User Manual

V988D
Network 4K Dome Camera

XX305-00-00

Vicon Industries Inc. does not warrant that the functions contained in this equipment will meet your requirements or that the operation will be entirely error free or perform precisely as described in the documentation. This system has not been designed to be used in life-critical situations and must not be used for this purpose.

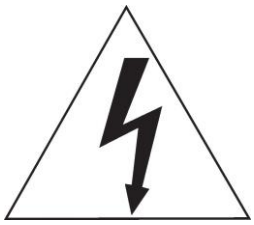
Document Number: 8009-8305-00-00 Product specifications subject to change without notice. Issued: 12/18 Copyright © 2018 Vicon Industries Inc. All rights reserved.

Vicon Industries Inc.
Tel: 631-952-2288
Fax: 631-951-2288
Toll Free: 800-645-9116
24-Hour Technical Support:
800-34-VICON

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

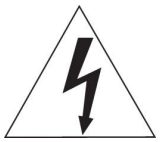


CAUTION

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 radiofrequency 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, 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 INSTRUCTIONS 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 **6**
1.1 Components 6
1.2 Key Features 7

2 Installation **8**
2.1 Overview 8
2.2 Connection 10
2.3 Resetting to the factory default settings 11
2.4 Network Connection & IP assignment 12

3 Operation **13**
3.1 Access from a browser 13
3.2 Access from the internet 14
3.3 Setting the admin password over a secure connection 14
3.4 Live View Page 15
3.5 Playback 18
3.6 Network Camera Setup 20
3.6.1 Basic Configuration 20
3.6.2 Video & Image 26
3.6.3 Audio 35
3.6.4 Event 36
3.6.5 System 62
3.7 Help 82

A Appendix **83**
A.1 Troubleshooting 83
A.2 Alarm Connection 84
A.3 Preventive Maintenance 84
A.4 System Requirement for Web Browser 85
A.5 General Performance Considerations 85
A.6 Product Specification 86

Shipping Instructions **88**

Vicon Standard Equipment Warranty **89**

1 Introduction

Vicon's V988D-W311MIR HD IP Dome Camera is designed for performance in demanding security installations. The camera provides 4K (8 MP) resolution with a 3.6-11 mm motorized varifocal lens. The camera offers IR illuminators that provide superior images in low-light environments.

The V988D-W311MIR supports H.264/H.265 compression technology, drastically reducing file sizes and conserving valuable network bandwidth. M-JPEG compression is also provided. The camera can provides quad streaming for multi-camera displays.

1.1 Components

This system comes with the following components;

Network Camera	1
Quick Installation Guide	1
Template Sheet	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 12 VDC 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 four 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. The network cameras external inputs and outputs can be connected to devices such as sensors and relays, enabling the system to react to alarms and activate lights or open/close doors.

- **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.

- **Micro-SD recording support**
  The network camera also supports a micro-SD memory slot for local recording with removable storage of type SDHC and SDXC.

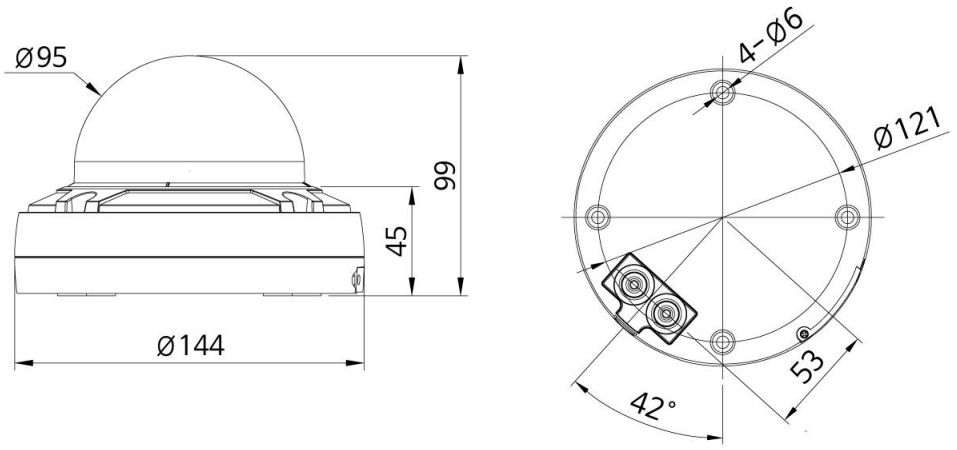
- **Audio support**
  The Network Camera also supports two-way audio.

2 Installation

For the operation of the network camera, it is necessary to connect a network cable for data transmission and power connection from customer-supplied power adapter. Depending on operation methods, it is also possible to connect an alarm cable.

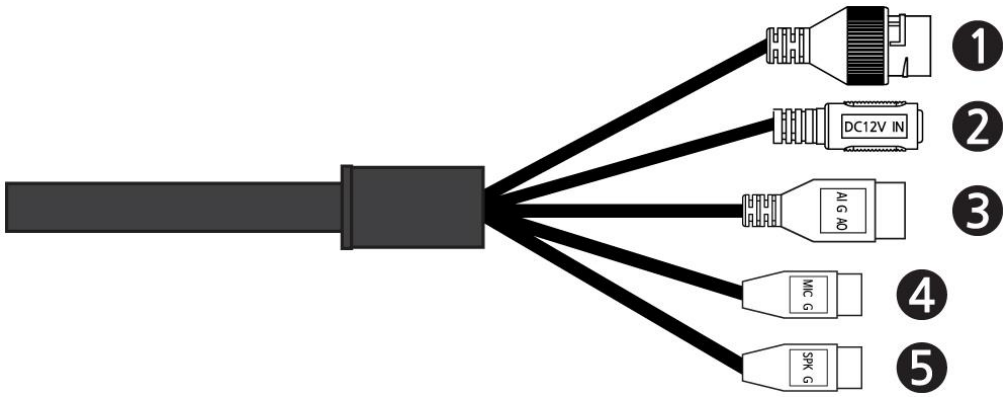
2.1 Overview

- **Dimension**



Dimensions Unit: mm

- **Extension Cable**

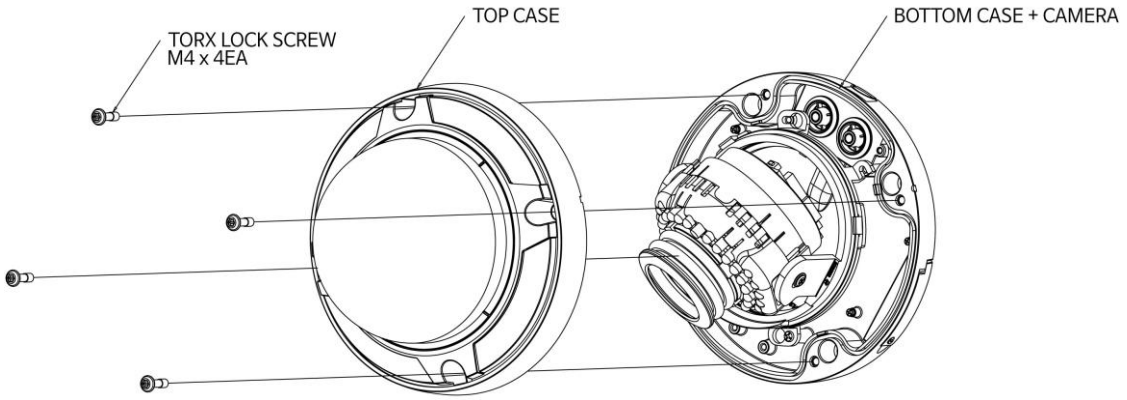


NO	Item	Description
1	RJ-45	Ethernet, RJ-45 port compatible with 10/100Mbps PoE Modular Jack
2	DC Jack	Main Power, DC Jack, 12 VDC
3	AI: Alarm In	Alarm input and output, 3-pin terminal
	G: GND	
	AO: Alarm Out	
4	MIC: Audio In	Audio line input, 2-pin terminal
	G: GND	
5	SPK: Audio Out	Audio line output, 2-pin terminal
	G: GND	

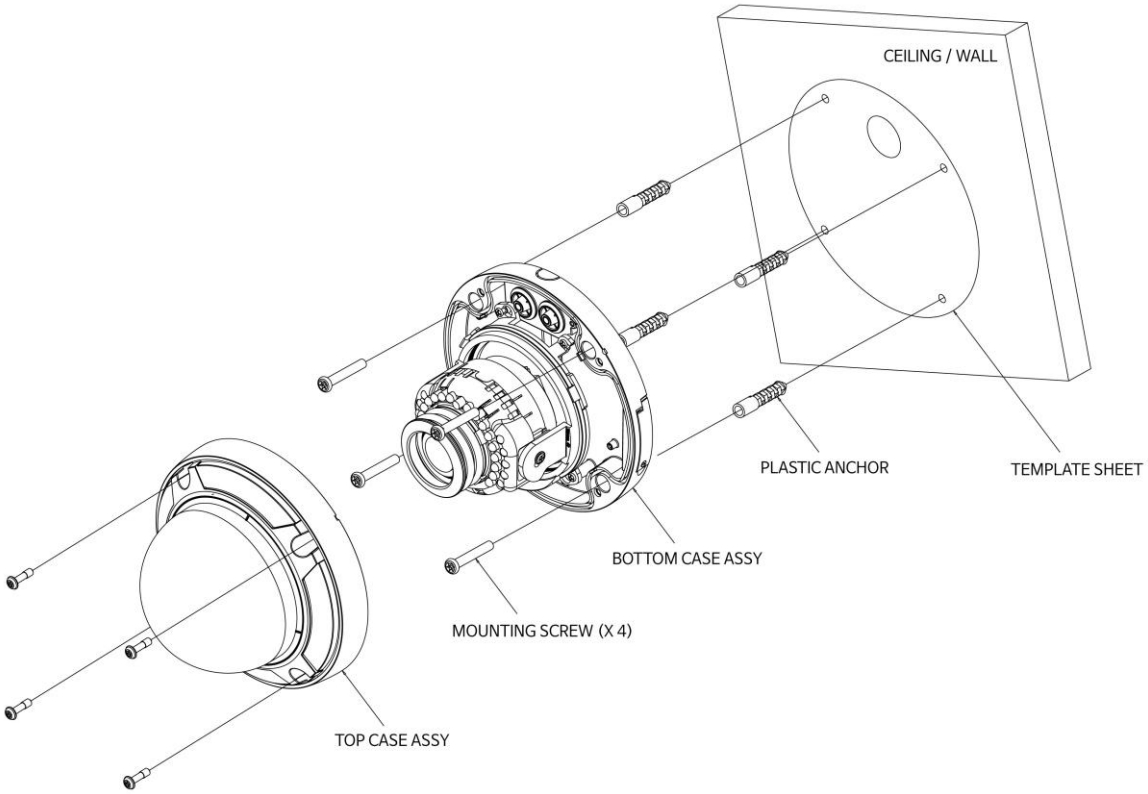
- **Installing & Adjusting Camera**

Carefully remove the contents from the box.

1) Loosen the four torx screws located on the front of the housing, leaving the screws intact in the front portion.



2) Using the template sheet, make mounting holes and cable hole in the location (ceiling or wall) where this dome is being installed.

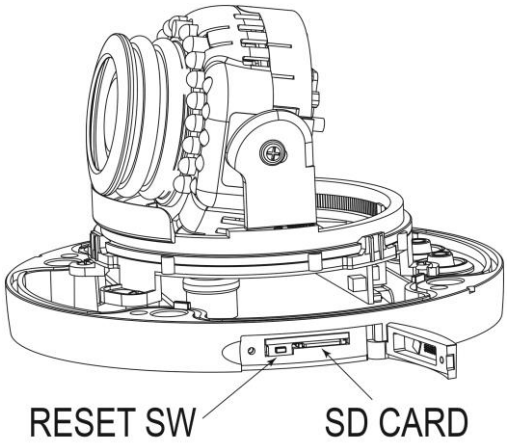


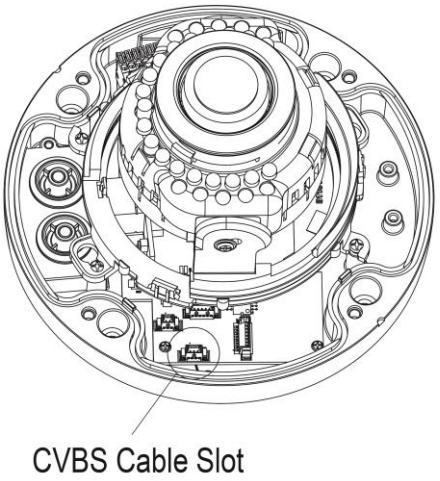
Do not continue to turn the camera in same direction.
The cable connector can be detached.

2.2 Connection

- **Micro SD memory slot on the bottom board**

Remove the cap at bottom of the camera to insert the SD memory card.





- **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 Alarms**

AI (Alarm In): You can use external devices to signal the network camera to react on events. Mechanical or electrical switches can be wired to the AI (Alarm In) and G (Ground) connectors.
G (Ground): Connect the ground side of the alarm input and/or alarm output to the G (Ground) connector.
AO (Alarm Out): The network camera can activate external devices such as buzzers or lights. Connect the device to the AO (Alarm Out) and G (Ground) connectors.

- **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.

- **Connecting Audio**

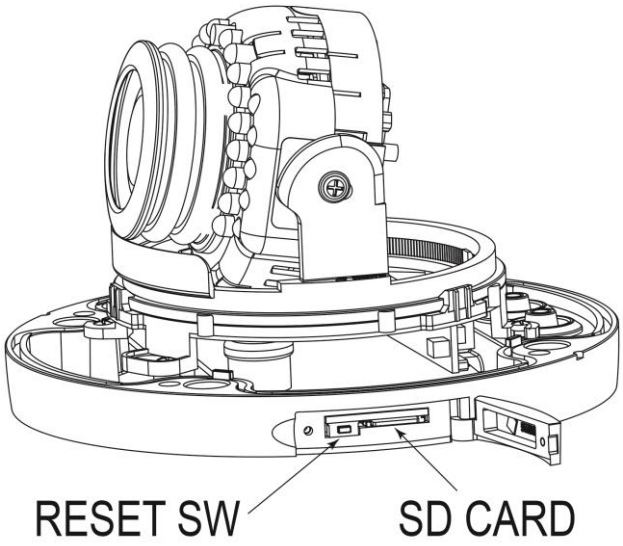
Connect speaker to audio line output and external Mic to audio input line.

- **Connecting Test Monitor Out (CVBS)**

Connect 3-pin test video cable (optional) to check test video. Use the optional cable assembly V800-USB-BNC.

2.3 Resetting to the factory default settings

To reset the network camera 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 network camera inside the bottom cap.



- **Using the Reset button:**

Follow the instructions below to reset the network camera to the factory default settings using the Reset button.

1) Switch off the network camera by disconnecting the power adapter.
2) Open the top cap.
3) Press and hold the Reset button with a straightened paperclip while reconnecting the power.
4) Keep the Reset button pressed for at least 5 (or more) seconds.
5) Release the Reset button.
6) The network camera resets to factory defaults and restarts after completing the factory reset.
7) Close the bottom cap tightly to ensure waterproof.

CAUTION: When performing a Factory Reset, you will lose any settings that have been saved.

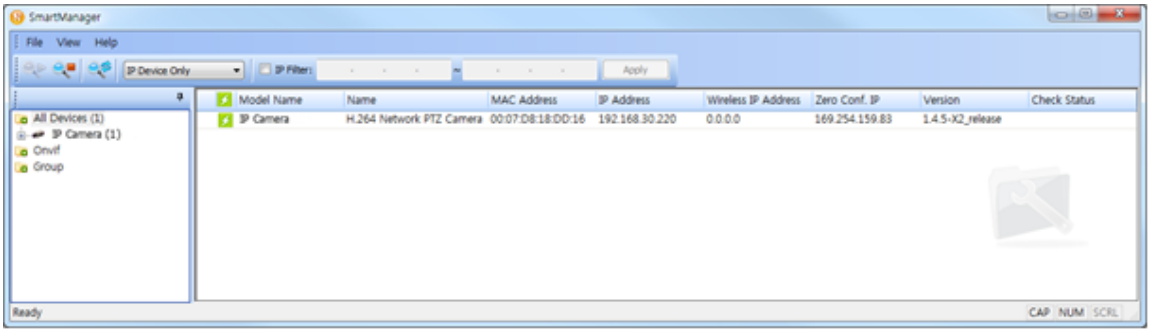
2.4 Network Connection & IP assignment

The network camera is designed for use on an Ethernet network and requires an IP address for access. Most networks today have a DHCP server that automatically assigns IP addresses to connected devices. By the factory default, your camera is set to obtain the IP address automatically via DHCP server. If your network does not have a DHCP server the network camera will use 192.168.1.100 as the default IP address.

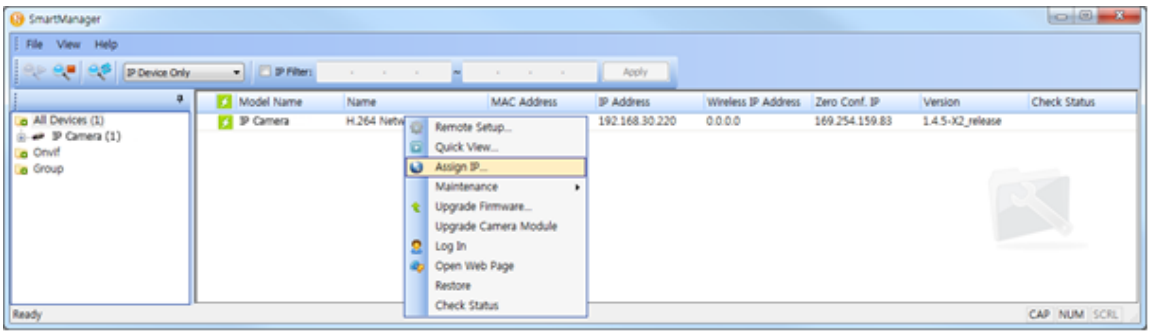
If DHCP is enabled and the product cannot be accessed, run the “Smart Manager” utility to search and allocate an IP address to your products, or reset the product to the factory default settings and then perform the installation again. The utility can be found on the Vicon website www.vicon-security.com, on the Software Downloads page for Vicon cameras.

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

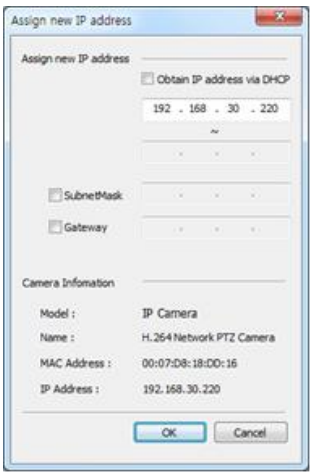
2) Start SmartManager utility (Start > All programs > SmartManager > SmartManager). The main window will display, and after a short while any network devices connected to the network will be displayed in the list.



3) Select the camera on the list and click right button of the mouse. The pop-up menu displays 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

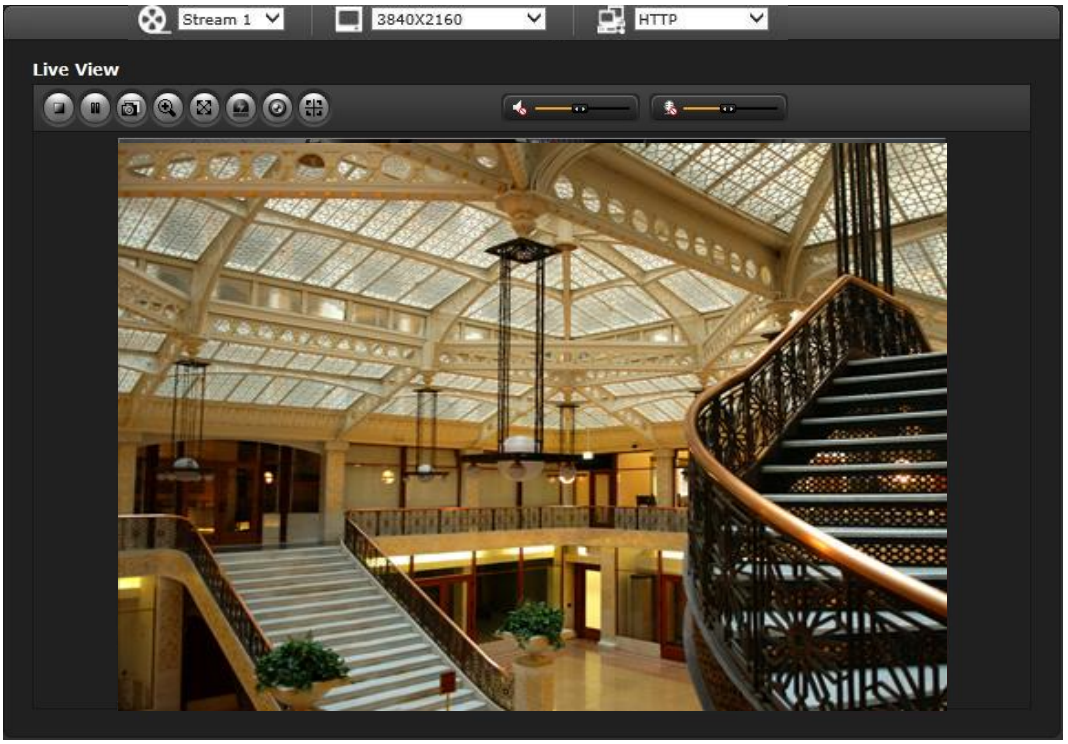
The network camera can be used with Windows® operating system and browsers. The recommended browsers are Internet Explorer®, Safari®, Firefox®, Opera® and Google® Chrome® with Windows.

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 (ex., Internet Explorer).
- Enter the IP address or host name of the network camera in the Location/Address field of your browser.
- A starting page displays. Click **Live View, Playback,** 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, refer to “System > Network > NAT”.

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.

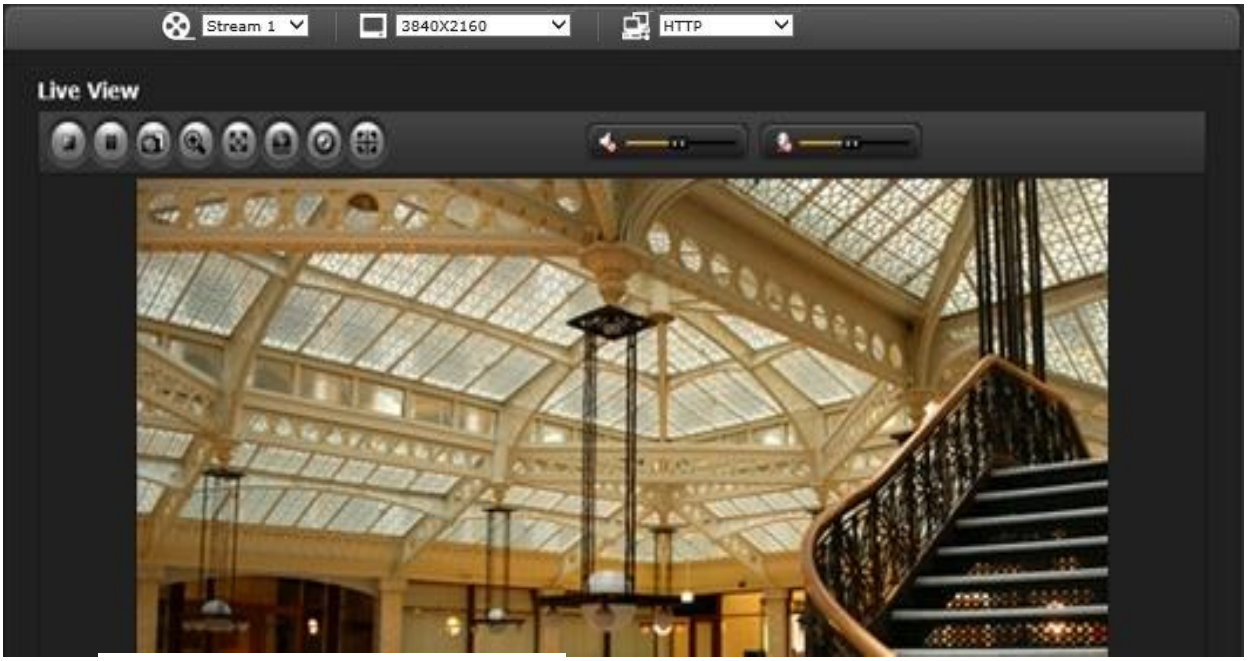
NOTE: The default administrator user name is “ADMIN” and password “1234”. If the password is lost, the network camera must be reset to the factory default settings. See “Resetting to the factory default settings” for more details.

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, 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 provides several screen modes. Select the most suitable mode in accordance with your PC specifications and monitoring purposes.

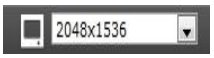


Live View showing Relay Output and VCA enabled buttons

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 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 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 **Remote Focus** button enables users to adjust focus and zoom remotely via network (motorized lens models only).

The **Fine Focus** (one push focus) button readjusts focus automatically to set the focus to the optimum position (motorized lens models only).

Use the **Speaker** icon scale to control the volume of the speakers.

Use the **Microphone** icon scale to control the volume of the microphone.

Use this button to toggle the Alarm Out port status (Normally Open/Normally Closed). This will control the status of the external device connected with the Alarm Out port.

When VCA is enabled, a VCA button displays. This will display the related lines, counters, boxes and grids, depending on the VCA.

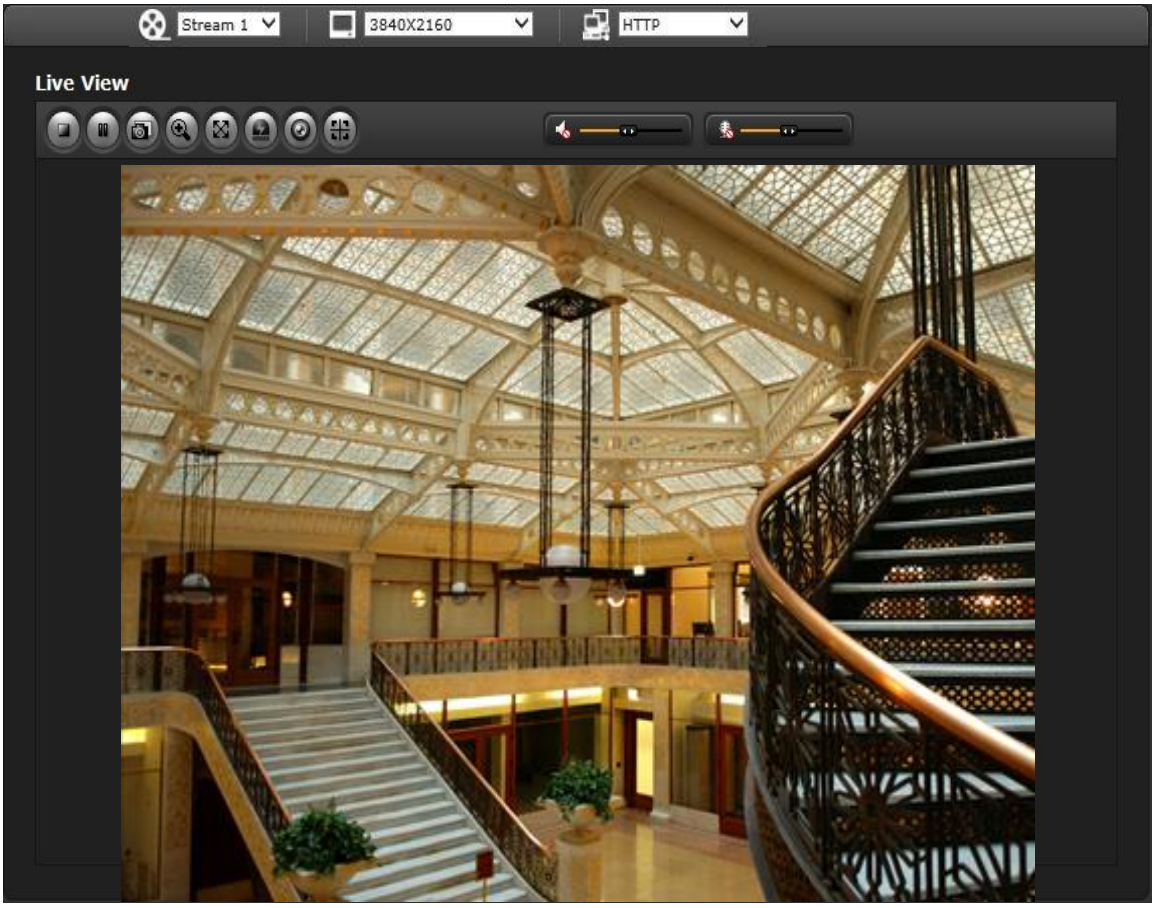
3) Video Streams

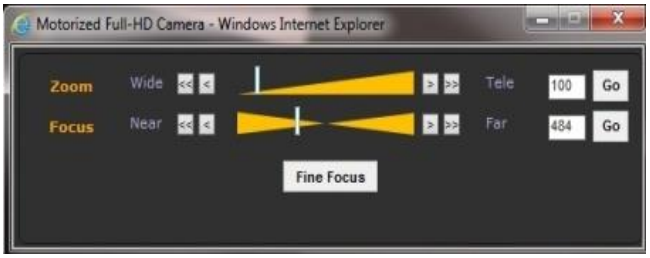
The network camera provides several images and video stream formats. Your requirements and the properties of your network will determine the type you use.

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.

4) Focus and Zoom Control (motorized lens models only).

You can control Zoom and Focus from the Live View screen. Press the button on the left top in the Live View screen to activate the Zoom and Focus control panel.





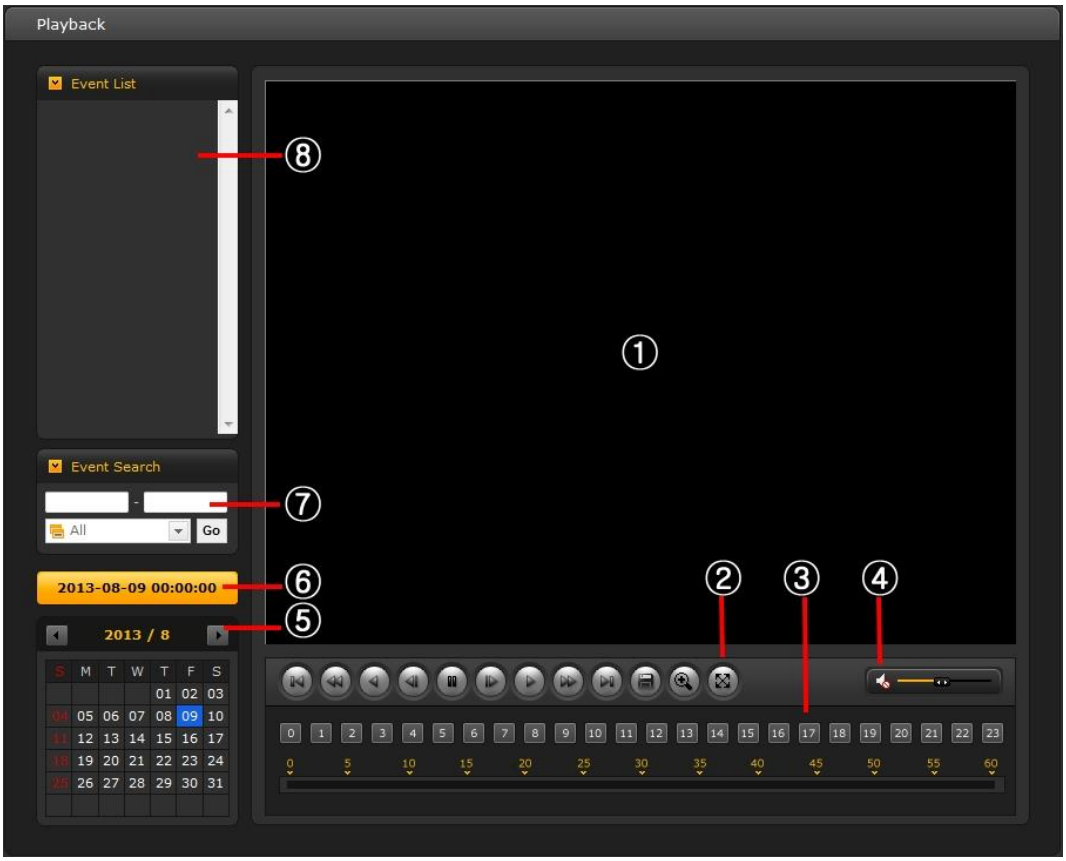
• Adjusting Zoom:
Click button to zoom out button to zoom in. The focus is moved slightly after adjusting zoom; adjust the focus again, as necessary.

• Adjusting Focus:
Click button for far focus and button to near focus.

• Fine Focus:
Click “Fine Focus” to fine tune and readjust focus automatically.

Note: Click the button in the Live View screen to set the focus to the optimum position.

3.5 Playback



The Playback window contains a list of recordings made to the memory card. It shows each recording's start time, length, the event type used to start the recording, calendar and time slice bar indicates if the recording is existed or not.

The description of playback window follows.

1) Video Screen

You can see the video screen when playing the video clip in the Micro SD memory.

2) Playback Buttons

To view a recording data in the SD local storage, select it from the list and click the Playback buttons.

- Go to First: go to the beginning of the video clip.
- Fast Backward: fast play backward (rewind) the video clip.
- Backward: play backward (rewind) the video clip.
- Backward Step: go back one frame the video clip.
- Pause: pause playback of the video clip.
- Forward Step: go forward one frame of the video clip.
- Forward: play forward the video clip.
- Fast Forward: play fast forward the video clip.

Go to Last: go to the end of the video clip.

Clip Copy: copy the video clip.

Digital Zoom: zoom in the video clip

Full Screen: display the video full screen.

3) Time Chart

Display an hour-based search screen for the chosen date. If there is recording data, a blue section will be displayed on a 24-hour basis. If you select a particular hour in the chart, a yellow square on the hour will be displayed.

4) Speaker Control Bar

Use this scale to control the volume of the speakers.

5) Search Calendar

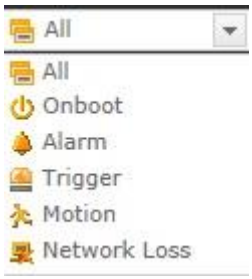
Search results from the SD local storage in the network camera connected are displayed monthly. If there is a recorded data for a particular date, a blue square on the date will be displayed. If you select a particular date in the calendar, a yellow square on the date will be displayed.

6) Play Time

Displays time of the video playing.

7) Event Search Window

Select a search option in the drop-down list and click GO button. You can also enter the time period for searching. If you click Start Date or End Date zone, Search Calendar displays.



8) Event List Window

Event List displays the event(s) that were recorded in the SD local storage. Select a list and click the play button. The video clip will be played.

3.6 Network Camera Setup

This section describes how to configure the network camera.

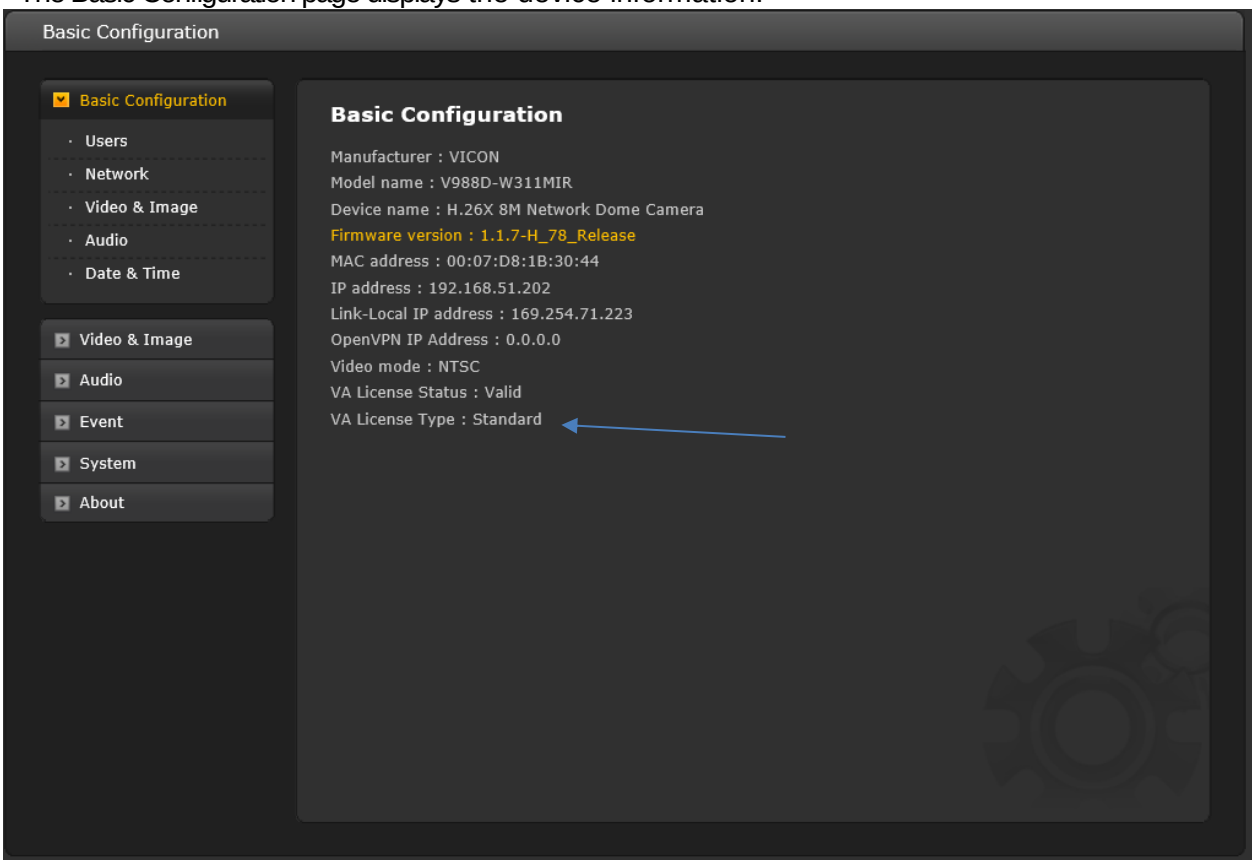
Administrator has unrestricted access to all the Setup tools, whereas Operators have access to the settings of Basic Configuration, which are Live View, Video & Image, Audio, Event and System.

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. The default administrator user name and password is “ADMIN” and the password is “1234”.

NOTE: If the password is lost, the network camera must be reset to the factory default settings. Refer to “Resetting to the Factory Default Setting.”

3.6.1 Basic Configuration

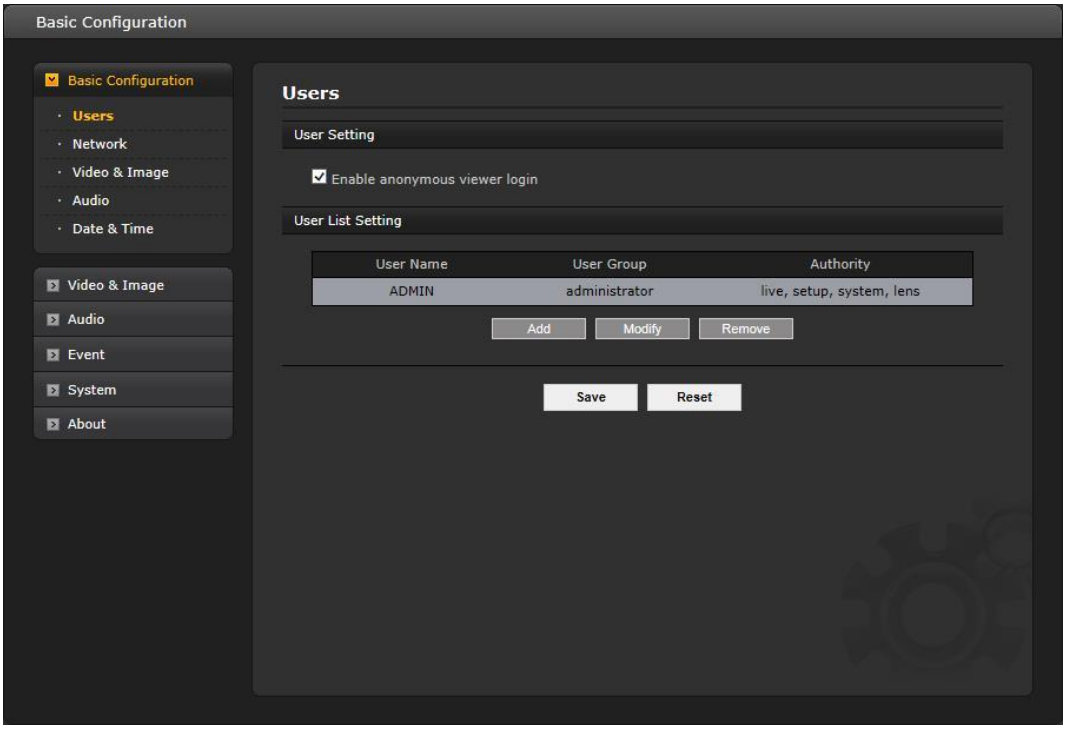
The Basic Configuration page displays the device information.



The VA License Type determines which analytics functions are available. Refer to VA (Video Analysis) section for details.

1) Users

User access control is enabled by default. The administrator can set up other users by creating 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):

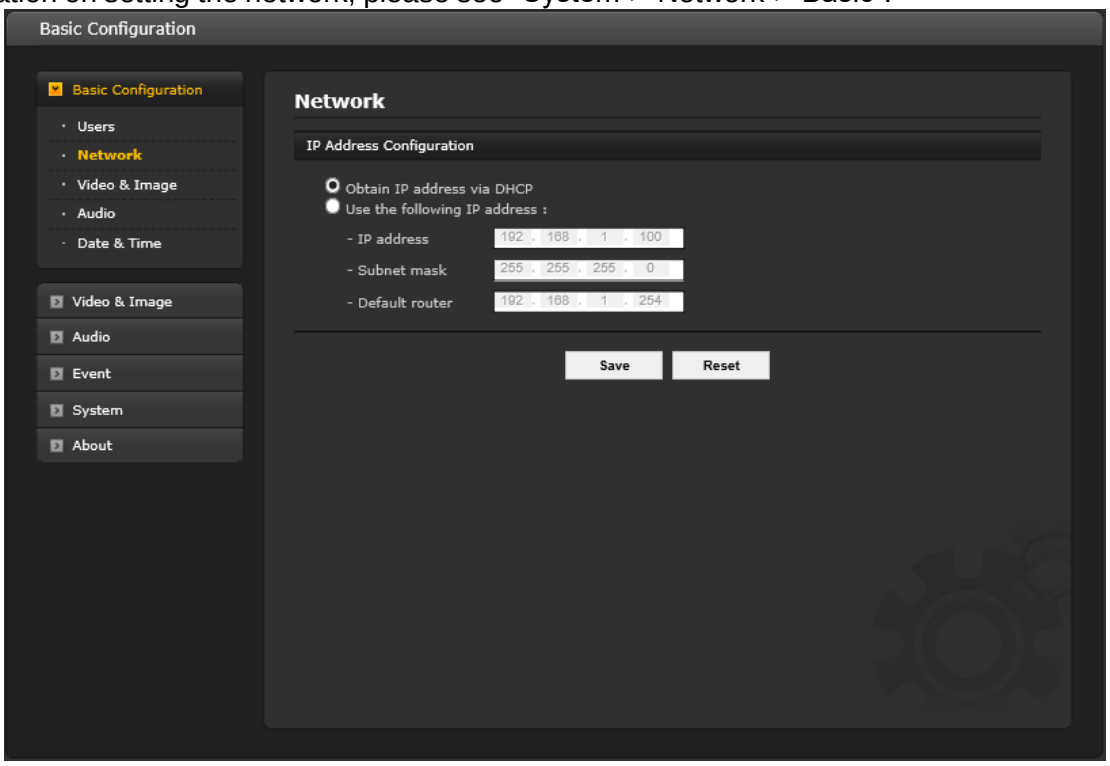
User Group	Authority
Guest	Provides the lowest level of access, which only allows access to the Live View page.
Operator	An operator can view the Live View page, create and modify events, and adjust certain other settings. Operators have no access to System Options.
Administrator	An administrator has 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 > Webcasting” for more details.

Please refer to “System > 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 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.
- **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.

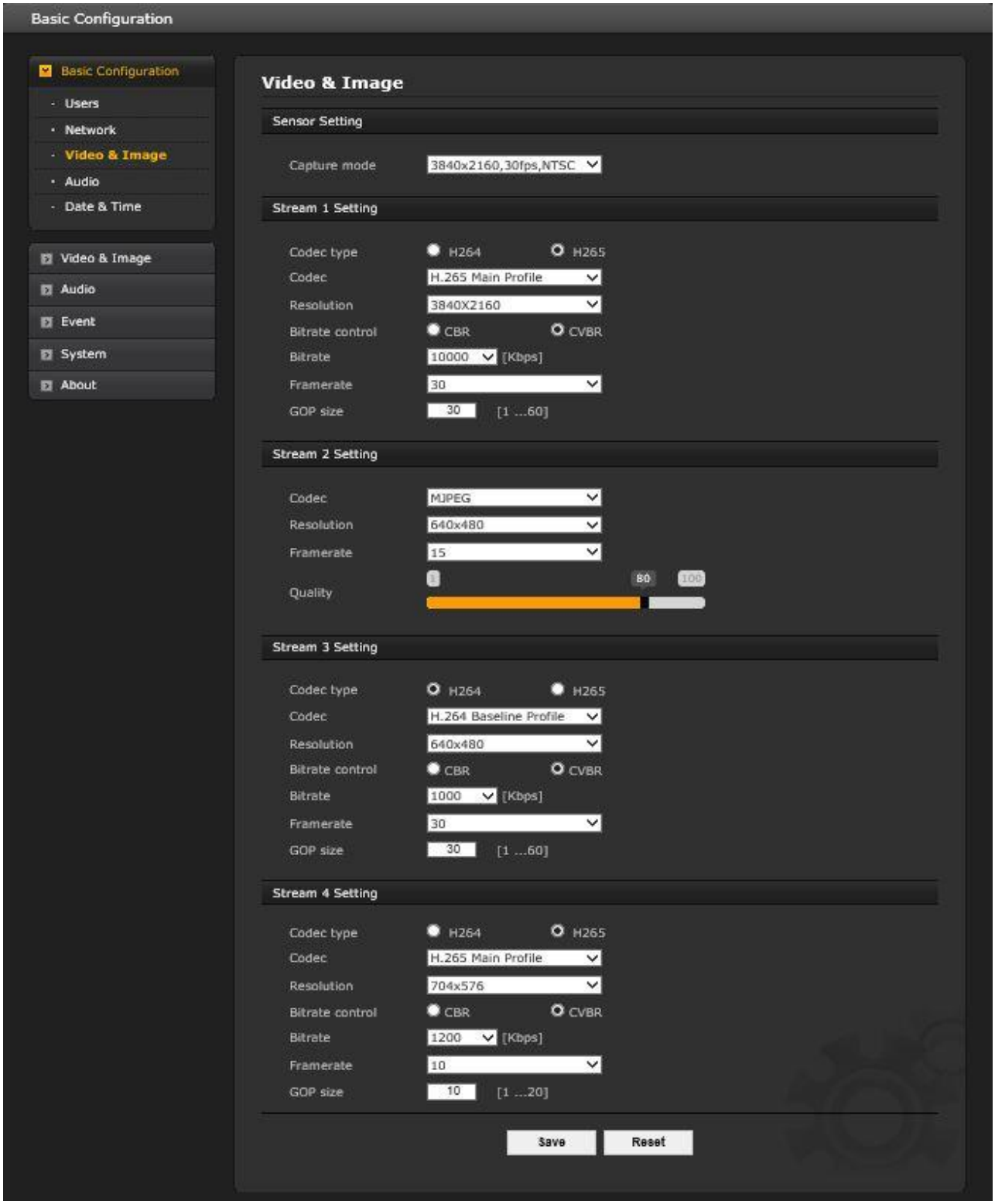
NOTES:

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.

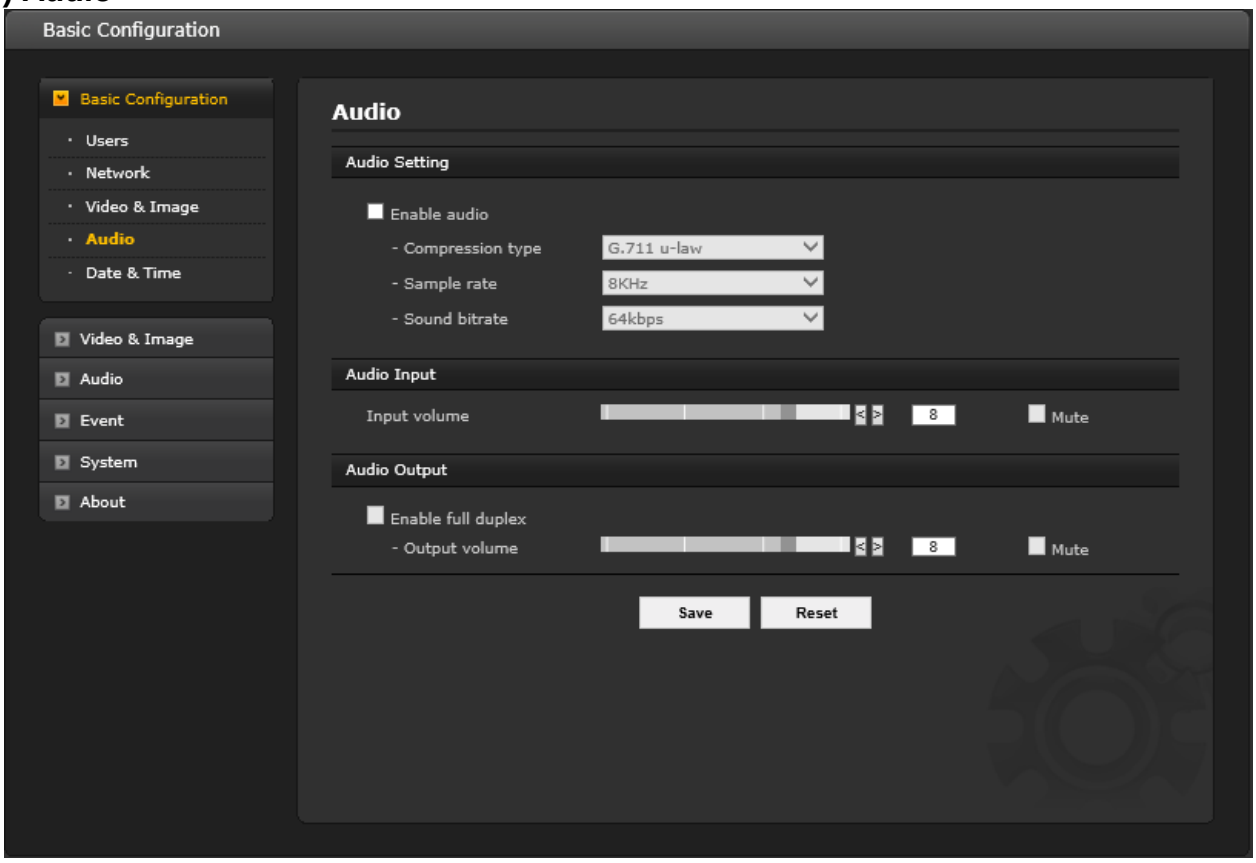
3) Video & Image

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.

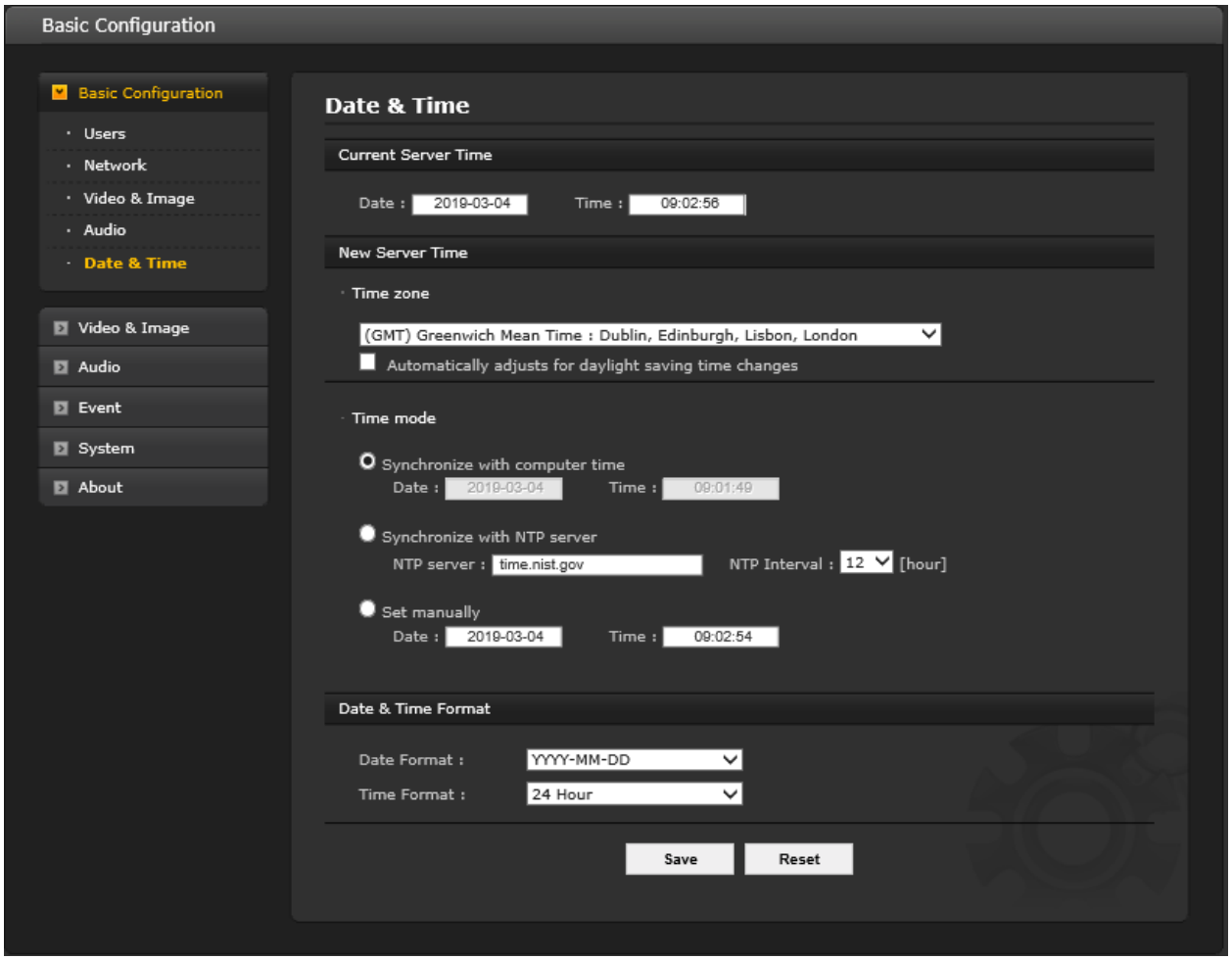
4) Audio



The network camera can transmit audio to other clients using an external microphone and can play audio received from other clients by attaching a speaker. User can setup and change setting of Audio in this page.

Please refer to “Audio” for more details about Audio setup.

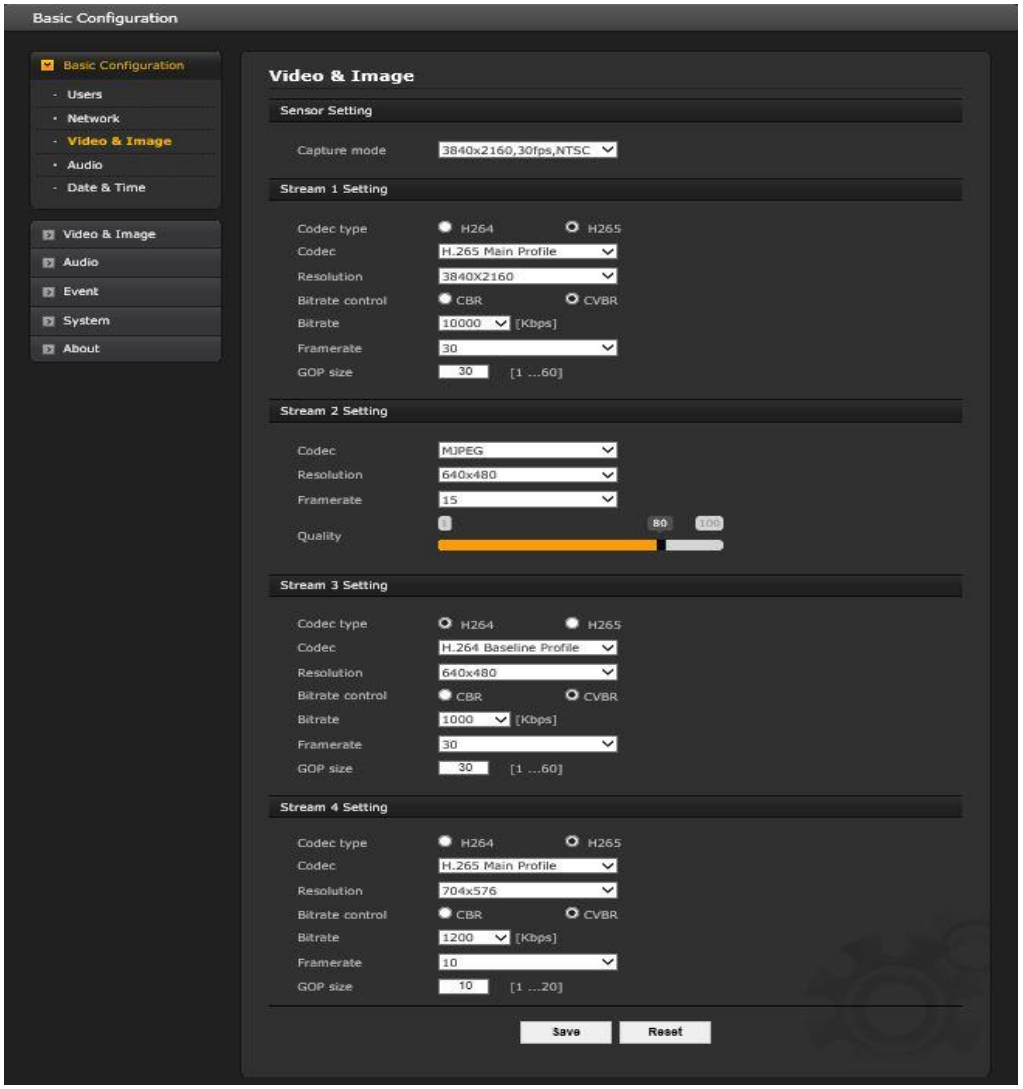
5) Date & Time



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.

3.6.2 Video & Image



1) Basic

- **Sensor Setting:**
  - **Capture mode:** User can select sensor capture mode resolution/fps and NTSC/PAL (some models are fixed to NTSC or PAL).

- **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.

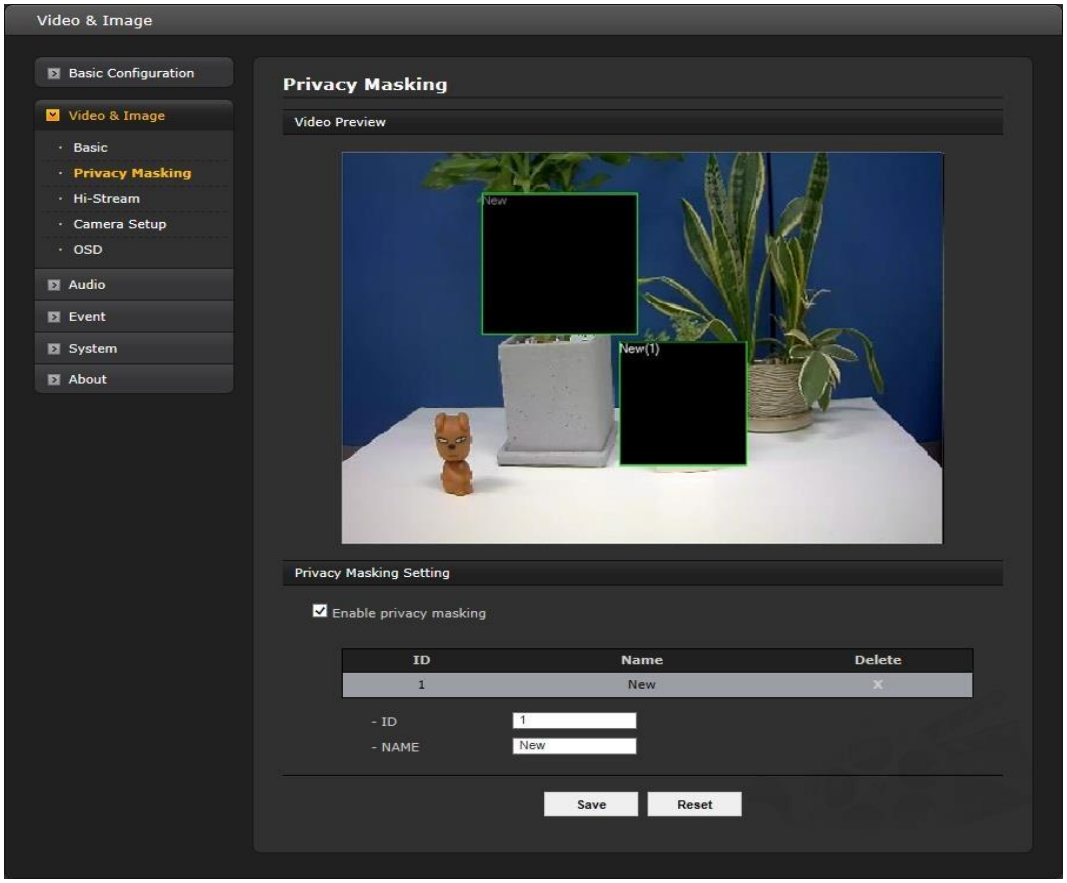
- **Resolution:**
  This enables users to determine a basic screen size when having an access through the Web Browser or PC program. The screen size control comes in several modes. Users can change the selected screen size anytime while monitoring the screen on a real-time basis.

- **Bitrate control:**
  The bit rate can be set as Constrained Bit Rate (CBR) or Constrained Variable Bit Rate (CVBR). Limiting the maximum bit rate helps control the bandwidth used by the H.264 or H.265 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.
  - **CBR:** Constrained bitrate.
  - **CVBR:** VBR with maximum bitrate which is set in Bitrate.
- **Bitrate:** Maximum bitrate for CBR in the range of 100kbps ~10Mbps.
- **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. Vicon recommends that GOP be the same as the fps.

- **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, decrease the value. For the purpose of general monitoring, 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 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 selected parts of the video image being transmitted to be masked from view. Up to eight privacy mask can be set.

NOTE: The masking is displayed only when the “Enable privacy masking” box is selected.

The privacy masks are configured by Mask windows. Click and drag mouse to designate a mask window area. 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.

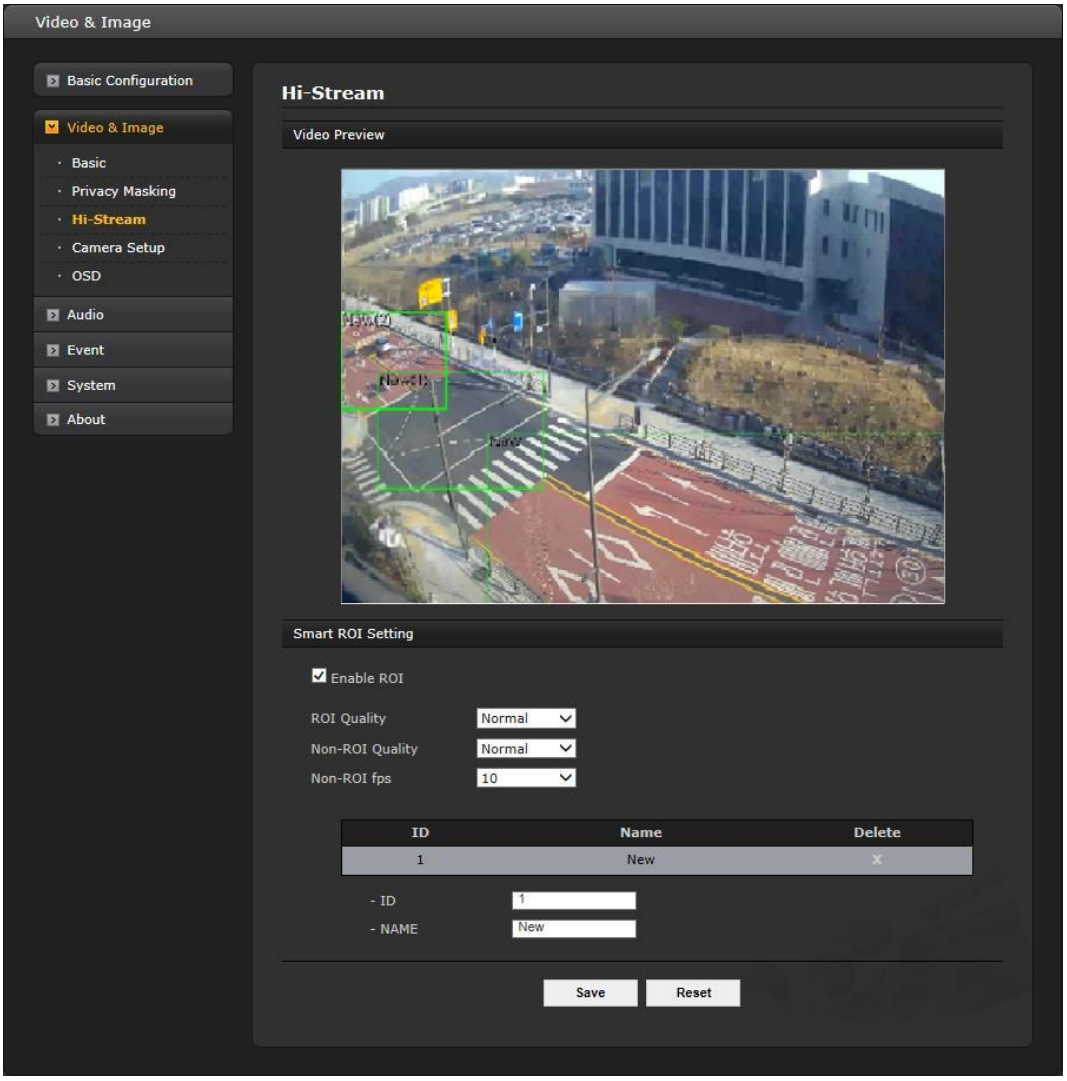
To create a mask window, follow steps:

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.

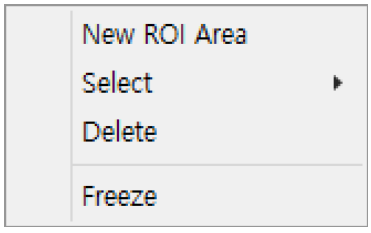
3) Hi-Stream

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



• **Enable ROI:** Select “Enable ROI” to activate 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.



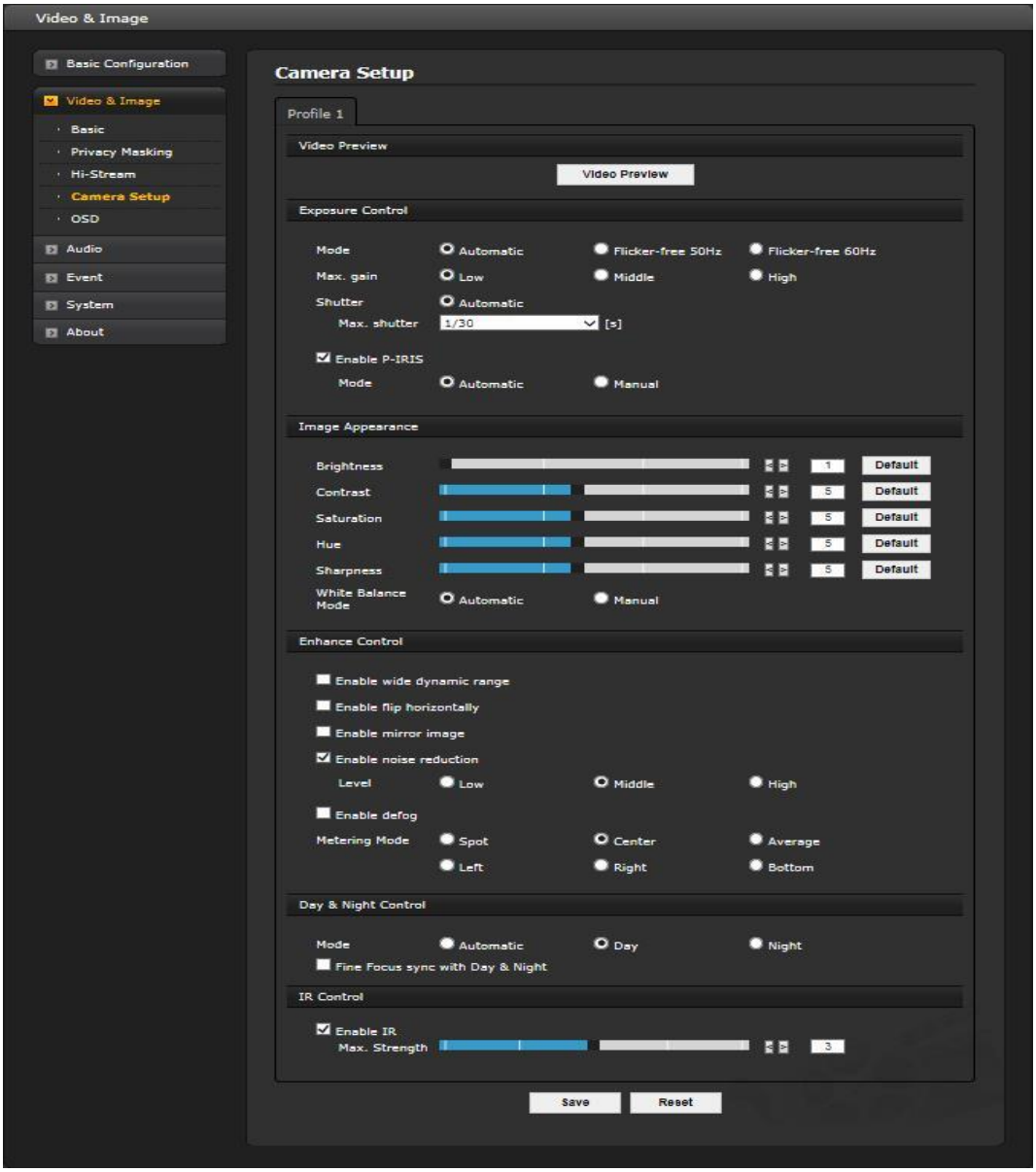
- Delete Region: Click the right button of mouse and select the region.
  Click **Delete** or click **X** from the region table.

- **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.

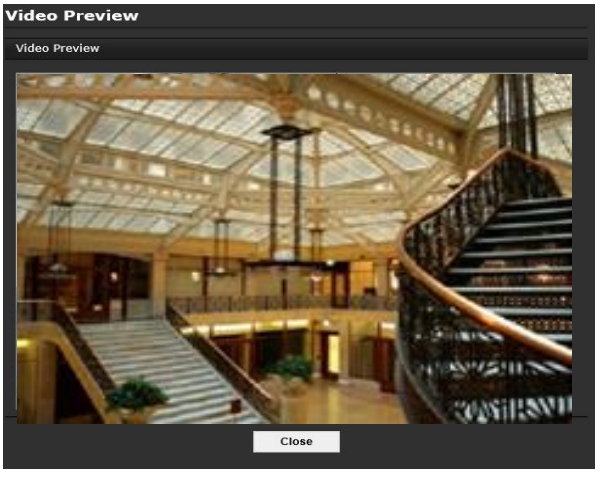
When the settings are complete, click **Save** button to save the settings, or click **Reset** button to clear all of the information you entered without saving it.

4) Camera Setup

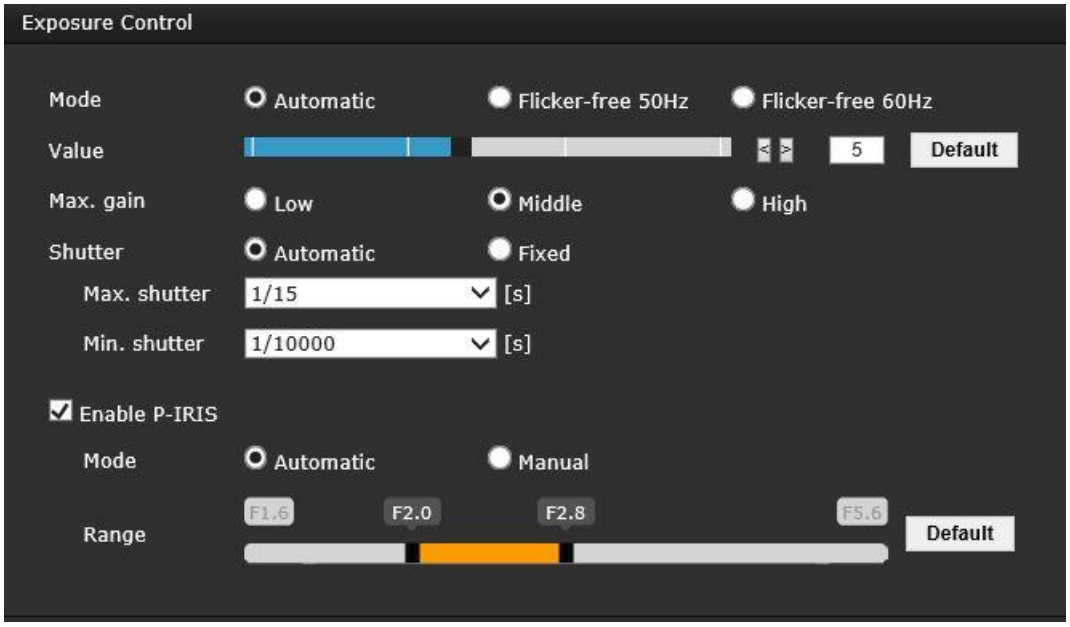
In this page, user can setup Exposure Control, White Balance Control, Image Appearance, Day & Night control and IR Control.



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



· **Exposure Control**



– **Mode:** Determines exposure mode between automatic and flicker-free modes. Users can use Automatic mode with full shutter speed or Flicker-free mode with a limited range of shutter due to an anti-flicker function.

– **Value:** Sets exposure target.

– **Max. gain:** Sets maximum gain threshold.

– **Shutter:** Select shutter speed of the sensor between automatic and fixed. In Automatic mode, Max shutter and Min shutter can be selected. In fixed mode, you can manually select the shutter speed.

* **Max. shutter:** Allows you to set the threshold for slow shutter speeds used in dark environments.

* **Min. shutter:** Allows you to set the threshold for fast shutter speeds used in bright environments.

If you are monitoring a fast object, such as a fast car, change the Max shutter to a faster value (e.g., 1/10 -> 1/120).

NOTE: When the shutter speed is manually selected, the screen may be saturated or dark.

– **Enable P-IRIS:** Check this box to activate the P-IRIS function.

If Automatic is selected, users can specify the range of P-IRIS to be used, and P-IRIS is automatically adjusted according to the amount of light around the camera.

If Manual is selected, P-IRIS is fixed.

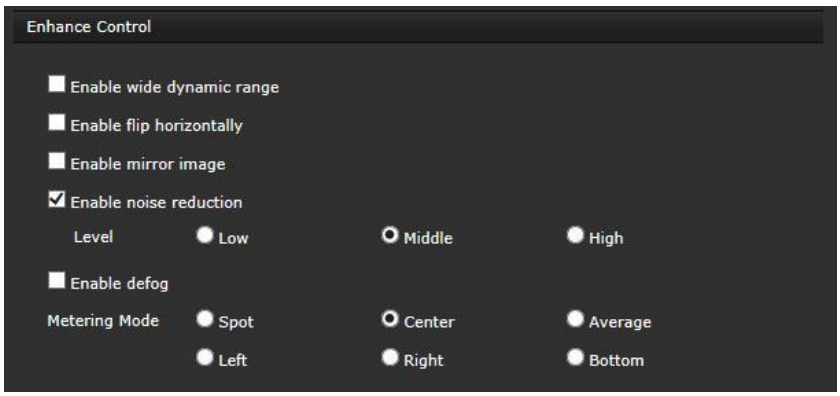
(P-IRIS changes to maximum open when changing to night mode to secure light intensity.)

· **Image Appearance**

This provides access to the advanced image settings for the network camera. User can either use slide bar or type in number.

- **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 that is appropriate for camera installation environment. If Manual mode is chosen, user can set R, G, B gain manually.

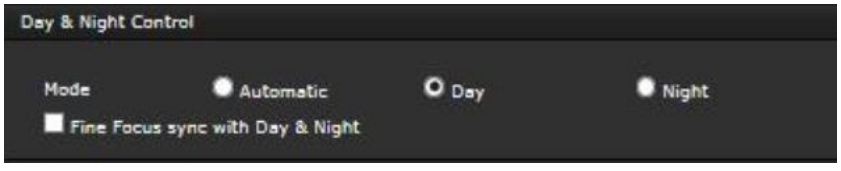
· **Enhance Control**



- **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 mirror image:** Check this box to mirror 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.
- **Metering Mode:** Users can change the metering mode when defog is enabled.
  ***** Metering Mode: Method of measuring the intensity of the light hitting and reflected by a subject in order to determine the exposure required.

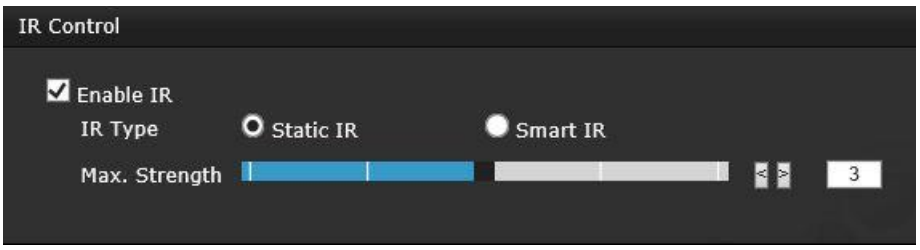
· **Day & Night Control**

User can setup Day & Night operation modes: Automatic, Day, and Night.



– **Mode:**
  - **Automatic:** Normally displays color image, and switches automatically to black & white image after the ambient light level reaches a pre-defined threshold.
  - **Day:** Always displays color image.
  - **Night:** Always displays black & white image.
– **Threshold:** Adjusts the level of light at which the camera automatically switches between color and black & white image.
– **Fine Focus sync with Day & Night:** Focus control automatically adjusts upon Day/Night change. (This menu appears for motorized lens model only.)

- **IR Control**
  This camera is equipped with IR illuminators. User can enable/disable built-in IR LED and setup related controls.



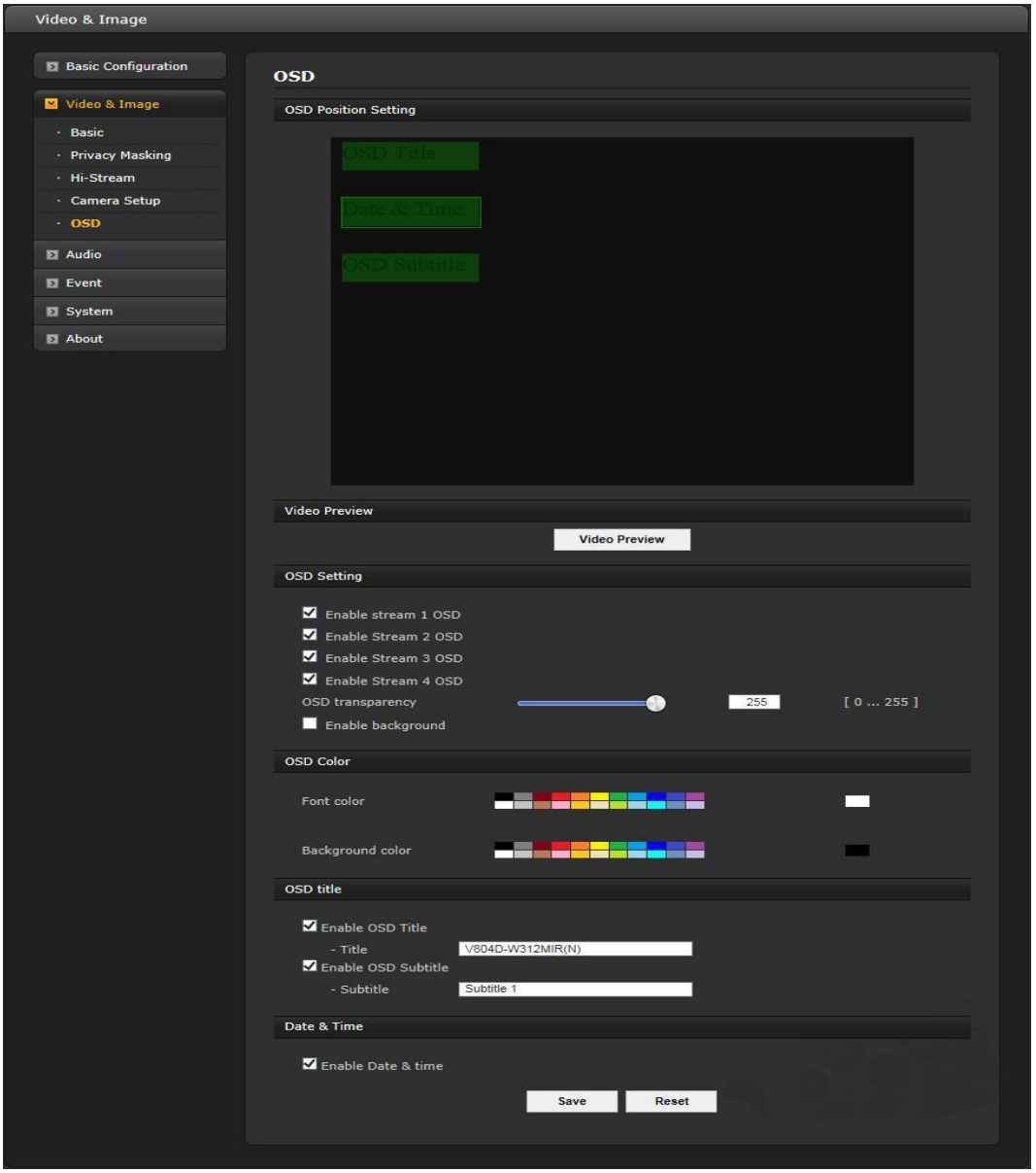
– **IR Type:**
  * **Static IR:** When switching to Night, IR is ON with the set value.
    • **Max Strength:** Users can specify the intensity of the IR to prevent saturation of the image.
  * **Smart IR:** This function adjusts IR for appropriate brightness if it is dark even using the set Gain at Night switching,
  * **Speed**: Users can adjust the control speed of the Smart IR.

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 camera provides two OSDs (on screen display) for each stream, title and date & time. User can drag green “OSD Title” and “Date & Time” to the desired position and check in preview window.

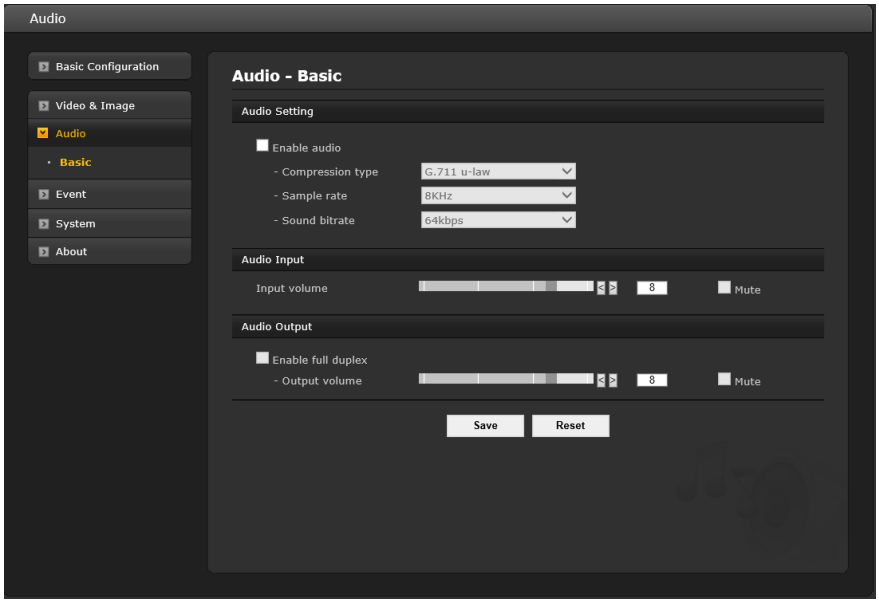
- **Video Preview:** User can check the position of OSD on actual video via preview pop-up window.



- **OSD Setting:** User can select to show or hide OSD for each stream. Also user can set the transparency level of OSD using the slide bar or typing in a number.
- **OSD Color:** User can select OSD font and background color.
- **OSD title:** User can show or hide OSD title by checking/unchecking the Enable box; OSD title can be changed by typing the name in the field. The default is the model name of the camera.
- **OSD subtitle:** User can show or hide OSD subtitle by checking/unchecking the Enable box; OSD title can be changed by typing the name in the field. The default is the Subtitle 1.
- **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.

3.6.3 Audio



The network camera can transmit audio to other clients using an external microphone and can play audio received from other clients by attaching a speaker. The Setup page has an additional menu item called Audio, which allows different audio configurations, such as full duplex and simplex.

- **Audio Setting:**
  - **Enable audio:** Check the box to enable audio in the video stream.
  - **Compression type:** Select the desired audio compression format for G.711. The "μ-law" is for North America and Japan; the "a-law" is for Europe and the rest of the world.
  - **Sample rate:** Select the required Sample rate (number of times per second the sound is sampled). The higher the sample rate, the better the audio quality and the greater the bandwidth required. Default is 8KHz
  - **Sound bit rate:** Depending on the selected encoding, set the desired audio quality (bit rate). The settings affect the available bandwidth and the required audio quality. Default is 64Kbps
- **Audio Input:** Audio from an external line source can be connected to the STEREO Jack I/O of the network camera.
  - **Input volume:** If there are problems with the sound input being too low or high, it is possible to adjust the input gain for the microphone attached to the network camera.
  - **Mute:** User can disable the input audio transmission by checking the box.
- **Audio Output:**
  - **Enable full duplex:** Check the box to enable Full Duplex mode. This means that you can transmit and receive audio (talk and listen) at the same time, without having to use any of the controls. This is just like having a telephone conversation. This mode requires that the client PC has a sound card with support for full-duplex audio.

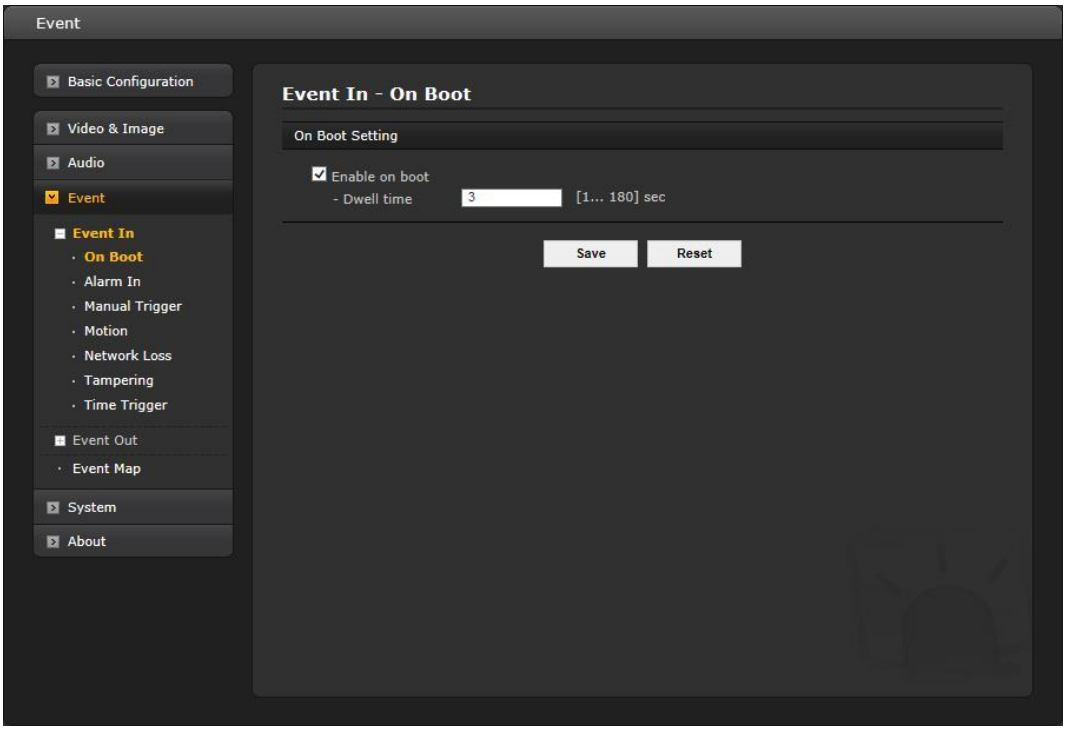
    Uncheck the box to enable Simplex mode. The simplex mode only transmits audio from the network camera to any web client. It does not receive audio from other web clients.
  - **Output volume:** If the sound from the speaker is too low or high it is possible to adjust the output gain for the active speaker attached to the network camera.
  - **Mute:** User can disable the output audio transmission by checking the 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.

3.6.4 Event

- **Event In**

▽ On Boot

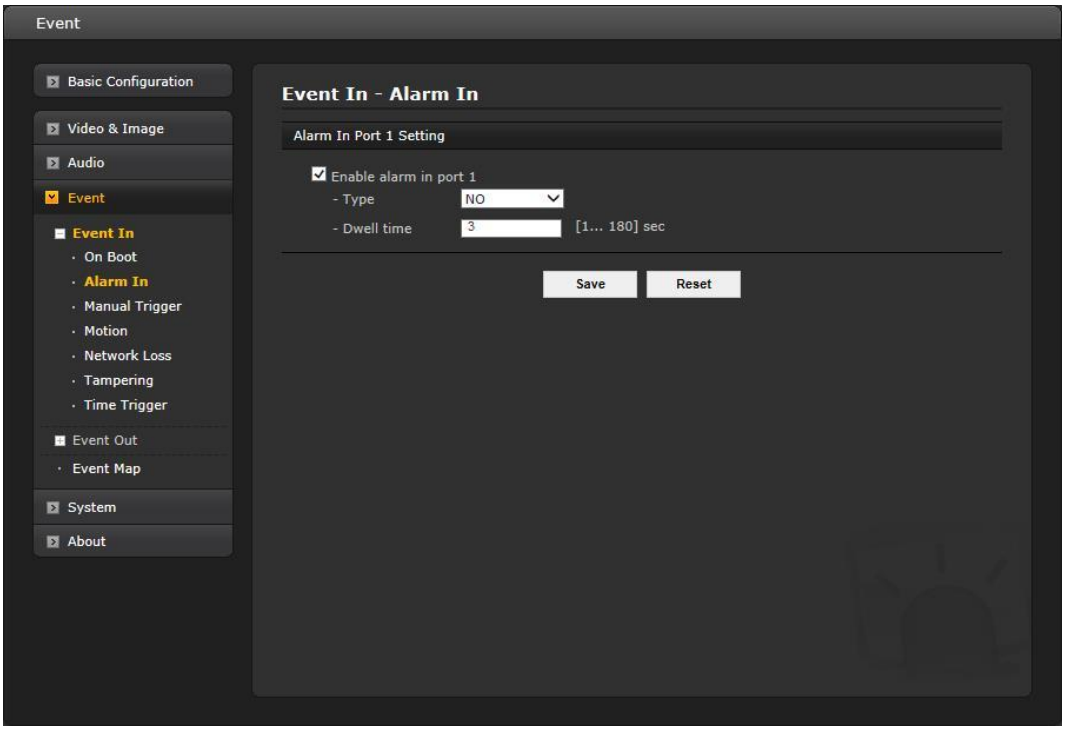


This is used to trigger an event every time the network camera is started.

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.

▽ Alarm In

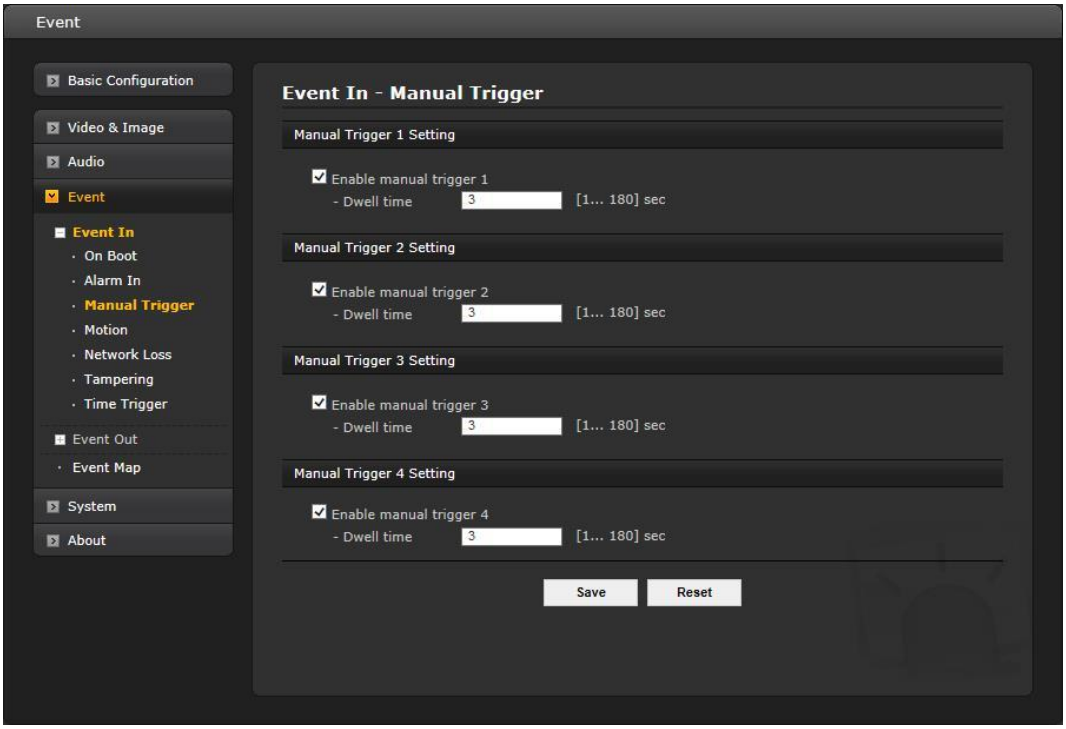


This camera provides 1 Alarm In port and user can set the port. The Port can be given as Normally Open or Normally Closed state, and its Normal state can be configured. In order to use the alarm port, first check the “Enable alarm port 1.”

- **Type:** Choose the type of alarm to use from the drop-down list, NO (Normally Open) or NC (Normally Closed).
- **Dwell Time:** Set the dwell time an event lasts from the point of detection of an alarm input, 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

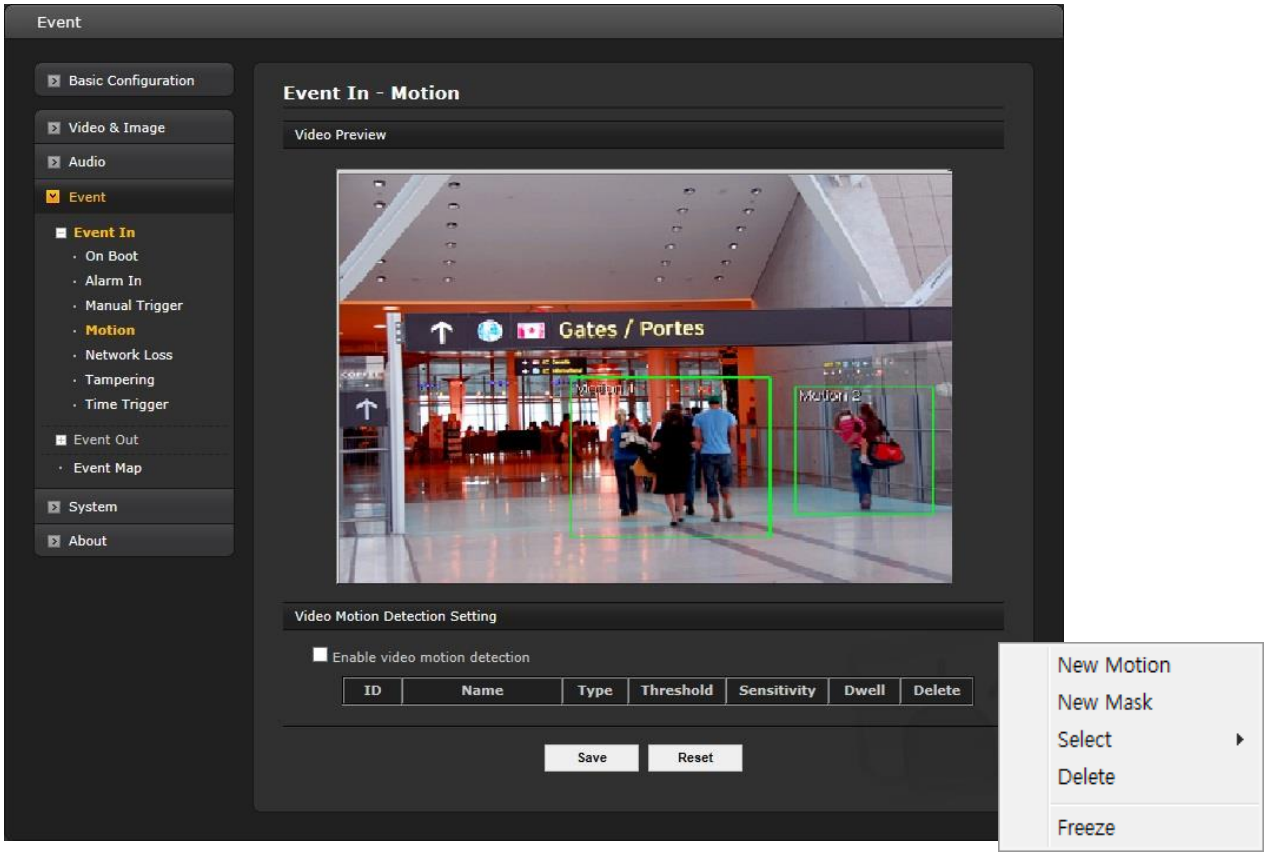


This option makes use of the manual trigger button provided on the Live View page, which is used to start or stop the event type manually. Alternatively, the event can be triggered via the product's API (Application Programming Interface).

Select "Enable manual trigger" to activate the manual trigger (for up to 4 manual triggers). Set the dwell time the trigger lasts, 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.

▽Motion

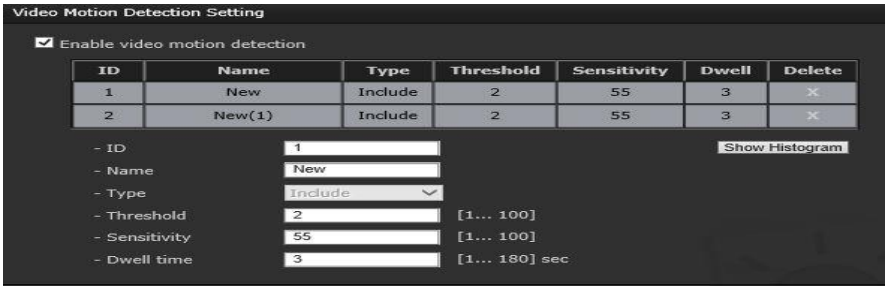


Motion detection is used to generate an alarm whenever movement occurs (or stops) in the video image. This option makes use of the motion detection function with 16 programmable areas, 8 **Include** and **Exclude** zones each.

Clicking the right mouse button on the preview window shows selection pop-up of **New Motion, New Mask, Select, Delete, and Freeze.**

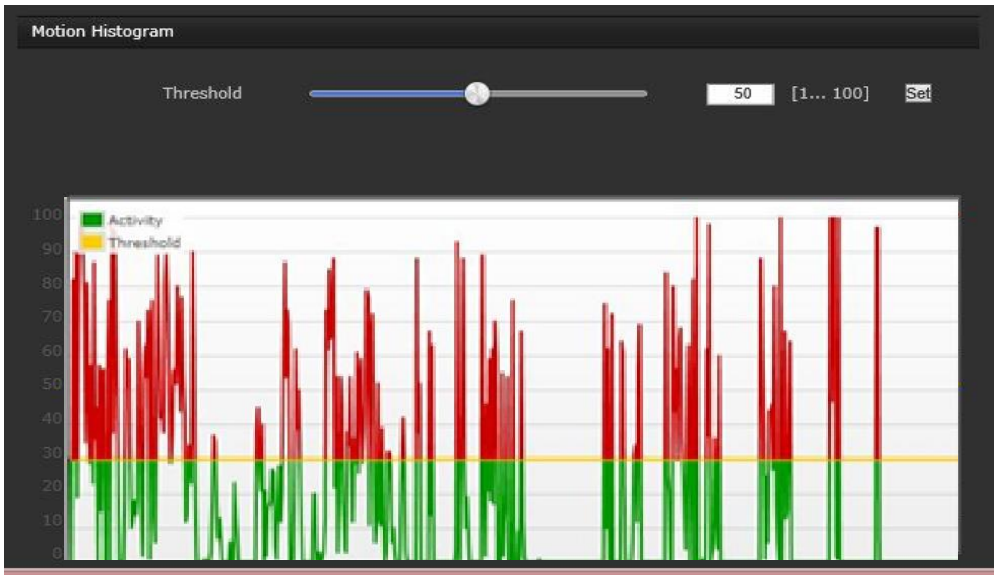
Select **New Motion** and click and drag the mouse to generate an **Include** box of green color.
Select **New Mask** and click and drag the mouse to generate an **Exclude** box of orange color.
Dragging a corner or line resizes the box and dragging from inside moves the box.
Select “Enable video motion detection” to activate motion detection.

- **Zone List**



- **ID:** Identification number generated in the order of generation, **Include** 1~8, **Exclude** 9~16.
- **Name:** User definable zone name.
- **Type:** Shows zone type and cannot be changed.
- **Threshold:** Determines the amount of change in the zone that will trigger event (percentage, 1-100); a lower number increases alarm frequency.

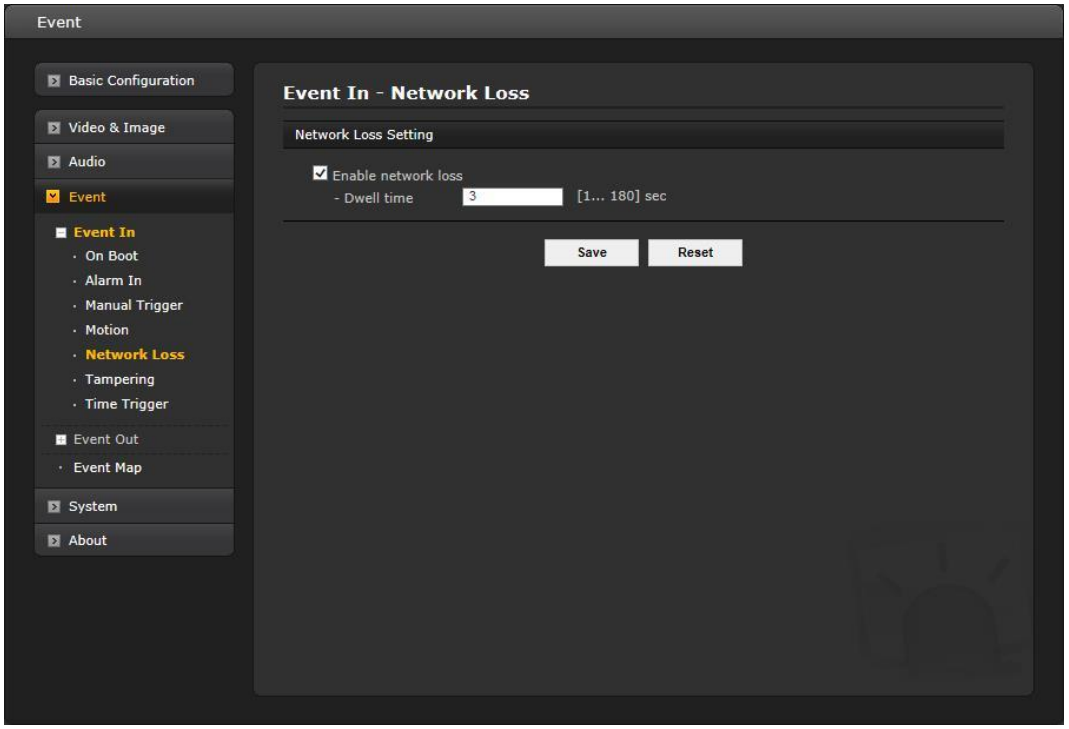
- **Sensitivity:** User can change sensitivity of this function, where larger value sets more sensitive detection.
- **Dwell time:** Set the time an event lasts from the point of detection of a motion (hold time).
- **Show Histogram:** This camera provides live histogram for easy setup of threshold level 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 on the list. User can delete selected zone via right mouse click selection for a selected box or clicking the **X** button in the zone 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.

▽ Network Loss

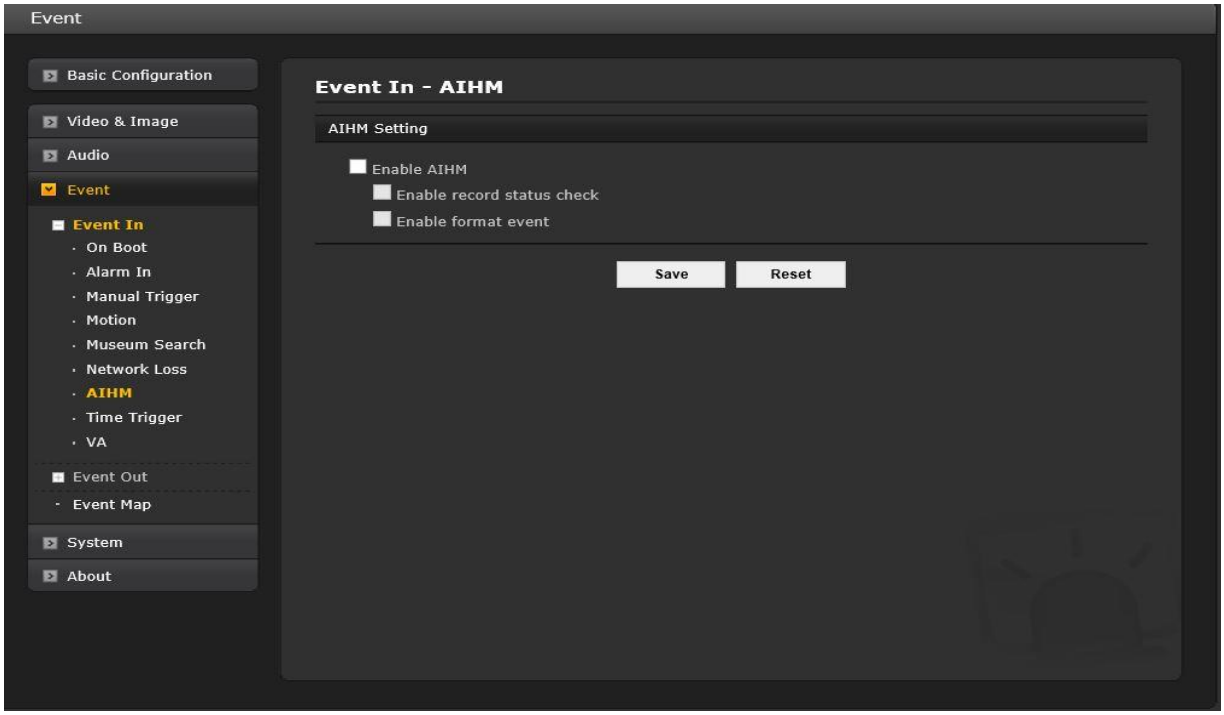


This is used to trigger an event every time the network connection is failed.

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.

▽ AIHM



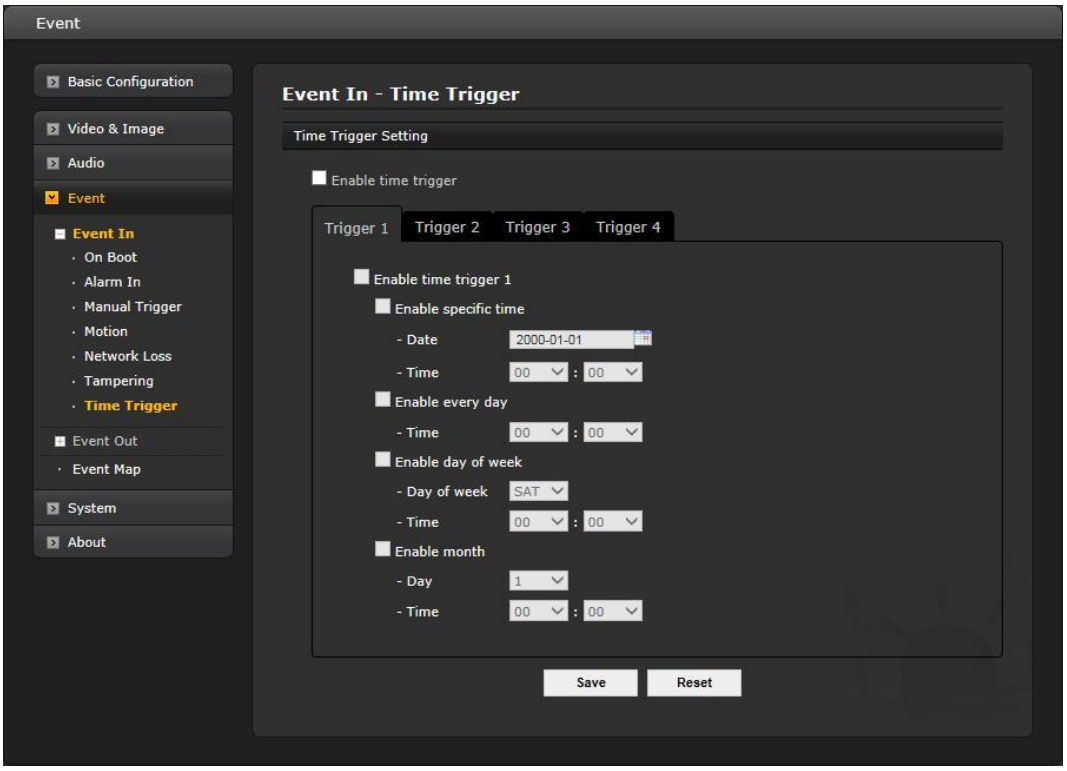
AIHM (Advanced Intelligent Health Monitoring) triggers an event when the camera failed to record or could not be formatted. It is a service that provides Health Information about the camera.

The AIHM event alarm trigger on Event-In makes running the feature of the Event-Out that connected with AHIM by Event-Map.

- **AIHM Setting:** Select “Enable AIHM” to activate the AIHM function.
  - **Enable record status check:** Trigger event if the record status is modified.
  - **Enable format event:** Trigger event if the micro-SD card is formatted.
- **AIHM Server Setting:** Select “Enable AIHM Server” to activate the function to send the AIHM event to the AIHM 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.

▽ 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.

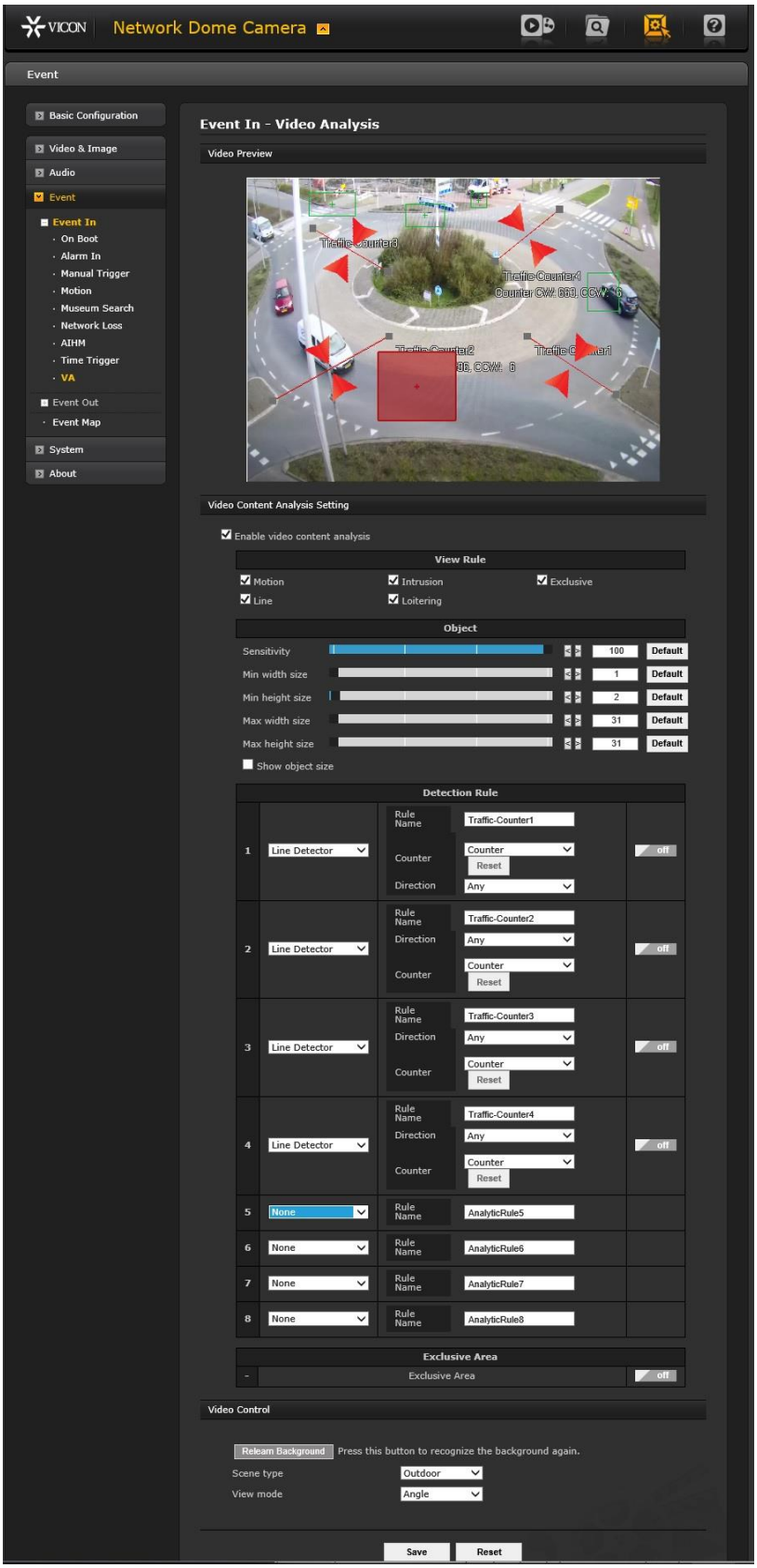
Select “Enable time trigger” to activate the Time Triggerfunction.

- **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 (Video Analysis)

The network cameras provide VA (Video Analysis) functions that analyze video to detect logical events of specified conditions from the camera's video input.



Click the "Enable video content analysis" check box.

NOTE: The VA function is limited to the events that can be used depending on the license type.

- **Standard Type:** Intelligent Motion, Intrusion Detector, Tampering. *These VA functions are available with the camera and do not require any special license.*

- **Advanced Type:** Intelligent Motion, Intrusion Detector, Tampering, Line Detect, Loitering, Human Detector. *These VA functions require an additional license.*

- **View Rule:** In setting VA Event, users can select events to be displayed in Video Preview.
- **Object:** Users can set Object settings.

- Sensitivity allows users to set the object sensitivity to be detected; a larger value increases the detection sensitivity. If there is a lot of noise (shaking leaves, etc.) on the screen, lower the Sensitivity value.

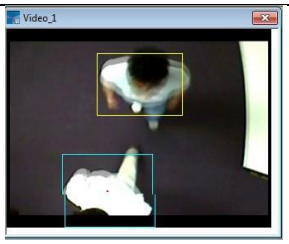
- Users can set the object size to be detected by Min/Max size adjustment.

- Select Show object size to display the object size set in Video Preview.

NOTE: Object size recommended settings

- Indoor installation (32.8 ft/10m distance, based on average height): Sensitivity 80, Min width size 2, height size 6 Max, width size 50, height size 60.

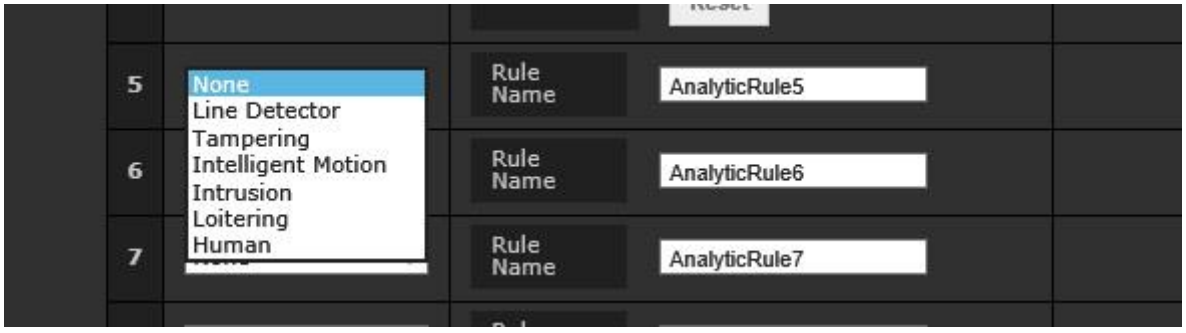
- Outdoor installation (98.4 ft/30m distance, based on vehicle): Sensitivity 80, Min width size 2, height size 4 Max, width size 60, height size 50.

Situation	Default set image	Recommended settings	Modified set image
Two objects are detected as one	In this scene, two objects are detected as one. This is usually due to the maximum size of the object that is not set correctly. Reduce the maximum size of the object.	Generally, when setting the minimum and maximum sizes, the average size should be set to the minimum size of the object, half the width and height of the object, and the maximum size of the object should be about 130% of the width and height of the average object.	 By adjusting the maximum size, two people are detected as separate objects.
One object is detected as two	In this scene, one object is detected as two objects. Usually this is because the minimum and maximum sizes are set incorrectly. Increase the minimum and maximum size of the object.	Generally, when setting the minimum and maximum sizes, the average size should be set to the minimum size of the object, half the width and height of the object, and the maximum size of the object should be about 130% of the width and height of the average object.	Increasing the minimum and maximum sizes will ensure that objects are accurately detected as one.
High amount of noise in image	Some scenes contain large amounts of noise, which can have an undesirable effect on the image analysis because unwanted objects are detected in the image or unwanted events occur.	To minimize the noise, reducing the sensitivity will only detect visible objects.	Users can ignore the noise in the image and still detect the object in the scene.

NOTE: A malfunction may occur under the following conditions.

- Dark environment.
- Changes in brightness due to lighting variations or clouds.
- When a moving object or facility is engaged or overlapped.
- When directing the camera towards a light source (e.g., cars in a tunnel, trains).
- When a shadow occurs.
- When trees and plants are shaking in the wind. (When possible, install the camera in a location free of trees and other plants; when impossible, specify the area as Exclusive Area.)
- Changes in a dynamic fountain, as the water may go up and down.
- An environment where reflections occur, such as rivers, lakes, glass, windows, mirrors, etc. (If possible, install the camera in a location where there are no reflective objects; when impossible, specify the area as Exclusive Area.)
- If the object size is less than 5% or more than 40% on the screen.
- When the brightness changes due to AGC or IRIS operation of the camera.
- When an object with a minor difference from its background and brightness moves.
- Bad weather conditions such as typhoon, snow or rain.
- If the object size changes significantly due to movement toward the camera.
- When passing behind an object such as a tree.
- When the movement is very slight.
- When moving at high speed.
- If there are too many moving objects, it is difficult to create a background (for example, a subway platform at commute time).
- When the image is shaken due to camera shake.
- When there is a flashing light in the shooting area.
- If the camera lens is not clear or out of focus.

- **Detection Rule:** Set VA Event.



- Select Event (default: None). When Event is selected, a menu for setting Rule Name and Event will be displayed. Users can set Event in Video Preview with on/off toggle switch.

NOTE: The number of Detection Rule differs depending on License Type.

- Standard Type: 3
- Advanced Type: 8

- **How to set up each VA:**
  - **Line Detector:**

1. Click the Detection Rule (default: None) menu to change to Line Detector.
2. Enter the Rule Name and select the Line Event type from the Counter menu. The Detector will generate an event when an object passes over the set line. Counter sets the direction and generates an event when an object moves in the set direction and increases the count. To reset the count, click the Reset button.
3. Set direction of line detection in Direction menu.
4. Enable the on/off toggle switch to On and set the line area in Video Preview window.

- **Tampering:**

1. Click the Detection Rule (default: None) menu to change to Tampering.
2. Enter the Rule Name and set the Dwell time. Tampering generates an event if there is a scene change. Users can adjust the tampering sensitivity in the Sensitivity menu.
3. In the Light Change menu, users can include lighting on/off as a tampering event. Users can adjust the sensitivity of Light Change in the Light Sensitivity menu.

- **Intelligent Motion:**

1. Click the Detection Rule (default: None) menu to change to Intelligent Motion.
2. Enter the Rule Name and set the Dwell time. Intelligent Motion generates an event when motion is detected in the set area. Users can adjust the sensitivity of Intelligent Motion in the Sensitivity menu.
3. Enable the on/off toggle switch to On and set the Intelligent Motion area in Video Preview window. The Intelligent Motion area is displayed as a blue cell.

NOTE: When Intelligent Motion is enabled, the existing Motion Detection is disabled.

- **Intrusion:**

1. Click the Detection Rule (default: None) menu to change to Intrusion.
2. Enter the Rule Name. Intrusion occurs when an object enters, appears or exits in/from set area.
3. Enable the on off toggle switch to On and set the Intrusion area in Video Preview window. The Intrusion area is displayed as a yellow cell.

- **Loitering:**

1. Click the Detection Rule (default: None) menu to change to Loitering.
2. Enter the Rule Name. Loitering generates an event if an object enters a set area and walks or stays for more than the set time.
3. Enable the on/off toggle switch to On and set the Loitering area in Video Preview window. The Loitering area is displayed as a purple cell.

- **Human:**

1. Click the Detection Rule (default: None) menu to change to Human.
2. Enter the Rule Name. Human generates an event if the detected object is a person.

NOTE: Conditions for distinguishing human:

- The object must be 10-20% of the screen size.
- Head and shoulders should be visible and moving.

The camera may not be able to distinguish human in the following situations:

- A person who is sitting, crawling or lying.
- Shooting vertically from the ceiling, so a person is directly under the camera.
- When a head is unseen.
- A person carrying a large piece of baggage or a large object.
- A person riding a bicycle.
- People close together, as when putting arms around each other or carrying on one's back.
- Shown less than a second.

- **Exclusive Area:** User can set up an area to be excluded from Object detection. This will reduce false alarms and CPU usage of the camera by cutting down unnecessary operation. Please note that Exclusive Area only effects Object-based events. Motion and Tampering event will operate regardless of Exclusive Area setting.

Situation	Default set image	Recommended settings	Modified set image
Scene with swaying trees	This scene involves many unwanted movements from the tree. These movements can cause unwanted objects to be detected during image analysis.	Reduce the sensitivity to avoid tree movement. As an alternative, users can set the area around the tree to Exclusive Area.	This setting avoids the detection of tree movement during the image analysis.

  - **How to set Exclusive Area**

    1. Enable the on/off toggle switch to On and set the Exclusive Area in Video Preview window. The Exclusive Area is displayed as red cells.

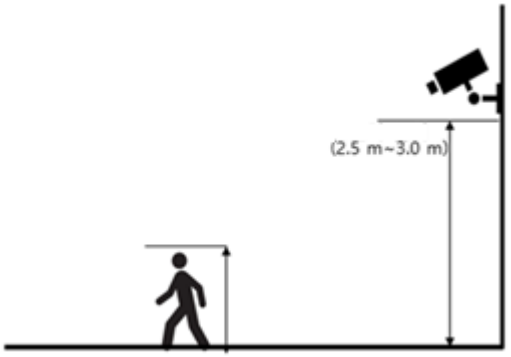
- **Video Control:** Users can adjust settings for optimal image analysis.
  - Click the Relearn Background button to remember the current image as background.
  - Use the Scene type menu to select the place where the camera is installed, Outdoor or Indoor.
  - Use the View mode menu to select the angle at which the camera is installed.

NOTE: View mode

- Overhead is generally suitable for counting or detecting a moving direction.
- Angle is suitable for detecting intrusions.
- Horizontal should only be used for home security.

Recommended camera installation conditions:

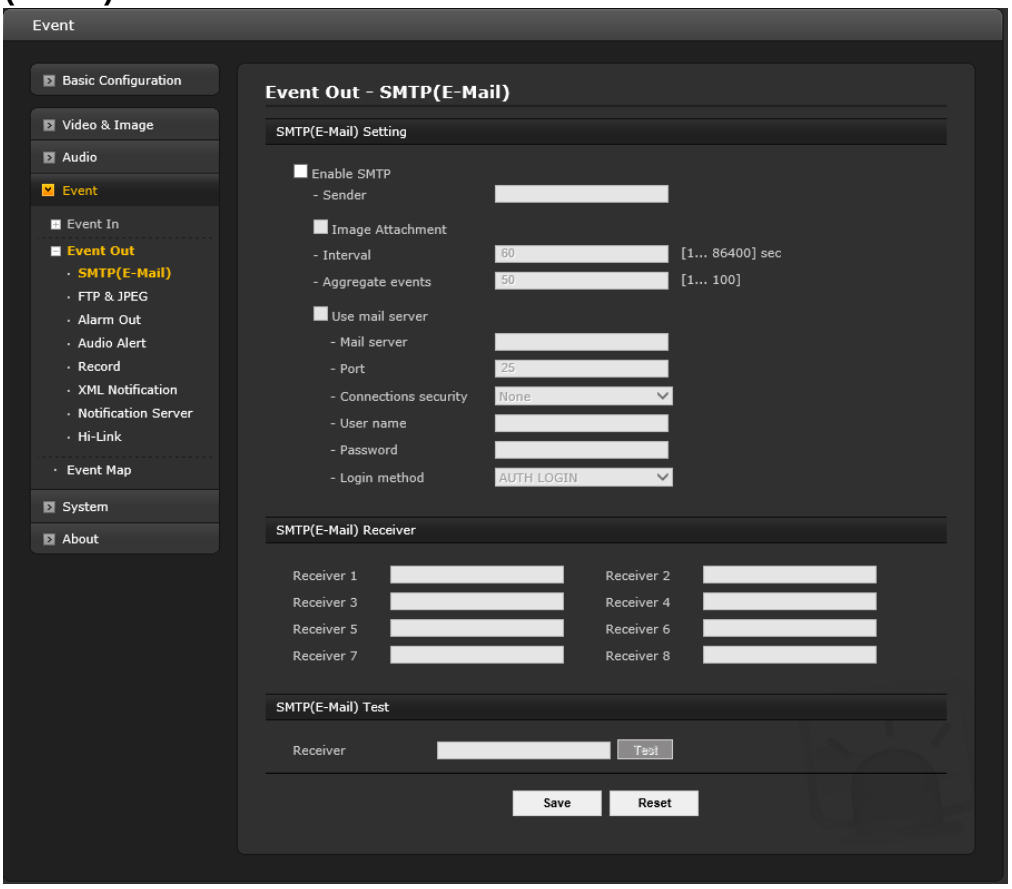
- Installation height: 8.2 ft/2.5m ~ 9.8 ft/3.0m
- Installation type: Tilt about 30 degrees horizontally and face downward.
- Object: The object must be at least 9.8 ft/3 meters away from the camera.



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.

- **Event Out**

▽ **SMTP (E-Mail)**

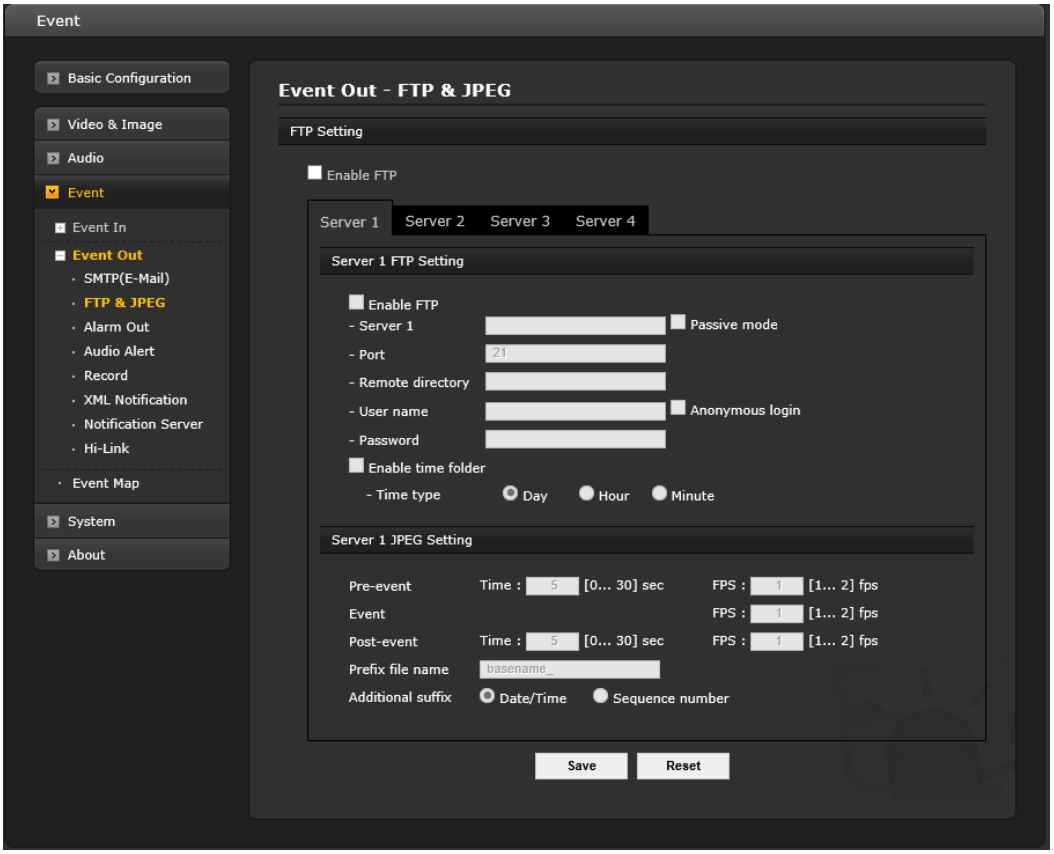


The network camera can be configured to send event and error email messages via SMTP (Simple Mail Transfer Protocol).

- **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 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**.
- **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 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 connection, whereby the network camera actively initiates both the FTP control and data connections to the target server. This is normally desirable if there is a 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.
  - **Enable time folder:** Create the folder in the FTP Server.

    - Time type: User can set the name of the folder where the uploaded image will be saved as the date, time, and minute the event occurred.

- **JPEG Setting**

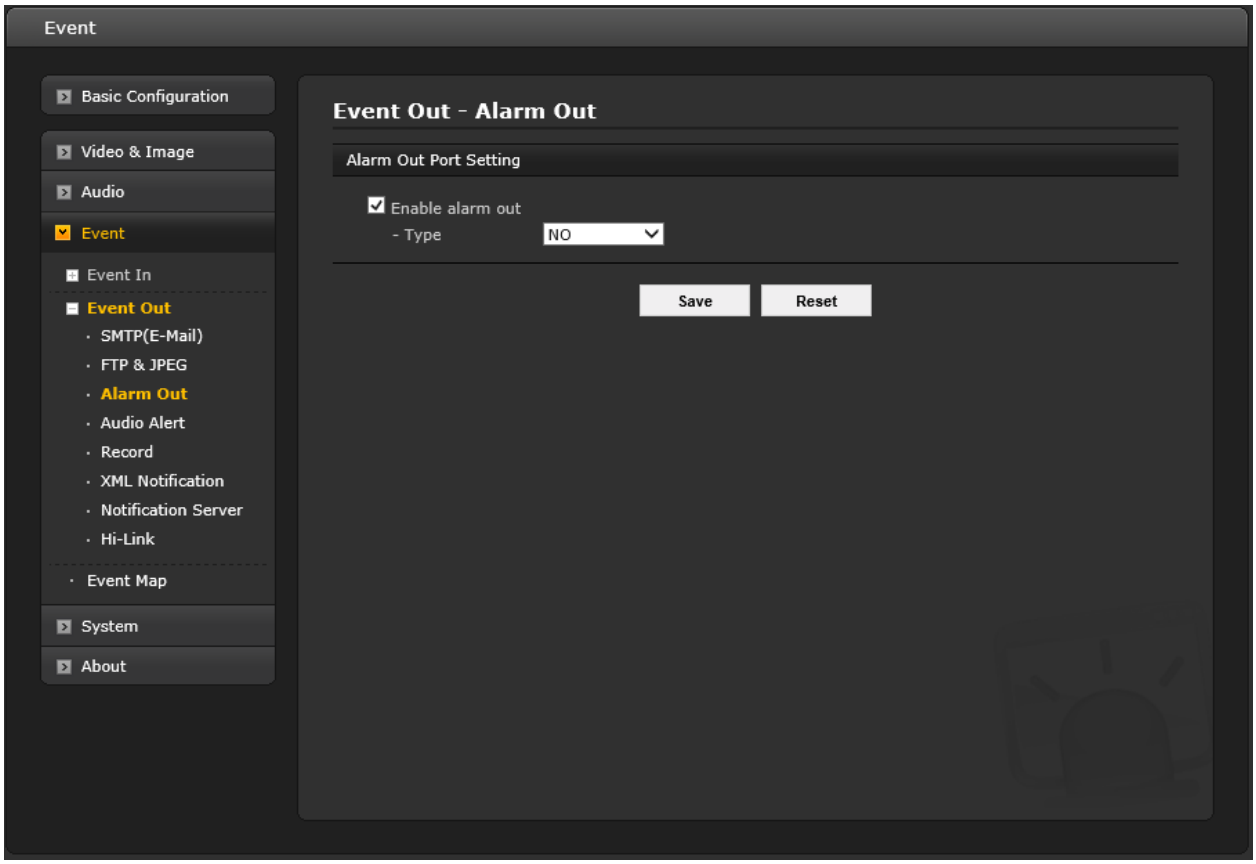
  - **Pre-event:** A pre-event buffer contains images from the time immediately preceding the event trigger. These are stored internally in the server. This buffer can be very useful when checking to see what happened to cause the event trigger. Check the box to

enable the pre-trigger buffer, enter the desired total length in seconds, minutes or hours, and specify the required image frequency.

- **Event:** This function can set required image frequency (1 ~ 2fps) when event is detected.
- **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.

▽ Alarm Out

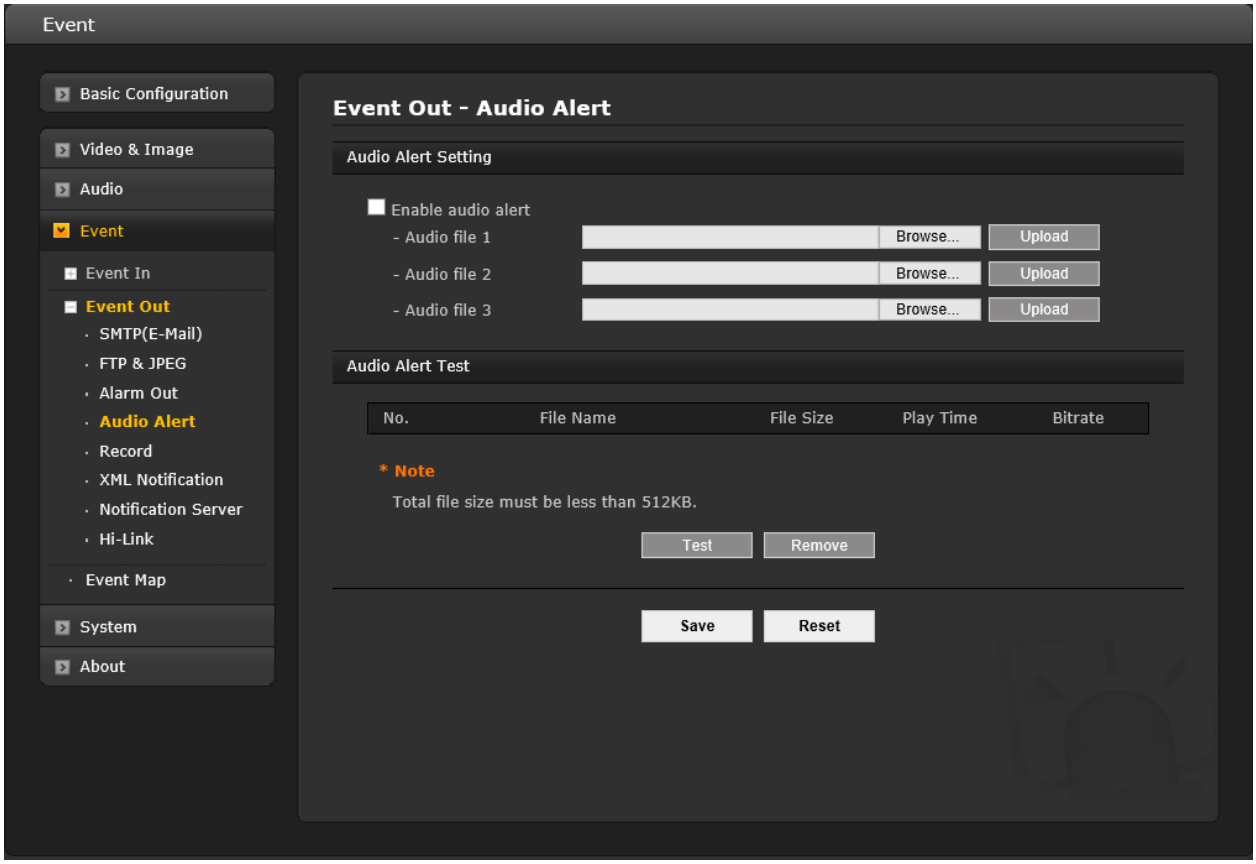


When the network camera detects an event, it can control external equipment connected to its alarm output port.

- **Enable alarm out:** If selected, the output becomes activated for as long as the event is active.
- **Type:** Select a type of NO (Normally Open) or NC (Normally Closed).

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.

▽ Audio Alert



When the network camera detects an event, it can output a predefined audio data to external speaker. Check the “Enable audio alert” box to enable the service.

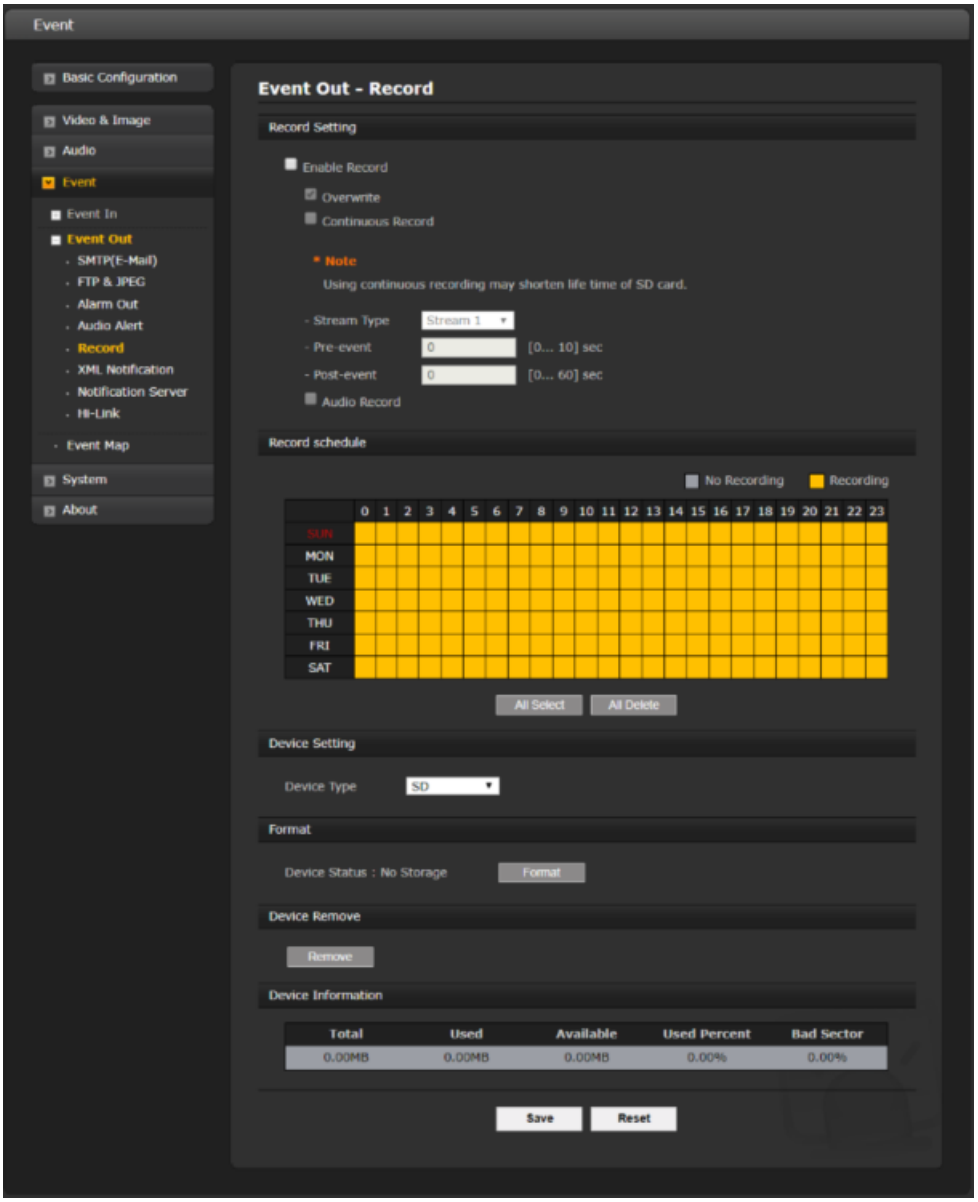
- **Audio Alert Setting**
  To use the audio alert with the network camera, an audio data file made by user must be uploaded from your PC. Provide the path to the file directly, or use the Browse button to locate it. Then click the Upload button. Up to 3 audio files are available. The total file size must be less than 512 KB.

- **Audio Alert Test**
  When the setup is complete, the audio output can be tested by clicking the Test button.
  To remove an audio file, select the file and click the Remove button.

NOTE: For a proper operation of Audio Alert, full duplex must be enabled in the Audio settings page.

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.

▽ Record



When the network camera detects an event, it can record the video stream onto the Micro SD Memory (not supplied) or NAS (Network Attached Device) as a storage device. Check the “Enable Record” box to enable the service.

- **Record Setting**
  - **Overwrite:** Click checkbox to overwrite the storage device; Continuous Record is available when not using an SD card.
  - **Stream Type:** You can select Stream 1, Stream 3 or Stream 4.
    - **Stream1, 3, 4:** H.264/H.265 data.

    Note: Stream2: MJPEG data cannot be recorded.
  - **Pre-event:** Enter pre-event time value for the storage device pre-recording.
  - **Post-event:** Enter post-event time value for the storage device pre-recording.
  - **Audio Record:** Check the box if you want to record audio with video.
- **Record Schedule**

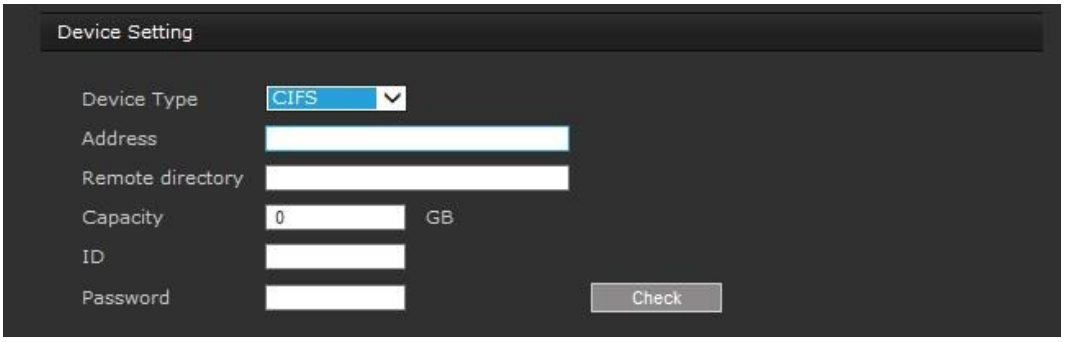
  You can set the weekly recording schedule for each day. Drag or click area by a box unit at first. Clicking the block toggles the recording between on and off. Click the All Select button to set a schedule for the entire week or a whole day, respectively.

- **Device Setting**
  Select the device type to be recorded in the drop-down list. The screen changes according to selection.
  - **SD:** Mounted SD card.
  - **CIFS:** A file format for a NAS device.
  - **NFS:** A file format for a NAS device.

  NOTE 1: Common Internet File System (CIFS) is a remote file access protocol that forms the basis for Windows file sharing, network printing, and various other network services. CIFS requires a large number of request/response transactions and its performance degrades significantly over high-latency WAN links such as the Internet.

  NOTE 2: Network File System (NFS) is a network file system protocol, allowing a user on a client computer to access files over a network in a manner similar to how local storage is accessed. NFS, like many other protocols, builds on the Open Network Computing Remote Procedure Call (ONC RPC) system.

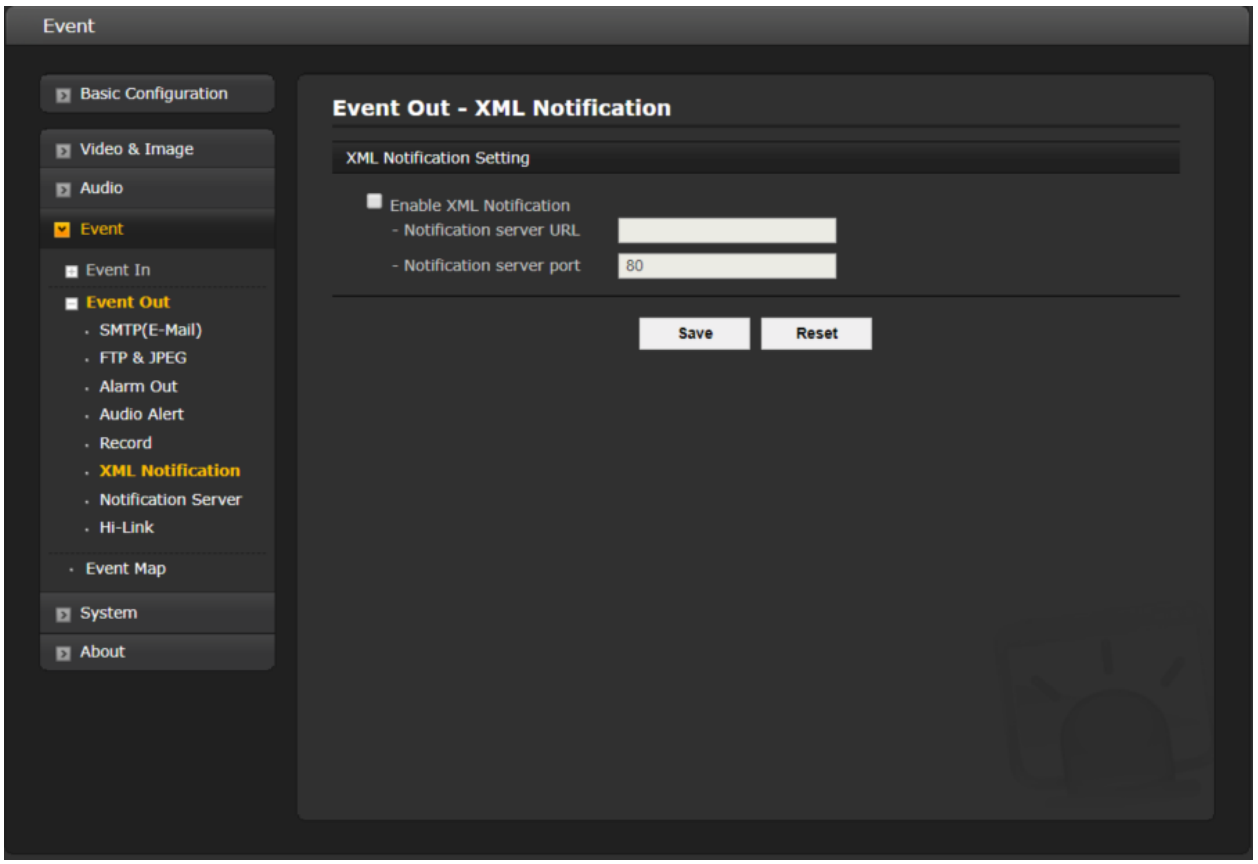
  The CIFS screen displays as below.



  - **Address:** Enter IP address for NAS device.
  - **Remote Directory:** Enter directory or folder location to be recorded in the NAS device.
  - **Capacity:** Enter the capacity of storage to be used. This must be less than the total storage capacity.
  - **ID/Password:** Enter ID and Password. The network camera will ask for these whenever you access NAS device.
  - **Check:** Press the Check button to check the validity of Device Setting data.
- **Format:** Click the Format button to format SD card.
- **Device Remove:** Click the Device Remove button before detaching SD card for data safety in the SD card.
- **Device Information:** Show current SD card information.

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

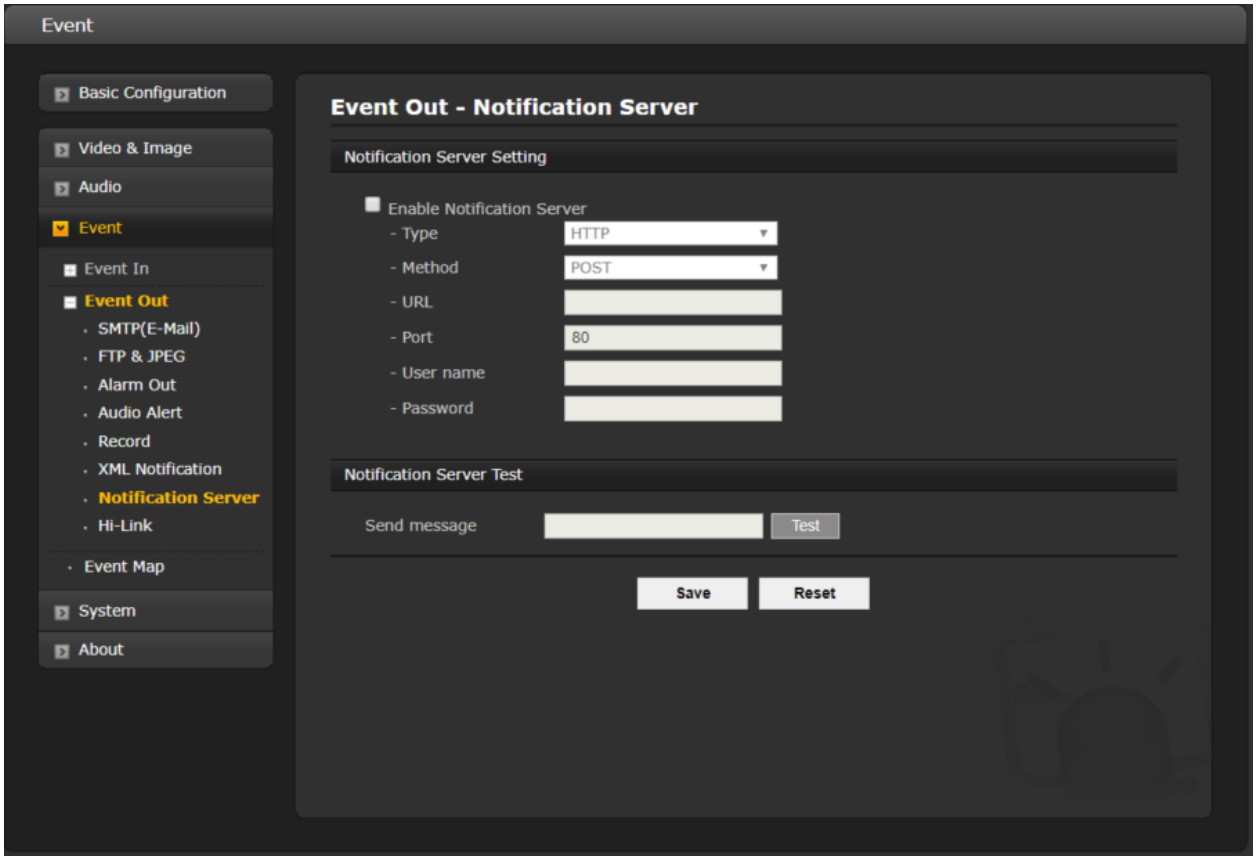


When the network camera detects an event, Notification server is used to receive notification messages as a type of XML data format. Check the box to enable the service.

- **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.

▽ Notification Server

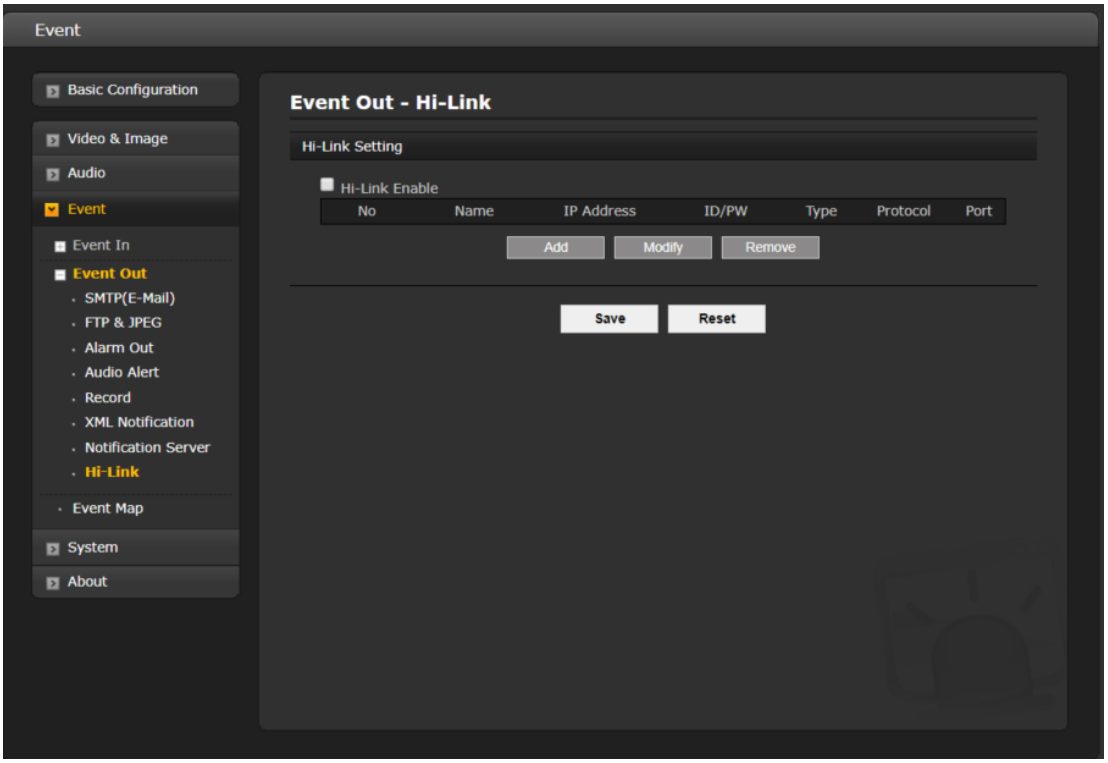


When the network camera detects an event, the Notification Server is used to receive up- loaded image files and/or notification messages. Check the box to enable the service.

- **Notification Server Setting:**
  - **Type:** User can select message transmission type from HTTP, HTTPS, TCP or 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.

▽ Hi-Link



When the network camera detects an event, the Hi-Link is used to operate preset event of PTZ camera.

- **Enable Hi-Link**

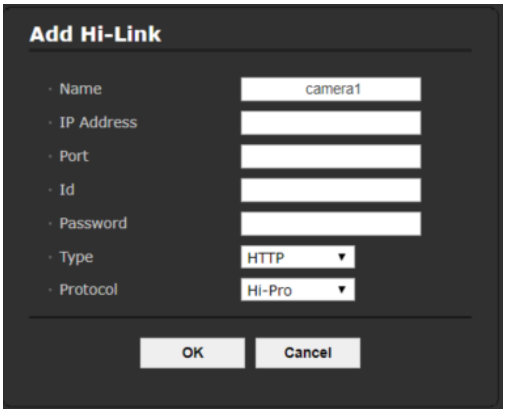
  Click the check box Hi-Link Enable to set the status (enable or disable) of Hi-Link.

- **Hi-Link List Setting**

  To add a new camera, click the Add button. To modify a camera, select a camera from the Camera List and click the Modify button. To remove a camera, select a camera from the Camera List and click the Remove button.

- **Add/Modify Camera**

When the Add and Modify buttons are selected, the following pop-up window appears.



- **Name**

  The maximum length of the Camera name is 14 characters. It must start with an alphabet letter (A-Z, a-z); the other characters can be alpha-numeric or underscore.

- **Address**

  PTZ camera IP address to operate preset event. For example: 192.168.12.244

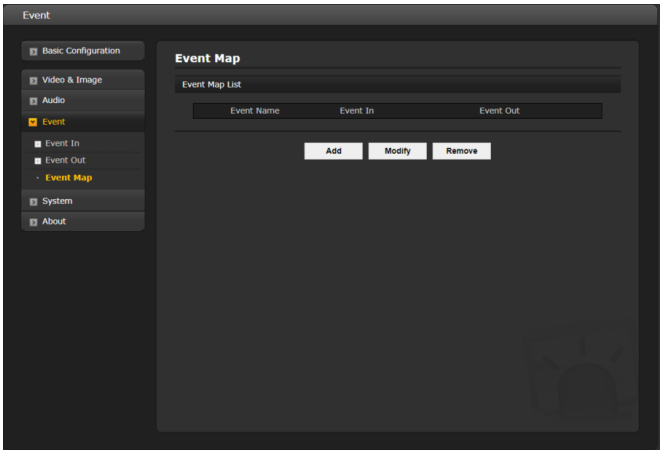
- **Port**

  The port number of the PTZ camera, for example: 80.

- **ID**
  Provide login information of the PTZ camera.
- **PW**
  Provide login information of the PTZ camera.
- **Type**
  Select the appropriate type from the drop-down list: HTTP, HTTPS.
- **Protocol**
  Select the appropriate type from the drop-down list: Hi-Pro Protocol.

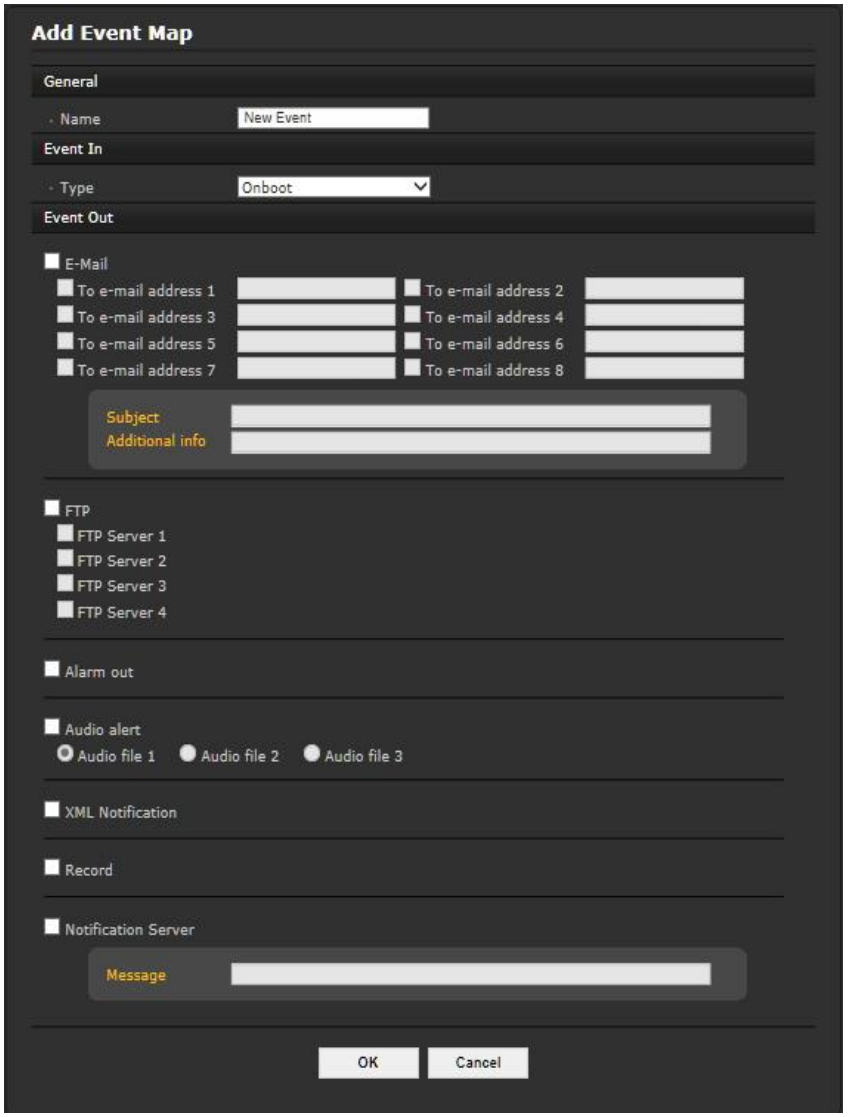
When the settings are complete, click **Save** button to save the settings, or click **Reset** button to clear all of the information you entered without saving it.

- **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.

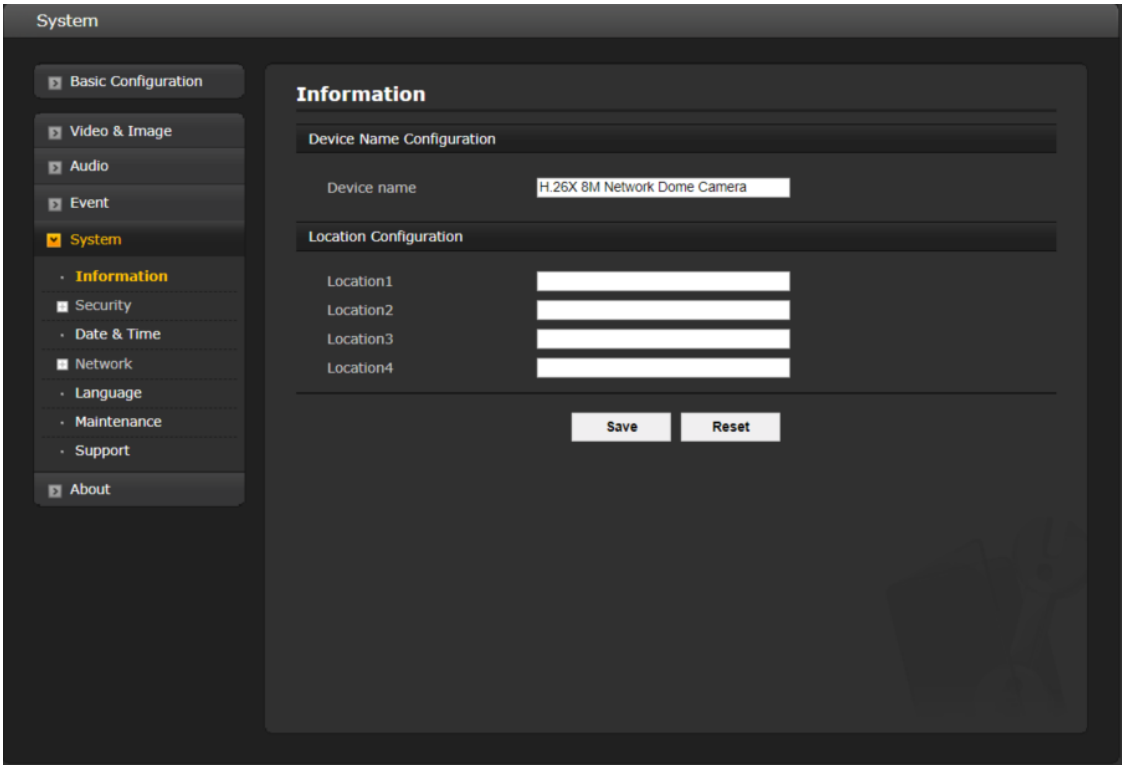


- **General:** Enter the name for a new event map.
- **Event In:** Select an event type in the drop-down list.
- **Event Out:**
  - **E-mail:** Select the email addresses you want to notify via email that an event has occurred.
  - **FTP:** Select checkbox beside FTP to record and save images to an FTP server when an event has occurred.
  - **Alarm out:** Check this box to enable the alarm out.
  - **Audio Alert:** Select an Audio Alert file as the Network Transmitter output when audio alert event triggered. The Audio Alert file must first be configured on the Event In page.
  - **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.
  - **Record:** Record video stream when an event has occurred. The Record option must first be configured on the Event Out page.
    Note: This button disappears if you select AIHM as Event In.
  - **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.

3.6.5 System

1) Information



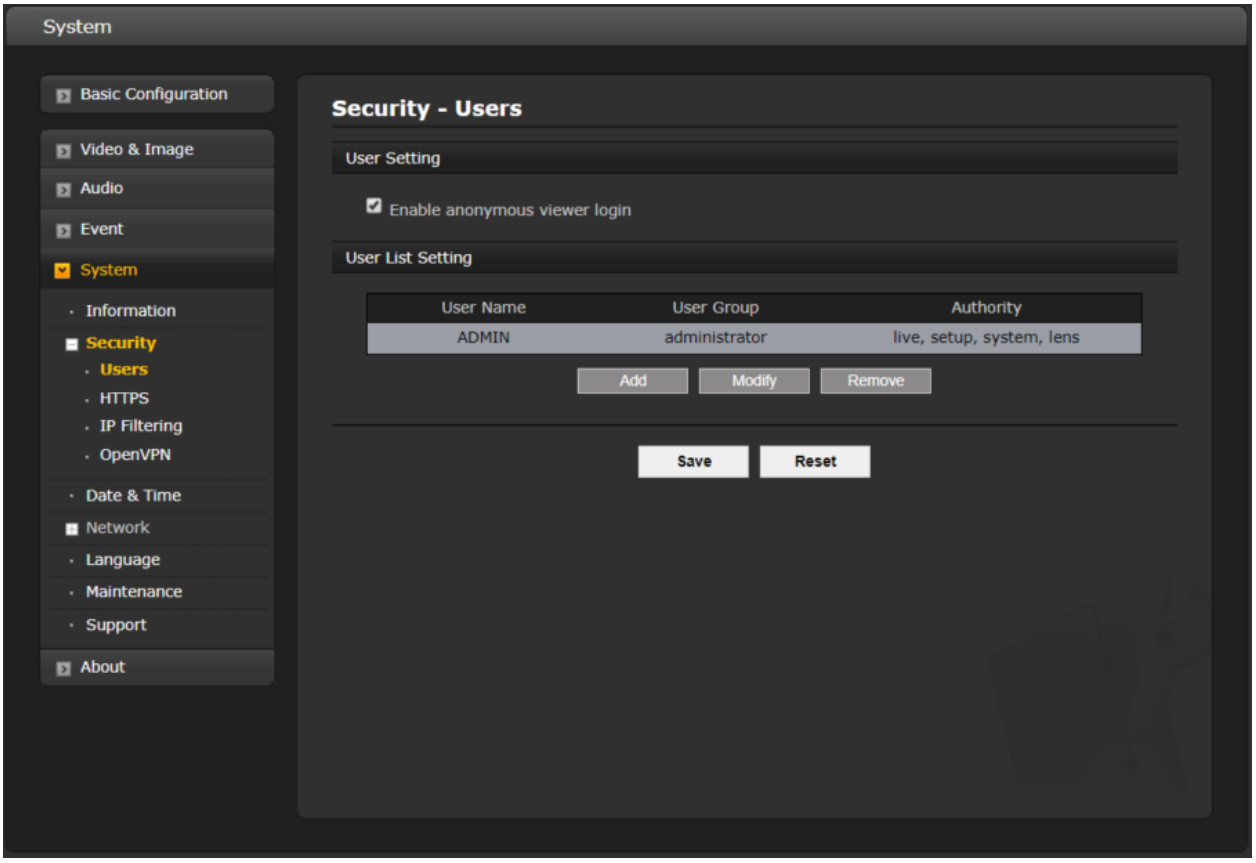
You can enter the system information. This page is very useful when you require device information after installation.

- **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



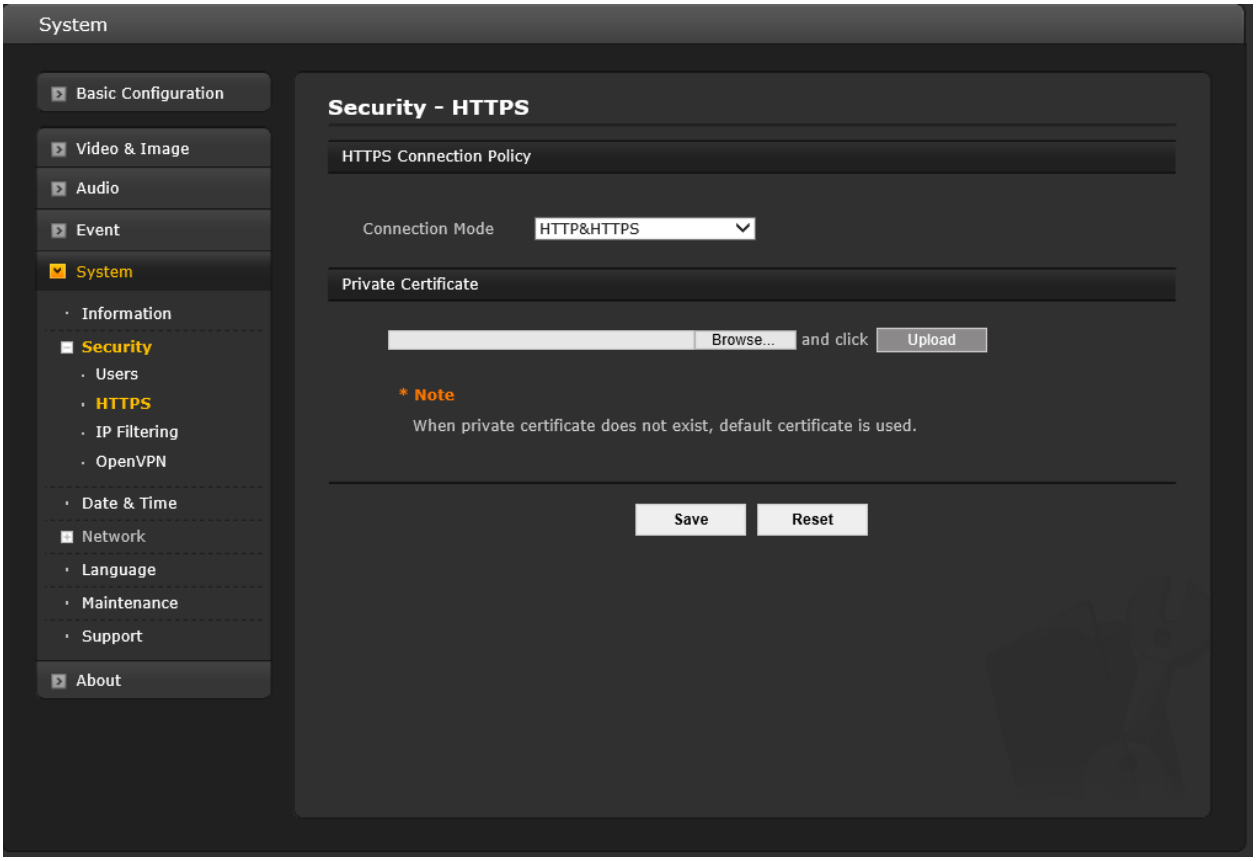
User access control is enabled by default when the administrator sets the root password on first access. New users are authorized with user names and passwords, or the administrator can choose to allow anonymous viewer login to the Live View page, as described below:

- **User Setting:** Check the box to enable anonymous viewer login to the 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. Press the Add button. A pop-up window displays as below.

Enter a user name and password to be added. Register them by pressing the OK button. User information can be changed by clicking the Modify button for the selected user; a user can be deleted by clicking the Remove button for the selected user.

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



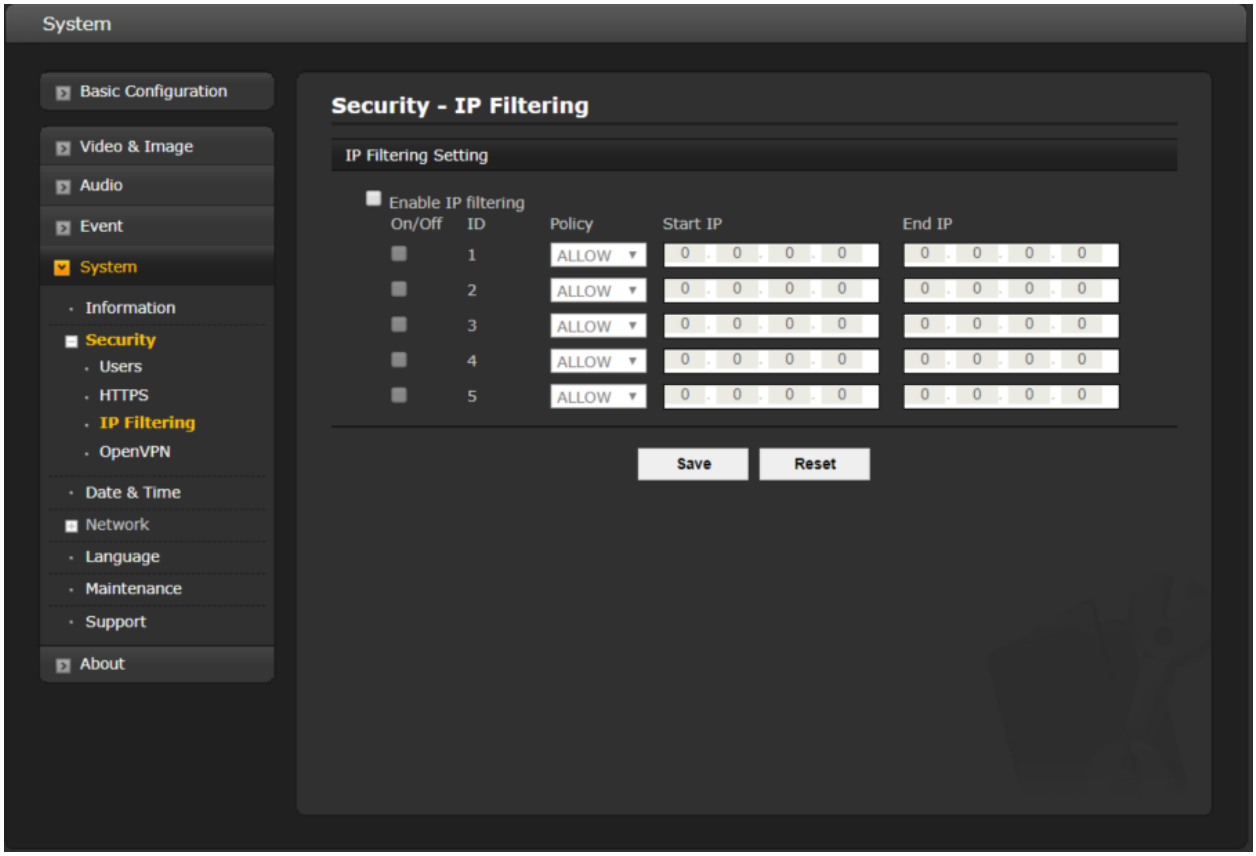
For greater security, the network camera can be configured to use HTTPS (Hypertext Transfer Protocol over SSL (Secure Socket Layer)). Then all communication that would otherwise go via HTTP will instead go via an encrypted HTTPS connection.

- **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**
- **Private 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.

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



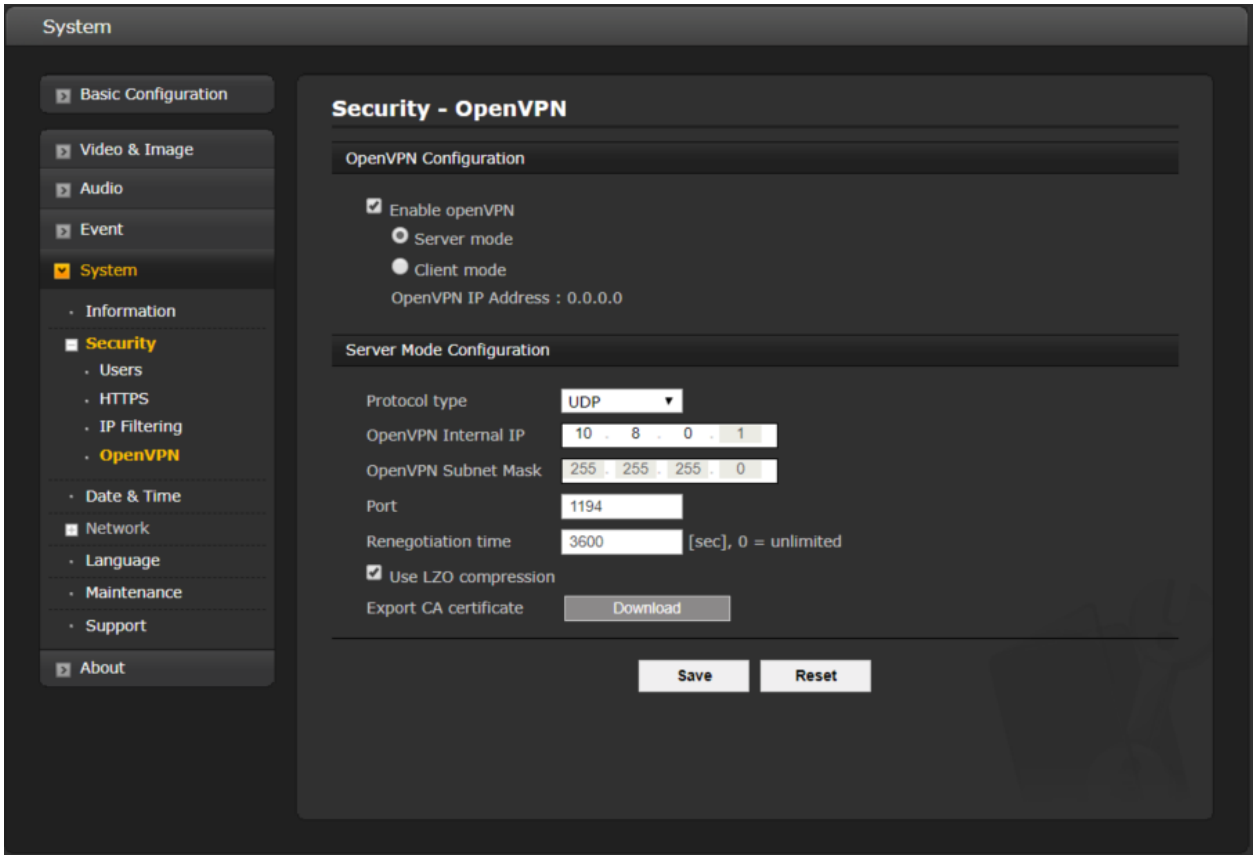
Checking the **Enable IP address filtering** box enables the IP address filtering function. Up to 256 IP address entries may be specified (a single entry can contain multiple IP addresses). Click the **Add** button to add new filtered addresses.

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.

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.

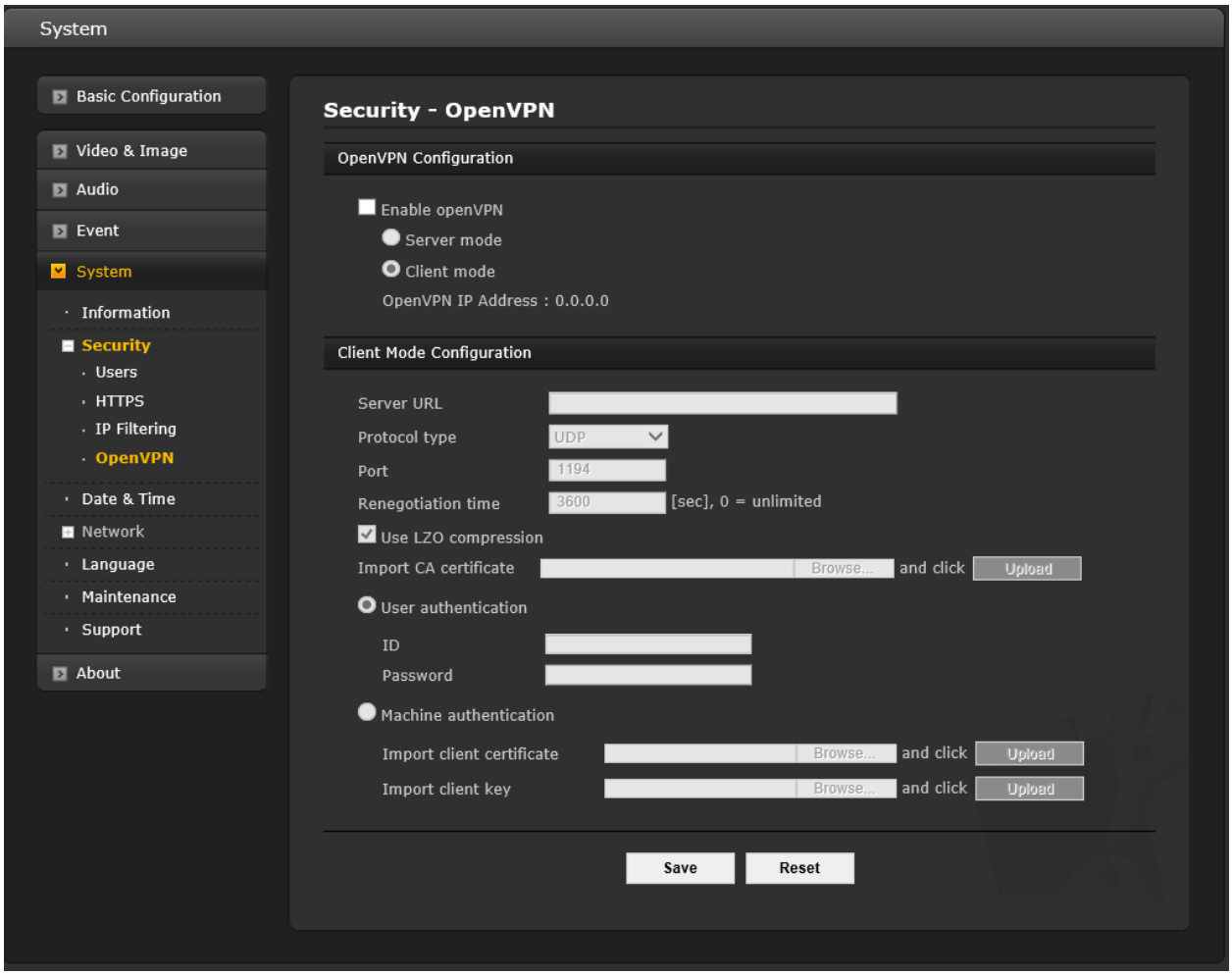
▽ OpenVPN



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. Checking the "Enable openVPN" box activates mode selection buttons. Choose Server mode; the Server Mode Configuration fields appear where so Server Mode Settings can be configured.
2. In Server Mode Configuration, 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; 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; click **Reset** to revert to previously saved settings.

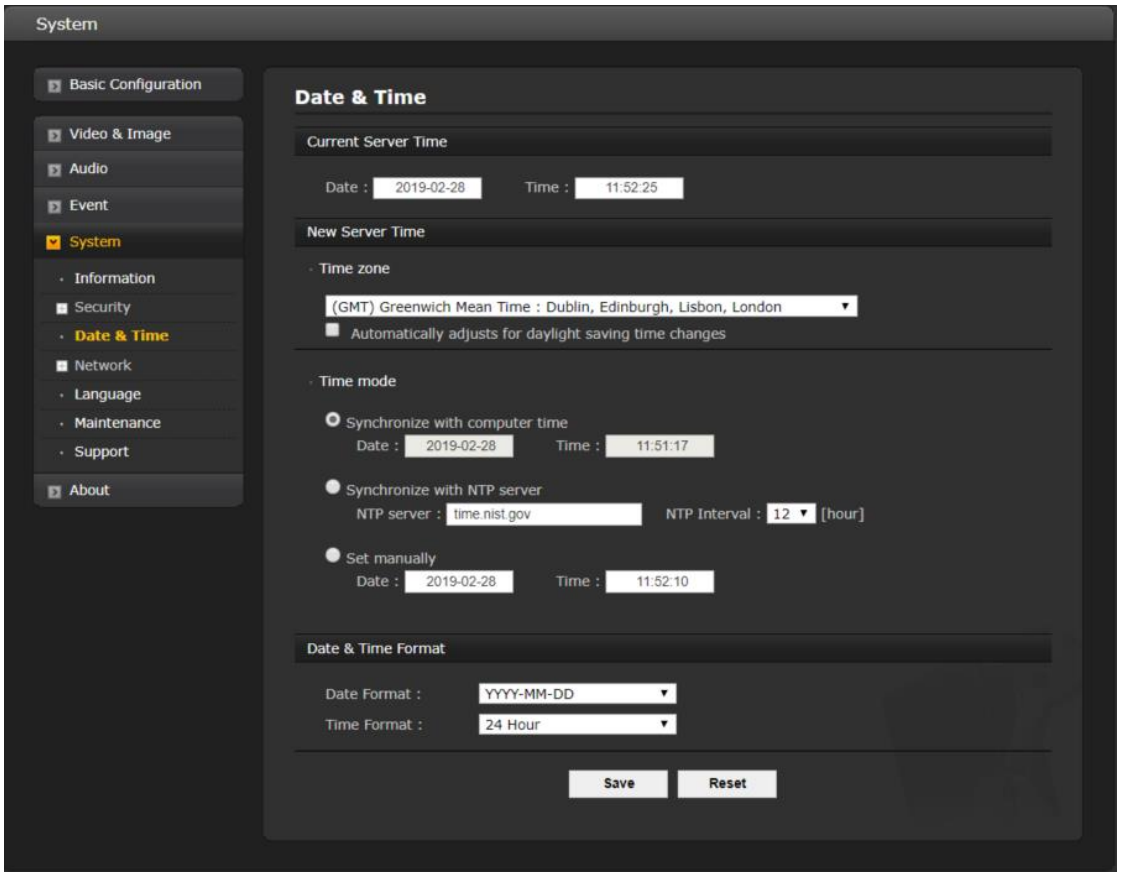


- OpenVPN Client Mode

1. Checking the “Enable openVPN” box activates mode selection buttons. Choose Client mode; the Client Mode Configuration fields appear so Client Mode Settings can be configured.
2. In Client Mode Configuration, 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; 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



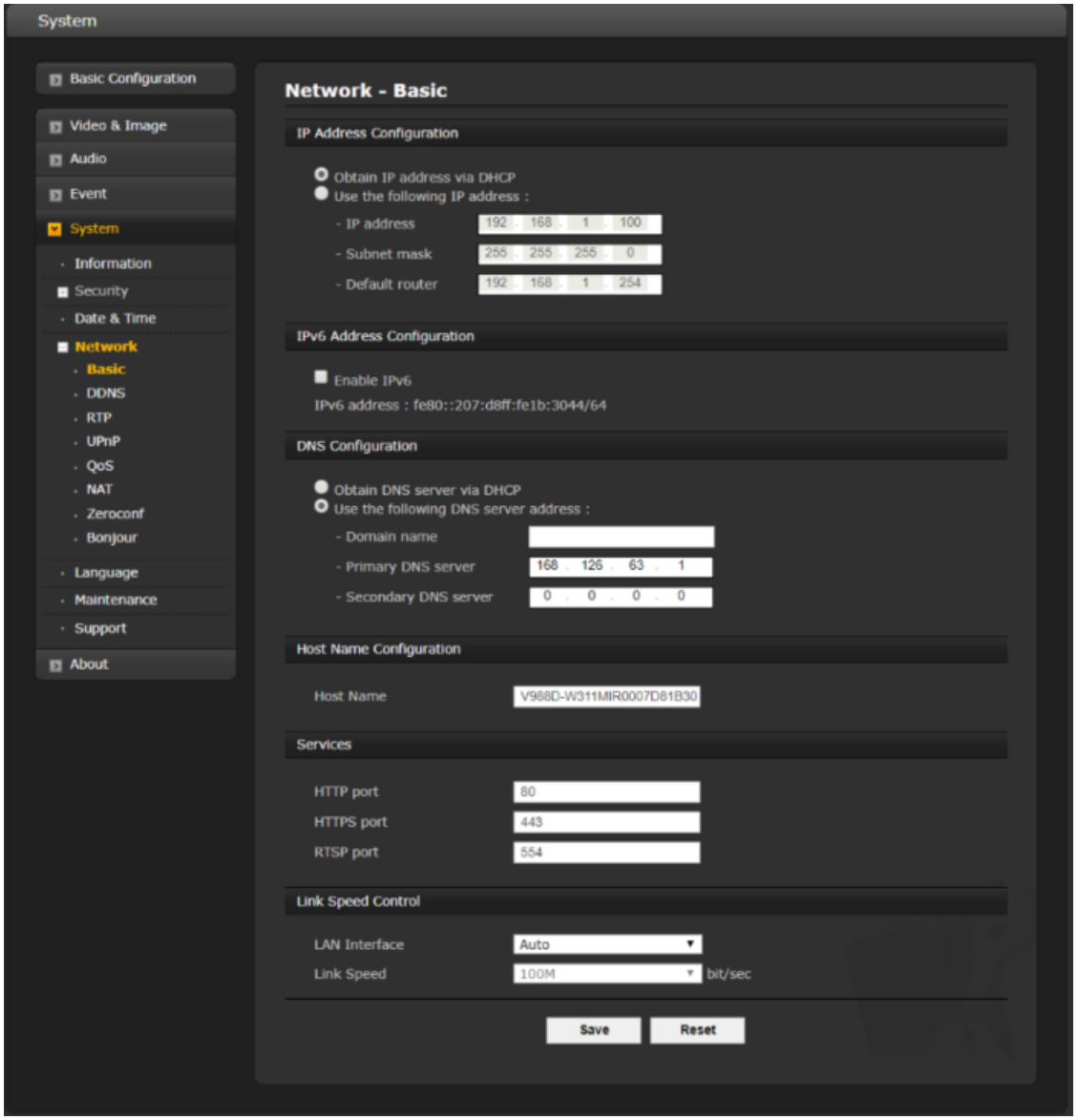
- **Current Server Time**
  This displays the current date and time (24h clock). The time can be displayed in 12h clock format (see below).
- **New Server Time**
  - **Time zone**
    Select your time zone from the drop-down list. If you want the server clock to automatically adjust for daylight savings 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 time 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 the “Enable IPv6” box to enable IPv6. Other settings for IPv6 are configured in the network router.

-

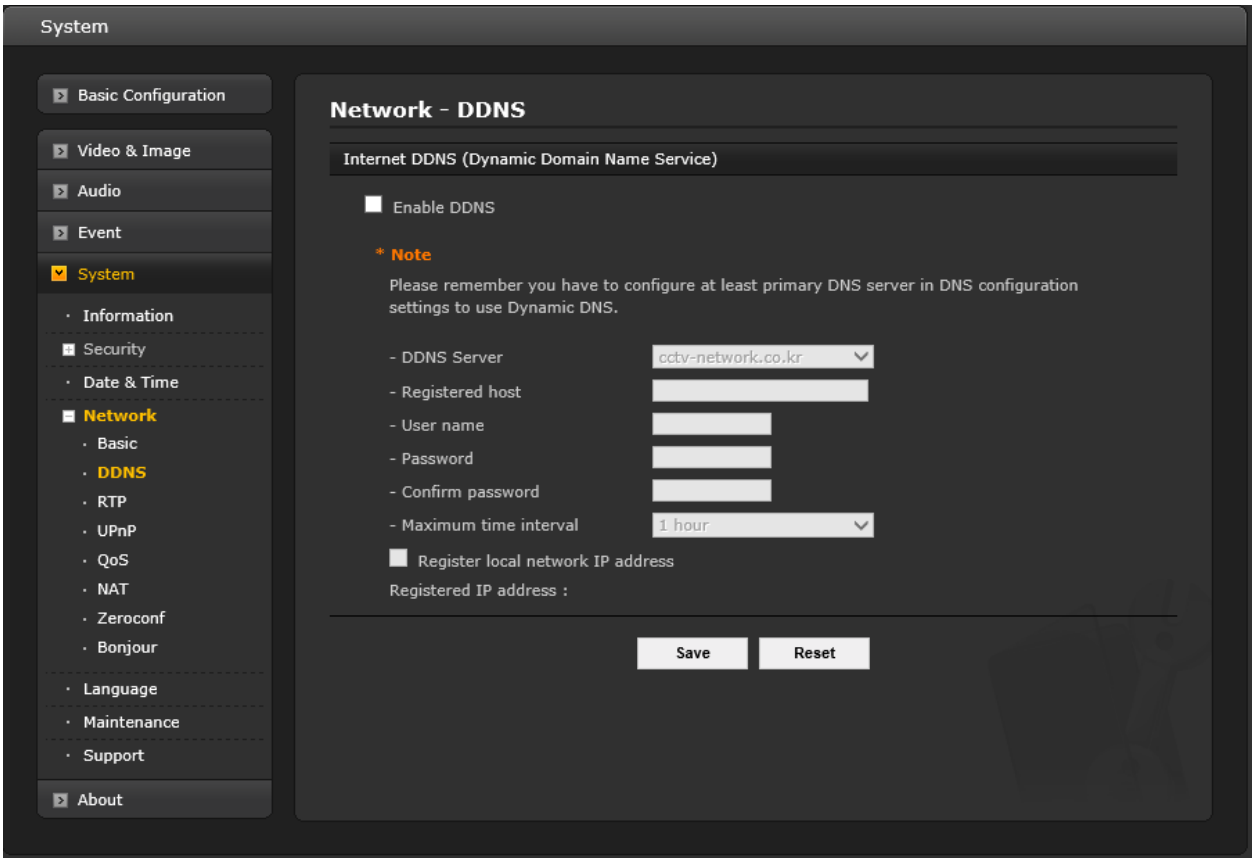
- **DNS Configuration**

  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 specifying 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**
  - **LAN Interface:** Select the transmission method: Auto/Half-Duplex/Full-Duplex.
  - **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



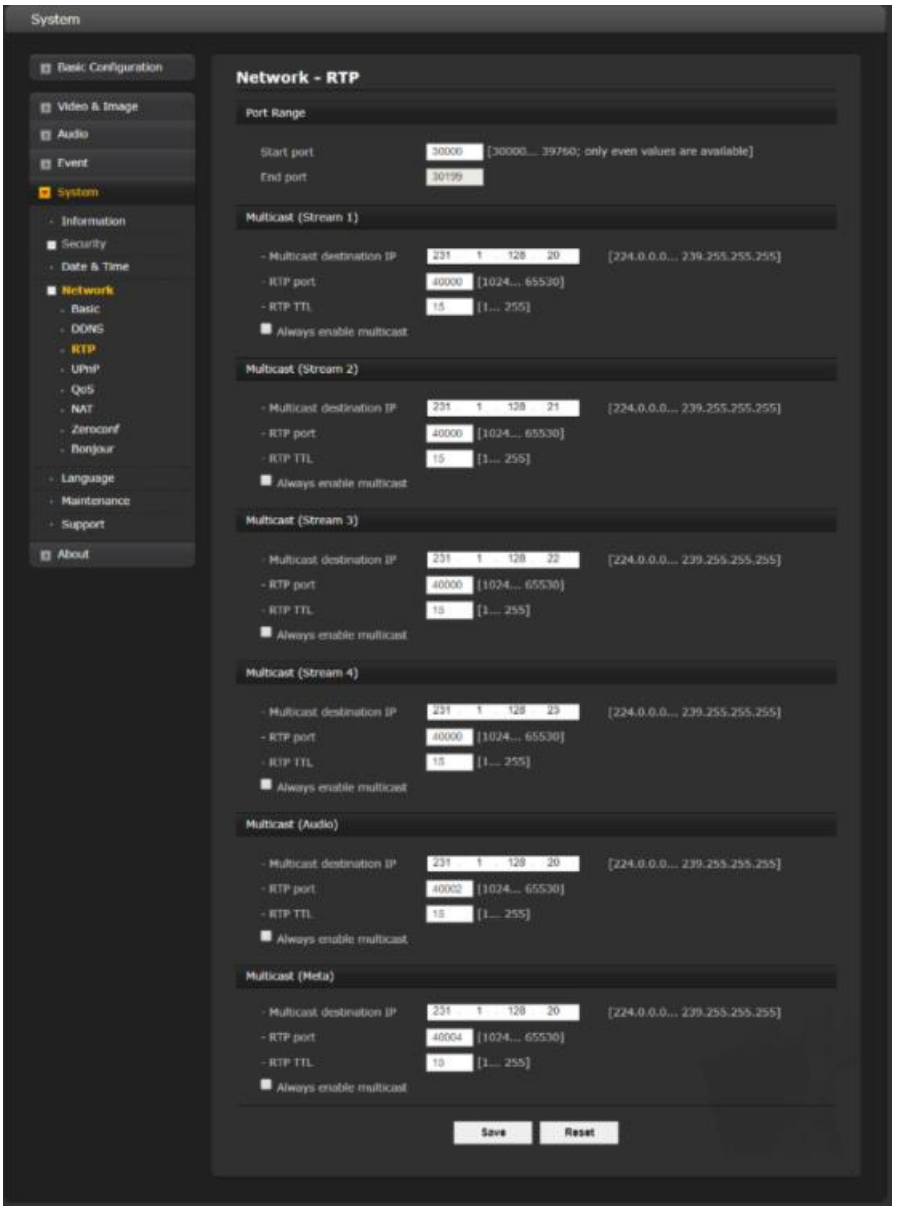
Internet DDNS (Dynamic Domain Name Service)

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



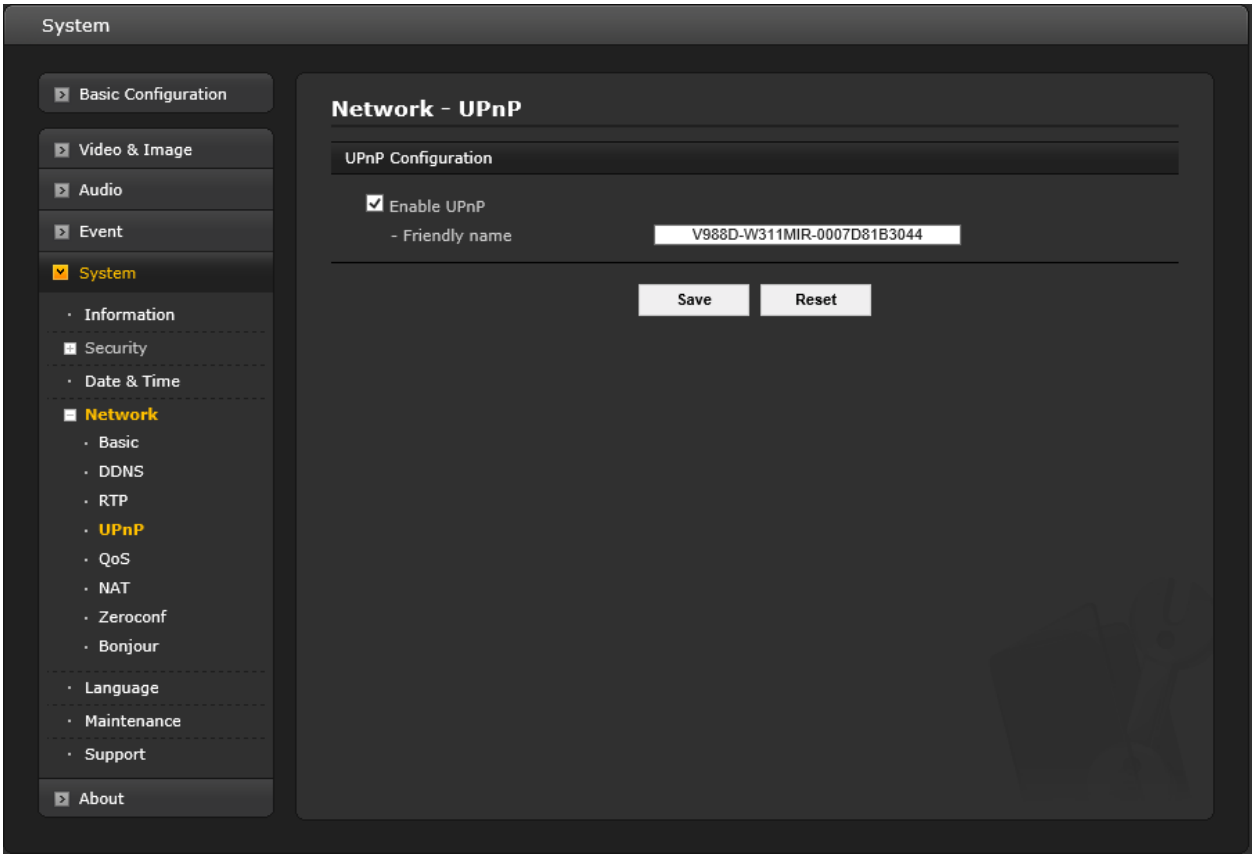
Create a setting for sending and receiving an audio or video on a real-time basis. These settings are the IP address, port number, and Time-To-Live value (TTL) to use for the media stream(s) in multicast H.264 format. Only certain IP addresses and port numbers should be used for multicast streams.

- **Port Range**
  - **Start/End port:** Enter a value between 30000 - 39760
- **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 65530.
  - **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

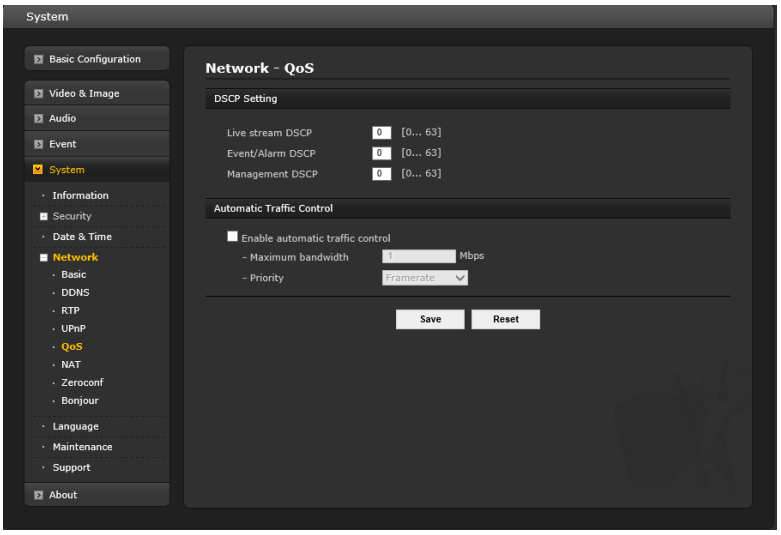


The network camera includes support for UPnP. UPnP is enabled by default, so the network camera is automatically detected by operating systems and clients that support this protocol.

Enter a name in the Friendly name field.

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:

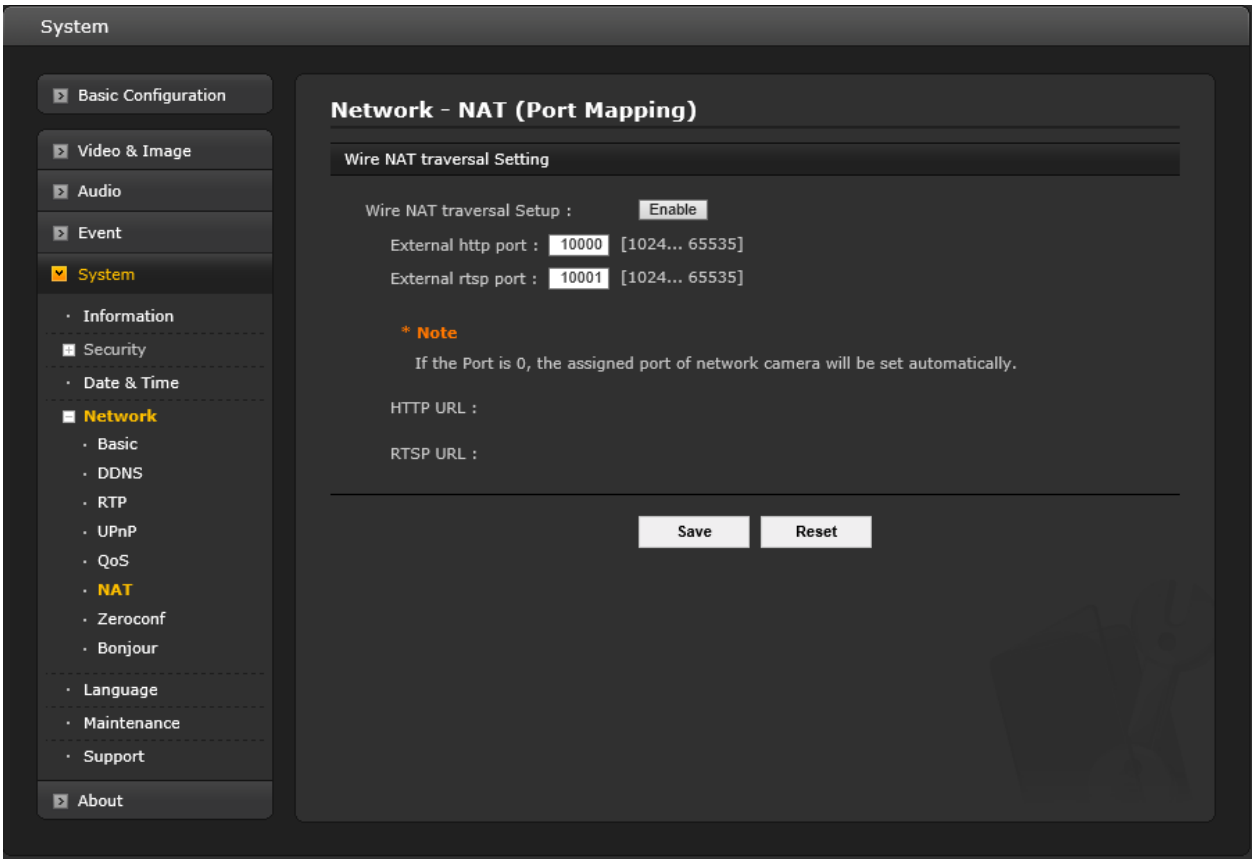
  - **Live Stream DSCP**
  - **Event/Alarm DSCP**
  - **Management DSCP**

- **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.
  - **Priority:** When the maximum bandwidth is exceeded, the data to be reduced is prioritized.

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)



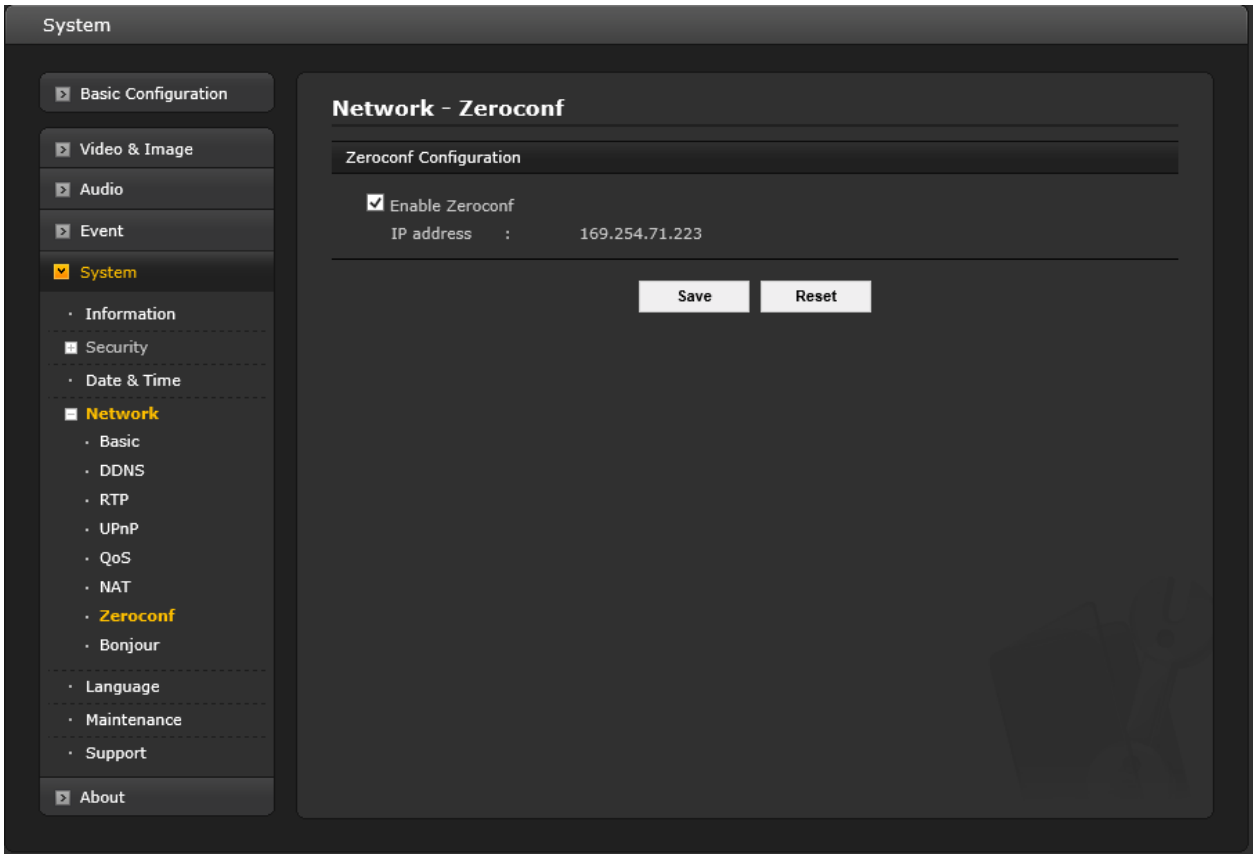
- **Wire NAT traversal Settings**
  - **Enable:** Check this box to enable NAT traversal. When enabled, the network camera attempts to configure port mapping in a NAT router on your network, using UPnP. Note that UPnP must be enabled in the network camera (see System > Network > UPnP).
    - **Automatic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

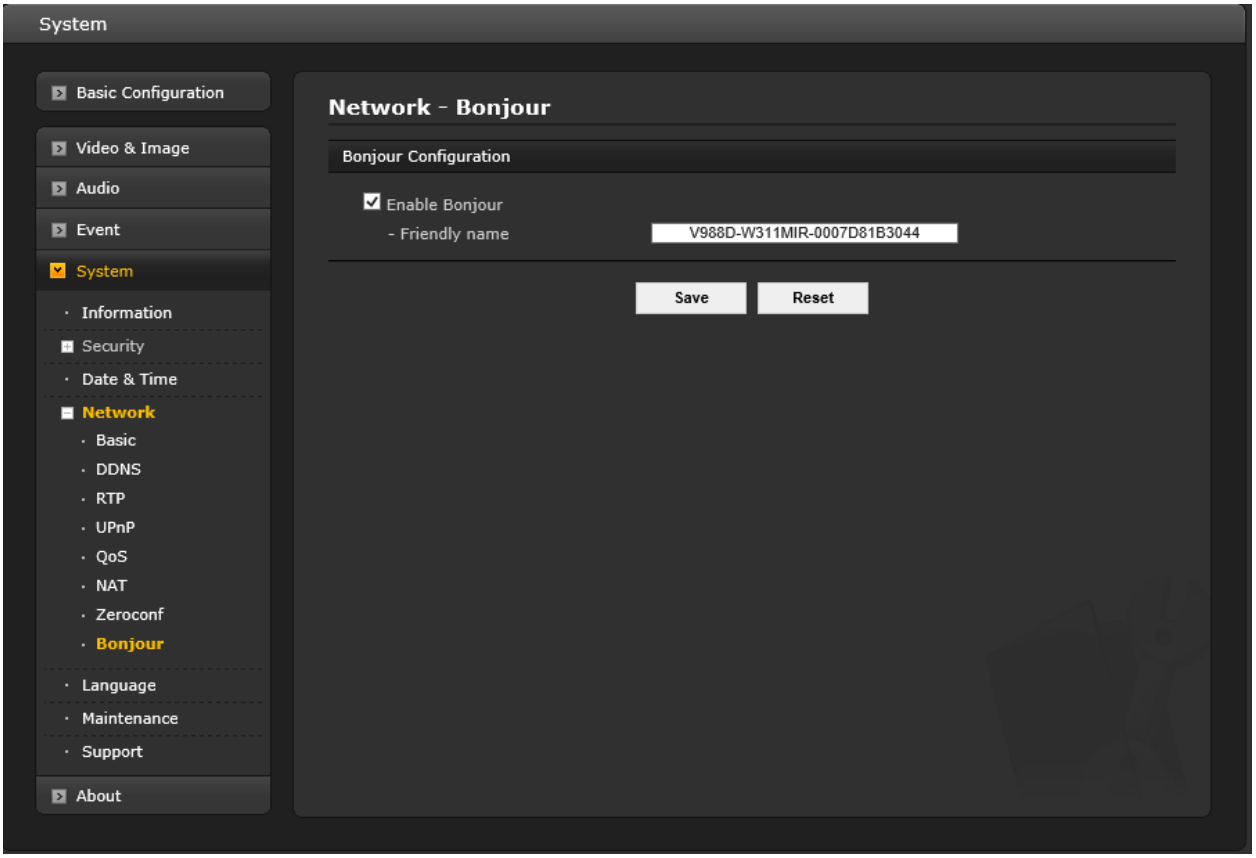
Zeroconf is built on three core technologies:

- 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



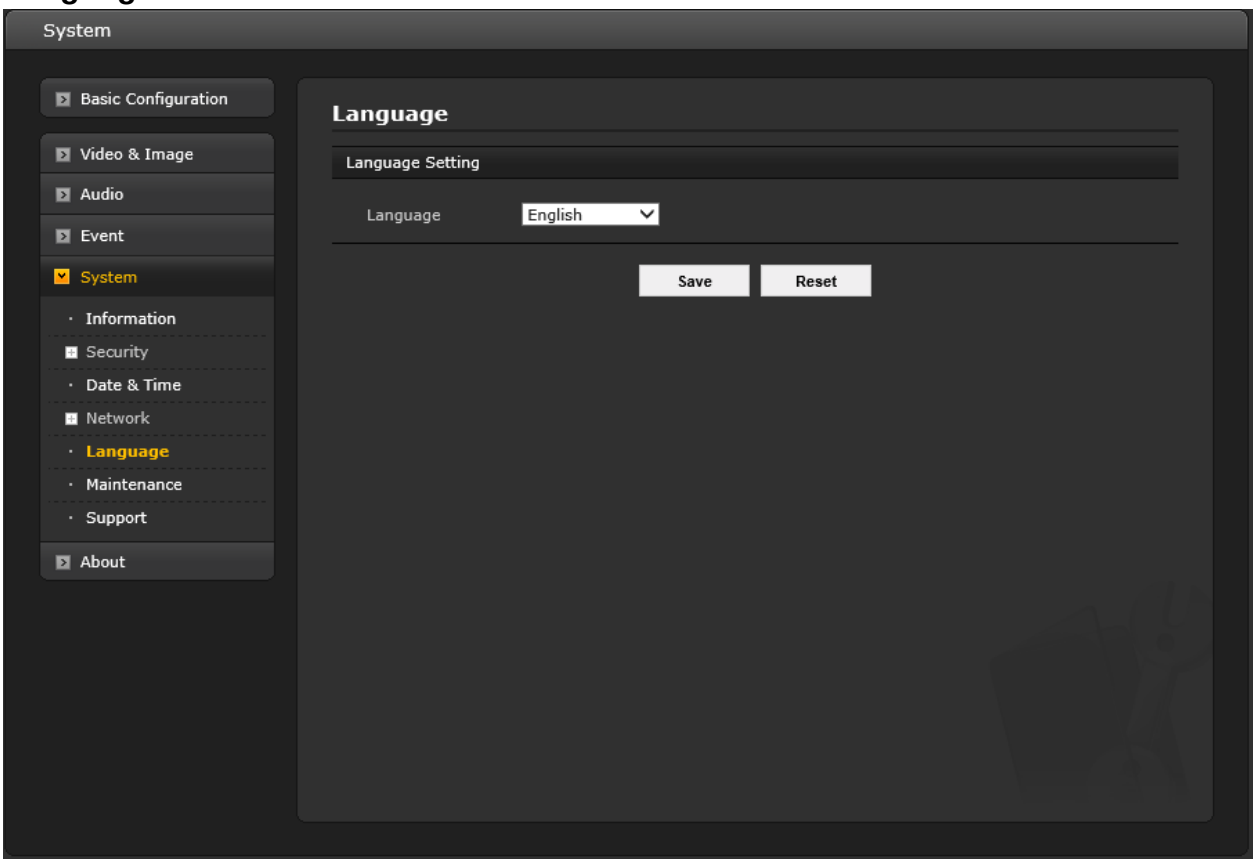
The network camera includes support for Bonjour. When enabled, the network camera is automatically detected by operating systems and clients that support this protocol.

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.

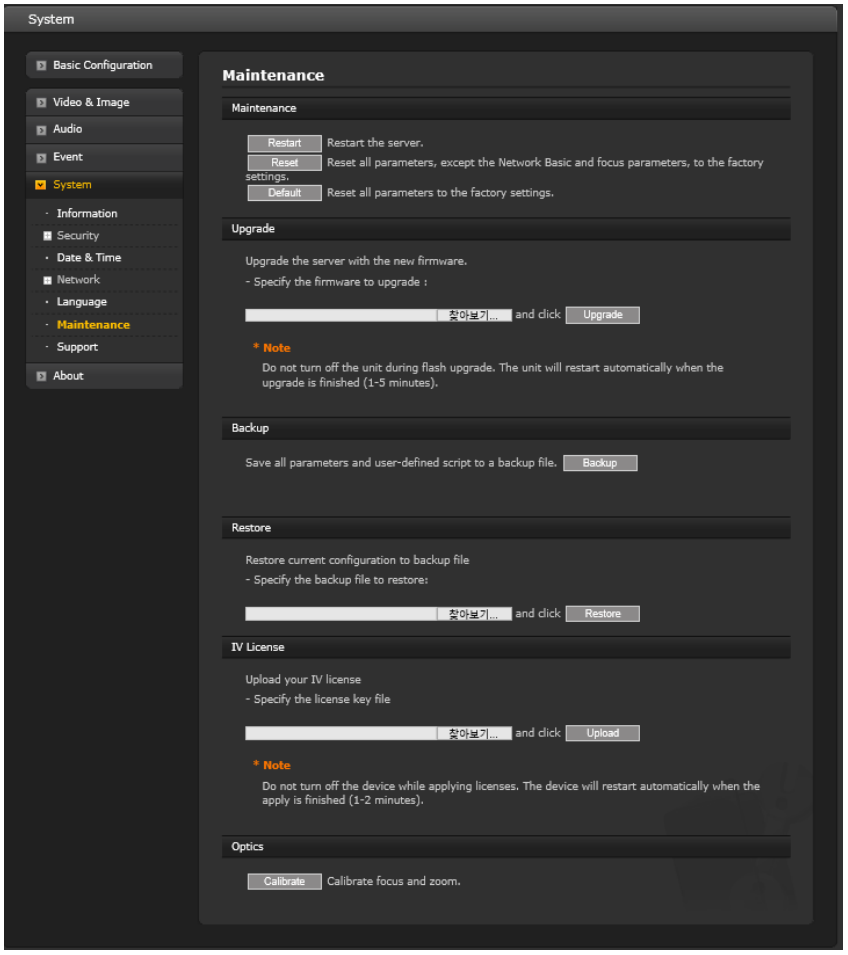
5) Language



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

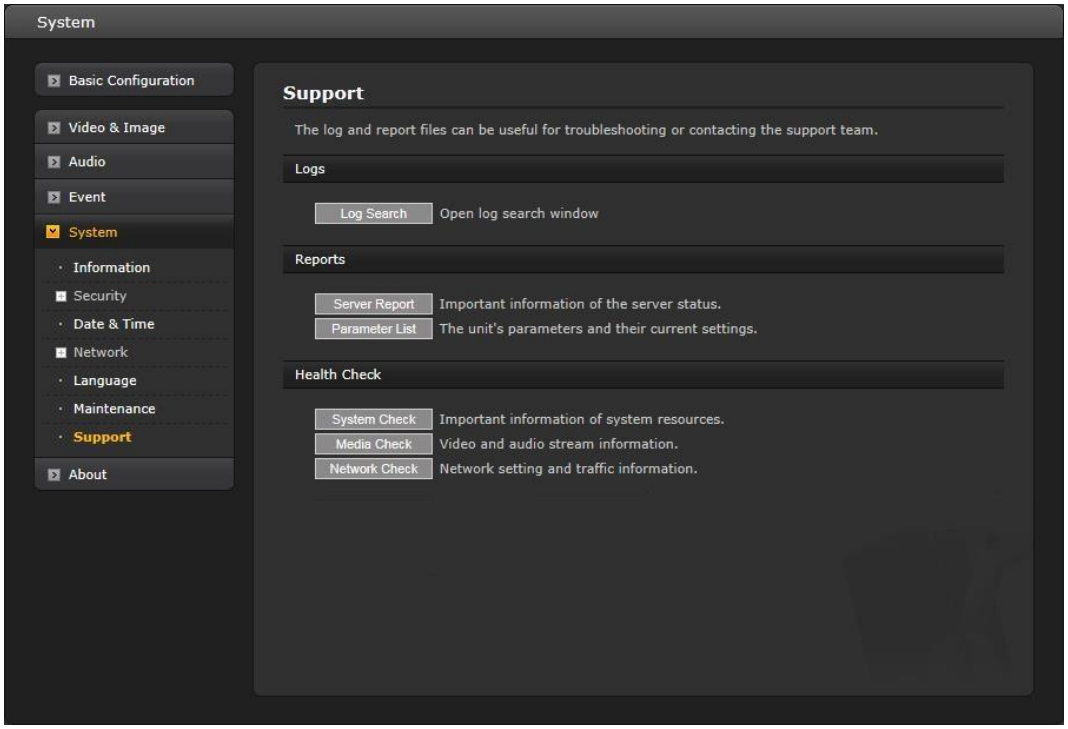


- **Maintenance:**
  - **Restart:** The unit is restarted without changing any of the settings. Use this method if the unit is not behaving as expected.
  - **Reset:** The unit is restarted and most current settings are reset to factory default values. The settings that are not affected are:
    - **the 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.
- **Optics:** Calibrate the zoom and focus of the lens. Once calibrated, zoom and focus will be reset and must be reconfigured.

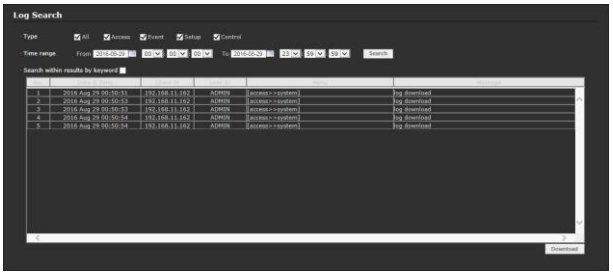
NOTE: Backup and Restore can only be used on the same unit running the same firmware. This feature is not intended for multi-configurations or for firmware upgrades.

7) Support

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



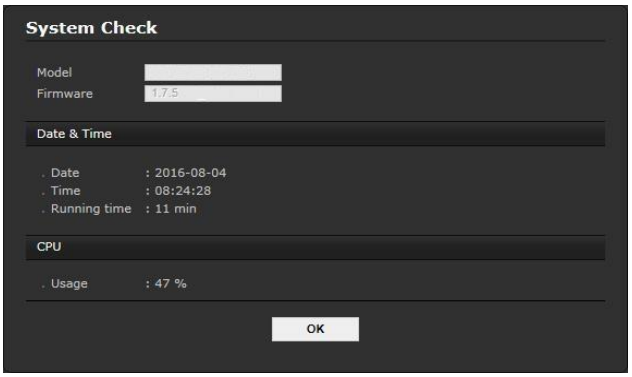
- **Logs:** The network camera supports system and event log information. Click the **Log Search** button to search the Access, Event, Setup or Control log data.



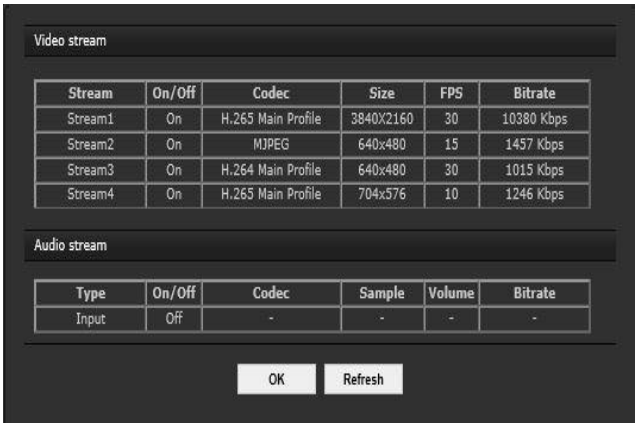
- **Reports:**
  - **Server Report:** Click the **Server Report** button to get the important information about the server's status; this should always be included when requesting support.
  - **Parameter List:** Click the **Parameter List** button to see the unit's parameters and their current settings.

- **Health Check:**

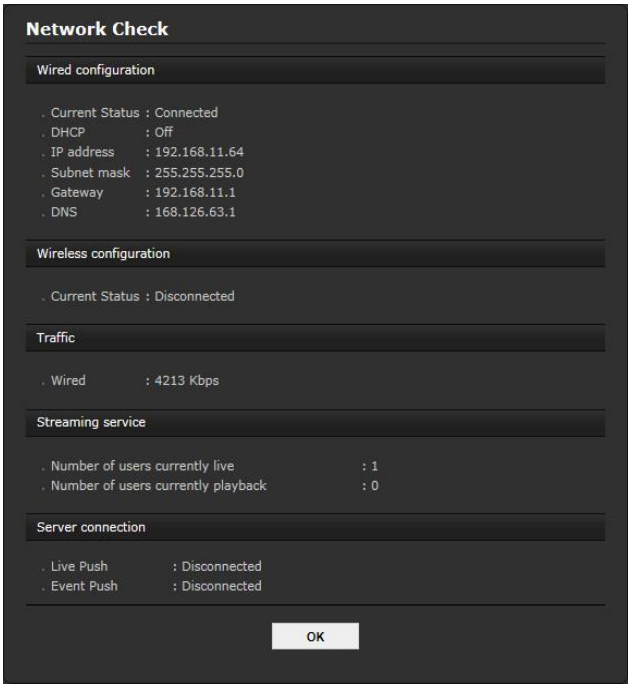
  - **System Check:** Click the **System Check** button to get the important information about the cameras system resources. The pop-up window below displays.



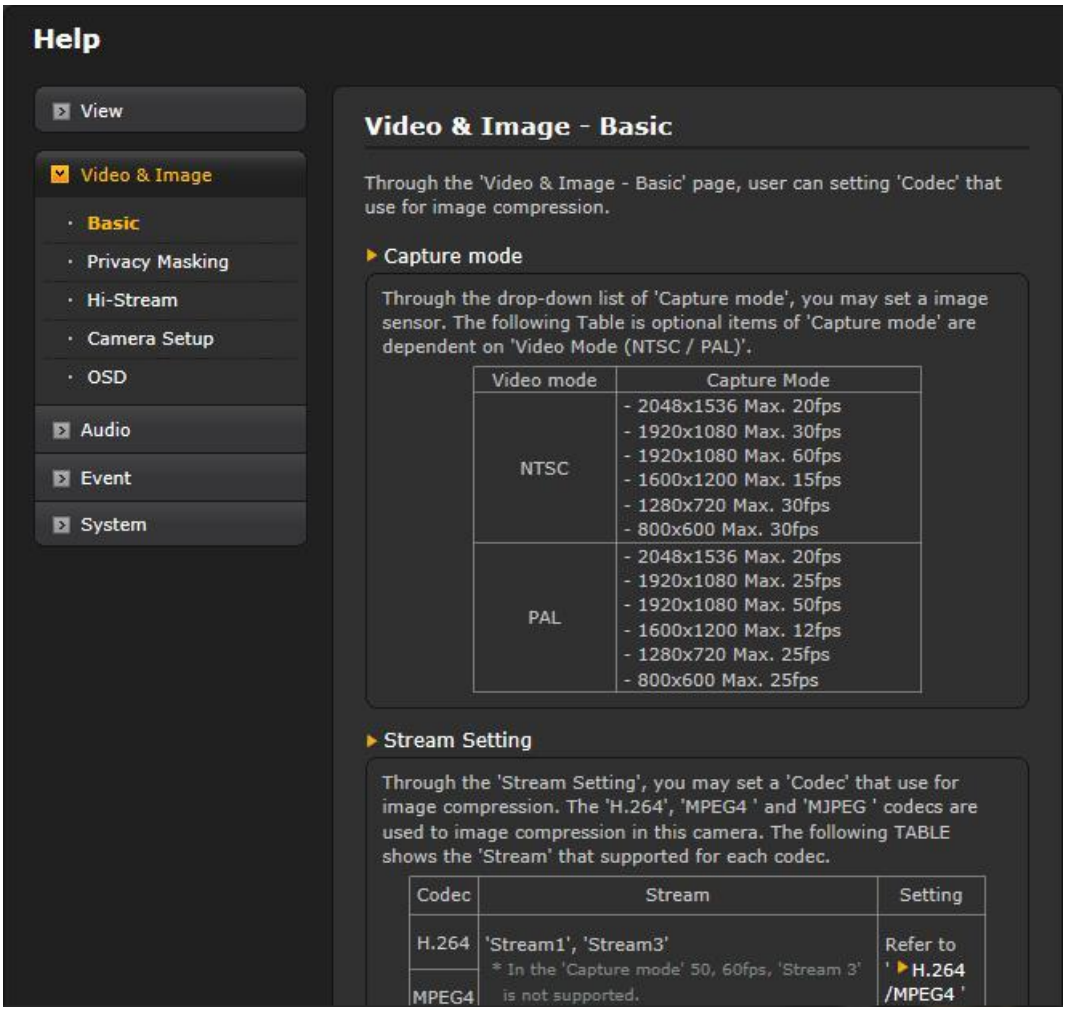
  - **Media Check:** Click the **Media Check** button to get the information about the cameras video and audio stream. The pop-up window below displays.



  - **Network Check:** Click the **Network Check** button to get information about the camera's network settings and traffic. The pop-up window below displays.



3.7 Help



The Help information 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 when there is no access to the user manual.

A Appendix

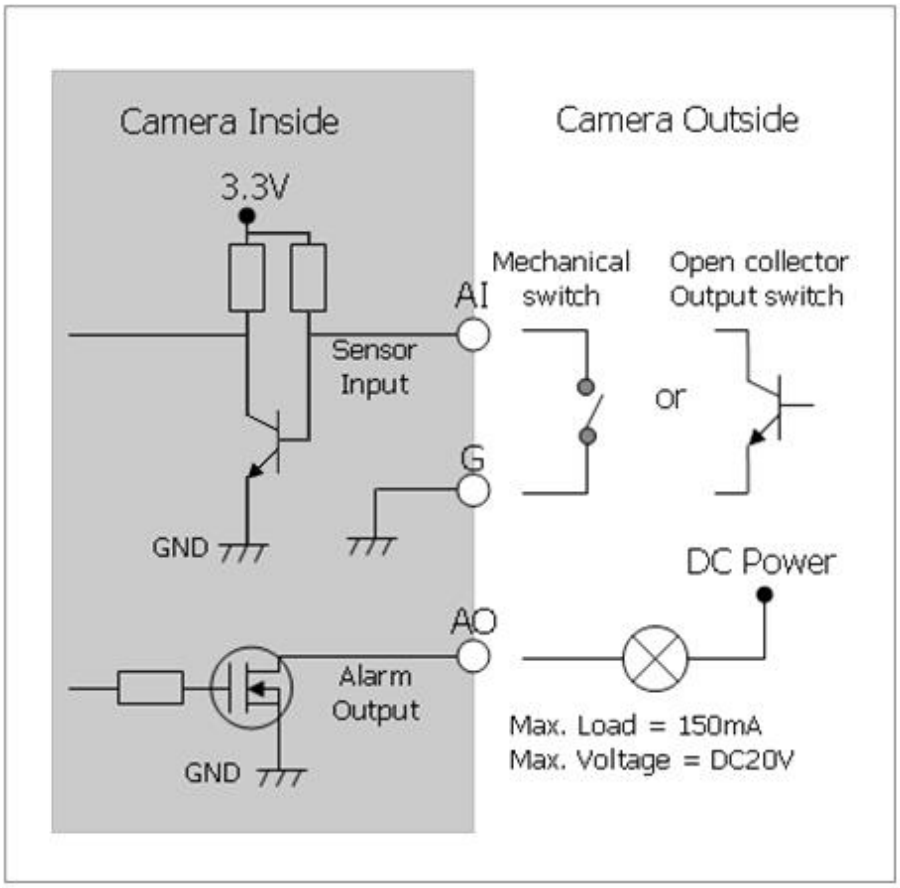
A.1 Troubleshooting

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 or H.265 not displayed in the client.	Check that the correct network interface is selected in the Video & Image/Stream.
Multicast H.264 or 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. Check with your network administrator to see if there is a firewall preventing viewing.
Multicast H.264 or 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 Alarm Connection

The following connection diagram gives an example of how to connect a network camera.



A.3 Preventive Maintenance

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

Every three months, 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.4 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.5 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.6 Product Specification

Model		V988D
Lens		MVF 3.6 ~ 11mm, F1.5, P-Iris
Angle of View		87° ~ 38°(H)
Image Sensor		1/2.5” Sony STARVIS CMOS
Min. Illumination		Color : 0.03Lux @ F1.5 BW : 0Lux @ IR LED On
Scanning Mode		Progressive Scan
Wide Dynamic Range		True WDR
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, Center, Average, Left, Right, Bottom
Image Effect		Flip, Mirror, Defog
Flicker Free Mode		50, 60Hz
Shutter Speed		Auto (1/10,000 ~ 1sec), Manual
IR Illuminator	Quantity	28 IR LEDs
	Distance	Up to 90 ft (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		3840x2160, 3072×2048, 2592x1944/1520, 2560x1440, 1920x1080, 1440x1080, 1280x1024/720, 1024x768, 800x600/480, D1, 640x480, 400x240, CIF
Frame Rate		Max. 25/30fps (NTSC/PAL)
Streaming		Quad Stream (H.264/H.265x3, MJPEGx1)
Audio Compression		G.711
Audio Streaming		2 Way
SYSTEM		
Video Contents Analysis		Tampering, Intelligent Motion, Intrusion Detector
Motion Detection Area		16 Programmable Areas (Include Area 8, Exclude Area 8)
Privacy Mask Zone		8 Programmable Zone
Smart Codec		Hi-Stream
FTP Uploading		MJPEG
Event Notification		E-mail, FTP, Notification Server, XML Notification, Audio Alert
Audio Alert		User-Defined 3 Audio files
Login Authority		Administrator, Operator, Guest
Event Buffering	FTP	Pre: 30 sec, Post: 30 sec
	SD Record	Pre: 10 sec, Post: 60 sec
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
SD Recording Mode	Event, Continuous
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	10 Users
API Support	Open API, ONVIF Compliance
Mobile Support	Android, i-OS
EXTERNAL IN/OUT	
Composite video out	3-Pin Connector
Audio	1 Input, 1 Output (Terminal Block)
Alarm	1 Input, 1 Output (Terminal Block)
Ethernet	RJ-45 (10/100/1000 Base-T)
u-SD Card	SDHC/SDXC
Factory Reset	Tact Switch
ETC.	
Operating Humidity	0 ~ 90% RH (non-condensing)
Operating Temperature	-4° to 122° F (-20°C ~ 50°C)
Power Supply	PoE (IEEE802.3af compliance, Class0), 12VDC
Power Consumption	200mA (9.6W) @PoE, 690mA (8.3W) @12VDC
Dimensions	5.7 in.(144mm) (Φ) x 3.9 in. (99mm) (H)
Net Weight	Approx. 1.7 lb (785g)
Ingress Protection	IP66

※ Specifications are subject to change without notice.

Shipping Instructions

Use the following procedure when returning a unit to the factory:

1. Call or write Vicon for a Return Authorization (R.A.) at one of the locations listed below. Record the name of the Vicon employee who issued the R.A.

   Vicon Industries Inc.
   135 Fell Court
   Hauppauge, NY 11788
   Phone: 631-952-2288; Toll-Free: 1-800-645-9116; Fax: 631-951-2288

   For service or returns from countries in Europe, contact:

   Vicon Industries Ltd
   Unit 4, Nelson Industrial Park,
   Hedge End, Southampton
   SO30 2JH, United Kingdom
   Phone: +44 (0)1489/566300; Fax: +44 (0)1489/566322

2. Attach a sheet of paper to the unit with the following information:
   a. Name and address of the company returning the unit
   b. Name of the Vicon employee who issued the R.A.
   c. R. A. number
   d. Brief description of the installation
   e. Complete description of the problem and circumstances under which it occurs
   f. Unit's original date of purchase, if still under warranty

3. Pack the unit carefully. Use the original shipping carton or its equivalent for maximum protection.
4. Mark the R.A. number on the outside of the carton on the shipping label.

Vicon Standard Equipment Warranty

Vicon Industries Inc. (the "Company") warrants your equipment to be free from defects in material and workmanship under Normal Use from the date of original retail purchase for a period of three years, with the following exceptions:

1. Access Control System Components: Two year from date of original retail purchase.
2. Uninterruptible Power Supplies: Two years from date of original retail purchase.
3. For PTZ cameras, "Normal Use" excludes prolonged use of lens and pan-and-tilt motors, gear heads, and gears due to continuous use of "autopan" or "tour" modes of operation. Such continuous operation is outside the scope of this warranty.
4. Any product sold as "special" or not listed in Vicon's commercial price list: One year from date of original retail purchase.

NOTE:

- If the product is to be used outdoors or in dusty, humid, or other hostile environments, it must be suitably protected.
- Camera products must be protected, whether in use or not, from exposure to direct sunlight or halogen light as the light may damage the camera image sensor. This applies to both indoor and outdoor use of the cameras.
- Failure to comply with any of the aforementioned requirements will invalidate this Limited Hardware Warranty.

Date of retail purchase is the date original end-user takes possession of the equipment, or, at the sole discretion of the Company, the date the equipment first becomes operational by the original end-user.

The sole remedy under this Warranty is that defective equipment be repaired or (at the Company's option) replaced, at Company repair centers, provided the equipment has been authorized for return by the Company, and the return shipment is prepaid in accordance with policy. Repaired or replacement hardware will be warranted for the remainder of the original Warranty Period or ninety (90) days, whichever is longer. When a product or part is exchanged the replacement hardware becomes the property of the original purchaser and all hardware or part thereof that is replaced shall become the property of Vicon.

The warranty does not apply (a) to faulty and improper installation, maintenance, service, repair and/or alteration in any way that is not contemplated in the documentation for the product or carried out with Vicon consent in writing, operation adjustments covered in the operating manual for the product or normal maintenance, (b) to cosmetic damages, (c) if the product is modified or tampered with, (d) if the product is damaged by acts of God, misuse, abuse, negligence, accident, normal wear and tear and deterioration, improper environmental conditions (including, but not limited to, electrical surges, water damage, chemical exposure, an/or heat/cold exposure) or lack of responsible care, (e) if the product has had the model or serial number altered, defaced or removed, (f) to consumables (such as storage media or batteries) (g) to products that have been purchased "as is" and Vicon the seller or the liquidator expressly disclaim their warranty obligation pertaining to the product, (h) to any non-Vicon hardware product or any software (irrespective of packaged or sold with Vicon hardware product) and Vicon products purchased from an unauthorized distributor/reseller, (i) to damage that occurs in shipment or (j) to damages by any other causes not related to defective design, workmanship and/or materials.

The warranty for the products shall run from Vicon to End User customers only (including product purchased through authorized partners and resellers). Vicon is not obligated under any circumstances to honor warranties on product(s) purchases from internet auction sites including eBay, uBid or from any other unauthorized resellers. Except as explicitly provided herein, Vicon disclaims all other warranties, including the implied warranties of fitness for a particular purpose and merchantability.

Software supplied either separately or in hardware is furnished on an "As Is" basis. Vicon does not warrant that such software shall be error (bug) free. Software support via telephone, if provided at no cost, may be discontinued at any time without notice at Vicon's sole discretion. Vicon reserves the right to make changes to its software in any of its products at any time and without notice.

The Warranty and remedies provided above are exclusive and in lieu of all other express or implied warranties including, but not limited to, the implied warranties of merchantability or fitness for a particular purpose. Certain jurisdictions do not allow the exclusion of implied warranties. If laws under such jurisdictions apply, then all express and implied warranties are limited to the warranty period identified above. Unless provided herein, any statements or representations made by any other person or firm are void. Except as provided in this written warranty and to the extent permitted by law, neither Vicon nor any affiliated shall be liable for any loss, (including loss of data and information), inconvenience, or damage, including, but not limited to, direct, special, incidental or consequential damages, resulting from the use or inability to use the Vicon product, whether resulting from breach of warranty or any other legal theory. Notwithstanding the foregoing, Vicon total liability for all claims under this warranty shall not exceed the price paid for the product. These limitations on potential liabilities have been an essential condition in setting the product.

No one is authorized to assume any liability on behalf of the Company, or impose any obligations on it in connection with the sale of any Goods, other than that which is specified above. In no event will the Company be liable for indirect, special, incidental, consequential, or other damages, whether arising from interrupted equipment operation, loss of data, replacement of equipment or software, costs or repairs undertaken by the Purchaser, or other causes.
This warranty applies to all sales made by the Company or its dealers and shall be governed by the laws of New York State without regard to its conflict of laws principles. This Warranty shall be enforceable against the Company only in the courts located in the State of New York.

The form of this Warranty is March 22, 2019.

THE TERMS OF THIS WARRANTY APPLY ONLY TO SALES MADE WHILE THIS WARRANTY IS IN EFFECT. THIS WARRANTY SHALL BE OF NO EFFECT IF AT THE TIME OF SALE A DIFFERENT WARRANTY IS POSTED ON THE COMPANY'S WEBSITE, *WWW.VICON-SECURITY.COM*. IN THAT EVENT, THE TERMS OF THE POSTED WARRANTY SHALL APPLY EXCLUSIVELY.

VICON INDUSTRIES INC.

For office locations, visit the website: www.vicon-security.com