

Compressor™

Analog to IP Video Encoder

DW-CP16



Username: admin

Password: 123456

WHAT'S IN THE BOX

QSG Manual		1 Set	Power Cord		1 Set
Socket Converters – 3pcs		1 Set	Rack Mount Ears – 2pcs		1 Set
Terminal Blocks		1 Set	Screws – 4pcs		1 Set

Attention: This document is intended to serve as a quick reference page for initial set-up. It is recommended that the user read the entire instruction manual for complete and proper Encoder usage.



Table of Contents

Precautions	6
Safety Instructions.....	8
Introduction.....	10
Package Contents.....	10
Physical Description.....	11
Installing the Compressor.....	14
Connecting External Devices	15
Connection Architecture	15
Connecting to Power	15
Connecting the Analog Camera.....	16
Connect to Network.....	16
Connecting Digital Input / Output Devices	17
DI/DO Connection Specifications.....	20
Connecting Audio Devices.....	20
Connecting an Audio Input Device.....	20
Connecting an Audio Output Device.....	21
Connecting a Serial Device.....	21
Accessing the Encoder	23



Configure the IP Addresses 23

Access the Encoder..... 29

Recommended PC Specifications 33

Live View 34

Login 34

Live View..... 35

 Dual Stream Capability 35

 Full Screen Mode..... 37

 Image Capture 37

 Audio Recording 37

 Digital Input / Output Controls 37

PTZ Control Panel..... 39

 How to Use Pan/Tilt 39

 How to Zoom the Device In or Out 40

 How to Set the Home Position 40

 How to Set Preset Points..... 41

Setup..... 42

Access the Setup Page..... 42

Host..... 43

 Host 43

 Serial Setting..... 45

 Video Channel’s PTZ Address 45



Date & Time	46
Network.....	49
IP Address Filtering.....	49
Port Mapping.....	51
Multicast Setting	53
HTTPS.....	54
SNMP Setting.....	56
RTP.....	58
Network (ToS, UPnP, Bonjour).....	59
IP Settings	63
Connection Type	63
DNS.....	65
Video & Audio.....	66
Video	66
Audio	81
Event	82
Event Server	82
Event Configuration	89
Event List	99
Manual Event	103
System	105
User Account	105
System Info.....	107
Factory Default.....	108
Firmware Upload.....	108



Save & Reboot 109

Logout..... 109



Precautions

Read these instructions

You should read all the safety and operating instructions before using this product.

Heed all warnings

You must adhere to all the warnings on the product and in the instruction manual. Failure to follow the safety instruction given may directly endanger people, cause damage to the system or to other equipment.

Servicing

Do not attempt to service this video device yourself as opening or removing covers may expose you to dangerous voltage or other hazards. Refer all servicing to qualified service personnel.

Trademarks

All names used in this manual are probably registered trademarks of respective companies.

Liability

Every reasonable care has been taken during the writing of this manual. Please inform your local office if you find any inaccuracies or omissions. We cannot be held responsible for any typographical or technical errors and reserve the right to make changes to the product and manuals without prior notice.



Federal Communications Commission Statement



This equipment has been tested and found to comply with the limits for a class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

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

European Community Compliance Statement



This product has been tested and found to comply with the limits for Class B Information Technology Equipment according to European Standard EN 55022 and EN 55024. In a domestic environment, this product may cause radio interference in which cause the user may be required to take adequate measures.



Safety Instructions

Cleaning

Disconnect this video product from the power supply before cleaning.

Attachments

Do not use attachments not recommended by the video product manufacturer as they may cause hazards.

Do not use accessories not recommended by the manufacturer

Only install this device in a dry place protected from weather

Servicing

Do not attempt to service this video product yourself. Refer all servicing to qualified service personnel.

Damage Requiring service

Disconnect this video product from the power supply immediately and refer servicing to qualified service personnel under the following conditions.



- 1) When the power-supply cord or plug is damaged
- 2) If liquid has been spilled, or objects have fallen into the video product.
- 3) If the inner parts of video product have been directly exposed to rain or water.
- 4) If the video product does not operate normally by following the operating Instructions in this manual. Adjust only those controls that are covered by the instruction manual, as an improper adjustment of other controls may result in damage, and will often require extensive work by a qualified technician to restore the video product to its normal operation.








Safety Check

Upon completion of any service or repairs to this video product, ask the service technician to perform safety checks to determine if the video product is in proper operating condition.

Introduction

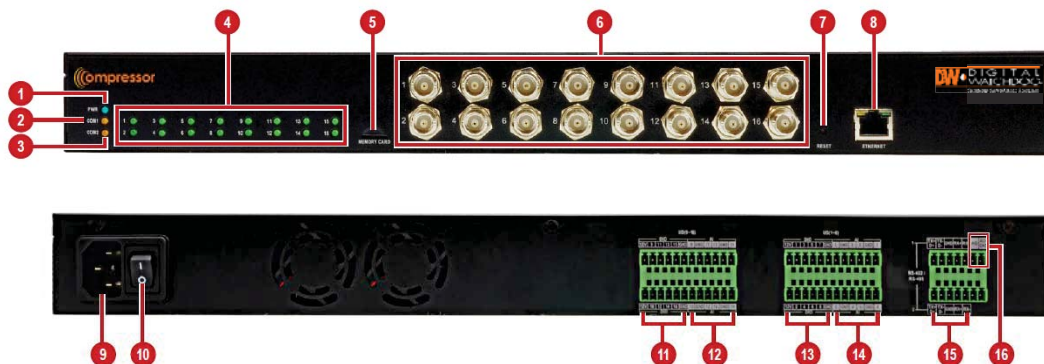
Package Contents

Please make sure the items below are included with your package.

Video Encoder	Power Cord	Socket Converter
		
Rack Mount Ears	Screw Pack	Serial Communication & Audio Output Terminal Blocks
		
Digital Input / Output Audio Input Terminal Blocks	Quick Installation Guide	
	Missing image**	

NOTE: The above pictures are for reference only; actual items may vary.

Physical Description



Item		Description
1	Power LED	Lights up when the device is powered on.
2	Serial Comm. 1 Activity LED	Serial device is connected to the RS-422/RS-485 Port 1 .
3	Serial Comm. 2 Activity LED	Serial device is connected to the RS-422/RS-485 Port 2 .
4	Video Input LEDs (1 ~ 16)	An analog camera is connected to a video input.
5	Memory Card Slot	Insert a memory card for local recording. NOTE: Supports micro SDHC/SDXC cards. Card not included.
6	Video Input Connectors (1 ~ 16)	Connect an analog camera through BNC. See <i>Connecting the Analog Camera</i> on page 16 for more information.
7	Reset Button	Restore the factory default settings, including the administrator’s password. Press and hold the Reset button for 5 seconds or until the Power LED goes off.



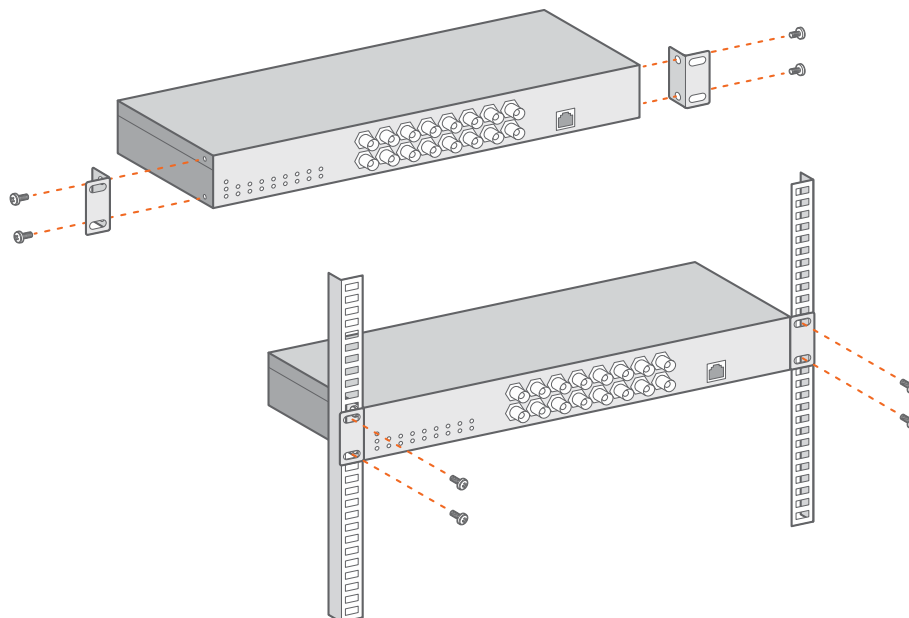
8	Ethernet Port	Connect the Compressor to the network using a standard Ethernet cable.
9	AC Power Input	Connect the bundled power cord. See <i>Connecting to Power</i> on page 15 for more information.
10	Power Switch	Turn the encoder on or off.
11	Digital Input / Output Connector (9 ~ 16)	Connect digital input or output devices, such as an alarm trigger, panic button, etc. See <i>Connecting the Digital Input / Output Devices</i> on page 17 for more information.
12	Audio Input Connectors (9 ~ 16)	Connect audio input devices, such as a microphone with built-in amplifier, etc. See <i>Connecting an Audio Input Device</i> on page 20 for more information. NOTE: Microphone must have a built-in amplifier. Connecting an ordinary microphone will dwarf sounds and will result in inaudible recording.
13	Digital Input / Output Connector (1 ~ 8)	See #11. See <i>Connecting the Digital Input / Output Devices</i> on page 17 for more information.
14	Audio Input Connectors (1 ~ 8)	See #12. See <i>Connecting an Audio Input Device</i> on page 20 for more information.
15	RS-422 / RS-485 Ports (1 ~ 2)	Connect an analog device via RS-485 / RS-422 serial communication. See <i>Connecting a Serial Device</i> on page 21 for more information.
16	Audio Output Connector	Connect an audio output device, such as a powered speaker. See <i>Connecting an Audio Output Device</i> on page 21 for more information.



Installing the Compressor

Mount the device on a 19" rack.

1. Attach the ears on each side of the encoder using the bundled screws.
2. Secure the encoder onto the rack using four (4) screws.



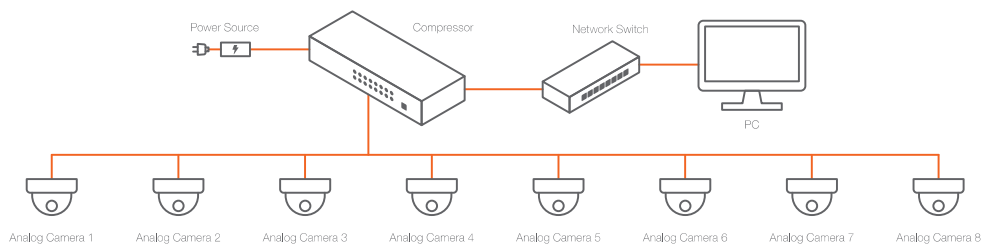
NOTE: Use the screws that came with the rack; or, purchase applicable screws for rack mounting.

Connecting External Devices

This section describes how to connect the encoder to the power, network and analog cameras. It also describes the procedures in preparing the external devices that you can connect to the encoder. The encoder supports Digital Input and Output (DI/DO), Audio Input and Output devices, as well as Serial Port Communication via RS-485 / RS-422 protocol using the bundled terminal blocks. The use of these devices, however, is optional.

Connection Architecture

The diagram below is an example of the basic connection within a local network.



Connecting to Power

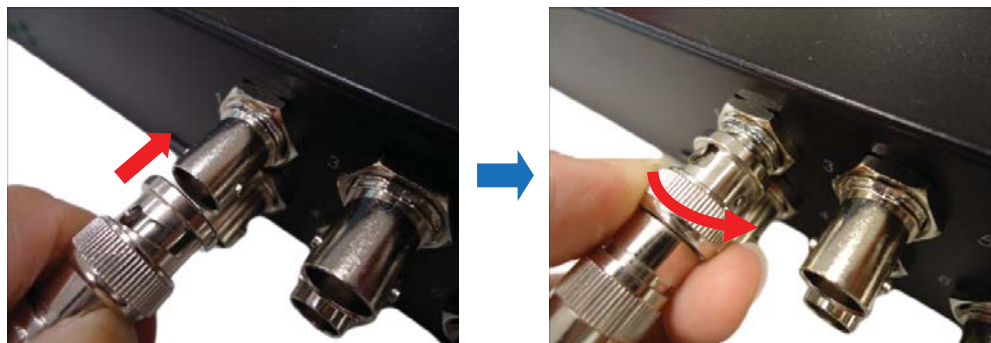
Plug the power cord to the **AC Power Input** port. Then, press the Power switch to turn on the encoder.



NOTE: Use only the bundled power cord that came with the encoder.

Connecting the Analog Camera

Connect the analog camera to the **Video Input** ports of the encoder using BNC cables.



Connect to Network

Connect one end of a network cable to the **Ethernet** port of the encoder. Connect the other end to a network switch or port.



Connecting Digital Input / Output Devices

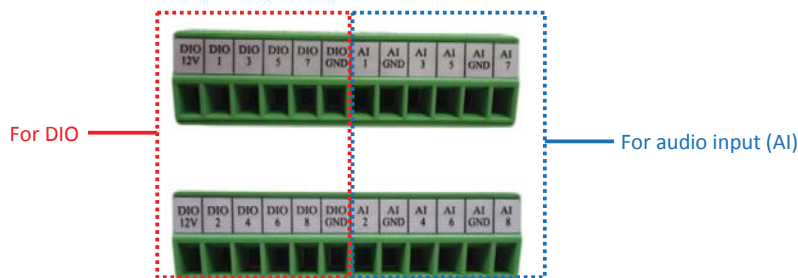
Depending on your surveillance needs, you may connect digital input / output devices to your encoder.

Digital Input (DI) devices can be used to notify the encoder of an activity in the camera on the encoder site. DI can be triggers of events. For example, you can connect a “panic button” to the encoder; as such when the panic button is pressed, the alarm signal will be sent through the encoder. Other common DI device applications are emergency button, smoke detector, passive infrared sensor, etc.

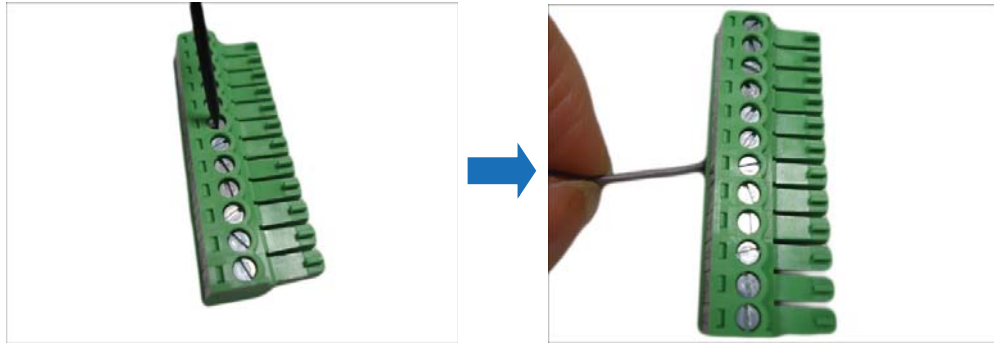
Digital Output (DO) devices are external devices that are activated by the encoder upon an event within the encoder (e.g. video connection is lost, etc.) or triggered by motion in the camera site among others. For example, you can connect an “alarm horn” to the encoder; as such when an event occurs on the camera side (e.g. detected intruder), the alarm horn will sound. Other common DO device applications are motion-triggered lights, electric fence, magnetic door locks, etc.

The digital input and output pins of the Compressor are configurable. Either a digital input or digital output device can be connected to a particular DIO pin. Once connected, the pin must be defined through the Web Configurator. The Compressor supports 16 DIO ports.

Four (4) DIO ports share the same terminal block with four (4) audio input ports. See samples below:



1. Loosen the screw of the pin and insert the wire through the pin slot.



- To connect digital input / output devices (DI/DO), map the pins to one of the pin combinations below:

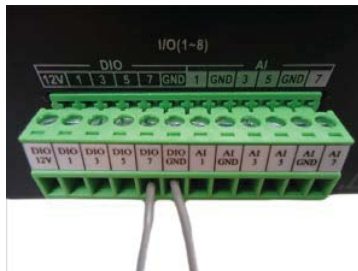
Device	Pin Label	Mapping Instructions
Digital Output (DO)	DIO (port number)	Connect the wires of the output device to a DIO and DIO 12V .
	DIO 12V	
Digital Input (DI)	DIO (port number)	Connect the wires of the input device to DI and DIO GND .
	DIO GND	

NOTE: For every digital output device, a wire must also be mapped to the **12V** pin. For every digital input device, a wire must also be mapped to the **GND** pin. The **GND** and **12V** pins may be mapped with more than one device.

- Tighten the screws to secure the wires within the pin slot.



- Connect the terminal block to the corresponding DIO connector of the encoder.



- Configure the DIO ports in the Compressor’s Web Configurator.

DI/DO Connection Specifications

The table below shows the DI/DO connection specifications:

Device			
DI	Connection design		TTL - compatible logic levels
	Voltage	To trigger (low)	Logic level 0: 0V ~ 0.4V
		Normal (high)	Logic level 1: 3.1V ~ 30V
	Current		10mA ~ 100mA
DO	Connection design		Transistor (Open Collector)
	Voltage & Current		< 24V DC, < 50mA

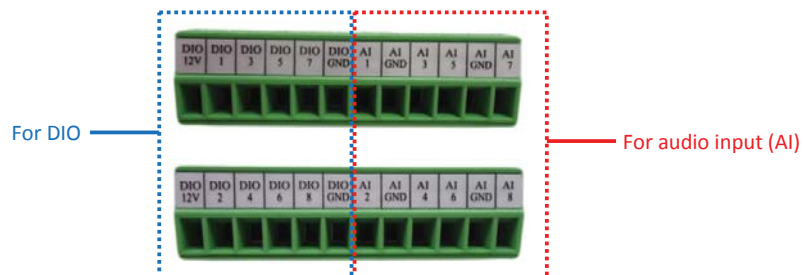
Connecting Audio Devices

Audio input / output devices, such as an active microphone or speaker can be connected to the encoder using the supplied terminal block.

Connecting an Audio Input Device

Each video channel has one audio input channel. The ports are labelled as **AI** followed with a number corresponding to the video channel.

Four (4) audio input ports share the same terminal block with four (4) DIO ports. For example, Audio port 1, 3, 5, and 7 are on the same terminal block with DIO ports 1, 3, 5, and 7. See samples below:



To connect an audio input device:

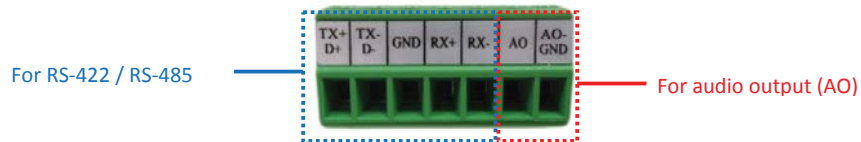
1. Loosen the screw of the pin and insert the wire through the pin slot.
2. Connect the wires of the audio input device to **AI** and **AI GND**.

NOTE: The **AI GND** pin may be mapped with more than one audio device.

3. Tighten the screws to secure the wires within the pin slot.

Connecting an Audio Output Device

The encoder has one audio output port. The audio output (AO) port shares the same terminal block with **RS-422 / RS-485 Port 1**.



NOTE: To ensure optimum performance, use active or powered speakers for audio out.

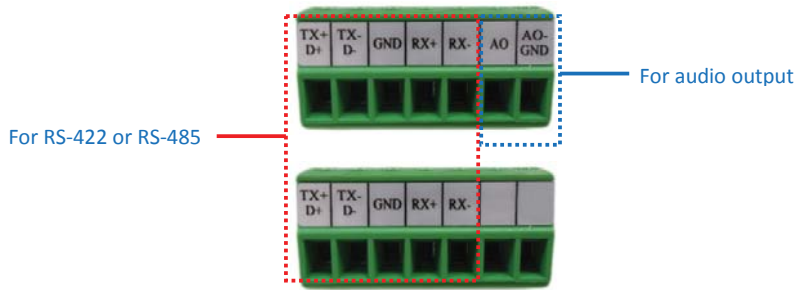
To connect an audio output device, do the following:

1. Loosen the screw of the pin and insert the wire through the pin slot.
2. Connect the wires of the audio output device to **AO** and **AO-GND**.
3. Tighten the screws to secure the wires within the pin slot.
4. Connect the speaker to a power source.

Connecting a Serial Device

The encoder can be connected to a camera with Pan-Tilt (PT) functions using the serial port connector, allowing the encoder to control the camera's pan and tilt using the RS-485 or RS-4522 ports. There are two (2) serial communication ports available on the encoder.

1. Loosen the screw of the pin and insert the wire through the pin slot.
2. Map the wires from the PT device to the encoder using the supplied terminal block according to one of the tables below.



Pin Label	RS-485 Connection		RS-422 Connection	
	Encoder Pin	PT Device Pin	Encoder Pin	PT Device Pin
RX-	-		RX -	TX -
RX+	-		RX +	TX +
GND	GROUND PIN			GROUND PIN
TX- / D-	TX -	DATA -	TX -	RX -
TX+ / D+	TX +	DATA +	TX +	RX +

NOTE: Consult the camera’s manual for proper wiring and labeling.



CAUTION: Incorrect wiring may cause damage to the connected devices.

DISCLAIMER: Digital Watchdog is not responsible for any damage caused by improper wiring.

3. Connect a ground wire to the **GND** terminal pin to complete the connection.
4. Tighten the screws to secure the wires within the pin slot.
5. Configure the serial communication settings on the Web Configurator.

Accessing the Encoder

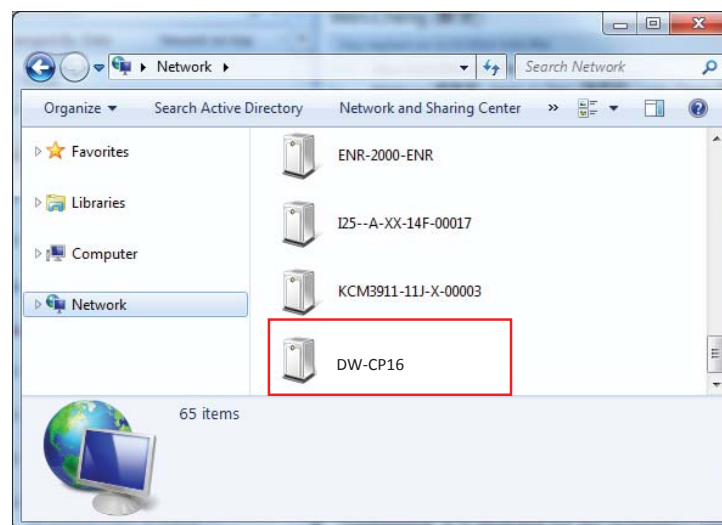
Configure the IP Addresses

In order to communicate with the encoder from your PC, both the encoder and the PC have to be in 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.

Using DHCP server to assign IP addresses:

If you have connected the computer and the encoder into a network that has a DHCP server running, you do not need to configure the IP addresses. In such case, the encoder will immediately be ready for the access from the PC. The encoder will be assigned all its network settings automatically to follow the current network's settings.

The quickest way to discover the encoders in the network is to use the UPnP function supported by the Compressor. Press the “Network” icon on your PC, and all the encoders on the local area network will be discovered by Windows.



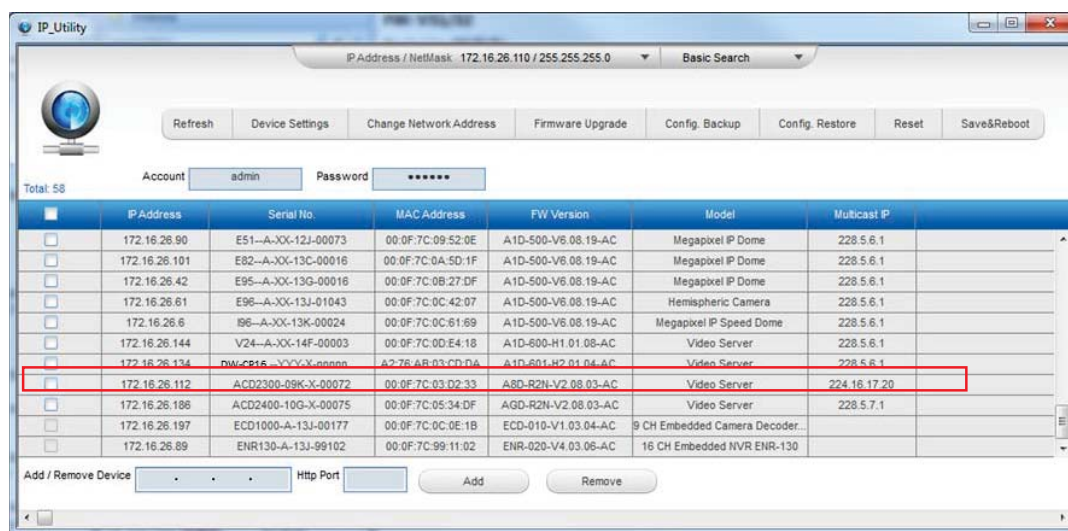
Double-click on the encoder model to launch the Compressor's web viewer automatically.



You may also discover and access your Compressor by using the **IP Utility** tool. The IP Utility is a light software tool that can discover the encoders, show their basic information such as IP and MAC addresses, serial numbers, firmware versions, etc., and allows quick configuration of multiple devices simultaneously.

The IP Utility can be downloaded for free from <http://www.digital-watchdog.com>

With just one click, you can launch the IP Utility:



You can locate the encoder model in the list. Click on the IP address to automatically launch the Compressor’s web viewer.

Compressor’s Default IP Address:

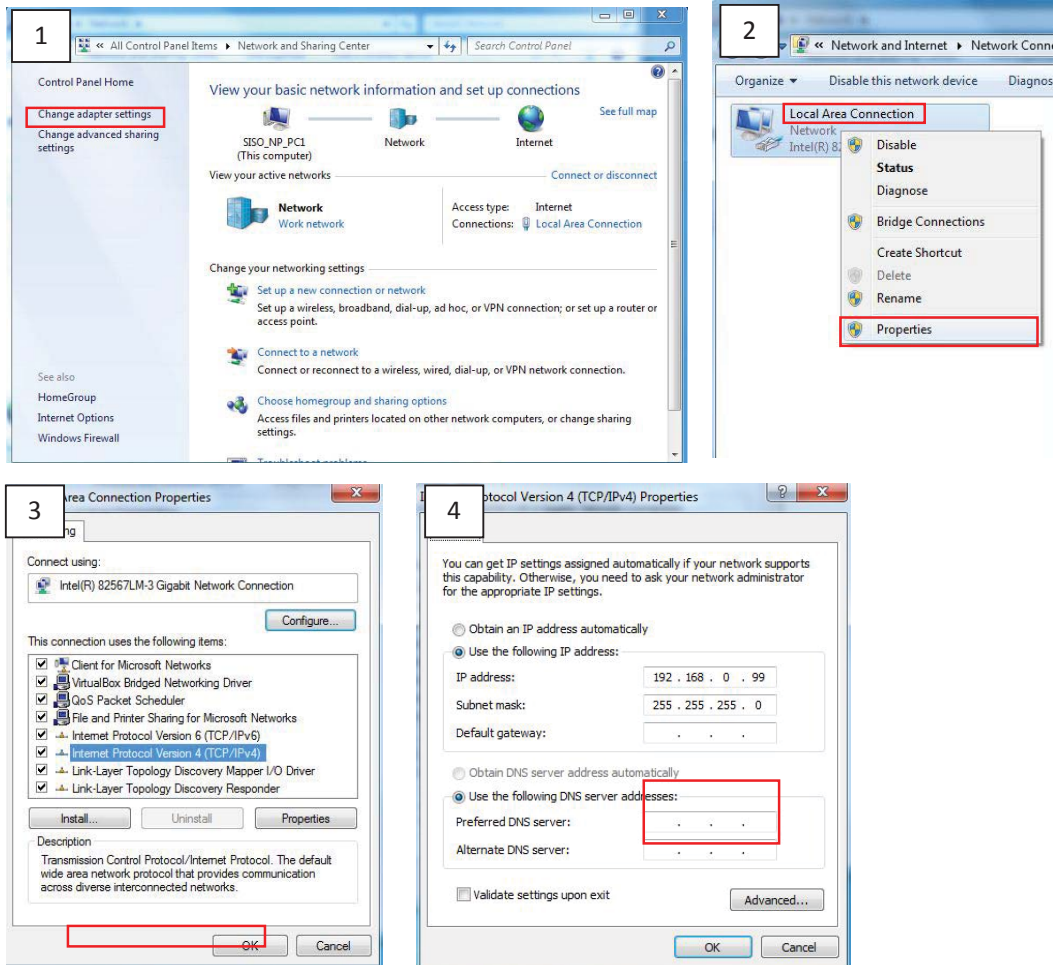
If there is no DHCP server in the given network, you may have to assign the IP addresses to the encoder manually.

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

192.168.0.100

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

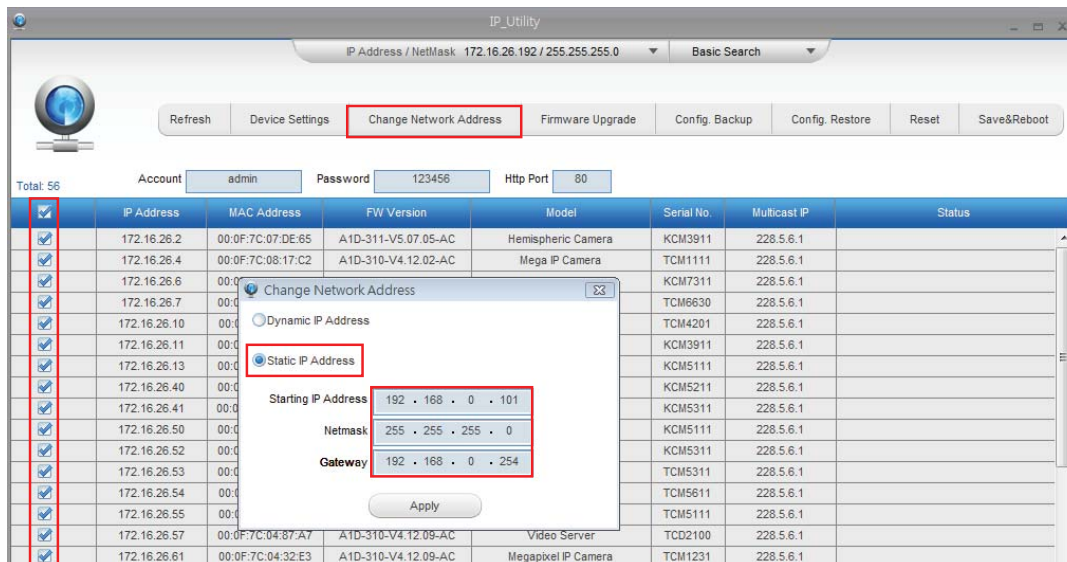
Manually adjust the IP address of the PC:





Manually adjust the IP addresses of multiple encoders:

If there are more than 1 encoder in the same local area network and there is no DHCP server, all of the encoders would then have the initial IP address of **192.168.0.100**. The easiest way to assign encoders the IP addresses is by using the **IP Utility**:



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

Press the “Refresh” button of the IP Utility to see the list of encoders with their new IP addresses.



Please note that it is also possible to change the IP addresses manually by using the Web browser, plugging in one encoder at a time, and changing its IP address using the Web browser.





Access the Encoder

You can use **any of the browsers** to access the encoder, 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 PC first to be able to get the live video feed from the encoder:

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

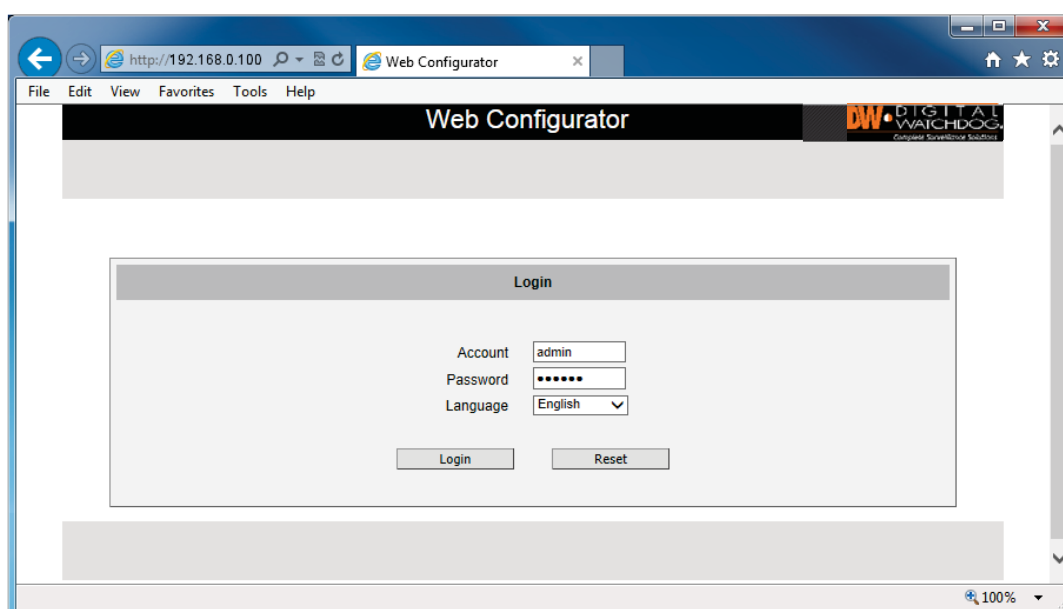
Disclaimer Notice: The encoder manufacturer does not guarantee the compatibility of its encoders with VLC player or QuickTime – since these are third party softwares. The third party has the right to modify their utility any time which might affect the compatibility. In such cases, please use Internet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



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

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

Upon successful connection to the encoder, 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 encoder 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 encoder.

Account: **Admin**

Password: **123456**





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	<ul style="list-style-type: none">› Windows XP with SP2 or above.› Windows 2003› Windows Vista› Windows 2008› Windows 7
Browser for Accessing Firmware	<ul style="list-style-type: none">› Internet Explorer 8.0 or newer (full functionality)› Safari 5.1.7 or newer with QuickTime installed (partial functionality)› Firefox 29.0 or newer or Chrome 34.0 or newer with Basic VLC Media Player (partial functionality)
Video Resolution	1024x768 or higher

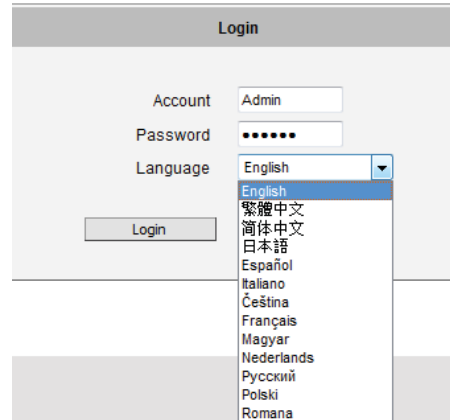
Live View

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.

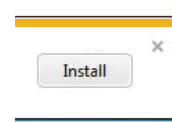
Login

Initially there is only an administrator's account in the device (**Default Account: Admin, Password: 123456**).


Feel free to choose your local language from the list of languages. After pressing "Login", you will be able to access the Compressor's web viewer.

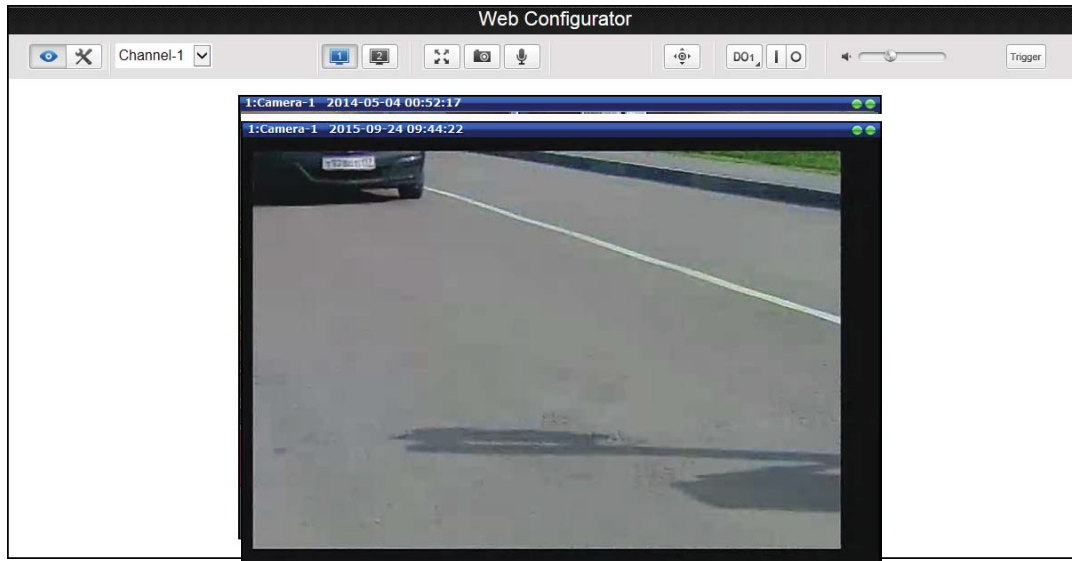


Once you login, the live view from connected cameras will be displayed. You may be prompted to install ActiveX files from the device. Live video will appear shortly after ActiveX is installed.



Live View

While in Live View, the Live View icon  will appear as being pressed. If you leave the Live View page, you can later return by pressing that button.



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

Select the channel to display on the Live View page by selecting the channel number from the channel list.



Dual Stream Capability

The Compressor supports dual streaming. The **Stream 1** is usually the high resolution stream with the purpose of being recorded by an NVR while **Stream 2** has lighter video configuration for live viewing, to reduce the computing power and bandwidth usage. Both streams can be configured under Web Viewer's Setup page. To alternate between the streams, press the corresponding buttons on the Live View page:



- Show Video from Stream 1



- Show Video from Stream 2

Full Screen Mode

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



- Full screen Mode

Press the **ESC** key to exit the full screen mode.

Image Capture

To capture a still image of the current live view, click the image capture button. The image will be saved in your local 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 (DO) controls allow users to manually trigger a DO device.




 - Select a Digital Output Port

Each DO port is 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. 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.

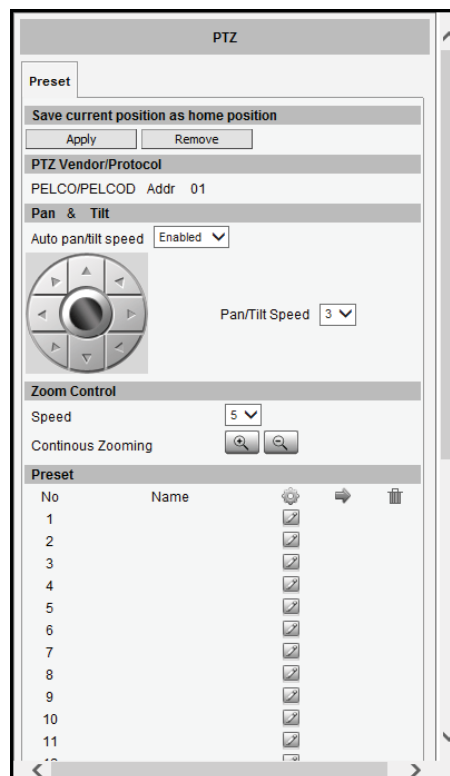
PTZ Control Panel

The PTZ Control Panel is used only on 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 45). Click the PTZ button on the Live View screen to display the PTZ Control Panel. On the PTZ Control Panel, users can do the following:

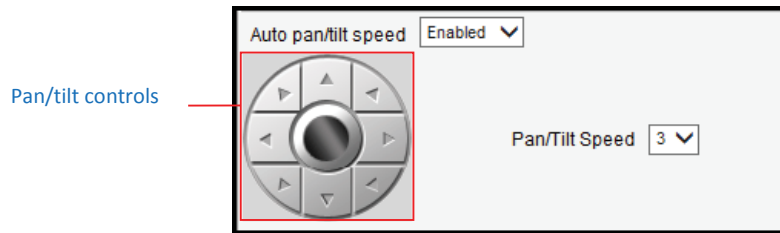
- Set home position
- View the PTZ Vendor/Protocol (can be set in *Serial Setting* on page 45)
- Pan the device
- Zoom the device in or out as well as adjust the zoom speed and step size
- Set the focus to auto refocus or manual
- Set Preset points

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 during movement. When “Disabled”, the pan/tilt speed follows the value selected on the **Pan/Tilt Speed** field.
- **Pan/Tilt Speed:** The bigger the number, the faster the speed is.

TIP: While the PTZ Control Panel is open, 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.

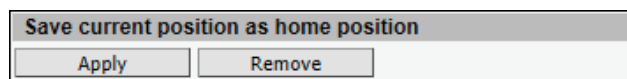
How to Zoom the Device In or Out



To zoom continuously, do the following:

1. On **Zoom Control**, select **Speed**. 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.



- Click the **Apply** button on the **Save current position as home position**.


How to Set Preset Points

Preset points are user-defined areas that the camera can zoom in to.

Preset				
No	Name			
1	1			
2	2			
3				
4				
5				

To create a preset point, do the following:

- On **Preset**, click the  icon to start creating a preset point.
- Under the **Name** field, type a preset point name.
- Pan, tilt, and zoom on the area that you want to set as the preset point.
- Once done, click the  icon again to close and complete the preset point.
- Repeat the above procedures to create more preset points.

To go to the preset point directly, click .

To delete the preset point, click .

Setup

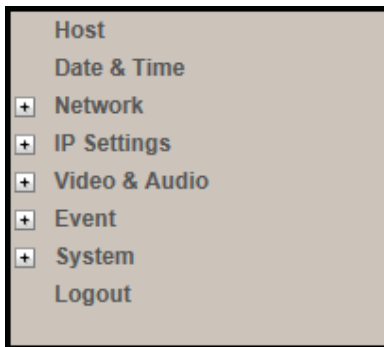
The following chapters guide you through the Setup functions of the device.

Access the Setup Page

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



- 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 depending on the actual capabilities of each device.*

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.

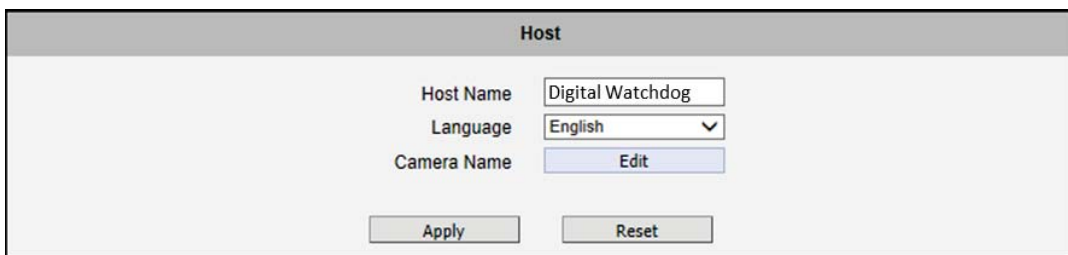
The following chapters of this manual explain each Setup item separately. The chapters are listed in the same order as the list of Setup menu items.

Host

Host The **Host** menu 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 language and set the name of a video channel.



The screenshot shows a web interface titled "Host". It contains three configuration fields: "Host Name" with a text input field containing "Digital Watchdog", "Language" with a dropdown menu set to "English", and "Camera Name" with an "Edit" button. At the bottom of the form are two buttons: "Apply" and "Reset".

Host Name: It is used to identify the device by a DHCP server. To include the Host Name in DHCP discovery packet sent from a device, go to **IP Settings** and make sure the device is in **Dynamic IP Address** mode and "Use host name" is checked.

Language: Select the user interface language.

Camera Name: Click the **Edit** button to configure the name of the cameras connected to the Compressor.



Camera Name			
Channel	Camera Name	Channel	Camera Name
1	Camera-1	2	Camera-2
3	Camera-3	4	Camera-4
5	Camera-5	6	Camera-6
7	Camera-7	8	Camera-8
9	Camera-9	10	Camera-10
11	Camera-11	12	Camera-12
13	Camera-13	14	Camera-14
15	Camera-15	16	Camera-16

Apply Reset

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** allows you to set the serial port configurations of the encoder. There are two serial ports that can be shared by the channels. The serial port on the connected devices must be the same as the configurations of the serial port on the encoder.

Serial Setting			
Serial Port	1	Serial Port	2
Serial Port Control	8,None,1	Serial Port Control	8,None,1
Serial Port Baud Rate	9600	Serial Port Baud Rate	9600
PTZ Vendor/Protocol	PELCO/PELCO	PTZ Vendor/Protocol	PELCO/PELCO
<input type="button" value="Apply"/>		<input type="button" value="Reset"/>	

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.

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

PTZ Vendor/Protocol: The Compressor 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.

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. All video channels share two (2) serial ports therefore the port number and PTZ address for each channel must be defined on this section.



Video Channel's PTZ Address					
Channel	Serial Port	PTZ Address	Channel	Serial Port	PTZ Address
1	1	0x01	2	1	0x02
3	1	0x03	4	1	0x04
5	1	0x05	6	1	0x06
7	1	0x07	8	1	0x08
9	2	0x09	10	2	0x0A
11	2	0x0B	12	2	0x0C
13	2	0x0D	14	2	0x0E
15	2	0x0F	16	2	0x10

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

Date & Time

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

There are two ways to adjust date and time – **automatically** by using an **NTP server**, or **manually**. If you are using a Network with no Internet access, use Manual adjustment mode.

Date Setting

SNTP/NTP Server

IP Address

Sync Time

Set Manually

Date / /

Time : :

Time Zone

Day Light Saving

Start Time

End Time

When choosing **SNTP/NTP Server**, enter the IP address of the NTP server and time interval for time synchronization. If using the domain name of an NTP server, make sure the DNS server has been set under IP Settings. To choose the most suitable NTP Server, refer to the worldwide pool of NTP Servers: <http://www.pool.ntp.org/en/>

When choosing **Set Manually** mode, adjust the date and time and **Time Zone** from the select box. If your location is not listed, pick a listed zone whose GMT is identical with your location.

When applicable, there is **Day Light Saving** function with two different types:

- **Type 1:** Start and end time of daylight savings is set by the **number of the week in the month** (First, Second, Third or Last week).
- **Type 2:** Start and end time of daylight savings is set by the **exact date of the month** (1-31).



Click **Apply** to save changes. The **Reset** button undoes changes that had been made but not applied.



Network

+ Network The **Network** menu provides 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

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

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



Select either **Allowed** or **Blocked** list to add items and **Enable** them with the checkbox in each row.



IP Address Filtering

Enabled

Set IP address

Blocked ▼ IP Address/Netmasks

NO.	IP address	Netmask	Enabled
1	0.0.0.0	0.0.0.0	<input type="checkbox"/>
2	0.0.0.0	0.0.0.0	<input type="checkbox"/>
3	0.0.0.0	0.0.0.0	<input type="checkbox"/>
4	0.0.0.0	0.0.0.0	<input type="checkbox"/>
5	0.0.0.0	0.0.0.0	<input type="checkbox"/>
6	0.0.0.0	0.0.0.0	<input type="checkbox"/>
7	0.0.0.0	0.0.0.0	<input type="checkbox"/>
8	0.0.0.0	0.0.0.0	<input type="checkbox"/>
9	0.0.0.0	0.0.0.0	<input type="checkbox"/>
10	0.0.0.0	0.0.0.0	<input type="checkbox"/>
11	0.0.0.0	0.0.0.0	<input type="checkbox"/>
12	0.0.0.0	0.0.0.0	<input type="checkbox"/>
13	0.0.0.0	0.0.0.0	<input type="checkbox"/>
14	0.0.0.0	0.0.0.0	<input type="checkbox"/>
15	0.0.0.0	0.0.0.0	<input type="checkbox"/>
16	0.0.0.0	0.0.0.0	<input type="checkbox"/>

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 the **Netmask** (Subnet Mask) allows you to filter a whole range of IP address. If you are unsure about the function of Netmask, use 255.255.255.255, to affect only a single IP address per line, 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 block your own IP address; you will not be able to access the device any more to undo the changes. If this happens by mistake, you can reset the hardware.



Port Mapping

Port Mapping The **Port Mapping** submenu provides a list of services and protocols that require their own port number for communication. 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.

Port Mapping

HTTP Port*	<input type="text" value="80"/>
HTTPS Port*	<input type="text" value="443"/>
Search Server Port1	<input type="text" value="6005"/>
Search Server Port2	<input type="text" value="6006"/>
Control Server Port	<input type="text" value="6001"/>
Streaming Server Port	<input type="text" value="6002"/>
RTSP Server Port	<input type="text" value="7070"/>

* New settings will only take effect after [Save & Reboot]

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

Port Name	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.



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 take effect after clicking **System > Save & Reboot**.



Multicast Setting

Multicast Setting

Multicast is an Internet protocol where a data stream is sent only once and shared to requesting devices to save network bandwidth. To use this, network devices, such as routers and switches, should support IP multicast.

Multicast Setting					
<input type="radio"/> Configuration setting is based on channel 1 <input checked="" type="radio"/> Manual					
Channel /Stream	Multicast IP [224.5.0.1 ~ 239.255.255.255]	Network Port [1025 ~ 65535]	Multicast TTL [1~255]	By Requests	
1	Stream 1	228.5.6.1	5100	16	<input checked="" type="checkbox"/>
	Stream 2	228.5.6.1	5200	16	<input checked="" type="checkbox"/>
	Audio	228.5.6.1	5300	16	<input checked="" type="checkbox"/>
2	Stream 1	228.5.6.2	5200	16	<input checked="" type="checkbox"/>
	Stream 2	228.5.6.2	5300	16	<input checked="" type="checkbox"/>
	Audio	228.5.6.2	5500	16	<input checked="" type="checkbox"/>
3	Stream 1	228.5.6.3	5200	16	<input checked="" type="checkbox"/>
	Stream 2	228.5.6.3	5300	16	<input checked="" type="checkbox"/>
	Audio	228.5.6.3	5500	16	<input checked="" type="checkbox"/>

The Multicast IP, port, and TTL are set to their default values but can be adjusted as needed.

Parameters	Description
Configuration setting is based on channel 1	Select to configure Channel 1 multicast settings and use these as a pattern to base the succeeding channel settings.
Manual	Select to manually configure the settings of all channels.
Channel (number)	Refers to the video channel.
Stream 1	Refers to the video stream 1 of the corresponding channel.
Stream 2	Refers to the video stream 2 of the corresponding channel.
Audio	Refers to the audio stream of the corresponding channel.
Multicast IP	Enter the multicast IP of the corresponding stream.
Network Port	Enter the assigned port of the corresponding stream.
Multicast TTL	Enter the multicast TTL (time-to-live) of the corresponding stream. This value determines the time span (in seconds) when the packet is retained in the



	network. When the time expires and no request is received, the packet is discarded.
By Request	<p>When checked, the video or audio stream will be streamed only to a particular receiver when that receiver sends a request or in the case of an NVR, selects to view or record the channel. If unchecked, the video or audio stream will constantly be streamed to the network whether there are devices viewing the channel or not.</p> <p>To save on network bandwidth, it is recommended to check this function.</p>

Scroll down the page and click the **Apply** button to save and apply the changes.

HTTPS

HTTPS protocol allows creating a secure channel over an insecure network to protect the data sent between the device and its counterpart. Two things are required for 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.

HTTPS

Certificate Signing Request (CSR) Management

Common Name

Certificate Management

Common Name

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 himself.

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

The new setting will only take effect after **Save & Reboot**.

SNMP Setting

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.

SNMP Setting

Enabled

SNMP V1 / V2

V1 Enabled
 Read Community:
 Write Community:

V2 Enabled

SNMP V3

Security Name:
 Password:
Must longer than 8 characters

Trap Enabled

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.

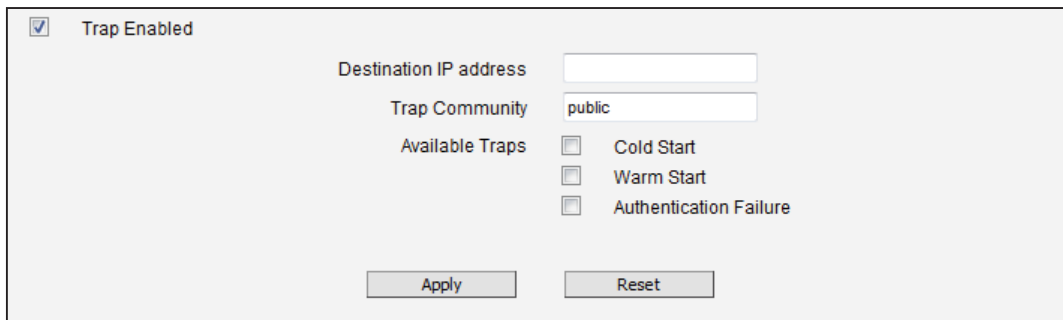
SNMP V1/V2 uses the “Community” name as password to authenticate identity. “Read Community” is the password for server to get information from devices. “Write Community” is the password for server to edit values on devices. The default is “public” for Read Community and “write” for Write Community. Of 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. You may now install and run the SNMP management software on the computer server.

SNMP Trap Usage:



Trap Enabled

Destination IP address

Trap Community

Available Traps

- Cold Start
- Warm Start
- Authentication Failure

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. <i>Ex: system description, system name.</i>
Interface	Provide general information from the physical interfaces. <i>Ex: interface speed, MAC address.</i>
Address Translation	Provide information about the mapping between network addresses and physical addresses for each physical interface <i>Ex: The IP/MAC addresses to connect to the managed device.</i>
IP	Provide the status and operation of Network Layer (Layer 3). <i>Ex: the information and traffic flow of received/delivered package.</i>
ICMP	Provide the status and statistics of ICMP. <i>Ex: amount of receive/error message of ICMP.</i>
TCP	Provide the status and operation of Transport Layer (Layer 4) using TCP protocol. <i>Ex: TCP Local Port, incoming/outgoing TCP segments.</i>
UDP	Provide the status and operation of Transport Layer (Layer 4) using UDP protocol. <i>Ex: UDP Local Port, in/out datagram.</i>
SNMP	Provide the related statistics through SNMP

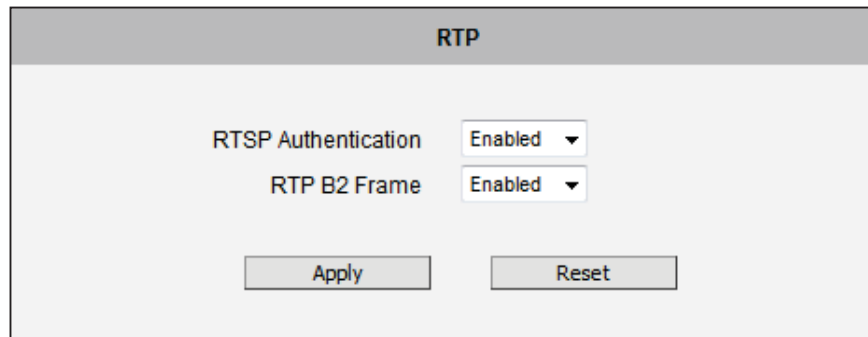
RTP



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.



RTP	
RTSP Authentication	Enabled ▾
RTP B2 Frame	Enabled ▾
Apply	Reset

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)

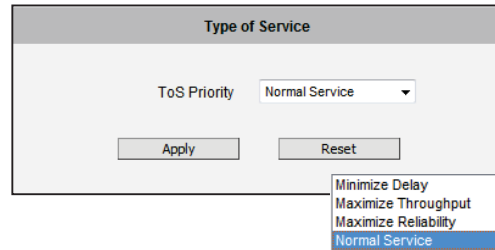
Network

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

- › Type of Service
- › UPnP
- › Bonjour
- › ONVIF

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**.



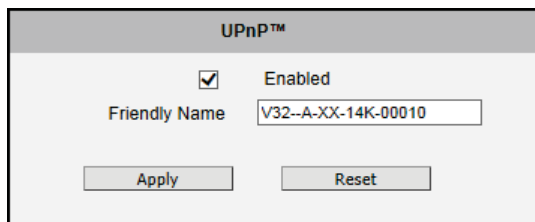
For special priority arrangement, there are three (3) more options:

- › 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™

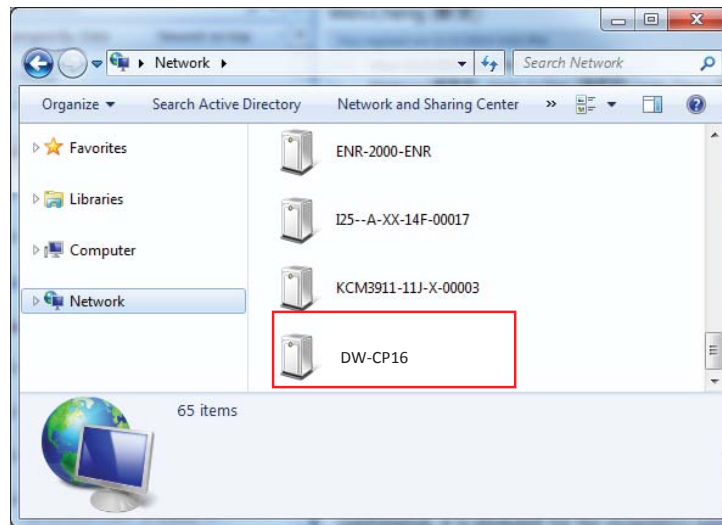
The **UPnP™** section provides the option to enable or disable the Universal Plug and Play capability of the device. Having the UPnP™ enabled allows other devices on the network to discover the Compressor on the network for convenient identification and access.



The **Friendly Name** 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.

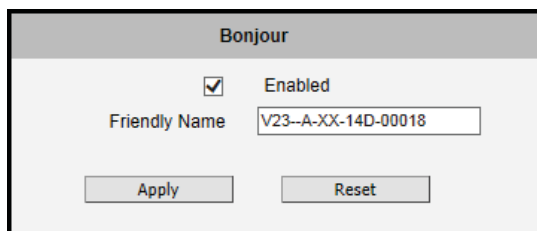
After changing any of the items above, click **Apply** to save the changes. The **Reset** button undoes the changes that had just been made but not applied yet.

Most Windows-based computers have the capability to discover the devices that support UPnP™.



Bonjour

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



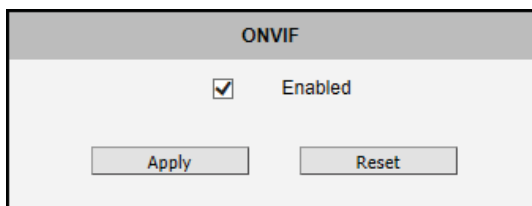
Similarly to UPnP, the **Friendly Name** can be defined by the user. That name will be displayed when the device is found in the network. By default, the Friendly Name is the serial number of the device; however, the user can modify the name according to the project needs.



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.

ONVIF

The **ONVIF** section provides the option to enable or disable the ability of the device to be discovered by the other network devices using the ONVIF protocol.



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

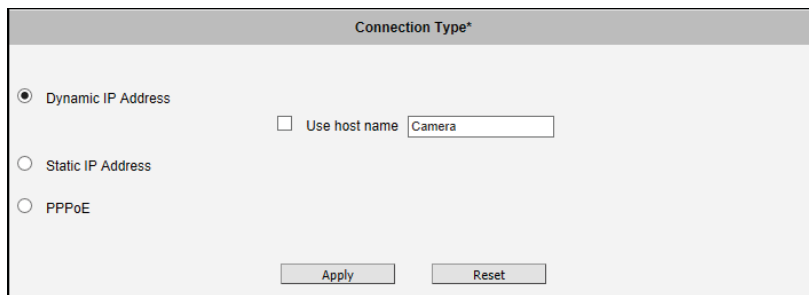
+ IP Settings

The **IP Settings** menu provides the options to define how the device would obtain its IP address and which DNS server it will connect to.

Connection Type

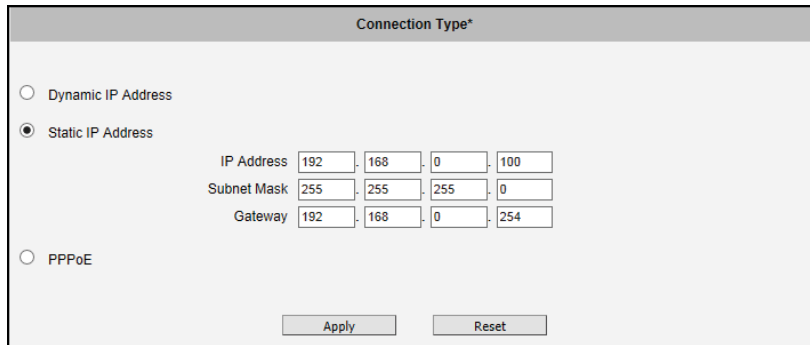
Connection Type

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, the device will automatically assign itself an IP address, listed under Static IP Address.

A screenshot of a web-based configuration interface titled "Connection Type*". It features three radio button options: "Dynamic IP Address" (which is selected), "Static IP Address", and "PPPoE". To the right of the "Dynamic IP Address" option, there is a checkbox labeled "Use host name" and a text input field containing the word "Camera". At the bottom of the form, there are two buttons: "Apply" and "Reset".

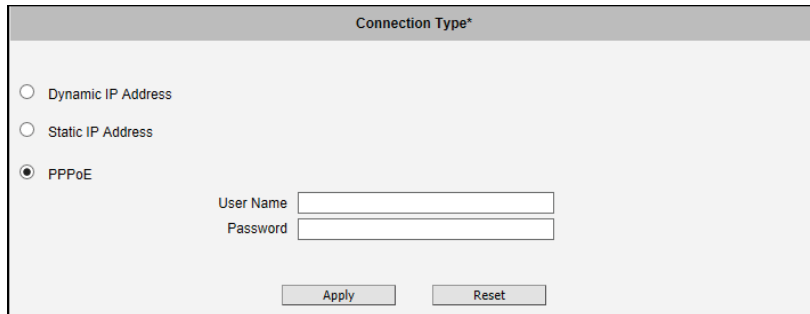
Host Name is used to identify the device by a DHCP server. In some networks with very strict security policy, it is required that all the network devices should have their host name, and when the devices attempt to access the network by requesting an IP address from a DHCP server, the DHCP server would 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.

If necessary, you can change the connection type to **Static IP Address** mode and manually modify the **IP Address**, **Subnet Mask** and **Gateway**.



The screenshot shows a web interface titled "Connection Type*" with three radio button options: "Dynamic IP Address", "Static IP Address" (which is selected), and "PPPoE". Under the "Static IP Address" option, there are three rows of input fields: "IP Address" with values 192, 168, 0, 100; "Subnet Mask" with values 255, 255, 255, 0; and "Gateway" with values 192, 168, 0, 254. At the bottom of the form are "Apply" and "Reset" buttons.

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**.



The screenshot shows the same "Connection Type*" web interface, but now the "PPPoE" radio button is selected. The "Dynamic IP Address" and "Static IP Address" options are unselected. Below the "PPPoE" option are two input fields labeled "User Name" and "Password". At the bottom are "Apply" and "Reset" buttons.

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**.

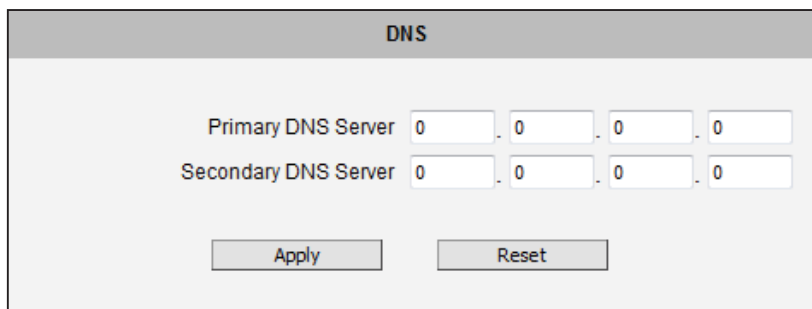
DNS

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

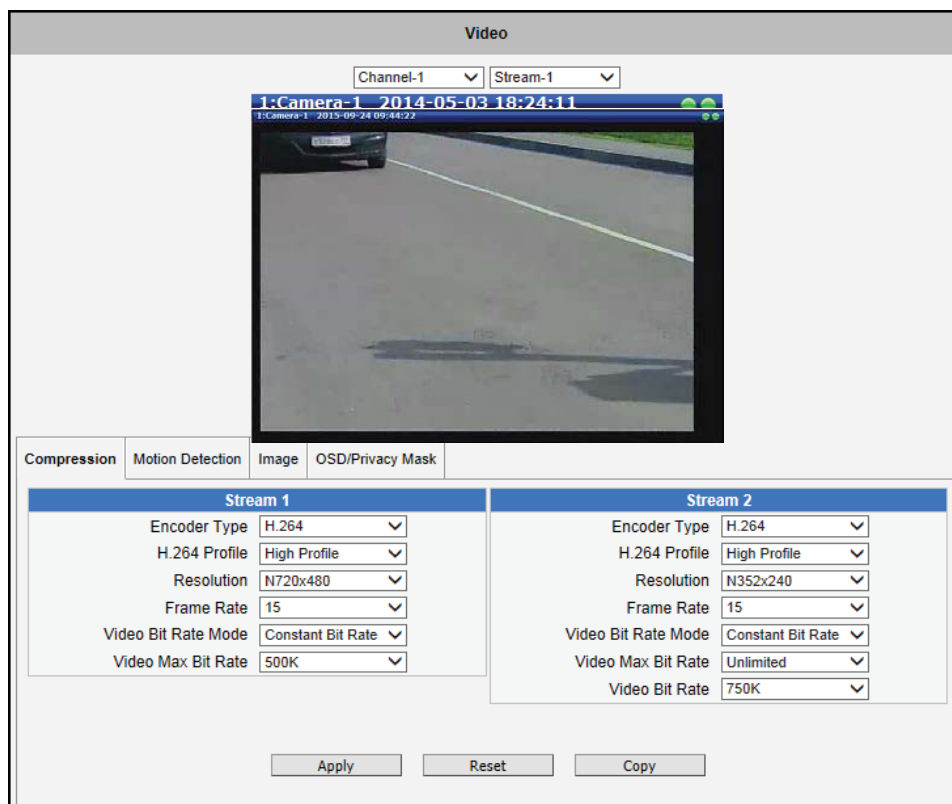
+ Video & Audio The **Video & Audio** menu provides the options to adjust the video quality, configure the streaming details of the device and audio settings.

The default settings of the device are sufficient for most environments and the video adjustments are not necessary. 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.

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. Users can select the channel to configure from the channel drop-down box and select which stream to display from the stream drop-down box.





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



Compression

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

Stream 1		Stream 2	
Encoder Type	H.264	Encoder Type	H.264
H.264 Profile	High Profile	H.264 Profile	High Profile
Resolution	N720x480	Resolution	N352x240
Frame Rate	15	Frame Rate	15
Video Bit Rate Mode	Constant Bit Rate	Video Bit Rate Mode	Constant Bit Rate
Video Max Bit Rate	500K	Video Max Bit Rate	Unlimited
		Video Bit Rate	750K
Apply		Reset	

Parameters	Description
Encoder Type	There are two encoder types available: H.264 (High Profile) and MJPEG .
H.264 Profile	<p>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 requires more computing power.</p> <p>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.</p>
Resolution	The default resolution setting of the device may not necessarily be the maximum resolution of the camera. 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 <i>(H.264 Only)</i>	Under Constant Bit Rate mode (CBR), the device keeps the stable bitrate regardless of the complexity of the scene. 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.



	<p>Under Variable Bit Rate mode (VBR), the device will keep the video quality stable while the bit rate goes up or down, depending on the complexity of the scene.</p>
<p>Video Max Bit Rate <i>(H.264 Only)</i></p>	<p>Defines the upper limit of the bitrate (if CBR mode is selected). The bitrate will be floating slightly under that limit.</p> <div data-bbox="589 506 911 611" style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p>Video Bit Rate Mode Constant Bit Rate ▾ Video Max Bit Rate Unlimited ▾ Video Bit Rate 2M ▾</p> </div> <p>If the Video Max Bit Rate is chosen as Unlimited, the Video Bit Rate selection box will define the bit rate level.</p>
<p>Video Bit Rate <i>(H.264 Only)</i></p>	<p>Under CBR mode, when Video Max Bit Rate is chosen Unlimited, the user can define the AVERAGE bit rate. This mode allows the most accurate storage estimations, however, while planning the bandwidth, please consider the occasional peaks of bit rate.</p>
<p>Quality</p>	<p>H.264 Compression:</p> <div data-bbox="589 1045 932 1157" style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p>Video Bit Rate Mode Variable Bit Rate ▾ Quality Medium ▾ GOP 1 I-frame / 1 Second ▾</p> </div> <p>Under VBR mode, the bit rate will be floating while the video quality will be stable. The user can choose either High, Medium or Low quality. The higher the quality level, the more bit rate the device will use to achieve the target quality.</p> <p>MJPEG Compression:</p> <p>The user can define the quality from 1 to 100. The default MJPEG quality is 60. The higher the quality level, the more bit rate the device will use to achieve the target quality.</p>
<p>GOP 1 I-frame <i>(H.264 Only)</i></p>	<p>The GOP length 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. 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 a static scene, long GOP can reduce bandwidth and storage consumption.</p>



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 Stream 1. By default, all the regions are disabled. To start, select the channel from the drop-down box to set its motion detection.

Runtime MD Profile ▾

Region	Enabled	Sensitivity	Trigger Interval [s]	Trigger Threshold
1	<input type="checkbox"/>	70 ▾	1 ▾	1 ▾ %
2	<input type="checkbox"/>	70 ▾	1 ▾	1 ▾ %
3	<input type="checkbox"/>	70 ▾	1 ▾	1 ▾ %

Setup

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

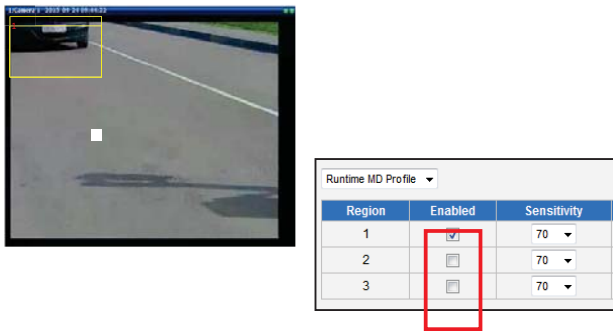
NOTE: Microsoft Internet Explorer browser is required to configure the motion detection regions.

There are three independently configurable motion detection regions. Each motion detection 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 motion detection regions can be enabled or disabled individually.



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. 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 be as big as the whole screen.



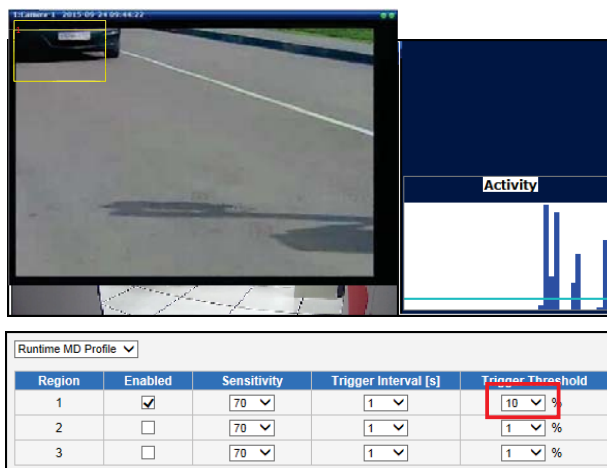
Sensitivity

In order to avoid false alarms, we might want the device be able to ignore small motion. The higher the sensitivity level, the smaller shift of the object is needed to trigger the alarm. For example, if the object 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. 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

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. You may notice that at certain moment the tallest bars in the activity graph reached about 25% – it means 25% of this motion detection area were filled with moving pixels at that moment.












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. Since we want to have a real alarm in case of human or vehicle passing by while ignoring birds, cats, 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.**

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: 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 the threshold value be if you want the same objects to trigger motion.



Trigger interval

Trigger interval is the time period from the beginning of the triggered event during which all other motion activities are ignored by the device. This is designed to avoid needless repetitive reporting of the same intrusion. Trigger interval 20 seconds means that when the even happens, the device will take a one-time action and ignore the continuing activity in the motion 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.

Profile of Motion Detection

Think of them as **Profile 1** (Runtime MD Profile) and **Profile 2** (Event MD Profile). You can configure two independent groups

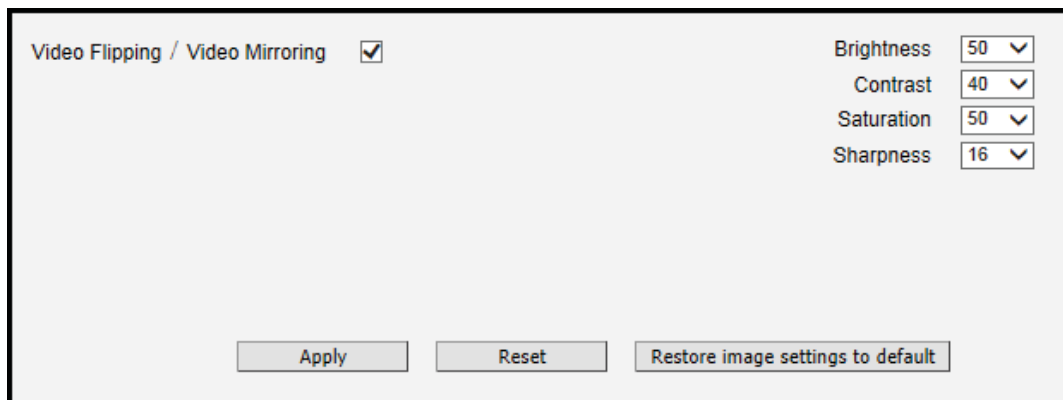
Runtime MD Profile	Event MD Profile	Enabled	Sensitivity
1		<input checked="" type="checkbox"/>	70
2		<input type="checkbox"/>	70
3		<input type="checkbox"/>	70

of Motion Detection regions with 3 regions per group. Normally, the Profile 1 (Runtime MD Profile) is used as an active profile. It is possible to switch to Profile 2 by using the Event Handler system. For example, you might want to have different motion detection parameters for day and night time.

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 the video image.



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 text will be embedded into video and cannot be removed later upon playback or export.
2. Mask sensitive areas of the video that should not be captured by the camera, such as manager’s computer screen or bathroom entrance with a **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, the texts will appear one below another, row by row.

Region	Enabled	Color	Background	Transparent	Position	Format of Texts
1	<input checked="" type="checkbox"/>	[Color]	[Background]	50	Top	Office View %YYYY%MM%DD
2	<input type="checkbox"/>	[Color]	[Background]	0	Top	
3	<input type="checkbox"/>	[Color]	[Background]	0	Top	
4	<input type="checkbox"/>	[Color]	[Background]	0	Top	

Buttons: Apply, Reset

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)

Press **Apply** to save the changes. The **Reset** button undoes changes made but not applied yet.

Privacy Mask

The **Privacy Mask** section allows the user to mask 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 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.

Privacy Mask ▾

Region	Enabled	Color	Setup
1	<input checked="" type="checkbox"/>	<div style="background-color: #90ee90; width: 20px; height: 10px; display: inline-block;"></div> ▾	<input checked="" type="checkbox"/>
2	<input type="checkbox"/>	<div style="background-color: black; width: 20px; height: 10px; display: inline-block;"></div> ▾	<input type="checkbox"/>
3	<input type="checkbox"/>	<div style="background-color: black; width: 20px; height: 10px; display: inline-block;"></div> ▾	<input type="checkbox"/>
4	<input type="checkbox"/>	<div style="background-color: black; width: 20px; height: 10px; display: inline-block;"></div> ▾	<input type="checkbox"/>

NOTE: 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 mask can be used for resizing the region.

There are 4 pre-defined color options for privacy masks. To use any other colors, use URL commands to set up the privacy mask. Refer to the Guide that explains the use of URL commands.

For PTZ device models, the privacy mask is dynamic. Thus, when the device pans away from the mask's position, the region remains covered for privacy. You can select one color for all 4 privacy masks.

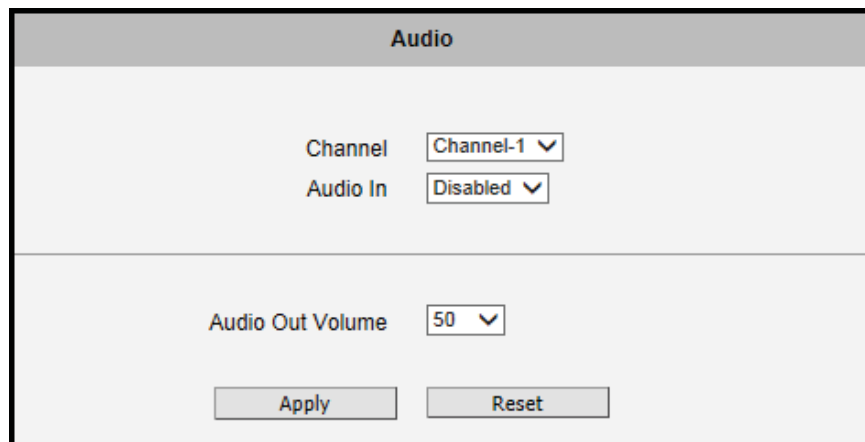
Please note that the Privacy Masks will take effect for both Stream 1 and Stream 2.

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!**

Audio

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



Parameters	Description
Channel	Select the video channel to adjust its audio settings.
Audio In	<p>The option “Enabled” would activate incoming audio. In this case, Audio In Level and Audio In Format options appear. Select the volume level and format to use.</p> <div style="border: 1px solid black; padding: 5px; width: fit-content; margin: 10px auto;"> <p>Channel <input type="text" value="Channel-1"/></p> <p>Audio In <input type="text" value="Enabled"/></p> <p>Audio In Level <input type="text" value="55"/></p> <p>Audio In Format <input type="text" value="G711A"/></p> </div> <p>The option “Disabled” would turn off the incoming audio. In such case, the video stream is captured without audio.</p>
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 Compressor responds to events. 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 server 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.***

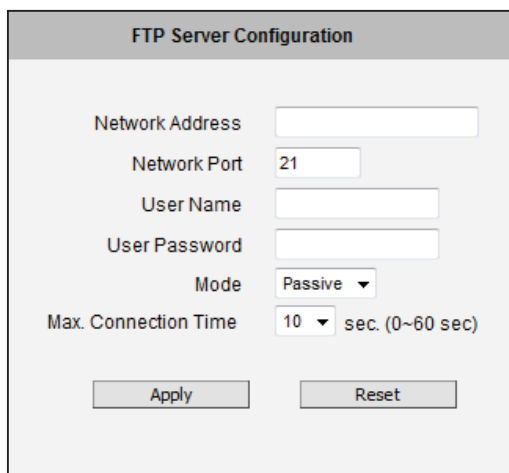
Event servers are classified as FTP servers, SMTP servers and HTTP servers

Event Server			
Type	Network Address	Ports	User Name
FTP Server Configuration	none	21	none
SMTP Server Configuration	none	none	none
HTTP Server 1 Configuration	none	80	none
HTTP Server 2 Configuration	none	80	none



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.

A screenshot of the 'FTP Server Configuration' dialog box. The dialog has a title bar with the text 'FTP Server Configuration'. Below the title bar, there are several fields and controls: 'Network Address' with an empty text input field; 'Network Port' with a text input field containing '21'; 'User Name' with an empty text input field; 'User Password' with an empty text input field; 'Mode' with a dropdown menu showing 'Passive'; and 'Max. Connection Time' with a dropdown menu showing '10' and the text 'sec. (0~60 sec)'. At the bottom of the dialog, there are two buttons: 'Apply' and 'Reset'.

To setup FTP servers, make sure to enter the **Network Address** of FTP server, the **Network (FTP) Port**, 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.

SMTP Server Configuration ✖

Primary SMTP Configurations

Enabled

Authentication Type Auto ▾

User Name

User Password

Sender Email Address

Network Address

Network Port 25

Max. Connection Time 10 ▾ sec. (0~300 sec)

Secondary SMTP Configurations

Enabled

Authentication Type Auto ▾

User Name

User Password

Sender Email Address

Network Address

Network Port 25

Max. Connection Time 10 ▾ sec. (0~300 sec)

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 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 example, 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.

The screenshot shows a configuration window titled "HTTP Server Configuration - 1". It contains the following fields and controls:

- Enabled:** A checkbox that is currently unchecked.
- User Name:** A text input field.
- User Password:** A text input field.
- Network Address:** A text input field.
- Network Port:** A text input field containing the value "80".
- Max. Connection Time:** A dropdown menu set to "10" with the unit "sec. (0~60 sec)".
- Buttons:** "Apply" and "Reset" buttons at the bottom.

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).

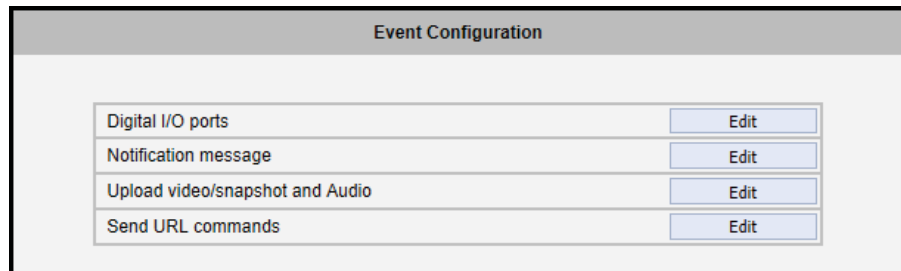


After changing any of the items above, click **Apply** to save the changes. The **Reset** button undoes the changes that had just been made but not applied yet.

Event Configuration

Event configuration are the responses to be performed when an event is triggered. For most types of responses, you can create several different 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 (DI) device is a trigger device like a switch or sensor (e.g. “panic button”), which when triggered, notifies the device to perform specific actions or the Digital Output (DO) device to respond. DO’s can be alarms or lights, etc.

The Digital I/O Ports page displays the number of available DIO ports on the device.



Digital I/O ports							
Port	I/O	Channel				Active Level	Interval (0-86400 seconds)
1	DO ▼	1 <input checked="" type="checkbox"/>	2 <input checked="" type="checkbox"/>	3 <input checked="" type="checkbox"/>	4 <input checked="" type="checkbox"/>	0 ▼	<input type="text" value="0"/>
		5 <input checked="" type="checkbox"/>	6 <input checked="" type="checkbox"/>	7 <input checked="" type="checkbox"/>	8 <input checked="" type="checkbox"/>		
		9 <input checked="" type="checkbox"/>	10 <input checked="" type="checkbox"/>	11 <input checked="" type="checkbox"/>	12 <input checked="" type="checkbox"/>		
		13 <input checked="" type="checkbox"/>	14 <input checked="" type="checkbox"/>	15 <input checked="" type="checkbox"/>	16 <input checked="" type="checkbox"/>		
2	DO ▼	1 <input checked="" type="checkbox"/>	2 <input checked="" type="checkbox"/>	3 <input checked="" type="checkbox"/>	4 <input checked="" type="checkbox"/>	0 ▼	<input type="text" value="0"/>
		5 <input checked="" type="checkbox"/>	6 <input checked="" type="checkbox"/>	7 <input checked="" type="checkbox"/>	8 <input checked="" type="checkbox"/>		
		9 <input checked="" type="checkbox"/>	10 <input checked="" type="checkbox"/>	11 <input checked="" type="checkbox"/>	12 <input checked="" type="checkbox"/>		
		13 <input checked="" type="checkbox"/>	14 <input checked="" type="checkbox"/>	15 <input checked="" type="checkbox"/>	16 <input checked="" type="checkbox"/>		
3	DI ▼	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	0 ▼	<input type="text" value="0"/>
		5 <input type="checkbox"/>	6 <input type="checkbox"/>	7 <input type="checkbox"/>	8 <input type="checkbox"/>		
		9 <input type="checkbox"/>	10 <input type="checkbox"/>	11 <input type="checkbox"/>	12 <input type="checkbox"/>		
		13 <input type="checkbox"/>	14 <input type="checkbox"/>	15 <input type="checkbox"/>	16 <input type="checkbox"/>		
4	DI ▼	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	0 ▼	<input type="text" value="0"/>
		5 <input type="checkbox"/>	6 <input type="checkbox"/>	7 <input type="checkbox"/>	8 <input type="checkbox"/>		
		9 <input type="checkbox"/>	10 <input type="checkbox"/>	11 <input type="checkbox"/>	12 <input type="checkbox"/>		
		13 <input type="checkbox"/>	14 <input type="checkbox"/>	15 <input type="checkbox"/>	16 <input type="checkbox"/>		
5	DO ▼	1 <input checked="" type="checkbox"/>	2 <input checked="" type="checkbox"/>	3 <input checked="" type="checkbox"/>	4 <input checked="" type="checkbox"/>	0 ▼	<input type="text" value="0"/>
		5 <input checked="" type="checkbox"/>	6 <input checked="" type="checkbox"/>	7 <input checked="" type="checkbox"/>	8 <input checked="" type="checkbox"/>		
		9 <input checked="" type="checkbox"/>	10 <input checked="" type="checkbox"/>	11 <input checked="" type="checkbox"/>	12 <input checked="" type="checkbox"/>		
		13 <input checked="" type="checkbox"/>	14 <input checked="" type="checkbox"/>	15 <input checked="" type="checkbox"/>	16 <input checked="" type="checkbox"/>		
6	DO ▼	1 <input checked="" type="checkbox"/>	2 <input checked="" type="checkbox"/>	3 <input checked="" type="checkbox"/>	4 <input checked="" type="checkbox"/>	0 ▼	<input type="text" value="0"/>
		5 <input checked="" type="checkbox"/>	6 <input checked="" type="checkbox"/>	7 <input checked="" type="checkbox"/>	8 <input checked="" type="checkbox"/>		
		9 <input checked="" type="checkbox"/>	10 <input checked="" type="checkbox"/>	11 <input checked="" type="checkbox"/>	12 <input checked="" type="checkbox"/>		
		13 <input checked="" type="checkbox"/>	14 <input checked="" type="checkbox"/>	15 <input checked="" type="checkbox"/>	16 <input checked="" type="checkbox"/>		

These DIO ports can be configured to either DI or DO on the **I/O** column. Check the channel number box on the **Channel** column to assign a video channel for that port.

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.

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.

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.

By default, the **Active Level** of each port is “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 messages. 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.



Notification message

Notification message 1

Send message to: HTTP CGI 1 Test

CGI Path & Program *
including path of CGI program

URL Command

Message *

Notification message 2

Send message to: E-Mail Test

E-Mail Recipients *
using ";" for multiple addresses

Subject *

Message *

Notification message 3

* : Fields must be filled in

To setup Notification Messages, make sure to enable the message and 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.

Upload video/snapshot and Audio

Upload video/snapshot and Audio 1

Upload Media Type Snapshot Video Test

Upload Media To E-Mail ▼

Upload Period 0 (0~86400 seconds)

Images during Upload Period 0
(Use 0 for maximum number of images)

Image File Name
[naming rule](#)

E-Mail Recipients
using ; for multiple addressed

Subject

Video Source 1 ▼

Upload video/snapshot and Audio 2

Upload video/snapshot and Audio 3

Apply Reset

The parameters needed to setup this function are different for each task combination, as seen below:

Enable						UI
						Upload video/snapshot and Audio 1 <input checked="" type="checkbox"/>
Upload Media Type	Snapshot					Upload Media Type <input checked="" type="radio"/> Snapshot <input type="radio"/> Video
Upload Media to	Email	FTP	CGI	FTP	CGI	Upload Media To E-Mail ▼
Pre-Buffer Time				Y	Y	Pre-Buffer Time 0 ▼ (0~10 Second)
Upload Period	Y	Y	Y	Y	Y	Upload Period 0 (0~86400 seconds)



Image during Upload Period	Y	Y	Y				Images during Upload Period <input type="text" value="0"/> (Use 0 for maximum number of images)
Image File Name	Y	Y	Y		Y	Y	Image File Name <input type="text" value="Front_Door_%YYYY_%MM_%DD"/>
Upload Path		Y			Y		Upload Path <input type="text" value="Camera/%N"/>
CGI Path & Program			Y			Y	CGI Path & Program <input type="text"/>
E-Mail Recipients	Y						E-Mail Recipients <input type="text"/> using ; for multiple addressed
Subject	Y						Subject <input type="text" value="Front Door Snapshot"/>
Video Source	Y	Y	Y		Y	Y	Video Source <input type="text" value="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.

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.

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.

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 with 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: stream 1 or stream 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	1, 2, 3, 4, 5,...

Send URL commands

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

Send URL commands

Send Command 1 to HTTP CGI 1

Command as event is triggered /cgi-bin/cmd/encoder?PTZ_PRESET_GO=1
including path of CGI program [max. 119 characters]

Command as event becomes inactive /cgi-bin/cmd/encoder?PTZ_PRESET_GO=2
including path of CGI program [max. 119 characters]

Send Command 2 to HTTP CGI 1

Command as event is triggered /cgi-bin/cmd/encoder?VIDEO_BITRATE=3M&V/I
including path of CGI program [max. 119 characters]

Command as event becomes inactive /cgi-bin/cmd/encoder?VIDEO_BITRATE=1M&V/I
including path of CGI program [max. 119 characters]

Send Command 3 to HTTP CGI 1

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 triggered, 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.

Event List					
Channel-1 ▾					
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”.

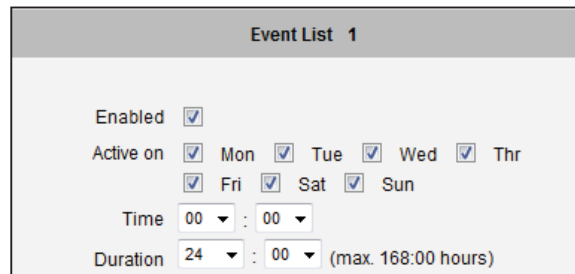
There are several parts to the Event rule:

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.

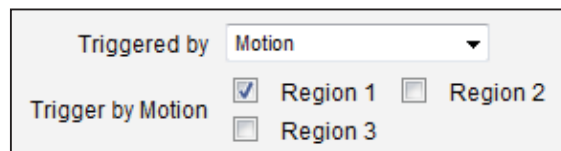


The screenshot shows the configuration for 'Event List 1'. It includes the following settings:

- Enabled:
- Active on: Mon Tue Wed Thr Fri Sat Sun
- Time: 00 : 00
- Duration: 24 : 00 (max. 168:00 hours)

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.



The screenshot shows the configuration for 'Triggered by'. It includes the following settings:

- Triggered by: Motion
- Trigger by Motion: Region 1 Region 2 Region 3

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 occurrence in **Occur Every** (minutes).

DIs: The device is 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.

Video Loss: This event is triggered when the analog video input is disconnected, which makes the video status as "lost". The video status returns to "normal" when the device receives the analog video signal. A common scenario is for the encoder to send an email to the administrator when the video signal is lost, and activate the DO signal to alarm that persists until the analog signal is restored.



Video Recovery: This event is triggered when the analog video input is detected by the encoder. A common scenario is for the encoder to activate a DO signal such as a light to indicate that video is being viewed.



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.

Response To	<input type="checkbox"/>	Send notification message
	<input type="checkbox"/>	Upload video/snapshots
	<input type="checkbox"/>	Change Motion Detection Profile
	<input type="checkbox"/>	Send URL command

Digital Output: Click to include a digital output as a response when an event is triggered. Check the box of the digital output.

Send notification Message: Select from the three pre-defined messages which you have 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.

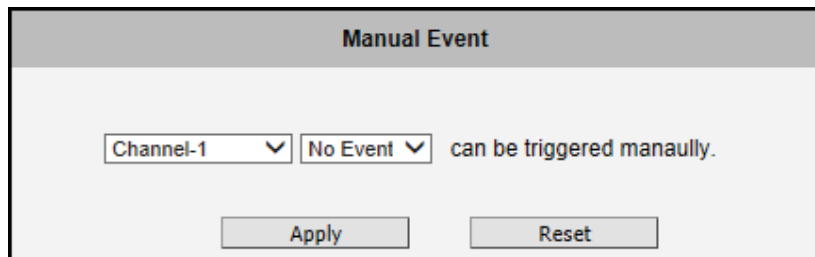
Change Motion Detection profile: This will switch the profile of the selected Motion Detection region from Runtime profile to Event profile. The profile will return to runtime settings at the end of this event. You may program one motion detection region to be disabled at runtime, but enable it with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

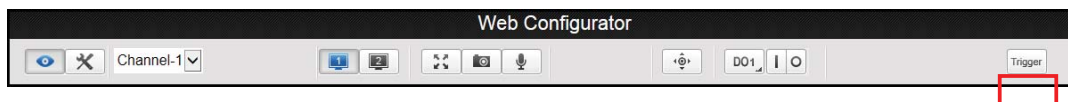
You may select one event per channel in the Manual Event section to be triggered via web user interface.



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:





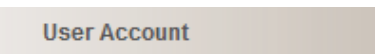


System



The **System** menu provides the list of functions that help manage the Compressor. The [+] mark 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 administrator account.
2. Create up to 10 common users with access for live view and PTZ control.
3. Enable or disable seeing live view without a user name and password (anonymous login), which is convenient for device installers on the field. For security reasons, account name and password is always required when entering the setup page or when using URL commands.

User Account

Live view without account name and password

User	Account	Password
Root	admin	123456
User 1		
User 2		
User 3		
User 4		
User 5		
User 6		
User 7		
User 8		
User 9		
User 10		

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 the Compressor’s status, settings and log. This information is helpful while doing device configuration, maintenance or troubleshooting.

System Information

System Information :

Firmware Version = A1D-600-H1.00.07-AC
 MAC Address = 00:0F:7C:0D:71:8B
 Production ID = V21--A-XX-14D-00018
 Model Number = V21
 Factory Default Type = Two Ways Audio (0x71)
 Company Name
 WEB Site
 PTZ_IV

WAN Status :

WAN_TYPE='1'
 WAN_IP='172.16.26.153'
 WAN_NETMASK='255.255.255.0'
 WAN_GATEWAY='172.16.26.253'
 DNS_PRIMARY='172.16.5.19'
 DNS_SECONDARY='172.16.5.20'
 MAC='00:0F:7C:0D:71:8B'
 BONJOUR_CONFIG='1,V21--A-XX-14D-00018'

System Log :

Mount Filesystem ...
 Bootloader Version Bootloader-600-H1.00.05
 Loading Drivers ...
 Starting Debug Service ...
 Starting Network Interface ...
 Starting WanDaemon ...
 Initial System Time Manager ...
 Start Streaming Server ...

Config file:

The unit's parameters and their current settings. Parameter List

Always attach the server report when contacting your support channel. Server Report

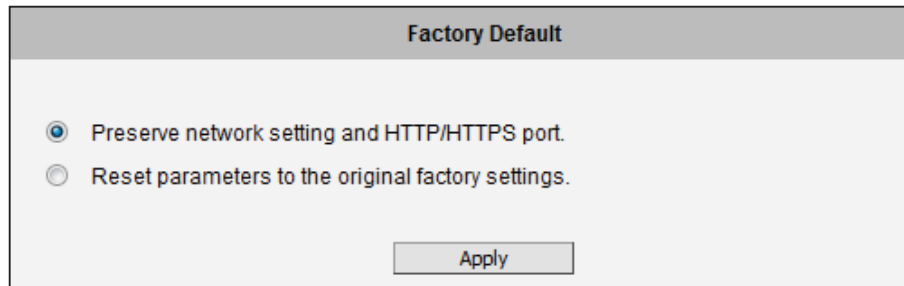
Third party software licenses. Show License

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** submenu allows the device settings be reset to the original factory settings.



The screenshot shows a web interface titled "Factory Default". It contains two radio button options: "Preserve network setting and HTTP/HTTPS port." (which is selected) and "Reset parameters to the original factory settings." Below the options is an "Apply" button.

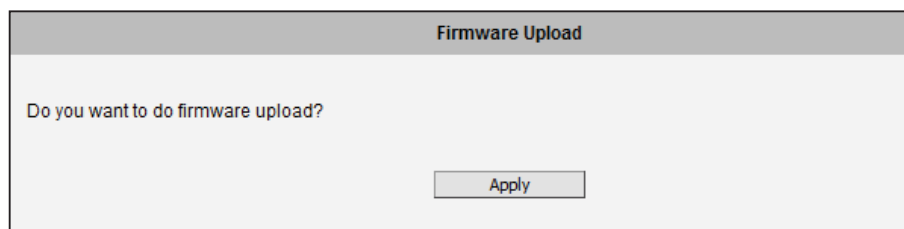
If you want to keep network settings and restore other settings to factory default, select the first option. The second reset option will erase all the settings and restore them to their factory default.

Firmware Upload

Firmware Upload

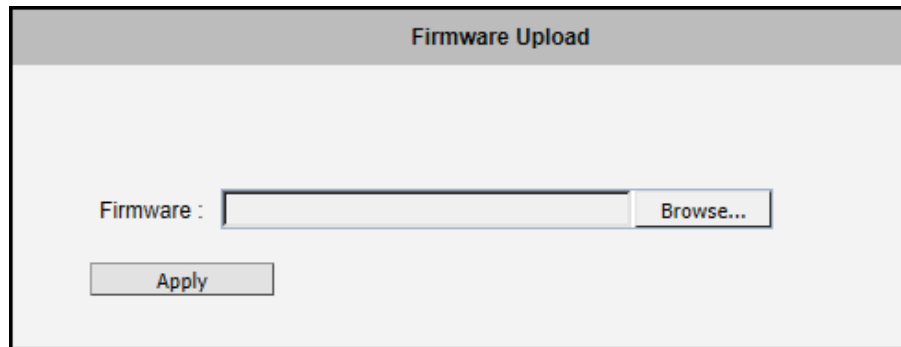
The **Firmware Upload** submenu allows remote upgrade or downgrade of the Compressor’s firmware.

The firmware image file can be downloaded from www.digital-watchdog.com website. It has the file extension “.upg”.



The screenshot shows a web interface titled "Firmware Upload". It contains a confirmation question: "Do you want to do firmware upload?". Below the question is an "Apply" button.

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.

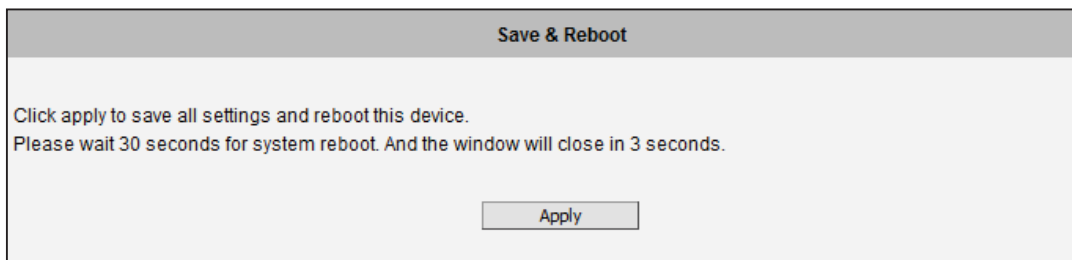


Click **Browse** to select the upload image file. Click the **Apply** button to start the upload.

Once the process is finished, you will get an **OK** message and system will reboot itself.

Save & Reboot

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

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.



Headquarters Office: 5436 W Crenshaw St, Tampa, FL 33634
Sales Office: 16220 Bloomfield Ave., Cerritos, California, USA 90703
PH: 866-446-3595 | FAX: 813-888-9262
www.Digital-Watchdog.com
technicalsupport@dwcc.tv
Technical Support PH:
USA & Canada 1+ (866) 446-3595
International 1+ (813) 888-9555
French Canadian 1+ (514) 360-1309
Technical Support Hours: Monday-Friday
9:00am to 8:00pm Eastern Standard Time

