ALL2295

Full HD Vandal Proof IP Outdoor Dome Camera

User's Manual

V1.0

Table of Contents

1. OVERVIEW 4
1.1 FEATURES 4
1.2 PACKAGE CONTENTS 5
2. INTRODUCTION OF THE IP DOME CAMERA 6
2.1 CAMERA DIMENSIONS 6
2.2 CAMERA'S CONNECTORS 7
3. SYSTEM REQUIREMENTS 9
4. DELETING THE EXISTING DC VIEWER 10
5. INSTALLATION 14
5.1 POWER AND ETHERNET CABLE CONNECTION 14
5.2 HARD CEILING 15
5.3 4S MOUNT ELECTRICAL BOX 21
6. ACCESSING CAMERA 24
7. CONFIGURATION & OPERATION 32
7.1 BROWSER-BASED VIEWER INTRODUCTION 32
7.2 HOME PAGE 34
7.2.1 Vari-focal Model 34
7.2.2 Motorized Model 36
7.3 SYSTEM RELATED SETTINGS 40
7.3.1 Host Name and System Time Setting 41
7.3.2 Security 43
7.3.3 Network 56
7.3.4 DDNS 67
7.3.5 Mail 69
7.3.6 FTP 70
7.3.7 HTTP 71
7.3.8 Application 72
7.3.9 Motion Detection 79
7.3.10 Tampering 84
7.3.11 Storage Management 87
7.3.12 Recording 90
7.3.13 File Location 91
7.3.14 Iris Adjustment 92
7.3.15 View Log File 93
7.3.16 View User Information 94
7.3.17 View Parameters 96
7.3.18 Factory Default 97
7.3.19 Software Version 98
7.3.20 Software Upgrade 99
7.3.21 Maintenance 102
7.4 VIDEO AND AUDIO STREAMING SETTINGS 104
7.4.1 Video Resolution and Rotate Type 104
7.4.2 Video Compression 108
7.4.3 Video OCX Protocol 110
7.4.4 Video Frame Skip 111
7.4.5 Video Mask 112

7.4.6 Audio Mode and Bit Rate Settings 113
7.5 CAMERA SETTINGS 115
7.5.1 Exposure Setting 116
7.5.2 White Balance Setting 117
7.5.3 Brightness Setting 118
7.5.4 Sharpness Setting 118
7.5.5 Contrast Setting 118
7.5.6 Saturation Setting 119
7.5.7 Hue Setting 120
7.5.8 IR Function 120
7.5.9 TV System Setup 120
7.6 LOGOUT 122
8. CMS SOFTWARE INTRODUCTION 123
APPENDIX A: TECHNICAL SPECIFICATIONS 124
APPENDIX B: INTERNET SECURITY SETTINGS 127
APPENDIX C: DC VIEWER DOWNLOAD PROCEDURE 132
APPENDIX D: INSTALL UPNP COMPONENTS 135

1. OVERVIEW

The Full HD Vandal Proof IP Dome Camera is capable of serving real-time streaming and makes image quality more smoothly. In addition to MJPEG real time streaming, this camera develops H.264 codec to apply for high resolution digital broadcast.

With compact and sophisticated mechanical design, the Full HD Vandal Proof IP Dome Camera is easy installed and aesthetic. Additionally, the IP Dome Camera's vandal proof cover can protect the camera from heavy damage.

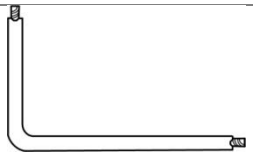
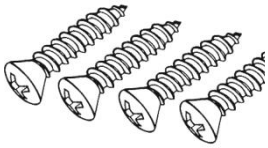
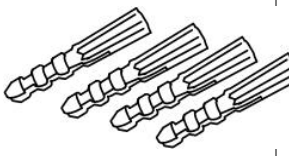
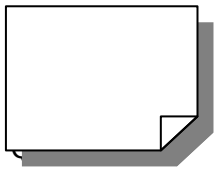
1.1 Features

Progressive Scan CMOS Sensor
Full HD 1080p / HD 720p real-time at dual streaming
H.264 and MJPEG compression
Motion Detection
Privacy Masks
Day/Night (ICR)
Micro SD support
BNC analog output
Weatherproof (IP66 international)
Vandal proof dome cover
Sun Shield & Outdoor Mounting Kit
ONVIF Support

1.2 Package Contents

Please check the package contains the following items listed below.

Camera Package Contents

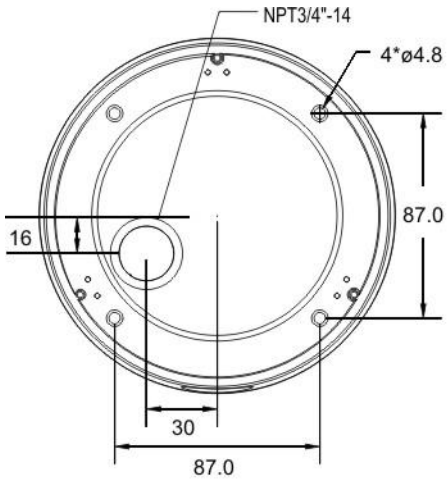
Vandal Proof IP Dome Camera	DC Jack Cable	
Power Terminal Block	 Security Torx	
 Self Tapping Screws (×4)	 Plastic Screw Anchors (×4)	Rubber Washers (× 6)
CD (bundled software and documentation)		

2. INTRODUCTION OF THE IP DOME CAMERA

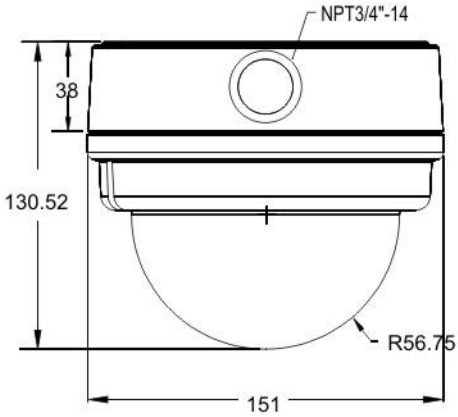
This chapter will provide the camera dimensions for reference before installation. Definition of each connector on the camera's PCB board will also be specified.

2.1 Camera Dimensions

The IP Dome Camera's dimensions are shown below.



Top View

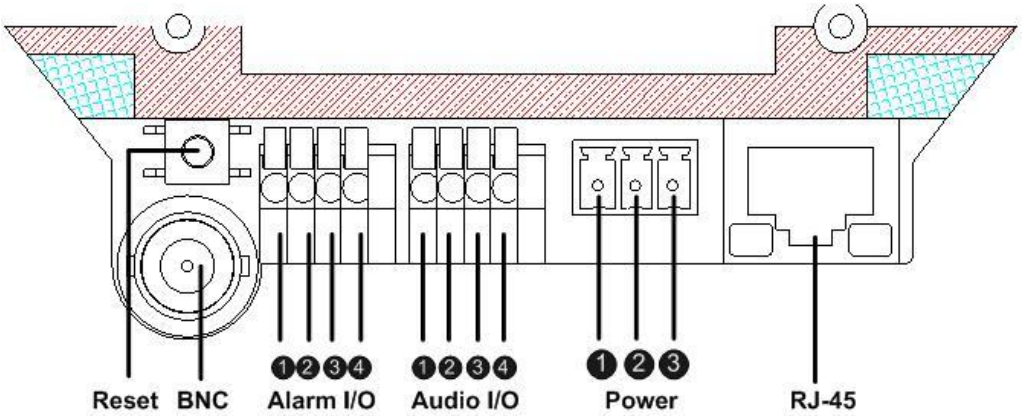


Side View

Unit: mm

2.2 Camera's Connectors

The diagram below shows the IP Dome Camera's reset button and various connectors. Definition for each connector will be given as follows.



Connector		Pin No.	Definition	Remarks
Reset Button		-	Restore to factory default	
BNC		-	Analog Video Output	
Alarm I/O		1	Output＋	Alarm connection
		2	Output－	
		3	Input＋	
		4	Input－	
Audio I/O		1	Input	Two-way audio transmission
		2	GND	
		3	Output (R)	
		4	Output (L)	
Power	**DC 12V**	1	Power	Power connection
		2	Reserved	
		3	GND	
	AC 24V	1	Power-1	
		2	Earth GND	
		3	Power-2	
RJ-45		-	10/100 Mbps Ethernet / PoE	

3. SYSTEM REQUIREMENTS

To perform the IP Camera via web browser, please ensure your PC is in good network connection, and meet system requirements as described below.

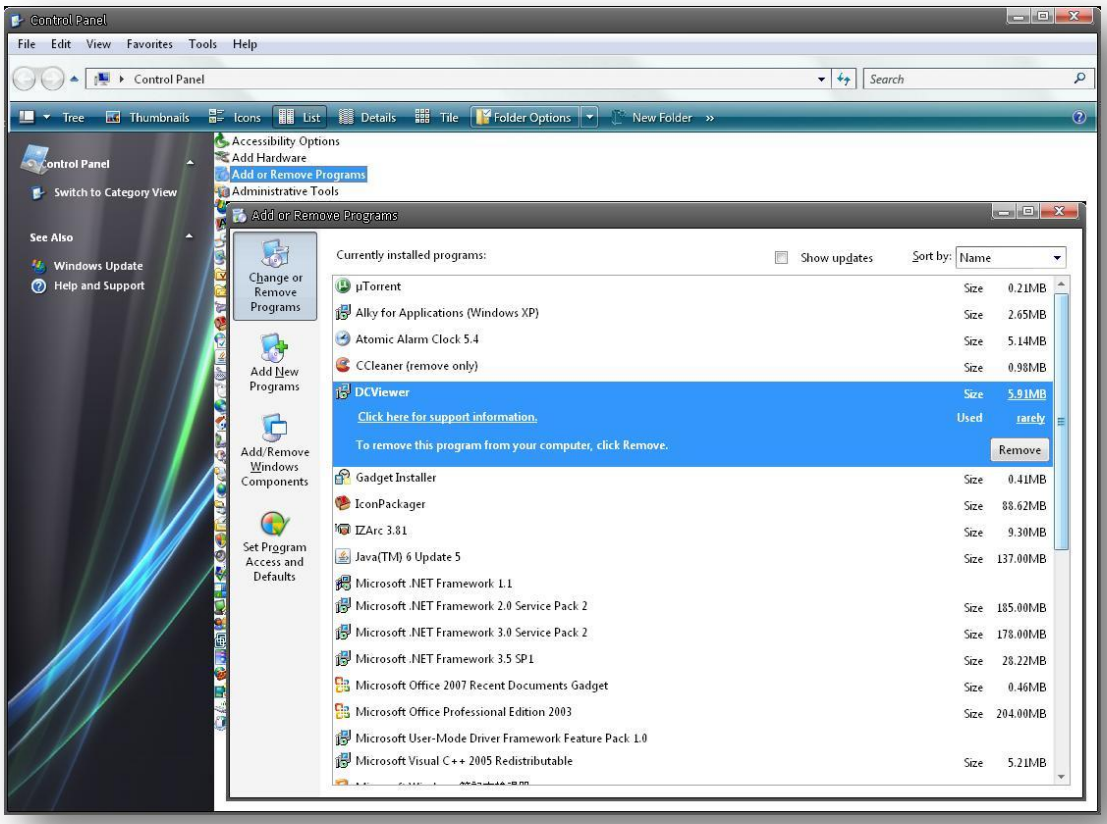
Items	System Requirement
Personal Computer	1. Intel®, Pentium®, M, 2.16 GHz or Intel®, Core™2 Duo, 2.0 GHz 2. 2 GB RAM or more
Operating System	Windows VISTA/ Windows XP/ Windows 7
Web Browser	Microsoft Internet Explorer 6.0 or later Firefox Chrome Safari
Network Card	10Base-T (10 Mbps) or 100Base-TX (100 Mbps) operation
Viewer	ActiveX control plug-in for Microsoft IE

4. DELETING THE EXISTING DC VIEWER

For users who have installed the DC Viewer in the PC previously, please first delete the existing DC Viewer from the PC before accessing to the IP Camera.

Deleting the DC Viewer

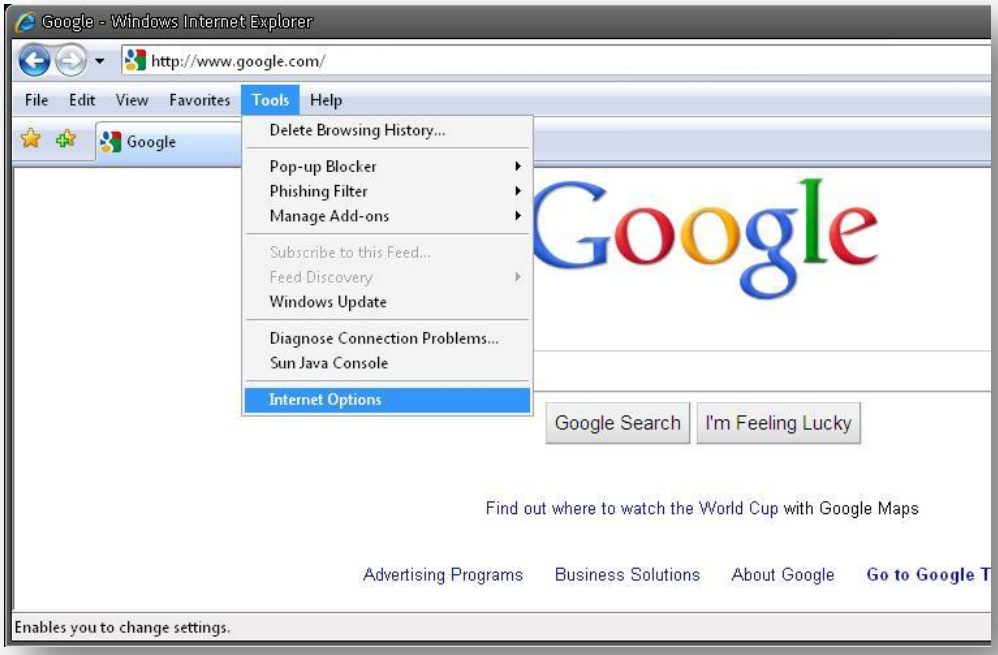
Click “Control Panel”, and then double click “Add or Remove Programs.” In the “Currently installed programs” list, select “DCViewer” and click the button “Remove” to uninstall the existing DC Viewer as shown in the figure below.



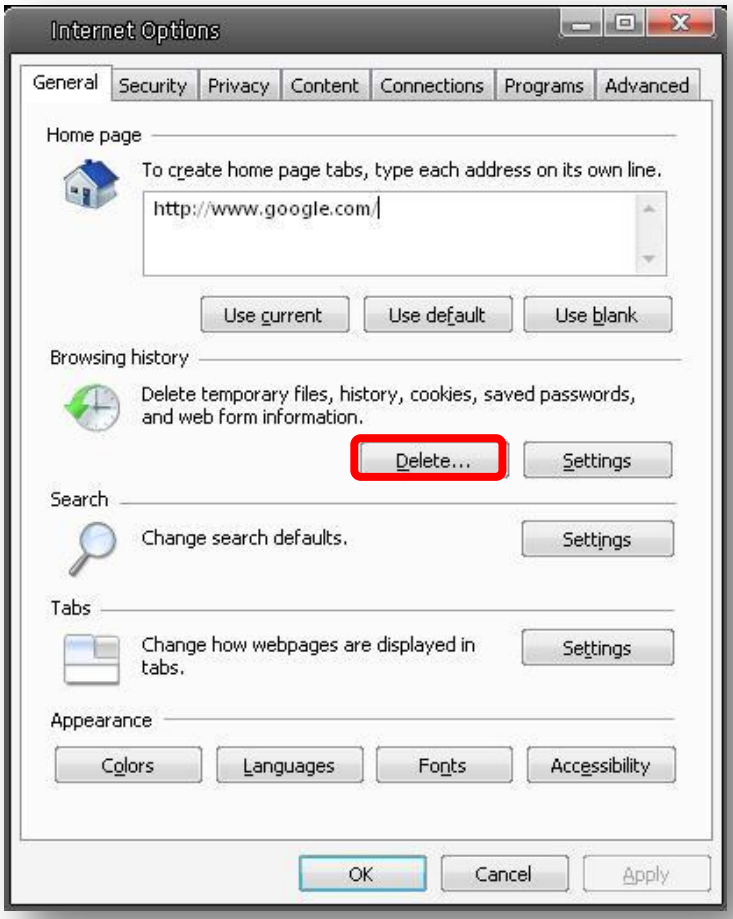
Deleting Temporary Internet Files

To improve browser performance, it is suggested to clean up the all the files in the Temporary Internet Files. The procedure is as follows:

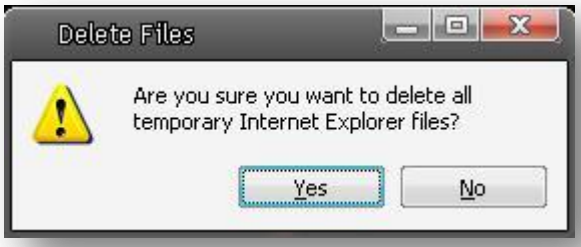
STEP 1: Click the “Tools” tab and select the option “Internet Options.”



STEP 2: Click on “Delete”, then tap the “Delete Files” in the “Temporary Internet files” section.


Internet Options
General
Security
Privacy
Content
Connections
Programs
Advanced
Home page
To create home page tabs, type each address on its own line.
http://www.google.com/
Use current
Use default
Use blank
Browsing history
Delete temporary files, history, cookies, saved passwords, and web form information.
Delete...
Settings
Search
Change search defaults.
Settings
Tabs
Change how webpages are displayed in tabs.
Settings
Appearance
Colors
Languages
Fonts
Accessibility
OK
Cancel
Apply

The popup window for confirmation will come out as shown below. Click “Yes” to start deleting the files.



5. INSTALLATION

Please read the instructions provided in this chapter thoroughly before installing the Full HD Multi-Res Vandal Proof IP Dome Camera.

5.1 Power and Ethernet Cable Connection

Power Connection

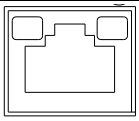
Make sure the camera's power cable is correctly and firmly connected; refer to the pin definition table in section 2.2 Camera's Connectors. If using Power over Ethernet (PoE), make sure Power Sourcing Equipment (PSE) is in use in the network.

Ethernet Cable Connection

Use of Category 5 Ethernet cable is recommended for network connection; to have best transmission quality, cable length shall not exceed 100 meters. Connect one end of the Ethernet cable to the RJ-45 connector of the IP Dome Camera, and the other end of the cable to the network switch or PC.

NOTE: In some cases, you may need use an Ethernet crossover cable when connecting the IP Dome Camera directly to the PC.

Check the status of the link indicator and activity indicator LEDs; if the LEDs are unlit, please check LAN connection.

	Green Link Light indicates good network connection. Orange Activity Light flashes for network activity indication.

5.2 Hard Ceiling

The Vandal Proof IP Dome Camera can be installed directly on a wall or ceiling. Please note that the wall or ceiling must have enough strength to support the IP Dome Camera.

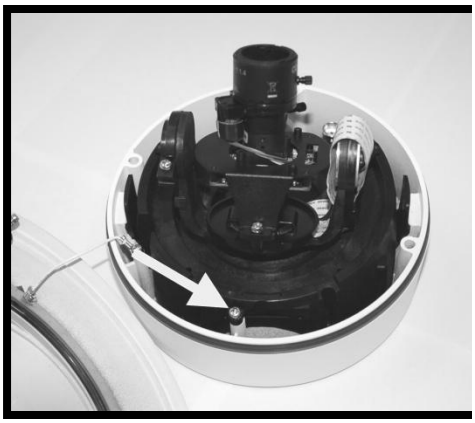
Follow the steps below to install the IP Dome Camera:

Step 1:
Unpack the Vandal Proof IP Dome Camera package and take out the IP Dome Camera.

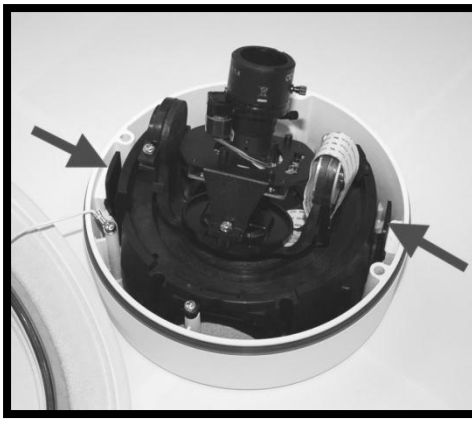
Step 2:
Use the supplied Security Torx to unscrew the two Torx screws on the side of the Dome Cover, as shown in the figure, and open the Dome Cover.

Step 3:
Press both sides of the Inner Cover and remove it from the Dome Camera unit.

Step 4:
Unscrew the module-fastened screw, as indicated in the figure.



Step 5:
Press the sides of the snap-on module, as indicated in the figure, and detach it from the Dome Camera's housing.



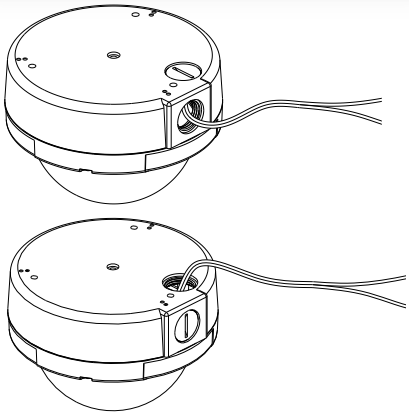
Step 6:
Mark the positions of the four screw holes on the base of the Dome Camera at the chosen installation location.

Step 7:
In the marked locations, drill each hole slightly smaller than the supplied screw anchors.

Step 8:
Put supplied anchors into these drilled holes.

Step 9:
Fasten the Dome Camera's housing with the four equipped self tapping screws.

Step 10:
Thread the power and Ethernet cables through either the side conduit entry or back conduit entry, as illustrated. Users may use a coin to screw off the conduit entry block.



NOTE: The Power Cable is omitted if using PoE.

Step 11:
Connect the power and Ethernet cables to the mating connectors on the Dome Camera unit.

Step 12:
Attach the snap-on module into the Dome Camera housing, and screw the module-fastened screw tightly to secure the camera module.

NOTE: The terminal blocks should face the side conduit entry, as shown in the figure.

Step 13:
Connect the power and network outputs.

NOTE: The Power Cable is omitted if using PoE.

STEP 14:
Access the camera browser-viewer for viewing images. Please refer to 6. Accessing Camera for further details. Users can also use the camera's BNC connector for video output.

Step 15:
Adjust the zoom ring screw to set the desired zoom; subsequently, modifying the focus ring screw to set the desired focal length.

Step 16:
Adjust the camera to a desired angle, as shown below. Pan adjustment range is nearly 360°; rotation angle range approaches to 270°. Tilt is adjustable between – 10° ~ 90°.

Pan Adjustment Rotation Adjustment Tilt Adjustment

NOTE: Adjust the lens carefully within the limits mentioned above, or the cables underneath would be harmed.

STEP 17:
Put the Inner Cover back to the Dome Camera unit.

STEP 18:
Replace the Dome Cover back, aligning the arrow mark on the Dome Cover with the one on the housing as shown in the figure.

STEP 19:
Screw on the two Torx screws on the side of the Dome Cover tightly to fasten the Dome Cover. Camera installation is complete.

5.3 4S Mount Electrical Box

Before installing the IP Dome Camera in the 4S Electrical Box, please unscrew and open the Dome Cover with the Security Torx.

Figure: 4S Mount Electrical Box

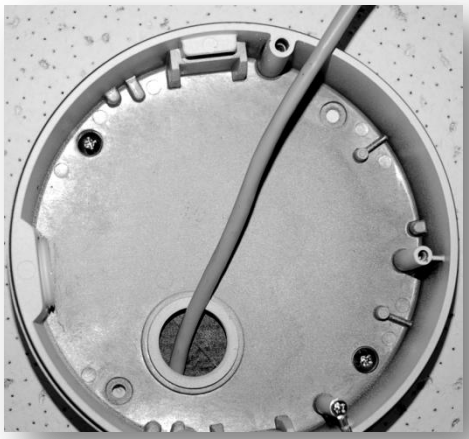
STEP 1:
Run the wires (Ethernet and power) through the wall.

NOTE: The power cable is omitted if using PoE.

STEP 2:
Disassemble the Dome Camera's Inner Cover (see the illustration in 5.2 Hard Ceiling: Step 3) from the Dome Camera unit.

STEP 3:
Detach the snap-on camera module from the Dome Camera's housing by unscrewing the module-fastened screw first. Then press the sides of camera module and pull it slightly up from the housing.

STEP 4:
Thread the power and Ethernet cables through either the side conduit entry or back conduit entry. Then fasten the Dome Camera's housing on the Electrical Box with the two screws.



STEP 5:
Connect the power and Ethernet cables to their connectors on the Dome Camera unit.

STEP 6:
Attach the snap-on camera module onto the Dome Camera's housing and. screw the module-fastened screw tightly to secure the camera module.

STEP 7:
Access the camera browser-viewer for viewing images. Please refer to
6. Accessing Camera for further details. Users can also use the camera's BNC connector for video output.

Step 8:
Adjust the camera's zoom level and focal length via zoom and focus ring screws.

STEP 9:
Position the camera at a desired angle by Pan/Tilt/Rotation adjustment.

STEP 10:
Replace the Dome Cover back, aligning the arrow mark on the Dome Cover with the one on the housing.

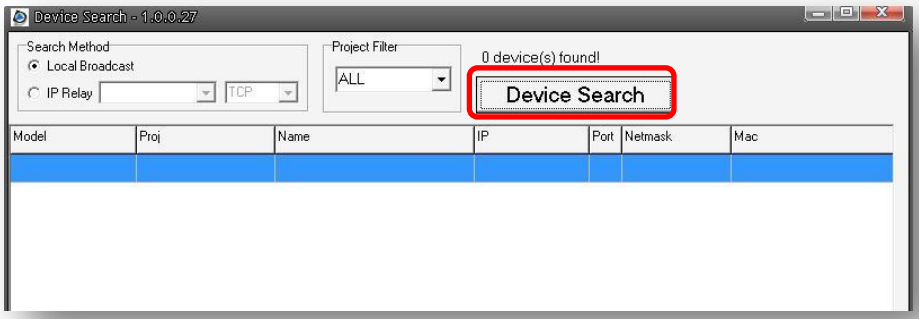
STEP 11:
Screw on the two Torx screws on the side of the Dome Cover tightly to fasten the Dome Cover. Camera installation is complete.

6. ACCESSING CAMERA

For initial access to the IP Camera, users can search the camera through the installer program: DeviceSearch.exe, which can be found in "DeviceSearch" folder in the supplied CD.

Device Search Software Setup

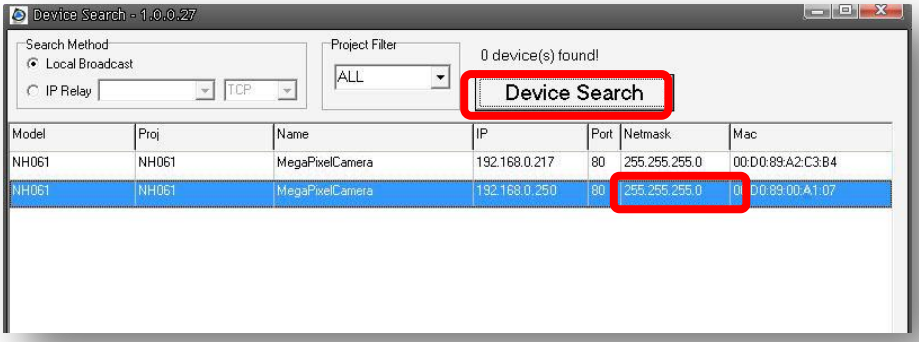
Step 1: Double click on the program Device Search.exe (see the icon below); its window will appear as shown below. Then click the "Device Search" button.



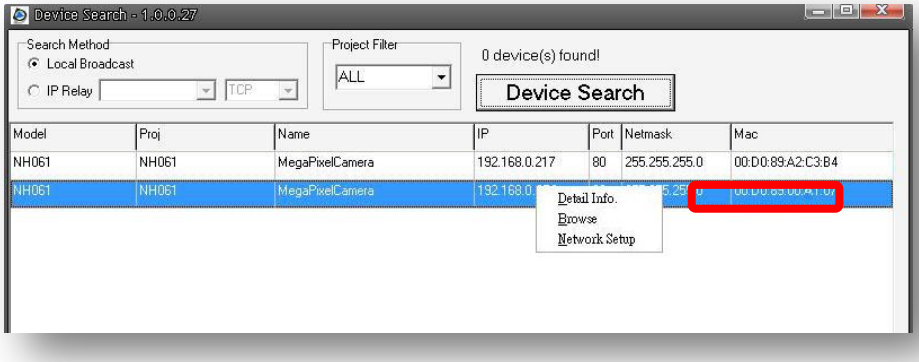
Step 2: The security alert window will pop up. Click "Unblock" to continue.

Device Search

Step 3: Click “Device Search” again, and all the finding IP devices will be listed in the page, as shown in the figure below. **The Camera don’t have a default IP Adress. It will be assigned by DHCP.**



Step 4: Double click or right click and select “Browse” to access the camera directly via web browser.



Step 5: Then the prompt window of request for entering default username and password (as shown below) will appear for login to the IP Dome Camera.

The default login ID and password for the Administrator are:

Login ID	Password
admin	admin

NOTE: ID and password are case sensitive.

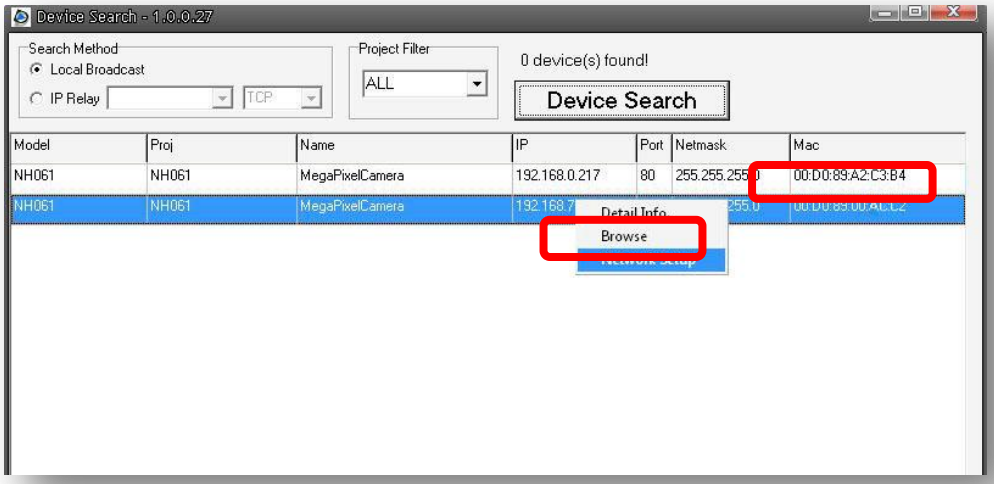
NOTE: It is strongly advised that administrator's password be altered for the security concerns. Refer to section 7.3.2 Security for further details.

Additionally, users can change the IP Camera's network property, either DHCP or Static IP directly in the device finding list. Refer to the following section for changing the IP Camera's network property.

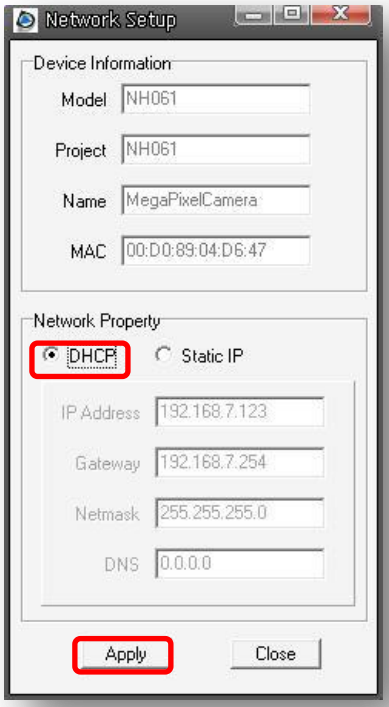
Example of Changing IP Camera's Network Property

Users can directly change an IP Camera's network property, ex. from static IP to DHCP, in the finding device list. The way to change the IP Camera's network property is specified below:

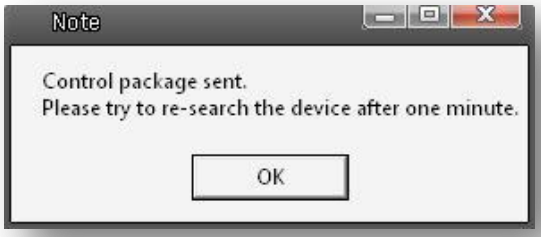
Step 1: In the finding device list, click on the IP Camera that you would like to change its network property. On the selected item, right click and select "Network Setup." Meanwhile, record the IP Camera's MAC address, for future identification.



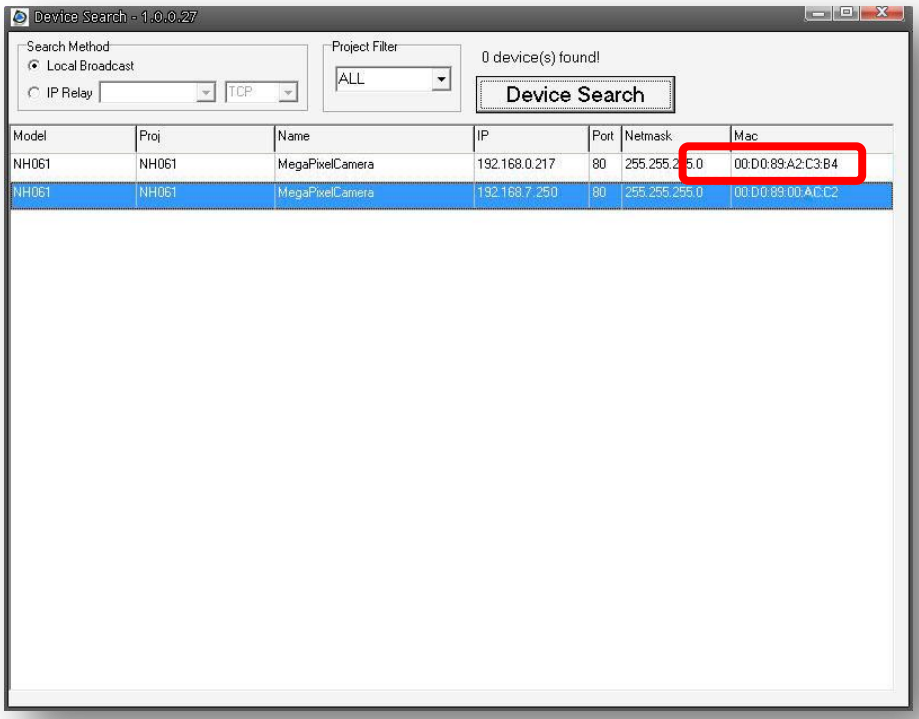
Step 2: The “Network Setup” page will come out. Select “DHCP,” and press “Apply” button down the page.



Step 3: Click “OK” on the Note of setting change. Wait for one minute to re-search the IP Camera.



Step 4: Click the “Device Search” button to re-search all the devices. Then select the IP Camera with the correct MAC address. Double click on the IP Camera, and the login window will come out.



Step 5: Enter User name and Password to access the IP Camera.

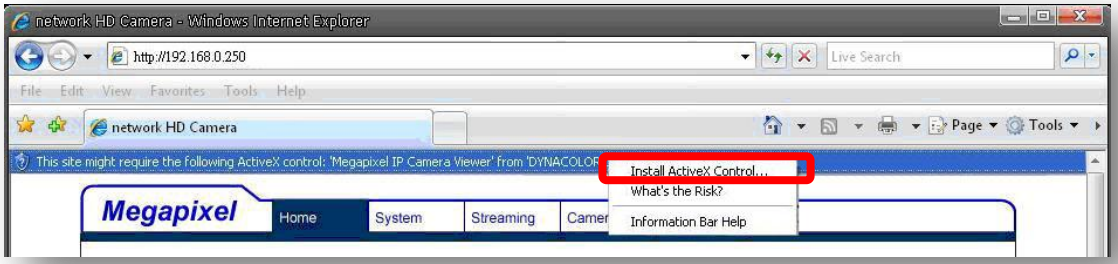
Installing DC Viewer Software Online

For the initial access to the IP Camera, a client program, DC Viewer, will be automatically installed to your PC when connecting to the IP Camera.

If the Web browser doesn’t allow DC Viewer installation, please check the Internet security settings or ActiveX controls and plug-ins settings (see Appendix B: Internet Security Settings) to continue the process.

The Information Bar (just below the URL bar) may come out and ask for

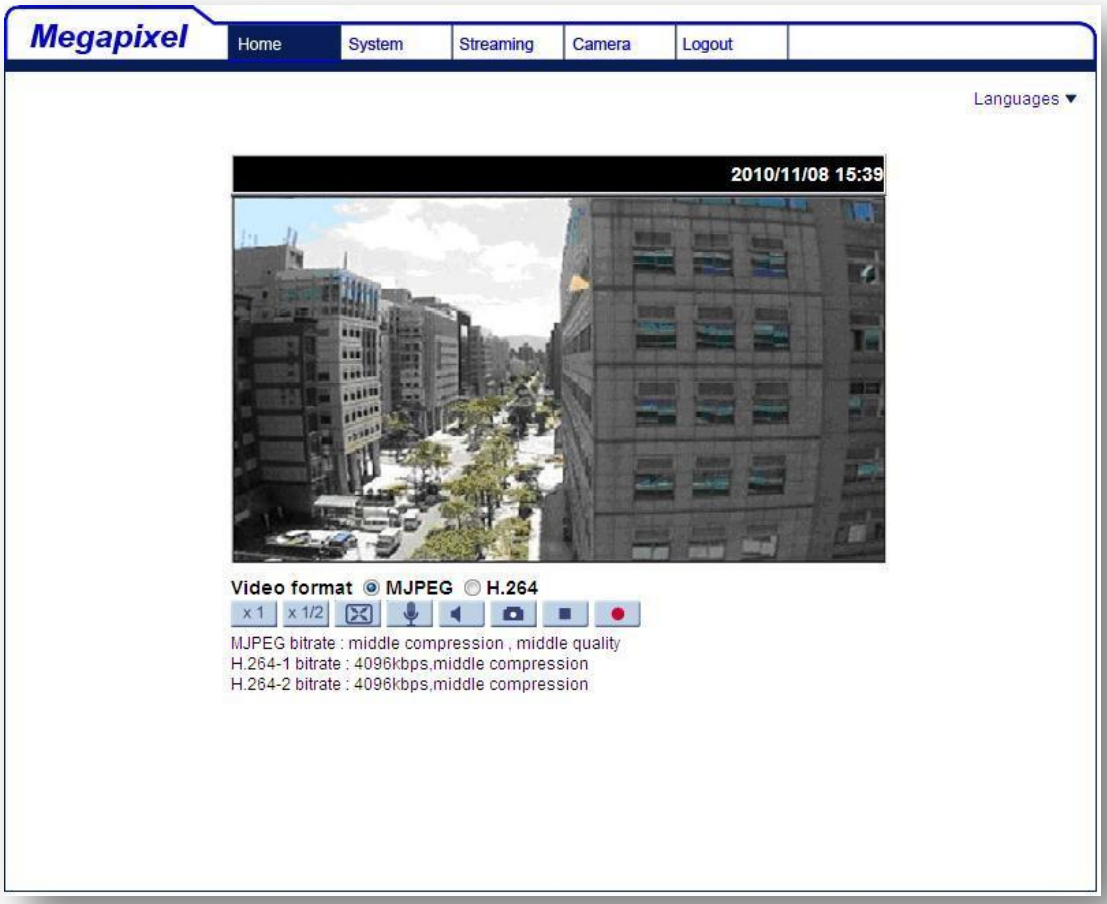
permission to install the ActiveX Control for displaying video in browser (see the figure below). Right click on the Information Bar and select “Install ActiveX Control…” to allow the installation.



Then the security warning window will pop up. Click “Install” to carry on software installation.
Click “Finish” to close the DC Viewer window when download is finished.
For the detailed software download procedure, please refer to Appendix C: DC Viewer Download Procedure.

Once login to the IP Camera, users will see the Home page as shown below:

Vari-focal Model



Administrator/User Privileges

"Administrator" represents the person who can configure the IP Camera and authorize users access to the camera; "User" refers to whoever has access to the camera with limited authority, i.e. entering Home and Camera setting pages.

Image and Focus Adjustment

The image displays on the Home page when successfully accessing to the IP Camera. Adjust zoom and focus as necessary to produce a clear image.

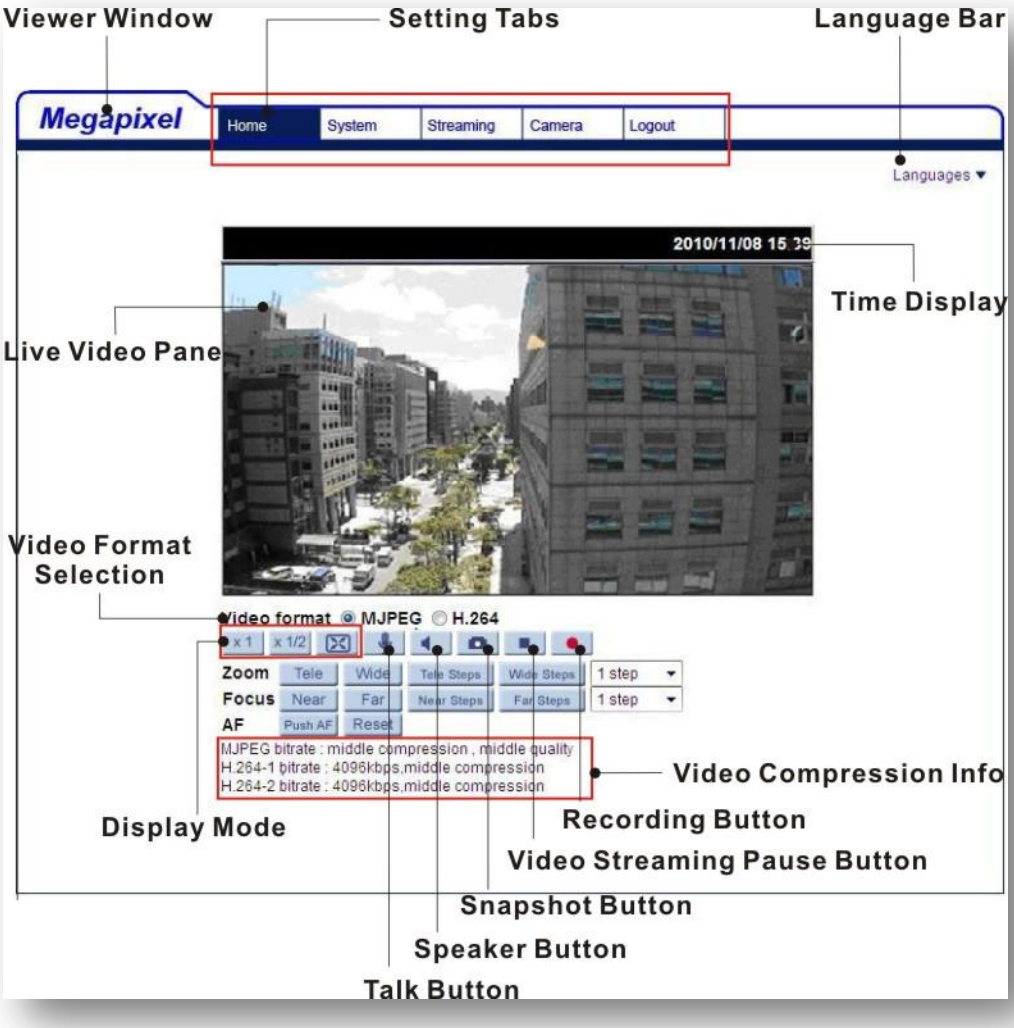
7. CONFIGURATION & OPERATION

The IP Camera is provided with a user-friendly browser-based configuration interface, and a free bundled CMS (Central Management System) for video playback and recording. In this chapter, information about main page introduction, system related settings and camera settings will be described in detail.

For further information about CMS software, please refer to 8. CMS Software Introduction and CMS user's manual.

7.1 Browser-based Viewer Introduction

The figure below shows the main page of the IP Camera user interface.



There are five tabs: Home, System, Streaming, Camera and Logout on the top panel.

Home
Users can monitor live video of the targeted area.

System setting
The administrator can set host name, system time, root password, network related settings, etc. Further details will be interpreted in section 7.3 System Related Settings.

Streaming setting
The administrator can modify video resolution and rotate type and select audio compression mode in this page.

Camera setting
Users can adjust various camera parameters, including <Exposure>, <White Balance>, <Brightness>, <Sharpness>, <Contrast>, <Saturation>, <Hue> and < TV System>.

Logout
Click on the tab to re-login the IP Camera with another username and password.

7.2 Home Page

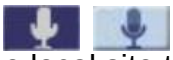
In the Home page, there are several function buttons right down the displayed image.

7.2.1 Vari-focal Model

Multiple Languages Support
Multiple languages are supported, including German, English, French, Italian, Russian, etc., for the viewer window interface.

Screen Size Adjustment
Image display size can be adjusted to x1/2 and full screen.

Digital Zoom Control
In the full screen mode, users can implement digital PTZ by rotating the mouse wheel (for zoom in/out), and drag the mouse into any direction.

Talk button (on/off) 
Talk function allows the local site to talk to the remote site. Click on the button to switch it to on/off. Please refer to section 7.3.2 Security: Add user >> Talk/Listen for further details. This function is only open to “User” who has been granted this privilege by the Administrator.

Speaker button (on/off)
Press the Speaker button to mute/activate the audio.

Snapshot button
Press the button, and the JPEG snapshots will automatically be saved in the specified place. The default place of saving snapshots is: C:\. To change the storage location, please refer to section 7.3.12 File Location for further details.

NOTE: For users with Windows 7 operating system, it is required to log on as an Administrator to implement the Snapshot function.

Video Streaming Pause /Restart button
(pause/restart)
Press the stop button to disable video streaming, the live video will be displayed as black. Press the restart button to show the live video again.

Web Recording button (on/off)
Press the <Recording> button and the recordings from the Live View will be directly to the specific location on the local hard drive, which could be configured in the “File Location” (snapshot) page. The default storage location for the web recording is: C:/. Please refer to section 7.3.13 File Location for further details.

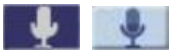
NOTE: For users with Windows 7 operating system, it is required to log on as an Administrator to implement the Web Recording function.

7.2.2 Motorized Model

Multiple Languages Support
Multiple languages are supported, including German, English, French, Italian, Russian, etc., for the viewer window interface.

Screen Size Adjustment
Image display size can be adjusted to x1/2 and full screen.

Digital Zoom Control
In the full screen mode, users can implement digital PTZ by rotating the mouse wheel (for zoom in/out), and drag the mouse into any direction.

Talk button (on/off) 
Talk function allows the local site to talk to the remote site. Click on the button to switch it to on/off. Please refer to section 7.3.2 Security: Add user >> Talk/Listen for further details. This function is only open to “User” who has been granted this privilege by the Administrator.

Speaker button (on/off)
Press the Speaker button to mute/activate the audio.

Snapshot button
Press the button, and the JPEG snapshots will automatically be saved in the appointed place. The default place of saving snapshots is: C:\. To change the storage location, please refer to section 7.3.13 File Location for further details.

Video Streaming Pause/Restart button (pause/restart)
Press the stop button to disable video streaming, the live video will be displayed as black. Press the restart button to show the live video again.

Web Recording button (on/off)
Press the <Recording> button and the recordings from the Live View will be saved directly to the specified location on the local hard drive, which could be configured in the “File Location” (snapshot) page . The default storage location for the web recording is: C:/. Please refer to section 7.3.13 File Location for further details.

Tele/Wide buttons

Hold the Tele/Wide button, and implement continuous zoom adjustment.

Near/Far buttons

Hold the Near/Far button, and implement continuous focus adjustment

Tele/Wide Steps buttons

Pressing the Tele/Wide Steps buttons will lead zoom to be shifted toward Tele/Wide sides in user-defined range, which can be selected from the drop-down menu.

Near/Far Steps buttons

Pressing the Near/Far buttons will lead focus to be altered toward Near/Far sides in user-defined range, which can be selected from the drop-down menu.

Push AF button

Please press the Push AF button once Zoom or Focus is adjusted.

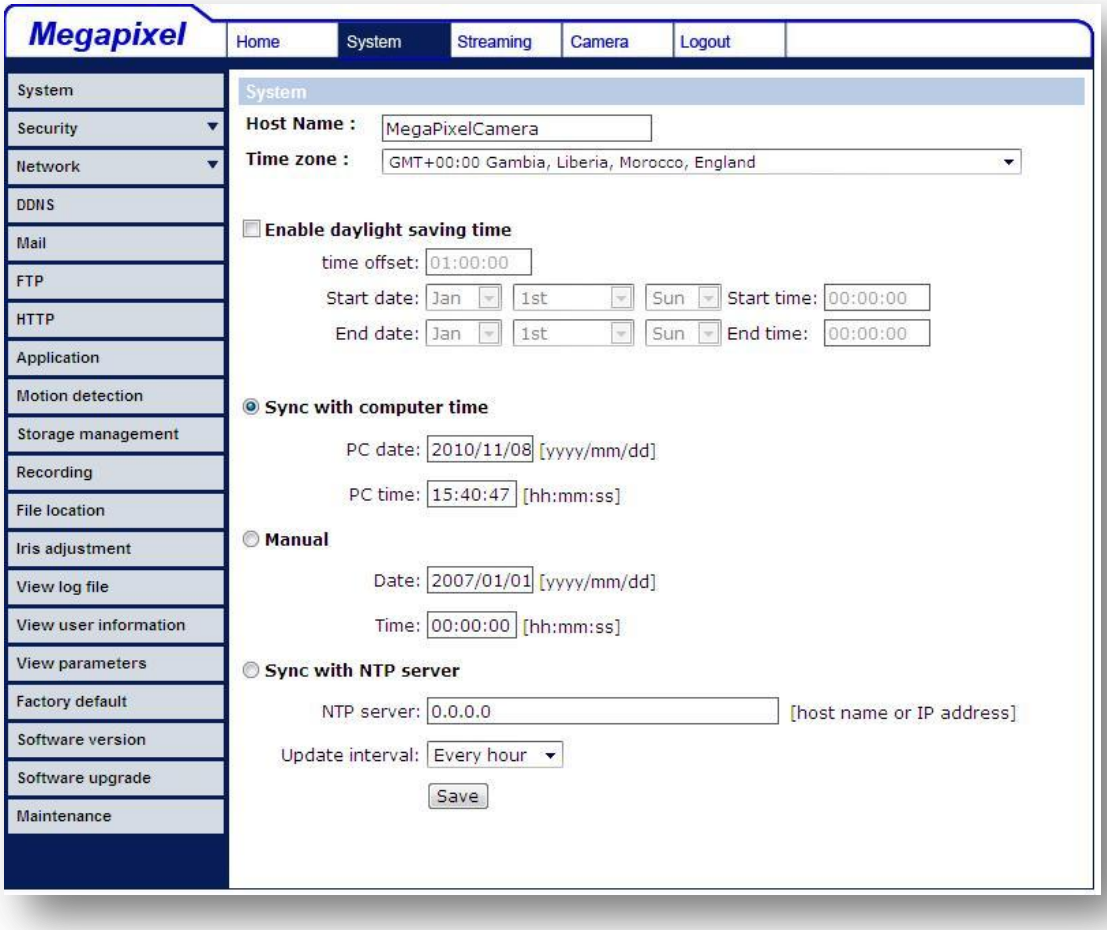
Reset button

Press the Reset button, and the camera lens will be calibrated at full wide end and infinity focus at once.

7.3 System Related Settings

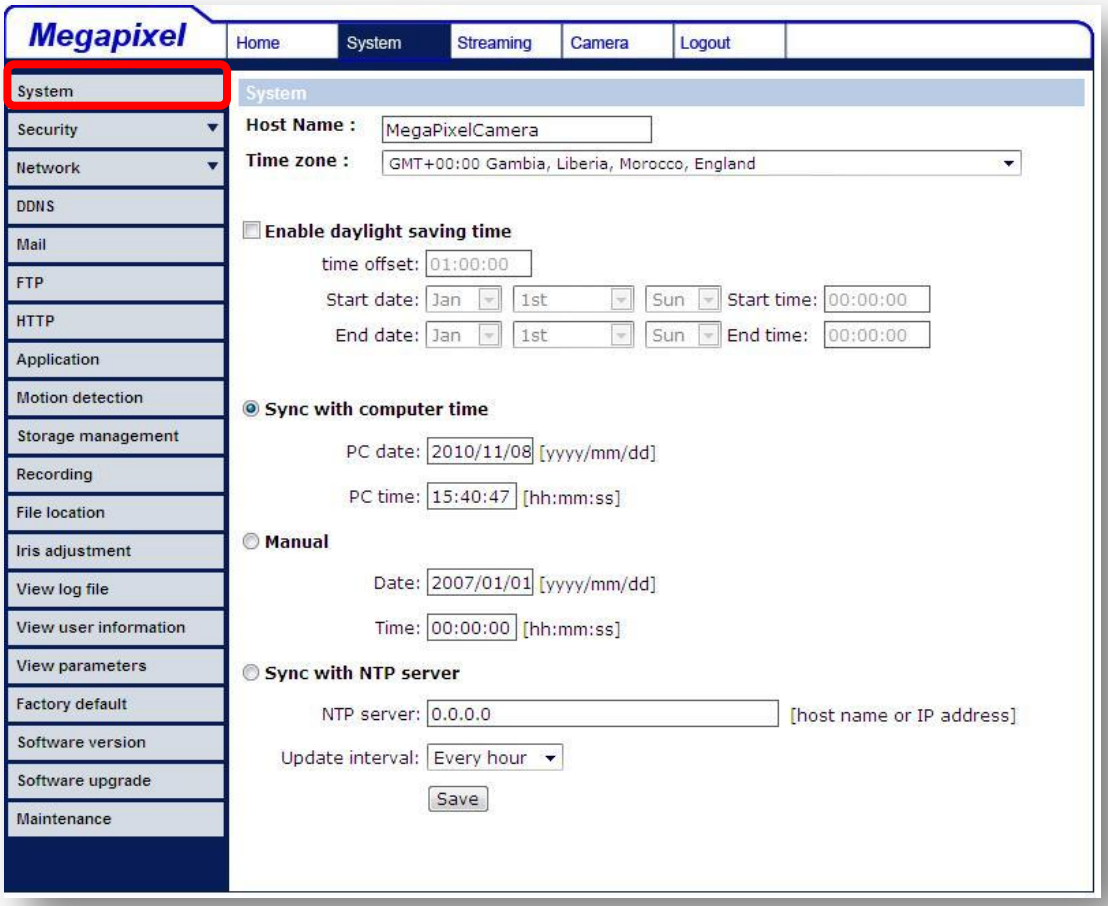
The figure below shows all categories under the "**System**" tab. Each category in the left column will be explained in the following sections.

NOTE: The "System" configuration page is only accessible by Administrator.



7.3.1 Host Name and System Time Setting

Press the first category: <System> in the left column; the page is shown as below.



Host Name

The name is for camera identification. If alarm function (see section 7.3.7 Application) is enabled and is set to send alarm message by Mail/FTP, the host name entered here will display in the alarm message. The maximum length of the Host Name is 30 characters.

Time Zone

Select the time zone you are in from the drop-down menu.

Enable Daylight Saving Time

To enable DST, please check the item and then specify time offset and DST duration. The format for time offset is [hh:mm:ss]; for instance, if the amount of time offset is one hour, please enter “01:00:00” into the field.

Sync With Computer Time

Select the item, and video date and time display will synchronize with the PC's.

Manual

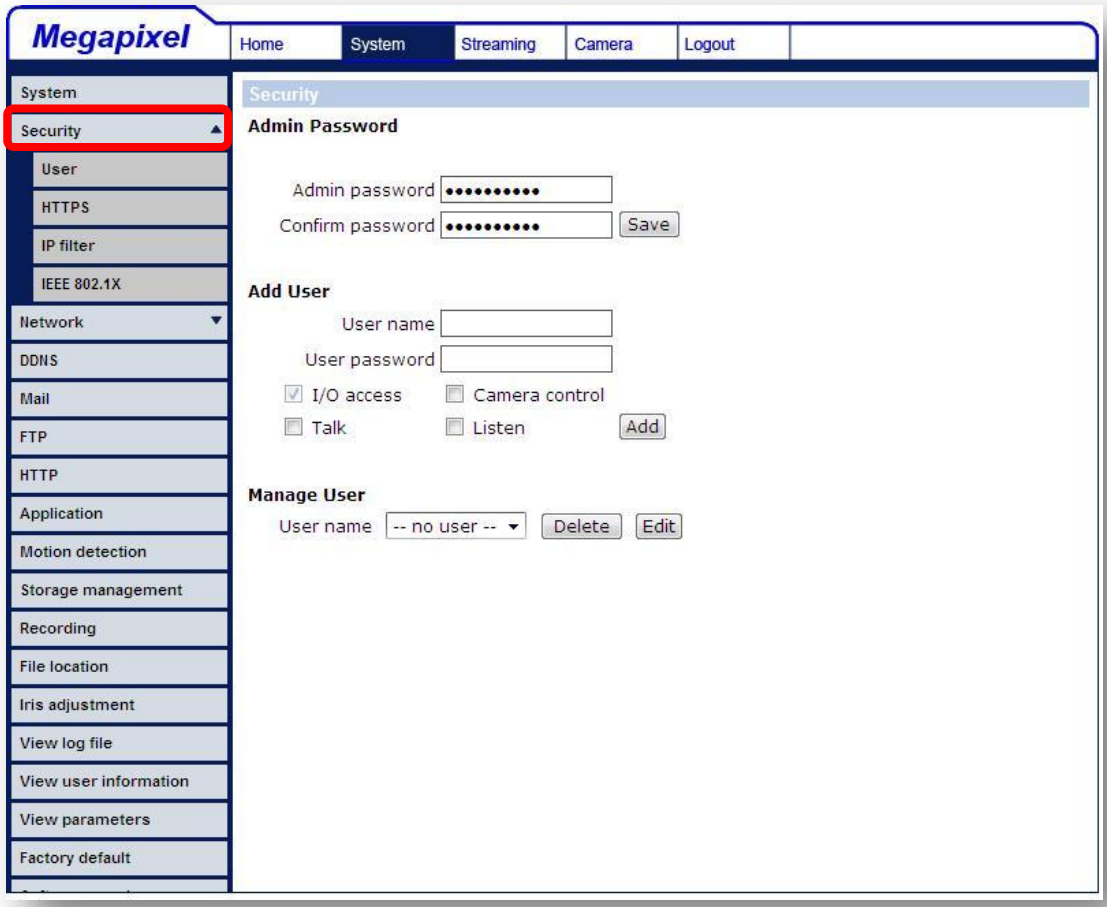
The Administrator can set video date, time and day manually. Entry format should be identical with that shown next to the enter field.

Sync with NTP Server

Network Time Protocol (NTP) is an alternate way to synchronize your camera's clock with a NTP server. Please specify the server you wish to synchronize in the enter field. Then select an update interval from the drop-down menu. For further information about NTP, please see the web site: www.ntp.org. (for example 192.53.103.108 or time.nist.gov)

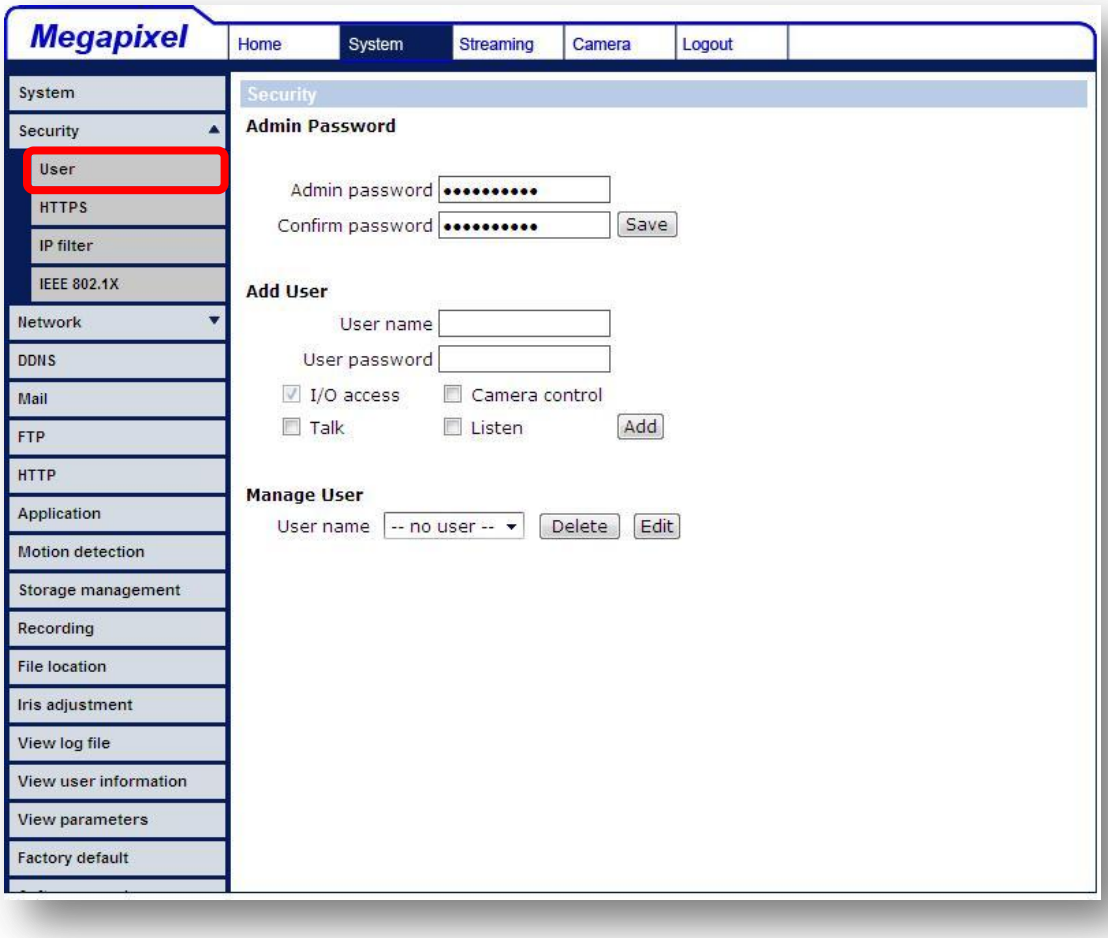
7.3.2 Security

Click the category: <Security>, there will be a drop-down menu with tabs including <User>, <HTTPS>, <IP Filter>, and <IEEE 802.1X>.



7.3.2.1User

Click the <User> tab under the category <Security> and the page is shown as the figure below.



Root password

Change the administrator's password by inputting the new password in both text boxes. The input characters/numbers will be displayed as dots for security purposes. After clicking <Save>, the web browser will ask the Administrator for the new password for access. The maximum length of the password is 14 characters.

NOTE: The following characters are valid: A-Z, a-z, 0-9, !#$%&'-.@^_~.

Add user

Type the new user's name and password and click <Add> to add the new user. User name and password can be up to 16 characters, and the maximum length of the password is 14 characters. The new user will be

displayed in the user name list. There is a maximum of twenty user accounts. Each user can be assigned the privileges of **"Camera control"**, **"Talk"** and **"Listen"**.

- **I/O access**
  This item supports fundamental functions that enable users to view video when accessing to the camera.

- **Camera control**
  This item allows the specified User to change camera parameters on the Camera Setting page.

- **Talk/Listen**
  Talk and Listen functions allow the appointed user in the local site (PC site) communicating with, for instance, the administrator in the remote site.

Manage User

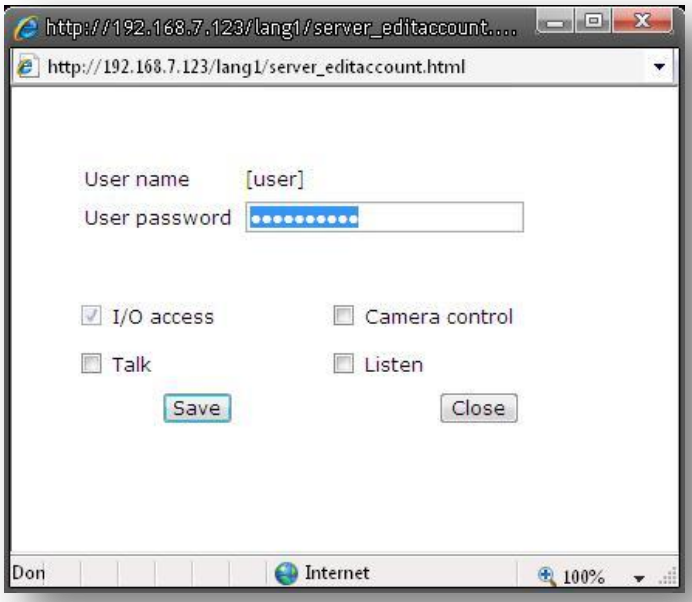
Delete user

To delete a user, pull down the user list, and select the user name you wish to delete. Then click <Delete> to remove it.

Edit user

Pull down the user list and select a user name. Click <Edit> to edit the user's password and privilege.

NOTE: It is required to enter the User password as well as select the function open to the user. When finished, click <Save> to modify the account authority.

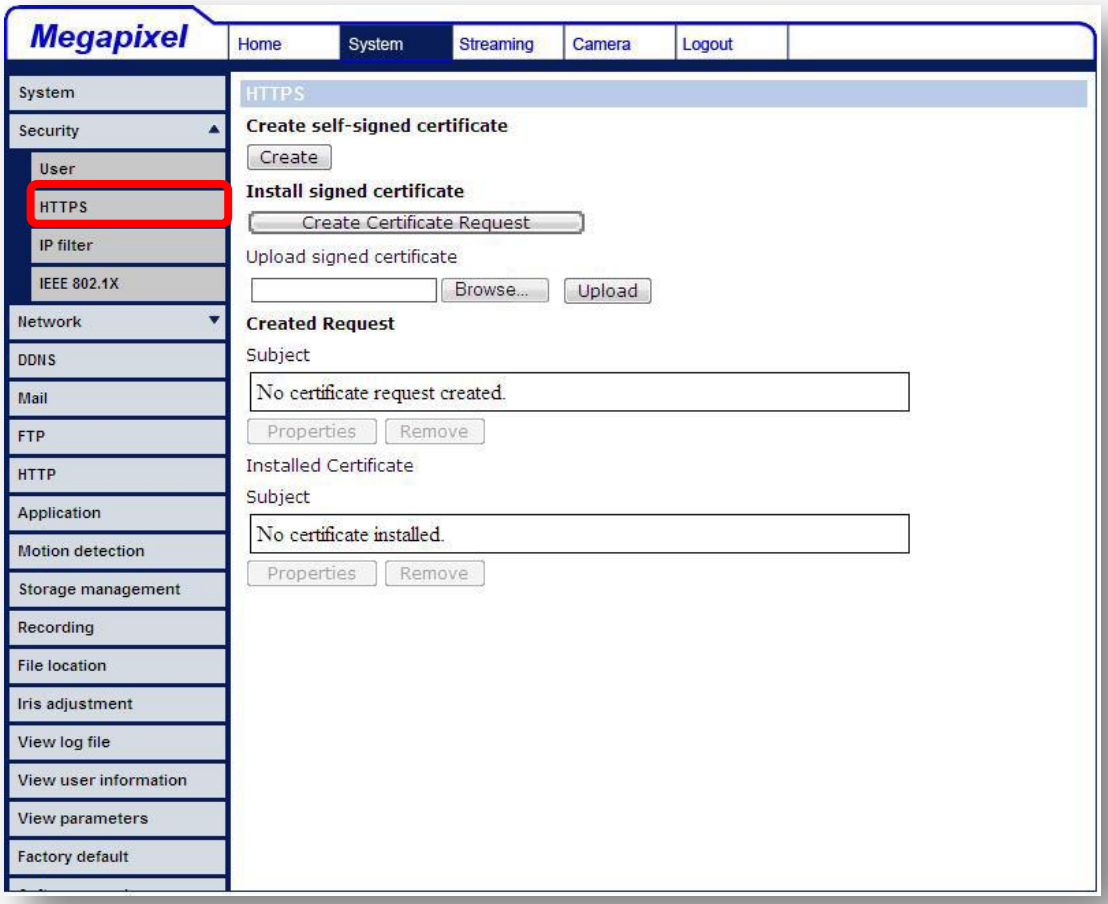

http://192.168.7.123/lang1/server_editaccount....
http://192.168.7.123/lang1/server_editaccount.html
User name [user]
User password
I/O access
Camera control
Talk
Listen
Save
Close
Don
Internet
100%

http://192.168.7.123/lang1/server_editaccount....
http://192.168.7.123/lang1/server_editaccount.html
User name [user]
User password
I/O access
Camera control
Talk
Listen
Save
Close
Don
Internet
100%

7.3.2.2HTTPS

<HTTPS> allows secure connections between the IP Camera and web browser using <Secure Socket Layer (SSL)> or <Transport Layer Security (TLS)>, which ensure camera settings or Username/ Password info from snooping. It is required to install a self-signed certificate or a CA-signed certificate for implementing <HTTPS>.

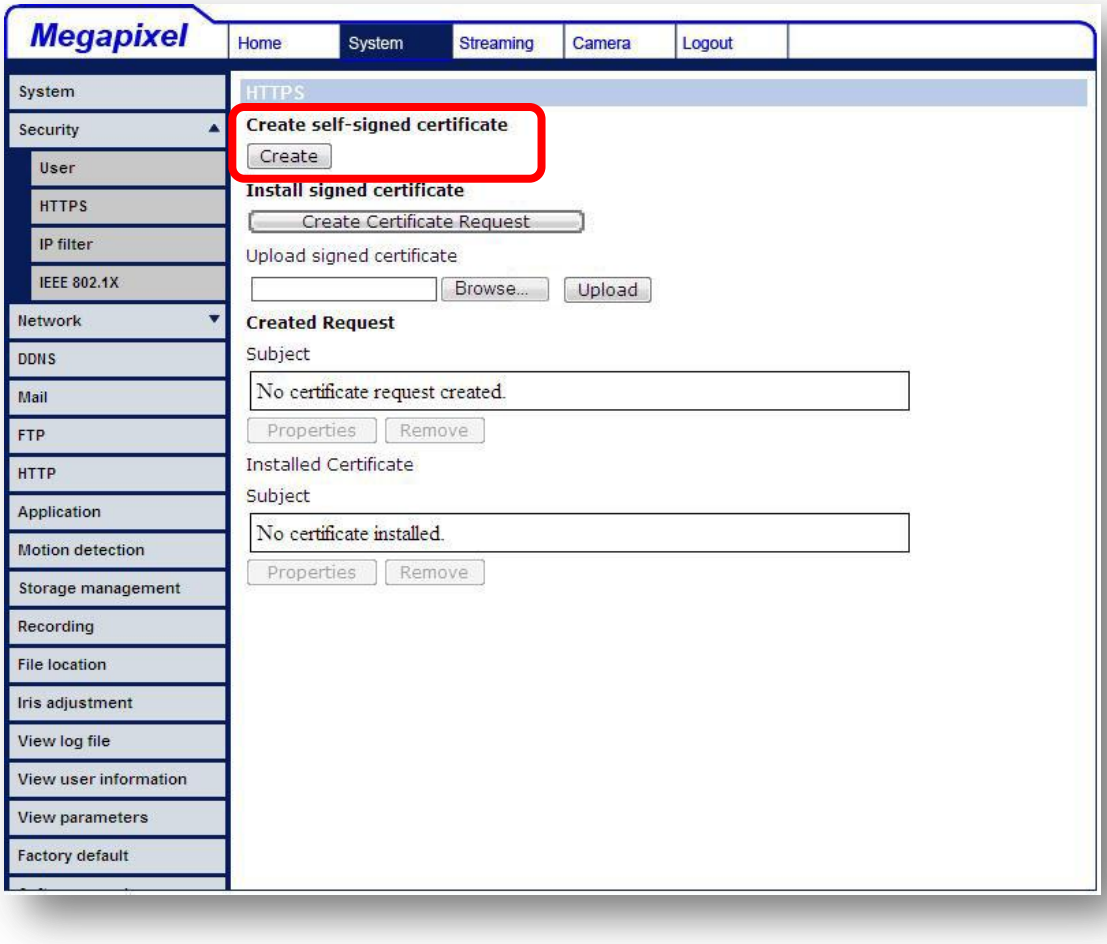
Click the <HTTPS> tab, and the HTTPS setting page is shown as the figure below.



To use HTTPS on the IP Camera, a HTTPS certificate must be installed. The HTTPS certificate can be obtained by either creating and sending a certificate request to a Certificate Authority (CA) or creating a self-signed HTTPS certificate, as described below.

Create Self-signed Certificate

Before a CA-issued certificate is obtained, users can create and install a self-signed certificate first.

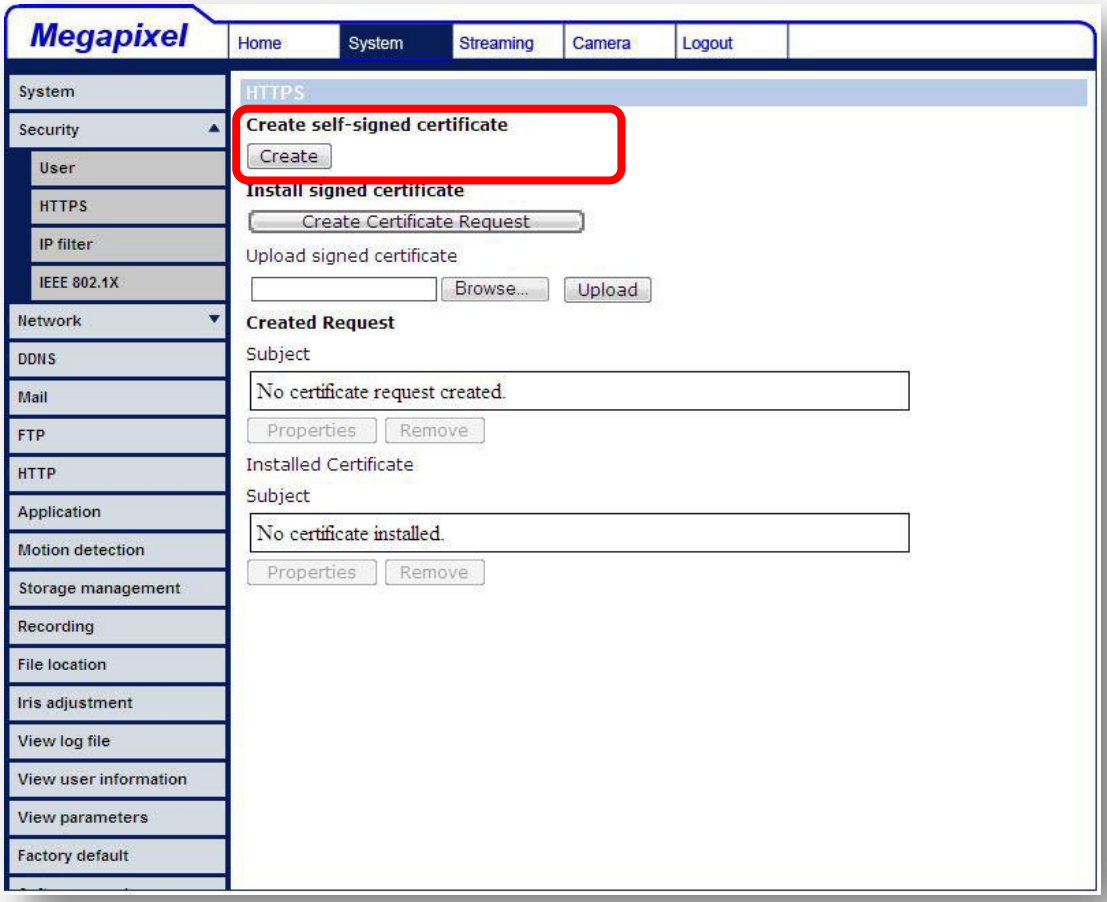


Click <Create> button under “Create self-signed certificate” and provide the requested information to install a self-signed certificate for the IP Camera. Please refer to the last part of this section: Provide the Certificate Information for more details.

NOTE: The self-signed certificate does not provide the same high level of security as when using a CA-issued certificate.

Create Certificate Request

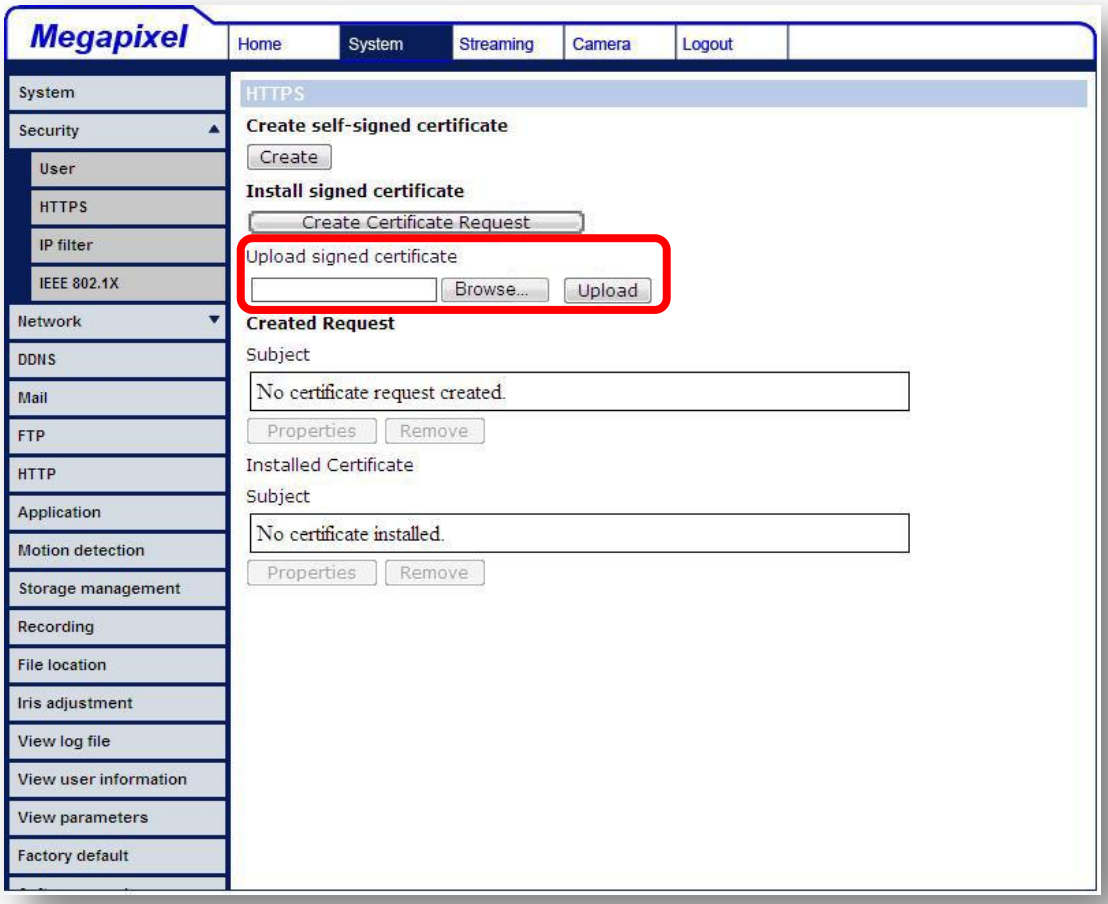
Click the “Create Certificate Request” button to create and submit a certificate request in order to obtain a signed certificate from CA.



Provide the request information in the create dialog. Please refer to the following Provide the Certificate Information for more details.

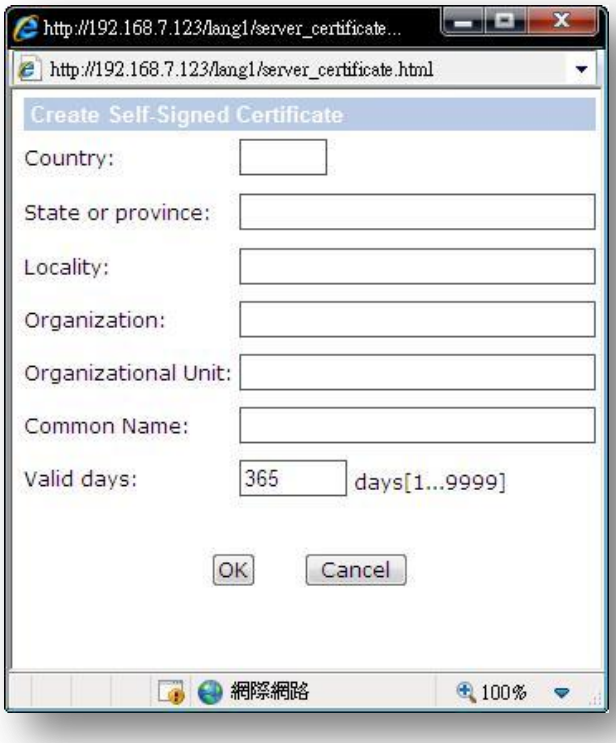
When the request is complete, the subject of the Created Request will be shown in the field. Click “Properties” below the Subject field, copy the PEM-formatted request and send it to your selected CA.

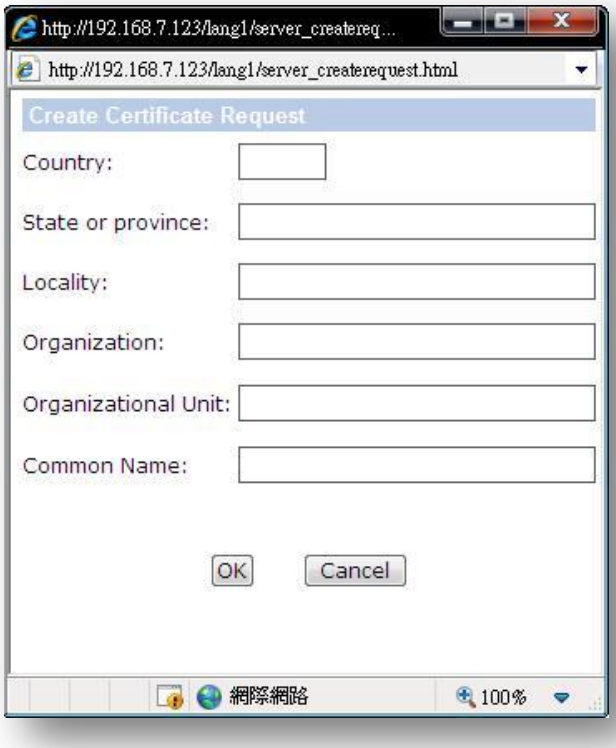
When the signed certificate is returned, install it by uploading the signed certificate.



Provide the Certificate Information

To create a Self-signed HTTPS Certificate or a Certificate Request to CA, please enter the information as requested:


http://192.168.7.123/lang1/server_certificate...
http://192.168.7.123/lang1/server_certificate.html
Create Self-Signed Certificate
Country:
State or province:
Locality:
Organization:
Organization Unit:
Common Name:
Valid days:
365
days[1...9999]
OK
Cancel
網際網路
100%


http://192.168.7.123/lang1/server_createreq...
http://192.168.7.123/lang1/server_createrequest.html
Create Certificate Request
Country:
State or province:
Locality:
Organization:
Organization Unit:
Common Name:
OK
Cancel
網際網路
100%

- **Country**
  Enter a 2-letter combination code to indicate the country the certificate will be used in. For instance, type in “US” to indicate United States.

- **State or province**
  Enter the local administrative region.

- **Locality**
  Enter other geographical information.

- **Organization**
  Enter the name of the organization to which the entity identified in “Common Name” belongs.

- **Organization Unit**
  Enter the name of the organizational unit to which the entity identified in “Common Name” belongs.

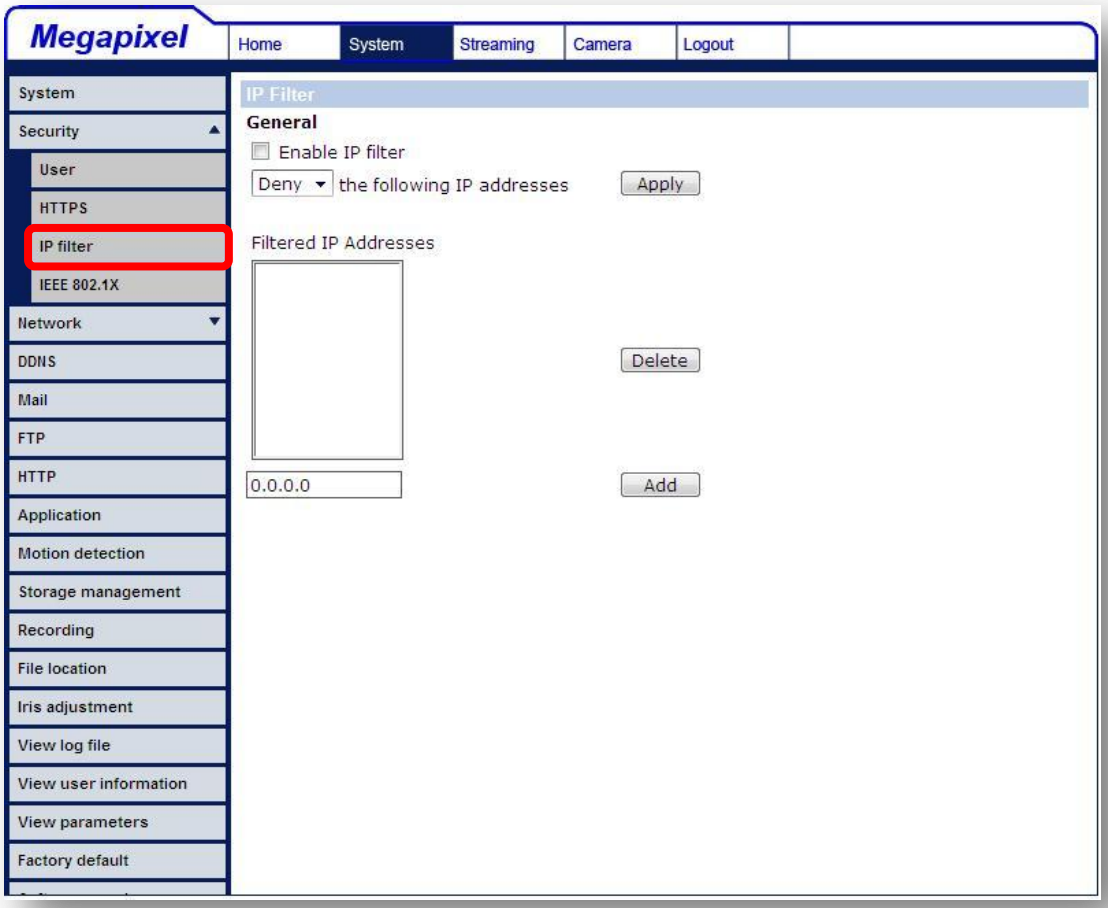
- **Common Name**
  Indicate the name of the person or other entity that the certificate identifies (often used to identify the website).

- **Valid days (Self-signed Certificate Only)**
  Enter the period in days (1~9999) to indicate the valid period of certificate.

  Click “OK” to save the Certificate Information after complete.

7.3.2.3IP Filter

Using the IP filter, access to the IP Camera can be restricted by denying/allowing specific IP addresses.



General

- **Enable IP Filter**
  Check the box to enable the IP Filter function. Once enabled, the listed IP addresses (IPv4) will be allowed/ denied access to the IP Camera.

  Select “Allow” or “Deny” from the drop-down list and click the <Apply> button to determine the IP Filter behavior.

- **Add/ Delete IP Address**
  Input the IP address and click the <Add> button to add a new filtered address.

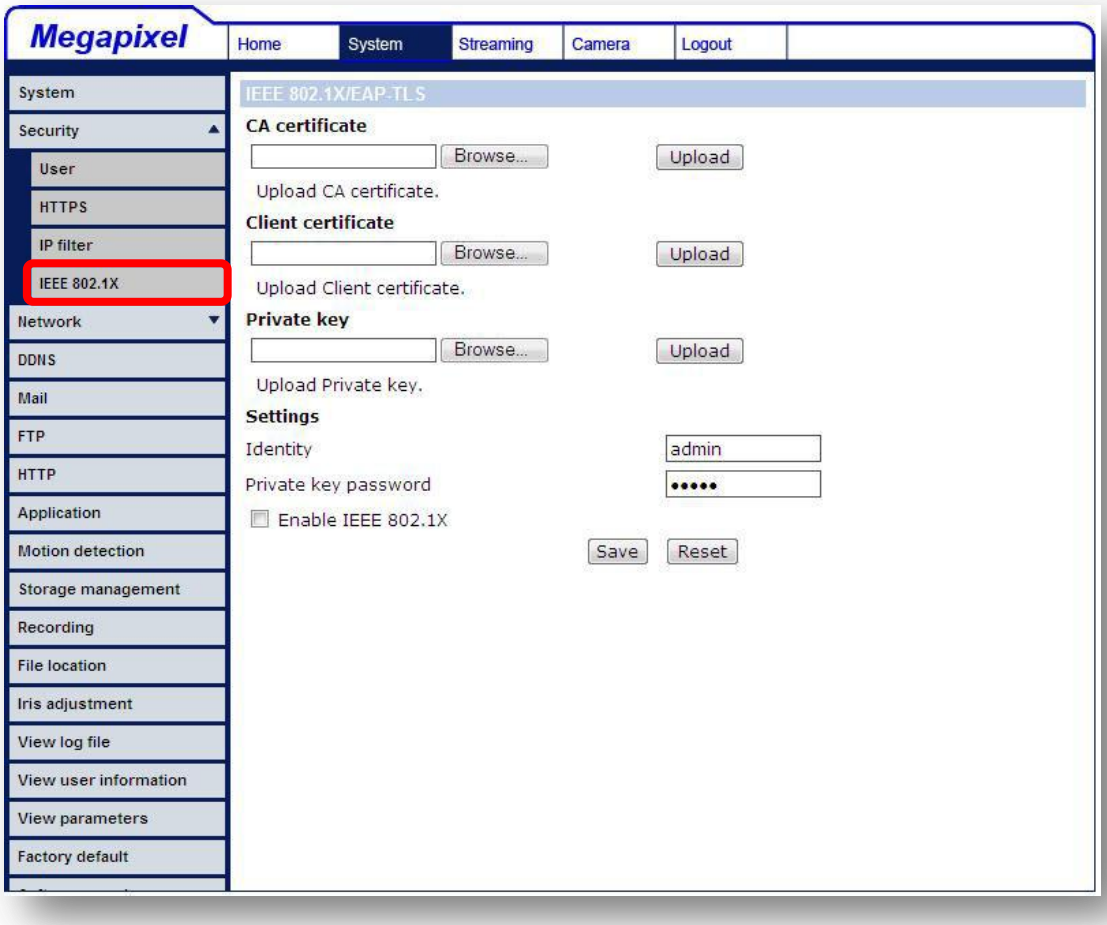
  The Filtered IP Addresses list box shows the currently configured IP addresses. Up to 256 IP address entries may be specified.

  To remove an IP address from the list, please select the IP and then click the <Delete> button.

7.3.2.4IEEE 802.1X

The IP Camera is allowed to access a network protected by 802.1X/EAPOL (Extensible Authentication Protocol over LAN).

Users need to contact with the network administrator for gaining certificates, user IDs and passwords



CA Certificate
The CA certificate is created by the Certification Authority for the purpose of validating itself. Upload the certificate for checking the server's identity.

Client Certificate/ Private Key
Upload the Client Certificate and Private Key for authenticating the IP Camera itself.

Settings

- **Identity**
  Enter the user identity associated with the certificate. Up to 16 characters can be used.

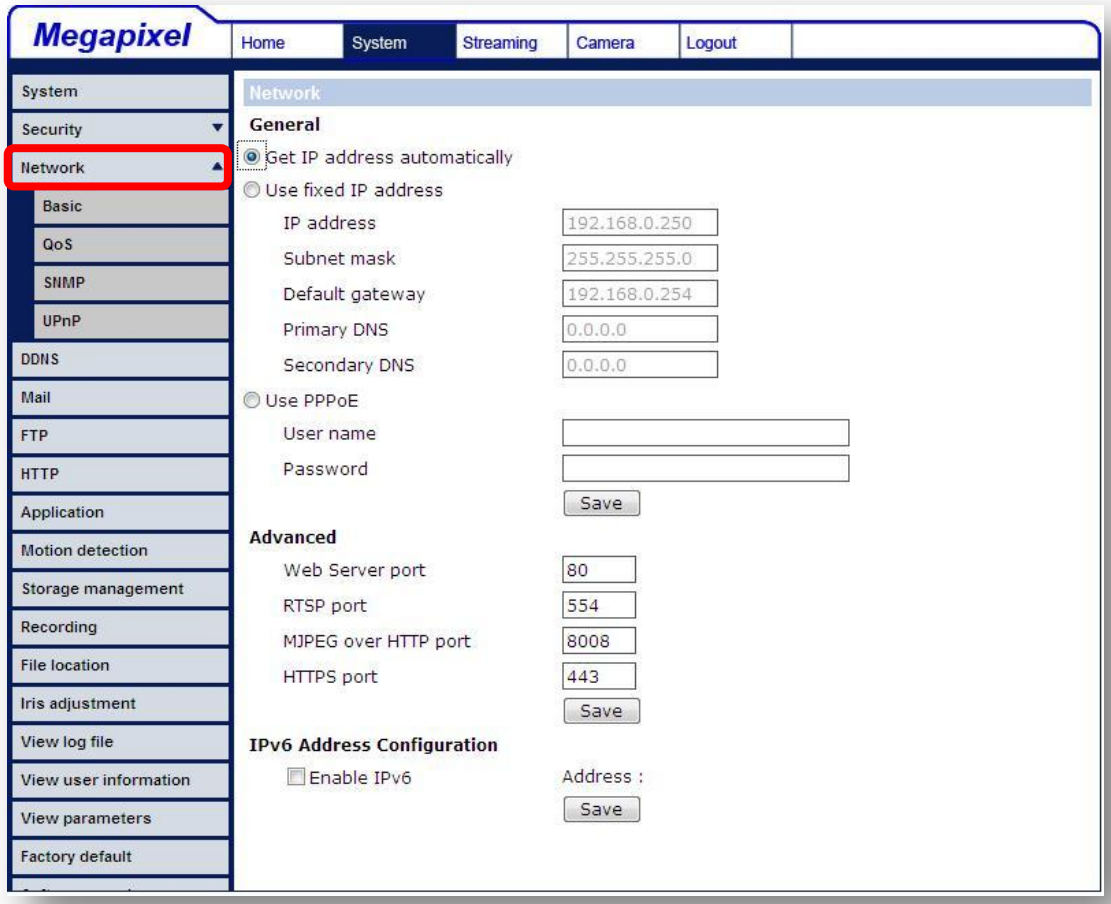
- **Private Key Password**
  Enter the password (maximum 16 characters) for your user identity.

Enable IEEE 802.1X
Check the box to enable IEEE 802.1X.

Click "Save" to save the IEEE 802.1X/ EAP- TLS setting.

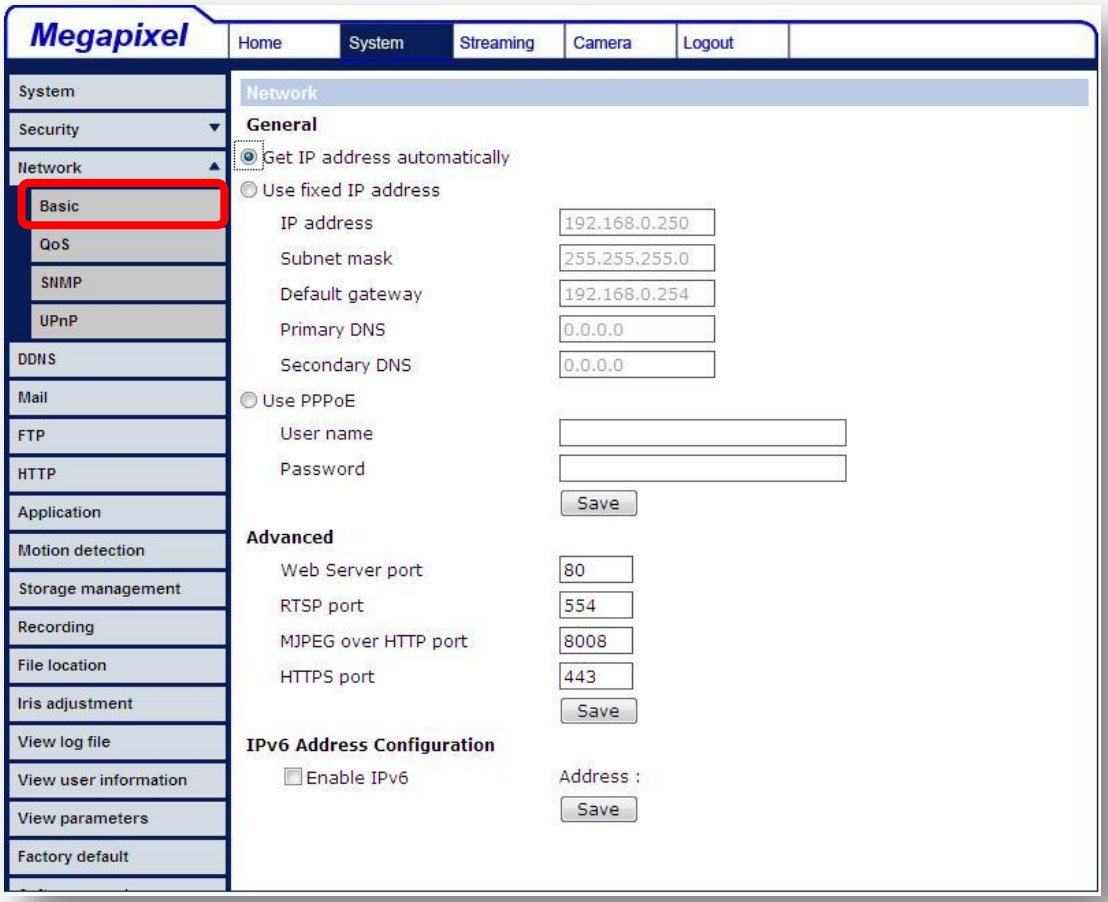
7.3.3 Network

Click the category: < Network>, there will be a drop-down menu with tabs including <Basic>, <QoS>, <SNMP>, and <UPnP>.



7.3.3.1 Basic

Users can choose to connect to the IP Camera with fixed or dynamic (DHCP) IP address. The IP Camera also provides PPPoE (Point-to-Point Protocol over Ethernet) support for users who connect to the network via PPPoE.



Get IP address automatically (DHCP)

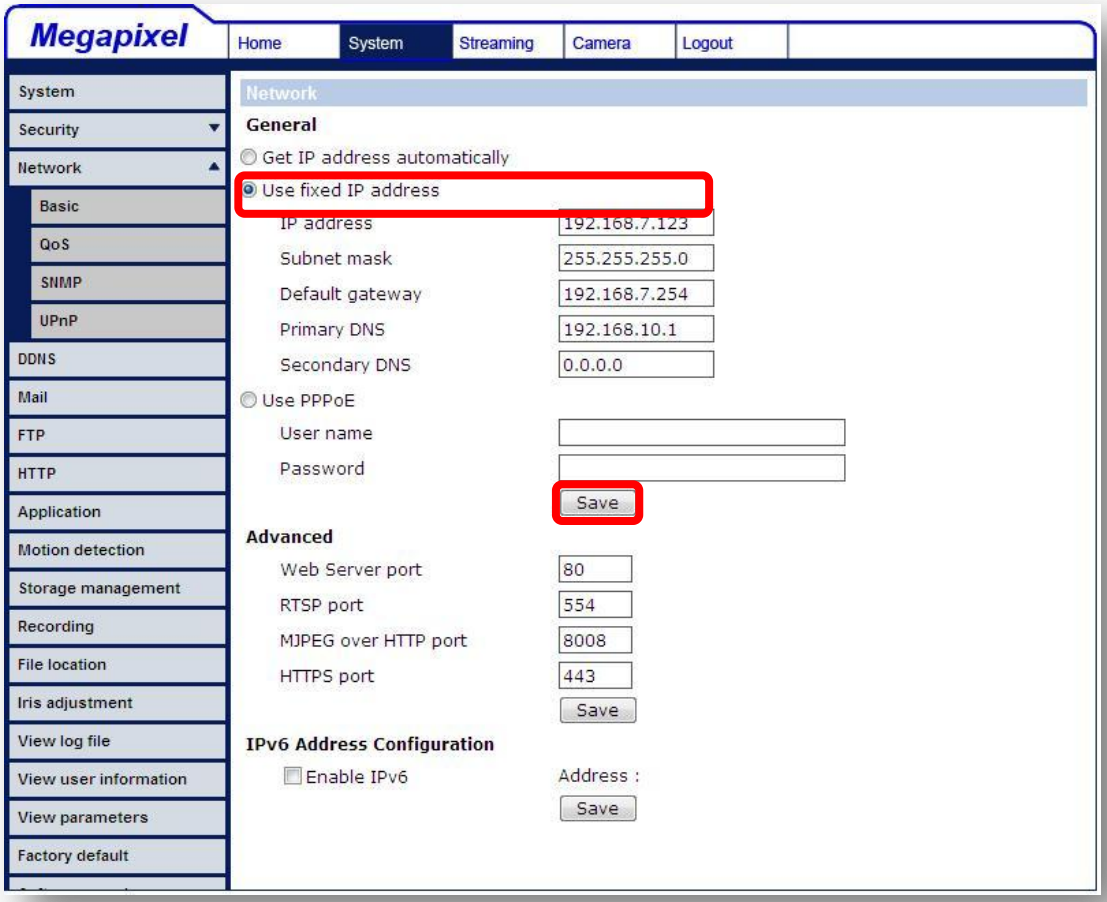
The camera's default setting is "**Use fixed IP address**". Please refer to the previous section 6. Accessing Camera for login with the default IP address.

If select "**Get IP address automatically**", after the IP Camera restarts, users can search it through the installer program: DeviceSearch.exe, which can be found in "DeviceSearch" folder in the supplied CD.

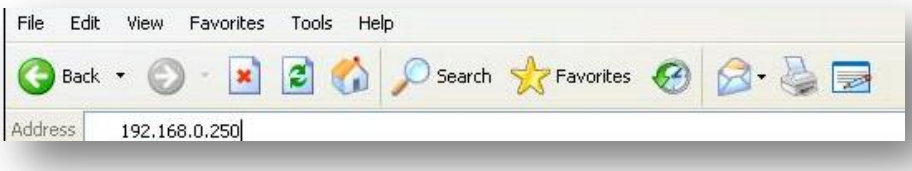
NOTE: Please make the record of the IP Camera's MAC address, which can be found in the label of the camera, for identification in the future.

Use fixed IP address

To setup static IP address, select "**Use fixed IP address**" and move the cursor to the IP address blank (as indicated below) and insert the new IP address, ex. 192.168.7.123; then go to the Default gateway (explained latter) blank and change the setting, ex. 192.168.7.254. Press "Save" to confirm the new setting.



When using static IP address to login to the IP Camera, users can access it either through "DeviceSearch" software (see 6. Accessing Camera) or input the IP address in the URL bar and press "Enter".



- **IP address**
  This is necessary for network identification.

- **Subnet mask**
  It is used to determine if the destination is in the same subnet. The default value is “255.255.255.0”.
- **Default gateway**
  This is the gateway used to forward frames to destinations in different subnet. Invalid gateway setting will fail the transmission to destinations in different subnet.

- **Primary DNS**
  Primary DNS is the primary domain name server that translates hostnames into IP addresses.

- **Secondary DNS**
  Secondary DNS is a secondary domain name server that backups the primary DNS.

Use PPPoE

For the PPPoE users, enter the PPPoE Username and Password into the fields, and click on the “Save” button to complete the setting.

Advanced

- **Web Server port**
  The default web server port is 80. Once the port is changed, the user must be notified the change for the connection to be successful. For instance, when the Administrator changes the HTTP port of the IP Camera whose IP address is 192.168.0.100 from 80 to 8080, the user must type in the web browser “http://192.168.0.100:8080” instead of http://192.168.0.100

- **RTSP port**
  The default setting of RTSP Port is 554; the setting range is from 1024 to 65535.

- **MJPEG over HTTP port**
  The default setting of MJPEG over HTTP Port is 8008; the setting range is from 1024 to 65535.

- **HTTPS port**
  The default setting of HTTPS Port is 443; the setting range is from 1024 to 65535.

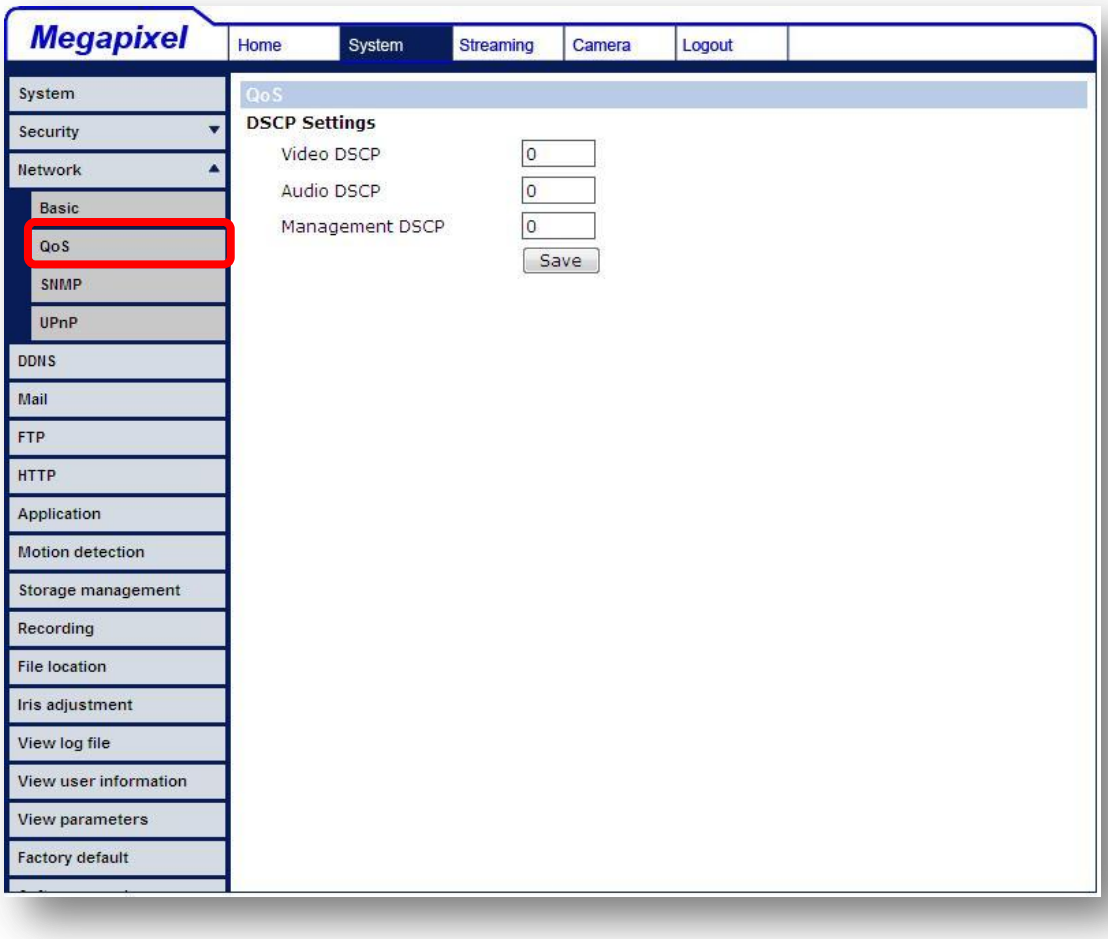
NOTE: Be aware to assign a different port number for each separate service mentioned above.

IPv6 Address Configuration

With IPv6 support, users can use the corresponding IPv6 address for browsing. Enable IPv6 by checking the box and click “Save” to complete the setting.

7.3.3.2 QoS (Quality of Service)

QoS allows providing differentiated service levels for different types of traffic packets, which guarantees delivery of priority services especially when network congestion occurs. Adapting the Differentiated Services (DiffServ) model, traffic flows are classified and marked with DSCP (DiffServ Codepoint) values, and thus receive the corresponding forwarding treatment from DiffServ capable routers.



DSCP Settings

The DSCP value range is from 0 to 63. The default DSCP value is 0, which means DSCP disabled.
The IP Camera uses the following QoS Classes: Video, Audio and Management.

- **Video**
  The class consists of applications such as MJPEG over HTTP, RTP/RTSP and RTSP/HTTP.

- **Audio**
  This setting is only available for the IP Cameras that support audio.

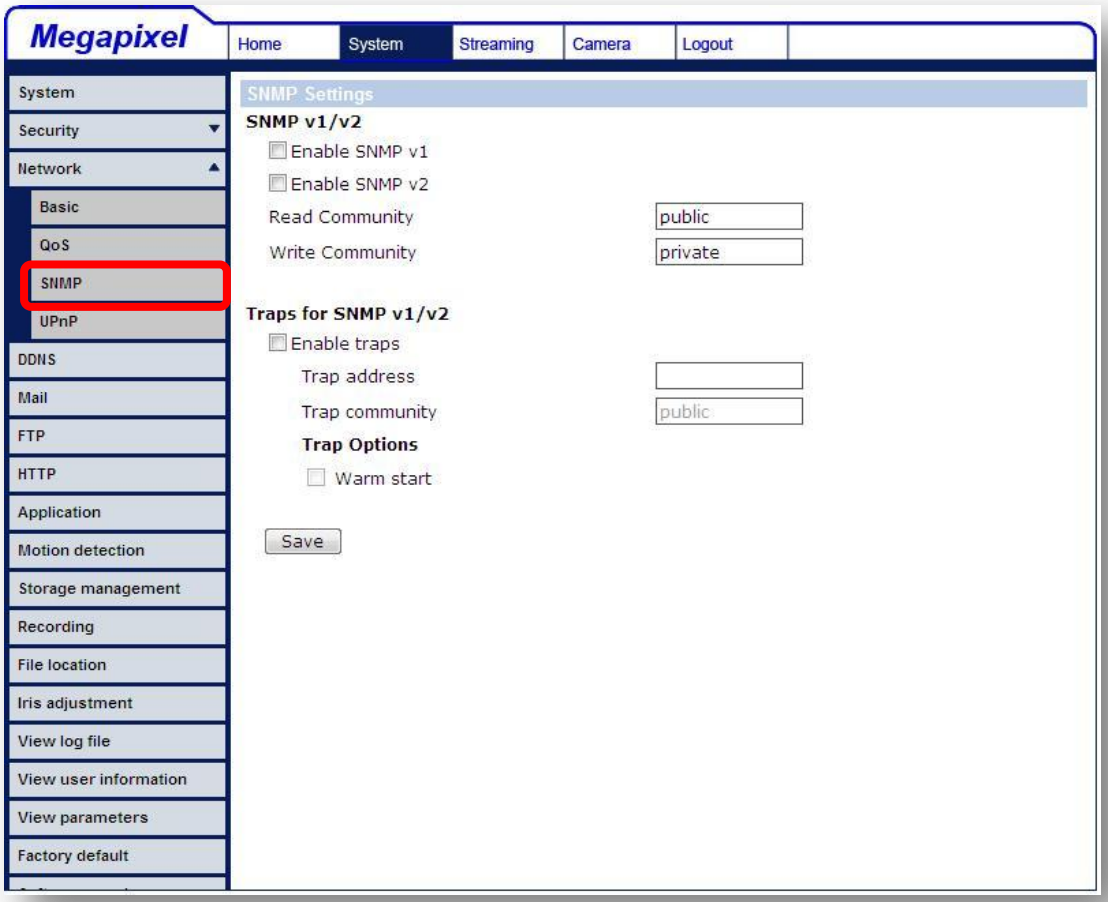
- **Management**
  The class consists of HTTP traffic: Web browsing.

  Click the “Save” button when complete.

NOTE: To enable this function, please make sure the switches/routers
in the network support QoS.

7.3.3.3 SNMP (Simple Network Management Protocol)

With Simple Network Management Protocol (SNMP) support, the IP Camera can be monitored and managed remotely by the network management system.


Megapixel
Home
System
Streaming
Camera
Logout
System
Security
Network
Basic
QoS
SNMP
UPnP
DDNS
Mail
FTP
HTTP
Application
Motion detection
Storage management
Recording
File location
Iris adjustment
View log file
View user information
View parameters
Factory default
SNMP Settings
SNMP v1/v2
Enable SNMP v1
Enable SNMP v2
Read Community
public
Write Community
private
Traps for SNMP v1/v2
Enable traps
Trap address
Trap community
public
Trap Options
Warm start
Save

SNMP v1/ v2

- **Enable SNMP**
  Select the version of SNMP to use by checking the box.

- **Read Community**
  Specify the community name that has read-only access to all supported SNMP objects. The default value is “public”.

- **Write Community**
  Specify the community name that has read/write access to all supported SNMP objects (except read-only objects). The default value is “write”.

Traps for SNMP v1/ v2

Traps are used by the IP Camera to send massages to a management system for important events or status changes.

- **Enable Traps**
  Check the box to activate trap reporting.

- **Trap address**
  Enter the IP address of the management server.

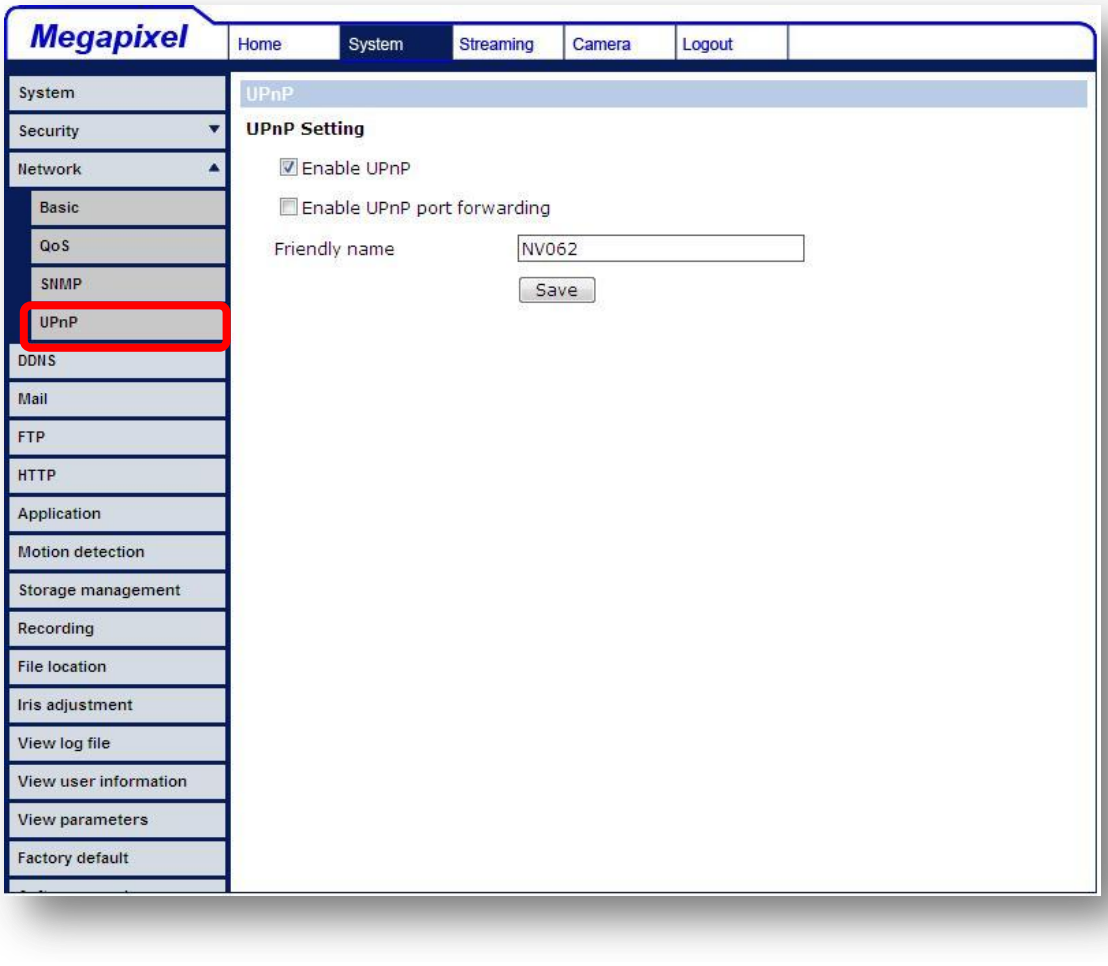
- **Trap community**
  Enter the community to use when sending a trap message to the management system.

Trap Option

- **Warm Start**
  A Warm Start SNMP trap signifies that the SNMP device, i.e. IP Camera, performs software reload.

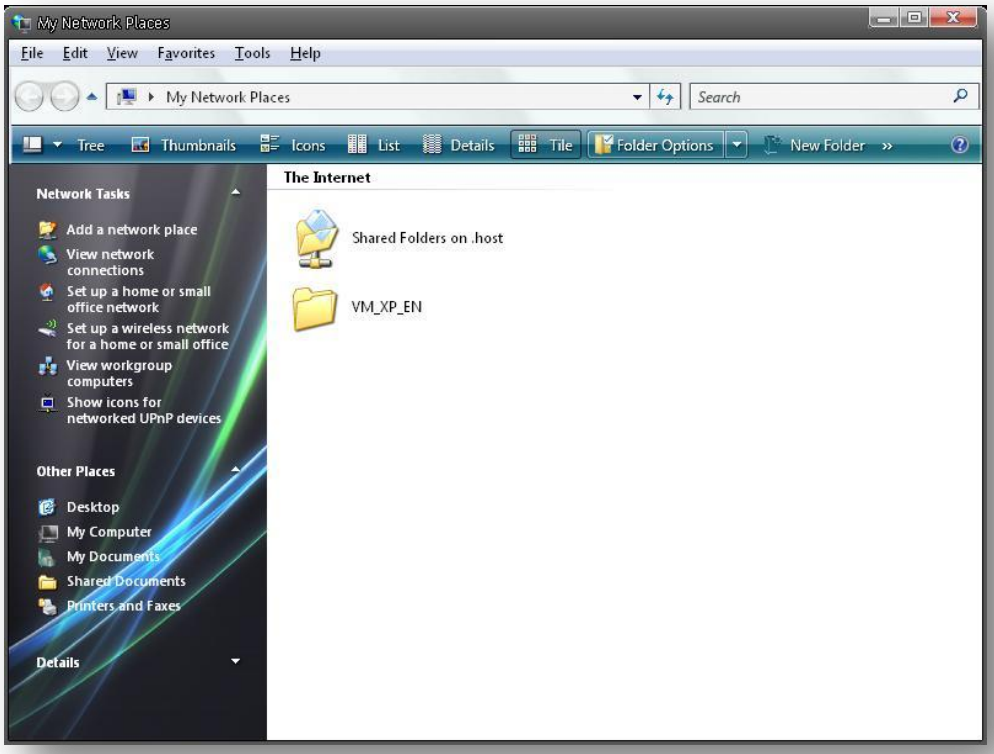
Click the “Save” button when complete.

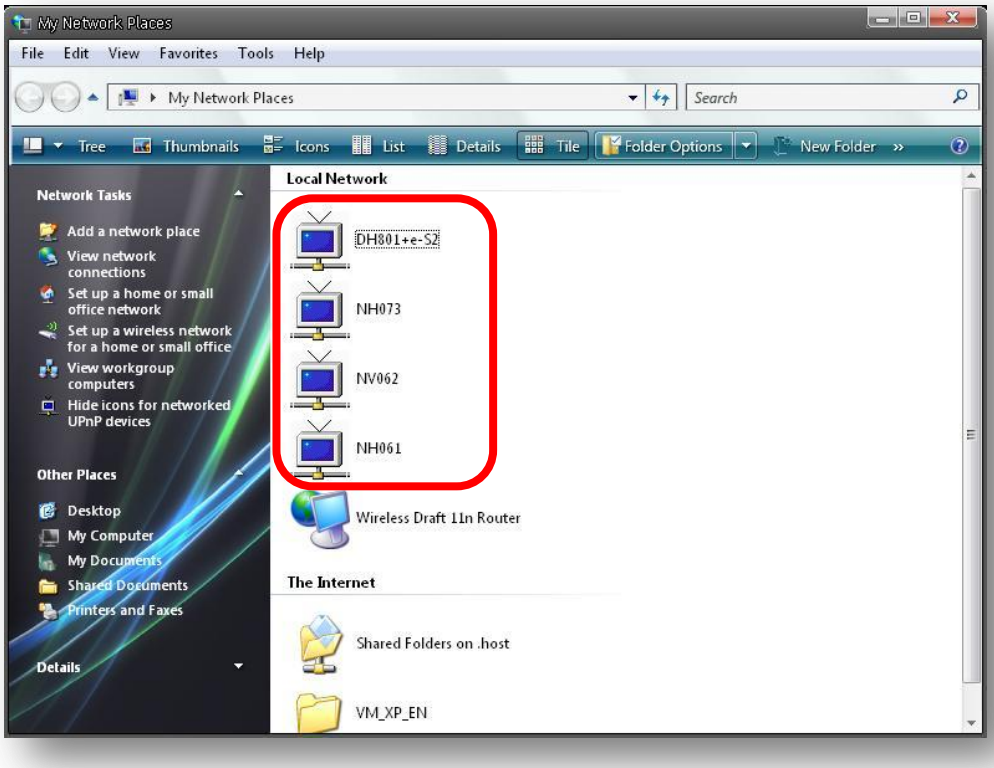
7.3.3.4UPnP



UPnP Setting

- **Enable UPnP**
  When the UPnP is enable, whenever the IP Camera is presented to the LAN, the icon of the connected IP Cameras will appear in My Network Places to allow for direct access as shown below.


My Network Places
File Edit View Favorites Tools Help
My Network Places
Search
Tree Thumbnails Icons List Details Tile Folder Options New Folder
Network Tasks
Add a network place
View network connections
Set up a home or small office network
Set up a wireless network for a home or small office
View workgroup computers
Show icons for networked UPnP devices
Other Places
Desktop
My Computer
My Documents
Shared Documents
Printers and Faxes
Details
The Internet
Shared Folders on .host
VM_XP_EN


My Network Places
File Edit View Favorites Tools Help
My Network Places
Search
Tree Thumbnails Icons List Details Tile Folder Options New Folder
Network Tasks
Add a network place
View network connections
Set up a home or small office network
Set up a wireless network for a home or small office
View workgroup computers
Hide icons for networked UPnP devices
Other Places
Desktop
My Computer
My Documents
Shared Documents
Printers and Faxes
Details
Local Network
DH801+e-S2
NH073
NV062
NH061
Wireless Draft 11n Router
The Internet
Shared Folders on .host
VM_XP_EN

NOTE: To enable this function, please make sure the UPnP component is installed on your computer. Please refer to Appendix D: Install UPnP components for UPnP component installation procedure.

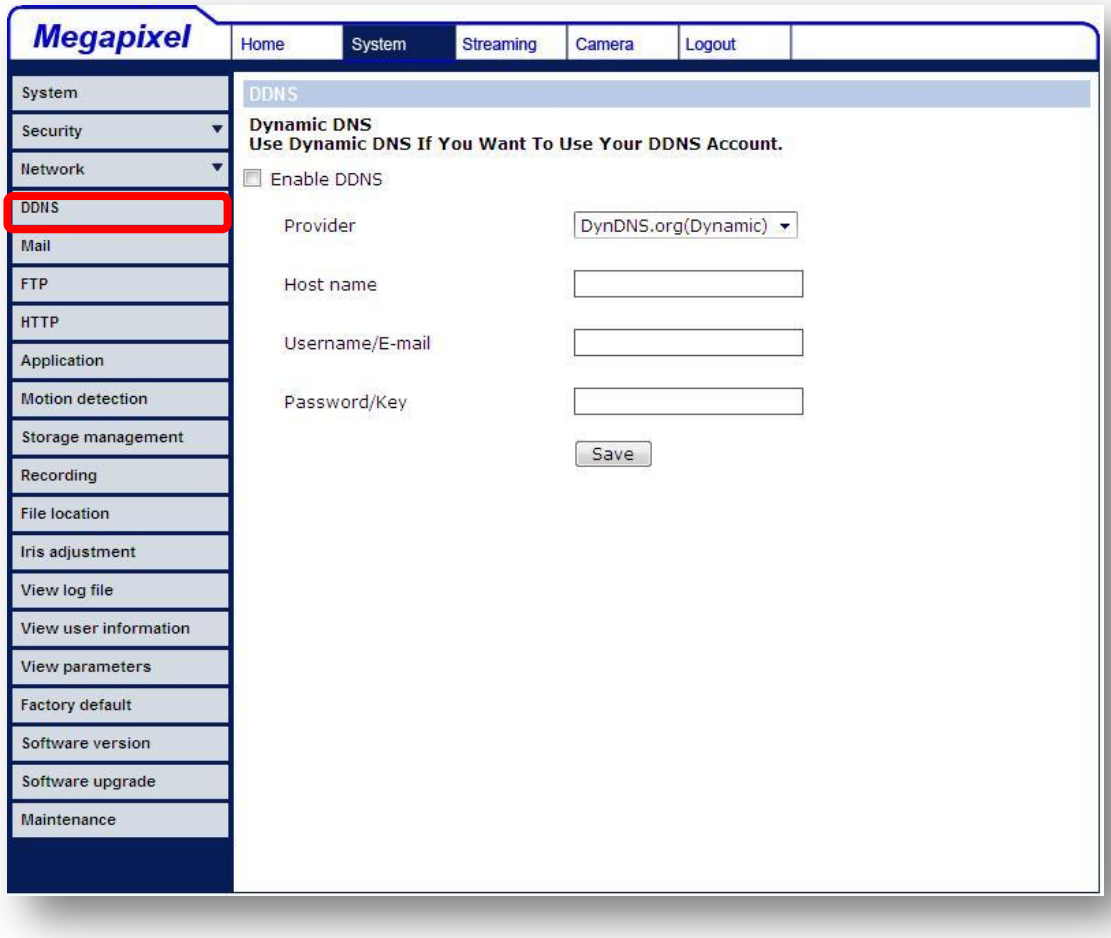
- **Enable UPnP port forwarding**
  When the UPnP port forwarding is enabled, the IP Camera is allowed to open the web server port on the router automatically.

  NOTE: To enable this function, please make sure that your router supports UPnP and it is activated

- **Friendly name**
  Set the name for the IP Camera for identity.

7.3.4 DDNS

Dynamic Domain Name System (DDNS) allows a host name to be constantly synchronized with a dynamic IP address. In other words, it allows those using a dynamic IP address to be associated to a static domain name so others can connect to it by name.



Enable DDNS
Check the item to enable DDNS.

Provider
Select one DDNS host from the provider list.

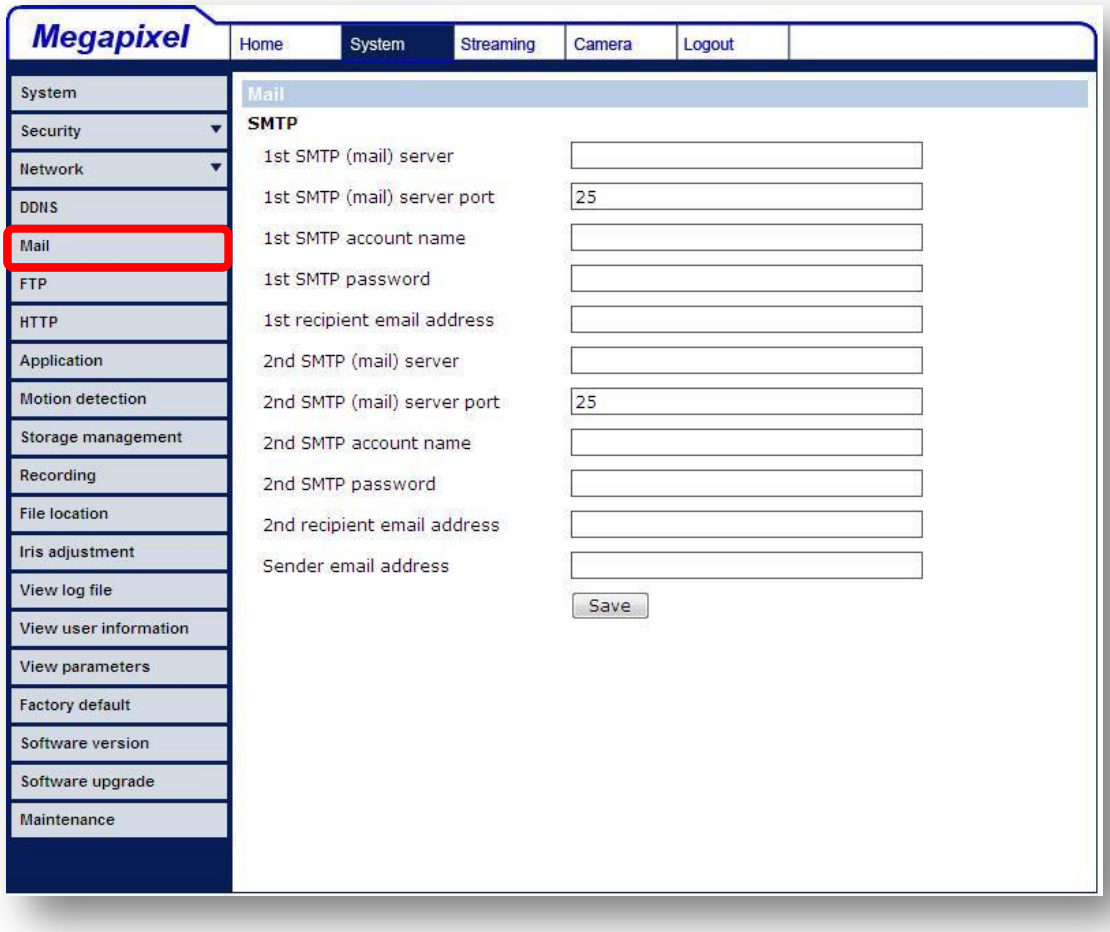
Host name
Enter the registered domain name in the field.

Username/E-mail
Enter the username or e-mail required by the DDNS provider for authentication.

Password/Key
Enter the password or key required by the DDNS provider for authentication.

7.3.5 Mail

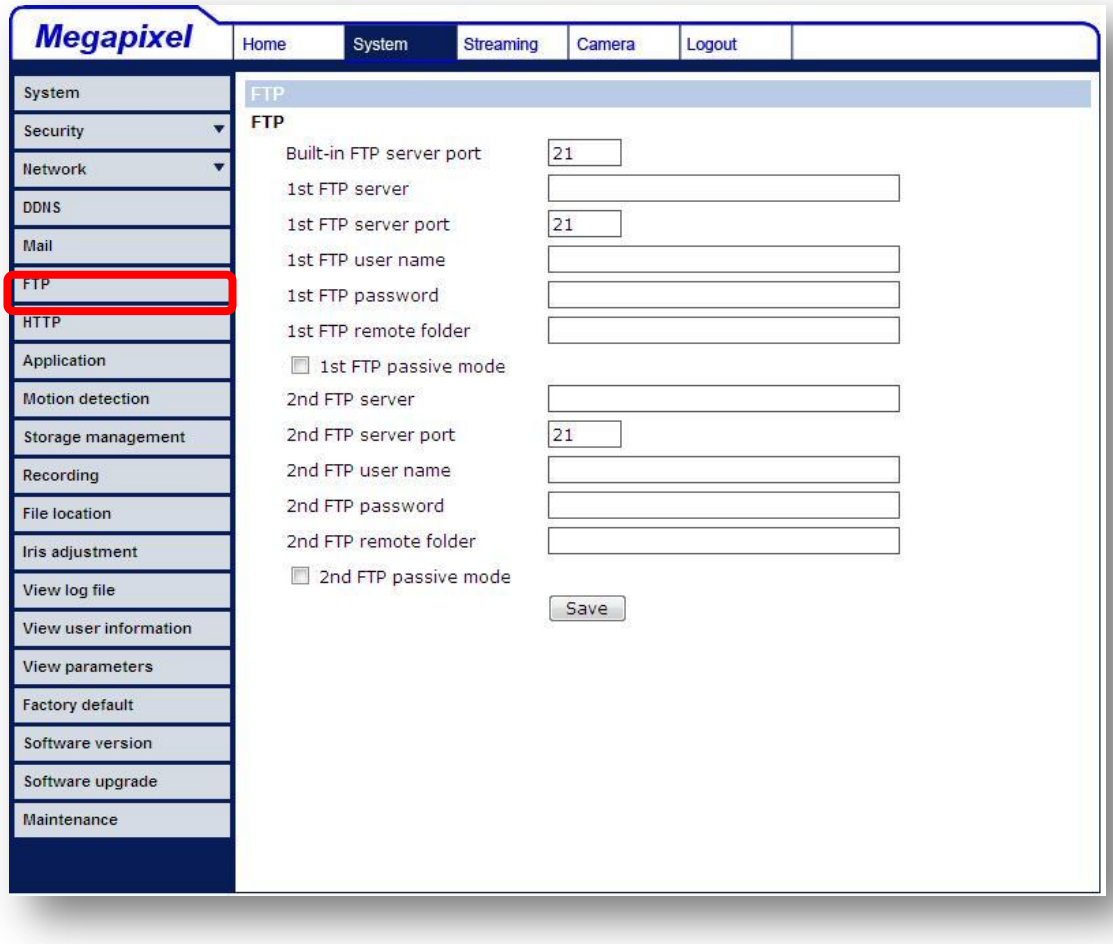
The Administrator can send an e-mail via Simple Mail Transfer Protocol (SMTP) when an alarm is triggered. SMTP is a protocol for sending e-mail messages between servers. SMTP is a relatively simple, text-based protocol, where one or more recipients of a message are specified and the message text is transferred. The configuration page is shown as follows:



Two sets of SMTP can be configured. Each set includes SMTP Server, Account Name, Password and E-mail Address settings. For SMTP server, contact your network service provider for more specific information.

7.3.6 FTP

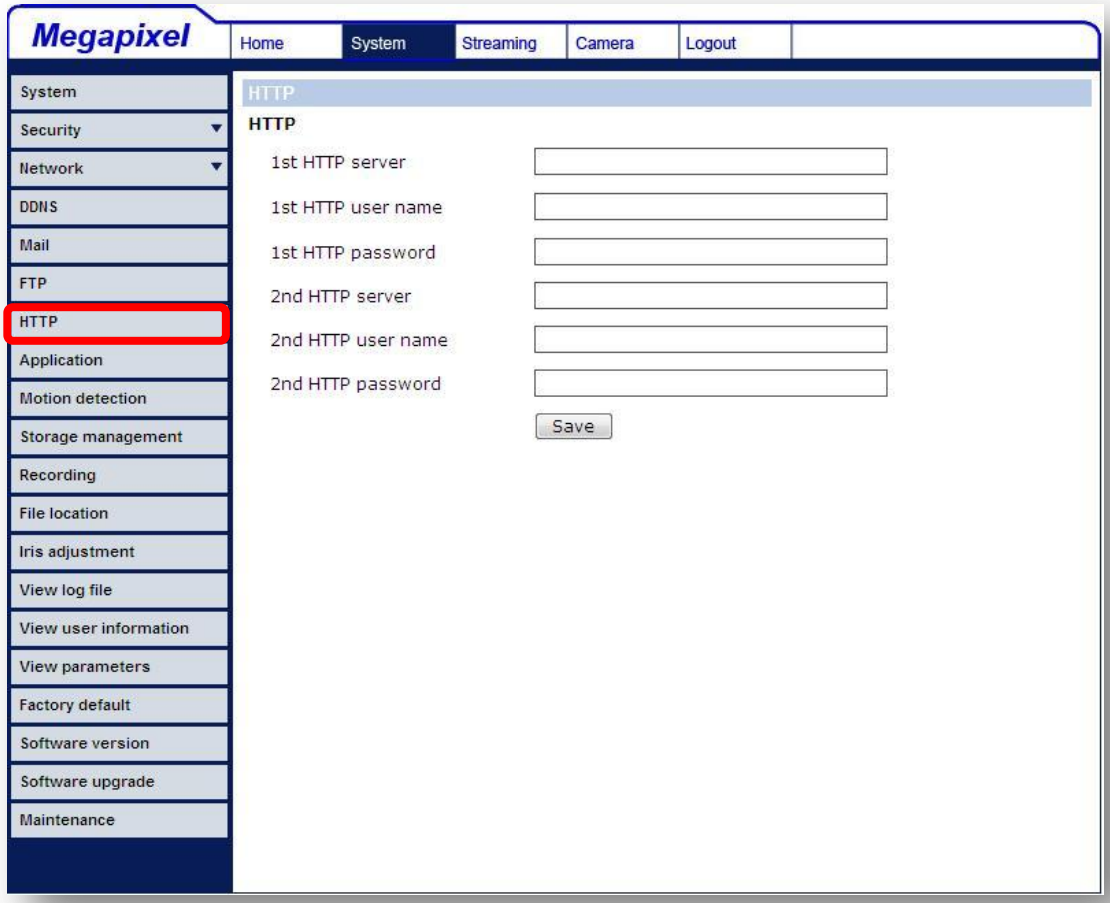
The Administrator can set as sending alarm message to a specific File Transfer Protocol (FTP) site when an alarm is triggered. Users can assign alarm message to up to two FTP sites. The FTP setting page is shown below. Enter the FTP details, which include server, server port, user name, password and remote folder, in the fields. Press “Save” when finished.



7.3.7 HTTP

A HTTP Notification server can listen for notification messages from IP Cameras by triggered events. The HTTP setting page is shown below. Enter the HTTP details, which include server, user name, and password in the fields. <Alarm> triggered and <Motion Detection> notifications can be sent to the specified <HTTP> server.

Click “Save” when finished.

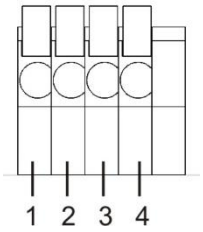


Please refer to: 7.3.8 Application: Send HTTP notification/ 7.3.9 Motion Detection for HTTP Notification settings.

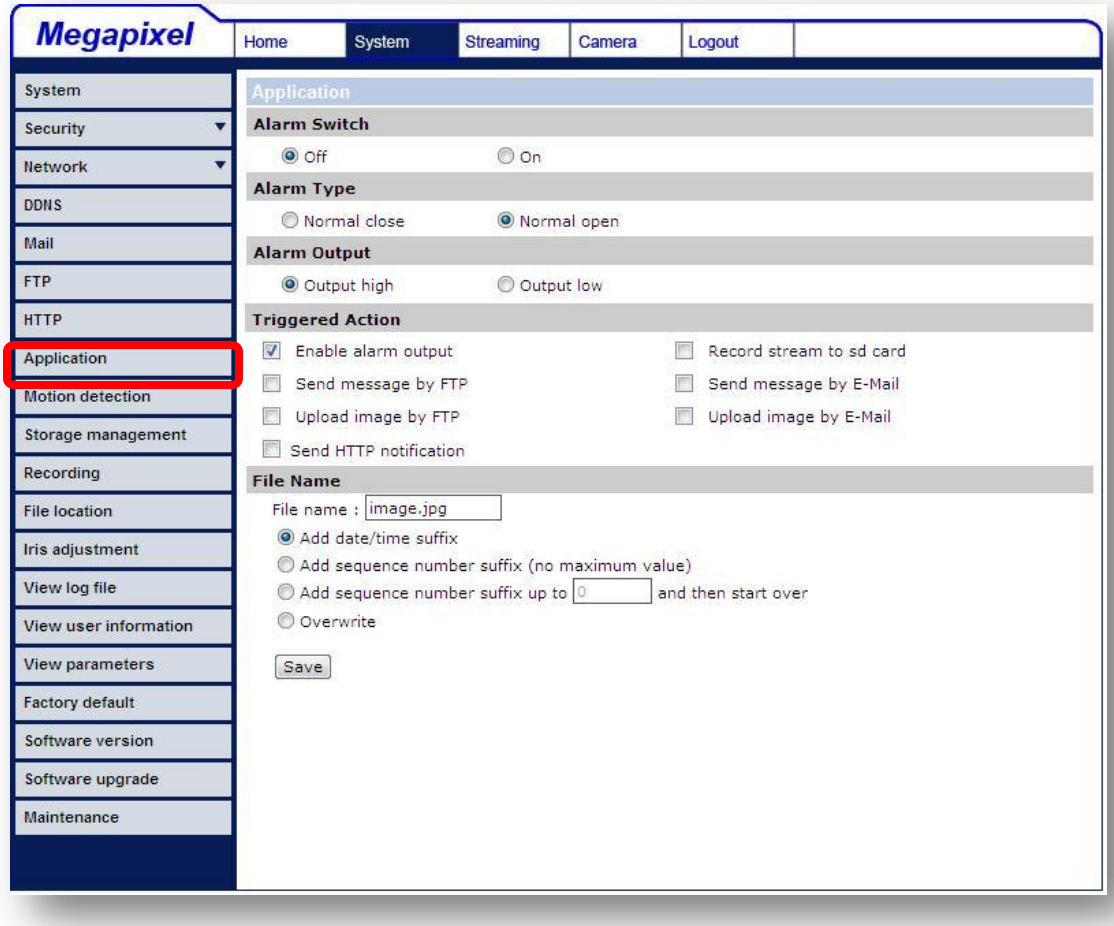
7.3.8 Application

The IP Camera equips one alarm input and one relay output for cooperating with alarm system to catch events' images. Refer to alarm pin definition below to connect alarm devices to the IP Camera if needed. The alarm configuration page is also shown below.

Alarm Pin Definition



PIN 1. Output+
PIN 2. Output-
PIN 3. Input+
PIN 4. Input-



Alarm Switch
The Administrator can enable or disable the alarm function.

Alarm Type
Select an alarm type, “Normal close” or “Normal open,” that corresponds with the alarm application.

Alarm Output
Define alarm output signal “high” or “low” as the normal alarm output status according to the current alarm application.

Triggered Action (Multi-option)
The Administrator can specify alarm actions that will take when the alarm is triggered. All options are listed as follows:

- **Enable Alarm Output**

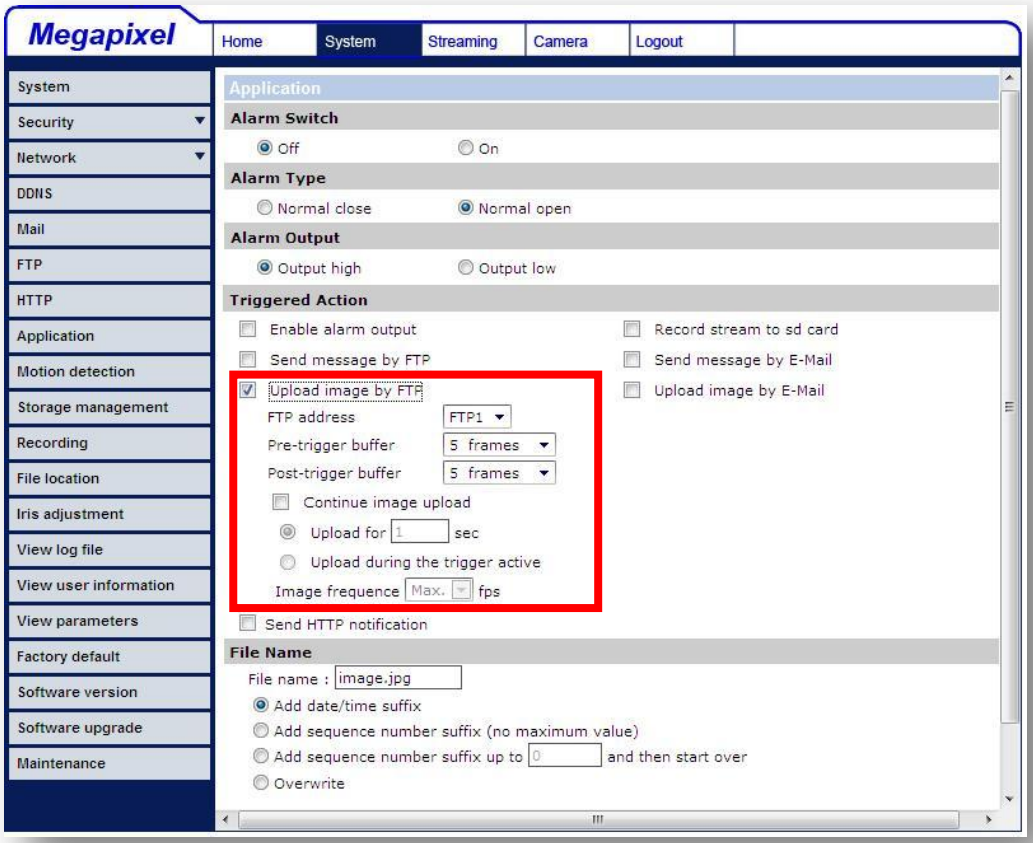
Select the item to enable alarm relay output.

- **Send Alarm Message by FTP/E-Mail**

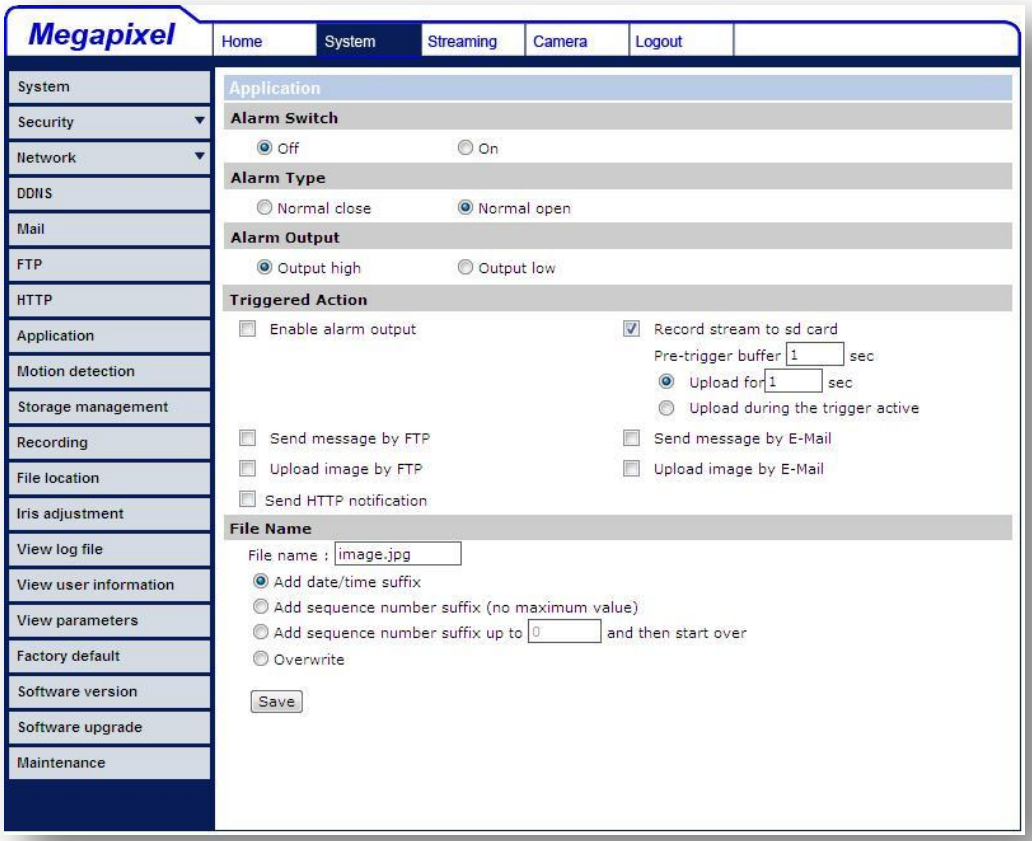
The Administrator can select whether to send an alarm message by FTP and/or E-Mail when an alarm is triggered.

- **Upload Image by FTP**

Select this item, and the Administrator can assign a FTP site and configure various parameters as shown in the figure below. When the alarm is triggered, event images will be uploaded to the appointed FTP site.



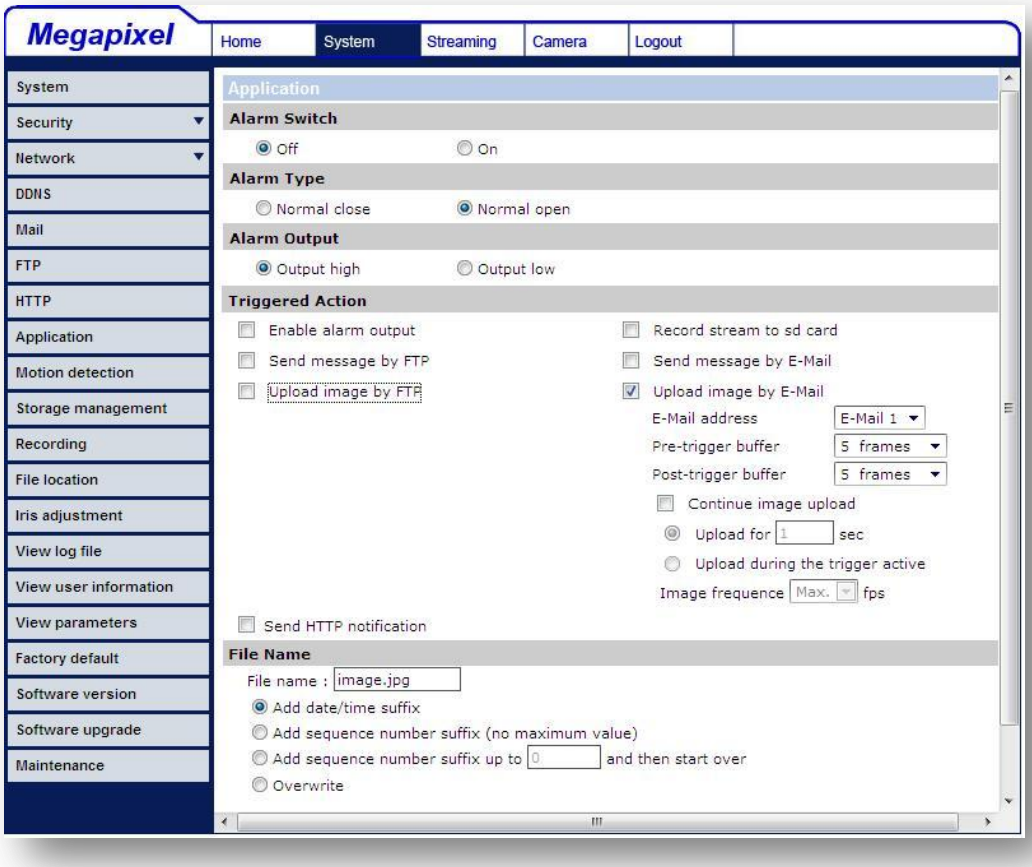
- **Record Stream to SD Card**
  Select the item and the alarm-triggered recording will be saved into your Micro SD card.



NOTE: Please make sure the local recording (with Micro SD/ SDHC card) is activated so that this function can be implemented. See section 7.3.12 Recording for further details.

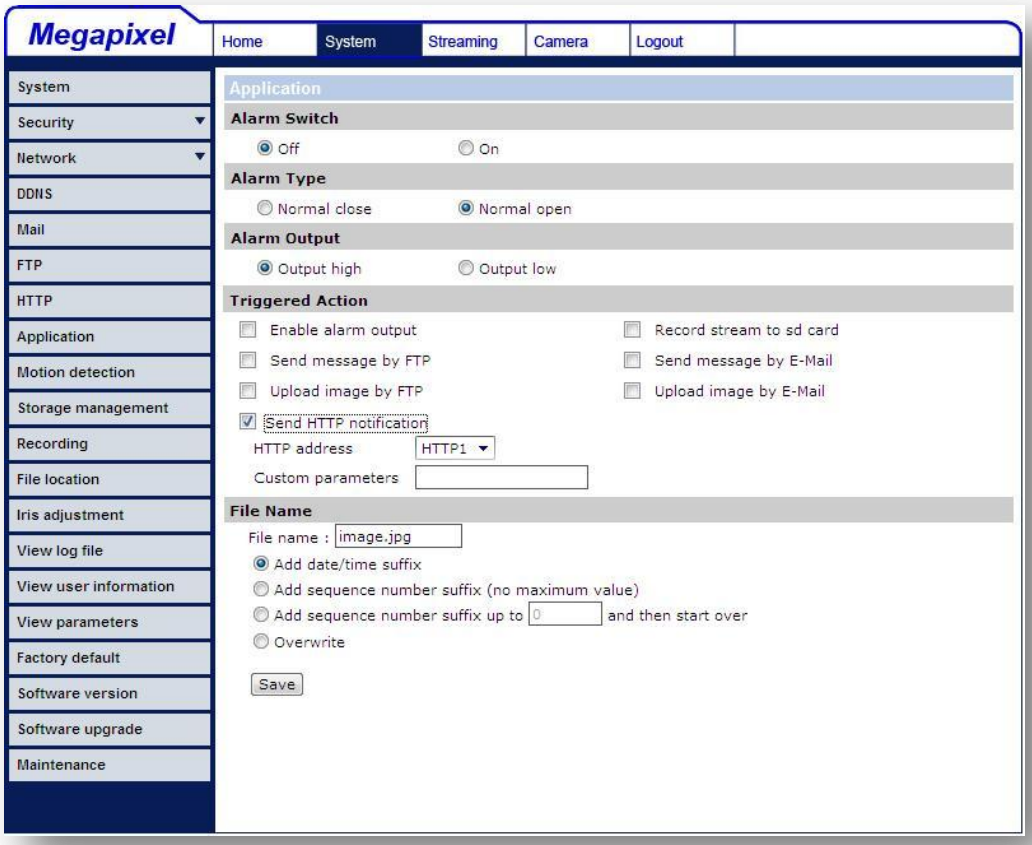
- **Upload Image by E-Mail**

Select this item, and the Administrator can assign an e-mail address and configure various parameters as shown in the figure below. When the alarm is triggered, event images will be sent to the appointed e-mail address.



NOTE: Make sure SMTP or FTP configuration has been completed. See section 7.3.5 Mail and 7.3.6 FTP for further details.

- **Send HTTP notification**
  Check this item, select the destination HTTP address, and specify the parameters for event notifications by <Alarm> triggered. When an alarm is triggered, the notification can be sent to the specified HTTP server.



File Name

Enter a file name in the blank, ex. image.jpg. The uploaded image's file name format can be set in this section. Please select the one that meets your requirements.

- **Add date/time suffix**

File name: imageYYMMDD_HHNNSS_XX.jpg
Y: Year, M: Month, D: Day
H: Hour, N: Minute, S: Second
X: Sequence Number

- **Add sequence number suffix (no maximum value)**

File name: imageXXXXXXX.jpg
X: Sequence Number

- **Add sequence number suffix (limited value)**
  File Name: imageXX.jpg
  X: Sequence Number
  The file name suffix will end at the number being set. For example, if the setting is up to “10,” the file name will start from 00, end at 10, and then start all over again.

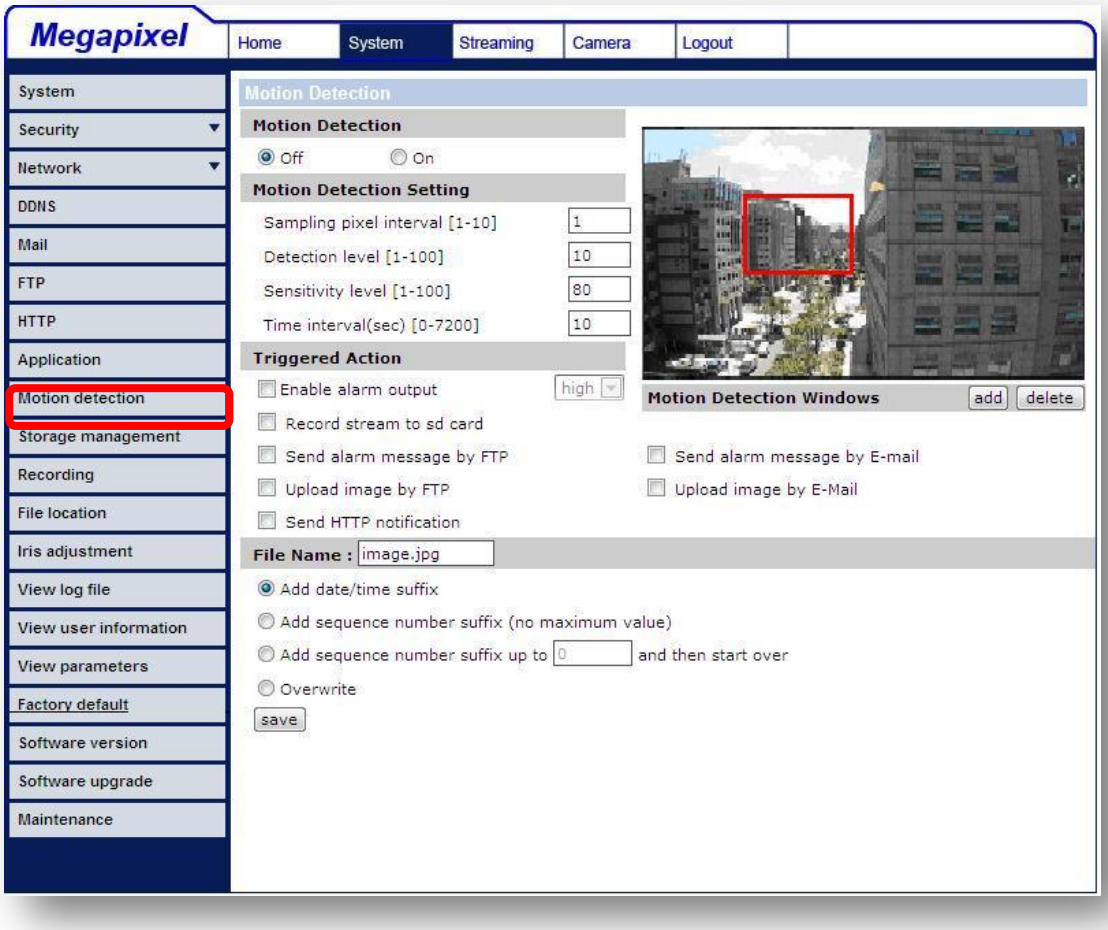
- **Overwrite**
  The original image in the FTP site will be overwritten by the new uploaded file with a static filename.

Save

After complete all the settings mentions above, please click on the Save button to save all the settings in this page.

7.3.9 Motion Detection

Motion Detection function allows detecting suspicious motion and triggering alarms when motion volume in the detected area reaches/exceeds the determined sensitivity threshold value.

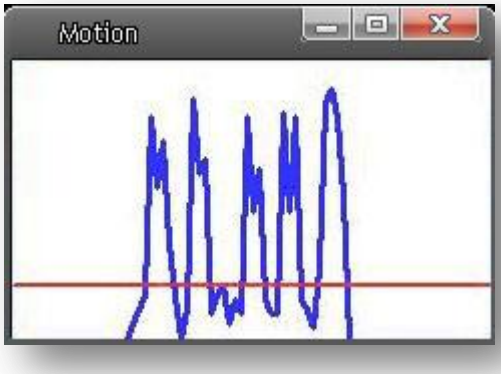


In the Motion Detection setting page, there is a frame (**Motion Detection Window**) displayed on the Live Video Pane. The Motion Detection Window is for defining the motion detection area. To change the size of the Motion Detection Window, move the mouse cursor to the edge of the frame and draw it outward/inward. Moving the mouse to the center of the frame can shift the frame to the intended location.

Up 10 Motion Detection Windows can be set. Press the “add” button under the Live Video Pane to add a Motion Detection Window. To cancel a Motion Detection Window, move the mouse cursor to the selected Window, and click on the “delete” button.

If Motion Detection function is activated, the pop-off window (Motion) with indication of motion will be shown.

When motion is detected, the signals will be displayed on the Motion window as shown below.



Detailed settings of Motion Detection are described as follows:

Motion Detection

You will be able to turn on/off Motion Detection in System section. Default setting is Off.

Motion Detection Setting

Users could adjust various parameters of Motion Detection in this section.

- **Sampling pixel interval [1-100]:**
  The default value is 10, which means system will take one sampling pixel for every 10 pixel.

- **Detection level [1-100]:**
  The default level is 10. The item is to set detection level for each sampling pixel; the smaller the value, the more sensitive it is.

- **Sensitivity level [1-100]:**
  The default level is 80, which means if 20% or more sampling pixels are detected differently, system will detect motion. The bigger the value, the more sensitive it is. Meanwhile, when the value is bigger, the red horizontal line in the motion indication window will be lower accordingly.

- **Time interval (sec) [0-7200]:**
  The default interval is 10. The value is the interval between each detected motion.

Triggered Action (Multi-option)
The Administrator can specify alarm actions that will take when motion is detected. All options are listed as follows:

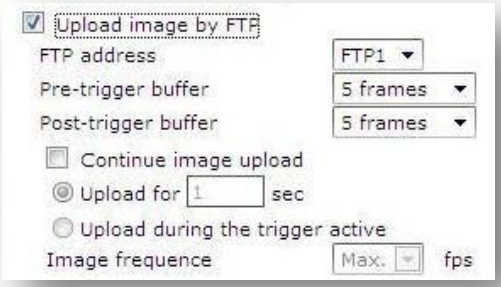
- **Enable Alarm Output**
  Check the item and select the predefined type of alarm output to enable alarm relay output when motion is detected.

- **Record stream to SD Card**
  Select this item, and the Motion Detection recording will be stored in Micro SD/ SDHC card when motion is detected.

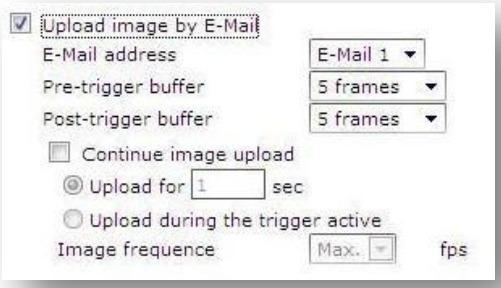
NOTE: Please make sure the local recording (with Micro SD/ SDHC card) is activated so that this function can be implemented. See section 7.3.12 Recording for further details.

- **Send Alarm Message by FTP/E-Mail**
  The Administrator can select whether to send an alarm message by FTP and/or E-Mail when motion is detected.

- **Upload Image by FTP**
  Select this item, and the Administrator can assign a FTP site and configure various parameters as shown in the figure below. When motion is detected, event images will be uploaded to the appointed FTP site.

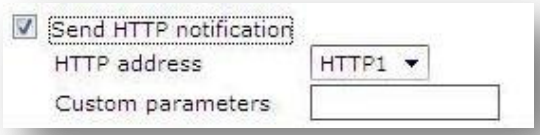


- **Upload Image by E-Mail**
  Select this item, and the Administrator can assign an e-mail address and configure various parameters as shown in the figure below. When motion is detected, event images will be sent to the appointed e-mail address.



NOTE: Make sure SMTP or FTP configuration has been completed. See section 7.3.5 Mail and 7.3.6 FTP for further details.

- **Send HTTP notification**
  Check this item, select the destination HTTP address, and specify the parameters for event notifications by <Motion Detection> triggered. When an alarm is triggered, the notification can be sent to the specified HTTP server.

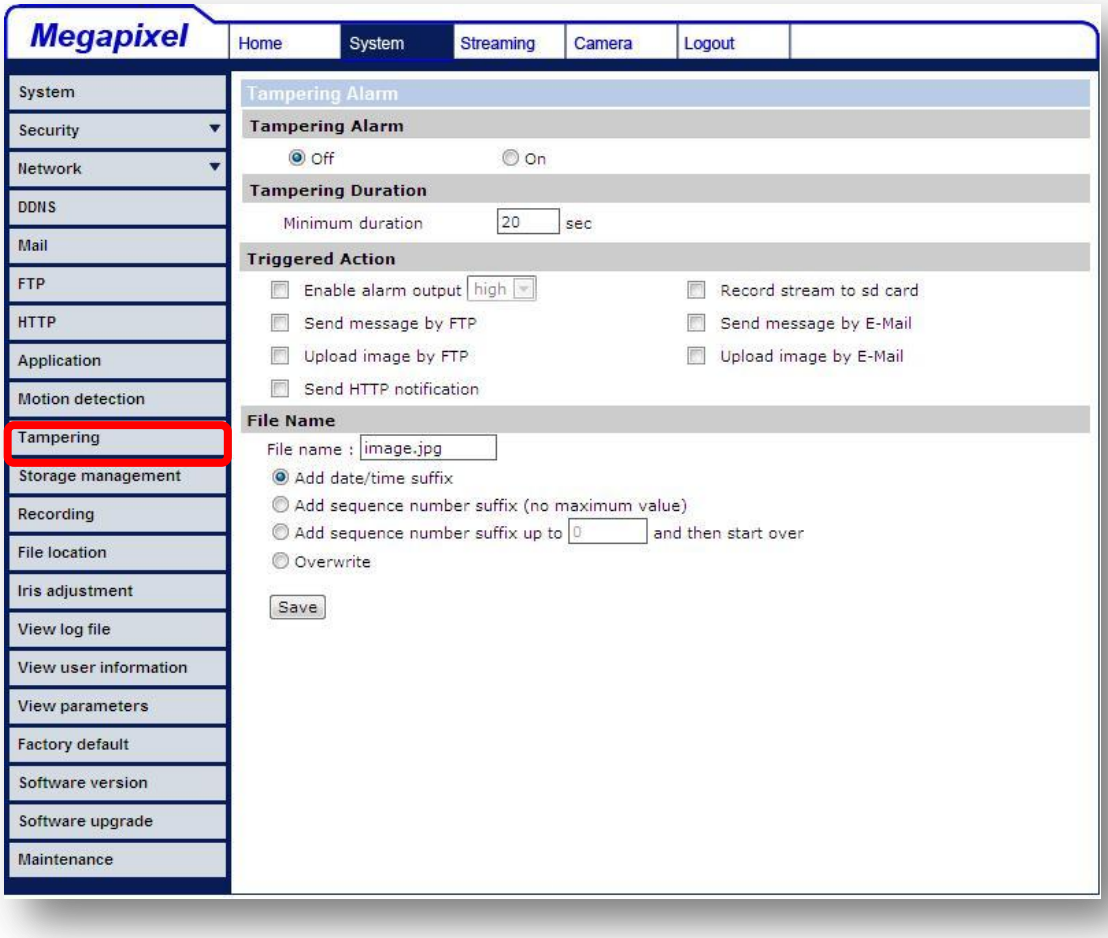


File Name
The uploaded image's filename format can be set in this section. Please select the one that meets your requirements.

Save
Click the Save button to save all the Motion Detection settings mentioned above.

7.3.10 Tampering

Tempering Alarm function helps the IP Camera against tampering such as deliberate redirection, blocking, paint spray, and lens cover, etc through video analysis and reaction to such events by sending out notifications or uploading snapshots to the specified destination(s).



Detection of camera tampering is achieved by measuring the differences between the older frames of video (which are stored in buffers) and more recent frames.

Tampering Alarm

You will be able to turn on/off Tampering Alarm function in Tampering Alarm setting page. The default setting is Off.

Tampering Duration

Minimum Tampering Duration is the time for video analysis to determine whether camera tampering has occurred. Minimum Duration could also be

interpreted as defining the Tampering threshold; longer duration represents higher threshold. Settable Tampering Duration time range is from 10 to 3600 seconds.

Triggered Action (Multi-option)
The Administrator can specify alarm actions that will take when tampering is detected. All options are listed as follows:

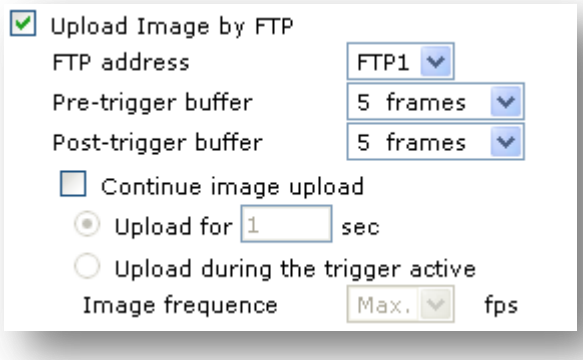
- **Enable Alarm Output**
  Check the item and select the predefined type of alarm output to enable alarm relay output when tampering is detected.

- **Record stream to SD Card**
  Select this item, and the Tampering Alarm recording will be stored in Micro SD/ SDHC card when tampering is detected.

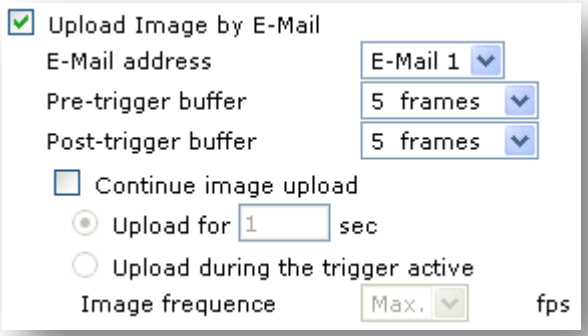
NOTE: Please make sure the local recording (with Micro SD/ SDHC card) is activated so that this function can be implemented. See section 7.3.12 Recording for further details.

- **Send Alarm Message by FTP/E-Mail**
  The Administrator can select whether to send an alarm message by FTP and/or E-Mail when tampering is detected.

- **Upload Image by FTP**
  Select this item, and the Administrator can assign a FTP site and configure various parameters as shown in the figure below. When tampering is detected, event images will be uploaded to the appointed FTP site.

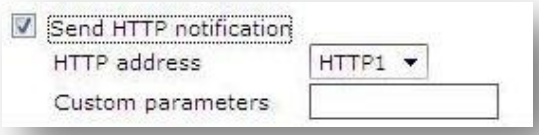


- **Upload Image by E-Mail**
  Select this item, and the Administrator can assign an e-mail address and configure various parameters as shown in the figure below. When tampering is detected, event images will be sent to the appointed e-mail address.



NOTE: Make sure SMTP or FTP configuration has been completed. See section 7.3.5 Mail and 7.3.6 FTP for further details.

- **Send HTTP notification**
  Check this item, select the destination HTTP address, and specify the parameters for HTTP notifications. When the Tampering Alarm is triggered, the HTTP notifications can be sent to the specified HTTP server.



File Name
The uploaded image's filename format can be set in this section. Please select the one that meets your requirements.

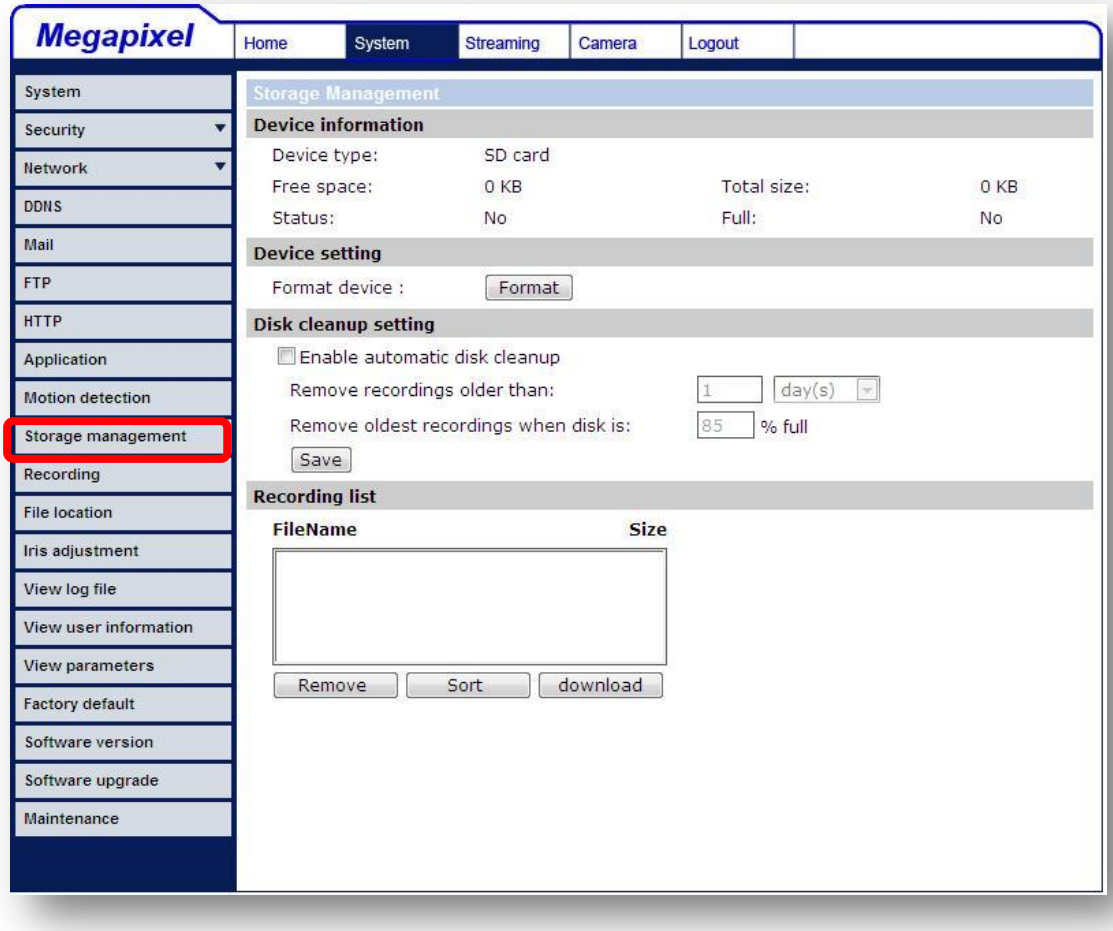
Save
Click the Save button to save all the Tampering Alarm settings mentioned above.

7.3.11 Storage Management

Users can implement local recording to the Micro SD/SDHC card up to 16GB. This page shows the capacity information of the Micro SD card and a recording list with all the recording files saved on the memory card. Users can also format the SD card and implement automatic recording cleanup through the setting page.

To implement Micro SD card recording, please go to the “Recording” page (see 7.3.12 Recording) for activation.

NOTE: Please format the Micro SD/SDHC card when using for the first time. Formatting will also be required when a memory card already being used on one camera and later transferred to another camera with different software platform.



Device information

When users insert the Micro SD/SDHC card, the card information such as the memory capacity and status will be shown at Device Information section.

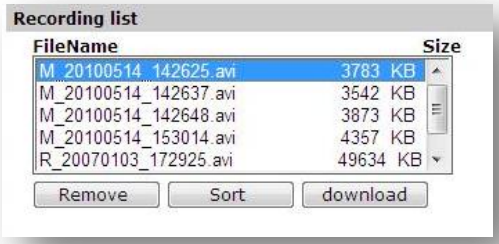
For the memory card being successfully installed, its status shall be shown at “Device information” section in the Storage Management page.

Device setting
Press the “Format” button to format the memory card.

Disk cleanup setting
Users can enable automatic recordings cleanup by specifying the time and storage limits

Recording List
Each video file on the Micro SD/SDHC card will be listed in the Recording list as shown below. The maximum file size is 60 MB (60 MB per file).

When the recording mode is set as “Always” (consecutive recording) and the Micro SD/ SDHC card recording is also allowed to be enabled by events triggered, once events occur, the system will immediately implement events recording to the memory card. Then the IP Camera will return to the regular recording mode after events recording.

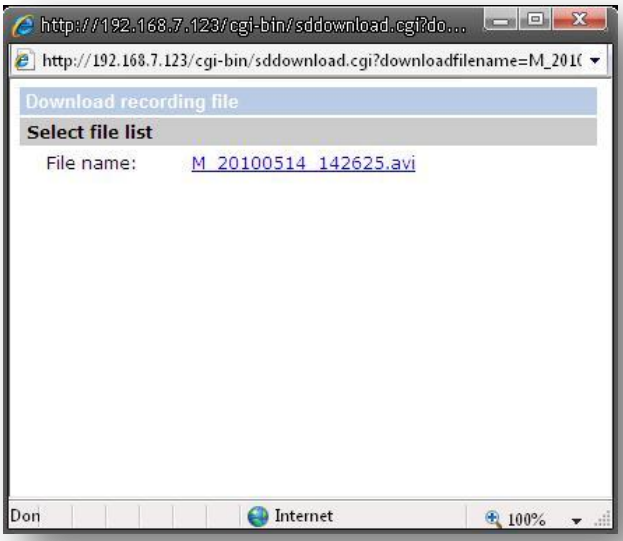


- **Remove**
  To remove a file, select the file first, and then press the “Remove” button.

- **Sort**
  Press the “Sort” button, and the files in the Recording list will be listed in name and date order.

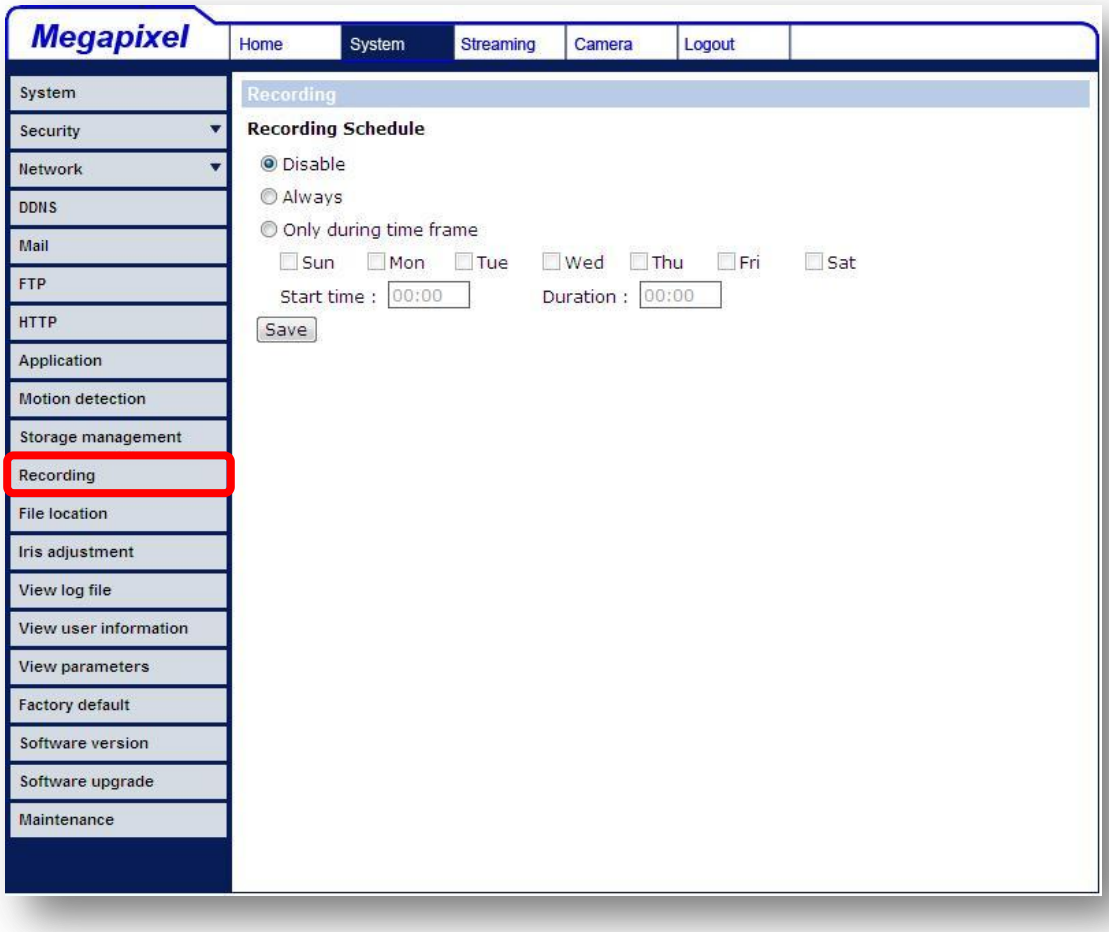
NOTE: The capital letter A/M/R appears in the very beginning of name denotes the sort of the recording: A stands for Alarm; M stands for Motion; R stands for regular recording.

- **Download**
  To open/download a video clip, select the file first, and then press the “download” button below the Recording list field. The selected file window will pop up as shown below. Click on the AVI file to directly play the video in the player or download it to a specified location.



7.3.12 Recording

In the Recording setting page, users can specify the recording schedule that fits the present surveillance requirement.



Activating Micro SD/SDHC Card Recording

Two types of schedule mode are offered: Always and Time Frame setting. Users can setup the time frame to fit the recording schedule or choose "Always" to activate Micro SD/SDHC Card Recording all the time.

Please click on the "Save" button for confirming the schedule mode.

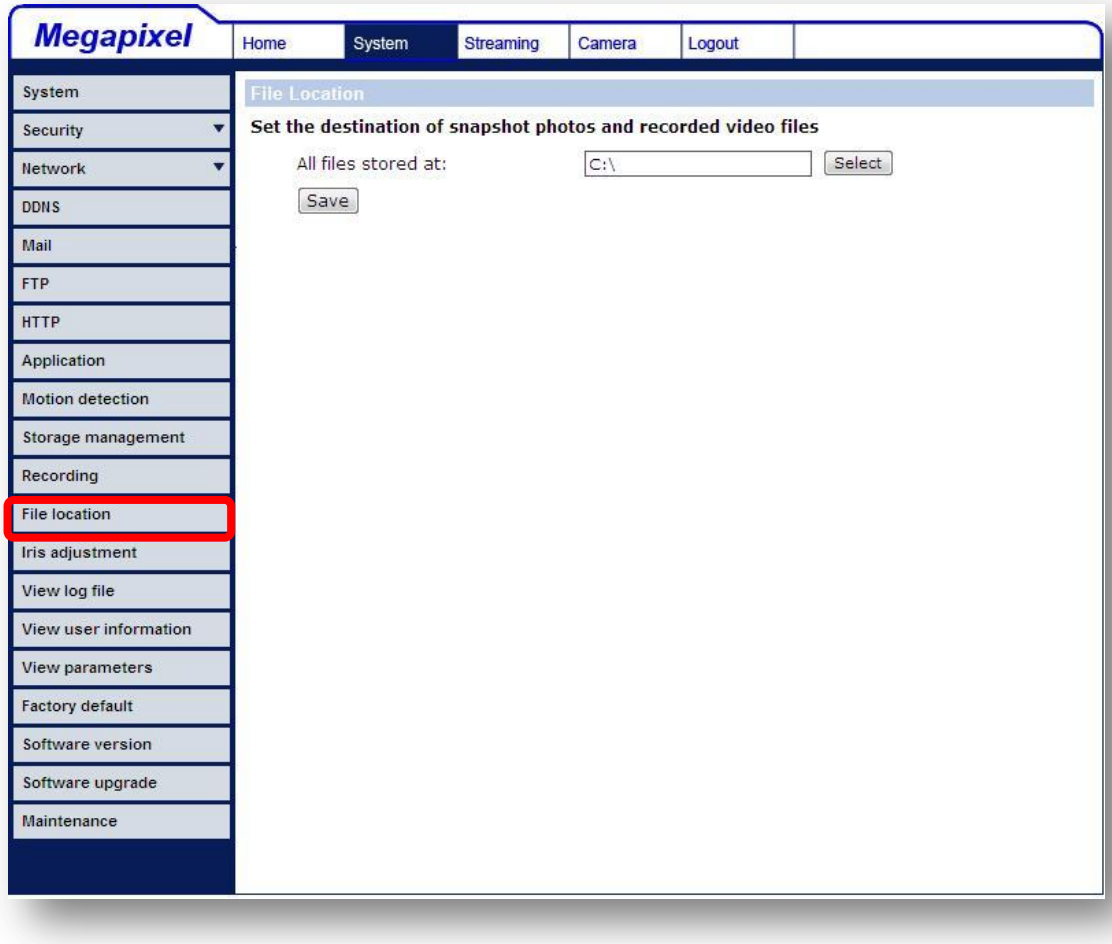
Terminating Micro SD/SDHC Card Recording

Select "Disable" to terminate the recording function.

7.3.13 File Location

Users can specify a storage location for the snapshots and web recording. The default setting is: C:\. Once confirm the setting, press “Save,” and all the snapshots and recording will be saved in the designate location.

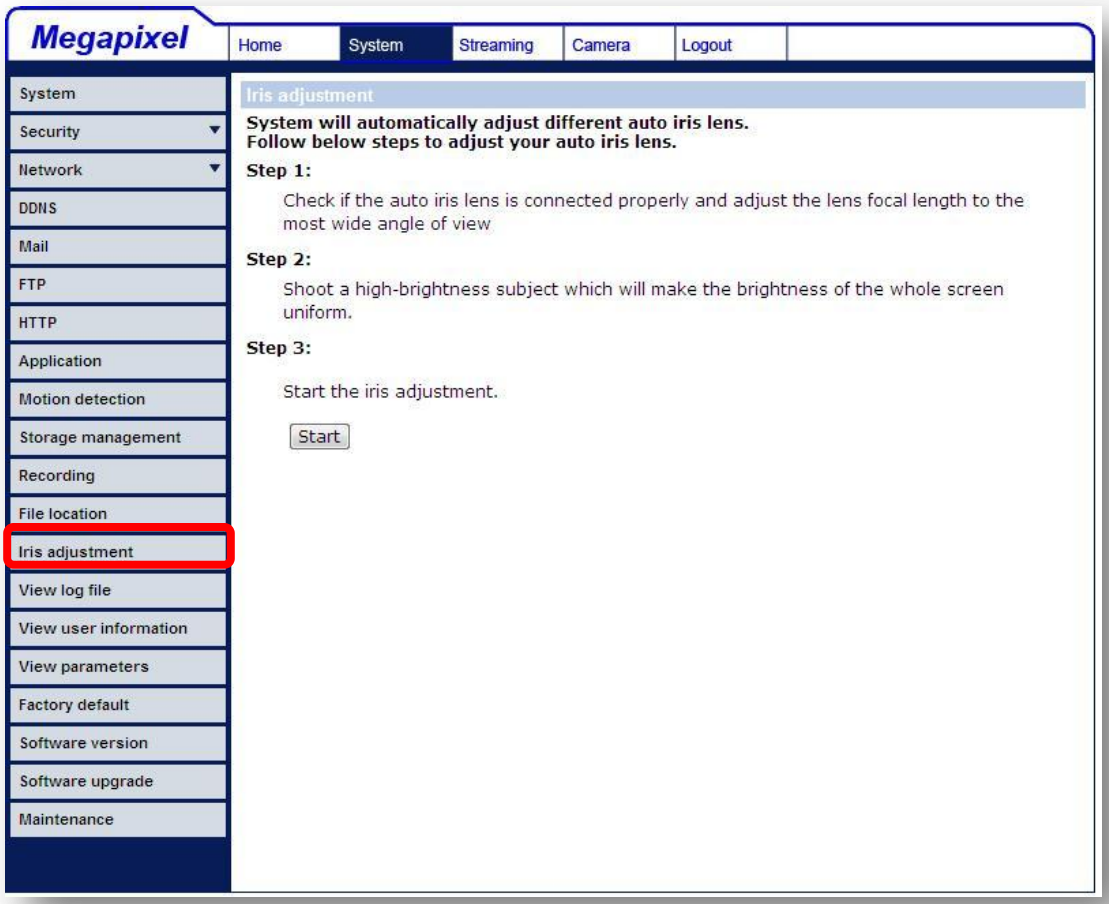
NOTE: Please make sure the selected file path contains valid characters such as letters and numbers.



NOTE: For users with Windows 7 operating system, it is required to log on as an Administrator to implement the Snapshot and Web Recording function.

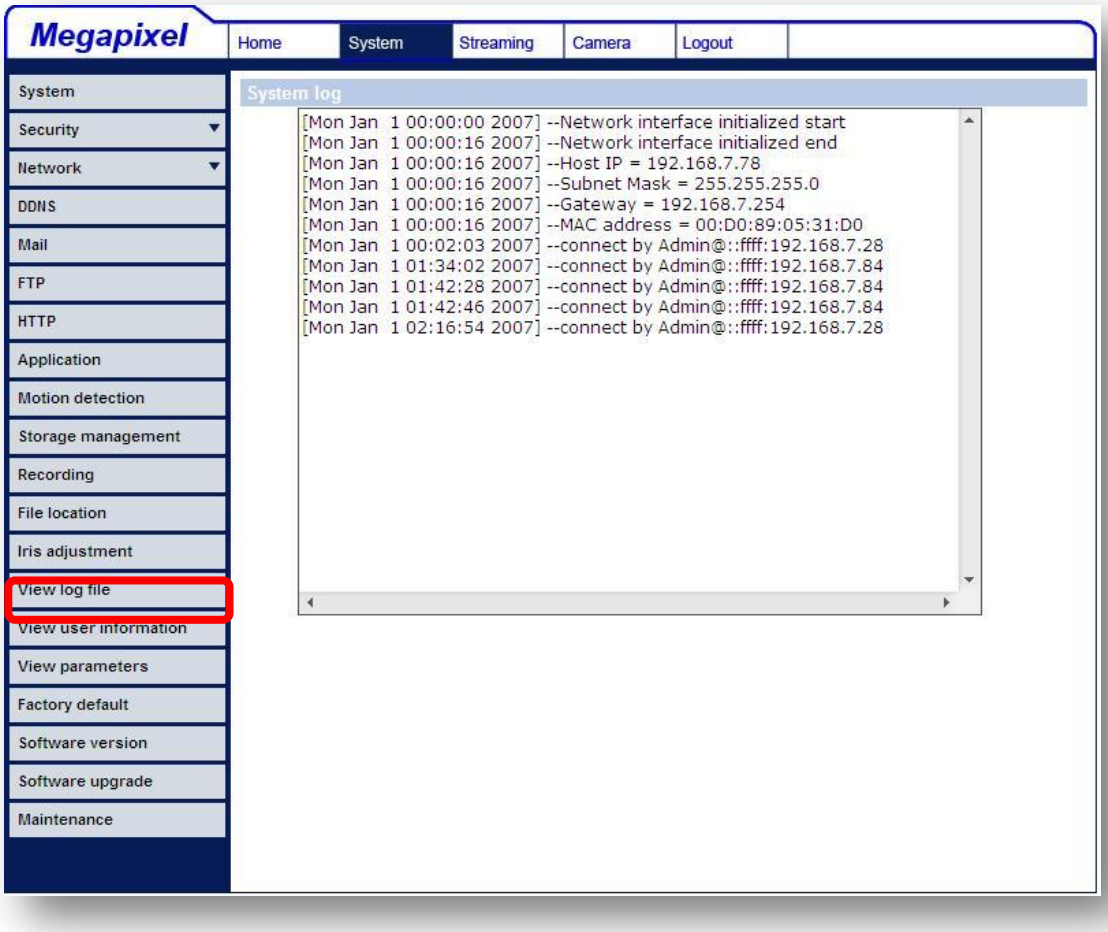
7.3.14 Iris Adjustment

For users who use Auto-iris lens, when it is required to implement iris adjustment, please refer to the Iris adjustment procedure in the setting page to adjust iris.



7.3.15 View Log File

Click on the link to view the system log file. The content of the file provides useful information about configuration and connections after system boot-up.



7.3.16 View User Information

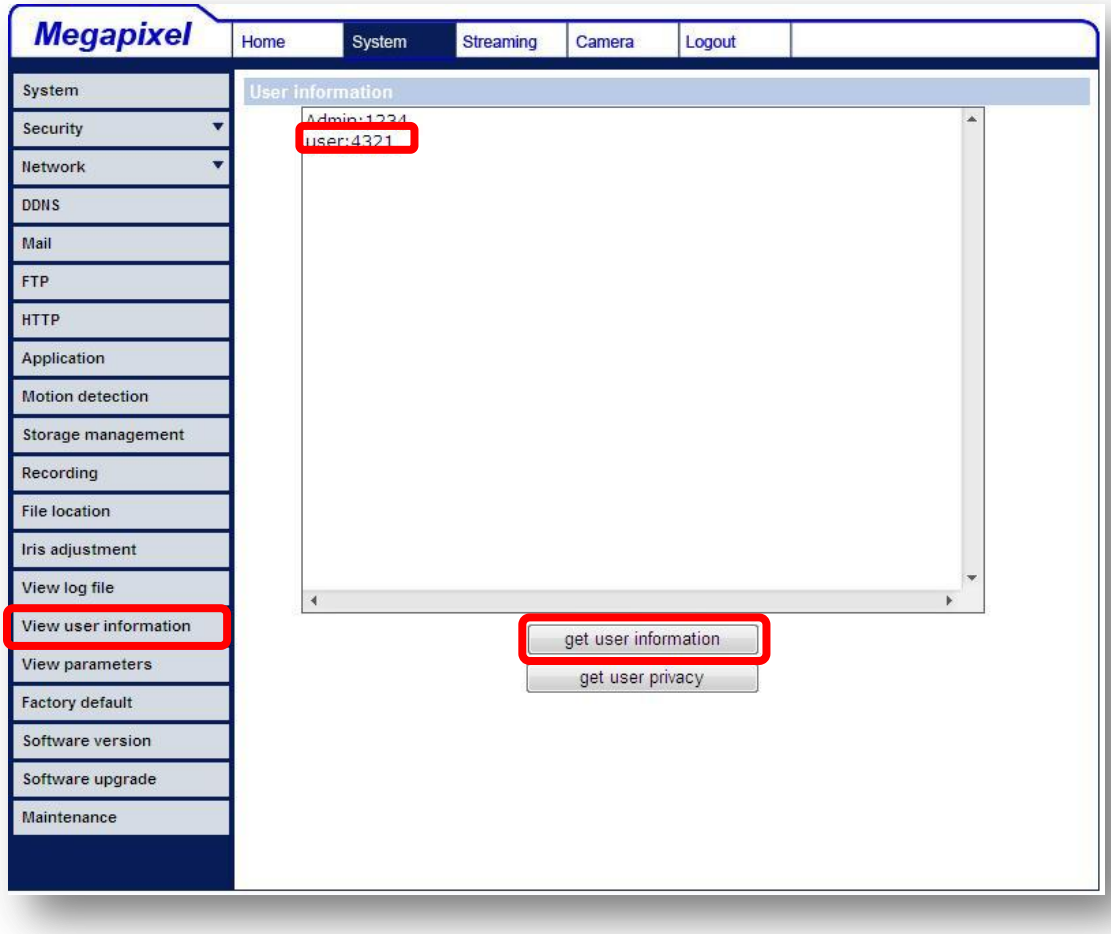
The Administrator can view each added user's login information and privileges (see 7.3.2 Security).

View User Login Information

All the users in the network will be listed in the "User information" zone, as shown below. As the figure below shows:

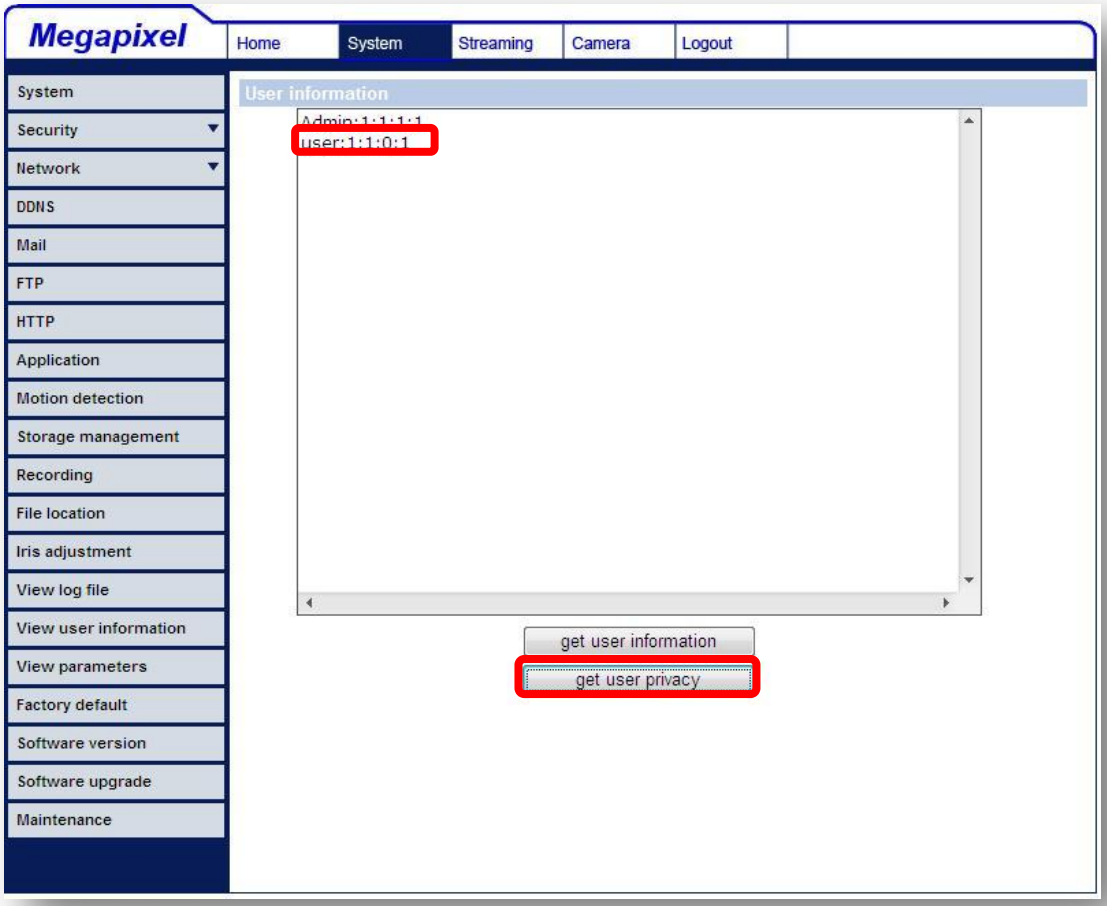
User: 4321

It indicates that one user's login username is: User, and the password is: 4321.



View User Privilege

Press “get user privacy” down the page, and the Administrator can view each user’s privileges.

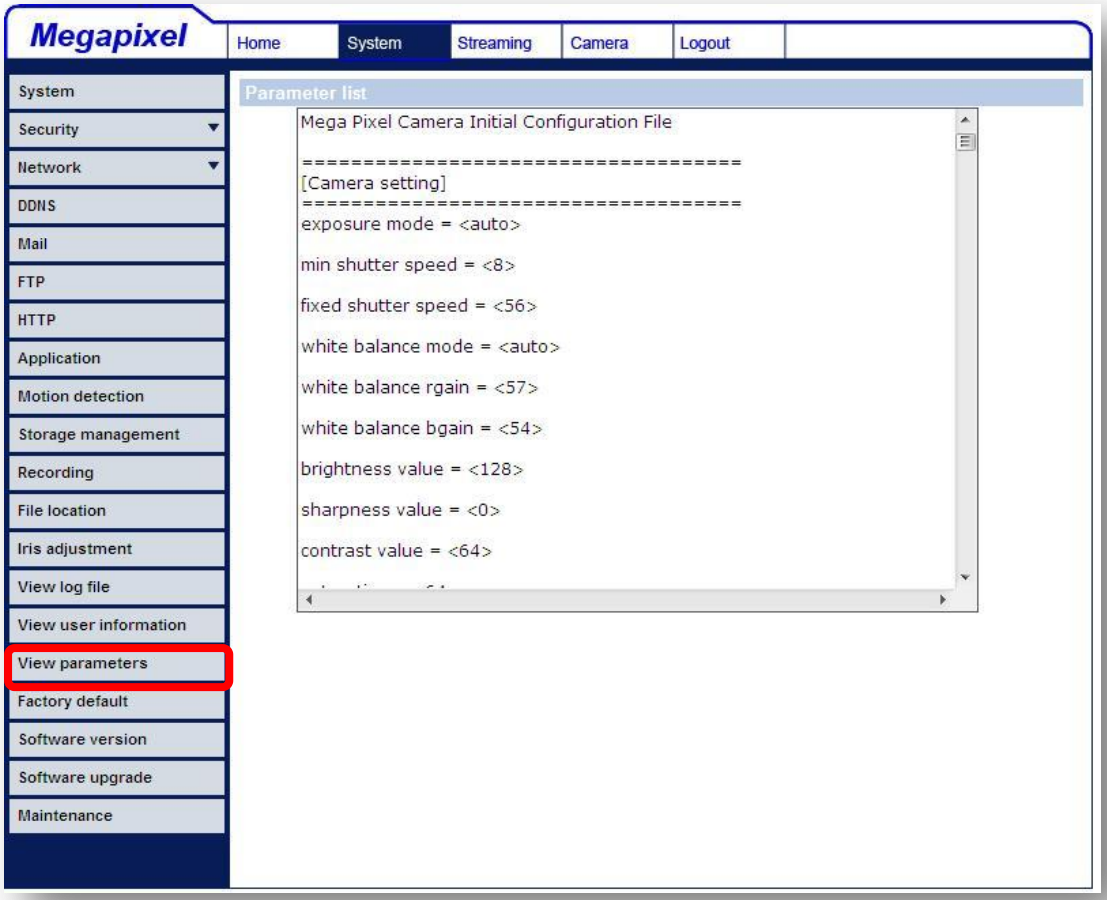


As the figure above shows:
User: 1:1:0:1
1:1:0:1= I/O access : Camera control : Talk : Listen (see 7.3.2 Security)

Therefore, it denotes the user is granted privileges of I/O access, Camera control and Listen.

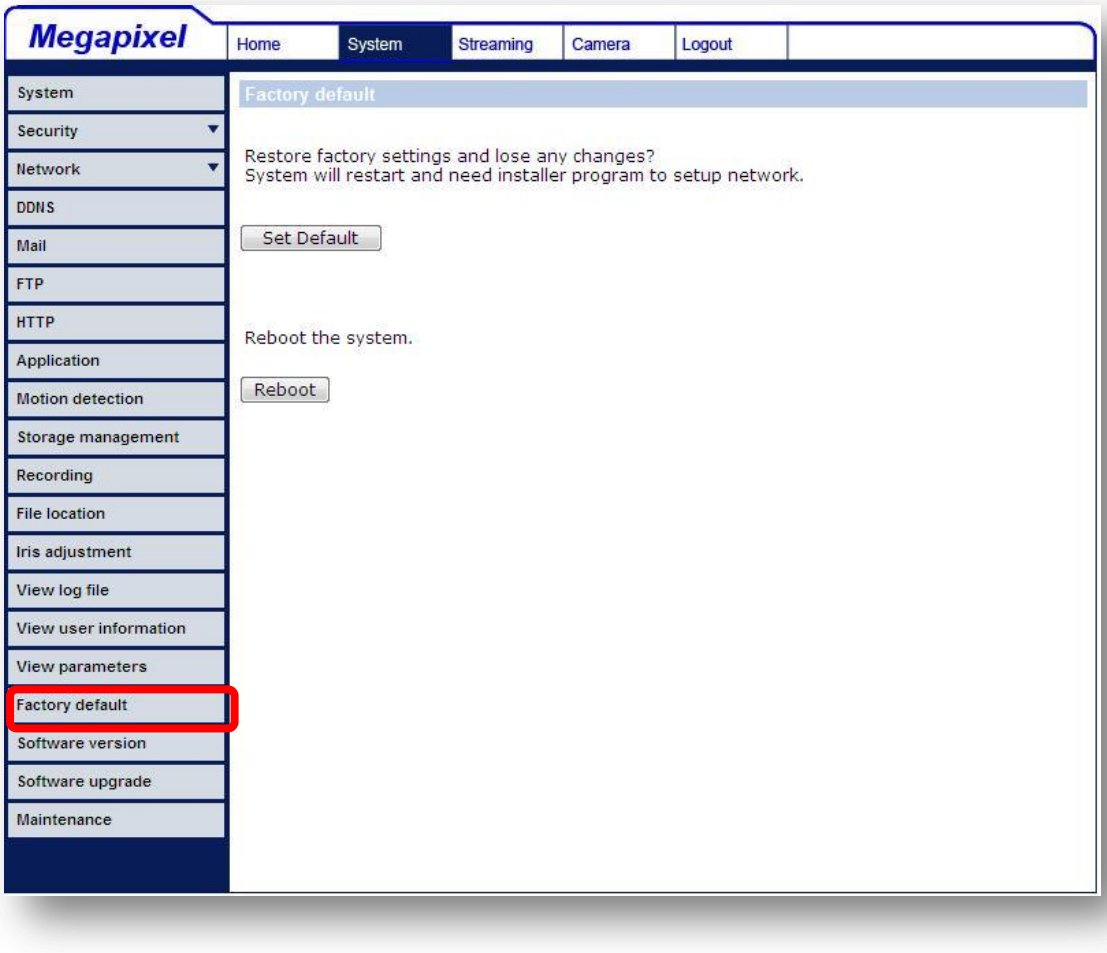
7.3.17 View Parameters

Click on this item to view the entire system's parameter setting.



7.3.18 Factory Default

The factory default setting page is shown as below. Follow the instructions to reset the IP Camera to factory default setting if needed.



Set Default

Click on the “Set Default” button to recall the factory default settings. Then the system will restart in 30 seconds.

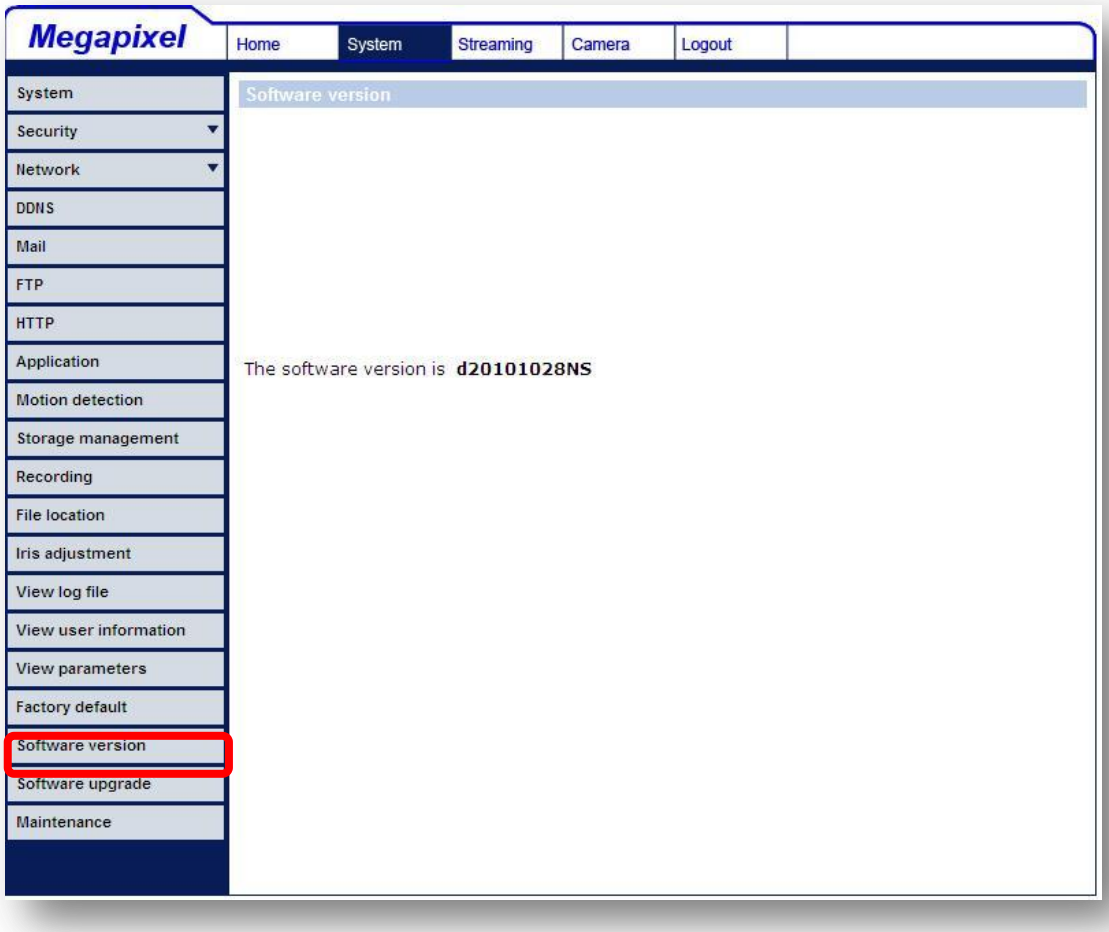
NOTE: The IP address will be restored to default.

Reboot

Click on the “Reboot” button, and the system will restart without changing current settings.

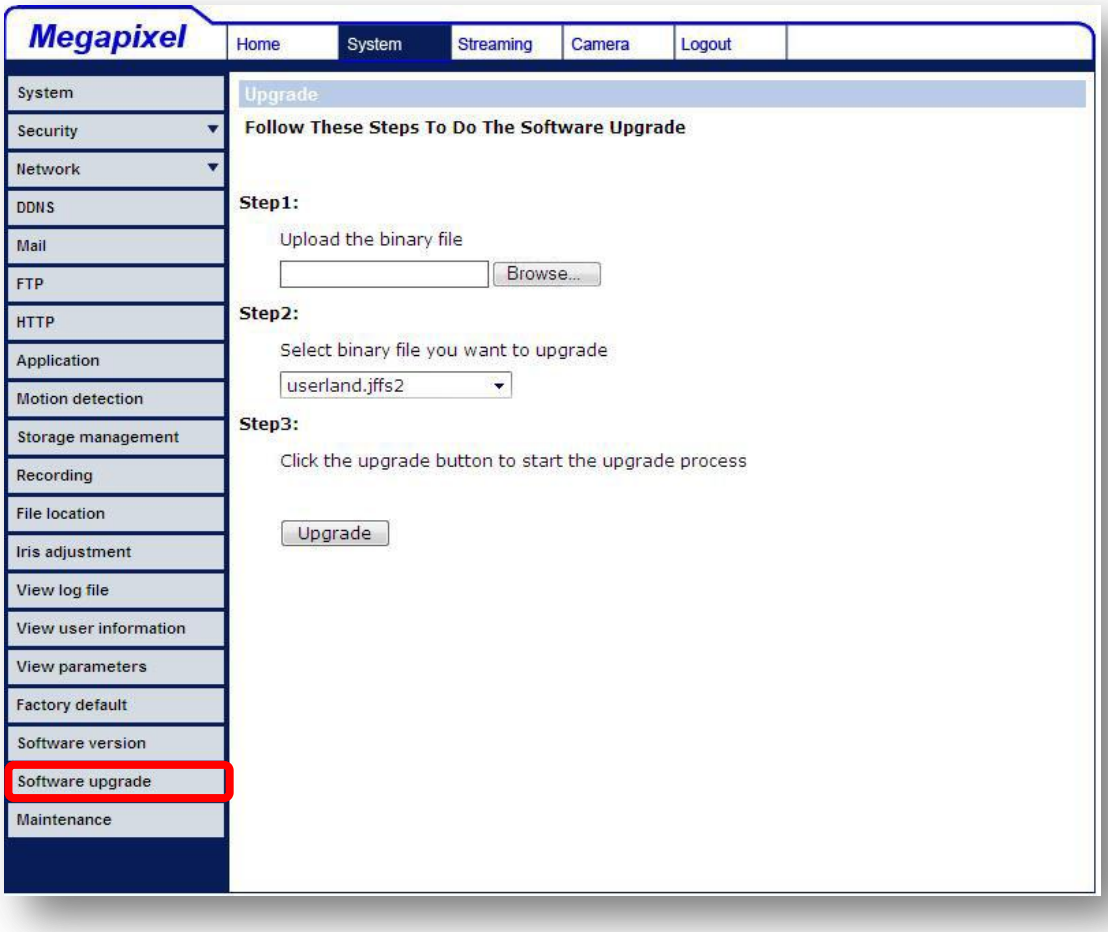
7.3.19 Software Version

The current software version is displayed in the software version page, which is shown as the figure below.



7.3.20 Software Upgrade

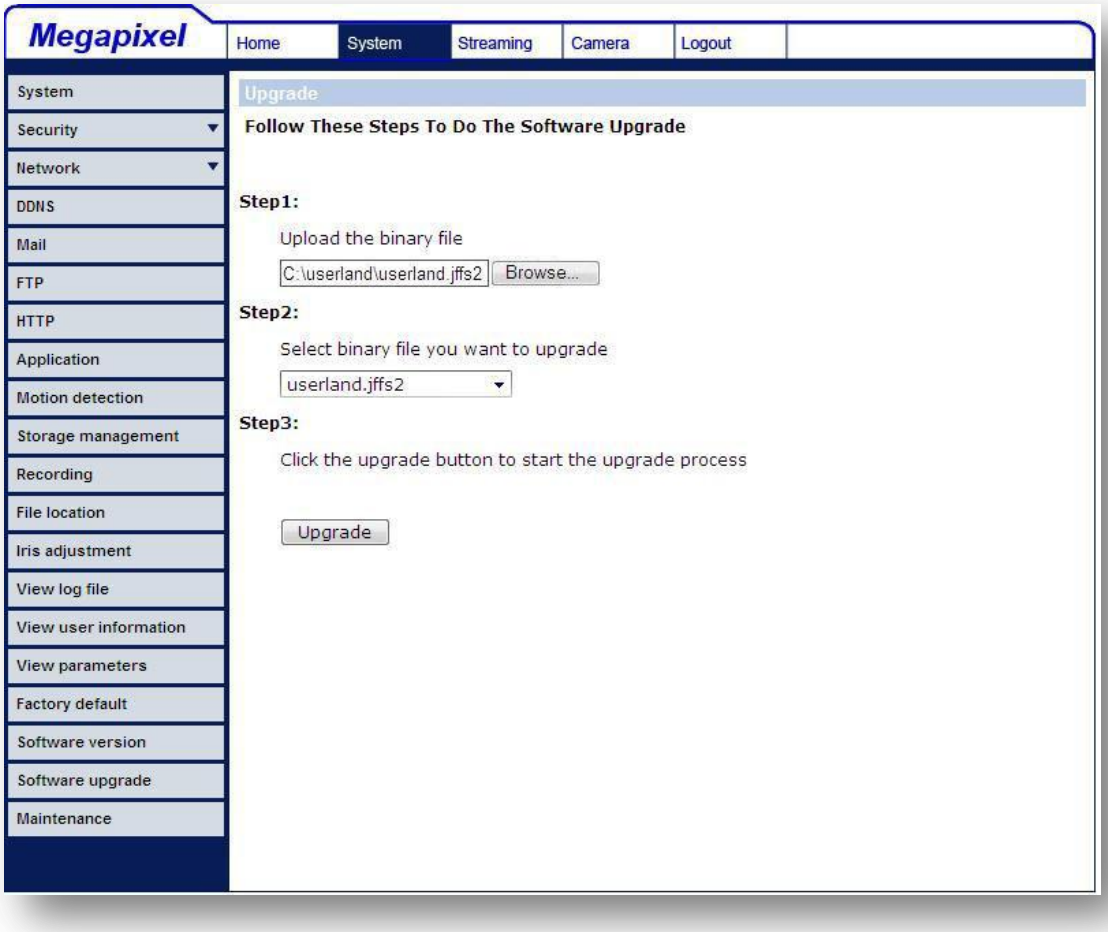
Software upgrade can be carried out in the “Software Upgrade” page, as shown below.



NOTE: Make sure the upgrade software file is available before carrying out software upgrade.

The procedure of software upgrade is like the following:

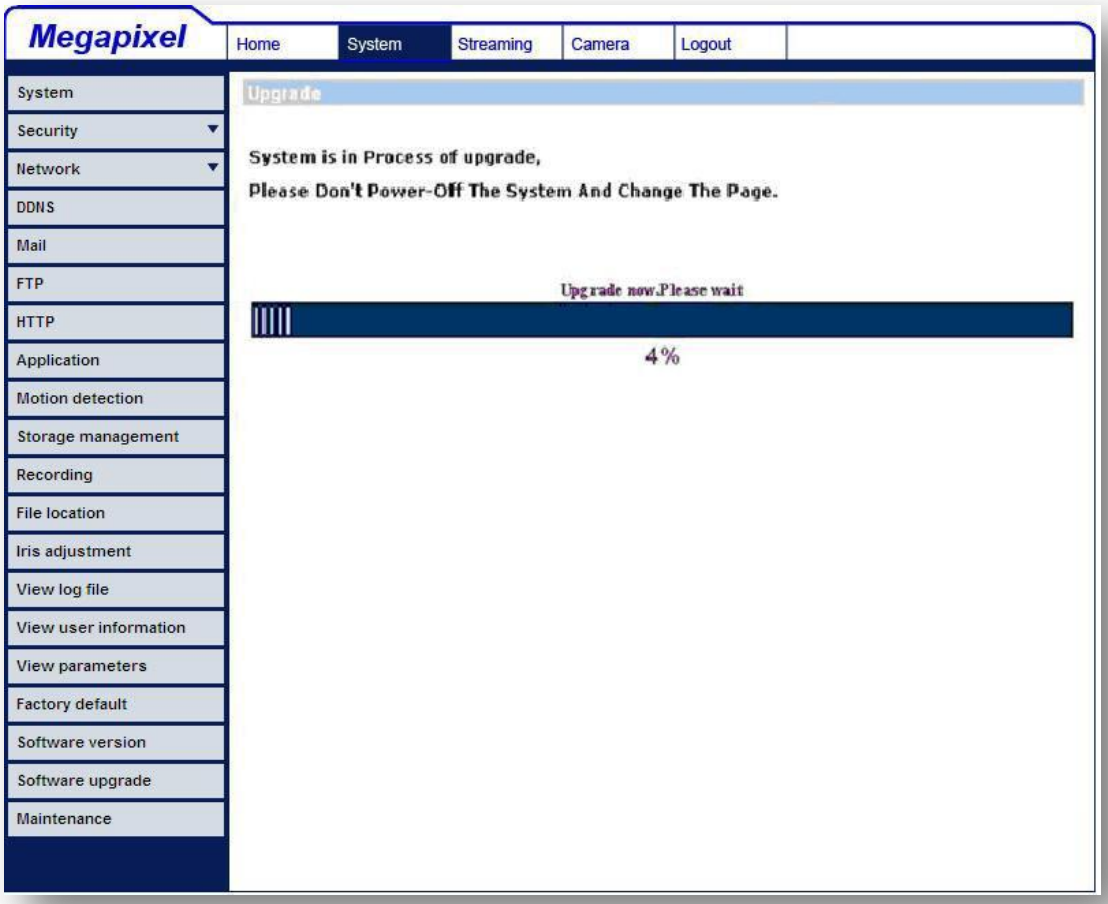
Step 1: Click “Browse” and select the binary file to be uploaded, ex. Userland.jffs2.



NOTE: Do not change the upgrade file name, or the system will fail to find the file.

Step 2: Pull down the upgrade binary file list and select the file you want to upgrade; in this case, select “userland.jffs2.”

Step 3: Press “Upgrade”. The system will first check whether the upgrade file exists or not, and then begin to upload the upgrade file. Subsequently, the upgrade status bar will display on the page. When it runs to 100%, the upgrade process is finished.



After the upgrade process is finished, the viewer will return to Home page.

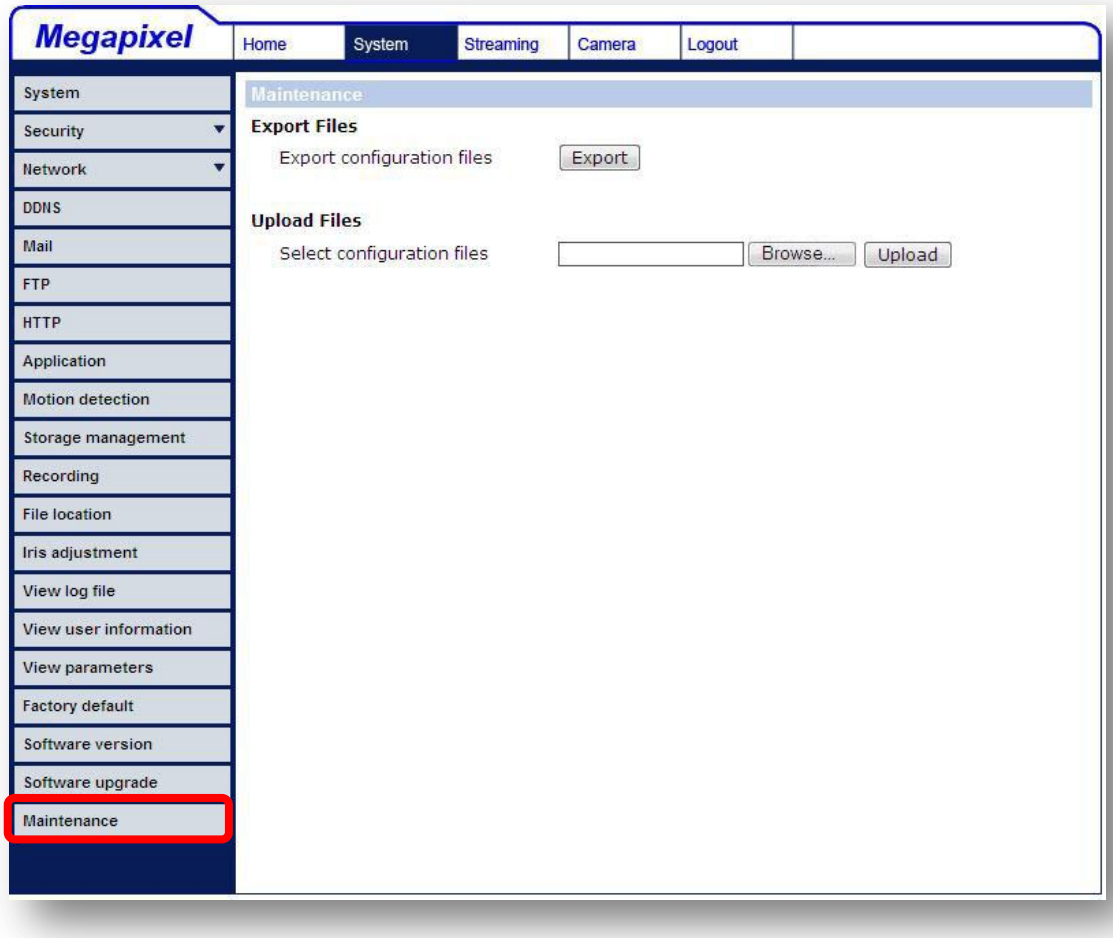
Step 4: Close the video browser.

Step 5: Click “Control Panel”, and then double click “Add or Remove Programs.” In the “Currently install programs” list, select “DCViewer” and click the button “Remove” to uninstall the existing DC Viewer.

Step 6: Open a new web browser, re-login the IP Camera, and then allow the automatic download of DC Viewer.

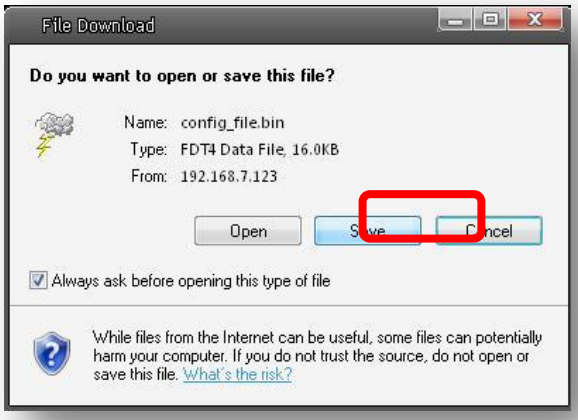
7.3.21 Maintenance

Users can export configuration files to a specified location and retrieve data by uploading an existing configuration file to the IP Camera.



Export

Users can save the system settings by exporting the configuration file (.bin) to a specified location for future use. Press the “Export” button, and the popup File Download window will come out as shown below. Click “Save” and specify a desired location for saving the configuration file.



Upload

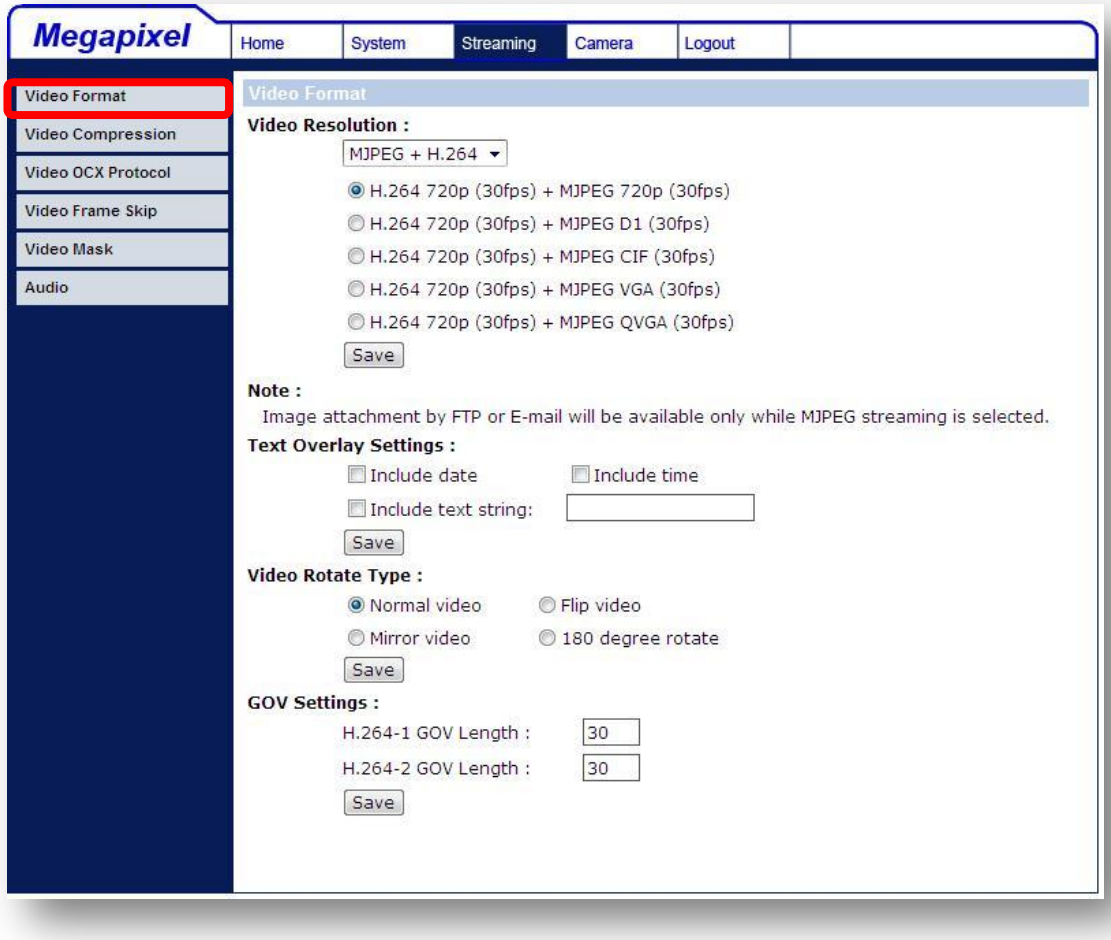
To copy an existing configuration file to the IP Camera, please first click on “Browse” to select the configuration file, and then press the “Upload” button for uploading.

7.4 Video and Audio Streaming Settings

Press the tab “Streaming” in the top of the page, and the configurable video and audio items will display in the left column. In Streaming, the Administrator can configure specific video resolution, video compression mode, video protocol, audio transmission mode, etc. Further details of these settings will be specified in the following sections.

7.4.1 Video Resolution and Rotate Type

The video setting page is shown below:



Video Format

Resolution for MJPEG & H.264 format includes:

- H.264 720p (30fps) + MJPEG 720p (30fps)
- H.264 720p (30fps) + MJPEG D1 (30fps)
- H.264 720p (30fps) + MJPEG CIF (30fps)
- H.264 720p (30fps) + MJPEG VGA (30fps)
- H.264 720p (30fps) + MJPEG QVGA (30fps)
- MJPEG 720p (30fps)+BNC Output
- MJPEG 1080p (30/ 15fps)
- MJPEG SXGA (30fps)
- H.264 720p (30fps)+H.264 D1 (30fps)
- H.264 720p (30fps) + H.264 CIF (30fps)
- H.264 720p (30fps) + H.264 VGA (30fps)
- H.264 720p (30fps) + H.264 VGA (30fps)
- H.264 720p (30fps) + H.264 QVGA (30fps Baseline)
- H.264 720p (30fps) + BNC Output
- H.264 1080p (30/ 15fps)
- H.264 SXGA (30fps)

Click “Save” to confirm the setting.

Text Overlay Settings

Users can select the items to display data including date/time/text on the live video pane. The maximum length of the string is 18 alphanumeric characters.

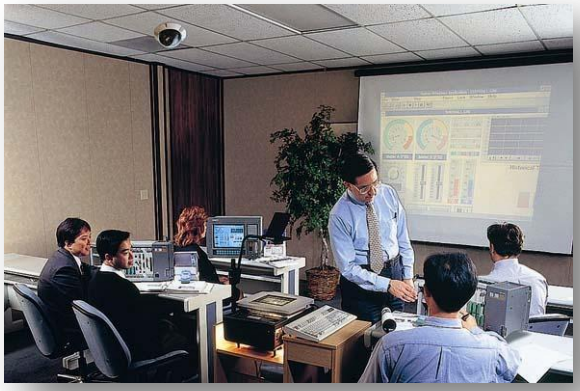
Click “Save” to confirm the Text Overlay setting.

Video Rotate Type

Users can change video display type if necessary. Selectable video rotate types include Normal, Flip, Mirror and 180 degree. Differences among these types are illustrated as below.

Suppose the displayed image of the IP Camera is shown as the figure below.

To rotate the image, users can select “Flip”, for instance. Then the displayed image will be reversed as shown below.



The following is descriptions for different video rotate type.

- **Flip**
  If select <Flip>, the image will be rotated vertically.

- **Mirror**
  If select <Mirror>, the image will be rotated horizontally.

- **180 Degree**
  Selecting <180 Degree> will make the image 180° counter-/clockwise inversed.

Click “Save” to confirm the setting.

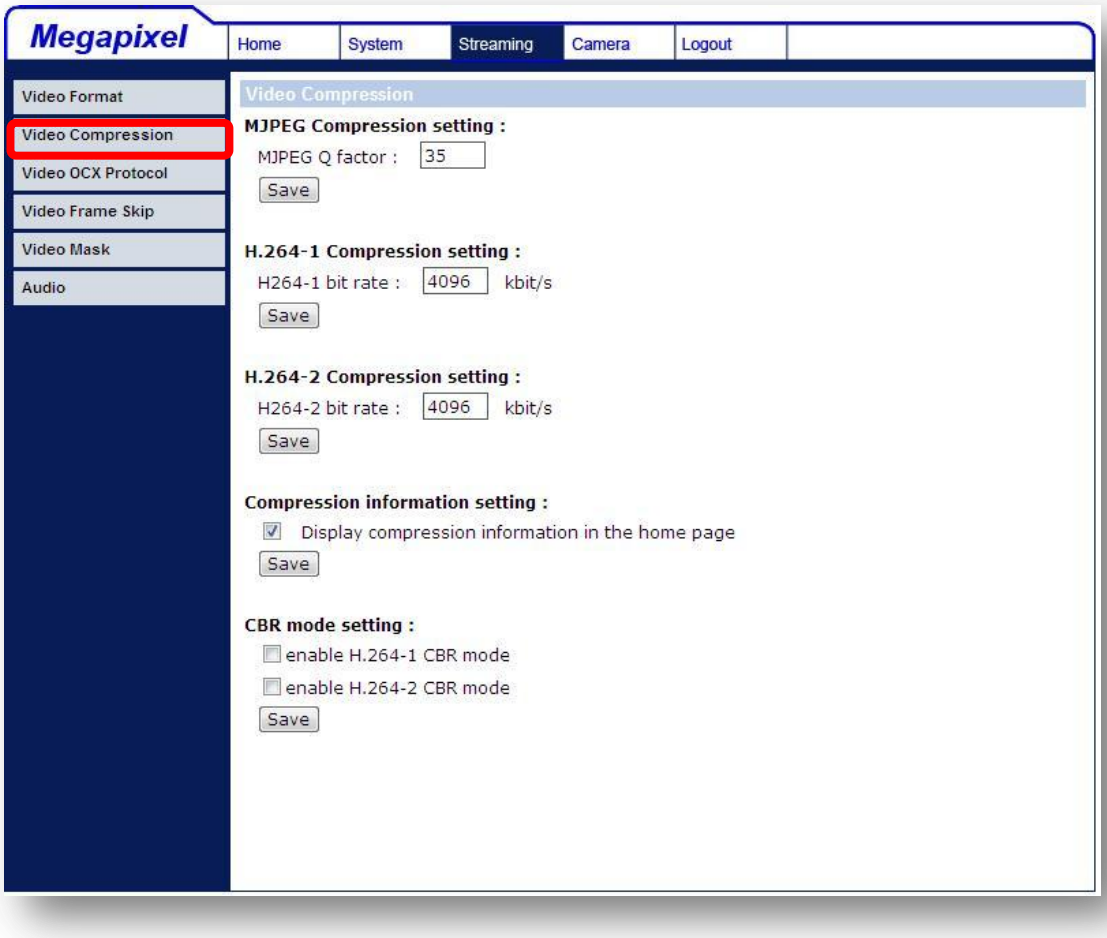
GOV Settings

Users can set the GOV length to determine the frame structure (I-frames and P-frames) in a video stream for saving bandwidth. Longer GOV means

decreasing the frequency of I-frames. Click “Save” to confirm the GOV setting.

7.4.2 Video Compression

Users can specify the values for MJPEG/H.264 compression mode in the video compression page (see the figure below), depending on the application.



MJPEG Q (Quality) factor

Higher value implies higher bit rates and higher visual quality. The default setting of MJPEG Q factor is 35; the setting range is from 1 to 70.

H.264-1/ H.264-2 bit rate

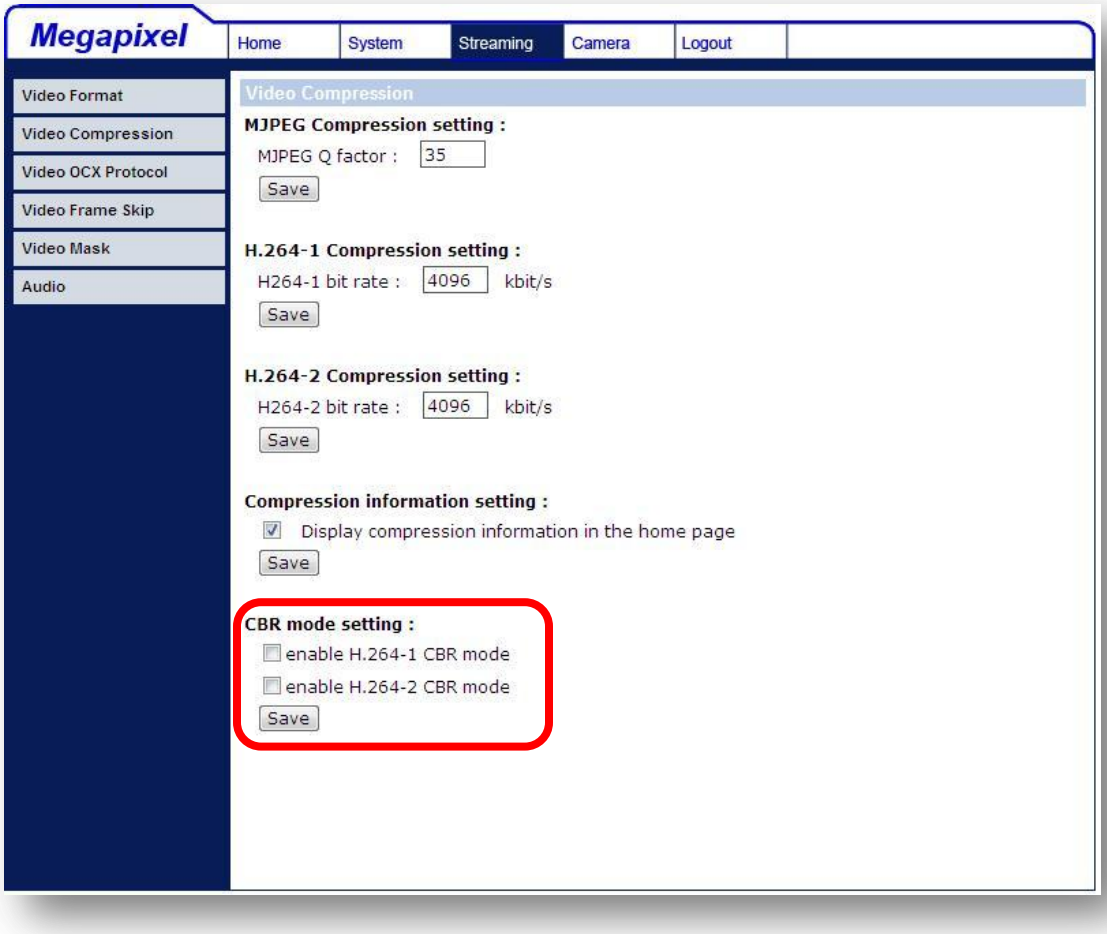
The default setting of H.264-1/ H.264-2 is 4096 kbps; the setting range is from 64 to 8192 kbps.

Display Compression Information

Users can also decide whether to display compression information on the Home page.

Click “Save” to confirm the setting.

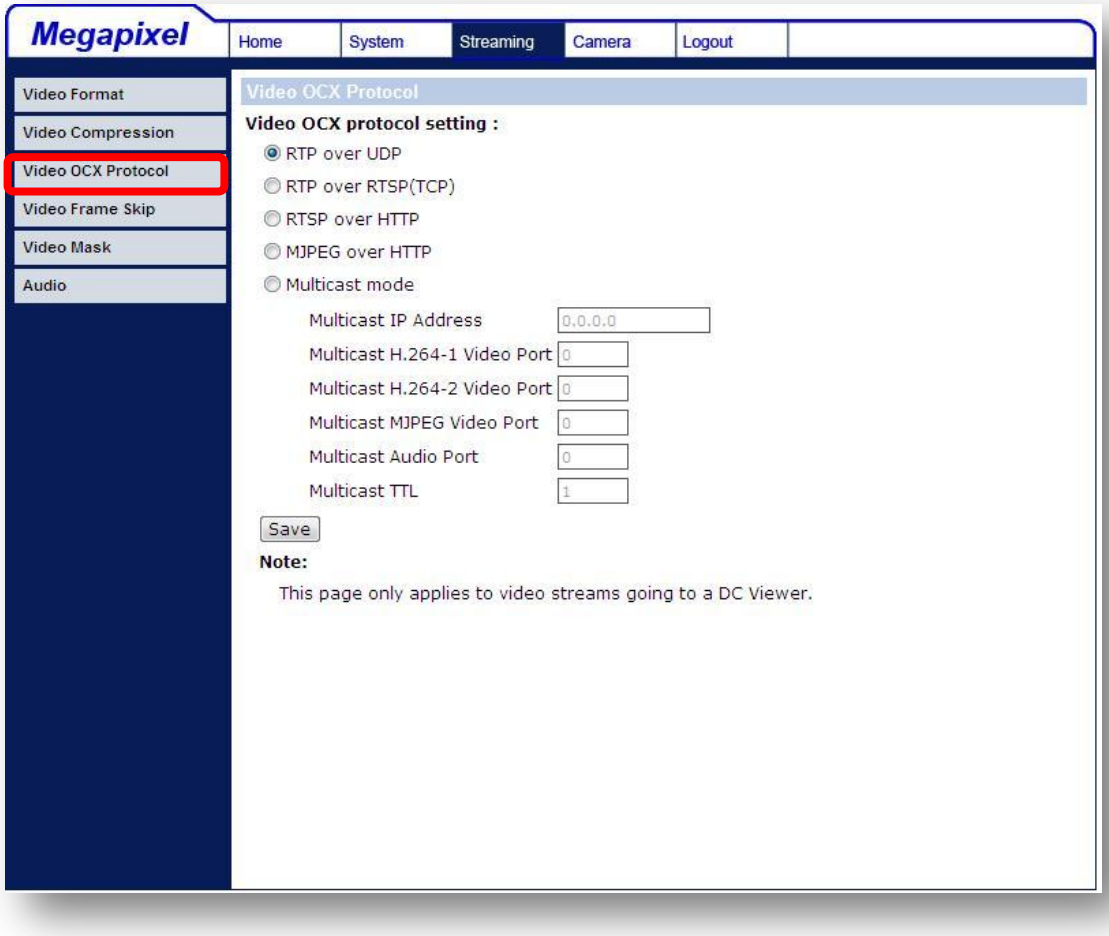
CBR Mode Setting



The CBR (Constant Bit Rate) mode could be the preferred bit rage mode if the bandwidth available is limited. It is important to take account of image quality while choosing to use CBR mode.

7.4.3 Video OCX Protocol

In the Video OCX protocol setting page, users can select RTP over UDP, RTP over TCP, RTSP over HTTP or MJPEG over HTTP, for streaming media over the network. In the case of multicast networking, users can select the Multicast mode. The page is shown as follows.



Video OCX protocol setting options include:

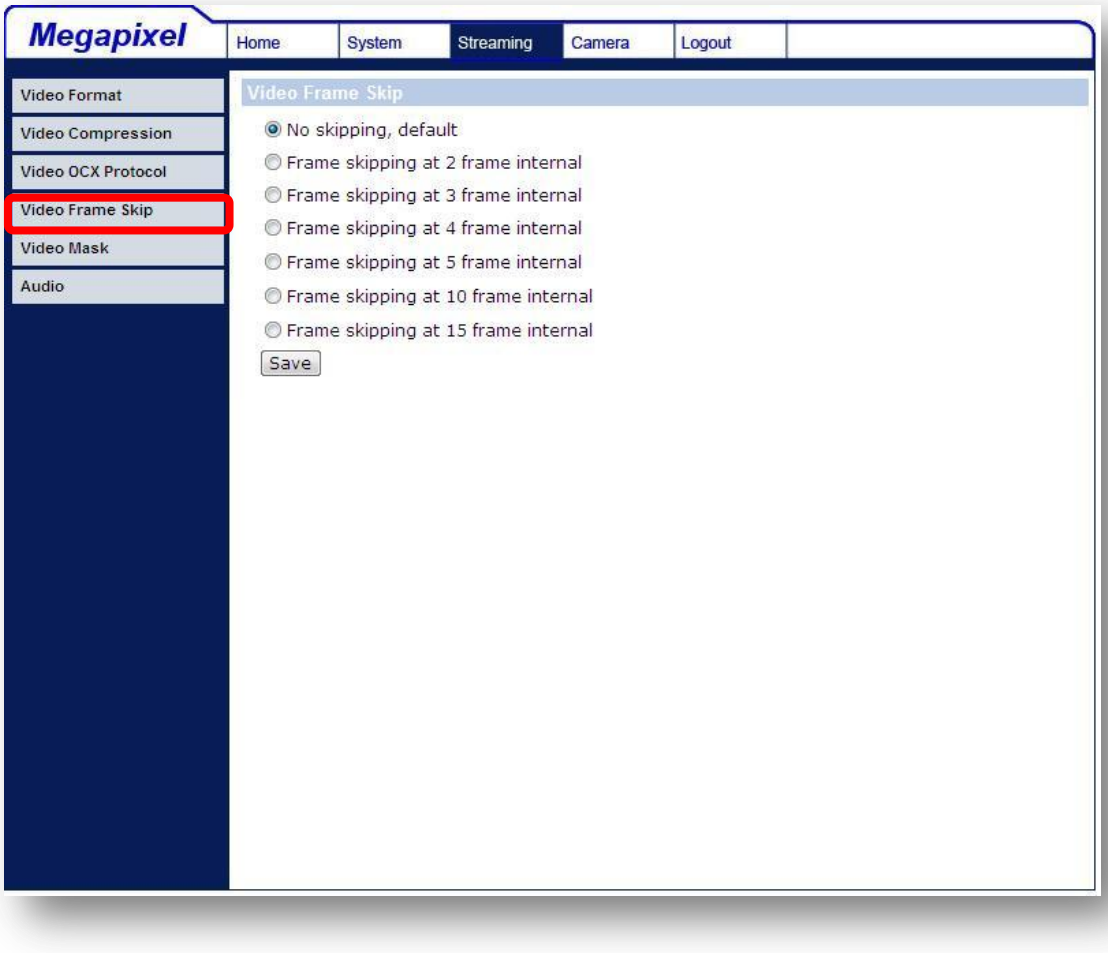
- RTP over UDP / RTP over RTSP(TCP) / RTSP over HTTP / MJPEG over HTTP

- Multicast Mode
  Enter all required data, including multicast IP address, H.264 video port, MJPEG video port, audio port and TTL into each blank.

Click “Save” to confirm the setting.

7.4.4 Video Frame Skip

Video frame skipping is for saving bandwidth, if necessary. The setting page is shown as below.



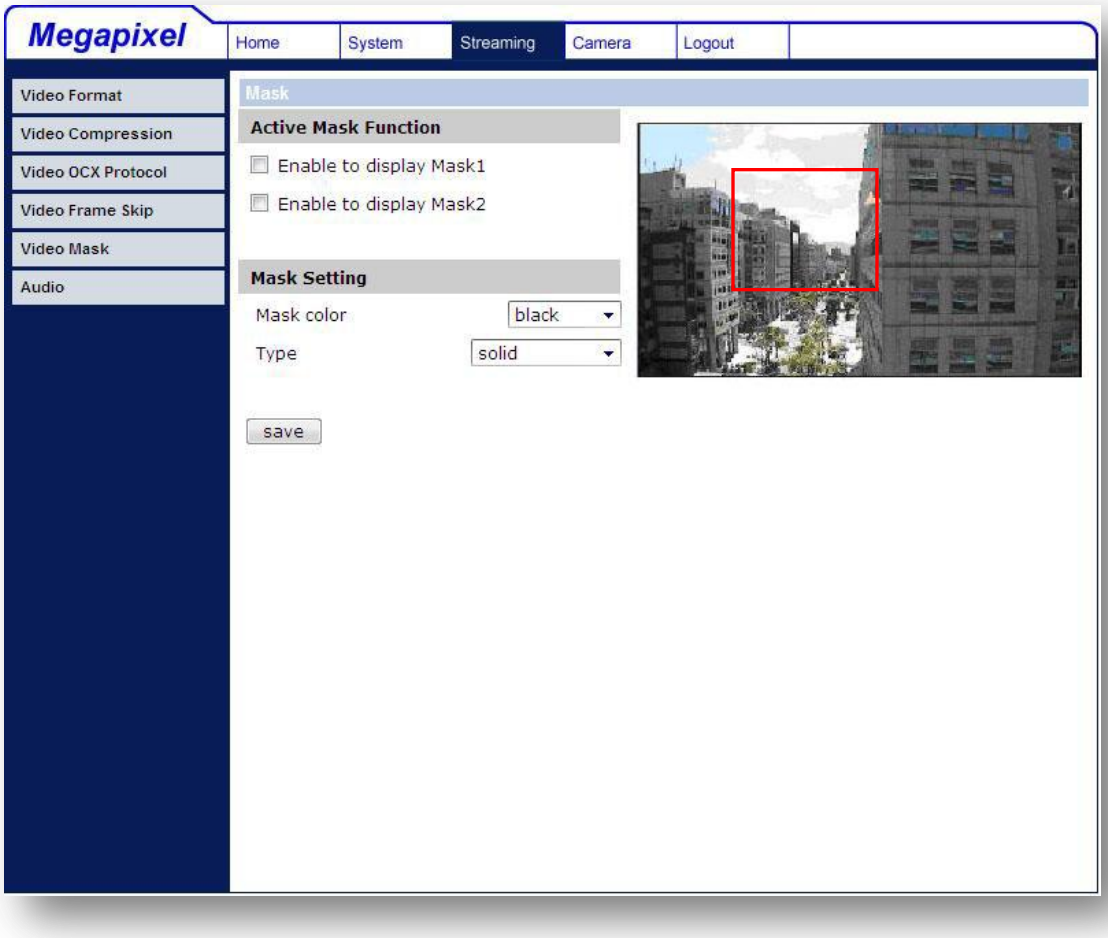
Video Frame Skip options include:

- No skipping, default
- Frame skipping at 2 frame internal
- Frame skipping at 3 frame internal
- Frame skipping at 4 frame internal
- Frame skipping at 5 frame internal
- Frame skipping at 10 frame internal
- Frame skipping to 15 frame internal

Click “Save” to confirm the setting.

NOTE: Higher frame skipping rate will decrease video smoothness.

7.4.5 Video Mask



Active Mask Function

- **Add a Mask**
  Check a Video Mask checkbox, and a red frame will come out in the Live Video pane at the right side. Use the mouse to drag and drop to adjust the mask's size and place it on the target zone.

NOTE: It is suggested to set the Video Mask twice bigger than the object.

- **Cancel a Mask**
  Uncheck the checkbox of the Video Mask meant to be deleted, and the selected mask will disappear from the Live Video pane instantly.

Mask Setting

- **Mask color**
  The selections of Mask color include red, black, white, yellow, green,

blue, cyan, and magenta.

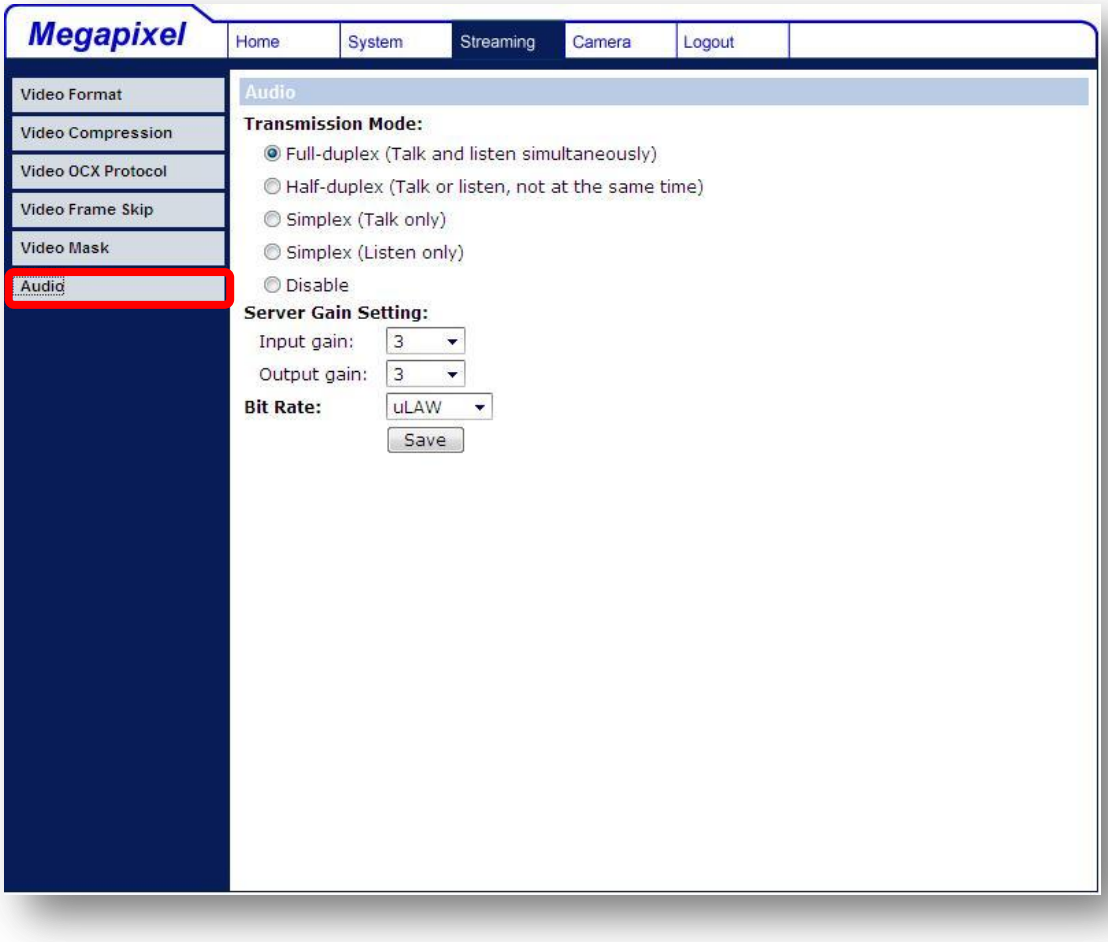
- **Type**

Select to change the mask type as solid or transparent.

Click “Save” to confirm the setting.

7.4.6 Audio Mode and Bit Rate Settings

The audio setting page is show as below. In the Audio page, the Administrator can select one transmission mode and audio bit rate.



Transmission Mode

- **Full-duplex (Talk and Listen simultaneously)**
  In the Full-duplex mode, the local and remote sites can communicate with each other simultaneously, i.e. both sites can speak and be heard at the same time.

- **Half-duplex (Talk or Listen, not at the same time)**

In the Half-duplex mode, the local/remote site can only talk or listen to the other site at a time.

- **Simplex (Talk only)**
  In the Talk only Simplex mode, the local/remote site can only talk to the other site.

- **Simplex (Listen only)**
  In the Listen only Simplex mode, the local/remote site can only listen to the other site.

- **Disable**
  Select the item to turn off the audio transmission function.

Server Gain Setting

Set the audio input/output gain levels for sound amplification. The audio gain values are adjustable from 1 to 6. The sound will be turned off if the audio gain is set to “Mute”.

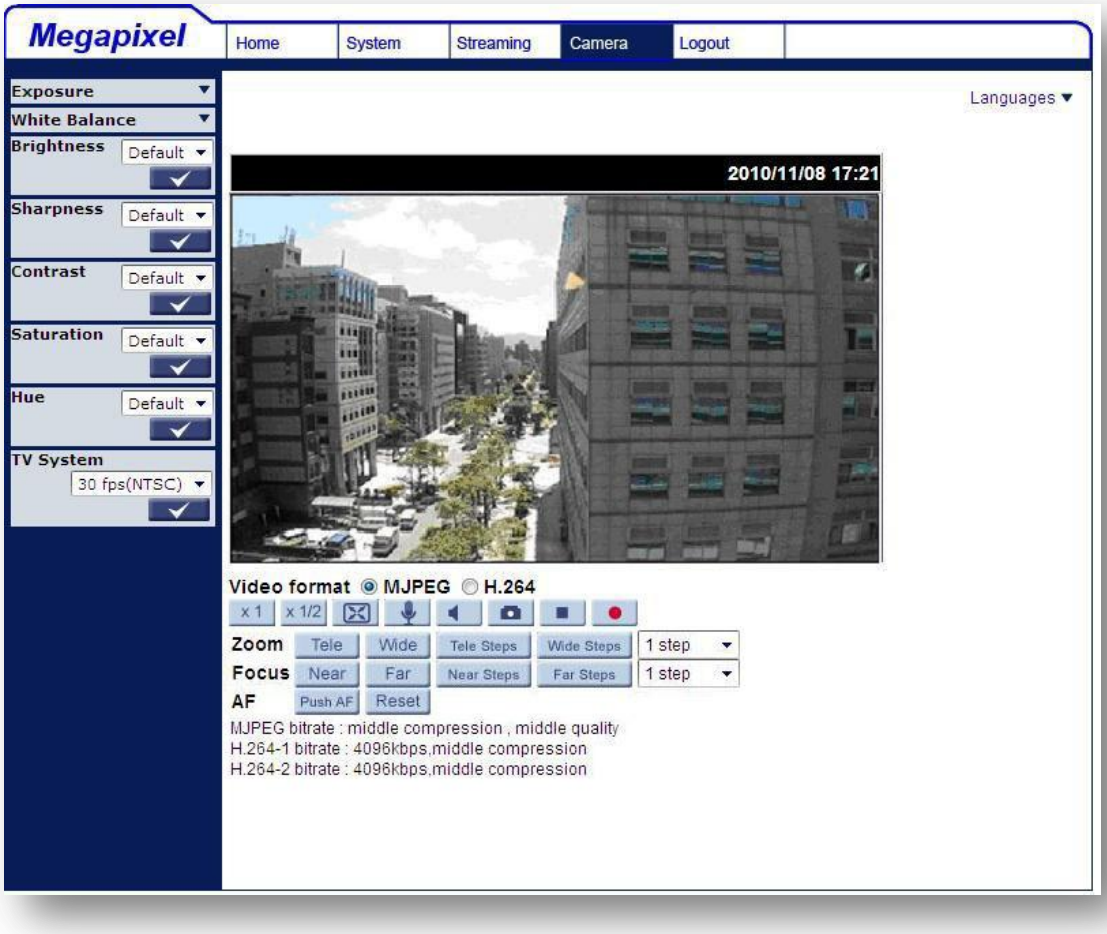
Bit Rate

Selectable audio transmission bit rate include 16 kbps (G.726), 24 kbps (G.726), 32 kbps (G.726), 40 kbps (G.726), uLAW (G.711) and ALAW (G.711). Both uLAW and ALAW signify 64 kbps but in different compression formats. Higher bit rate will let higher audio quality and require bigger bandwidth.

Click “Save” to confirm the setting.

7.5 Camera Settings

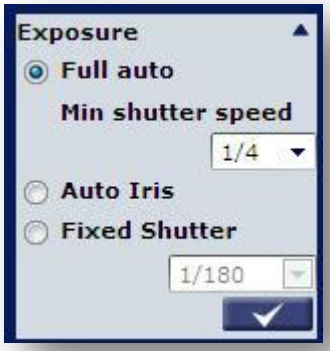
The figure below is the camera configuration page. Details of each parameter setting are described in the following subsections.



NOTE: Please note that the function buttons will vary depending on the camera model.

7.5.1 Exposure Setting

The Exposure pull-down menu is shown as follows:



The exposure is the amount of light received by the image sensor and is determined by the width of lens diaphragm opening, the amount of exposure by the sensor (shutter speed) and other exposure parameters. With this item, users can define how the Auto Exposure function works.

Each exposure mode is specified as follows:

Full Auto Mode

In this mode, the camera's Shutter Speed, IRIS and AGC (Auto Gain Control) control circuits work together automatically to get consistent video output level.
The shutter speed range is from 1 (1/1.5) to 1/30 (1/25) sec. with 6 (5) options. Users could select suitable shutter speed according to the environmental illuminance.

NOTE: The minimum shutter speed set in the Full Auto Mode will be applied to **Auto Iris Mode**.

Auto Iris

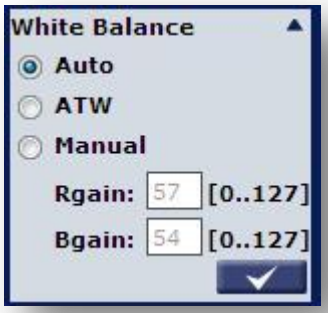
In this mode, the exposure gives priority to the auto iris. Shutter speed and AGC circuit will function automatically in cooperating with IRIS to get consistent exposure output.

NOTE: The minimum shutter speed will vary depending on the setting in **Full Auto Mode**.

Fixed Shutter Mode
In this mode, fixed shutter speed could be selected from the dropdown menu. The shutter speed range is from 1/10000 to1 (1/1.5) sec. with 19 (18) options. Users could select suitable shutter speed according to the environmental illuminance.

7.5.2 White Balance Setting

The White Balance pull-down menu is shown as follows:



A camera needs to find reference color temperature, which is a way of measuring the quality of a light source, for calculating all the other colors. The unit for measuring this ratio is in degree Kelvin (K). Users can select one of the White Balance Control modes according to the operating environment. The following table shows the color temperature of some light sources for reference.

Light Sources	Color Temperature in K
Cloudy Sky	6,000 to 8,000
Noon Sun and Clear Sky	6,500
Household Lighting	2,500 to 3,000
75-watt Bulb	2,820
Candle Flame	1,200 to 1,500

Auto Mode
The Auto Balance White mode is suitable for environment with light source having color temperature in the range roughly from 2700 ~ 8000K.

ATW Mode (Auto Tracking White Balance)
With Auto Tracking White Balance function, the white balance in a scene will be automatically adjusted while temperature color is changing. The ATW Mode is suitable for environment with light source having color temperature in the range roughly from 2450 ~ 10500K.

Manual Mode

In this mode, users can change the White Balance value manually. Users can select a number between 0 ~127 of “Rgain/ Bgain” item to gain the red/ blue illuminant on the Live Video Pane. Press < √ > to confirm the new setting.

7.5.3 Brightness Setting

Users can adjust the image’s brightness by adjusting the item. To increase video brightness, select a bigger number. Press < √ > to confirm the new setting.

7.5.4 Sharpness Setting

Increasing the sharpness level can make the image looked sharper; especially enhance the object’s edge. Press < √ > to confirm the new setting.

7.5.5 Contrast Setting

Camera image contrast level is adjustable; please select ranging from -6 to +19. Press < √ > to confirm the new setting.

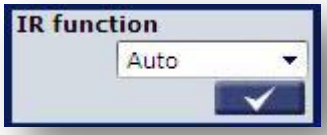
7.5.6 Saturation Setting

Camera image saturation level is adjustable; please select ranging from -6 to +19. Press < √ > to confirm the new setting.

7.5.7 Hue Setting

Camera image hue level is adjustable; please select ranging from -12 to +13. Press < √ > to confirm the new setting.

7.5.8 IR Function



Auto/On/Off Mode
With the IR cut filter, the Dome Camera can still catch clear image at night time or in low light conditions.

For the camera with the built-in IR LED module, there will be three additional IR function modes as follows:

Light Sensor Mode
IR LED lights will be turned on/off depending on the light sensor.

Light On Mode
In this mode, IR LED lights will be always on.

Light Off Mode
In this mode, IR LED lights will be always off.

Press < √ > to confirm the new setting.

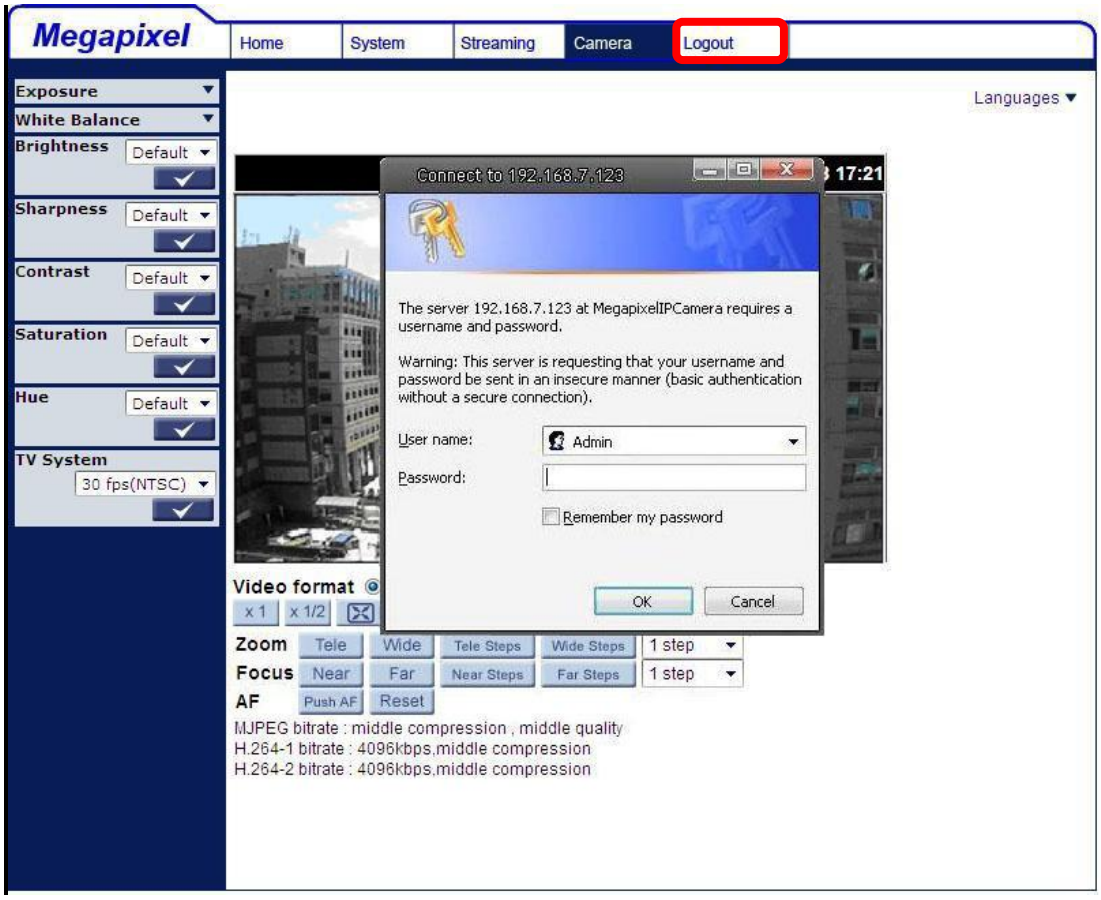
7.5.9 TV System Setup

Select the video format that matches the present TV system. Press < √ > to

confirm the new setting.

7.6 Logout

Press the tab “Logout” in the top of the page, and the login window will pop up. This enables login with another user name.



8. CMS SOFTWARE INTRODUCTION

The IP Camera bundles Central Management System (CMS) software. Offering powerful functionalities via intuitive interface, it is a centralized monitoring solution of your video surveillance equipments.

It gives the user access to monitor multiple IP Cameras and Digital Video Recorders (DVRs), and allows the user to simultaneously monitor 16 sites per group (up to 10 groups) within several clicks.

For further information on CMS software, please refer to the supplied CD.

Note: The free bundle CMS is a function-limited software. For additional features, please purchase a licensed CMS.

APPENDIX A: TECHNICAL SPECIFICATIONS

Camera		**Full HD Real-time**	**Full HD**
Image Sensor		1/2.5” Progressive CMOS	
Effective Pixels		1920(H) x 1080(V)	
Minimum Illumination	Color	0.2 lux @ F1.4	0.2 lux @ F1.4
	B/W	0.02 lux @ F1.4	0.02 lux @ F1.4
Shutter Speed		1~ 1/10000 sec.	
White Balance		Manual / AWB/ ATW	
Lens			
Lens Type	Varifocal lens/ Motorized lens	F 1.4 / f = 3.3~12 mm	
FOV		21°~71°	
Operation			
Video Compression		H.264/ MJPEG	
Video Streaming		Simultaneous	H.264 + MJPEG
			H.264 + H.264
Resolution	H.264	Full HD 1080p/ HD 720p/ SXGA/ D1/ VGA/ QVGA/ CIF	
	MJPEG	Full HD 1080p/ HD 720p/ SXGA/ D1/ VGA/ QVGA/ CIF	
Frame Rate		Full HD 25/30 fps	HD 25/30 fps Full HD 15 fps
Image Setting	Brightness	Manual	
	Exposure	Auto / Manual	
	Sharpness	Manual	
	Contrast	Manual	
	White Balance	Auto / Manual	
	Saturation	Manual	
	Hue	Manual	
	Digital Zoom	Support	
	Motion detection	On/Off	
	Privacy Mask	Support	
	Privacy Mask Type	Transparent, Color	
	ICR (Optional)	Auto/ On/ Off	
	Tampering Alarm	On/Off	

Audio	Two-way Audio	Line out, Line in/ mic in
	Compression	G.711/G.726
Alarm	Input	5V 10kΩ pull up
	Output	Photo Relay Output 300V DC/AC
Event Notification		HTTP, FTP, SMTP
Multiple Languages		English, French, German, Italian, Korean, Simplified Chinese, Russian, Korean
Network		
Interface		10/100Mbps Ethernet (RJ-45)
Protocol		IPv4/ v6, TCP/IP, UDP, RTP, RTSP, HTTP, HTTPS, ICMP,FTP, SMTP, DHCP, PPPoE, UPnP, IGMP, SNMP, QoS, and ONVIF
Password Levels		User and Administrator
Security		HTTPS, IP Filter
Internet Browser		Internet Explorer (6.0+), Chrome, Firefox, Safari
User Account		20
Mechanical		
Built-in IR Illuminator (Optional)	Working distance	up to 30m
	Wavelength	850nm
	Number of LEDs	23
Connectors	Power	3 pins terminal block
	Ethernet	RJ-45
	Micro SD	SDHC support
	Audio	4 pins terminal block
	Alarm	4 pins terminal block
	Analog Video	1.0 Vp-p / 75 Ω, BNC
LED Indicator		Power, Link, ACT
General		
Operating Temperature		-10°C ~ 50°C -35°C ~ 50°C with Heater & Fan Humidity: 10% to 90%, no condensation
Power Source		DC12V/ AC24V/ PoE
Power Consumption		System: 5.5W
Regulatory		CE, FCC, RoHS Compliant
Dimension	Indoor	151 x 130 mm (5.9 x 5.1 inches)

	Outdoor	⌀ 170 x 210 mm (⌀ 6.7 x 8.3 inches)
Weight	Indoor	0.8 kg (1.8 lbs)
	Outdoor	1.3 kg (2.9 lbs)

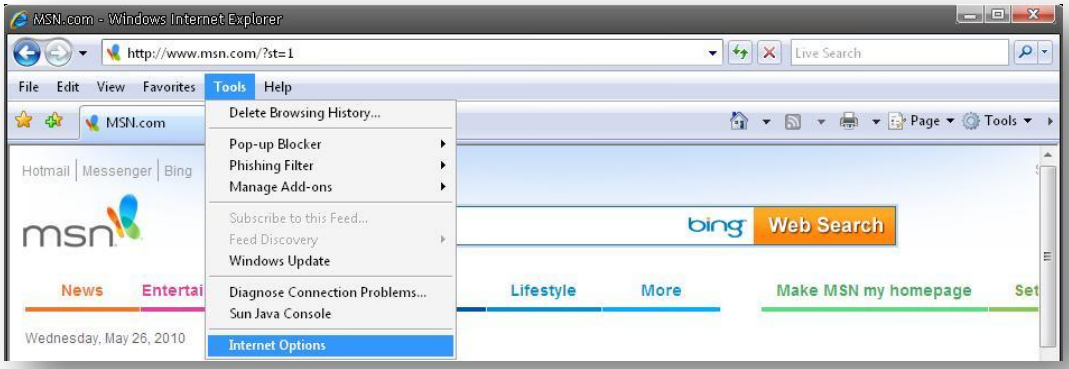
APPENDIX B: INTERNET SECURITY SETTINGS

If ActiveX control installation is blocked, please either set Internet security level to default or change ActiveX controls and plug-ins settings.

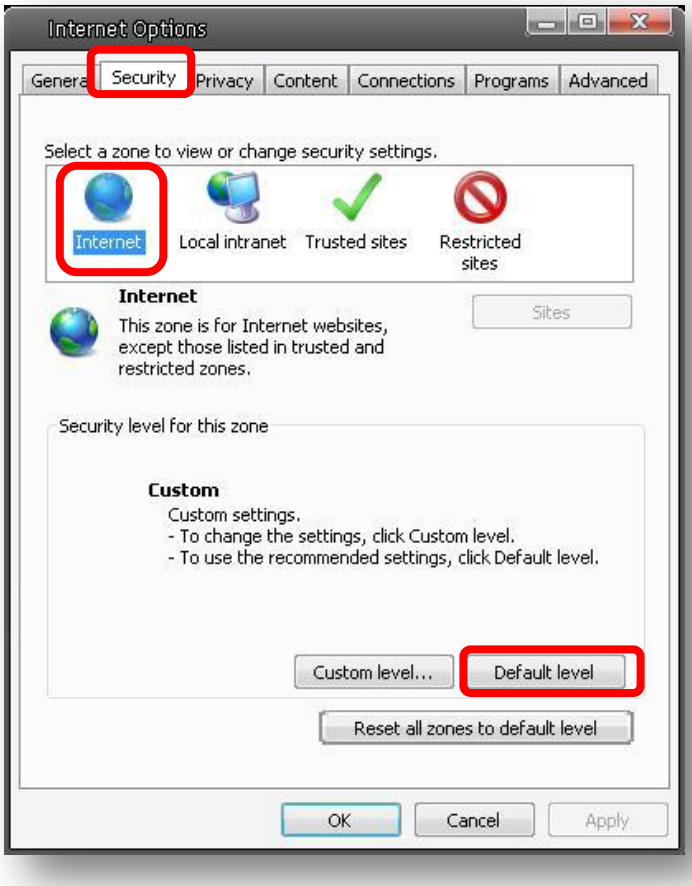
Internet Security Level: Default

Step 1: Start the Internet Explorer (IE).

Step 2: Select <Tools> from the main menu of the browser. Then Click <Internet Options>.



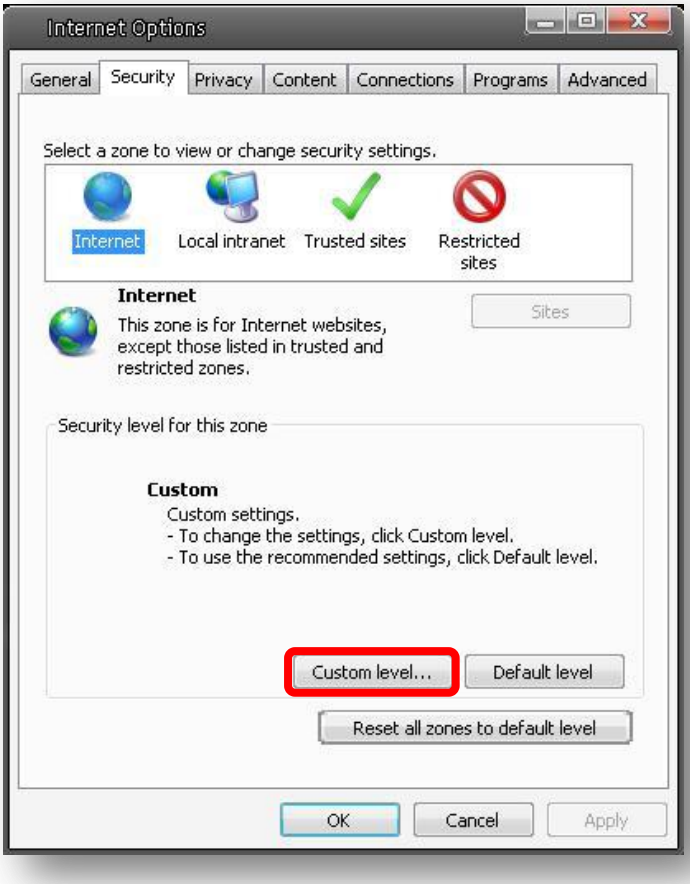
Step 3: Click the <Security> tab, and select <Internet>.


Internet Options
Genera
Security
Privacy
Content
Connections
Programs
Advanced
Select a zone to view or change security settings.
Internet
Local intranet
Trusted sites
Restricted sites
Internet
This zone is for Internet websites, except those listed in trusted and restricted zones.
Sites
Security level for this zone
Custom
Custom settings.
- To change the settings, click Custom level.
- To use the recommended settings, click Default level.
Custom level...
Default level
Reset all zones to default level
OK
Cancel
Apply

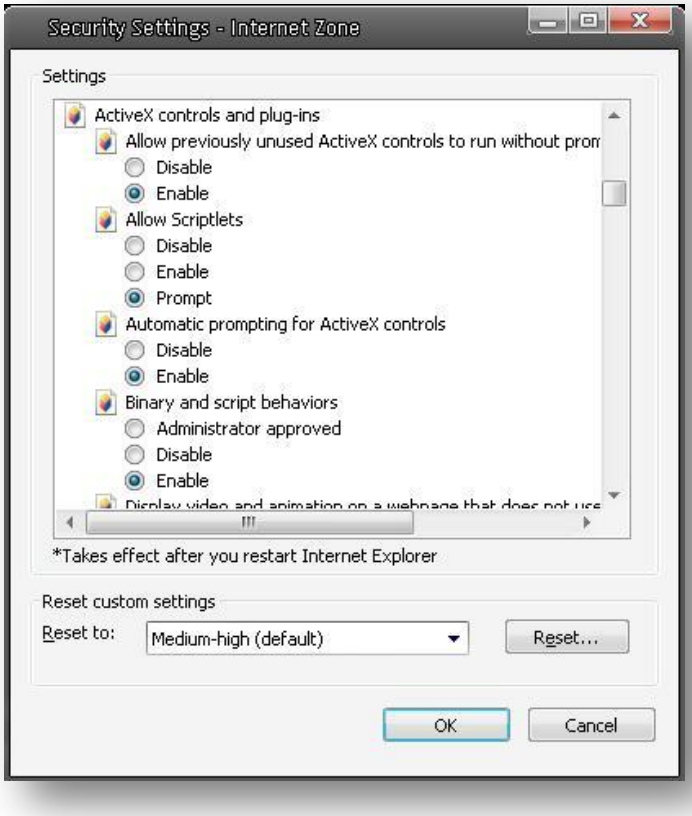
Step 4: Down the page, press “Default Level” (see the figure above) and click “OK” to confirm the setting. Close the browser window, and open a new one later when accessing the IP Camera.

ActiveX Controls and Plug-ins Settings

Step 1~3: Refer to the previous section above.
Step 4: Down the page, press “Custom Level” (see the figure below) to change ActiveX controls and plug-ins settings.



The Security Settings screen is displayed as below:



Step 5: Under “ActiveX controls and plug-ins”, set ALL items (as listed below) to <Enable> or <Prompt>. Please note that the items vary by IE version.

ActiveX controls and plug-ins settings:

1. Allow previously unused ActiveX controls to run without prompt.
2. Allow Scriptlets.
3. Automatic prompting for ActiveX controls.
4. Binary and script behaviors.
5. Display video and animation on a webpage that does not use external media player
6. Download signed ActiveX controls
7. Download unsigned ActiveX controls
8. Initialize and script ActiveX controls not marked as safe for

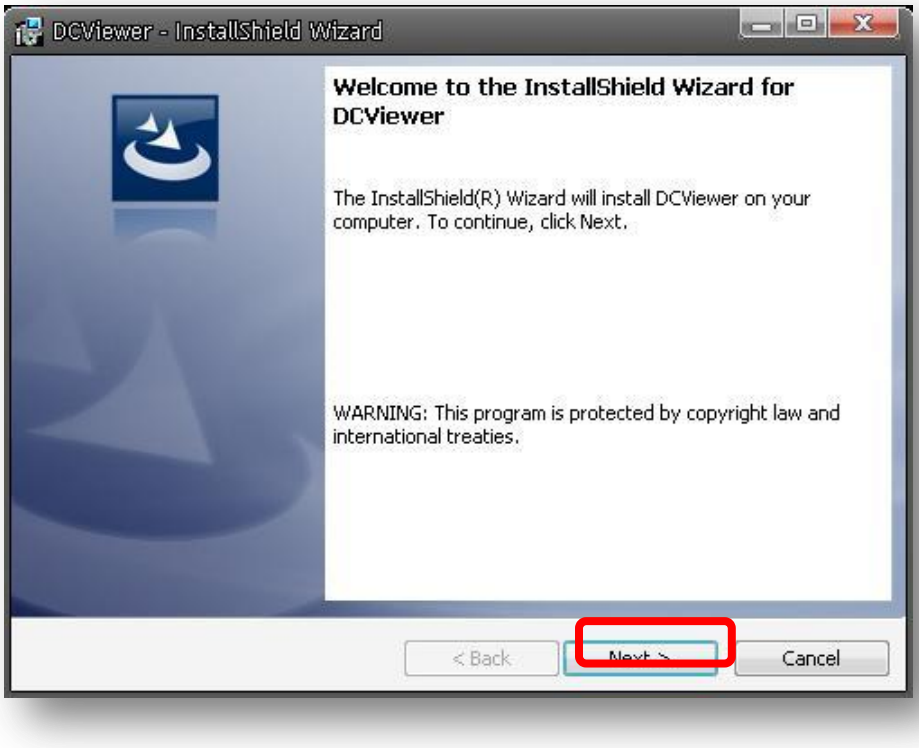
scripting
9. Run ActiveX controls and plug-ins
10. Script ActiveX controls marked safe for scripting

Step 6: Click <OK> to accept the settings and close the <Security> screen.
Step 7: Click <OK> to close the Internet Options screen.
Step 8: Close the browser window, and restart a new one later for accessing the IP Camera.

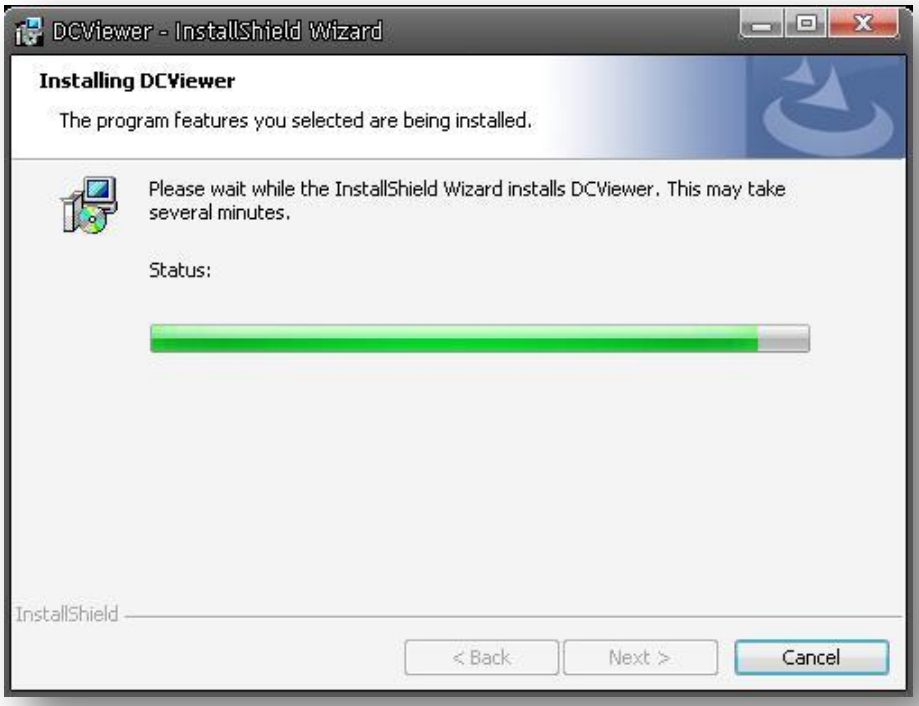
APPENDIX C: DC VIEWER DOWNLOAD PROCEDURE

The procedure of DC Viewer software download is specified as follows.

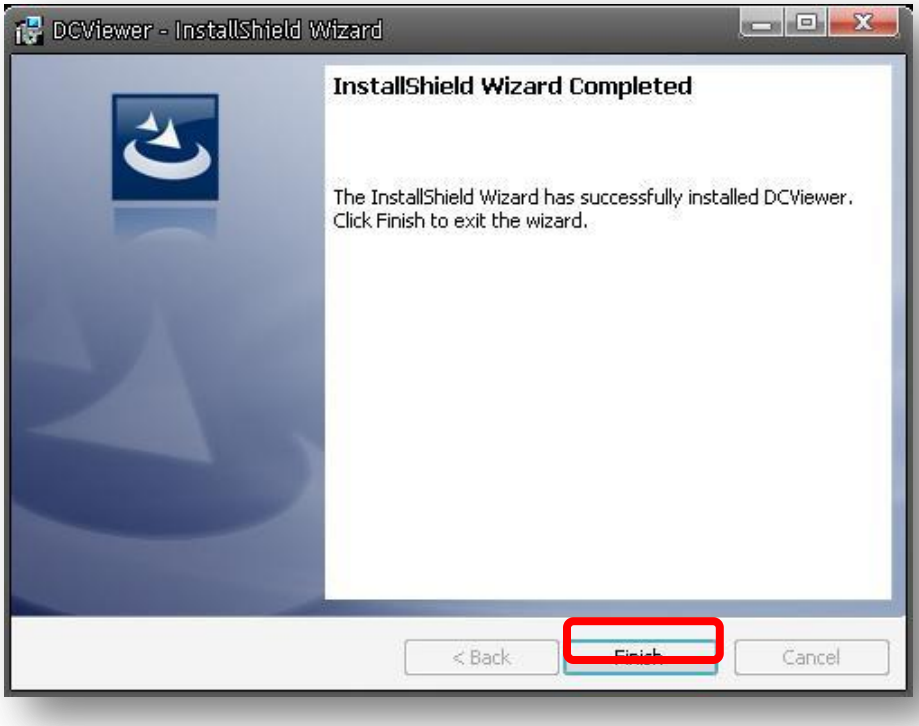
Step 1: In the DC Viewer installation page, click “Next” for starting installing.



Step 2: Setup starts. Please wait for a while until the loading bar runs out.



Step 3: Click “Finish” to close the DC Viewer installation page.

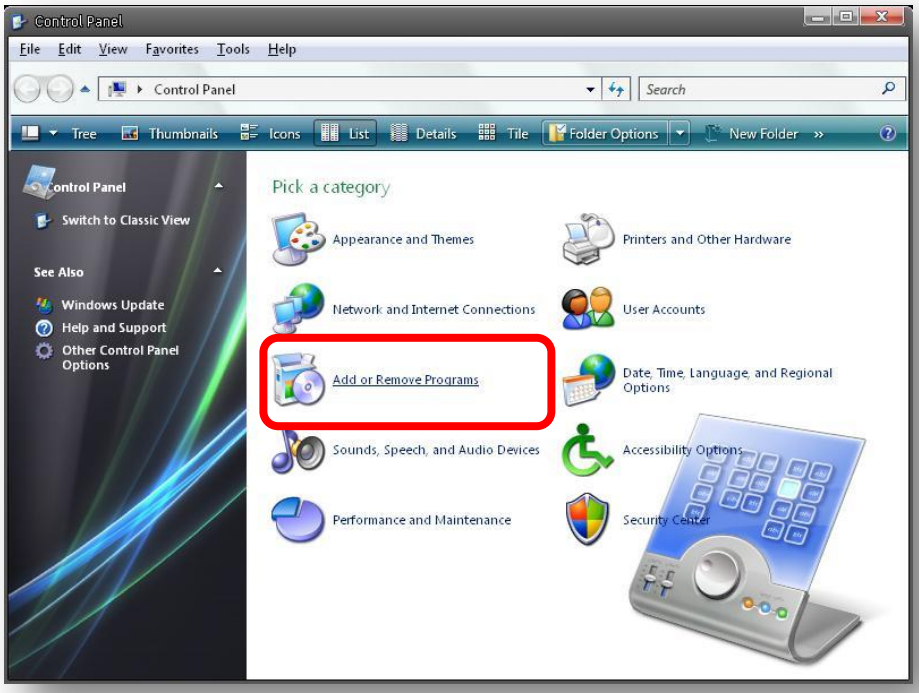


Then, the IP Camera's Home page will display as follows:

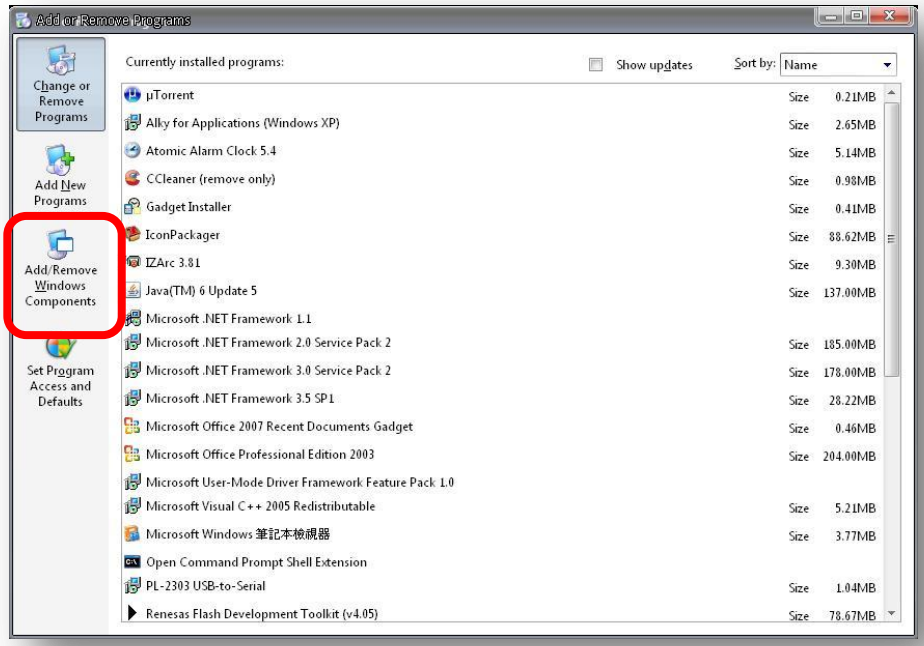
APPENDIX D: INSTALL UPNP COMPONENTS

Please follow the instructions below to install UPnP components.

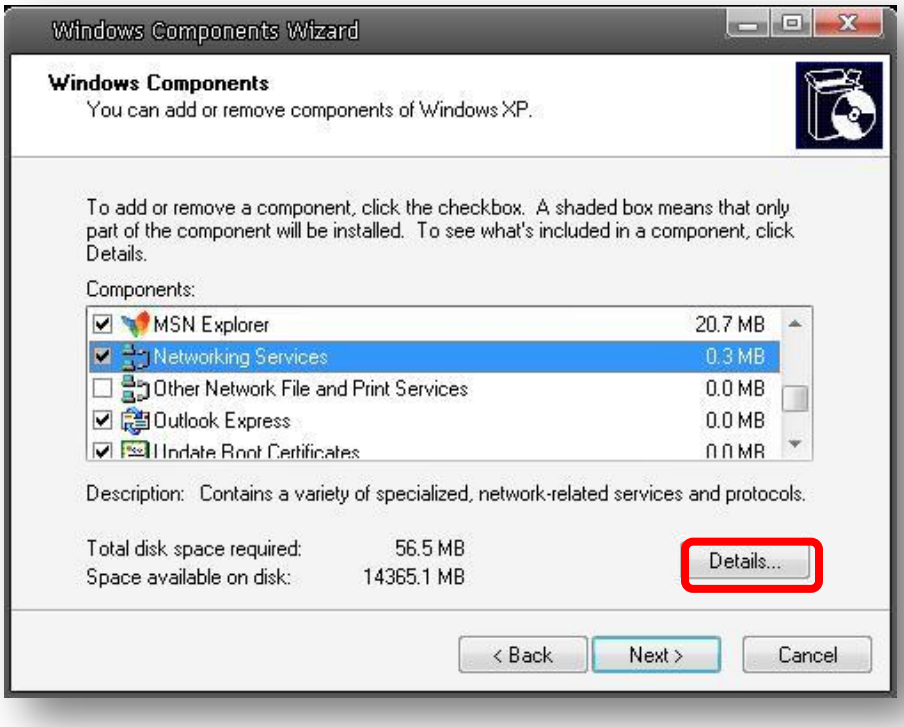
Step 1: Go to “Start”, click on “Control Panel”, and then double click “Add or Remove Programs”.



Step 2: Click on “Add/Remove Windows Components” in the Add or Remove Programs page.

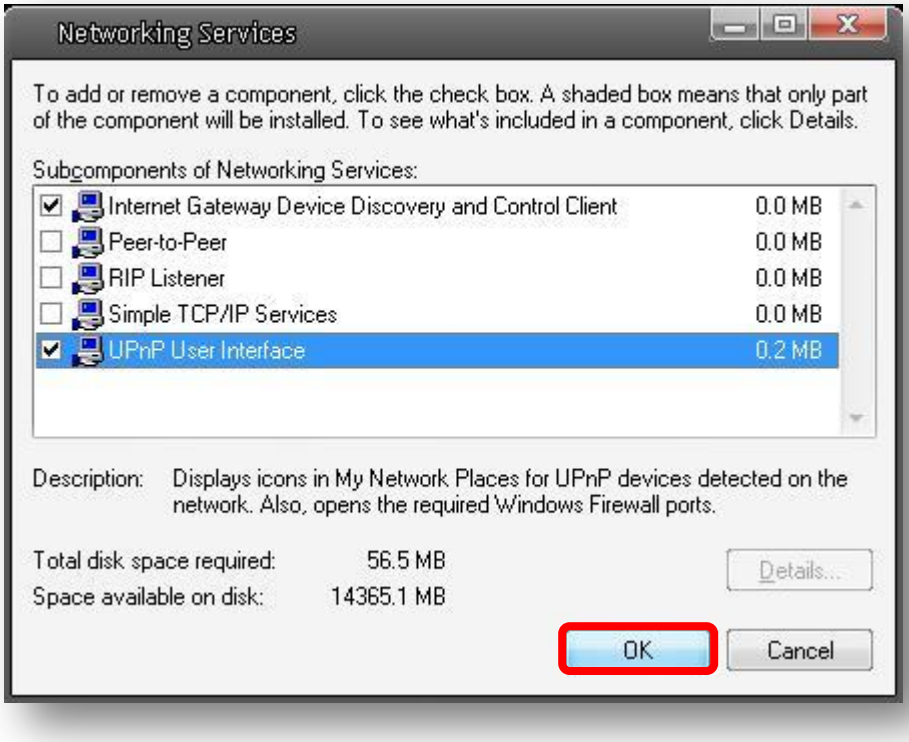


Step 3: Select “Networking Services” from the Components list in the Windows Components Wizard window, and then click “Details”.

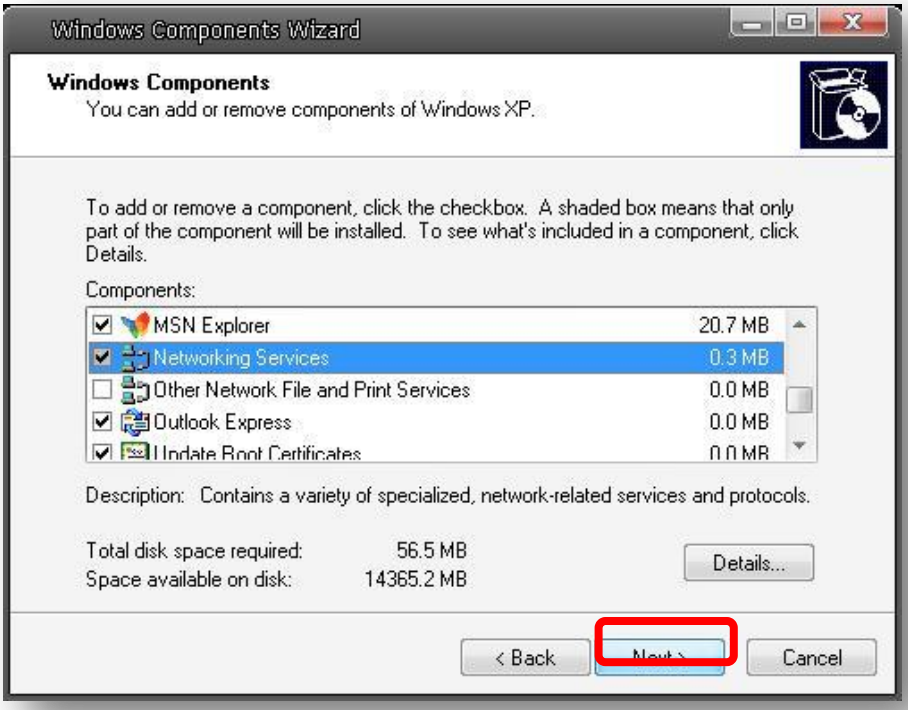


Step 4: Select “UPnP User Interface” in the Networking Services’

subcomponents list and then click “OK”.



Step 5: Click “Next” in the Windows Components Wizard page.



Step 6: Click “Finish” to complete installation.

Windows Components Wizard
Completing the Windows Components Wizard
You have successfully completed the Windows Components Wizard.
To close this wizard, click Finish.
< Back
Finish

COPYRIGHT © 2010. All rights reserved.

No part of this document may be reproduced, republished, or retransmitted in any form or by any means whatsoever, whether electronically or mechanically, including, but not limited to, by way of photocopying, recording, information recording, or through retrieval systems without the express written permission of the owner. Product specifications contained in this document are subject to change without notice. All other company or product names mentioned are used for identification purposes only and may be trademarks of their respective owners.

Manufacturer:

ALLNET GmbH

ALLNET Deutschland GmbH
Maistrasse 2
82110 Germering
Tel. +49 89 894 222 22
Fax +49 89 894 222 33
email: info@allnet.de

Konformitätserklärung
Declaration of Conformity

Hersteller / Manufacturer:	ALLNET GmbH
Produkt / Product:	ALL2295
Typ / Type:	Full HD Real-time Vandal Proof IP Dome Camera

CE

Report No. : E081901

The equipment beyond was tested by Global Certification Corp. for compliance with the requirements set forth in the European Council Directive 2004/108/EC and the technical standards mentioned above. The results of testing in this report apply only to the product/system, which was tested. Other similar equipment will not necessarily produce the same results due to production tolerance. This test report shall not be reproducing in part without written approval of Global Certification Corp.

Getestete Normen:
tested norms:

AS/NZS CISPR 22: 2006
EN 55022 CLASS A: 2006+A1:2007
EN61000-3-2:2006
EN61000-3-3:1995+A1:2001*A2:2005
AS/NZS CISPR 24:2006
EN50130-4:1995+A1:1998+A2:2003
IEC 61000-4-2:2001
IEC 61000-4-3:2008
IEC 61000-4-4:2004
IEC 61000-4-5:2005
IEC 61000-4-6:2008
IEC 61000-4-8:2009
IEC 61000-4-11:2004

ALLNET®

Germering, February 17, 2011

Anschrift:	Allnet GmbH Maistraße 2 82110 Germering Germany
E-Mail:	info@allnet.de support@allnet.de
Phone:	+49 (0)89 894 222 22
Fax:	+49 (0)89 894 222 33