EN

User Manual

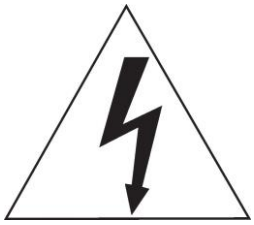
Multisignal Converter, HD-TVI , AHD, 960H to IP, H.264, 1920x1080, 12VDC

MAM-5ME1001MTA

WARNING

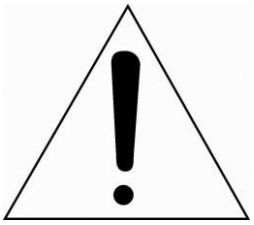
TO REDUCE THE RISK OF FIRE OR ELECTRIC SHOCK, DO NOT EXPOSE THIS PRODUCT TO RAIN OR MOISTURE. DO NOT INSERT ANY METALLIC OBJECT THROUGH THE VENTILATION GRILLS OR OTHER OPENNINGS ON THE EQUIPMENT.

CAUTION



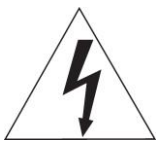
CAUTION

RISK OF ELECTRIC SHOCK
DO NOT OPEN



WARNING: TO REDUCE THE RISK OF ELECTRIC SHOCK,
DO NOT REMOVE COVER (OR BACK).
NO USER-SERVICABLE PARTS INSIDE.
REFER SERVICING TO QUALIFIED SERVICE PERSONNEL

EXPLANATION OF GRAPHICAL SYMBOLS



The lightning flash with arrowhead symbol, within an equilateral triangle, is intended to alert the user to the presence of dangerous voltage within the products enclosure that may be of sufficient magnitude to constitute a risk of electric shock to persons.

The exclamation point within an equilateral triangle is intended to alert the user to the presence of important operating and maintenance (servicing) instructions in the literature accompanying the product.

FCC COMPLIANCE STATEMENT

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, includinginterference that may cause undesired operation.

FCC INFORMATION: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interferenceat his own expense.

CAUTION: Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate theequipment.

This Class A digital apparatus complies with Canadian ICES-003.
Cet appareil numèrique de la classe A est conforme á la norme NMB-003 du Canada.

CE COMPLIANCE STATEMENT

WARNING

This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequatemeasures.

CAUTION

RISK OF EXPLOSION IF BATTERY IS REPLACED BY AN INCORRECT TYPE. DISPOSE OF USED BATTERIES ACCORDING TO THE INSTRUCTIONS.

IMPORTANT SAFETY INSTRUCTIONS

1. Read these instructions.
2. Keep these instructions.
3. Heed all warnings.
4. Follow all instructions.
5. Do not use this apparatus near water.
6. Clean only with dry cloth.
7. Do not block any ventilation openings. Install in accordance with the manufacturers instructions.
8. Do not install near any heat sources such as radiators, heat registers, stoves, or other apparatus (including amplifiers) that produce heat.
9. Do not defeat the safety purpose of the polarized or grounding-type plug. A polarized plug has two blades with one wider than the other. A grounding type plug has two blades and a third grounding prong. The wide blade or the third prong are provided for your safety, If the provided plug does not fit into your outlet, consult an electrician for replacement of the obsolete outlet.
10. Protect the power cord from being walked on or pinched particularly at plugs, convenience receptacles, and the point where they exit from the apparatus.
11. Only use attachments/accessories specified by the manufacturer.
12. Use only with the cart, stand, tripod, bracket, or table specified by the manufacturer, or sold with the apparatus. When a cart is used. Use caution when moving the cart/apparatus combination to avoid injury from tip-over.

13. Unplug this apparatus during lightning storms or when unused for long periods of time.
14. Refer all servicing to qualified service personnel. Servicing is required when the apparatus has been damaged in any way, such as power-supply cord or plug is damaged, liquid has been spilled or objects have fallen into the apparatus, the apparatus has been exposed to rain or moisture, does not operate normally, or has been dropped.

15. ***CAUTION − THESE SERVICING INSTRUCTIONS ARE FOR USE BY QUALIFIED SERVICE PERSONNEL ONLY. TO REDUCE THE RISK OF ELECTRIC SHOCK DO NOT PERFORM ANY SERVICING OTHER THAN THAT CONTAINED IN THE OPERATING IN- STRUCTIONS UNLESS YOU QRE QUALIFIED TO DO SO.***

16. ***Use satisfy clause 2.5 of IEC60950-1/UL60950-1 or Certified/Listed Class 2 power source only.***

17. ITE is to be connected only to PoE networks without routing to the outside plant.

Contents

1 Introduction

The HD encoder supports the network service for an SD and HD analog camera. An analog image entered can be monitored on a real-time screen regardless of distances and locations. By using its dedicated program, many users are able to have an access to the HD encoder at once or a single user can monitor various HD encoder at the same time. It also enables users to play, store and retrieve a monitoring image by using a PC. All the settings and real-time monitoring screens are also provided through an access to the web.

The HD encoder is a one-port video transmitter fully featured for security surveillance and remote monitoring needs. It is based on the DSP compression chip, and can digitize one analog video source and make it available on the network as real-time, full frame rate Motion JPEG and H.264 video streams.

The HD encoder is equipped with RS-485 port for connecting third party PTZ systems.

1.1 Components

This system comes with the following components;

HD encoder	1
Installation Guide/CD	1
Mounting bracket	2
Accessory Kit	4

Note 1. Check your package to make sure that you received the complete system, including all components listed above.

Note 2. Adapter for DC 12V is not supplied.

1.2 Key Features

- **Brilliant video quality**
  The HD encoder offers the highly efficient H.264 video compression, which drastically reduces bandwidth and storage requirements without compromising image quality. Motion JPEG is also supported for increased flexibility.

- **Dual or Triple Streams**
  The HD encoder can deliver dual or triple video streams simultaneously using H.264 and Motion JPEG. This means that several video streams can be configured with different compression formats, resolutions and frame rates for different needs.

- **Intelligent video capabilities**
  The HD encoder includes intelligent capabilities such as enhanced video motion detection.

- **Improved Security**
  The HD encoder logs all user access, and lists currently connected users. Also, its full frame rate video can be provided over HTTPS.

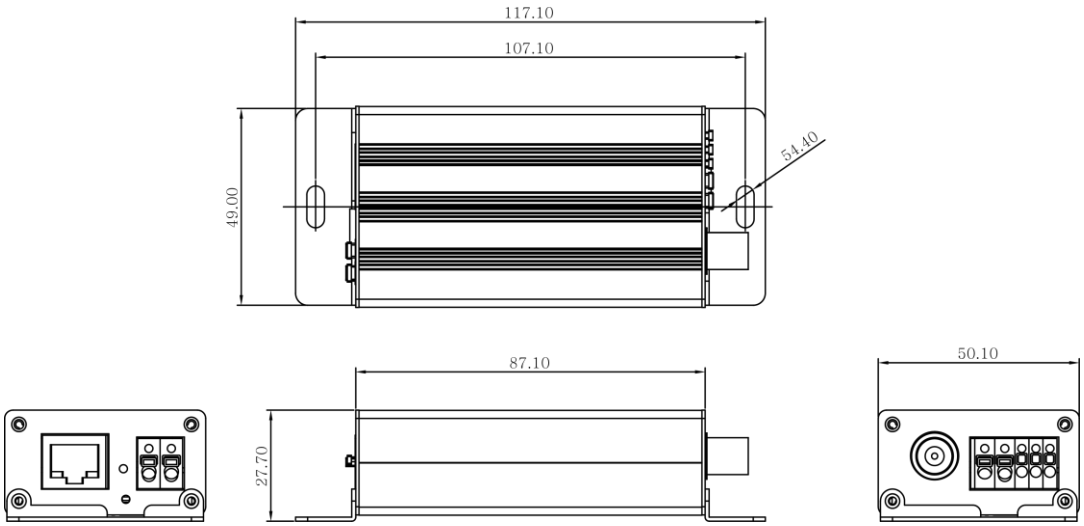
- **ONVIF Certificate**
  This is a global interface standard that makes it easier for end users, integrators, consultants, and manufacturers to take advantage of the possibilities offered by network video technology. ONVIF enables interoperability between different vendor products, increased flexibility, reduced cost, and future-proof systems.

2 Installation

For the operation of the HD encoder, it is necessary to connect a network cable for data transmission, power connection from supplied power adapter. For its fixation on different locations, please consult with an installer.

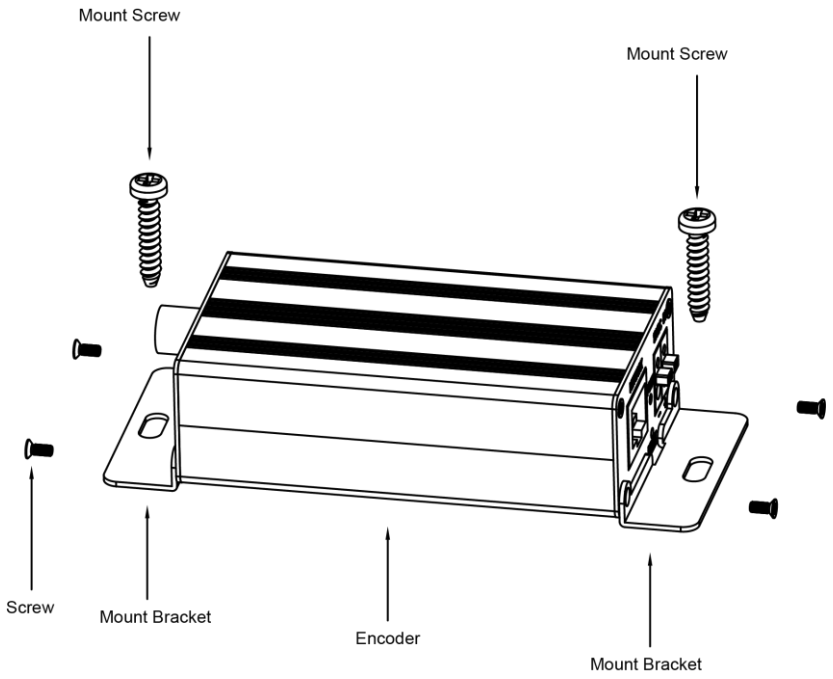
2.1 Overview

- **Dimension**

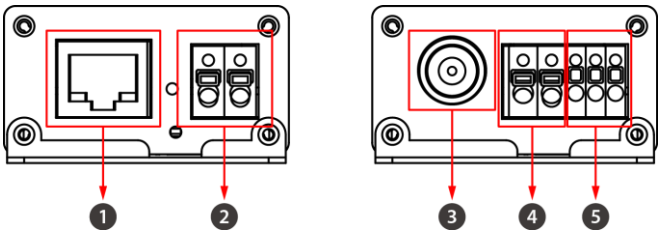


Dimensions Unit: mm

- **Installing Encoder**



• **Connectors**



NO	Item	Description
1	RJ-45	Ethernet, RJ-45 port compatible with 10/100Mbps modular Jack
2	2-pin terminal	12VDC input
3	BNC	BNC camera video input
4	2-pin terminal	12VDC output for BNC camera
5	3-pin terminal	RS485

2.2 Connection

- **Connecting to the RJ-45**

Connect a standard RJ-45 cable to the network port of the encoder. Generally a cross-over cable is used for directly connection to PC, while a direct cable is used for connection to a hub.

- **Connecting the Power**

Connect the power of 12 VDC for the encoder. Connect the positive (+) pole to the '+' position and the negative (-) pole to the '-' position for the DC power.

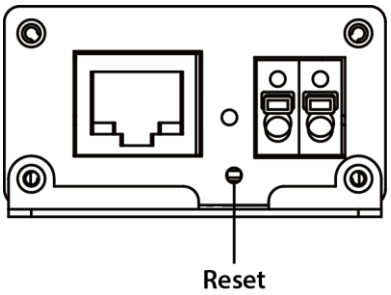
- Be careful not to reverse the polarity when connecting the power cable.
- For the power specifications, refer to the Appendix, Product Specification.

- **Connecting RS485**

Connect PTZ camera to RS485 terminal to control PTZ camera.

2.3 Resetting to the factory default settings

To reset the encoder to the original factory settings, go to the Setup > System > Maintenance web page (described in “System > Maintenance” of User Manual) or use the **Reset** button on the encoder.



- **Using the Reset button:**

Follow the instructions below to reset the encoder to the factory default settings us ing the Reset button.

1. Switch off the encoder by disconnecting the power adapter.
2. Press and hold the Reset button with a straightened paperclip while reconnecting the power.
3. Keep the Reset button pressed until the Status indicator blink.
4. Release the Reset button.
5. When the Power Indicator changes to Green (may take up to 40 seconds), the process is complete and the network video camera has been reset.
6. The encoder resets to factory defaults and restarts after completing the factory reset.

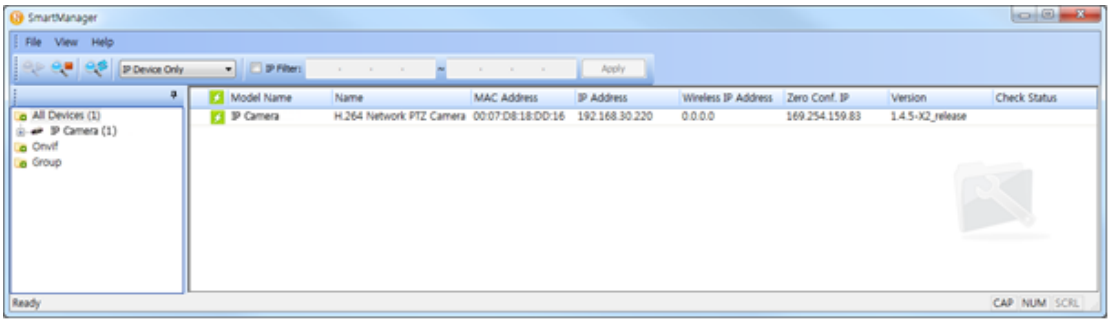
CAUTION: When performing a Factory Reset, you will lose any settings that have been saved. (Default IP 192.168.30.220)

2.4 Network Connection & IP assignment

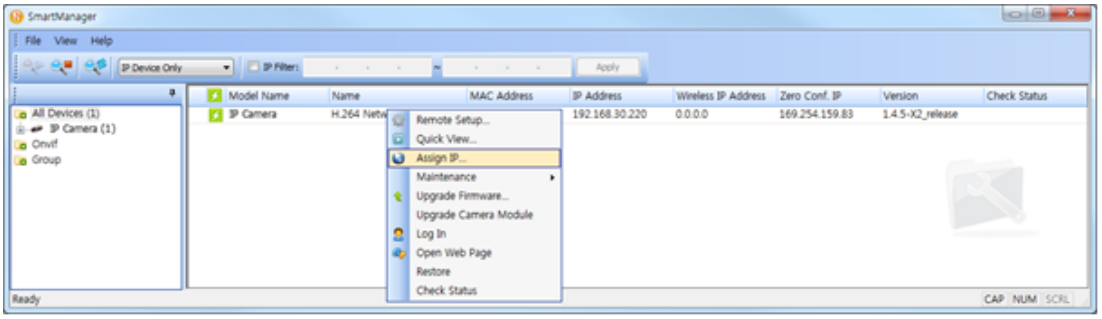
The encoder supports the operation through the network. When a encoder is first connected to the network, it is necessary to allocate an IP address to the device with the “SmartMan- ager” utility on the CD. (Default IP 192.168.30.220)

1) Connect the encoder/device to the network and power up.

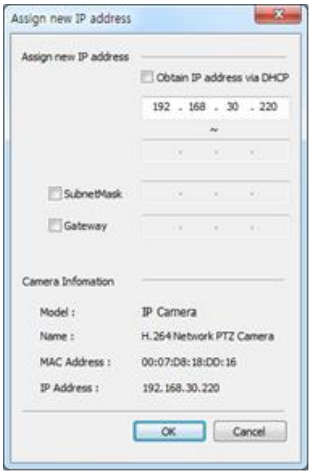
2) Start SmartManager utility (Start > All programs > SmartManager > SmartManager). The main window will display, and after a short while any network devices connected to the network will be displayed in the list.



3) Select the encoder on the list and click right button of the mouse. You can see the pop-up menu as below.



4) Select Assign IP Address. The Assign IP window will display. Enter the required IP address.



NOTE: For more information, refer to the SmartManager User Manual.

3 Operation

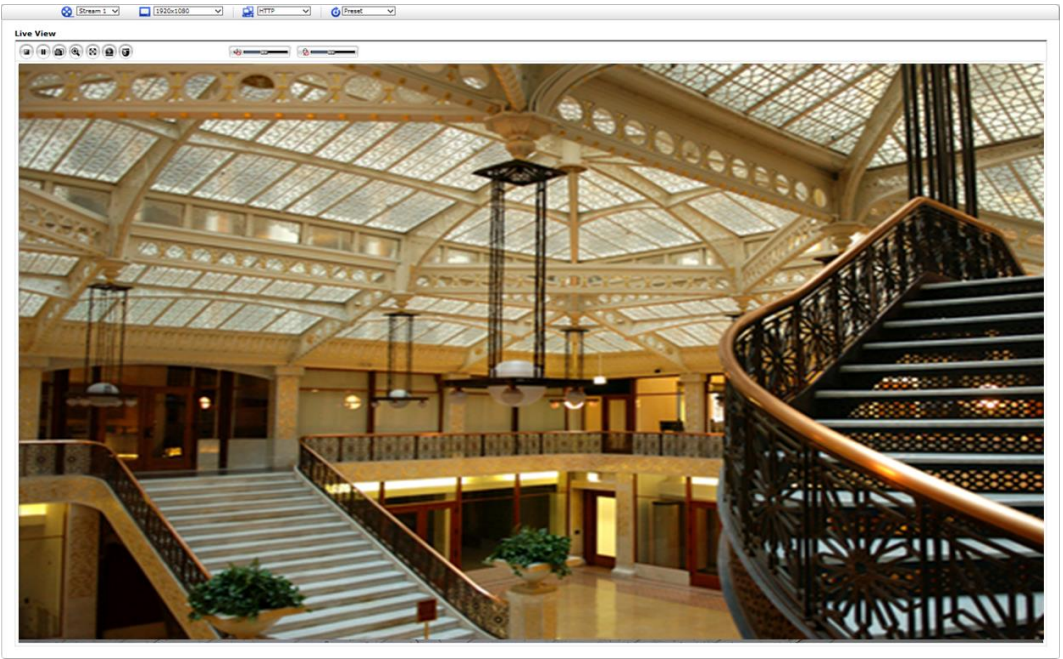
The encoder can be used with Windows operating system and browsers. The recommended browsers are Internet Explorer, Safari, Firefox, Opera and Google Chrome with Windows.

NOTE: To view streaming video in Microsoft Internet Explorer, set your browser to allow ActiveX controls.

3.1 Access from a browser

- Start a browser (Internet Explorer).
- Enter the IP address or host name of the encoder in the Location/Address field of your browser.
- You can see a starting page. Click **Live View** or **Setup** to enter web page.

- The encoder **Live View** page appears in your browser.



3.2 Access from the internet

Once connected, the encoder is accessible on your local network (LAN). To access the encoder from the Internet you must configure your broadband router to allow incoming data traffic to the encoder. To do this, enable the NAT traversal feature, which will attempt to automatically configure the router to allow access to the encoder. This is enabled from Setup > System > Network > NAT. For more information, please see " System > Network > NAT" of User's Manual.

3.3 Setting the admin password over a secure connection

To gain access to the product, the password for the default administrator user must be set. This is done in the "Admin Password" dialog, which is displayed when the encoder is accessed for the setup at the first time. Enter your admin name and password, set by the administrator.

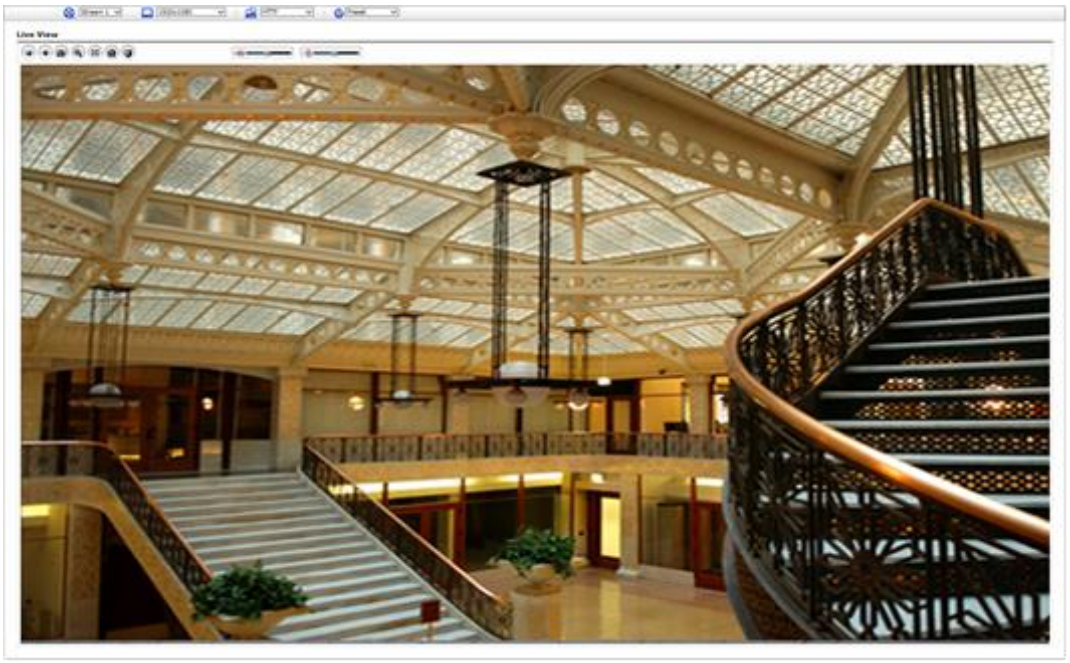
NOTE: The default administrator user name and password is "admin". If the password is lost, the encoder must be reset to the factory default settings. Please see "Resetting to the factory default settings."

To prevent network eavesdropping when setting the admin password, this can be done via an encrypted HTTPS connection, which requires an HTTPS certificate (see NOTE below). To set the password via a standard HTTP connection, enter it directly in the first dialog shown below. To set the password via an encrypted HTTPS connection, please see "System > Security > HTTPS" of User's Manual.

NOTE: HTTPS (Hypertext Transfer Protocol over SSL) is a protocol used to encrypt the traffic between web browsers and servers. The HTTPS certificate controls the encrypted exchange of information.

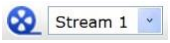
3.4 Live View Page

The Live View page comes in several screen modes. Users are allowed to select the most suitable one out of those modes. Adjust the mode in accordance with your PC specifications and monitoring purposes.



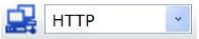
1) General controls

Live View Page Playback Page Setup Page Help Page



The video drop-down list allows you to select a customized or pre-programmed video stream on the Live View page. Stream profiles are configured under Setup > Basic Configuration > Video & Image. For more information, please see “Basic Configuration > Video & Image” of User’s Manual.

The resolution drop-down list allows you to select the most suitable one out of video resolutions to be displayed on Live View page.



The protocol drop-down list allows you to select which combination of protocols and methods to use depending on your viewing requirements, and on the properties of your network.

2) Control toolbar

The live viewer toolbar is available in the web browser page only. It displays the following buttons:

The **Stop** button stops the video stream being played. Pressing the key again toggles the start and stop. The **Start** button connects to the encoder or starts playing a video stream.

The **Pause** button pauses the video stream being played.

The **Snapshot** button takes a snapshot of the current image. The location where the image is saved can be specified.

The **Digital Zoom** button activates a zoom-in or zoom-out function for video image on the live screen.

The **Full Screen** button causes the video image to fill the entire screen area. No other windows will be visible. Press the 'Esc' button on the computer keyboard to cancel full screen view.

The **Manual Trigger** button activates a pop-up window to manually start or stop the event.

The **VCA** button shows/hides VCA rule setting and detected objects.

3) Video Streams

The encoder provides several images and video stream formats. Your requirements and the properties of your network will determine the type you use.

The Live View page in the encoder provides access to H.264 and Motion JPEG video streams, and to the list of available video streams. Other applications and clients can also access these video streams/images directly, without going via the Live View page.

3.5 Encoder Setup

This section describes how to configure the encoder.

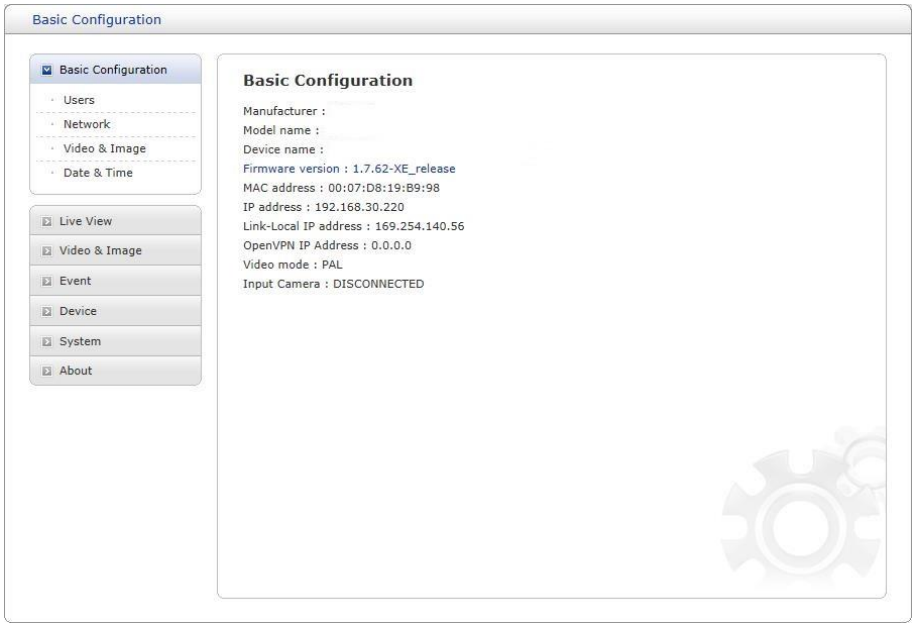
Administrator has unrestricted access to all the Setup tools, whereas Operators have access to the settings of Basic Configuration, which are Live View, Video & Image, Audio, Event, Dome Configuration, and System.

You can configure the encoder by clicking Setup either in the first connection page or the top second-right button of the Live View page. Accessing the encoder from a computer for the first time opens the Admin Password dialog box. Enter your administrator or operator id and password to get into setup page.

NOTE: If the password is lost, the encoder must be reset to the factory default settings. Please see “Resetting to the Factory Default Setting”.

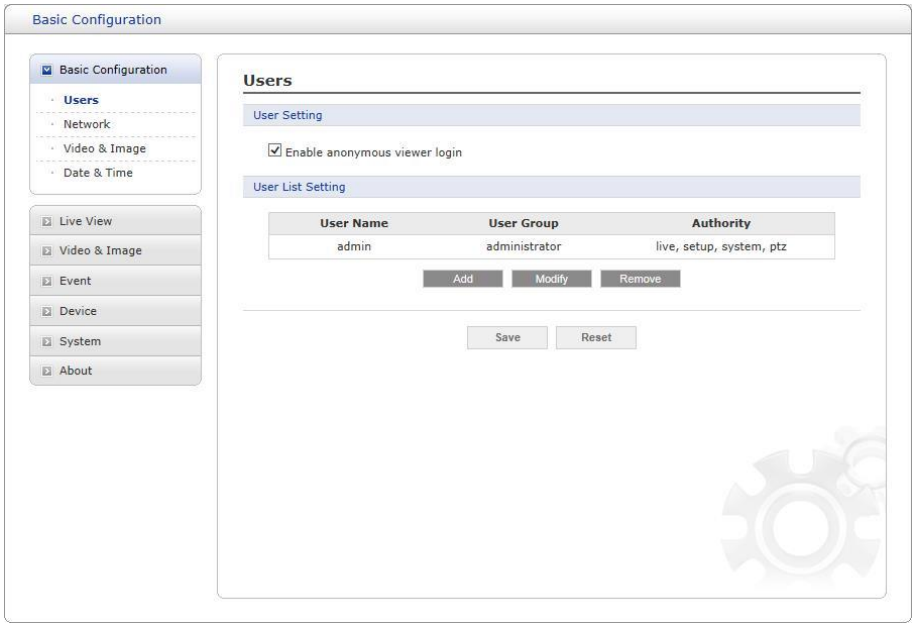
3.5.1 Basic Configuration

You can see the device information in this information page.



2) Users

User access control is enabled by default. The administrator can set up other users, by giving user names and passwords. It is also possible to allow anonymous viewer login, which means that anybody may access the Live View page, as described below:



The **user list** displays the authorized users and user groups (levels):

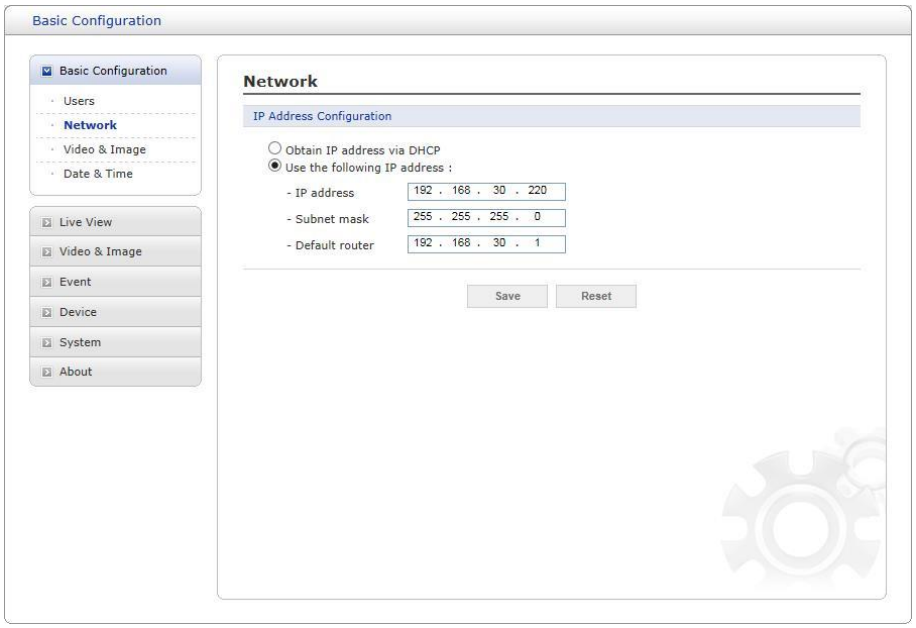
User Group	Authority
Guest	Provides the lowest level of access, which only allows access to the Live View page.
Operator	An operator can view the Live View page, create and modify events, and adjust certain other settings. Operators have no access to System Options.
Administrator	An administrator has unrestricted access to the Setup tools and can determine the registration of all other users.

- **Enable anonymous viewer login:** Check the box to use the webcasting features. Refer to " Video & Image 3) Webcasting" for more details.

  Please refer to " System 2) Security Users" for more details about User setup.

3) Network

The encoder supports both IP version 4 and IP version 6. Both versions may be enabled simultaneously, and at least one version must always be enabled. When using IPv4, the IP address for the encoder can be set automatically via DHCP, or a static IP address can be set manually. If IPv6 is enabled, the encoder receives an IP ad- dress according to the configuration in the network router. There is also an option of using the Internet Dynamic DNS Service. For more information on setting the network, please see “System > Network > Basic”.



Obtain IP address via DHCP: Dynamic Host Configuration Protocol (DHCP) is a pro- tocol that lets network administrators centrally manage and automate the assignment of IP addresses on a network. DHCP is enabled by default. Although a DHCP server is mostly used to set an IP address dynamically, it is also possible to use it to set a static, known IP address for a particular MAC address.

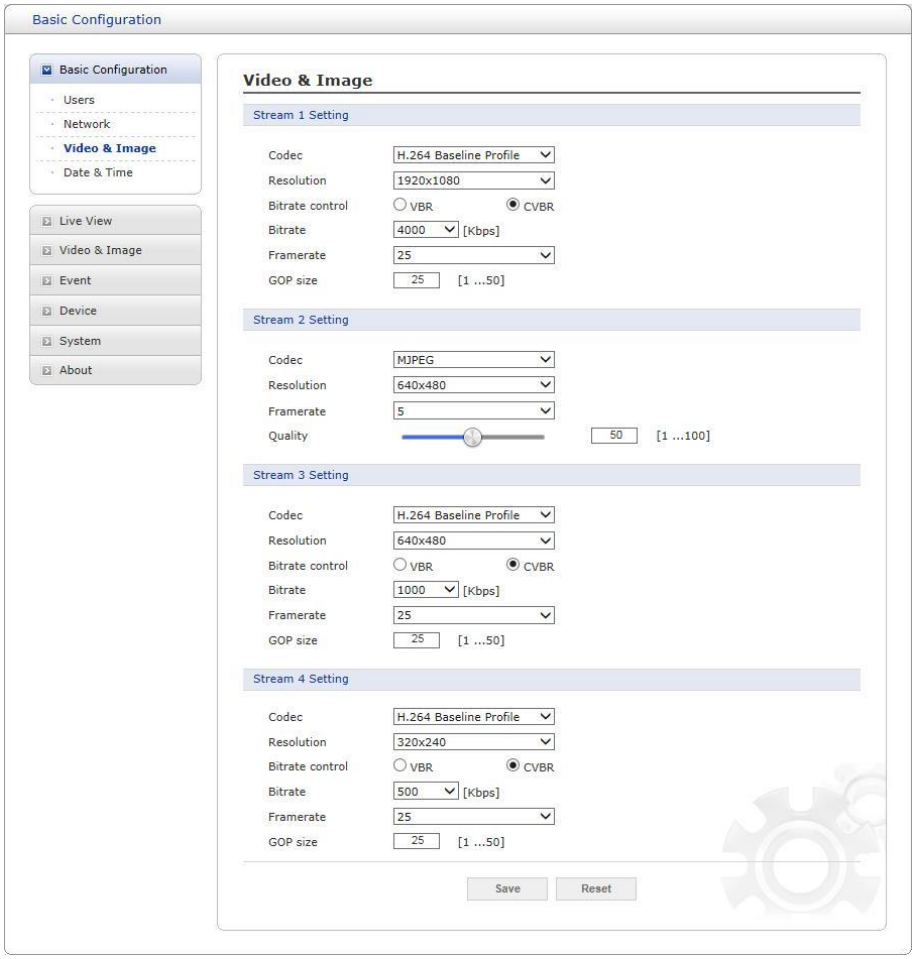
- **Use the following IP address:** To use a static IP address for the encoder, check the radio button and then make the following settings:
  - **IP address:** Specify a unique IP address for your encoder.
  - **Subnet mask:** Specify the mask for the subnet the encoder is located on.
  - **Default router:** Specify the IP address of the default router (gateway) used for connecting devices attached to different networks and network segments.

NOTES:

1. DHCP should only be enabled if using dynamic IP address notification, or if your DHCP server can update a DNS server, which then allows you to access the encoder by name (host name). If DHCP is enabled and you cannot access the unit, you may have to reset it to the factory default settings and then perform the installation again.
2. The ARP/Ping service is automatically disabled two minutes after the unit is started, or as soon as an IP address is set.
3. Pinging the unit is still possible when this service is disabled.

Please refer to “System > Network > Basic” for more details about Network setup.

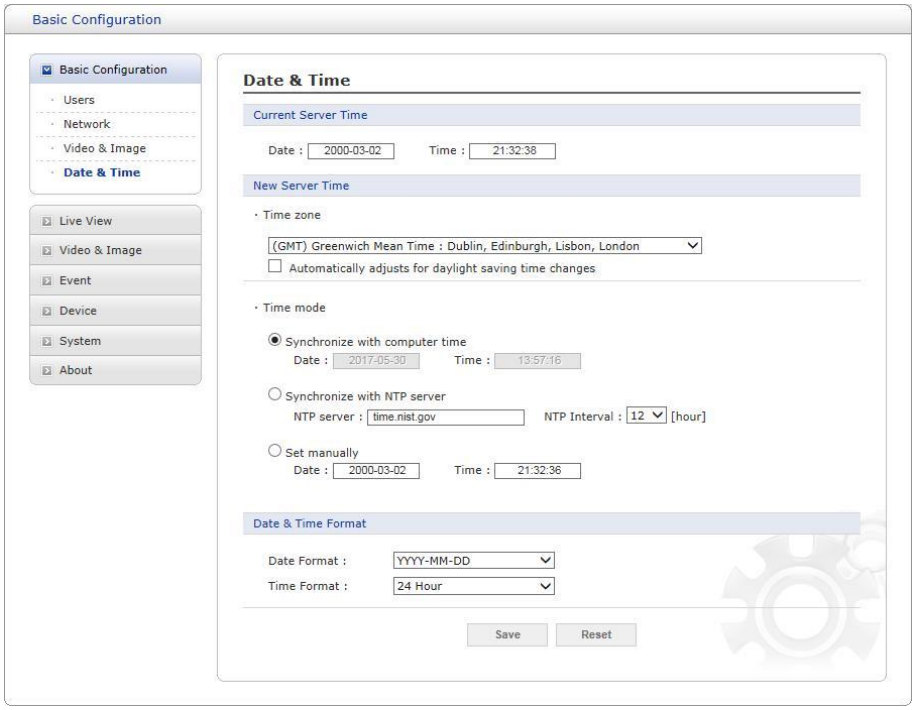
4) Video & Image



User can setup and change setting of individual video stream in this page.

Please refer to “Video & Image > Basic” for more details about Video & Image setup.

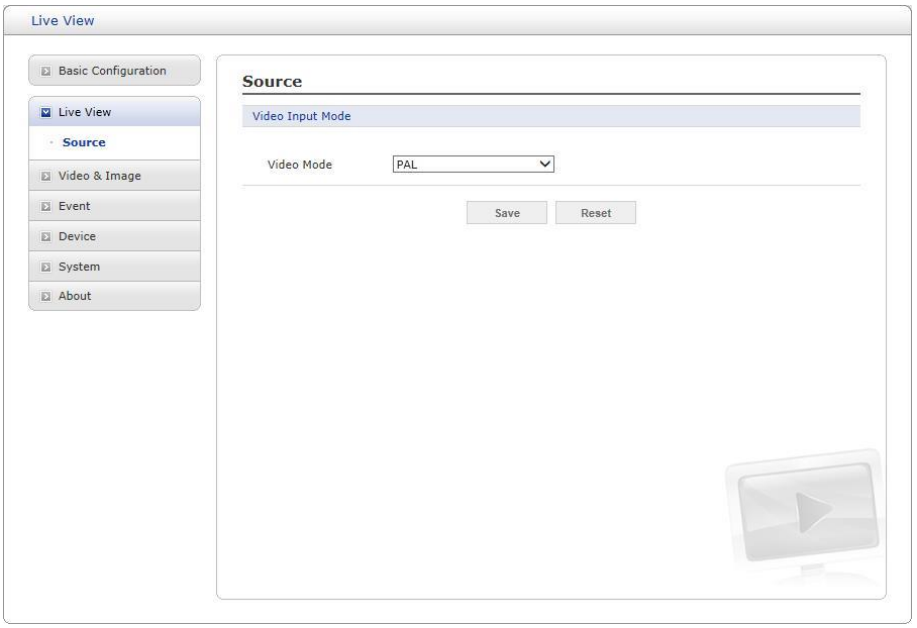
5) Date & Time



User can set time directly or assign time server to get the current time, as well as determine Date & Time format in this page.

Please refer to “System > Date & Time” for more details about Date & Time setup.

3.5.1 Live View

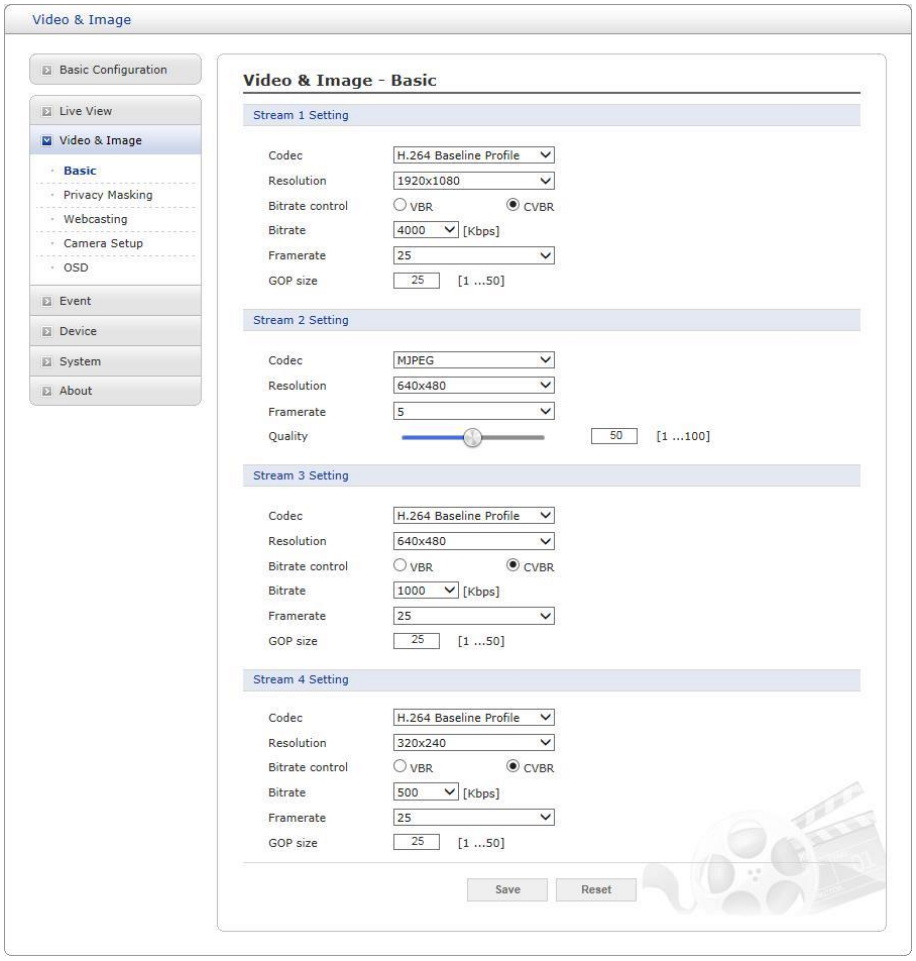


- **Video Input Mode:**
  - **Video Mode:** Choose Video Mode you wish to use from the drop-down list: NTSC or PAL

NOTE: This function may not be applicable, depending on the model.

3.5.2 Video & Image

1) Basic



Stream 1 Setting:

- **Codec:** The codec supported in Stream 1 is H.264.
  There are 3 pre-programmed stream profiles available for quick set-up. Choose the form of video encoding you wish to use from the drop-down list:
  - **H.264 HP (High Profile):**
    Primary profile for broadcast and disc storage applications, particularly for high-definition television applications (for example, this is the profile adopted by the Blu-ray Disc storage format and the DVB HDTV broadcast service).
  - **H.264 MP (Main Profile):**
    Primary profile for low-cost applications that require additional error robust-ness, this profile is used rarely in videoconferencing and mobile applications; it does add additional error resilience tools to the Constrained Baseline Pro- file. The importance of this profile is fading after the Constrained Baseline Profile has been defined.
  - **H.264 BP (Baseline Profile):**
    Originally intended as the mainstream consumer profile for broadcast and storage applications, the importance of this profile faded when the High Profile was developed for those applications.
- **Resolution:**
  This enables users to determine a basic screen size when having an access through the Web Browser or PC program. The screen size control comes in

several modes. Users can change the selected screen size anytime while monitoring the screen on a real-time basis.

- **Bitrate control:**
  The bit rate can be set as Variable Bit Rate (VBR) or Constrained Variable Bit Rate (CVBR). VBR adjusts the bit rate according to the image complexity, using up bandwidth for increased activity in the image, and less for lower activity in the monitored area. Limiting the maximum bit rate helps control the bandwidth used by the H.264 video stream. Leaving the Maximum bit rate as unlimited maintains consistently good image quality but increases bandwidth usage when there is more activity in the image. Limiting the bit rate to a defined value prevents excessive bandwidth usage, but images are degraded when the limit is exceeded.
  - **VBR:** unlimited maximum bitrate.
  - **CVBR:** VBR with maximum bitrate which is set in **Bitrate**.
- **Bitrate:** Maximum bitrate for CVBR in the range of 100kbps ~ 8Mbps.
  This is disabled if Bitrate control is set to VBR.
- **Frame rate:**
  Upon the real-time play, users should select a frame refresh rate per second. If the rate is high, the image will become smooth. On the other hand, if the rate is low, the image will not be natural but it can reduce a network load.
- **GOP size:**
  Select the GOP (Group of Picture) size. If users want to have a high quality of fast image one by one, please decrease the value. For the purpose of general monitoring, please do not change a basic value. Such act may cause a problem to the system performance. For the details of GOP setting, please contact the service center.

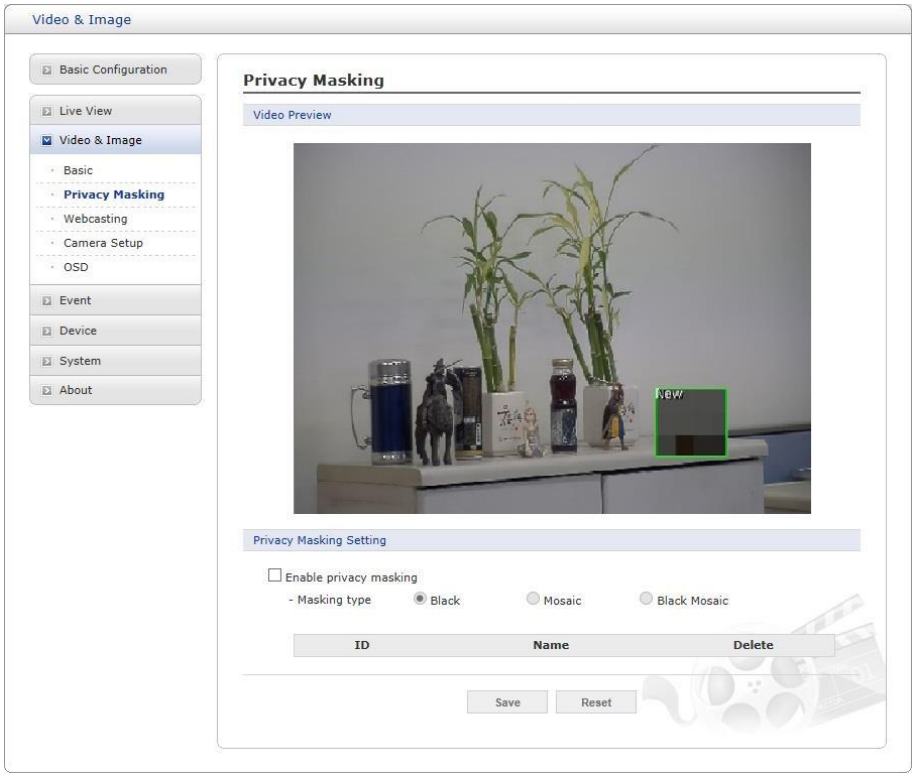
- **Stream 2 Setting:**
  Sometimes the image size is large due to low light or complex scenery. Adjusting the frame rate and quality helps to control the bandwidth and storage used by the Motion JPEG video stream in these situations. Limiting the frame rate and quality optimizes bandwidth and storage usage, but may give poor image quality. To prevent increased bandwidth and storage usage, the Resolution, Frame rate, and Frame Quality should be set to an optimal value.

  - **MJPEG Resolution:** Same as the stream 1 settings except the largest resolution, 2048x1536.
  - **MJPEG Frame rate:** Same as the stream 1 settings.
  - **MJPEG Quality:** Select the picture quality. If users want to have a high quality of fast image one by one, please decrease the value. For the purpose of general monitoring, please do not change a basic value. Such act may cause a problem to the system performance.

- **Stream 3, Stream4 Setting:** Same as the Stream 1 Setting, except for the resolution and bitrate which are confined by stream 1 setting.

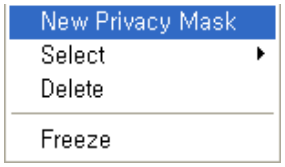
When the settings are complete, click **Save** button to save the settings, or click **Reset** button to clear all of the information you entered without saving it.

2) Privacy Masking



The privacy masking function allows you to mask parts of the video image to be transmitted. You can set up to eight privacy masks. You can choose masking type among **Black, Mosaic,** and **Black Mosaic**. Black mosaic is a mosaic with added black. The masking type applies to all Mask windows.

The privacy masks are configured by Mask windows. Each window can be selected by clicking with the mouse. It is also possible to resize or delete, or move the window, by selecting the appropriate window at the mouse menu on the video screen.

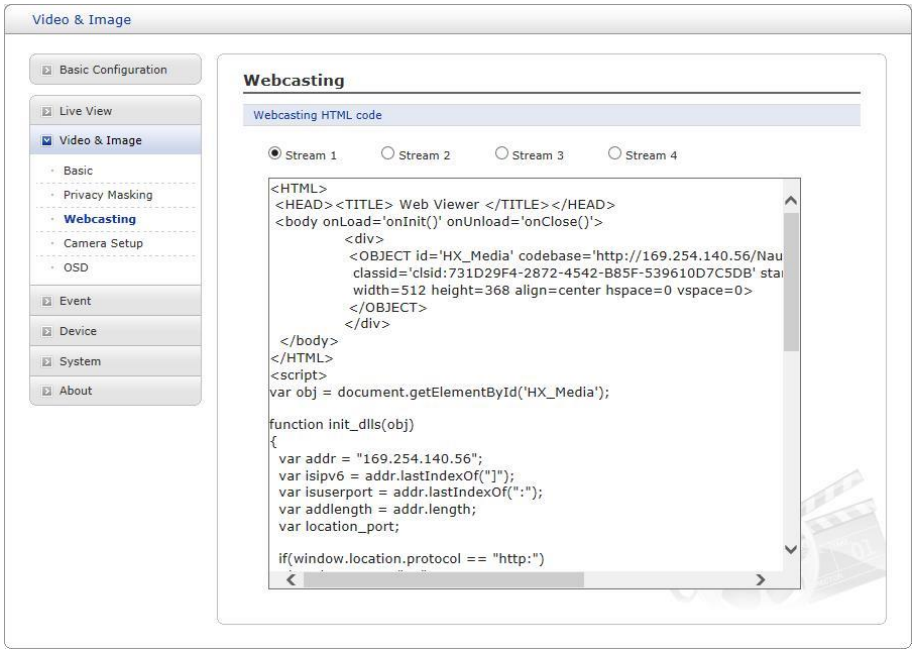


To create a mask window, follow steps:

1. Click the right button of mouse to see the mouse menu.
2. Select New Privacy Mask in the mouse menu.
3. Click and drag mouse to designate a mask window area.

When the settings are complete, click **Save** button to save the settings, or click **Reset** button to clear all of the information you entered without saving it.

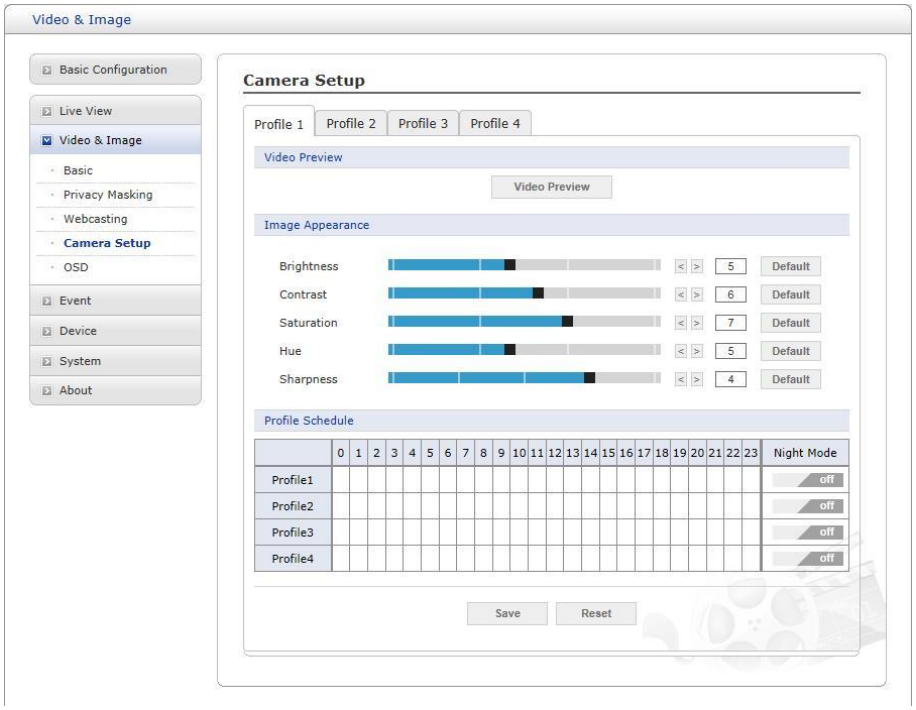
3) Webcasting



The live video of the encoder can be streamed to a website. User can copy and paste the HTML code generated on the screen to the website page code, where user wants to display live video.

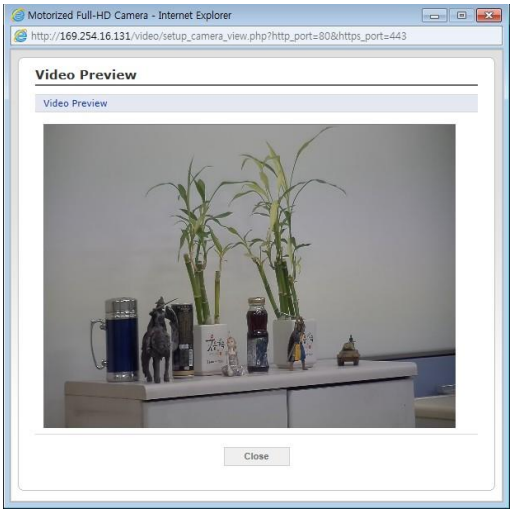
NOTE: To use webcasting service, the Enable Anonymous viewer login option must be checked.

4) Camera Setup



In this page, user can setup camera Image Appearance, and Profiles.

- **Video Preview:** User can check the setting via video preview pop-up window



- **Image Appearance**

  This provides access to the advanced image settings for the encoder.

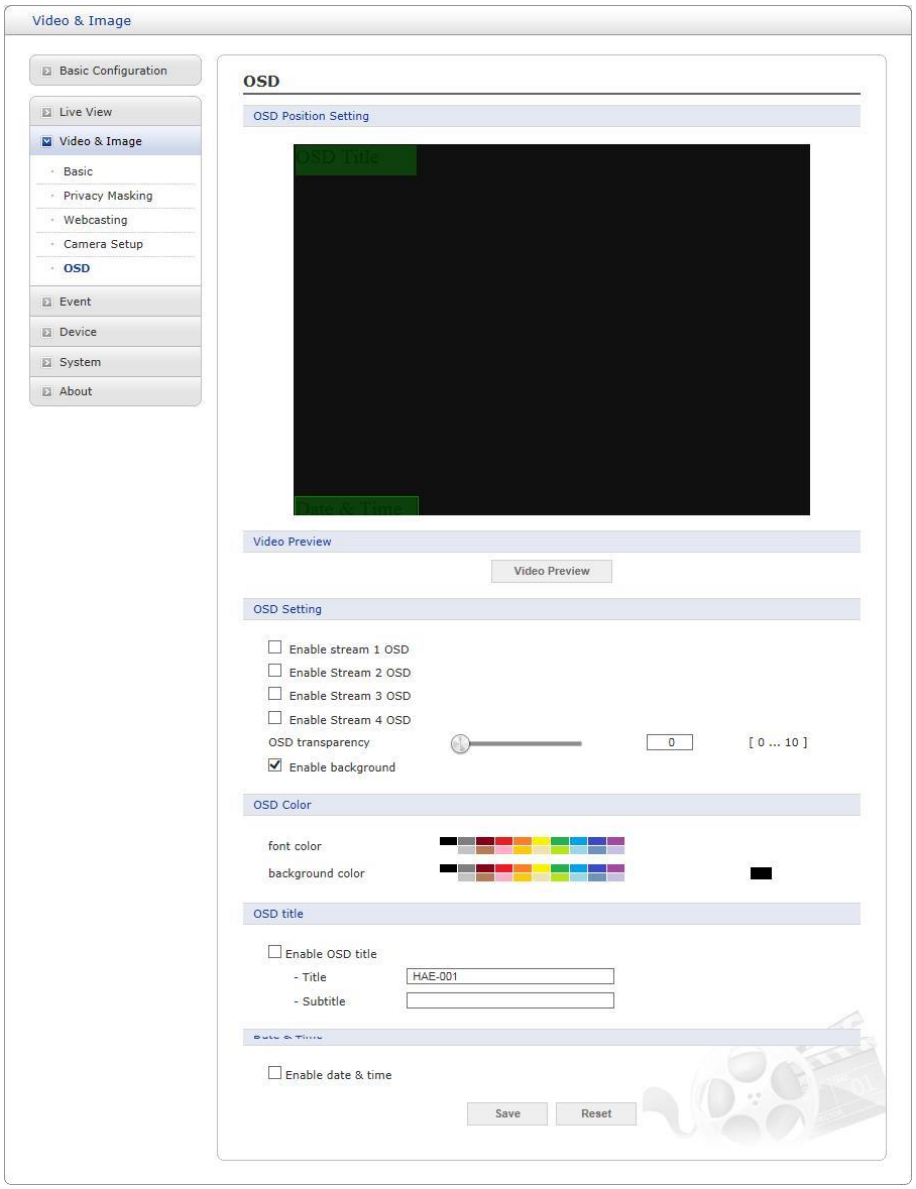
  – **Brightness:** The image brightness can be adjusted in the range 1-10, where a higher value produces a brighter image.
  – **Contrast:** Adjust the image's contrast by raising or lowering the value in this field.
  – **Saturation:** Set an appropriate value in the range 1-10. Lower values mean less color saturation.
  – **Hue:** Set an appropriate value in the range 1-10. The value distinguishes color, such as red, yellow, green, or violet.
  – **Sharpness:** Set the amount of sharpening applied to the image. A sharper image might increase image noise especially in low light conditions. A lower setting reduces image noise, but the image would be less sharp.

- **Profile Schedule**

  User can make schedule for 4 different profiles.

When the settings are complete, click **Save** button to save the settings, or click **Reset** button to clear all of the information you entered without saving it.

5) OSD



This encoder provides two OSD's (on screen display) on each stream, title and date & time. User can drag green "OSD Title" and "Date & Time" to the desired position and check at preview window.

- **Video Preview:** User can check the position of OSD on actual video via preview pop-up window.
- **OSD Setting:** User can select to show or hide OSD for each stream. Also user can set the transparency level of OSD by slide bar or type in number.
  - **Enable background:** User can set background for visibility of the OSD.
- **OSD Color:** User can set OSD font color and background color.
- **OSD title:** User can show or hide OSD title; when enabled the OSD title and subtitle can be typed in. The default is the model name of the camera.

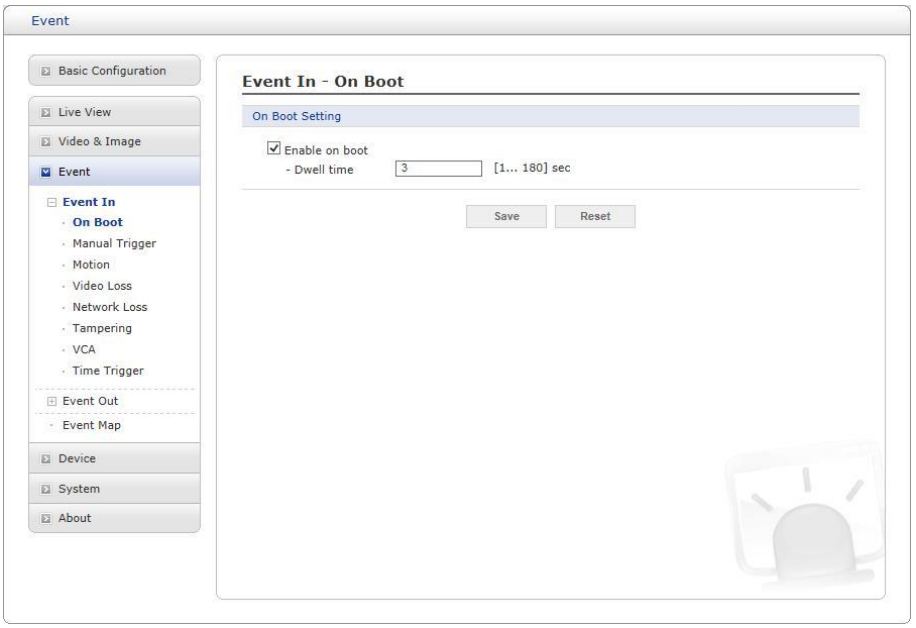
- **Date & Time:** User can show or hide date & time on OSD.

When the settings are complete, click **Save** button to save the settings, or click **Reset** button to clear all of the information you entered without saving it.

3.5.3 Event

1) Event In

▽ On Boot



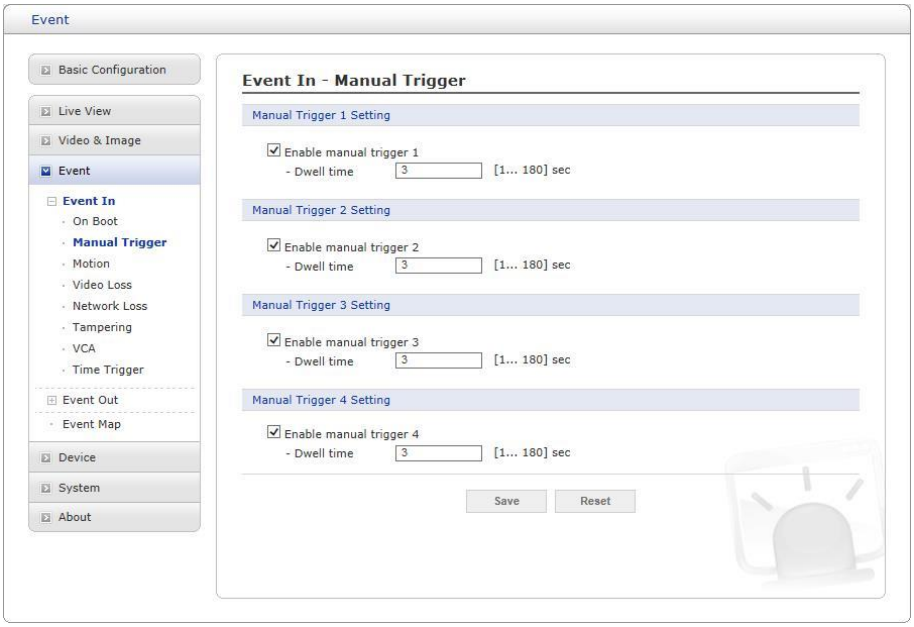
This is used to trigger an event every time the encoder is started. Select

“Enable on boot” to activate the On Boot event.

Enter the Dwell time the event lasts from the point of detection, 1-180 seconds.

When the settings are complete, click **Save** button to save the settings, or click **Reset** button to clear all of the information you entered without saving it.

▽ Manual Trigger



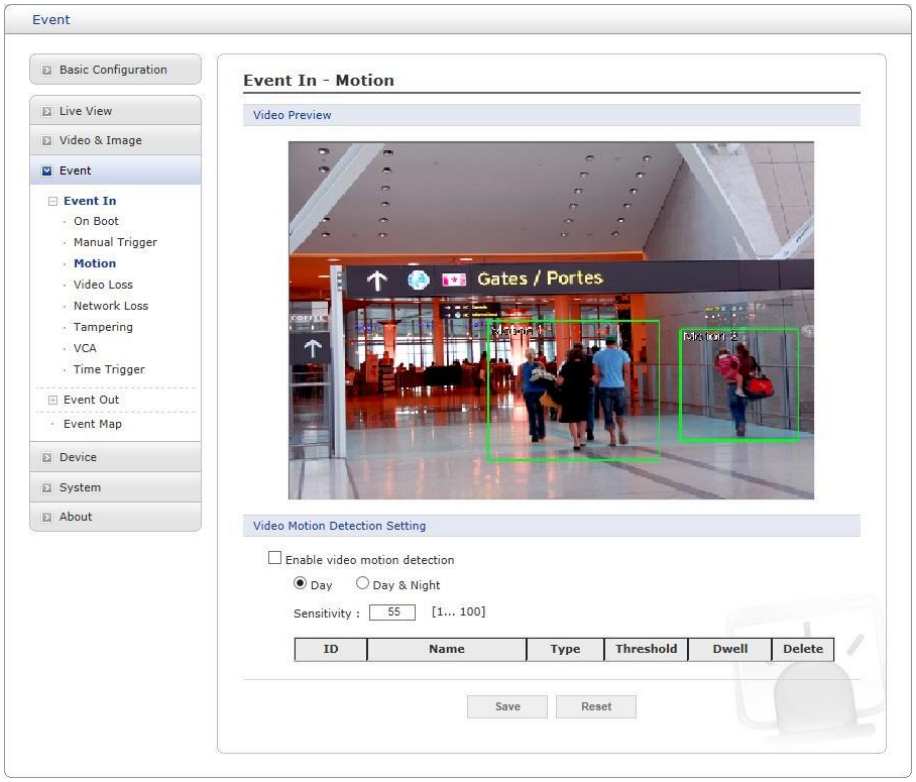
This option makes use of the manual trigger button provided on the Live View page, which is used to start or stop the event type manually. Alternatively, the event can be triggered via the product's API (Application Programming Interface).

Select "Enable manual trigger" to activate the manual trigger (for up to 4 manual triggers).

Set the dwell time the trigger lasts.

When the settings are complete, click **Save** button to save the settings, or click **Reset** button to clear all of the information you entered without saving it.

▽ Motion

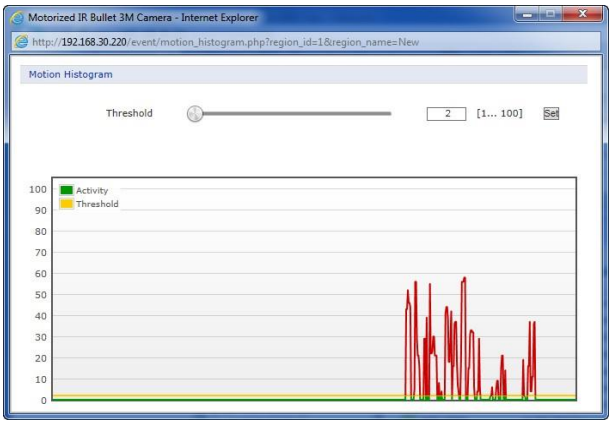


This option makes use of the motion detection function with 16 programmable areas, 8 **Include** and **Exclude** zones each.
Click right mouse button on the preview window shows selection pop-up of **New Motion, New Mask, Select, Delete, and Freeze.**
Select **New Motion** and click&drag generates an **Include** box of green color.
Select **New Mask** and click&drag generates an **Exclude** box of orange color.
Drag corner or line resizes and drag inside moves the box.
Select “Enable video motion detection” to activate motion detection.

- **Day & Night** selection
  - **Day:** Sensitivity and threshold values are not changed regardless of lighting condition.
  - **Day & Night:** User can set different sensitivity and threshold values for Day and Night condition.
- **Sensitivity:** User can change sensitivity of this function, where large value sets more sensitive detection.
- **Zone List**
  - **ID:** Order of generation, **Include** 1~8, **Exclude** 9~16.
  - **Name:** User definable zone name.
  - **Type:** shows zone type and cannot be changed.
  - **Threshold:** Determines how large the motion in the zone can trigger event in percentage.

– **Dwell time:** Determines how long the triggered event holds from the last triggering.

– **Show Histogram:** This encoder provides live histogram for easy setup of thresh- old level in motion window. The pop-up window shows activity strength and threshold level, and user can determine threshold level for triggering motion event by slide bar or type in number.

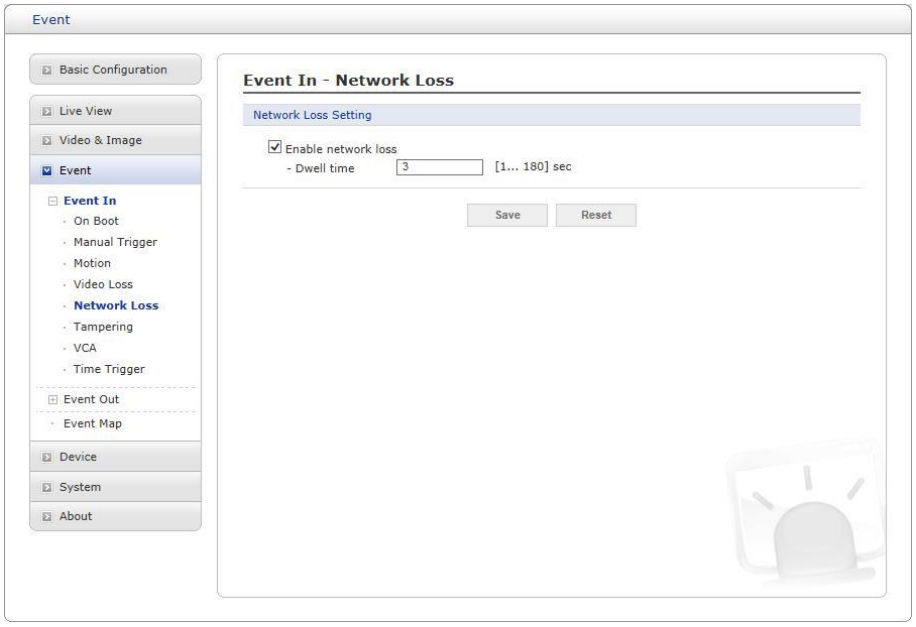


User can select any box by clicking name on the preview window or click on the list. User can delete selected zone via right mouse click selection for a selected box, or click any one of **X** button in the zone list.

NOTE: Video Motion detection function cannot be used in conjunction with Video Content Analysis function. If you choose **Enable video motion detection,** video content analysis function is automatically turned off.

When the settings are complete, click **Save** button to save the settings, or click **Reset** button to clear all of the information you entered without saving it.

▽ Video Loss

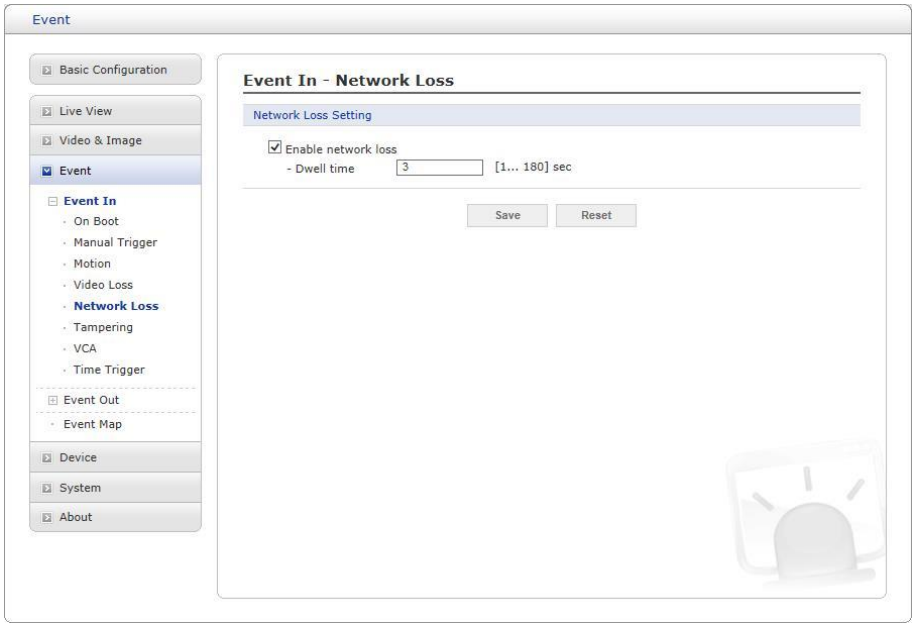


This is used to trigger an event every time the camera is disconnected.

Select “Enable video loss” to activate the Video Loss event. Select a dwell time for how long the event will last from the point of detection.

When the settings are complete, click **Save** button to save the settings, or click **Reset** button to clear all of the information you entered without saving it.

▽ Network Loss

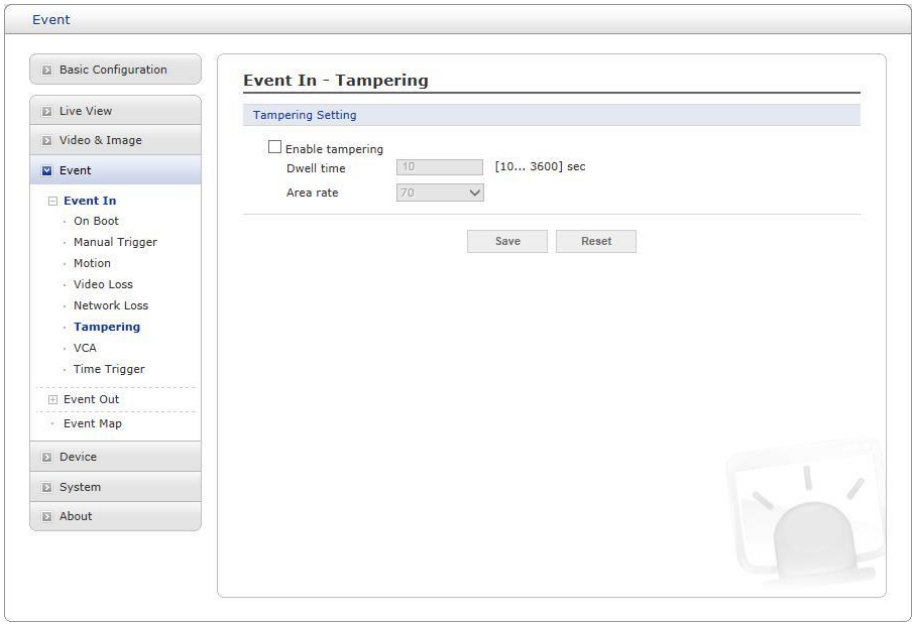


This is used to trigger an event every time the network connection is failed.

Select “Enable network loss” to activate the Network Loss event. Select a dwell time for how long the event will last from the point of detection.

When the settings are complete, click **Save** button to save the settings, or click **Reset** button to clear all of the information you entered without saving it.

▽ Tampering



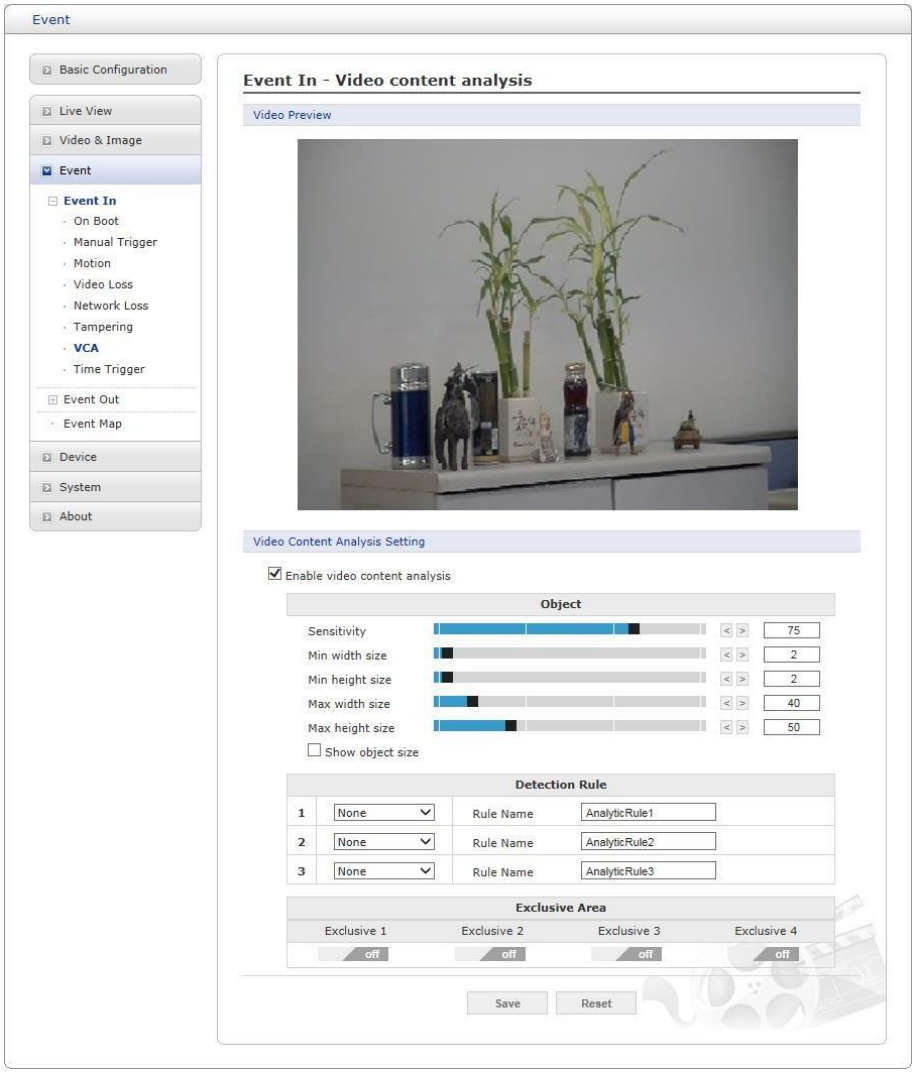
This is used to trigger an event when camera tampering occurs, for example, obstruct the camera with foreign material or move camera direction using external force.

Select “Enable tampering” to activate the Tampering event.

- **Dwell time:** Determine how long the event will last from the point of detection.

When the settings are complete, click **Save** button to save the settings, or click **Reset** button to clear all of the information you entered without saving it.

▽ VCA



The encoder provide VCA(Video Content Analysis) functions of “Line Detector” and “Field Detector.”

- **Video Content Analysis Setting**
  Check **Enable video content analysis** box to use a VCA function.
  - **Object:** Determines detection sensitivity.
    - **Sensitivity:** As the value becomes bigger, the detection sensitivity increases.
    - **Min width size:** Minimum horizontal pixel size for detections in a 1920x1080 format.
    - **Min height size:** Minimum vertical pixel size for detections in a 1920x1080 format.
    - **Max width size:** Maximum horizontal pixel size for detections in a 1920x1080 format.
    - **Max height size:** Maximum vertical pixel size for detections in a 1920x1080 format.

– **Detection Rule:** User can assign up to 3 different rules for each preset position.

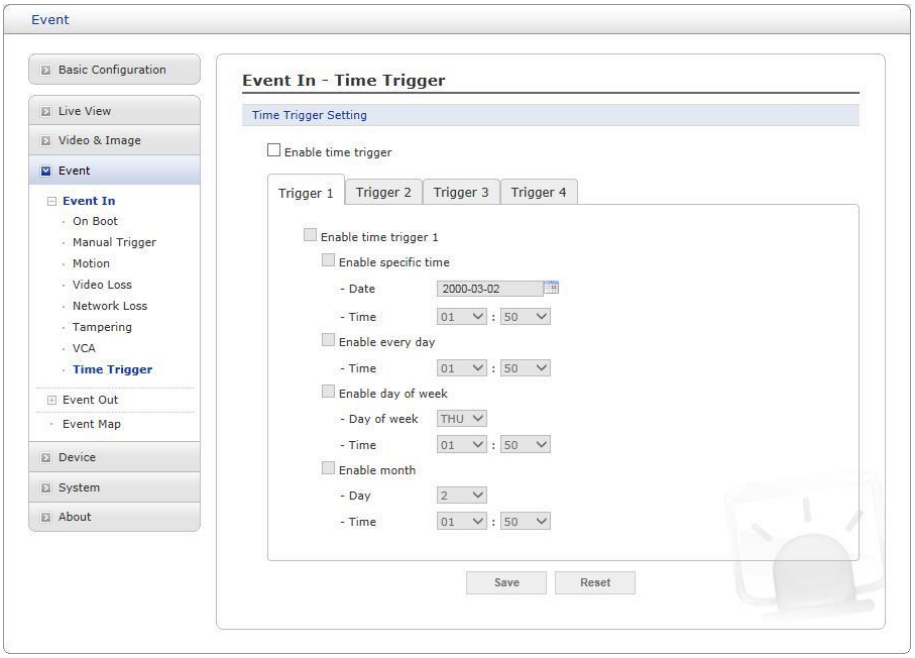
- **Line Detector**
  Once selected, a **red** line appears on the video preview window. Drag and drop the line at the desired position. User can change the length and the slope by dragging each end of the line.
  - **Rule Name:** User can type in the rule name.
  - **Direction:** This detector can detect line crossing events and also count up number of the event; the direction of the event appears as a solid triangle shape at the center of the line.
  - **Base:** The reference point of the object detection.
  - **Counter:** User can choose between Counter and Detector.
- **Field Detector**
  Once selected, a **blue** line appears on the video preview window. Drag and drop the box at the desired position. User can change the shape of the box by dragging each corner to any shape of a quadrilateral.
  - **Rule Name:** User can type in the rule name.
  - **Base:** The reference point of the object detection.
  - **Mode:** Currently Enter rule only.

– **Exclusive Area**
User can set up to 4 areas where the rules are not applied. Once selected, a **purple** line appears on the video preview window. Drag and drop the box at the desired position. User can change the shape of the box by dragging each corner to any form of a quadrilateral.

NOTE: Video Content Analysis function cannot be used in conjunction with Motion Detection function. If you choose **Enable video content analysis,** motion detection function is automatically turned off.

When the settings are complete, click **Save** button to save the settings, or click **Reset** button to clear all of the information you entered without saving it.

▽ Time Trigger



Time Trigger is to set alarms at specific time. User can set up to four time triggers and each time trigger can be set to specific date in the calendar, every day, day of the week, or date of every month.

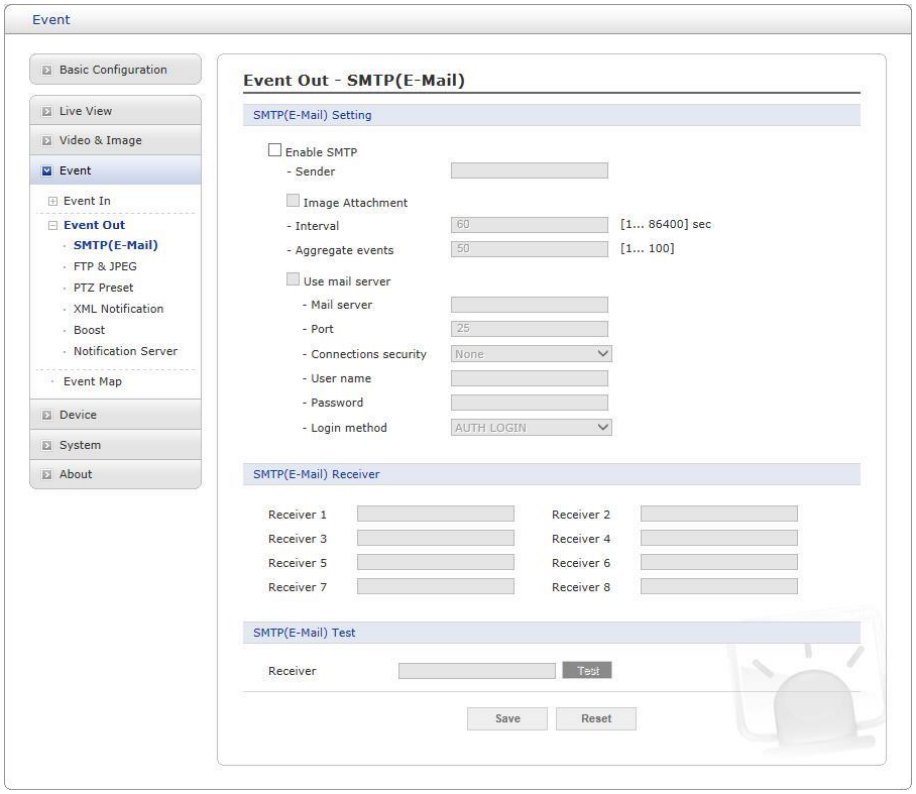
Select “Enable time trigger” to activate the Time Trigger function.

- **Enable specific time:** User can select a date in the calendar or type in date, and specify time for event trigger.
- **Enable every day:** Trigger event every day at specified time.
- **Enable day of week:** Trigger event at the day of every week at specified time.
- **Enable month:** Trigger event at the date of every month at specified time.

When the settings are complete, click **Save** button to save the settings, or click **Reset** button to clear all of the information you entered without saving it.

2) Event Out

▽ SMTP(E-Mail)



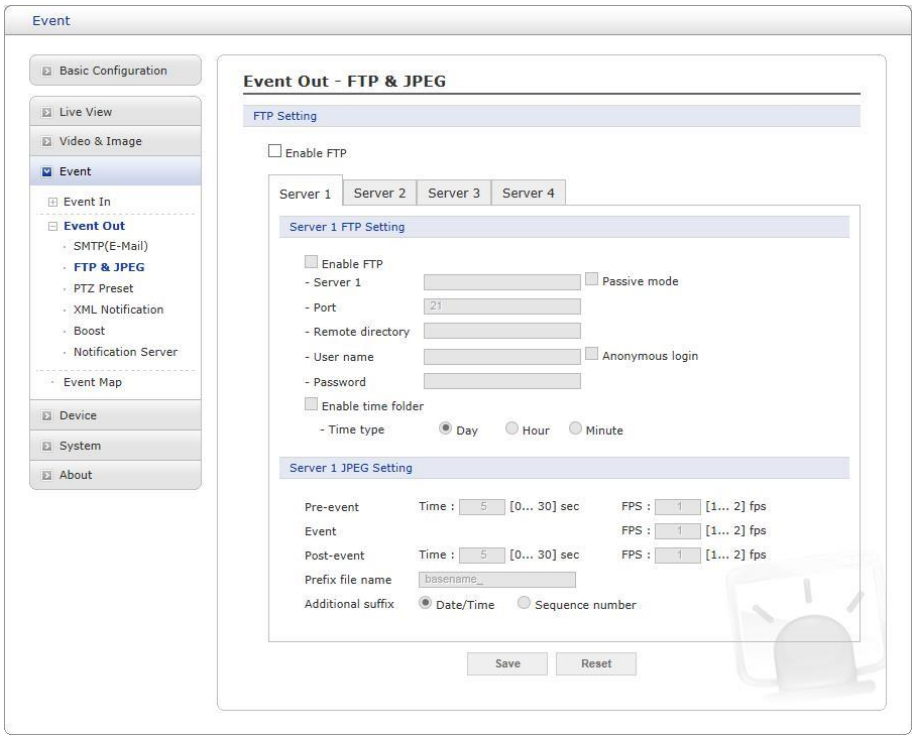
The encoder can be configured to send event and error email messages via SMTP (Simple Mail Transfer Protocol).

- **SMTP (E-Mail) Setting:** Select “Enable” to activate the SMTP operation.
  - **Sender:** Enter an email address to be used as the sender for all messages sent by the encoder.
  - **Interval:** Represents the time interval of the email notification when events occur several times.
  - **Aggregate events:** Shows the maximum number of emails sent within each interval.
  - **Use Mail Server:** Check the box if you are using a mail server to receive event notification and image email.
    - **Mail Server:** Enter the host names (or IP addresses) for your mail server.
    - **Port:** Enter the port number for your mail server.
    - **Connection security:** Select a connection security type in the drop-down list: **None, StartTLS, SSL**.
  - **Enable use(SMTP) authentication:** Check the box if your mail server requires authentication.
    - **User name/Password:** Enter the User name and Password as provided by your network administrator or ISP (Internet Service Provider).
    - **Login method:** Choose a log-in method in the drop-down list: **AUTH LOGIN / AUTH PLAIN**
- **SMTP (E-Mail) Receiver:** User can assign up to 8 receivers
  - **Receiver #:** Enter an email address.

- **SMTP (E-Mail) Test:** User can check the SMTP setting via a sample email.
  - **Receiver:** Enter an email address and click the Test button to test that the mail servers are functioning and that the email address is valid.

When the settings are complete, click **Save** button to save the settings, or click **Reset** button to clear all of the information you entered without saving it.

▽ FTP & JPEG



When the encoder detects an event, it can record and save images to an FTP server. Images can be sent as e-mail attachments. Check the “Enable FTP” box to enable the service. This encoder can support multiple FTP servers and user can configure each server settings separately.

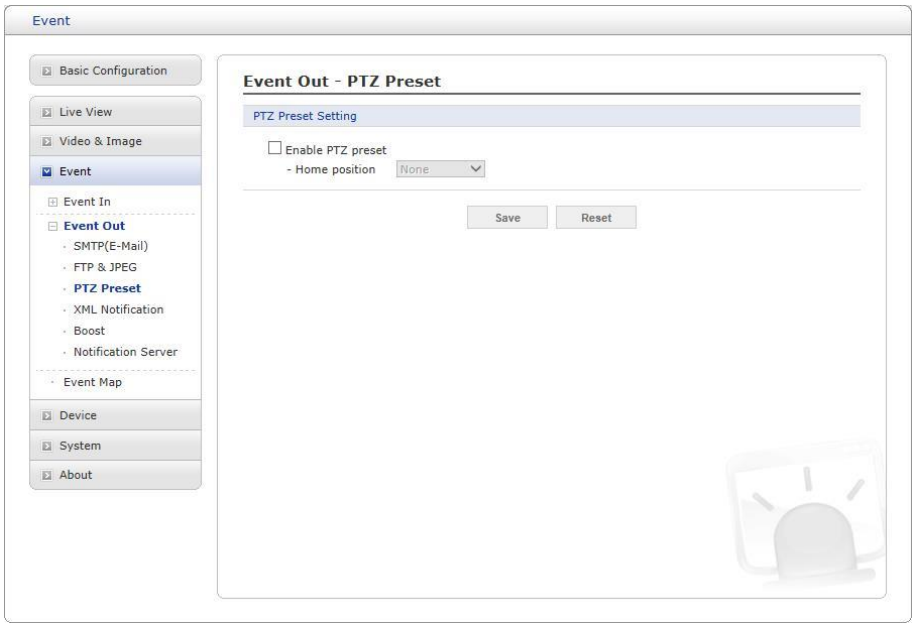
- **FTP Setting**
  - **Server:** Enter the server’s IP address or host name. Note that a DNS server must be specified in the TCP/IP network settings if using a host name.
  - **Port:** Enter the port number used by the FTP server. The default is 21.
  - **Passive mode:** Under normal circumstances the encoder simply re- quests 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 con- nection, whereby the encoder actively initiates both the FTP control and data connections to the target server. This is normally desirable if there is a firewall between the encoder and the target FTP server.
  - **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/Password:** Provide your log-in information.
  - **Anonymous login:** Check the box if you want to use anonymous login method and the server supports it.

- **JPEG Setting**
  - **Pre-event:** A pre-event buffer contains images from the time immediately preced- ing the event trigger. These are stored internally in the server. This buffer can be very useful when checking to see what happened to cause the event trigger. Check the box to enable the pre-trigger buffer, enter the desired total length in seconds, minutes or hours, and specify the required image frequency.
  - **Post-event:** This function is the counterpart to the pre-trigger buffer described above and contains images from the time immediately after the trigger. Configure as for pre-event.
  - **Prefix file name:** This name will be used for all the image files saved. If suffixes are also used, the file name will take the form <prefix> ≤suffix>.<extension>.
  - **Additional suffix:** Add either a date/time suffix or a sequence number, with or without a maximum value.

When the settings are complete, click **Save** button to save the settings, or click **Reset** button to clear all of the information you entered without saving it.

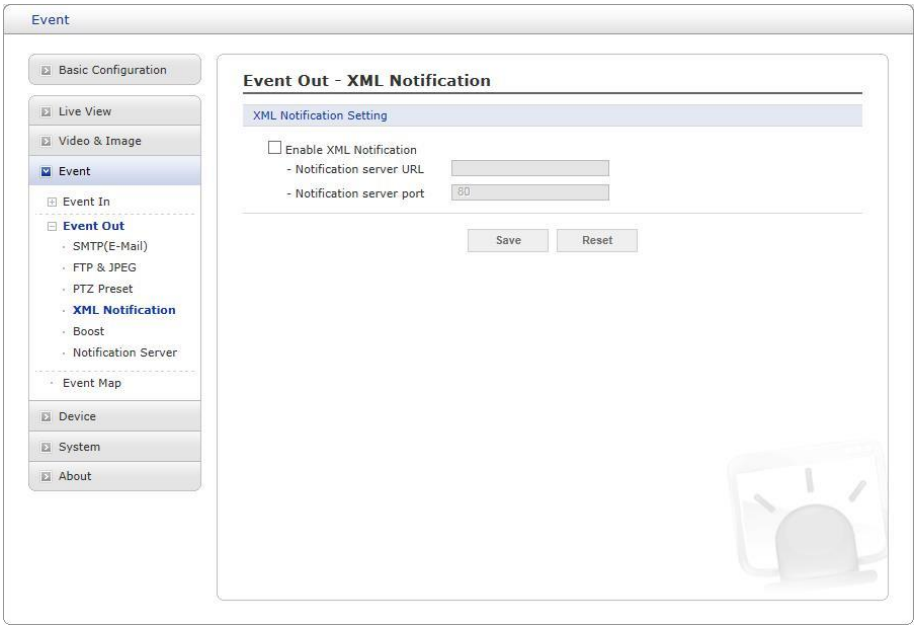
▽ PTZ Preset



When the camera detects an event, you can move the camera to a predefined preset position. Check the box to enable the service and return to the Home position once the event has ended.

When the settings are complete, click **Save** button to save the settings, or click **Reset** button to clear all of the information you entered without saving it.

▽ XML Notification

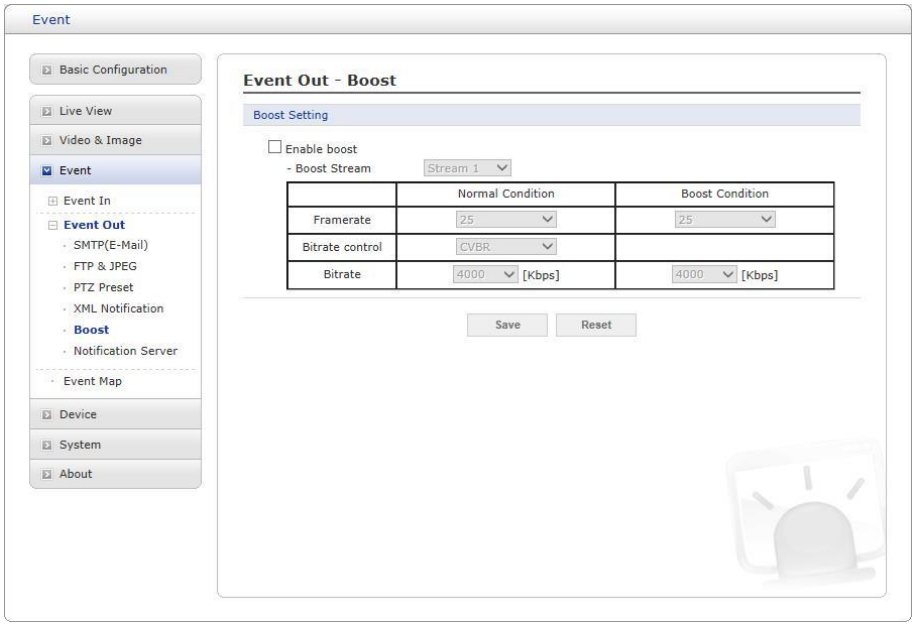


When the encoder detects an event, Notification server is used to receive notification messages as a type of XML data format. Check the box to enable the service.

- **XML Notification Setting:**
  - **Notification server URL:** The network address to the server and the script that will handle the request.
  - **Notification server port:** The port number of the notification server.

When the settings are complete, click **Save** button to save the settings, or click **Reset** button to clear all of the information you entered without saving it.

▽Boost



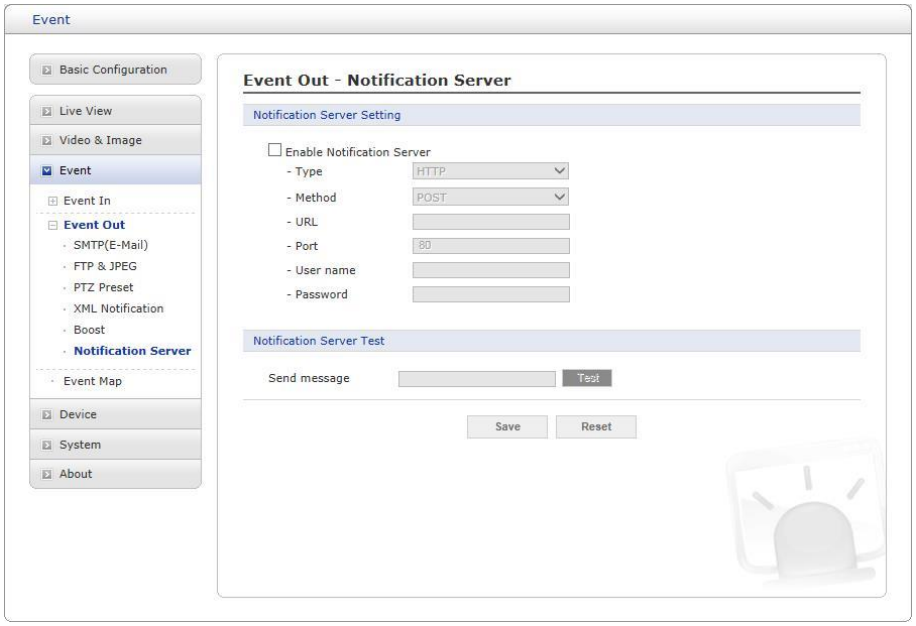
The Boost feature is used in conjunction with event detection. When this feature is turned ON, the Frame rate and Bit rate in the boost condition can be set to a different value than the ones in the normal condition field. When an event is detected, the encoder will boost the Frame rate and Bit rate from the normal condition to this boosted level for the duration of the event.

Check the box to enable the service.

- **Boost Setting:** You can set the condition in Normal and Boost mode.
  - **Boot Stream:** Select a video stream for each condition in the drop-down list.
  - **Frame rate:** Select a frame refresh rate per second for each condition in the drop-down list.
  - **Bit rate control:** Select VBR or CVBR in the drop-down list in Normal Condition. You can't change it in Boost Condition.
  - **Bit rate:** Select a value for each condition in the drop-down list.

When the settings are complete, click **Save** button to save the settings, or click **Reset** button to clear all of the information you entered without saving it.

▽ Notification Server

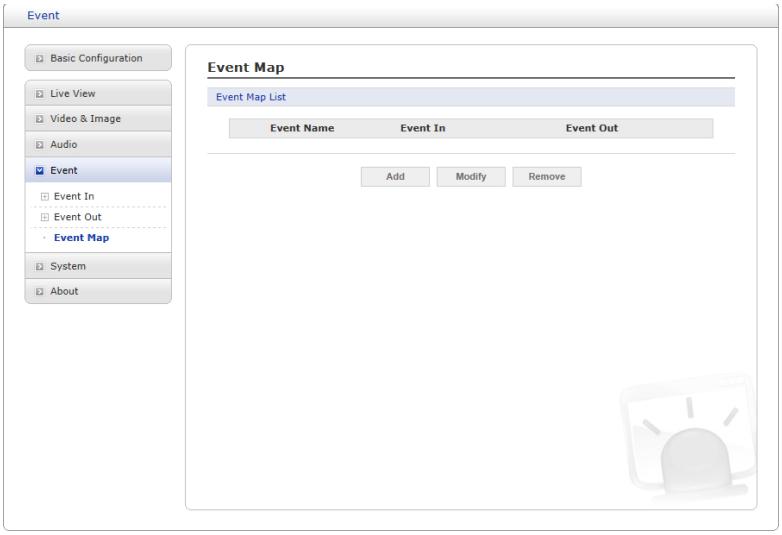


When the encoder detects an event, the Notification Server is used to receive up- loaded image files and/or notification messages. Check the box to enable the service.

- **Notification Server Setting:**
  - **Type:** User can select message transmission type among HTTP, HTTPS, TCP, and UTP.
  - **URL:** The network address to the server and the script that will handle the request. For example: http://192.168.12.244/cgi-bin/upload.cgi
  - **Port:** The port number of the server.
  - **User name/Password:** Provide your log-in information.
- **Notification Server Test:** When the setup is complete, the connection can be tested by clicking the Test button using the contents in “Send message” box.

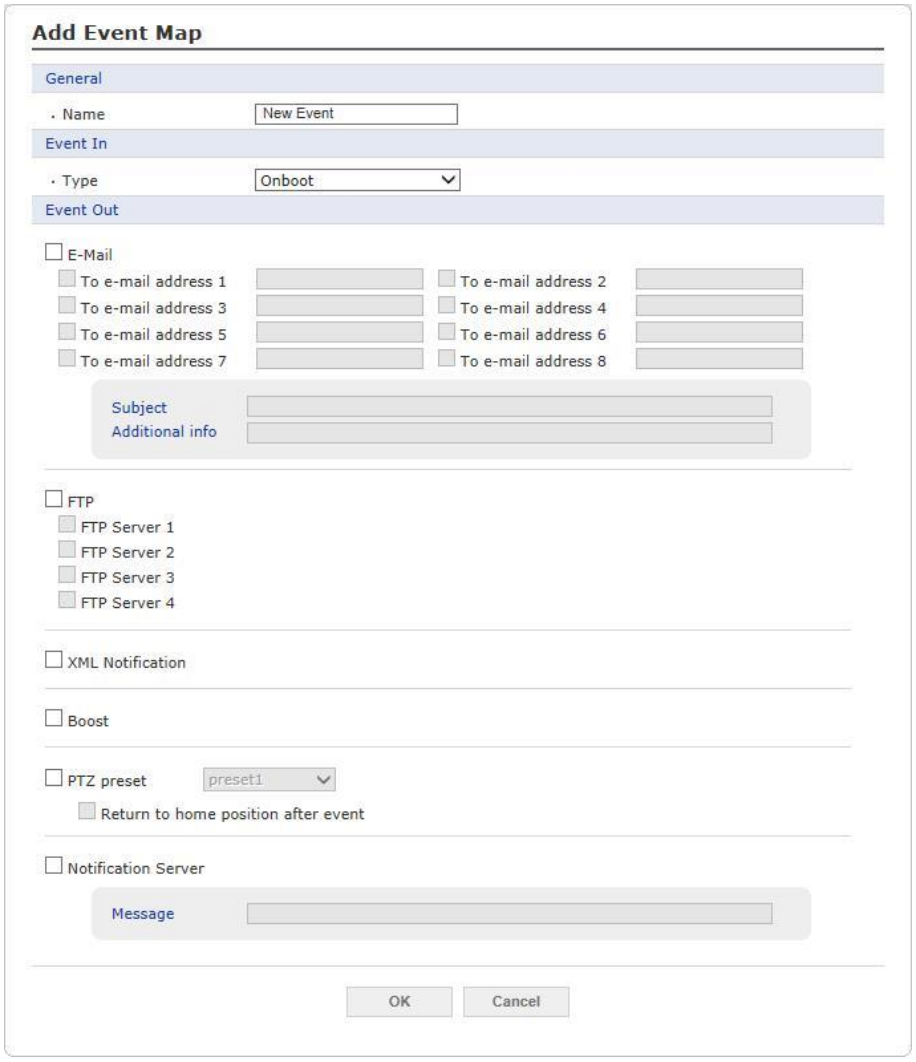
When the settings are complete, click **Save** button to save the settings, or click **Reset** button to clear all of the information you entered without saving it.

3) Event Map



The event map allows you to change the settings and establish a schedule for each event trigger from the encoder; up to a max. 15 events can be registered.

Click the **Add** button to make a new event map; a popup window displays as below. To change an existing event, select that event and click the **Modify** button; this same window will display and the information can be changed as required. Selecting an event and clicking **Remove** deletes the event.

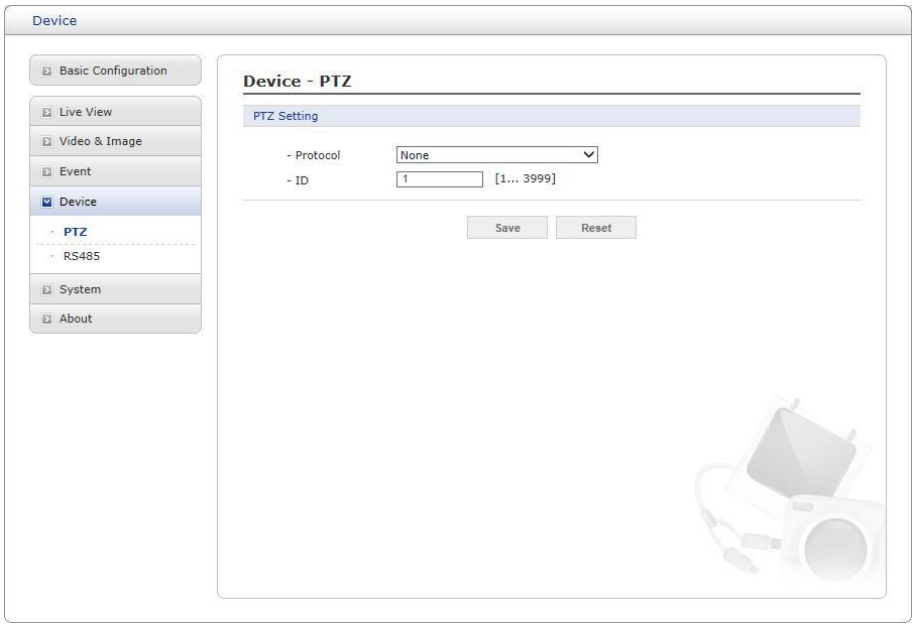


- **General:** Enter the name for a new event map.
- **Event In:** Select an event type in the drop-down list.
- **Event Out:**
  - **E-mail:** Select the email addresses you want to notify via email that an event has occurred.
  - **FTP:** Select checkbox beside FTP to record and save images to an FTP server when an event has occurred.
  - **XML Notification:** It sends XML messages to a Notification server that listens for these. The destination server must first be configured on the Event In page.
  - **Boost:** When an event has occurred, the encoder will boost the Frame rate and Bit rate from the normal condition to this boosted level for the duration of the event. Check the box to enable the Function.
  - **PTZ preset:** Select the preset position you want to move at event. If you want to move back to home position after the event, which is pre-defined in the Alarm Out - PTZ Preset page, check “Return to home position after event” box.
  - **Notification Server:** It sends notification messages to the notification server that listens for these. The destination server must first be configured on the Event In page. Enter a message you want to send.

When the settings are complete, click **OK** button to save the settings, or click **Cancel** button to clear all of the information you entered without saving it.

3.5.4 Device

1) PTZ



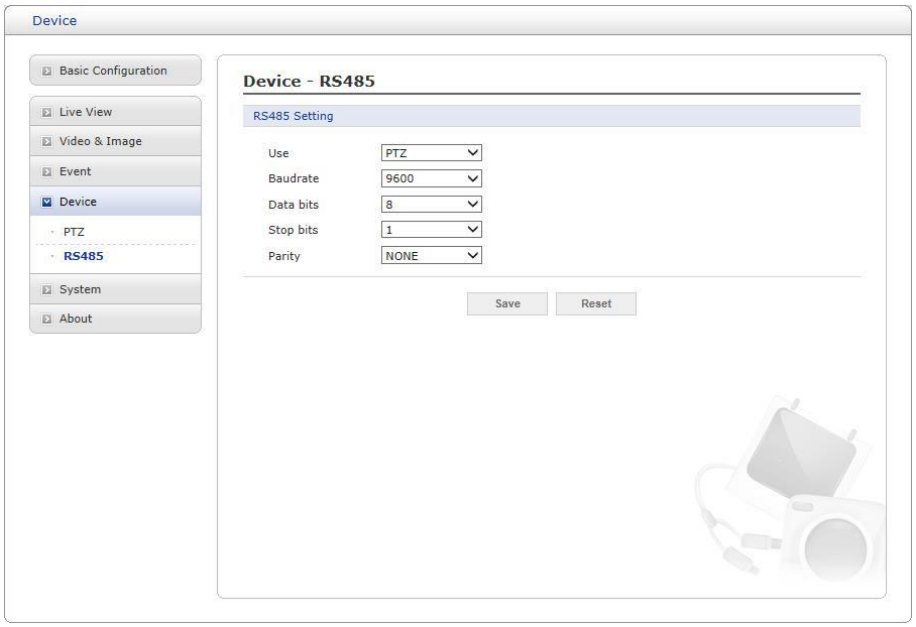
If you want to use the camera with PT device and/or motorized zoom lens, this camera provides RS-485 connectivity for that purpose. You need to select a PTZ protocol in the drop-down list and type in ID for PTZ device.

• **PTZ Setting**

- **Protocol:** Selects PTZ protocol to communicate with external PTZ device.
- **ID:** Enter identification number for external PTZ device. The ID can be adjusted in the range 1-255.

When the settings are complete, click Save button to save the settings, or click Reset button to clear all of the information you entered without saving it.

2) RS485



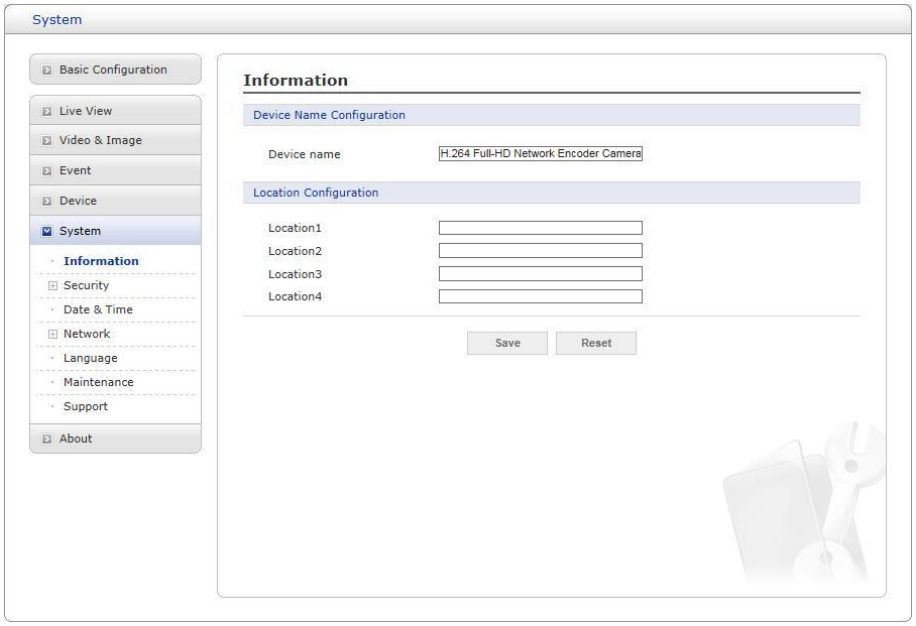
If the camera supports RS-485 communication, you can setup details for RS-485 in this page.

- **RS485 Setting:**
  - **Use:** Selects device type for communication.
  - **Baud rate:** Selects one of the Baud rate.
  - **Stop bits:** Selects number of stop bits between 1 and 2.
  - **Parity:** Selects one of the Parity bit among none, even and odd.

When the settings are complete, click **Save** button to save the settings, or click **Reset** button to clear all of the information you entered without saving it.

3.5.5 System

1) Information



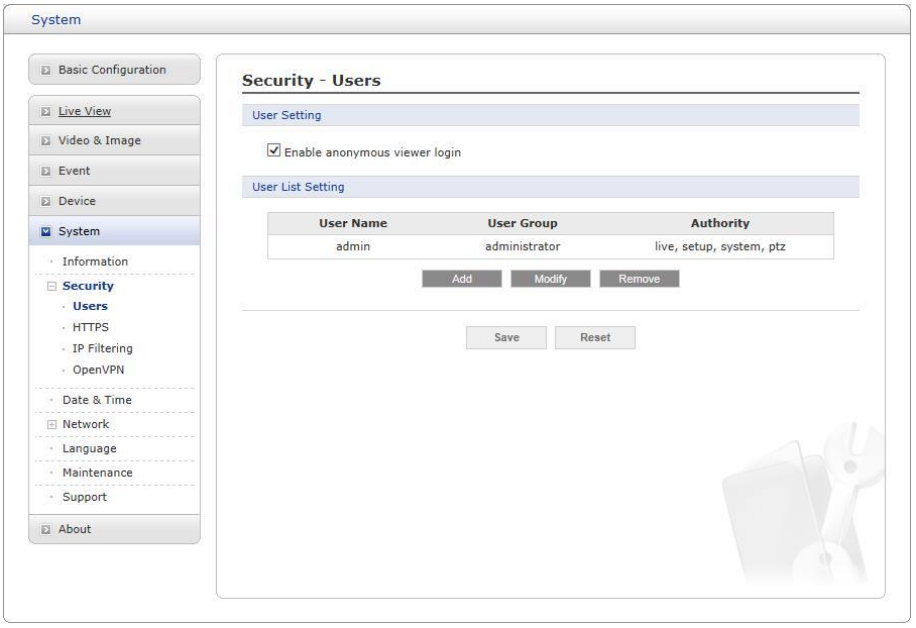
You can enter the system information. This page is very useful when you require device information after installation.

- **Device Name Configuration:** Enter the device name.
- **Location Configuration:** Enter the location information. You can enter up to four locations.

When the settings are complete, click **Save** button to save the settings, or click **Reset** button to clear all of the information you entered without saving it.

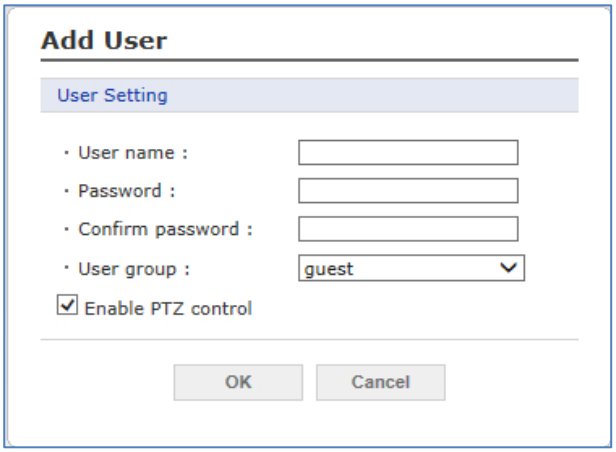
2) Security

▽ Users



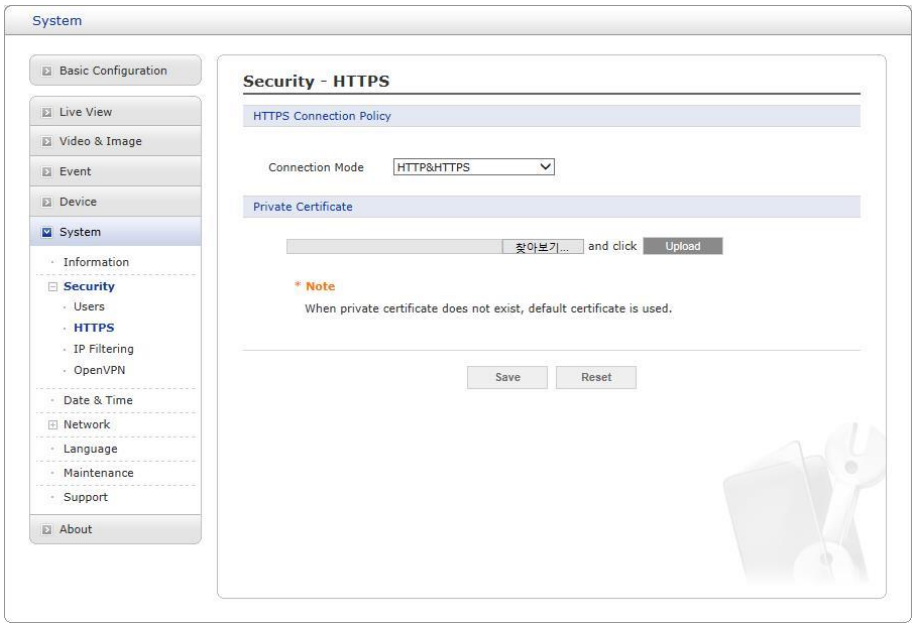
User access control is enabled by default when the administrator sets the root password on first access. New users are authorized with user names and passwords, or the administrator can choose to allow anonymous viewer login to the Live View page, as described below:

- **User Setting:** Check the box to enable anonymous viewer login to the encoder without a user account. When using the user account, users have to log-in at every access.
- **User List Setting:** This section shows how to register a user account. Enter a user name and password to be added, and register them by pressing the Add button. You will see the pop-up window as below.



When the settings are complete, click **Save** button to save the settings, or click **Reset** button to clear all of the information you entered without saving it.

▽HTTPS



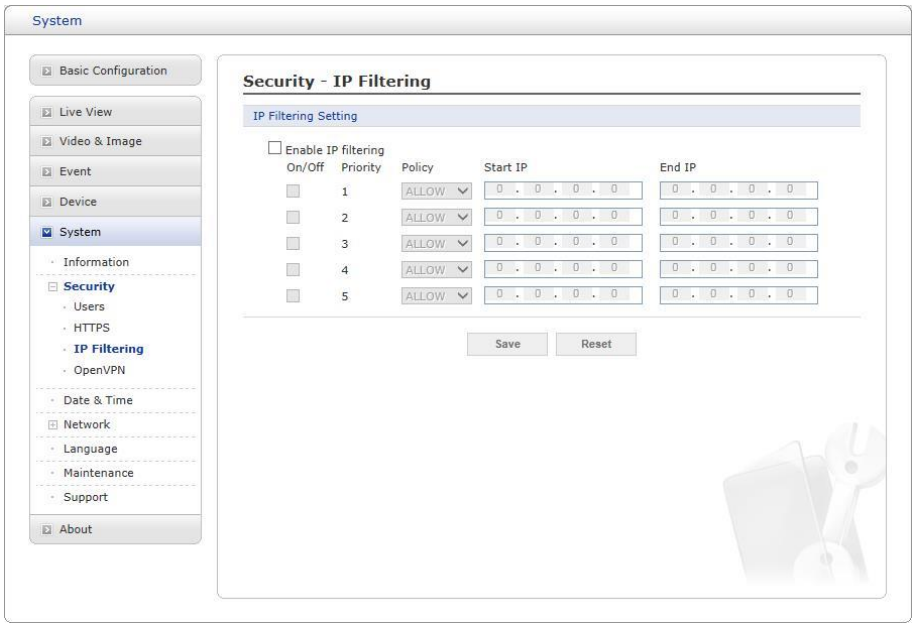
For greater security, the encoder can be configured to use HTTPS (Hypertext Trans- fer Protocol over SSL (Secure Socket Layer)). Then all communication that would otherwise go via HTTP will instead go via an encrypted HTTPS connection.

- **HTTPS Connection Policy:** Choose the form of connection you wish to use from the drop-down list for the administrator, Operator and Viewer to enable HTTPS connection (set to HTTP by default).
  - **HTTP**
  - **HTTPS**
  - **HTTP & HTTPS**
- **Upload Certificate:** To use HTTPS for communication with the encoder, an official certificate issued by a CA (Certificate Authority) must be uploaded from your PC. Provide the path to the certificate directly, or use the **Browse** button to locate it. Then click the **Upload** button.

Please refer to the home page of your preferred CA for information on where to send the request. For more information, please see the online help.

When the settings are complete, click **Save** button to save the settings, or click **Reset** button to clear all of the information you entered without saving it.

▽ IP Filtering



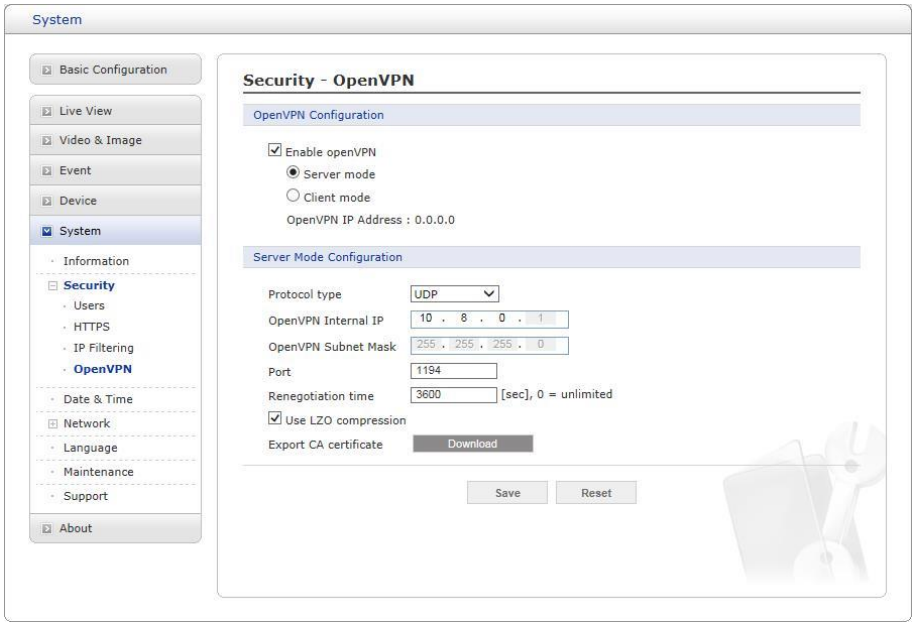
Checking the **Enable IP address filtering** box enables the IP address filtering function. Up to 256 IP address entries may be specified (a single entry can contain multiple IP addresses). Click the **Add** button to add new filtered addresses.

When the IP address filter is enabled, addresses added to the list are set as allowed or denied addresses. All other IP addresses not in this list will then be allowed or denied access accordingly, that is, if the addresses in the list are allowed, then all others are denied access, and vice versa. Also see the online help for more information.

NOTE: Users from IP addresses that will be allowed must also be registered with the appropriate access rights. This is done from Setup > System > Security > Users.

When the settings are complete, click **Save** button to save the settings, or click **Reset** button to clear all of the information you entered without saving it.

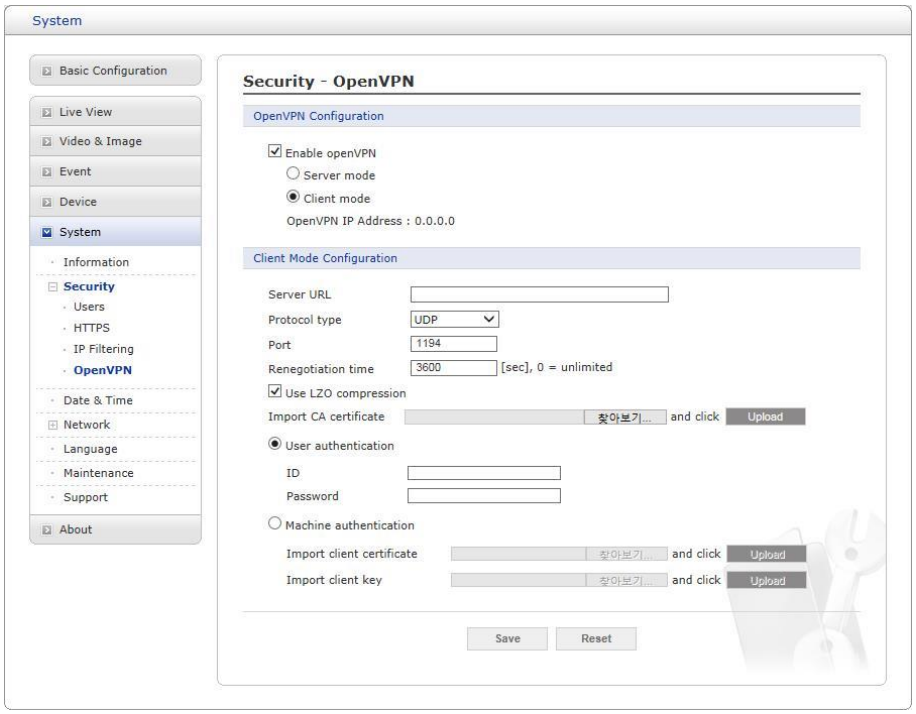
▽ OpenVPN



OpenVPN is a Virtual Private Network using OpenSSL authentication. User can set the encoder in either Server mode or Client mode.

- **OpenVPN Server Mode**

  1. Select Enable openVPN activates mode selection buttons. Choose Server mode, then Server Mode Configuration appears where you can configure Server Mode Settings.
  2. In Server Mode Configuration, you can setup Protocol type, Port number, LZO compression usage, and Renegotiation time, as well as download Server certificate file.
     - Choose Protocol type between UDP and TCP, UDP is preferred. Type in Port number you want to use, default is 1194.
     - Default Renegotiation time is 3600 seconds, and 0 means no verification.
     - “Use LZO compression” determines whether to use cypher compression in connection or not.
     - CA certificate is the certification file issued by Server for Client setup.
  3. After finishing setup, click Save button and then the encoder operates as an Open- VPN Server.

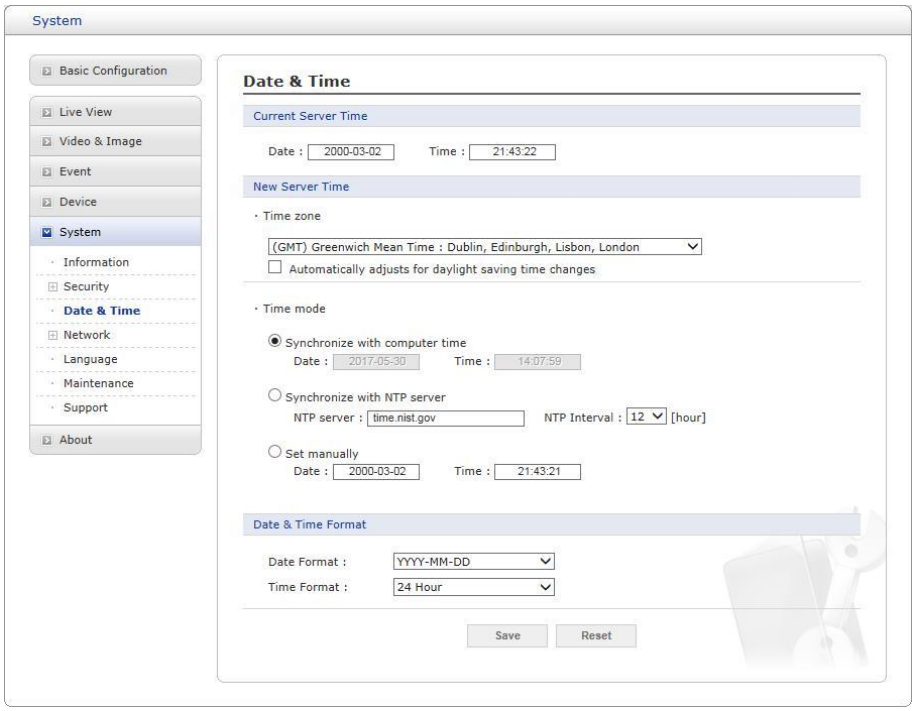


- OpenVPN Client Mode

1. Select Enable openVPN activates mode selection buttons. Choose Client mode, then Client Mode Configuration appears where you can configure Client Mode Settings.
2. In Client Mode Configuration, you can setup Server URL, Protocol type, Port number, LZO usage, and Renegotiation time.
   - Server URL sets OpenVPN IP address.
   - Protocol type, Port number, and LZO setting must match Server setting.
   - Default Renegotiation time is 3600 seconds, and 0 means no verification.
   - Upload CA certificate issued by Server.
3. Select authentication method between User authentication and Machine authentication.
   - For Machine authentication, upload client certificate and client key provided by Server.
   - For User authentication, type in registered ID and Password.
4. After finishing setup, click Save button and then the encoder operates as an Open- VPN Client.

When the settings are complete, click **Save** button to save the settings, or click **Reset** button to clear all of the information you entered without saving it.

3) Date & Time



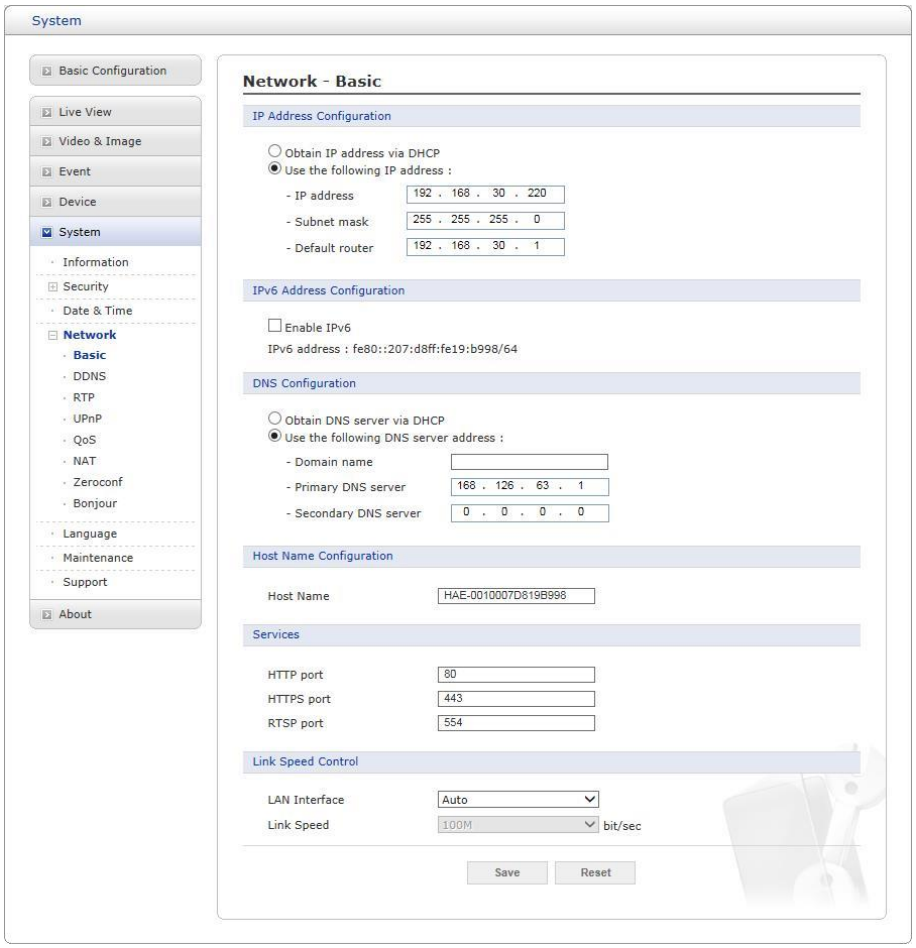
- **Current Server Time**
  This displays the current date and time (24h clock). The time can be displayed in 12h clock format (see below).
- **New Server Time**
  - **Time zone**
    Select your time zone from the drop-down list. If you want the server clock to automatically adjust for daylight savings time, check the box “Automatically adjust for daylight saving time changes”.
  - **Time mode:** Select the preferred method to use for setting the time:
    - **Synchronize with computer time:** Sets the time from the clock on your computer.
    - **Synchronize with NTP Server:** The encoder will obtain the time from an NTP server every 60 minutes.
    - **Set manually:** Allows you to manually set the time and date.
- **Date & Time Format**
  Specify the formats for the date and time (12h or 24h) displayed in the video streams. Select Date & Time format from the drop-down list.
  - **Date Format:** Specify the date format. YYYY: Year, MM: Month, DD: Day
  - **Time Format:** Specify the date format. 24 Hours or 12 Hours

NOTE: If using a host name for the NTP server, a DNS server must be configured under TCP/IP settings.

When the settings are complete, click **Save** button to save the settings, or click **Reset** button to clear all of the information you entered without saving it.

4) Network

▽Basic



- **IP Address Configuration:**
  - **Obtain IP address via DHCP:** Dynamic Host Configuration Protocol (DHCP) is a protocol that lets network administrators centrally manage and automate the assignment of IP addresses on a network. DHCP is enabled by default. Although a DHCP server is mostly used to set an IP address dynamically, it is also possible to use it to set a static, known IP address for a particular MAC address. To obtain IP address via DHCP, check the radio button.
  - **Use the following IP address:** To use a static IP address for the encoder, check the radio button and then make the following settings:
    - **IP address:** Specify a unique IP address for your encoder.
    - **Subnet mask:** Specify the mask for the subnet the encoder is located on.
    - **Default router:** Specify the IP address of the default router (gateway) used for connecting devices attached to different networks and network segments.
- **IPv6 Address Configuration**
  Check this “Enable IPv6” box to enable IPv6. Other settings for IPv6 are configured in the network router.
- **DNS Configuration**
  DNS (Domain Name Service) provides the translation of host names to IP addresses

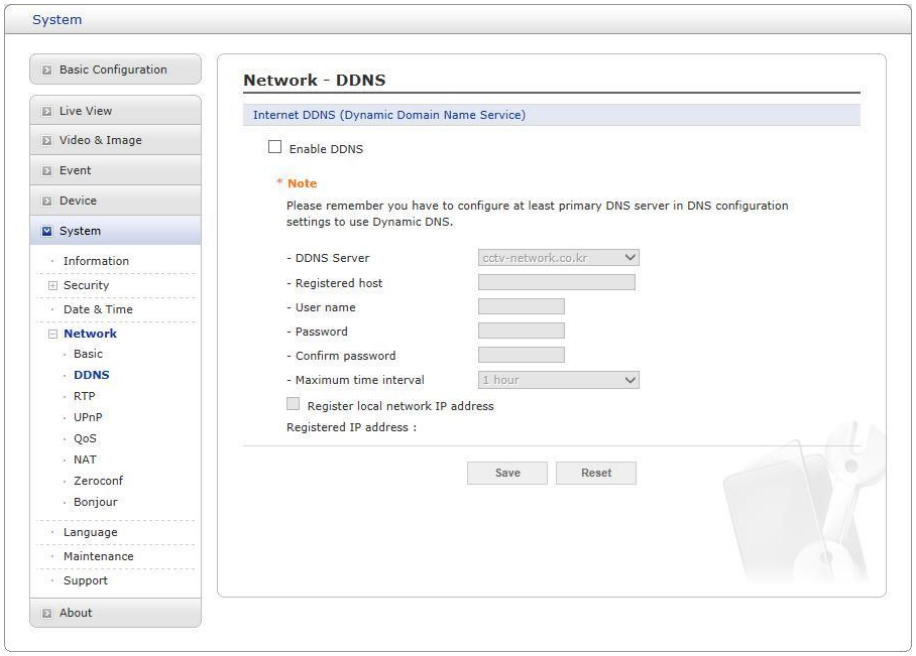
on your network. Check the radio button to obtain DNS server via DHCP or set the DNS server.

- **Obtain DNS Server via DHCP:** Automatically use the DNS server settings provided by the DHCP server.
- **Use the following DNS server address** to enter the desired DNS server by specifying the following:
  - **Domain name:** Enter the domain(s) to search for the host name used by the encoder. Multiple domains can be separated by semicolons (;).
    The host name is always the first part of a Fully Qualified Domain Name, for example, myserver is the host name in the Fully Qualified Domain Name myserver.mycompany.com where mycompany.com is the Domain name.
  - **DNS servers:** Enter the IP addresses of the primary and secondary DNS servers.

- **Host Name Configuration**
  - **Host Name:** Enter the host name to be used as device information in the client software or SmartManager.
- **Services**
  - **HTTP port:** Enter a port to receive a service through the HTTP. Default port number is “80”.
  - **HTTPS port:** Enter a port to receive a service through the HTTPS. Default port number is “443”.
  - **RTSP port:** Enter a port to receive a service through the RTSP. Default port number is “554”.
- **Link Speed Control**
  - **Link Speed:** User can select either 10Mbps or 100Mbps.

When the settings are complete, click **Save** button to save the settings, or click **Reset** button to clear all of the information you entered without saving it.

▽ DDNS

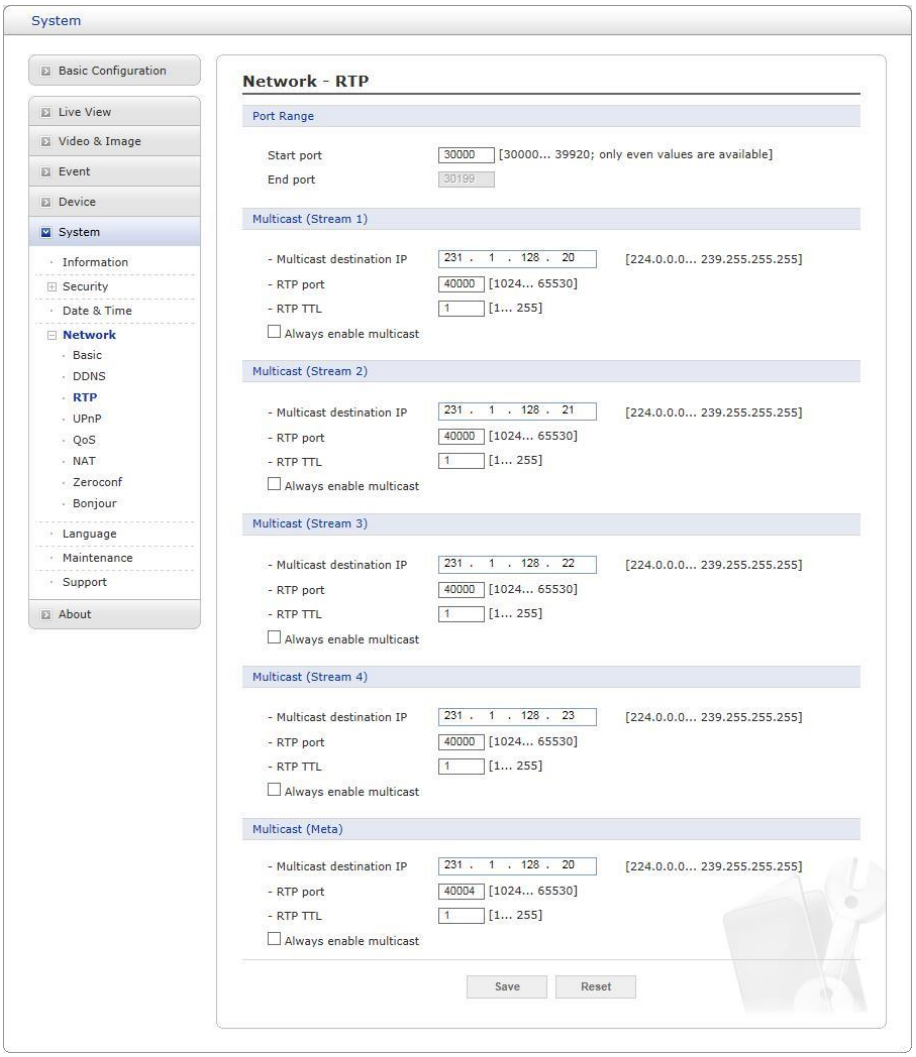


- **Internet DDNS (Dynamic Domain Name Service)**
  When using the high-speed Internet with the telephone or cable network, users can operate the encoder on the floating IP environment in which IPs are changed at every access. Users should receive an account and password by visiting a DDNS service like http://www.dyndns.com/.

  – **Enable DDNS:** Check to have DDNS service available.
    - **DDNS Server:** Select the DDNS server.
    - **Registered host:** Enter an address of the DDNS server.
    - **Username:** Enter an ID to access to the DDNS server.
    - **Password:** Enter a password to be used for accessing the DDNS server.
    - **Confirm:** Enter the password again to confirm it.
    - **Maximum time interval:** Set a time interval to synchronize with the DDNS server. Select the time interval from the drop-down list.
    - **Register local network IP address:** Register a Network Video Server IP address to the DDNS server by checking the box and enter the Registered IP address.

When the settings are complete, click **Save** button to save the settings, or click **Reset** button to clear all of the information you entered without saving it.

▽ RTP

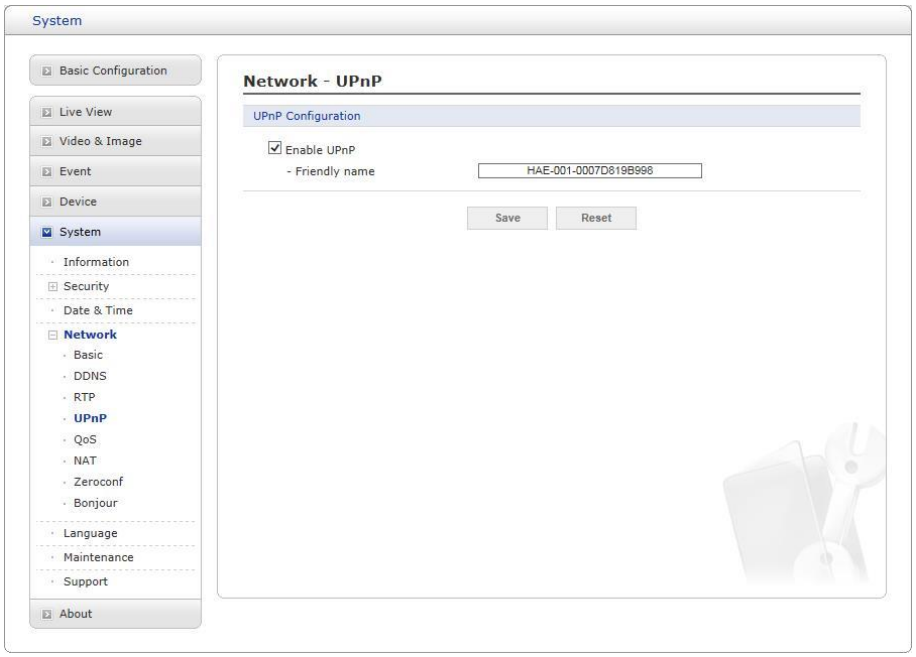


Create a setting for sending and receiving an audio or video on a real-time basis. These settings are the IP address, port number, and Time-To-Live value (TTL) to use for the media stream(s) in multicast H.264 format. Only certain IP addresses and port numbers should be used for multicast streams.

- **Port Range**
  - **Start/End port:** Enter a value between 1024 and 65532
- **Multicast (Stream1/Stream2/Stream3/Audio/Meta)**
  This function is for sending Video and Meta Data to Multicast group.
  - **Enable Multicast:** Check the box to enable multicast operation.
  - **Multicast destination IP:** Enter an IP between 224.0.0.0 and 239.255.255.255.
  - **RTP port:** Enter a value between 1024 and 65532.
  - **RTP TTL:** Enter a value between 1 and 255. If a network status is smooth, enter a lower value. However, if a network status is poor, enter a higher value. When there are many encoder or users, a higher value may cause a heavy load to the network. Consult with a network manager for detailed information.
  - **Always enable multicast:** Check the box to start multicast streaming without opening an RTSP session.

When the settings are complete, click **Save** button to save the settings, or click **Reset** button to clear all of the information you entered without saving it.

▽UPnP

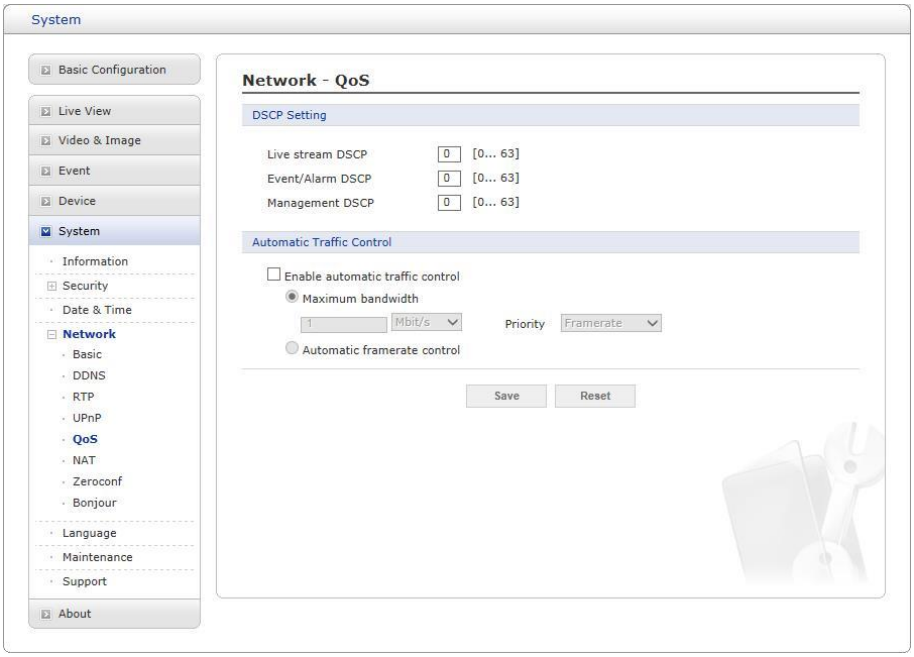


The encoder includes support for UPnP. UPnP is enabled by default, so the encoder is automatically detected by operating systems and clients that support this protocol. Enter a name in the Friendly name field.

NOTE: UPnP must be installed on your workstation if running Windows XP. To do this, open the Control Panel from the Start Menu and select Add/Remove Programs. Select Add/Remove Windows Components and open the Networking Services section. Click Details and then select UPnP as the service to add.

When the settings are complete, click **Save** button to save the settings, or click **Reset** button to clear all of the information you entered without saving it.

▽ QoS



Quality of Service (QoS) provides the means to guarantee a certain level of a specified resource to selected traffic on a network. Quality can be defined as a maintained level of bandwidth, low latency, and no packet losses.

The main benefits of a QoS-aware network are:

1. The ability to prioritize traffic and thus allow critical flows to be served before flows with lesser priority.
2. Greater reliability in the network, due to the control of the amount of bandwidth an application may use, and thus control over bandwidth races between applications.

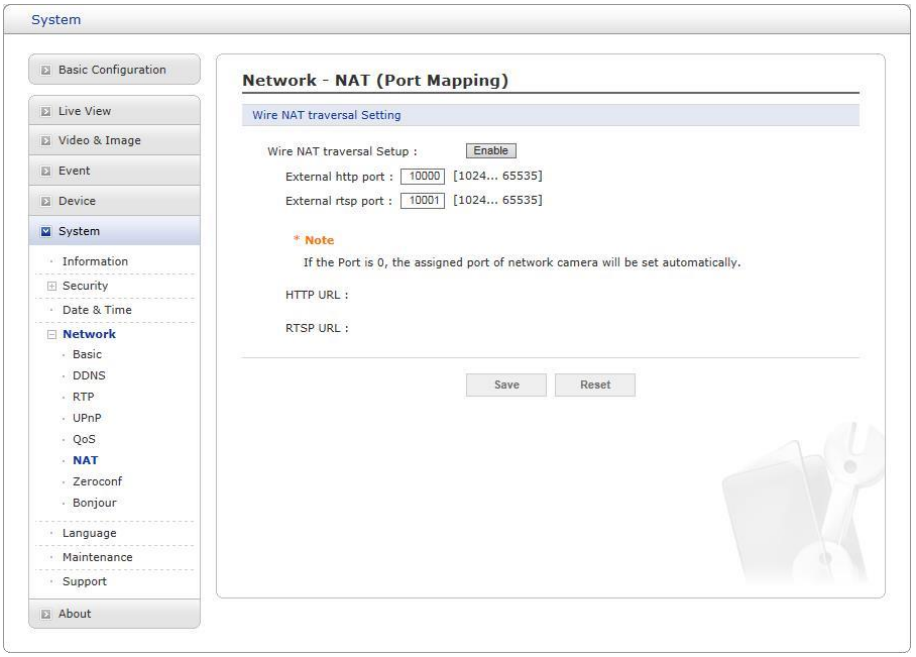
- **DSCP Settings**
  For each type of network traffic supported by your network video product, enter a DSCP (Differentiated Services Code Point) value. This value is used to mark the traffics IP header. When the marked traffic reaches a network router or switch, the DSCP value in the IP header tells the router or switch which type of treatment to apply to this type of traffic, for example, how much bandwidth to reserve for it. Note that DSCP values can be entered in decimal or hex form, but saved values are always shown in decimal. The following types of traffic are marked; enter a value for each type of traffic used:
  - **Live Stream DSCP**
  - **Event/Alarm DSCP**
  - **Management DSCP**
- **Automatic Traffic Control**
  Check the box to enable automatic traffic control. Set a limitation on user network resources by designating the maximum bandwidth. Select either the Maximum bandwidth or Automatic framerate radio button.
  - **Maximum bandwidth:** When sharing other network programs or equipment, it is possible to set a limitation on the maximum bandwidth in the unit of Mbit/s or

kbit/s.

– **Automatic frame rate:** Selected if not influenced by a network-related program or equipment without a limitation on the network bandwidth.

When the settings are complete, click **Save** button to save the settings, or click **Reset** button to clear all of the information you entered without saving it.

▽ NAT (Port Mapping)



- **NAT Settings**

  – **Enable:** Check this box to enable NAT traversal. When enabled, the encoder attempts to configure port mapping in a NAT router on your network, using UPnP. Note that UPnP must be enabled in the encoder (see System > Network > UPnP).

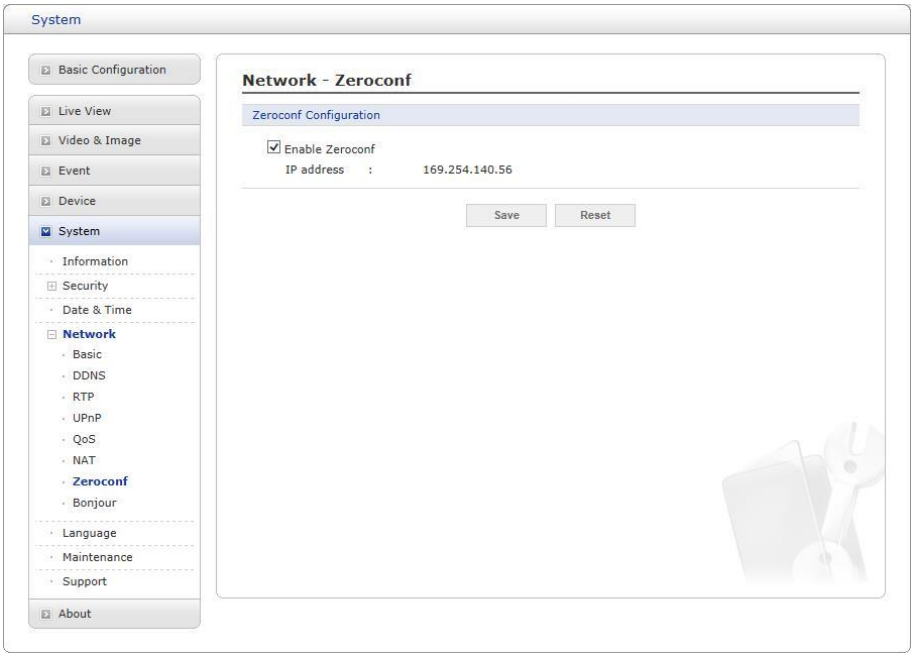
    - **Automatic setting:** When selected, the encoder automatically searches for NAT routers on your network.
    - **Manual setting:** Select this option to manually select a NAT router and enter the external port number for the router in the field provided.

NOTES:

- If you attempt to manually enter a port that is already in use, an alert message will be displayed.
- When the port is selected automatically it is displayed in this field. To change this enter a new port number and click Save.
- For NAT (port mapping) to work, this must be supported by the broadband router.
- The broadband router has many different names: “NAT router,” “Network router,” “Internet Gateway,” “Broadband sharing device” or ”Home firewall,” but the essential purpose of the device is the same.

When the settings are complete, click **Save** button to save the settings, or click **Reset** button to clear all of the information you entered without saving it.

▽ Zeroconf



Zero configuration networking (zeroconf) 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.

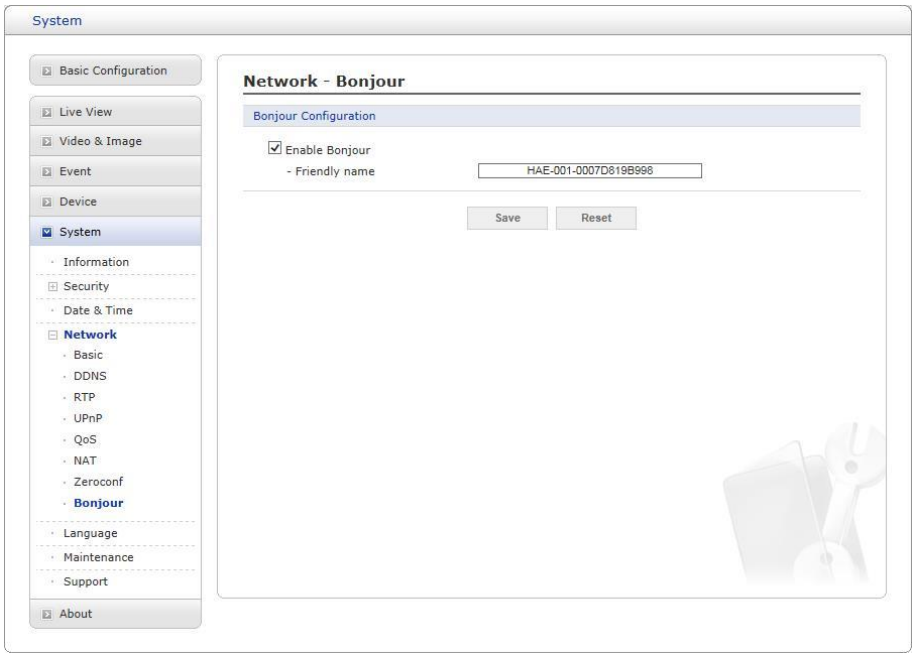
Zeroconf is built on three core technologies:

- Assignment of numeric network addresses for networked devices (link-local address auto configuration)
- Automatic resolution and distribution of computer hostnames (multicast DNS)
- Automatic location of network services, such as printing devices through DNS service discovery.

Click the checkbox to enable Zeroconf.

When the settings are complete, click **Save** button to save the settings, or click **Reset** button to clear all of the information you entered without saving it.

▽ Bonjour



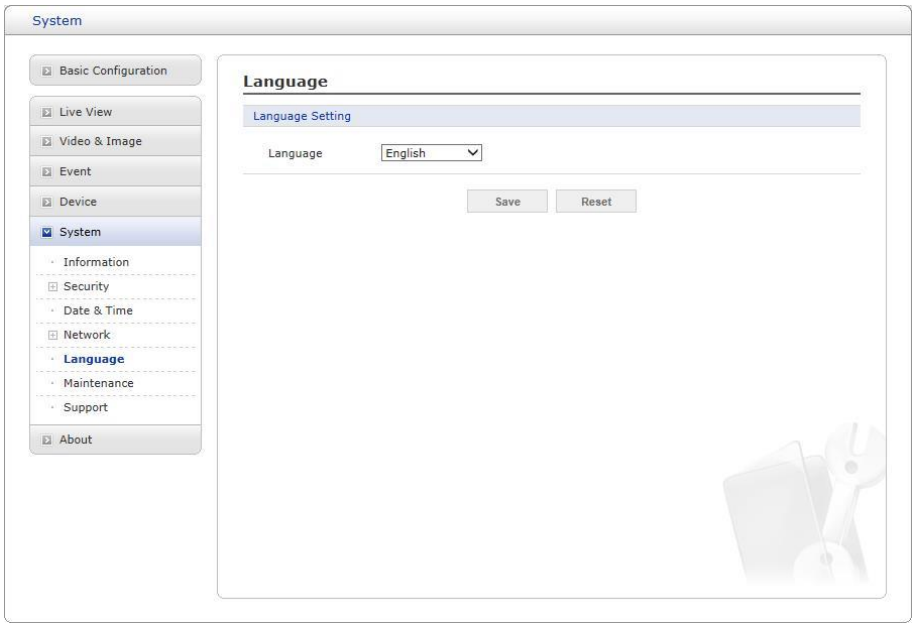
The encoder includes support for Bonjour. When enabled, the encoder is automatically detected by operating systems and clients that support this protocol.

Click the check box to enable Bonjour. Enter a name in the Friendly name field.

NOTE: Also known as zero-configuration networking, Bonjour enables devices to automatically discover each other on a network, without having to enter IP addresses or configure DNS servers. (Bonjour is a trademark of Apple Computer, Inc.)

When the settings are complete, click **Save** button to save the settings, or click **Reset** button to clear all of the information you entered without saving it.

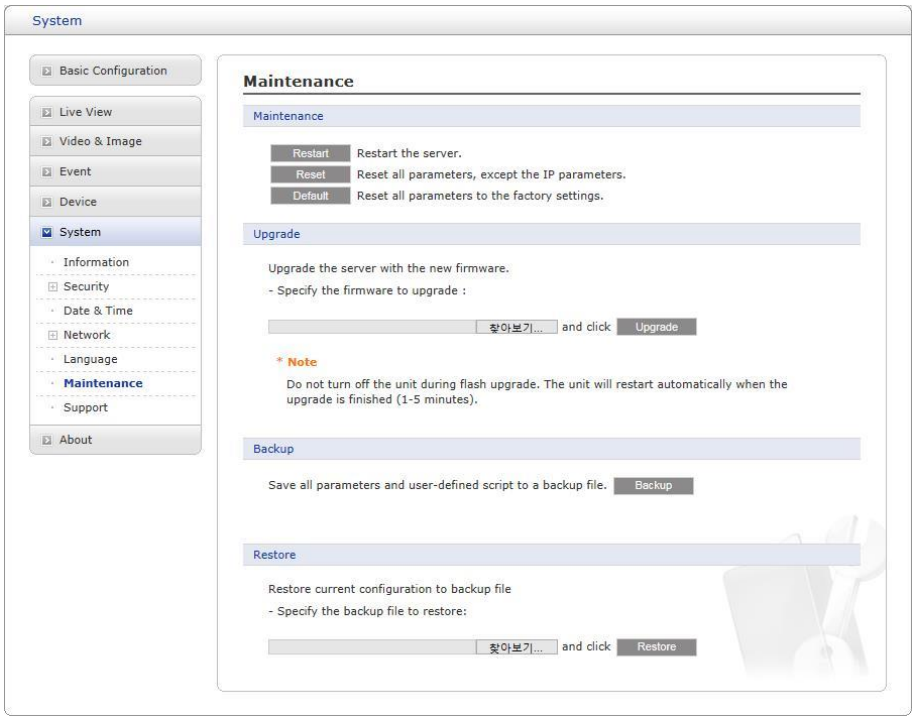
5) Language



Select a user language. The language choices are English, Korean, French, German, Russian and Chinese.

When the settings are complete, click **Save** button to save the settings, or click **Reset** button to clear all of the information you entered without saving it.

6) Maintenance

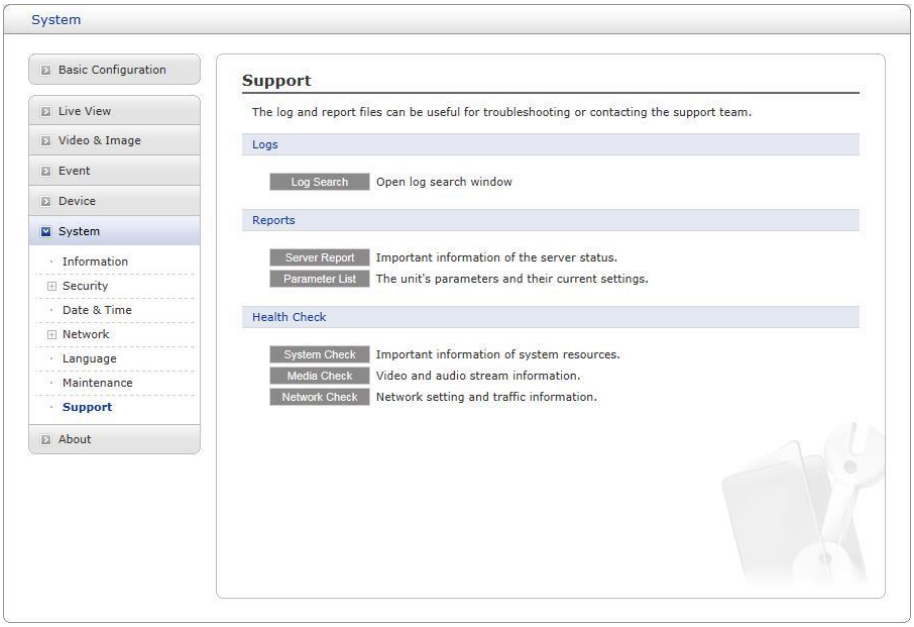


- **Maintenance:**
  - **Restart:** The unit is restarted without changing any of the settings. Use this method if the unit is not behaving as expected.
  - **Reset:** The unit is restarted and most current settings are reset to factory default values. The settings that are not affected are:
    - **the 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 will return all of the encoder's settings to the factory default values (including the IP address).
- **Upgrade:** Upgrade your encoder by importing an upgrade file and pressing the **Upgrade** button. During the upgrade, do not turn off the power of the encoder. Wait at least five minutes and then try to access the encoder again.
- **Backup:** Save the setting values that users have entered to the encoder to a user PC.
- **Restore:** Import and apply a setting value previously saved to a user PC.

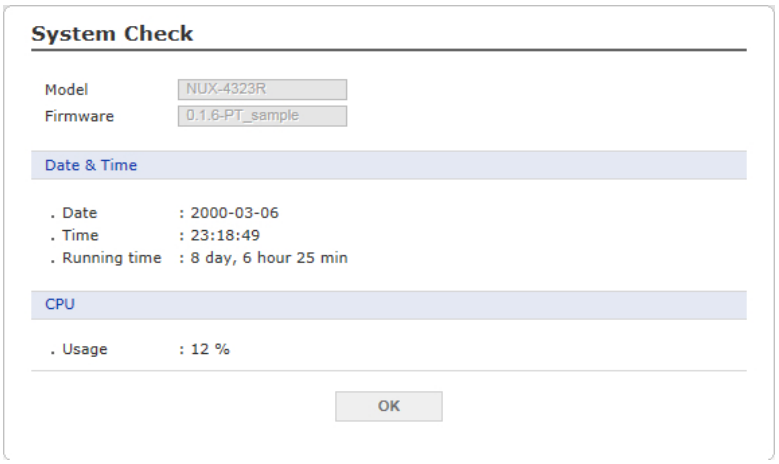
NOTE: Backup and Restore can only be used on the same unit running the same firmware. This feature is not intended for multi-configurations or for firmware upgrades.

7) Support

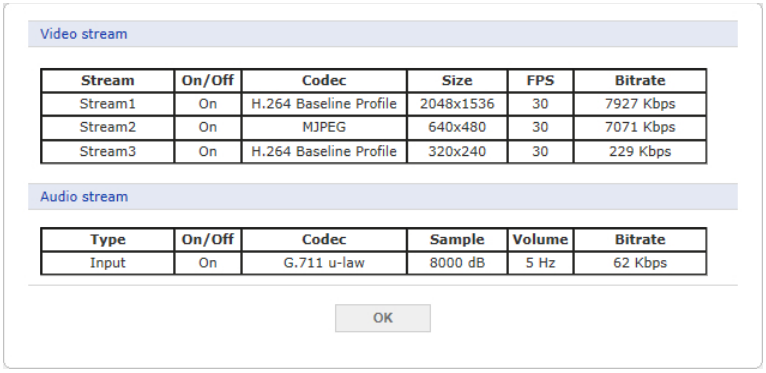
The support page provides valuable information on troubleshooting and contact information, should you require technical assistance.



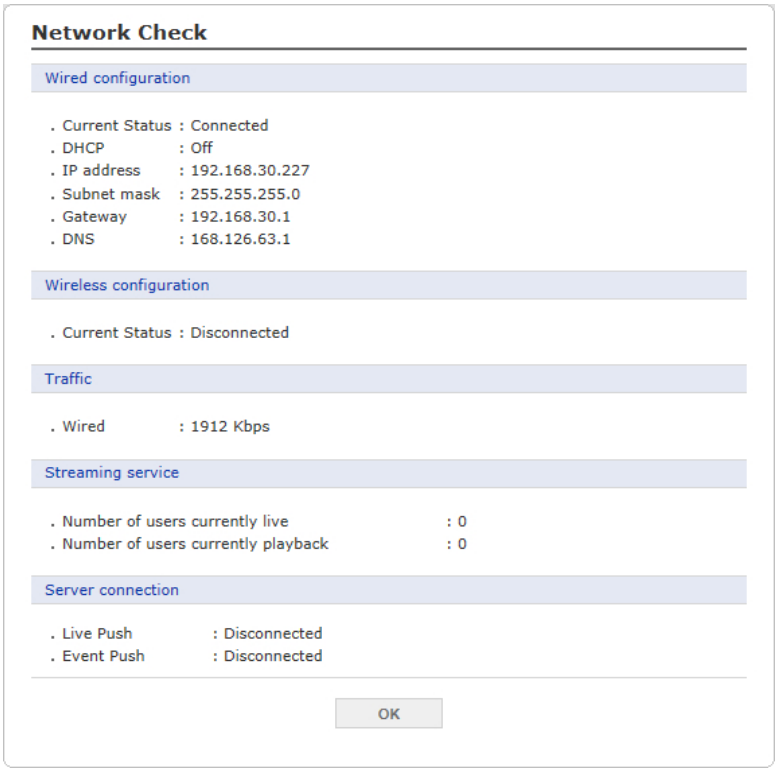
- **Logs:** The encoder supports various log information. Click the **Log Search** button to get the access, event, setup and control information.
- **Reports:**
  - **Server Report:** Click the **Server Report** button to get the important information about the server's status; this should always be included when requesting support.
  - **Parameter List:** Click the **Parameter List** button to see the unit's parameters and their current settings.
- **Health Check:**
  - **System Check:** Click the **System Check** button to get the important information about the encoders system resources. You can see the pop-up window below.



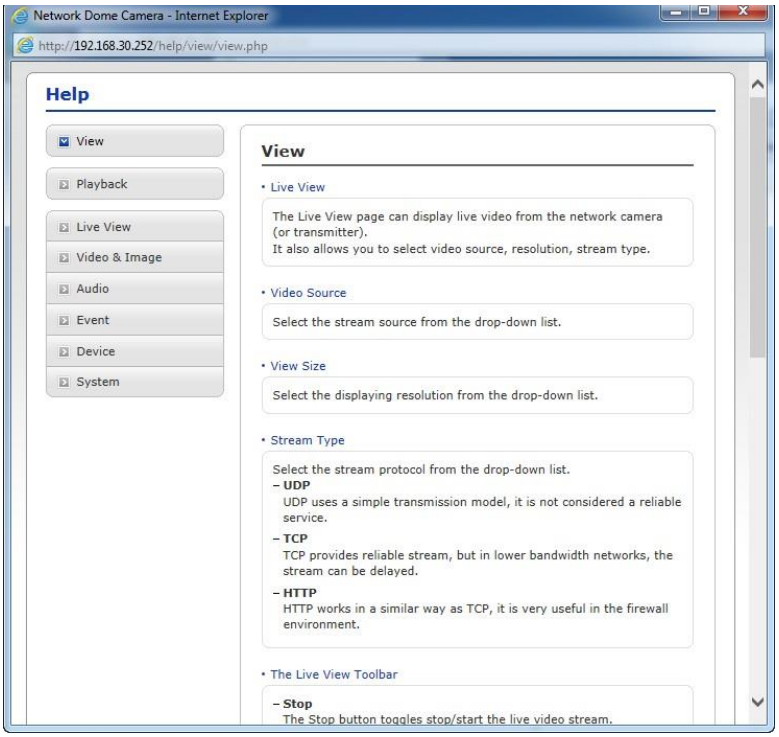
  - **Media Check:** Click the **Media Check** button to get the information about the encoder video and audio stream. You can see the pop-up window below.



– **Networks Check:** Click the **Network Check** button to get the information about the encoders network setting and traffic. You can see the pop-up window below.



3.6 **Help**



The Help information window will be provided as a popup window so that users can open and read it without needing to log-in. It will offer a description of the setting and Help page so that users can manipulate the encoder without a reference to the manual.

A Appendix

A.1 Troubleshooting

Troubleshooting if problems occur, verify the installation of the HD encoder with the instructions in this manual and with other operating equipment. Isolate the problem to the specific piece of equipment in the system and refer to the equipment manual for further information.

Problems/Symptoms	Possible Causes or Corrective Actions
The encoder cannot be accessed by some clients.	If using a proxy server, try disabling the proxy setting in your browser. Check all cabling and connectors.
The encoder 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.
Poor or intermittent network connection.	If using a network switch, check that the port on that device uses the same setting for the network connection type (speed/duplex).
The encoder cannot be accessed via a host name.	Check that the host name and DNS server settings are correct.
Not possible to log in.	When HTTPS is enabled, ensure that 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.
No image using Refresh and/or slow updating of images.	If images are very complex, try limiting the number of clients accessing the encoder.
Images only shown in black & white.	Check the Video & Image setting.
Blurred images.	Refocus the camera.
Poor image quality.	Increased lighting can often improve image quality. Check that there is sufficient lighting at the monitored location. Check all image and lighting settings.
Rolling dark bands or flickering in image.	Try adjusting the Exposure Control setting under AE and AWB part.
H.264 not displayed in the client.	Check that the correct network interface is selected in the Video & Image/Stream.
Multicast H.264 not displayed in the client.	Check with your network administrator that the multicast addresses used by the encoder are valid for your network. Check that the Enable multicast checkbox are enabled in the System/Network/RTP tab. Checks with your network administrator to see if there is a firewall preventing viewing.
Multicast H.264 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.
Color saturation is different in H.264 and Motion JPEG.	Modify the settings for your graphics adapter. Please see the adapter's documentation for more information.
Video cannot be recorded.	Check that the Micro-SD card is inserted properly. Check that the Micro-SD card is formatted properly.

A.2 Preventive Maintenance

Preventive maintenance allows detection and correction of minor that faults before they become serious and cause equipment failure.

Every three-month, perform the following maintenance.

1. Inspect all connection cables for deterioration or other damage.
2. Clean components with a clean damp cloth.
3. Verify that all the mounting hardware is secure.

A.3 System Requirement for Web Browser

- **Operating System:** Microsoft Windows OS Series
- **CPU:** Intel Core 2 Duo 2GHz or higher, 1GB RAM or more, 10GB free disk or higher
- **VGA:** AGP, Video RAM 32MB or higher (1024x768, 24bpp or higher)

A.4 General Performance Considerations

When setting up your system, it is important to consider how various settings and situations will affect performance. Some factors affect the amount of bandwidth (the bit rate) required, others can affect the frame rate, and some affect both. If the load on the CPU reaches its maximum, this will also affect the frame rate.

The following factors are among the most important to consider:

- High image resolutions and/or lower compression levels (or high bitrates) result in larger images. Frame rate and Bandwidth affected.
- Accessing both Motion JPEG and H.264 video streams simultaneously. Frame rate and bandwidth affected.
- Heavy network utilization due to poor infrastructure. Frame rate and Bandwidth affected.
- Heavy network utilization via wireless router due to poor infrastructure. Frame rate and bandwidth affected.
- Viewing on poorly performing client PCs lowers perceived performance. Frame rate affected.

A.5 Product Specification

1CH HD ENCODER

Model		***Specification***
VIDEO		
Video Input		HD-TVI, AHD, CVBS
Video Input Resolution		1080p, 720p, 960H, D1
Compression		H.264 (Baseline, Main, High Profile), MJPEG
Bitrate Control		CVBR, VBR
Resolution		1920x1080, 1280x1024, 1280x720/960, 1024x768, 704x480/576, 640x360/480, 320x240
Frame Rate		Max. 25fps/30fps
Streaming		25/30fps (Quad Stream : H.264 x 3, MJPEG x 1)
SYSTEM		
Video Contents Analysis		Tampering, Line Detector, Field Detector
Motion Detection Area		16 Programmable Area (Include Area 8, Exclude Area 8)
Privacy Mask Zone		8 Programmable Zone
FTP Uploading		MJPEG
Event Notification		E-mail, FTP, Notification Server, XML Notification
Login Authority		Administrator, Operator, Guest
Event Buffering	FTP	Pre: 30sec, Post: 30sec
Manual Trigger		4 Programmable Trigger
Security		Multi User Authority, IP Filtering, HTTPS, SSL
Network Time Sync		NTP Server, Synchronized Computer, Manual
Software Reset		Restart, Reset, Factory Default
Hardware Factory Reset		Yes
Auto Recovery		Backup, Restore
Remote Upgrade		Web Browsing(IE, Chrome, Safari, Firefox), SmartManager
NETWORK		
Protocols		TCP/IP, UDP, IPv4/v6, HTTP, HTTPS, QoS, FTP, UPnP, RTP, RTSP, RTCP, DHCP, ARP, Zeroconf, Bonjour
Client Software		Web, SmartManager, Client S/W, Mobile S/W
Max. User Connection		Live : 10 Users, Playback : 3 Users
API Support		Open API, ONVIF Compliance
Mobile Support		Android, i-OS
EXTERNAL IN/OUT		
Video In		BNC connector
Ethernet		RJ-45 (10/100Base-T)
Serial Port		RS485(Terminal block)
PTZ Control		RS485, UTC
Factory Reset		Tact Switch
Power In		2pin terminal block(up to 1A, 12VDC)
Power Out		2pin terminal block
ETC		
Operating Humidity		0 ~ 90% RH (Non-condensing)
Operating Temperature		-10℃ ~ +45℃
Power Supply		12VDC
Power Consumption		300mA (3.6W)
Dimensions		50.1(W) x 27.7(H) x 117.1(D)mm
Net Weight		Approx. 105g

VIDEOR E. Hartig GmbH
Carl-Zeiss-Straße 8
63322 Rödermark/Germany
Tel. +49 (0) 6074 / 888-0
Fax +49 (0) 6074 / 888-100
www.videor.com
www.eneo-security.com