

# User Guide

## V810B Network Outdoor Bullet Camera



XX296-00-00



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.

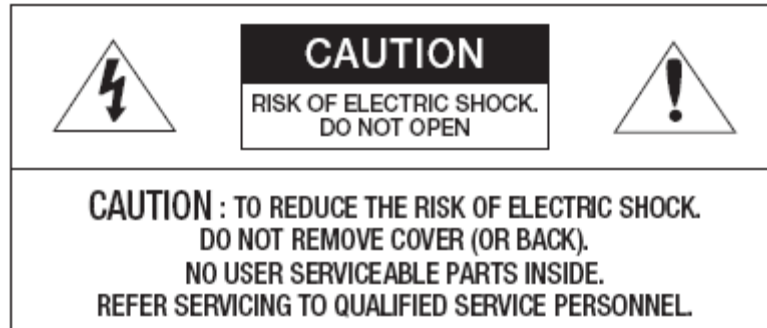
Document Number: 8009-8296-00-00 Product specifications subject to change without notice. Issued: 7/17  
Copyright © 2017 Vicon Industries Inc. All rights reserved.

Vicon Industries Inc.  
Tel: 631-952-2288) Fax: 631-951-2288  
Toll Free: 800-645-9116  
24-Hour Technical Support: 800-34-VICON  
(800-348-4266) UK: 44/(0) 1489-566300  
[www.vicon-security.com](http://www.vicon-security.com)

## WARNING

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

## CAUTION



## EXPLANATION OF GRAPHICAL SYMBOLS



The lightning flash with arrowhead symbol, within an equilateral triangle, is intended to alert the user to the presence of uninsulated "dangerous voltage" within the product's 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 appliance.

## FCC COMPLIANCE STATEMENT

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

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

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

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à 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's 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 is 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 ARE 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

<b>1. Introduction-----</b>	<b>6</b>
1.1 Components - -----	6
1.2 Key Features- -----	7
<b>2. Installation -----</b>	<b>8</b>
2.1 Installation-----	8
2.2 Network Connection and IP Assignment -----	11
<b>3. Operation -----</b>	<b>12</b>
3.1 Access from a browser-----	12
3.2 Access from the internet-----	13
3.3 Setting the admin password over a secure connection-----	13
3.4 Live View Page -----	13
3.5 Network Camera Setup -----	16
3.5.1 Basic Configuration -----	16
3.5.2 Video & Image -----	22
3.5.3 Event -----	29
1) Event-In -----	29
2) Event-Out -----	36
3) Event Map -----	40
3.5.4 System -----	42
1) Information -----	42
2) Security -----	43
3) Date & Time -----	48
4) Network -----	49
5) Language -----	59
6) Maintenance-----	59
7) Support-----	61
3.6 Help-----	63
<b>A. Appendix -----</b>	<b>64</b>
A.1 Troubleshooting -----	64
A.2 Preventive Maintenance -----	65
A.3 System Requirement for Web Browser -----	65
A.4 Product Specification -----	66

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: 8009-8296-00-00 Product specifications subject to change without notice. Issued: 7/17  
Copyright © 2017 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  
(800-348-4266) UK: 44/(0) 1489-566300  
[www.vicon-security.com](http://www.vicon-security.com)

# 1. Introduction

The information in this manual provides installation and setup procedures for the V810B series network bullet cameras. These units should only be installed by a qualified technician using approved materials in conformance with federal, state, and local codes. Read these instructions thoroughly before beginning an installation. Always refer to Vicon's website to assure you have the most up-to-date manual, [www.vicon-security.com](http://www.vicon-security.com).

These camera series are designed for demanding security installations. They offer a number of fixed network camera versions with a variety of resolutions and a choice of fixed or motorized varifocal autoiris lens to fit almost any installation need. The camera includes IR illuminators. These cameras are fully compatible with Vicon Valerus and ViconNet VMS systems.

The cameras support H.264/H.265 compression technology and are designed for easy installation.

## 1.1 Components

This system comes with the following components; Network

Camera	1
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 DC 12V is not supplied.

## 1.2 Key Features

- **Brilliant video quality**

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

- **Wide Dynamic Range**

The network camera provides WDR (Wide Dynamic Range) that improves video exposure quality in scenes with high contrast between bright and dark areas in the video, for example a shady area and a sunny area in the same scene.

- **Dual or Triple Streams**

The network camera can deliver dual or triple video streams simultaneously using H.264, H.265 and MotionJPEG. This means that several video streams can be configured with different compression formats, resolutions and frame rates for different needs.

- **Intelligent video capabilities**

The network camera includes intelligent capabilities such as enhanced video motion detection.

- **Improved Security**

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

- **PoE (Power over Ethernet)**

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

- **ONVIF Certificate**

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

## 2. Installation

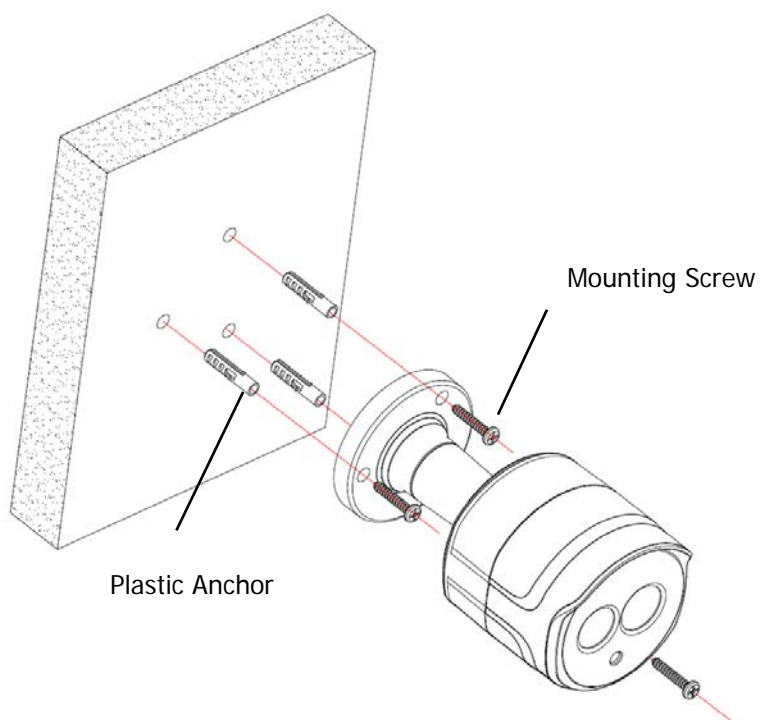
For the network camera to operate, it is necessary to connect a network cable for data transmission and power connection from a power adapter.

### 2.1 Installation

Carefully remove the contents from the box.

#### · Fixed Bullet Camera

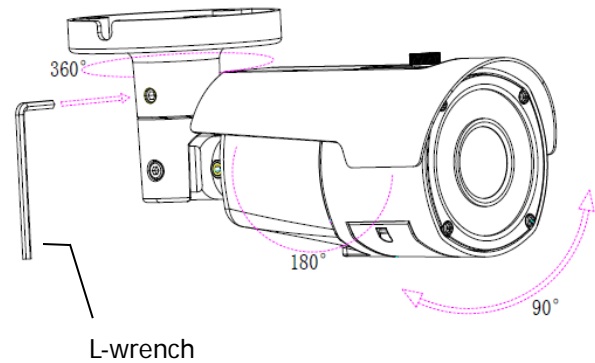
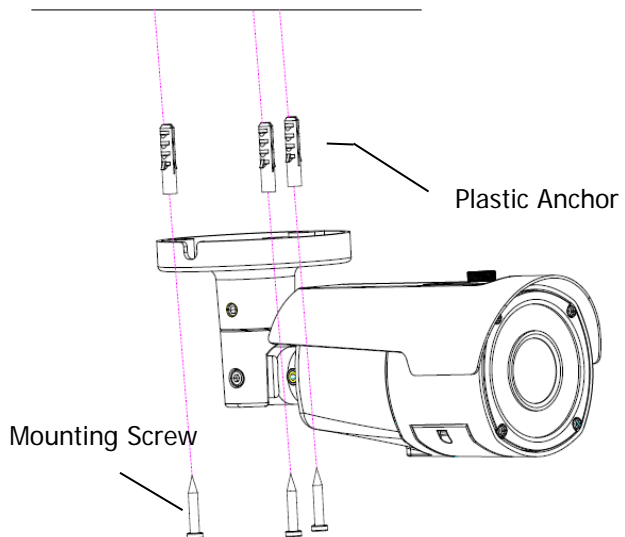
To mount the bullet camera, fix the base of the camera with the three screws provided in the accessory kit.



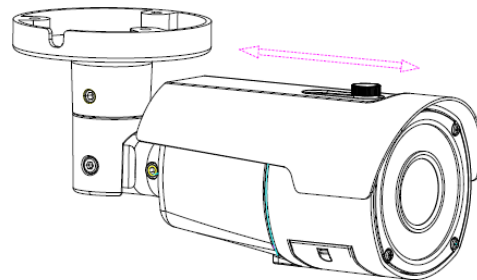
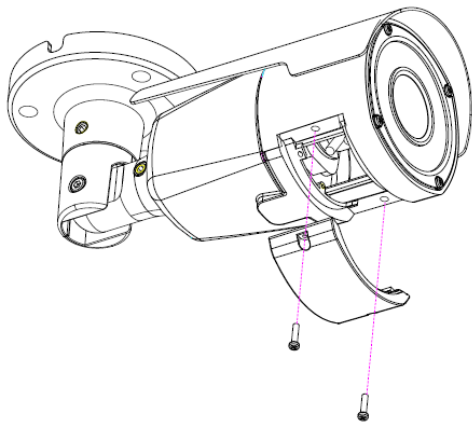


## · MVF Bullet Camera

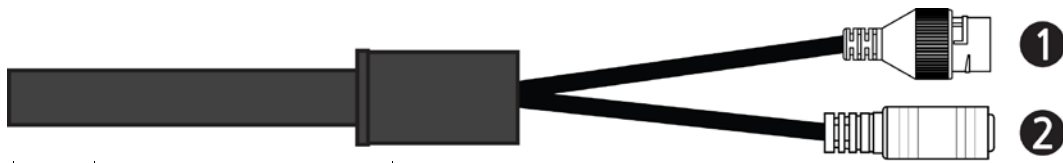
- 1) To mount the bullet camera, fix the base of the camera with the three screws provided in the accessory kit.
- 2) Adjust the camera angle and tighten the mount using the L-wrench.



- 3) Open the lens cover and adjust zoom and focus.
- 4) Adjust sunshield position.



- **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

- **Connecting to the RJ-45**

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

- **Connecting the Power**

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

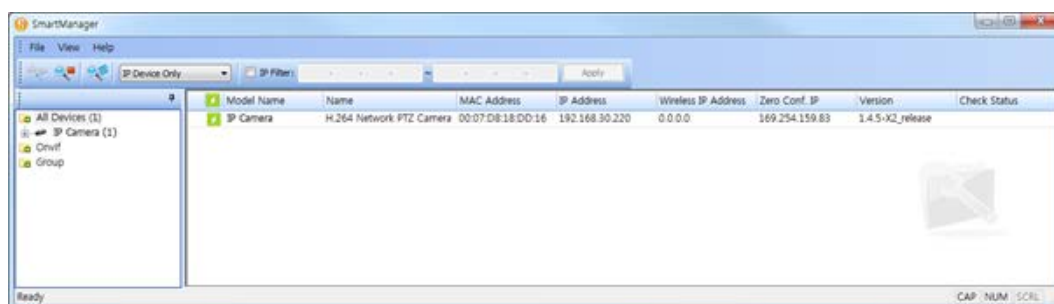
- **Be careful not to reverse the polarity when connecting the power cable.**
- A router featuring PoE (Power over Ethernet) can also be used to supply power to the camera.
- For the power specifications, refer to the Appendix, Product Specification.
- Power for PoE switch must be turned off if using 12 VDC.

## 2.2 Network Connection and IP assignment

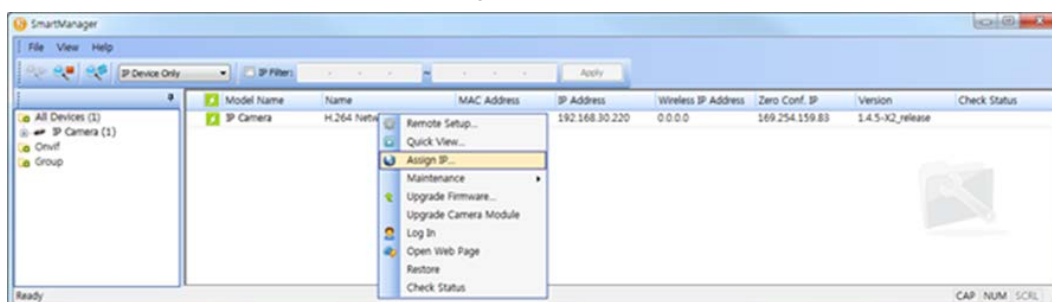
The network camera is designed for use on an Ethernet network and requires an IP address for access. Most networks today have a DHCP server that automatically assigns IP addresses to connected devices. By the factory default, your camera is set to obtain the IP address automatically via DHCP server. 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 on the CD 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.

- 1) Connect the network camera to the network and power up.
- 2) Start SmartManager utility (Start>All Programs>SmartManager>SmartManager); the main window displays. 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 below displays.



- 4) Select Assign IP. The Assign IP window displays. Enter the required IP address.



**Note:** For more information, refer to the Smart Manager User's 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.

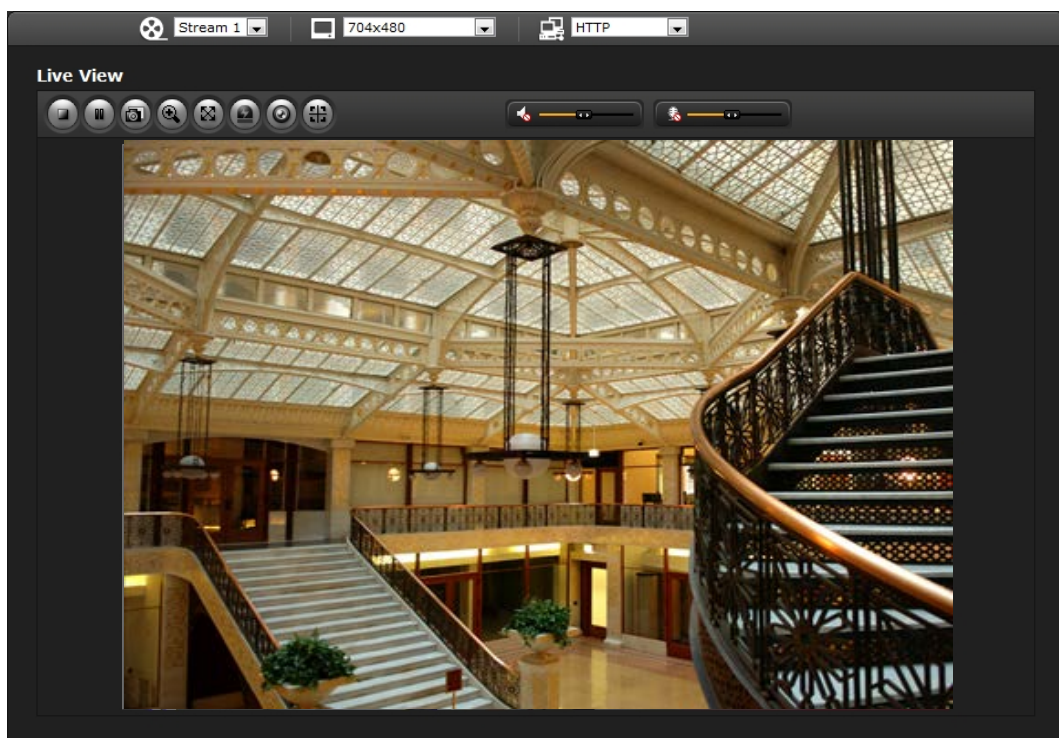
**Note:** Some screens may appear different (i.e., color scheme) depending on the firmware version, but the functionality is the same or similar.

### 3.1 Access from a Browser

- 1) Start a browser (i.e., Internet Explorer).
- 2) Enter the IP address or host name of the network camera in the Location/Address field of the browser.
- 3) A starting page displays. Click Live View, Playback or Setup to select corresponding web page.



- 4) Click Live View for the network camera's **Live View** page to appear in the 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 camera. This is enabled from Setup > System > Network > NAT.

For more information, refer to section “3.5.4 System>Network>NAT” of this manual.

## 3.3 Setting the Admin Password over a Secure Connection

To gain access to the camera, 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 setup the first time. Enter your admin name and password, set by the administrator.

**Note:** The default administrator username is “ADMIN” and password is “1234”. If the password is lost, the network camera must be reset to the factory default settings.



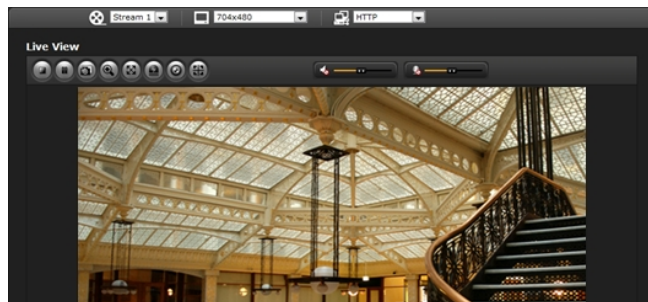
To prevent network eavesdropping when setting the admin password, it can be done via an encrypted HTTPS connection, which requires an HTTPS certificate (see note below).

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 “3.5.4 System > Security > HTTPS”.

**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.



## 1) General controls



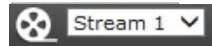
Live View Page



Setup Page

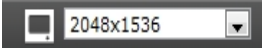


Help Page



Stream 1

The video drop-down list allows the selection of 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, see section "3.5.1 Basic Configuration > Video & Image" of this manual.



2048x1536

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



HTTP

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

## 2) Control toolbar

The live viewer toolbar is available on 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 start playing a video stream.



The Pause button temporarily stops (pauses) the video stream being played.



The Snapshot button takes a picture (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 the 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).




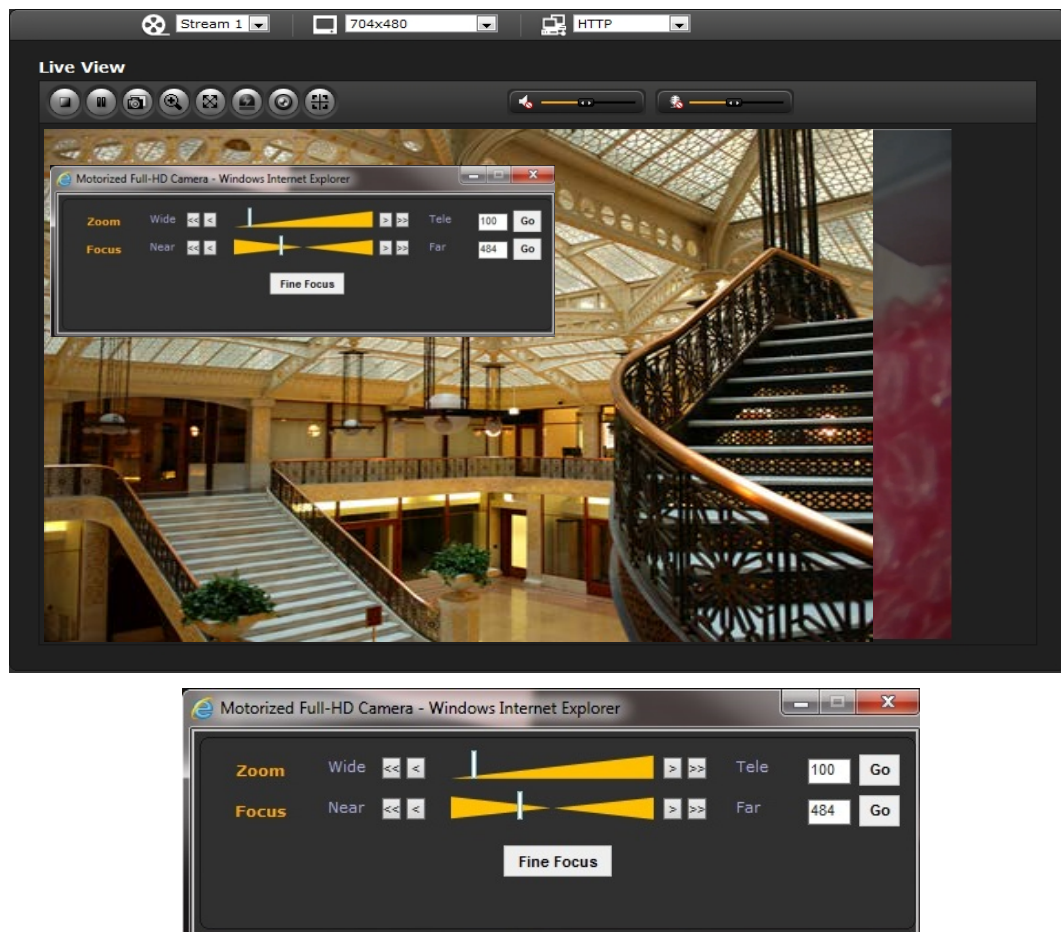
### 3) Video Streams

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


The Live View page of 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.



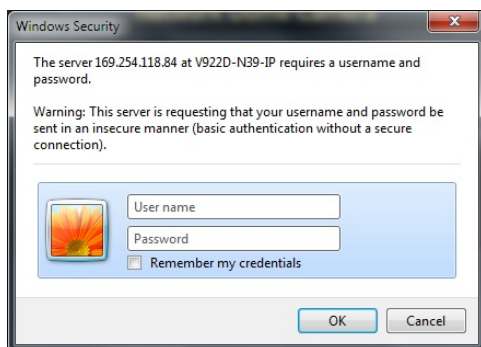
- Adjusting Zoom:  
Click "<" button to zoom out and click ">" button to zoom in. The focus is moved slightly after adjusting zoom; adjust the focus again, as necessary.
- Adjusting Focus:  
Click ">" button for far focus and click "<" button to near focus.
- Fine Focus:  
Click "Fine Focus" to fine tune and readjust focus automatically.

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

## 3.5 Network Camera Setup

This section describes how to configure the network camera and is intended for product Administrators, who have unrestricted access to all the Setup tools, and Operators, who have access to the settings for Basic, Live View, Video & Image, Audio, Event, and System Configuration.

The network camera is configured by clicking Setup in the top right-hand corner of the Live View page. Click on this page to access the online help that explains the setup tools.



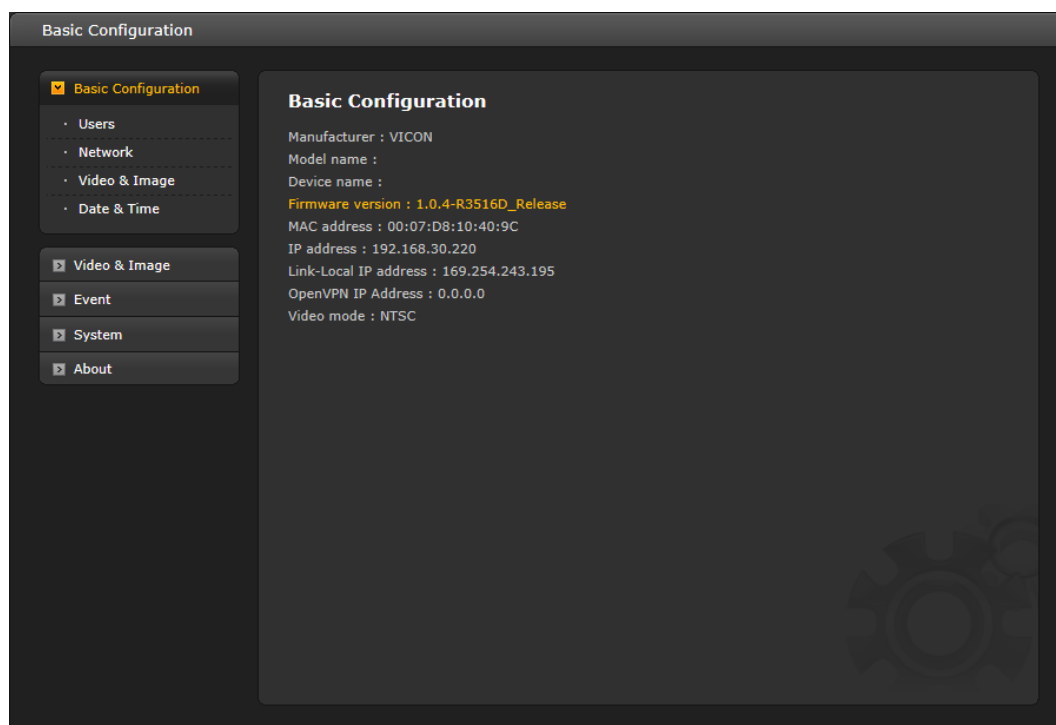
When accessing the network camera for the first time, the "Admin Password" dialog appears. Enter your admin name and password, set by the administrator.

**Note:** If the password is lost, the network camera must be reset to the factory default settings. See Maintenance section for the Factory Default Settings. The default administrator username is "ADMIN" and password is "1234".

**Note:** The configuration screens on your unit may be slightly different, but will be similar in functionality.

### 3.5.1 Basic Configuration

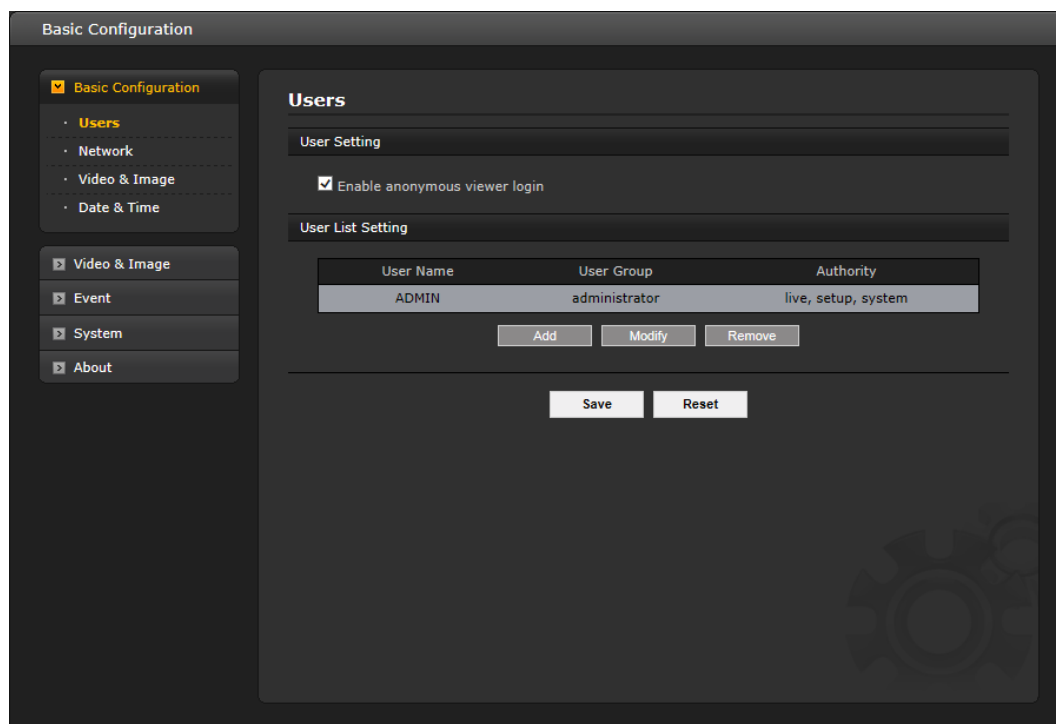
The device information is displayed on this Basic Configuration page.





## 1) Users

User access control is enabled by default. An administrator can create additional users 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):

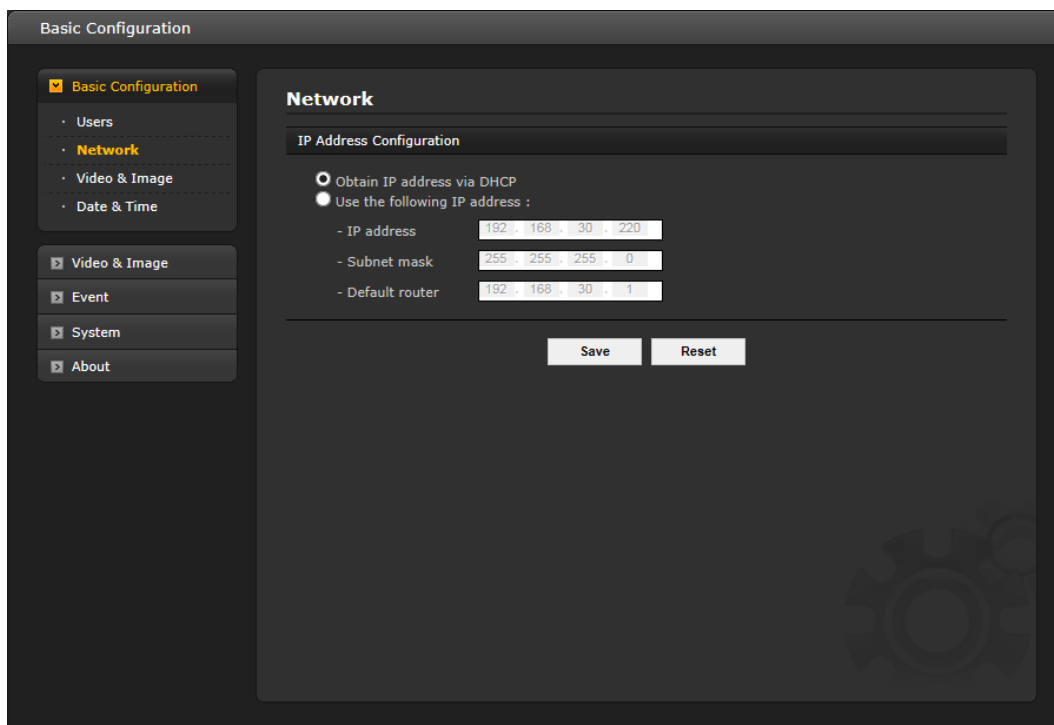
User Group	Authority
Guest	Provides the lowest level of access, which only allows access to the Live View page.
Operator	An operator can view the Live View page, create and modify events, and adjust certain other settings. Operators have no access to System Options.
Administrator	An administrator has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

An administrator can Add, Modify or Remove users in the list by clicking the appropriate button. Click Save to save the settings or Reset to cancel.

- **Enable anonymous viewer login:** Check the box to use the webcasting features. Refer to "3.5.3 Video & Image" for more details.

## 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 address according to the configuration in the network router. There is also the option of using the Internet Dynamic DNS Service. For more information on setting the network, refer to Setup> System>Security>Network.



The screenshot shows the 'Basic Configuration' window with the 'Network' tab selected. Under 'IP Address Configuration', the 'Obtain IP address via DHCP' radio button is selected. Below this, there are three rows of input fields for static IP configuration: 'IP address' (192.168.30.220), 'Subnet mask' (255.255.255.0), and 'Default router' (192.168.30.1). At the bottom right are 'Save' and 'Reset' buttons. A sidebar on the left contains links to 'Basic Configuration', 'Users', 'Network', 'Video & Image', 'Date & Time', 'Video & Image', 'Event', 'System', and 'About'.

- **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 where the network camera is located.
  - **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 the unit cannot be accessed, 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.

### 3) Video & Image

The screenshot displays the 'Basic Configuration' window with the 'Video & Image' tab selected. The left sidebar shows a navigation menu with 'Basic Configuration' (checked), 'Users', 'Network', 'Video & Image' (highlighted), 'Event', 'System', and 'About'. The main content area is titled 'Video & Image' and contains four sections: 'Sensor Setting', 'Stream 1 Setting', 'Stream 2 Setting', and 'Stream 3 Setting'. 'Sensor Setting' has a 'Capture mode' dropdown set to '1920x1080,30fps,NTSC'. 'Stream 1 Setting' includes 'Codec type' (radio buttons for H.264 and H.265, with H.264 selected), 'Codec' (dropdown set to 'H.264 Main Profile'), 'Resolution' (dropdown set to '1920x1080'), 'Bitrate control' (radio buttons for CBR and CVBR, with CBR selected), 'Bitrate' (dropdown set to '4000' with '[Kbps]' next to it), 'Framerate' (dropdown set to '30'), and 'GOP size' (input field set to '30' with '[1 ...60]' next to it). 'Stream 2 Setting' includes 'Codec' (dropdown set to 'MJPEG'), 'Resolution' (dropdown set to '1280x720'), 'Framerate' (dropdown set to '15'), and 'Quality' (a slider set to '80' with '[1 ...100]' next to it). 'Stream 3 Setting' includes 'Codec type' (radio buttons for H.264 and H.265, with H.264 selected), 'Codec' (dropdown set to 'H.264 Baseline Profile'), 'Resolution' (dropdown set to '640x480'), 'Bitrate control' (radio buttons for CBR and CVBR, with CBR selected), 'Bitrate' (dropdown set to '1000' with '[Kbps]' next to it), 'Framerate' (dropdown set to '30'), and 'GOP size' (input field set to '30' with '[1 ...60]' next to it). At the bottom right of the settings area are 'Save' and 'Reset' buttons.

- **Sensor Setting:**

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

- **Stream1 Setting**

- **Codec type:** The codec supported in Stream 1 is H.264 or H.265.
- **Codec:** There are 3 pre-programmed stream profiles available for quick set-up. Choose the form of video encoding to use from the drop-down list:
  - \* **H.264 High Profile:**  
The 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:**  
Primarily for low-cost applications that require additional error robustness, this profile is used rarely in video-conferencing 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:**

Resolution enables users to determine a basic screen size when having access through the Web Browser or PC program. The screen size control provides several modes, such as like 2592x1520, 2304x1296, 1920x1080, 1440x1080, 1280x1024, 1280x720, 1024x768, 704x480(576), 640x480, 400x240, and 320x240. Users can reset the selected screen size anytime while monitoring the screen on a real-time basis.

- **Bitrate control:**

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

\* **CBR:** Constant bitrate.

\* **CVBR:** VBR with maximum bitrate which is set in Bitrate.

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

- **Frame rate:**

Upon real-time play, users should select a frame refresh rate per second. If the rate is high, the image will become smooth; 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 fast image one after the other, decrease this value. For general monitoring purposes, do not change a basic value; this may cause a problem to the system performance. Vicon recommends that GOP be the same as the fps.

• **Stream2 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 stream1 setting.

- **MJPEG frame rate:** Same as the stream1 setting.

- **JPEG quality:** Select the picture quality. If users want to have a high quality fast image one after the other, decrease the value. For general monitoring purposes, do not change a basic value. Such act may cause a problem to the system performance.

• **Stream3 Setting:** Same as the Stream1 settings.

When the settings are complete, click **Save**, or click **Reset** to revert to previously saved settings.

## 4) Date & Time

Basic Configuration

- Basic Configuration
- Users
- Network
- Video & Image
- Date & Time**
- Video & Image
- Event
- System
- About

### Date & Time

**Current Server Time**

Date : 2017-05-17 Time : 08:00:01

**New Server Time**

**Time zone**

(GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London

☐ Automatically adjusts for daylight saving time changes

**Time mode**

☒ Synchronize with computer time  
Date : 2017-05-17 Time : 16:59:59

☐ Synchronize with NTP server  
NTP server : time.nist.gov NTP Interval : 12 [hour]

☐ Set manually  
Date : 2017-05-17 Time : 07:59:52

**Date & Time Format**

Date Format : YYYY-MM-DD

Time Format : 24 Hour

Save Reset

- **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 saving time, check the box "Automatically adjust for daylight saving time changes".

From the **Time Mode** section, select the preferred method to use for setting the time:

- **Synchronize with computer time:** Sets the time from the clock on your computer.
- **Synchronize with NTP Server:** The network camera will obtain the time from an NTP server every 60 minutes.
- **Set manually:** Allows you to manually set the time and date.

- **Date & Time Format**

Specify the formats for the date and time (12h or 24h) displayed in the video streams. Select Date & Time format from the drop-down list.

- **Date Format:** Specify the date format. YYYY: Year, MM: Month, DD: Day
- **Time Format:** Specify the date format. 24 Hours or 12 Hours

When the settings are complete, click **Save**, or click **Reset** to revert to previously saved settings.

## 3.5.2 Video & Image

### ▼ Basic

The screenshot displays the 'Video & Image' configuration window, specifically the 'Basic' tab. On the left, a sidebar lists navigation options: 'Basic Configuration', 'Video & Image' (selected), 'Basic' (sub-tab), 'Privacy Masking', 'Hi-Stream', 'Camera Setup', 'OSD', 'Event', 'System', and 'About'. The main panel is titled 'Video & Image - Basic' and contains three sections: 'Sensor Setting', 'Stream 1 Setting', and 'Stream 2 Setting' (Stream 3 is partially visible). 'Sensor Setting' shows 'Capture mode' as '1920x1080,30fps,NTSC'. 'Stream 1 Setting' includes 'Codec type' (H264 selected), 'Codec' (H.264 Main Profile), 'Resolution' (1920x1080), 'Bitrate control' (CBR selected), 'Bitrate' (4000 Kbps), 'Framerate' (30), and 'GOP size' (30). 'Stream 2 Setting' includes 'Codec' (MJPEG), 'Resolution' (1280x720), 'Framerate' (15), and 'Quality' (80). 'Stream 3 Setting' includes 'Codec type' (H264 selected), 'Codec' (H.264 Baseline Profile), 'Resolution' (640x480), 'Bitrate control' (CBR selected), 'Bitrate' (1000 Kbps), 'Framerate' (30), and 'GOP size' (30). 'Save' and 'Reset' buttons are at the bottom right.

Video & Image

Basic Configuration

Video & Image

- Basic
- Privacy Masking
- Hi-Stream
- Camera Setup
- OSD

Event

System

About

### Video & Image - Basic

#### Sensor Setting

Capture mode: 1920x1080,30fps,NTSC

#### Stream 1 Setting

Codec type: ☒ H264 ☐ H265

Codec: H.264 Main Profile

Resolution: 1920x1080

Bitrate control: ☒ CBR ☐ CVBR

Bitrate: 4000 [Kbps]

Framerate: 30

GOP size: 30 [1 ...60]

#### Stream 2 Setting

Codec: MJPEG

Resolution: 1280x720

Framerate: 15

Quality: 80 [1 ...100]

#### Stream 3 Setting

Codec type: ☒ H264 ☐ H265

Codec: H.264 Baseline Profile

Resolution: 640x480

Bitrate control: ☒ CBR ☐ CVBR

Bitrate: 1000 [Kbps]

Framerate: 30

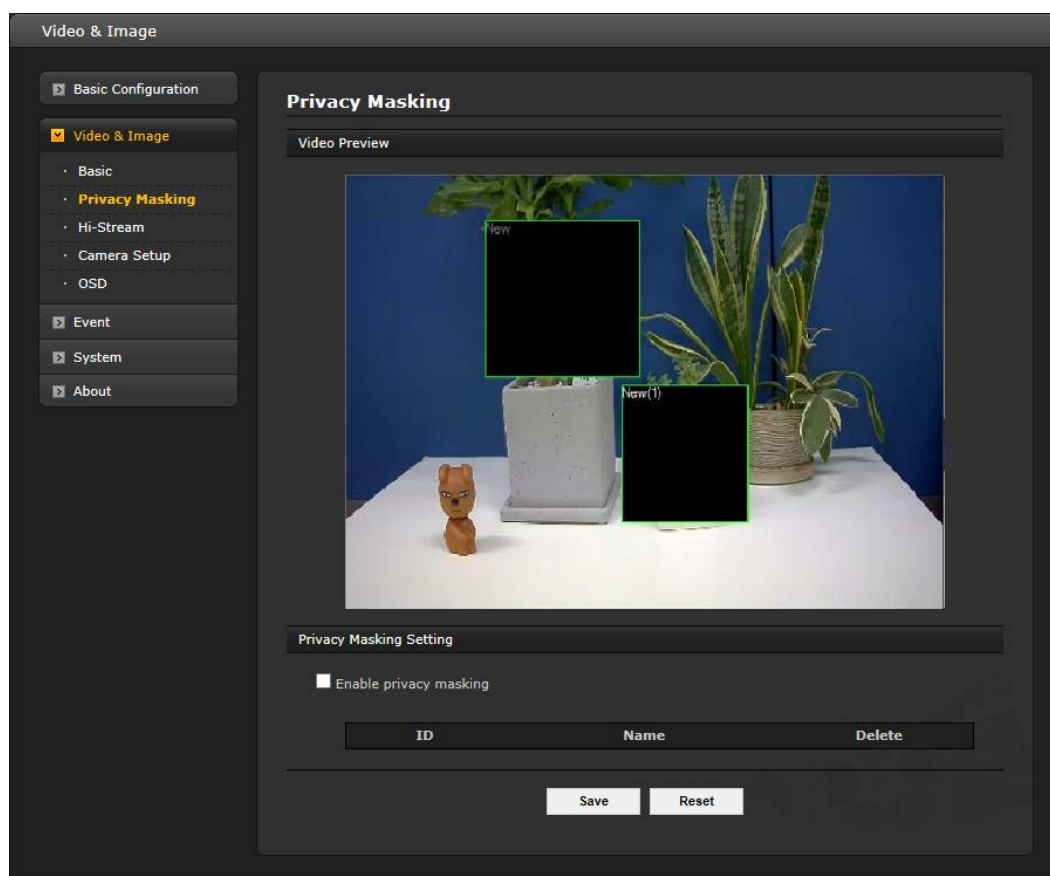
GOP size: 30 [1 ...60]

Save Reset

Refer to "3.5.1 Basic Configuration > Video & Image" for details.

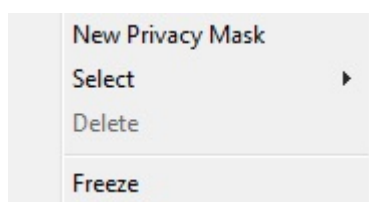
## ▼ Privacy Masking

The privacy masking function allows selected parts of the video image being transmitted to be masked from view. Up to eight privacy masks (or motion detection windows) can be set; the type of privacy masks are black, mosaic or black mosaic.



Select “Enable privacy masking” to activate the privacy masking function.

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



To create a mask window, follow the steps below:

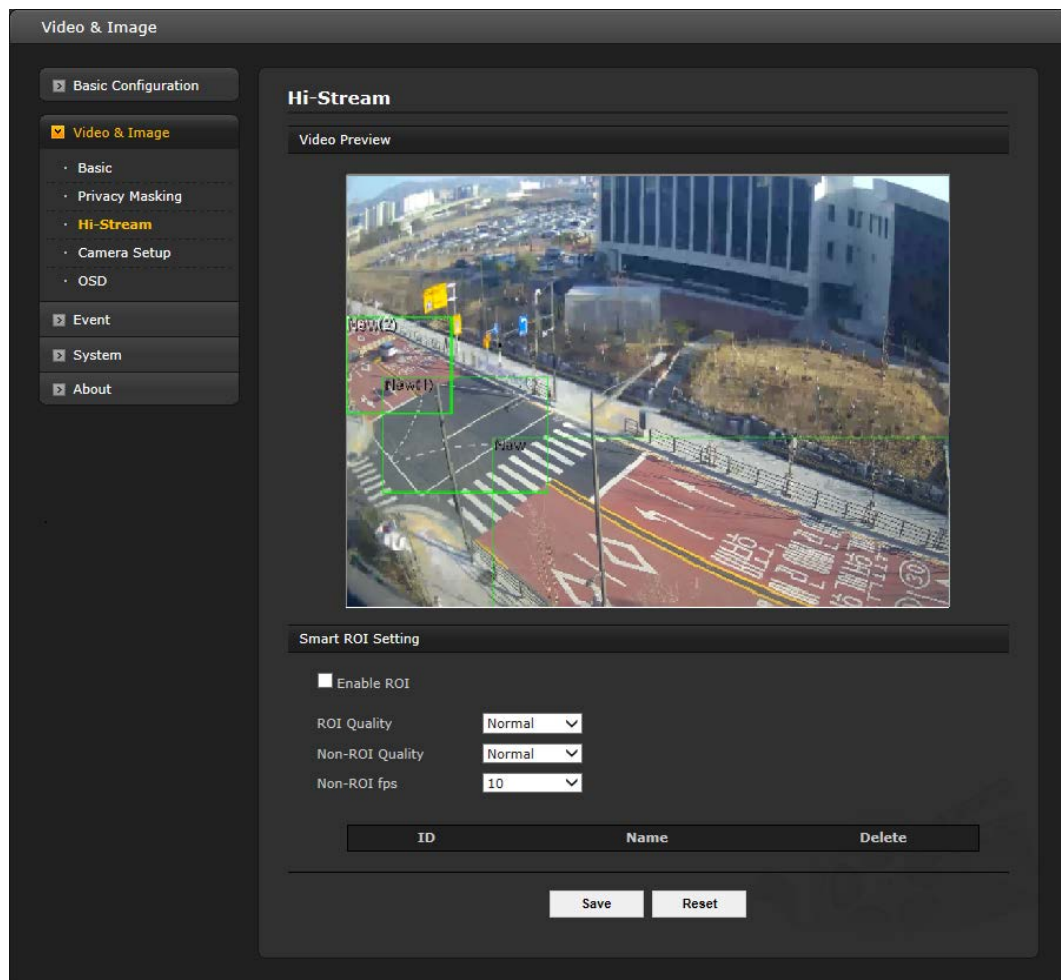
1. Click the right button of mouse to display the mouse menu.
2. Select New Privacy Mask in the mouse menu.
3. Click and drag to designate a mask window area.

A mask window name can also be modified or deleted. Select a name and then modify it in the Name field or click the X in the delete column to delete. Change the size of the mask by dragging the borders or corners of the mask or click in the center of the mask to change the location; select delete button to completely remove the mask.

When the settings are complete, click **Save**, or click **Reset** to revert to previously saved settings.

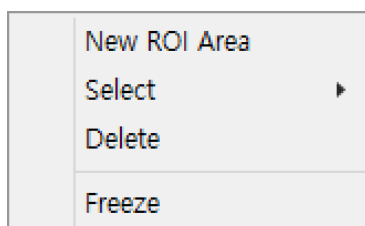
## ▼ Hi-Stream

The Hi-Stream function is used to reduce bandwidth by using compression and frame rate control.

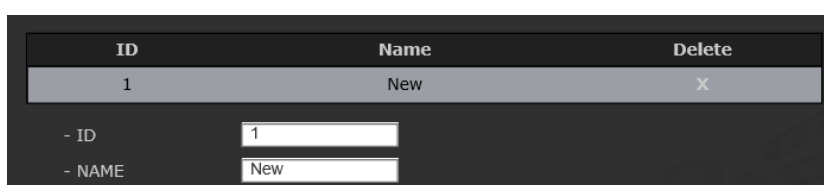


- **Enable ROI:** Select "Enable ROI" to activate Hi-Stream function. Video mode will be fixed to CVBR.

- Create region: Click the right button of mouse and select **New ROI Area**.  
Click the left button of mouse and drag to make a 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**, or click **Reset** to revert to previously saved settings.

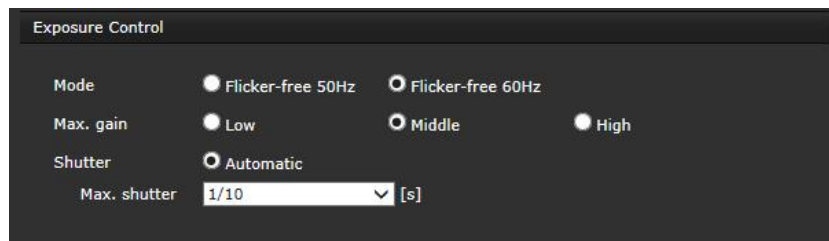
## ▼ Camera Setup

The screenshot shows the 'Camera Setup' configuration window. On the left, a sidebar lists various settings categories, with 'Video & Image' and its sub-item 'Camera Setup' selected. The main panel is titled 'Camera Setup' and contains several sections for configuring the camera's performance and appearance. The 'Exposure Control' section allows setting the mode (Flicker-free 50Hz or 60Hz), maximum gain (Low, Middle, or High), and shutter speed (Automatic or a specific value like 1/10). The 'Image Appearance' section provides sliders for adjusting brightness, contrast, saturation, hue, and sharpness, with a 'Default' button for each. It also includes a White Balance Mode selector (Automatic or Manual). The 'Enhance Control' section features checkboxes for enabling wide dynamic range, horizontal flipping, mirroring, noise reduction (which is checked), and defogging, along with a Metering Mode selector (Spot, Center, Average, Left, Right, or Bottom). The 'Day & Night Control' section has a Mode selector (Automatic, Day, or Night). Finally, the 'IR Control' section has a checked checkbox for 'Enable IR'. At the bottom of the window are 'Save' and 'Reset' buttons.

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

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

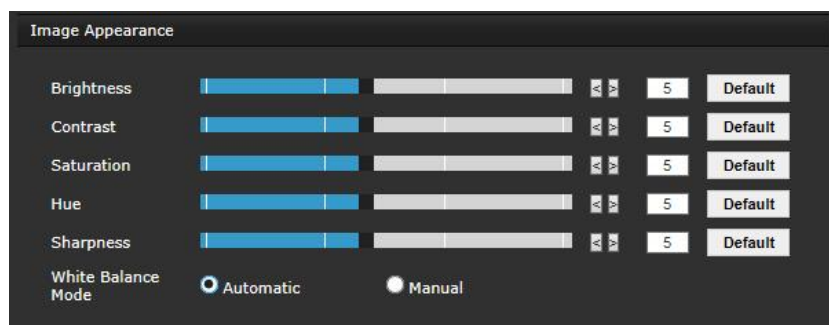
User can set the exposure of the network camera.



- **Mode:** Determines exposure mode between automatic and Flicker-free (60 or 50 Hz depending on camera mode).
- **Max. gain:** Sets maximum gain if Mode is automatic, Low, Middle or High.
- **Shutter:** Determines shutter mode between automatic and fixed.
- **Max. shutter:** Select maximum shutter speed if shutter is in automatic mode. The dropdown shows selectable maximum shutter speeds depending on the exposure selections.

- **Image Appearance**

User can setup image related controls.

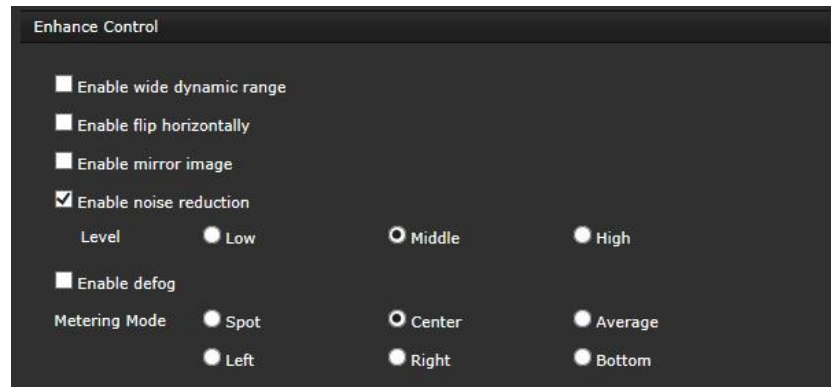


Brightness/Contrast/Saturation/Hue/Sharpness: User can either use slide bar or type the number.

- **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:** Select an appropriate level by entering a value in the range 1-10. Lower values mean less color saturation.
- **Hue:** Select an appropriate level by entering a value in the range 1-10.
- **Sharpness:** Controls 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 will be less sharp.
- **White Balance Mode:** Select white balance mode that is appropriate for camera installation environment.

- **Enhance Control**

Use these controls to enable image controls, such as image flip and mirror, WDR, noise reduction and defog.

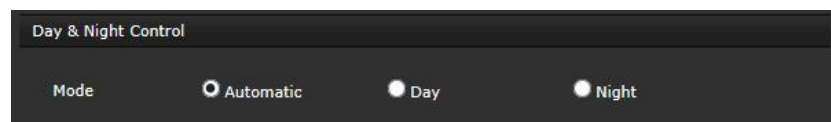


- **Enable wide dynamic range:** Activates WDR, which cannot be used with Defog function. If WDR is activated, shutter mode becomes automatic only.
- **Enable flip horizontally:** Check this box to flip the image horizontally.
- **Enable mirror image:** Check this checkbox to create a mirror view of the image.
- **Enable Noise Reduction:** Check this box to activate the noise reduction and select a level, Low, Middle or High.
- **Enable defog:** Check this checkbox to active the defog function.

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

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

- **Day & Night Control**



- **Mode:** Select the day & night mode from three modes.
- \* **Automatic:** Normally works in day mode; switches automatically to night mode when environment turns dark.
- \* **Day:** Always works in day mode.
- \* **Night:** Always works in night mode.

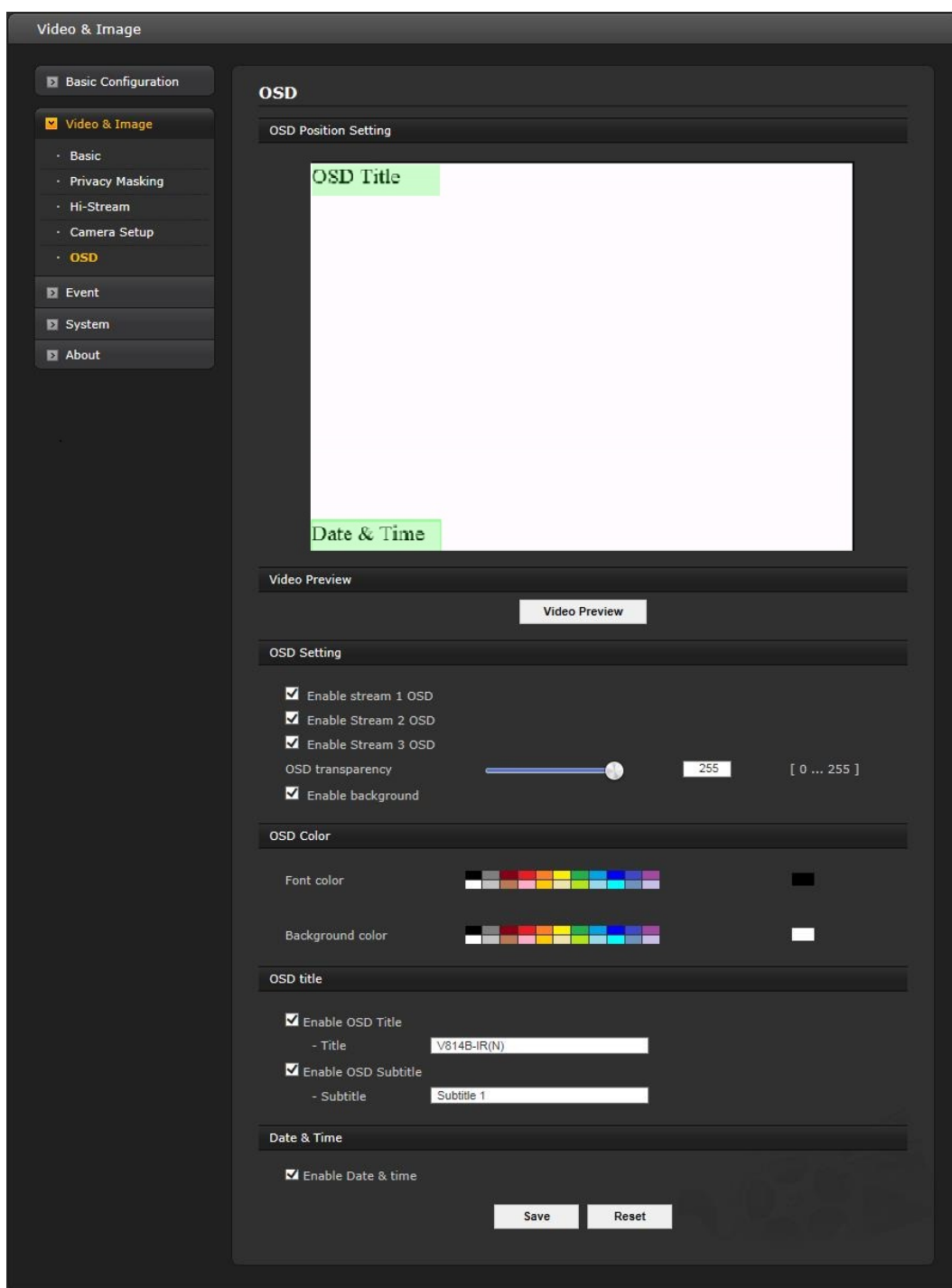
- **IR Control**

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

When the settings are complete, click **Save**, or click **Reset** to revert to previously saved settings.

## ▼ OSD

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



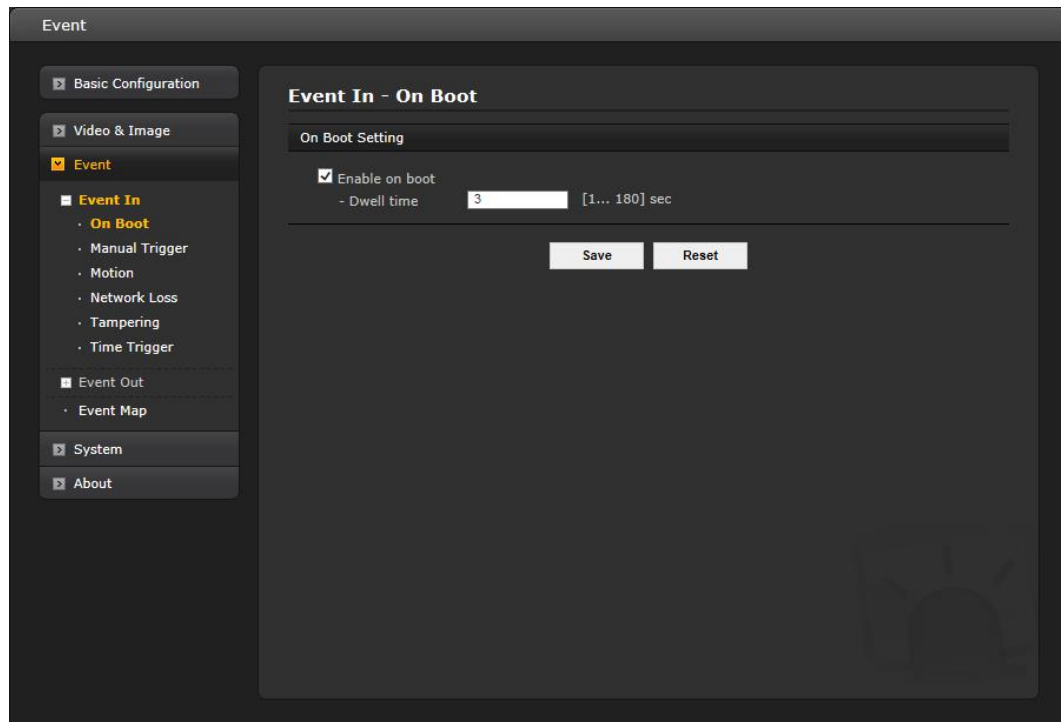
- **Video Preview:** User can check the position of OSD on actual video via preview popup window.
- **OSD Setting:** User can select to show or hide OSD for each stream. Also user can set the transparency level of OSD by slide bar or type in number.
  - **Enable background:** User can set background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

**NOTE:** The change in this page immediately affects video stream.

### 3.5.3 Event

#### 1) Event-In

##### ▼ On Boot



This is used to trigger the event every time the network camera is started. Select “Enable on boot” to activate the motion event.

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

When the settings are complete, click **Save**, or click **Reset** to revert to previously saved settings.

## ▼ Manual Trigger

Event

Basic Configuration

Video & Image

Event

Event In

- On Boot
- Manual Trigger
- Motion
- Network Loss
- Tampering
- Time Trigger

Event Out

- Event Map

System

About

### Event In - Manual Trigger

Manual Trigger 1 Setting

☒ Enable manual trigger 1  
- Dwell time  [1... 180] sec

Manual Trigger 2 Setting

☒ Enable manual trigger 2  
- Dwell time  [1... 180] sec

Manual Trigger 3 Setting

☒ Enable manual trigger 3  
- Dwell time  [1... 180] sec

Manual Trigger 4 Setting

☒ Enable manual trigger 4  
- Dwell time  [1... 180] sec

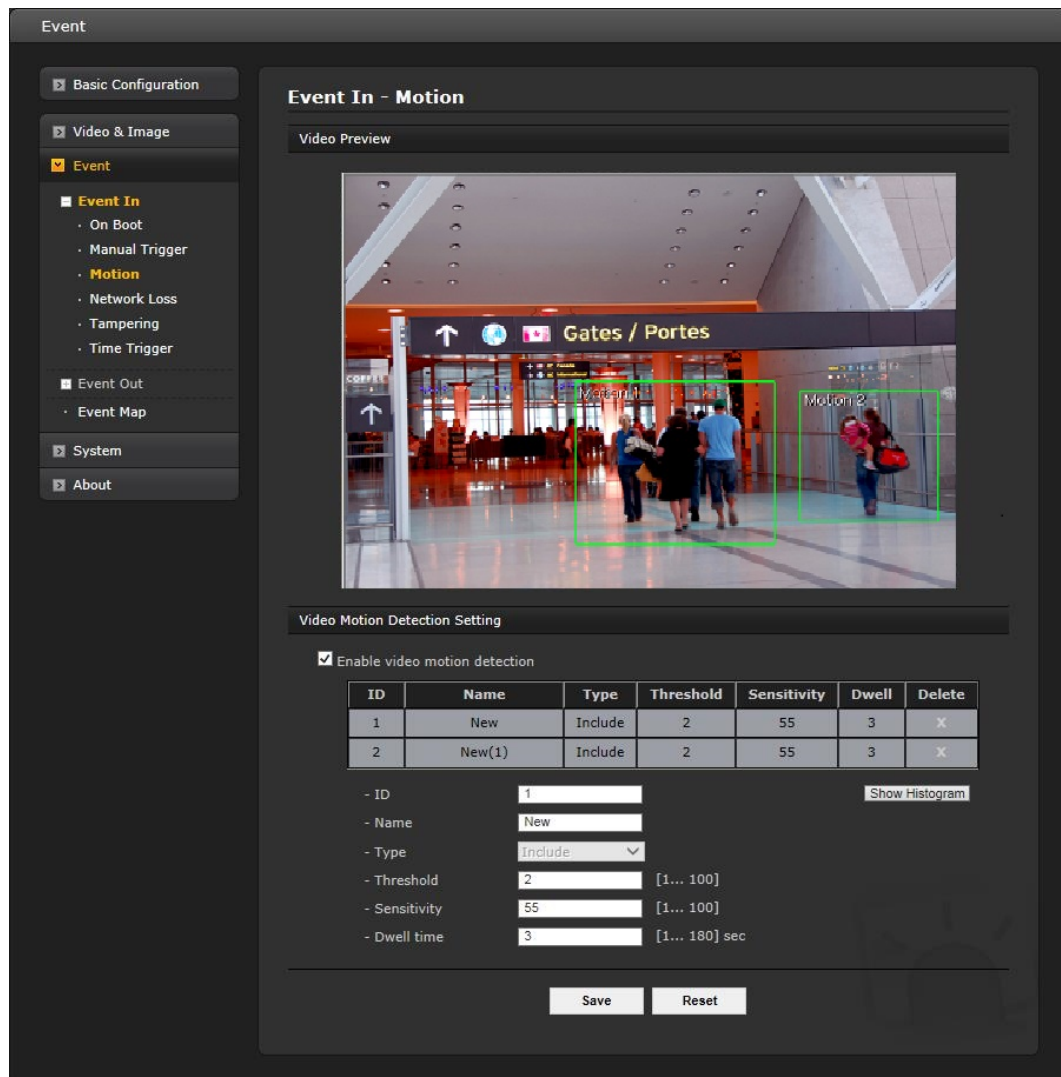
Save Reset

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

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

When the settings are complete, click **Save**, or click **Reset** to revert to previously saved settings.

## ▼ Motion



Motion detection is used to generate an alarm whenever movement occurs (or stops) in the video image. A total of 8 Motion and/or Mask windows can be created and configured.

Motion is detected in defined **Motion** windows, which are placed in the video image to target specific areas. Movement in the areas outside the motion windows will be ignored. If part of a motion window needs to be masked, this can be configured in a **Mask** window.

- **Pre-Viewer**

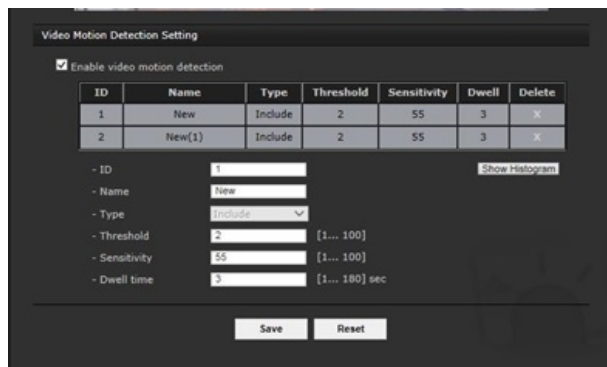
Motion detection windows are configured by Motion or Mask windows. Each window can be selected by clicking with the mouse. It is also possible to **resize**, **delete**, or **move** the window, by selecting the appropriate window at the mouse menu on the video screen.

Select "Enable video motion detection" to activate the motion window.



To create a motion or mask window, follow the steps below:

1. Click the right button of mouse to display the mouse menu.
2. Select New Motion (or Mask) window in the mouse menu.
3. Click and drag mouse to designate a motion area.



### • Motion Detection Setting

The behavior for each window is defined by adjusting the Threshold and Sensitivity, as described below. The combination of these parameters defines whether motion has occurred; motion detection frequency is increased with a high sensitivity and a low threshold.

A motion index is a set of parameters describing Window Name, Type, Threshold, Sensitivity, and Dwell Time. Window Type is Include at the Motion, and Exclude at the Mask window.

- **Threshold:** Sets up the threshold for the motion detection. Threshold judges the amount of change in the area. Select from 1-100; a lower number increase frequency of alarms.
- **Sensitivity:** Sets up the sensitivity for the motion detection. Sensitivity measures the level of motion in each motion area. Select from 1-100, 1 being the least sensitive to alarm condition.
- **Dwell Time:** Set the hold time an event lasts from the point of detection of a motion (hold time).

You can also modify or delete a motion index. It can be deleted using the table and modified by selecting it and changing parameters in the table. Change the size of the mask by dragging the borders or corners of the mask or click in the center of the mask to change the location; select delete button to completely remove the mask. When the settings are complete, click **Save**, or click **Reset** to revert to previously saved settings.

To exclude parts of the Include window, select the New Mask at the mouse menu and position the Mask window as required.





## ▼ Museum Search

Event

Basic Configuration

Video & Image

Event

Event In

- On Boot
- Manual Trigger
- Motion
- Museum Search**
- Network Loss
- Tampering
- Time Trigger

Event Out

- Event Map

System

About

### Event In - Museum Search

#### Museum Search Setting

☐ Enable Museum Search

- Sensitivity  [1... 100]

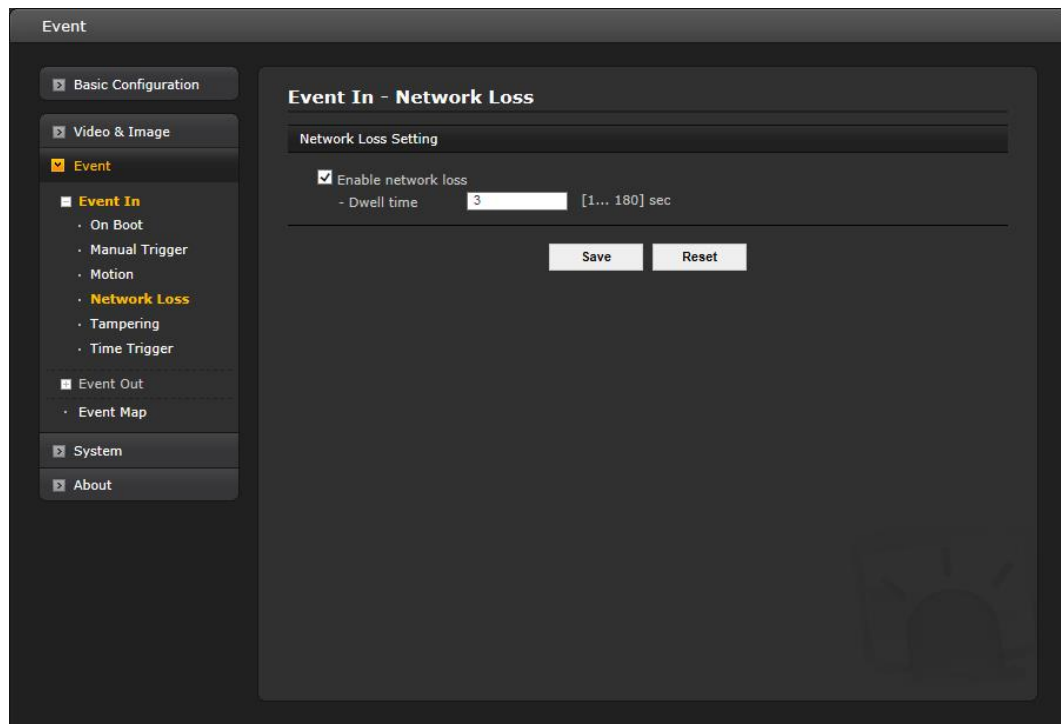
- Threshold  [1... 100]

Save Reset

Museum Search is used to find video where a defined amount of change in a region of interest is detected. The amount of change in a scene's region of interest that will be searched for is defined using the Threshold and Sensitivity, as described below. The combination of these parameters defines whether change has occurred; a high sensitivity and a low threshold will provide increase the number of searches detected.

- **Threshold:** Sets up the threshold for the museum search detection. Threshold judges the amount of change in the area. Select from 1-100; a lower number increase frequency of detections.
- **Sensitivity:** Sets up the sensitivity for the museum search detection. Sensitivity measures the level of change in each region. Select from 1-100, 1 being the least sensitive to detection.

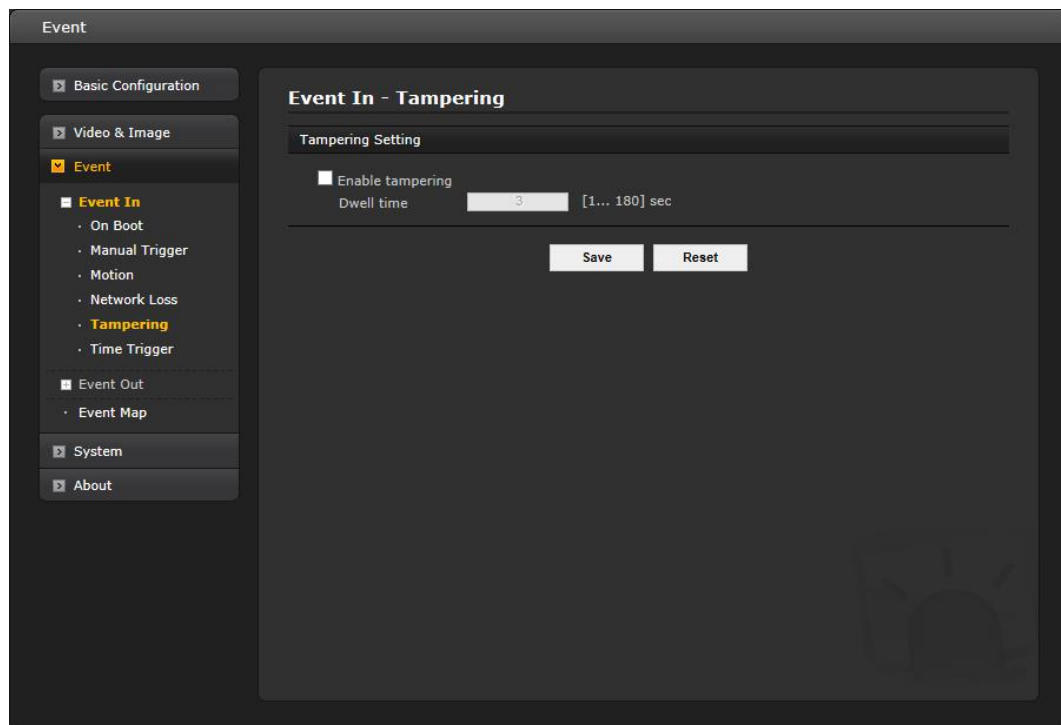
## ▼ Network Loss



This is used to trigger the event every time the network connection fails. 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**, or click **Reset** to revert to previously saved settings.

## ▼ Tampering



This is used to trigger an event when tampering with the camera occurs, for example, obstructing the camera with foreign material or moving the camera direction using external force. Select “Enable tampering” to activate the Tampering event.

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

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

## ▼ Time Trigger

Event

Basic Configuration

Video & Image

Event

Event In

- On Boot
- Manual Trigger
- Motion
- Network Loss
- Tampering
- Time Trigger

Event Out

- Event Map

System

About

### Event In - Time Trigger

Time Trigger Setting

☐ Enable time trigger

Trigger 1 Trigger 2 Trigger 3 Trigger 4

☐ Enable time trigger 1

☐ Enable specific time

- Date 2017-05-17

- Time 08 : 09

☐ Enable every day

- Time 08 : 09

☐ Enable day of week

- Day of week WED

- Time 08 : 09

☐ Enable month

- Day 17

- Time 08 : 09

Save Reset

Time Trigger is to set alarms at specific time. User can set up to four (4) time triggers and each time trigger can be set to a specific date in the calendar, every day, day of the week, or date of every month.

Select "Enable time trigger" to activate the Time Trigger function.

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

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

## 2) Event-Out

### ▼ SMTP (E-Mail).

The screenshot shows the 'Event Out - SMTP(E-Mail)' configuration page. The left sidebar has a tree view with 'Event' selected, which includes 'Event In', 'Event Out', 'System', and 'About'. Under 'Event Out', 'SMTP(E-Mail)' is highlighted. The main content area is titled 'Event Out - SMTP(E-Mail)' and contains three sections: 'SMTP(E-Mail) Setting', 'SMTP(E-Mail) Receiver', and 'SMTP(E-Mail) Test'. The 'SMTP(E-Mail) Setting' section has a checkbox for 'Enable SMTP' and several input fields for 'Sender', 'Image Attachment', 'Interval', 'Aggregate events', 'Use mail server', 'Mail server', 'Port', 'Connections security', 'User name', 'Password', and 'Login method'. The 'SMTP(E-Mail) Receiver' section has eight input fields for 'Receiver 1' through 'Receiver 8'. The 'SMTP(E-Mail) Test' section has a 'Receiver' input field and a 'Test' button. At the bottom are 'Save' and 'Reset' buttons.

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 SMTP" to activate the SMTP operation.

- **Sender:** Enter the email address to be used as the sender for all messages sent by the network camera.
- **Image attachment:** Check this box if attaching an image to the email. The Interval and Aggregate fields are removed.
- **Interval:** Represents the frequency of the email notification when an event occurs.
- **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. Enable the sending of notifications and image email messages from the network camera to predefined addresses via SMTP.
- **Enable use (SMTP) authentication:** Check the box if your mail server requires authentication.
- \* **User name/Password:** Enter the User name and Password as provided by your network administrator or ISP (Internet Service Provider).
- \* **Login method:** Choose a log-in method in the drop-down list: **AUTH LOGIN/AUTH PLAIN.**

- **SMTP (E-Mail) Receiver**

- **Receiver:** Enter an email address for a receiver. You can register up to 8 e-mail addresses of recipients.

- **SMTP (E-Mail) Test**

- **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**, or click **Reset** to revert to previously saved settings.

## ▼ 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 firewall 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.
  - **Enable time folder:** Check to create a folder in the FTP server; then select the type of folder by day (daily), Hour (hourly) or Minute (every minute). Note that user must be authorized to create the folder.
- **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.  
Enter the desired total length in seconds, minutes or hours, and specify the required image frequency.
    - **Event:** Specify the required image frequency (1-2 fps) for the event when it 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**, or click **Reset** to revert to previously saved settings.

## ▼ XML Notification

The screenshot shows a web interface for configuring XML notifications. On the left is a sidebar menu with the following items: 'Basic Configuration', 'Video & Image', 'Event' (highlighted with a yellow checkmark), 'Event In', 'Event Out' (expanded), 'SMTP(E-Mail)', 'FTP & JPEG', 'XML Notification' (highlighted in orange), 'Notification Server', 'Event Map', 'System', and 'About'. The main content area is titled 'Event Out - XML Notification' and contains a section 'XML Notification Setting'. This section has a checkbox labeled 'Enable XML Notification' which is currently unchecked. Below the checkbox are two input fields: 'Notification server URL' and 'Notification server port' (which has '80' entered). At the bottom of the settings area are two buttons: 'Save' and 'Reset'.

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

The screenshot shows a web interface for configuring the Notification Server. On the left is a sidebar menu with options: Basic Configuration, Video & Image, Event (selected), Event In, Event Out (expanded), System, and About. Under 'Event Out', the options are SMTP(E-Mail), FTP & JPEG, XML Notification, Notification Server (selected), and Event Map. The main content area is titled 'Event Out - Notification Server' and contains two sections: 'Notification Server Setting' and 'Notification Server Test'. In the 'Notification Server Setting' section, there is a checkbox 'Enable Notification Server'. Below it are fields for Type (HTTP), Method (POST), URL, Port (80), User name, and Password. The 'Notification Server Test' section has a 'Send message' input field and a 'Test' button. At the bottom of the main area are 'Save' and 'Reset' buttons.

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

- **Notification Server Setting:**

- **Type:** User can select message transmission type among HTTP, HTTPS, TCP, and UDP.
- **Method:** Select GET or POST. This is only available in HTTP or HTTPS protocols.
- **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.

## 3) Event Map

The screenshot shows the 'Event Map' configuration page. The sidebar menu is the same as in the previous screenshot, but 'Event Map' is now selected under 'Event Out'. The main content area is titled 'Event Map' and contains an 'Event Map List' section. Below this is a table with three columns: Event Name, Event In, and Event Out. At the bottom of the main area are 'Add', 'Modify', and 'Remove' buttons.

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.

The screenshot shows a 'Add Event Map' dialog box with the following fields and sections:

- General** (tab selected)
- Event In**
  - Name: New Event
  - Type: Onboot (dropdown)
- Event Out**
  - E-Mail**
    - To e-mail address 1, 2, 3, 4, 5, 6, 7, 8 (checkboxes and text fields)
  - Subject** (text field)
  - Additional info** (text field)
  - FTP**
    - FTP Server 1, 2, 3, 4 (checkboxes)
  - XML Notification** (checkbox)
  - Notification Server**
    - Message (text field)
- Buttons**: OK, Cancel

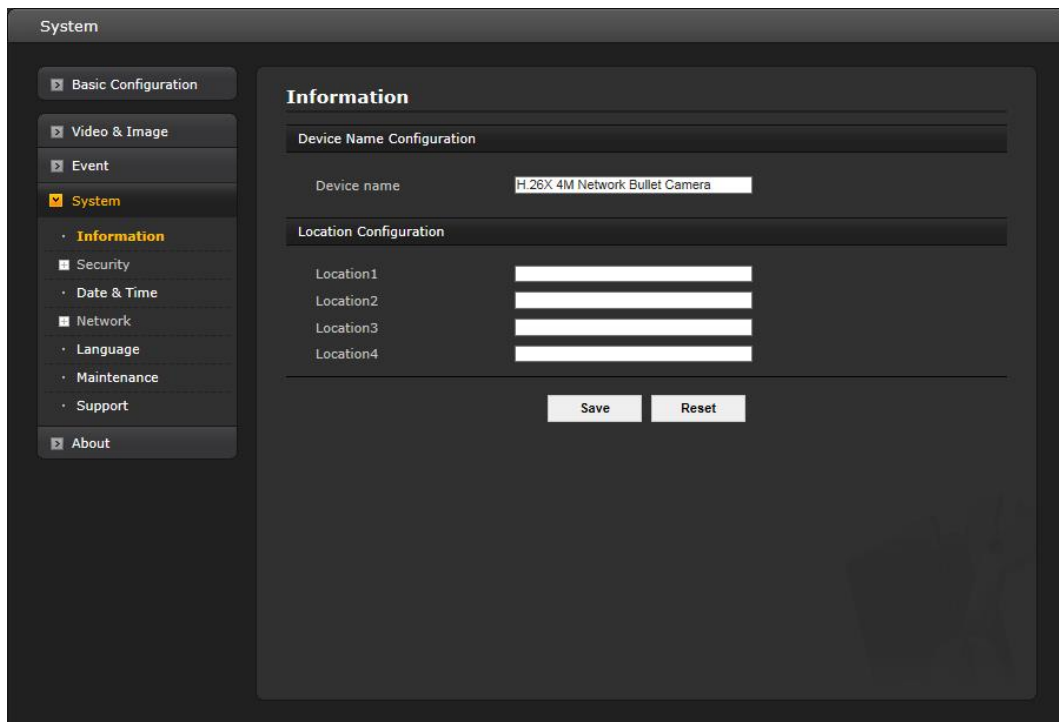
- **General**  
Enter the name for a new event map.
- **Event In**  
Select an event type in the drop-down list.
- **Event Out**  
Select checkbox for those features you want to use.
  - **E-mail:** Select email addresses to send message via email that an event has occurred.
  - **FTP:** Record and save images to an FTP server when an event has occurred.
  - **XML Notification:** It sends XML messages to a Notification server that listens for these. The destination server must first be configured on the Event In page.
  - **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**, or click **Cancel** to cancel settings.

## 3.5.4 System

### 1) Information

You can enter the system information. This page is very useful as a reference for device information after installation.



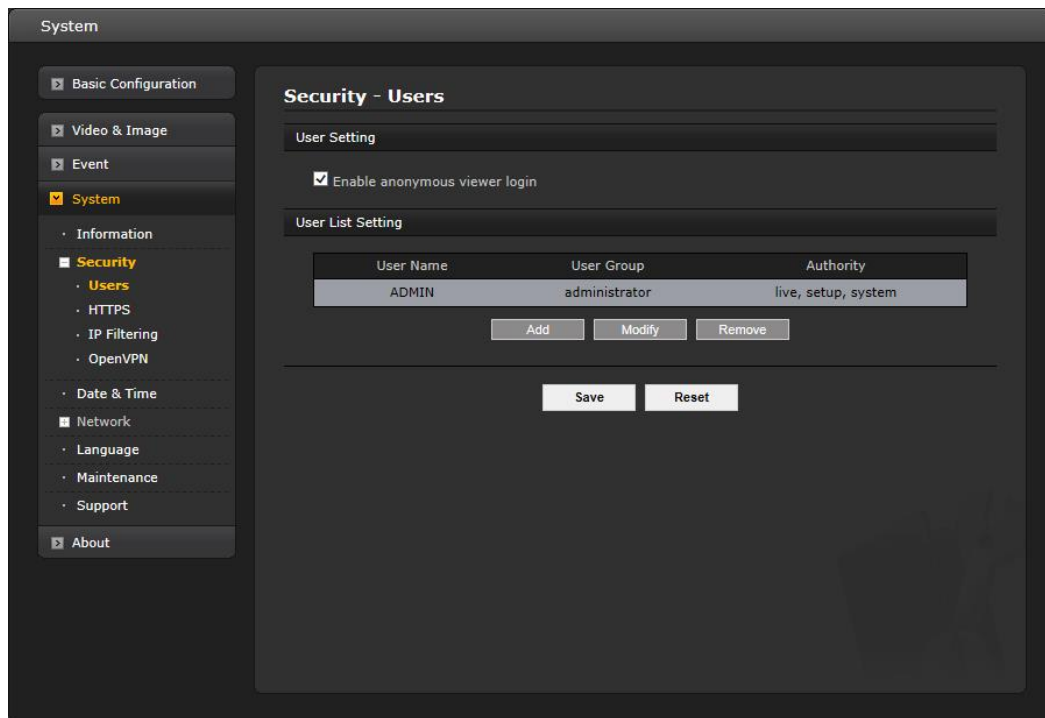
The screenshot shows a web interface for system configuration. On the left is a sidebar menu with the following items: Basic Configuration, Video & Image, Event, System (highlighted with a yellow checkmark), Information (sub-item under System), Security, Date & Time, Network, Language, Maintenance, Support, and About. The main content area is titled 'System' and contains a section titled 'Information'. This section has two sub-sections: 'Device Name Configuration' and 'Location Configuration'. Under 'Device Name Configuration', there is a text input field labeled 'Device name' containing the text 'H.26X 4M Network Bullet Camera'. Under 'Location Configuration', there are four text input fields labeled 'Location1', 'Location2', 'Location3', and 'Location4'. At the bottom of the 'Information' section, there are two buttons: 'Save' and 'Reset'.

- **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**, or click **Reset** to revert to previously saved settings.

## 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.

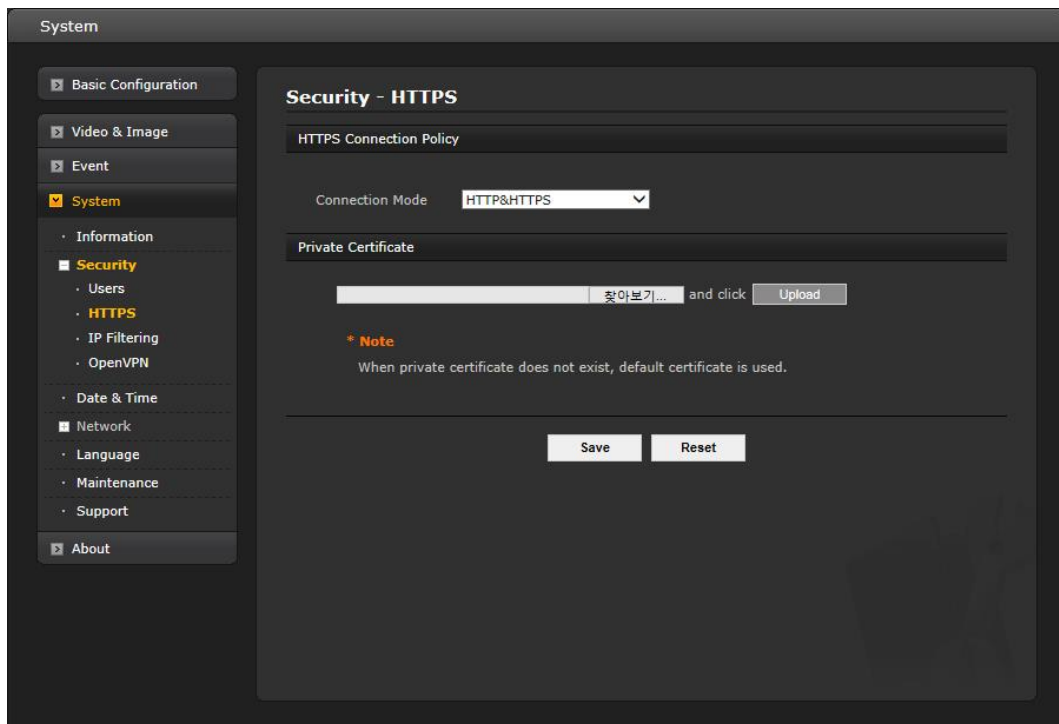
- **User List Setting**

This section shows a list of registered user accounts. Press the Add button; the pop-up window displays as below. Enter a user name and password to be added and select the user group from the drop-down list; click OK to register the user or Cancel to negate the user. User information can also be modified by selecting the user from the list and clicking the Modify button; this same screen will display. Change any information as needed. Selecting a user and clicking Remove deletes the user.

The 'Add User' pop-up window has a title bar 'Add User'. Below it is a section 'User Setting'. It contains four input fields: 'User name :', 'Password :', 'Confirm password :', and 'User group :'. The 'User group' dropdown menu is currently set to 'guest'. At the bottom of the window are 'OK' and 'Cancel' buttons.

When the settings are complete, click **Save**, or click **Reset** to revert to previously saved settings.

## ▼ HTTPS



For greater security, the network camera can be configured to use HTTPS (Hypertext Transfer Protocol over SSL (Secure Socket Layer)), so that 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.

Refer to the home page of your preferred CA for information on where to send the request.

When the settings are complete, click **Save**, or click **Reset** to revert to previously saved settings.

## ▼ IP Filtering

System

Basic Configuration

Video & Image

Event

System

- Information
- Security
  - Users
  - HTTPS
  - IP Filtering
  - OpenVPN
- Date & Time
- Network
- Language
- Maintenance
- Support

About

### Security - IP Filtering

#### IP Filtering Setting

☐ Enable IP filtering

On/Off	Priority	Policy	Start IP	End IP
<input type="checkbox"/>	1	ALLOW	0 . 0 . 0 . 0	0 . 0 . 0 . 0
<input type="checkbox"/>	2	ALLOW	0 . 0 . 0 . 0	0 . 0 . 0 . 0
<input type="checkbox"/>	3	ALLOW	0 . 0 . 0 . 0	0 . 0 . 0 . 0
<input type="checkbox"/>	4	ALLOW	0 . 0 . 0 . 0	0 . 0 . 0 . 0
<input type="checkbox"/>	5	ALLOW	0 . 0 . 0 . 0	0 . 0 . 0 . 0

Save Reset

Checking the "Enable IP address filtering" box enables the IP address filtering function. 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 that users from IP addresses that will be allowed must also be registered with the appropriate access rights (Guest, Operator or Administrator). This is done from Setup> System>Security>Users.

When the settings are complete, click **Save**, or click **Reset** to revert to previously saved settings.

## ▼ OpenVPN

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

System

Basic Configuration

Video & Image

Event

System

Information

Security

Users

HTTPS

IP Filtering

OpenVPN

Date & Time

Network

Language

Maintenance

Support

About

### Security - OpenVPN

#### OpenVPN Configuration

☒ Enable openVPN

☐ Server mode

☐ Client mode

OpenVPN IP Address : 0.0.0.0

#### Server Mode Configuration

Protocol type: UDP

OpenVPN Internal IP: 10 . 8 . 0 . 1

OpenVPN Subnet Mask: 255 . 255 . 255 . 0

Port: 1194

Renegotiation time: 3600 [sec], 0 = unlimited

☒ Use LZO compression

Export CA certificate: Download

Save Reset

### • OpenVPN Server Mode

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

#### • OpenVPN Client Mode

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

The screenshot shows the 'Date & Time' configuration page. The sidebar on the left lists various system settings, with 'System' and 'Date & Time' highlighted. The main panel is divided into several sections: 'Current Server Time' (showing 2017-05-17 17:45:23), 'New Server Time' (with a time zone dropdown set to GMT and a checkbox for daylight saving), 'Time mode' (with three options: 'Synchronize with computer time' selected, 'Synchronize with NTP server' with a server address and interval, and 'Set manually'), and 'Date & Time Format' (with date and time format dropdowns). 'Save' and 'Reset' buttons are at the bottom.

- **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**

Select your time zone from the drop-down list. If you want the server clock to automatically adjust for daylight saving time, check the box "Automatically adjust for daylight saving time changes".

From the **Time Mode** section, select the preferred method to use for setting the time:

- **Synchronize with computer time:** Sets the time from the clock on your computer.
- **Synchronize with NTP Server:** The network camera will obtain the time from an NTP server every 60 minutes.
- **Set manually:** Allows you to manually set the time and date.

- **Date & Time Format**

Specify the formats for the date and time (12h or 24h) displayed in the video streams. Select Date & Time format from the drop-down list.

- **Date Format:** Specify the date format. YYYY: Year, MM: Month, DD: Day
- **Time Format:** Specify the date format. 24 Hours or 12 Hours

When the settings are complete, click **Save**, or click **Reset** to revert to previously saved settings.

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

## 4) Network

Settings regarding the network can be executed for IP, DNS, Host Name, Port, and ARP/Ping can be established, along with setting for DDNS, uPnP, QoS, Zeroconfig, and Bonjour.

### ▼ Basic

The screenshot shows a web interface for network configuration. On the left is a sidebar with a tree view containing: Basic Configuration, Video & Image, Event, System (selected), Information, Security, Date & Time, Network (expanded), Basic (selected), DDNS, RTP, uPnP, QoS, NAT, Zeroconf, Bonjour, Language, Maintenance, Support, and About. The main content area is titled 'Network - Basic' and contains several sections: 'IP Address Configuration' with radio buttons for 'Obtain IP address via DHCP' (selected) and 'Use the following IP address :', followed by input fields for IP address (192.168.1.100), Subnet mask (255.255.255.0), and Default router (192.168.1.254); 'IPv6 Address Configuration' with a checkbox for 'Enable IPv6' (unchecked) and an IPv6 address field (fe80::207:d8ff:fe10:409c/64); 'DNS Configuration' with radio buttons for 'Obtain DNS server via DHCP' (selected) and 'Use the following DNS server address :', followed by input fields for Domain name, Primary DNS server (168.126.63.1), and Secondary DNS server (0.0.0.0); 'Host Name Configuration' with a Host Name field (V814B-IRN0007D810409C); 'Services' with input fields for HTTP port (80), HTTPS port (443), and RTSP port (554); and 'Link Speed Control' with dropdown menus for LAN Interface (Auto) and Link Speed (100M bit/sec). At the bottom are 'Save' and 'Reset' buttons.

- **IP Address Configuration:**

- **Obtain IP address via DHCP:** Dynamic Host Configuration Protocol (DHCP) is a protocol that lets network administrators centrally manage and automate the assignment of IP addresses on a network. DHCP is enabled by default. Although a DHCP server is mostly used to set an IP address dynamically, it is also possible to use it to set a static, known IP address for a particular MAC address. To obtain IP address via DHCP, check the radio button.
- **Use the following IP address:** To use a static IP address for the network camera, check the radio button and then make the following settings:
  - \* **IP address:** Specify a unique IP address for your network camera.
  - \* **Subnet mask:** Specify the mask for the subnet the network camera is located on.
  - \* **Default router:** Specify the IP address of the default router (gateway) used for connecting devices attached to different networks and network segments.

- **IPv6 Address Configuration**

Check this "Enable IPv6" box to enable IPv6. Other settings for IPv6 are configured in the network router.

- **DNS Configuration**

DNS (Domain Name Service) provides the translation of host names to IP addresses on your network. Check the radio button to obtain DNS server via DHCP or set the DNS server.

- **Obtain DNS Server via DHCP:** Automatically use the DNS server settings provided by the DHCP server.
- Use the following DNS server address to enter the desired DNS server by specifying the following:
  - \* **Domain name:** Enter the domain(s) to search for the host name used by the 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. This is the camera name that will show up in the Site List in ViconNet.

- **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'.

- **ARP/Ping Setting**

- **Enable ARP/Ping setting:** The IP address can be set using the ARP/Ping method, which associates the unit's MAC address with an IP address. Check this box to enable the service. Leave disabled to prevent unintentional resetting of the IP address.

- **Link Speed Control:**

- **LAN Interface:** User can select Auto, Half or Full.
- **Link Speed:** User can select either 10Mbps or 100Mbps when LAN interface was selected Half or Full.

When the settings are complete, click **Save**, or click **Reset** to revert to previously saved settings.

## ▼ DDNS

The screenshot shows a web interface for configuring DDNS. On the left is a sidebar menu with categories: System, Video & Image, Event, and System (expanded). Under 'System', there are links for Information, Security, Date & Time, Network (selected), Basic, DDNS (highlighted), RTP, UPnP, QoS, NAT, Zeroconf, Bonjour, Language, Maintenance, Support, and About. The main content area is titled 'Network - DDNS' and contains the 'Internet DDNS (Dynamic Domain Name Service)' configuration. It includes a checkbox for 'Enable DDNS', a note about configuring a primary DNS server, and fields for 'DDNS Server' (a dropdown menu showing 'cctv-network.co.kr'), 'Registered host', 'User name', 'Password', 'Confirm password', and 'Maximum time interval' (a dropdown menu showing '1 hour'). There is also a checkbox for 'Register local network IP address' and a label 'Registered IP address :'. At the bottom right are 'Save' and 'Reset' buttons.

- **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**, or click **Reset** to revert to previously saved settings.

## ▼ RTP

The screenshot shows a web interface for configuring RTP settings. On the left is a sidebar with a menu: Basic Configuration, Video & Image, Event, System (selected), Information, Security, Date & Time, Network (selected), Basic, DDNS, RTP (selected), UPnP, QoS, NAT, Zeroconf, Bonjour, Language, Maintenance, Support, and About. The main content area is titled 'Network - RTP'. It contains several sections: 'Port Range' with 'Start port' (30000) and 'End port' (30238); 'Multicast (Stream 1)' with 'Multicast destination IP' (231.1.128.20), 'RTP port' (40000), 'RTP TTL' (15), and an unchecked 'Always enable multicast' checkbox; 'Multicast (Stream 2)' with 'Multicast destination IP' (231.1.128.21), 'RTP port' (40000), 'RTP TTL' (15), and an unchecked 'Always enable multicast' checkbox; 'Multicast (Stream 3)' with 'Multicast destination IP' (231.1.128.22), 'RTP port' (40000), 'RTP TTL' (15), and an unchecked 'Always enable multicast' checkbox; and 'Multicast (Meta)' with 'Multicast destination IP' (231.1.128.20), 'RTP port' (40004), 'RTP TTL' (15), and an unchecked 'Always enable multicast' checkbox. At the bottom right are 'Save' and 'Reset' buttons.

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

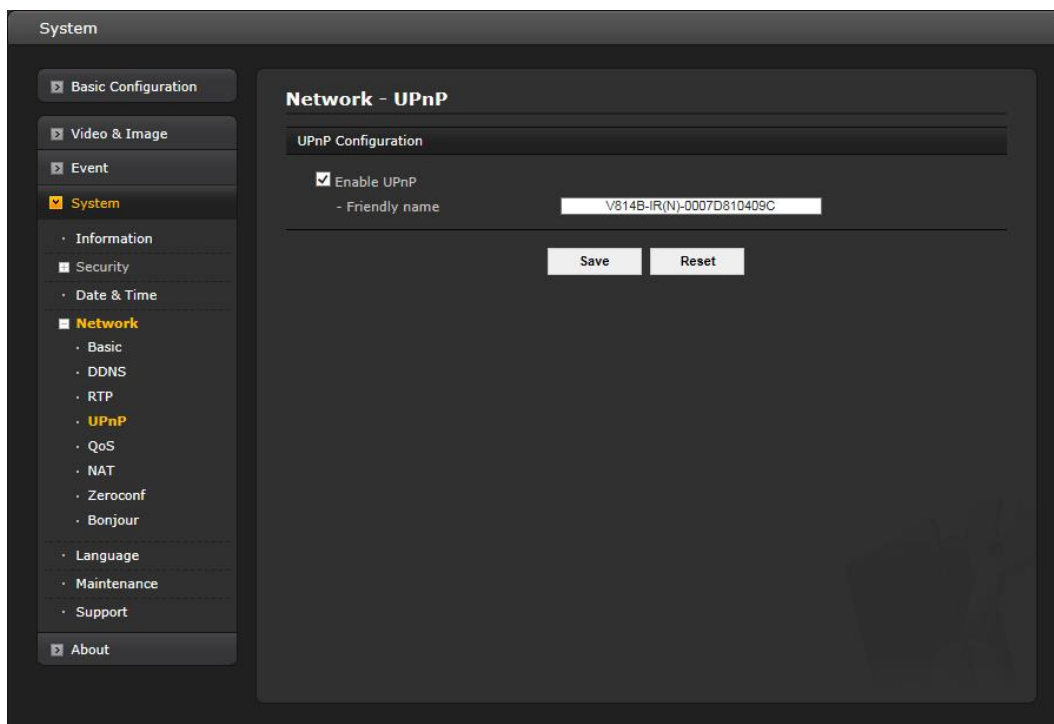
- **Port Range**
  - **Start/End port:** Enter a value between 1024 and 65532
- **Multicast (Stream1/Stream2/Stream3)**

This function is for sending Video and Audio to Multicast group.

  - **Enable Multicast:** Check the box to enable multicast operation.
  - **Multicast destination IP:** Enter an IP between 224.0.0.0 and 239.255.255.255.
  - **RTP port:** Enter a value between 1024 and 65532.
  - **RTP TTL:** Enter a value between 1 and 255. If a network status is smooth, enter a lower value. However, if a network status is poor, enter a higher value. When there are many network cameras or users, a higher value may cause a heavy load to the network. Consult with a network manager for detailed information.
  - **Always enable multicast:** Check the box to start multicast streaming without opening an RTSP session.

When the settings are complete, click **Save**, or click **Reset** to revert to previously saved settings.

## ▼ UPnP



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

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

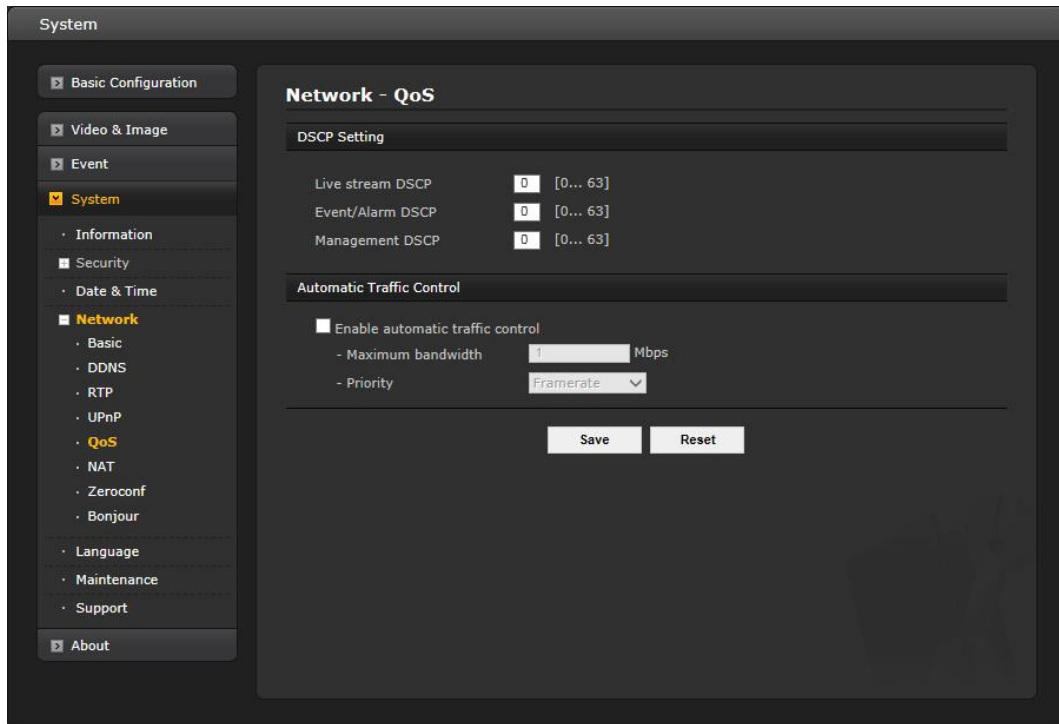
When the settings are complete, click **Save**, or click **Reset** to revert to previously saved settings.

## ▼ 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:

- The ability to prioritize traffic and thus allow critical flows to be served before flows with lesser priority.
- 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 traffic's IP header. When the marked traffic reaches a network router or switch, the DSCP value in the IP header tells the router or switch which type of treatment to apply to this type of traffic, for example, how much bandwidth to reserve for it. Note that DSCP values can be entered in decimal or hex form, but saved values are always shown in decimal.

The following types of traffic are marked; enter a value for each type of traffic used:

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

### • Automatic Traffic Control

Check the box to enable automatic traffic control.

Set a limitation on user network resources by designating the maximum bandwidth. Select either the Maximum bandwidth or Automatic framerate radio button.

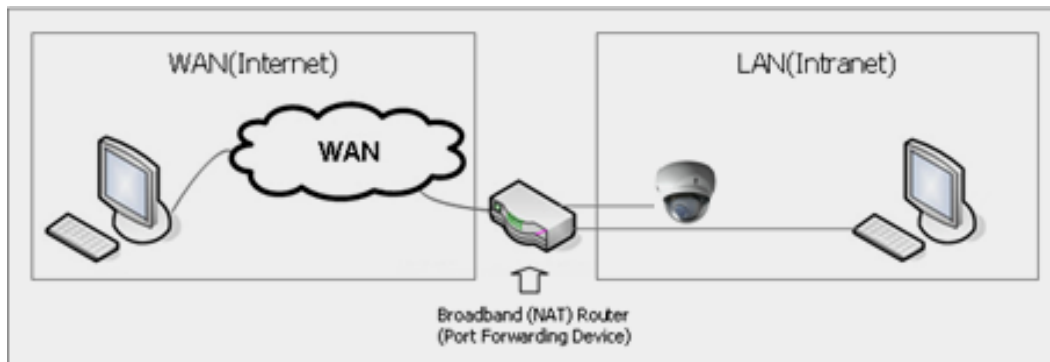
- **Maximum bandwidth** - When sharing other network programs or equipment, it is possible to set a limitation on the maximum bandwidth in the unit of Mbit/s or kbit/s.
- **Automatic frame rate** - Selected if not influenced by a network-related program or equipment without a limitation on the network bandwidth.

When the settings are complete, click **Save**, or click **Reset** to revert to previously saved settings.

### ▼ NAT (Port Mapping)

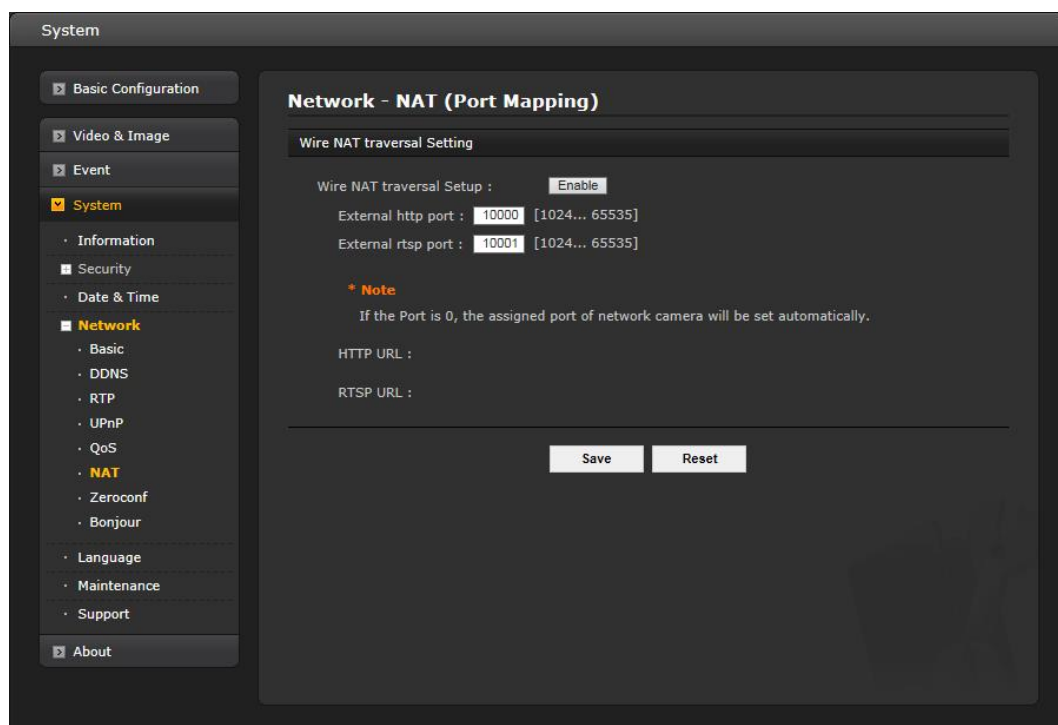
A broadband router allows devices on a private network (LAN) to share a single connection to the Internet. This is done by forwarding network traffic from the private network to the "outside," that is, the Internet. Security on the private network (LAN) is increased since most broadband routers are pre-configured to stop attempts to access the private network (LAN) from the public network/Internet.

Use **NAT** when your network cameras are located on an intranet (LAN) and you wish to make it available from the other (WAN) side of a NAT router. With NAT traversal properly configured, all HTTP traffic to an external HTTP port in the NAT router is forwarded to the network camera.



#### Notes:

- 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.





- **NAT Settings**

- **Enable** – Check this box to enable NAT traversal. When enabled, the network camera attempts to configure port mapping in a NAT router on your network, using UPnP. Note that UPnP must be enabled in the network camera (see System>Network>UPnP).
- \* **Automatic setting:** When selected, the network camera automatically searches for NAT routers on your network.
- \* **Manual setting:** Select this option to manually select a NAT router and enter the external port number for the router in the field provided.

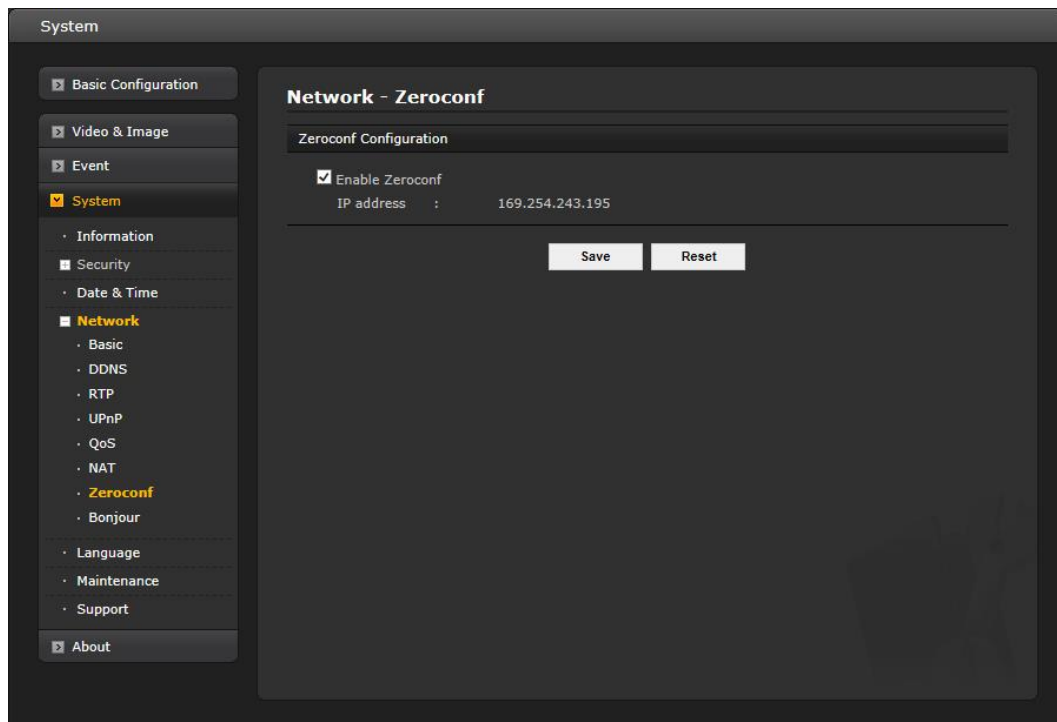
**Notes:**

- If you attempt to manually enter a port that is already in use, an alert message will be displayed.
- When the port is selected automatically it is displayed in this field. To change this enter a new port number and click Save.

When the settings are complete, click **Save**, or click **Reset** to revert to previously saved settings.

## ▼ Zeroconf

Zeroconf allows the network camera to create and assign the IP address for network cameras and connect to a network automatically.



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:

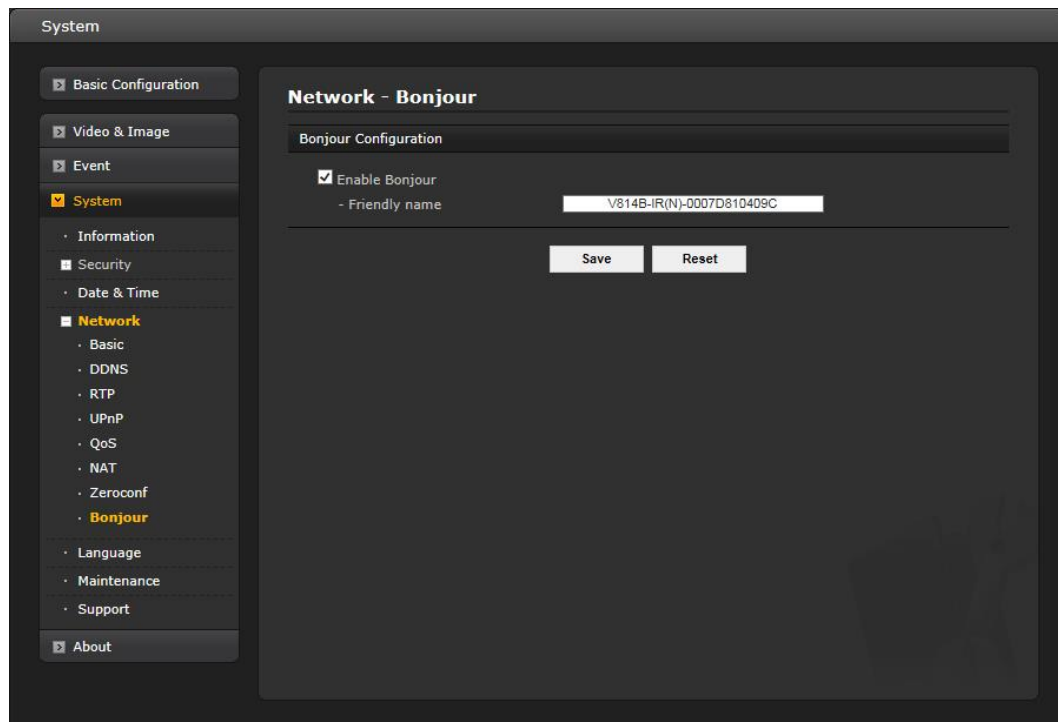
- Assignment of numeric network addresses for networked devices (link-local address auto configuration)
- Automatic resolution and distribution of computer hostnames (multicast DNS)
- Automatic location of network services, such as printing devices through DNS service discovery.

Click the checkbox to enable Zeroconf.

When the settings are complete, click **Save**, or click **Reset** to revert to previously saved settings.

## ▼ 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.



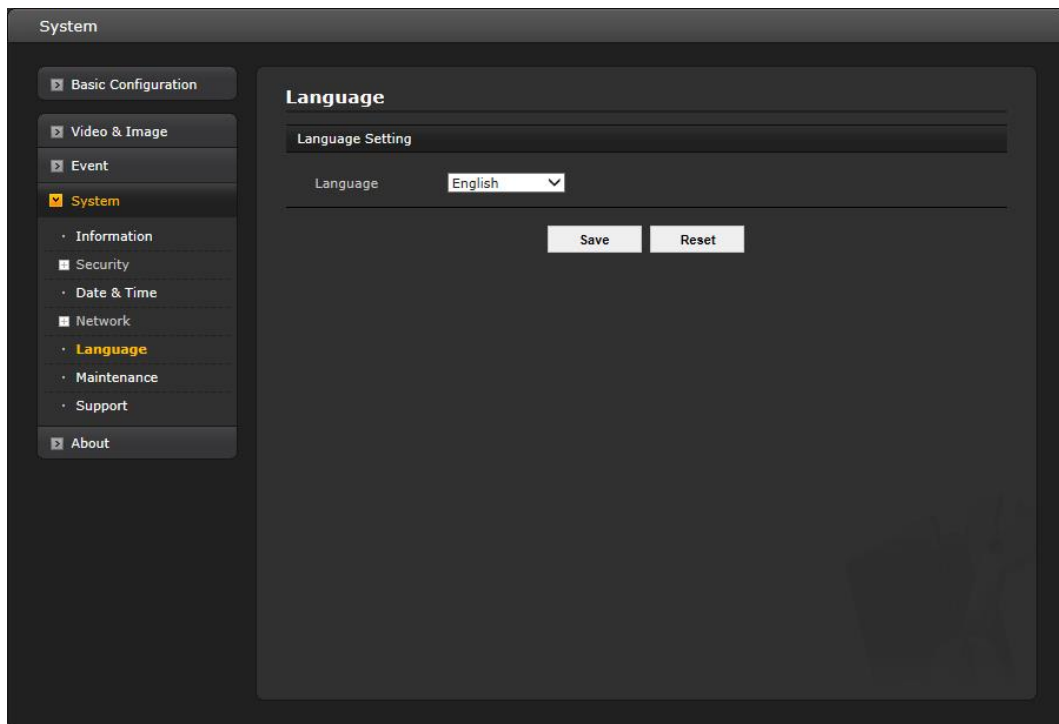
Click the check box to enable Bonjour. Enter a name in the Friendly name field.

When the settings are complete, click **Save**, or click **Reset** to revert to previously saved settings.

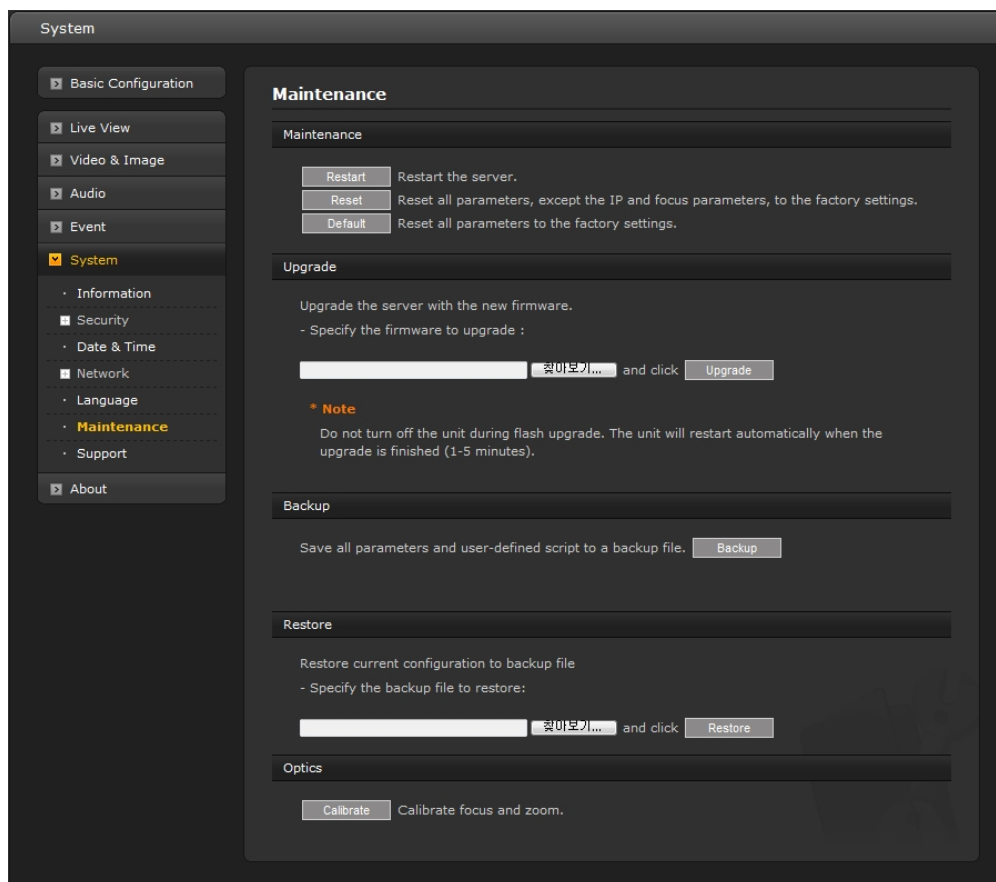
**Note:** Also known as zero-configuration networking, Bonjour enables devices to automatically discover each other on a network, without having to enter IP addresses or configure DNS servers. (Bonjour is a trademark of Apple Computer, Inc.)

## 5) Language

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



## 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 the camera by importing an upgrade file and pressing the **Upgrade** button. During the upgrade, do not turn off the power to the network camera. After waiting five minutes or longer, try to access the camera again.

To perform an update for multiple cameras at one time, use the SmartManager discovery and update tool and select them using the SHIFT and CTRL keys (see SmartManager manual for details).

- **Backup**

Click the **Backup** button to save setting values that users enter to the network camera to a user PC.

- **Restore**

Click the **Restore** button to import and apply setting values saved to a user PC.

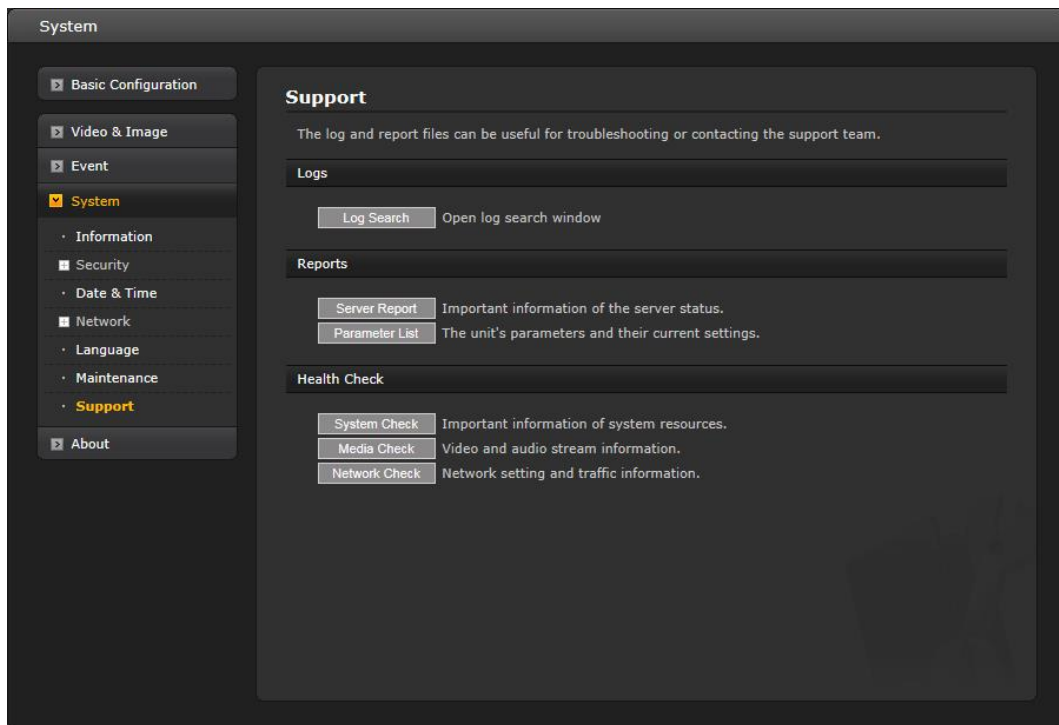
- **Optics (Motorized lens only)**

Click the **Calibrate** button when the Fine Focus function can't adjust the focus.

**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 when troubleshooting a problem or when contacting the technical assistants.



- **Logs**

The network camera supports system log information. Click the **Log Search** button to get the 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 camera's system resources. The pop-up window below displays.

**System Check**

Model :

Firmware : 1.7.5

**Date & Time**

. Date : 2016-08-04

. Time : 08:24:28

. Running time : 11 min

**CPU**

. Usage : 47 %

OK

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

**Video stream**

Stream	On/Off	Codec	Size	FPS	Bitrate
Stream1	On	H.264 Baseline Profile	1920x1080	30	4094 Kbps
Stream2	On	undefined	1920x1080	0	0 Kbps
Stream3	On	H.264 Baseline Profile	640x480	30	744 Kbps

**Audio stream**

Type	On/Off	Codec	Sample	Volume	Bitrate
Input	Off	-	-	-	-

OK

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

**Network Check**

**Wired configuration**

. Current Status : Connected

. DHCP : Off

. IP address : 192.168.11.64

. Subnet mask : 255.255.255.0

. Gateway : 192.168.11.1

. DNS : 168.126.63.1

**Wireless configuration**

. Current Status : Disconnected

**Traffic**

. Wired : 4213 Kbps

**Streaming service**

. Number of users currently live : 1

. Number of users currently playback : 0

**Server connection**

. Live Push : Disconnected

. Event Push : Disconnected

OK

## 3.6 Help

The Help information window is provided as a popup window so that users can open and read it without a need for log-in. It offers descriptions of settings and a Help page, so users can manipulate the network camera without having to reference the manual.

### Help

View

Video & Image

Basic

Privacy Masking

Hi-Stream

Camera Setup

OSD

Event

System

#### Video & Image - Basic

Through the 'Video & Image - Basic' page, user can setting 'Codec' that use for image compression.

▶ Capture mode

Through the drop-down list of 'Capture mode', you may set a image sensor. The following Table is optional items of 'Capture mode' are dependent on 'Video Mode (NTSC / PAL)'.

Video mode	Capture Mode
NTSC	- 2048x1536 Max. 20fps - 1920x1080 Max. 30fps - 1920x1080 Max. 60fps - 1600x1200 Max. 15fps - 1280x720 Max. 30fps - 800x600 Max. 30fps
PAL	- 2048x1536 Max. 20fps - 1920x1080 Max. 25fps - 1920x1080 Max. 50fps - 1600x1200 Max. 12fps - 1280x720 Max. 25fps - 800x600 Max. 25fps

▶ Stream Setting

Through the 'Stream Setting', you may set a 'Codec' that use for image compression. The 'H.264', 'MPEG4' and 'MJPEG' codecs are used to image compression in this camera. The following TABLE shows the 'Stream' that supported for each codec.

Codec	Stream	Setting
H.264	'Stream1', 'Stream3' * In the 'Capture mode' 50, 60fps, 'Stream 3' is not supported.	Refer to '▶ H.264 /MPEG4'
MPEG4		



## A. Appendix

### A.1 Troubleshooting

When 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 not displayed in the client.	Check that the correct network interface is selected in the Video & Image/Stream.
Multicast H.264 not displayed in the client.	Check with your network administrator that the multicast addresses used by the camera are valid for your network. Check that the Enable multicast checkbox is enabled in the System/Network/RTP tab. Checks with your network administrator to see if there is a firewall preventing viewing.
Multicast H.264 only accessible by local clients.	Check if your router supports multicasting, or if the router settings between the client and the server need to be configured. The TTL value may need to be increased.
Color saturation is different in H.264 and Motion JPEG.	Modify the settings for your graphics adapter. Please see the adapter's documentation for more information.
Poor audio quality.	Too many users/clients connected to the camera may affect the sound quality adversely. Try limiting the number of clients allowed to connect.
Distorted audio.	Check that the correct Audio Input source is selected. Select Microphone for a connected external microphone. Select Line for a connected line in source.
Video cannot be recorded.	Check that the SD Card is inserted properly. Check that the SD Card is formatted properly.

## A.2 Preventive Maintenance

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

Every three-month, perform the following maintenance.

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

## A.3 System Requirement for Web Browser

**Operating System:** Microsoft® Windows® 98, Microsoft Windows ME, Microsoft Windows 2000, Microsoft Windows XP, or Microsoft Windows Vista®, Windows 7, Windows 8.1 and Windows 10.

**CPU:** Intel® Core™ 2 Duo 2GHz or higher, 1 GB RAM or more, 10 GB free disk or higher

**VGA:** AGP, Video RAM 32 MB or higher (1024x768, 24 bpp or higher)

## A.4 Product Specification

- **Bullet Network Camera**

Model		V812B-IR	V812B-312MIR	V814B-IR	V814B-312MIR
IMAGE					
Lens		3.6mm, F2.1	MVF 2.8~12mm, F1.4	3.6mm, F2.1	MVF 2.8~12mm, F1.4
Angle of View		84°(H)	95°(H) ~ 35°(H)	84°(H)	95°(H) ~ 35°(H)
Image Sensor	Type	1/2.9" Sony Exmor CMOS sensor		1/3" CMOS Sensor	
	Pixels	1984(H) x 1125(V)		2688(H) x 1520(V)	
Min. Illumination		Color : 0.1 Lux / BW : 0 Lux @ IR ON			
Scanning Mode		Progressive Scan			
Wide Dynamic Range		Yes			
Day and Night Mode		True D/N (Auto, Day, Night)			
Noise Reduction		2DNR, 3DNR			
Digital Zoom		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		50Hz, 60Hz			
Shutter Speed		Auto (1/10,000 ~ 1sec), Manual			
IR Illuminator	Quantity	1 Array LEDs	24 SMD LEDs	1 Array LEDs	24 SMD LEDs
	Distance	Up to 30m	Up to 30m	Up to 30m	Up to 30m
Motorized Lens Control		-	Smart Focus, Manual	-	Smart Focus, Manual
VIDEO/AUDIO					
Compression		H.264 (Baseline, Main, High Profile), H.265(Main Profile), MJPEG			
Bitrate Control		CBR, CVBR			
Resolution		1920x1080, 1440x1080, 1280x1024, 1280x720, 1024x768, 704x480(576), 640x480, 400x240, 320x240		4M capture mode: 2592x1520, 2304x1296, 1920x1080, 1440x1080, 1280x1024, 1280x720, 1024x768, 704x480(576), 640x480, 400x240, 320x240. 2M capture mode: 1920x1080, 1440x1080, 1280x1024, 1280x720, 1024x768, 704x480(576), 640x480, 400x240, 320x240	
Frame Rate		Max. 30fps/25fps			
Streaming		Triple Stream: H.264/H.265 x 2, MJPEG x 1			

SYSTEM					
Video Contents Analysis		Tampering			
Motion Detection Area		16 Programmable Area (Include Area 8, Exclude Area 8)			
Privacy Mask Zone		4 Programmable Zones			
Hi-Stream (Smart Codec)		8 Regions, quality setup, non-ROI fps setup			
FTP Uploading		MJPEG			
Event Notification		E-mail, FTP, Notification Server, XML Notification			
Login Authority		Administrator, Operator, Guest			
Event Buffering	FTP	Pre: 30sec, Post: 30sec			
Manual Trigger		4 Programmable Trigger			
Security		Multi User Authority, IP Filtering, HTTPS, SSL, OpenVPN			
Network Time Sync		NTP Server, Synchronized Computer, Manual			
Software Reset		Restart, Reset, Factory Default			
Auto Recovery		Backup, Restore			
Remote Upgrade		Web Browsing (IE, Chrome, Safari, Firefox), SmartManager			
NETWORK					
Protocols		TCP/IP, UDP, IPv4/v6, HTTP, HTTPS, QoS, FTP, UPnP, RTP, RTSP, RTCP, DHCP, ARP, Zeroconf, Bonjour			
Client Software		Web, SmartManager, Client S/W, Mobile S/W			
Max. User Connection		Live: 10 Users, Playback: 3 Users			
API Support		Open API, ONVIF Compliance			
Mobile Support		Android, i-OS			
EXTERNAL IN/OUT					
Ethernet		RJ-45 (10/100Base-T)			
ETC					
Operating Humidity		0 ~ 90% RH (Non-condensing)			
Operating Temperature		14°F ~ +122°F (-10°C ~ +50°C)			
Power Supply		PoE (IEEE802.3af compliance, Class0), 12 VDC			
Power Consumption		87mA (4.2W)@ PoE 280mA (3.4W)@ 12VDC	145mA (7W)@ PoE 520mA (6.2W)@ 12VDC	106mA (5.1W)@ PoE 320mA (3.8W)@ 12VDC	145mA (7W)@ PoE 480mA (5.8W)@ 12VDC
Dimensions		3.0 in. (77mm) (Φ) x 6.1 in (155mm) (H)	3.3 in. (84mm)(Φ) x 9.4 in. (239mm)(H)	3.0 in. (77mm) (Φ) x 6.1 in (155mm) (H)	3.3 in. (84mm)(Φ) x 9.4 in. (239mm)(H)
Net Weight		Approx 0.66 lb (300g)	Approx 1.5 lb (680g)	Approx 0.66 lb (300g)	Approx 1.5 lb (680g)
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. All IQEYE Cameras: Two years if purchased before 1/1/2011.
2. Alliance-mini (IQD3xx), Alliance-mx (IQMxxx) and 3 Series (IQ03xx): Five years if purchased between 1/2/2011 – 12/31/2014.
3. Alliance-Pro (IQA3xx): Five years if purchased between 3/2/2012 – 12/31/2014. Three years if the motorized lens (IQA3xx-A3) option.
4. Access Control System Components: Two year from date of original retail purchase.
5. Uninterruptible Power Supplies: Two years from date of original retail purchase.
6. VDR-700 Recorder Series: One year from date of original retail purchase.
7. V5616MUX: One year from date of original retail purchase.
8. Arecont Cameras: One year from date of original retail purchase.
9. FMC series fiber-optic media converters and associated accessories: Lifetime warranty.
10. 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.
11. 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.
- For camera products supplied without a lens, extreme care should be used when mounting a lens on these products. Damage to the product due to incorrectly mounted lenses will invalidate this limited hardware warranty.
- 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 effective August 1, 2015.

**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](http://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](http://www.vicon-security.com)

