

User Guide

ROUGHNECK V-CELL-HD-B Corner-Mount Network Camera



XX247-12-03



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.

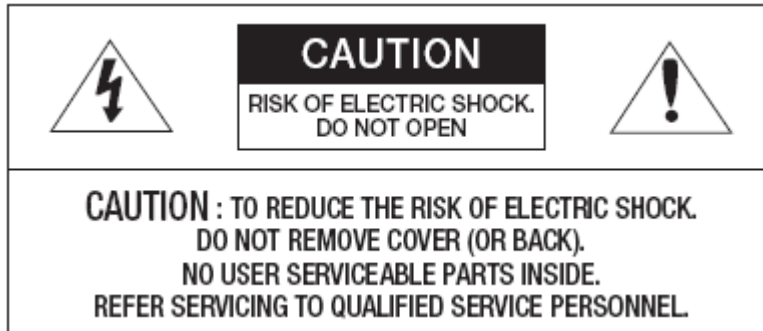
Document Number: 8009-8247-12-03 Product specifications subject to change without notice. Issued: 2/20 Copyright © 2020 Vicon Industries Inc. All rights reserved.

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

WARNING

TO REDUCE THE RISK OF FIRE OR ELECTRIC SHOCK, DO NOT INSERT ANY METALLIC OBJECT 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.



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.

PRECAUTIONS

Safety ----- Installation -----

Should any liquid or solid object fall into the cabinet, unplug the unit and have it checked by the qualified personnel before operating it any further.

Unplug the unit from the wall outlet if it is not going to be used for several days or more. To disconnect the cord, pull it out by the plug. Never pull the cord itself.

Allow adequate air circulation to prevent internal heat build-up. Do not place the unit on surfaces (rugs, blankets, etc.) or near materials (curtains, draperies) that may block the ventilation holes.

Height and vertical linearity controls located at the rear panel are for special adjustments by qualified personnel only.

Before installation, carefully read the manual to ensure correct operation and setup, heeding all warnings and instructions.

Do not install the device near any heat sources such as radiators, heat registers, stoves, or other equipment (including amplifiers) that produce heat.

Only use attachments/accessories specified by the manufacturer.

Do not install the device in a place where it is exposed to gas or oil.

Cleaning -----

Clean the unit with a slightly damp soft cloth. Use a mild household detergent. Never use strong solvents such as thinner or benzene as they might damage the finish of the unit.

Retain the original carton and packing materials for safe transport of this unit in the future.

FCC COMPLIANCE STATEMENT

INFORMATION TO THE USER: 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.

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.

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

1. Description	6
1.1 Components	6
1.2 Key Features	7
2. Installation	8
2.1 Overview	8
2.2 Unpacking and Inspection	11
2.3 Physical Inspection	11
2.3 Network Connection and IP Assignment	14
3. Operation	15
3.1 Access from a browser	15
3.2 Access from the internet	16
3.3 Setting the admin password over a secure connection	16
3.4 Live View Page	16
3.5 Network Camera Setup	18
3.5.1 Basic Configuration	18
1) Users	19
2) Network	20
3) Video & Image	21
4) Audio	23
5) Date & Time	24
3.5.2 Live View, Source	25
3.5.3 Video & Image	26
3.5.4 Audio	34
3.5.5 Event	34
1) Event-In	34
2) Event-Out	44
3) Event Map	51
3.5.6 System	53
1) Information	53
2) Security	54
3) Date & Time	59
4) Network	60
5) Language	69
6) Maintenance	69
7) Support	71
3.6 Playback	72
3.7 Help	74
3.8 Resetting to the factory default settings	75
4. Appendix	76
4.1 Troubleshooting	76
4.2 Alarm Connection	77
4.3 Preventive Maintenance	77
4.4 Product Specification	78

1. Description

The information in this manual provides quick installation and setup procedures for the V-CELL-HD-B of High-Security Corner-Mounted 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. Refer to the complete manual for detailed information. Always refer to Vicon's website to assure you have the most up-to-date manual, <http://www.vicon-security.com>.

The Roughneck® V-CELL-HD-B high-security camera is an integrated housing, camera, lens and IR illuminators system specifically designed for use in custodial suites and prison cells. It is available in an IP version that is fully compatible with all Vicon Valerus® and ViconNet® systems; its ONVIF certification provides an open-platform for integration into other video management systems.

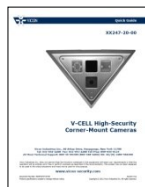
The housing is designed to fit into a corner; once installed, the base plate should be permanently sealed to the wall so that the housing is ligature proof. The housing consists of a two part stainless steel assembly, a fixed base plate and a removable front plate, that allows ease of installation and servicing. The front plate is secured with security screws and has two polycarbonate windows to protect the camera and IR illuminators. The alarm input and alarm output can be used to connect various third party devices, such as door sensors and alarm bells.

1.1 Components

The system comes with the following components:



Camera unit



Installation Guide



Installation CD



Accessory Kit

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

1.2 Key Features

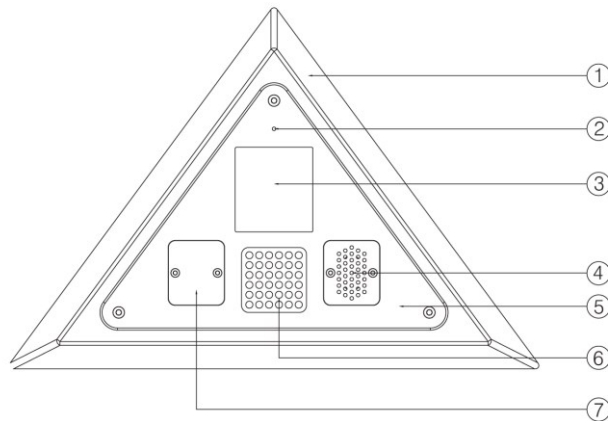
- **Brilliant video quality**
The network camera offers the highly efficient H.264 video compression, which drastically reduces bandwidth and storage requirements without compromising image quality. Motion JPEG is also supported for increased flexibility.
- **Triple streams**
The network camera can deliver triple video streams simultaneously at full frame rate in all resolutions up to 3MP (2045x1536) using Motion JPEG and H.264 (or MPEG-4). This means that several video streams can be configured with different compression formats, resolutions and frame rates for different needs.
- **Image setting adjustment**
The network camera also enables users to adjust image settings such as contrast, brightness and saturation to improve images before encoding takes place.
- **Intelligent video capabilities**
The network camera includes intelligent capabilities such as enhanced video motion detection. The camera's external inputs and outputs can be connected to devices such as sensors and relays, enabling the system to react to alarms and activate lights or open/close doors.
- **Micro-SD recording support**
The network camera also supports a micro-SD memory slot for local recording with removable storage.
- **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.
- **IR illumination**
36 IR LED illuminators (940nm with low visibility) light up to 66 ft (20m); intensity; adjustable.
- **Audio In/Out**
1 Mic/1 Speaker (G.711)
- **Power over Ethernet**
Support for Power over Ethernet (IEEE802.3af) enables the unit, as well as the camera module that is connected to it, to receive power through the same cable as for data transmission. This makes for easy installation since no power outlet is needed.
- **ONVIF**
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 customer-supplied power supply.

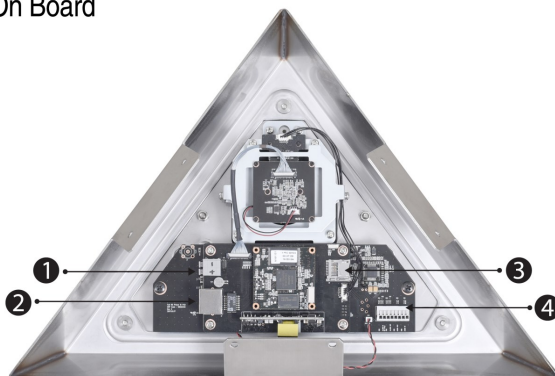
2.1 Overview

● Parts and Description



- ① Mounting Frame
- ② Mic
- ③ Camera/Lens
- ④ Speaker
- ⑤ Camera Bracket
- ⑥ IR Window & IR LED
- ⑦ Status LED

On Board



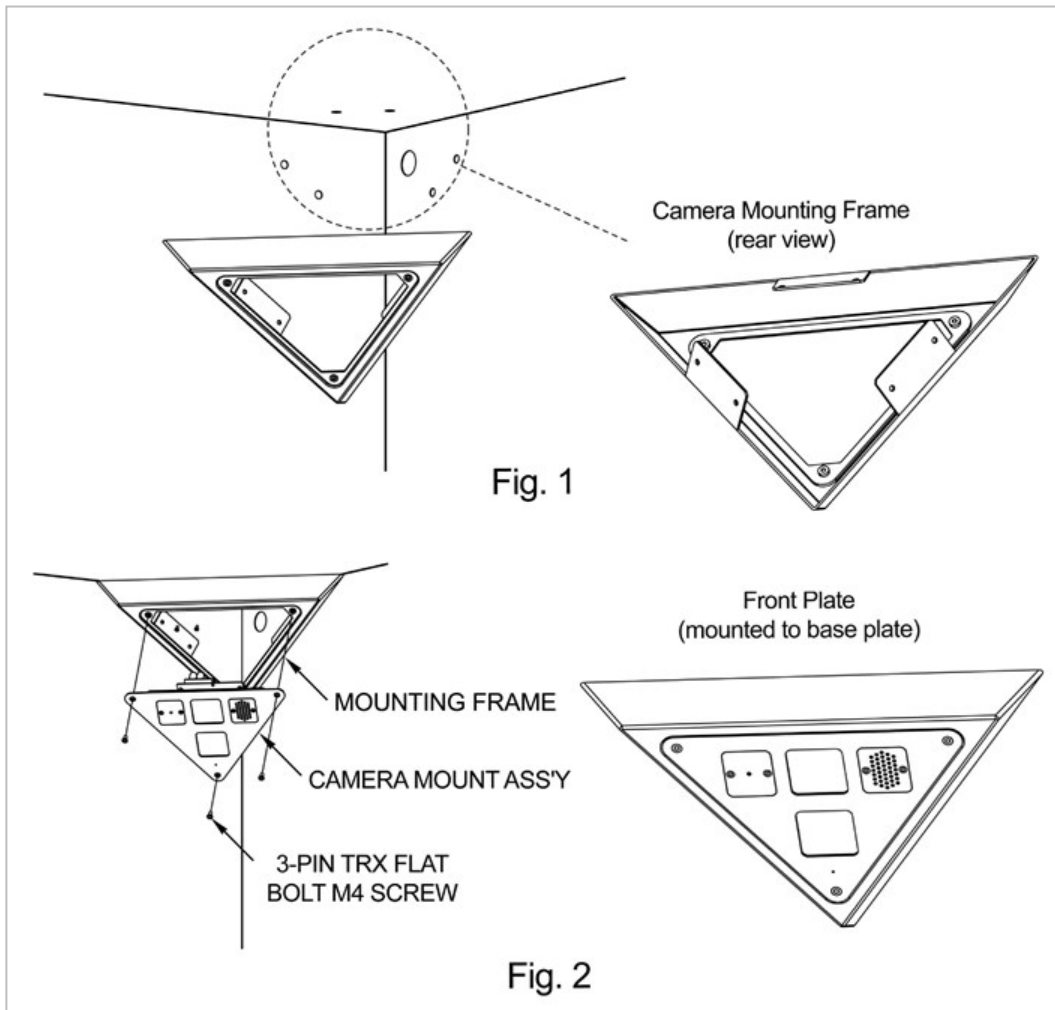
- ① Main Power 12 VDC (↑(-) pole / ↓(+) pole)
- ② RJ45 (PoE) Port
- ③ Micro-SD Card Slot
- ④ Alarm & Audio In/Out Port
- ⑤ Status LED

Upon boot-up, green and red LEDs are both on for a short time and then only green will be on. If red is lit, this indicates a failure (no picture); if flashing green and no red, this indicates that a good picture is displaying.

● Quick Installation

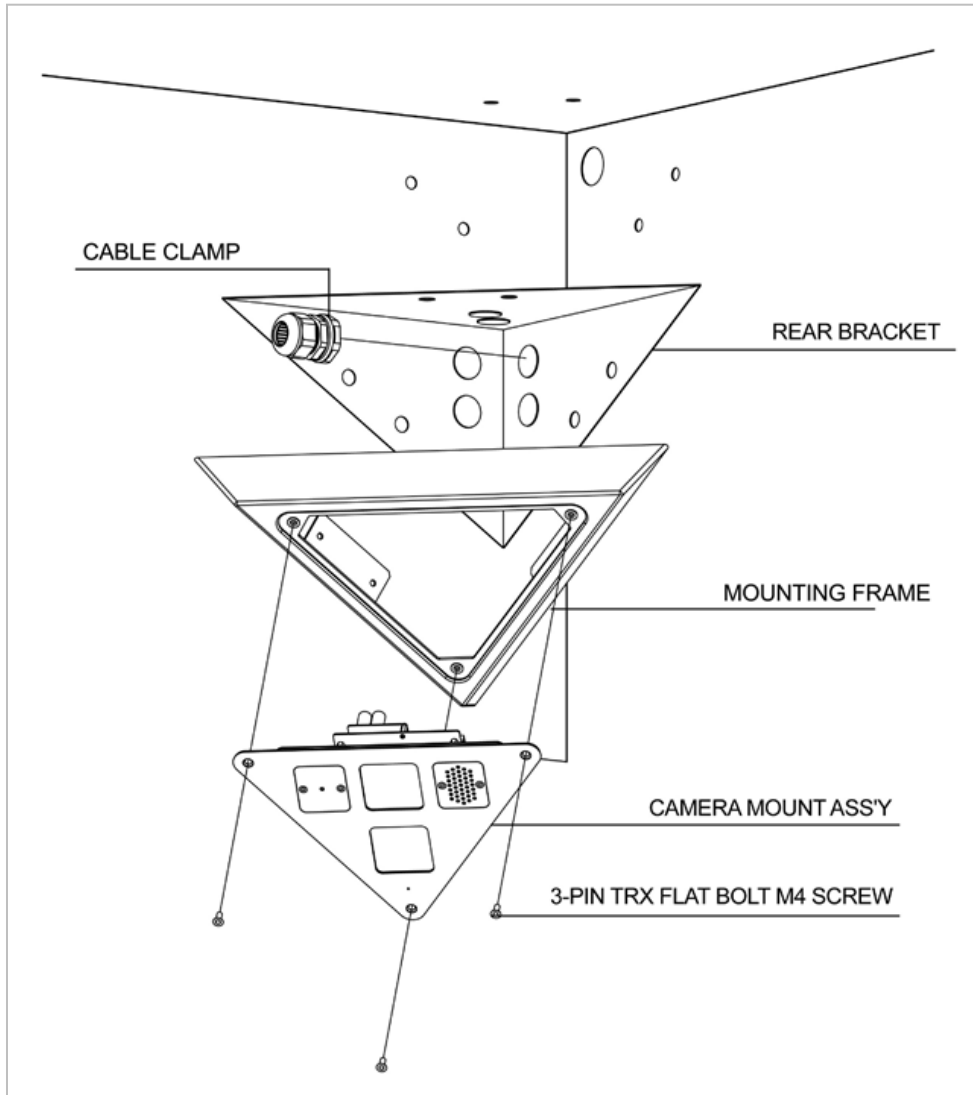
Below is an overview for installing the camera.

1) Installation (without Rear Cover)



1. Use camera mounting frame as template to mark mounting holes on mounting surface. (Fig.1)
2. Drill holes for mounting base and a minimum 3/4 in. hole for routing wires. (Fig.1)
3. Mount camera mounting frame using appropriate hardware for mounting surface. (Fig.2)
4. Route wires through hole in wall and out through base plate. (Fig.2).
5. Terminate wires to camera board.
6. Mount front plate to base plate. (Fig.2)

2) Installation (using Rear Cover)



1. Use rear cover as template to mark mounting and cable access holes.
2. Drill mounting and cable access holes in mounting surface.
3. Insert cable clamp into access hole, route cables through clamp and mount cover using appropriate hardware.
4. Use camera mounting frame to mark its mounting holes, drill holes and mount using appropriate hardware.
5. Terminate wires to camera board. Feed the excess wire back through cable clamp and tighten clamp.
6. Mount front plate to camera mounting frame.

Note: Installation of the rear cover is required for UL/Canadian UL compliance.

2.2 Unpacking and Inspection

All Vicon equipment is inspected and tested before leaving the factory. It is the carrier's responsibility to deliver the equipment in the same condition in which it left the factory.

Inspection for Visible Damage

Immediately inspect the cartons upon delivery. On all copies of the carrier's freight bill, make a note of any visible damage.

Make sure the carrier's agent (the person making the delivery) signs the note on all copies of the bill. If the agent does not have claim forms, contact the carrier's office.

Inspection for Concealed Damage

As soon as possible after delivery, unpack the unit and inspect it for concealed damage. Do not discard the carton or packing materials. If the unit is damaged, contact the carrier immediately and request forms for filing a damage claim. Make arrangements for a representative of the carrier to inspect the damaged equipment. If the equipment must be returned for repair, follow the Shipping Instructions at the end of this document.

2.3 Physical Installation

The Camera is designed to fit into a corner where two walls and a ceiling meet. It is fastened to both walls and the ceiling. Refer to Figure 1. Cable access is provided by removing the front plate. The camera has an adjustable mount that may be tilted slightly to give a precise angle of view. A 2.3 mm wide angle lens enables the camera to view the cell with no "blind spots;" 36 IR LED illuminators are provided to light up to 66 ft (20 m).

The wall/ceiling material must provide suitable strength to support the weight of the unit (3.5 lb/1.6 kg). Be sure the area around the selected location is clear of obstacles (such as steel beams, headers, pipes, electrical wiring, etc.) that would interfere with mounting. All cables must be routed to the installation location. Before beginning installation, read the Cable Recommendations at the end of this manual and verify that the accessory pack contains the items listed in below table.

Item	Quantity	Function
No. 20 Torx Bit	1	Use to remove and install tamperproof screws from front plate
No. 20 Torx Bit	1	Use to remove and install tamperproof screws from front plate access cover plate
2-Pin Terminal Block	1	Use to make power cable connections
Back Cover	1	Fire barrier; required for UL/cUL compliance
Quick Guide/Documentation CD/ ViconNet CD	1	Installation and operation instructions; ViconNet setup CD

● Mounting the Housing

The housing consists of two main assemblies, the camera mounting frame and the removable front plate, where the camera and all electronics are mounted. The front plate is secured to the base plate with Resistorx tamperproof screws. A special bit is supplied in the accessory pack for removing and replacing these screws. When the installation is complete, retain the Torx bit in case access to the interior of the housing is required later. Additionally, a rear cover is supplied for those installations requiring Canadian UL compliance or extra protection from fire.

1) Installation without the rear cover:

1. Remove the front plate using the no. 20 Torx bit provided; retain the screws in a safe place. Using the camera mounting frame as a template, mark the locations of the mounting holes on the three mounting tabs (2 holes per tab). Open a hole in the wall or ceiling to accommodate routing the cables to the camera.
2. Route all necessary cables to the location if not already done so.
3. Drill suitable holes for the hardware selected appropriate for the wall/ceiling material. The use of No. 8 (or 4 mm metric) mounting hardware is recommended. Use hollow-wall anchors or, if the housing is being mounted on a sheet metal surface, use rivet nuts.
4. Secure the camera mounting frame to the wall/ceiling with fasteners appropriate for the mounting surface. Route the cables through the access hole in the wall or ceiling.
5. When the camera mounting frame is secured to the surface, apply an epoxy security sealant around the perimeter of the base plate where it meets the ceiling/wall. [Vicon recommends DynaPoxy™ EP1200 (US) or Arbokol 1025 (UK) or equivalent for this purpose.]

2) Installation with the rear cover:

Note: The installation corner must be sharp and clean; if necessary, clean any excess material from the installation location.

1. Remove the front plate using the no. 20 Torx bit provided; retain the screws in a safe place.
2. Select the cable access hole in the rear cover to be used (6 provided) and knockout the hole. Place the rear cover in the corner; using it as a template, mark the locations of the three (3) mounting holes and the cable access hole. Remove it from the corner.
3. Drill suitable mounting holes and open the hole to accommodate routing the cables to the camera in the wall/ceiling. Be sure the cable access hole is large enough to accommodate the cable clamp.
4. Route all necessary cables to the location if not already done so. Fasten the cable clamp (provided) into the cable access knockout hole so that the clamp is on the inside of the rear cover. Route cables through the access hole and through the rear cover; be sure to allow enough cable length to make connections to the camera board. Mount the rear cover to the wall/ceiling through the 3 holes provided; use hardware appropriate for the mounting surface.
5. Using the camera mounting frame as a template, insert it into the rear cover and mark the mounting holes on the 3 tabs (2 holes per tab) that align with the holes in the rear cover; drill suitable mounting holes. Attach the camera mounting frame onto the wall/ceiling and secure it using appropriate hardware for the mounting surface. The use of No. 8 (or 4 mm metric) mounting hardware is recommended. Use hollow wall anchors or, if the housing is being mounted on a sheet metal surface, use rivet nuts.
6. Make cable connections to the camera board. See instructions below. Adjust the cable length as necessary and secure the cable clamp.

Caution: Installation of the rear cover is required for UL/Canadian UL compliance.

7. When the camera mounting frame assembly is secured to the surface, apply an epoxy security sealant around the perimeter of the base plate assembly where it meets the ceiling/wall. [Vicon recommends DynaPoxy™ EP1200 (US) or Arbokol 1025 (UK) or equivalent for this purpose.]

● Cable Connections

All cabling is done to the boards located on the back of the front plate.

Note: Vicon systems and components, like most electronic equipment, require a clean, stable power source. Voltage irregularities such as surges, drops, and interruptions can affect the operation of your equipment and, in severe cases, damage certain components.

1) Micro SD memory slot on the Board

Card Slot for Micro SD memory: Socket "J2." (SD card customer-supplied.)

2) Connecting to the RJ-45

Connect a standard RJ-45 cable to the network port of the network camera. Generally a crossover cable is used for direct connection to a PC, while a direct cable is used for connection to a hub.

3) Connecting Alarms

- **AI (Alarm In):**

External devices can be used to signal the network camera to react upon events. Mechanical or electrical switches can be wired to the AI (Alarm In) and G (Ground) connectors.

- **G (Ground):**

Connect the ground side of the alarm input and/or alarm output to the G (Ground) connector.

- **Alarm Out:**

The network camera can activate external devices such as buzzers or lights. Connect the device to the AO (Alarm Out) and G (Ground) connectors.

4) 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.
- The heater can be powered by a 12 VDC, or PoE power source.
- For the power specifications, refer to the Appendix, Product Specification.
- If PoE and 12 VDC are both applied, the camera will be supplied with power from PoE. If PoE power goes down, 12 VDC will take over.

5) IR Control

To adjust the intensity of the IR illuminators, use the Day & Night menu in the web browser.

● Final Installation

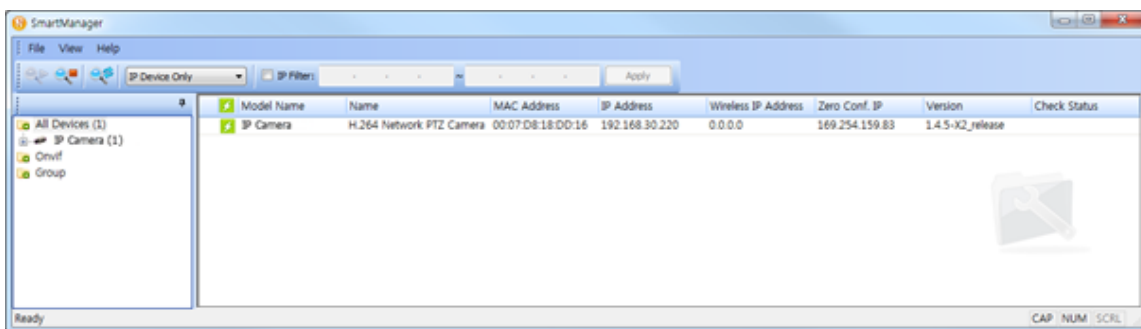
When all connections are made, secure the front plate to the base plate using the security screws previously removed using no. 20 Torx bit.

2.4 Network Connection and IP assignment

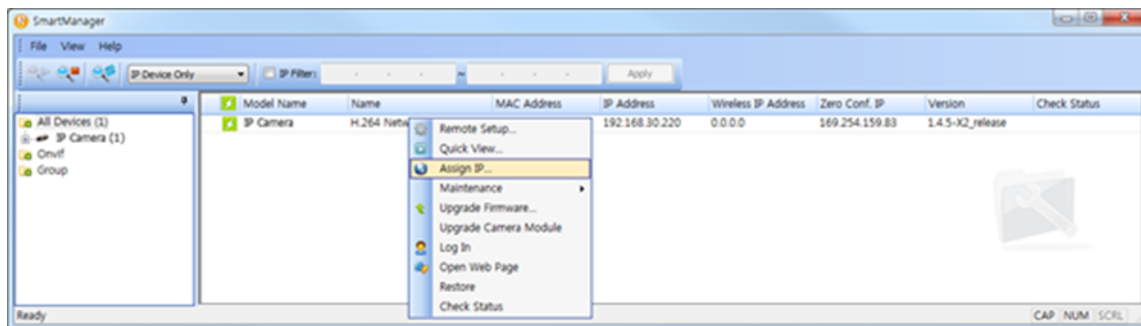
The network camera is designed for use on an Ethernet network and requires an IP address for access. Most networks today have a DHCP server that automatically assigns IP addresses to connected devices. By the factory default, your camera is set to obtain the IP address automatically via DHCP server.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

3. Operation

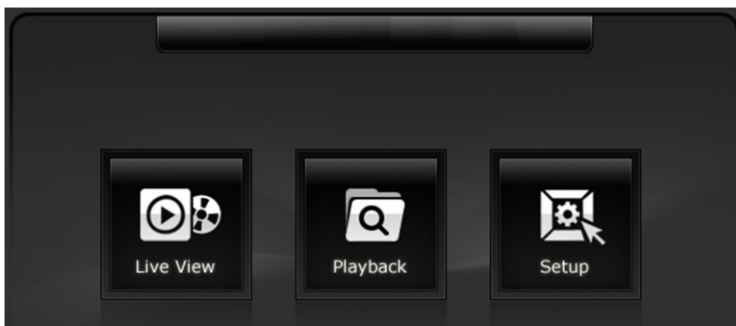
The network camera can be used with Windows® operating system and browsers. The recommended browsers are Internet Explorer®, Safari®, Firefox®, Opera® and Google® Chrome® with Windows.

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

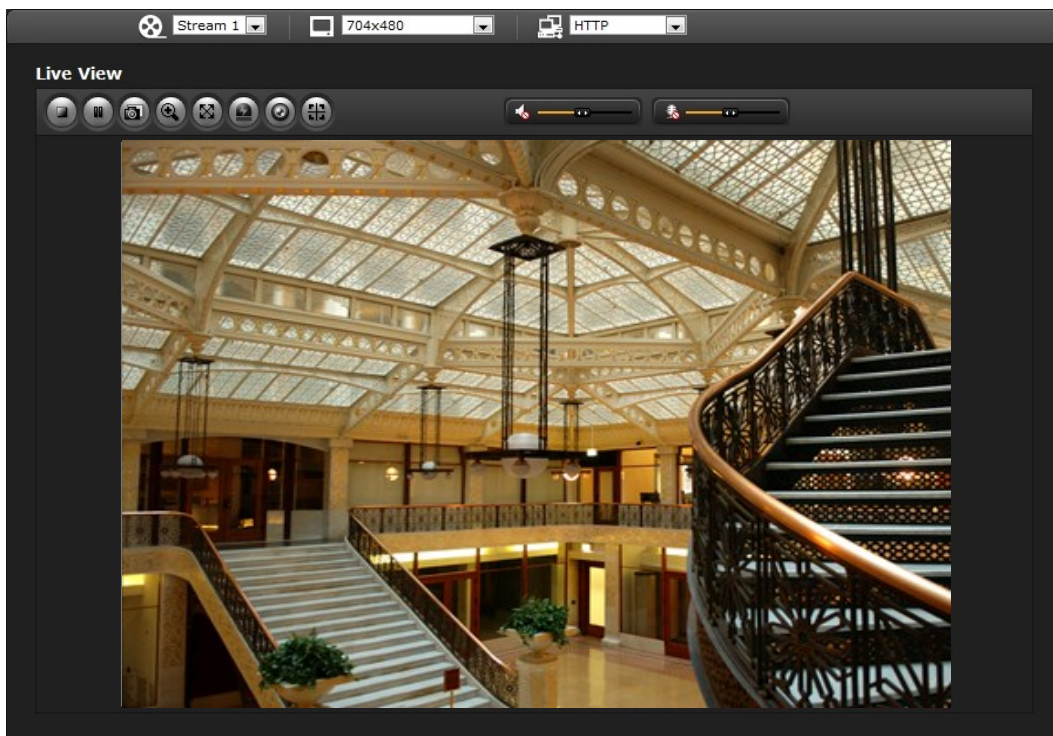
Note: Some screens may appear different (i.e., color scheme) depending on the firmware version, but the functionality is the same or similar.

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 "3.5.6 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. See section "3.8 Resetting to the Factory Default Settings" for more details.



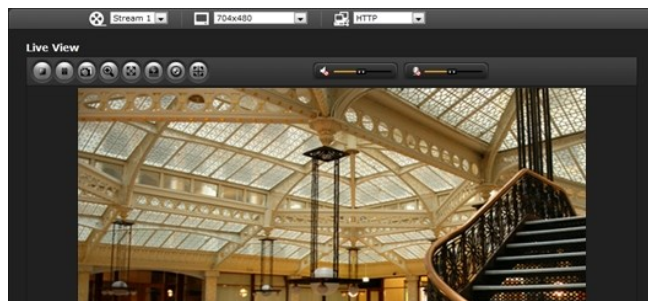
To prevent network eavesdropping when setting the admin password, it can be done via an encrypted HTTPS connection, which requires an HTTPS certificate (see note below).

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 "3.5.6 System > Security > HTTPS".

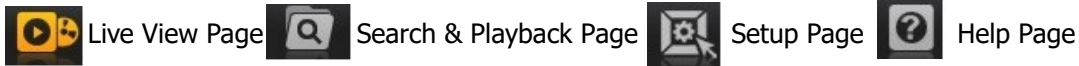
Note: HTTPS (Hypertext Transfer Protocol over SSL) is a protocol used to encrypt the traffic between web browsers and servers. The HTTPS certificate controls the encrypted exchange of information.

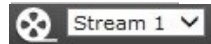
3.4 Live View Page


The Live View page provides several screen modes: 2048x1536, 1920x1080, 1280x1024, 1280x720, 704x480 (576), 640x480, 352x240 (288), and 320x240. Select the most suitable mode in accordance with your PC specifications and monitoring purposes.




1) General controls



 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.

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

 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 pauses the video stream being played.



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



The Digital Zoom button activates a zoom-in or zoom-out function for 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.



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



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

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, MPEG-4 and Motion JPEG video streams and to the list of available video streams. Other applications and clients can also access these video streams/images directly, without going via the Live View page.

3.5 Network Camera Setup

This section describes how to configure the network camera 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.

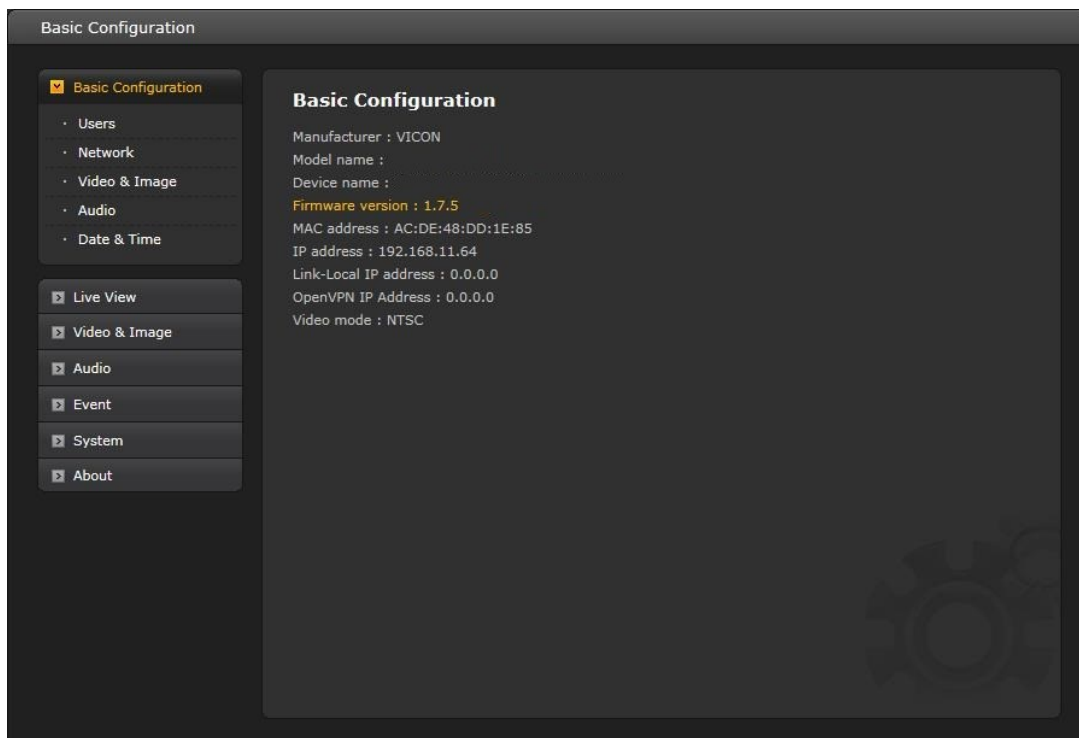


When accessing the network camera for the first time, the "Admin Password" dialog appears. Enter your admin name and password, set by the administrator.

Note: If the password is lost, the network camera must be reset to the factory default settings. See section "3.8 Resetting to the Factory Default Settings". The default administrator username is "ADMIN" and password is "1234".

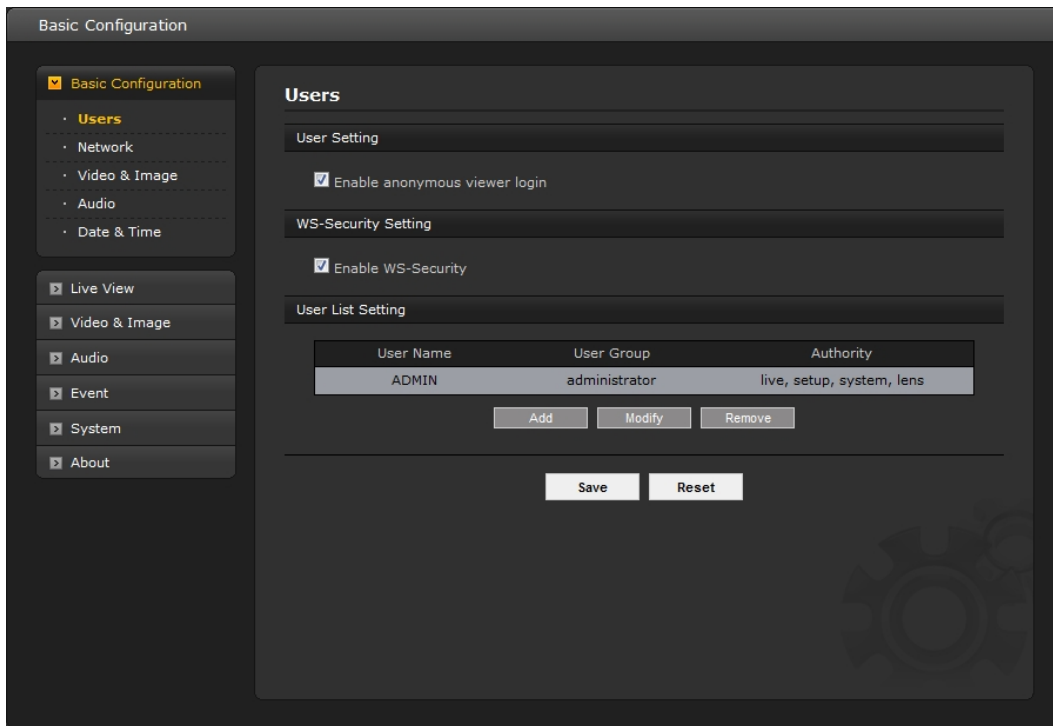
3.5.1 Basic Configuration

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.

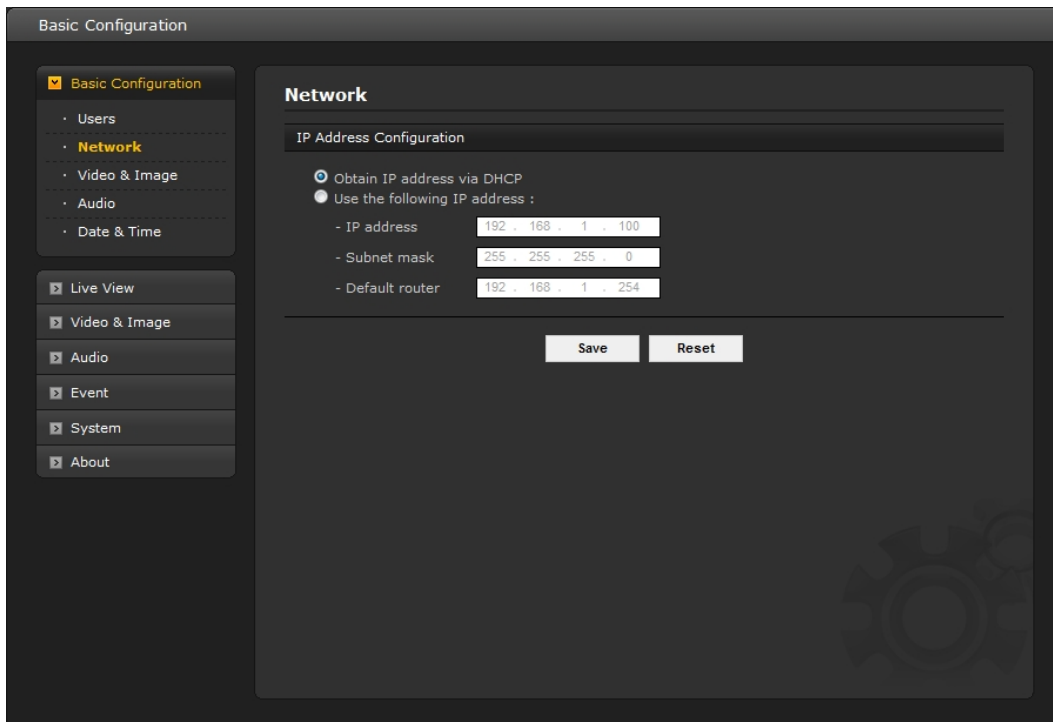
An administrator can Add, Modify or Remove users in the list by clicking the appropriate button. Click Save to save the settings or Reset to cancel.

- **Enable anonymous viewer login:** Check the box to use the webcasting features. Refer to "3.5.3 Video & Image" for more details.
- **Enable WS-Security:** Do not check this box to connect and monitor the network camera through Vicon's viewing software using drivers older than 935.

Note: WS-Security is an open format for signing and encryption of message parts, for supplying credentials in the form of security tokens, and for security passing those tokens in a message.

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.

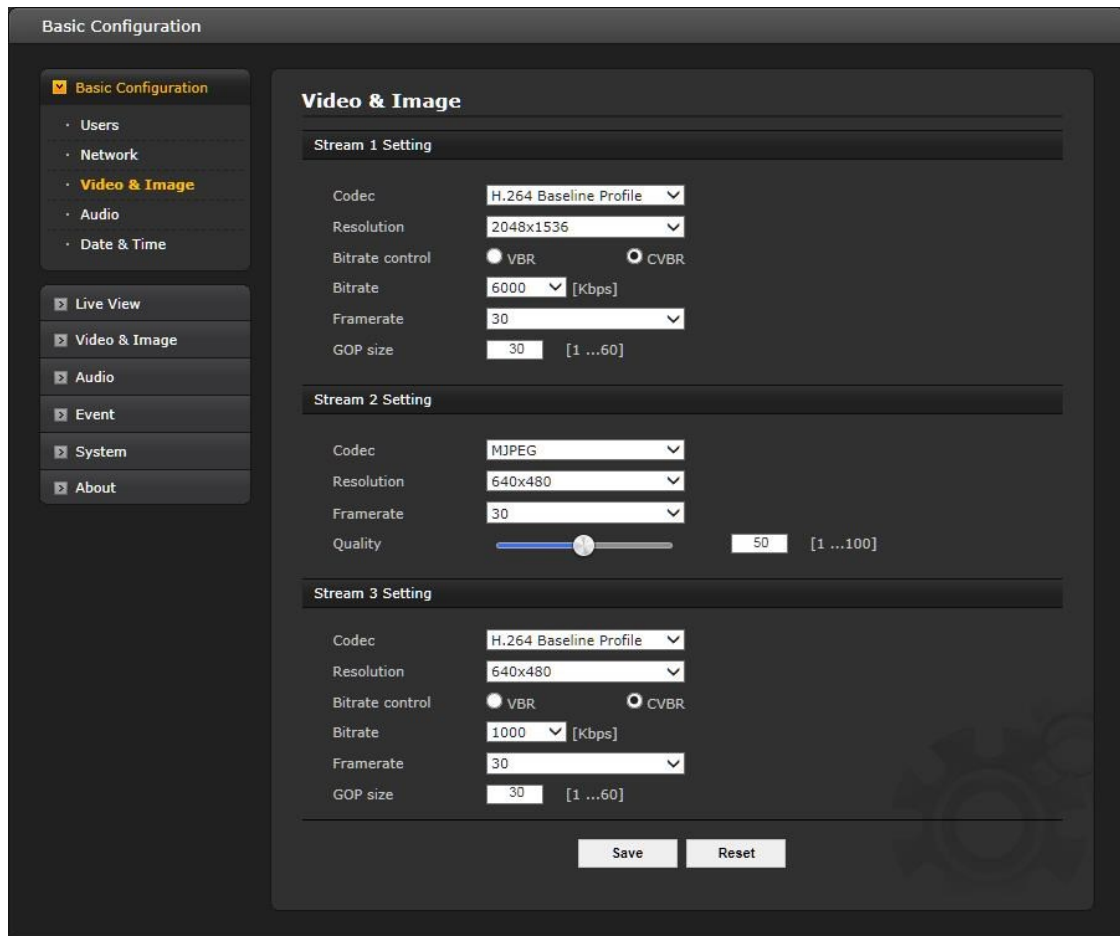


- **Obtain IP address via DHCP** - Dynamic Host Configuration Protocol (DHCP) is a protocol that lets network administrators centrally manage and automate the assignment of IP addresses on a network. DHCP is enabled by default. Although a DHCP server is mostly used to set an IP address dynamically, it 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



- **Stream1 Setting**

- **Codec:** The codec supported in Stream 1 is H.264.
There are 3 pre-programmed stream profiles available for quick set-up. Choose the form of video encoding you wish to use from the drop-down list:
- * **H.264 HP (High Profile):** 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 MP (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 BP (Baseline Profile):**

Originally intended as the mainstream consumer profile for broadcast and storage applications, the importance of this profile faded when the High Profile was developed for those applications.

- **Resolution:**

Resolution enables users to determine a basic screen size when having access through the Web Browser or PC program. The screen size control provides in several modes, 2048x1536, 1920x1080, 1280x1024, 1280x960, 1280x720, 1024x768, 704x480(576), 640x480, 640x360, 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 Variable Bit Rate (VBR) or Constrained Variable BitRate (CVBR). VBR adjusts the bit rate according to the image complexity, using up bandwidth for increased activity in the image, and less for lower activity in the monitored area. Limiting the maximum bit rate helps control the bandwidth used by the H.264 video stream. Leaving the Maximum bit rate as unlimited maintains consistently good image quality but increases bandwidth usage when there is more activity in the image. Limiting the bit rate to a defined value prevents excessive bandwidth usage, but images are degraded when the limit is exceeded.

* **VBR:** unlimited maximum bitrate.

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

- **Bitrate:** Maximum bitrate for CVBR in the range of 100kbps ~ 8Mbps.
This is disabled if Bitrate control is set to VBR.

- **Frame rate:**

Upon 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. Such act 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.

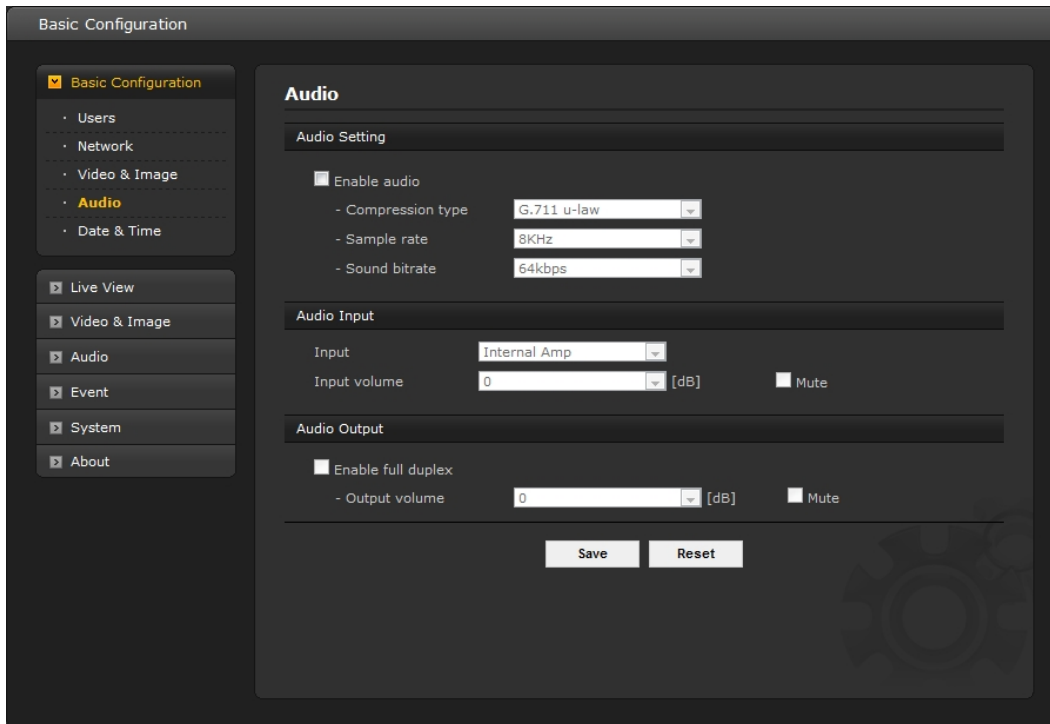
- **MJPEG frame rate:** Same as the stream1 setting.

- **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) Audio



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

- **Audio Setting**

- **Enable audio:**

Check the box to enable audio in the video stream.

- **Compression type:**

Select the desired audio compression format, G711. The "u-law" is for North America and Japan; the "a-law" is for Europe and the rest of the world.

- **Sample rate:**

Select the required Sample rate (number of times per second the sound is sampled). The higher the sample rate, the better the audio quality and the greater the bandwidth required.

- **Sound bitrate:**

Depending on the selected encoding, set the desired audio quality (bitrate). The settings affect the available bandwidth and the required audio quality.

- **Audio Input**

Audio from an internal or external line source can be connected to the I/O terminal of the network camera.

- **Input:** User can select amplifier between internal Amp or external Amp.

- **Input volume:**

If there are problems with the sound input being too low or high, it is possible to adjust the input gain for the microphone attached to the network camera. A Mute button is provided; check the box to hear no sound on the device.

- **Audio Output**

- **Enable full duplex:**
Check the box to enable Full Duplex mode. This means that audio (talk and listen) can be transmitted and received at the same time, without having to use any of the controls. This is just like having a telephone conversation. A Mute button is provided; check the box to hear no sound from the speakers.
This mode requires that the client PC has a sound card with support for full-duplex audio.
- **Output volume:**
If the sound from the speaker is too low or high it is possible to adjust the output gain for the active speaker attached to the network camera.

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

5) Date & Time

The screenshot shows the 'Basic Configuration' web interface. On the left is a navigation menu with options: Basic Configuration (selected), Users, Network, Video & Image, Audio, Date & Time, Live View, Video & Image, Audio, Event, System, and About. The main content area is titled 'Date & Time' and contains the following settings:

- Current Server Time:** Date: 2013-08-09, Time: 14:53:11
- New Server Time:**
 - Time zone:** (GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London (dropdown menu). A checkbox for 'Automatically adjusts for daylight saving time changes' is present.
 - Time mode:**
 - Synchronize with computer time: Date: 2013-08-09, Time: 14:53:13
 - Synchronize with NTP server: NTP server: time.nist.gov, NTP Interval: 12 [hour]
 - Set manually: Date: 2013-08-09, Time: 14:53:04
- Date & Time Format:**
 - Date Format: YYYY-MM-DD (dropdown menu)
 - Time Format: 24 Hour (dropdown menu)

At the bottom of the settings area are 'Save' and 'Reset' buttons.

- **Current Server Time**
This displays the current date and time (24h clock). The time can be displayed in 12h clock format (see below).
- **New Server Time**
 - **Time zone:** Select your time zone from the drop-down list. If you want the server clock to automatically adjust for daylight savings time, check the box "Automatically adjust for daylight saving time changes".

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.

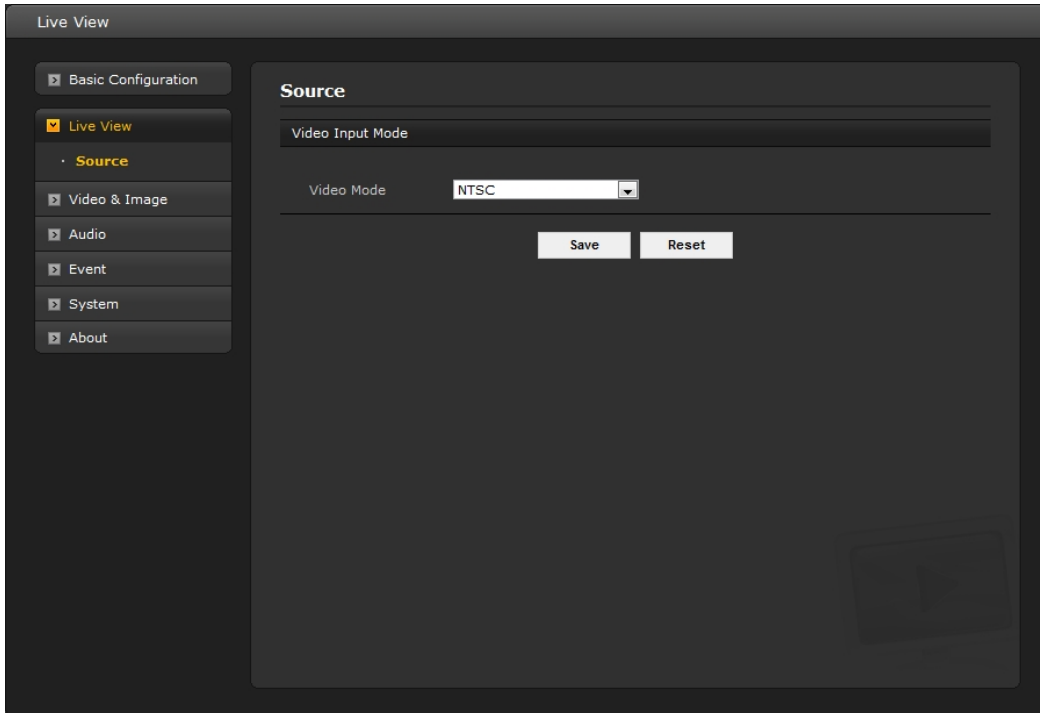
- **Date & Time Format**

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 Live View, Source



Use the Video Mode drop-down list to select the video input mode, NTSC or PAL. This defines the Video Output Port for the Service Monitor.

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

3.5.3 Video & Image

▼ Basic

Video & Image

- Basic Configuration
- Live View
- Video & Image**
 - Basic**
 - Privacy Masking
 - Webcasting
 - Camera Setup
 - OSD
- Audio
- Event
- System
- About

Video & Image - Basic

Stream 1 Setting

Codec: H.264 Baseline Profile
Resolution: 2048x1536
Bitrate control: VBR CVBR
Bitrate: 6000 [Kbps]
Framerate: 30
GOP size: 30 [1 ...60]

Stream 2 Setting

Codec: MJPEG
Resolution: 640x480
Framerate: 1
Quality: 30 [1 ...100]

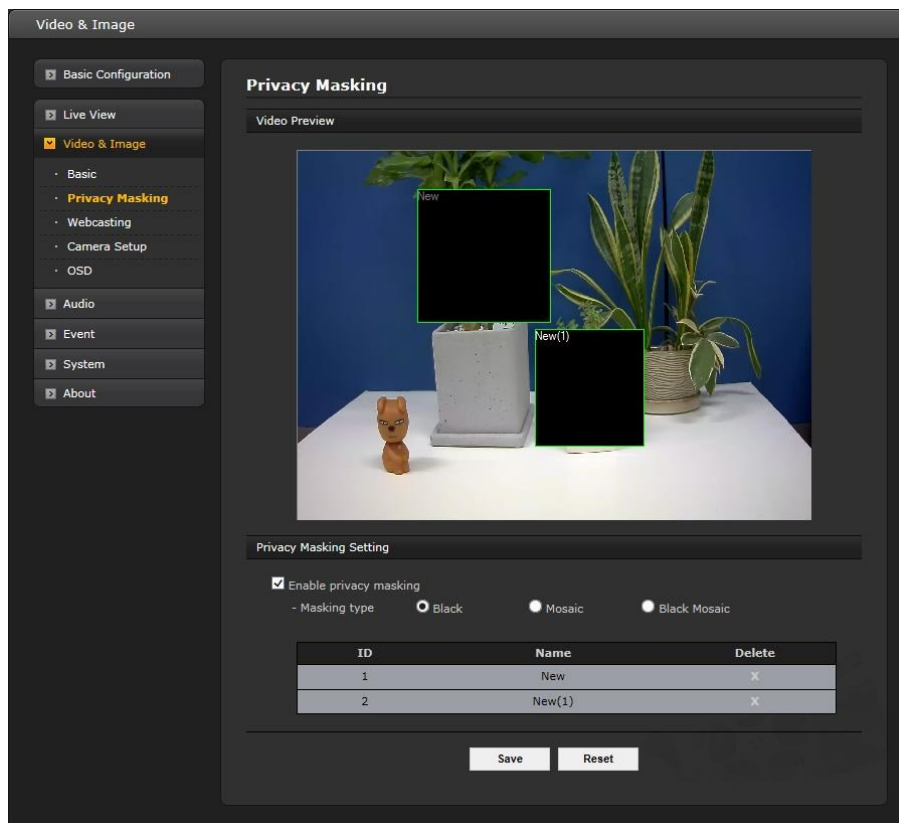
Stream 3 Setting

Codec: H.264 Baseline Profile
Resolution: 640x480
Bitrate control: VBR CVBR
Bitrate: 1000 [Kbps]
Framerate: 30
GOP size: 30 [1 ...60]

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

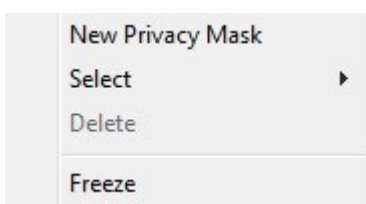
▼ Privacy Masking

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 color of privacy masks is black.



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:

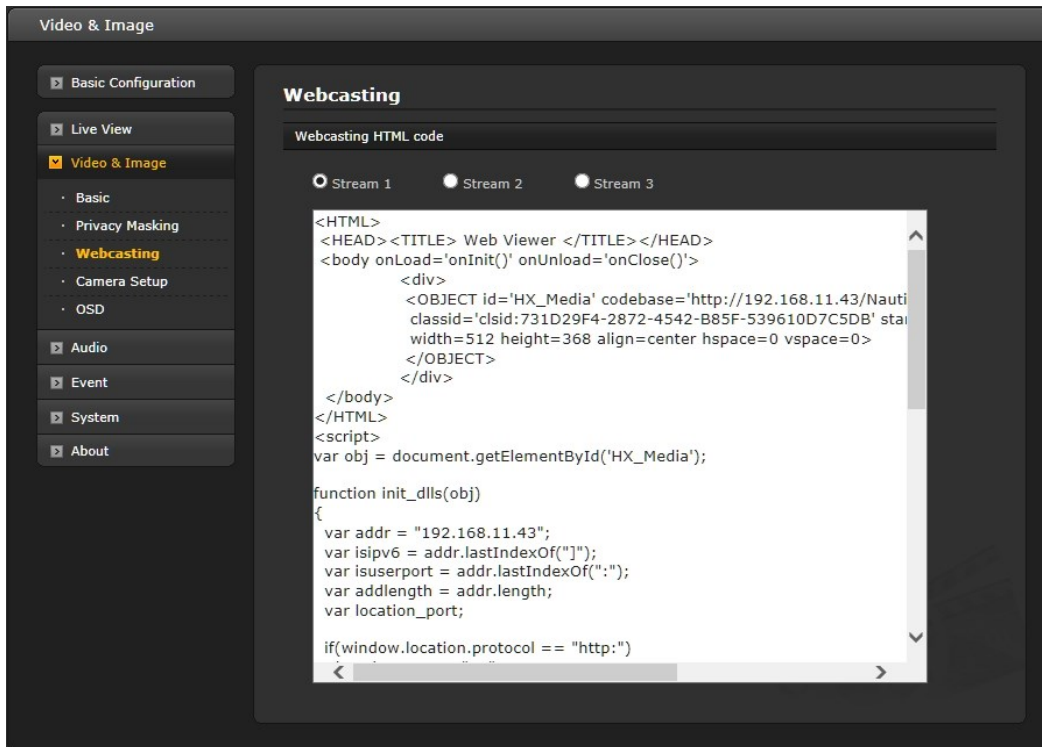
1. Click the right button of mouse to display the mouse menu.
2. Select New Privacy Mask in the mouse menu.
3. Click and drag to designate a mask window area.

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.

▼ Webcasting

The network camera can stream live video to a website. Copy the HTML code generated on the screen and paste it in page code of the website you want to display live video.



Note: To use webcasting service, the Enable Anonymous viewer login option must be checked. Refer to “3.5.1 Basic Configuration > Users” for more details.

▼ Camera Setup

The screenshot displays the 'Camera Setup' interface within a 'Video & Image' configuration window. The interface is organized into several sections:

- Exposure Control:** Includes Mode (Automatic, Flicker-free 50Hz, Flicker-free 60Hz), Value (slider), Max. gain (Low, Middle, High), Shutter (Automatic, Fixed), Max. shutter (1/30 [s]), and checkboxes for automatic IRIS adjustment, high light compensation, backlight compensation, and wide dynamic range (with Low, Middle, High strength options).
- White Balance Control:** Includes Mode (Automatic, Fixed incandescent, Fixed fluorescent, Fixed outdoor, Manual).
- Image Appearance:** Includes sliders for Brightness, Contrast, Saturation, Hue, and Sharpness, and checkboxes for flip horizontally, mirror image, noise reduction (with Low, Middle, High levels), defog, aisle, and simple distortion compensation.
- Day & Night Control:** Includes Mode (Automatic, Day, Night), Threshold (Low, High), and a checkbox for Fine Focus sync with Day & Night.
- IR Control:** Includes a checkbox for Enable IR and a Max. Strength slider.
- Profile Schedule:** A table showing the activation of profiles across a 24-hour cycle.

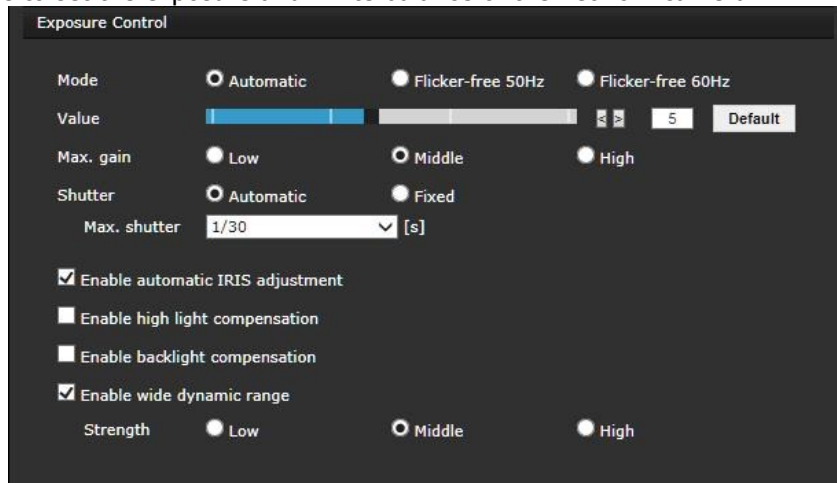
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	Night Mode	
Profile1																									off	
Profile2																										off
Profile3																										off
Profile4																										off

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

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

- **Exposure Control**

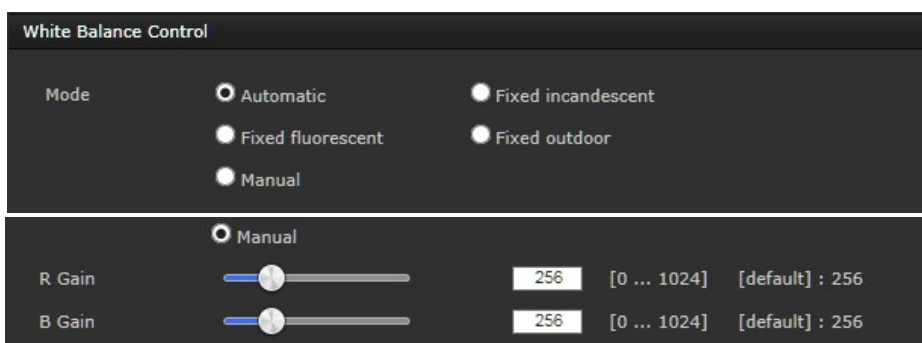
User can access to set the exposure and white balance of the network camera.



- **Mode:** Used to control the amount of light detected by the camera sensor based on settings for light conditions. Select exposure mode between automatic and Flicker-free.
- **Value:** Used to fine tune the Exposure level.
- **Max. gain:** Sets maximum gain if Mode is automatic.
- **Shutter:** Select the shutter mode between automatic and fixed.
- **Max. shutter:** Select maximum shutter speed if shutter is in automatic mode. The drop-down shows selectable maximum shutter speeds depending on the exposure selection in Mode.
- **Enable automatic IRIS adjustment:** Activates autoiris function.
- **Enable backlight compensation:** Activates BLC function which cannot be used with WDR.
- **Enable wide dynamic range:** Activates WDR which cannot be used with BLC or Defog function.

- **White Balance Control**

This adjusts the relative amount of red, green and blue primary colors in the image so that the neutral colors are reproduced correctly. The camera can be set to automatically adjust for the type of light and compensate for its color. Alternatively, the type of light source can be set manually.



Select the white balance setting suitable for the lighting used for your camera. The available options are:

- **Automatic:** Automatic identification and compensation for the light source color. This can be used in most situations and is the recommended setting.
- **Fixed Incandescent:** Fixed color adjustment, ideal for a room with incandescent (glowing) lighting and good for a normal color temperature around 2600K.
- **Fixed Fluorescent:** Fixed color adjustment; good for fluorescent lighting with a color temperature around 4000K to 5000K.
- **Fixed Outdoor:** Fixed color adjustment for sunny environment, with a color temperature around 6500K to 7500K.

- **Manual:** User can separately set R Gain and B Gain in manual mode.
- * **R Gain: Red color gain in the range of 1-255 with default value 256**
- * **B Gain: Blue color gain in the range of 1-255 with default value 256.**

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

- **Image Appearance**

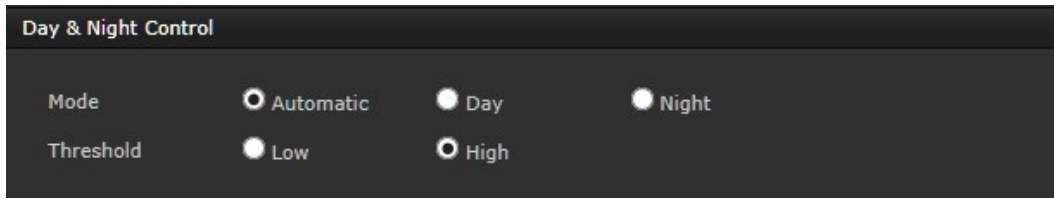
User can setup image related controls.



Brightness/Contrast/Saturation/Hue/Sharpness: User can either use slide bar or type the number.
 Flip/Mirror/NR/Defog/DIS/aisle: User can select individual function and level.

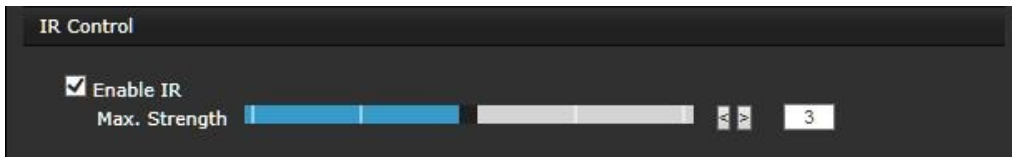
- **Brightness:** The image brightness can be adjusted in the range 1-10, where a higher value produces a brighter image.
- **Contrast:** Adjust the image's contrast by raising or lowering the value in this field.
- **Saturation:** Select an appropriate level by entering a value in the range 1-10. Lower 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.
- **Enable flip image:** Check this checkbox to flip the image.
- **Enable mirror image:** Check this checkbox to mirror the image.
- **Enable Noise Reduction:** Check this box to activate the noise reduction.
- **Enable defog:** Check this checkbox to active the defog function.
- **Enable aisle:** Check this checkbox to aisle the image.

- **Day & Night Control**



- **Mode:** Select the day & night mode from three modes.
- * **Automatic:** Normally works in day mode; switches automatically to night mode in a dark place.
- * **Day:** Always works in day mode.
- * **Night:** Always works in night mode.
- **Threshold:** Controls the how fast the change is from day to night or night to day. Select high or low.

- **IR Control (For IR models only)**



- **Enable IR:** Set this checkbox to activate IR operation.
- * **Max Strength:** Select a value in the drop-down list to tune the strength. The default setting is 3.

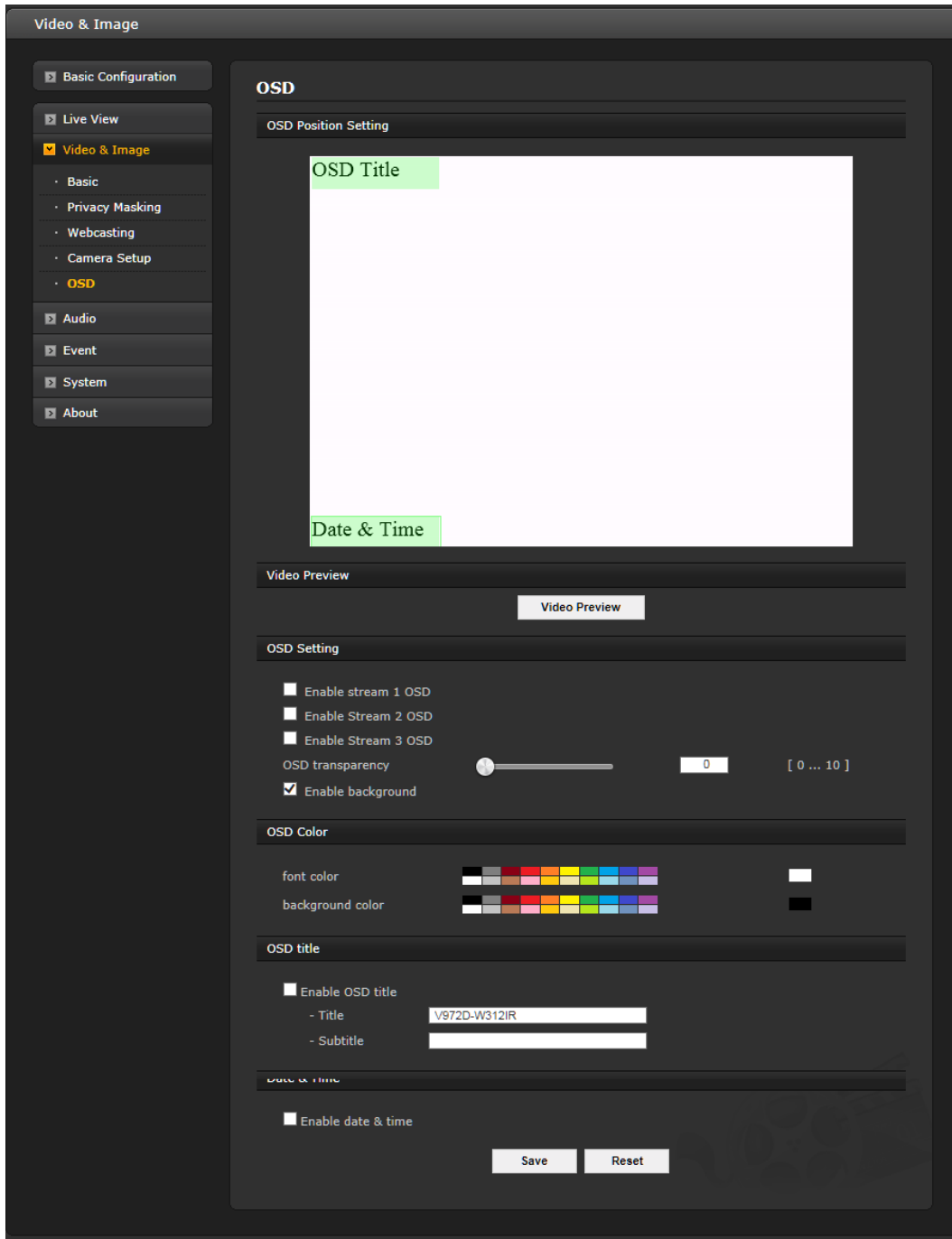
- **Profile Schedule**

User can make schedule for 4 different profiles.

Profile Schedule																									
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	Night Mode
Profile1																									<input type="checkbox"/> off
Profile2																									<input type="checkbox"/> off
Profile3																									<input type="checkbox"/> off
Profile4																									<input type="checkbox"/> off

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

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

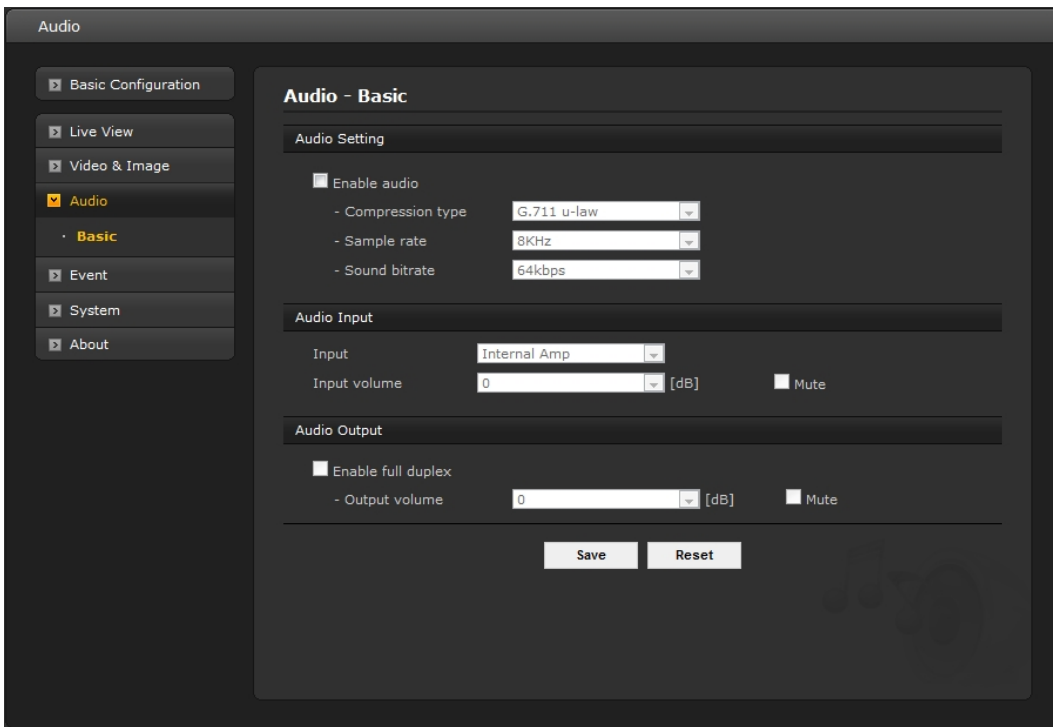


- **Video Preview:** User can check the position of OSD on actual video via preview popup window.
- **OSD Setting:** User can determine show or hide OSD for each stream. Also user can set the transparency level of OSD by slide bar or type in number.
- **OSD title:** User can show or hide OSD title, and can change OSD title by type in. The default is the model name of the camera.
- **Date & Time:** User can show or hide date & time on OSD.

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

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

3.5.4 Audio

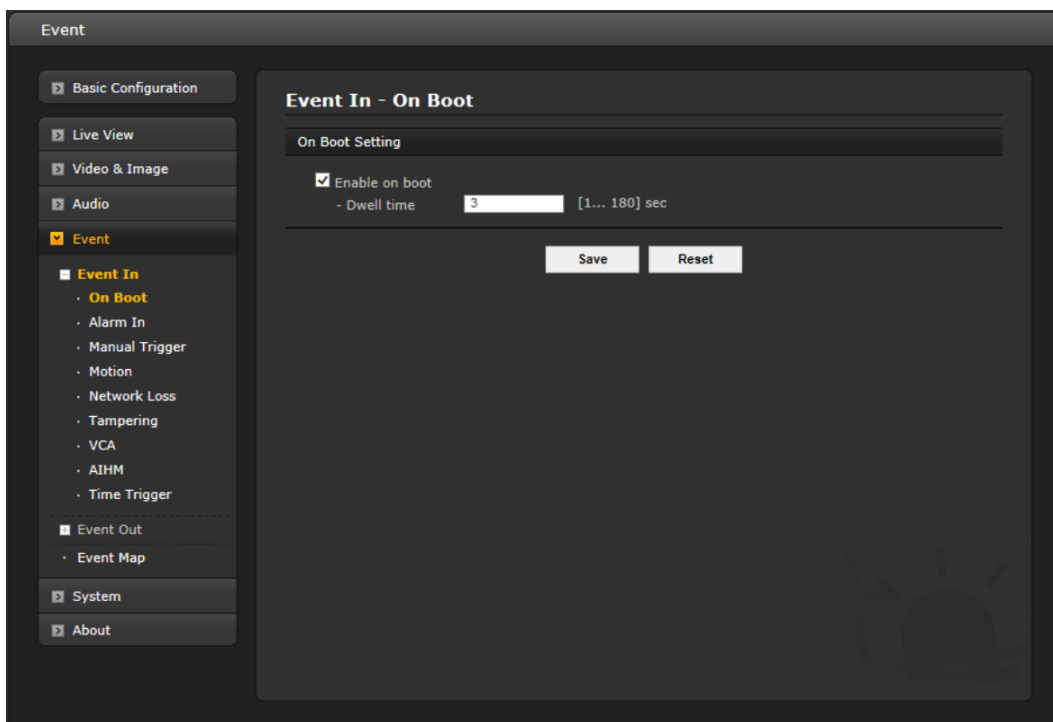


Refer to “3.5.1 Basic Configuration > Audio” for details.

3.5.5 Event

1) Event-In

▼ On Boot

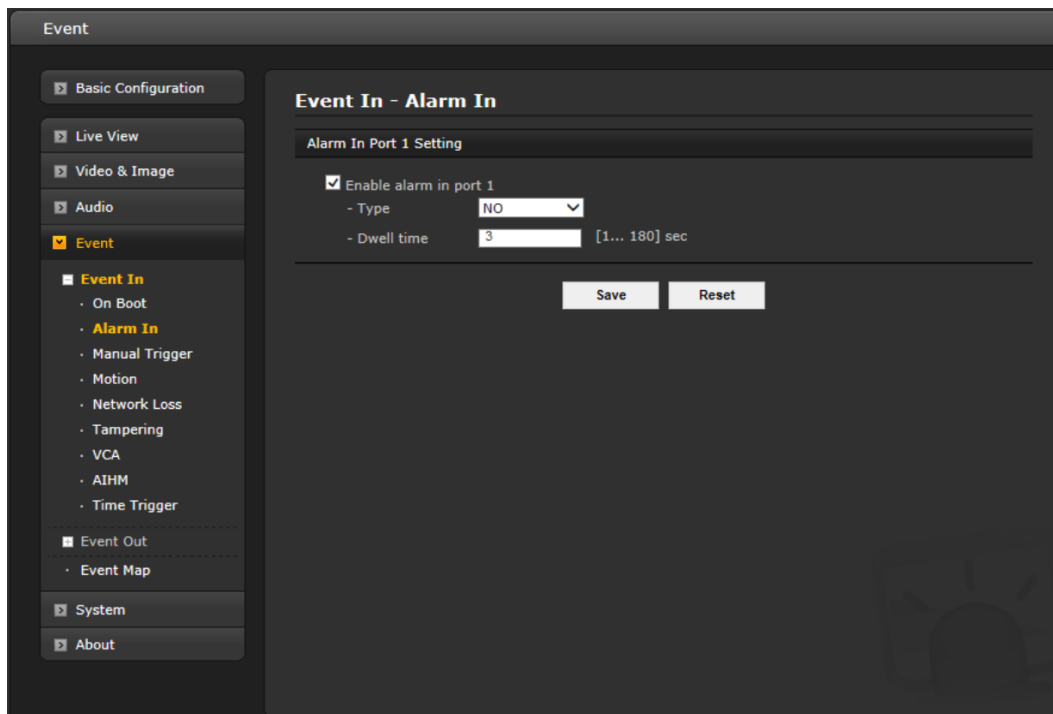


This is used to trigger the event every time the network camera is started. Select “Enable on boot” to activate the motion event.

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.

▼ Alarm In



This page allows you to configure the input supported by the camera and the Normal state configured. The port can be defined as Normally Open or Normally Closed state. An input will be inactive as long as its Normal state equals its Current state. The options for Normal state are NO (Normally Open) and NC (Normally Close). The input is activated when the Current state changes so that it no longer equals the Normal state.

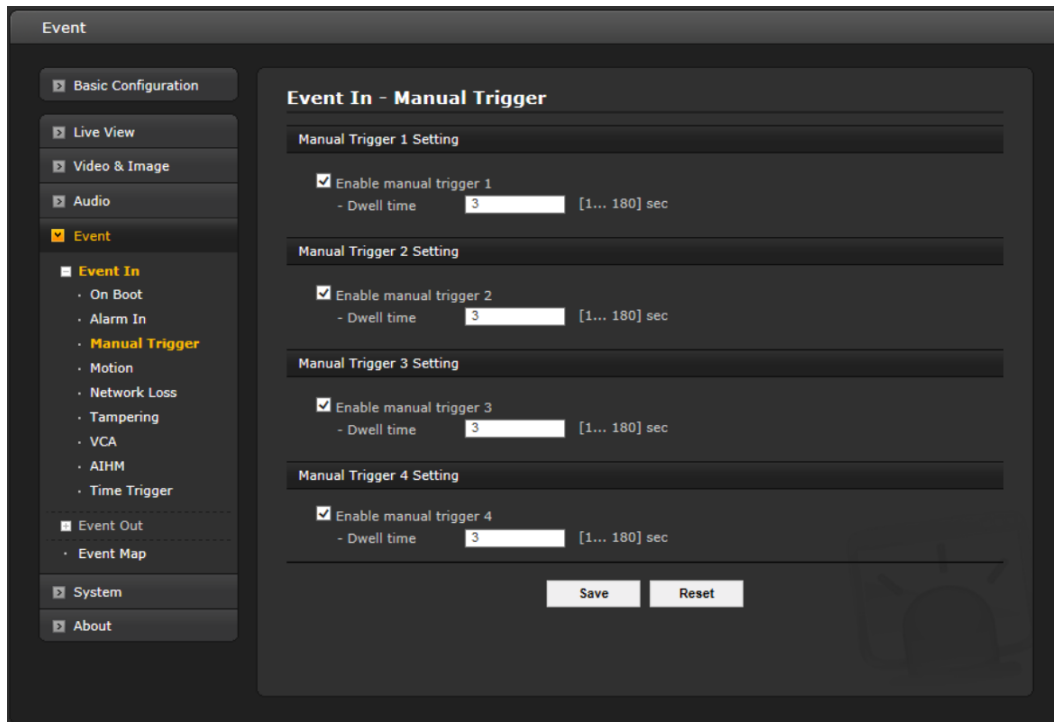
● Alarm In Port 1 Setting

Select "Enable alarm in port 1" to activate the alarm event. The network camera supports 1 alarm input port.

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

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

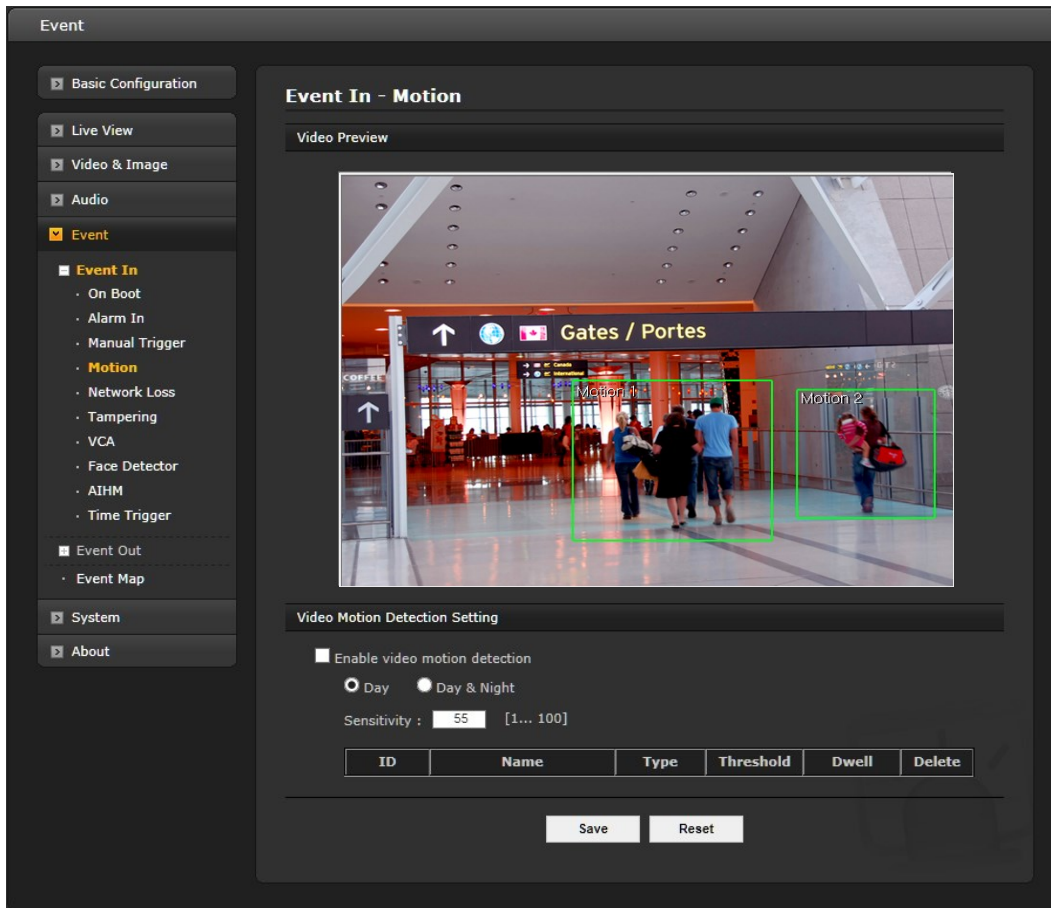
▼ Manual Trigger



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

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

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



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.

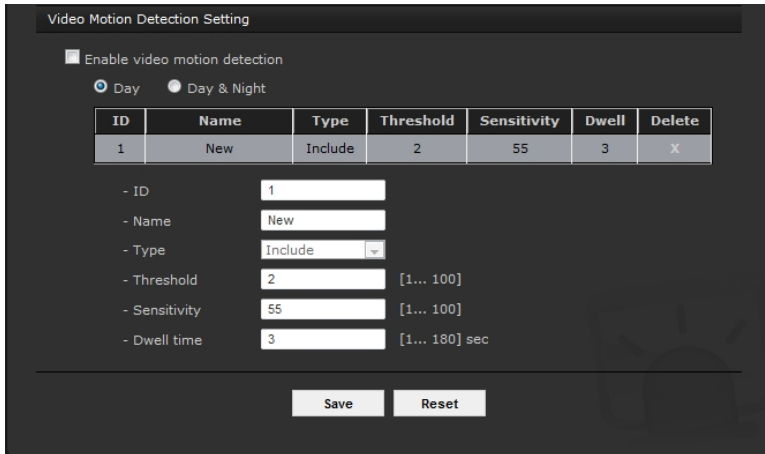
Select "Enable video motion detection" to activate the motion window.



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.

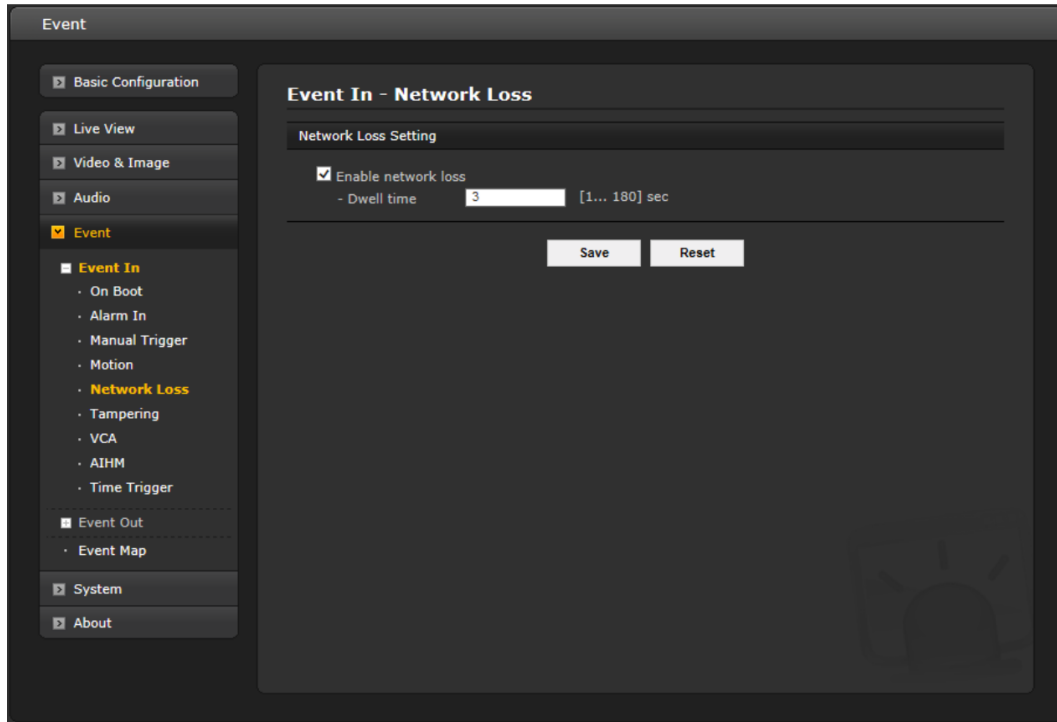
- **Threshold:** Sets up the threshold for the motion detection. Threshold judges the amount of change in the area. Select from 1-100; a lower number increase frequency of alarms.
- **Sensitivity:** Sets up the sensitivity for the motion detection. Sensitivity measures the level of motion in each motion 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.



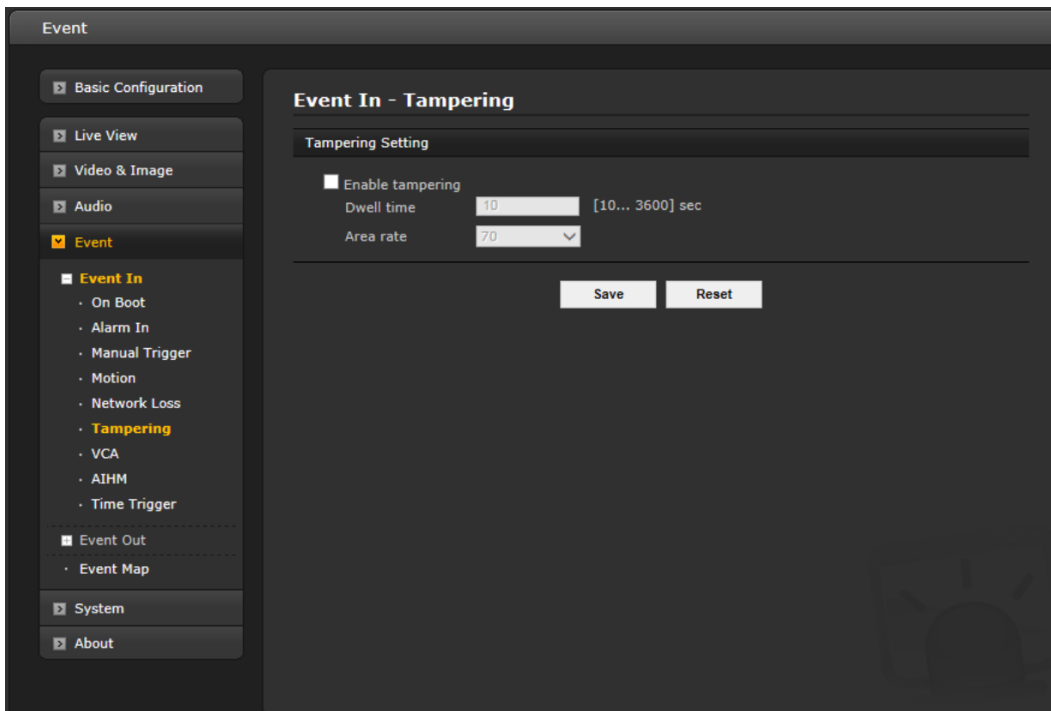
▼ Network Loss



This is used to trigger the event every time the network connection is failed. Select “Enable network loss” to activate the Network Loss event. Select a dwell time for how long the event will last from the point of detection.

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

▼ Tampering

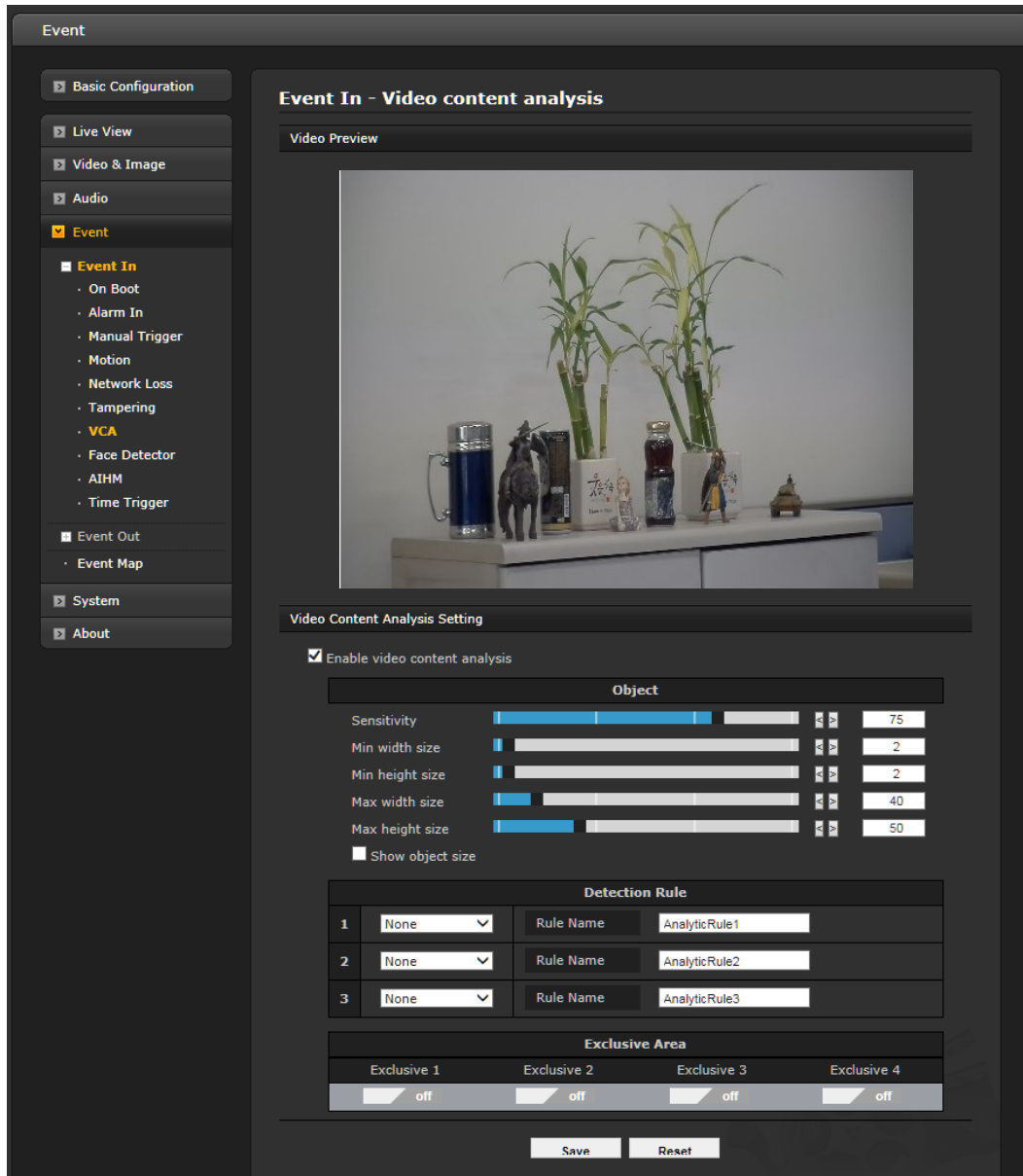


This is used to trigger an event when camera tampering occurs, for example, obstruct the camera with foreign material or move camera direction using external force. Select “Enable tampering” to activate the Tampering event.

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

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

▼ VCA



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

- **Video Content Analysis Setting:** Check “Enable video content analysis” box to use a VCA function.

– **Object:** Determines detection sensitivity.

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

* **Min width size:** Minimum horizontal pixel size for detections in a 1920x1080 format.

* **Min height size:** Minimum vertical pixel size for detections in a 1920x1080 format.

* **Max width size:** Maximum horizontal pixel size for detections in a 1920x1080 format.

* **Max height size:** Maximum vertical pixel size for detections in a 1920x1080 format.

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

* **Line Detector:** Once selected, a **red** line appears on the video preview window. Drag and drop the line at the desired position. User can change the length and the slope by dragging each end of the line.

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

. **Direction:** This detector can detect line crossing events and also count up number of the event; the direction of the event appears as a solid triangle shape at the center of the line.

. **Base:** The reference point of the object detection.

. **Counter:** User can choose between Counter and Detector.

* **Field Detector:** Once selected, a **blue** line appears on the video preview window. Drag and drop the box at the desired position. User can change the shape of the box by dragging each corner to any shape of a quadrilateral.

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

. **Base:** The reference point of the object detection.

. **Mode:** Currently Enter rule only.

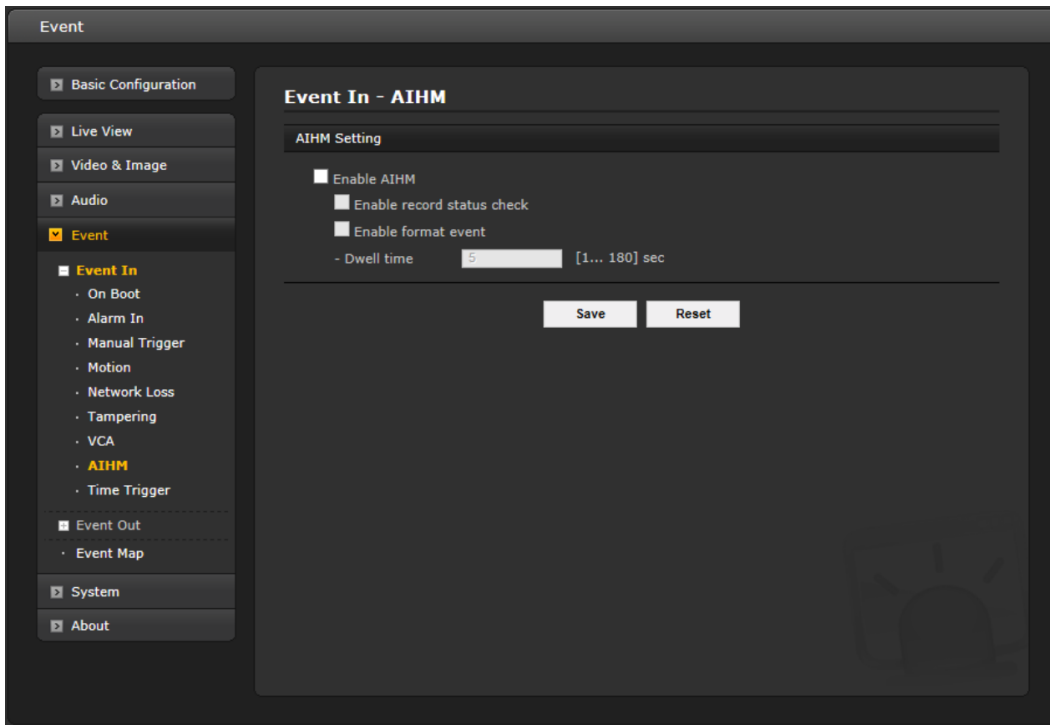
– **Exclusive Area:** The area where the rules are not applied. Once selected, a **purple** line appears on the video preview window. Drag and drop the box at the desired position.

User can change the shape of the box by dragging each corner to any form of a quadrilateral.

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

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

▼ AIHM



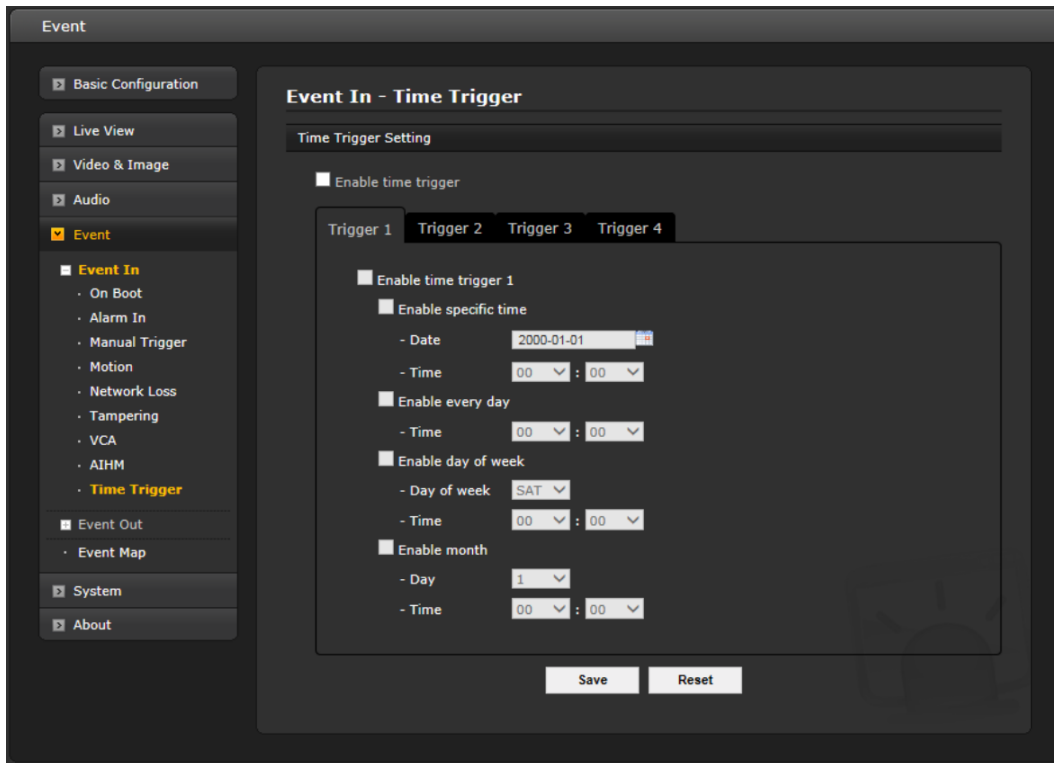
AIHM (Advanced Intelligent Health Monitoring) triggers an event when abnormality of the camera occurs.

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

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.

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

▼ Time Trigger



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

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

- **Enable specific time:** User can select type in date and time in the calendar for triggering the event.
- **Enable every day:** Trigger event every day at specified time.
- **Enable day of week:** Trigger event at the day of every week at specified time.
- **Enable month:** Trigger event at the 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 configuration page for SMTP (E-Mail) under the Event Out section. The interface is dark-themed. On the left is a sidebar with navigation options: Basic Configuration, Live View, Video & Image, Audio, Event (selected), System, and About. Under 'Event', there are sub-options: Event In, Event Out (selected), FTP & JPEG, Alarm Out, Audio Alert, Record, XML Notification, Notification Server, and Event Map. The main content area is titled 'Event Out - SMTP(E-Mail)'. It has three main sections: 1. 'SMTP(E-Mail) Setting': Includes a checkbox for 'Enable SMTP', a text input for 'Sender', a checkbox for 'Image attachment', an 'Interval' input (60) with a range [1... 86400] sec, an 'Aggregate events' input (50) with a range [1... 100], a checkbox for 'Use mail server', and fields for 'Mail server', 'Port' (25), 'Connections security' (None), 'User name', 'Password', and 'Login method' (AUTH LOGIN). 2. 'SMTP(E-Mail) Receiver': A grid of eight input fields labeled Receiver 1 through Receiver 8. 3. 'SMTP(E-Mail) Test': 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.
- **Interval:** Represents the frequency of the email notification when an event occurs.
- **Aggregate events:** Shows the maximum number of emails sent within each interval. Check the box to "Use mail server" if required.
- **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

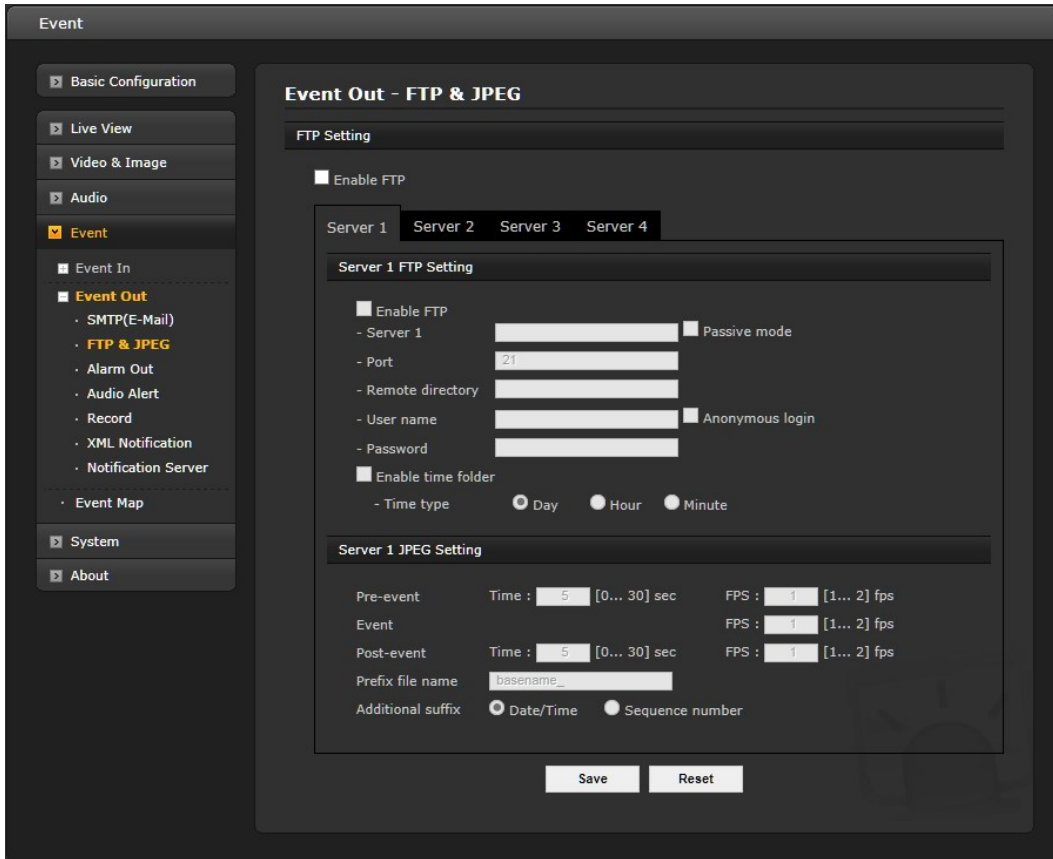
- **Receiver:** Enter an email address for a receiver. You can register up to 8 e-mail addresses of recipients.

- **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**

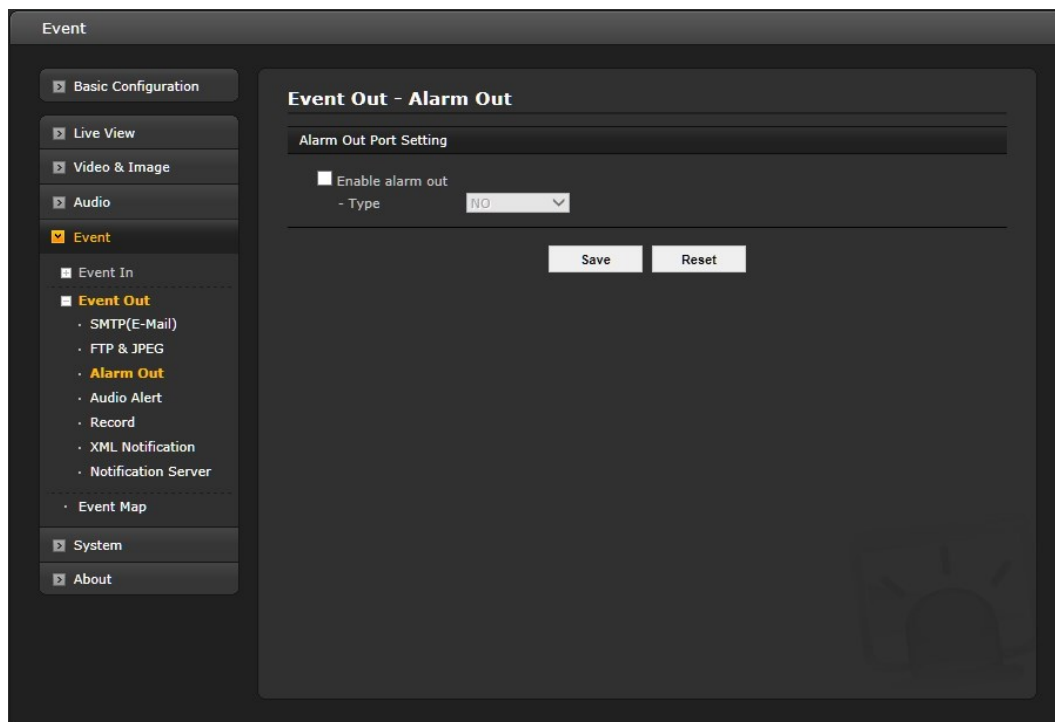
- **Server:** Enter the server's IP address or host name. Note that a DNS server must be specified in the TCP/IP network settings if using a host name.
- **Port:** Enter the port number used by the FTP server. The default is 21.
- **Passive mode:** Under normal circumstances the network camera simply 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.

- **JPEG Setting**

- **Pre-event:** A pre-event buffer contains images from the time immediately preceding the event trigger. These are stored internally in the server. This buffer can be very useful when checking to see what happened to cause the event trigger.
Check the box to enable the pre-trigger buffer, enter the desired total length in seconds, minutes or hours, and specify the required image frequency.
- **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.

- ▼ **Alarm Out**

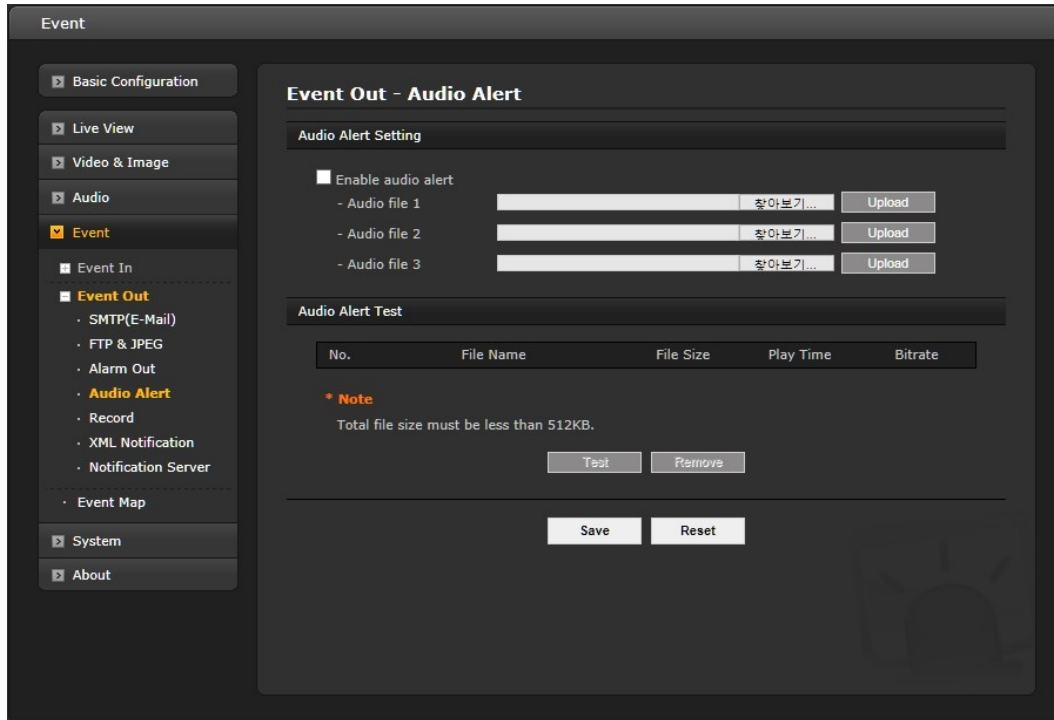


When the network camera detects an event, it can control external equipment connected to its alarm output port.

- **Enable:** Select **"Enable alarm out"** and the output will be activated for as long as the event is active. Select a Type of NO or NC (Normally Open or Normally Closed).

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

▼ Audio Alert



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

- **Audio Alert Setting**

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

- **Audio Alert Test**

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

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

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

▼ Record

Event Out - Record

Record Setting

- Enable Record
 - Overwrite
 - Continuous Record
- * Note : Using continuous recording may shorten life time of SD card.
- Stream Type:
- Pre-event: [0... 10] sec
- Post-event: [0... 60] sec
- Audio Record

Record schedule

No Recording Recording

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
SUN	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording
MON	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording
TUE	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording
WED	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording
THU	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording
FRI	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording
SAT	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording	Recording

Device Setting

Device Type:

Format

Device Status : No Storage

Device Remove

Device Information

Total	Used	Available	Used Percent	Bad Sector
0.00MB	0.00MB	0.00MB	0.00%	0.00%

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

- **Record Setting**

- **Overwrite:** Click checkbox to overwrite the storage device; Continuous Record is available when not using an SD card.
- **Stream Type:** You can select Stream 1, Stream 2, or Stream 3.
 - * **Stream1:** H.264 or MPEG-4 data
 - * **Stream2:** MJPEG data
 - * **Stream3:** H.264 or MPEG-4 data
- **Pre-event:** Enter pre-event time value for the storage device pre-recording.
- **Post-event:** Enter post-event time value for the storage device pre-recording.

- **Record Schedule**

The weekly recording schedule can be set for each day. Drag or click a box area; clicking the block toggles the recording between on and off. Click the "All Select" button to set a schedule for the entire week, 24/7; to record for a whole day, click in the "0" box and drag to "23."

Note that the time is in 24 hour format, where 0 indicates midnight.

- **Device Setting**

Select the device type to be recorded in the drop-down list.

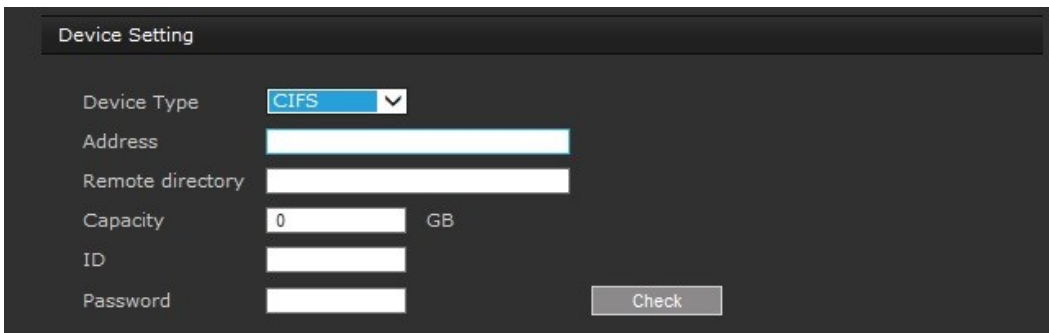
The screen changes according to selection.

- **SD:** Built-in SD card.
- **CIFS:** A file format for a NAS device.
- **NFS:** A file format for a NAS device.

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

Note2: Network File System (NFS) is a network file system protocol, allowing a user on a client computer to access files over a network in a manner similar to how local storage is accessed. NFS, like many other protocols, builds on the Open Network Computing Remote Procedure Call (ONC RPC) system.

The CIFS screen displays as below.



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

- **Format**

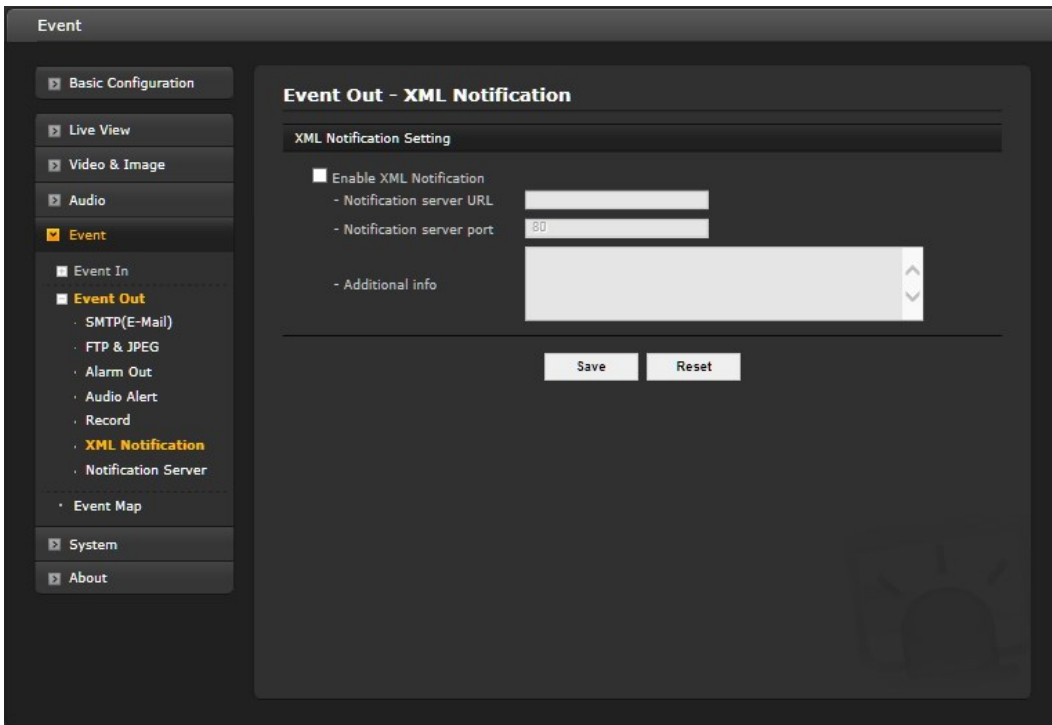
Click the Format button to format SD card.

- **Device Information**

Show current SD card information.

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

▼ XML Notification



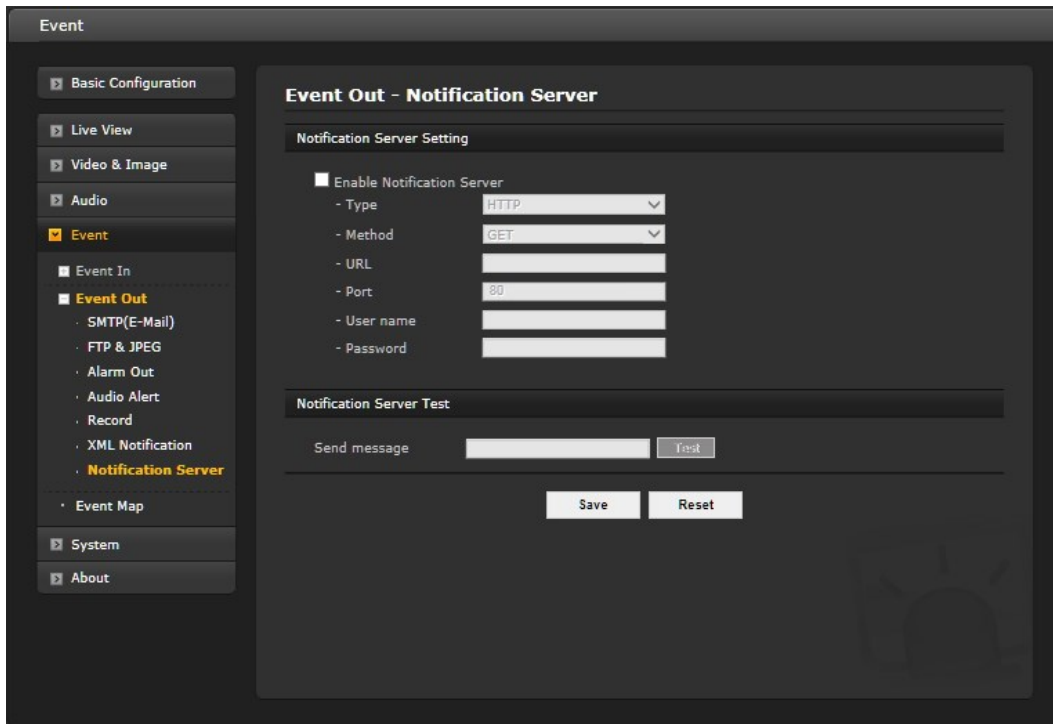
When the network camera detects an event, Notification server is used to receive notification messages as a type of XML data format. Check the box to enable the service.

● XML Notification Setting:

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

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

▼ Notification Server



When the network camera detects an event, the Notification Server is used to receive 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 UTP.

- **URL:** The network address to the server and the script that will handle the request.

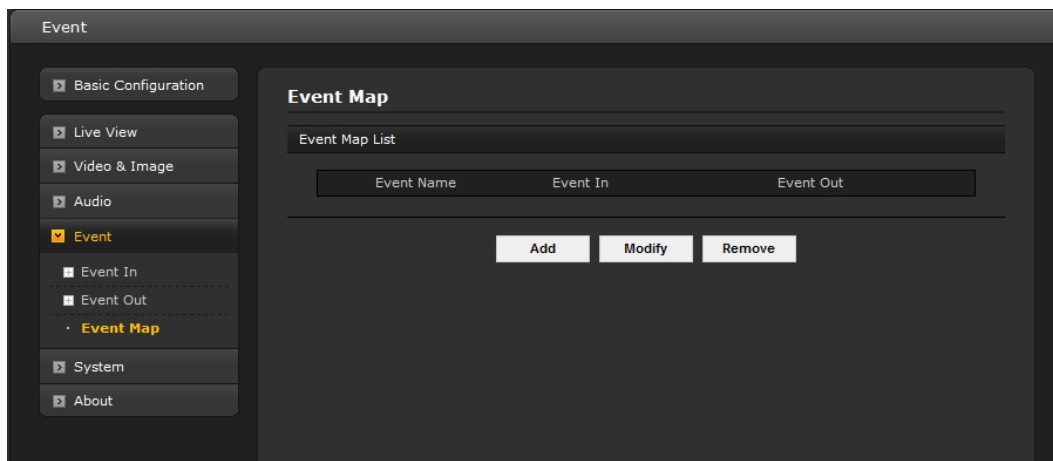
For example: <http://192.168.12.244/cgi-bin/upload.cgi>

- **Port:** The port number of the server.

- **User name/Password:** Provide your log-in information.

- **Notification Server Test:** When the setup is complete, the connection can be tested by clicking the Test button using the contents in "Send message" box.

3) Event Map



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

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

- **General**
Enter the name for a new event map.
- **Event In**
Select an event type in the drop-down list.
- **Event Out**
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.
 - **Alarm out:** Check this box to enable the alarm out.
 - **Audio alert:** Check this box to enable the audio alert.
 - **XML Notification:** It sends XML messages to a Notification server that listens for these. The destination server must first be configured on the Event In page.
 - **Record:** Record video stream when an event has occurred. The Record option must first be configured on the Event Out page.
 - **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.

3.5.6 System

1) Information

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

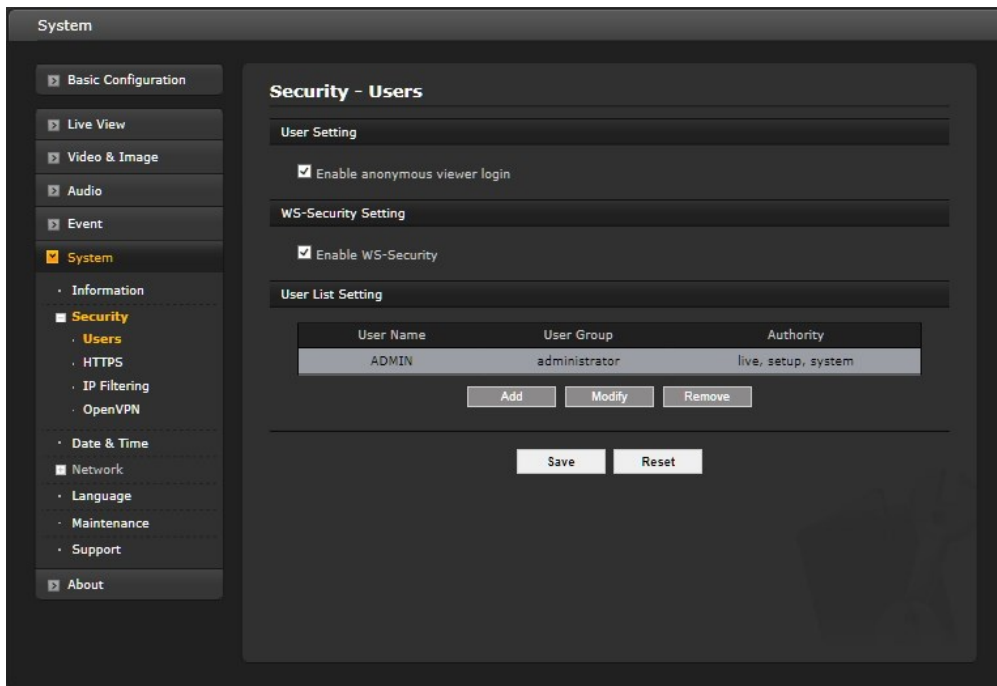
The screenshot shows a web interface for system configuration. The sidebar on the left lists various settings categories, with 'System' and 'Information' highlighted. The main panel displays the 'Information' configuration page, which includes a 'Device Name Configuration' section with a text input field containing 'H.264 Motorized IR 3M Camera', and a 'Location Configuration' section with four text input fields labeled 'Location1', 'Location2', 'Location3', and 'Location4'. At the bottom of the main panel are 'Save' and 'Reset' buttons.

- **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**

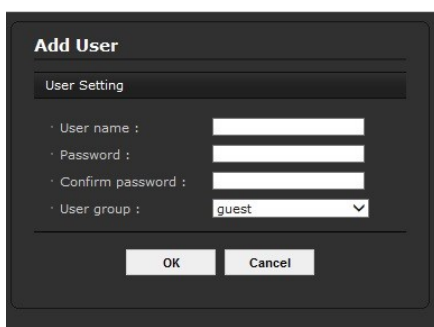
Check the box to "Enable anonymous viewer login" to the network camera without a user account. When using the user account, users have to log-in at every access.

- **WS Security Setting:** Check the box to enable WS Security. Do not check this box to connect and monitor the network camera through Vicon's viewing software using drivers older than 935.

Note: WS-Security is an open format for signing and encryption of message parts, for supplying credentials in the form of security tokens, and for security passing those tokens in a message.

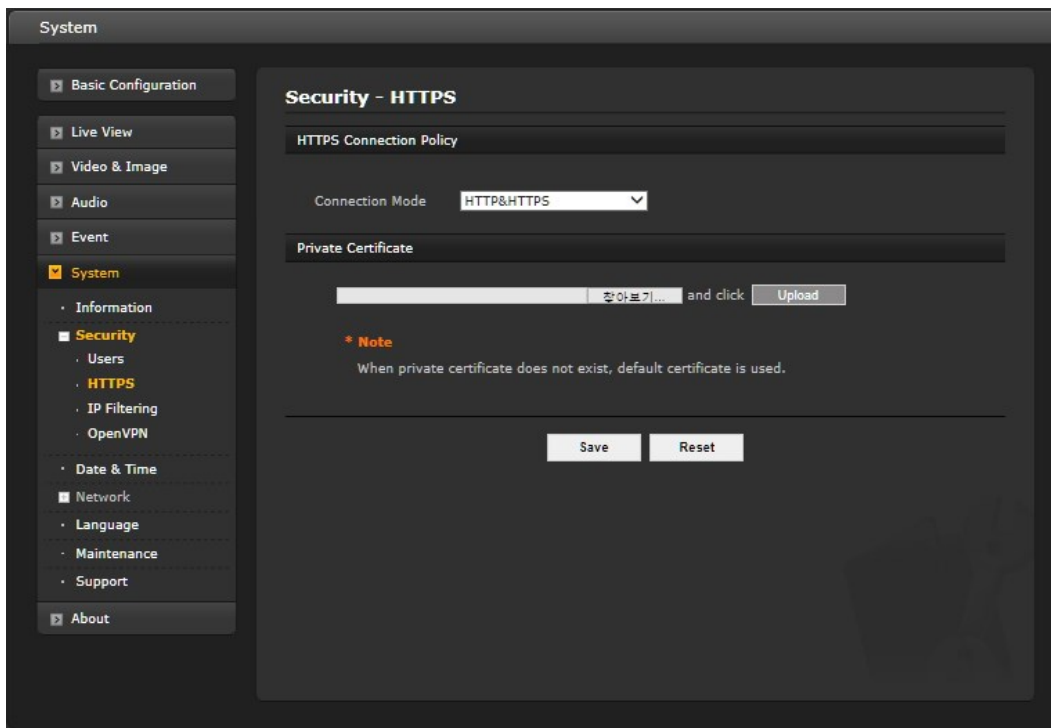
- **User List Setting**

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.



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**

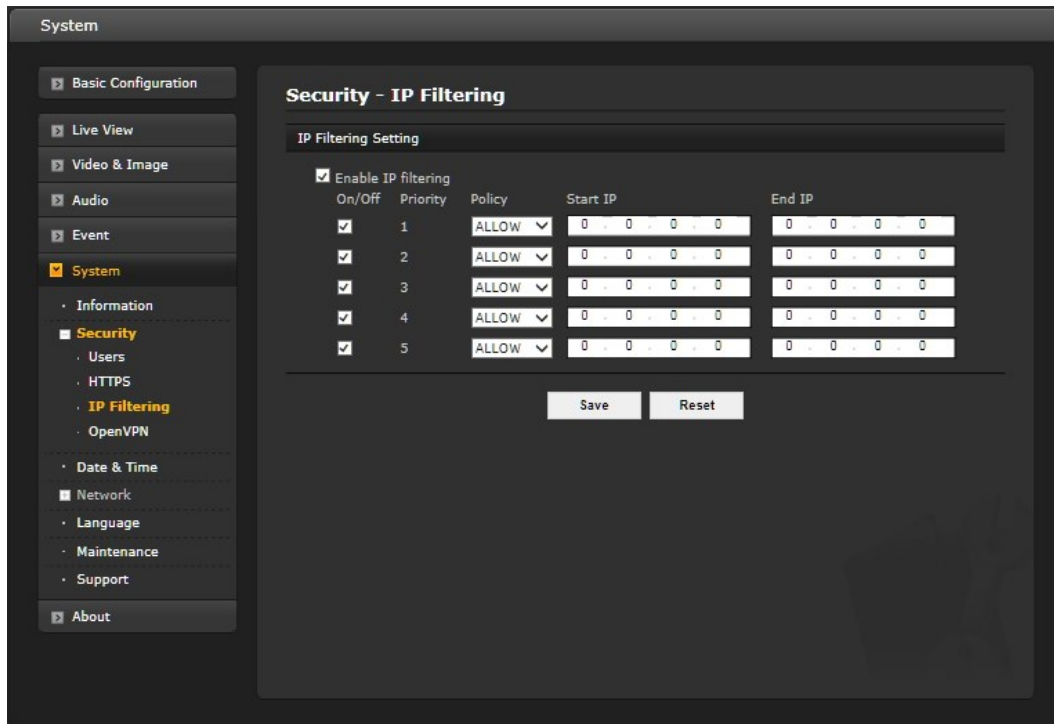
- **Private Certificate**

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



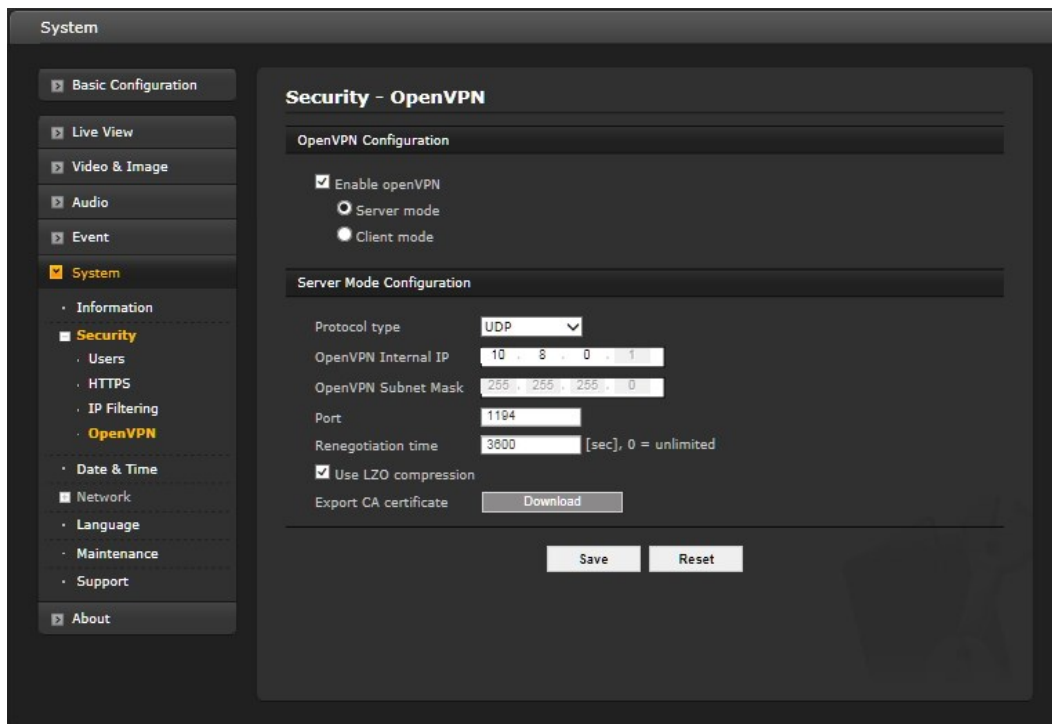
Checking the "Enable IP address filtering" box enables the IP address filtering function. When the IP address filter is enabled, addresses added to the list are set as allowed or denied addresses. All other IP addresses not in this list will then be allowed or denied access accordingly, that is, if the 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.

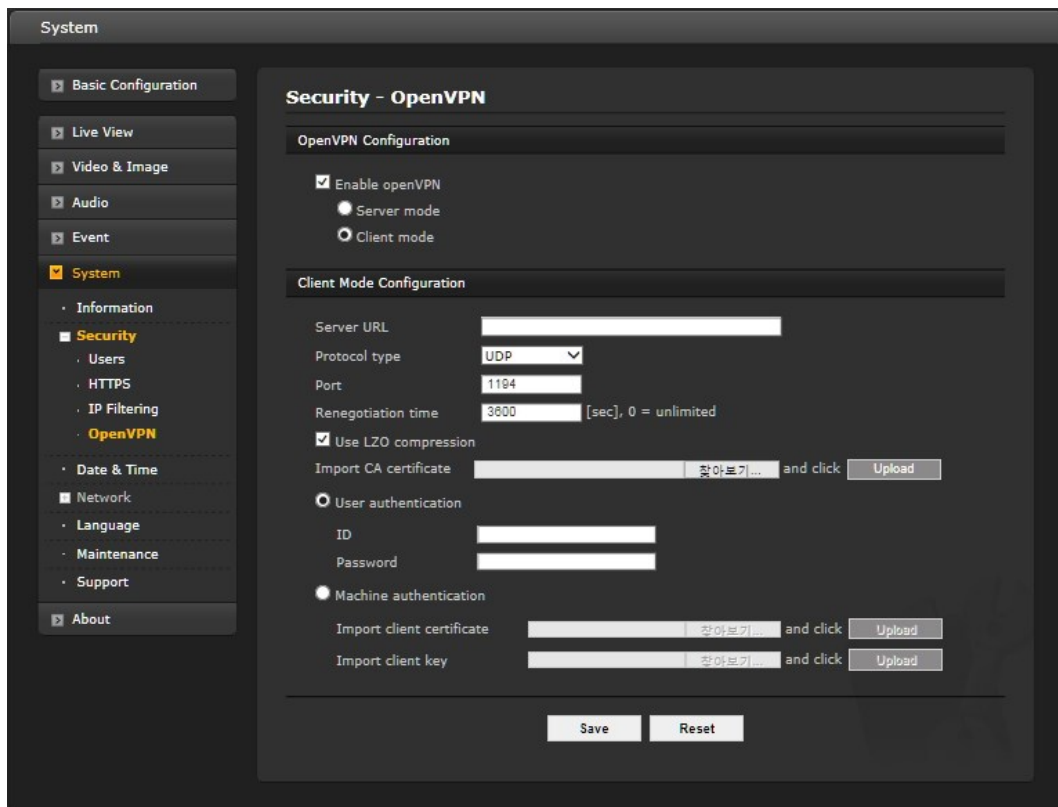
▼ OpenVPN

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



● 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.



● 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 a web interface for system configuration. On the left is a sidebar menu with categories: Basic Configuration, Live View, Video & Image, Audio, Event, System (selected), Information, Security, Date & Time (selected), Network, Language, Maintenance, Support, and About. The main content area is titled 'Date & Time' and contains several sections: 'Current Server Time' with input fields for Date (2013-08-09) and Time (15:25:05); 'New Server Time' with a 'Time zone' dropdown set to '(GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London' and a checkbox for 'Automatically adjusts for daylight saving time changes'; 'Time mode' with three radio buttons: 'Synchronize with computer time' (selected), 'Synchronize with NTP server' (with NTP server: time.nist.gov and NTP Interval: 12 [hour]), and 'Set manually' (with Date: 2013-08-09 and Time: 15:25:01); and 'Date & Time Format' with dropdowns for Date Format (YYYY-MM-DD) and Time Format (24 Hour). At the bottom are 'Save' and 'Reset' buttons.

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

4) Network

System

Basic Configuration

Live View

Video & Image

Audio

Event

System

Information

Security

Date & Time

Network

Basic

DDNS

RTP

UPnP

QoS

NAT

Zeroconf

Bonjour

Language

Maintenance

Support

About

Network - Basic

IP Address Configuration

Obtain IP address via DHCP
 Use the following IP address :

- IP address: 192 . 168 . 1 . 100
- Subnet mask: 255 . 255 . 255 . 0
- Default router: 192 . 168 . 1 . 254

IPv6 Address Configuration

Enable IPv6
IPv6 address : fe80::aede:48ff:fedd:1d09/64

DNS Configuration

Obtain DNS server via DHCP
 Use the following DNS server address :

- Domain name:
- Primary DNS server: 168 . 126 . 63 . 1
- Secondary DNS server: 0 . 0 . 0 . 0

Host Name Configuration

Host Name: V923D-N39MIR-IPACDE48DD1C

Services

HTTP port: 80
HTTPS port: 443
RTSP port: 554

ARP/Ping setting

Enable ARP/Ping setting

Save Reset

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

▼ Basic

● IP Address Configuration:

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

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

- **DNS Configuration**
DNS (Domain Name Service) provides the translation of host names to IP addresses on your network. Check the radio button to obtain DNS server via DHCP or set the DNS server.
 - **Obtain DNS Server via DHCP:** Automatically use the DNS server settings 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:**
 - **Link Speed:** User can select either 10Mbps or 100Mbps.

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

▼ DDNS

The screenshot shows a web-based configuration interface for a system. On the left is a navigation menu with categories like Basic Configuration, Live View, Video & Image, Audio, Event, System (selected), Information, Security, Date & Time, Network (expanded), and About. The Network section includes sub-items: Basic, DDNS (highlighted), RTP, UPnP, QoS, NAT, Zeroconf, Bonjour, Language, Maintenance, and Support. The main content area is titled 'Network - DDNS' and contains the following settings:

- Internet DDNS (Dynamic Domain Name Service)**
- Enable DDNS
- * Note**
Please remember you have to configure at least primary DNS server in DNS configuration settings to use Dynamic DNS.
- DDNS Server:
- Registered host:
- User name:
- Password:
- Confirm password:
- Maximum time interval:
- Register local network IP address
- Registered IP address :
- Buttons: Save, Reset

- **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

System

Basic Configuration

Live View

Video & Image

Audio

Event

System

- Information
- Security
- Date & Time
- Network
 - Basic
 - DDNS
 - RTP
 - UPnP
 - QoS
 - NAT
 - Zeroconf
 - Bonjour
- Language
- Maintenance
- Support

About

Network - RTP

Port Range

Start port: 30000 [30000... 39920; only even values are available]

End port: 30199

Multicast (Stream 1)

- Multicast destination IP: 231.1.128.20 [224.0.0.0... 239.255.255.255]
- RTP port: 40000 [1024... 65530]
- RTP TTL: 15 [1... 255]
- Always enable multicast

Multicast (Stream 2)

- Multicast destination IP: 231.1.128.21 [224.0.0.0... 239.255.255.255]
- RTP port: 40000 [1024... 65530]
- RTP TTL: 15 [1... 255]
- Always enable multicast

Multicast (Stream 3)

- Multicast destination IP: 231.1.128.22 [224.0.0.0... 239.255.255.255]
- RTP port: 40000 [1024... 65530]
- RTP TTL: 15 [1... 255]
- Always enable multicast

Multicast (Audio)

- Multicast destination IP: 231.1.128.20 [224.0.0.0... 239.255.255.255]
- RTP port: 40002 [1024... 65530]
- RTP TTL: 15 [1... 255]
- Always enable multicast

Multicast (Meta)

- Multicast destination IP: 231.1.128.20 [224.0.0.0... 239.255.255.255]
- RTP port: 40004 [1024... 65530]
- RTP TTL: 15 [1... 255]
- Always enable multicast

Save Reset

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.

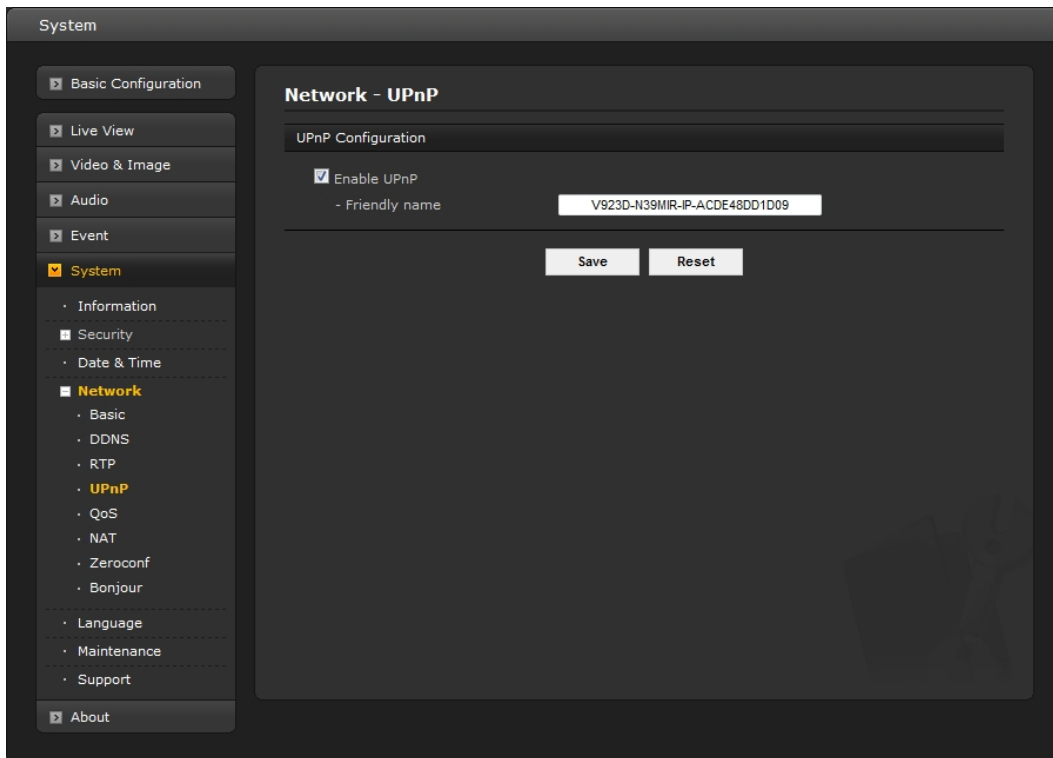
- **Enable Multicast:** Check the box to enable multicast operation.
- **Multicast destination IP:** Enter an IP between 224.0.0.0 and 239.255.255.255.
- **RTP port:** Enter a value between 1024 and 65532.
- **RTP TTL:** Enter a value between 1 and 255. If a network status is smooth, enter a lower value. 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.

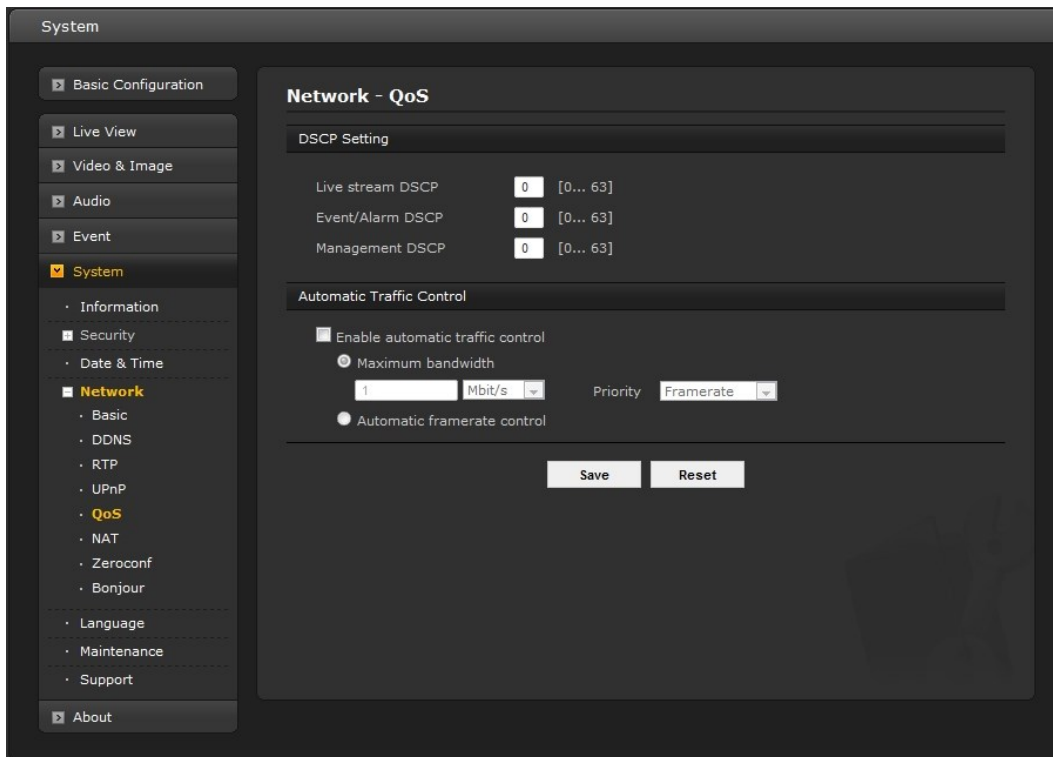
When the settings are complete, click **Save**, or click **Reset** to revert to previously saved settings.

▼ 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.

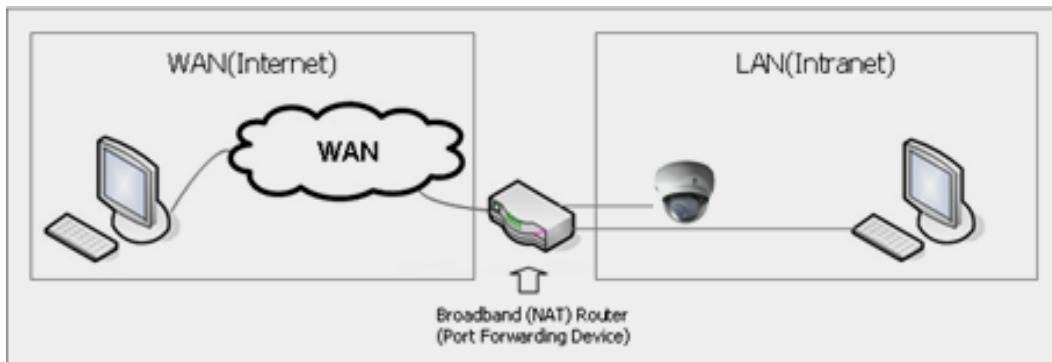
- **Maximum bandwidth** - When sharing other network programs or equipment, it is possible to set a limitation on the maximum bandwidth in the unit of Mbit/s or kbit/s.
- **Automatic frame rate** - Selected if not influenced by a network-related program or equipment without a limitation on the network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

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

▼ NAT (Port Mapping)

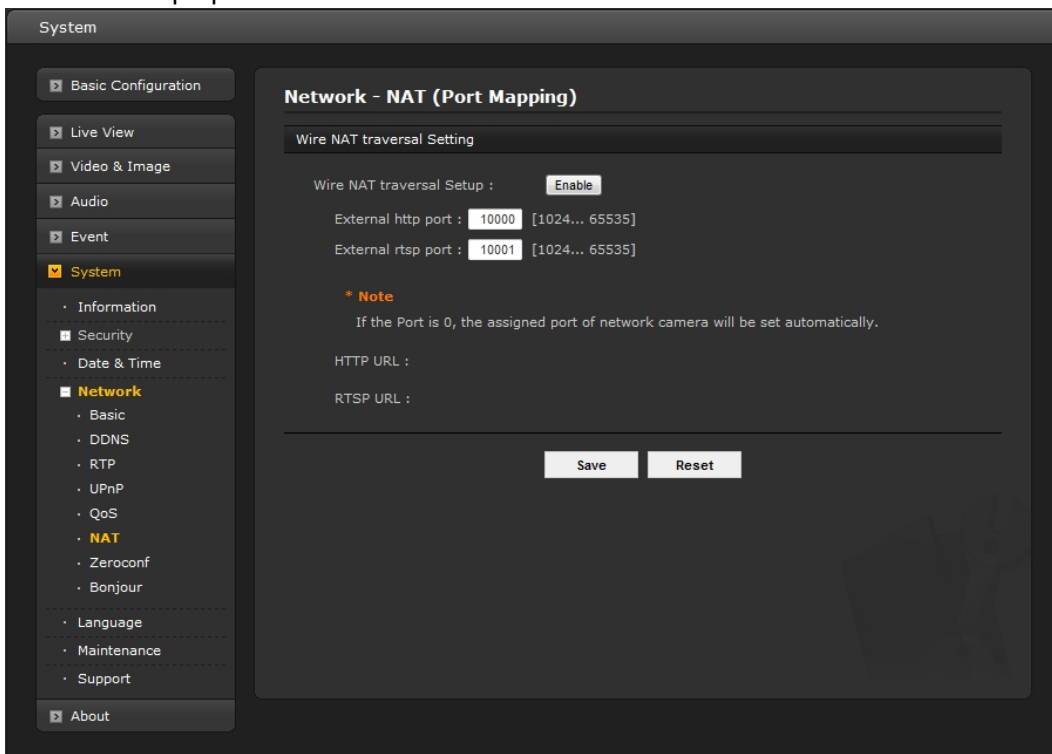
A broadband router allows devices on a private network (LAN) to share a single connection to the Internet. This is done by forwarding network traffic from the private network to the "outside," that is, the Internet. Security on the private network (LAN) is increased since most broadband routers are pre-configured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

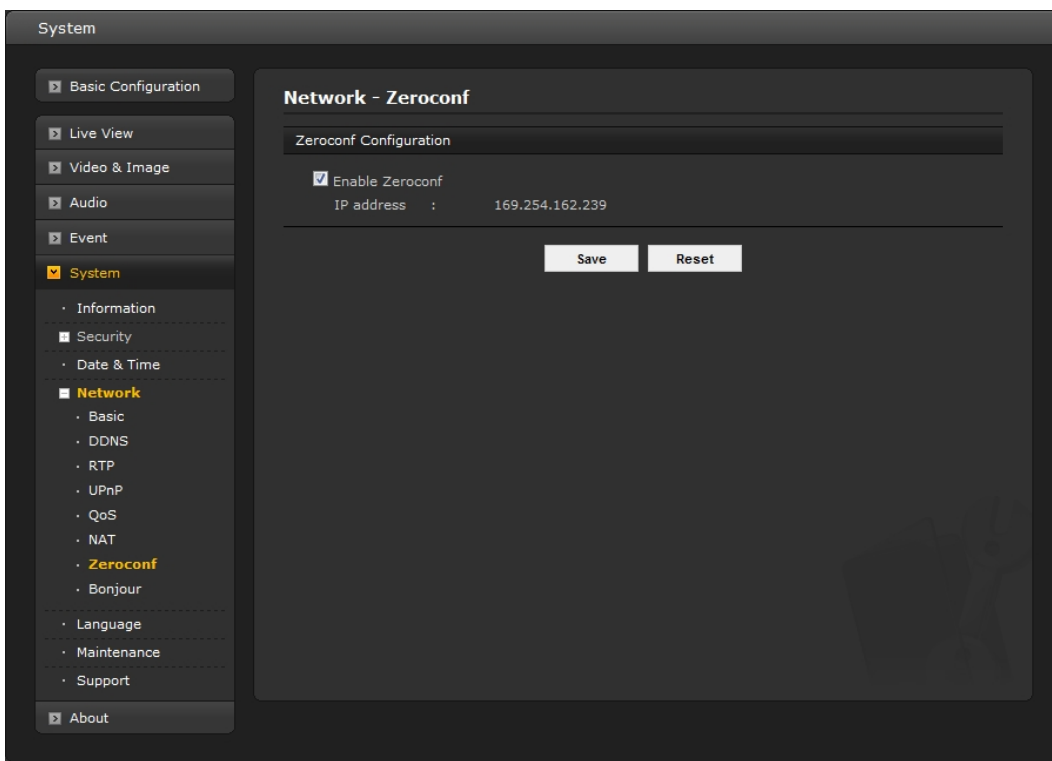
Notes:

- 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.

▼ **Zeroconfig**

Zeroconfig 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)

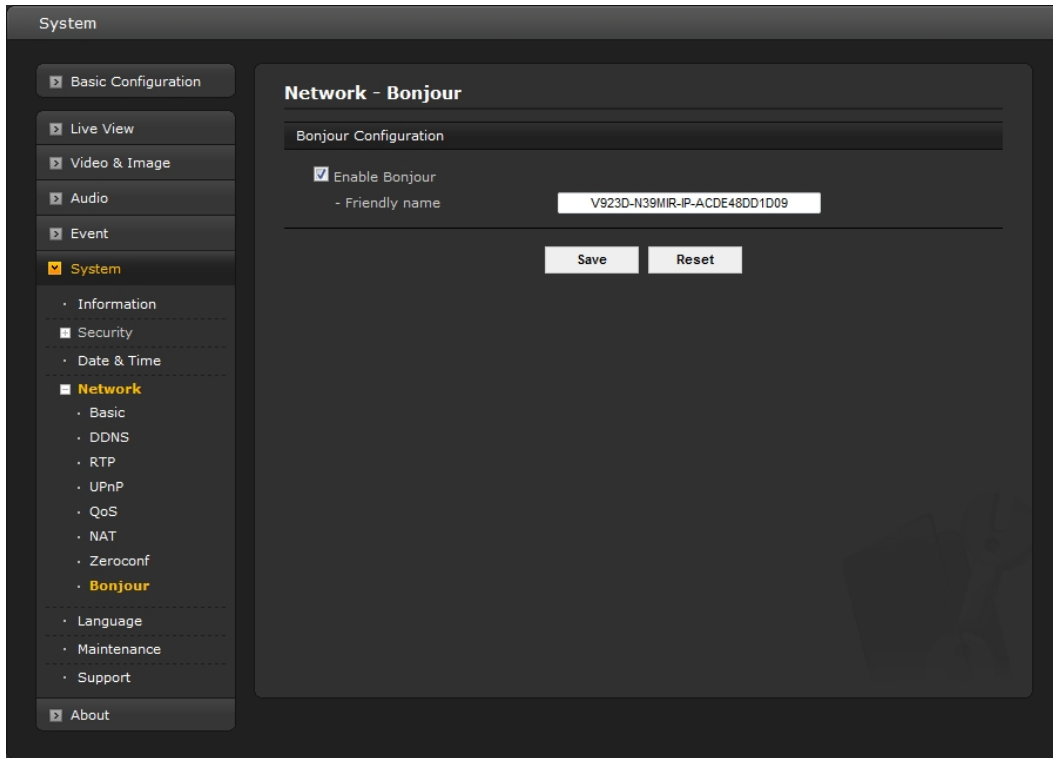
- Automatic location of network services, such as printing devices through DNS service discovery.

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.



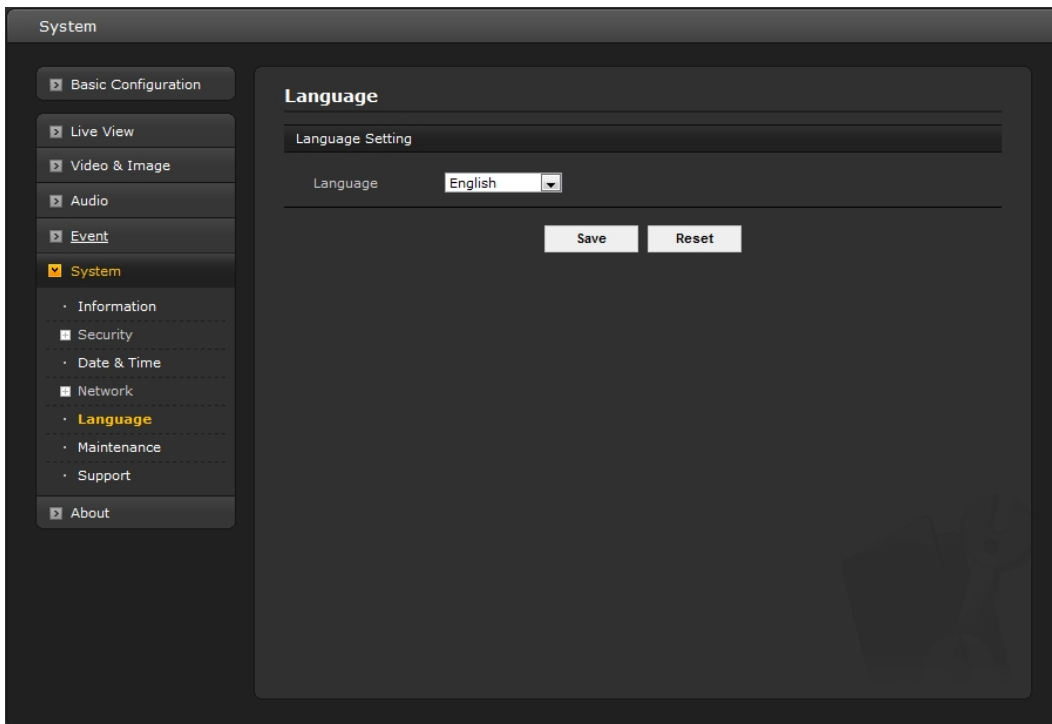
Click the check box to enable Bonjour. Enter a name in the Friendly name field.

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

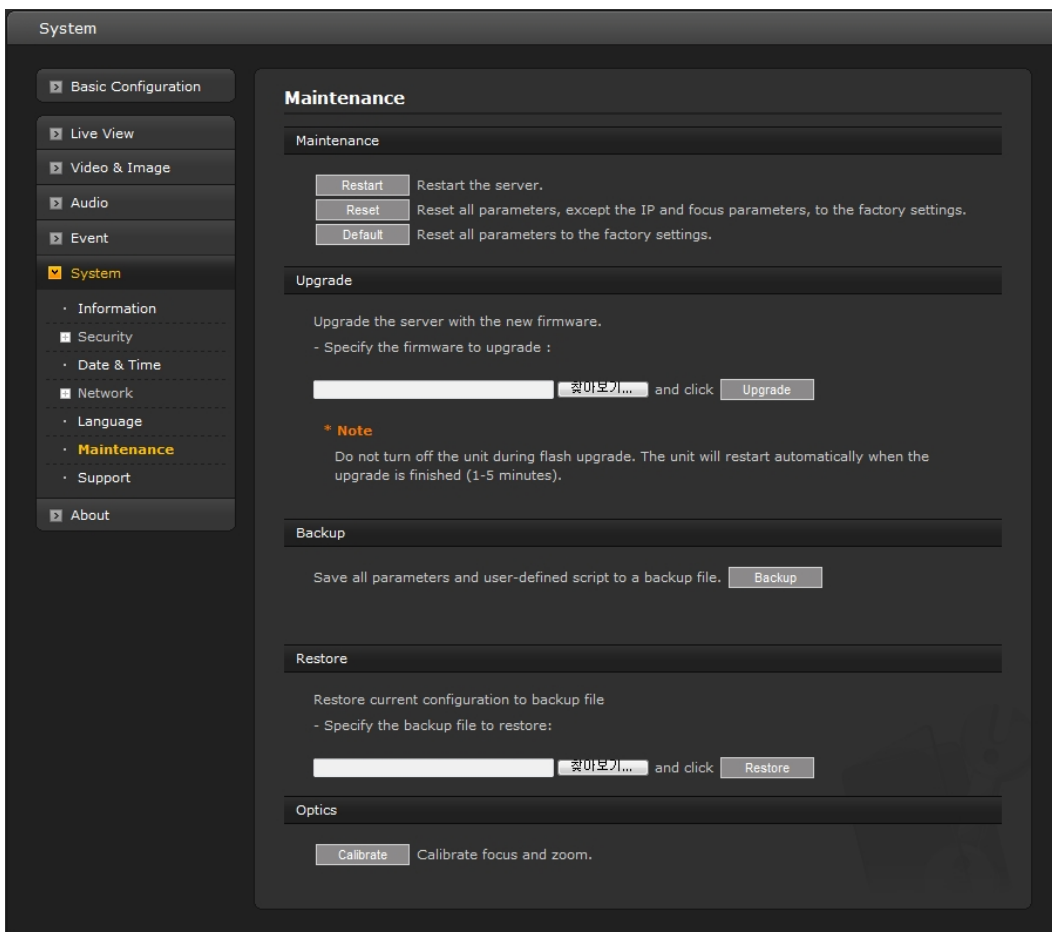
Note: Also known as zero-configuration networking, Bonjour enables devices to automatically discover each other on a network, without having to enter IP addresses or configure DNS servers. (Bonjour is a trademark of Apple Computer, Inc.)

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.

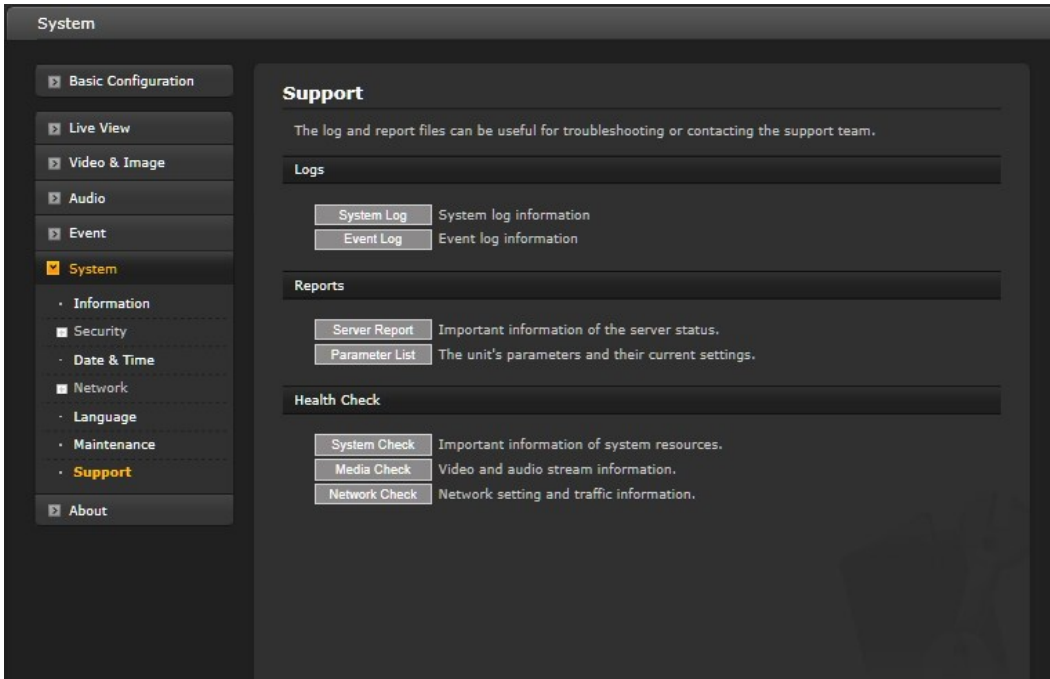
- **Optics**

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

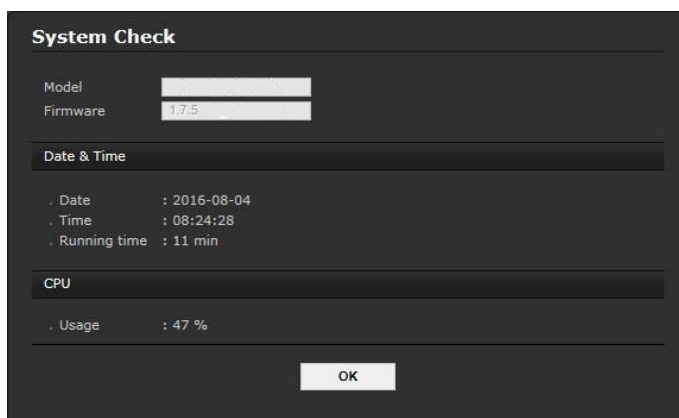
Note: Backup and Restore can only be used on the same unit running the same firmware. This feature is not intended for multi-configurations or for firmware upgrades.

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 **System Log** button to get the log data and the **Event Log** button for event information.
- **Reports**
 - **Server Report:** Click the Server Report button to get the important information about the server's status; this should always be included when requesting support.
 - **Parameter List:** Click the Parameter List button to see the unit's parameters and their current settings.
- **Health Check**
 - **System Check:** Click the System Check button to get the important information about the camera's system resources. You can see the pop-up window below.



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

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

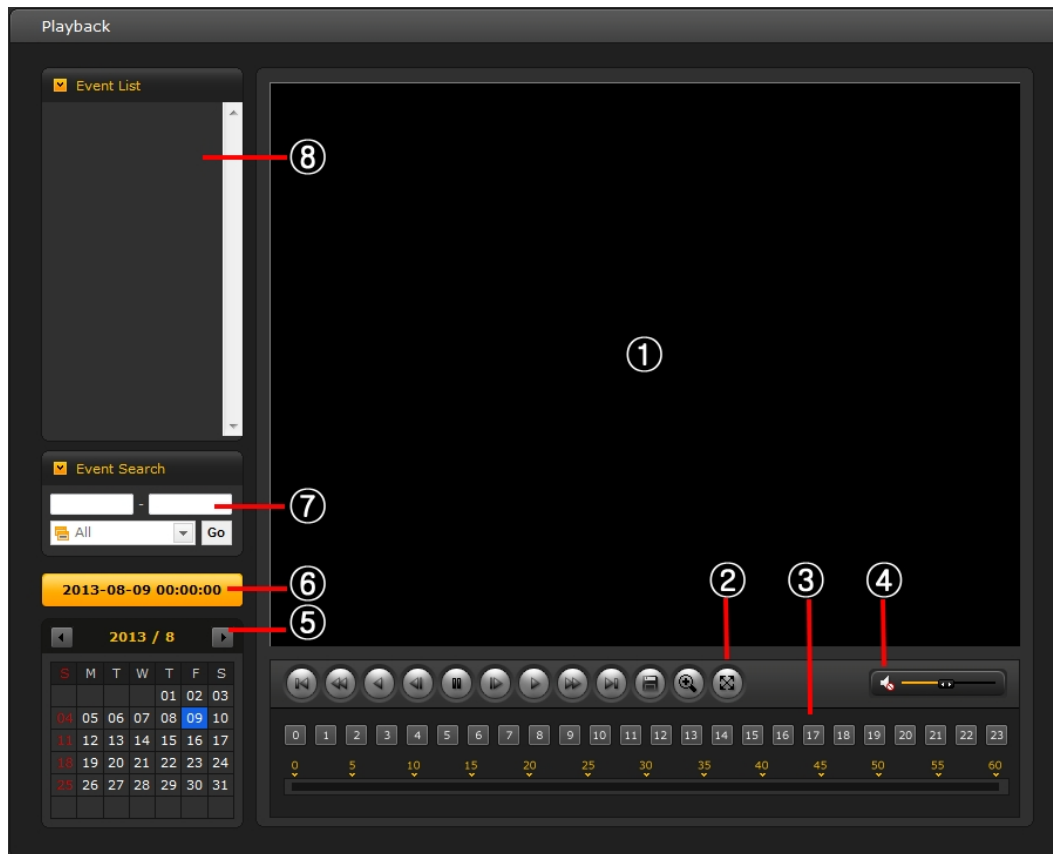
- **Network Check:** Click the Network Check button to get the information about the cameras network setting and traffic. You can see the pop-up window below.

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 Playback

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












The description of playback window follows.




(1) Video Screen

The video screen displays the video clip in the Micro SD memory.

(2) Playback Buttons

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

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

-  Clip Copy: copy the video clip.
-  Digital Zoom: zoom in the video clip
-  Full Screen: display full screen of the video.

(3) Time Chart

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

(4) Speaker Control Bar

Use this scale to control the volume of the speakers.

(5) Search Calendar

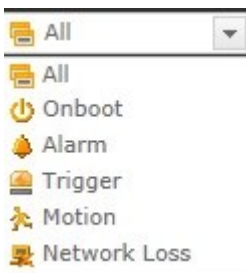
Search results from the SD local storage in the network camera connected are displayed monthly. If there is recorded data for a particular date, a blue square on the date will be displayed. If a particular date in the calendar is selected, a yellow square on the date will be displayed.

(6) Play Time

Displays time of the video playing.

(7) Event Search Window

Select a search option in the drop-down list and click **Go** button. As an alternative, enter the time period for searching. If you click Start Date or End Date zone, the Search Calendar displays.



(8) Event List Window

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

3.7 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
- ▶ Playback
- ▶ Live View
- ▶ **Video & Image**
 - **Basic**
 - Webcasting
 - Camera Setup
 - OSD
- ▶ Audio
- ▶ Event
- ▶ System

Video & Image - Basic

Through the 'Video & Image - Basic' page, user can setting 'Capture mode' of image sensor and '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**

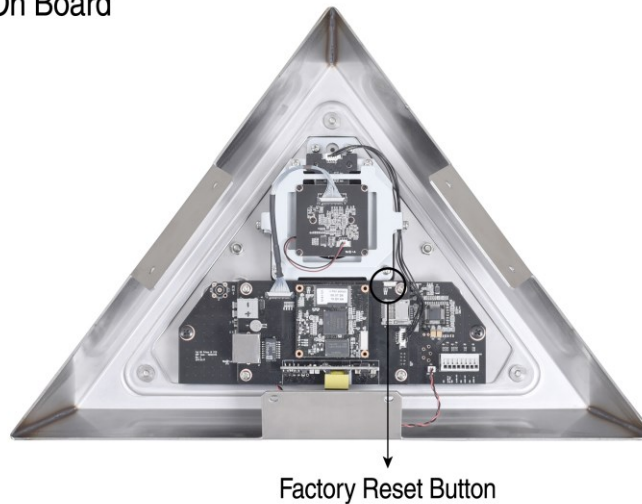
Through the 'Stream Setting', you may set a 'Codec' that use for image compression. The 'H.264', 'MPEG4' and 'MJPEG' codecs are used to image compression in this camera. The following TABLE shows the 'Stream' that supported for each codec.

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

3.8 Resetting to the Factory Default Settings

To reset the network camera to the original factory settings, go to the Setup > System > Maintenance web page (described in "System > Maintenance" of User's Manual) or use the **Reset** button on the network camera.

On Board



- **Using the Reset Button**

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

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

CAUTION: When performing a Factory Reset, you will lose any settings that have been saved.
(Default IP 192.168.1.100)

4. Appendix

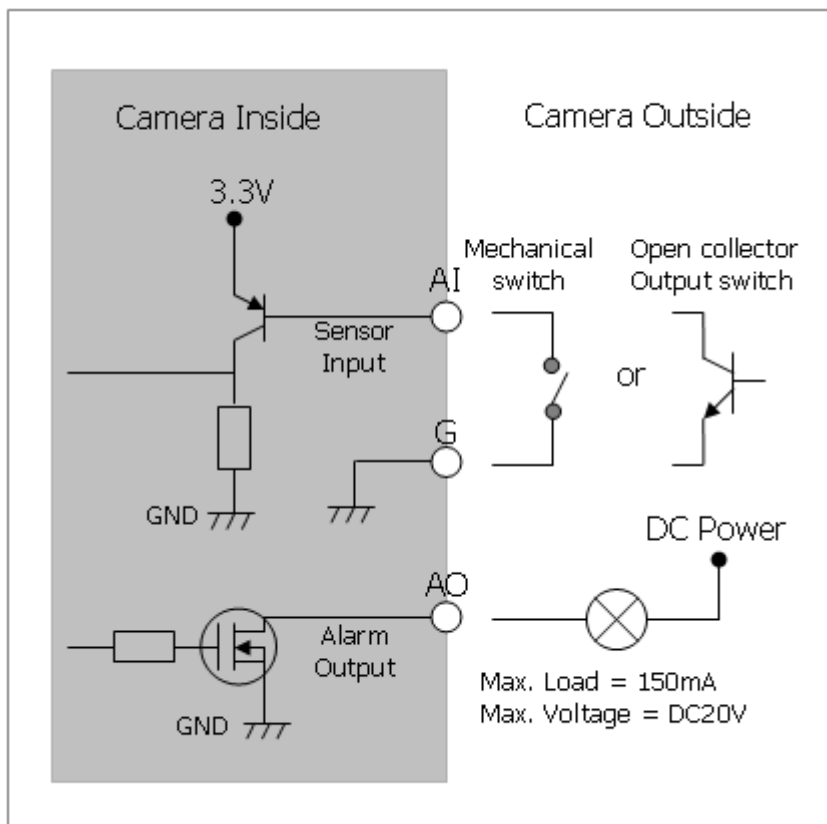
4.1 Troubleshooting

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.

4.2 Alarm Connection

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



4.3 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.

4.4 Product Specification

Main Item		Specification
I M A G E	Model	V-CELL-HD-B
	Lens	Megapixel Fixed 2.3mm F2.2
	Angle of View	130°(H)
	Image Sensor	1/2.8" SONY Exmor CMOS sensor
	Type	2,065(H) x 1,565(V)
	Pixels	Color: 0.2 Lux@F2.2, BW: 0 Lux(IR ON)
	Min. Illumination	Progressive Scan
	Scanning Mode	DWDR (72dB)
	Wide Dynamic Range	True D/N (Auto, Day, Night)
	Day and Night Mode	2DNR, 3DNR
	Noise Reduction	Yes (ROI)
	Digital Zoom	Auto
	Exposure Control	Auto, Incandescent, Fluorescent, Outdoor, Manual
	White Balance Control	Yes
	Back Light Compensation	Flip, Mirror, Aisle, Defog, DIS
	Image effect	50Hz, 60Hz
	Flicker Free Mode	Auto(1/10,000 ~ 1sec), Manual
Shutter Speed	36 IR LEDs(940nm, Invisible)	
IR Illuminator	Quantity	140°
	Angle	20m
	Distance	
V I D E O / A U D I O	Compression	H.264 (Baseline, Main, High Profile), MJPEG
	Bitrate Control	CVBR, VBR
	Resolution	2048x1536, 1920x1080, 1280x1024, 1280x720/960, 1024x768, 704x480/576, 640x360/480, 320x240
	Frame Rate	Max. 50fps/60fps
	Streaming	25/30fps (Triple Stream: H.264 x 2, MJPEG x 1)
	Composite Out	No
	Audio Compression	G.711
Audio Streaming	2 Way	
S Y S T E M	Video Contents Analysis	Tampering, Line Detector, Field Detector
	Motion Detection Area	16 Programmable Area (Include Area 8, Exclude Area 8)
	Privacy Mask Zone	8 Programmable Zone
	FTP Uploading	MJPEG
	Event Notification	E-mail, FTP, Notification Server, XML Notification, Audio Alert, AIHM
	Audio Alert	User-Defined 3 Audio files
	Login Authority	Administrator, Operator, Guest
	Event Buffering	Pre : 30sec, Post : 30sec
	FTP SD Record	Pre : 10sec, Post : 60sec
	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
	Hardware Factory Reset	Yes
	Auto Recovery	Watch dog
Remote Upgrade	Web Browsing(IE, Chrome, Safari, Firefox), SmartManager	
SD Recording Mode	Event, Continuous	
N E T W O R K	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
E X T E R N A L I N / O U T	Audio	1 Input, 1 Output(Terminal Block)
	Alarm	2 Input, 1 Output(Terminal Block)
	Ethernet	RJ-45 (10/100Base-T)
	u-SD Card	SDHC (Max. 32GB)
E T C	Operating Humidity	0 ~ 90% RH (Non-condensing)
	Operating Temperature	-20°C ~ +50°C
	Power Supply	PoE(IEEE802.3af compliance, Class0), 12VDC
	Power Consumption	200mA (9.6W) @ PoE 600mA (7.2W) @ 12VDC
	Dimensions	380mm x 320mm
Net Weight	Approx. 1600g	

System Requirement for Web Browser

Operating System: Microsoft® Windows® 98, Microsoft Windows ME, Microsoft Windows 2000, Microsoft Windows XP, Microsoft Windows Vista®, Windows 7, Windows 8.1 or 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)



VICON INDUSTRIES INC.

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

