eneo®

User Manual

1/3" Network Camera/Dome, Day&Night, 2592x1520, H.265, Infrared, PoE, IP66

IED-54F0036MBA
IEB-54F0036M0A
IEB-64M2812M0A
IED-64M2812MBA

WARNING

TO REDUCE THE RISK OF FIRE OR ELECTRIC SHOCK, DO NOT EX-POSE 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 in-tended 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, including interference 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 interference at his own expense.

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

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 adequate measures.

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 manufacturer 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, conve nience 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 in- jury 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 network camera supports the network service for a sensor image with progressive scan, which 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 network camera at once or a single user can monitor various network cameras 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 network camera is fully featured for security surveillance and remote monitoring needs. It is based on the DSP compression chip, and makes it available on the network as real-time, full frame rate Motion JPEG, H.264 and H.265 video streams.

The alarm input and alarm output can be used to connect various third party devices, such as, door sensors and alarm bells.

1.1   Components

This system comes with the following components;

Network Camera   1

Installation Guide/CD   1

Accessory Kit   1

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 network camera offers the highly efficient H.265 or H.264 video compression, which drastically reduces bandwidth and storage requirements without compromising image quality. Motion JPEG is also supported for increased flexibility.

- **Quad streams**

  The network camera can deliver quad video streams simultaneously using H.264/H.265 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 network camera includes intelligent capabilities such as enhanced video motion detection.

- **Improved Security**

  The network camera logs all user access, and lists currently connected users. Also, its full frame rate video can be provided over HTTPS.

- **PoE (Power over Ethernet)**

  This network camera can be powered through PoE (IEEE802.3af), which simplifies installation since only one cable is needed for carrying power, as well as video controls.

- **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 Network Camera, it is necessary to connect a network cable for data transmission, power connection from power adapter. For its fixation on different locations, please consult with an installer.

2.1   Installation

Carefully remove the contents from the box.

- **Fixed Bullet Camera**

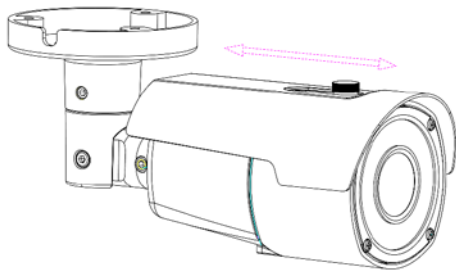To mount the bullet camera, fix the base of the camera with the three screws provided in the accessory kit.

Mounting Screw

Plastic Anchor
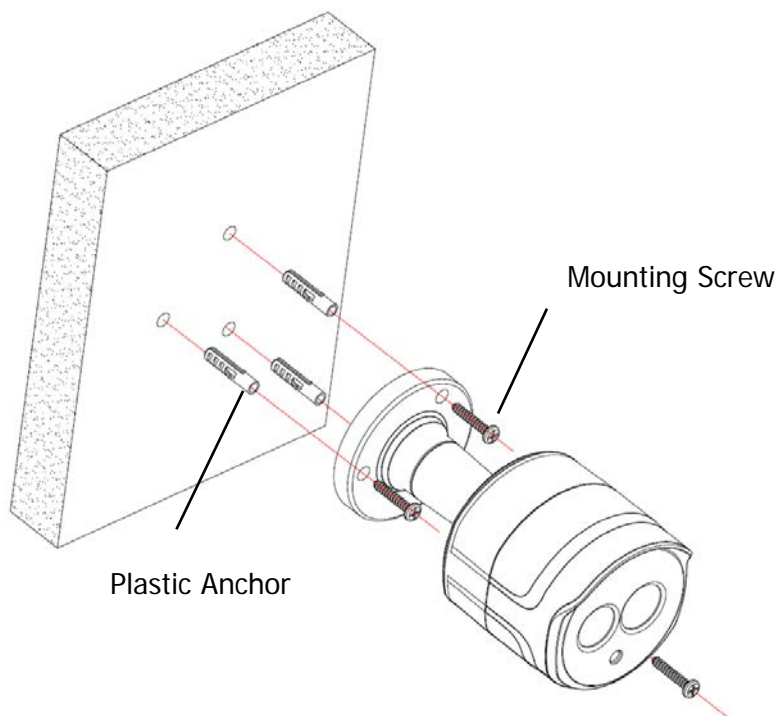
- **MVF Bullet Camera**

1) To mounting the bullet camera, fix the base of the camera with the three screws provided in the accessory kit.

2) Adjust the camera angle and tighten the mount using the L-wrench.

Plastic Anchor

Mounting
Screw

360°

180°
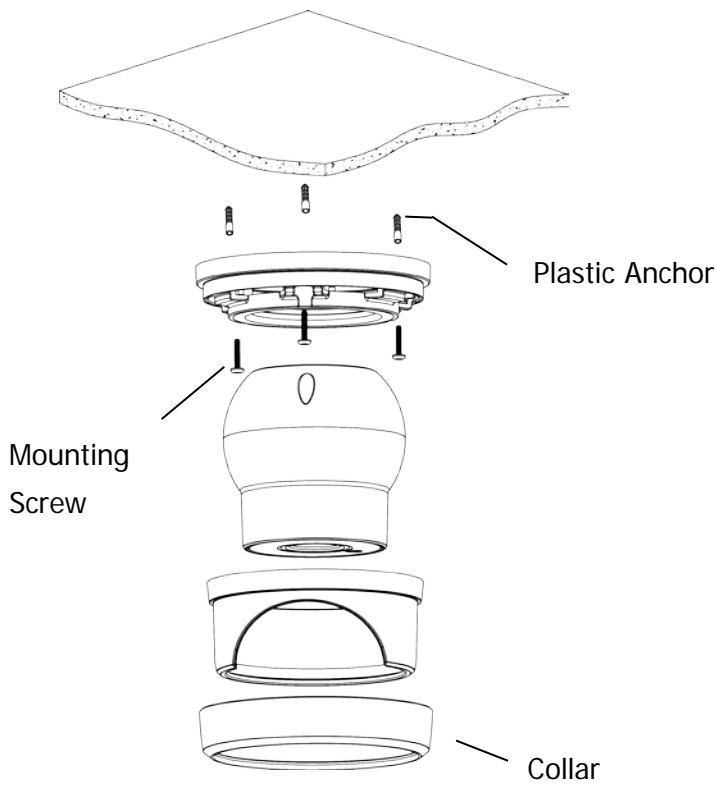
90°

L-wrench
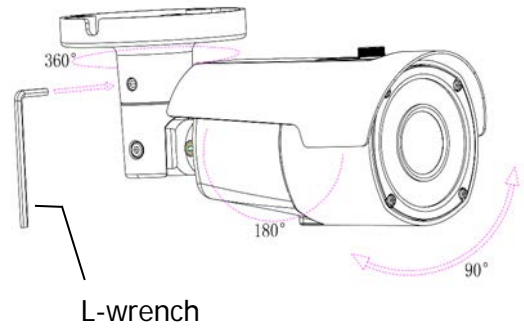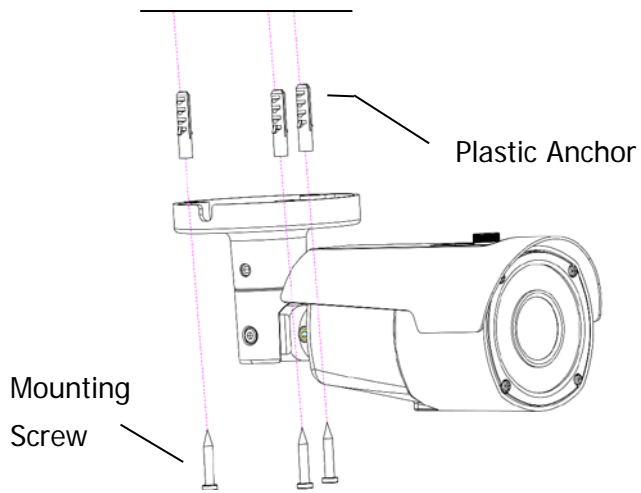
3) Adjust sun-shield position.

- **Fixed Turret Camera**

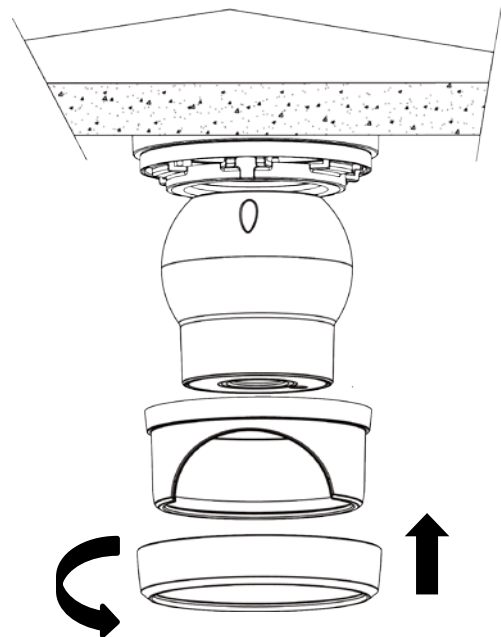1) Paste the template sheet in place at the pro
   per position.
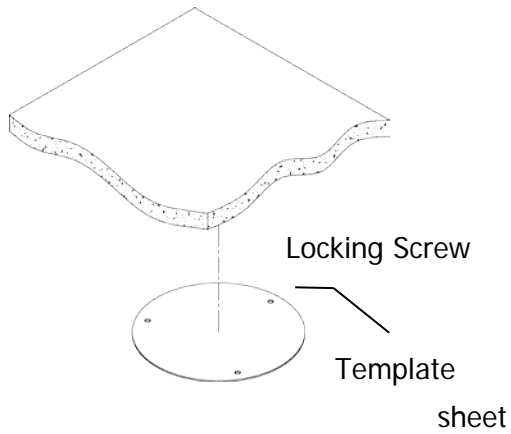
2) Remove the collar off the camera b
   y rotating it down.

Locking Screw

Template

sheet

Collar

3) Fix the base of the camera with the three sc
   rews provided in the accessory kit.

4) Mount the collar back by rotating it
   up.

Plastic Anchor
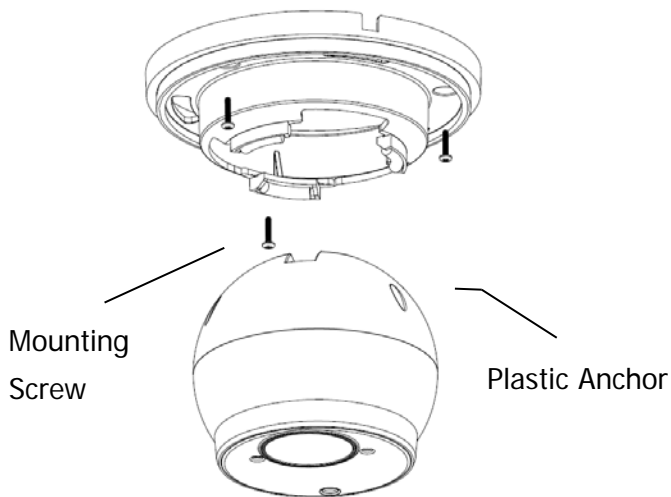
Mounting

Screw

Collar

- **MVF Turret Camera**

1) Paste the template sheet in place at the p roper position.

2) Remove the collar off the camera by rotat ing it down.

Template sheet

Collar

3) Fix the base of the camera with the three screws provided in the accessory kit.

4) Mount the collar back by rotating it up.

Mounting Screw

Plastic Anchor
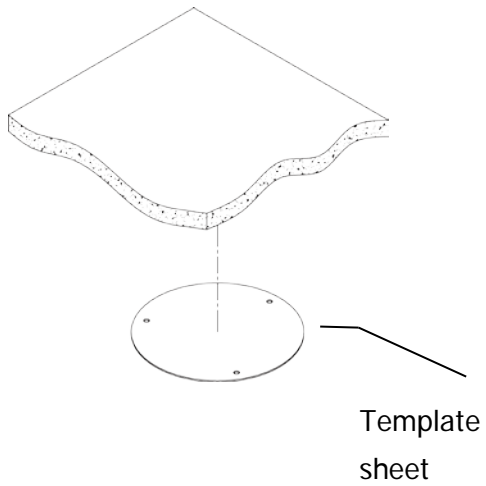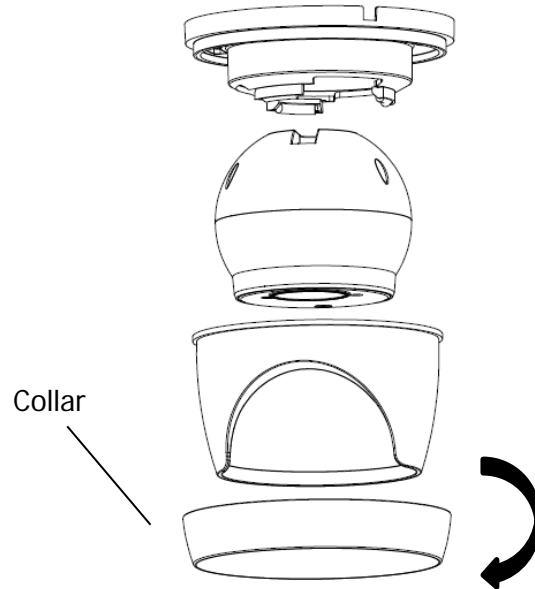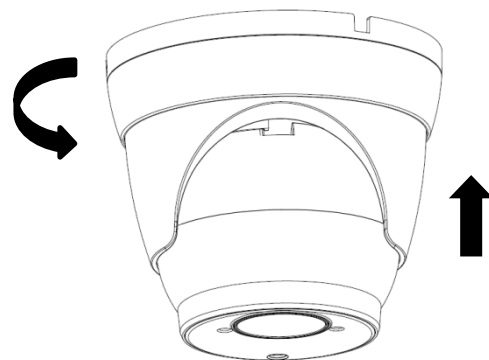
- **Extension cable**

NO	Item	Description
1	RJ-45	Ethernet, RJ-45 port compatible
2	DC Jack	Main Power, DC Jack, DC12V

- **Connecting to the RJ-45**

Connect a standard RJ-45 cable to the network port of the network camera. Generally a cross-over cable is used for directly connection to PC, while a direct cable is used for connection to a hub. You can also use a router featuring PoE (Power over Ethernet) to supply power to the camera.

- **Connecting the Power**

Connect the power of 12 VDC for the network camera. 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.
- A router featuring PoE (Power over Ethernet) can also be used to supply power to the camera.
- For the power specifications, refer to the Appendix, Product Specification.
- If PoE and 12 VDC are both applied, the camera will be supplied with power from PoE.

2.2 Network Connection & IP assignment

The camera supports the operation through the network. When a camera is first connected to the network, it is necessary to allocate an IP address to the device with the "SmartManager" utility on the CD. (Default IP 192.168.30.220)

1) Connect the network camera/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.
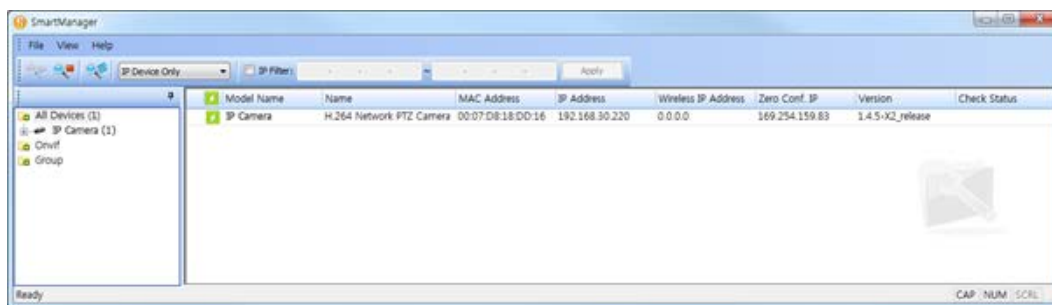
3) Select the camera on the list and click right button of the mouse. You can see the pop-up menu as below.
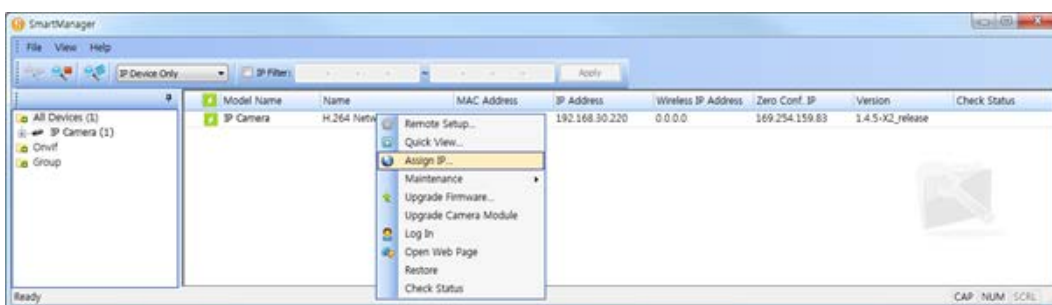
4) Select Assign IP Address. The Assign IP window will display. Enter the required IP address.

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

3. Operation

The network camera 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 network camera in the Location/Address field of your browser.

- You can see a starting page. Click **Live View,** or **Setup** to enter web page.

- The network cameras **Live View** page appears in your browser.
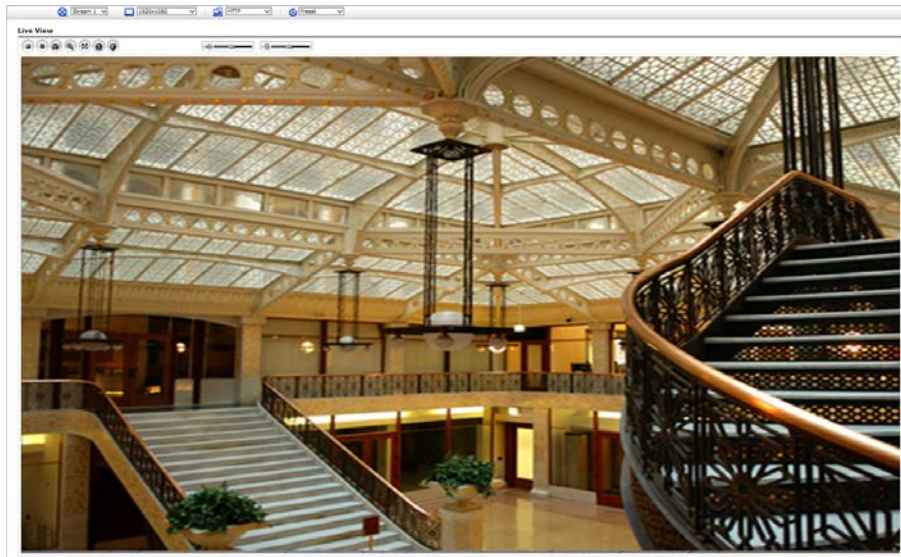
3.2   Access from the internet

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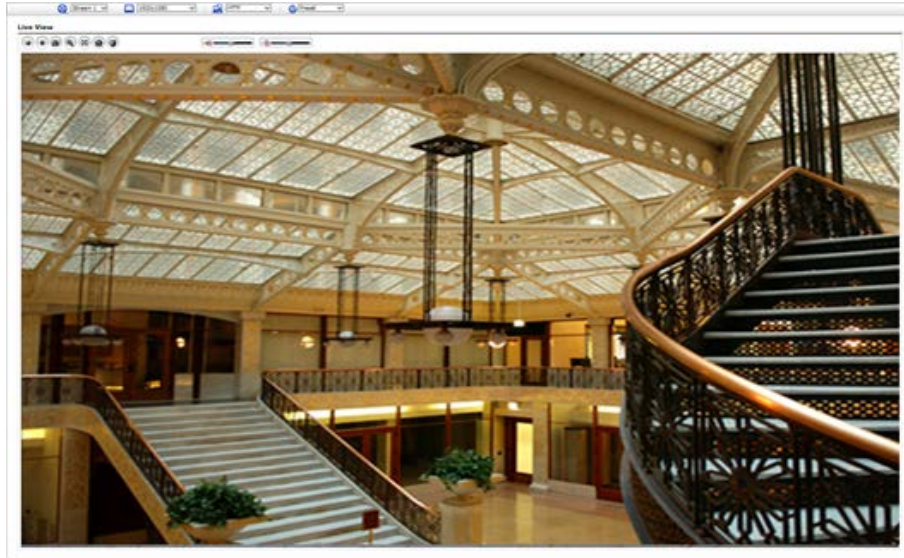
1) General controls

Live View Page   Playback Page   Setup Page   Help Page

Stream 1 The video drop-down list allows you to select a customized or pre-programmed video stream on the Live View page. Stream profiles are con- figured under Setup > Basic Configuration > Video & Image. For more in- formation, please see "Basic Configuration > Video & Image" of User Manual.

2048x1536 The resolution drop-down list allows you to select the most suitable one out of video resolutions to be displayed on Live View page.

HTTP The protocol drop-down list allows you to select which combination of pro- tocols 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 network camera 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 **Lens Control** button allows user to control Zoom and Focus manually. (This Icon appears for motorized lens model only.)
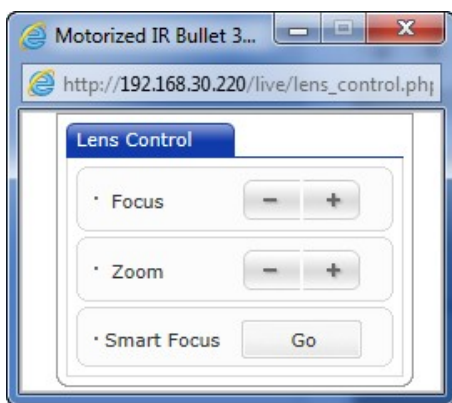
- **Focus:** Click "-" button for far focus and click "+" button to near focus.
- **Zoom:** Click "-" button to zoom out and click "+" button to zoom in. The focus is moved slightly after adjusting zoom; adjust the focus again, as necessary.
- **Smart Focus** User can get automated focus here.

The **Smart Focus** button activates smart focus function which set the focus to the optimum position. (This Icon appears for motorized lens model only.)

3) Video Streams

The network camera 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 network camera provides access to H.264, H.265 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 Network Camera Setup

This section describes how to configure the network camera.

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, Event, and System.

You can configure the network camera by clicking Setup either in the first connection page or the top second-right button of the Live View page. Accessing the network camera 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.

3.5.1 Basic Configuration

You can see the device information in this information page.

1) 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:
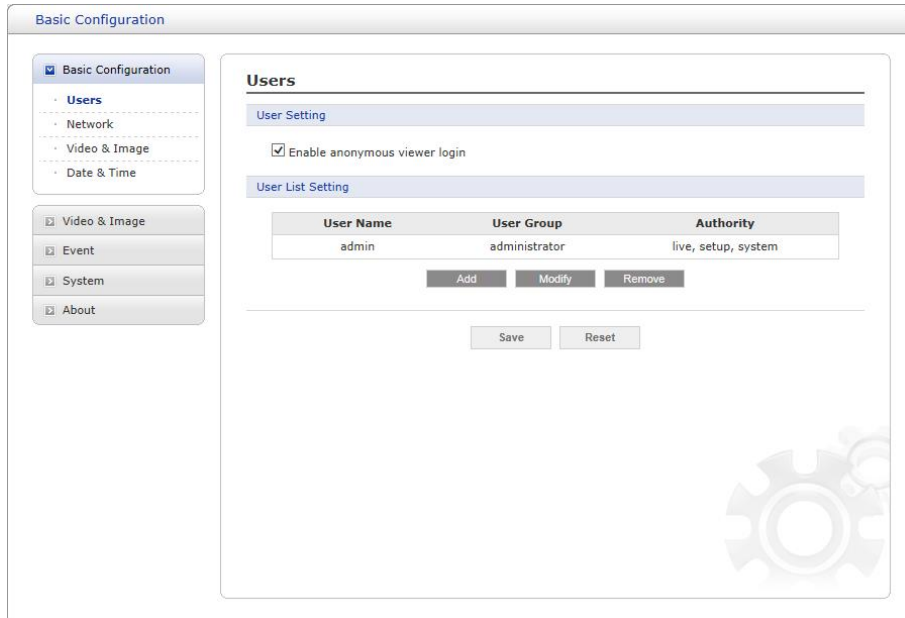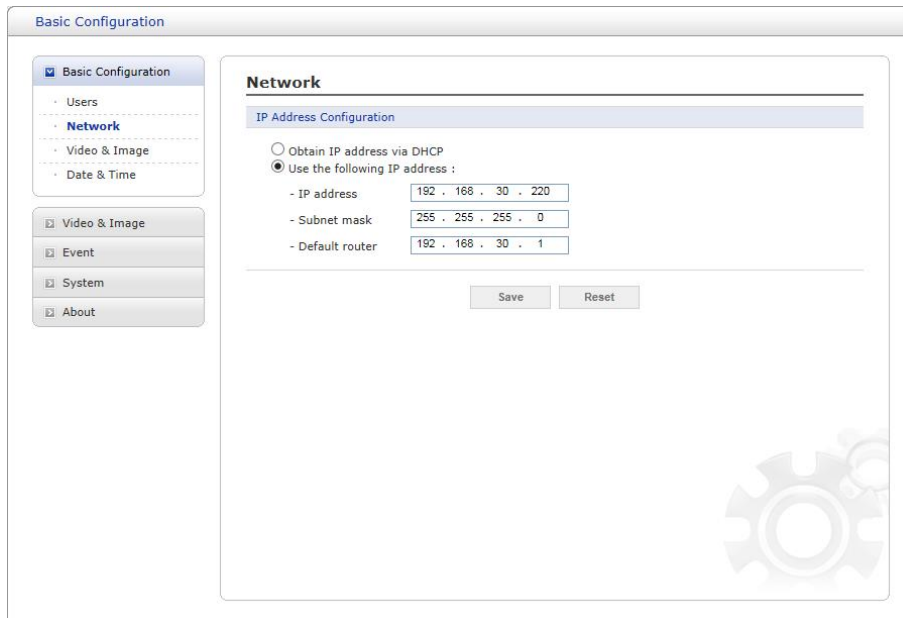
The **user list** displays the authorized users and user groups (levels):

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.

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

2) Network

The network camera 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 network camera can be set automatically via DHCP, or a static IP address can be set manually. If IPv6 is enabled, the network camera 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 network camera, check the radio button and then make the following settings:

    - **IP address:** Specify a unique IP address for your network camera.

    - **Subnet mask:** Specify the mask for the subnet the network camera 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 network camera 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.

3) Video & Image
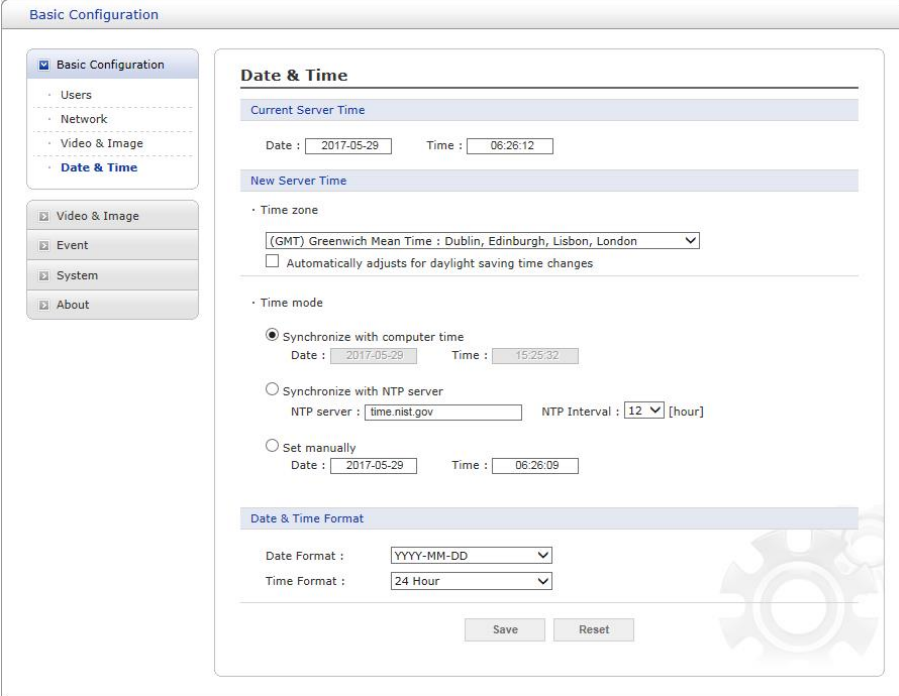

User can setup and change setting of individual video stream in this page.

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

4) 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.

3.5.2 Video & Image

1) Basic

- **Sensor Setting:**

    – **Capture mode:** User can select sensor capture mode between 1920x1080(2MP) /2592x1520(4MP) and NTSC/PAL (Some models are fixed to NTSC or PAL). If 4MP is selected, max frame rate is limited to 20fps(4MP model only).

- **Stream 1 Setting:**

    – **Codec:** The codec supported in Stream 1 is H.264 and H.265

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 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/H.265 Main Profile:**

Primary profile for low-cost applications that require additional error   robustness, this profile is used rarely in videoconferencing and mobile applications; it does add additional error resilience tools to the Constrained Baseline Profile. The importance of this profile is fading after the Constrained Baseline Profile has been defined.

    · **H.264 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 Constant Bit Rate(CBR) or Constrained Variable Bit Rate (CVBR). Constant bit rate means that the rate at which a codec's output data should be consumed is constant. CBR is useful for streaming on limited capacity channels since it is the maximum bit rate that matters, not the average, so CBR would be used to take advantage of all of the capacity. CBR would not be the optimal choice for storage as it would not allocate enough data for complex sections (resulting in degraded quality) while wasting data on simple sections.

- **CBR:** Constrained Bit Rate.
- **CVBR:** VBR with maximum bitrate which is set in Bitrate.

- **Bitrate:** Maximum bitrate for CBR or CVBR in the range of 100kbps ~8Mbps.

- **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 setting.
- **MJPEG Frame rate:** Same as the stream 1 setting.
- **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:** Same as the Stream 1 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.

2) Privacy Masking
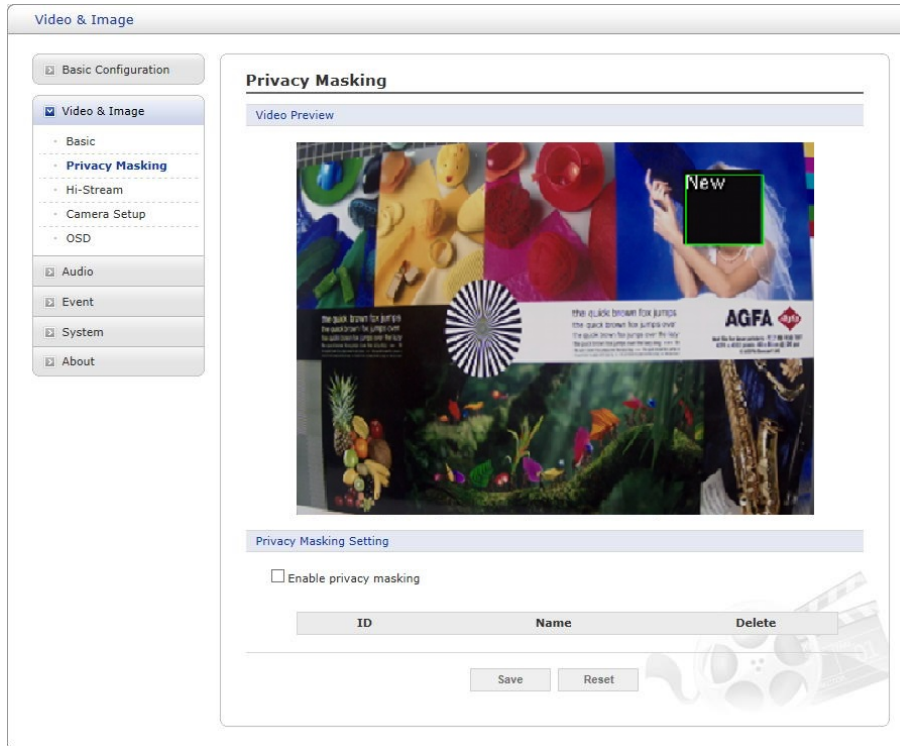
The privacy masking function allows you to mask parts of the video image to be transmitted. You can set up to eight privacy masks.

The privacy masks are configured by Mask windows. Each window can be selected by click- ing 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.

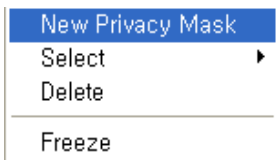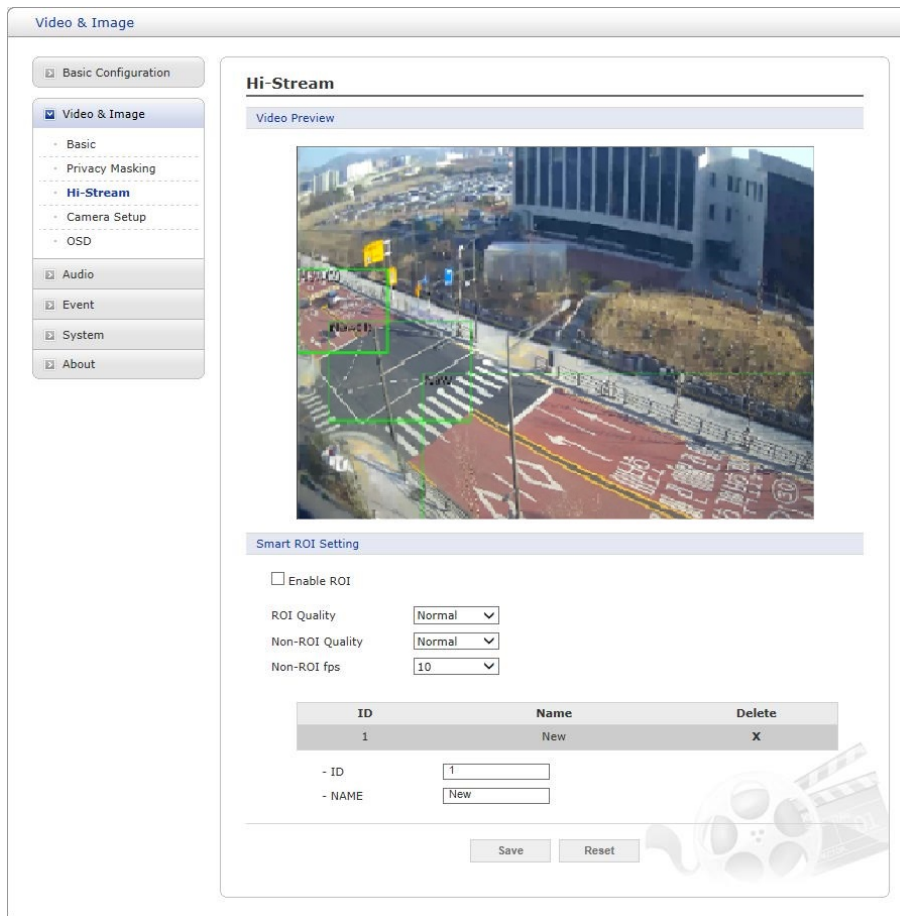3. Click and drag mouse to designate a mask window area.

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.

4) Hi-Stream
The Hi-Stream function allows reduce bandwidth by using compression and frame rate control.

- **Enable ROI:** Select 'Enable ROI' to active Hi-Stream function. Video mode will be fixed to CVBR.

  - Create region: Click the right button of mouse and select **New ROI Area**.
       Click the left button of mouse and drag to make window.
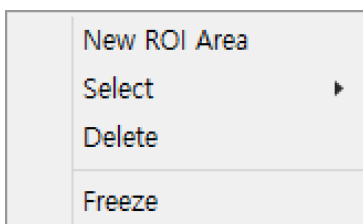
  - Delete Region: Click the right button of mouse and select the region.
       Click **Delete** or click **X** from the region table.

  - **ROI Quality:** Set quality of the selected area.
  - **Non-ROI Quality:** Set quality of the non-selected area.
  - **Non-ROI fps:** Set frame rate of the non-selected area.

5) Camera Setup

In this page, user can setup Exposure Control, White Balance Control, Image Appearance, and Day & Night control.

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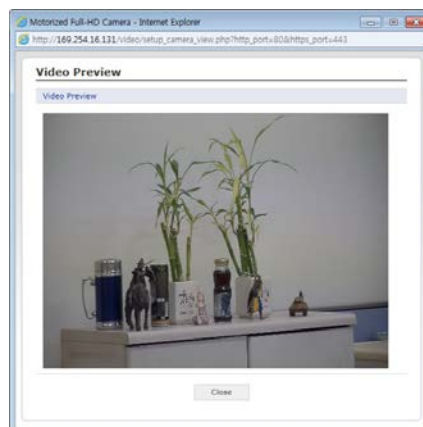
- **Exposure Control**

- **Mode:** Determines exposure mode among automatic and flicker-free modes.
- **Max. gain:** Sets maximum gain threshold.
- **Shutter:** Determines shutter mode between automatic and fixed. For automatic 6 sets the maximum shutter speed, and for fixed 5 sets the shutter speed for the camera.

  In case of fixed shutter speed, this pull-down shows selectable shutter speeds depend on the exposure selection in 1.
- **Max. shutter:** Select maximum shutter speed if Shutter is in automatic mode. The pull-down shows selectable maximum shutter speeds depend on the exposure selection in 1.

- **Image Appearance**
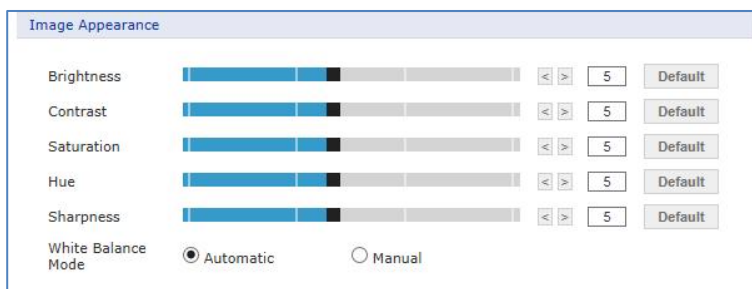
This provides access to the advanced image settings for the network camera.

- **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.
- **White Balance Mode:** Select white balance mode which fits camera installation environment. In case of Manual mode, user can set R, G, B gain manually.

- **Enhance Control**
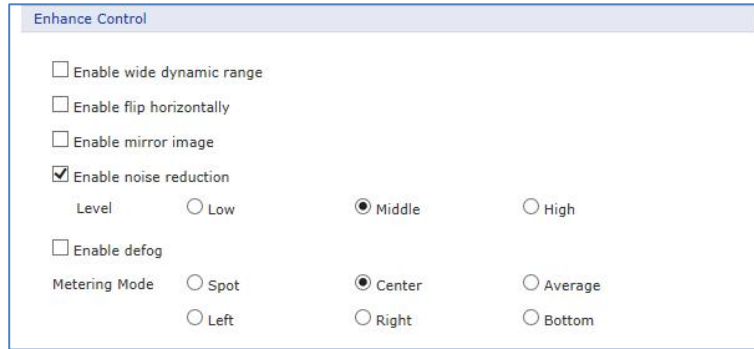
- – **Enable wide dynamic range:** Activates WDR which cannot be used with Defog function. If WDR is activated, shutter mode becomes automatic only.
- – **Enable flip horizontally:** Check this box to flip the image.
- – **Enable noise reduction:** Check this box to activate the noise reduction. Once enabled, you can select noise reduction level.
- – **Enable defog:** Check this box to activate the defog function.

Once enabled, you can select **Metering Mode.**

* Metering Mode: Method of measuring the intensity of the light hitting and reflected by a subject in order to determine the exposure required.

- • **Day & Night Control**

User can setup Day & Night operation mode among Automatic, Day, and Night.
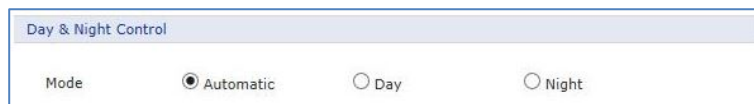
- – **Mode:**
  - ᐧ **Automatic:** Normally displays color image, and switches automatically to black & white image after the ambient light level reaches a pre-defined thresh- old.
  - ᐧ **Day:** Always displays color image.
  - ᐧ **Night:** Always displays black & white image.
- • **IR Control**

- – **Enable IR:** Set this checkbox to activate IR operation.

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) OSD

This camera 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.
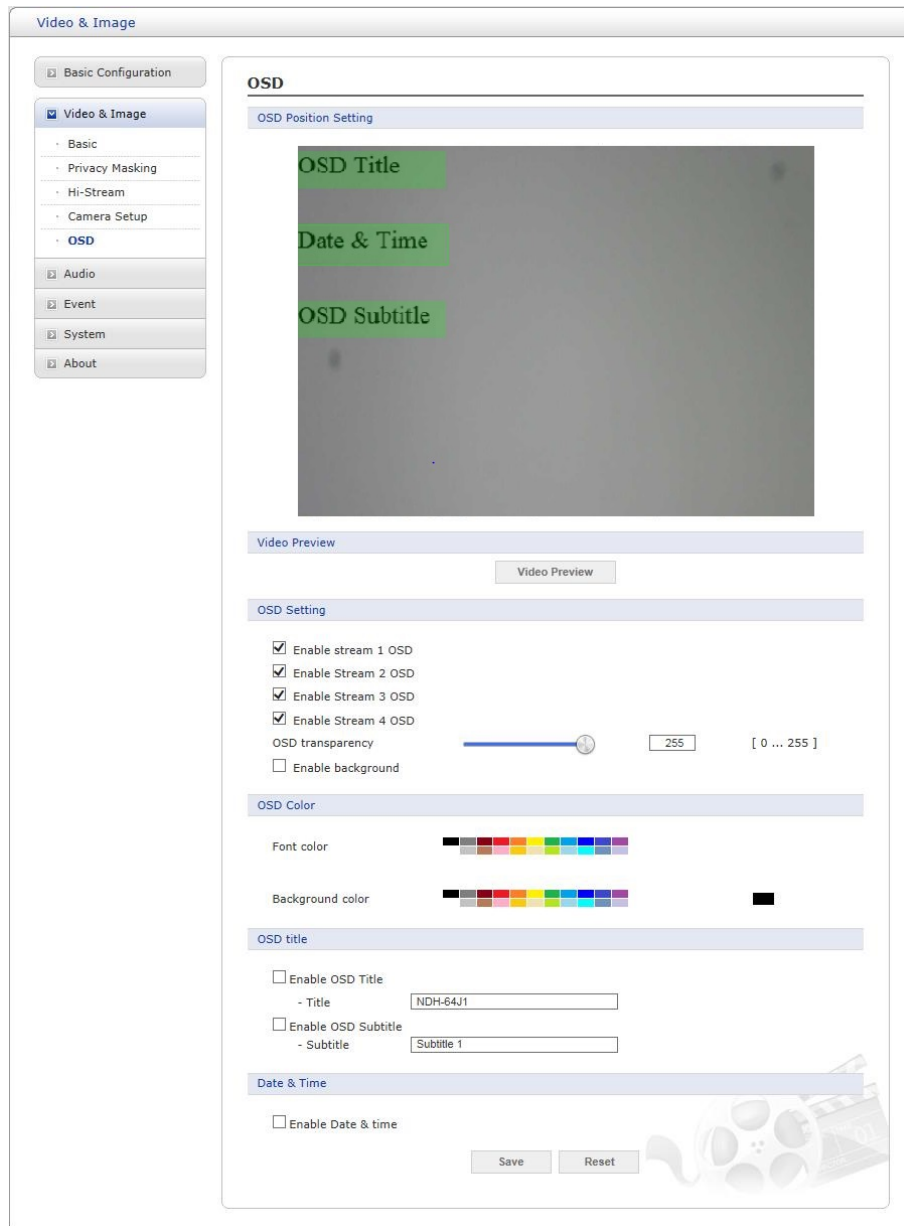
- **Video Preview:** User can check the position of OSD on actual video via preview pop- up window.

- **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.

- **OSD title:** User can show or hide OSD title and subtitle, and can change OSD title by type 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
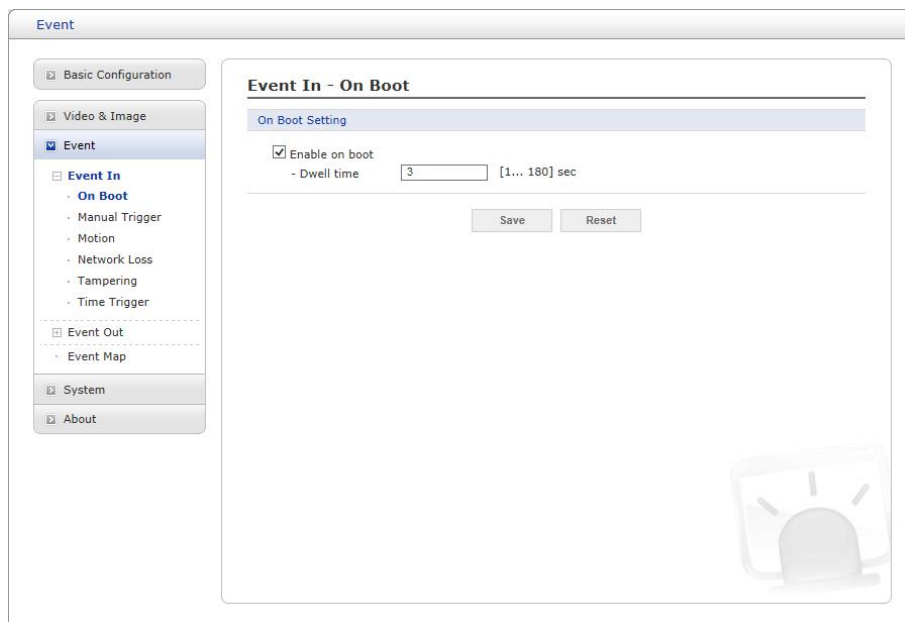
This is used to trigger an event every time the network camera is started. Select "Enable on boot" to activate the On Boot event.

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**
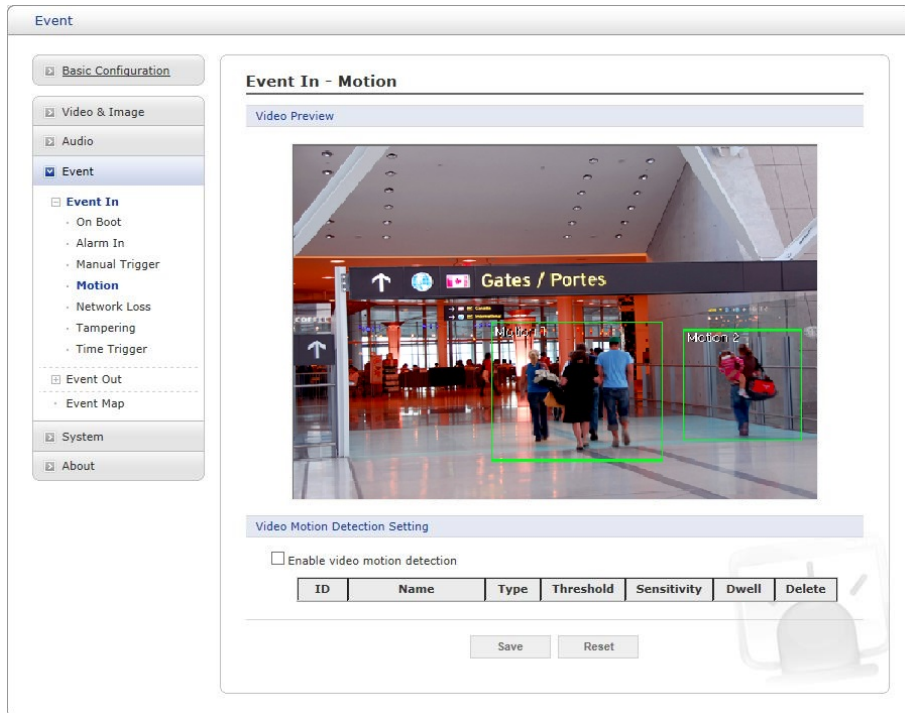

This option makes use of the motion detection function with 16 programmable areas, 8 **Include** and **Exclude** zones each.
Click right mouse button on the preview window shows selection pop-up of **New Motion, New Mask, Select, Delete, and Freeze.**

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**

33
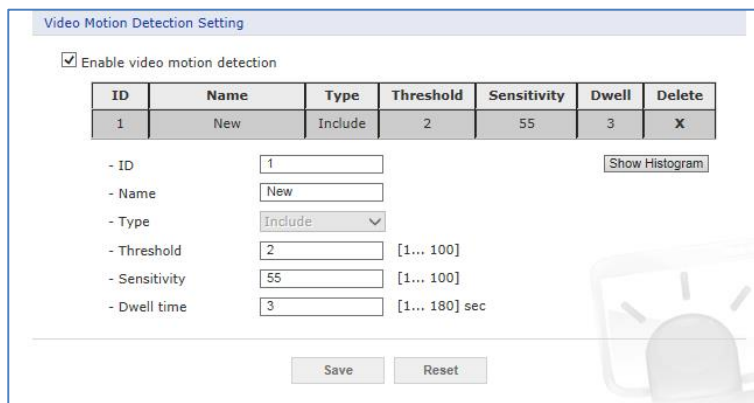
- **ID:** Order of generation, **Include** 1~8, **Exclude** 9~16.

- **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 trigger- ing.

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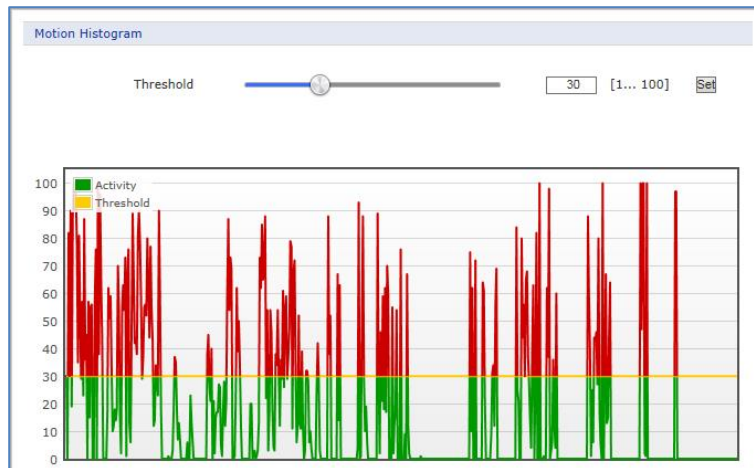
User can select any box by clicking name on the preview window or click on the list. User can delete selected zone via right mouse click selection for a selected box, or click any one of **X** button in the zone list.

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.

▽ **Network Loss**
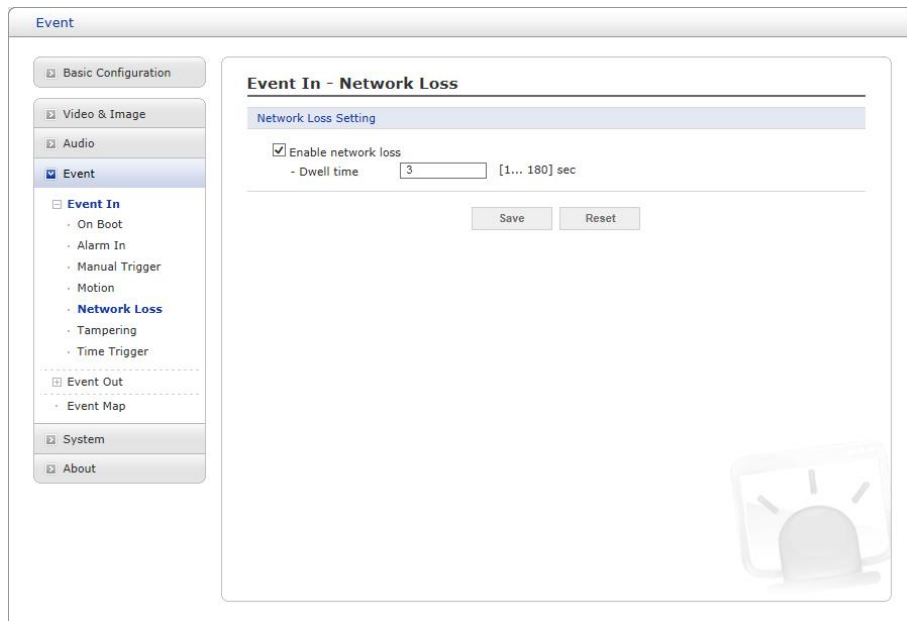
This is used to trigger an event every time the network connection is failed.

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.

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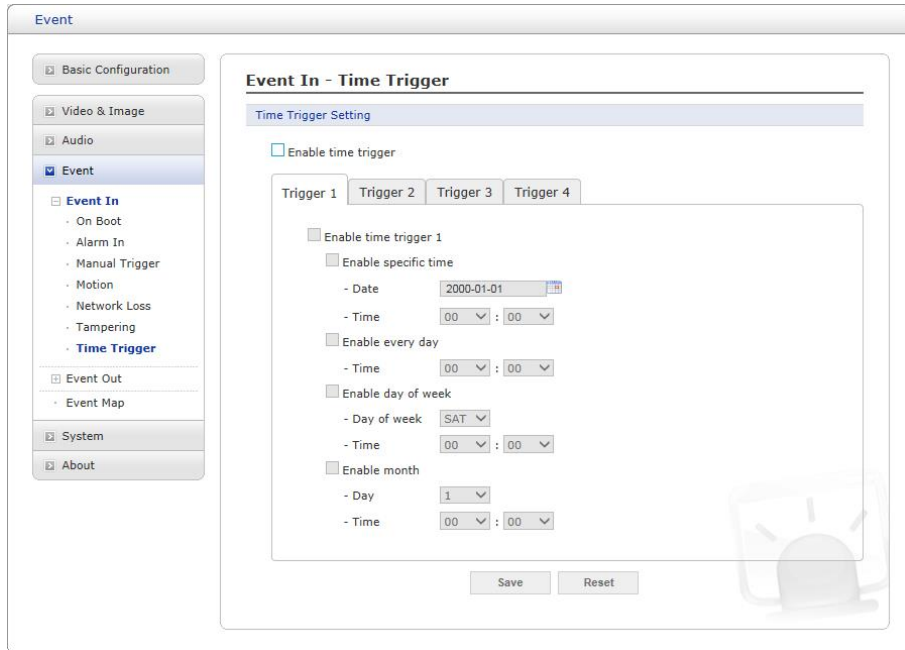
Time Trigger is to set alarms at specific time. User can set up to four time triggers and each time trigger can be set to specific date in the calendar, every day, day of the week, or date of every month.

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.
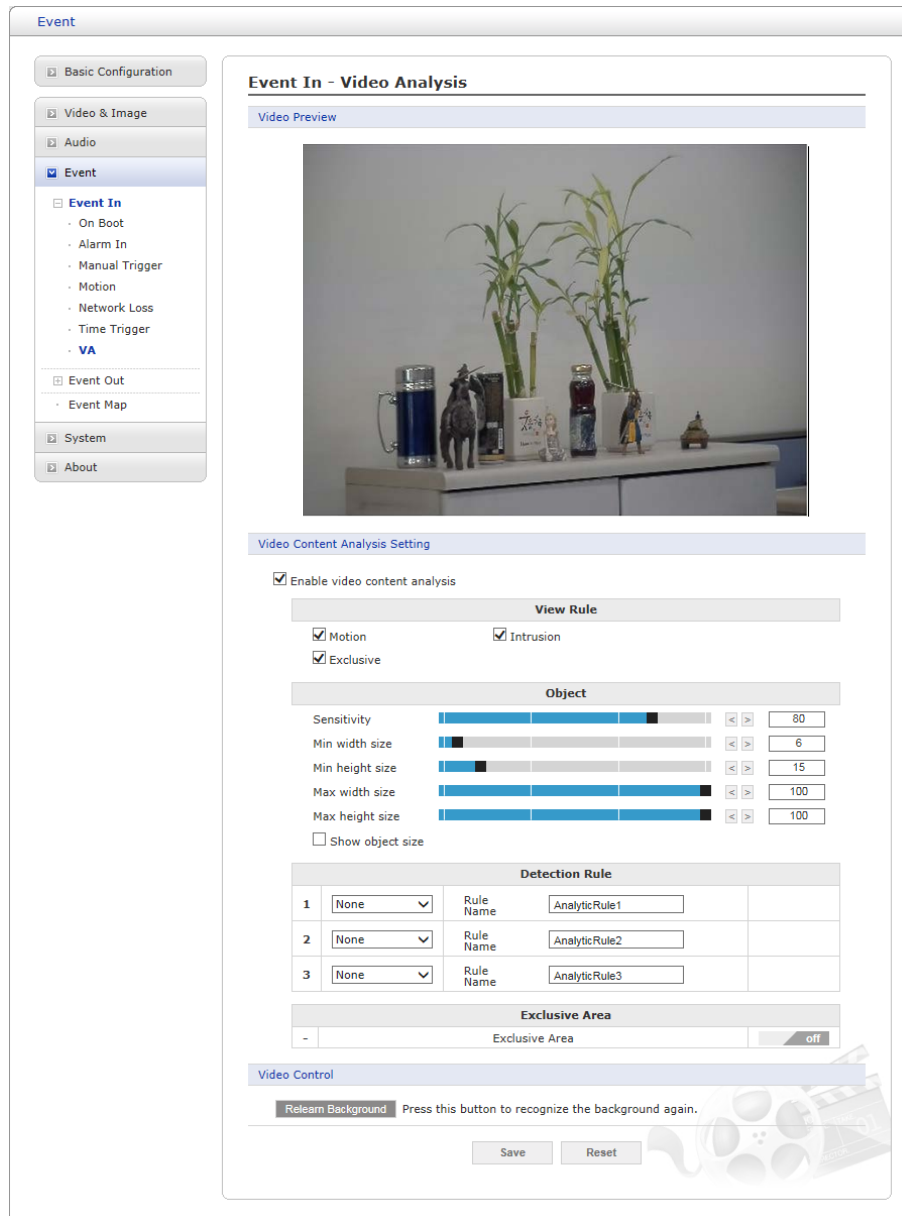
▽ VA

The network cameras provide VA (Video Analysis) functions of "Intelligent Motion", "Intrusion" and "Tampering".

- **Video Content Analysis Setting:** Check **Enable video content analysis** box to use a VA function. In order to setup VA function.

  – **View Rule:** User can see the each configured VA rules on the Video Preview.

  – **Object:** In order to avoid merging of several objects into one or splitting of a single object into multiple, please appropriately set sizes of minimal and maximal object that can enter the scene.

    * **Sensitivity:** As the value becomes bigger, the detection sensitivity increases.

    * **Min width size:** Minimum horizontal pixel size for detections in a 320x240 format.

    * **Min height size:** Minimum vertical pixel size for detections in a 320x240 format.

    * **Max width size:** Maximum horizontal pixel size for detections in a 320x240 format.

    * **Max height size:** Maximum vertical pixel size for detections in a 320x240 format.

NOTE: Format size depend on the performance.

  – **Detection Rule:**

37

* **Intelligent Motion:** Once selected, **blue** cells appear on the video preview window. Select cells at the desired position. The following is a description of 'Setting items' for 'Intelligent Motion'.

    . **Rule Name:** User can type in the rule name.

    . **Sensitivity:** As the value becomes bigger, the detection sensitivity increase.

* **Intrusion:** Once selected, **orange** cells appear on the video preview window. Select cells at the desired position. The following is a description of 'Setting items' for 'Intrusion'.

    . **Rule Name:** User can type in the rule name.

* **Tampering:** Once selected, the entire area is detecting for camera being tampered, obstructed, turned aside or lens defocused. The following is a description of 'Setting items' for 'Tampering'.

    . **Rule Name:** User can type in the rule name.

    . **Sensitivity:** As the value becomes bigger, the detection sensitivity increase.

    . **Light Change:** Whether Light on / off is detected as an event.

    . **Light Sensitivity:** As the value becomes bigger, the detection sensitivity increase.

– **Exclusive Area:** The area where the rules are not applied. Once selected, a **red** cell appears on the video preview window. Select cells at the desired position.

NOTE: Intelligent Motion of the Video Analysis function cannot be used in conjunction with Motion Detection function. If you choose **Enable Intelligent Motion**, motion detection function is automatically turned off.

• **Video Control:** User can the settings which affect the object detection can be adjusted.

– **Relearn Background:** By the 'Relearn Background' button click, you may learn the current image as background.

– **Scene type:** Through drop-down list of Scene type you may assign different scene type in engine. Select the scene type to set the VA Engine.

– **View mode:** Through drop-down list of View mode you may assign different view mode in engine. Select the view mode to set the VA Engine.

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 network camera 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 network camera.

    - **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 in- terval.

    - **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.

39

- **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 network camera 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 camera 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 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 con- nection, 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 fire- wall between the camera 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.

▽ XML Notification

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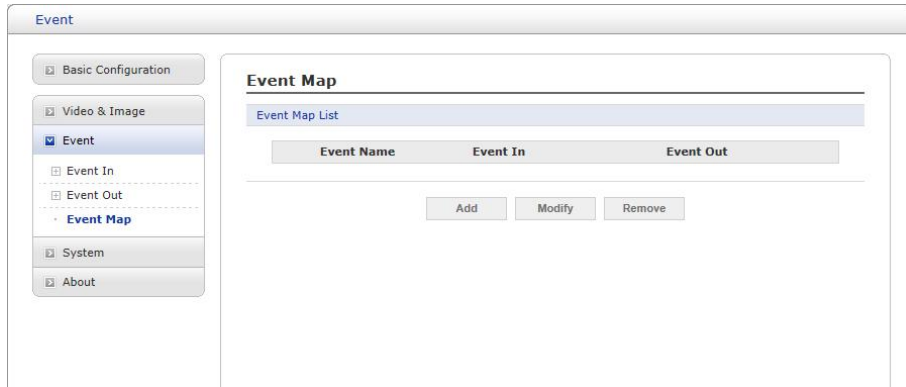
The event map allows you to change the settings and establish a schedule for each event trigger from the network camera; up to a max. 15 events can be registered.

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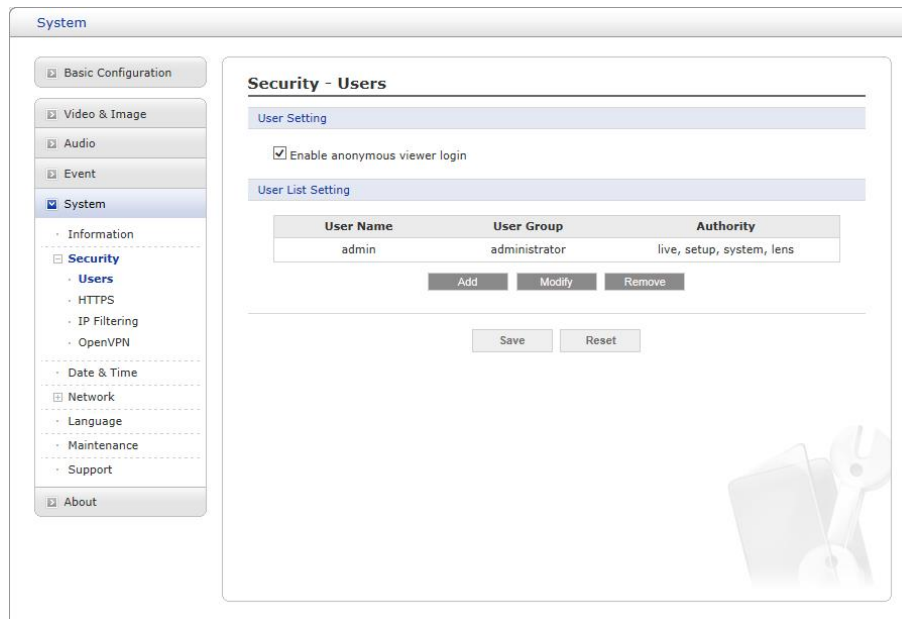
User access control is enabled by default when the administrator sets the root password on first access. New users are authorized with user names and passwords, or the administrator can choose to allow anonymous viewer login to the Live View page, as described below:

- **User Setting:** Check the box to enable anonymous viewer login to the network camera 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.
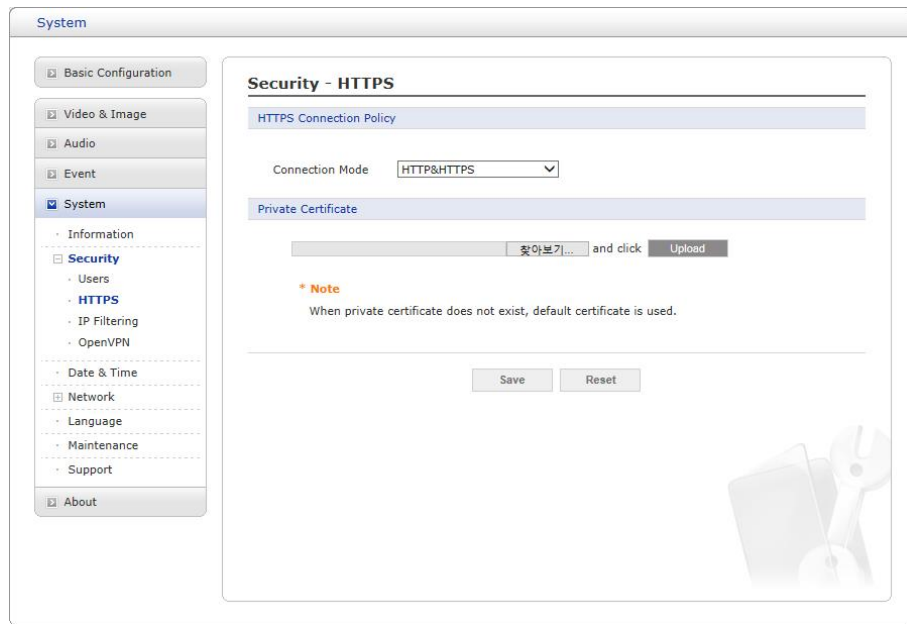
▽ HTTPS

For greater security, the network camera 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 network camera, 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**
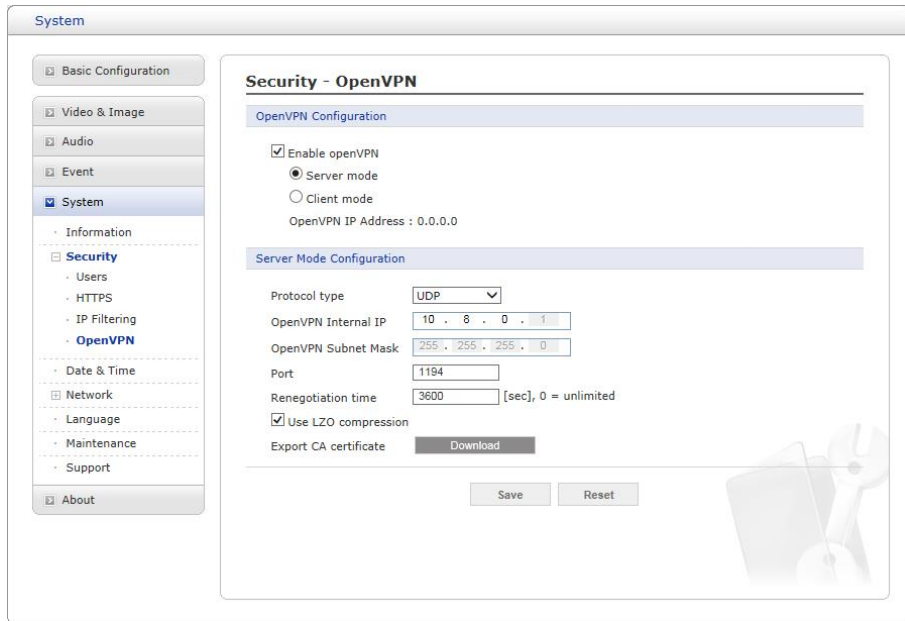
OpenVPN is a Virtual Private Network using OpenSSL authentication. User can set the camera in either Server mode or Client mode.

- **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 camera operates as an Open- VPN Server.
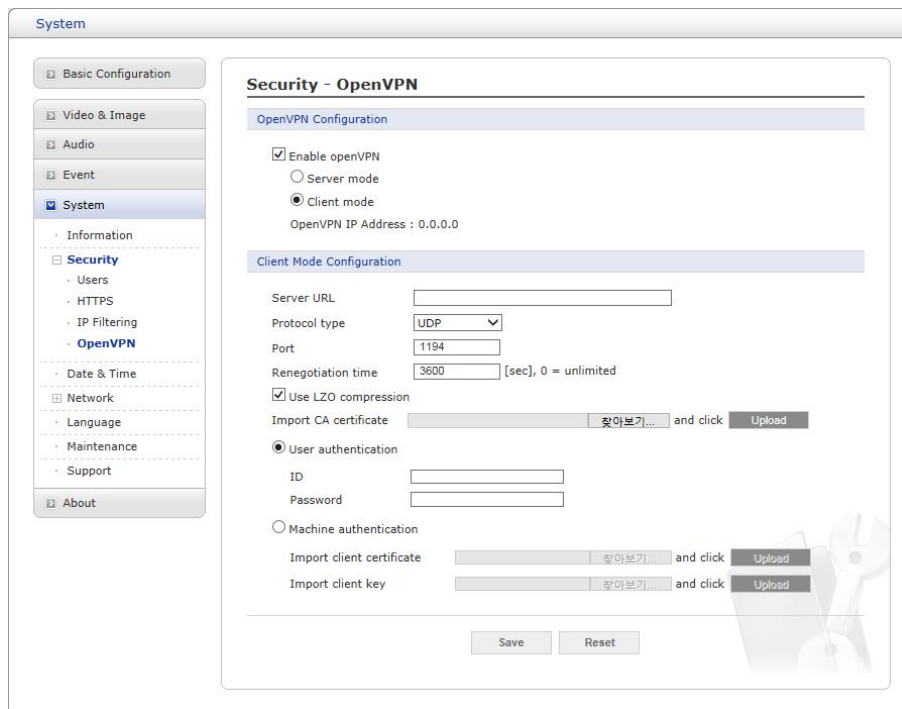
- OpenVPN Client Mode

    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 camera 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 network camera 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 network camera, check the radio button and then make the following settings:
    - **IP address:** Specify a unique IP address for your network camera.
    - **Subnet mask:** Specify the mask for the subnet the network camera 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 pro- vided by the DHCP server.

  – **Use the following DNS server address** to enter the desired DNS server by spec- ifying the following:

  · **Domain name:** Enter the domain(s) to search for the host name used by the network camera. 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 network camera 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.
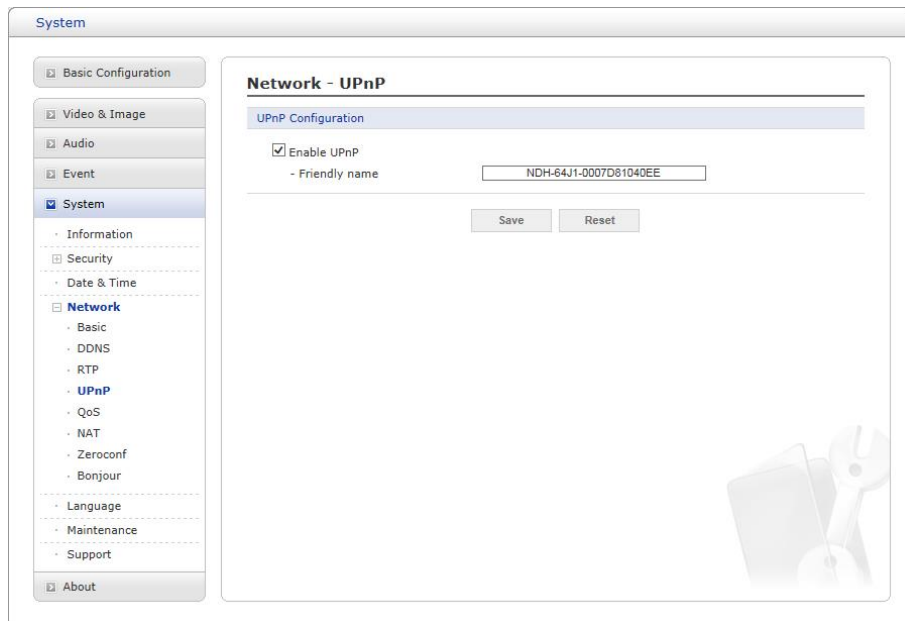
  – **Enable Multicast:** Check the box to enable multicast operation.

  – **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 network cameras 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 network camera includes support for UPnP. UPnP is enabled by default, so the network camera 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
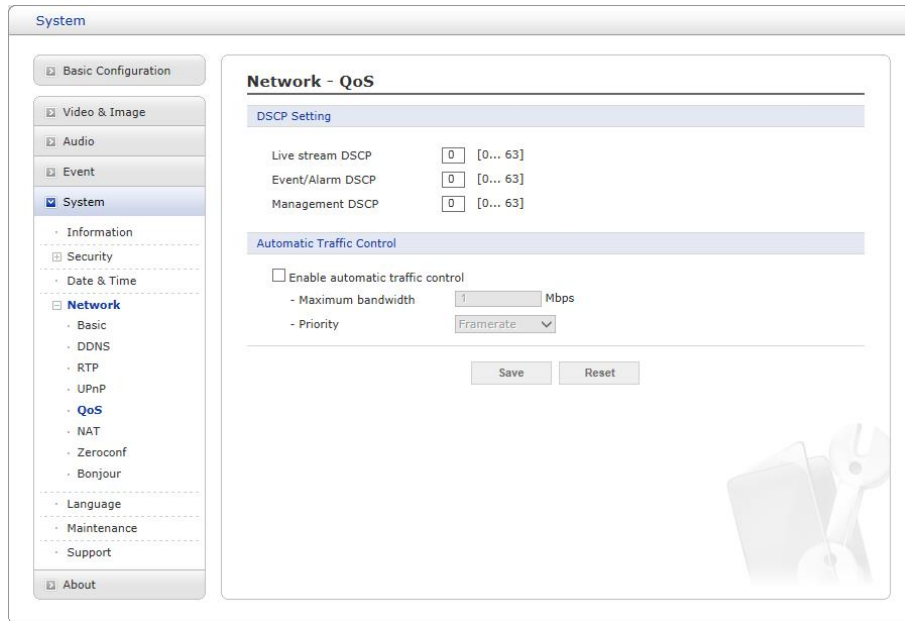
Quality of Service (QoS) provides the means to guarantee a certain level of a specified re- source to selected traffic on a network. Quality can be defined as a maintained level of bandwidth, low latency, and no packet losses.

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 band- width or Automatic framerate radio button.
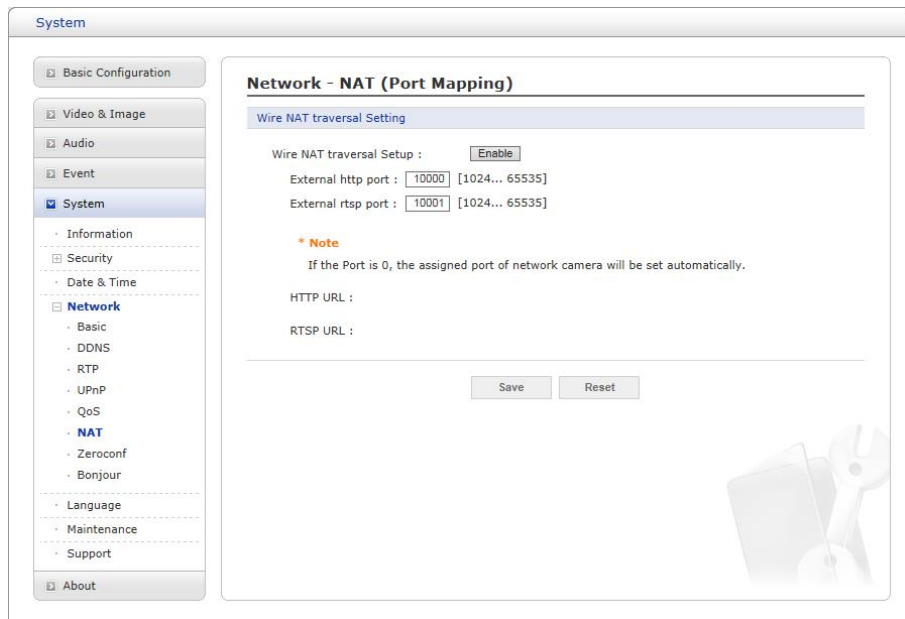
– **Maximum bandwidth:** When sharing other network programs or equipment, it is possible

60

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 network camera attempts to configure port mapping in a NAT router on your network, using UPnP. Note that UPnP must be enabled in the network camera (see System > Network > UPnP).

    ・ **Automatic setting:** When selected, the network camera 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**
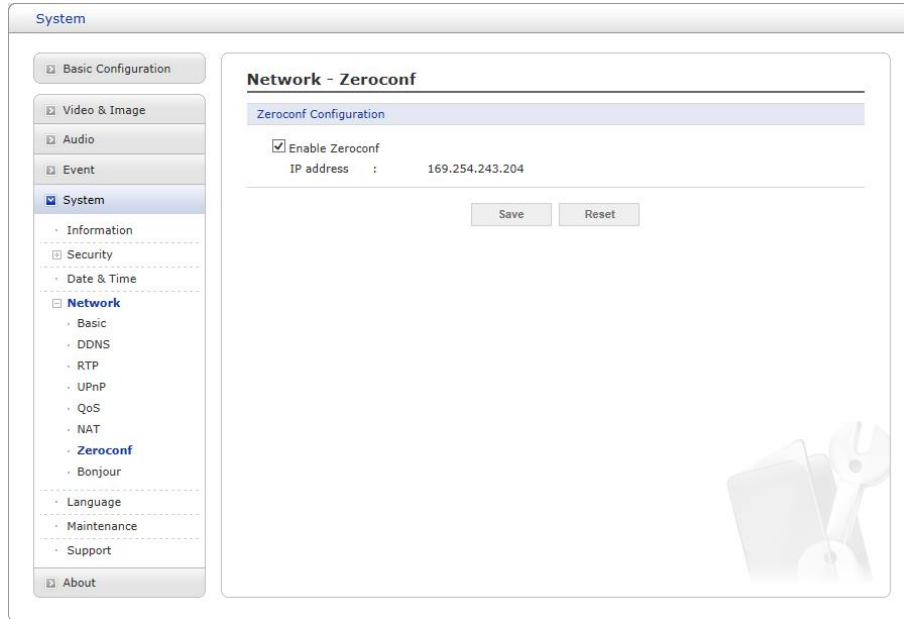
Zero configuration networking (zeroconf) is a set of techniques that automatically creates a usable Internet Protocol (IP) network without manual operator intervention or special configuration servers.

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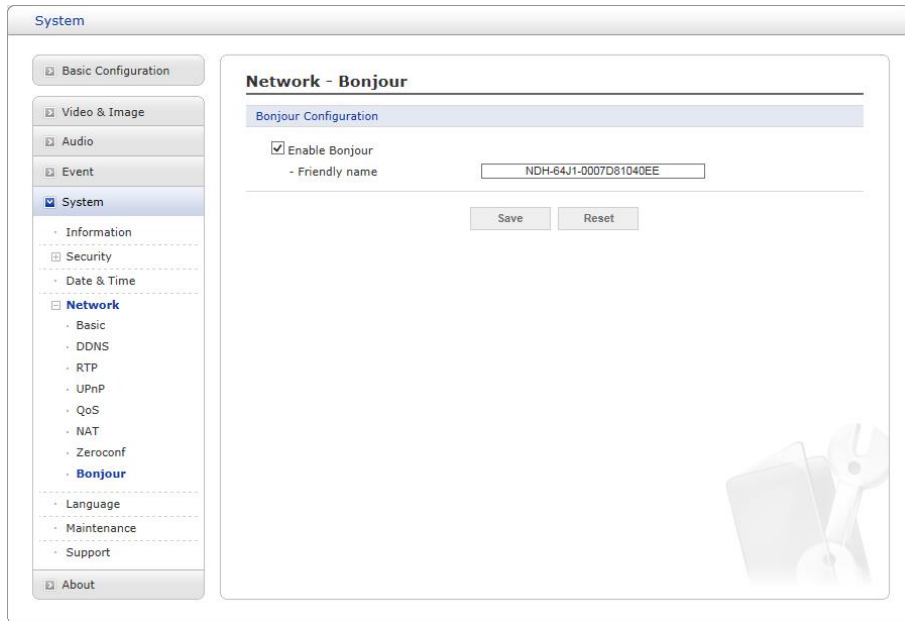
The network camera includes support for Bonjour. When enabled, the network camera is automatically detected by operating systems and clients that support this protocol.

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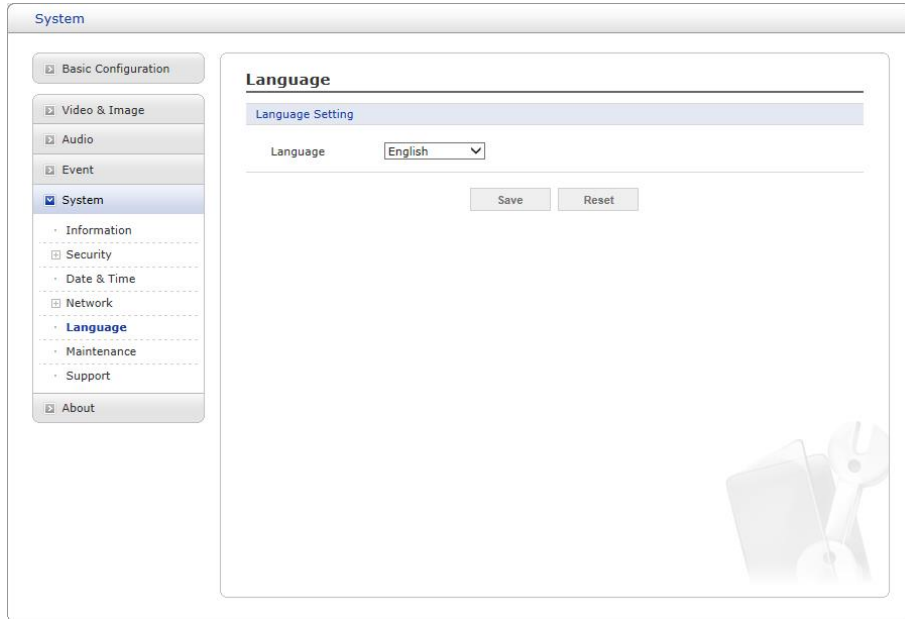
Select a user language. The language choices are English, Korean, French, German, Russian and Chinese.

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
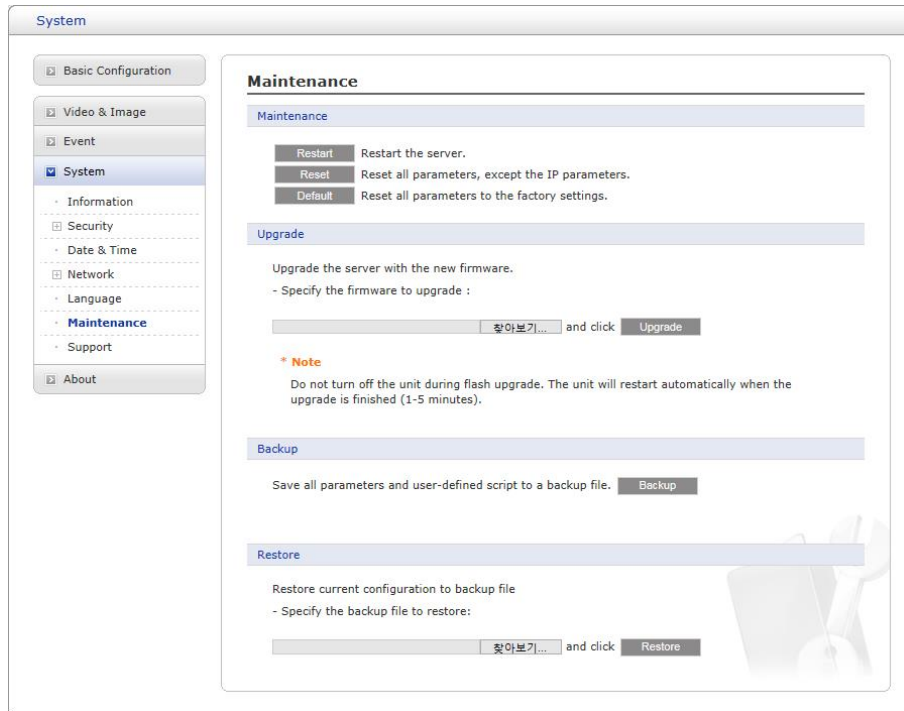
- **Maintenance:**

  - **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 network camera's settings to the factory default values (including the IP address).

- **Upgrade:** Upgrade your camera by importing an upgrade file and pressing the **Upgrade** button. During the upgrade, do not turn off the power of the network camera. Wait at least five minutes and then try to access the camera again.

- **Backup:** Save the setting values that users have entered to the network camera 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.
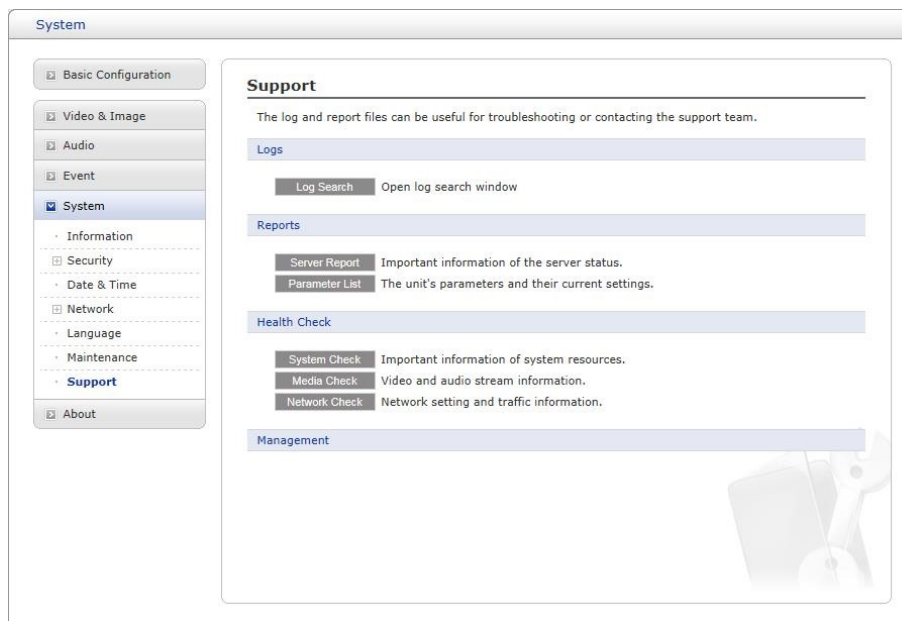
- **Log Search:** The network camera supports system and event log information. Click the **log Search** button to search the Access, Event, Setup or Control log data.
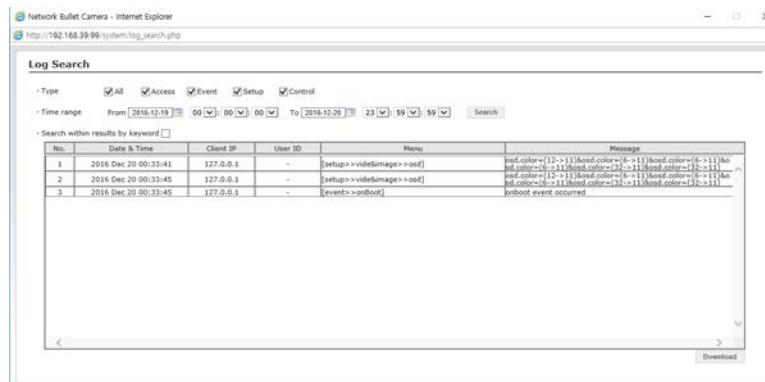
- **Reports:**

    - **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 cameras system resources. You can see the pop-up window below.
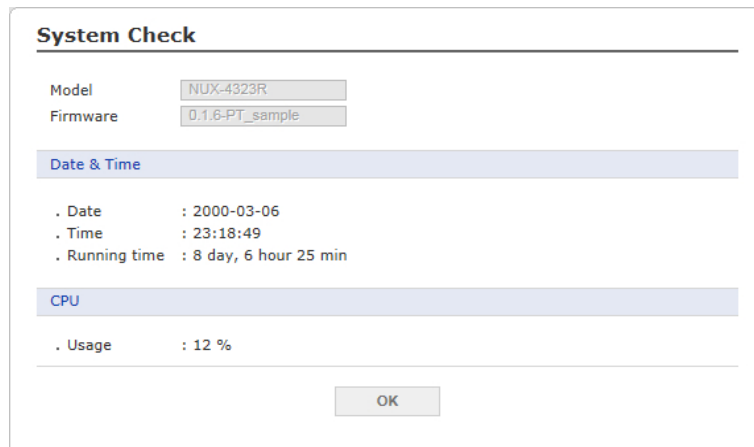
– **Media Check:** Click the **Media Check** button to get the information about the cameras video and audio stream. You can see the pop-up window below.
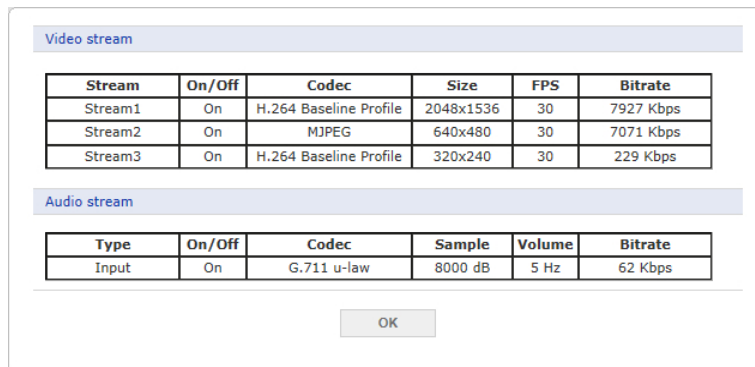
– **Networks Check:** Click the **Network Check** button to get the information about the cameras network setting and traffic. You can see the pop-up window below.

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 network camera without a reference to the manual.

A Appendix

A.1 Troubleshooting

Troubleshooting if problems occur, verify the installation of the network camera 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 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.
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.
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 camera 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 camera.
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/H.265 not displayed in the	Check that the correct network interface is selected in the Video & Image/Stream.
Multicast H.264/H.265 not displayed in the client.	Check with your network administrator that the multicast addresses used by the camera 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/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.
Color saturation is different in H.264, H.265 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 be- come 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/H.265 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

BULLET NETWORK CAMERA

Model		4MP Fixed Lens	4MP MVF Lens
IMAGE			
Lens		3.6mm, F2.1	MVF 2.8~12mm, F1.6
Angle of View		83°(H)	94°(H) ~ 34°(H)
Image Sensor		1/3" CMOS Sensor	
Min. Illumination		Color: 0.1Lux@F1.6, BW: 0Lux@F1.6(IR LED On)	
Scanning Mode		Progressive Scan	
Wide Dynamic Range		Yes	
Day and Night Mode		True D/N (Auto, Day, Night)	
Noise Reduction		2DNR, 3DNR	
Digital Zoom		Yes(ROI)	
Exposure Control		Auto	
White Balance Control		Auto, Manual	
Metering Mode		Spot(BLC), Center, Average, Left, Right, Bottom	
Image effect		Flip, Mirror, Defog	
Flicker Free Mode		50Hz, 60Hz	
Shutter Speed		Auto (1/10,000 ~ 1sec)	
IR Illuminator	Quantity	1 Array LEDs	24 SMD LEDs
	Distance	Up to 30m	Up to 30m
Motorized Lens Control		-	Smart Focus, Manual
VIDEO/AUDIO			
Compression		H.264 (Baseline, Main, High Profile), H.265(Main Profile), MJPEG	
Bitrate Control		CBR, CVBR	
Resolution		2592x1520, 2304x1296, 1920x1080, 1440x1080, 1280x1024/720, 1024x768, 800x600/480, D1, 640x480, 400x240, CIF	
Frame Rate		4M capture mode : Max. 20/20fps (PAL/NTSC) 2M capture mode : Max. 25/30fps (PAL/NTSC)	
Streaming		Quad Stream(H.264/H.265 x 3, MJPEG x 1)	
SYSTEM			
Video Contents Analysis		Tampering, iVMD, Intrusion Detector	
Motion Detection Area		16 Programmable Area (Include Area 8, Exclude Area 8)	
Privacy Mask Zone		4 Programmable Zone	
Hi-Stream(Smart Codec)		8 Regions, quality setup, non-ROI fps setup	
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, OpenVPN	
Network Time Sync		NTP Server, Synchronized Computer, Manual	
Software Reset		Restart, Reset, Factory Default	
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		
Ethernet	RJ-45 (10/100Base-T)	
ETC		
Operating Humidity	0 ~ 90% RH (Non-condensing)	
Operating Temperature	-20℃ ~ +50℃	
Power Supply	PoE(IEEE802.3af compliance, Class0), DC12V	
Power Consumption	106mA(5.1W)@ PoE 320mA(3.8W)@ DC12V	145mA(7.0W)@ PoE 480mA(5.8W)@ DC12V
Dimensions	75.8(W) x 76.6(H) x 150.4(D)mm	81(W) x 82(H) x 239(D)mm
Net Weight	Approx. 465g	Approx. 600g
Ingress Protection	IP66	

* Specifications are subject to change without notice.

TURRET NETWORK CAMERA

Model		4MP Fixed Lens	4MP MVF Lens
IMAGE			
Lens		3.6mm, F2.1	MVF 2.8~12mm, F1.6
Angle of View		83°(H)	94°(H) ~ 34°(H)
Image Sensor		1/3" CMOS Sensor	
Min. Illumination		Color : 0.1Lux@F1.6, BW: 0Lux@F1.6(IR LED On)	
Scanning Mode		Progressive Scan	
Wide Dynamic Range		Yes	
Day and Night Mode		True D/N (Auto, Day, Night)	
Noise Reduction		2DNR, 3DNR	
Digital Zoom		Yes(ROI)	
Exposure Control		Auto	
White Balance Control		Auto, Manual	
Metering Mode		Spot(BLC), Center, Average, Left, Right, Bottom	
Image effect		Flip, Mirror, Defog	
Flicker Free Mode		50Hz, 60Hz	
Shutter Speed		Auto (1/10,000 ~ 1sec)	
IR Illuminator	Quantity	18 SMD LEDs	40 SMD LEDs
	Distance	Up to 30m	Up to 30m
Motorized Lens Control		-	Smart Focus, Manual
VIDEO/AUDIO			
Compression		H.264 (Baseline, Main, High Profile), H.265(Main Profile), MJPEG	
Bitrate Control		CBR, CVBR	
Resolution		2592x1520, 2304x1296, 1920x1080, 1440x1080, 1280x1024/720, 1024x768, 800x600/480, D1, 640x480, 400x240, CIF	
Frame Rate		4M capture mode : Max. 20/20fps (PAL/NTSC) 2M capture mode : Max. 25/30fps (PAL/NTSC)	
Streaming		Quad Stream(H.264/H.265 x 3, MJPEG x 1)	
SYSTEM			
Video Contents Analysis		Tampering, iVMD, Intrusion Detector	
Motion Detection Area		16 Programmable Area (Include Area 8, Exclude Area 8)	
Privacy Mask Zone		4 Programmable Zone	
Hi-Stream(Smart Codec)		8 Regions, quality setup, non-ROI fps setup	
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, OpenVPN
Network Time Sync		NTP Server, Synchronized Computer, Manual
Software Reset		Restart, Reset, Factory Default
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		
Ethernet		RJ-45 (10/100Base-T)
ETC		
Operating Humidity		0 ~ 90% RH (Non-condensing)
Operating Temperature		-20℃ ~ +50℃
Power Supply		PoE(IEEE802.3af compliance, Class0), DC12V
Power Consumption		124mA(6.0W)@ PoE 380mA(4.6W)@ DC12V / 175mA(8.4W)@ PoE 550mA(6.6W)@ DC12V
Dimensions		90mm(Φ) x 85mm(H) / 135.4mm(Φ) x 127.7mm(H)
Net Weight		Approx. 385g / Approx. 770g
Ingress Protection		IP66

* Specifications are subject to change without notice.

A.6   System Requirement for Web Browser

Operating System: Microsoft® Windows® 98, Microsoft Windows ME, Microsoft Windows 2000, Microsoft Windows XP, or Microsoft Windows Vista®, Windows 7, Windows 8.1 and Windows 10.
CPU: Intel® Core™ 2 Duo 2GHz or higher, 1 GB RAM or more, 10 GB free disk or higher
VGA: AGP, Video RAM 32 MB or higher (1024x768, 24 bpp or higher)

eneo