INSTRUCTION MANUAL

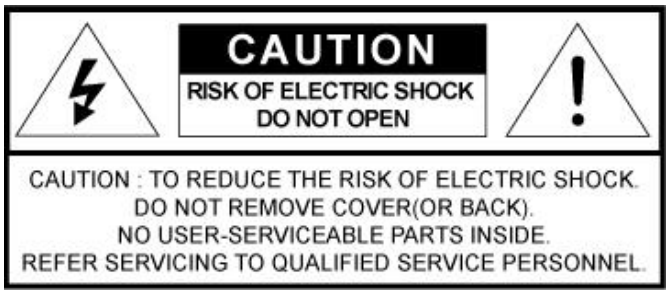
NETWORK TRANSMITTER

Please read this manual thoroughly before use, and keep it handy for future reference.

WARNING

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

CAUTION



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.

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.
OPERATION OF THIS EQUIPMENT IN A RESIDENTIAL AREA IS LIKELY TO CAUSE HARMFUL INTERFERENCE IN WHICH CASE THE USER WILL BE REQUIRED TO CORRECT THE INTERFERENCE AT HIS OWN EXPENSE.

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.
OPERATION OF THIS EQUIPMENT IN A RESIDENTIAL AREA IS LIKELY TO CAUSE HARMFUL INTERFERENCE IN WHICH CASE THE USER WILL BE REQUIRED TO CORRECT THE INTERFERENCE AT HIS OWN EXPENSE.

CAUTION: CHANGES OR MODIFICATIONS NOT EXPRESSLY APPROVED BY THE PARTY RESPONSIBLE FOR COMPLIANCE COULD VOID THE USER'S AUTHORITY TO OPERATE THE EQUIPMENT.

THIS CLASS A DIGITAL APPARATUS COMPLIES WITH CANADIAN ICES-003.

CET APPAREIL NUMERIQUE DE LA CLASSE A SET CONFORME A 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 are provided for your safety. If the provided plug does not fit into your outlet, consult an electrician for replacement of the obsolete outlet.
10. Protect the power cord from being walked on or pinched particularly at plugs, convenience receptacles, and the point where they exit from the apparatus.
11. Only use attachments/accessories specified by the manufacturer.
12. Use only with the cart, stand, tripod, bracket, or table specified by the manufacturer, or sold with the apparatus. When a cart is used, use caution when moving the cart/apparatus combination to avoid injury from tip-over.

13. Unplug this apparatus during lightning storms or when unused for long periods of time.
14. Refer all servicing to qualified service personnel. Servicing is required when the apparatus has been damaged in any way, such as power-supply cord or plug is damaged, liquid has been moisture, does not operate normally, or has been dropped.
15. ***CAUTION – THESE SERVICING INSTRUCTIONS ARE FOR USE BY QUALIFIED SERVICE PERSONNEL ONLY. TO REDUCE THE RISK OF ELECTRIC SHOCK DO NOT PERFORM ANY SERVICING OTHER THAN THAT CONTAINED IN THE OPERATING INSTRUCTIONS UNLESS YOU QRE QUALIFIED TO DO SO.***
16. ***Use satisfy clause 2.5 of IEC60950-1/UL60950-1 or Certified/Listed Class 2 power source only.***
17. ITE is to be connected only to PoE networks without routing to the outside plant.

Table of Contents

1. Product Description

This manual applies to the IPE1CH network transmitter.

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

The Network Transmitter is a one-port video transmitter including two-way audio, fully featured for security surveillance and remote monitoring needs. It is based on the DSP compression chip, and can digitize one analog video source and make it available on the network as real-time, full frame rate Motion JPEG and H.264 (or MPEG-4) video streams.

The Network Transmitter is equipped with RS-485 port for connecting third party PTZ systems. The alarm input and alarm output can be used to connect various third party devices, such as, door sensors and alarm bells.

Components

The system comes with the following components:


Network Transmitter unit


Installation CD


User's Guide


Mounting Bracket


Mounting Screws

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

Key Features

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

• Dual streams
The Network Transmitter can deliver dual video streams simultaneously at full frame rate in all resolutions up to D1 (720x480 in NTSC, 720x576 in PAL) 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 Transmitter 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 Transmitter includes intelligent capabilities such as enhanced video motion detection. The encoder'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.

• Power over Ethernet
Support for Power over Ethernet (IEEE802.3af) enables the unit, as well as the analog camera 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.

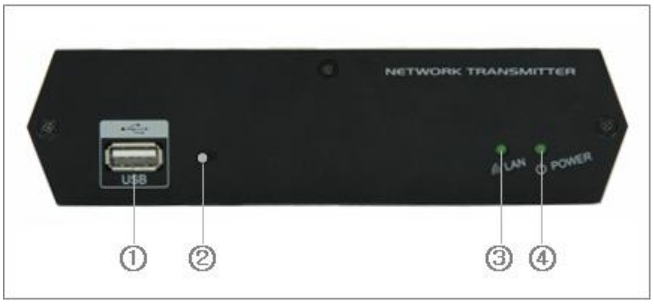
• Audio support
The Network Transmitter also supports two-way audio.

• Improved Security
The Network Transmitter logs all user access, and lists currently connected users. Also, its full frame rate video can be provided over HTTPS.

• 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.

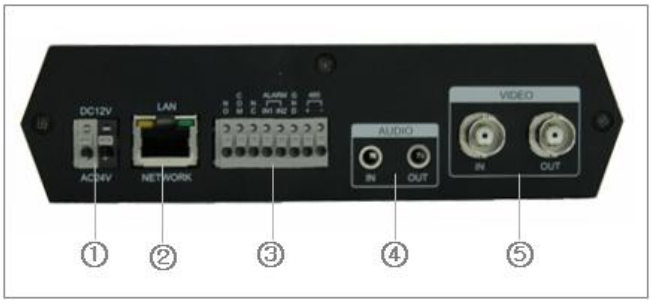
Overview

• Front Panel



NO	Function	Description
1	USB	Not used.
2	Reset Button	Press this button to restore the factory default settings
3	Network Indicator	Lights when a remote user is connected to the unit.
4	Power Indicator	Lights when the power is on. Steady amber during booting and flash amber during factory default. Steady green for normal operation and steady red for failed upgrade.

• Rear Panel



NO	Function	Description
1	Power adaptor connector	Connects the supplied power adapter or an external power supply 12V DC or 24V AC, max. 5W.
2	Network connector(PoE)	RJ-45 port compatible with 10/100Mbps having PoE functionality.
3	8-pin I/O terminal	Connects RS485, alarm input and output.
4	Audio In/Out	Connects the port to the microphone and speaker, which have an amplifier function.
5	Video In/Out	Connects the video input and output.

2. Installation

For the operation of the Network Transmitter, it is necessary to connect a network cable for data transmission, power connection from supplied power adapter and connect a general analog camera. Depending on operation methods, it is possible to connect an alarm cable or audio cable additionally. For its fixation on different locations, please consult with an installer.

Network Connection

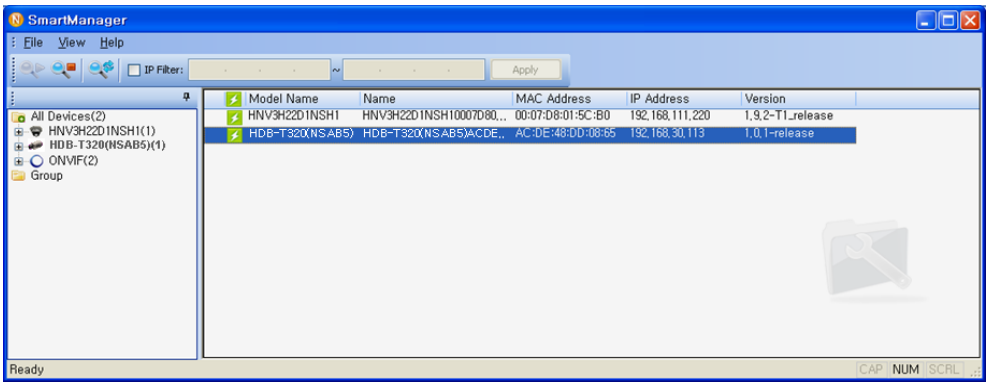
The Network Transmitter supports the operation through the network. Therefore, it is necessary to connect a standard RJ-45 cable to it. Generally a cross-over cable is used for directly connection to PC, while a direct cable is used for connection to a hub.

IP Assignment

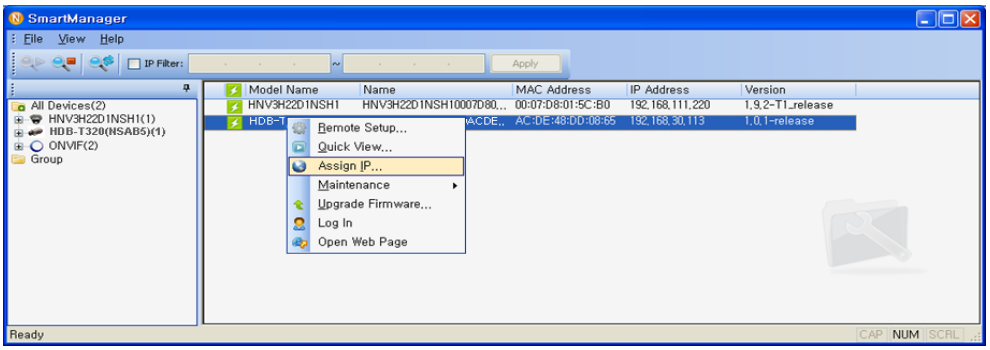
When the Network Transmitter is first connected to the network it has no IP address. So, it is necessary to allocate an IP address to the device with the "Smart Manager" utility on the CD.

1. Connect the Network Transmitter / device to the network and power up.

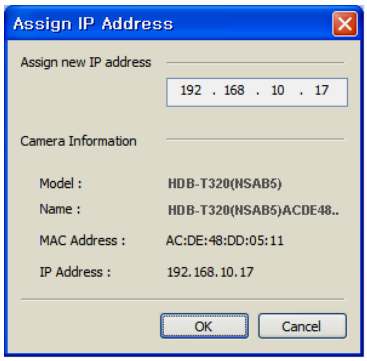
2. Start Smart Manager utility (Start>All Programs>SmartManager>SmartManager), the main window will be displayed, after a short while any network devices connected to the network will be displayed in the list.



3. Select the Network Transmitter on the list and click the right button of the mouse. You can see the popup menu below.



4. Selecting the "Assign IP" in the popup menu displays the following window. Enter a proper IP address and click the OK button.



Enter the required IP address.

Note: For more information, refer to the SmartManger User's Manual.

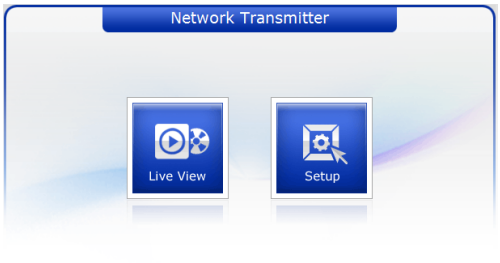
3. Operation

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

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

3.1 Access from a browser

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



4. The Network Transmitter's **Live View** page appears in your browser.

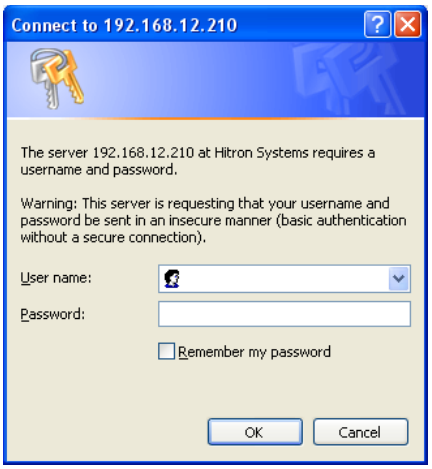
3.2. Access from the internet

Access from the internet Once connected, the Network Transmitter is accessible on your local network (LAN). To access the Network Transmitter from the Internet you must configure your broadband router to allow incoming data traffic to the Network Transmitter. To do this, enable the NAT-traversal feature, which will attempt to automatically configure the router to allow access to the video encoder. This is enabled from Setup>System>Network>NAT.

For more information, please see "3.5.7 System>Network>NAT" of User's Manual.

3.3 Setting the admin password over a secure connection

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



Note: The default administrator username and password is "admin". If the password is lost, the Network Transmitter must be reset to the factory default settings. See "3.8 Resetting to the Factory Default Settings".

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

To set the password via a standard HTTP connection, enter it directly in the first dialog shown below. To set the password via an encrypted HTTPS connection, see "3.5.7 System>Security>HTTPS" of User's Manual.

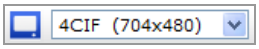
Note: HTTPS (Hypertext Transfer Protocol over SSL) is a protocol used to encrypt the traffic between web browsers and servers. The HTTPS certificate controls the encrypted exchange of information. The default administrator user cannot be deleted.

3.4 Live View Page

The live view page comes in eight screen modes like 704x480(576), 704x240(288), 352x240(288), 176x120(144), 640x480, 320x240, and 160x120. Users are allowed to select the most suitable one out of those modes. Please, adjust the mode in accordance with your PC specifications and monitoring purposes.

• General controls

The video drop-down list allows you to select a customized or pre-programmed video stream on the live view page. Stream profiles are configured under Setup > Basic Configuration > Video & Image. See Basic Configuration, on page 15 for more information.



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

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

The preset drop-down list allows you to select the preset number for the PTZ camera being used. This icon is inactivated if the PTZ settings are not set.

• Control toolbar

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


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


The Pause button pause the video stream being played.


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


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


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

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

 The PTZ button activates a pop-up window for Pan, Tilt and Zoom control.

 Use this scale to control the volume of the speakers.

 Use this scale to control the volume of the microphone.

 Use this scale to control the volume of the speakers and microphones.

• Pan/Tilt/Zoom controls

If the Network Transmitter has been appropriately configured, the Live View page displays the controls available for the installed Pan Tilt Zoom (PTZ) device. The administrator can enable/disable the controls for specified users.

Please see "3.6 PTZ Control" for more information.

• Video and Audio Streams

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

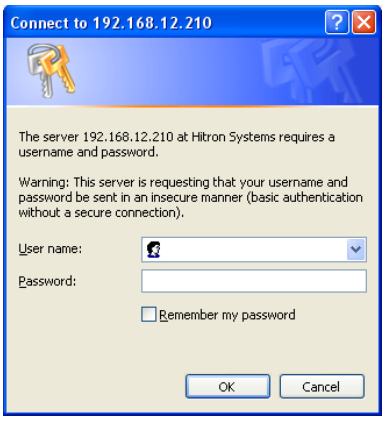
The Live View page in the network transmitter provides access to H.264, MPEG-4 and Motion JPEG video streams, and to the list of available video streams. Other applications and clients can also access these video streams/images directly, without going via the Live View page.

3.5 Setup

This section describes how to configure the network transmitter, 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.

You can configure the network transmitter 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 Transmitter for the first time, the "Admin Password" dialog appears. Enter your admin name and password, set by the administrator.

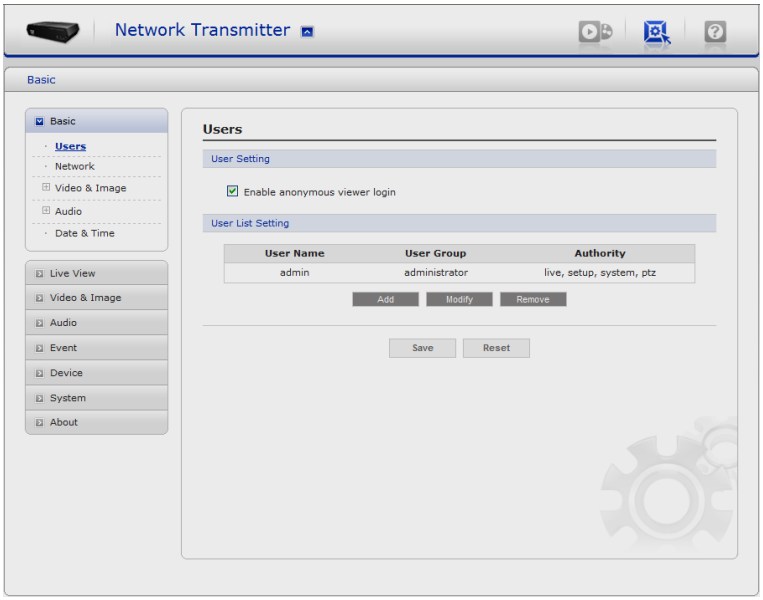


Note: If the password is lost, the Network Transmitter must be reset to the factory default settings. See "3.8 Resetting to the Factory Default Settings".

3.5.1 Basic Configuration

3.5.1.1 Users

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



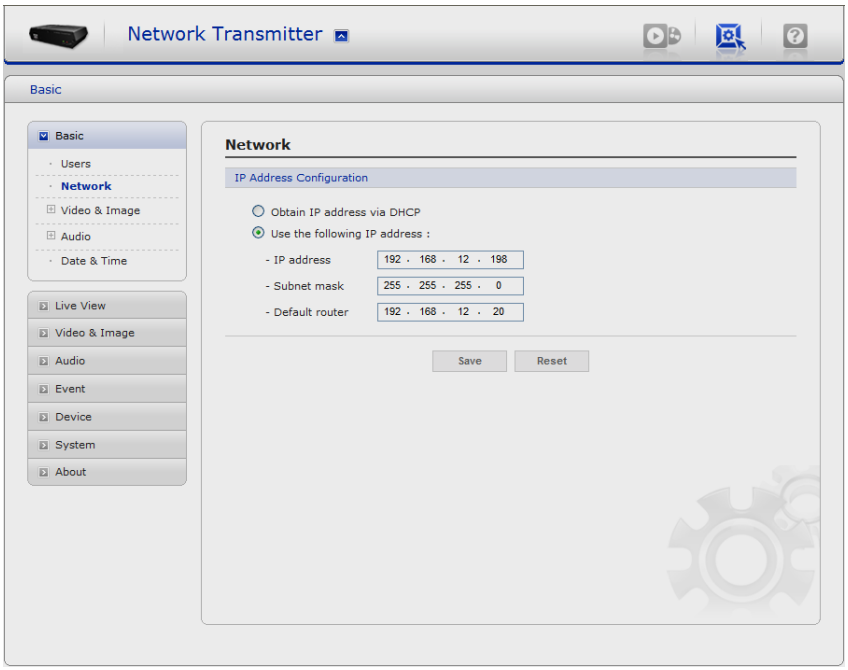
The **user list** displays the authorized users and user groups (levels):

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

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

3.5.1.2 Network

The network transmitter 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 video encoder can be set automatically via DHCP, or a static IP address can be set manually. If IPv6 is enabled, the video encoders receive 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 IP address, please see Setup> System>Security>Network.



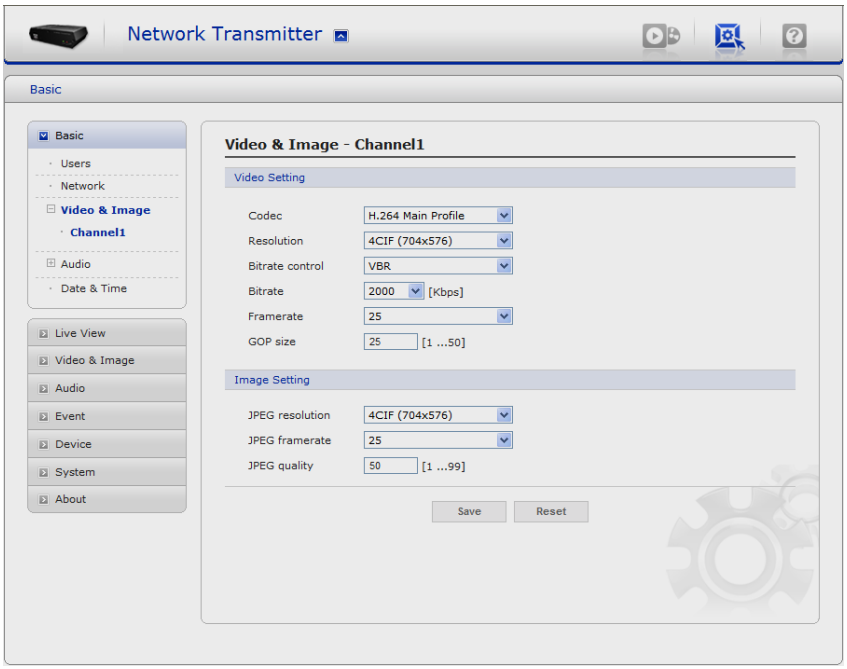
• Obtain IP address via DHCP - Dynamic Host Configuration Protocol (DHCP) is a protocol that lets network administrators centrally manage and automate the assignment of IP addresses on a network. DHCP is enabled by default. Although a DHCP server is mostly used to set an IP address dynamically, it is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

Notes:

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

3.5.1.3 Video & Image



• Video Setting

-. Codec

The codec settings are separated into MPEG4 and H.264.

H.264 is also known as MPEG-4 Part 10. This is the new generation compression standard for digital video. This function offers higher video resolution than Motion JPEG or MPEG-4 at the same bit rate and bandwidth, or the same quality video at a lower bit rate.

-. Profile

There are 4 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 MP(Main Profile):

Primarily for low-cost applications that requires additional error robustness, this profile is used rarely in videoconferencing and mobile applications, it does add additional error

resilience tools to the Constrained Baseline Profile. The importance of this profile is fading after the Constrained Baseline Profile has been defined.

* H.264 BP(Base 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.

* MPEG4 SP(Simple Profile):
Mostly aimed for use in situations where low bit rate and low resolution are mandated by other conditions of the applications, like network bandwidth, device size etc.

* MPEG4 ASP(Advanced Simple Profile):
Its notable technical features relative to the Simple Profile, which is roughly similar to H.263, including "MPEG"-style quantization, interlaced video, B pictures (also known as B Frames), Quarter Pixel motion compensation (Qpel), Global motion compensation (GMC).

-. Resolution
It enables users to determine a basic screen size when having an access through the Web Browser or PC program. The screen size control comes in seven modes like 4CIF(704x480), 2CIF(704x240), CIF(352x240), QCIF(176x120), VGA(640x480), QVGA(320x240), and QQVGA(160x120). Users can reset the selected screen size anytime while monitoring the screen on a real-time basis.

-. Bitrate control
Limiting the maximum bit rate helps control the bandwidth used by the H.264 or MPEG-4 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 lost when the limit is exceeded.
Note that the maximum bit rate can be used for both variable and constant bit rates.

The bitrate can be set as Variable Bit Rate (VBR) or Constant Bit Rate (CBR). 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.
CBR allows you to set a fixed target bitrate that consumes a predictable amount of bandwidth. As the bit rate would usually need to increase for increased image activity, but in this case cannot, the frame rate and image quality are affected negatively. To partly compensate for this, it is possible to prioritize either the frame rate or the image quality whenever the bit rate needs to be increased. Not setting a priority means the frame rate and image quality are equally affected.

-. Compression
When it is necessary to adjust a smooth transmission status according to network situations, users can increase the compressibility to carry out the network transmission stably. On the other hand, when it is necessary to maintain a detailed monitoring screen by enhancing the image quality, users can do so by decreasing the compressibility. In ease case, please adjust this function according to the network status and monitoring purposes. The default is 2000(Kbps).

-. Framerate
Upon the real-time play, users should select a frame refresh rate per second. If the rate is high, the image will become smooth. On the other hand, if the rate is low, the image will not be natural but it can reduce a network load.

-. GOP size
Select the GOP(Group of Picture) size. If users want to have a high quality of fast image one by one, please decrease the value. For the purpose of general monitoring, please do not change a basic value. Such act may cause a problem to the system performance. For the details of GOP setting, please contact the service center.

• Image 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.

-. JPEG resolution
Same as the video settings.

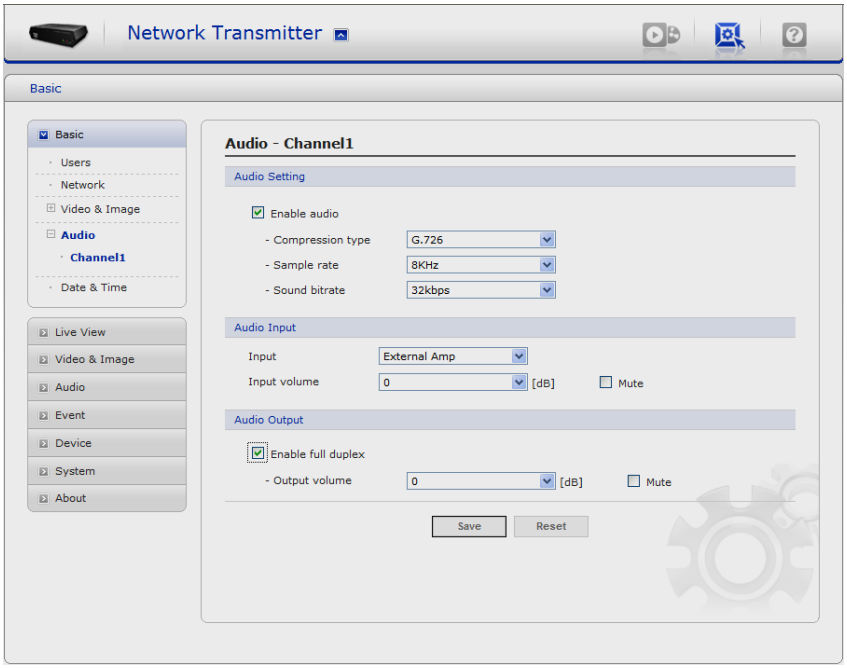
-. JPEG framerate
Same as the video settings.

-. JPEG quality
Select the picture quality. If users want to have a high quality of fast image one by one, please decrease the value. For the purpose of general monitoring, please do not change a basic value. Such act may cause a problem to the system performance.

When satisfied with the settings, click **Save**, or click **Reset** to revert to previously saved settings.

3.5.1.4 Audio

The Network Transmitter 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, G726.

-. 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 external line source can be connected to the Line/Mic in jack of the network transmitter.

-. 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 transmitter.

• Audio Output

-. Enable full duplex
Check the box to enable Full Duplex mode. It means that you can transmit and receive audio (talk and listen) at the same time, without having to use any of the controls. This is

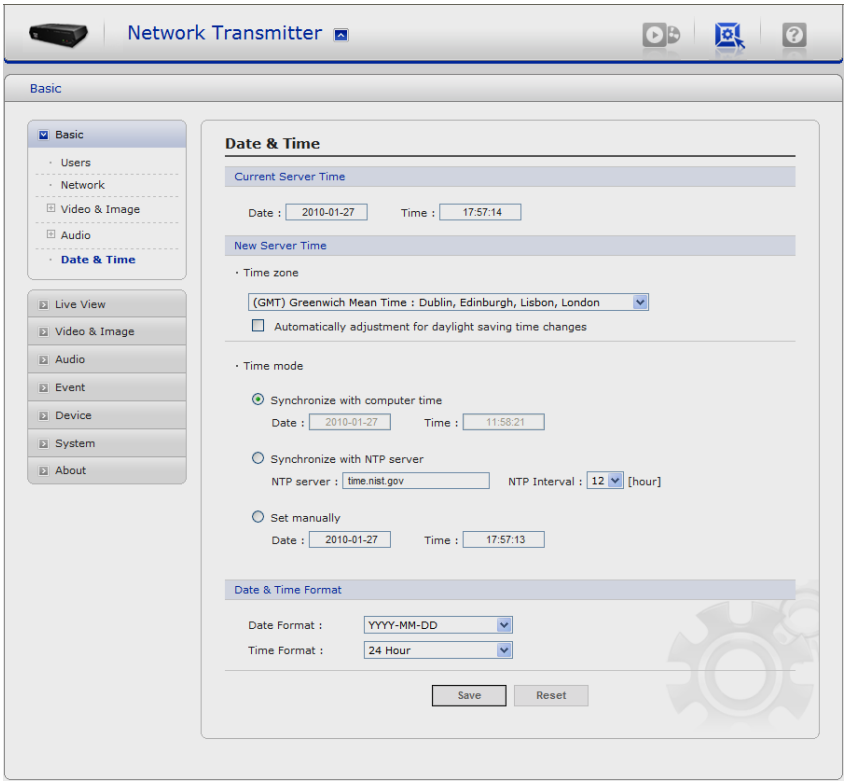
just like having a telephone conversation.
This mode requires that the client PC has a sound card with support for full-duplex audio.

Uncheck the box enable Simplex mode. The simplex mode only transmits audio from the network transmitter to any web client. It does not receive audio from other web clients.

-. Output volume
If the sound from the speaker is too low or high it is possible to adjust the output gain for the active speaker attached to the network transmitter.

When satisfied with the settings, click Save, or click Reset to revert to previously saved settings.

3.5.1.5 Date & Time



• Current Server Time

It displays the current date and time (24h clock). The time can be displayed in 12h clock format in the overlay (see below).

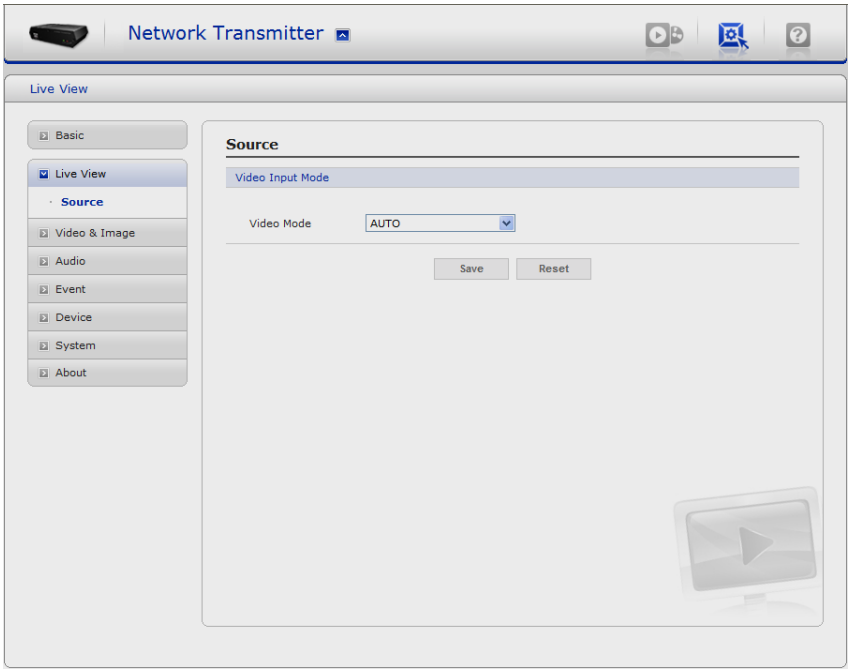
• New Server Time

Select your time zone from the drop-down list. If you want the server clock to automatically adjust for daylight savings time, select the "Automatically adjustment 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 video encoder will obtain the time from an NTP server every 60 minutes.
-. Set manually - this option allows you to manually set the time and date.

3.5.2 Live View

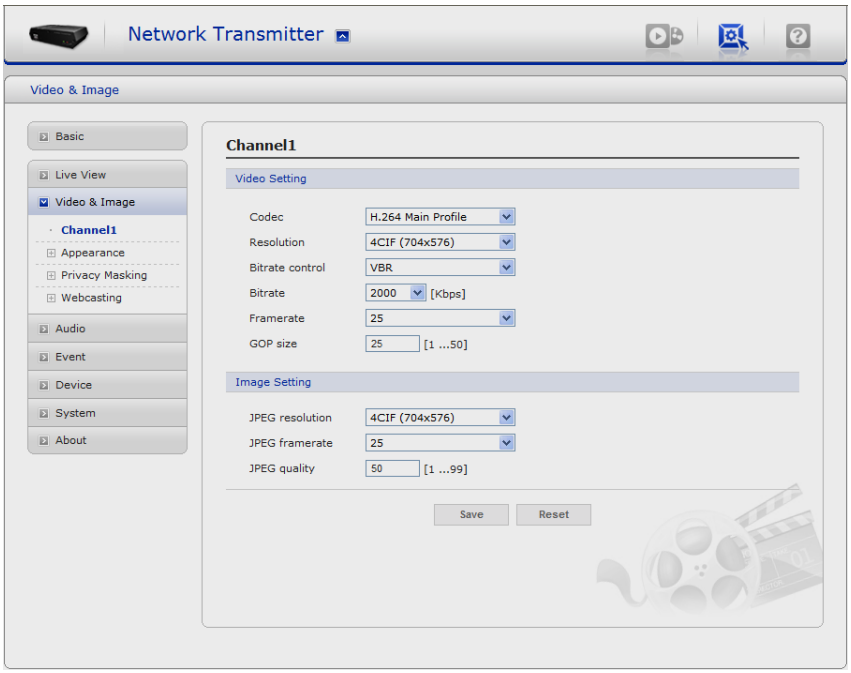
You can select video input mode in this page. If you set to AUTO, the network transmitter check automatically whether the video input signal is NTSC or PAL.



The factory default is AUTO.

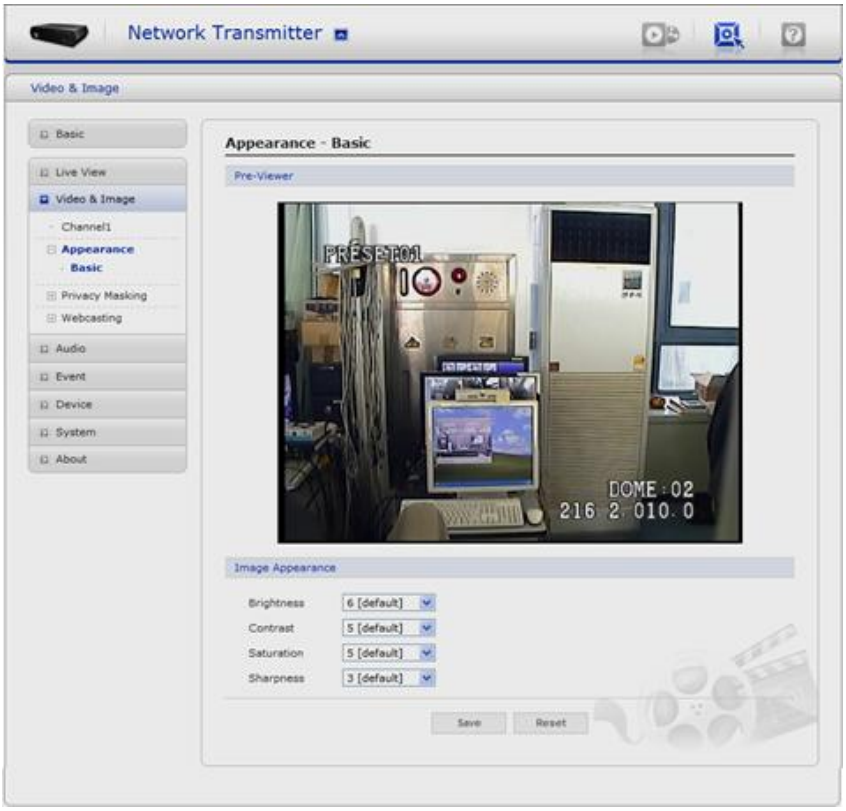
3.5.3 Video & Image

▼ Channel1



Refer to "3.5.1.3 Video & Image" for more details.

▼ **Appearance - Basic**

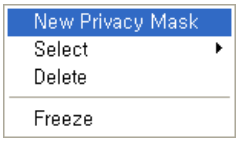


• Image Appearance
-. Brightness - The image brightness can be adjusted in the range 1-255, where a higher value produces a brighter image.
-. Color level -Select an appropriate level by entering a value in the range 1-14. Lower values mean less color saturation.
-. Saturation - Adjust the image's contrast by raising or lowering the value in this field.
-. 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 would be less sharp.

▼ Privacy Masking - Basic

The privacy masking function allows you to mask parts of the video image to be transmitted. You can set up to eight privacy masks and the color of privacy masks is black.

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



To create a mask window, follow steps:

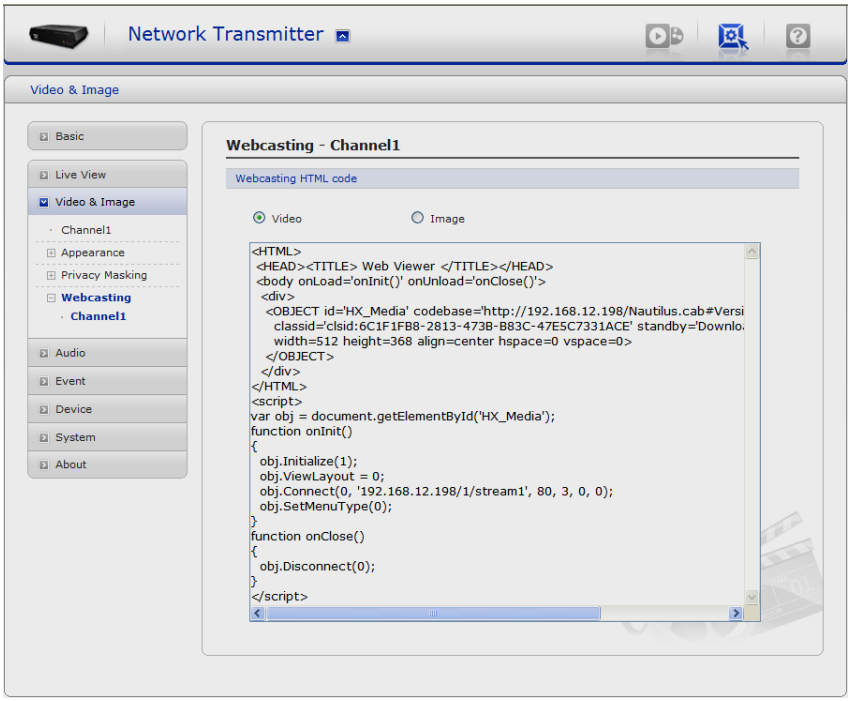
1. Click the right button of mouse to see the mouse menu.
2. Select New Privacy Mask in the mouse menu.
3. Click and drag mouse to designate a mask window area.

You can also modify or delete a mask window index. Select an index and then, modify items or delete button.

Select "Enable" to activate the privacy masking function.

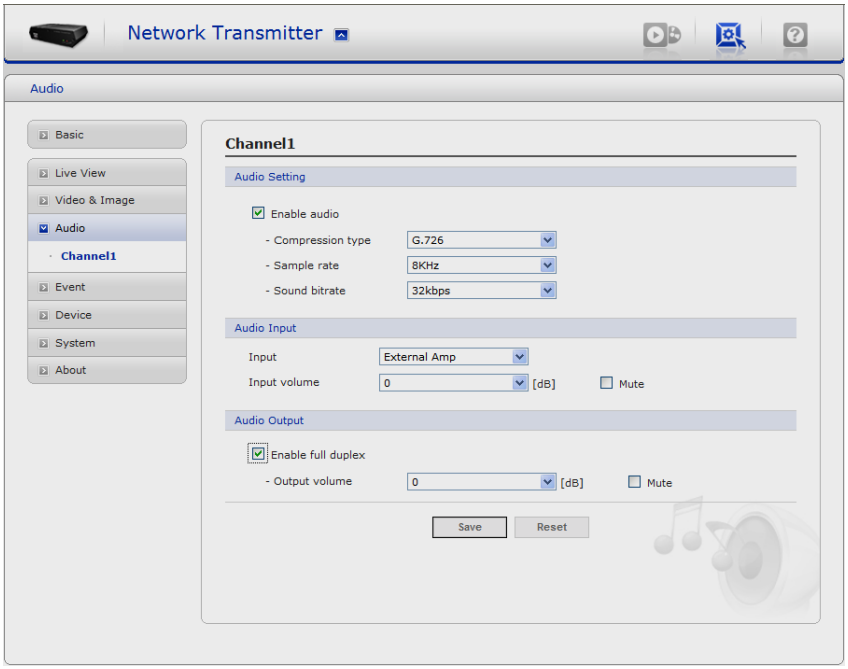
▼ Webcasting – Channel1

The network transmitter 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 "3.5.1.1 Users" for more details.

3.5.4 Audio

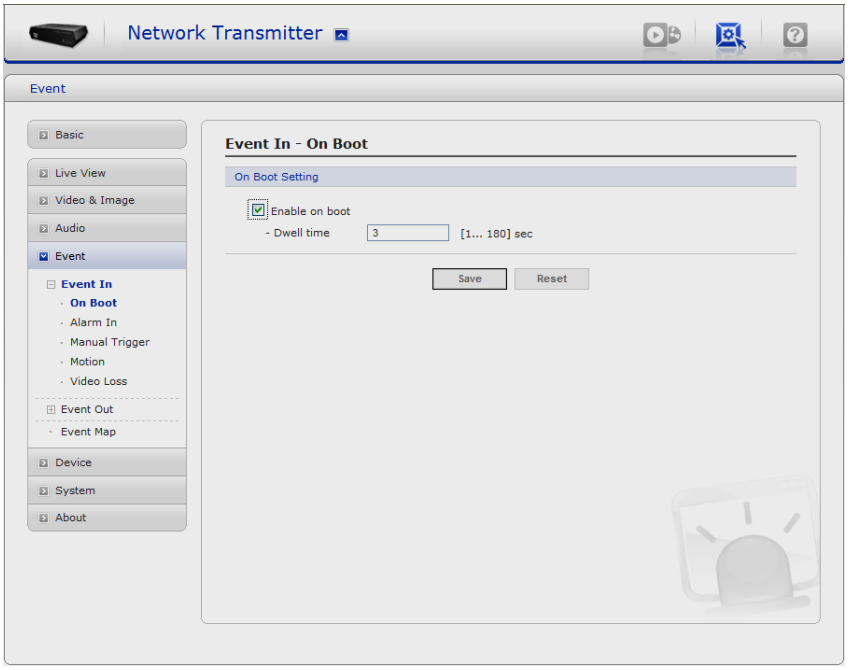


Refer to "3.5.1.4 Audio" for more details.

3.5.5 Event

3.5.5.1 Event-In

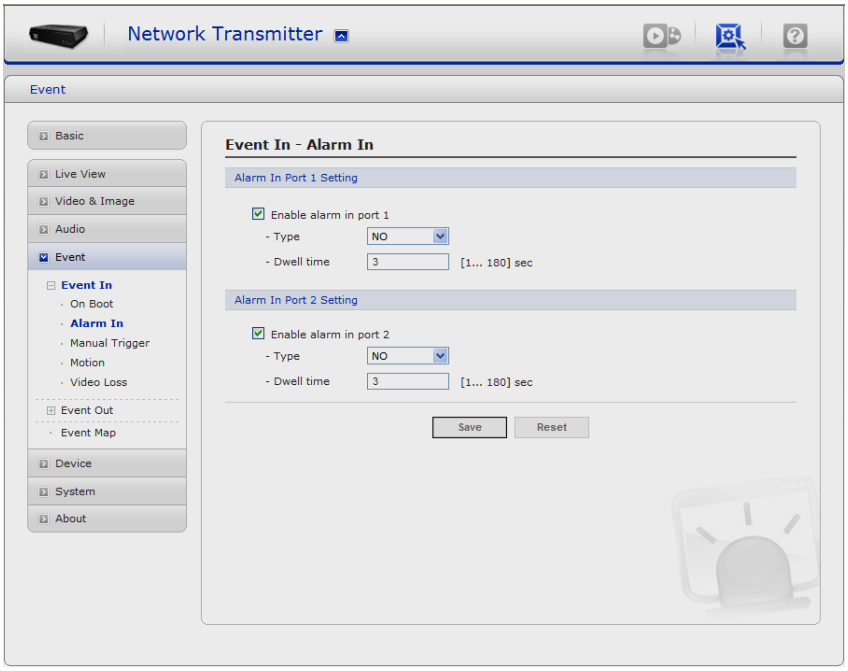
▼ On Boot



This is used to trigger the event every time the Network Transmitter is started.

Select "Enable" to activate the motion event.

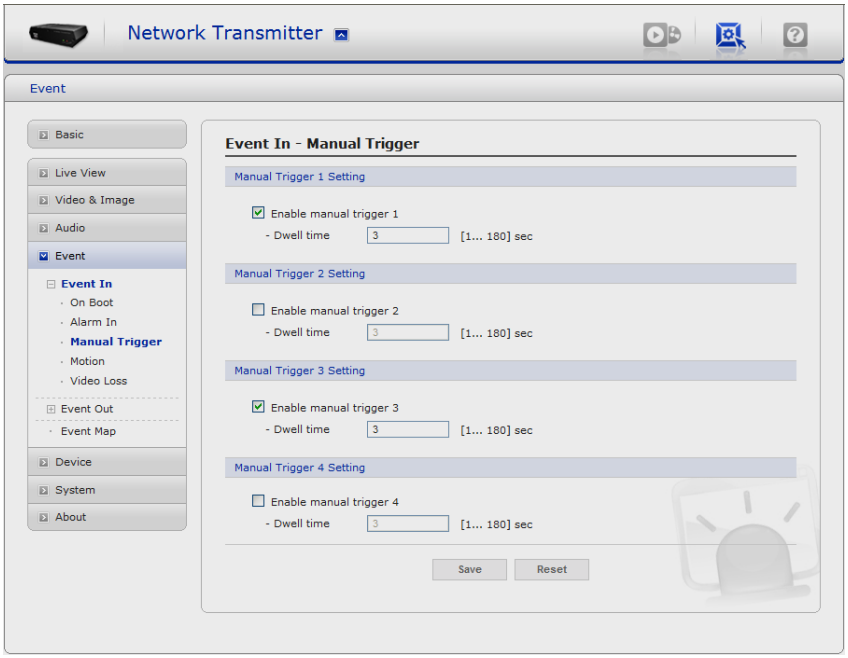
▼ Alarm In



Select "Enable" to activate the alarm event. The network transmitter supports 2 alarm input ports.

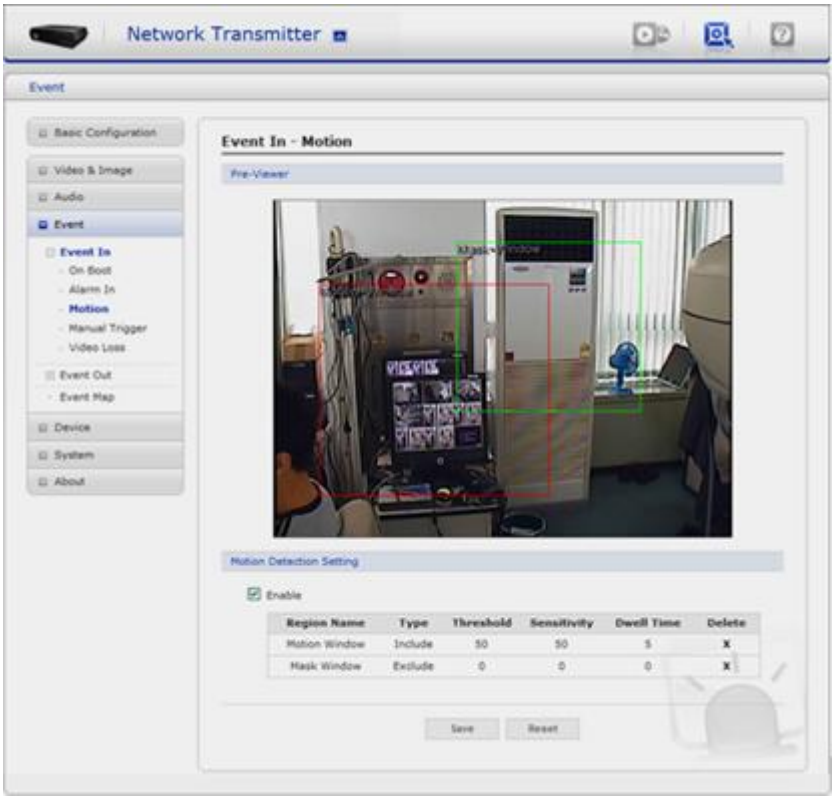
-. Type - Choose the type of alarm you wish to use from the drop-down list.
-. Dwell Time - Set the dwell time of an event lasts for the specified dwell time from the point of detection of an alarm input.

▼ Manual Trigger



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

▼ Motion



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

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

• Pre-Viewer

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

To create a motion or mask window, follow steps:

4. Click the right button of mouse to see the mouse menu.
5. Select New Motion (or Mask) Window in the mouse menu.
6. Click and drag mouse to designate a motion window area.

• Motion Detection Setting
The behavior for each window is defined by adjusting the Threshold and Sensitivity, as described below.

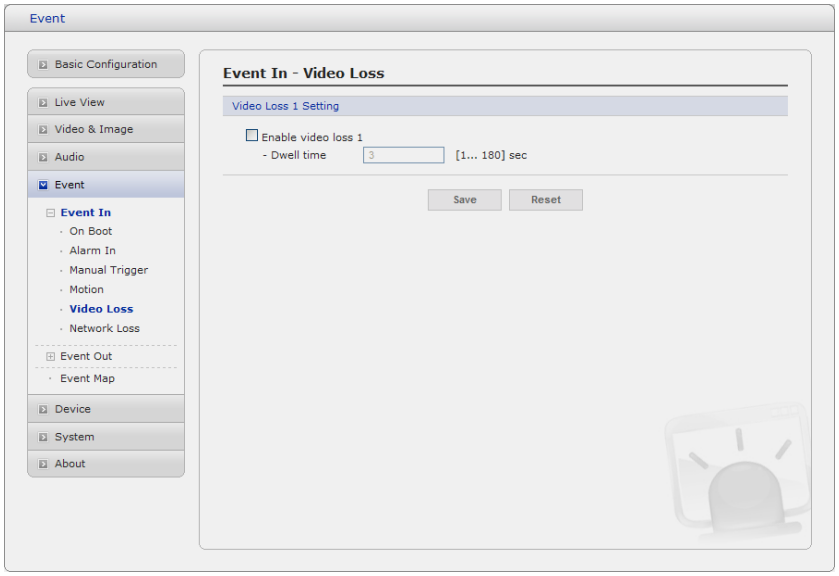
A motion index is a set of parameters describing Window Name, Type, Threshold, Sensitivity, and Dwell Time. Window Types is one of Motion and Mask windows.

-. Threshold - Sets up the threshold for the motion detection.
-. Sensitivity - Sets up the sensitivity for the motion detection.
-. Dwell Time - Set the hold time an event lasts for the specified hold time from the point of detection of a motion.

You can also modify or delete a motion index. Select an index and then, click the Modify or Delete button.

Select "Enable" to activate the motion event.

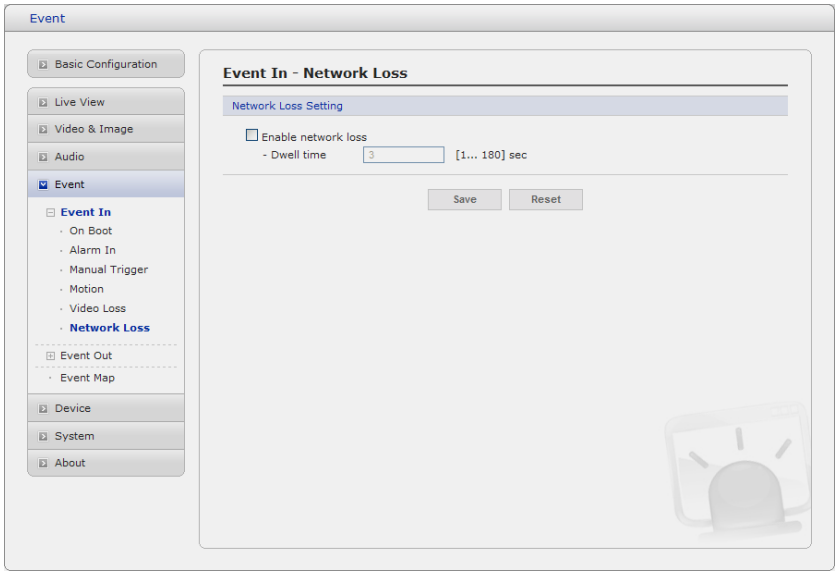
▼ Video Loss



This is used to trigger the video loss event. When there is no input signal from a video input connector, it can be processed as an event.

Select "Enable" to activate the Network Loss event.

▼ Network Loss



This is used to trigger the event every time the network connection is failed. Select "Enable" to activate the Network Loss event.

3.5.5.2 Event-Out

▼ SMTP(E-Mail)

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

• SMTP(E-Mail) Setting

Select "Enable" to activate the SMTP operation.

-. Mail Server / Port - Enter the host names (or IP addresses) and port numbers for your mail server in the fields provided, to enable the sending of notifications and image email messages from the network transmitter to predefined addresses via SMTP.

-. Sender – Enter the email address to be used as the sender for all messages sent by the Network Transmitter.

-. Interval - Represents the frequency of the email notification when an event occurs.

-. Aggregate events - Shows the maximum number of emails sent within each interval.

If your mail server requires authentication, check the box for Use authentication to log in to this server and enter the necessary information.

-. User Name / Password - Enter the User Name and Password as provided by your network administrator or ISP (Internet Service Provider).

To ensure that the login procedure is performed as securely as possible when using SMTP authentication, you must define the weakest authentication method allowed.

-. Login Method - Set the Weakest method allowed to the highest/safest method supported by the mail server. The most secure method is listed in the drop-down list: Login / Plain / CRAM-MD5 / DIGEST-MD5

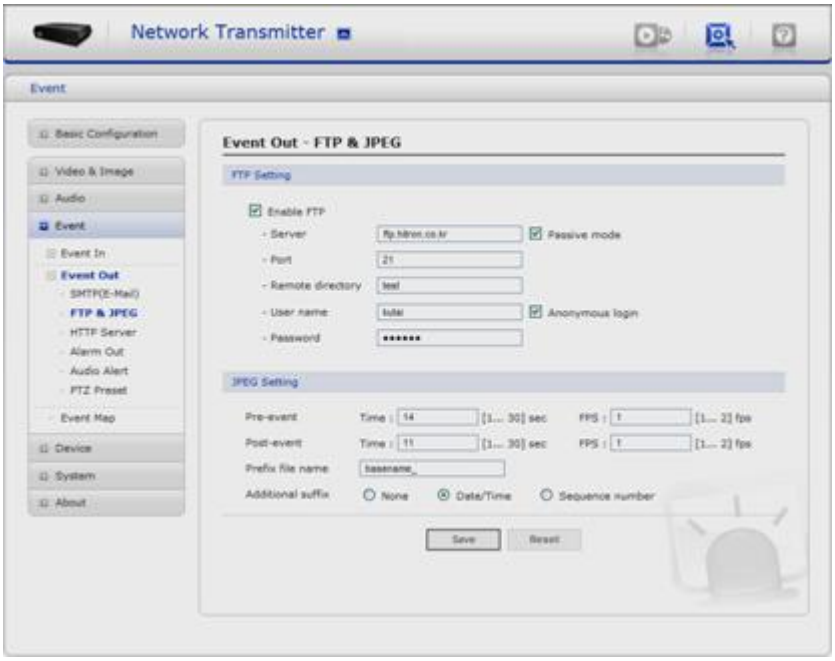
• SMTP(E-Mail) Receiver

-. Receiver - Enter an email address. You can also register the e-mail address of recipients up to 5.

• 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.

▼ FTP & JPEG



When the network transmitter detects an event, it can record and save images to an FTP server. Images can be sent as e-mail attachments. Check the box to enable the service.

• 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.

-. Use passive mode - Under normal circumstances the Network Transmitter 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 Transmitter actively initiates both the FTP control and data connections to the target server. This is normally desirable if there is a firewall between the network transmitter 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

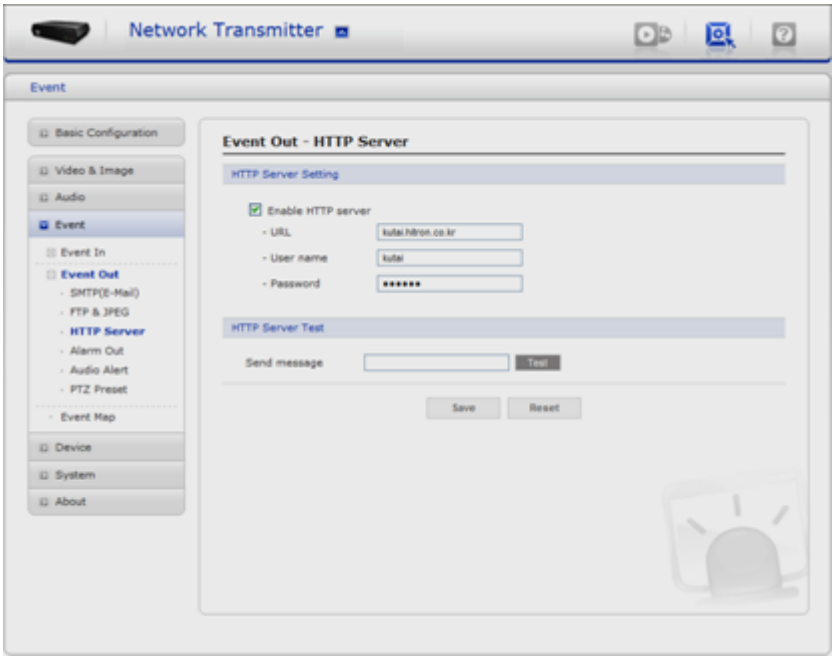
-. Pre-event - A pre-event buffer contains images from the time immediately preceding the event trigger. These are stored internally in the server. This buffer can be very useful when checking to see what happened to cause the event trigger.
Check the box to enable the pre-trigger buffer, enter the desired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

▼ HTTP Server



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

• HTTP Server Setting

-. Name - The name of the HTTP event server. Use a descriptive name.

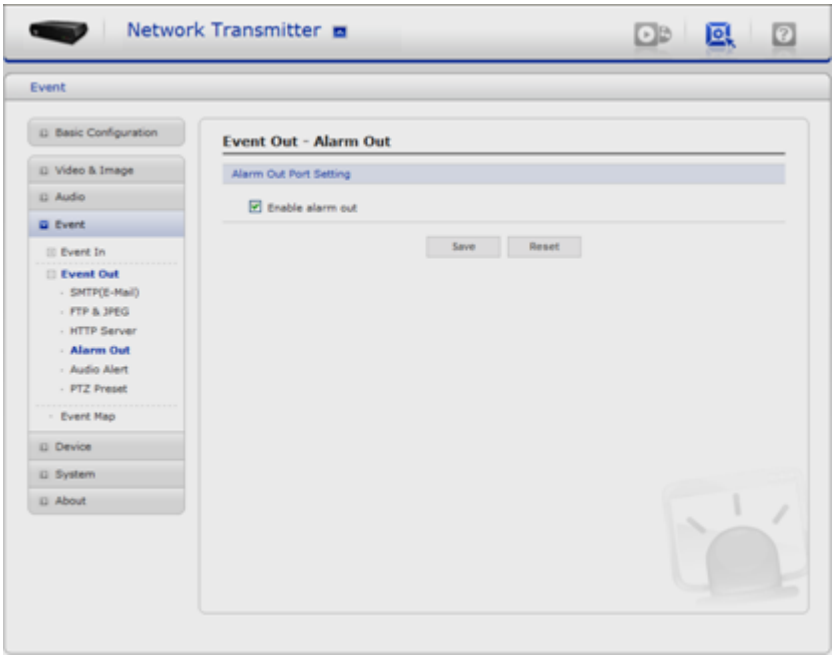
-. URL - The network address to the server and the script that will handle the request. For example: http://192.168.12.244/cgi-bin/upload.cgi

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

• HTTP Server Test

When the setup is complete, the connection can be tested by clicking the Test button.

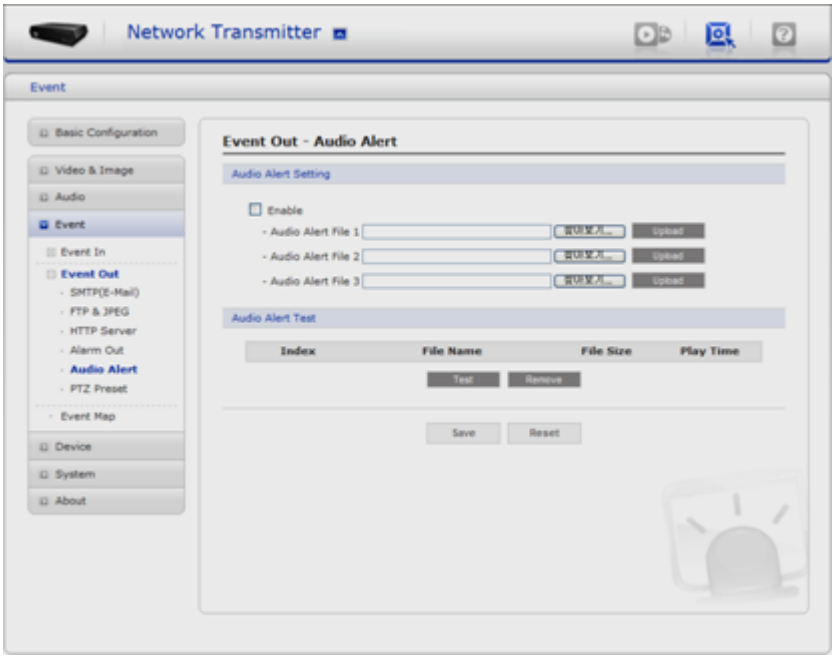
▼ Alarm Out



When the network transmitter detects an event, it can control external equipment connected to its alarm output port. Check the box to enable and then select either:

-. Enable – When you select "Enable alarm out", the output will be activated for as long as the event is active.

▼ Audio Alert



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

• Audio Alert Setting

To use the audio alert with the Network Transmitter, the G.711 audio 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.

An audio file for Audio Alert can be made by Audio Recorder tool in the NautilusClient16 software.

• Audio Alert Test

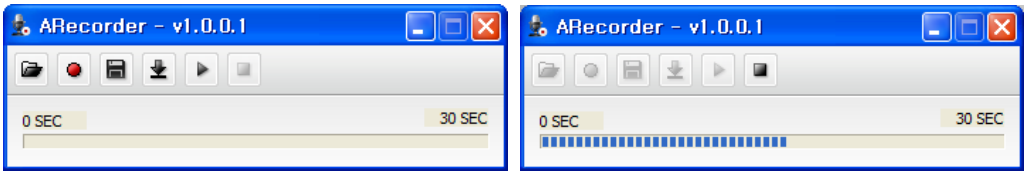
When the setup is complete, the audio output can be tested by clicking the Test button. To remove an audio file, select index and click the **Remove** button.

Note: For a proper operation of Audio Alert, you must enable "full duplex" in Audio setting page.

Audio Recorder

To use Audio Recorder tool to make an audio file for Audio Alert function, you must install the NCTitanium on the installation CD at first.

Start the ARecorder program (All Programs>NCTitanium>Tools>ARecorder) in your PC, the main window will be displayed as below.



The description of each button in the ARecorder window follows.

 Open: Open an audio file.

 Capture: Capture audio from the microphone in your PC.

 Save: Save a captured file to your PC. (PCM format)

 Encode: Encode a current capture file or opened PCM file to G.711 file for Audio Alert.

 Play: Play a current audio file.

 Stop: Stop playing audio.

Procedures to make an audio file in G.711 format for Audio Alert.

1. Connect the microphone in your PC.

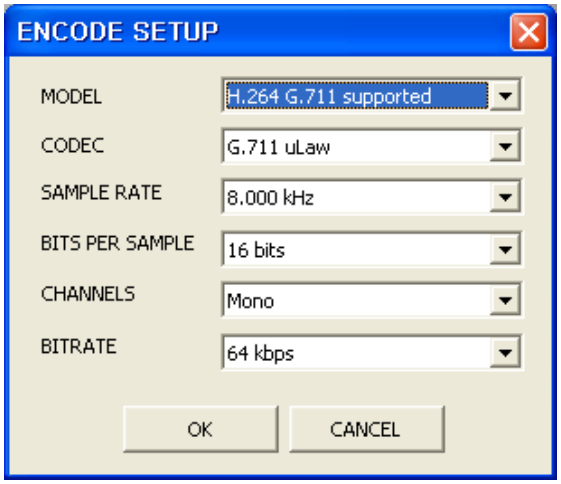
2. Click the Capture button and talk to the microphone to record the audio or voice. You can record up to 30 seconds. Click the Stop button to stop on capturing.

3. Click the Save button and then set the file name to save a current capture file with PCM format.

   If you don't need to make any PCM file, skip this step and then go to the step 5 directly.

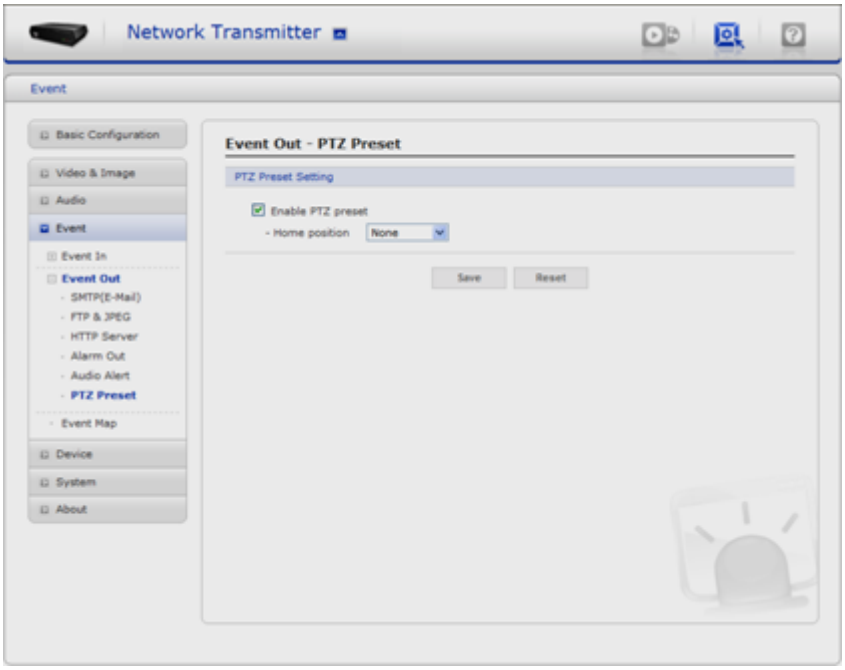
4. Click the Open button and then select the file name to open an audio file in PCM format.

5. Click the Encode button to encode a current audio file to G.711 format for Audio Alert. Set the file name and encode parameters.



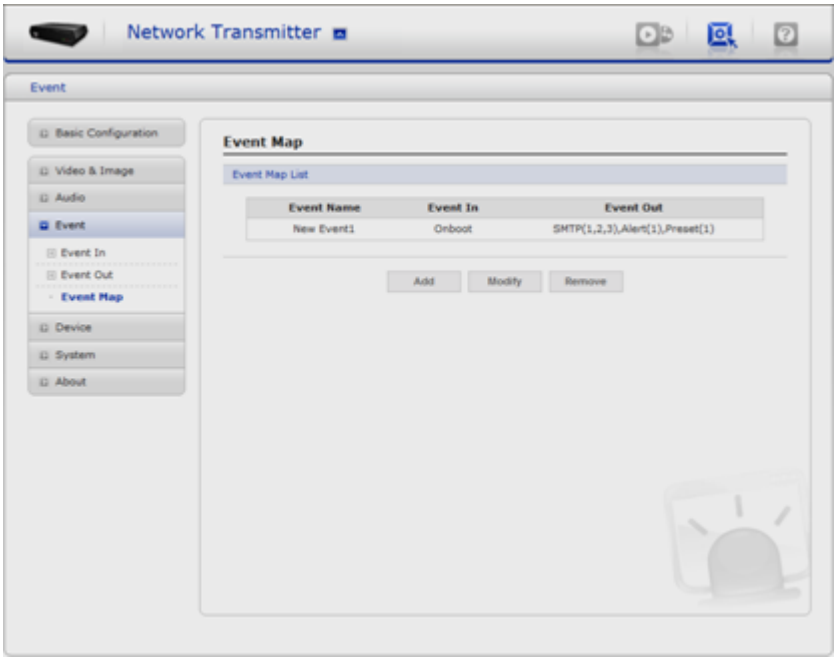
Caution: All parameters must be synchronized with ones in audio setting page of network devices for a proper operation.

▼ **PTZ Preset**



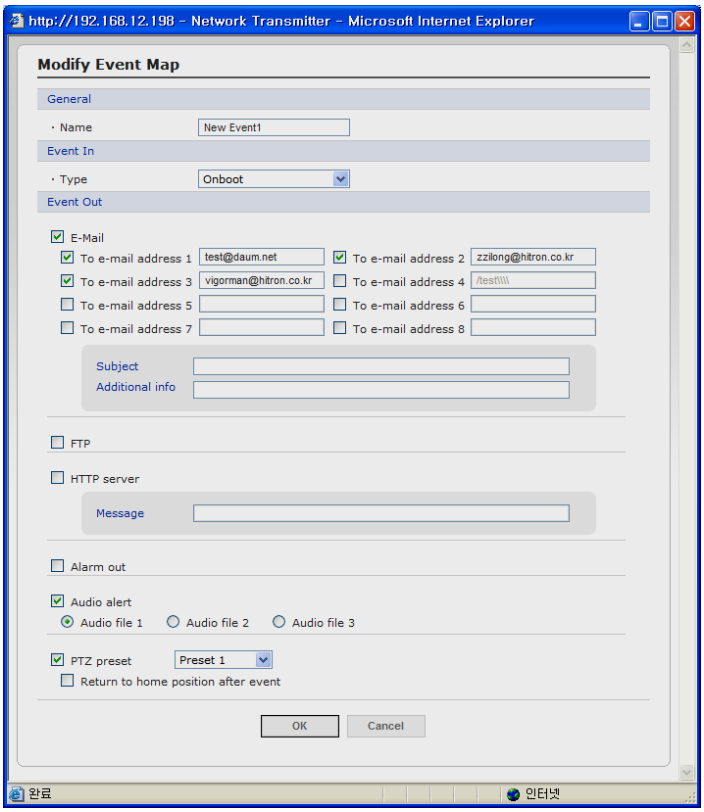
When the network transmitter detects an event, you can make a PTZ camera connected to its RS485 port to move to a predefined preset position. Check the box to enable the service and return to the Home position once the event has ended.

3.5.5.3 Event Map



The event map allows you to change the settings and establish a schedule for each event trigger from the network transmitter. You can register the event map up to max. 16.

Click Add button to make a new event map and you can see a popup window as below.



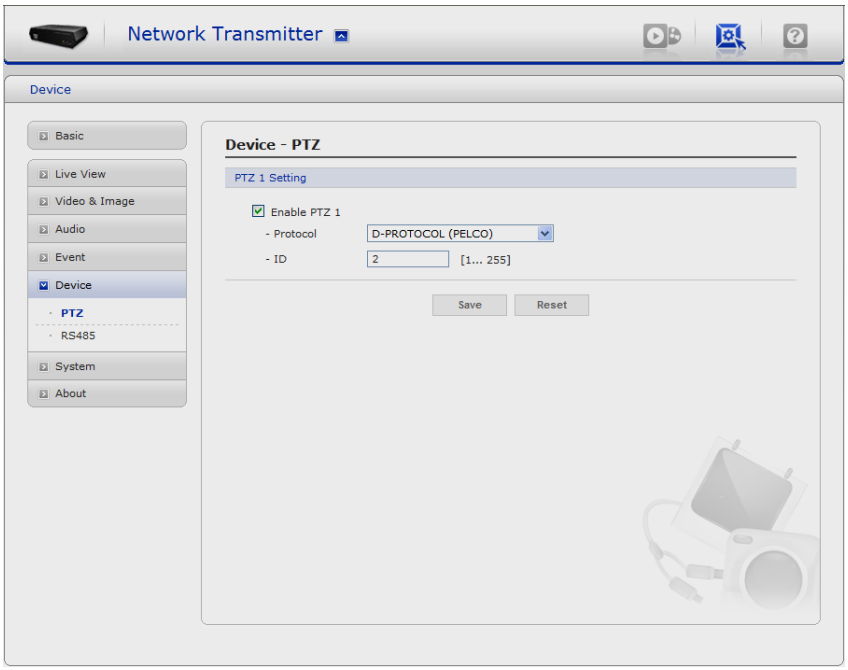
• General
Enter the name for a new event map.

• Event In
Select an event type in the drop down list.

• Event Out
-. E-mail: Select email addresses you want to send via email that an event has occurred.
-. FTP: Select checkbox beside FTP to record and saves images to an FTP server when an event has occurred.
-. HTTP Server: It sends notification messages to an HTTP server that listens for these. The destination server must first be configured on the Event In page. Enter a message you want to send.
-. Audio Alert: Select a Audio alert file the Network Transmitter output when audio alert event triggered. The Audio alert file must first be configured on the Event In page.
-. PTZ Preset: Select checkbox to activate and a preset number in the drop down list. Check the box to return to the Home position once the event has ended.

3.5.6 Device

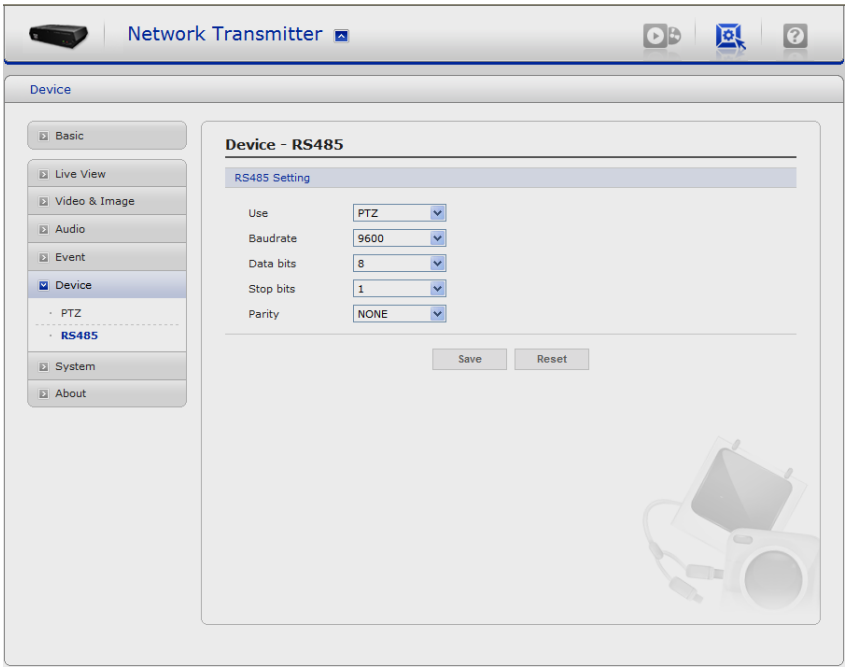
▼ PTZ



The Network Transmitter supports several PTZ devices. Using an appropriate cable, connect the device to your RS-485 port. These ports are available via the I/O terminal connector.

• PTZ settings
  -. Enable - Check the box to enable the PTZ function.
  -. Protocol - Select the PTZ camera you wish to configure.
  -. Device ID - Setting PTZ Camera Address (ID)

▼ RS485

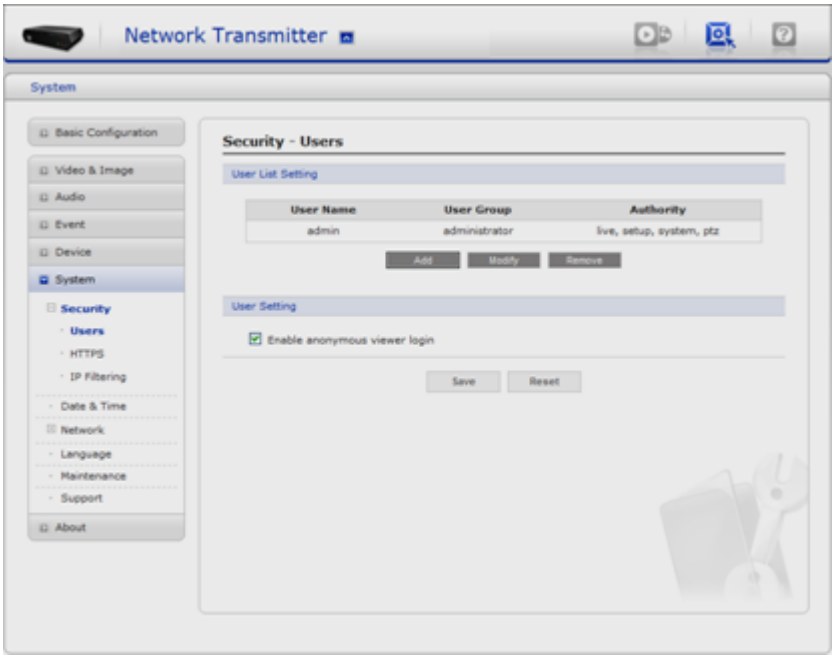


• RS485 settings
-. Baud rate - Select a Baud Rate in the drop-down list. (Default 9600 bps)
-. Data bits - Select Data Bits in the drop-down list. (Default None)
-. Parity bits - Select Parity Bits in the drop-down list. (Default 8 bits)
-. Stop bits - Select Stop Bits in the drop-down list. (Default 1 bit)

Factory Default:
-. Baud rate : 9600 bps
-. Data bits : None
-. Parity bits : 8 bits
-. Stop bits : 1 bit

3.5.7 System
3.5.7.1 Security

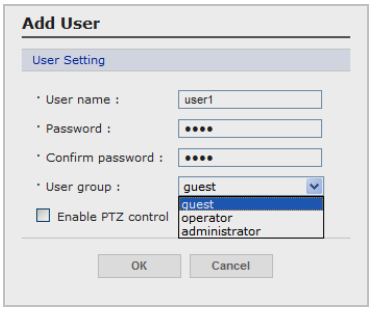
▼ **Users**



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 Transmitter without the user account. When using the user account, users have to try log-in at every access.

• User List Setting
  This section shows a registered user account. Enter a user name and password to be added, and register them by pressing the Add button. You can see the pop-up window as below.



▼ HTTPS

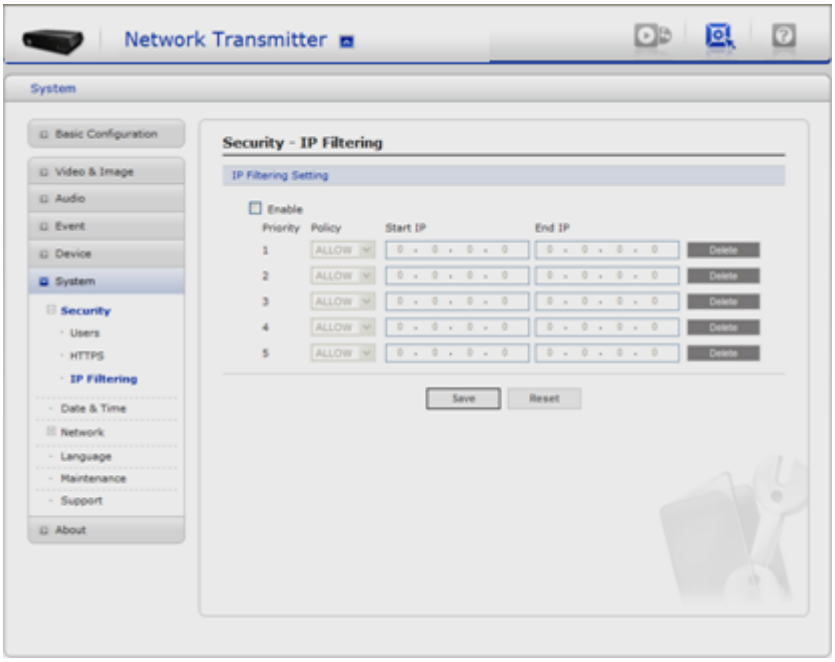
For greater security, the Network Transmitter can be configured to use HTTPS (Hypertext Transfer Protocol over SSL (Secure Socket Layer)). That is, all communication that would otherwise go via HTTP will instead go via an encrypted HTTPS connection.

- 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 & HTTPS by default).
  -. HTTP
  -. HTTPS
  -. HTTP & HTTPS

- Upload Certificate
  To use HTTPS for communication with the Network Transmitter, An official certificate issued by a CA (Certificate Authority) must be uploaded from your PC. Provide the path to the certificate directly, or use the **Browse** button to locate it. Then click the **Upload** button.

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

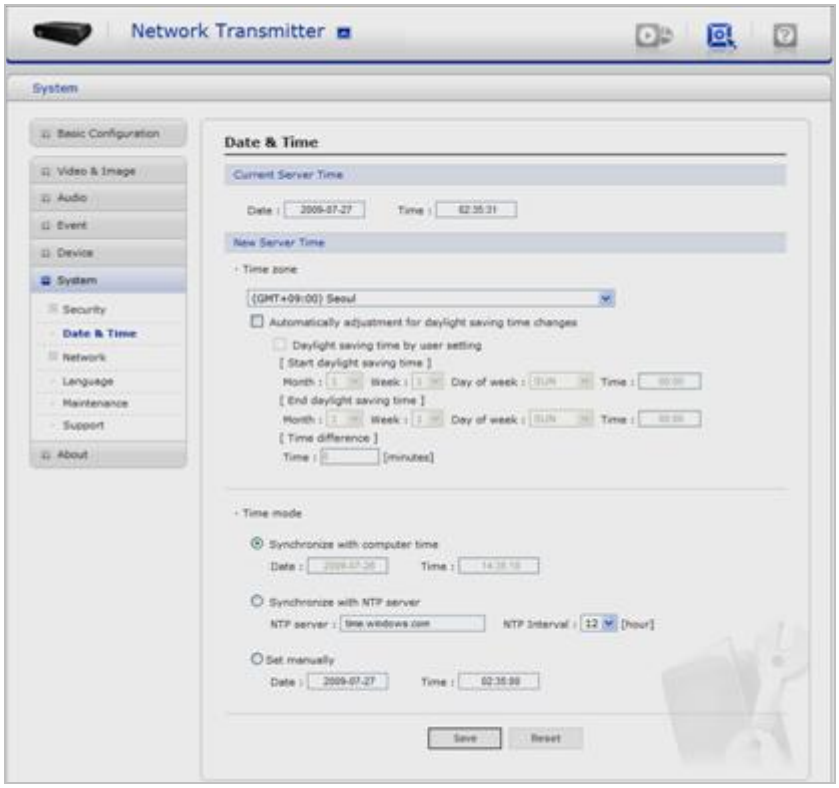
▼ IP Filtering



Checking the **Enable IP address filtering** box enables the IP address filtering function. Up to 256 IP address entries may be specified (a single entry can contain multiple IP addresses).
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. See also the online help for more information.

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.

3.5.7.2 Date & Time



• Current Server Time

It displays the current date and time (24h clock). The time can be displayed in 12h clock format in the overlay (see below).

• New Server Time

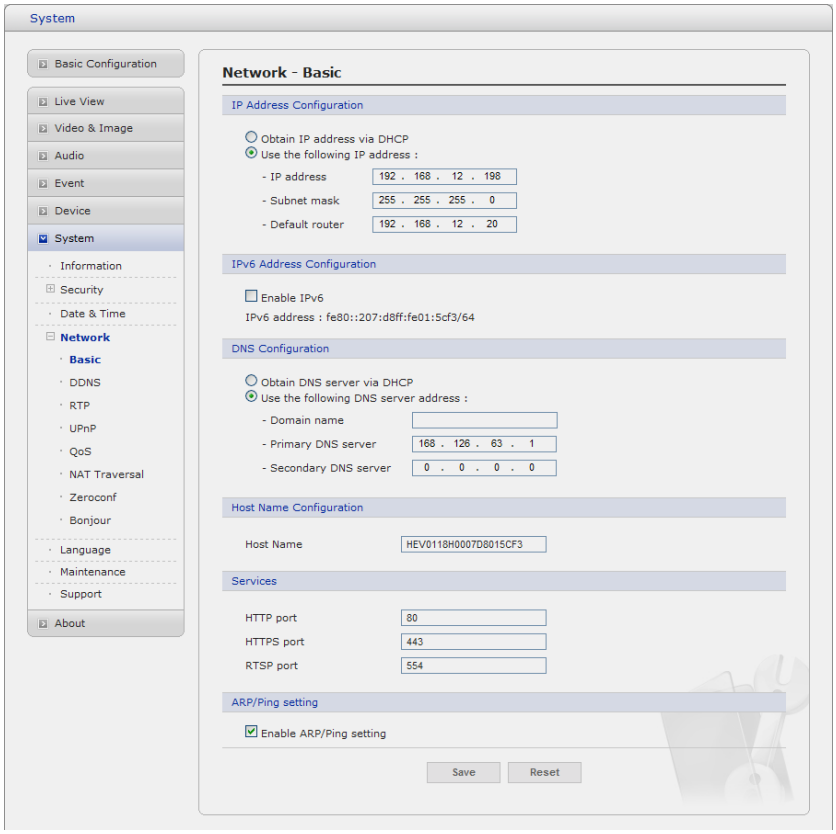
Select your time zone from the drop-down list. If you want the server clock to automatically adjust for daylight savings time, activate "Automatically adjustment for daylight saving time changes".

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 video encoder will obtain the time from an NTP server every 60 minutes.
-. Set manually - this option allows you to manually set the time and date.

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

3.5.7.3 Network



Setting in regard to 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.
-. Use the following IP address - To use a static IP address for the Network Transmitter, check the radio button and then make the following settings:
* IP address - Specify a unique IP address for your Network Transmitter.
* Subnet mask - Specify the mask for the subnet the Network Transmitter 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.

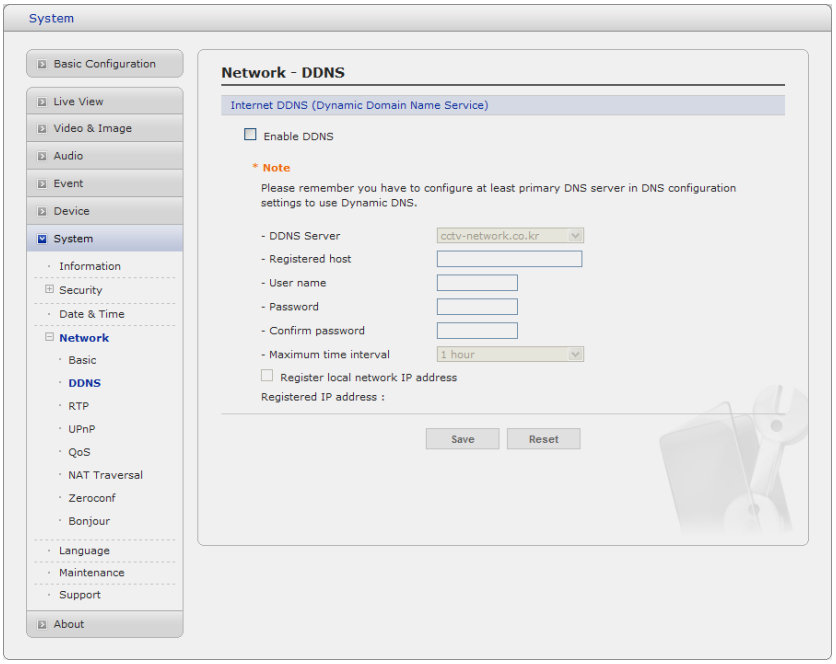
• IPv6 Address Configuration
Check this box to enable IPv6. Other settings for IPv6 are configured in the network router.

• DNS Configuration
DNS (Domain Name Service) provides the translation of host names to IP addresses on your network.
-. Obtain DNS Server via DHCP - Automatically use the DNS server settings provided by the DHCP server. Click the View button to see the current settings.
-. 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 Transmitter. 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.

• 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 of IP address - 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.

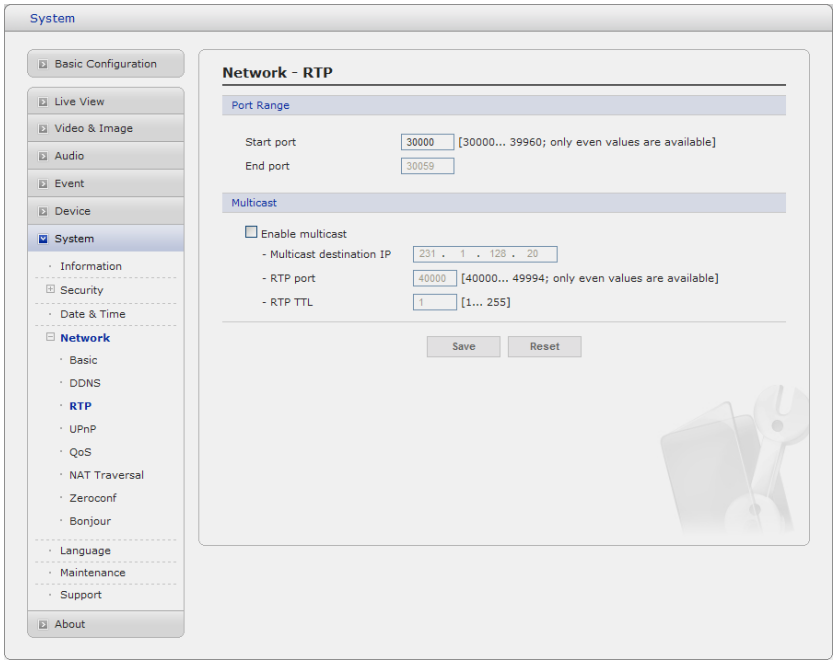
▼ DDNS



• Internet DDNS(Dynamic Domain Name Service)
When using the high-speed Internet with the telephone or cable network, users can operate the Network Transmitter even 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/, or http://www.security-device.name/.

-. Enable DDNS - Check to get DDNS service to be 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 a password again to confirm it.
* Maximum time interval: Set a time interval to synchronize with the DDNS server. Select an item in the interval drop-down list.
* Register local network IP address: Register a Network Video Server IP address to the DDNS server

▼ RTP



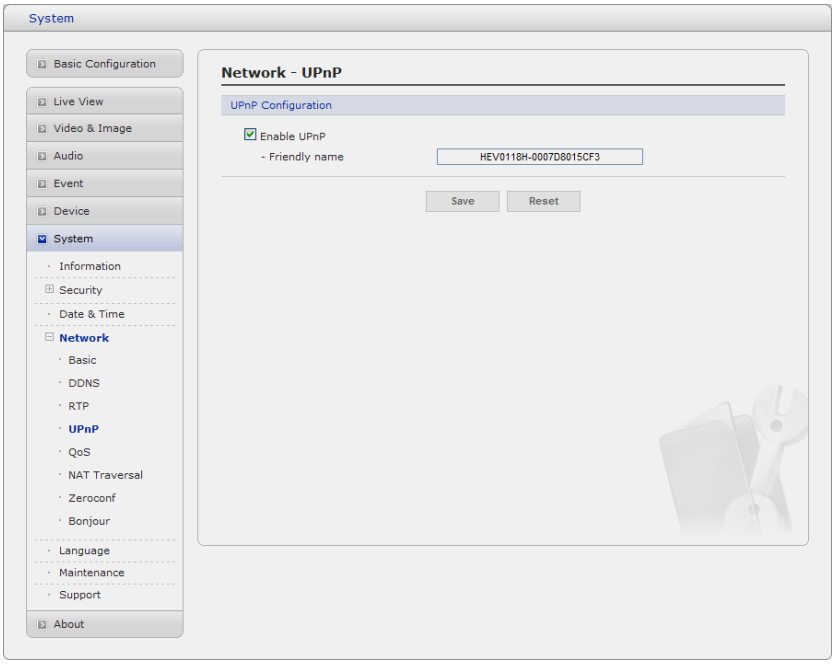
Have a setting for sending and receiving an audio or video on a real-time basis. These settings are the IP address, port number, and Time-To-Live value to use for the media stream(s) in multicast H.264 format. Only certain IP addresses and port numbers should be used for multicast streams. For more information,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

• Port Range
-. Start port - Enter a value between 1024 and 65532

• Multicast
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. Although it is empty, an IP will be entered automatically.
-. 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. On the other hand, if a network status is poor, enter a higher value. When there are many Network Transmitters or users, a higher value may cause a heavy load to the network. For a detailed setting, please consult with a network manager.

▼ UPnP



The Network Transmitter includes support for UPnP™. UPnP™ is enabled by default, and the Network Transmitter then is automatically detected by operating systems and clients that support this protocol.

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.

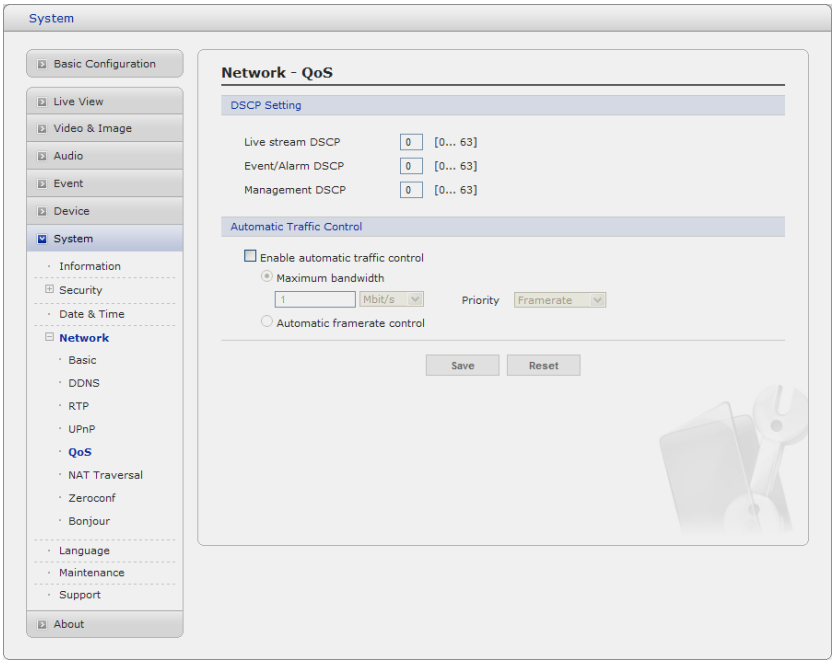
▼ QoS

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, thanks 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:

-. Live Stream DSCP:

-. Event/Alarm DSCP:

-. Management DSCP:

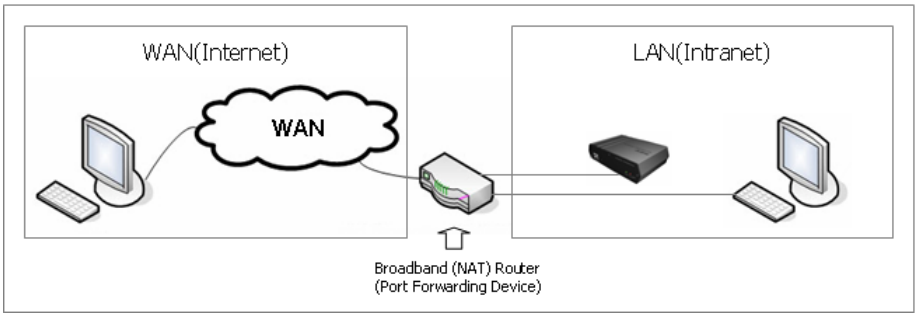
• Automatic Traffic Control
Set a limitation on user network resources by designating the maximum bandwidth.

-. Maximum bandwidth - In case of 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 framerate control - Selected if not influenced by a network-related program or equipment without a limitation on the network bandwidth.

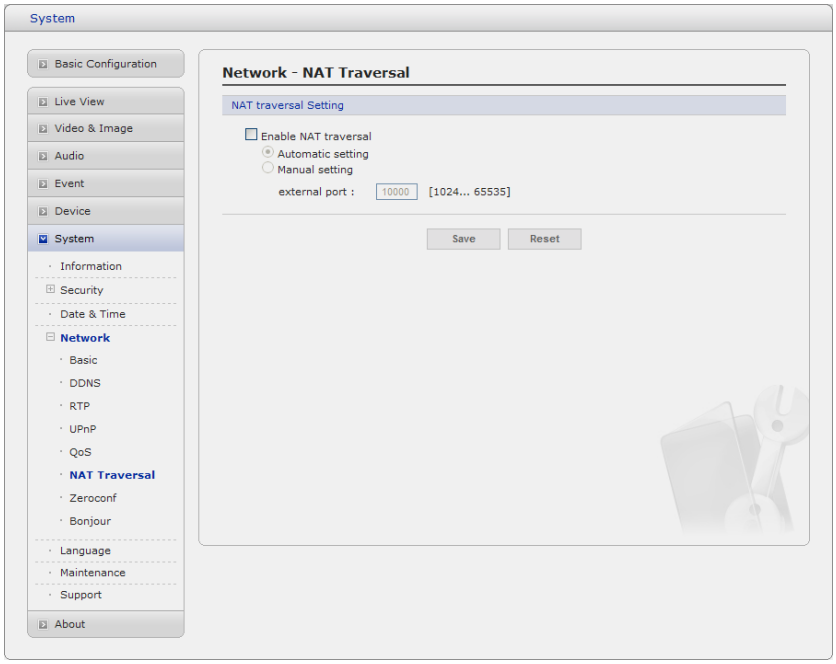
▼ NAT Traversal

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 traversal** when your network transmitters 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 transmitter.



Notes:
-. For NAT traversal 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 traversal Settings

-. Enable - when enabled, the network transmitters attempt to configure port mapping in a NAT router on your network, using UPnP™. Note that UPnP™ must be enabled in the Network Transmitter (see System>Network>UPnP).

* automatic setting: The Network Transmitter automatically search 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.

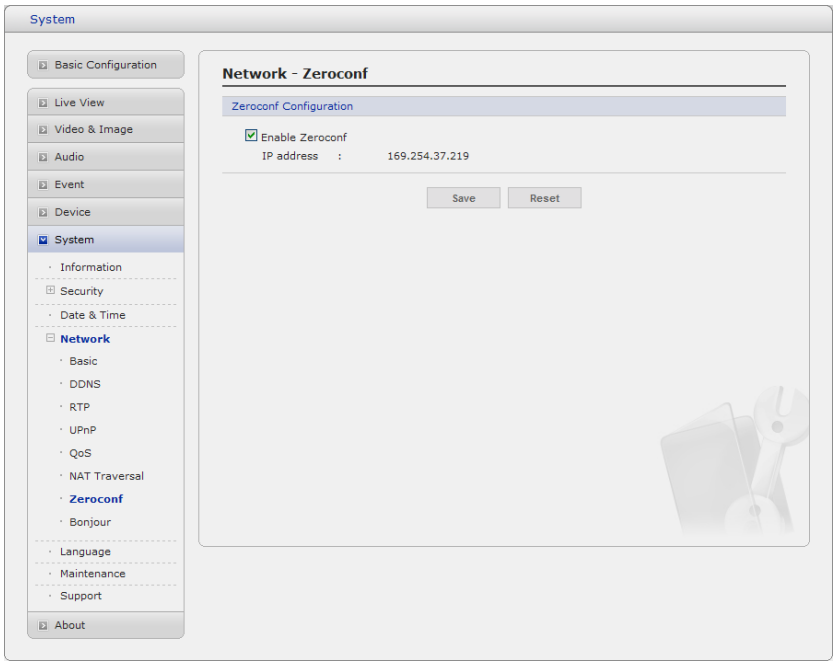
Notes:

-. 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.

▼ Zeroconfig

Zeroconfig allows the network transmitter to create and assign IP address for network transmitter 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.

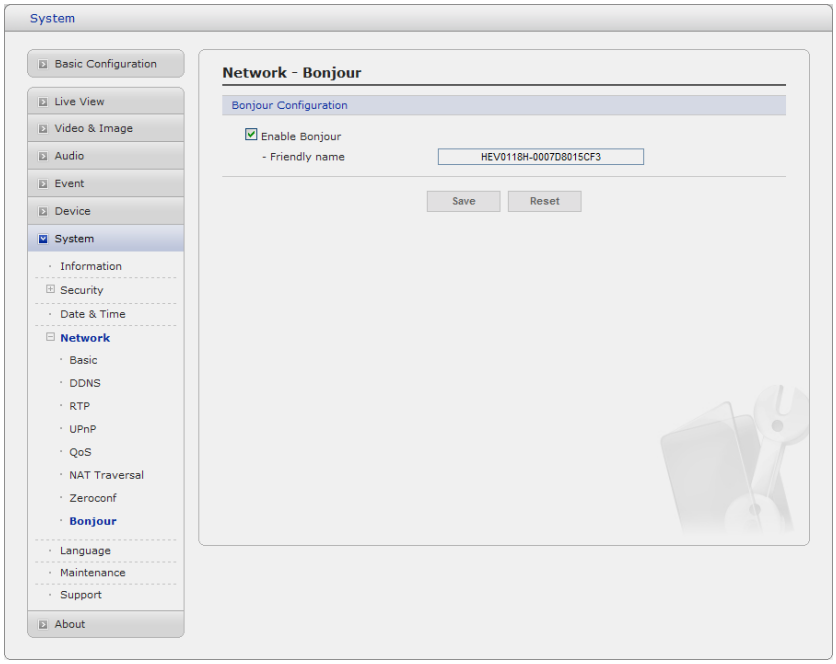
Zero configuration networking allows devices such as computers and printers to connect to a network automatically. Without zeroconf, a network administrator must set up services, such as Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS), or configure each computer's network settings 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.

▼ Bonjour

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

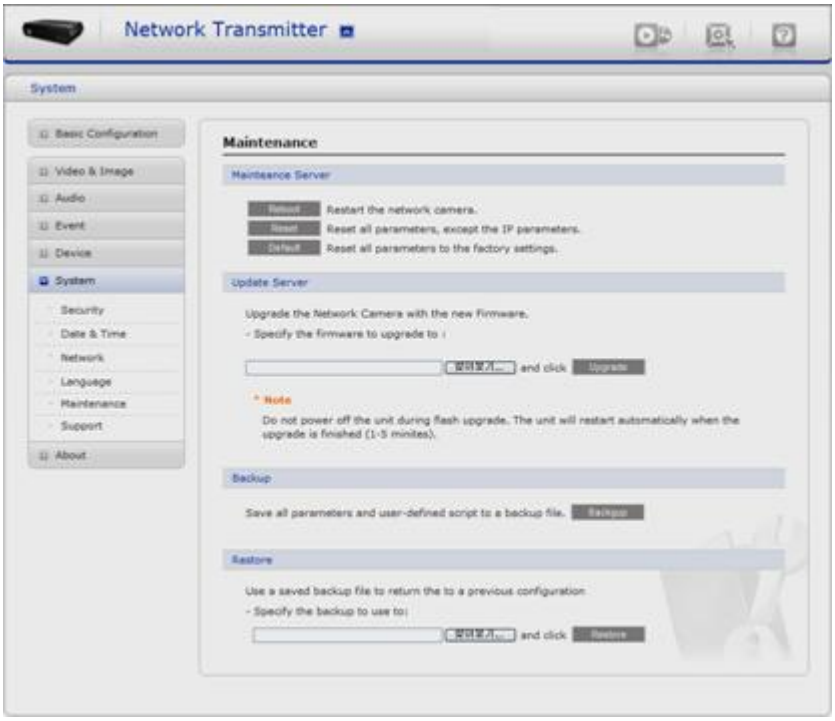


Note: Bonjour - Also known as zero-configuration networking, Bonjour enables devices to automatically discover each other on a network, without having to enter IP addresses or configure DNS servers. Bonjour is a trademark of Apple Computer, Inc

3.5.7.4 Language

It will be able to select a user language. The type of language it will be able to select is the English, the French, the German, the Spanish and the Italian.

3.5.7.5. Maintenance



• Maintenance Server
 -. Restart - The unit is restarted without changing any of the settings. Use this method if the unit is not behaving as expected.
 -. Restore - 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 Transmitter's settings to the factory default values (including the IP address)

• Update Server
 Carry out the upgrade by importing an upgrade file and pressing the Upgrade button. During the upgrade, do not turn off the power of the Network Transmitter. And try an access again after waiting five minutes or longer.

• Backup
 Save a setting value that users enter to the Network Transmitter, to a user PC.

• Restore
 Import and apply a setting value saved to a user PC.

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

3.5.7.6 Support

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

• Logs
The network Transmitter support system log information. Click the System Log button to get the log data.

• Update Server
-. Server Report – Click the Server Report button to get the important information about the server's status and should always be included when requesting support.

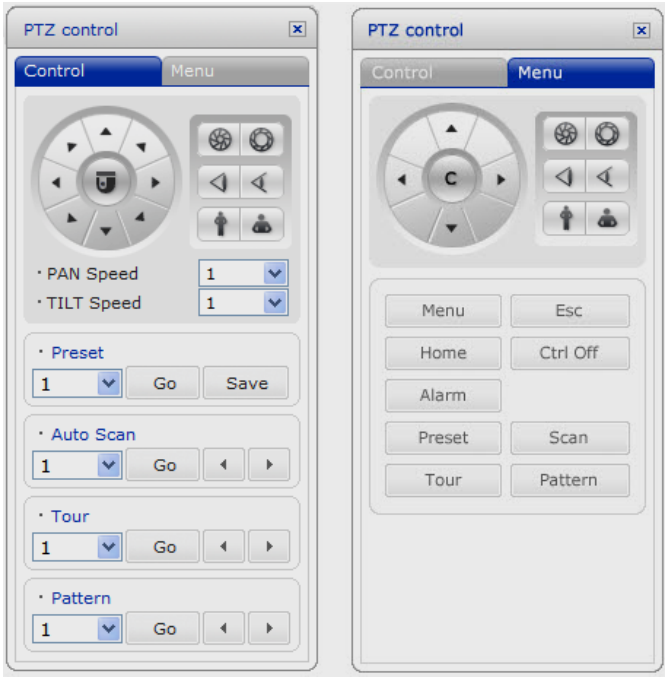
-. Parameter List – Click the Parameter List button to see the unit's parameters and their current settings.

3.5.8 About

The following website will provide the support information for the Network Transmitter information and operation.

3.6 PTZ Control

You can control PTZ camera in the live screen. Press the button on the left top in the live screen to activate the PTZ control panel.



PTZ Control Panel PTZ Menu Panel

Direction Buttons

Iris/Focus/Zoom Buttons

• Control Panel

-. Left/Right button: Go into the sub-menu items. Execute the command (exit). Change value. Navigate through the menu items.

-. Up/Down button: Navigate through the menu items

-. PAN/TILT Speed: It sets a speed when adjusting the PTZ Camera. The higher a value is, the faster a speed will be.

-. Focus: Overrides auto focus. Moving the Zoom handle reactivates Auto Focus mode.

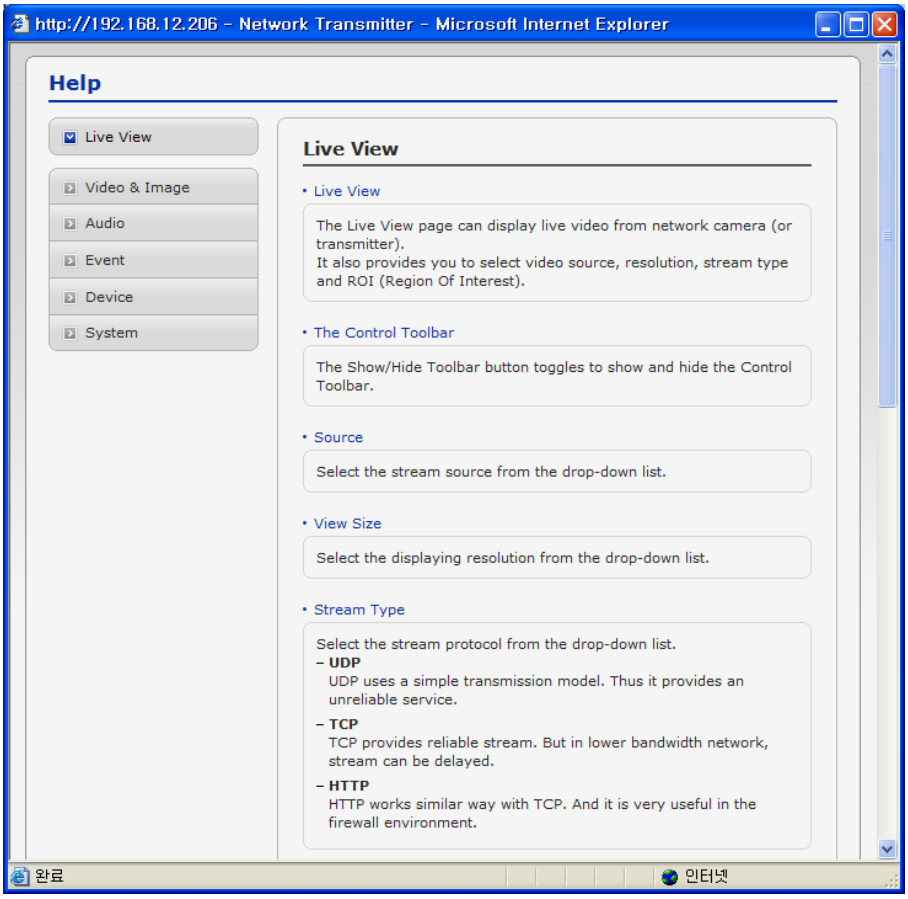
-. Iris: Overrides auto iris. Moving the joystick reactivates Auto Iris mode.

-. Zoom: Zoom control.

• Manu Panel
-. Menu: Enters programming menu.
-. Esc: Cancels current inputs. Exits from currently running functions or menu, error status, etc
-. Home: Immediately calls Home function. Deletes selected value or function in programming mode
-. Ctrl Off: Control function.
ex) CTRL + Up, Down, Right, Left Button >> Operated turbo mode.
-. Preset: Pressing the Preset will bring up the preset programming menu.
-. Auto Scan: Pressing the Scan will bring up the Auto Scan programming menu.
-. Tour: Pressing the Tour button will bring up the tour programming menu directly.
-. Pattern: Pressing the Pattern button will bring up the pattern programming menu directly.

3.7 Help

The Help information window will be provided as a popup window so that users can open and read it without a need for log-in. It will offer a description on setting and Help page by which users can manipulate the Network Transmitter without a reference to the manual.



3.8 Resetting to the factory default settings

To reset the Network Transmitter to the original factory settings, go to the Setup>System >Maintenance web page (described in Maintenance, on page 54) or use the control button on the network video transmitter, as described below:

• Using the Reset Button

Follow the instructions below to reset the Network Transmitter to the factory default settings using the Reset Button.

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

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

4. Appendix

4.1 Troubleshooting

Troubleshooting if problems occur, verify the installation of the Network Transmitter 1CH 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	Area to Check
No video	Verify that power is connected to all pieces of equipment in the system. Verify that the power switches are in the ON position. Check the video connections.
Poor video quality.	Check that the BNC connectors are inserted properly. Check the voltage level of the Network Transmitter 1CH. Cable for video is shielded.
Camera number does not match the number on PC Program or Web browser.	Check the camera ID of the 1CH Network Transmitter. Check PTZ setting on the PC Program and Web browser.
Frame rate decrease.	Change current value more lower resolution, compression rate and frame rate.
A connection is cut-off at short intervals.	Check network traffic and contact with network administrator.

4.2 Preventive Maintenance

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

Every three-month, perform the following maintenance.

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

4.3 Product Specification

Main Item	Sub Item	Specification
VIDEO	Video In/Out	1BNC/1BNC, 1.0Vp-p[75ohm, composite]
	Compression	Motion JPEG MPEG-4 Part2 H.264 (MPEG-4 Part 10) Profiles: H.264 MP and BP, MPEG-4 ASP and SP
	Resolutions	4CIF, 2CIF, CIF, QCIF, VGA, QVGA, QQVGA Max. 704x480/704x576[NTSC/PAL] Min. 160x120,
	Frame Rate, H.264	Up to 30/25fps[NTSC/PAL] @ all resolutions
	Frame Rate, MPEG-4	Up to 30/25fps[NTSC/PAL] @ all resolutions
	Frame Rate, MJPEG	Up to 30/25fps[NTSC/PAL] @ all resolutions
	Video Streaming	Simultaneously H.264(or MPEG-4) and MJPEG Controllable Frame Rate and Bandwidth VBR/CBR H.264 and MPEG-4
AUDIO	Audio In/Out	1/1 Phone Jack
	Audio Streaming	2 Way
	Compression	G.711 ADPCM 40kbps~16kbps
NETWORK	Security	Multi-user authority, HTTPS, IP Filtering, Privacy Zone
	Supported Protocol	TCP/IP, UDP, IPv4/v6, HTTP, HTTPS, QoS, FTP, SNMP, uPnP, RTP, RTSP, RTCP, DHCP, ARP, Zeroconf, Bonjour
	Installation Tool	SmartManager, NCTitanium
	Upgrade	Web browser, SmartManager, NCTitanium
SYSTEM REQUIREMENT	API Programming Interface	API Supported, Open Platform Compatible: ONVIF
	Alarm Triggers	Motion Detection, External Input, Video Loss
	Alarm Events	File upload via FTP and HTTP Notification via E-mail, HTTP and TCP External Output activation Audio alert activation
	Video Buffering	Pre and Post Alarm
FEATURE	Motion Detection	Yes, Max 8 window
	Privacy Mask	Yes, Max 8 window
	Network Time Synchronization	Yes
	Software Reset	Yes
	Factory Reset	Yes
	Auto Recovery	Yes
IN/OUT	Alarm In/Out	1 TTL / 1 Relay Output
	Auxiliary	1 x RS485
	Ethernet	RJ-45 10BASE-T/100BASE-TX PoE
	LED Indicator	Power, Network
	Buttons	Factory Reset

GENERAL	Casing	Metal Casing, Standalone or with Bracket for wall mount
	Operating Temperature	0°C ~ 50°C
	Operation Humidity	0~90% (non-condensing)
	Power Consumption	AC24/DC12V max. 5watt, Power over Ethernet IEEE 802.3af Class2/3
	Dimensions (W x H x D)	6.1" / 155mm X 1.57"/40mm X 4.03"/102.4mm
	Unit Weight	455g
	Approval	FCC, CE, MIC

System Requirement for Web Browser

- Operating System: Microsoft Windows 98, Microsoft Windows ME, Microsoft Windows 2000, Microsoft Windows XP, or Microsoft Windows Vista
- CPU: Over Pentium IV 2.4Ghz, 512MB RAM, 10GB free disk or higher
- VGA: AGP, Video RAM 32MB or higher (1024x768, 24bpp or higher)

NETWORK TRANSMITTER

PLEASE RECYCLE

Printed in Korea