SIQURA

User’s manual

SA-BL37

2MP Corrosion proof compact bullet, 3.7 mm

Note: To ensure proper operation, please read this manual thoroughly before using the product and retain the information for future reference.

SA-BL37
Installation Manual v1.0

Brand names

Any brand names mentioned in this manual are registered trademarks of their respective owners.

Liability

Siqura accepts no liability for claims from third parties arising from improper use other than that stated in this manual. Although considerable care has been taken to ensure a correct and suitably comprehensive description of all relevant product components, this manual may nonetheless contain errors and inaccuracies. We invite you to offer your suggestions and comments by email. Your feedback will help us to further improve our documentation.

How to contact us

If you have any comments or queries concerning any aspect related to the product, do not hesitate to contact:
Siqura
Meridiaan 32
2801 DA Gouda The Netherlands
General : +31 182 592 333
Fax : +31 182 592 123
E-mail : sales.nl@siqura.com
WWW : siqura.com

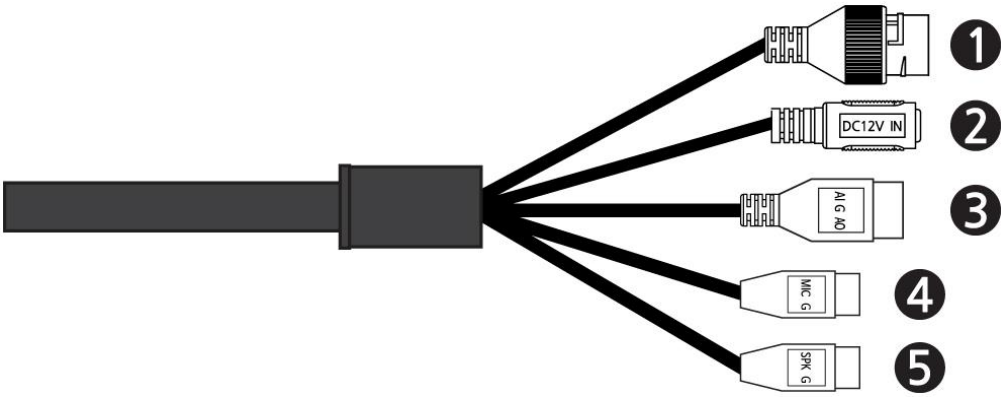
Contents

1. SA-BL37 - User's Manual

Preserve this manual as a reference for future needs.

	Used electrical, electronic, battery-powered, and stainless steel products should not be mixed with general waste. For proper treatment, recovery and recycling of old products, take them to applicable collection points, in accordance with your national legislation and the Directives 2002/95/EC and 2002/96/EC. By disposing of these products correctly, you help to save valuable resources and prevent any potential negative effects on human health and the environment which could otherwise arise from inappropriate waste handling. For more information about collection and recycling of old products, contact your local municipality or your waste disposal service. Penalties may be applicable for incorrect disposal of this waste, in accordance with national legislation.

1.1. Basic Configuration of Camera System



No.	Connector	Description
1	RJ-45	Ethernet, RJ-45 port compatible with 10/100Mbps having PoE functionality
2	DC-Jack	12 VDC
3	3-pin terminal block	AI: Alarm in
		G: Ground
		AO: Alarm out
4	2-pin terminal	MIC: AUDIO input (line level)
		G: Ground
5	2-pin terminal	SPK: AUDIO output
		G: Ground

The camera must be installed by qualified service personnel in accordance with all local and federal electrical and building codes.

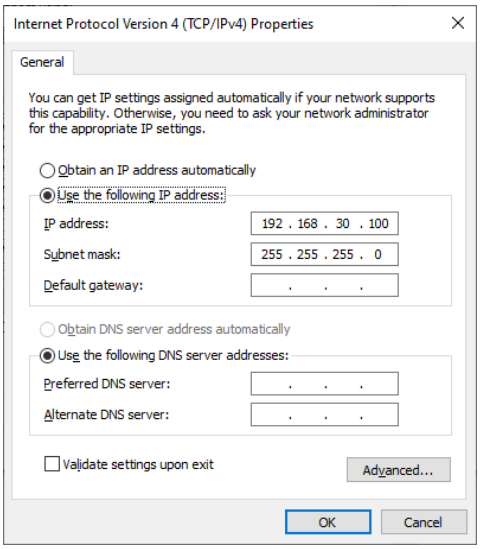
1.2. Connections

- **Network**
  Connect a standard RJ-45 cable to the network port of the camera..
- **Audio**
  Connect speaker to audio output line and external mic to audio input line.
- **Alarms**
  - AI (Alarm Input)
    You can use external devices to signal the camera to react on events. Mechanical or electrical switches can be wired to the AI and G (Ground) connectors.
  - G (Ground)
    NOTE: All the connectors marked G or GND are common.
    Connect the ground side of the alarm input and/or alarm output to the G (Ground) connector.
  - AO (Alarm Output)
    The camera can activate external devices such as buzzers or lights. Connect the device to the AO (Alarm Output) and G (Ground) connectors.
- **Power**
  Connect power of 12VDC for the camera.
  When using a 12VDC adapter, connect the positive (+) pole to the '+' position and the negative (-) pole to the '-' position.
  Use satisfy clause 2.5 of IEC60950-1/UL60950-1 or Certified/Listed Class 2 power source only.
  - Be careful not to reverse the polarity when you connect the power cable.
  - You can also use a router featuring PoE (Power over Ethernet) to supply power to the camera.
  - If using PoE and 12 Vdc, PoE will be used to power the camera

1.3. Network Connection & IP Assignment

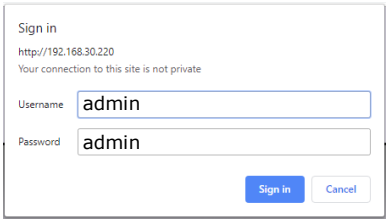
The camera supports the operation through the network. When a camera is first connected to the network, it is necessary to allocate an IP address to the device. To find and change the IP-address you can use the Siqura Device Manager 2 (SDM2) on https://siqura.com/downloads/software/

To be able to find the camera, make sure your computers network card is set to the proper network settings:



The default IP address of the camera is **192.168.30.220**. By typing this address in your browser, you also get access to the web interface of the camera. The recommended browsers are Internet Explorer, Safari, Firefox, Opera and Google Chrome, but to have full access Internet Explorer is recommended.

The default username and password are:

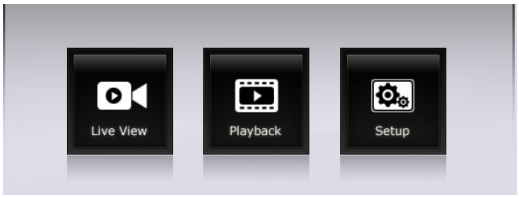


NOTE: Please, change the default password as soon as possible with a strong password (more than 6 characters, containing capitals, lower case, numbers and special characters)

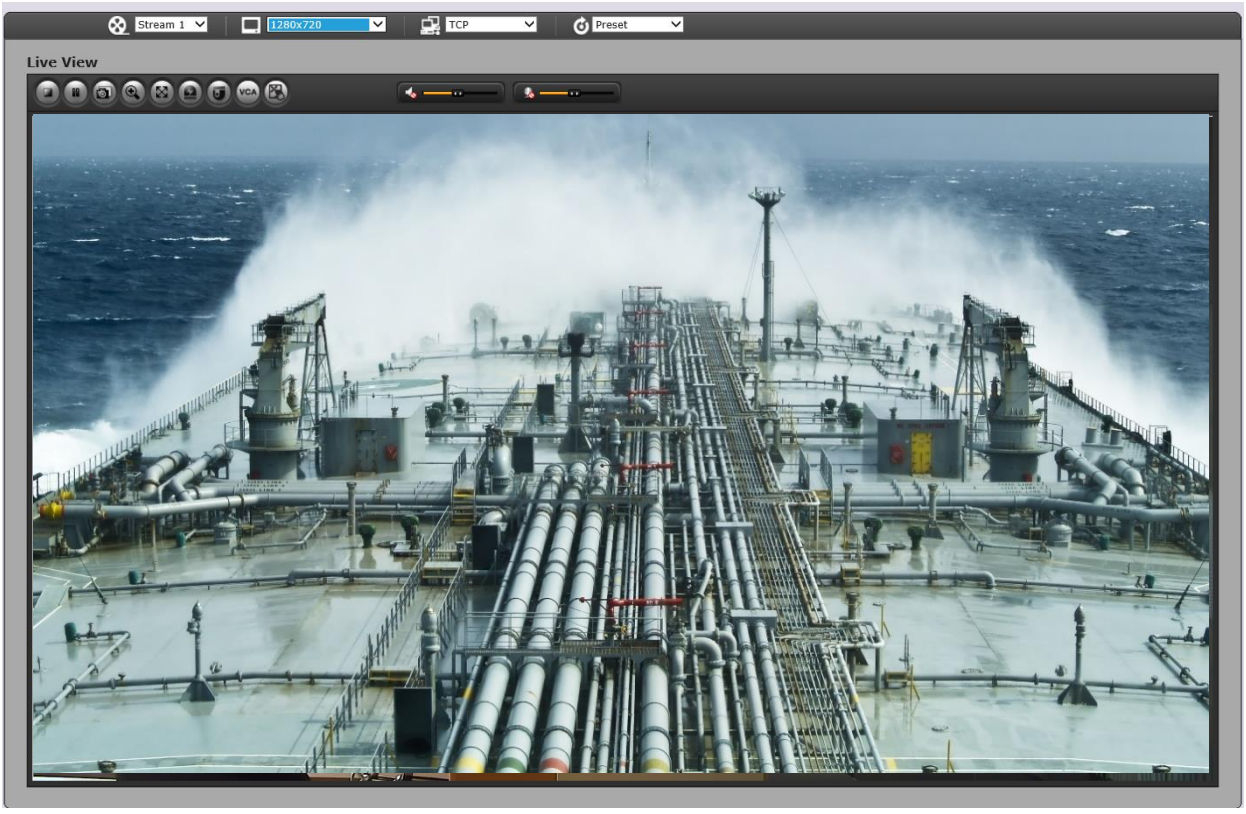
1.4. Operation

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.

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



4. The network cameras Live View page appears in your browser.



1.5. 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, please see “System > Network > NAT” of User’s Manual.

1.6. Setting the admin password over a secure connection

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

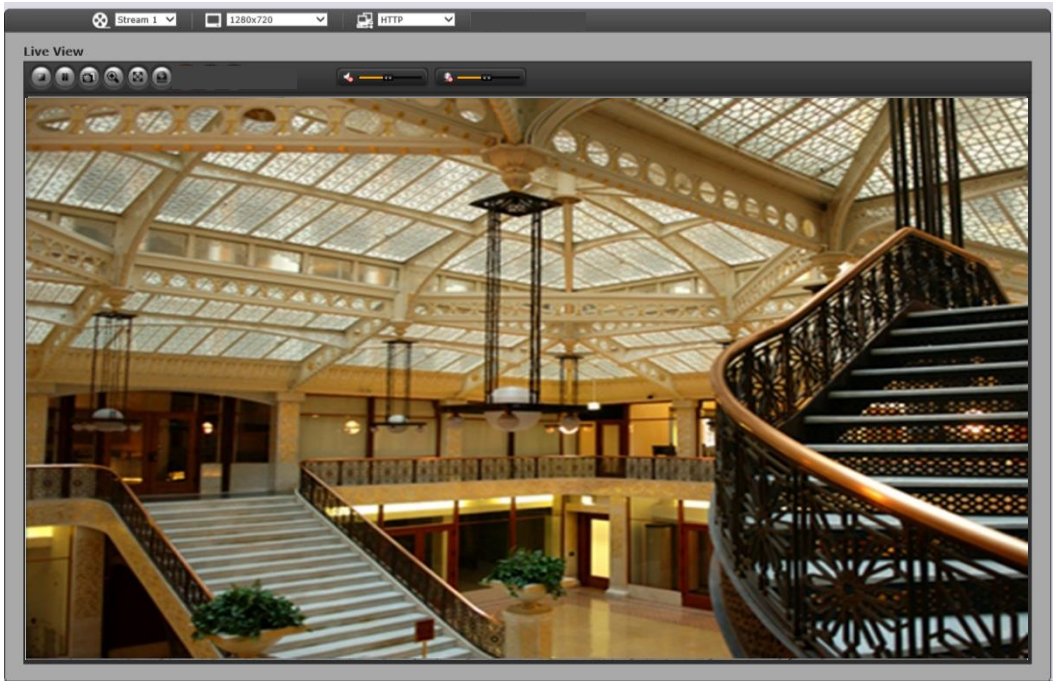
NOTE: The default administrator user name and password is admin. If the password is lost, the network camera must be reset to the factory default settings. Please see “Resetting to the factory default settings”.

To prevent network eavesdropping when setting the admin password, this can be done via an encrypted HTTPS connection, which requires an HTTPS certificate (see NOTE below). To set the password via a standard HTTP connection, enter it directly in the first dialog shown below. To set the password via an encrypted HTTPS connection, please see “System > Security > HTTPS” of User’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.

1.7. Live View Page

The Live View page comes in several screen modes. Users are allowed to select the most suitable one out of those modes. Adjust the mode in accordance with your PC specifications and monitoring purposes.



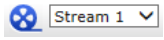
1.7.1. General controls


Live View Page

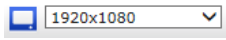

Playback Page


Setup Page


Help Page



The video drop-down list allows you to select a customized or preprogramed video stream on the Live View page. stream profiles are configured under Setup > Basic Configuration > Video & Image. For more information, please see “Basic Configuration > Video & Image” of User’s Manual.



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

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

1.7.2. Control toolbar

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


The **Stop** button stops the video stream being played. Pressing the key again toggles the play and stop.


The **Play** button connects to the network camera or starts playing a video stream.


The **Pause** button pauses the video stream being played.


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


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


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


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


The **Face Detector** button shows/hides detected faces.


The **Speaker** button activates/deactivates external speaker.


The **Mic** button activates/deactivates microphone input.


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

1.7.3. Video Streams

The network camera provides several images and video stream formats. Your requirements and the properties of your network will determine the type you use.
The Live View page in the network camera provides access to H.265, H.264 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.

1.8. Playback

Playback and SD -card are not supported.

2. Network Camera Setup

This section describes how to configure the network camera.

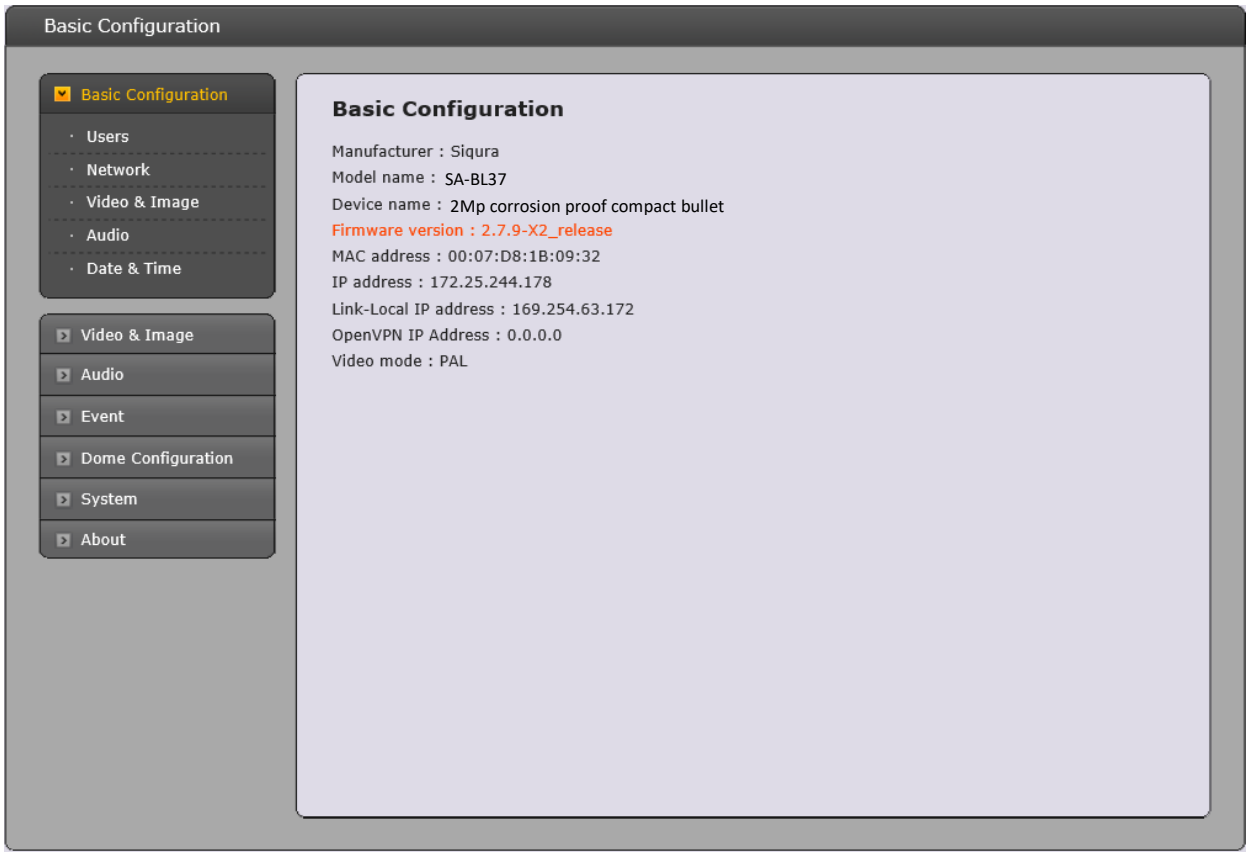
Administrator has unrestricted access to all the Setup tools, whereas Operators have access to the settings of Basic Configuration, which are Live View, Video & Image, Audio, Event, Dome Configuration, and System.

You can configure the network camera by clicking Setup either in the first connection page or the top second-right button of the Live View page. Accessing the network camera from a computer for the first time opens the Admin Password dialog box. Enter your administrator or operator id and password to get into setup page.

NOTE: If the password is lost, the network camera must be reset to the factory default settings. Please see "Resetting to the factory default setting".

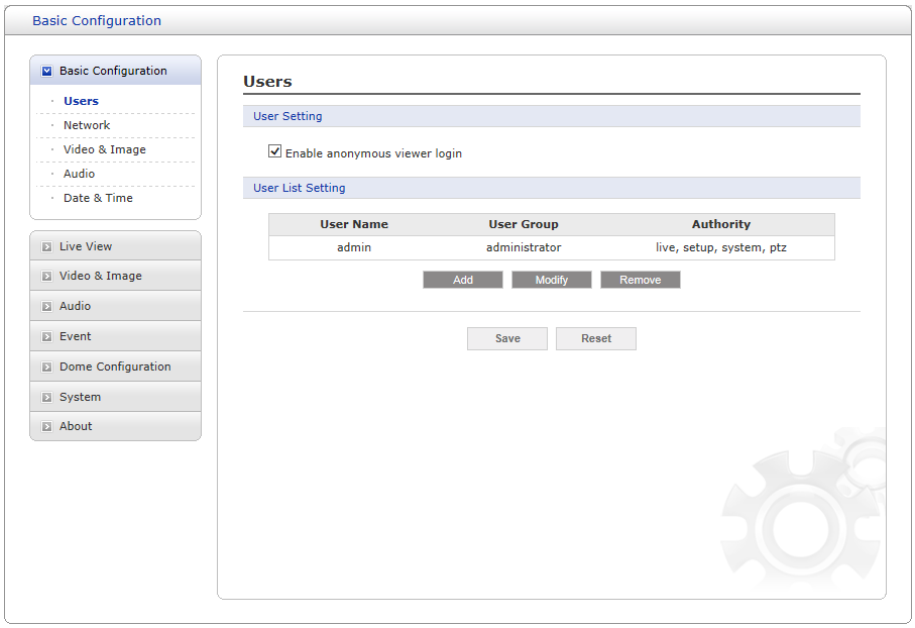
2.1. Basic Configuration

You can see the device information in this information page.



2.1.1. Users

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



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

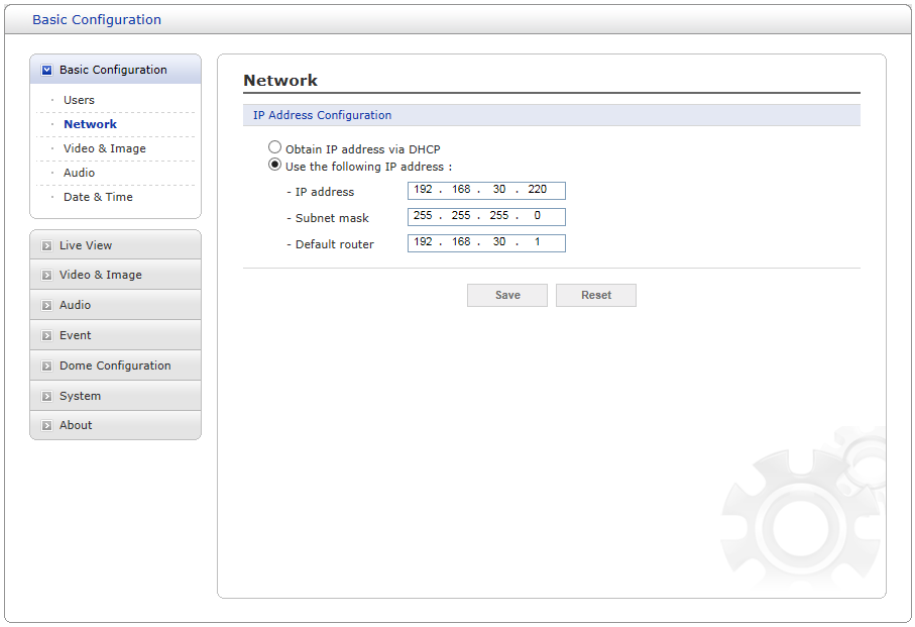
User Group	Authority
Guest	Provides the lowest level of access, which only allows access to the Live View page.
Operator	An operator can view the Live View page, create and modify events, and adjust certain other settings. Operators have no access to System Options.
Administrator	An administrator has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

- **Enable anonymous viewer login:** Check the box to use the webcasting features. Refer to “Video & Image > Webcasting” for more details.

Please refer to “System > Security > Users” for more details about User setup.

2.1.2. 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 an option of using the Internet Dynamic DNS Service. For more information on setting the network, please see “System > Network > Basic”.



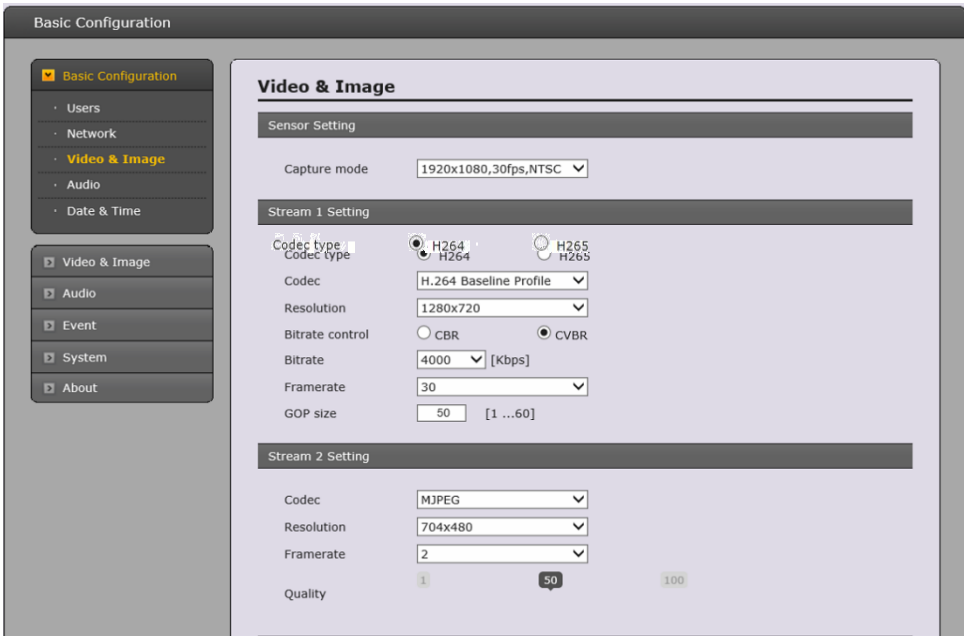
Obtain IP address via DHCP: Dynamic Host Configuration Protocol (DHCP) is a protocol that lets network administrators centrally manage and automate the assignment of IP addresses on a network. DHCP is enabled by default. Although a DHCP server is mostly used to set an IP address dynamically, it is also possible to use it to set a static, known IP address for a particular MAC address.

Use the following IP address: To use a static IP address for the network camera, check the radio button and then make the following settings:

- **IP address:** Specify a unique IP address for your network camera.
- **Subnet mask:** Specify the mask for the subnet the network camera is located on.
- **Default router:** Specify the IP address of the default router (gateway) used for connecting devices attached to different networks and network segments.

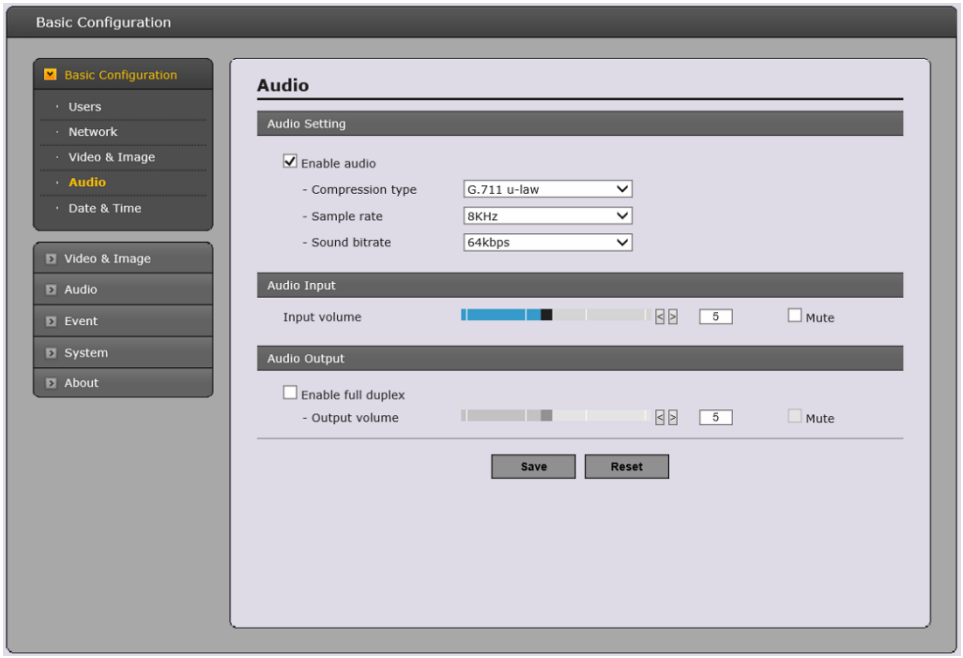
NOTES: DHCP should only be enabled if using dynamic IP address notification, or if your DHCP server can update a DNS server, which then allows you to access the network camera by name (host name). If DHCP is enabled and you cannot access the unit, you may have to reset it to the factory default settings and then perform the installation again.
The ARP/Ping service is automatically disabled two minutes after the unit is started, or as soon as an IP address is set. Pinging the unit is still possible when this service is disabled. Please refer to “System > Network > Basic” for more details about Network setup.

2.1.3. Video & Image



User can setup and change setting of individual video stream in this page.
Please refer to “Video & Image > Basic” for more details about Video & Image setup.

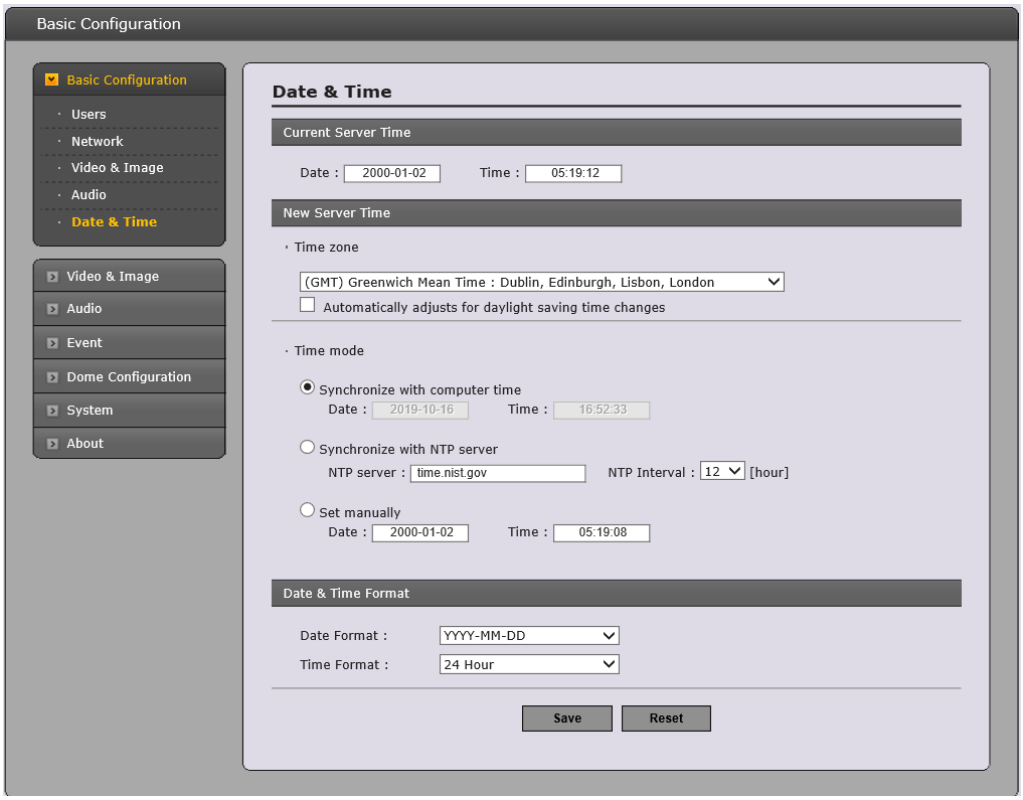
2.1.4. Audio



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

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

2.1.5. Date & Time

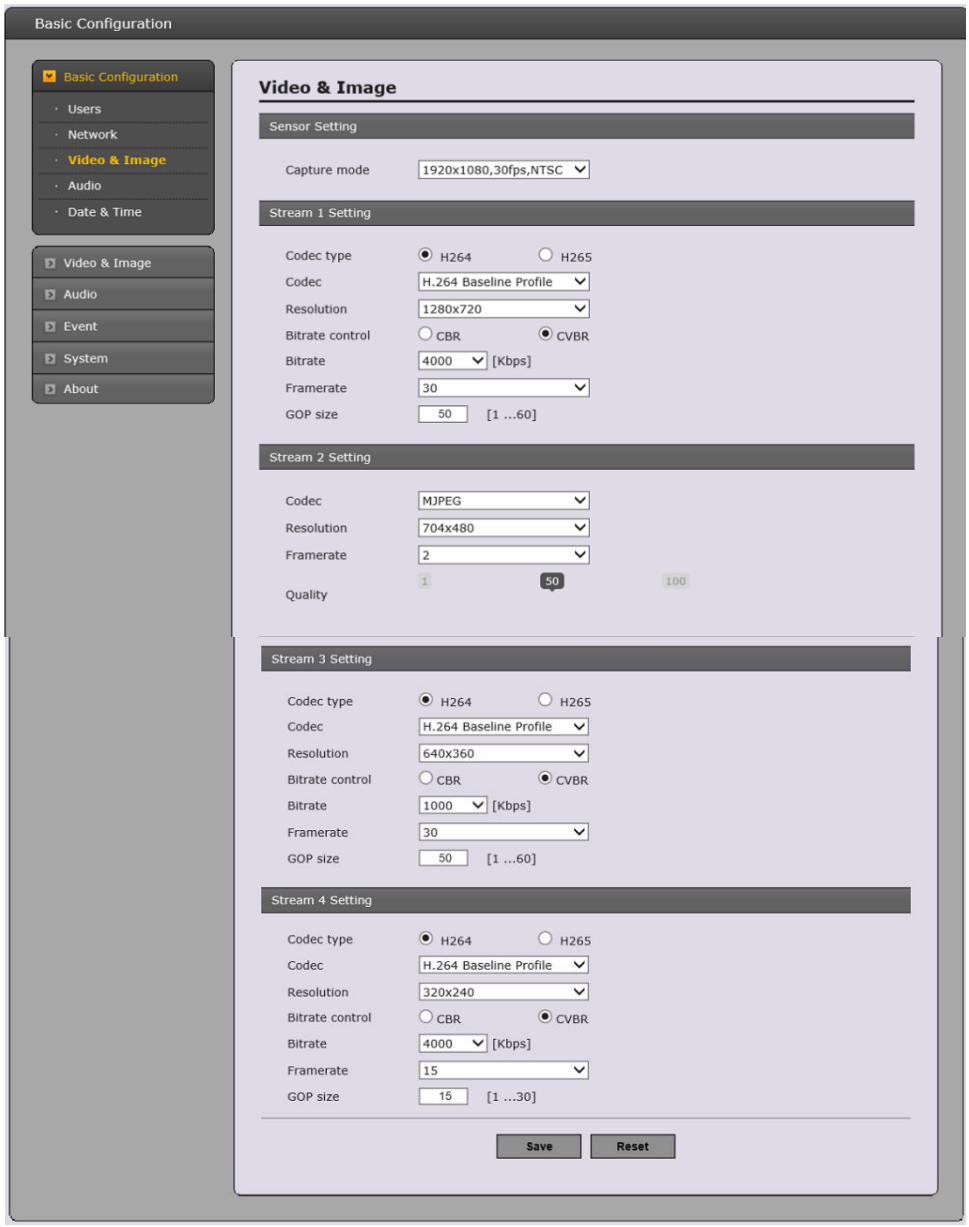


User can set time directly or assign time server to get the current time, as well as determine Date & Time format in this page.

Please refer to “System > Date & Time” for more details about Date & Time setup.

2.2. Video & Image

2.2.1. Basic



Sensor Setting:

- Capture mode: User can select sensor capture mode between 30 fps and 60 fps in full-HD resolution. If 60fps is selected, Stream 3 is disabled and hidden from the window. In other words, the camera provides triple stream at 30 fps and dual stream at 60 fps.
- Stream 1 Setting:
  Codec: The codec supported in Stream 1 is H.264 and H.265. There are 3 pre-programmed stream profiles available for quick set-up. Choose the form of video encoding you wish to use from the drop-down list:
  - H.264 HP (High Profile): Primary profile for broadcast and disc storage applications, particularly for high-definition television applications (for example, this is the profile adopted by the Blu-ray Disc storage format and the DVB HDTV broadcast service).
  - H.264/H265 MP (Main Profile): Primary profile for low-cost applications that require additional error robustness, this profile is used rarely in videoconferencing and mobile applications; it does add additional error resilience tools to the Constrained Baseline Profile. The importance of this profile is fading after the Constrained Baseline Profile has been defined.
  - H.264 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: This enables users to determine a basic screen size when having an access through the Web Browser or PC program. The screen size control comes in seven modes like 1920x1080, 1280x1024, 1280x960, 1280x720, 1024x768, 704x576, 704x480, 640x480, 640x360 and 320x240. Users can change the selected screen size anytime while monitoring the screen on a real-time basis.
- Bitrate control: The bit rate can be set as Variable Bit Rate (VBR) or Constrained Variable Bit Rate (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 the real-time play, users should select a frame refresh rate per second. If the rate is high, the image will become smooth. On the other hand, if the rate is low, the image will not be natural but it can reduce a network load.
- GOP size: Select the GOP (Group of Picture) size. If users want to have a high quality of fast image one by one, please decrease the value. For the purpose of general monitoring, please do not change a basic value. Such act may cause a problem to the system performance. For the details of GOP setting, please contact the service center.

Stream 2 Setting:

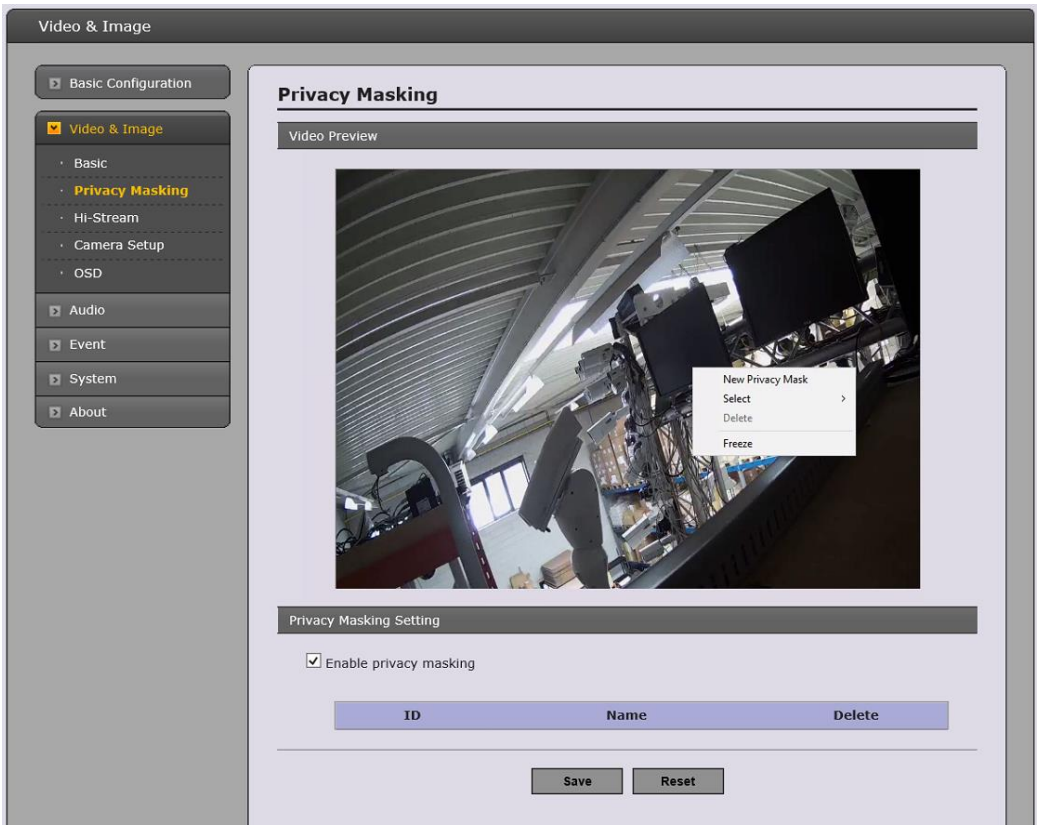
- Sometimes the image size is large due to low light or complex scenery. Adjusting the frame rate and quality helps to control the bandwidth and storage used by the Motion JPEG video stream in these situations. Limiting the frame rate and quality optimizes bandwidth and storage usage, but may give poor image quality. To prevent increased bandwidth and storage usage, the Resolution, Frame rate, and Frame Quality should be set to an optimal value.
  - MJPEG Resolution: Same as the stream 1 settings.
  - MJPEG Frame rate: Same as the stream 1 settings.
  - MJPEG Quality**:** Select the picture quality. If users want to have a high quality of fast image one by one, please decrease the value. For the purpose of general monitoring, please do not change a basic value. Such act may cause a problem to the system performance.

Stream 3 and Stream 4 Setting:

- Same as the Stream 1 Setting.

Important: 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.

2.2.2. Privacy Masking

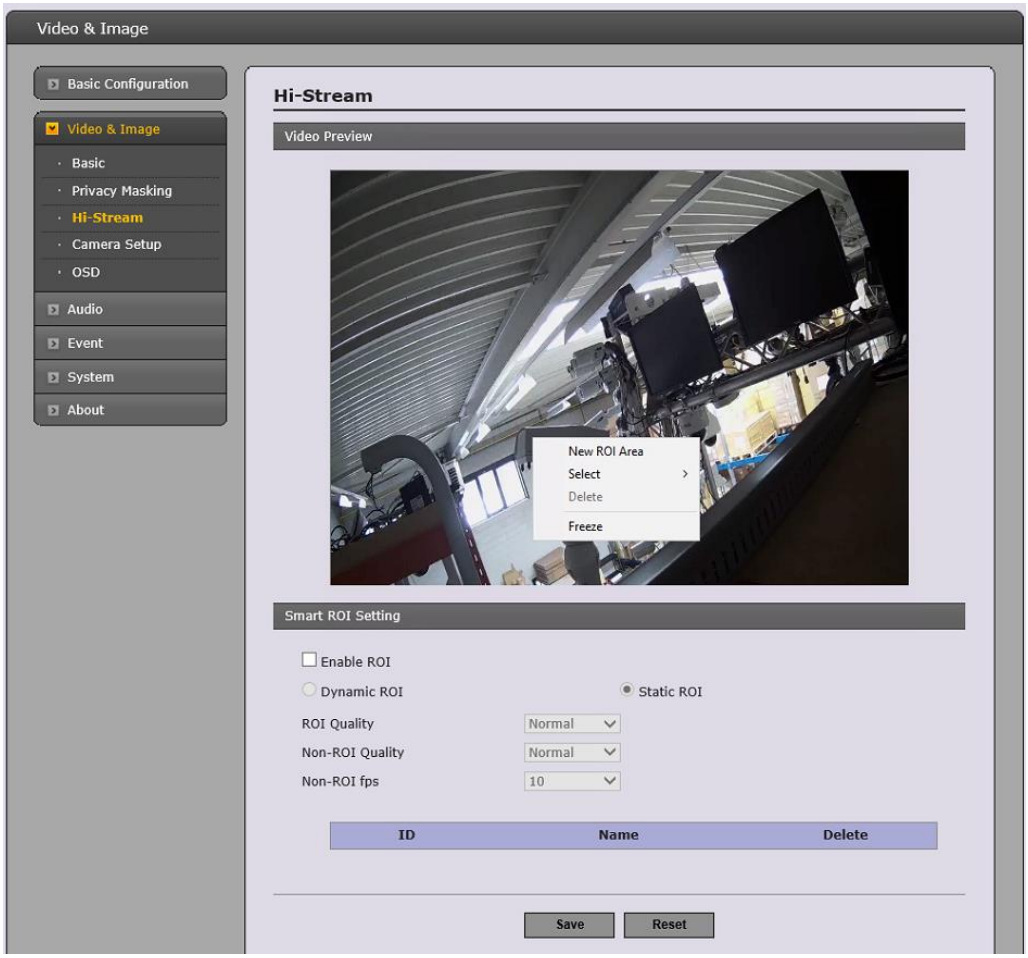


The privacy masking function allows you to mask parts of the video image to be transmitted. You can set up to sixteen privacy masks.
The privacy masks are configured by mask windows. Each window can be selected by click- ing with the mouse. It is also possible to resize or delete, or move the window, by selecting the appropriate window at the mouse menu on the video screen.

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

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

2.2.3. Hi-Stream



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

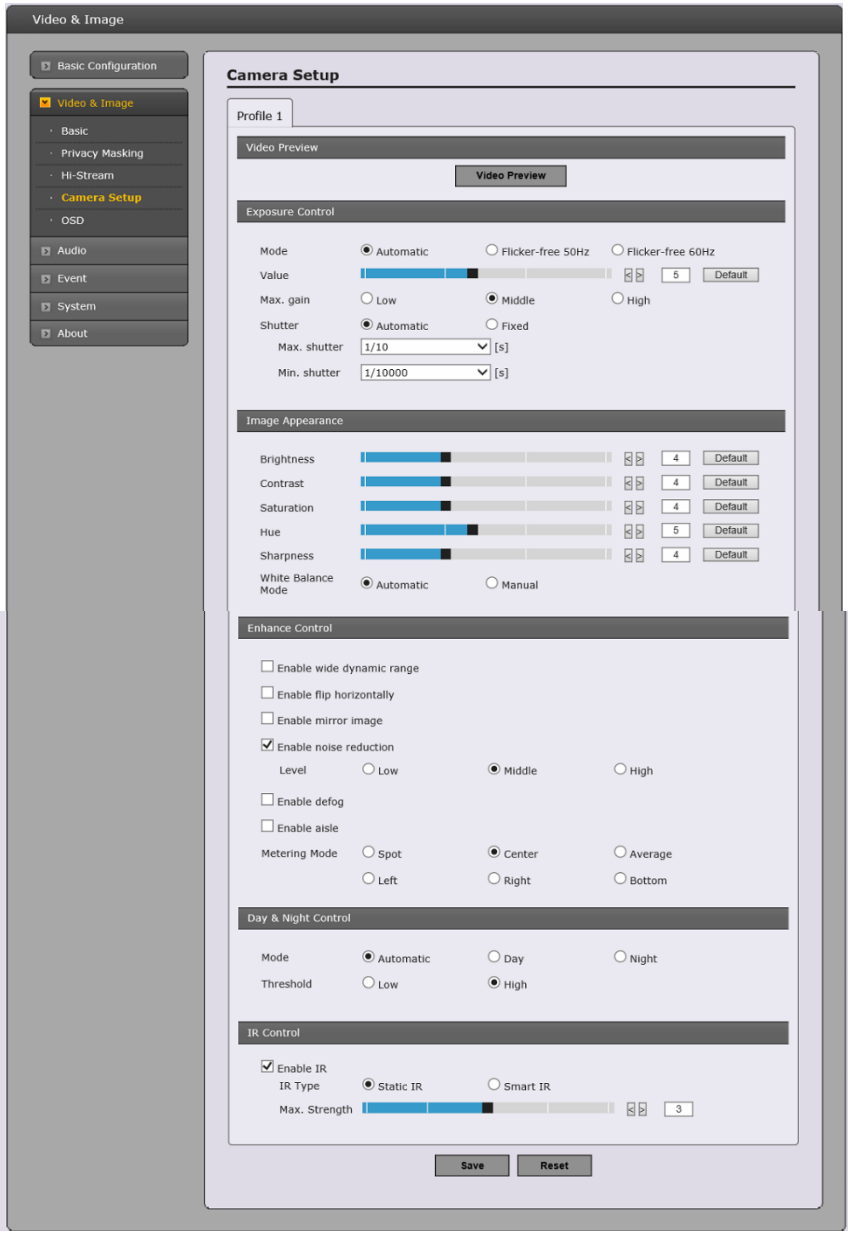
Enable ROI: Select 'Enable ROI' to active Hi-Stream function. Video mode will be fixed to CVBR.

- Create region: Click the right button of mouse and select **New ROI Area**.
  Click the left button of mouse and drag to make window.

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

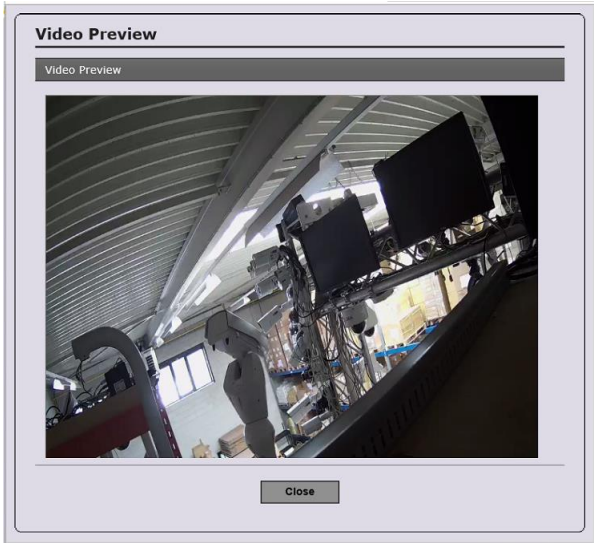
- **ROI Quality**: Set quality of the selected area.
- **Non-ROI Quality**: Set quality of the non-selected area.
- **Non-ROI fps**: Set frame rate of the non-selected area.

2.2.4. Camera Setup

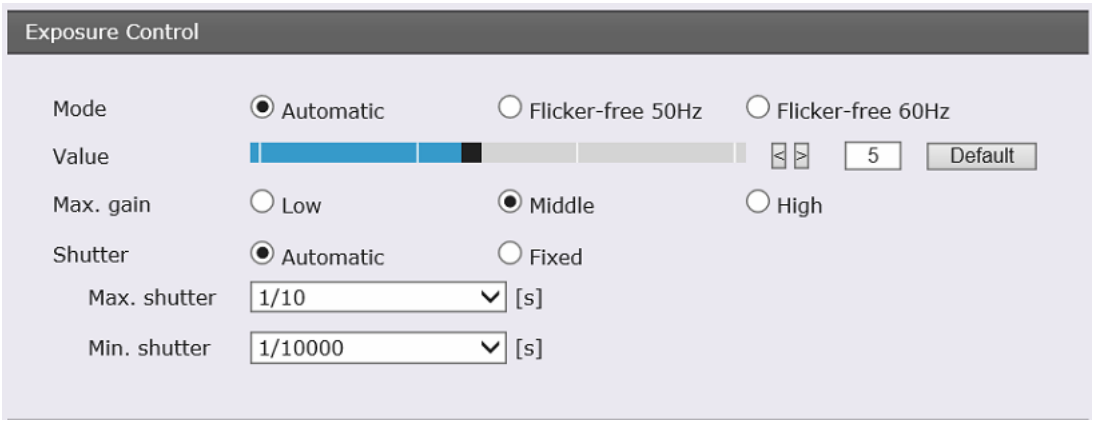


In this page, user can setup Exposure Control, White Balance Control, Image Appearance, and Day & Night Control.

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

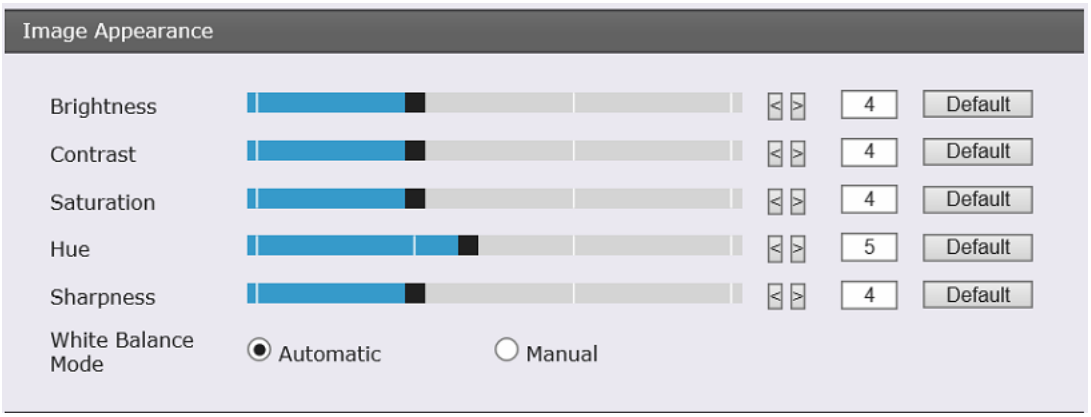


Exposure Control



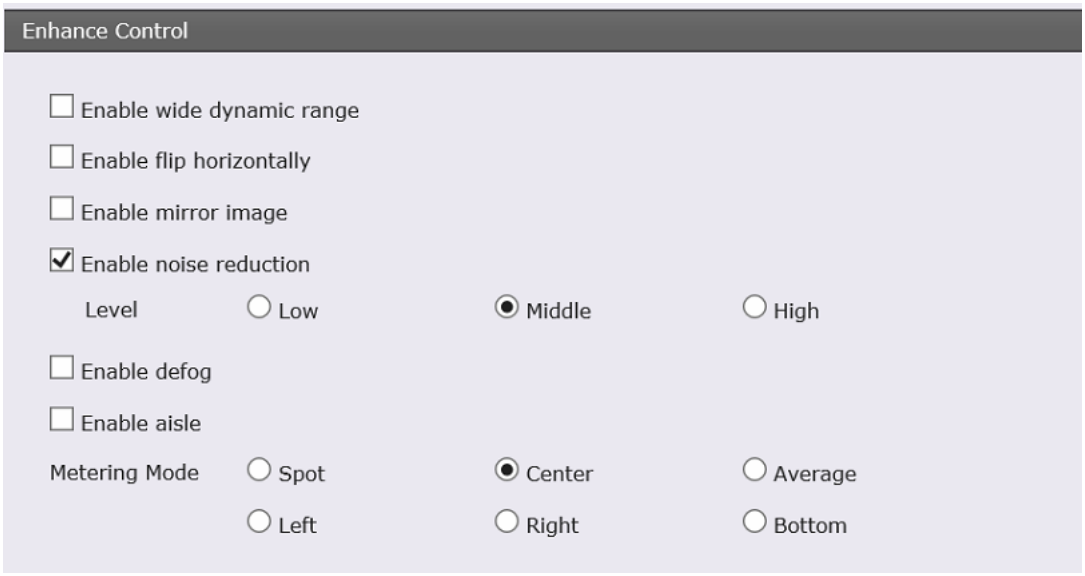
Mode: Determines exposure mode among automatic and flicker-free modes.
Users can use Automatic mode with full shutter speed or Flicker-free mode with a limited range of shutter due to an anti-flicker function.
Max. gain: Sets maximum gain threshold.
Shutter: Sets shutter speed of the sensor. If users set Automatic, Max shutter and Min shutter can be selected.
If the object is as fast as a car, please change the Max shutter to a faster value (eg 1/10 -> 1/120). If users set Manual, fixed shutter speed can be selected.
Note: If the shutter speed is set Manual, the screen may be saturated or dark.
Max. shutter: Users can set the limit for slow shutter speeds used in dark environments.
Min. shutter: Users can set the limit for fast shutter speeds used in bright environments.
Enable P-IRIS: Check this box to activate the P-IRIS function
If users set Automatic, users can specify the range of P-IRIS to be used, and P-IRIS is automatically adjusted according to the amount of light around the camera.
If users set Manual, P-IRIS is fixed.
(Only, P-IRIS is changed to maximum open due to the securing of light intensity at night shift.)

Image Appearance



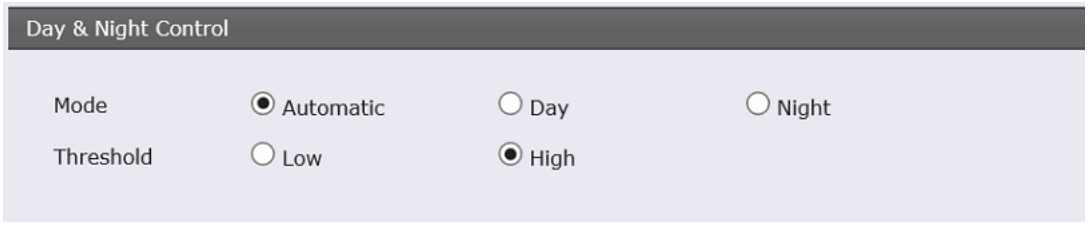
This provides access to the advanced image settings for the network camera.
Brightness: The image brightness can be adjusted in the range 1-10, where a higher value produces a brighter image.
Contrast: Adjust the image's contrast by raising or lowering the value in this field.
Saturation: Set an appropriate value in the range 1-10. Lower values mean less color saturation.
Hue: Set an appropriate value in the range 1-10. The value distinguishes color, such as red, yellow, green, or violet.
Sharpness: Set the amount of sharpening applied to the image. A sharper image might increase image noise especially in low light conditions. A lower setting reduces image noise, but the image would be less sharp.
White Balance Mode: Select white balance mode which fits camera installation environment. In case of Manual mode, user can set R, G, B gain manually.

Enhance Control



Enable wide dynamic range: Activates WDR which cannot be used with Defog function. If WDR is activated, shutter mode becomes automatic only.
Enable flip horizontally: Check this box to flip the image.
Enable mirror image: Check this box to mirror the image.
Enable noise reduction: Check this box to activate the noise reduction.
Once enabled, you can select noise reduction level.
Enable defog: Check this box to activate the defog function.
Metering Mode: Users can change the metering mode.
* Metering Mode: Method of measuring the intensity of the light hitting and reflected by a subject in order to determine the exposure required.

Day & Night Control

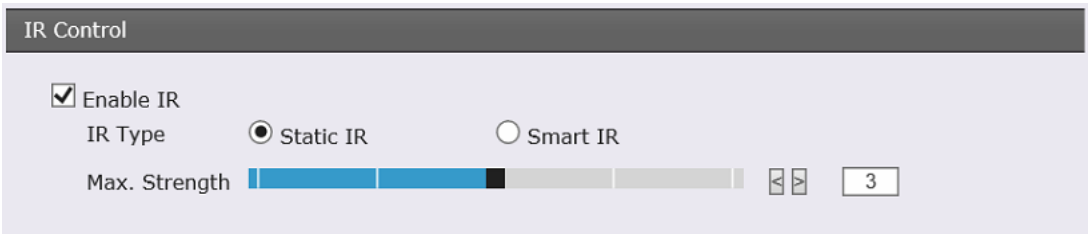


User can setup Day & Night operation mode among Automatic, Day, and Night.
Mode:

- Automatic: Normally displays color image, and switches automatically to black & white image after the ambient light level reaches a pre-defined thresh- old.
- Day: Always displays color image.
- Night: Always displays black & white image.

Threshold: Adjusts the level of light which the camera automatically switches between color and black & white image.
Smart Focus sync with Day & Night: Focus control automatically adjusts upon Day/Night change. (This menu appears for motorized lens model only.)

IR Control

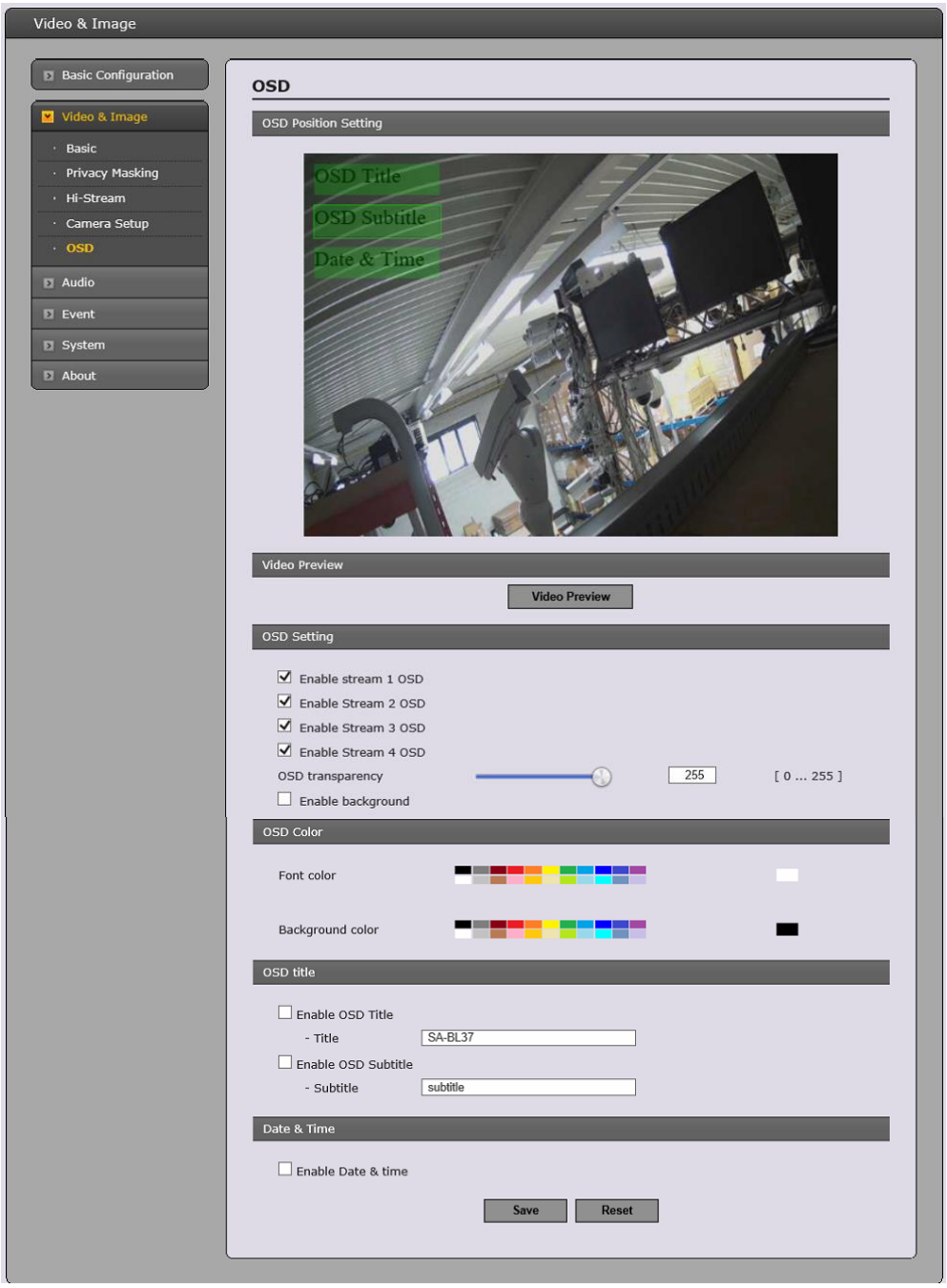


User can enable/disable built-in IR LED and
IR Type:

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

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

2.2.5. OSD

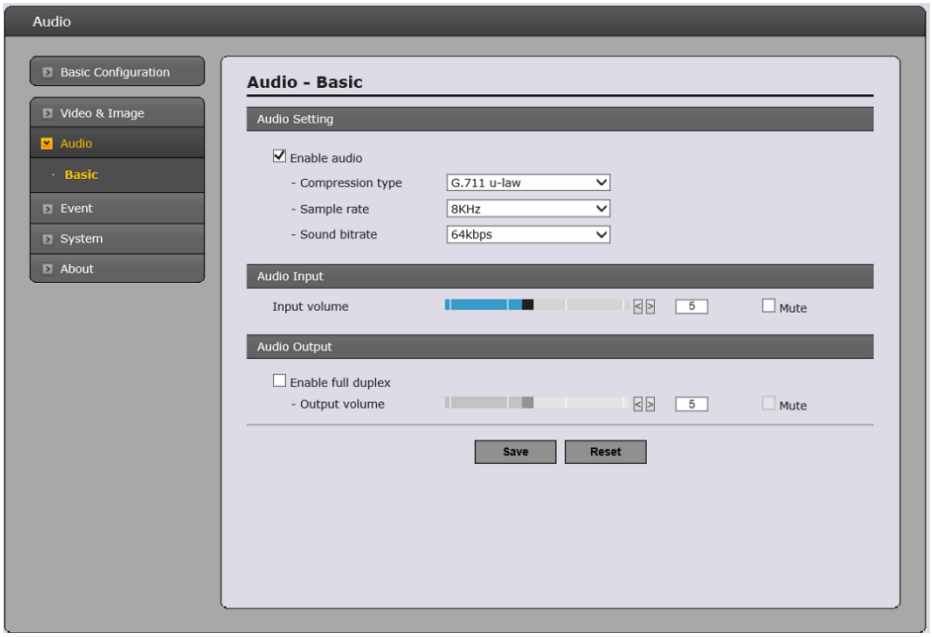


This camera provides two OSD's (on screen display) on each stream, title and date & time. User can drag "OSD Title", "Date & Time" and "PTZ Function" to the desired position and check at preview window.

- **Video Preview**: User can check the position of OSD on actual video via preview pop- up window.
- **OSD Setting**: User can select to show or hide OSD for each stream. Also user can set the transparency level of OSD by slide bar or type in number.
- **OSD title**: User can show or hide OSD title, and can change OSD title by type in. The default is the model name of the camera.
- **OSD subtitle**: User can show or hide OSD subtitle, and can change OSD subtitle by type in. The default is the Subtitle 1.
- **Date & Time**: User can show or hide date & time on OSD.

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

2.2.6. 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: G.711 µ-law
- Sample rate: 8KHz
- Sound bit rate: 64Kbps

Audio Input: Audio from an external line source can be connected to the STEREO Jack I/O of the network camera.

- Input volume: If there are problems with the sound input being too low or high, it is possible to adjust the input gain for the microphone attached to the network camera.
- Mute: User can disable the input audio transmission by checking the box.

Audio Output:

- Enable full duplex: Check the box to enable Full Duplex mode. This means that you can transmit and receive audio (talk and listen) at the same time, without having to use any of the controls. This is just like having a telephone conversation. This mode requires that the client PC has a sound card with support for full-duplex audio.

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

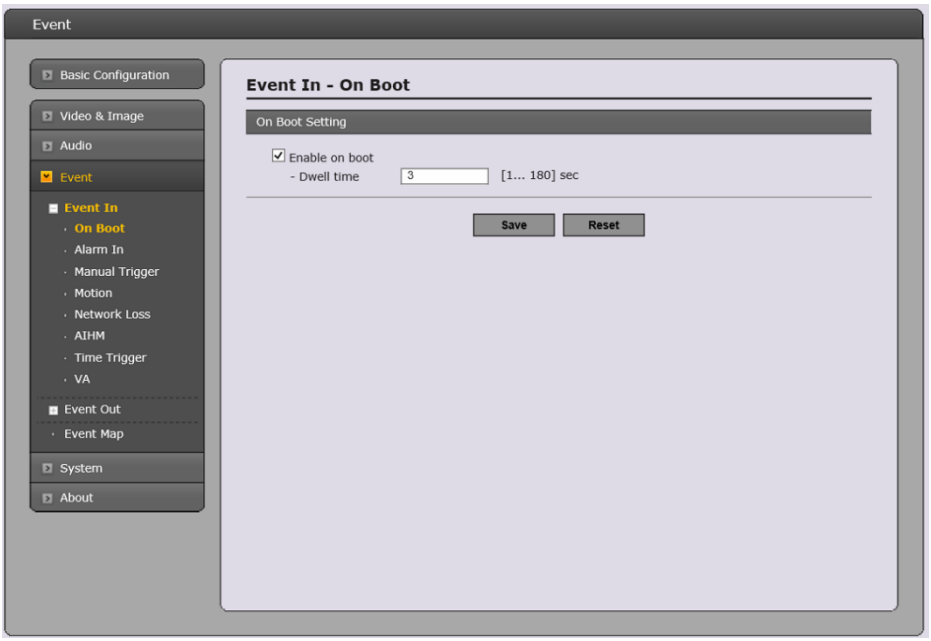
- Output volume: If the sound from the speaker is too low or high it is possible to adjust the output gain for the active speaker attached to the network camera.
- Mute: User can disable the output audio transmission by checking the box.

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

2.3. Event

2.3.1. Event In

On Boot

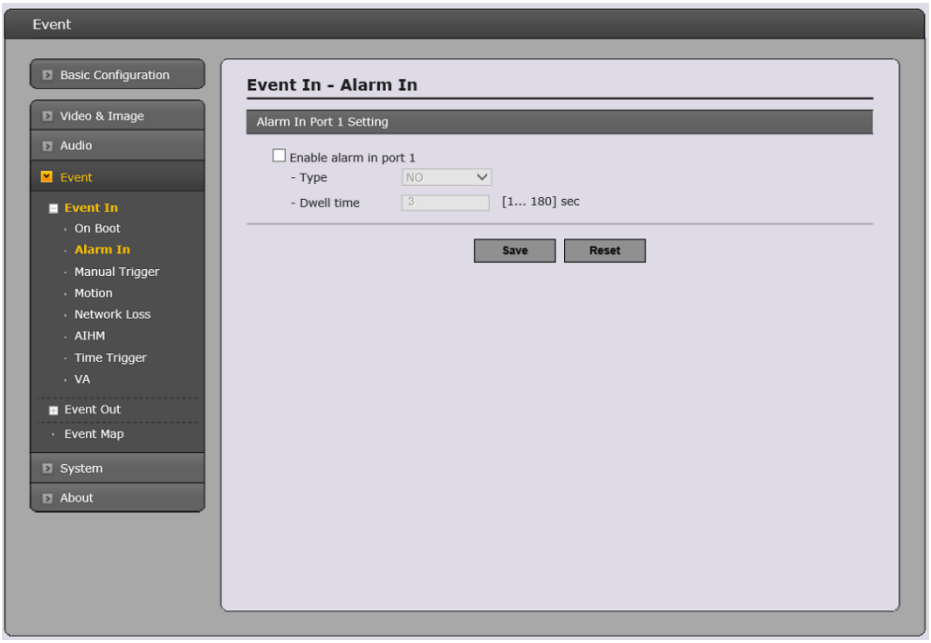


This is used to trigger an event every time the network camera is started. Select “Enable on boot” to activate the On Boot event.

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

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

Alarm In

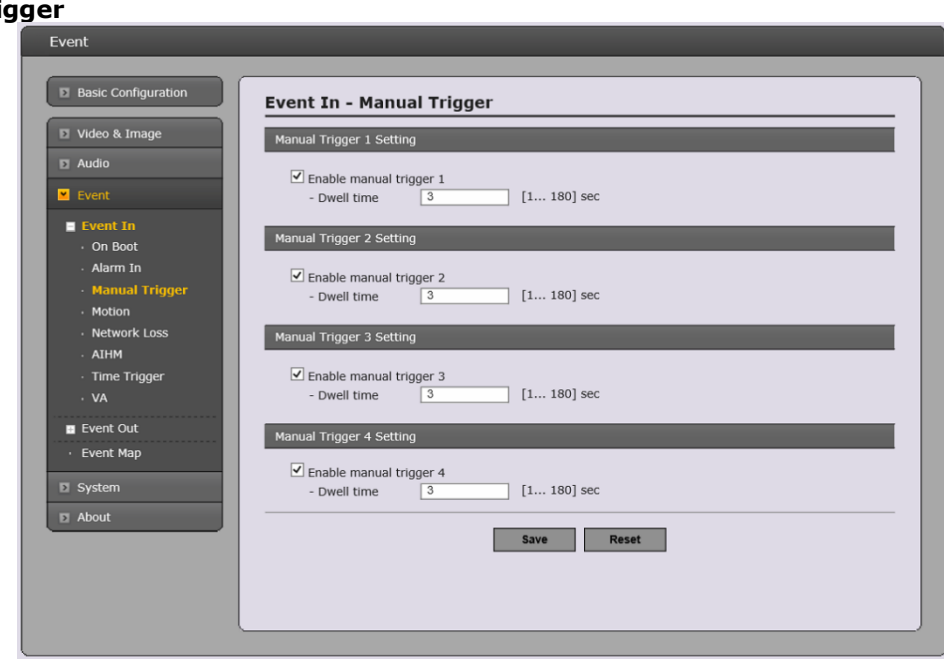


This camera provides 1 Alarm In port and user can set the port. The Port can be given as Normally Open or Normally Close state, and its Normal state can be configured. In order to use the alarm port, check the “Enable alarm port 1” first.

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

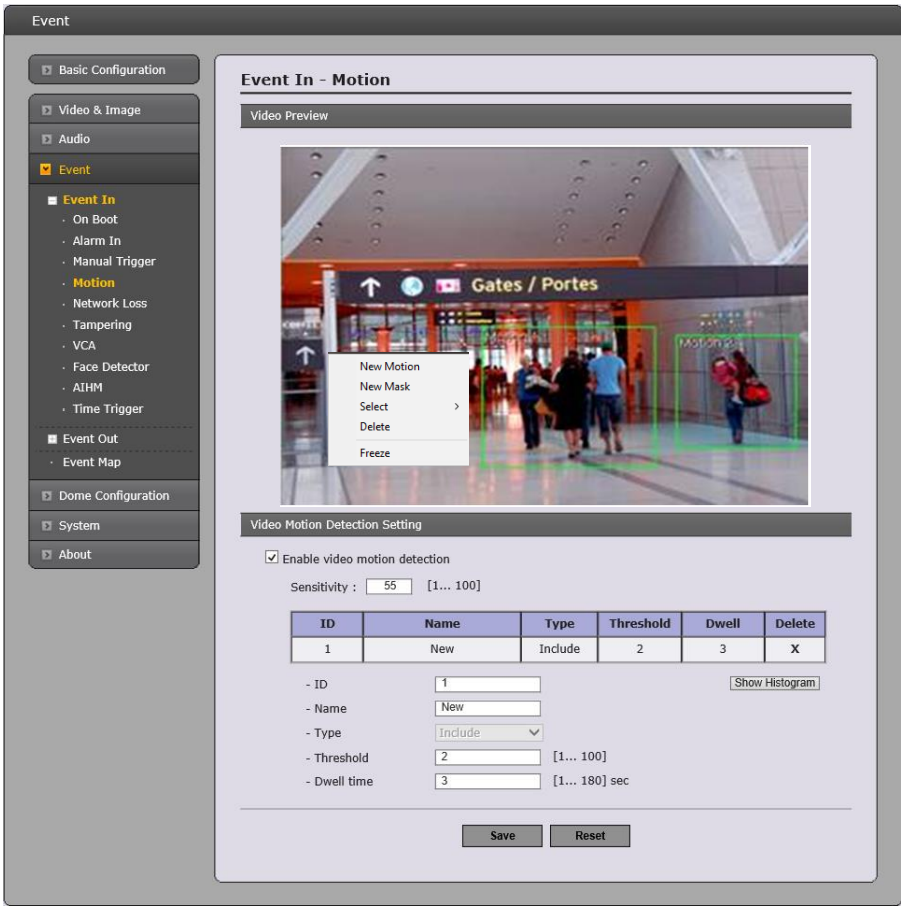
Manual Trigger



This option makes use of the manual trigger button provided on the Live View page, which is used to start or stop the event type manually. Alternatively, the event can be triggered via the product's API (Application Programming Interface). Select "Enable manual trigger" to activate the manual trigger (for up to 4 manual triggers).
Set the dwell time the trigger lasts.

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

Motion



This option makes use of the motion detection function with 16 programmable areas, 8 **Include** and **Exclude** zones each.

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

- Select New Motion and click&drag generates an Include box of green color.
- Select New Mask and click&drag generates an Exclude box of orange color.
- Drag corner or line resizes and drag inside moves the box.
- Select “Enable video motion detection” to activate motion detection.

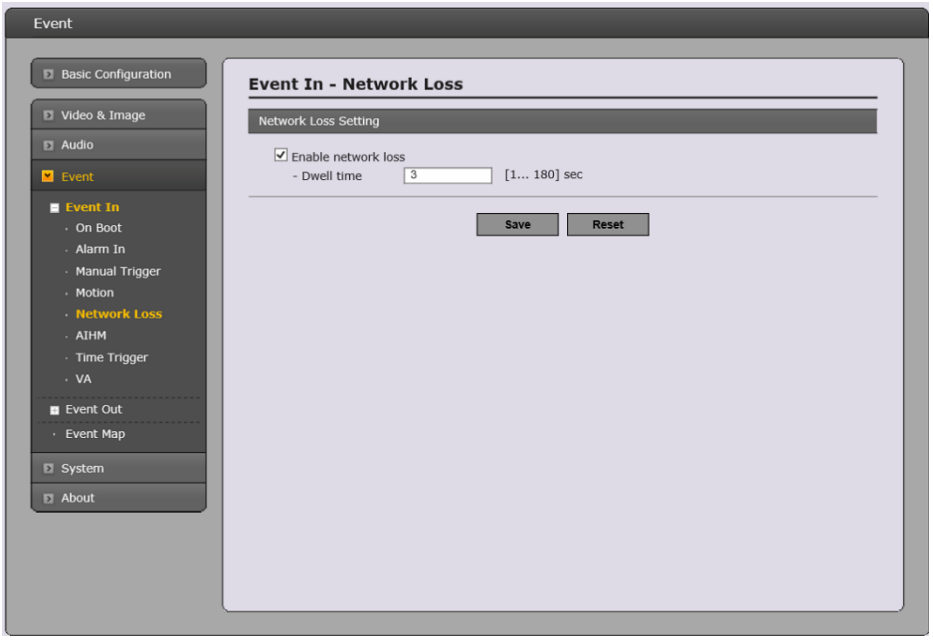
Sensitivity: User can change sensitivity of this function, where large value sets more sensitive detection.

Zone List
ID: Order of generation, Include 1~8, Exclude 9~16.
Name: User definable zone name.
Type: shows zone type and cannot be changed.
Threshold: Determines how large the motion in the zone can trigger event in percentage.
Dwell time: Determines how long the triggered event holds from the last triggering.

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

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

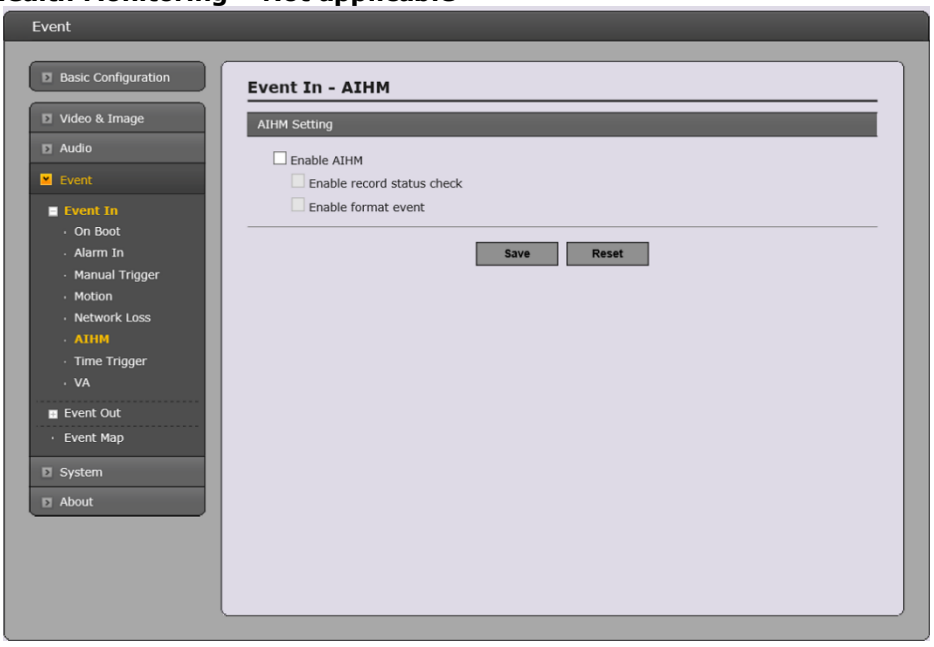
Network Loss



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

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

Advanced Health Monitoring – Not applicable



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.

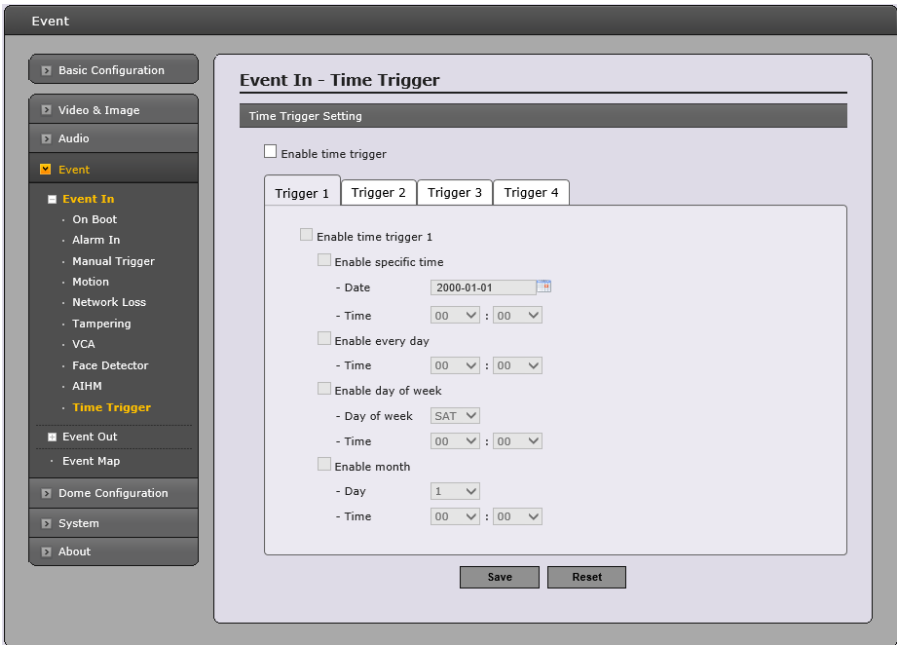
AIHM Server Setting: Select “Enable AIHM Server” to activate the AIHM Server function

- Enable AIHM Server: If selected, the message is sent to the AIHM server.

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

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.

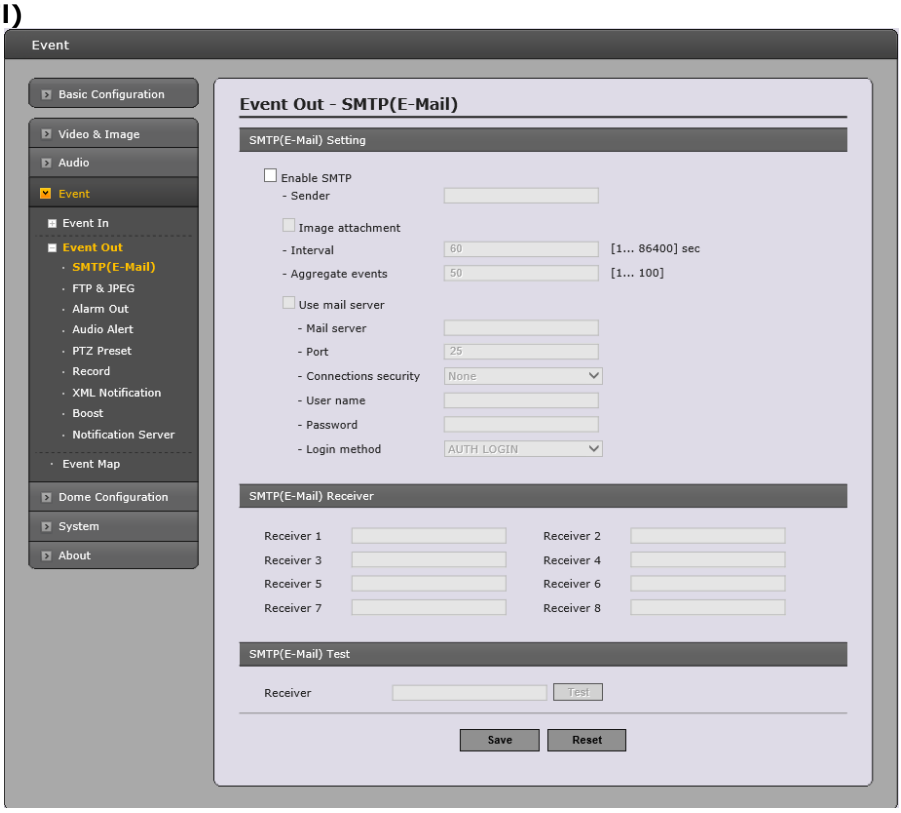
Select “Enable time trigger” to activate the Time Trigger function.

- **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.

2.3.2. Event Out

SMTP (E-Mail)



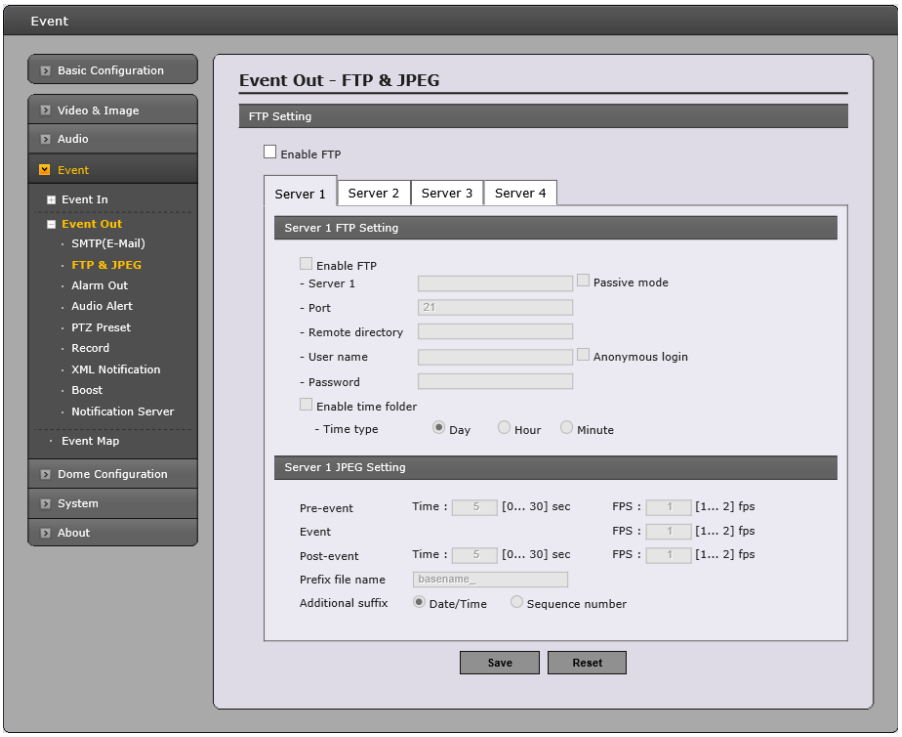
The network camera can be configured to send event and error email messages via SMTP (Simple Mail Transfer Protocol).

- SMTP (E-Mail) Setting: Select “Enable” to activate the SMTP operation.
    - Sender: Enter an email address to be used as the sender for all messages sent by the network camera.
    - Interval: Represents the time interval of the email notification when events occur several times.
    - Aggregate events: Shows the maximum number of emails sent within each interval.
    - Use Mail Server: Check the box is 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: User can assign up to 8 receivers.
    - Receiver #: Enter an email address.

- SMTP (E-Mail) Test: User can check the SMTP setting via a sample email.
    - Receiver: Enter an email address and click the Test button to test that the mail servers are functioning and that the email address is valid.

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

FTP & JPEG

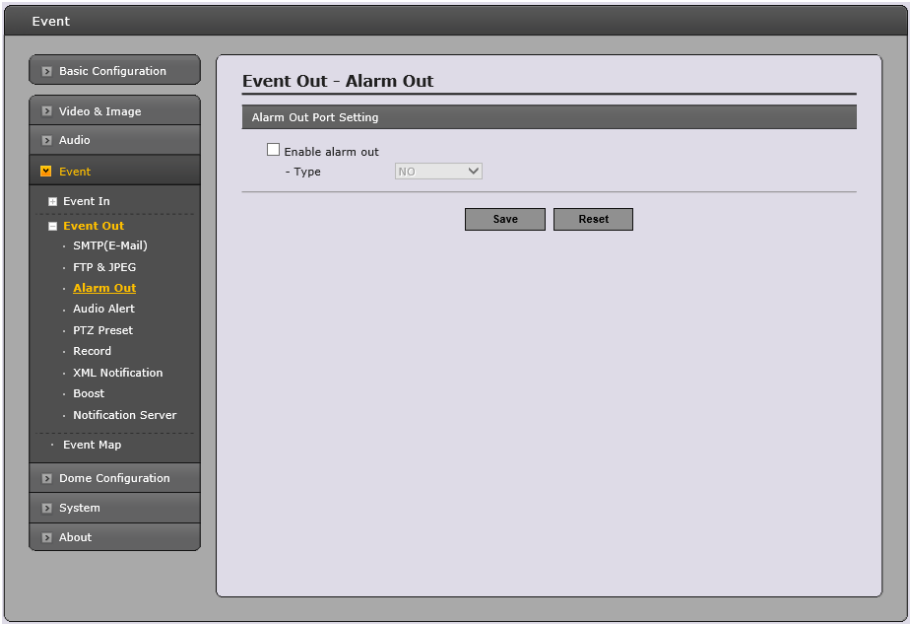


When the network camera detects an event, it can record and save images to an FTP server. Images can be sent as e-mail attachments. Check the “Enable FTP” box to enable the service. This camera can support multiple FTP servers and user can configure each server settings separately.

- FTP Setting:
  - Server: Enter the server’s IP address or host name. Note that a DNS server must be specified in the TCP/IP network settings if using a host name.
  - 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.
  - Port: Enter the port number used by the FTP server.
  - Remote directory: Specify the path to the directory where the uploaded images will be stored. If this directory does not already exist on the FTP server, there will be an error message when uploading.
    - User name/Password: Provide your log-in information.
    - Anonymous login: Check the box if you want to use anonymous login method and the server supports it.
  - Enable time folder: To create the folder in the FTP Server.
    - Time type: Create the folder by daily, hourly and every minute. .
- JPEG Setting:
  - Pre-event: A pre-event buffer contains images from the time immediately preceding the event trigger. These are stored internally in the server. This buffer can be very useful when checking to see what happened to cause the event trigger. Check the box to enable the pre-trigger buffer, enter the desired total length in seconds, minutes or hours, and specify the required image frequency.
  - Event: This function can set required image frequency (1~2fps) when event detected.
  - Post-event: This function is the counterpart to the pre-trigger buffer described above and contains images from the time immediately after the trigger. Configure as for pre-event.
  - Prefix file name: This name will be used for all the image files saved. If suffixes are also used, the file name will take the form <prefix> <suffix>.<extension>.
  - Additional suffix: Add either a date/time suffix or a sequence number, with or without a maximum value.

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

Alarm Out

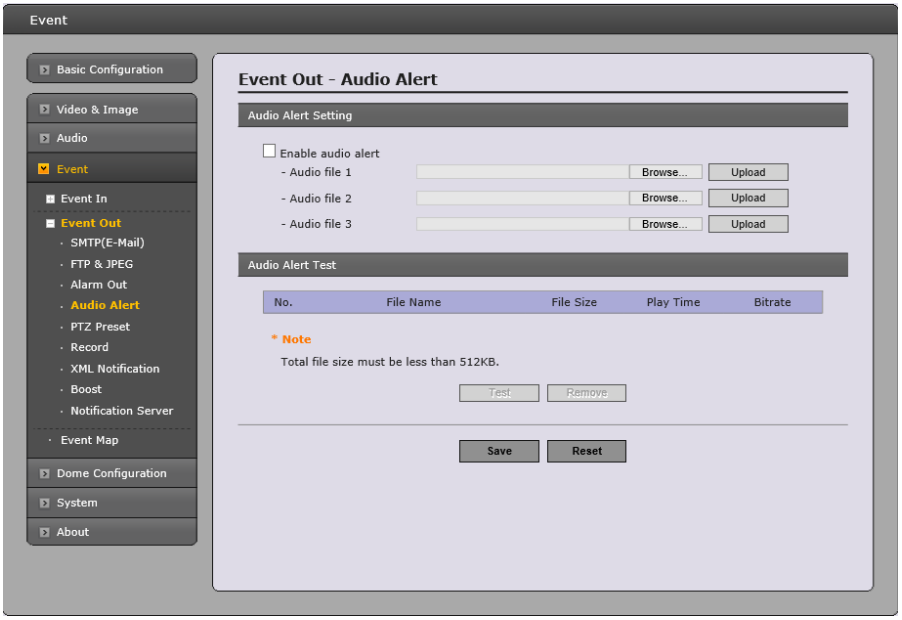


When the network camera detects an event, it can control external equipment connected to its alarm output port.

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

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

Audio Alert



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

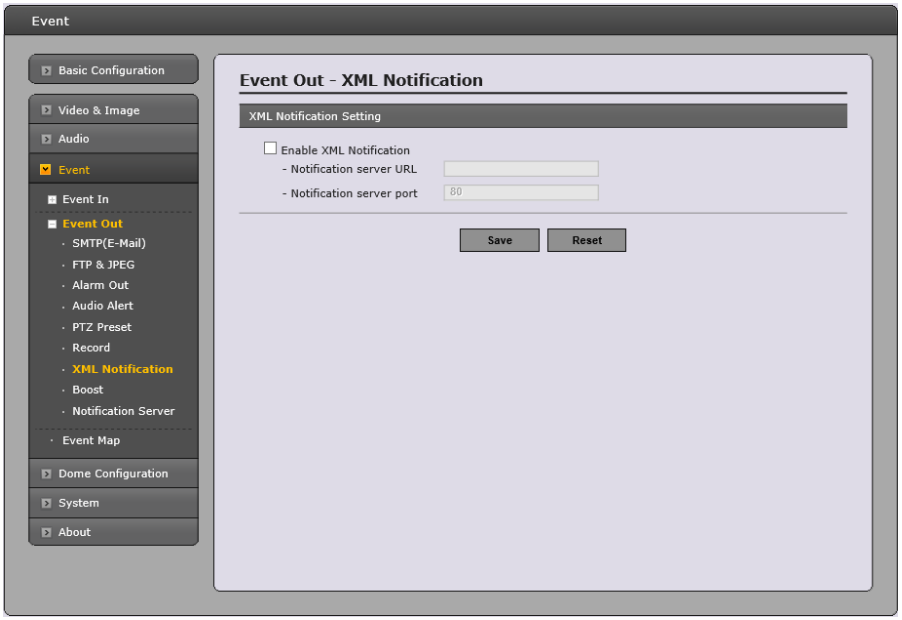
- Audio Alert Setting: To use the audio alert with the network camera, an audio data file made by user must be uploaded from your PC. Provide the path to the file directly, or use the Browse button to locate it. Then click the Upload button. Up to 3 audio files are available. The total file size must be less than 512 KB.
- Audio Alert Test: When the setup is complete, the audio output can be tested by clicking the Test button. To remove an audio file, select the file and click the Remove button.

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

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

Record
Local recording is not supported

XML Notification



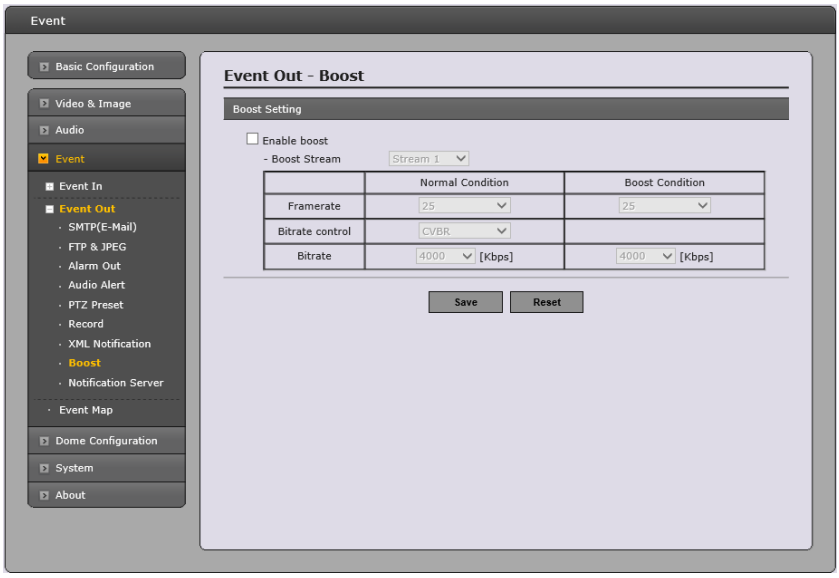
When the network camera detects an event, Notification server is used to receive notification messages as a type of XML data format. Check the box to enable the service.

XML Notification Setting:

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

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

Boost



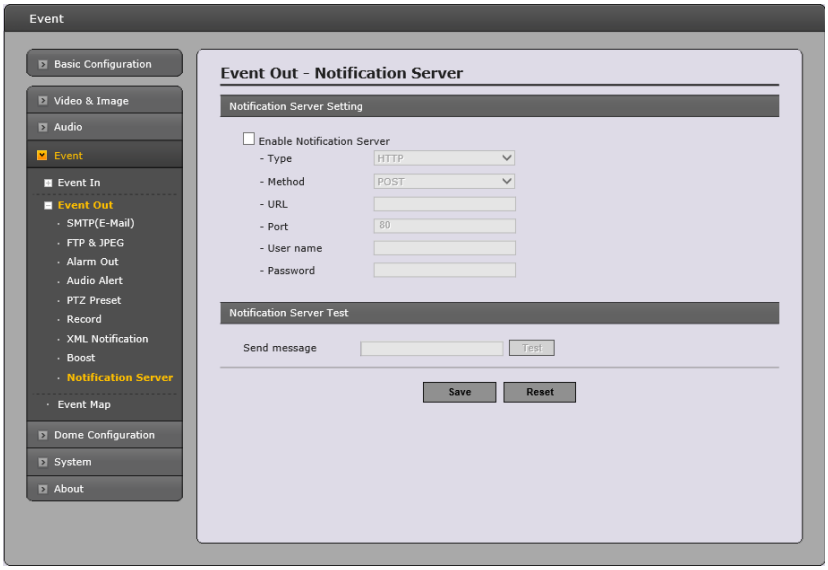
The Boost feature is used in conjunction with event detection. When this feature is turned ON, the Frame rate and Bit rate in the boost condition can be set to a different value than the ones in the normal condition field. When an event is detected, the camera will boost the Frame rate and Bit rate from the normal condition to this boosted level for the duration of the event.

Check the box to enable the service.
Boost Setting: You can set the condition in Normal and Boost mode.

- **Boot Stream**: Select a video stream for each condition in the drop-down list.
- **Frame rate**: Select a frame refresh rate per second for each condition in the drop-down list.
- **Bit rate control**: Select VBR or CBR in the drop-down list in Normal Condition. You cannot change it in Boost Condition.
- **Bit rate**: Select a value for each condition in the drop-down list.

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

Notification Server



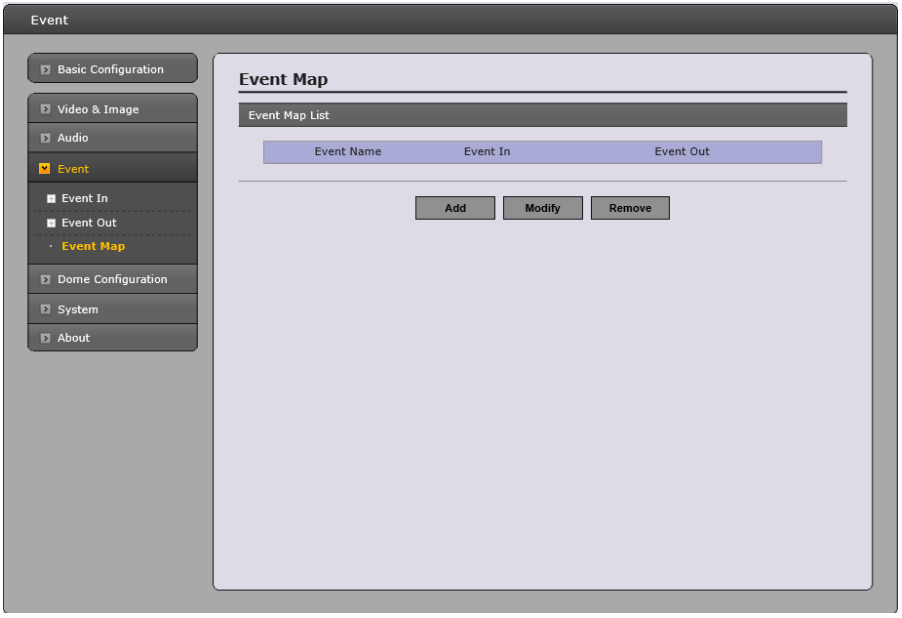
When the network camera detects an event, the Notification Server is used to receive uploaded image files and/or notification messages. Check the box to enable the service.

Notification Server Setting:

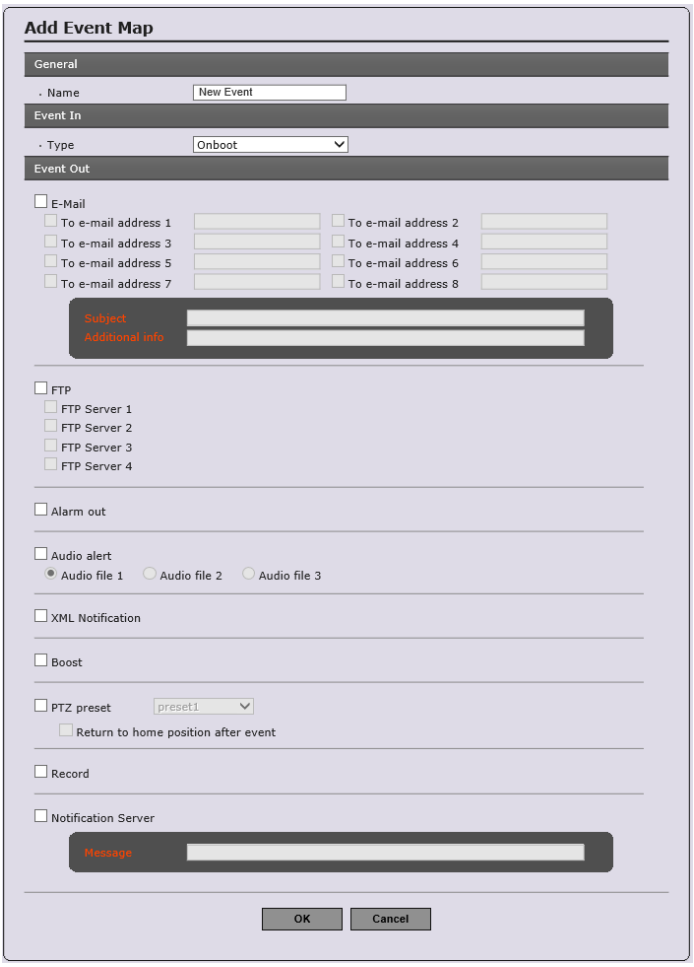
- Type: User can select message transmission type among HTTP, HTTPS, TCP, and UTP.
- URL: The network address to the server and the script that will handle the request.
- For example: http://192.168.12.244/cgi-bin/upload.cgi
- Port: The port number of the server.
- User name/Password: Provide your log-in 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.

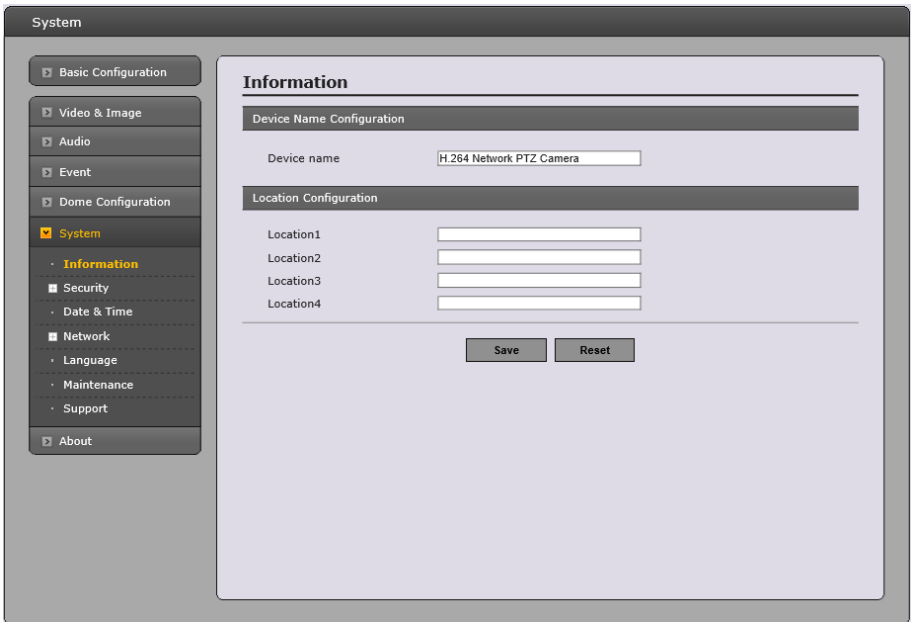
- Event Out:

- **E-mail:** Select the email addresses you want to notify via email that an event has occurred.
- **FTP:** Select checkbox beside FTP and FTP Servers to record and save images to FTP server when an event has occurred.
- **Alarm out:** Check this box to enable the alarm out.
- **Audio Alert:** Select an Audio Alert file as the Network Transmitter output when audio alert event triggered. The Audio Alert file must first be configured on the Event In page.
- **XML Notification:** It sends XML messages to a Notification server that listens for these. The destination server must first be configured on the Event In page.
- **Boost:** When an event has occurred, the camera will boost the Frame rate and Bit rate from the normal condition to this boosted level for the duration of the event. Check the box to enable the Function.
- **PTZ preset:** Select the preset position you want to move at event. If you want to move back to home position after the event, which is pre-defined in the Alarm Out - PTZ Preset page, check “Return to home position after event” box.
- **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 **Save** button to save the settings, or click **Reset** button to clear all of the information you entered without saving it.

2.4. System

2.4.1. Information



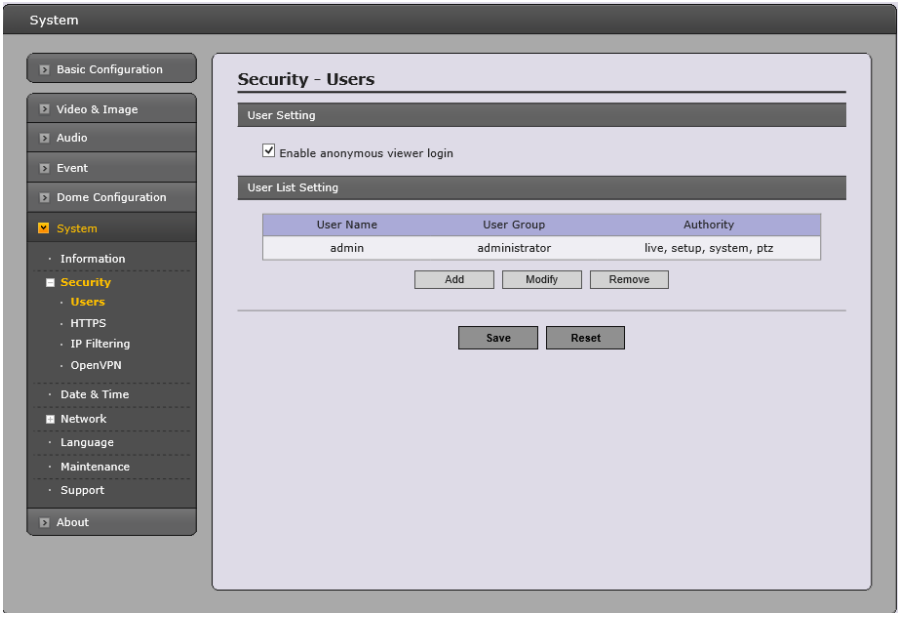
You can enter the system information. This page is very useful when you require device information after installation.

- Device Name Configuration: Enter the device name.
- Location Configuration: Enter the location information. You can enter up to four locations.

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

2.4.2. Security

Users

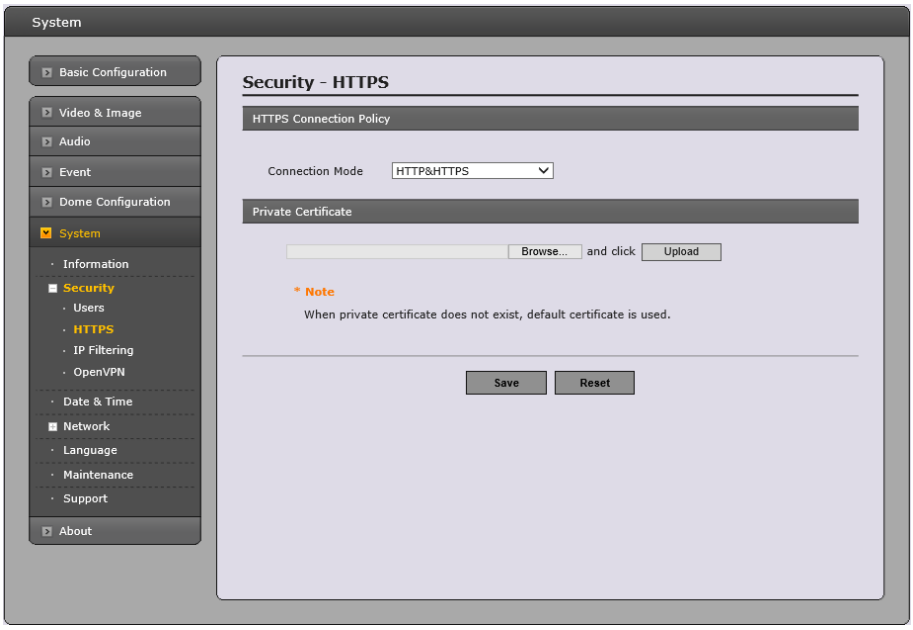


User access control is enabled by default when the administrator sets the root password on first access. New users are authorized with user names and passwords, or the administrator can choose to allow anonymous viewer login to the Live View page, as described below:

- **User Setting**: Check the box to enable anonymous viewer login to the network camera without a user account. When using the user account, users have to log-in at every access.
- **User List Setting**: This section shows how to register a user account. Enter a user name and password to be added, and register them by pressing the Add button. You will see the pop-up window as below.

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

HTTPS



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

- **HTTPS Connection Policy**: Choose the form of connection you wish to use from the drop-down list for the administrator, Operator and Viewer to enable HTTPS connection (set to HTTP by default).
    - HTTP
    - HTTPS
    - HTTP & HTTPS
- **Upload Certificate**: To use HTTPS for communication with the network camera, an official certificate issued by a CA (Certificate Authority) must be uploaded from your PC. Provide the path to the certificate directly, or use the Browse button to locate it. Then click the Upload button.

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

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

IP Filtering

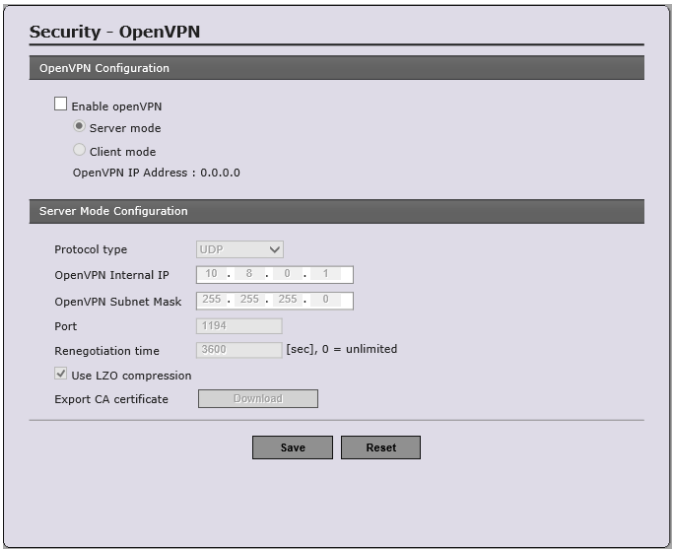
Checking the “Enable IP filtering” box enables the IP address filtering function.

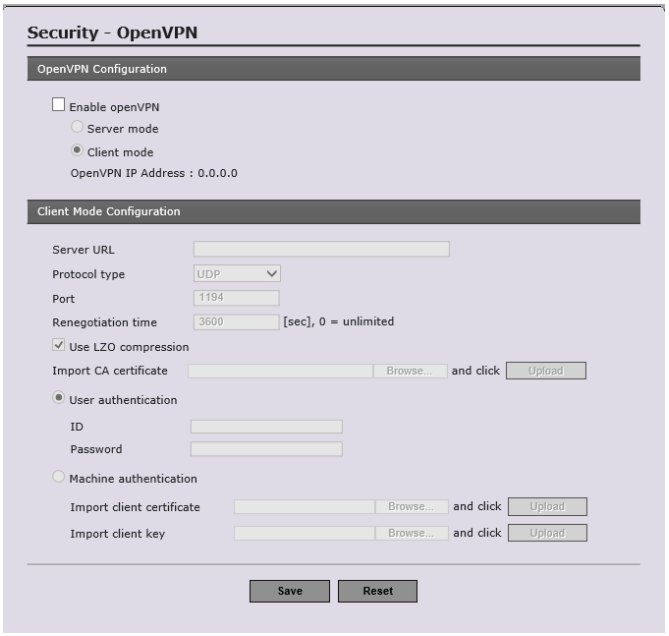
When the IP address filter is enabled, addresses added to the list are set as allowed or denied addresses. All other IP addresses not in this list will then be allowed or denied access accordingly, that is, if the addresses in the list are allowed, then all others are denied access, and vice versa. Also see the online help for more information.

NOTE: Users from IP addresses that will be allowed must also be registered with the appropriate access rights. This is done from Setup > System > Security > Users.

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

OpenVPN





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

OpenVPN Server Mode

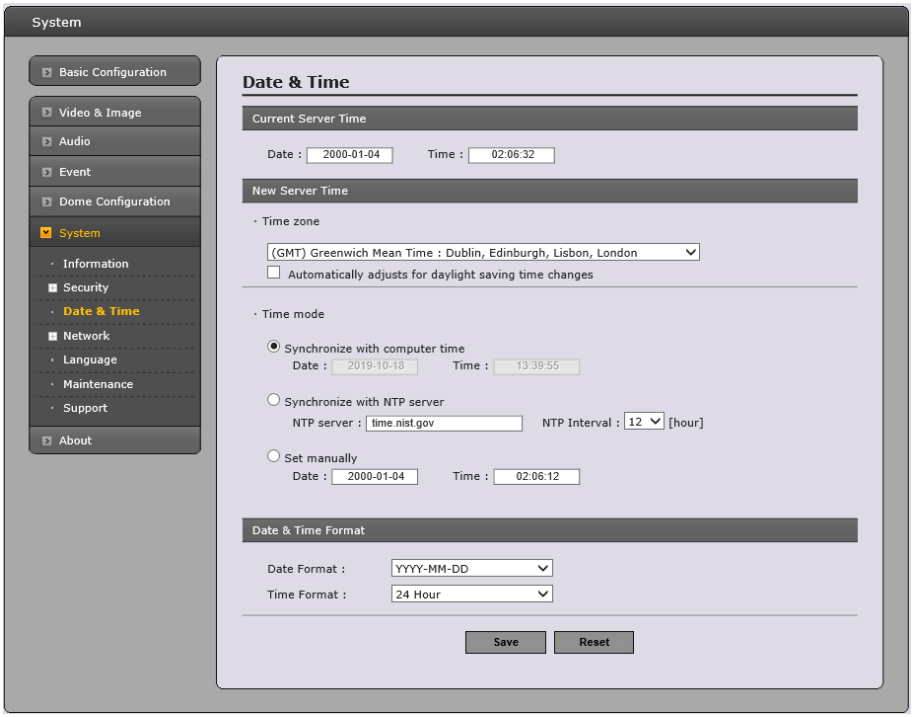
1. Checking the “Enable OpenVPN” box activates mode selection buttons. Choose Server mode, then Server Mode Configuration appears where you can configure Server Mode Settings.
2. In Server Mode Configuration, you can setup Protocol type, Port number, LZO compression usage, and Renegotiation time, as 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. Checking the “Enable OpenVPN” box 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.

2.4.3. Date & Time



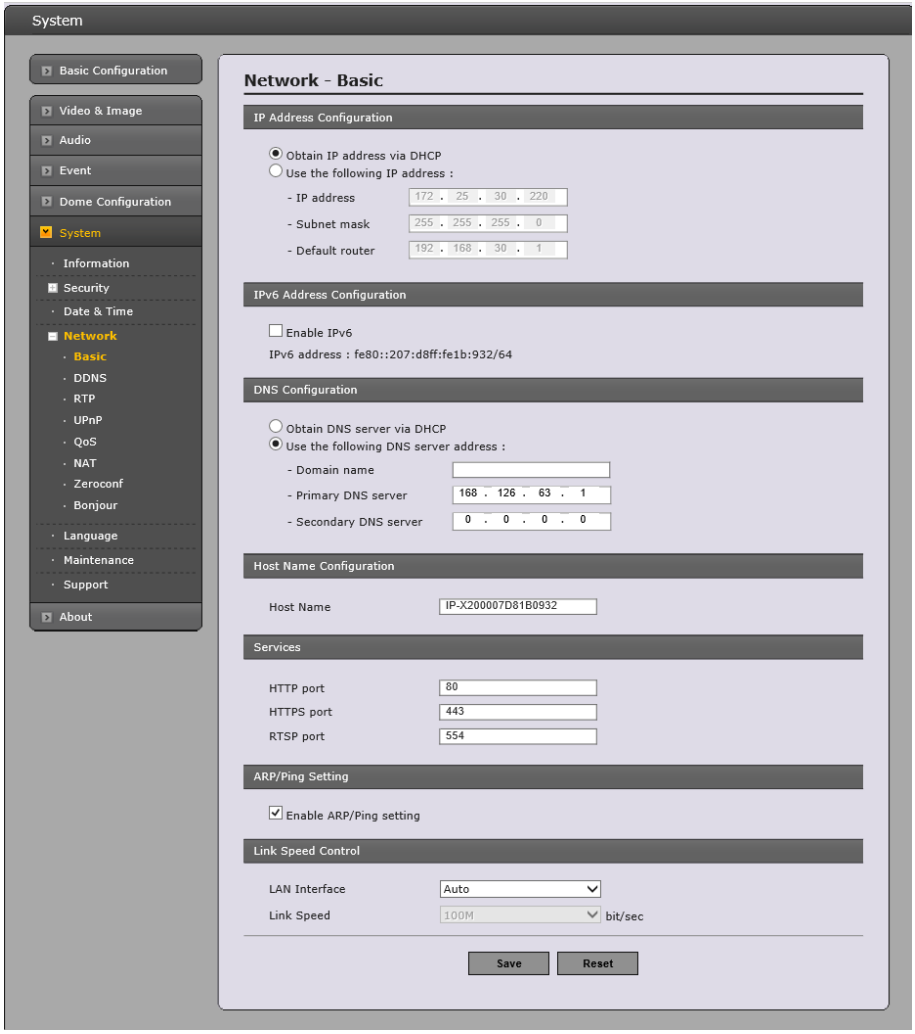
- Current Server Time: This displays the current date and time (24h clock). The time can be displayed in 12h clock format (see below).
- New Server Time:
  - Time zone: Select your time zone from the drop-down list. If you want the server clock to automatically adjust for daylight savings time, check the box “Automatically adjust for daylight saving time changes”.
  - Time mode: Select the preferred method to use for setting the time:
    - Synchronize with computer time: Sets the time from the clock on your computer.
    - Synchronize with NTP Server: The network camera will obtain the time from an NTP server every 60 minutes.
    - Set manually: Allows you to manually set the time and date.
- Date & Time Format: Specify the formats for the date and time (12h or 24h) displayed in the video streams. Select Date & Time format from the drop-down list.
  - Date Format: Specify the date format. YYYY: Year, MM: Month, DD: Day
  - Time Format: Specify the date format. 24 Hours or 12 Hours

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

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

2.4.4. Network

Basic



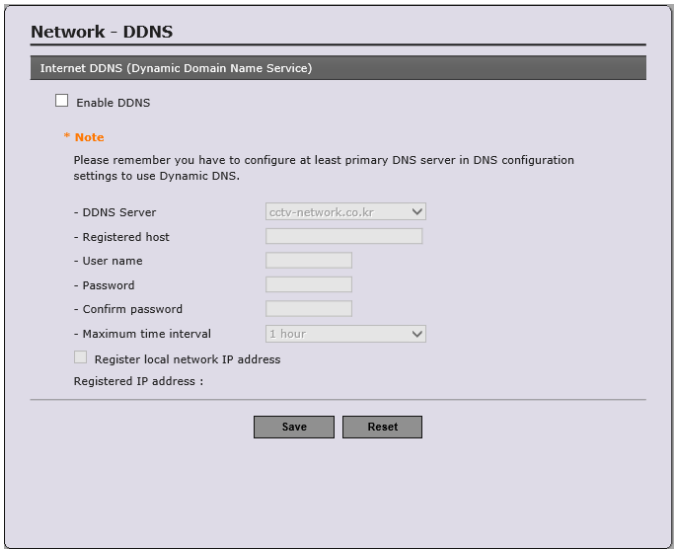
- IP Address Configuration:
  - Obtain IP address via DHCP: Dynamic Host Configuration Protocol (DHCP) is a protocol that lets network administrators centrally manage and automate the assignment of IP addresses on a network. DHCP is enabled by default. Although a DHCP server is mostly used to set an IP address dynamically, it is also possible to use it to set a static, known IP address for a particular MAC address. To obtain IP address via DHCP, check the radio button.
  - Use the following IP address: To use a static IP address for the network camera, check the radio button and then make the following settings:
    - IP address: Specify a unique IP address for your network camera.
    - Subnet mask: Specify the mask for the subnet the network camera is located on.
    - Default router: Specify the IP address of the default router (gateway) used for connecting devices attached to different networks and network segments.
- IPv6 Address Configuration: Check this “Enable IPv6” box to enable IPv6. Other settings for IPv6 are configured in the network router.
- DNS Configuration: DNS (Domain Name Service) provides the translation of host names to IP addresses on your network. Check the radio button to obtain DNS server via DHCP or set the DNS server.
  - Obtain DNS Server via DHCP: Automatically use the DNS server settings 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.
- 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 Speed Control:
  - Link Speed: of the IP address.
- Link: User can select either 10Mbps or 100Mbps.

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

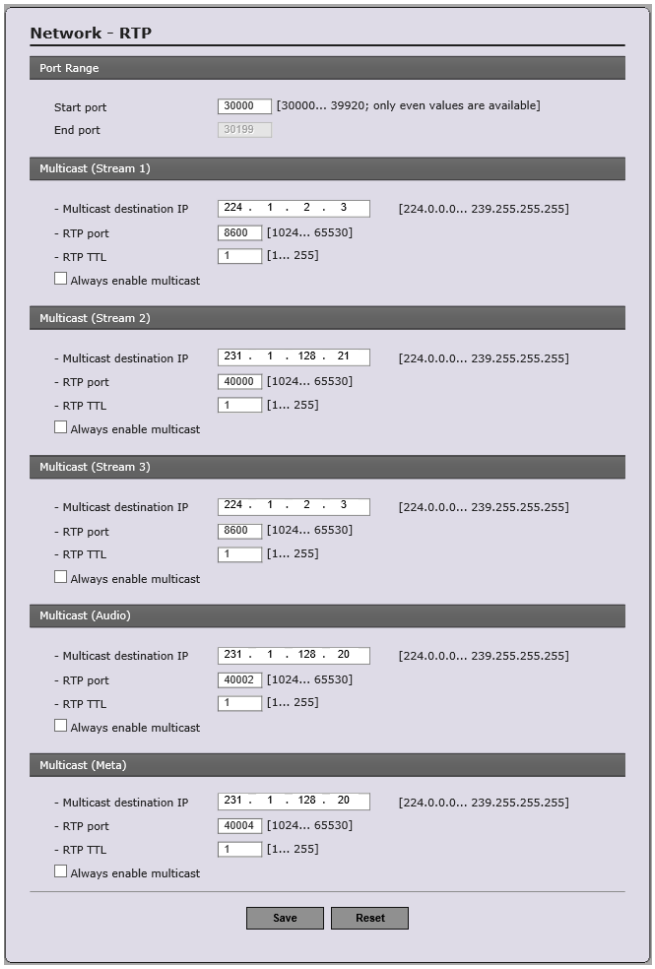
DDNS



- Internet DDNS (Dynamic Domain Name Service): When using the high-speed Internet with the telephone or cable network, users can operate the network camera on the floating IP environment in which IPs are changed at every access. Users should receive an account and password by visiting a DDNS service like http://www.dyndns.org/.
  - Enable DDNS: Check to have DDNS service available.
    - DDNS Server: Select the DDNS server.
    - Registered host: Enter an address of the DDNS server.
    - Username: Enter an ID to access to the DDNS server.
    - Password: Enter a password to be used for accessing the DDNS server.
    - Confirm: Enter the password again to confirm it.
    - Maximum time interval: Set a time interval to synchronize with the DDNS server. Select the time interval from the drop-down list.
    - Register local network IP address: Register a Network Video Server IP address to the DDNS server by checking the box and enter the Registered IP address.

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

RTP

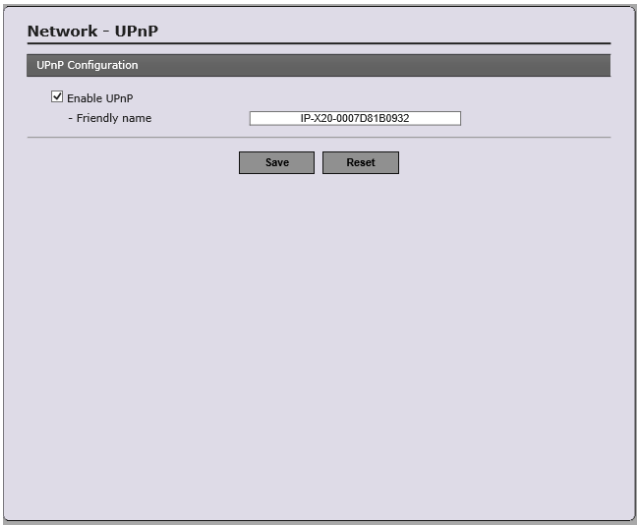


Create a setting for sending and receiving an audio or video on a real-time basis. These settings are the IP address, port number, and Time-To-Live value (TTL) to use for the media stream(s) in multicast H.264 format. Only certain IP addresses and port numbers should be used for multicast streams.

- Port Range:
  - Start/End port: Enter a value between 1024 and 65532.
- Multicast (Stream1/Stream2/Stream3/Audio/Meta): This function is for sending Video, Audio, and Meta Data to Multicast group.
  - Enable Multicast: Check the box to enable multicast operation.
  - Multicast destination IP: Enter an IP between 224.0.0.0 and 239.255.255.255.
  - RTP port: Enter a value between 1024 and 65532.
  - RTP TTL: Enter a value between 1 and 255. If a network status is smooth, enter a lower value. However, if a network status is poor, enter a higher value. When there are many network cameras or users, a higher value may cause a heavy load to the network. Consult with a network manager for detailed information.
  - Always enable multicast: Check the box to start multicast streaming without opening an RTSP session.

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

UPnP



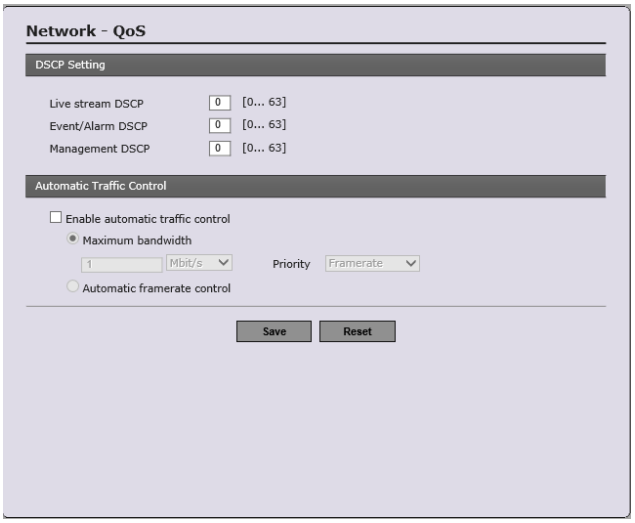
The network camera includes support for UPnP. UPnP is enabled by default, so the network camera is automatically detected by operating systems and clients that support this protocol.

Enter a name in the Friendly name field.

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

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

QoS



Quality of Service (QoS) provides the means to guarantee a certain level of a specified resource to selected traffic on a network. Quality can be defined as a maintained level of bandwidth, low latency, and no packet losses.

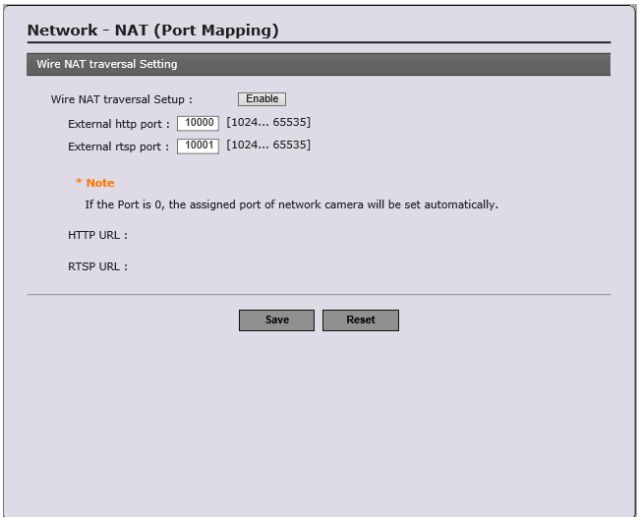
The main benefits of a QoS-aware network are:

1. The ability to prioritize traffic and thus allow critical flows to be served before flows with lesser priority.
2. Greater reliability in the network, due to the control of the amount of bandwidth an application may use, and thus control over bandwidth races between applications.

- DSCP Settings: For each type of network traffic supported by your network video product, enter a DSCP (Differentiated Services Code Point) value. This value is used to mark the traffics IP header. When the marked traffic reaches a network router or switch, the DSCP value in the IP header tells the router or switch which type of treatment to apply to this type of traffic, for example, how much bandwidth to reserve for it. Note that DSCP values can be entered in decimal or hex form, but saved values are always shown in decimal.
- The following types of traffic are marked; enter a value for each type of traffic used:
  - Live Stream DSCP
  - Event/Alarm DSCP
  - Management DSCP
- Automatic Traffic Control: Check the box to enable automatic traffic control. Set a limitation on user network resources by designating the maximum bandwidth. Select either the Maximum bandwidth or Automatic framerate radio button.
  - Maximum bandwidth: When sharing other network programs or equipment, it is possible to set a limitation on the maximum bandwidth in the unit of Mbit/s or Kbit/s.
  - Automatic frame rate: Selected if not influenced by a network-related program or equipment without a limitation on the network bandwidth.

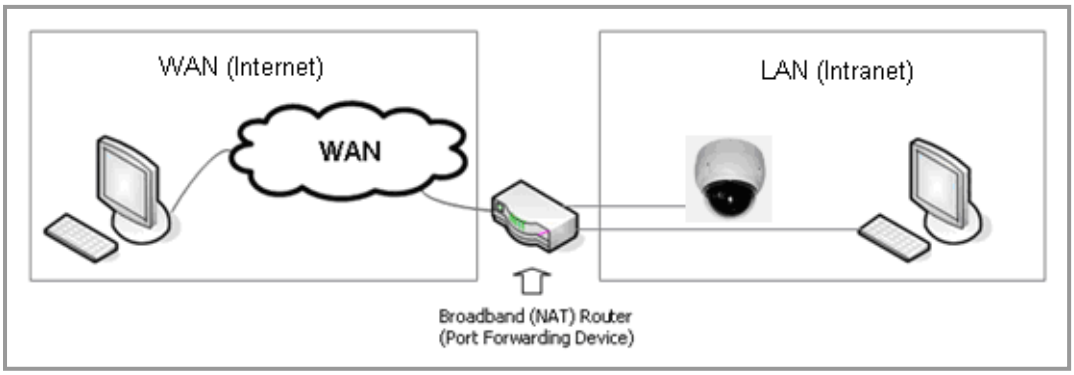
When the settings are complete, click **Save** button to save the settings, or click **Reset** button to clear all of the information you entered without saving it.

NAT (Port Mapping)



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 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.

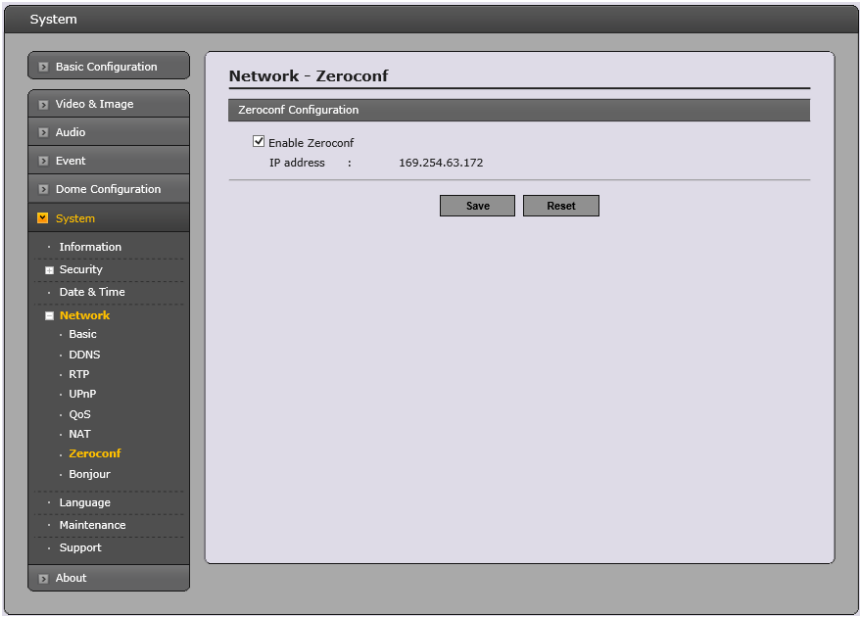


NOTES:

- 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.

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

Zeroconf



Zero configuration networking (zeroconf) is a set of techniques that automatically creates a usable Internet Protocol (IP) network without manual operator intervention or special configuration servers.

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

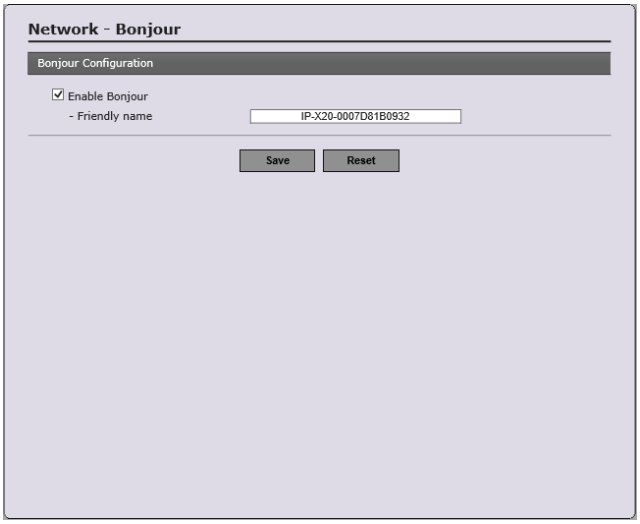
Zeroconf is built on three core technologies:

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

Click the checkbox to enable Zeroconf.

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

Bonjour



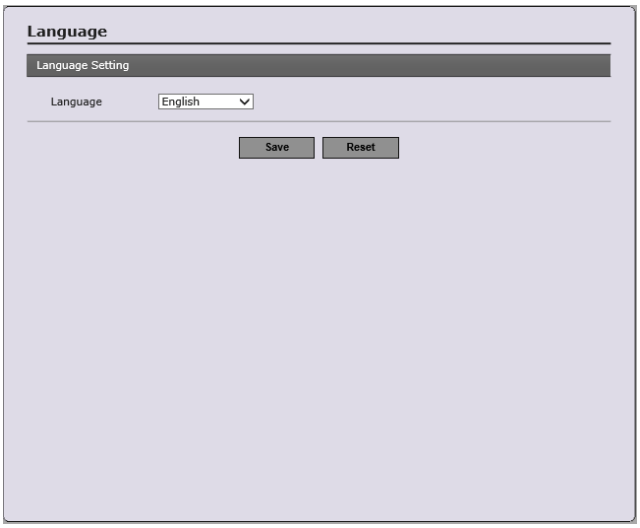
The network camera includes support for Bonjour. When enabled, the network camera is automatically detected by operating systems and clients that support this protocol.

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

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

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

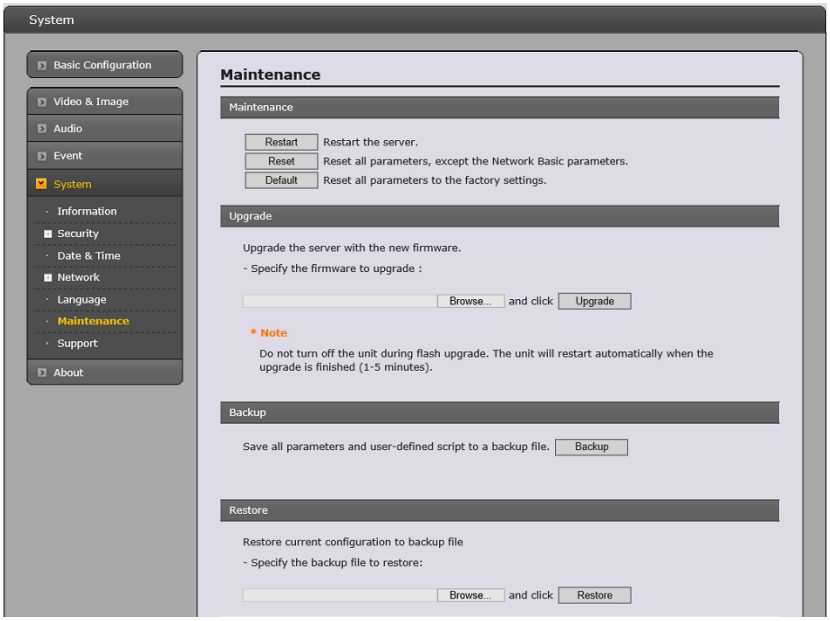
2.4.5. Language



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

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

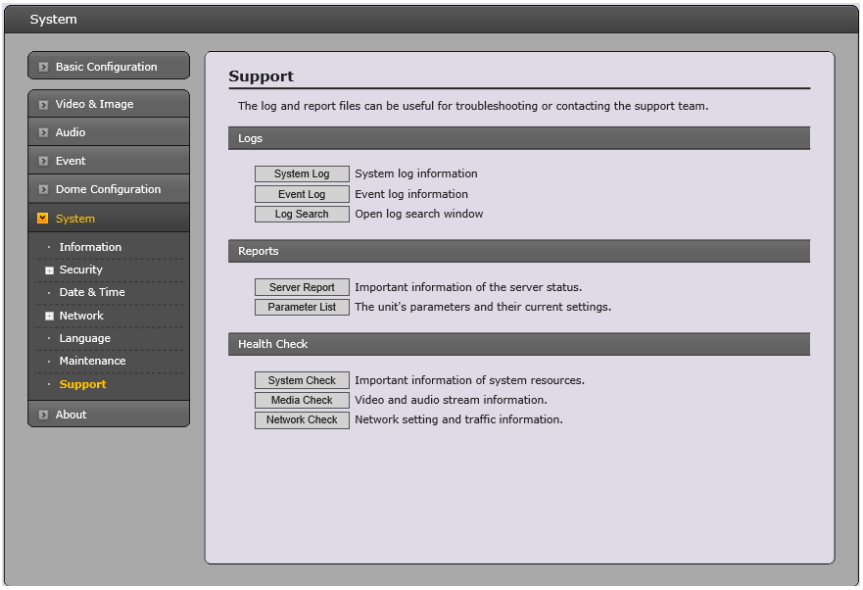
2.4.6. Maintenance



- Maintenance:
  - Restart: The unit is restarted without changing any of the settings. Use this method if the unit is not behaving as expected.
  - Reset: The unit is restarted and most current settings are reset to factory default values. The settings that are not affected are:
    - the boot protocol (DHCP or static)
    - the static IP address
    - the default router
    - the subnet mask
    - the system time
  - Default: The Default button should be used with caution. Pressing this will return all of the network camera's settings to the factory default values (including the IP address).
- Upgrade: Upgrade your camera by importing an upgrade file and pressing the Upgrade button. During the upgrade, do not turn off the power of the network camera. Wait at least five minutes and then try to access the camera again.
- Backup: Save the setting values that users have entered to the network camera to a user PC.
- Restore: Import and apply a setting value previously saved to a user PC.

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

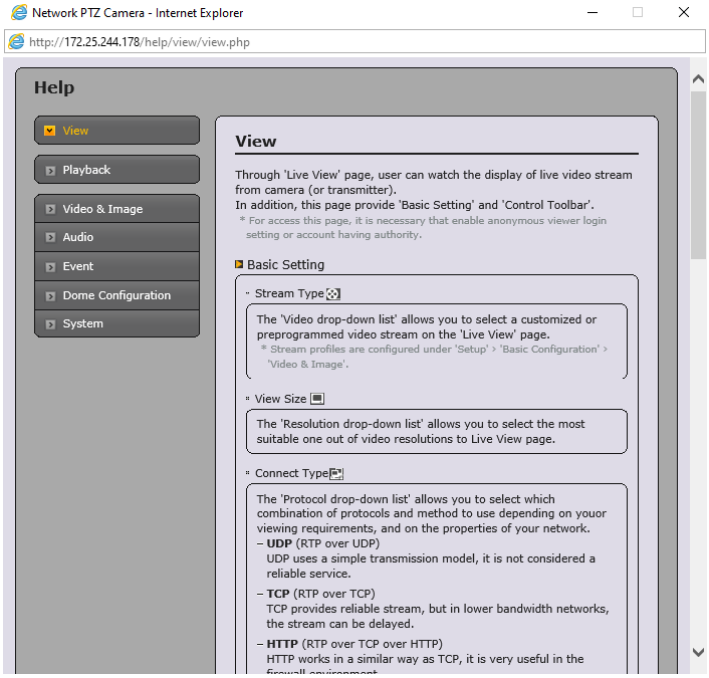
2.4.7. Support



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

- Logs: The network camera supports system and event log information. Click the System Log button to get the system log data or the Event Log button to get information on events.
- Reports:
  - Server Report: Click the Server Report button to get the important information about the server status; this should always be included when requesting support.
  - Parameter List: Click the Parameter List button to see the unit's parameters and their current settings.
- Health Check:
  - System Check: Click the System Check button to get the important information about the cameras system resources.
  - Media Check: Click the Media Check button to get the information about the cameras video and audio stream..
  - Network Check: Click the Network Check button to get the information about the cameras network setting and traffic.

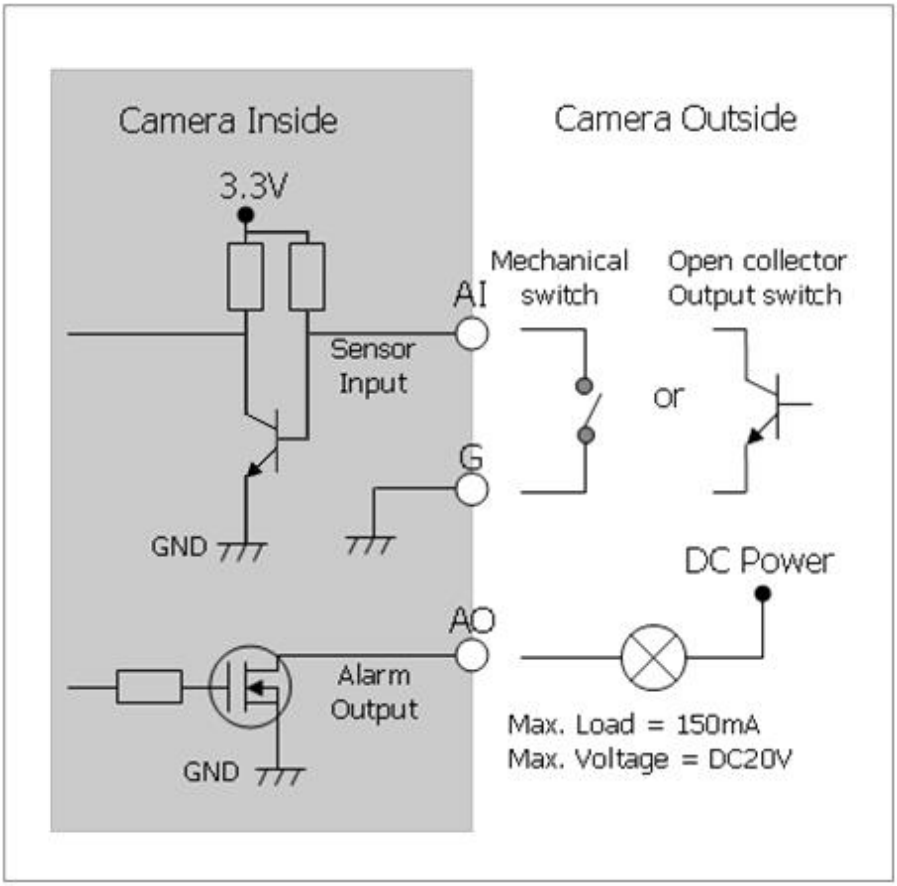
2.5. Help



The Help information window will be provided as a popup window so that users can open and read it without needing to log-in. It will offer a description of the setting and Help page so that users can manipulate the network camera without a reference to the manual.

3. Alarm Connection

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



4. 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.

5. Dimensions