. Displays the current ONVIF version applied to the device.

To save the settings, click the **Apply** button. To refresh the page, click the **Refresh** button. To reset to default settings, click the **Default** button.

Date & Time

The **Date & Time** menu allows the user to adjust the time zone, system time, date and time format, etc.

Time Zone: This dropdown box allows the user to change the time zone used in the camera.
System Time: This field allows the user to enter in the date and time manually or sync to the PC. The NTP Setting must be disabled to update this option.
Date Format: This dropdown box allows the user to change the date format used in the camera.
Time Format: This dropdown box allows the user to change the time format used in the camera.
NTP Setting: This checkbox allows the camera to sync to the NTP server.
- **NTP Server**: Manually update or enter the NTP server (time.windows.com)
- **Port**: This field allows the user to enter in the port number for the NTP server.
- Update Cycle: The cycle time in minutes between the camera and NTP server.

Daylight Savings Time: This checkbox allows the user to enable daylight savings time for the camera.
- **Start Time**: This dropdown box and field allow the user to enter in the start time for DST.
- **End Time**: This dropdown box and field allow the user to enter in the end time for DST.

To save the settings, click the **Apply** button. To refresh the page, click the **Refresh** button. To reset to default settings, click the **Default** button.

Maintenance

The **Maintenance** menu allows the user to set auto reboot settings, restore factory defaults, upgrade firmware, etc.

Upgrade and Maintenance

The **Upgrade and Maintenance** menu allows the user to set auto-reboot settings, factory default, upgrade the camera, etc.

Auto Reboot: A scheduled maintenance feature that automatically restarts the device at a specific time to clear system cache, prevent memory leaks, and ensure long-term stability.
Restore: Resets all settings except for any network or user management settings.
Default: Resets all settings back to factory default.
Import Config: Click Browse to import an exported camera config file.
Export: Export a camera config file
Firmware Upgrade: Click **Browse** to upload a firmware file to the camera, click **Upgrade**. To get the latest firmware for your device please visit: https://amlinksecurity.com/pages/firmware
Online Upgrade: Select **Automatic Detection** to allow the camera to automatically perform an automatic firmware update from the cloud. To check if you are on the latest version, click **Manual Check**.
System Version: Displays the current firmware and build date of your device.

Backup Captured Packet

The **Backup Captured Packet** menu allows the user to export raw network traffic logs (PCAP files) from the camera to an external storage device for advanced troubleshooting and diagnostic analysis of communication issues. To export a captured packet file, click the  and  icon to create export a packet file.

System Log

The **System Log** menu provides a searchable chronological record of all camera activities, including user login, configuration changes, hardware alarms, and system errors, to help you monitor usage and diagnose operational issues.

To view system logs, enter a start and end time, type, encryption type, etc. and click **Search** to view the log. If you would like to export the log, click the **Backup** option and select a storage path for the log file.

Run Log

The **Run Log** menu generates a highly technical, real-time record of the camera's internal software processes and low-level kernel activities, primarily used by developers or support technicians to debug deep-seated system crashes or firmware glitches.

If you would like these logs to be stored locally on a microSD card, select the Store **Running Logs Locally** option. To export a log file, select the log from the log list and click **Export**. To refresh the interface, click **Refresh**. To delete a log, select a log from the log list and click **Delete**. To download a file, click the Download icon  to download the file.

Security

The **Security** menu provides a centralized interface for managing device or system security permissions such as mobile push notifications, multicast/broadcast, SSH, or other security settings related to your device.

System Service

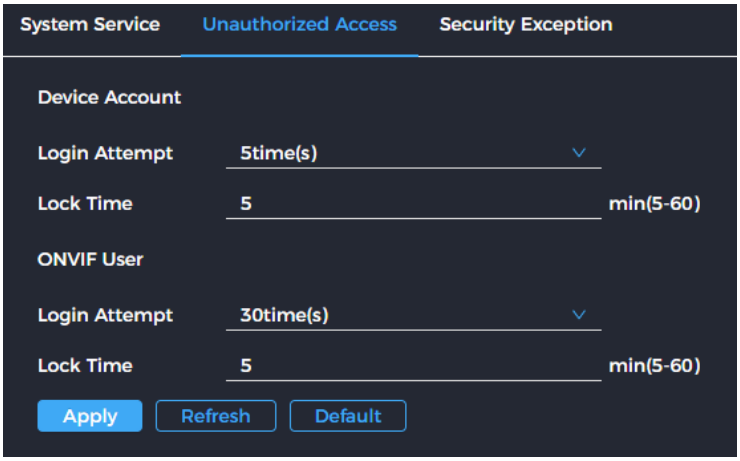
The **System Service** menu allows you to enable or disable specific network protocols and hardware functions, such as SSH for secure command-line access, TLSv1.1, or web-based management ports, to balance the camera's functionality with your network's security requirements.

Mobile Push Notifications: Enable or disable the ability to allow the device to send push notifications to the AMLINK Pro mobile app.
Retrieve by Multicast/Broadcast: Allows the camera to be automatically discovered and identified by video management software or recorders on the local network by responding to general "shout-out" queries rather than requiring you to manually enter the camera's specific IP address.
SSH: enables a secure, encrypted command-line interface that allows administrators or technical support to remotely access the camera's internal operating system to perform advanced configuration, manual file management, or deep-level troubleshooting. While powerful, keeping SSH enabled when not in use can be a security risk, as it provides a potential doorway for unauthorized access if your password isn't extremely strong.
TLSv1.1: Allows you to toggle support for an older version of the Transport Layer Security protocol, which ensures compatibility with legacy web browsers and older software at the cost of using a security standard that is now considered mathematically vulnerable to modern cyberattacks.
Online Log Backup: allows the camera to automatically send its activity logs to a remote server or network storage location in real-time or on a schedule, ensuring that a permanent record of events is preserved even if the camera is physically damaged or its local storage is cleared.
CGI (Common Gateway Interface: Enables a standardized communication protocol that allows third-party software and external applications to interact with the camera, pull video streams, or change settings using simple web commands.

To save the settings, click the **Apply** button. To refresh the page, click the **Refresh** button. To reset to default settings, click the **Default** button.

Unauthorized Access

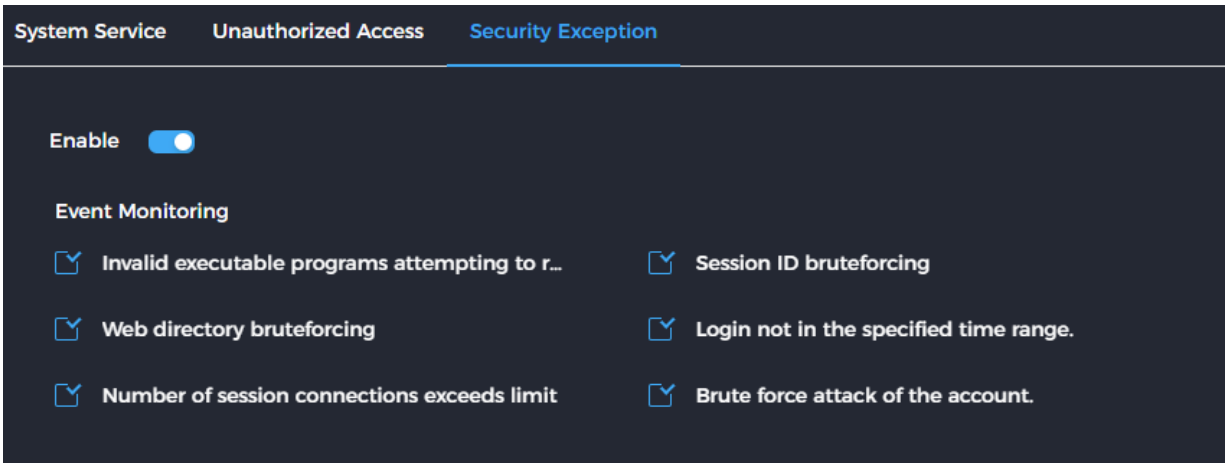
The **Unauthorized Access** menu allows the user to configure security triggers that will automatically lock the camera's login interface or block specific IP addresses after a set number of failed password attempts to protect the device against "brute-force" hacking attacks. By setting a limit, for example, five failed attempts, you ensure that an automated script cannot keep guessing passwords until it finds the right one.



To save the settings, click the **Apply** button. To refresh the page, click the **Refresh** button. To reset to default settings, click the **Default** button.

Security Exception

The **Security Exception** menu allows the user to 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. To enable or modify this option, select Enable and use the options provided in the **Event Monitoring** options.



Invalid executable programs attempting to run: Allows the camera's security system to ignore or permit certain background processes or scripts that might otherwise be flagged and blocked as suspicious by the device's internal "firmware watchdog" or malware protection.

Session ID brute forcing: Activates a specialized defense mechanism that detects and blocks repeated attempts by a hacker to guess a valid "session cookie," preventing them from hijacking an active user's authenticated connection without needing a password. When enabled, the camera monitors how many times an external source tries to present an incorrect or expired session token; if the frequency suggests a brute-force attack, the camera will temporarily blacklist that source to keep your current login session secure.

Web directory brute forcing: activates a security filter that detects and blocks automated bots or attackers attempting to map out the camera's internal file structure by rapidly guessing hidden folder names and URL paths. By monitoring the high frequencies of "404 Not Found" errors coming from a single source, the camera identifies that someone is "fishing" for unprotected directories or sensitive configuration files and automatically severs the connection to that user.

Login not in the specified time range: allows you to restrict user access to the camera's interface to specific days and hours, automatically blocking any login attempts that occur outside of those authorized windows.
This is a powerful "time-lock" security feature that ensures even if someone has a valid username and password, they cannot access the camera feed or settings during off-hours, such as late at night or over the weekend when administrative activity isn't expected.

Number of session connections exceeds limit: allows the camera to detect and block a "Denial of Service" (DoS) style attack where an intruder attempts to crash the system or lock out legitimate users by opening a massive number of simultaneous connection requests. By enabling this, the camera monitors the total volume of active sessions; if a single IP address or the system surpasses a safe threshold, the camera will reject new connection attempts to preserve its processing power for video recording and authorized users.

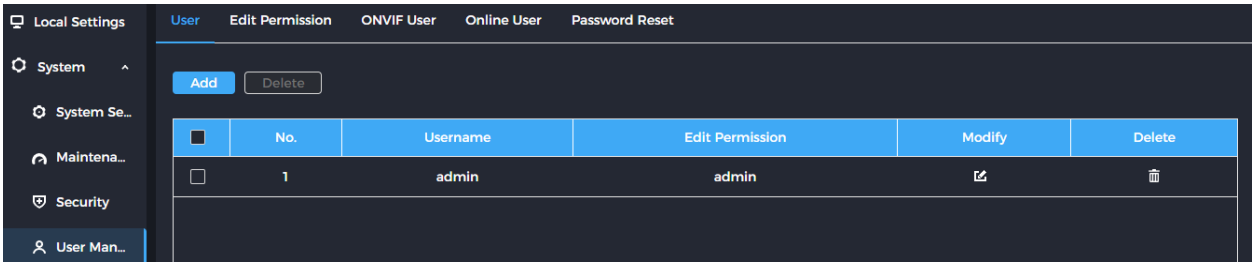
Brute force attack of the account: enables a defense mechanism that monitors rapid, repetitive login attempts using different passwords and automatically triggers a lockout or an alarm once a specific threshold is met to prevent hackers from "guessing" their way into your camera. Unlike general session or directory protection, this specifically guards the **front door** of your camera, the user login screen, by identifying the signature pattern of automated software trying thousands of password combinations in a short window.

Send Email: Enable this option to send an email if an event monitoring option is triggered.

To save the settings, click the **Apply** button. To refresh the page, click the **Refresh** button. To reset to default settings, click the **Default** button.

User Management

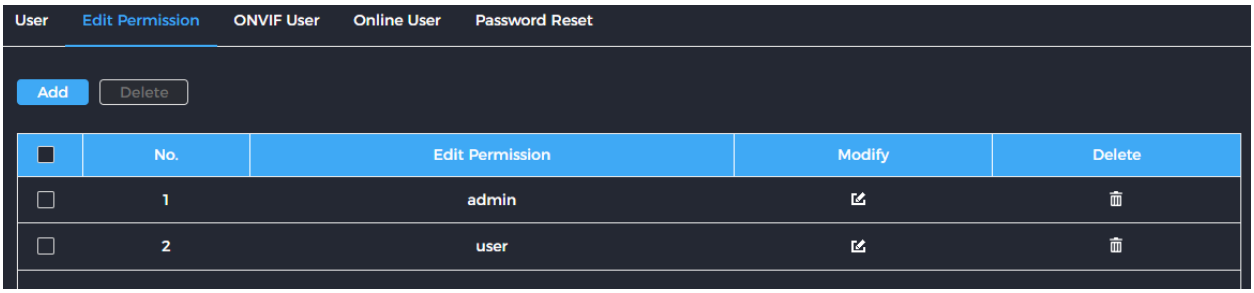
The **User Management** menu allows the user to set, edit, or change user management and password settings.



Add: Add a shared user to access the camera and set permissions such as live view, system, etc.
Delete: Select a user and click Delete to remove the user from the interface.

Edit Permissions

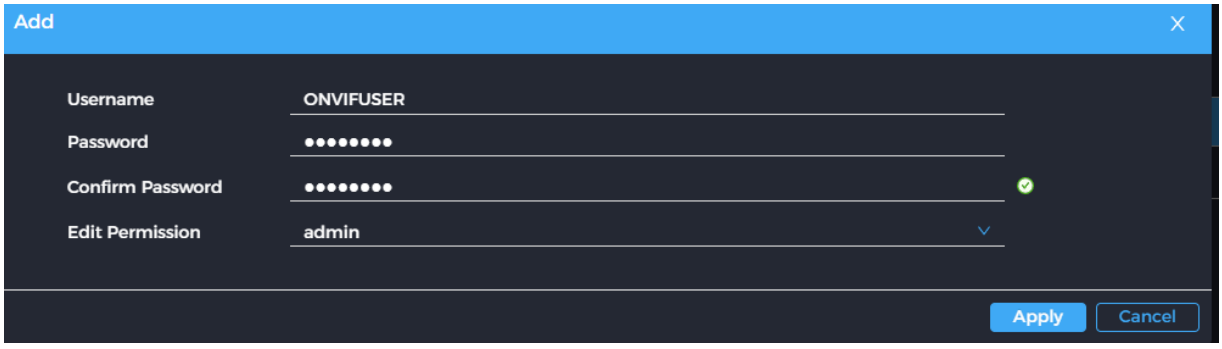
The **Edit Permissions** menu provides a separate menu to add new users or admin to modify user permissions. Click the modify icon and set user permissions if needed.



Add: Add a shared user to access the camera and set permissions such as live view, system, etc.
Delete: Select a user and click Delete to remove the user from the interface.

ONVIF User

The **ONVIF User** menu allows the user to create dedicated credentials that enable third-party recording software and NVRs to access the camera's video stream using a standardized industry protocol, keeping these external connections separate from your main administrative web account.



Online User

The **Online User** menu displays a real-time list of every person or device currently logged into the camera, showing their IP addresses, login times, and privilege levels so you can monitor unauthorized active connections.

Password Reset

The **Password Reset** menu allows the user to configure modify or verify an email address that can be used to recover access to your camera if you forget the administrator password, preventing the need for a physical factory reset of the device.

To save the settings, click the **Apply** button. To refresh the page, click the **Refresh** button. To reset to default settings, click the **Default** button.

Network

The **Network** menu allows the user to set or modify general network settings including TCP/IP, port, DDNS, or other network related settings.

TCP/IP

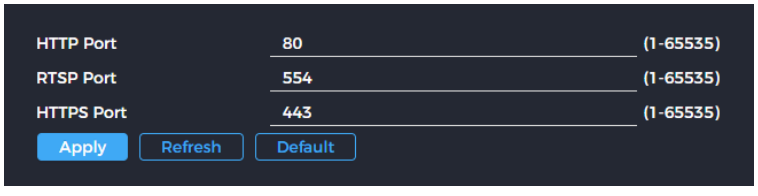
TCP/IP stands for Transmission Control Protocol/Internet Protocol and it is the language/protocol that allows communication between an internet-connected device, whether on a local network and the Internet. This screen allows for TCP/IP settings to be modified for the camera to establish a connection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

IP Version: Displays the IP version, IPV4 or IPV6.
Name: Displays the name of the connection method
MAC: Displays the device's MAC address.
DHCP: Select between a DHCP or Static IP address.
IP Address: The current IP address of the device.
Subnet Mask: Identifies which portion of the camera's IP address represents the network and which portion represents the specific device, effectively defining the size and boundaries of your local network segment.
Default Gateway: The IP address of your network router, acting as the designated "exit door" that allows the camera to communicate with devices outside its local subnet, such as the internet or a remote monitoring server.
Preferred DNS Server: The primary IP address the camera contacts to translate human-readable domain names into numerical IP addresses, enabling it to connect to external services like email alerts or cloud storage
Backup DNS Server: A secondary IP address the camera uses to resolve domain names if the Preferred DNS Server fails to respond, ensuring your camera maintains its connection to cloud services and email alerts without interruption.

To save the settings, click the **Apply** button. To refresh the page, click the **Refresh** button. To reset to default settings, click the **Default** button.

Port

The **Port** menu allows the user to view or customize HTTP, RTSP, and HTTPS port details for your device. If using AMLINK DDNS, the HTTP port must be port forwarded on your network.



To save the settings, click the **Apply** button. To refresh the page, click the **Refresh** button. To reset to default settings, click the **Default** button.

DDNS

The **DDNS** (Dynamic Domain Name System) menu allows you to assign a persistent, easy-to-remember web address to your camera that automatically stays linked to your network even when your internet provider changes your public IP address.

AMLINK DDNS: The default, preferred method for DDNS. This is a DDNS service provided by AMLINK that can be used to set up a custom hostname (*e.g. domainname.amlinkddns.com:port#*).
Dyndns DDNS: A specific third-party service provider that the camera uses to keep your remote access link active by automatically updating a custom hostname (e.g., *yourcamera.dyndns.org*) whenever your internet service provider changes your home's public IP address.
NO-IP DDNS: maps your frequently changing home IP address to a static, custom hostname (like *myhome.ddns.net*), allowing you to access your device remotely without a paid static IP from your internet provider.

AMLINK DDNS Setup

The device must be port forwarded on your network to set up AMLINK DDNS.

1. Go to the **Network** menu and select the **Port** menu.
2. Modify the **HTTP** port, for instance 37779, and click **Apply** and allow the device to restart.
3. Access the admin portal for your router and locate the AMLINK device. Port forward the HTTP port for this device on your router. Please refer to the user manual on your specific router for more details on how to port forward a device if needed. To check if your device is properly port forwarded, you can go to canyouseeme.org to check and verify the camera's port is properly port forwarded on your network.
4. Enter the IP address on your camera into the browser with the port number IPaddress:port# to access the UI.
5. Log in and go to the DDNS menu. Enable the DDNS option and make sure AMLINK DDNS is selected.
6. Enter the Port number and create a domain name.
7. Enter the username and password for your device into the interface and click **Apply**.
8. The device can now be accessed remotely using the DDNS domain created (domainname.amlinkddns.com:port#). If you are having issues or need assistance, please feel free to contact us at https://amlinksecurity.com/pages/contact

To save the settings, click the **Apply** button. To refresh the page, click the **Refresh** button. To reset to default settings, click the **Default** button.

AMLINK Cloud

The **AMLINK Cloud** menu allows the user to view Cloud SDK data as well as quick links via QR code directly to the AMLINK Pro mobile app as well as the device's serial number.

Cloud SDK: Enable or disable the connection between the device and the AMLINK Cloud platform.
Cloud SDK Version: Displays the current cloud SDK version.
Device Setting Schema Version: A technical identifier that defines the organizational structure and formatting of the camera's configuration data, ensuring that the device's internal settings remain perfectly compatible with the software or apps used to manage it.
Device Properties Version: Specific metadata identifier that tells management software exactly which physical hardware features and capabilities are present on that specific camera model, ensuring the user interface correctly displays the appropriate controls.
Mobile APP Download: Scan this QR code for direct access to download the AMLINK Pro mobile app.

Email

The **Email** menu allows for the configuration of email settings to permit the camera to send emails when an alarm is triggered. Select an email provider from the options provided.



Enable: Enable or disable the ability to send email notifications.
SMTP Server: SMTP stands for Simple Mail Transfer Protocol. This field allows the user to enter the SMTP server used by the email service.
Port: This field allows the user to enter the port that corresponds to the selected SMTP server.
Attachment: This checkbox allows a snapshot of the event to be attached to the email notification.
Username: This field allows the user to enter the SMTP username.
Password: This field allows the user to enter the password associated with the SMTP username. If using Gmail, a generated app password will be required. To generate an app password, access your Gmail account, and click on **Manage Your Google Account**. Click on **Security** and make sure 2-step Verification is enabled. Scroll down and select **App Passwords**. Enter a name for the app and click **Create**. Note the generated password provided by Google. This will be the password used to set up email notifications on your device.
Test: Send a test email to the email address provided**.**Click Apply before testing****
Sender: This field allows the user to enter the sender email address. This email address will be the one that sends out all emails pertaining to the alerts and alarm emails sent by the camera.
Encryption Type: This dropdown box allows the user to select an encryption type. There are two types of email encryption protocols that are available:

- **SSL:** Secure Socket Layer
- **TLS:** Transport Layer Security

Subject: Title of the email notification.
Name 1: Name of the recipient.
Address: 1: Email address of the recipient.
Name 2: Name of the recipient.
Address: 2: Email address of the recipient
Name 3: Name of the recipient.
Address: 3: Email address of the recipient

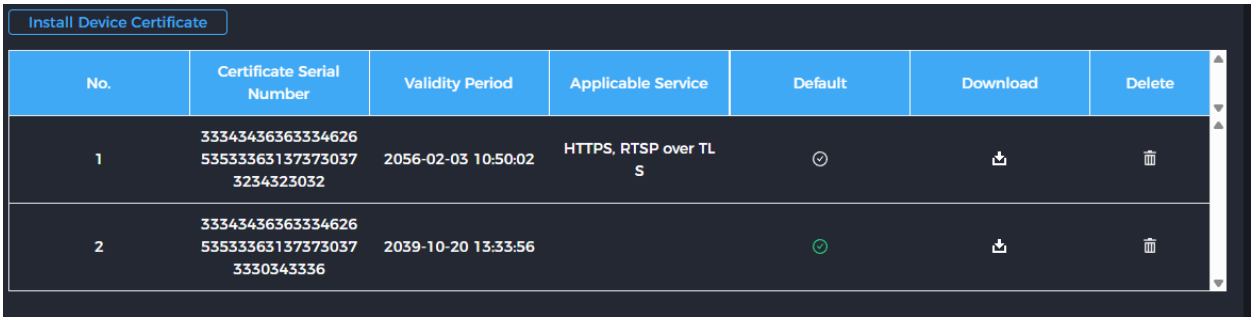
For any additional assistance setting up email alerts feel free to contact us directly at https://amlinksecurity.com/pages/contact

To save the settings, click the **Apply** button. To refresh the page, click the **Refresh** button. To reset to default settings, click the **Default** button.

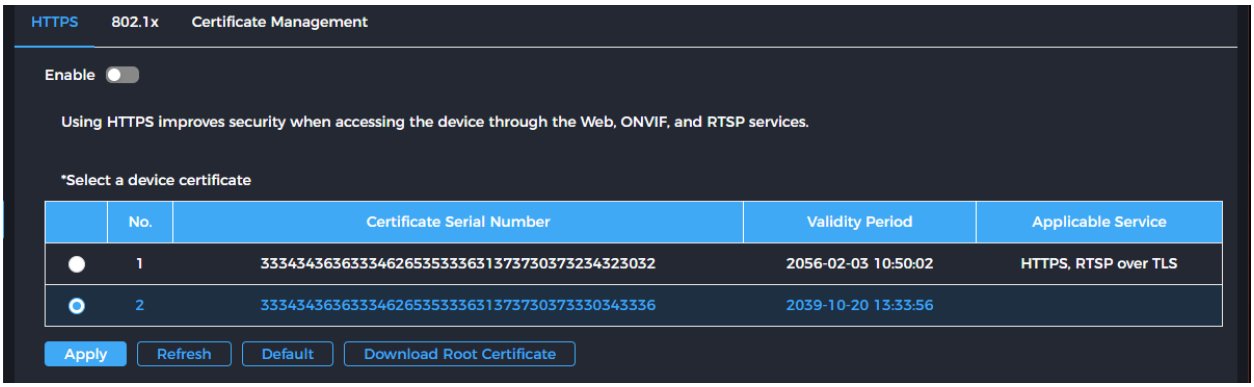
HTTPS

The **HTTPS** menu allows you to enable and manage encrypted communication for the camera's web interface by installing security certificates, ensuring that your login credentials and video data remain private and protected from "snooping" while traveling over the network. By enabling this, your connection moves from the standard **HTTP** (Port 80) to the secure **HTTPS** (Port 443), which prevents hackers on your network from intercepting your password in plain text.

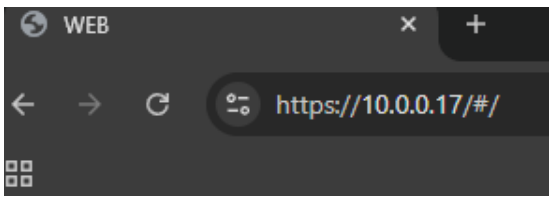
To enable HTTPS, open the **Certificate Management** menu and click Install **Device Certificate** to create a cert file. Enter the requested information and click **Create And Install Certificate**. Select the newly created cert in the default menu and download the cert to your computer.

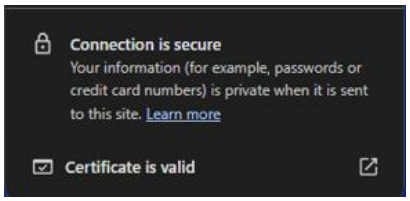


Right click on the root cert you just downloaded and install the certificate to your computer (be sure to place the cert in the **Trusted Root Certification Authorities** folder). Return to the HTTPS menu and select the newly created cert in the interface.



Click **Enable** and allow the browser to restart. Once the page refreshes it will now be set to HTTPS.



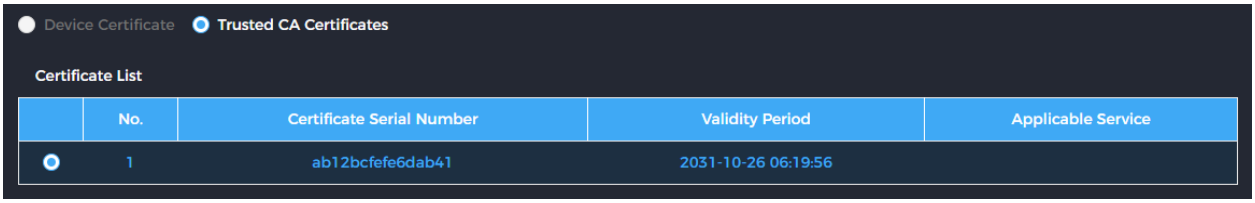


Note: If it is not setting to HTTPS, please be sure to clear the cache and close the browser, reopen the browser. If you are still having issues, please feel free to contact us at https://amlinksecurity.com/pages/contact

802.1x

The **802.1x** is a network access control protocol which can effectively prevent access from unauthorized hosts. To use the 802.1x option, you must configure the camera to provide specific authentication credentials (usually a username and password or a security certificate) to a network switch or controller before the switch will allow the camera to access the local network.

To configure this option, enable the 802.1x protocol and select the correct authentication mode (PEAP or TLS). Enter the username and password for the device and select **CA Certificate** (Use a trusted CA certificate to verify the validity of peer authentication server (switch or Radius server).



Select the Trusted CA Certificates available and click **Apply** to save the setting.

To save the settings, click the **Apply** button. To refresh the page, click the **Refresh** button. To reset to default settings, click the **Default** button.

Advanced

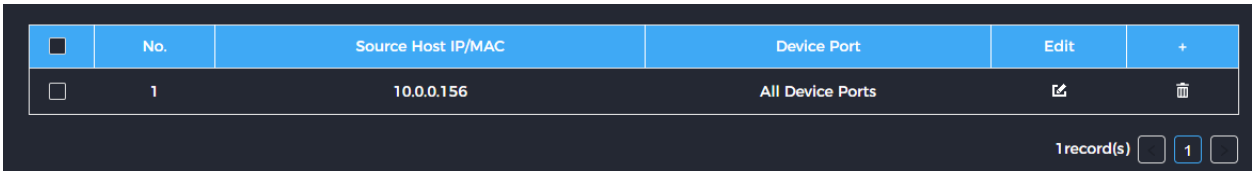
The **Advanced** menu allows the user to view and configure network settings such as firewall, Onvif, PPPOE, UPnP, etc.

Firewall

The **Firewall** menu acts as a security gatekeeper that controls which specific devices are permitted to access the camera's video stream and settings based on their unique network addresses.

Enable: Enable or disable the firewall function.
Allowlist: Often called a "Whitelist" is a "restrictive by default" security setting where the camera blocks **all** incoming traffic except for the specific IP or MAC addresses you have explicitly trusted.
Blocklist: Often called a "Blacklist" is a "permissive by default" security setting where the camera allows access to **everyone** except for the specific IP or MAC addresses you have explicitly banned.

Click the + icon to add an IP into either the allowlist or blocklist.



To save the settings, click the **Apply** button. To refresh the page, click the **Refresh** button. To reset to default settings, click the **Default** button.

ONVIF

The **ONVIF** menu is used to manage the camera's standardized communication protocols, allowing the device to "speak" to third-party hardware like NVRs or software like Blue Iris, etc.

Login Verification: Acts as a security switch that, when enabled, requires third-party devices and software to provide a valid username and password before they can access the camera's video stream or settings via the **ONVIF protocol:** The master toggle that enables or disables the standardized communication protocol, allowing the camera to be discovered and managed by third-party network video recorders and software.

To save the settings, click the **Apply** button. To refresh the page, click the **Refresh** button. To reset to default settings, click the **Default** button.

PPPoE

The **PPPoE** (Point-to-Point Protocol over Ethernet) menu allows the camera to connect directly to an Internet Service Provider (ISP) modem to obtain its own public IP address, bypassing the need for a separate router. When you enable PPPoE, you enter a **username** and **password** provided by your ISP. The camera then "calls out" to the ISP's server to establish a direct internet connection. This essentially turns the camera into its own independent network node on the wide-area web.

To save the settings, click the **Apply** button. To refresh the page, click the **Refresh** button. To reset to default settings, click the **Default** button.

UPnP

The **UPnP (Universal Plug and Play)** menu is a networking feature designed to simplify remote access by allowing the camera to automatically communicate with your router to "punch a hole" through its firewall.

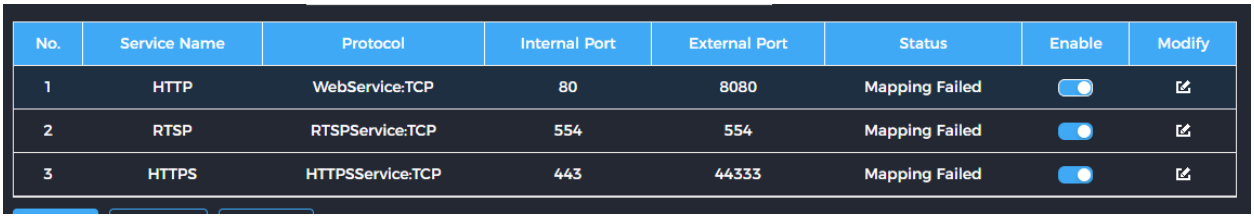
Enable: Enable or disable this feature on the camera.
Enable the Device Discovery: Allows the camera to broadcast its identity and service details to other devices on the same local network.
Router Status: Serves as a real-time diagnostic indicator that tells you whether the camera has successfully communicated with your router to open the necessary network ports. It essentially acts as a "handshake confirmation" between your security hardware and your networking hardware.
Mode: Sets it to map automatically or default.

Automatic: The camera takes full control of the port selection process to ensure there are no "traffic jams" on your network.

- **How it works:** If the camera's standard port (e.g., 80) is already being used by another device on your network, the camera will automatically pick a different, random port number (like 8081) to communicate through.
- **Best for:** Systems with multiple cameras. It prevents "port conflicts" where two cameras try to use the same "door" on the router at the same time.

Default: The camera insists on using its factory-set port numbers for external communication.

- **How it works:** The camera will try to map its internal ports directly to the exact same port numbers on the router (e.g., Internal Port 80 maps to External Port 80).
- **Best for:** Simple setups with only one camera, or environments where you need to know exactly which port is being used so you can hard-code it into a specific software or mobile app.



No.	Service Name	Protocol	Internal Port	External Port	Status	Enable	Modify
1	HTTP	WebService:TCP	80	8080	Mapping Failed		
2	RTSP	RTSPService:TCP	554	554	Mapping Failed		
3	HTTPS	HTTPSService:TCP	443	44333	Mapping Failed		

To save the settings, click the **Apply** button. To refresh the page, click the **Refresh** button. To reset to default settings, click the **Default** button.

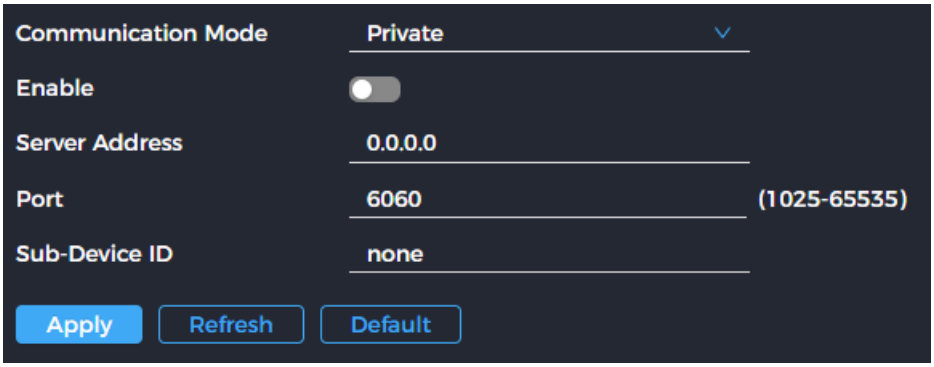
Remote Log Records

The **Remote Log Records** option allows the camera to automatically send its activity history and system alerts to an external server for centralized monitoring and permanent, tamper-proof storage. An external server address, port number, and device number, will be needed to set this feature.

To save the settings, click the **Apply** button. To refresh the page, click the **Refresh** button. To reset to default settings, click the **Default** button.

Auto Registration

The **Auto Registration** menu enables the camera to proactively connect to a central management server or NVR by reporting its identity and current location, which ensures a stable connection even if the camera's IP address changes or it is located behind a complex firewall.



Communication Mode: Set as a private or CGI mode.

Private Mode: Uses the AMLINK's proprietary communication language.

CGI (Common Gateway Interface) is a standardized web-based protocol used for cross-brand communication. It uses standard HTTP/HTTPS requests to send commands and data. It is essentially a "universal" way for different systems to interact.

Enable: Enable or disable this function.

Server Address: The destination where the camera sends its check-in data. You enter the **Static IP address** or **Domain Name** of your server here.

Port: This is the specific "doorway" on the server that is listening for auto-registration requests. The industry standard for this service is typically **7000**, but it must match the "Registration Port" configured in your server's network settings.

Sub-Device ID: This is a unique alphanumeric name you assign to the camera. Because the server might receive check-ins from dozens of cameras, it uses this ID to recognize exactly which camera is calling and which channel it should be assigned to.

To save the settings, click the **Apply** button. To refresh the page, click the **Refresh** button. To reset to default settings, click the **Default** button.

Video/Audio

The **Video/Audio** menu allows the user to view and customize video and audio settings for your camera.

Video

The **Video** menu allows the user to modify video stream settings such as compression, resolution, frame rate, etc.

Video Stream

The **Video Stream** menu allows the user to view and modify mainstream and substream settings for your device.

Encoding Strategy: Select between a general or smart encoding strategy.

- **General:** The default coding strategy of the camera.
- **Smart Encoding:** A function in most AMLINK cameras which aim to reduce bandwidth consumption without losing visible image quality by intelligently increasing compression where it will not make a visible difference in the scene.

Compression: View or modify the compression of your device.
Resolution: Allows the user to set the resolution. The system supports various resolutions, and they can be selected from this dropdown list.
Frame Rate (fps): Allows the user to select and modify the device's frame rate.
Bit Rate Type: Allows the user to select a bit rate type.

VBR (Variable Bitrate): A smart encoding setting that adjusts the amount of data the camera uses based on the amount of activity in the scene.

CBR (Constant Bitrate): A fixed, unvarying amount of data usage regardless of whether the scene is still or full of motion, ensuring predictable storage consumption and consistent network bandwidth requirements.

Quality: Determines the level of visual clarity and detail it attempts to maintain when the bitrate is set to **VBR.**
Bit Rate: Defines the specific volume of data transmitted per second, directly controlling the balance between the visual clarity of the video and the amount of storage space and network bandwidth the camera consumes.
I Frame Interval: Determines how often the camera transmits a complete, high-detail reference frame versus smaller "delta" frames that only record changes in motion, directly impacting the video's stability and its ability to recover from network errors.
Smooth Stream: Manages the flow of data packets and increases buffering to prevent video stuttering or freezing, ensuring a fluid playback experience even on unstable or low-bandwidth network connections.
Watermark: Embeds a custom text overlay or digital signature directly into the video frames to verify the authenticity of the stream and prevent unauthorized tampering or distribution.
Watermark String: The specific sequence of characters, such as a camera name or location, that you manually type in to be embedded as the visible text overlay on the live stream

Sub Stream 1 is a lower quality stream that allows the feed to take up less resources and bandwidth when streaming.

To save the settings, click the **Apply** button. To refresh the page, click the **Refresh** button. To reset to default settings, click the **Default** button.

Region of Interest

The **Region of Interest** menu allows the user to select specific areas of the camera's field of view to be recorded in higher quality than the rest of the image. This is a highly efficient way to capture critical details while significantly reducing the overall bandwidth and storage requirements.

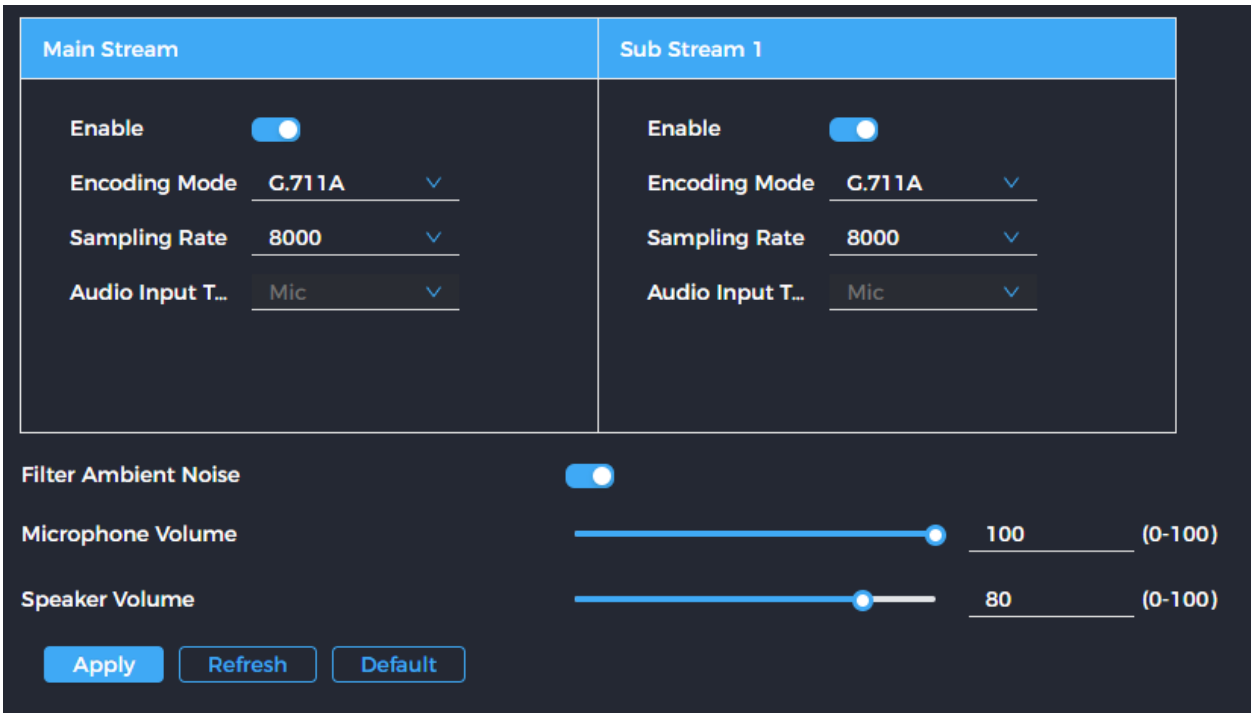
Enable: Enable or disable the feature.
Quality: The higher the quality the least compression applies to the region of interest.

To set a region of interest, enable the toggle switch and set the quality. Click the "+" icon and use your mouse to move and adjust the region of interest on the screen. A max of 4 regions can be set.

To save the settings, click the **Apply** button. To refresh the page, click the **Refresh** button. To reset to default settings, click the **Default** button.

Audio

The **Audio** menu allows the user to view and modify audio settings for the main and substream of the device as well as set alarm audio files.



Enable: Enable audio on the mainstream or substream.

Encoding Mode: Determines the digital format used to compress and transmit audio data.

PCM (Pulse Code Modulation: The raw, uncompressed audio. It provides the highest possible fidelity but uses the most bandwidth.

G.711A (A-law): Uses very little processing power but has a lower dynamic range.

G.711Mu (U-law): Uses very little processing power but has a lower dynamic range.

AAC (Advanced Audio Coding): Overall audio quality and modern compatibility. It provides much clearer sound at lower bitrates than older codecs.

Sampling Rate: Determines how many times per second the camera captures "snapshots" of the continuous analog sound wave to convert it into digital data, with higher values (measured in Hz) resulting in a more accurate and natural-sounding audio reproduction.

Audio Input Type: Displays the types of audio inputs used on your device.

Filter Ambient Noise: Use this toggle switch to enable or disable the ability to filter out ambient noise in the area.

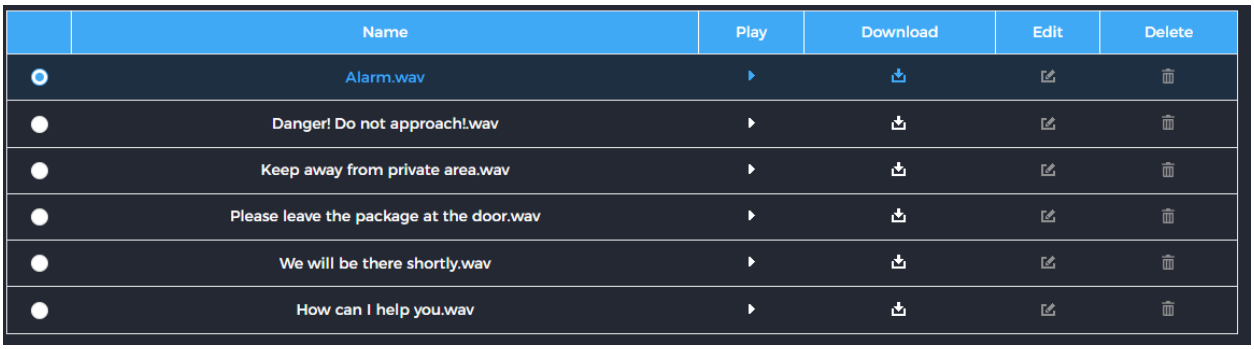
Microphone Volume: Use this slider to adjust the volume of the incoming audio from the microphone.

Speaker Volume: Use this slider to adjust the volume of the outgoing audio from the speaker.

To save the settings, click the **Apply** button. To refresh the page, click the **Refresh** button. To reset to default settings, click the **Default** button.

Alarm Audio Files

The **Alarm Audio Files** menu allows the user to play, download, or change the audio



Select an audio file from the provided list that you would like to use as your siren or warning alarm sound.

Camera

The **Camera** menu allows the user to adjust camera settings, OSD, and privacy masking settings.

Camera Settings

The **Camera Settings** menu allows the user to view and set camera settings, adjust other settings such as night vision, and schedules.

Configuration file: Select between one or two config profiles set for the camera.

Style: Acts as a collection of "visual presets" that instantly recalibrate the image sensor's color, contrast, and sharpness to match specific environments or aesthetic preferences.

- **Standard:** The factory-balanced setting designed for natural color reproduction in average lighting.
- **Soft:** Reduces the digital sharpening and contrast. This can help reduce "image noise" in low-light conditions or make the image look less "processed."
- **Vivid:** Boosts color saturation and contrast.

Brightness: Use this slider to adjust the overall brightness of the video stream.

Contrast: Use this slider to adjust the degree of difference between the darkest and lightest areas of the image.

Saturation: Use this slider to control the intensity and richness of colors in the video feed, where higher values produce more vibrant, vivid hues and lower values pull the color out, eventually resulting in a black and white image.

Sharpness: Use this slider to enhance the definition of edges and fine details within the frame to make the image appear crisper, though setting it too high can introduce "halos" and digital noise that may obscure actual evidence.

Gamma: Use this slider to adjust the brightness of the image's mid-tones without significantly altering the absolute black or white points, allowing you to reveal details hidden in shadows or tone down overexposed areas for a more balanced exposure.

Anti-Flicker: Synchronizes the camera's shutter speed with the frequency of your local power grid, **60Hz** for North America, or **50Hz** for Europe, to eliminate the strobing or rolling dark bands caused by the pulse of artificial lighting like LEDs and fluorescents. The outdoor setting disables the fixed frequency locking (50Hz or 60Hz) and allows the camera's electronic shutter to fluctuate freely based on the available natural light.

Mode: The provided options in this menu tells the camera how to prioritize its internal sensors to handle changing light conditions throughout the day.

- **Automatic:** This is the "set it and forget it" option. The camera automatically balances the **Iris, Shutter Speed, and Gain** to maintain a clear image. It is designed to handle the transition from bright daylight to pitch-black night without any manual intervention.
- **Gain Priority:** An exposure mode that prioritizes keeping the **shutter speed** and **iris** at a fixed or preferred setting while using **Gain** (digital amplification) as the primary tool to maintain image brightness.

Shutter Priority: You set a fixed shutter speed to prevent motion blur, and the camera automatically adjusts the "Gain" (digital brightness) to compensate. This is ideal for license plate capture or areas with high-speed movement.

Manual: This gives you total control over the exposure. You can manually lock the **Shutter Speed** (e.g., at 1/250 to catch fast-moving cars) and the **Aperture/Gain**.

Exposure Compensation: Allows you to manually override the camera's automatic light meter to make the overall image consistently brighter or darker, which is particularly useful for correcting scenes where a very bright background (like a window or white wall) causes the main subject to appear as an underexposed silhouette.

3D NR: Use this toggle switch to enable or disable 3D noise reduction.

3D NR Level: Use this slider to adjust the intensity of 3D noise reduction.

2D NR Level: Use this slider to adjust the intensity of the 2D noise reduction.

To save the settings, click the **Apply** button. To refresh the page, click the **Refresh** button. To reset to default settings, click the **Default** button.

Adjustment

The **Adjustment** menu allows the user to modify and adjust the visual angle, white balance modes, night vision modes, etc.

Visual Angle: Flip or rotate the image 0° (Normal), 90°, 180°, 270°.

Mirror Image: Enable or disable the ability to mirror the image.

Backlight Mode: Allows the user to disable or enable BLC, HLC, or WDR.

Off: Disables backlight mode.

BLC (Backlight Compensation: Increases the exposure for the entire frame to brighten a dark subject in the foreground when they are being "washed out" by a strong light source behind them, such as a bright window or an open doorway.

HLC (Highlight Compensation): Identifies and "masks" the brightest spots in a scene, such as car headlights or intense floodlights, to prevent them from blinding the camera sensor, allowing the surrounding details and background to remain visible.

WDR (Wide Dynamic Range): imaging technology that captures multiple scans of a scene, some exposed to the brightest areas and others to the darkest, and merges them into a single, perfectly balanced frame where both the indoor shadows and the bright outdoor background are clearly visible.

White Balance Mode: Select different presets that adjust the camera's color temperature settings to ensure that white objects appear naturally white under different lighting conditions.

Natural: Automatically optimizes the camera's color processing to mimic how the human eye perceives white under balanced, organic light, providing the most realistic and life-like color accuracy for typical outdoor or daylight-heavy environments.

Street Lamp: Calibrated to neutralize the heavy orange or yellow color cast produced by high-pressure sodium (HPS) street lights, ensuring that skin tones and vehicle colors appear more accurate in nighttime urban environments.

Outdoor: Designed for environments dominated by natural sunlight, utilizing a wide color temperature range to maintain consistent, true-to-life colors as lighting shifts from the bright blueish tint of high noon to the warmer, golden tones of late afternoon.

Manual: Allows you to precisely lock in the color temperature by manually adjusting the red and blue gain sliders, which prevents the camera's colors from "drifting" or shifting in environments with constant, unchanging artificial lighting.

Custom Area: Allows you to precisely lock in the color temperature by manually adjusting the red and blue gain sliders, which prevents the camera's colors from "drifting" or shifting in environments with constant, unchanging artificial lighting.

Auto: Continuously analyzes the entire scene in real-time to identify the brightest neutral point and automatically shifts the color temperature to ensure whites stay white, regardless of whether the light source changes from sun to clouds or artificial bulbs.

Day and Night Mode: Allow you to determine how the camera manages its mechanical IR cut filter and infrared illuminators, controlling whether the image stays in full color, switches to light sensitive black and white, or transitions automatically based on the environment's lux level.

Auto: Uses a built-in light sensor to automatically retract the IR-cut filter and activate infrared LEDs when light levels drop below a certain threshold, seamlessly switching the camera from a full-color day image to a high-contrast black-and-white night image.

Color: Forces the camera to keep its mechanical IR-cut filter engaged and its infrared LEDs off, maintaining a permanent color image even in low-light conditions.

B/W (Black and White): forces the camera to permanently remove its IR-cut filter and switch to a monochrome image, maximizing its sensitivity to light and allowing it to utilize infrared illumination even during the day.

Sensitivity: Determines the specific light threshold required to trigger the transition between Day (Color) and Night (Black and White) modes, with higher settings making the camera switch to infrared mode sooner as light begins to fade. It is set to 2 by default however it can range from 0 to 4.

Delay: Sets the specific number of seconds the camera must detect a consistent change in light levels before switching between Day and Night modes, preventing the camera from flickering back and forth due to momentary flashes of light like passing car headlights or lightning.

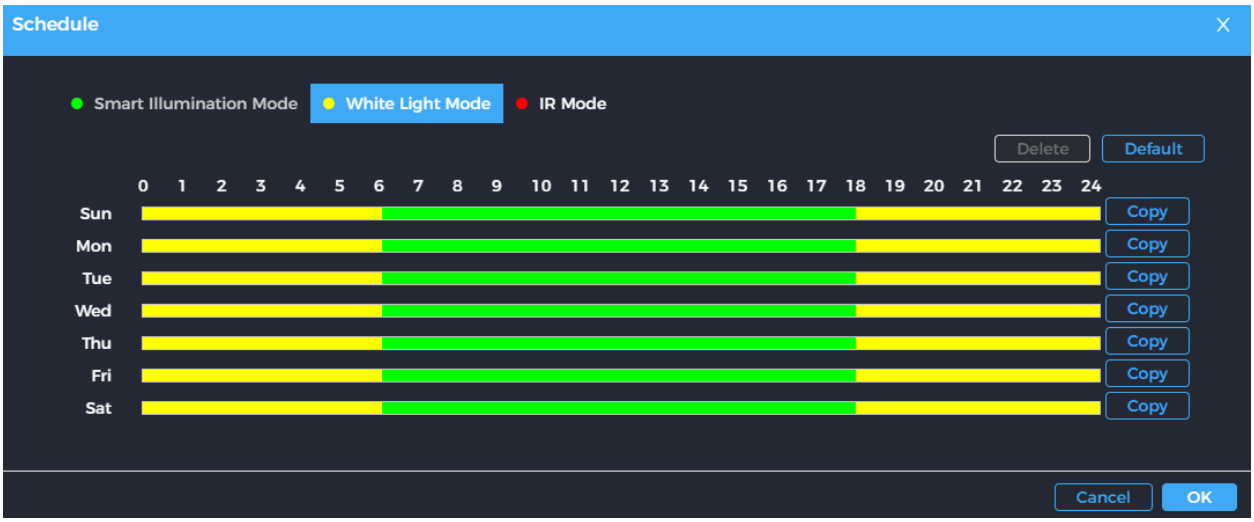
Night Vision: Set different night vision settings, smart illumination, white light, or IR Mode.

Smart Illumination Mode: Camera is set to IR mode, however, once an event is detected it switches to white light as an active deterrent.

White Light Mode: Enables the white light LEDs at night for full color night vision.

IR Mode: Enables the infrared LEDs for black and white night vision.

Schedule: Click the **Setting** option to set a night vision schedule. This will allow night vision to only activate at a specific date and time. Select between white light mode or IR mode and set the schedule. For instance, if we only want the white light LEDs to only be on from 6pm – 6am all week, use your mouse on the schedule interface to set the time. Click **Copy** and set for all days, click **OK** to set the schedule.

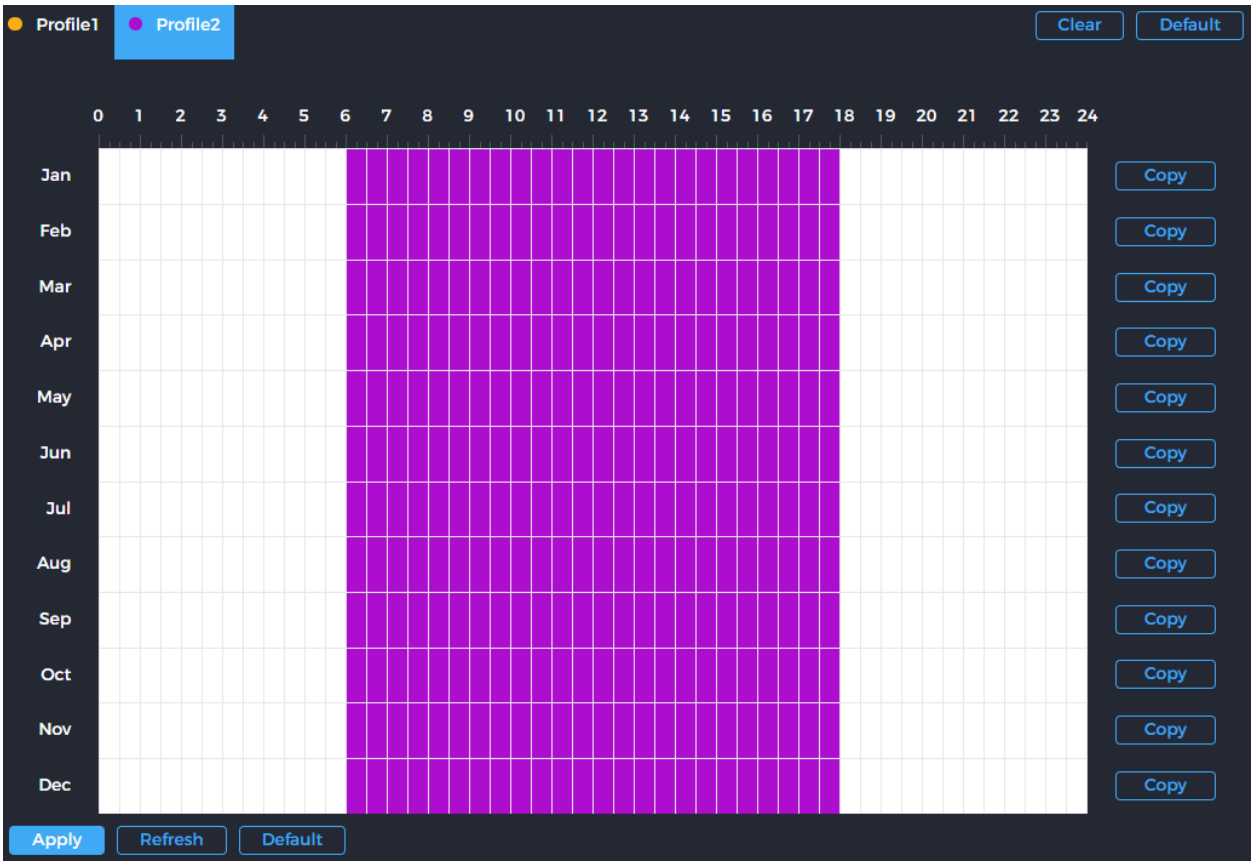


Night Vision Mode: The night vision options will be set to automatically enable or disable.
Illumination Delay: Determines the amount of time the camera waits after switching to Night Mode before activating its LED lights, ensuring that the image sensor has fully stabilized to prevent a temporary "blinding" flare or white-out effect.
Brightness Upper Limit: Use this slider to set the maximum intensity level the camera's LEDs are allowed to reach, preventing the infrared or white light from becoming so powerful that it "blows out" the foreground and obscures the details of nearby objects.
Overexposure Reduction: Actively identifies and dims intense light sources, such as headlights or reflective street signs within the frame to ensure the camera can still capture clear details in the surrounding darker areas.

To save the settings, click the **Apply** button. To refresh the page, click the **Refresh** button. To reset to default settings, click the **Default** button.

Schedule

The **Schedule** menu allows the user to create a schedule for different configuration profiles set on the camera. For instance, if you want to have a schedule to apply to profile 2 from 6am – 6pm, click the **Clear** option and select profile 2. Use your mouse to set the schedule on the interface to apply to all months. Click **Apply**.



To save the settings, click the **Apply** button. To refresh the page, click the **Refresh** button. To reset to default settings, click the **Default** button.

OSD

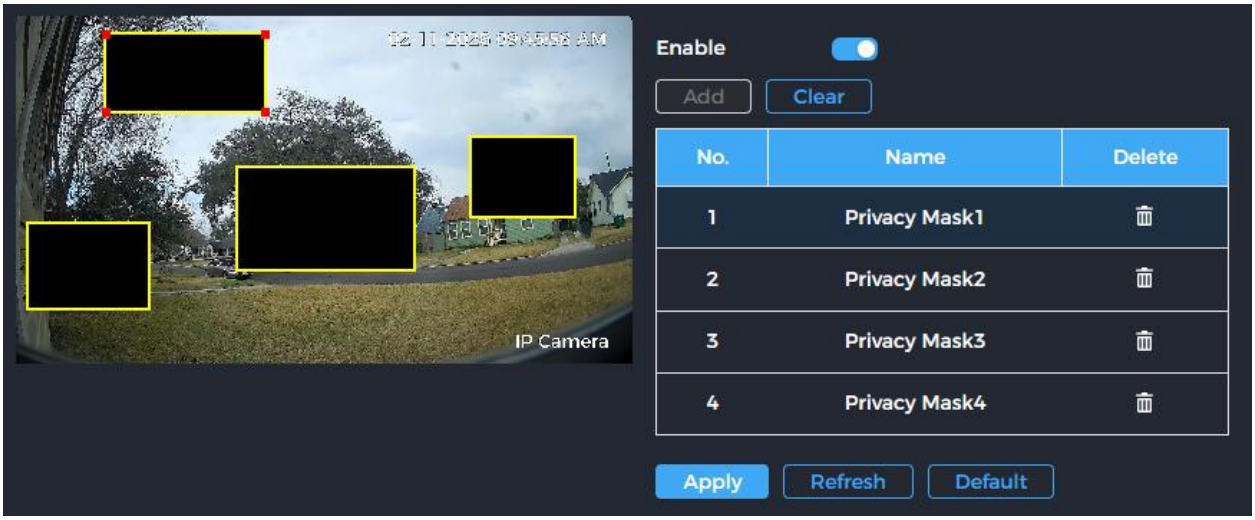
The **OSD** menu allows the user to customize font color, font size, channel name, time, set a custom overlay, etc. Use your mouse to move the overlays on the screen if needed.

OSD Font Color: Select between white or black and white reversed color options.
OSD Font Size: Select between small, medium, large, or automatic.
Display Channel Name: Modify and display the name of the camera displayed on the live stream.
Display Time: Display the date & time on the live stream.
Display Week: Display the day of the week on the live stream.
Display Custom Overlay: Create your own custom text to display on the live stream.

To save the settings, click the **Apply** button. To refresh the page, click the **Refresh** button. To reset to default settings, click the **Default** button.

Privacy Masking

Privacy Masking allows the user to enable and disable up to 4 privacy masking blocks on the live view window. To set a privacy mask, click one of the boxes in the live view screen and use your mouse to position or resize it as needed.



To remove a box, click on it, then click the delete button. To remove all privacy filter boxes, click the Clear button.

To save the settings, click the **Apply** button. To refresh the page, click the **Refresh** button. To reset to default settings, click the **Default** button.

Event

The **Event** menu allows the user to view and modify general motion detection, video tampering, abnormality settings, etc.

General Settings

The **General Settings** menu allows the user to view and modify motion detection and video tampering settings.

Motion Detection

The **Motion Detection** menu allows the user to adjust HVD (Human/Vehicle Detection) options as well as basic motion detection settings. Motion detection region settings can be adjusted on the live feed of this menu which will allow the camera to only monitor specific areas of the feed. Use your mouse to adjust this area, select the clear button to remove all detection areas.



The **Threshold** slider determines the specific amount of pixel change or "magnitude" of movement required within a detection zone to trigger an alarm, where a higher value requires more significant motion (like a person walking) and a lower value allows for the detection of subtle movements (like a cat or a swaying branch).

Enable: Enable or disable motion detection settings.
Event Interval: Sets a mandatory cooldown period between consecutive motion triggers, preventing the camera from sending a flood of redundant notifications for a single, continuous event.
HVD: Enable or disable human and vehicle detection.

- **Human:** Detect an event only when a human is detected by the camera.
- **Motor Vehicle:** Detect an event only when a vehicle is detected by the camera.

Sensitivity: Controls how easily the camera identifies any change in pixels as potential movement, with higher levels allowing it to detect smaller or more distant objects while lower levels ignore minor disturbances like wind-blown leaves or digital noise.
Schedule: Allows you to set a schedule that will allow motion detection to only apply to specific days & times. To set a motion detection schedule, select the settings ( )option. A motion schedule can be set in this menu. For instance, if you want motion detection to only apply between 6am – 6pm all week, use your mouse to adjust the time, click **Copy** and apply to other days of the week. Click Apply to set the motion schedule.



Record: Enable this option to allow the device to record the event to a desired storage path.
Recording Delay: Determines the specific number of seconds the camera captures before an event is triggered or continues to record after the movement has stopped, ensuring you see the full context of an incident from start to finish.
Siren: Enable or disable the built-in alarm sound when an event is detected.
Play Count: The number of times the siren will sound after it has been triggered.
Audio File: The audio clip that will be activated once the siren is triggered.
Warning Light: Enable or disable the white light LED to flash as an active deterrent when an event is detected.
Mode: The activation setting of the warning light, it should be set to flicker by default.
Flicker Frequency: The intensity of the warning light after it is activated.
Duration: The amount of time the deterrent will be active after it is triggered.
Schedule: Set a schedule in which the white light LED deterrent and siren will apply.
Brightness: Use this slider to adjust the brightness of the white light LED after it is triggered.
Send Email: This checkbox allows the user to enable the camera to send an email notification an event is triggered.
Snapshot: This checkbox allows the user to enable the camera to take a snapshot when an event is triggered.

To save the settings, click the **Apply** button. To refresh the page, click the **Refresh** button. To reset to default settings, click the **Default** button.

Video Tampering

The **Video Tampering** menu allows the user to configure automated alerts that trigger if the camera's view is obstructed, redirected, or defocused, ensuring you are immediately notified if someone attempts to blind the lens with spray paint or physically move the camera.

Enable: Enable or disable this function.
Schedule: Click the settings icon to set a video tampering schedule.
Record: Enable this option to allow the device to record the event to a desired storage path.

Recording Delay: Determines the specific number of seconds the camera captures before an event is triggered or continues to record after the movement has stopped, ensuring you see the full context of an incident from start to finish.
Send Email: This checkbox allows the user to enable the camera to send an email notification an event is triggered.
Snapshot: This checkbox allows the user to enable the camera to take a snapshot when an event is triggered.

To save the settings, click the **Apply** button. To refresh the page, click the **Refresh** button. To reset to default settings, click the **Default** button.

Abnormality

The **Abnormality** menu allows the user to configure automated alerts for system level issues such as SD card failures, IP address conflicts, or voltage exceptions, etc. to ensure you are notified when the camera's hardware or network stability is compromised.

No SD Card: Enable this option to send an email notification if an inserted microSD card is not detected.
Insufficient SD Card Space: Enable this option to send an email notification if the microSD card storage falls below a set percentage of free space.
SD card error: Enable this option to send an email notification if the microSD card receives an error while inserted.
Offline: Select the **Record** option to send an alert once the camera goes offline.
IP Conflict: Select the **Record** option to send an alert if there is an IP conflict. This happens if another device on the same network is assigned to the identical IP address as your camera, which would otherwise cause the video stream to drop or become unreachable.
Voltage Exception: Triggers an automated alert if the camera detects that its incoming power supply has fluctuated above or below the required operating range, helping to prevent hardware damage or unexpected reboots caused by unstable electrical sources.

- **OSD:** Enable an overlay on the live stream if the abnormality is triggered.
- **Send Email:** Allow an email notification of the abnormality to be sent after it is triggered.

To save the settings, click the **Apply** button. To refresh the page, click the **Refresh** button. To reset to default settings, click the **Default** button.

Alarm

The **Alarm** menu allows the user to set any disarming and alarm settings associated with your device.

Disarming

The **Disarming** menu allows the user to temporarily suspend all alarm actions (such as emails, sirens, or push notifications) without turning off the camera's actual recording or detection capabilities.

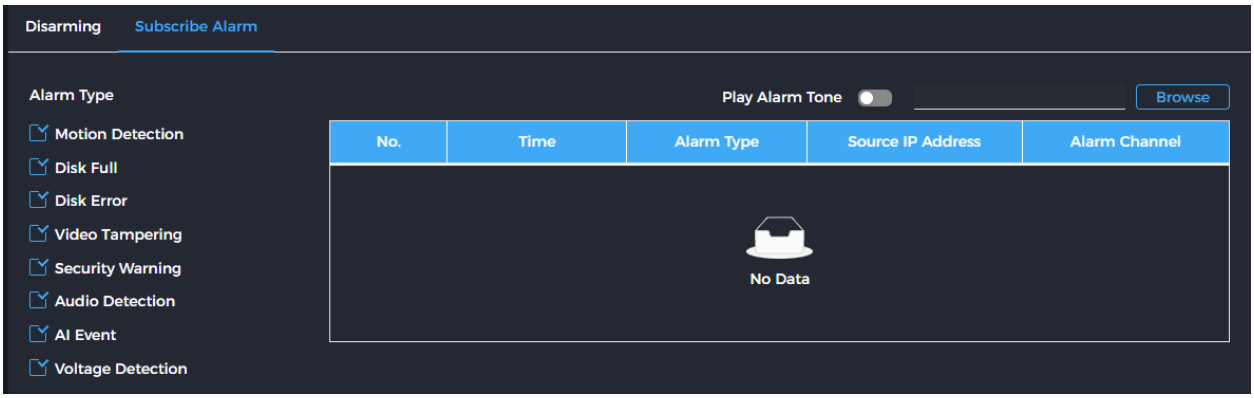
Disarming: Enable or disable (close) the disarming feature.
Disarm by Period: Allow the device to only disarm based on a schedule.
Disarm Period: Sets a disarming schedule to allow the rule only to apply to certain times of the day.
Disarm Alarm Linkage Action: Select which action that will still occur when an alarm is triggered.

- **Select all:** Enable all event notification options.
- **Send Email:** Enable an email to be sent when actively disarmed.
- **Siren:** Enable the siren to sound when actively disarmed.
- **Warning Light:** Enable the white light LED to illuminate or flash when actively disarmed.

To save the settings, click the **Apply** button. To refresh the page, click the **Refresh** button. To reset to default settings, click the **Default** button.

Subscribe Alarm

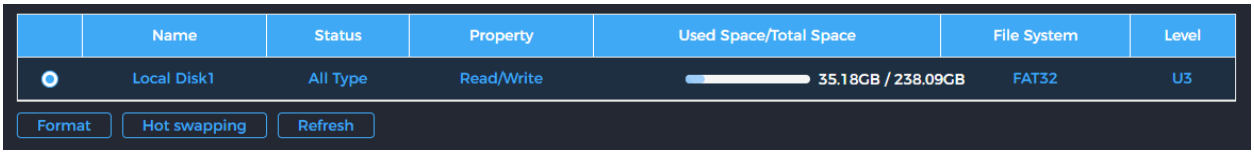
The **Subscribe Alarm** menu allows the user to choose which specific types of events or system alerts are actively pushed to your client software or mobile app, ensuring you only receive real-time notifications for the incidents you find most critical.



Play Alarm Tone: Enable this option to set a specific alarm tone file into the interface.
Browse: Browse your computer to import an audio file for the alarm tone.

Storage

The **Storage** menu allows the user to format local storage (microSD) card and view microSD card details. To format the microSD card, select the local disk and click **Format**.



Hot swapping refers to the ability to remove and replace an SD card or local storage drive while the camera is still powered on and running, allowing for maintenance or data retrieval without interrupting the live video stream. Click the Refresh button to refresh the interface.

Note: All microSD card recordings and playback will be performed in the AMLINK Pro mobile app. For more information on playback, please visit amlinksecurity.com/support

Logout

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

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 operated in conjunction with any other antenna or transmitter.

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

Appendix A: Toxic or Hazardous Materials or Elements

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

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

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

Note:

This user manual is for reference only. Slight differences may be found in the user interface.

All the designs and software here are subject to change without prior written notice.

All trademarks and registered trademarks mentioned are the properties of their respective owners.