Network Camera

User's Manual

Important Information Before Using This Manual

This is a fundamental guide for operating a S&M Technology network camera. Whether you are a first-time user or someone with experience using similar devices, it is essential to read this manual carefully before using the product. Pay close attention to the warnings and precautions outlined in this manual to ensure safe and effective use of the product. Following these safety guidelines will help prevent accidents and damage to property.

- The manufacturer is not liable for any damage to the product caused by the use of unauthorized parts or accessories or by failure to follow the instructions in this manual.
- The information in this manual is believed to be accurate as of the publication date. However, some features may not be described, and the manufacturer cannot be held responsible for any issues arising from their use. The content may change without notice, and future editions may be issued to incorporate any revisions.
- First-time users and those unfamiliar with the network camera should seek assistance from their retailer for installation and use.
- For expansion, repair, or disassembly purposes, always contact the retailer and request professional help.
- Both retailers and users should be aware that this product has been certified for electromagnetic compatibility for commercial use. If the product was unintentionally sold or purchased, please ensure it is replaced with a consumer version.

Safety Symbols

In-Text Symbols

- Caution: Important information regarding a specific function.
- Note: Useful information about a specific function.

Safety Symbols

WARNING

RISK OF ELECTRIC SHOCK
DO NOT OPEN

Warning: To reduce the risk of electric shock,
do not remove the cover or back.
There are no user-serviceable parts inside.
Refer servicing to qualified personnel.

Important Safety Instructions

1. Read Instructions

All safety and operating instructions should be read before using the equipment.

2. Retain Instructions

Keep the safety and operating instructions for future reference.

3. Cleaning

Unplug the equipment before cleaning. Do not use liquid aerosol cleaners. Use a damp, soft cloth for cleaning.

4. Attachments

Never add any attachments or equipment without the approval of the manufacturer, as such additions may result in fire, electric shock, or personal injury.

5. Water and Moisture

Do not use this equipment near water or in contact with water.

6. Placement and Accessories

Ensure the equipment is installed on a wall or ceiling strong enough to support it. Improper installation could cause the equipment to fall, resulting in injury or damage. Follow the manufacturer's instructions for mounting and use only approved mounting kits. When moving the equipment, do so carefully, as quick stops or excessive force can cause the equipment to overturn. Do not place the equipment in an enclosed space. Adequate ventilation is necessary to prevent overheating and reduce the risk of fire.

7. Power Sources

The equipment should be powered only from the type of source indicated on the labeling. If unsure of the power requirements, consult the dealer or local power company. Consider installing an Uninterruptible Power Supply (UPS) system for safe operation, preventing damage from unexpected power outages.

8. Power Cord

Always disconnect the power and cables before handling the equipment.

9. Lightning

For added protection during lightning storms, or when the equipment is left unused for long periods, unplug it from the wall outlet and disconnect any antenna or cable system. This will prevent lightning and power surge damage. Use a surge protector if lightning is common in the area.

10. Overloading

Avoid overloading wall outlets or extension cords, as this could result in fire or electric shock.

11. Objects and Liquids

Never insert objects into the equipment's openings, as they may contact dangerous voltage points or cause a short circuit. Avoid spilling liquids on the equipment.

12. Servicing

Do not attempt to service this equipment yourself. Refer servicing to qualified service personnel.

13. Damage Requiring Service

If the equipment shows signs of damage such as the following, unplug it and consult qualified service

personnel: A. Damage to the power supply cord or plug B. Spilled liquid or impact damage C. Exposure to rain or water D. If the equipment does not operate normally, follow the operating instructions to avoid unnecessary adjustments that could cause further damage. E. If the equipment has been dropped or the casing is damaged F. A noticeable change in performance indicates a need for servicing.

14. Replacement Parts

When replacing parts, ensure that the service technician uses parts specified by the manufacturer or parts with equivalent characteristics. Unauthorized substitutions could result in fire, electric shock, or other hazards.

15. Safety Check

After any service or repair, ask the service technician to perform safety checks to ensure the equipment is in proper working condition.

16. Installation

Installation should be carried out by a qualified technician and must comply with local codes.

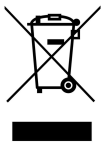
17. Maximum Ambient Temperature (Tmra)

Ensure that the equipment's maximum recommended operating temperature (Tmra) is specified, so the customer and installer can determine a suitable operating environment.

WEEE (Waste Electrical & Electronic Equipment)

Proper Disposal of This Product

Applicable in the European Union and countries with separate waste collection systems.



The symbol displayed on the product or its packaging indicates that this device should not be disposed of with household waste at the end of its life cycle. To prevent potential environmental harm or health risks from improper disposal, please separate it from other waste and recycle it responsibly. This will promote the sustainable reuse of materials.

For Household Users:

Contact the retailer from whom you purchased the product, or your local government office, for information on how to dispose of this product in an environmentally responsible manner.

For Business Users:

Consult your supplier to check the terms and conditions in the purchase agreement. This product should not be mixed with other commercial waste for disposal.

Contents

OVERVIEW

This camera is a megapixel motorized network camera module with a built-in web based viewer accessible by multiple browsers.
This camera supports dual compression formats and triple streaming simultaneously. The three standard compression formats include H.265, H.264 and MJPEG. The streams can be configured to a variety of resolutions, bit rates and frame rates.

** NOTE*
The several features are dependent on camera model.

System Requirements

1. Operating System
   - Windows Vista (32 bit) Ultimate, Business Edition
   - Windows 7, 8 (32/64 bit), 10, 11 (32/64 bit) Home, Professional Edition

2. Processor
   - Intel Core 2 Duo 2.4 GHz or higher
   - Intel Core i5, i7 2.8 GHz or higher

3. Memory
   - 4 GB or more

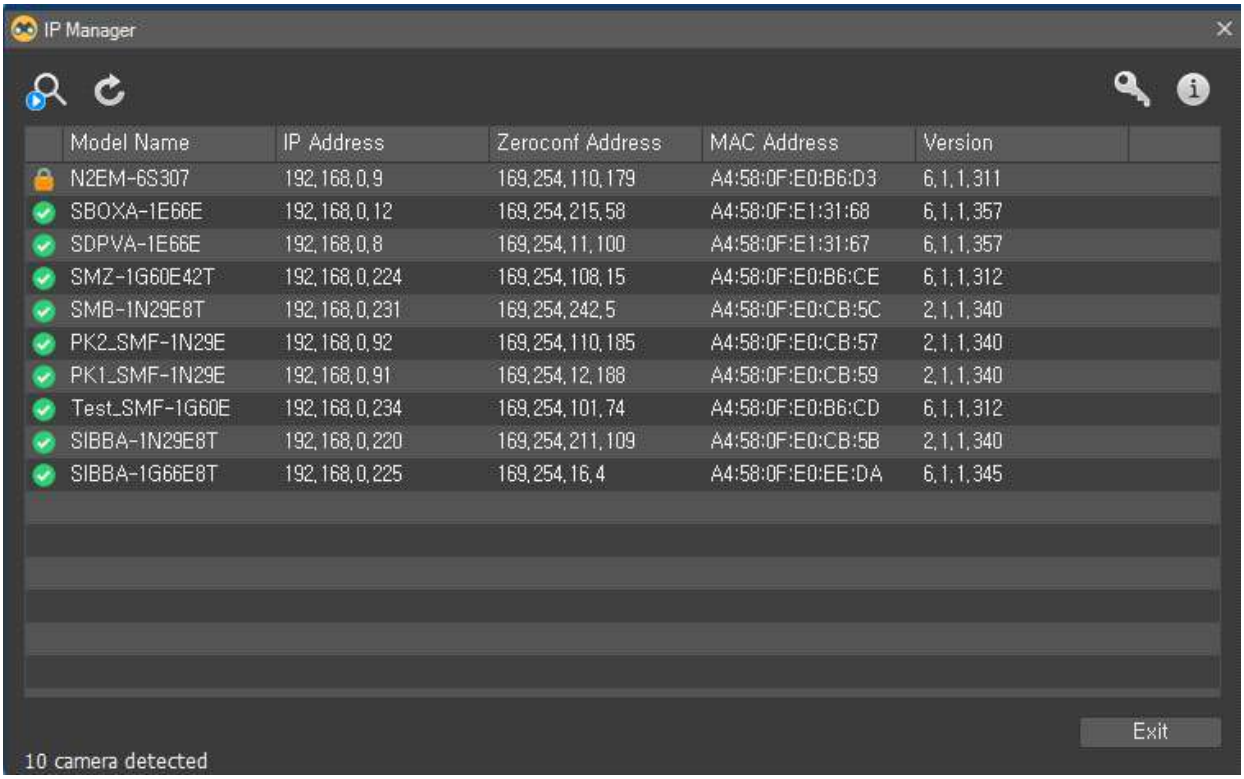
4. Resolution
   - 1280X1024 pixels or higher (32 bit color)

5. Supported web browsers
   - Microsoft edge
   - Google Chrome
   - Apple Safari
   - Mozilla Firefox
   - Opera
   - Brave

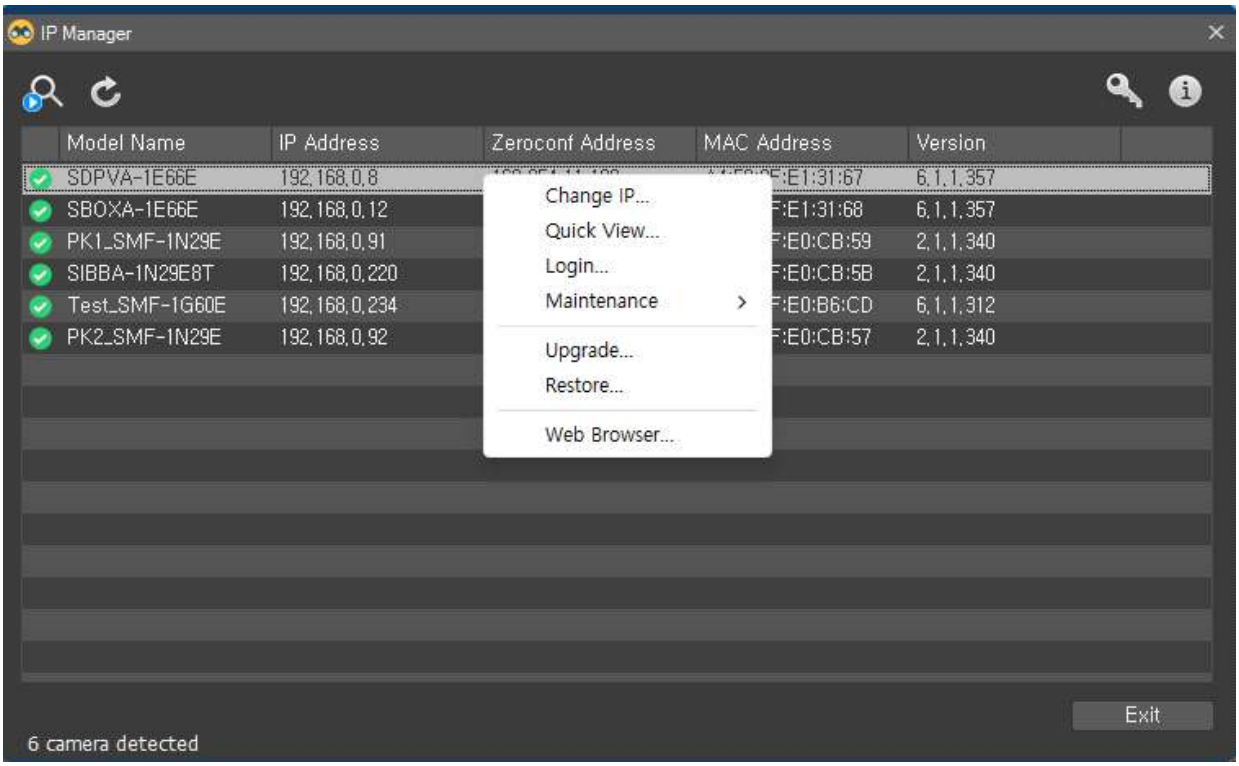
IP MANAGER USAGE

IP Manager Setting

Run the IP Manager.exe



Designation	Function
Stop Discovery	Product Navigation stop or restart.
Start Discovery	
Refresh	
Model Name	The model name of the connected camera.
IP Address	The IP address of the camera.
Zeroconf Address	Zero configuration networking (zeoconf) is a set of techniques that automatically creates a usable Internet Protocol (IP) network without manual operator intervention or special configuration servers. Zero configuration networking allows devices such as computers and printers to connect to a network automatically. Without zeroconf, a network administrator must set up services, such as Dynamic Host Configuration Protocol(DHCP) and Domain Name System(DNS), or configure each computer's network settings manually, which may be difficult and time-consuming.
MAC Address	IP camera MAC Address
Version	The firmware version of the product.



Change IP: Select a product and click this button to reset the product's IP address.

Quick View: Displays live video.

Login: The default user name / password are admin / admin

Maintenance: Click on the "Scan" tab and click on the product from the "Maintenance" tab, you can restart or reset the camera settings.

- Restart: Restart the network camera.
- Reset: Reset all parameters, except the IP parameters to the original factory setting.
- Default: Reset all parameters to the original factory setting.

Calibration: White pixel compensation.

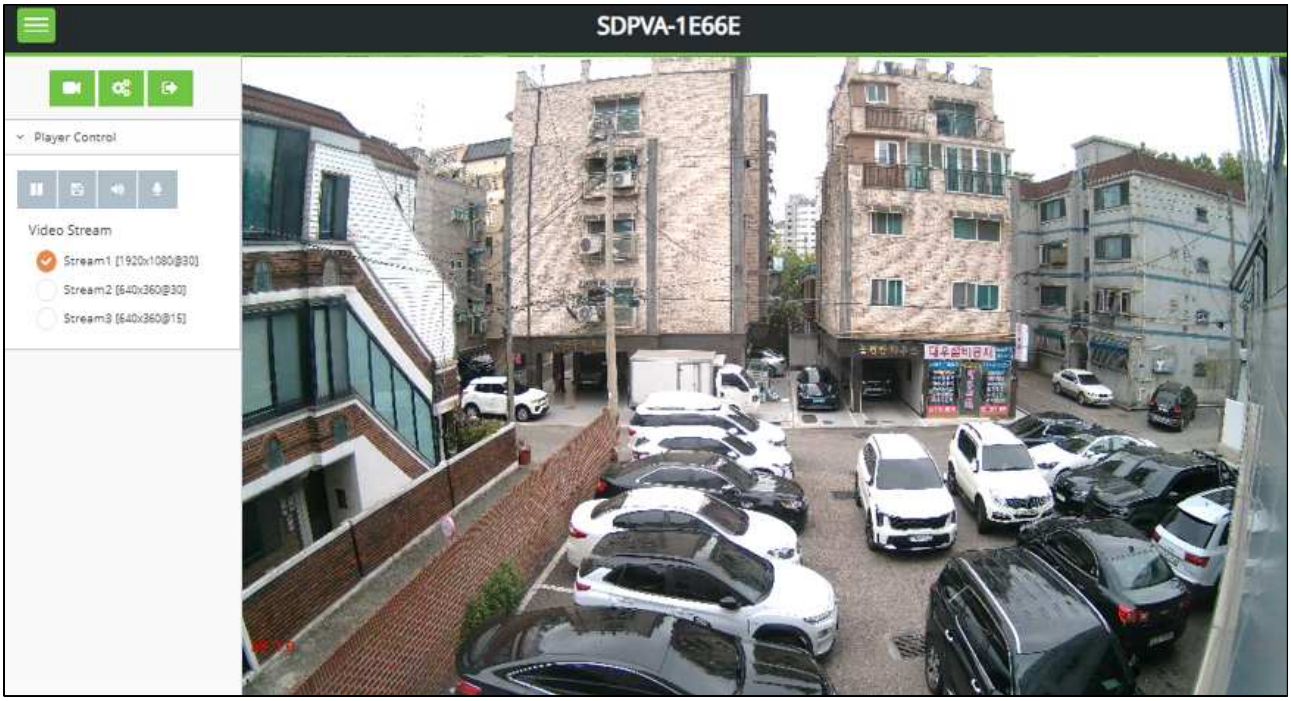
Upgrade: Provides the latest firmware to the camera. When you upgrade the firmware with a file, your camera receives the latest available functionality and unparalleled reliability.

Web Browser: Connects to the home page.

Accessing the IP camera

1. Open the web browser.
2. Enter the camera's IP address in the address bar of the web browser.
   - When the product is shipped, it is configured to have the IP address automatically assigned by the DHCP server.
   - If there is no DHCP server, the IP address is set to **192.168.0.10**
3. Enter the user ID and password in the login window to access the camera webpage.
   - **ID: admin**
   - **Password: admin**

WEB UI Menu



Show Menu and Live Video

Display Live Video

Enter Setup Menu

Exit Current Login and/or Enter New Login

Player Control

Pause: Freeze the current windows

Snapshot: Take a picture of the video image currently on display

Speaker: Set the speaker volume

Microphone: Enable or Disable the microphone

Display

Show the display mode

- Window Fit: Automatically fit the live video size into the current window size.
- Full Screen: Displays the current video size into full screen size.
- Custom: Adjusts the video size from Min.0% to Max.200%.

Protocol

Specify the protocol that is used

- HTTPS: Hypertext Transfer Protocol Secure (SSL/TLS)
- HTTP: Hyper Text Transfer Protocol
- TCP: Transmission Control Protocol
- UDP: User Datagram Protocol

Video Stream

Specify the video source that is used

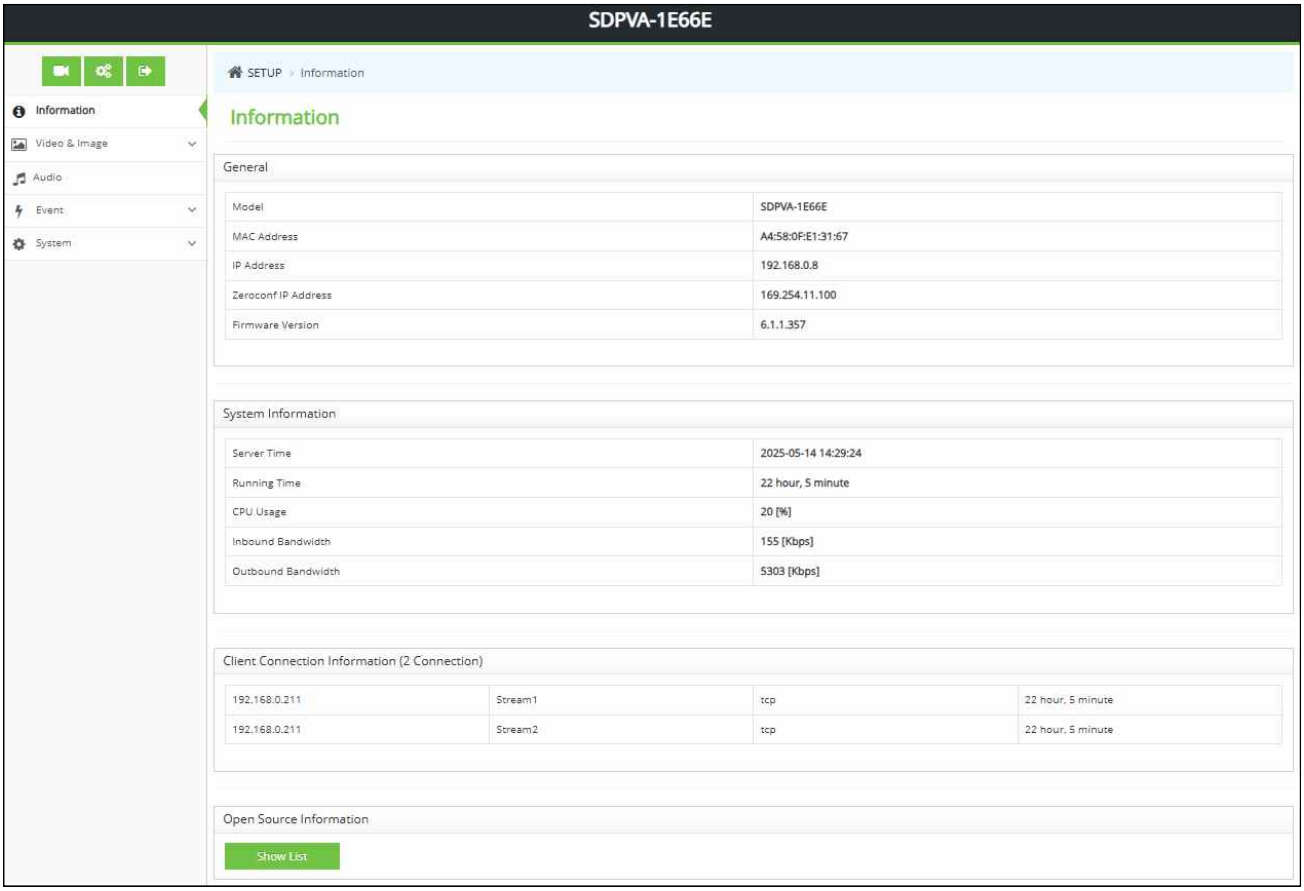
- Stream1: Show stream1 resolution and frame rate
- Stream2: Show stream2 resolution and frame rate
- Stream3: Show stream3 resolution and frame rate

Note

The total number of stream is dependent on camera model.

SETUP

Information



General: Display basic information about the camera, such as Model name, MAC address, IP address, Zeroconf IP address, and Firmware version.

System Information: Display system information, including Server time, Running time, CPU usage, inbound bandwidth, and Outbound bandwidth.

Open Source Information: Display the list of open-source components used in this camera.

Video & Image > Source

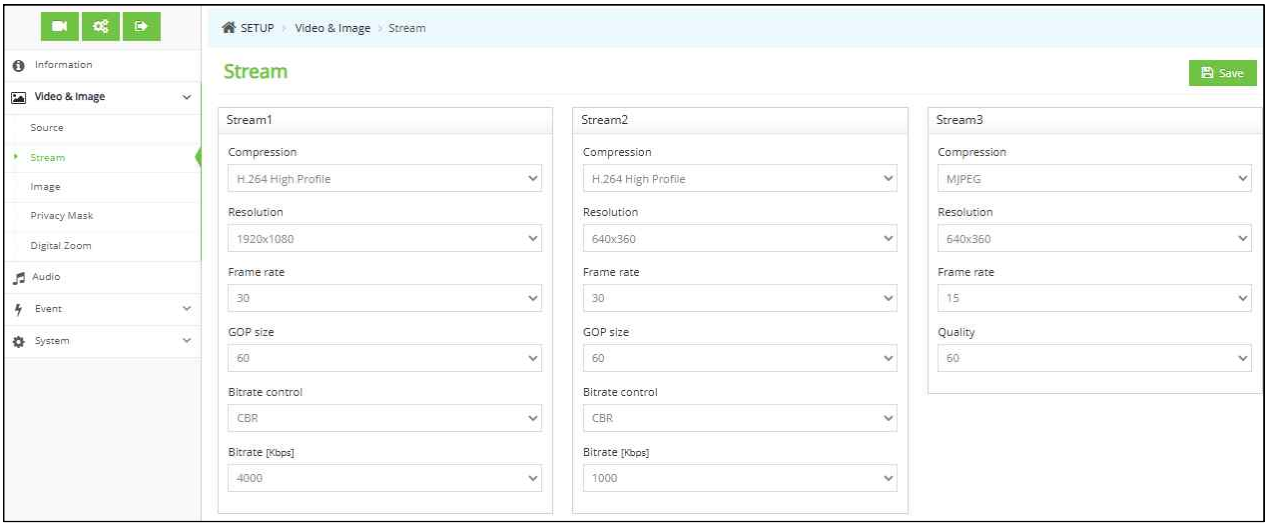
Specify the video source. Depending on the source signal or mode, each stream configuration will be affected and the streaming will be automatically adjusted based on system performance.

Signal: Select the video standard signal: NTSC or PAL.

Mode: Specify the video mode to be used.

Video & Image > STREAM

Configure the setting for H.264, H.265, and MJPEG video streams.



Compression: Select the video compression standard for the stream (e.g., H.264, H265, or MJPEG)

Resolution: Specify the resolution as the width (pixel columns) by height (Pixel rows).

Frame rate: Set the frame rate for video stream in frames per second (fps).

GOP size: The Group of Pictures (GOP) setting determines the number of partial frames between full frames in the video stream. In a typical scene, such as a door opening and a person walking through, only the movement of the door and the person is encoded. The stationary background, which has not changed, is not encoded in the partial frames but is encoded in the full frames.

By using partial frames, video compression is more efficient, reducing the overall size of the video file. As the GOP value increases, more partial frames are generated between full frames. This results in a lower video size and reduced bandwidth usage. However, higher GOP values can impact image quality, as less frequent full frames may reduce the sharpness of movement or detail.

This setting is available only with H.264 or H.265 compression standards. A higher GOP value saves bandwidth but may negatively affect image quality, so it is recommended only for networks with high reliability. Before adjusting the GOP size, consult with your network administrator to ensure compatibility with your system and network conditions.

Bitrate control: The bitrate can be configured to either VBR (Variable Bit Rate) or CBR (Constant Bit Rate), depending on the needs.

• VBR (Variable Bit Rate): The bitrate is dynamically adjusted based on the complexity of the image. It allocates more bandwidth for scenes with higher activity, such as fast-moving objects, and less bandwidth for scenes with minimal movement or less detail. This helps optimize bandwidth usage while maintaining video quality.

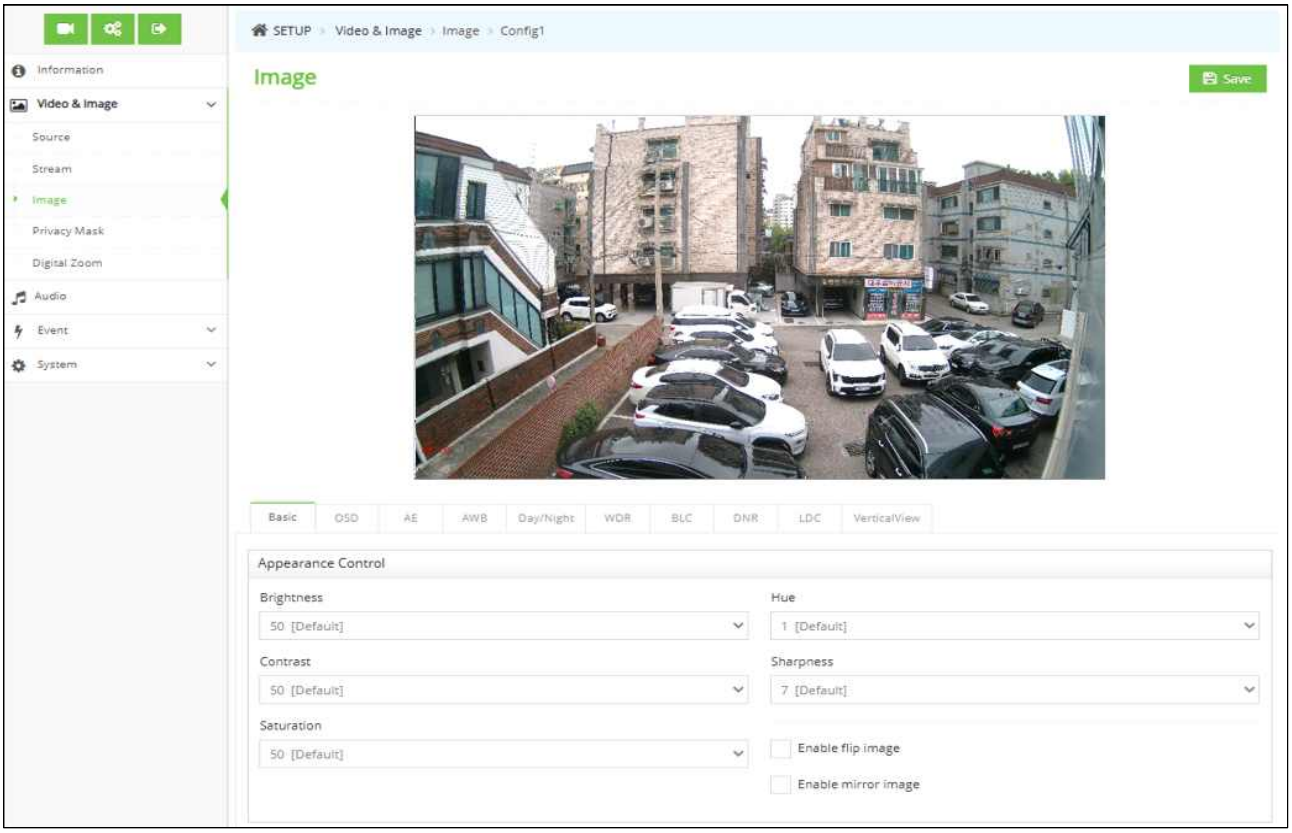
• CBR (Constant Bit Rate): This setting allows you to specify a fixed target bitrate, resulting in a consistent bandwidth consumption. While this ensures predictable network usage, the bitrate typically needs to increase for scenes with more activity. However, this can negatively affect frame rate and image quality in such cases, as the fixed bitrate may not be sufficient for high-motion or complex scenes.

Bitrate: This setting specifies the video stream quality in kilobits per second (kbps). A higher bitrate generally improves video quality but also increases the bandwidth requirement.

Video & Image > IMAGE

Basic

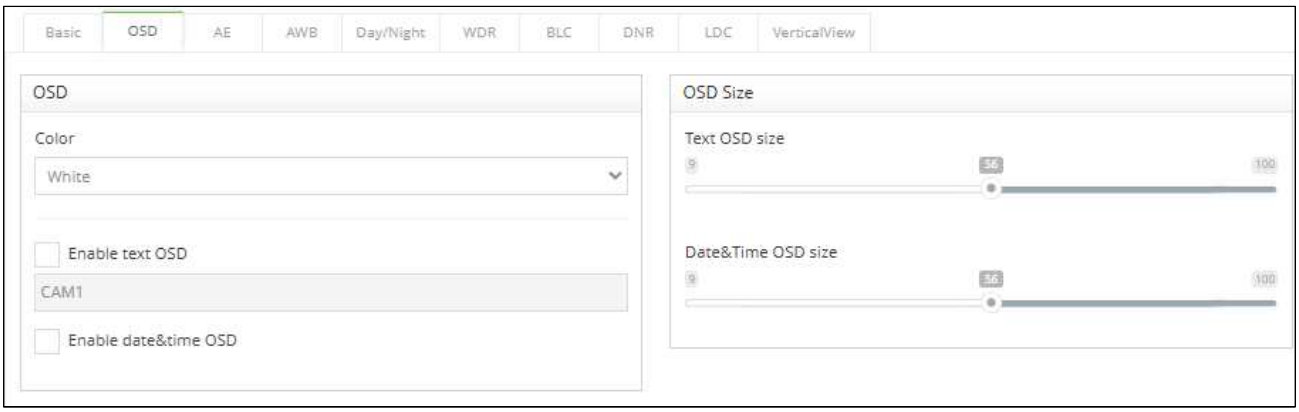
The image appearance settings allow adjustment of various camera parameters and camera orientation. It is recommended to modify all parameters to achieve optimal image quality for the installation location.



Brightness: Control the brightness of the image.
Contrast: Adjust the contrast of the image.
Saturation: Control the saturation of the image.
Hue: Adjust the hue of the image.
Sharpness: Control the sharpness of the image.
Enable Flip Image: Rotate the camera image 180 degrees vertically.
Enable Mirror Image: Rotate the camera image 180 degrees horizontally. Reflecting a duplicate of the camera image.

OSD

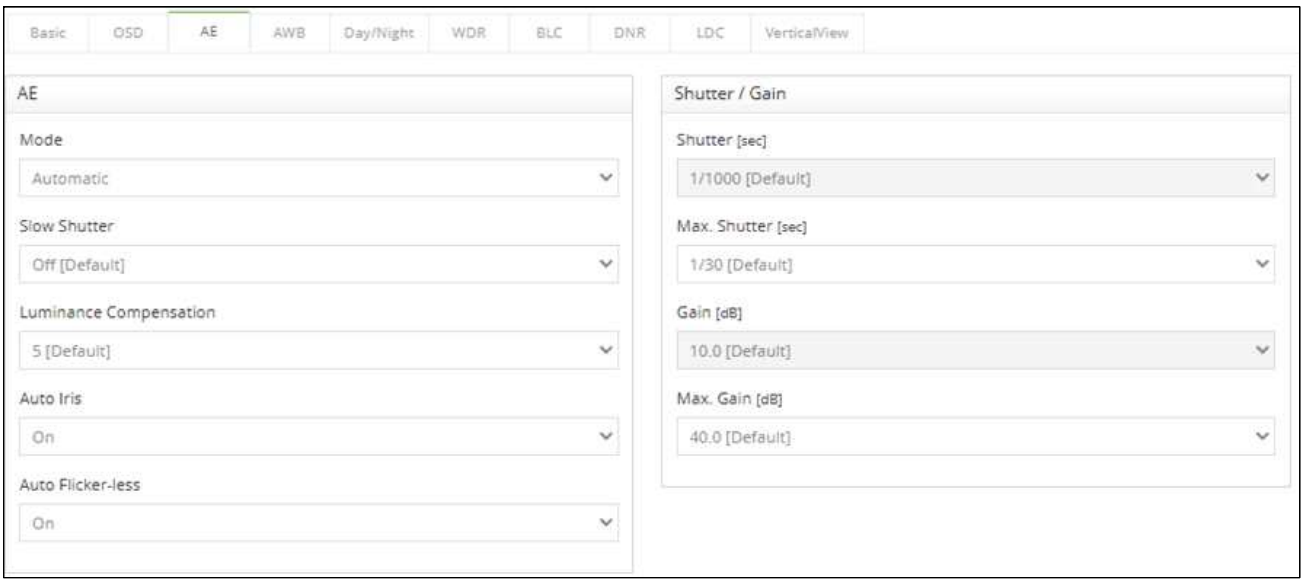
The On-Screen Display (OSD) displays camera status information on the video stream.



Color: Select the color for the OSD text.
Enable text OSD: Display user-defined text, such as the camera name.
Enable date & time OSD: Display the current date and time information from the camera.
Text OSD Size: Adjust the font size of the text OSD.
Day & Time OSD Size: Adjust the font size of the date and time OSD.

AE

Configure the exposure control to meet image quality requirements based on lighting conditions. This camera supports both automatic and manual exposure control modes.
The shutter and gain settings influence the level of motion blur and noise in the image. To adapt to different lighting, available storage space and bandwidth, it is often necessary to prioritize either low motion blur or low noise. This camera allows using different prioritization in normal light and in low light. Shutter speed determines how long the camera sensor is exposed to light and is measured in seconds(s).



Mode: The automatic mode adjusts the sensor's gain, shutter time, and aperture automatically to achieve optimal image brightness. The manual mode allows users to manually control the gain and shutter speed for more precise exposure.
Slow Shutter: A slow shutter allows more light to reach the sensor, helping produce a brighter image in low-light conditions. However, a slow shutter speed can cause moving objects to appear blurry.
Luminance Compensation: A function that automatically or manually adjusts the overall brightness (luminance) of the image captured by the camera. It compensates for lighting variations such as low-light or backlight conditions to ensure that subjects remain clearly visible.
Auto Iris: Controls the shutter speed, gain, and aperture of the mechanical iris lens to adjust the luminance. In this mode, luminance can also be adjusted using the gain and aperture while keeping the exposure time fixed.
Shutter: Controls the gain while keeping the shutter speed fixed to adjust luminance.
Max. Shutter: Adjusts the maximum shutter speed within the specified range.
Gain: The level of amplification applied to the image. A higher gain improves visibility in low-light conditions but may increase image noise.
Max. Gain: Adjust the maximum gain within the specified range.

AWB

Auto White Balance (AWB) ensures colors appear the same regardless of the light source's color temperature. The camera can automatically identify the light source and adjust accordingly. Alternatively, select the light source type from the drop-down list.

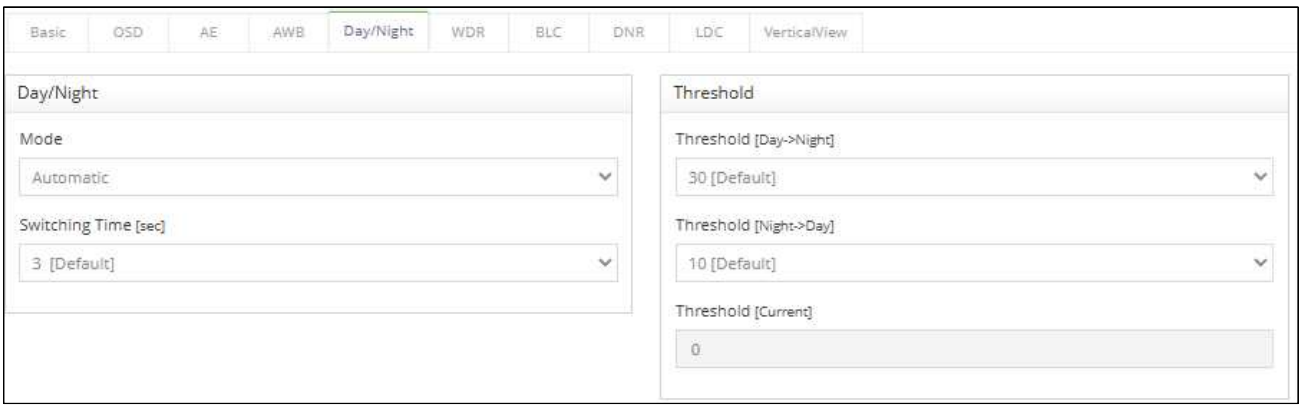
Mode: Configure the options for White Balance. The default setting is ATW-Indoor.

Cb Gain: Adjust the picture output in the blue range. The White balance B gain can be adjusted in the range, where a higher value produces a higher blue image.

Cr Gain: Adjust the picture output in the red range. The White balance R gain can be adjusted in the range, where a higher value produces a higher red image.

Day / Night

The IR cut filter prevents infrared (IR) light from reaching the image sensor. In low-light conditions, such as nighttime or when using an IR lamp, set the mode to Night to increase light sensitivity and allow the camera to capture infrared light. The image will be displayed in black and white in Night mode. Set the mode to Automatic to automatically switch between Day and Night based on lighting conditions.



Mode: Configure the IR cut filter transition mode. Switching Time: Adjust the IR cut filter transition time to the desired dwell time after detecting the transition point. Threshold: Set the threshold level for the IR cut filter based on the installation environment. Ensure the "Threshold [Night → Day]" value is higher than the "Threshold [Day → Night]" value to prevent Day / Night hunting.

WDR

Adjust the Wide Dynamic Range to improve image quality in scenes with both bright and dark areas. This feature adjusts brightness levels using slope and contrast adjustments on the tone curve.

WDR: WDR is controlled by slope and contrast gain on the tone curve as tracking level grade brightness.

Mode: Select the WDR mode that is used.

DWDR : Digital-WDR is a digital technology that enhances image quality in scenes with both bright and dark areas by adjusting brightness and contrast.

Mode: Select the DWDR mode.

Level: Adjust the level of the DWDR effect.

* Note

D-WDR functionality depends on the camera model.

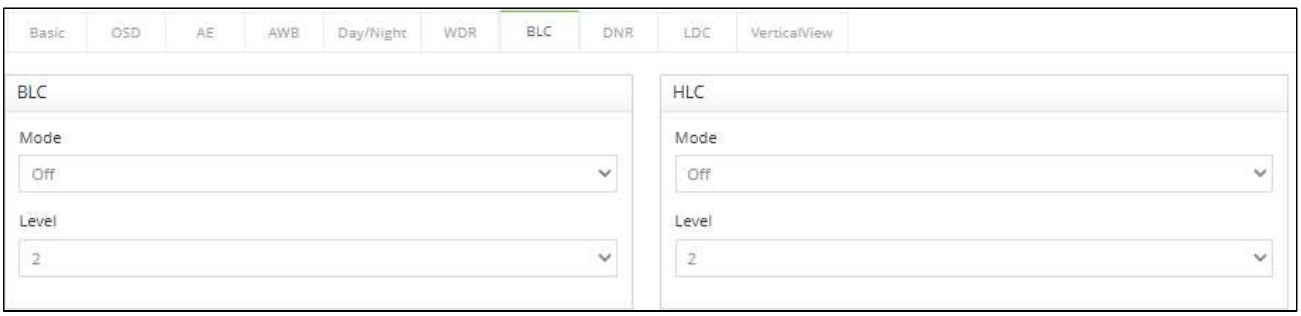
Defog: Automatically detects foggy conditions and provides hight contrast pictures. This feature improves visibility in foggy situations through intelligent image analysis.

Mode: Select the Defog mode.

Level: Adjust the level of the Defog effect.

BLC

Adjust the brightness of subjects that appear dark due to strong backlighting.



Mode: Select the BLC mode to apply.

Level: Adjust the BLC level to optimize subject brightness.

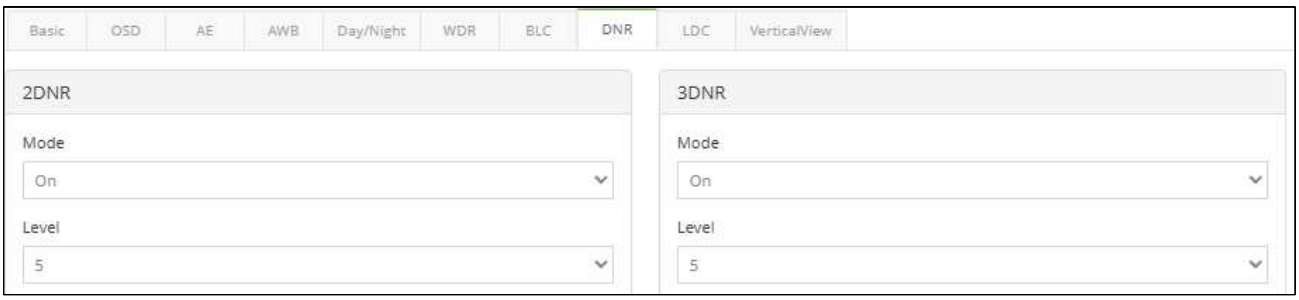
HLC: Reduce the impact of intense light sources, such as headlights or spotlights. The default setting is off.

Mode: Select the HLC mode to apply.

Level: Adjust the HLC level to achieve the desired balance between light and dark areas.

DNR

Reduce image noise to improve overall picture quality.



2D-NR / 3D-NR: The noise reduction (NR) feature reduces image noise to enhance the camera's video quality. The 2D-NR function removes noise within a single frame by analyzing pixel correlation, while the 3D-NR function minimizes noise across multiple frames by utilizing frame memory and analyzing inter-frame correlations.

Mode: The default setting is off.

Level: Select a noise reduction level from Level 1, Level 2, Level 3, or Level 4.

LDC

Lens Distortion Correction Corrects distortions caused by wide-angle lenses to produce a more natural image. Simple-LDC corrects vertical distortions but does not address horizontal distortions. Vertical lines are straightened, but horizontal lines may retain a curved appearance.

Mode: The default setting is off.

Level: Configure one of the available levels.

Note

The functionality of LDC depends on the camera model.

Vertical View

The Vertical View format provides a vertically oriented video stream optimized for monitoring narrow spaces such as corridors, hallways, or aisles. This feature maximizes image quality and minimizes bandwidth and storage usage. For modern HDTV network cameras with a 16:9 aspect ratio, the Corridor Format adjusts the video to a 9:16 aspect ratio.

Mode: The default setting is off.

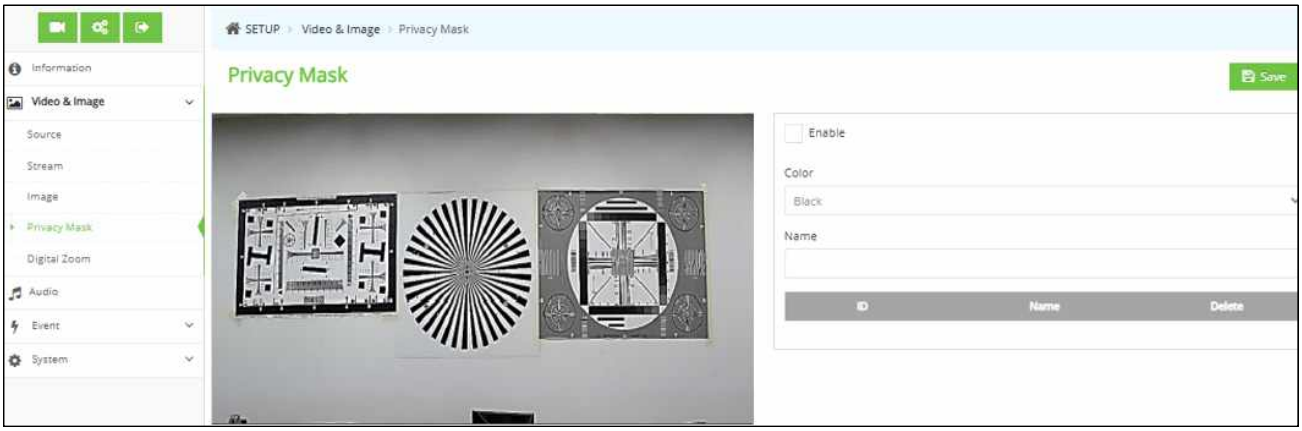
Rotation: Configure the rotation degree as required.

Video & Image > Privacy Mask

A privacy mask is an area of solid color that prohibits users from viewing parts of the monitored area. The Privacy Mask List shows all the masks that are currently configured in this product and indicates if they are enabled.

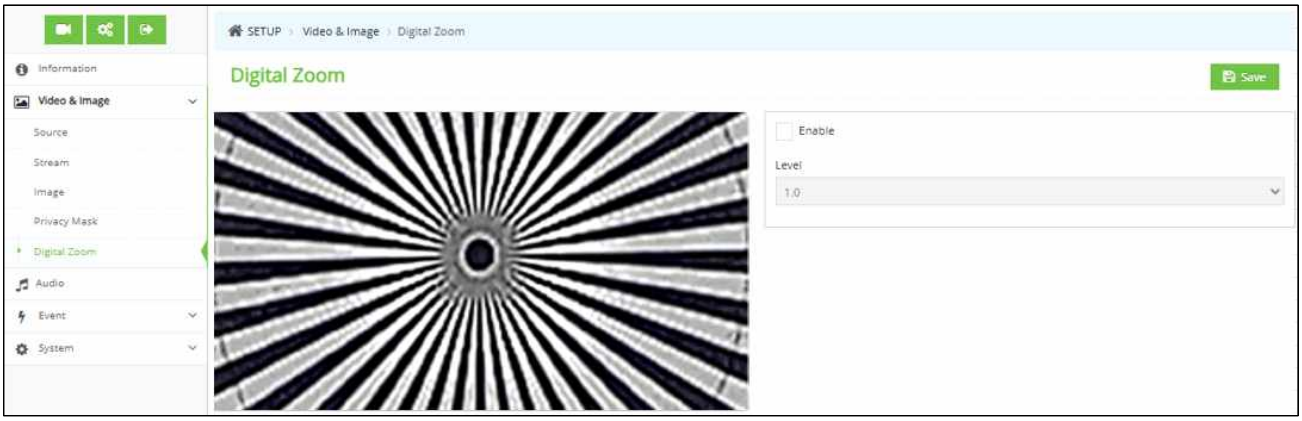
New mask can be added, resized with the mouse, and given a mask name. The color of the privacy mask will be set automatically after Save. To set the privacy mask,

1. Check the 'Enable' privacy mask checking box.
2. Right-click on the screen and specify the area.
3. Enter the name and click Save.
4. To delete a mask area from the list, click the X icon

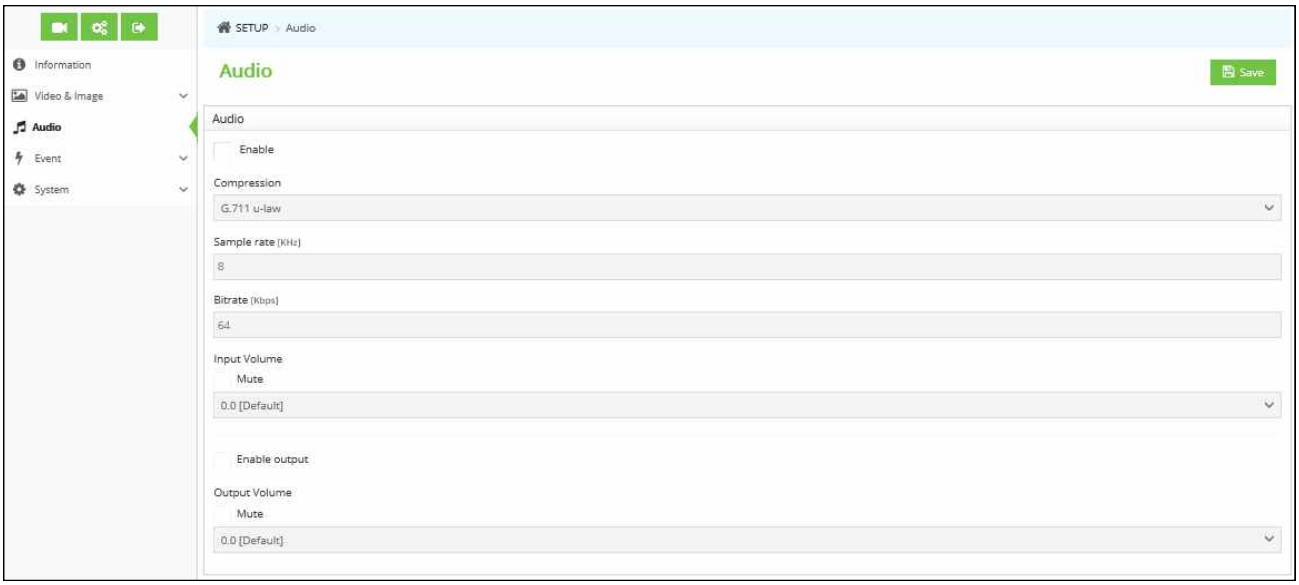


Video & Image > Digital Zoom

Click the 'Enable' checkbox to activate digital zoom. The digital zoom ratio can be set from x1 to x12. To adjust to the desired zoom level, click the 'Save' to finalize the setting.



Audio



Audio: Enable audio by clicking the enable audio checkbox. This page provides instructions for configuring the camera's basic audio settings. The camera supports full-duplex audio, allowing simultaneous transmission and reception of audio in both directions.

Compression: G.711 is the international standard for encoding wired-telephone audio on a 64kBit/s channel. It uses PCM (Pulse Code Modulation) with an 8 kHz sample rate. The default setting is G.711 μ-law.

Sample rate: Indicates the number of times per second the sound is sampled. The default setting is 8 kHz.

**** Note***

G.711, also known as Pulse Code Modulation (PCM), is a very commonly used waveform codec. G.711 uses a sampling rate of 8,000 samples per second, with the tolerance on that rate 50 parts per million (ppm). Non-uniform quantization (logarithmic) with 8 bits is used to represent each sample, resulting in a 64 kbit/s bit rate. There are two slightly different versions; μ-law, which is used primarily in North America, and A-law, which is in use in most other countries outside North America. G.711 μ- law tends to give more resolution to higher range signals while G.711 A-law provides more quantization levels at lower signal levels.

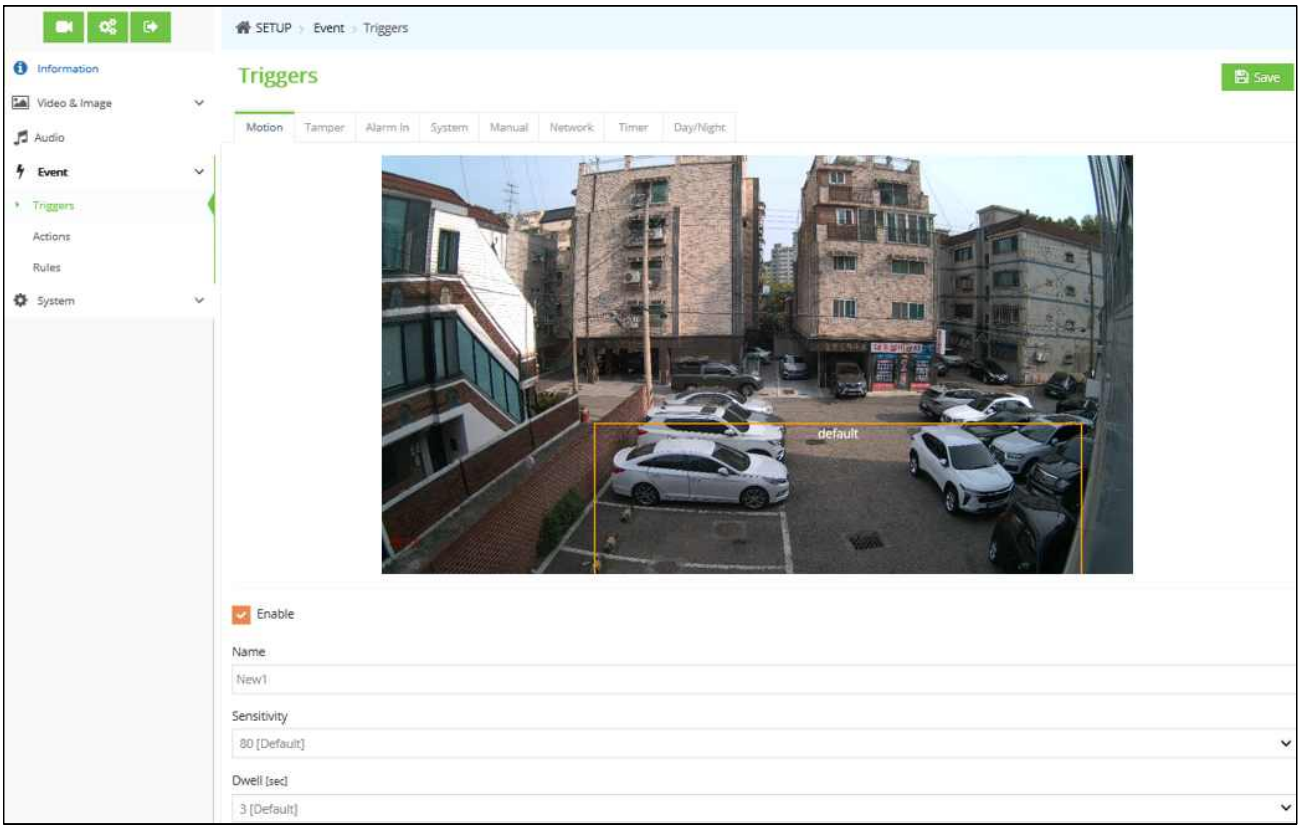
Input volume: The Input volume is adjustable within a range of -12.00 to 12.00 dB, with a default setting of 0 dB. Use the Mute box to disable the audio input if needed.

Output volume: The Output volume is adjustable within a range of 9 to -24 dB, with a default setting of 0 dB. Use the Mute box to disable the audio output if needed.

Event > Triggers

Motion

Motion detection generates an alarm whenever movement occurs (or stops) in the viewer. A total of 8 Motion/Mask areas can be created and configured.



Name: Enter a name of motion or mask area.

Sensitivity: Adjust the sensitivity level for motion detection.

Dwell time: Configure how long the motion or mask signal remains active as an input signaling source.

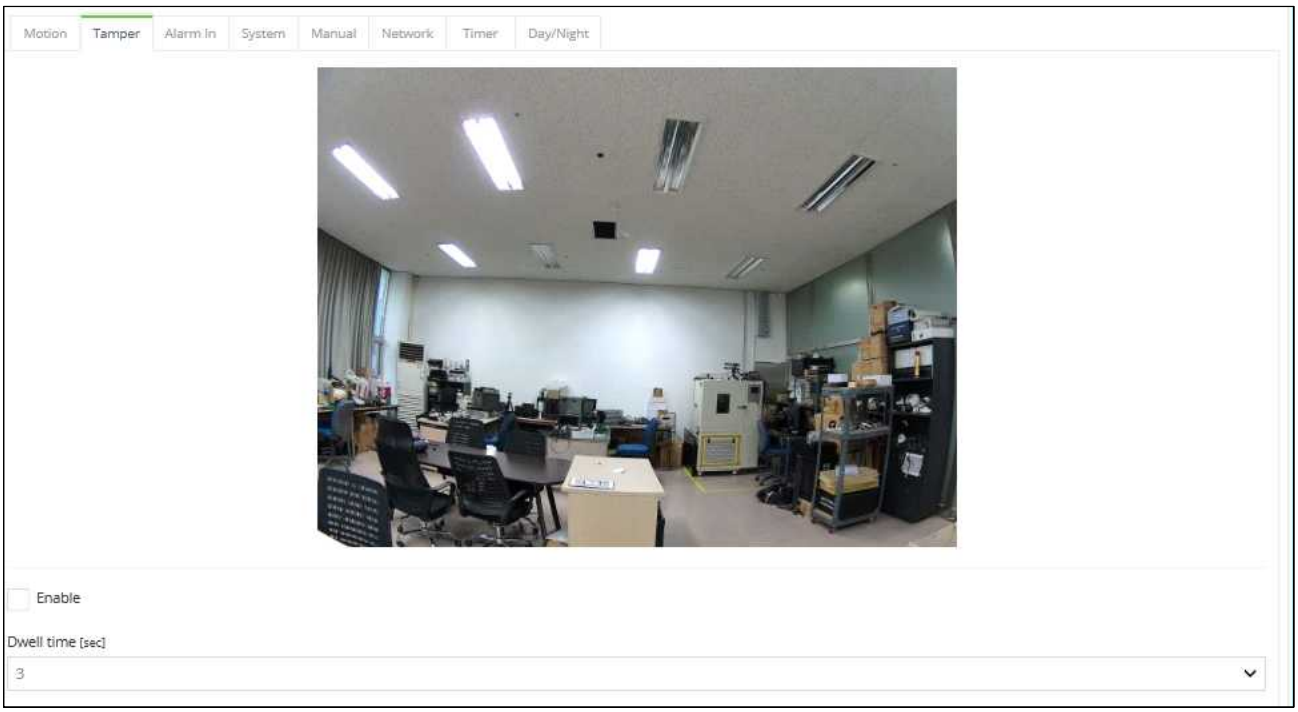
Once motion detection areas are configured, this camera can perform actions when motion is detected. Possible actions include uploads, alarm out and emailing. To create a motion or mask area, follow steps:

1. Right-click the mouse to access the menu.
2. Select Create detection area or Create masking area from the menu.
3. Click and drag the mouse to designate a motion area.
   - Create detection area — define areas where motion should be detected.
   - Create masking area — define areas where motion should be ignored.

To delete a motion or mask area, click the delete button.

Tamper

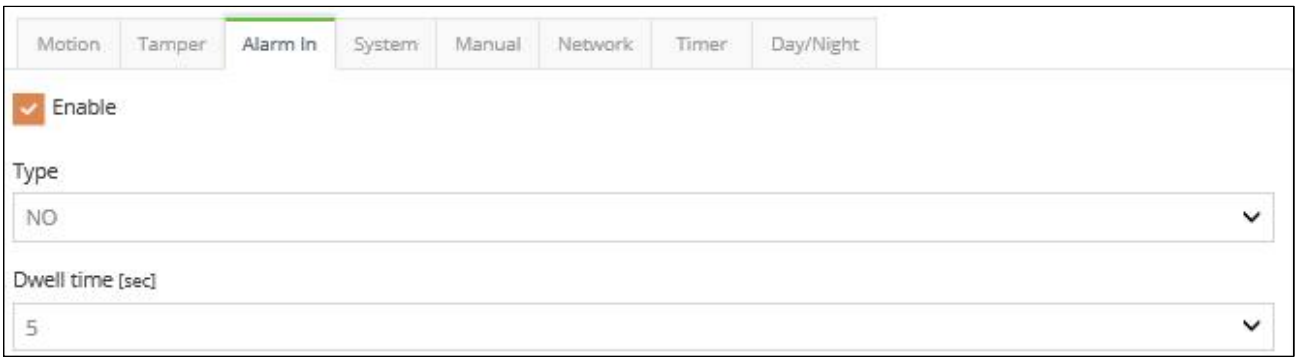
Detects if the camera's view is obstructed, rotated, or tampered with. When such an event occurs, a warning is immediately sent to the administrator.



Dwell time: Configure the duration that the tampering event must persist to trigger an alarm.

Alarm In

Enable alarm in by checking the 'Enable' checkbox.



Type: The default setting is NO.

• **NO**: Normally Open

If the normal state of a pushbutton connected to an input is an open circuit, the input state remains inactive as long as the button is not pushed.

• **NC**: Normally Close When the button is pushed, the circuit is grounded, and the input's state changes from its normal state (grounded circuit) to an active state.

An input on the camera is in an open circuit state when disconnected or when there is a voltage.

Dwell time: Configure the duration that the alarm input signal must persist to act as a valid input signaling source.

** Note*

The total number of alarm in is depends on camera model.

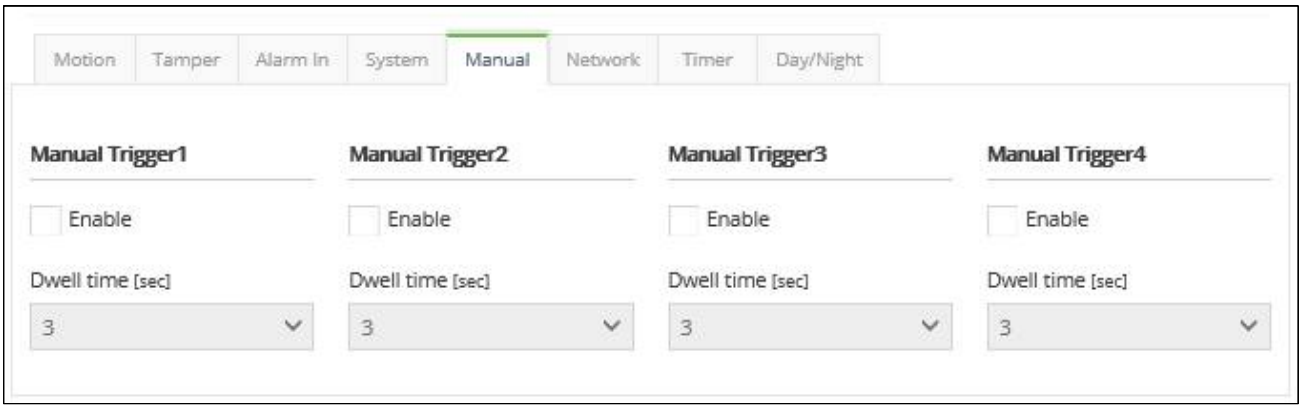
System

This is used to trigger the event every time the Network Camera is started.

Dwell time: The default setting is 3 seconds.

Manual

The Manual Trigger features an alarm out signaling, JPEG file transfer to FTP server, and sends email to SMTP server whenever operator clicks Manual Trigger button in the Live View window.



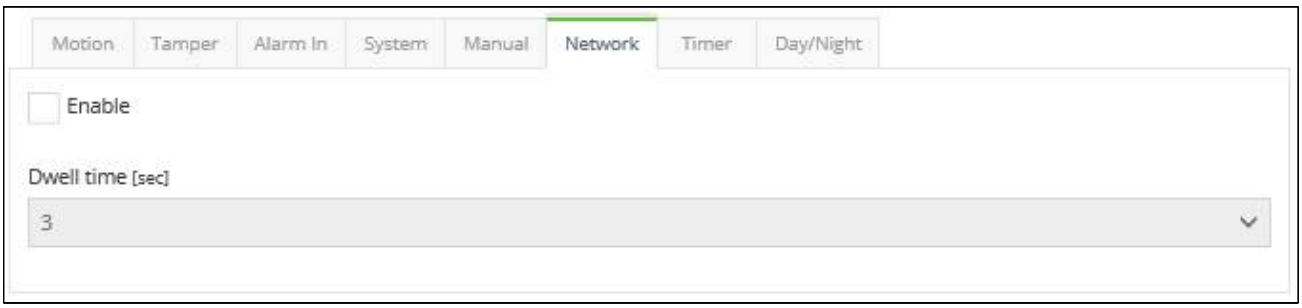
Dwell time: The default setting is 3 seconds.

** Note*

Dwell time means how long time the alarm output signal hold on as an output signaling source.

Network

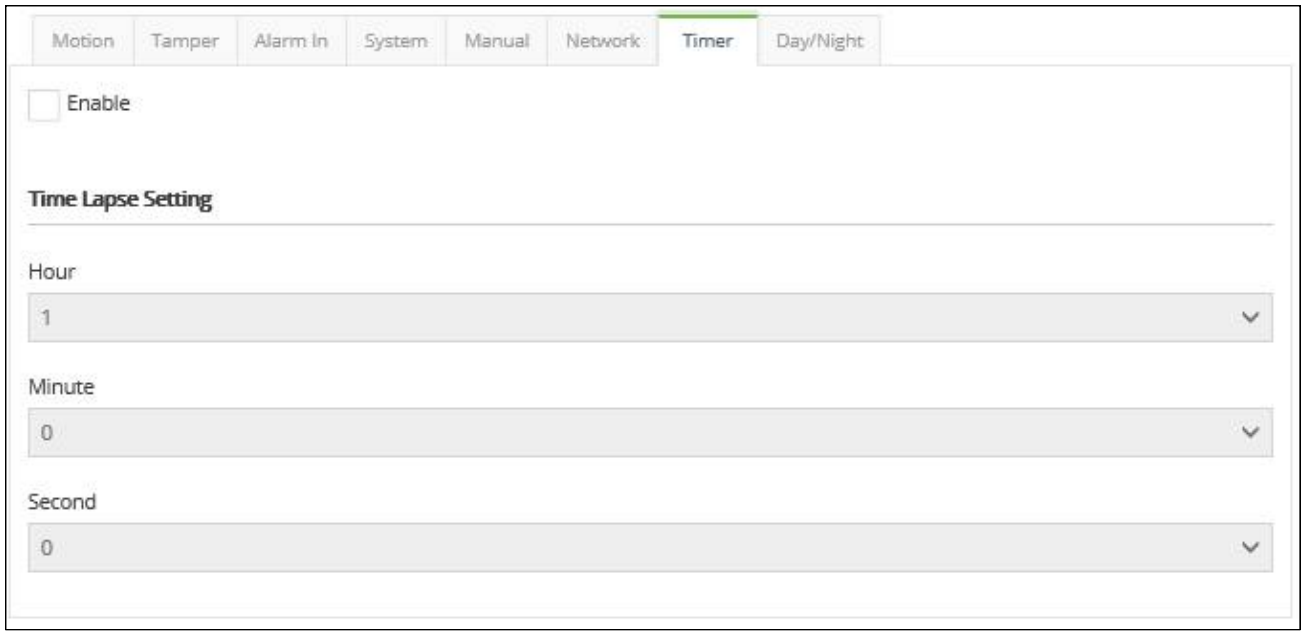
This is used to trigger the event every time the network connection fails. Click the checkbox to activate the Network Loss event.



Dwell time: The default setting is 3 seconds.

Timer

This is used to trigger the event according to time settings. Click the checkbox to activate the Time Laps Setting.

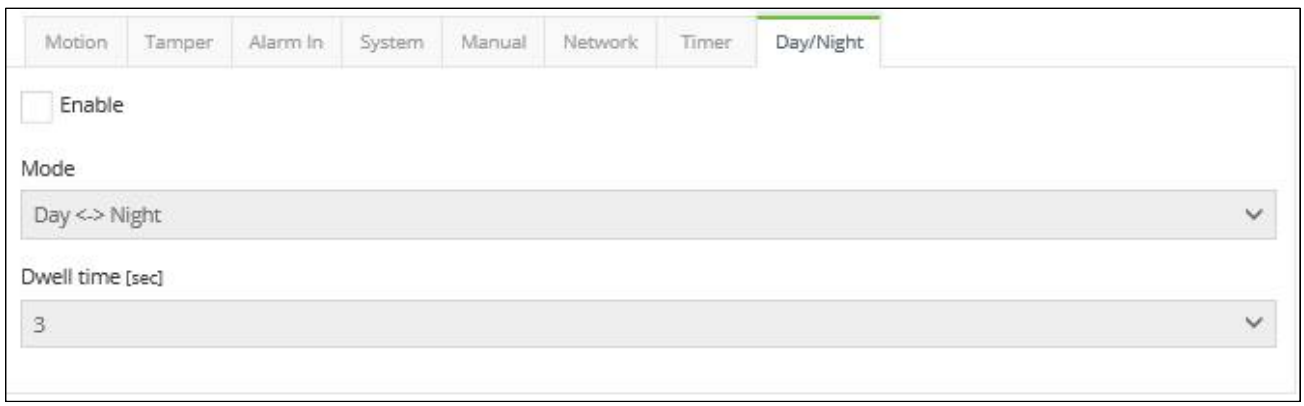


Time Laps Setting: The default setting is 3 seconds.

- Hour: Set the event trigger every hour.
- Minute: Set the event trigger every minute.
- Second: Set the event trigger every second.

Day/Night

This is used to trigger the event every time Day and Night exchange. Click the checkbox to activate the Day/Night event trigger.



Dwell time: The default setting is 3 seconds.

Event > Actions

Alarm Out

This page allows you to configure the alarm output supported by the camera. Port can be given as Normally Open or Normally Close state.

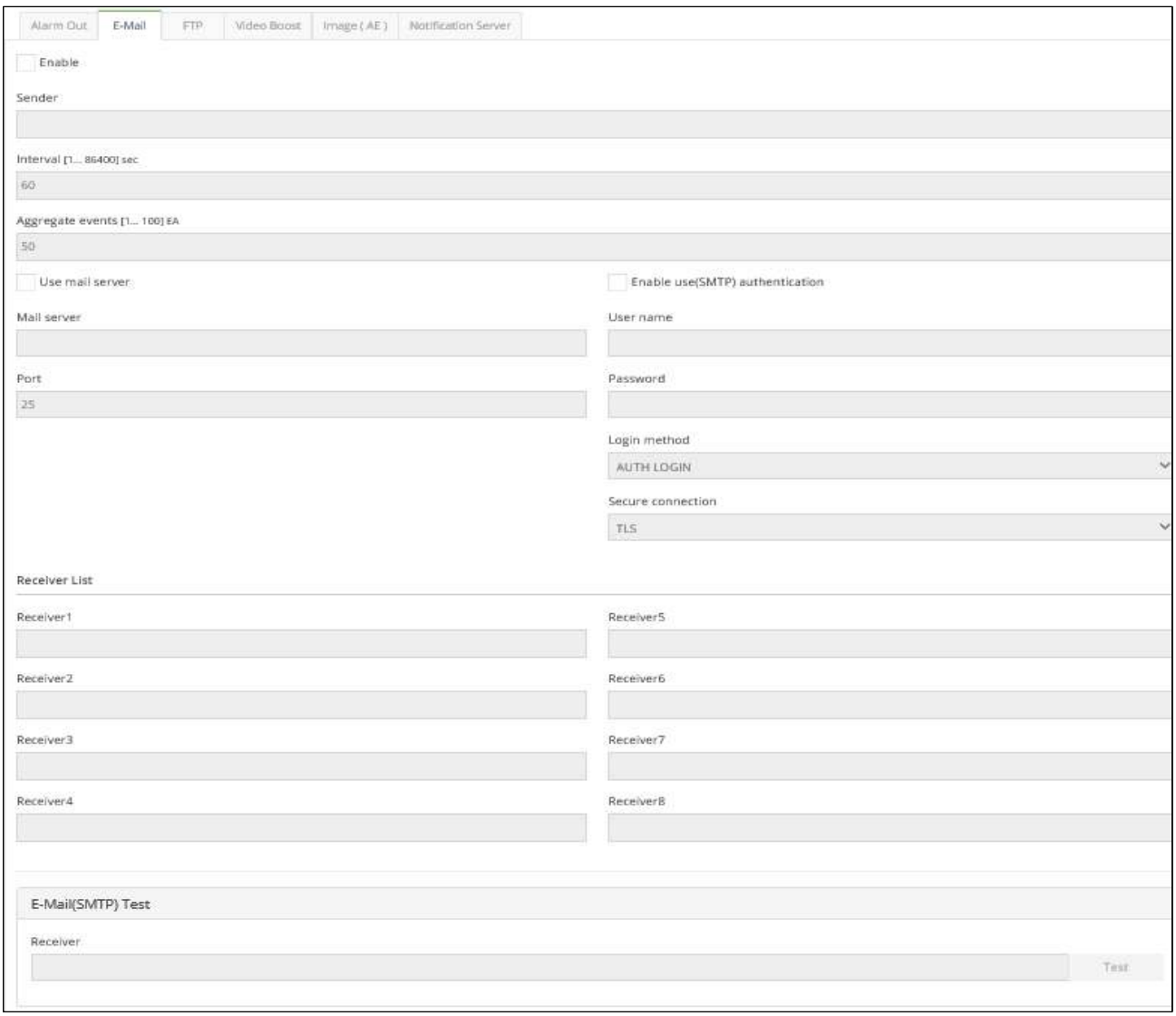
Type: The default setting is NO.

**** Note***

The total number of alarm out is dependent on camera model.

E-Mail

Use the Simple Mail Transfer Protocol (SMTP) server to send an email notification when an event server is activated. The camera can be configured to send event and email messages via SMTP.



Sender: Click in the Sender box and enter the E-mail address as the sender.
Interval: Enter the E-mail sending time interval after event occurred.
Aggregate events: Enter the number of events for E-mail sending. If the event numbers are reached the setting value, E-mail sending is available.
Use mail server: Click the Use mail server checkbox and provide the following information for E-mail server. Mail Server: Enter the host names or IP addresses for your mail servers in the fields provided.

** Note*

If a host name is used, a valid DNS server must be specified in the Network-Basic settings.

Port: Enter the SMTP server port number for the SMTP Server. The Port number can be adjusted in the range 1-65535. The default setting is 25.

** Note*

- If your mail server requires authentication, click the Use (SMTP) authentication checkbox for use authentication to log in to this server.

- Please consult with your network administrator, if you want to change the port number.

Enable use (SMTP) authentication: If your mail server requires authentication, click the Use (SMTP) authentication checkbox for use authentication to log in to this server.
User name: Enter the User name as provided by your network administrator.
Password: Enter the Password as provided by your network administrator.
Login method: Select one for SMTP authentication method allowed.

** Note*

- If a PLAIN or LOGIN mechanism is negotiated, the camera sends user name and password to the SMTP server.

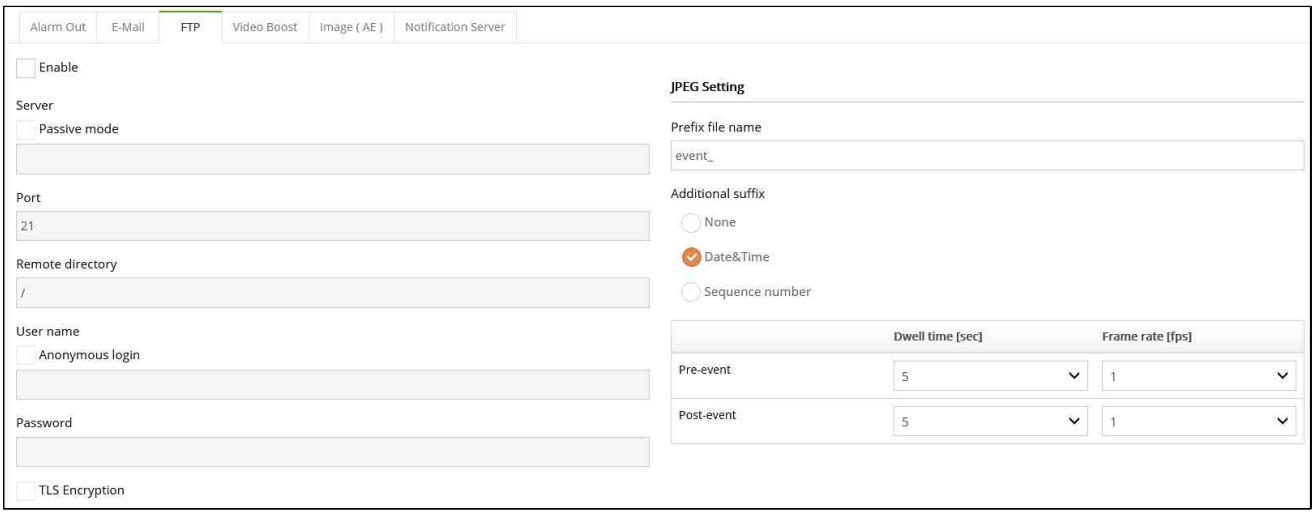
- The LOGIN mechanism is supported by Microsoft, as well as by some other clients. Most other clients support the PLAIN authentication mechanism.

- Since the vast majority of Email clients support only PLAIN or LOGIN, mail server administrators will probably want to consider using STARTTLS to provide an encryption "tunnel" between the client and server, to protect the user name and password.

Receiver List: Enter the recipient's E-mail address as the receivers. Receiver1~8: Enter the recipient's E-mail address as the receiver to test.
E-Mail (SMTP) Test: Enter the recipient's E-mail address and click the Test button to test that the mail servers are functioning and that the E-mail address is valid. When the setup is complete, the connection can be tested by clicking the Test button.
Receiver: Enter the recipient's E-mail address as the receiver to test.

FTP

FTP notification will save a file on the specified FTP server. Click the Enable FTP checkbox and provide the following information for FTP notification.



Server: Enter the IP address or host name of the target FTP server.

Passive Mode: Under normal circumstances the network camera simply requests the target FTP server to open the data connection. Checking this box issues a PASV command to the FTP server and

establishes a passive FTP connection; whereby the network camera actively initiates both the FTP control and data connections to the target server. This is normally desirable if there is a firewall between the network camera and the target FTP server.

Port: Enter the port number used by the FTP server. The Port number can be adjusted in the range 1-65535. The default setting is 21.

Remote directory: Specify the path to the directory where the uploaded images will be stored. If this directory does not already exist on the FTP server, there will be an error message when uploading.

User name: Enter the User name as provided by your network administrator.

Anonymous login: Click the Anonymous login checkbox to permit anyone to access FTP server.

Password: Enter the Password as provided by your network administrator.

**** Note***

If you permit login to the FTP server by anyone without a password, click the Anonymous login checkbox.

JPEG Setting: Configure the JPEG image to send the FTP server.

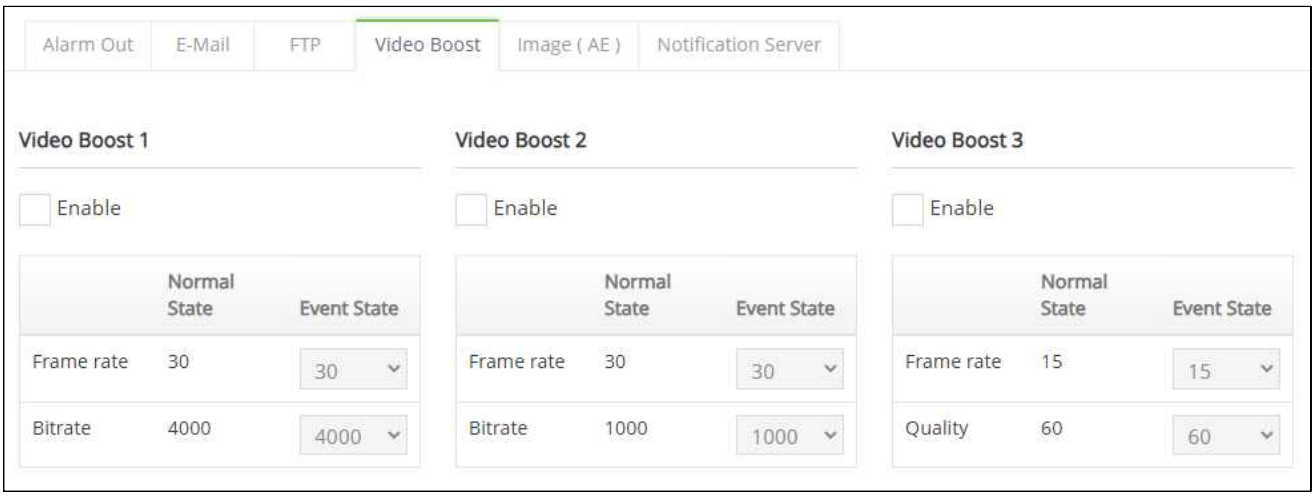
Prefix file name: Click in the Prefix file name box and type a name for JPEG image file (1 to 32 alphanumeric characters).

Additional suffix: Provide additional information for JPEG image file. Pre-event: Defines how many JPEG files will be made, along with the dwell time and frame rate, before the event is generated.

Post-event: Defines how many JPEG files will be made, along with the dwell time and frame rate, after the event is generated.

Video Boost

When the camera detects an event based on the event rule settings, it will boost the streaming performance according to each video stream setting.



Normal State: Display the current frame rate and bitrate.

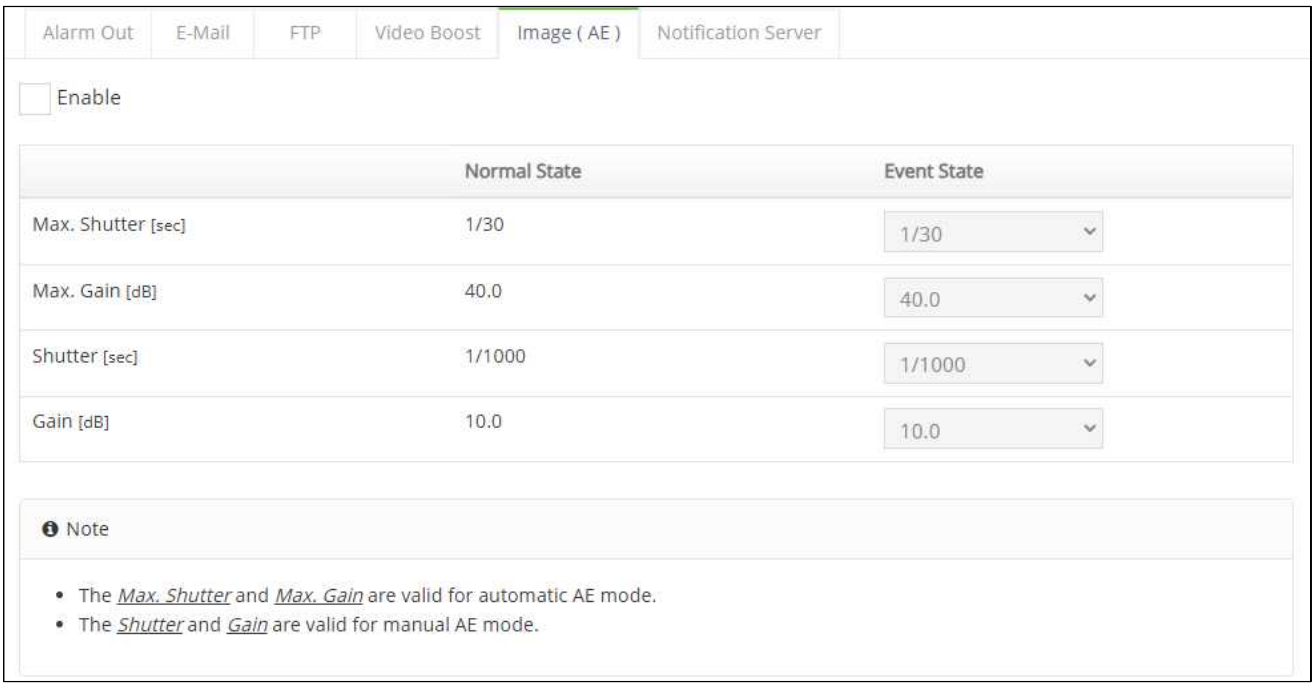
Event State: Set the frame rate and bitrate in video boost mode.

** Note*

The total number of video boost is dependent on the camera model.

Image (AE)

When this camera detects an event according to event rule setting, this camera will change the Shutter and Gain state.



Normal State: Show the normal state Shutter and Gain values.

Event State: Set the Shutter and Gain values in the event state.

**** Note***

The function of Image (AE) is dependent on camera model.

Notification Server

When this camera detects an event, this camera will inform camera event into specified server.

Type: Select command type.

Server URL: Enter server URL.

Username: Enter server user name.

Password: Enter password of the server.

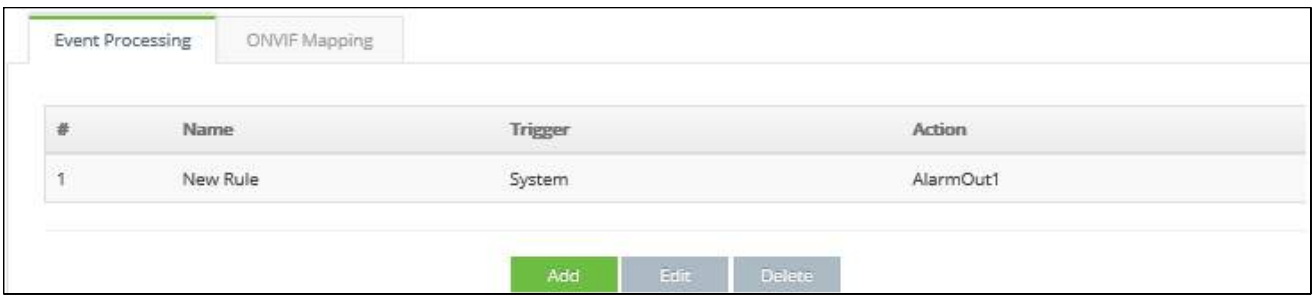
Notification Test: Enter the message and click the Test button to check that the servers are functioning.

Event > Rules

This page shows current configuration status when event is activated. The common event actions will upload images to a specified destination or send an email or active an output port.

Event Processing

An event processing is a set of parameters describing how the camera will perform certain actions. Event type may be set up as Triggered according to requirements.



Name: Show the descriptive name provided by the user.

Trigger: Show the source of event type as Alarm-In, Manual Trigger, VMD, and Etc. configured by the user.

Action: Show the destination of event output as SMTP server, FTP server, Alarm-out port, Audio alert and SD record (depending on models).

** Note*

To add new event, click the Add button. This button opens new dialog window, which are used to make all the necessary settings for the new event map.

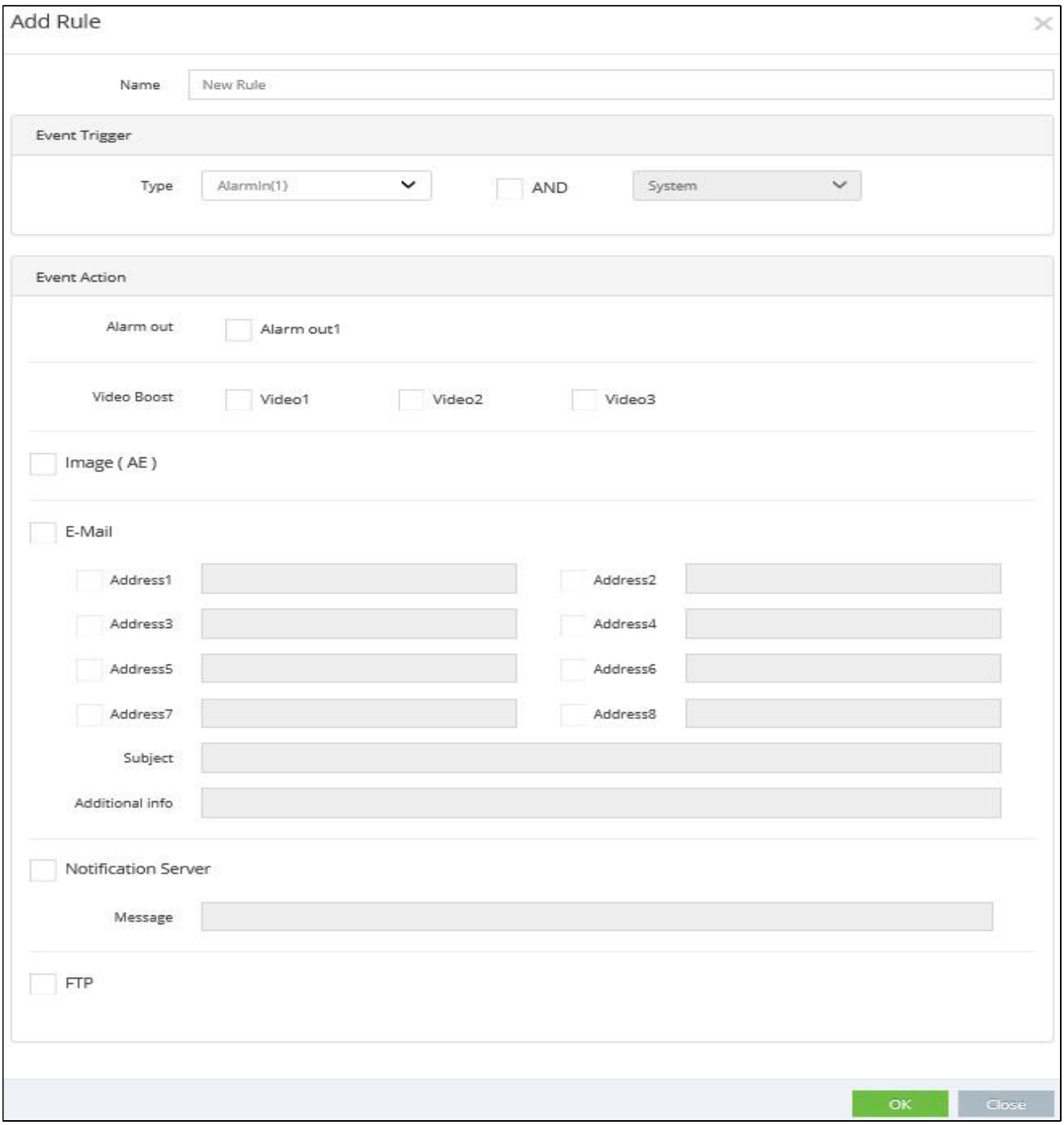
Add: To add a new event map list, select it and click the Add button.

Edit: To modify an existing event map list, select it and click the Modify button.

Delete: To delete an event map list, select it and click the Delete button.

Add Rule

Event Add Rule page provides how to configure the event action if there is event triggering such as Alarm-In, Manual trigger, Motion, and Etc.



Name: Enter a name for the event (1 to 31 alphanumeric characters).

Event Trigger: Display the type of event source to be configured.

Type: Select the event source type. To add a trigger condition for the event action, check the And box and select one or more tigger types.

Event Action: Specifies the actions the camera will perform when the event is triggered.

Alarm out: Enable the alarm output port by selecting the 'Alarm output1' checkbox.

Video Boost: Enable the Video Boost stream by checking the checkbox.

Image (AE): Enable the Shutter and Gain state change by selecting the checkbox.

E-mail: Enable email notifications by checking the 'Email' box. To include recipients, check the box next to each email address.

* Note

If you want to include an additional message in the email, click the additional info box and enter your message (0 to 255 alphanumeric characters).

Notification Server: Enter the message to notify the server. FTP: Enable image uploading to an FTP server by checking the FTP box. Image will be uploaded in JPEG format.

ONVIF Mapping

An ONVIF mapping is a set of parameters describing ONVIF standard how the camera will perform certain actions.

Event Topic: Describe the event topic on this camera.

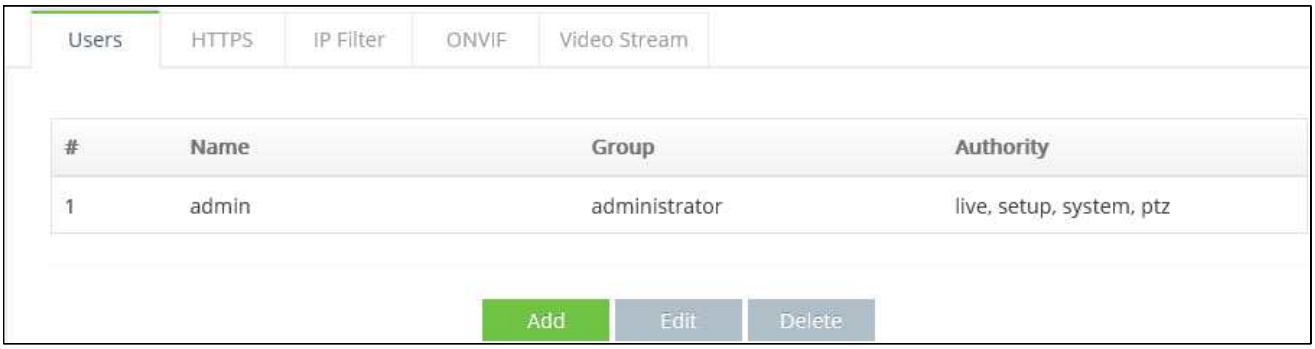
Event Notification: Indicate the selected event type.

Edit: Select one of the event notification types.

System > Security

Users

User accounts can be added or modified or removed. The authority depends on the user group and automatically shows the permission status to access the menus.



Name: Display the name which registered to access the camera.
Group: Display how the assigned permission given to users.
Authority: Display the permission status to access the menus.

- Click the Add, Edit, or Delete button for managing user account.

Add User

1. Click the Add tab. A new pop-up window appears.
2. Click in the Name box and type a new user name (1 to 14 alphanumeric characters).
   - User names are not case-sensitive.
3. Click in the Password box and type a password (1 to 8 alphanumeric characters).
   - Passwords are case sensitive.
4. Click in the Confirm password box and retype a password.
5. Click in the Group box and select one of the groups you wish to assign to the user.
6. Click the OK button to save the settings and add a new user.

Edit User

1. Select one of the User Name in the User List you want to modify.
2. Click the Edit tab. A new pop-up window appears.
3. Click in the Password box and type a password (1 to 8 alphanumeric characters).
   - Passwords are case sensitive.
4. Click in the Confirm password box and retype a password.
5. Click in the User Group box and select one of the groups you wish to assign to the user.
6. Click the OK button to save the settings and modify the user.

To delete a user

1. Select one of the User Names in the User List you want to remove.
2. Click the Delete tab. A dialog box appears with a confirmation message.
3. Click the OK button. The user profile is removed from the User List.

HTTPS

Connection mode: The default setting is HTTP & HTTPS.

• **HTTP**: The sensitive data will be transfer without encrypted during transmission. Support a URL that only starts with "HTTP://"

• **HTTPS**: HTTPS (Hypertext Transfer Protocol over SSL) is a protocol used to provide the encrypted transmission. Supports a URL that only starts with "HTTPS://"

• **HTTP & HTTPS**: Supports both HTTP and HTTPS simultaneously. You can access the camera using a standard "HTTP:" URL, but sensitive data is not encrypted during transmission. To ensure that sensitive data is encrypted, you must use a secure "HTTPS: " URL.

** Note*

- To ensure security on the internet, all web browsers provide several security levels that can be adjusted for site that use SSL (Secure Socket Layer) technology to transfer data. SSL encrypts communications, making it difficult for unauthorized users to intercept and view user names and passwords.

- SSL requires signed certificates to determine if the web browser accessing the camera has a required authentication. This camera can generate a self-signed certificate using Open SSL. - If you select the HTTP connection policy to HTTP, you cannot access the camera using a URL beginning with "HTTPS:"

- Self-signed certificates are valid for 10 years.

IP Filter

Provides the IP filtering elements such as On/Off, Priority, Policy and IP Ranges. The default setting is disabling.

Enable IP address filtering: Click the Enable IP filtering checkbox to enable the IP address filtering function. This dialog allows adding new allowed/denied IP addresses. Entire IP address ranges (Subnets) can be added directly.

On/Off: Click the checkbox to activate the settings (Priority, Policy, and IP ranges).

Priority: The number represents the priority in case of duplicated IP addresses in each IP range.

Policy: Determines the filtering attribute of the selected IP address.

Start IP: Enter the start IP address to ALLOW/ DENY in the selected IP range.

End IP: Enter the end IP address to ALLOW/ DENY in the selected IP range.

** Note*

To add a subnet of network addresses, use CIDR (Classless Inter-Domain Routing) notation. For example, entering 192.168.1.0/24 will add all the addresses in the range 192.168.1.1 to 192.168.1.254. For more detail, contact the network administrator.

- If accessing the network camera through a proxy server, the IP address of the proxy server must be added as an allowed address.

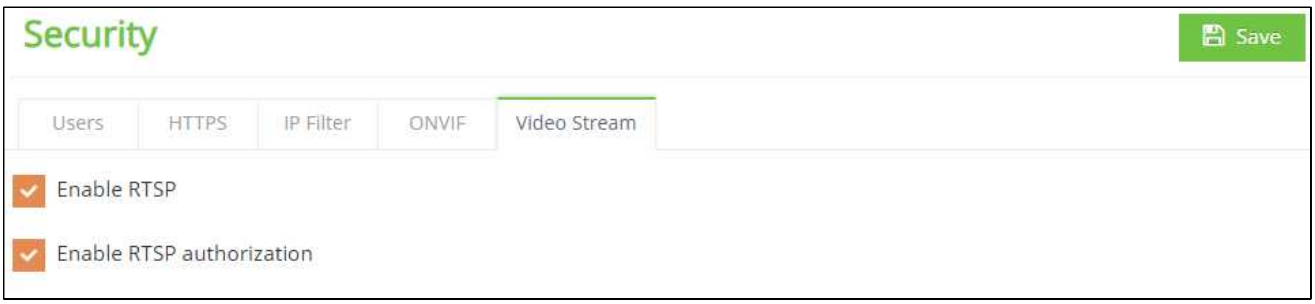
ONVIF

This camera supports an authentication process (Web Service security protocol) using a user ID/Password to connect to ONVIF devices.

Enable WS security: It defines a standard command set that can be used to provide Web Services message integrity and confidentiality. To use this, click the checkbox. The default setting is off, meaning the camera tries to connect to other ONVIF devices without a user ID/Password.

Video Stream

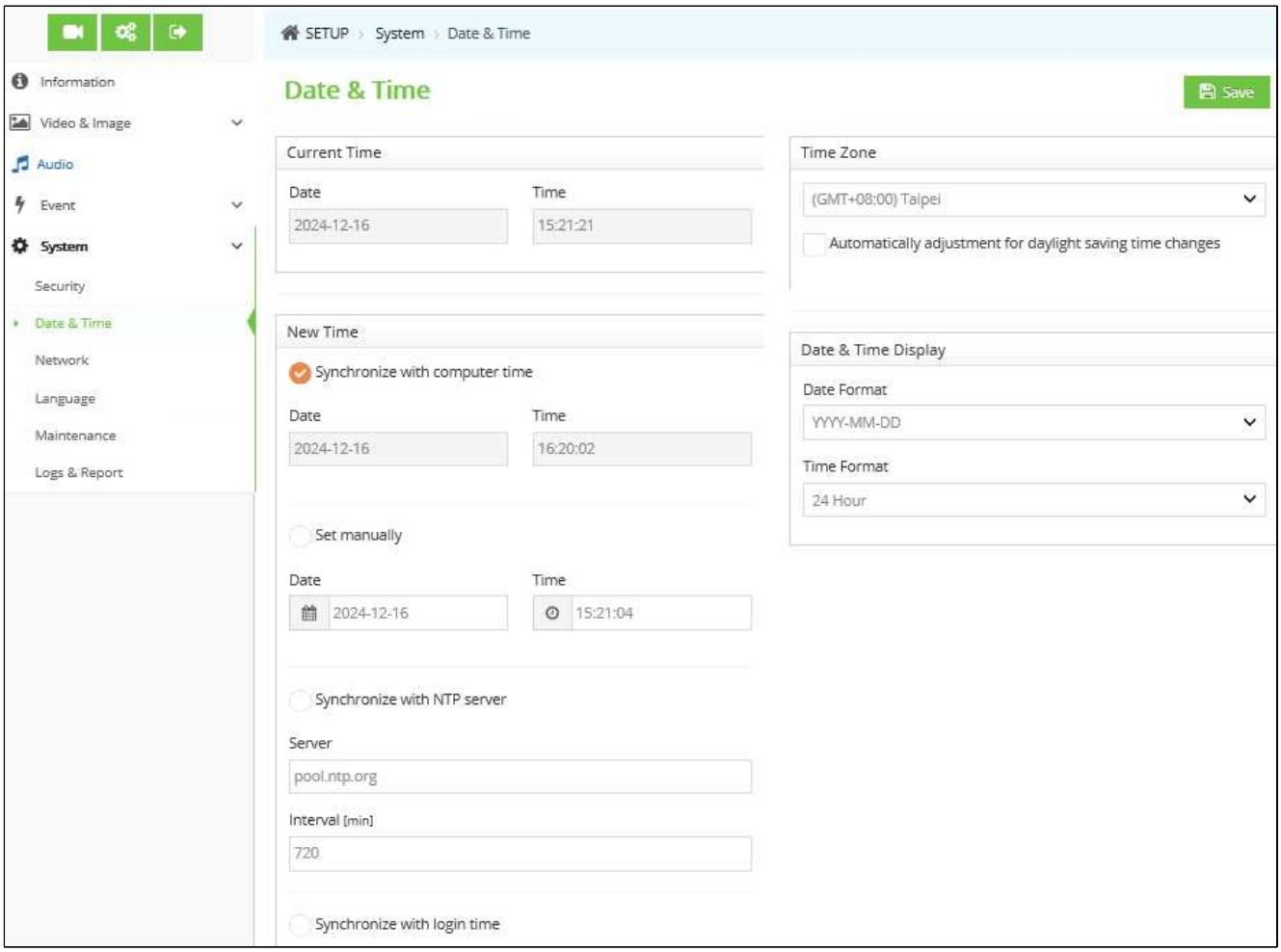
This camera allows secure video streaming by requiring user authentication (ID and password) when using the RTSP protocol.



Enable RTSP: Enables the camera to stream live video via RTSP (Real-Time Streaming Protocol). If this option is disabled, external systems cannot access the RTSP stream.

Enable RTSP Authorization: Activate this feature to require user authentication for RTSP video streaming. When enabled, clients such as video management systems or other devices must enter a user ID and password to access the camera's video stream.

System > Date & Time



Current Time: Display the current date and time.

- **Date**: The default setting is 1970-01-01.
- **Time**: The default setting is 00:00:00.

New Time: Select one of the server times.

- **Synchronize with computer time**: Set the time according to the computer's clock.
- **Set manually**: Use this option to manually enter the date and time.
- **Synchronize with NTP Server**: This option will obtain the correct time from an NTP server every 60 minutes. The NTP server's IP address or host name is specified in the time server.
- **Time Zone**: Select the time zone where the camera is located.

Click the "Automatically adjust for daylight saving changes" checkbox to automatically update the time changes caused by daylight saving.

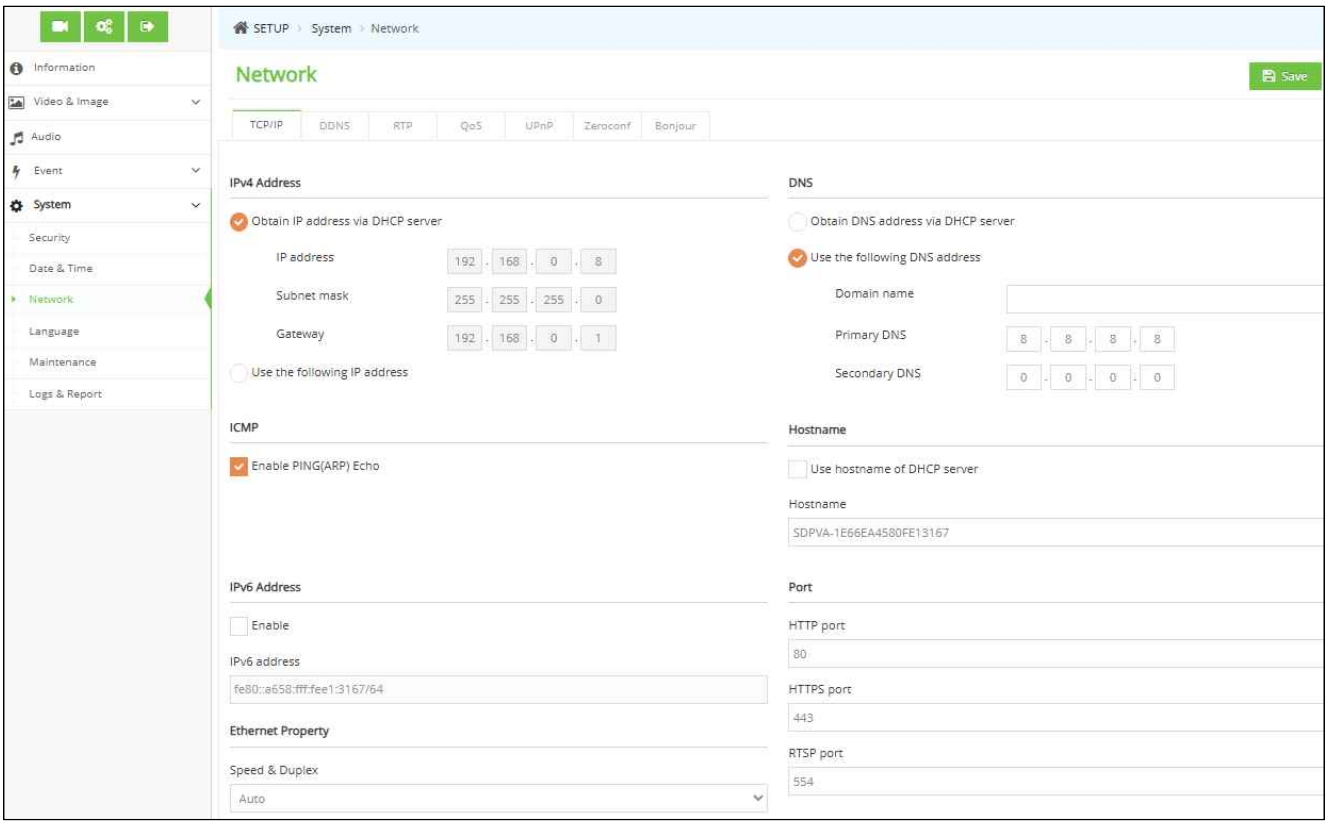
Time zone: The default setting is GMT.

Date & Time Display: Select one of the Date and Time format.

- **Date Format**: The default setting is YYYY-MM-DD.
- **Time Format**: The default setting is 24 hours.

System > Network

TCP/IP



IPv4 Address: The DHCP (Dynamic Host Configuration Protocol) server automatically assigns an IP address to the device if there is a device on the network.

Obtain IP address via DHCP server: Select the checkbox to assign the IP address automatically from DHCP server. Once selected, the remaining settings are read-only.

Use the following IP address: Select this option to assign the IP address manually.

IP address: Specify the unique IP address for the camera on the network.

Subnet mask: Specify the subnet mask for the network that the camera is connected to.

Gateway: Enter the IP address of the default router (Gateway) used to connect devices on different networks.

ICMP (Internet Control Message Protocol): This protocol checks the status of network connections and provides error notifications.

Enable PING (ARP) Echo: Activate this feature to allow the camera to respond to PING or ARP Echo requests, which are commonly used for network diagnostics.

IPv6 Address: Enable IPv6 address configuration by checking this box. Other settings for IPv6 are configured in the network router.

DNS: DNS (Domain Name Service) translates host names to IP addresses.

Obtain DNS server via DHCP server: Select this option to use the DNS server settings provided by the DHCP server automatically. Once selected, the remaining settings are read-only.

Use the following DNS server address: Select this option to manually set the DNS server address.
Domain name: Enter the domain name used by the network camera.

Primary DNS server: Enter the IP address of the primary DNS server. Secondary DNS server: Enter the IP address of the secondary DNS server.

Hostname: Access the camera using a host name instead of an IP address. The host name is usually the same as the assigned DNS name.

Port: Configure the communication ports for web access and video streaming.

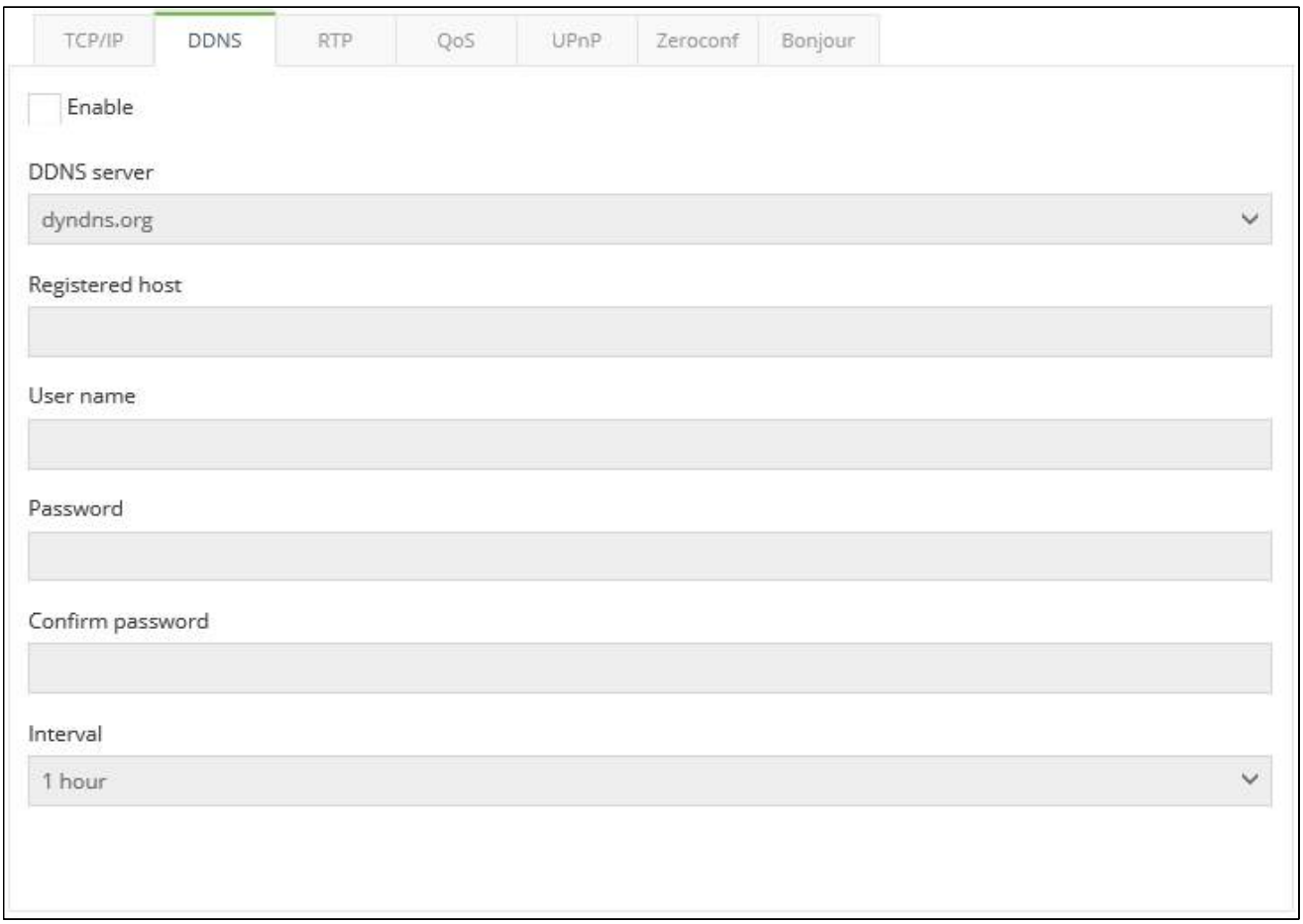
HTTP port: The default port is 80 and can be changed to any port within the range 1024-65535.

HTTPS port: The default port is 443 and can be changed to any port within the range 1024-65535.

RTSP port: The default port for RTSP is 554 and can be changed to any port within the range 1024-65535.

DDNS

The DDNS (Dynamic DNS) provides a unique URL (web address) for accessing the camera over the internet. Use DDNS to assign a host name for easier access to the network camera.



* Note

- Registration at the Dynamic DNS service is required if it has not been previously completed.

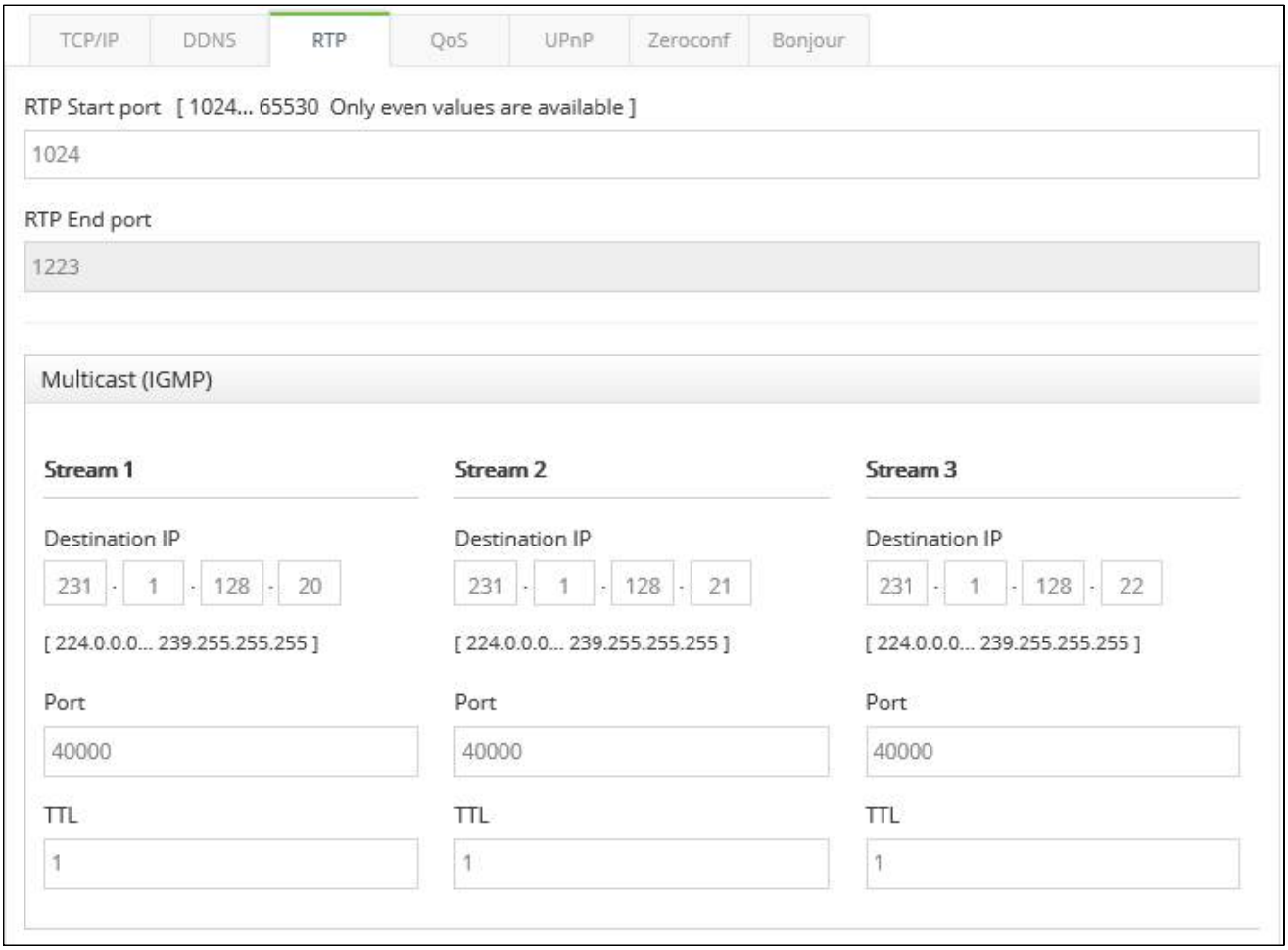
- If the camera is already registered and its IP address changes, the DNS service must be updated with the new IP address.

- Regular updates occur at the set interval, regardless of whether automatic updates are configured. Enable DDNS service by selecting the checkbox.

DDNS server: Enter the name of the DDNS server.
Registered host: Enter the registered host name.
User name: Enter the registered user name for accessing the DDNS server.
Password: Enter the user password for accessing the DDNS server.
Confirm password: Re-enter the user password for confirmation.
Interval: Set the interval for regularly updating the DDNS service. The default setting is 1 hour.

RTP

The RTP Port range specifies the range of ports from which the video/audio ports are selected automatically. This configuration is beneficial when connecting the camera to a NAT router with manually configured port mapping.



* Note

Define the range of ports allowed for RTP unicast or multicast by entering the Start port and End port in the designated fields.

Start port: Specify the starting port number within the range of 3000-39800. The default value is 3000.
End port: Specify the ending port number within the range of 3000-39800. The default value is 30199.

• The value is usually measured in 'hops', i.e. the number of network routers that can be passed before the packet arrives at its destination or is dropped.

Multicast (IGMP): Enable multicast to send data to multiple devices simultaneously.

Destination IP: Enter the IP address where the multicast data will be sent.

Port: Enter the port number for receiving multicast data on the destination device.

TTL (Time To Live): Define the range (in hops) for how far multicast packets will travel through network routers to reach devices within the multicast group.

QoS (Quality of Service)

Prioritize network traffic to maintain smooth video streaming and reliable performance of other network services.

Video/Audio DSCP: Set traffic priority for video and audio data.

Event/Alarm DSCP: Set traffic priority for event and alarm notifications.

Management DSCP: Set traffic priority for network management and control data.

UPnP

The UPnP feature is enabled by default, allowing automatic detection of the network camera by operating systems and clients that support this protocol.

UPnP (Universal Plug & Play): Enable or disable the UPnP feature by toggling the checkbox. The default setting is enabled.

Friendly name: Enter a description (1 to 32 alphanumeric characters) in the Friendly name box. When UPnP is enabled, the camera is automatically detected, and a new icon is added in the format " Model Name-MAC address".

**** Note***

UPnP must also be enabled on the Windows computer. To enable it, open the control panel, go to Add/Remove programs, select Add/Remove Windows Components and navigate to the Networking services section. Click Details, then enable UPnP as a service.

Zeroconf

Zero Configurations Networking (Zeroconf) is a set of protocols that allows devices to automatically create a functional IP network without requiring manual configuration or dedicated servers. Zeroconf enables devices, such as computers and printers to connect to a network without intervention. Without zeroconf, configuring services like Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) or setting network parameters manually can be complex and time-consuming. By default, zoroconf is enabled.

Zeroconf address: The default zeroconf IP is 169.254.xxx.xxx

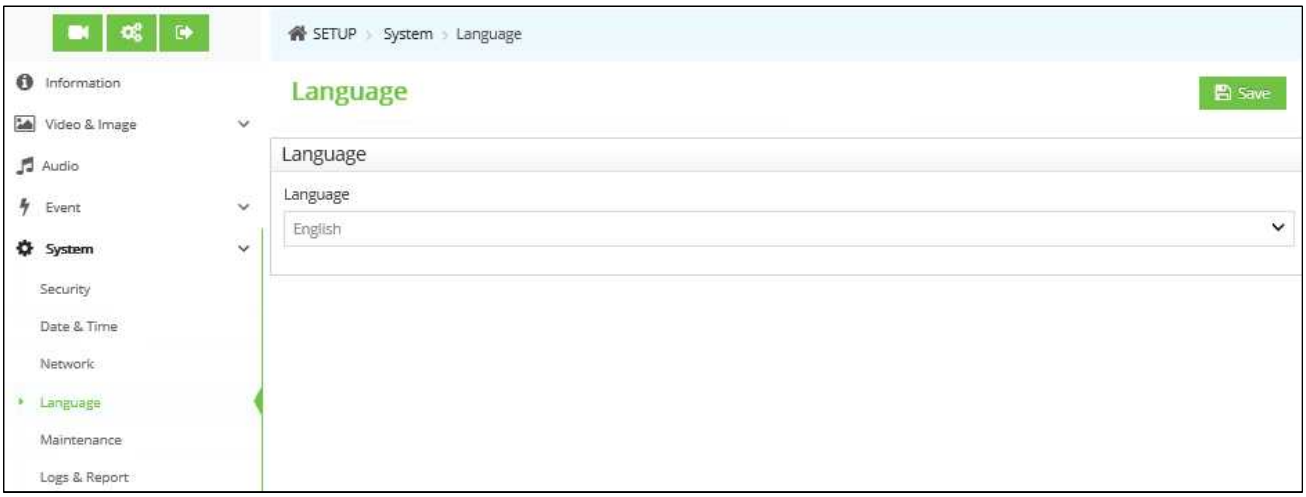
Bonjour

Bonjour is Apple's version of zero-configuration networking (zeroconf), a set of protocols that allows a network device to automatically recognize and communicate with other devices on the network. This streamlined technology enables users with no experience to easily set up and use devices on the network.

Friendly name: Enter your preferred name.

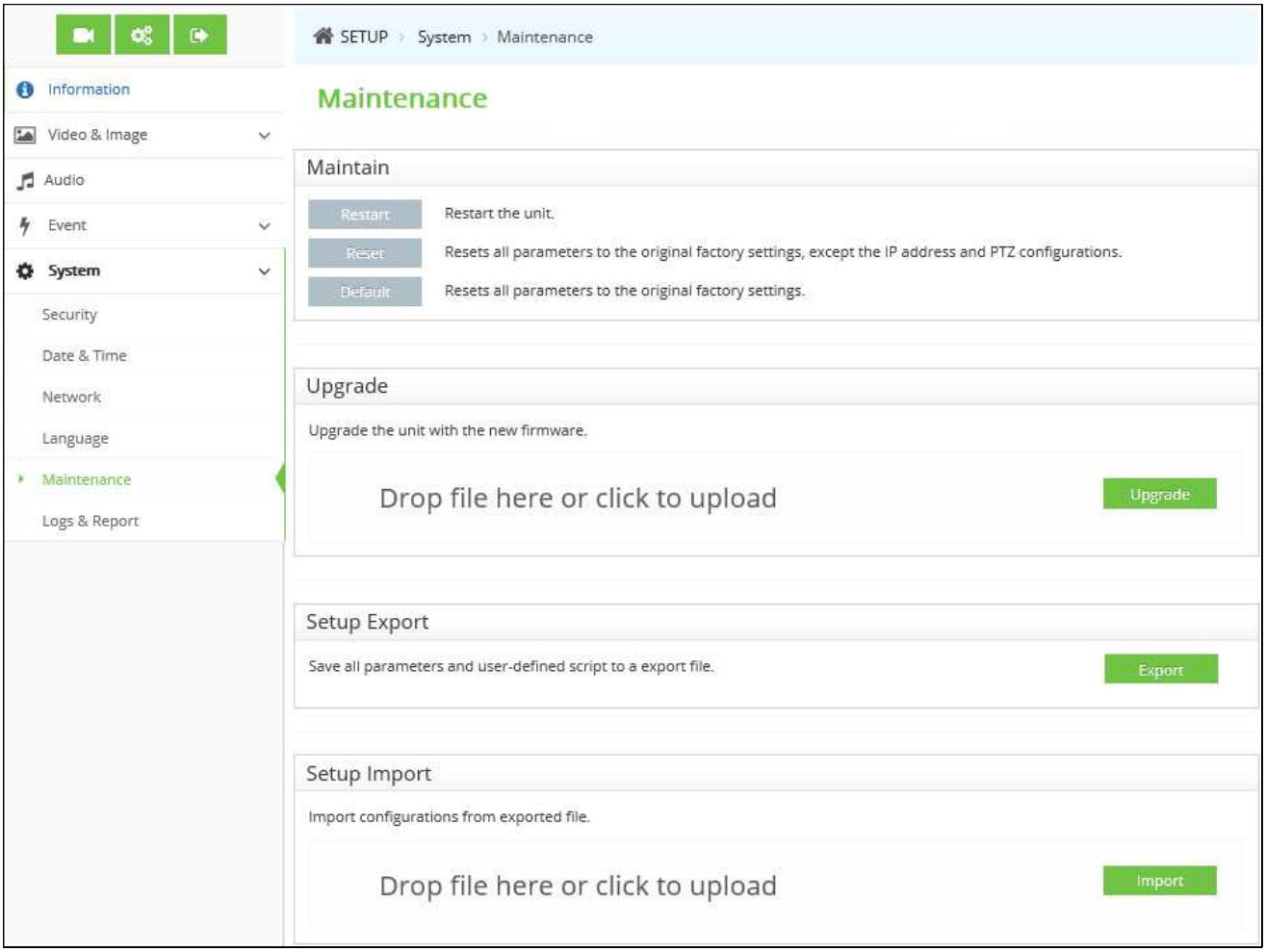
System > Language

The default setting is English.



System > Maintenance

Provides a software reset for the camera when troubleshooting.



Restart: Camera is restarted without changing any settings. Use this method if the camera is not behaving as expected.

Reset: Camera is restarted and most current settings are reset to factory default values, but the following settings does not reset.

- The boot protocol (DHCP or static)
- The static IP address
- The default router
- The subnet mask
- The system time

Default: The Default button should be used with caution. Pressing this returns the camera's settings to the factory default values, including the IP address.

Upgrade: Provides the latest firmware for the camera. When you upgrade the firmware with a file, the camera receives the latest available functionality and enhanced reliability. Follow these steps to upgrade the firmware:

1. Click the Browse button.
2. Browse to the desired firmware file on your computer.
3. Click Upgrade button.

** Note*

Do not disconnect power to the camera during the upgrade. The camera will restarts automatically after the upgrade has completed. (Approximately 2~3 minutes)

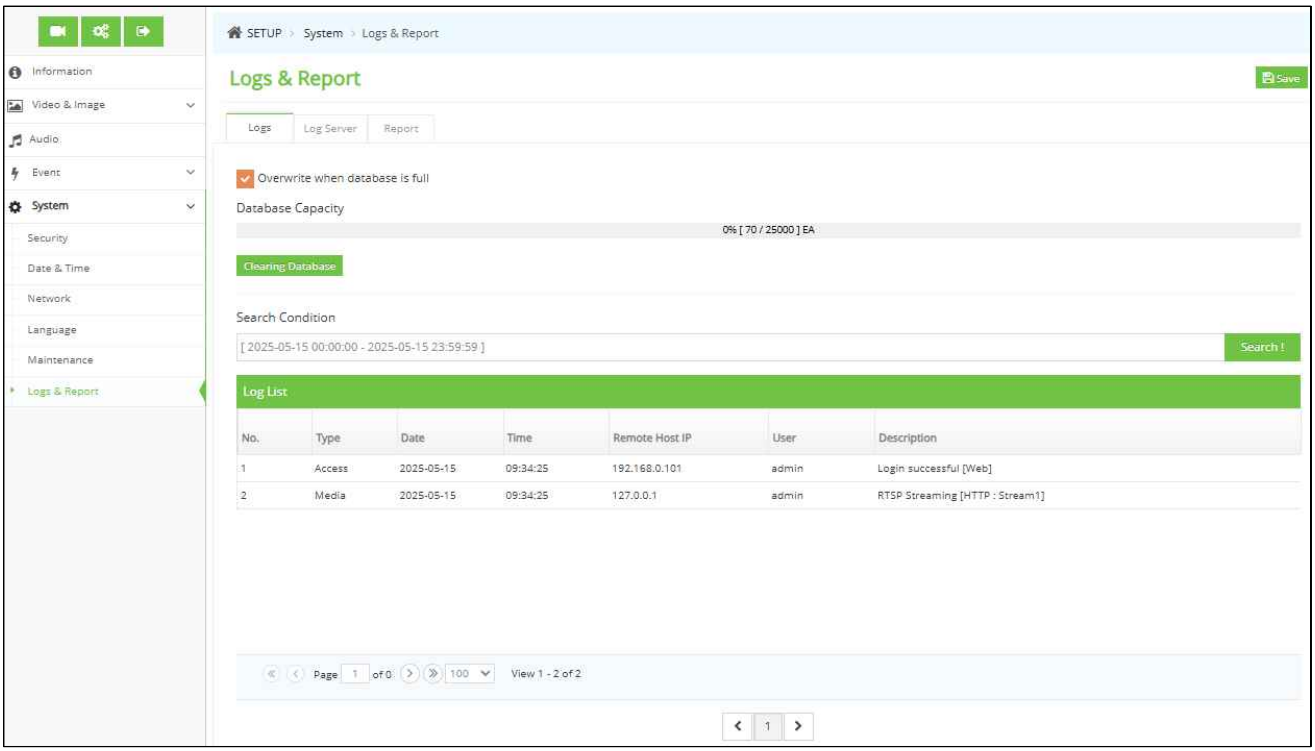
Setup Export: Save all parameters and user-defined scripts to a backup file. Click the Backup button to create a backup of all the parameters and any user-defined scripts.

Setup Import: Use a saved backup file to restore the unit to a previous configuration. Click the Browse button to locate the saved backup file and then click the Restore button.

** Note*

The Setup Export and Import functions can only be used on the same unit running the same firmware. This feature is not intended for the configuring of multiple units or for firmware upgrades.

System > Logs & Report



Logs: The log files record events in the unit since the last system restart and can be a useful diagnostic tool when troubleshooting. The Report contains important information about the system.

Database Capacity: Indicate the log file capacity.

Clearing Database; Delete log files in the database.

Search Condition: Enter a log parameter to search for specific log item.

Log List: Provides log information.

Report: Provides information about the server status and should be included when requesting a report. Information found here includes the camera's firmware version, MAC address, system information, IP address and network connections.

Troubleshooting

If a problem is suspected to be caused by incorrect configuration or some other minor issue, refer to the troubleshooting guide below.

Upgrading the Firmware

Firmware is software that determines the functionality of the network camera. One of the first actions when troubleshooting a problem should be to check the current firmware version. The latest version may contain a correction for the particular issue. The current firmware version in the camera is displayed in the Basic Configuration or About section. For the latest firmware, contact your product administrator. Detailed instructions on how to perform the upgrade process are provided with each new release. See also the Maintenance/Upgrade section for more information.

General Troubleshooting

The following list covers some of the problems that may be encountered and suggests possible remedies:

Symptom → Possible Causes or Corrective Actions

1. The camera cannot be accessed by some clients.
   → If using a proxy server, try disabling the proxy setting in your browser. Check all cabling and connectors.
2. The camera works locally, but not externally.
   → Check if there are firewall settings that need to be adjusted. Check if there are router settings that need to be configured.
3. Poor or intermittent network connection.
   → If using a network switch, ensure the port on the device uses the same setting for the network connection type (speed/duplex).
4. The camera cannot be accessed via a host name.
   → Check that the host name and DNS server settings are correct.
5. Uable to log in.
   → When HTTPS is enabled, ensure the correct protocol (HTTP or HTTPS) is used. When attempting to log in, you may need to manually type in http or https in the browser's address bar.
6. No image using Refresh and/or slow updating of images.
   → If images are very complex, try limiting the number of clients accessing the camera.
7. Images only shown in black & white.
   → Check the Video & Image setting.
8. Blurred images.
   → Refocus the camera.
9. Poor image quality.
   → Increasing lighting can often improve image quality. Check that there is sufficient lighting in the monitored area. Check all image and lighting settings.
10. Rolling dark bands or flickering in image.

→ Try adjusting the Exposure Control setting under AE and AWB settings.

11. H.264/H.265 not displayed in the client.

→ Ensure that the correct network interface is selected in the Video & Image/Stream settings.

12. Multicast H.264/H.265 not displayed in the client.

→ Check with your network administrator to ensure the multicast addresses used by the camera are valid for your network. Ensure that the Enable multicast checkbox is selected in the System/Network/RTP tab. Check with your network administrator if a firewall is preventing viewing.

13. Multicast H.264/H.265 only accessible by local clients.

→ Check if your router supports multicasting, or if the router settings between the client and the server need to be configured. The TTL value may need to be increased.

14. Color saturation is different in H.264/H.265 and Motion JPEG.

→ Modify the settings for your graphics adapter. Refer to the adapter's documentation for more information.

15. Poor audio quality.

→ Too many users/clients connected to the camera may affect the sound quality. Try limiting the number of clients allowed to connect.

16. Distorted audio.

→ Ensure the correct Audio Input source is selected. Select Microphone for a connected external microphone. Select Line for a connected line-in source.

* Note

If the required help cannot be found, refer to the User's Manual, or contact your network administrator.