V-Series Encoder Firmware User's Manual

A1D-600-H1.01.08-AC

2014/09/12

ACTi
Connecting Vision

Table of Contents

Recommended PC Specifications

In order to configure or test the devices, a PC with following basic specifications is needed:

CPU	Core 2 Duo 2.13 GHz or above
Memory	2 GB or above
Operating System	● Windows XP with SP2 or above. ● Windows 2003 ● Windows Vista ● Windows 2008 ● Windows 7
Browser for Accessing Firmware	● Internet Explorer 8.0 or newer (full functionality) ● Safari with QuickTime installed (partial functionality) ● Other Browsers with Basic VLC Media Player (partial functionality)
Video Resolution	1024x768 or higher

Preparation

Connect the Equipment

To be able to connect to the device firmware from your PC, both the device and the PC have to be connected to each other via Ethernet cable. At the same time, the device has to have its own power supply. In case of PoE devices, you can use a PoE Injector or a PoE Switch between the device and the PC. The devices that have the DC power connectors may be powered on by using a power adaptor.

The Ethernet port LED or Power LED of the device will indicate that the power supply for the device works normally.

Configure the IP Addresses

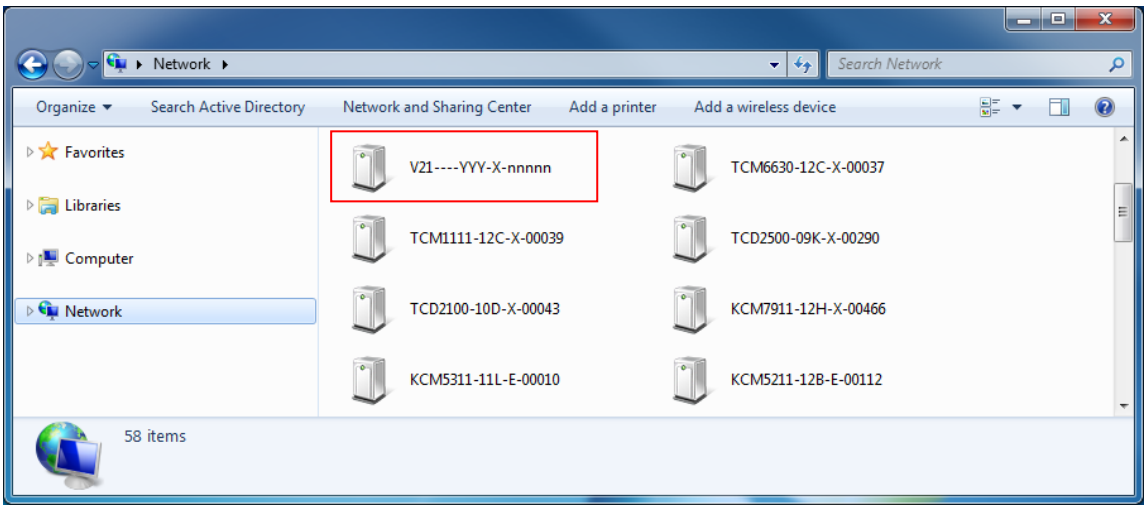
In order to be able to communicate with the device from your PC, both the device and the PC have to be within the same network segment. In most cases, it means that they both should have very similar IP addresses, where only the last number of the IP address is different from each other. There are 2 different approaches to IP Address management in Local Area Networks – by DHCP Server or Manually.

Use the DHCP Server to Assign IP Addresses

If you have connected the computer and the device into the network that has a DHCP server running, then you do not need to configure the IP addresses at all – both the device and the PC would request a unique IP address from DHCP server automatically. In such case, the device will immediately be ready for the access from the PC. The user, however, might not know the IP address of the device yet. It is necessary to know the IP address of the device in other to be able to access it by using a Web browser.

The quickest way to discover the devices in the network is to use the simplest network search, built in the Windows system – just by pressing the "Network" icon, all the devices of the local area network will be discovered by Windows thanks to the UPnP function support of our devices.

In the example below, we successfully found **D11** device that we had just connected to the network.

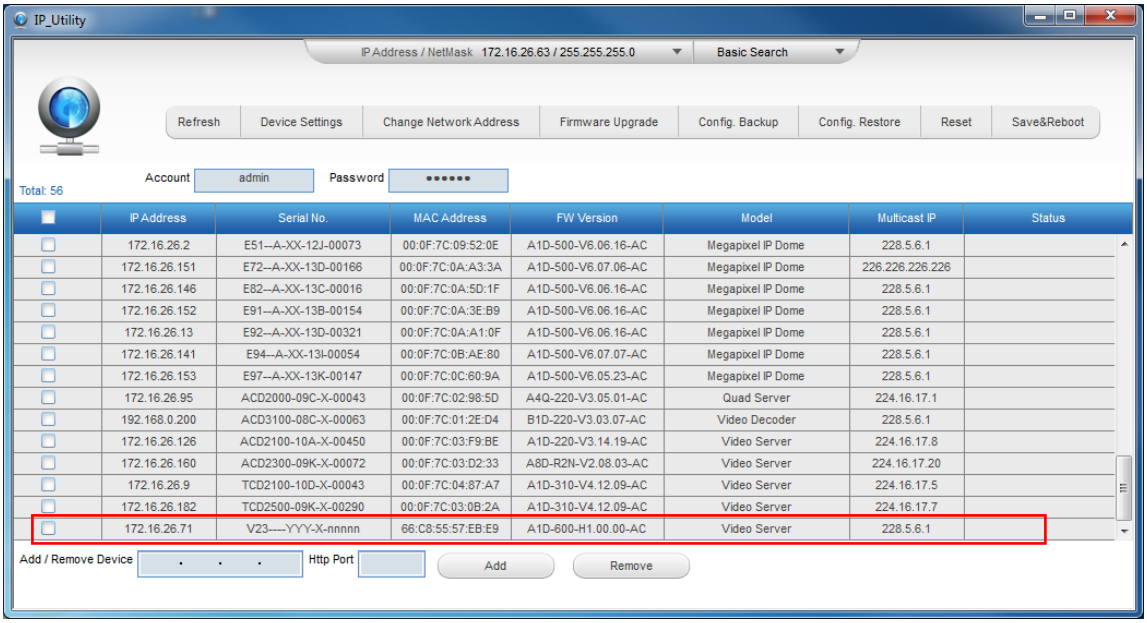


By clicking with the left mouse click on the device model, it is possible to automatically launch the default browser of the PC with the IP address of the target device filled in the address bar of the browser already.

If you work with our devices regularly, then **there is even a better way to discover the devices in the network** – by using **IP Utility**. The IP Utility is a light software tool that can not only discover the devices, but also list lots of valuable information, such as IP and MAC addresses, serial numbers, firmware versions, etc, and allows quick configuration of multiple devices at the same time.

The IP Utility can be downloaded for free from **http://www.acti.com/IP_Utility**

With just one click, you can launch the IP Utility and there will be an instant report as follows:



You can quickly notice the device model in the list. Click on the IP address to automatically launch the default browser of the PC with the IP address of the target device filled in the address bar of the browser already.

Use the Device Default IP Address

If there is no DHCP server in the given network, the user may have to assign the IP addresses to both PC and device manually to make sure they are in the same network segment.

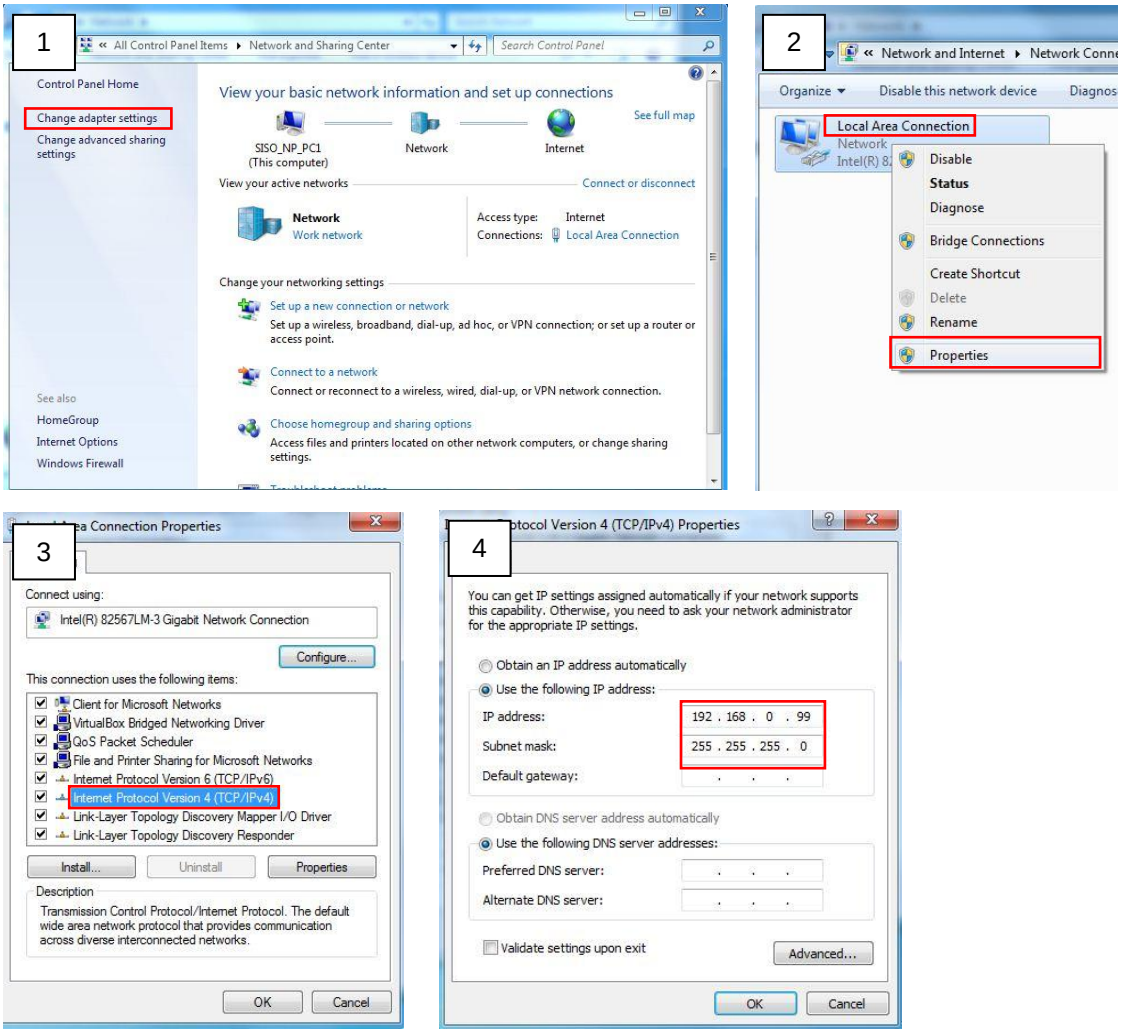
When the device is plugged into network and it does not detect any DHCP services, it will automatically assign itself a default IP:

192.168.0.100

Whereas the default port number would be **80**. In order to access that device, the IP address of the PC has to be configured to match the network segment of the device.

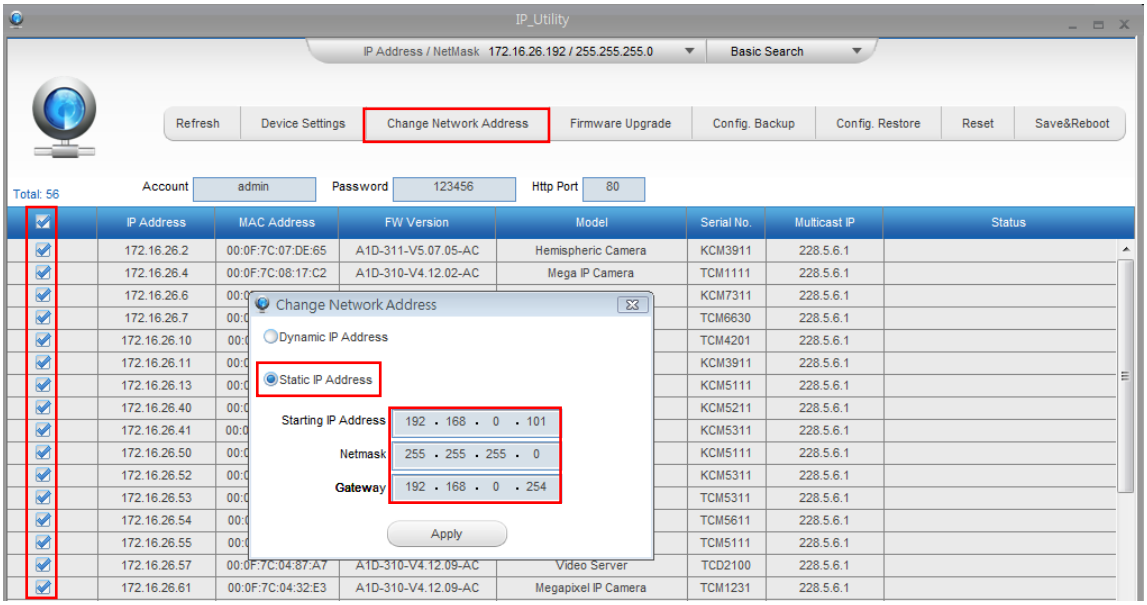
Manually Adjust the IP Address of the PC

In the following example, based on Windows 7, we will configure the IP address to **192.168.0.99** and set Subnet Mask to **255.255.255.0** by using the steps below:



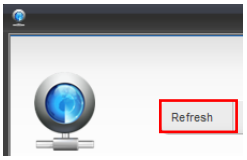
Manually Adjust the IP Addresses of Multiple Device:

If there are more than 1 device to be used in the same local area network and there is no DHCP server to assign unique IP addresses to each of them, all of the devices would then have the initial IP address of **192.168.0.100**, which is not a proper situation for network devices – all the IP addresses have to be different from each other. The easiest way to assign devices the IP addresses is by using **IP Utility**:



With the procedure shown above, all the devices will have unique IP addresses, starting from 192.168.0.101. In case there are 20 devices selected, the last one of the devices would have the IP 192.168.0.120.

Later, by pressing the "Refresh" button of the IP Utility, you will be able to see the list of devices with their new IP addresses.



Please note that it is also possible to change the IP addresses manually by using the Web browser. In such case, please plug in only one device at a time, and change its IP address by using the Web browser before plugging in the next one. This way, the Web browser will not be confused about two devices having the same IP address at the same time.

Access the Device

Now that the device and the PC are both having their unique IP addresses and are under the same network segment, it is possible to use the Web browser of the PC to access the device.

You can use **any of the browsers** to access the device, however, the full functionality is provided only for **Microsoft Internet Explorer**.

The browser functionality comparison:

Functionality	Internet Explorer	Other browsers
Live Video	Yes	Yes*
Live Video Area Resizable	Yes	No
PTZ Control	Yes	Yes
Capture the snapshot	Yes	Yes
Video overlay based configuration (Motion Detection regions, Privacy Mask regions)	Yes	No
All the other configurations	Yes	Yes

* When using non-Internet Explorer browsers, free third-party software plug-ins must be installed to the PC first to be able to get the live video feed from the device:

Browser	Required Plug-In
Safari	QuickTime (http://www.apple.com/quicktime/download/)
Any Other Browser	Basic VLC Media Player (http://www.videolan.org)

Disclaimer Notice: The device manufacturer does not guarantee the compatibility of its devices with QuickTime and VLC – since they are third party softwares; the third party has the right to modify their utility any time which might affect the compatibility. In such cases, please use Internet Explorer browser instead.

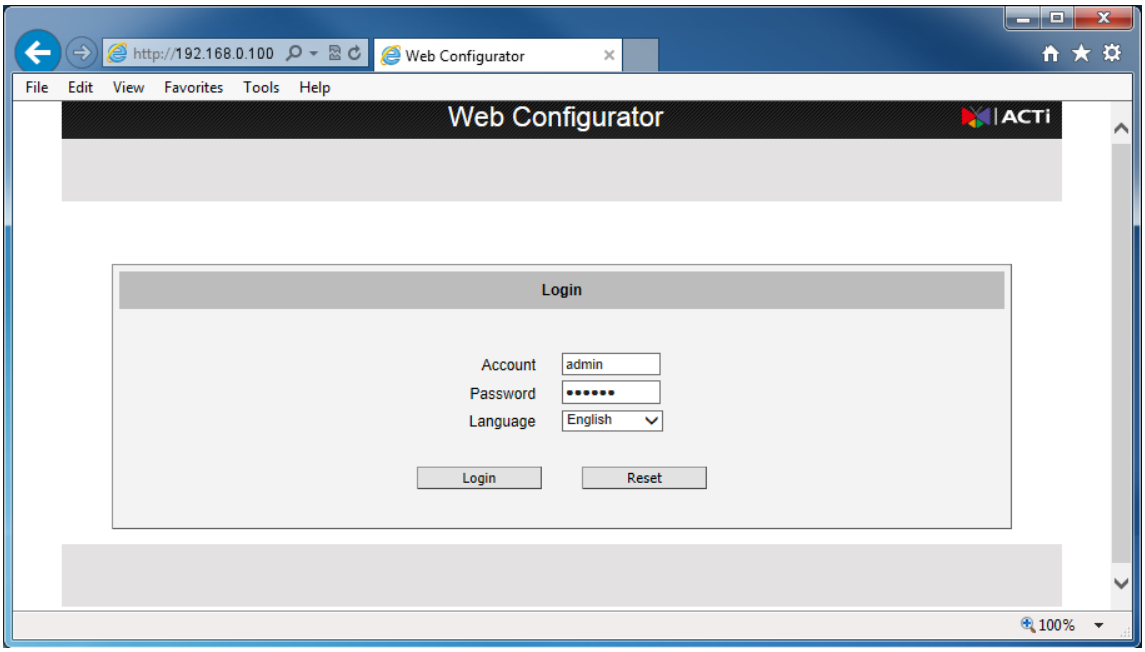
When using Internet Explorer browser, the ActiveX control for video stream management will be downloaded from the device directly – the user just has to accept the use of such control when prompted so. No other third party utilities are required to be installed in such case.

The following examples in this manual are based on Internet Explorer browser in order to cover all functions of the device.

Assuming that the device's IP address is **192.168.0.100**, you can access it by opening the Web browser and typing the following address into Web browser's address bar:

http://192.168.0.100

Upon successful connection to the device, the user interface called **Web Configurator** would appear together with the login page. The HTTP port number was not added behind the IP address since the default HTTP port of the device is 80, which can be omitted from the address for convenience.



Before logging in, you need to know the factory default Account and Password of the device.

Account: **Admin**

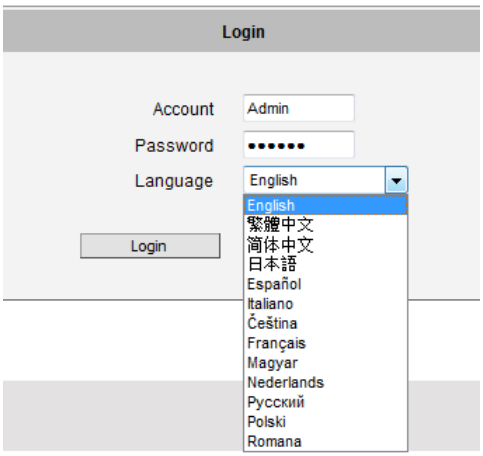
Password: **123456**

Live View

This section describes how to configure the device. The administrator has unlimited access to all settings, while the normal user can only view the live video.

Login

Initially there exists only an administrator's account in the device **(Account: Admin, Password: 123456)** – you have to use that account to log in. You can later create normal user accounts with limited access rights, if necessary.



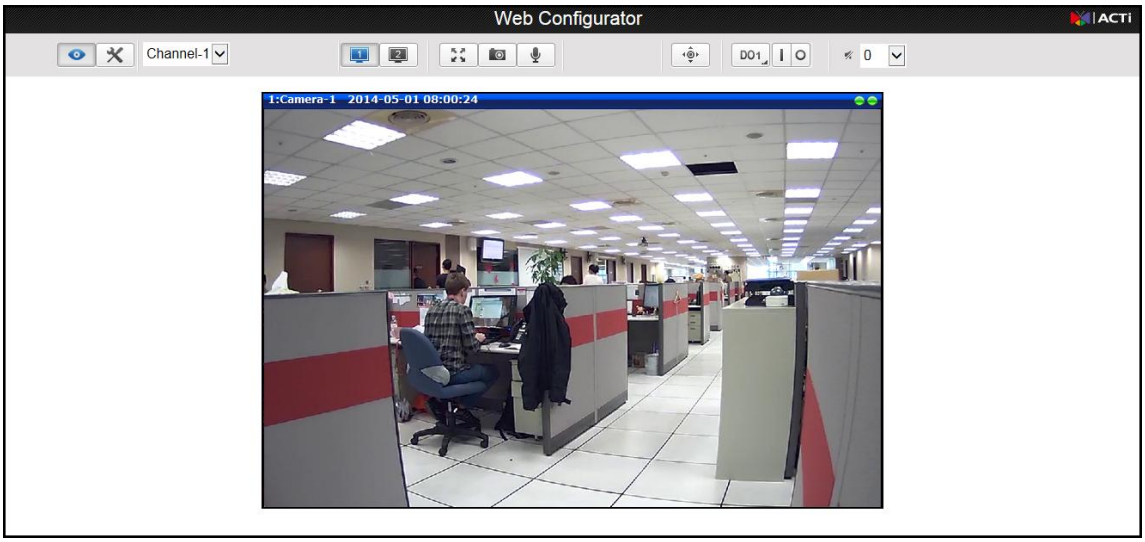
Feel free to choose your local language from the list of languages or keep it as English. After pressing "Login", you will be able to access the user interface of Web Configurator.

Upon successful login, you will be able to see the Live View page. In case of **Internet Explorer browser**, you may be prompted to allow the installation of ActiveX control from the device. Click "Install" then. The live video will appear shortly after that.

Live View

The live view appears automatically. While on the Live View page, the Live View icon  appears as being pressed:

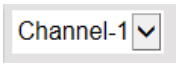
If you leave the Live View page, you can later return by pressing that button.



The buttons shown on the Live View page vary depending on the functions supported by the device.

Video Channel Selection (for Multi-Channel models only)

For encoder models with more than one (1) channel video, you can select the channel to display on the Live View page by selecting the channel number from the channel list.



- Select the channel number

Dual Stream Capability

The devices have the **dual stream** capability – the **Stream 1** is usually the high resolution stream with the purpose of being recorded by NVR while **Stream 2** has lighter video configuration for NVR live view purposes, to reduce the computing power of the NVR PC. Both streams can be configured under Web Configurator's Setup page. To see how each of the stream looks like, there are quick buttons on the Live View page:

- Show the Stream 1 video

- Show the Stream 2 video

Full Screen Mode

You can also digitally re-scale the video to fully match the size of your display with just one click:

 **- Full screen Mode**

You may use **ESC** key from the keyboard to exit the full screen mode.

Take Snapshot

To capture the snapshots of the current live view, click the snapshot button. The snapshots are saved in Pictures folder.

 **- Take a Snapshot**

Audio Recording

Devices with audio out function have the audio controls on Live View page.

 - **Speak to Device**

To speak to the device, click the  button. If the device is connected to a network video recorder, the audio will be recorded with the video stream. If an audio out device, such as a speaker, is connected to the encoder, the audio will be heard through the speaker.

Digital Input / Output Controls

The digital output controls appear on the Live View page of the devices with digital input/output function. The controls allow users to manually trigger a DO device.

- Select DO Port

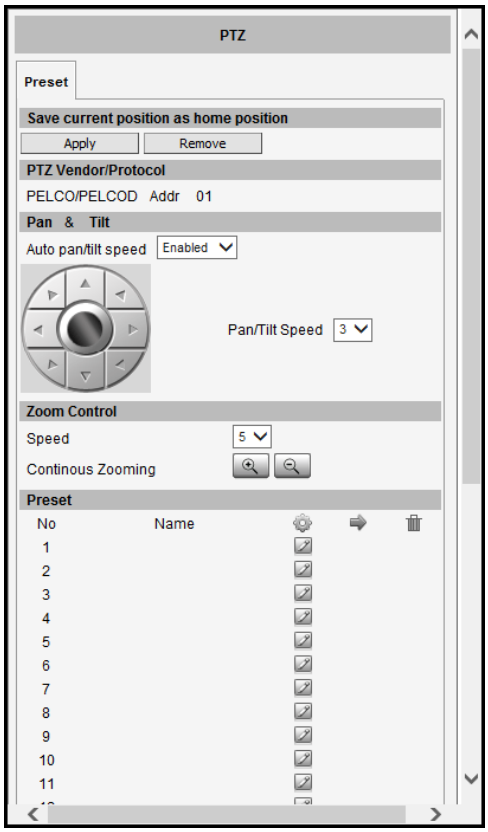
Each DO ports are controlled separately. For devices with more than one DO ports, select the DO port and click  to set the output power level to high or  to set the output power level to low. Consequently, setting the port to a high power level "activates" the DO device and setting the

port to a low power level "deactivates" the DO device. For example, if an alarm is set as DO1 and  is pressed, the alarm will continuously sound until  is pressed to deactivate the device.

PTZ Control Panel (for V2x Models only)

The PTZ Control Panel is used only on connected cameras with PTZ capabilities. The PTZ button  is displayed on the Live View screen only when the channel serial port is enabled on the **Host** menu (see ***Serial Setting*** on page 21). Click the PTZ button on the Live View screen to display the PTZ Control Panel. On the PTZ Control Panel, users can do any the following:

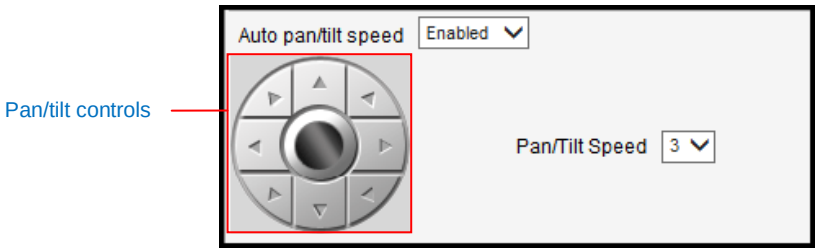
- Set the home position
- View the PTZ Vendor/Protocol (this configuration can be set in ***Serial Setting*** on page 21.
- Pan the device
- Zoom the device in or out as well as adjust the zoom speed and step size
- Set the focus to auto refocus or manual
- Set Preset points



NOTE: The PTZ Control Panel may differ depending on device model.

How to Use Pan/Tilt

Click the pan/tilt controls to pan/tilt the PTZ device.



Other pan/tilt features include:

- **Auto pan/tilt speed**: When "Enabled", the device automatically sets the pan/tilt speed according to the zoom ratio and the selected pan/tilt speed while retaining the clarity and quality of image even as the device is panning or tilting. When "Disabled", the pan/tilt speed follows the value selected on the **Pan/Tilt Speed** field.
- **Pan/Tilt Speed**: Select the desired pan/tilt speed. The bigger the number, the faster the speed is.

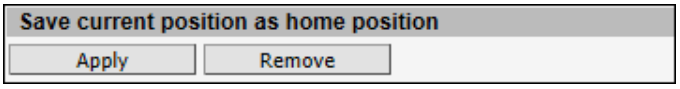
TIP: While the PTZ Control Panel is open, instead of using the pan/tilt controls, move the mouse cursor over the Live View, the mouse cursor will turn into zoom in/out or directional icons (e.g. / / / / etc.). Click or drag the mouse to zoom in/out or pan/tilt the device view.

How to Zoom the Device In or Out

To zoom continuously, do the following:

1. On **Zoom Control**, select the **Speed**, wherein the bigger the number, the faster is the zooming speed.
2. Click and hold the left mouse button on zoom in or zoom out . When the mouse button is released, zooming stops.

How to Set the Home Position



1. Pan, tilt, and zoom on the area that you want to set as the home position.
2. Click the **Apply** button on the **Save current position as home position**.

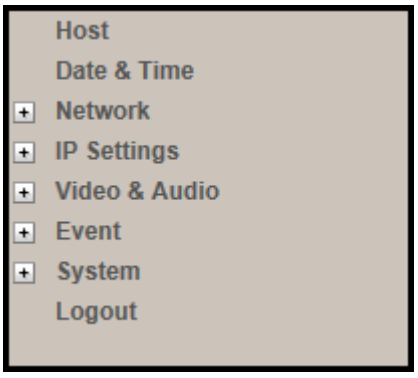
Setup

The following chapters guide you through the Setup functions of the device.

Access the Setup Page

To configure any of the device settings, go to the Setup menu by pressing the following button on Live View page:

 **- Go to Setup**



The left side of the Setup page contains the list of Setup items.

NOTE: *The exact content of the menu list varies for each device, depending on the actual capabilities of each device. This manual, however, is designed to explain all the possible functions.*

Several items in the Setup page are divided into groups, such as Network, IP Settings, etc. You can expand the groups to see the sub-items by pressing the [+] button.

The following chapters of this manual explain each Setup item separately. The chapters are listed in the same order as the list of Setup menu items.

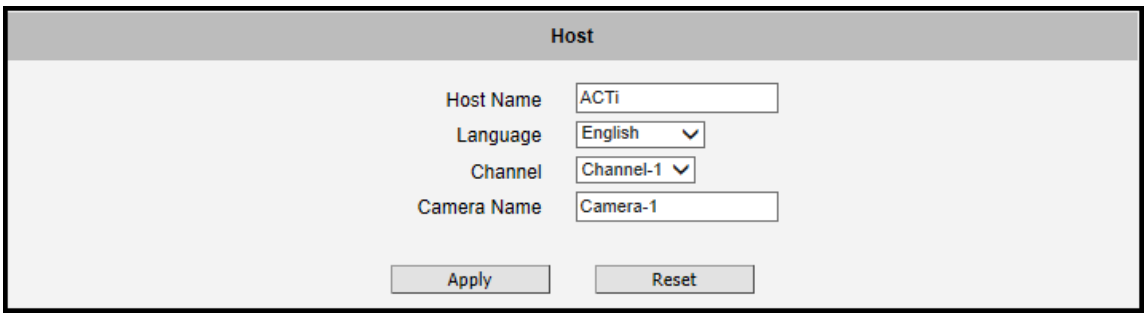
Host

Host

The **Host** menu allows is divided into three (3) sections: **Host**, **Serial Setting**, and **Video Channel's PTZ Address**.

Host

The **Host** section allows the user to define the name of the device, preferred user interface language and set the name of a video channel.



Host Name: It is used to identify the device by a DHCP server. In some networks with very strict security policy, it is required that all the network devices should have their host name, and when the devices attempt to access the network by requesting an IP address from a DHCP server, the DHCP server would check if the host name is among the allowed devices. On this page, it is possible to edit the Host Name. To actually include the Host Name in DHCP discovery packet sent from a device, please go to **IP Settings** and make sure the device is in **Dynamic IP Address** mode and "Use host name" is checked.

Language: This item allows users to select the user interface language, same function as that of the **Language** item on the Login page of the Web Configurator.

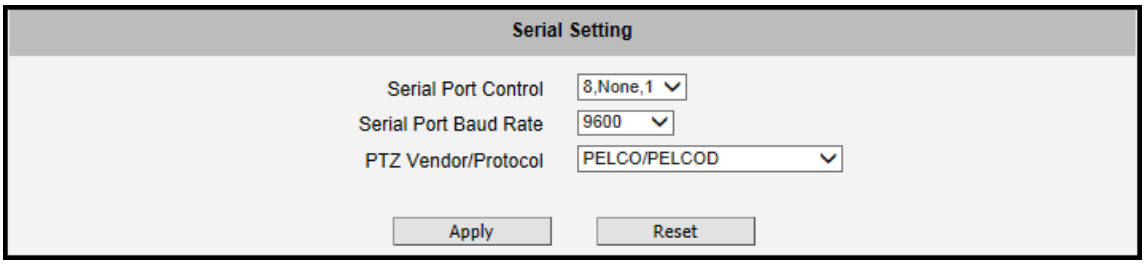
Channel (not available in 1-channel models): It is used select the video channel. This item is used with **Camera Name**; where once a channel is selected, users can define its name.

Camera Name: This item is used to identify the camera in a **Video Management System** (VMS) or by **Software Tools**. Usually, upon installation of the camera, the actual installation location is used as an easy-to-remember camera name, such as "Front Gate" or "Elevator 1". In many cases the VMS is able to modify the camera name directly via its own user interface without needing to access Web Configurator.

After changing any of the items above, click **Apply** to save the changes. The Reset button undoes the changes that had just been made but not applied yet.

Serial Setting

The **Serial Setting** section allows the user to set the serial port configurations of the encoder to synchronize it with the serial port configurations of the PT device. For multi-channel encoders, since all video channels will share one serial port, the serial port configurations on all the connected devices must have the same serial port configurations.



Serial Port Control: Select the serial port control that matches with the serial port configured on the PT device. This function is equivalent to the DIP switch of the PT device.

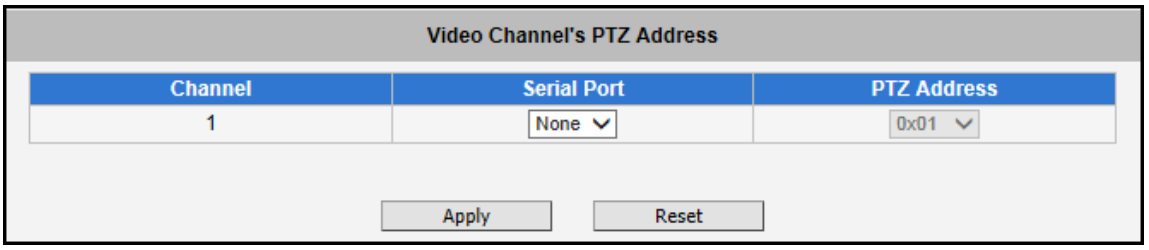
Seral Port Baud Rate: Select the serial port baud rate that matches with the baud rate set on the PT device.

PTZ Vendor/Protocol: ACTi devices and video management systems fully support the URL Command, a high level PT command set. However, in case the devices will be used with devices from third party vendors that only support Serial Hex Command (low level PT command set), users must select the **PTZ Vendor/Protocol** to use. Otherwise, leave the default settings.

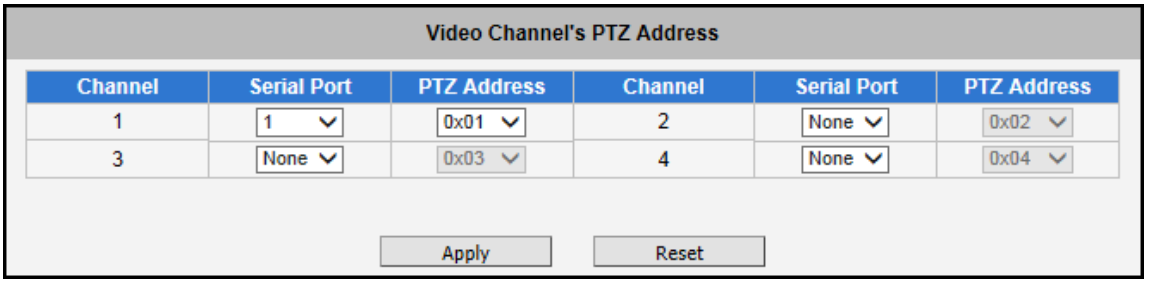
After changing any of the items above, click **Apply** to save the changes. The **Reset** button undoes the changes that had just been made but not applied yet.

Video Channel's PTZ Address

The **Video Channel's PTZ Address** section allows the user to enable the serial port and assign the PTZ address of a video channel. For multi-channel encoders, all video channels share one (1) serial port therefore the address for each channel must be defined on this section.



1-Channel Encoder Example



4-Channel Encoder Example

After changing any of the items above, click **Apply** to save the changes. The **Reset** button undoes the changes that had just been made but not applied yet.

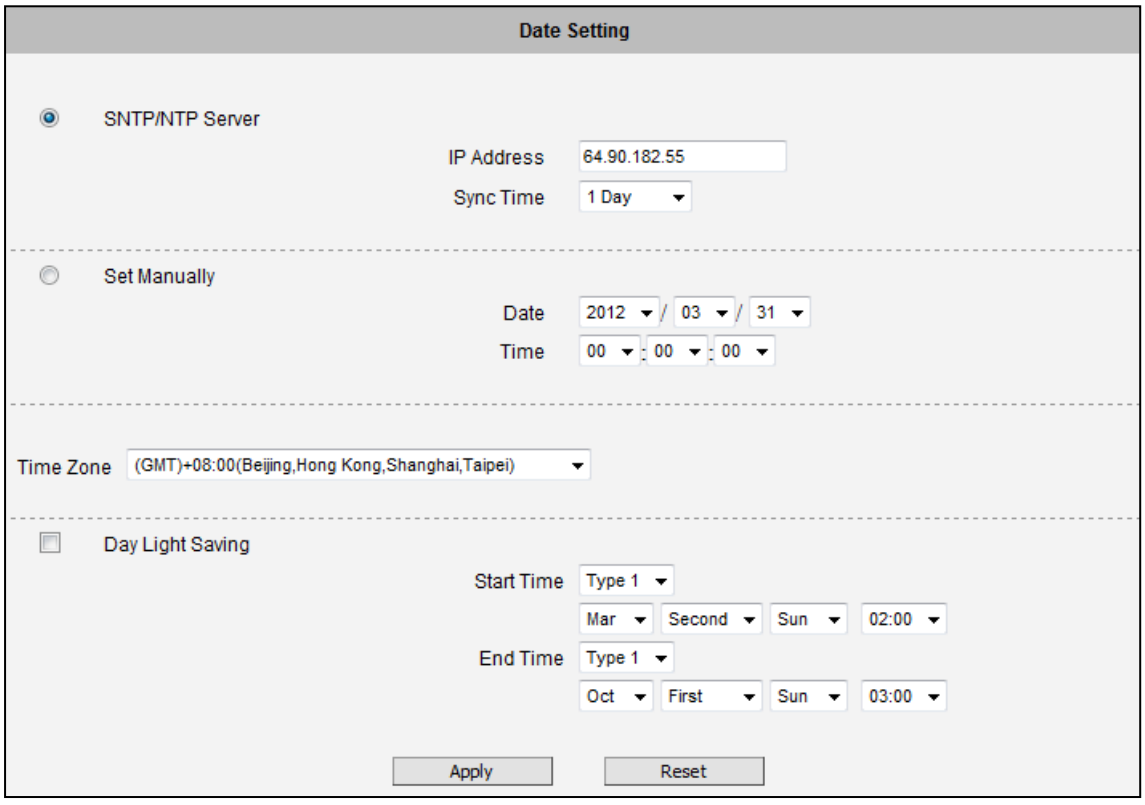
Date & Time

Each video frame contains a time stamp. The accuracy of the time stamp is very important for incident investigators. Therefore the clock of the device has to be adjusted to most accurate time possible.

Date & Time

The **Date & Time** menu provides the options for adjusting the date and time of the device.

There are two ways to adjust the date and time – **automatically** by getting date and time regularly from any of the **NTP servers** worldwide, or **manually** by selecting proper time zone, date and time. The automatic way can be used only if the device has an access to NTP servers. If you are using an isolated Local Area Network without Internet access, you can only use Manual date and time adjustment mode.



When choosing **SNTP/NTP Server** for automatic date and time updating, you can key in the IP address of the NTP server and the time interval for automatic time synchronization. If you want to key in the domain name of NTP server instead, please make sure the DNS server IP address has been set under IP Settings; otherwise the device will not be able to resolve the domain name of the NTP server.

If all the devices are getting the date and time from the same NTP Server, you can be most sure that the video clips from different devices can be well synchronized later for comparison purposes.

To choose the most suitable NTP Server to synchronize date and time with, please refer to the worldwide pool of NTP Servers: http://www.pool.ntp.org/en/

When choosing **Set Manually** mode, you can adjust the date and time by the select boxes. Choose the appropriate **Time Zone** from the select box, too. If your location is not listed there, then pick any of the listed zones which GMT is identical with your location.

For the countries with daylight saving policy, there is **Day Light Saving** function with two different types:

- **Type 1**: Defines the starting or ending time of daylight saving period by the **number of the week in the month** (First, Second, Third or Last week).
- **Type 2**: Defines the starting or ending time of daylight saving period by the **exact date in the month** (1-31).

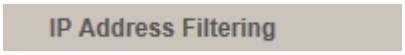
Whether to choose Type 1 or Type 2, please refer to the daylight saving policy of given country.

After changing any of the items above, click **Apply** to save the changes. The **Reset** button undoes the changes that had just been made but not applied yet.

Network

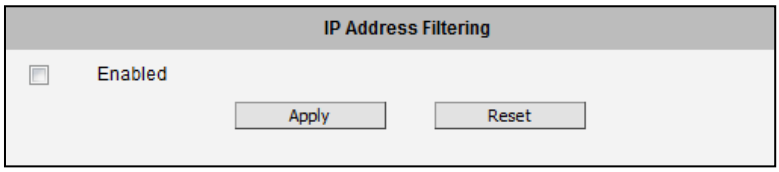
The **Network** menu provides the list of network related functions and services. The [+] mark before Network indicates that the list can be expanded by clicking on it. Once expanded, the list can later be collapsed again by clicking on the [-] mark.

IP Address Filtering

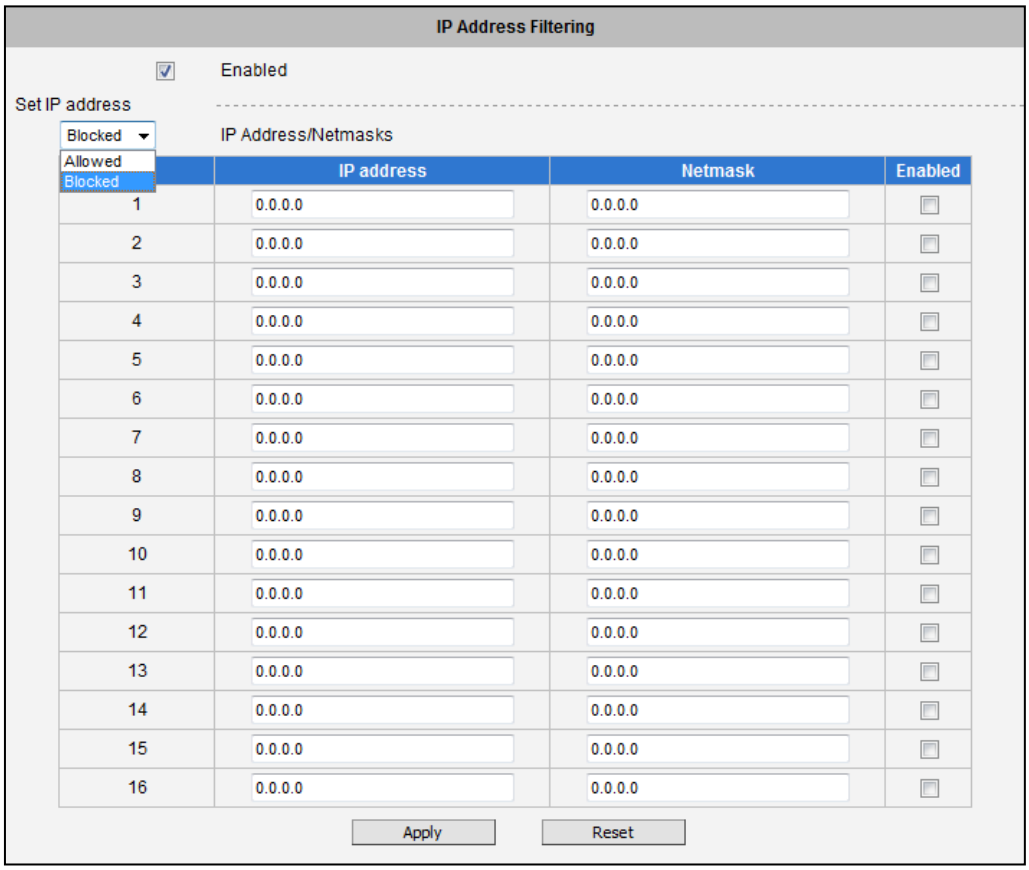


Use the **IP Address Filtering** submenu to define which devices (using the IP addresses) are allowed to connect to this device, and which devices are forbidden to connect to this device.

Check the box **Enabled** to activate the IP address filtering function and click **Apply**.



Below you can select either **Allowed** or **Blocked** list to add items there and **Enable** them with the checkbox behind each row.



Allowed mode will refuse access to all IP addresses except the ones listed below.
Blocked mode will accept all incoming access except the IP addresses listed below.

Using **Netmask** (Subnet Mask) allows you to set filtering for a whole range of IP address at once, without the need to enter all of them individually. If you are not sure about the function of Netmask, then you should use 255.255.255.255, and it will affect only a single IP address per line of entry, or use 255.255.255.0 to use the same setting for all IP addresses starting with the same three numbers. .

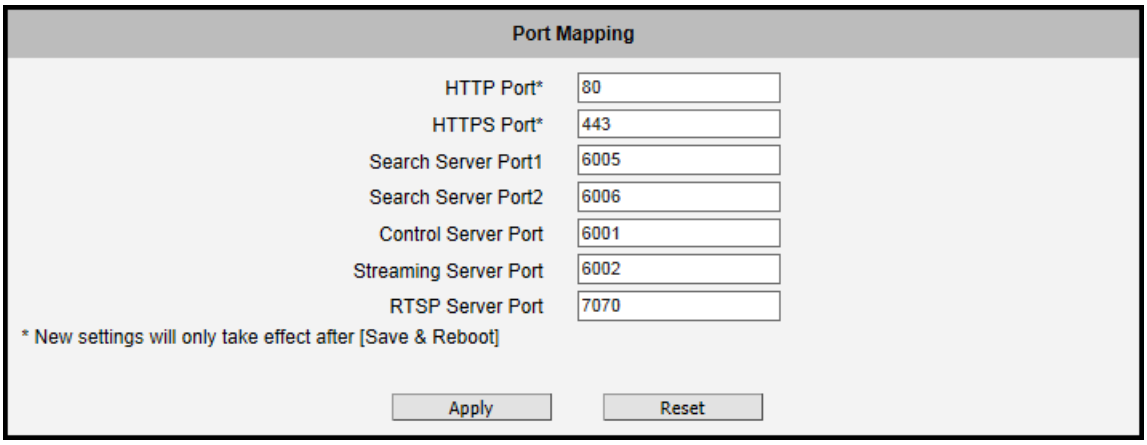
After changing any of the items above, click **Apply** to save the changes. The **Reset** button undoes the changes that had just been made but not applied yet.

Warning! Do not accidentally block your own IP address that you are connecting from; otherwise you will not be able to access the device any more to undo the changes. If this happens by mistake, you can do the hardware reset – it will clear all the filtering rules.

Port Mapping

Port Mapping

The **Port Mapping** submenu provides the list of services and protocols that require their own port number for communication. By default, the device already has all the ports defined. On this page, the user can modify the port numbers in case there is a specific need for that. Most often, the HTTP port is changed to something other than 80 in order to match with easy-to-remember port forwarding rules of the router that acts as a bridge between local area network and Internet.



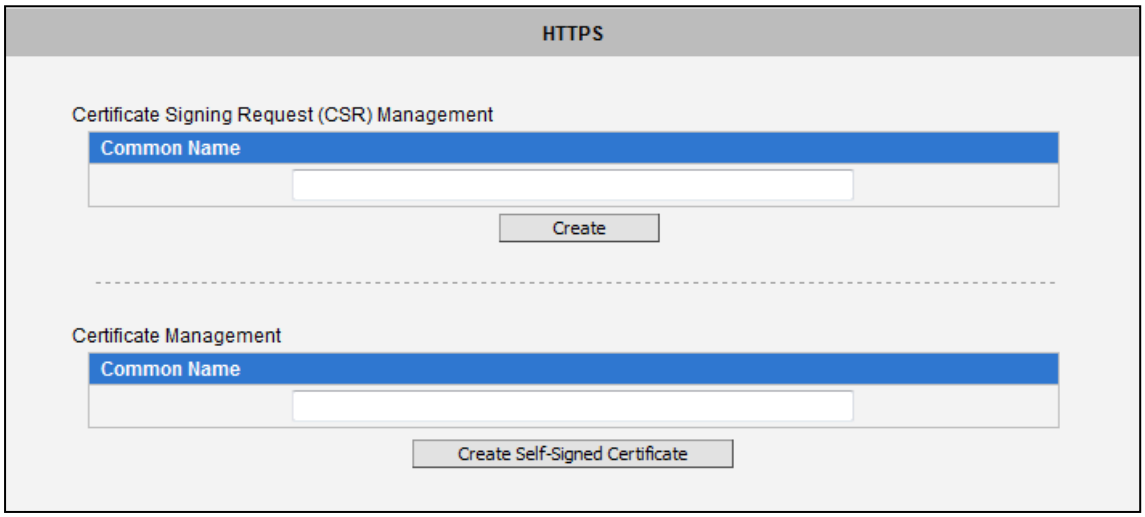
NOTE: Some items appear only if the device model supports the function.

Parameters	Description
HTTP port	Select the port assigned for HTTP protocol access.
HTTPS Port	Select the port assigned for HTTPS protocol access.
Search Server Port1	Select the first port used by server search applications to detect this IP device (e.g. IP Utility).
Search Server Port2	Select the second port used by server search applications to detect this IP device (e.g. IP Utility).
Control Server Port	Select the port used to support video control function by application programs (e.g. NVR).
Streaming Server Port	Select the port used by this IP device for Video Streaming (TCP).
RTSP Server Port	Select the port assigned for RTSP protocol access.

After changing any of the items above, click **Apply** to save the changes. The **Reset** button undoes the changes that had just been made but not applied yet. New port settings will only take effect after clicking **System > Save & Reboot**.

HTTPS

HTTPS protocol allows creating a secure channel over an insecure network in order to protect the data sent between the device and its counterpart. Two things are required to have a secure communication – encrypted data, and verified counterpart of the communication. To make sure that the messages are being sent and received from true counterpart, the certificate is needed.



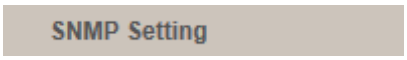
There are two methods to create certificates – **Certificate Signing Request (CSR)** and **Self-Signed Certificate**.

- **Certificate Signing Request (CSR)**: User uses a signed certificate issued by trusted Certification Authority (CA).
- **Self-Signed Certificate**: User wants to use the certificate created and issued by user himself.

Click **Create** or **Create Self-Signed Certificate** button and configure settings in the pop-up screen to install the certificate.

Note that the new setting will only take effect after **Save & Reboot**.

SNMP Setting

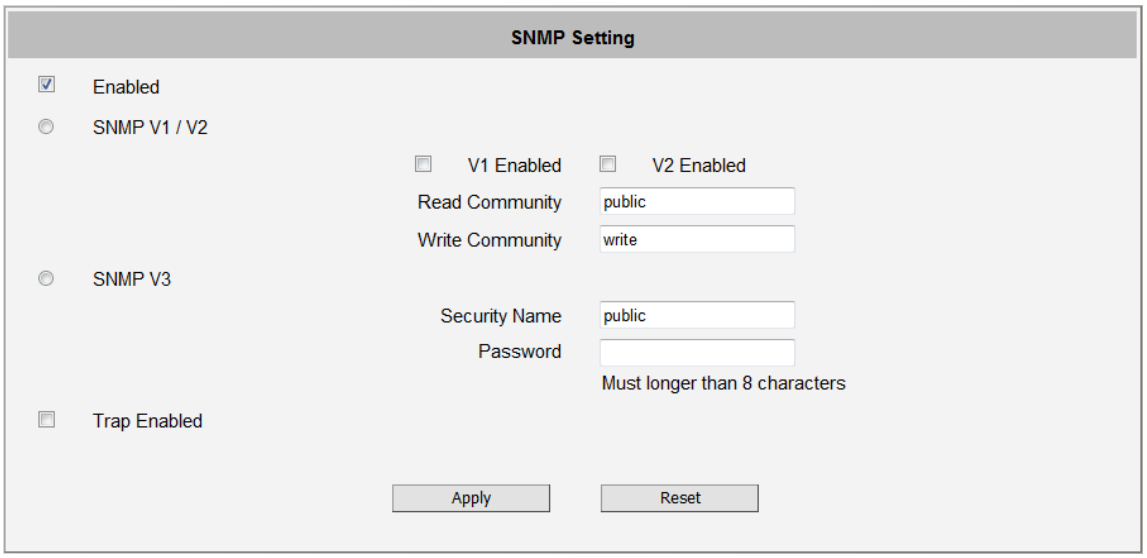


The **SNMP Setting** submenu displays the SNMP configuration page.

SNMP provides an easy way to manage network devices. The main features are:

1. Monitoring device uptime
2. System detail description. (Ex: model name, model description and firmware version.)
3. Collect interface information. (Ex: MAC address, interface speed, local port.)
4. Measuring network interface throughput.

To use SNMP, just **enable** SNMP function in the device (SNMP agents) and run SNMP management software in server (NMS: Network Management Station) to connect to the devices.



The SNMP agent supports versions V1, V2 and V3. SNMP V1 is the initial implementation of SNMP. SNMP V2 is proposed to enhance the performance of management, such as the communication of server and devices, the confirmation of information delivery and receipt. Primary additions in SNMP V3 concern security and remote configuration enhancements.

SNMP V1/V2 uses the "Community" name as password to authenticate identity. "Read Community" is the password for server to get information from devices. "Write Community" is the password for server to edit values on devices. The default is "public" for Read Community and "write" for Write Community. Of course, you can set any other password as your read/write community.

You can enable V1, V2 or both. Click **Apply** after setup is complete.

SNMP V3 uses account/password for authentication. "Security Name" is the account name to be used with your "Password". The default security name is "public" and the password must be at least 8 characters long. You also can set any other security name or password.

Click "**Apply**" after setup is complete.

SNMP function is now enabled. You may now install and run the SNMP management software on the computer server.

SNMP Trap Usage:

SNMP traps enable notifications from devices. Devices may send message to the management server whenever significant events occur such as cold start, warm start and authentication failure. The manager will get the information immediately and take action if necessary.

Cold start means device reboot by power disconnection. **Warm start** means device reboot by firmware without power disconnection. If there other parties attempt to connect to the device with wrong security password under SNMP V1, V2 or V3 setting, the device will send an **authentication failure** message to the management server.

To enable SNMP Trap function in the device, type the IP address of the computer running the SNMP management software and type trap community as password to allow server to get trap message from device (Default is public). Select available traps and click "**Apply**".

Device's SNMP offers following information:

Group	Description
System	Provide general information about the managed device. *Ex: system description, system name.*
Interface	Provide general information from the physical interfaces. *Ex: interface speed, MAC address.*
Address Translation	Provide information about the mapping between network addresses and physical addresses for each physical interface *Ex: The IP/MAC addresses to connect to the managed device.*

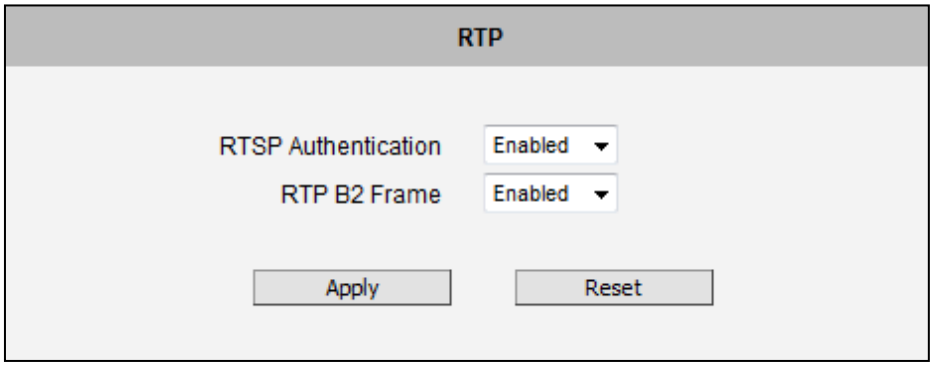
IP	Provide the status and operation of Network Layer (Layer 3). *Ex: the information and traffic flow of received/delivered package.*
ICMP	Provide the status and statistics of ICMP. *Ex: amount of receive/error message of ICMP.*
TCP	Provide the status and operation of Transport Layer (Layer 4) using TCP protocol. *Ex: TCP Local Port, incoming/outgoing TCP segments.*
UDP	Provide the status and operation of Transport Layer (Layer 4) using UDP protocol. *Ex: UDP Local Port, in/out datagram.*
SNMP	Provide the related statistics through SNMP

RTP

RTP The **RTP** submenu allows the user to configure RTP Settings.

If the **RTSP Authentication** is **Enabled**, then the RTP streaming will require account name and password authentication.

If the **RTP B2 Frame** is **Enabled** then the B2 frame is added to every video frame, containing additional information, such as **motion detection status on each frame, digital input and digital output levels, passive infrared status, other video intelligence data, frame counter, frame-rate mode and the frame-rate, bitrate, resolution, timestamp and much more**. The user side can operate with video data easily, including event management, storage consumption estimation, image resizing for preview, etc.



After changing any of the items above, click **Apply** to save the changes. The **Reset** button undoes the changes that had just been made but not applied yet.

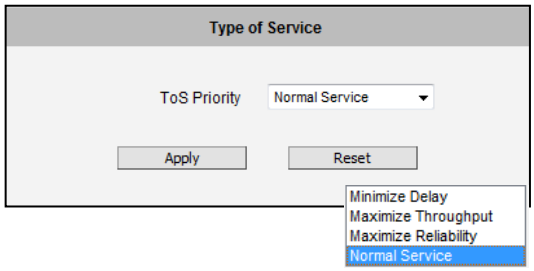
Network (ToS, UPnP, Bonjour)

The **Network** menu vcontains the controls for following functions:

- Type of Service
- UPnP
- Bonjour

Type of Service

The **Type of Service** provides four (4) options to define the priorities of how the data from the device should be handled by the routers that support ToS concept. By the default, the ToS priority is set as **Normal Service**.



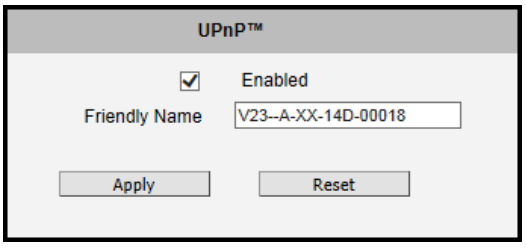
For special priority arrangement, there are three (3) more options:

- Minimize Delay
- Maximize Throughput
- Maximize Reliability

After changing any of the items above, click **Apply** to save the changes. The **Reset** button undoes the changes that had just been made but not applied yet.

UPnP™

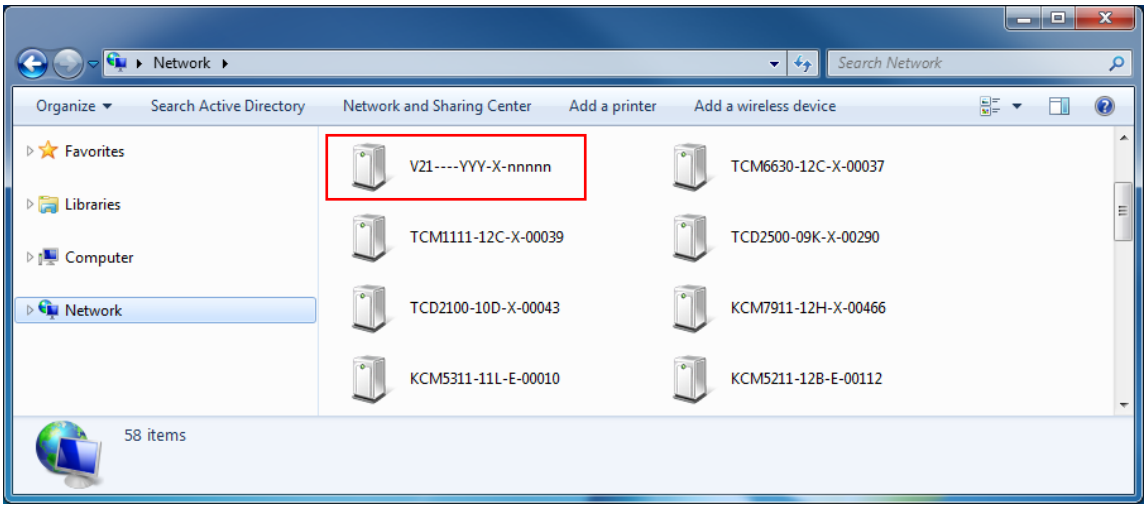
The **UPnP™** section provides the option to enable or disable the Universal Plug and Play capability of the device. Having the UPnP™ enabled allows the other network devices to seamlessly discover it on the network for convenient identification and access.



The **Friendly Name** is a human-readable name for the device that will be displayed when the device is found. By default, the serial number of the device is used as a friendly name; however, the user can modify the name according to the project needs.

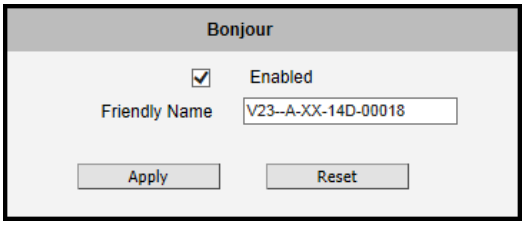
After changing any of the items above, click **Apply** to save the changes. The **Reset** button undoes the changes that had just been made but not applied yet.

Most of the Windows-based computers have the capability to discover the devices that support UPnP™. Below is the example of Windows 7: by clicking on the **Network** icon of **Windows 7**, the PC will discover the devices instantly.



Bonjour

The **Bonjour** section provides the option to enable or disable the ability of the device to be discovered by the other network devices using Bonjour protocol, developed by Apple Inc. Both Bonjour and UPnP serve the similar purpose – to discover devices conveniently.



Similarly to UPnP, the human readable **Friendly Name** can be defined by the user. That name will be displayed when the device is found in the network. By default, the Friendly Name is the serial number of the device; however, the user can modify the name according to the project needs.

After changing any of the items above, click **Apply** to save the changes. The **Reset** button undoes the changes that had just been made but not applied yet.

IP Settings

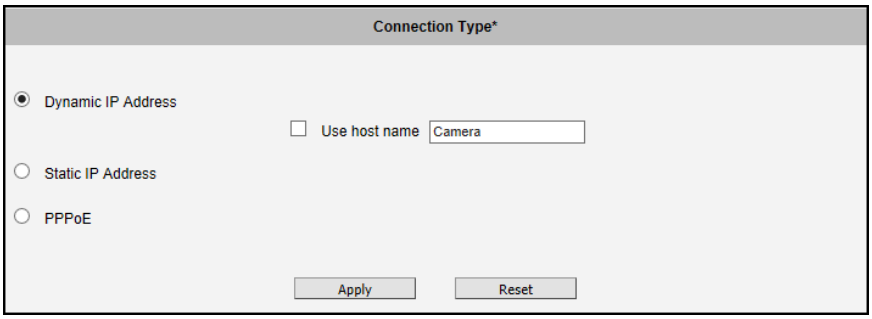
IP Settings

The **IP Settings** menu provides the options to define how the device would obtain its IP address; and to which DNS server should the device connect to, in order to resolve domain names.

Connection Type

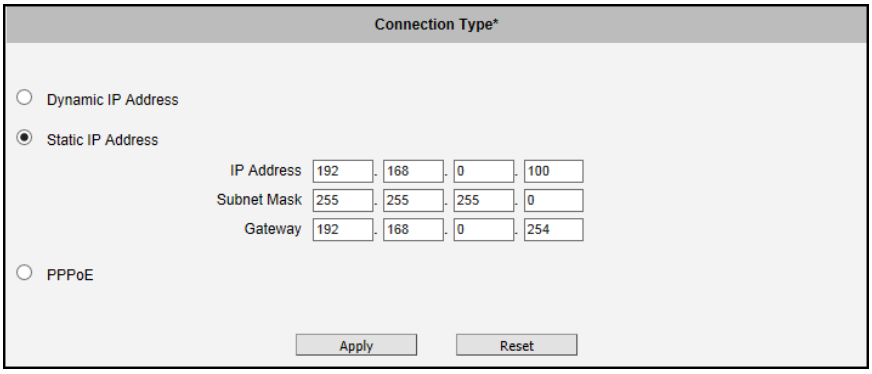
Connection Type

The **Connection Type** submenu allows defining the method of obtaining the IP address of the device. By default, the device is in **Dynamic IP Address** mode and attempts to get the IP address from a DHCP server. If such attempt fails after several seconds (for example the DHCP server does not exist), the device will automatically assign itself an IP address, listed under Static IP Address.

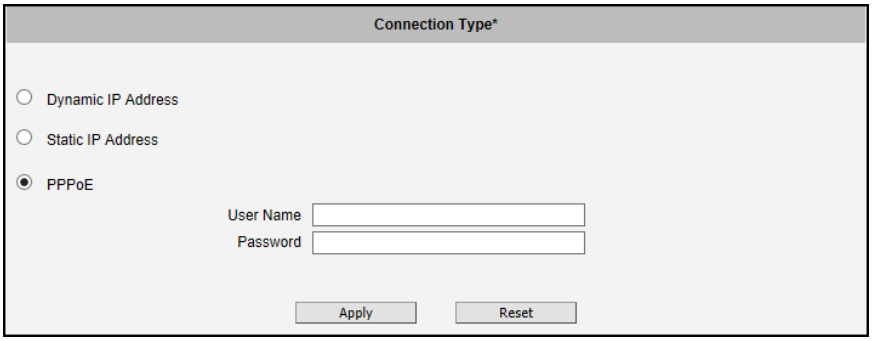


Host Name is used to identify the device by a DHCP server. In some networks with very strict security policy, it is required that all the network devices should have their host name, and when the devices attempt to access the network by requesting an IP address from a DHCP server, the DHCP server would check if the host name is among the allowed devices. On this page, it is possible to edit the Host Name and enable or disable the use of host name.

Most installation projects include clear network topology and static IP addresses for each device. In such cases, you can change the device to **Static IP Address** mode and modify the **IP Address, Subnet Mask** and **Gateway** accordingly.



In some rare cases, the device may be connected to the control center over Internet. Usually, the most cost efficient way is to use ADSL connection with **PPPoE**. To avoid the unexpected changes of IP addresses by Internet Service Provider upon the restart of the device, it is recommended to activate a DDNS service for such scenario, and let the control center connect to the device by the domain name instead. Please refer to the DDNS section for more details.



To set the device in PPPoE mode, set the button to **PPPoE** and key in the **User Name** and **Password**, provided by Internet Service Provider.

After changing any of the items above, click **Apply** to save the changes. The **Reset** button undoes the changes that had just been made but not applied yet.

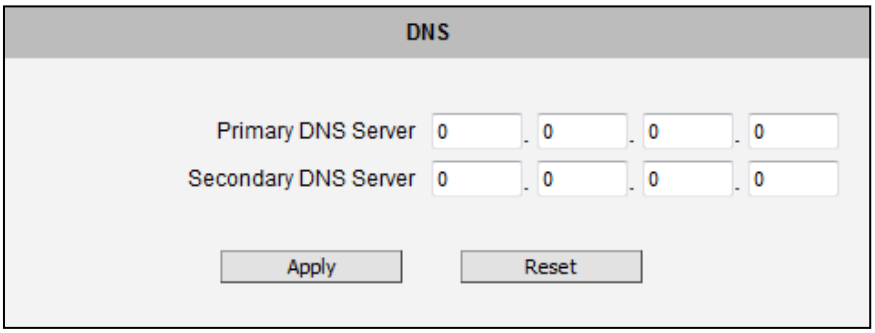
The new IP address settings will only take effect after clicking **System -> Save & Reboot**.

DNS

The **DNS** submenu allows setting up the Domain Name Service for the device. The device will connect to the DNS server when there is a need to resolve a domain name for sending data to.

The most common usage is the ftp or e-mail server in the Event Handler section is defined by using domain names. Without having DNS service configured, the device would not know how to resolve the domain names of FTP or e-mail servers.

It is possible to configure both **Primary** and **Secondary DNS servers**. The Secondary DNS Server will be used when the connection to the Primary DNS Server fails.



After changing any of the items above, click **Apply** to save the changes. The **Reset** button undoes the changes that had just been made but not applied yet.

Video & Audio

The **Video & Audio** menu provides the options to adjust the video quality, configure the streaming details of the device, and audio settings, which will be described in the succeeding pages.

The default settings of the device are sufficient for most environments and the video adjustments are not necessary. The following sections explain the ways to configure the video quality or streaming details in case it is required to do so.

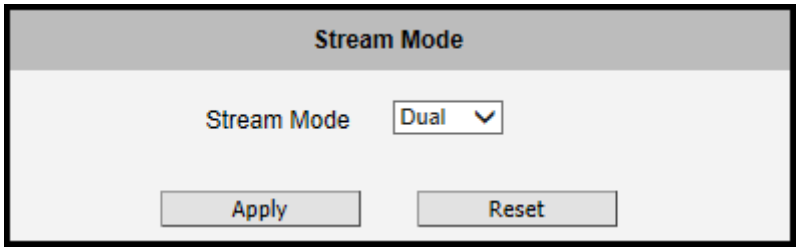
The **[+]** mark before Video indicates that the list can be expanded by clicking on it. Once expanded, the list can later be collapsed again by clicking on the **[-]** mark.

Camera Options

The **Camera Options** submenu allows the user to set the stream mode and TV standards of the video signal.

Stream Mode

The encoder is a dual stream device. Usually, Stream-1 is configured to be high quality video with maximum resolution and frame rate for recording purposes while Stream-2 is usually a moderate quality stream for live view purposes of the VMS, to reduce VMS computing power during video decoding of multiple channels. In some third-party VMS, the dual stream occupies two (2) channels. In this case, the user can use this feature to set the stream mode as **Single** and save up channel allotment on the VMS.



Stream Mode: Select **Single** or **Dual** number of streams.

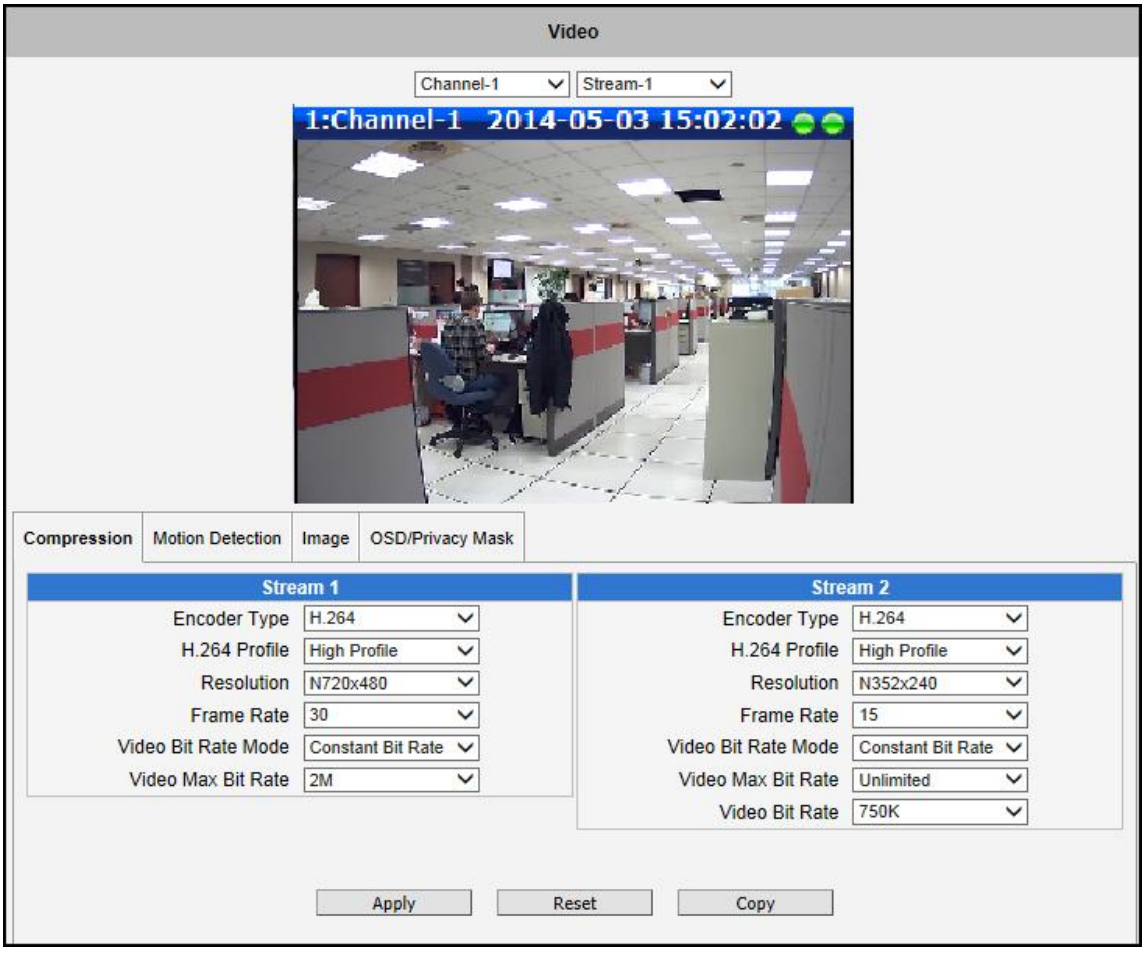
After changing the item above, click **Apply** to save the changes. The **Reset** button undoes the changes that had just been made but not applied yet.

Video

Video

The **Video** submenu is further divided into tabs. The functionality of each tab is explained separately below.

Upon opening the **Video** submenu, the live view of stream 1 is displayed. If **Stream Mode** in **Camera Options** is set to **Dual**, then select which stream to display from the stream drop-down box. For models with more than one (1) channel, select the channel to configure from the channel drop-down box. Note that the channel drop-down box appears only in models with multiple channel support.

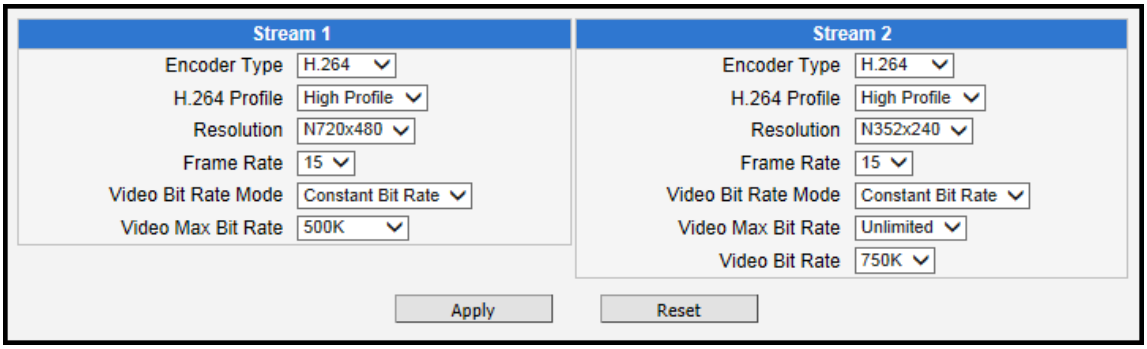


Usually, Stream-1 is configured to be high quality video with maximum resolution and frame rate for recording purposes while Stream-2 is usually a moderate quality stream for live view purposes of the VMS, to reduce VMS computing power during video decoding of multiple channels.

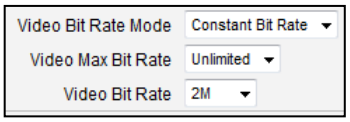
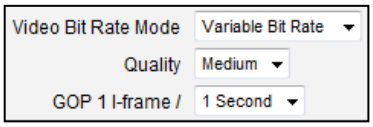
Compression

The **Compression** section allows the user to define the compression settings of the video stream 1 and stream 2. The purpose of compression is to reduce the bandwidth and VMS storage consumption.

Usually the stream 1 is configured to be the best quality stream for NVR recording purposes while the stream 2 is configured to be with the basic quality for the live view of NVR, to minimize the computing power of NVR used for video decoding.



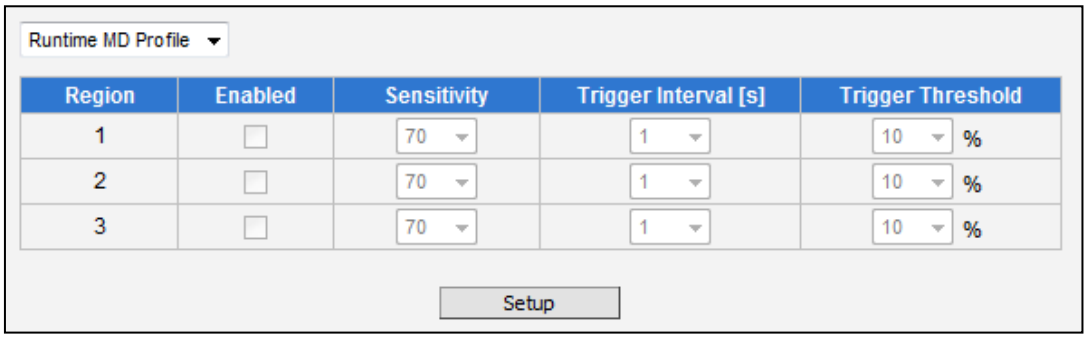
Parameters	Description
Encoder Type	There are two encoder types available: **H.264** (High Profile) and **MJPEG**.
H.264 Profile	This item is available only if the **Encoder Type** is **H.264**. The **H.264 Profile** defines the video compression scheme: **High Profile**, **Main Profile**, and **Baseline**. These schemes vary from least compressed, **Baseline**, to most compressed, **High Profile**. By default, the H.264 Profile is **High Profile**, which provides the most compression with the best video quality, but more computing power. Some third-party video management system has longer latency or takes more time to decode High Profile compression scheme, in this case, you can select **Main Profile** or **Baseline**. In order to get the same video quality, you can select a higher bit rate with lower compression; this is the same as having a lower bit rate with a High Profile. For example, a video on High Profile with 2M bit rate will have the same video quality as a video with Baseline Profile at 3.5M bit rate.
Resolution	Depending on the device model, the number of available resolutions may be different. The default resolution setting of the device may not necessarily be the maximum resolution of the device. If the user wants to use the maximum resolution, it is possible to do it here. The maximum possible resolution of the stream 2 will be smaller than stream 1.
Frame Rate	Defines the amount of frames per second.
Video Bit Rate Mode *(only for H.264)*	Under **Constant Bit Rate** mode (CBR), the device keeps the stable bitrate regardless of the complexity of the scene. Under this mode, the video quality may vary if the bit rate value is set too low. It is easier to do storage and network bandwidth consumption estimations under

	this mode compared to Variable Bit Rate mode. Under **Variable Bit Rate** mode (VBR), the device will keep the video quality stable while the bit rate may occasionally go up or down, depending on the complexity of the scene.
Video Max Bit Rate *(only for H.264)*	Defines the upper limit of the bitrate (only available under CBR mode). The bitrate will be floating slightly under that limit. For example, if the limit is set as 2M, the bitrate will be floating around 1.6~2.0 Mbps.  If the Video Max Bit Rate is chosen as **Unlimited**, then the **Video Bit Rate** selection box will appear that defines the bit rate level.
Video Bit Rate *(only for H.264)*	Under CBR mode, when **Video Max Bit Rate** is chosen **Unlimited**, the user can define the AVERAGE bit rate. For example, if the **Video Bit Rate** is chosen **2M**, then occasionally, the actual bit rate may go below or beyond 2M, but in the long run, the average bit rate will be very close to 2M. This mode allows the most accurate storage estimations, however, while planning the bandwidth, please consider the occasional peaks of bit rate.
Quality	**H.264 Compression:**  Under VBR mode, the bit rate will be floating while the video quality will be stable and follows the quality standard set by the user. The user can choose either **High**, **Medium** or **Low** quality. The higher is the quality level, the more bit rate the device will use to achieve the target quality. **MJPEG Compression:** The user can define the quality with the numeric scale from 1 to 100. The default MJPEG quality is 60. The higher is the quality level, the more bit rate the device will use to achieve the target quality.
GOP 1 I-frame *(only for H.264)*	Under VBR mode it is possible to adjust the GOP length - that is the occurrence rate of I-frames. By default, there is one I-frame per second. For example, in case of 30fps, there will be 1 I-frame and 29 P-frames every second by default. When the GOP is changed to "1 I-frame per 5 seconds", then there will be one I-frame, followed by 149 P-frames. In case of the static scenes, long GOP can further minimize the bandwidth and storage consumption.

After changing any of the items above, click **Apply** to save the changes. The **Reset** button undoes the changes that had just been made but not applied yet.

Motion Detection

The **Motion Detection** section allows the user to configure the video motion detection system of the device. Motion detection regions are based on the Stream 1. By default, all the regions are disabled. For multiple channel devices, select the channel from the drop-down box to set its motion detection.



Click **Setup** to adjust the motion detection regions or its parameters.

NOTE: **Microsoft Internet Explorer** browser is required to configure the motion detection regions.

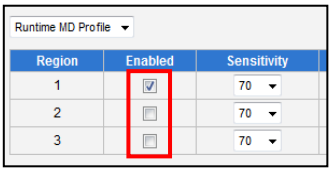
There are three independently configurable motion detection regions in the device. Each motion detection region has 6 configuration parameters:

- Enabled or disabled
- Location of the region
- Size of the region
- Sensitivity
- Trigger threshold
- Trigger interval

Enabled or Disabled

Each of the 3 motion detection regions can be enabled or disabled individually. Look at the example: Only the region 1 is enabled while 2 and 3 are disabled. The disabled regions disappear from the video display.

Note that the number of the motion detection region is written in the upper left corner of the region.



Location of the region

You can move the motion detection region anywhere on the field of view by dragging the top of the motion detection rectangle as shown on the image. The motion detection regions may even be overlapping if you like.

Size of the region

By dragging the lower right corner of the motion detection region you can change the size of the region. The maximum size of the region can even be as big as the whole screen.

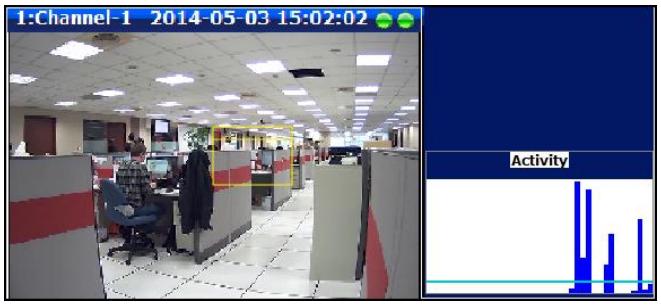
Sensitivity

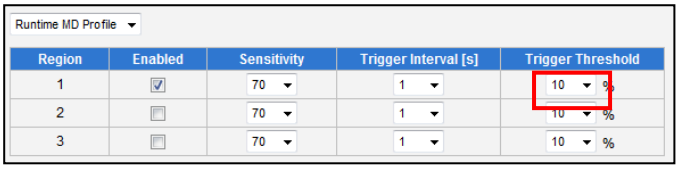
Sensitivity is the parameter that helps us distinguish actual moving targets (people, vehicles) from the slightly moving background, such as leaves of the trees waving in the wind. In order to avoid false alarms, we might want the device be able to ignore small motion. The higher is the sensitivity level of the device the smaller shift of the object is needed to trigger the alarm. For example, if the object within motion detection region has moved for about 1-3 pixels during two video frames, then such small motion will be discarded by device if the sensitivity is low, and will still trigger an alarm if the sensitivity is high. In other words, you can think of sensitivity level as a ***reversed speed limit*** – the smaller is the sensitivity, the faster are the objects allowed to move without being detected.

The biggest challenge of motion detection configuration is to find the settings that do not produce false alarms and at the same time do not miss any actual intrusions. The rule of thumb is: **the sensitivity should be as high as possible while not producing false alarms.** The default sensitivity level of the devices is 70 (on a scale of 0-100) and it is a good setting for most standard cases.

Trigger threshold

Look at the moving object entering the area of motion detection: although moving quite slowly, it caused motion activity – several pixel regions reported a motion that was faster than allowed "speed limit" of sensitivity (70).





The blue graph on the right side of the image shows how many percent of pixels within the motion detection region were considered as "currently in motion". The activity panel itself is a timeline – for each moment of time you can see the height of the blue bars. You may notice that at certain moment the tallest bars in the activity graph reached about 25% (a quarter of the total height in activity panel) – it means, 25% of this motion detection area were filled with moving pixels at that moment. By visual observation you can also see that the object standing inside the motion detection region indeed covers about 25% of its size.

What if the object is really small but moves rather fast (gets triggered by the current sensitivity level)? For example, we want to detect people but not the cat walking in the room. Although both people and cat may move with the speed that will trigger motion, they have different size of triggered pixels. For example, a human passing by the motion detection region will trigger 25% of pixels in that region while the cat would trigger only 2%. Since we want to have a real alarm in case of human or vehicle passing by while ignoring birds, cats, butterflies, mice, etc, we need a filter that can define how many percent of triggered pixels will be considered as a real alarm. This parameter is called **trigger threshold**. The default value of trigger threshold is 10%. It means, only the objects that are bigger than 10% of the motion detection region size and move faster than allowed by sensitivity level (70) will produce actual alarm.

How to choose the most optimal trigger threshold level? The rule of thumb, **keep the trigger threshold as small as possible while not causing false alarms by the moving objects that are not humans or vehicles.**

You can have different sensitivity level and trigger threshold level for each motion detection region.

In order to understand all of the above even better, please refer to the table below containing four possible combinations of settings using sensitivity level and trigger threshold percentage.

The objects listed in each cell will trigger an alarm under given settings:

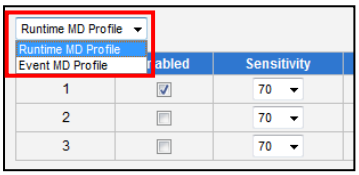
	Low threshold (0-5%)	**High threshold (5-100%)**
Low sensitivity (0-65)	Big and fast  Small and fast 	Big and fast 
High sensitivity (65-100)	Big and fast  Big and slow  Small and fast  Small and slow 	Big and fast  Big and slow 

The device's default sensitivity is 70 and threshold is 10%. By these default values, only the rabbit and the turtle would trigger an alarm while the butterfly and the snail would be ignored by the motion detection system.

Important: Please remember that changing the size of the motion detection region has an impact on the threshold – the bigger is the size of the motion detection region the smaller should be the threshold value if you want the same object size to trigger motion. For example, if you increase the motion detection region to twice the previous size, please remember to reduce the threshold to half its original value (from 10% to 5%). On the other hand, changing the location of the motion detection region has no impact on threshold.

Trigger interval

The last configuration item is the trigger interval. It is the time period from the beginning of the triggered event during which the all motion activities are ignored by the device. This is designed to avoid needless repetitive reporting of the same intrusion. Trigger interval 20 seconds would mean that when the even happens, device will take certain one-time actions and ignore the continuing activity in the motion detection region for 20 seconds. When 20 seconds are over, the device will produce a new alarm if there are still action in the motion detection region, and take actions again.



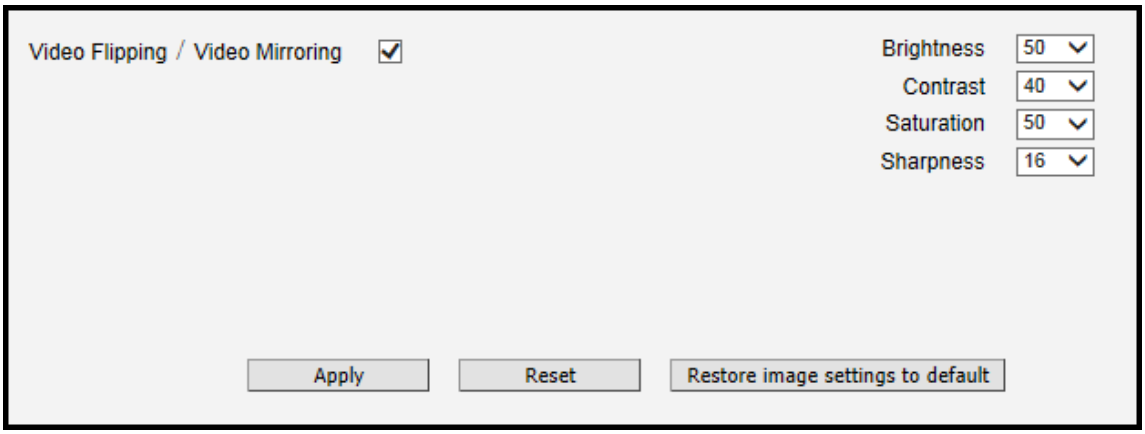
There is one more item on the Motion Detection configuration page which was not explained above – the **Profile of Motion Detection**. Think of them as **Profile 1** (Runtime MD Profile) and **Profile 2** (Event MD Profile). It means that you can configure two independent groups of Motion Detection regions with at most 3 regions in each group. Normally, the Profile 1 (Runtime MD Profile) is used as an active profile of the device. However, in some cases it is possible to let the device switch to Profile 2 by using the Event Handler system of the device.

For example, you might want to have different motion detection parameters for day and night time. Then the two profiles become really handy. In such case, remember to configure the motion detection parameters for both profiles before moving on to configure the event response system.

After changing any of the items above, click **Apply** to save the changes. The **Reset** button undoes the changes that had just been made but not applied yet.

Image

The **Image** section allows the user to control certain parameters of a video frame.



Parameters	Description
Video Flipping / Video Mirroring	Check this box to flip the video up-down and left-right to achieve the 180-degree rotation effect.
Brightness	Select the Brightness value (0~100). The higher the value, the brighter the image.
Contrast	Contrast adjusts the separation of the dark and bright areas of an image. Select the Contrast level (0~100). Increasing contrast makes the dark areas darker and bright areas brighter.
Saturation	Saturation makes colors appear more vivid. Select the Saturation level (0~100). The higher the value, the more saturated the image becomes.
Sharpness	Sharpness makes the contours of the image more distinct. Select the Sharpness level (0~255). The higher the value, the sharper the image.

After changing any of the items above, click **Apply** to save the changes. The **Reset** button undoes the changes that had just been made but not applied yet.

The **Restore image settings to default** button is a quick way of restoring factory default image settings without needing to reset the whole device to factory default.

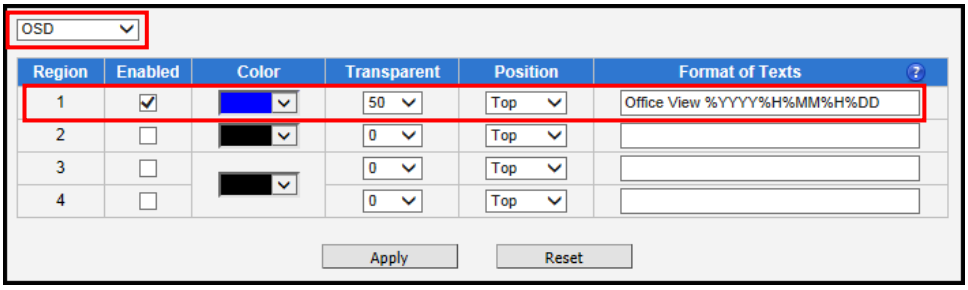
OSD/Privacy Mask

The section **OSD / Privacy Mask** allows user to do one of the two on-video operations:

1. Add text to the upper or lower left corner of the video. This function is called **On-Screen Display (OSD)** or **Text Overlay**. It is possible to display the camera name, date and time, IP address or any custom text as Text Overlay. **The text is kept as small as possible and is not resizable.** The text can be read normally when the video is enlarged on the display to 1:1 ratio. The purpose of having the text so small is to provide sufficient legal evidence while blocking the smallest possible area of the video to avoid valuable video evidence being blocked by text overlay. The text will be embedded into video and cannot be removed later upon playback or export.
2. Cover up some sensitive areas of the video that should not be captured by the camera, such as manager's computer screen or bathroom entrance. This function is called **Privacy Mask.** It is possible to configure several independent regions for masking. **Microsoft Internet Explorer** browser is required to configure the Privacy Mask. The privacy masks will be embedded into video and cannot be removed later upon playback or export.

On-Screen Display (OSD)

It is possible to define up to 4 regions of text. If more than 1 region of text is **enabled** and positioned in the same location, then the texts will appear one below another, row by row.



In the example above, one region of text was enabled with blue color and 50% transparency, located at left lower corner and containing the text of "Office View" together with current date. The date would be automatically changing every day, according to camera's date and time settings. The result of the example configuration would look like this (Live View page, 1:1 scale):

Below is the list of characters with special meaning that can be used in the text field:

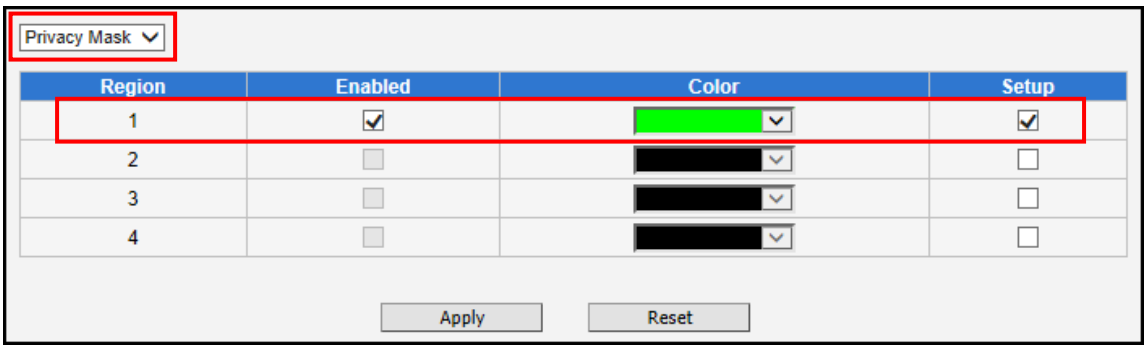
Parameters	Description
%YYYY	Year in four-digit format. For example, 2008
%YY	Year in two-digit format. For example, 08
%MM	Month in two-digit format. For example, 01 for January, 12 for December
%DD	Date in two-digit format. 01~31
%hh	Hour in two-digit format. 00~23. Note that only 24-hour indication is supported.
%mm	Minutes in two-digit format. 00~59
%ss	Seconds in two-digit format. 00~59
%H	a hyphen, "-"
%C	a colon, ":"
%X	a slash, "/"
%N	show Camera Name (It might be truncated if exceeds max OSD length)

After changing any of the items above, press **Apply** to save the changes. The **Reset** button undoes the changes that had just been made but not Applied yet.

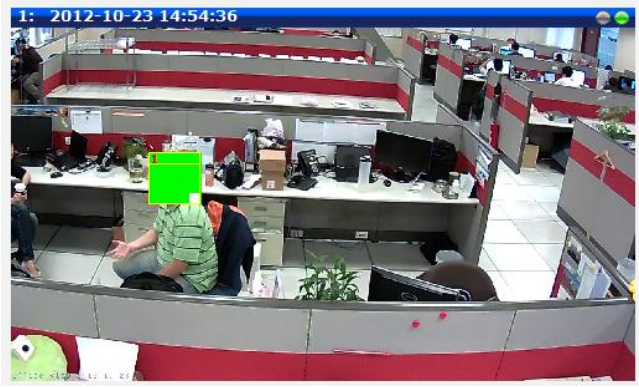
Privacy Mask

The **Privacy Mask** section allows the user to cover up some sensitive areas of the video that should not be captured by the device, such as a manager's computer screen or bathroom entrance. It is possible to configure several independent regions for masking.

It is possible to set up to 4 regions of privacy masks. The adjustment of the privacy mask region can be done when the region is checked under the **Setup** column.



NOTE: This feature is recommended for fixed and vari-focal cameras only. Due to continuous camera movements, PTZ and zoom cameras may yield inaccurate results when used with this feature.



You may resize and drag the region the same way as the motion detection regions: upper bar that contains the number of the region can be used for dragging the region across the video while the white box at the right lower corner of the privacy mask region can be used for resizing the region.

There are 4 pre-defined color options for privacy masks. If the user wants to use any other colors, please use URL commands to set up the privacy mask instead. To do that, please refer to the Guide that explains the use of URL commands.

When switching back to live view, the privacy mask would look like this:

For PTZ device models, the privacy mask is dynamic. Thus, when the device is panned to other directions, the region that is originally covered remains covered for privacy. Also, the user can only select one color for all 4 privacy masks.

Please note that the Privacy Masks will take effect for both Stream 1 and Stream 2.

After changing any of the items above, click **Apply** to save the changes. The Reset button undoes the changes that had just been made but not applied yet.

NOTE: It may take several seconds to update the region location on video display after pressing **Apply**!

On-Screen Graphics (OSG)

On-Screen Graphics (OSG) is a new feature that allows placing custom image files on the top of the video as a layer. For example, it can be used as a watermark for security purposes, or a brand logo in the corner of the video image.

There is no interface within Web Configurator to configure On-Screen Graphics since it is a rarely used feature. The URL commands can be used to complete the task instead.

The image that can be used as OSG has to be in YUV format (Image raster graphics) before uploading to the camera. There are several freeware converters available that convert images to YUV format.

For example, one free trial version of YUV converter can be downloaded from Sunrayimage.com:
http://www.sunrayimage.com/download/YUVTools_3.0_trial.zip
We do not guarantee the performance, terms of usage or availability of this product. The user has to read the terms of use first and proceed with installation if the terms are acceptable.

Please note that the image should not be larger than 640x480 pixels and should contain an even number of pixels. The image, once uploaded, cannot be resized. Therefore, please make sure that you have the image with the right size before uploading to the camera.

For example, we have the BMP logo with the size 204x106 that has been converted into YUV:

When the image is ready, upload it to the camera by the following URL command:

http://192.168.0.100/cgi-bin/cmd/encoder?OSG_IMAGE

Upon successful entry of user name ans password, the following upload window will appear. **Browse** for the **yuv** file in your computer that you had prepared and press **Apply**.

When done, use another URL command to configure its position:

http://192.168.0.100/cgi-bin/cmd/encoder?OSG_CONFIG=1,0,0,240,106,EB8080,4

... where the 7 parameters behind OSG_CONFIG mean following:

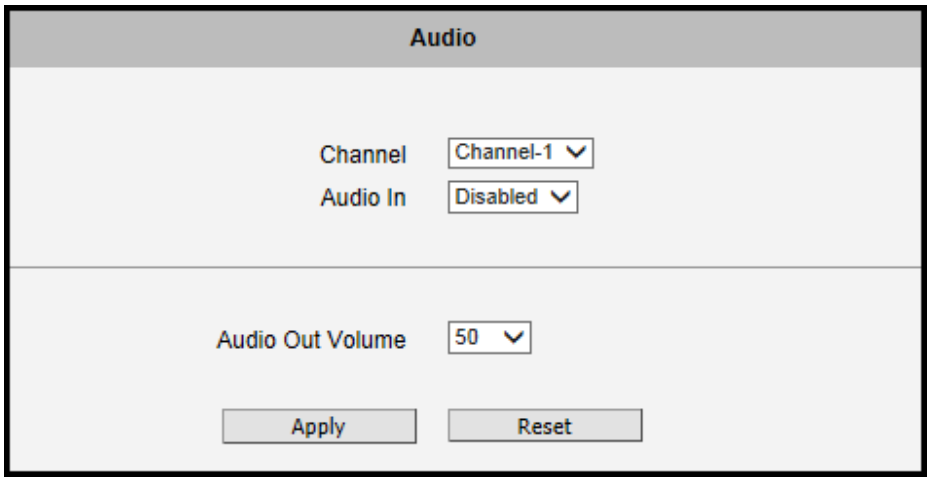
Parameter Position	Description
1	1 means enabled, 0 means disabled
2	X position
3	Y position
4	Width of the image
5	Height of the image
6	YYUUVV value of the background color of the image that is to be blended
7	Transparency level: 0 means 0%, 1 means 25%, 2 means 50%, 3 means 75%, 4 means 100%

The result would look like this:

Audio

Audio

The **Audio** submenu is used to configure the audio input and output settings of the video channel.



Parameters	Description
Channel *(for multi-channel encoders only)*	Select the video channel to adjust its audio settings.
Audio In	The option "Enabled" would activate incoming audio. The option "Disabled" would turn off the incoming audio. In such case, the video stream is captured without audio.
Audio Out Volume	The audio out volume level can be adjusted in the scale of 0-100. It will only influence the volume level of the PC speakers but not the external speakers connected directly to the encoder.

The volume level can be adjusted from 0 up to 100. Where "0" mutes the audio and 100 is the maximum volume.

This volume control appears in user interface only when the Audio-in function of the device has been **Enabled**.

Event

This section describes how to setup the Event Handler, which deals with how the IP devices respond to situations. Each IP device can have a maximum of 10 Event Rules. Each rule includes one single trigger, and one or many responses. Several types of responses are available. And there are multiple external servers for the device to interact with.

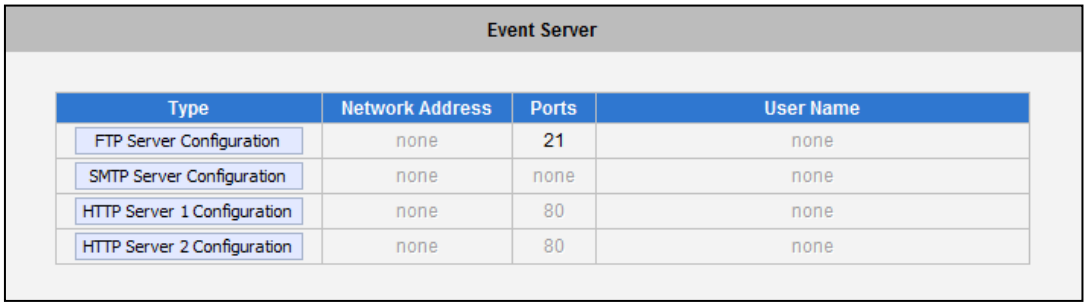
When setting up Event Handler, there are four types of settings. Event Server, Event Configuration, Event Rules and Manual Event

Click the ⊞ item before **Event** to expand the list.

Event Server

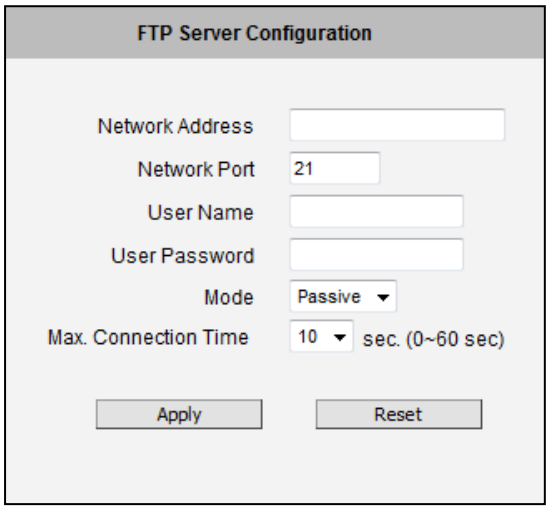
Event servers define whom the device may interact with. They can be other servers or devices on the network, or even the device itself. **Event Configuration** sets up a list of what to tell the other party during interaction. Event list lays down the rules and conditions about when to initiate which responses from which triggers. ***The options available for Event rules are selected from the event servers and event configurations.***

Event servers are classified as FTP servers, SMTP servers and HTTP servers



FTP Server

FTP servers can receive snapshot or video uploads that are issued as part of the response from event handlers. You may setup one FTP server.

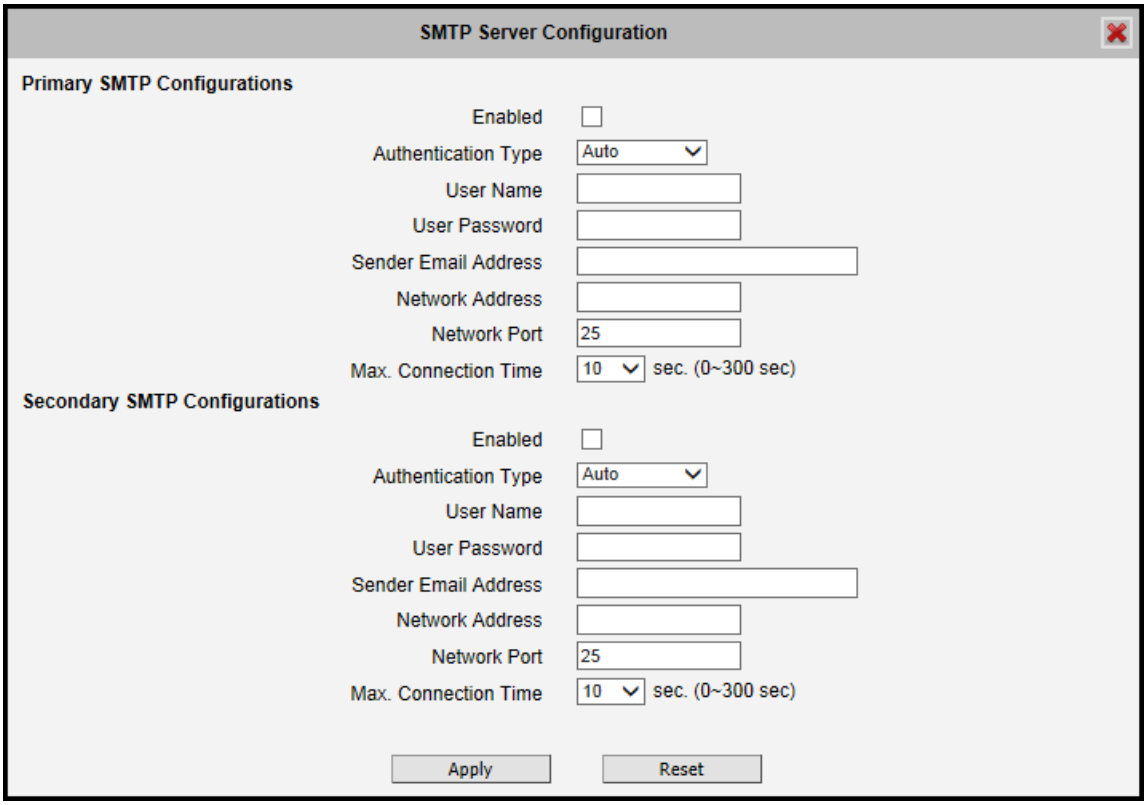


To setup FTP servers, make sure to enter the **Network Address** of FTP server, the **Network** (FTP) P**ort**, the **User Name** and **Password** of FTP account, connection **Mode** (**Passive** or **Active**) and **Max. Connection Time** before timeout.

After changing any of the items above, click **Apply** to save the changes. The **Reset** button undoes the changes that had just been made but not applied yet.

SMTP Server

SMTP servers can send email upon request from the IP device. The email can be a simple subject and text email, or attached with snapshot / video. You may setup two SMTP servers. The device will first attempt to send the message via the Primary email SMTP server. If the first attempt fails (after the Max connecting time), then the device will attempt to send via the secondary SMTP server. If the device sends email successfully via the primary SMTP server, then it will not use the secondary SMTP server.



To setup SMTP servers, make sure to enable the SMTP account and choose the proper **Authentication Type**. There are many types available. The default is **Login**. We recommend you to use **Auto Detection**. Available authentication types include: **Auto Detection**, **None**, **Login**, **Plain**, **Cram MD5**, **Digest MD5** and **PoP Relay**. Please also enter the **User Name**, **Password**, the **Email Address** displayed as sender (can be different than the user name), **Network** (SMTP server) **Address**, **Network** (SMTP server) **Port number** and **Max Connection Time** before timeout (in seconds).

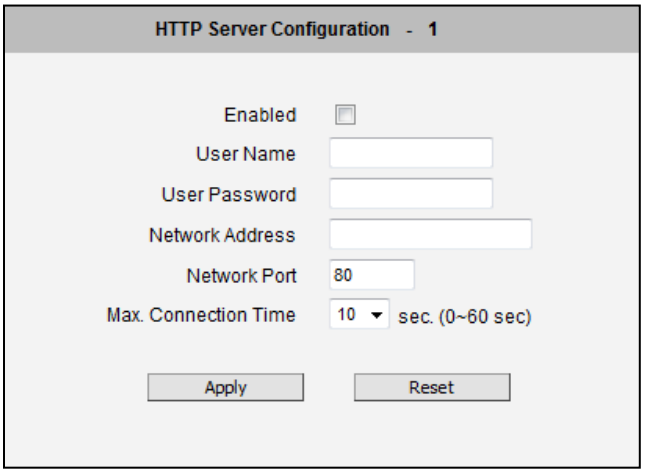
After changing any of the items above, click **Apply** to save the changes. The **Reset** button undoes the changes that had just been made but not applied yet.

HTTP Server

HTTP CGI servers are programs that run on web sites or many devices. They can be custom programmed to perform a large variety of actions based upon the input. You can define which CGI server to connect to here, and the user / password required to log into the target server. The actual message / command is setup in the Notification messages / URL commands section. You may define two separate CGI servers.

IP devices are also CGI servers. This means that IP devices can now issue commands to each other, which creates endless possibilities for highly coordinated response. The IP device can also give a loopback command to itself, in effect changing almost all possible settings dynamically. For detail on the commands used to control the devices, please contact your customer representative.

An example will help you gain a better sense of how to utilize this unique function. Device A is a fixed device that looks at a corridor leading to the main hall. It has a motion detection window located near the point where the corridor arrives at the large hall. Device B is a PTZ device located in the hall, which is usually left on auto-tour patrol. When motion activity in the motion detection region triggers MD1 in Device A, this then in turn activates an event rule in Device A that gives out a command to Device B. Device B would then swivel to the preset point where the corridor leads into the entrance and switch to higher bit rate to temporarily provide clearer image. After the event ends, Device B will go back to its normal routine in lower bit rate.



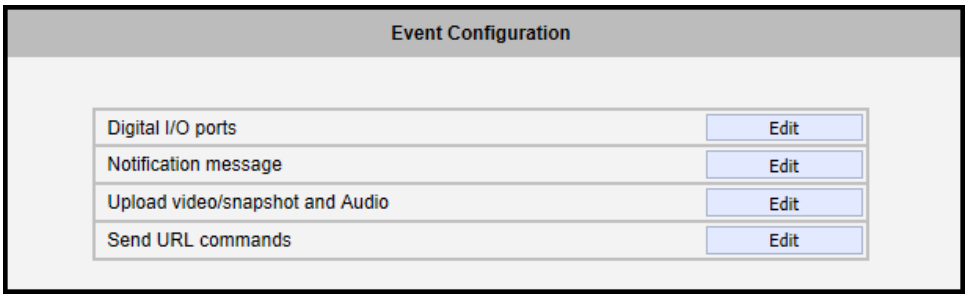
To setup HTTP servers, make sure to enable the HTTP server, enter the user name, the user password, Network (HTTP Server) address, Network (HTTP Server) port number and Max connection time before timeout (in seconds).

After changing any of the items above, click **Apply** to save the changes. The **Reset** button undoes the changes that had just been made but not applied yet.

Event Configuration

Event configurations are the responses to be performed when an event is triggered. For most types of responses, you can create several different preset responses, then mix and match in event rules.

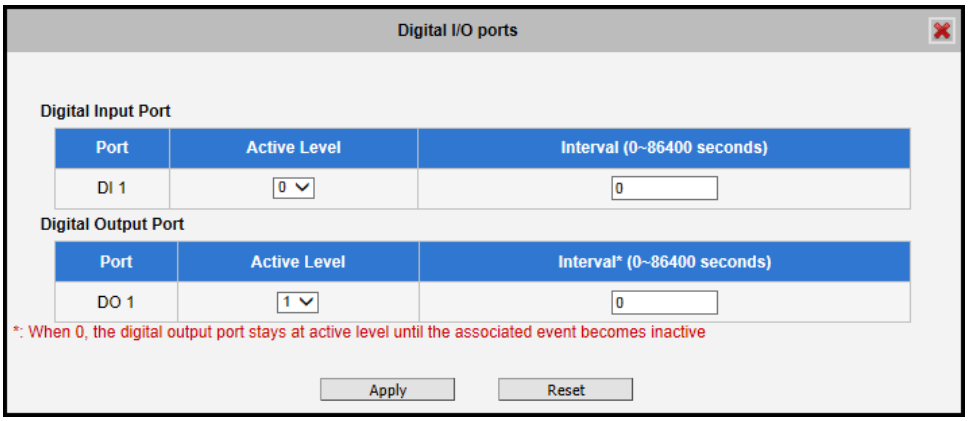
The configurable responses are classified as **Digital I/O ports**, **Notification messages**, **Upload Video/Snapshot and Audio** and **Send URL Commands**.



Digital I/O Ports

Digital input/output ports are used to connect digital input (DI) and digital output (DO) devices. DI is a trigger device like a switch or sensor (e.g. "panic button"), which when pressed or triggered, notifies the device to perform specific actions or the DO device to respond. DO's can be alarms or lights, etc.

The Digital I/O Ports page displays the number of available DI and DO ports on the device, which varies depending on device model.



Digital I/O Ports Section of V21 / V22

DI: To configure the digital input device, define the active level and trigger interval of the DI. The default **Active Level** is "0", which means the DI device remains inactive unless triggered. A good

example is a "panic button", which always stays in inactive mode "0" until the button is pressed; when the button is pressed, its active level becomes "1" which means the DI is triggered. Active level "1" returns back to "0" (inactive mode) after the specified **Interval**. The **Interval** is the duration of time when the trigger remains in active mode which is also the minimum time interval between the previous trigger and the next. For example, if the interval is set to "5 seconds", the DI will not respond if the "panic button" is pressed within 3 seconds after the previous trigger. To issue another trigger, click the button after 5 seconds from the previous trigger.

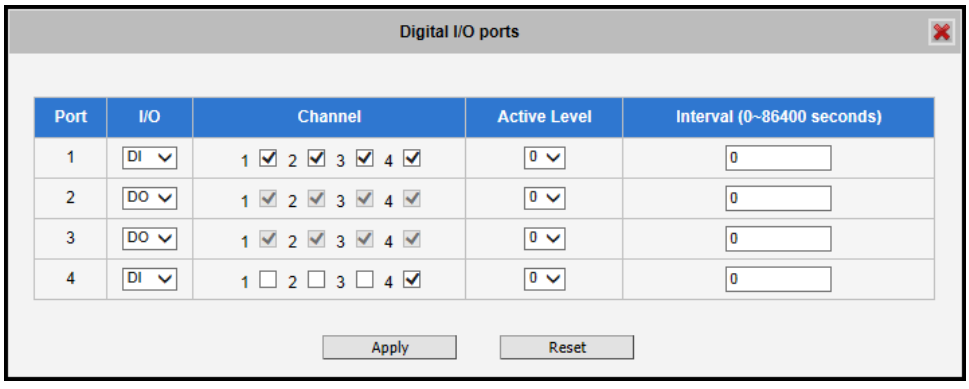
DO: To configure the digital output device, define the active level and response interval. The default **Active Level** is "1", which means the DO will turn to active mode and respond once triggered. The duration of its response will last according to the set **Interval**. A good example is an alarm siren, wherein the siren will start sounding only when it is triggered by an event or another device like a DI. The siren will stop sounding once the set interval time elapsed.

After changing any of the items above, click **Apply** to save the changes. The Reset button undoes the changes that had just been made but not yet applied or saved.

Setting Configurable DI/DO Ports (for V23 / V24 only)

There are four (4) DIO ports for V23 and V24 models. These DIO ports can be configured to either DI or DO on the **I/O** column. Every video channel can have up to 4 DIs and 4 DOs. Check the channel number box on the **Channel** column to assign a video channel for that port.

A DO port is automatically associated to every video channel thus the channel numbers on **Channel** are automatically checked for the port that is set as DO.



Digital I/O Ports Section of V23 / V24

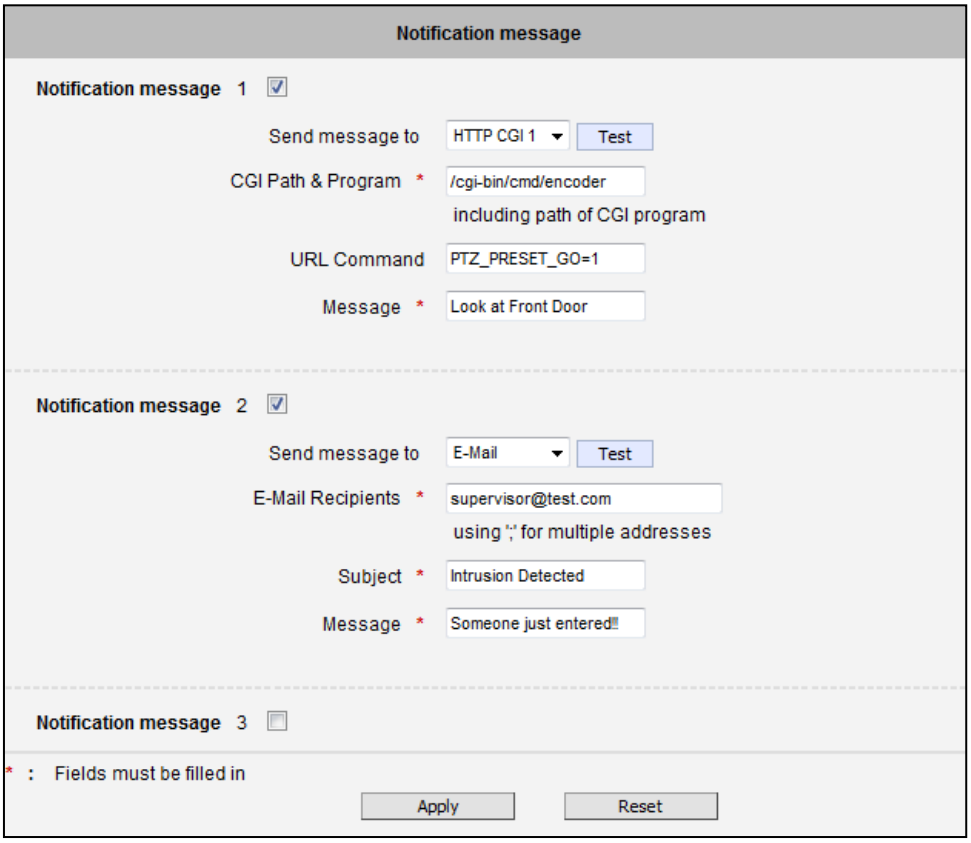
By default, the **Active Level** of each ports are "0", which means the DI/DO device will remain inactive unless triggered. The duration of its response will last according to the set **Interval**.

After changing any of the items above, click **Apply** to save the changes. The Reset button undoes the changes that had just been made but not yet applied or saved.

Notification Message

*Pre-requisites: **SMTP server / HTTP CGI server setup.**

Notification messages may be sent to either an email or a HTTP CGI server. If sent to a CGI server, it works the same as an URL command, but it does not allow a second message at end of event. You may configure up to three preset massages. You can configure a message, but disable it. This will allow you to keep the settings without using it, which will be useful in testing and troubleshooting.



To setup Notification Messages, make sure to enable the message and then determine what type of message to send (HTTP CGI or email).

If you are sending to CGI server, you need to enter the CGI path, the URL command itself, and an optional message.

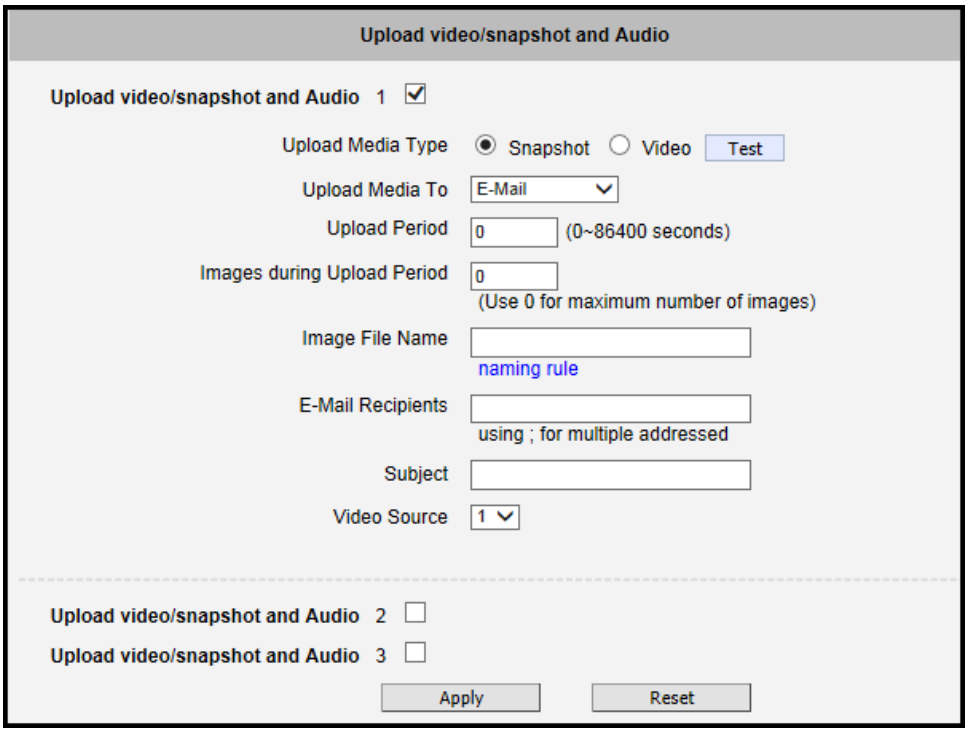
If you are sending email, please enter the recipient E-Mail address, the email subject, and the body message.

After changing any of the items above, click **Apply** to save the changes. The **Reset** button undoes the changes that had just been made but not applied yet.

Upload Video/Snapshot and Audio

*Pre-requisites: **SMTP server / FTP server / HTTP CGI server setup.**

IP devices may send video recording / snapshots to your chosen server upon event. Video will be in .RAW format, while snapshots will be .JPG files. You can define up to three groups of settings to upload video/snapshot. Snapshots can be sent to **E-Mail**, **FTP Server**, or **HTTP CGI**, while video can only be uploaded to **FTP** or **HTTP CGI** servers. If Audio in is enabled in device, the uploaded video will include audio.



The parameters needed to setup this function are different for each task combination (snapshot / ftp or video / HTTP… etc), and are explained below:

Enable						UI
						Upload video/snapshot and Audio 1 ☑
Upload Media Type	Snapshot			Video		Upload Media Type ◉ Snapshot ○ Video
Upload Media to	Email	FTP	CGI	FTP	CGI	Upload Media To E-Mail
Upload Period	Y	Y	Y	Y	Y	Upload Period 0 (0~86400 seconds)
Image during Upload Period	Y	Y	Y			Images during Upload Period 0 (Use 0 for maximum number of images)

Upload Media Type	Snapshot			Video		
Pre-Buffer Time				Y	Y	Pre-Buffer Time 0 (0~10 Second)
Image File Name	Y	Y	Y	Y	Y	Image File Name Front_Door_%YYYY_%MM_%DD
Upload Path		Y	Y	Y	Y	Upload Path Camera/%N
CGI Path & Program			Y		Y	CGI Path & Program
E-Mail Recipients	Y					E-Mail Recipients using ; for multiple addressed
Subject	Y					Subject Front Door Snapshot
Video Source	Y	Y	Y	Y	Y	Video Source 1

Upload Video/snapshot and Audio checkbox: this decides if this rule is in effect, or disabled. Sometimes it is useful to keep the settings for troubleshooting purposes, but keep them as disabled.

Upload Media to: these define the task at hand, and change the field that needs to be filled out.

Upload Period: IP device will provide video/snapshots for the number of seconds here. It will stop uploading video/snapshot at the end of this period. If you have video management software recording from this device at the same time, the normal recording through NVR will not be affected, and goes on throughout the event period and afterwards. But the special upload session will end as the event ends.

Image during Upload Period: This is used only by snapshots. This tells the device how many snapshots it should attempt to capture during the Upload Time. If this value is set to 0, then the IP device will attempt to capture as many snapshots as possible. Depending upon the device loading, the number of snapshots taken may not reach the number you specified.

Pre-Buffer Time: This is only used by video. If this is set to more than 0, then the IP device will start to buffer video in its internal memory. The maximum pre buffer is **10 seconds**. When an event requires video upload, the IP device will first upload the video taken right before the event then keep uploading until it reaches the upload time.

Image File Name/ Upload Path: You will need to specify rule for file names and upload paths (upload path is not needed for Email. Just put a slash "/" in the field). The rules contain flexible parameters. A sample rule and corresponding filename will look like this:
Front_Door_%YYYY_%MM_%DD@%hh%mm%ss
Front_Door_2009_10_12@195037.JPG

Upload Path folders may also be named dynamically. For the IP device to create folders on FTP and HTTP CGI servers properly, your FTP/CGI account will need to have permission to create folders. For syntax on auto naming, please see online help or the inset box at the end of this section.

The symbol "%" cannot be the first character in filename or upload path. Please use either an alphabet or a number as the starting character. For Upload Path, be sure to start and end eith a backslash"\". An example will be : \Backgate%MM%DD\

CGI path & Program: Some CGI servers may require special info and settings. Please refer to CGI server designer for this section. IP devices do not allow upload of Snapshots / Video into their embedded CGI servers.

E-Mail Recipient / Subject: When uploading video/ snapshots via email, these fields are required.

Video Source: Choosing the video source from video 1 or video 2.

Auto Naming Rules for Files and Folders:

To properly track images and videos, a well thought out naming rule is necessary. There are a number of automatic variables available to design a proper naming system, which may be used both on files and folders.

Symbol	Description	Example
%YYYY	4 digits for year	2009 for year 2009
%YY	the last 2 digits of 4 digits year	09 for year 2009
%MM	two digits for month. 01~12	01 for January
%DD	two digits for date. 01~31	01 for the 1st day of a month
%hh	two digits for hour. 00~23	
%mm	two digits for minute. 00~59	
%ss	two digits for second. 00~59	
%W	a space character. ' '	' '
%N	device name	device-1
%Y	File serial counter. It starts from 1 in every uploading task. The counter will be increased by 1 for next uploading file.	1,2,3,4,5,...

Example

1. Entrance-%YYYY-%MM-%DD@%hh%mm%ss for time 2009/06/05 22:50:30.

The full name is Entrance-2009-06-05@225030

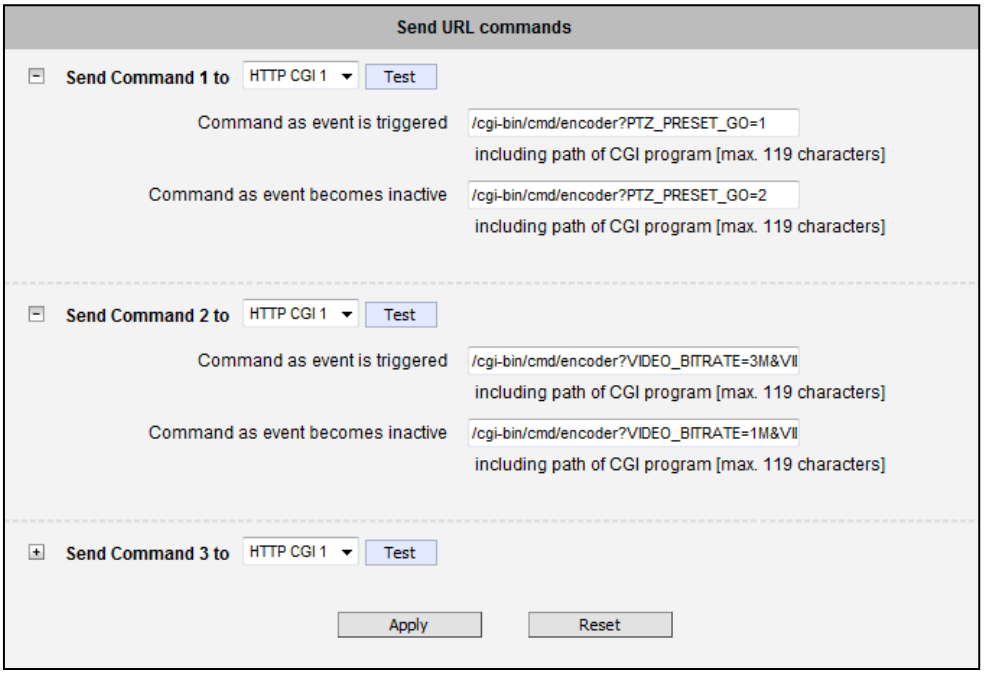
2. X_%w-%N_TEST%Y for device name is 'my-device' and three successive uploaded files.

The full names of these three files are

X_ -my-device_TEST1, X_ -my-device_TEST2, X_ -my-device_TEST3

Send URL commands

*Pre-requisites: **HTTP CGI server setup.**



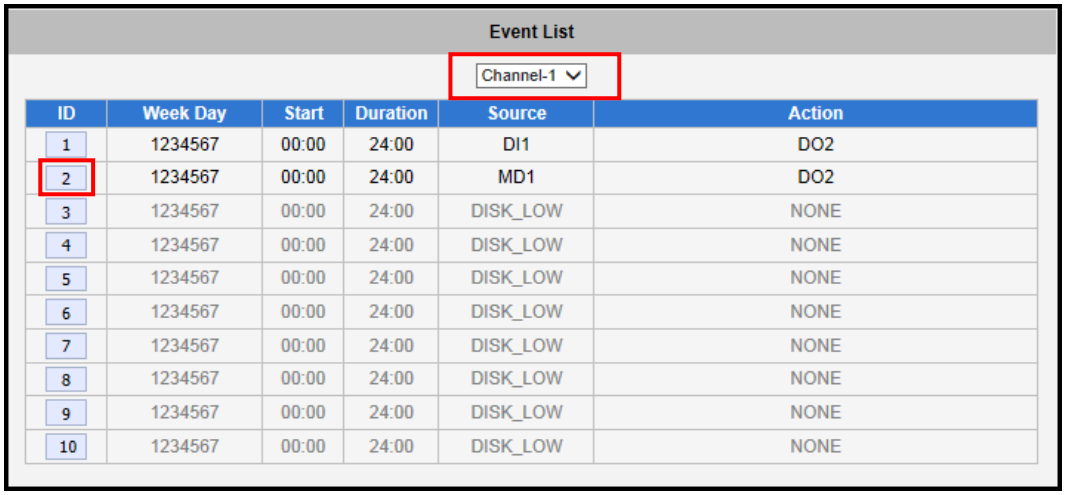
URL commands can be sent to HTTP CGI servers upon event. This provides the possibility of highly intelligent response upon event. IP devices and many other devices also have embedded CGI servers that may be controlled.

When Event Handler sends an URL command, it will send one set of command when the event is trigged, and another as the event becomes inactive. Depending on the CGI design, the URL commands may be able to be stringed together, and multiple commands may be issued in a single line.

An example would be when the access control device at the entrance detects an entry, this device provides a DI signal to the PTZ device, and triggers an event. This event then sends a loopback command to the PTZ Device itself (by setting its own IP as the HTTP CGI server). The PTZ Device then moves to a preset location, stays until the event is over, and then moves back to another location. At the same time it moves to the pre-set location, it increases the bitrate from 1M to 3M, and the frame rate from 4 fps to 8 fps. The bitrate / fps changes are reverted at the end of event.

Event List

You may define a maximum of 10 Event rules, which will be shown in abbreviated form in the Event List panel. It will display under each Event ID, the days of the week it will be active, the start time and duration of the active period, the type of the source of trigger, and the actions used in the response. If the row is grayed out, this means the rule is currently not enabled and stays inactive.



ID	Week Day	Start	Duration	Source	Action
1	1234567	00:00	24:00	DI1	DO2
2	1234567	00:00	24:00	MD1	DO2
3	1234567	00:00	24:00	DISK_LOW	NONE
4	1234567	00:00	24:00	DISK_LOW	NONE
5	1234567	00:00	24:00	DISK_LOW	NONE
6	1234567	00:00	24:00	DISK_LOW	NONE
7	1234567	00:00	24:00	DISK_LOW	NONE
8	1234567	00:00	24:00	DISK_LOW	NONE
9	1234567	00:00	24:00	DISK_LOW	NONE
10	1234567	00:00	24:00	DISK_LOW	NONE

For device models with multiple video channels, select first the video channel to configure from the channel box.

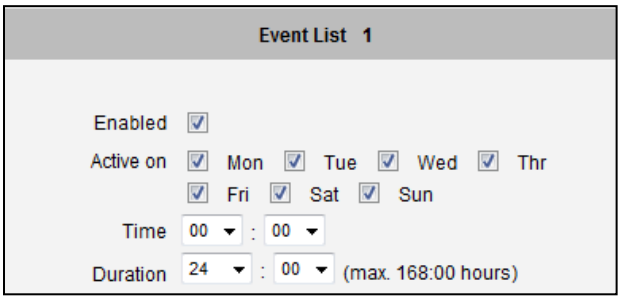
You may start creating a new event by clicking the event ID number in the list, for example "2". There are several parts to the Event rule:

When is It Active?

You may choose to enable the rule or not. The settings will be kept in internal memory even if the event rule is disabled. Select the days in a weekly cycle in which this rule and schedule is active.

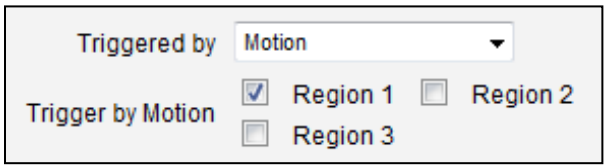
Determine the start time and duration of the active period. For example, a rule that lets motion detection trigger snapshot uploads to FTP would only take place after 19:00 each day for 12 hours. Outside of this time the rule will not be active.

In the example below, the event handler rule is active 24 hours a day, 7 days a week.



How is It Triggered?

Events may be triggered by one of the several sources. In the example below, Motion Detection region 1 is used as the event trigger.



You may also ask the event to be repeatedly triggered during this scheduled time. The interval is determined in minutes. You may use this with email / FTP upload to take snapshots at regular intervals.

Scheduler: The trigger occurs on the specified time. Set the frequency of the occurence in **Occur Every** (minutes).

DIs: The device is be triggered by a digital input.

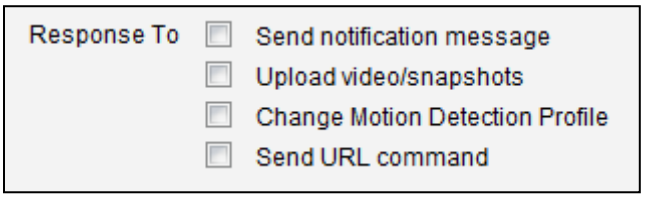
Motion: You may trigger the event if one or many Motion Detection regions encounter a motion trigger. Trigger from any of them will initiate the event. The duration of event will be the same as the MD trigger length, or the Trigger interval time, defined in the Motion Detection section on Video Adjust page.

Device boots successfully: This will trigger the event responses once the device boots up. You can use this to create a notification system that keeps record of when the device has been rebooted via email.

Reboot device: This triggers the event response when the device is shut down via web UI "Save and Reboot". Use this to keep record of when was the device setting edited. Note that this will not take effect when the device is unplugged, as this is not normal shutdown.

What Responses Will Occur?

Available responses vary depending on what triggered the event.



Digital Output: This is a useful link to other devices. Click to include this in the response for this rule.

Send notification Message: Select from the three pre-defined messages which you've setup in the Event Configuration section. You may enable multiple messages at the same time. For sending Email, please limit the recipient to one per event rule. If you need to send email to more than one recipient, please use separate event rules triggered by the same trigger.

Upload video/snapshots and Audio: Select which of the event configurations to include in this response set. If you are sending email via upload video and sending notification message at the same time, the system will automatically merge the two emails into one. The subject and image will be based upon the Upload snapshot Event configuration enabled, but the message in the body text will be based upon the Notification messages.

In general, please stick to the "one email per event rule" limit for best performance.

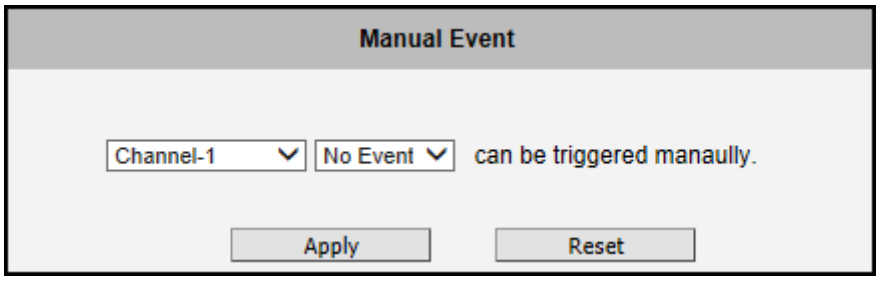
Change Motion Detection profile: This will switch the profile of the selected Motion Detection region from Runtime profile to Event profile. The profile will return to runtime settings at the end of this event. You may program one motion detection region to be disabled at runtime, but enable it with event handler under some circumstances.

Send URL command: Select the URL command to include in the response set. Two different commands will be sent at the time when the event is triggered and un-triggered.

After changing any of the items above, click **Apply** to save the changes. The **Reset** button undoes the changes that had just been made but not applied yet.

Manual Event

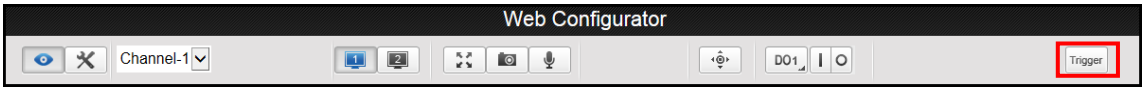
You may select one event per channel in the Manual Event section to be triggered via web user interface.



After changing any of the items above, click **Apply** to save the changes. The **Reset** button undoes the changes that had just been made but not applied yet.

Once selected, the trigger button on the video display screen will show as clickable. Click to trigger the selected event. This is useful during event rule testing.

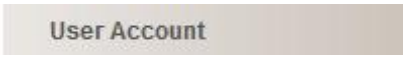
The live view panel would look like this:



System

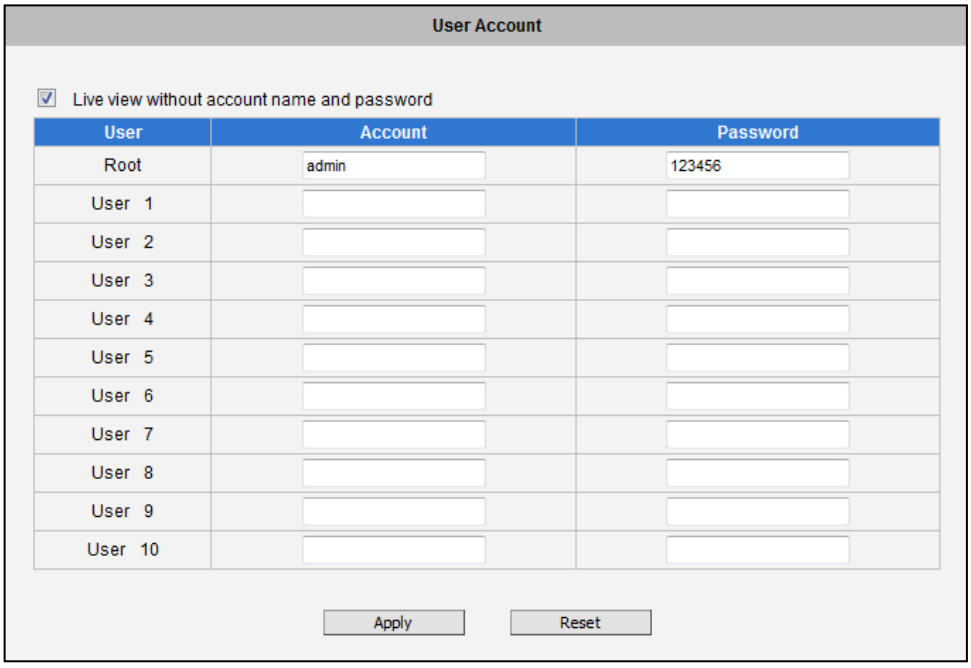
The **System** menu provides the list of functions that help manage the device. The [+] mark before System indicates that the list can be expanded by clicking on it. Once expanded, the list can later be collapsed again by clicking on the [-] mark.

User Account



The **User Account** submenu allows the users to define the user management tasks, such as:

1. Change the account name or password of the Root account that has a full access to the device.
2. Create up to 10 common users that only have an access for live view and PTZ control.
3. Enable/disable the option of seeing the live view without needing user name and password (anonymous login), which is especially convenient function for device installers on the field. For security reasons, account name and password is always required when entering Setup page of Web Configurator or when trying to access device or change settings by URL commands.

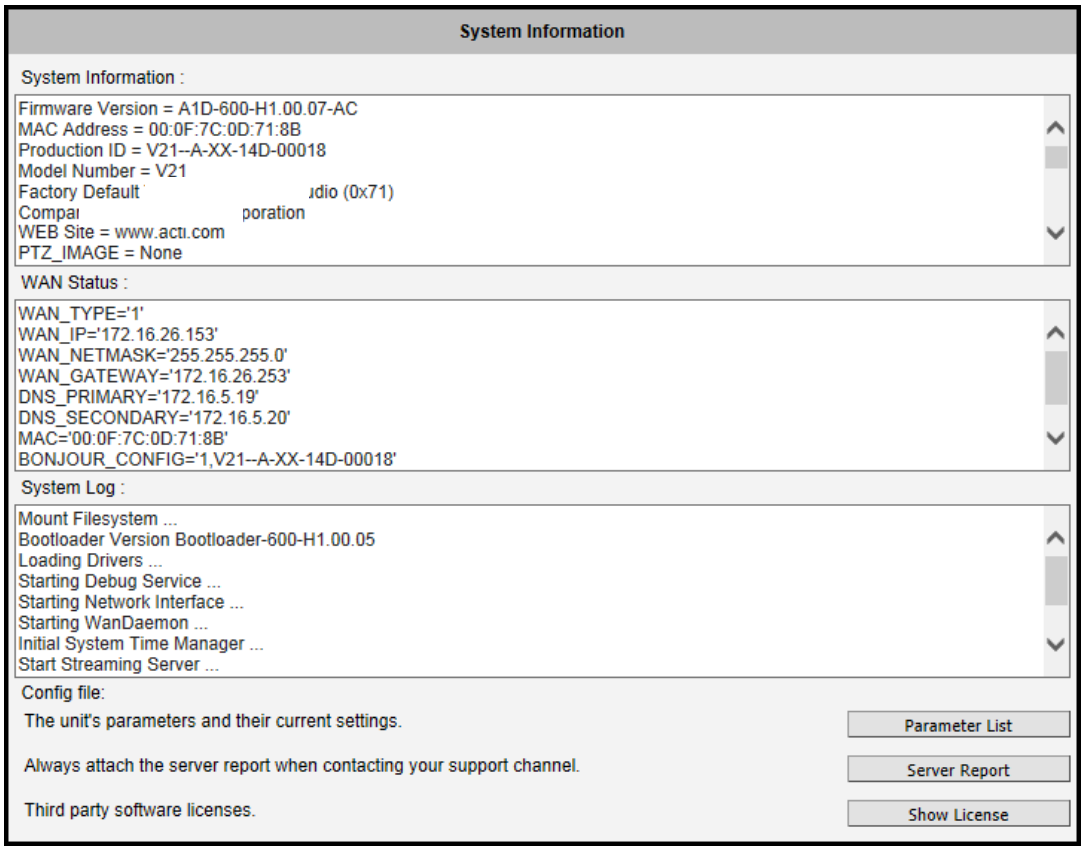


After changing any of the items above, click **Apply** to save the changes. The **Reset** button undoes the changes that had just been made but not applied yet.

System Info

System Info

The **System Info** submenu provides the full information about device status, settings and log. This information is very helpful while doing the device configuration, maintenance or troubleshooting.

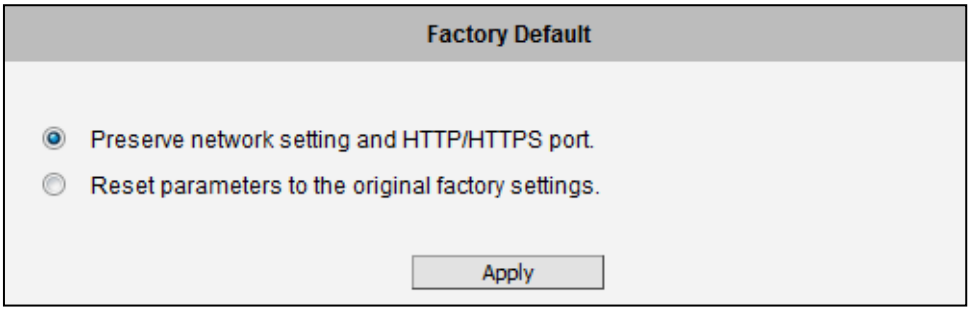


The **Server Report** is a convenient way of exporting the full list of device related information in a text format, so that it can be sent to the technical support team for faster service.

Factory Default

Factory Default

The **Factory Default** subemenu allows the device settings be reset to the original factory settings.



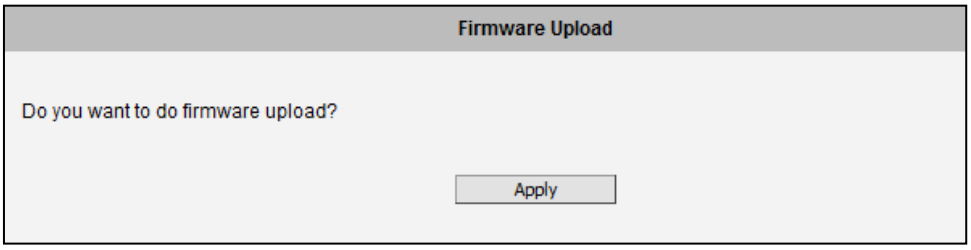
If you want to keep network settings and restore other settings to factory default, please select the first option. If you select the second one instead, all the settings would be removed during factory default. You will have to use factory default IP setting to connect to this device.

Firmware Upload

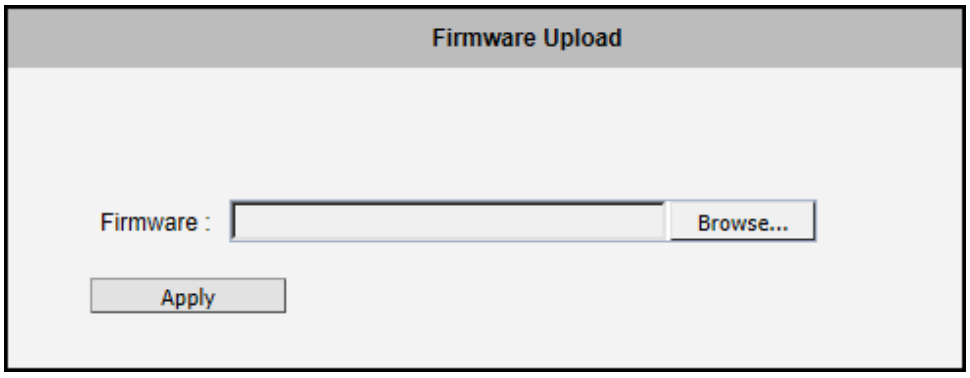
Firmware Upload

The **Firmware Upload** submenu allows remote upgrade or downgrade of device firmware. The upgrade to newer version is usually done in order to gain new functions or fix existing bugs or limitations while downgrade to older version is used mostly for integration purposes where the newly purchased device model comes with the newer firmware version than supported by a third party video management system of a given project.

The firmware image file can be downloaded from the website. It has the file extension ".upg".

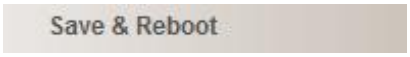


After pressing **Apply** button, it is possible to browse for firmware image file that has already been downloaded to the computer that has the Web Configurator running.

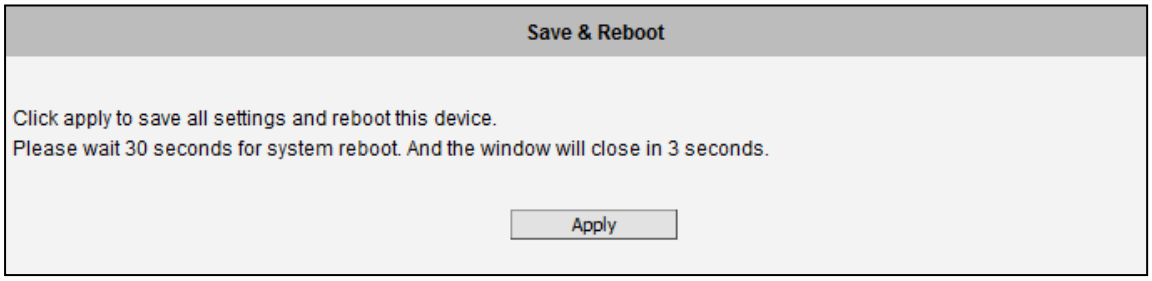


Click **Browse** to select the upload image file. Click the **Apply** button to start the upload. Once the process is finished, you will get an **OK** message and system will reboot itself.

Save & Reboot



The **Save & Reboot** submenu allows saving the settings and rebooting the device remotely. This is critical because some settings might not take effect before save & reboot.



Logout

Clicking this item allows you to log out of the IP device. Be sure to logout this IP device once you have completed all the tasks via Web Configurator.

7F, No. 1, Alley 20, Lane 407, Sec. 2, Ti-Ding Blvd., Neihu District, Taipei, Taiwan 114, R.O.C.

TEL : +886-2-2656-2588 FAX : +886-2-2656-2599

Email: sales@acti.com