



Firmware User's Manual

A1D-900-**A2.01.08**-AC

2017/08/10



ACTi
Connecting Vision

Table of Contents

Recommended PC Specifications 4

Preparation 5

Connect the Equipment	5
Configure the IP Addresses	5
Access the Camera.....	9

Live View 12

Login.....	12
Live View	13
PTZ Control Panel.....	16
How to Zoom the Camera In or Out	16
How to Set the Home Position	17
How to Adjust the Focus	17

Setup 18

Access the Setup Page	18
Host.....	19
GPS Position.....	20
Date & Time	21
Network	23
IP Address Filtering	23
Port Mapping.....	25
HTTPS	27
IEEE 802.1X	28
SNMP Setting	30
RTP.....	33
Network (ToS, UPnP, Bonjour, ONVIF)	34

IP Settings	37
Connection Type	37
DNS	39
DDNS.....	40
Video & Audio	43
Camera Options.....	43
Video.....	45
Motion Detection	47
Day/Night	53
Image.....	54
Exposure / White Balance.....	56
OSD	60
Privacy Mask.....	62
On-Screen Graphics	64
Audio.....	66
System	67
User Account.....	67
System Info	68
Factory Default.....	69
Firmware Upload.....	70
Save & Reboot.....	71
Logout.....	71

Troubleshooting

72

Recommended PC Specifications

In order to configure or test the cameras, 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 7 ● Windows 8
Browser for Accessing Firmware	<ul style="list-style-type: none"> ● Internet Explorer 11
Video Resolution	1024x768 or higher

Preparation

Connect the Equipment

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

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

Configure the IP Addresses

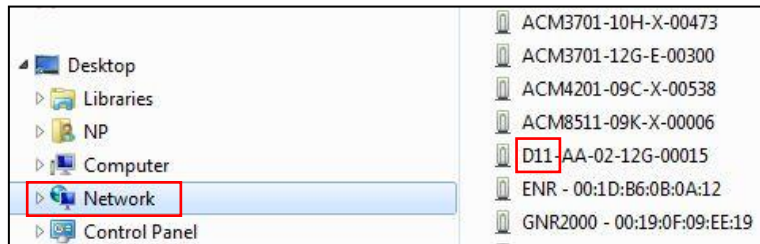
In order to be able to communicate with the camera from your PC, both the camera and the PC have to be within the same network segment. In most cases, it means that they both should have very similar IP addresses, where only the last number of the IP address is different from each other. There are 2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

Using DHCP server to assign IP addresses:

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

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

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

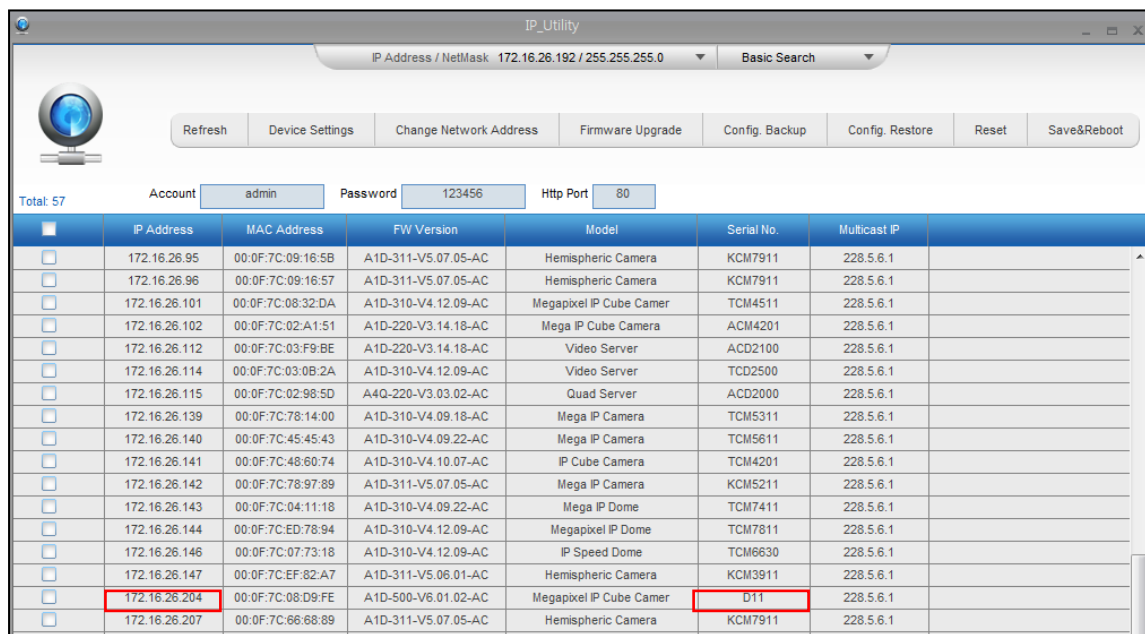


With the left mouse click on D11 it is possible to automatically launch the default browser of the PC with the IP address of the target camera filled in the address bar of the browser already.

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

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

With just 1 click, you can launch the IP Utility and there will be an instant report as follows:



	IP Address	MAC Address	FW Version	Model	Serial No.	Multicast IP
<input type="checkbox"/>	172.16.26.95	00:0F:7C:09:16:5B	A1D-311-V5.07.05-AC	Hemispheric Camera	KCM7911	228.5.6.1
<input type="checkbox"/>	172.16.26.96	00:0F:7C:09:16:57	A1D-311-V5.07.05-AC	Hemispheric Camera	KCM7911	228.5.6.1
<input type="checkbox"/>	172.16.26.101	00:0F:7C:08:32:DA	A1D-310-V4.12.09-AC	Megapixel IP Cube Camer	TCM4511	228.5.6.1
<input type="checkbox"/>	172.16.26.102	00:0F:7C:02:A1:51	A1D-220-V3.14.18-AC	Mega IP Cube Camera	ACM4201	228.5.6.1
<input type="checkbox"/>	172.16.26.112	00:0F:7C:03:F9:BE	A1D-220-V3.14.18-AC	Video Server	ACD2100	228.5.6.1
<input type="checkbox"/>	172.16.26.114	00:0F:7C:03:0B:2A	A1D-310-V4.12.09-AC	Video Server	TCD2500	228.5.6.1
<input type="checkbox"/>	172.16.26.115	00:0F:7C:02:98:5D	A4Q-220-V3.03.02-AC	Quad Server	ACD2000	228.5.6.1
<input type="checkbox"/>	172.16.26.139	00:0F:7C:78:14:00	A1D-310-V4.09.18-AC	Mega IP Camera	TCM5311	228.5.6.1
<input type="checkbox"/>	172.16.26.140	00:0F:7C:45:45:43	A1D-310-V4.09.22-AC	Mega IP Camera	TCM5611	228.5.6.1
<input type="checkbox"/>	172.16.26.141	00:0F:7C:48:60:74	A1D-310-V4.10.07-AC	IP Cube Camera	TCM4201	228.5.6.1
<input type="checkbox"/>	172.16.26.142	00:0F:7C:78:97:89	A1D-311-V5.07.05-AC	Mega IP Camera	KCM5211	228.5.6.1
<input type="checkbox"/>	172.16.26.143	00:0F:7C:04:11:18	A1D-310-V4.09.22-AC	Mega IP Dome	TCM7411	228.5.6.1
<input type="checkbox"/>	172.16.26.144	00:0F:7C:ED:78:94	A1D-310-V4.12.09-AC	Megapixel IP Dome	TCM7811	228.5.6.1
<input type="checkbox"/>	172.16.26.146	00:0F:7C:07:73:18	A1D-310-V4.12.09-AC	IP Speed Dome	TCM6630	228.5.6.1
<input type="checkbox"/>	172.16.26.147	00:0F:7C:EF:82:A7	A1D-311-V5.06.01-AC	Hemispheric Camera	KCM3911	228.5.6.1
<input type="checkbox"/>	172.16.26.204	00:0F:7C:08:D9:FE	A1D-500-V6.01.02-AC	Megapixel IP Cube Camer	D11	228.5.6.1
<input type="checkbox"/>	172.16.26.207	00:0F:7C:66:68:89	A1D-311-V5.07.05-AC	Hemispheric Camera	KCM7911	228.5.6.1

You can quickly notice the **D11** model in the list. Click on the IP address to automatically launch the default browser of the PC with the IP address of the target camera filled in the address bar of the browser already.

Use the default IP address of a camera:

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

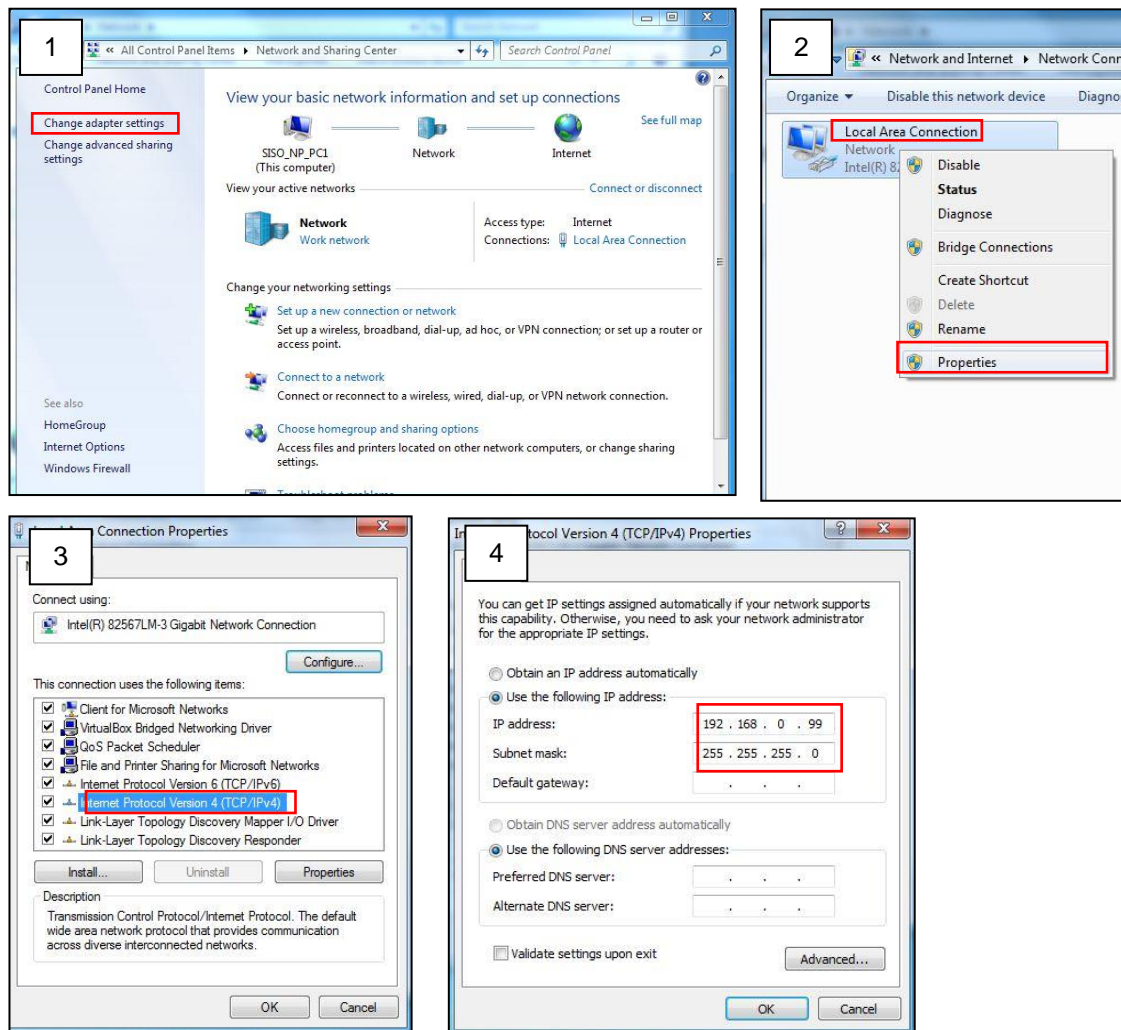
When the camera is plugged into network and it does not detect any DHCP services, it will automatically assign itself a default IP:

192.168.0.100

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

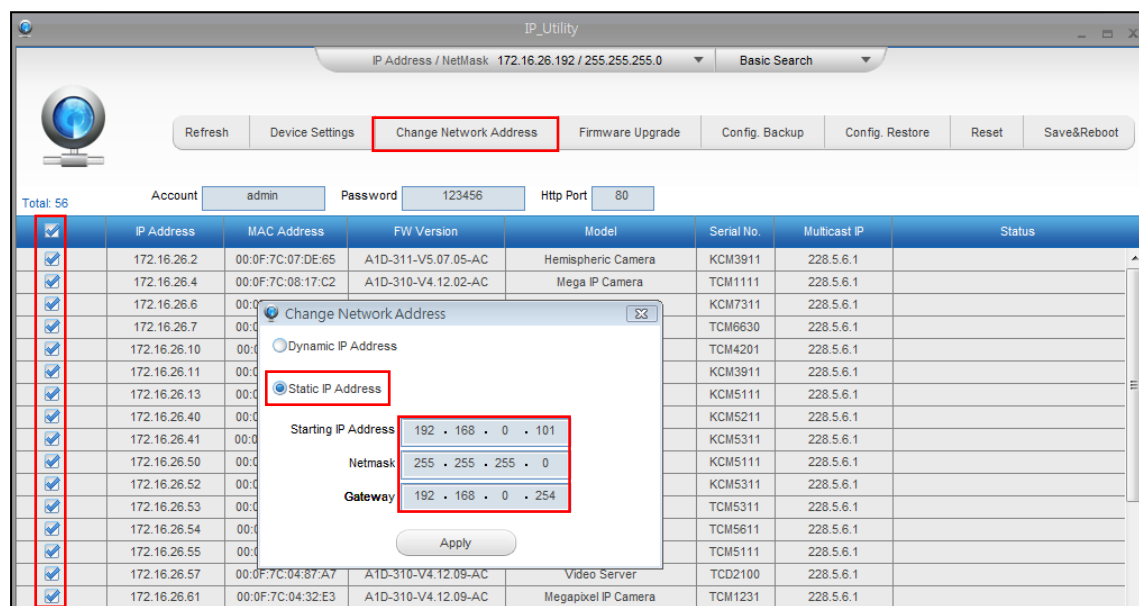
Manually adjust the IP address of the PC:

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



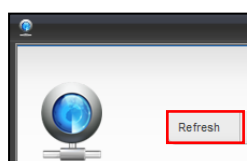
Manually adjust the IP addresses of multiple cameras:

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



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

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



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

Access the Camera

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

You can use **Microsoft Internet Explorer** to access the camera.

Functionality	Internet Explorer
Live Video	Yes
Live Video Area Resizable	Yes
PTZ Control	Yes
Capture the snapshot	Yes
Video overlay based configuration (Motion Detection regions, Privacy Mask regions)	Yes
All the other configurations	Yes

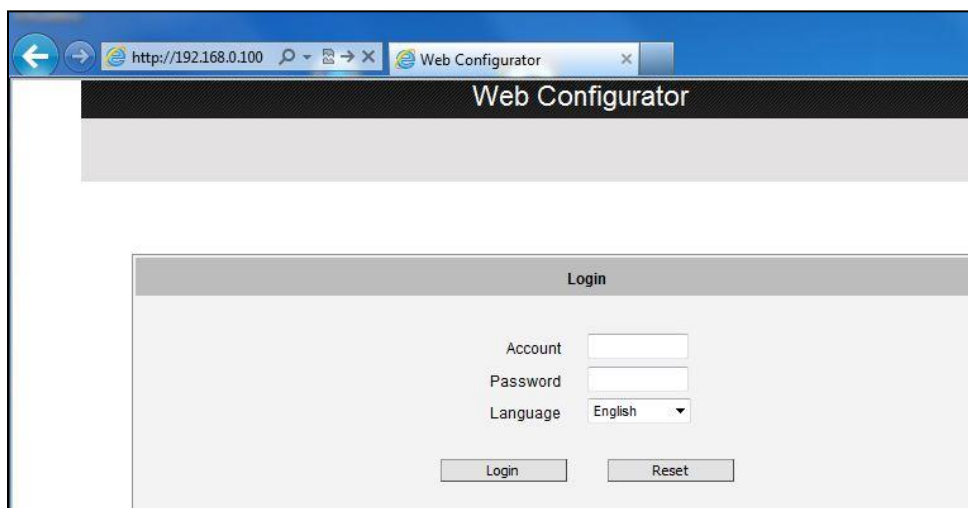
When using Internet Explorer browser, the ActiveX control for video stream management will be downloaded from the camera directly – the user just has to accept the use of such control when prompted so. No other third party utilities are required to be installed in such case.

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

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

http://192.168.0.100

Upon successful connection to the camera, 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 camera is 80, which can be omitted from the address for convenience.



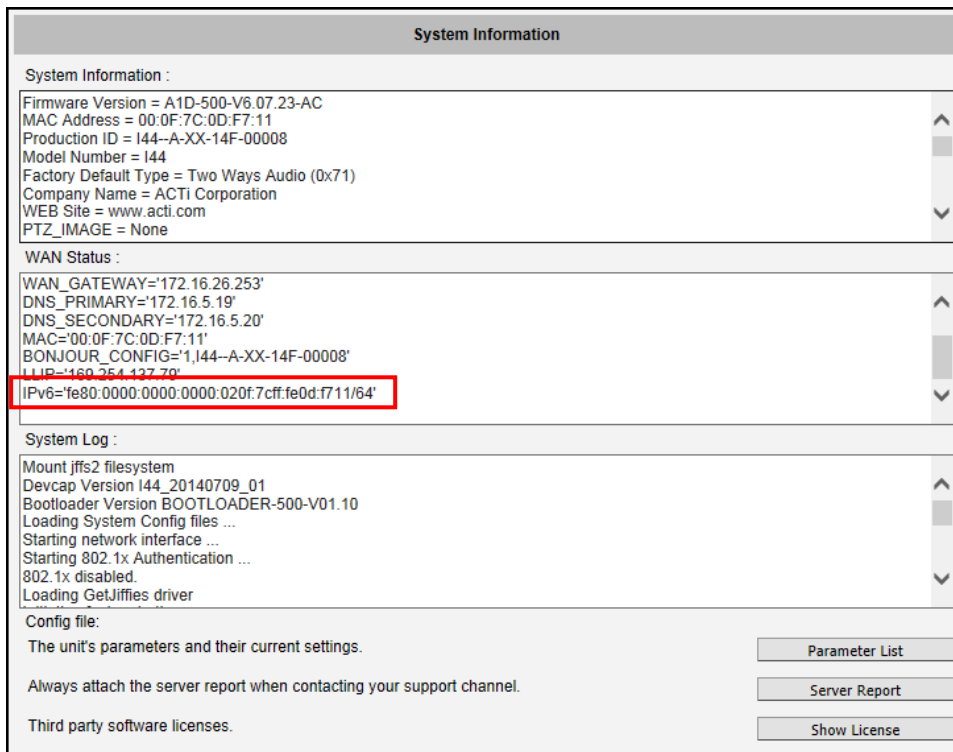
Before logging in, you need to know the factory default Account and Password of the camera.

Account: **Admin**

Password: **123456**

Using IPv6 to Access the Camera

The camera is IPv6-ready and has been assigned its unique static IPv6 address. The IPv6 address can be found under the **System > System Info** menu (see [System Info](#) on page 68 for more information).



To access the camera with the IPv6 address, type the IPv6 address enclosed in square brackets on the web browser address bar. For example:

http://[fe80:0000:0000:0000:020f:7cff:fe0d:f711]

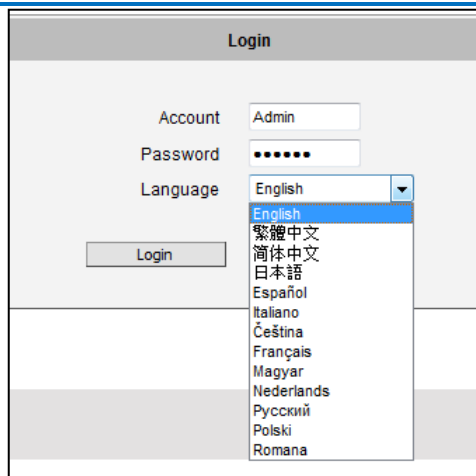
Live View

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

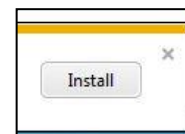
Login

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

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

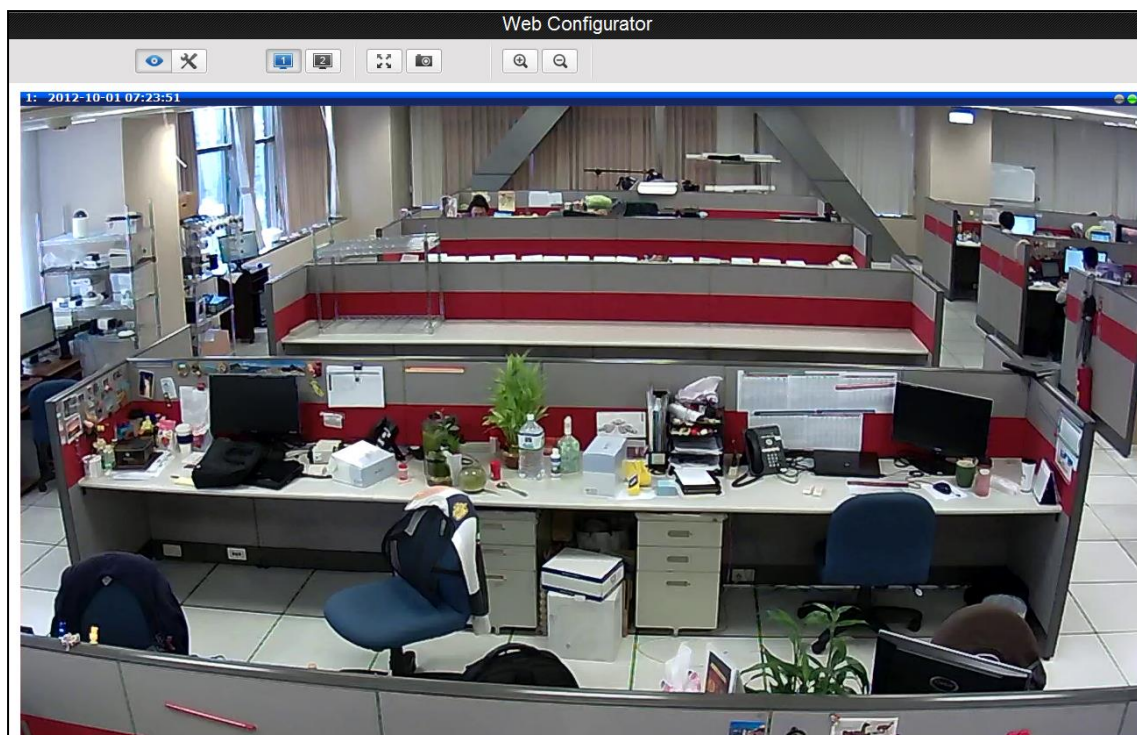


Upon successful login, you will be able to see the Live View page. In case of **Internet Explorer browser**, you may be prompted to allow the installation of ActiveX control from the camera. Press “Install” then. The live video will appear shortly after that.



Live View

The live view will appear automatically with the video resolution of **1280x720** (1MP cameras) or **1920x1080** (2-5MP cameras).



While being on the Live View page, the Live View icon appears as being pressed:



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

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

If the resolution of the PC's monitor is bigger than the resolution of the live video, you will be able to see the whole size of the video immediately. If not, you will only see part of the video at first and you would have to use the scroll bars to see the rest of the video area. In order to see the whole video on your display, you can temporarily re-scale the video to better fit your screen by pressing the digital zoom buttons:



- Enlarge the video size digitally



- Reduce the video size digitally

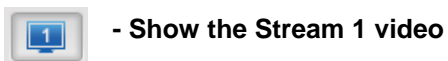
Notice: These digital zoom adjustments do not influence the actual video resolution of the camera. Regardless of how large or small the video appears on the display after pressing the digital zoom buttons, the actual video stream size of the camera is the same as before.

You can also digitally re-scale the video to fully match the size of your display with just 1 click:



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

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



When pressing the Stream 2 button, the Live View would look like this:




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



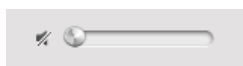
Cameras with audio function have the audio controls on Live View page.



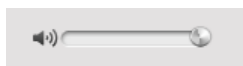
To speak to the camera, press the  button. If the camera is connected to a network video recorder, the audio will be recorded with the video stream.

To adjust the volume level of the speakers connected to the PC that runs the Web Configurator in order to hear the audio from the camera's microphone or line-in device, use the audio controls as below:

Audio Muted:




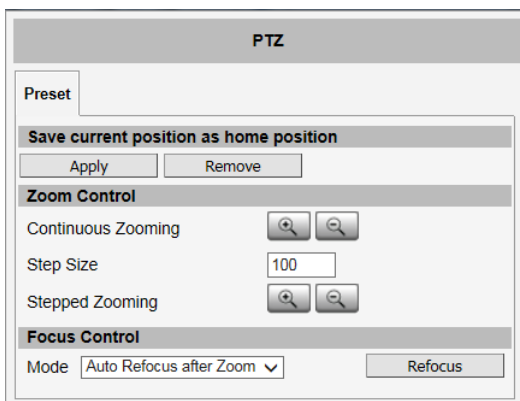
Audio level adjusted to the maximum:



This volume control appears on the user interface only when the Audio-in function of the camera has been "Enabled" under Setup page.

PTZ Control Panel

For PTZ and zoom camera models, click the PTZ button  on the Live View screen to display the PTZ Control Panel.





On the PTZ Control Panel, users can do any the following:

- Set the home position
- Zoom the camera in or out as well as adjust the step size
- Set the focus to auto refocus or manual



How to Zoom the Camera In or Out

Zooming can be done continuously or by one step (one click) at a time.

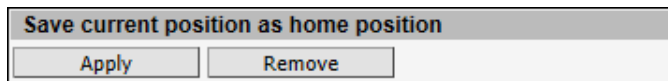
To zoom continuously, do the following:

1. On **Zoom Control**, click and hold the left mouse button on zoom in  or zoom out . When the mouse button is released, zooming stops.

To zoom by step zooming, do the following:

1. On **Zoom Control**, enter the desired step size. **Size** is the amount of zoom scale taken in each step.
2. Click the left mouse button on zoom in  or zoom out . One zoom step is taken for each click.

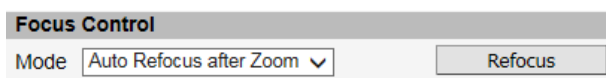
How to Set the Home Position





1. Zoom on the area that you want to set as the home position.
2. Click the **Apply** button on the **Save current position as home position**.

How to Adjust the Focus

After zooming the camera in or out, it is recommended to readjust the focus in **Focus Control**.



Options are:

- **Auto Refocus after Zoom:** Select this option to let the camera automatically adjust the focus after zooming.
- **Manual:** Select this option to manually adjust the focus. This feature is useful if the automatic focus position is not the position that the user wants to achieve. To adjust the focus manually, select the **Step Size** and then click the step focus in  or focus out  icons until the desired focus is achieved.

When an option is selected, click the **Refocus** button to apply the focus adjustment.

Setup

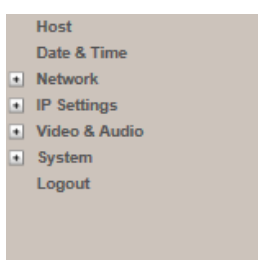
The following chapters guide you through the Setup functions of the camera.

Access the Setup Page

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



- Go to Setup



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

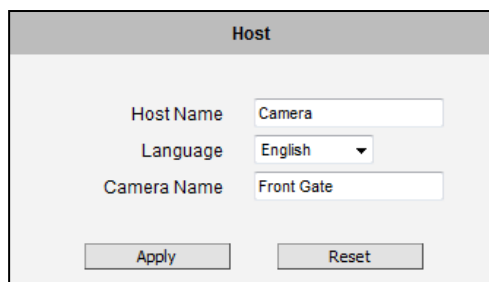
Several items in the Setup page are divided into groups, such as Network, IP Settings, etc. You can expand the groups to see the sub-items by pressing the [+] button.

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 section “Host” allows the administrator to define the name of the camera and preferred user interface language.



The screenshot shows a web configuration interface titled "Host". It contains three input fields: "Host Name" with the value "Camera", "Language" with a dropdown menu set to "English", and "Camera Name" with the value "Front Gate". At the bottom of the form are two buttons: "Apply" and "Reset".

There are two kinds of names – Host Name and Camera Name.

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

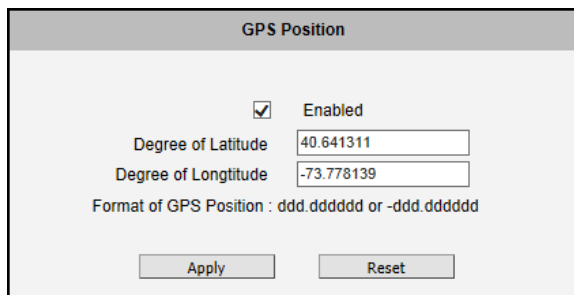
Camera Name is used to identify the device by **Video Management System** or by **Software Tools**. Usually, upon installation of the camera, the actual installation location is used as an easy-to-remember Camera Name, such as “Front Gate” or “Elevator 1”. In many cases the VMS is able to modify the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

Language selection under Host has the same purpose as the one on the login page of Web Configurator.

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

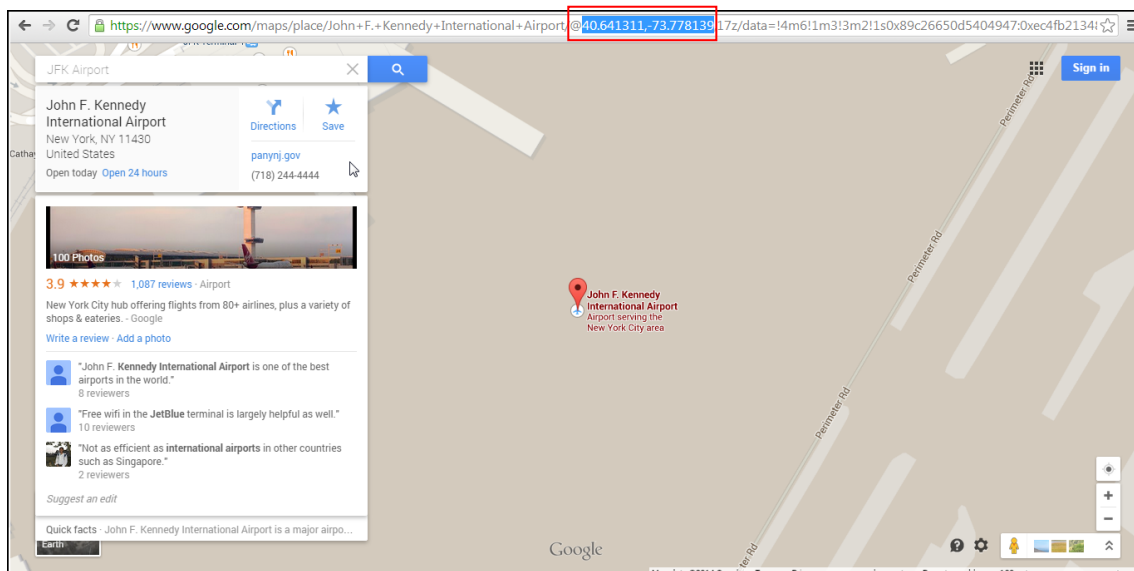
GPS Position

This section allows users to manually set the GPS position of the camera and find the location of the camera on the map when using a Network Video Recorder (NVR).



Check the **Enabled** box to enable this feature.

Find the camera location on google maps, for example, installed in the airport.



Copy the first GPS coordinates from the URL bar and paste it on **Degree of Latitude**. Copy the second part of the GPS coordinates to **Degree of Longitude**.

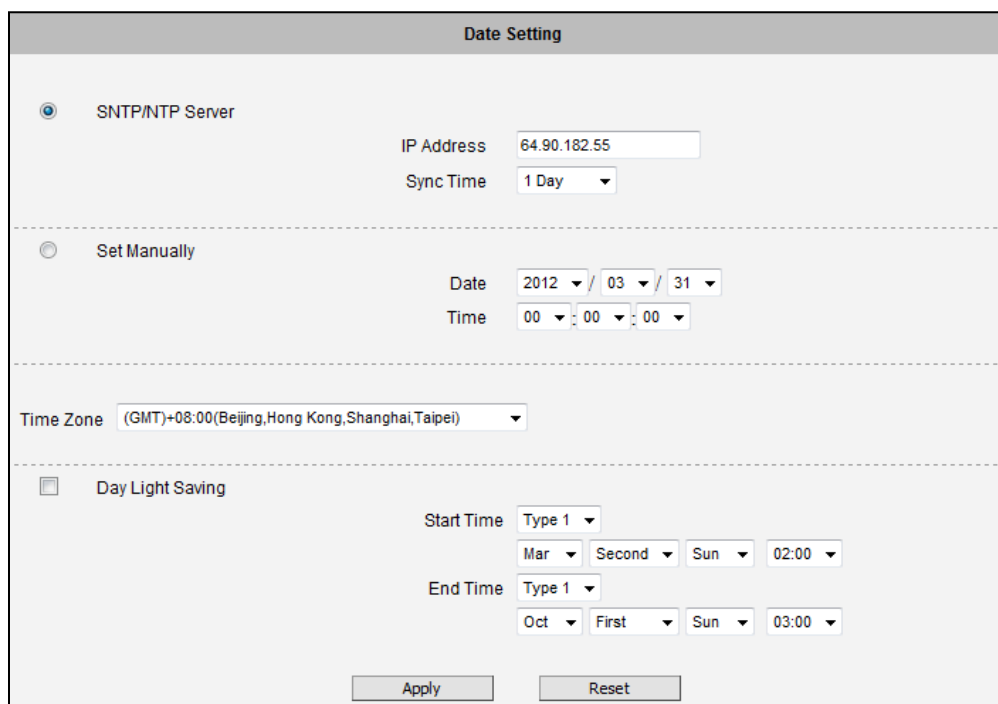
Press **Apply** to save the changes.

Date & Time

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

Date & Time The section **Date & Time** provides the options for adjusting the date and time of the camera.

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



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

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

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

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

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

Type 1 – define the starting or ending time of daylight saving period by the **number of the week in the month** (First, Second, Third or Last week).

Type 2 – define the starting or ending time of daylight saving period by the **exact date in the month** (1-31).

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

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

Network

Network

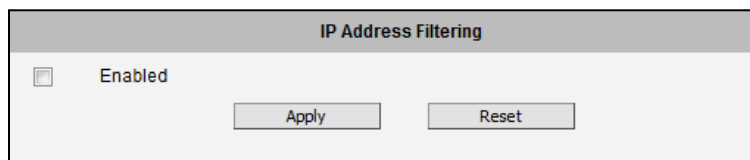
The section **Network** provides the list of network related functions and services. The [+] mark before Network indicates that the list can be expanded by clicking on it. Once expanded, the list can later be collapsed again by clicking on the [-] mark.

IP Address Filtering

IP Address Filtering

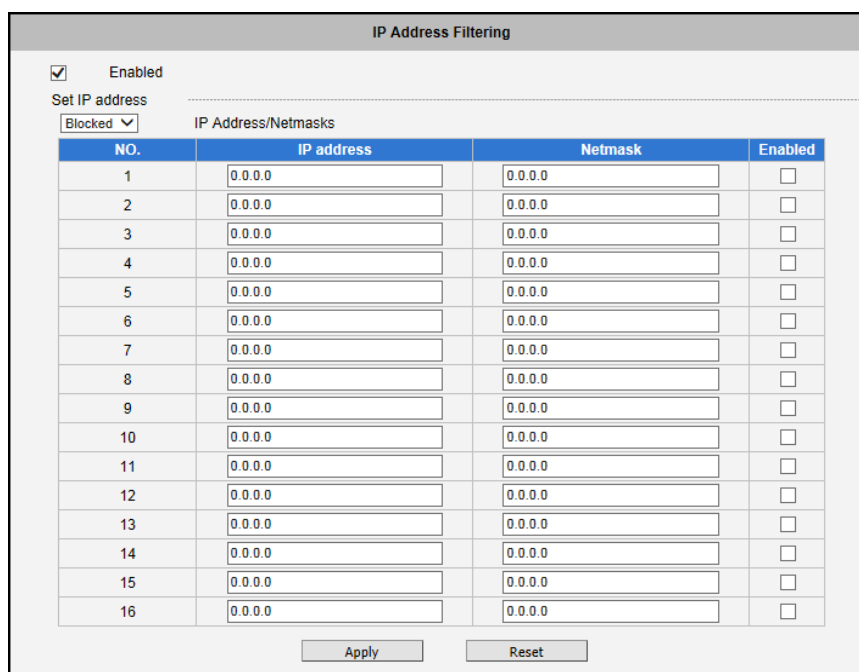
By “**IP Address Filtering**” function it is possible to define which devices (their IP addresses) are allowed to connect to this camera, and which devices are forbidden to connect to this camera.

Check the box “Enabled” to activate the IP address filtering function and press Apply.



The screenshot shows a control panel titled "IP Address Filtering". It features a checkbox labeled "Enabled" which is currently unchecked. Below the checkbox are two buttons: "Apply" and "Reset".

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



The screenshot shows a detailed configuration window for "IP Address Filtering". At the top, the "Enabled" checkbox is checked. Below it, there is a "Set IP address" section with a dropdown menu currently set to "Blocked". The main part of the window is a table with 16 rows, each representing a filter entry. Each row has columns for "NO.", "IP address", "Netmask", and "Enabled". All IP addresses and netmasks are currently set to "0.0.0.0". The "Enabled" checkbox for each row is unchecked. At the bottom of the window are "Apply" and "Reset" buttons.

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

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

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

Port Mapping

Port Mapping

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

Port Mapping

HTTP Port*

HTTPS Port*

Search Server Port1

Search Server Port2

RTSP Server Port

Multicast Setting

	By Requests	Multicast IP	Network Port	Multicast TTL
Stream 1	<input checked="" type="checkbox"/>	<input type="text" value="228.5.6.1"/>	<input type="text" value="5100"/>	<input type="text" value="16"/>
Stream 2	<input checked="" type="checkbox"/>	<input type="text" value="228.5.6.2"/>	<input type="text" value="5104"/>	<input type="text" value="16"/>
Audio	<input checked="" type="checkbox"/>	<input type="text" value="228.5.6.3"/>	<input type="text" value="5102"/>	<input type="text" value="16"/>

Multicast IP [224.5.0.1 ~ 239.255.255.255]
 Multicast TTL [1~255]

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

Parameters	Description
HTTP port	Select the port assigned for HTTP protocol access.
HTTPS Port	Select the port assigned for HTTPS protocol access.
Search Server Port1	Select the first port used by server search applications to detect this IP device (e.g. IP Utility).
Search Server Port2	Select the second port used by server search applications to detect this IP device (e.g. IP Utility).
RTSP Server Port	Select the port assigned for RTSP protocol access.

Multicast Setting allows users to configure the IP addresses and ports for multicast video and audio (supported models only) streams. Multicast is a protocol where a data stream is sent only once and shared to requesting devices. This in turn saves network bandwidth. However, to use this feature, network devices, such as routers and switches, should support IP multicast.

Parameters	Description
Stream 1	Refers to the video stream 1.
Stream 2	Refers to the video stream 2.
Audio	Refers to the audio stream. NOTE: Appears only if the camera model supports audio input/output.
By Request	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 the Network Video Recorder (NVR), selects to view or record the stream. If unchecked, the video or audio stream will constantly be streamed to the network whether there are devices viewing the video or not. To save on network bandwidth, it is recommended to check this function.
Multicast IP	Set the multicast IP of the corresponding stream.
Network Port	Enter the assigned port for 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 then discarded.

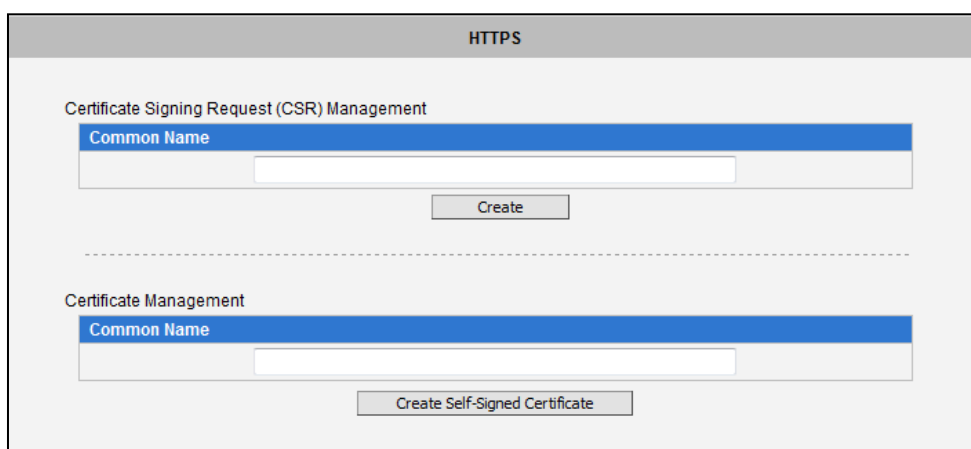
After changing any of the items above, press **Apply** to save the changes. The Reset button undoes the changes that had just been made but not Applied yet. New port settings will only take effect after pressing **System -> Save & Reboot**.

HTTPS

HTTPS

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

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



The screenshot shows a web interface titled "HTTPS". It contains two main sections:

- Certificate Signing Request (CSR) Management:** This section has a blue header "Common Name" above a text input field. Below the input field is a "Create" button.
- Certificate Management:** This section also has a blue header "Common Name" above a text input field. Below the input field is a "Create Self-Signed Certificate" button.

A horizontal dashed line separates the two sections.

Certificate Signing Request (CSR): User uses a signed certificate issued by trusted Certification Authority (CA).

Self-Signed Certificate: User wants to use the certificate created and issued by user himself.

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

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

IEEE 802.1X

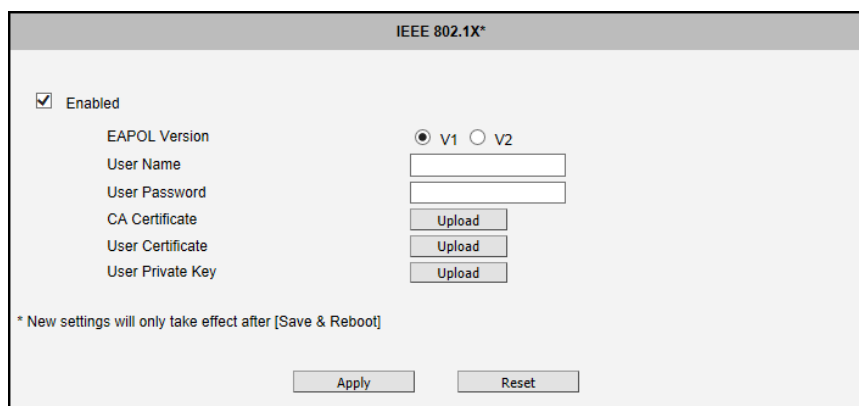
IEEE 802.1X

IEEE 802.1X is an IEEE standard for port-based Network Access Control. 802.1X authentication involves three parties: a supplicant, an authenticator, and an authentication server.

The supplicant is a client device (such as an IP camera) that wishes to attach to the LAN/WLAN. The authenticator is a network device, such as an Ethernet switch or wireless access point; and the authentication server is typically a host running software supporting the RADIUS and EAP protocols.

The authenticator acts like a security guard to a protected network. The supplicant (i.e., client device) is not allowed access through the authenticator to the protected side of the network until the supplicant's identity has been validated and authorized. An analogy to this is providing a valid passport at an airport before being allowed to pass through security to the terminal. With 802.1X port-based authentication, the supplicant provides credentials, such as user name / password or digital certificate, to the authenticator, and the authenticator forwards the credentials to the authentication server for verification. If the authentication server determines the credentials are valid, the supplicant (client device) is allowed to access resources located on the protected side of the network.

Please **enable** IEEE 802.1x and configure settings on the screen below. Note that the new setting will only take effect after "Save & Reboot".



EAPOL Version V1 and V2 are the 802.1X communication types. **User name** and **User password** area created by user and set in RADIUS server. **Certificates** and **Private Key** are provided by RADIUS Server.

If certificates or private key exist already, there will be a **Remove** button behind these items, in order to remove these items when necessary.

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

SNMP Setting

SNMP Setting

The **SNMP Setting** item 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 camera (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 “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 you’ve completed setup.

The security method of **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 you’ve completed setup.

SNMP function is now enabled. You may now install and run the SNMP management software on 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 camera, 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**”.

Camera’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>

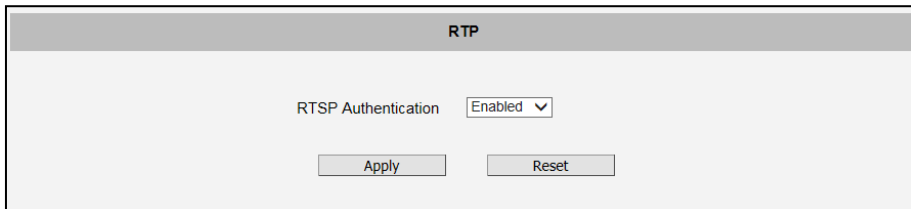
ICMP	Provide the status and statistics of ICMP. <i>Ex: amount of receive/error message of ICMP.</i>
TCP	Provide the status and operation of Transport Layer (Layer 4) using TCP protocol. <i>Ex: TCP Local Port, incoming/outgoing TCP segments.</i>
UDP	Provide the status and operation of Transport Layer (Layer 4) using UDP protocol. <i>Ex: UDP Local Port, in/out datagram.</i>
SNMP	Provide the related statistics through SNMP

RTP

RTP

The **RTP** section allows user to configure RTP Settings.

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



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

Network (ToS, UPnP, Bonjour, ONVIF)

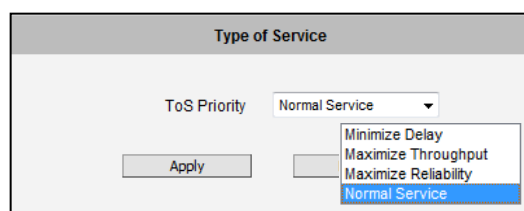
Network

The section Network contains the controls for following functions:

- Type of Service
- UPnP
- Bonjour
- ONVIF

Type of Service

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



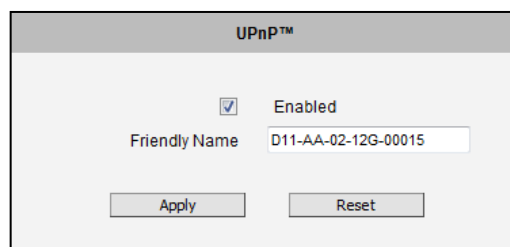
For special priority arrangement, there are 3 more options:

- Minimize Delay
- Maximize Throughput
- Maximize Reliability

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

UPnP™

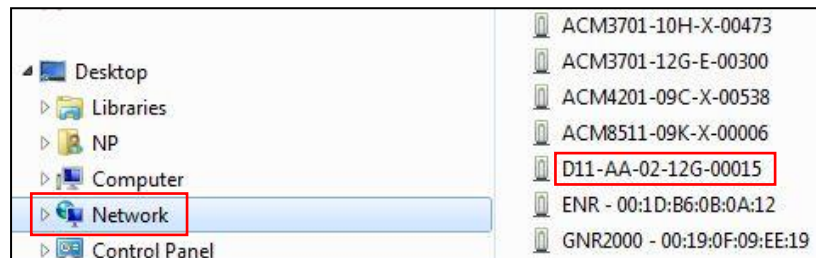
The section **UPnP™** provides the option to enable or disable the Universal Plug and Play capability of the camera. Having the UPnP™ enabled allows the other network devices to seamlessly discover it on the network for convenient identification and access.



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

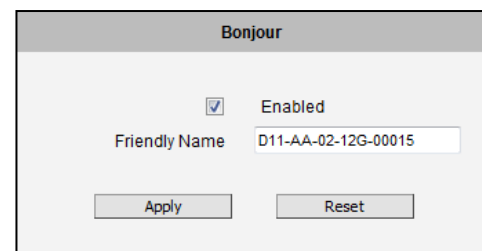
After changing any of the items above, press **Apply** to save the changes. The Reset button undoes the changes that had just been made but not Applied yet.

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



Bonjour

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



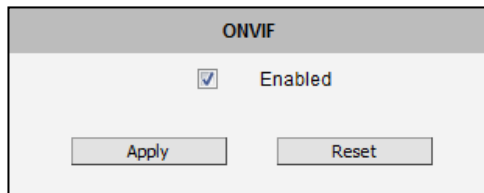
Similarly to UPnP, the human readable **Friendly Name** can be defined by the user. That name will be displayed when the camera is found in the network. By default, the Friendly Name is the serial number of the camera; however, the user can modify the name according to the project needs.

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

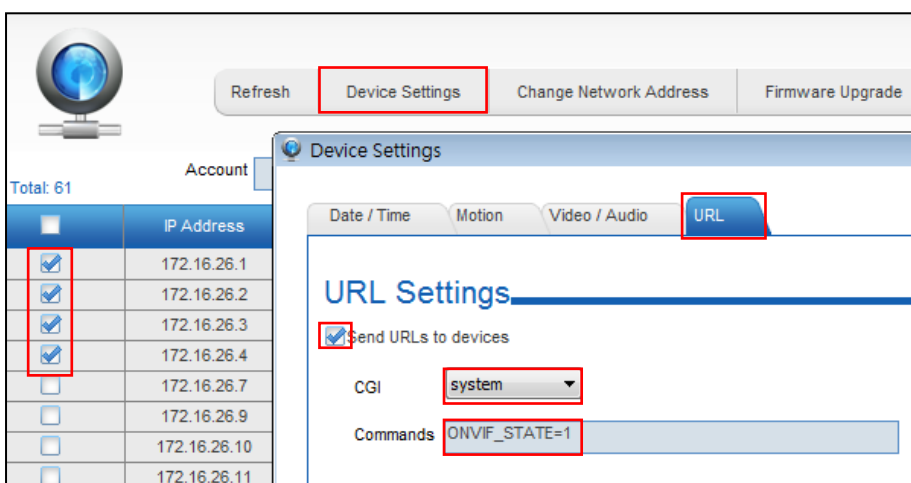
ONVIF

The camera with given firmware is ONVIF 2.2 compliant. By default, the ONVIF function is enabled.

To disable the ONVIF support, remove the check on the box and press **Apply**.



If you need to activate ONVIF on multiple cameras conveniently, you may use the IP Utility instead, using **system** cgi and **ONVIF_STATE=1** as URL command.



IP Settings

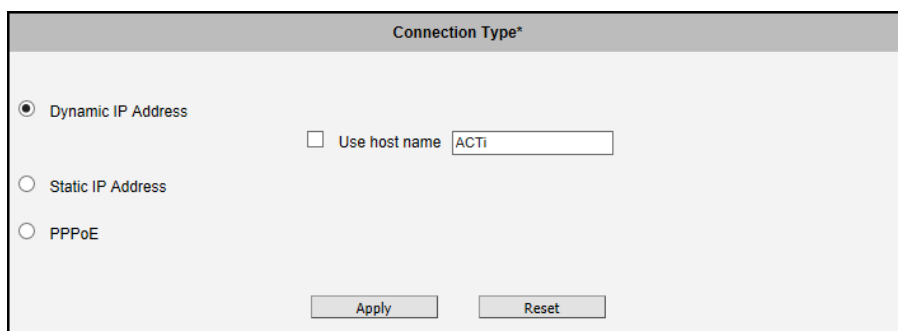
IP Settings

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

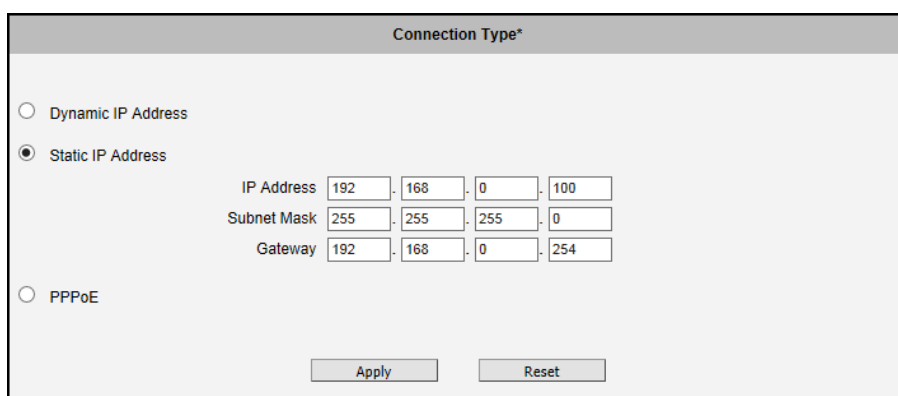
Connection Type

Connection Type

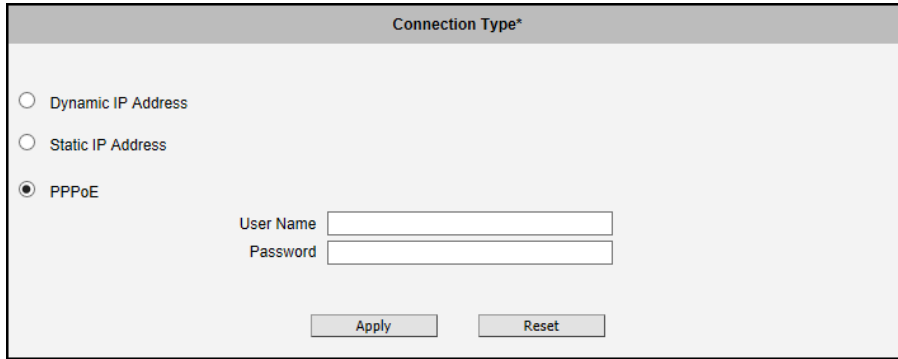
The sub-section **Connection Type** allows defining the method of obtaining the IP address of the camera. By default, the camera is in **Dynamic IP Address** mode and attempts to get the IP address from a DHCP server. If such attempt fails after several seconds (for example the DHCP server does not exist),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



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



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



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

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

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

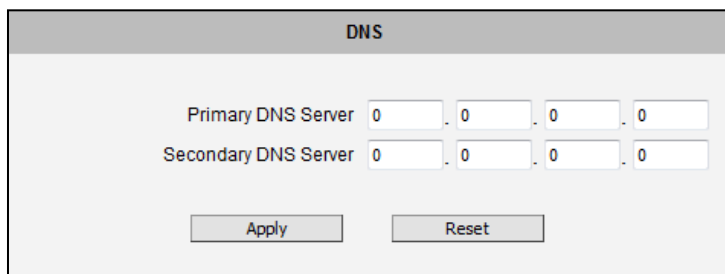
New IP address settings will only take effect after pressing **System -> Save & Reboot**.

DNS

DNS The section **DNS** allows setting up the Domain Name Service for the camera. The camera 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 camera 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.



DNS

Primary DNS Server 0 . 0 . 0 . 0

Secondary DNS Server 0 . 0 . 0 . 0

Apply Reset

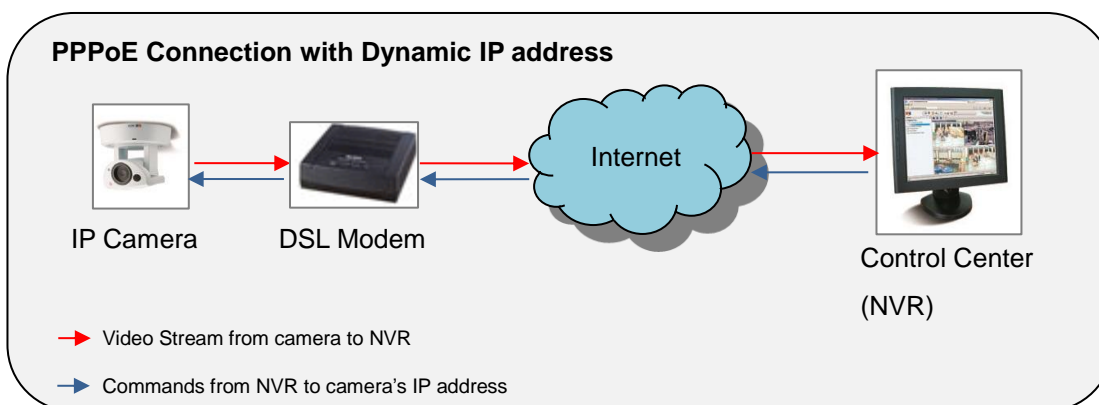
After changing any of the items above, press **Apply** to save the changes. The **Reset** button undoes the changes that had just been made but not Applied yet.

DDNS

DDNS

There are surveillance solutions that consist of single cameras scattered over a wide territory, therefore each of those cameras should be connected to the Internet in order to become accessible by Control Center. For example, the chain stores, bus stops, currency exchange booths, etc.

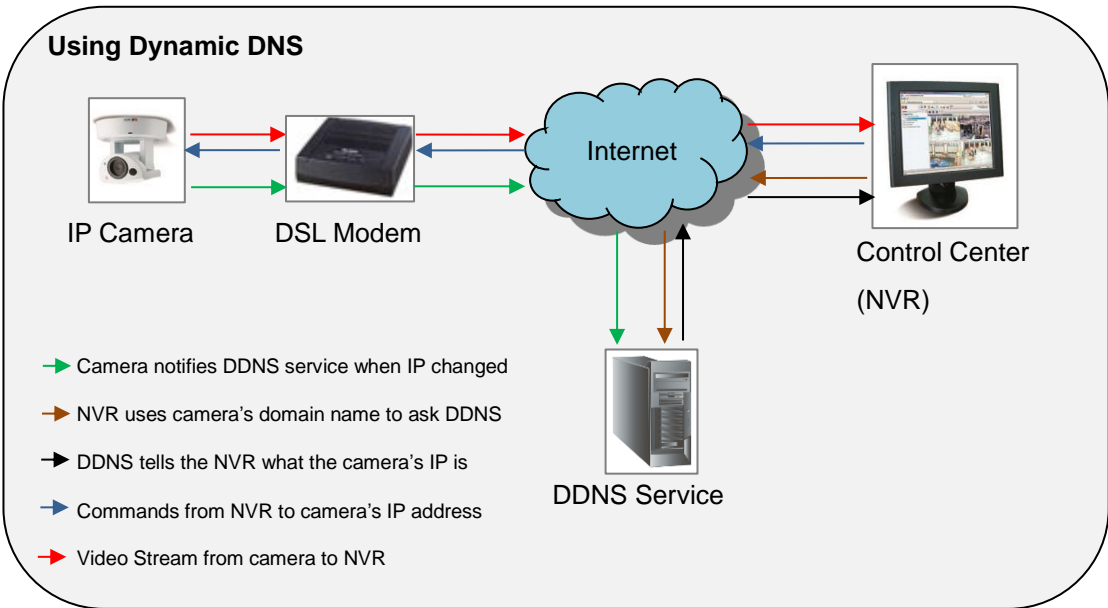
In such cases, one of the practical networking solutions is to use DSL modem on camera site and let the camera obtain the dynamic IP address from the Internet Service Provider through the DSL modem using PPPoE connection, which is much more cost-effective than applying for static IP address.



However, there is one drawback in this solution – in order to do the remote surveillance from the Control Center, the NVR Server in the Control Center has to know the address of the IP camera at all times in order to get the video stream from the camera. If the camera's network connection has been reset for any reason, the camera will get a new IP address through DSL Modem, which may be different from the previous one. NVR will not know about this change, and the connection between the camera and NVR will fail.

There however exists a solution that makes sure the NVR can find the camera even if the camera IP changes frequently. Our cameras support **Dynamic DNS** or **DDNS** service that allows frequently changing IP be mapped to a certain unchangeable domain name. The mapping database and its updating engine are hosted in one of the Dynamic DNS servers, most of which offer basic services for free, such as www.dyndns.org.

How does it work? Look at the graph below.



Every time the IP camera gets an IP that is different from previous one, it notifies the public DDNS Service about the change. The DDNS Service updates its database immediately, mapping the assigned domain name (for example *camera123.dyndns.org*) to the new IP address. In NVR settings, only the domain name (*camera123.dyndns.org*) is used to identify the camera. Every time when NVR needs to connect to the camera, it asks from DDNS Service what the current camera's IP is. The DDNS Service instantly responds to NVR and tells it the camera's IP. Now NVR will use the IP of the camera to connect to the camera and the video stream from the camera to NVR can be initiated.

As a result, NVR can always find the IP camera regardless of frequently changing IP address of the camera. Since there are so many public DDNS Services available for free, the PPPoE-based connection is really a good and low-cost solution for single-camera sites.

DDNS

Enabled

As a service / As a protocol reference:

Host Name:

User Name:

Password:

To activate DDNS, please check the **“Enabled”**. Select the service reference, input the **Host Name** (the domain name given to the camera by DDNS service, **User Name** and **Password** of the DDNS server account.

You will get the needed Host Name, User Name and Password information from the DDNS service provider once you have registered an account there and requested a domain name for your camera.

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

Video & Audio

Video

The section **Video** or **Video & Audio** (for audio supported cameras) provides the options to adjust the video quality, configure the streaming details of the camera, and audio settings (for Audio supported cameras only), which will be described in the succeeding pages.

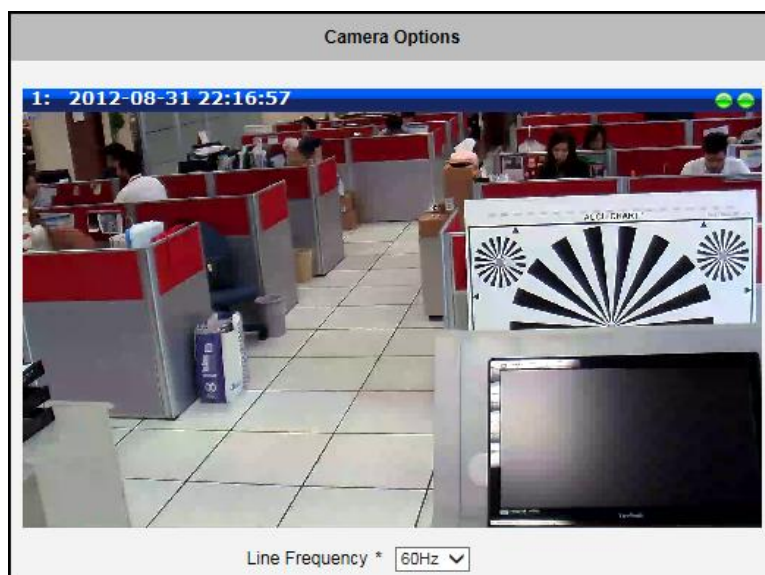
The default settings of the camera are sufficient for most environments and the video adjustments are not necessary. The following sections explain the ways to configure the video quality or streaming details in case it is required to do so.

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

Camera Options

Camera Options

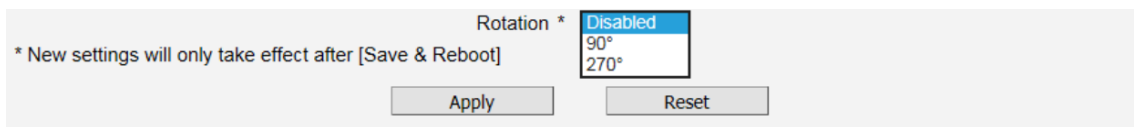
In general, the **Camera Options** submenu allows users to set the **Line Frequency** and **Stream Mode** properties of the camera. Depending on the camera type, the parameters on the **Camera Options** screen vary.



Line Frequency is the function that adjusts the shutter speed options to match with the frequency of artificial light source of given country. For example, in Europe the light frequency (due to power supply frequency of lights) is 50Hz, that is 50 flashes per second. By setting line frequency to 50Hz in such case, the shutter speed options will be proportional with light source frequency, such as 1/25s, 1/50s, 1/100s, etc.

It is necessary to have the camera's Line Frequency adjusted according to the power frequency of the light source to avoid flickering effect.

The natural light source (sun light) is a seamless flow of light – the Line Frequency setting does not matter for the cameras that are only exposed to natural light.



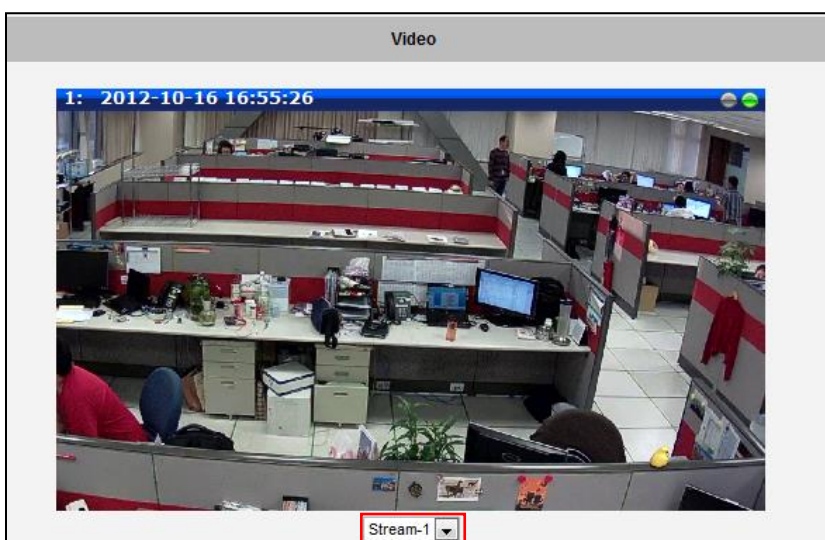
Rotation allows users to specify the rotation angle of the video view.

After changing any of the items above, press **Apply** to save the changes.

Video

Video The sub-section is also named **Video**. For Audio supported cameras, there will also be a sub-section named Audio. The video section is divided into tabs. The functionality of each tab is explained separately below.

Upon opening the sub-section named Video, the live view of the Stream 1 of the camera will appear. Since the camera is a dual stream device, it is possible to see how each of the 2 streaming configurations looks like, by selecting either **Stream-1** or **Stream-2** under the live video window.



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

Compression

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

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

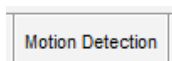
Stream 1	Stream 2
Encoder Type <input type="text" value="H264"/>	Encoder Type <input type="text" value="H264"/>
H.264 Profile <input type="text" value="Baseline"/>	H.264 Profile <input type="text" value="Baseline"/>
Resolution <input type="text" value="N1920x1080"/>	Resolution <input type="text" value="N320x240"/>
Frame Rate <input type="text" value="30"/>	Frame Rate <input type="text" value="5"/>
Video Bit Rate Mode <input type="text" value="Variable Bit Rate"/>	Video Bit Rate Mode <input type="text" value="Variable Bit Rate"/>
Quality <input type="text" value="Medium"/>	Quality <input type="text" value="Medium"/>
GOP 1 I-frame / <input type="text" value="3 Second"/>	GOP 1 I-frame / <input type="text" value="3 Second"/>

Parameters	Description
Encoder Type	3 available encoder types: H.264 (High Profile), H.265, and MJPEG.
H.264 Profile	This item is available only if the Encoder Type is H.264. The H.264 Profile defines the video compression scheme: High Profile , Main Profile , and Baseline . These schemes vary from least compressed, Baseline , to most compressed, High Profile . By default, the H.264 Profile is High Profile , which provides the most compression with the best video quality, but more computing power. Some third-party video management system has longer latency or takes more time to decode High Profile compression scheme, in this case, you can select Main Profile or Baseline . In order to get the same video quality, you can select a higher bit rate with lower compression; this is the same as having a lower bit rate with a High Profile. For example, a video on High Profile with 2M bit rate will have the same video quality as a video with Baseline Profile at 3.5M bit rate.
Resolution	Depending on the camera model, the number of available resolutions may be different. The default resolution setting of the camera 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>(only H.264 / H.265)</i>	Under "Constant Bit Rate" mode (CBR), the camera keeps the stable bitrate regardless of the complexity of the scene. Under this mode, the video quality may vary if the bit rate value is set too low. It is easier to do storage and network bandwidth consumption estimations under this mode compared to Variable Bit Rate mode. Under "Variable Bit Rate" mode (VBR), the camera will keep the video quality stable while the bit rate may occasionally go up or down, depending on the complexity of the scene.
Video Max Bit Rate <i>(only H.264 / H.265)</i>	Defines the upper limit of the bitrate (only available under CBR mode). The bitrate will be floating slightly under that limit. For example, if the limit is set as 2M, the bitrate will be floating around 1.6~2.0 Mbps. <div style="border: 1px solid #ccc; padding: 5px; width: fit-content; margin: 10px auto;"> Video Bit Rate Mode <input type="text" value="Constant Bit Rate"/> Video Max Bit Rate <input type="text" value="Unlimited"/> Video Bit Rate <input type="text" value="2M"/> </div> <p>If the Video Max Bit Rate is chosen as "Unlimited", then the "Video Bit Rate" selection box will appear that defines the bit rate level.</p>

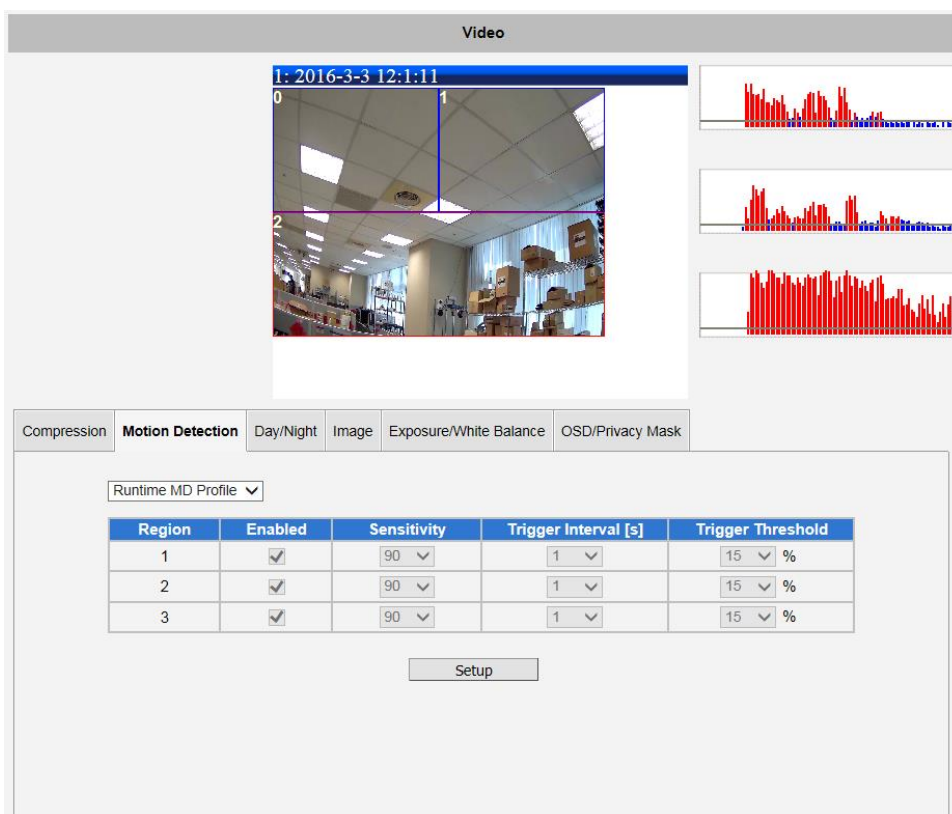
<p>Video Bit Rate <i>(only H.264 / H.265)</i></p>	<p>Under CBR mode, when Video Max Bit Rate is chosen “Unlimited”, the user can define the AVERAGE bit rate. For example, if the Video Bit Rate is chosen 2M, then occasionally, the actual bit rate may go below or beyond 2M, but in the long run, the average bit rate will be very close to 2M. This mode allows the most accurate storage estimations, however, while planning the bandwidth, please consider the occasional peaks of bit rate.</p>
<p>Quality</p>	<p>H.264 / H.265 Compression:</p> <div data-bbox="544 539 911 658" style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> <p>Video Bit Rate Mode Variable Bit Rate ▾</p> <p style="text-align: center;">Quality Medium ▾</p> <p>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 and follows the quality standard set by the user. The user can choose either “High”, “Medium” or “Low” quality. The higher is the quality level, the more bit rate the camera will use to achieve the target quality.</p> <p>MJPEG Compression: The user can define the quality with the numeric scale from 1 to 100. The default MJPEG quality is 60. The higher is the quality level, the more bit rate the camera will use to achieve the target quality.</p>
<p>GOP <i>(only H.264 / H.265)</i></p>	<p>Under VBR mode it is possible to adjust the GOP length - that is the occurrence rate of I-frames. By default, there is one I-frame per second. For example, in case of 30fps, there will be 1 I-frame and 29 P-frames every second by default. When the GOP is changed to “1 I-frame per 5 seconds”, then there will be one I-frame, followed by 149 P-frames. In case of the static scenes, long GOP can further minimize the bandwidth and storage consumption.</p>

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

Motion Detection



The section “Motion Detection” allows the user to configure the video motion detection system of the camera. Motion detection regions are based on Stream 1. By default, there are three (3) enabled pre-defined regions covering the whole camera view.



Click on “Setup” to adjust the motion detection regions or its parameters. **Microsoft Internet Explorer** browser is required to configure the motion detection regions.

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

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

Enabled or disabled

Although all 3 motion detection regions are enabled by default, each can be disabled and enabled individually. Look at the example: Only the region 1 is enabled while 2 and 3 are disabled. The disabled regions disappear from the video display.



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

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

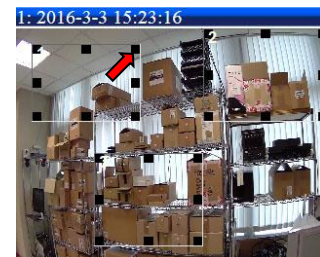
Location of the region

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



Size of the region

By clicking and dragging the black squares locating in the motion detection region you can change the size of the area. The maximum size of the region can even be as big as the whole screen.



Sensitivity

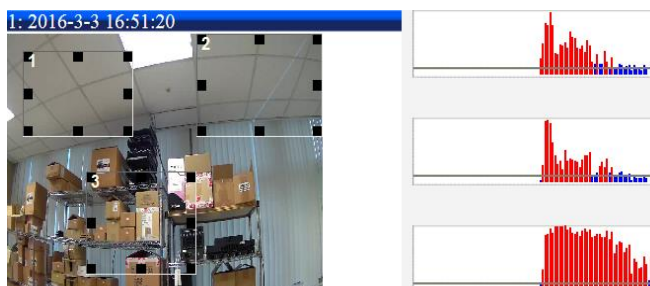
Sensitivity is the parameter that helps us distinguish actual moving targets (people, vehicles) from the slightly moving background, such as leaves of the trees waving in the wind. In order to avoid false alarms, we might want the camera be able to ignore small motion. The higher is the sensitivity level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

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

standard cases.

Trigger threshold

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



The blue graph on the right side of the image shows how many percent of pixels within the motion detection region were considered as “currently in motion”. The activity panel itself is a timeline – for each moment of time you

Compression **Motion Detection** Day/Night Image Exposure/White Balance OSD/Privacy Mask

Runtime MD Profile ▾

Region	Enabled	Sensitivity	Trigger Interval [s]	Trigger Threshold
1	<input checked="" type="checkbox"/>	90 ▾	1 ▾	15 ▾ %
2	<input checked="" type="checkbox"/>	90 ▾	1 ▾	15 ▾ %
3	<input checked="" type="checkbox"/>	90 ▾	1 ▾	15 ▾ %

Apply Reset

can see the height of the blue bars. You may notice that at certain moment the tallest bars in the activity graph reached about 25% (a quarter of the total height in activity panel) – it means, 25% of this motion detection area were filled with moving pixels at that moment. By visual observation you can also see that the object standing inside the motion detection region indeed covers about 25% of its size.

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










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

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

region.

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

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

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

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

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

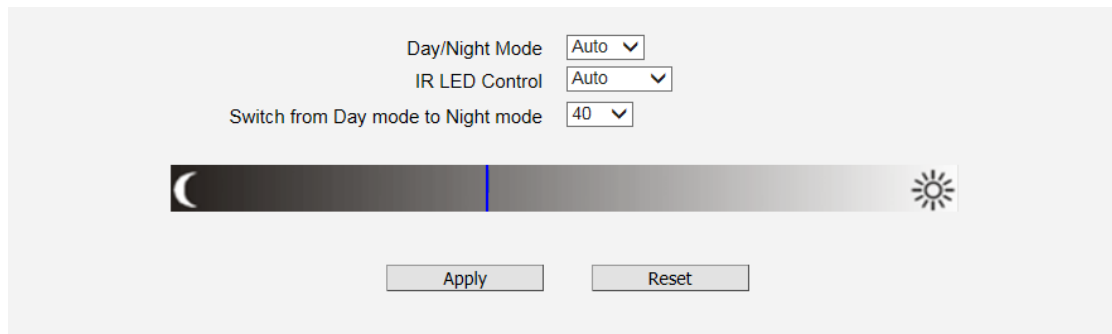
Trigger interval

The last configuration item is the trigger interval. It is the time period from the beginning of the triggered event during which the all motion activities are ignored by the camera. This is designed to avoid needless repetitive reporting of the same intrusion. Trigger interval 20 seconds would mean that when the even happens, camera will take certain one-time actions and ignore the

continuing activity in the motion detection region for 20 seconds. When 20 seconds are over, the camera will produce a new alarm if there are still action in the motion detection region, and take actions again.

Day/Night

Day/Night The section **Day/Night** allows user to control the switching between day mode and night mode. This section will be displayed only for day/night models.

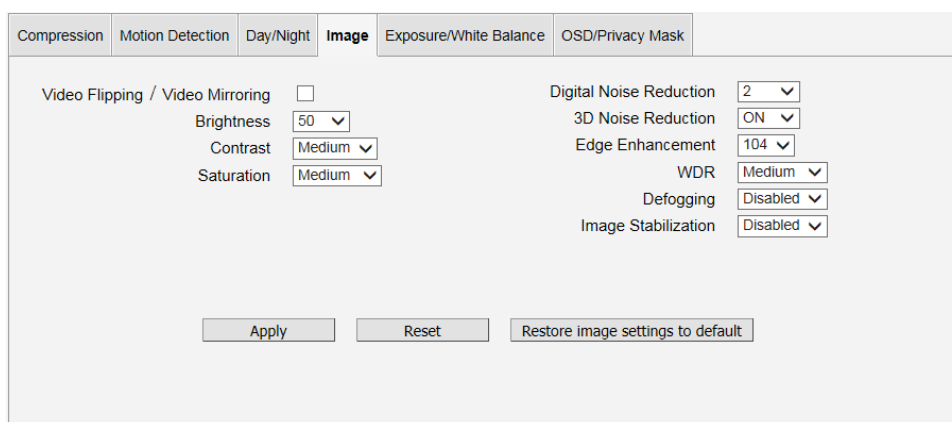


Parameters	Description
Day/Night mode	<p>There are three modes:</p> <p>Auto: The camera will automatically switch between day mode (color) and night mode (black/white) under certain exposure level, defined by user at “Switch from Day mode to Night mode”.</p> <p>Day: The camera always stays in day mode (color) regardless of exposure level.</p> <p>Night: The camera always stays in night mode (black/white) regardless of exposure level.</p>
IR LED Control	<p>This feature is visible only in cameras with built-in IR LED.</p> <p>There are two modes:</p> <p>Auto: The built-in IR LED will be turned on automatically upon day to night switch and turned off upon night to day switch.</p> <p>Disabled: The IR LED will be off regardless of day and night mode.</p> <p>Zoom cameras have adaptive IR profile, which means that when IR LED Control is set to “Auto” (default setting), the IR LED automatically adapts to the required IR LED power as the camera is zoomed in or out.</p>
Switch from Day mode to Night mode	<p>The scale of 0~100 allows user define the exposure level at which the day to night switch should happen. The higher is the value, the darker the environment has to be to trigger the day to night switch.</p>

Image



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



Parameters	Description
Video Flipping / Video Mirroring	Check this box to flip the video up-down and left-right to achieve the 180-degree rotation effect.
Brightness	Select the Brightness value (0~100). The higher the value, the brighter the image.
Contrast	Select the Contrast level from following options: Lowest, low, medium, high, highest
Saturation	Saturation makes colors appear more vivid. Select the Saturation level from the following options: Disabled, low, medium, high, highest.
Digital Noise Reduction	Turn ON (scale 1-4) or OFF the Digital Noise Reduction. When turned on, the noise reduction in the video (especially in low light) is reduced and image will look smoother and clearer. The higher the value, the more
WDR	Choose the WDR level from following options: Disabled, low, medium, high, highest. NOTE: WDR is disabled and will not appear on screen if Exposure Mode is set to "Manual". See <i>Exposure / White Balance</i> on page 56.
3D Noise Reduction	Enable this feature for smooth and clear image. Disable this feature if the scene contains extreme details that may be smoothed over with 3DNR.
Edge Enhancement	Select the Edge Enhancement value. The higher the value, the sharper the image.
Defogging	This feature provides a clear image even when the camera is installed in a foggy environment. Select the Defogging level: Disabled, Low, Medium, High, and Highest. Wherein "Low" is ideal for a slightly foggy environment and "Highest" for the foggiest environment.
Image Stabilization	This feature has no obvious effect under normal viewing conditions. However, if the camera is installed inside a moving vehicle, such as a train, etc., enable this feature to make the image stable even when the environment is in constant motion.

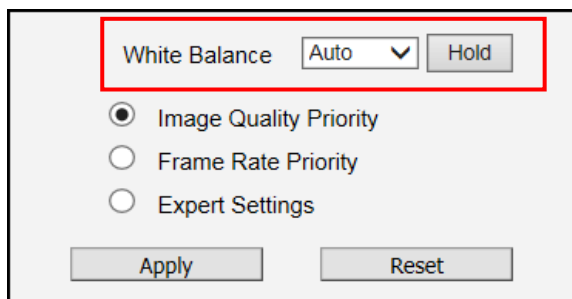
After changing any of the items above, press **Apply** to save the changes. The **Reset** button undoes the changes that had just been made but not Applied yet.

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

Exposure / White Balance

Exposure/White Balance

The section **Exposure / White Balance** allows the user to configure Exposure (shutter, iris and gain control) and White Balance settings. In most cases, the default settings are sufficient and no adjustment is needed. Some options will only appear under certain Exposure / White balance modes. Each mode is described in detail below.



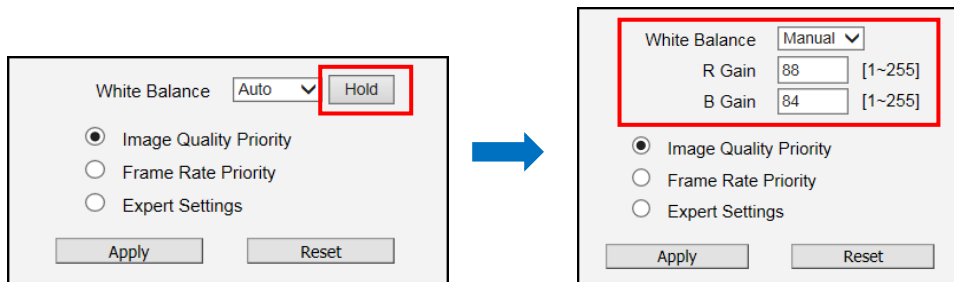
White balance refers to the capability of the camera to understand what “true white color is”. When the camera knows the true white color, then the rest of the colors will be accurate, too. While human eye can easily adapt to different lighting sources (even mixed sources, such as sun light through the window and indoor lights turned on at the same time), the camera has to understand what is the dominant light source in given scene and what is the “white color” of such light source.

By default the camera is in **auto white balance** mode and attempts to recognize the light source and its color spectrum automatically and adjusts the image accordingly. This function works continuously in the background. It is re-evaluated for each frame, to make sure if there is any change in dominant light source (e.g. the user closes the curtains to block the sun light and turns on the indoor lights).

In most cases the auto white balance works perfectly and the user does not have to adjust anything! In some rare installation cases, especially when there are no white color objects in the field of view, and the light sources are mixed, the camera may have difficulty to identify the true white color to fine tune the rest of the colors.

In such cases, the installer can “help” the camera to understand the true colors by placing a white object (for example a piece of white paper) in front of the camera to cover the whole field of view and wait a few seconds – the auto white balance system will adjust the colors until the white paper will really look white on the display. At that moment, the user can freeze these white balance settings by pressing the **Hold** button. After pressing that button, the White Balance will switch from Auto mode to Manual mode, together with the color values captured at the moment of

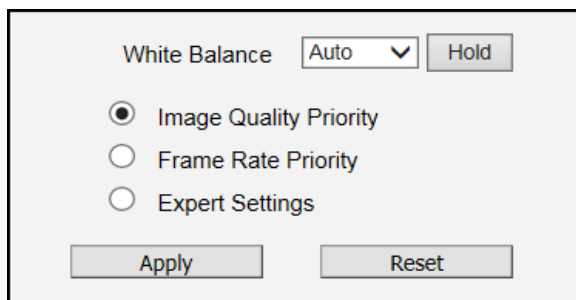
Hold. The user can now remove the white object from the field of view, and the colors will stay correct for given scene.



For advanced users, there is also an option to switch from Auto mode to **Manual mode** of White Balance directly and input the R Gain and B Gain values manually.

To simplify exposure settings, the camera firmware sets the “Slowest Auto Shutter Speed” to achieve two exposure control settings, namely:

- **Image Quality Priority**
- **Frame Rate Priority**

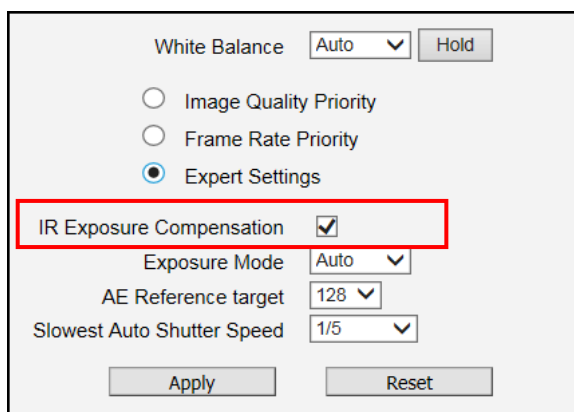


Select **Image Quality Priority** if users want to get a clear image of static objects but accept motion blur for fast moving objects in low light.

Select **Frame Rate Priority** if users do not want to have motion blur but accept noise on the image in low light.

For advance users, select **Expert Settings** to display and manually configure the exposure settings.

IR Exposure Compensation – Enabled



White Balance

Image Quality Priority
 Frame Rate Priority
 Expert Settings

IR Exposure Compensation

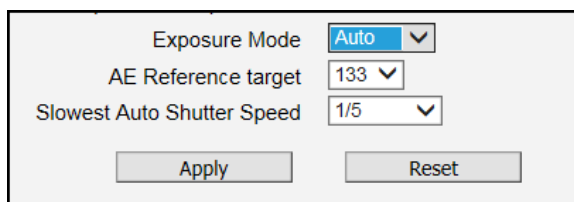
Exposure Mode

AE Reference target

Slowest Auto Shutter Speed

IR Exposure Compensation is available on all cameras with IR LEDs. This feature automatically balances the IR exposure to eliminate over-exposed images caused by too much IR on the subject. When enabled, the AE reference target is automatically adjusted to control the sensor's shutter speed and gain to compensate IR effect.

Exposure Mode - Auto



Exposure Mode

AE Reference target

Slowest Auto Shutter Speed

In Auto Exposure Mode, you control the image brightness by configuring the AE Reference Target and Slowest Auto Shutter.

AE Reference Target (Auto Exposure reference target) can be considered as the “Target Brightness on Sensor”. The camera will use several internal parameters to achieve best quality with reference to this. **The higher this value, the brighter the overall scene, however, there may be more noise at night in such case.** The range of AE Reference Target is 1~255.

The camera will automatically control shutter speed, auto iris (if available) and signal gain to achieve the target level set by the user. If the auto iris does not exist or is already opened to a maximum size, and the image is still darker than the user defined target, it will further slow down the shutter speed within the allowed range (set by user under Slowest Auto Shutter Speed) and increase the signal gain.

Slowest Auto Shutter Speed is the user defined threshold for slowest allowed speed of auto shutter. For example, if by default the shutter speed would vary between 1/5s ~ 1/2000s depending on the lighting conditions, then setting the Slowest Auto Shutter Speed to 1/30s would narrow down the auto shutter range to work between 1/30s ~ 1/2000s. The purpose of allowing user to define the threshold for slowest speed is to avoid motion blur caused by too slow shutter at night.

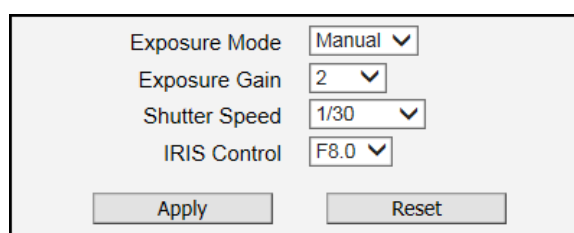
It is also important to know that very high shutter speed is not recommended for indoor solutions with artificial light that flashes with certain frequency, as it may produce flickering effect, regardless of Exposure mode.

In extreme low light conditions, the shutter speed is slow down to get more light into one image, but not slower than the user defined threshold.

If the exposure time extends beyond the interval between frames (too slow shutter), (i.e. 1/30 second), then the frame rate will be automatically reduced. **Longer time in this value gives clearer images at night for slow moving objects, but more motion blur for fast moving objects.**

Exposure Mode - Manual

When the lighting conditions are stable 24 hours a day, the advanced users may consider using manual exposure mode, to further fine tune the image quality in order to fulfill the special project requirements. Please note that in most cases, it is highly recommended to keep the camera in Auto Exposure mode and let the intelligent system of the camera find the best possible exposure settings instead.



Exposure Mode	Manual
Exposure Gain	2
Shutter Speed	1/30
IRIS Control	F8.0
<input type="button" value="Apply"/> <input type="button" value="Reset"/>	

In manual exposure mode, the user can directly manually adjust the signal **Exposure Gain**, **Shutter Speed**, and even on select models, the **IRIS Control** (I-series zoom cameras only).

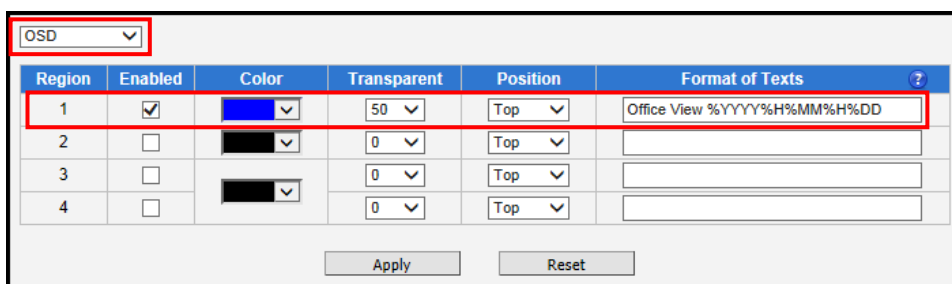
NOTE: WDR is disabled in manual exposure mode (see *Image* on page 54).

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

OSD

OSD The section **OSD** (or **OSD / Privacy Mask** as shown in some cameras) allows users to add text to the upper or lower left corner of the video. This function is called **Text Overlay** or **On-Screen Display (OSD)**. It is possible to display the camera name, date and time, IP address or any custom text as Text Overlay. **The text is kept as small as possible and is not resizable.** The text can be read normally when the video is enlarged on the display to 1:1 ratio. The purpose of having the text so small is to provide sufficient legal evidence while blocking the smallest possible area of the video to avoid valuable video evidence being blocked by text overlay. The text will be embedded into video and cannot be removed later upon playback or export.

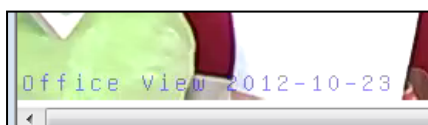
It is possible to define up to 4 regions of text. If more than 1 region of text is **enabled** and positioned in the same location, then the texts will appear one below another, row by row.



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

Buttons: Apply, Reset

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



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

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

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

Privacy Mask



Privacy Mask allows (or OSD/pusers to cover up some sensitive areas of the

video that should not be captured by the camera, such as manager's computer screen or bathroom ntrance. 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.

NOTE: Privacy Mask is not available on hemispheric cameras in ePTZ mode.

On some cameras, **OSD** and **Privacy Mask** appear together on the same page tab as "OSD/Privacy Mask".

Privacy Mask of Fixed, Varifocal and Zoom Cameras

NOTE: This section describes the privacy mask setup for fixed and varifocal cameras, as well as zoom cameras under the E-series and models B210 and B410. For other zoom camera models, please refer to **Error! Reference source not found.** on page **Error! Bookmark not defined.**

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

Privacy Mask (Don't overlap privacy mask regions)

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



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

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

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



Please note that the Text Overlay (OSD) and Privacy Masks will take effect for both Stream 1 and Stream 2.

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

NOTE:

1. It may take several seconds to update the region location on video display after pressing **Apply**!
2. The privacy mask set on zoom cameras is retained on its original position. The image which is masked may move out of the masked area when the camera is zoomed in or out.

On-Screen Graphics

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

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

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

For example, one free trial version of YUV converter can be downloaded from Sunrayimage.com: http://www.sunrayimage.com/download/YUVTools_3.0_trial.zip

We do not guarantee the performance, terms of usage or availability of this product. The user has to read the terms of use first and proceed with installation if the terms are acceptable.

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

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



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

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

Upon successful entry of user name and password, the following upload window will appear.

Browse for the **yuv** file in your computer that you had prepared and press **Apply**.



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

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

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

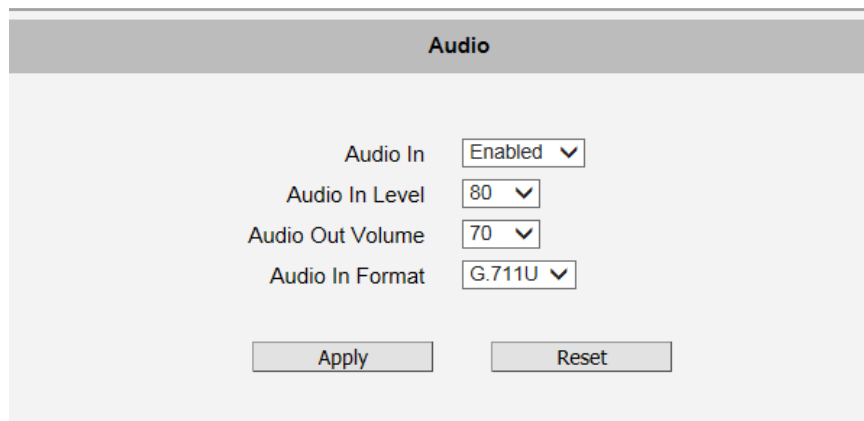
Parameter Position	Description
1	1 means enabled, 0 means disabled
2	X position
3	Y position
4	Width of the image
5	Height of the image
6	YYUUVV value of the background color of the image that is to be blended
7	Transparency level: 0 means 0%, 1 means 25%, 2 means 50%, 3 means 75%, 4 means 100%

The result would look like this:



Audio

Audio The section **Audio** is available only for audio-supported models. The user interface for audio control looks as below:



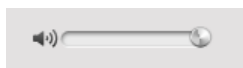
Parameters	Description
Audio In	The option “Enabled” would activate incoming audio (either active or passive microphone). The option “Disabled” would turn off the incoming audio. In such case, the video stream is captured without audio.
Audio In Level	Use this function to adjust the sensitivity level of audio input.
Audio Out Volume	The audio out volume level can be adjusted in the scale of 0-100. It will influence the volume level of the speakers connected to the camera.
Audio Format	Displays audio format: G.711U (<i>μ-law</i>).

To adjust the volume level of the speakers connected to the PC that runs the Web Configurator in order to hear the audio from the camera’s microphone or line-in device, go to **Live View** page and use the audio controls there:

Audio Muted:



Audio level adjusted to the maximum:



This volume control appears in user interface only when the Audio-in function of the camera has been “Enabled”.

System

System

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

User Account

User Account

The section User Accounts allows doing following user management tasks:

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

User Account

Live view without account name and password

User	Account	Password
Root	<input type="text" value="admin"/>	<input type="text" value="123456"/>
User 1	<input type="text"/>	<input type="text"/>
User 2	<input type="text"/>	<input type="text"/>
User 3	<input type="text"/>	<input type="text"/>
User 4	<input type="text"/>	<input type="text"/>
User 5	<input type="text"/>	<input type="text"/>
User 6	<input type="text"/>	<input type="text"/>
User 7	<input type="text"/>	<input type="text"/>
User 8	<input type="text"/>	<input type="text"/>
User 9	<input type="text"/>	<input type="text"/>
User 10	<input type="text"/>	<input type="text"/>

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

System Info

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

System Information

System Information :

Firmware Version = A1D-500-V6.xx.xx-XX
 MAC Address = 00:0F:7C:0C:D9:D1
 Production ID = B47--A-XX-14C-00014
 Model Number = B47
 Factory Default Type = Two Ways Audio (0x71)
 Company Name = ACTI Corporation
 WEB Site = www.acti.com
 Build Revision = 1

WAN Status :

WAN_TYPE='2'
 WAN_IP='172.16.26.4'
 WAN_NETMASK='255.255.255.0'
 WAN_GATEWAY='172.16.26.252'
 DNS_PRIMARY=""
 DNS_SECONDARY=""
 MAC='00:0F:7C:0C:D9:D1'
 BONJOUR_CONFIG='1,B47--A-XX-14C-00014'

System Log :

Mount jffs2 filesystem
 Devcap Version B47_20150717_01
 Loading System Config files ...
 Bootloader Version BOOTLOADER-500-V01.15
 Starting network interface ...
 Starting 802.1x Authentication ...
 802.1x disabled.
 Loading GetJiffies driver

Config file:

The unit's parameters and their current settings.

Always attach the server report when contacting your support channel.

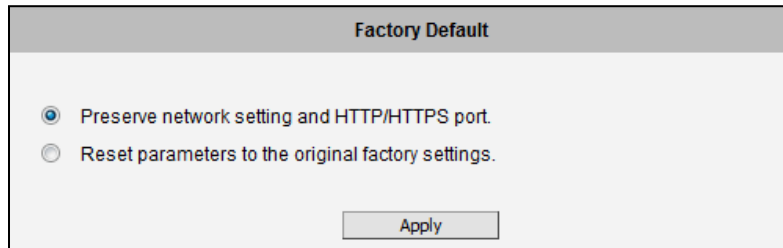
Third party software licenses.

The **Server Report** is a convenient way of exporting the full list of camera 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 section **Factory Default** allows the camera 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.
- Reset parameters to the original factory settings.

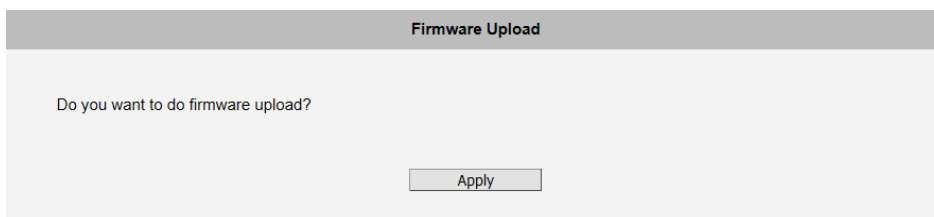
Below the options is an "Apply" button.

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

Firmware Upload

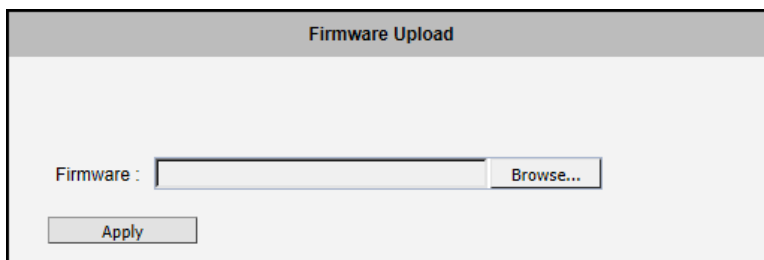
Firmware Upload The section **Firmware Upload** allows remote upgrade or downgrade of camera firmware. The upgrade to newer version is usually done in order to gain new functions or fix existing bugs or limitations while downgrade to older version is used mostly for integration purposes where the newly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

Firmware uploading can be done by selecting the firmware image manually.



Firmware Upload from Local

To upload the firmware manually, download the firmware image file, which contains the file extension “.upg”, from the website. Choose “Firmware Upload from Local” and press the **Apply** button.

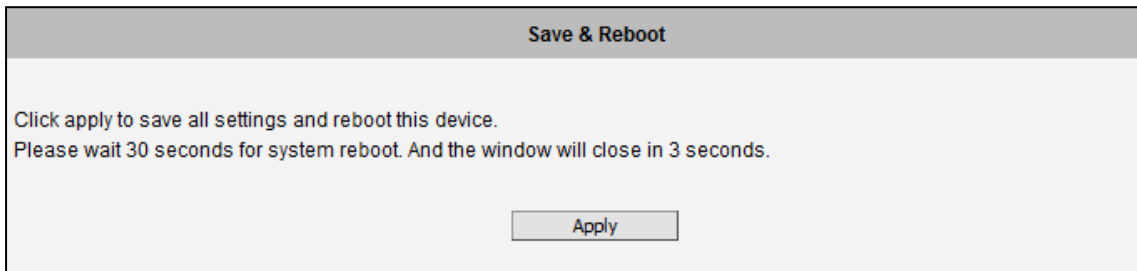


Click **Browse** to select the downloaded firmware image file. Click the **Apply** button to start the upload.

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

Save & Reboot

Save & Reboot The **Save & Reboot** section allows saving the settings and rebooting the camera 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.

Troubleshooting

Although the default settings of the camera are ideal for 90% of the cases, there may be some rare cases when the settings need to be adjusted or the device has to be examined. The following section provides easy troubleshooting solutions for most cases. In some occasions, the unexpected symptoms may be the result of selecting the product that is not suitable for given environment.

For more detailed explanations and instructions of each situation, please refer to the complete **Troubleshooting Guide** at http://www.acti.com/kb/detail.asp?KB_ID=KB20130130001

Image Quality Troubleshooting	
Problem	Solution
Motion blur	Increase shutter speed
Blurry image	Auto Focus: Refocus button; Manual focus: adjust manually
Too narrow DoF	Reduce aperture size, widen the viewing angle, install camera farther from objects
Too narrow viewing angle	Vari-focal lens: widen the viewing angle; Zoom lens: press the zoom-out button; Fixed lens: replace it with wide angle fixed lens or choose another model with wide angle lens
Objects too small	Increase video resolution; zoom-in (zoom lens) or adjust lens to telephoto position (vari-focal); Install the camera closer to target; Change to the lens with longer focal length; Change the camera model with higher resolution or longer focal length
Underexposed image	Use Auto Exposure Mode and increase AE Reference Target; set the Slowest Auto Shutter Speed to slowest possible (1/5s); Add external light source to illuminate the area the camera is shooting
Overexposed image	Use Auto Exposure Mode and reduce AE Reference Target if necessary
Noise	Enable DNR; Enlarge the aperture; Lower AE Reference Target in Auto Exposure mode; Lower the Exposure Gain in Manual Exposure mode; Lower video resolution; Add extra visible or IR lights
Blocking & mosaic	Increase the bitrate
Wrong colors or color rolling	Manually correct the colors by using white paper "Hold" button in Auto White Balance mode; Adjust the camera's position or viewing direction; Adjust the light source
Black image	Make sure there is sufficient light; Make sure the Day/Night Mode and IR LED Control are both in Auto mode; Make sure that the "Switch from Day mode to Night mode" does NOT have the most extreme value – 100; Manual iris: open the iris by rotating the ring towards "O"; Remove the protective cap of the lens during installation

IR light reflection	Make sure the dome or bullet cover is tightly mounted; Reduce the AE reference target in Auto Exposure mode; Reduce the Exposure Gain in Manual Exposure mode
---------------------	---

Streaming Quality Troubleshooting	
Frame Rate Too Low at Night	In auto exposure mode, set the Slowest Auto Shutter Speed to be not slower than the interval of frames; In manual exposure mode, set the Shutter Speed to be not slower than the interval of frames
Latency	Use dual stream (stream 1 for recording, stream 2 for live view); Lower the bitrate; Lower the resolution (if acceptable for user); Check the cable quality; Make sure to use industrial grade switches and routers; Check the NVR server & client PC requirements from NVR manual
Jitter	Use the NVR that has the video smoothening algorithm for live view and playback
Dropped Frames	Use the Playback function of NVR – use frame-by-frame validation of jitter-looking sections, to see if any frames are dropped; To troubleshoot the data switch/router and VMS computer, you may also ask for assistance from technical support team of camera manufacturer



Copyright © 2015, ACTi Corporation All Rights Reserved

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

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

Email: sales@acti.com